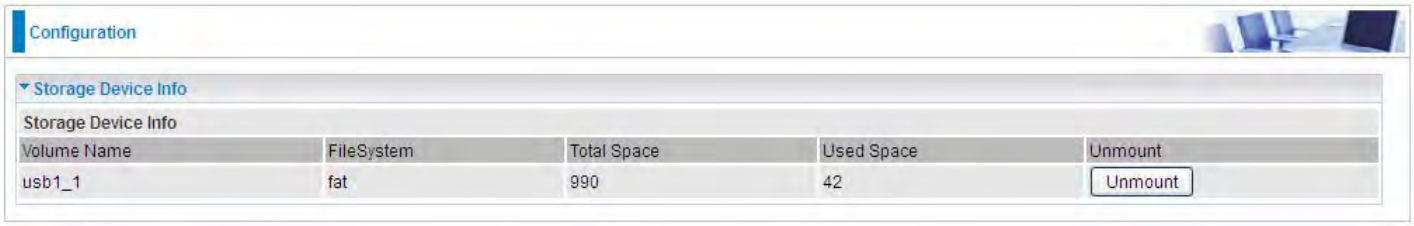
USB

Storage here refers to network sharing in the network environment, USB devices act as the storage carrier for **DLNA**, NAS (**Samba server, FTP server**).

Storage Device Info

This part provides users direct access to the storage information like the total volume, the used and the remaining capacity of the device.



Volume Name: Display the storage volume name

FileSystem: Display the storage device's file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

Used Space: Display the remaining space of each partition, unit MB.

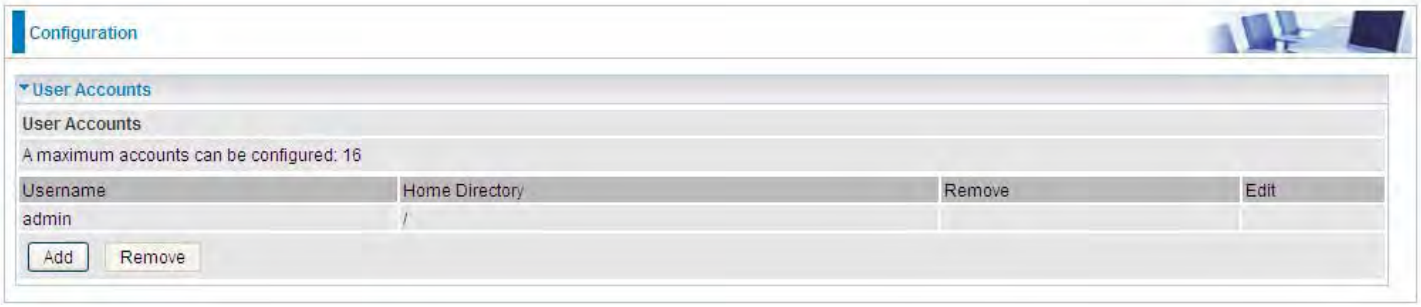
Unmount: Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

User Account

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Users added here are entitled to have access to both **Samba server** and **FTP server**.

Default user admin.



Click **Add** button, enter the user account-adding page:

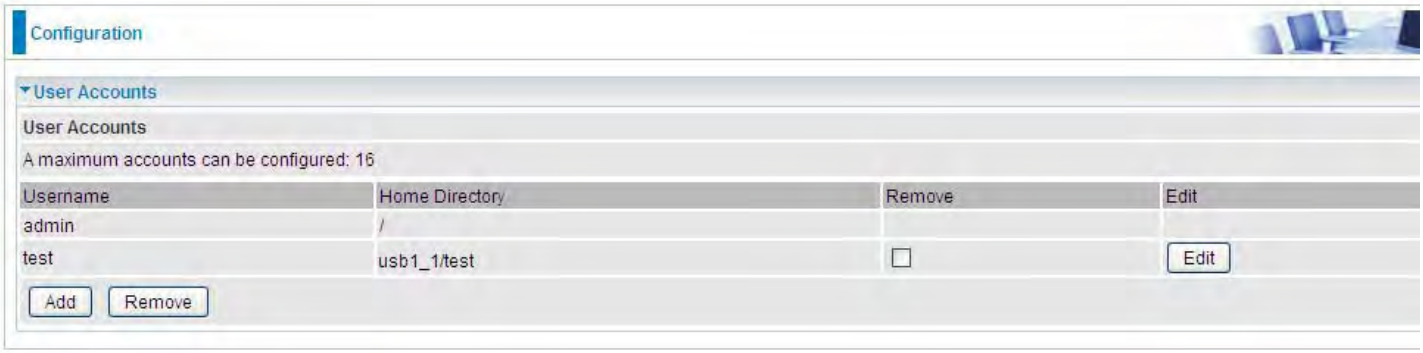
Username: user-defined name, but simpler and more convenient to remember would be favorable.

Password: Set the password.

Confirm Password: Reset the password for confirmation.

Volume Name: Select Volume name, as to create access to the volume of the specified partition of the storage.

For example, a user ***test*** is setup behind the usb1_1.



The user “test” has the right to access both **Samba** and **FTP server**.

How to access Samba:

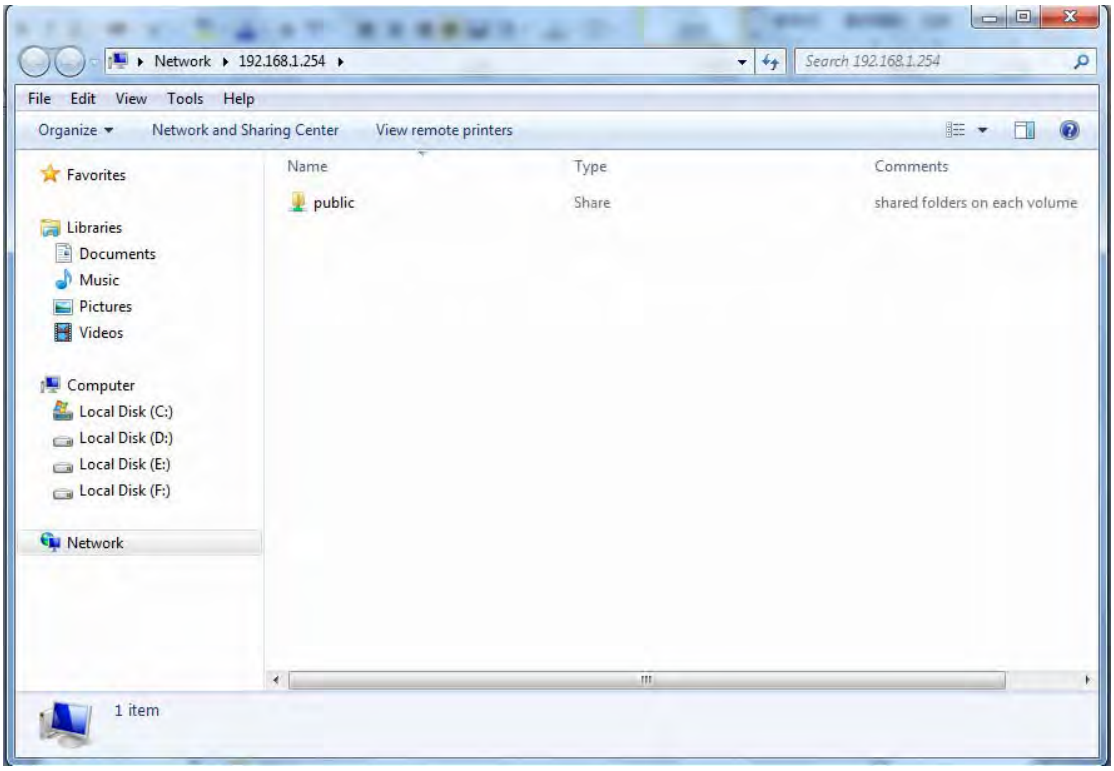
In your computer, Click **Start** > **Run**, enter \\192.168.1.254 (LAN IP)

When accessing the network storage, you can see a folder named “***public***”, users should have the account to enter, and the account can be set at the User Accounts section.

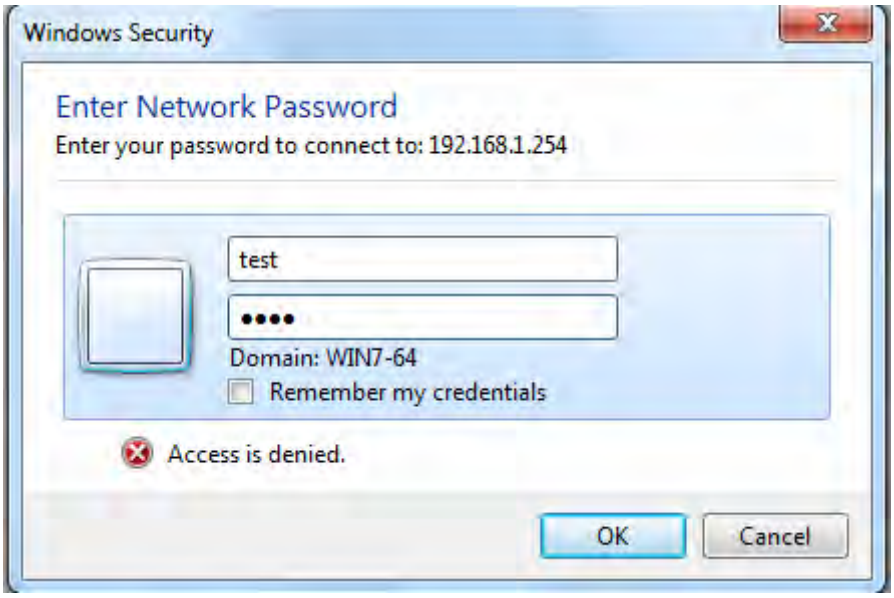
When first logged on to the network folder, you will see the “***public***” folder.

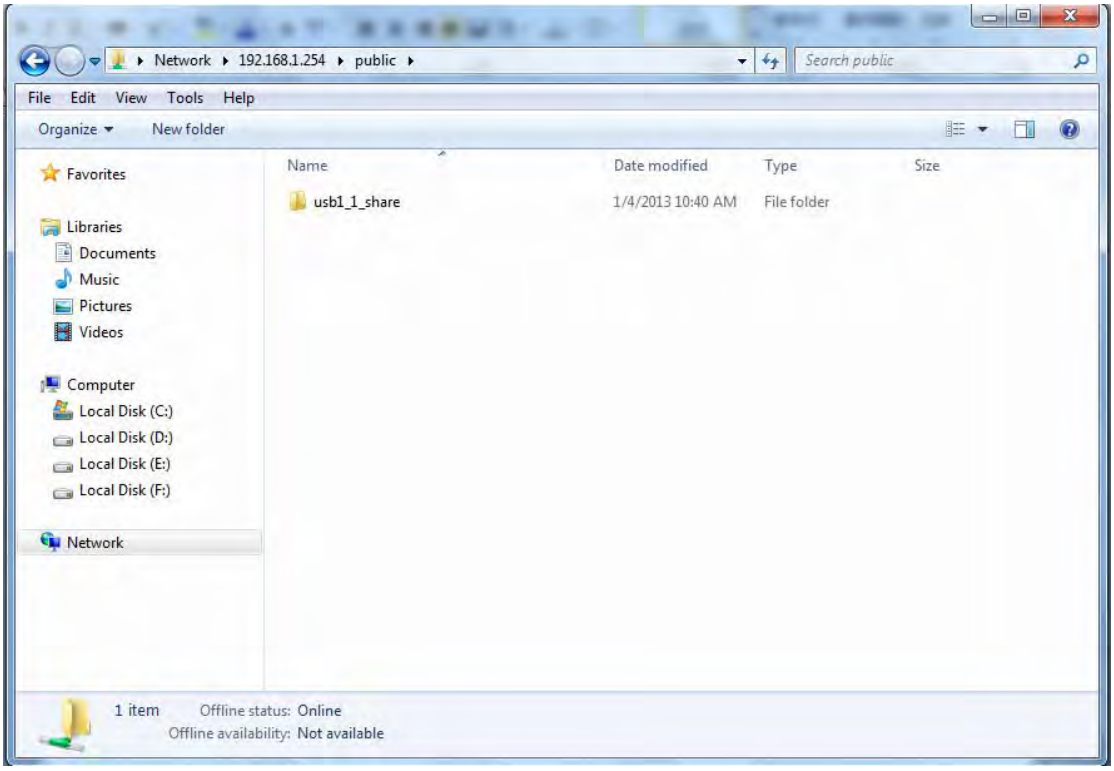
Public: The public sharing space for each user in the USB Storage.

When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.

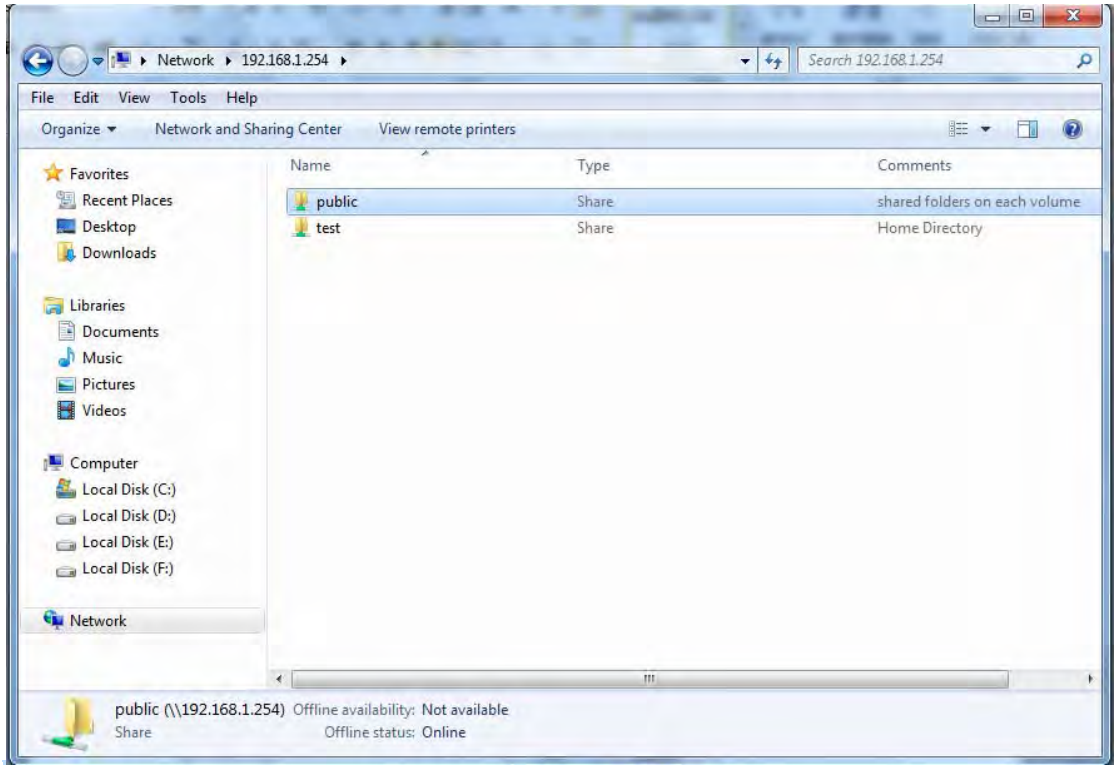


Access the folder ***public***.





When successfully accessed, the private folder of each user is established, and user can see from the following picture. The ***test*** fold in the picture is the private space for each user.



How to use FTP:
Please **note** to enable remote FTP access in Remote Access.

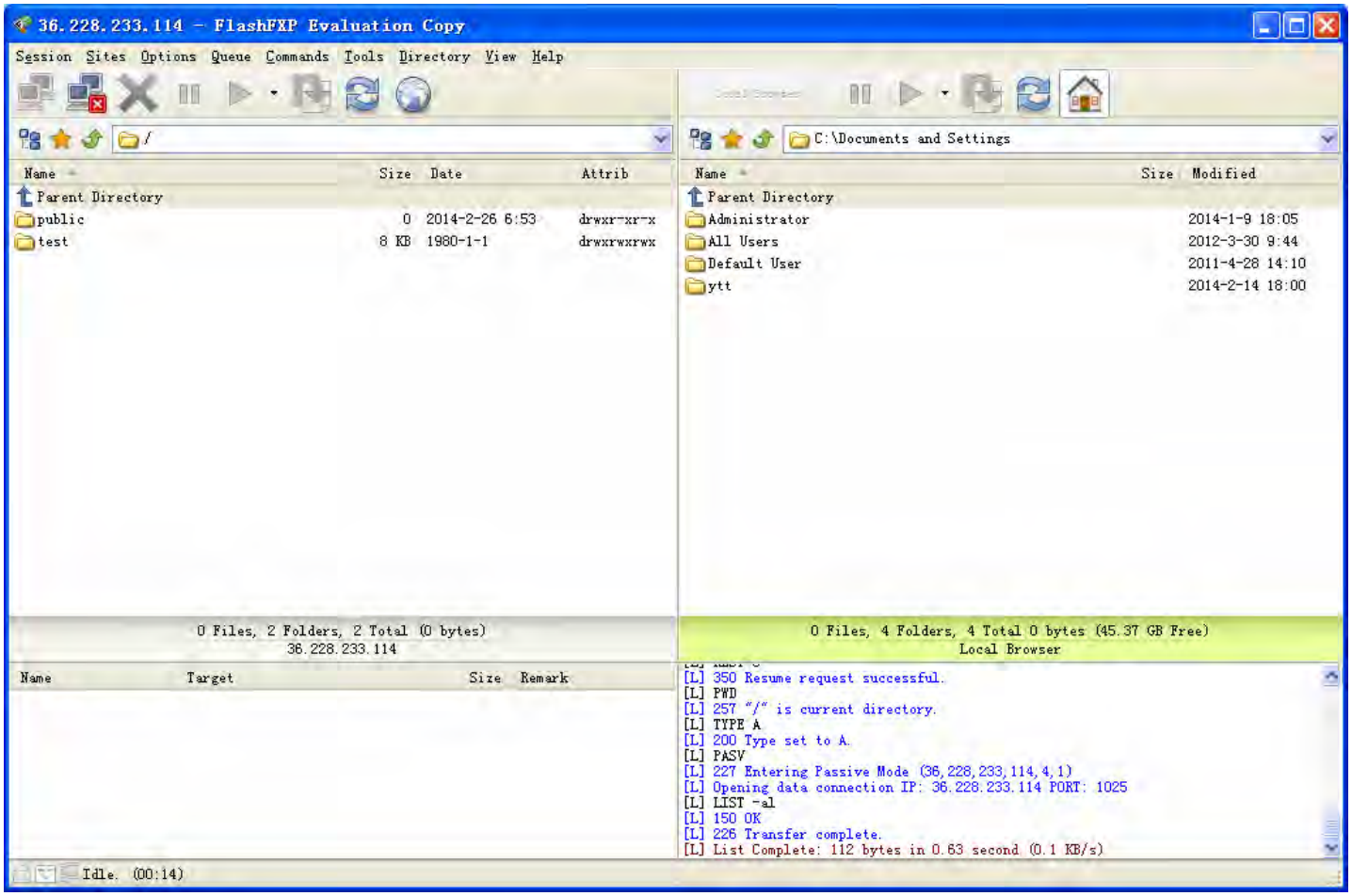
1. **Access via FTP tools**

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP

2) Create ftp sites (LAN IP / WAN IP, and set the account, port).

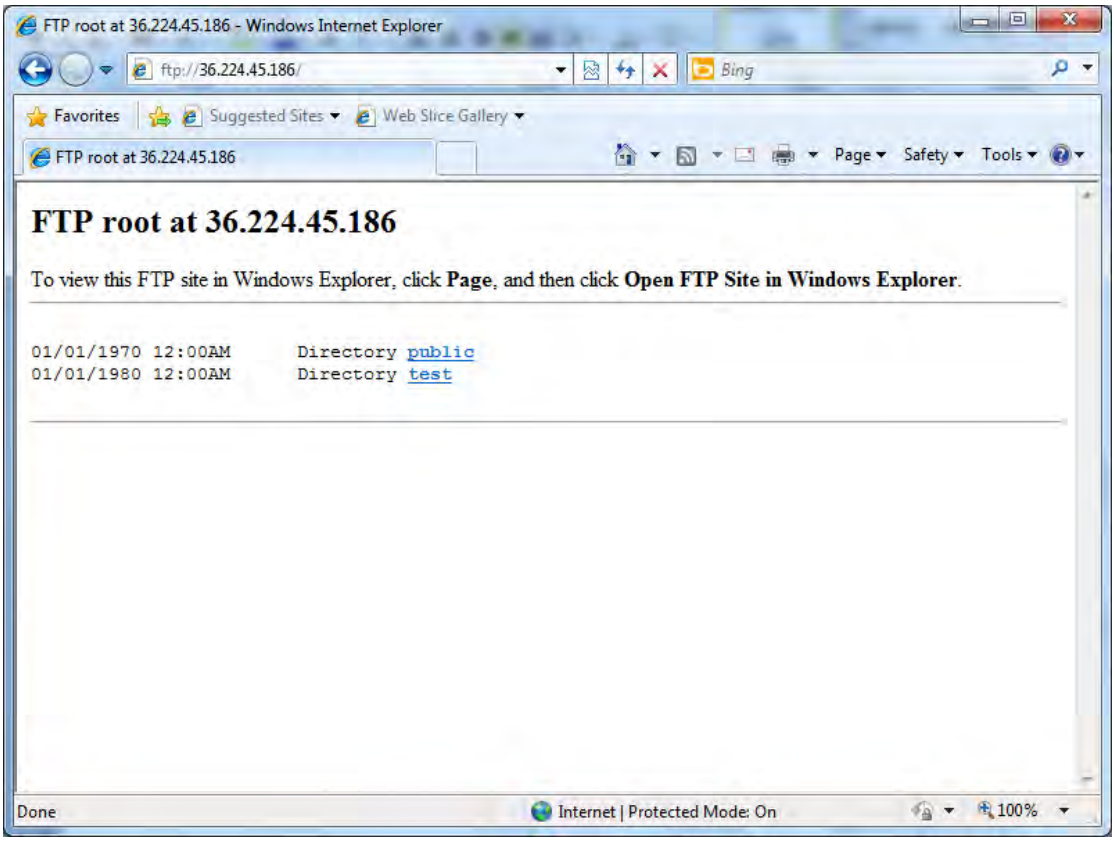
3) Connect to the ftp site.



2. **Web FTP access**

1) Enter ftp://admin@WAN-IP or ftp://admin@LAN-IP at the address bar of the IE. In terms of other browsers, type ftp://WAN-IP or ftp:// LAN-IP directly.

2) Enter the account's username and password.



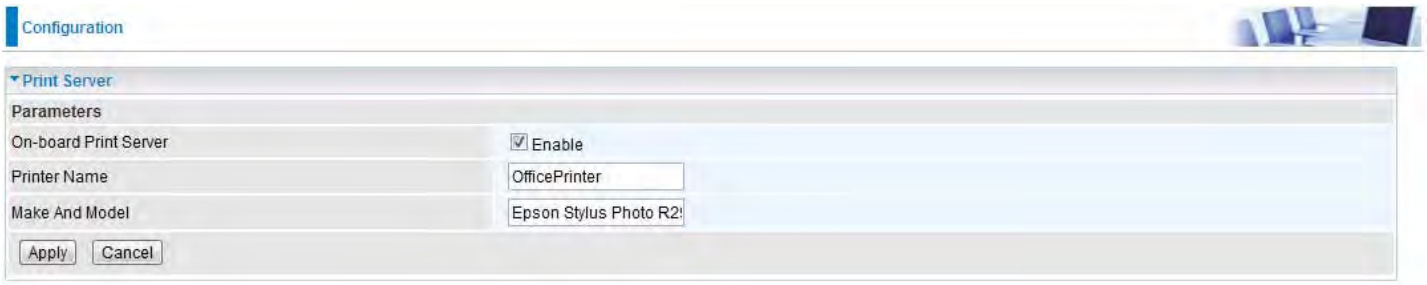
Print Server

The Print Server feature allows you to share a printer on your network by connecting a USB cable from your printer to the USB port on the 7820NZ. This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 3 step process (7820NZ for example)

1. Connect the printer to the 7820NZ's USB port
2. Enable the print server on the 7820NZ
3. Install the printer drivers on the PC you want to print from



On-board Print Server: Check Enable to activate the print server
Printer Name: Enter the Printer name, for example, *OfficePrinter*
Make and Model: Enter in the Make and Model information for the printer, for example, *Epson Stylus Photo R290*

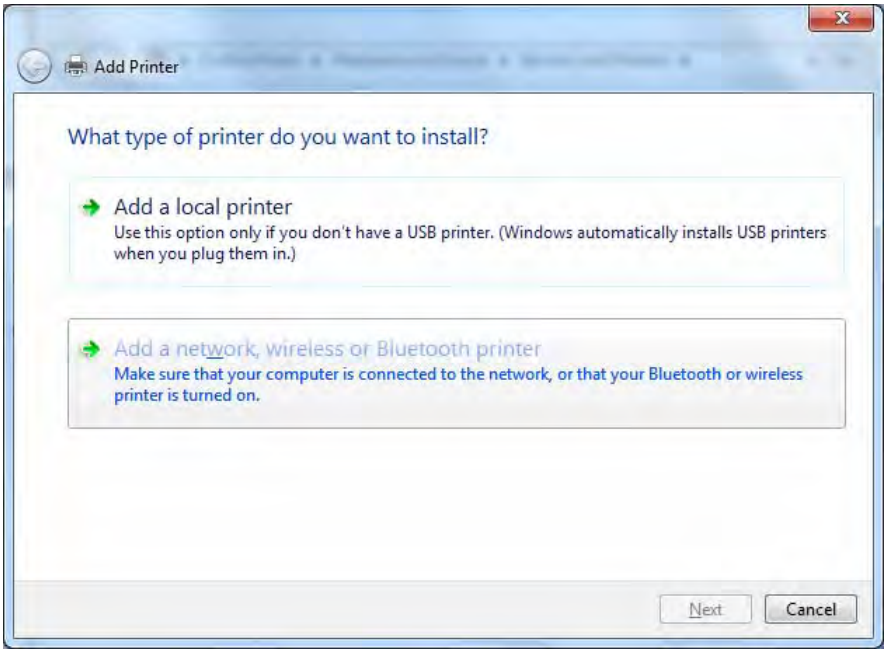
Note:
The ***Printer name*** can be any text string up to **40** characters. It cannot contain spaces.
The ***Make and Mode***l can be any text string up to **128** characters.

Set up of Printer client (Windows 7)

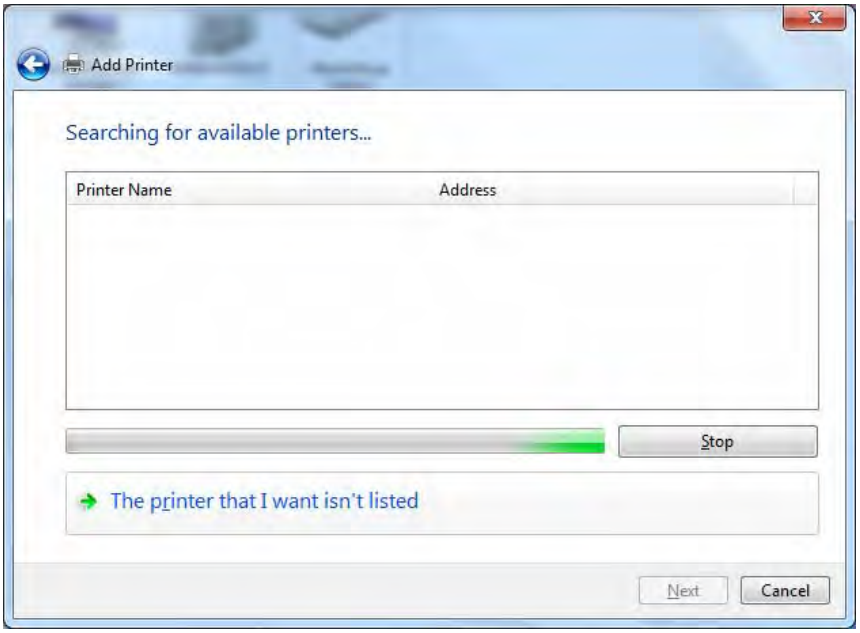
Step 1: Click **Start** and select "Devices and Printers"

Step 2: Click ‘’Add a Printer’’.

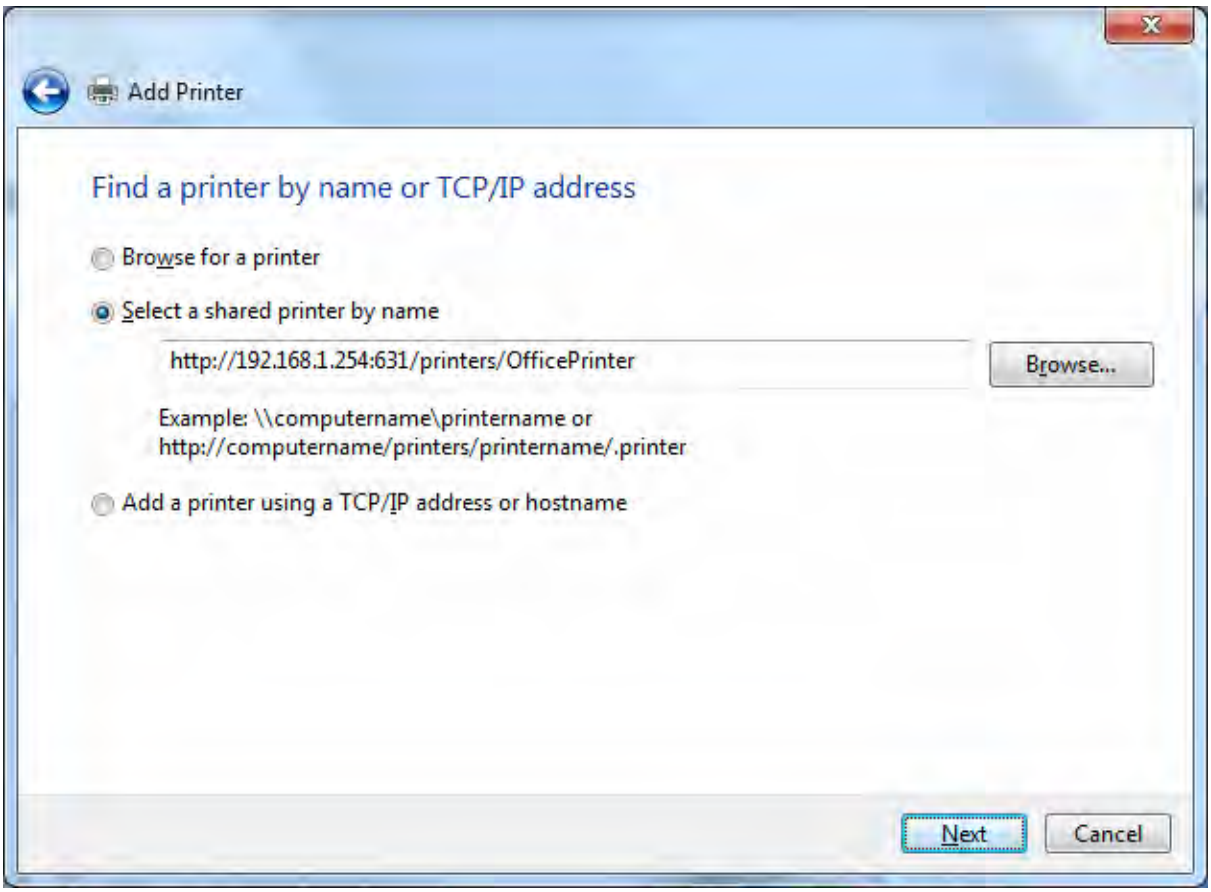
Step 3: Click “Add a network, wireless or Bluetooth printer



Step 4: Click “The printer that I want isn’t listed”

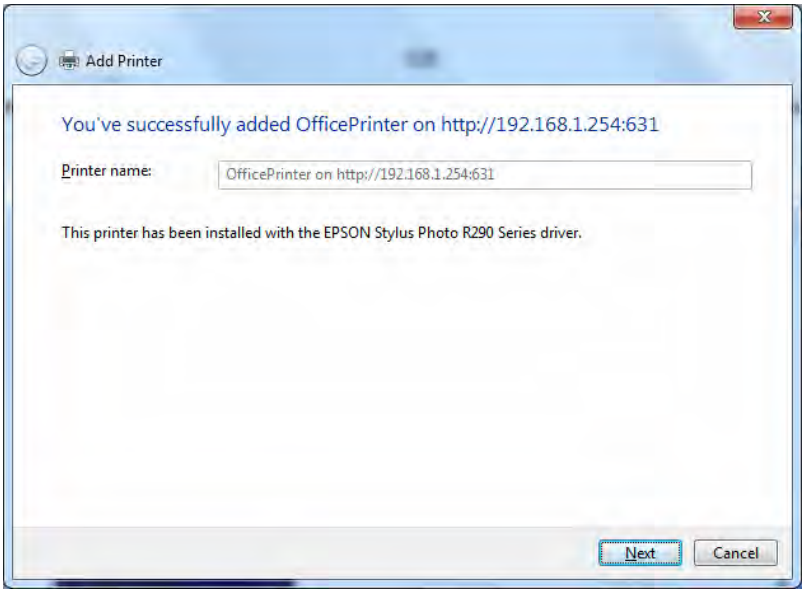


Step 5: Select “Select a shared printer by name”
Enter http://7820NZ- LAN-IP:631/printers/printer-name or. Make sure printer’s name is the same as what you set in the 7820NZ earlier
For Example: *http:///192.168.1.254:631/printers/OfficePrinter*
OfficePrinter is the Printer Name we setup earlier

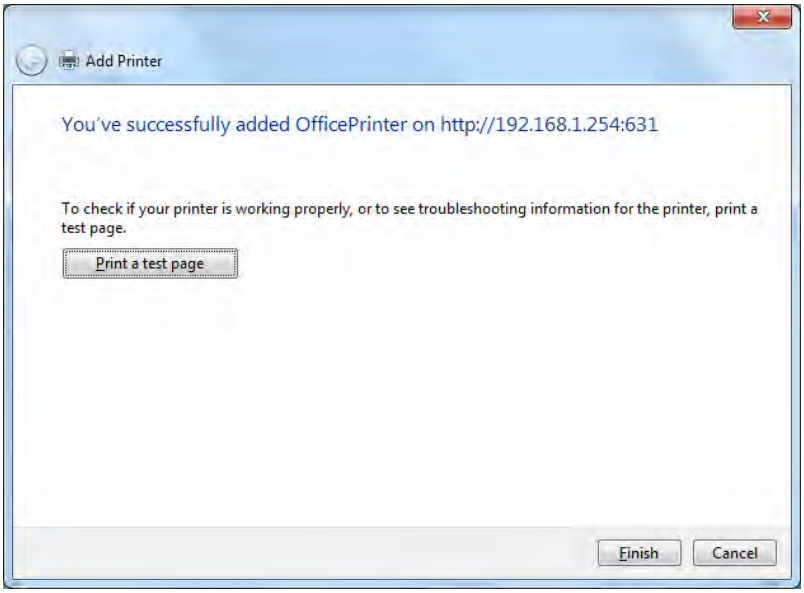


Step 6: Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.

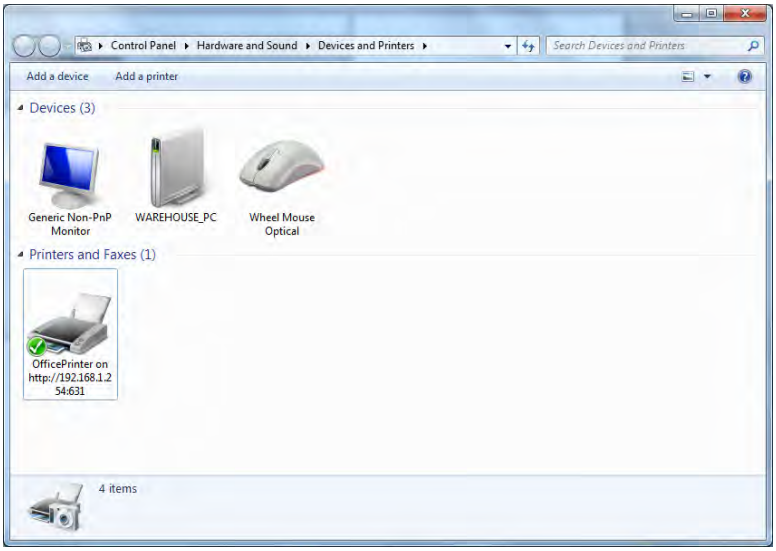
Step 7: Click “Next”



Step 8: Click “Next” and you are done



You will now be able to see your printer on the Devices and Printers Page



DLNA

The Digital Living Network Alliance (DLNA) is a non-profit collaborative trade organization established by Sony in June 2003, which is responsible for defining interoperability guidelines to enable sharing of digital media between consumer devices such as computers, printers, cameras, cell phones and other multiple devices.

DLNA uses Universal Plug and Play (UPnP) for media management, discovery and control. UPnP defines the types of devices (‘server’, ‘renderer’, ‘controller’) that DLNA supports and the mechanism for accessing media over a network.

Overall, DLNA allows more convenience, more choices and enjoyment of your digital content through DLNA certified devices. Any DLNA certified devices or software can access the DLNA server.

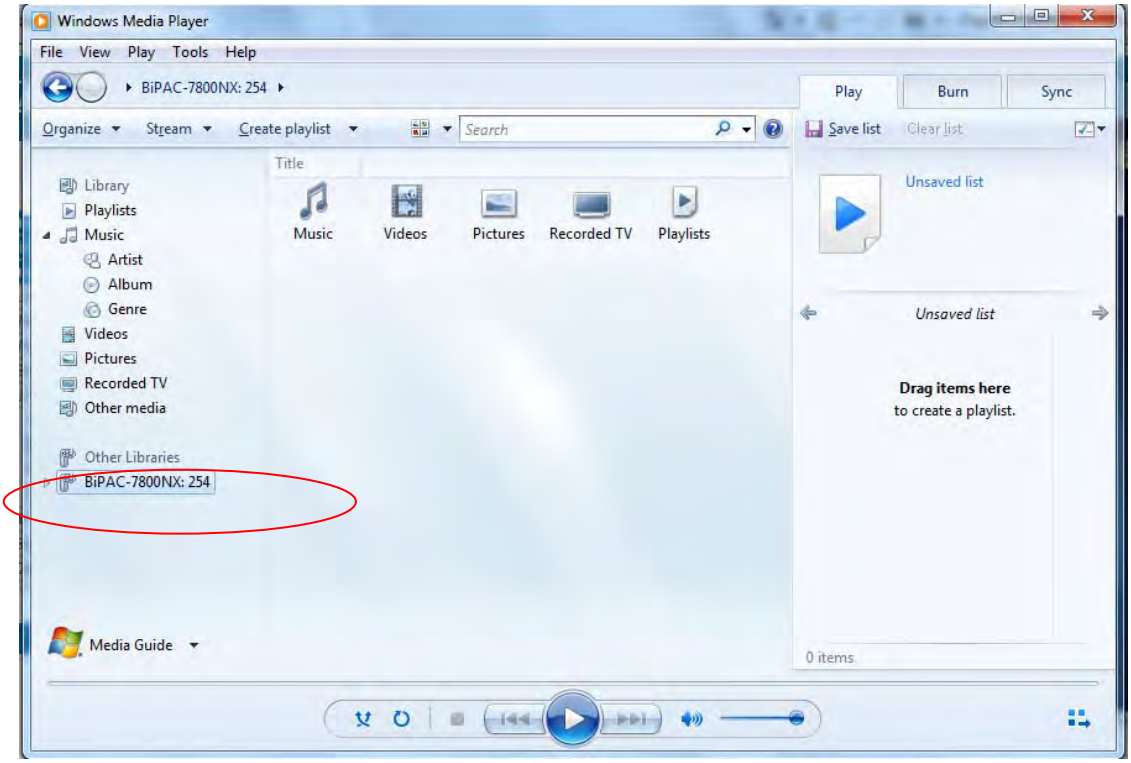
With USB storage, 7820NZ can serve as a DLNA server.

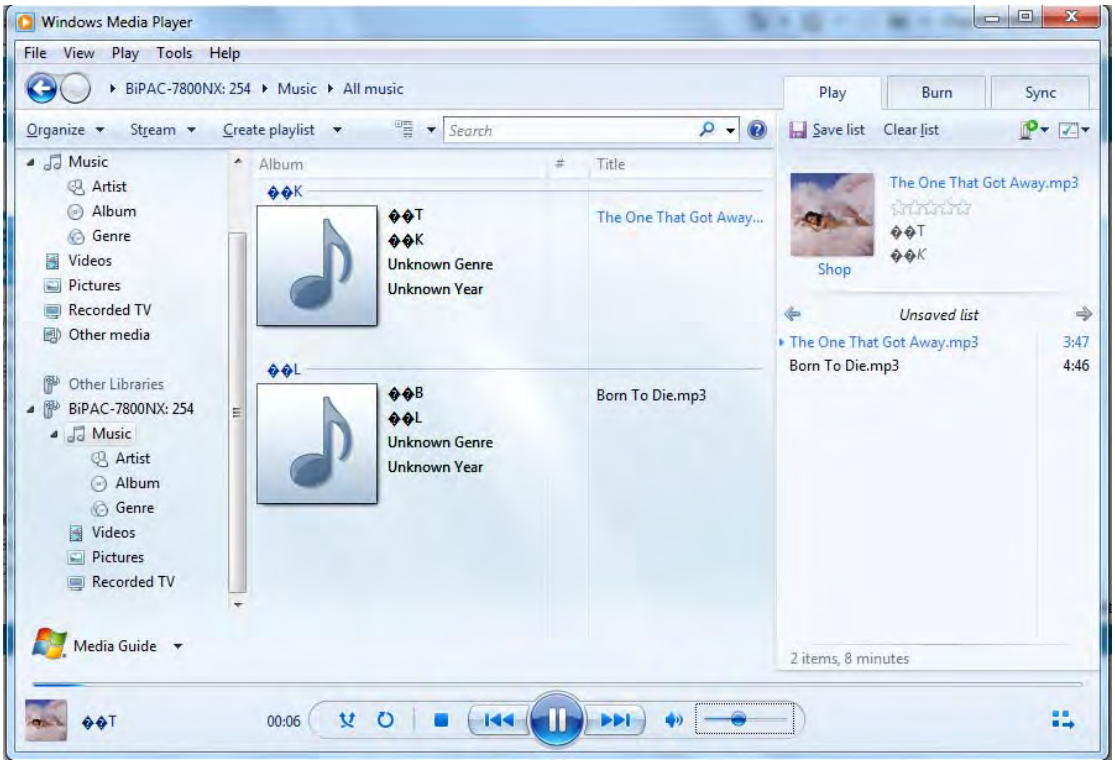
On-board digital media server: Enable to share the device as a DLNA server.

Interface: The VLAN group, it is the bound interface for DLNA server accessing.

Media Library Path: Default is usb1_1, total USB space (pictures, videos, music, etc, all can be accessed with this path).

Take Windows media player in Windows 7 accessing the DLNA server for example for usage of DLNA .





IP Tunnel

An IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets.

IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 internet.

IPv6inIPv4

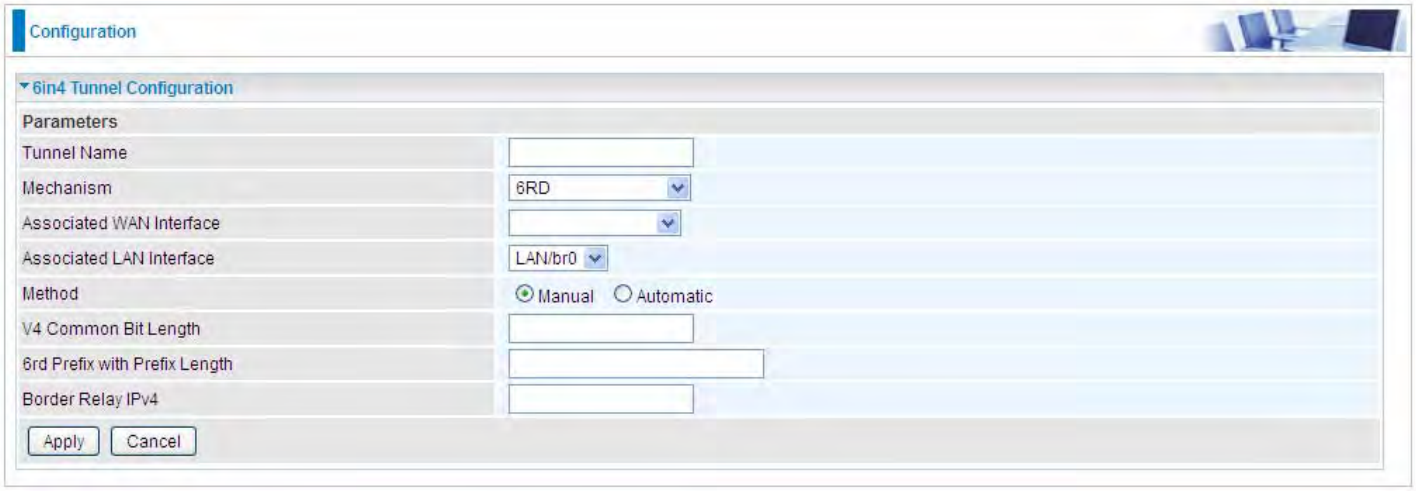
6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP Protocol number set to 41. This protocol number is specifically designated for IPv6 capsulation.

6RD:

6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the enduser's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.

Click **Add** button to manually add the 6in4 rules.



Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

Method: 6rd operation mechanism: manually configured or automatically configured. If manually, please fill out the following 6rd parameters.

V4 Common Bit Length: Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

6rd Prefix with Prefix Length: Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP(The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

Border Relay IPv4 Address: The IPv4 address of the border relay. The relay is used to unwrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

IPv4inIPv6

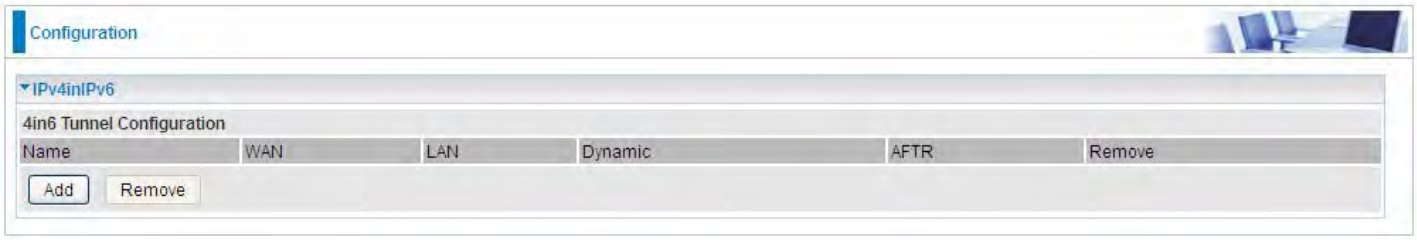
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

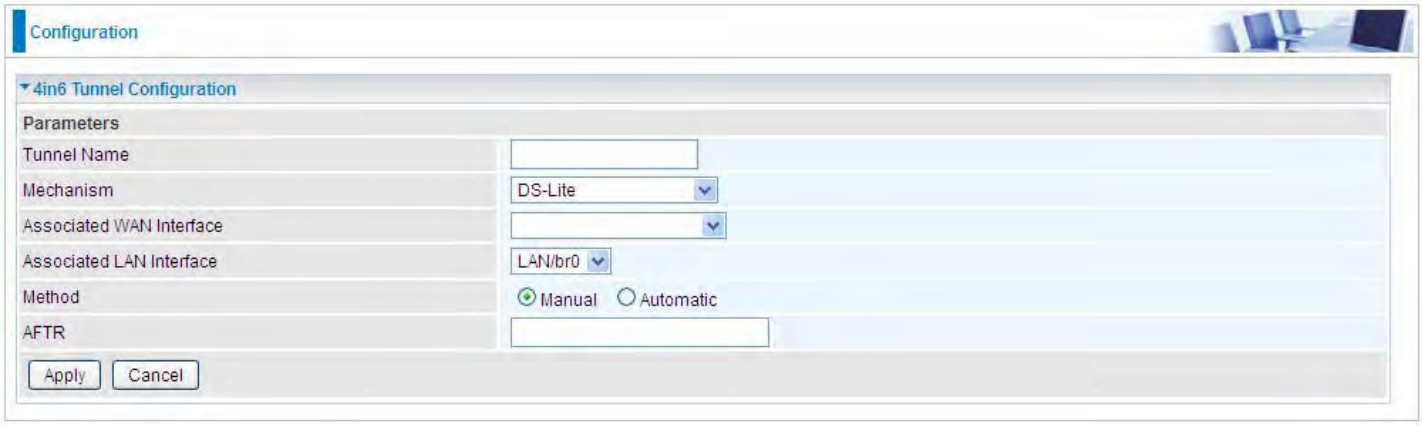
DS – Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



Click **Add** button to manually add the 4in6 rules.



Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

Associated WAN Interface: The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

Method: Manually to specify the AFTP (Address Family Transition Router) address or Automatic.
AFTR: Specify the address of AFTP (Address Family Transition Router) from your ISP.

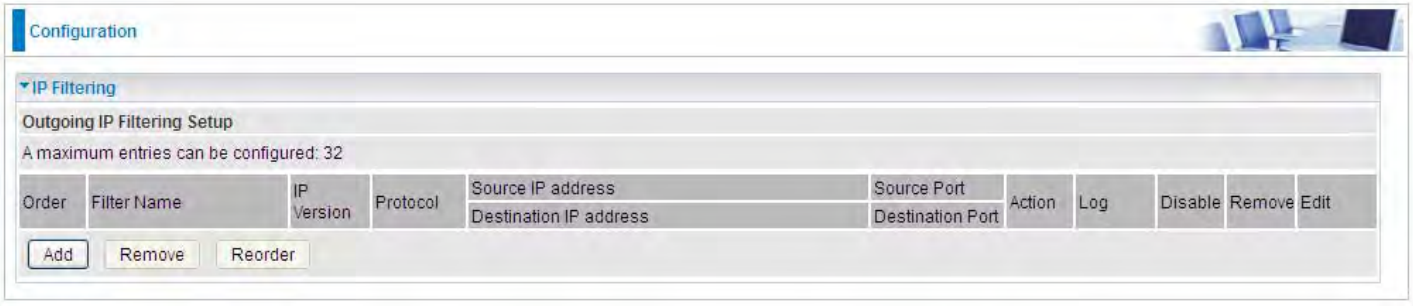
Security

IP Filtering Outgoing

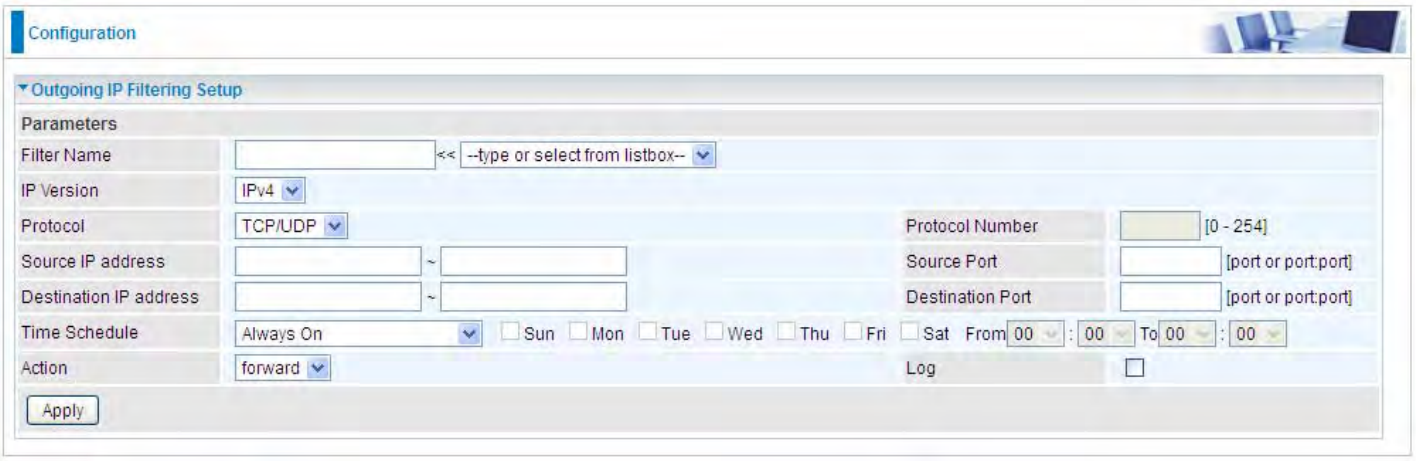
IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.



Click **Add** button to enter the exact rule setting page.



Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

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

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address

above.

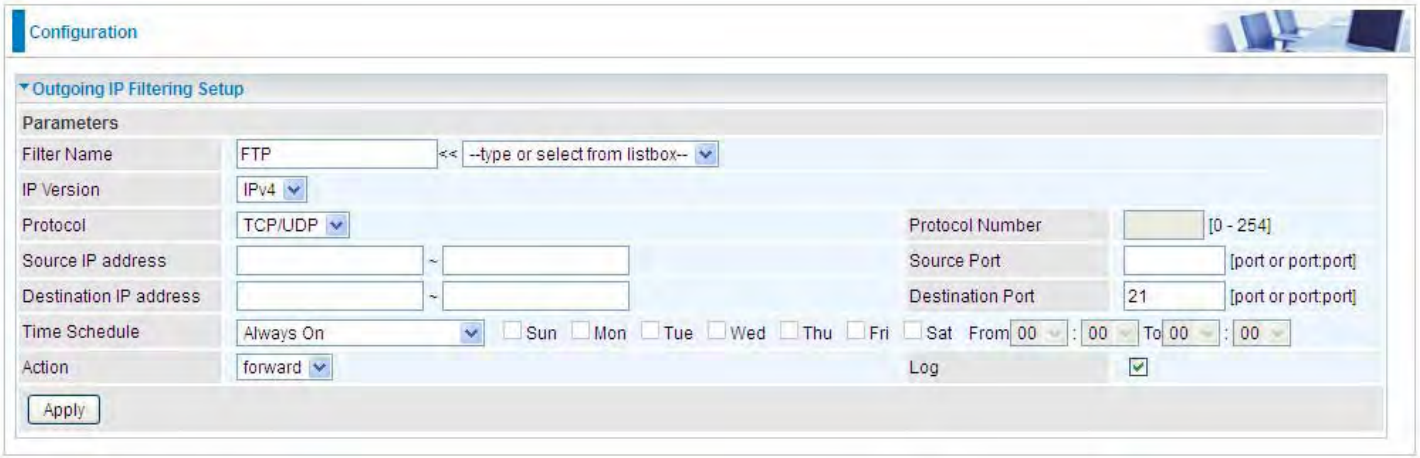
Destination Port [port or port: port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon “ ” in list table indicating the rule is inactive. See Time Schedule.

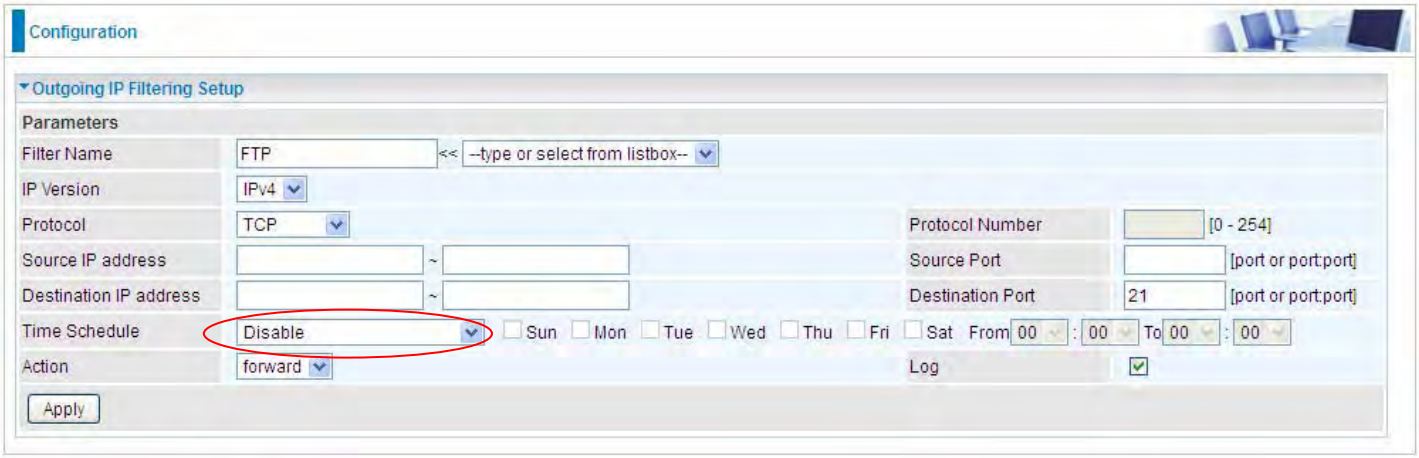
Action: Select to **drop** or **forward** the packets fit the outgoing filtering rule.

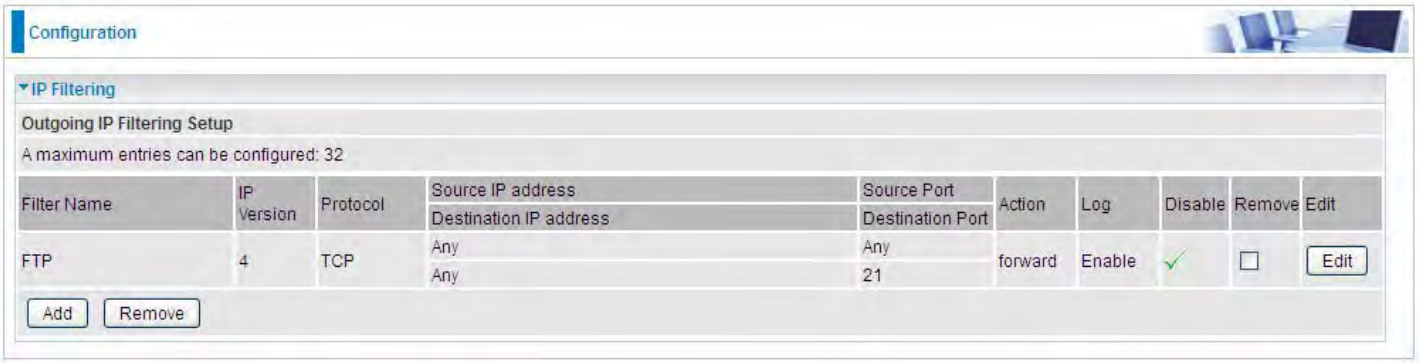
Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

Example: For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be forwarded. Or exactly in the rule below, all traffic trying to access FTP will be forwarded.



(The rule is active; disable field shows the status of the rule, active or inactive)





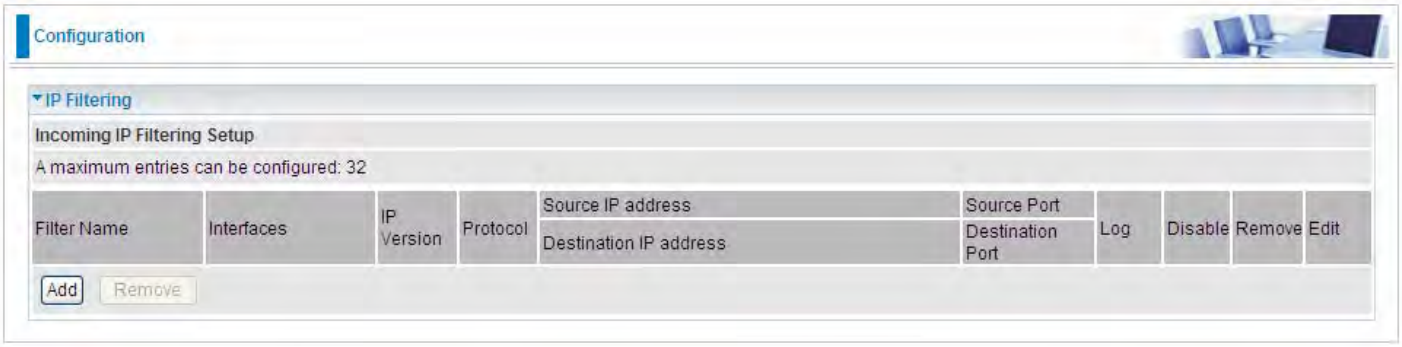
(Rule inactive)

IP Filtering Incoming

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to **forward** the specific incoming traffic.

Note:

1. The maximum number of entries: 32.
2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.



Click **Add** button to enter the exact rule setting page.

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

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

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port : port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535

Interfaces: Check if the filter rule applies to all interfaces. User can base on need select interfaces to make the rule take effect with those interfaces.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” in the list table indicating the rule is inactive. See Time Schedule.

Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

FORWARDED means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.

BLOCKED means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.

By default, all MAC frames of the interface in Bridge Mode will be **forwarded**, you can check **Change** checkbox and then press **Change Policy** to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode, and all the MAC layer frames will be **forward**, but you can set some rules to let some item matched the rules to be **blocked**.

Click **Add** button to add the rules.

Protocol type: Select from the drop-down menu the protocol that applies to this rule.

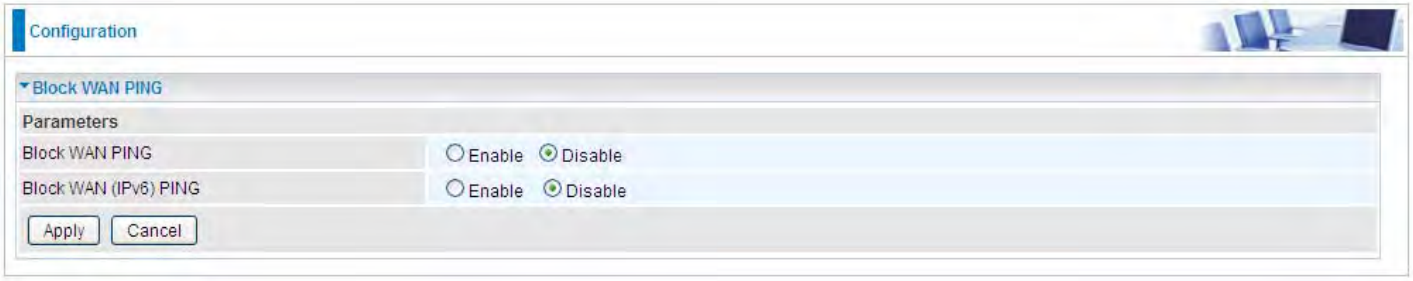
Destination /Source MAC Address: Enter the destination/source address.

Frame Direction: Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only LAN to WAN: LAN=>WAN, only WAN to LAN: WAN=>LAN.

WAN Interfaces: Select the interfaces configured in Bridge mode.

Blocking WAN PING

This feature is enabled to let your router not respond to any ping command when someone others “Ping” your WAN IP.

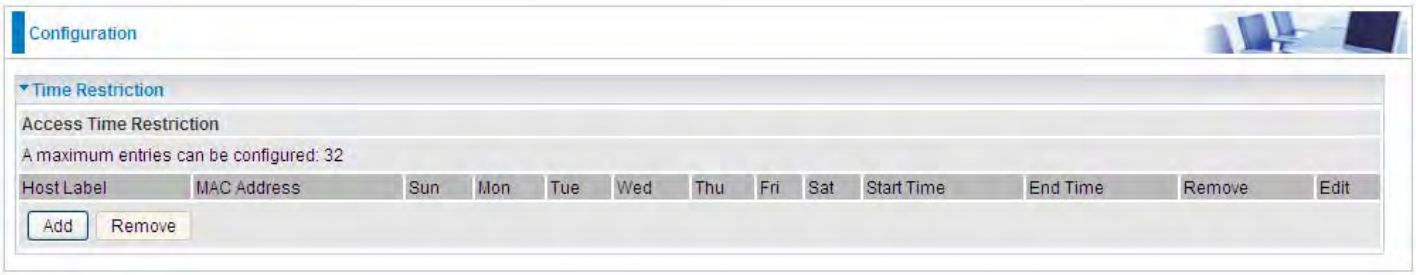


Time Restriction

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



Click **Add** to add the rules.

Host Label: User-defined name.

MAC Address: Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

Time Schedule: To determine when the rule works.

- **Drop:** To drop the MAC entries always; in other words, the MACs are blocked access to router and internet always.
- **Forward:** To forward the MAC entries always; in other words, the MACs are granted access to the router and internet always.
- **Check or select from listbox:** To set the time duration during which the MACs are blocked from access the router and internet. "**select from listbox**" means that you can select the already set timeslot in "**Time Schedule**" section during which the MACs are blocked from access the router and internet.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

An example:

Here you can see that the user “child-use” with a MAC of 18:a9:05:04:12:23 is blocked to access the router from 00:00 to 23:59 Monday through Friday.
The “test” can access the internet always.

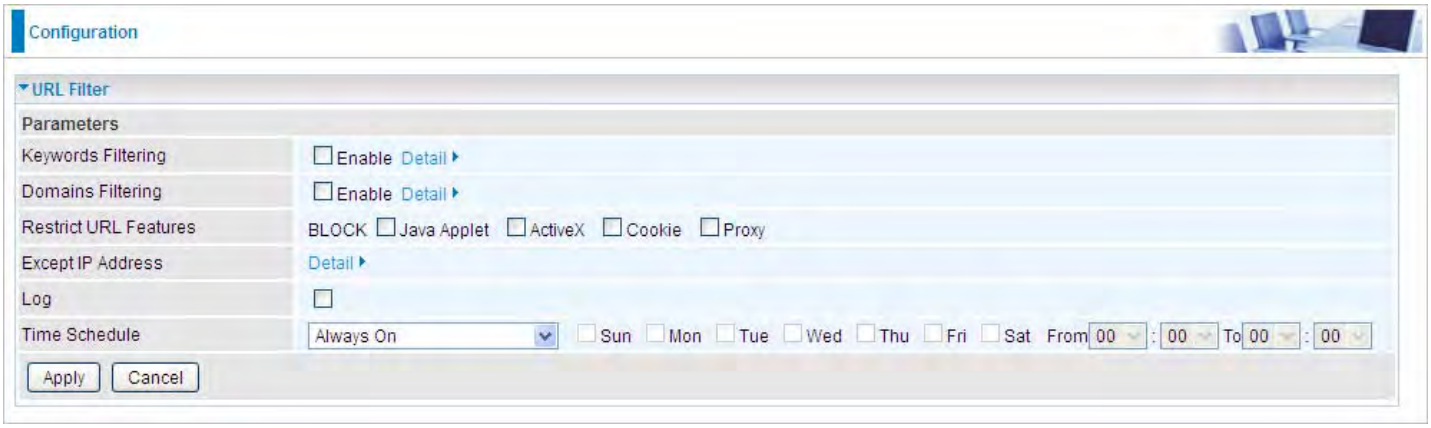
If you needn’t this rule, you can check the box, press Remove, it will be OK.

.

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.

Note:
1) URL Filter rules apply to both IPv4 and IPv6 sources.
2) But in **Exception IP Address** part, user can click Detail to set the exception IP address(es) for IPv4 and IPv6 respectively.



Keywords Filtering: Allow blocking against 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.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering. These IPs will not be covered by the URL rules.

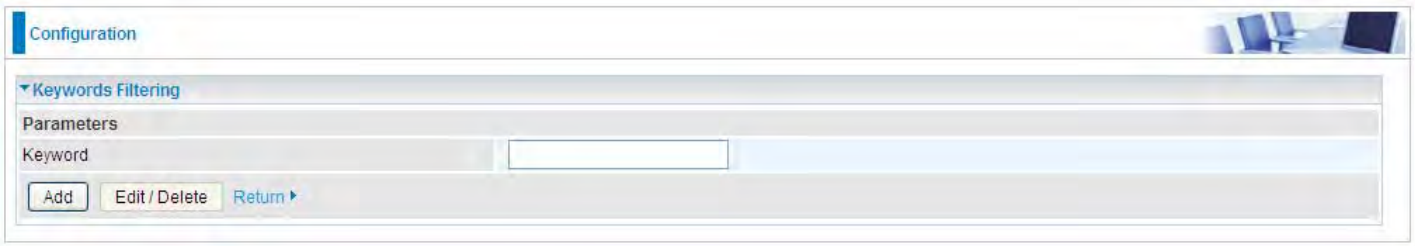
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled. See Time Schedule.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to Security Log.

Keywords Filtering

Note: Maximum number of entries: 32.

Click Detail to add the keywords.



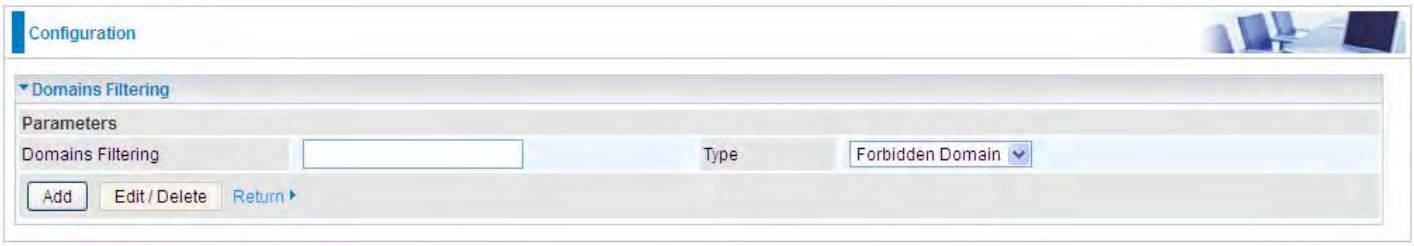
Enter the Keyword, for example image, and then click **Add.**

You can add other keywords like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, and then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domain Filtering

Note: Maximum number of entries: 32.

Click Detail to add Domains.



Domain Filtering: enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

- **Forbidden Domain:** The domain is forbidden access.
- **Trusted Domain:** The domain is trusted and allowed access.

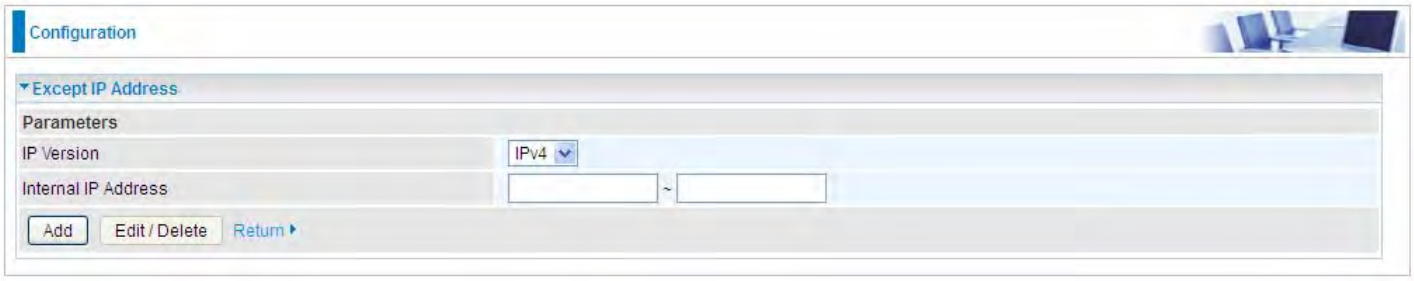
Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to ***Keywords***

Filtering.

Exception IP Address

In the section, users can set the exception IP respectively for IPv4 and IPv6.

Click Detail to add the IP Addresses.



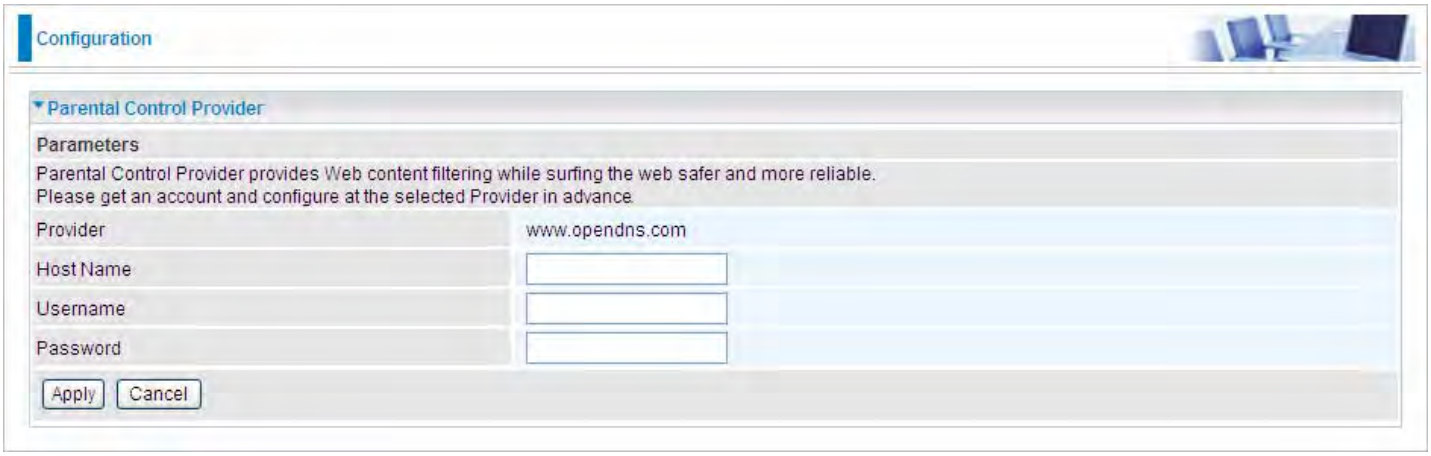
Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the ***Exception List***, and excluded from the URL filtering rules in effect. For specific process, please refer to ***Keywords Filtering*****.**

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter (or IPv4 clients (a range)). And also an IPv6 client (2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients(a range) can be the exceptions from the URL rules.

At the URL Filter page, press **Apply** to confirm your settings.

Parental Control Provider

Parental Control Provider provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider “www.opendns.com” in advance. To use parental control (DNS), user needs to configure to use parental control (DNS provided by parental control provider) to access internet at WAN configuration or DNS page(See DNS).

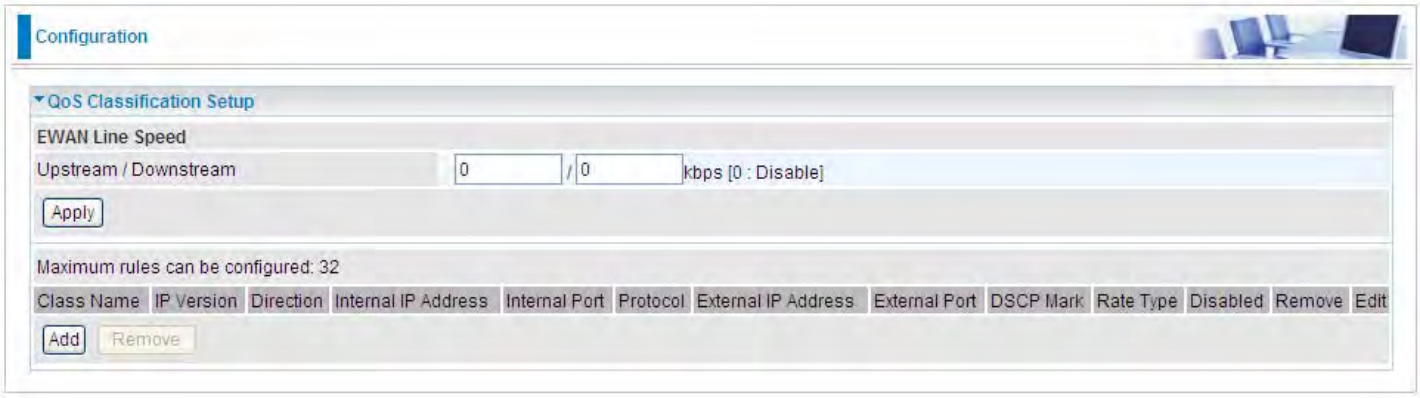


Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website www.opendns.com.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

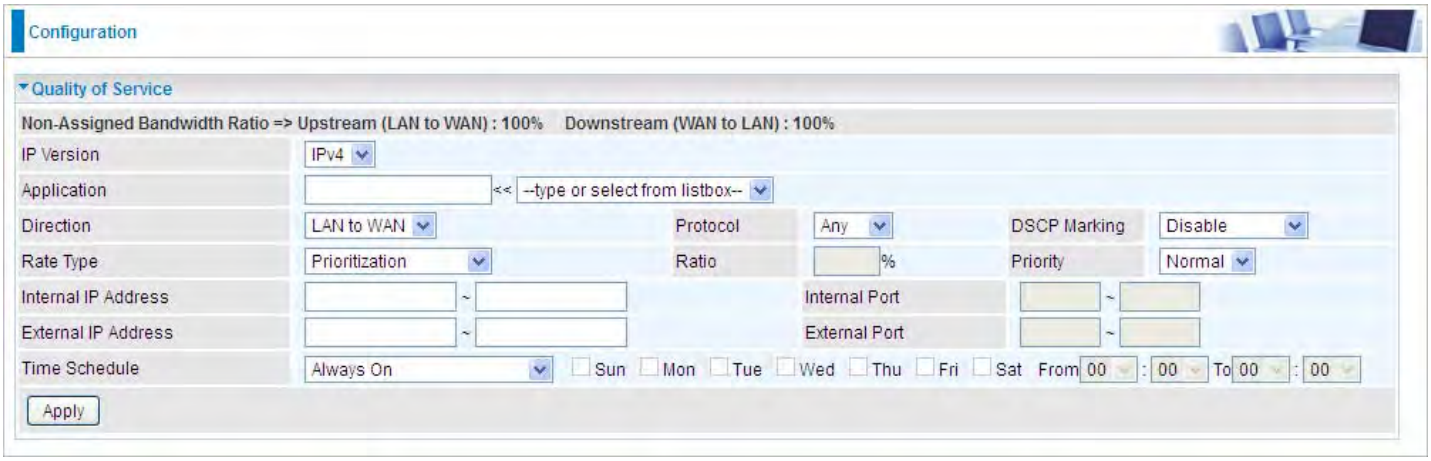
Note: ADSL line speed is based on the ADSL sync rate. But there is no QoS on 3G/LTE as the 3G/LTE line speed is various and can not be known exactly.



EWAN Line Speed

Upstream / Downstream: Specify the upstream and downstream rate of the EWAN interface. Click **Apply** to save the EWAN rate settings.

Click **Add** to enter QoS rules.



IP Version: Select either IPv4 or IPv6 base on need.

Application: Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Shows the direction mode of the QoS application.

- **LAN to WAN:** You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.
  Eg: you have a FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.
- **WAN to LAN:** Control traffic from WAN to LAN (Downstream).

Protocol: Select the supported protocol from the drop down list.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the

DSCP value.

IP Precedence and DSCP Mapping Table

Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP offers three levels of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four levels of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Rate Type: You can choose ***Limited*** or ***Prioritization***.

- **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximum rate for this policy. When you choose ***Limited***, type the ***Ratio*** proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- **Prioritization:** Specify the rate type control for the rule to used. If you choose ***Prioritization*** for the rule, you parameter ***Priority*** would be available, you can set the priority for this rule.
- **Set DSCP Marking:** When select ***Set DSCP Marking***, the packets matching the rule will be forwarded according to the pre-set DSCP marking.

Ratio: The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8)

Priority: Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

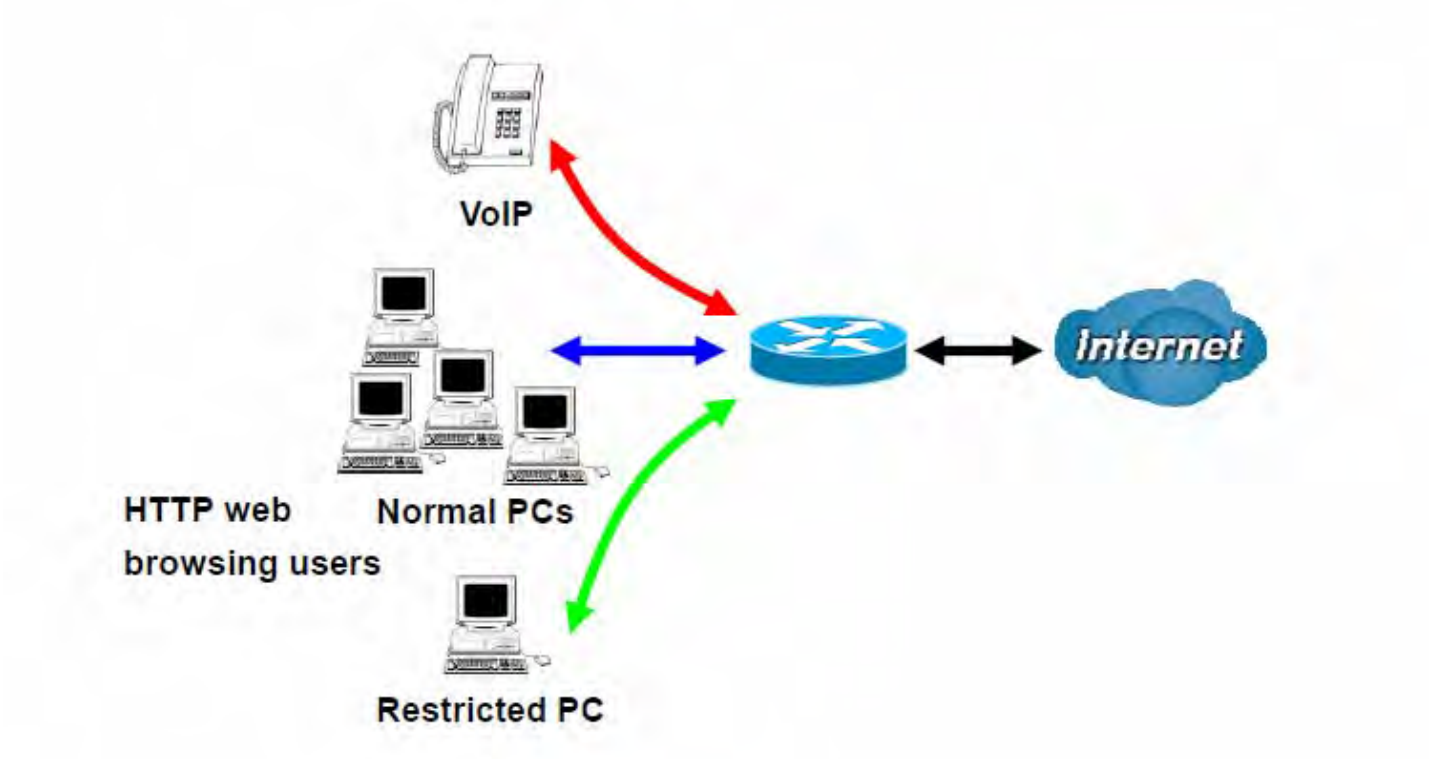
Internal Port: The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

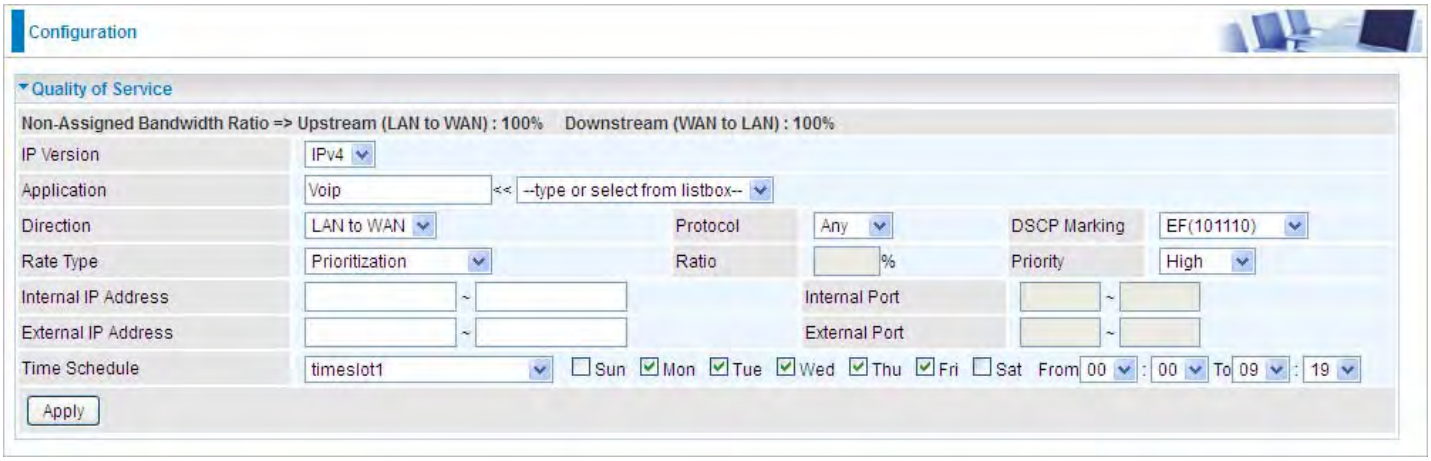
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” indicating the rule is inactive. See Time Schedule.

Examples: Common usage

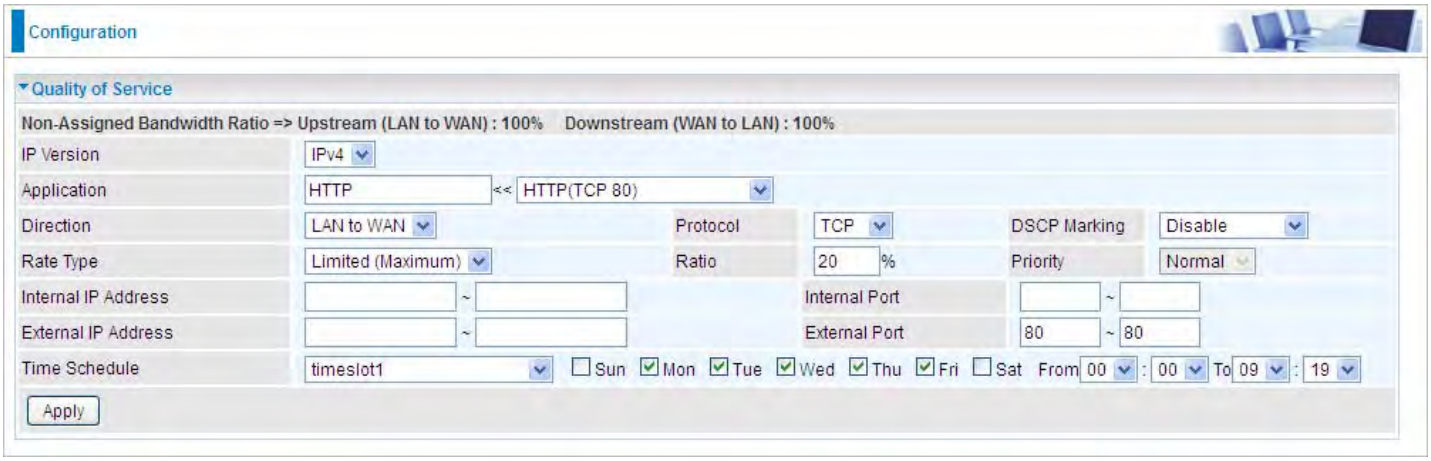


1. Give outgoing VoIP traffic more priority.

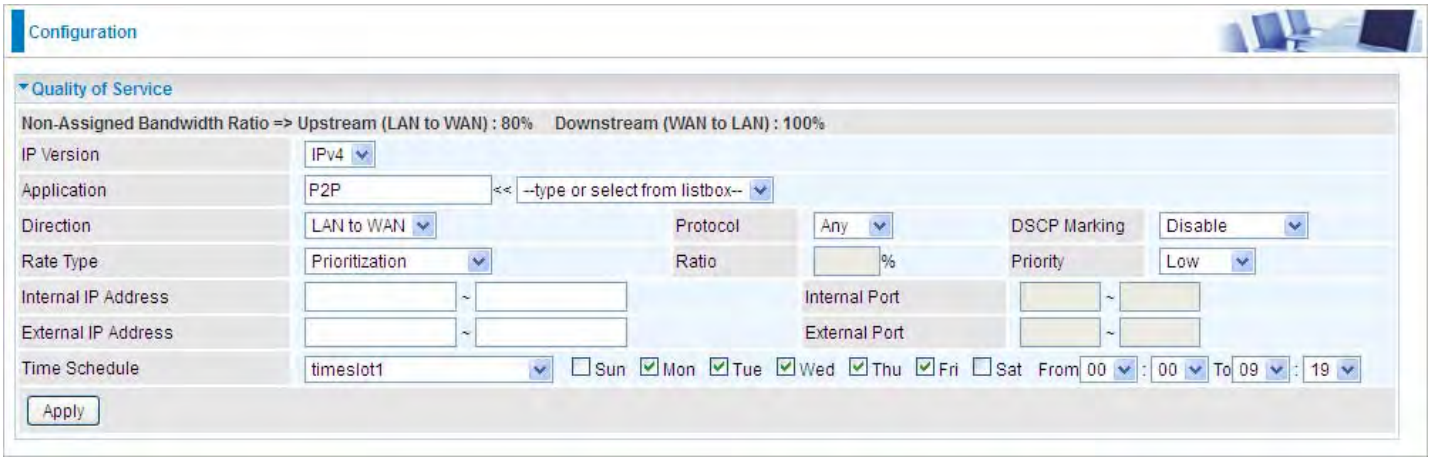
The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.



2. Give regular web http access a limited rate



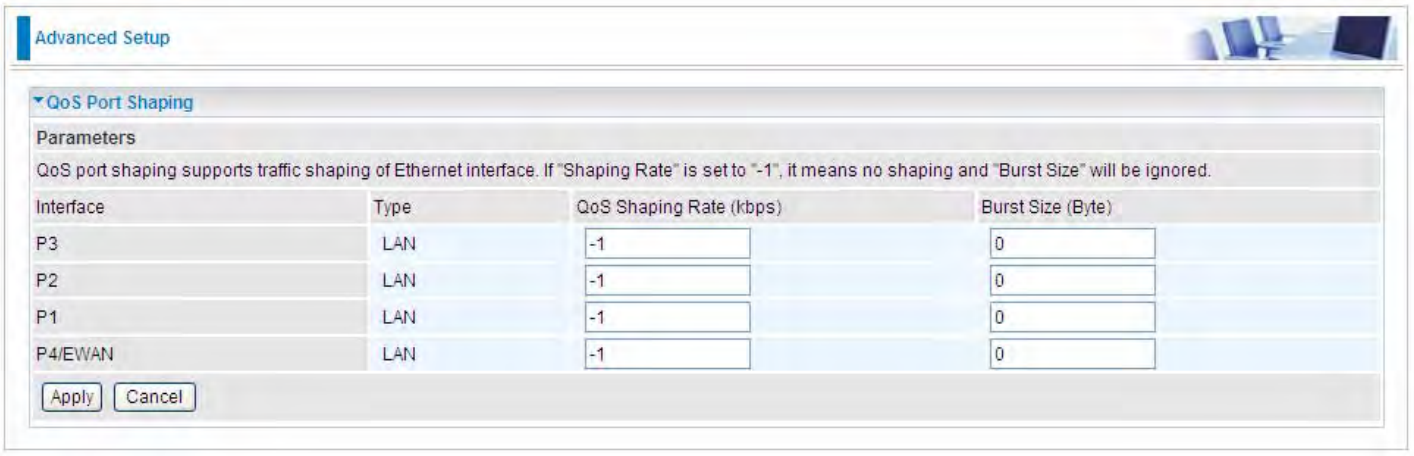
3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.



Other applications, like FTP, Mail access, users can use QoS to control based on need.

QoS Port Shaping

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When “Shaping Rate” is set to “-1”, no shaping will be in place and the “Burst Size” is to be ignored.



Interface: P1-P4. P4 used as EWAN also covered.

Type: All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

Burst Size(Bytes): Set the forcefully Burst Size.

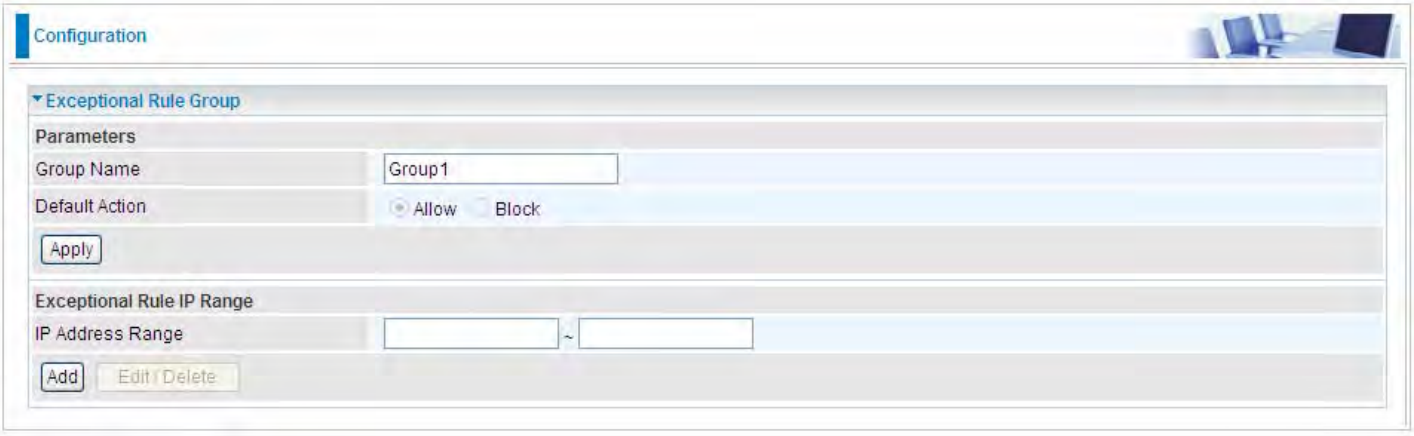
NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

Exceptional Rule Group

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

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



Default Action: Please first set the range to make **"Default Action"** setting available**.** Set "Allow" to ban the listed IP or IPs to access the Virtual Server and DMZ Host

Check "Block" to grant access to the listed IP or IPs to Virtual Server and DMZ Host.

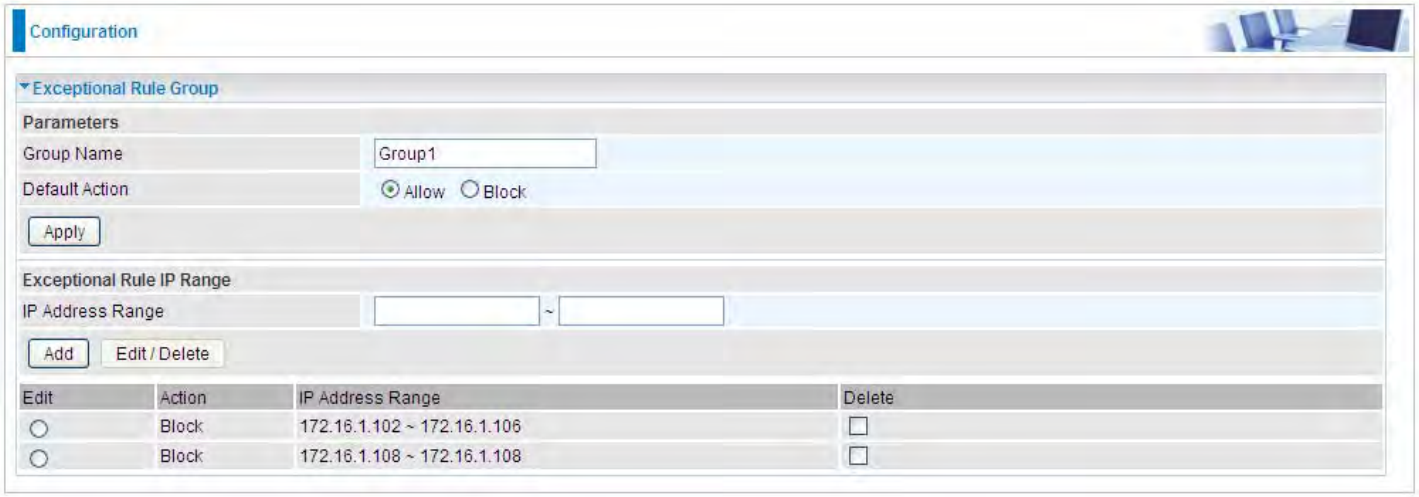
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

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

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

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



Virtual Servers

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.

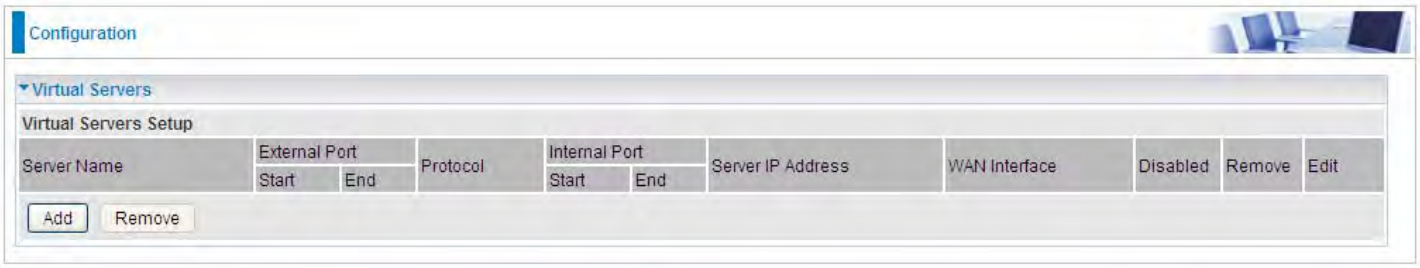
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing 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.

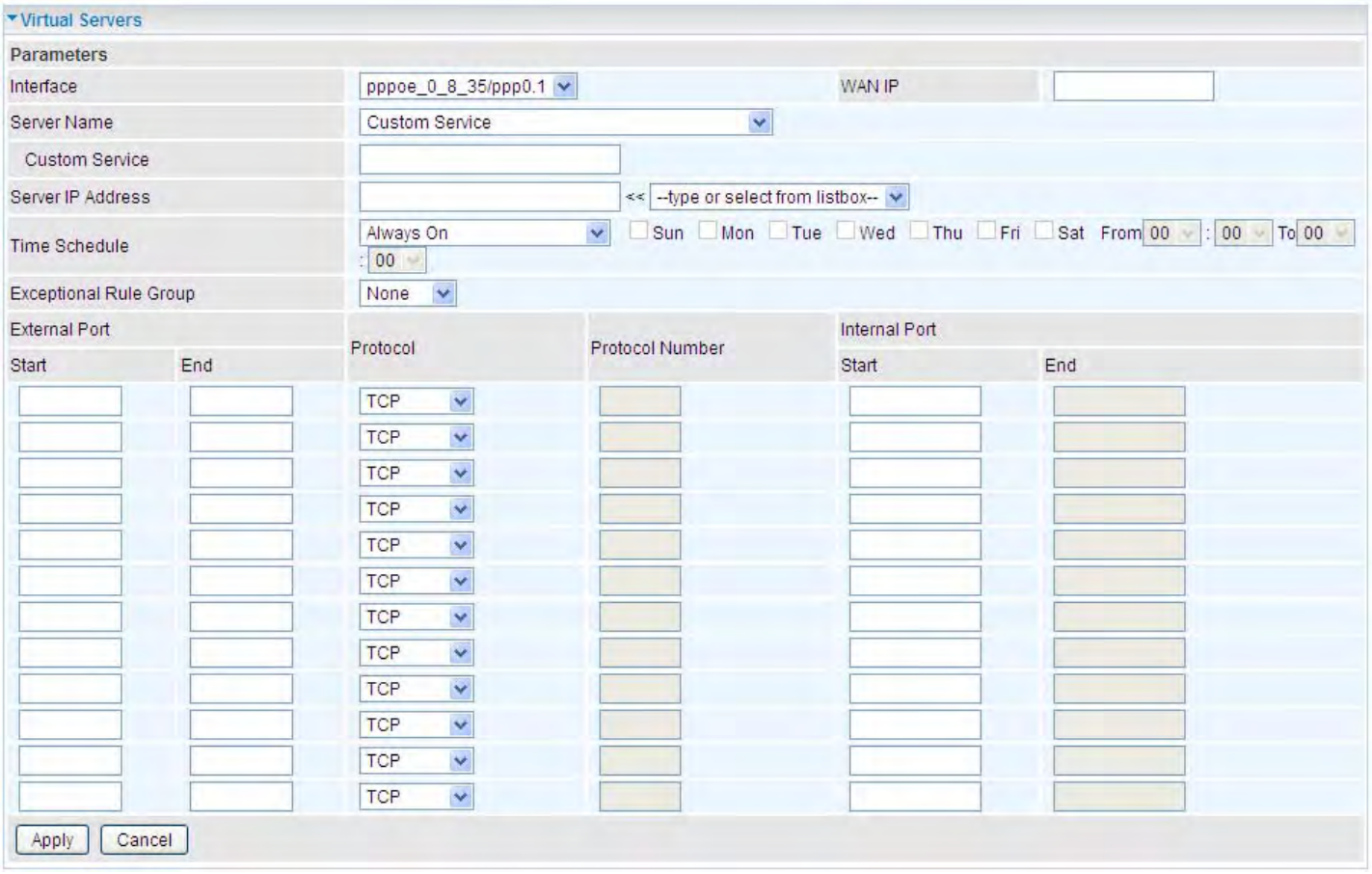
This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.



It is virtual server listing table as you see, Click **Add** to move on.

The following configuration page will appear to let you configure.



Interface: select from the drop-down menu the interface you want the virtual server(s) to apply.

Server Name: select the server name from the drop-down menu.

Custom Service: It is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.

Server IP Address: Enter your server IP Address here. User can select from the list box for quick setup.

External Port

- **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
- **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

Internal Port

- **Start:** Enter a port number as the internal staring number.
- **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

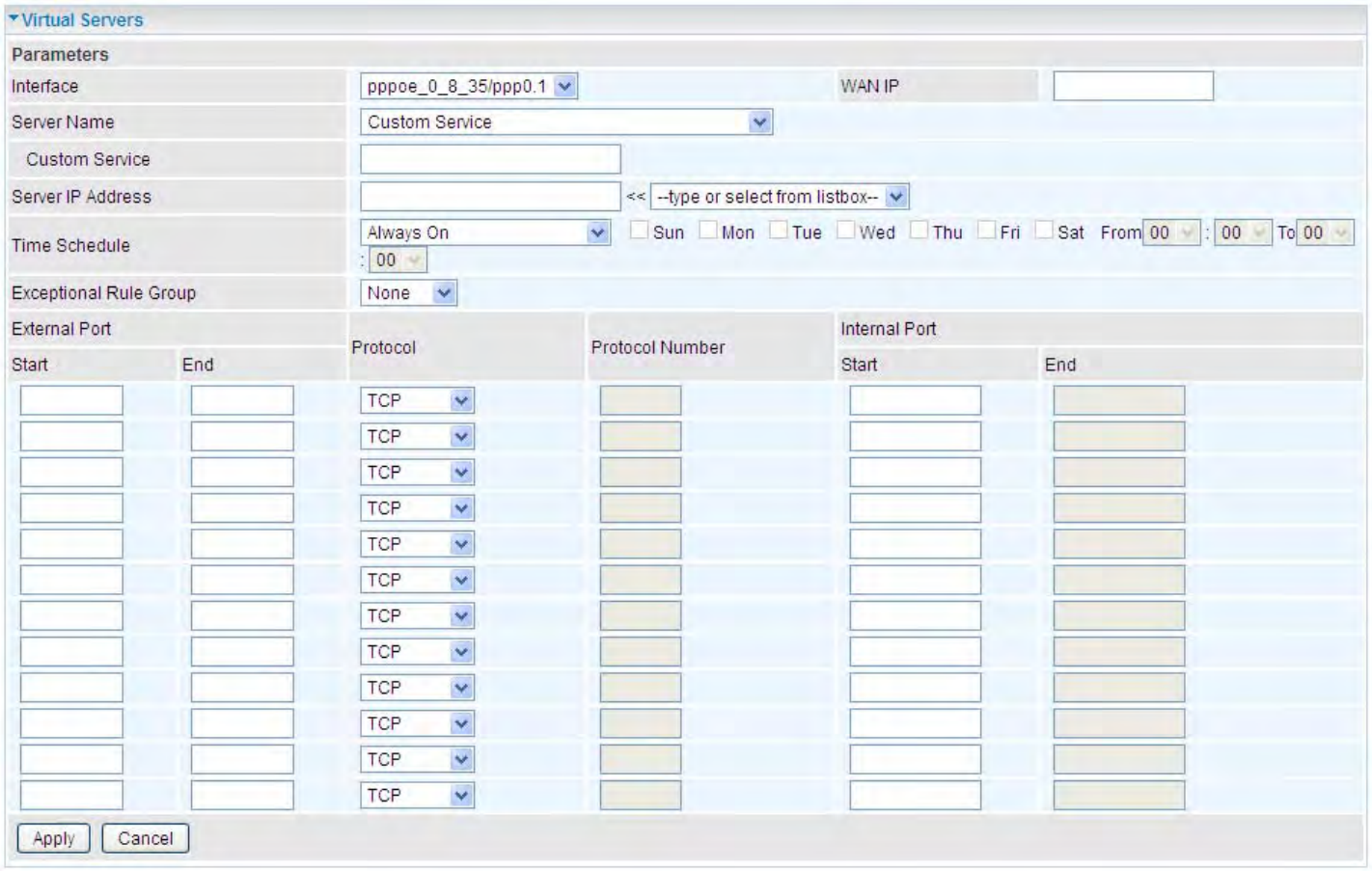
Time Schedule: Select or set exactly when the Virtual Server works. When set to "Always On", the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to "Disable", the rule is disabled and there will be an icon ✓ in the list table indicating the rule is disabled. See Time Schedule.

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block Virtual Server

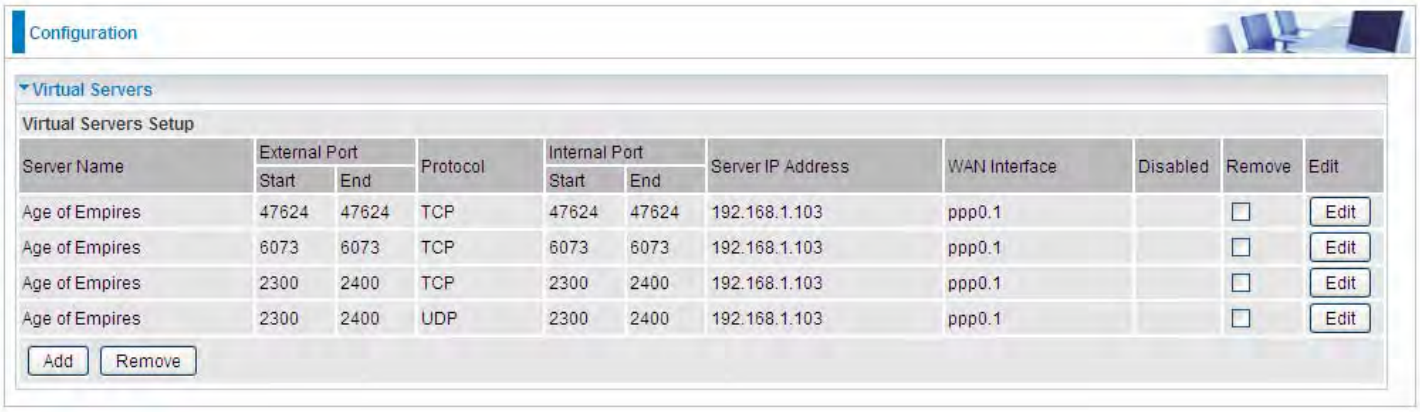
access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

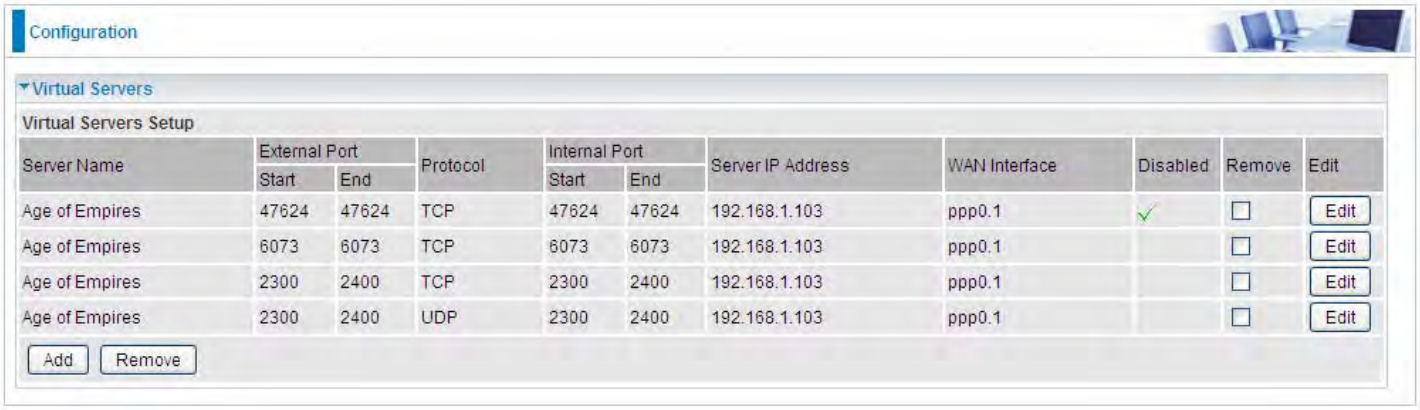
Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

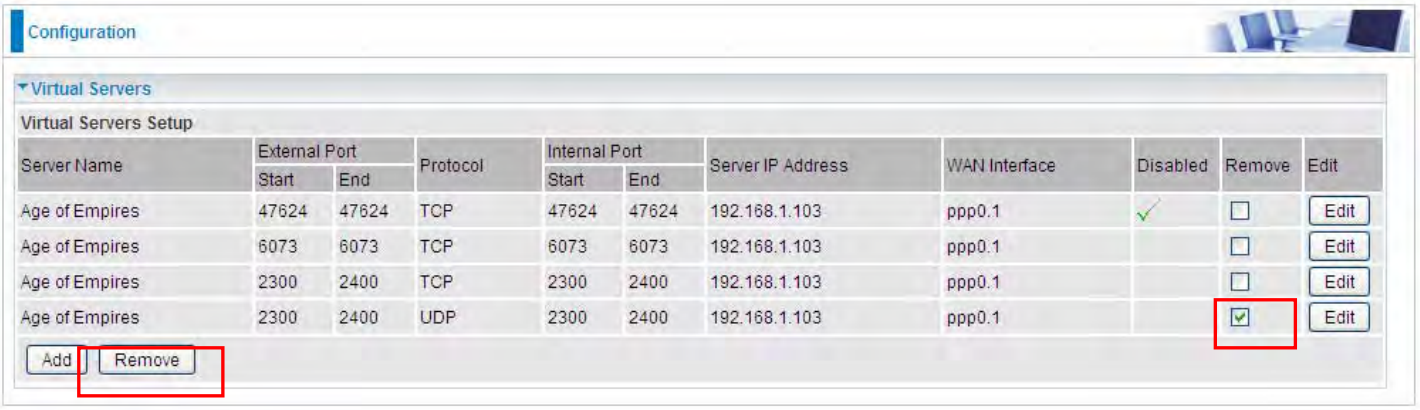




(✓ Means the rule is inactive)

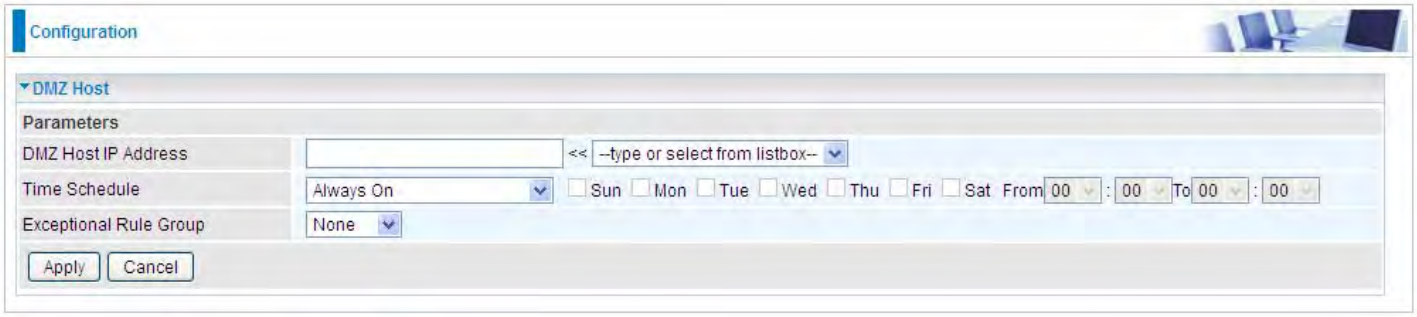
Remove

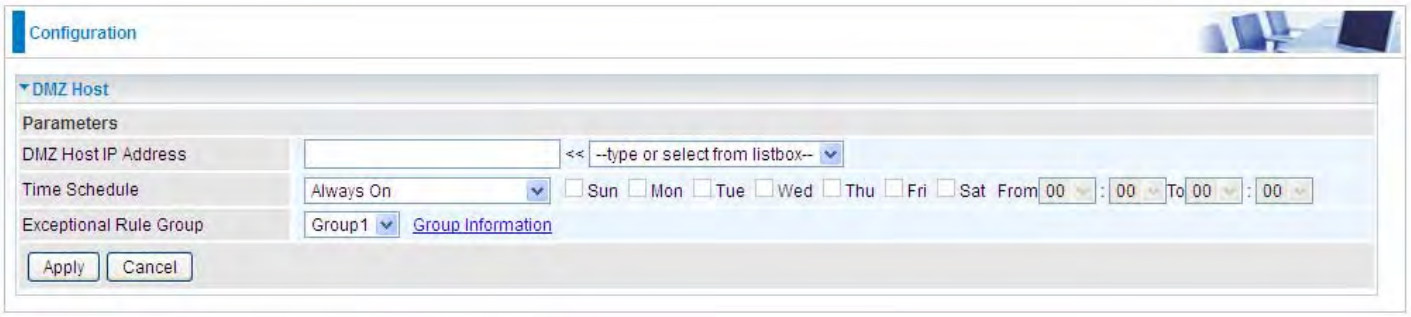
If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.



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 Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.





Group Index	1
Group Name	Group1
Action	Block
IP Address Range	172.16.1.102~172.16.1.106
	172.16.1.108~172.16.1.108

(Group Information)

DMZ Host IP Address: Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

Time Schedule: Select or set exactly when the DMZ works. When set to “Always On”, the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to “Disable”, the DMZ Host is disabled. See Time Schedule.

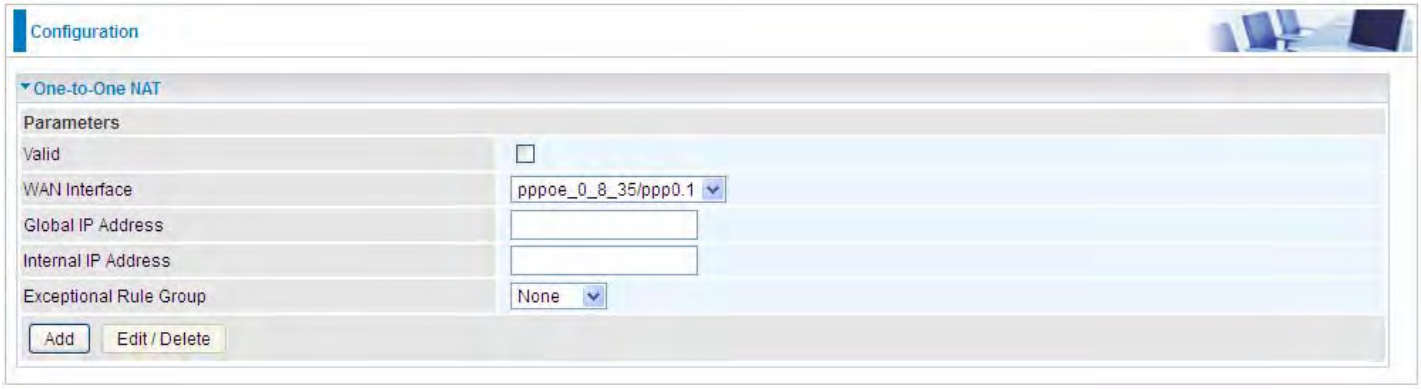
Exceptional Rule Group: Select the exceptional group listed. It is to grant or block DMZ access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block DMZ Access to this IP range, you can select Group1.

NOTE:	Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

Attention	If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid. If the DHCP server 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.

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address. If user has multiple global/public IP addresses from your ISP, you are free to use one-to-one NAT to assign some specific public IP for an internal IP like a public web server mapped with a global/public IP for outside access.



Valid: Check whether to valid the one-to-one NAT mapping rule.

WAN Interface: Select one based WAN interface to configure the one-to-one NAT.

Global IP address: The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

Internal Address: The IP address of an internal device in the LAN.

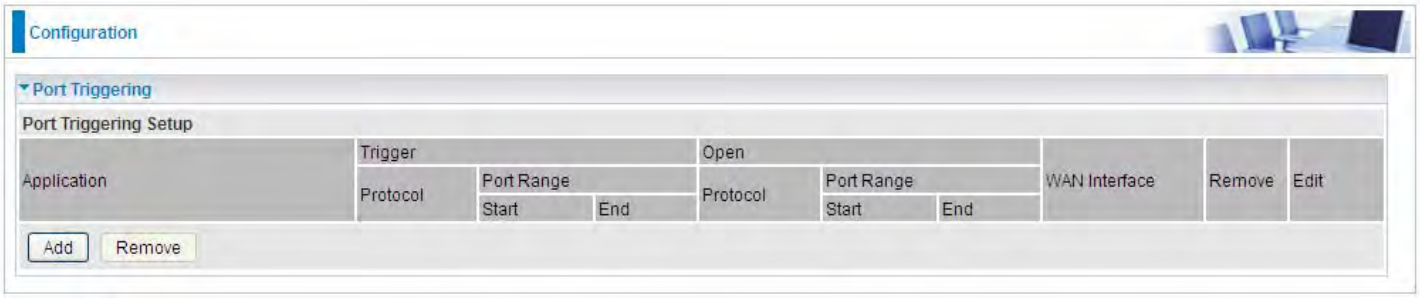
Exceptional Rule Group: Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 123.1.1.2.

For example, you have an ADSL connection of pppoe_0_8_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

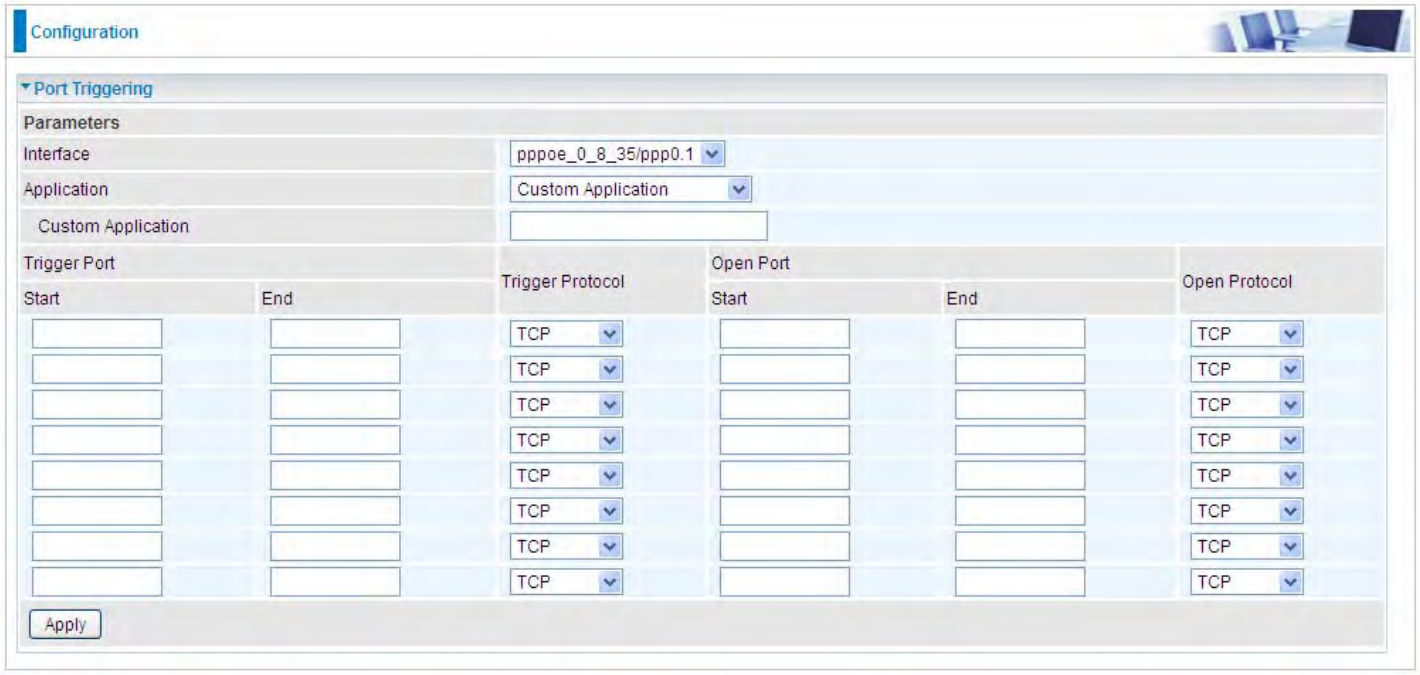
If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses.

Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.



Click **Add** to add a port triggering rule.



Interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application: Preinstalled applications or Custom Application user can customize the utility yourself.

Custom Application: It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

Trigger Port

- **Start:** Enter a port number as the triggering port starting number.
- **End:** Enter a port number as the triggering port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

- **Start:** Enter a port number as the open port staring number.
- **End:** Enter a port number as the open port ending number.

Any port in the range delimited by the ‘Start’ and ‘End’ would be the preset forwarding port or open port.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

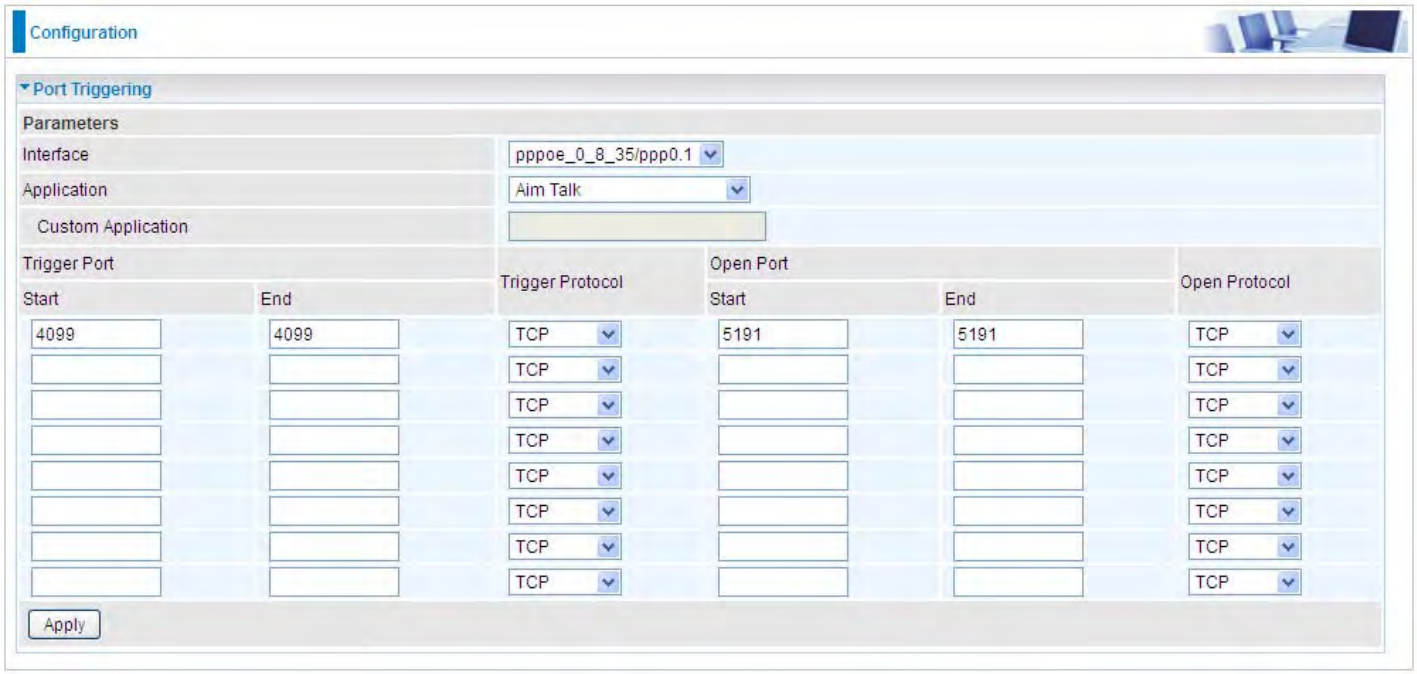
Set up

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

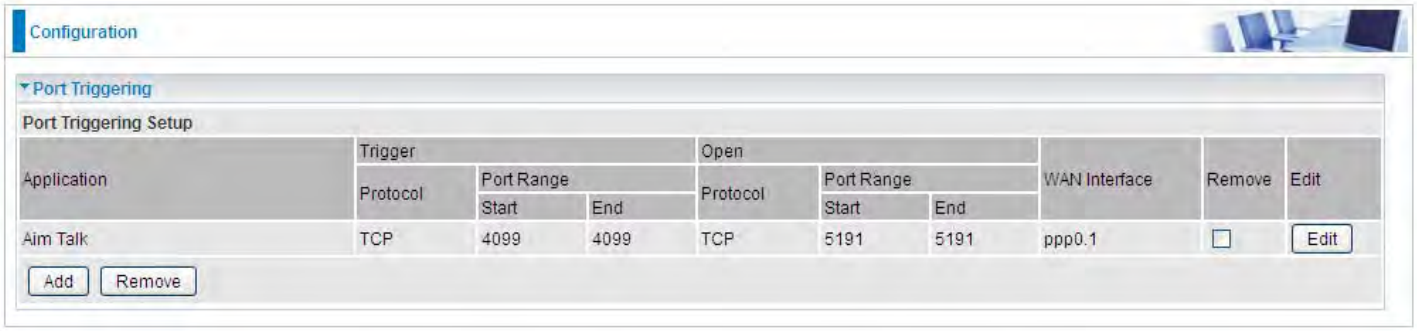
When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



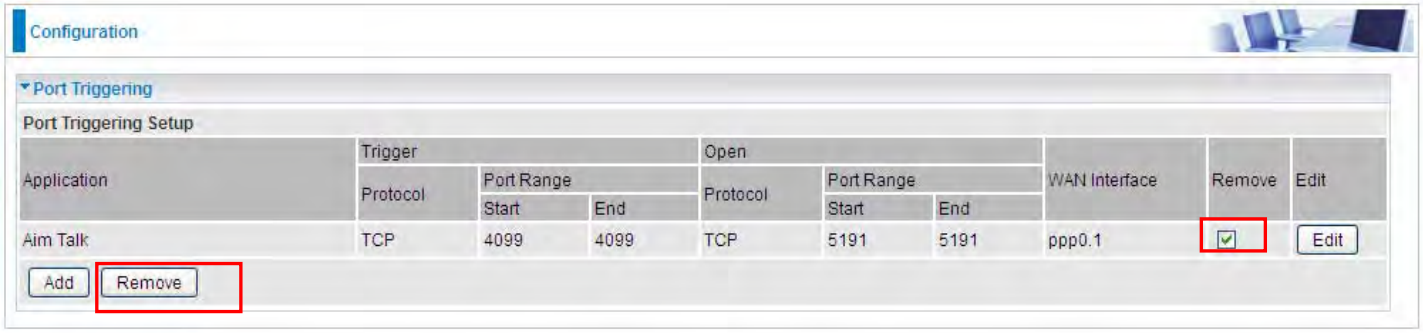
2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.



Edit/Remove

If you don’t need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press **Remove**.

Click **Edit** to re-edit your port-triggering rule.



ALG

The ALG Controls enable or disable protocols over application layer.

SIP: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP when SIP phone includes NAT-Traversal algorithm.

H.323: Enable to secure the voice communication using H.323 protocol when one or both terminals are behind a NAT.

IPSec: Enable IPSec ALG to allow one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

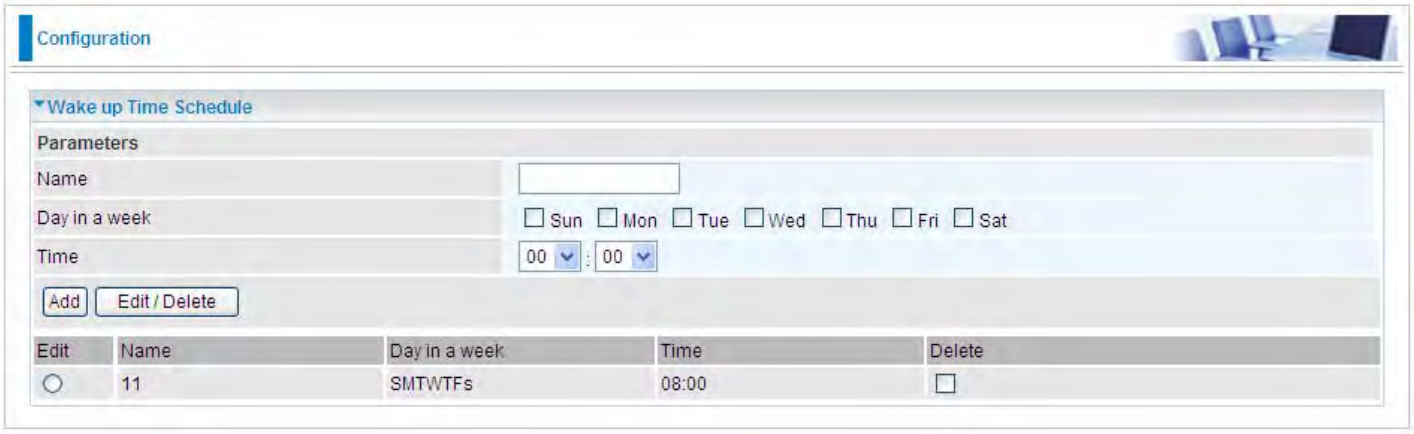
Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

Host Label: Enter identification for the host.

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Wake by Schedule: Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click Schedule to enter time schedule configuring page to set the exact timeline.



Add: After selecting, click Add then you can submit the Wake-up action.

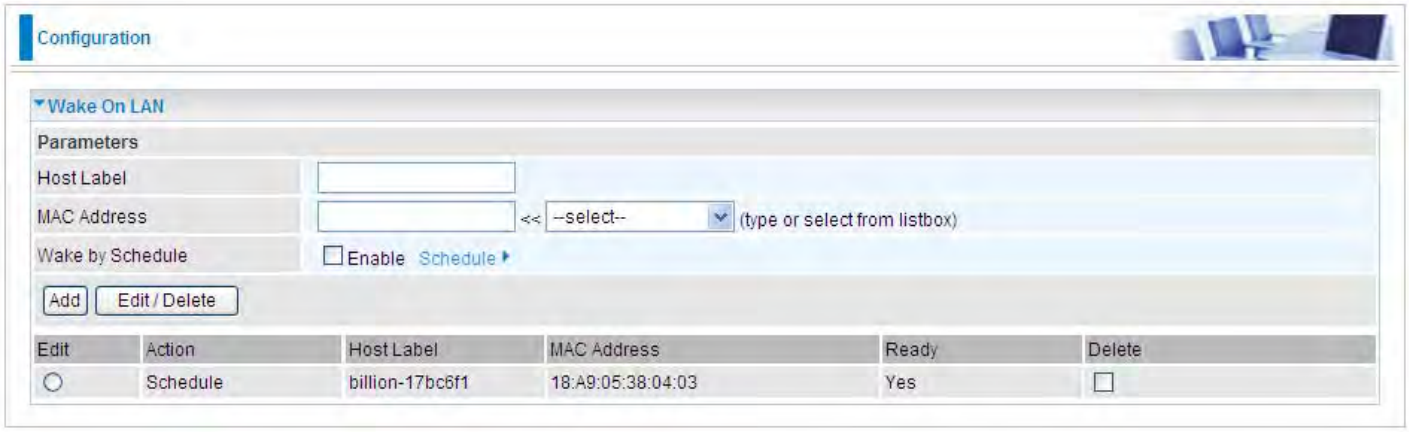
Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

"Yes" indicating the remote computer is ready for your waking up.

"No" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.


Configuration
Wake On LAN
Parameters
Host Label
MAC Address
<< --select-- (type or select from listbox)
Wake by Schedule
Enable Schedule
Add
Edit / Delete
Edit
Action
Host Label
MAC Address
Ready
Delete
Schedule
billion-17bc6f1
18:A9:05:38:04:03
Yes

VPN

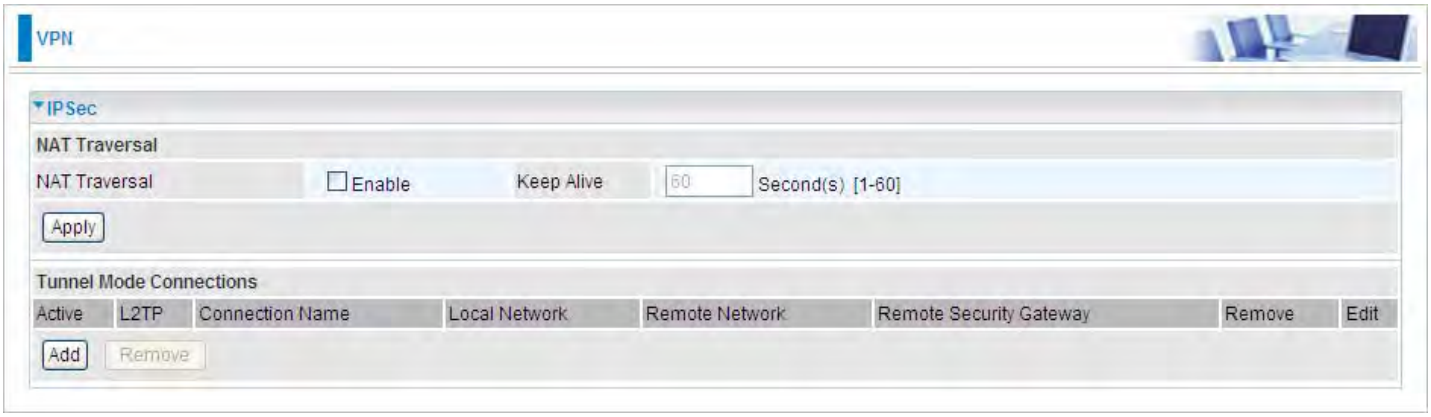
A **virtual private network** (**VPN**) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption.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

IPSec

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

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

Note: A maximum of 16 sessions for IPSec.



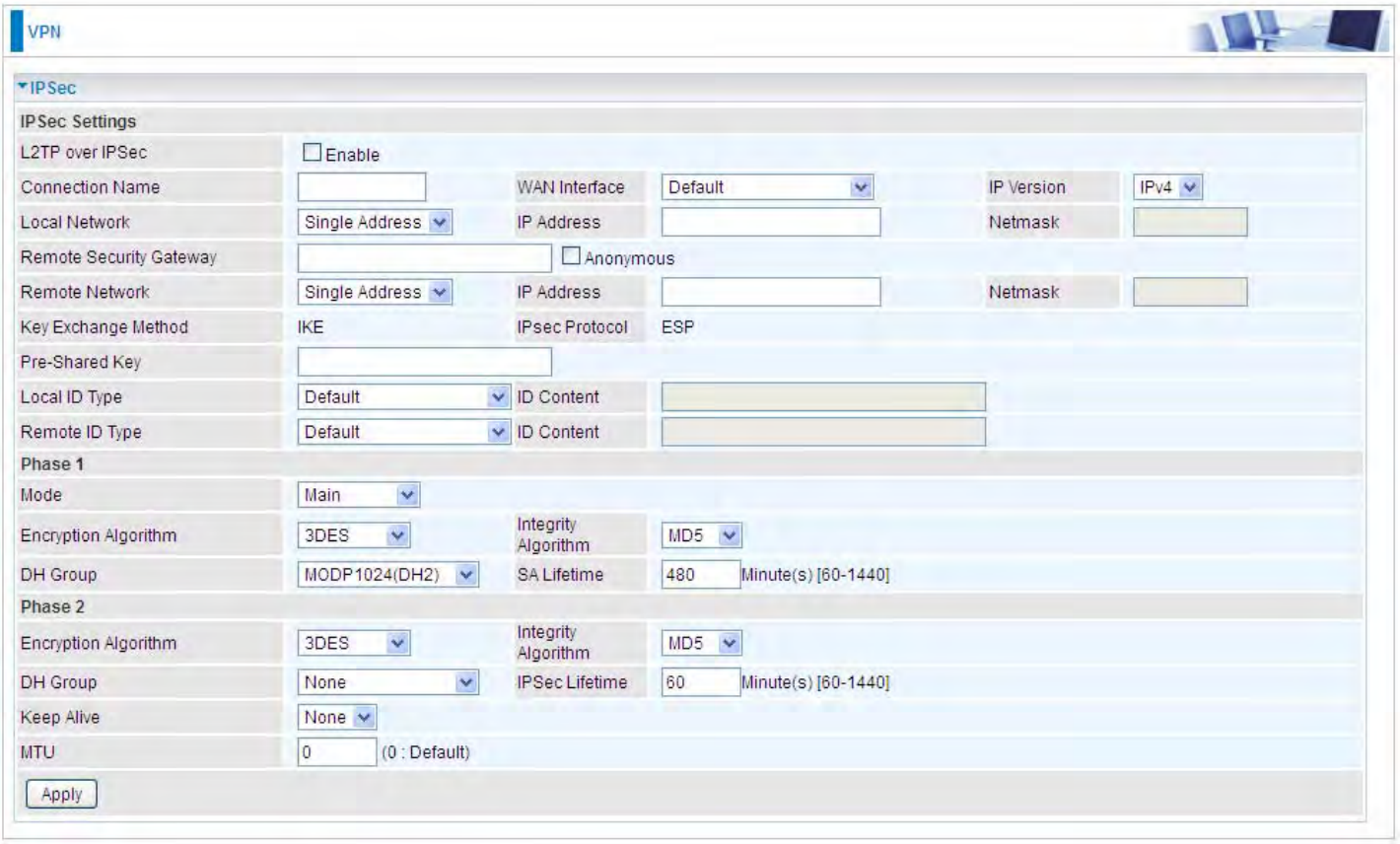
NAT Traversal

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

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

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

Click **Add** to create IPSec connections.



IPSec Settings

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See L2TPover IPSec

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

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

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

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

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

IP Address: The local network address.

Netmask: The local network netmask.

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

Anonymous: Enable any IP to connect in.

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

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

Key Exchange Method: Displays key exchange method.

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

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

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

Phase 1

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

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

- **DES:** Stands for Triple 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.

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

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

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

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

Phase 2

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

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

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

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

Ping for Keep Alive: Select the operation methods:

- **None:** The default setting is “None”. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.

- **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

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

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

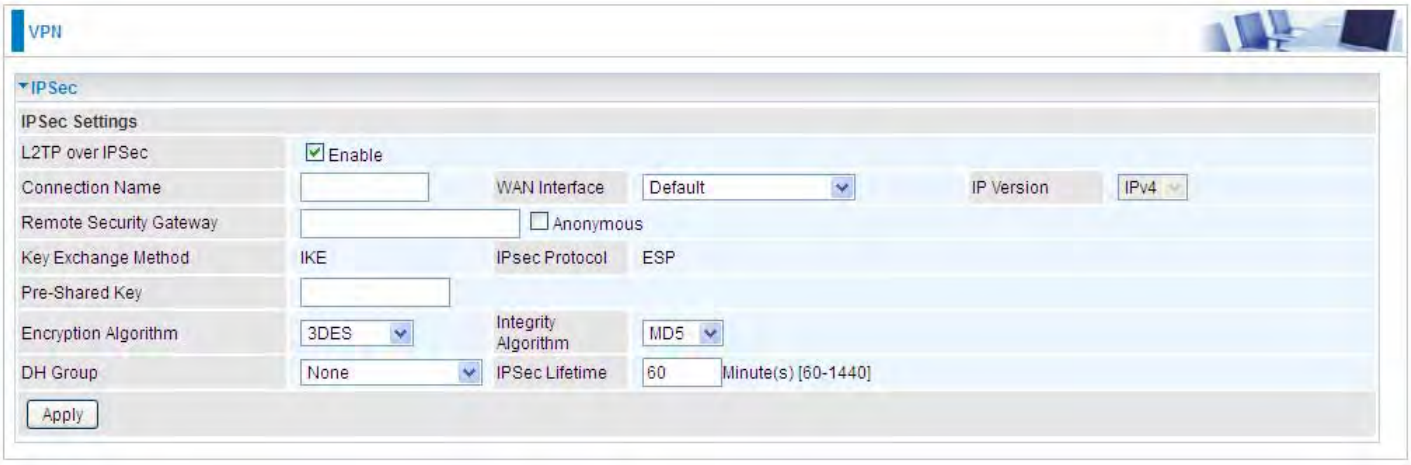
- **Ping:** This mode will detect whether the remote IPSec peer has lost or not by pinging specify IP address.

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

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

MTU: Maximum Transmission Unit, maximum value is 1500.

IPSec for L2TP



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

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

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

Key Exchange Method: Displays key exchange method.

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

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

- **DES:** Stands for Triple 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.

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

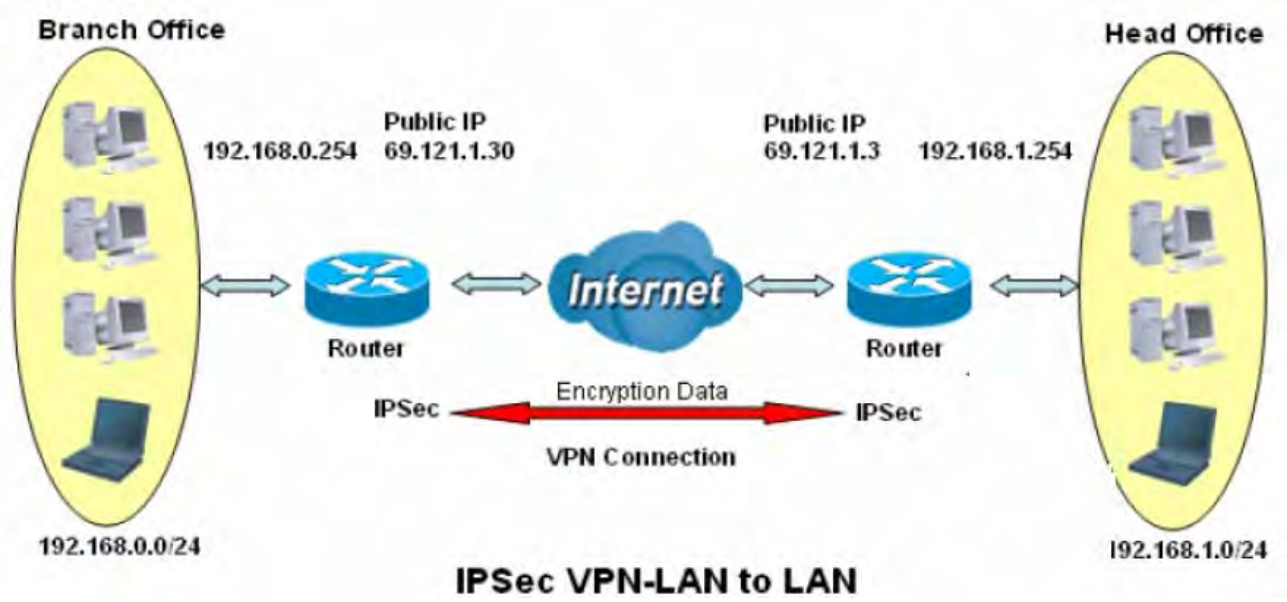
- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

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

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

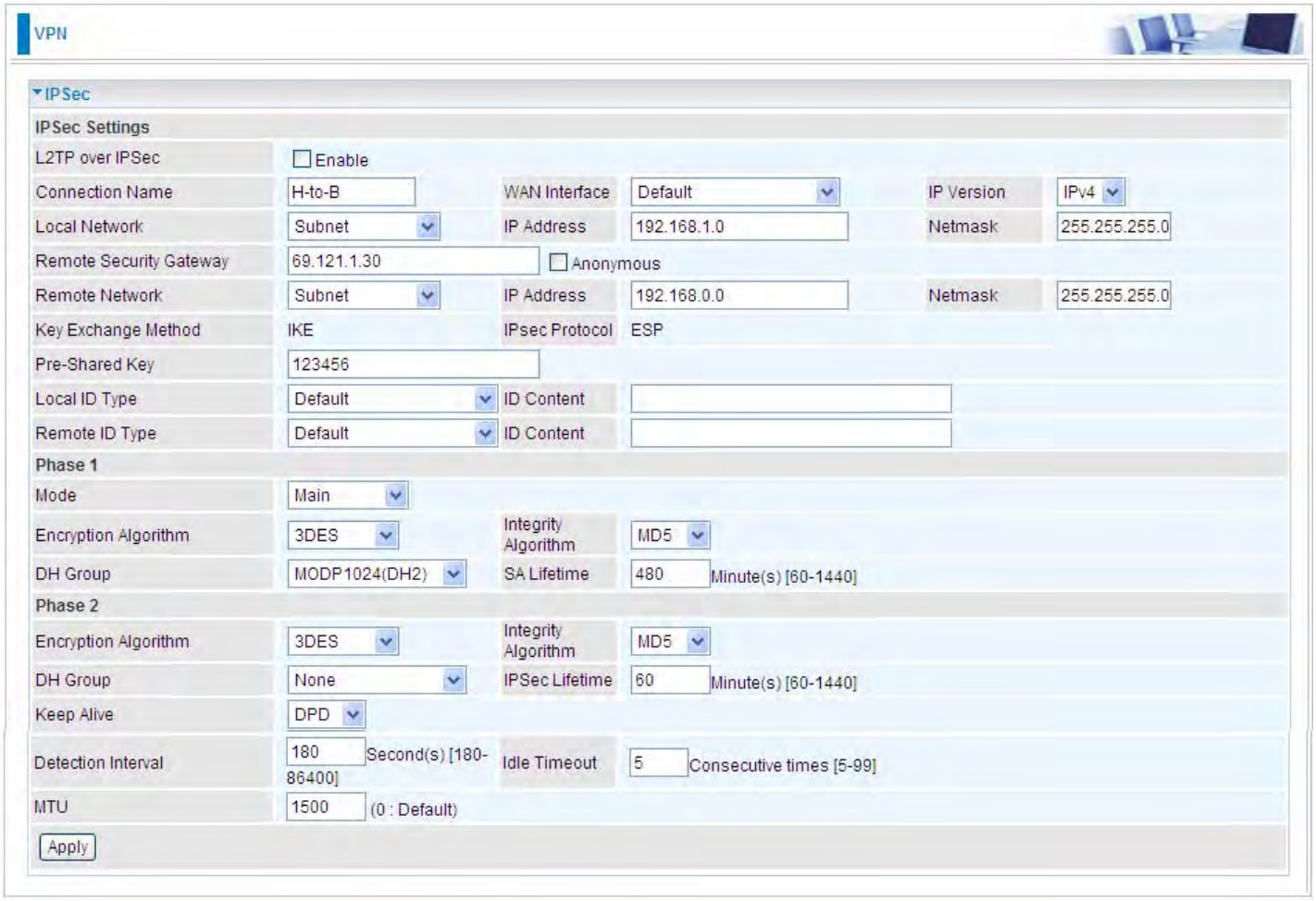
Examples:

1. **LAN-to-LAN connection**
Two BiPAC 7820NZs want to setup a secure IPSec VPN tunnel
Note: The IPSec Settings shall be consistent between the two routers.



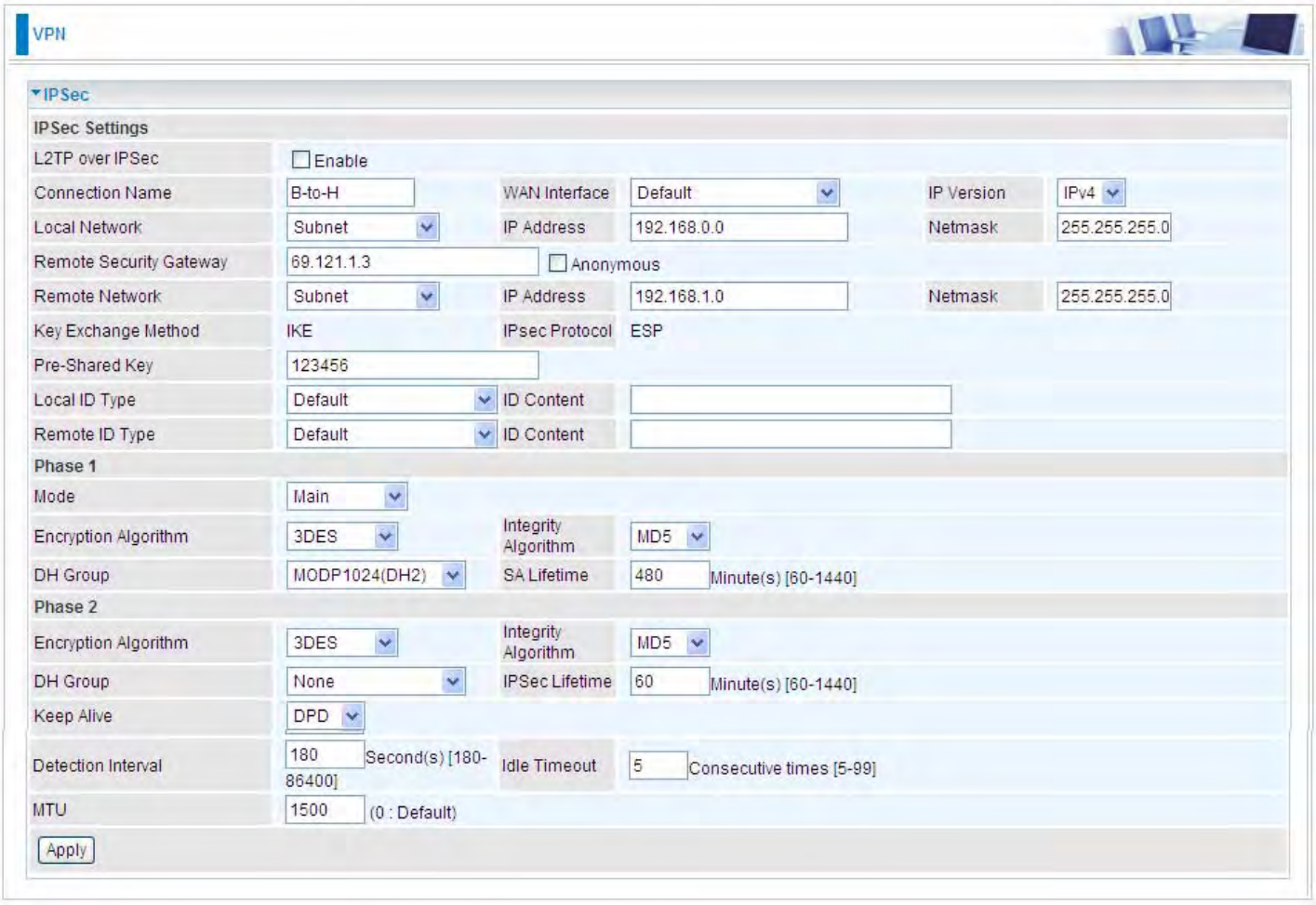
Head Office Side:
Setup details:

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


VPN
IPSec
IPSec Settings
L2TP over IPSec
Enable
Connection Name
H-to-B
WAN Interface
Default
IP Version
IPv4
Local Network
Subnet
IP Address
192.168.1.0
Netmask
255.255.255.0
Remote Security Gateway
69.121.1.30
Anonymous
Remote Network
Subnet
IP Address
192.168.0.0
Netmask
255.255.255.0
Key Exchange Method
IKE
IPsec Protocol
ESP
Pre-Shared Key
123456
Local ID Type
Default
ID Content
Remote ID Type
Default
ID Content
Phase 1
Mode
Main
Encryption Algorithm
3DES
Integrity Algorithm
MD5
DH Group
MODP1024(DH2)
SA Lifetime
480
Minute(s) [60-1440]
Phase 2
Encryption Algorithm
3DES
Integrity Algorithm
MD5
DH Group
None
IPSec Lifetime
60
Minute(s) [60-1440]
Keep Alive
DPD
Detection Interval
180
Second(s) [180-86400]
Idle Timeout
5
Consecutive times [5-99]
MTU
1500
(0 : Default)
Apply

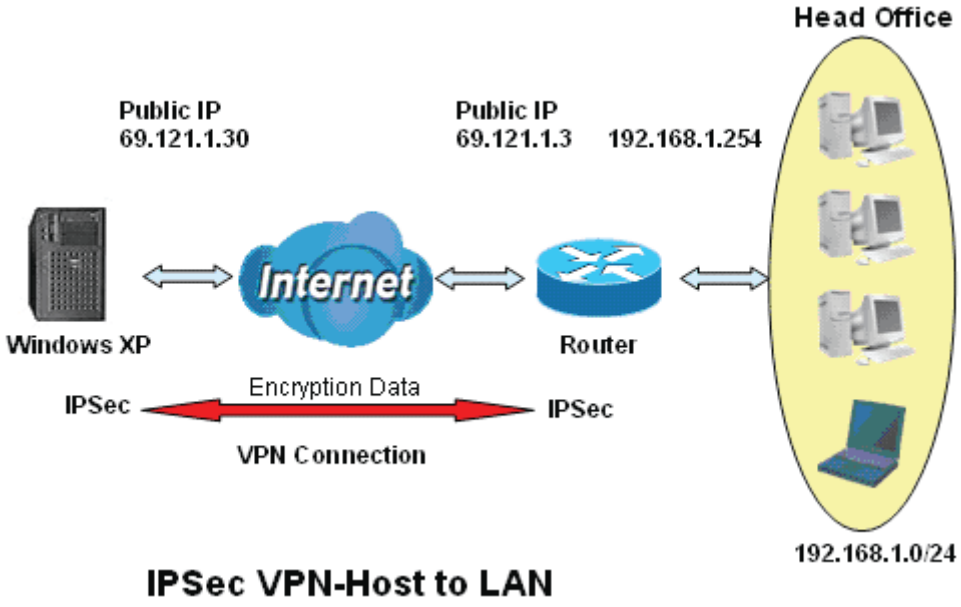
Branch Office Side:
Setup details: the same operation as done in Head Office side

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



3. Host to LAN

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



IPSec VPN-Host to LAN

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

VPN

IPSec

IPSec Settings					
L2TP over IPSec	☐ Enable				
Connection Name	Headoffice-to-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30 ☐ Anonymous				
Remote Network	Single Address	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD				
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				

Apply

VPN Account

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

Name: A user-defined name for the connection.

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

Username: Please input the username for this account.

Password: Please input the password for this account.

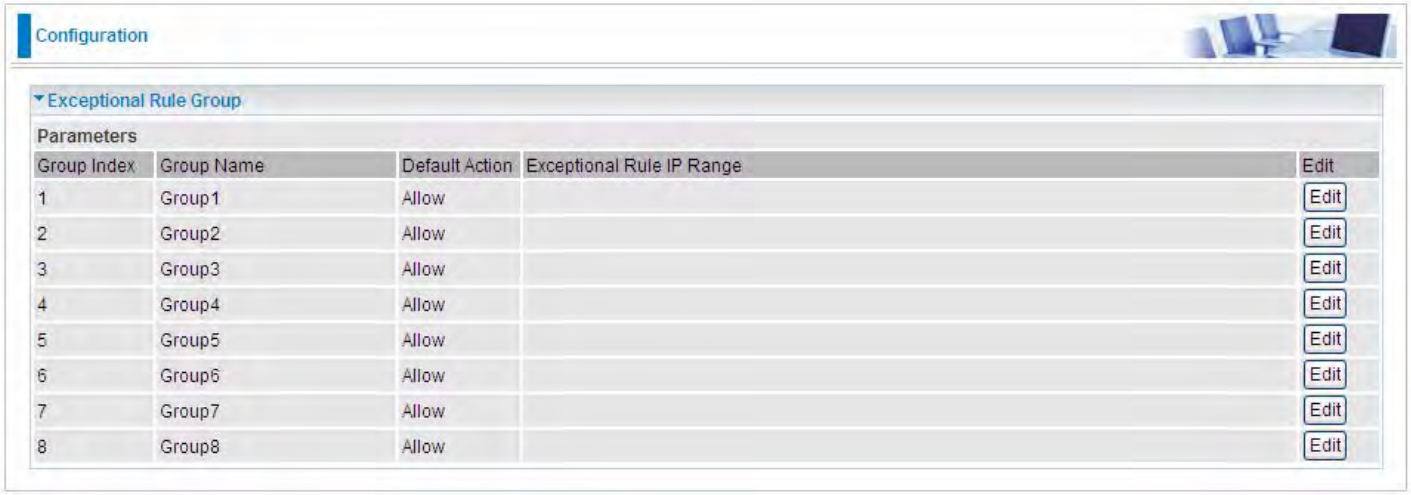
Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

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

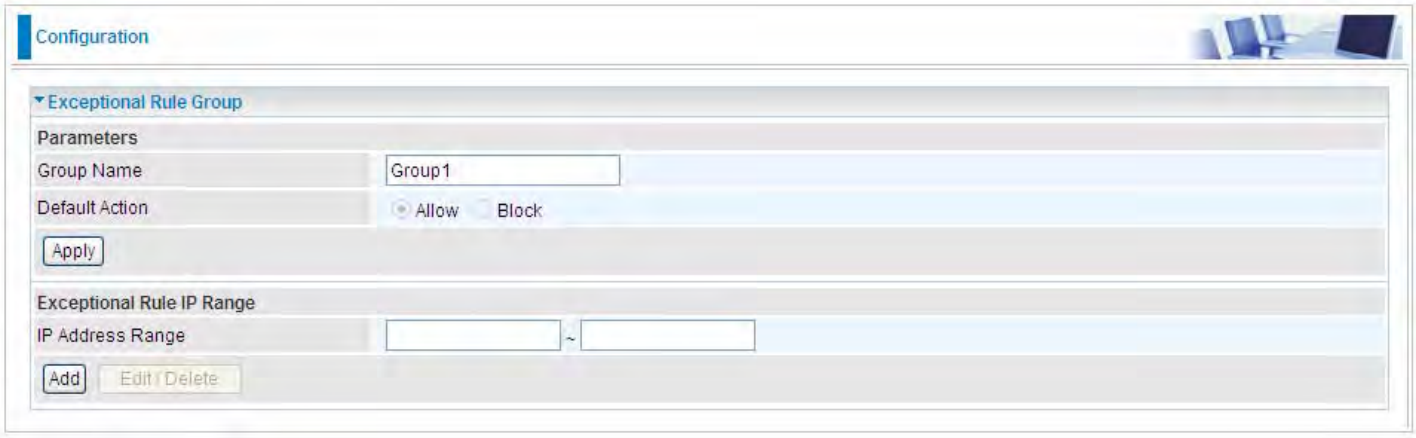
Peer Netmask: Please input the Netmask for remote network.

Exceptional Rule Group

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



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



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

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

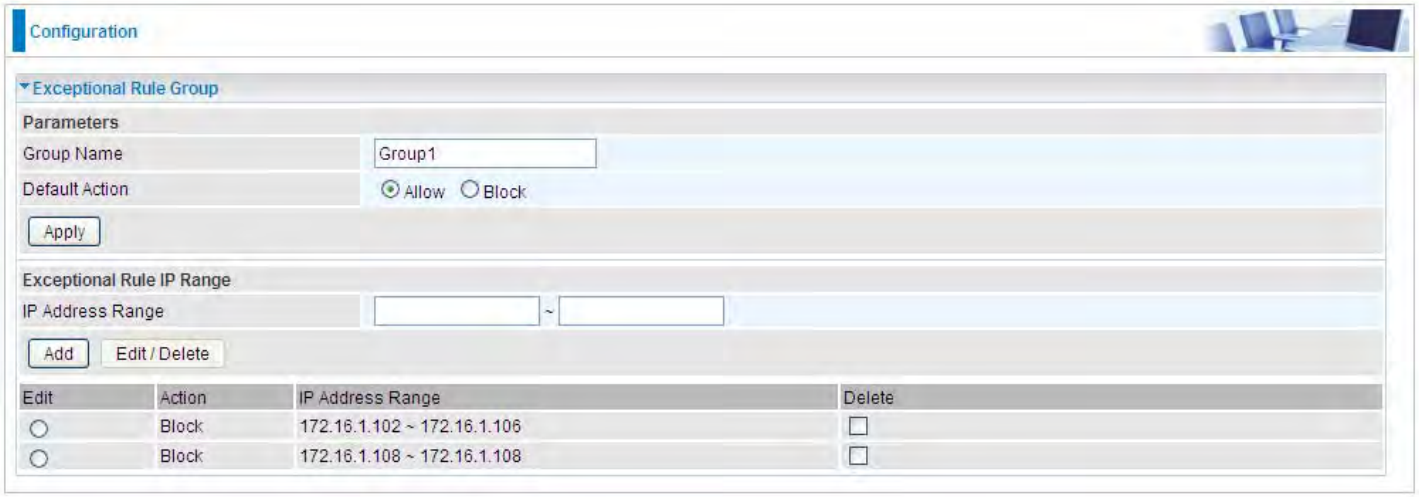
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

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

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

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



PPTP

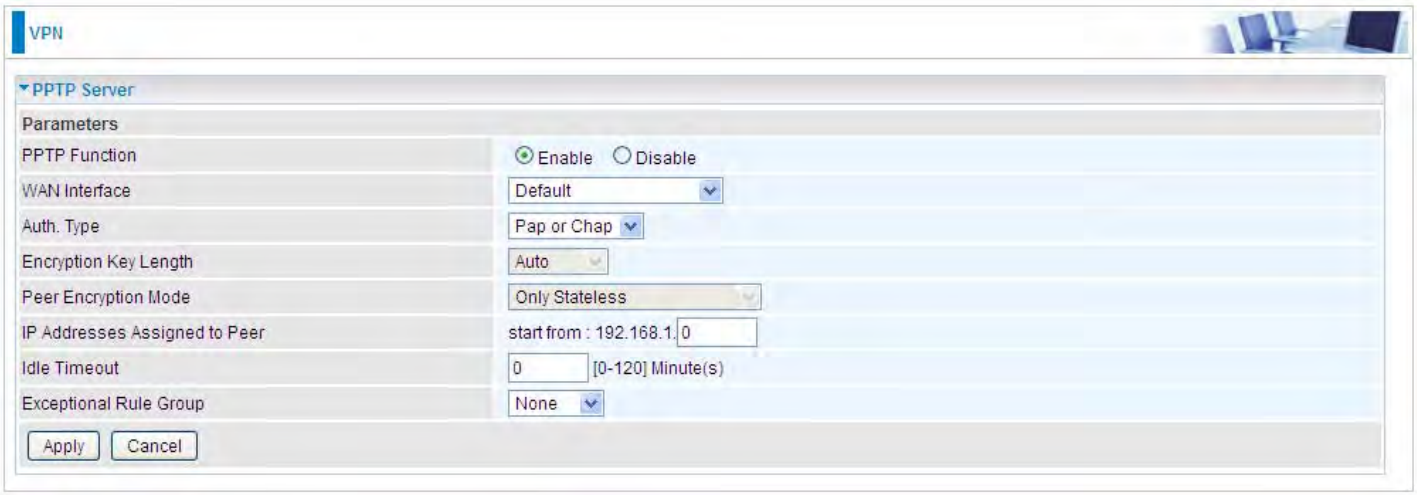
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP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

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

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

PPTP Server

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



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

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

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

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

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

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

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

minutes.

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

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

PPTP Client

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

Name: user-defined name for identification.

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

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

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

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

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

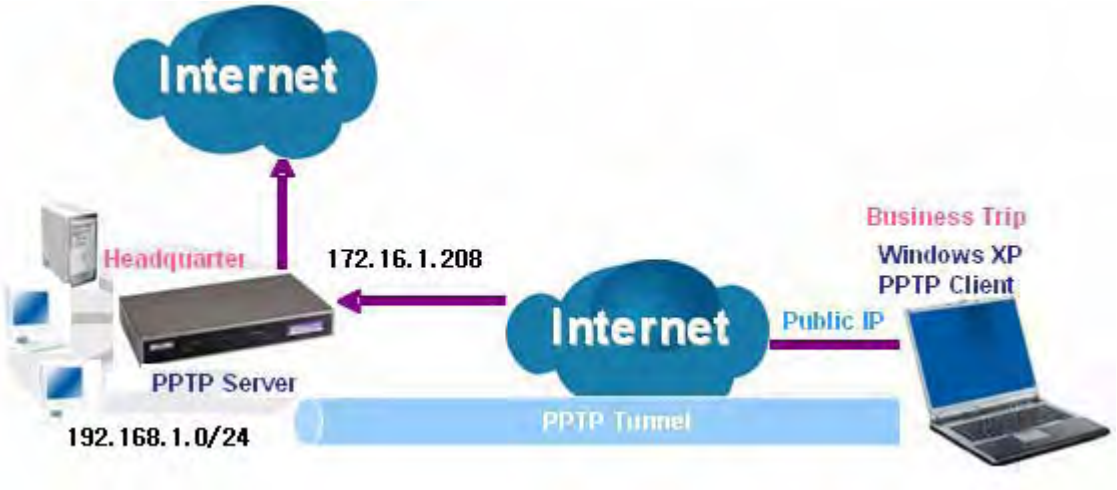
Time to Connect: Select Always to keep the connection always on, or Manual to connect manually any time.

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

Peer Netmask: Please input the Netmask for server peer.

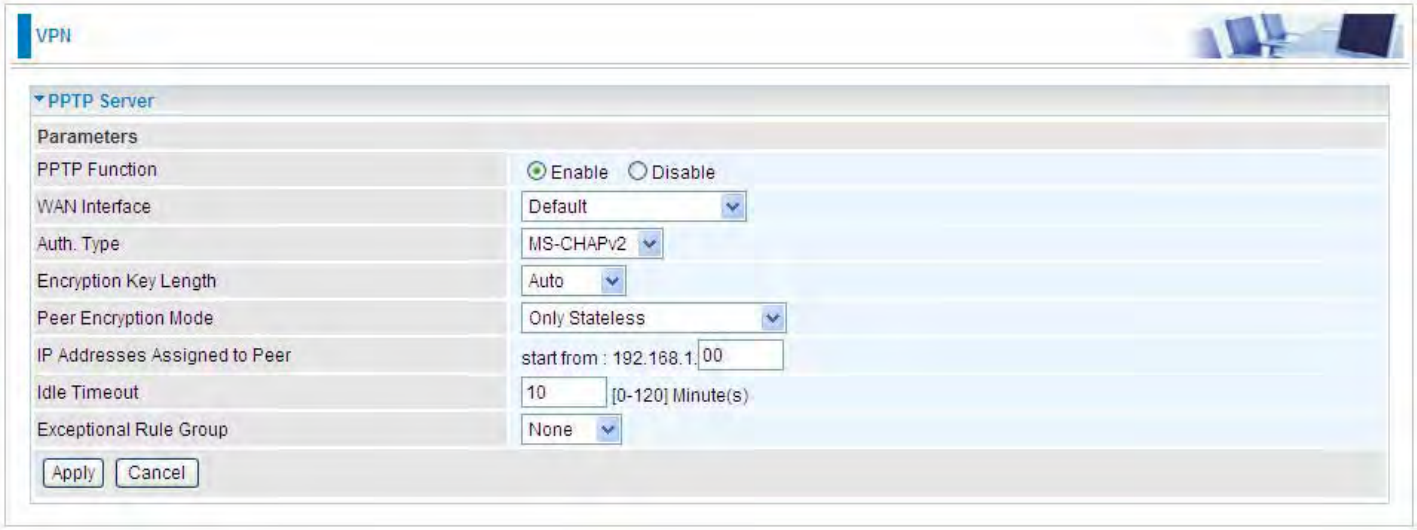
Click **Add** button to save your changes.

Example: PPTP Remote Access with Windows7
(Note: inside test with 172.16.1.208, just an example for illustration)



Server Side:

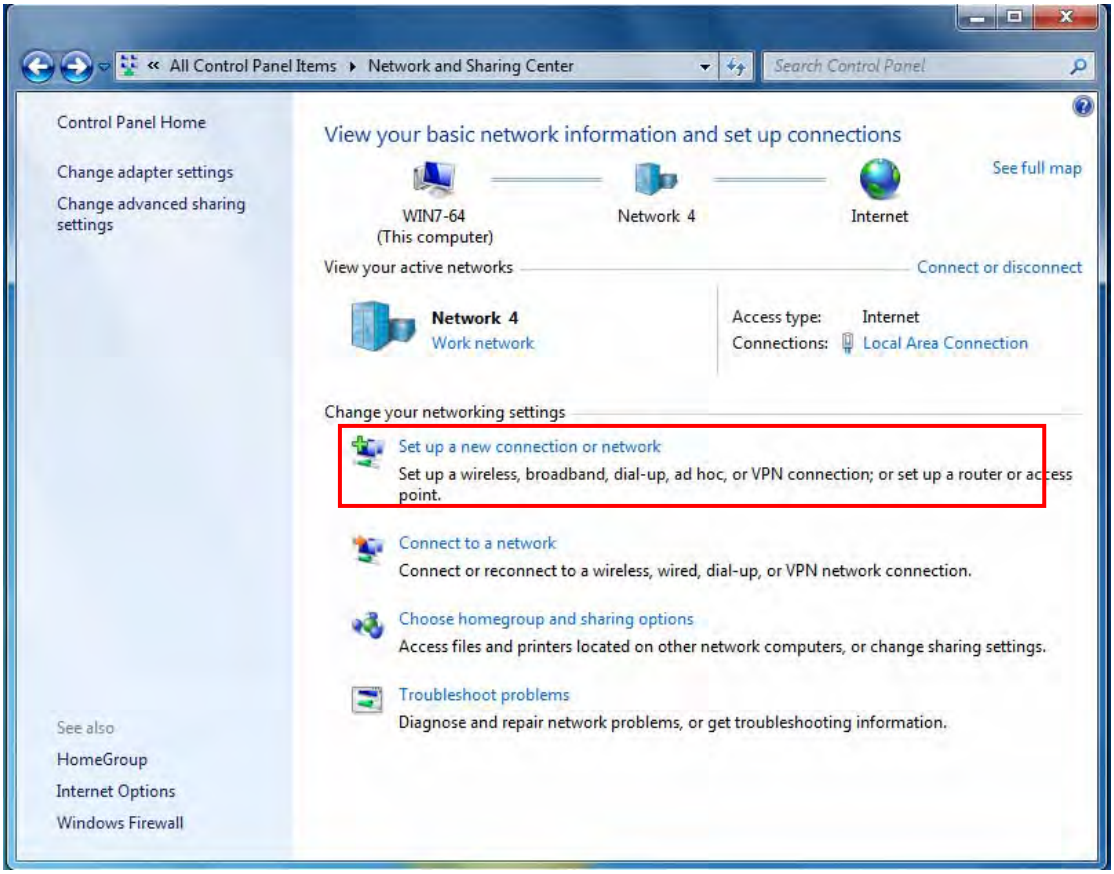
1. Configuration > **VPN** > **PPTP** and Enable the PPTP function, Click **Apply**.



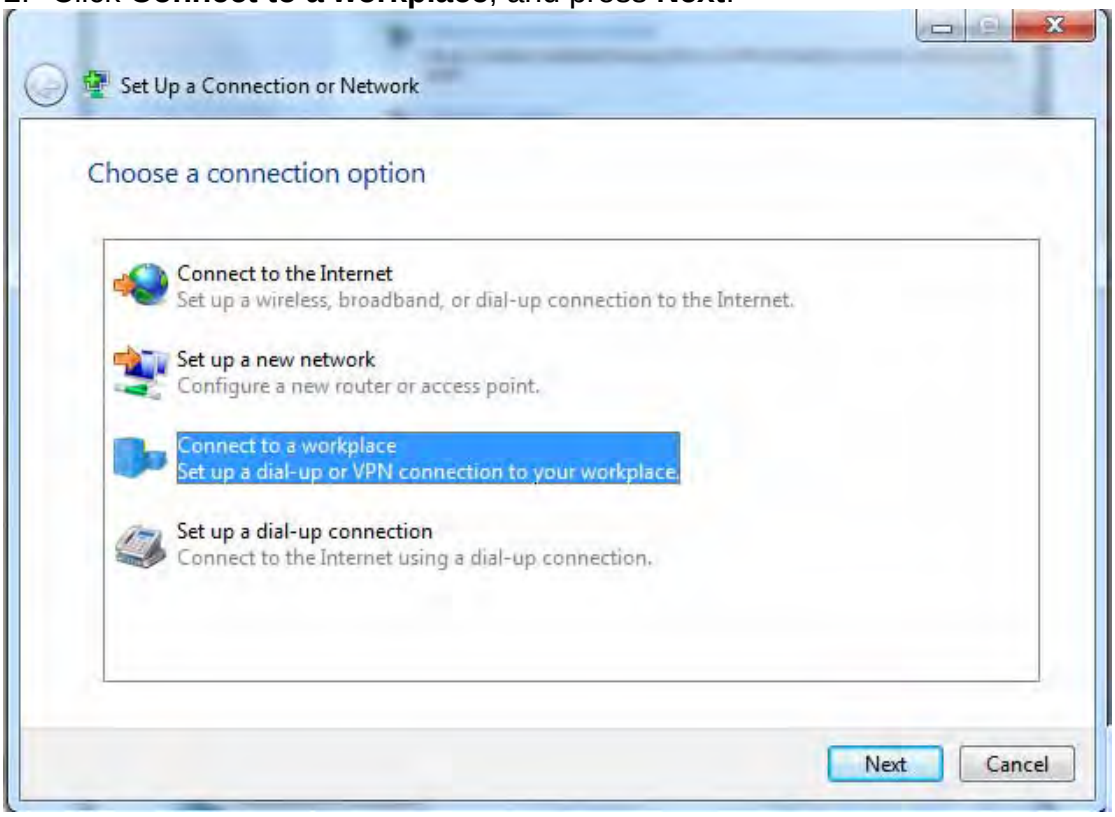
2. Create a PPTP Account “test”.

Client Side:

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

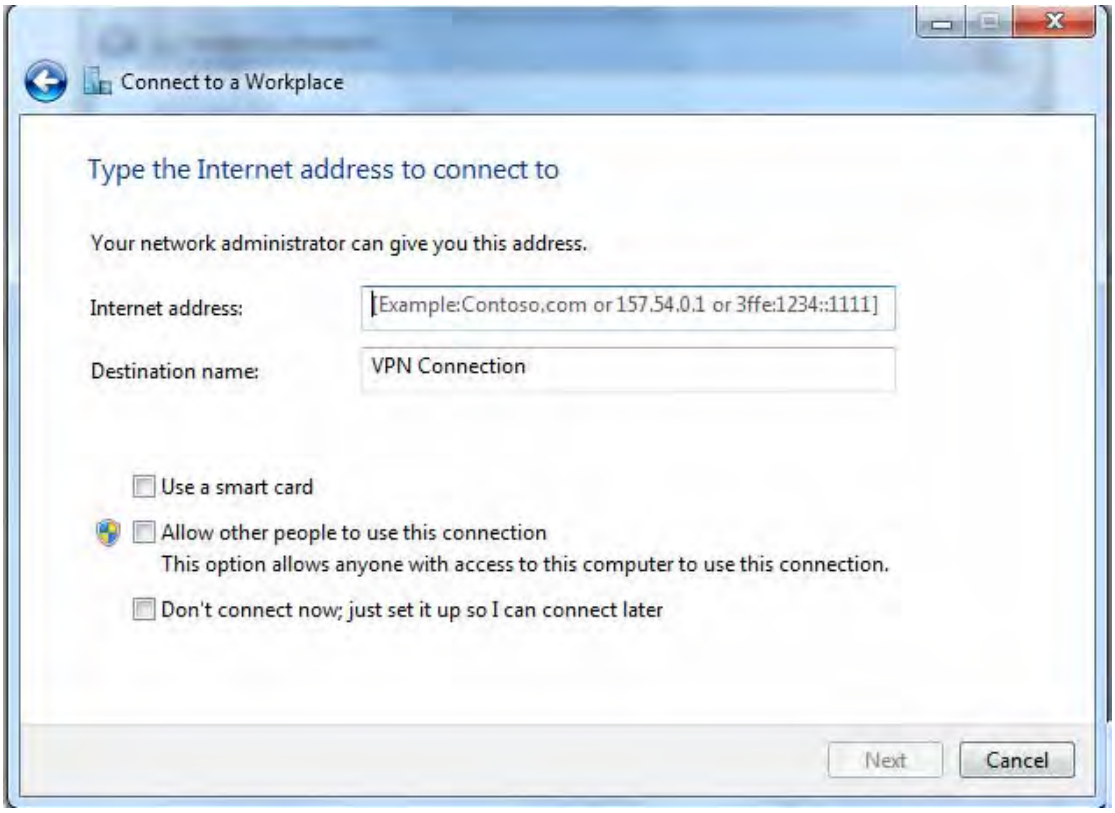


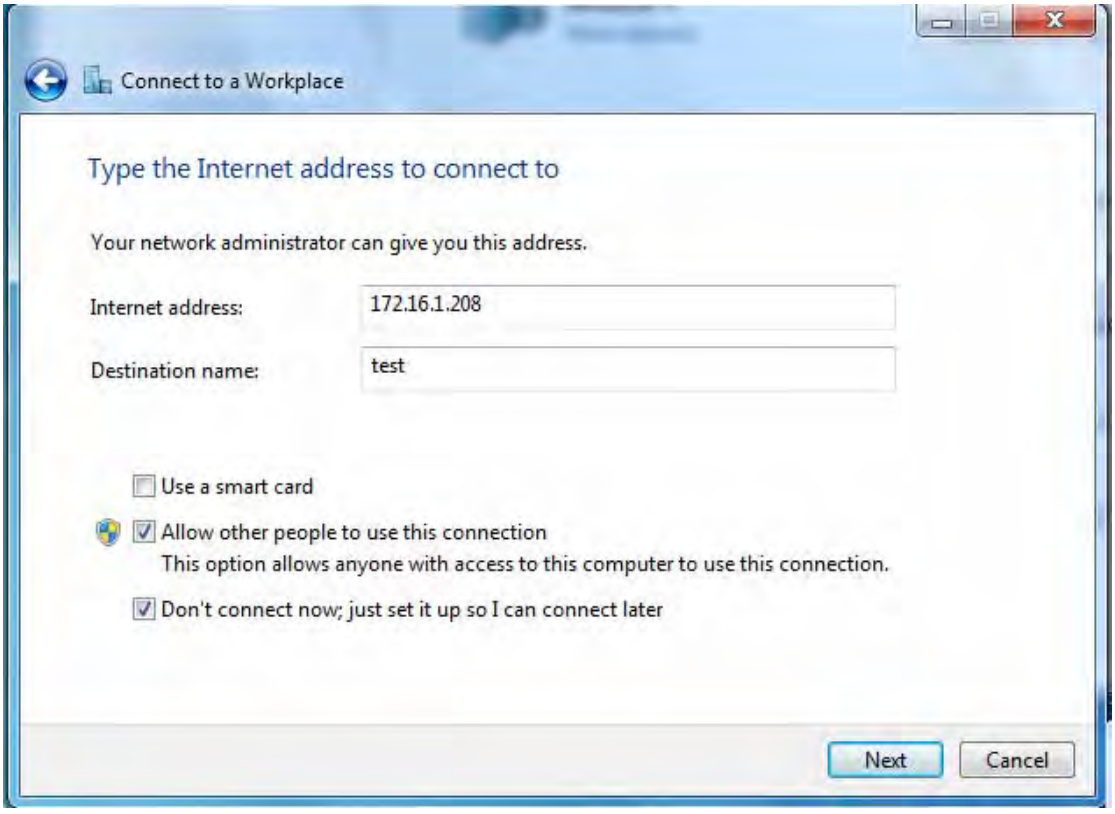
2. Click **Connect to a workplace**, and press **Next**.



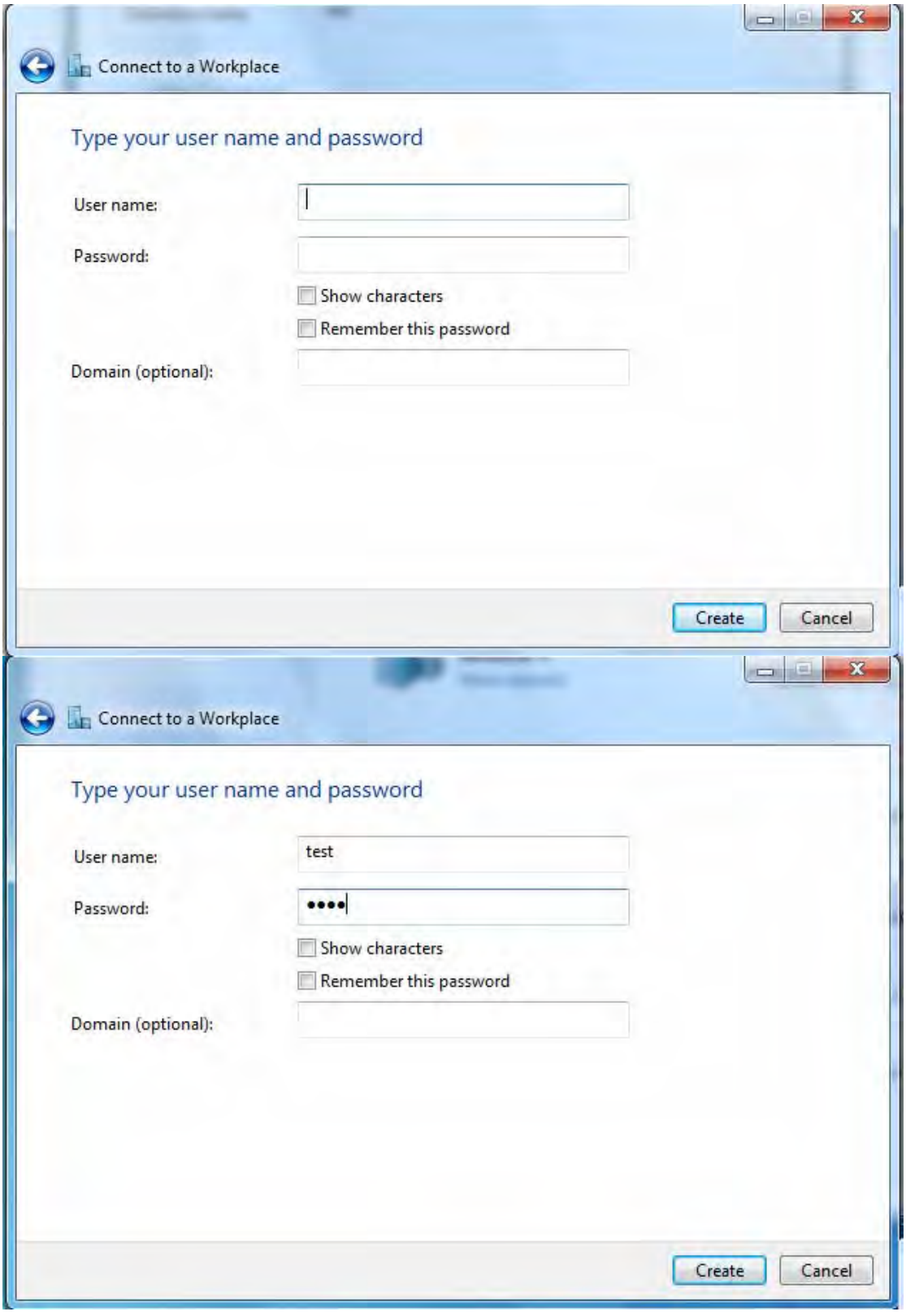
3. Select **Use my Internet connection (VPN)** and press **Next**.

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

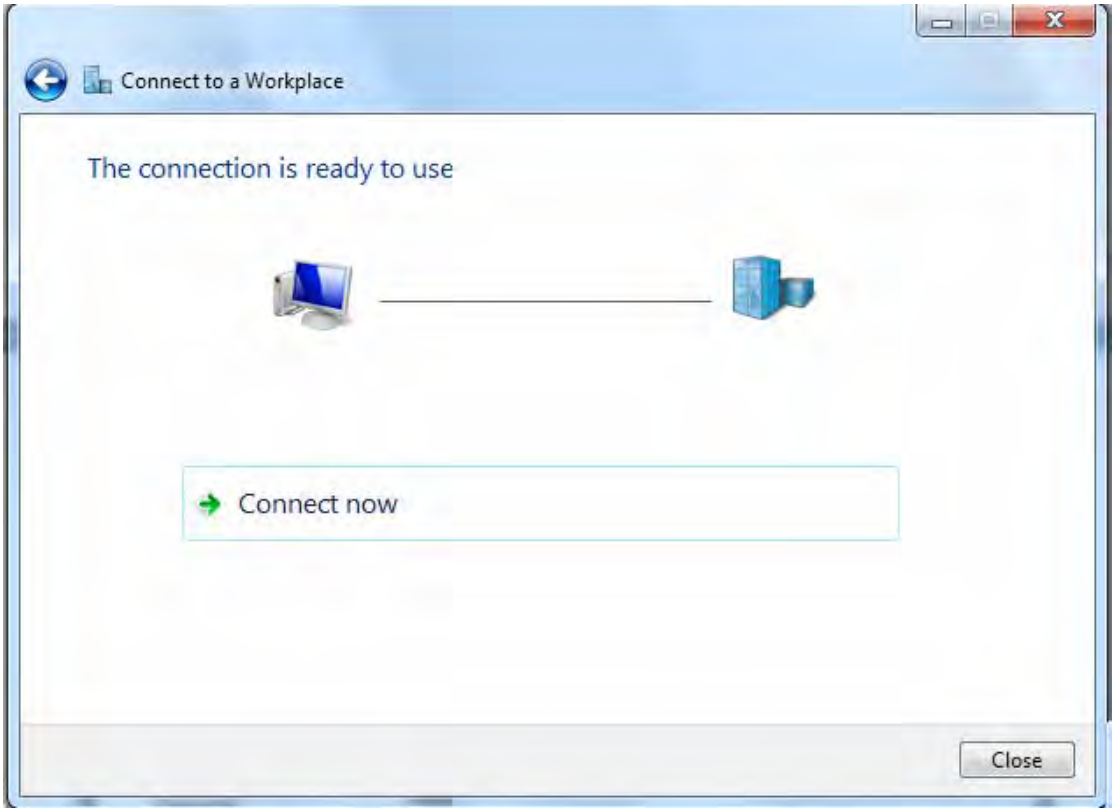


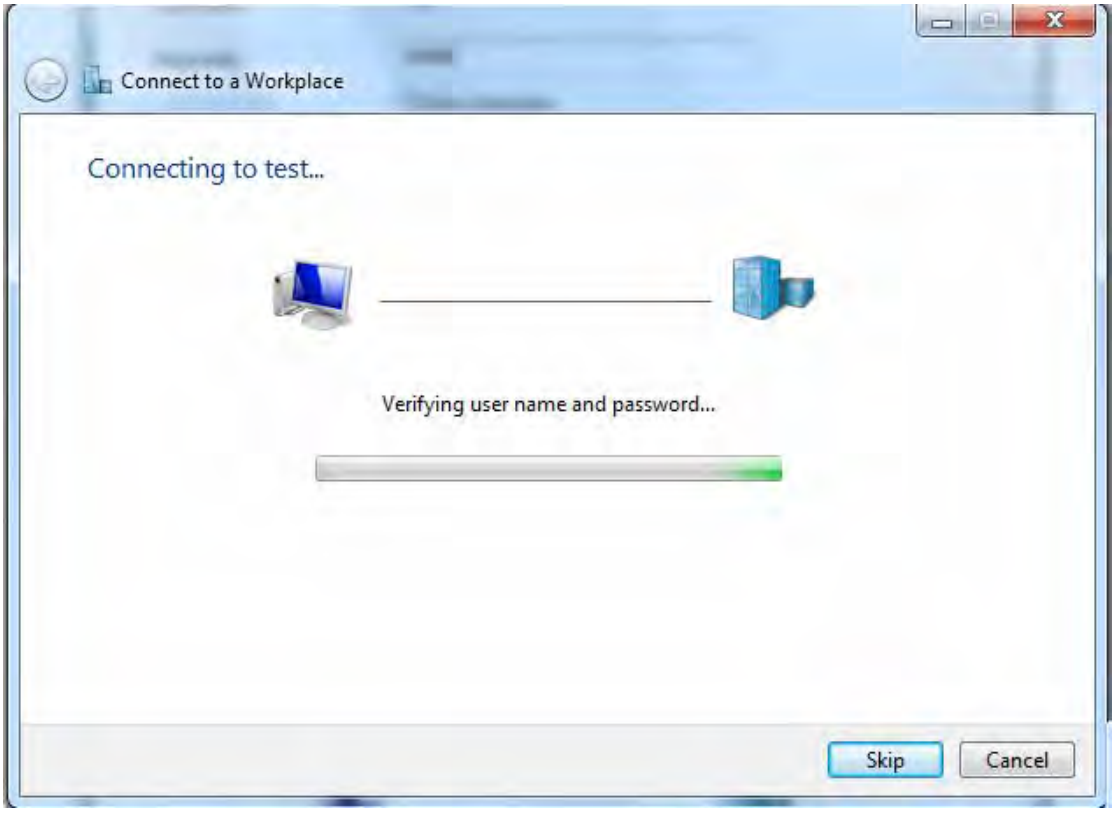


5. Input the account (**user name** and **password**) and press **Create**.

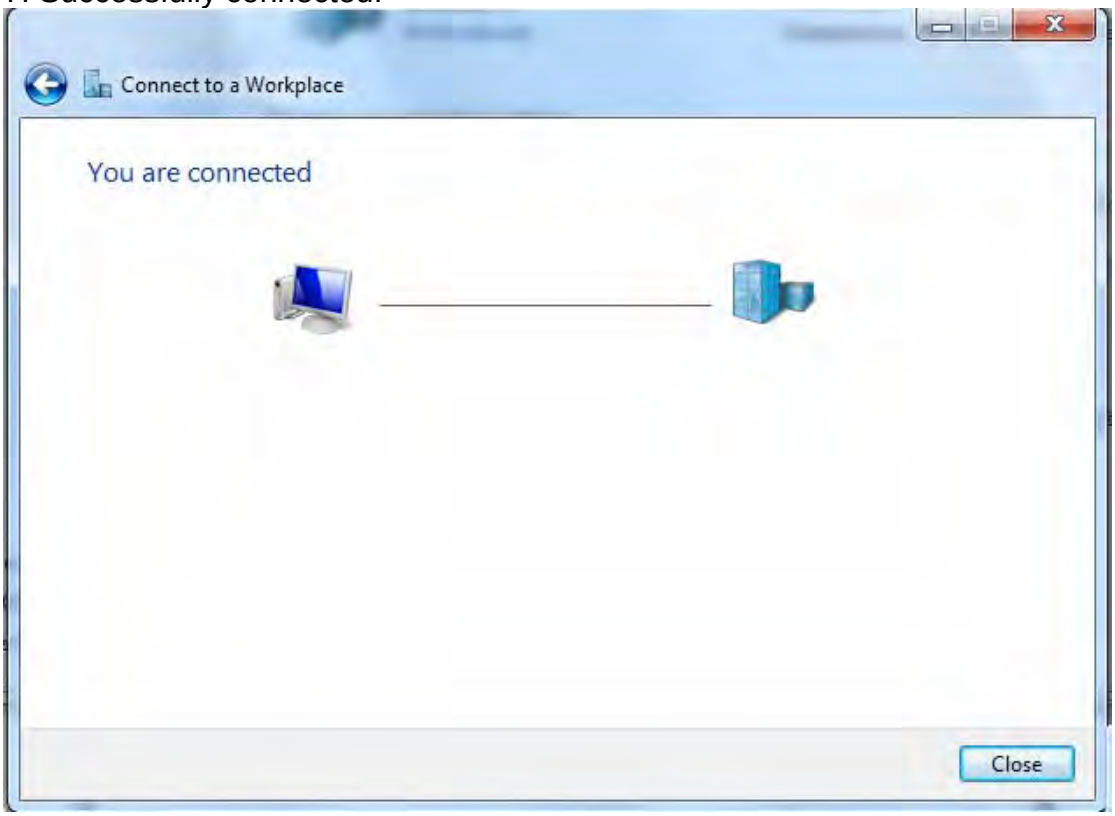


6. Connect to the server.

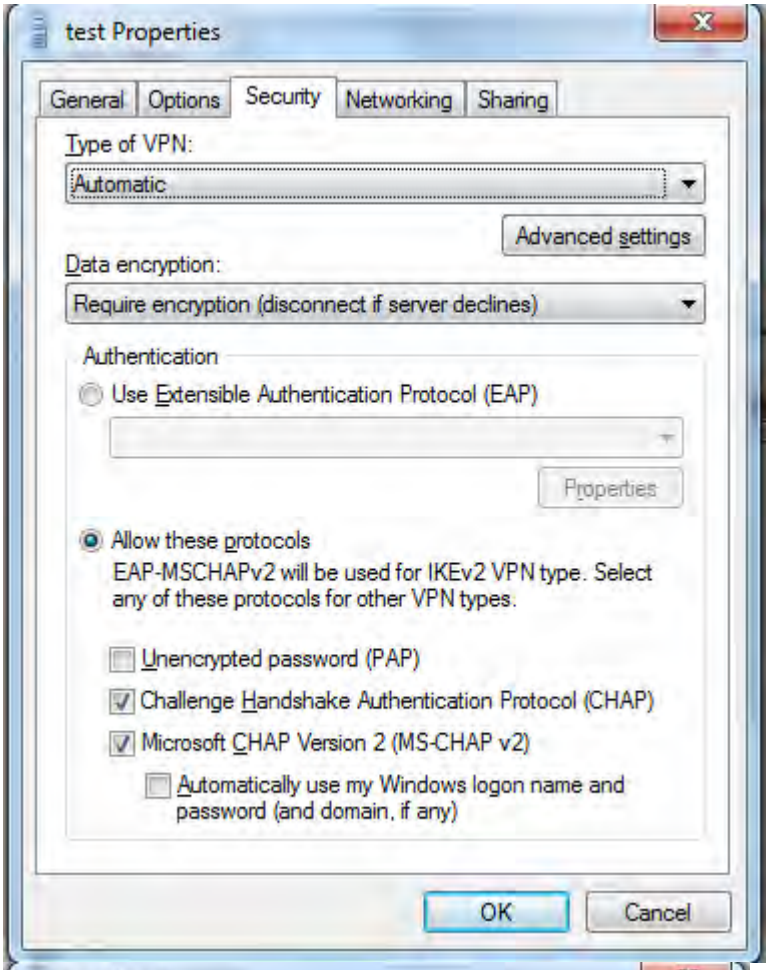


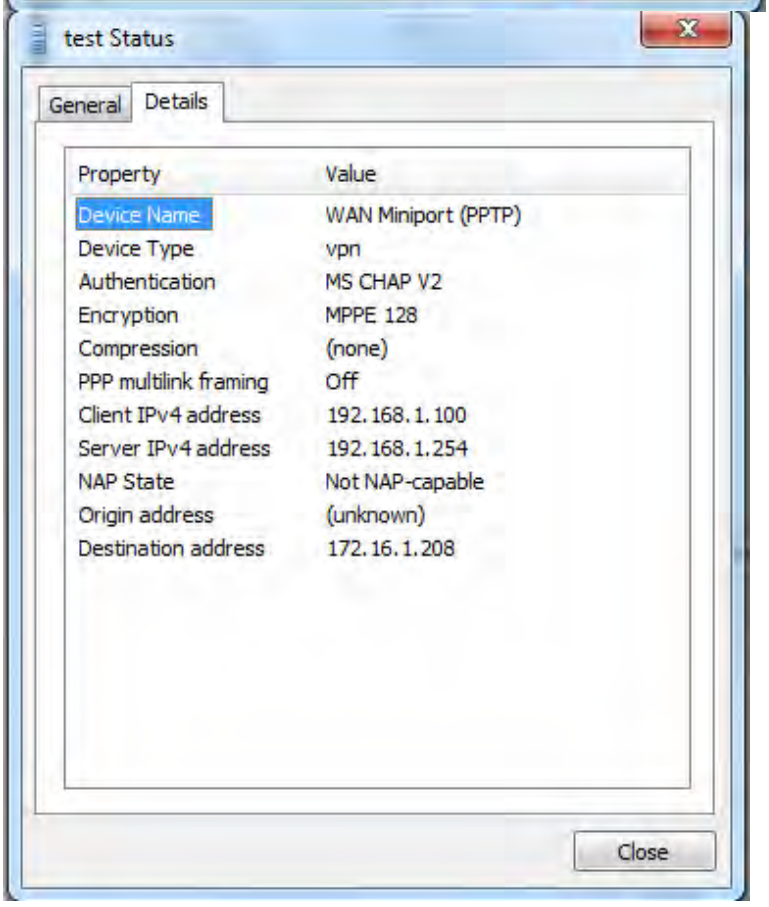


7. Successfully connected.



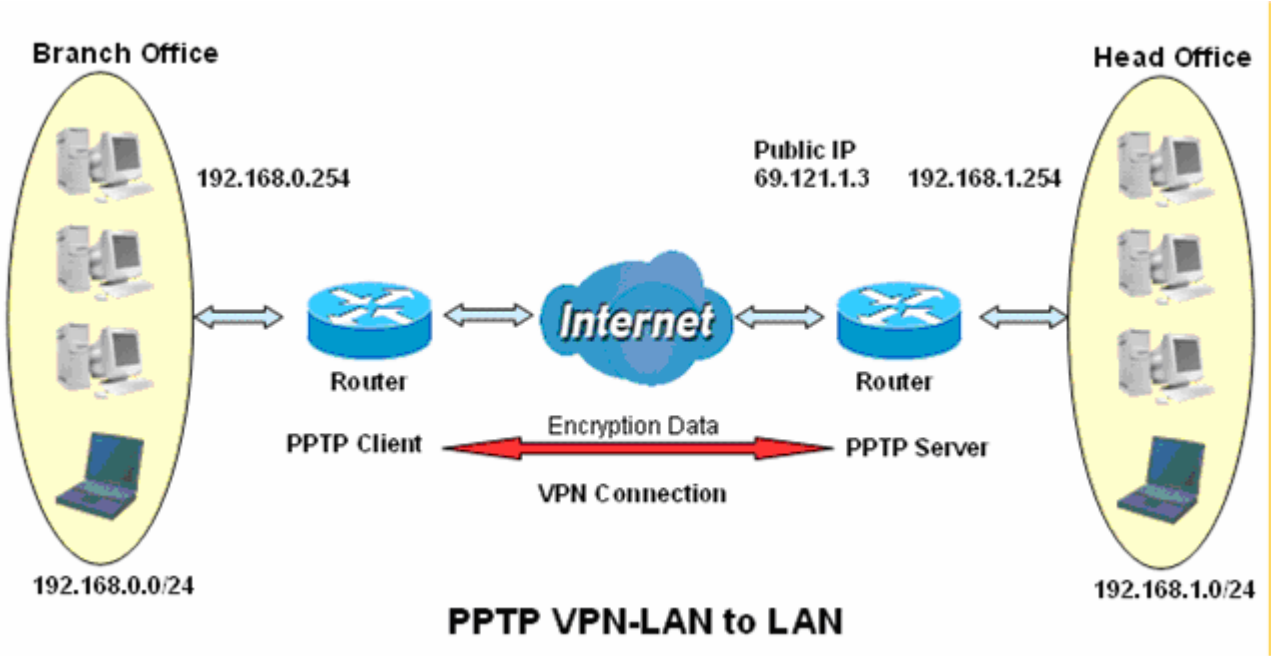
PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click “test” icon, and select “**Properties**” to change the security parameters (if the connection fails, users can go here to change the settings)


test Properties
General
Options
Security
Networking
Sharing
Type of VPN:
Automatic
Advanced settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK
Cancel

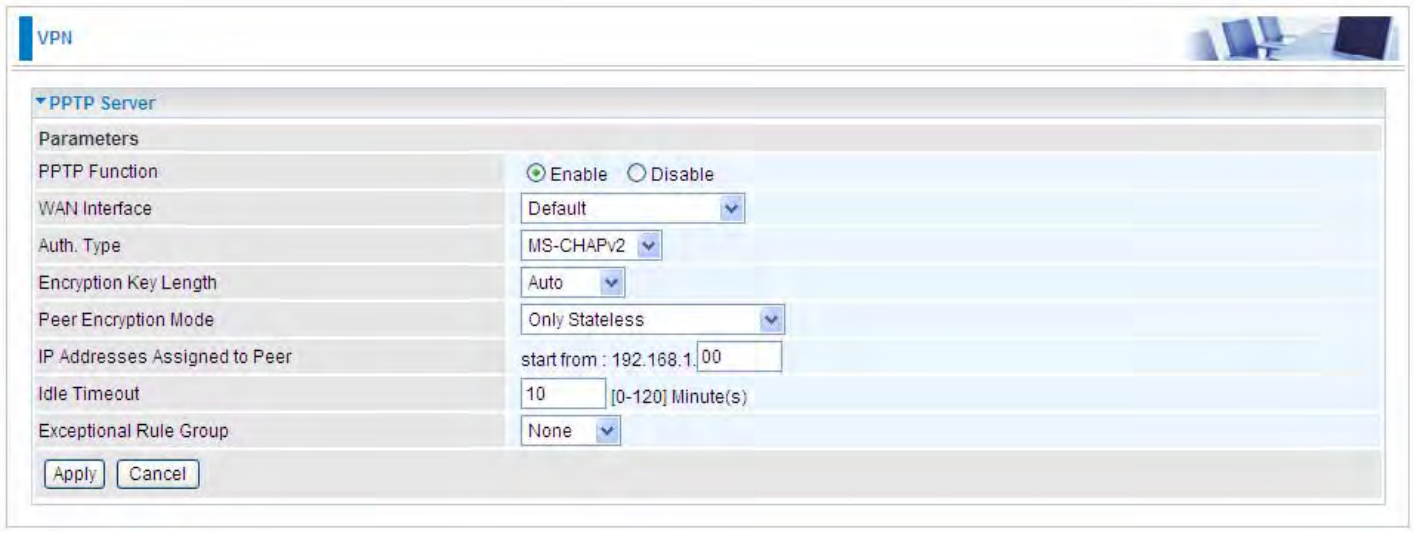

test Status
General
Details
Property
Value
Device Name
WAN Miniport (PPTP)
Device Type
vpn
Authentication
MS CHAP V2
Encryption
MPPE 128
Compression
(none)
PPP multilink framing
Off
Client IPv4 address
192.168.1.100
Server IPv4 address
192.168.1.254
NAP State
Not NAP-capable
Origin address
(unknown)
Destination address
172.16.1.208
Close

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

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



Server side: Head Office



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

Then the PPTP Account.

Client Side: Branch Office

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

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

L2TP

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

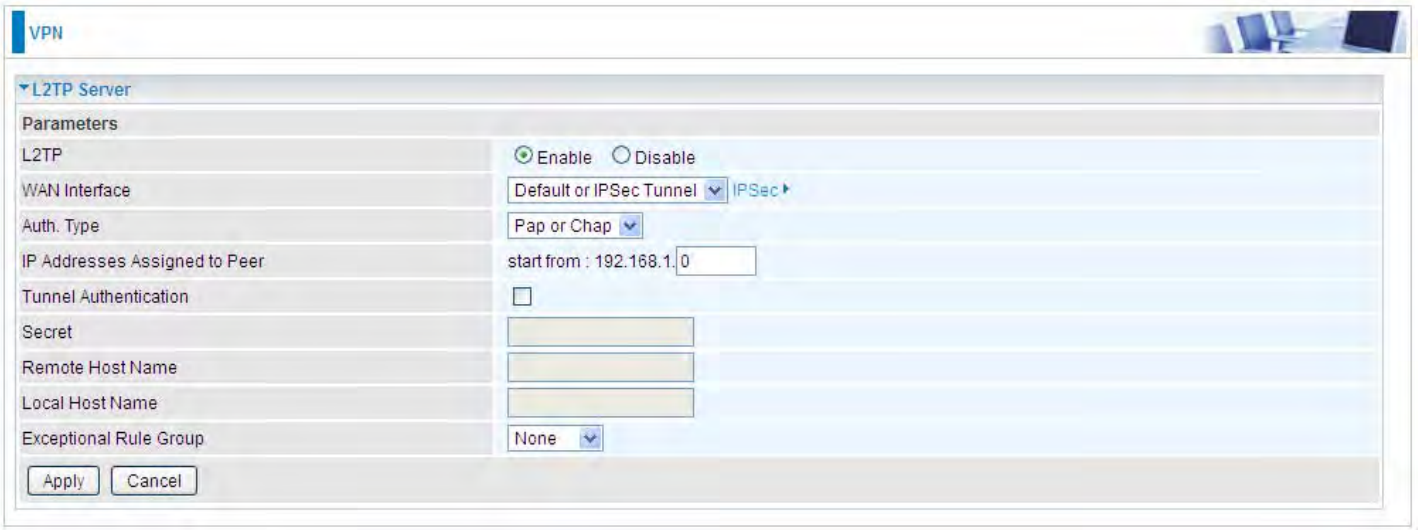
L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

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

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

L2TP Server

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



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

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

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

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

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

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

and set the same in the client side.

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

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

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

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

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

L2TP Client

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

Name: user-defined name for identification.

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

ⓘ **Enable**

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

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

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

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

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

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

Peer Netmask: Please input the Netmask for Server.

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

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

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

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

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

ⓘ Disable

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

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

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

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

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

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

Peer Netmask: Please input the Netmask for server.

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

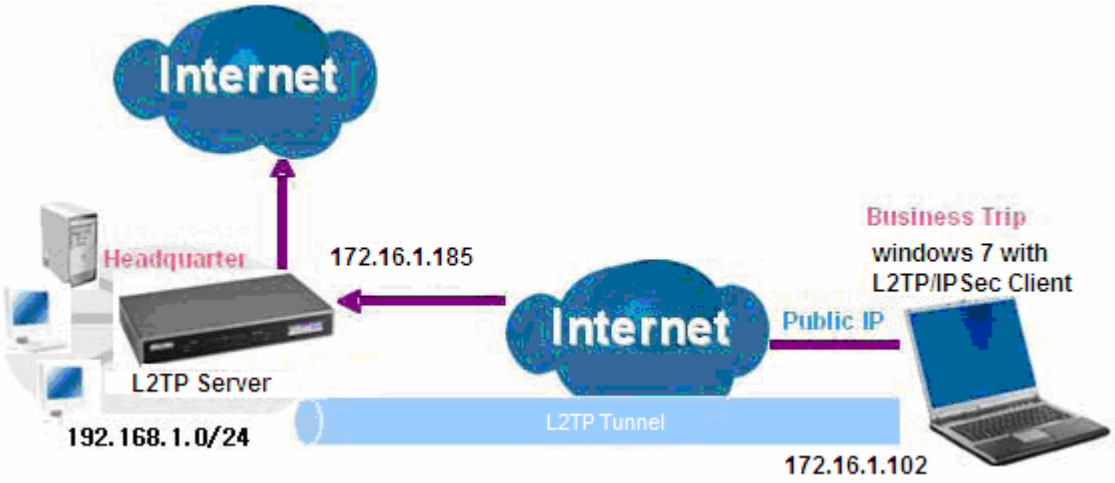
Secret: Enter the set secret password in the server side.

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

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

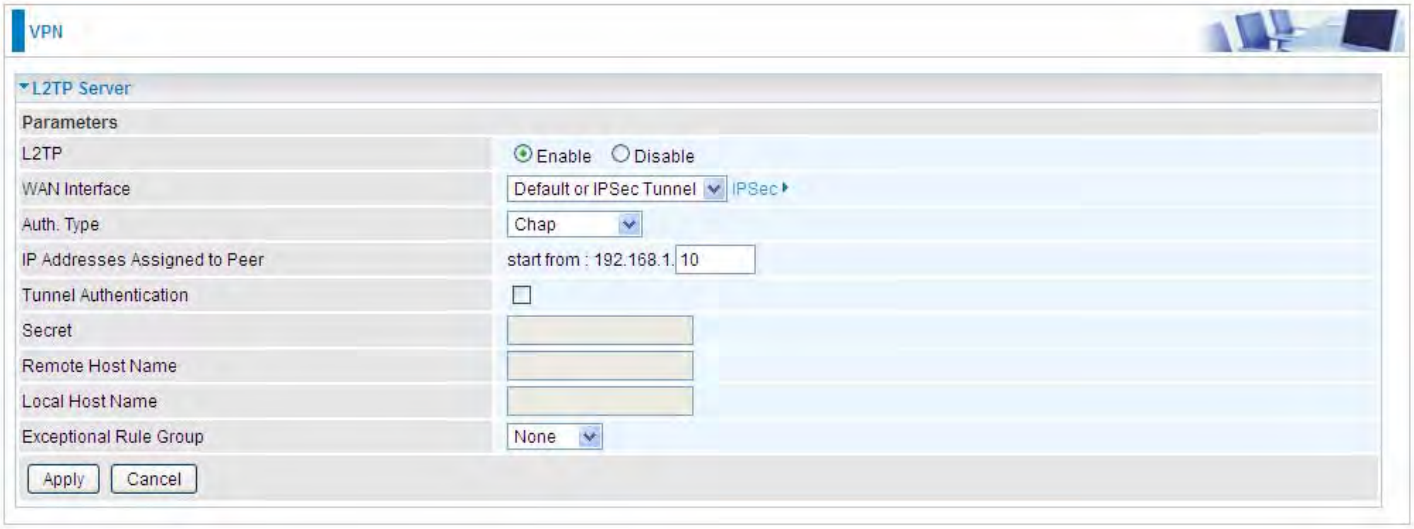
Click **Add** button to save your changes.

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

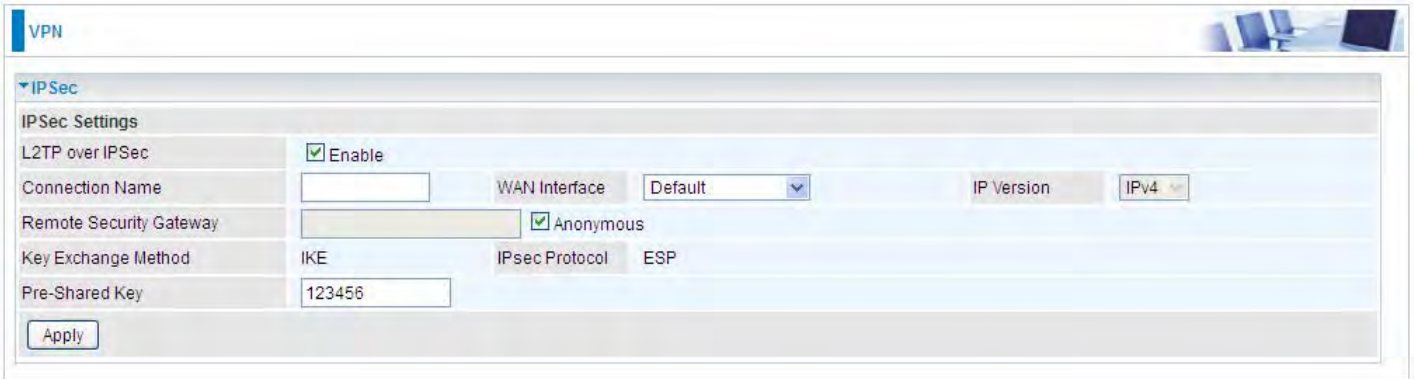


Server Side:

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



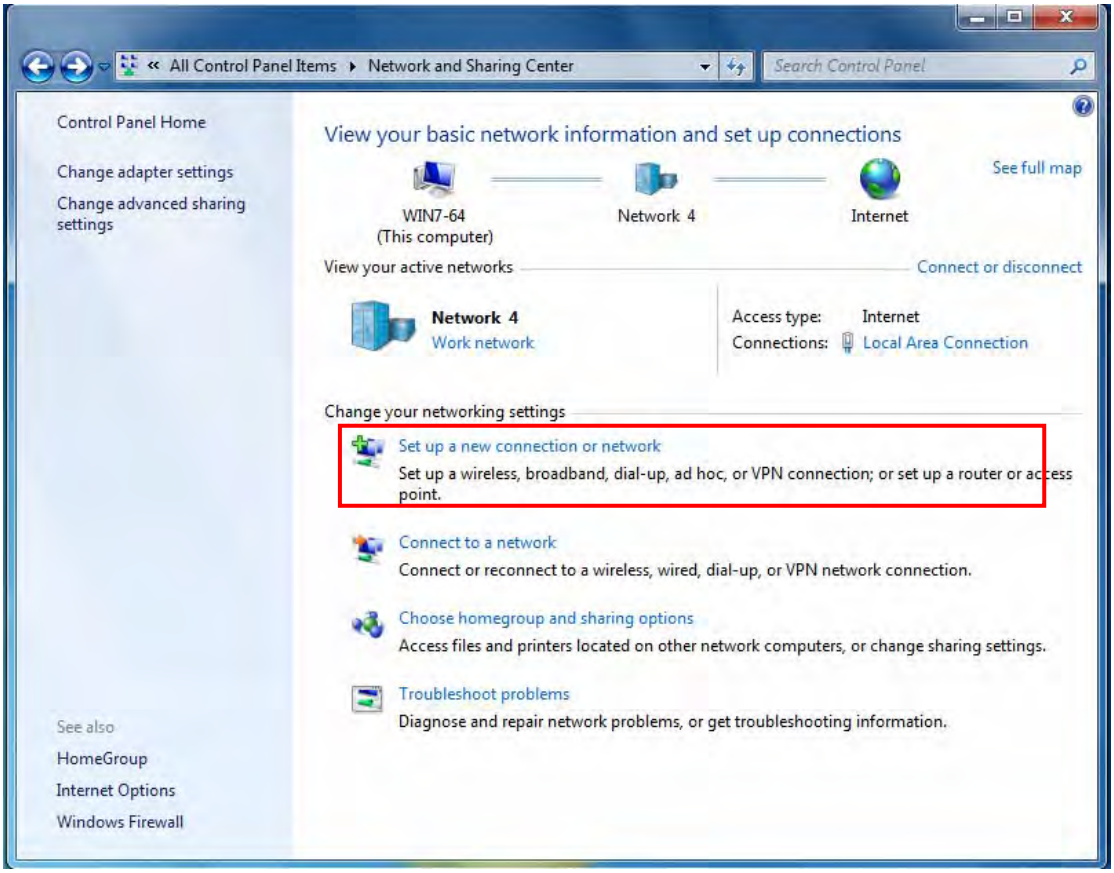
The IPSec for L2TP rule



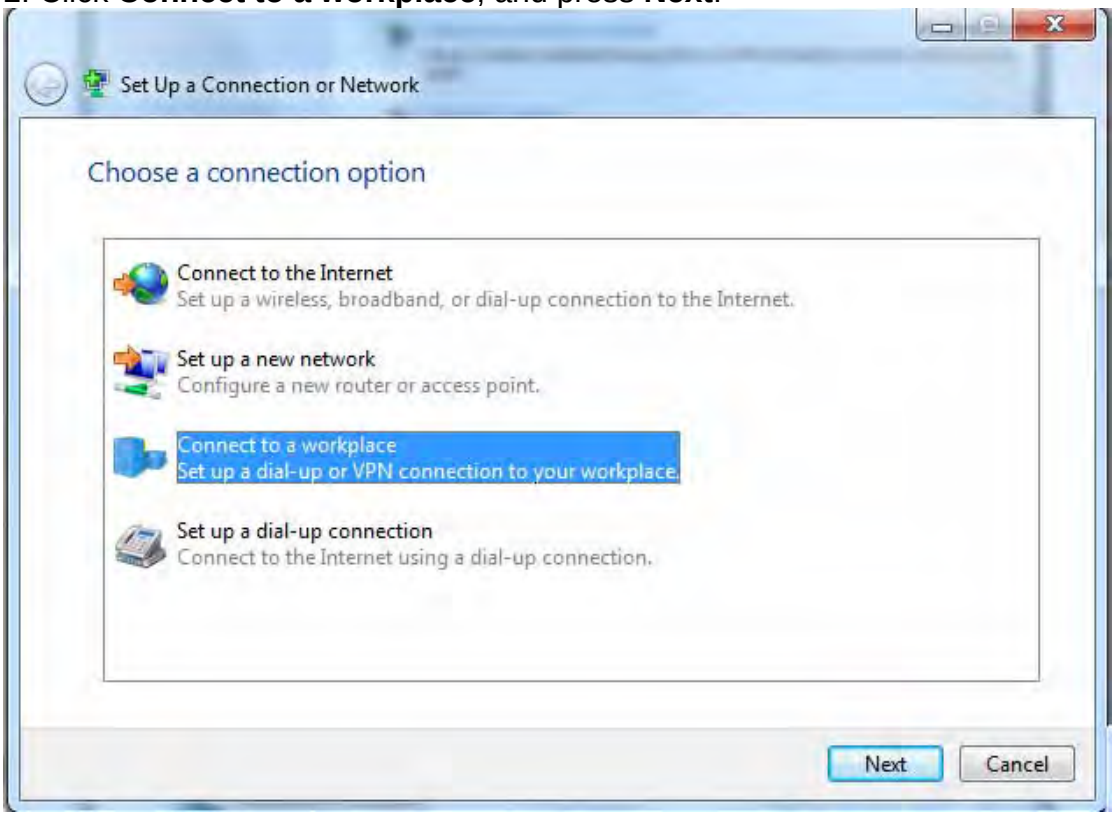
2. Create a L2TP Account “test1”.

Client Side:

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

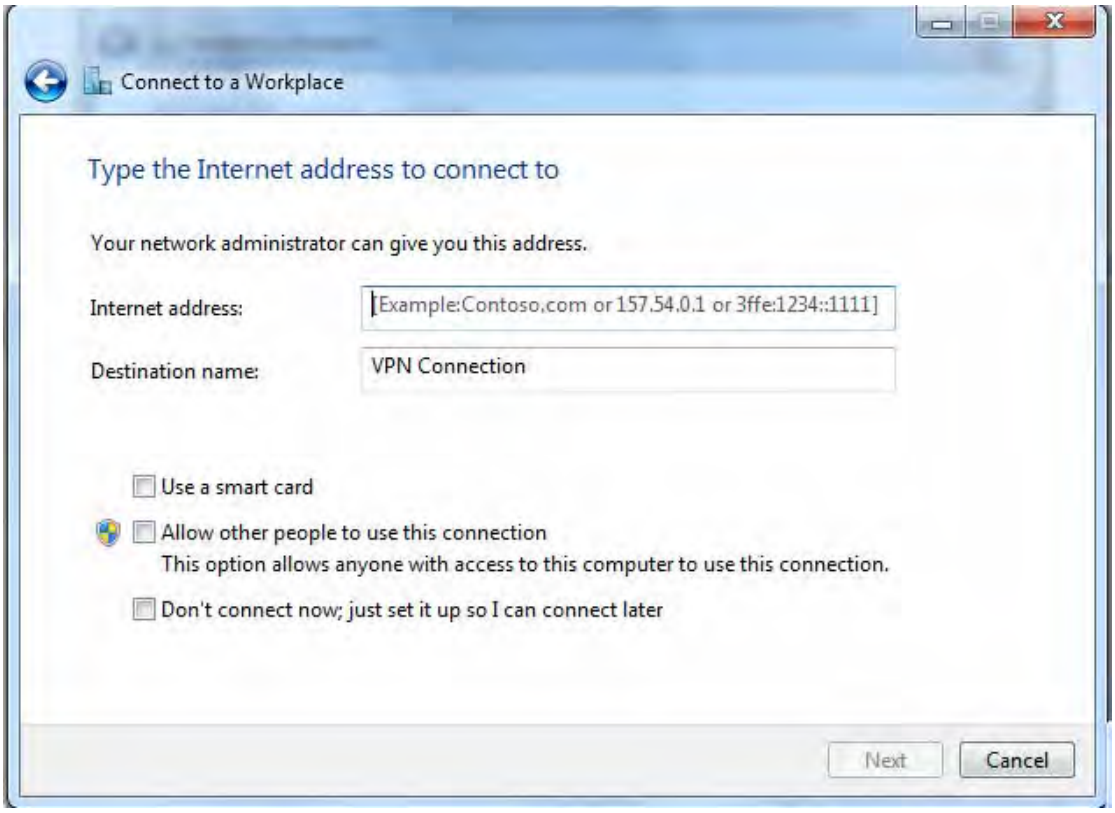


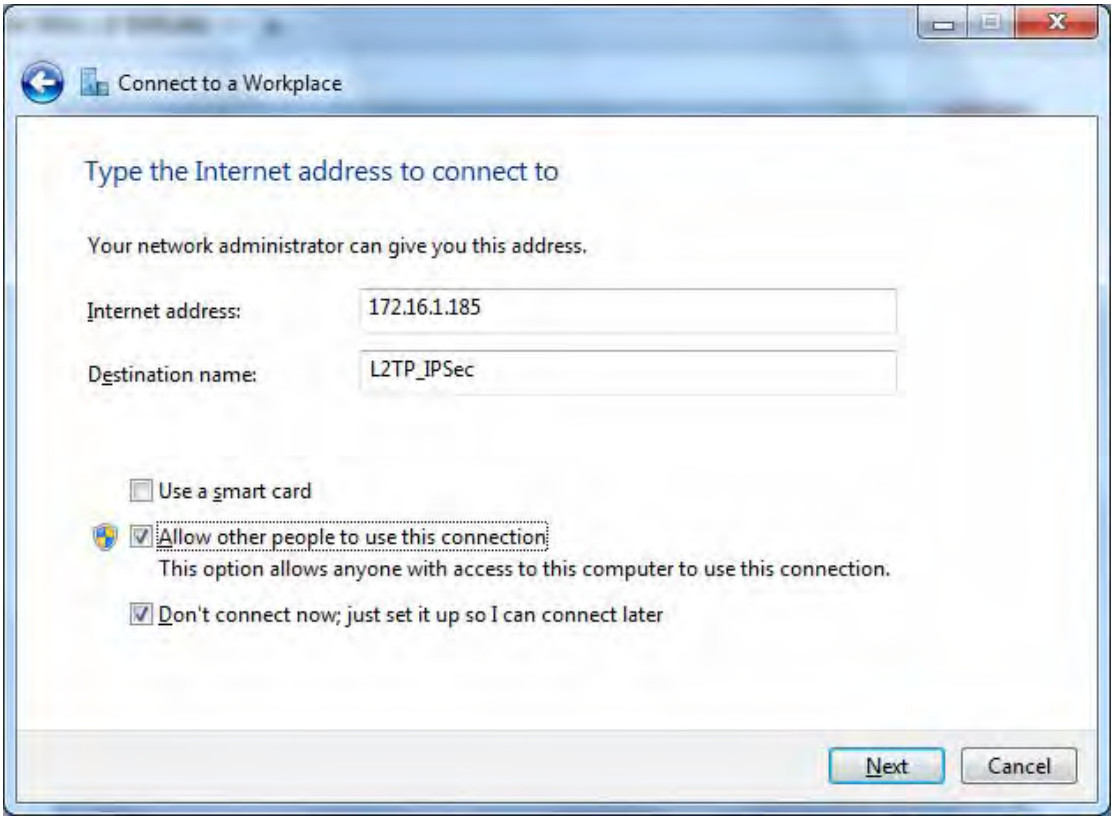
2. Click **Connect to a workplace**, and press **Next**.



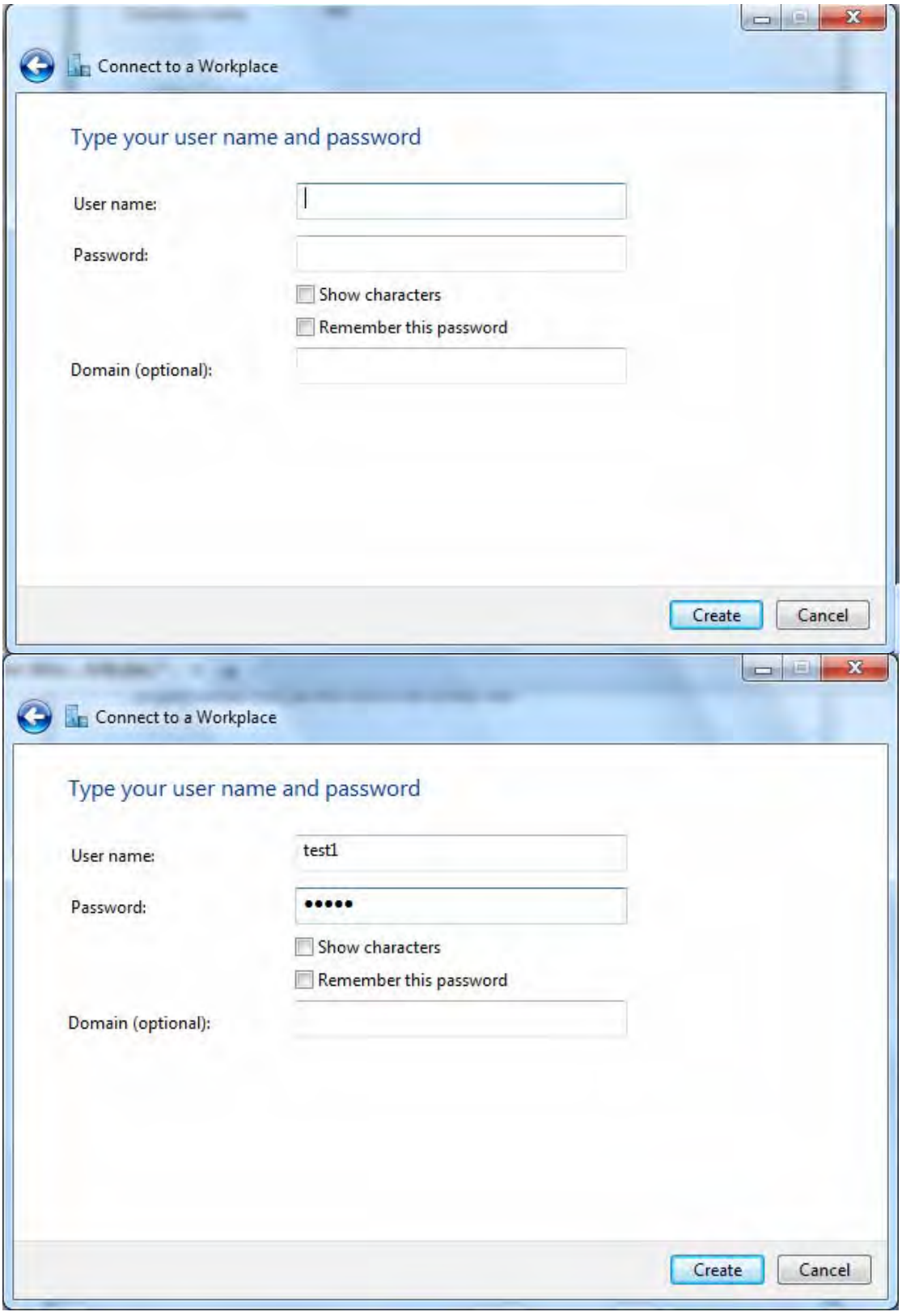
3. Select **Use my Internet connection (VPN)** and press **Next**.

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

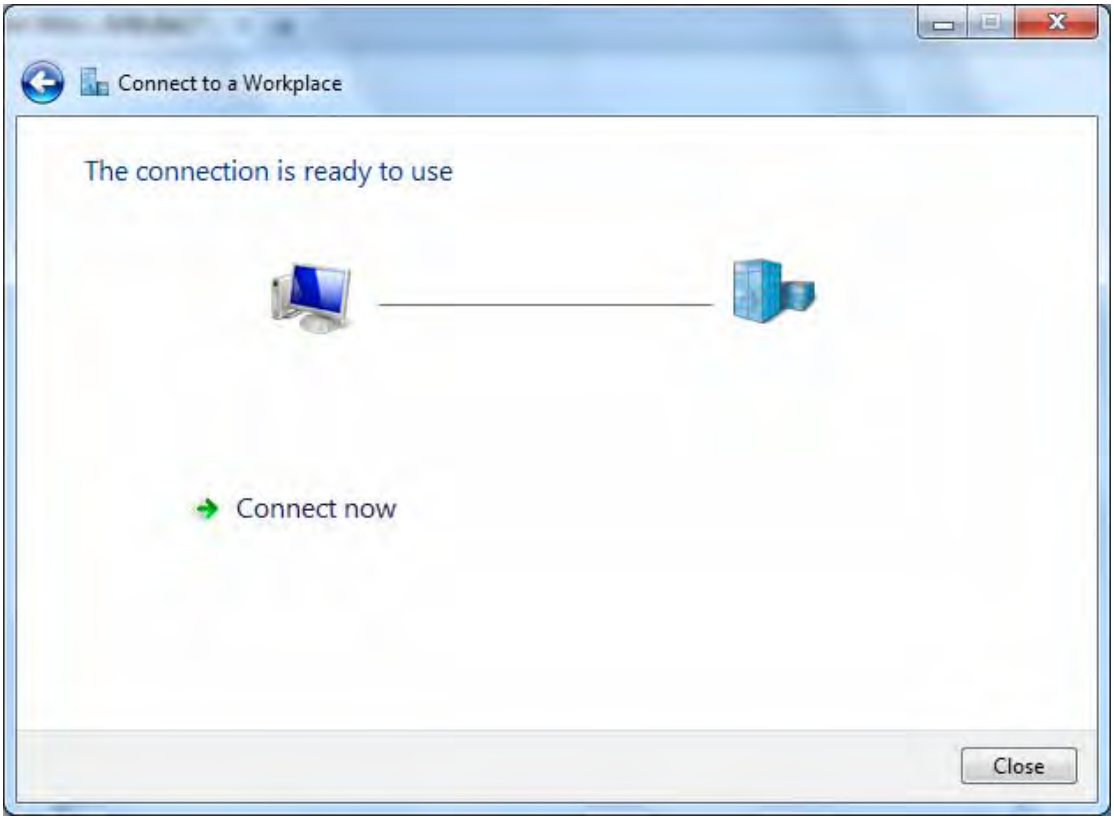




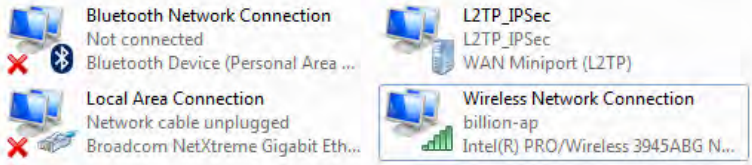
5. Input the account (**user name** and **password**) and press **Create**.



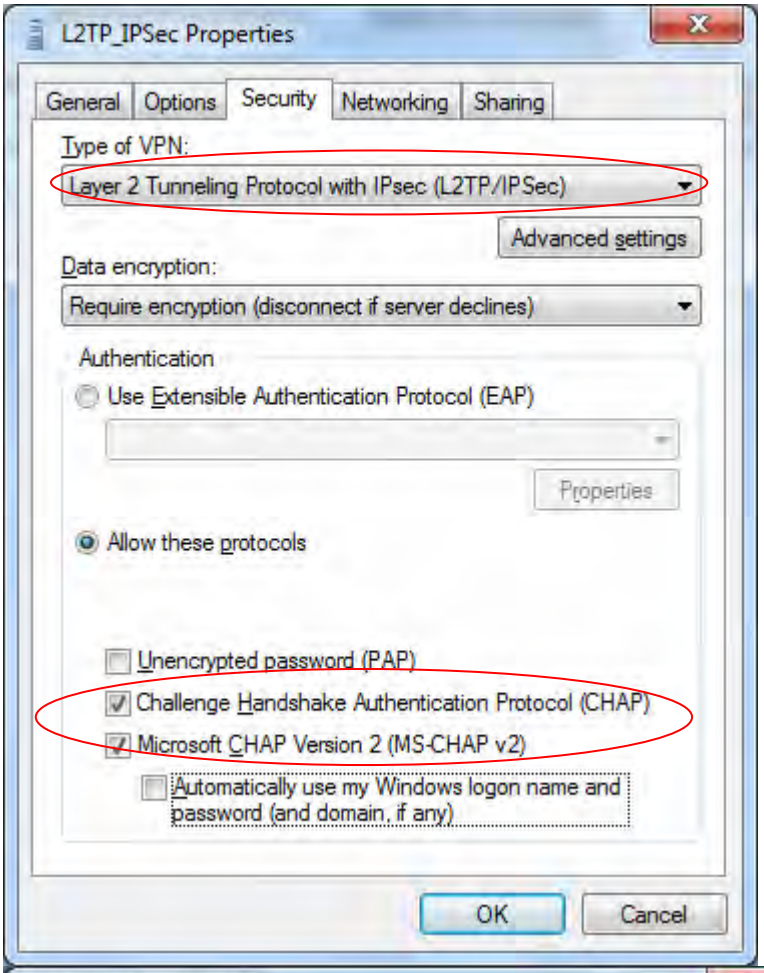
6. Connection created. Press **Close**.

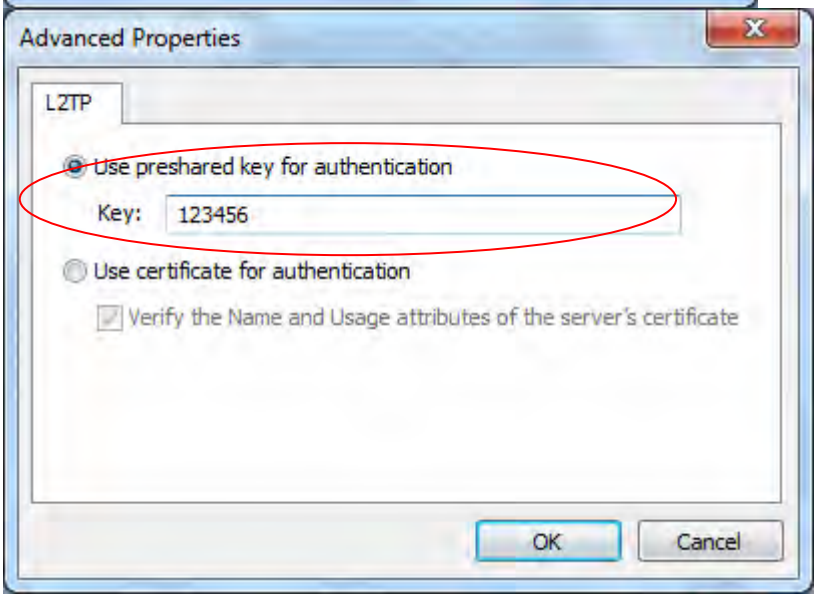


7. Go to **Network Connections** shown below to check the detail of the connection. Right click "L2TP_IPSec" icon, and select "**Properties**" to change the security parameters.

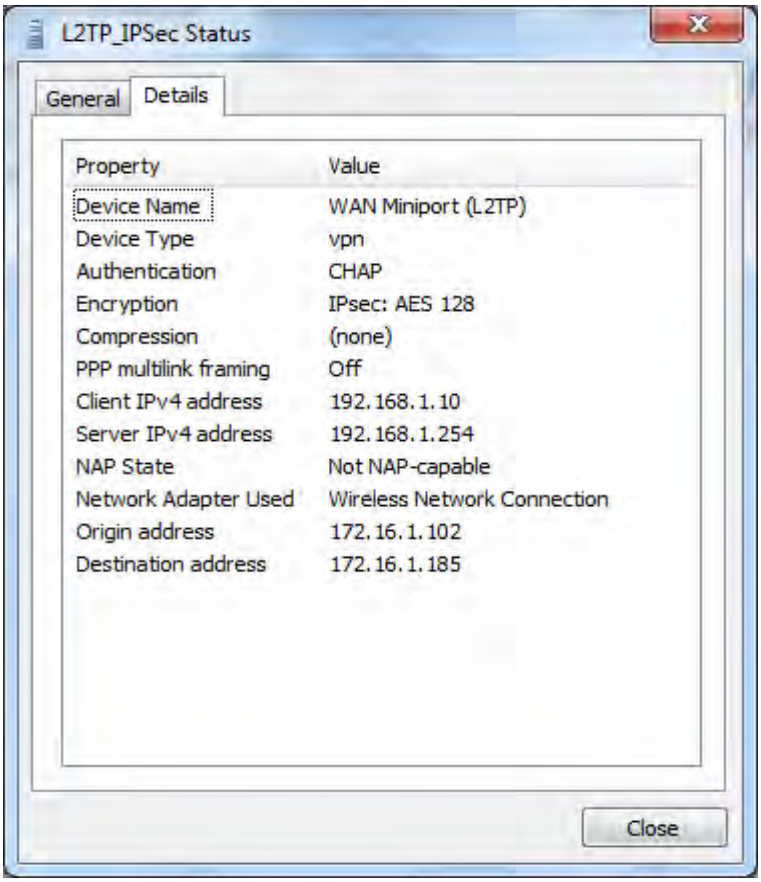


8. Chang the type of VPN to “**Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)**” and Click Advanced Settings to set the pre-shared (set in IPSec) key for authentication.





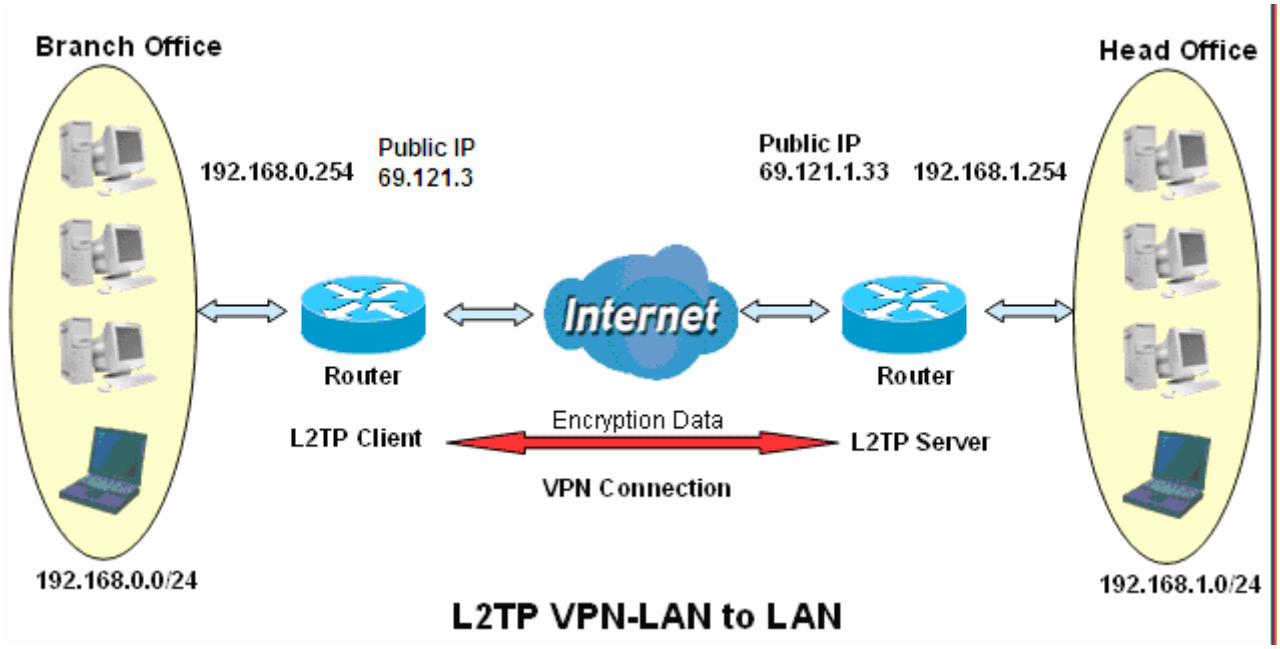
9. Go to **Network connections**, enter username and password to connect L2TP_IPSec and check the connection status.



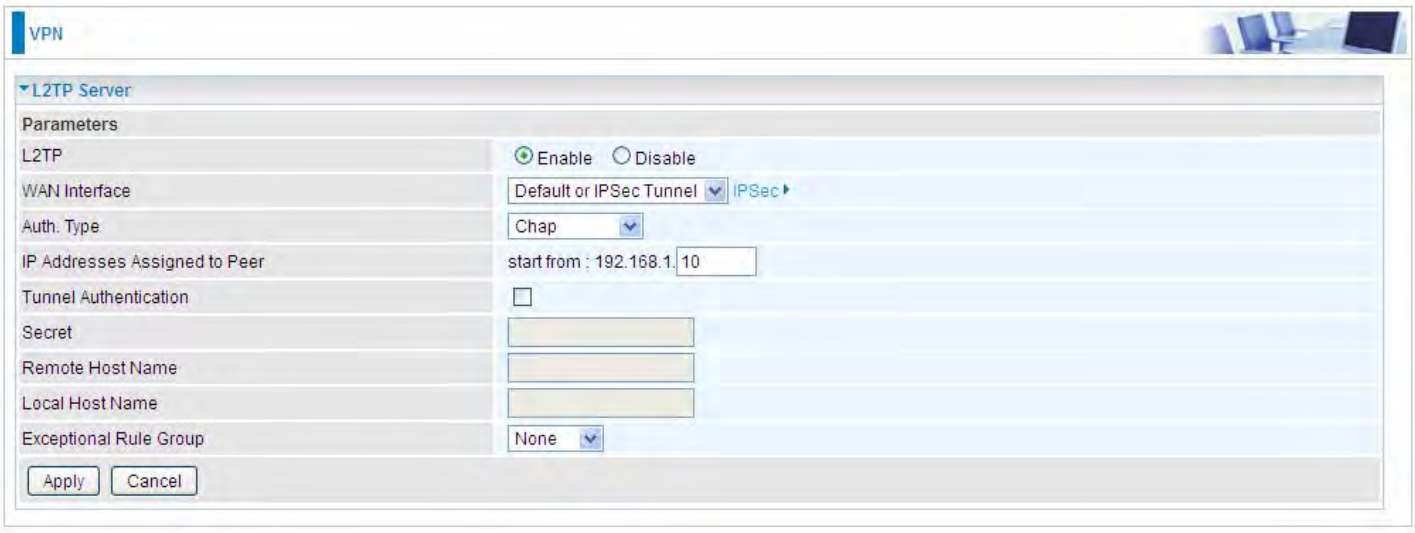
Example: Configuring L2TP LAN-to-LAN VPN Connection

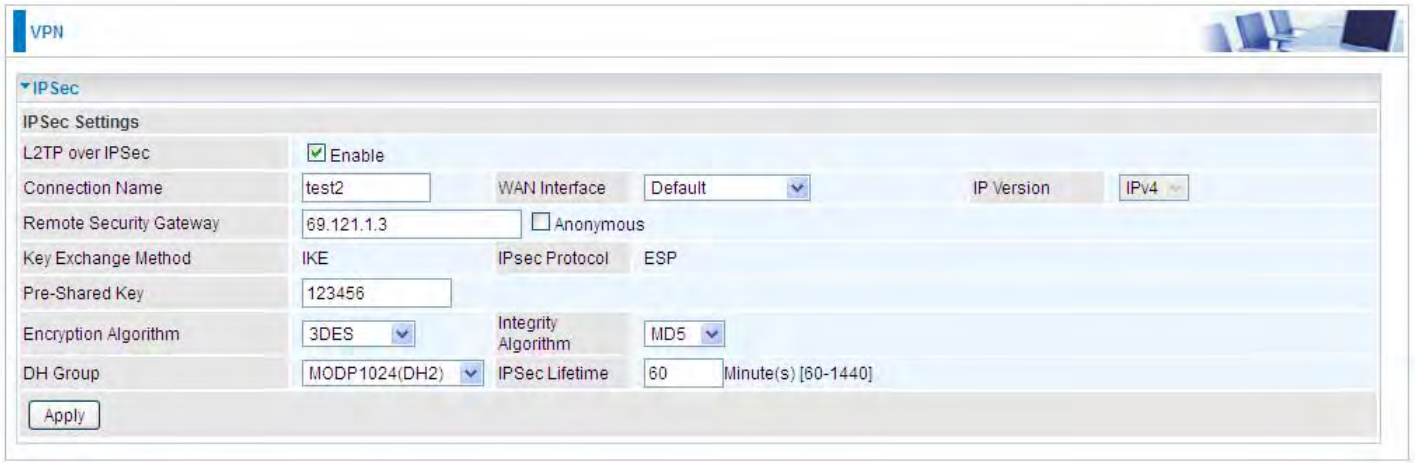
The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

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



Server side: Head Office





Tunnel Mode Connections

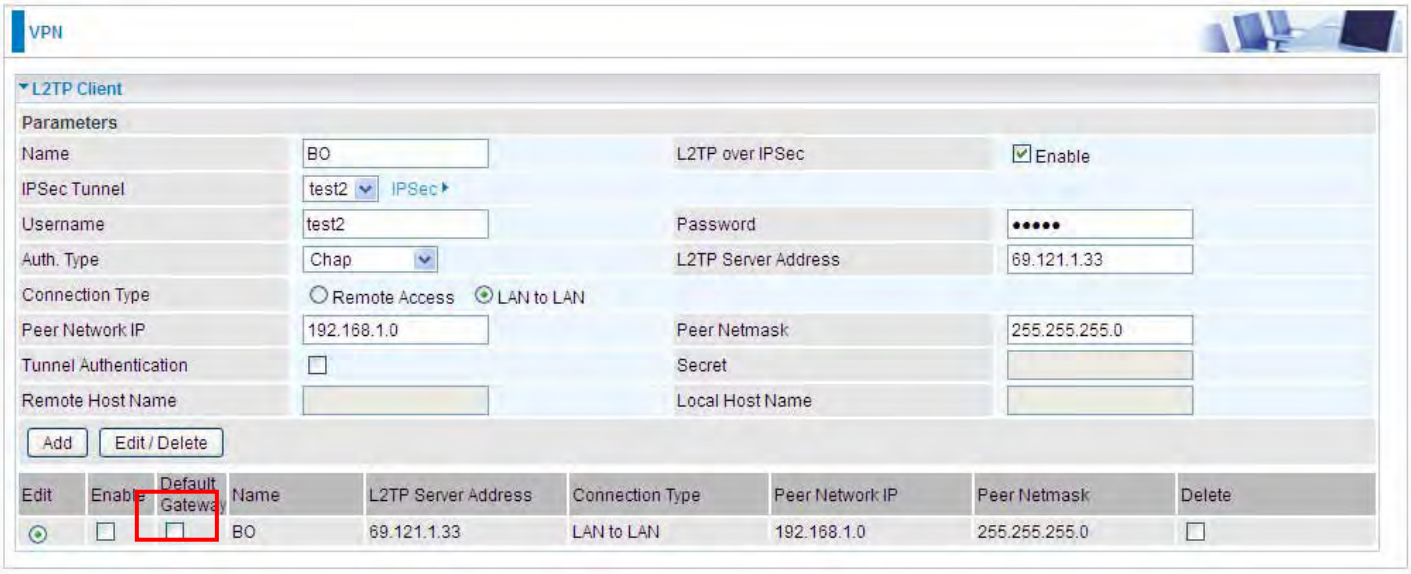
Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
☑	✓	test1			Anonymous	☐	Edit
☐	✓	test2			69.121.1.3	☐	Edit

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

Then account the L2TP Account.

Client Side: Branch Office

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



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

OpenVPN

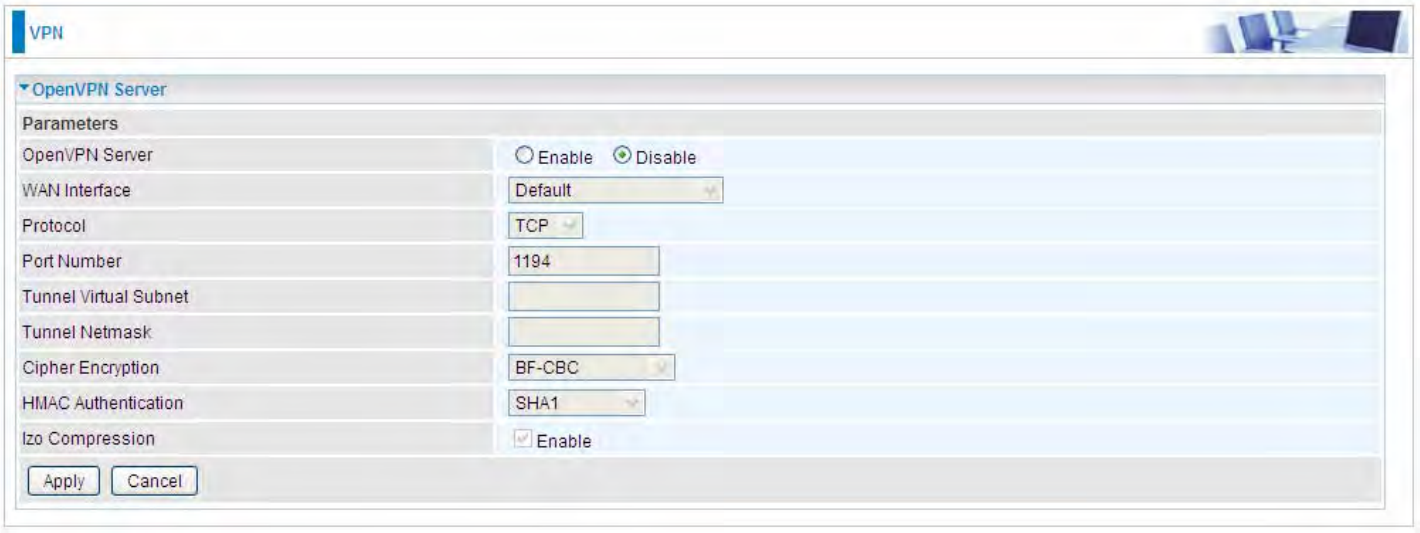
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

OpenVPN is good at portability. OpenVPN has been ported and embedded to several systems.

OpenVPN Server

Users can set the bassic parameters(source/destination address, protocl/port, authentication, encyption, etc) for OpenVPN Server.



OpenVPN Server: Select **Enable** to activate OpenVPN Server.

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

Protocol: OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports. Select the protocol.

Port Number: Port 1194 is the official assigned port number for OpenVPN

Tunnel Virtual Subnet: Set the tunnel virtual subnet IP for OpenVPN server.

Tunnel Network: Set the tunnel virtual subnet mask.

Cipher Encryption: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select the encryption method.

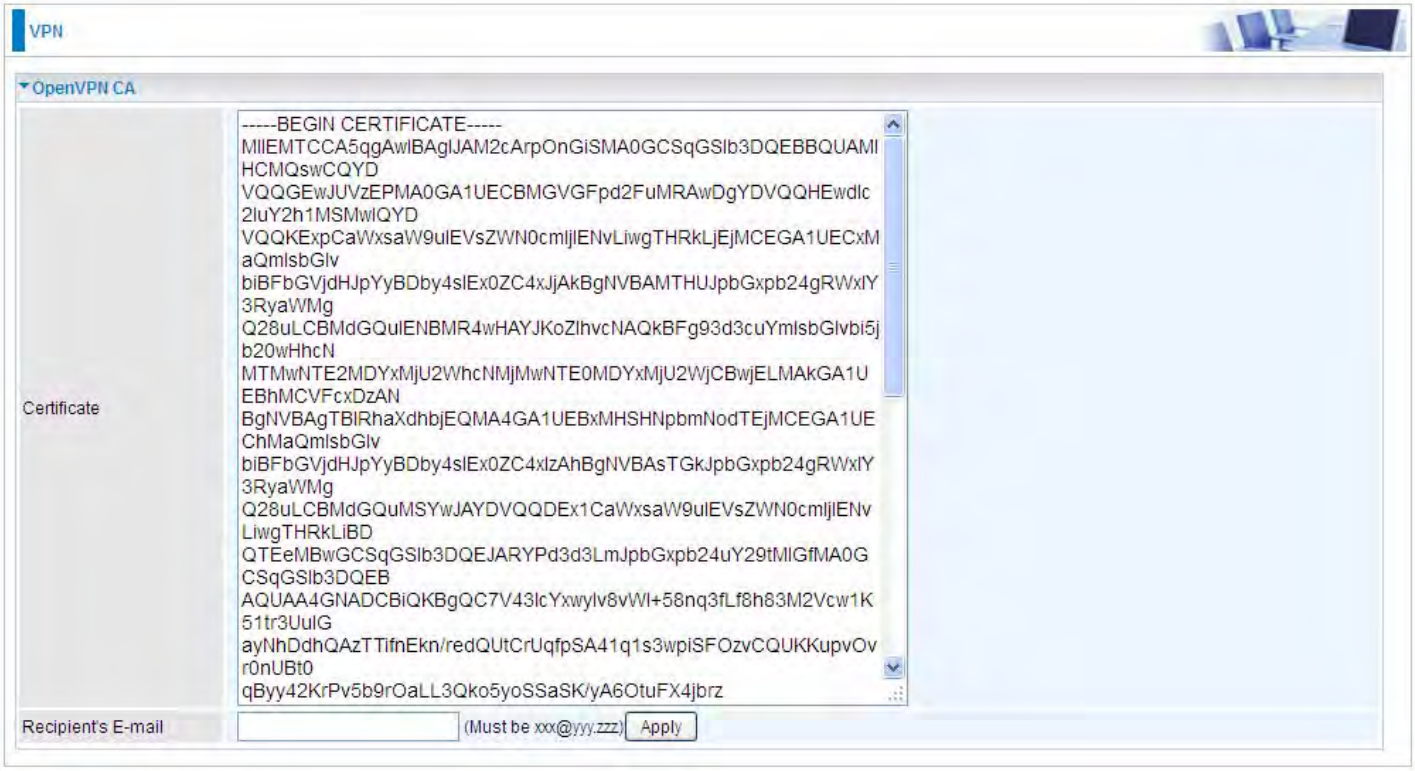
HMAC Authentication: OpenVPN support HMAC authentication, please select authentication item from the list.

lzo Compression: Enable to use the LZO compression library to compress the data stream.

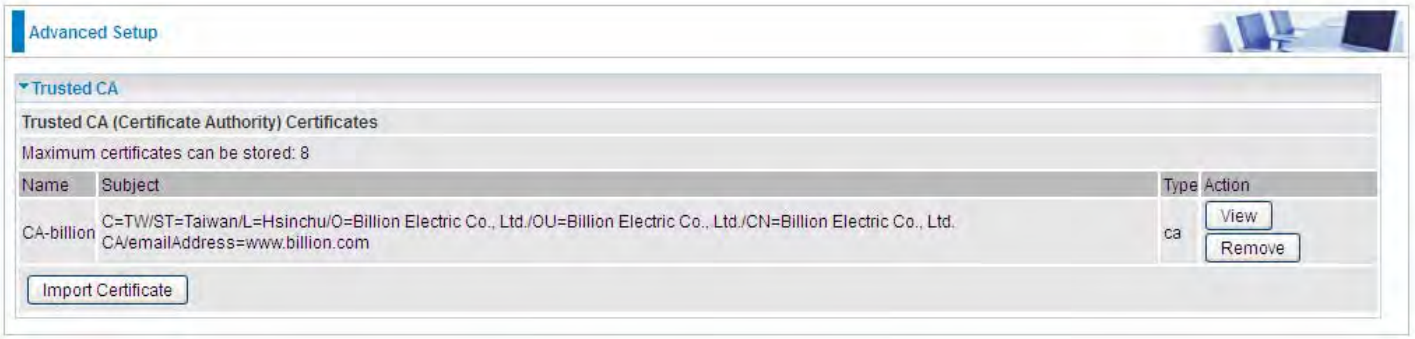
Click **Apply** to submit your OpenVPN Server basic settings.

OpenVPN CA

OpenVPN offers pre-shared keys, certificate-based, and username/password-based authentication, with certificate-based being the most robust. Generally, the part offers the billion factory-defined authentication certificate.



Recipient's Email: Set the recipient's email address to send the trusted CA to the OpenVPN client. OpenVPN server and client need matched certificate to establish trusted VPN tunnel, on client side, please import this certificate in Trusted CA.



(client side CA)

OpenVPN Client

OpenVPN client can help you dial-in the OpenVPN server to establish a trusted OpenVPN tunnel over Internet.

Name: user-defined name for identification.

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

Username: Enter the username provided by your OpenVPN Server.

Password: Enter the password provided by your OpenVPN Server.

OpenVPN Server Address: Enter the WAN IP address of the OpenVPN server.

Protocol: The protocol, same as set in server side.

Port Number: 1194.

Cipher Encryption: Be consistent with what set on server side.

HMAC Authentication: Be consistent with what set on server side.

lzo Compression: Enable to use the LZO compression library to compress the data stream

Certificate Authority: Select your trusted CA from your server side to establish the trusted VPN tunnel with server.

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

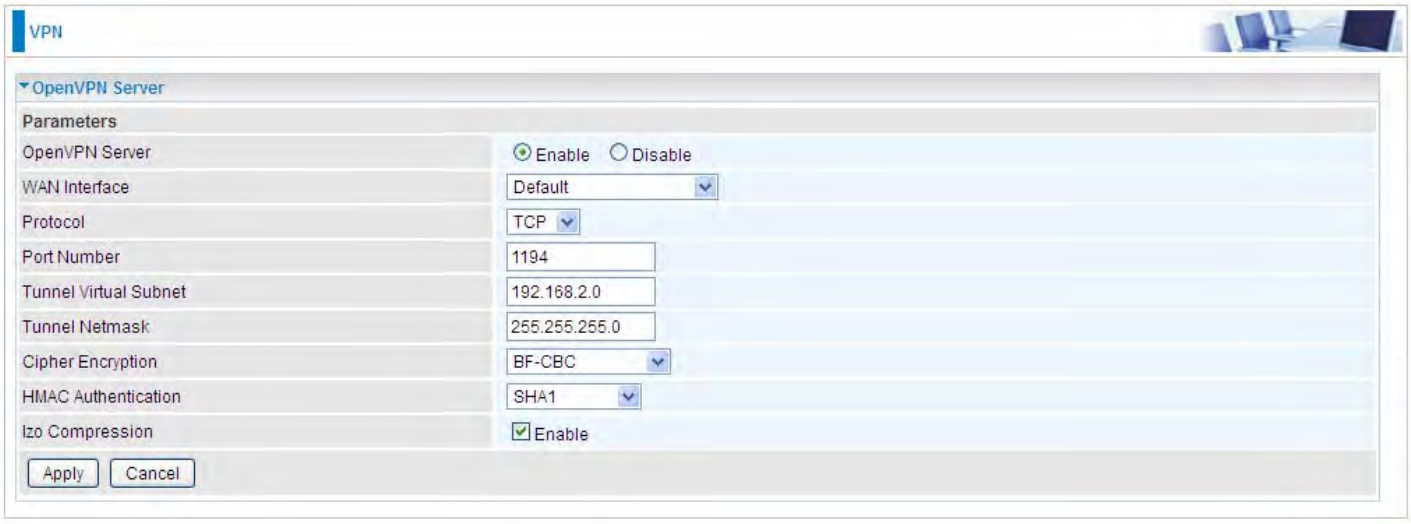
How to establish OpenVPN tunnel

1. Remote Access OpenVPN

(If the client wants to remotely access the OpenVPN Server, on client side, users had better install an OpenVPN client application/installer and connect to server accordingly. Here only give the configuration on server side.)

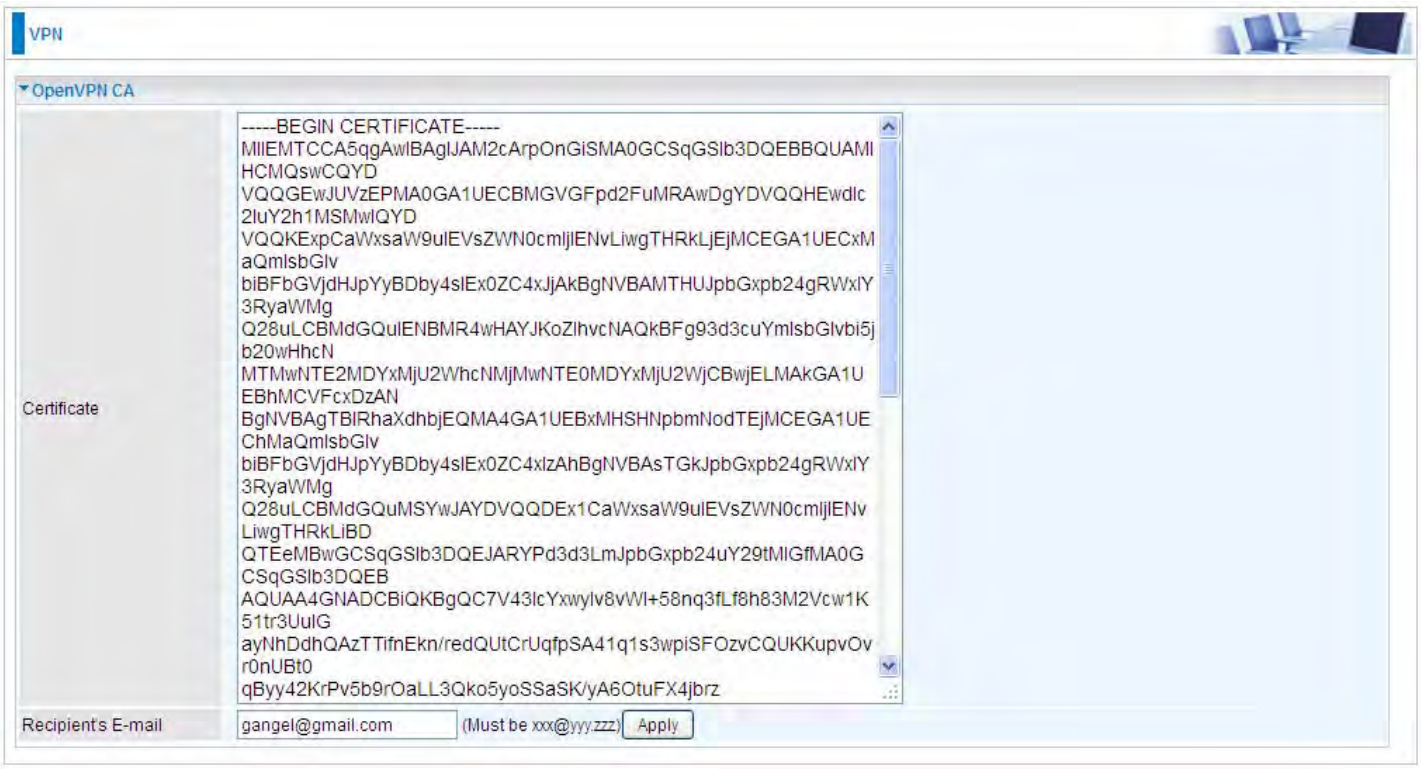
Server side on router

1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.



2. Create an account for the OpenVPN tunnel for client to connect in.

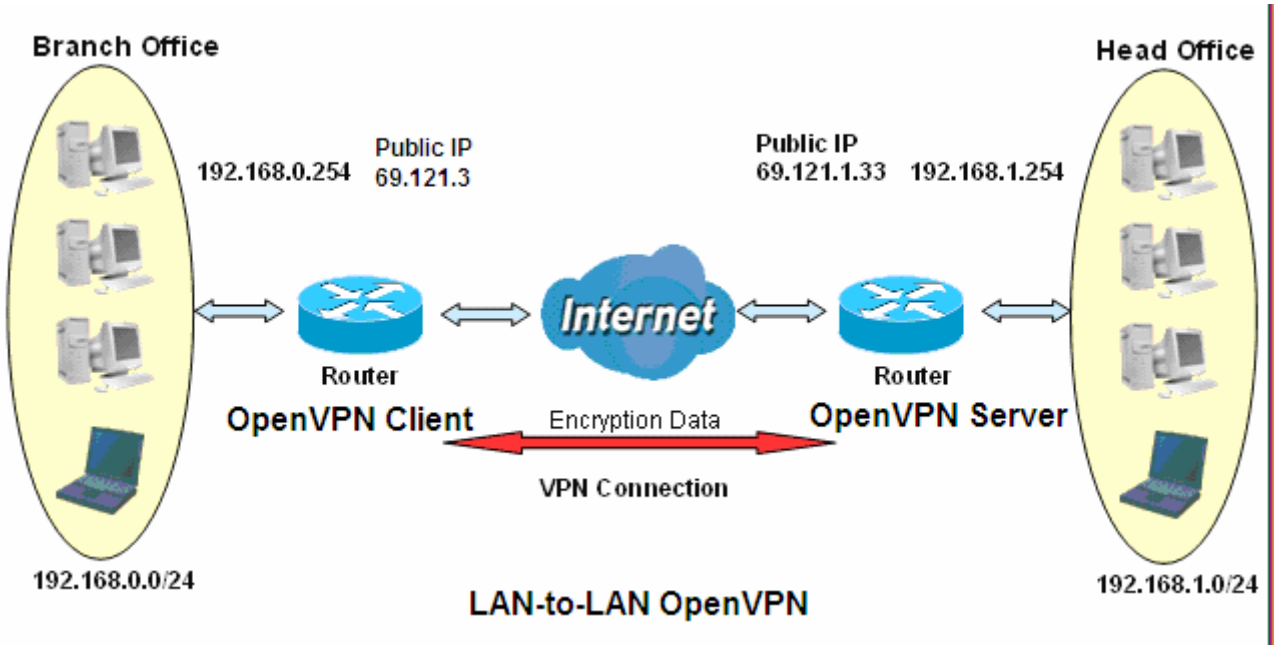
3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.



2. LAN-to-LAN OpenVPN

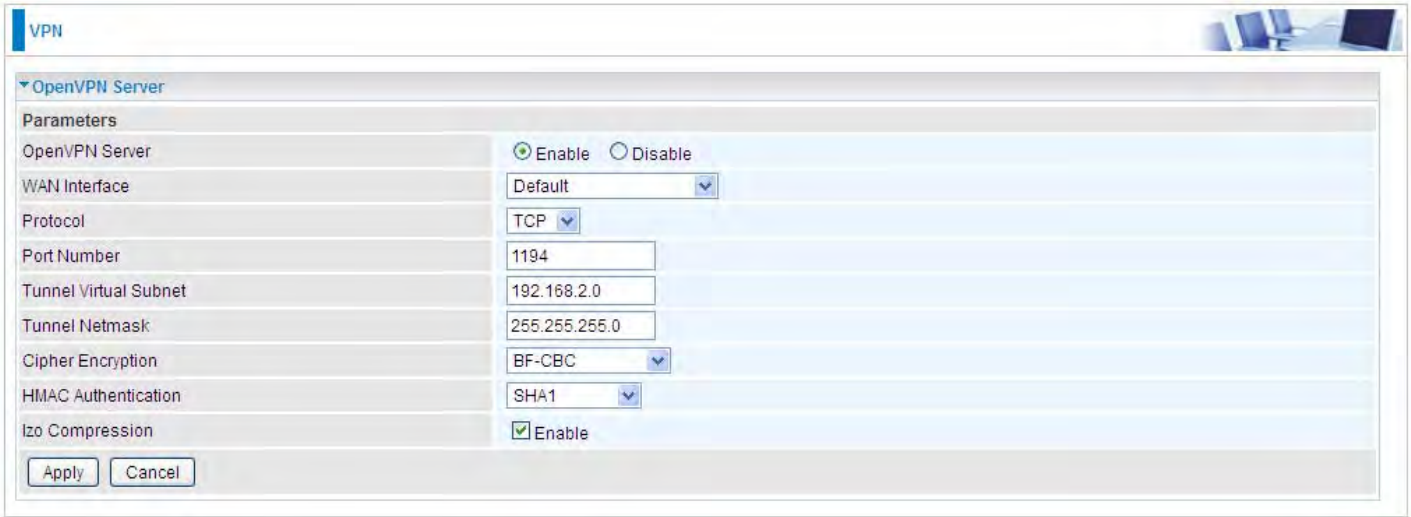
The branch office establishes a OpenVPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly. Configured in this way, head office and branch office can access each other.

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

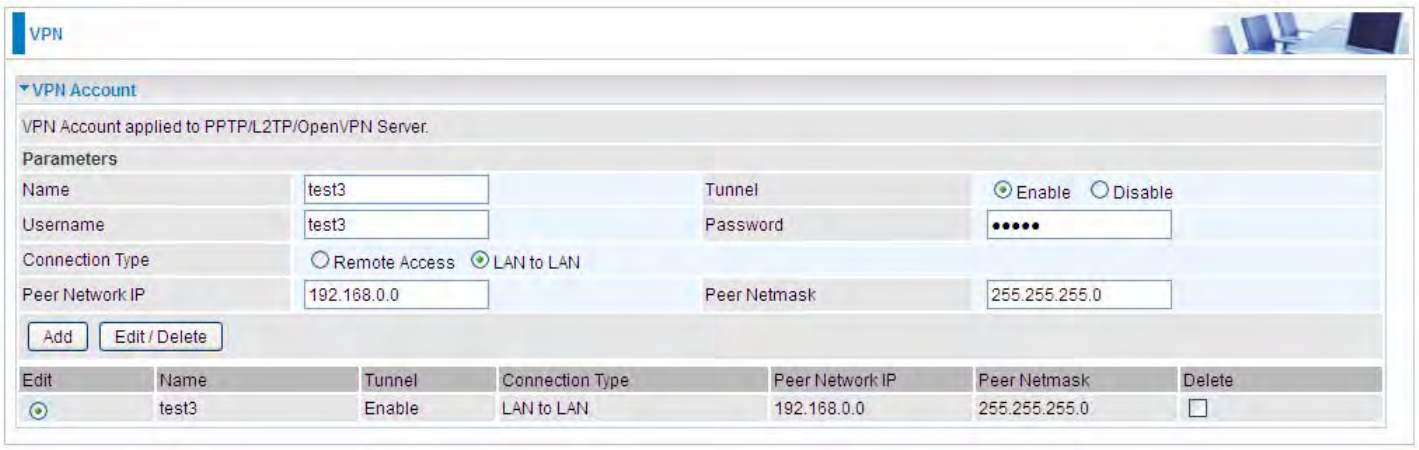


Server side: Head Office

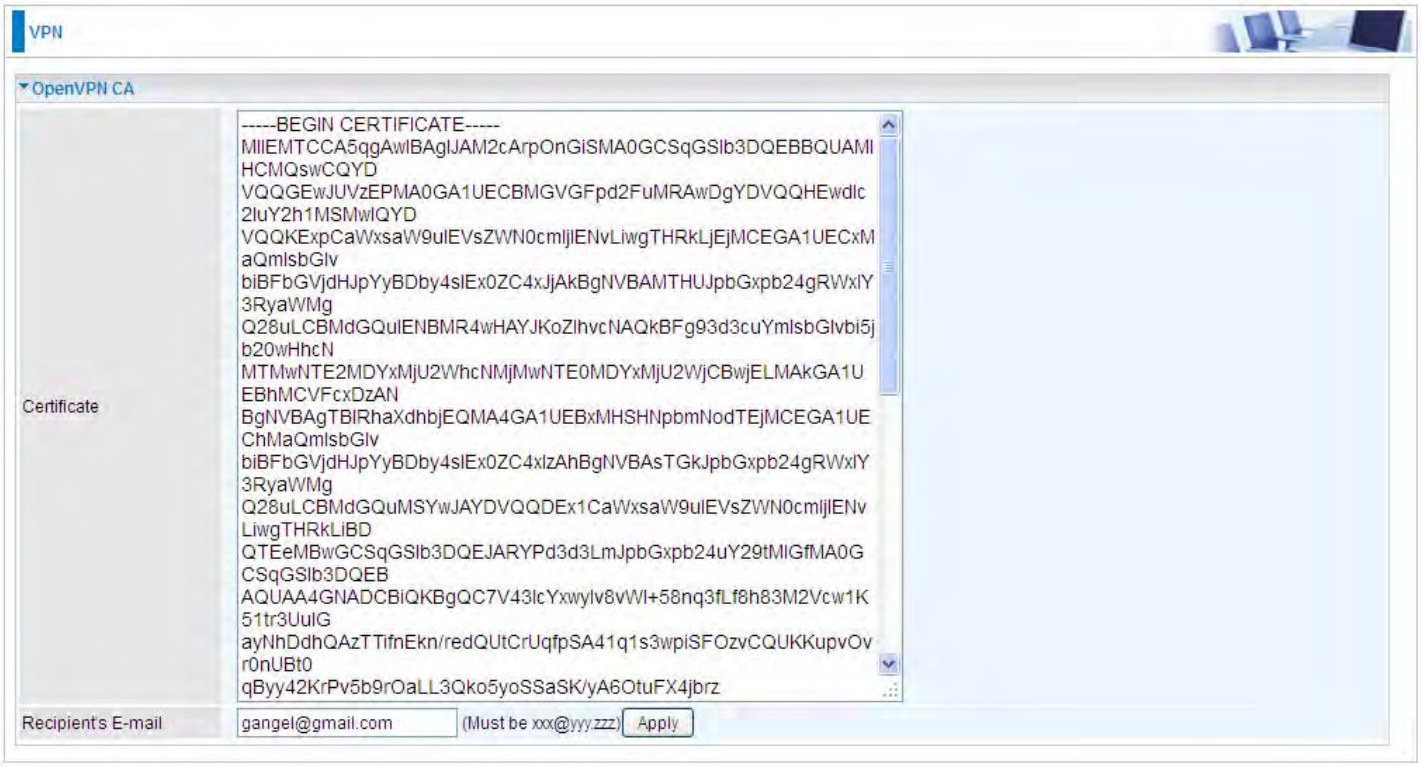
1. Set up parameters (WAN interface, port, tunnel virtual subnet IP/mask, encryption, authentication, etc) on OpenVPN server side.



2. Create an account for client to connect in

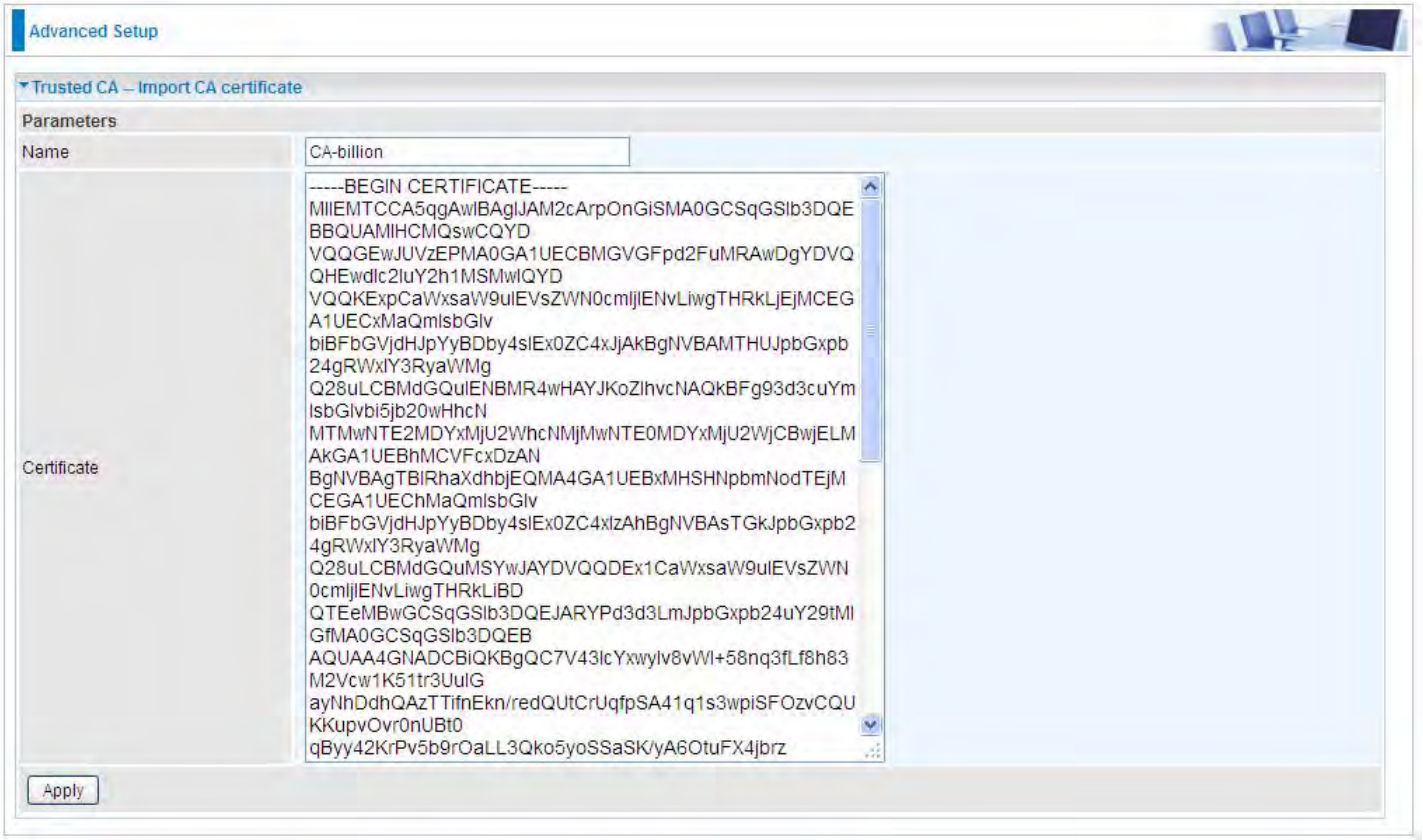


3. Set the OpenVPN client's E-mail address to receive trusted CA from server to establish a trusted OpenVPN tunnel.

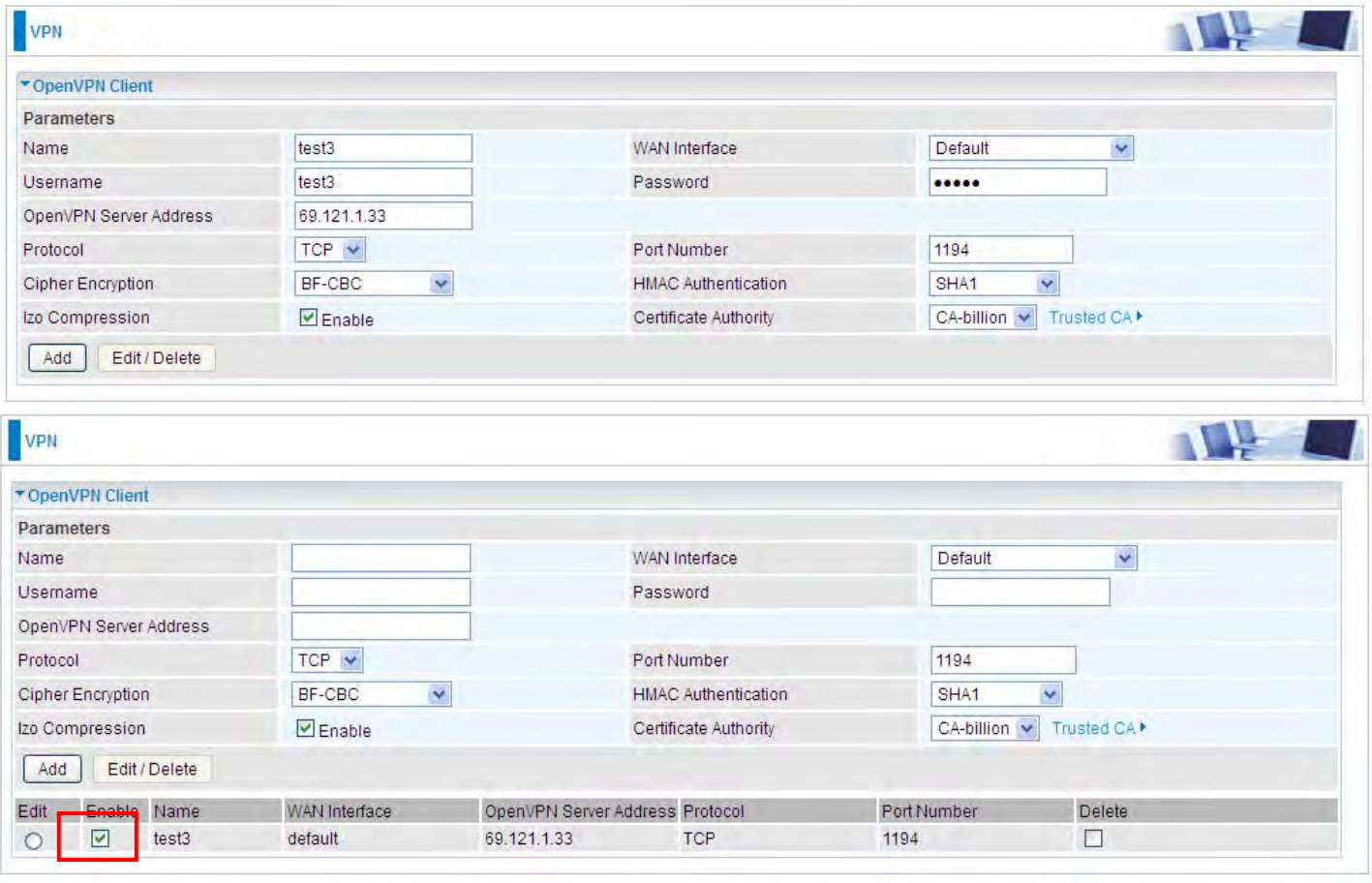


Client Side: Branch Office

1. Import your trusted certificate from server side, which is used to authenticate between client and server for establishing trusted OpenVPN tunnel.



2. On the OpenVPN client side, fill in the parameters the same as set for OpenVPN server.

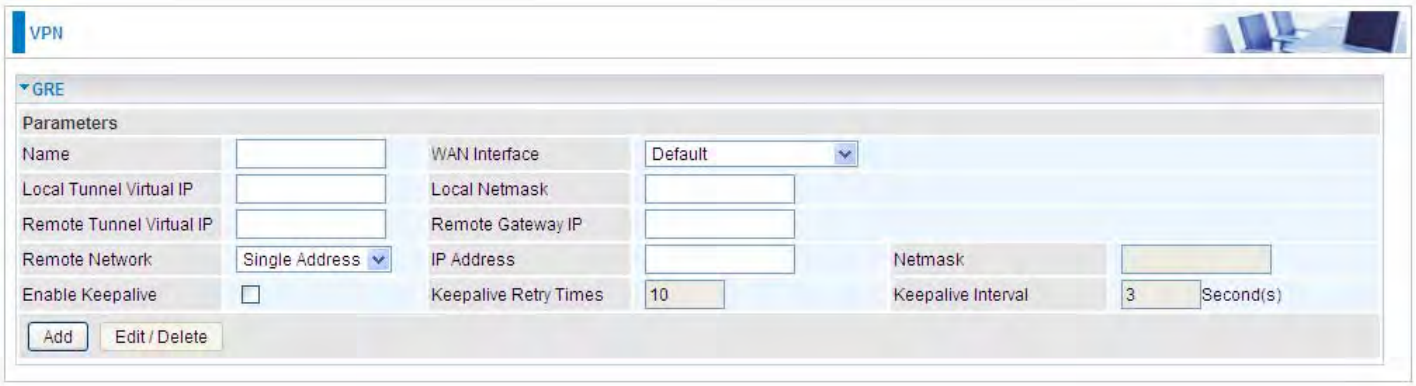


Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

GRE

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

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



Name: User-defined identification.

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

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

Local Netmask: Input the netmask for the local tunnel side.

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

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

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

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

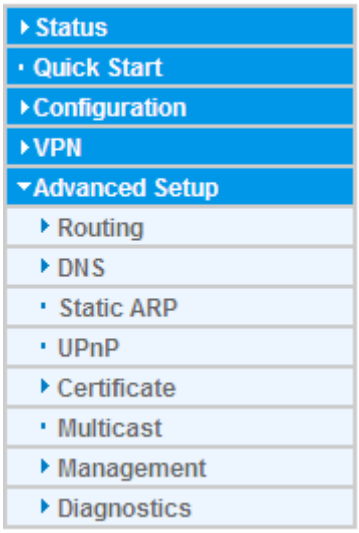
Enable Keepalive: Normally, the tunnel interface is always up. Enable keepalive to determine when the tunnel interface is to be closed. The local router sends keepalive packets to the peer router, if keepalive response is not received from peer router within the allowed time (‘retry time’ multiply ‘interval’,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

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

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

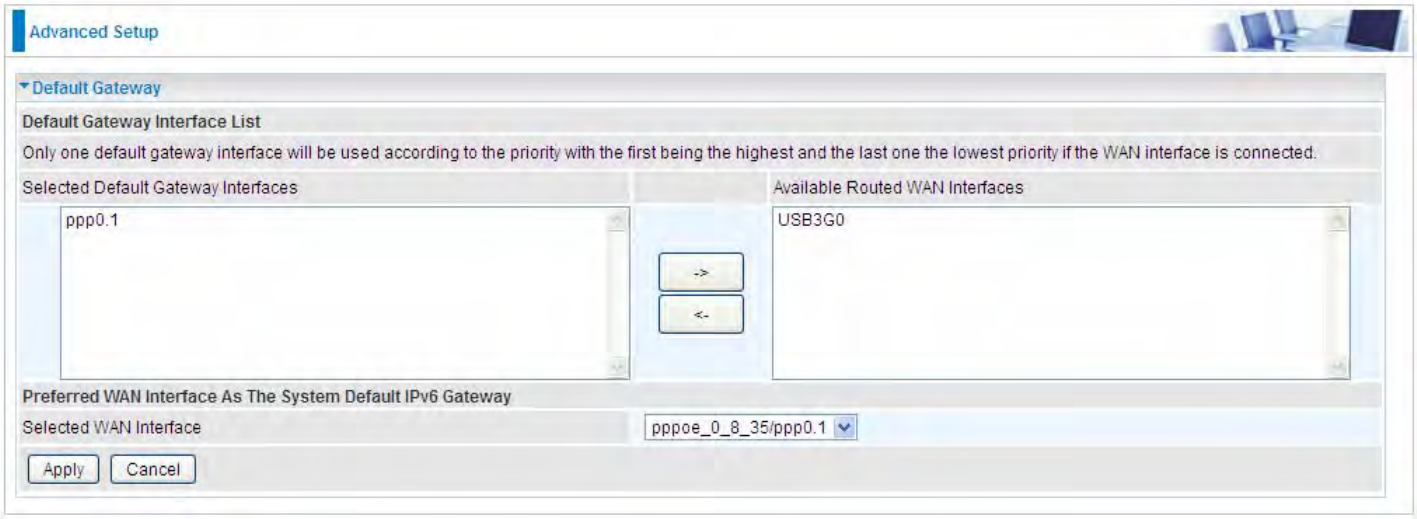
Advanced Setup

There are sub-items within the System section: **Routing**, **DNS**, **Static ARP, UPnP**, **Certificate**, **Multicast**, **Management**, and **Diagnostics.**



Routing

Default Gateway



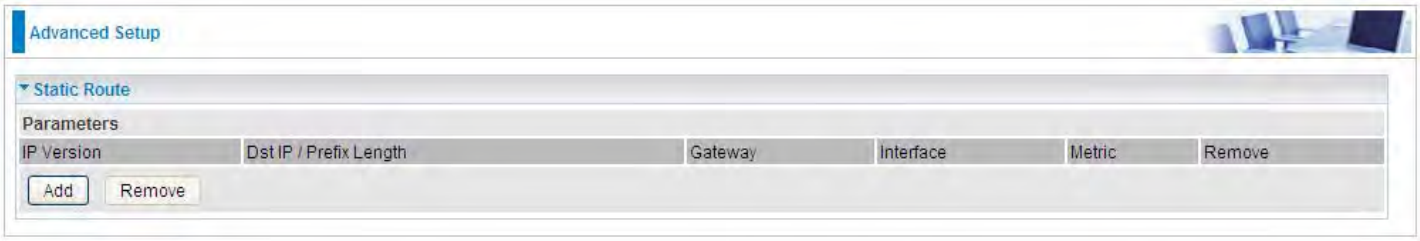
WAN port: Select the port this gateway applies to.

To set ***Default Gateway*** and ***Available Routed WAN Interface***. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via -> or <-. And select a Default IPv6 Gateway from the drop-down menu.

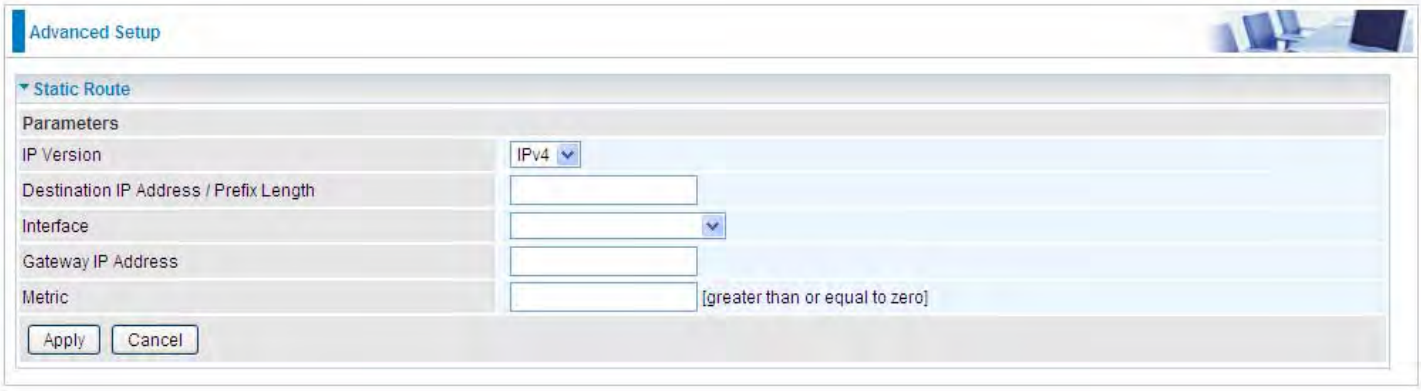
Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

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



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



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

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

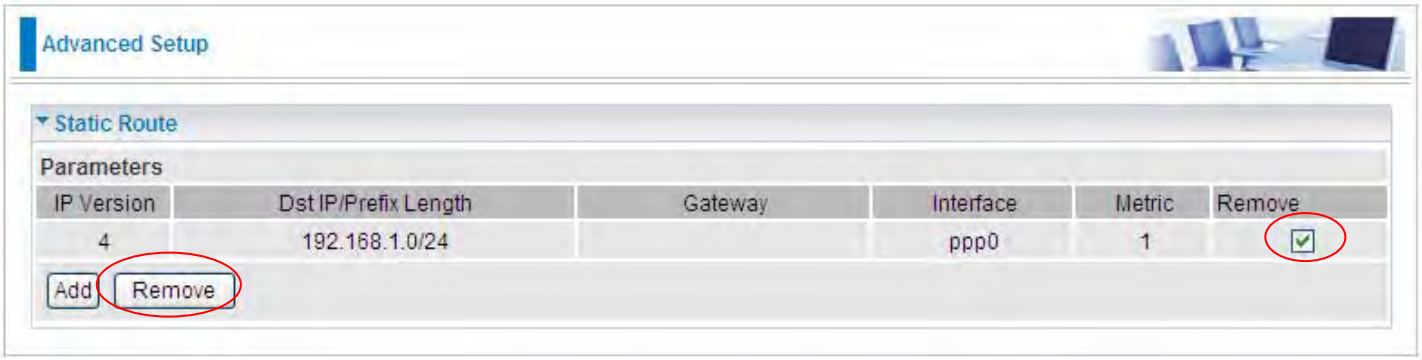
Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

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

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

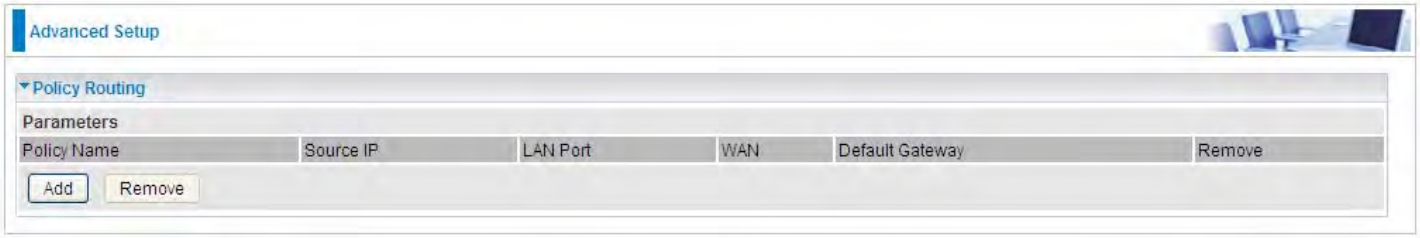
In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.



Policy Routing

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

The following is the policy Routing listing table.



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

Policy Name: User-defined name.

Physical LAN Port: Select the LAN port.

Source IP: Enter the Host Source IP.

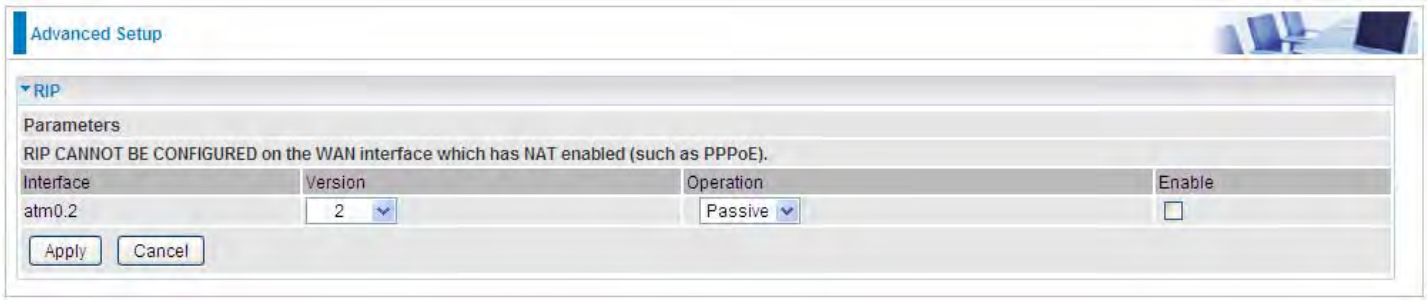
Interface: Select the WAN interface which you want the Source IP to access outside through.

Default Gateway: Enter the default gateway which you want the Source IP to access outside through.

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

RIP

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



Interface: the interface the rule applies to.

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

Operation: RIP has two operation mode.

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

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

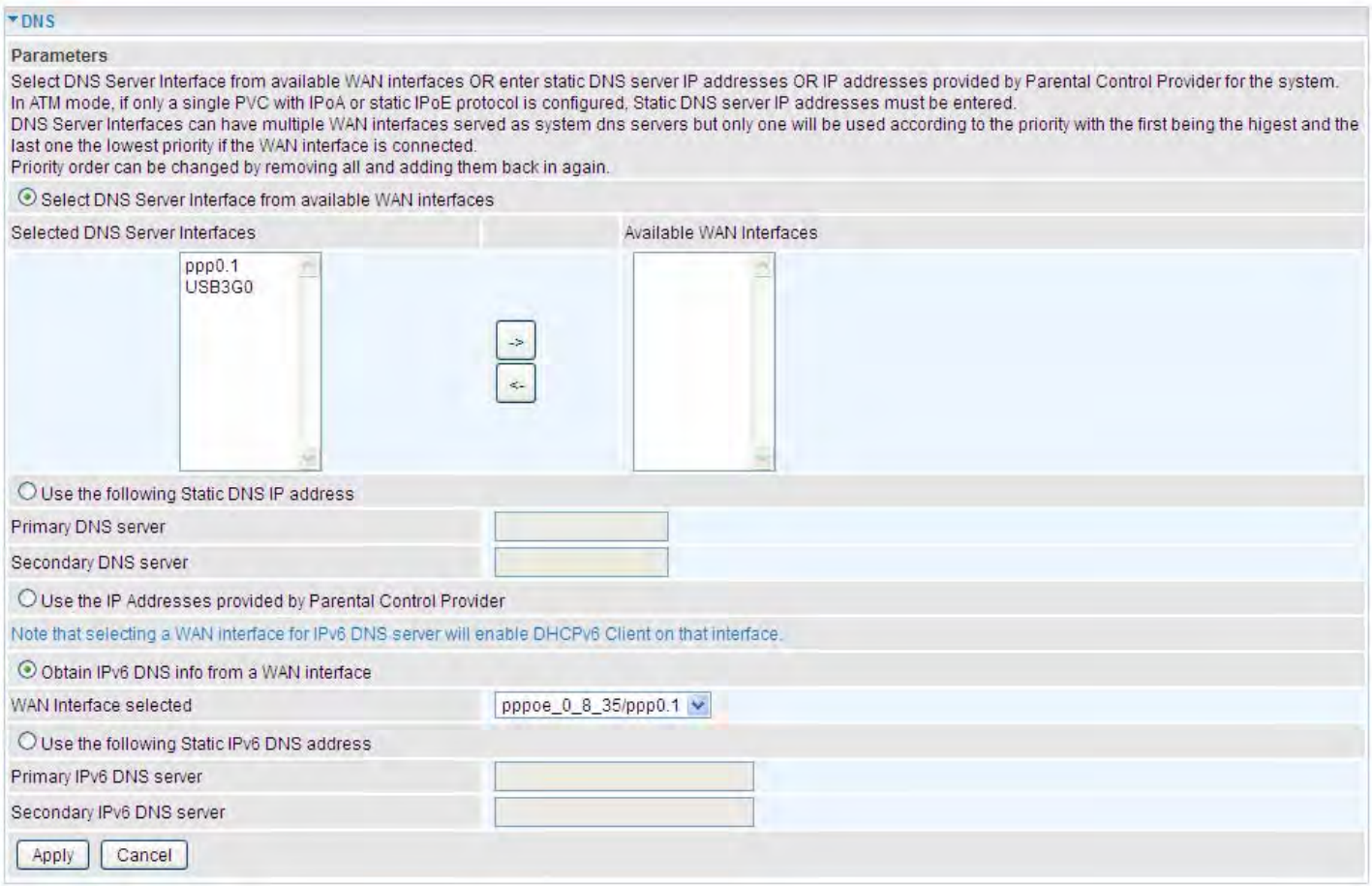
Note: RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

Click **Apply** to apply your settings.

DNS

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

DNS



➢ IPv4

Three ways to set an IPv4 DNS server

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

➢ IPv6:

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

Obtain IPv6 DNS info from a WAN interface

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

Use the following Static IPv6 DNS address

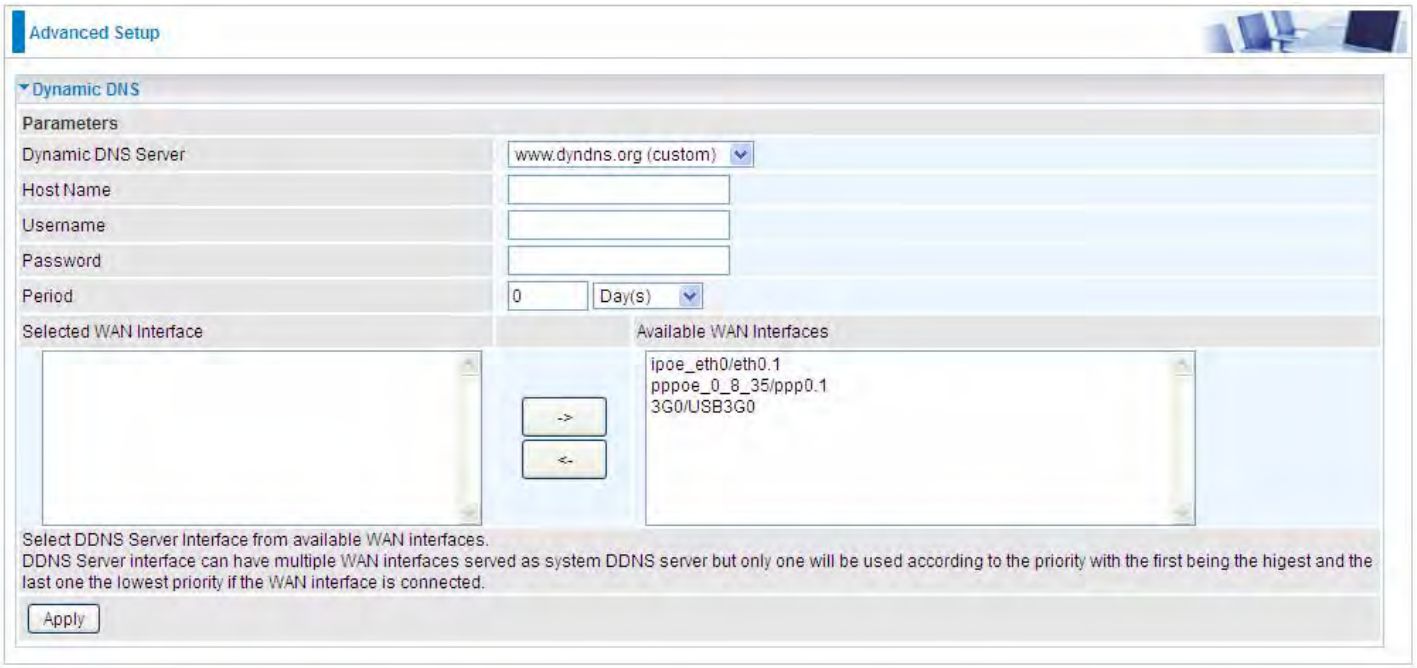
Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

Dynamic DNS

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

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

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



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

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

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

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

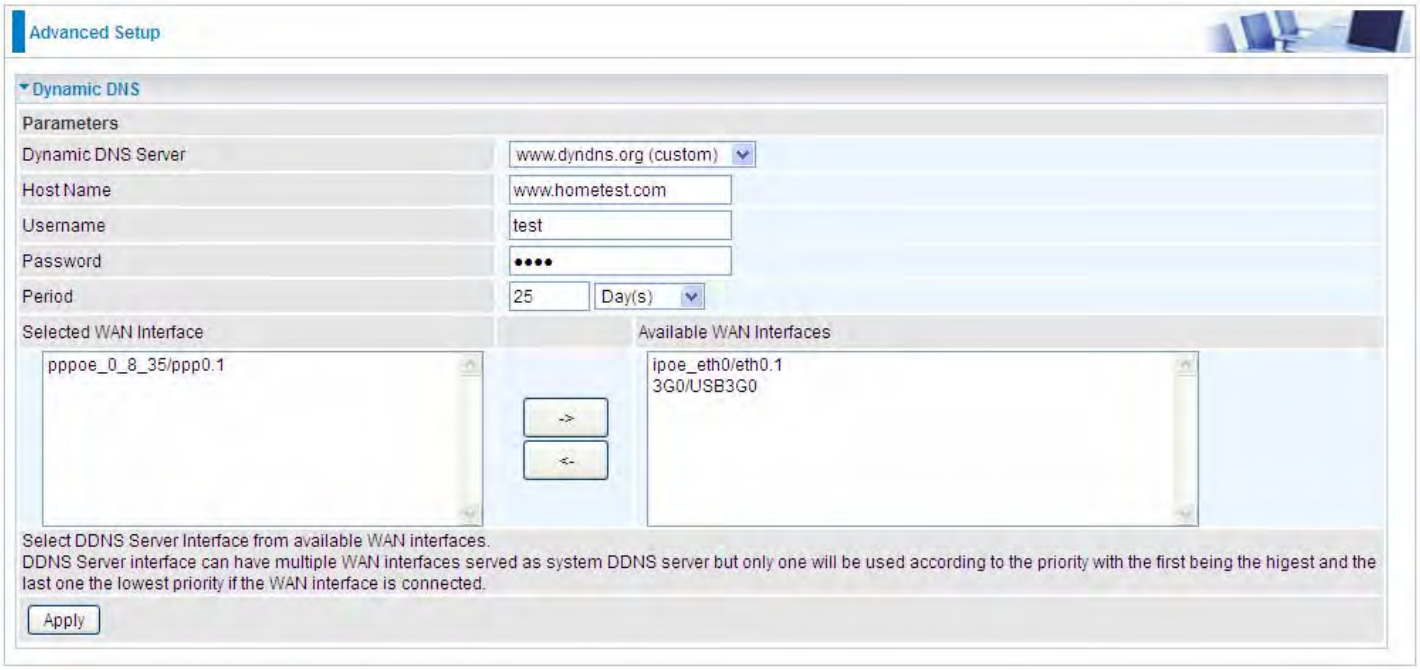
Selected WAN Interface: Select the Interface that is bound to the registered Domain name.

User can register different DDNS to different interfaces.

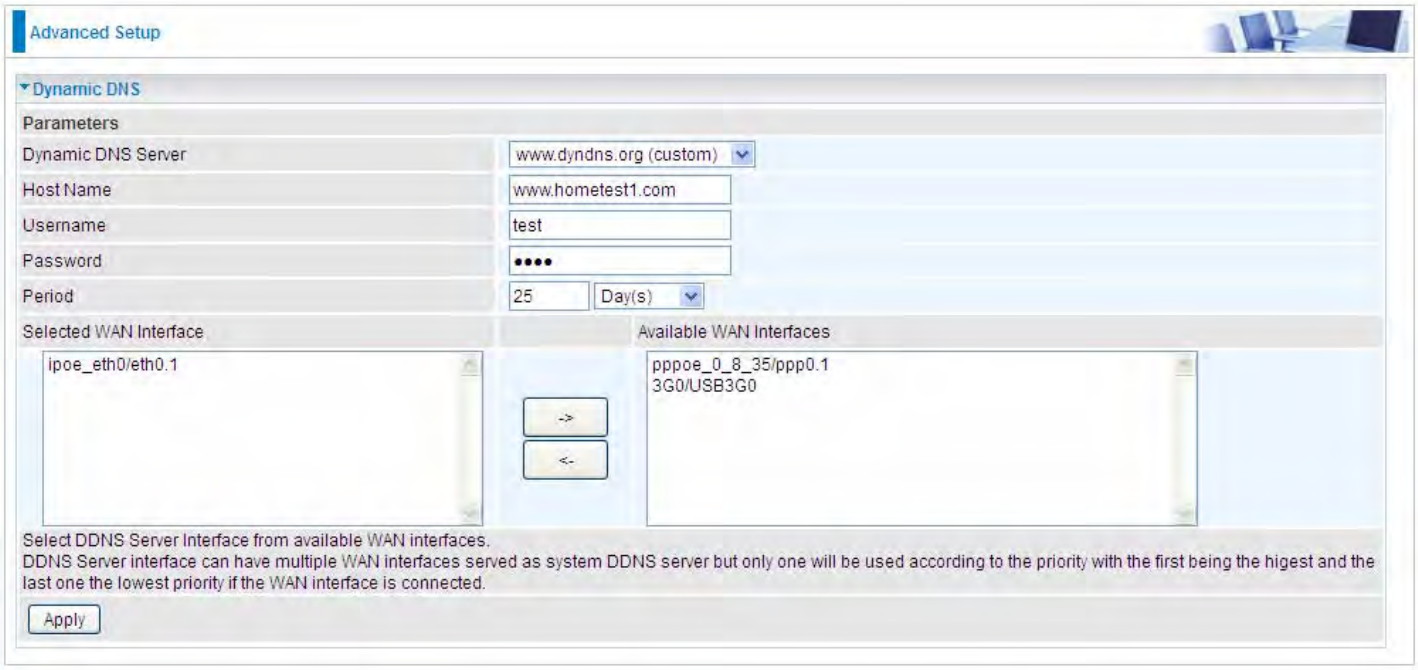
Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

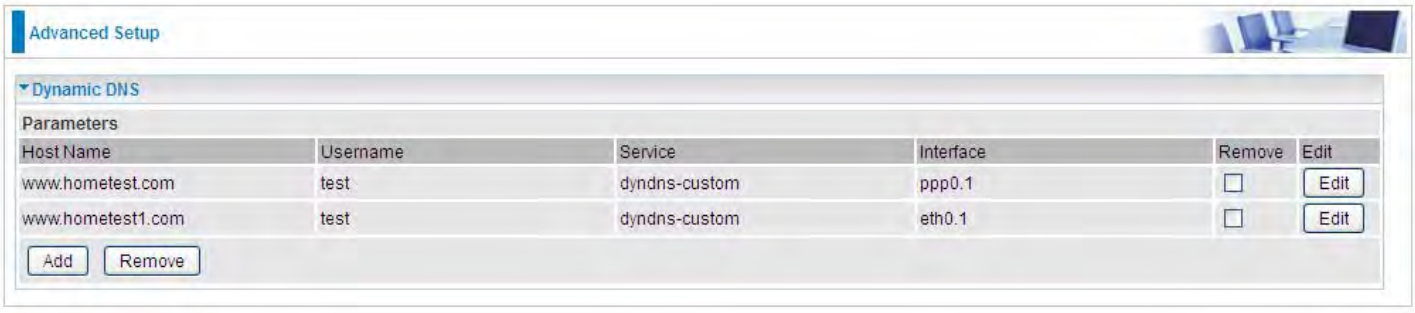
User ***test*** register two Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

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



2. ipoe_eth0 with DDNS: www.hometest1.com using username/password test/test.





DNS Proxy

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

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

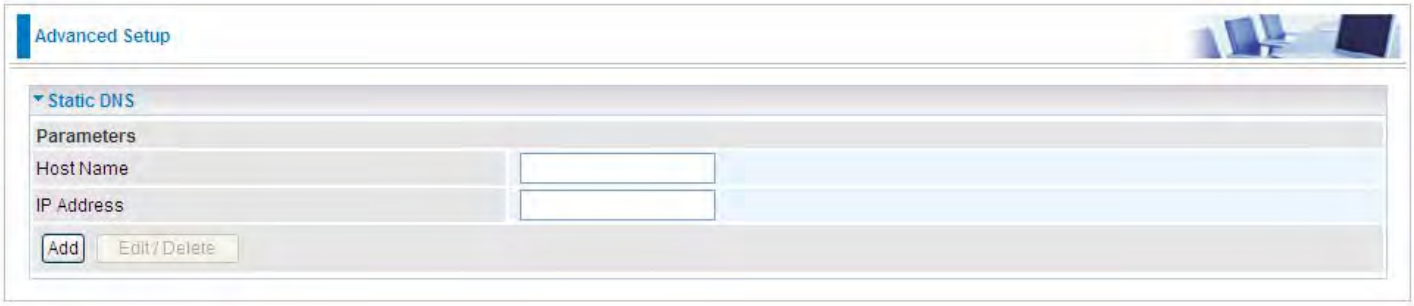
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

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

Static DNS

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

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



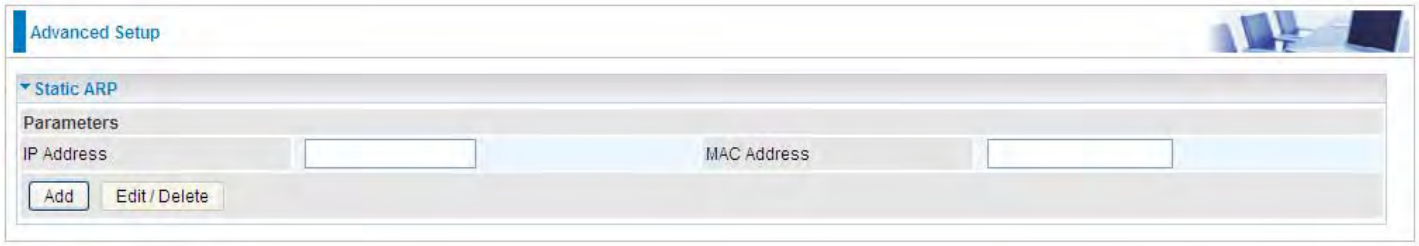
Host Name: Type the domain name (host name) for the specific IP .

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

Click **Add** to save your settings.

Static ARP

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



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

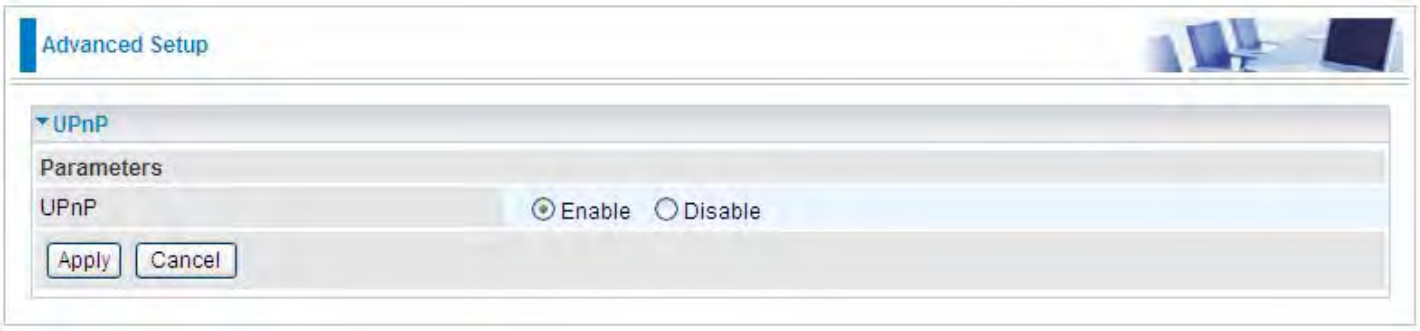
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

UPnP

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

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



UPnP:

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

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.
Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.
Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

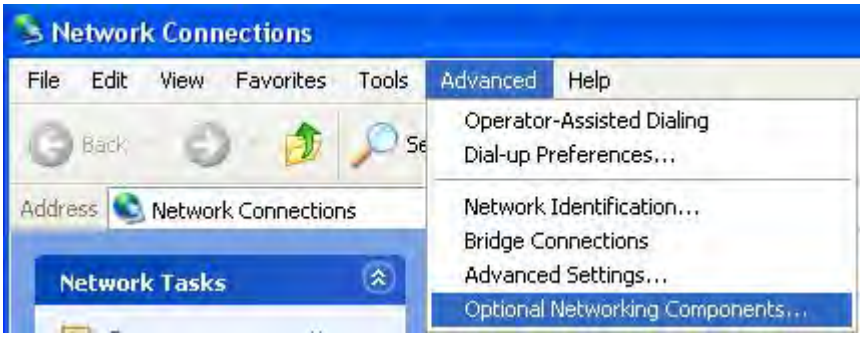
Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.

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

Step 5: Restart the computer when prompted.

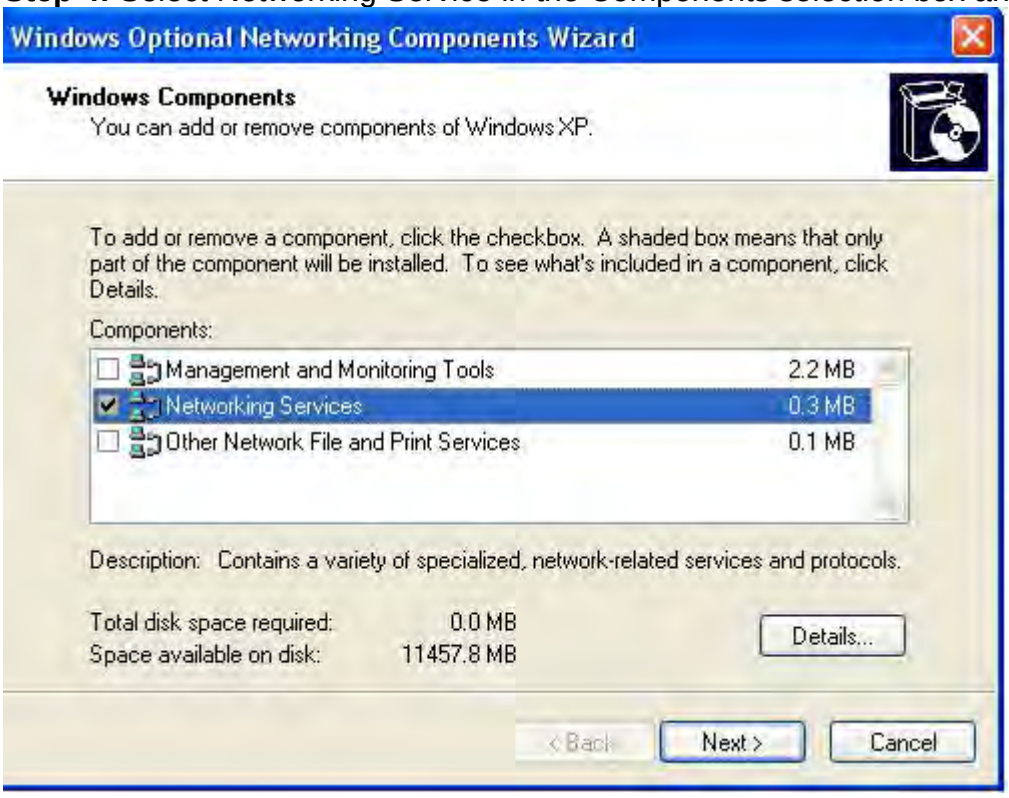
Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.
Step 2: Double-click Network Connections.
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

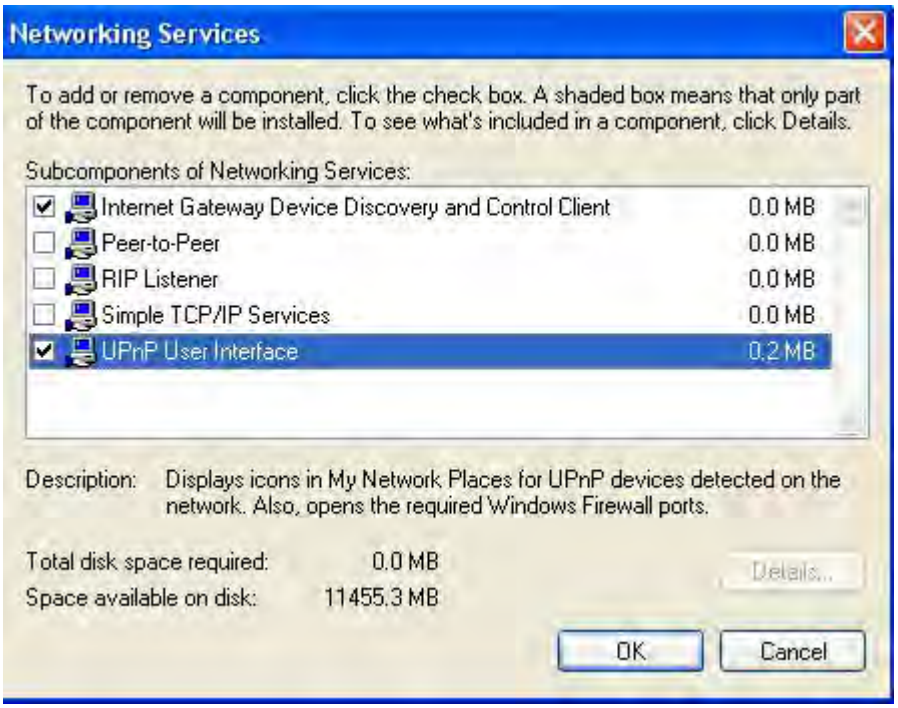


The Windows Optional Networking Components Wizard window displays.

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



Step 5: In the Networking Services window, select the Universal Plug and Play check box.
Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.

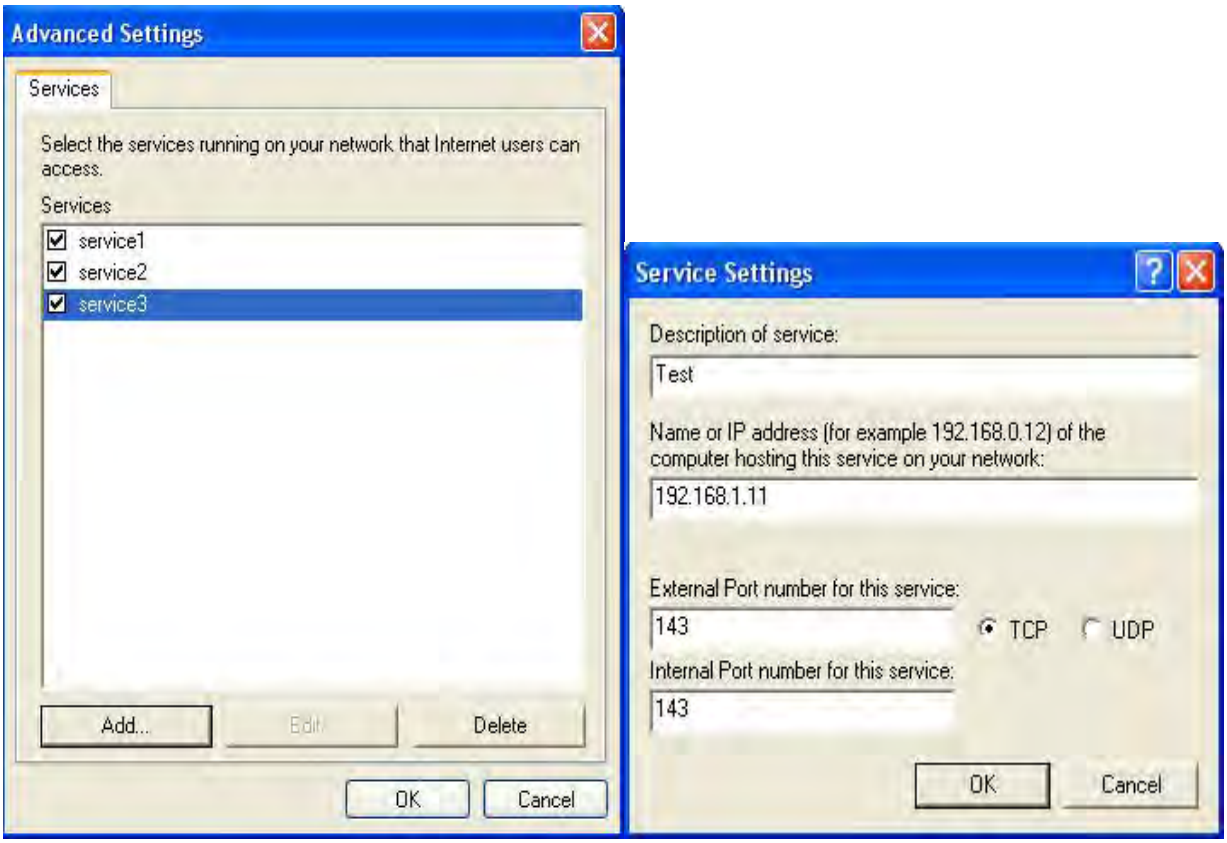


Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.
Step 2: Right-click the icon and select Properties.

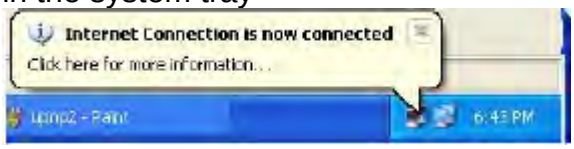
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

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



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

in the system tray



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

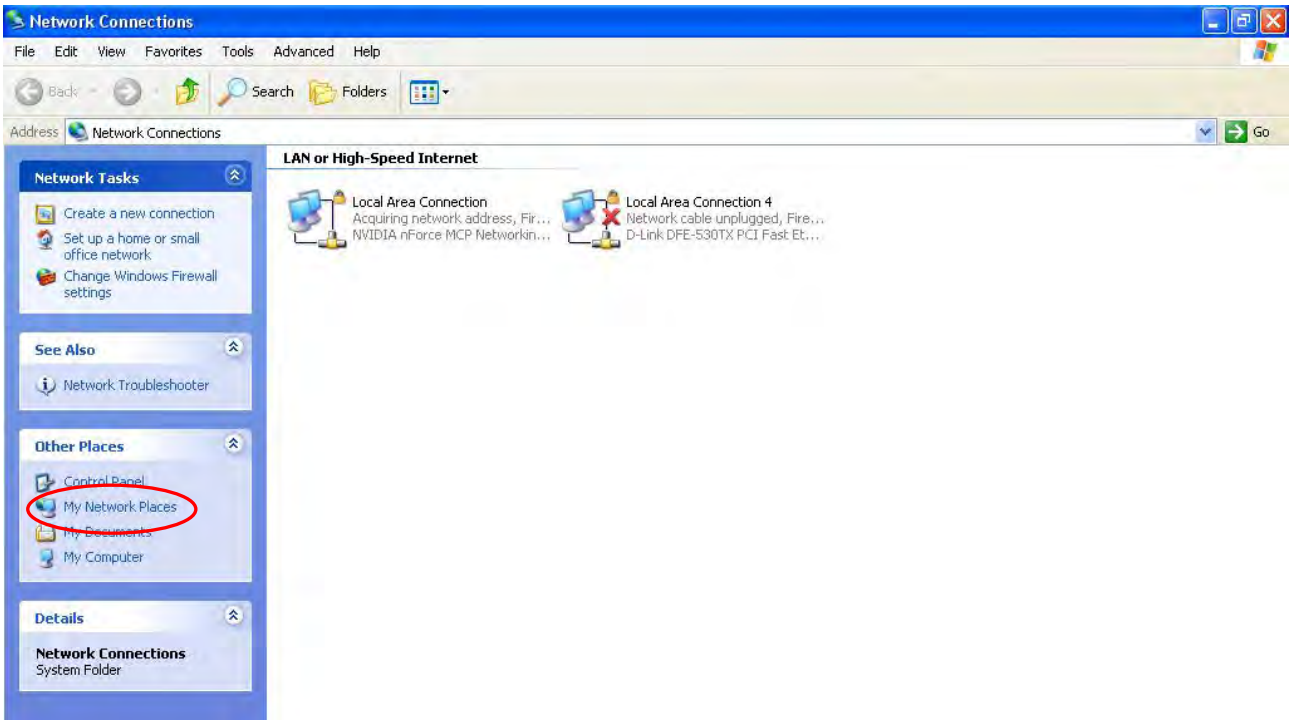
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7820NZ without first finding out the IP address of the router. This helps if you do not know the router's IP address.
Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Step 4: An icon describing each UPnP-enabled device shows under Local Network.

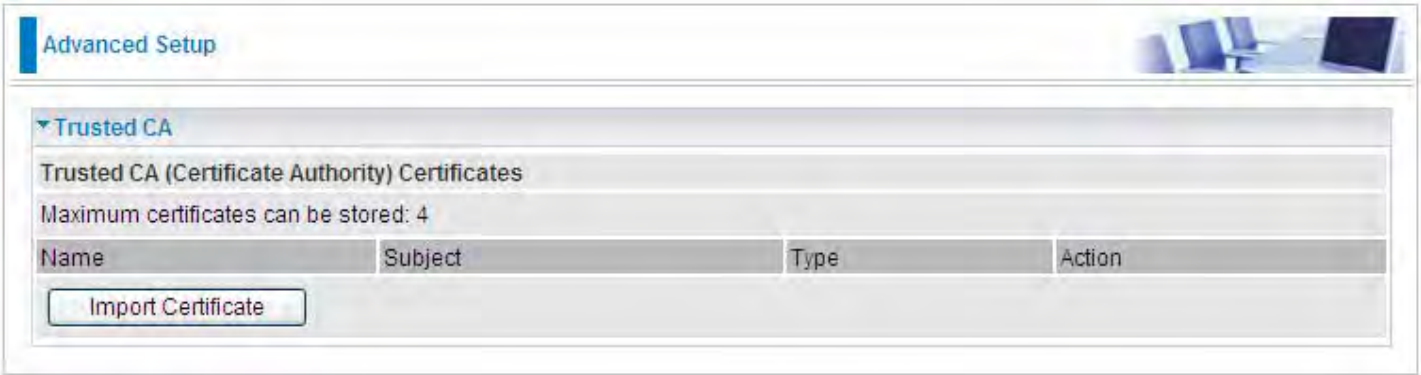
Step 5: Right-click on the icon of your BiPAC 7820NZ and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7820NZ and select Properties. A properties window displays basic information about the BiPAC 7820NZ.

Certificate

The feature is to facilitate users to import different certificates for server certificate authentication, like TR-069, OpenVPN etc. If the imported certificate doesn't match the authorized certificate of the ACS Server, OpenVPN Server, the device will have no access to the server.

Trusted CA



Certificate Name: The certificate identification name.

Subject: The certificate subject.

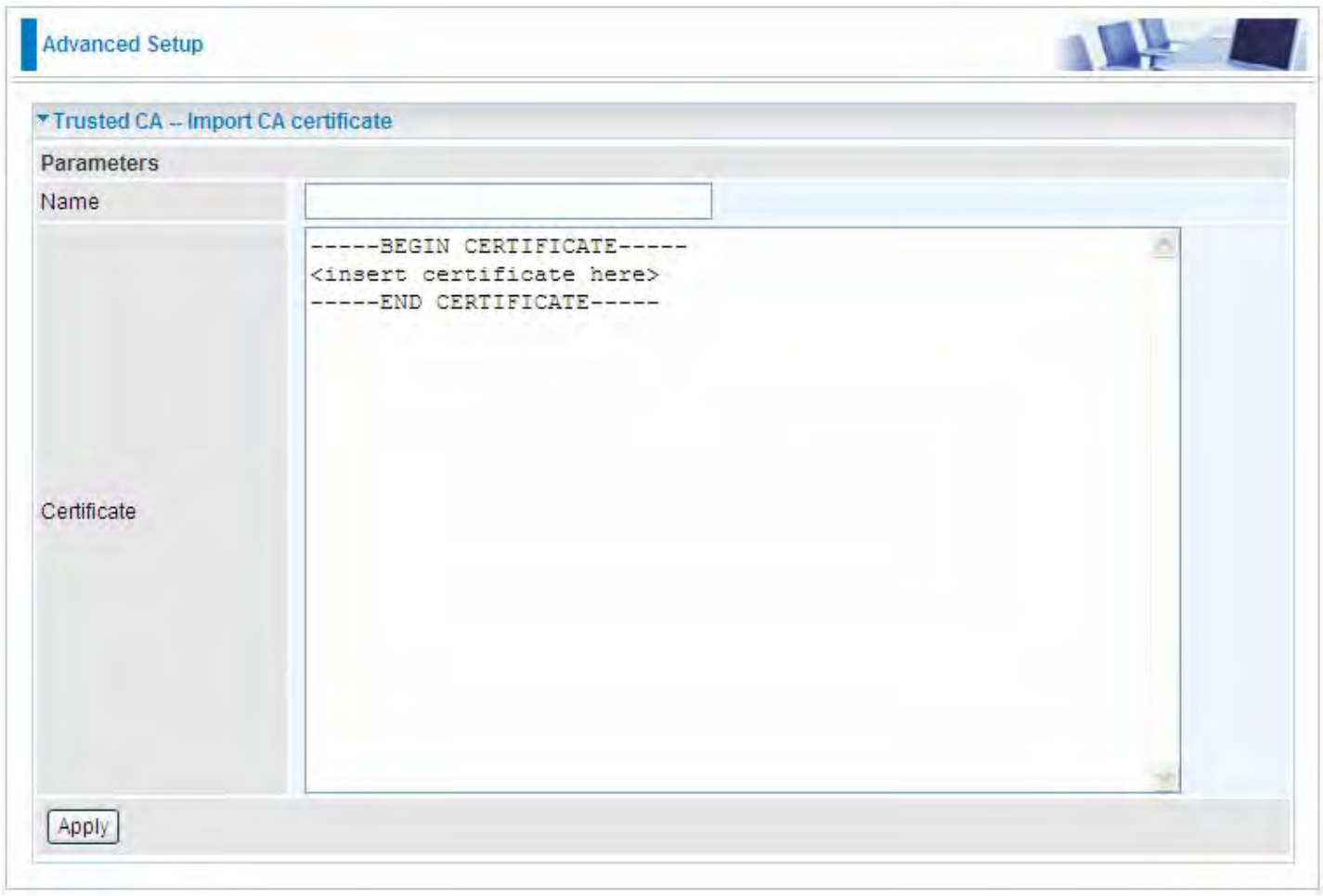
Type: The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

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

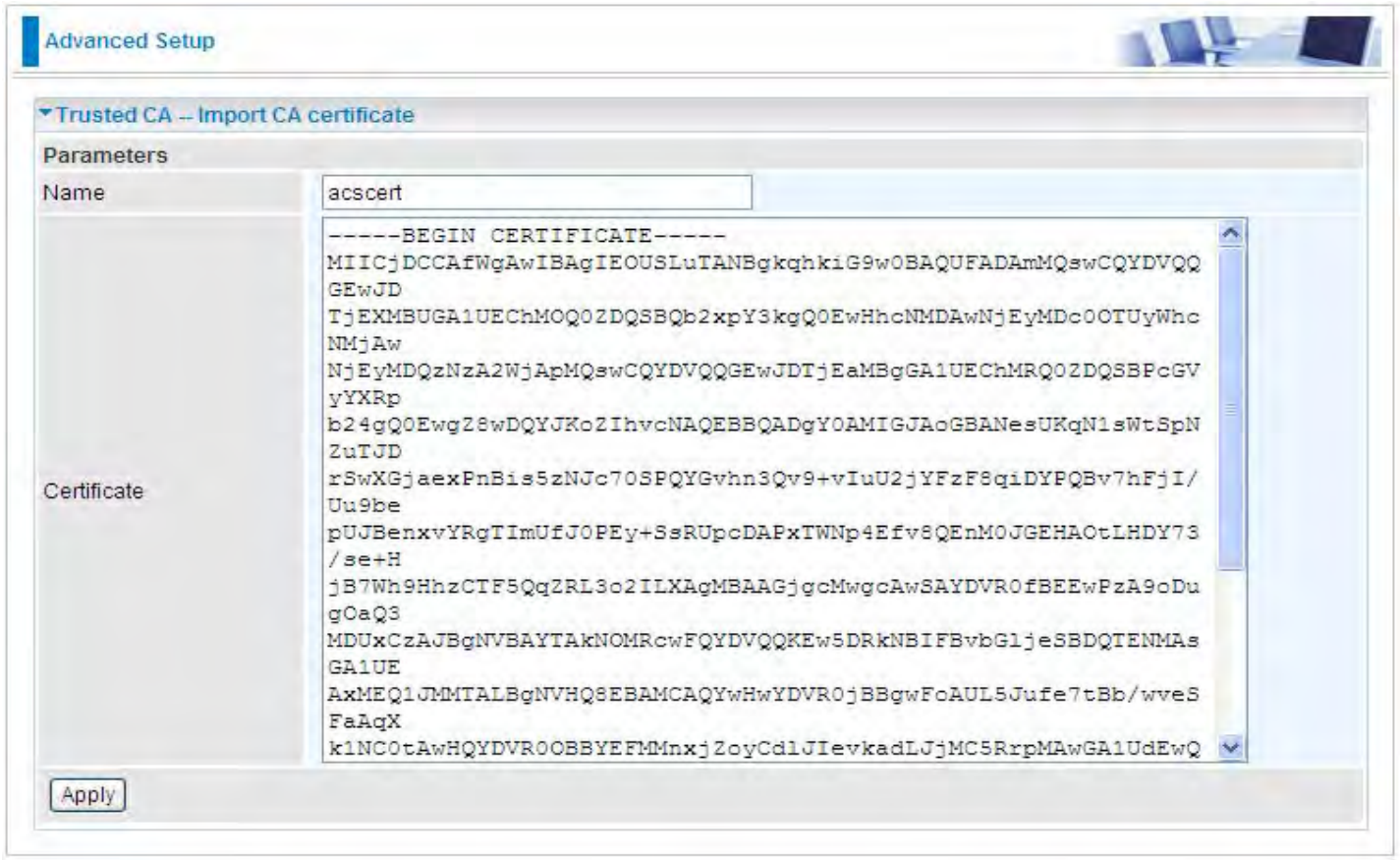
Action:

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

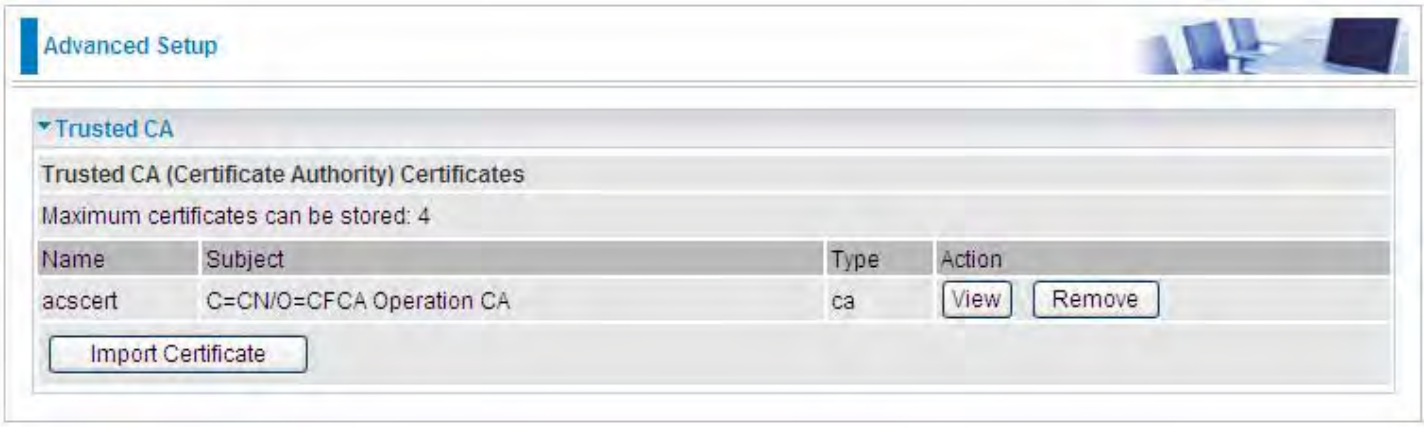
Click **Import Certificate** button to import your certificate.



Enter the certificate name and insert the certificate.



Click Apply to confirm your settings.

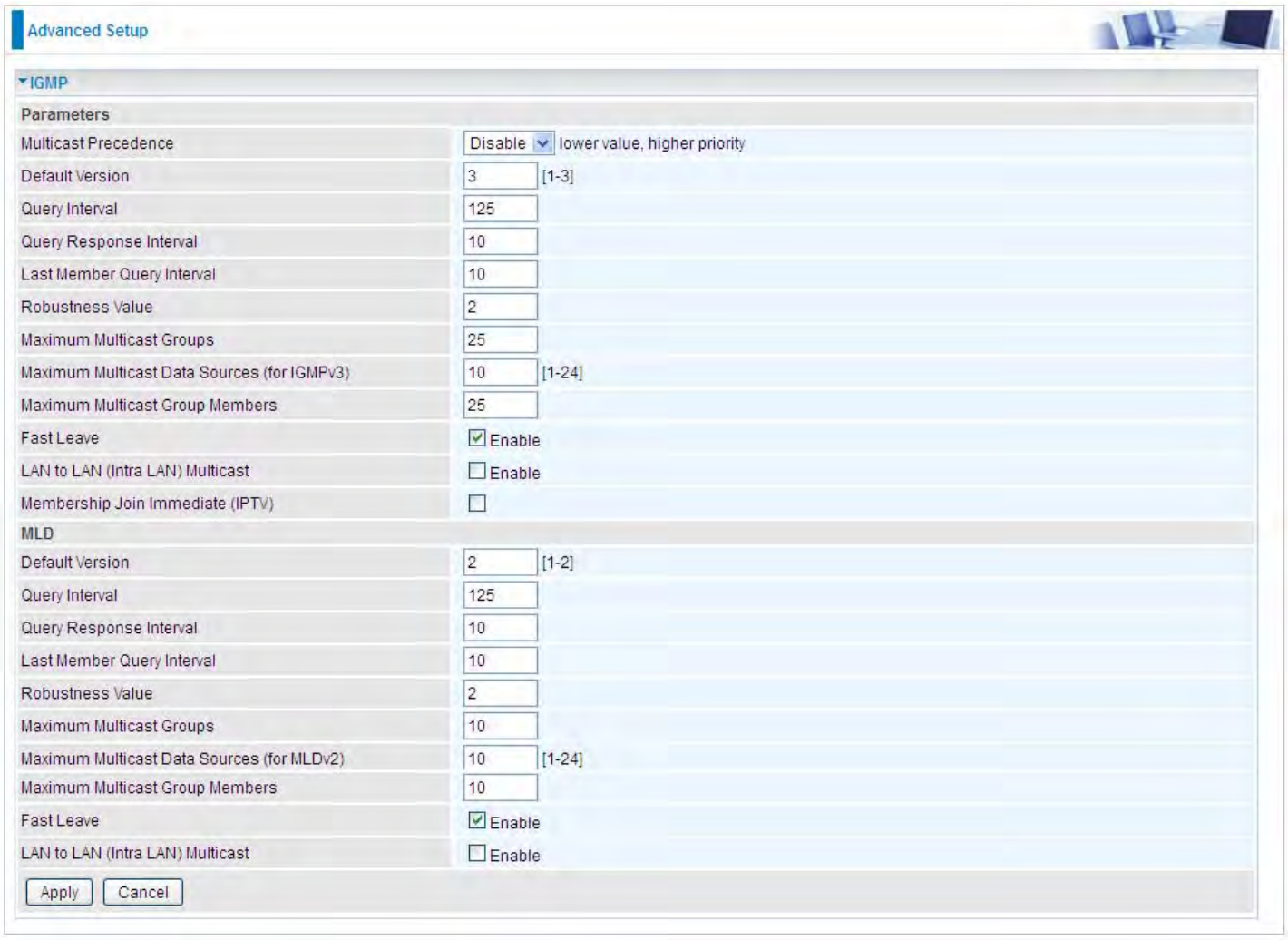


Multicast

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

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

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



IGMP

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

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

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

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

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

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

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

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

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

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

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Membership Join Immediate (IPTV): When a host joins a multicast session, it sends unsolicited join report to its upstream router immediately. The Startup Query Interval has been set to 1/4 of the General Query value to enable the faster join at startup.

MLD

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

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

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

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

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

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

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

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

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

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Management

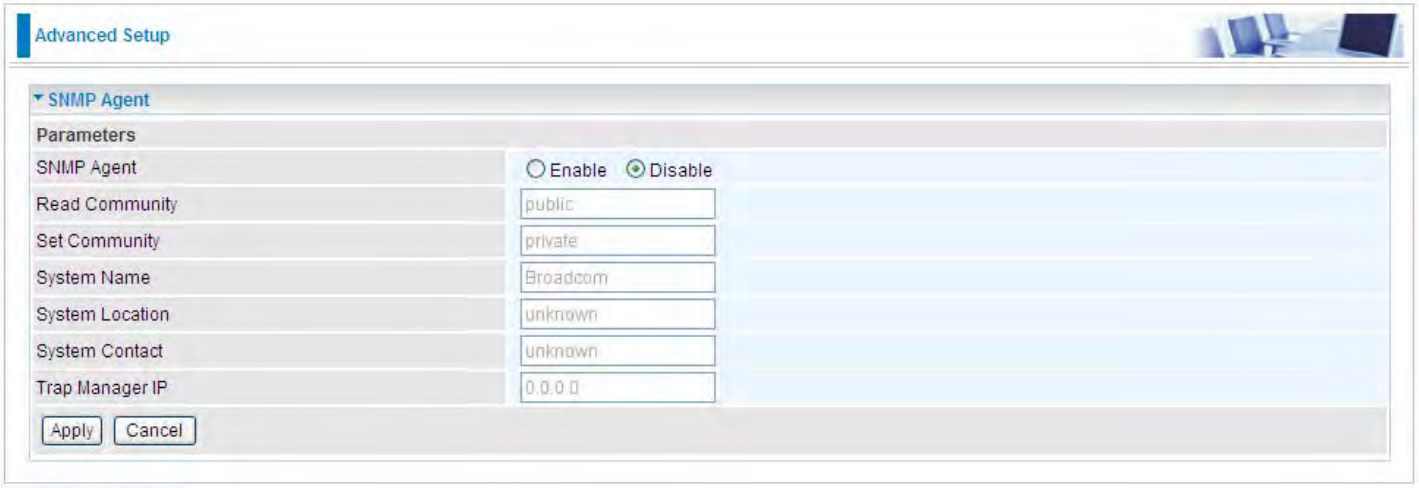
SNMP Agent

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

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

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

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



SNMP Agent: enable or disable SNMP Agent.

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

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

System Name: here it refers to your router.

System Location: user-defined location.

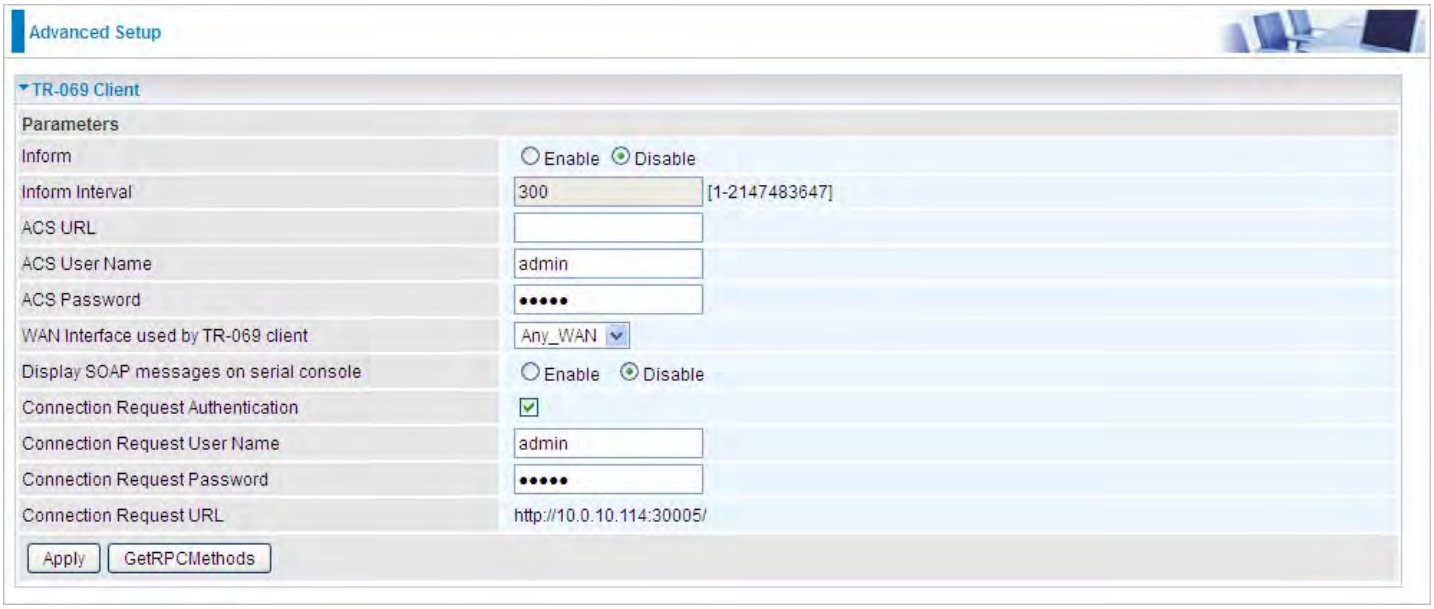
System Contact: user-defined contact message.

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

TR- 069 Client

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

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



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

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

ACS URL: Enter the ACS server login name.

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

ACS password: Enter the ACS server login password.

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

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

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

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

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

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

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

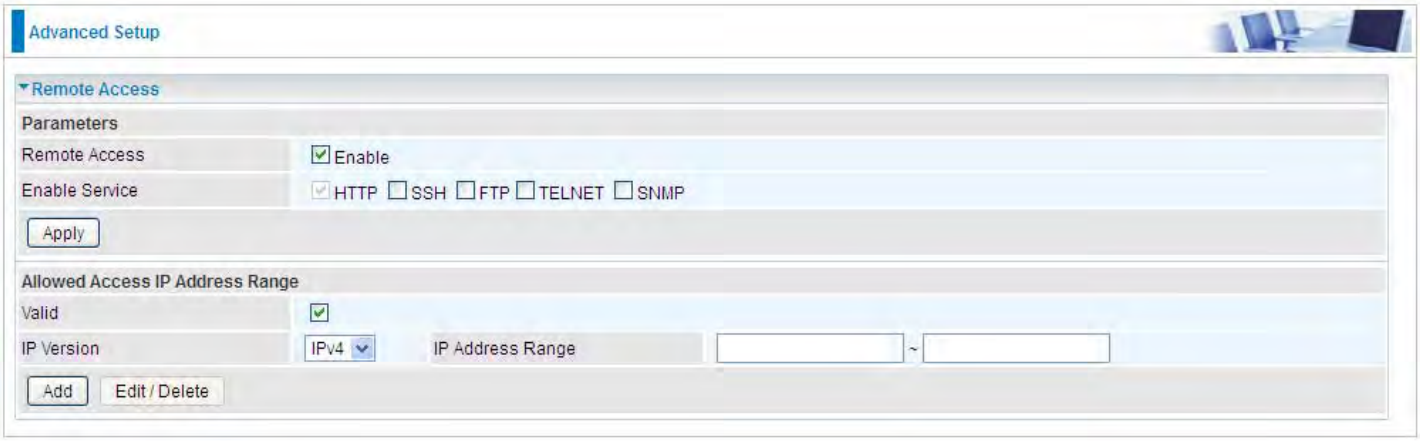
Click **Apply** to apply your settings.

HTTP Port

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

Remote Access

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



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

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

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

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

Valid: Enable/Disable Allowed Access IP Address Range

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

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

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

2. Remote Access enabled:

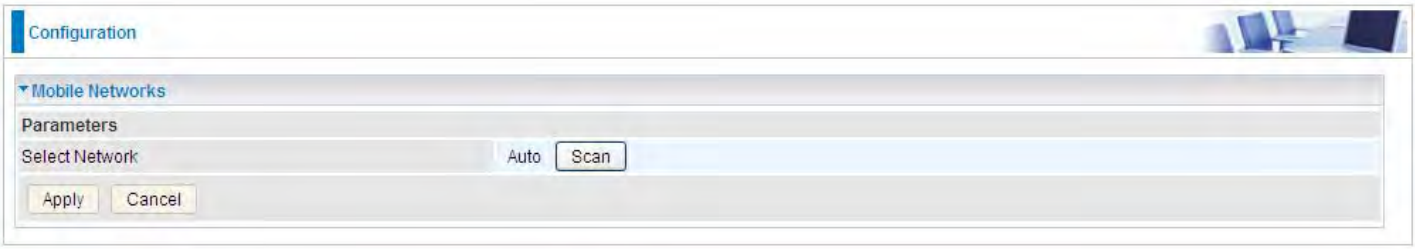
1) Enable ***Valid*** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.

2) Disable ***Valid*** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.

3) No listing of IP range is to allow any IP(s) to remote access the router.

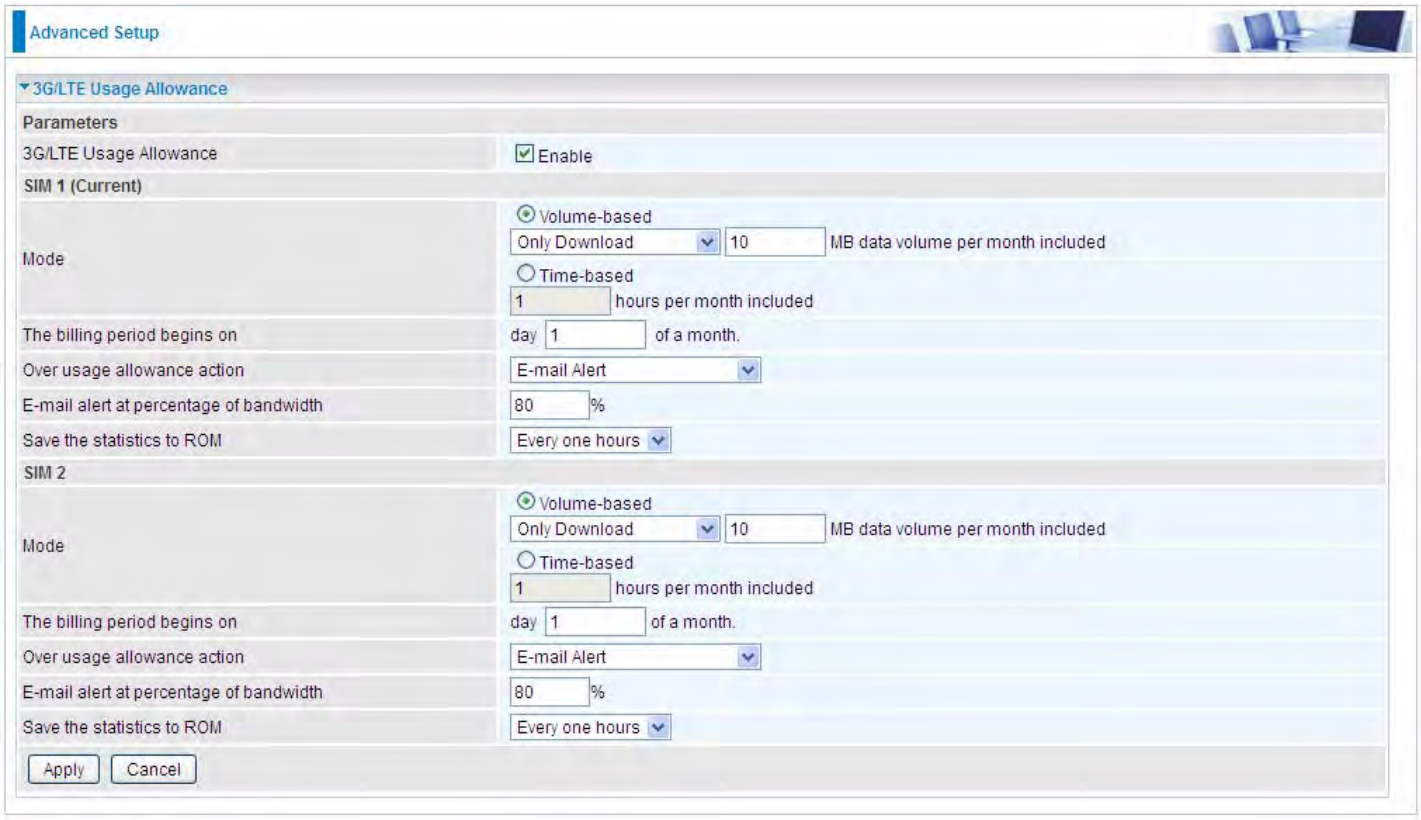
Mobile Network

User can press **Scan** to discover available 3G/LTE mobile network.



3G/LTE Usage Allowance

3G/LTE usage allowance is designated for users to monitor and control the 3G flow usage. 7820NZ's 3G/LTE usage allowance offers exact control settings for each SIM card.



3G/LTE Usage Allowance: Enable to monitor 3G/LTE usage.

SIM 1 & SIM 2

Mode: include Volume-based and Time-based control.

- **Volume-based** include "only Download", "only Upload" and "Download and Upload" to limit the flow.
- **Time-based** control the flow by providing specific hours per month.

The billing period begins on: The beginning day of billing each month.

Over usage allowance action: What to do when the flow is over usage allowance, the available methods are "E-mail Alert", "Email Alert and Disconnect" and "Disconnect".

E-mail alert at percentage of bandwidth: When the used bandwidth exceeds the set proportion, the system will send email to alert.

Save the statistics to ROM: To save the statistics to ROM system.

Power Management

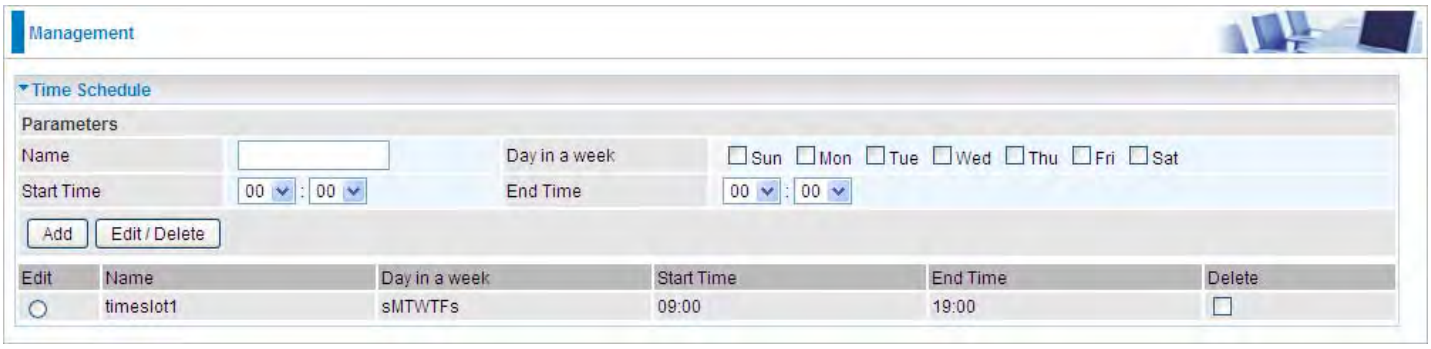
Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.

Time Schedule

The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.
This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Internet Times** for details.

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

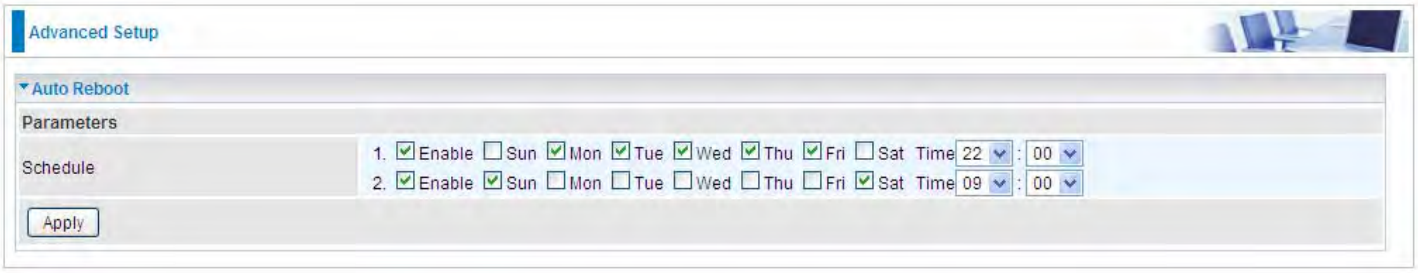


Auto Reboot

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

Enable to set the time schedule for rebooting.

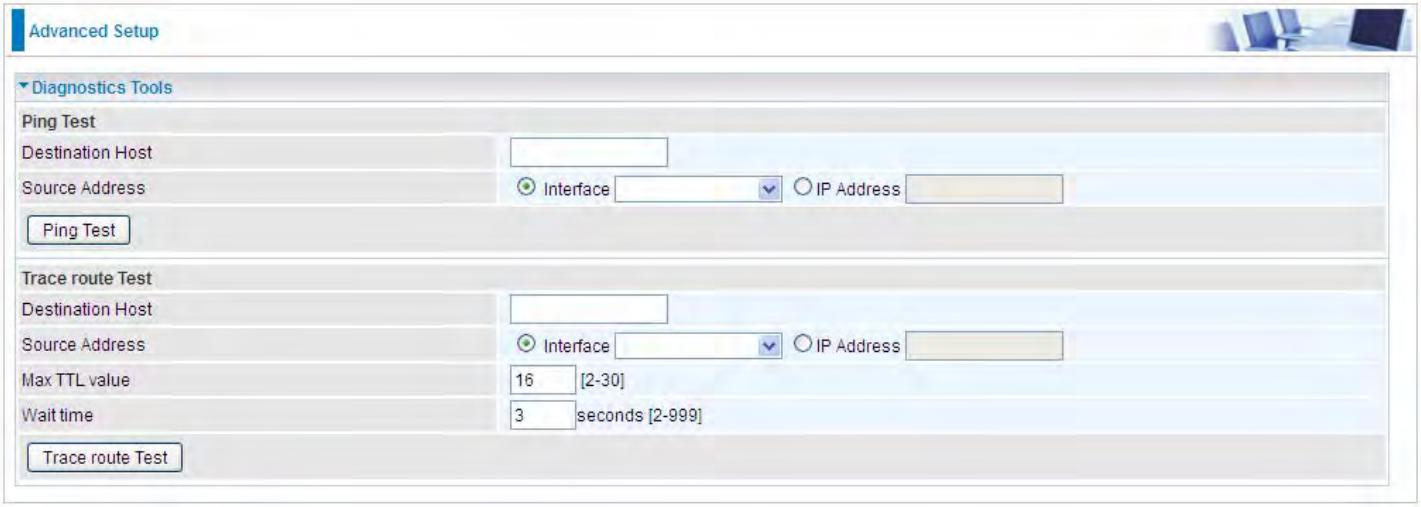
For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:



Diagnostics

Diagnostics Tools

BiPAC 7820NZ offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.



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

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

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

Ping Test: Press this button to proceed ping test.

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

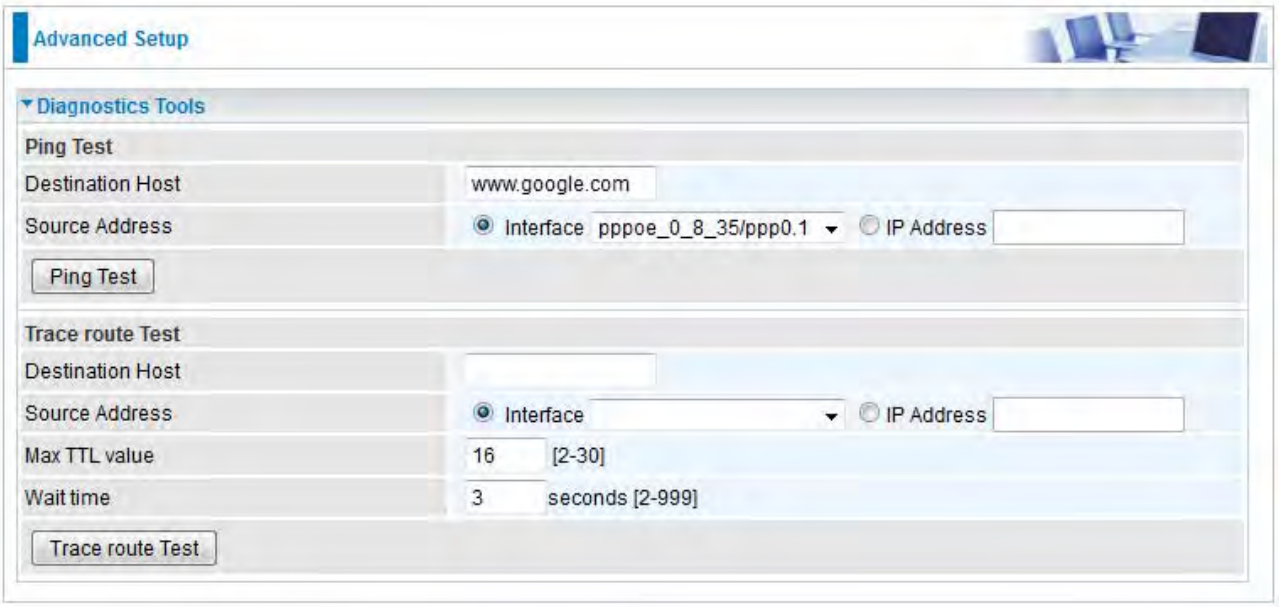
Destination Host: Set the destination host (IP, domain name) to be traced.

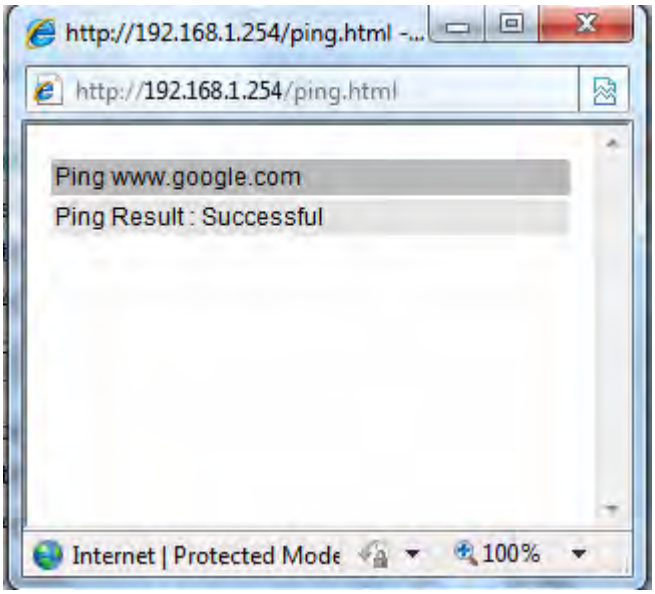
Source Address: Select or set the source address to trace the route from the source to the destination.

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

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

Example: Ping www.google.com





Example: “trace” www.google.com

Push Service

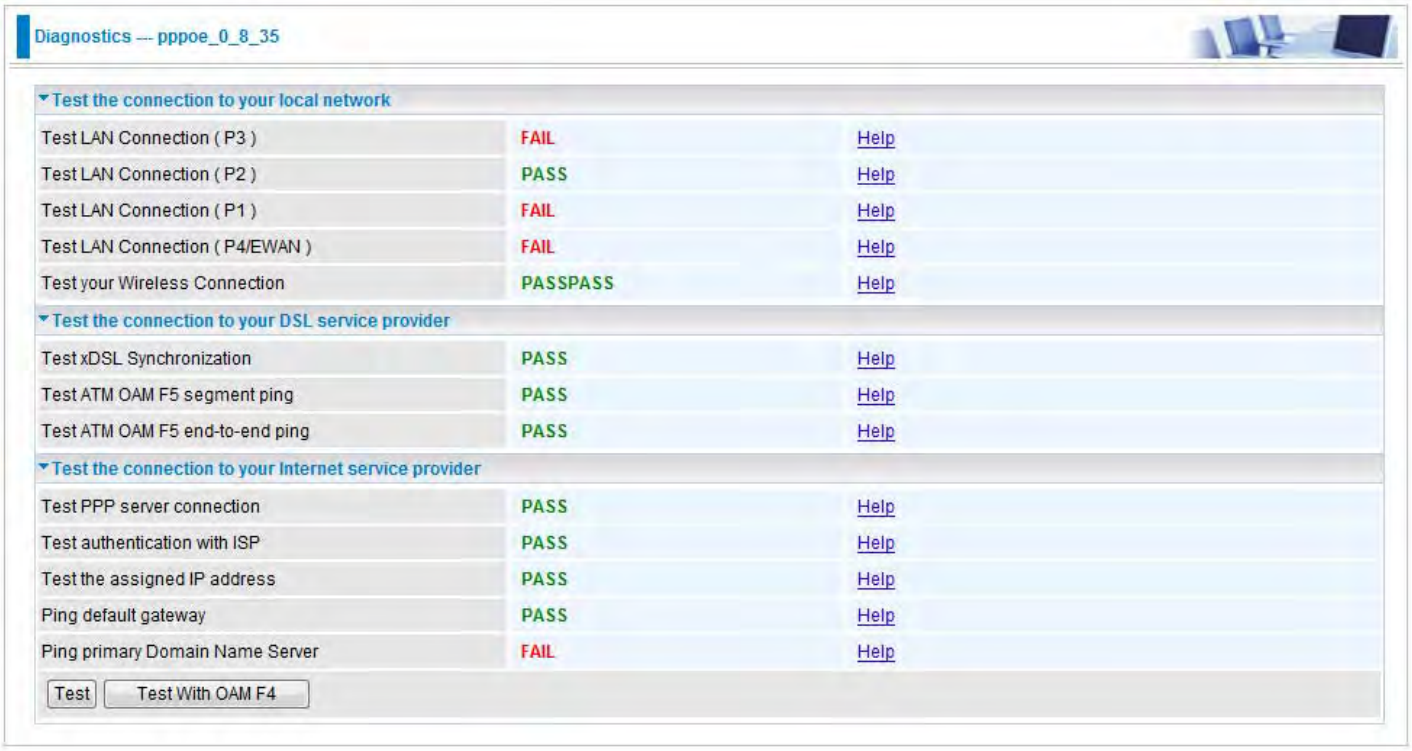
With push service, the system can send email messages with consumption data and system information.

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

Note: Please first set correct the SMTP server parameters in Mail Alert.

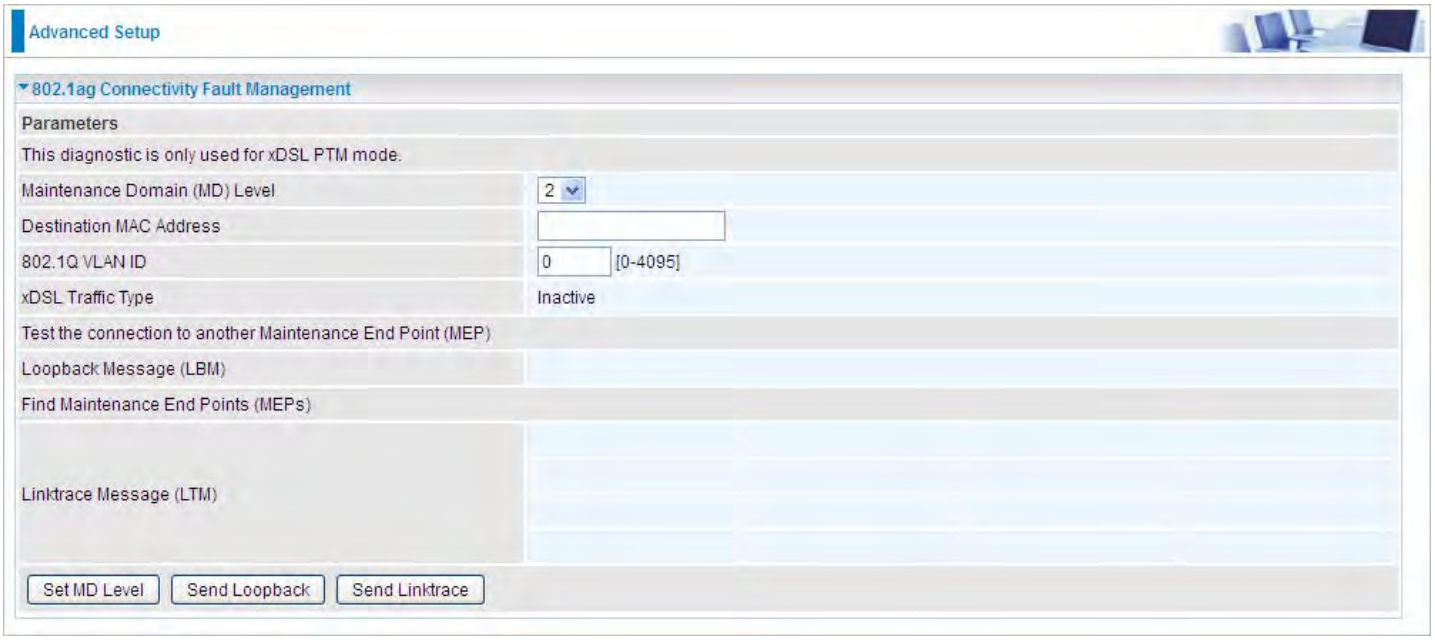
Diagnostics

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



Fault Management

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



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

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

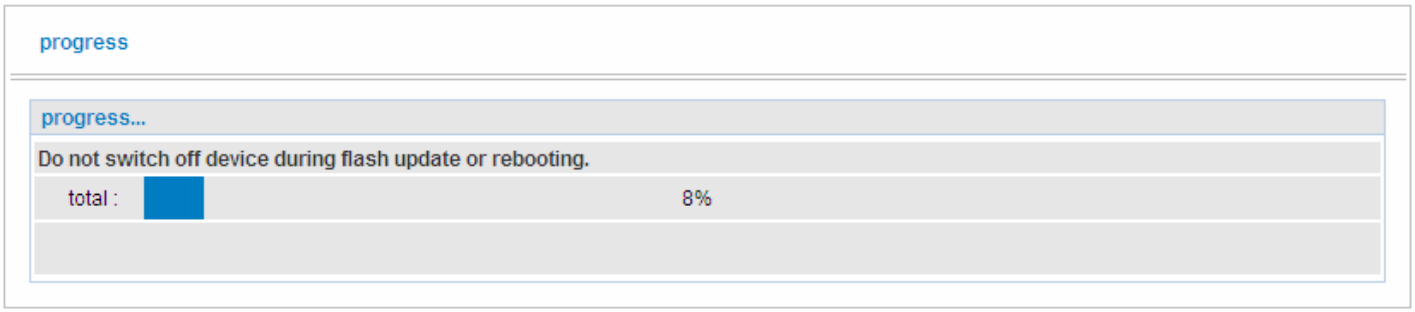
Link Trace: Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating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

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

Restart

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

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



Chapter 5: Troubleshooting

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

Problems with the router

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

Problems with WAN interface

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

Problem with LAN interface

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

Appendix: Product Support & Contact

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

Contact Billion

Worldwide:

http://www.billion.com

Federal Communication Commission Interference Statement

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

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

FCC Caution:

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

(1) This device may not cause harmful interference

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

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

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.

IC Warning:

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) this device may not cause interference, and

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.