BiPAC 4700ZU

4G/LTE VPN Outdoor Router

BiPAC 4700ZUL

4G/LTE Outdoor Router

User Manual

Version release: 1.04.1.x

Last revised date: November 22, 2017

Table of Contents

Chapter 1: Introduction *1*

Introduction to your Router **1**

Features & Specifications **2**

Hardware Specifications **4**

Application Diagram **5**

Chapter 2: Product Overview *6*

Important Note for Using This Router **6**

Device Description **7**

The detail instruction in Reset Button **8**

Chapter 3: Basic Installation *9*

Installation Reference **10**

Cabling **13**

Default Settings **14**

Information from Your ISP **15**

Chapter 4: Device Configuration *16*

Login to your Device **16**

Status **18**

Device Info 19

System Status 20

System Log 21

4G/LTE Status 22

Statistics 24

DHCP Table 26

IPSec Status (BiPAC 4700ZU only) 27

PPTP Status (BiPAC 4700ZU only) 28

L2TP Status (BiPAC 4700ZU only) 29

GRE Status (BiPAC 4700ZU only) 30

OpenVPN Status (BiPAC 4700ZU only) 31

ARP Table 32

VRRP Status 33

Quick Start **34**

Configuration **36**

Interface Setup 37

Internet 38

LAN 41

Loopback 45

Advanced Setup 46

Firewall 47

Routing 48

Dynamic Routing....49
NAT....51
VRRP....56
Static DNS....57
Time Schedule....58
Mail Alert....59
VPN (BiPAC 4700ZU only)....60
IPSec....61
PPTP Server....71
PPTP Client....73
L2TP....82
GRE Tunnel....92
OpenVPN Server....97
OpenVPN Client....99
Access Management....104
Device Management....105
SNMP....106
Remote Syslog....107
Universal Plug & Play....108
Dynamic DNS....109
Access Control....111
Packet Filter....113
CWMP (TR-069)....116
Parental Control....118
Maintenance....119
User Management....120
Certificate Management....123
Time Zone....125
Firmware & Configuration....126
System Restart....128
Auto Reboot....129
Diagnostics Tool....130
Chapter 5: Troubleshooting....132
Problems with the Router....132
Problem with LAN Interface....132
Recovery Procedures....132
Appendix: Product Support & Contact....134

Chapter 1: Introduction

Introduction to your Router

Integrated with Latest 4G LTE Network and Dual-Polarized MIMO Antenna Technology

BiPAC 4700ZU/ 4700ZUL integrates the latest high speed 4G/LTE module enabling support of multiple high bandwidth applications. Areas with a weak or nonexistent wireless signal can benefit from the extended range and reach of the Dual-Polarized MIMO antenna technology for their environment or application whether LOS(Line of Sight) or NLOS(Non-Line of Sight).

IP67 Industrial-Grade Secure Design

BiPAC 4700ZU/ 4700ZUL is an industrial-grade design with an IP67 rated enclosure to withstand the extreme weather conditions, Also, built-in ±6K surge(K.21) and ±15KV ESD(EN 61000-4-5) protection design protects against storm/lightning surges and ensuring robust and reliable operation.

Easy Installation with PoE Support

Easy Installation is realized with integrated Power over Ethernet (PoE) support, eliminating the need for separate power and data cables.

Secure VPN Connections (BiPAC 4700ZU only)

BiPAC 4700ZU supports comprehensive and robust IPSec/ PPTP/ L2TP/ GRE/ OpenVPN VPN(Virtual Private Network) protocols for business users to establish private encrypted tunnels over the public Internet to secure data transmission between headquarters and branch offices. It also supports VPN dial in from smart phones for secure remote Internet connection via your home broadband. With a built-in VPN accelerator, the router enhances IPSec VPN performance significantly.

IPv6 Supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. The router is already supporting IPv6, you can use it in IPv6 environment no need to change device. The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6.

Quick Start Wizard

Support a WEB GUI page to install this device quickly. With this wizard, simple steps will get you connected to the Internet immediately.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI or CWMP(TR-069).

Features & Specifications

- 4G/LTE for high speed mobile broadband connectivity
- High performance antenna for increased coverage, signal reception and efficiency
- Gigabit Ethernet LAN (PoE)
- IPv6 ready (IPv4/IPv6 dual stack) *1
- Support to obtain power via PoE(Power over Ethernet)
- Enterprise level routing functionality - OSPF, BGP
- Firewall Security with DoS Preventing and Packet Filtering
- Universal Plug and Play (UPnP) Compliance
- Ease of Use with Quick Installation Wizard
- IPSec VPN with powerful DES/ 3DES/ AES
- PPTP VPN with Pap/ Chap/ MPPE authentication
- L2TP VPN with Pap/Chap authentication
- GRE VPN tunnel
- OpenVPN tunnel
- CWMP(TR-069)
- Industrial-grade design with an IP67 rated enclosure
- Built-in ±6K surge(K.21) and ±15KV ESD(EN 61000-4-5) protection design protects against storm/lightning surges

High-speed mobile wireless data communication

- Embedded 4G/LTE module
- High performance antenna

Network Protocols and Features

- IPv4, IPv6, IPv4/ IPv6 Dual Stack*1
- NAT
- Static Routing and Dynamic Routing - RIP-1/2, OSPF, BGP
- Virtual Server and DMZ
- DHCPv4/v6
- Universal Plug and Play(UPnP) Compliant
- Dynamic Domain Name System(DDNS)
- SNTP, DNS proxy
- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy

- VRRP(Virtual Router Redundancy Protocol)

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention including Land Attack, Ping of Death, etc
- Access control
- IP&MAC filter, URL Content Filter
- Password protection for system management
- VPN pass-through

Virtual Private Network (VPN)

- Secured IPSec VPN with powerful DES/ AES
- Secured PPTP VPN with Pap/ Chap/ MPPE authentication
- Secured L2TP VPN with Pap/Chap authentication
- Secured GRE VPN tunnels
- Secured OpenVPN Server and Client

Management

- Quick Installation wizard
- Web-based GUI for remote and local management
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server / client / relay
- Supports SNMP v1, v2, v3, MIB-I and MIB-II
- CWMP(TR-069)[*1] supports remote management

1. Only upon request for Telco/ ISP projects.
2. Specifications on this manual are subject to change without prior notice.
3. Features described in this manual subject to the equipped modules' capabilities. The different module installed for a different country. For detailed information, please contact your local distributors.

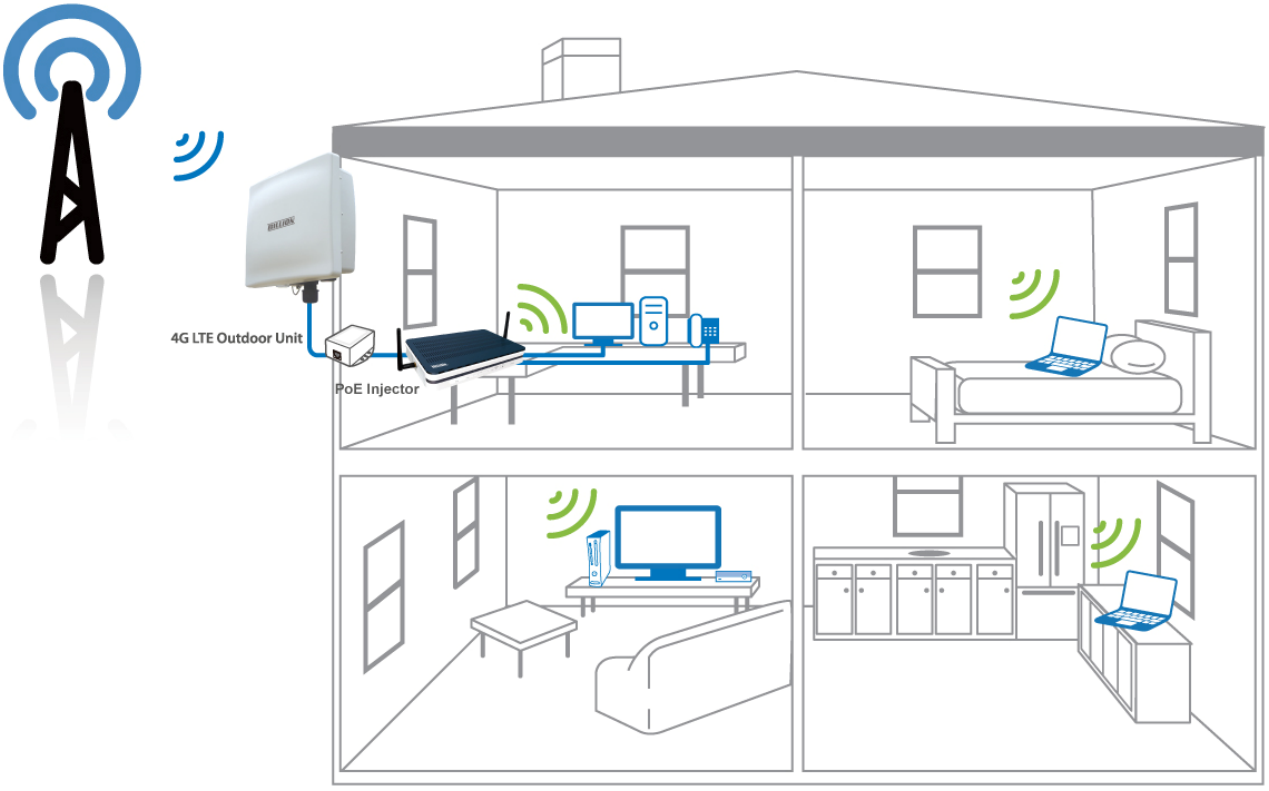
Hardware Specifications

Physical interface

- One(1) Embeded 4G/LTE module
- One(1) mini-SIM(2FF) card slot
- One(1) Gigabit Ethernet LAN with PoE, can obtain power via PoE - equipped switch or power injector.
- Factory default reset button

Application Diagram

BiPAC 4700ZU/ 4700ZUL:



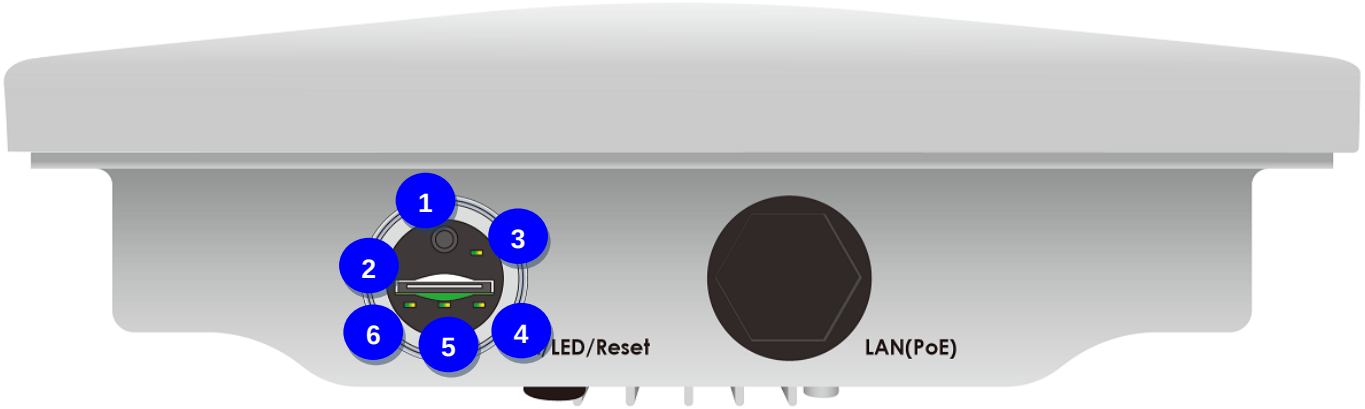
Chapter 2: Product Overview

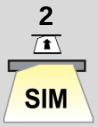
Important Note for Using This Router

Warning

- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Place the router on a stable surface.
- ✓ This equipment should be installed and operated with minimum distance 20cm away from your body.

Device Description



PORT		MEANING	
1	**Reset button**	After the device is powered on, press it **6 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)	
2 	**SIM Card Slot**	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it	
3	**LTE (Received Signal Strength Indicator)**	Green	RSSI greater than -69 dBm. Excellent signal condition
		Green Flashing quickly	RSSI from -81 to -69 dBm. Good signal condition
		Orange Flashing quickly	RSSI from -99 to -81 dBm. Fair signal condition.
		Orange Flashing slowly	RSSI less than -99 dBm. Poor signal condition.
		Orange	No signal and the 4G LTE module is in service
		Off	No LTE module or LTE module fails
4	**Internet**	Green	IP connected and traffic is passing through the device.
		Orange	IP request failed.
		Off	Either in bridged mode or WAN connection not present.
5	**Ethernet (LAN)**	Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
6	**Power**	Green	System is up and ready
		Orange	Boot failure

The detail instruction in Reset Button

Recovery procedures for non-working devices (e.g. after a failed firmware upgrade flash):

Please follow the steps, the router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state.

Please note that the router will only respond with its web interface at this address (**192.168.1.1**), and will not respond to ping request from your PC or other telnet operations.

Steps:

Before starting recovery process, please configure the IP address of the PC as 192.168.1.100 and proceed with the following step-by-step guide.

1. Power the router off.

2. Press reset button and power on the router, once the Power flashes Red and Green, keeping press reset button over 6 seconds.

3. Internet led flashes Green and Red, router entering recovery procedure and router's IP will reset to Emergency IP address (Say 192.168.1.1).

4. Open browser and access http://192.168.1.1 to upload the firmware.

5. Internet led lit Red, and router starts to write firmware into flash. Please DO NOT power off the router at this step.

6. Internet led lit Green when successfully upgrade firmware.

7. Power the router off and then on again.

Chapter 3: Basic Installation

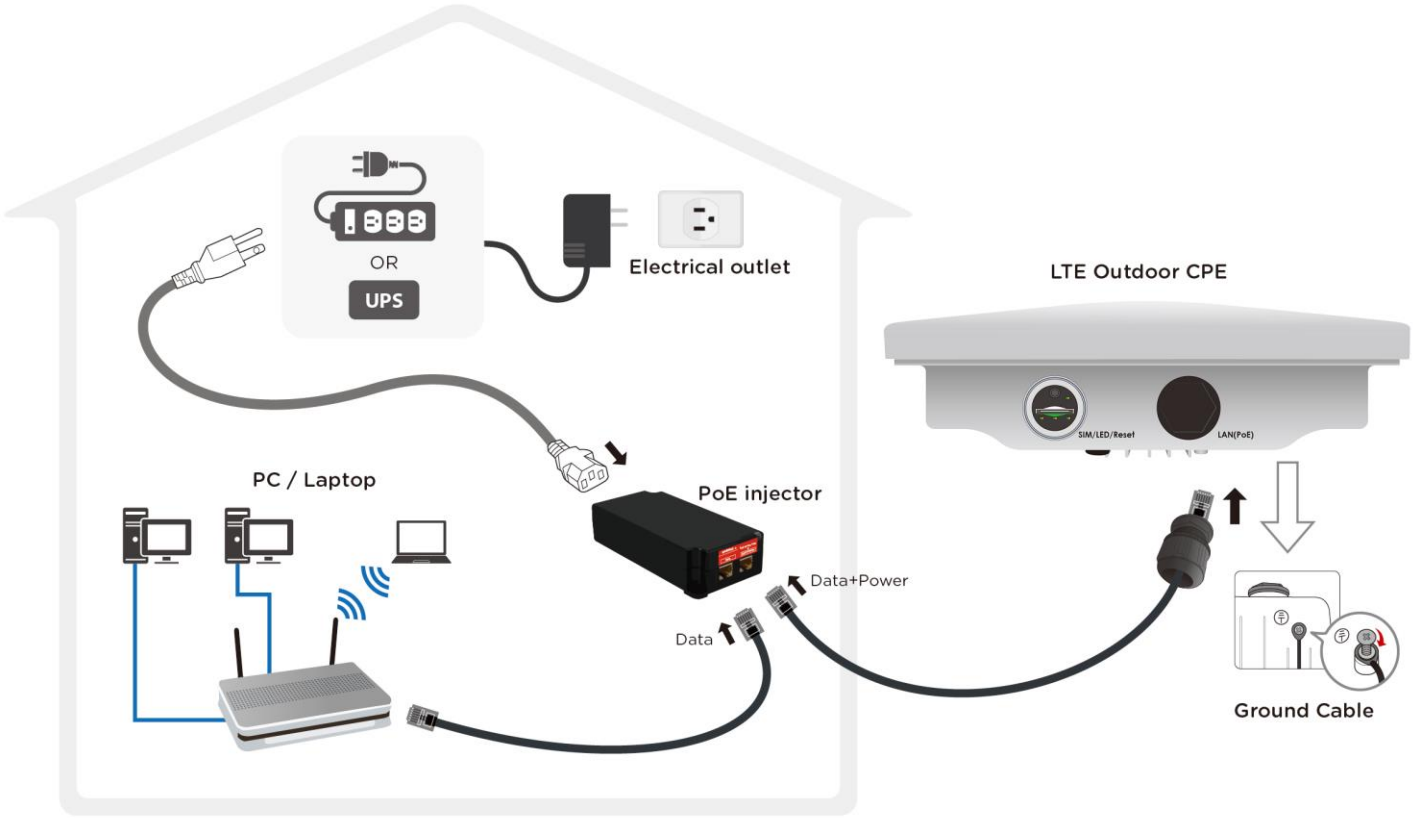
The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

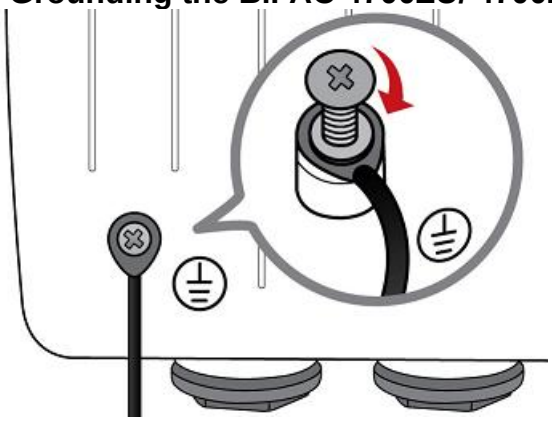
Any TCP/IP capable workstation can be used to communicate with or through the router. To configure other types of workstations, please consult the manufacturer's documentation.

Installation Reference



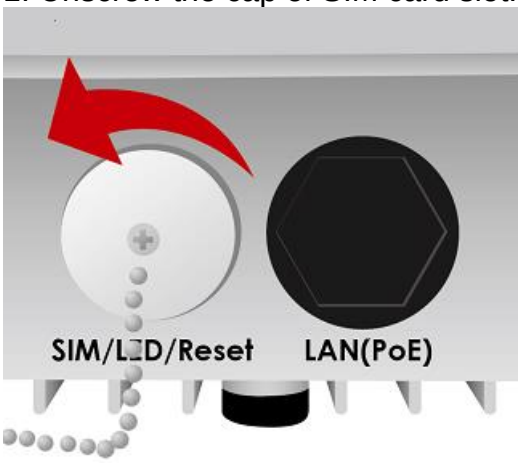
IMPORTANT: It is recommended to put the Gigabit PoE Injector on an UPS or Surge Protector. Use the supplied grounding wire to ground your BiPAC 4700ZU/ 4700ZUL ODU is REQUIRED!

I. Grounding the BiPAC 4700ZU/ 4700ZUL

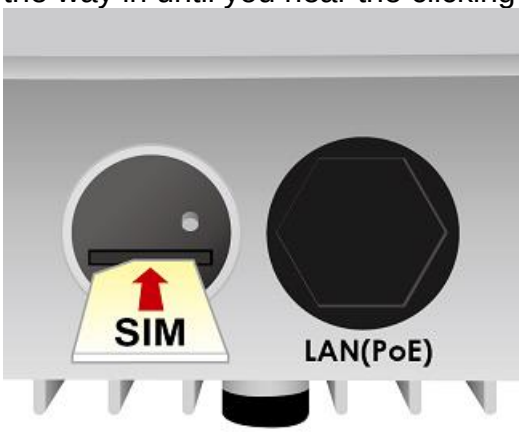


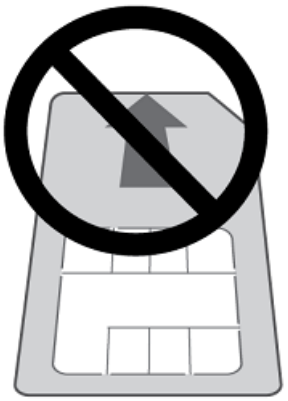
II. Insert SIM card

1. Unscrew the cap of SIM card slot.

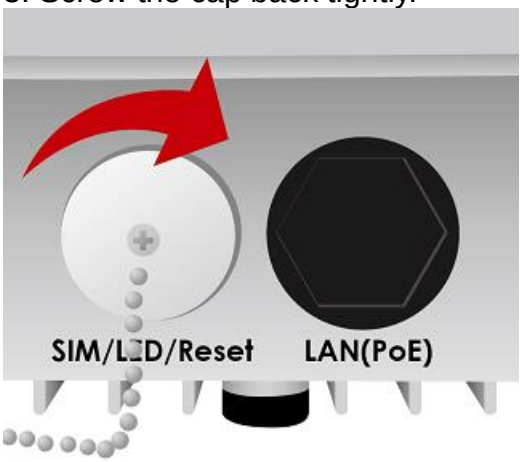


2. Slide the SIM card with the mental contacts (gold plate) facing down to the SIM slot then push it all the way in until you hear the clicking sound.





3. Screw the cap back tightly.



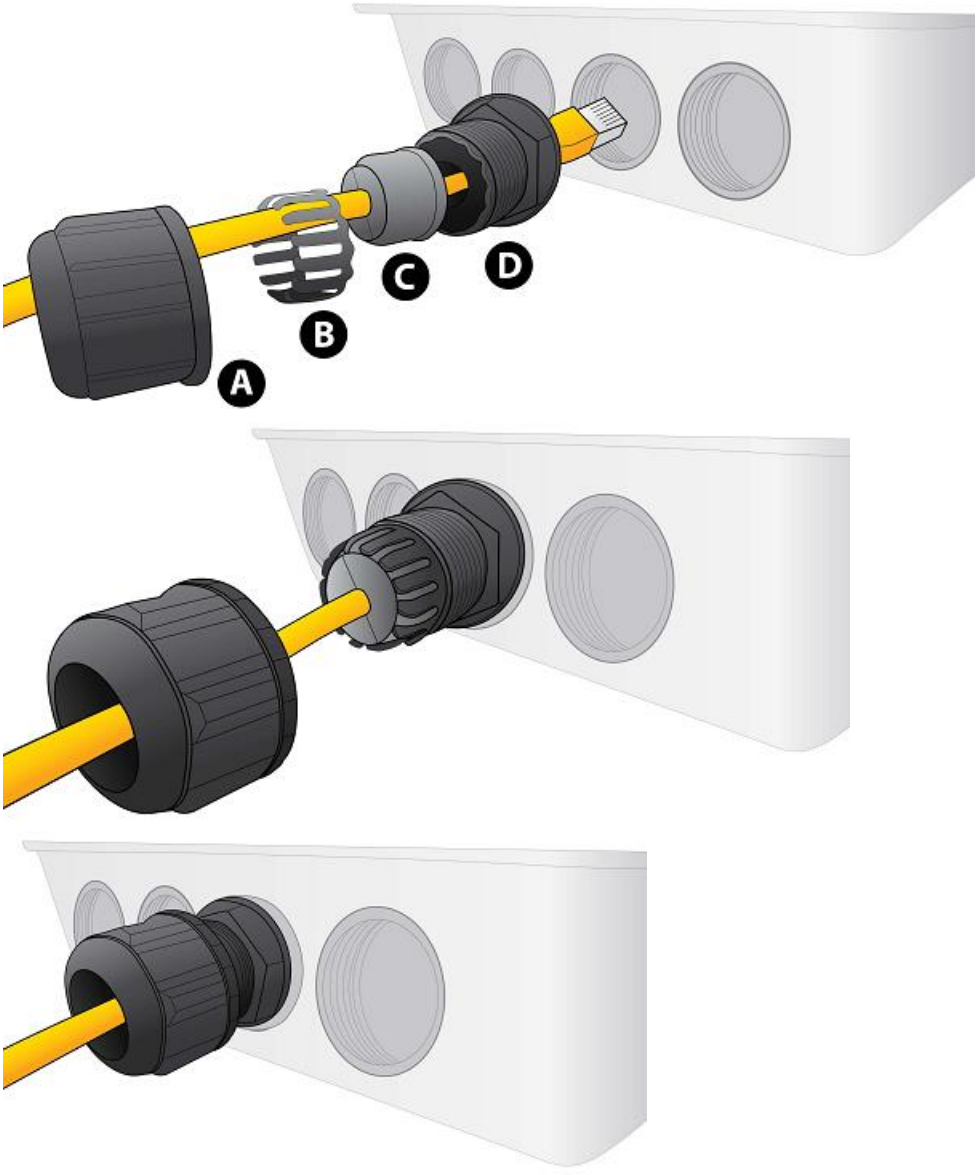
Attention: Please power off the device before inserting or removing the SIM card.
It is recommended to use an Industrial-grade SIM card.

III. Power on BiPAC 4700ZU/ 4700ZUL

Step 1: Assemble M25 cable gland

Step 2: Unscrew the LAN (PoE) port and insert the supplied outdoor Ethernet cable (RJ-45) through material A-D, and then connect the RJ-45 Ethernet cable into the LAN (PoE) port.

2.1: Insert C at the back end of D
2.2: clip B on C
2.3: keep B close to D
2.4: then tighten A.



Step 3: Insert the other end of outdoor Ethernet cable (RJ-45) to the supplied Gigabit PoE injector Data+Power port. Connect another Ethernet cable (RJ-45) directly to the Data port and the other end of cable to a switch or broadband router.

IMPORTANT: It is recommended to put the Gigabit PoE Injector on an UPS or Surge Protector. Use the supplied grounding wire to ground your BiPAC 4700ZUL ODU is REQUIRED!

Cabling

One of the most common causes of problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of the product is a bank of LEDs. Verify that the LAN Link and LEDs are lit. If they are not, verify that you are using the proper cables.

Default Settings

Before configuring the router, you need to know the following default settings.

Web Interface: (Username and Password)

- ✔ Username: admin
- ✔ Password: admin

The default username and password are **admin** and **admin** respectively.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

- ✔ IP Address: 192.168.1.254
- ✔ Subnet Mask: 255.255.255.0

DHCP Server:

- ✔ DHCP server is enabled.
- ✔ Start IP Address: 192.168.1.100
- ✔ IP pool counts: 20

Information from Your ISP

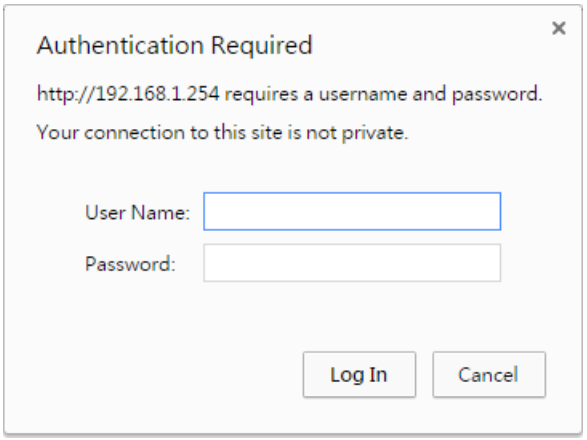
Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided.

Chapter 4: Device Configuration

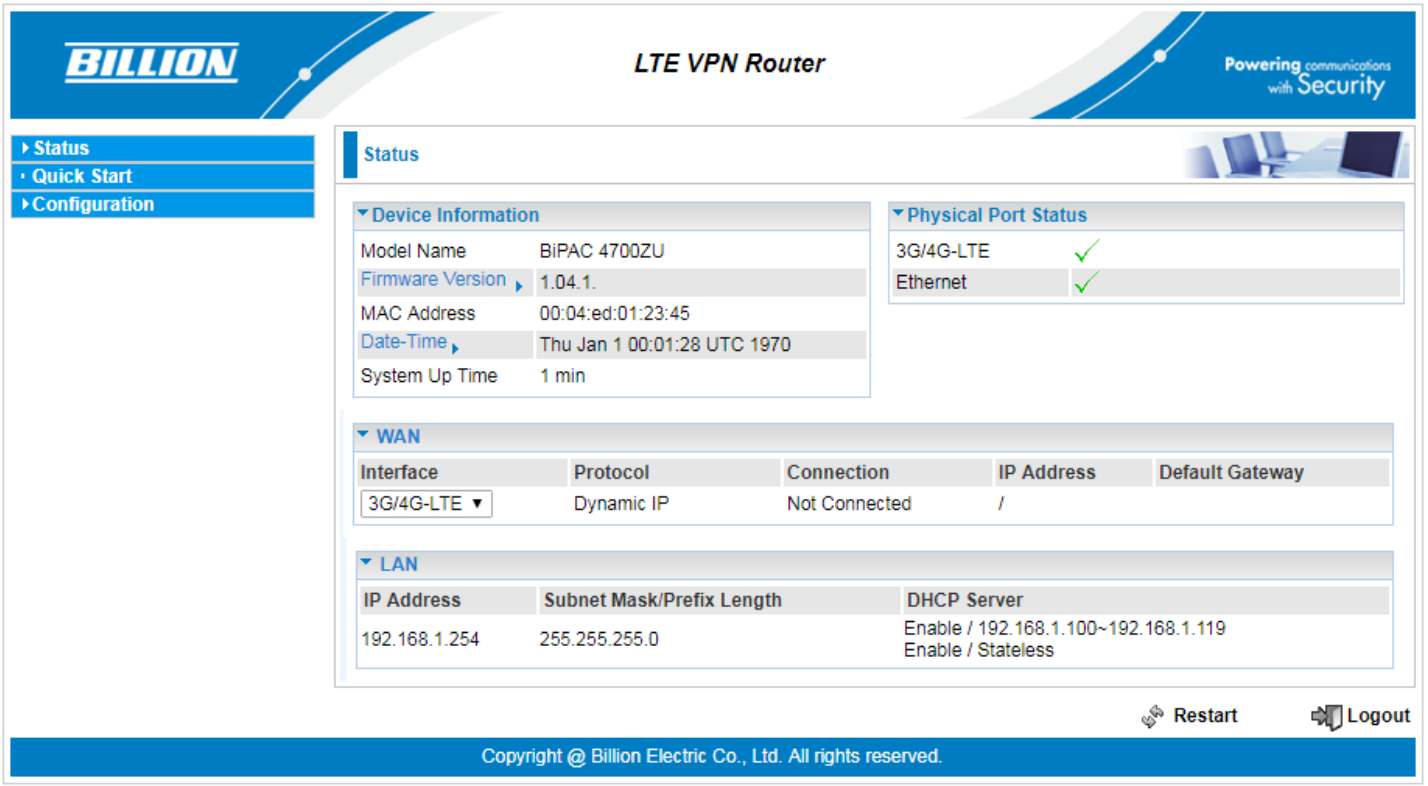
Login to your Device

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click **Go**, a user name and password window prompt appears.

The default username and password is **admin** and **admin** respectively for the **Administrator.**



Congratulations! You have successfully logged on to your Industrial LTE Router !



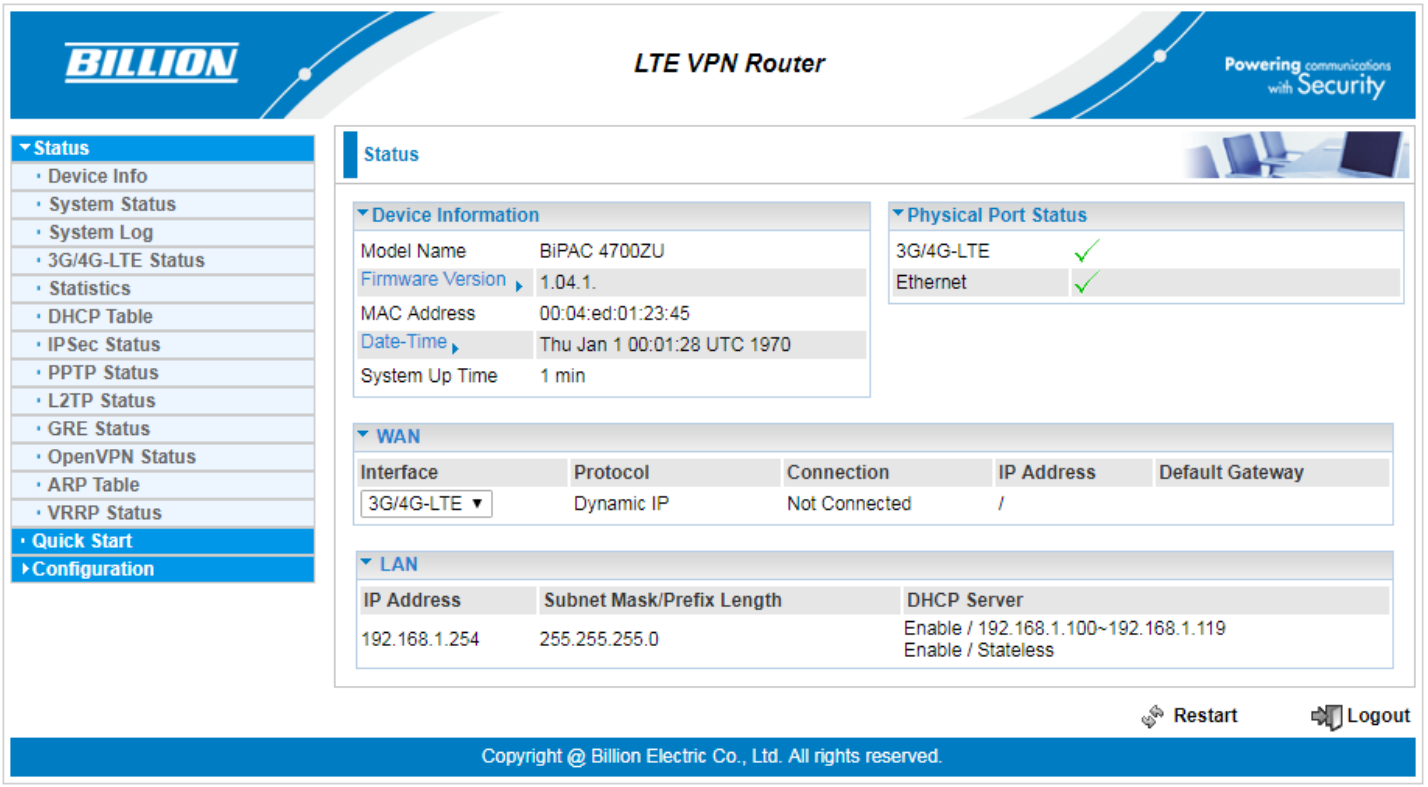
Once you have logged on to your Industrial LTE Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup page, which includes:

- **Status**(Device Info, System Status, System Log, 4G/LTE Status, Statistics, DHCP Table, IPSec Status, PPTP Status, L2TP Status, GRE Status, OpenVPN Status, ARP Table, VRRP Status)
- **Quick Start** (Wizard Setup)
- **Configuration** (Interface Setup, Advanced Setup, VPN, Access Management, Maintenance)

Please see the relevant sections of this manual for detailed instructions on how to configure your gateway.

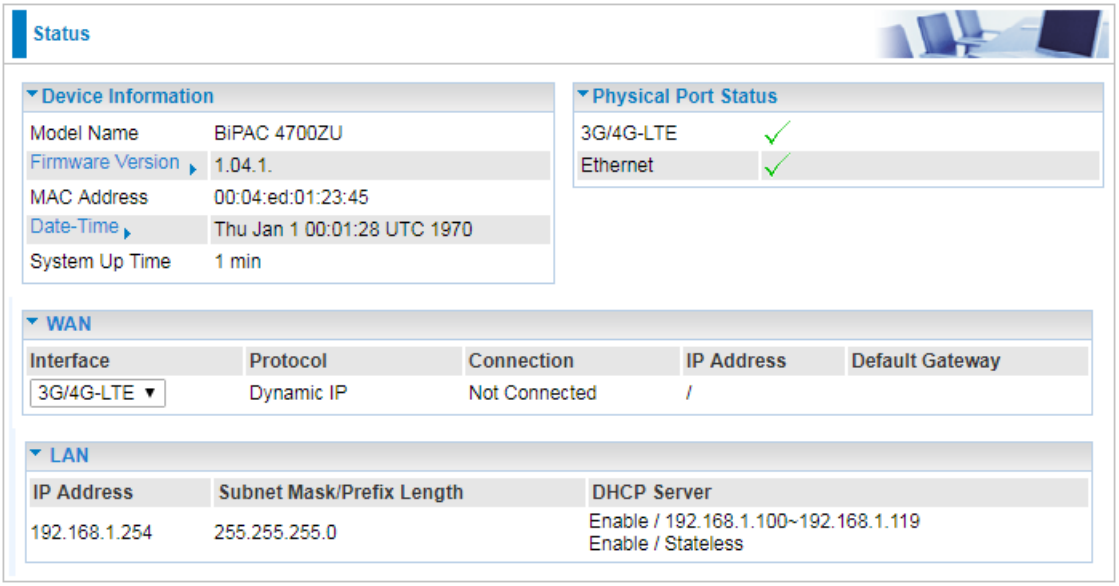
Status

In this section, you can check the router working status, including **Device Info, System Status, System Log, 4G/LTE Status, Statistics, DHCP Table, IPSec Status, PPTP Status, L2TP Status, GRE Status, OpenVPN Status, ARP Table, VRRP Status.**



Device Info

It contains basic information of the device.



Device Information

Model Name: Show model name of the router

Firmware Version: This is the Firmware version

MAC Address: This is the MAC Address

Date Time: The current date and time.

System Up Time: The duration since system is up.

Physical Port Status

Here the page shows the status of physical port of 4G/LTE and Ethernet.

WAN

Interface: The WAN interface **4G/LTE**.

Protocol: The protocol in use.

Connection: The connection status of the link.

IP Address: The WAN interface IP address obtained.

Default Gateway: The default gateway address.

LAN

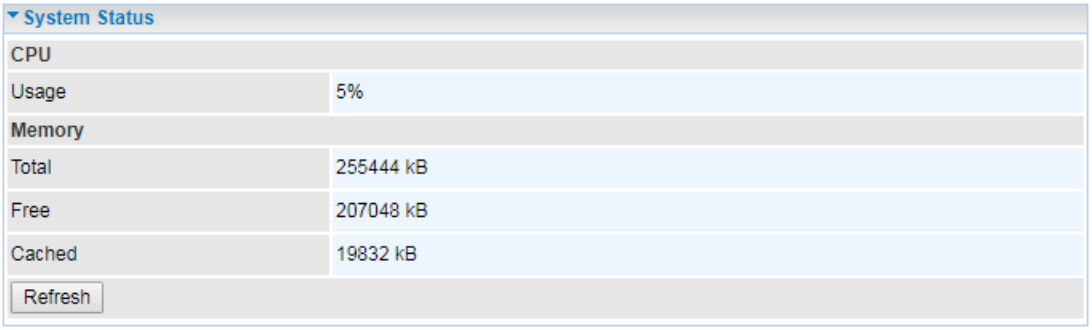
IP Address: LAN IP address.

Subnet Mask/Prefix Length: Subnet mask for IPv4 or Prefix length for IPv6 on LAN..

DHCP Server: LAN port DHCP information.

System Status

System status displays the current system (CPU and Memory) loading.



CPU Usage: To show the current CPU Usage.

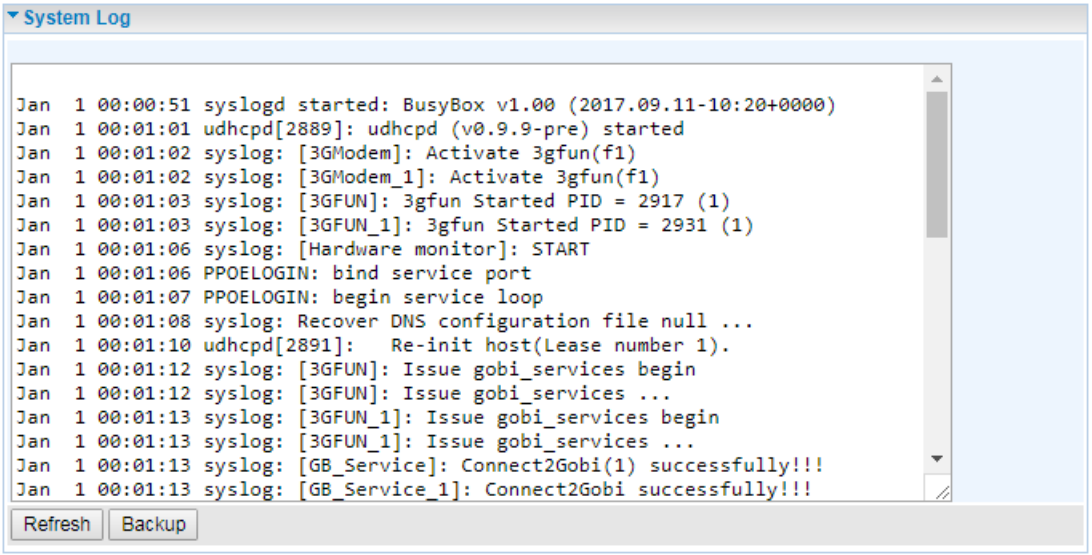
Memory Total: To show the total memory of the system in KB.

Memory Free: To show the current free memory or avalavle memory in KB.

Memory Cached: To show the cache memory in KB.

System Log

In system log, you can check the operations status and any glitches to the router.

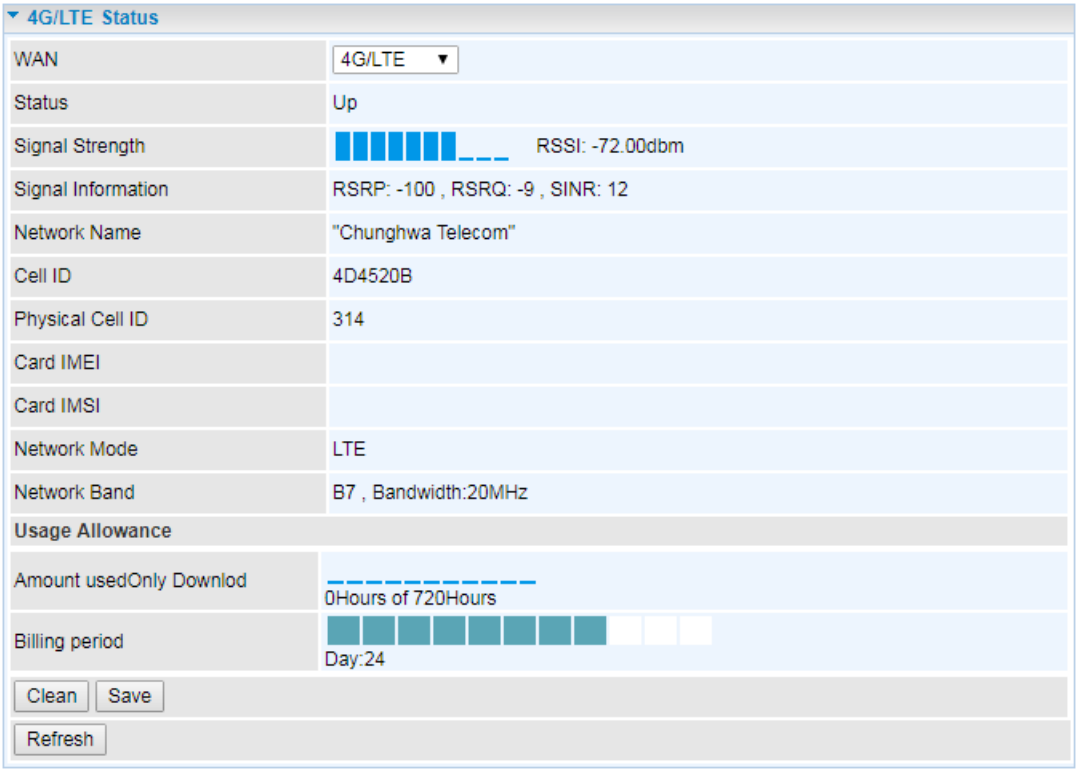


Refresh: Press this button to refresh the statistics.

Backup: Back up the current system log file and save it to your computer.

4G/LTE Status

This page contains 4G/LTE connection information.



Status: The current status of the 4G/LTE connection.

Signal Strength: The signal strength bar and dBm value indicates the current 4G/LTE signal strength. The front panel 4G/LTE Signal Strength LED indicates the signal strength as well.

Signal Information: Shows important LTE signal parameters such as RSRP (Reference Signal Receiving Power), RSRQ (Reference Signal Receiving Quality), SINR (Signal to Interference plus Noise Ratio).

- RSRP (Reference Signal Receiving Power): is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- RSRQ (Reference Signal Receiving Quality): measures the signal strength and is calculated based on both RSRP and RSSI.
- SINR (Signal to Interference plus Noise Ratio): is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput.

  Note: Some LTE modules do not provide this information.

Network Name: The name of the LTE network the router is connecting to.

Cell ID: The ID of base station that the device is connected to.

Card IMEI: The unique identification number that is used to identify the 4G/LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the user of a celluar network – a number provisioned in the SIM card..

Network Mode: Show the using network mode.

Network Band: Show the using network band.

Amount used: Show the volumn used, the amount can be refered to **only Download**, **only Upload** and **Download and Upload**, please move to **Usage Allowance** to check.

Billing period: The lasting days since the biling begins each month(the beginning day counted).

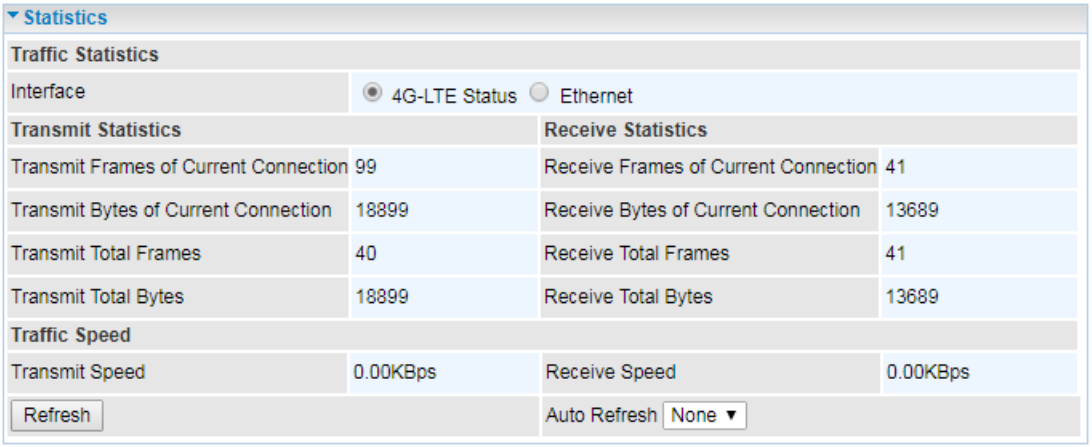
Clean: To clear the usage statistics.

Save: Press to save the usage statistics to FLASH, else the usage will be cleared after reboot.

Refresh: Press this button to refresh the statistics.

Statistics

❖ 4G/LTE



Interface: List all available network interfaces in the router. You are currently checking on the physical status of **4G/LTE** interface**.**

Transmit Frames of Current Connection: This field displays the total number of 4G/LTE frames transmitted until the latest second for the current connection.

Transmit Bytes of Current Connection: This field shows the total bytes transmitted till the latest second for the current connection for the current connection.

Transmit Total Frames: The field displays the total number of frames transmitted till the latest second since system is up.

Transmit Total Bytes: This field displays the total number of bytes transmitted until the latest second since system is up.

Receive Frames of Current Connection: This field displays the number of frames received until the latest second for the current connection.

Receive Bytes of Current Connection: This field shows the total bytes received till the latest second for the current connection.

Receive Total Frames: This field displays the total number of frames received until the latest second since system is up.

Receive Total Bytes: This field displays the total frames received till the latest second since system is up.

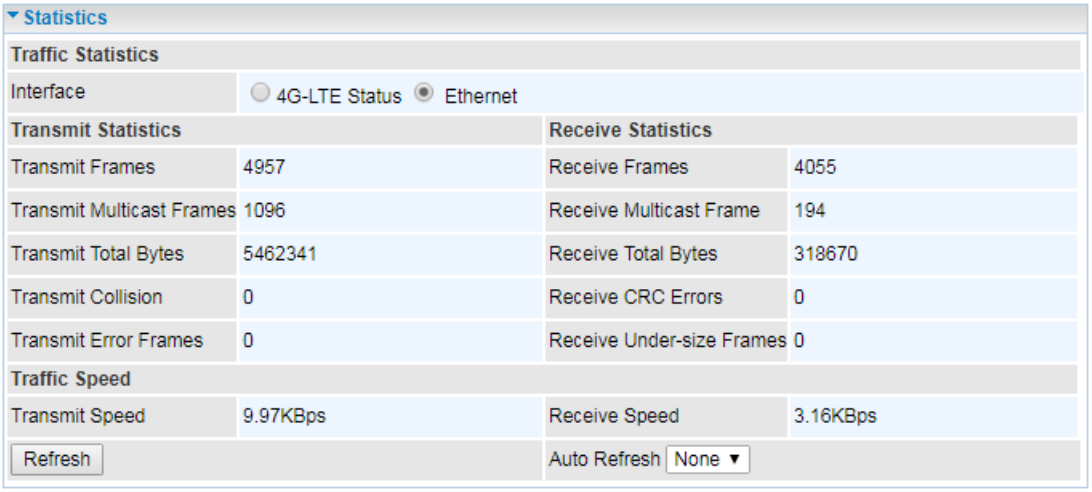
Transmit Speed: Display the current upload rate.

Receive Speed: Display the current download rate.

Auto Refresh: Choose whether to refresh the data automatically and how often. Select None to disable the feature. Or automatically refresh the statistics every 10 sec or 30 sec.

Refresh: Press this button to refresh the statistics.

❖ Ethernet



Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **Ethernet** port**.**

Transmit Frames: This field displays the number of frames transmitted until the latest second.

Transmit Multicast Frames: This field displays the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: This field displays the number of bytes transmitted until the latest second.

Transmit Collision: This is the number of collisions on this port.

Transmit Error Frames: This field displays the number of error packets on this port.

Receive Frames: This field displays the number of frames received until the latest second.

Receive Multicast Frames: This field displays the number of multicast frames received until the latest second.

Receive Total Bytes: This field displays the number of bytes received until the latest second.

Receive CRC Errors: This field displays the number of error packets on this port.

Receive Under-size Frames: This field displays the number of under-size frames received until the latest second.

Transmit Speed: Display the current upload rate.

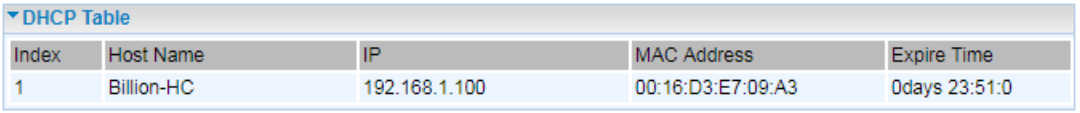
Receive Speed: Display the current download rate.

Auto Refresh: Choose whether to refresh the data automatically and how often. Select None to disable the feature. Or automatically refresh the statistics every 10 sec or 30 sec.

Refresh: Press this button to refresh the statistics.

DHCP Table

DHCP table displays the devices connected to the router with clear information.



Index: The index identifying the connected devices.

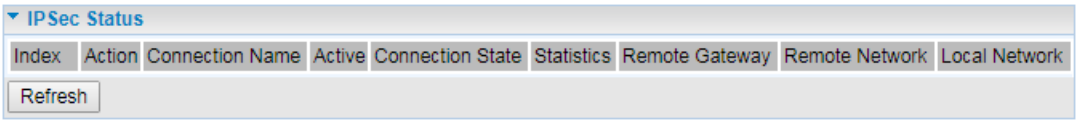
Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Expire Time: The total remaining interval since the IP assignment to the PC.

IPSec Status (BiPAC 4700ZU only)



Index: The IPSec tunnel index number.

Action: Connect or Drop the connection.

Connection Name: User-defined IPSes VPN connection name.

Active: Show if the tunnel is active for connection.

Connection State: Show the IPSec phase 1 and phase 2 connecting status.

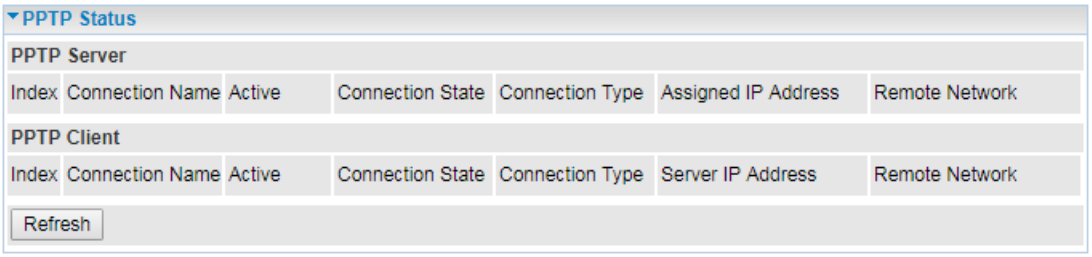
Statistics: Display the upstream/downstream traffic per session in KB. The value clears when session disconnects.

Remote Gateway: The IP of the remote IPSec gateway.

Remote Network: The IP and netmask of remote access range.

Local Network: The IP and netmask of local access range.

PPTP Status (BiPAC 4700ZU only)



Index: The PPTP server tunnel index number.

Connection Name: Show user-defined PPTP VPN connection name.

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

Connection Type: Remote Access or LAN to LAN.

Assigned IP Address: Show the IP assigned to the client by PPTP Server.

Server IP Address: Show the IP of remote PPTP Server.

Remote Network: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Refresh: Click this button to refresh the connection status.

L2TP Status (BiPAC 4700ZU only)

Index: The L2TP tunnel index number.

Connection Name: Display the user-defined L2TP connection name.

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

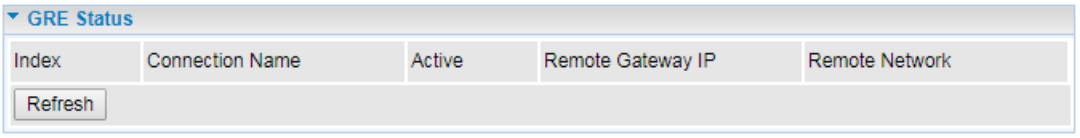
Connection Mode: The L2TP mode is dialin or dialout.

Connection Type: Remote Access or LAN to LAN.

Tunnel Remote IP Address: Display the remote tunnel IP address.

Refresh: Click this button to refresh the connection status.

GRE Status (BiPAC 4700ZU only)



Index: The GRE tunnel index number.

Connection Name: Display the user-defined GRE connection name.

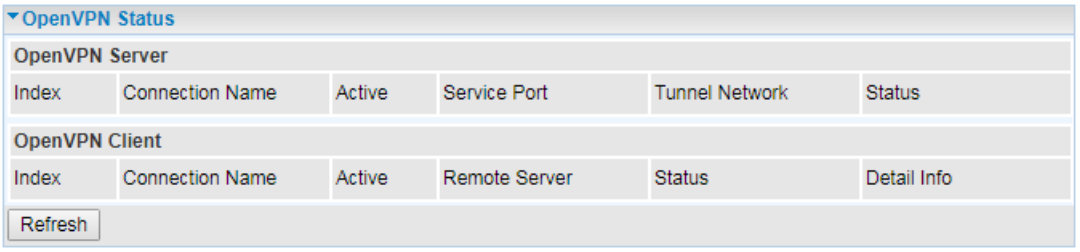
Active: Show if the tunnel is active for connection.

Remote Gateway IP: The IP of the remote GRE gateway.

Remote Network: Display the remote network.

Refresh: Click this button to refresh the connection status.

OpenVPN Status (BiPAC 4700ZU only)



Index: The index to identify the OpenVPN connection/rule.

Connection Name: User-defined name to mark the connection/rule.

Active: Yes or no to demosntrate the rule is active or not.

Service Port: Show the service port/protocl.

Tunnel Network: The virtual tunnel subnet of the server.

Status: The status of the rule.

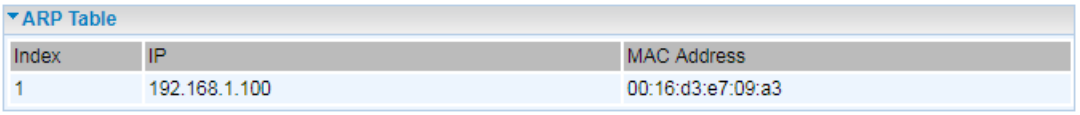
Remote Server: Show the remote server public IP: port/protocl.

Detail Info: Show the assigned virtual IP and routing by the sever.

Refresh: Click this button to refresh the connection status.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of IP addresses to Ethernet MAC addresses.



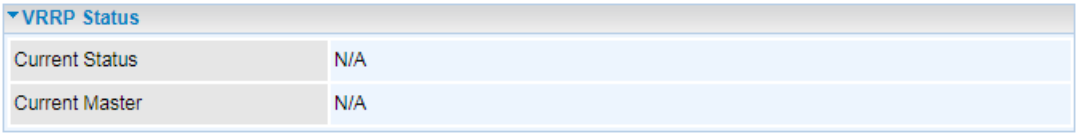
Index: The Index of the ARP rule item.

IP Address: Shows the IP Address of the device that the MAC address maps to.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

VRRP Status

Show the VRRP status.

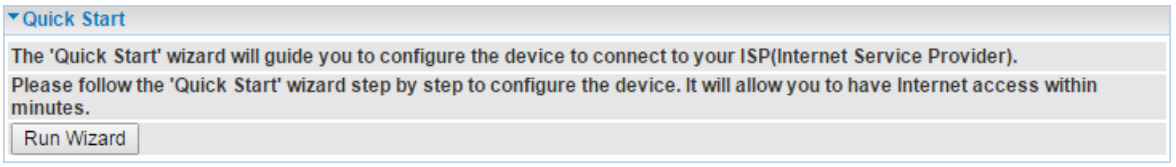


Current Status: Show VRRP current status, Master or Backup.

Current Master: Show the IP address of current master.

Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup password, time zone, and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

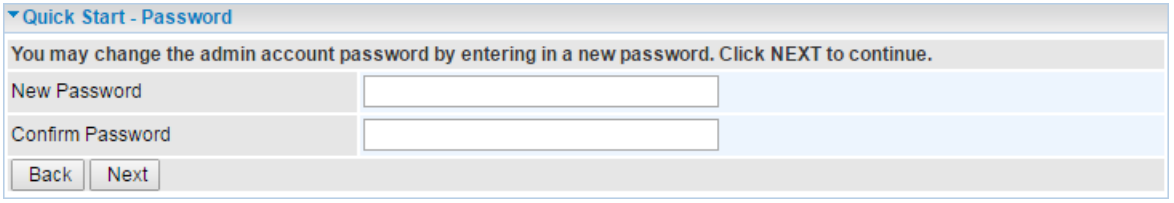


For detailed instructions on configuring WAN settings, see refer to the **Interface Setup** section.

Click **Next** to move on to Step 1.

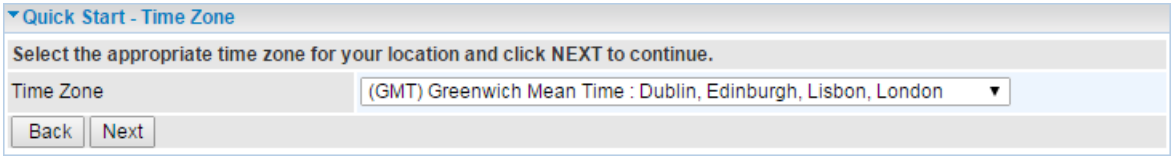
Step 1 – Password

Set new password of the **admin** account to access for router management. The default is **admin**. Once changed, please use this new password next time when accessing to the router. Click **Next** to continue.



Step 2 – Time Zone

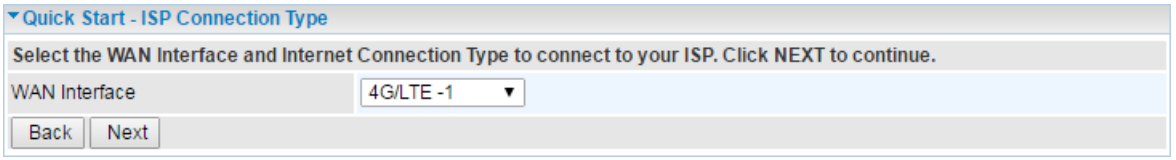
Choose your time zone. Click **Next** to continue.



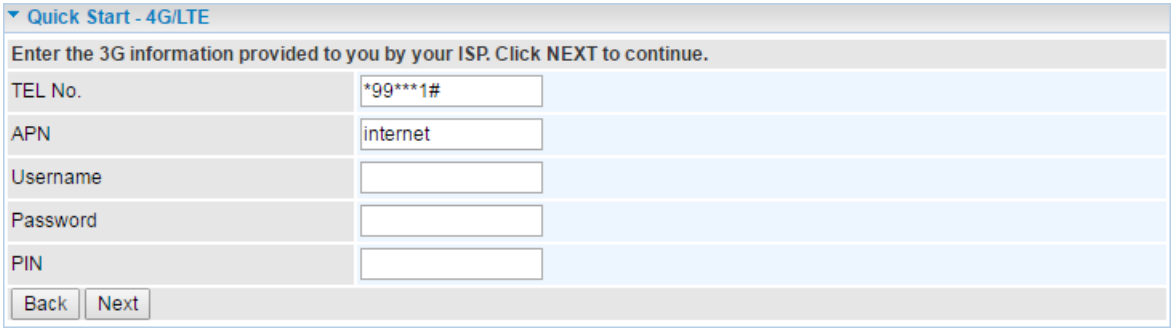
Step 3 – ISP Connection Type

Set up your Internet connection.

Select an appropriate WAN connection protocol then click **Next** to continue.

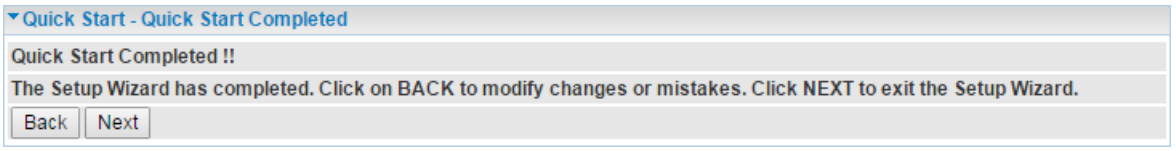


Input all relevant 3G/4G-LTE parameters from your ISP.



Step 4 – Quick Start Completed

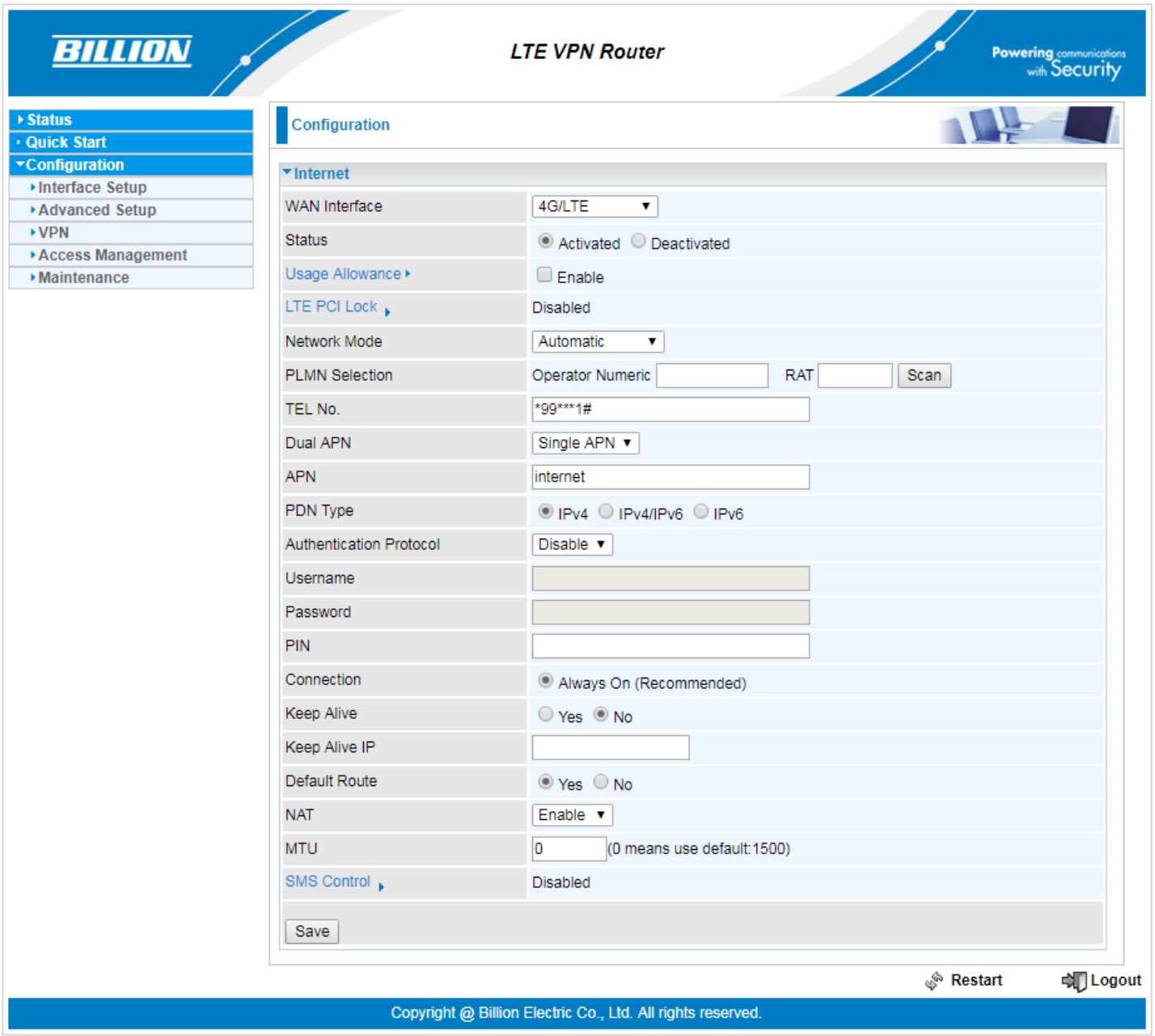
The Setup Wizard has completed. Click on **Back** to modify changes or mistakes. Click **Next** to save the current settings.



Step 5 – Quick Start Completed

Configuration

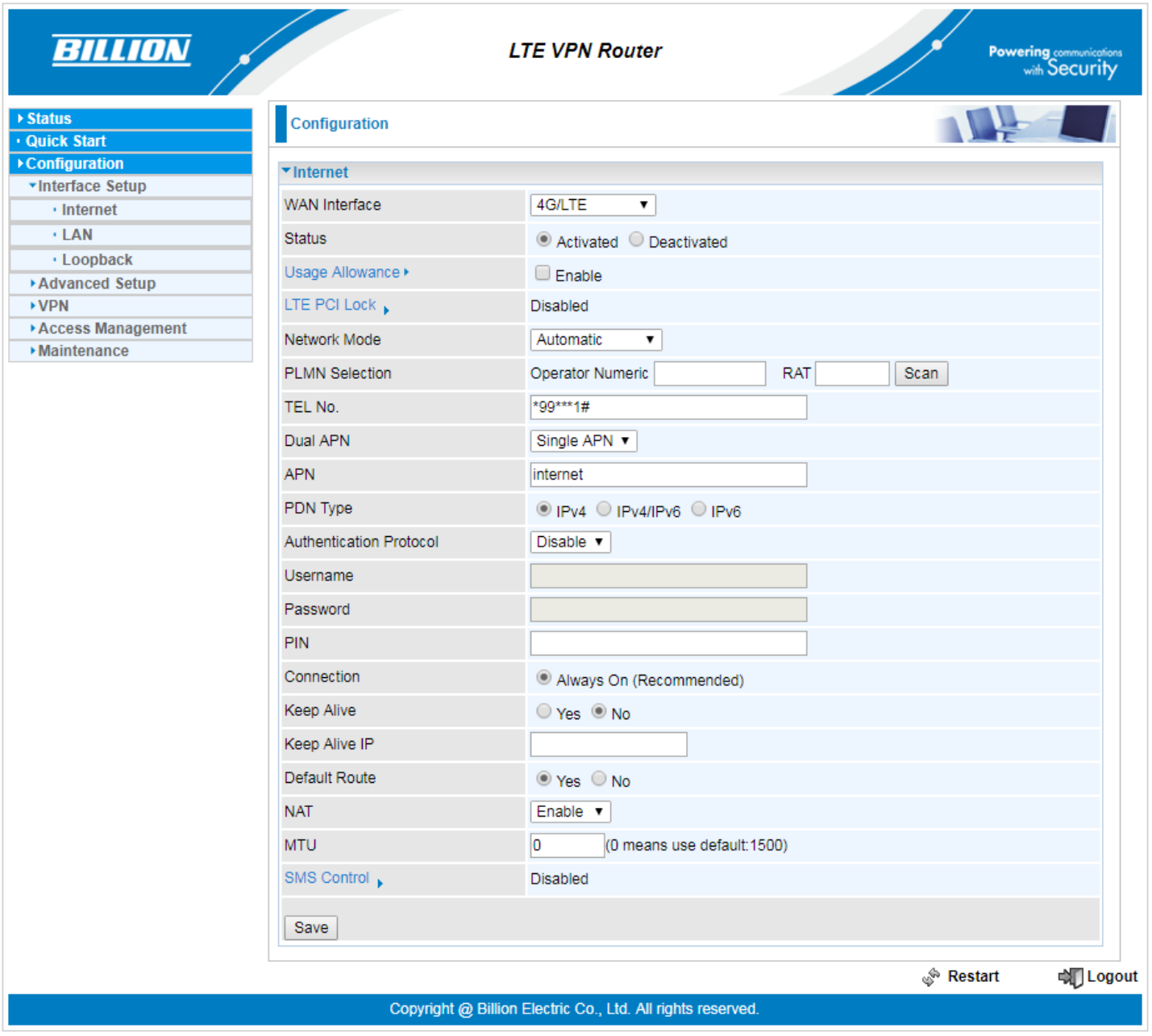
Click to access and configure the available features in the following: **Interface Setup, Advanced Setup, VPN, Access Management,** and **Maintenance.**



These functions are described in the following sections.

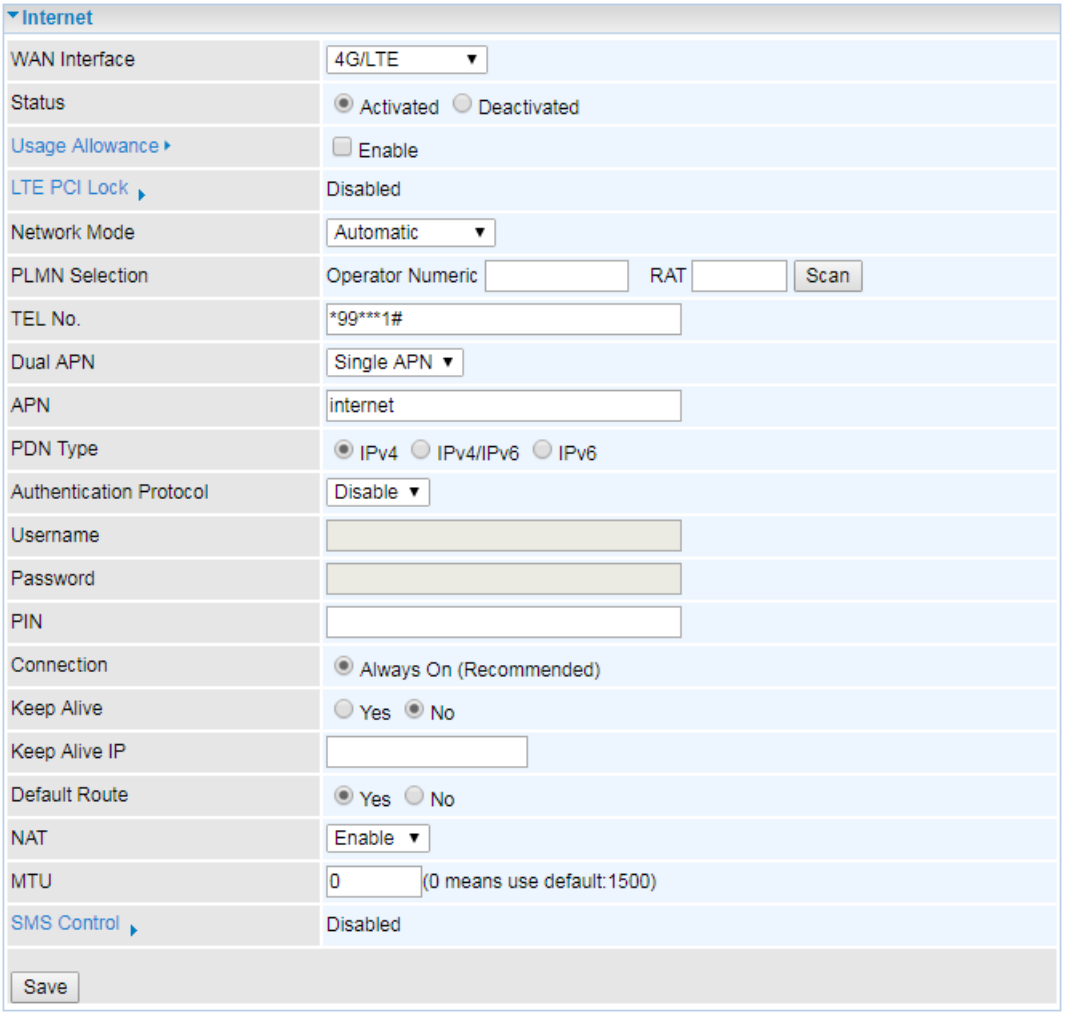
Interface Setup

Here are the features under **Interface Setup: Internet**, **LAN** and **Loopback**.



Internet

❖ 4G/LTE



Status: Choose Activated to enable the 3G/4G-LTE connection.

Usage Allowance: to control 4G/LTE flow, click it to further configure about 4G/LTE flow control, refer to the following **Usage Allowance** for more information.

LTE PCI Lock: Choose whether to lock to a specified PCI(Physical Cell Identifier). Users must know the target PCI or else ignore this setting. See **LTE PCI Lock** for more information.

IP Pass-Through Mode: When **enabled**, the device will gain a WAN IP via 4G/LTE dial-up and pass on to the PC connected to device, thus your PC gets a public WAN IP working on the internet.

Note: Under this circumstance, often only one PC is connected to the device. If you want to change PC, pls be reminded to release IP firstly.

Network Mode: There are some options of service standards: **Automatic**, **UMTS 3G only**, **GSM 2G Only**, **LTE Only**. If you are not sure which mode to use, you may select **Automatic** to auto detect the best mode for you.

PLMN Selection: Enter or press Scan button to detect a cloest base station(mobile service provider) from where you are. See **PLMN Selection** for more information.

TEL No.: The dial string to make a GPRS / 3G/4G-LTE user internetworking call. It may provide by your mobile service provider.

Dual APN: The Router can support up to two APNs. Select Single or Dual.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The

service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is **internet**.

PDN Type: Select the supported IP version, IPv4, Both IPv4/IPv6 or IPv6 only.

Authentication Protocol: Check if the ISP wants authentication, select PAP or ChAP.

Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authenticate. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly 3 times in a row, then the SIM card will be blocked and you will require a PUK code from your network/service provider.

Connection: Default set to Always on to keep an always-on 3G/4G-LTE connection.

Keep Alive: Select **Yes** to keep the 3G/4G-LTE connection always on.

Keep Alive IP: Enter the IP address whic is used for **ping**, and router will ping the IP to find whether the connection is on or not, if not, router will recover the connection.

Default Route: Select **Yes** to use this interface as default route interface.

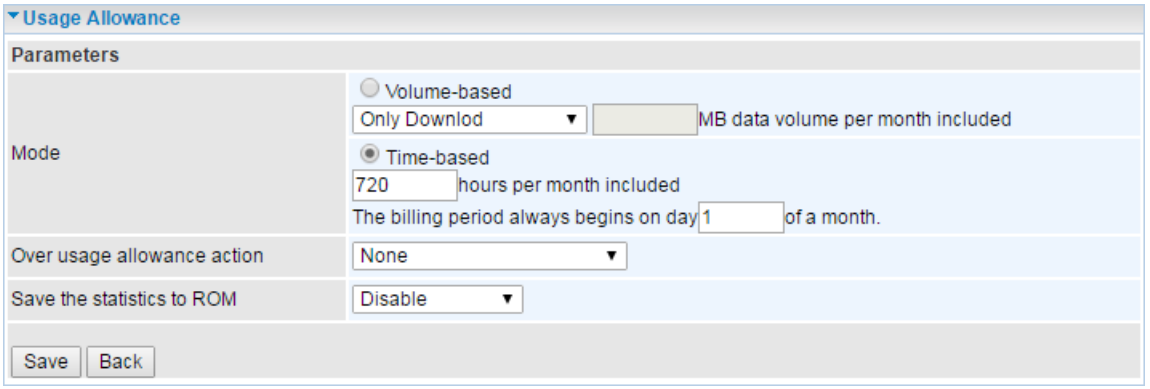
NAT: Select this option to Disabled/Enable the NAT (Network Address Translation) function. Enable NAT to grant multiples devices in LAN to access to the Internet through a single WAN IP.

MTU: Set the MTU(maximum transimission unit) value.

SMS Control*: SMS(Short Message Service) allows users to send short message using your smartphone to control the device remotely. Now it allows users to get status of LTE or remotely restart the device, refer to the following **SMS Control** for more information.

Note: SMS control depends on the equipped module's capabilities.

Usage Allowance:



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

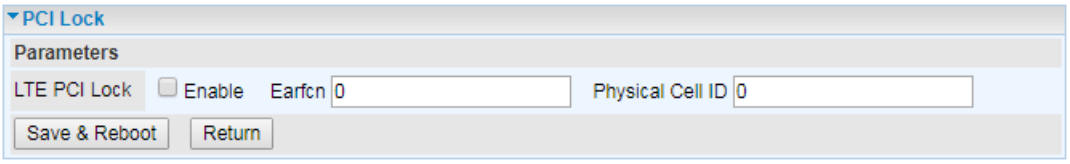
Volume-based include **only Download**, **only Upload** and **Download and Upload** to limit the flow. Time-based control the flow by providing specific hours per month.

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

Over usage allowance action: what to do when the flow is over usage allowance, the availablemethods are **Disconnect**, **E-mail Alert**, **E-mail Alert and Disconnect**.

Save the statistics to ROM: Save the statistics data to ROM system to avoid lost data if system reboot.

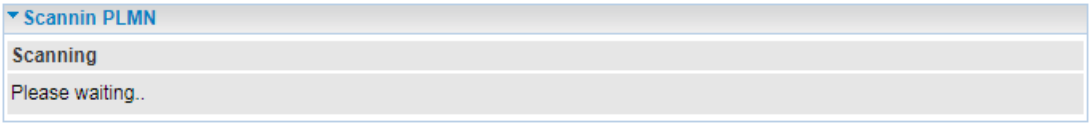
LTE PCI Lock:

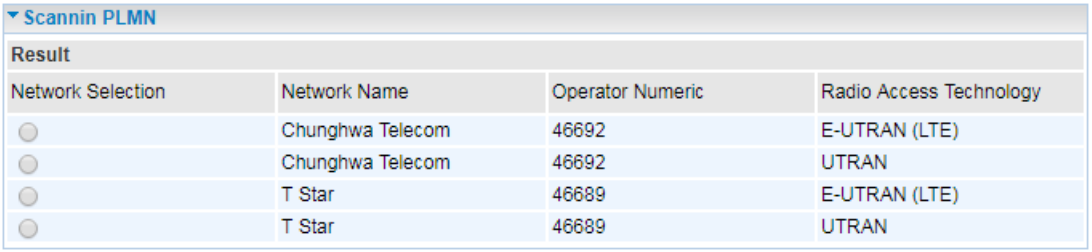


If an advanced user wants to lock to a designated PCI, please set the physical cell ID here.

PLMN Selection:

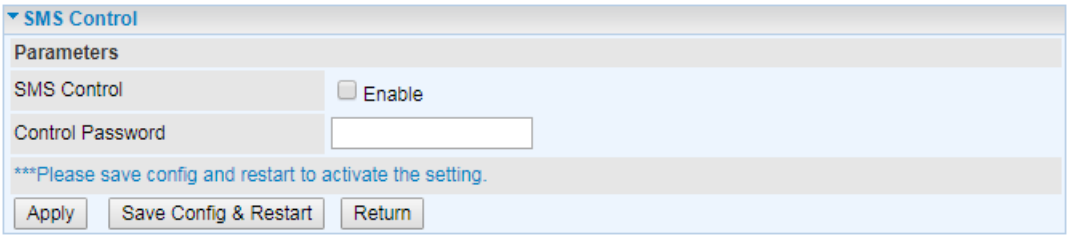
PLMN(Public Land Mobile Network) is a network that is established and operated by a mobile service provider. Each operator providing mobile services has its own PLMN identified by PLMN ID(MCC / MNC, digital sequence, no more than 6 digits) which is made up of MCC(Mobile Country Code) and MNC(Mobile Network Code). See the information in the sancing PLMN, choose the appropriate operator.





SMS Control:

SMS(Short Message Service) allows users to send short message using your smartphone to the SIM card's number to control the device remotely.



SMS Control: Check to enable the SMS control feature.

Control Password: Set the operation control password. The password is to avoid illegal operation directive to control the device.

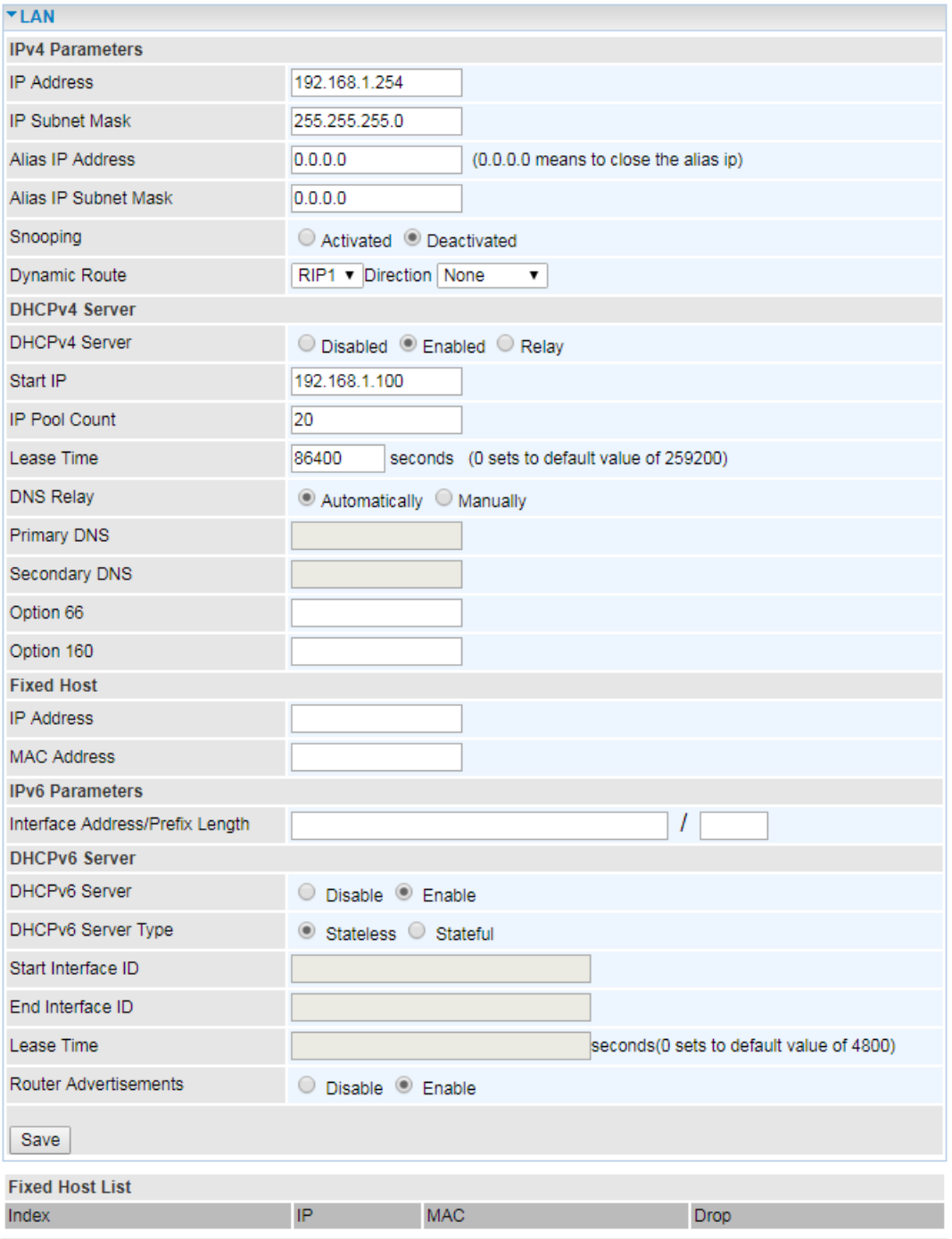
Now the SMS control supports 2 options:

- **Get status:** Issuing SMS with content *60 from smartphone to LTE Router to get LTE status of LTE Router.
- **Reboot device:** Issuing SMS with content reboot#password (e.g. the password is 123456, the content is reboot#123456) from smartphone to LTE Router, LTE Router will reboot when receiveing this SMS message.

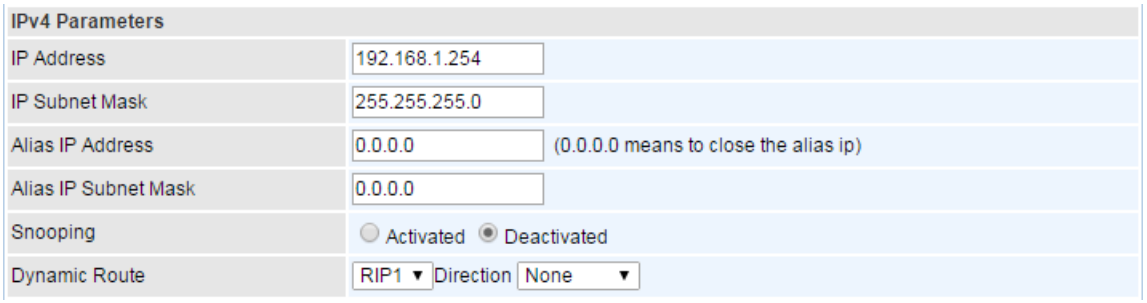
Note: SMS control depends on the equipped module's capabilities.

LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.



IPv4 Parameters



IP Address: Enter the IP address of Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

IP Subnet Mask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

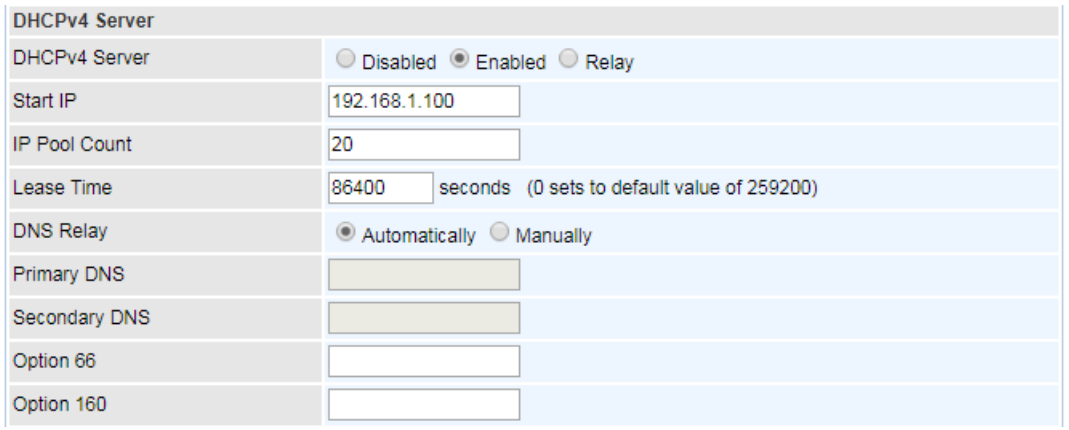
Alias IP Address: This is for local networks virtual IP interface. Specify an IP address on this virtual interface.

Alias IP Subnet Mask: Specify a subnet mask on this virtual interface.

Snooping: Select **Activated** to enable IGMP/MLD Snooping function, Without IGMP/MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP/MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

Dynamic Route: Select the RIP version from RIP1 or RIP2.

DHCPv4 Server



DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a server.

DHCPv4 Server: If set to **Enabled**, your M100 can assign IP addresses, default gateway and DNS servers to the DHCP client.

- If set to **Disabled**, the DHCP server will be disabled.
- If set to **Relay**, the M100 acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- When DHCP is used, the following items need to be set.

Start IP: This field specifies the first of the contiguous addresses in the IP address pool.

IP Pool Count: This field specifies the count of the IP address pool.

Lease Time: The current lease time of client.

Physical Ports: To determine which port(s) is/are subject to the DHCP address assignment by DHCPv4 server.

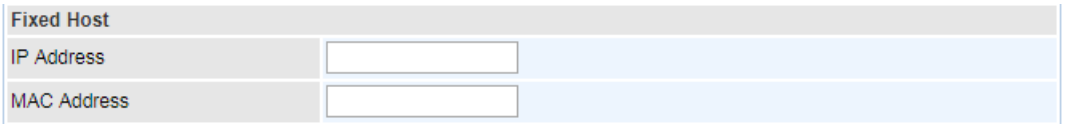
DNS Relay Select Automatically obtained or Manually set (if selected. Please set the exactly information).

Primary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Fixed Host

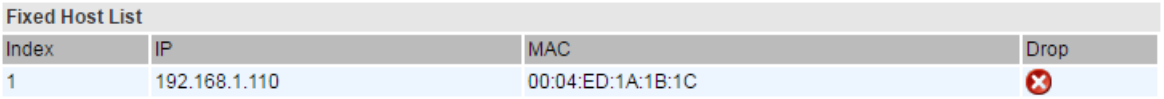
In this field, users can map the specific IP (must in the DHCP IP pool) for some specific MAC, and this information can be listed in the following table.



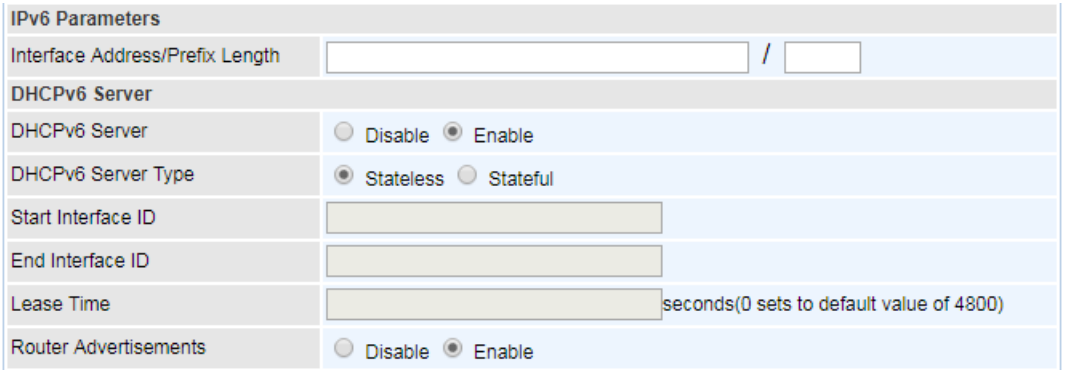
IP Address: Enter the specific IP. For example: 192.168.1.110.

MAC Address: Enter the responding MAC. For example: 00:0A:F7:45:6D:ED

When added, you can see the ones listed as showed below:



IPv6 parameters



The IPv6 address composes of two parts, thus, the prefix and the interface ID.

Interface Address / Prefix Length: Enter a static LAN IPv6 address. If you are not sure what to do with this field, please leave it empty as if contains false information it could result in LAN devices not being able to access other IPv6 device. Router will take the same WAN's prefix to LAN side if the field is empty.

DHCPv6 Server

There are two methods to dynamically configure IPv6 address on hosts, **Stateless** and **Stateful**.

Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a

link, while hosts generate an **interface identifier** that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

Stateful configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available.

- **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server.
- **Stateful:** If selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

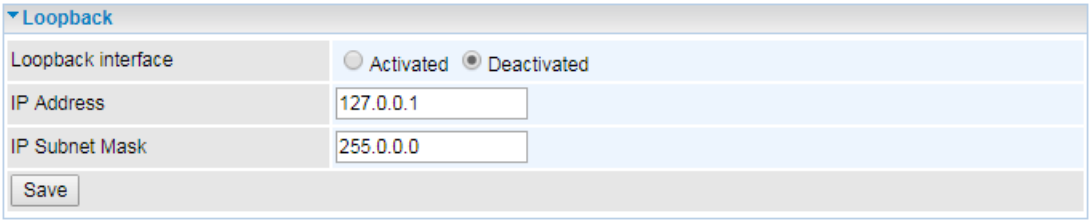
End interface ID: enter the end interface ID.

Leased Time (hour): the leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Router Advertisement: Check to Enable or Disable the Issue Router Advertisement feature. This feature is to send Router Advertisement messages periodically which would multicast the IPv6 Prefix information (similar to v4 network number 192.168.1.0) to all LAN devices if the field is enabled. We suggest enabling this field.

Loopback

Lookback interface is a widely known virtual interface on routers which is highly robust and always up, not like physical interfaces which disconnect every now and then. The lookback interface can have its own IP and subnet mask. It is often used for router management as Telnet management IP and involved in BGP as BGP Update-Source, involved in OSPF as Router ID.

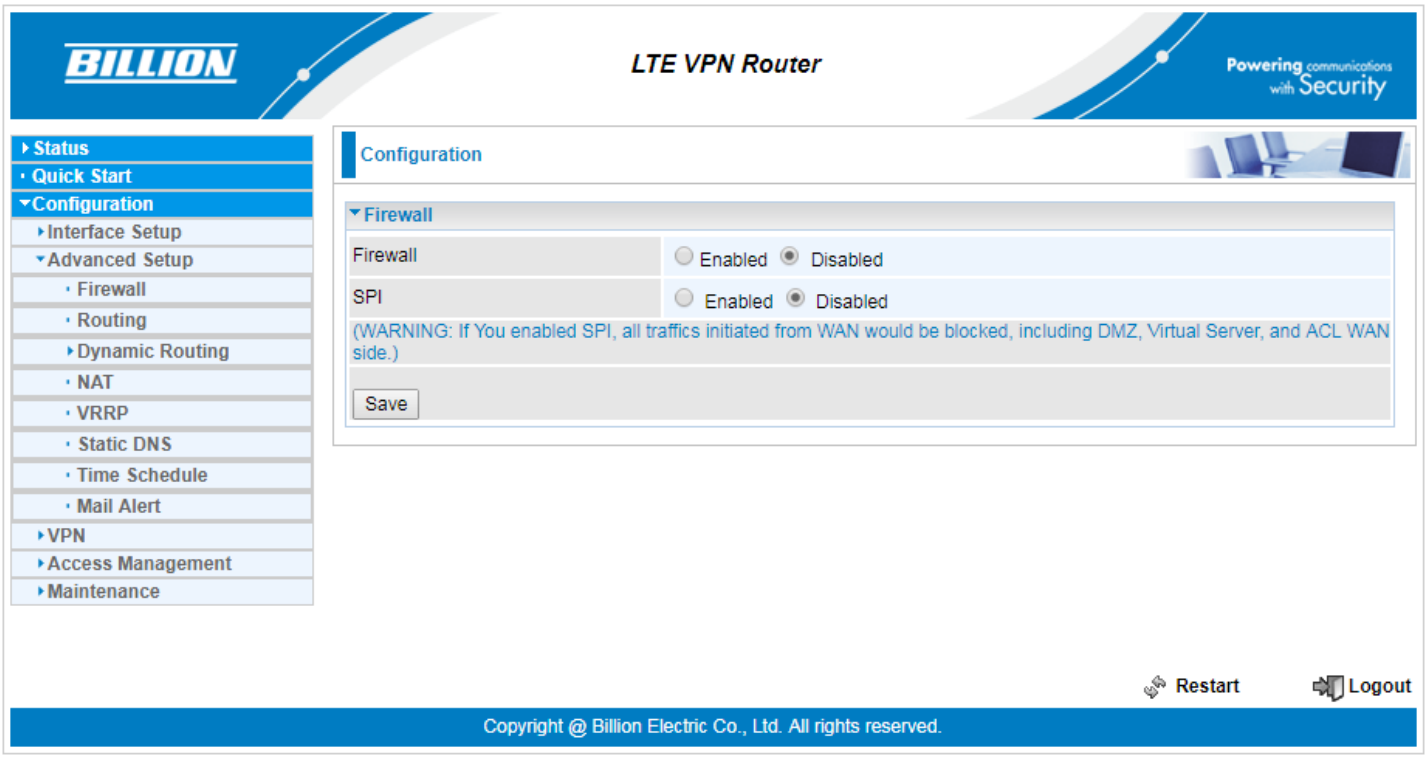


IP Address: To specify the IP for the lookback interface.

IP Subnet Mask: To specify the subnet mask for the lookback interface.

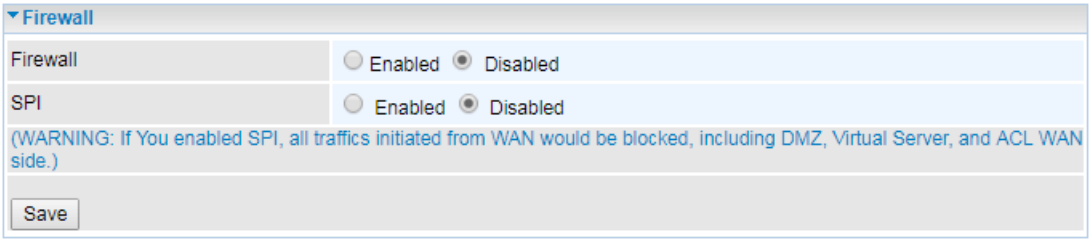
Advanced Setup

Advanced Step provides advanced features including **Firewall**, **Routing**, **Dynamic Routing**, **NAT**, **VRRP, Static DNS**, **Time Schedule** and **Mail Alert** for advanced users.



Firewall

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



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

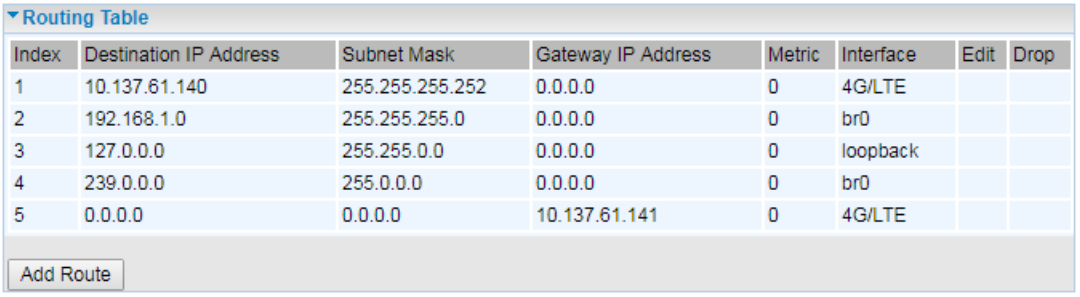
- **Enabled:** It activates your firewall function.
- **Disabled:** It disables the firewall function.

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

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

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.



Index: 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.

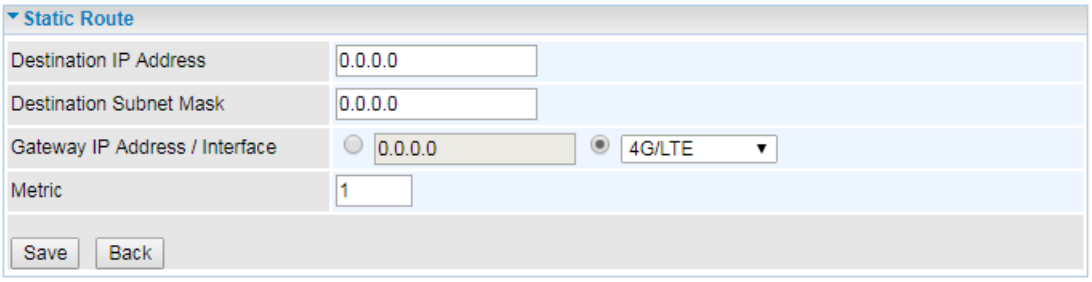
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

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



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.

Dynamic Routing

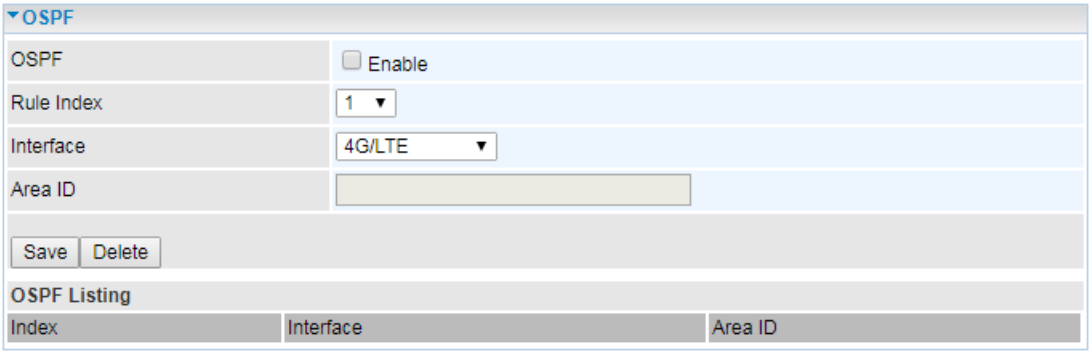
OSPF

Open Shortest Path First (**OSPF**) is a most widely used interior gateway protocil (IGP) for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

OSPF allows collections of rotuers to be grouped together. Such a group is called an area (AS). Each area runs a seprate copy of the basic link-state routing algorithm. This means that each area has its own link-state database and cooresponding shortest path tree.

The structure of an area is invisible from other areas. This isolation of knowledge makes the protocol more scalable if multiple areas are used.

The most widely used exterior gateway protocol is the Border Gatewat Protocol (BGP), which will be our next topic, the pricipal routing protocol between autonomous systems on the itnernet.



OSPF: Enable to actiavte OSPF routing.

Rule Index: A totoal 10 OSPF rules are allowed, ranging from 0 to 9.

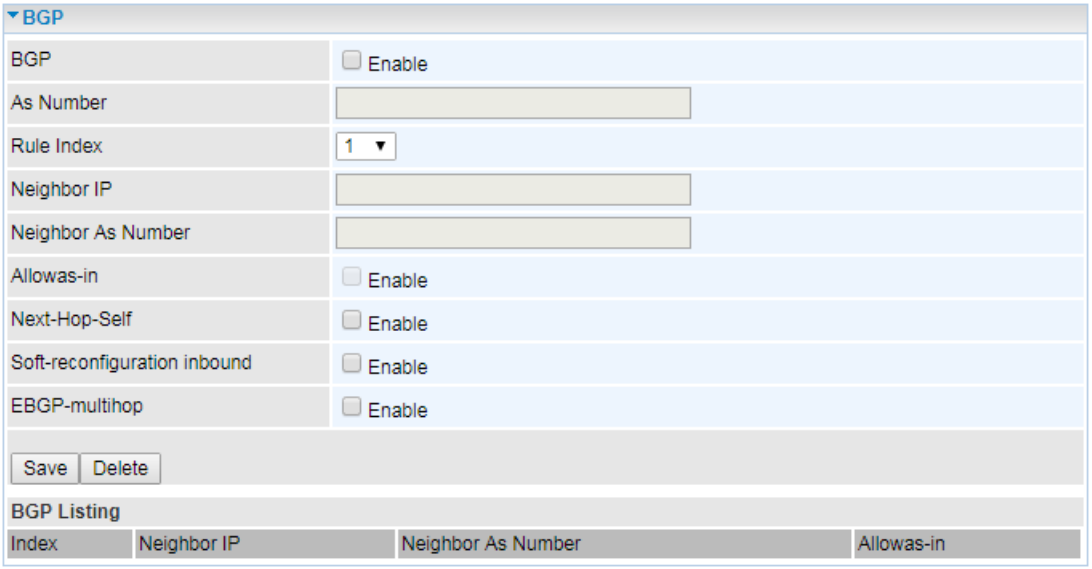
Interface: Set the interface which runs the OSPF process (involved in OSPF routing). It can be WAN interfaces or established GRE tunnels.

Area ID: The OSPF area identifier. It is a decimal number in the rang of 0-4294967295. Here to set the area ID which the inteface belongs to. The area with area-id=**0** is the backbone area.

If the router has networks in more than one area, then an area with area-id=**0** (the backbone) must always be present. All other areas are connected to it. The backbone is responsible for distributing routing information between non-backbone areas. The backbone must be contiguous, i.e. there must be no disconnected segments. However, area border routers do not need to be physically connected to the backbone - connection to it may be simulated using a virtual link.

BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol (an uniquely TCP basded inter-Autonomous System routing protocol) designed to allow setting up an inter-domain dynamic routing system that automatically updates routing tables of devices running BGP in case of network topology changes.



BGP: Enable to activate BGP routing.

AS Number: Designate the AS number of local router. The AS number is used to identify the IBGP or EBGP your neighbor is running.The same AS number means the IBGP, and the different means EBGP.

Rule Index: A totoal 10 BGP rules are allowed, ranging from 0 to 9.

Neighbor IP: Set your neighbor IP.

Neighbor AS Number: Set your neghbor AS number.

Allowas-in: Enable to allow inter-communication between devices in the same AS. If the local and neighbor AS number are the same, thus, a inter-AS communication, please enable the allowas-in. Otherwise, the router only support EBGP routing between different domains.

Next-Hop-Self: Enable to use the router's own loopback address as the next-hop address.

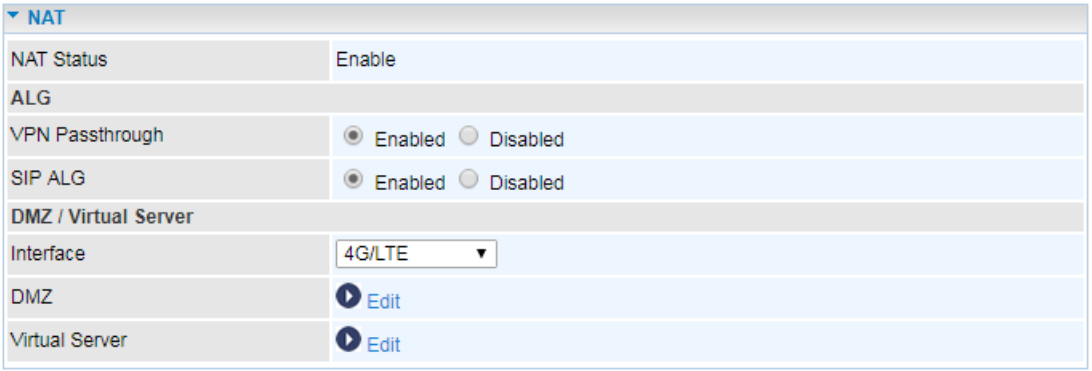
Self-reconfiguration inbound: Enable to tells the router (BGP course) to save all recived updates of the routing information from all neighbors. When the BGP connections are reset (Clear IP BCP), these updates are used to generate the new inbound updates.

EBGP-Multihop: Eanble to allows a BGP speaker to establish a peering session with a router that is not directly connected.

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.



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.

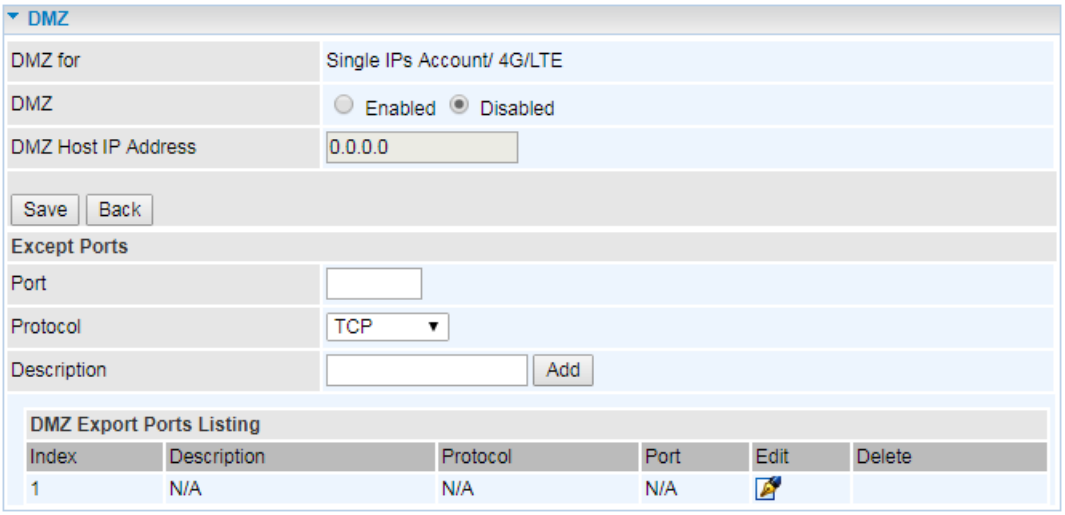
Interface: Select to set DMZ/Virtual Server for **4G/LTE 1**, **4G/LTE 2** or **Wireless Client**.

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

Note: This feature disables automatically if WAN connection is in BRIDGE mode.

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



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

DMZ:

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

Except Ports: Commonly, all incoming packets will be passed to the DMZ host after being checked by the Firewall and NAT algorithms. But if a packet matching the rules set under **except ports**, it will be passed on to virtual server or dropped when no matches found in virtual server.

Port: Set the port to be monitored.

Protocol: Choose the protocol to be monitored.

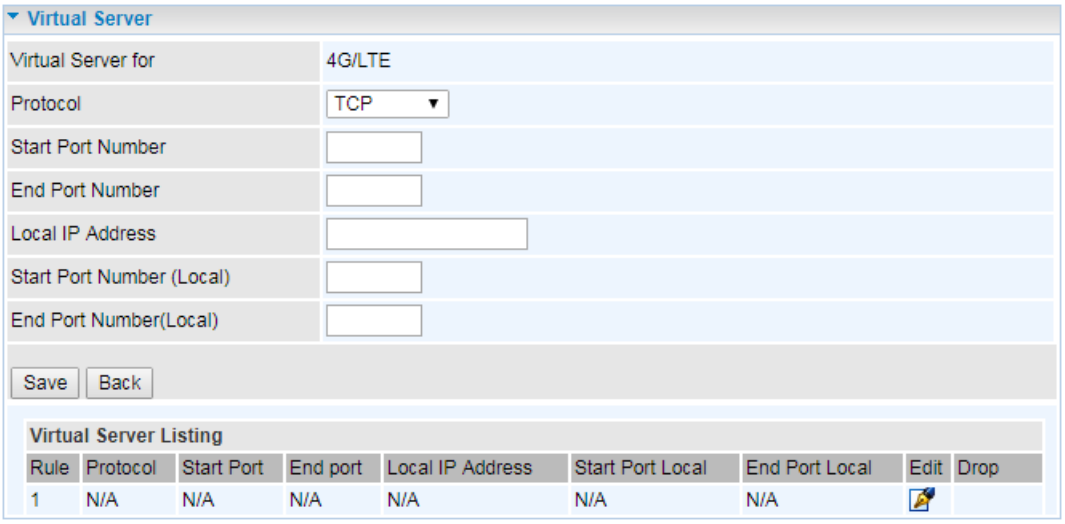
Description: The description given to the DMZ exception rule .

Click **Add** to add except rules.

Virtual Server

Note: This feature disables automatically if WAN connection is in BRIDGE mode.

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



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

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 21 or Start: 1000, End: 2000).

The starting greater than zero (0) and the ending port must be the same or larger than the starting port.

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

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

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

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 Interface Setup - Internet 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.

Example: How to setup Port Forwarding for port 21 (FTP server)

If you have a FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server.**

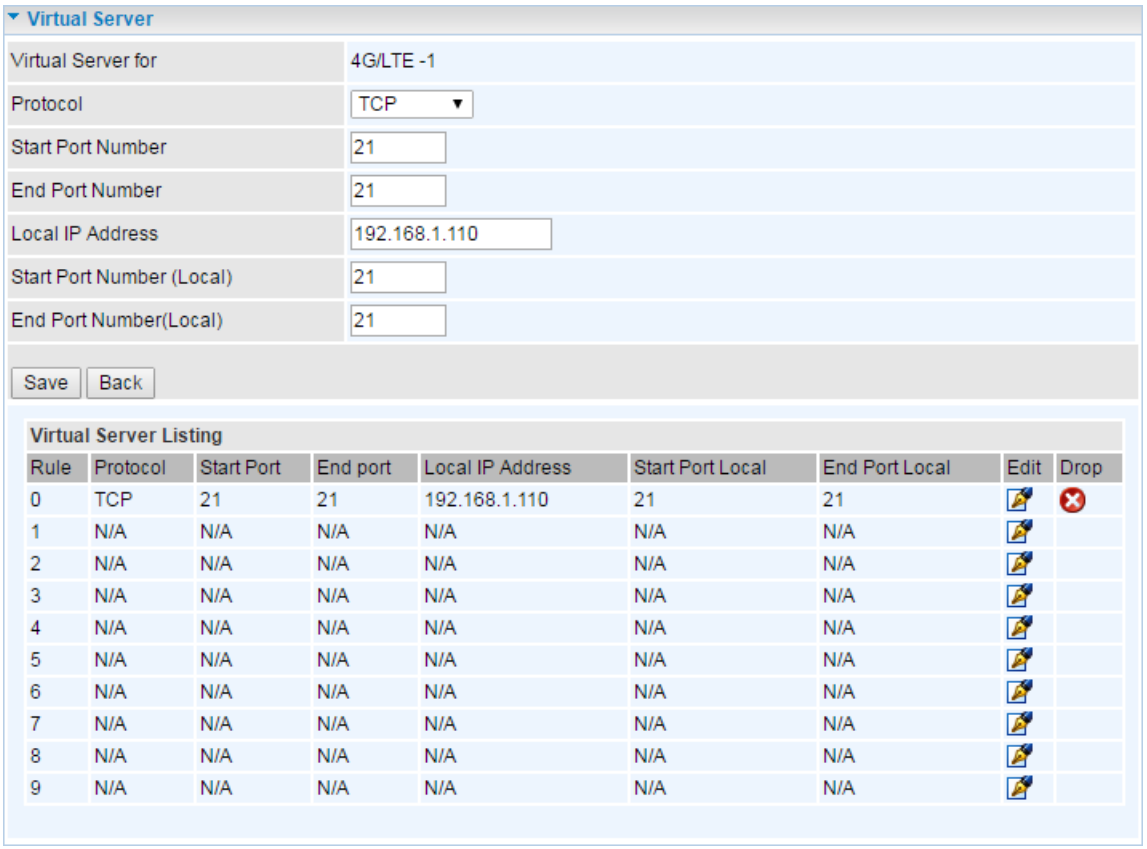
FTP server uses TCP protocol with port 21.

Enter **21** to Start and End Port Number. M100 will accept port 21 requests from WAN side.

Eneter the static IP assiged to the local PC that is hosting the FTP server. Ex: 192.168.1.110

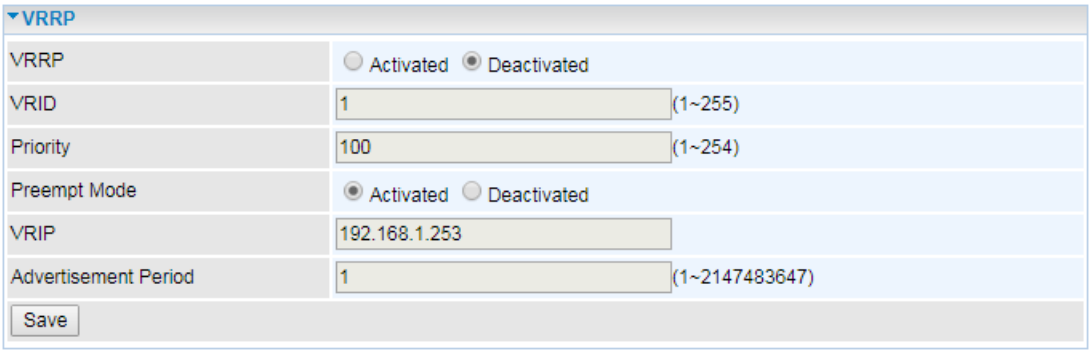
Enter **21** to Local Start and End Port number. M100 will forward port 21 request from WAN to the specific LAN PC (ex:192.168.1.110) in the network.

Step 3: Click **Save** to save settings.



VRRP

The VRRP(Virtual Router Redundancy Protocol) is a computer networking protocol that provides for automatic assignment of available gateway to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.



VRRP: Check to activate this feature.

VRID: A master or backup router running the VRRP protocol may participate in one VRID instance.

Priority: Specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. The priority value for the VRRP router that owns the IP address associated with the virtual router MUST be 255. VRRP routers backing up a virtual router MUST use priority values between 1 and 254. The default priority value for VRRP routers backing up a virtual router is 100. The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.

Preempt Mode: When preempt mode is activated, a backup router always takes over the responsibility of the master router. When deactivated, the lower priority backup is left in the master state.

VRIP: One IP address that is associated with the virtual router.

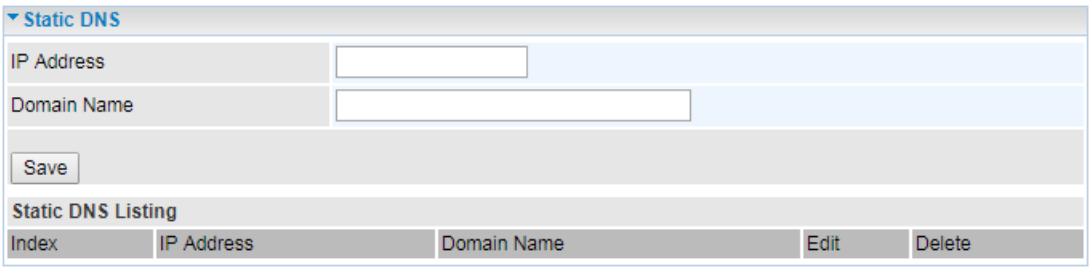
Advertisement period: Indicates the time interval in seconds between advertisements.

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

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).



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

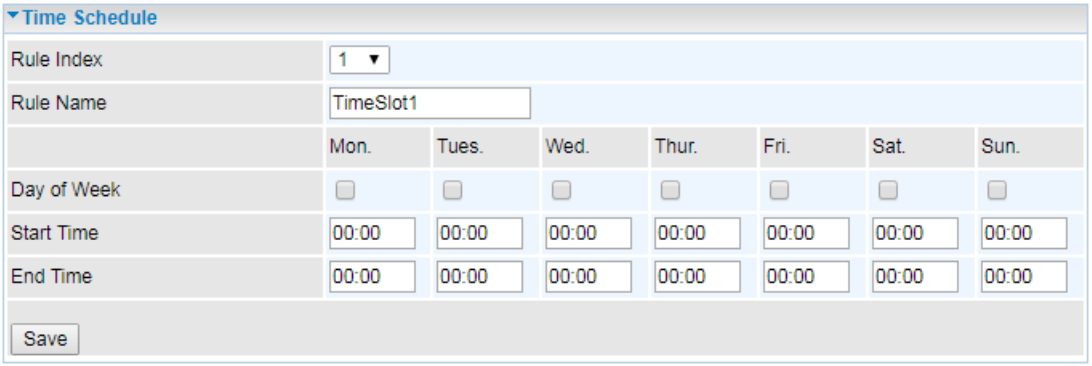
Domain Name: The friendly domain name for the IP address.

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

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.



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

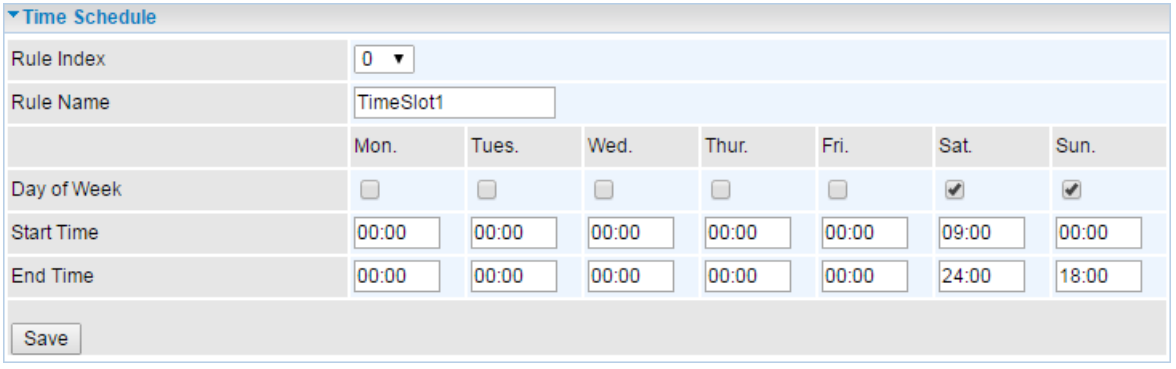
Rule Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from **Day of Week**.

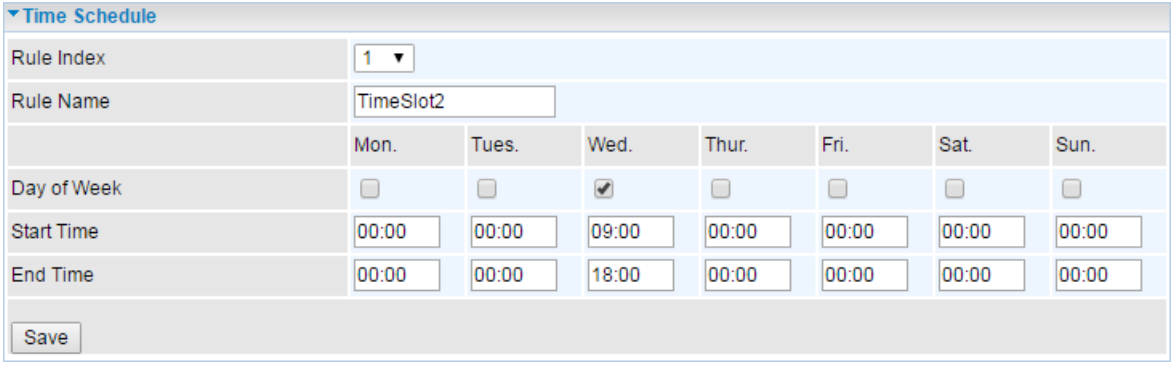
Start Time: The starting point of the interval for the timeslot, anytime in 00:00 – 24:00.

End Time: The ending point of the interval for the timeslot, anytime in 00:00 – 24:00.

For example, user can add a timeslot named **TimeSlot1** which features a period from 9:00 of Saturday to 18:00 of Sunday.

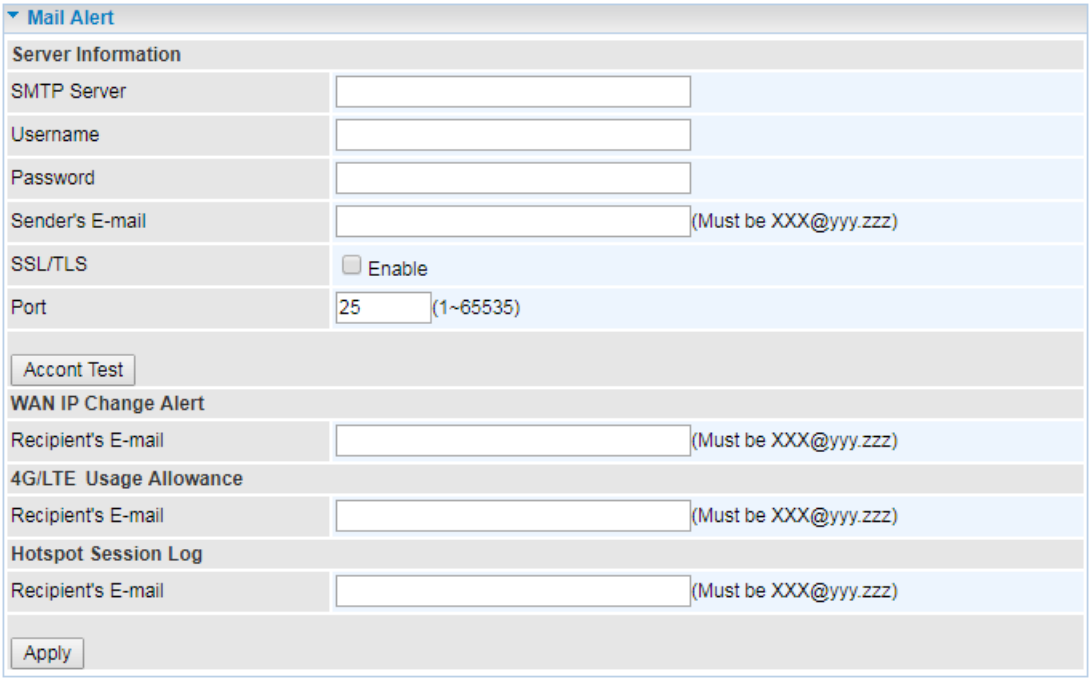


Another TimeSlot2 spanning from 09:00 to 18:00 of Wednesday



Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL/TLS: Check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

WAN IP Change Alert (Recipient's Email): Enter the email address that will receive the alert message once a WAN IP change has been detected.

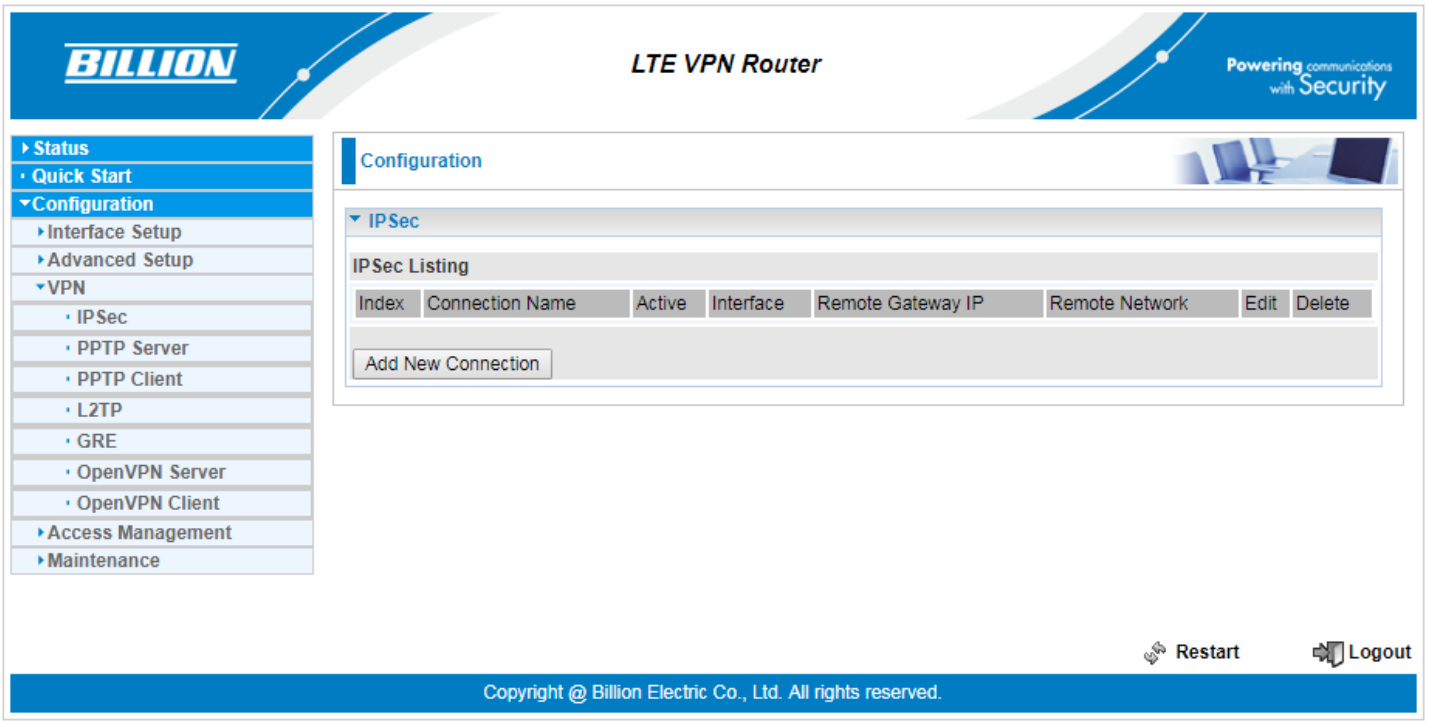
3G/LTE Usage Allowance (Recipient's Email): Enter the email address that will receive the alert message once the 3G/4G LTE over Usage Allowance occurs.

Hotspot Session Log (Recipient's Email): Enter the email address that will receive the periodic mail of the session log information to track the hotspot session information.

VPN (BiPAC 4700ZU 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.

BiPAC 4700ZU supports **IPSec, PPTP, L2TP, GRE, OpenVPN** for enterprise users.

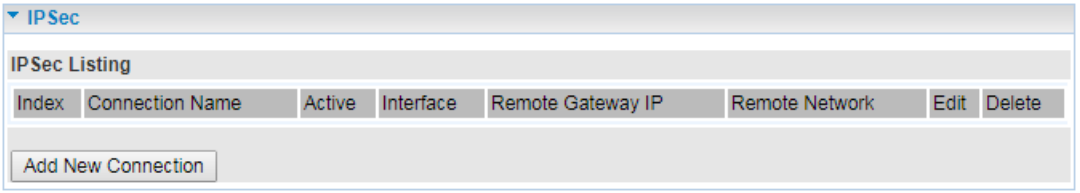


IPSec

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

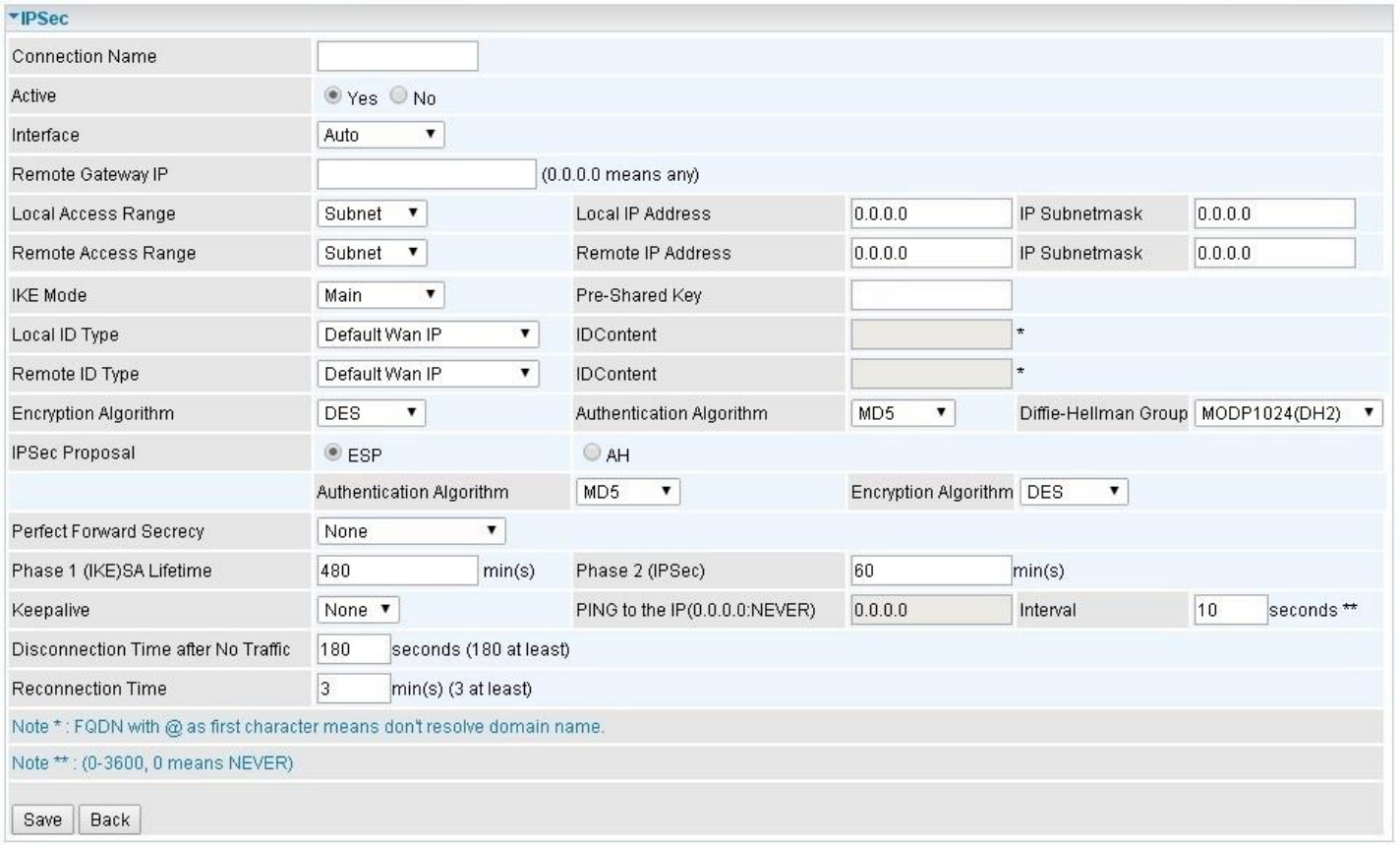
IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

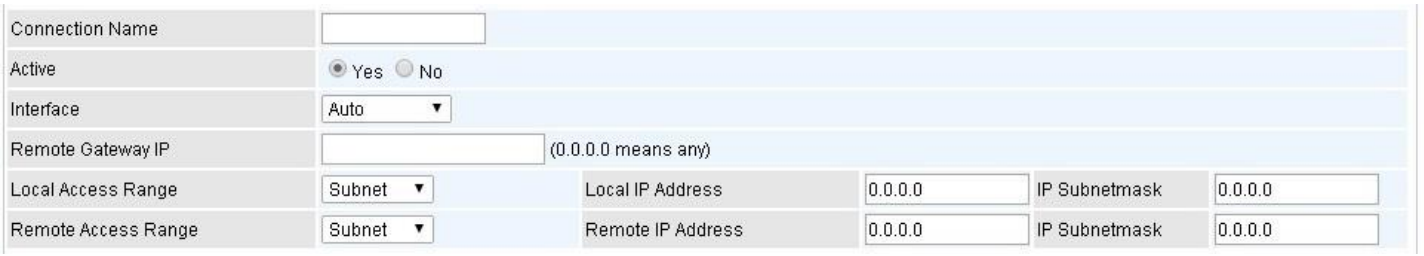
Note: up to 16 IPSec tunnels can be added.



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

IPSec Connection Setting





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

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

Interface: Select the set used interface for the IPSec connection, when you select 3G/4G-LTE interface, the IPSec tunnel would 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.

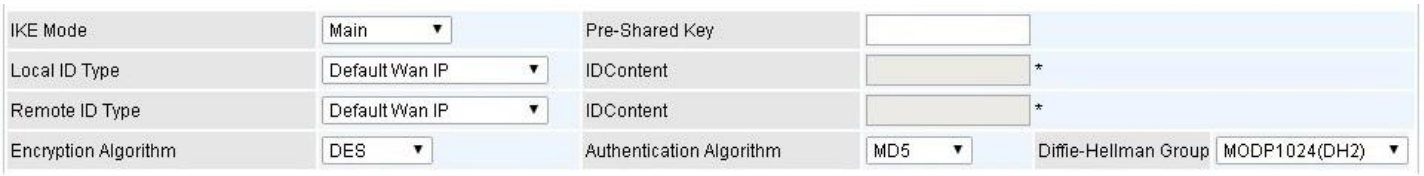
- **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

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.

IPSec Phase 1(IKE)



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

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

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

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

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

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

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

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

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

IPSec Phase 2(IPSec)

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.

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.

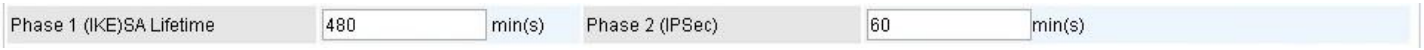
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

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.

Perfect Forward Secrecy: 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.

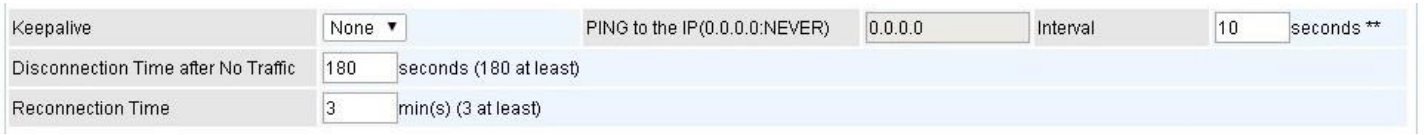
IPSec SA Lifetime



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.

IPSec Conneciton Keep Alvie



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.

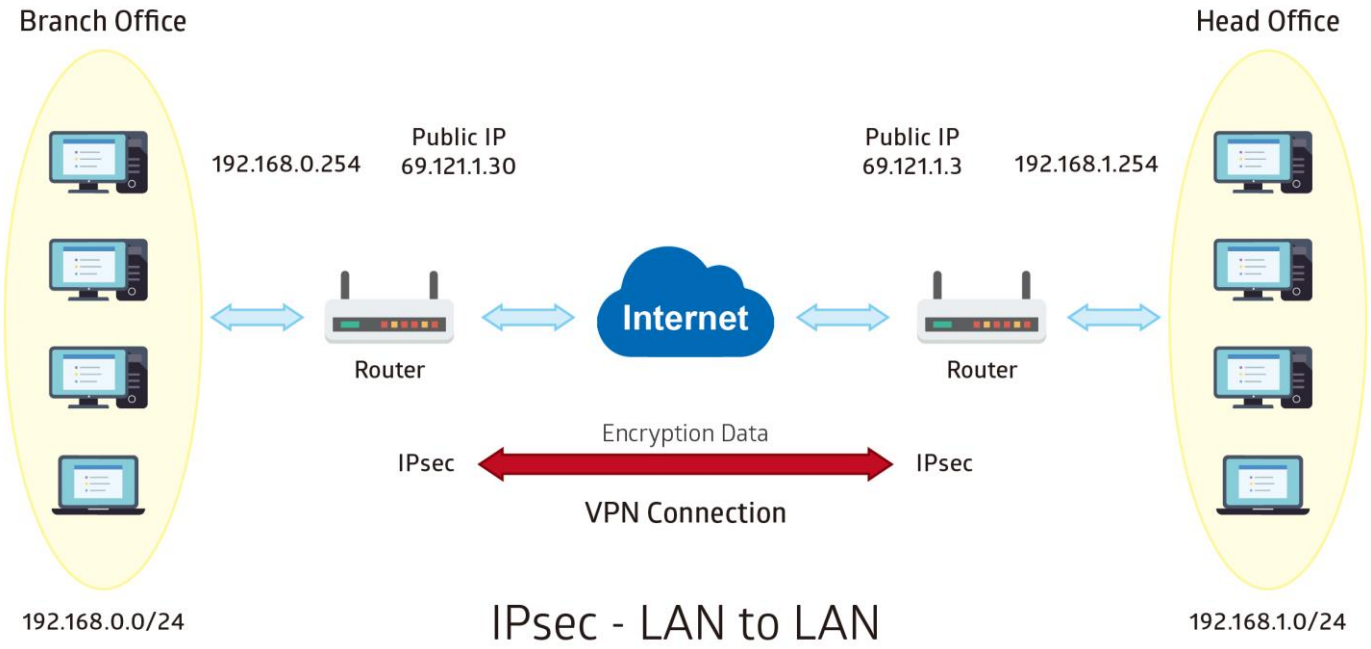
Click **SAVE** to submit the settings.

Example: How to establish an IPSec Tunnel

1. LAN-to-LAN connection

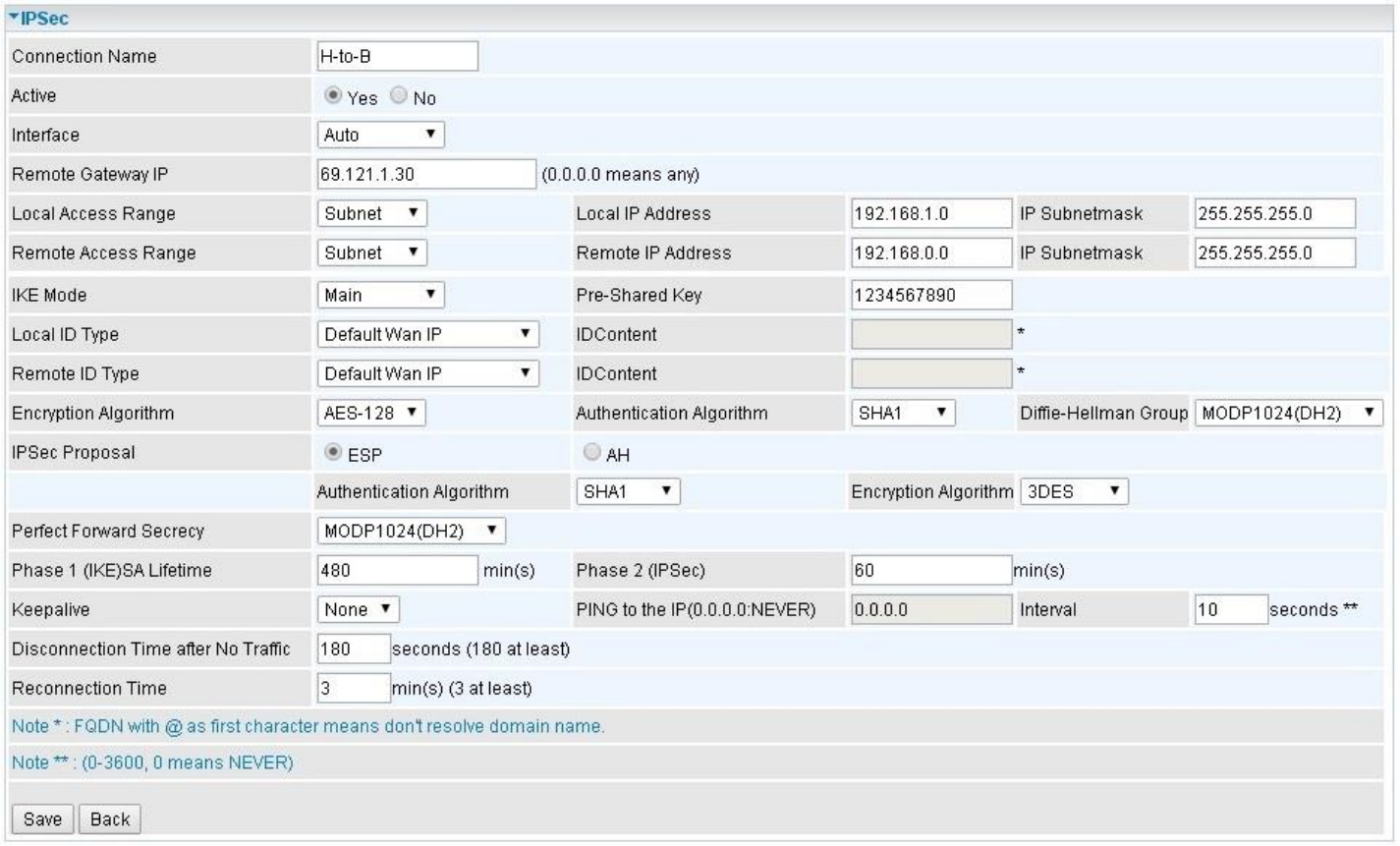
Two VPN router want to setup a secure IPSec VPN tunnel

Note: The IPSec Settings shall be consistent between the two routers.



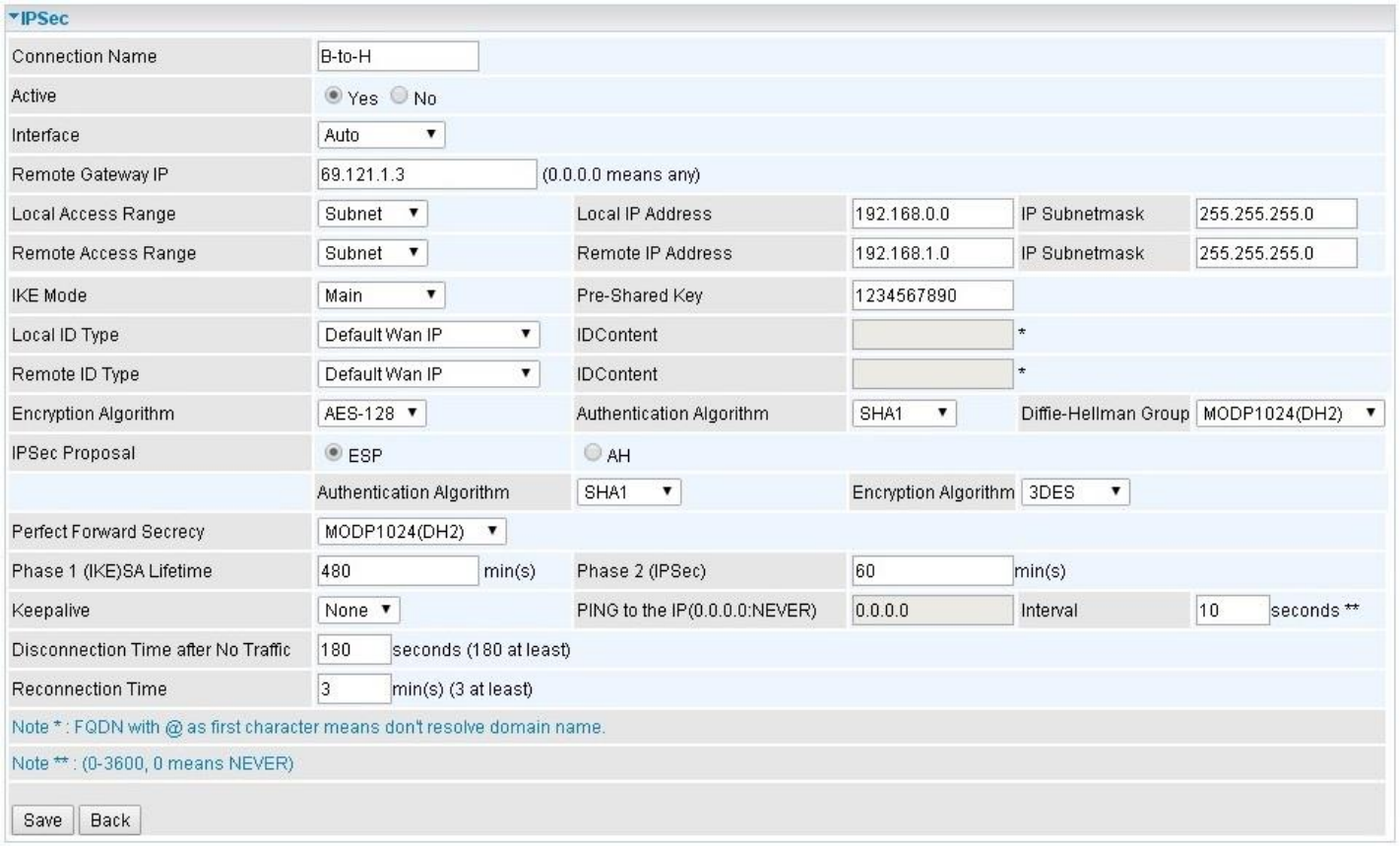
Head Office Side:

Item		Description
Connection Name	H-to-B	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Head Office network
Local Netwrok IP Address	192.168.1.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Netwrok IP Address	192.168.0.0	
Remote Netwrok Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	



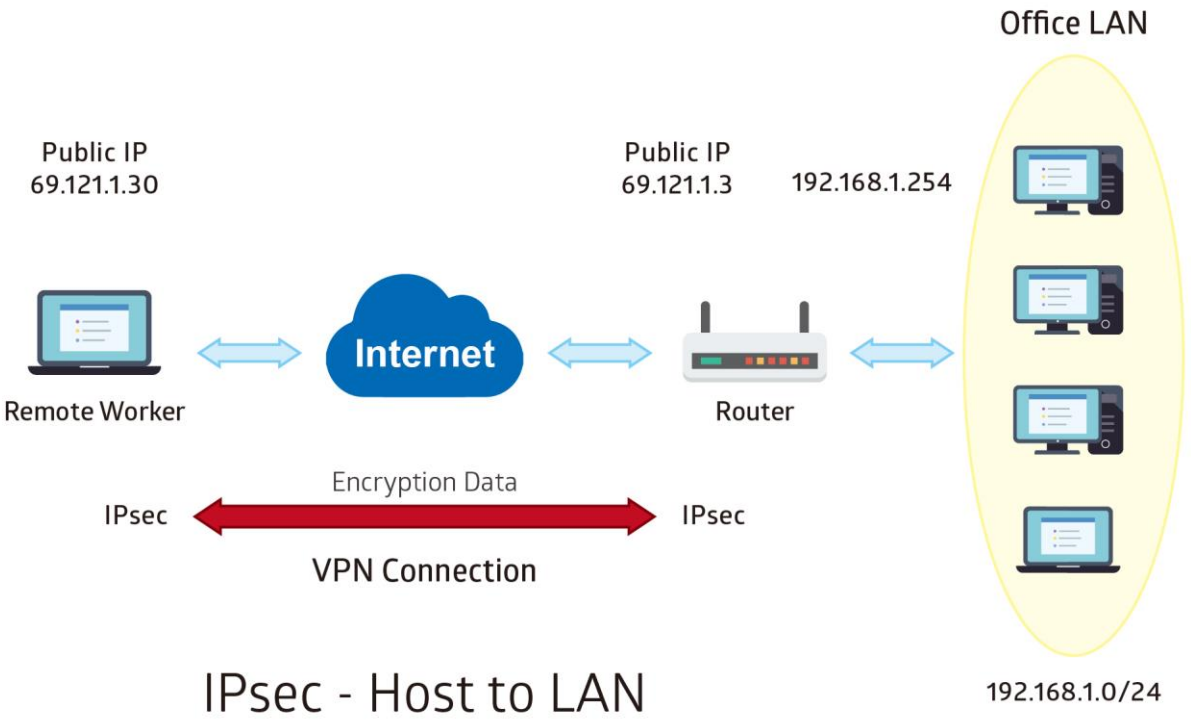
Branch Office Side:

Item		Description
Connection Name	B-to-H	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.3	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Head Office network
Local Netwrok IP Address	192.168.0.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Netwrok IP Address	192.168.1.0	
Remote Netwrok Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	



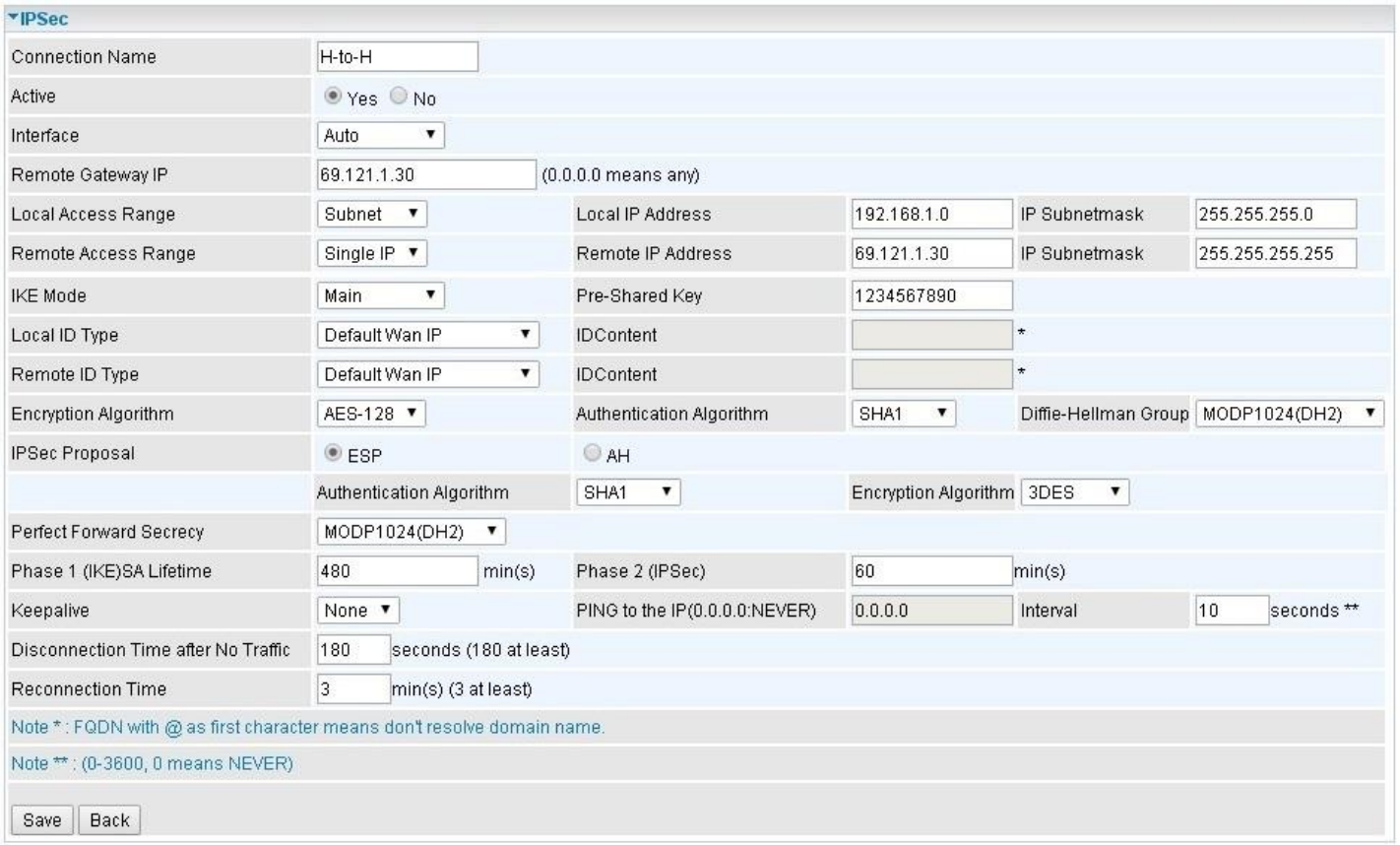
2. Host to LAN

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



Head Office Side:

Item		Description
Connection Name	H-to-H	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Netork		
Local Access Range	Subnet	Head Office network
Local Netwrok IP Address	192.168.1.0	
Local Netwrok Netmask	255.255.255.0	
Remote Access Range	Signal IP	Host
Remote Netwrok IP Address	69.121.1.30	
Remote Netwrok Netmask	255.255.255.255	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	

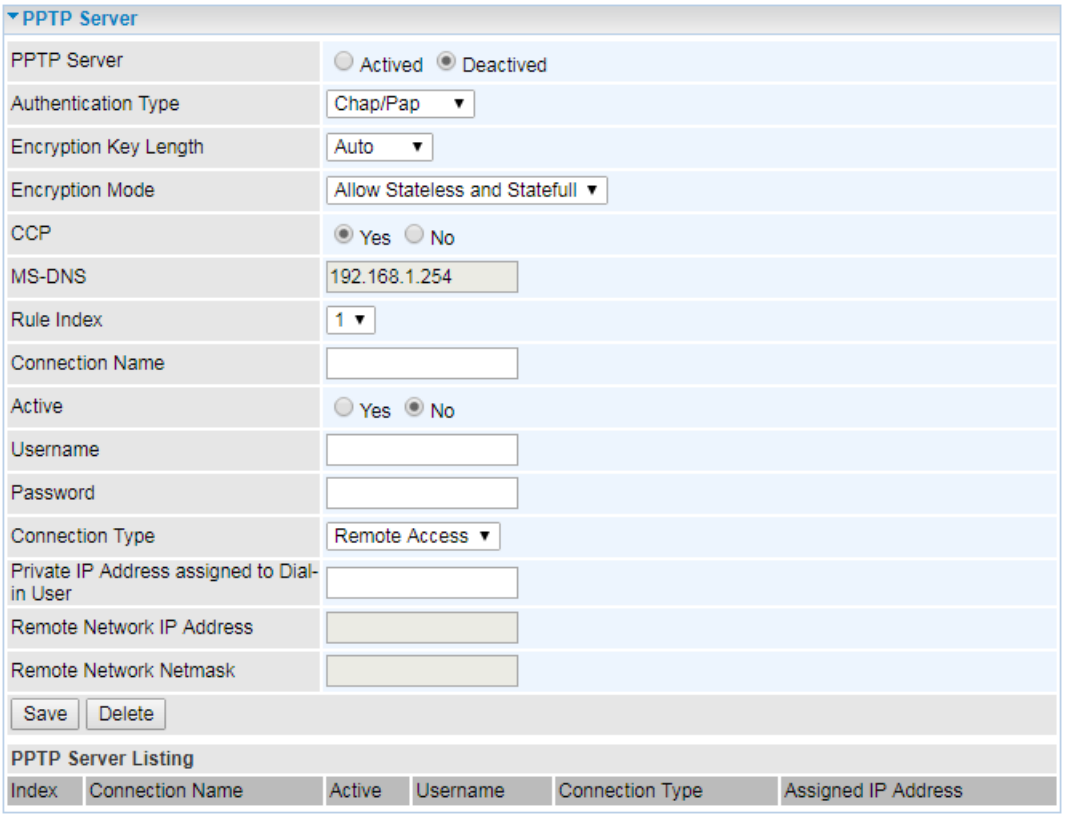


PPTP Server

The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network.

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: 8 sessions for Server and 8 sessions for Client respectively.



PPTP Server: Select **Actived** to activate PPTP Server. **Deactived** to deactivate PPTP Server.

Authentication Type: The authentication type, Chap/Pap, Pap, Chap or MS-CHAPv2 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.

Encryption Ley Length: Available when using MS-CHAPv2 authentication mode. The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Encryption Mode: Select the encryption mode, Allow stateless and statefull or only stateless. The key will be changed every packet when you select Stateless mode.

CPC: Choose whether to enbale CCP(Compression Control Protocol) which is used for establishing and configuring data compression algorithms on both ends of the point-to-point link.

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.

Rule Index: The Index to mark the session.

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

Active: Select **Yes** 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 Dial-in 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.

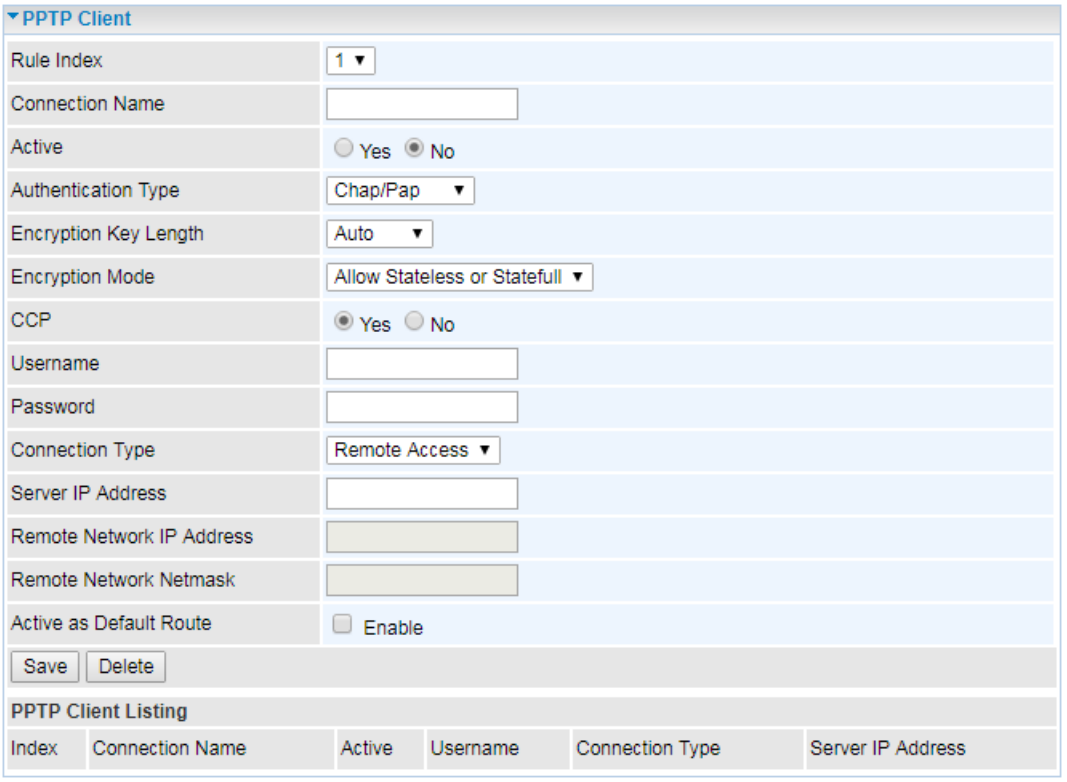
Remote Network IP Address: Please input the subnet IP for remote network.

Remote Network Netmask: Please input the Netmask for remote network.

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

PPTP Client

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



Rule Index: The Index to mark the session.

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

Active: Select **Yes** to activate the account. PPTP server is waiting for the client to connect to this account.

Authentication 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.

Encryption Key Length: Available when using MS-CHAPv2 authentication mode. The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Encryption Mode: Select the encryption mode, Allow stateless and statefull or only stateless. The key will be changed every packet when you select Stateless mode.

CPC: Choose whether to enbale CCP(Compression Control Protocol) which is used for establishing and configuring data compression algorithms on both ends of the point-to-point link.

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.

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

Remote Network IP Address: Please input the subnet IP for remote network.

Remote Network Netmask: Please input the Netmask for remote network.

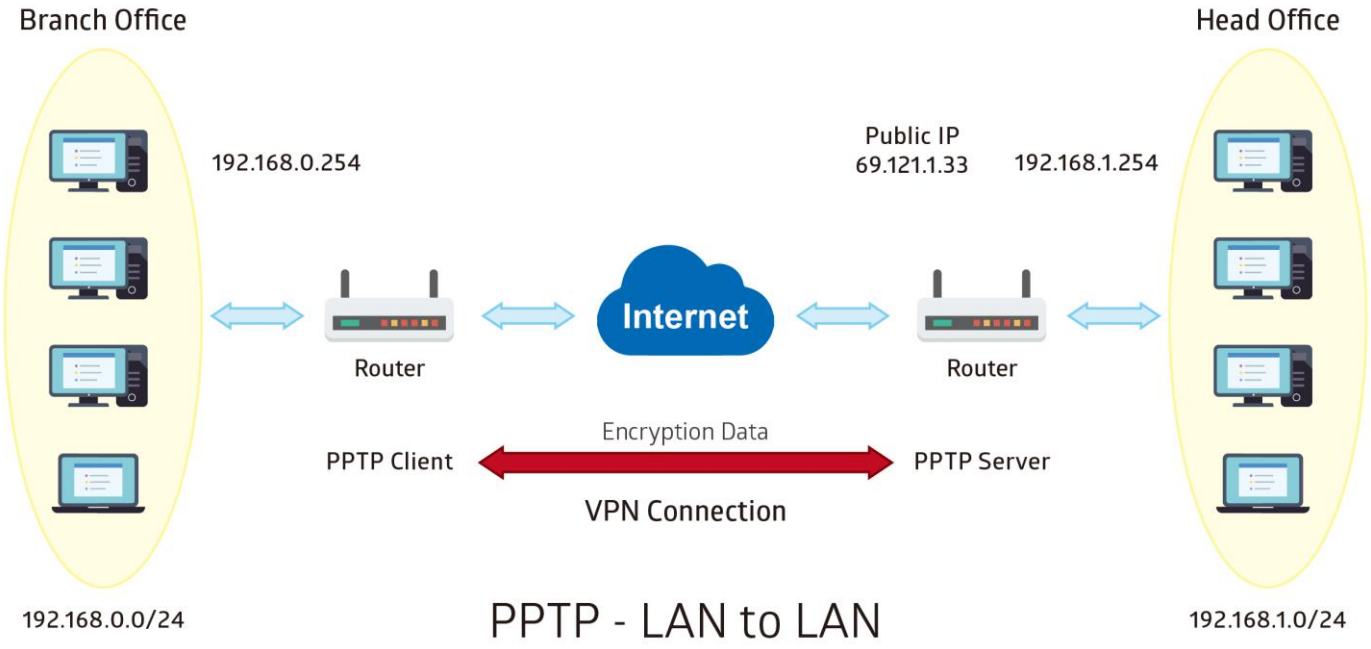
Active as Default Route: Check to select the tunnel as the default route for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

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

Example: PPTP LAN-to-LAN 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.

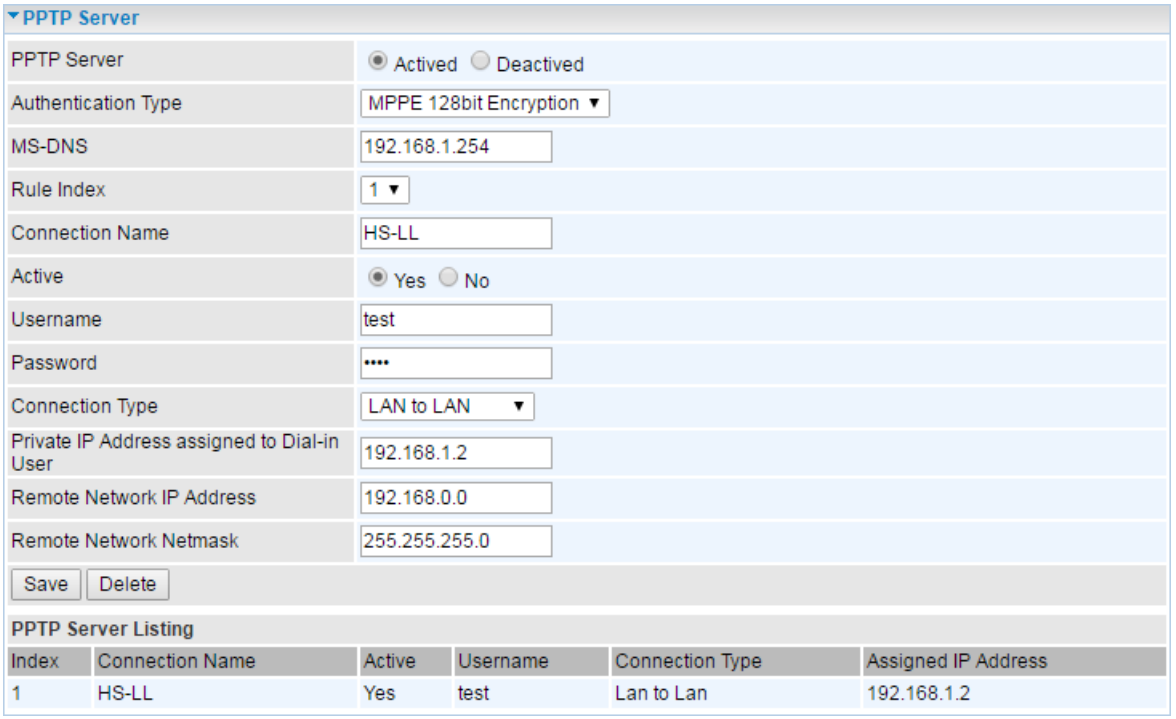
Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring PPTP server in the head office

The IP address 192.168.1.2 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.

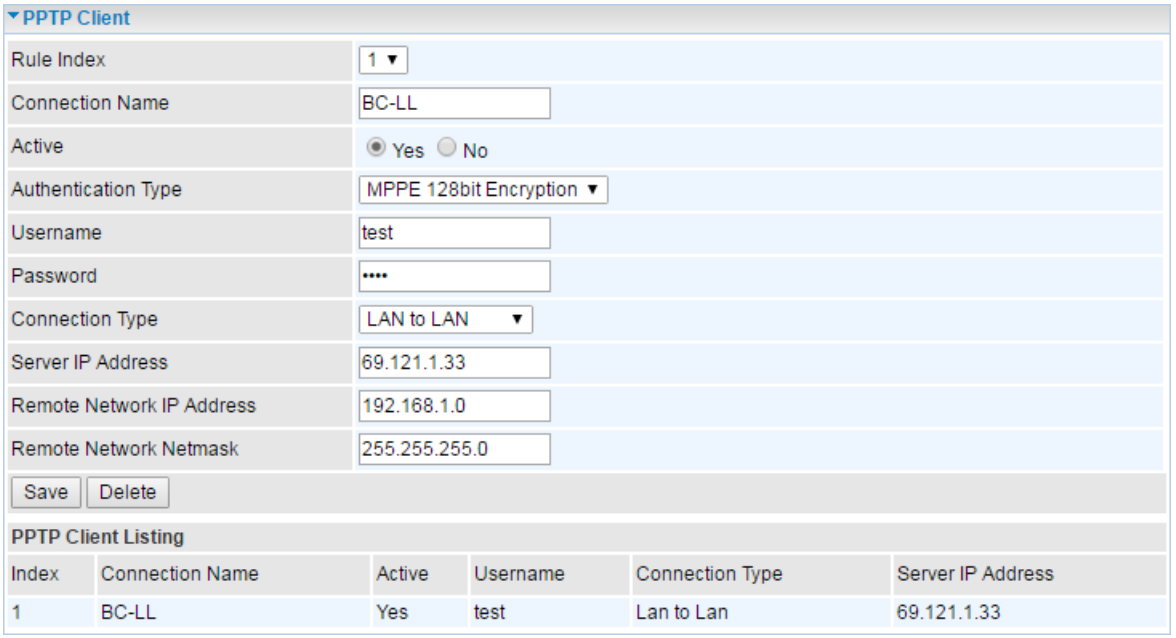
Item		Description
Connection Name	HS-LL	Give a name of PPTP conneciton
Authentication Type	MPPE 128bit	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Conneciton Type	LAN to LAN	LAN to LAN for dial in
Assigned IP	192.168.1.2	An IP assigned to the dial in client
Remote Network IP	129.168.0.0	Remote access network
Remote Network Netmask	255.255.255.0	



Configuring PPTP client in the branch office

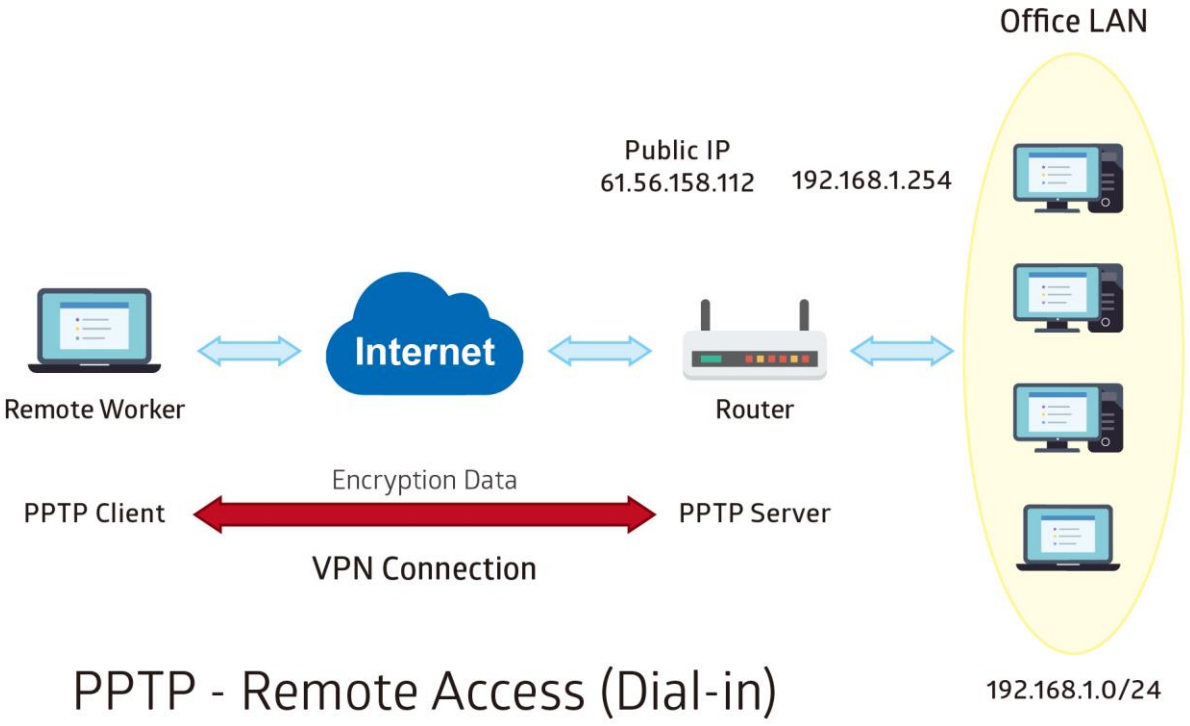
The IP address 69.121.1.33 is the public IP address of the router located in head office.

Item		Description
Connection Name	BC-LL	Give a name of PPTP conneciton
Authentication Type	MPPE 128bit	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Conneciton Type	LAN to LAN	LAN to LAN for dial in
Server IP	69.121.1.33	Dialed server IP
Remote Network IP	129.168.1.0	Remote access network
Remote Network Netmask	255.255.255.0	



Example: PPTP Remote Access Dial-in connection

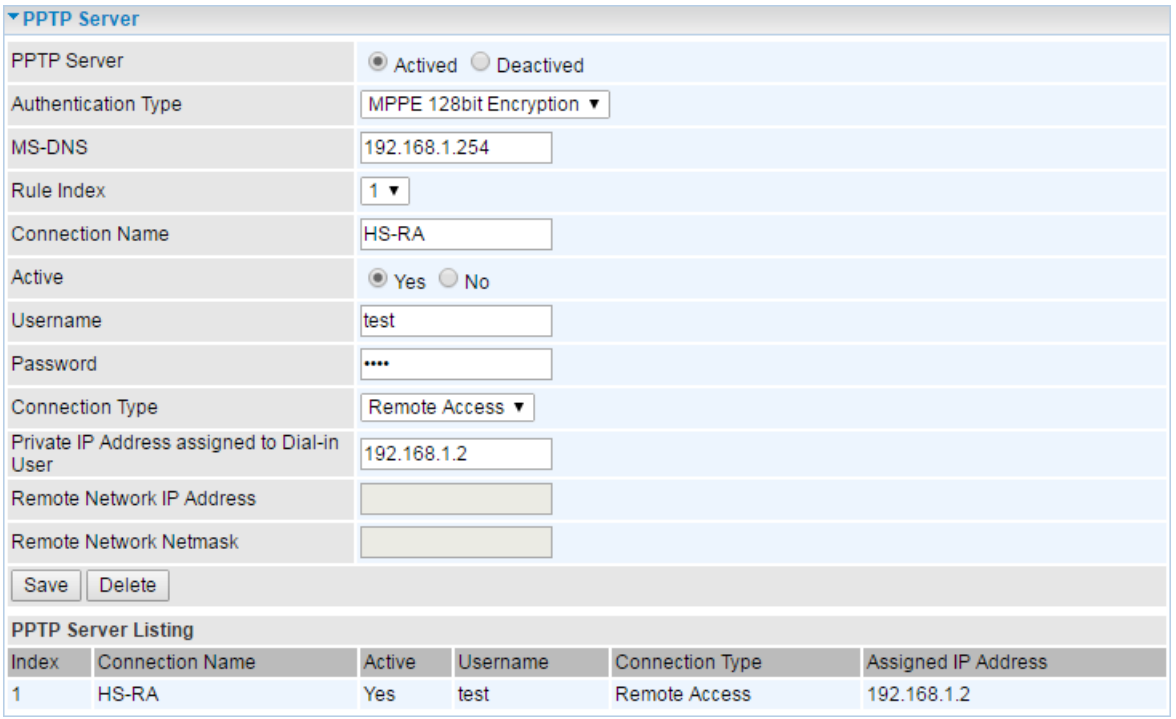
A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter. The router is installed in the head office, connected to a couple of PCs and Servers.



Configuring PPTP server(dial-in) in the office

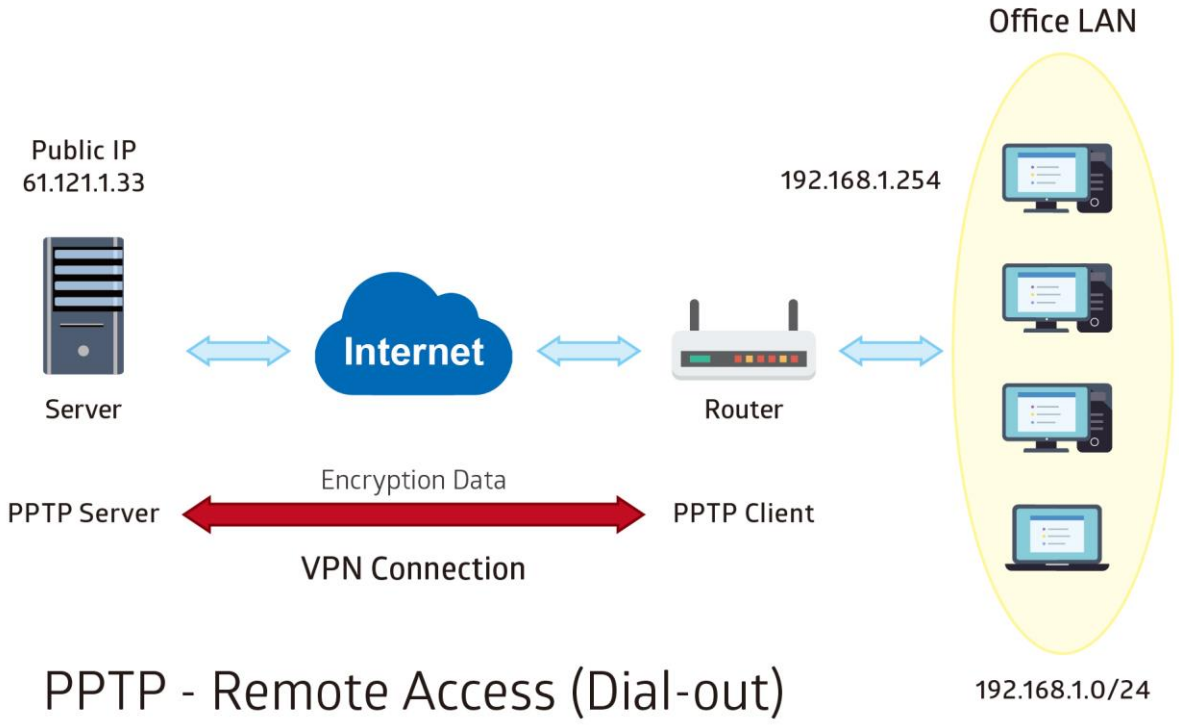
The input IP address 192.168.1.2 will be assigned to the remote worker. Please make sure this IP is not used in the office LAN.

Item		Description
Connection Name	HS-RA	Give a name of L2TP conneciton
Authentication Type	MPPE 128bit	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Conneciton Type	Remote Access	Remote access for dial in
Assigned IP	192.168.1.2	An IP assigned to the dial in client



Example: PPTP Remote Access Dial-out connection

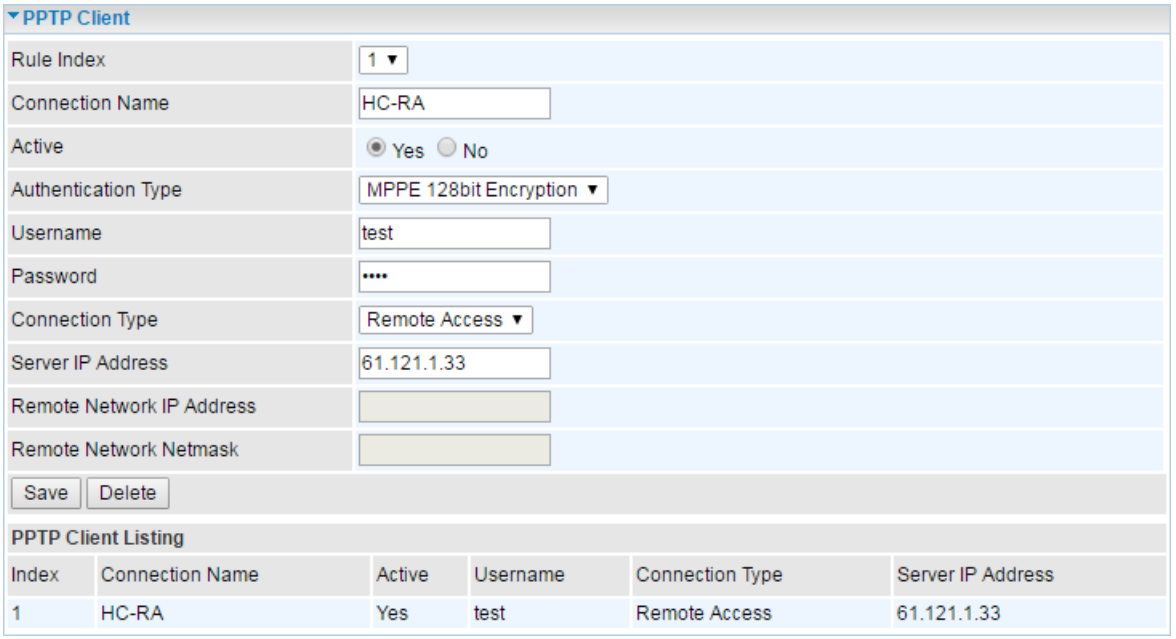
A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



Configuring PPTP client(dial-out) in the office

The IP address 61.121.1.33 is the public IP address of the router located in head office.

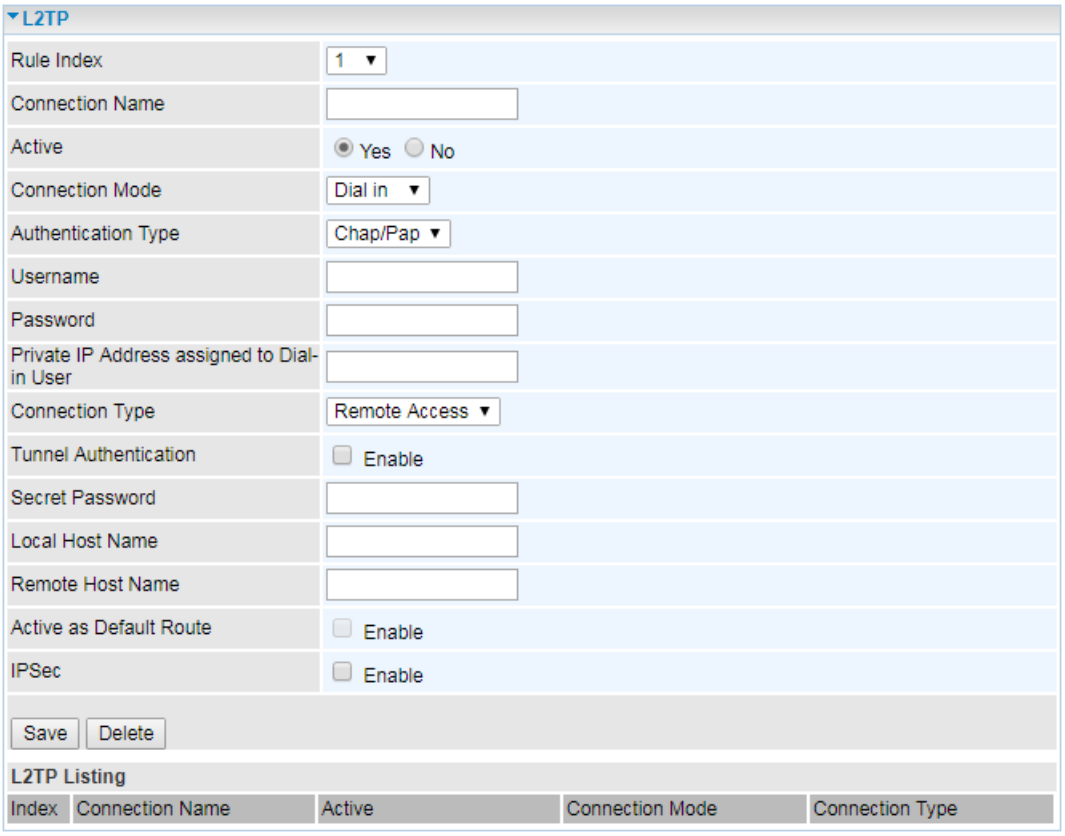
Item		Description
Connection Name	HC-RA	Give a name of PPTP conneciton
Authentication Type	MPPE 128bit	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Conneciton Type	Remote Access	Remote access for dial out
Server IP	61.121.1.33	Dialed server IP



L2TP

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: 8 sessions for dial-in connections and 8 sessions for dial-out connections

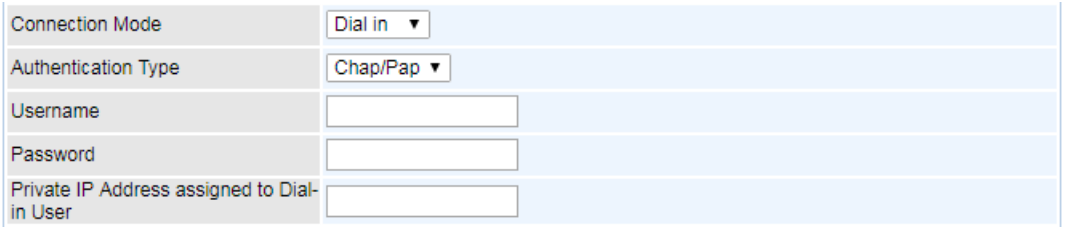


Rule Index: The Index to mark the session.

Connection Name: User-defined name for the connection.

Active: To enable or disable the tunnel.

Conneciton Mode:



Connection Mode: Select **Dial In** to operate as a L2TP server.

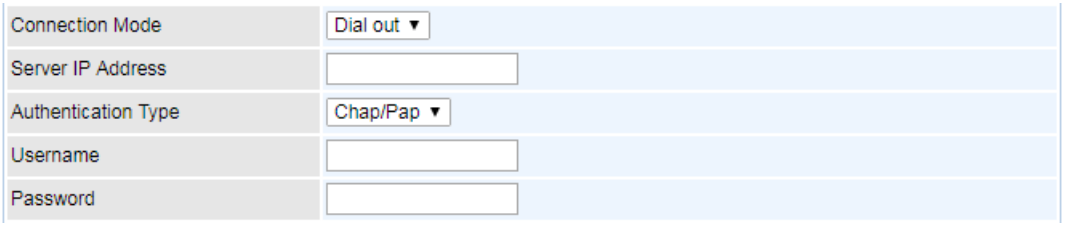
Authentication Type: Default is Chap/Pap(CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol.) if you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

Username: Please input the username for this account.

Password: Please input the password for this account.

Private IP Address Assigned to Dial-in 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.



Connection Mode: Choose **Dial Out** if you want your router to operate as a client (connecting to a remote L2TP Server, e.g, your office server).

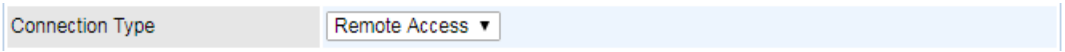
Server IP Address: Enter the IP address of your VPN Server.

Authentication Type: Default is Chap/Pap(CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol.) if you want the router to determine the authentication type to use, or else manually specify PAP 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).

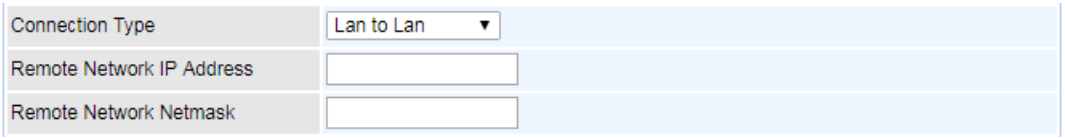
Username: Please input the username for this account.

Password: Please input the password for this account.

Conneciton Type:

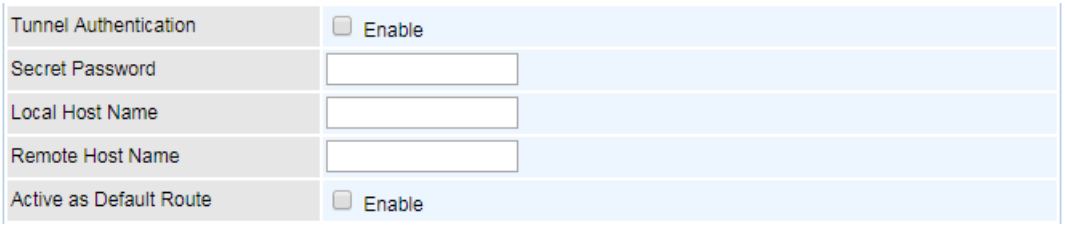


Connection Type: Remote Access for single user.



Connection Type: If **LAN to LAN** is selected, enter the peer network information, such as network address and netmask.

Tunel Authentication and Active as Default Router:



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

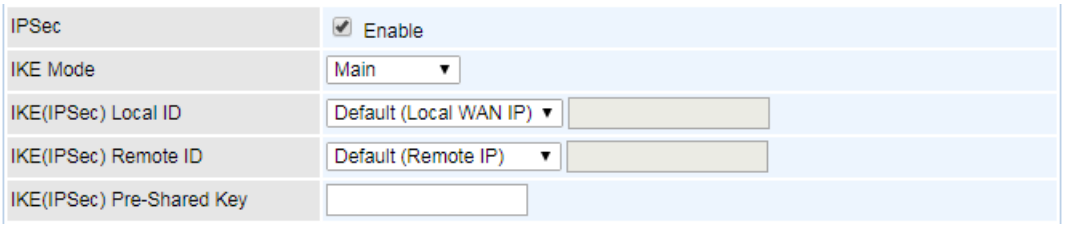
Secret Password: The secure password length should be 16 characters which may include numbers and characters.

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

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.

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.

L2TP over IPSec



IPSec: This enables L2TP tunnel over IPSec

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.

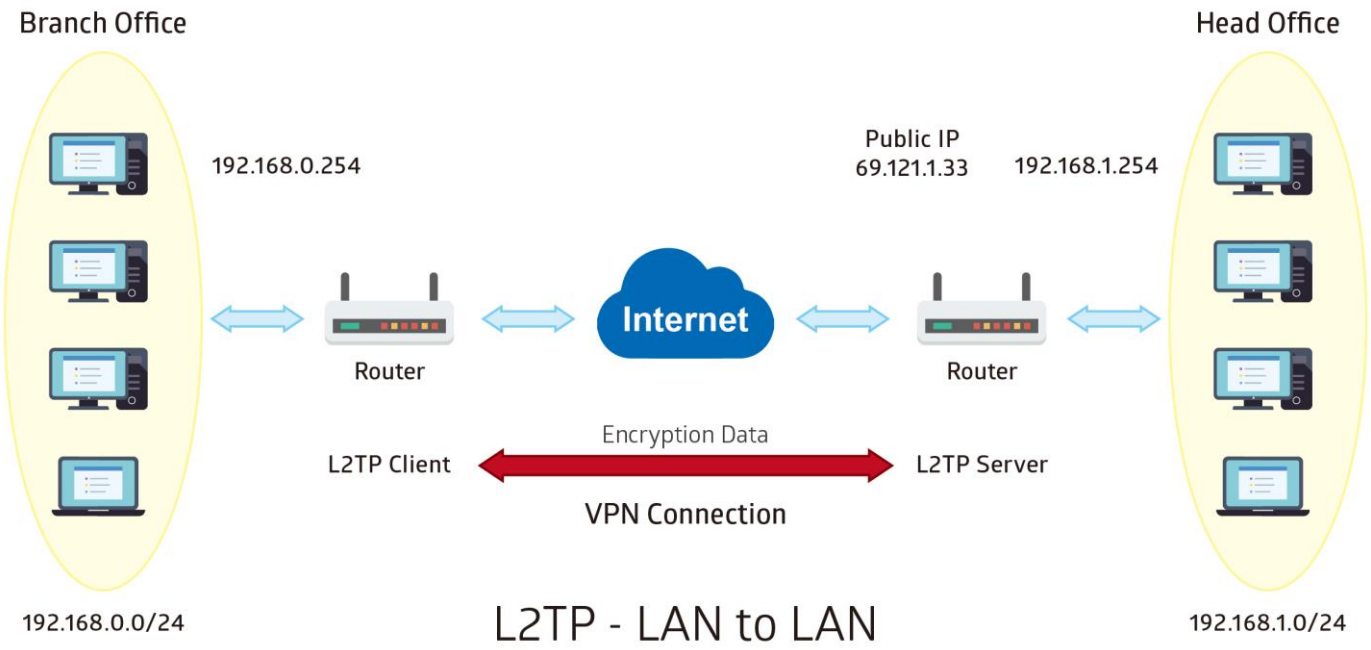
IKE Local ID Type and **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IKE 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).

Example: L2TP LAN-to-LAN 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.

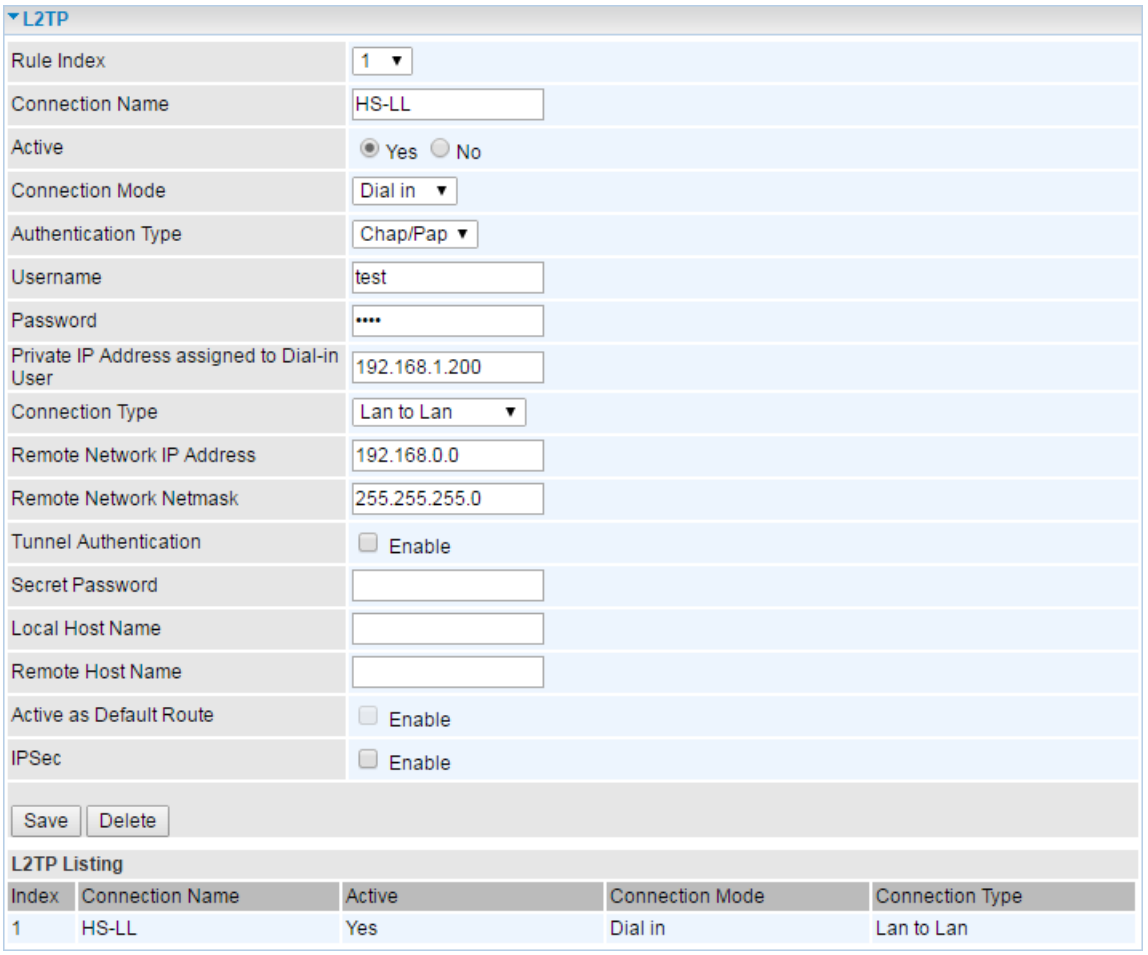
Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring L2TP Dial-in in the head office

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

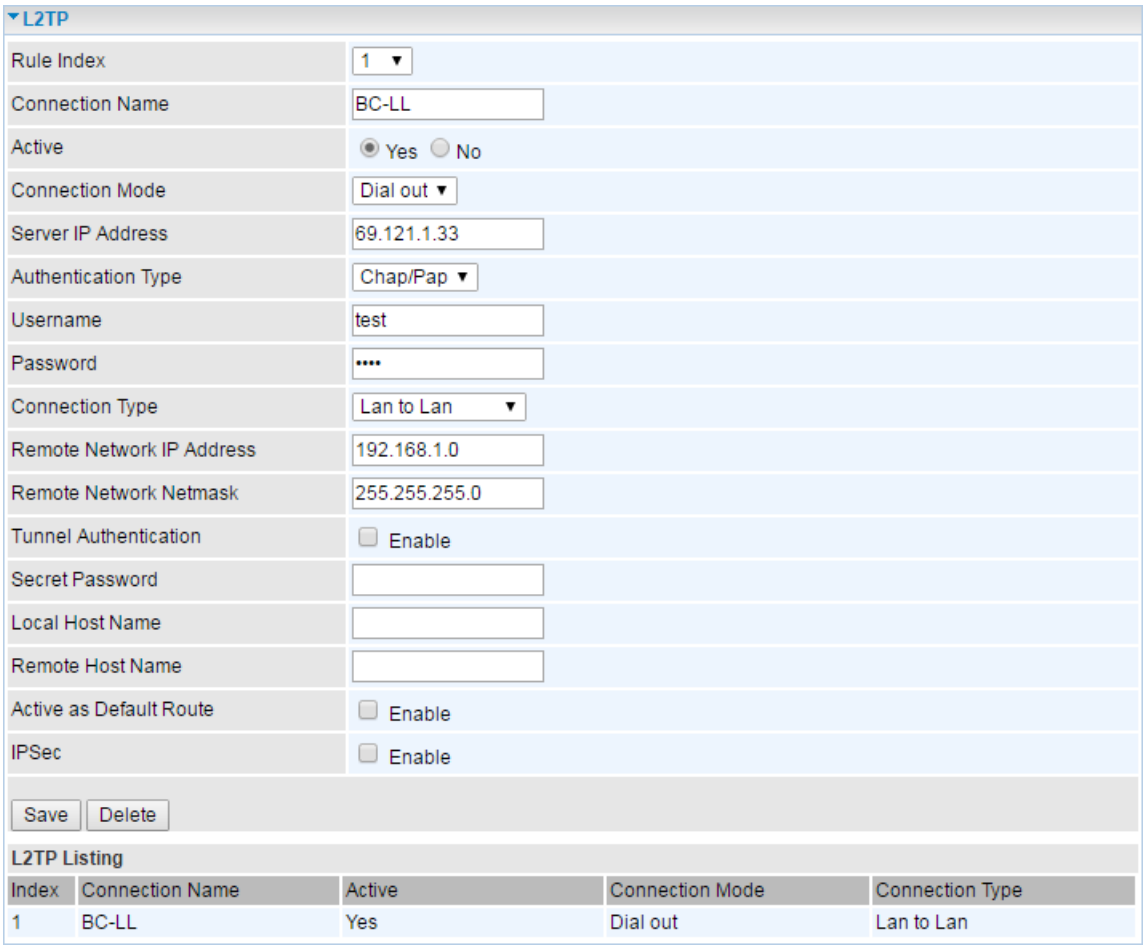
Item		Description
Connection Name	HS-LL	Give a name of L2TP conneciton
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	Test	Dial in authenticate user name
Passwrod	Test	Dial in authenticate user password
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Conneciton Type	LAN to LAN	LAN to LAN for dial in
Remote Network IP	129.168.0.0	Remote access network
Remote Network Netmask	255.255.255.0	



Configuring L2TP Dial-out in the branch office

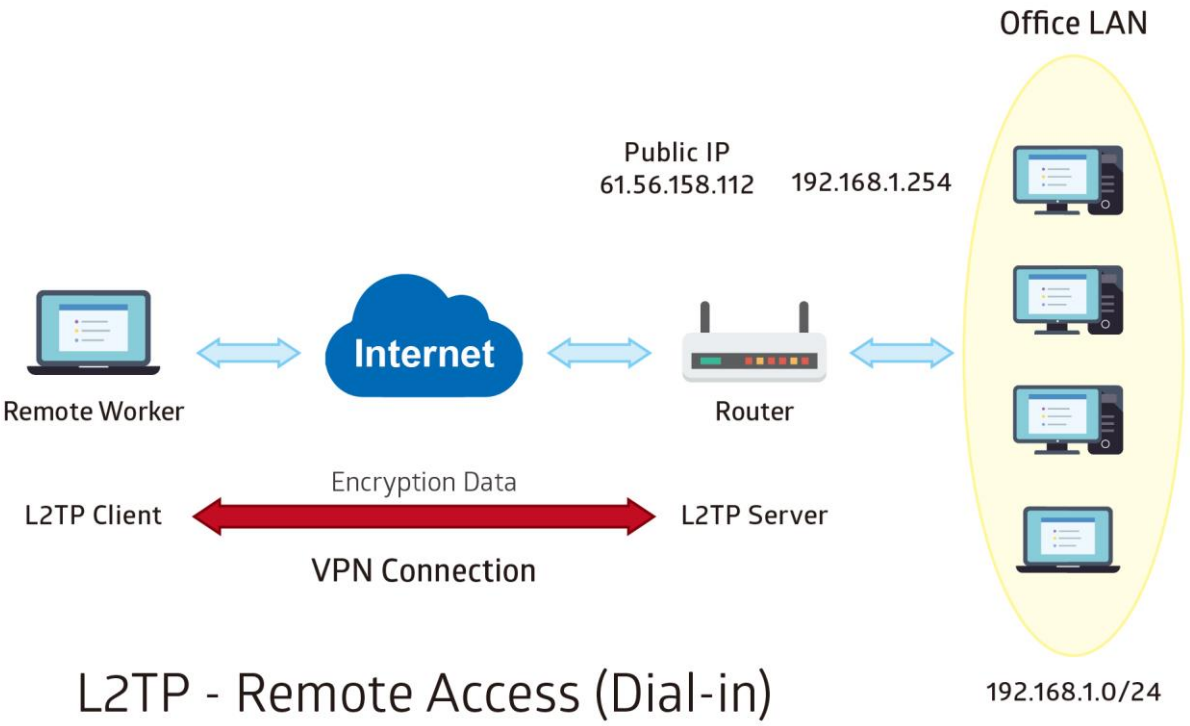
The IP address 69.1.121.33 is the Public IP address of the router located in head office.

Item		Description
Connection Name	BC-LL	Give a name of L2TP conneciton
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	Dialed server IP
Authentication Type	Chap/Pap	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Conneciton Type	LAN to LAN	LAN to LAN for dial out
Remote Network IP	129.168.1.0	Remote access network
Remote Network Netmask	255.255.255.0	



Example: L2TP Remote Access Dial-in connection

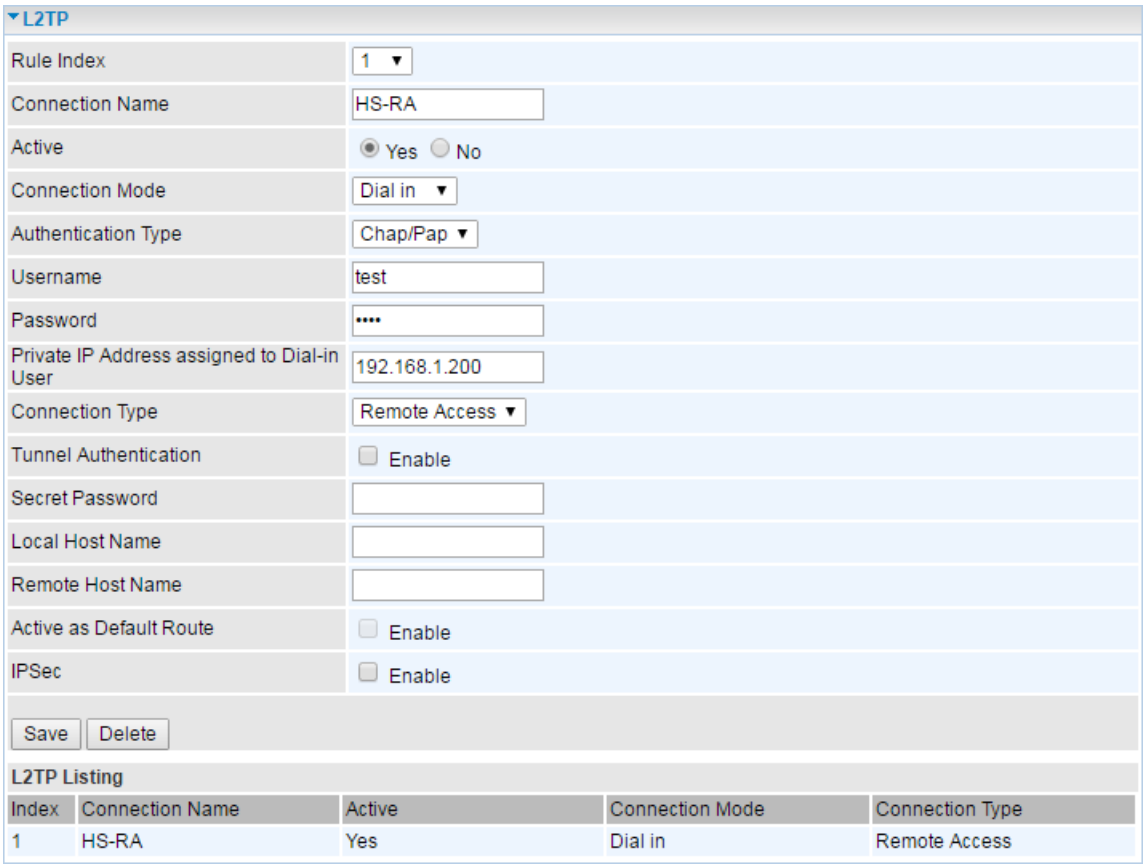
A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter. The router is installed in the head office, connected to a couple of PCs and Servers.



Configuring L2TP VPN Dial-in in the Office

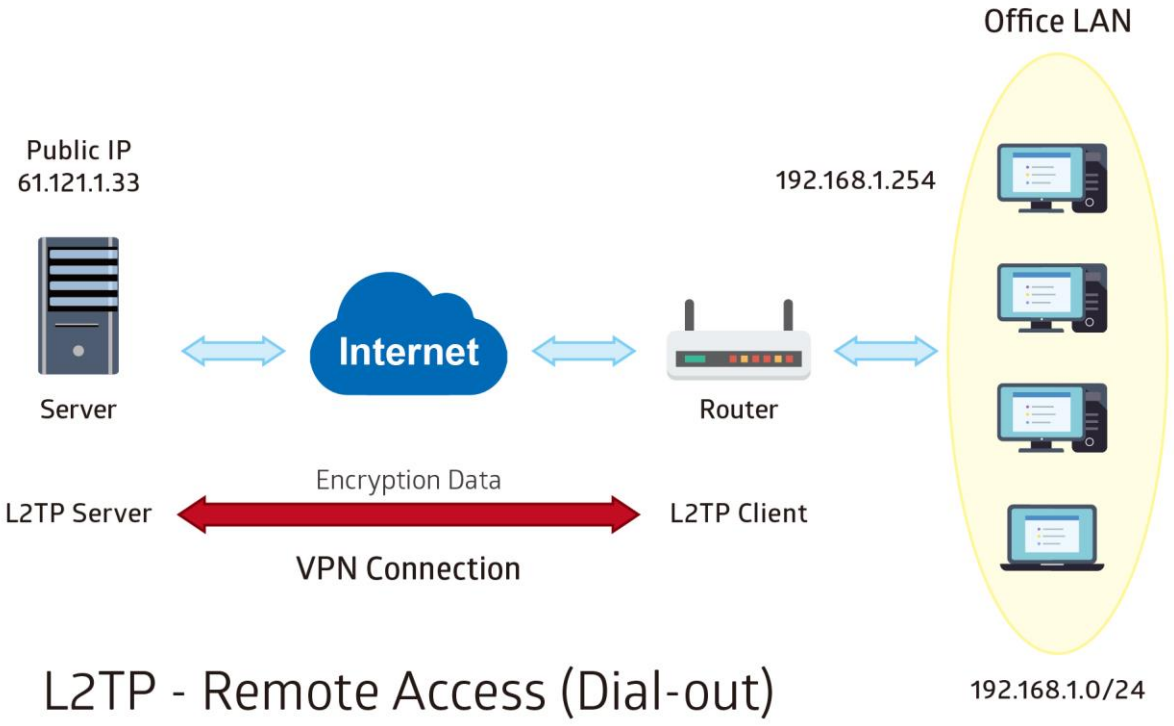
The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Item		Description
Connection Name	HS-RA	Give a name of L2TP conneciton
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	test	Dial in authenticate user name
Passwrod	test	Dial in authenticate user password
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Conneciton Type	Remote Access	Remote access for dial in



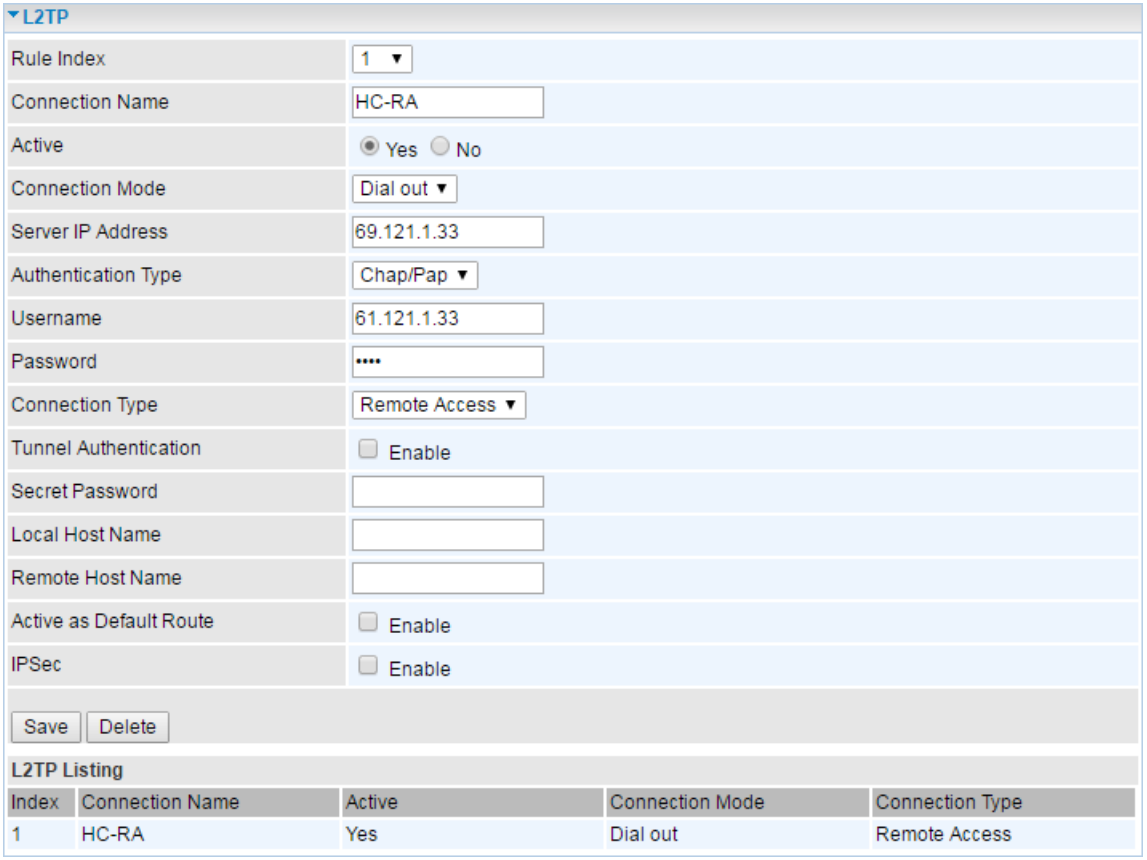
Example: L2TP Remote Access Dial-out connection

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 Dial-out in the office

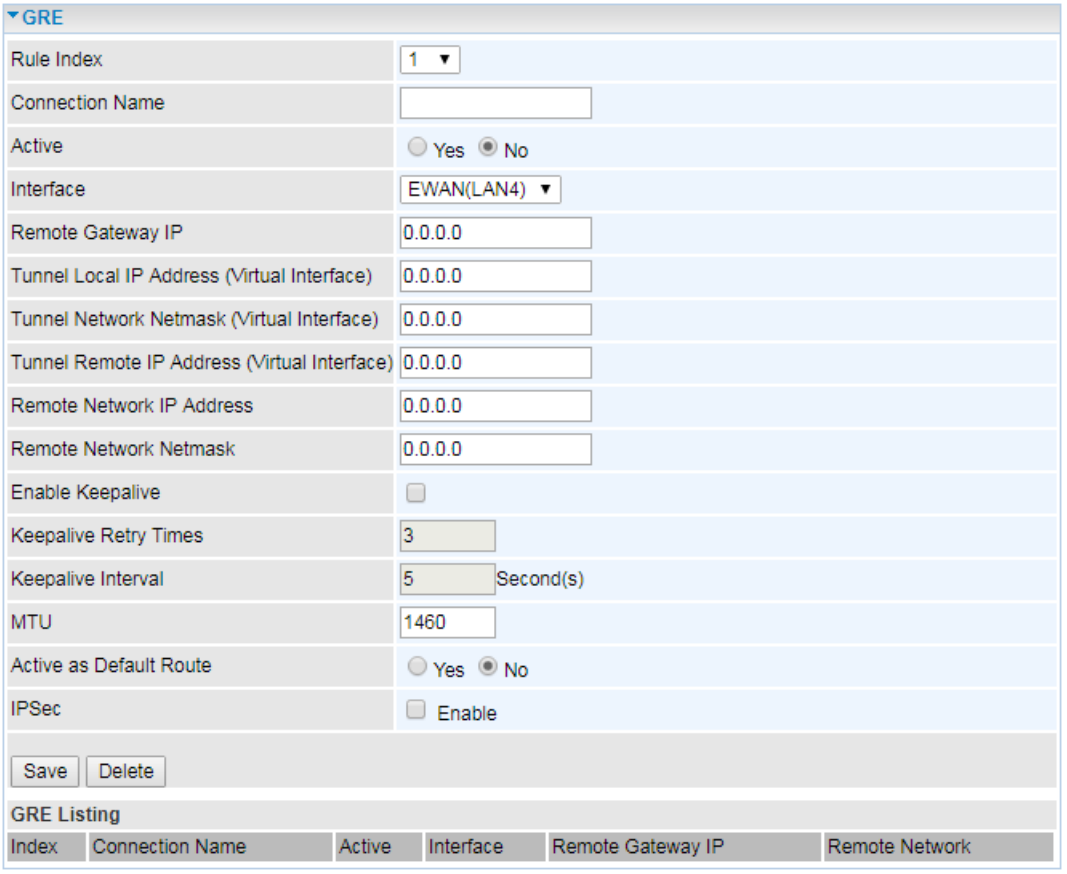
Item		Description
Connection Name	HC-RA	Give a name of L2TP conneciton
Connection Mode	Dial out	Operate as L2TP client
Server IP	61.121.1.33	Dialed server IP
Authentication Type	Chap/Pap	Authentication type
Username	test	Dial out authenticate user name
Passwrod	test	Dial out authenticate user password
Conneciton Type	Remote Access	Remote access for dial out



GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an IP network.

Note: up to 16 tunnels can be added.



Rule Index: The Index to mark the session.

Connection Name: User-defined name for the connection.

Active: Select Yes to activate the GRE tunnel.

Interface: Select the exact WAN interface configured for the tunnel as the local IP.

Remote Gateway: The remote GRE gateway IP.

Tunnel Local IP: Please set the source IP for the local tunnel. It is a virtual interface for the tunnel.

Tunnel Network Netmask: Please set the netmask for the local tunnel.

Tunnel Remote IP Address: Set the peer IP address of the tunnel. It is a virtual interface for the tunnel.

Remote Network IP Address: Please set the subnet IP for remote network.

Remote Network Netmask: Please set the Netmask for remote network.

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

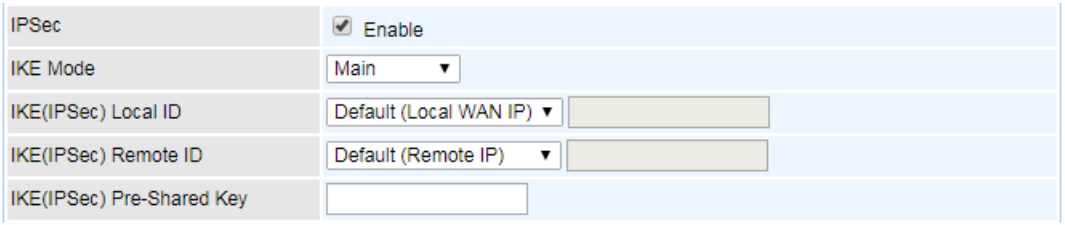
Keepalive Retry Times: Set the keepalive retry times, default is 3.

Keepalive Interval: Set the keepalive Interval, unit in seconds. Default is 5 seconds.

MTU: Maximum Transmission Unit.

Active as Default Route: Select if to set the GRE tunnel as the default route.

GRE over IPSec



IPSec: This enables GRE tunnel over IPSec

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.

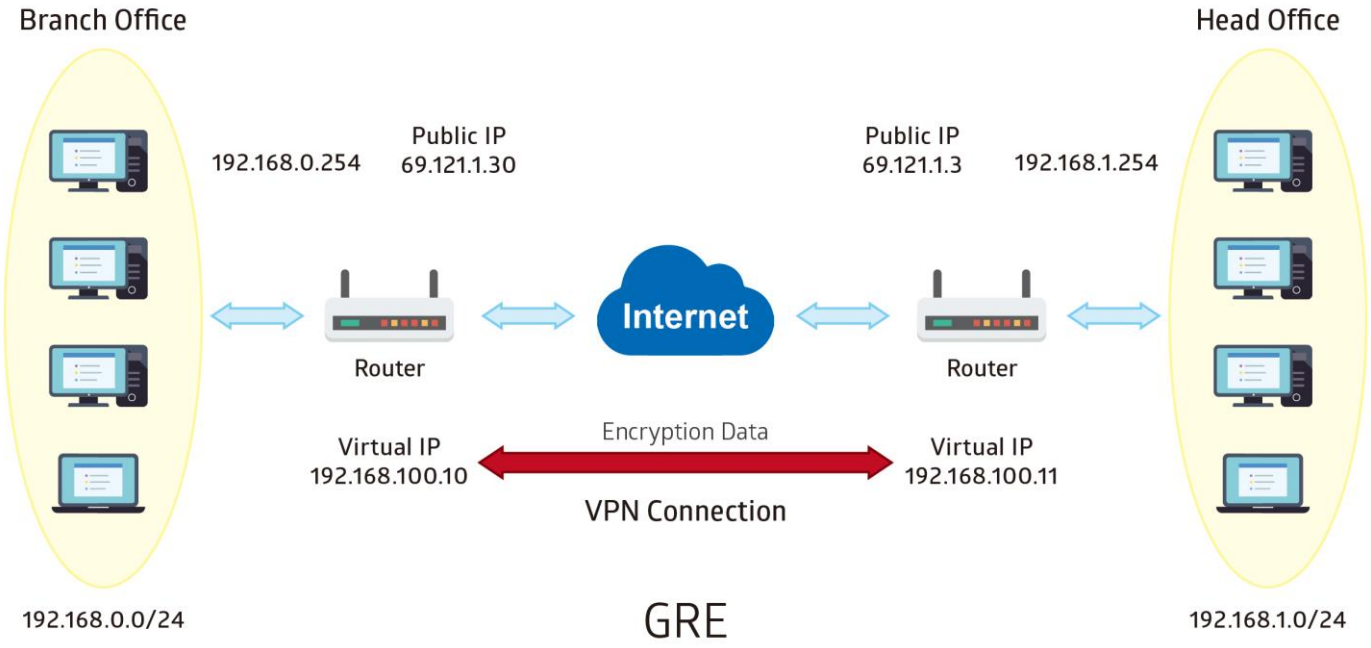
IKE Local ID Type and **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IKE 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).

Example: GRE VPN Connection

The branch office establishes a GRE 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.

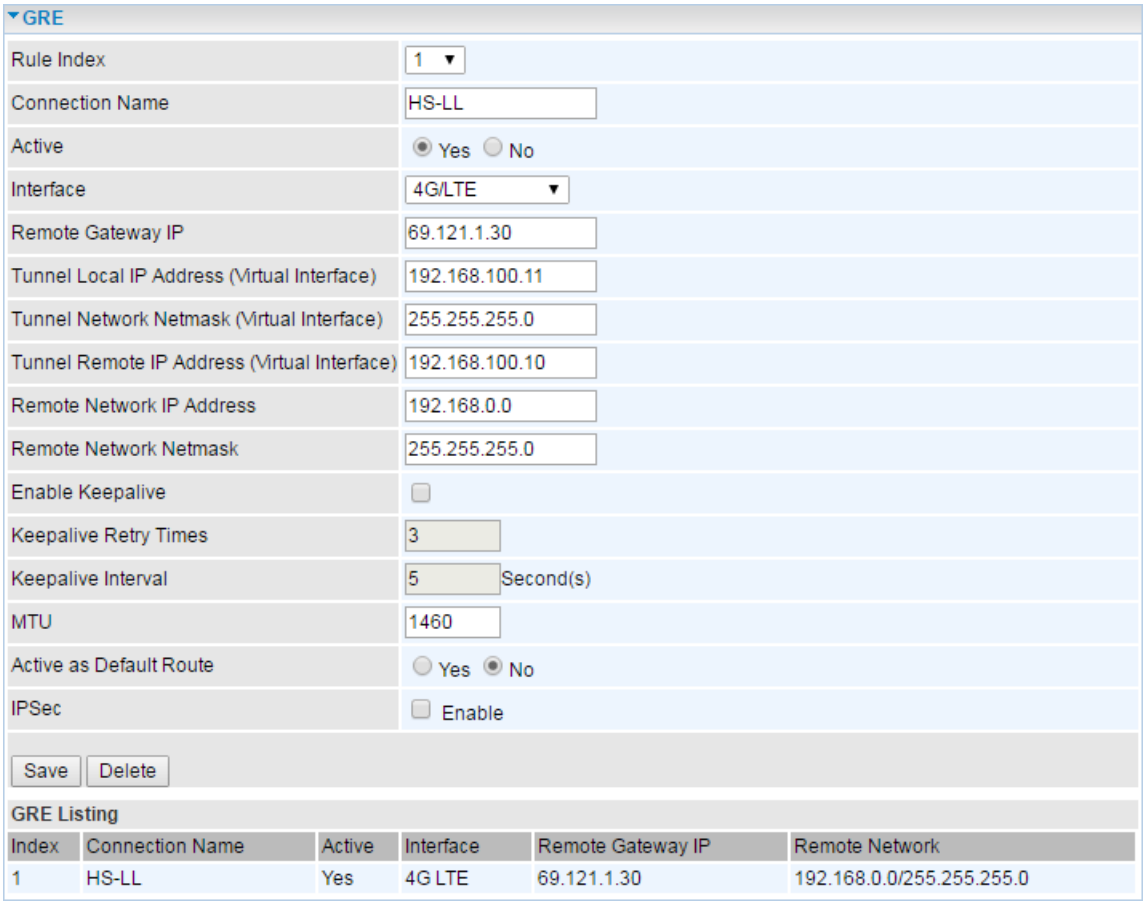
Note: Both office LAN networks must be in different subnets with the GRE VPN connection.



Configuring GRE connection in the head office

The IP address 69.1.121.30 is the Public IP address of the router located in branch office.

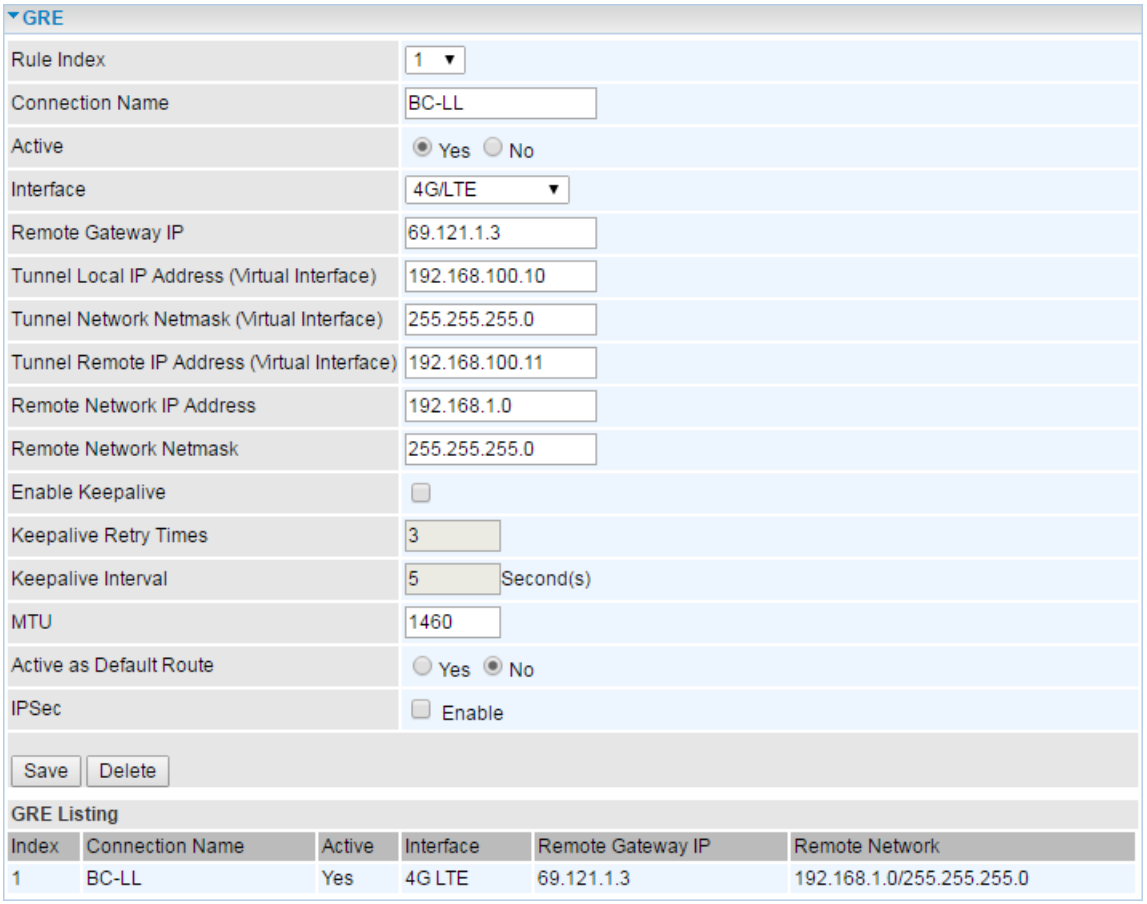
Item		Description
Connection Name	HS-LL	Give a name of GRE conneciton
Remote Gateway IP	69.121.1.30	Authentication type
Tunnel Local IP Address (Virtual Interface)	192.168.100.11	The local virtual interface IP address for the tunnel.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10	The remote virtual interface IP address for the tunnel.
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	The network netmask for tunnel virtual interface.
Remote Network IP/ Netmask	192.168.0.0/ 255.255.255.0	The remote network subnet.



Configuring GRE connection in the branch office

The IP address 69.1.121.3 is the Public IP address of the router located in head office.

Item		Description
Connection Name	BC-LL	Give a name of GRE conneciton
Remote Gateway IP	69.121.1.3	Authentication type
Tunnel Local IP Address (Virtual Interface)	192.168.100.10	The local virtual interface IP address for the tunnel.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11	The remote virtual interface IP address for the tunnel.
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	The network netmask for tunnel virtual interface.
Remote Network IP/ Netmask	192.168.1.0/ 255.255.255.0	The remote network subnet.



OpenVPN

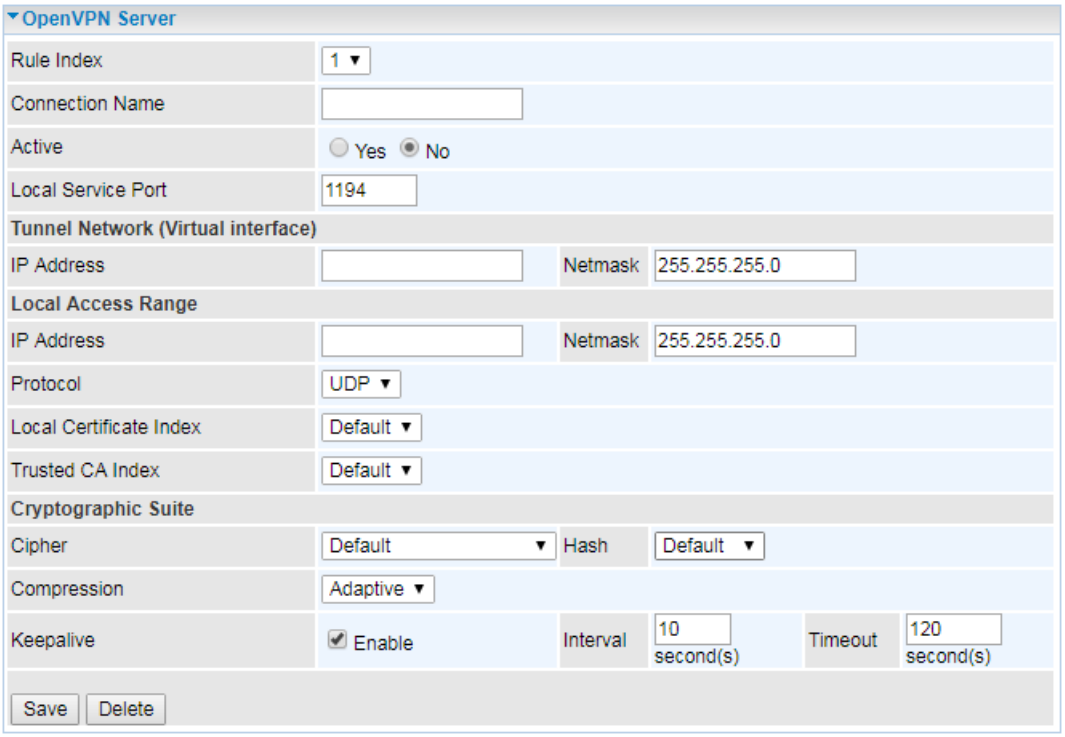
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. It is capable of traversing network address translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. Preshared secret key is the easiest, with certificate based being the most robust and feature-rich. It uses the OpenSSL encryption library extensively, allowing OpenVPN to use all the ciphers available in the OpenSSL package, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

It has integrated with OpenVPN package, allowing users to run OpenVPN in server or client mode from their network routers.

OpenVPN Server

Set the basic parameters for an OpenVPN server.



Rule Index: The index to identify the OpenVPN connection/rule.

Connection Name: user-defined name to mark the connection/rule.

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

Local Service Port: Port 1194 is the official assigned port number for OpenVPN

Tunnel Network (Virtual interface)

IP Address: Set the tunnel virtual subnet ID for OpenVPN server to assign IP address to tunnel interface, usually user-given, but different from the local and remote network(and not used in your Network Topology).

Netmask: Set the tunnel virtual subnet mask.

Local Access Range

IP Address: Set the local network address.

Netmask: Set the local subnet mask.

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

Local Certificate Index: Select the local certificate. Please Edit certificates in Maintenance >> Certificate Management. OpenVPN mutually authenticate each other based on certificates and CA. If not edited first, only Default(the embedded certificate) is listed.

Trusted CA Index: Select the trusted CA. Please Edit certificates in Maintenance >> Certificate Management.

Cryptographic Suite

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

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are 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.

Compression: Choose adaptive to use the LZO compression library to compress the data stream.

Keepalive: Enable to allow the router to check the connectivity to the peer every 10 seconds (can be changed based on need) by sending ping package to keep the OpenVPN tunnel active.

Interval: This period between Pings is set to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second.

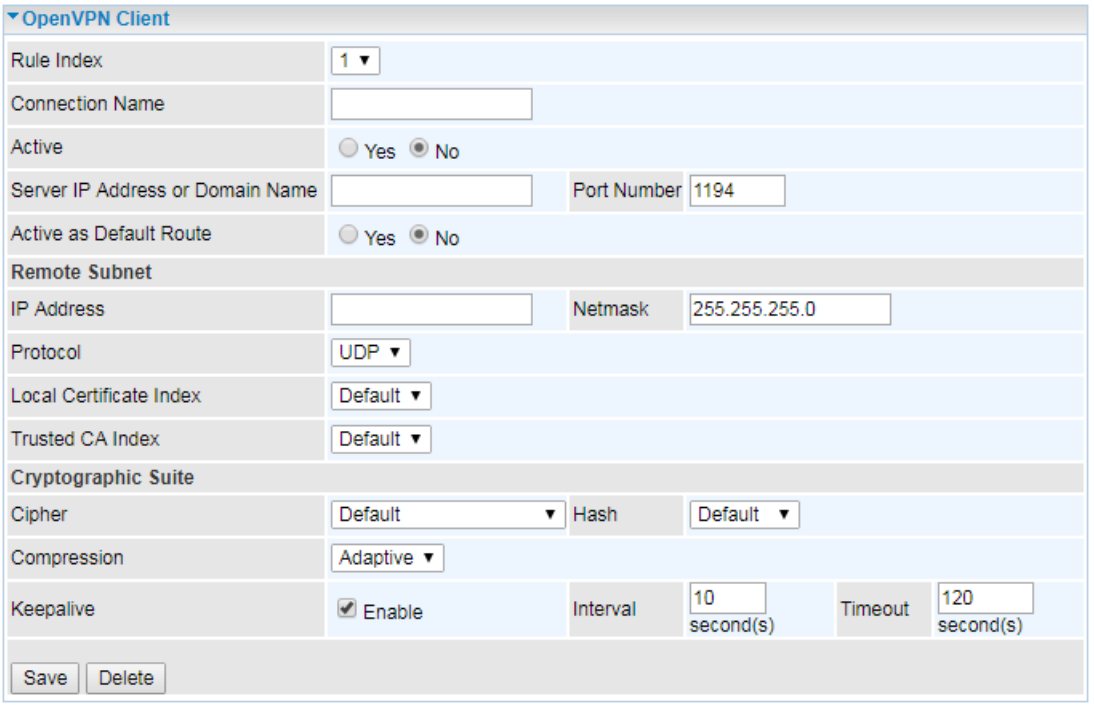
Timeout: Restart if receiving no response until the timeout period expires, by default, 120s.

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

OpenVPN Client

The settings of the OpenVPN client should match what's set on the server side.

Note: up to 4 tunnels can be added.



Rule Index: The index to identify the OpenVPN connection/rule.

Connection Name: user-defined name to mark the connection/rule.

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

Server IP Address or Domain Name: Enter the WAN IP address or Domain name of the OpenVPN server.

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

Active as Default Route: Choose **Yes** to let the OpenVPN tunnel/connection be the default route for traffic, under this circumstance, all outgoing packets will be forwarded to this tunnel and routed to the next hop.

Remote Subnet

IP Address: Set the network address of the remote peer.

Netmask: Set the subnet mask of the remote peer.

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

Local Certificate Index: Select the local certificate. Please Edit certificates in Maintenance >> Certificate Management. OpenVPN mutually authenticate each other based on certificates and CA. If not edited, only Default(the embedded certificate) is listed.

Trusted CA Index: Select the local CA. Please Edit certificates in Maintenance >> Certificate Management. If not edited, only Default(the embedded CA) is listed

Cryptographic Suite

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

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are 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.

Keepalive: Enable to allow the router to check the connectivity to the peer every 10 seconds (can be changed based on need) by sending ping package to keep the OpenVPN tunnel active.

Interval: This period between Pings is set to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second.

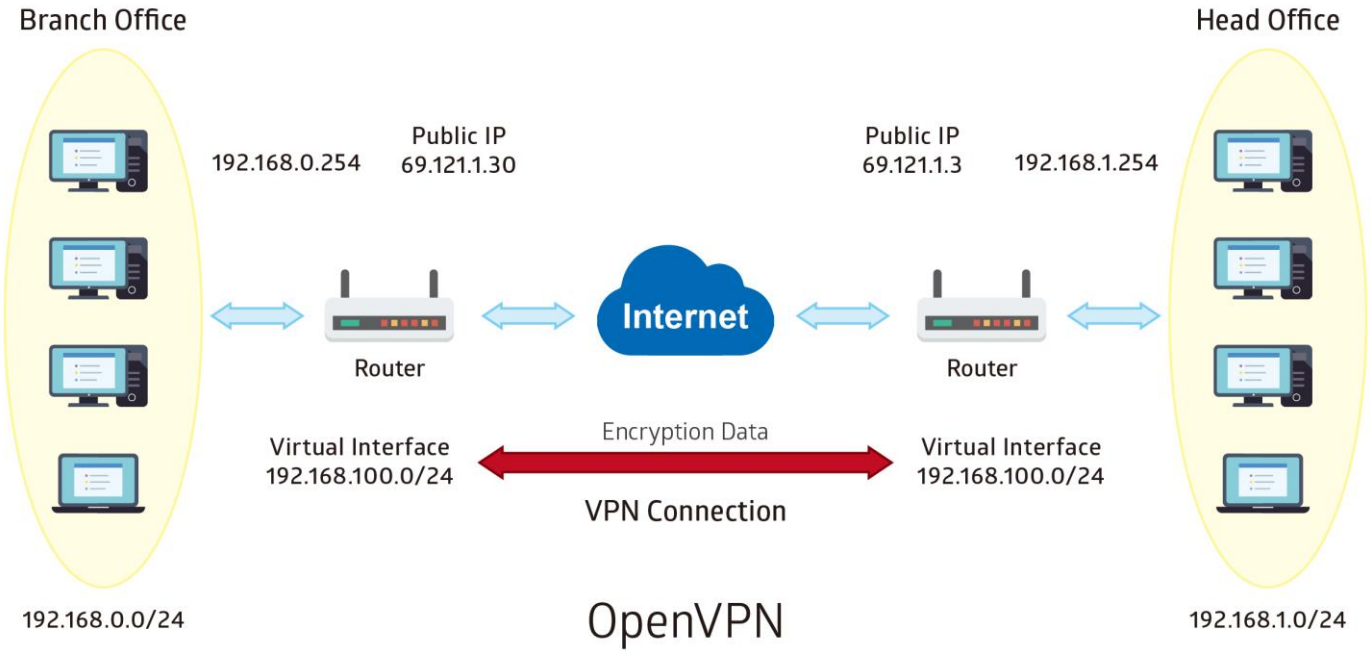
Timeout: Restart if receiving no response until the timeout period expires, by default, 120s.

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

Example: OpenVPN VPN Connection

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

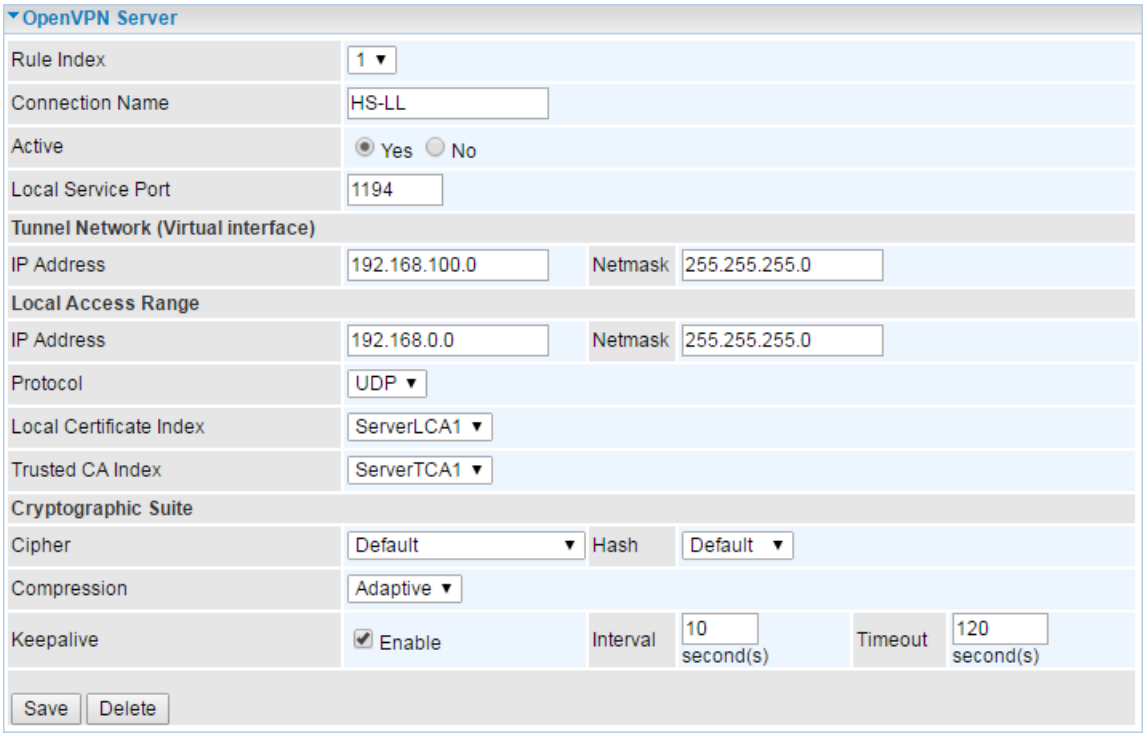
Note: Both office LAN networks must be in different subnets with the OpenVPN connection.



Configuring OpenVPN server in the head office

The IP address 69.1.121.30 is the Public IP address of the router located in branch office. The OpenVPN tunnel netwrok virtual interface is 192.168.100.0/24.

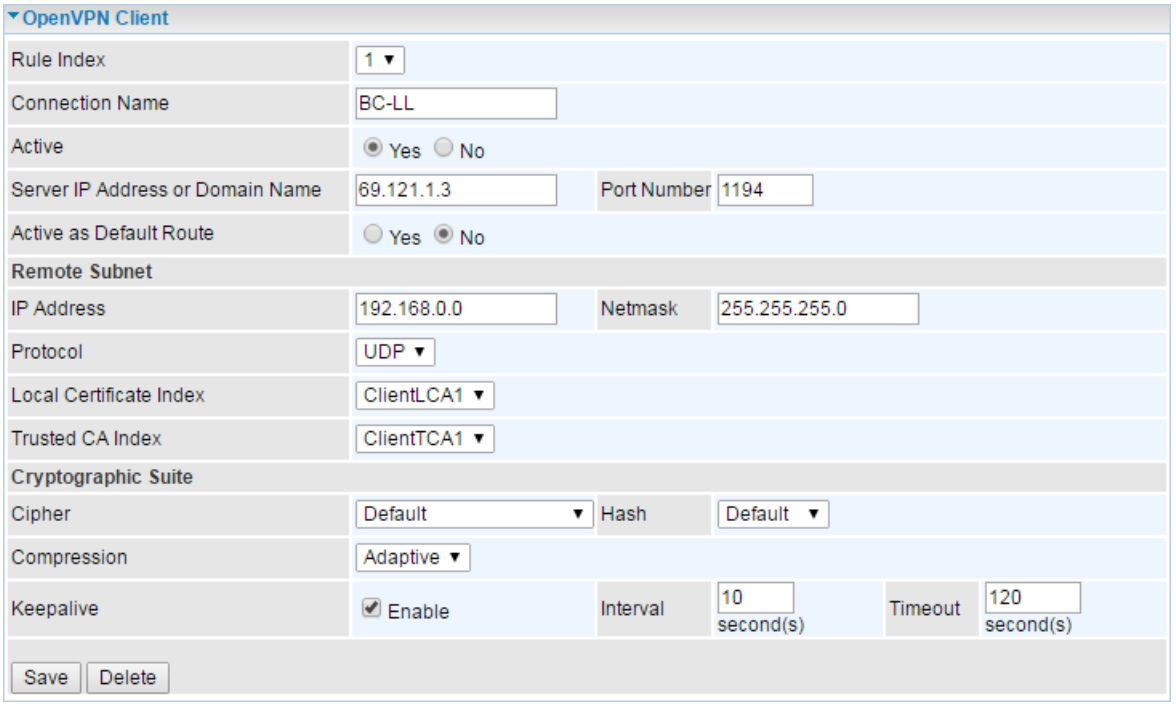
Item		Description
Connection Name	HS-LL	Give a name of GRE conneciton
Tunnel Network (Virtual Interface)	192.168.100.0/ 255.255.255.0	The network for tunnel virtual interface.
Local Access Range	192.168.0.0/ 255.255.255.0	The local network.



Configuring OpenVPN client in the branch office

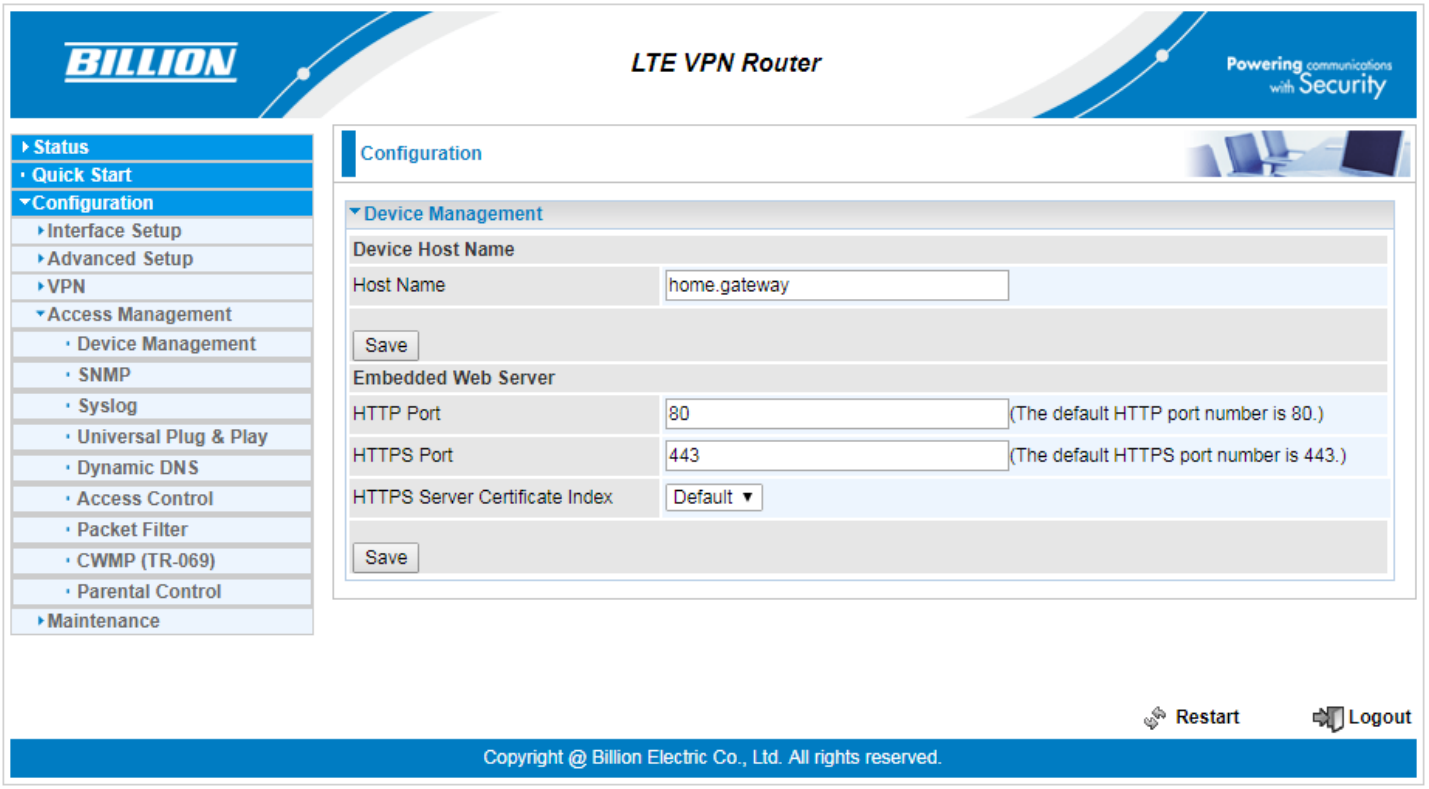
The IP address 69.1.121.3 is the Public IP address of the router located in head office.

Item		Description
Connection Name	BC-LL	Give a name of GRE conneciton
Server IP Address	69.121.1.3	The IP address of OpenVPN server.
Remote Subnet	192.168.0.0/ 255.255.255.0	The remote network.

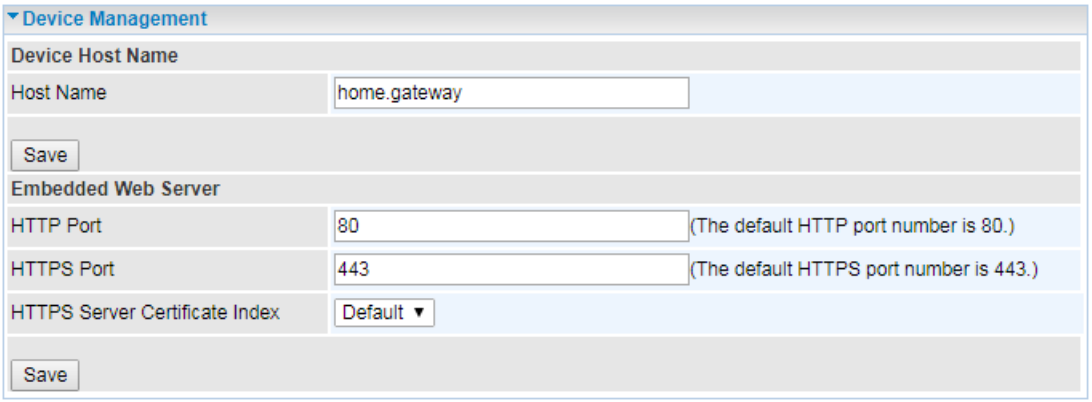


Access Management

Access Management equipments the users with the ability of maintaining the access management, including **Device Management**, **SNMP**, **Remote Syslog, Universal Plug & Play**, **Dynamic DNS**, **Access Control**, **Packet Filter**, **CWMP(TR-069)** and **Parental Control.**



Device Management



Device Host Name:

Host Name: Set the hostname for the device.

Embedded Web Server:

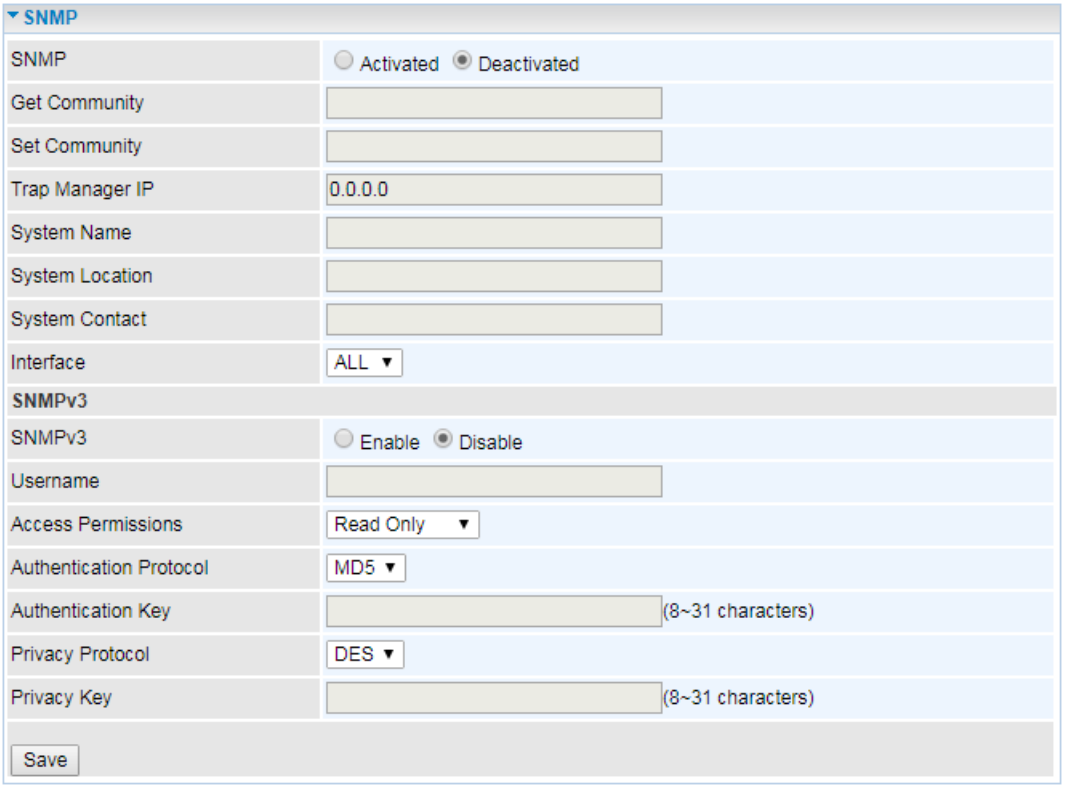
HTTP Port: The HTTP Port number, change if needed.

HTTPS Port: The HTTPS Port number, change if needed.

HTTPS Server Certificate Index: Choose the server security certificate. Users need to upload the certificate for the https server. See Certificate Management. Using the Default certificate, when being accessed, a page comes up warning of the insecure connection. You decide if to go ahead.

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. M100 serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.



SNMP: Select to enable SNMP feature.

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

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

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

SNMPv3: Enable to activate the SNMPv3.

Username: 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.

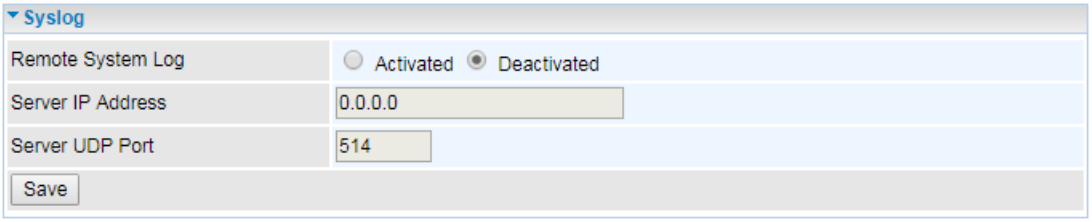
Authentication Key: Set the authentication key, 8-31 characters.

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

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

Remote Syslog

Remote System Log is designed to keep remote administrators informed of the system-operating information. Administrator can set up a remote system log server for receiving and monitoring the system information by enabling remote system log feature on the router.



Remote System Log: Select whether to activate **Remote System Log**.

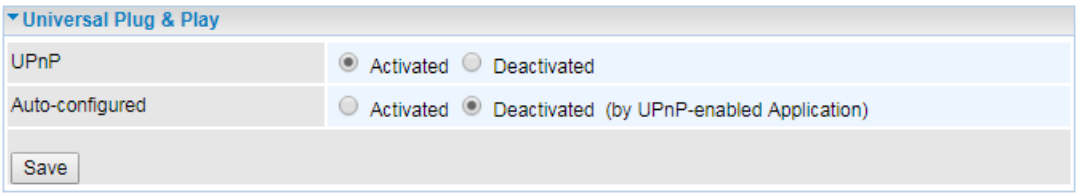
Server IP Address: Enter the remote syslog server IP address.

Server UDP Port: Enter the UDP port of the remote syslog server.

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.



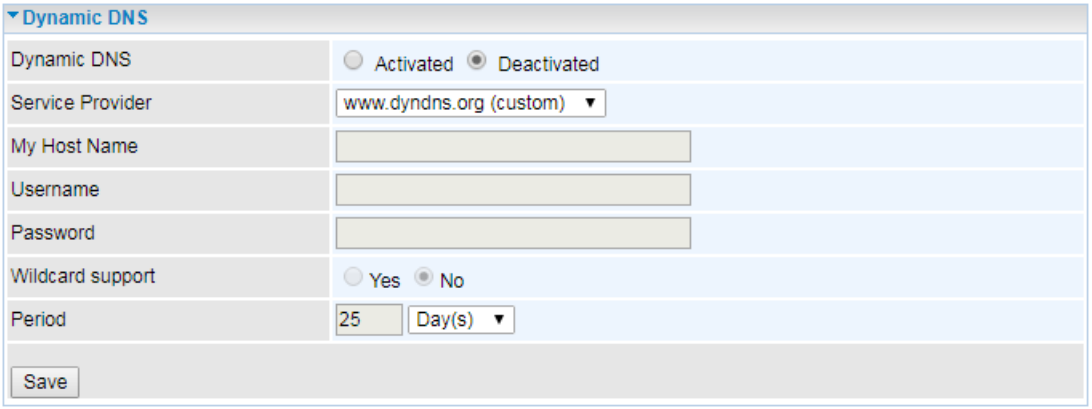
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the M100 IP address.

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the M100 so that they can communicate through the gateway, 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.

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.



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 router by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

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

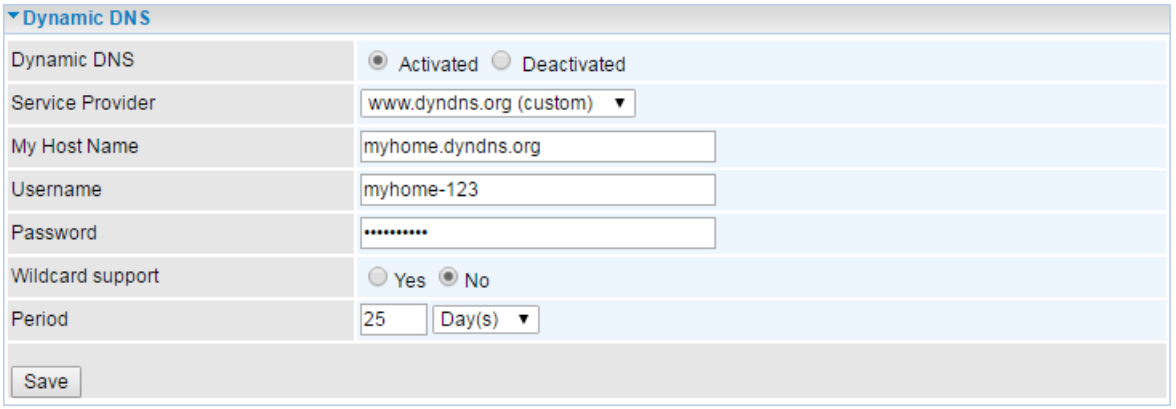
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Example: How to register a DDNS account

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/ .

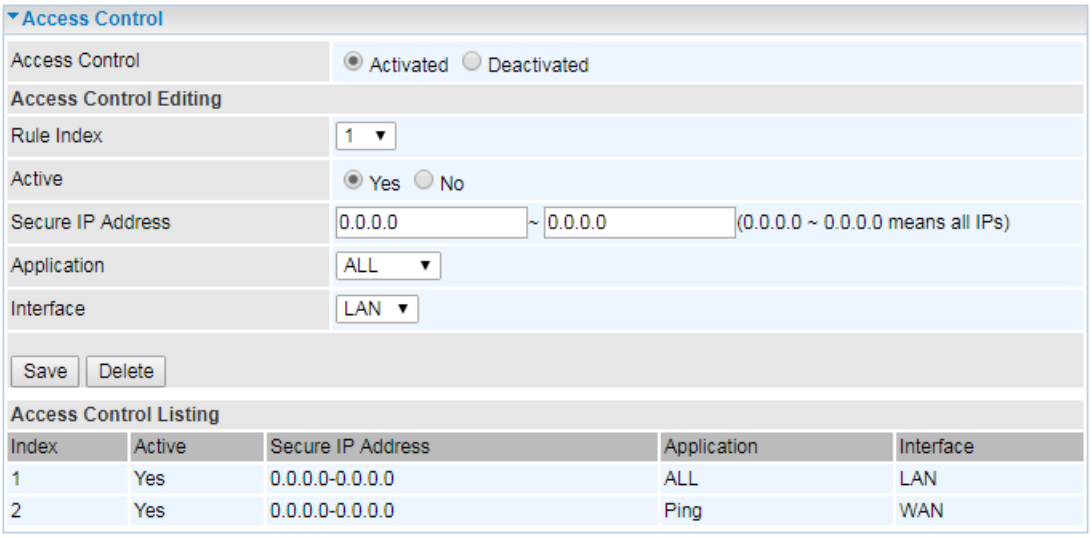
DDNS: www.hometest.com using username/password test/test



Access Control

Access Control Listing allows you to determine which services/protocols can access M100 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**.



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

Rule Index: This is item number

Active: Select to activate the rule.

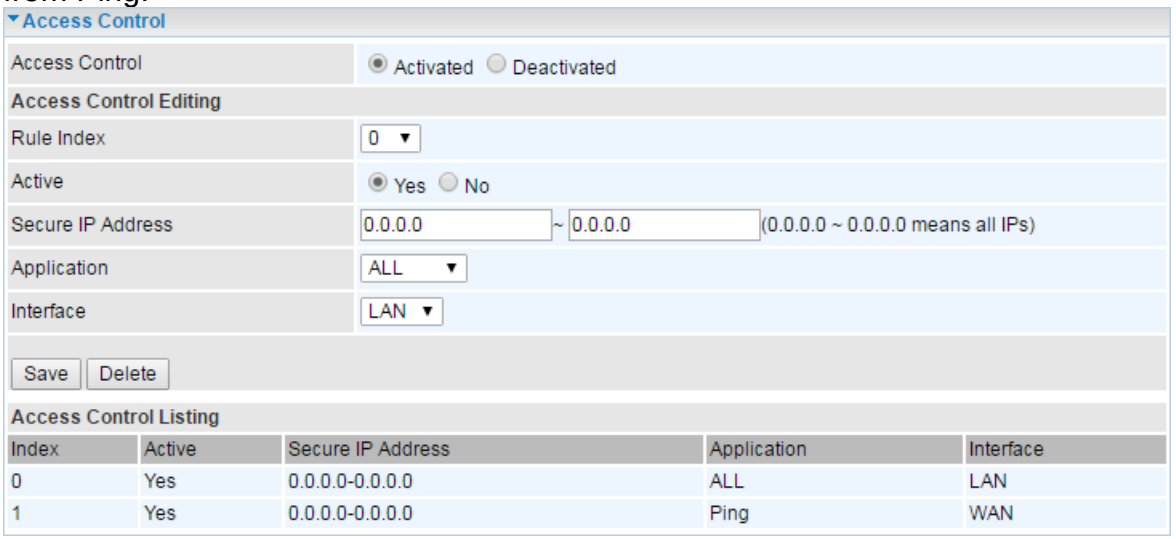
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the gateway. Type an IP address range to restrict access to the client(s) without a matching IP address.

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**.

Default Rule 1: (Index 0), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN cannot access the router even from Ping.



Access Control

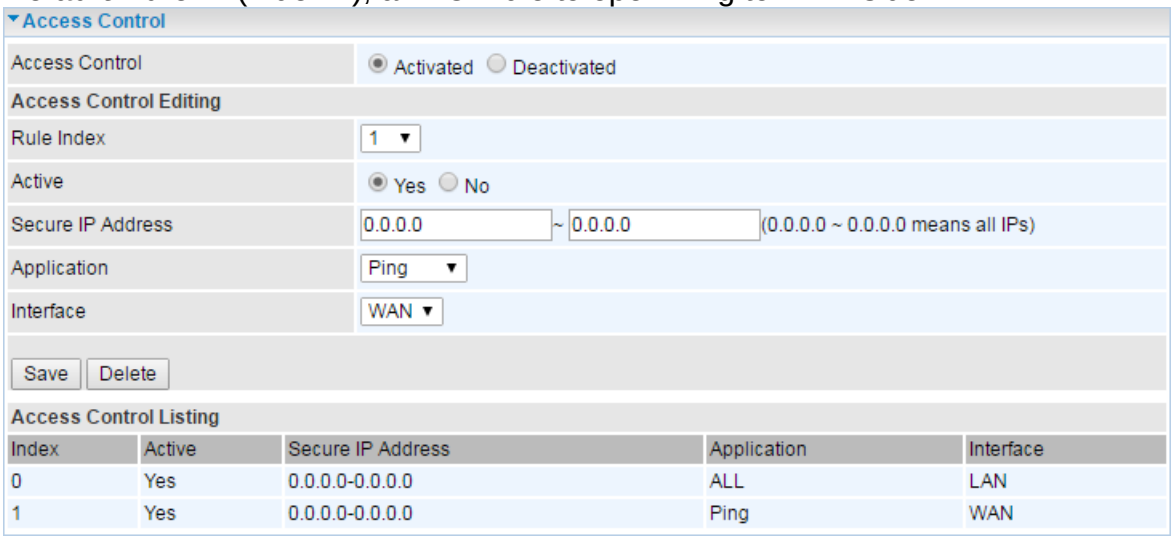
Access Control	Activated / Deactivated
Access Control Editing	
Rule Index	0
Active	Yes / No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL
Interface	LAN

Save Delete

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
0	Yes	0.0.0.0-0.0.0.0	ALL	LAN
1	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Default Rule 2: (Index 1), an ACL rule to open Ping to WAN side.



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	Ping
Interface	WAN

Save Delete

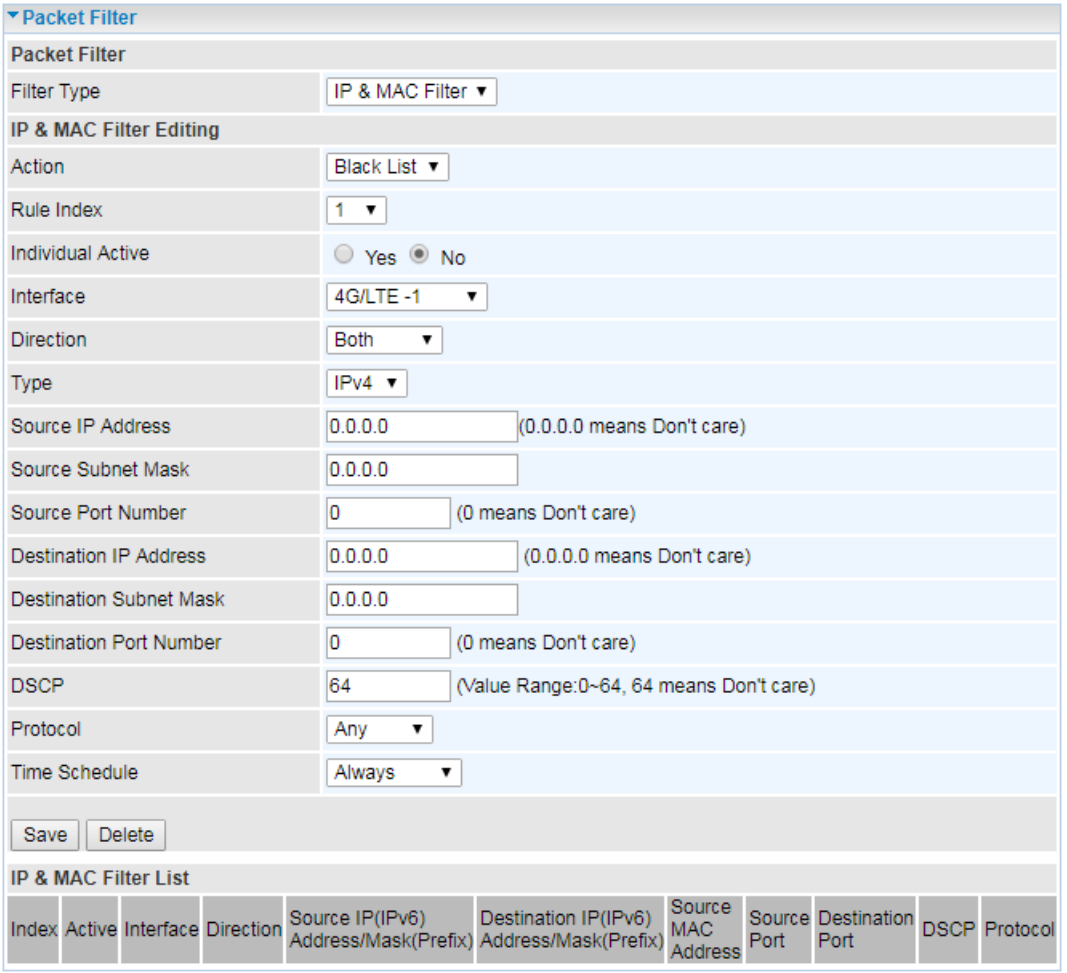
Access Control Listing

Index	Active	Secure IP Address	Application	Interface
0	Yes	0.0.0.0-0.0.0.0	ALL	LAN
1	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Packet Filter

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

❖ Packet Filter - IP & MAC Filter



Packet Filter

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

IP & MAC Filter Editing

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

Rule Index: This is item number

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

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 is 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, and ICMPv6) that the rule applies to.

Time Schedule: To determine when the rule takes effect. The rule works always or winthin the set timeslot.

IP/MAC Filter List

Index: 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.

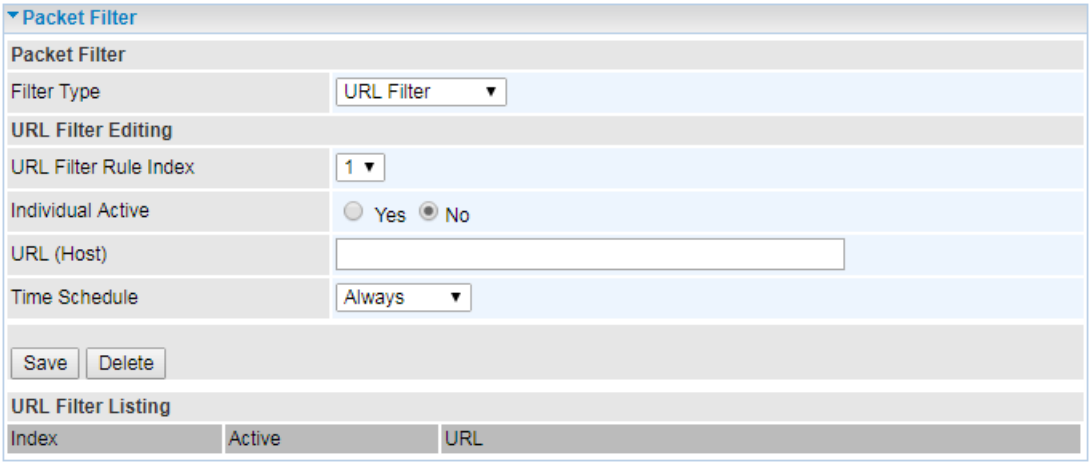
Source Port: The source port number of packets to be monitored.

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**

❖ Packet Filter - URL Filter



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

URL Filter Rule Index: This is item number.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first 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.

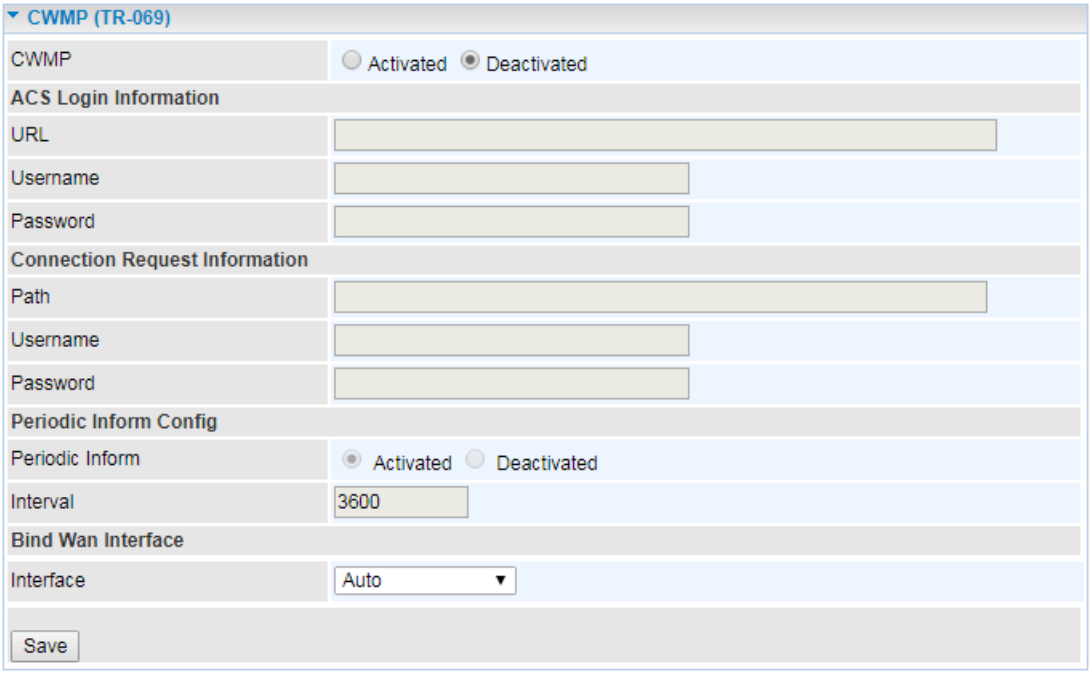
URL (Host): Specified URL which is prohibited from accessing.

Time Schedule: To determine when the rule takes effect. The rule works always or winthin the set timeslot.

CWMP (TR-069)

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

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



CWMP: Select activated to enable CWMP(TR-069)

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.

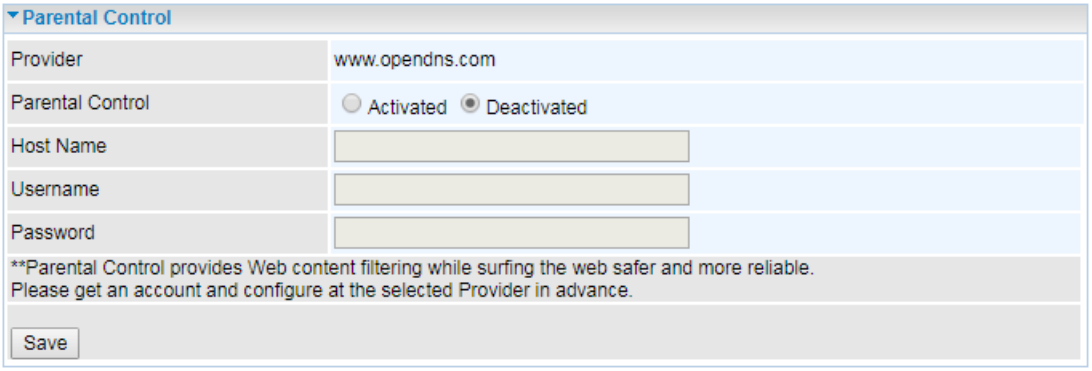
Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

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.

Parental Control

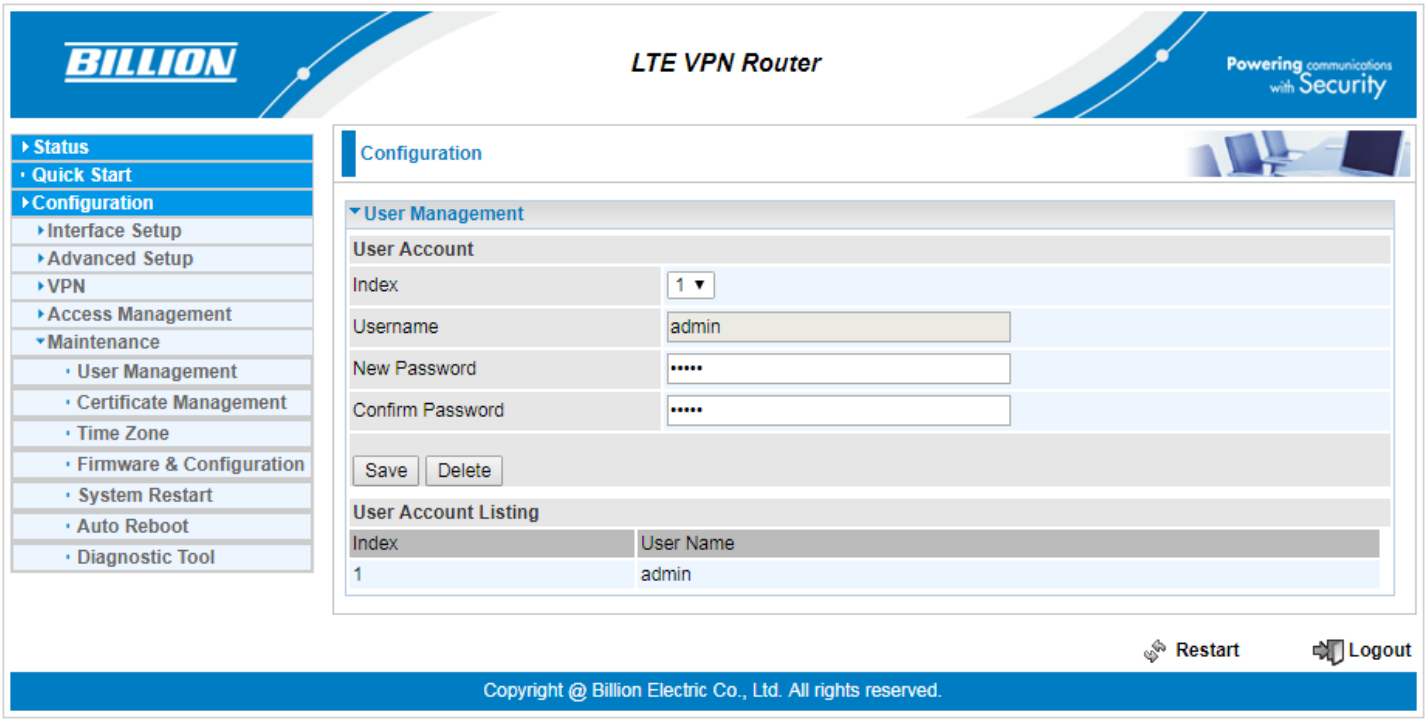
Parental Control provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider “www.opendns.com” in advance. If activated, the Parental Control has the top priority as DNS when accessing internet.



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

Maintenance

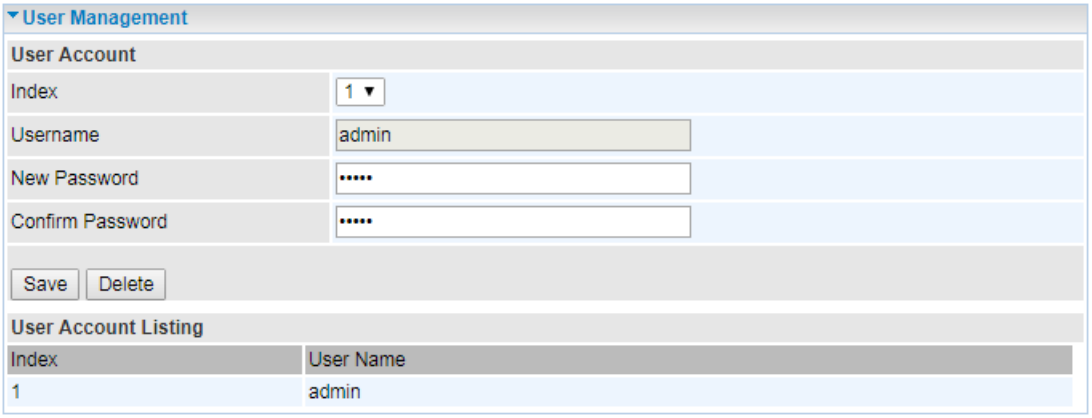
Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including **User Management**, **Certificate Management, Time Zone**, **Firmware & Configuration**, **System Restart**, **Auto Reboot** and **Diagnostic Tool.**



User Management

User Management controls the Router Web GUI permission to the specific account.

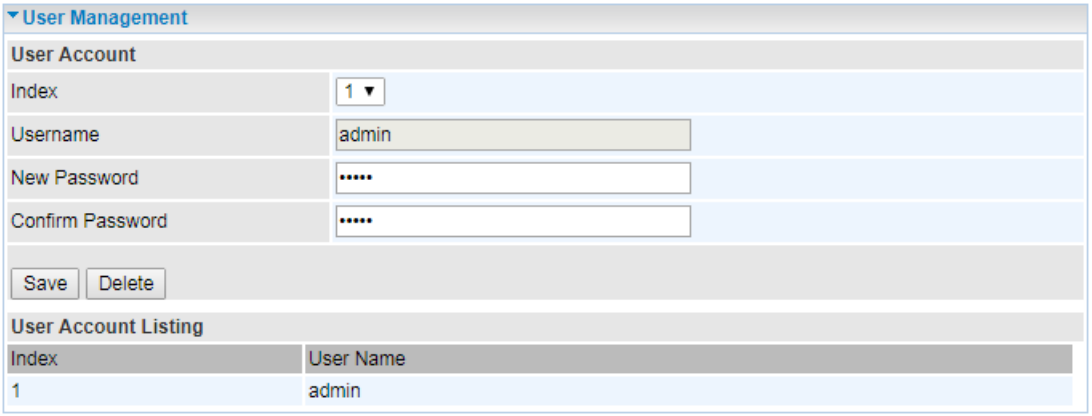
In factory setting, the default accounts are **admin/admin.** The default root account admin has been authorized to web access of router.



❖ Admin / Admin

admin/admin is the root account provided by our router.

Login using the Administrator account, you will have the full accessibility to manage & control your gateway device and can also create user accounts for others to control some of the open configuration settings.



User Setup

Index: User account index.

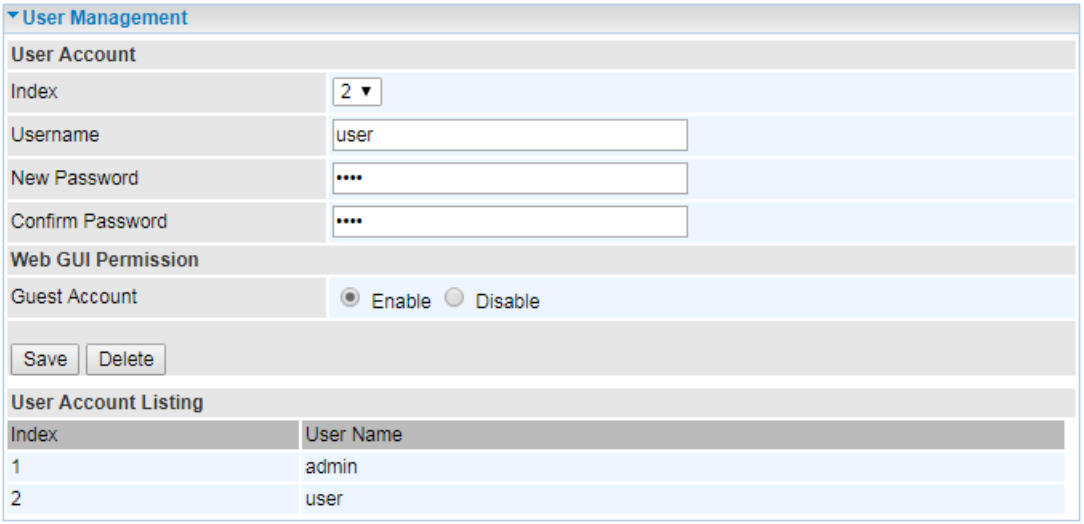
User Name: Users can create account(s) to give it (them) access to router.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password exactly the same as in the previous field.

Login using the Administrator account, you will have the full accessibility to manage & control your gateway device and can also create user accounts for others to control some of the open configuration settings.

❖ Adding additonal user accounts



User Setup

Index: User account index.

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

New Password: Type the password for the user account.

Confirmed Password: Type password again for confirmation.

Web GUI Permission

Guest Account: A pre-set guest account setting granted with **Interface Setup**, **Advanced Setup**, **Access Management** and **Maintenance** access. Enable to have access to Interface Setup, Advanced Setup and Access Management or disable to set the specifics yourself.

Interface Setup: Enable to allowing access to Interface Setup with this account.

Advanced Setup: Enable to allowing access to Advanced Setup with this account.

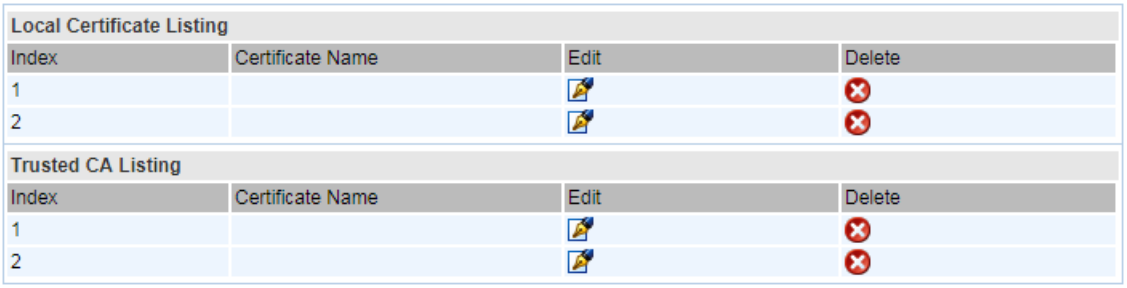
Access Management: Enable to allowing access to Access Management with this account.

Maintenance: Enable to allowing access to Maintenance with this account.

When customers use the additonal user account to login to the router, they are offered with only configuration items set in **Web GUI Permission**.

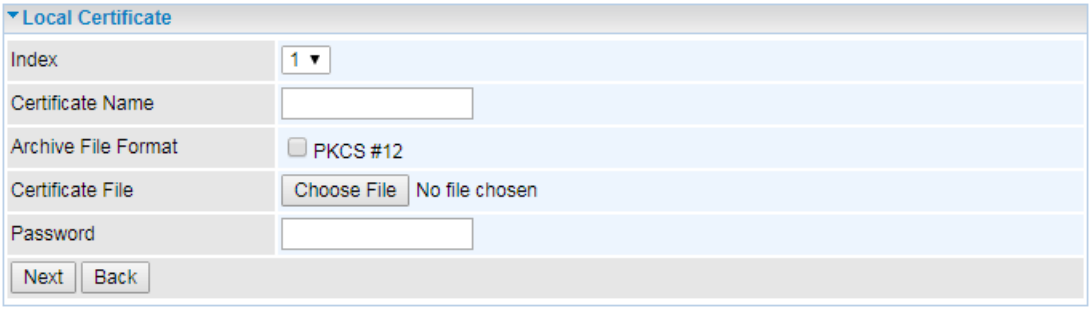
Certificate Management

OpenVPN mutually authenticate each other based on Local Certificate and Trusted CA.



Local Certificate Listing

Edit certificate: Click , move to Local Certificate editing page.

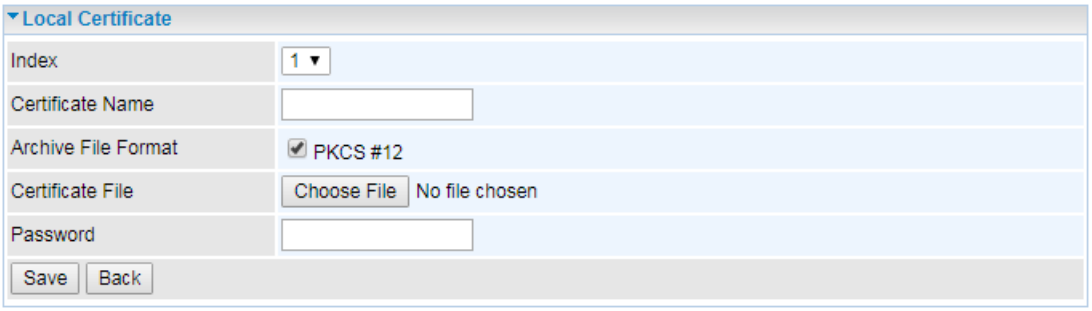


Index: To identify the local certificate. 2 certificates supported.

Certificate Name: User-defined certificate name.

PKCS12: Every certificate is accompanied by a private key. Upload both files if PKCS is disabled. Enable PKCS12 to put Certificate & Private Key in the same file, like *.p12, *.pfx.

- **Check PKS#12:** Check **PKS#12** when the certificate and private key are packed into one file. Browser to locate the target file and upload it.

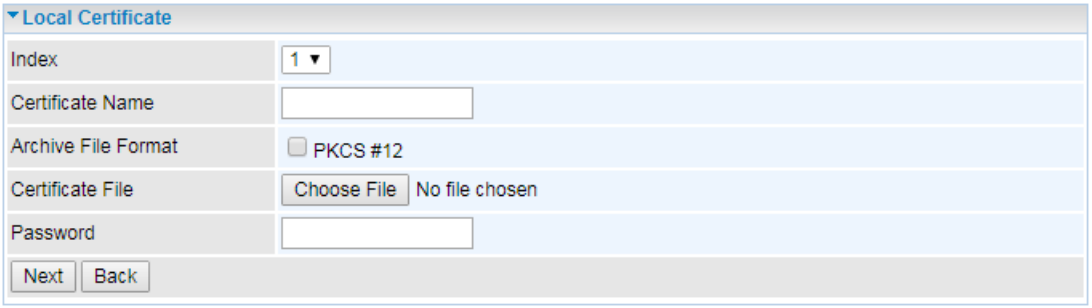


Certificate File: Browse to locate the target certificate file on PC before uploading it.

Password: Enter the password if any, which is used to protect the private key. Otherwise, leave it empty.

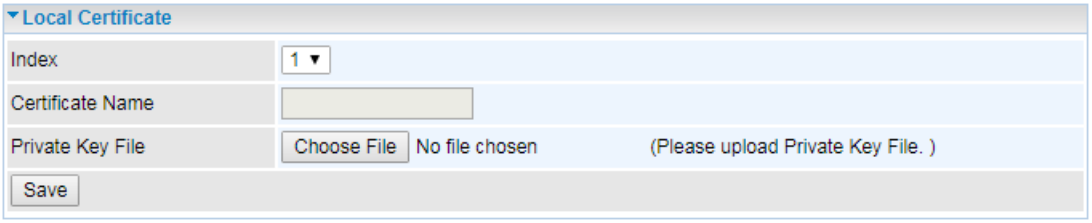
Click **Save** to save the settings.

- **Uncheck PKS#12:** UnCheck **PKS#12** when the certificate and privake key are put in two separate files. Both files need to be uploaded separately.



(Upload the certificate file.)

Certificate File: Browse to locate the target certificate file on PC before uploading it.



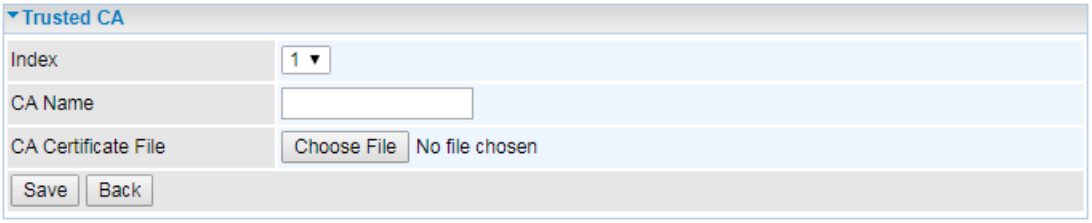
(Upload the private key file.)

Private Key File: Browse to locate the target file on PC before uploading it.

Click **Save** to submit the settings.

Trusted CA Listing

Edit certificate: Click , move to Trusted CA editing page.



Index: To identify the CA files. 2 CAs supported.

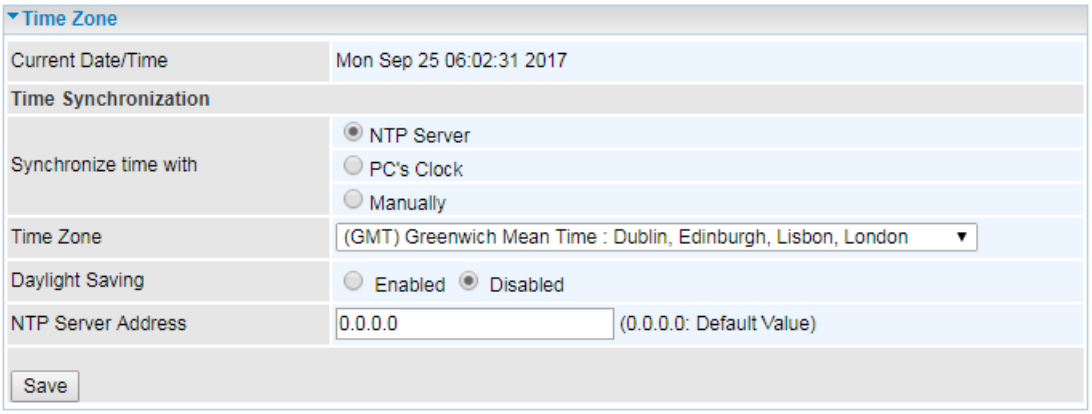
CA Name: User-defined CA name.

CA Certificate File: Browse to locate the target CA certificate file on PC before uploading it.

Click **Save** to save the settings.

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 the default, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



Current Date/Time: To show the current time based on the time synchronization mechanism users choose below.

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

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

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

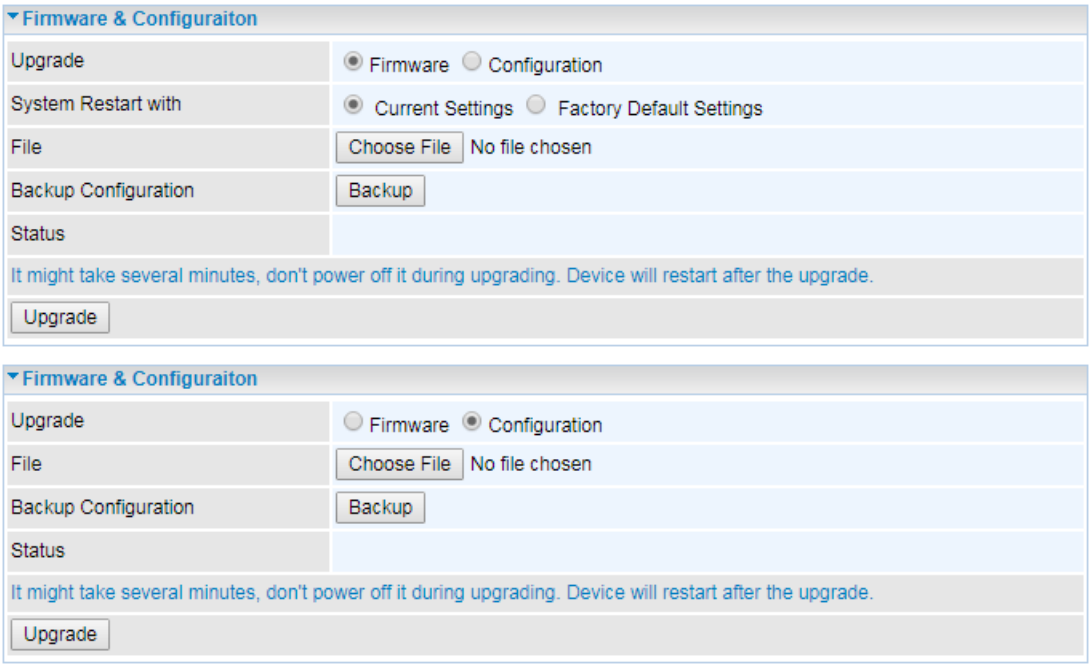
Daylight Saving: Select this option if you use daylight savings time.

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

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your M100 provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of M100, you should download or copy the firmware to your local environment first. Press the **Choose File** button to specify the path of the firmware file. Then, click **Upgrade** to start upgrading. When the procedure is completed, M100 will reset automatically to make the new firmware work.



Upgrade: Choose **Firmware** or **Configuration** you want to update.

System Restart with:

- **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- **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 **Choose File** to find it.

Choose File: Click **Choose File** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

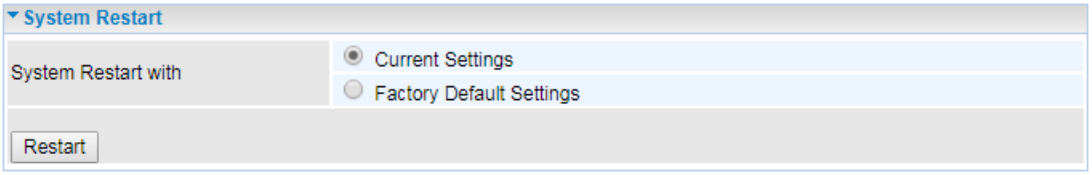
Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your device when making false configurations and want to restore to the original settings.

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

DO NOT turn off / power off the device or interrupt the firmware upgrading while it is still in process. Improper operation could damage your Industrial LTE Router.

System Restart

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

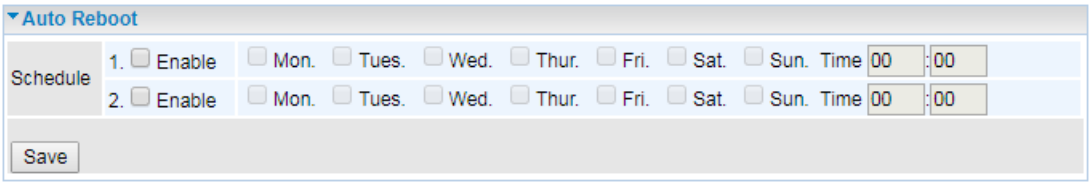


If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to restore to factory default settings.

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

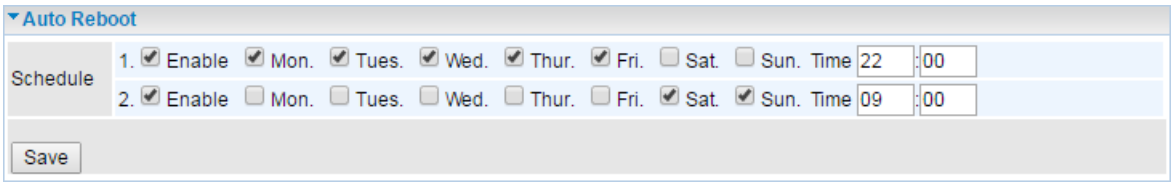
Auto Reboot

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



Enable to set the time schedule for rebooting.

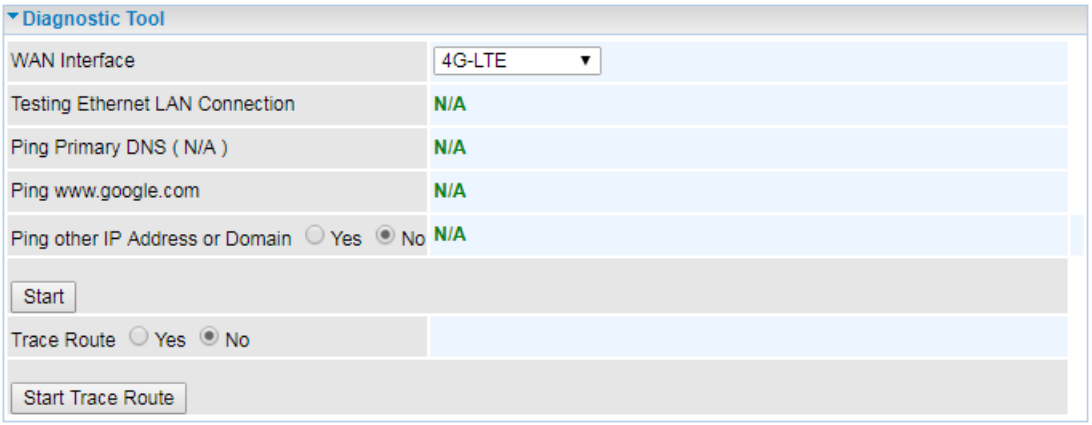
For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:



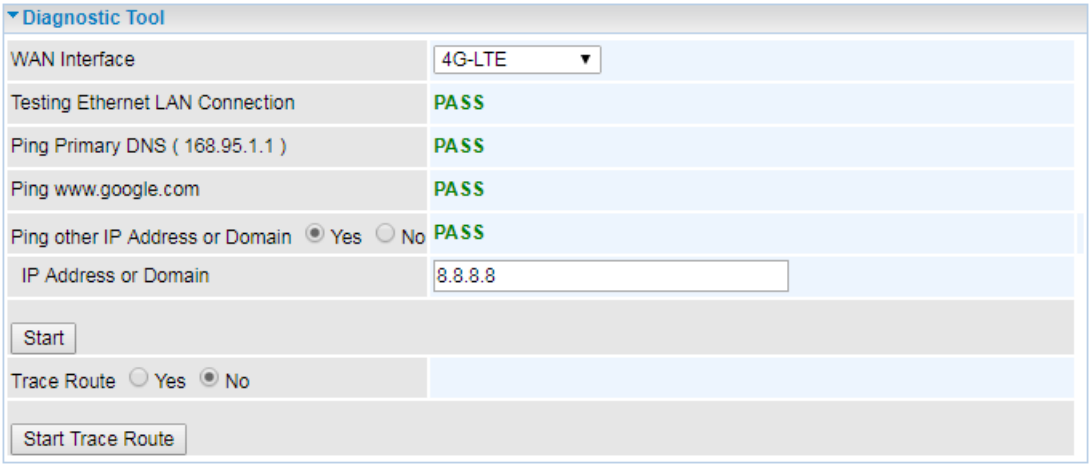
Diagnostics Tool

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

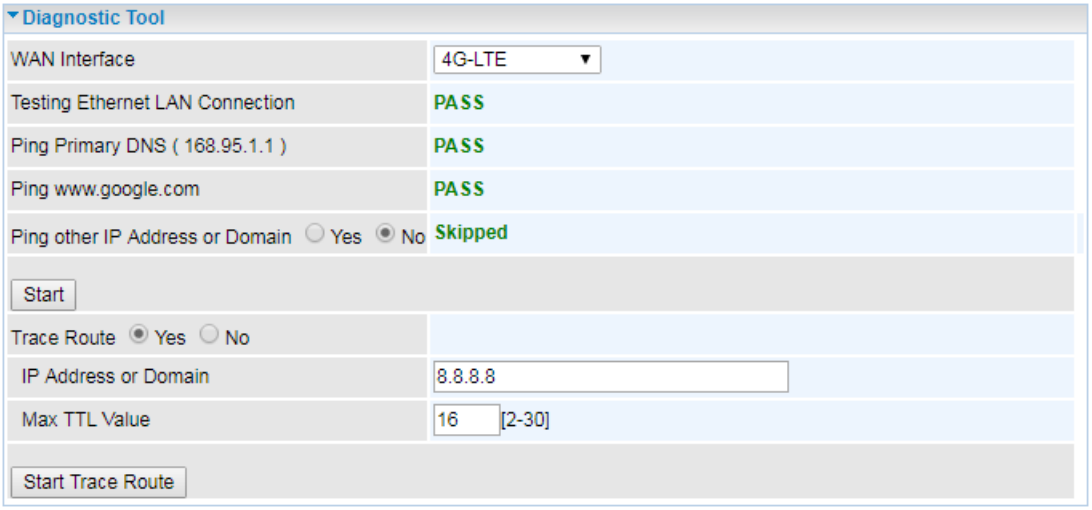
4G/LTE:



Click Start to begin to diagnose the connection.



Click Start Trace Route to begin to trace routing path.



Trace 8.8.8.8

```
traceroute to 8.8.8.8 (8.8.8.8), 16 hops max, 60 byte packets
 1  168.95.98.254 (168.95.98.254)  5.694 ms  5.242 ms  6.335 ms
 2  168.95.25.210 (168.95.25.210)  5.317 ms  5.616 ms  5.796 ms
 3  220.128.8.246 (220.128.8.246)  5.923 ms  6.204 ms  6.302 ms
 4  220.128.1.30 (220.128.1.30)  8.477 ms  8.114 ms  7.942 ms
 5  220.128.26.6 (220.128.26.6)  5.573 ms  8.107 ms  7.919 ms
 6  220.128.26.77 (220.128.26.77)  5.687 ms  5.870 ms  5.926 ms
 7  72.14.202.34 (72.14.202.34)  5.919 ms  6.015 ms  5.592 ms
 8  108.170.244.129 (108.170.244.129)  5.779 ms  5.153 ms  4.964 ms
 9  72.14.238.97 (72.14.238.97)  5.315 ms  5.295 ms  5.269 ms
10  8.8.8.8 (8.8.8.8)  6.854 ms  6.697 ms  6.267 ms
```

Chapter 5: Troubleshooting

If your M100 is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

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

Problem with LAN Interface

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

Recovery Procedures

Problem	Suggested Action

- The front LEDs display incorrectly **- Still cannot access to the router management interface after pressing the RESET button.** **- Software/ Firmware upgrade failure**	Before starting recovery process, please configure the IP address of the PC as 192.168.1.100 and proceed with the following step-by-step guide. 1. Power the router off. 2. Press reset button and power on the router, once the Power flashes Red and Green, keeping press reset button over 6 seconds. 3. Internet LED flashes Green and Red, router entering recovery procedure and router's IP will reset to Emergency IP address (Say 192.168.1.1). 4. Open browser and access http://192.168.1.1 to upload the firmware. 5. Internet LED lit Red, and router starts to write firmware into flash. Please DO NOT power off the router at this step. 6. Internet LED lit Green when successfully upgrade firmware. 7. Power the router off and then on.

Appendix: Product Support & Contact

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

Contact Billion

WORLDWIDE

http://www.billion.com/

MAC OS is a registered Trademark of Apple Computer, Inc.
Windows XP/ Vista/ 7/ 8/ 8.1/ 10 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.