by 3 consecutive fails, the router will determine failover to WAN2 (backup port)).

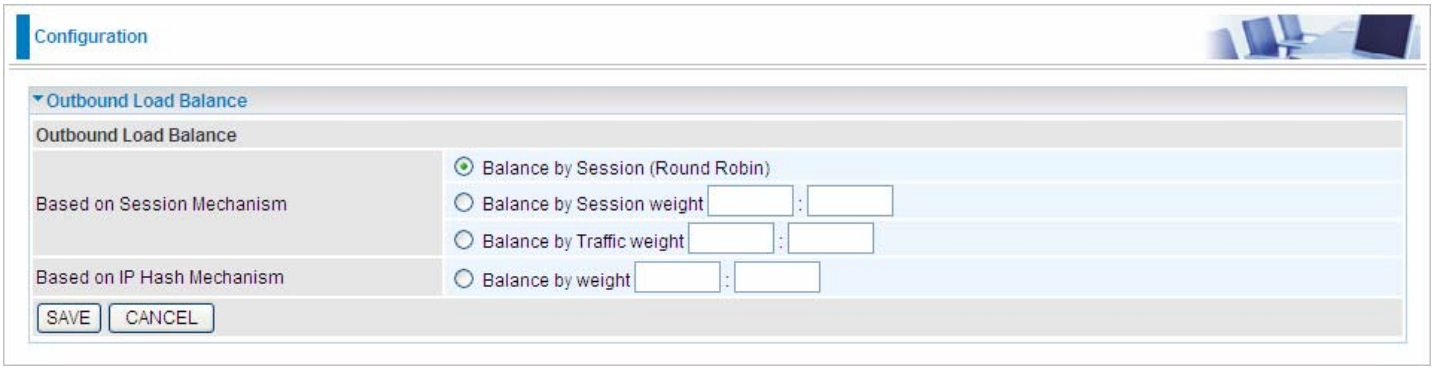
2).The failback setting follow the same decision policy as the failover. For example, according to settings above in the screenshot, the connection probe will be carried out every 30 seconds, and 3 consecutive times of probe success is found, the router will determine failback to WAN1 (main WAN).

Probe WAN 1/2: Choose the probe policy, to probe gateway or host (users decide themselves)

- ⓘ **Gateway:** It will send ping packets to gateway of Wan1 interface and wait for response from it in every “Probe Cycle” to check the connectivity of the gateway of WAN1 interface.
- ⓘ **Host:** It will send ping packets to specific host and wait for response in every “Probe Cycle”. The host must be an IP address

5.5.2 Outbound Load Balance *(7600NX only)*

The connections are distributed over WAN1 and WAN2 so that it can utilize bandwidth of both WAN ports. With Outbound load balance, traffic may be routed to a faster link when one of the WAN is slower or congested so that user gains better throughput and less delay.



User can distribute outbound traffic based on **Session Mechanism** or **IP Hash Mechanism**.

Based on Session Mechanism

Balance by Session (Round Robin): Balance session traffic based on a round robin method.

Balance by Session weight: Balance session traffic based on a weight ratio. Enter the desired ratio in the fields provided.

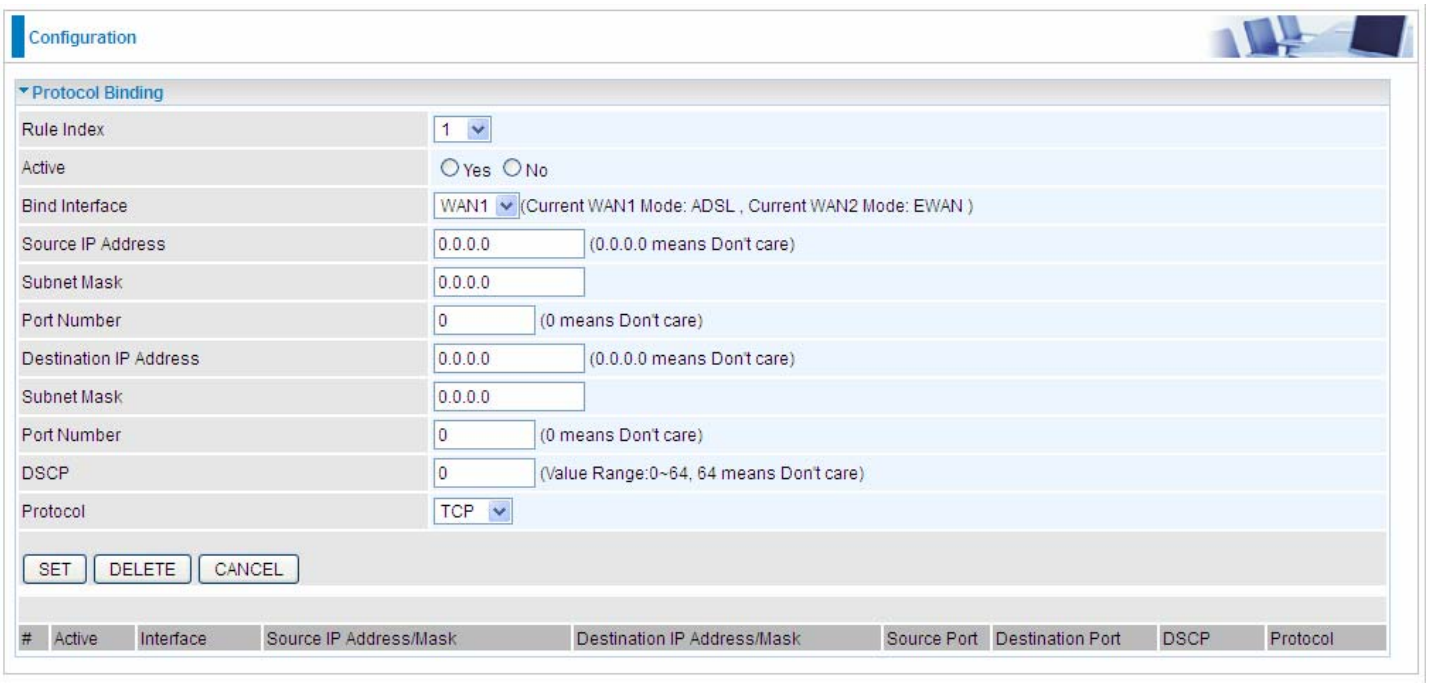
Balance by Traffic weight: Balance traffic based on a traffic weight ratio. Enter the desired ratio into the fields provided.

Based on IP Hash Mechanism

Balance by weight: Use an IP hash to balance traffic based on a ratio. Enter the desired ratio into the fields provided.

5.5.3 Protocol Binding *(7600NX only)*

Protocol Binding lets you direct specific traffic to go out from a specific WAN port. Policies determine how specific types of internet traffic are routed, for example, traffic from a particular IP(es) granted access to only one WAN port rather than using both of the WAN ports as with load balancing.



Rule Index: The index marking the rule. Maximum entries can be 16.

Active: Select whether to enable the rule.

Bind Interface: To determine the WAN interface the to-be-set rule will apply to and what type of traffic is to be bound to forward to the which WAN interface.

Source IP Address: Enter the source IP address featuring the traffic origin.

Subnet mask: Enter the subnet mask of the source network.

Port Number: Enter the port number.

Destination IP Address: Enter the destination IP address featuring the traffic destination.

Subnet mask: Enter the subnet of the designation network.

Port Number: Enter the port number which defines the application.

DSCP: The DSCP value. Value Range:0~64, 64 means Don't care

Protocol: Select the protocol traffic is using (TCP, UDP, ICMP).

Press **SET** to submit the settings.

For example:

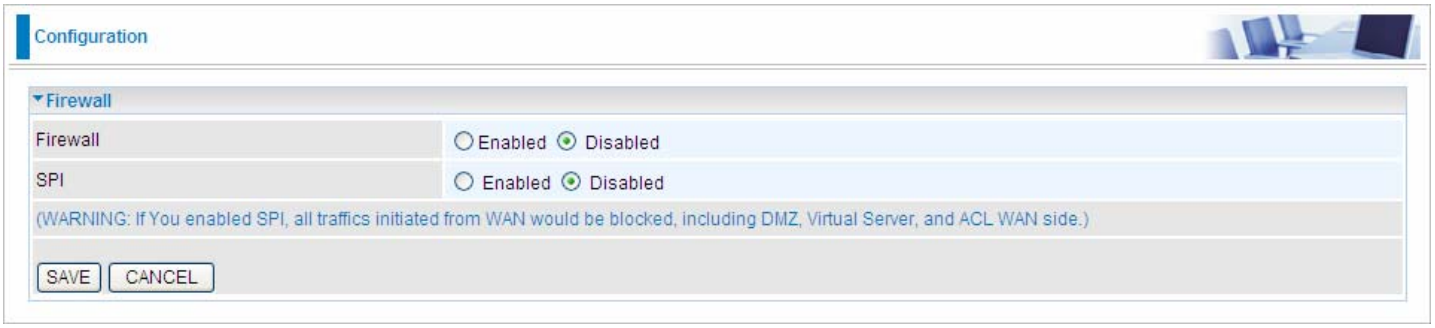
All traffic from 192.168.1.105 with port 80 (exclusive for http web access) will be routed to WAN 1, or this IP communicates with Internet through WAN1.

#	Active	Interface	Src IP Address/Mask	Destination IP Address/Mask	Src Port	Dest Port	DSCP	Protocol
1	Yes	WAN1	192.168.1.105/ 255.255.255.0	0.0.0.0/ 0.0.0.0	80	0	0	TCP

5.6 Advanced Setup

5.6.1 Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

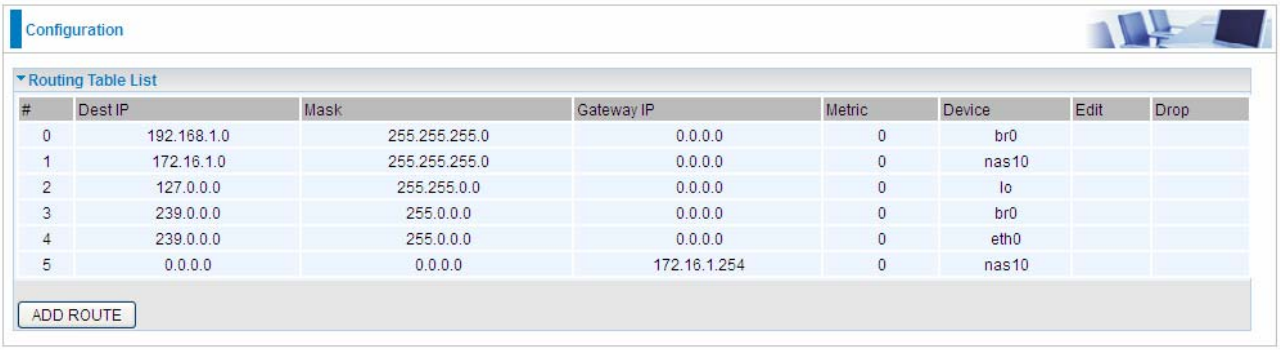
- **Enabled:** As set in default setting**,** it activates your firewall function.
- **Disabled:** It disables the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- **Enabled:** As set in default setting**,** it activates your SPI function.
- **Disabled:** It disables the SPI function.

5.6.2 Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.



#	Dest IP	Mask	Gateway IP	Metric	Device	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	172.16.1.0	255.255.255.0	0.0.0.0	0	nas10		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	eth0		
5	0.0.0.0	0.0.0.0	172.16.1.254	0	nas10		

#: Item number

Dest IP: IP address of the destination network

Mask: The subnet mask of destination network.

Gateway IP: IP address of the gateway or existing interface that this route uses.

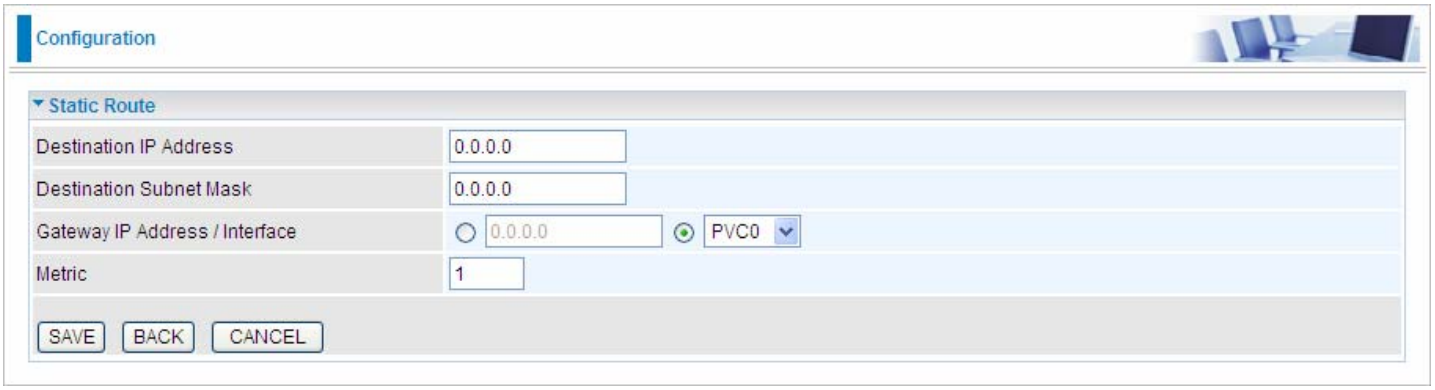
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Device: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

ADD Route



Destination IP Address: This is the destination subnet IP address.

IP Subnet Mask: The subnet mask of destination network.

Gateway IP Address/Interface：This is the gateway IP address or existing interface to which packets are to be forwarded.

Metric：It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

5.6.3 NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

In this session, there are “VPN Switch”, “SIP Switch”, “DMZ” and “Virtual Server” provided to solve these nasty problems.

VPN Switch: It is VPN pass-throughput. VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

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

Interface: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. There are eight groups of PVC can be defined and used.

NAT Status: Show the NAT status, Enable.

Click DMZ or Virtual Server to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

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

DMZ setting for: Indicate the related WAN interface which allows outside network to connect in and communicate. **Note:** Here you can see the Sing IP Account/EWAN. It is the interface set in the previous NAT page.

DMZ:

- **Disabled:** It disables the DMZ function.
- **Enabled:** It activates your DMZ function.

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

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

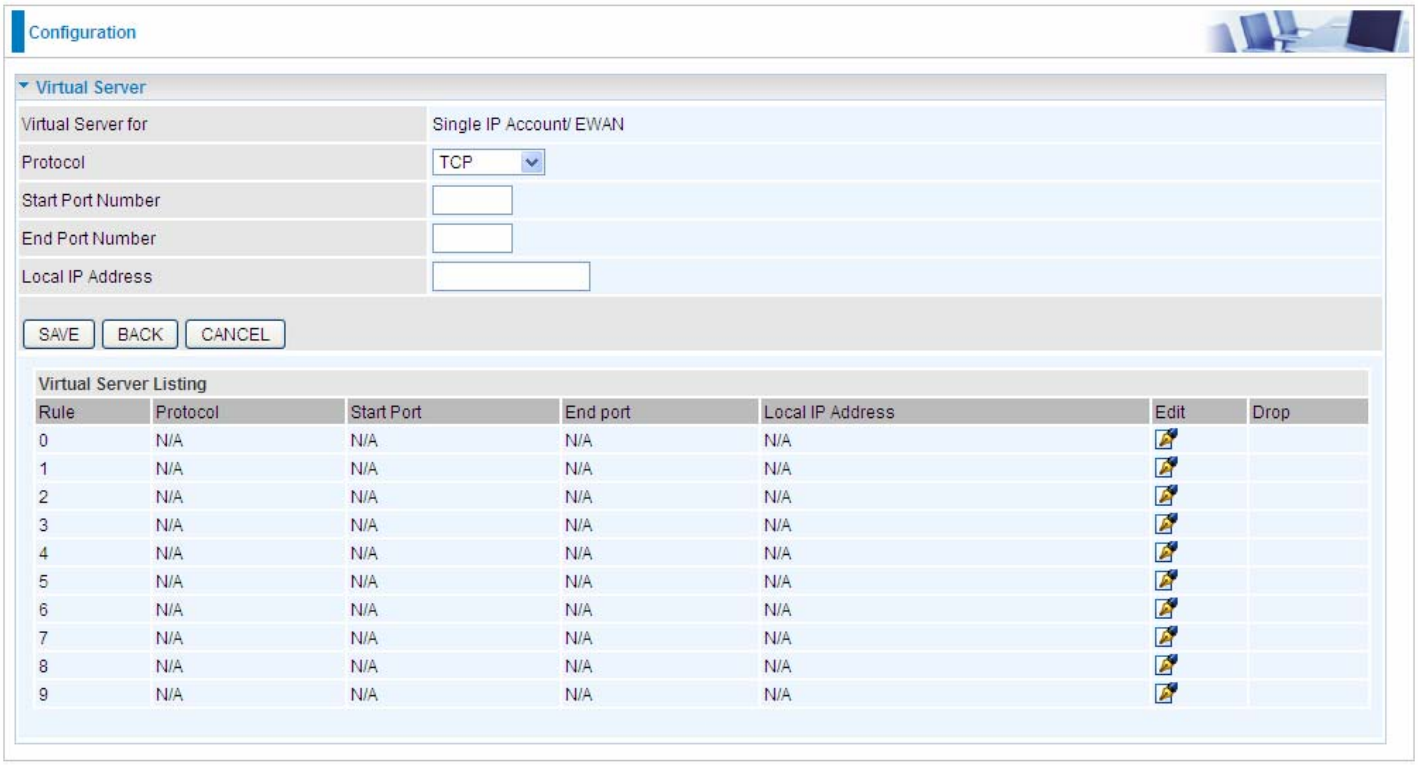
Virtual Server

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.



Virtual Server for: Indicate the related WAN interface which allows outside network to connect in and communicate.

Protocol: Choose the application protocol.

Start Port Number: Enter a port number as the starting number of the range which you want to give access to internal server.

End Port Number: Enter a port number as the end number of the range which you want to give access to internal server..

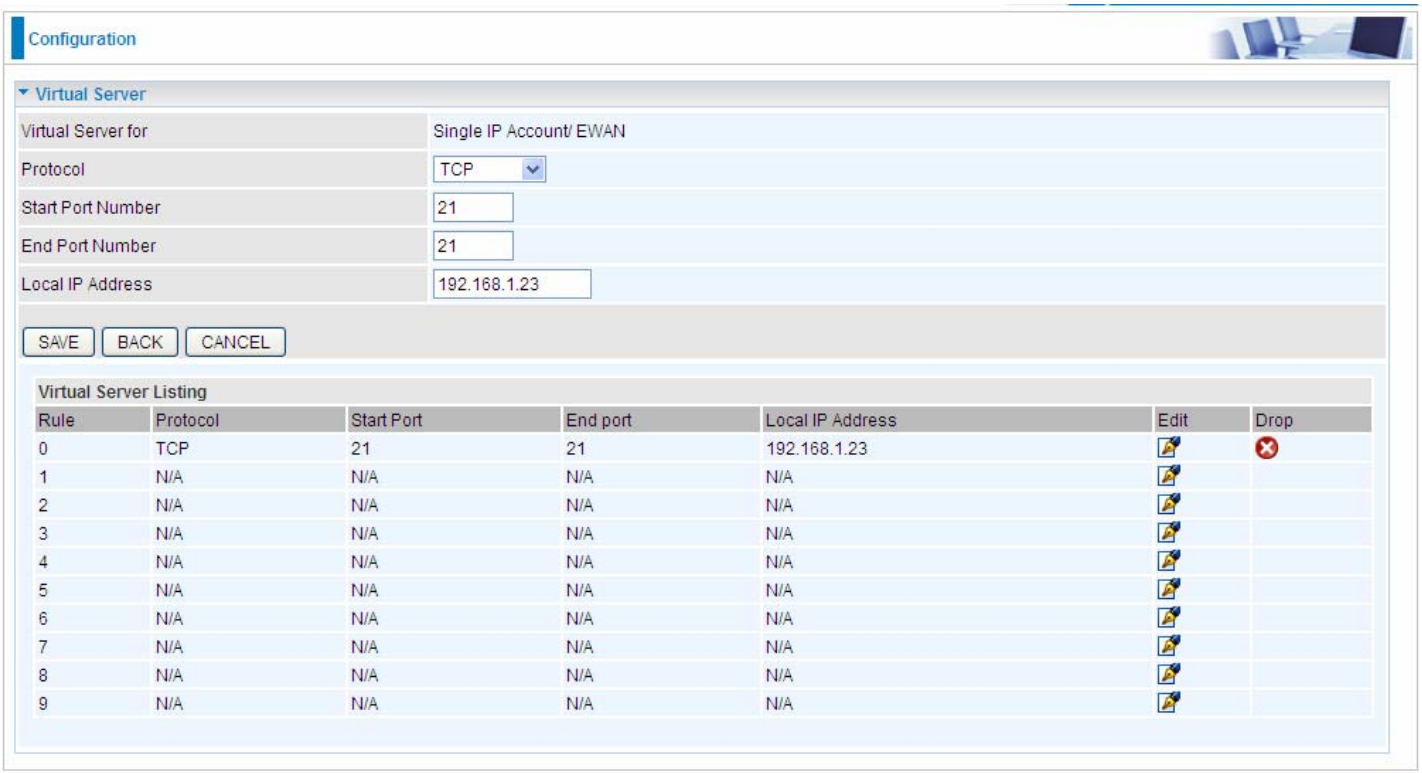
Local IP Address: Enter your server IP address in this field.

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at at: http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

If you have a FTP server in your LAN network, and want to be accessing through WAN, you can have it set as virtual server.



Some tips for using DMZ and Virtual Server:

Using port forwarding does have security implications, as outside users will be 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 using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

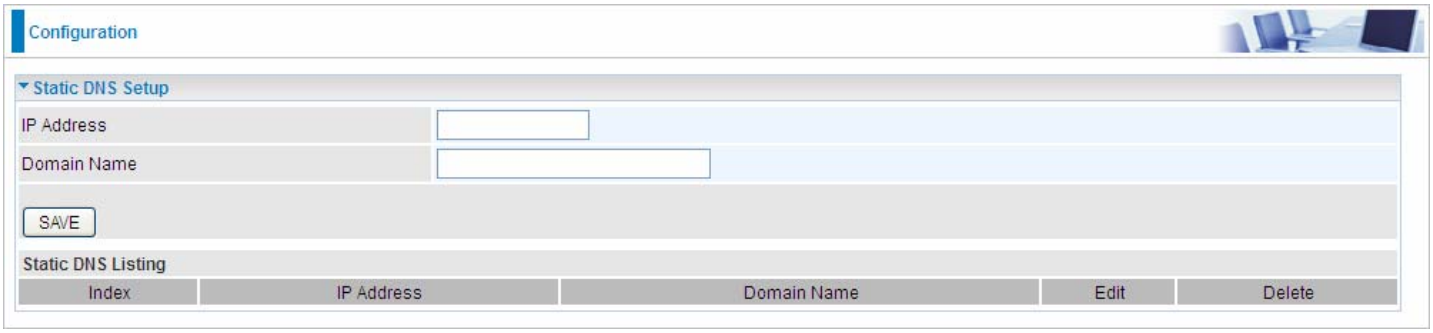
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers 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.

5.6.4 Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).

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



IP Address: The IP address you are going to give a specific domain name.

Domain Name: The friendly domain name for the IP address.

Press **SAVE** button to apply your settings.

5.6.5 ADSL

SRA: Enable to allow seamless rate adaptation.

ADSL Mode: The default setting is **Auto Sync-Up**. This mode will automatically detect your ADSL2+, ADSL2, G.DMT, G.lite and T1.413. But in some area, multimode cannot detect the ADSL2+ line code well. If it is the case, please adjust the ADSL2+ line code to G.DMT or T1.413 first.

ADSLType: There are five modes ”Annex A”, ”Annex I”, “Annex A/L”, ”Annex M” and “Annex A/I/J/L/M” that user can select for this connection.

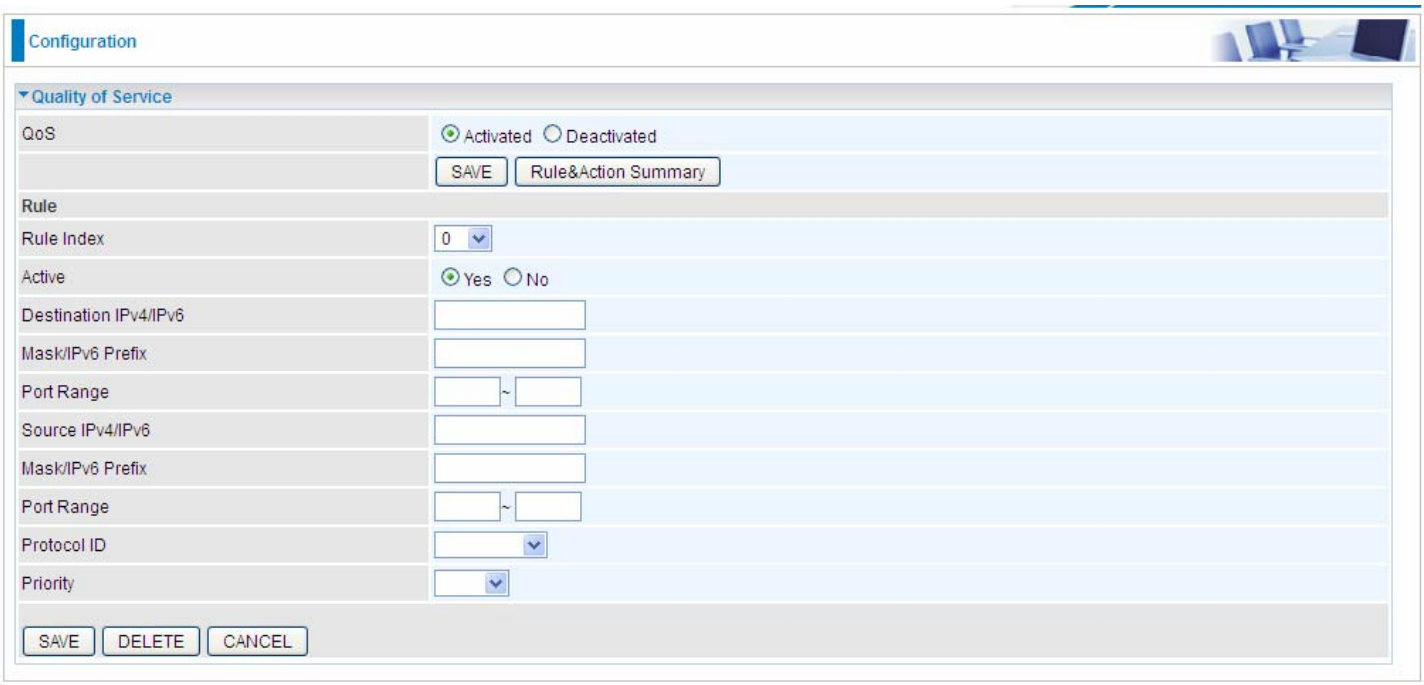
5.6.6 QoS

QoS helps you control the upload traffic of each application from LAN(Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want giver higher priority to, such as voice data packets given higher priority than web data packets.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on **SAVE** to save your changes.

Click on **Rule&Action Summary** to view the list of QoS rules that have been added.



Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: Physical Ports, IP, Port, Protocol, etc, you can modify the value to any new one you wish. Please notice that only when the packet fulfill every detail setting conditions here, then this packet will be remarked as the priority queue of each rule. The non-selected setting part will be treated as “don’t care” and the system will not handle this setting part.

Rule Index: Select 16 different rules, each rule’s detail can be set and saved.

Active: Select whether to activate the rule.

Destination IPv4/IPv6: Set the IPv4/IPv6 address that you want to filter on destination side.

Mask/Prefix: Specify the Mask for IPv4 or prefix for IPv6.

Port Range: Set the port range value that you want to filter on destination side.

Source IPv4/IPv6: Set the IP address value that you want to filter on source side in IPv4 or IPv6.

Mask/Prefix: Specify the Mask for IPv4 or prefix for IPv6.

Port Range: Set the port range value that you want to filter on source side.

Protocol ID: Set the protocol ID type of packets that you want to filter (TCP, UDP, ICMP, IGMP).

Priority: Select to prioritize the traffic which the rule categorizes. High and Low.

5.6.7 Interface Grouping *(7600NXL only)*

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **SAVE** button.

Active: Select Yes to enable Interface Grouping feature.

Group Index: The index number indicating the current goup ranging from 0 to 15.

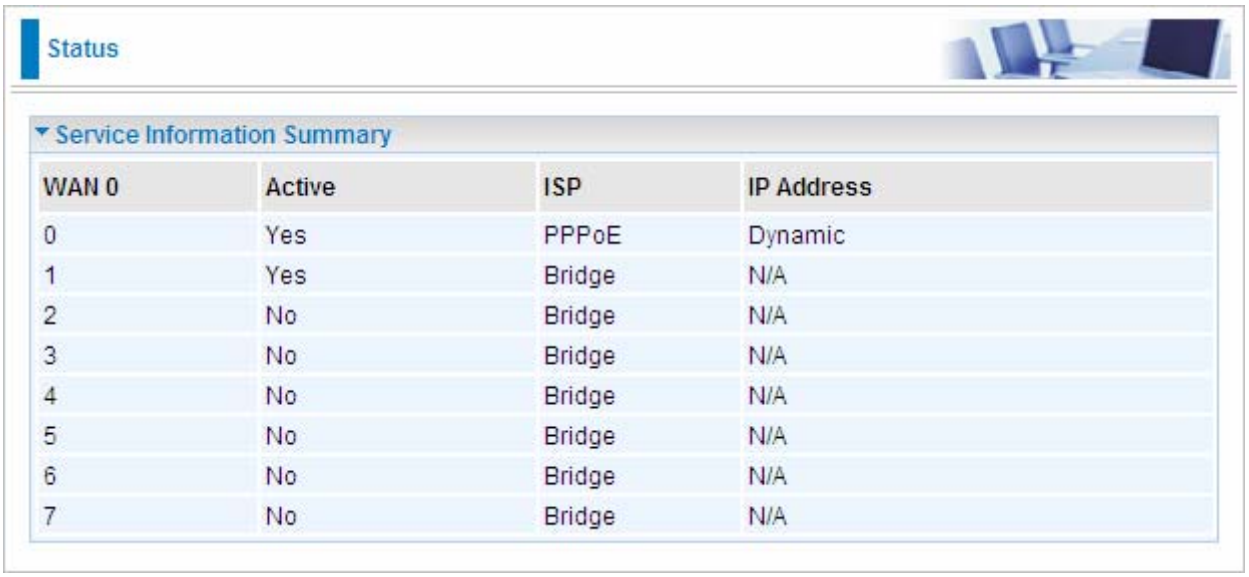
EWAN Service: The available EWAN interface. Move to 5.4.1 Interface Setup to add other EWAN interface.

Ethernet: The available Ethernet ports.

WLan: The available wireless ports.

Group Summary: Press **PortBinding Summary** to check the current group information.

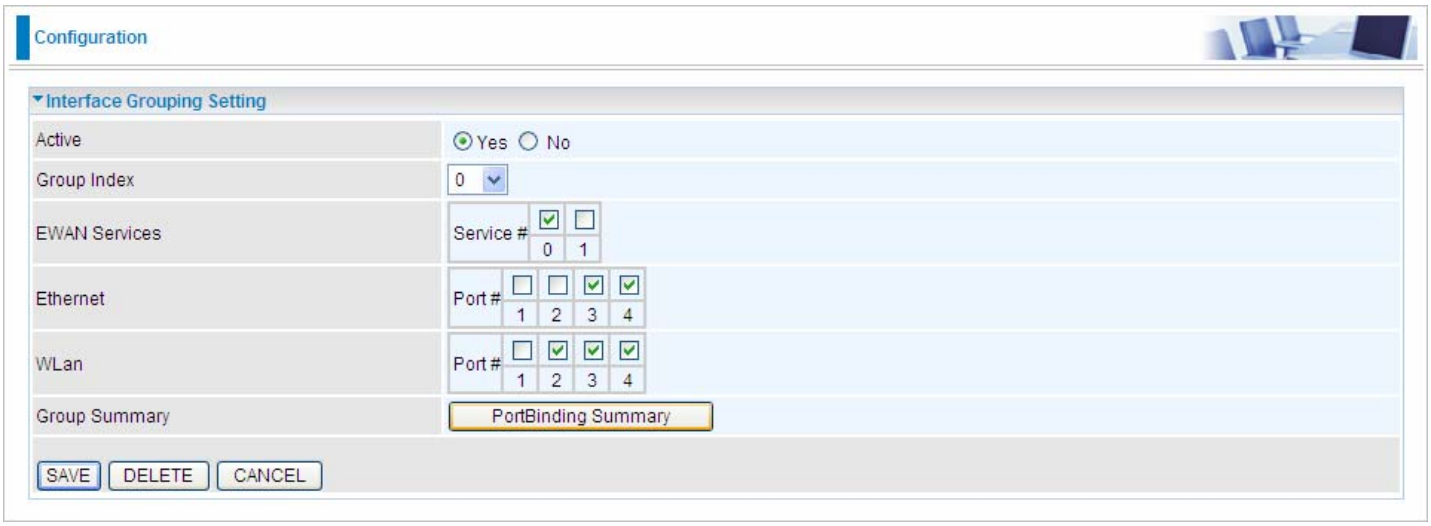
For example, you can create tow EWAN services, Service0(PPPoE) and Service1(Bridge).

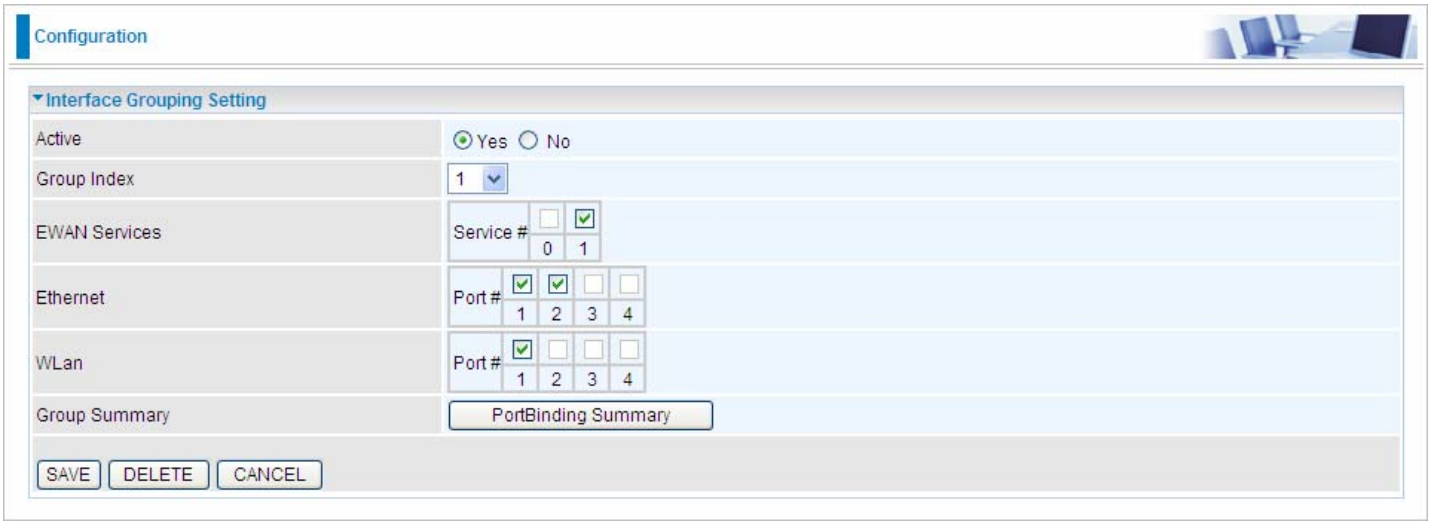


WAN 0	Active	ISP	IP Address
0	Yes	PPPoE	Dynamic
1	Yes	Bridge	N/A
2	No	Bridge	N/A
3	No	Bridge	N/A
4	No	Bridge	N/A
5	No	Bridge	N/A
6	No	Bridge	N/A
7	No	Bridge	N/A

You are going to group the ports and services into two working group, as shown below.

Group Index	Group Port
0	ewan0_0,e3,e4,w2,w3,w4
1	ewan0_1,e1,e2,w1





Click **PortBinding Summary** to show the configuration results.

Group ID	Group port
0	wan0_0,e3,e4,w2,w3,w4
1	wan0_1,e1,e2,w1

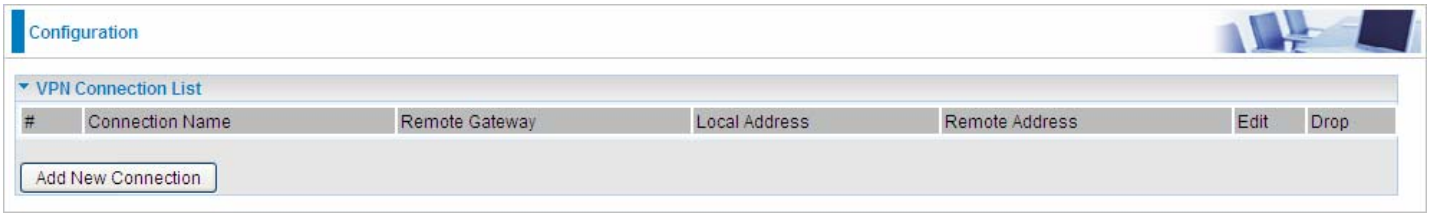
5.6.7 IPSEC Setting *(7600NX only)*

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

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*).

A total of **8** IPSec tunnels can be added.



Click **Add New Connection** to create IPSec connections.

Configuration

VPN Connection Setting

Active	Yes No				
Connection Name		Interface	EWAN		
Remote Gateway IP	(0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
Remote Access Range	Subnet	Remote IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
IKE Mode	Main	Pre-Shared Key			
Local ID Type	Default Wan IP	IDContent			
Remote ID Type	Default Wan IP	IDContent			
Encryption Algorithm	DES	Authentication Algorithm	MD5	Diffie-Hellman Group	MODP1024(HD2)
IPSec Proposal	ESP	AH			
	Authentication Algorithm	MD5	Encryption Algorithm	DES	
Perfect Forward Secrecy	None				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				
Note * : (0-3600, 0 means NEVER)					

SAVE BACK

VPN Connection Setting

Active: Select **Yes** to activate the tunnel.

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

Interface: Select the set used interface for the IPSec connection, when you select EWAN interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

Remote Gateway IP: The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.

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

- **Single IP:** 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*)

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

- **Single IP:** 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.

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations(SA). Select Main or Aggressive mode.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

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

IDContent: Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses

(IPv4 and IPv6 supported).

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

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

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). 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.

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

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

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

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

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

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

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

- **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
- **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keep Alive:

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

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is

required. Default setting is 0.0.0.0 which disables the function

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

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

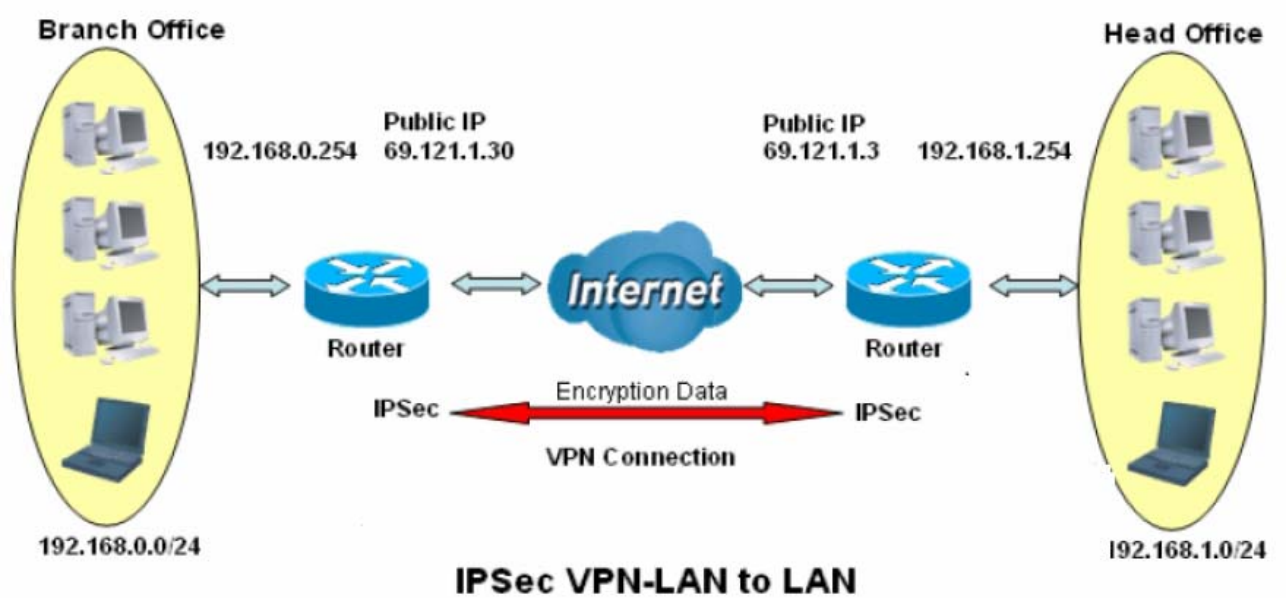
Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. 180 seconds is minimum time interval for this function.

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

Click **SAVE** to submit the settings.

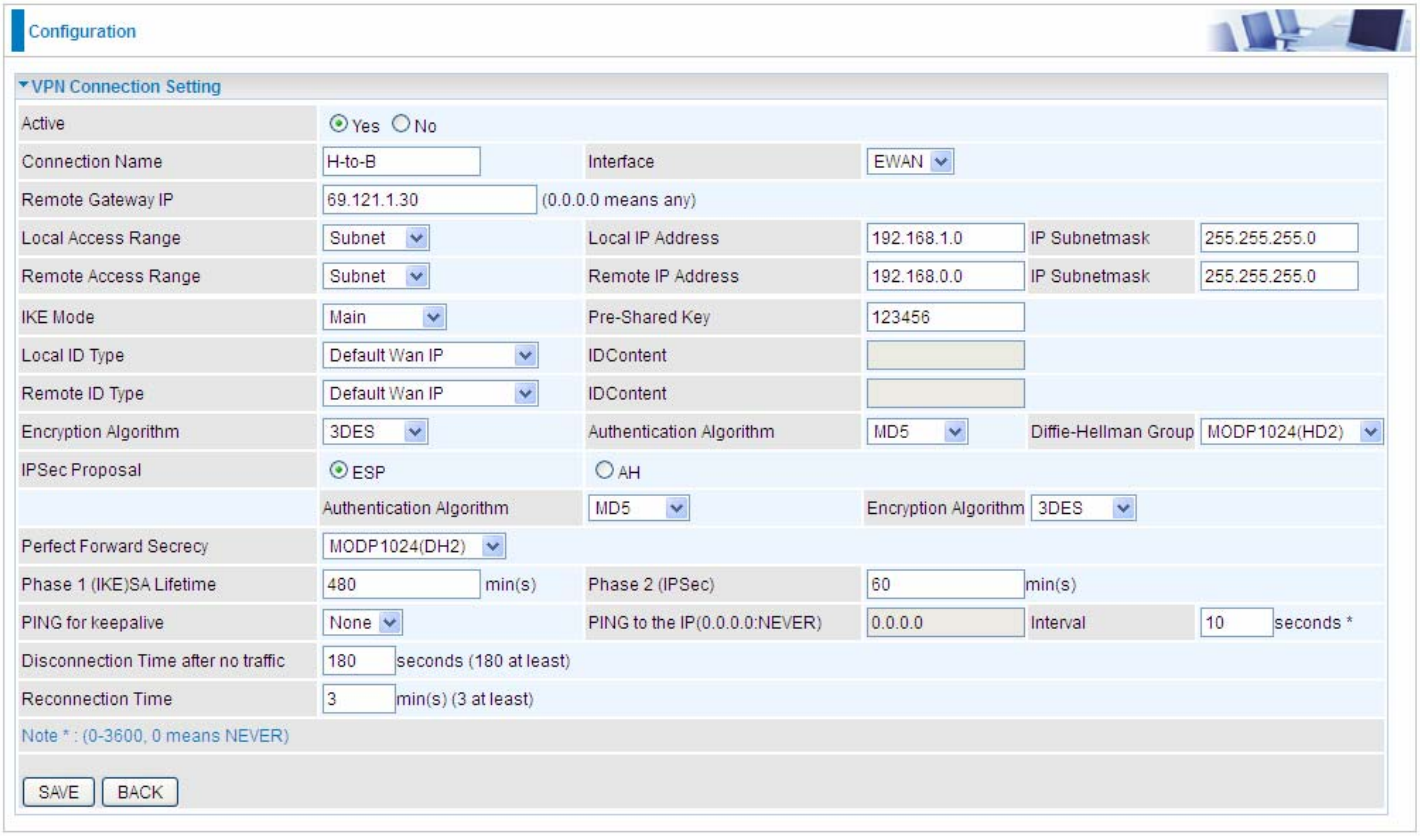
Examples:

1. **LAN-to-LAN connection**
Two BiPAC 7600NXs want to setup a secure IPSec VPN tunnel
Note: The IPSec Settings shall be consistent between the two routers.



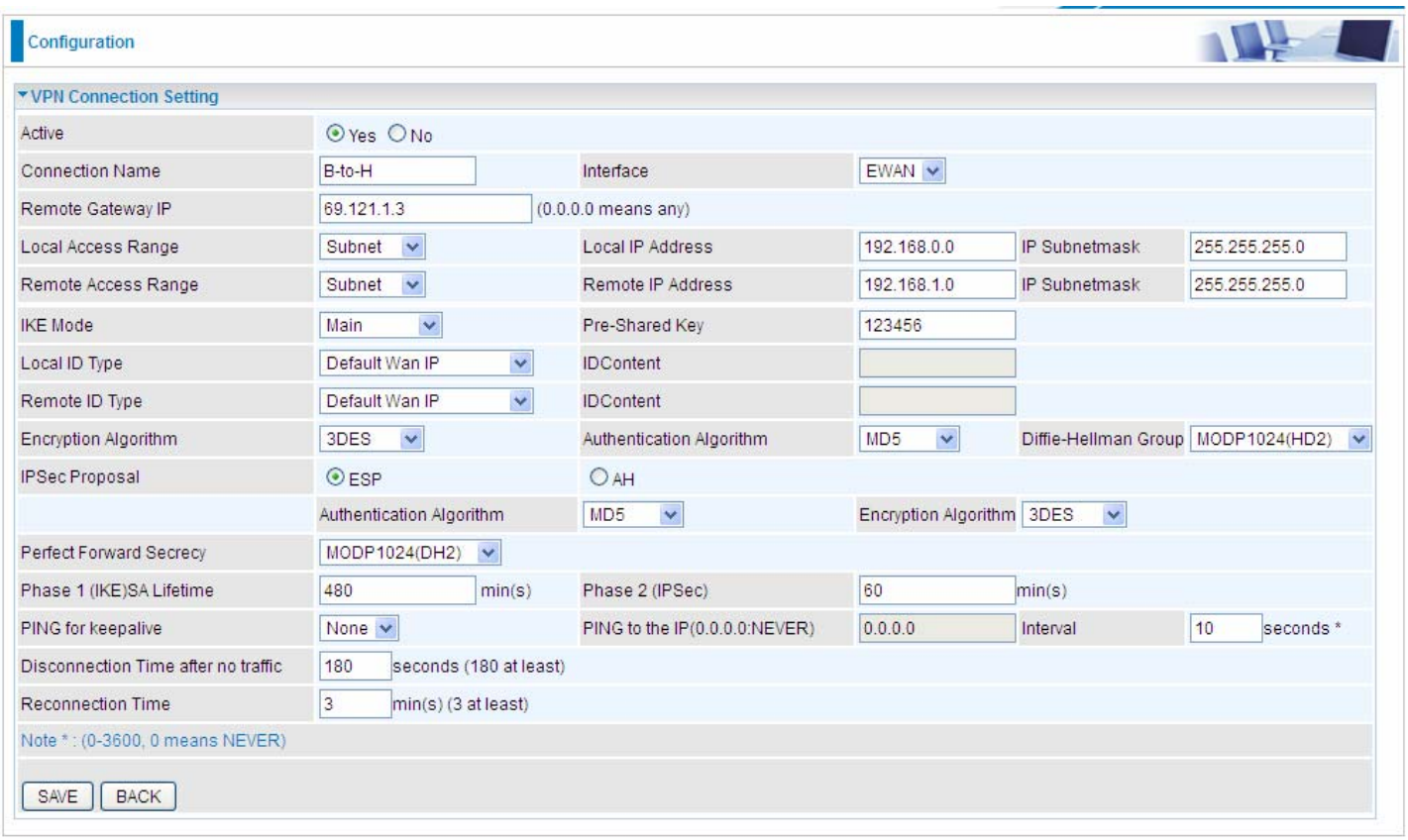
Head Office Side:
Setup details:

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	



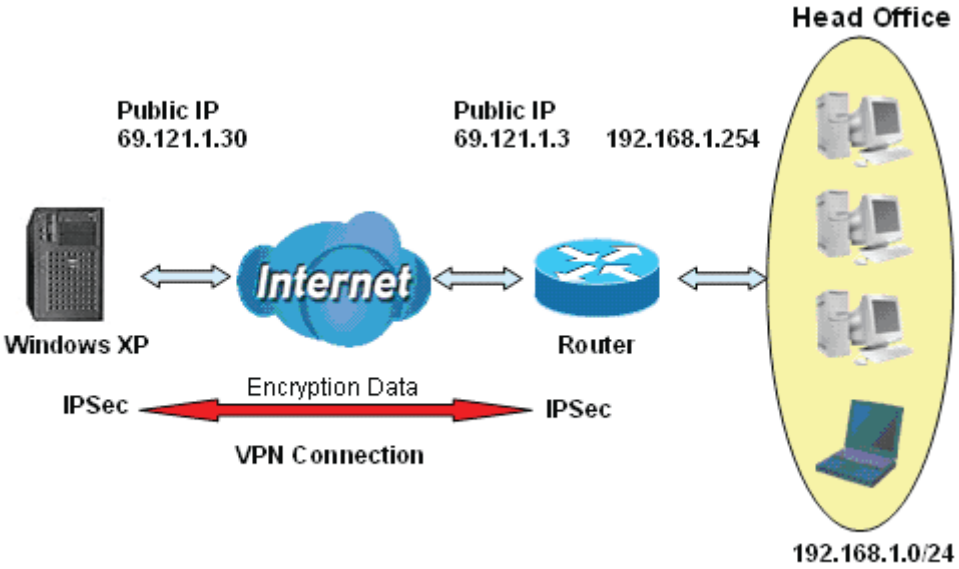
Branch Office Side:
Setup details: the same operation as done in Head Office side

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	



2. **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	Host-to-Headoff	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	

Configuration

VPN Connection Setting

Active	⦿ Yes ○ No				
Connection Name	Host-to-Headoff	Interface	EWAN		
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
Remote Access Range	Single IP	Remote IP Address	69.121.1.30	IP Subnetmask	255.255.255.255
IKE Mode	Main	Pre-Shared Key	123456		
Local ID Type	Default Wan IP	IDContent			
Remote ID Type	Default Wan IP	IDContent			
Encryption Algorithm	3DES	Authentication Algorithm	MD5	Diffie-Hellman Group	MODP1024(HD2)
IPSec Proposal	⦿ ESP	○ AH			
	Authentication Algorithm	MD5	Encryption Algorithm	3DES	
Perfect Forward Secrecy	MODP1024(DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : (0-3600, 0 means NEVER)

SAVE BACK

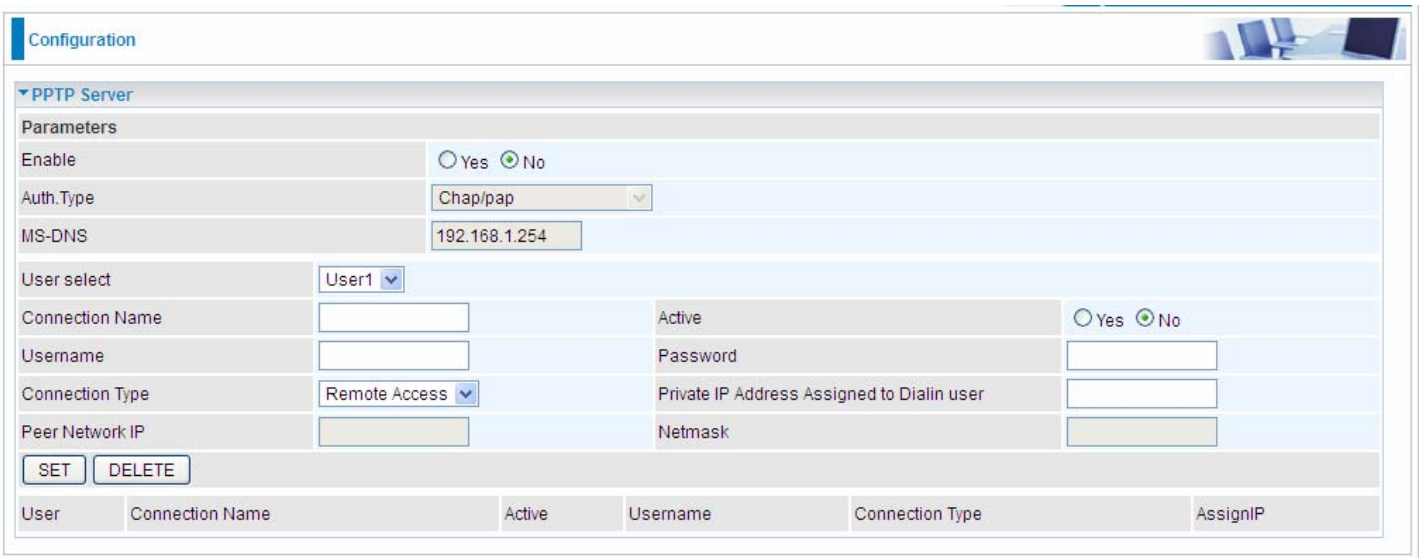
5.6.8 PPTP *(7600NX only)*

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, and Microsoft CHAP V1/V2 . The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2.

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

In PPTP session, users can set the basaic parameters(authentication, encyption, peer address, etc) for PPTP Server and then set the accounts, and 4 accounts or connections are to be set for PPTP Server.



Enable: Select **Yes** to activate PPTP Server. **No** to deactivate PPTP Server.

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, and MPPE 128bit Encryption. 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.

MS-DNS: Directly set the IP of DNS server or let the 192.168.1.254(the router by default) be the MS-DNS server.

User select: 4 sessions for server by default, user1 stands for the first session, and so does user2, etc.

Connection Name: User-defined name for the PPTP connection.

Active: Select **Enable** to activate the account. PPTP 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.

Private IP Address Assigned to Dialin user: Specify the private IP address to be assigned to dialin clients,

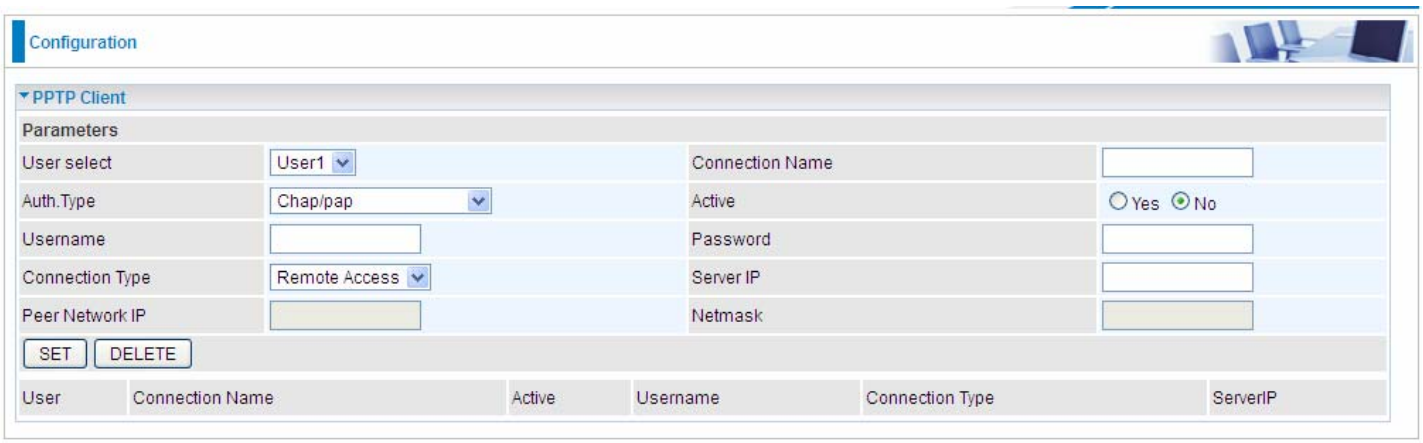
and the IP should be in the same subnet as local LAN, but not occupied.

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

Peer Netmask: Please input the Netmask for remote network.

5.6.9 PPTP Client *(7600NX only)*

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet. A total of 4 sessions can be created for PPTP client.



User select: 4 sessions for client connection by default, user1 stands for the first session, and so does user2, etc.

Connection Name: user-defined name for identification.

Auth. Type: The authentication type, Pap or Chap, and MPPE 128bit Encryption. 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. Set the same authentication type as set in the server side.

Active: Select **Yes** to enable the connection to the VPN server.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

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

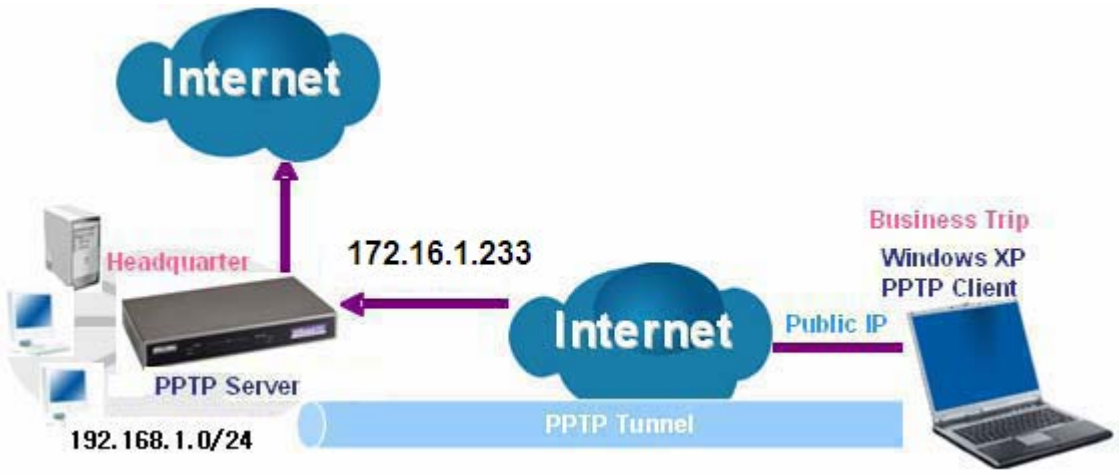
PPTP Server Address: Enter the WAN IP address of the PPTP server.

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

Peer Netmask: Please input the Netmask for server peer.

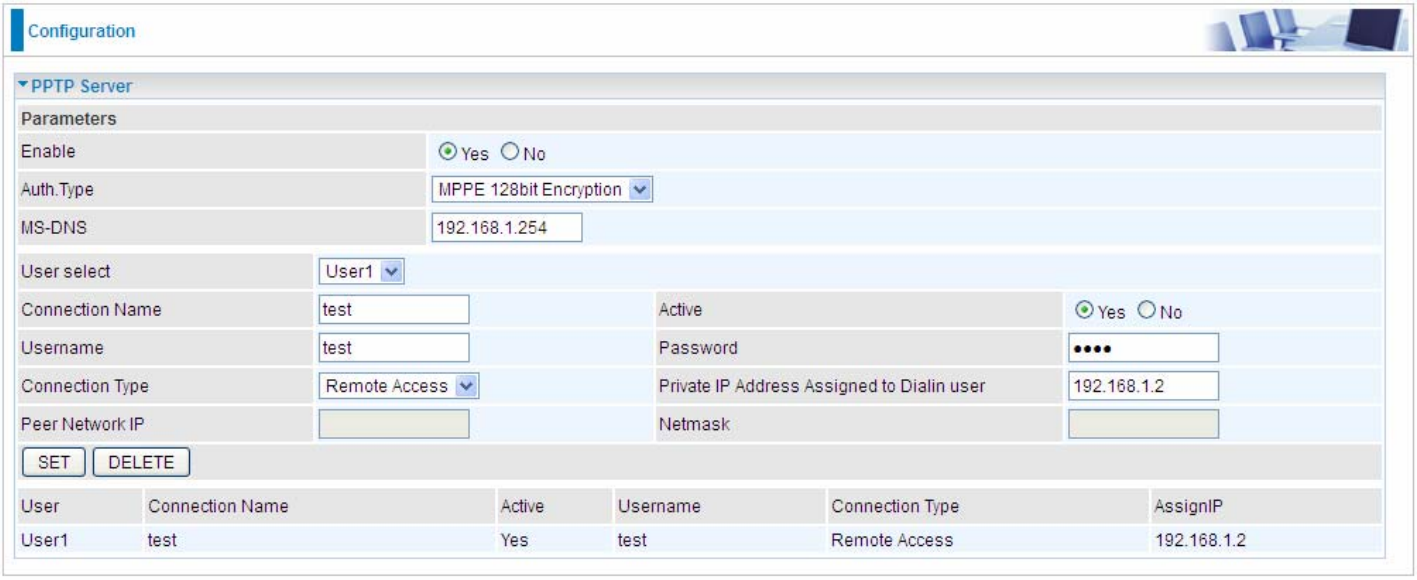
Click **SET** button to save your changes.

Example: PPTP Remote Access with Windows7
(Note: inside test with 172.16.1.233, just an example for illustration)



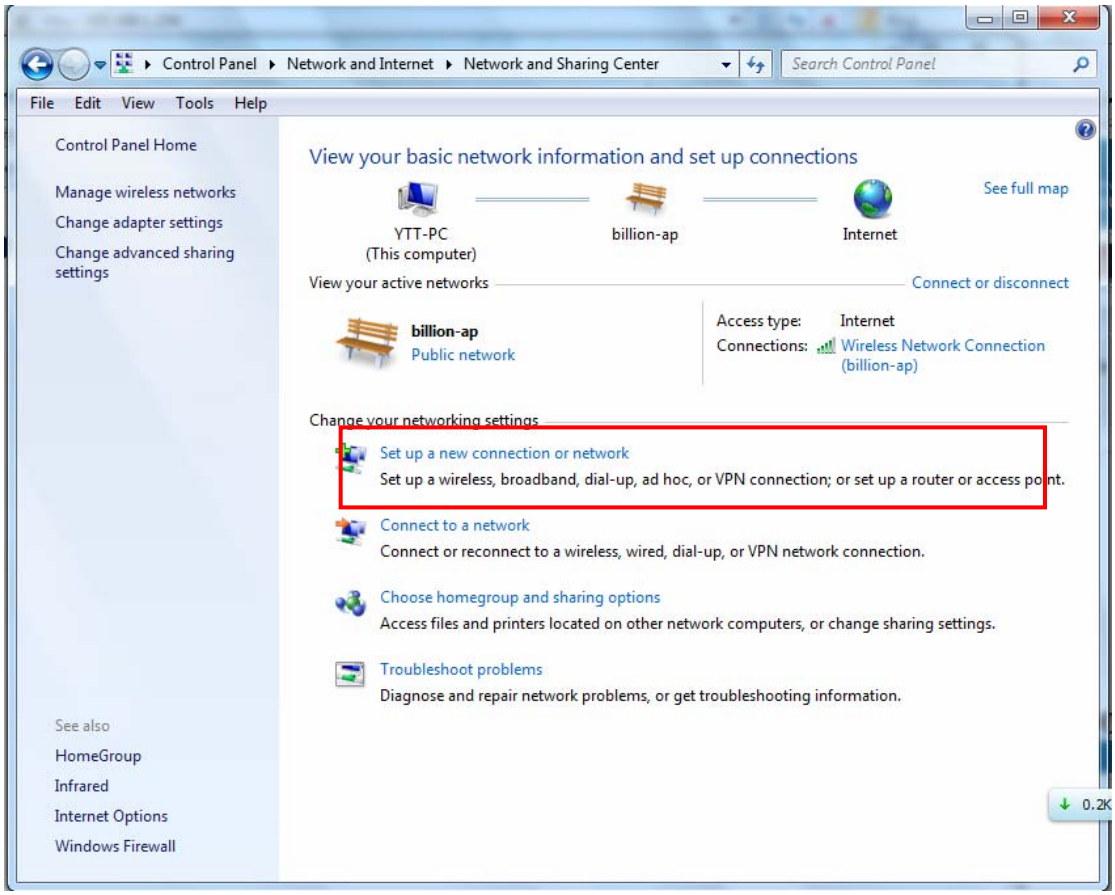
Server Side:

1. Please move to **Configuration** > **PPTP Server**, Enable the PPTP Server and add an account as "test". The exact setting can be found in the screenshot shown below.

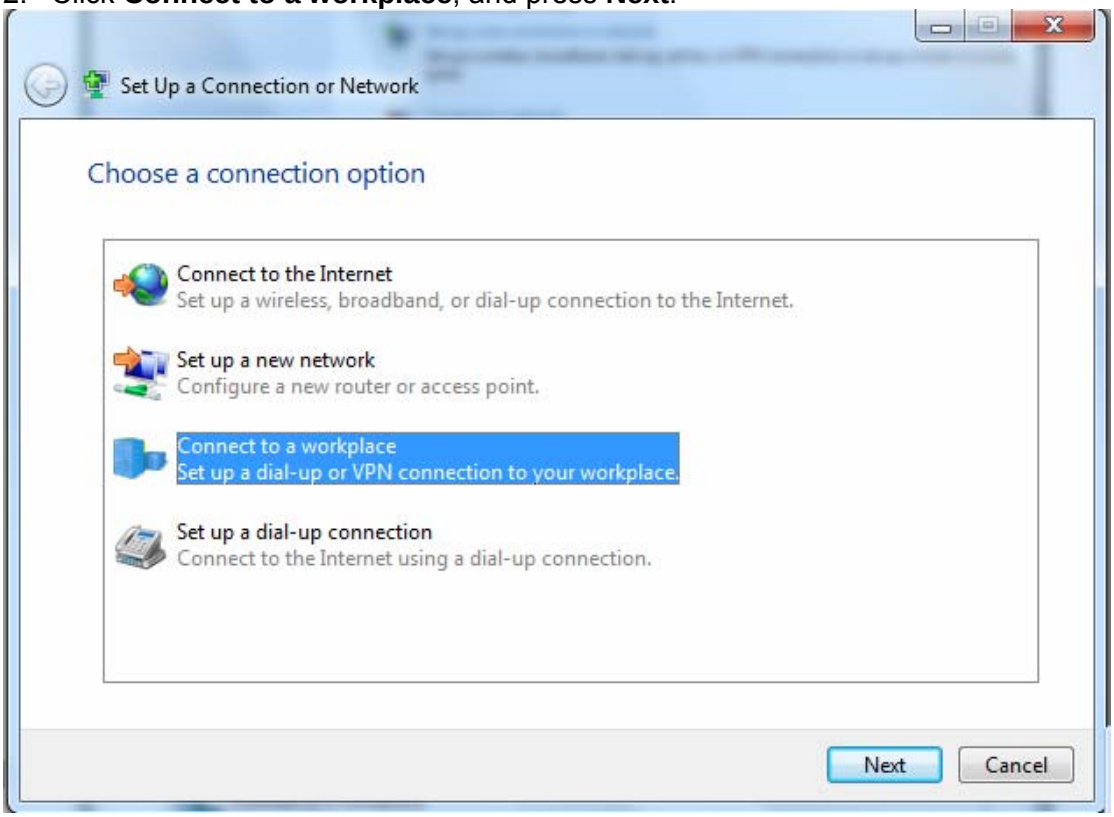


Client Side:

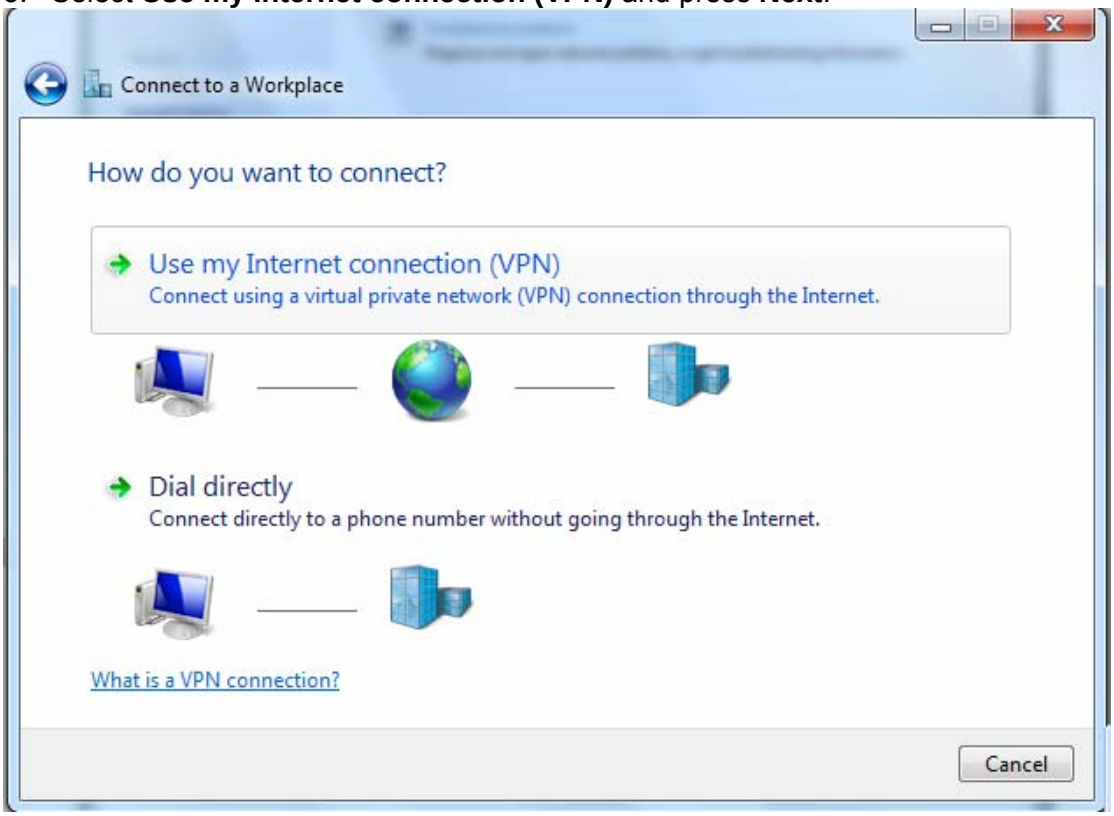
1. In Windows7 click **Start** > **Control Panel**> **Network and Sharing Center,** Click **Set up a new connection or network**.



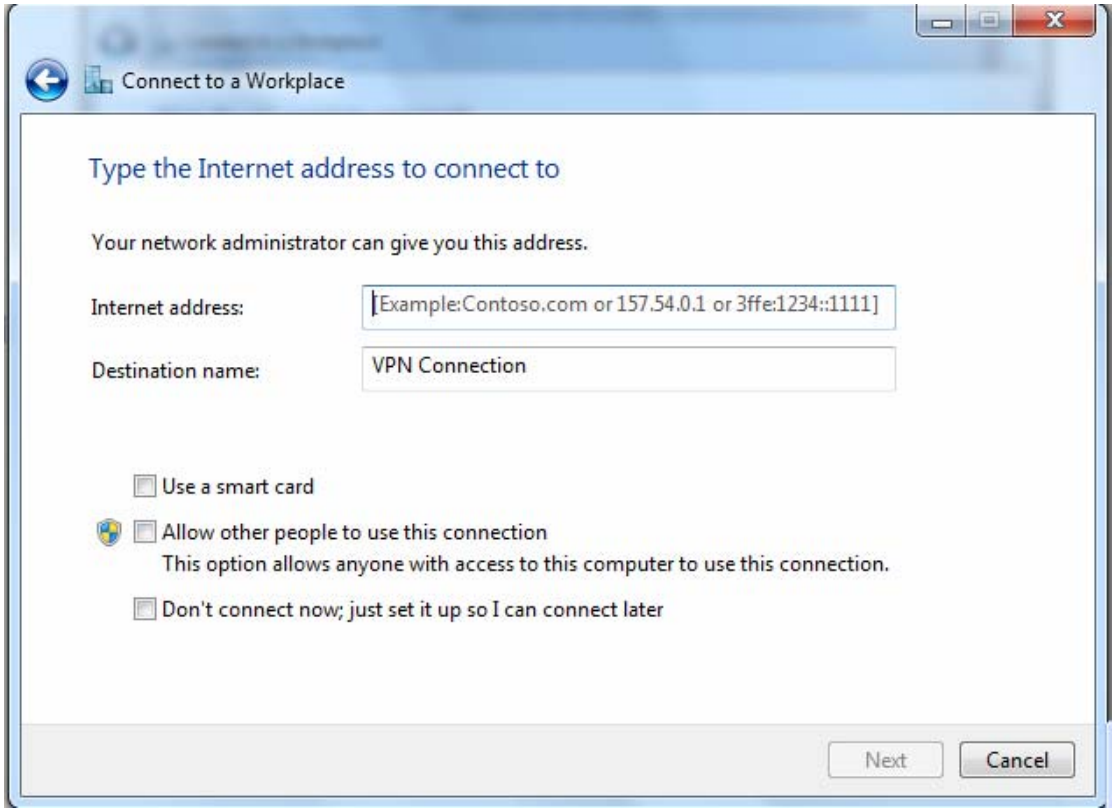
2. Click **Connect to a workplace**, and press **Next**.

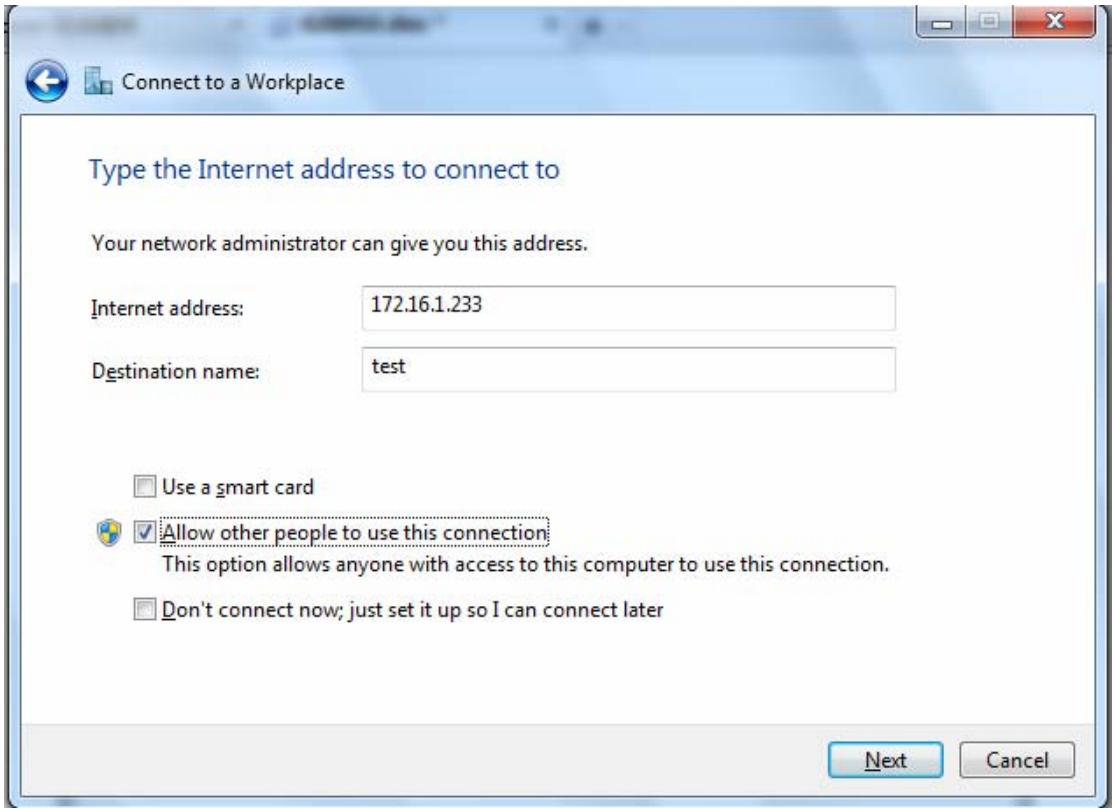


3. Select **Use my Internet connection (VPN)** and press **Next**.

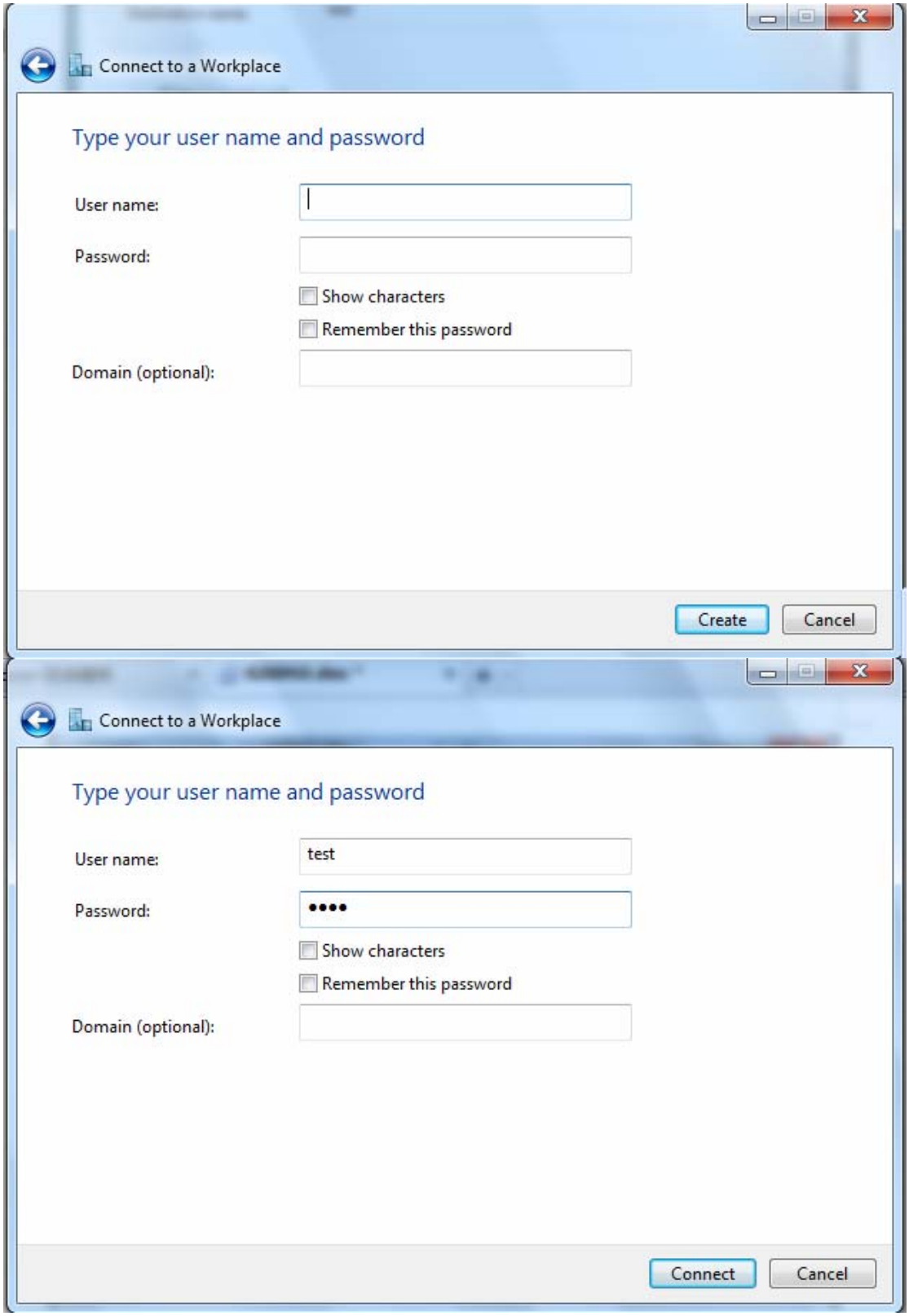


4. Input **Internet address** and **Destination name** for this connection and press **Next**.

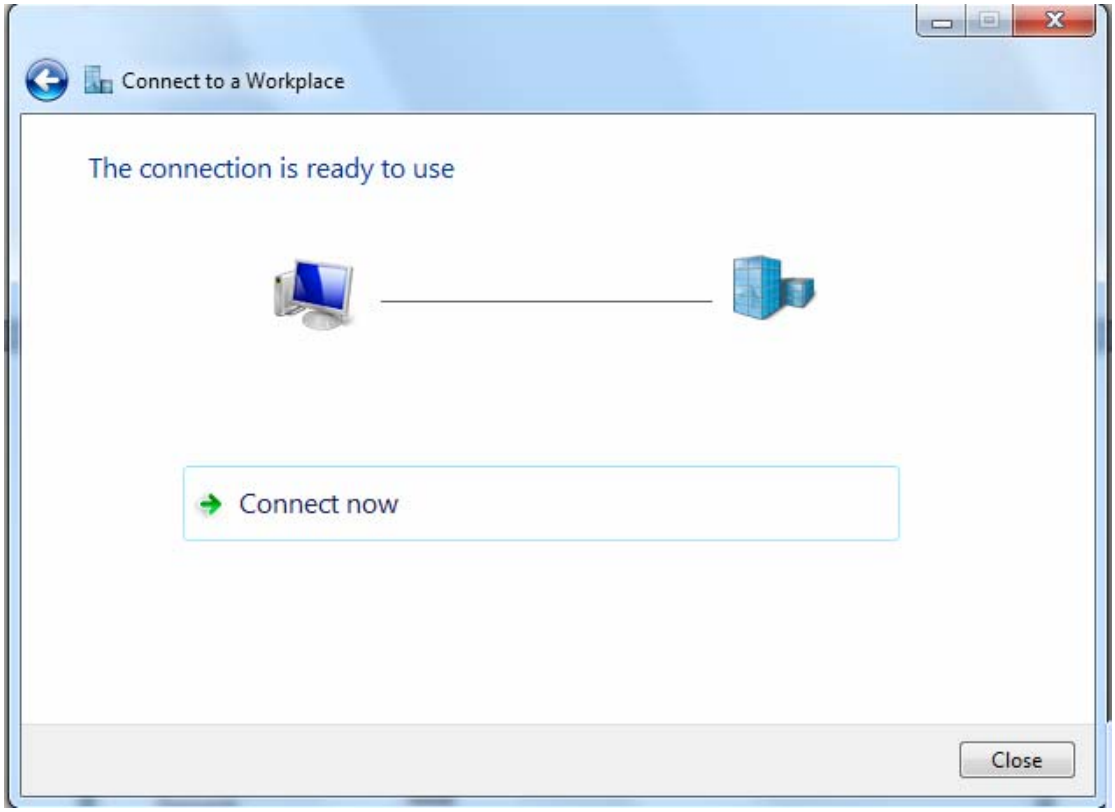


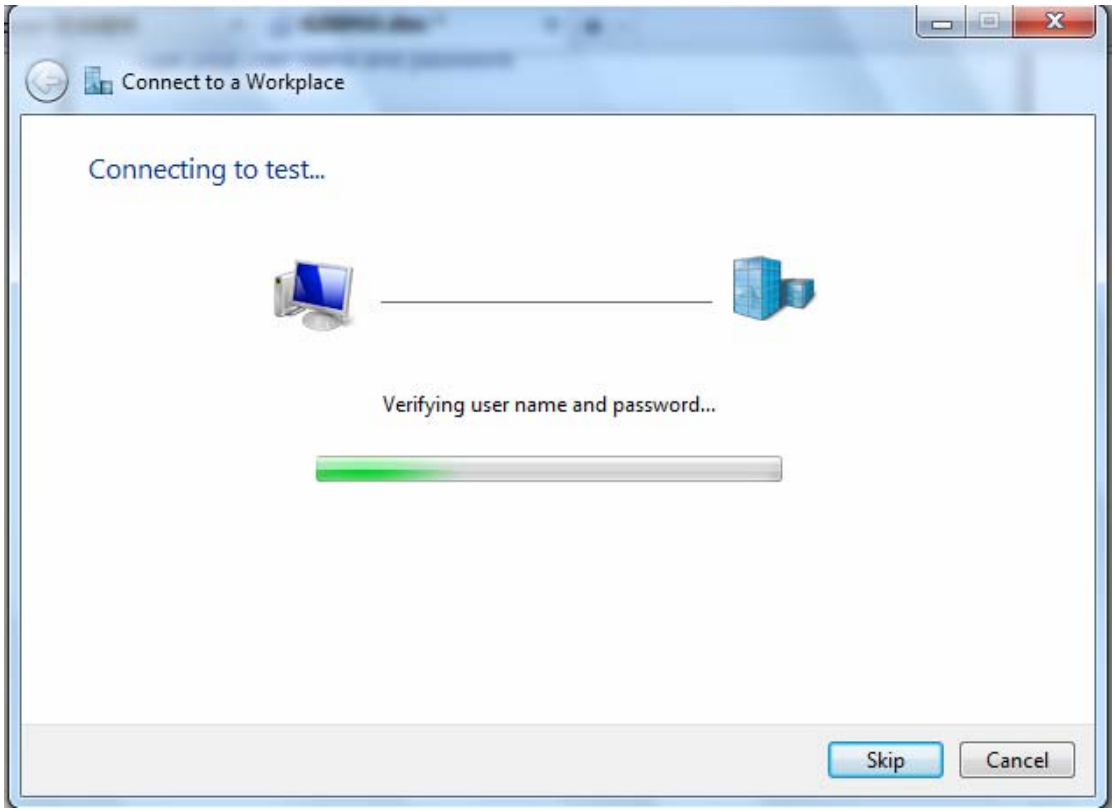


5. Input the account (**user name** and **password**) and press **Create**.

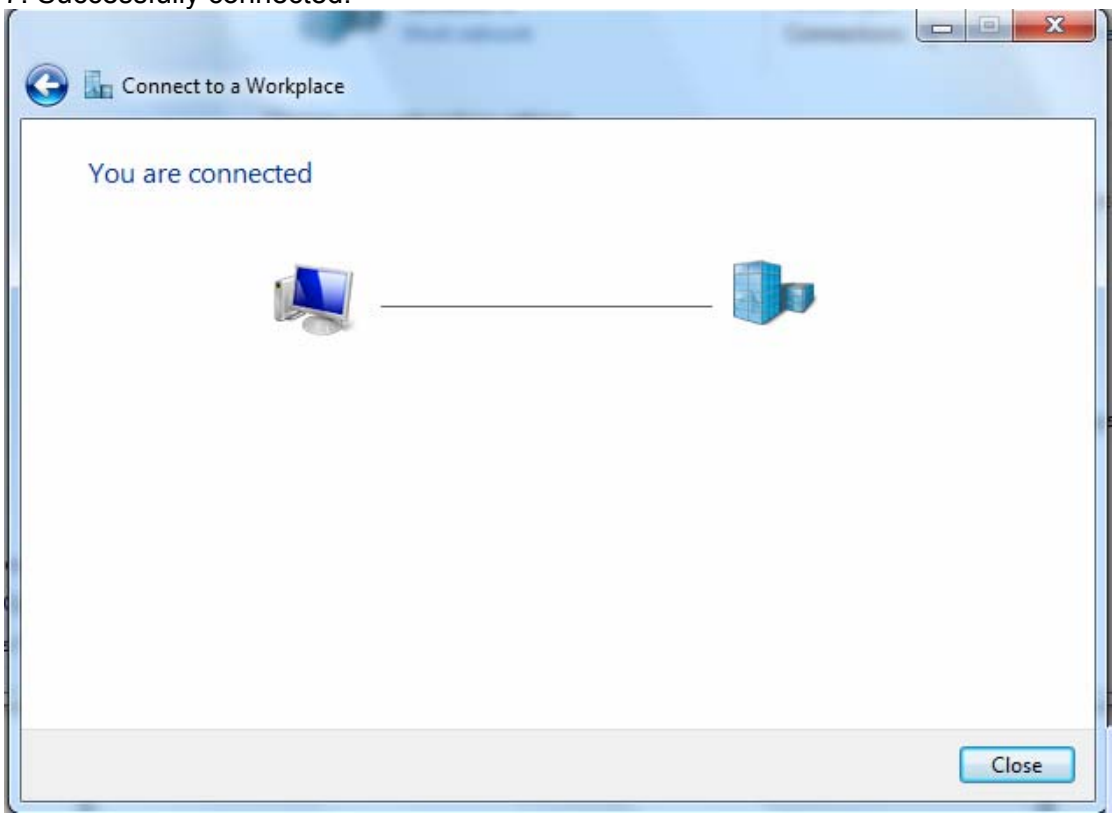


6. Connect to the server.

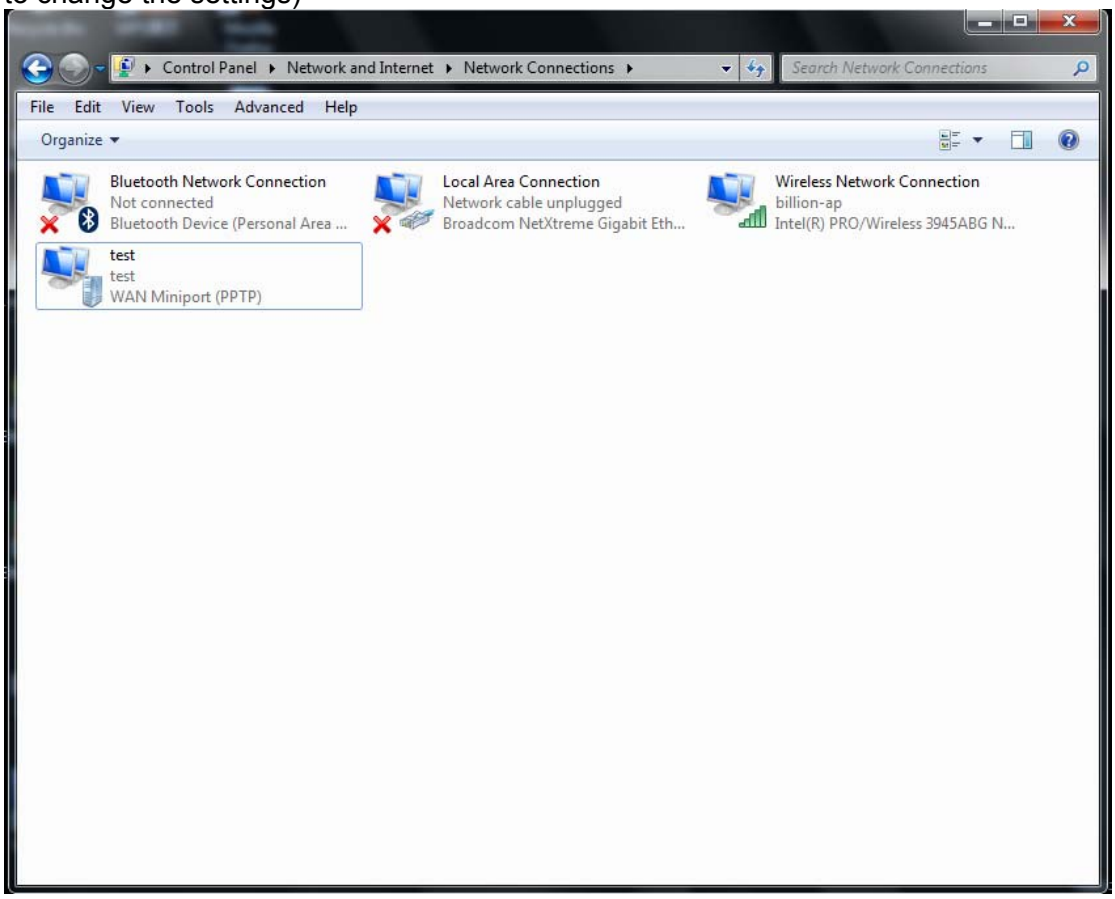


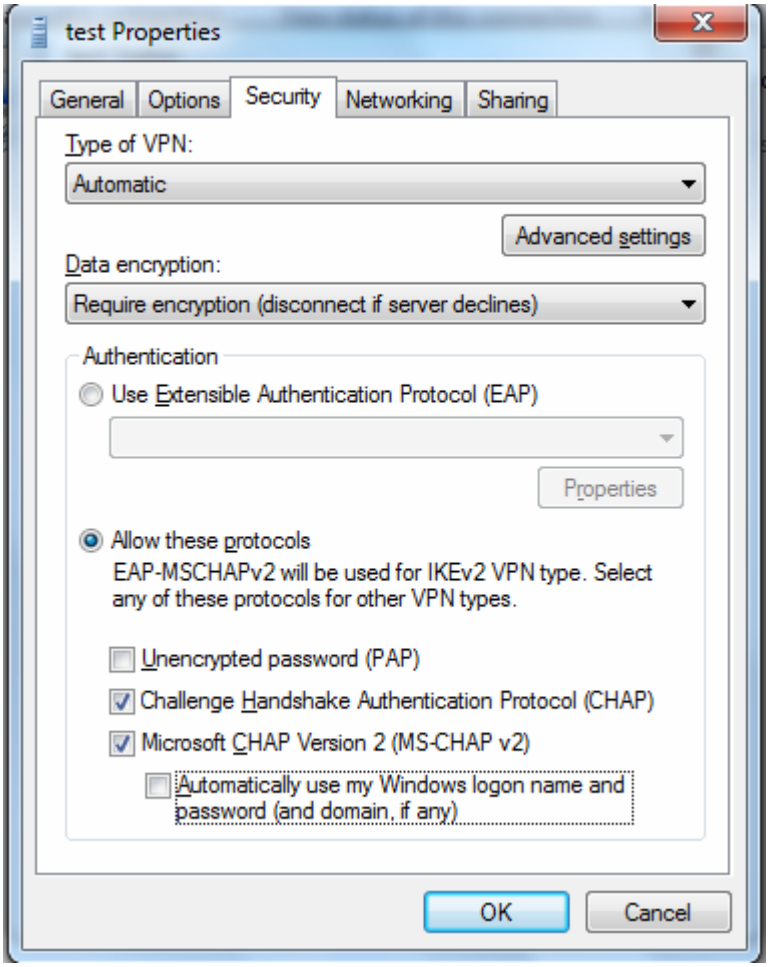


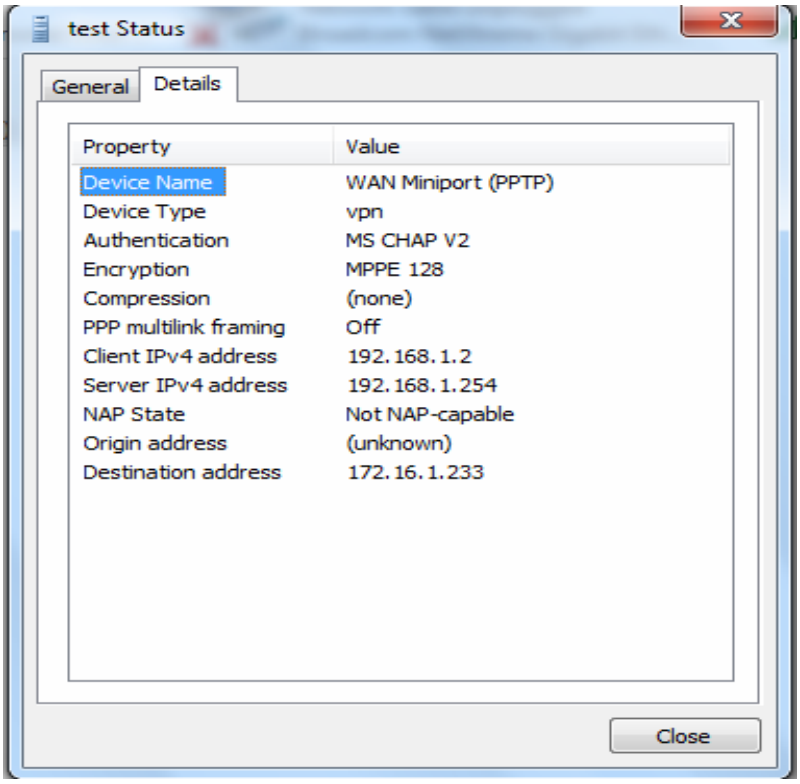
7. Successfully connected.



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)



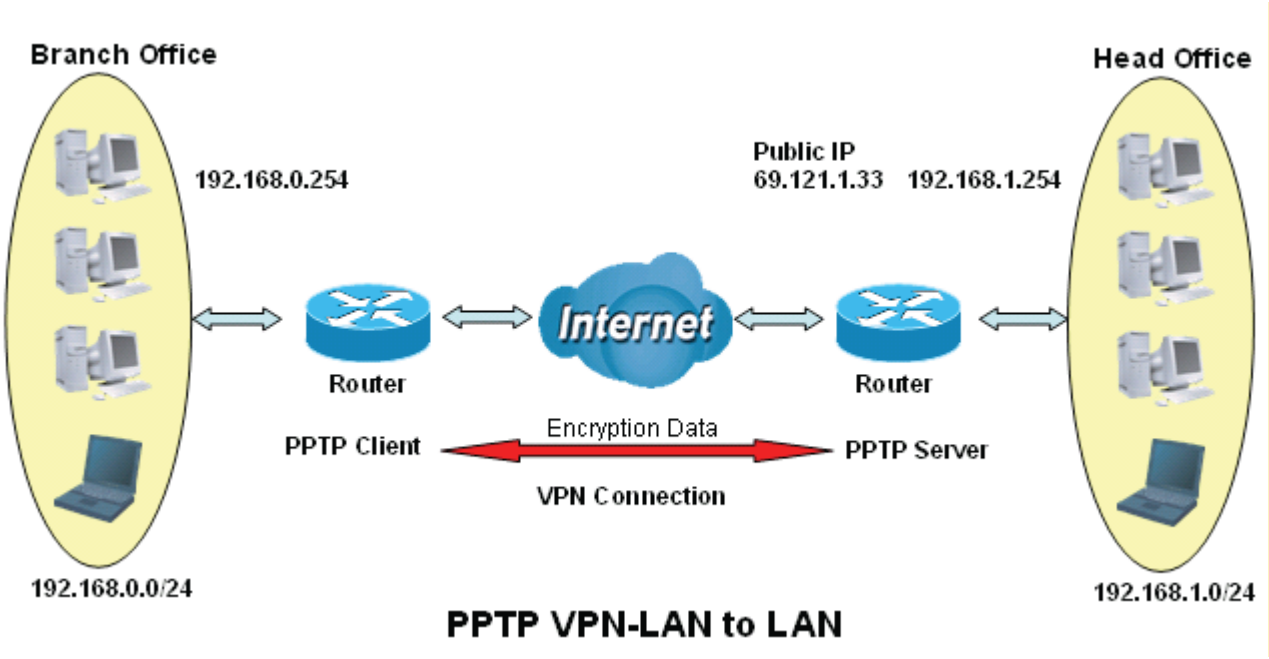

test Properties
General
Options
Security
Networking
Sharing
Type of VPN:
Automatic
Advanced settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Allow these protocols
EAP-MSCHAPv2 will be used for IKEv2 VPN 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
192.168.1.2
Server IPv4 address
192.168.1.254
NAP State
Not NAP-capable
Origin address
(unknown)
Destination address
172.16.1.233
Close

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

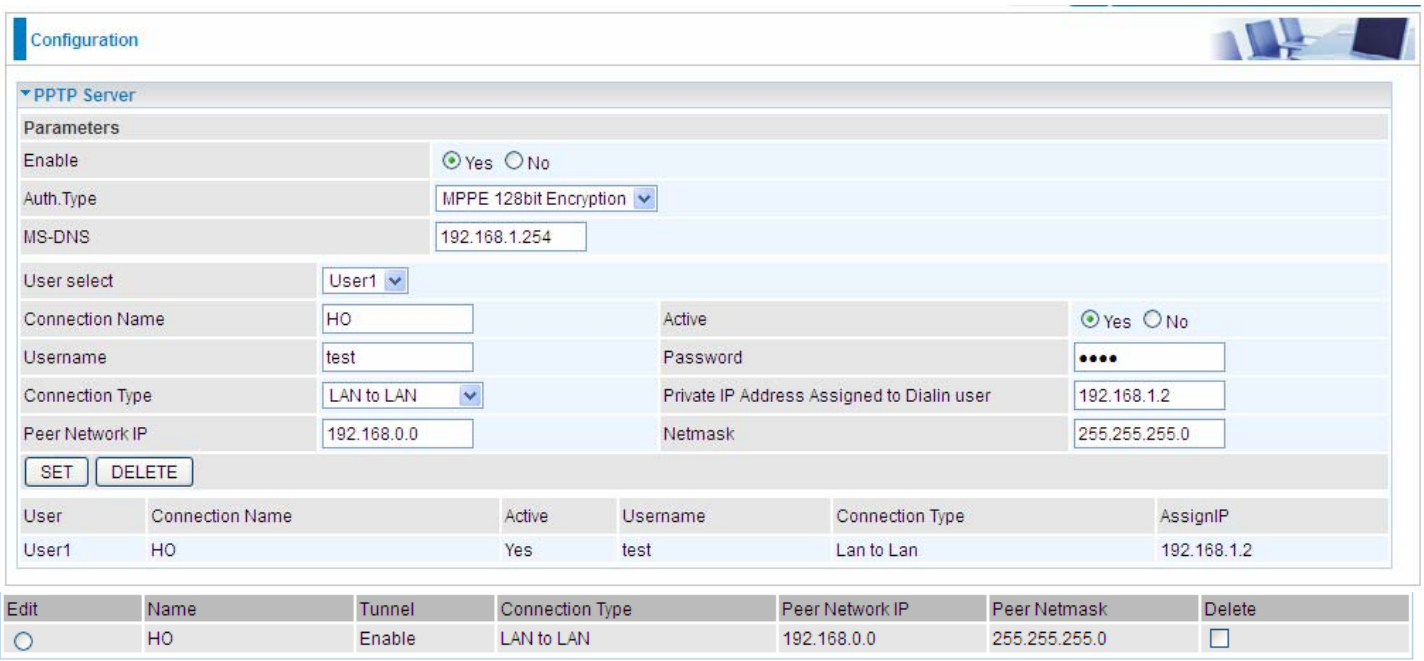
The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.

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



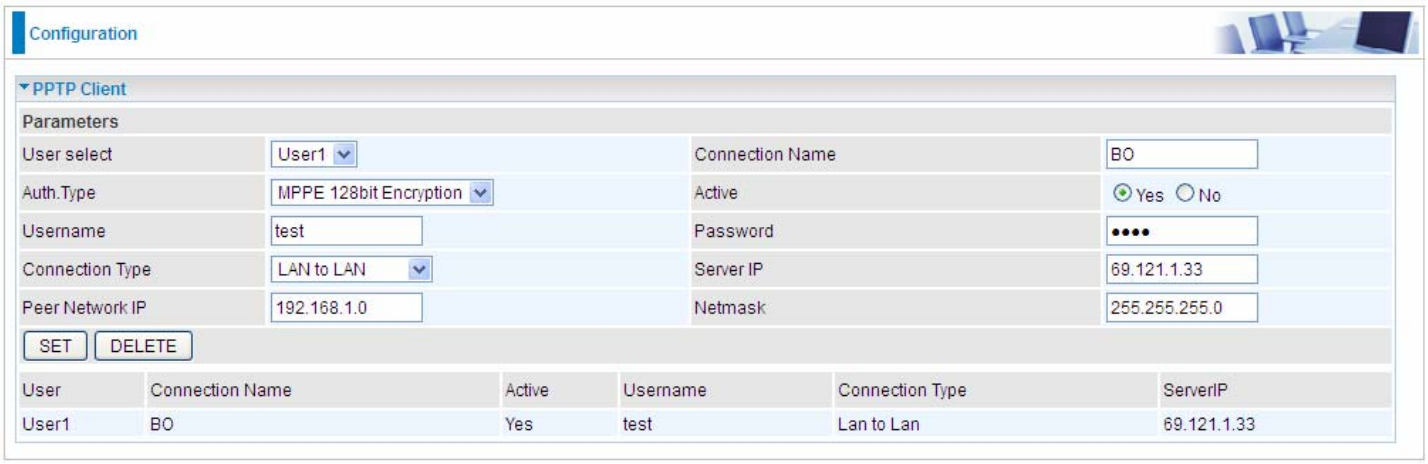
Server side: Head Office

Set an account of "test" in PPTP server waiting to connect in from PPTP client (192.168.0.0/24). The exact authentication type and other parameters are shown below.



Client Side: Branch Office

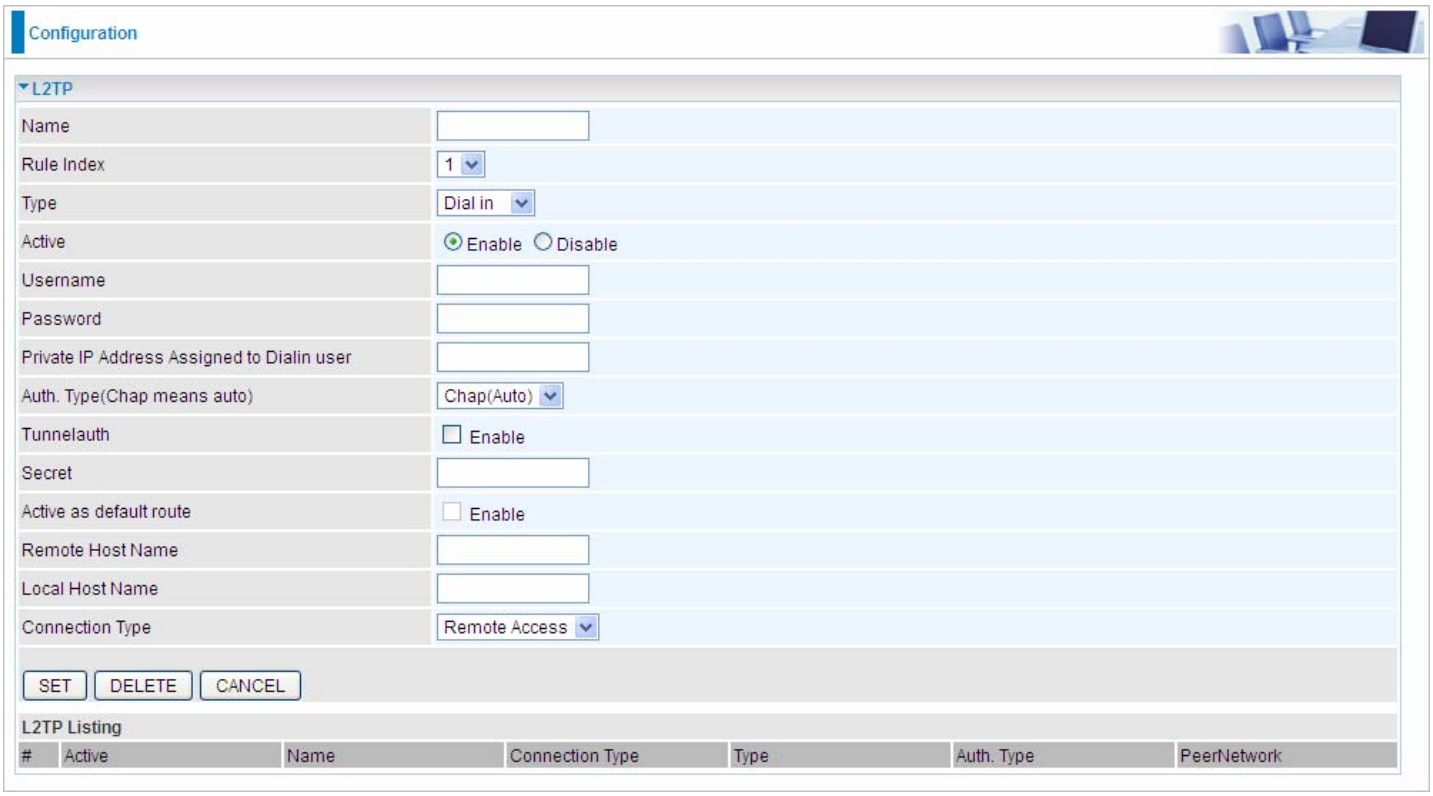
The client user can set up a session connecting to the PPTP server.



5.6.10 L2TP *(7600NX only)*

L2TP, Layer 2 Tunneling Protocol is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide.

Note: 4 sessions for dial-in connections and 4 sessions for dial-out connections



Name: User-defined name for the connection.

Rule Index: The Index to mark the session.

Type: Select Dial Out if you want your router to operate as a client (connecting to a remote VPN Server, e.g, your office server), while choose Dial In to operate as a VPN server.

Active: To enable or disable the tunnel.

Username: Set a username for the client to connect in.

Password: Set the password for the username.

Private IP Address Assigned to Dialin user: The private IP to be assigned to dialin user by L2TP server. The IP should be in the same subnet as local LAN, and should not be occupied.

Auth. Type: Default is Auto(CHAP, Challenge Handshake Authentication Protocol) if you want the router to determine the authentication type to use, or else manually specify 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.

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

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

Active as default route: Commonly used in dialout setting, enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

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

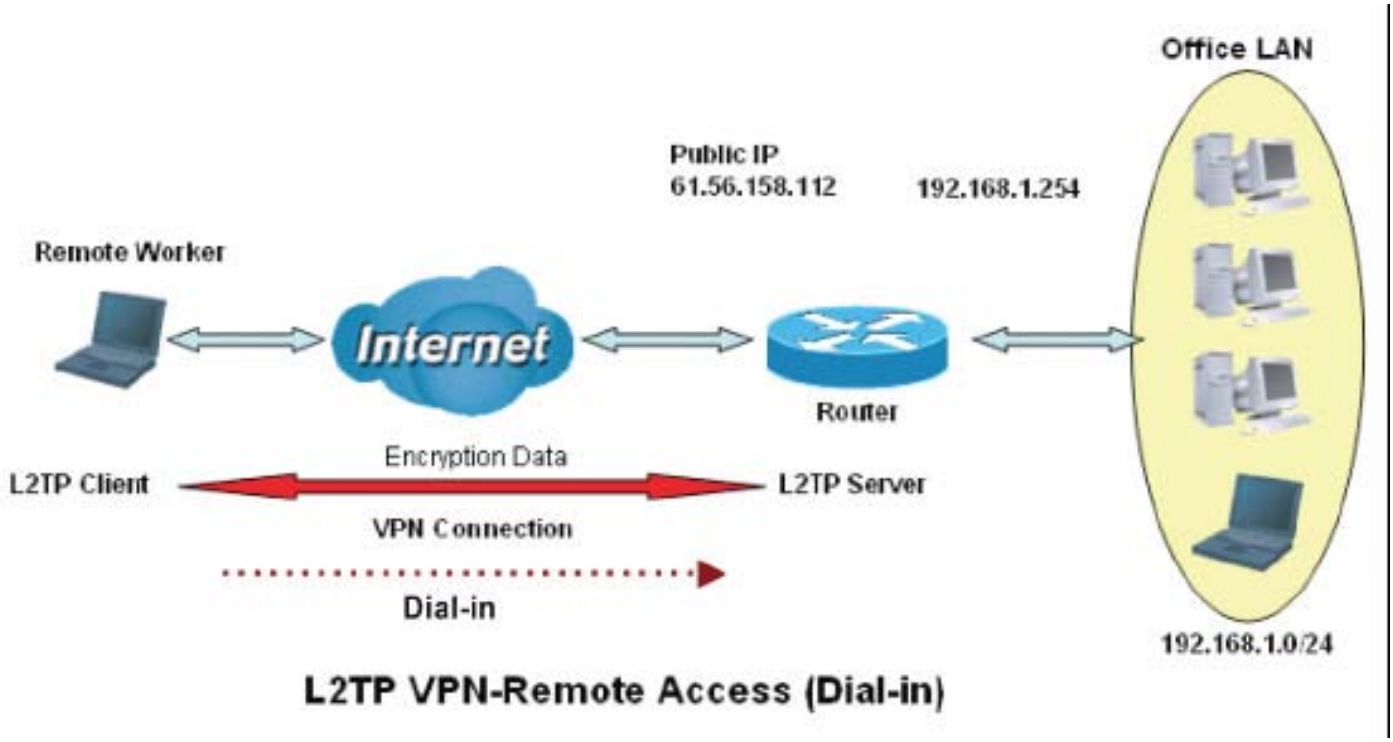
Local Host Name: Enter hostname of Local VPN device that is connected / establishes a VPN tunnel.

Connection Type: Remote Access or LAN to LAN. If “LAN to LAN” is selected, enter the network information, such as network address and netmask.

Examples:

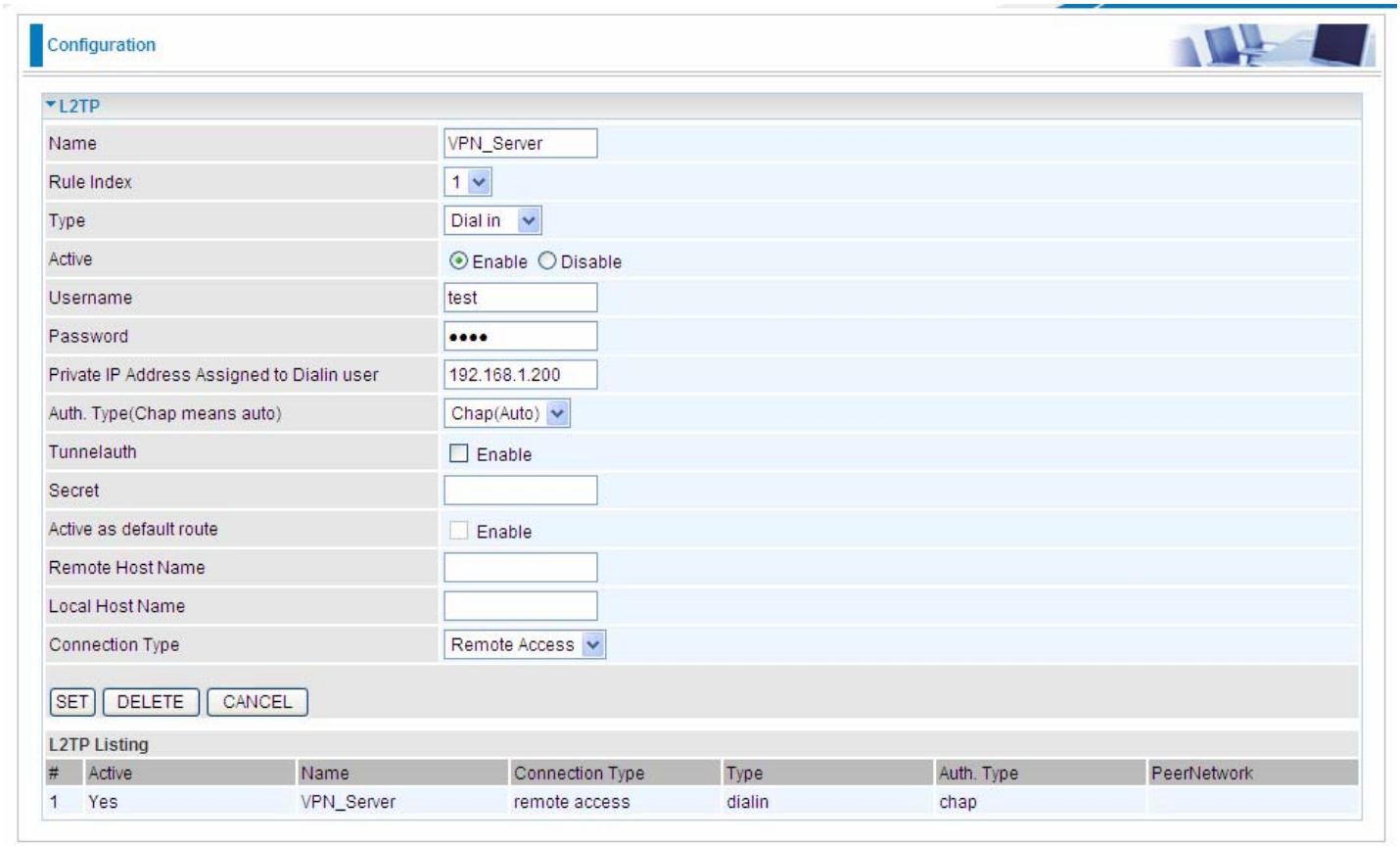
1. **Configuring a L2TP VPN - Remote Access Dial-in Connection**

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



Configuring L2TP VPN in the Office

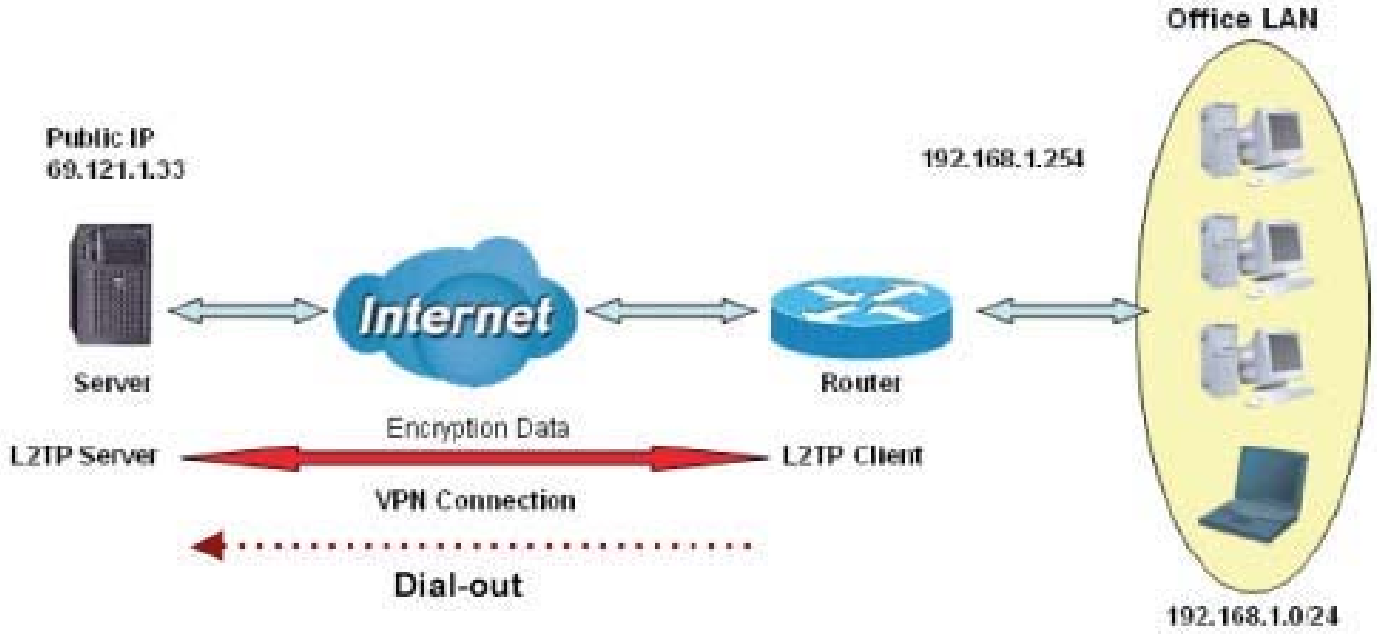
The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.



Function		Description
Name	VPN_Server	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	An IP assigned to the remote client
Username	test	Enter the username and password to authenticate a remote client
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

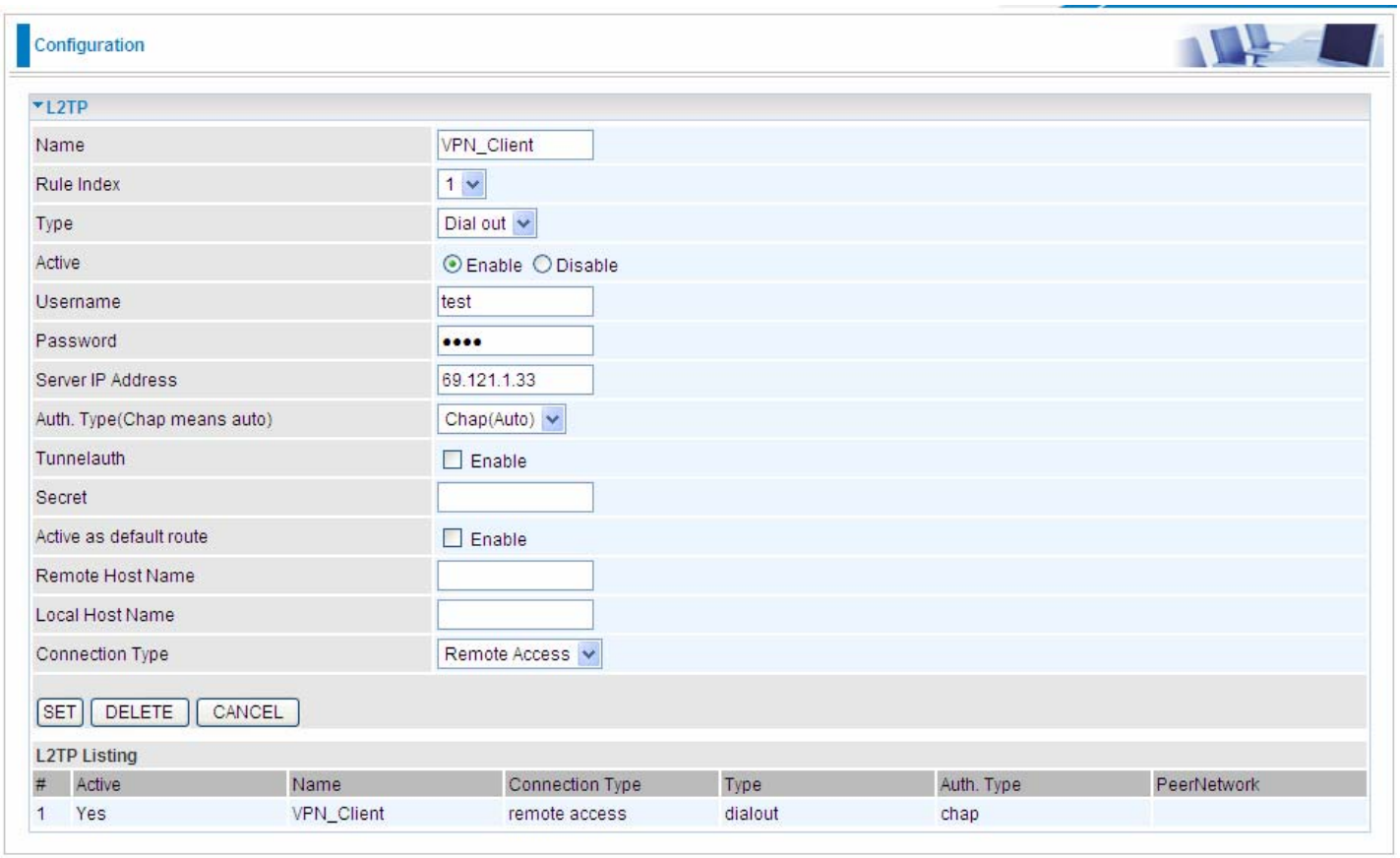
2. **Configuring a Remote Access L2TP VPN Dial-out Connection**

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



L2TP VPN-Remote Access (Dial-out)

Configuring L2TP VPN in the Office



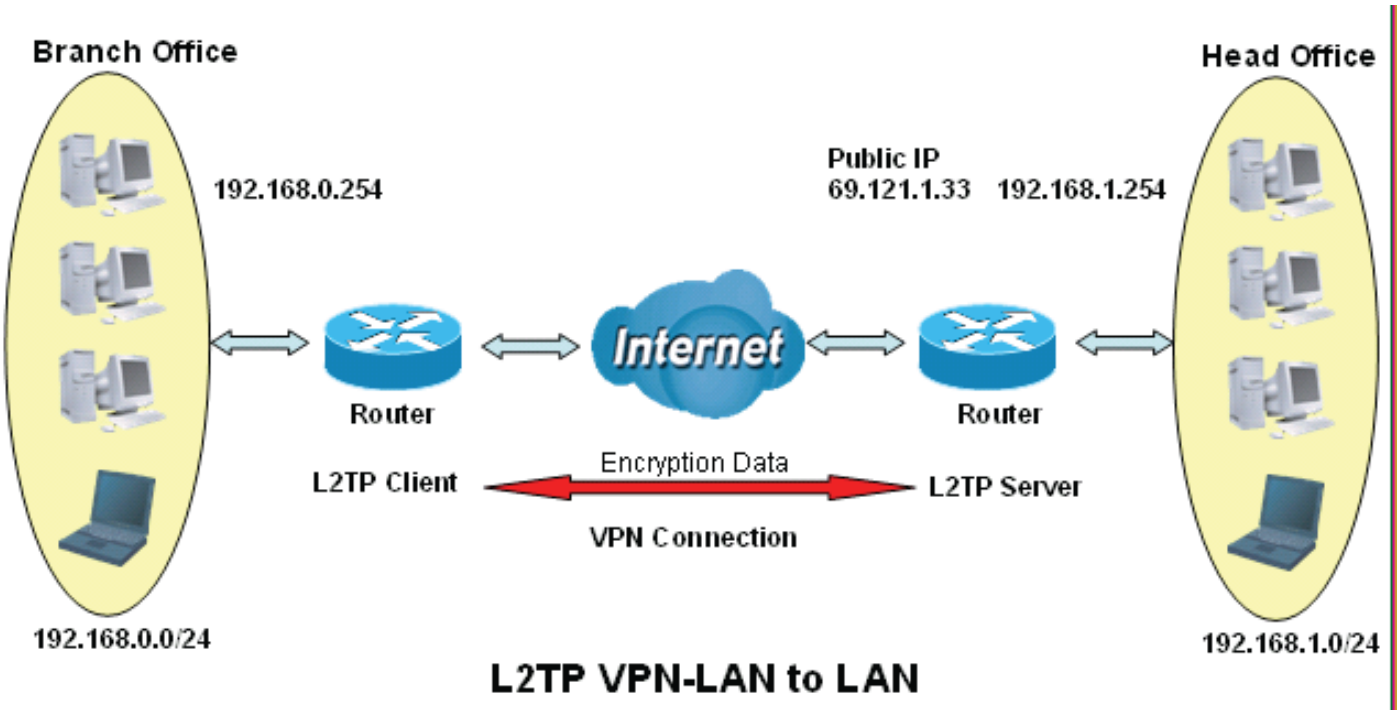
Function		Description
Name	VPN_Client	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop down menu
IP Address (or Domain Name)	69.121.1.33	A Dialed Server IP
Username	test	An assigned username and password
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

.

Example: Configuring L2TP LAN-to-LAN VPN Connection

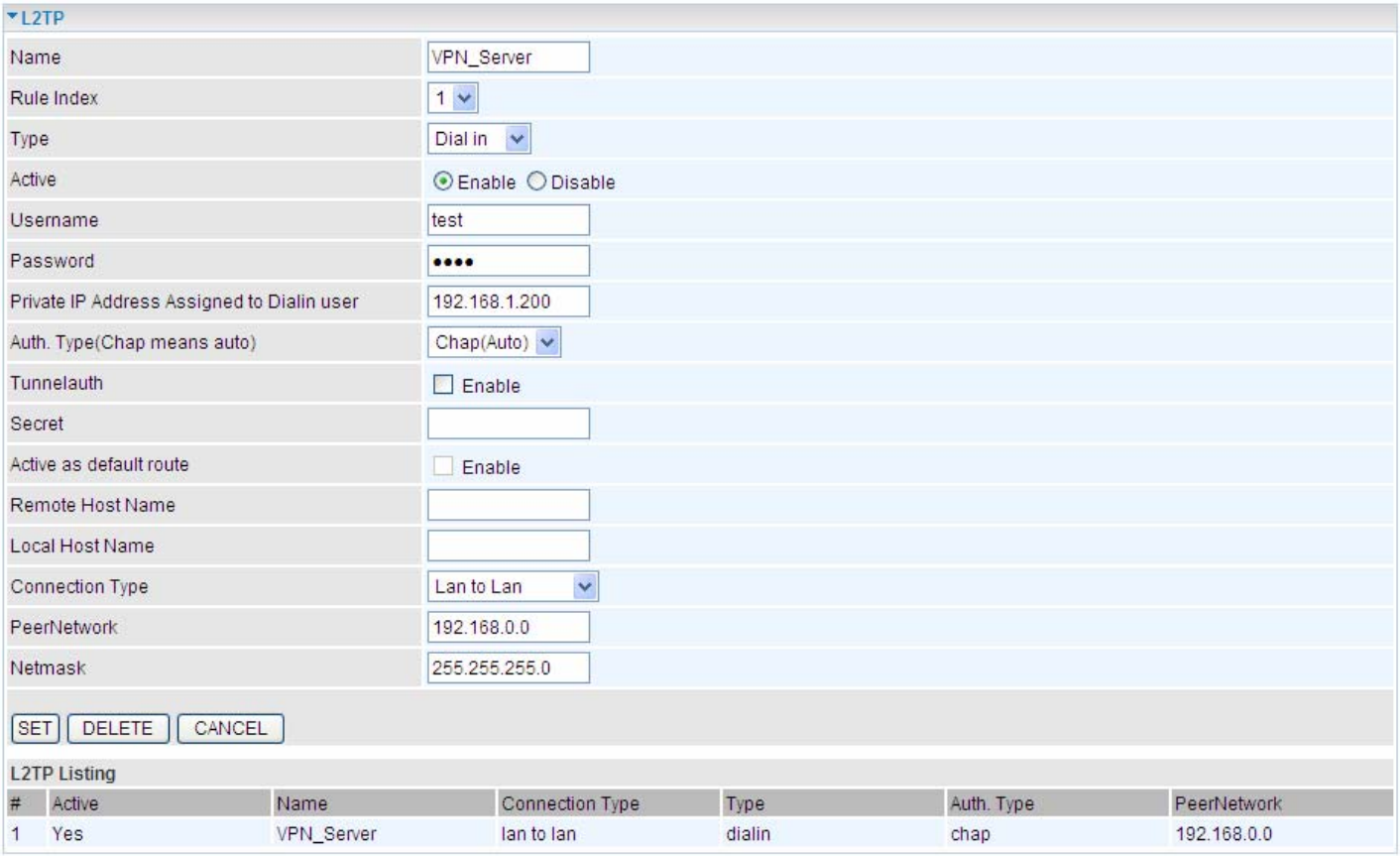
The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

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



Configuring L2TP VPN in the Head Office

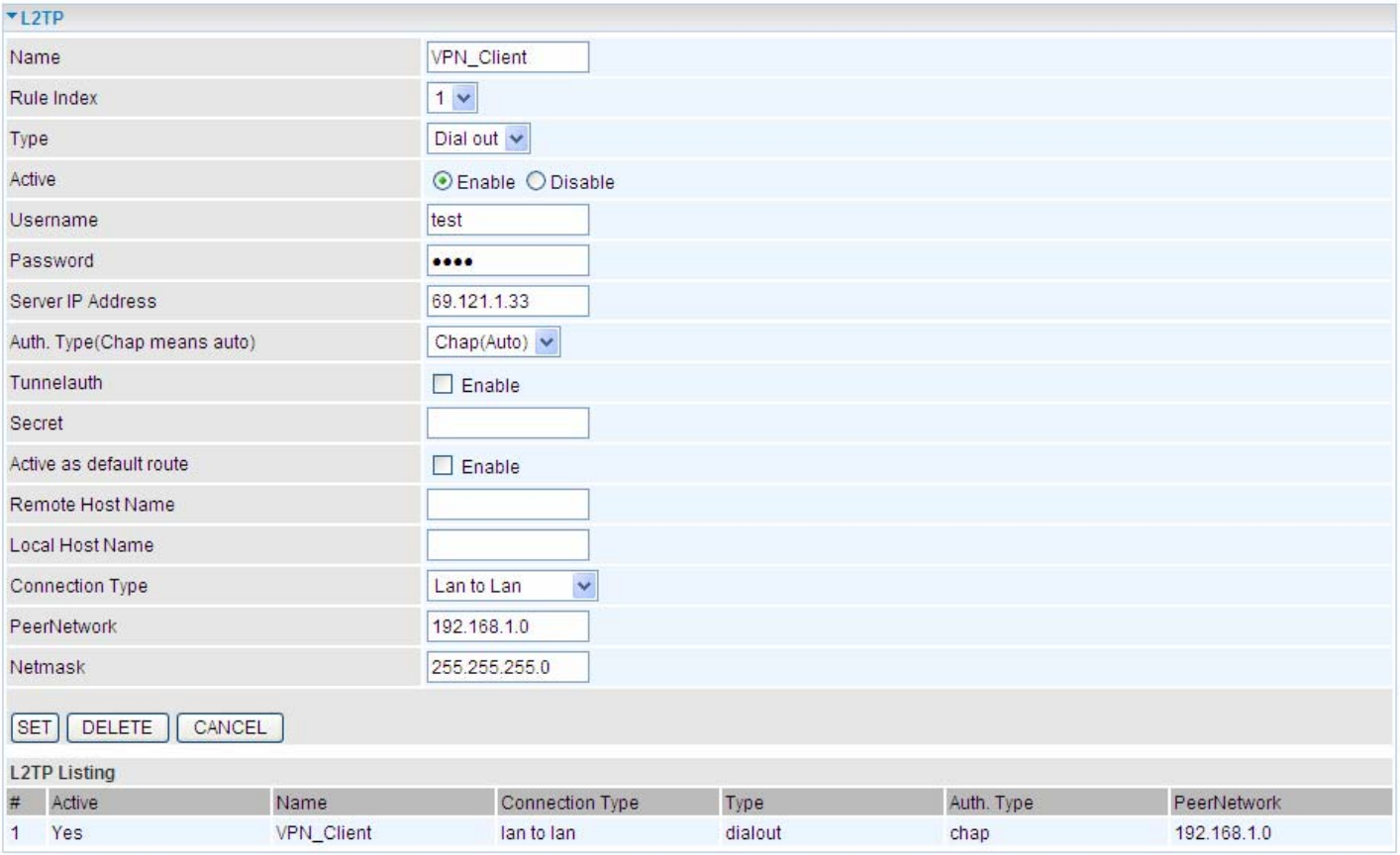
The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Function		Description
Name	HeadOffice	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	IP address assigned to branch office network
Peer Network IP	192.168.0.0	Branch office network
Username	test	An assigned username and password to authenticate branch office network
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.33 is the Public IP address of the router located in head office. If you registered the DDNS (please refer to the DDNS section of this manual), you can also use the domain name instead of the IP address to reach the router.



Function		Description
Name	VPN_Client	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type
Type	Dial out	Select Dial out from the Type drop down menu
IP Address	69.121.1.33	IP address of the server
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	test	An assigned username and password to authenticate branch office network
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

5.6.11 Port Isolation

Port isolation is a mechanism to allow or block devices in one port (indicates the P1-P4 and WP1 – WP4) to access other devices in other ports. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.

Configuration

Port Isolation Setting

Port Group	Lan Port				WLan Port			
	P1	P2	P3	P4	WP1	WP2	WP3	WP4
Group 1	☑	☑	☑	☑	☑	☑	☑	☑
Group 2	☐	☐	☐	☐	☐	☐	☐	☐
Group 3	☐	☐	☐	☐	☐	☐	☐	☐
Group 4	☐	☐	☐	☐	☐	☐	☐	☐
Group 5	☐	☐	☐	☐	☐	☐	☐	☐
Group 6	☐	☐	☐	☐	☐	☐	☐	☐
Group 7	☐	☐	☐	☐	☐	☐	☐	☐
Group 8	☐	☐	☐	☐	☐	☐	☐	☐

SAVE CANCEL

The most typical one example is to isolate all port from each other shown below. Each port has its own group, under this circumstance, devices connected to each port have no access to other devices connected to other ports. This is a special example, and users can change the settings to determine how the ports are belonged to the group.

Configuration

Port Isolation Setting

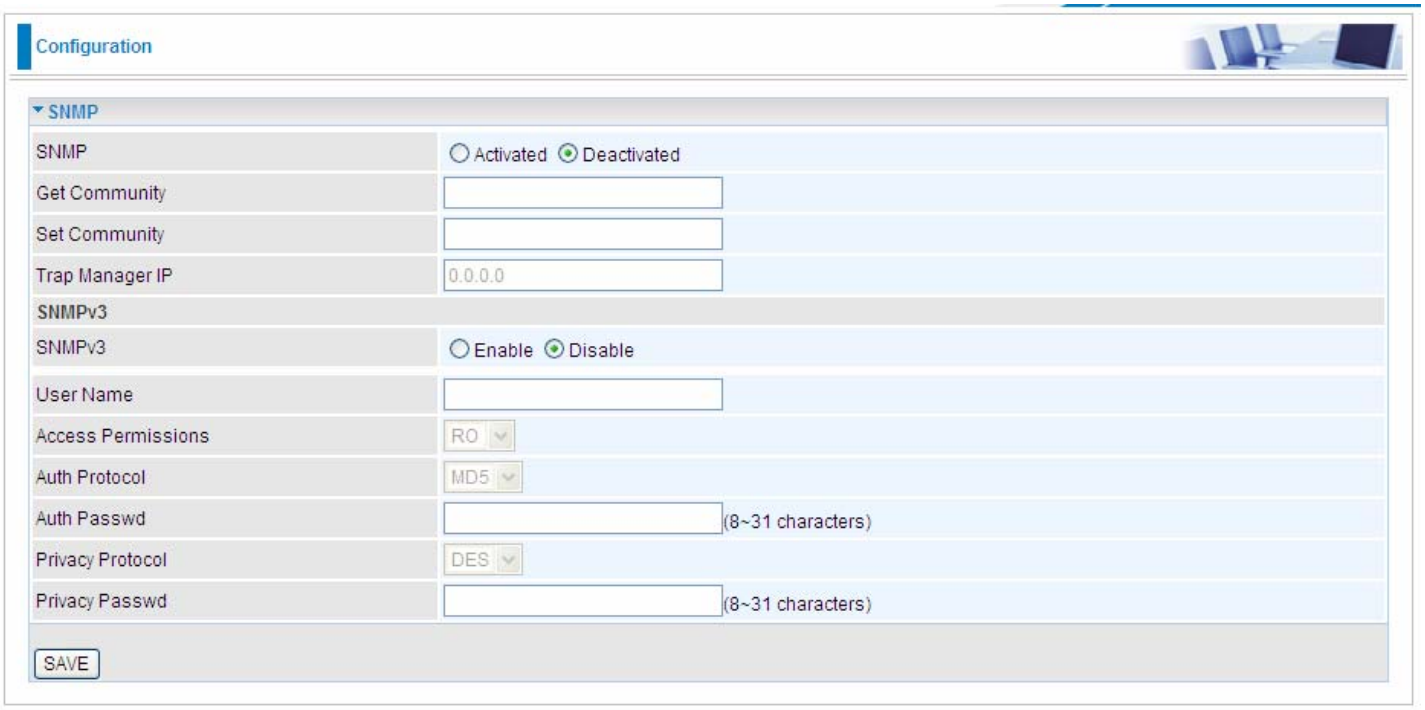
Port Group	Lan Port				WLan Port			
	P1	P2	P3	P4	WP1	WP2	WP3	WP4
Group 1	☑	☐	☐	☐	☐	☐	☐	☐
Group 2	☐	☑	☐	☐	☐	☐	☐	☐
Group 3	☐	☐	☑	☐	☐	☐	☐	☐
Group 4	☐	☐	☐	☑	☐	☐	☐	☐
Group 5	☐	☐	☐	☐	☑	☐	☐	☐
Group 6	☐	☐	☐	☐	☐	☑	☐	☐
Group 7	☐	☐	☐	☐	☐	☐	☑	☐
Group 8	☐	☐	☐	☐	☐	☐	☐	☑

SAVE CANCEL

5.7 Access Management

5.7.1 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BiPAC 7600NX(L) serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.



SNMP: Select to enable SNMP feature.

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

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

Trap Manager IP: Enter the IP of the server receiving the trap message(when some exception occurs) sent by this SNMP agent.

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Auth Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Auth Password: Set the authentication password, 8-31 characters.

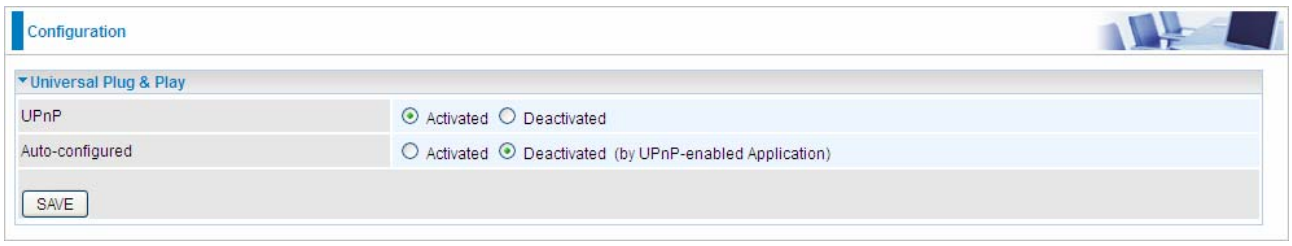
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Password: Set the privacy password, 8-31 characters.

5.7.2 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.



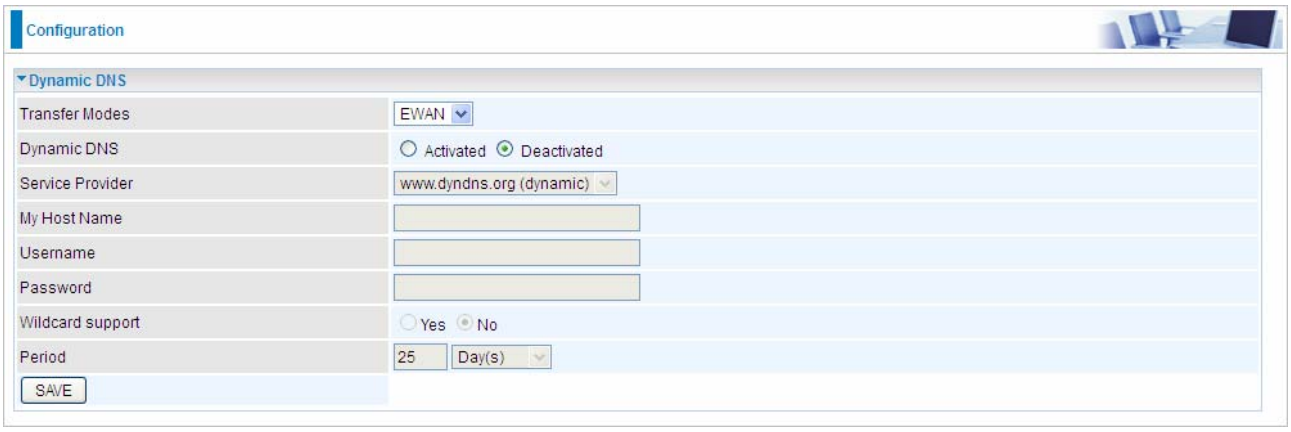
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the BiPAC 7600NX(L)' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BiPAC 7600NX(L) so that they can communicate through the BiPAC 7600NX(L), for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

5.7.3 DDNS

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 internet 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). But note that first users have to go to the Dynamic DNS registration service provider to register an account.



Transfer Modes: Select the interface the following DNS transformation rule will be applied to. For example, when EWAN is selected, your host name assigned (the registration information set here) by your Dynamic DNS provider will be bound to the IP of the EWAN.

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your BiPAC 7600NX(L) by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

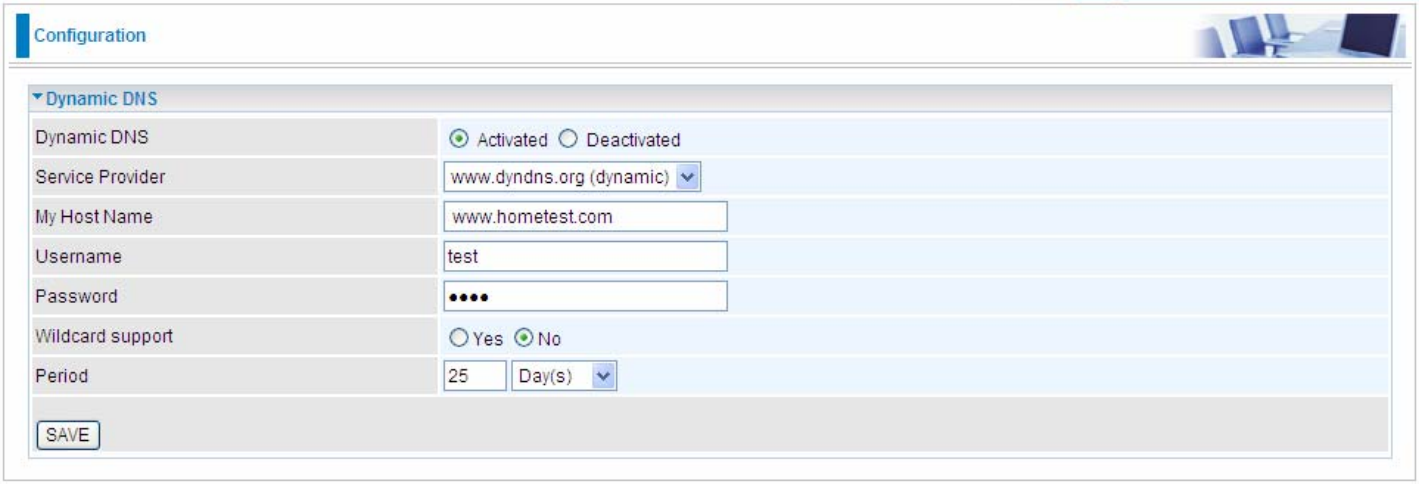
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

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/** .

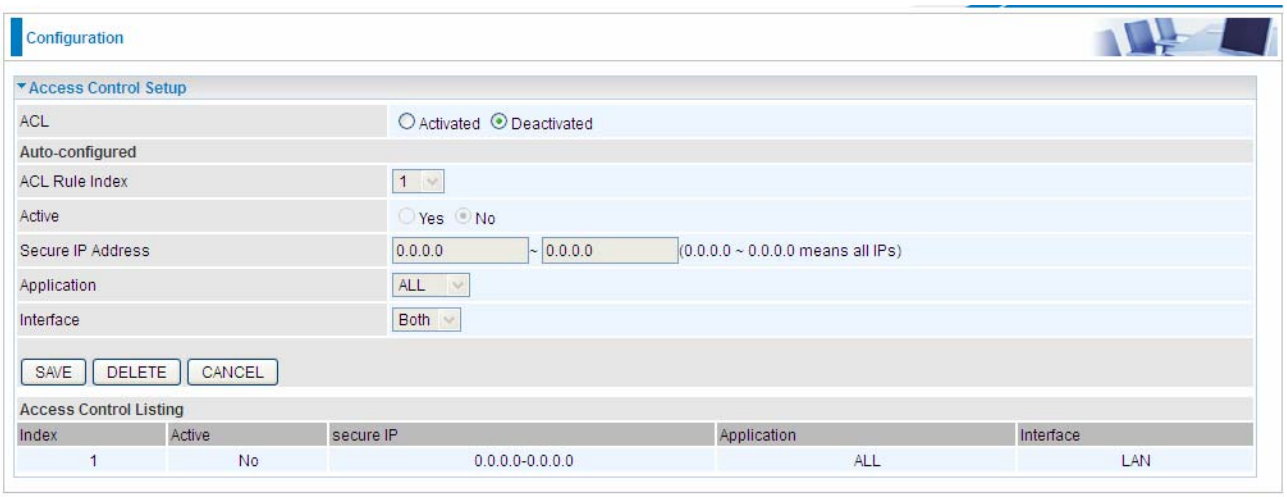
DDNS: www.hometest.com using username/password test/test



5.7.4 ACL

Access Control Listing allows you to determine which services/protocols can access BiPAC 7600NX(L) interface from which computers. It is a management tool aimed to allow IPs(set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is 16.



ACL Rule Index: This is item number

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BiPAC 7600NX(L). Type an IP address range to restrict access to the client(s) without a matching IP address.

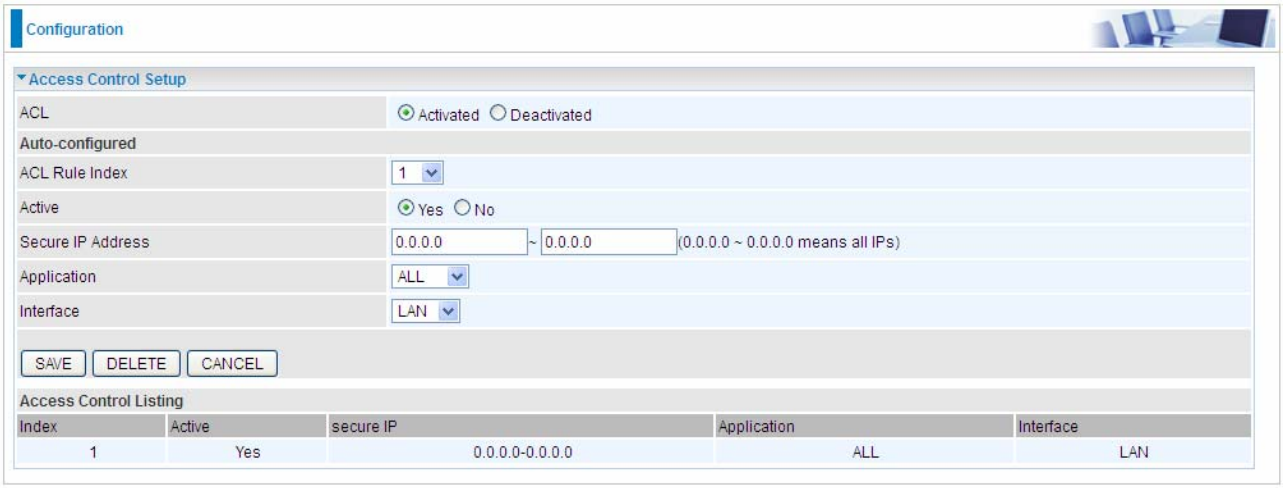
Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **Both**.

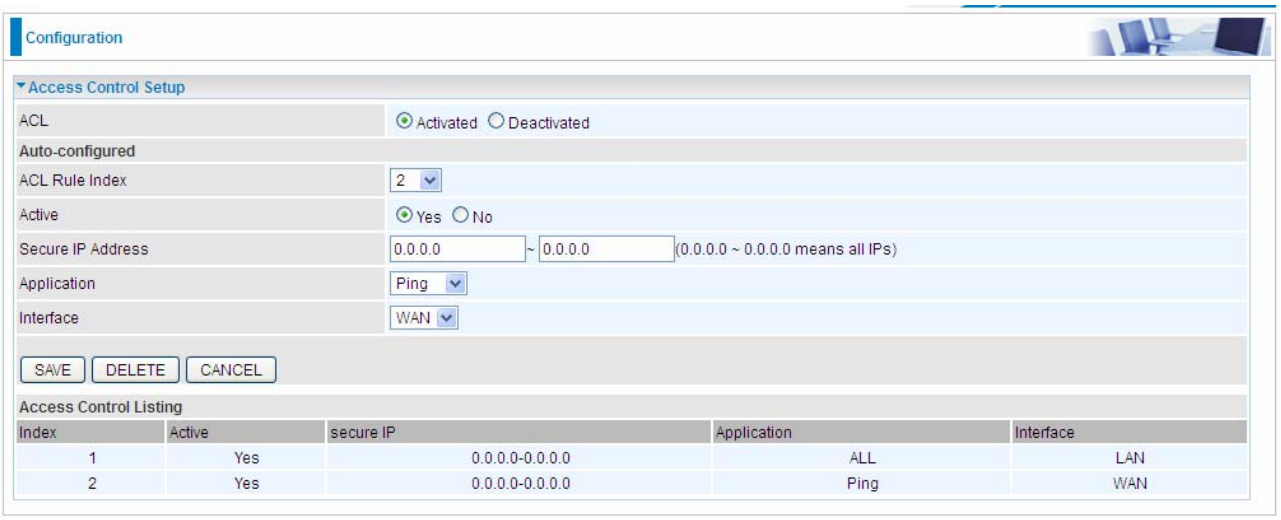
By default, the ACL is deactivated, so there is no default rule limiting the access to the router. The router is all open to both LAN and WAN side, user can add rules if needed.

Examples:

1). Set a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN can not access the router even from Ping.



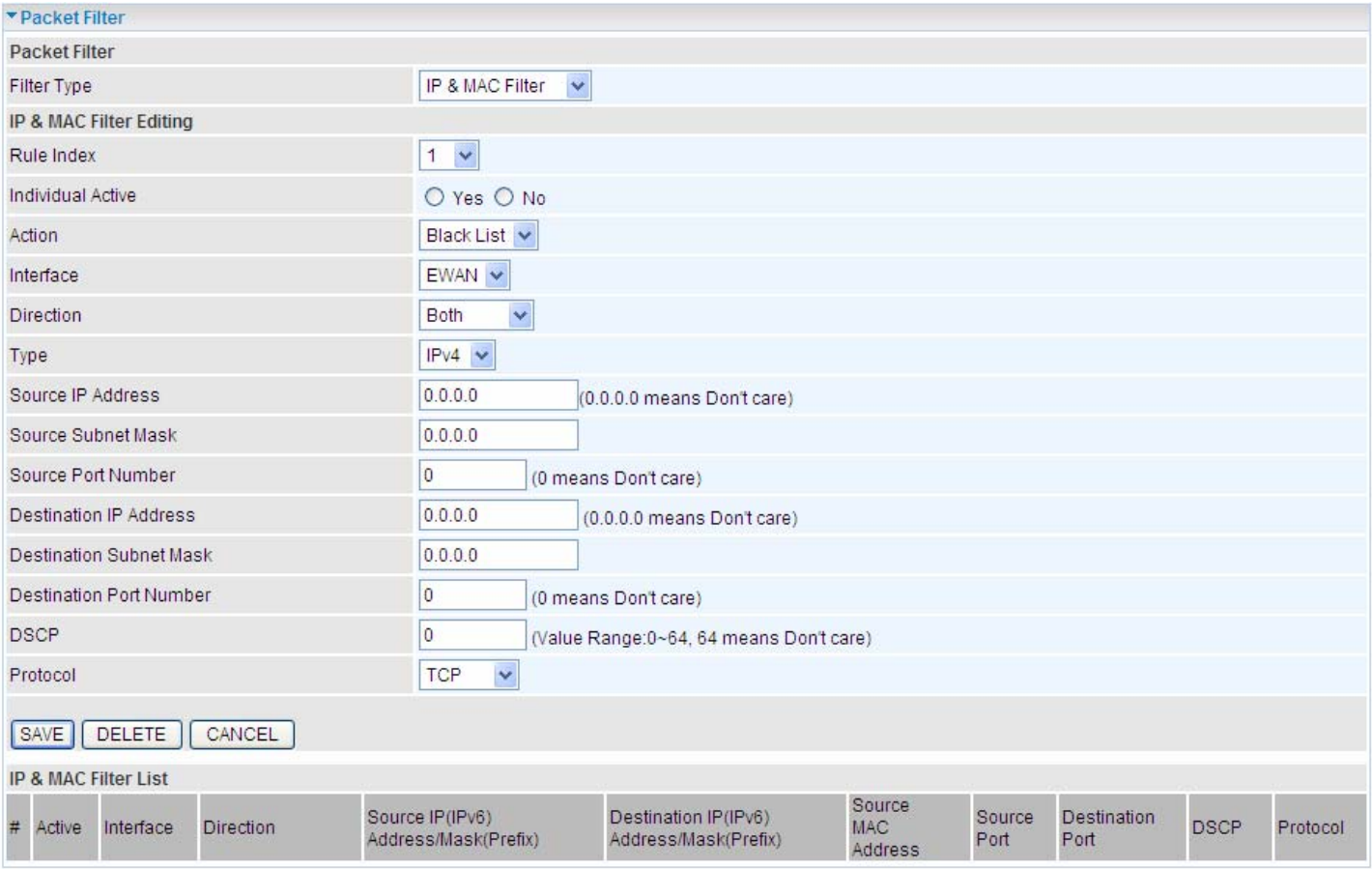
2). Generally, we always open Ping to WAN side, and user can now add another ACL rule granting Ping service to WAN side clients.



5.7.5 Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

➢ **IP & MAC Filter**



Packet Filter

Filter Type: There are three types "**IP & MAC Filter**", "**Application Filter**", and "**URL Filter**" that user can select for this filter rule. Here we set **IP & MAC Filter**.

IP & MAC Filter Editing

Rule Index: This is item number

Individual Active: Select **Yes** to activate the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or block selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select "IP" for IPv4 address, port number and protocol. Select "IPv6" for IPv6 address, port number and protocol. Select "MAC" for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means "Don't care".

Source SubnetMask: It is the source IP addresses based on above source subnet IP

Source Port Number: This Port defines the port allowed to be used by the Remote/WAN to connect to the

application. It is recommended that this option be configured by an advanced user. 0 means “Don’t care”.

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Destination SubnetMask: It is the destination IP addresses based on above destination subnet IP

Destination Port Number: This is the Port that defines the application. (E.g. HTTP port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, ICMPv6) that the rule applies to.

IP/MAC Filter Listing

#: Item number**.**

Active: Whether the connection is currently active.

Interface: show the interface the rule applied to.

Direction: show the direction the rule applied to.

Source IP(IPv4) Address/Mask(Prefix): The source IP address or range of packets to be monitored.

Destination IP(IPv6) Address/Mask(Prefix): This is the destination subnet IP address.

Source MAC Address: show the MAC address of the rule applied.

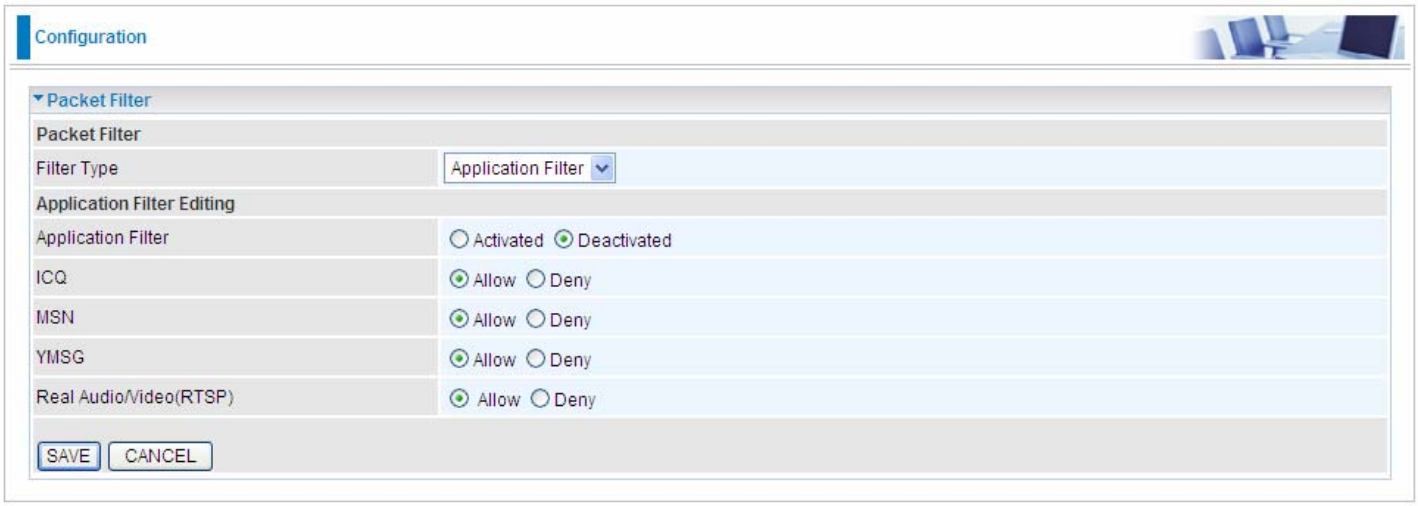
Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535.** It is recommended that this option be configured by an advanced user.

Destination Port: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP or ICMPv6**

➢ Application Filter



Application Filter: Select this option to Activated/Deactivated the Application filter.

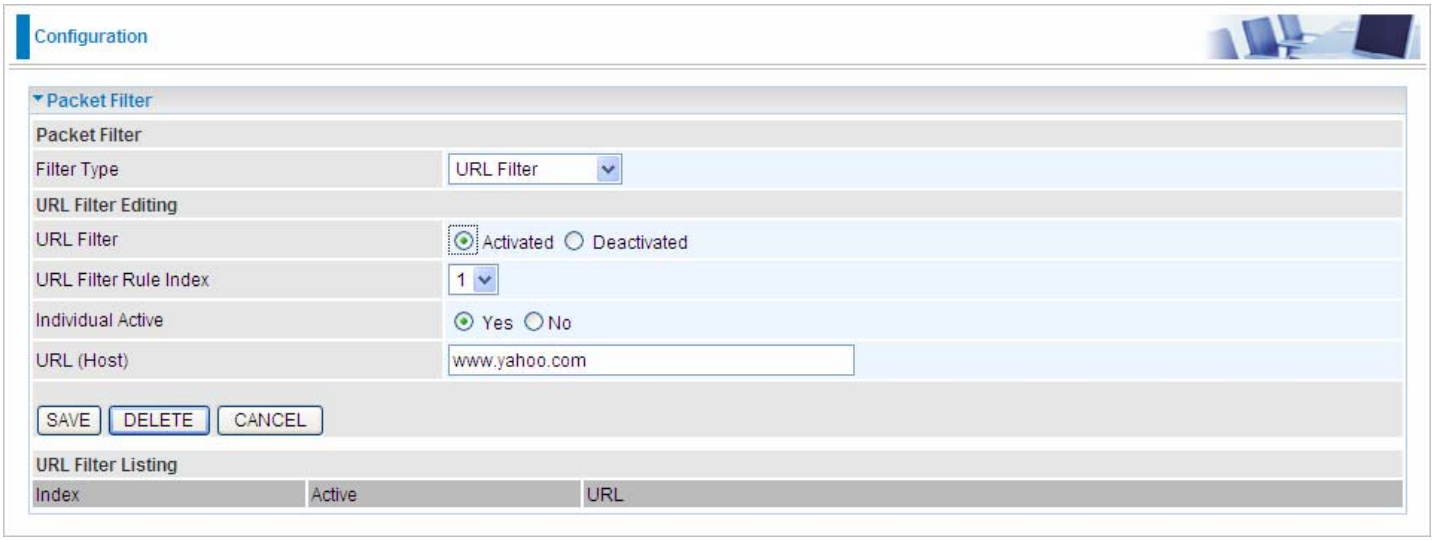
ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video(RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

➢ URL Filter



URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: This is item number.

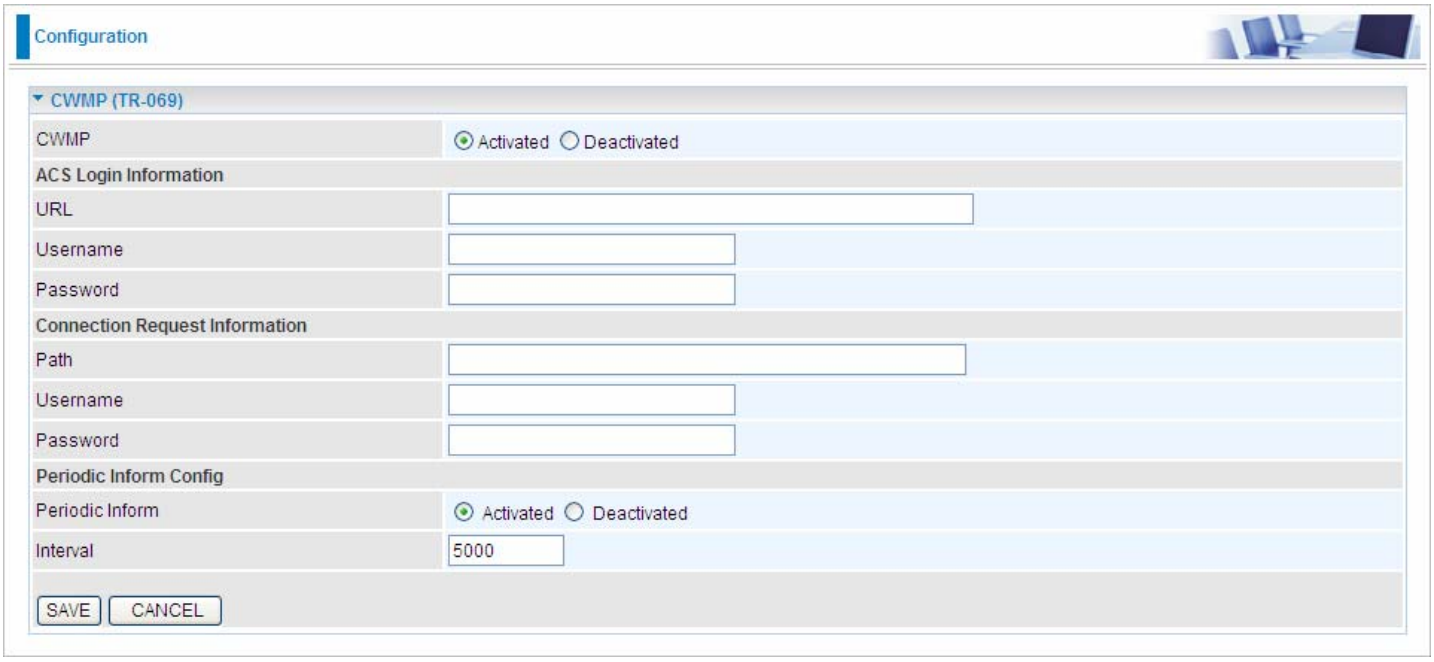
Individual active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first Yes in Active field, and also Yes in individual active field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL(Host): Specified URL which is prohibited from accessing.

5.7.6 CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. 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.



CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

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

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

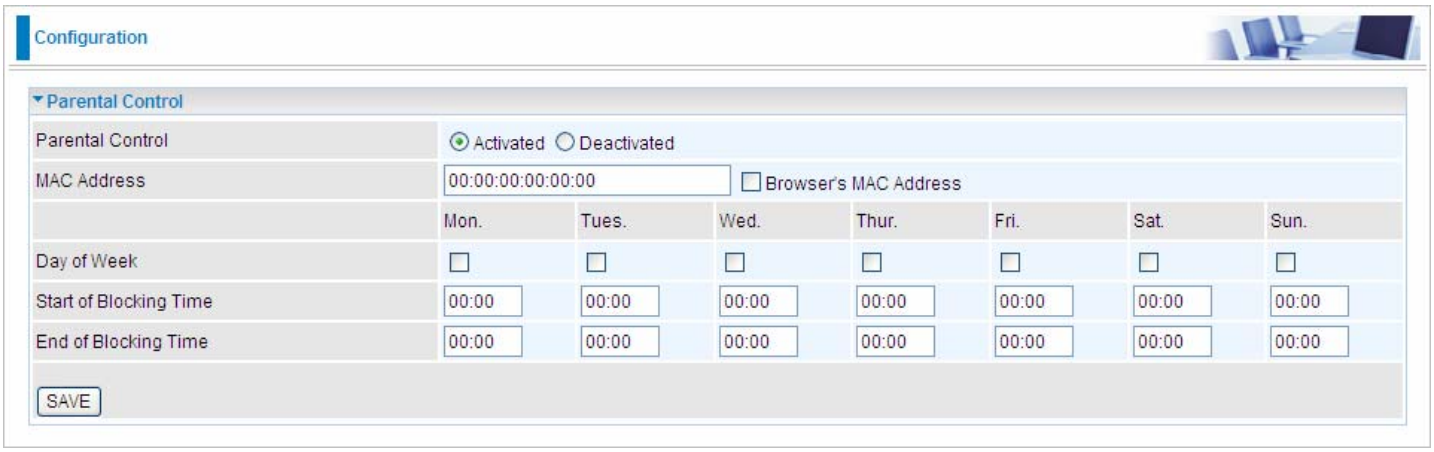
Periodic Inform Config

Periodic Inform: Select activated to enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Interval(s): 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.

5.7.7 Parental Control

With this feature, router can reject to provide **internet** services to the specified computer during some specified time interval. This can be very useful for parents to give control to children using computer without restraint.



Parent Control: Select Activated to enable this feature.

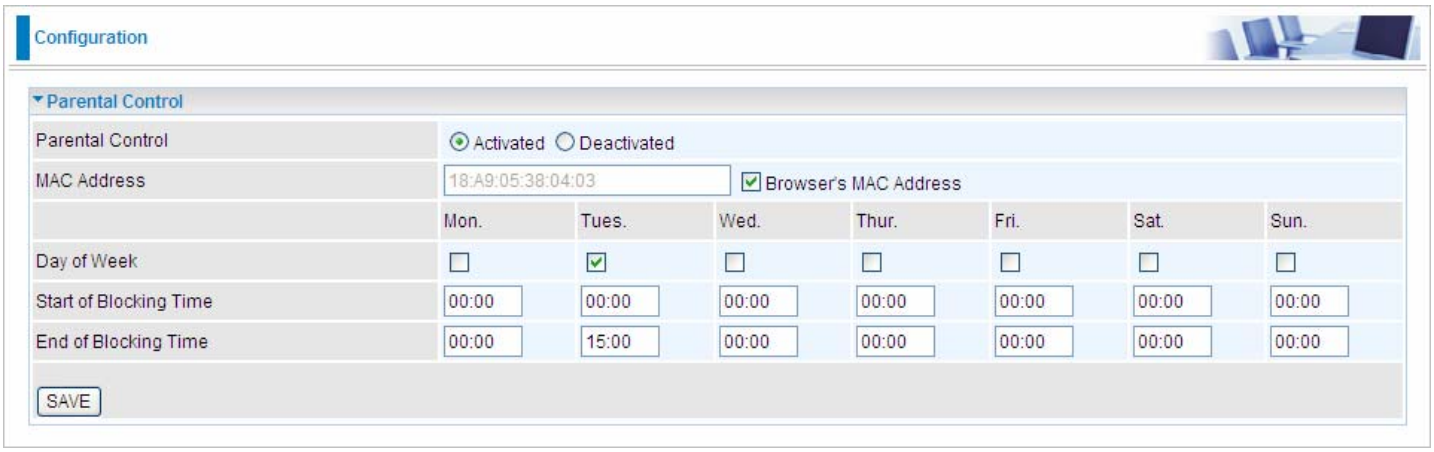
MAC Address: Type the MAC address(es) you want to block to access the internet (access to the router is sustained). The format of MAC address could be: xx:xx:xx:xx:xx:xx . If you want to set restriction to the Browser PC, you can directly check the checkbox of Browser's MAC Address.

Days of Week: Select the days of a week the rule takes effect.

Start of Blocking Time: Enter the start time of each day in hh:mm format. Default is 00:00.

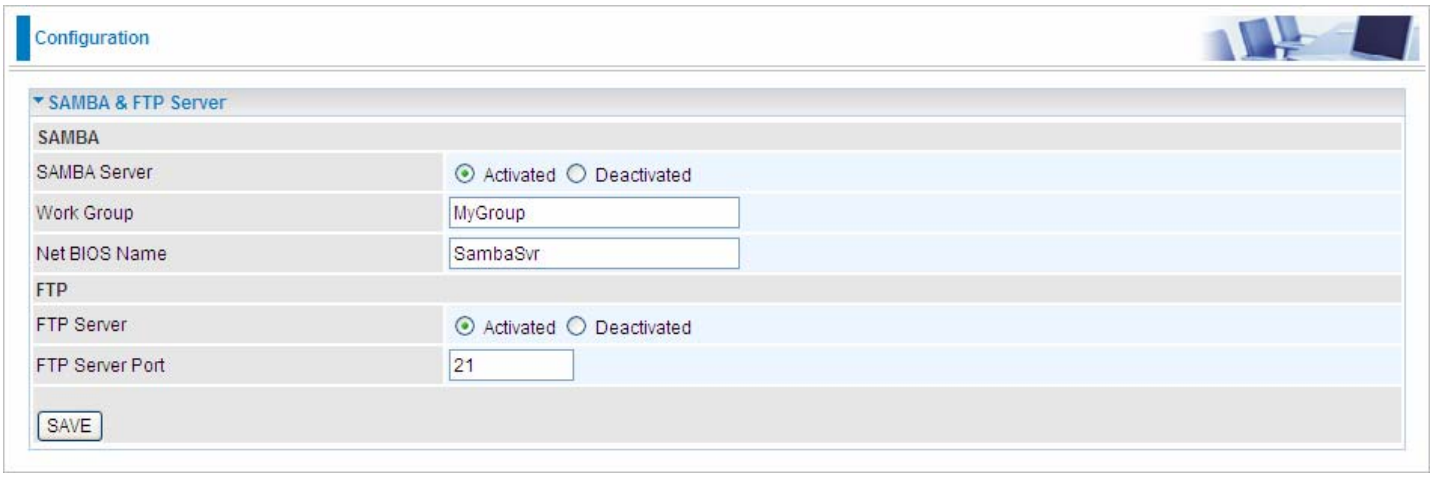
End of Blocking Time: Enter the end time of the day in hh:mm format. Default is 00:00.

In the screenshot shown below, for example, you can see the PC with MAC address 18:A9:05:38:04:03 is restricted to access the **internet** during interval of 00:00 to 15:00 on Tuesday (other features like accessing and managing the router are sustained).



5.7.8 SAMBA & FTP Server

Samba and FTP are served as network sharing.



SAMBA Server: Activated to enable Samba sharing.

Work Group: The same mechanism like in miscrosoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

Samba/FTP login account:

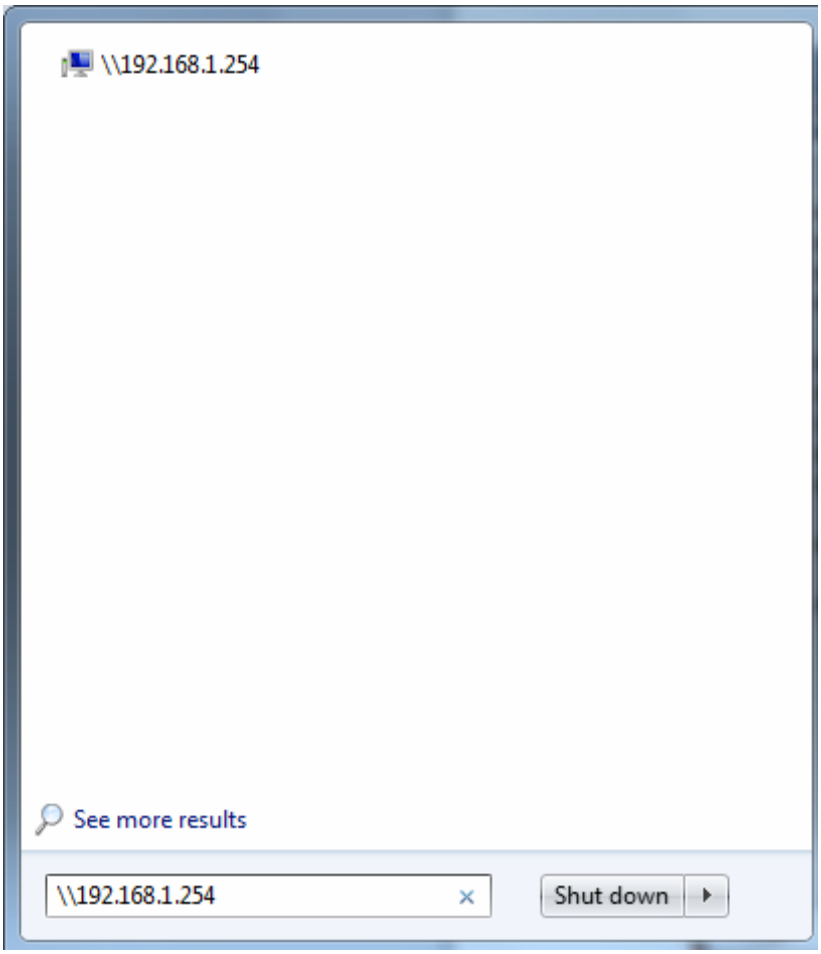
1) **Default user:** admin/admin, it is the administrative user and a super user, it has the full authority of Samba/FTP access and operation permission of objects in Samba and FTP server.

2) **New user:** users can create new user(s) to grant it (them) access and permission to the Samba & FTP server.

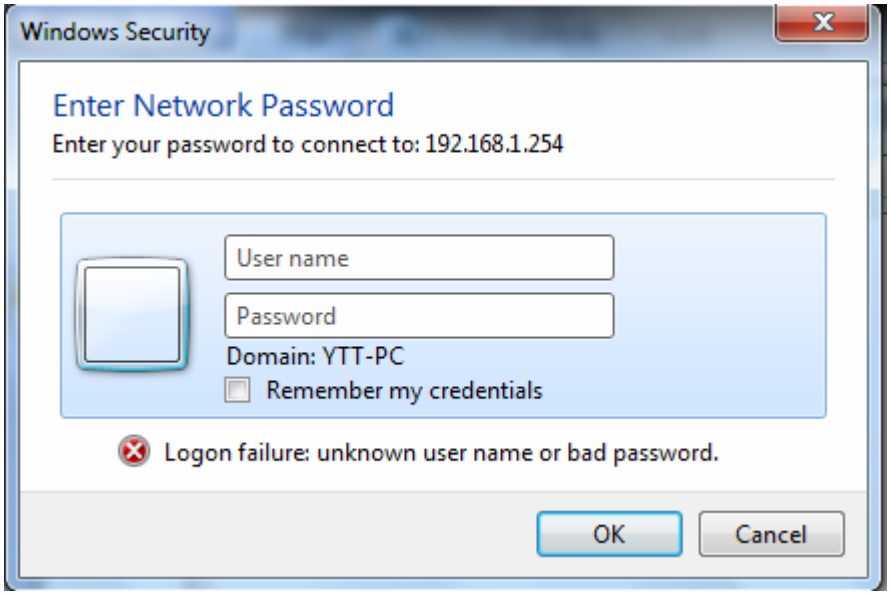
Please see 5.8.1 User Management.

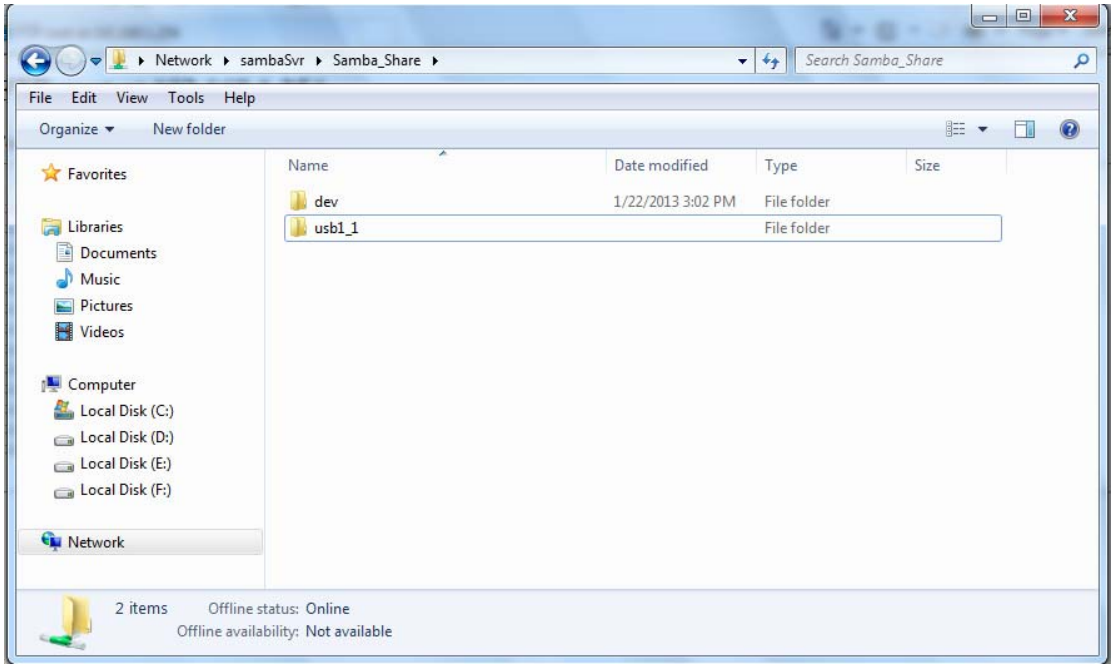
Samba Usage:

1. Go directly to Start > Run (enter \\192,168,1,254 (from LAN side), \\WAN IP (from WAN side), \\SambaSvr , but if you enter \\SambaSvr, please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



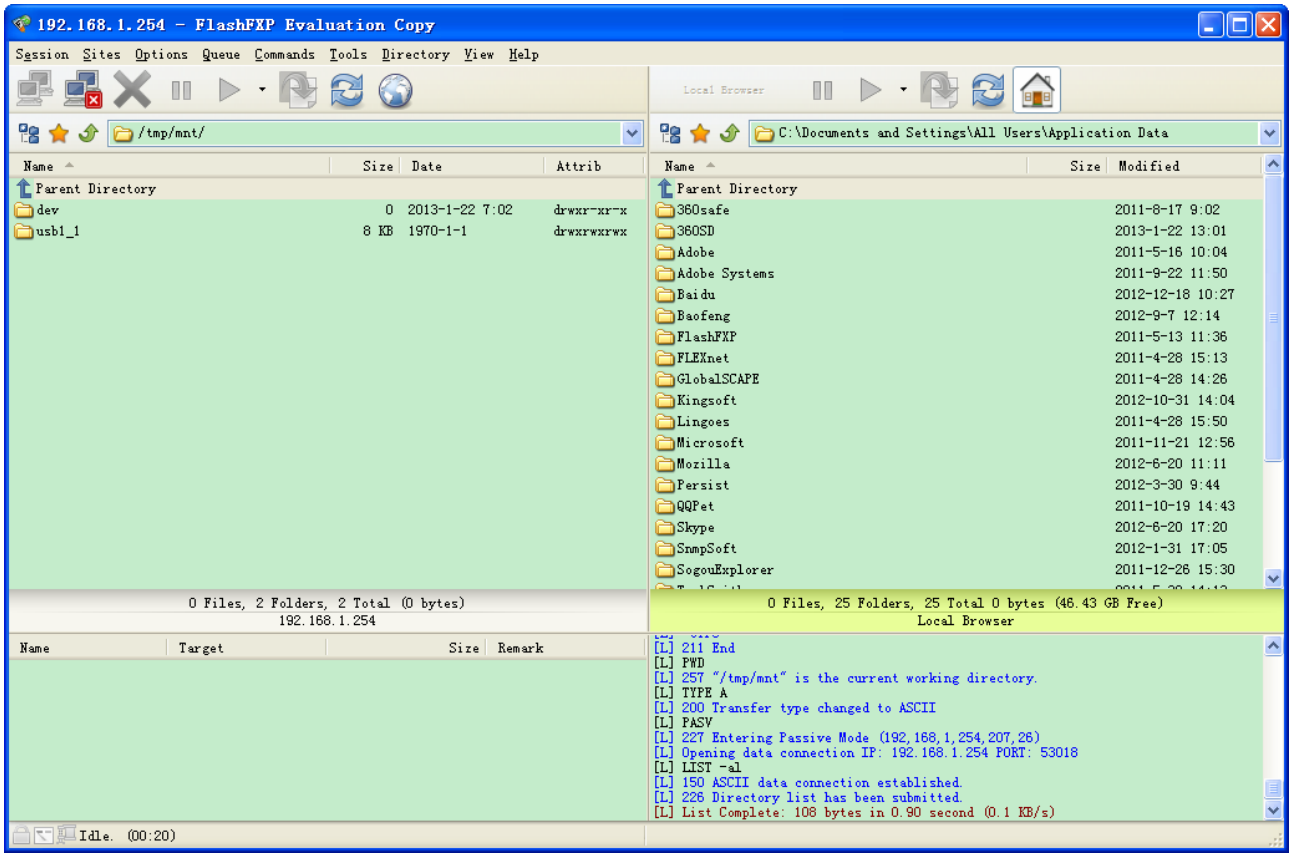


FTP usage:

1. **Access via FTP tools**

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP
2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).
3) Connect to the ftp site.

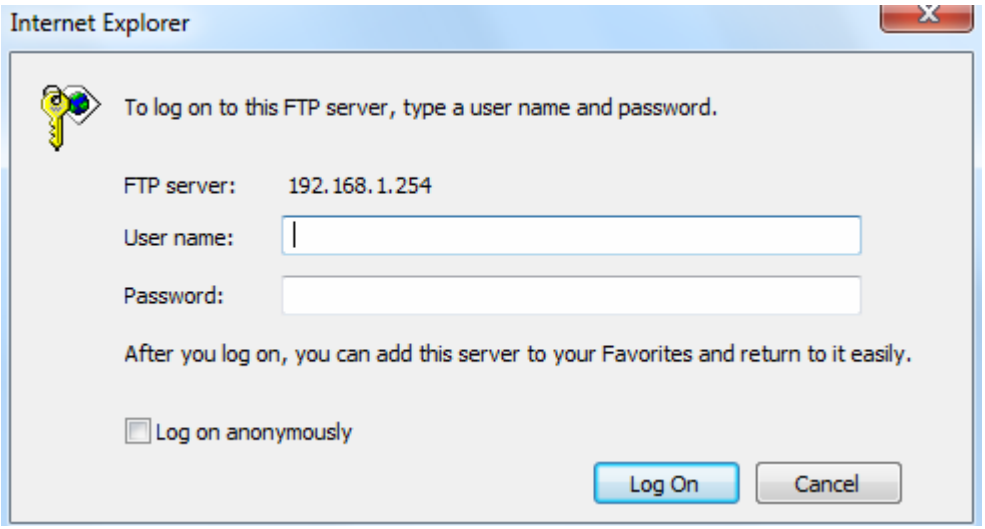


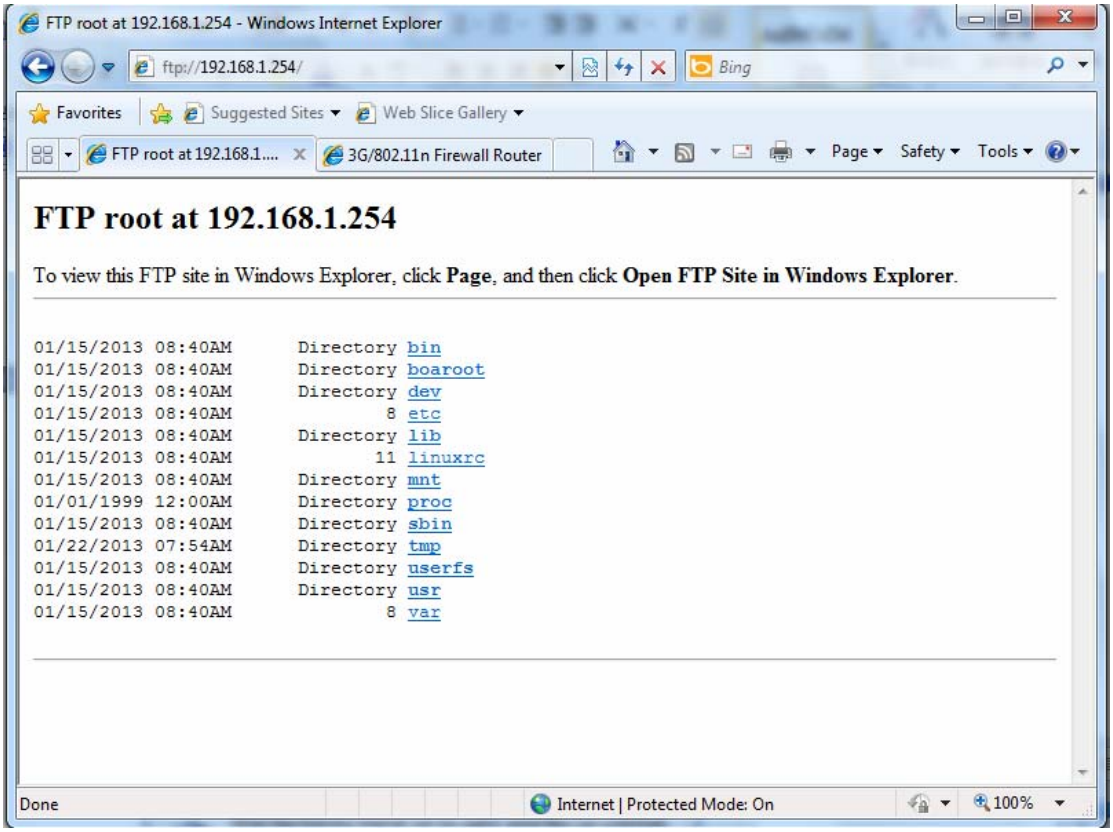
2. **Web ftp access**

ftp:// LAN IP(ftp:192.168.1.254) or ftp://WAN IP

1) Enter ftp://192.168.1.254 at the address bar of the web page.

2) Enter the account's username and password.



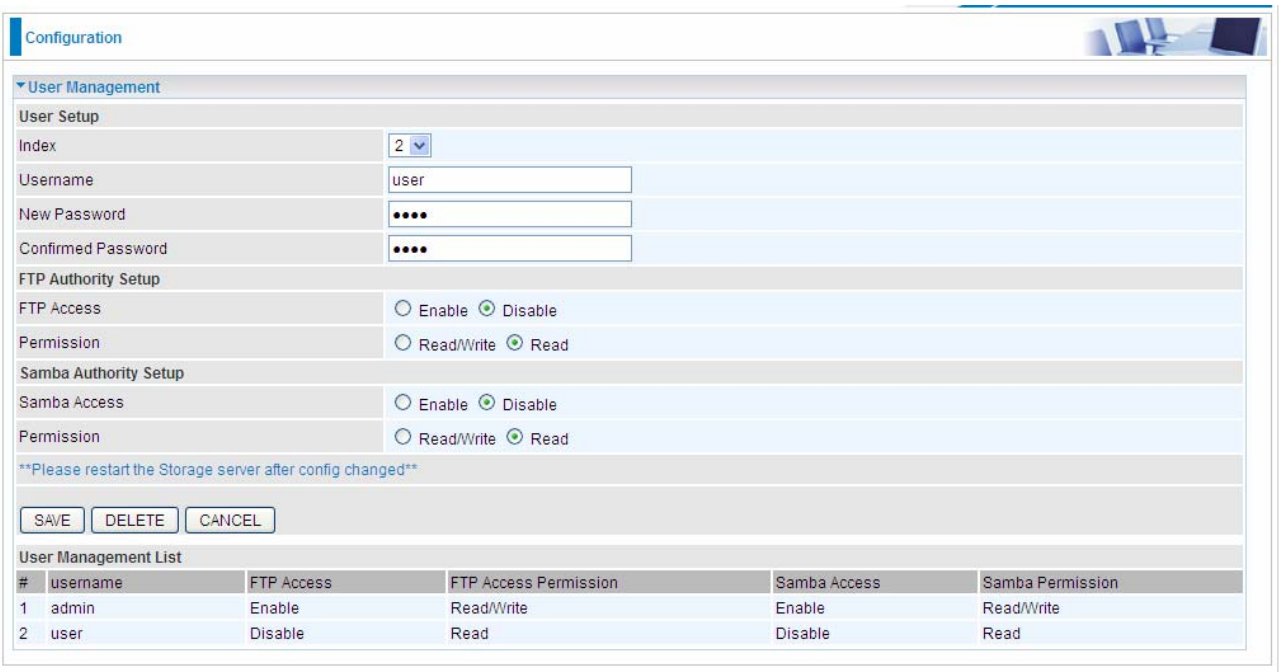


5.8 Maintenance

5.8.1 User Management

In factory setting, the default accounts are **admin/admin** and **user/user.** The default account admin has been authorized to web access of router, Samba access, and FTP access. The user **user/user** has only access to the FTP and Samba server, but disabled by default. A total of **6** other accounts can be created to grant access to the access of Samba and FTP but not router's web.

Note: Please go to 5.7.8 SAMBA & FTP Server to re-activate FTP and Samba server to enable the changes to the FTP and Samba account set here.



User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to Samba and FTP.

New Password: Type the password for the user account. Default user admin's password can be changed here and confirmed in the next field.

Confirmed Password: Type password again for confirmation.

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read, Writer or Read.

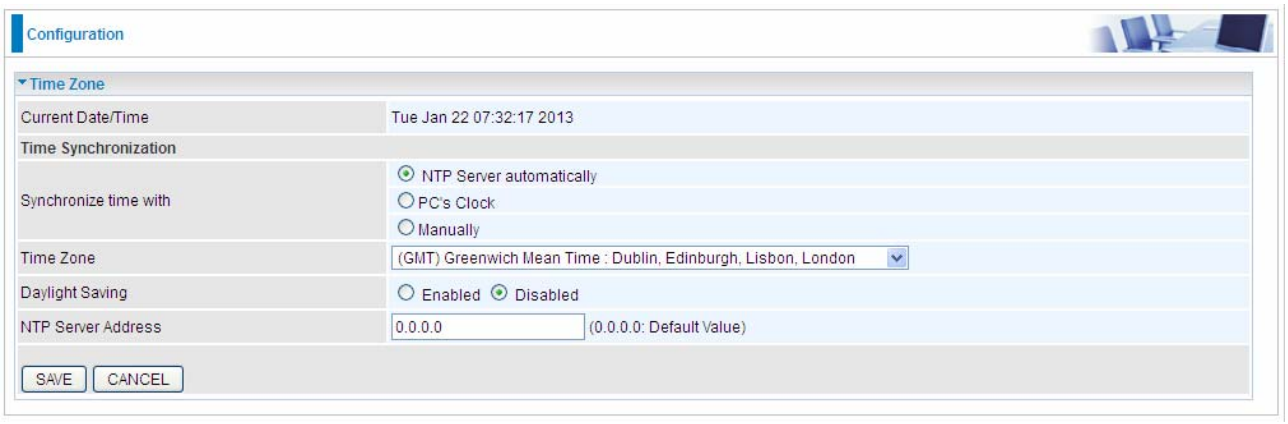
Samba Authority

Samba Access: Enable to grant the user access to the Samba server.

Permission: Set the operation permission for the user, Read, Writer or Read.

5.8.2 Time Zone

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those default, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



Synchronize time with: Select the methods to synchronize the time.

- **NTP Server automatically:** To synchronize time with the NTP server.
- **PC's Clock:** To synchronize time with the PC's clock.
- **Manually:** Select this, user need to set the time yourself manually.

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

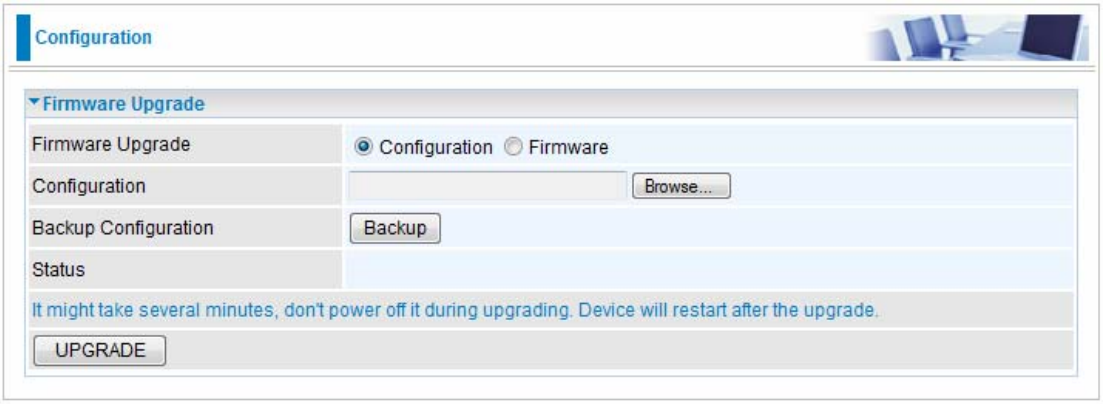
Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

5.8.3 Firmware

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your router allows you to upgrade the software it runs to take advantage of these changes.

To upgrade the firmware of BiPAC 7600NX(L), you should download or copy the firmware to your local environment first. Press the **"Browse…"** button to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading. When the procedure is completed, BiPAC 7600NX(L) will reset automatically to make the new firmware work.

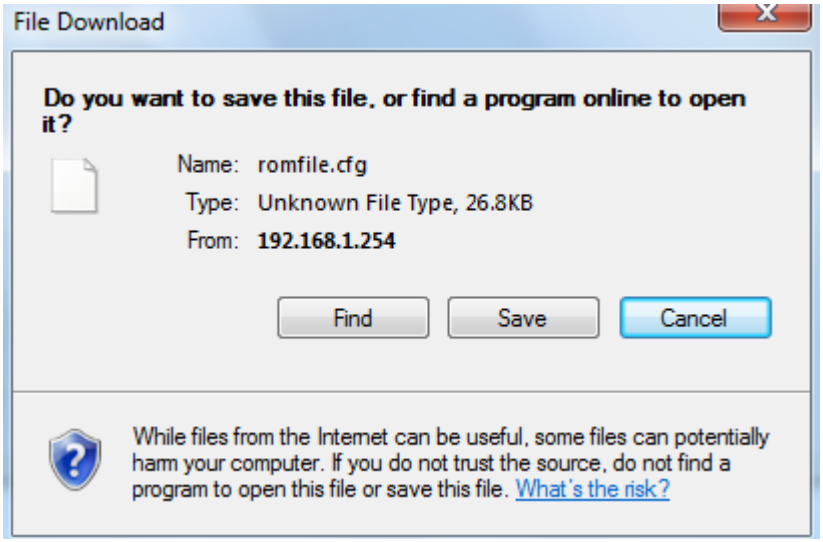


Configuration or Firmware: Choose configuration or firmware you want to update.

New Firmware Location: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Browse: Click **Browse...** to find the configuration file or firmware file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

Backup Configuration: Click **Backup** button to back up the now running configuration file to your computer in the event that you need this configuration file to restore the device especially when you make some wrong configurations and you need to restore the original settings.



UPGRADE: Click **UPGRADE** to begin the upload process. This process may take up to two minutes.

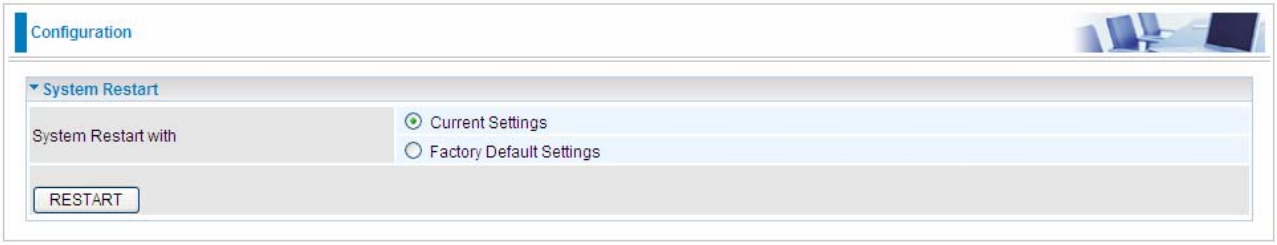
If the upload was not successful, the following screen will appear. Click Back to go back to the Firmware screen.

Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router. If you accidentally power down the router, resulting in the failed upgrading, please refer to steps in restoration to restore your router to a functional state.

5.8.4 System Restart

Click **System Restart** with option **Current Settings** to reboot your router.



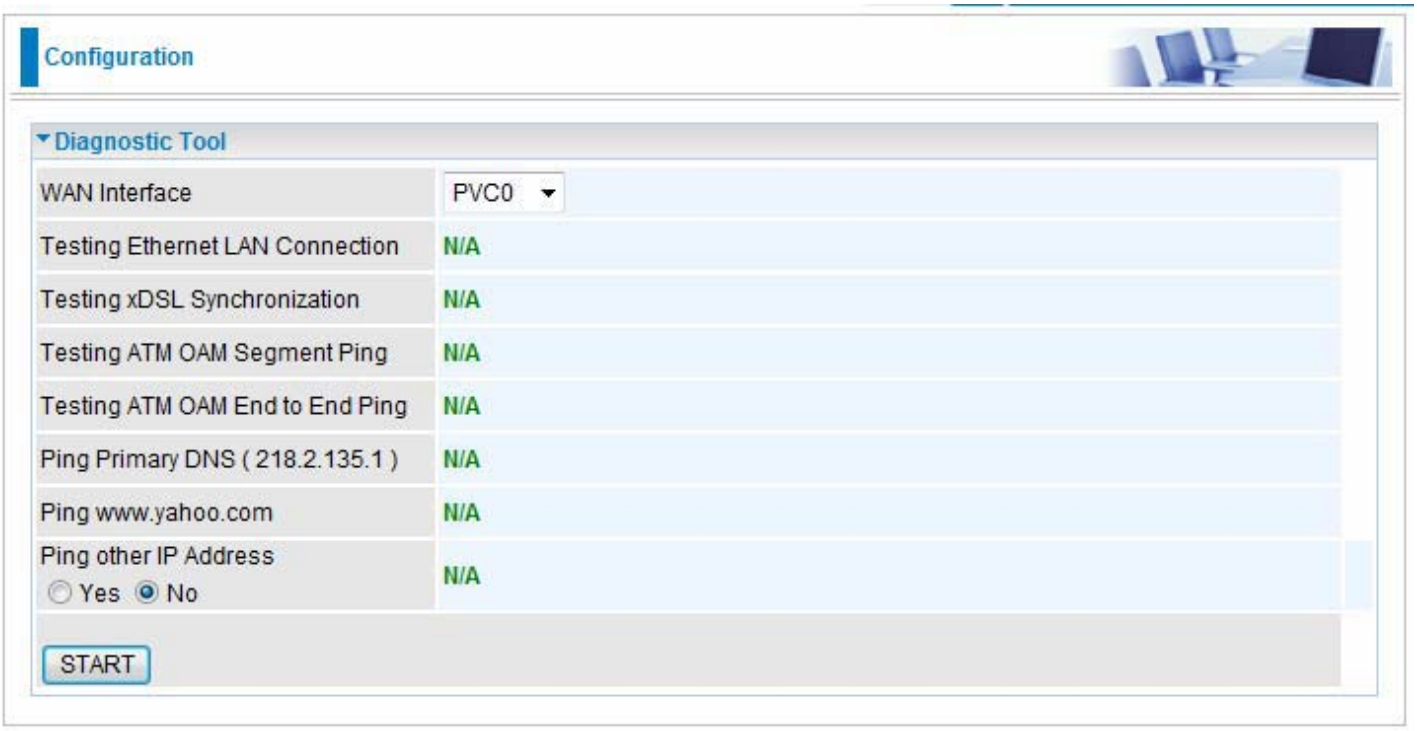
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to restore to factory default settings.

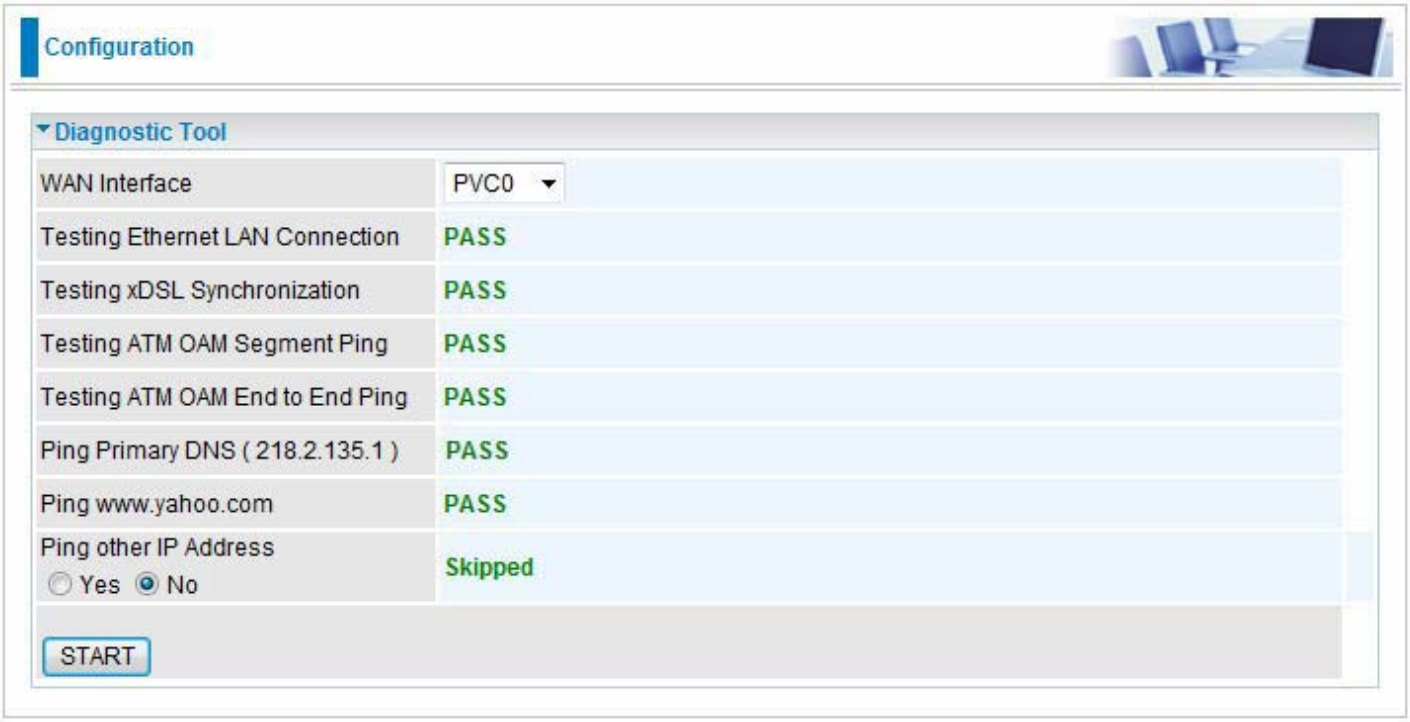
You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

5.8.5 Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

ADSL (8 services ranging from PVC0 to PVC7, user can diagnose each service accordingly):





EWAN:

Click START to begin to diagnose the connection.

Chapter 6
Troubleshooting

If the router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login username and/or password.	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection ("linesync") failed.	Ensure that the telephone cable is connected properly from the xDSL port to the wall jack. The xDSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problems, you may need to verify these settings with your ISP.

Frequent loss of DSL linesync (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 DSL connection, including causing frequent disconnections.

Recovery procedures for non-working routers

Problem	Corrective Action
Recovery procedures for non-working routers(e.g. after a failed firmware upgrade flash)	Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (**192.168.1.1**), and will not respond to ping request from your PC or other telnet operations.

APPENDIX
Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this 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.

Co-location statement

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

FCC Radiation Exposure Statement

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