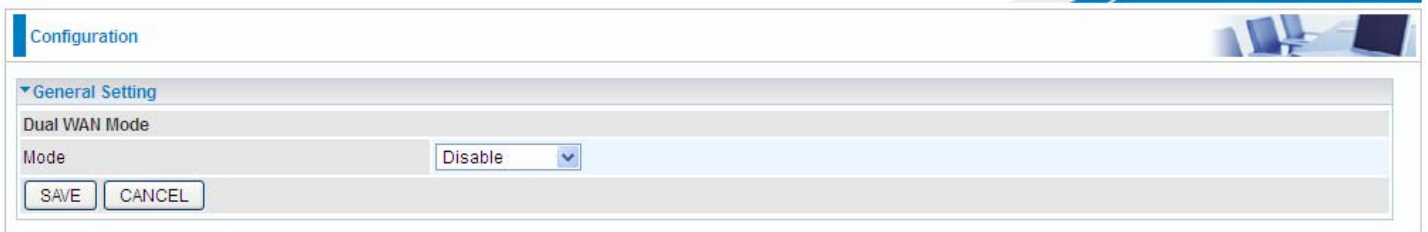


4.4.2 Dual WAN

Dual WAN is specially designed to offer users Failover/Fallback or Load Balance feature.

Auto Failover/Fallback is to ensure an always-on internet connection. Users can set a WAN1 (main WAN) and WAN 2 (backup WAN), and when WAN1 fails, it will switch to WAN2, and when WAN1 restores, it will switch to WAN1 again.

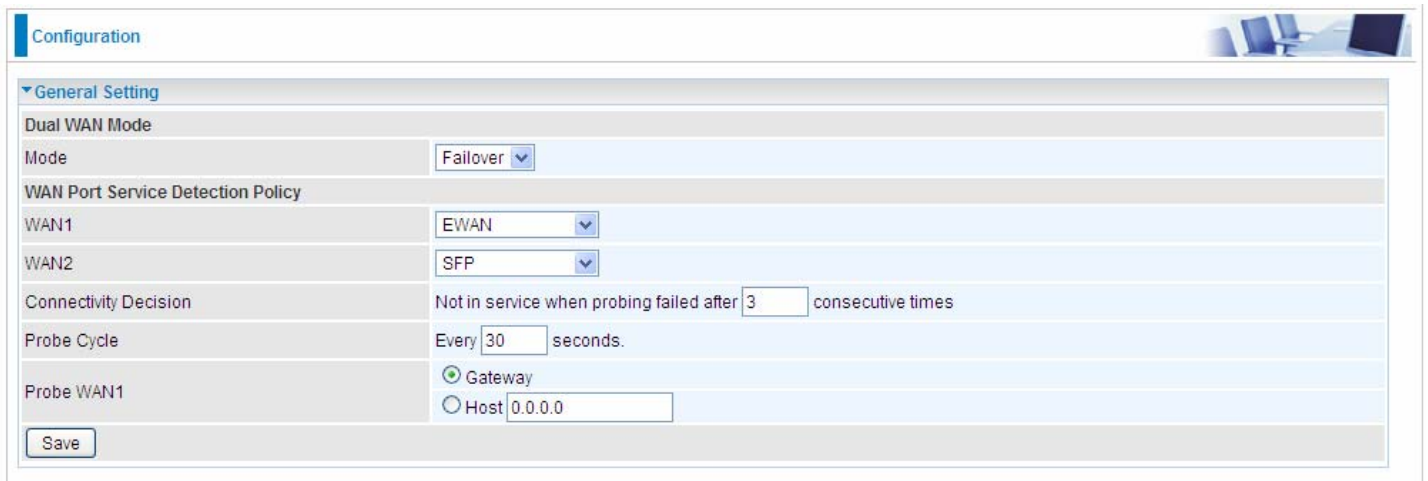
4.4.2.1 General Setting



The screenshot shows the 'Configuration' page with the 'General Setting' tab selected. Under 'Dual WAN Mode', the 'Mode' is set to 'Disable'. There are 'SAVE' and 'CANCEL' buttons at the bottom.

Select **Failover** to enable the failover/fallback feature or **Load Balance** to make the router work in load balance mode.

➤ Failover



The screenshot shows the 'Configuration' page with the 'General Setting' tab selected. Under 'Dual WAN Mode', the 'Mode' is set to 'Failover'. Below this, the 'WAN Port Service Detection Policy' is configured with the following settings: WAN1 is 'EWAN', WAN2 is 'SFP', Connectivity Decision is 'Not in service when probing failed after 3 consecutive times', Probe Cycle is 'Every 30 seconds', and Probe WAN1 is set to 'Gateway'.

WAN Port Service Detection Policy

WAN1: Select “EWAN”, “SFP” or “3G/4G-LTE USB” for WAN1 (The main WAN).

WAN2: Select the “SFP” or “3G/4G-LTE USB” for WAN2 as backup port if you select “EWAN” as WAN1.

Connectivity Decision: Set how many times of probing failure to switch to backup port.

Probe Cycle: Set the time duration for the **Probe Cycle** to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails. For example, when set to 30 seconds, the probe will be conducted every 30 seconds.

Note:

1) The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle** multiplied by **connection Decision amount** (e.g. From the image above it will be 30 seconds multiplied by 3 consecutive fails, the router will determine failover to WAN2 (backup port)).

2).The fallback 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: Choose the probe policy, to probe gateway or host (users decide themselves)

- ① **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.
- ① **Host:** It will send ping packets to specific host and wait for response in every “Probe Cycle”. The host must be an IP address.

4.4.3 Advanced Setup

Advanced Step provides some advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **QoS**, **IPSEC Setting**, **PPTP Server**, **PPTP Client**, **L2TP**, **Port Isolation** and **Time Schedule** for all advanced users. Please move on to have a picture of what the exact feature is about and how to use it.

BILLION Point-to-Point Fiber Wireless-N VPN VoIP Gateway Powering communications with Security

► Status
► Quick Start
▼ Configuration
 ► Interface Setup
 ► Dual WAN
 ▼ Advanced Setup
 • Firewall
 • Routing
 • NAT
 • Static DNS
 • QoS
 • IPSEC Setting
 • PPTP Server
 • PPTP Client
 • L2TP
 • Port Isolation
 • Time Schedule
 ► VoIP
 ► Access Management
 ► Maintenance
► Language

Configuration

▼ Firewall

Firewall Enabled Disabled

SPI Enabled Disabled

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

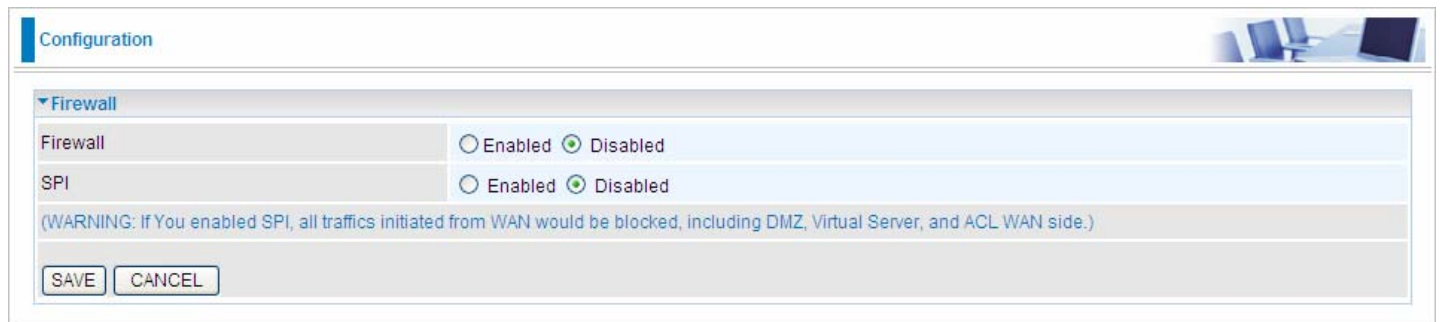
Save

Restart Logout

Copyright © Billion Electric Co., Ltd. All rights reserved.

4.4.3.1 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.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a 'Firewall' section is expanded, showing two settings: 'Firewall' and 'SPI'. Both settings have radio buttons for 'Enabled' and 'Disabled', with 'Disabled' selected for both. A warning message is displayed below the settings: '(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)'. At the bottom of the configuration area, there are 'SAVE' and 'CANCEL' buttons.

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

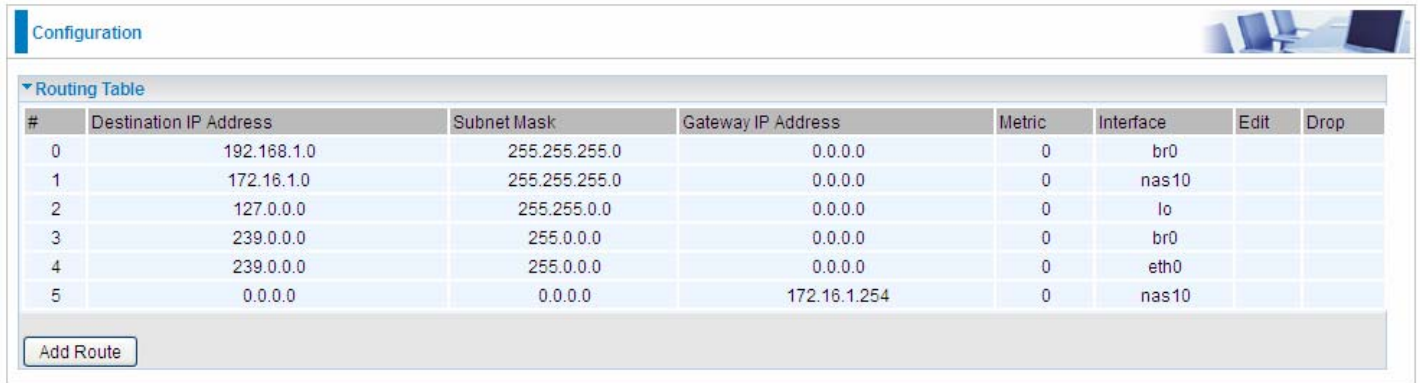
- ① **Enabled:** It activates your firewall function.
- ① **Disabled:** It disables the firewall function.

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

- ① **Enabled:** It activates your SPI function.
- ① **Disabled:** It disables the SPI function.

4.4.3.2 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.



#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	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		

Add Route

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

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

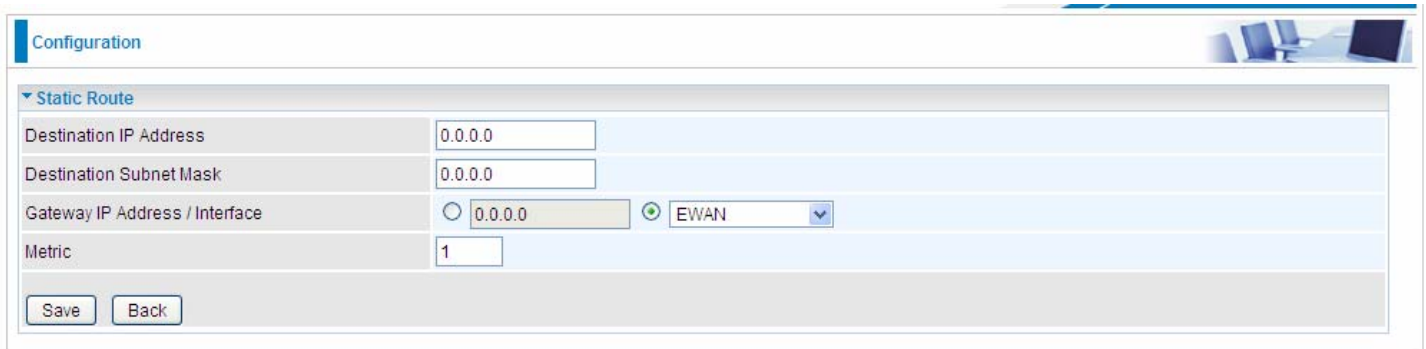
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: 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



The screenshot shows a web-based configuration interface for adding a static route. The page title is "Configuration". Under the "Static Route" section, there are four input fields: "Destination IP Address" (0.0.0.0), "Destination Subnet Mask" (0.0.0.0), "Gateway IP Address / Interface" (radio button for 0.0.0.0 and a dropdown menu for EWAN), and "Metric" (1). At the bottom, there are "Save" and "Back" buttons.

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	<input type="radio"/> 0.0.0.0 <input checked="" type="radio"/> EWAN
Metric	1

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

Destination 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.

4.4.3.3 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 Passthrough”, “SIP ALG”, “DMZ” and “Virtual Server” provided to solve these nasty problems.

Configuration	
▼ NAT	
NAT Status	Enable
ALG	
VPN Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DMZ / Virtual Server	
Interface	EWAN
DMZ	Edit
Virtual Server	Edit

NAT Status: Enabled. It depends on ISP Connection Type in Internet settings.

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

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: Select to set DMZ/Virtual Server for “EWAN”, “SFP” or “3G/4G-LTE USB”.

Click **DMZ** [Edit](#) or **Virtual Server** [Edit](#) 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.

Configuration	
▼ DMZ	
DMZ for	Single IPs Account/ EWAN
DMZ	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ Host IP Address	0.0.0.0
Save Back	

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

Note: Here you can see the Multiple IPs Account/EWAN. It is the interface set in the previous NAT page.

DMZ:

① **Enabled:** It activates your DMZ function.

① **Disabled:** It disables the 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.

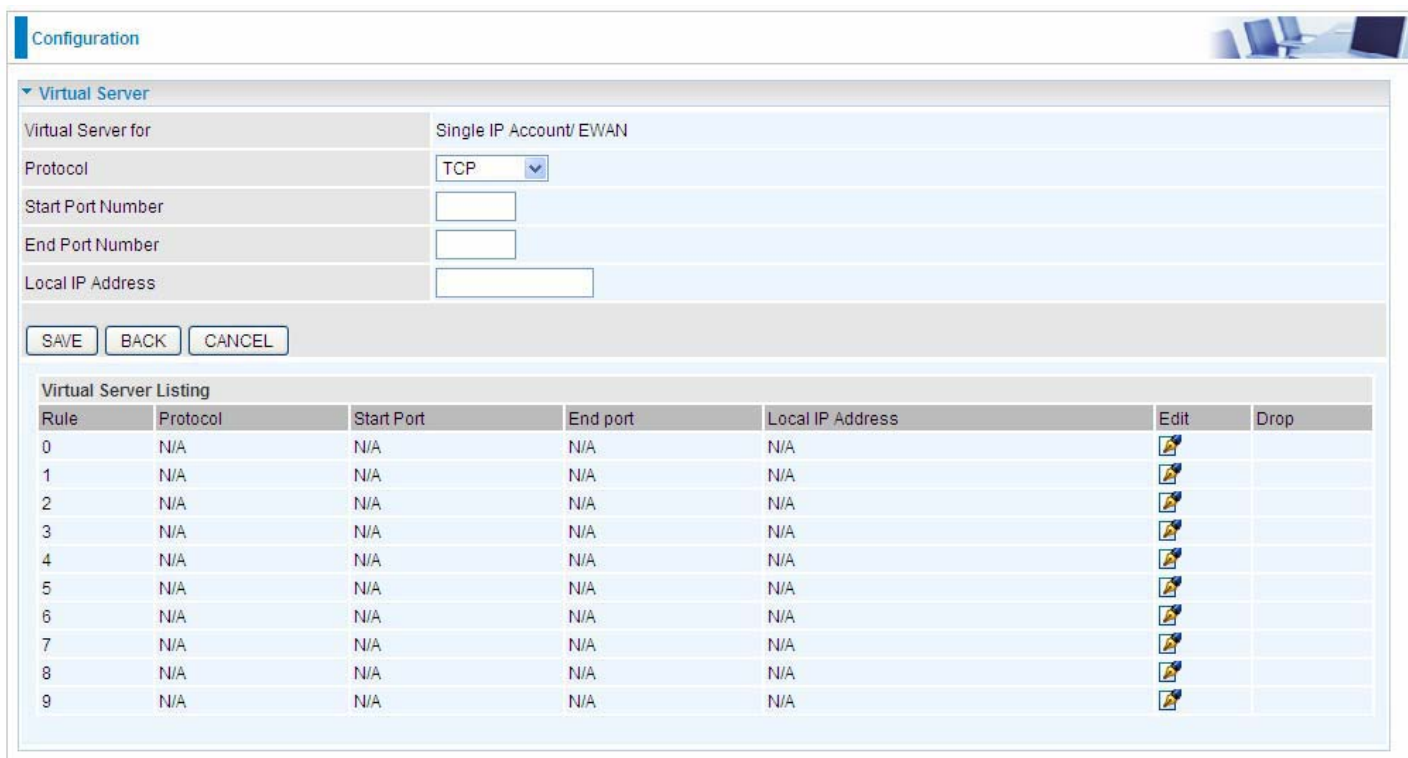
Virtual Server

In TCP/IP 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.



Configuration

Virtual Server

Virtual Server for: Single IP Account/ EWAN

Protocol: TCP

Start Port Number:

End Port Number:

Local IP Address:

SAVE BACK CANCEL

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Edit	Drop
0	N/A	N/A	N/A	N/A		
1	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A		

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 <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.

Configuration

Virtual Server

Virtual Server for: Single IP Account/ EWAN

Protocol: TCP

Start Port Number: 21

End Port Number: 21

Local IP Address: 192.168.1.23

[SAVE] [BACK] [CANCEL]

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Edit	Drop
0	TCP	21	21	192.168.1.23		
1	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A		

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

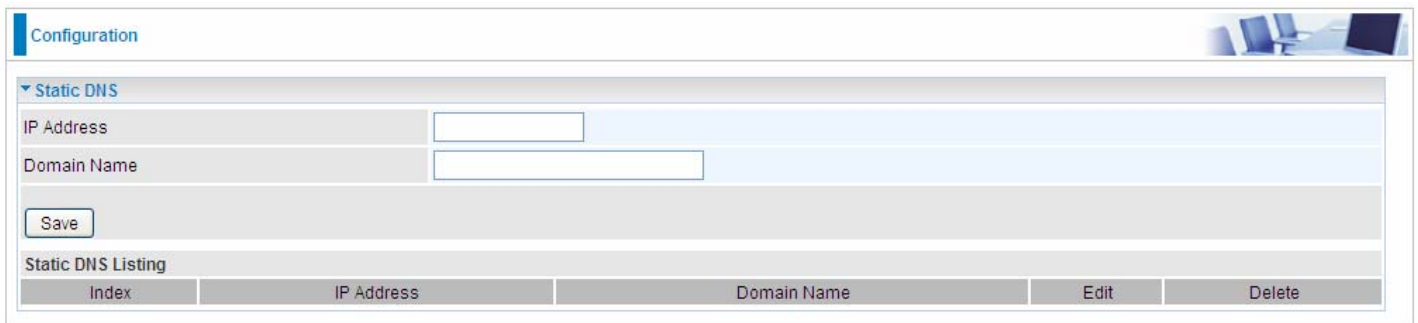
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers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

4.4.3.4 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.



The screenshot shows a web configuration interface. At the top left, there is a 'Configuration' header. Below it, a 'Static DNS' section is expanded, showing two input fields: 'IP Address' and 'Domain Name'. A 'Save' button is located below these fields. At the bottom of the section, there is a 'Static DNS Listing' table with the following columns: Index, IP Address, Domain Name, Edit, and Delete.

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.

4.4.3.5 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 give higher priority to, such as voice data packets given higher priority than web data packets.

Note: EWAN/SFP line speed is based on the rate provided by ISP. But there is no QoS on 3G/4G LTE as the 3G/LTE line speed is various and can not be known exactly.

The screenshot shows a web interface for configuration. At the top, there is a 'Configuration' tab. Below it, the 'Bandwidth Settings' section is expanded. It contains a table for 'Max Bandwidth Provided by ISP' with columns for interface (EWAN, SFP), direction (Upstream Rate, Downstream Rate), a text input field, and unit (kbps). Below this table is a warning message: '(WARNING: These bandwidth settings will be referenced by QoS Rules.)'. The next section is 'Lan Port Rate Control', which has a similar table for LAN1 through LAN4. At the bottom of this section is a 'Save' button. Below the 'Bandwidth Settings' section is the 'QoS Rule Option' section, which has a 'QoS Rule' label and a 'SETTING' button.

Max Bandwidth Provided by ISP			
EWAN	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps
SFP	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps

(WARNING: These bandwidth settings will be referenced by QoS Rules.)

Lan Port Rate Control			
LAN1	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps
LAN2	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps
LAN3	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps
LAN4	Upstream Rate	<input type="text"/>	kbps
	Downstream Rate	<input type="text"/>	kbps

QoS Rule Option

QoS Rule

EWAN Upstream / Downstream: Specify the upstream and downstream rate of the EWAN interface.

SFP Upstream / Downstream: Specify the upstream and downstream rate of the SFP interface.

LAN1-4 Upstream / Downstream: Specify the upstream and downstream rate of the LAN1-LAN4 interface.

Note: The above bandwidth(rate) settings will be taken as a reference by QoS rules.

Click **Save** to save the EWAN rate settings.

Click **SETTING** to add QoS rules (up to **32** QoS rules is offered).

Rule Index: The index marking the rule with a maximum of 32.

Application Name: 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.

- ① **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.
- ① **WAN to LAN:** Control traffic from WAN to LAN (Downstream).

Protocol: Select the supported protocol (Any, TCP, UDP, ICMP, GRE) 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.

DSCP Mapping Table

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

Bandwidth Base: Select SFP or EWAN as the bandwidth base whose upstream/downstream data rate is pre-set in the previous page.

Ratio: The rate percent of each application/policy compared to total traffic on the interface. For example, we want to only allow 20% of the total data (note that the Bandwidth base, the ratio is based on the bandwidth base)for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

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. 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. See [4.4.3.11 Time Schedule](#).

For example, you can give outgoing VoIP traffic more bandwidth to ensure the quality of bandwidth-sensitive audio service.

Configuration

QoS

Rule Index: 1

Application Name: VoIP << -- select

Direction: LAN to WAN Protocol: Any DSCP Marking: Gold service(H)

Bandwidth Base: EWAN SFP Ratio: 20 % Priority Marking: Disable

Internal IP Address: Internal IP Mask: Internal Port:

External IP Address: External IP Mask: External Port:

Time Schedule: Always

Save Delete BACK

QoS Rule Listing

Index	Application	Direction	Protocol	DSCP Marking	Ratio	Priority Marking	Time Schedule
-------	-------------	-----------	----------	--------------	-------	------------------	---------------

4.4.3.6 IPSEC Setting (9800VNX 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.

The screenshot shows a web-based configuration interface for a VPN connection. The title is 'Configuration' and the section is 'VPN Connection Setting'. The interface includes several rows of configuration options:

- Active:** Radio buttons for 'Yes' (selected) and 'No'.
- Connection Name:** A text input field.
- Interface:** A dropdown menu set to 'EWAN'.
- Remote Gateway IP:** A text input field with a note '(0.0.0.0 means any)'.
- Local Access Range:** A dropdown menu set to 'Subnet', followed by 'Local IP Address' (0.0.0.0) and 'IP Subnetmask' (0.0.0.0).
- Remote Access Range:** A dropdown menu set to 'Subnet', followed by 'Remote IP Address' (0.0.0.0) and 'IP Subnetmask' (0.0.0.0).
- IKE Mode:** A dropdown menu set to 'Main', followed by a 'Pre-Shared Key' text input field.
- Local ID Type:** A dropdown menu set to 'Default Wan IP', followed by an 'IDContent' text input field.
- Remote ID Type:** A dropdown menu set to 'Default Wan IP', followed by an 'IDContent' text input field.
- Encryption Algorithm:** A dropdown menu set to 'DES', followed by 'Authentication Algorithm' (MD5) and 'Diffie-Hellman Group' (MODP1024(HD2)).
- IPSec Proposal:** Radio buttons for 'ESP' (selected) and 'AH', followed by 'Authentication Algorithm' (MD5) and 'Encryption Algorithm' (DES).
- Perfect Forward Secrecy:** A dropdown menu set to 'None'.
- Phase 1 (IKE)SA Lifetime:** 480 min(s), followed by 'Phase 2 (IPSec)' 60 min(s).
- PING for keepalive:** A dropdown menu set to 'None', followed by 'PING to the IP(0.0.0.0:NEVER)' 0.0.0.0 and 'Interval' 10 seconds*.
- Disconnection Time after no traffic:** 180 seconds (180 at least).
- Reconnection Time:** 3 min(s) (3 at least).

A note at the bottom states: 'Note *: (0-3600, 0 means NEVER)'. At the bottom left, there are 'SAVE' and 'BACK' buttons.

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.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). 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.

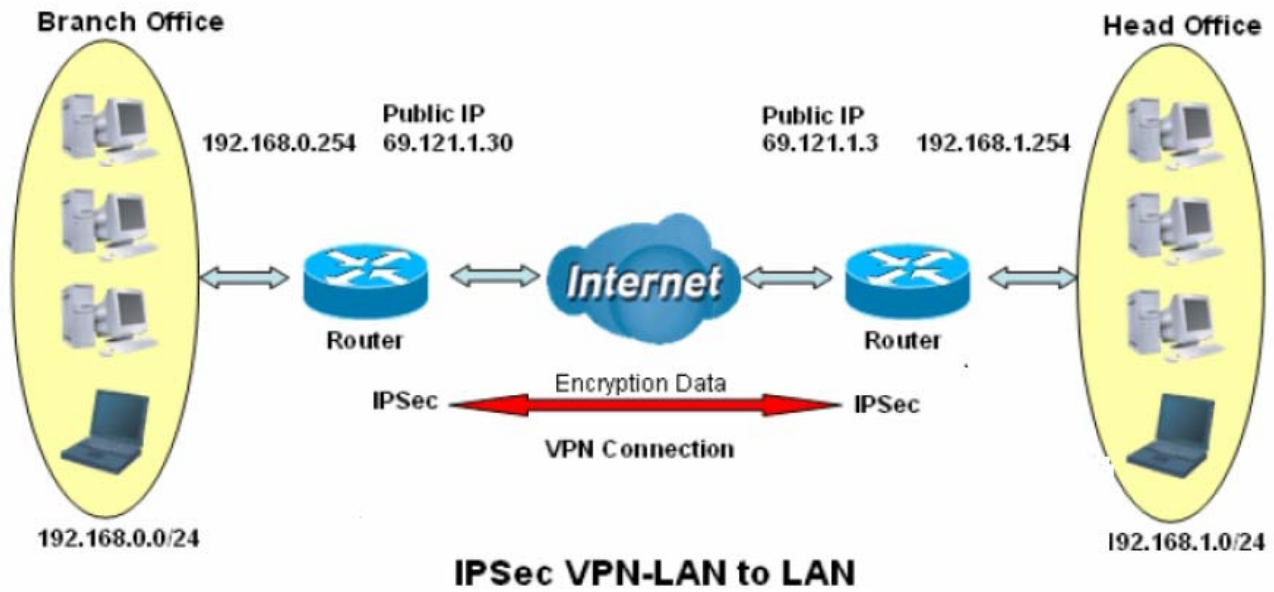
Click **SAVE** to submit the settings.

Examples:

1. LAN-to-LAN connection

Two BiPAC 9800VNXs 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
2	Local Network	
	Subnet	
	IP Address	192.168.1.0
	Netmask	255.255.255.0
3	Secure Gateway Address(Hostanme)	69.121.1.30
4	Remote Network	
	Subnet	
	IP Address	192.168.0.0
	Netmask	255.255.255.0
5	Proposal	
	Method	ESP
	Authentication	MD5
	Encryption	3DES
	Prefer Forward Security	MODP 1024(group2)
	Pre-shared Key	123456

Configuration

VPN Connection Setting

Active Yes No

Connection Name: Interface:

Remote Gateway IP: (0.0.0.0 means any)

Local Access Range: Local IP Address: IP Subnetmask:

Remote Access Range: Remote IP Address: IP Subnetmask:

IKE Mode: Pre-Shared Key:

Local ID Type: IDContent:

Remote ID Type: IDContent:

Encryption Algorithm: Authentication Algorithm: Diffie-Hellman Group:

IPSec Proposal: ESP AH

Authentication Algorithm: Encryption Algorithm:

Perfect Forward Secrecy:

Phase 1 (IKE)SA Lifetime: min(s) Phase 2 (IPSec): min(s)

PING for keepalive: PING to the IP(0.0.0.0:NEVER): Interval: seconds *

Disconnection Time after no traffic: seconds (180 at least)

Reconnection Time: min(s) (3 at least)

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

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(Hostname)	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	

Configuration

VPN Connection Setting

Active Yes No

Connection Name: B-to-H Interface: EWAN

Remote Gateway IP: 69.121.1.3 (0.0.0.0 means any)

Local Access Range: Subnet Local IP Address: 192.168.0.0 IP Subnetmask: 255.255.255.0

Remote Access Range: Subnet Remote IP Address: 192.168.1.0 IP Subnetmask: 255.255.255.0

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 *

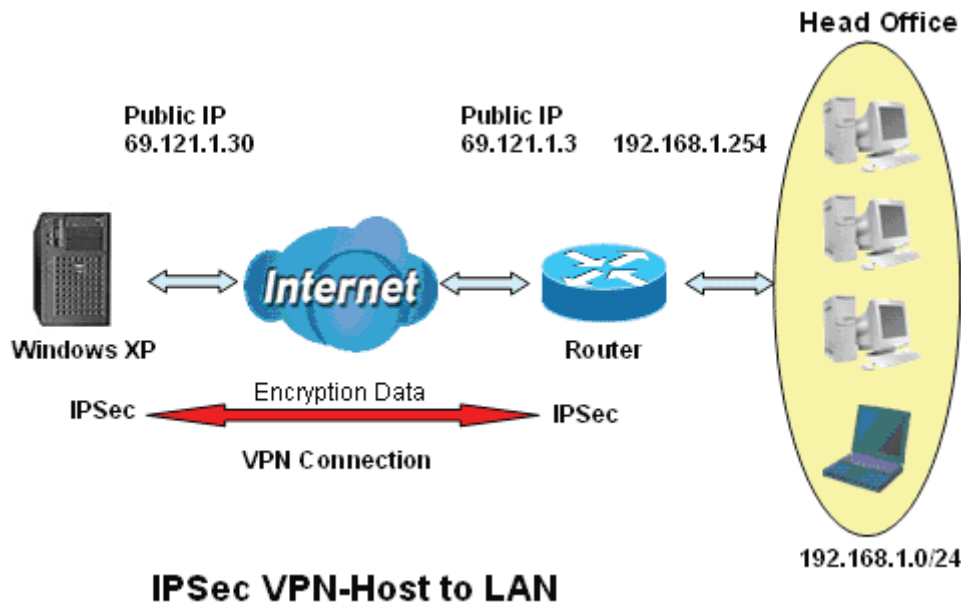
Disconnection Time after no traffic: 180 seconds (180 at least)

Reconnection Time: 3 min(s) (3 at least)

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

2. Host to LAN

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



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	



VPN Connection Setting

Active	<input checked="" type="radio"/> Yes <input type="radio"/> 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	<input checked="" type="radio"/> ESP <input type="radio"/> 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

4.4.3.7 PPTP (9800VNX 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 basic parameters(authentication, encryption, peer address, etc) for PPTP Server and then set the accounts, and 4 accounts or connections are to be set for PPTP Server.

User	Connection Name	Active	Username	Connection Type	AssignIP
		<input type="radio"/> Yes <input checked="" type="radio"/> No			

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.

4.4.3.8 PPTP Client (9800VNX 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	Connection Name	Active	Username	Connection Type	ServerIP
------	-----------------	--------	----------	-----------------	----------

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.

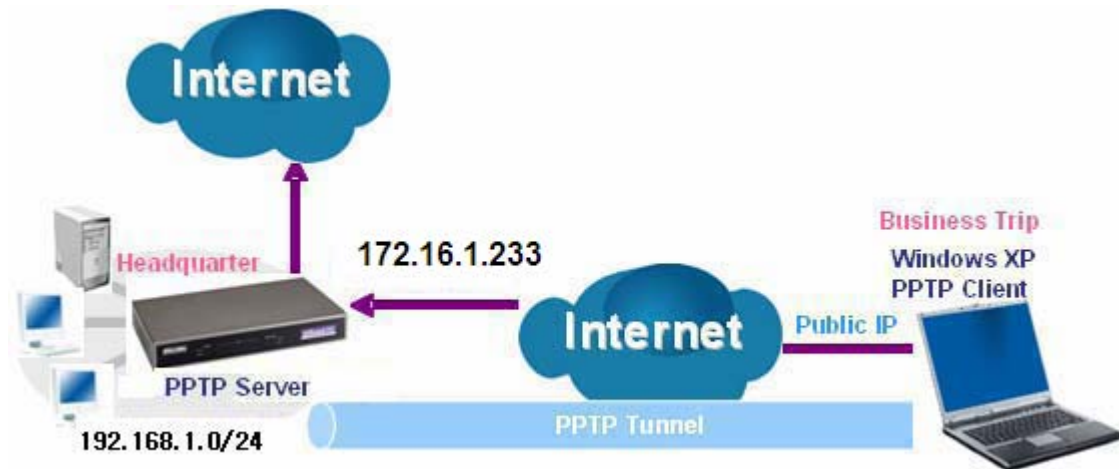
Peer Network IP: Please input the subnet IP for Server peer.

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.

Configuration

▼ PPTP Server

Parameters

Enable Yes No

Auth.Type MPPE 128bit Encryption

MS-DNS 192.168.1.254

User select User1

Connection Name test Active Yes No

Username test Password ●●●●

Connection Type Remote Access Private IP Address Assigned to Dialin user 192.168.1.2

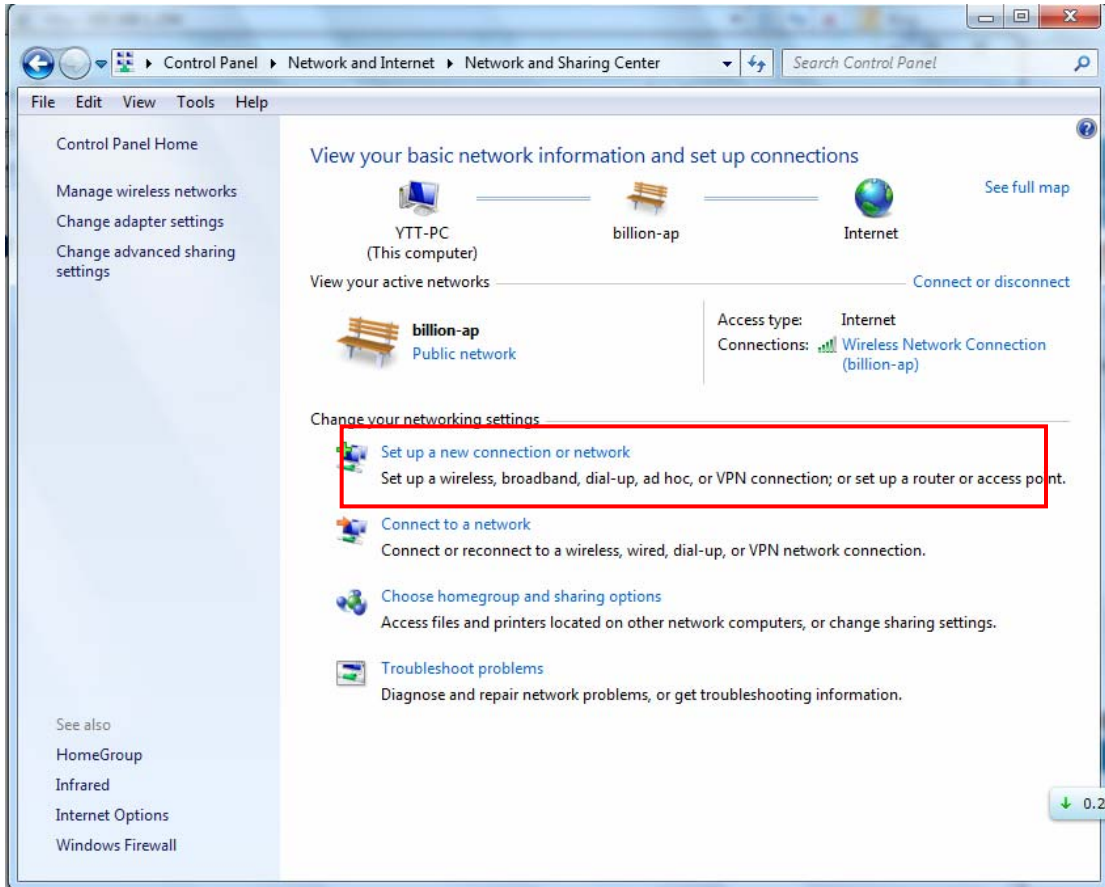
Peer Network IP Netmask

SET DELETE

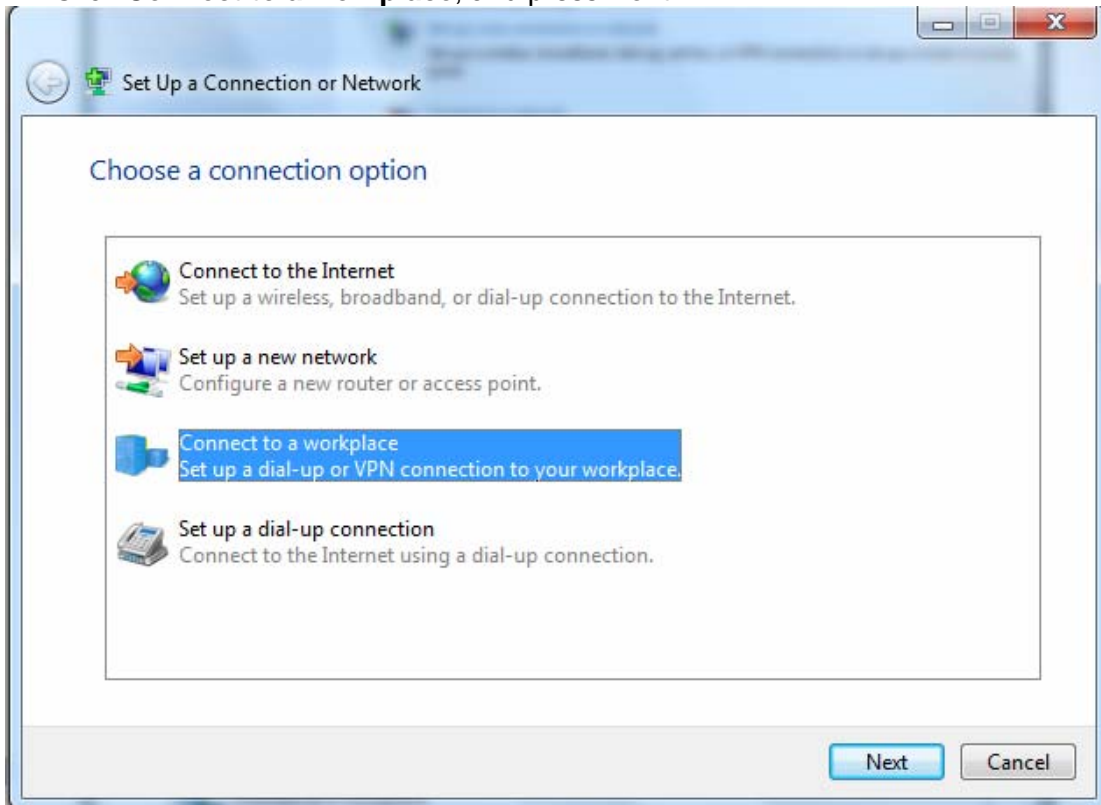
User	Connection Name	Active	Username	Connection Type	AssignIP
User1	test	Yes	test	Remote Access	192.168.1.2

Client Side:

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

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

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

Destination name: VPN Connection

Use a smart card

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

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

Next Cancel

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.233

Destination name: test

Use a smart card

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

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

Next Cancel

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

Connect to a Workplace

Type your user name and password

User name:

Password:

Show characters

Remember this password

Domain (optional):

Create Cancel

Connect to a Workplace

Type your user name and password

User name:

Password:

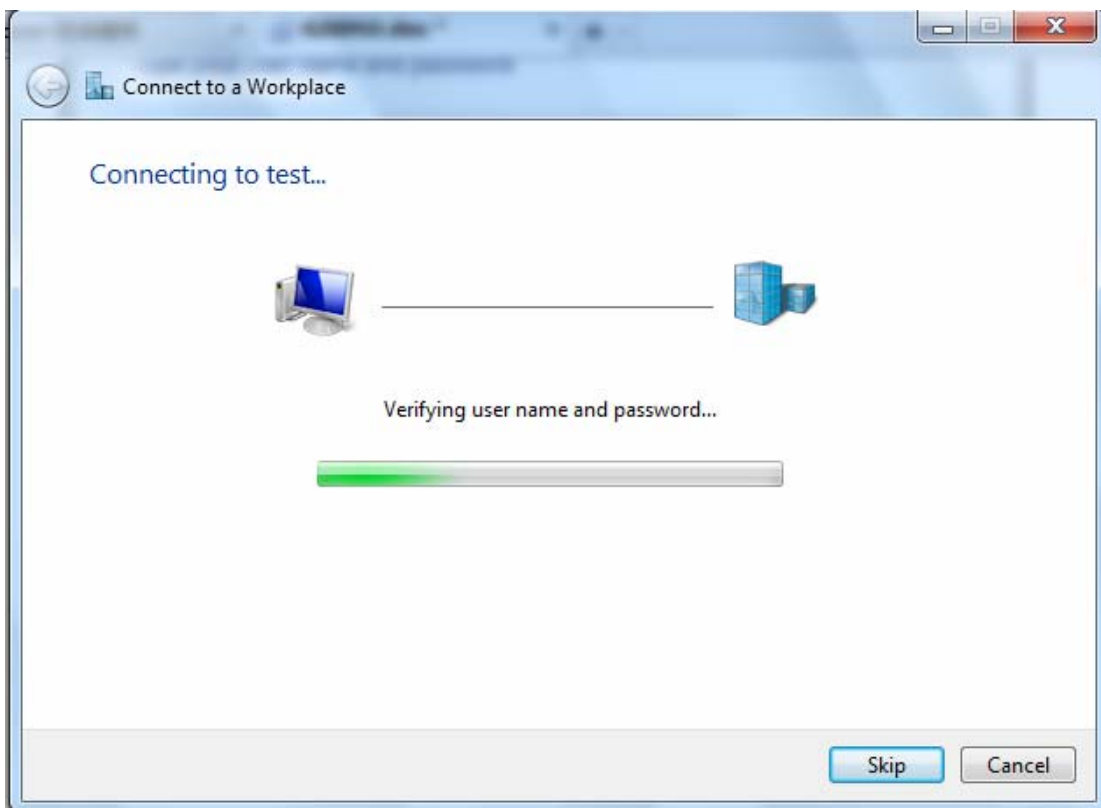
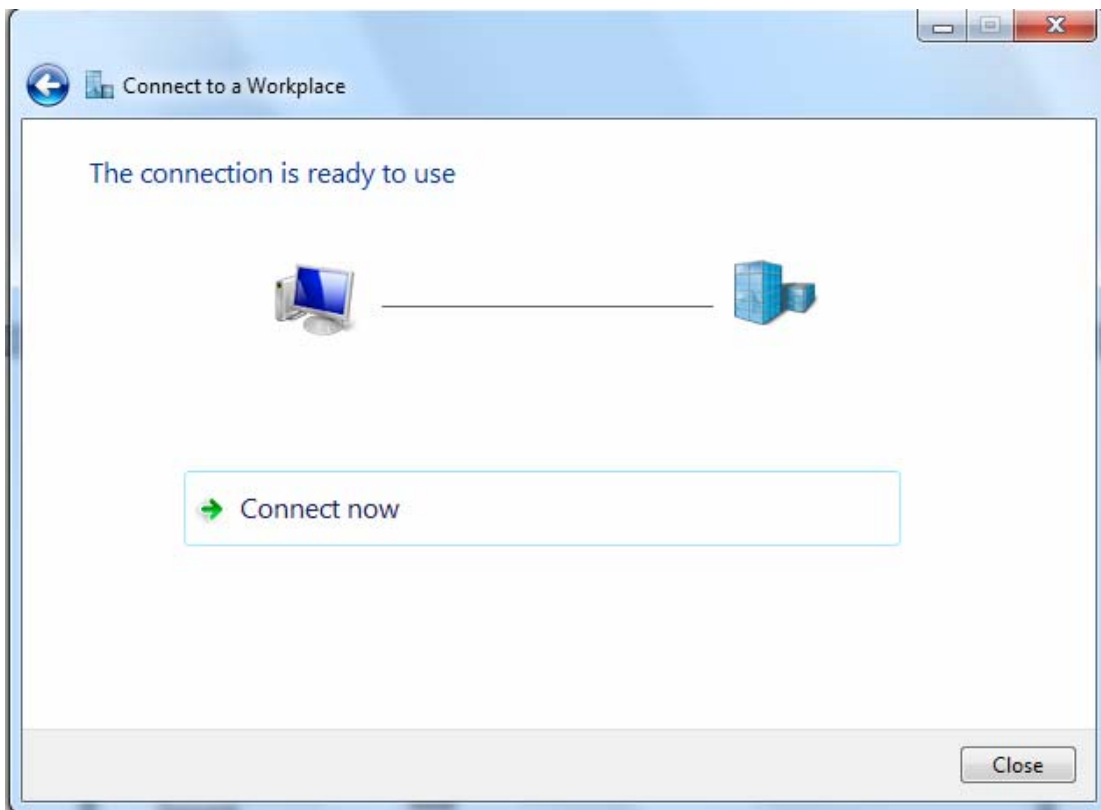
Show characters

Remember this password

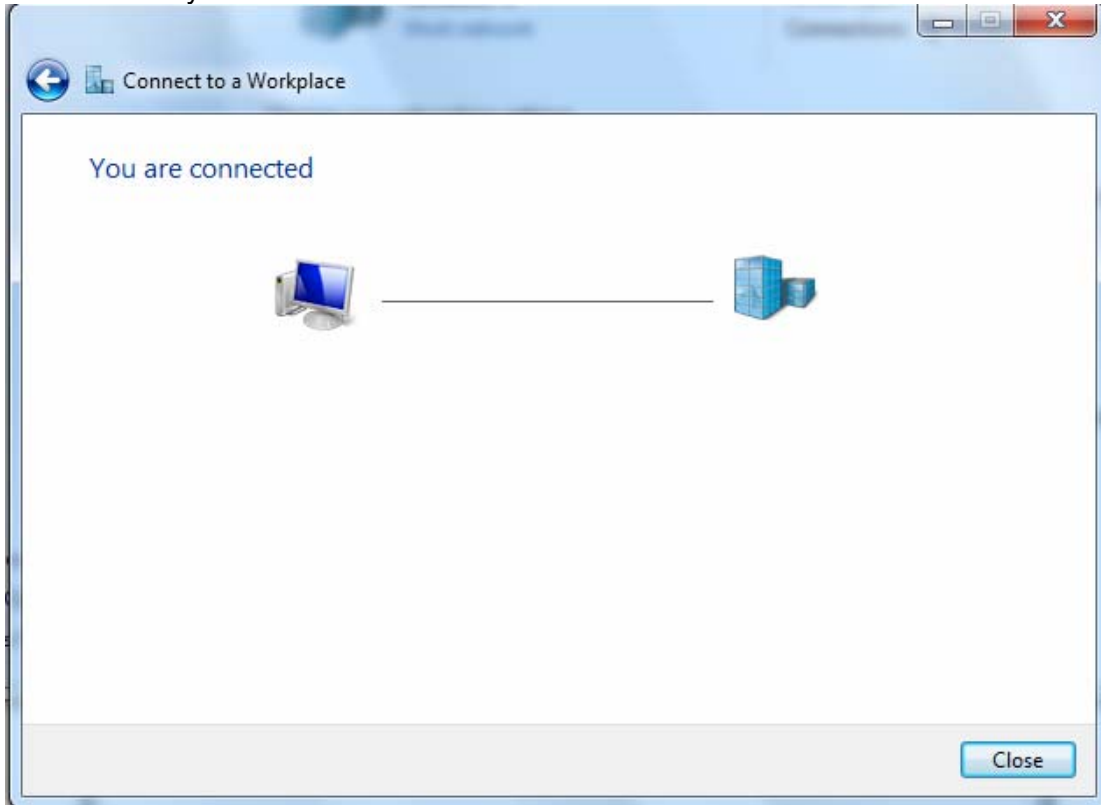
Domain (optional):

Connect Cancel

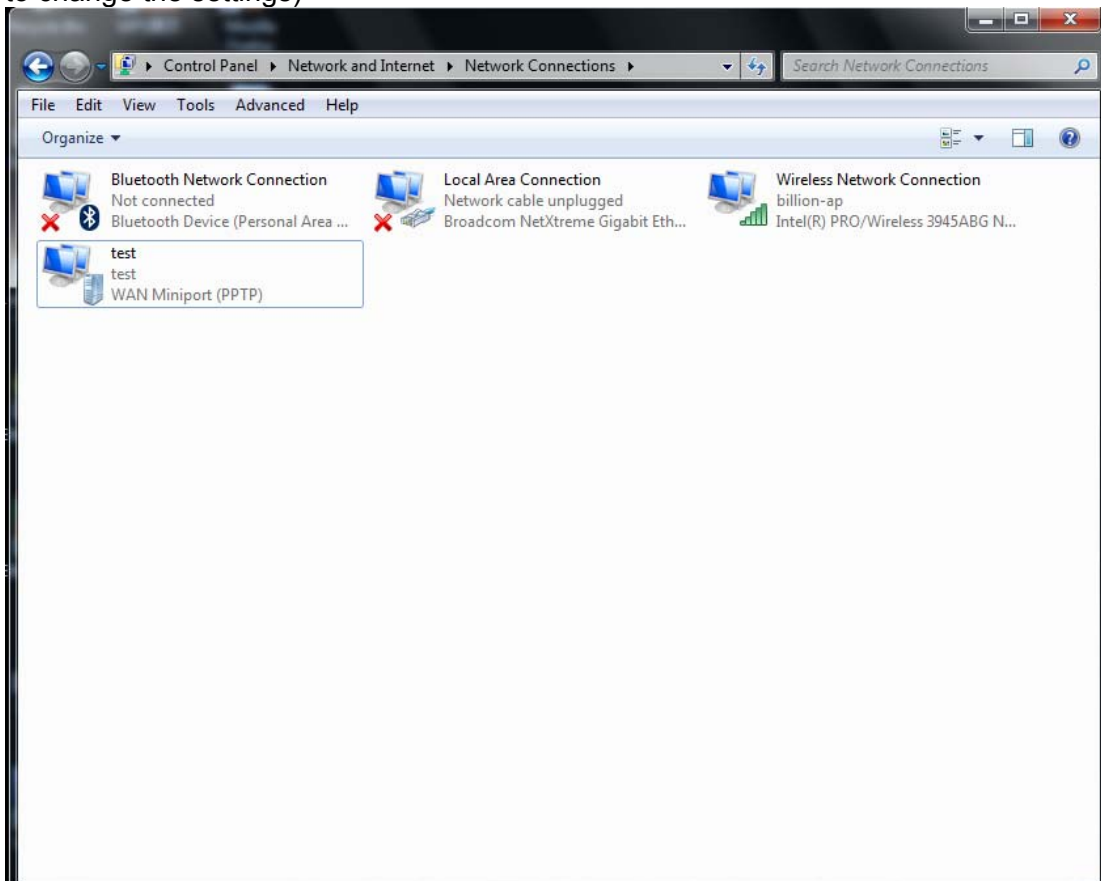
6. Connect to the server.

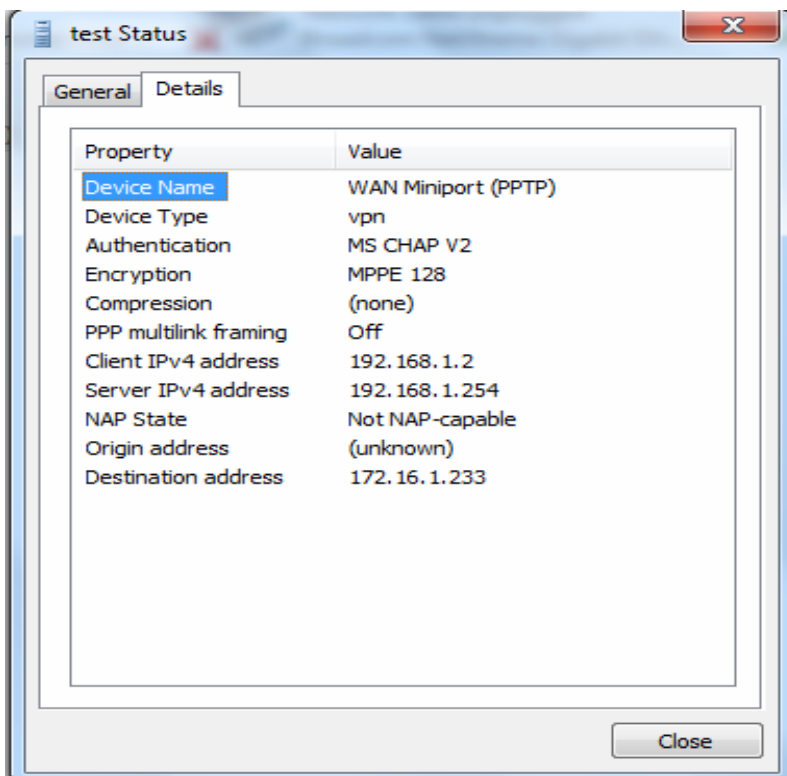
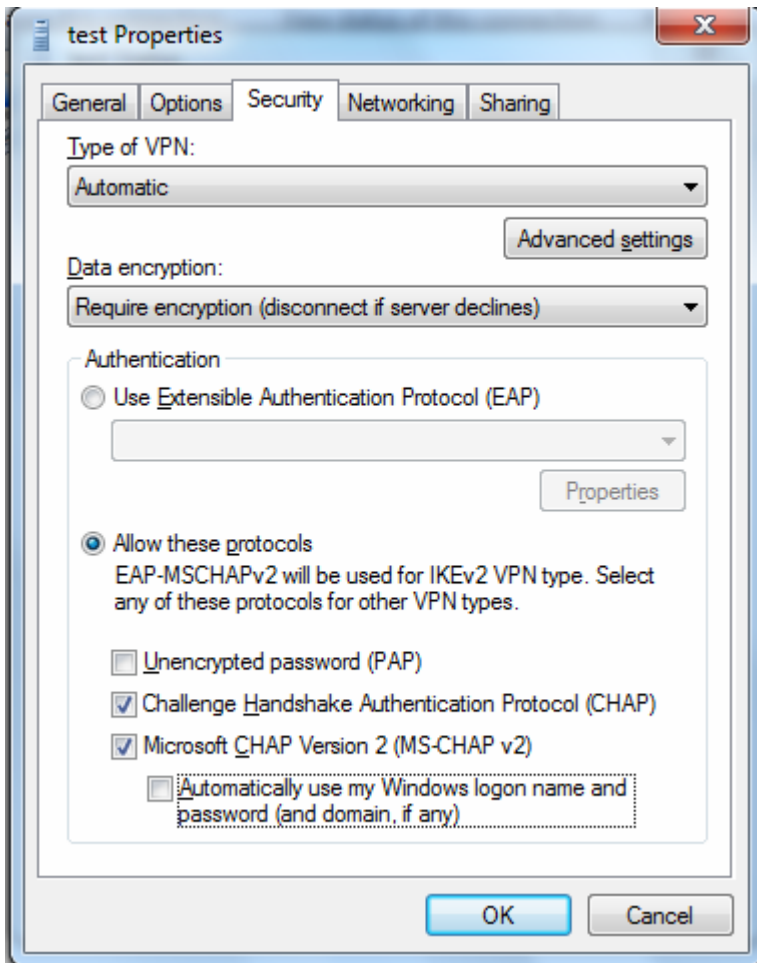


7. Successfully connected.



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

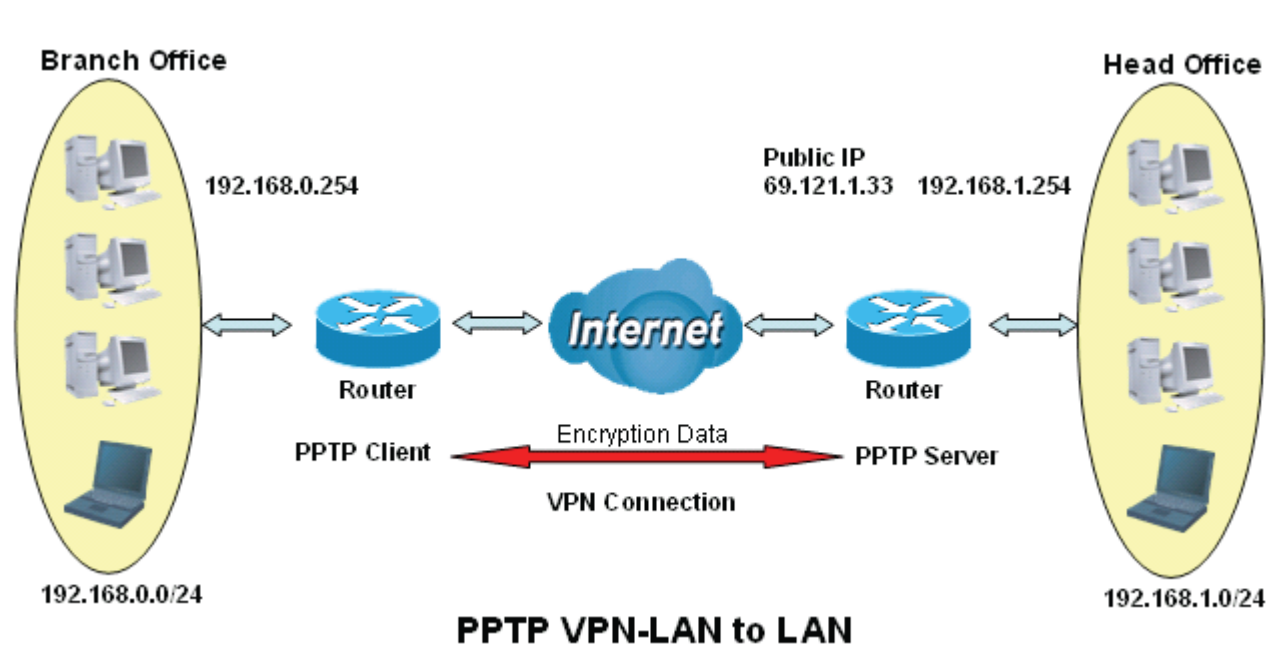




Example: Configuring a LAN-to-LAN PPTP VPN Connection

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

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.

Configuration

▼ PPTP Server

Parameters

Enable Yes No

Auth.Type MPPE 128bit Encryption

MS-DNS 192.168.1.254

User select User1

Connection Name HO Active Yes No

Username test Password

Connection Type LAN to LAN Private IP Address Assigned to Dialin user 192.168.1.2

Peer Network IP 192.168.0.0 Netmask 255.255.255.0


SET DELETE

User	Connection Name	Active	Username	Connection Type	AssignIP
User1	HO	Yes	test	Lan to Lan	192.168.1.2

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>

Client Side: Branch Office

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

Configuration 

PPTP Client

Parameters

User select	User1	Connection Name	BO
Auth.Type	MPPE 128bit Encryption	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Username	test	Password	••••
Connection Type	LAN to LAN	Server IP	69.121.1.33
Peer Network IP	192.168.1.0	Netmask	255.255.255.0

User	Connection Name	Active	Username	Connection Type	ServerIP
User1	BO	Yes	test	Lan to Lan	69.121.1.33

4.4.3.9 L2TP (9800VNX 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

Configuration

L2TP

Name:

Rule Index: 1

Type: Dial in

Active: Enable Disable

Username:

Password:

Private IP Address Assigned to Dialin user:

Auth. Type(Chap means auto): Chap(Auto)

Tunnelauth: Enable

Secret:

Active as default route: Enable

Remote Host Name:

Local Host Name:

Connection Type: Remote Access

SET DELETE CANCEL

L2TP Listing

#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
---	--------	------	-----------------	------	------------	-------------

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.

➤ **Dial In**

Type	Dial in ▼
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Private IP Address Assigned to Dialin user	<input type="text"/>
Auth. Type(Chap means auto)	Chap(Auto) ▼
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	Remote Access ▼

Active: To enable or disable the tunnel.

Username: Please input the username for this account.

Password: Please input the password for this account.

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.

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 peer network information, such as network address and netmask.

➤ **Dial Out**

Type	Dial out ▼
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Server IP Address	<input type="text"/>
Auth. Type(Chap means auto)	Chap(Auto) ▼
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	Remote Access ▼

Active: To enable or disable the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Server IP Address: Enter the IP address of your VPN Server.

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: 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.

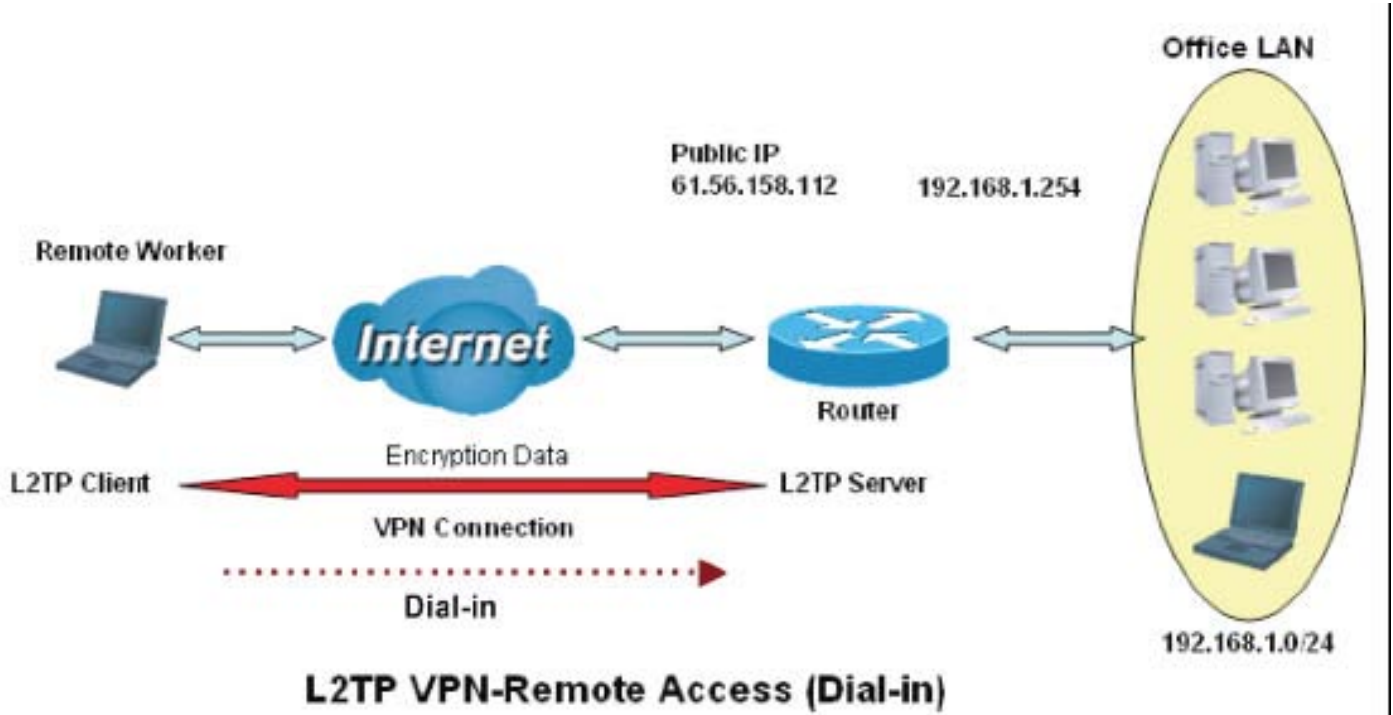
Local Host Name: Enter hostname of Local VPN device that is connected / establishes a VPN tunnel.

Connection Type: Remote Access or LAN to LAN. If “LAN to LAN” is selected, enter the peer 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.

Configuration

L2TP

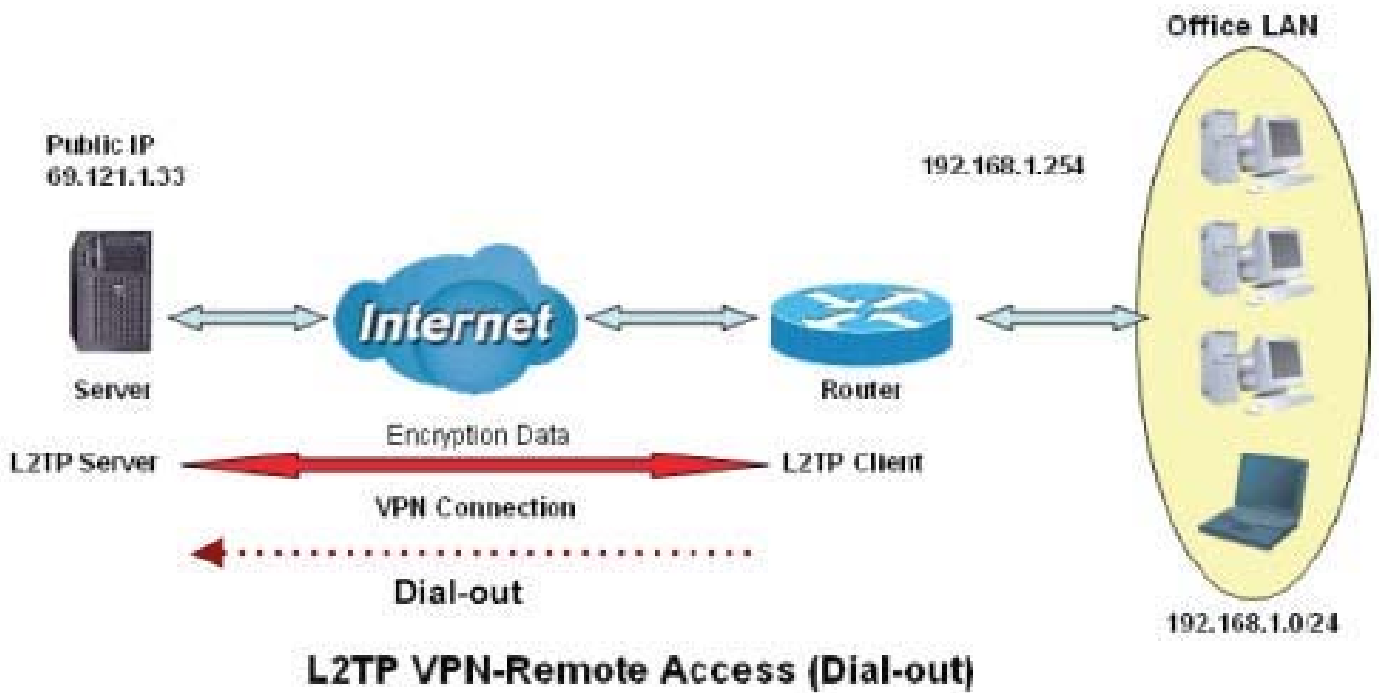
Name	VPN_Server
Rule Index	1
Type	Dial in
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Private IP Address Assigned to Dialin user	192.168.1.200
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Remote Access

#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Server	remote access	dialin	chap	

Function	Value	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.



Configuring L2TP VPN in the Office

Configuration

▼ L2TP

Name	VPN_Client
Rule Index	1
Type	Dial out
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Server IP Address	69.121.1.33
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Remote Access

L2TP Listing

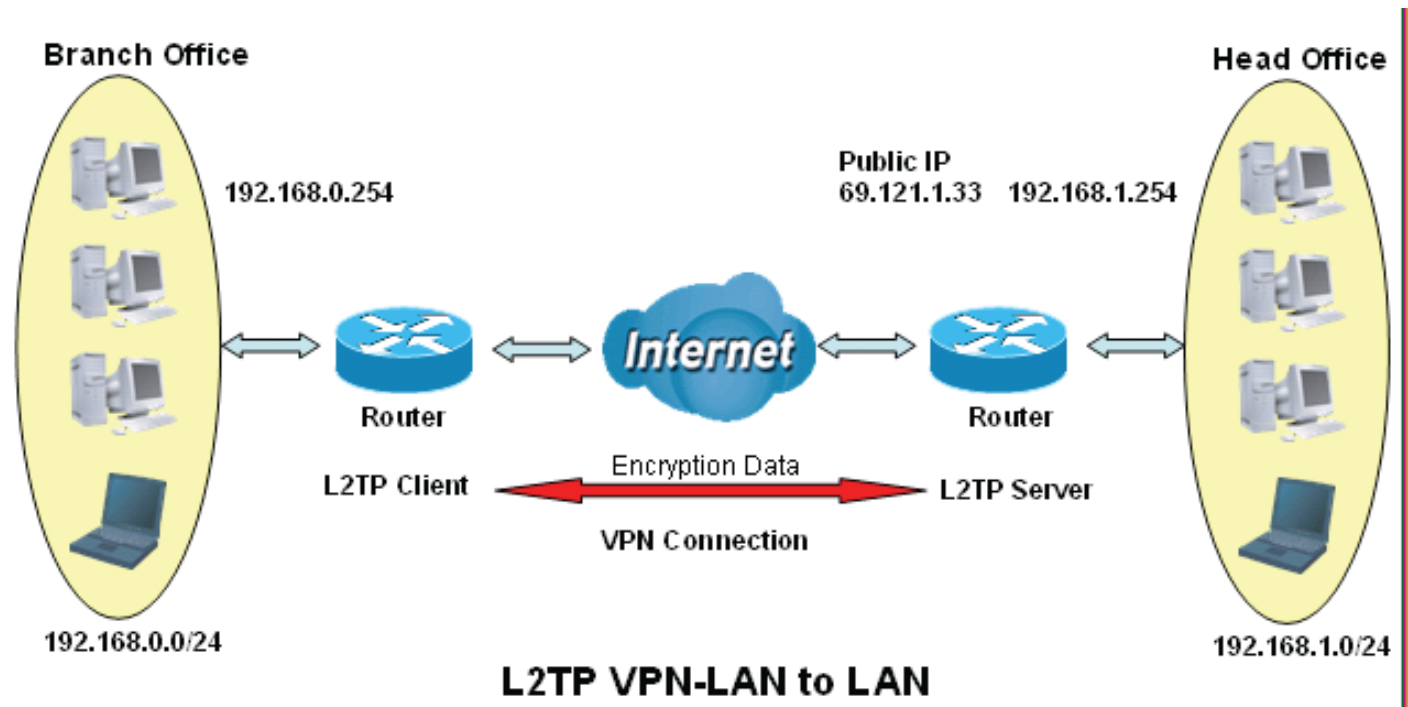
#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Client	remote access	dialout	chap	

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.

▼ L2TP

Name	VPN_Server
Rule Index	1
Type	Dial in
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Private IP Address Assigned to Dialin user	192.168.1.200
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Lan to Lan
PeerNetwork	192.168.0.0
Netmask	255.255.255.0

L2TP Listing

#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Server	lan to lan	dialin	chap	192.168.0.0

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.

▼ L2TP

Name	VPN_Client
Rule Index	1
Type	Dial out
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Server IP Address	69.121.1.33
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Lan to Lan
PeerNetwork	192.168.1.0
Netmask	255.255.255.0

L2TP Listing

#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Client	lan to lan	dialout	chap	192.168.1.0

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
Netmask	255.255.255.0 Head office network
Username	test
Password	test An assigned username and password to authenticate branch office network
Auth. Type	Chap (Auto) Keep this as the default value for most cases

4.4.3.10 Port Isolation

Port isolation is a mechanism to allow or block devices in one port (indicates the LAN1 - LAN3 and WLAN1 - WLAN4, need to enable multiple SSID in wireless section) 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

Port Group	Ethernet LAN				Wireless LAN
	LAN1	LAN2	LAN3	LAN4	WLAN1
Group 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save

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

Port Group	Ethernet LAN				Wireless LAN			
	LAN1	LAN2	LAN3	LAN4	WLAN1	WLAN2	WLAN3	WLAN4
Group 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Save

4.4.3.11 Time Schedule

The Time Schedule supports up to **16** 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.

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Time Index	0						
Name	TimeSlot1						
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00

Time Index: The rule index(0-15) for identifying each timeslot.

Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week". For example, user can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

Start Time: Set the start time of the day, as early as 00:00.

End Time: Set the end time of the day, as late as 24:00.

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Time Index	0						
Name	TimeSlot1						
Day of Week	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	09:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	24:00	18:00	00:00	00:00	00:00	00:00	00:00

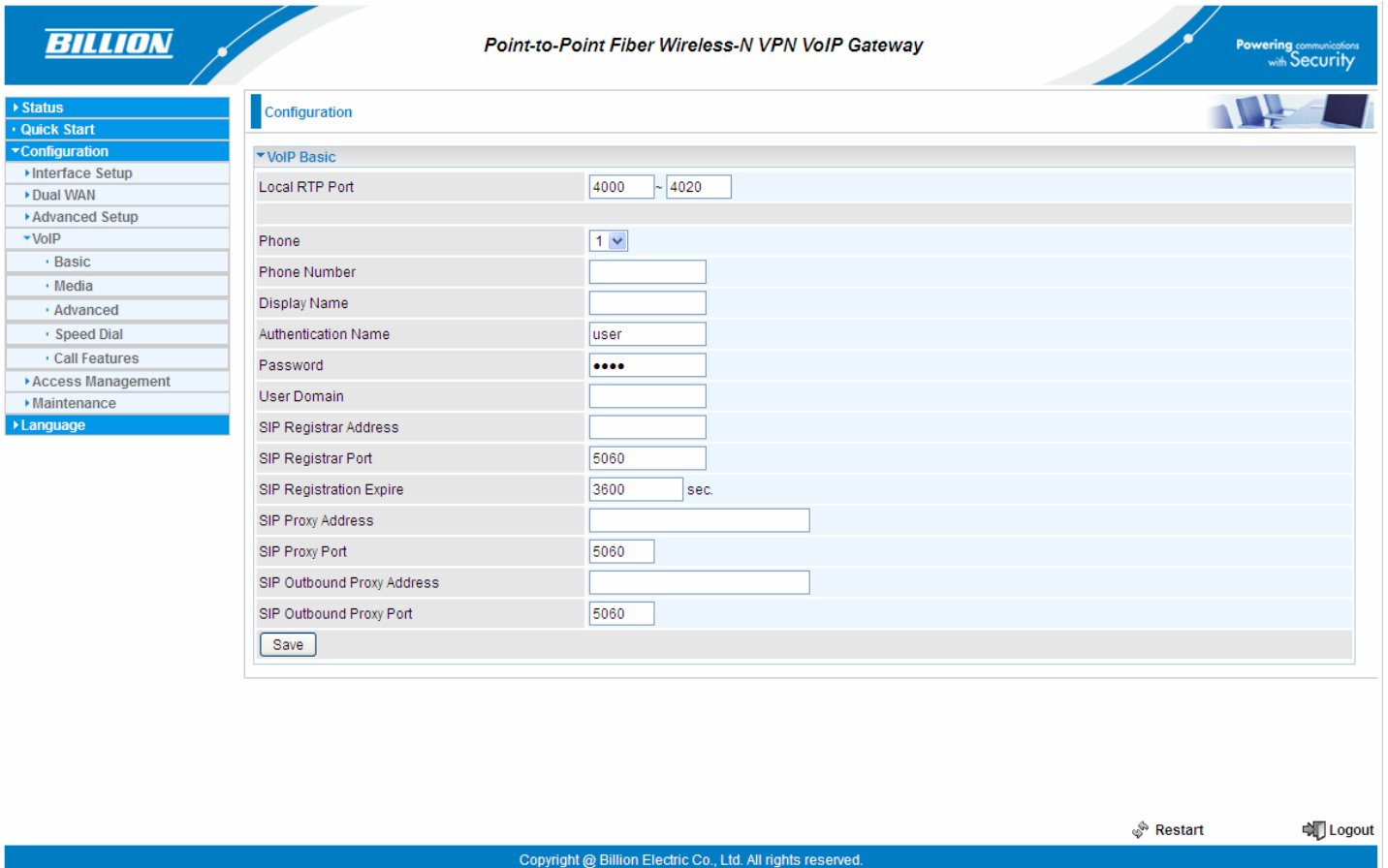
Another TimeSlot2 spanning from 09:00 to 18:00 of Friday

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Time Index	1						
Name	TimeSlot2						
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	09:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	18:00	00:00	00:00

4.4.4 VoIP

VoIP, or Voice over Internet Protocol, enables telephone calls through existing internet connections instead of going through the traditional PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long-distance call, but also top quality voice calls over the internet.

Five sub-items to be covered to configure the VoIP feature, namely **Basic**, **Media**, **Advanced**, **Speed Dial**, **Call Features**.



BILLION Point-to-Point Fiber Wireless-N VPN VoIP Gateway Powering communications with Security

Configuration

VoIP Basic

Local RTP Port 4000 ~ 4020

Phone 1

Phone Number

Display Name

Authentication Name user

Password

User Domain

SIP Registrar Address

SIP Registrar Port 5060

SIP Registration Expire 3600 sec.

SIP Proxy Address

SIP Proxy Port 5060

SIP Outbound Proxy Address

SIP Outbound Proxy Port 5060

Save

Restart Logout

Copyright @ Billion Electric Co., Ltd. All rights reserved.

4.4.4.1 Basic

Register to a SIP service provider is an essential step before making the VoIP call. Users can find out SIP service provider, and register a SIP account, jotting down the registration information and configuring in router.

The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a 'VoIP Basic' section is expanded, showing a list of configuration parameters. The 'Local RTP Port' is set to a range of 4000 to 4020. The 'Phone' dropdown menu is set to '1'. The 'SIP Registrar Port' is set to 5060, and the 'SIP Registration Expire' is set to 3600 seconds. The 'SIP Proxy Port' and 'SIP Outbound Proxy Port' are also set to 5060. A 'Save' button is located at the bottom left of the configuration area.

Local RTP Port: Set the local RTP port range used to receive voice packet. The setting is to be applied to the two FXS, name phone 1 and phone 2, and the two FXS share the same local RTP port.

Phone: Select “1”, the following parameters will be applicable to Phone1. In 9800VNX(L), phone 1 and phone 2 are allowed to be of different characteristics, including different SIP registrar. So, user needs to configure individually for phone1 and phone 2.

Phone Number: Set you phone number or outgoing call number, which is usually obtained when registering in your ITSP. It is used for destination to identify which this call is made from.

Display Name: A user-friendly display name for the phone number to be easily identified.

Authentication Name: Set the account used to register, usually the Phone Number.

Password: Set the registering account password.

User Domain: Set the SIP Registrar Domain name you are going to register to, usually just the SIP registrar address.

SIP Registrar Address: Enter the SIP registrar address where offers the service of registering the VoIP account. It is definitely a VoIP server.

SIP Registrar Port: Type the port; it will listen to register requests from VoIP devices.

SIP Registration Expire: Set the time interval. The device can update (usually re-login the account) the VoIP account information with the SIP server very the time interval.

SIP Proxy Address: Enter the SIP proxy address provided by your ITSP. When destination and source phones are not sharing the same SIP registrar domain, the SIP proxy is needed to deliver call information and make the communication through.

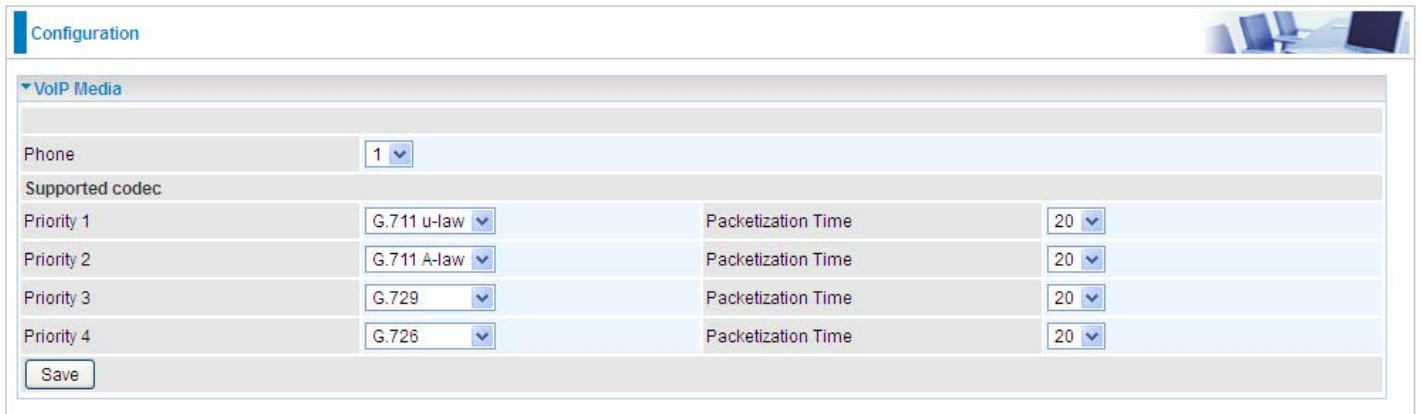
SIP Proxy Port: Set the SIP proxy port.

SIP Outbound Proxy Address: Set the SIP outbound proxy address. It is usually used to realize the communication between two phones when at least one of them is located behind a NAT router.

SIP Outbound Proxy Port: Set the SIP Outbound proxy port.

4.4.4.2 Media

Media offers for kinds of codec, G.711 u-law, G.711 A-law, G.729, G.726, from greatest to lowest in priority.



Configuration			
VoIP Media			
Phone	1		
Supported codec			
Priority 1	G.711 u-law	Packetization Time	20
Priority 2	G.711 A-law	Packetization Time	20
Priority 3	G.729	Packetization Time	20
Priority 4	G.726	Packetization Time	20
<input type="button" value="Save"/>			

Phone: Select to set the following configurations for Phone 1 or Phone2. When phone1 is selected, the following set media codec will be applied to phone1.

- ① **G.711u-Law:** It is a basic non-compressed encoder and decoder technique. μ -LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.
- ① **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample into 8-bit value.
- ① **G.729:** It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- ① **G.726:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.

4.4.4.3 Advanced

Advance section equipment the users with the ability to do some advanced settings to each phone port. Go on to see.

The screenshot shows a web-based configuration interface for VoIP settings. The page is titled 'Configuration' and features a 'VoIP Advanced' section. The settings are as follows:

Setting	Value
Region	CHN-China
Phone	1
Silence Suppression(VAD)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Echo Cancellation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DTMF Transport Mode	Inband
Listening Volume	0 db (-6-6)
Speaking Volume	0 db (-6-6)

A 'Save' button is located at the bottom left of the configuration area.

Region: Select the exact region from the drop-down menu to adjust the phone custom in the exact region, like ring tone, busy tone, dial tone, etc, as different regions may have different phone using traditions. The setting is to be applied to both phone 1 and phone 2.

Phone: Select the phone 1 or Phone 2 to have the following configurations applied to the phone.

Silence Suppression (VAD): Enable to minimize the use of bandwidth by automatically decreasing transmission of background noise when the device detects on voice input by the user on the phone.

Echo Cancellation: Enable to cancel echo for the other side in communication so as to make a clear listening environment. In order to avoid the other side in communication hearing the echo, please enable echo cancellation.

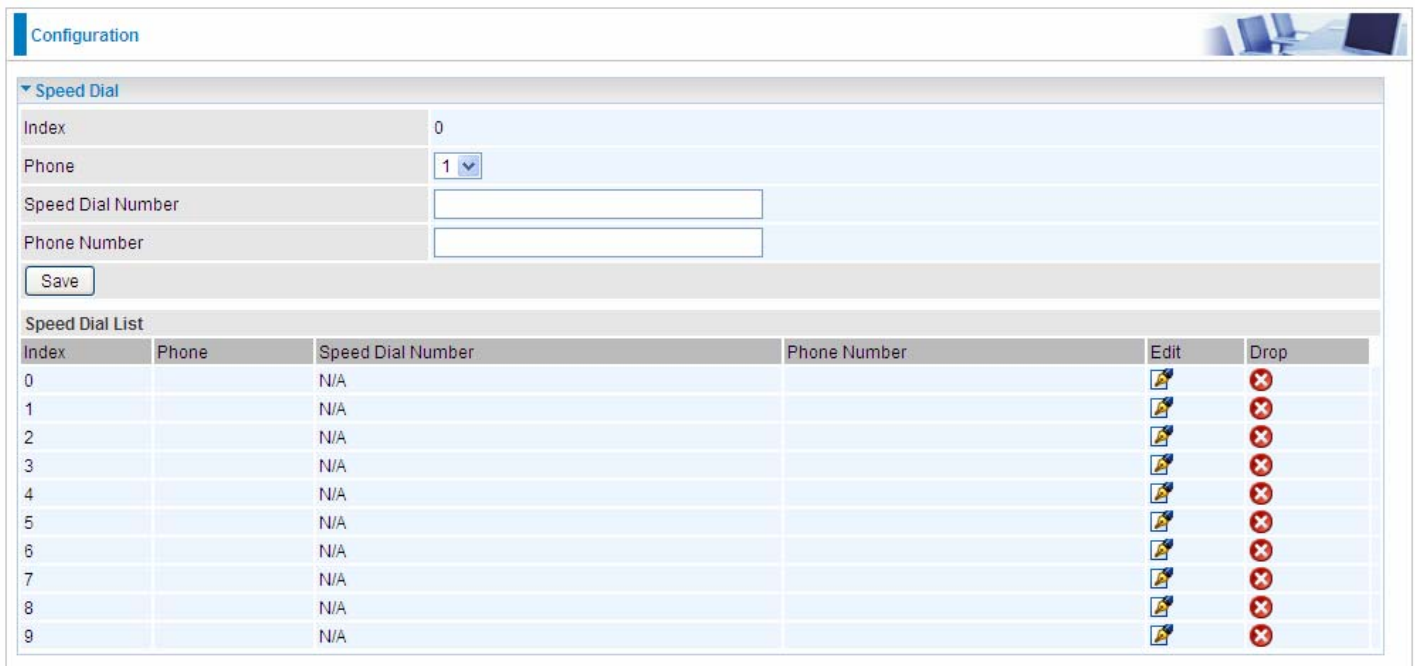
DTMF Transport Mode: Select the DTMF mode.

Listening Volume: Adjust the volume of listener, -6 to 6, from lowest to highest.

Speaking Volume: Adjust the volume of microphone; -6 to 6, from lowest to highest.

4.4.4.4 Speed Dial

Speed Dial comes at hand to store frequently used telephone number(s) that you can press set 'speed dial number' instead of the exact dialing-out number on the phone keyboard to make a quick dialing.



The screenshot shows the 'Configuration' page for 'Speed Dial'. It features a form with the following fields:

- Index:** 0
- Phone:** 1 (selected from a dropdown)
- Speed Dial Number:** (empty text box)
- Phone Number:** (empty text box)

Below the form is a 'Save' button and a 'Speed Dial List' table:

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0		N/A			
1		N/A			
2		N/A			
3		N/A			
4		N/A			
5		N/A			
6		N/A			
7		N/A			
8		N/A			
9		N/A			

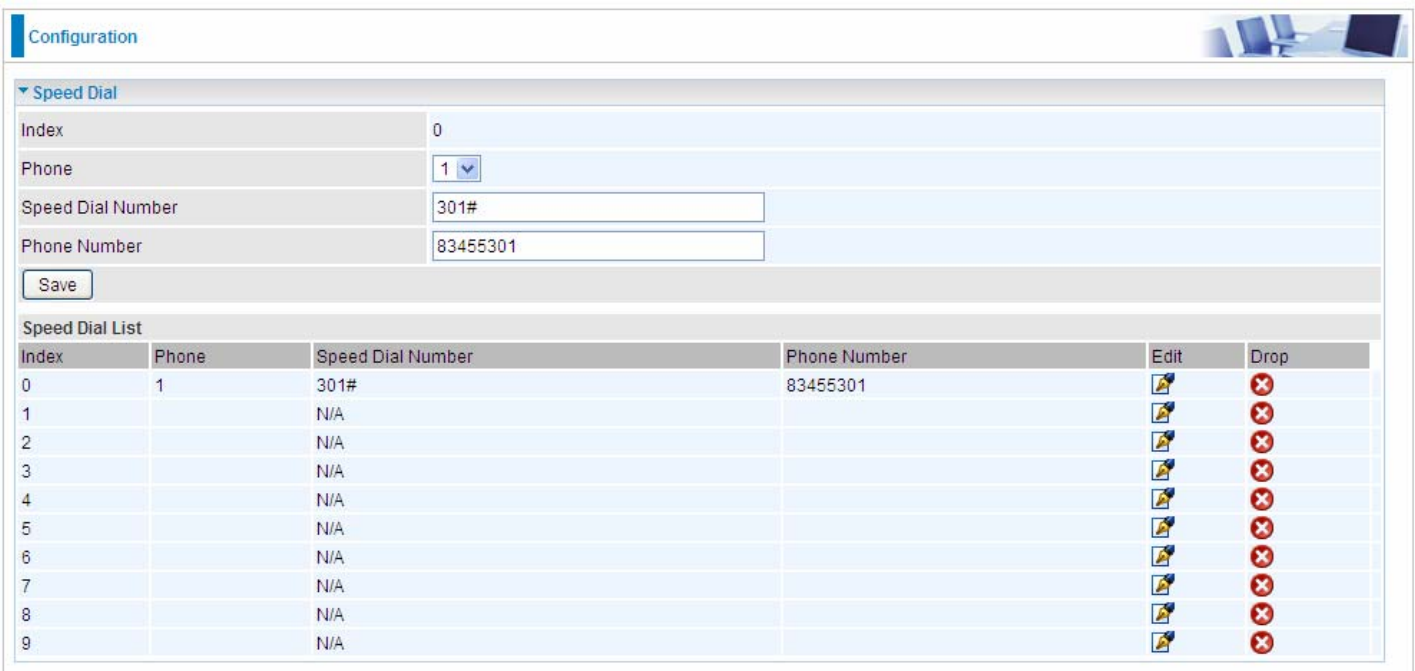
Index: The index to mark the speed dial number mapping, 0-9.

Phone: Select Phone 1 or Phone 2 to have your set speed dial number applied to the phone. If phone 1 is selected, your set speed dial number is about to be applied to phone 1.

Speed Dial Number: Set a easily remembered and simplified number to replace the Phone number, it can be a sequence in varying length from 0, 1,2, 3, 4, 5, 6, 7, 8,9 *. #, but note * or # must be included in the sequence.

Phone Number: The complete destination number

For example, a destination: 83455301. You want to replace it with a friendly speed dial numbr stored in your speed dial list , then set as follows.



The screenshot shows the 'Configuration' page for 'Speed Dial' with the following fields filled:

- Index:** 0
- Phone:** 1 (selected from a dropdown)
- Speed Dial Number:** 301#
- Phone Number:** 83455301

Below the form is a 'Save' button and a 'Speed Dial List' table:

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0	1	301#	83455301		
1		N/A			
2		N/A			
3		N/A			
4		N/A			
5		N/A			
6		N/A			
7		N/A			
8		N/A			
9		N/A			

When you want call 83455301 through phone 1, you can simply dial 301# to make your desired call.

4.4.4.5 Call Features

Call Features provides users with some advanced phone characteristics, including Call waiting, Conference Call, etc.

Call Features	
Phone	1
Call Waiting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Conference Call	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Vertical service code (VSC)	
Pass VSC to Softswitch	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Return Call(Dial number: *69)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Redial(Dial number: *68)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Don't Disturb(Enable: *78, Disable: *79)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

Phone: Select the phone 1 or Phone 2 to have the following characteristics applied to the phone.

Call Waiting: Enable to activate Call Waiting feature. When you are busy on a call with, for example, A, and another call comes in, B, while the Call Waiting feature is enabled, you can hear a hint sound indicating there is another call in for you to decide to answer B by slightly pressing Hook to keep the original call with A.

Conference Call: Enable to allow 3-way conference call. Please note, only 3 parties are allowed (device, A, and B).

Pass VSC to Softswitch: Enable to pass VSC(vertical service code) to the SIP server of ITSP which can provide the VSC service to CPE to achieve call features like Return Call, Call Redial and Don't Disturb for user. Under this circumstance, users need to pay for such service. Disable to let the device itself to make the call features happen, for example, dial *69 to redial the latest incoming call number.

Return Call (Dial number: *69): Dial *69 to redial the latest incoming call number.

Redial (Dial number: *68): Dial *68 to redial the latest outgoing call number.

Don't Disturb (Enable: *78, Disable: *79): Press *78 to enable Don't Disturb feature so as to make it not ring when a call comes in; while press *79 to disable Don't Disturb feature, if a call comes with a ringing indication.

How to establish 3-way conference call



Case 1: Bill and Larry are talking. Bill wants to invite Mark to join a conference call.

Step – 1: Billy and Larry are discussing on the phone. Bill tells Larry that he wants to set up a conference call with Mark.

Step – 2: Bill **presses flash** (hold original call), and Bill hears the dial tone.

Step – 3: Bill calls Mark. Bill and Mark are on a new call.

Step – 4: Bill tells Mark that Mark is invited to join a conference call.

Step – 5: Bill **presses flash** (hold new call) and return to original call.

Step – 4: Bill tells Larry that Mark is on the phone.

Step – 6: Bill **presses flash again** to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Case 2: When Bill and Larry are talking on the phone, Bill received a phone call from Mark. Bill decided to ask Mark to join the conference call.

Step – 1: Bill and Larry on a call, then Mark dials Bill and Bill hears a waiting tone.

Step – 2: Bill **presses flash** and picks up the call waiting call.

Step – 3: Bill tells Mark that he and Larry are talking on the phone, they can have a conference call.

Step – 4: Bill **presses flash** to hold the call with Mark and return to original call with Larry.

Step – 5: Bill tells Larry that it is Mark and he wants to set up a conference with Mark.

Step – 6: Bill **presses flash again** to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

4.4.5 Access Management

The screenshot shows the configuration interface for a Billion gateway. The top header includes the 'BILLION' logo, the product name 'Point-to-Point Fiber Wireless-N VPN VoIP Gateway', and the slogan 'Powering communications with Security'. A left-hand navigation menu lists various configuration options, with 'Access Management' expanded to show 'Device Management'. The main content area is titled 'Configuration' and contains a section for 'Device Management' with a sub-section for 'Embedded Web Server'. The 'HTTP Port' is set to '80', with a note '(The HTTP portnumber is 80.)'. A 'Save' button is visible below the input field. At the bottom right, there are 'Restart' and 'Logout' buttons. The footer contains the copyright notice: 'Copyright @ Billion Electric Co., Ltd. All rights reserved.'

4.4.5.1 Device Management

Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.

This is a close-up view of the 'Embedded Web Server' configuration section from the previous screenshot. It shows the 'HTTP Port' input field containing the value '80' and the text '(The HTTP portnumber is 80.)' to its right. A 'Save' button is located at the bottom left of this section.

4.4.5.1 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 9800VNX(L) serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.

Configuration

SNMP

SNMP Activated Deactivated

Get Community

Set Community

Trap Manager IP

SNMPv3

SNMPv3 Enable Disable

Username

Access Permissions

Authentication Protocol

Authentication Key (8~31 characters)

Privacy Protocol

Privacy Key (8~31 characters)

Save

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.

Authentication 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.

Authentication Key: Set the authentication key, 8-31 characters.

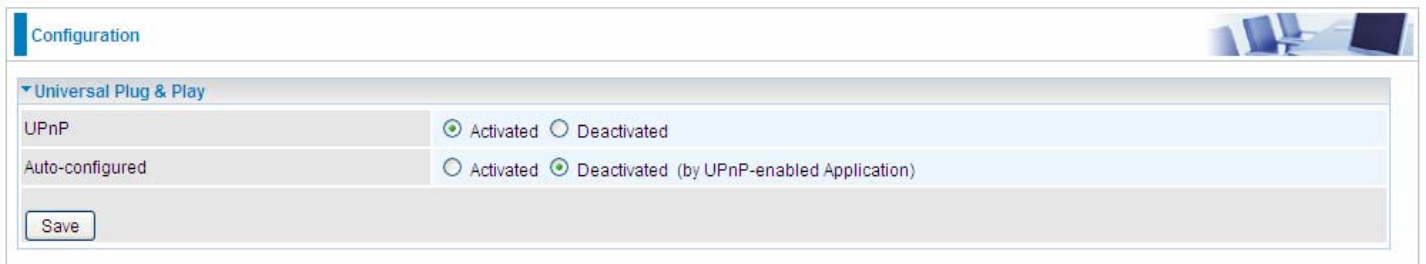
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

4.4.5.2 Universal Plug & Play

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.



The screenshot shows a web configuration interface with a 'Configuration' header. Underneath, there is a section for 'Universal Plug & Play'. It contains two rows of settings:

Setting	Value
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)

At the bottom of the configuration area is a 'Save' button.

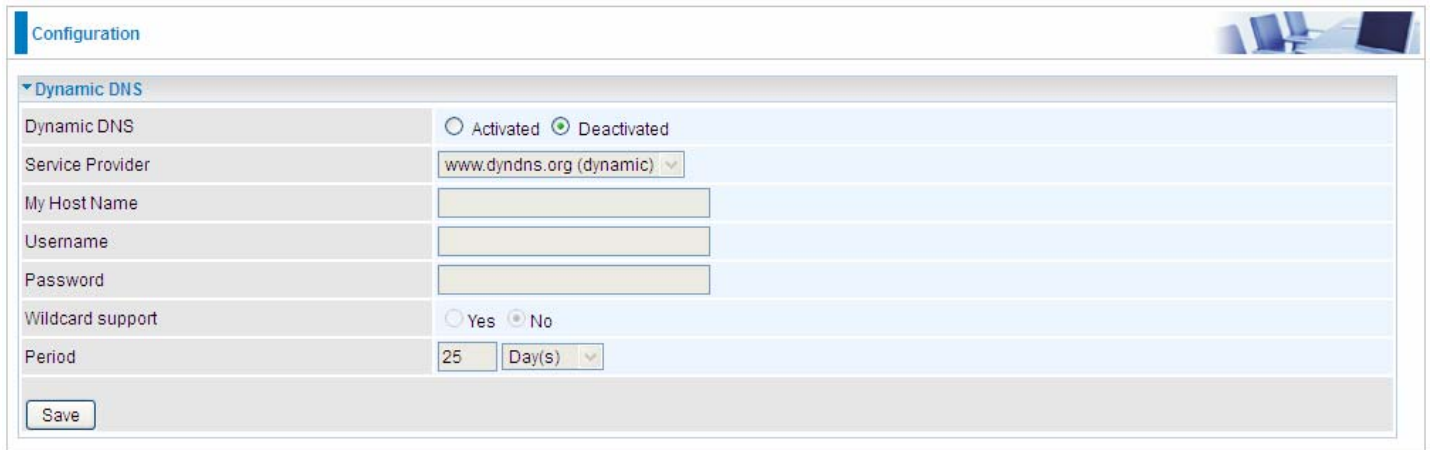
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BIPAC 9800VNX(L)' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BIPAC 9800VNX(L) so that they can communicate through the BIPAC 9800VNX(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.

4.4.5.3 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 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.



Configuration	
Dynamic DNS	
Dynamic DNS	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic)
My Host Name	
Username	
Password	
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s)
<input type="button" value="Save"/>	

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 9800VNX(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 a DDNS

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

User **test1** register a Dynamic Domain Names in DDNS provider <http://www.dyndns.org/> .

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



The image shows a web-based configuration interface for Dynamic DNS. The page title is "Configuration". Under the "Dynamic DNS" section, there are several fields and options:

Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	www.hometest.com
Username	test1
Password	••••
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼

At the bottom left of the configuration area, there is a "Save" button.

4.4.5.4 Access Control

Access Control Listing allows you to determine which services/protocols can access BIPAC 9800VNX(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.

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: This is item number

Active: Select to activate the rule.

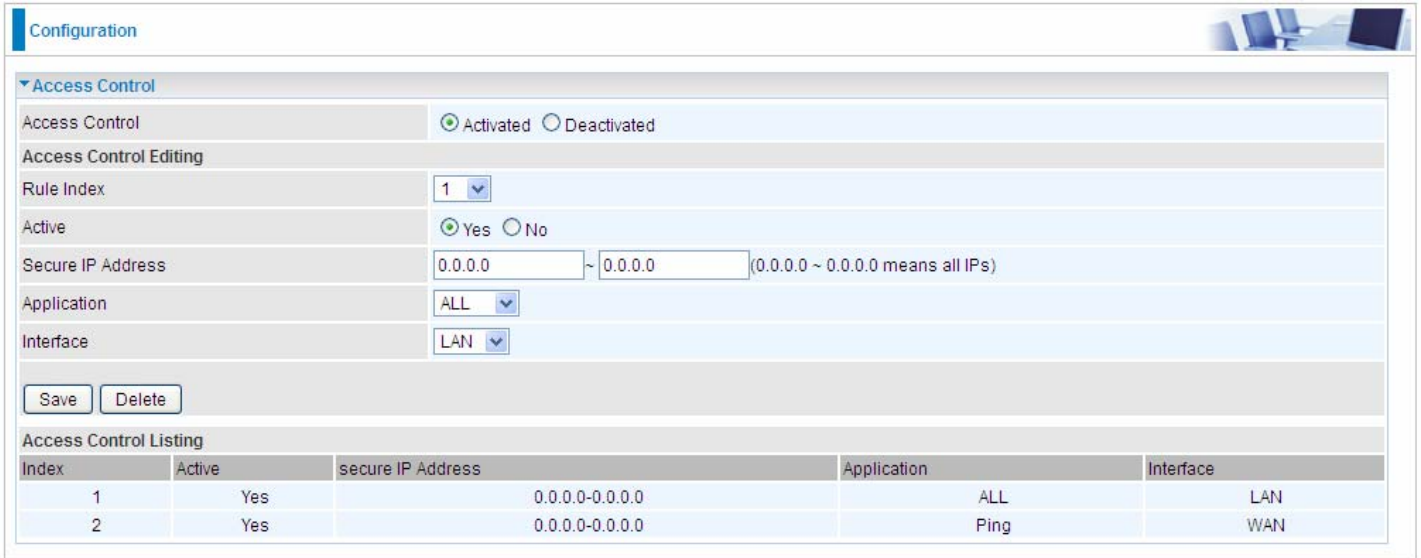
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BIPAC 9800VNX(L). Type an IP address range to restrict access to the client(s) without a matching IP address.

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 “Access Control” has two default rules.

1. Rule 1(Index 1), 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.



Configuration

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 1

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

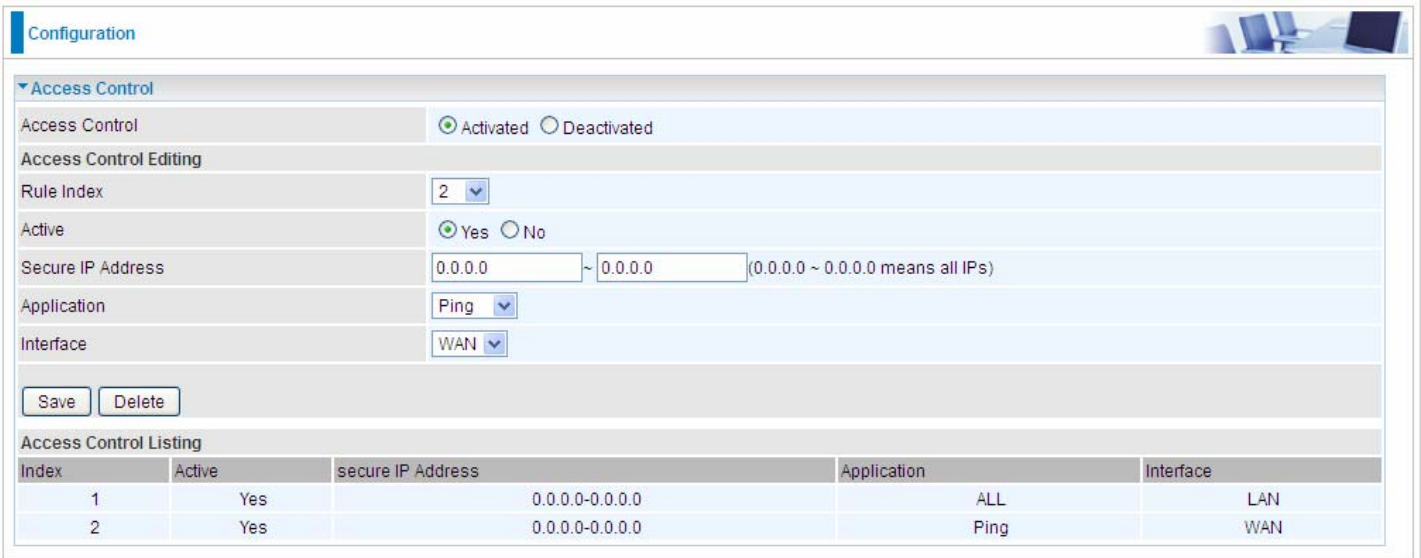
Application: ALL

Interface: LAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

2, Rule 2(Index 2), a ACL rule to open Ping to WAN side.



Configuration

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 2

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application: Ping

Interface: WAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

4.4.5.5 Packet Filter

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

➤ IP & MAC Filter

#	Active	Interface	Direction	Source IP(IPv6) Address/Mask(Prefix)	Destination IP(IPv6) Address/Mask(Prefix)	Source MAC Address	Source Port	Destination Port	DSCP	Protocol
---	--------	-----------	-----------	--------------------------------------	---	--------------------	-------------	------------------	------	----------

■ 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 “IPv4” 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 Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 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 Subnet Mask: Enter the subnet mask of the destination network.

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(IPv6) 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.

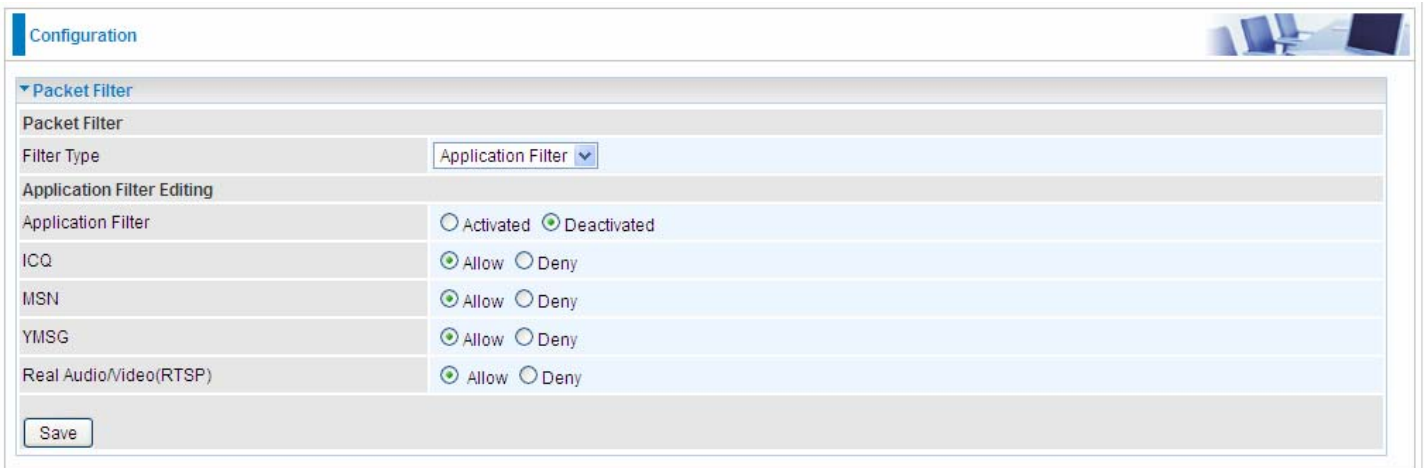
Source Port: The source port number of packets to be monitored.

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



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Packet Filter". The "Filter Type" is set to "Application Filter". Under "Application Filter Editing", there are several options with radio buttons:

Application Filter	Options
Application Filter	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ICQ	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
MSN	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
YMSG	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Real Audio/Video(RTSP)	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

A "Save" button is located at the bottom left of the configuration area.

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

Configuration

Packet Filter

Packet Filter

Filter Type: URL Filter

URL Filter Editing

URL Filter: Activated Deactivated

URL Filter Rule Index: 1

Individual Active: Yes No

URL (Host):

URL Filter Listing

Index	Active	URL
1	Yes	www.yahoo.com

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 press Activated in “URL Filter” 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.

4.4.5.6 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.

The screenshot shows a web-based configuration interface for CWMP (TR-069). The interface is titled "Configuration" and has a sub-section for "CWMP (TR-069)". The "CWMP" status is currently set to "Deactivated". Below this, there are three main sections: "ACS Login Information" with fields for URL, Username, and Password; "Connection Request Information" with fields for Path, Username, and Password; and "Periodic Inform Config" with a "Periodic Inform" status set to "Activated" and an "Interval" of 5000. A "Save" button is located at the bottom left of the configuration area.

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.

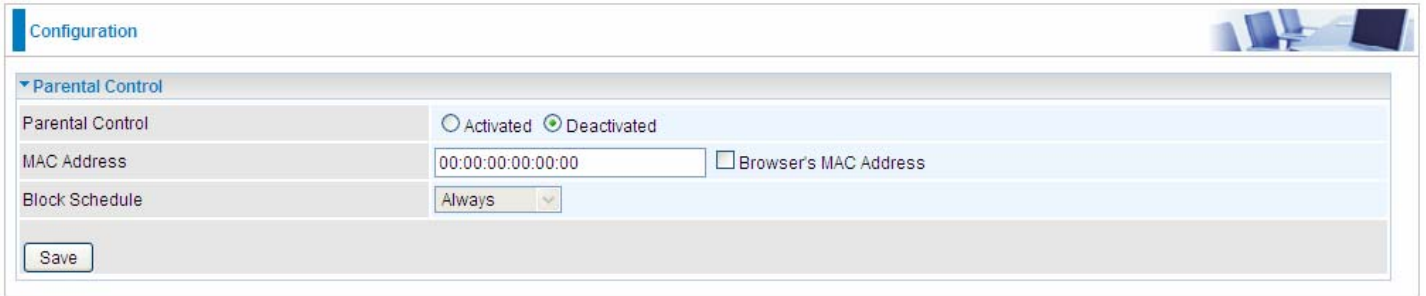
Periodic Inform Config

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.

4.4.5.7 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.



Configuration

Parental Control

Parental Control Activated Deactivated

MAC Address Browser's MAC Address

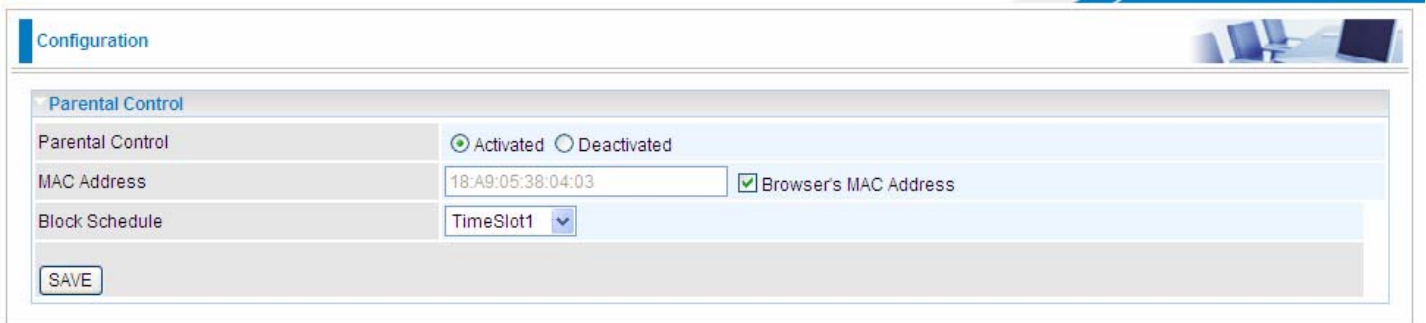
Block Schedule

Save

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.

Block Schedule: Select a timeslot throughout which the above set MAC is restricted to access internet. See [4.4.3.11 Time Schedule](#) to set the exact timeslot.



Configuration

Parental Control

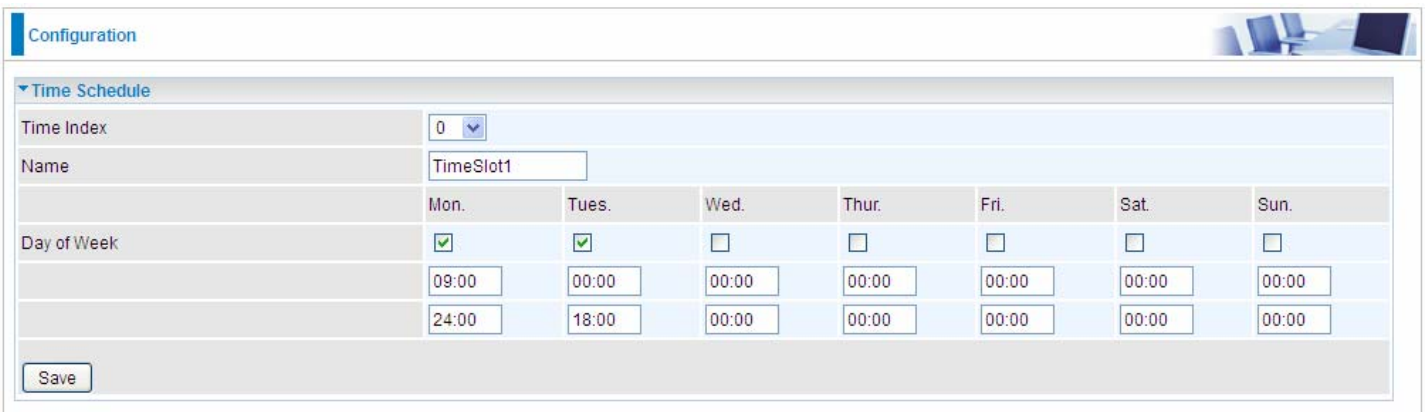
Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

SAVE

Timeslot1 at Time Schedule:



Configuration

Time Schedule

Time Index

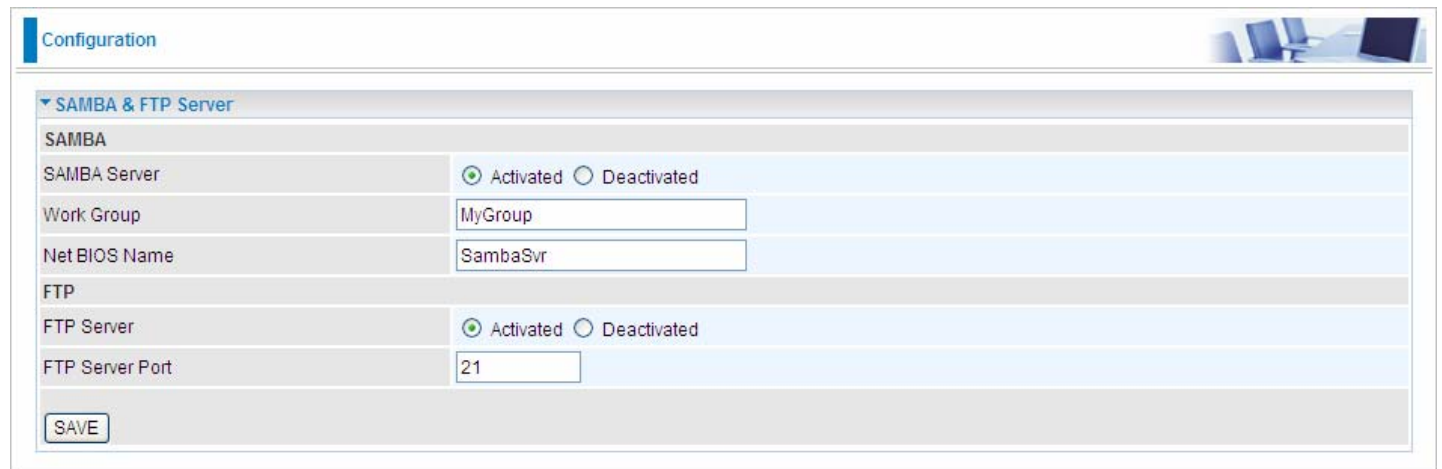
Name

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="text" value="09:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
	<input type="text" value="24:00"/>	<input type="text" value="18:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>

Save

4.4.5.8 SAMBA & FTP Server

Samba and FTP are served as network sharing.



The screenshot shows a configuration interface for SAMBA & FTP Server. The interface is titled "Configuration" and has a sub-section "SAMBA & FTP Server". Under the "SAMBA" section, there are three rows: "SAMBA Server" with radio buttons for "Activated" (selected) and "Deactivated"; "Work Group" with a text input field containing "MyGroup"; and "Net BIOS Name" with a text input field containing "SambaSvr". Under the "FTP" section, there are two rows: "FTP Server" with radio buttons for "Activated" (selected) and "Deactivated"; and "FTP Server Port" with a text input field containing "21". A "SAVE" button is located at the bottom left of the configuration area.

SAMBA Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft 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.

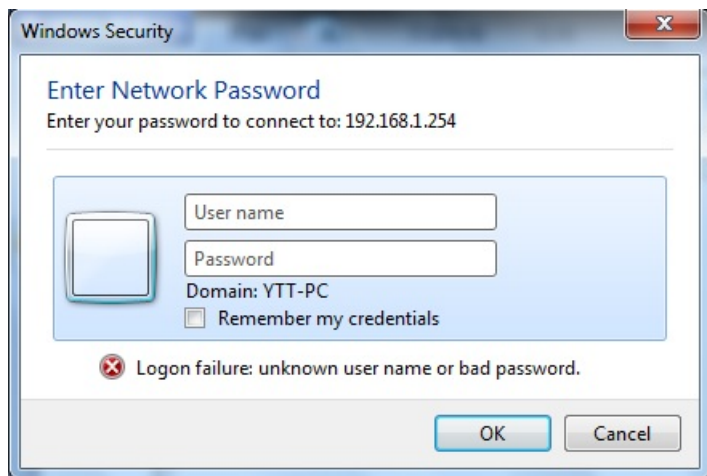
Please see [4.4.6.1 User Management](#).

Samba Usage:

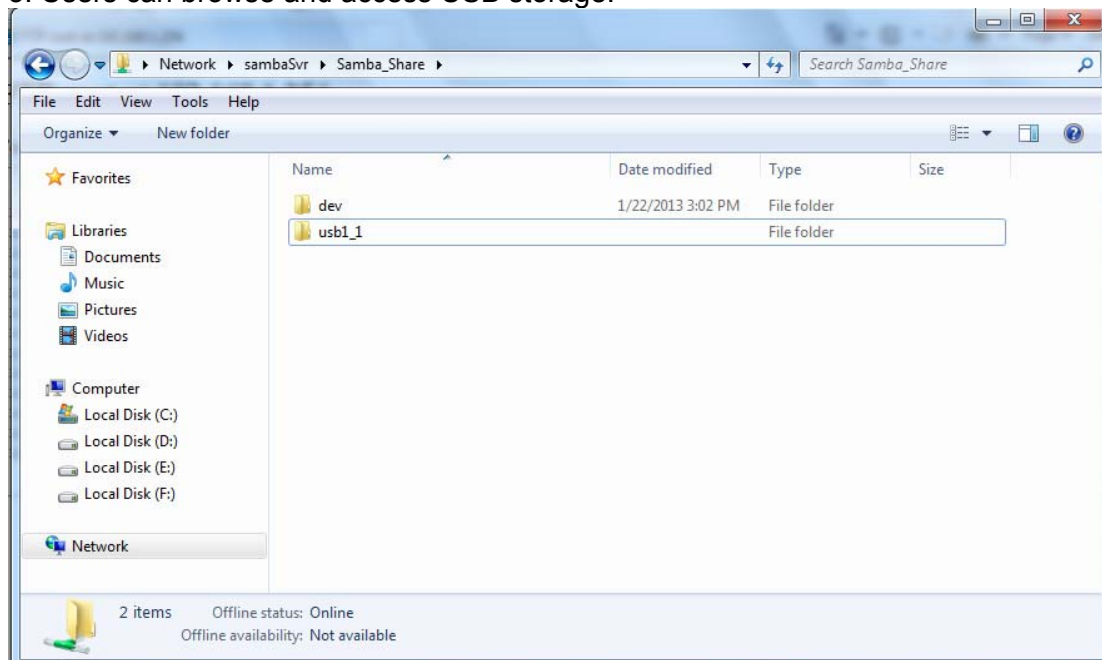
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.

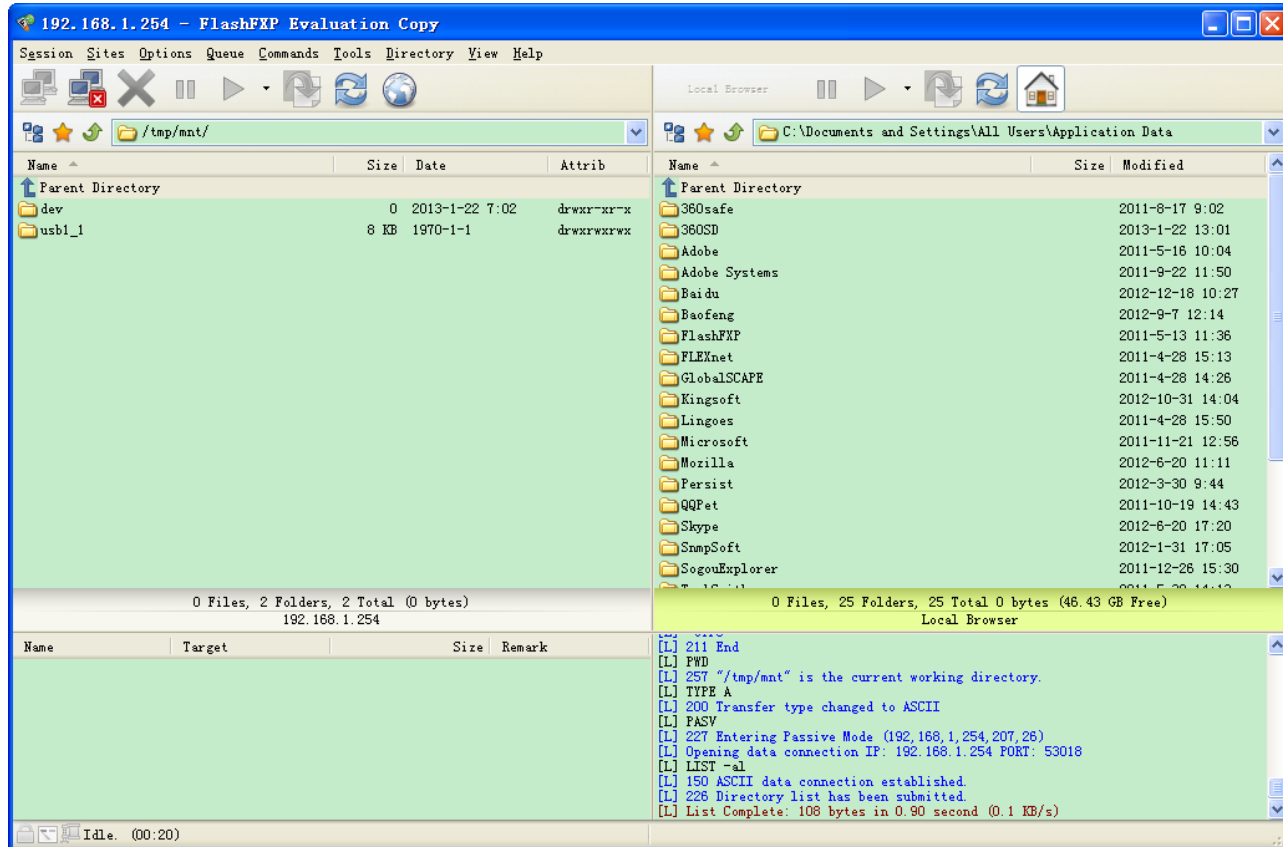


FTP usage:

1. Access via FTP tools

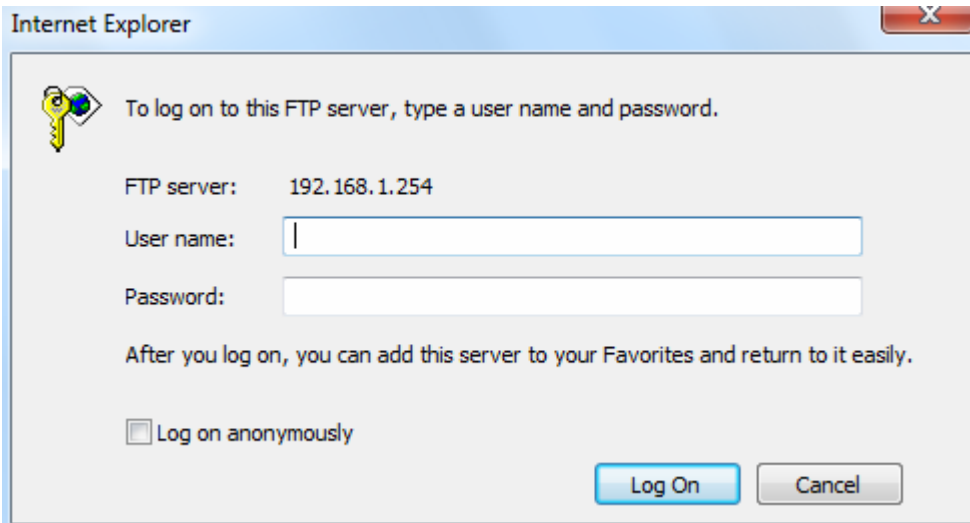
Take popular FTP tool of FlashFXP for example:

- 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

- 1) Enter <ftp://192.168.1.254> at the address bar of the web page.
- 2) Enter the account's username and password.



The image shows a dialog box titled "Internet Explorer" with a close button (X) in the top right corner. The dialog box contains a key icon on the left and the following text: "To log on to this FTP server, type a user name and password." Below this text, there are three input fields: "FTP server:" with the value "192.168.1.254", "User name:" with an empty text box, and "Password:" with an empty text box. Below the input fields, there is a line of text: "After you log on, you can add this server to your Favorites and return to it easily." At the bottom left, there is a checkbox labeled "Log on anonymously" which is currently unchecked. At the bottom right, there are two buttons: "Log On" and "Cancel".

Internet Explorer

To log on to this FTP server, type a user name and password.

FTP server: 192.168.1.254

User name:

Password:


After you log on, you can add this server to your Favorites and return to it easily.

Log on anonymously


Log On Cancel

4.4.6 Maintenance

Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including **User Management**, **Time Zone**, **Firmware & Configuration**, **System Restart**, **Diagnostic Tool**. Usage of each feature is to be presented in the following scenarios.



Point-to-Point Fiber Wireless-N VPN VoIP Gateway



- ▶ Status
- ▶ Quick Start
- ▶ Configuration
 - ▶ Interface Setup
 - ▶ Dual WAN
 - ▶ Advanced Setup
 - ▶ VoIP
 - ▶ Access Management
 - ▼ Maintenance
 - User Management
 - Time Zone
 - Firmware & Configuration
 - System Restart
 - Diagnostic Tool
- ▶ Language

Configuration

▼ User Management

User Account

Index: 1

Username:

New Password:

Confirm Password:

FTP Authority Setup

FTP Access: Enable Disable

Permission: Read/Write Read

SAMBA Authority Setup

SAMBA Access: Enable Disable

Permission: Read/Write Read

Please restart the Storage server after config changed

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

Restart
Logout

Copyright © Billion Electric Co., Ltd. All rights reserved.

4.4.6.1 User Management

User Management controls the Router Web GUI permission, FTP/SAMBA access to the specific account. In factory setting, the default accounts are **admin/admin** and **user/user**. The default root 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 [4.4.5.8 SAMBA & FTP Server](#) to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

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/Write or Read.

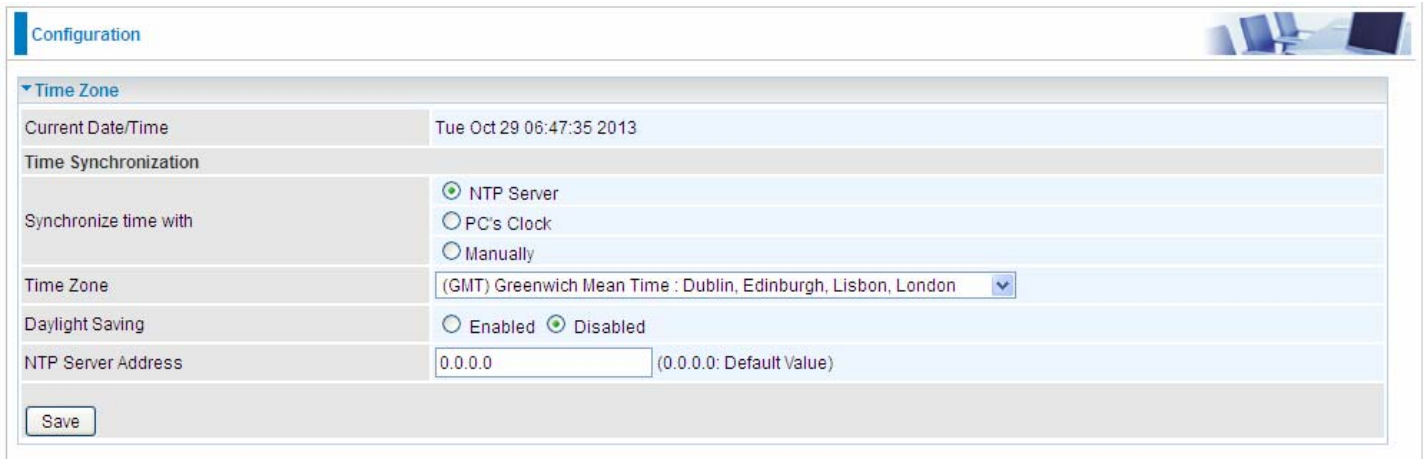
SAMBA Authority

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

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

4.4.6.2 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.



The screenshot shows a configuration page titled "Configuration" with a sub-section for "Time Zone". The current date and time are "Tue Oct 29 06:47:35 2013". Under "Time Synchronization", the "NTP Server" option is selected. The "Time Zone" is set to "(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London". "Daylight Saving" is set to "Disabled". The "NTP Server Address" is "0.0.0.0". A "Save" button is at the bottom left.

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

- ① **NTP Server automatically:** To synchronize time with the NTP server.
- ① **PC's Clock:** To synchronize time with the PC's clock.
- ① **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.

4.4.6.3 Firmware & Configuration

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 9800VNX(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 9800VNX(L) will reset automatically to make the new firmware work.

The screenshot shows the 'Firmware & Configuration' section of a router's web interface. It includes options to upgrade firmware or configuration, choose current or factory default settings for a system restart, a file upload field with a 'Browse...' button, and a 'Backup' button. A warning message states: 'It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.' An 'Upgrade' button is located at the bottom of the section.

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

- ① **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- ① **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: 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.

The screenshot shows a file dialog box with the text: 'Do you want to open or save romfile.cfg (35.8 KB) from 192.168.1.254?'. The dialog has three buttons: 'Open', 'Save' with a dropdown arrow, and 'Cancel' with a close icon (X).

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

Configuration 

▼ Firmware Upgrade

File upload succeeded, starting flash erasing and programming!!

Progress 

Percent %

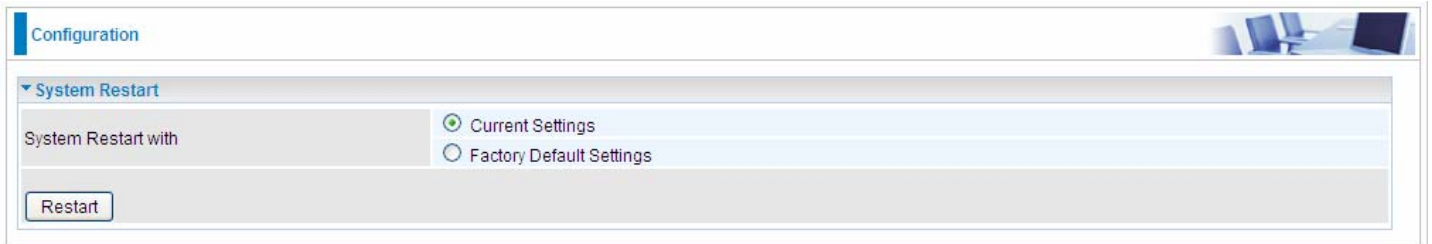


Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

4.4.6.4 System Restart

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



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' header. Below it, a 'System Restart' section is expanded, showing two radio button options: 'Current Settings' (which is selected) and 'Factory Default Settings'. A 'Restart' button is located at the bottom of this section.

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.

4.4.6.5 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.


SFP:

Configuration 

▼ Diagnostic Tool

WAN Interface	SFP
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

Start

Configuration 

▼ Diagnostic Tool

WAN Interface	SFP
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (192.168.17.245)	PASS
Ping www.google.com	PASS
Ping other IP Address <input checked="" type="radio"/> Yes <input type="radio"/> No	PASS
IP Address	8.8.8.8

Start


3G/4G-LTE USB:

Configuration 

▼ Diagnostic Tool

WAN Interface	3G/4G-LTE USB
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

Click START to begin to diagnose the connection.

Configuration 

▼ Diagnostic Tool

WAN Interface	3G/4G-LTE USB
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (221.6.4.66)	PASS
Ping www.google.com	PASS
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped

EWAN:

Configuration 

▼ Diagnostic Tool

WAN Interface	EWAN ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (218.2.135.1)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

Click START to begin to diagnose the connection.

Configuration 

▼ Diagnostic Tool

WAN Interface	EWAN ▼
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (218.2.135.1)	PASS
Ping www.google.com	PASS
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped

Chapter 5

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 WAN Interface

Problem	Corrective Action
Obtaining WAN IP failure	Check that your internet settings are the same as those provided by your ISP. Reboot the router if you still have problems, you may need to verify these settings with your ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	<ol style="list-style-type: none">1. 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.2. Verify that the IP address and the subnet mask are consistent between the router and the PC.

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>

MAC OS is a registered Trademark of Apple Inc.

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

Federal Communication Commission Interference Statement

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

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

FCC Caution:

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

(1) This device may not cause harmful interference

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

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

Co-location statement

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

FCC Radiation Exposure Statement

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