User Manual

BEC 9900VA

Active Ethernet Fiber

802.11ac Gateway with VoIP

April 2020
Version release: v1.2

Copyright Notice

Support Contact Information

Contact Support: http://bectechnologies.net/support/.

Telephone: +1 972 422 0877

TABLE OF CONTENTS

COPYRIGHT NOTICE 1

SUPPORT CONTACT INFORMATION 1

CHAPTER 1: INTRODUCTION 1

INTRODUCTION TO YOUR BEC DEVICE 1

FEATURES & SPECIFICATIONS 3

HARDWARE SPECIFICATIONS 6

CHAPTER 2: PRODUCT OVERVIEW 7

IMPORTANT NOTE FOR USING THIS DEVICE 7

PACKAGE CONTENTS 7

DEVICE DESCRIPTION 8

Front Panel LEDs 8

Rear Panel Connectors 10

SYSTEM RECOVERY PROCEDURES 11

CABLING 11

CHAPTER 3: BASIC INSTALLATION 12

NETWORK CONFIGURATION – IPV4 13

Configuring PC in Windows 10 (IPv4) 13

Configuring PC in Windows 7/8 (IPv4) 15

Configuring PC in Windows Vista (IPv4) 17

NETWORK CONFIGURATION – IPV6 19

Configuring PC in Windows 10 (IPv6) 19

Configuring PC in Windows 7/8 (IPv6) 21

Configuring PC in Windows Vista (IPv6) 23

DEFAULT SETTINGS 25

INFORMATION FROM YOUR ISP 26

CHAPTER 4: DEVICE CONFIGURATION 27

LOGIN TO YOUR DEVICE 27

STATUS 30

Device Info 30
System Status 32
System Log 32
Wireless Status 33
Hotspot Status 33
Statistics 35
DHCP Table 39
IPSec Status 39
PPTP Status 40
L2TP Status 41
GRE Status 41
OpenVPN Status 42
Disk Status 43
VoIP Status 43
ARP Table 45
VRRP Status 45

QUICK START 46

DEVICE CONFIGURATION 49

Interface Setup 49
Internet 49
LAN 54
Wireless (2.4GHz & 5GHz) 57
Wireless MAC Filter (2.4GHz & 5GHz) 68
Wireless 5G Repeater 69
Loopback 70
Dual WAN 71
General Setting 71
Outbound Load Balance 75
Protocol Binding 76
Hotspot 78
General Setting 78
Built-in User Account 81
Authorized of Client 82
Walled Garden 83

Advertisement *84*
Hotspot Status Log *85*
Customization *86*
Advanced Setup 88
Firewall *88*
Routing *89*
Dynamic Routing *90*
NAT *92*
VRRP *97*
Static DNS *98*
QoS *99*
Interface Grouping *103*
Port Isolation *106*
Time Schedule *107*
Mail Alert *108*
VPN 109
IPSec *109*
PPTP Server *119*
PPTP Client *121*
L2TP *128*
GRE Tunnel *136*
OpenVPN *144*
OpenVPN Server *144*
OpenVPN Client *146*
VoIP 154
Basic *154*
Media *156*
Advanced *157*
Speed Dial *158*
Dial Plan *160*
Call Features *164*
NAT Traversal for VoIP *167*
Access Management 169
Device Management *169*
SNMP *170*
Syslog *172*
Universal Plug & Play *173*
Dynamic DNS (DDNS) *174*
Access Control *176*
Packet Filter *179*
CWMP (TR-069) *184*
Parental Control *186*

SAMBA & FTP Server *187*
BECentral Management *190*
Maintenance 191
User Management *191*
Certificate Management *193*
Time Zone *195*
Firmware & Configuration *196*
System Restart *197*
Auto Reboot *198*
Diagnostics Tool *199*

CHAPTER 5: TROUBLESHOOTING 202

Problems with the Router 202
Problem with LAN Interface 202
Recovery Procedures 203

APPENDIX: PRODUCT SUPPORT & CONTACT 204

FCC STATEMENT 205

CHAPTER 1: INTRODUCTION

Introduction to your BEC Device

The BEC 9900VA is a point-to-point (P2P) Active Ethernet Fiber Gateway – featuring a combo WAN, 3-port Gigabit Ethernet Switch, VoIP, Firewall and Wi-Fi 802.11ac access point.

The Combo WAN interface of the BEC 9900VA supports FTTH deployment over fiber optical or copper cables. Operators can use either the optical Small Form Factor Pluggable (SFP) with 100Base and 1000Base auto-sensing functionality or the traditional RJ-45 Gigabit interface for broadband connectivity. Furthermore, the BEC 9900VA integrates a high-power 4×4 MU-MIMO 802.11ac Wireless Access Point delivering wireless speeds up to 2Gbps and two FXS interfaces for VoIP and advanced telephony functionality.

Deliver Uninterrupted Internet Service

The 9900VA is a classic broadband bonding gateway with dual WAN interfaces for redundancy or seamless failover between fiber network via SFP and the wireline, an interchangeable Gigabit Ethernet LAN/WAN, to ensure continuous Internet connectivity. The load balancing and traffic prioritization mechanisms can be enabled to enhance failover performance and maximize bandwidth utilization for critical applications delivery. In the event of a connectivity failure of the primary WAN interface, traffic will automatically redirect to the secondary WAN interface and seamless fallback when the primary interface connection is restored.

New Experience with Wi-Fi Speed and Coverage

With the next wireless generation, 802.11ac, integrated in the BEC 9900VA, the router delivers fast Wi-Fi speeds of up to 2Gbps. The 9900VA supports a link rate up to 300Mbps in 2.4GHz frequency range & 1700Mbps in 5GHz range and is also backward compatible with existing 802.11 a / b / g / n wireless equipment in the network. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over Wireless LAN. BEC 9900VA also supports the Wi-Fi Protected Setup (WPS) standard for easy and secure establishment of a wireless home network. If the user's network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function expands the wireless network without needing any external wires or cables.

Integrated SIP VoIP and Advanced Telephony Features

BEC 9900VA is compliant with SIP standard (RFC3261) and supports SIP registrar. This device integrates with two FXS ports by connecting with two standard analog telephones to receive or place calls over VoIP accounts. The router offers much more great features, Call Waiting, Conference Call, Return Call, etc. The unique Speed Dial Plan provides custom hotkeys of frequently used phone numbers. This state-of-the-art feature is ideal for users who do not need a landline service, delivering high quality, free communication between offices and customers. Making online call is just as easy as dialing an extension number.

Wi-Fi Hotspot with Captive Portal

BEC 9900VA offer Wi-Fi hotspot to share the Internet connection via the active WAN interface with any wireless-enabled devices which is completed separate from the private Wi-Fi network. The captive portal enables highly secure connectivity with multiple authentication options and extensive controls for access and bandwidth management. Customization options allow for operator logos, branding or advertisement placement.

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.

Features & Specifications

- Optical Small Form Factor Pluggable (SFP) and Ethernet IP broadband connectivity
- Versatile Gigabit LAN & Ethernet WAN (GbE WAN) for Cable/Fiber/xDSL high WAN throughput
- Gigabit Ethernet LAN
- IPv6 ready (IPv4/IPv6 dual stack)
- Multiple wireless SSIDs with wireless guest access and client isolation
- IEEE 802.11 a/ac/b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP)
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization management
- Universal Plug and Play (UPnP) Compliance
- Voice over IP compliant with SIP standard
- Two FXS ports for connecting to regular analog telephones
- Call Waiting, Conference Call
- Speed Dial, Return Call, Redial
- Don’t Disturb
- Ease of Use with Quick Installation Wizard
- One USB port for NAS (FTP/ SAMBA server)
- Ideal for SOHO, office, and home users

Availability and Resilience

- Dual-WAN Interfaces
- Auto failover and failback
- High performance external dual-band Wi-Fi antennas

Network Protocols and Features

- IPv4, IPv6, IPv4 / IPv6 dual stack
- IP Tunnel IPv6 in IPv4 (6RD)
- IP Tunnel IPv4 in IPv6 (DS-Lite)
- NAT, static routing and RIP-1/2
- Universal Plug and Play (UPnP) compliant
- Dynamic Domain Name System (DDNS)
- Virtual server and DMZ

- SNTP, DNS relay
- IGMP proxy and IGMP snooping
- MLD proxy and MLD snooping
- Supports port-based Virtual LAN (VLAN)

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

Secured Wi-Fi Access Point

- Compliant with IEEE 802.11 a/b/g/n/ac standards
- 2.4GHz & 5GHz frequency range
- 20/40-MHz channel bandwidth
- Up to 300Mbps (2.4GHz) & 866Mbps (5GHz) wireless data phy rate
- 64/128 bits WEP supported for encryption
- Wireless security with WPA-PSK, WPA2-PSK, Mixed WPA/WAP2-PSK, (TKIP/AES), 802.1x/Radius
- AP, Client Bridge and WDS Operational Modes
- Multiple SSID (4 SSIDs), BSSID
- Wireless MAC filtering
- Wireless Client Isolation
- Wi-Fi Hotspot with Captive Portal
- Dynamic, Wi-Fi client rate-limiting

Quality of Service Control

- Traffic prioritization management based-on Protocol, Port Number and IP Address (IPv4/ IPv6)

USB Application Server

- Storage/NAS: SAMBA Server, FTP Server

VoIP

- Compliant with SIP standard (RFC3261)
- Codec: G.729, G.726, G.711 A-Law, G.711 u-Law
- DTMF Method: Inband, RFC 2833, SIP Info
- Caller ID Generation: DTMF, FSK
- Silence Suppression (VAD), Echo Cancellation
- Call Waiting, Conference Call
- Speed Dial, Return Call, Redial
- Don't Disturb
- FAX Relay: T.38
- Call Detailed Records (CDR)

Management

- Quick Installation wizard
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server / client / relay
- Supports SNMP
- TR-069 supports remote management

Hardware Specifications

Physical Interface

- Dual-Band (2.4GHz & 5G) Wi-Fi: 6 external female RP-SMA connectors
- Power On/Off Button
- Power DC Jack
- Optical SFP 1000Base Port
- Ethernet: 3-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Switch
  - 1 x Versatile Port : LAN 1 / WAN
- USB: USB 2.0 port for storage service
- Wireless on/off and WPS push button
- Factory default reset button
- VoIP phone port: 2 RJ-11 FXS phone ports to connect with 2 regular analog phones.
- LED Indicators: Power / SFP / Ethernet 1-3 / USB / 2.4G & 5G Wi-Fi / WPS / VoIP 1&2 / Internet

Physical Specifications

- Dimensions (W*H*D): 9.04" x 1.69" x 6.10" (229.5mm x 43mm x 155mm)

CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Device

Warning

- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not use the same power source for the 9900VA on other equipment.
- ✓ 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.
- ✓ Avoid using this product and all accessories outdoors.

Attention

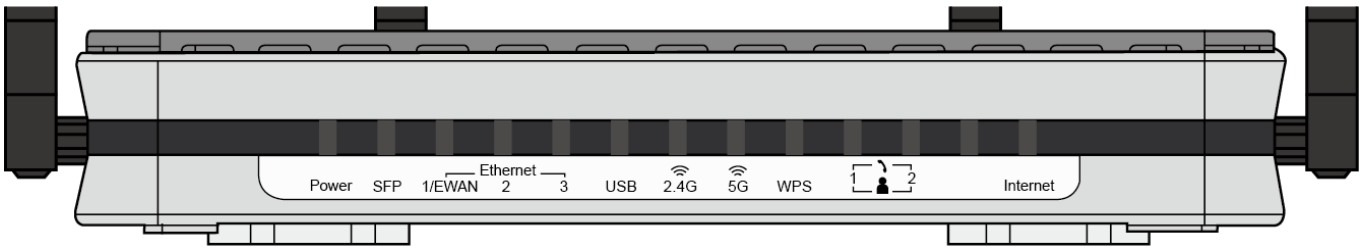
- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

Package Contents

- ✓ BEC 9900VA, the Active Ethernet Router * 1
- ✓ Quick Installation Guide * 1
- ✓ RJ-45 Ethernet cable * 1
- ✓ Dual-Band Wi-Fi Antenna * 6
- ✓ DC Power Adapter * 1

Device Description

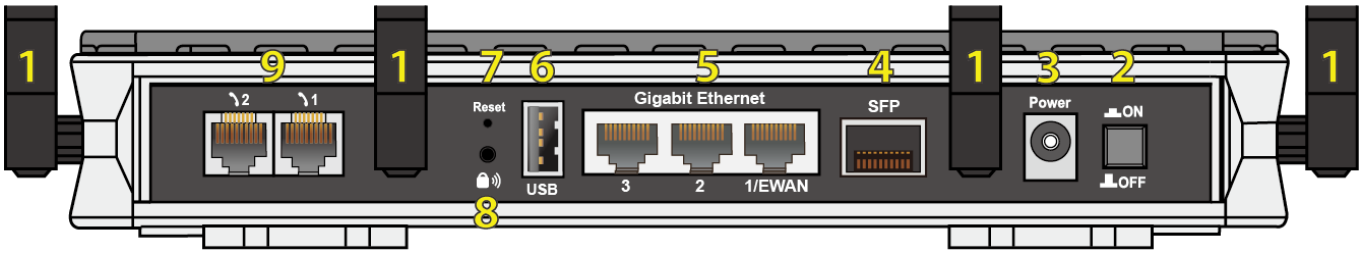
Front Panel LEDs



LED	STATUS	DESCRIPTION
Power	Green	System is up and ready
	Red	System failure
SFP	Green	SFP fiber connection is ready
Gigabit LAN1 / EWAN	Interchangeable LAN/WAN Ethernet – WAN management & configuration via GUI	
	Green	**(Default) Ethernet LAN**: Connected with a gigabit Ethernet device. **(Configured via GUI) Ethernet WAN**: Successfully connected with a broadband device, e.g. ADSL / VDSL / Cable Modem / FTTH router/modem.
	Orange	LAN port is connected with a 10/100Mbps Ethernet device
	Blinking	Data is being transmitted/received
	Off	No device is connected to the Ethernet port
Ethernet Port LAN 2 - 3	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data is being transmitted/received
USB	Green	Connected with a USB dongle or a hard drive.
Wireless 2.4GHz / 5GHz	Green	Wi-Fi connection is established
	Blinking	Data is being transmitted / received
	Off	Wi-Fi connection is turned off
WPS	Green	Wireless device(s) is connected successfully via WPS mode
	Blinking	WPS is enabled and trying to establish a WPS connection
	Off	WPS is turned off

	Green	Successfully registered and ready to use.
	Orange	Phone is off-hook, in-use.
Internet	Green	IP address has received, and traffic is passing thru the device.
	Red	IP address request has failed.

Rear Panel Connectors



INTERFACE		MEANING
1	**Wi-Fi Antenna Connectors**	Female RP-SMA connectors, total of 6. Manually screw the dual-band Wi-Fi antennas tight to each connector.
2	**Power**	Power on/off button.
3	**Power Jack (DC IN)**	Connect the supplied power adapter to this jack.
4	**SFP**	Insert and gently push a 1000Base SFP module until it snaps into the slot tightly.
5	**Gigabit Ethernet (LAN 1 - 3)**	Connect an Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports with a 10Mbps /100Mbps /1000Mbps PC or an office/home network device. *** 1/EWAN** Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable for broadband connectivity. **Note: LAN 1 automatically becomes an EWAN port when ETH WAN interface is selected and configured in the GUI.**
6	**USB**	Connect with a USB hard drive for storage/file sharing.
7	**Reset**	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).
8	**WPS & Wi-Fi On/Off**	By controlling the pressing time, users can achieve two different effects: **(1) WPS*: ** Press &hold the button for **2 seconds** to trigger WPS function. **(2) Wireless ON/OFF button**: Press & hold the button for **more than 6 seconds** to turn on/off the wireless. *** For WPS configuration, please refer to the WPS section in the User Manual.**
9	**FXS Ports (1-2)**	Connect your analog phone(s) to the FXS port(s) with RJ-11 cable(s).

System Recovery Procedures

The purpose is to allow users to restore the 9900VA to its initial stage when the device is outage, upgraded to a wrong / broken firmware, cannot access to the GUI with wrong username and/or password, etc.

Step 1 – Configure your PC Network IP Address

Before performing the system recovery, assign this IP address and Netmask to your PC, **192.168.1.100** and **255.255.255.0** respectively.

Step 2 – Reset your 9900VA Device

2.1 Power off your 9900VA

2.2 Power on the 9900VA while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, etc.).

2.3 When the POWER LED turns RED, keep holding and pushing the RESET button until the INTERNET LED flashes in GREEN

Step 3 – Restore your 9900VA Device

With INTERNET light flashes green, 9900VA is in recovery mode and ready for a new Firmware.

3.1 Open a web browser and type the IP address, **192.168.1.1**, to access to the recovery page.

NOTE: In the recovery mode, 9900VA will not respond to any PING or other requests.

3.2 Browse to the new Firmware image file then click Upload to start the upgrade process.

3.3 INTERNET LED turns red means the Firmware upgrade is in process.

DO NOT power off or reboot the device, it would permanently damage your 9900VA.

3.4 INTERNET LED turns green after the Firmware upgrade completed

3.5 Power cycle on & off to regain access to the 9900VA.

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.

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 10 / 8 / 7/ Vista, 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 or 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. Check your PC's network components first. 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.

Attention

Any TCP/IP capable workstation can be used to communicate with or through the 9900VA. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

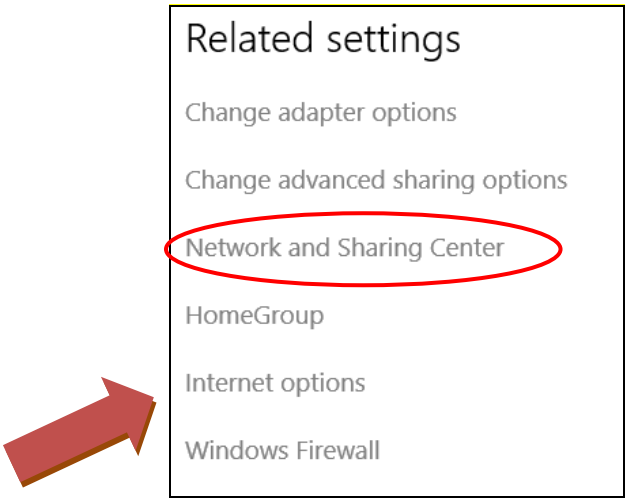
Configuring PC in Windows 10 (IPv4)

1. Click  .

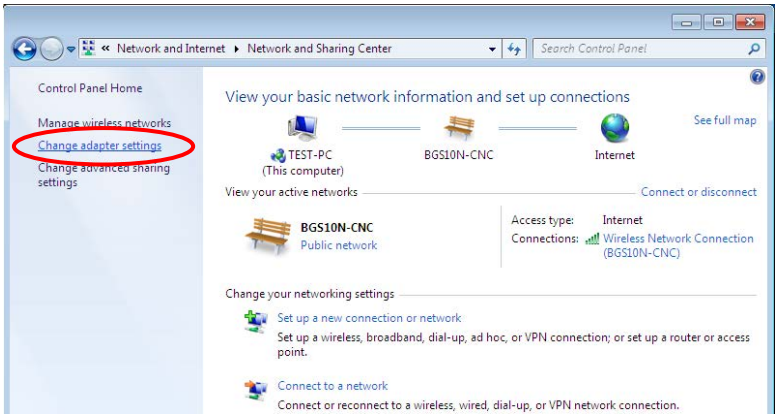
2. Click 

3. Then click on **Network and Internet**.

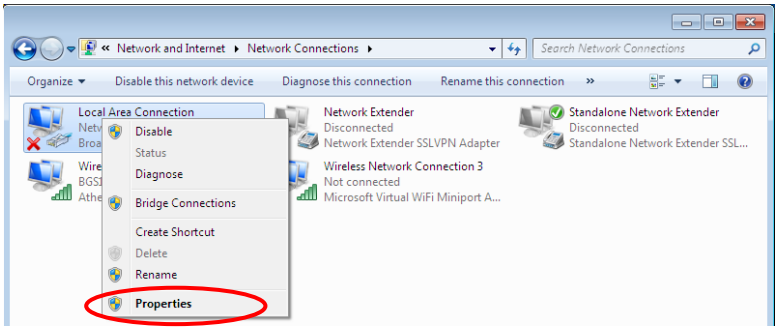

4. Under **Related settings,** select **Network and Sharing Center**



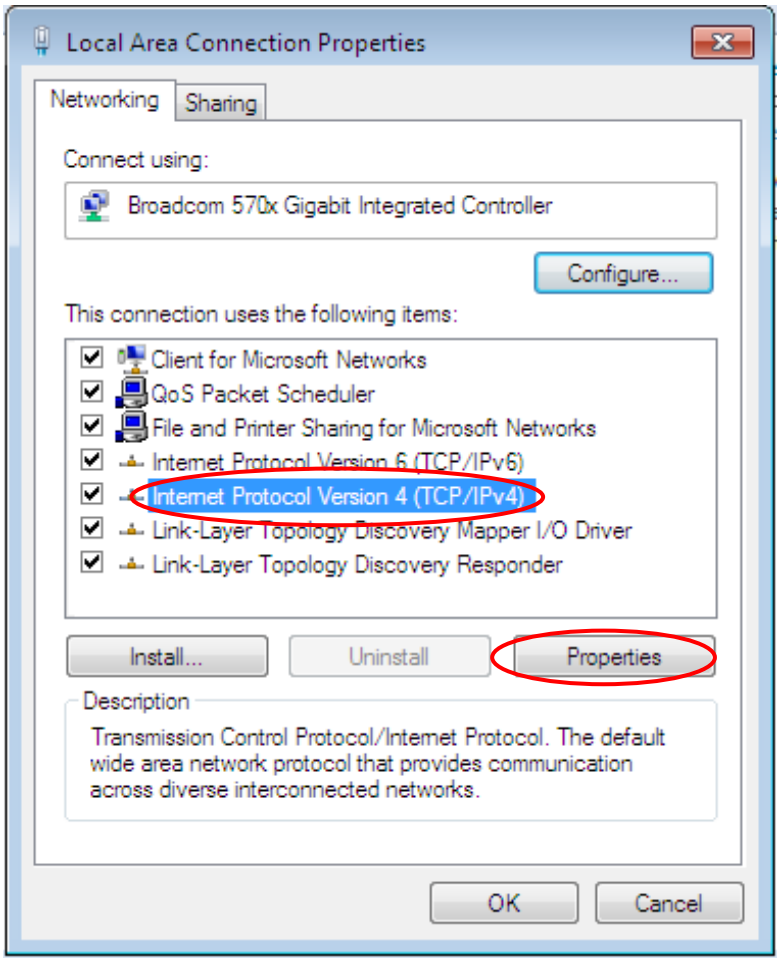
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



6. Select the **Local Area Connection**, and right click the icon to select **Properties**.

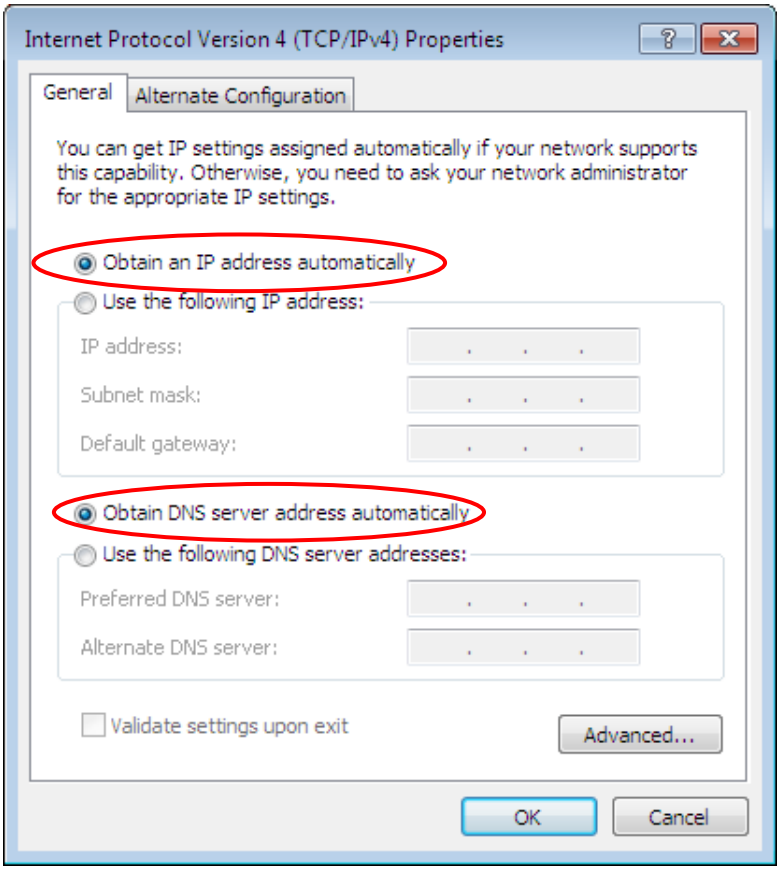


7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

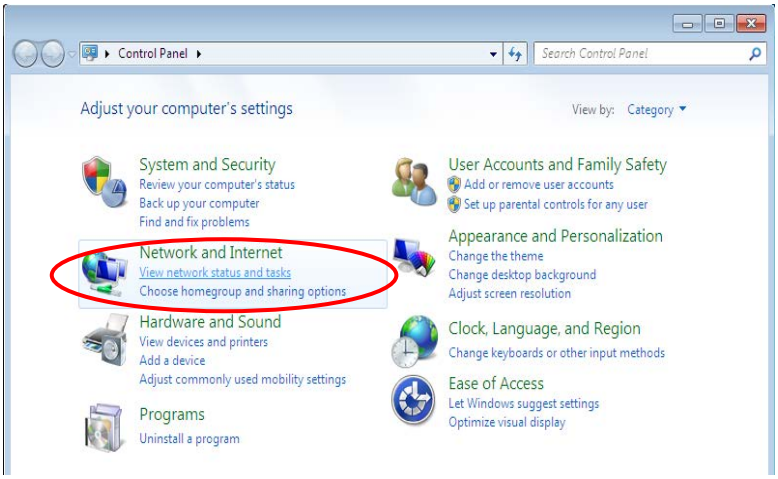
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



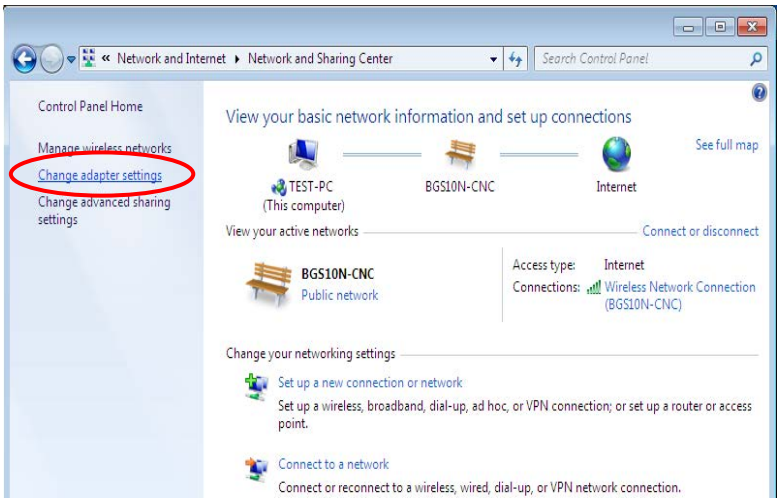
Configuring PC in Windows 7/8 (IPv4)

1. Go to **Start**. Click on **Control Panel**.

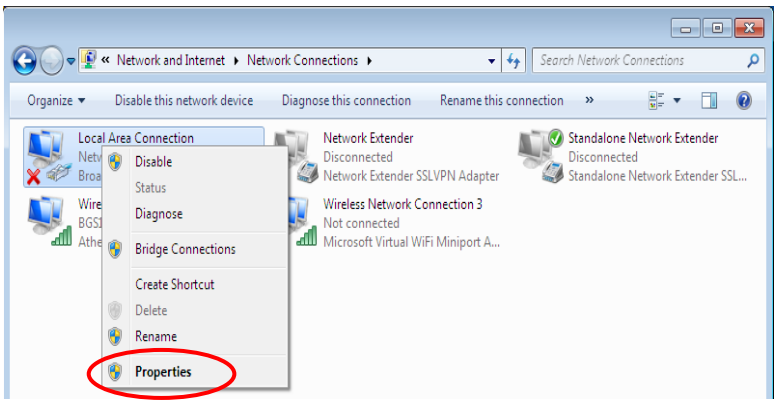
2. Then click on **Network and Internet**.



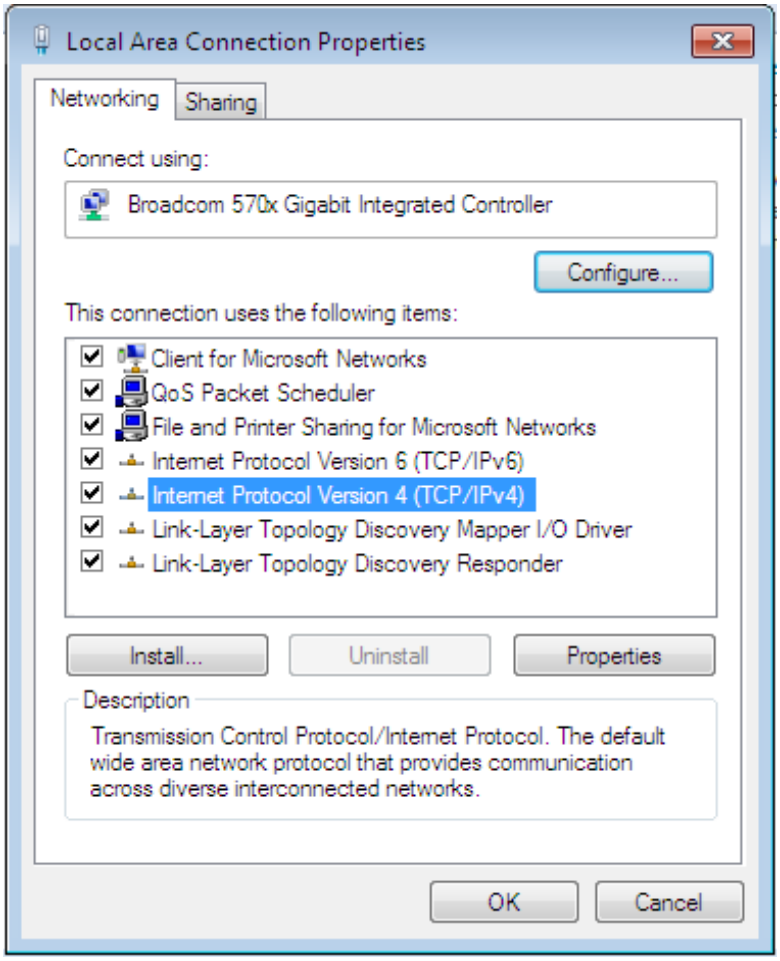
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



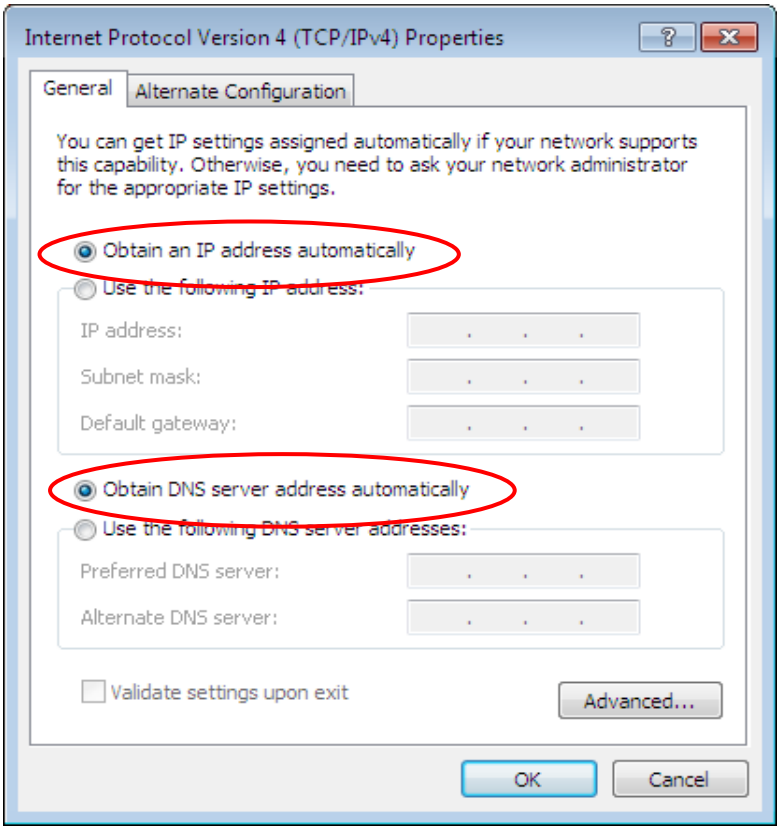
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.

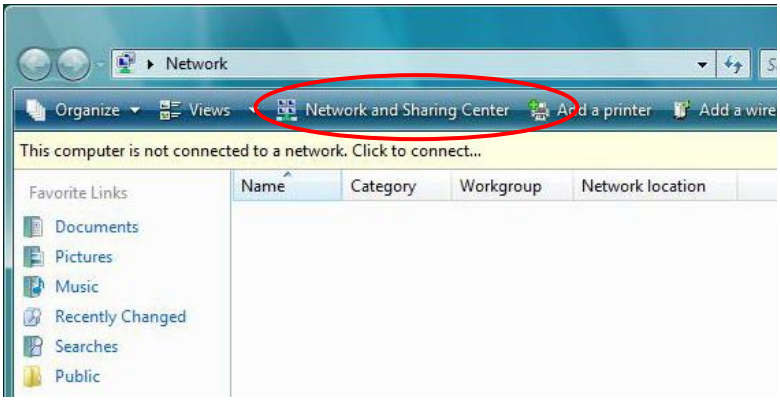


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

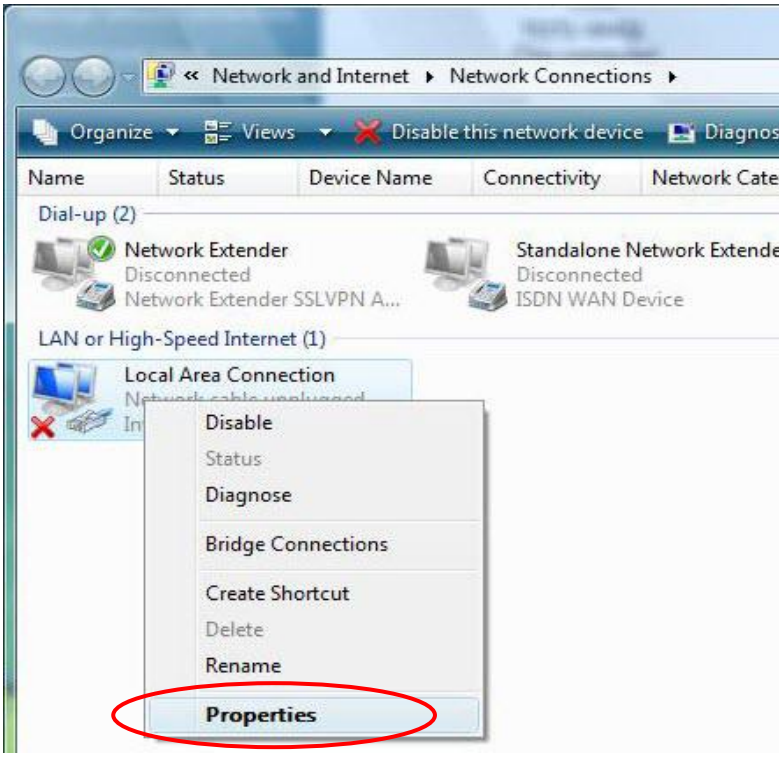
1. Go to **Start**. Click on **Network**.



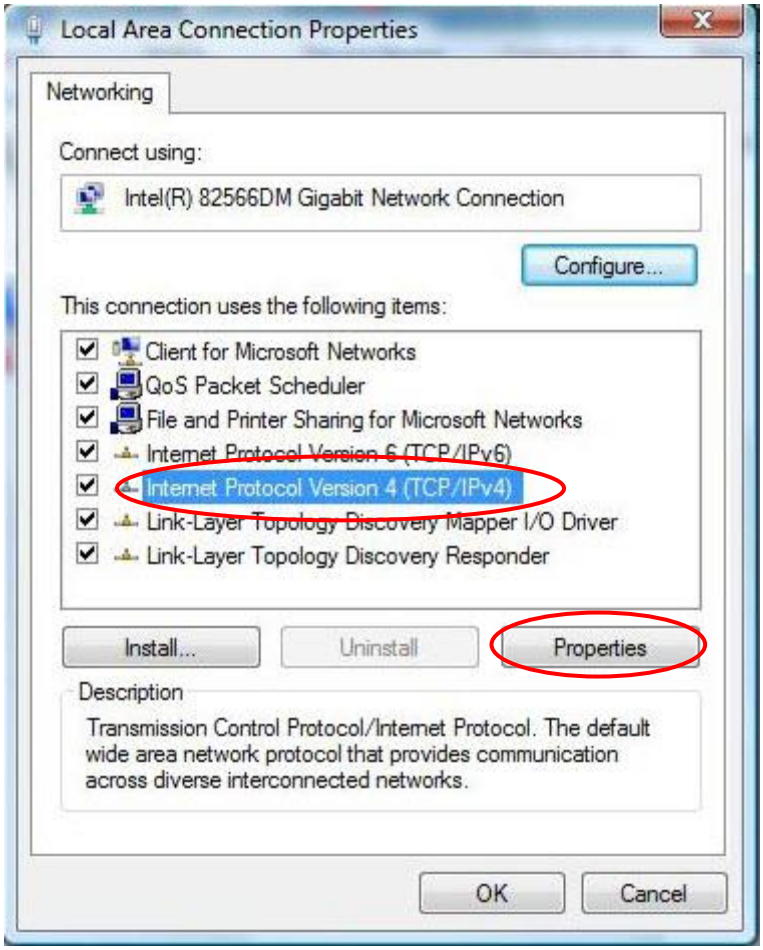
2. Then click on **Network and Sharing Center** at the top bar.

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left windowpane.

4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

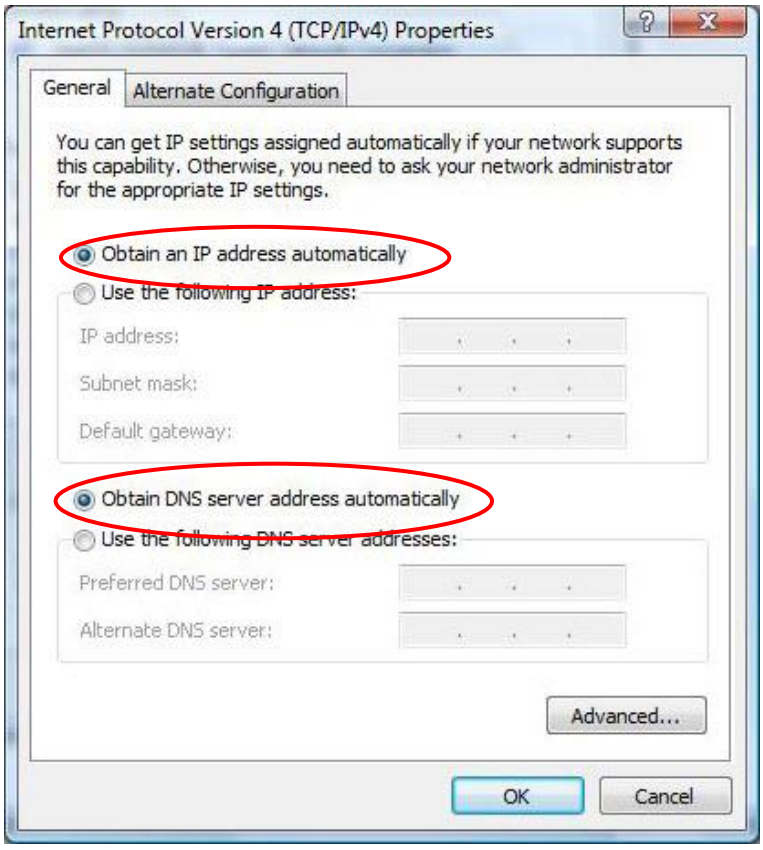


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Network Configuration – IPv6

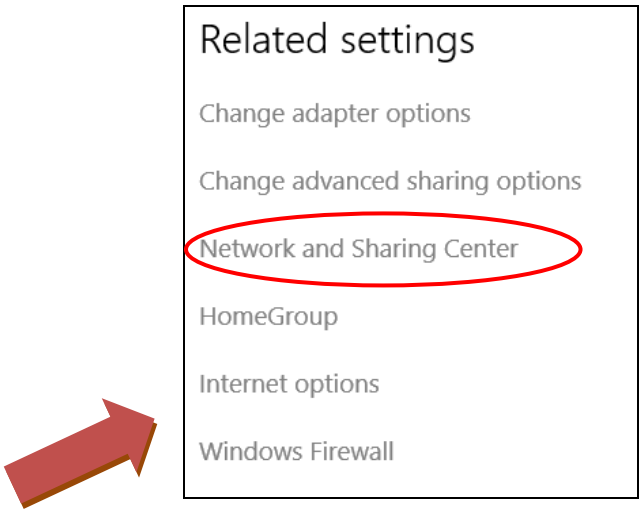
Configuring PC in Windows 10 (IPv6)

1. Click  .

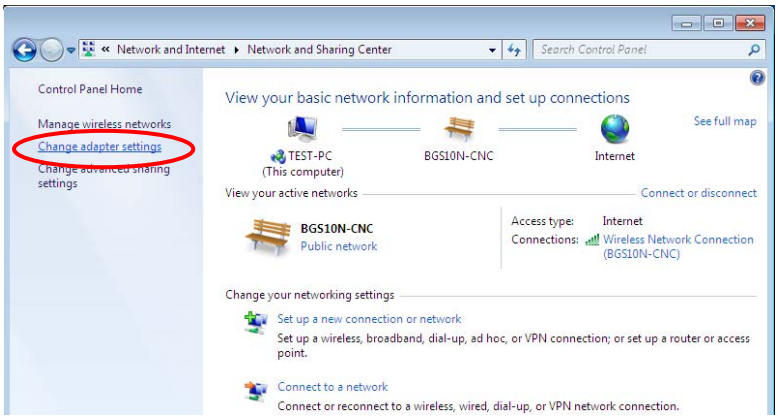
2. Click 

3. Then click on **Network and Internet**.

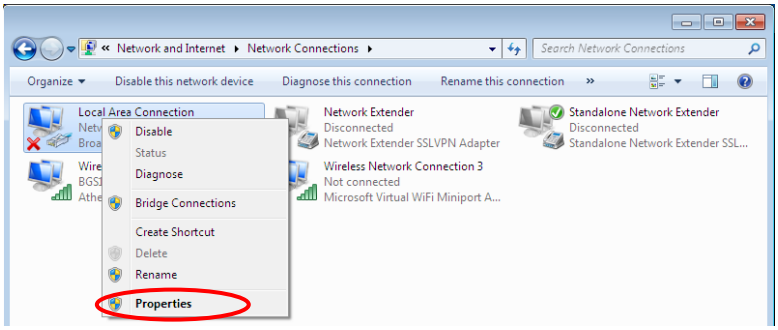

4. Under **Related settings,** select **Network and Sharing Center**



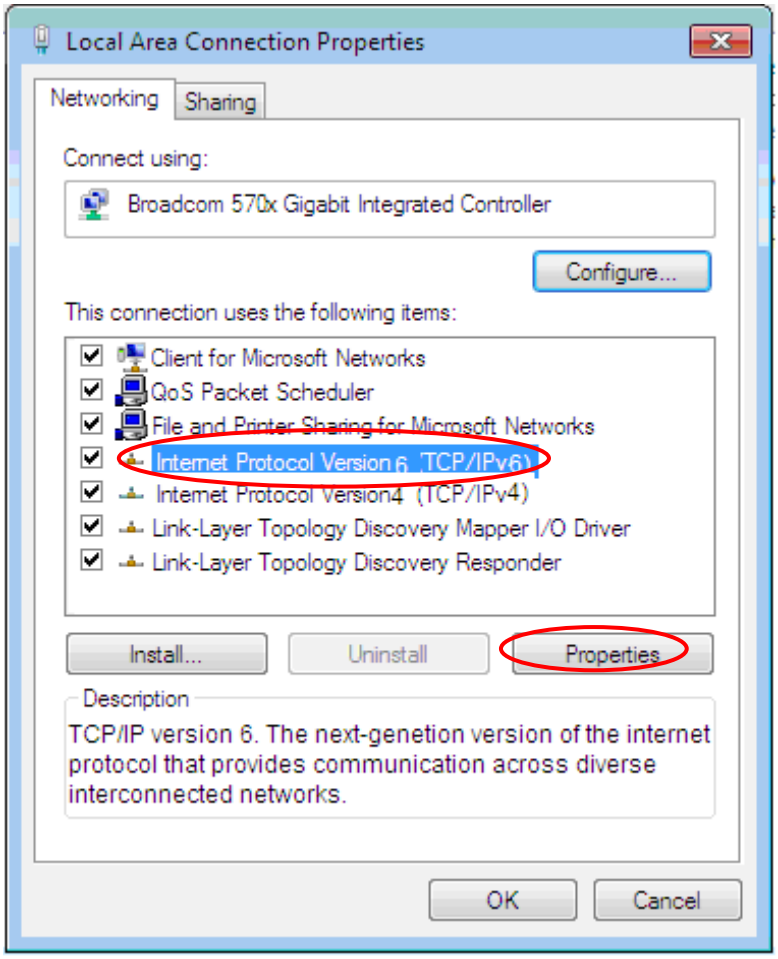
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



6. Select the **Local Area Connection**, and right click the icon to select **Properties**.

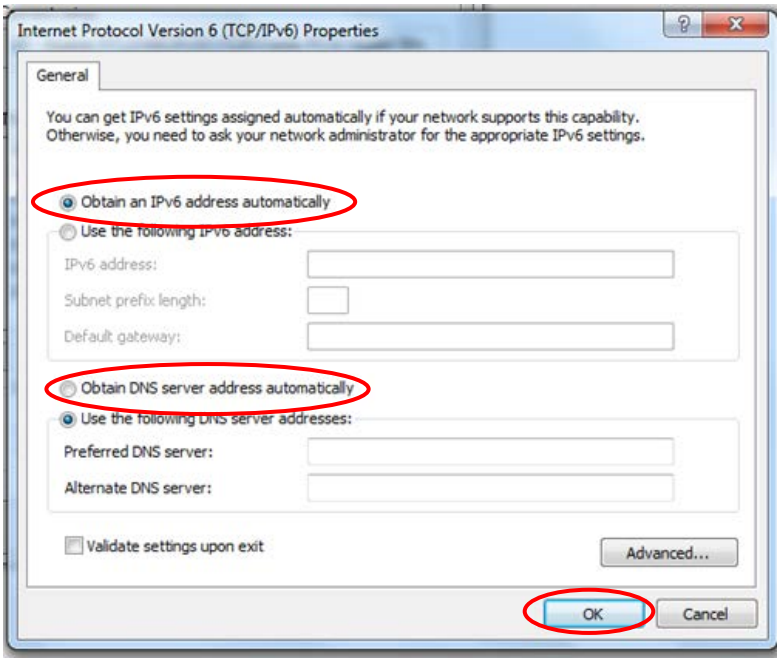


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



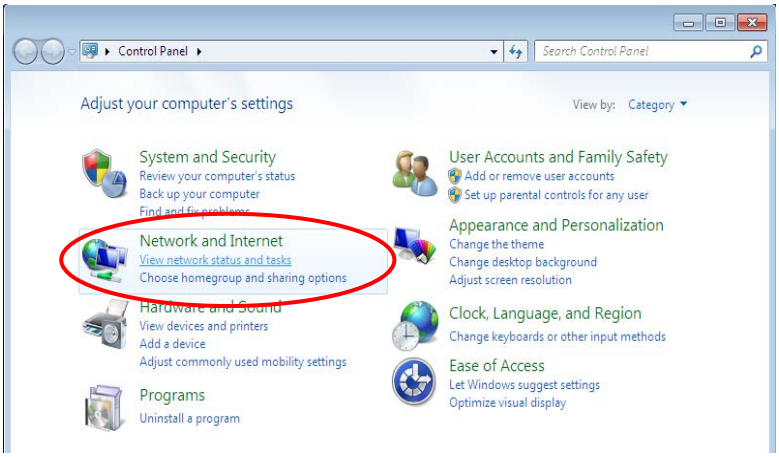
8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



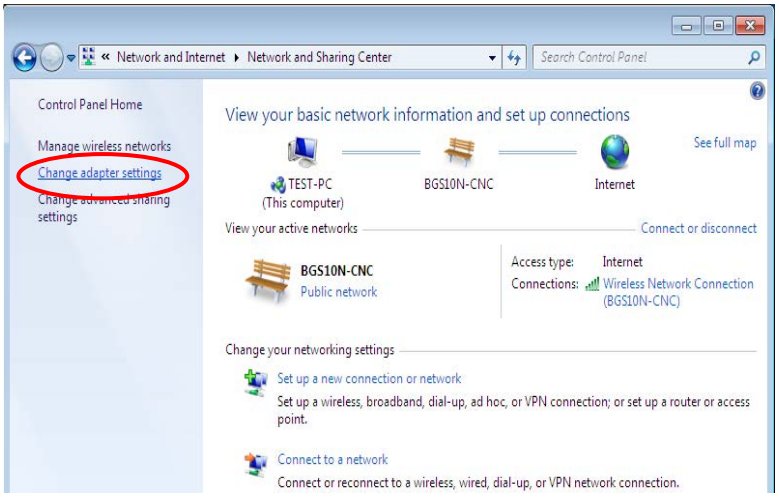
Configuring PC in Windows 7/8 (IPv6)

1. Go to **Start**. Click on **Control Panel**.

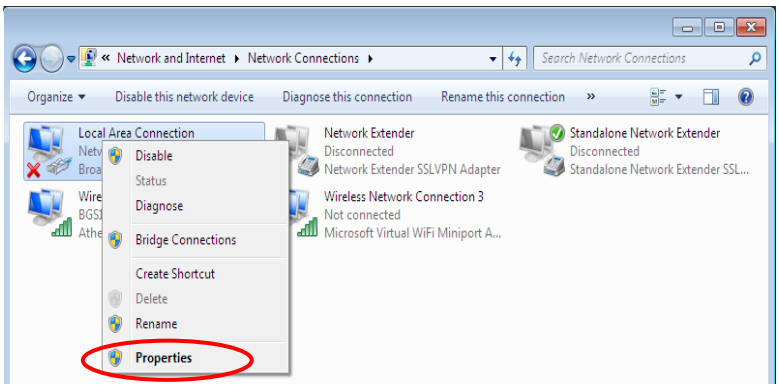


2. Then click on **Network and Internet**.

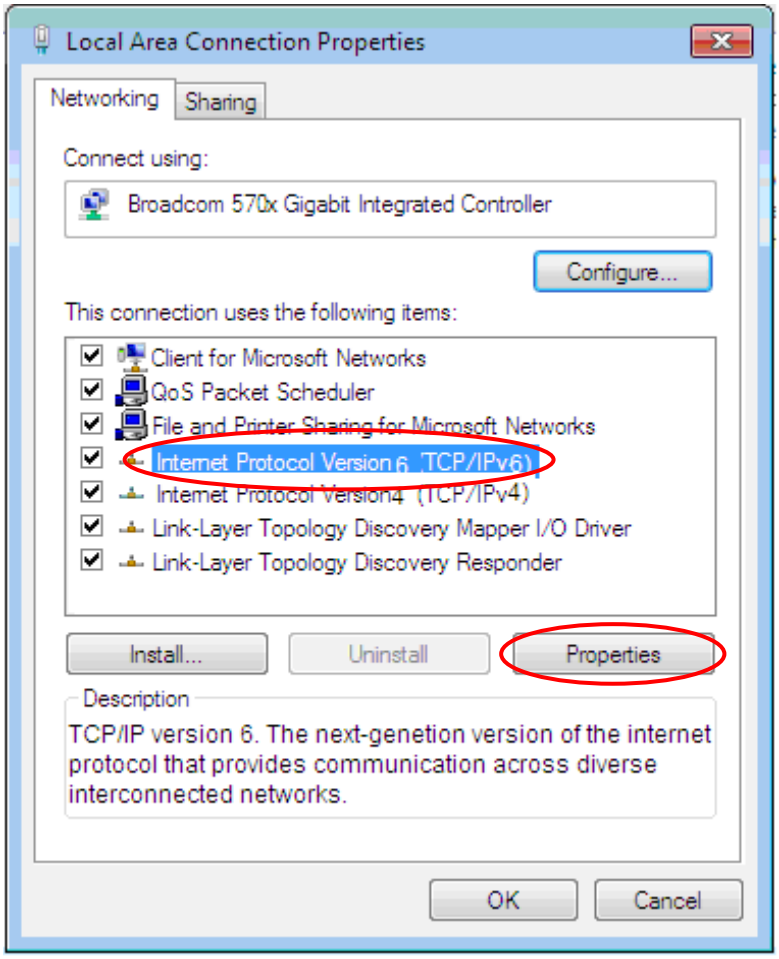
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

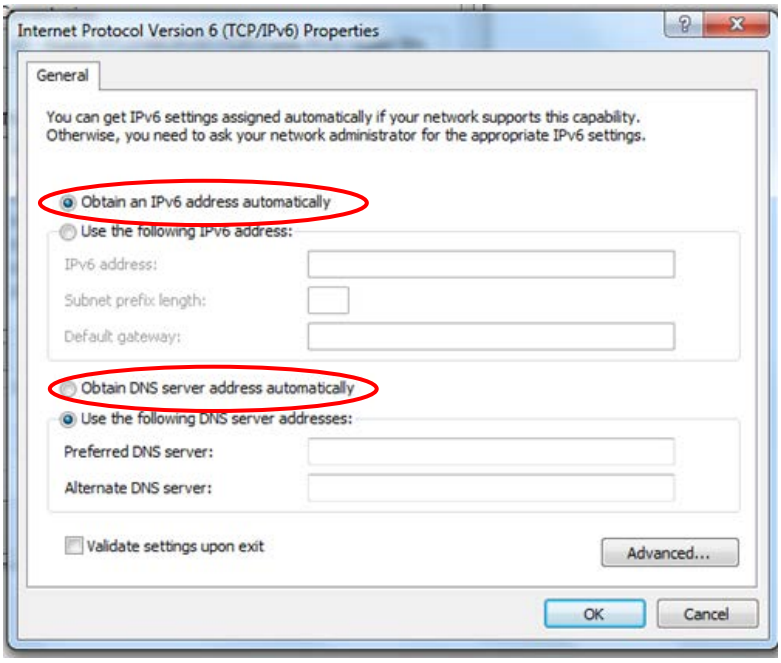


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



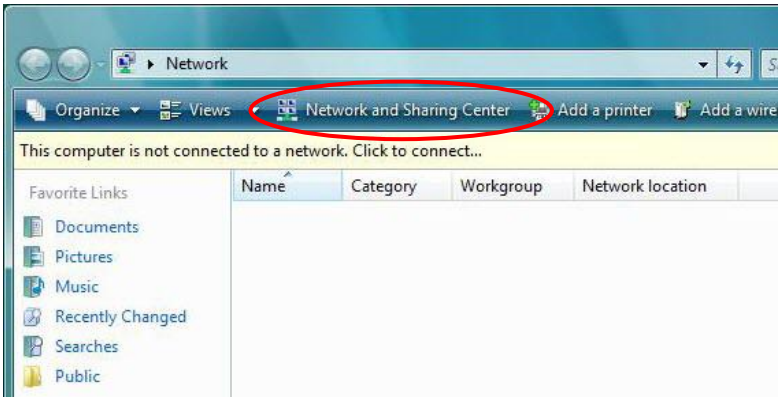
6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



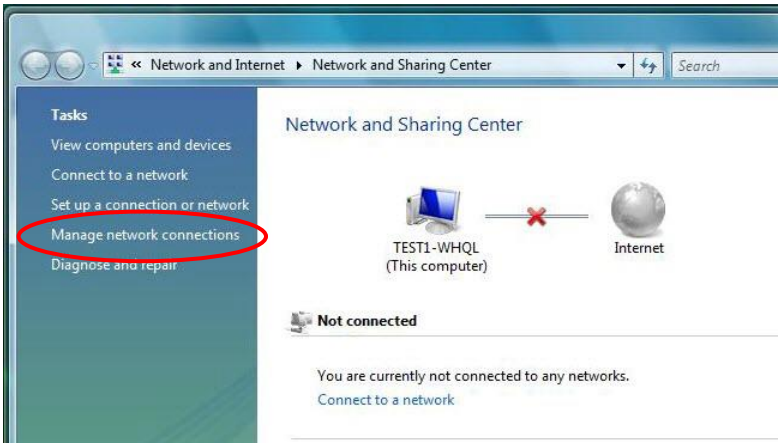
Configuring PC in Windows Vista (IPv6)

1. Go to **Start**. Click on **Network**.

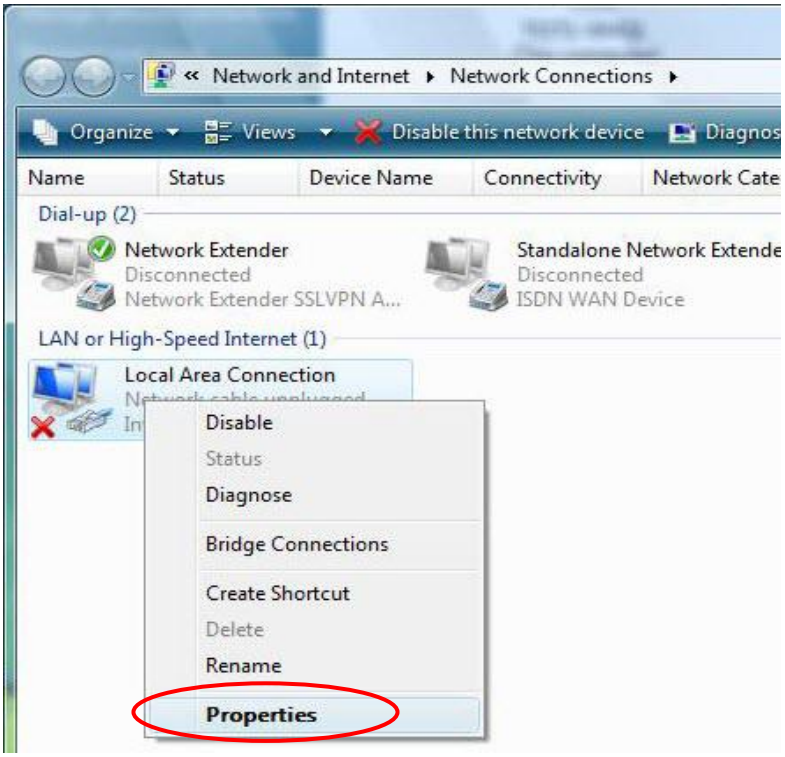


2. Then click on **Network and Sharing Center** at the top bar.

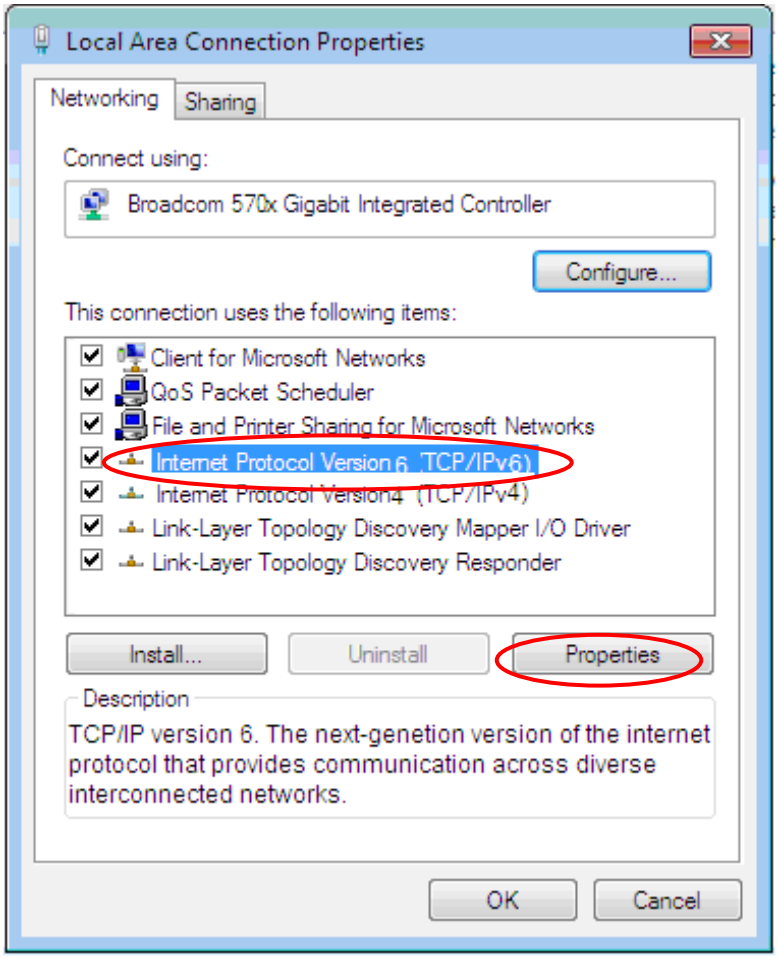
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left windowpane.



4. Select the **Local Area Connection**, and right click the icon to select **Properties**.

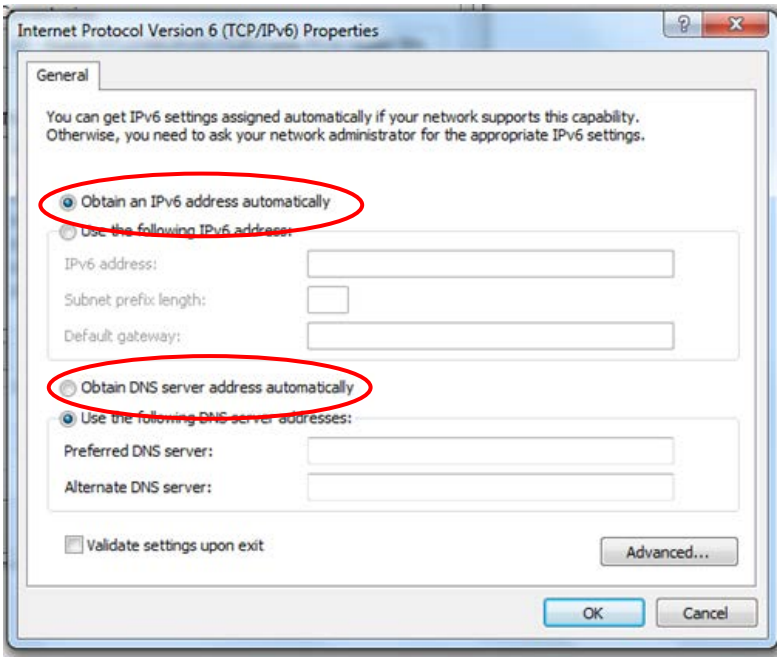


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



6. In the **TCP/IPv6 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Default Settings

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

Web Interface: (Username and Password)

Administrator

- ✔ Username: admin
- ✔ Password: admin

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: 100

Information from Your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is offered, Dynamic IP address, Static IP address, PPPoE or Bridge Mode.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Dynamic IP Address	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Static IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
Bridge Mode	Pure Bridge

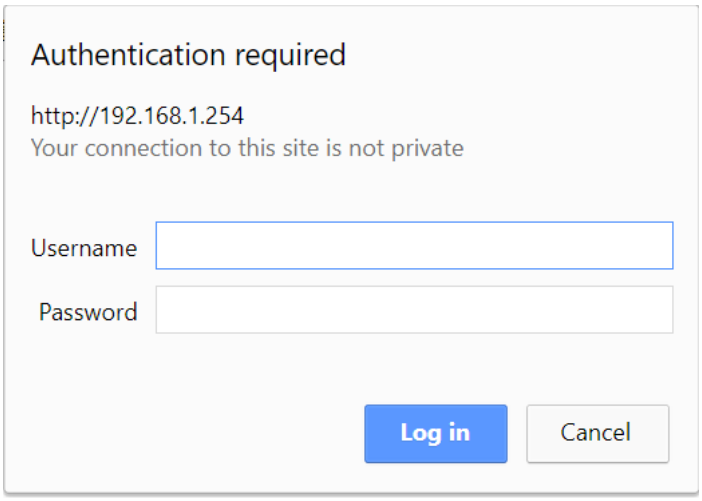
CHAPTER 4: DEVICE CONFIGURATION

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 username and password window prompt appears.

The default **Administrator** username is **"admin"** and password is **"admin".**

NOTE: This username / password may vary by different Internet Service Providers.



Congratulations! You have successfully logged on to your 9900VA

Once you have logged on to your 9900VA 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 pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	Device Info System Status System Log Wireless Status Hotspot Status Statistics DHCP Table IPSec Status PPTP Status L2TP Status GRE Status OpenVPN Status Disk Status VoIP - VoIP Status - VoIP Call Log ARP Table VRRP Status		**Interface Setup** - Internet - LAN - Wireless 2.4G & 5G - Wireless MAC Filter 2.4G & 5G - Loopback **Dual WAN** - General Setting - Outbound Load Balance - Protocol Binding **Hotspot** - General Setting - Built-in User Account - Authorized of Client - Walled Garden - Advertisement - Hotspot Status Log - Customized **Advanced Setup** - Firewall - Routing - Dynamic Routing - NAT - VRRP - Static DNS - QoS - Interface Grouping - Time Schedule - Mail Alert **VPN** - IPSec - PPTP Server & Client - L2TP - GRE - OpenVPN Server & Client **VoIP** - Basic - Media - Advanced - Speed Dial - Dial Plan - Call Features - NAT Traversal **Access Management** - Device Management - SNMP - Syslog - Universal Plug & Play - Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - SAMBA & FTP Server - BECentral Management **Maintenance**

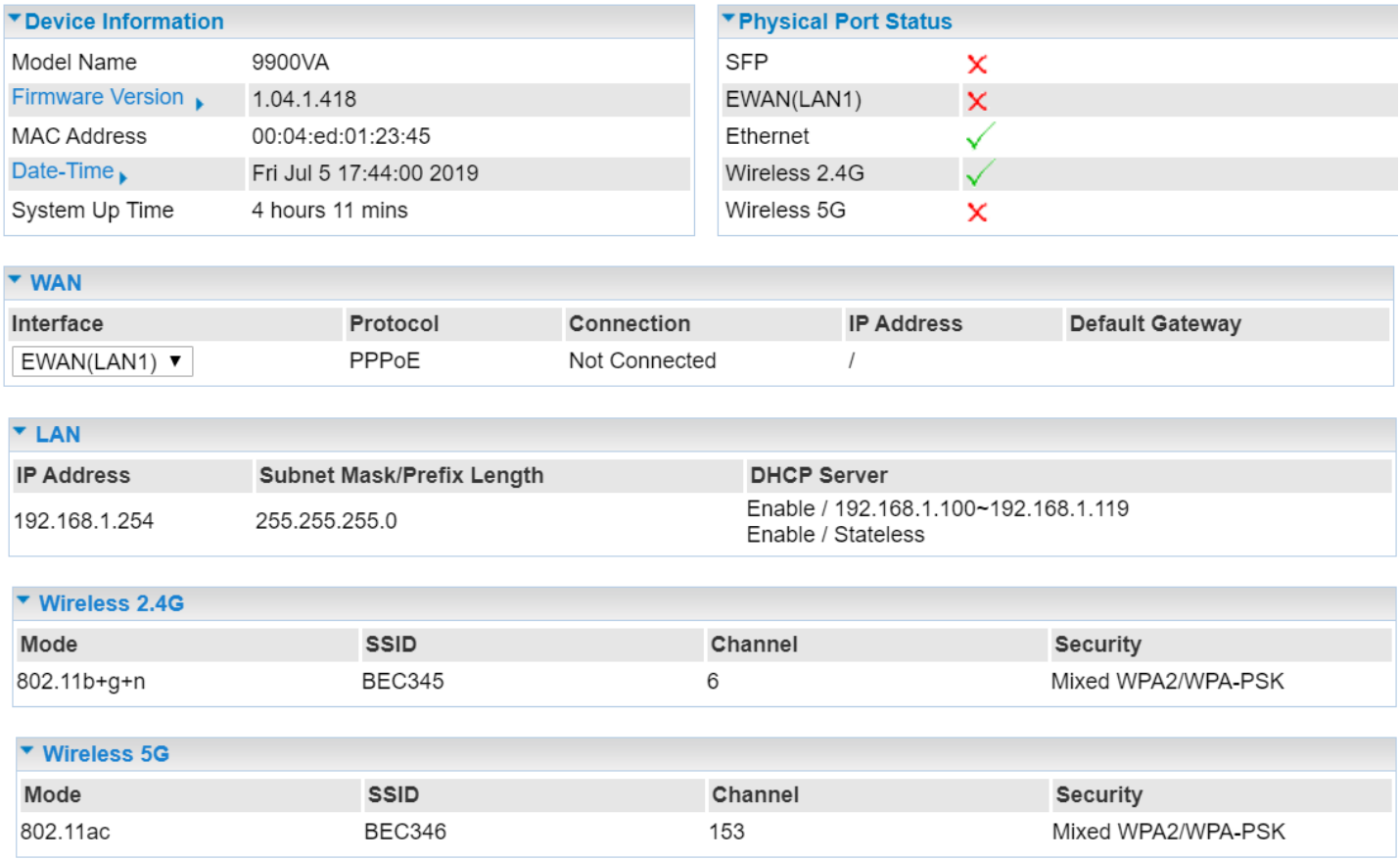
			- User Management - Certificate Management - Time Zone - Firmware & Configuration - System Restart - Auto Reboot - Diagnostic Tool

Please see the relevant sections of this manual for detailed instructions on how to configure your **9900VA** device.

Status

Device Info

It provides brief status summary of the device.



Device Information

Model Name	9900VA
Firmware Version	1.04.1.418
MAC Address	00:04:ed:01:23:45
Date-Time	Fri Jul 5 17:44:00 2019
System Up Time	4 hours 11 mins

Physical Port Status

SFP	✗
EWAN(LAN1)	✗
Ethernet	✓
Wireless 2.4G	✓
Wireless 5G	✗

WAN

Interface	Protocol	Connection	IP Address	Default Gateway
EWAN(LAN1)	PPPoE	Not Connected	/	

LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.119 Enable / Stateless

Wireless 2.4G

Mode	SSID	Channel	Security
802.11b+g+n	BEC345	6	Mixed WPA2/WPA-PSK

Wireless 5G

Mode	SSID	Channel	Security
802.11ac	BEC346	153	Mixed WPA2/WPA-PSK

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Data Time: Setup correct time on the **9900VA** with your PC. Check on **Time Zone** section for more configuration information.

System Uptime: Display how long the **9900VA** has been powered on.

Physical Port Status

Physical Port Status：Display available connection interfaces, WAN (SFP, Ethernet WAN) and LAN (Ethernet, Wireless 2.4G, and Wireless 5G) are supported in the 9900VA.

WAN

Interface: List current available WAN connections.

Protocol: Display selected WAN connection protocol

Connection: The current connection status.

IP Address: WAN port IP address.

Default Gateway: The IP address of the default gateway.

LAN

IP Address: LAN port IPv4 address.

Subnet Mask/Prefix Length: Display LAN port IP subnet mask of IPv4 and/or Prefix length of IPv6.

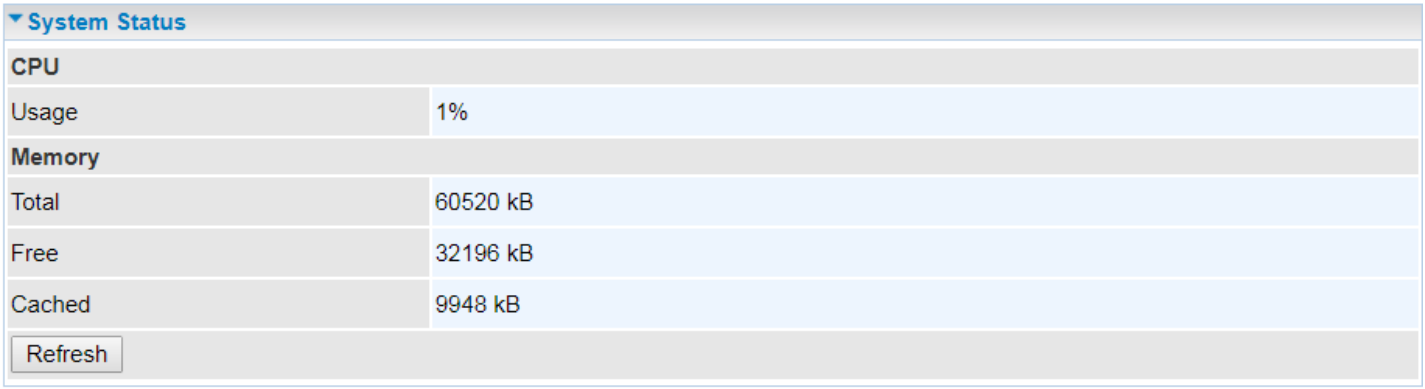
DHCP Server: Display LAN DHCP status of IPv4 and IPv6.

- **Enable / 192.168.1.100~199**: DHCPv4 server status on or off / DHCP IP range
- **Enable / Stateless**: DHCPv6 server status on or off / DHCPv6 server Type

- **Wireless**
- **Mode:** Display selected Wi-Fi mode.
- **SSID:** Display the name of the Wi-Fi AP(s) to use
- **Channel:** Display radio frequency to be used for this wireless link
- **Security:** Display security method to be used for this wireless link

System Status

Display device CPU and memory usage information



CPU

Usage: Display the amount of CPU's processing capacity is being used in percentage (%). Higher the % rate may result in slow Internet loading, experiencing video lags, etc. To reduce high CPU consumption by resetting the device, power off and on, an easiest way to regain the service.

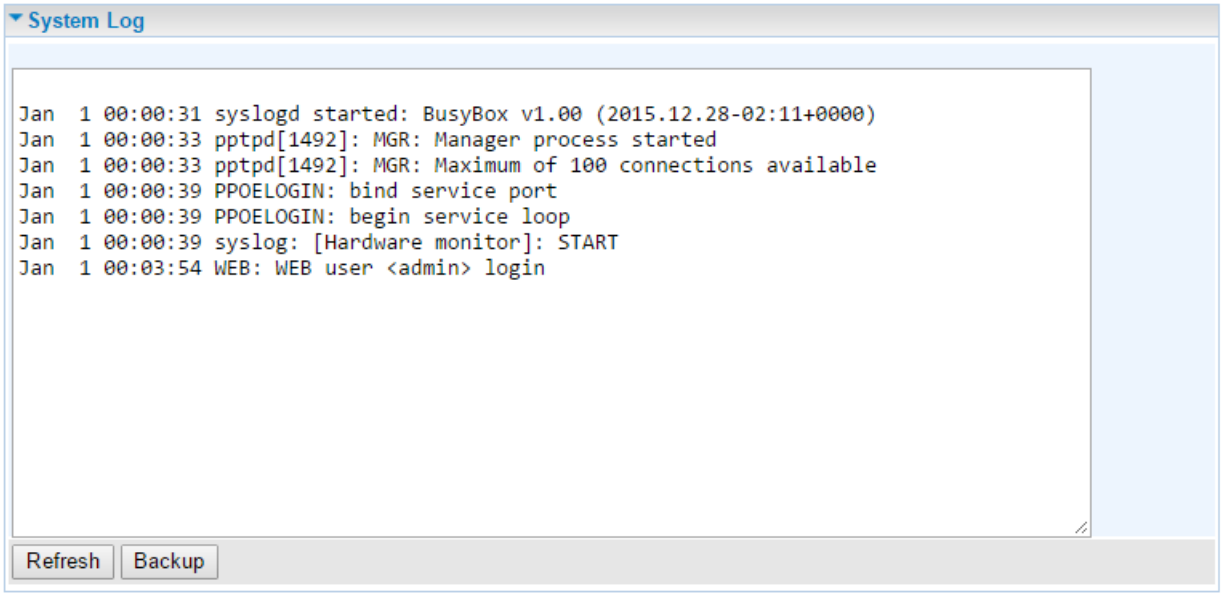
Memory

Total / Free / Cached (in Kbyte): Display the memory consumptions in kilobytes (kB).

Click **Refresh** button to update the status.

System Log

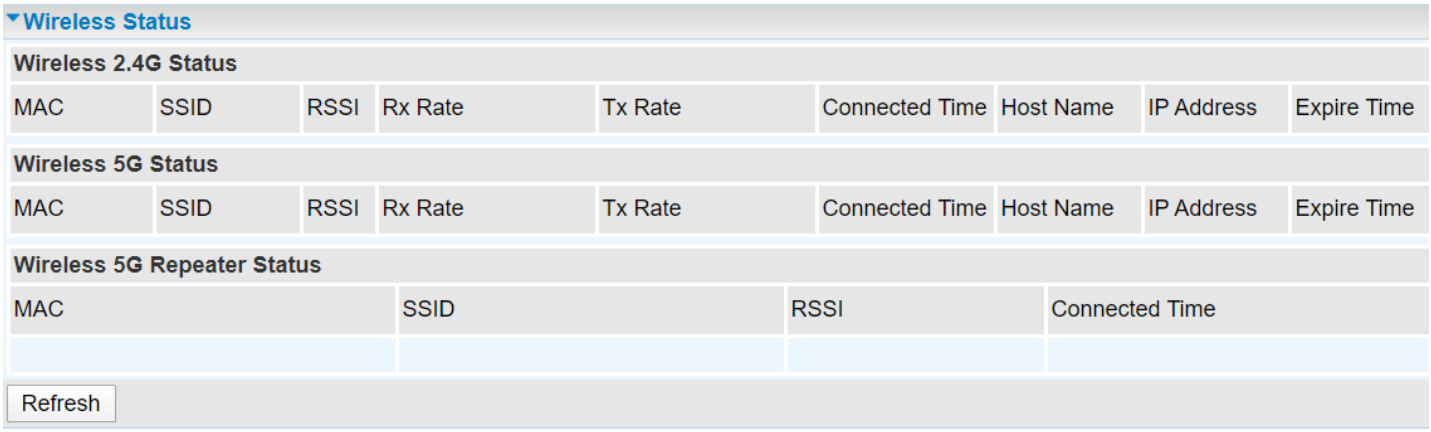
In system log, you can check the operations status and any glitches to the router.



Refresh: Press this button to refresh the statistics.

Backup: Press to save the System log, log.cfg, to your computer / notebook.

Wireless Status



MAC: The MAC of the connected wireless device.

SSID: Display the total bytes transmitted till the latest second for the current connection for the current connection.

RSSI: Display the signal strength between the wireless client and the AP (Access Point)

Connected Time: Display the total amount of time the wireless client has connected with the wireless AP

Host Name: Display the hostname of the Wi-Fi client.

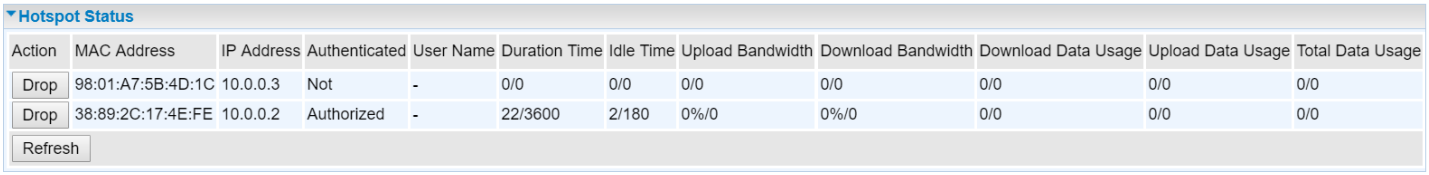
IP Address: The LAN IP address assigned to the wireless device.

Expire Time: Display remaining time before connection expires or timeout.

Click **Refresh** button to update the status.

Hotspot Status

The status table displays a list of connected Wi-Fi clients via the hotspot. .



Action: Click **Drop** to discount the user connection to the Wi-Fi network.

MAC Address: The MAC of the connected wireless device.

IP Address: The LAN IP address assigned to the wireless device.

Authentication: Identification of the wireless device is being authorized or not.

Username: The authentication username used to login to the hotspot. Go to Built-in User Account for detailed login account list.

Duration Time (remaining time / available session time interval): Display remaining interval available before session expires/timeout.

Idle Time (current idle time / total idle timeout period): Display current idle time of the Wi-Fi device.

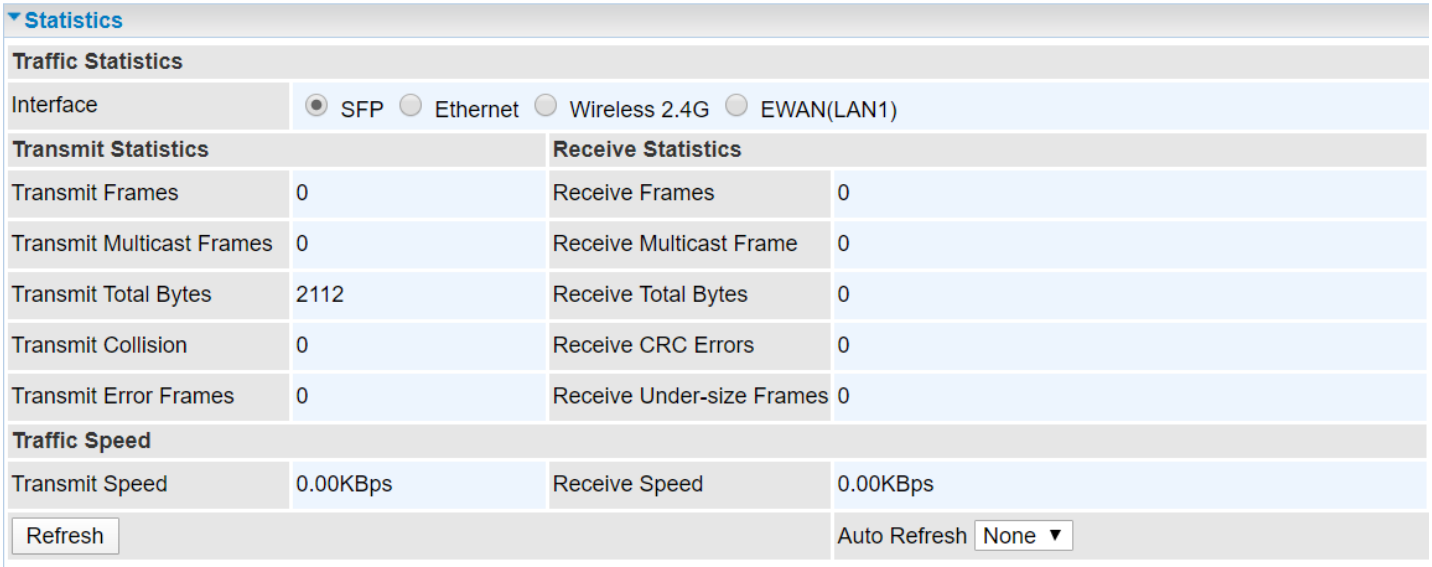
If it reaches to total idle timeout period, the Internet connection will get disconnected immediately.

Upload / Download (used / available bandwidth in %): Display current used bandwidths, in upload and download, out of the maximum allow usage in %.

Total Data Usage: Display total data usage of the Wi-Fi user.

Statistics

❖ SFP



Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **SFP (Small Form-Factor Pluggable) Fiber** port**.**

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Multicast Frames: Display the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: Display the number of bytes transmitted until the latest second.

Transmit Collision: Numbers of collisions have occurred on this port.

Transmit Error Frames: Display the number of error packets on this port.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Multicast Frames: Display the number of multicast frames received until the latest second.

Receive Total Bytes: Display the number of bytes received until the latest second.

Receive CRC Errors: Display the number of error packets on this port.

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

Traffic Speed

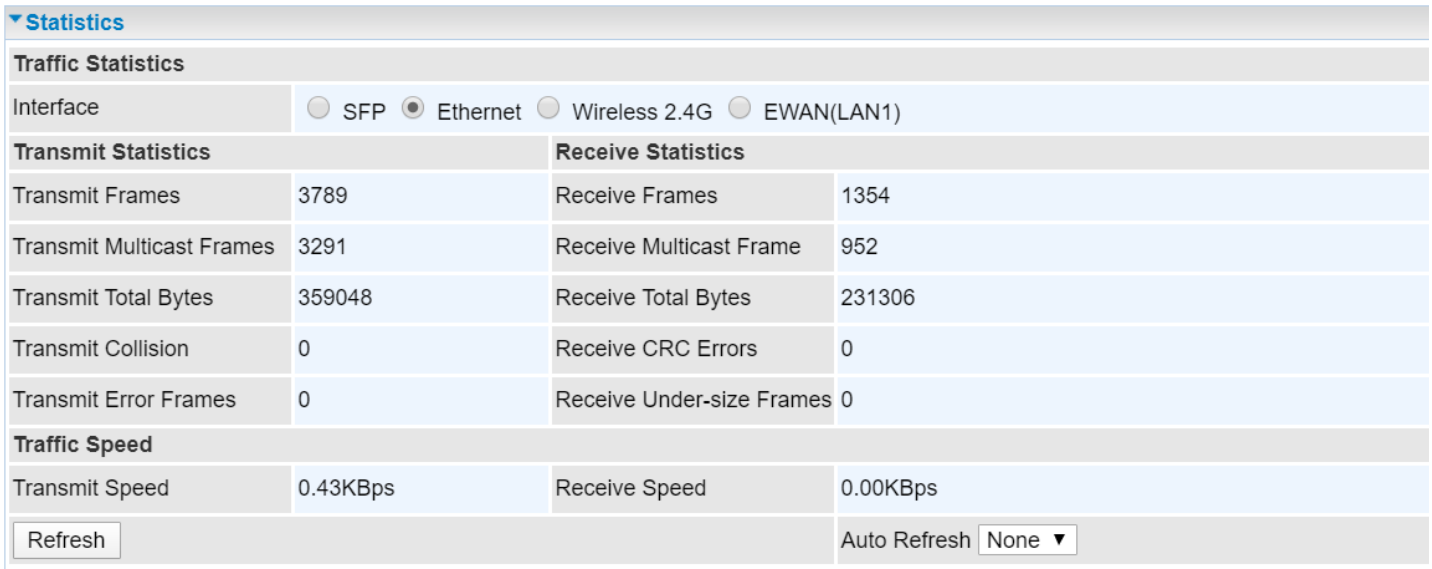
Transmit Speed: Display the data rate can be transferred to the server, the Broadband Internet Service Provider.

Receive Speed: Display the data rate receives from the Broadband Internet Service Provider.

Refresh: Click to manually refresh the data.

Auto Refresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ Ethernet



Traffic Statistics

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

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Multicast Frames: Display the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: Display the number of bytes transmitted until the latest second.

Transmit Collision: Numbers of collisions have occurred on this port.

Transmit Error Frames: Display the number of error packets on this port.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Multicast Frames: Display the number of multicast frames received until the latest second.

Receive Total Bytes: Display the number of bytes received until the latest second.

Receive CRC Errors: Display the number of error packets on this port.

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

Traffic Speed

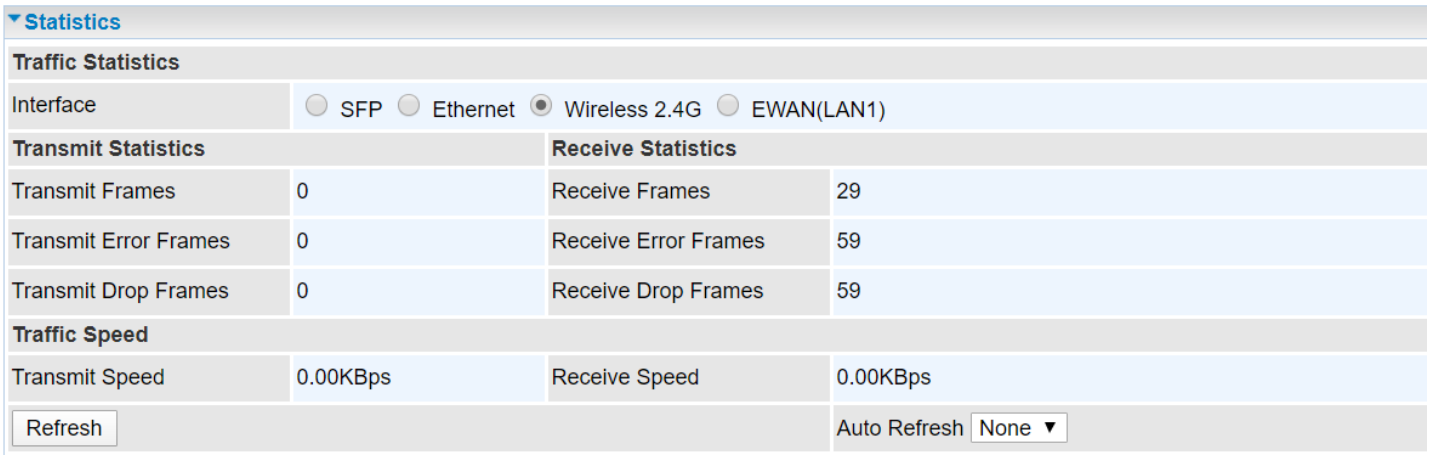
Transmit Speed: Display the data rate can be transferred to the server, the LAN network.

Receive Speed: Display the data rate receives from the LAN network.

Refresh: Click to manually refresh the data.

Auto Refresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ Wireless 2.4G/5G



Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **Wireless 2.4G/5G.**

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Error Frames: Display the number of error frames transmitted until the latest second.

Transmit Drop Frames: Display the number of drop frames transmitted until the latest second.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Error Frames: Display the number of error frames received until the latest second.

Receive Drop Frames: Display the number of drop frames received until the latest second.

Traffic Speed

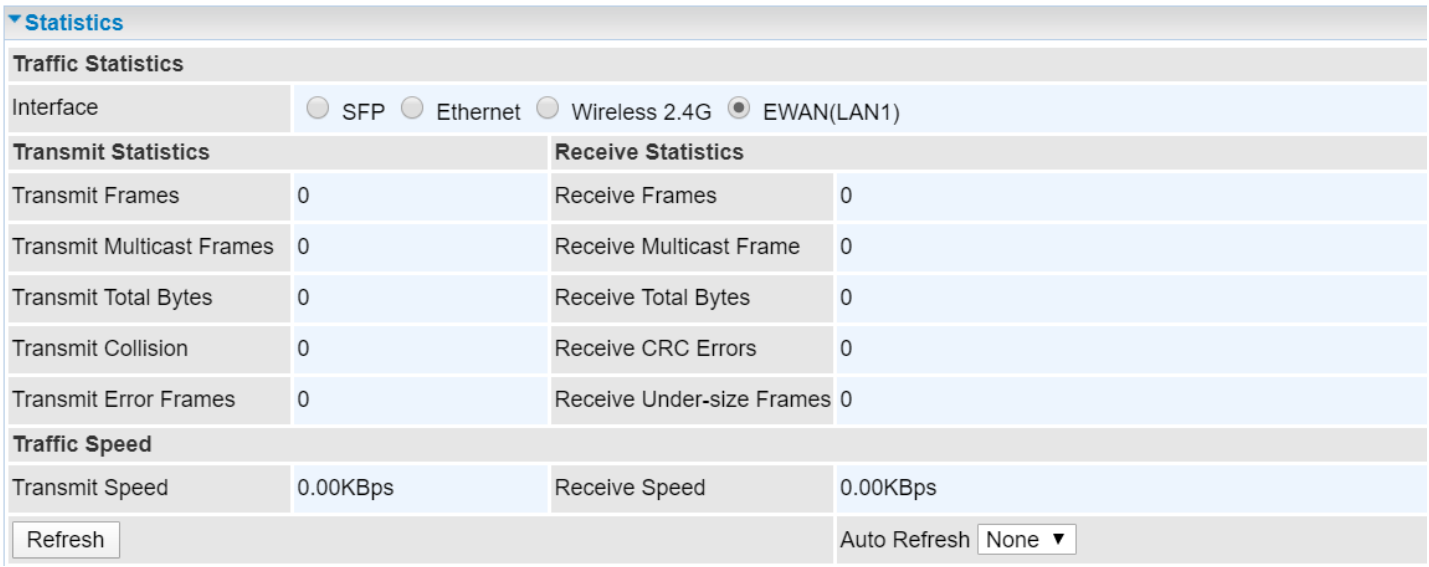
Transmit Speed: Display the data rate can be transferred to the server, the Wireless AP.

Receive Speed: Display the data rate receives from the Wireless AP.

Refresh: Click to manually refresh the data.

Auto Refresh: Select a time interval to refresh the data automatically or none to disable the feature.

❖ Ethernet WAN (LAN1)



Traffic Statistics

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **ETH WAN (Ethernet #1)** port**.**

Transmit Statistics

Transmit Frames: Display the number of frames transmitted until the latest second.

Transmit Multicast Frames: Display the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: Display the number of bytes transmitted until the latest second.

Transmit Collision: Numbers of collisions have occurred on this port.

Transmit Error Frames: Display the number of error packets on this port.

Receive Statistics

Receive Frames: Display the number of frames received until the latest second.

Receive Multicast Frames: Display the number of multicast frames received until the latest second.

Receive Total Bytes: Display the number of bytes received until the latest second.

Receive CRC Errors: Display the number of error packets on this port.

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

Traffic Speed

Transmit Speed: Display the data rate can be transferred to the server, the Broadband Internet Service Provider.

Receive Speed: Display the data rate receives from the Broadband Internet Service Provider.

Refresh: Click to manually refresh the data.

Auto Refresh: Select a time interval to refresh the data automatically or none to disable the feature.

DHCP Table

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

DHCP Table

Index	Host Name	IP	MAC Address	Expire Time
1	DESKTOP-PPUSERT	192.168.1.100	[redacted]09	0days 22:29:22

Index #: The numeric indicator for devices using dynamic IP addresses.

Host Name: Display 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

IPSec Status

Index	Action	Connection Name	Active	Connection State	Statistics	Remote Gateway	Remote Network	Local Network
0	Connect / Drop	H-to-B	Yes	Phase1 Established Phase2 Established	191408/43308	69.121.1.30	192.168.0.0/24	192.168.1.0/24

Refresh

Index #: The numeric IPSec VPN tunnel/ rule.

Action: Display Connect or Drop the connection.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display statuses of IPSec phase 1 and phase 2 connections.

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

Remote Gateway: Display remote gateway IP address.

Remote Network: Display remote local IP address and Netmask.

Local Network: Display local IP address and Netmask.

Refresh: Click to refresh the page.

PPTP Status

❖ PPTP Server

PPTP Status

PPTP Server						
Index	Connection Name	Active	Connection State	Connection Type	Assigned IP Address	Remote Network
1	HS-LL	Yes	Yes	Lan to Lan	192.168.1.2	192.168.0.0 / 255.255.255.0
PPTP Client						
Index	Connection Name	Active	Connection State	Connection Type	Server IP Address	Remote Network

Refresh

Index #: The numeric PPTP VPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display the VPN connection status.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

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

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

Refresh: Click to refresh the page.

❖ PPTP Client

PPTP Status

PPTP Server						
Index	Connection Name	Active	Connection State	Connection Type	Assigned IP Address	Remote Network
PPTP Client						
Index	Connection Name	Active	Connection State	Connection Type	Server IP Address	Remote Network
1	BC-LL	Yes	Yes	Lan to Lan	69.121.1.33	192.168.1.0 / 255.255.255.0

Refresh

Index #: The numeric PPTP VPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display Yes/No to indicate the VPN connection status.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

Server IP Address: Display the WAN IP address of remote PPTP Server.

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

Refresh: Click to refresh the page.

L2TP Status


L2TP Status

Index	Connection Name	Active	Connection State	Connection Mode	Connection Type	Tunnel Remote IP Address
1	HS-LL	Yes	Connected	Dial in	Lan to Lan	192.168.1.200

Refresh

Index #: The numeric L2TP VPN tunnel/rule indicator.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

Connection State: Display Yes/No to indicate the VPN connection status.

Connection Mode: Display if L2TP mode is a dial-in or dial-out.

Connection Type: Display if VPN connection is for single PC use (Remote Access) or multi-user use (LAN to LAN).

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

Refresh: Click to refresh the page.

GRE Status


GRE Status

Index	Connection Name	Active	Connection State	Remote Gateway IP	Remote Network
1	GRE-0	Yes	Connected	69.121.1.30	192.168.0.0/255.255.255.0

Index #: The numerical GRE tunnel/rule indication.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

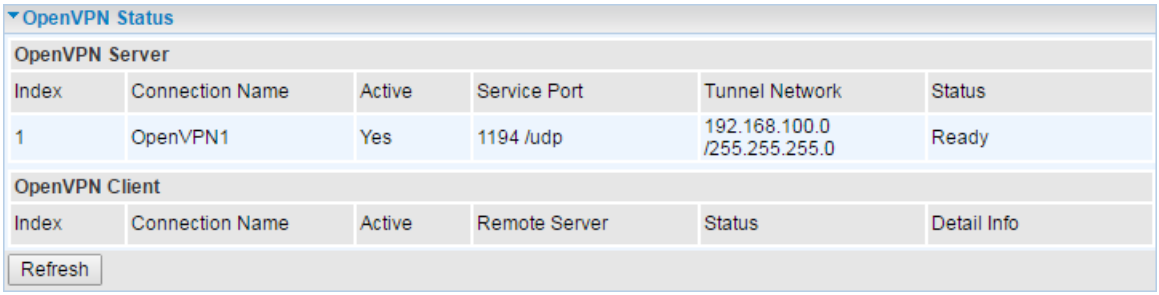
Connection State: Display Yes/No to indicate the VPN connection status.

Remote Gateway IP: Display the remote gateway IP address.

Remote Network: Display the remote local network IP address / Netmask.

OpenVPN Status

❖ OpenVPN Server


OpenVPN Status

OpenVPN Server

Index	Connection Name	Active	Service Port	Tunnel Network	Status
1	OpenVPN1	Yes	1194 /udp	192.168.100.0 /255.255.255.0	Ready

OpenVPN Client

Index	Connection Name	Active	Remote Server	Status	Detail Info

Refresh

Index #: The numeric OpenVPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

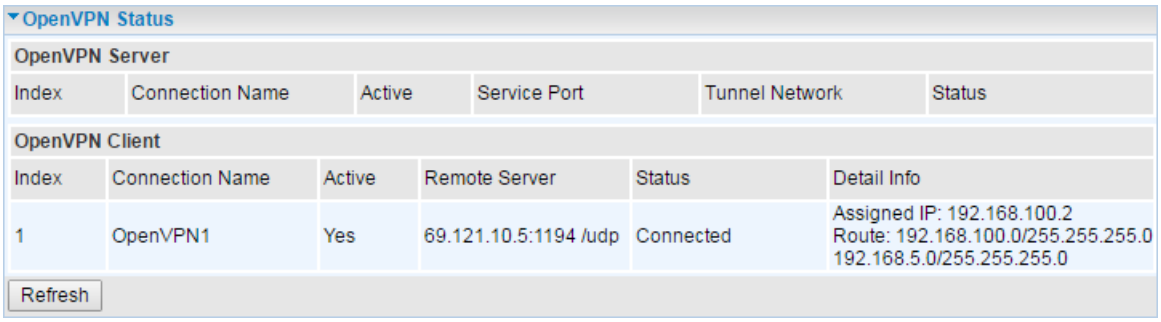
Service Port: Display the port/protocol (1194/udp) used for OpenVPN connection.

Tunnel Network: Display the virtual tunnel IP address and Netmask of the OpenVPN server.

Status: Display the status of the profile/rule

Refresh: Click to refresh the page.

❖ OpenVPN Client


OpenVPN Status

OpenVPN Server

Index	Connection Name	Active	Service Port	Tunnel Network	Status

OpenVPN Client

Index	Connection Name	Active	Remote Server	Status	Detail Info
1	OpenVPN1	Yes	69.121.10.5:1194 /udp	Connected	Assigned IP: 192.168.100.2 Route: 192.168.100.0/255.255.255.0 192.168.5.0/255.255.255.0

Refresh

Index #: The numeric OpenVPN tunnel/ rule.

Connection Name: The profile name of the VPN connection/tunnel.

Active: Display Yes or No to indicate the profile is enabled or disabled.

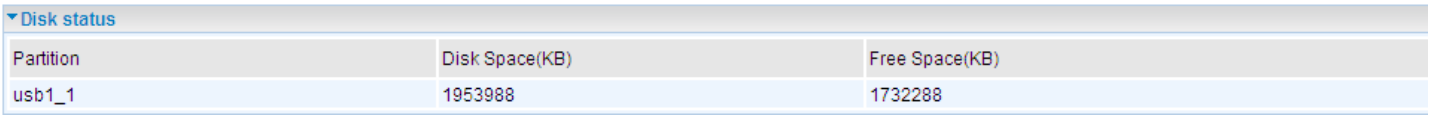
Remote Server: Display the remote server public IP address and used port/protocol for this connection.

Status: Display the status of the profile/rule

Detailed Info: Display detailed IP assignment and routing information of this VPN connection.

Refresh: Click to refresh the page.

Disk Status



Partition: Display the USB storage partition.

Disk Space (KB): Display the total storage space of the NAS in Kbytes unit.

Free Space (KB): Display the available space in Kbytes unit.

VoIP Status

❖ VoIP Status

VoIP status gives you a directive picture on the registered VoIP accounts.

Phone Number: The number you use to register in the Basic page of VoIP.

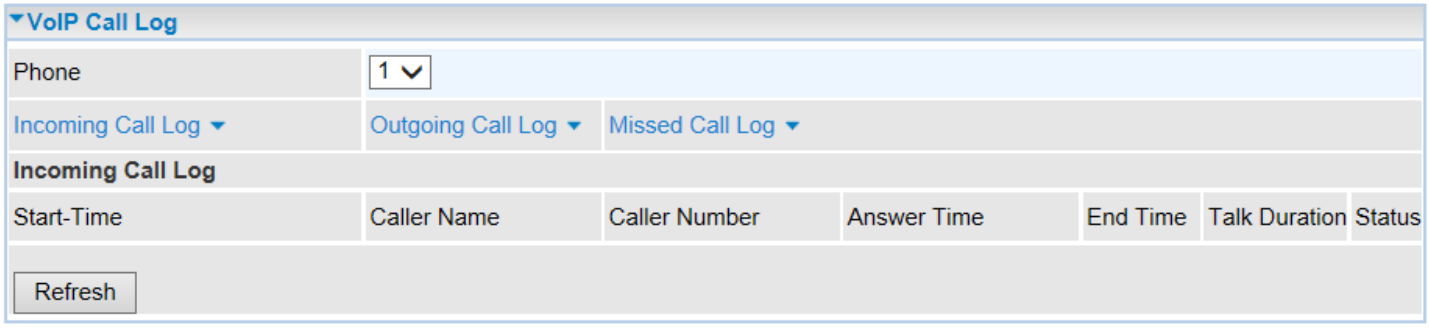
Host: Show the IP address and port number of SIP Registrar.

Status: The status of the registered SIP account.

Registered Time: The duration the account has been successfully registered to the SIP registrar.

❖ VoIP Call Log

VoIP call log records all inbound / outbound calls in detail within your VoIP accounts. You can quickly view the call date, time, incoming/outgoing/missed call telephone number, and more.



Phone Number: The number you use to register in the Basic page of VoIP.

Incoming / Outgoing / Miss Call Log: Click the call log you want to view.

Start-Time: The start time of the call

Caller/Called Name: Display the caller ID of the dialing party / the party you dialed to reach to.

Caller/Called Number: Display caller telephone number / telephone number you dialed to reach to

Answer Time: The answer time of phone call

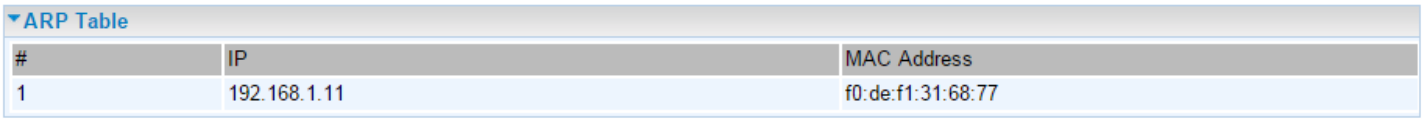
End Time: The end time of the call

Talk Duration: Time duration of individual calls from dial/call to hang-up.

Status: Current call status if phones are off hook or in a call.

ARP Table

ARP (Address Resolution Protocol) table displays a mapping IP address with a PC's MAC address.


ARP Table

#	IP	MAC Address
1	192.168.1.11	f0:de:f1:31:68:77

#: The numeric table list indicator.

IP Address: It is the internal/local IP address to access to the network.

MAC Address: The MAC address of a device, e.g. PC, notebook, printer, etc., that is corresponded with the IP address.

VRRP Status


VRRP Status

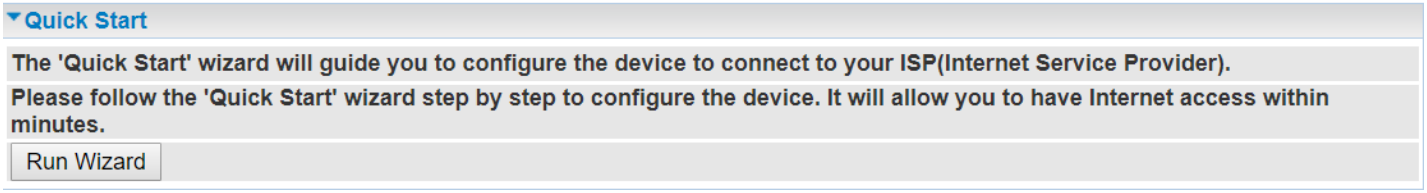
Current Status	N/A
Current Master	N/A

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

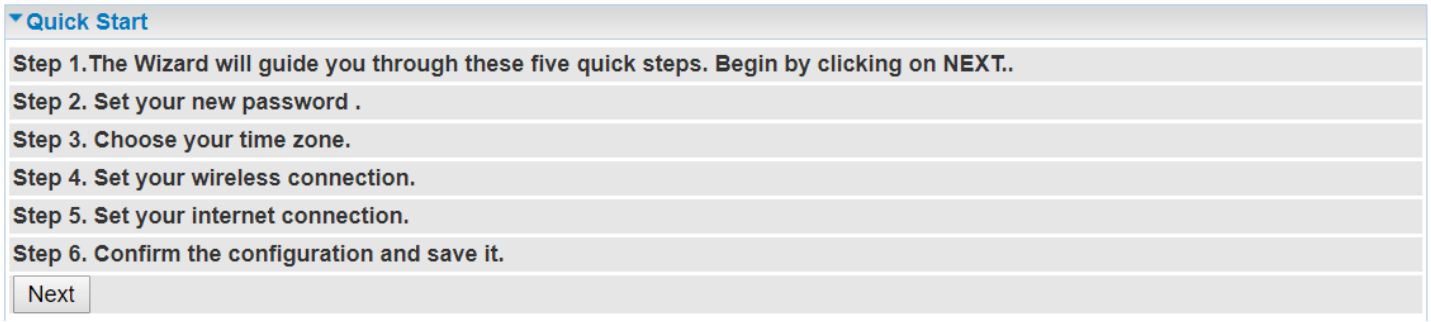
Current Master: Display the IP address of the Master

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.



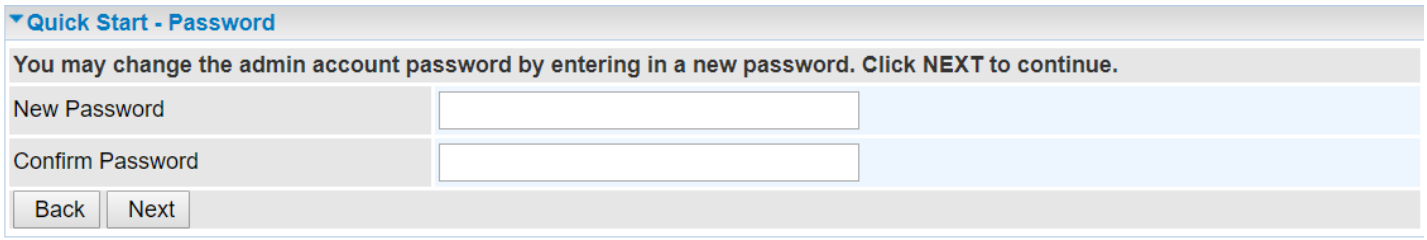
For detailed instructions on configuring WAN settings, see refer to the **Interface Setup** section.



Click **NEXT** to move on to Step 2.

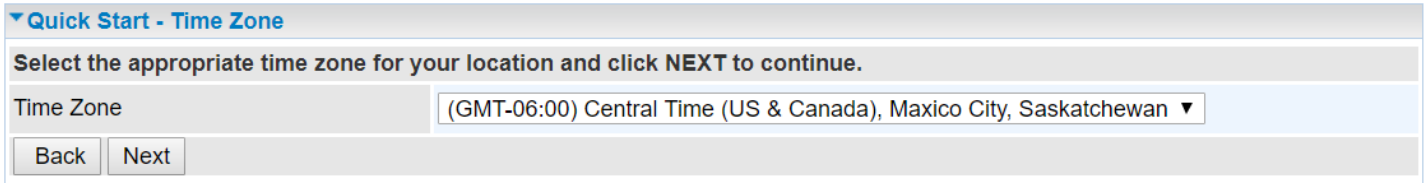
Step 2 – Password

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.



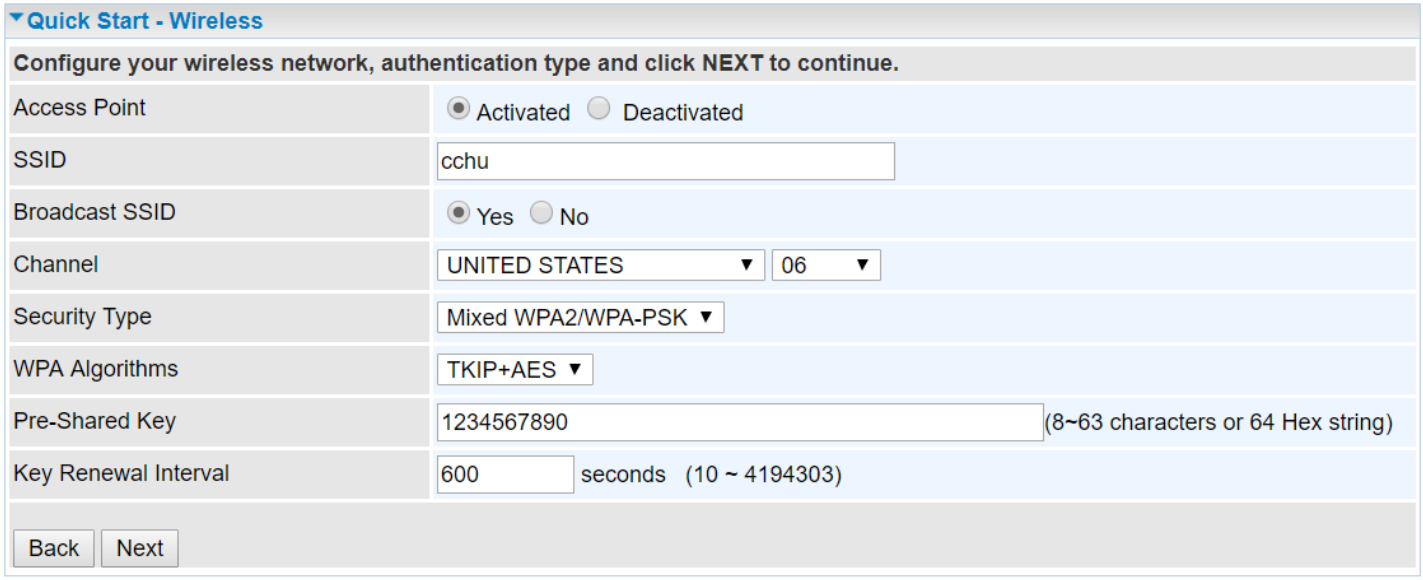
Step 3 – Time Zone

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



Step 4 – Wireless

Set up your wireless connection if you want to connect to the Internet wirelessly on your PCs. Click **NEXT** to continue.



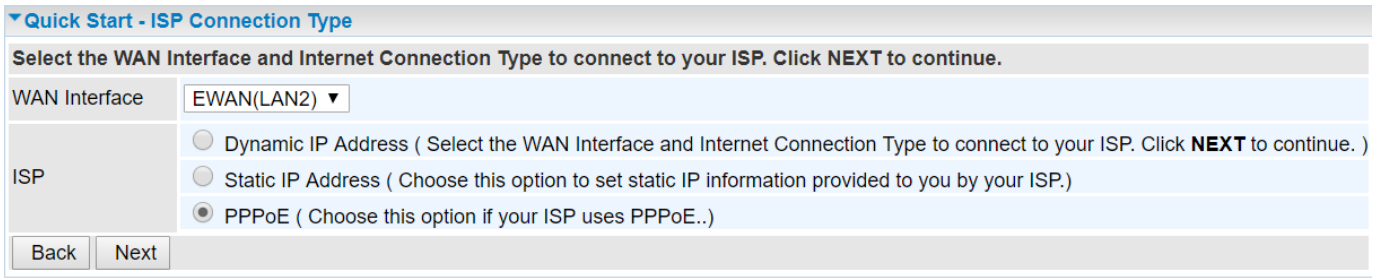
Step 5 – ISP Connection Type

Set up your Internet connection.

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

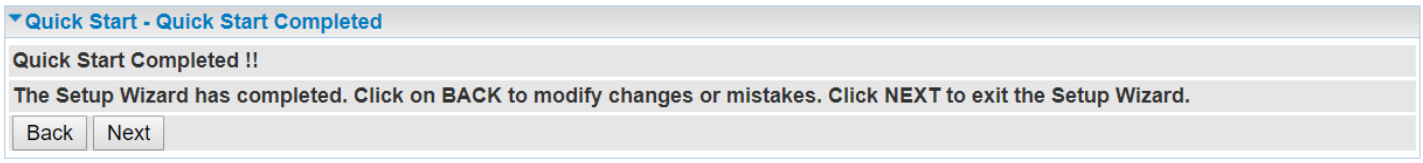
If selected **Static IP** or **PPPoE**, enter the static IP address or PPPoE account information provided by your ISP.

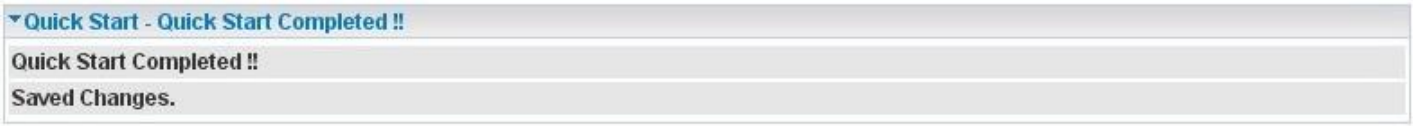
Click **NEXT** to continue.



Step 6 – Quick Start Completed

The Setup Wizard has completed. Click on BACK to make changes or correct mistakes. Click **NEXT** to save the current settings and complete the Quick Start setups.





Go back to the **Status > Device Info** to view the status.

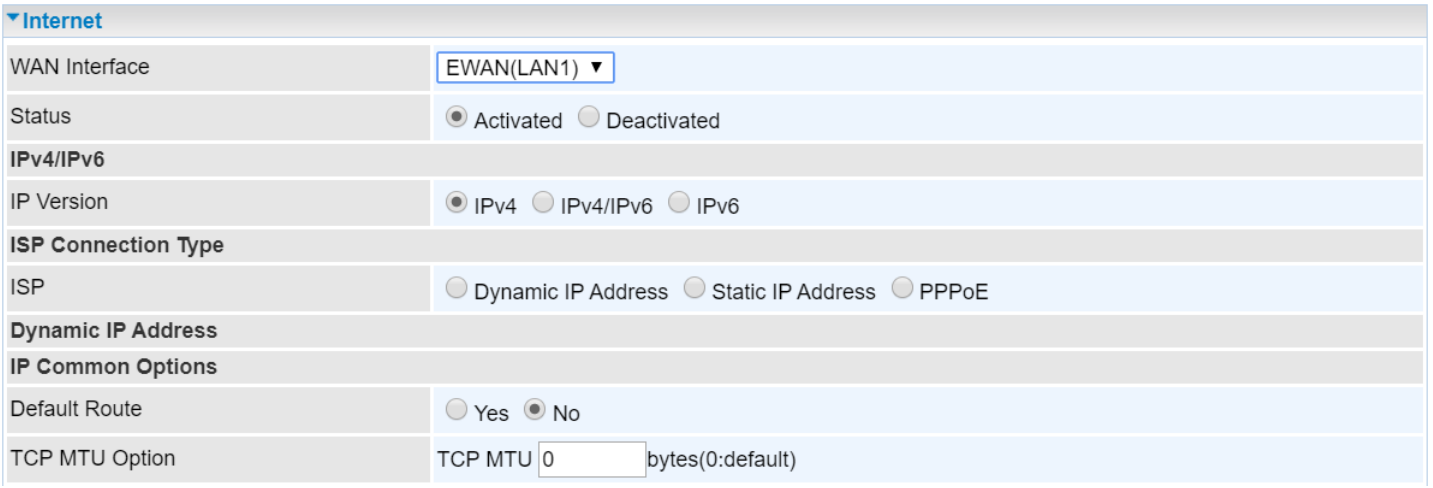
Device Configuration

Interface Setup

Here are the features in **Interface Setup:** Internet, LAN, Wireless 2.4G/5G, Wireless MAC Filter and Loopback

Internet

❖ EWAN (LAN 1) or SPF



Status: Select to enable/activate or disable/deactivated the service.

IPv4/IPv6

IP Version: Choose **IPv4, IPv4/IPv6, IPv6** based on your environment. If you don't know which one to choose from, please choose IPv4/IPv6 instead.

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

- **Dynamic IP:** Select this option if your ISP provides you an IP address automatically.
- **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form. IP address from by four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.
- **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.

PPPoE (If selected PPPoE as WAN Connection Type; otherwise, skip this part)

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Bridge Interface for PPPoE: When "Activated", the device will gain WAN IP from your ISP with the

PPPoE account. But if your PC is connected to the router working as a DHCP client, in this mode, the device acts as a NAT router; while if you dial up with the account within your PC, the device will then work as a bridge forwarding the PPPoE information to the PPPoE server and send the response to your PC, thus your PC gets a WAN IP working in the internet.

Connection Setting (If selected PPPoE)

Connection:

- **Always On:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Connect Manually:** Select Connect Manually when you don't want the connection up all the time.

TCP MSS Option: Enter the maximum size of the data that TCP can send in a segment. Maximum Segment Size (MSS).

802.1q Options

802.1q Options	
802.1q	○ Activated ◉ Deactivated
VLAN ID	0 (range: 0~4095)

802.1q: When activated, please enter a VLAN ID.

VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4095.

IP Common Options

IP Common Options

IP Common Options	
Default Route	◉ Yes ○ No
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)

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

TCP MTU Option: Enter the maximum packet that can be transmitted. Default MTU **0** means it is set to 1492 bytes.

IPv4 Options (Dynamic IP Address)

IPv4 Options	
NAT	Enable ▼
Client ID	
Vendor ID	
Dynamic Route	RIP1 ▼ Direction None ▼
IGMP Proxy	○ Enable ◉ Disable

NAT: Enable to allow 9900VA to assign private network IPs to all devices in the network for get Internet

access.

Client ID: It is known as DHCP Option 61. Enter the client identifier from your ISP.

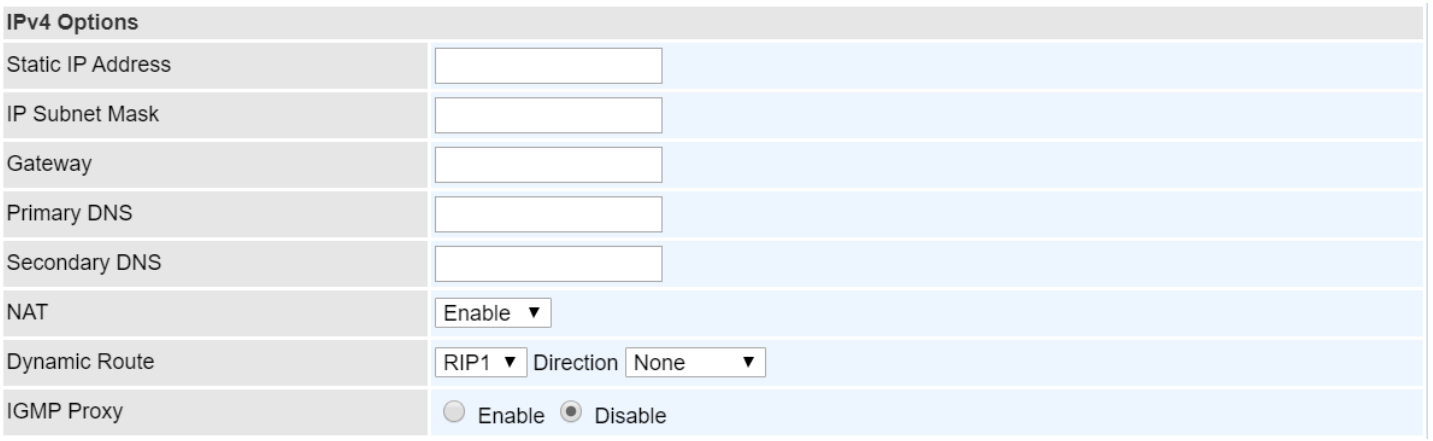
Vendor ID: It is known as DHCP Option 60. Enter the vendor identifier from your ISP.

Dynamic Route

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2.
- **RIP Direction:** Select this option to specify the RIP direction.
  - **None** is for disabling the RIP function.
  - **Both** means the router will periodically send routing information and accept routing information then incorporate into routing table.
  - **IN only** means the router will only accept but will not send RIP packet.
  - **OUT only** means the router will only send but will not accept RIP packet

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. Choose whether enable IGMP proxy.

IPv4 Options (Static IP Address)



Static IP Address: If **Static** is selected in the above field, please enter the specific IP address you get from ISP and the following IP subnet mask and gateway address.

IP Subnet Mask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the specific gateway IP address you get from ISP.

Primary / 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.

NAT: Enable to allow 9900VA to assign private network IPs to all devices in the network for get Internet access.

Dynamic Route

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2.
- **RIP Direction:** Select this option to specify the RIP direction.
  - **None** is for disabling the RIP function.

- **Both** means the router will periodically send routing information and accept routing information then incorporate into routing table.
- **IN only** means the router will only accept but will not send RIP packet.
- **OUT only** means the router will only send but will not accept RIP packet.

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. Choose whether enable IGMP proxy.

IPv4 Options (PPPoE)

IPv4 Options	
Get IP Address	○ Static ◉ Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable ▼
Dynamic Route	RIP1 ▼ Direction None ▼
IGMP Proxy	○ Enable ◉ Disable

Get IP Address: Choose Static or Dynamic

Static IP Address: If **Static** is selected in the above field, please enter the specific IP address you get from ISP and the following IP subnet mask and gateway address.

IP Subnet Mask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the specific gateway IP address you get from ISP.

NAT: Enable to allow 9900VA to assign private network IPs to all devices in the network for get Internet access.

Dynamic Route

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2.
- **RIP Direction:** Select this option to specify the RIP direction.
  - **None** is for disabling the RIP function.
  - **Both** means the router will periodically send routing information and accept routing information then incorporate into routing table.
  - **IN only** means the router will only accept but will not send RIP packet.
  - **OUT only** means the router will only send but will not accept RIP packet.

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. Choose whether enable IGMP proxy.

IPv6 options (only when choose IPv4/IPv6 or just IPv6 in IP version field above):

IPv6 Options	
IPv6 Address	/
Obtain IPv6 DNS	Enable Disable
Primary DNS	
Secondary DNS	
MLD Proxy	Enable Disable

IPv6 Address / Default Gateway: Enter the WAN IPv6 address and/or default gateway given by your ISP.

Obtain IPv6 DNS: Choose if you want to obtain DNS automatically.

Primary/Secondary: if you choose Disable in the Obtain IPv6 DNS field, please type the exactly primary and secondary DNS.

MLD Proxy: MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a Multicast Management protocol for IPv6 multicast packets.

When router's Internet configuration is finished successfully, you can go to status to get the connection information.

Click **Save** to apply settings.

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

IPv4 Parameters	
IP Address	192.168.1.254
IP Subnet Mask	255.255.255.0
Alias IP Address	0.0.0.0 (0.0.0.0 means to close the alias ip)
Alias IP Subnet Mask	0.0.0.0
Snooping	○ Activated ◉ Deactivated
Dynamic Route	RIP1 ▼ Direction None ▼

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.

IGMP Snooping: Select **Activated** to enable IGMP Snooping function. Without the IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic to be forwarded to all ports. With IGMP 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	
DHCPv4 Server	○ Disabled ◉ Enabled ○ Relay
Start IP Address	192.168.1.100
IP Pool Count	20
Lease Time	86400 seconds (0 sets to default value of 259200)
DNS Relay	◉ Automatically ○ Manually
Primary DNS	
Secondary DNS	
Option 66	
Option 160	

DHCPv4 Server: If set to **Enabled**, your 9900VA 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 9900VA 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.

DNS Relay

- Select **Automatic** detection or
- **Manually** specific Primary and Secondary DNS IP addresses

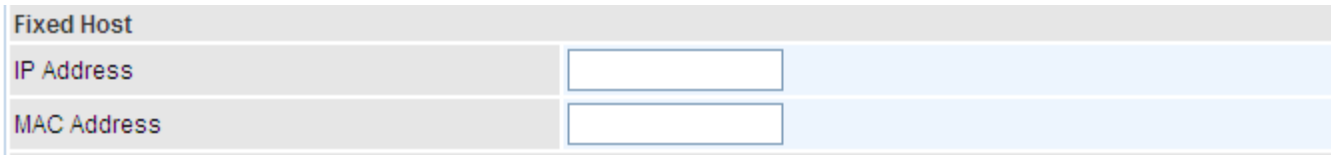
  Primary / Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Option 66: Set the IP or hostname of the TFTP server for devices, like IPTV Set Box, to get configuration settings from the TFTP server.

Option 160: Set the IP or hostname of the TFTP server for devices, like IPTV Set Box, to get configuration settings from the TFTP server. (The option 160 is an extended feature in DHCP option, similar to option 66, but using http or https protocols.)

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.



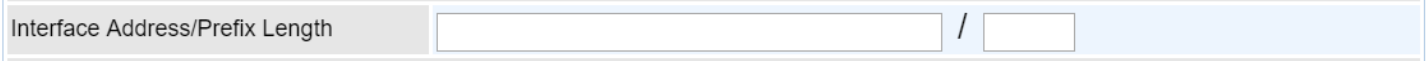
IP Address: Enter the specific IP. For example: 192.168.1.110.

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

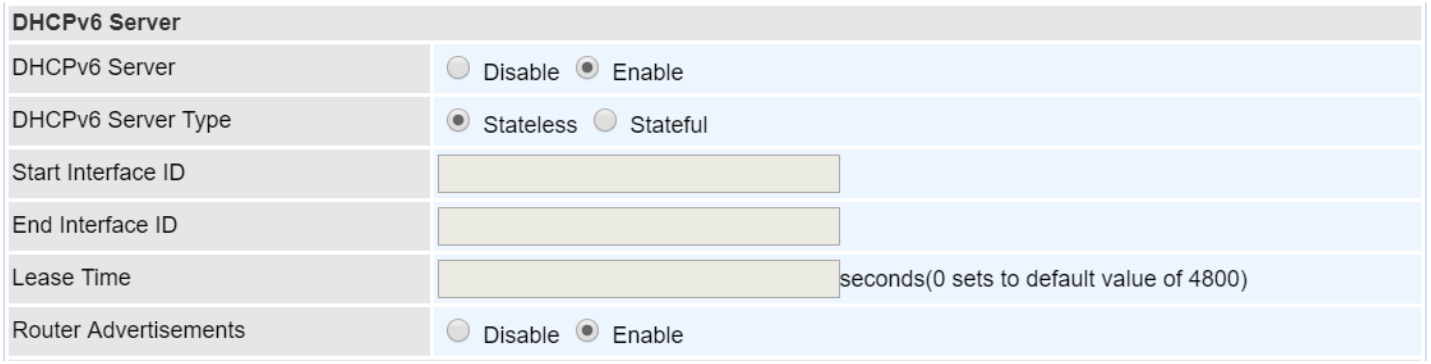
The IPv6 address composes of two parts, thus, the prefix and the interface ID.



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 (seconds): 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.

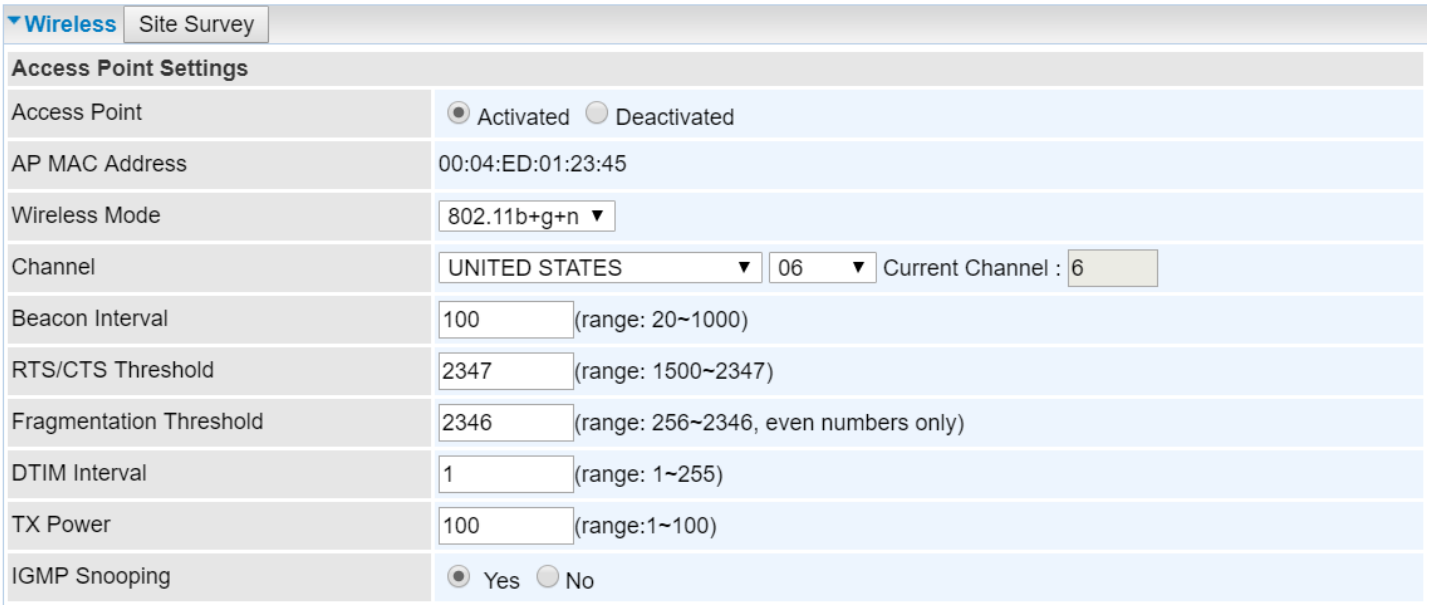
Click **Save** to apply settings

Wireless (2.4GHz & 5GHz)

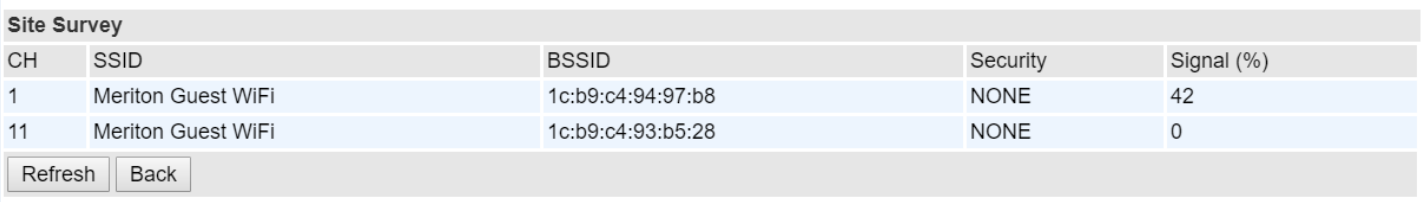
This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.

NOTE: WLAN1 / 2 / 3 / 4 Interface refers to as SSID1 / 2 / 3 / 4 Wi-Fi networks.

Access Point Settings



Site Survey: Click to view all other available Wireless-AP devices around the 9900VA.



- **CH (Channel)**: Channel ID used.
- **SSID**: The name of the wireless AP.
- **BSSID**: The MAC address of the wireless AP.
- **Security:** The security mode in the wireless AP.
- **Signal (%):** Signal strength of the wireless AP. Signal increases means the wireless AP is closer to your 9900VA and may cause interferences.

Access Point: Default setting is set to **Activated**. If you want to close the wireless interface, select **Deactivated.**

AP MAC Address: The MAC address of wireless AP.

Wireless Mode: The default setting is **802.11b+g+n** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b** and if you only have 802.11n then select **802.11n**.

Channel: The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a

channel. There are Regulation Domains and Channel ID in this field. The Channel ID will be different based on Regulation Domains. Select a channel from the drop-down list box.

Beacon interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request to Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Enter a value between 1500 and 2347.

Fragmentation Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346, even number only.

DTIM Interval: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

TX Power: The transmission power of the antennas, ranging from 1-100, the higher the more powerful of the transmission performance.

IGMP Snooping: Enable or disable the IGMP Snooping function for wireless. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

11n Settings

Channel Bandwidth: Select **20 MHz, 40 MHz,** or **20/40 MHz** for the channel bandwidth. The wider the Channel bandwidth the better the performance will be.

Extension Channel (20/40 MHz only): Select either **Auto** or **Above the control channel**.

Guard Interval: Select either **800nsec** or **Automatic** for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other. It also prevents propagation delays, echoing and reflections. The shorter the Guard Interval, the better the performance will be. We recommend users to select **Auto**.

MCS (Modulation and Coding Scheme): There are options **0~15** and **AUTO** to select from. **AUTO** is recommended.

SSID Settings

SSID Settings	
Available SSID	4 ▼
SSID Index	◉ SSID1 ○ SSID2 ○ SSID3 ○ SSID4
SSID	cchu
Broadcast SSID	◉ Yes ○ No
Clients Isolation	○ Yes ◉ No

Available SSID: User can determine how many virtual SSIDs to be used. Default is 1, maximum is 4.

SSID Index: Select the number of SSIDs you want to use; up to 4 SSIDs are available in the list.

- **SSID1 SSID** known as **wlan-ap1** Interface
- **SSID2** known as **wlan-ap2**Interface
- **SSID3** known as **wlan-ap3** Interface
- **SSID4** known as **wlan-ap4** Interface

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default SSID to a unique ID name to the AP which is already built-in to the router's wireless interface. Make sure your wireless clients have exactly the SSID as the device to get connected to your network.

Broadcast SSID: Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning. Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning.

Client Isolation: Enable by clicking **Yes** to prevent wireless clients communicating with other wireless clients.

WPS Settings

WPS Settings	
Use WPS	◉ Yes ○ No
WPS State	Configured
WPS Mode	○ PIN code ◉ PBC

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method (Personal Information Number)** & **PBC Method (Push Button Configuration)**.

Use WPS: Enable this feature by choosing the "YES" radio button.

WPS State: Display whether the WPS is **configured** or **unconfigured**.

WPS Mode: Select the mode which to start WPS, choose between **PIN Code** and **PBC** (Push Button). Selecting **Pin Code** mode will require you to know the enrollee PIN code.

To future understand the two modes of configuration; please refer to the example of the **Wi-Fi Protected Setup.**

Security Settings

Security Type: You can disable or enable wireless security for protecting wireless network. The default type of wireless security is OPEN and to allow all wireless stations to communicate with the access points without any data encryption.

To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP and WPA.

There are multiple security mode to select from: Open (no security), WEP 64-bit, WEP 128-bit, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. If you require high security for transmissions, please select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK.

WEP

Security Settings	
Security Type	WEP 64-bit ▼
WEP Authentication Method	Both ▼
WEP 64-bit	For each key, please enter either (1) 5 characters, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
Key #1	842CFFDE
Key #2	
Key #3	
Key #4	

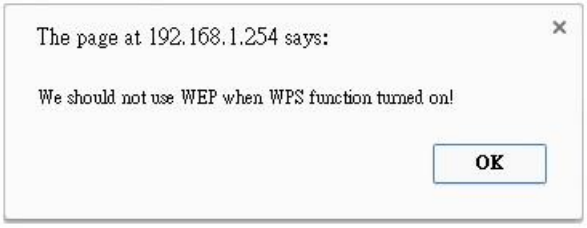
WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If chose **WEP 64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If chose **WEP 128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.



NOTE: WPS requires a higher level of security than WEP, 64bits or 128bits. Select WAP / WAP2 security when using WPS.

WPA-PSK / WPA2-PSK / Mixed WPA & WPA2

Security Settings	
Security Type	Mixed WPA2/WPA-PSK ▼
WPA Algorithms	TKIP+AES ▼
Pre-Shared Key	842CFFDE (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

Pre-Shared key: The key for network authentication. The input format should be 8-63 ASCII characters or 64 hexadecimal characters

Key Renewal Interval: The time interval for changing the security key automatically between wireless client and AP.

WDS Settings

WDS (Wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, just define the peer's MAC of the connected AP.

WDS Mode: select Activated to enable WDS feature and Deactivated to disable this feature.

MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.

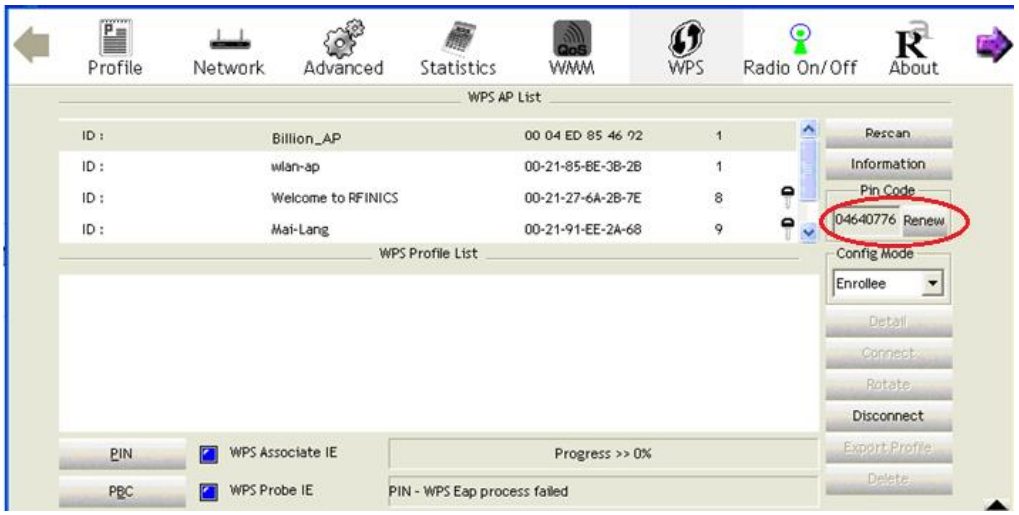
WDS Settings	
AP MAC Address	00:04:ED:01:23:45
WDS Mode	○ Activated ◉ Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00
Save	

Click **Save** to apply the settings.

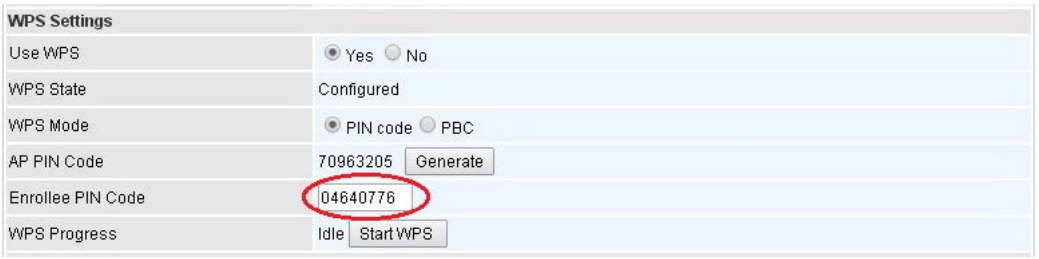
Example: WPS using PIN Method (Personal Information Number)

PIN Method – Configure 9900VA as a Registrar

1. Jot down the client's Pin (e.g. 04640776) from the WPS utility (e.g. Ralink Utility)

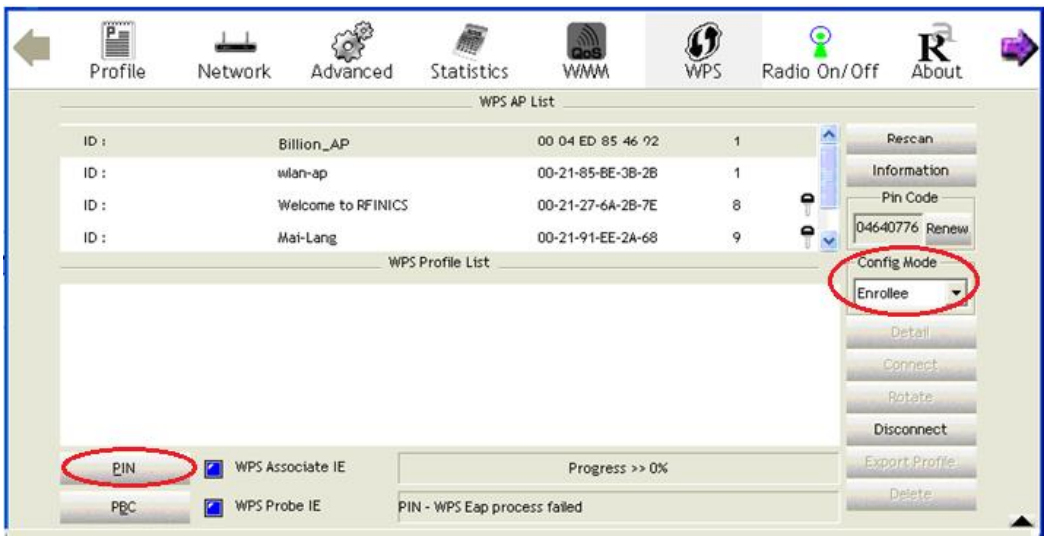


2. Enter the Enrollee (Client) PIN code and then press **Start WPS**.

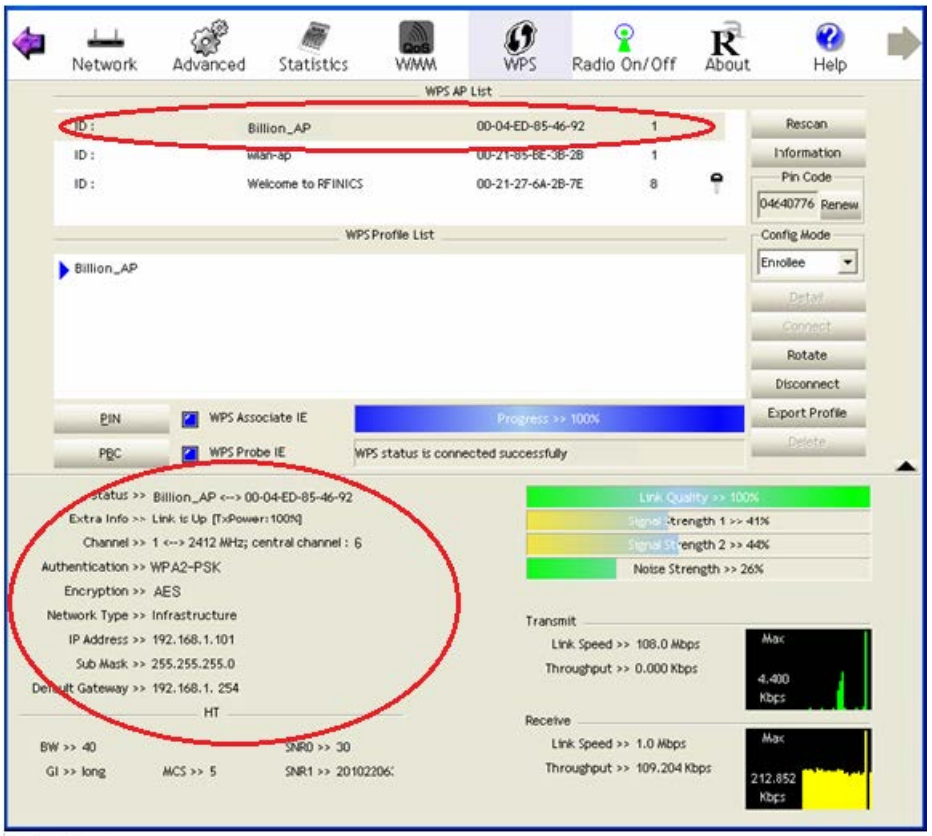


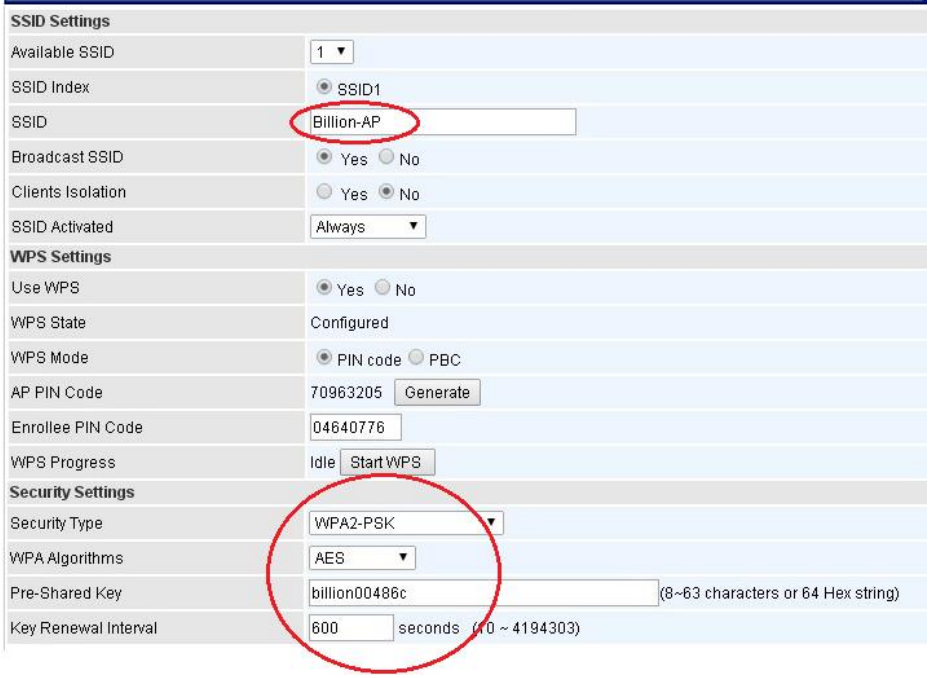
3. Go back to the wireless client's WPS utility (e.g. Ralink Utility).

Set the Config Mode as **Enrollee**, press the WPS button on the top bar, select the AP (e.g. Billion_AP) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



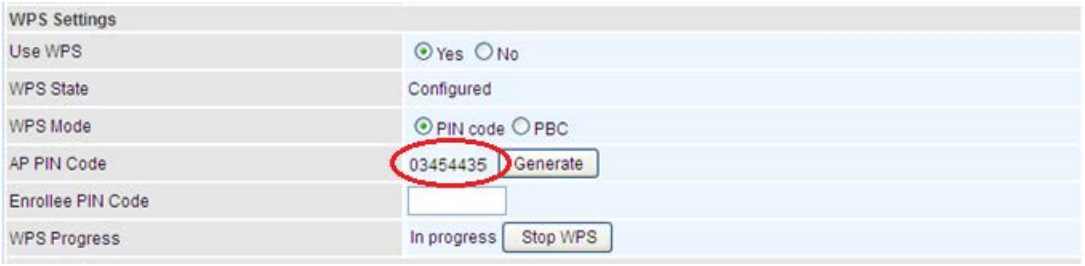
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar, the 9900VA router.



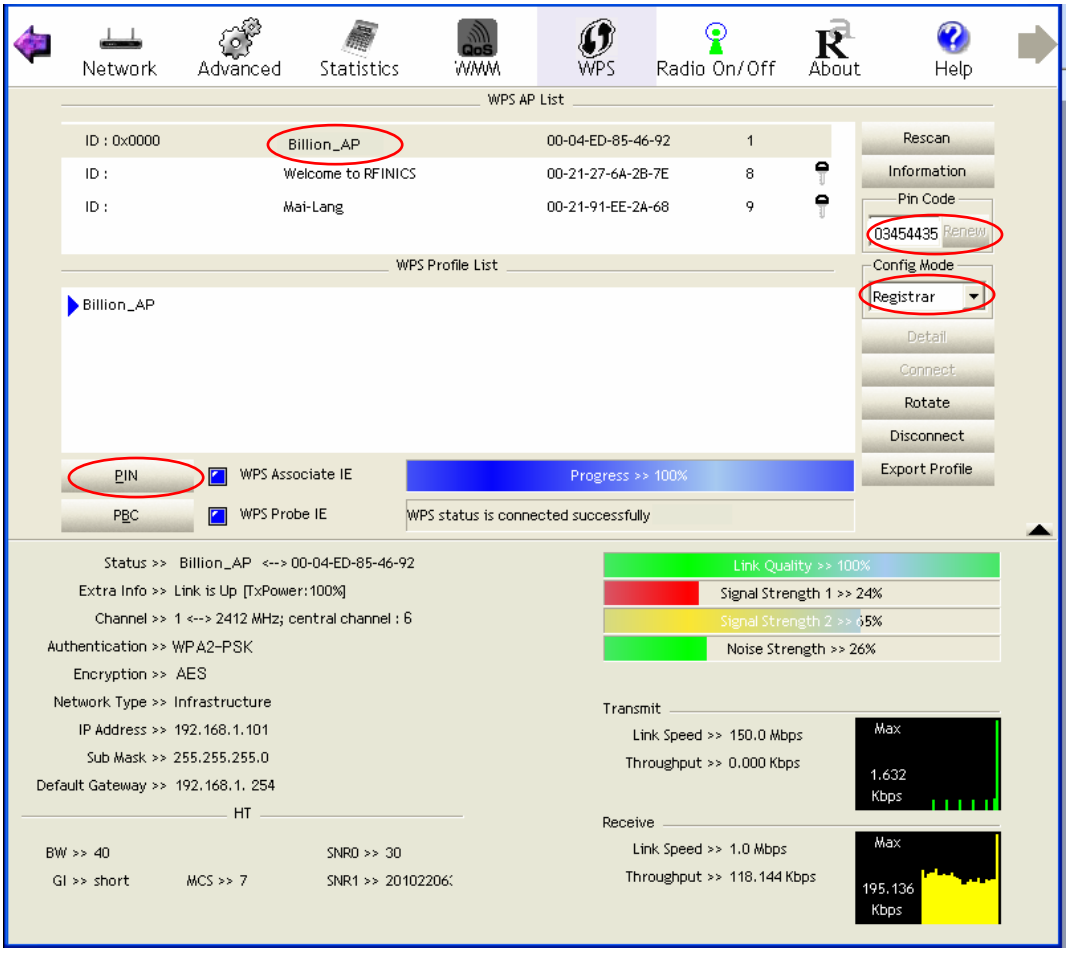


PIN Method – Configure 9900VA as an Enrollee

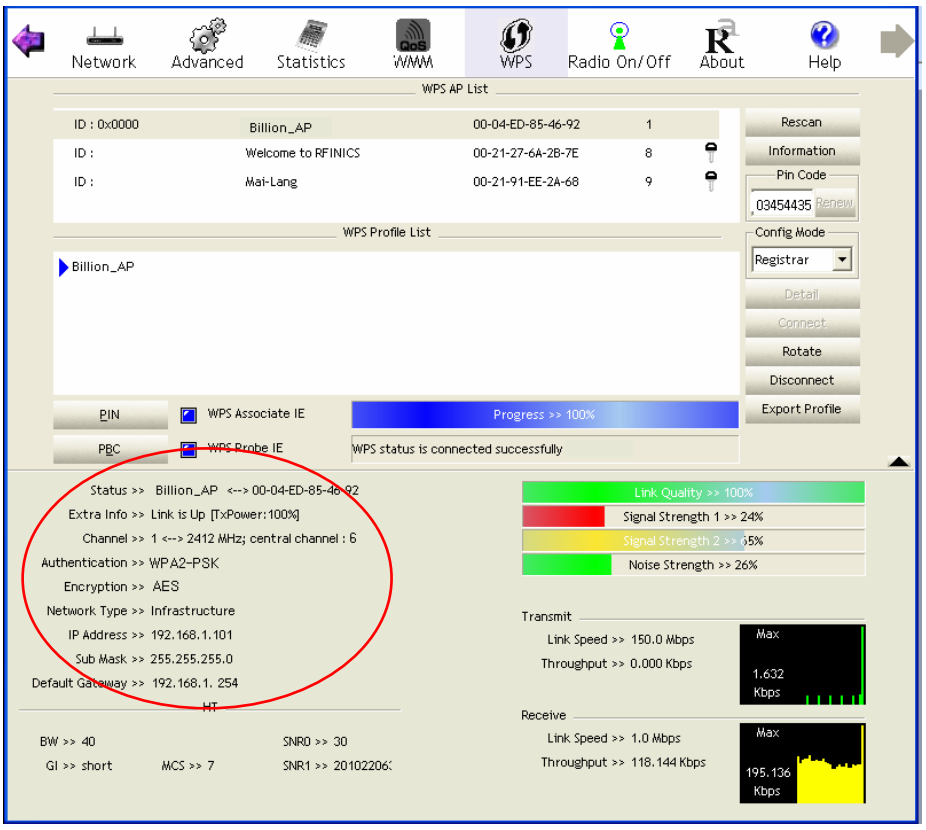
1. Jot down the AP PIN Code (e.g. 03454435) from the 9900VA. Press **Start** WPS.

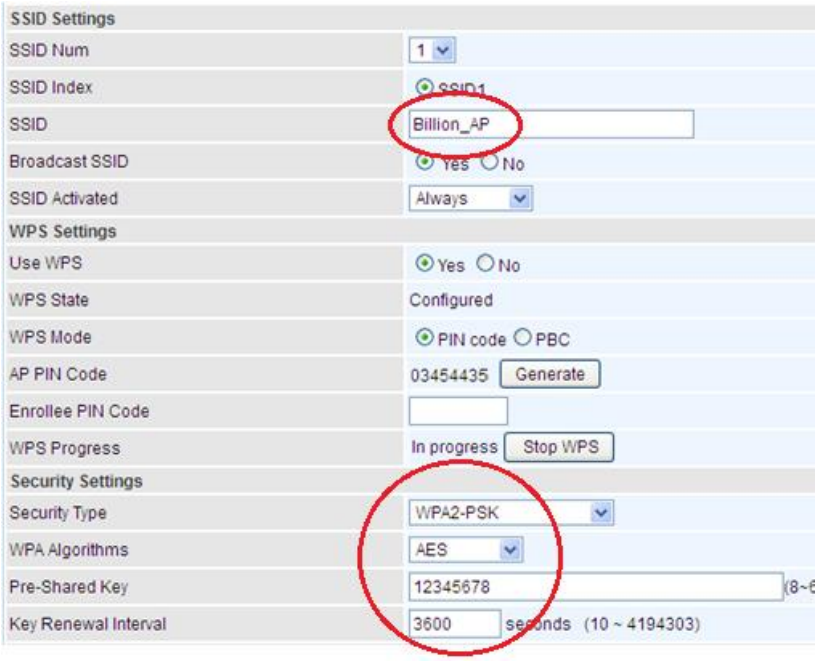


2. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code (e.g. 03454435) column then choose the correct AP (e.g. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.



3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar (client).

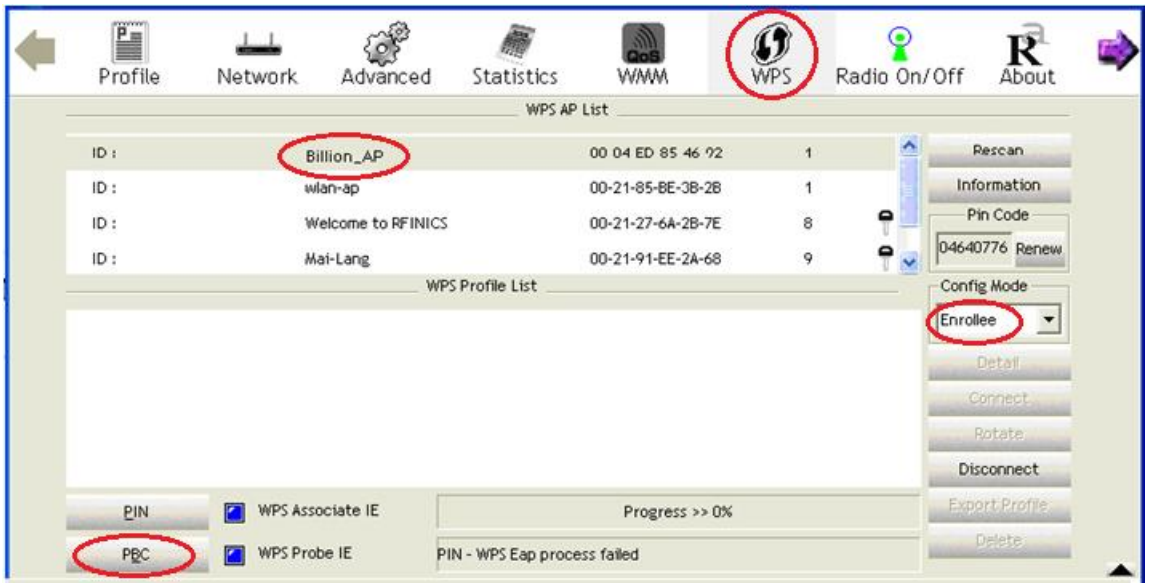




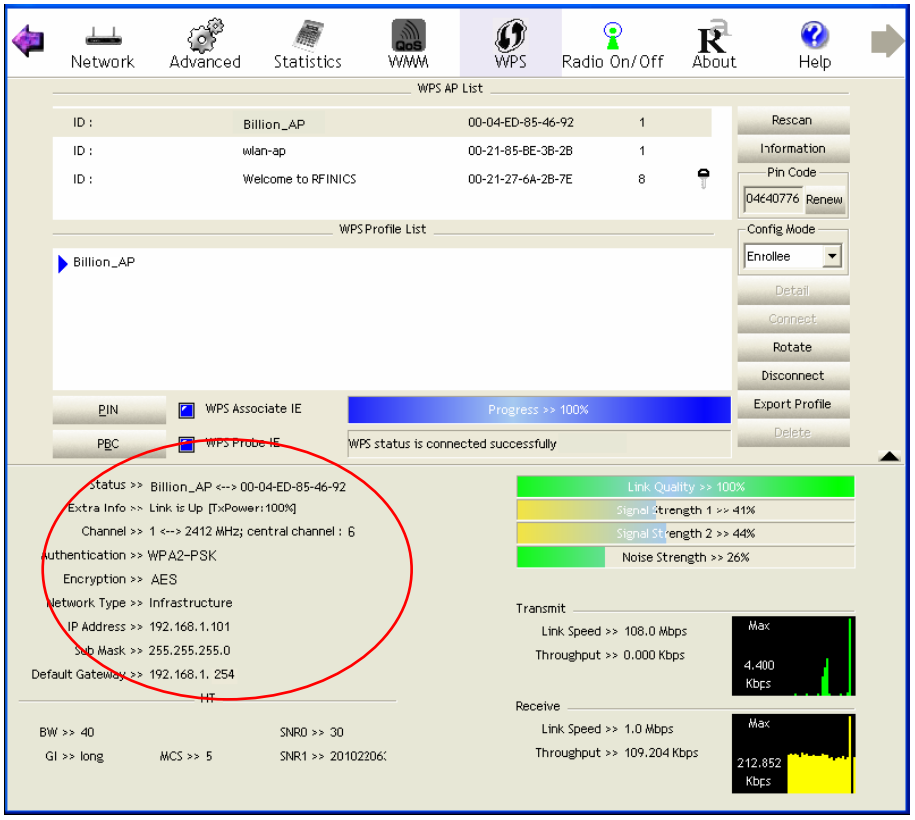
Example: WPS using PBC Method (Push Button Configuration)

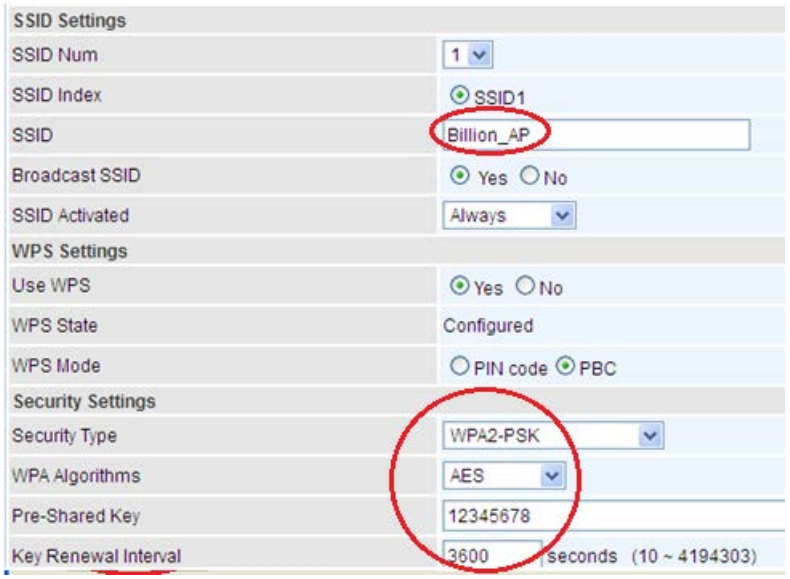
1. Click the **PBC** radio button and click **Save** to apply the settings

2. Launch the wireless client's WPS Utility (e.g. Ralink Utility). Set the Config Mode as **Enrollee**. Then press the **WPS button** and choose the correct AP (e.g. **Billion_AP**) from the WPS AP List section before pressing the **PBC** button to run the scan.



3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

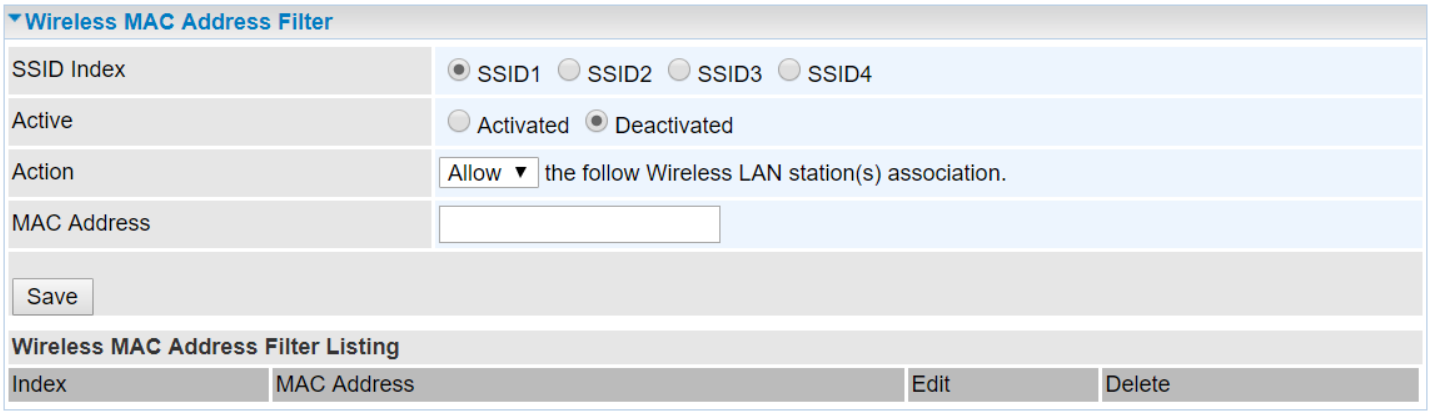




Wireless MAC Filter (2.4GHz & 5GHz)

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02.

You need to know the MAC address of the devices you wish to filter.



SSID Index: Select the targeted SSID you want the MAC filter rules to apply to.

Active: Select **Activated** to enable MAC address filtering.

Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

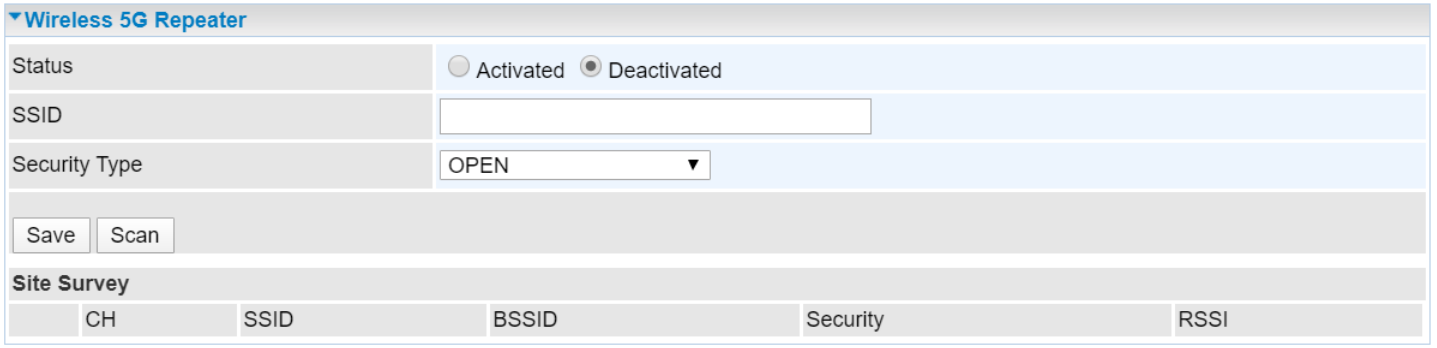
- Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router.
- Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

Click **Save** to apply the settings.

Wireless 5G Repeater

Wireless repeater mode allows you to pick up an existing wireless signal from an Access point then rebroadcast it to create a new Wi-Fi network.



Status: Click Activated to enable the Wi-Fi Repeater feature.

Manually Fill-in

SSID: Enter the SSID of the primary AP.

Security Type: Enter the Wi-Fi security type of the primary AP.

WPA Algorithms: Enter the WPA algorithms of the primary AP.

Pre-Shared Key: Enter the Wi-Fi password/pre-shared key of the primary AP.

Automatically

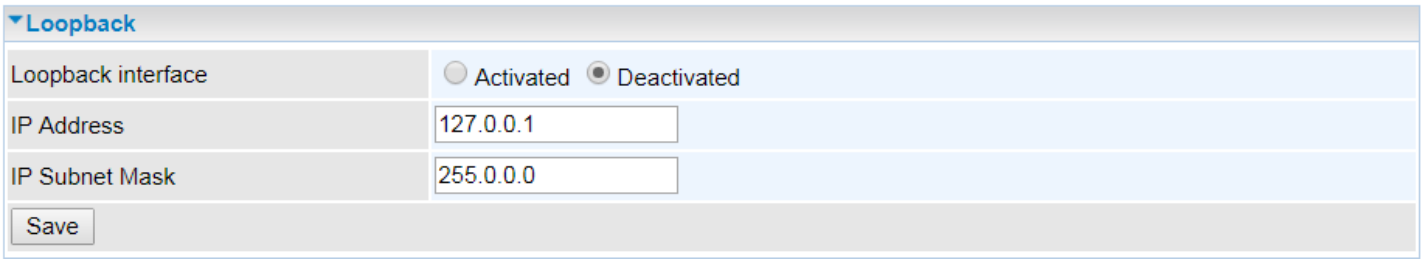
Scan: Click to view all other available Wireless-AP devices near the 9900VA. Select the desired AP you wish to extend the signal.

- **CH (Channel)**: Channel ID used.
- **SSID**: The name of the wireless AP.
- **BSSID**: The MAC address of the wireless AP.
- **Security:** The security mode in the wireless AP.
- **Signal (%):** Signal strength of the wireless AP. Signal increases means the wireless AP is closer to your BEC 4700A and may cause interferences.

Click **Save** to apply the settings.

Loopback

Loopback interface is a widely known virtual interface, not the physical interface, on router and is highly robust and always up. The loopback interface has its own IP and subnet mask, often used for router management as Telnet management IP and involved in BGP as BGP Update-Source and OSPF as Router ID.



IP Address: Enter a dedicated IP address for the loopback interface.

IP Subnet Mask: Enter the subnet mask for the loopback interface.

Click **Save** to apply settings.

Dual WAN

Dual WAN, is a feature to have two independent Internet connections connected concurrently, offers a reliable Internet connectivity and maximize bandwidth utilization for critical applications delivery.

Here are the features in **Dual WAN:** General Setting, Outbound Load Balance and Protocol Binding.

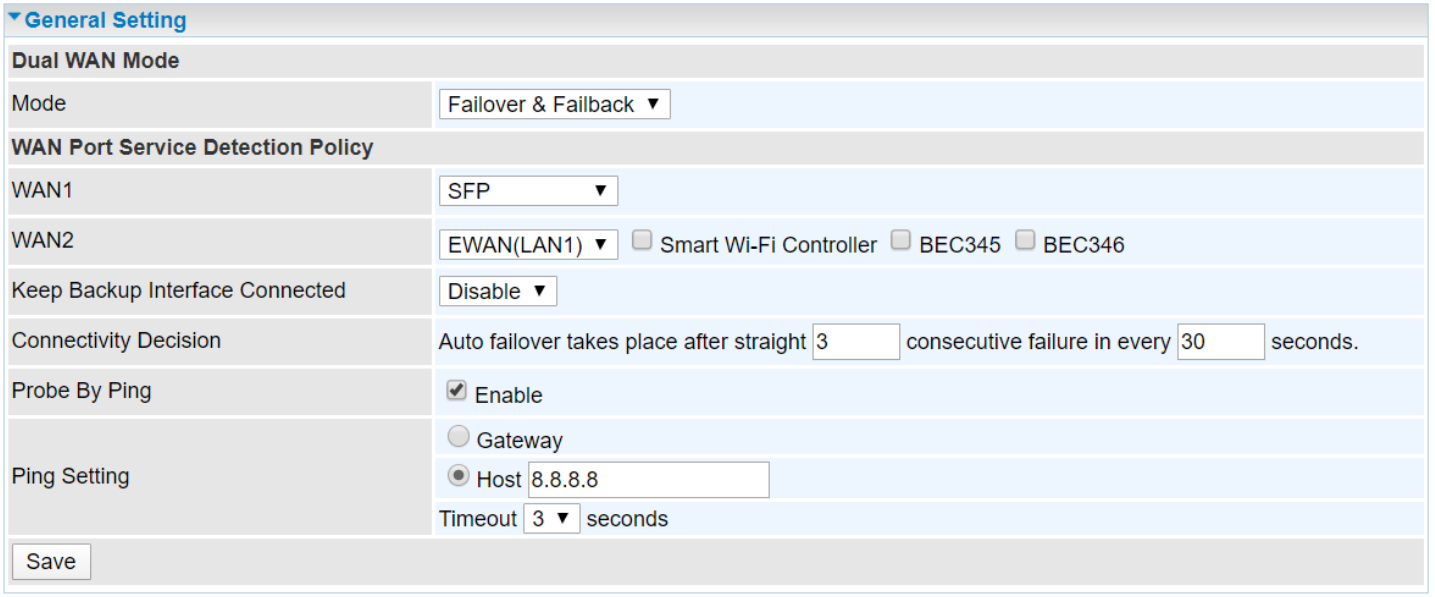
General Setting

Mode: Select a mode then click **Save** to proceed.

❖ Failover & Failback

Auto failover/failback ensures always-online network connectivity. When primary WAN link (WAN1) fails, all traffic will switch over to the backup WAN (WAN2) seamlessly.

Again, when the primary link is restored, traffic will be handled over from WAN2 to WAN1.



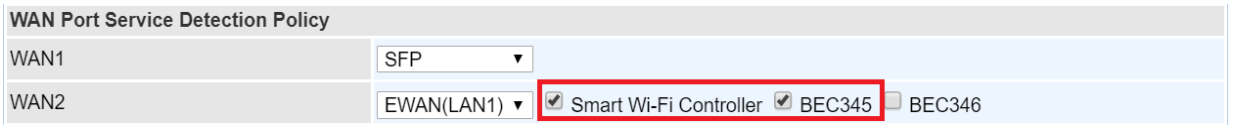
WAN Port Service Detection Policy

WAN1 (Primary): Choose a desired WAN as the primary WAN Link from the list.

WAN2 (Backup): Choose a desired WAN as the backup WAN Link from the list.

- **Smart Wi-Fi Controller:** It is used to allow specific Wi-Fi AP network(s) to access to the Internet. Only the connected Wi-Fi clients attached to the AP can have internet access; the wired LAN users are not limited to this rule. Click the **Smart Wi-Fi Controller** + a specific Wi-Fi AP SSID to enable this feature.

  Example: User only grants AP, SSID **BEC345**, to have internet access via Ethernet WAN, WAN2 interface.



Keep Backup Interface Connected: Select the following option whether to keep the backup WAN (WAN2) interface connected to the Internet.

- **Disable:** Inactivate this feature.
- **Always:** Keep the backup WAN (WAN2) interface always connected to the Internet

Connectivity Decision & Probe Cycle: Set a number of times and time in seconds to determine when to switch to the backup link (WAN2) when primary link (WAN1) fails and vice versa.

Example, *Auto failover takes place after straight* **3** *consecutive failures in every* **30** *seconds* meaning all traffic will hand over to backup link (WAN2) after primary link fails to response in total of 90 seconds, 30 seconds for 3 consecutive failures.

Note: Failover and Failback follow the same **Connectivity Decision & Probe Cycle** rule to failover from WAN1 to WAN2 or fallback from WAN2 to WAN1.

Failover/Fallback Rule Decisions:

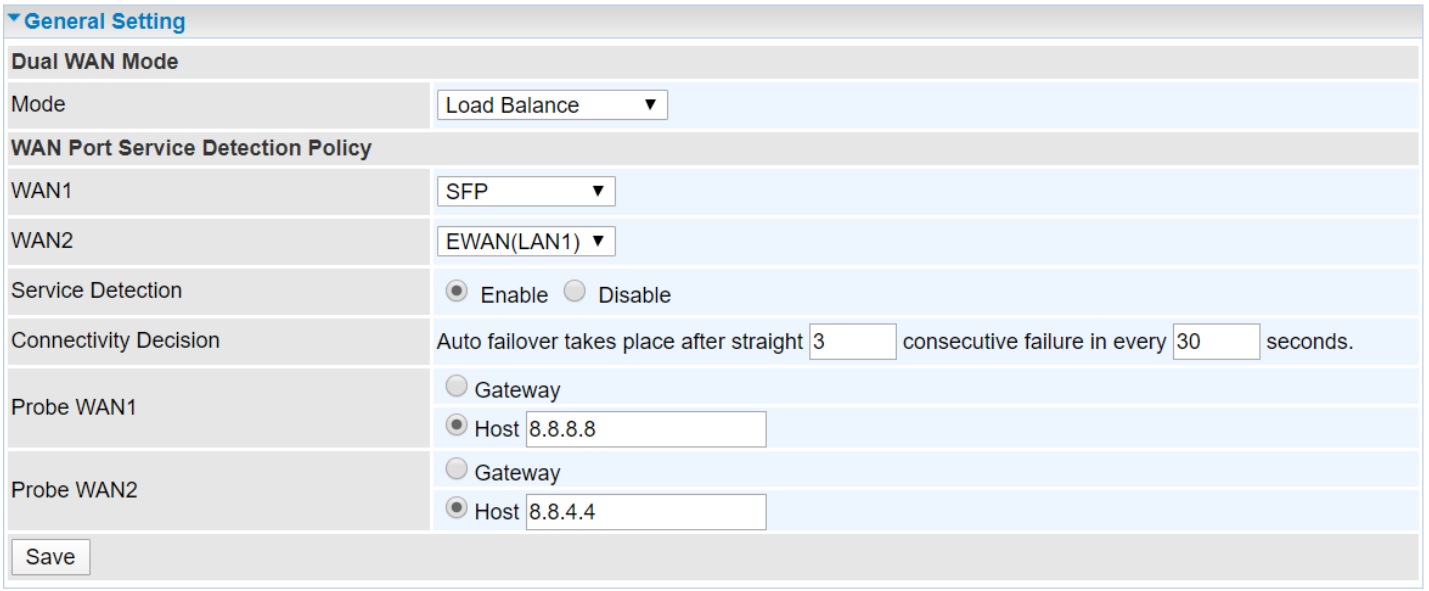
1. **Probe by Ping:** Enable Ping to the gateway or an IP address
   - **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.
   - **Host:** Internal system will wait for responses to the pings from a fixed IP address.

Click **Save** to apply settings.

❖ Load Balance

Load balance aggregates the bandwidth of the two WAN links to optimize traffic distribution.

When primary link, WAN1, goes down, all traffic will be redirected to the backup, WAN2, to ensure service continuity.



WAN Port Service Detection Policy

WAN1 (Primary): Choose a desired WAN as the primary WAN Link from the list.

WAN2 (Backup): Choose a desired WAN as the backup WAN Link from the list.

Service Detection: Enable to detect WAN connectivity automatically.

Connectivity Decision: Set a number of times and time in seconds to determine when to turn-off the Load Balancing service.

Example, *Disable Load Balance after straight* **3** *consecutive failures in every* **30** *seconds* meaning all traffic will hand over to backup link (WAN2) after primary link fails to response in total of 90 seconds, 30 seconds for 3 consecutive failures.

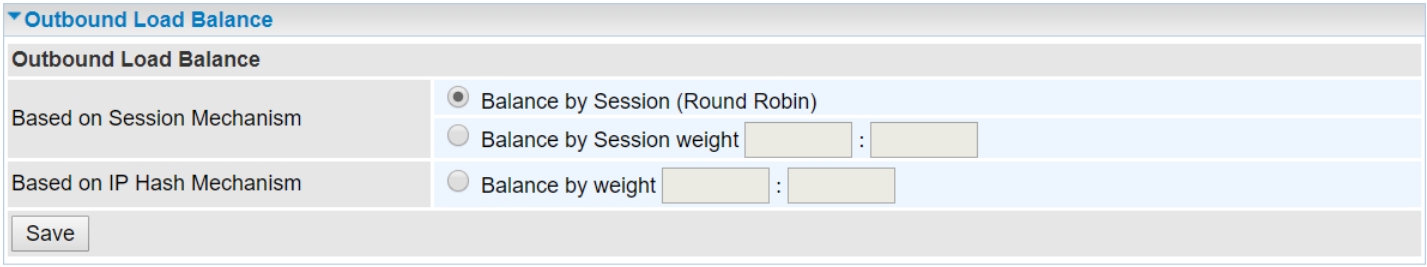
Probe Ping on WAN 1 / WAN2: Enable Ping to the gateway or an IP address

- **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.
- **Host:** Internal system will wait for responses to the pings from a fixed IP address.

Click **Save** to apply settings

Outbound Load Balance

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



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

Base on Session Mechanism:

Balance by Session (Round Robin): Automatically assign requests/traffics to each WAN interface based on real-time WAN traffic-handling capacity.

OR

Balance by Session weight: Manually Balance session traffic based on a weight ratio.

Example: Session weight by 3:1 meaning forward 3 requests to WAN1 and 1 request to WAN2.

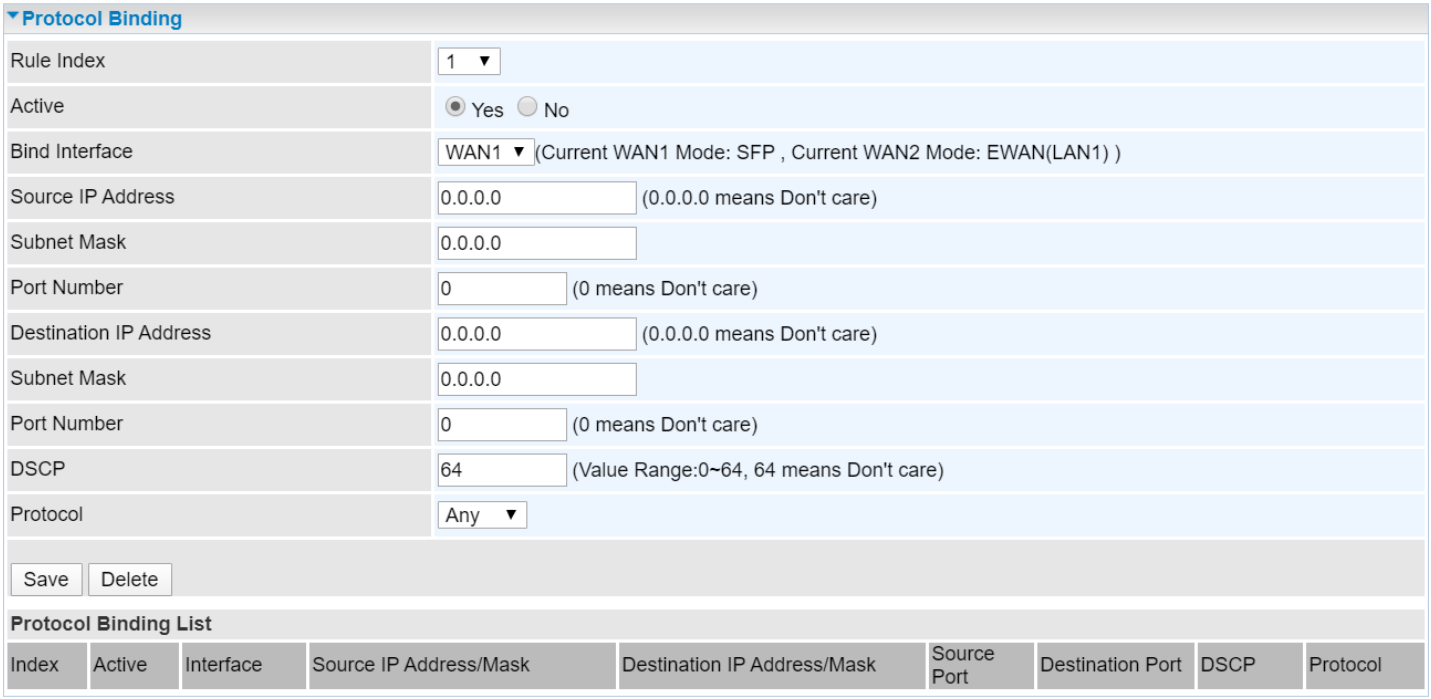
Base on IP Hash Mechanism:

Balance by weight: Use an IP hash to balance traffic based on a ratio. It is to guarantee requests from the same IP address get forward to the same WAN interface.

Click **Save** to apply settings

Protocol Binding

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



Rule Index: The numeric rule indicator. The maximum entry is up to 16.

Active: Click YES to activate the rule

Bind Interface: The dedicated WAN interface that guarantees to handle this traffic request.

Source IP Address: Enter the local network, known as source, IP address of the origin of a traffic/packet. **0.0.0.0** means any IP address in the network.

Subnet Mask: Enter the subnet of the source network.

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

Destination IP Address: Enter the destination / remote WAN IP address where the traffic/packet is going to. Enter **0.0.0.0** if no need to route to a specific IP address

Subnet Mask: Enter the subnet of the designation network.

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

DSCP: The DSCP value. Value Range from 0~64; **64** means any value/unspecified

Protocol: Select a protocol, TCP, UDP, ICMP, to use for this traffic.

Click **Save** to apply settings

Example:

All traffics from IP 192.168.10.1/255.255.255.0 with port 8080 will go through WAN1 interface.

The only time it would go through WAN2 interface is when WAN1 has no Internet connection.

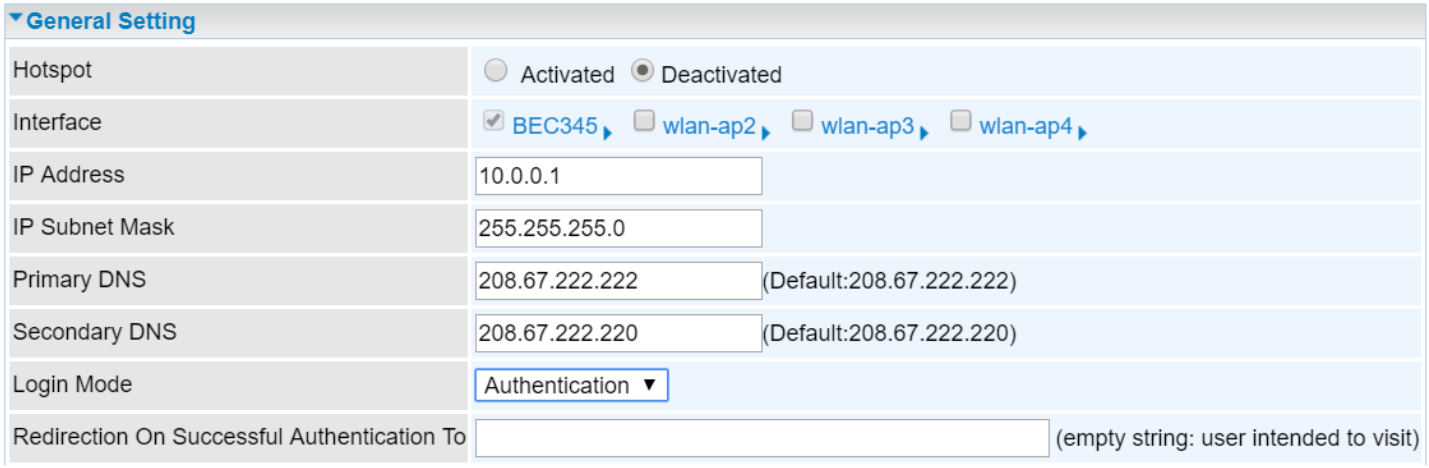
Protocol Binding List

Index	Active	Interface	Source IP Address/Mask	Destination IP Address/Mask	Source Port	Destination Port	DSCP	Protocol
1	Yes	WAN1	192.168.10.1/ 255.255.255.0	0.0.0.0/ 0.0.0.0	8080	0	64	ANY

Hotspot

The Wi-Fi hotspot offers Internet access for mobile devices like smart phones, laptops, or smart pad to connect wirelessly in public locations such as in coffee shops, train station, airport, hotel, and much more. A captive portal with a login page will prompt on the mobile devices and require all Wi-Fi clients to accept the term of use before accessing to the Internet.

General Setting



General Setting

Hotspot: Activate to enable the Wi-Fi hotspot feature.

Interface: Select Wi-Fi interface(s), example: BEC345 (SSID 1) to handles the hotspot traffic.

IP Address: The IP address for the Wi-Fi hotspot network.

IP Subnet Mask: Enter the subnet of the network.

Primary / 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.

Login Mode: Two (2) types of login modes to join the network.

- **Authentication:** Username and Password (credential) is required to join the hotspot network. Go down to the Authentication section below and select a method.
- **Agreement:** No Username and Password is required. Automatically login to the hotspot network after accepting and agree to the terms ("Terms") of use.

Redirect URL after Successful Login: Enter a redirect URL (**http://** is not required). After Wi-Fi client is successful login to the network, the page will get redirected to the specific URL. Leave it blank if no redirection is necessary.

NOTE: This new URL will be added to the Walled Garden automatically.

Authentication

Authentication	
Authentication Method	RADIUS Built-in User Account
Primary RADIUS Server	
Secondary RADIUS Server	
Shared Secret Key	Show Character
Authentication Protocol	CHAP

Authentication Methods: Two (2) network authentication methods, local built-in user account or a remote, external RADIUS server. If the credential matches, the Wi-Fi client is granted access to the network.

- **RADIUS (an external authentication server)**
  - **Primary RADIUS Server:** The main IP address of the server.
  - **Secondary RADIUS Server:** The backup IP address of the server, if any.
  - **Shared Secret Key:** Enter the shared Secret given by the server. Click **Show Character** to view your key.
- **Built-in User Account (local database handled by the BEC device)**

  Go to the **Built-in User Account** to setup account usernames and passwords for the hotspot.

Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol) or MSCHAPv2. When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Session Settings

Session Settings		
Session Timeout	3600	seconds (0~86400,0:disable)
Idle Timeout	180	seconds (0~86400,0:disable)
Upload Bandwidth	0	Kbps (0~5120,0:not limited)
Download Bandwidth	0	Kbps (0~5120,0:not limited)
Maximum Download Data Usage	0	MBytes (0~5120,0:not limited)
Maximum Upload Data Usage	0	MBytes (0~5120,0:not limited)
Maximum Total Data Usage	0	MBytes (0~5120,0:not limited)

Session Timeout (in seconds): The time period of a Wi-Fi client is allowed to access to the Internet. After this timeout period, a new authentication is required.

Idle Timeout (in seconds): The allowed inactivity time of a Wi-Fi client. After this timeout period, a new authentication is required.

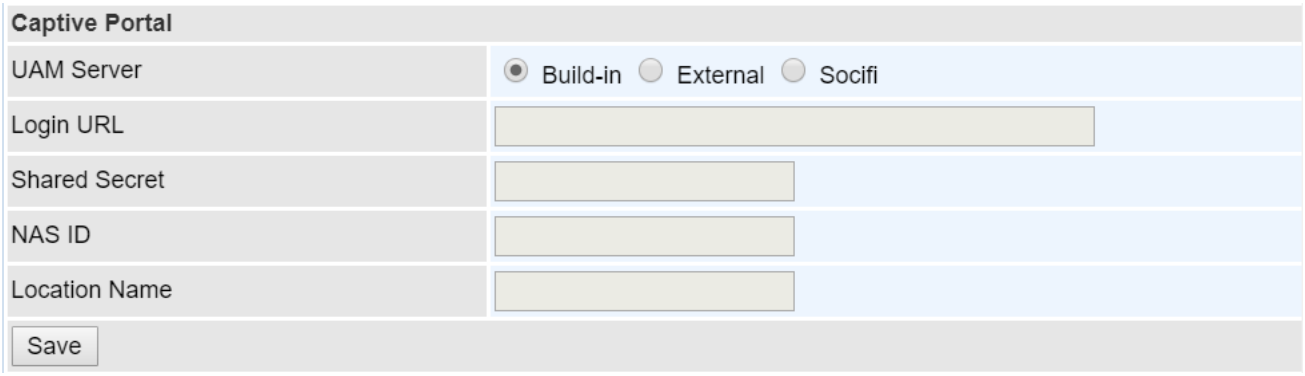
Upload / Download Bandwidth (in Kbps): The maximum upload and download link speed, value range from 0 ~ 5120Kbps; **0** means no speed limitation.

Maximum Upload / Download Data Usage (in MBytes): Pre-configure a maximum upload and download data allowed for each session. value range from 0 ~ 5120MB; **0** means no speed limitation.

Maximum Total Data Usage (in MBytes): Pre-configure total data usage allowed for each session.

value range from 0 ~ 5120MB; **0** means no speed limitation.

Captive Portal



UAM Server: Select a server you wish to use, **Build-in**, **External** or **Socifi**. Fill in the blanks to use External UAM server.

UAM Server: Built-in & External

Login URL: Enter the login URL offered by the UAM server.

Shared Secret: Set the shared secret password offered.

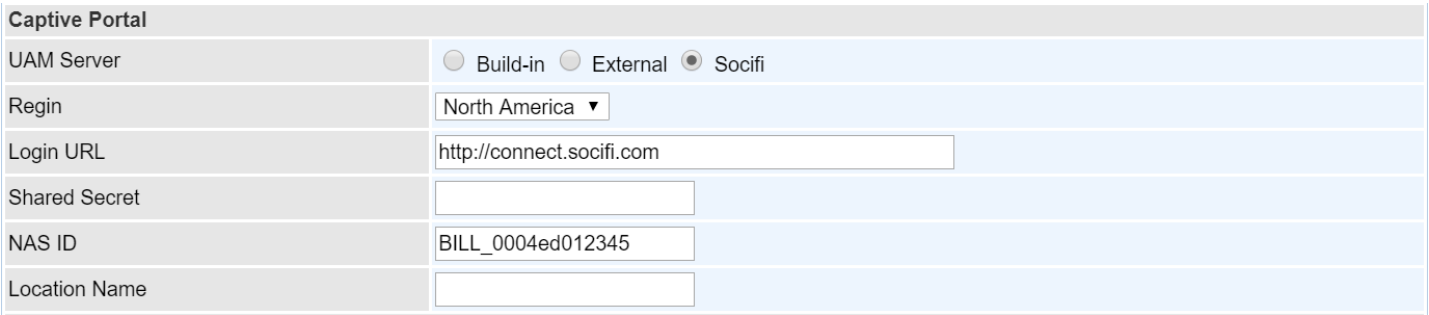
NAS ID: An assigned string for identification.

Location Name: An assigned string for identification.

Click **Save** to apply the settings

UAM Server: Socifi

SOCIFI is a cloud-based technology platform that enables the monetization of 4G/WiFi networks.



Regin: Select your location.

Login URL: Enter the new login page of Socifi if different.

Shared Secret: Enter the shared secret given from Socifi.

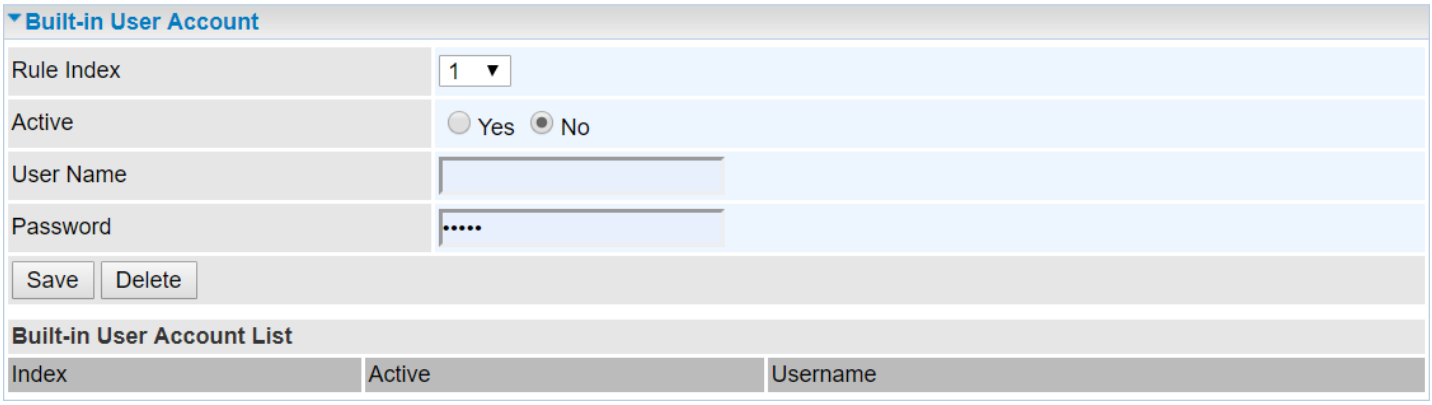
NAS ID: It is the device MAC address. Use this MAC address to create or add a new hotspot in your Socifi dashboard.

Location Name: It is not used by Socifi. Use it if needed.

Built-in User Account

It is a local database on the router with pre-defined user accounts authorized by the BEC device to grant and provide Wi-Fi hotspot access for Wi-Fi capable devices/users.

16, maximum, accounts are allowed.



Rule Index: The numeric rule indicator. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the account.

Username / Password: Create a username and password for this user account.

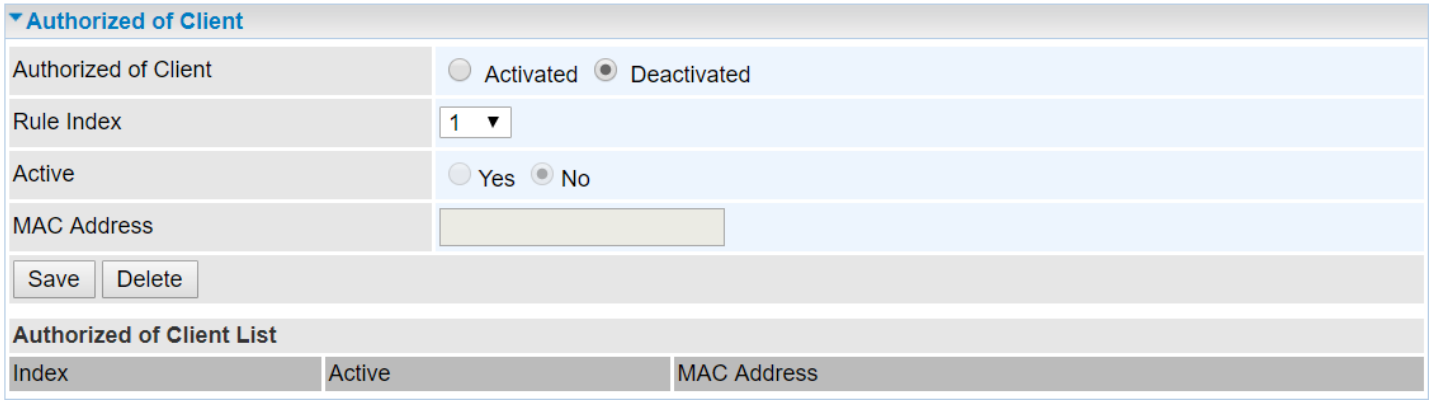
Save: Click the **Save** button to apply the settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Account list.

Authorized of Client

Add and predefine a trusted wireless MAC address of a Wi-Fi capable device for an immediate hotspot/Internet access. Hotspot/Internet access requires no authentication.

16, maximum, accounts are allowed.



Authorized of Client: Select **Activated** to enable this feature.

Rule Index: The numeric rule indicator. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the client.

MAC Address: Enter the wireless MAC address of the Wi-Fi device.

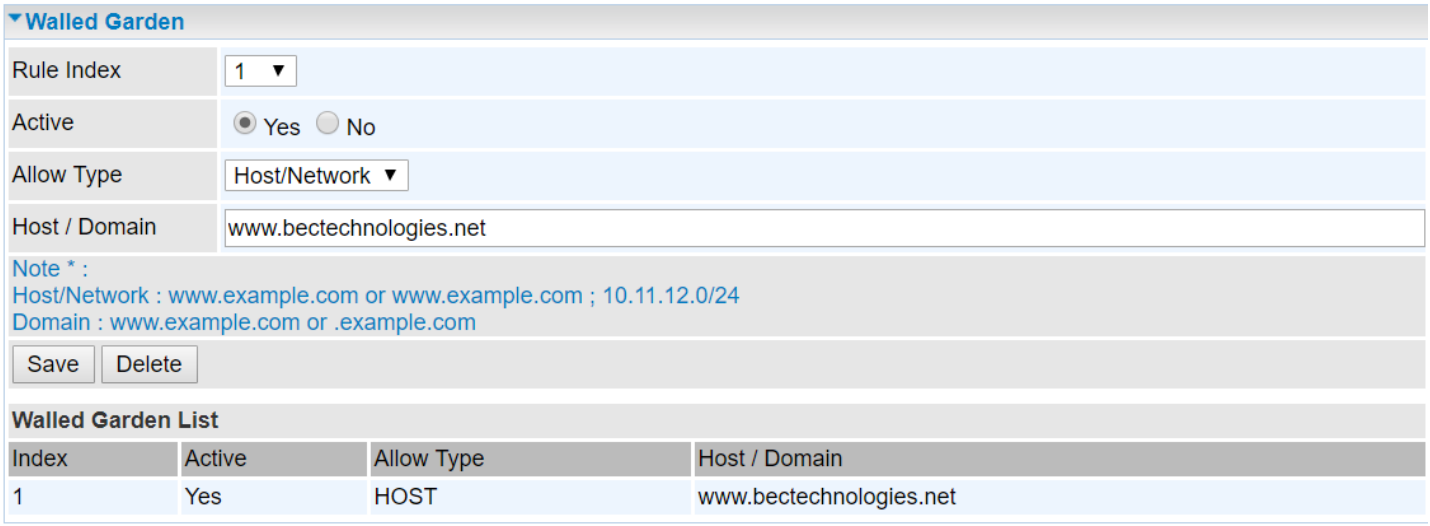
Save: Click the **Save** button to apply the settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Client list.

Walled Garden

Add and predefine websites (domain names) or web IP address to allow Wi-Fi devices / clients to access to. Web site access requires no authentication.

16, maximum, websites / domains are allowed.



Rule Index: The numeric rule indicator. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the walled garden.

Allow Type: Either a **Host/Network** or **Domain**.

Host / Domain name: Enter a valid domain, network, or website for unauthorized clients to access to.

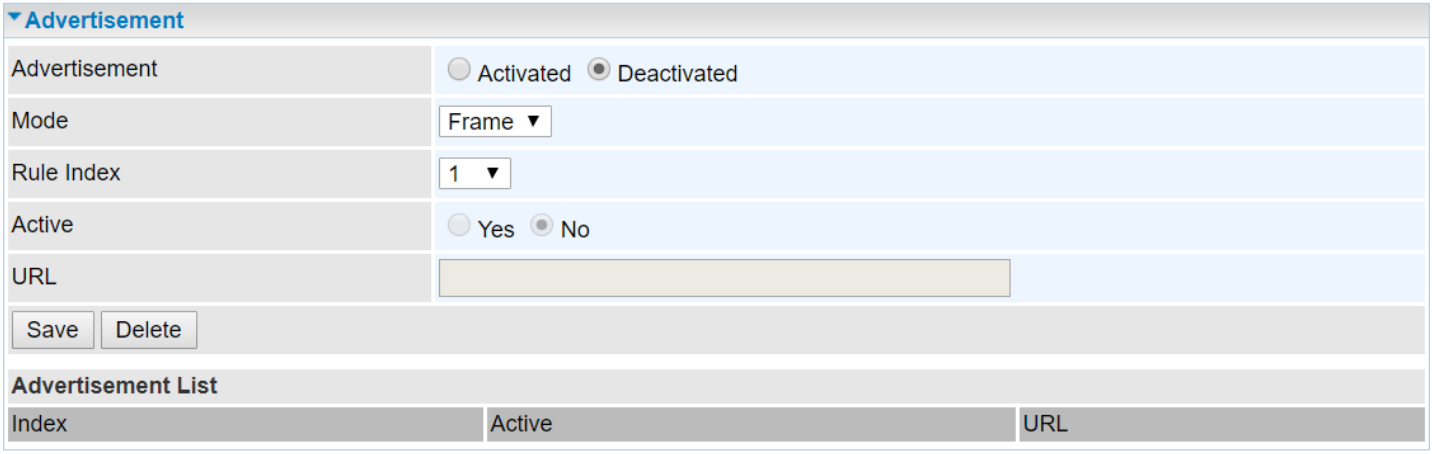
Save: Click the **Save** button to apply the settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Walled Garden list.

Advertisement

Add pop-ups ads and redirects to BEC Wi-Fi Hotspot, and only a random ad will be displayed per a login.

16, maximum, ads are allowed.



Advertisement: Select **Activated** to enable this feature.

Mode: Two (2) web advertising methods are available.

- **Frame:** Redirect to a random ad site, a full-page ad, before reaching to the login page. This full-page ad will get redirect to the login page after 5-10 seconds.
- **Popups:** A random pop-up ad display in a separate window after the login page.

Rule Index: The numeric rule indicator. The maximum entry is up to 16.

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

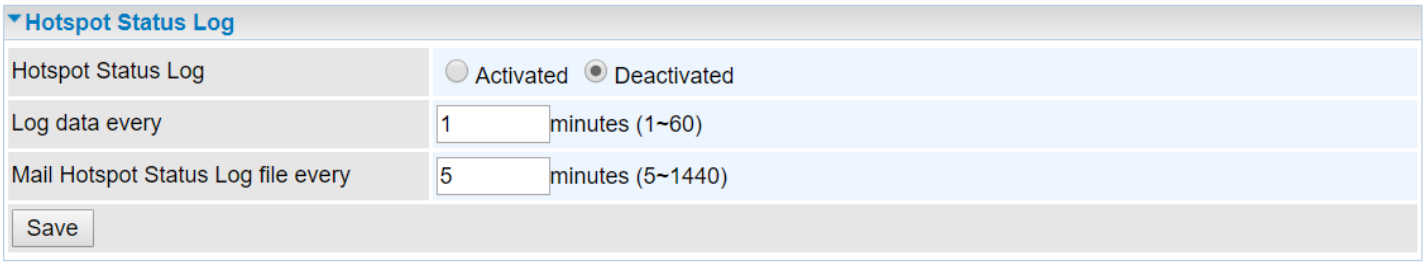
URL: Enter a valid

Save: Click the **Save** button to apply the settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Walled Garden list.

Hotspot Status Log

Record all hotspot access information and e-mail the statistics report of the hotspot clients in a specific duration.



Hotspot Status Log: Select **Activated** to enable this feature.

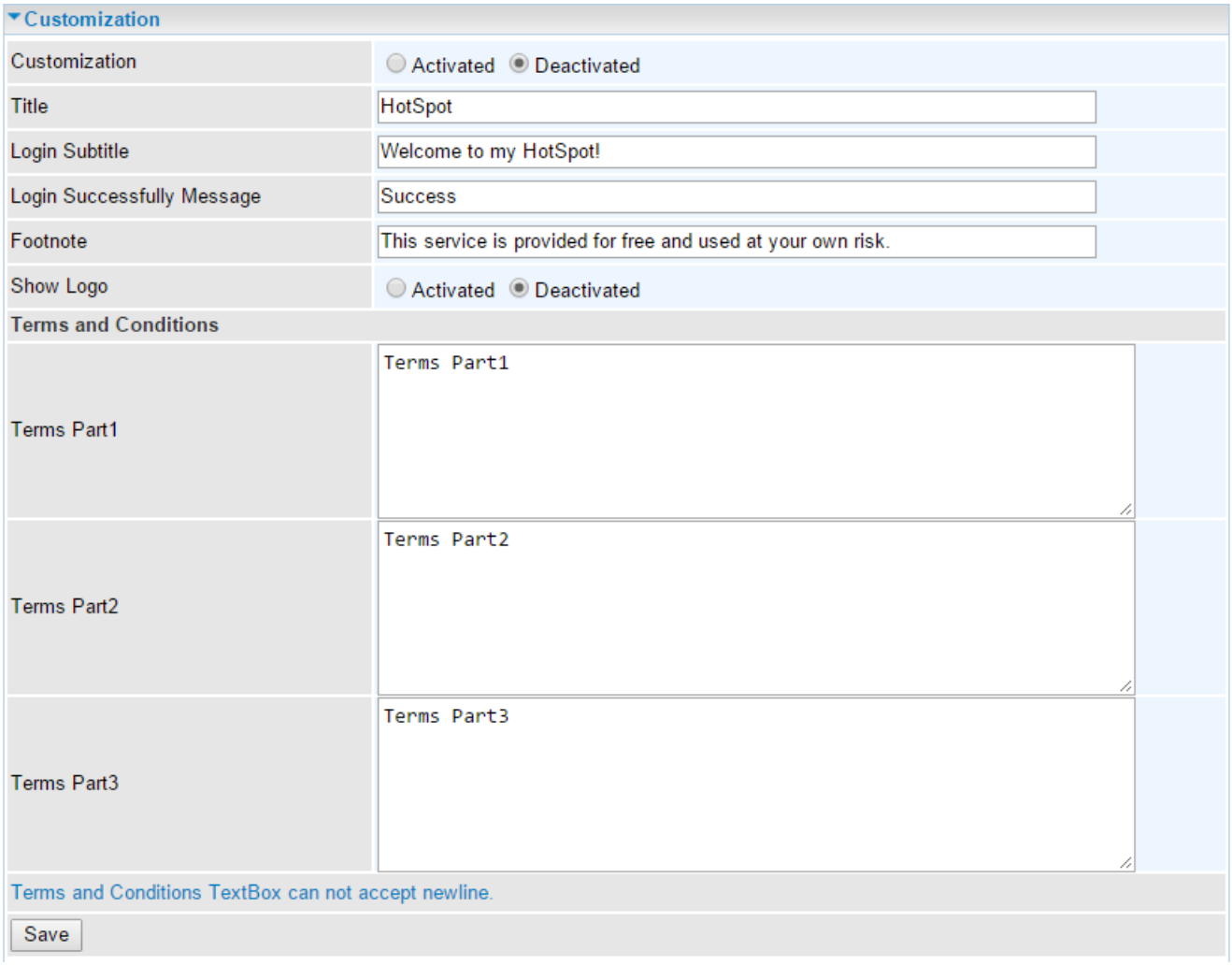
Log Data in every (minute): Input session log time duration, (min)1 to (max) 60 minutes.

Mail Session Log File in every (minute): BEC device will send all access information, such as access IP addresses, NAT tables, etc., to the administrator's mailbox in the specific time/minute.

NOTE: Please set up a dedicated or administrator e-mail account to receive Hotspot access information in the **Mail Alert**.

Customization

Allow modification to some of the captive portal settings.



Customization: Select **Activated** to enable this feature.

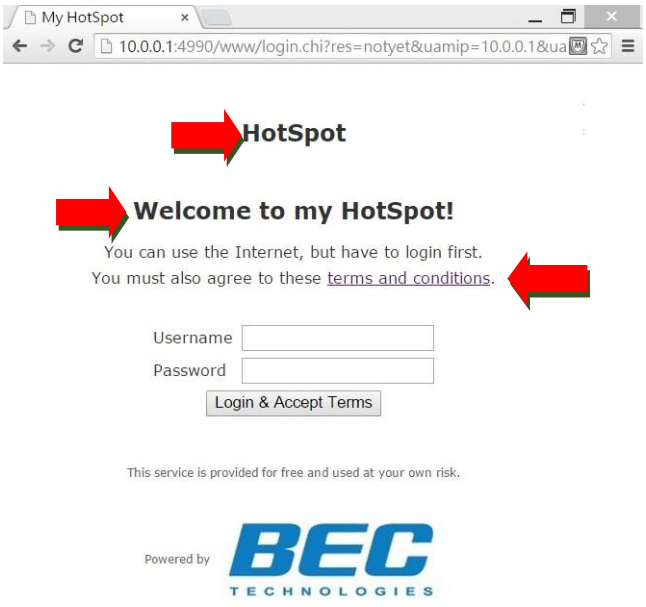
Title: The Banner message. Default is “Hotspot”

Login Subtitle: Default is “Welcome to my Hotspot”

Term Part 1 / 2 / 3: Create your own Terms and Conditions. To use default, same terms, please skip this part.

NOTE: No newline is accepted in each text box.

Login Successfully Message: BEC device will send all access information, such as access IP addresses, NAT tables, etc., to the administrator’s mailbox in the specific time/minute.

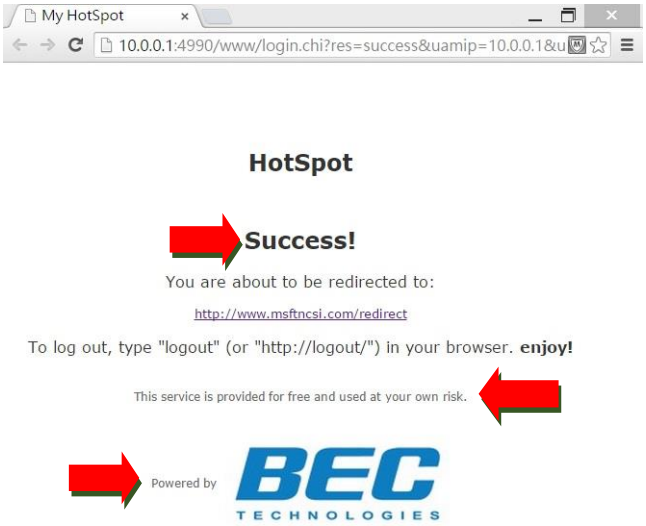


Login Successfully Message: A greeting message after successful login to the Wi-Fi hotspot. Default is “Success!”

Footnote: Additional information, if needed.

Default is “This service is provided for free and used at your own risk.”

Show Logo: Select **Activated** to display company Logo on the portal. (To change logo, please contact with BEC technical support for more information)

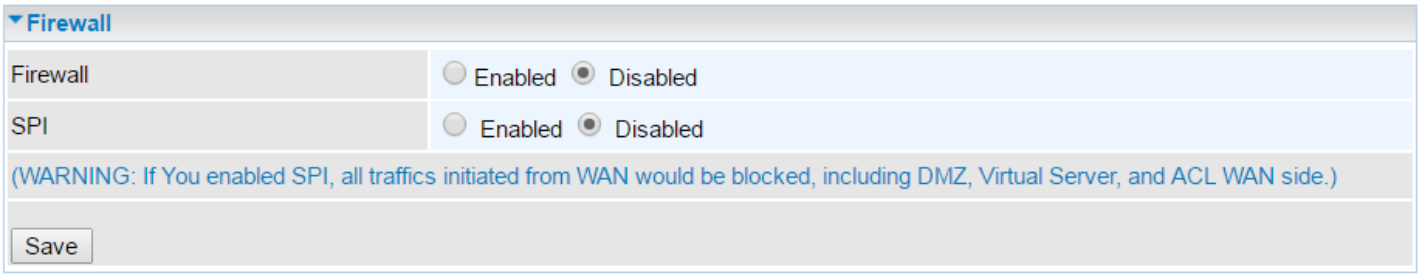


Advanced Setup

Advanced configuration features provide advanced features, including Firewall, Routing, Dynamic Routing, NAT, VRRP, Static DNS, QoS, Interface Grouping, 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:** Activate your firewall function.
- **Disabled:** Deactivate 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:** Activate your SPI function.
- **Disabled:** Deactivate the SPI function.

Click **Save** to apply settings

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.

Routing Table

Index	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
1	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	loopback		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		

Add Route

Index #: The numeric route indicator.

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

Static Route

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	○ 0.0.0.0 ◉ 4G/LTE
Metric	1

Save Back

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

Destination Subnet Mask: The subnet mask of destination network.

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

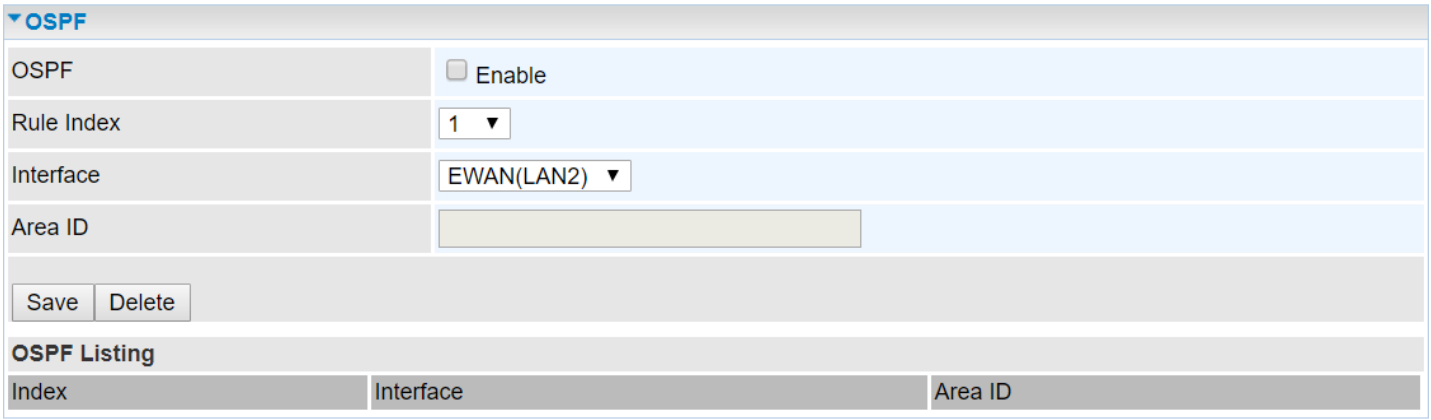
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Click **Save** to add this route

Dynamic Routing

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.

❖ Open Shortest Path First (OSPF)



OSPF: Enable to activate OSPF routing.

Rule Index: The numeric route indicator. The maximum entry is up to 10, ranging from 1 to 10.

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

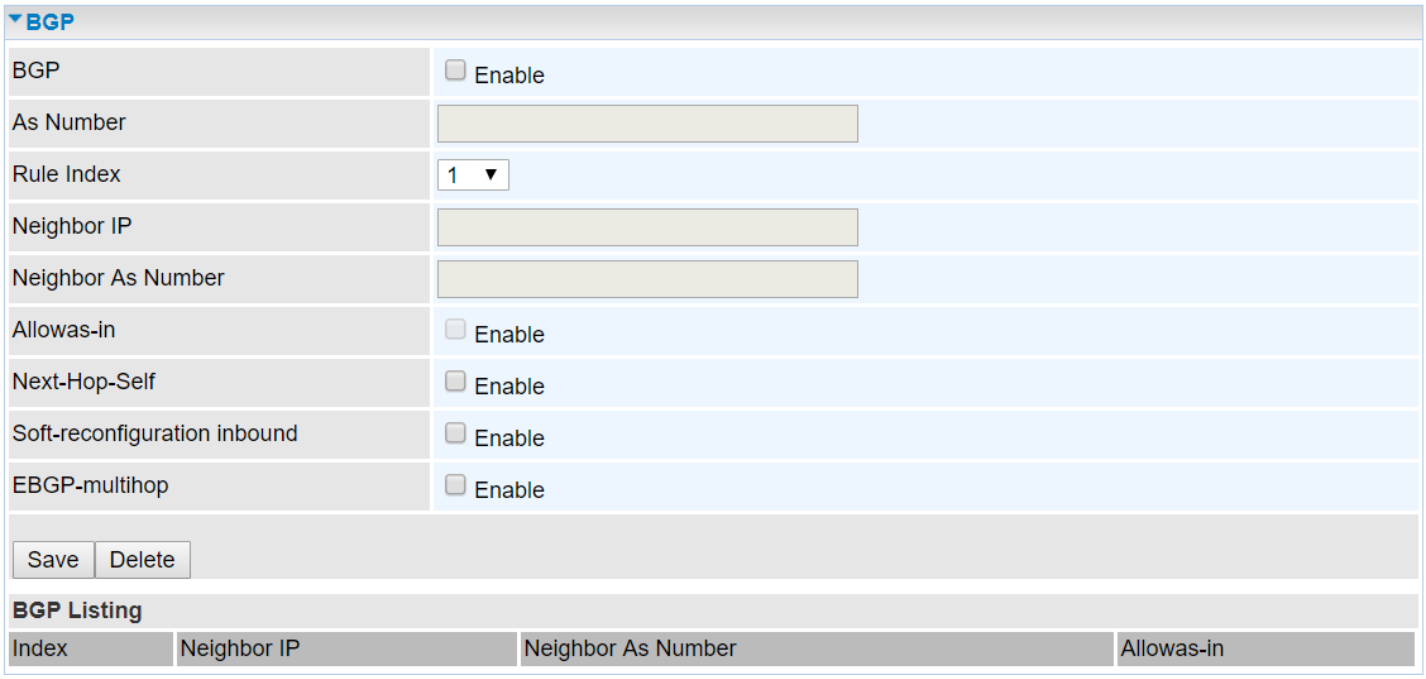
Area ID: The OSPF area identifier. It is a decimal number in the range of 0-4294967295. Enter the area ID in which the interface belongs to. The area with area-id=”0” is the backbone area.

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.

Click **Save** to add this rule.

❖ Border Gateway Protocol (BGP)

A standardized exterior gateway protocol (an uniquely TCP based 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 routers. 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: The numeric route indicator. The maximum entry is up to 10, ranging from 0 to 9.

Neighbor IP: Enter the neighbor IP address.

Neighbor AS Number: Enter the neighbor 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, an 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.

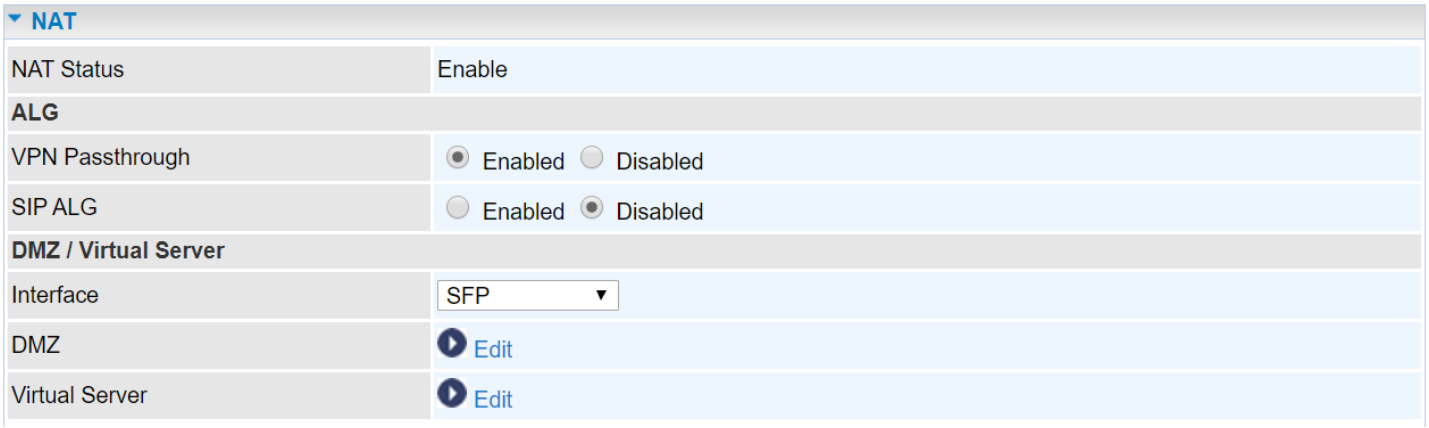
Soft-reconfiguration inbound: Enable to save, pre-stored, a new inbound policy to the BGP table without interrupting the network when applying this new policy.

EBGP (External BGP)-multihop: Enable to build up peer connection/information with external neighbors.

Click **Save** to add this rule.

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.



NAT Status: Enabled. (Disabled if WAN connection is in **BRIDGE** mode)

ALG

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.

DMZ / Virtual Server

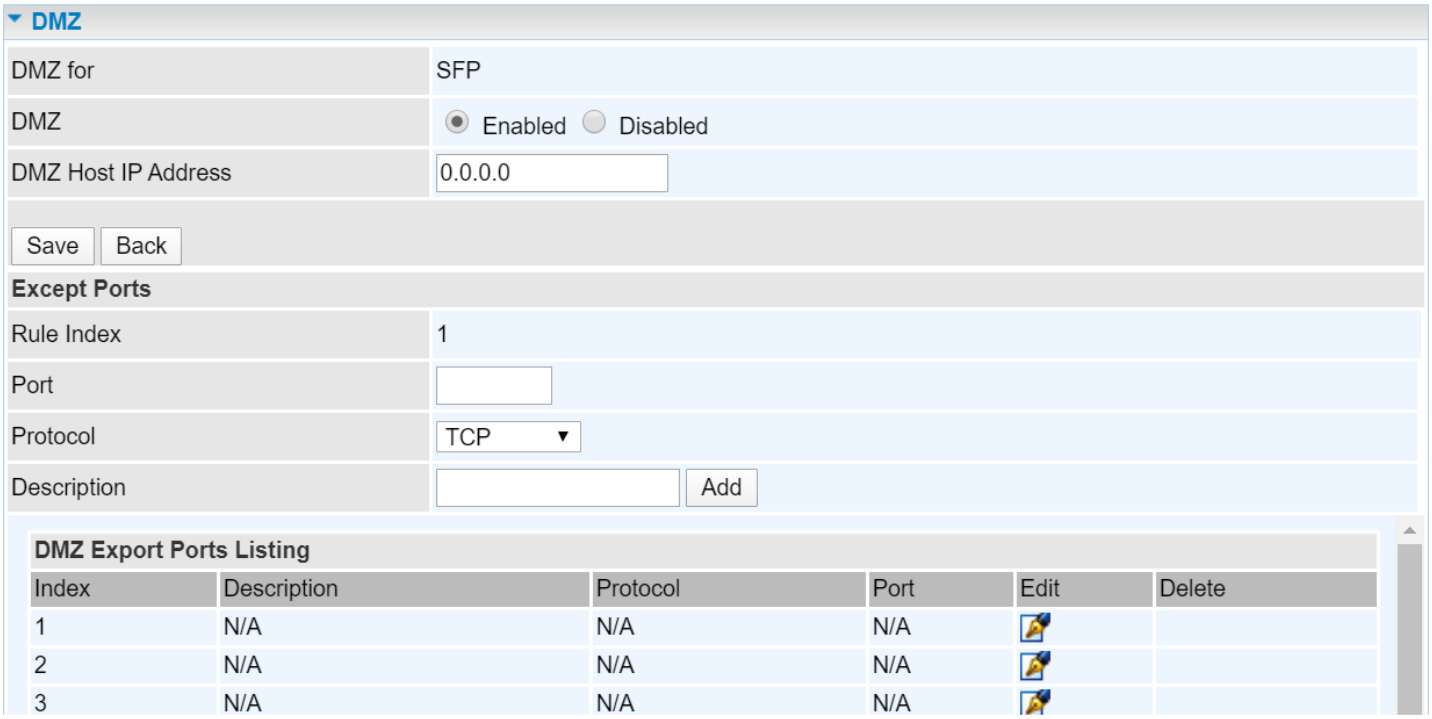
Interface: Select a WAN interface connection to allow external access to your internal network.

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 or NAT is being turned OFF.

The DMZ Host is a local computer which has all UDP and TCP ports exposed to the Internet. When setting an internal IP address as the DMZ Host, all incoming packets will be forwarded to this local host device. Packet filter or virtual server entries will take priority over forwarding internet packets to the DMZ host.



DMZ for (via a WAN Interface): Allows outside network to connect in and communicate with internal LAN devices via a specific WAN interface.

DMZ:

- **Enabled:** Activate the DMZ function.
- **Disabled:** Deactivate 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.

Click **Save** to apply settings

Except Ports

Except Ports: Bypass UDP or/and TCP ports, in the list, being forwarded to the DMZ host.

Port: Enter port to be monitored.

Protocol: Enter the protocol to be monitored.

Description: Enter a description to this rule.

Example: Skip port 80 (UDP/TCP) in the list. All Incoming request to access to port 80 (Web GUI) will be forwarded to the embedded HTTP server of 9900VA instead of the DMZ host.

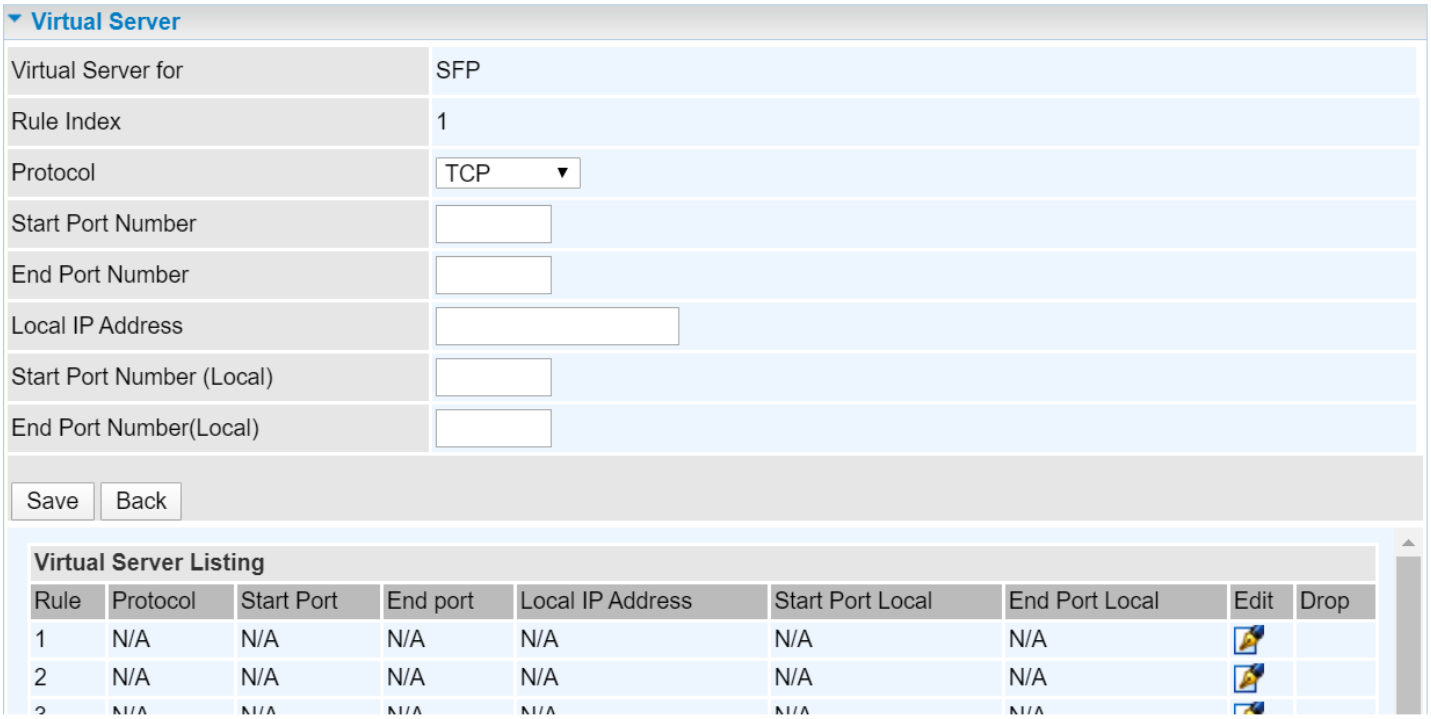
Click **Add** to add an entry to the Except Listing.

Virtual Server

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

Virtual Server is also known as Port Forwarding that allows 9900VA to direct incoming traffic to a specific device in the network.

Configure a virtual rule in 9900VA for remote users accessing services such as Web or FTP services via the public (WAN) IP address that 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 to allow outside network to communicate with the internal LAN device.

Protocol: Choose the application protocol.

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

(Example: Start / End: 1000 or Start: 1000 & End: 2000).

The starting port must be greater than zero (0). The end port must be greater than or equal to the start port.

Local IP Address: Enter the server IP address in the network to receive the traffic/packets.

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

Attention

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.

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

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

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

If you have an 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.**

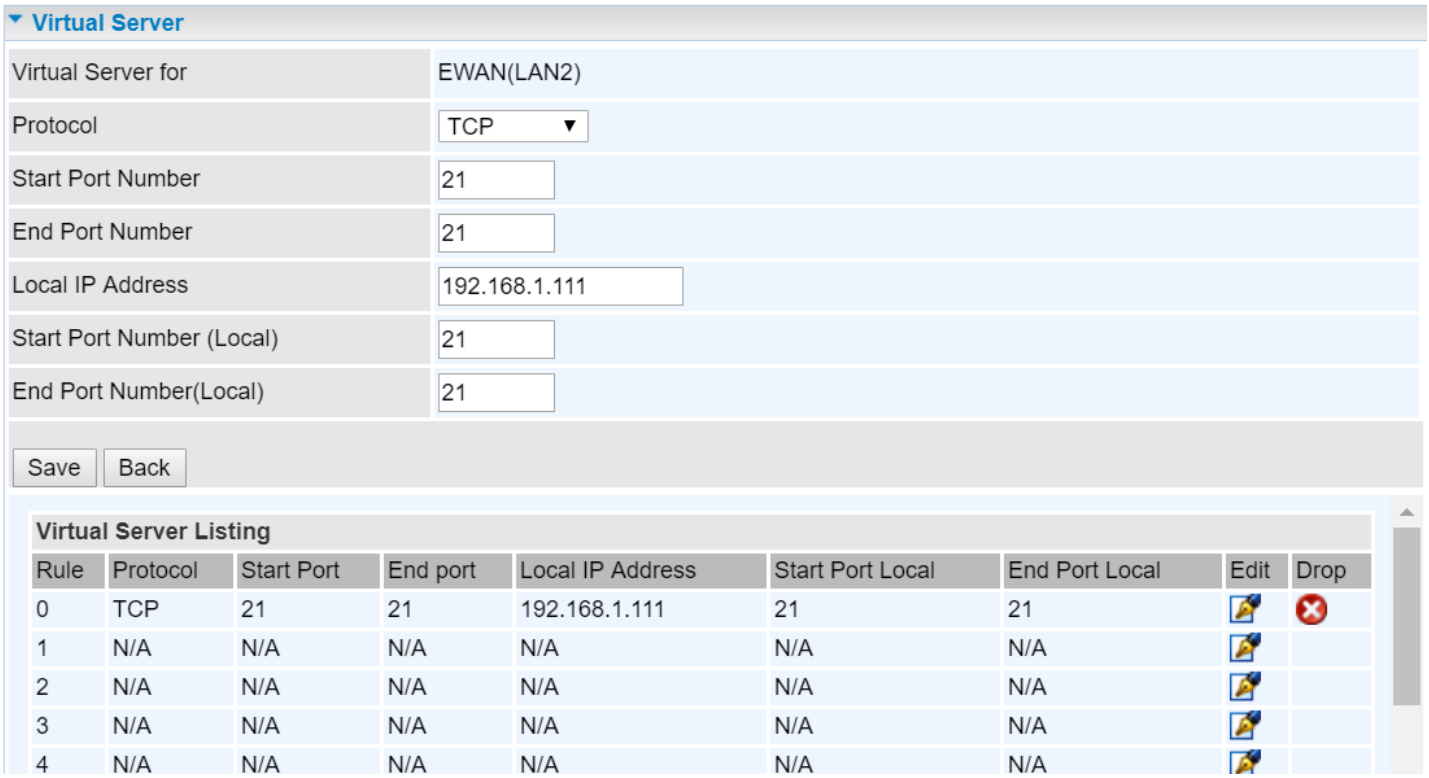
FTP server uses TCP protocol with port 21.

Enter "21" to Start and End Port Number. The 9900VA will accept port 21 requests from WAN side.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.111

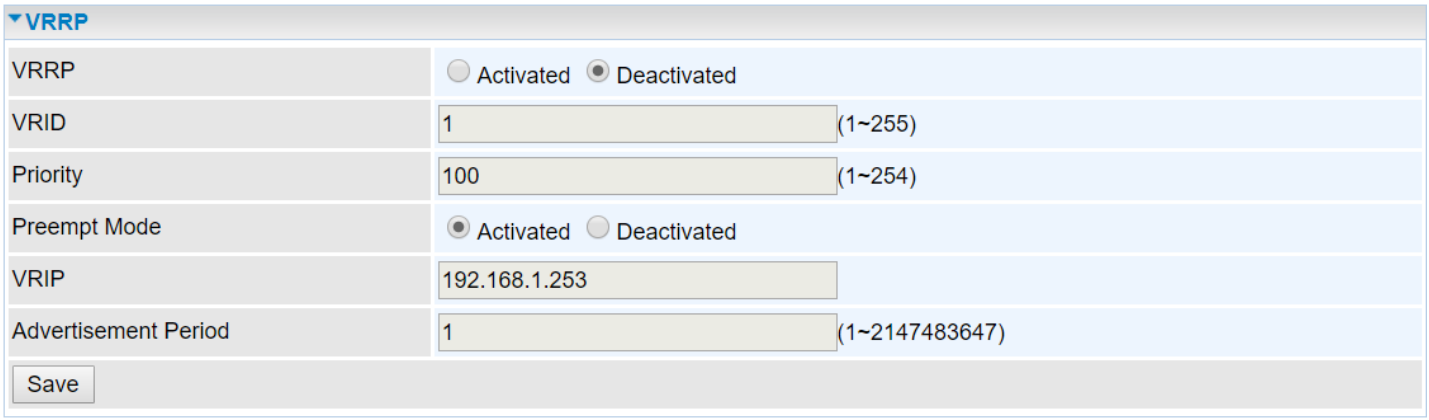
Enter "21" to Local Start and End Port number. The 9900VA will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.111) in the network.

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



VRRP

VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers in a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses in a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.



VRRP: Click to activate the feature.

VRID: Virtual Router Identifier, range from 1-255 (decimal). 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: An IP address which is associated with the virtual router.

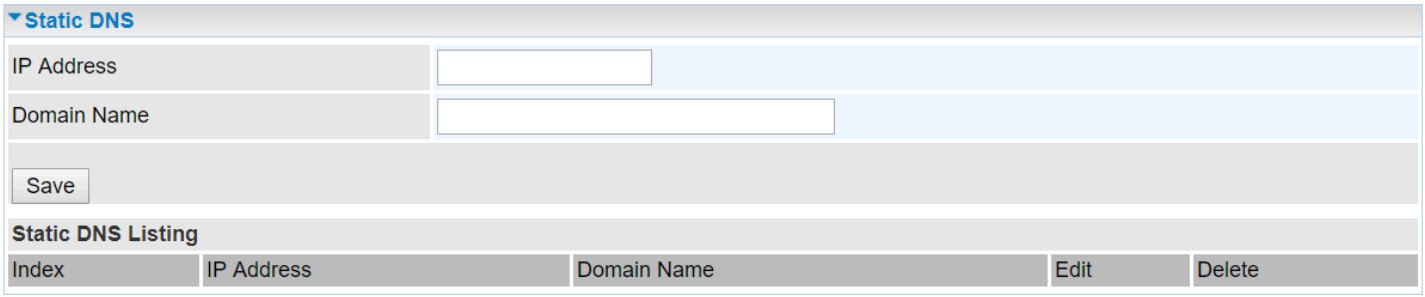
Advertisement period: Indicates the time interval in seconds between advertisements. Default in 1 second.

Click **Save** to apply 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 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.

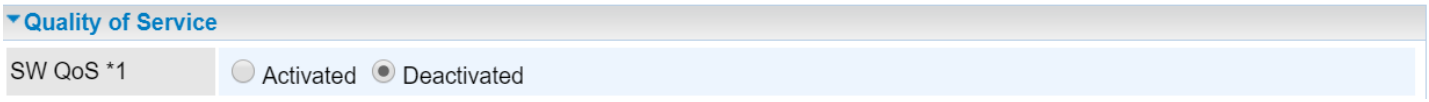
Domain Name: The friendly domain name for the IP address.

Click **Save** to apply settings.

QoS

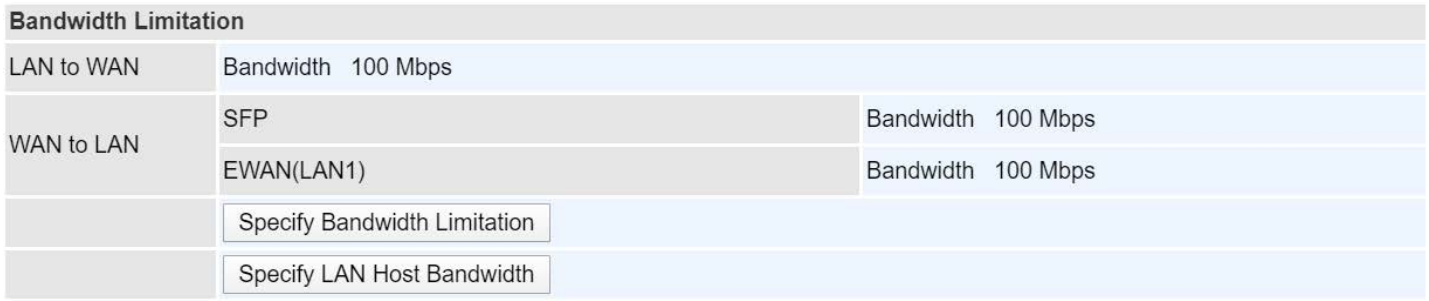
QoS helps you control the upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet).

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



SW QoS: Select **Activate** to enable the QoS

Bandwidth Limitation

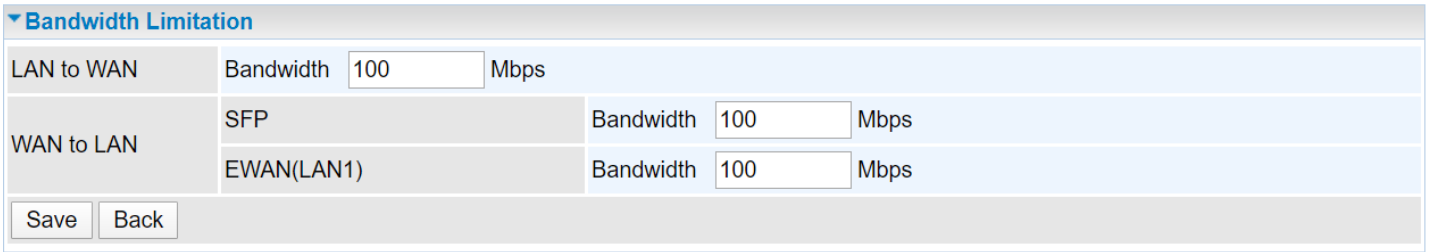


LAN to WAN (Bandwidth): Display current upstream traffic bandwidth, traffic from local network to the outside.

Example: If you have an FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.

WAN to LAN (Bandwidth): Control traffic from WAN to LAN (Downstream).

Bandwidth Limitation on WAN

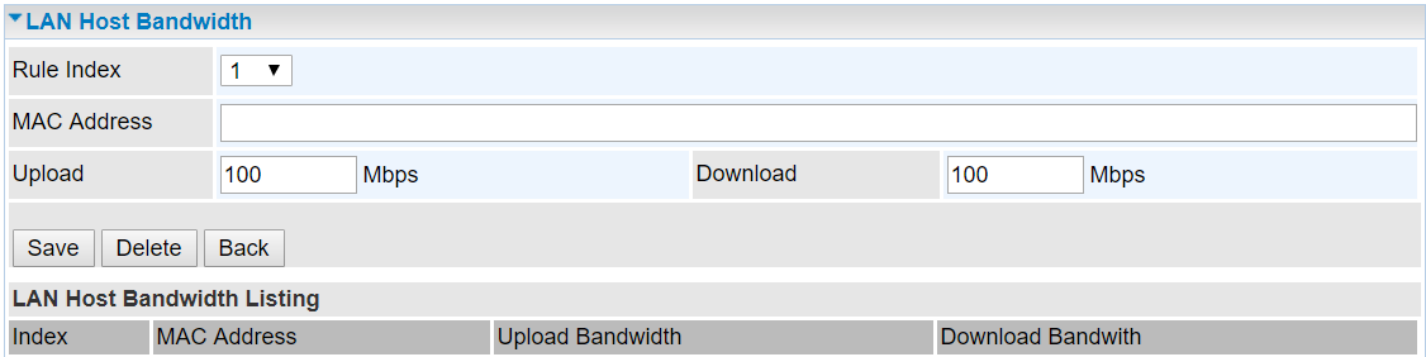


Click **Specific Bandwidth Limitation** to change the traffic bandwidth of the downstream and upstream rates.

Click **Save** to apply settings.

Bandwidth Limitation on LAN Host

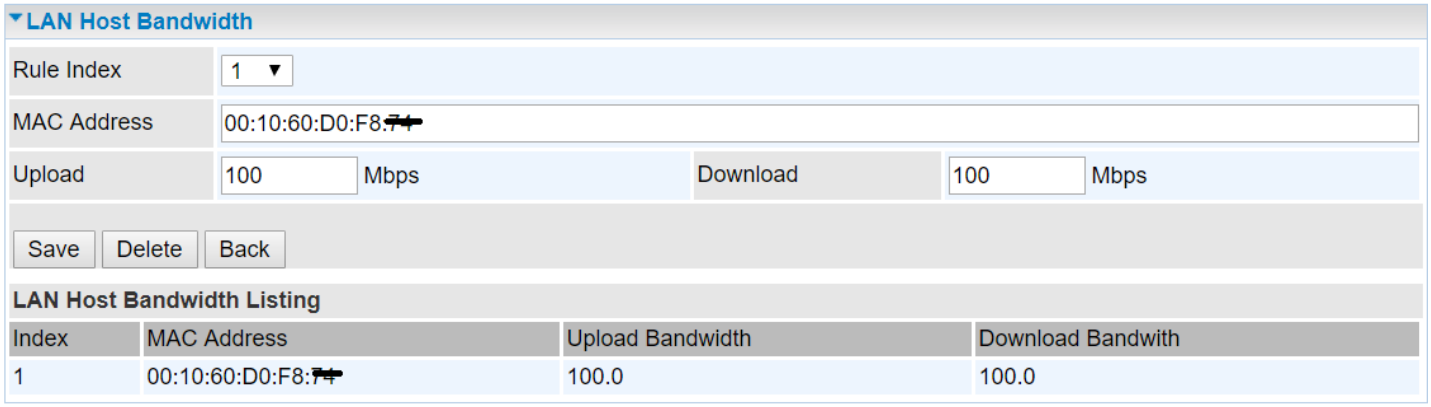
Manually apply a bandwidth restriction for a specific LAN ethernet device, up to 32 devices are allowed.



Rule Index: Index marking for each rule up to maximum of 32.

MAC Address: Enter the LAN MAC address of an ethernet device you wish to limit the bandwidth consumption. Enter the MAC addresses in XX:XX:XX:XX:XX:XX format.

Example:



Upload Speed / Download (Mbps): Specific the allowed bandwidth for the ethernet device.

Click **Save** to apply settings.

To Remove a Policy: Simply select the Index then hit the **Delete** button to remove from the list.

SW QoS Rule

Setup a priority given to a policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth.

SW QoS Rule			
Rule Index	1 ▼		
Application			
Direction	LAN to WAN ▼	WAN Interface	ALL ▼
QoS Type	Limited(Maximum) ▼	Priority	High ▼
Bandwidth Type	◉ Share Bandwidth ○ Bandwidth per Host		
Bandwidth	Mbps	DSCP Marking	Disable ▼
Protocol	Any ▼		
Internal IP Address	0.0.0.0 ~ 0.0.0.0 *2	Internal Port	0 ~ 0 *3
External IP Address	0.0.0.0 ~ 0.0.0.0 *2	External Port	0 ~ 0 *3
Note *1 : The hardware acceleration of packet processing will be disable if active SW QoS.			
Note *2 : 0.0.0.0 ~ 0.0.0.0 means all IPs			
Note *3 : 0 ~ 0 means all Ports			
Save Delete			

Rule Index: Index marking for each rule up to maximum of 16.

Application: Assign a name that identifies the new QoS application rule.

Direction: Specific the direction mode, LAN to WAN (upload) or WAN to LAN (download), for this QoS application.

WAN Interface: Select a WAN interface connection to allow external access to your internal network.

- **(Direction) LAN to WAN (Upload) – WAN Interface** is fixed to **ALL.**
- **(Direction) WAN to LAN (Download) – WAN Interface** can be selected from the list.

QoS Type Choose ***Limited*** (Maximum) or ***Guaranteed*** (Minimum) to specify the date rate is allowed for this policy.

- **Limited(Maximum) – Priority** is automatic set to High.
- **Guaranteed (Minimum) – Priority** can be selected from High, Normal or Low.

Bandwidth Type: It is available when select **Limited (Maximum)** of QoS Type.

- **Share Bandwidth –** The specific bandwidth, can be configured below, is shared by all devices within the internal IP address/range.
  - **Example:** Share Bandwidth**,** Bandwidth set to 100Mbps, Internal IP Address: 192.168.1.100-104 (total of 5).

    Result: IP 192.168.100-104, those 5 devices will share bandwidth of 100Mbps.
- **Bandwidth per Host –** Each of the LAN devices within the internal IP address/range obtain the specific bandwidth configured below.
  - **Example:** Bandwidth per Host**,** Bandwidth set to 50Mbps, Internal IP Address: 192.168.1.100-104 (total of 5).

    Result: The IP address/device, 192.168.100-104, each will obtain up to 50Mbps bandwidth/data to access to the Internet.

Bandwidth (Mbps): Specify the bandwidth for this application.

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

Protocol: Select a protocol from the drop-down list.

Internal IP Address: The LAN IP address associates with the internal LAN devices you want to give control.

- **Internal Port:** The Port number on the LAN side, it is used to identify a service.

External IP Address: The IP address / range from the remote / WAN side.

- **External Port:** The Port number from the remote / WAN side.

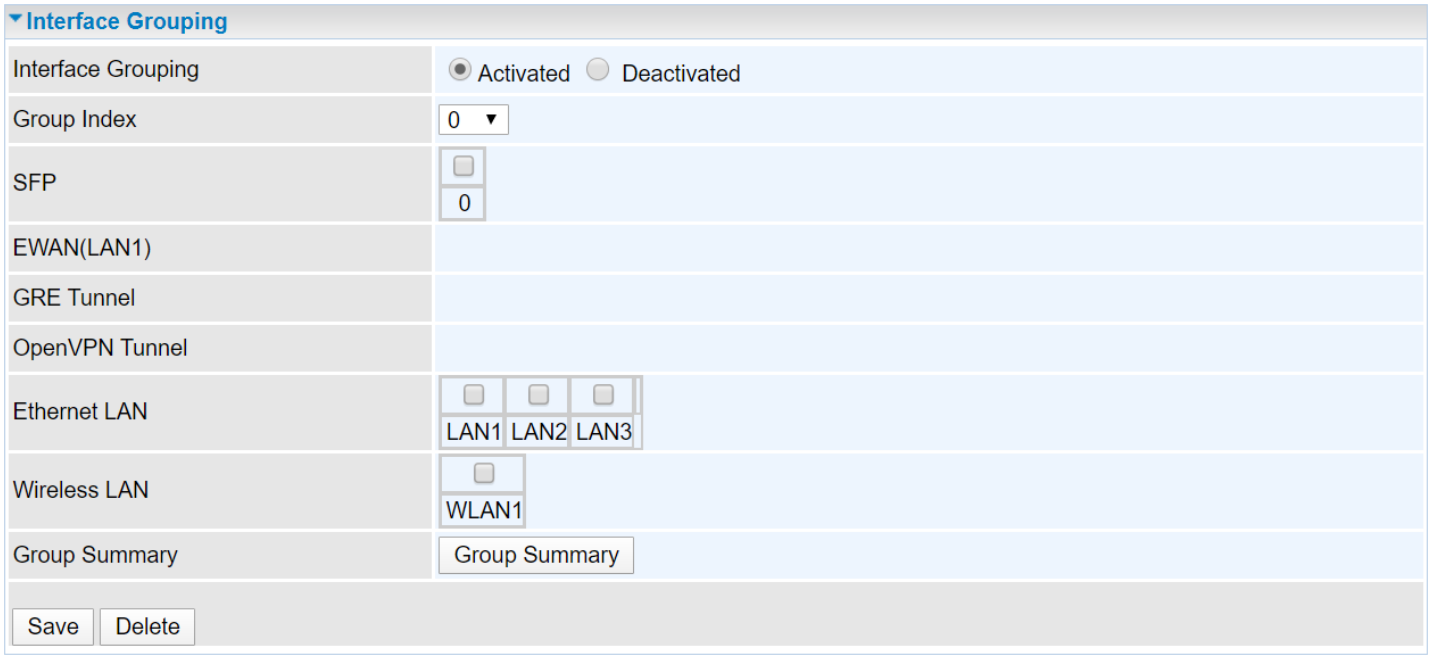
Click **Save** to apply settings.

To Remove a Policy: Select the Rule Index then hit the **Delete** button to remove from the list.

Interface Grouping

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

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



Interface Grouping: Select **Yes** to enable Interface Grouping feature.

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

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

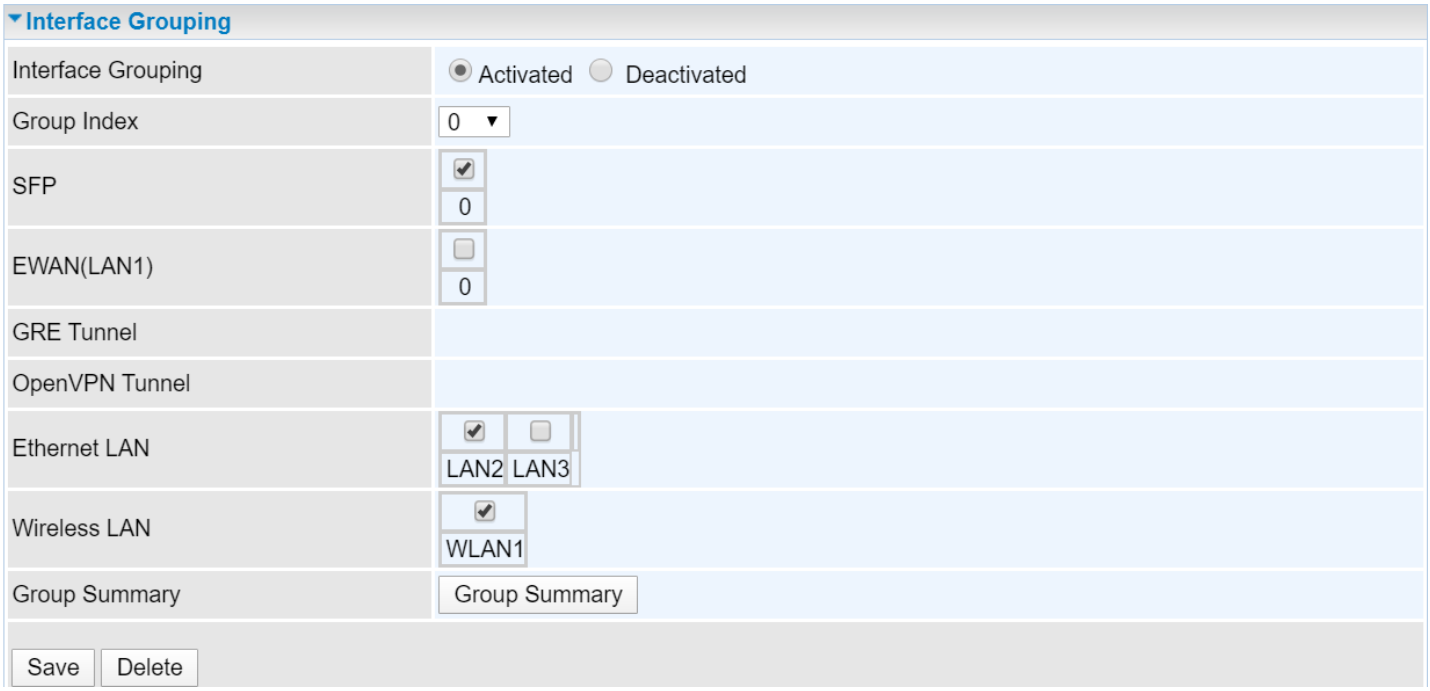
SFP / GRE Tunnel / OpenVPN Tunnel / Ethernet LAN / Wireless LAN: If the interface is ready/available, the click box will be shown.

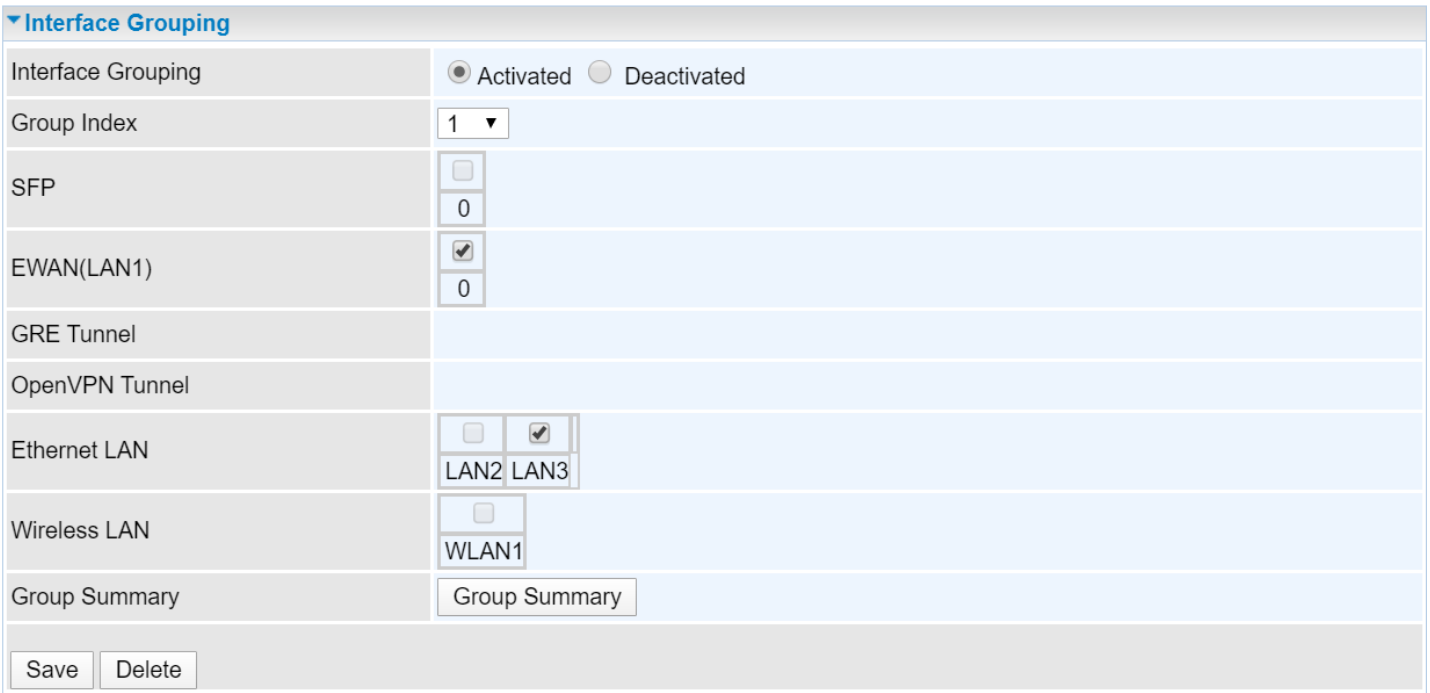
Group Summary: Click to review all configured grouping information.

Example: Create two WAN services, SFP and EWAN

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

Group Index	Group Port
0	SFP, LAN2, WLAN1
1	EWAN, LAN3





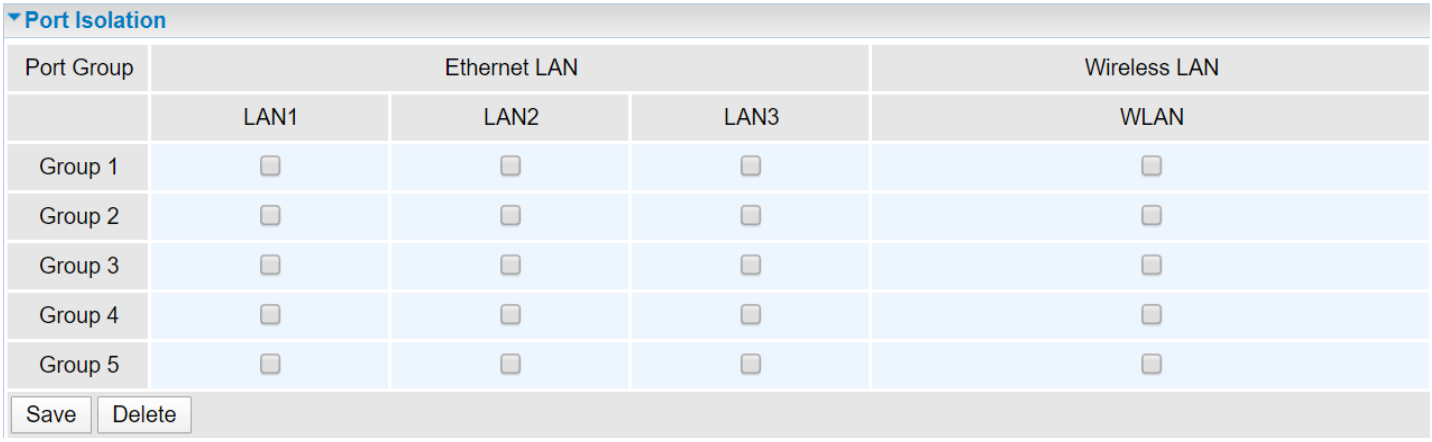
Click **Group Summary** to show the configuration results.

Interface Grouping

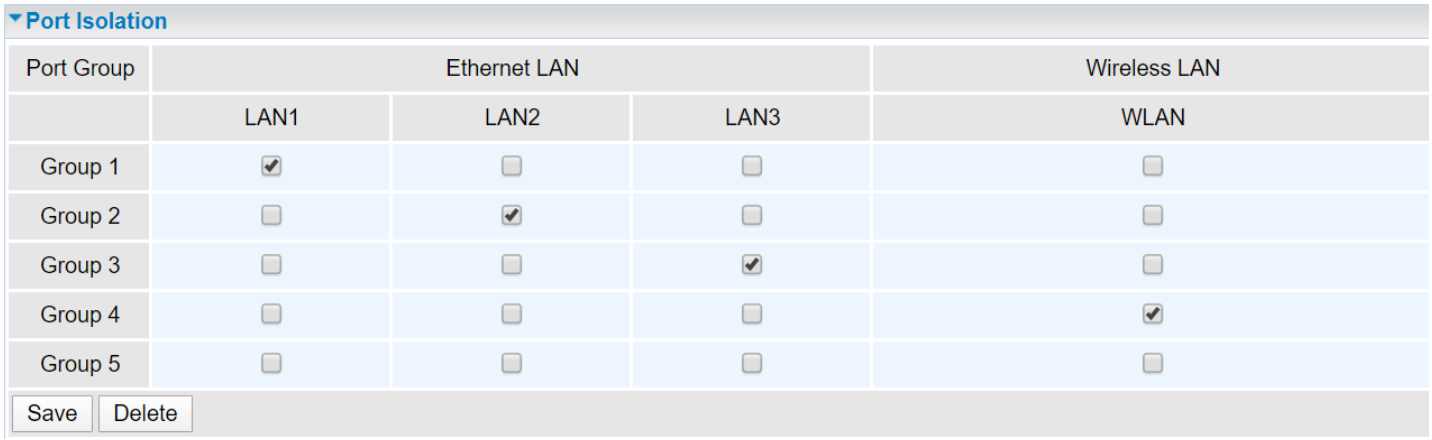
Group ID	Group Interface
0	SFP,LAN2,WLAN1
1	EWAN(LAN1),LAN3

Port Isolation

Port isolation is to prevent LAN (Wired or Wireless) devices, e.g. PC, Notebook, to associate or communicate with each other devices. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.



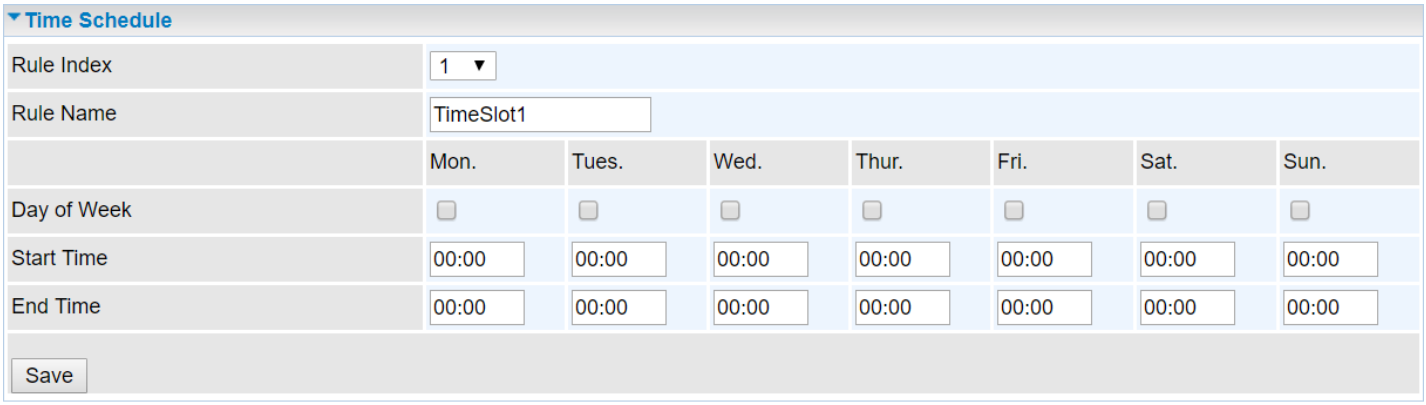
The most typical one example is to isolate all port from each other shown below. Each port has its own group; under this circumstance, devices connected to each port have no access to other devices connected to other ports. This is a special example, and users can change the settings to determine how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



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.



Time Index: The rule indicator (1-16) for identifying each timeslot.

Name: User-defined identification for each time period.

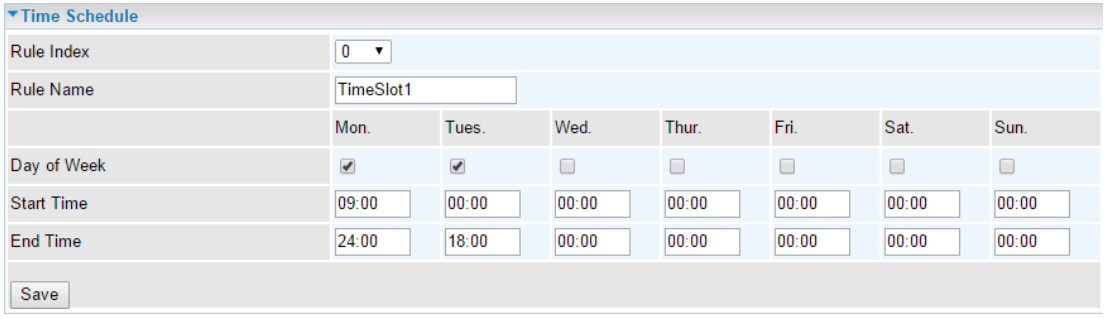
Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week".

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

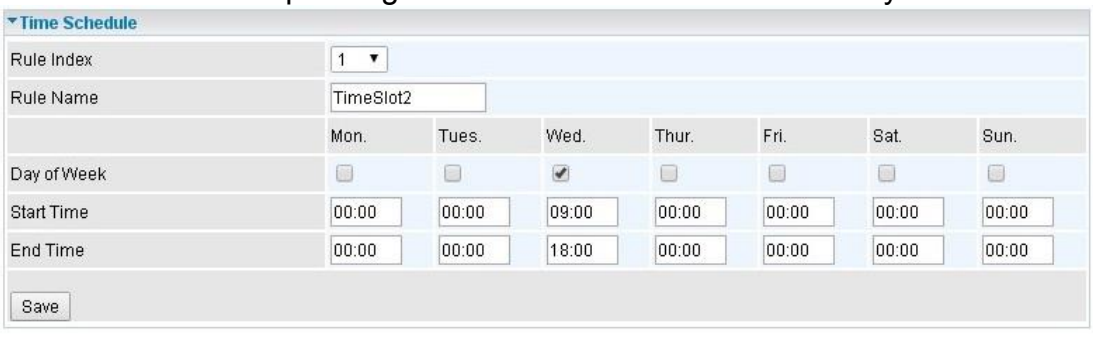
End Time: The ending point of the interval for the timeslot, anytime in 00:00 – 24:00.

Click **Save** to apply your settings.

Example, you can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

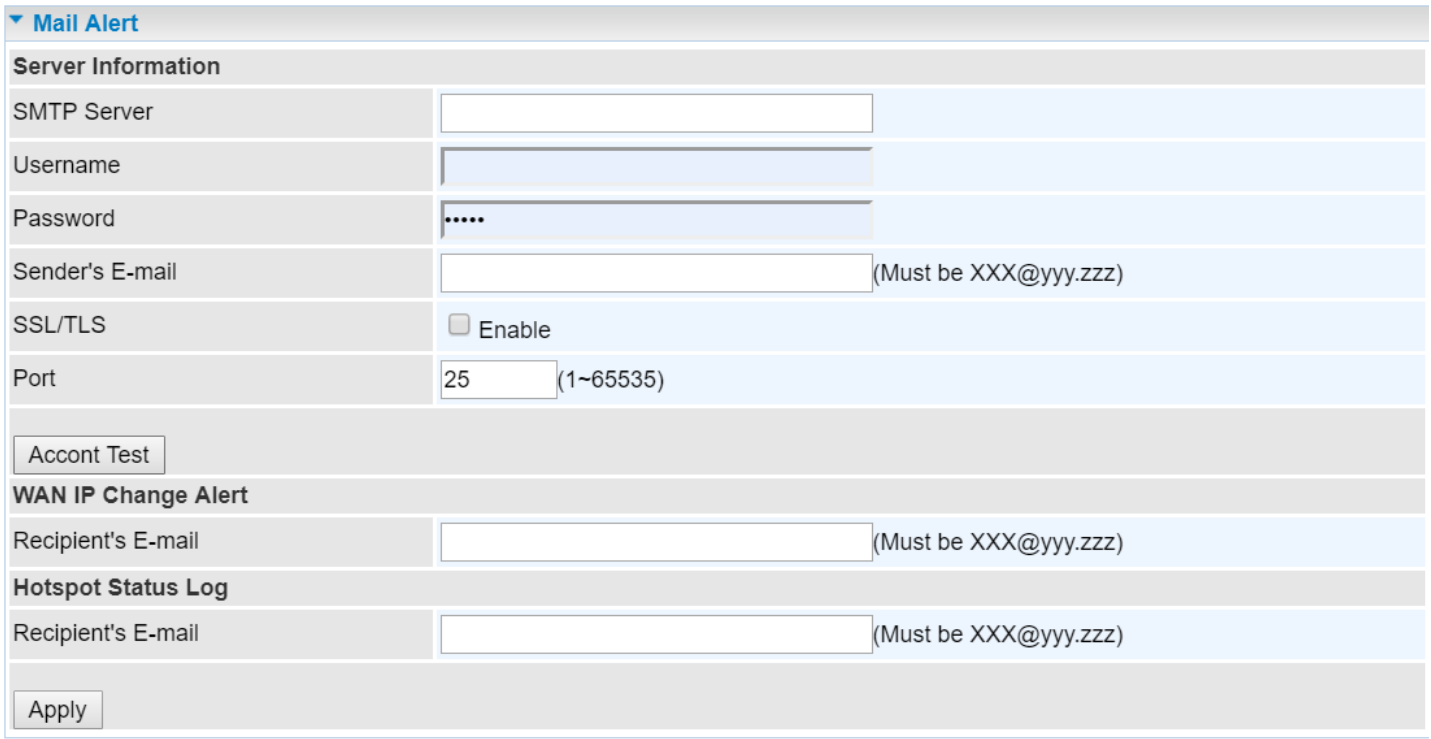


Another TimeSlot2 spanning from 09:00 to 18:00 of Wednesday



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.



Server Information

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: Click the button to test the connectivity and feasibility to your sender's e-mail.

WAN IP Change Alert

Recipient's Email (WAN IP Change Alert): Enter a valid e-mail address to receive an alert message when WAN IP change has been detected.

Recipient's Email (Hotspot Status Log): Enter a valid e-mail address to receive hotspot status log email.

Click **Apply** button to save settings.

VPN

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

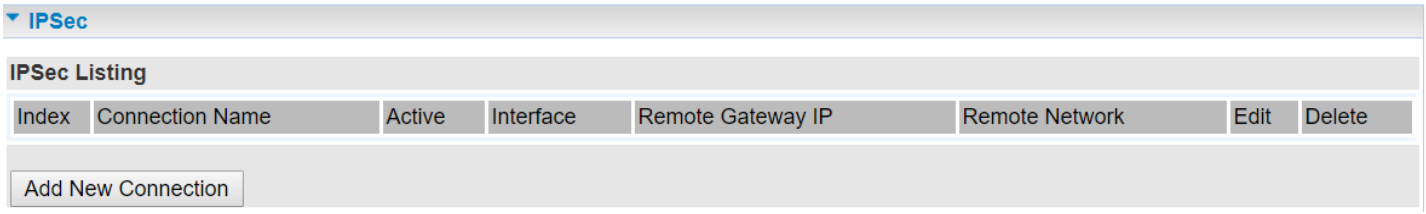
BEC 9900VA supports IPSec, PPTP, L2TP, GRE, and OpenVPN Server / Client VPN features.

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.

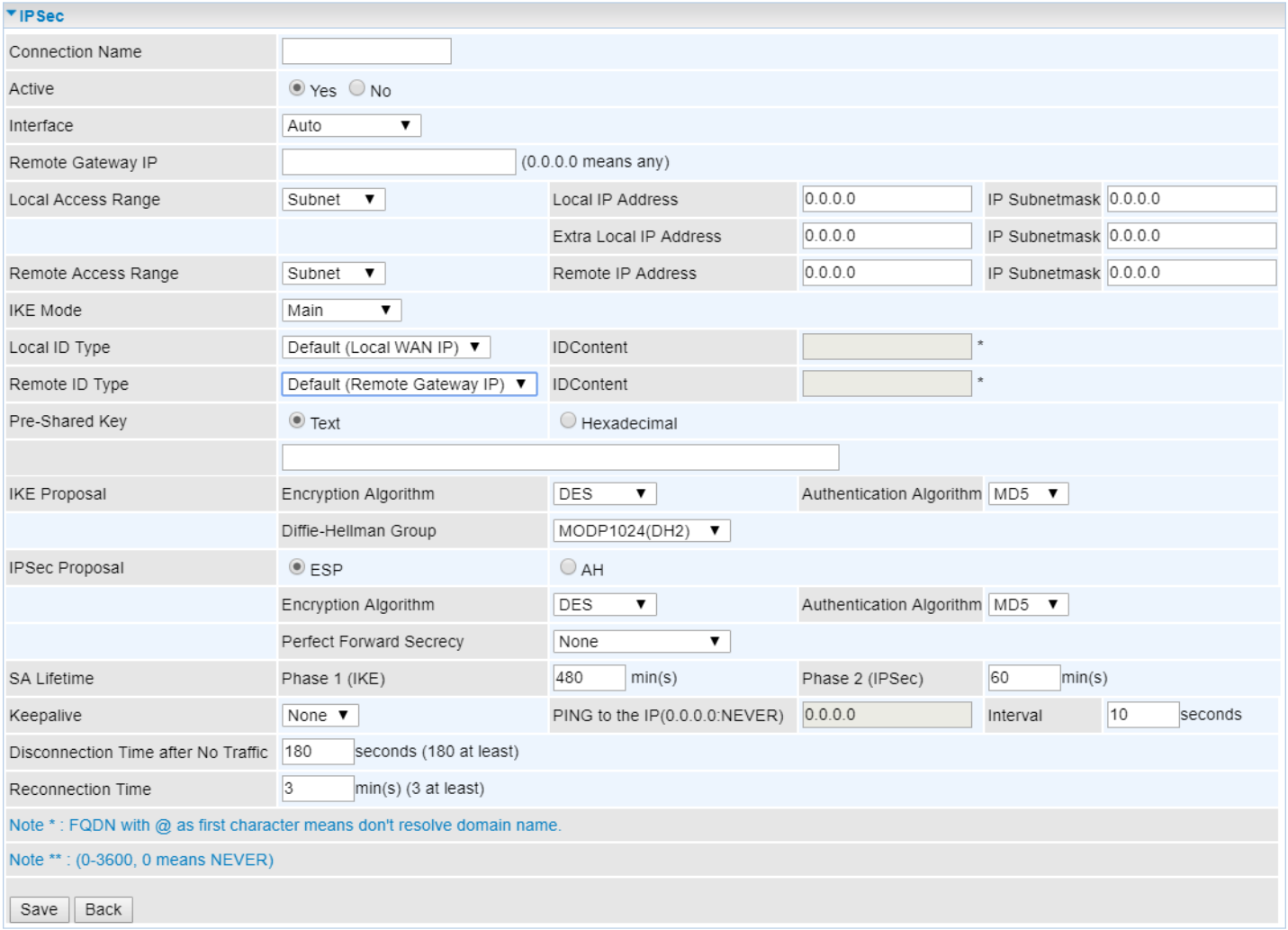
IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

A total of 8 IPSec tunnels can be added.



Click **Add New Connection** to create a new IPSec profile.

IPSec Connection Setting



Connection Name: Enter a name or description for this connection/profile.

Active: Yes to activate the connection.

Interface: Select a WAN interface to establish a tunnel with the remote VPN device. **Auto** allows system to automatically initiate a connection via current connected WAN interface.

Remote Gateway IP: The WAN IP address of the remote VPN device. Enter **0.0.0.0** for unknown remote WAN IP address – only the peer can initiate the tunnel connection.

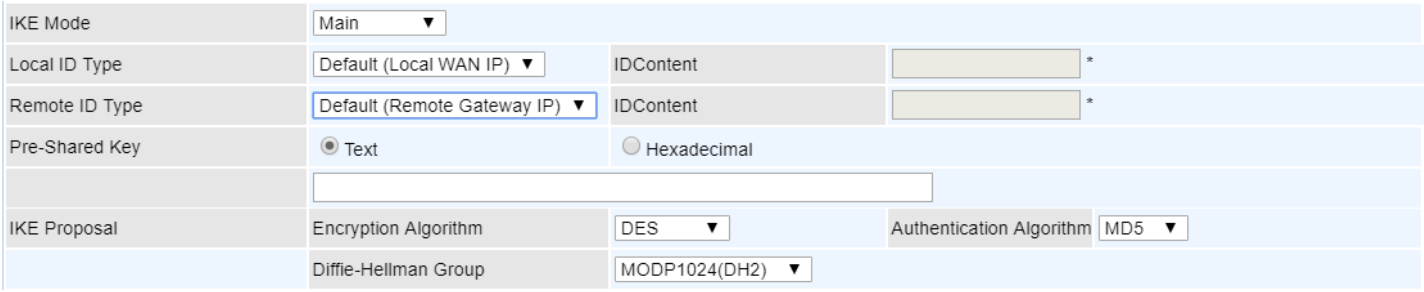
Local Access Range: Set the IP address or subnet of the local network.

- **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.

Local ID Type / **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).

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).

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

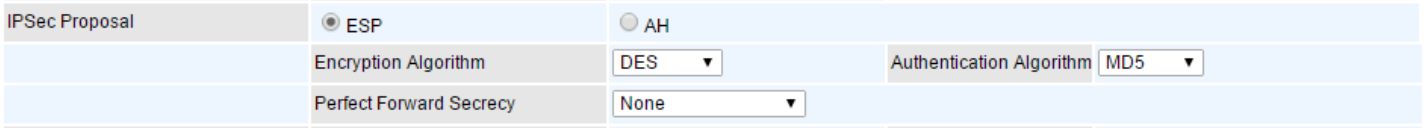
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

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

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

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

IPSec 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.

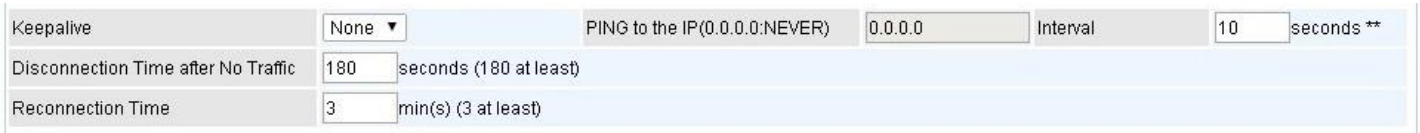
Perfect Forward Secrecy: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

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, and 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 Connection Keep Alive



Keep Alive:

- **None:** Disable. The system will not detect remote IPSec peer is still alive or lost. The remote peer will get disconnected after the interval, in seconds, is up.
- **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.

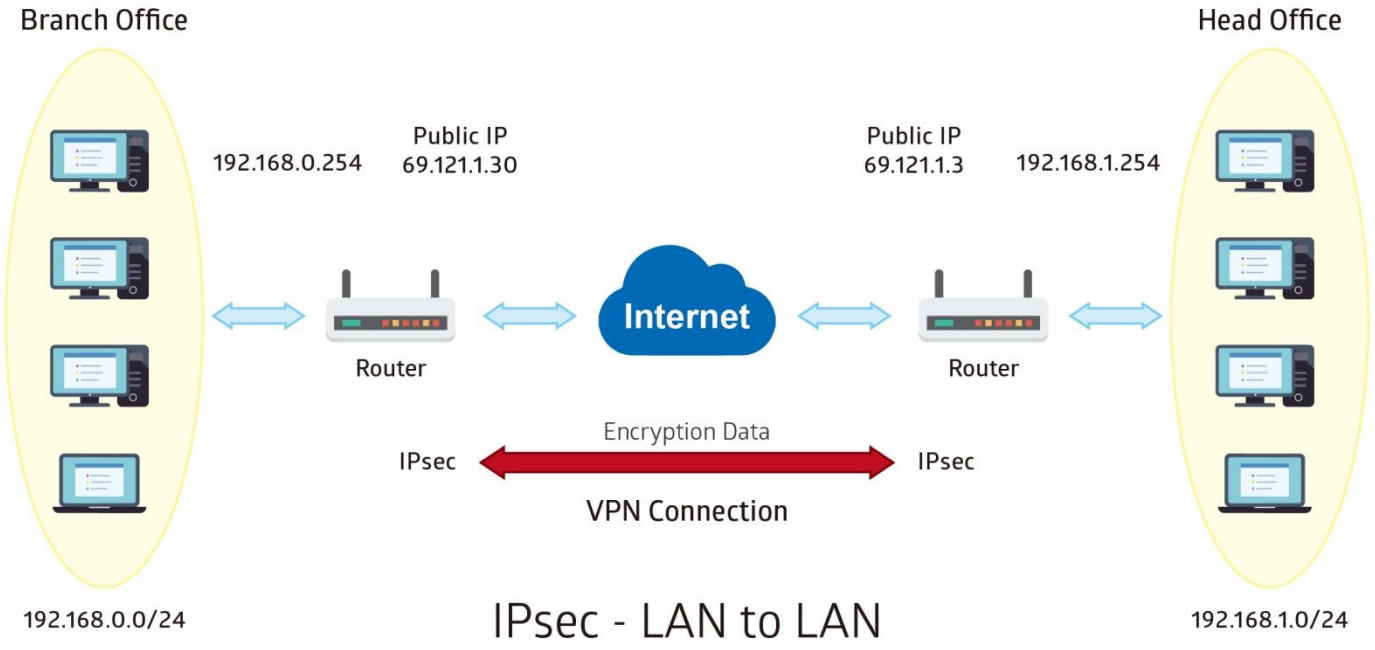
Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply settings.

Examples: IPSec – Network (LAN) to Network (LAN)

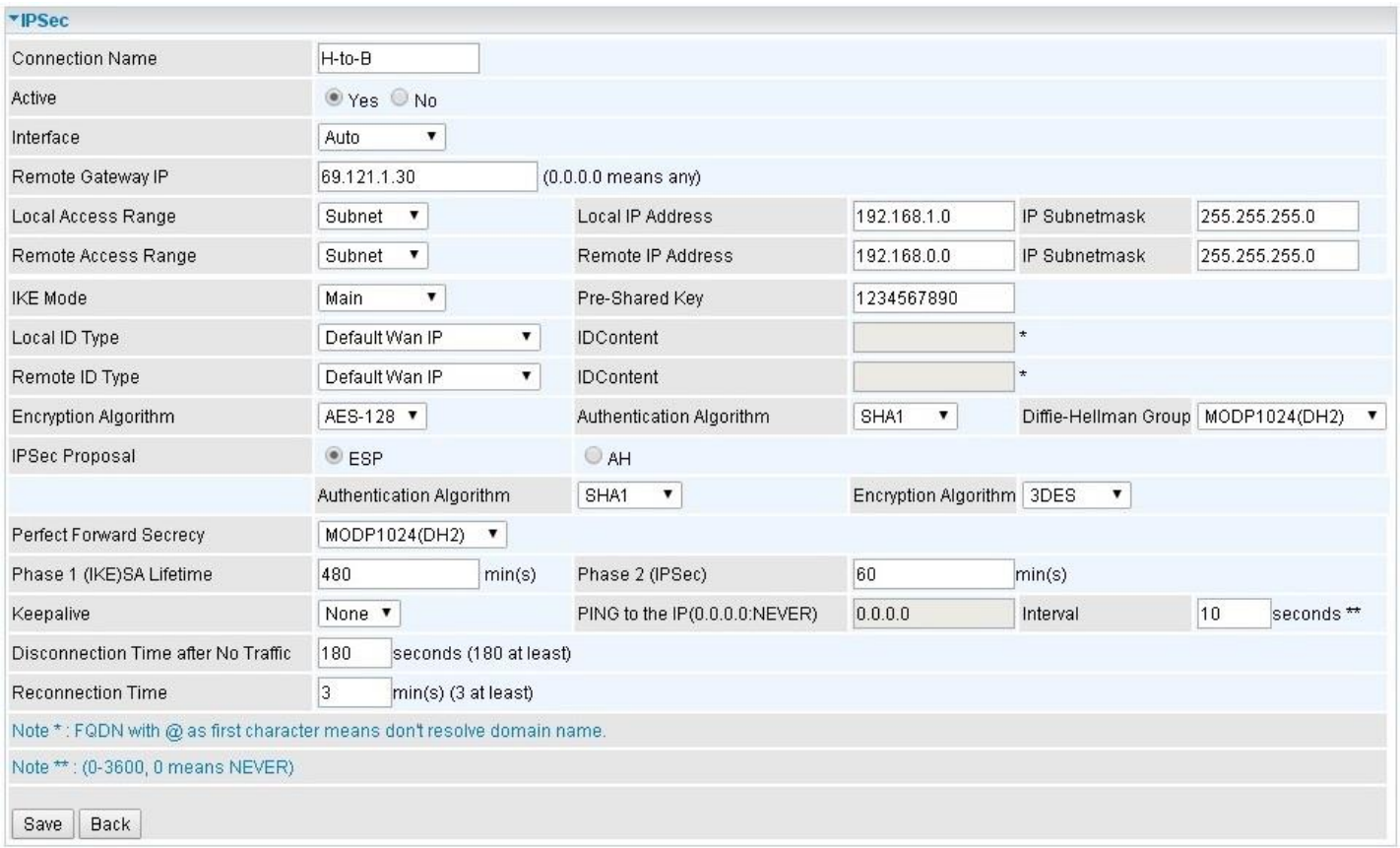
Two of the BEC 9900VA devices want to setup a secure IPSec VPN tunnel

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



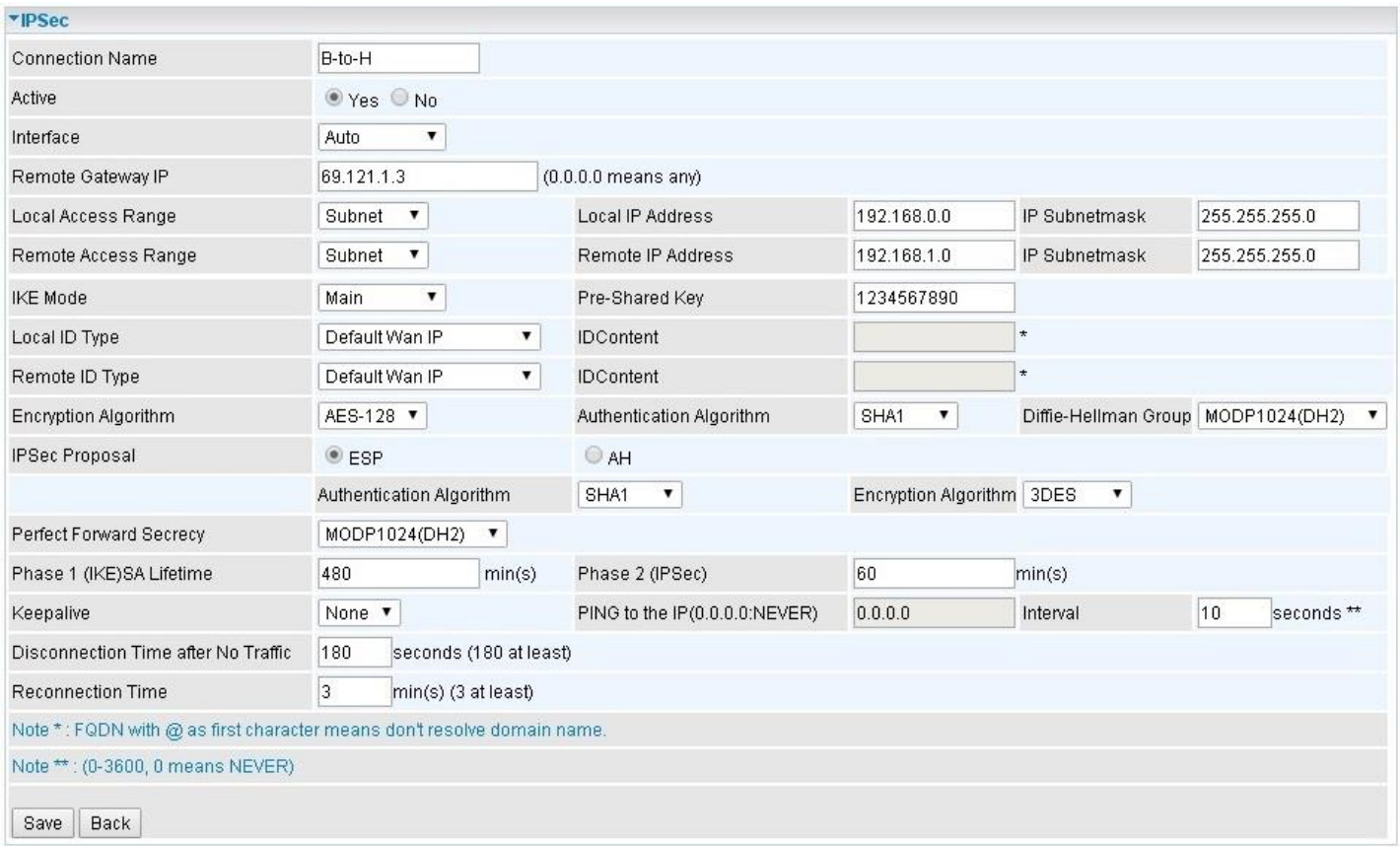
Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-B	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.0.0	
Remote Network 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)	



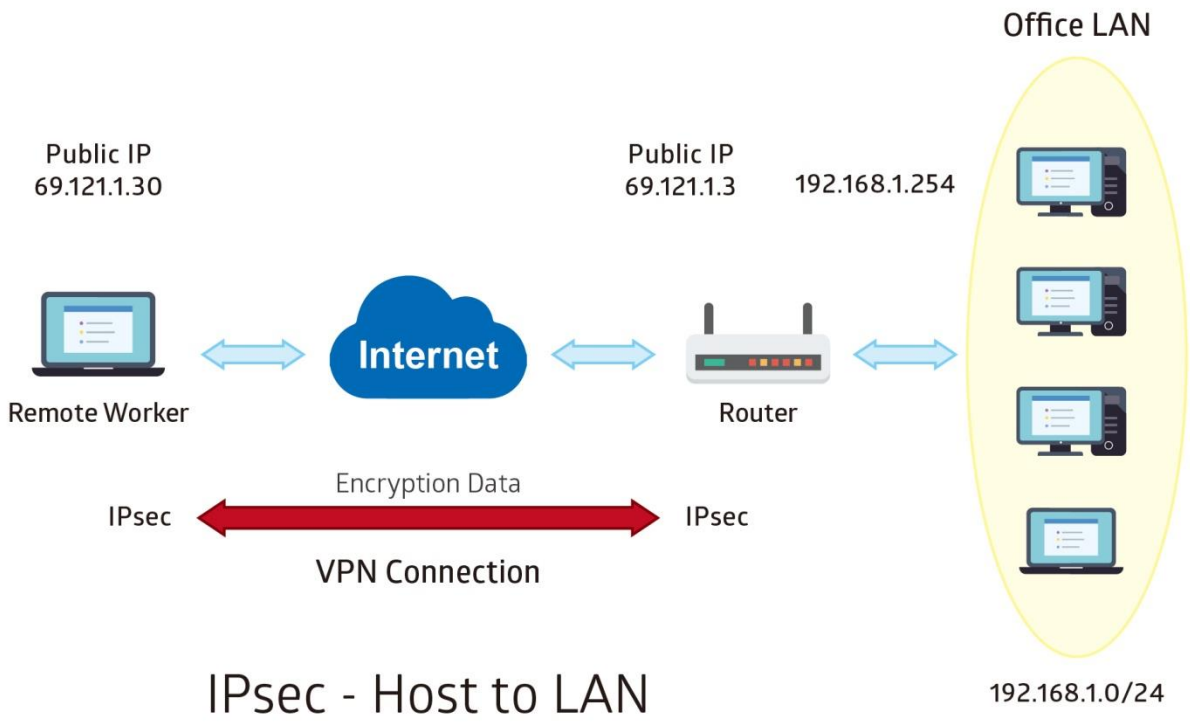
Branch Office Side:

Configuration Settings		Description
Connection Name	B-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.3	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.0.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.1.0	
Remote Network 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)	



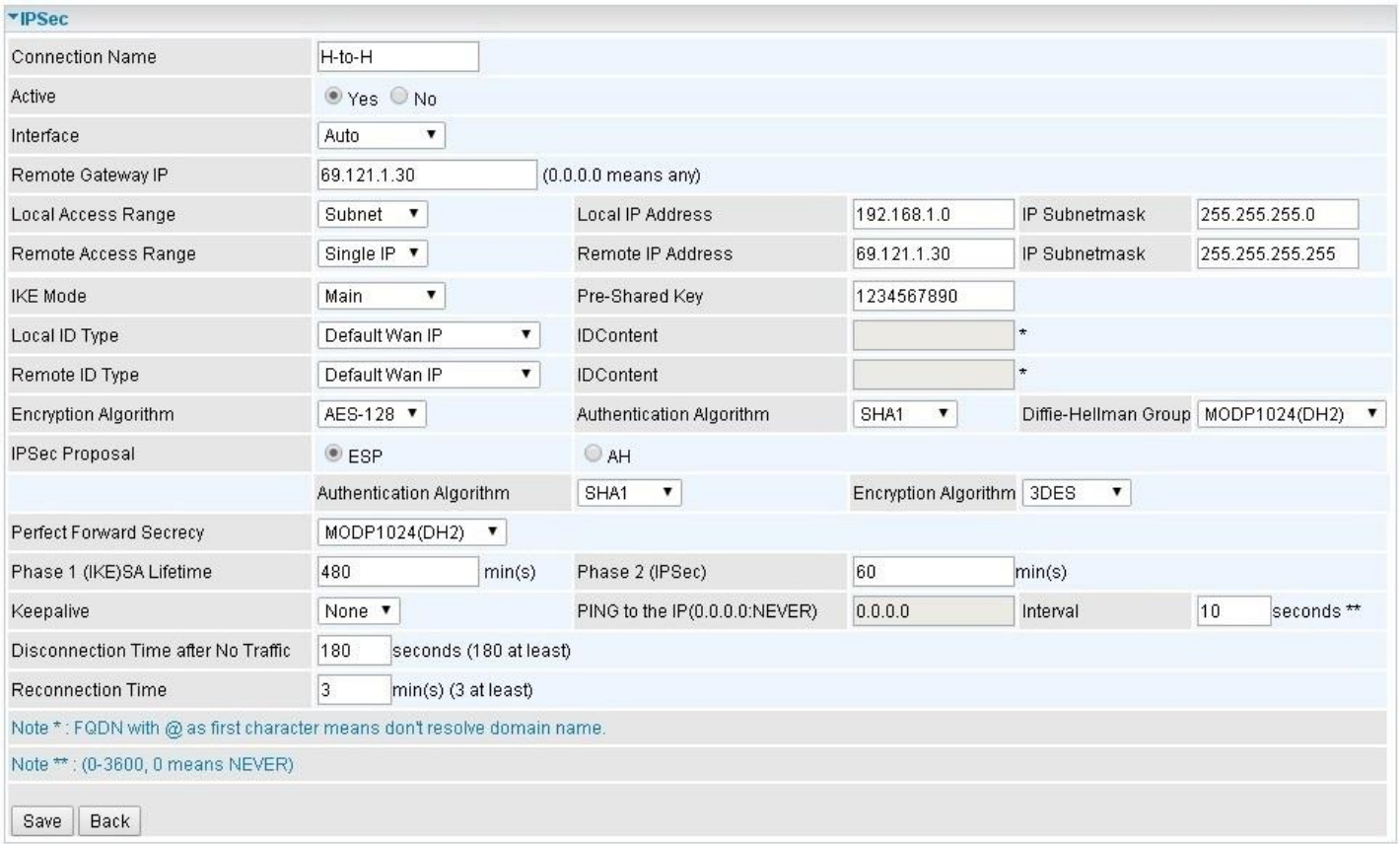
Examples: IPSec – Remote Employee to BEC 9900VA Connection

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



Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office LAN network information
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Signal IP	Remote worker IP address
Remote Network IP Address	69.121.1.30	
Remote Network 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)	

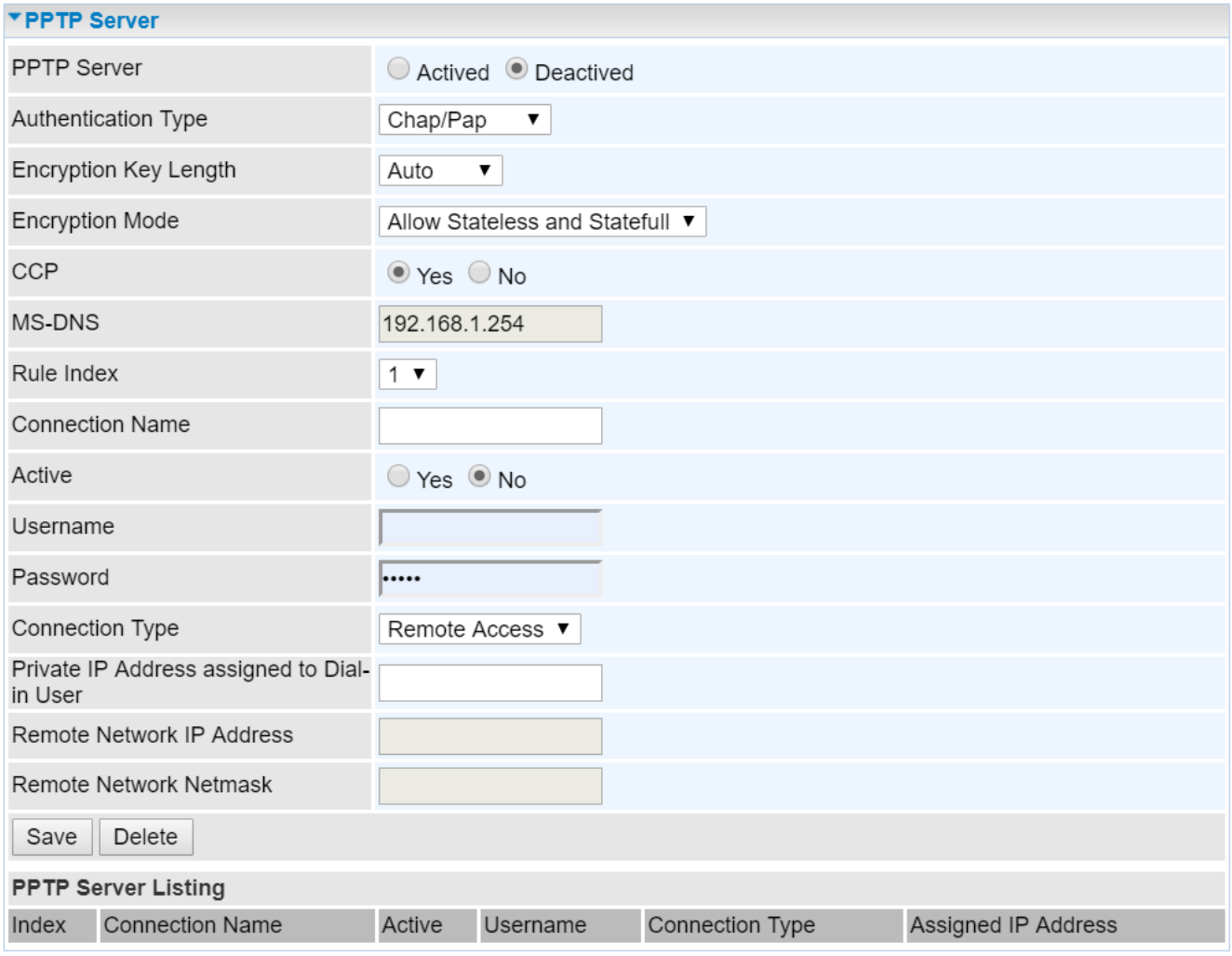


PPTP Server

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



PPTP Server: Select **Activate / Deactivate** to enable or disable the PPTP Server.

Authentication Type: Pick an authentication type from the drop-down list. 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: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

MS-DNS: Assign a DNS server or use router default IP address to be the MS-DNS server IP address.

Rule Index: The numeric rule indicator for PPTP server. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

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

Username / Password: Enter the username / password for this profile.

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

Remote Network IP Address: Enter the subnet IP of the remote LAN network.

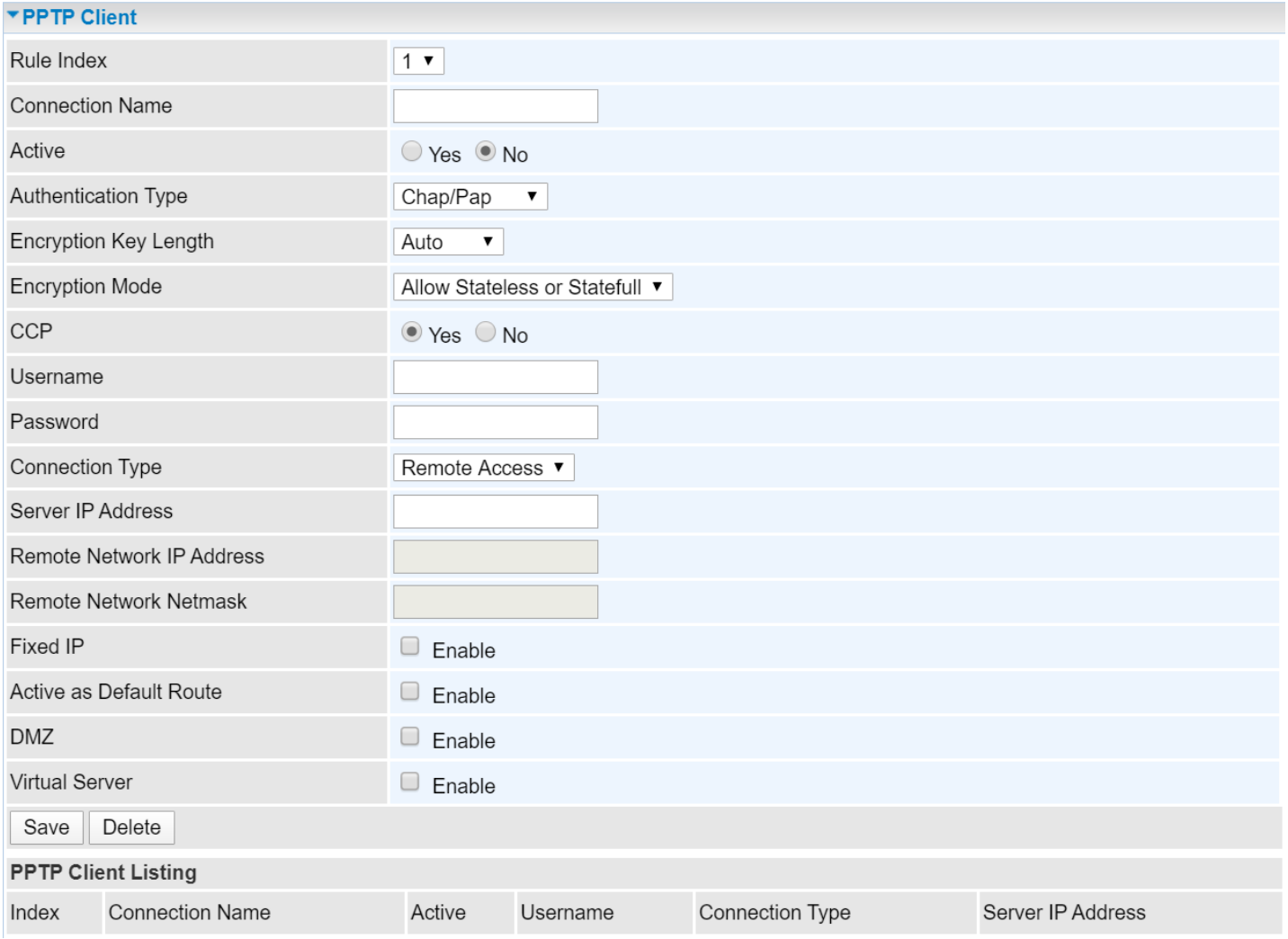
Remote Network Netmask: Enter the Netmask of the remote LAN network.

Click **Save** to apply settings.

PPTP Client

Establish a PPTP tunnel over Internet to connect with a PPTP server.

A total of 4 PPTP Client sessions can be created.



Rule Index: The numeric rule indicator for PPTP client. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

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

Authentication Type: Pick an authentication type from the drop-down list. 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: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

Username / Password: Enter the username / password provided by the PPTP server/host.

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: Enter the subnet IP of the server/host LAN network.

Remote Network Netmask: Enter the Netmask of the server/host LAN network.

Fixed IP: Specific and reserve a LAN IP address from the remote PPTP server. Click **Enable** then enter the request IP address.

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.

DMZ: Specific an internal DMZ host to add an additional layer of protection to the network. All received incoming packets will first go through the Virtual Server list, if no service redirection required, then packets can get forwarded to the DMZ host. Click **Enable** then enter the DMZ IP address.

Virtual Server: Click **Enable** to enable redirection of Internet packets.

Virtual Server Index: Index marking for each rule up to maximum of 4.

Protocol: Choose the application protocol.

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

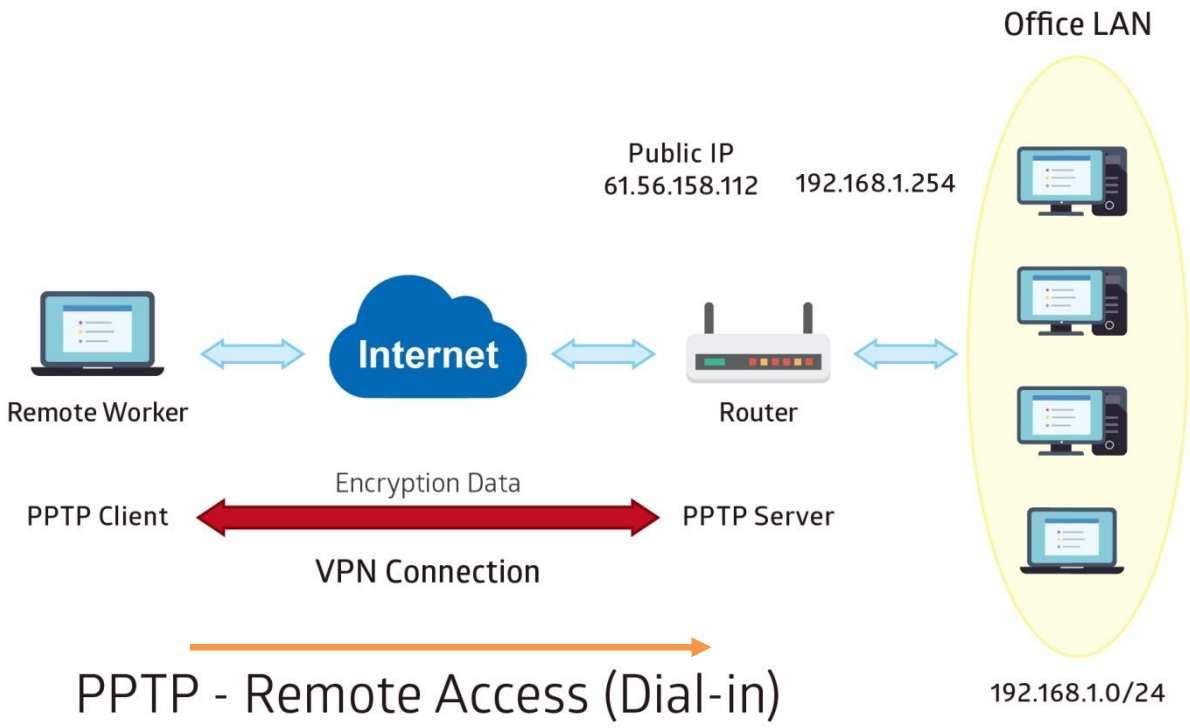
(Example: Start / End: 1000 or Start: 1000, End: 2000).

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

Local IP Address: Enter the local IP address of the default start/end port of the application / service.

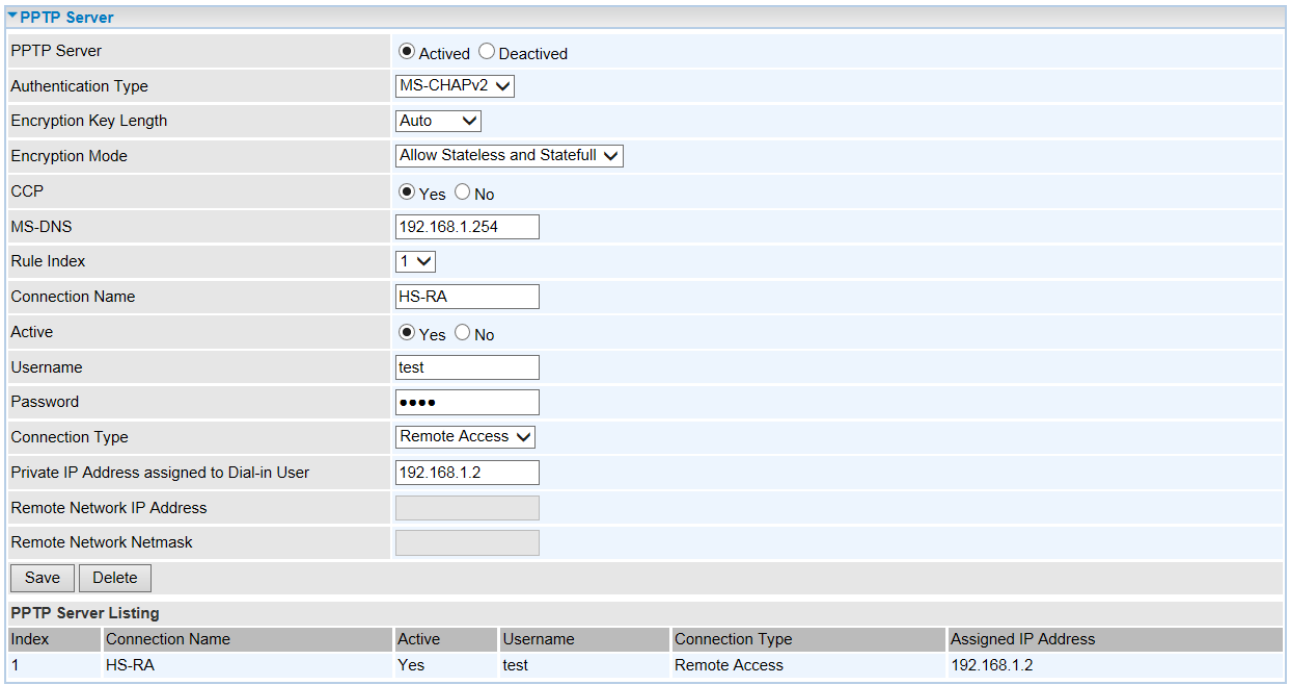
Click **Save** to apply settings.

Example: PPTP – Remote Employee Dial-in to BEC 9900VA



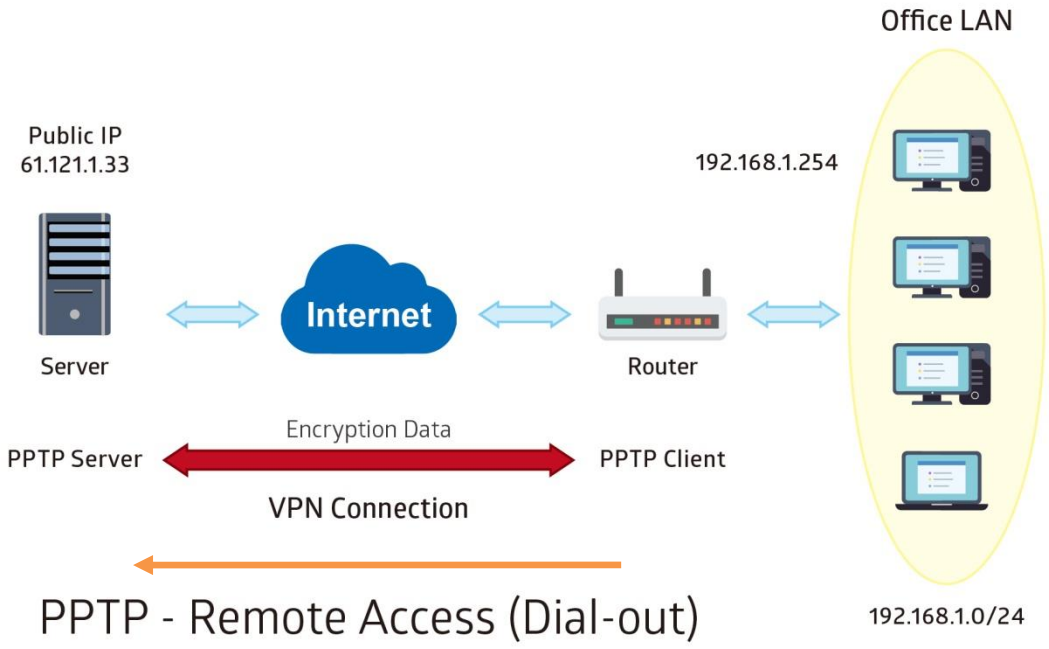
The input IP address 192.168.1.2 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created from the device to a PPTP client to dial-in to the network.
Password	test	
Connection Type	Remote Access	Remote access for a dial-in
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client



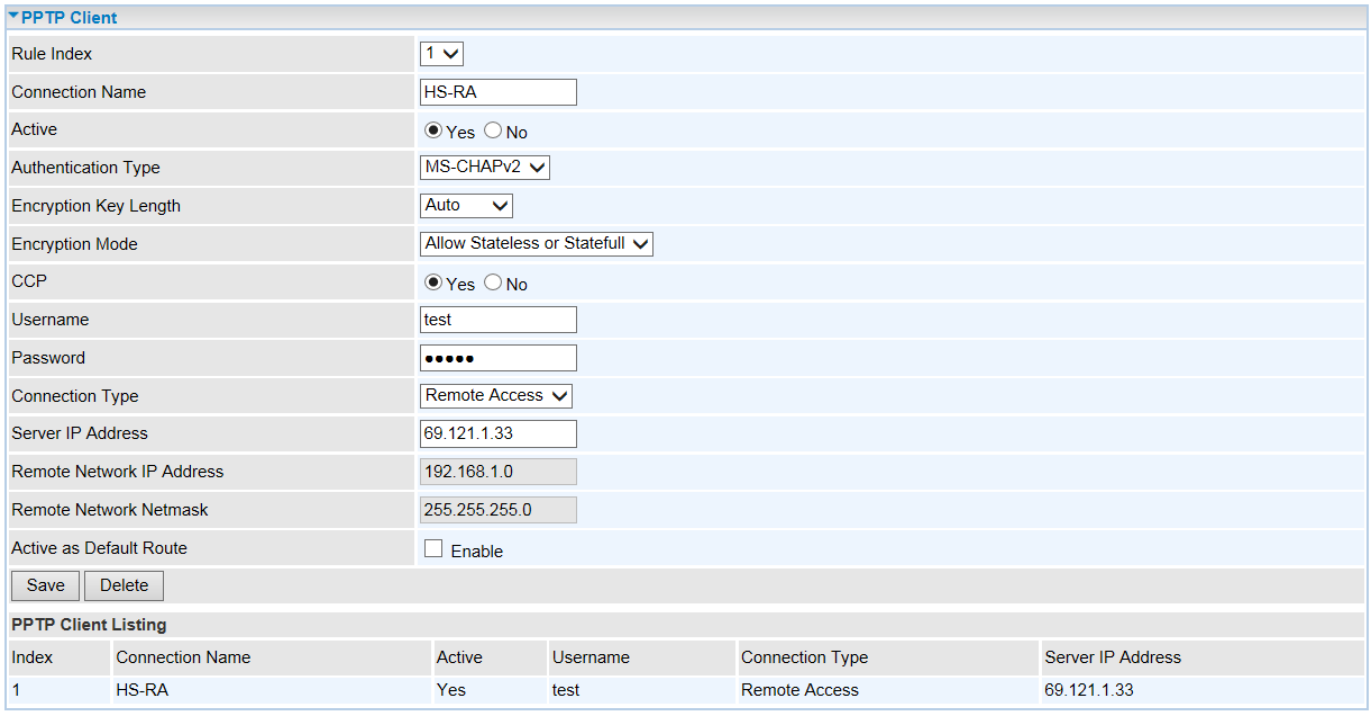
Example: PPTP – Remote Employee Dial-out to BEC 9900VA

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



PPTP Server WAN IP address is 61.121.1.33 of the Headquarter office.

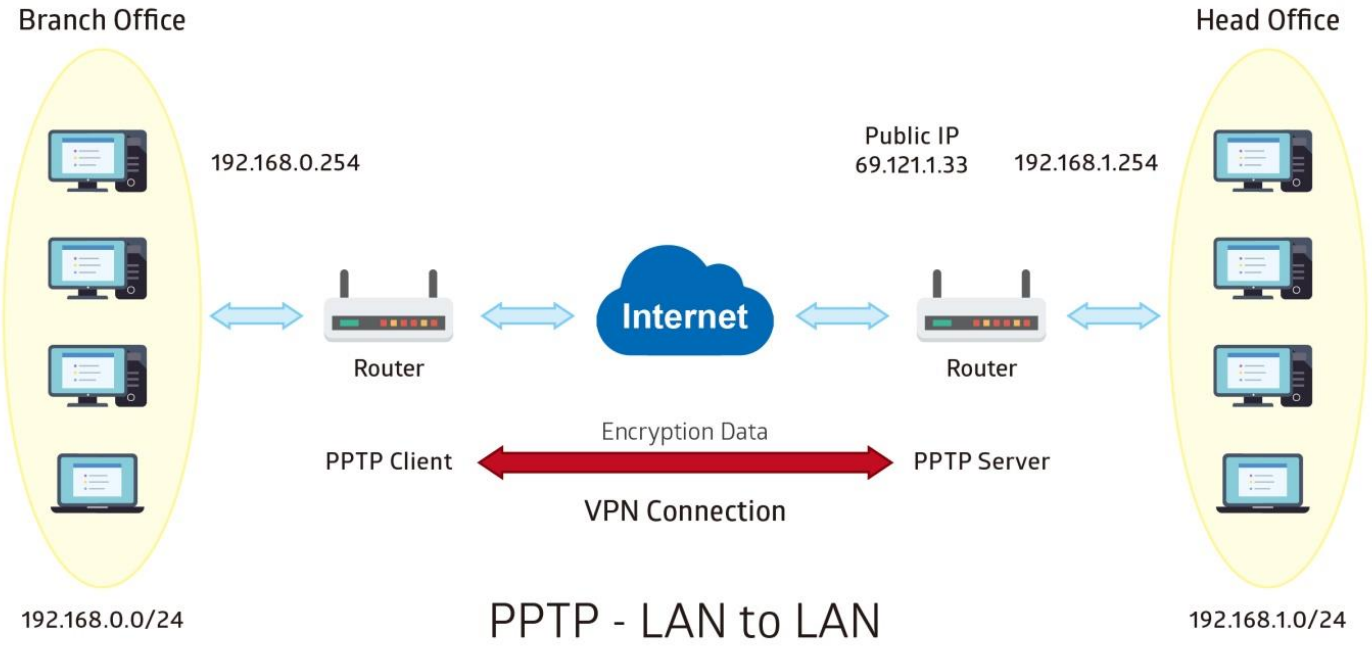
Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the PPTP server for PPP client to dial-in to its network.
Password	test	
Connection Type	Remote Access	Remote access for a dial-in
Server IP	61.121.1.33	VPN server WAN IP address



Example: PPTP – Network (LAN) to Network (LAN) Connection

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

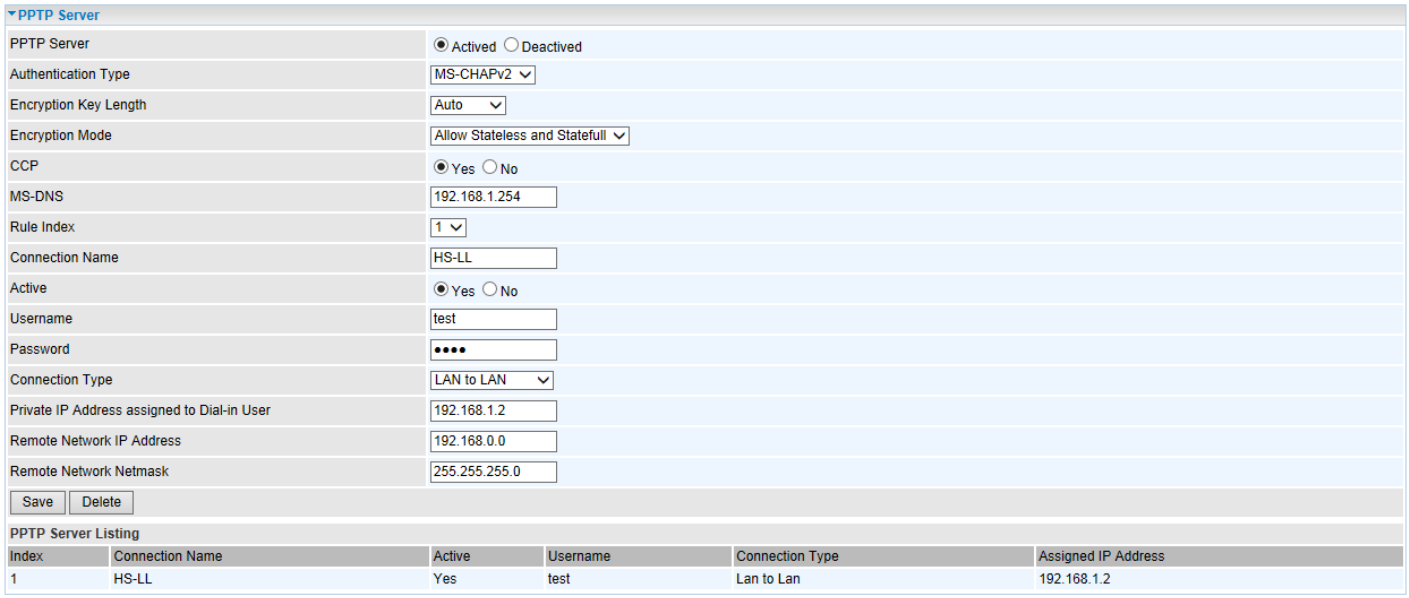
NOTE: Both office LAN networks must be in **different subnets** with the LAN-LAN application.



Configuring PPTP Server in the Headquarter 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 Headquarter office LAN.

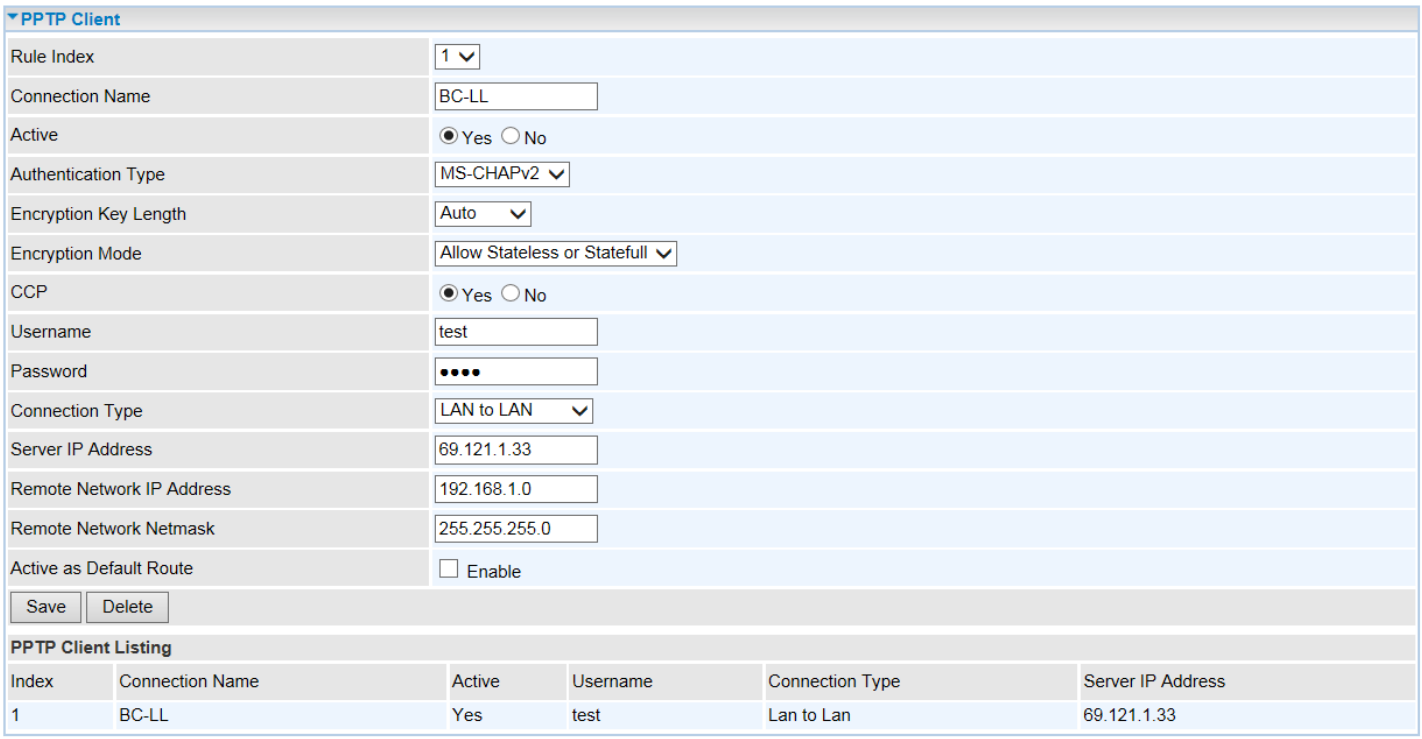
Configuration Settings		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created for a PPTP client to dial-in to its local network.
Password	test	
Connection Type	LAN to LAN	LAN to LAN connection
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



Configuring PPTP Client in the Branch office

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

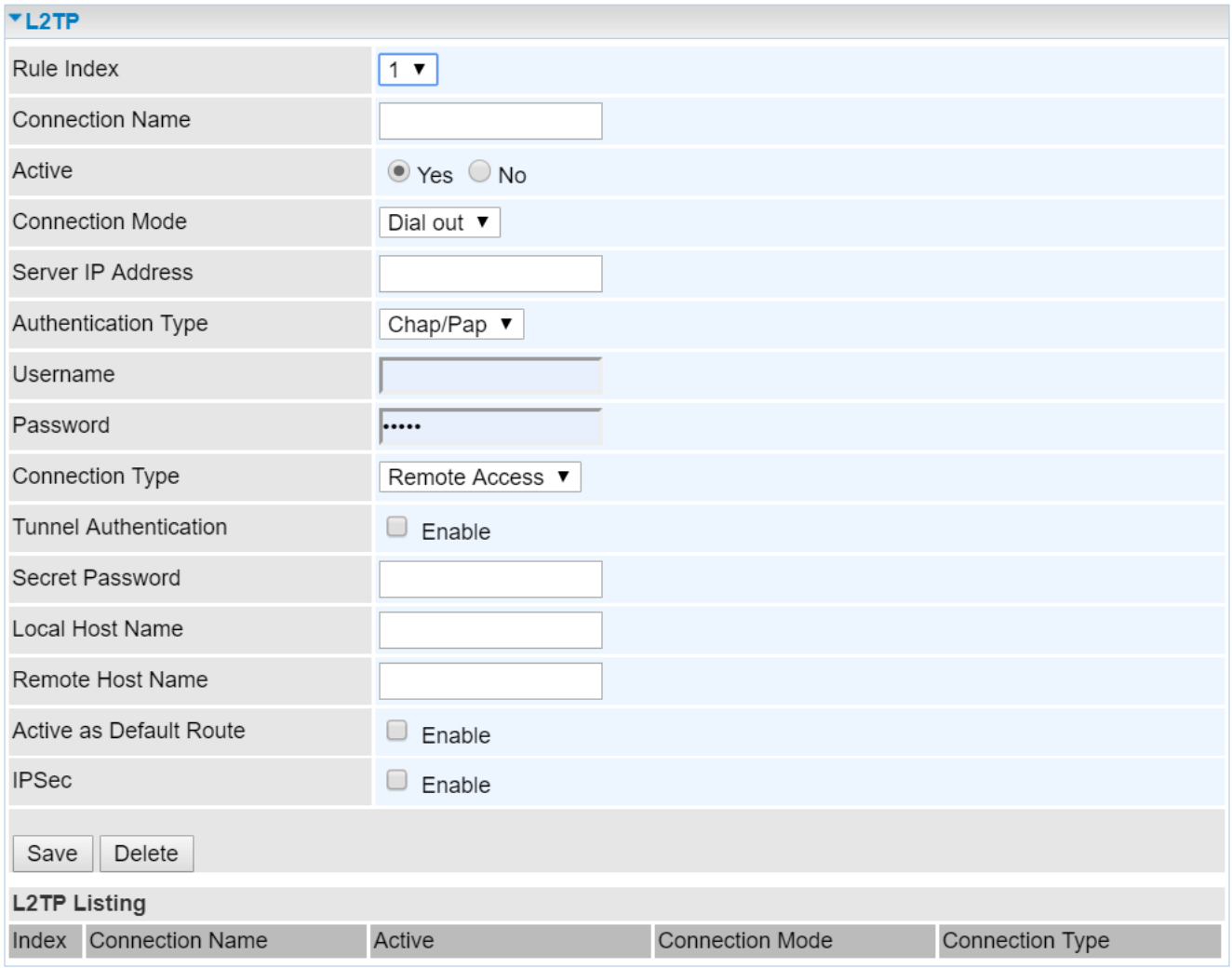
Configuration Settings		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the Headquarter Server to dial-in.
Password	test	
Connection Type	LAN to LAN	LAN to LAN connection
Server IP	69.121.1.33	Headquarter Serve WAN IP address
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



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

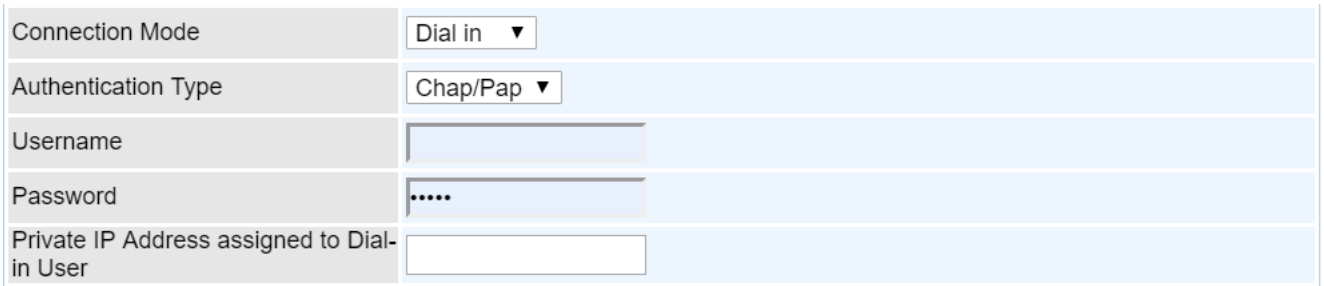


Rule Index: The numeric rule indicator for L2TP. The maximum entry is up to 8 (4 dial-in and 4 dial-out profiles).

Connection Name: Enter a description for this connection/profile.

Active: To enable or disable this profile.

Connection Mode (Dial in)



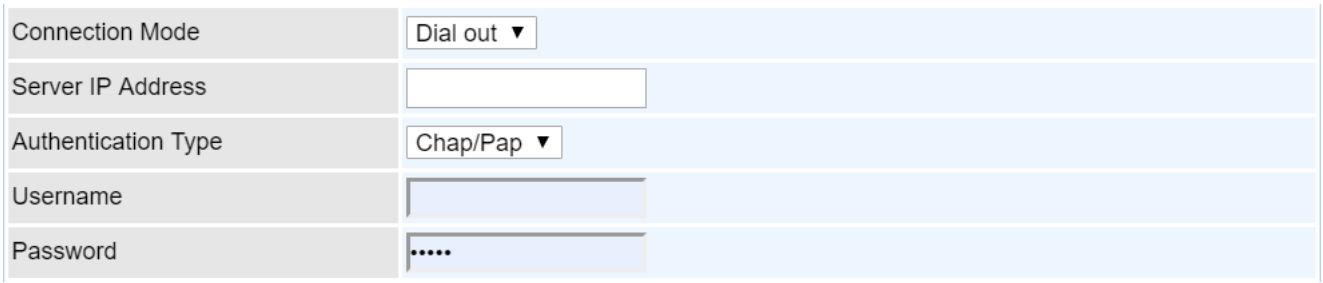
Connection Mode: Select Dial In to operate as a L2TP server.

Authentication Type: Default in 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 / Password (Server/Host): Enter the username / password for this profile.

Private IP Address Assigned to Dial-in User: The private IP to be assigned to dial-in user by L2TP server. The IP should be in the same subnet as local LAN and should not be occupied.

Connection Mode (Dial out)



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.

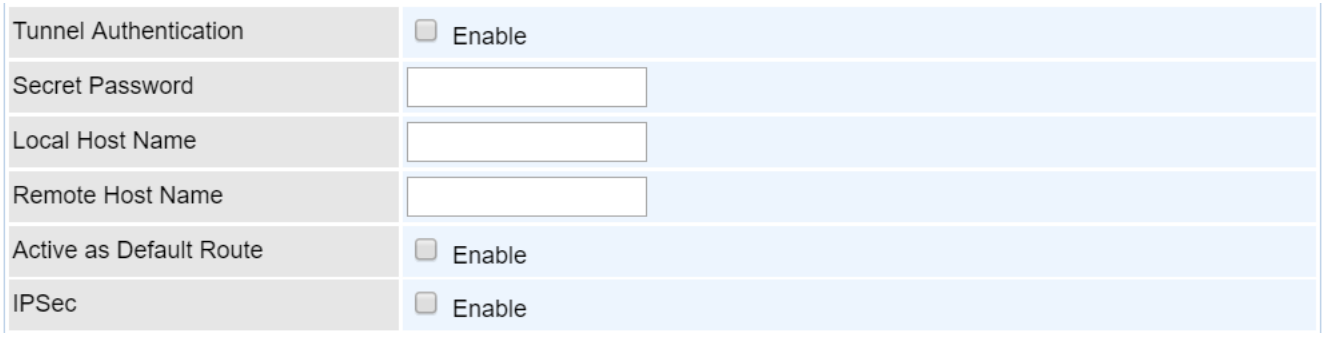
Authentication Type: Default is Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or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

Username / Password (Client): Enter the username / password provide by the Server/Host.

Connection Type

- **Remote Access:** From a single user.
- **LAN to LAN:** Enter the peer network information, such as network address and Netmask.

Tunnel Authentication and Active



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 / established 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.

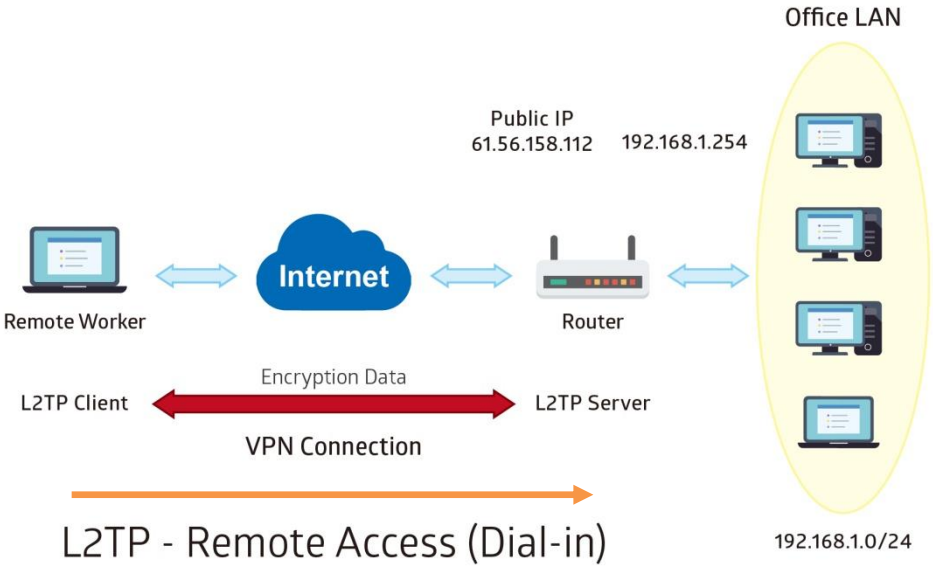
Active as Default Route: Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

IPSec: Click the checkbox to establish a L2TP tunnel inside of the IPSec tunnel.

Click **Save** to apply settings.

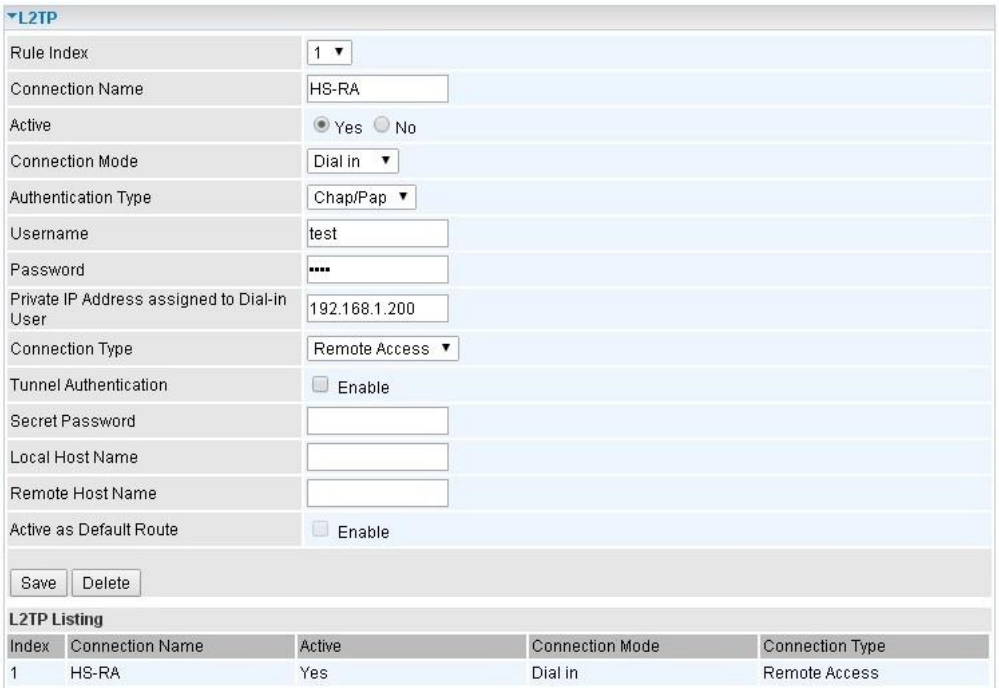
Example: L2TP VPN – Remote Employee Dial-in to BEC 9900VA

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



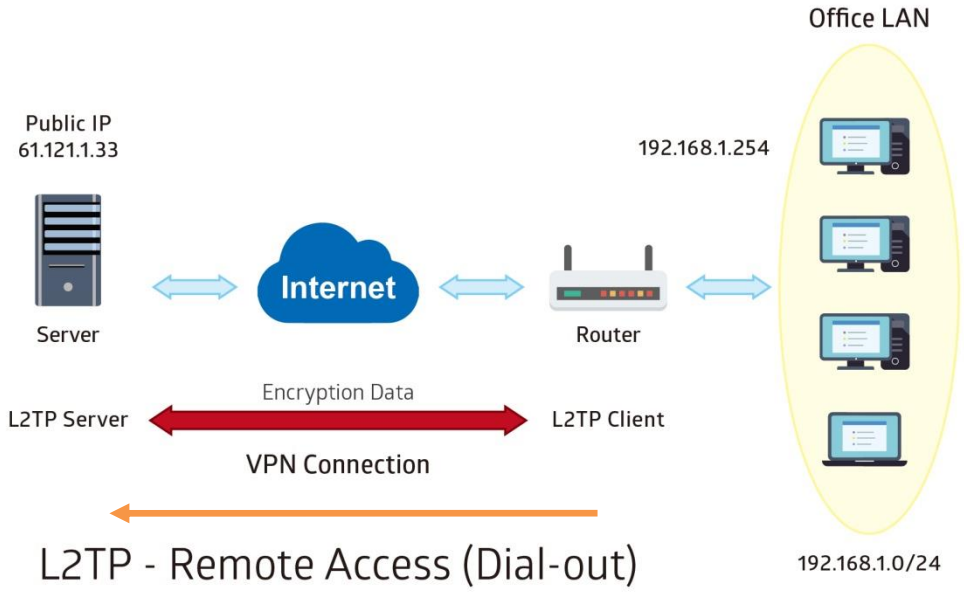
The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the device for remote client to dial-in to the network.
Password	test	
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	Remote Access	Remote access for dial in

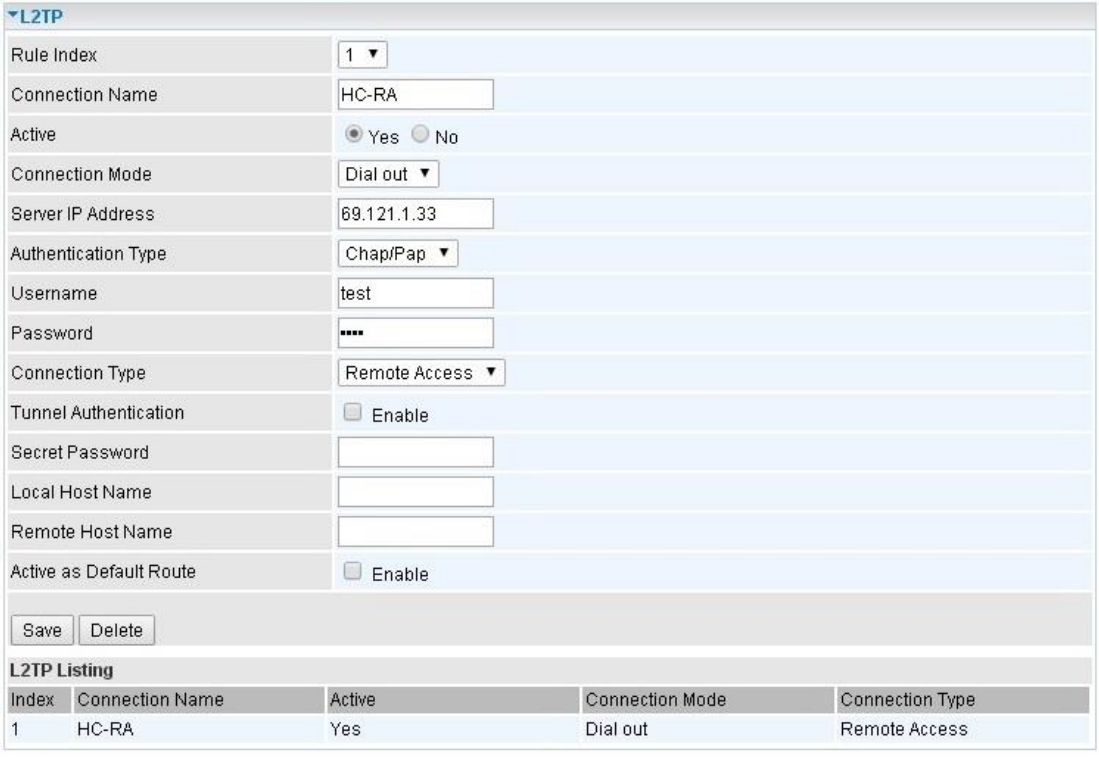


Example: L2TP VPN – BEC 9900VA Dial-out to a Server

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.



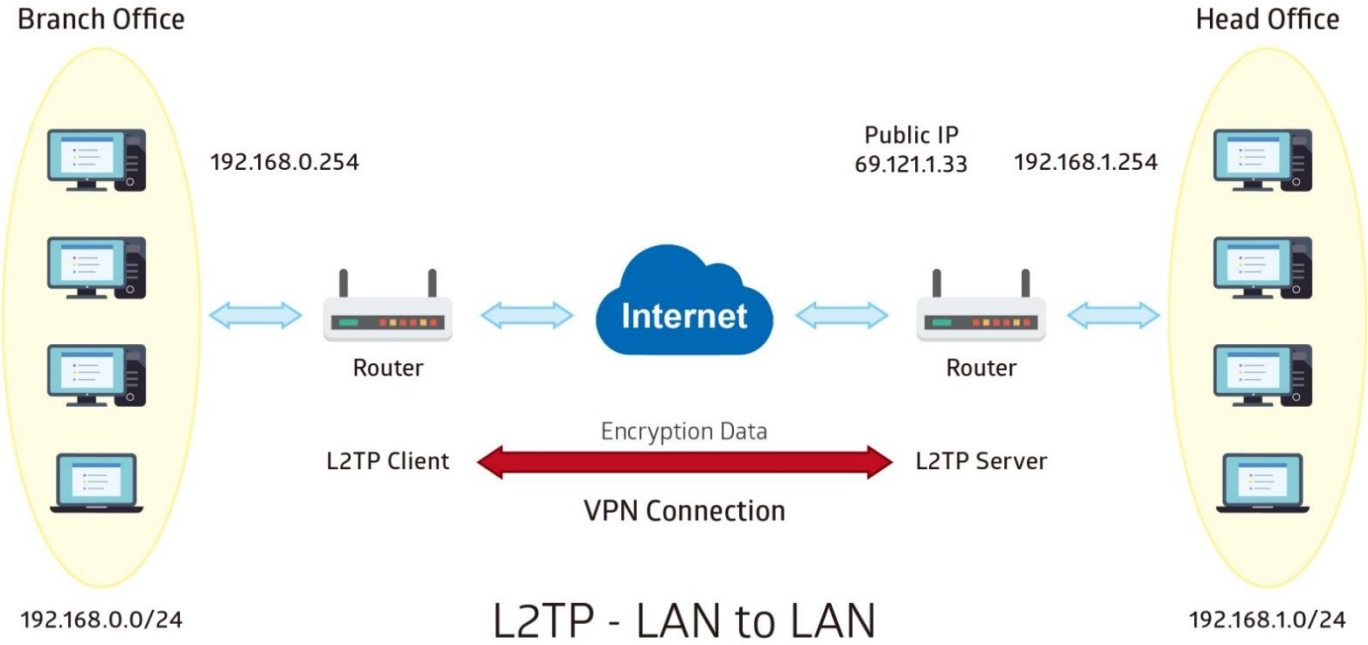
Item		Description
Connection Name	HC-RA	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	VPN server WAN IP address
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the VPN Server for remote clients to dial-in to the network.
Password	test	
Connection Type	Remote Access	Remote access for dial out



Example: L2TP VPN – Network (LAN) to Network (LAN) Connection

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

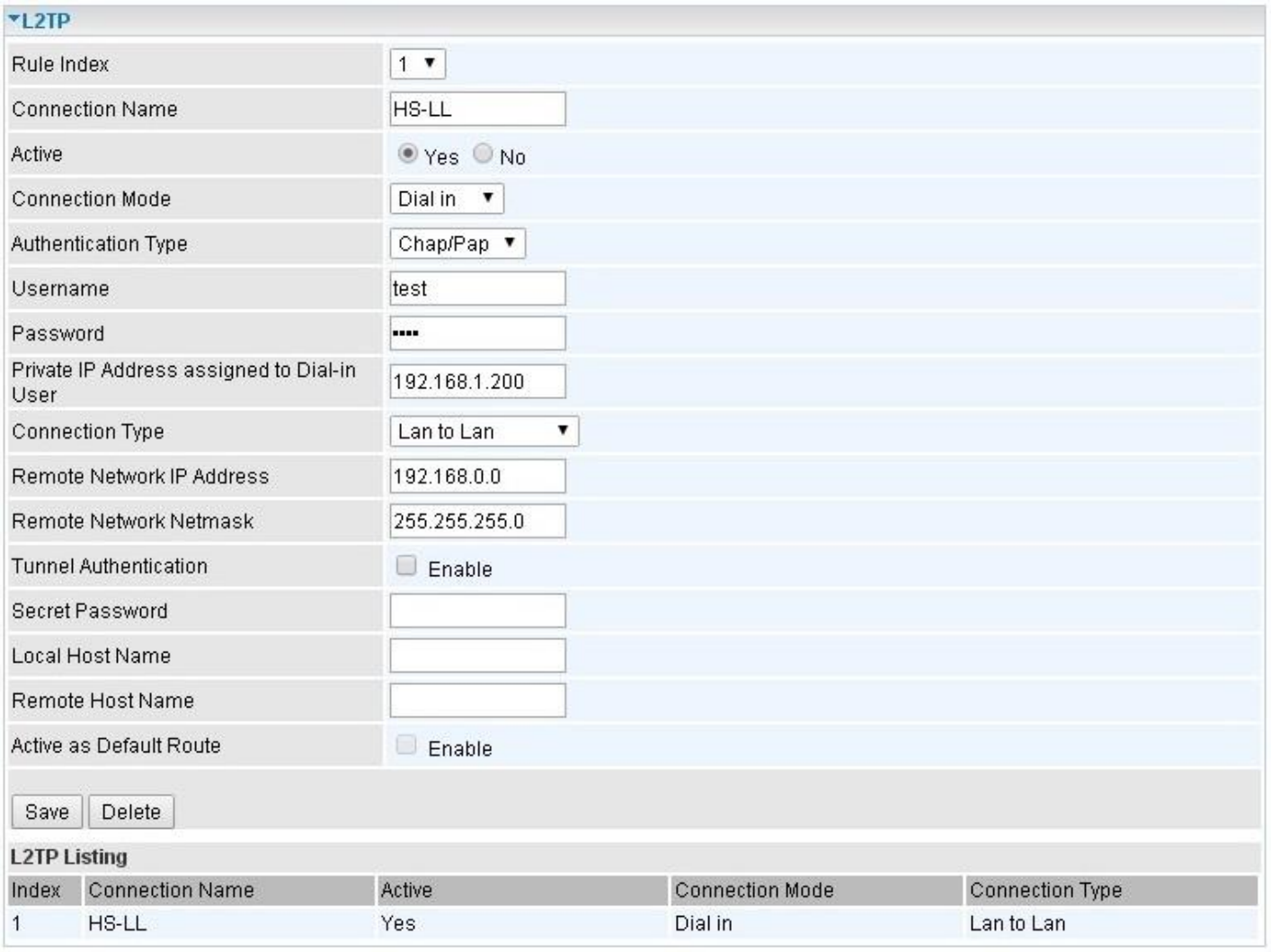
NOTE: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring L2TP VPN Dial-in in the Headquarter office

The IP address 192.168.1.200 will be assigned to the router located in the branch office.

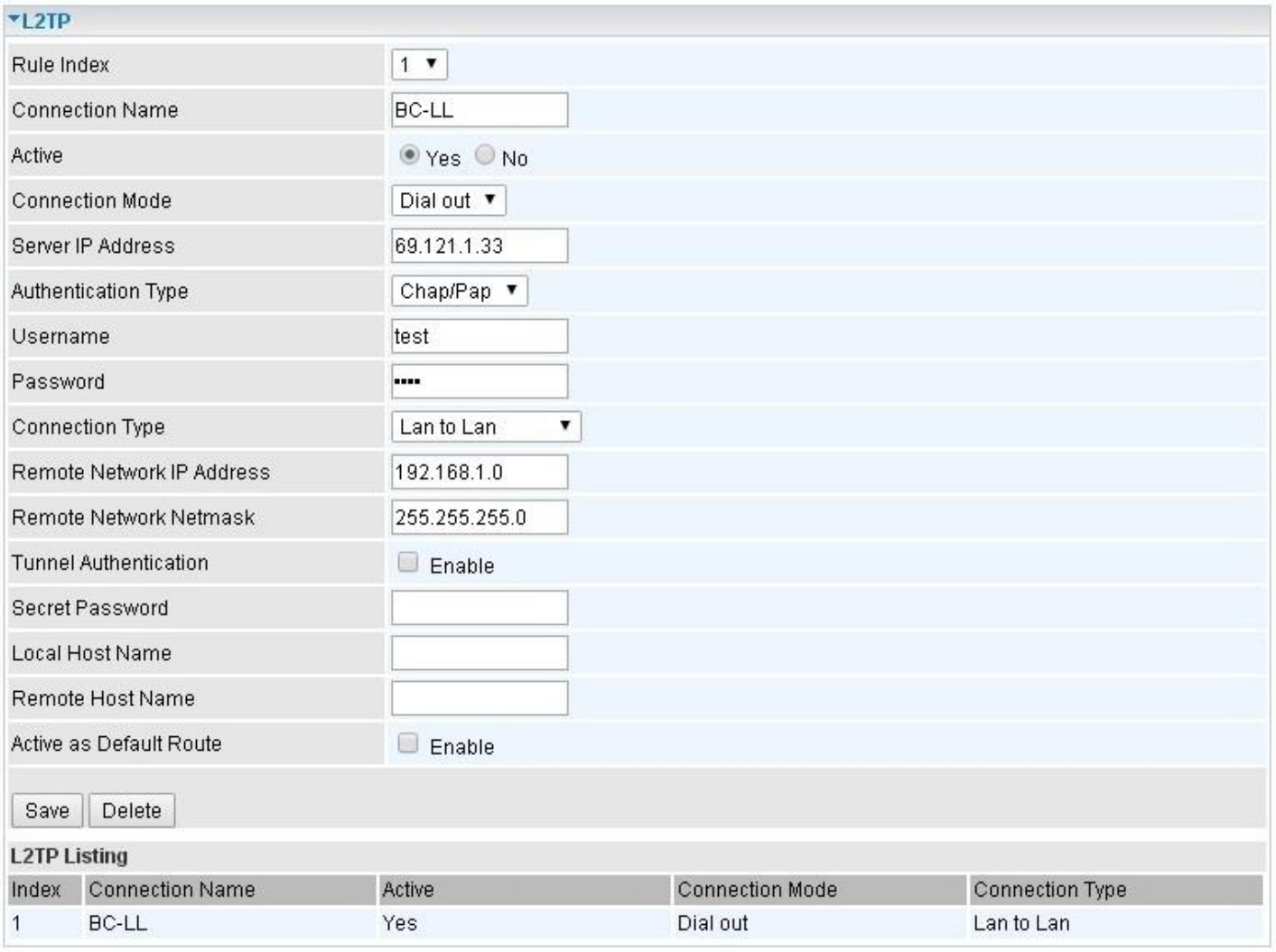
Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	Test	Credential for a PPTP client to dial-in to the network.
Password	Test	
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	LAN to LAN	LAN to LAN for dial in
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



Configuring L2TP VPN Dial-out in the Branch office

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

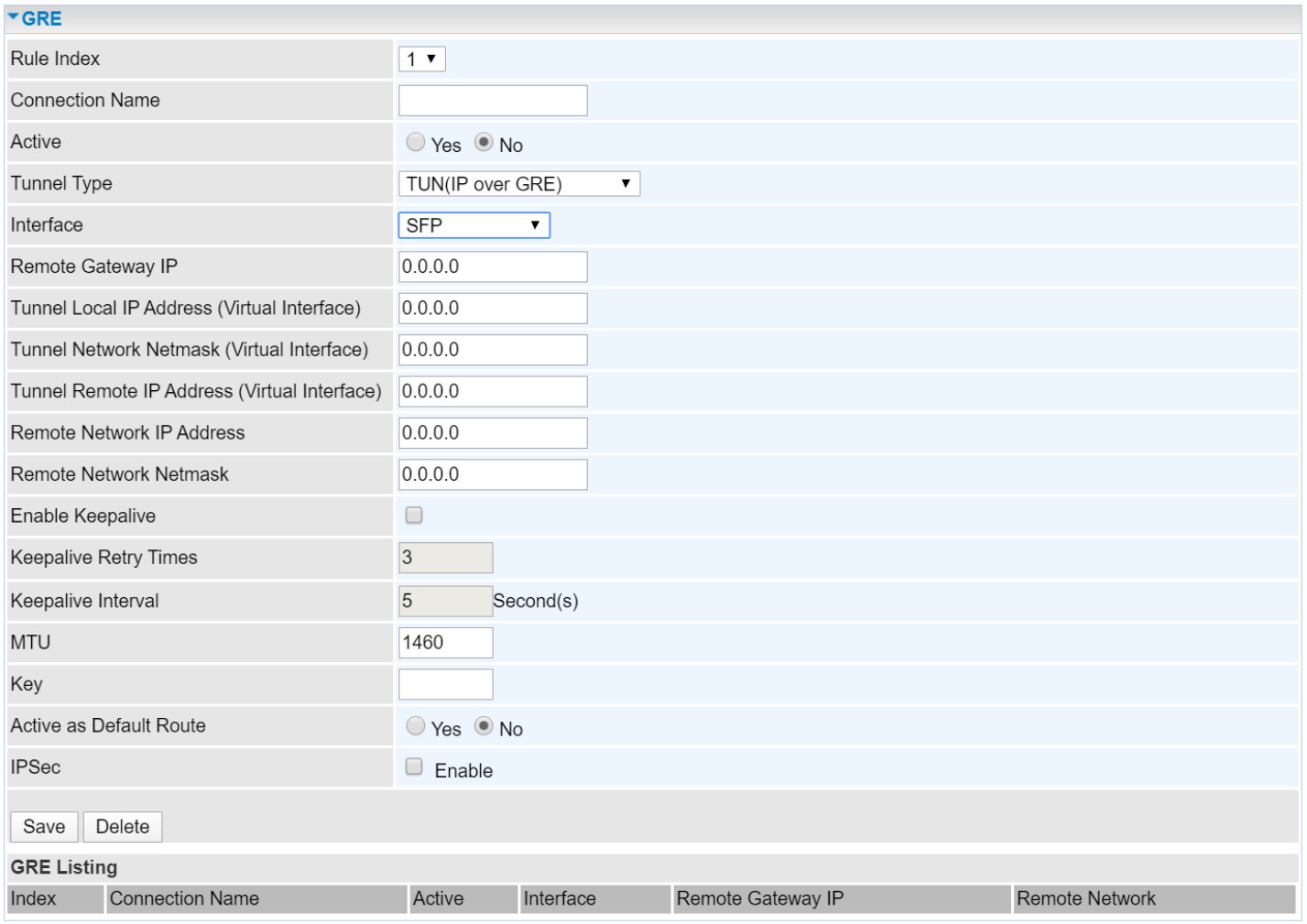
Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	Dialed server IP
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the PPTP server to dial-in to the network
Password	test	
Connection Type	LAN to LAN	LAN to LAN for dial out
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



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 8 GRE tunnels supported.



Rule Index: The numeric rule indicator for GRE. The maximum entry is up to 8.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this GRE profile.

Tunnel Type: Two types of tunnels, **TUN (IP over GRE)** and **TAP (Ethernet over GRE)**.

TUN (IP over GRE)

TUN is in layer 3, networking level which routes packets via GRE tunnels.

Tunnel Type	TUN(IP over GRE)
Interface	SFP
Remote Gateway IP	0.0.0.0
Tunnel Local IP Address (Virtual Interface)	0.0.0.0
Tunnel Network Netmask (Virtual Interface)	0.0.0.0
Tunnel Remote IP Address (Virtual Interface)	0.0.0.0
Remote Network IP Address	0.0.0.0
Remote Network Netmask	0.0.0.0
Enable Keepalive	☐
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Key	
Active as Default Route	○ Yes ◉ No
IPSec	☐ Enable

Save Delete

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

Tunnel Local IP Address & Remote IP Address (Virtual Interface): Enter a virtual IP address for local and peer network of the GRE tunnel.

Tunnel Network Netmask (Virtual Interface): Enter the Netmask for this virtual interface.

NOTE: The virtual Local and Remote IP addresses must in **same subnet** and **cannot be existed or used** in both networks.

Remote Network IP Address: Enter the actual remote LAN network IP address.

Remote Network Netmask: Enter the actual remote LAN network Netmask.

Enable Keepalive: Check the box to enable the keepalive. The system will detect remote peer is still alive or lost. If no responses from the remote peer after certain times, **#-of-retry-time x interval**, the connection will get dropped.

Keep-alive Retry Times: Set the keep-alive retry times, default is 3.

Keep-alive Interval: Set the keep-alive Interval, unit in seconds. Default is 5 seconds.

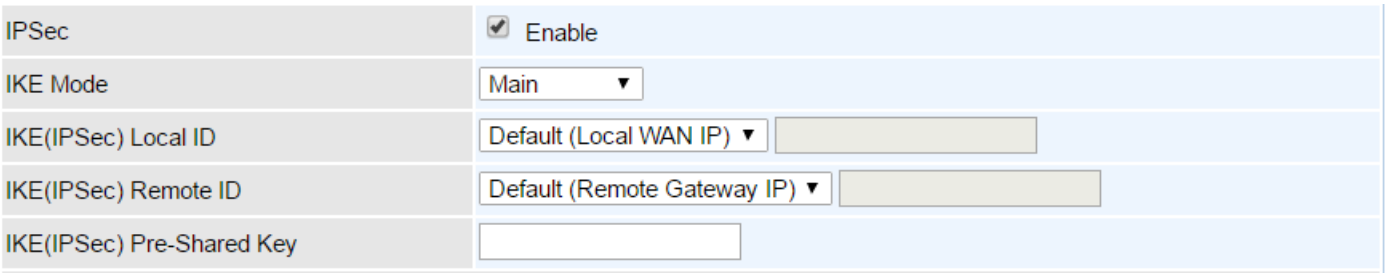
Example: Keepalive retry time (3) x keepalive interval (5) = 15 seconds. If no responses for 15 seconds, GRE connection will get aborted.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

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

IPSec: Click the checkbox to establish a GRE tunnel inside of the IPSec tunnel.



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.

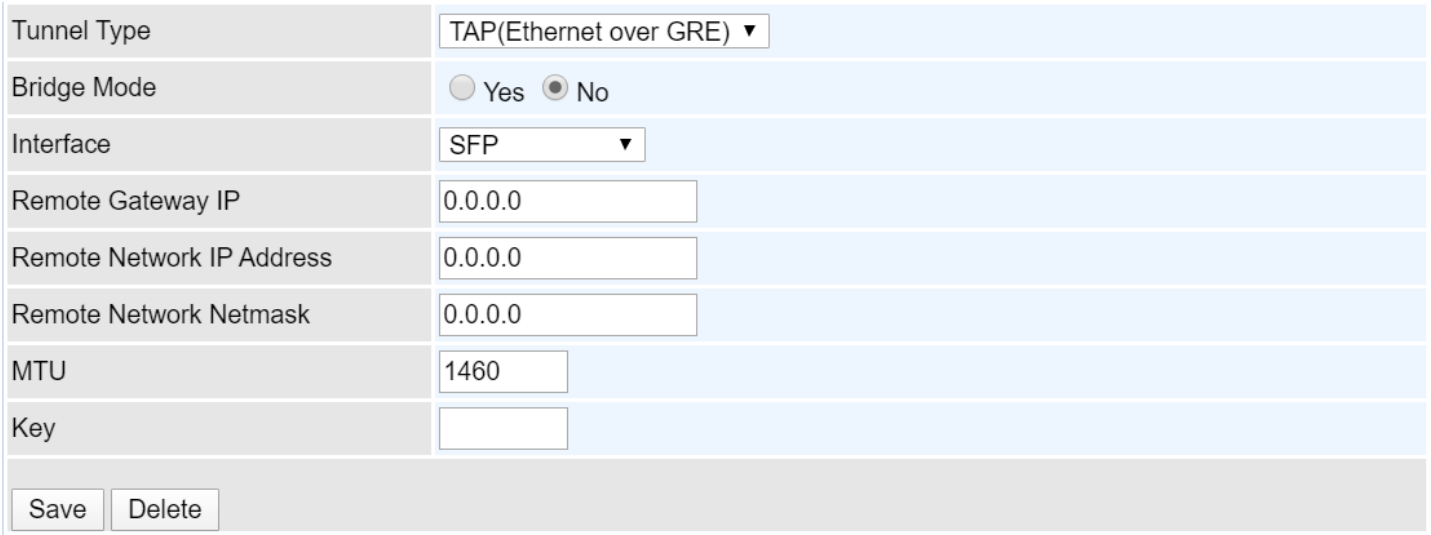
IKE (IPSec) Local ID Type and **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

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

Click **Save** to apply settings.

TAN (Ethernet over GRE)

TAN is in layer 2, Ethernet level which acts as a switch adding Ethernet frame passed over the GRE tunnels.



Bridge Mode: Select **Yes** to enable TAN bridge mode.

Bridge Mode – No

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

Remote Network IP Address: Enter the actual remote LAN network IP address.

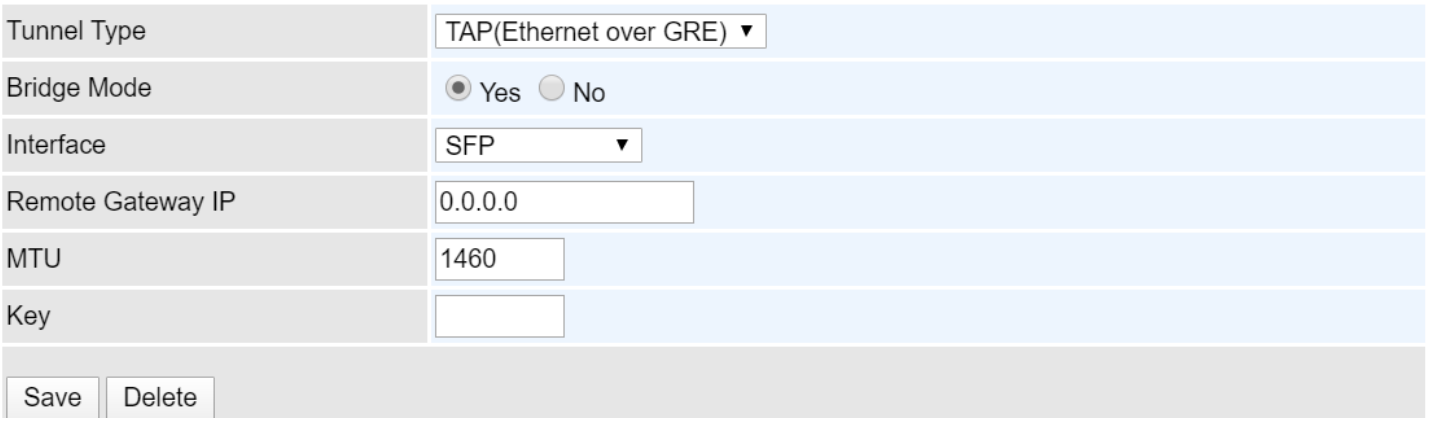
Remote Network Netmask: Enter the actual remote LAN network Netmask.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

Click **Save** to apply settings.

Bridge Mode – Yes



Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-

specific headers) an IP attempts to send through the interface.

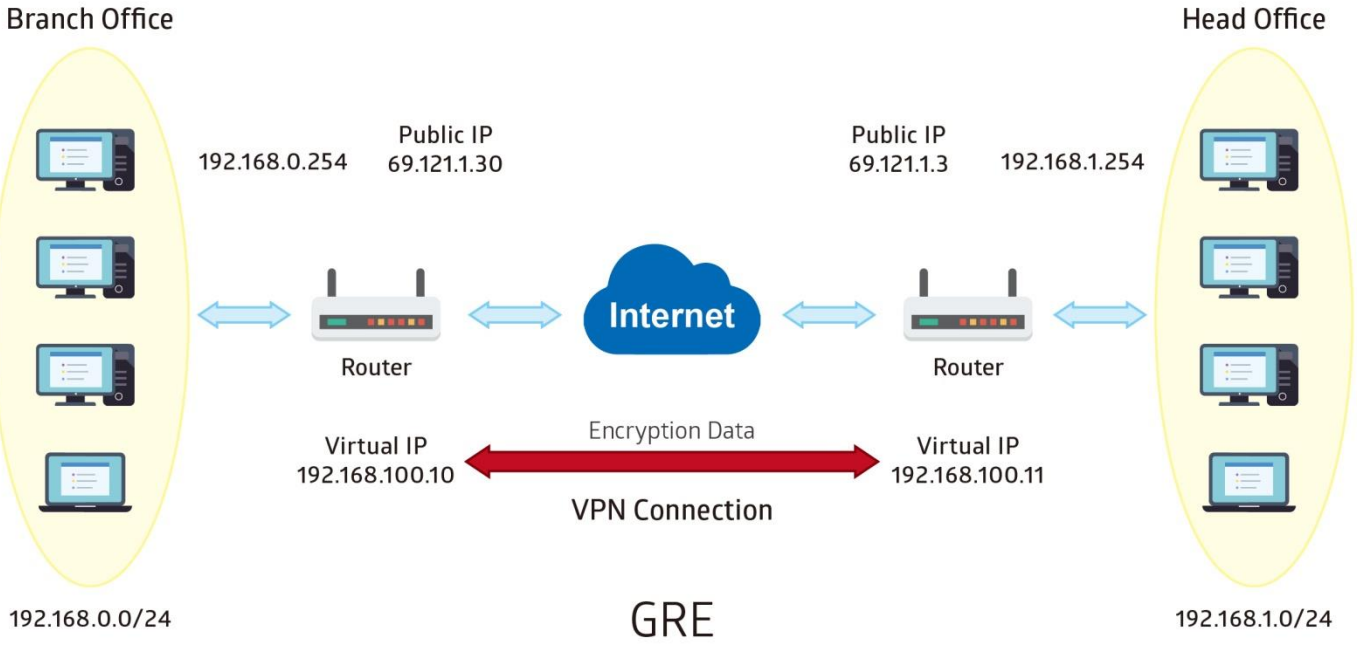
Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

Click **Save** to apply settings.

Example: GRE VPN – Network (LAN) to Network (LAN) Connection

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

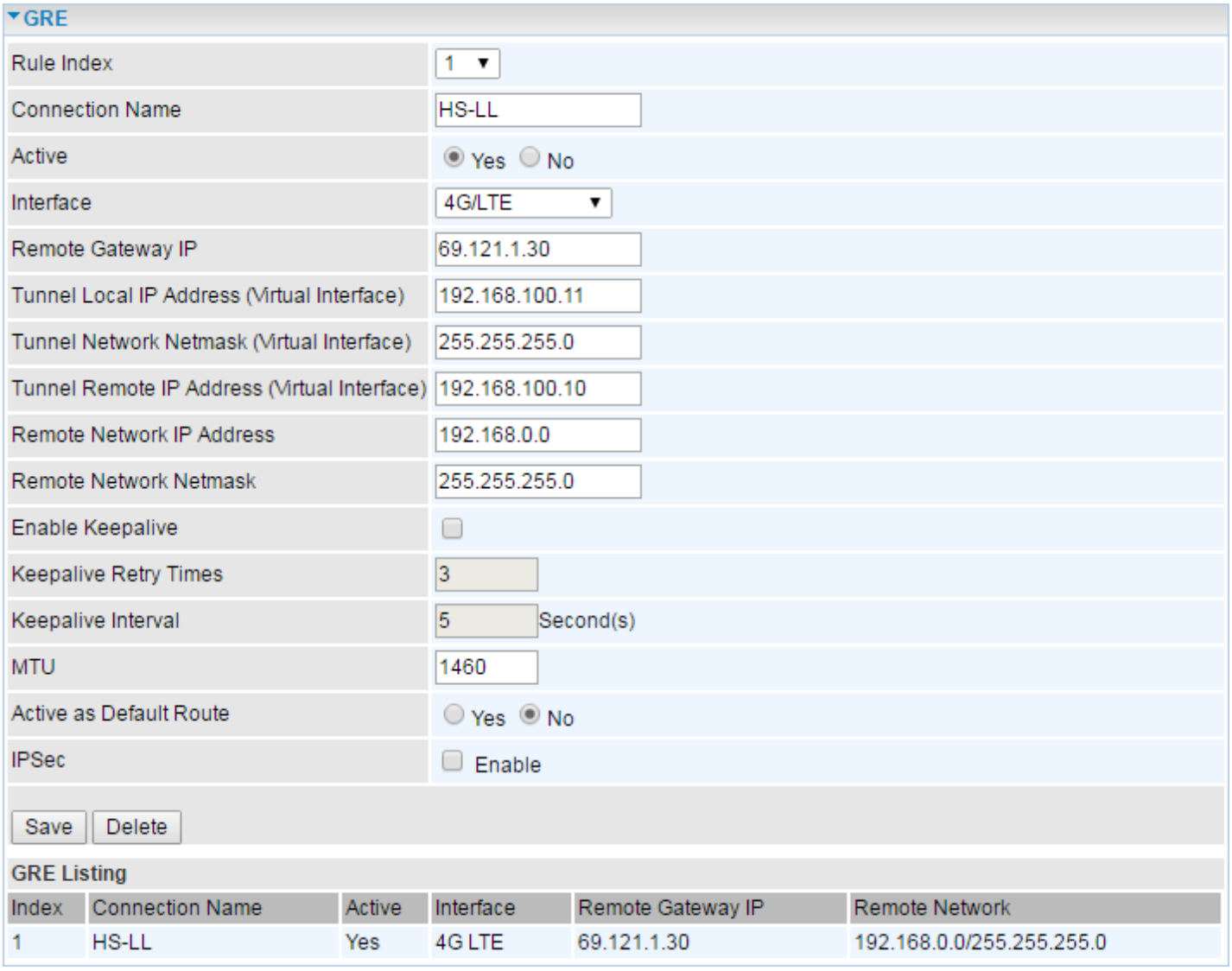
NOTE: Both office LAN networks must be in different subnets with the GRE VPN connection.



Configuring GRE connection in the Headquarter office

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

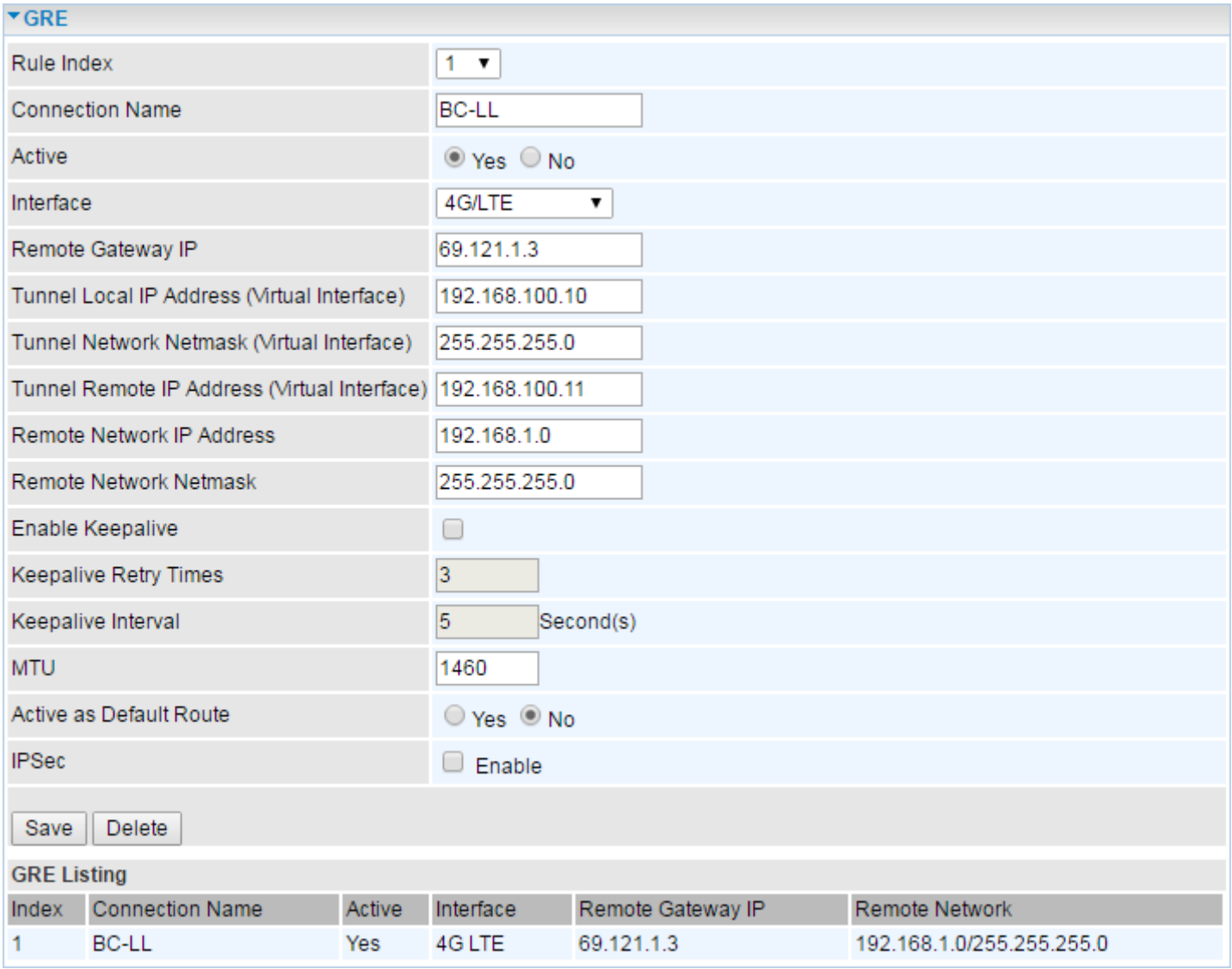
Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.30	WAN IP address of Branch office
Tunnel Local IP Address (Virtual Interface)	192.168.100.11	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.0.0/ 255.255.255.0	The remote, branch office, LAN network IP and Netmask.



Configuring GRE connection in the Branch office

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

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.3	WAN IP address of Headquarter office
Tunnel Local IP Address (Virtual Interface)	192.168.100.10	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.1.0/ 255.255.255.0	The remote, Headquarter office, LAN network IP and Netmask.



OpenVPN

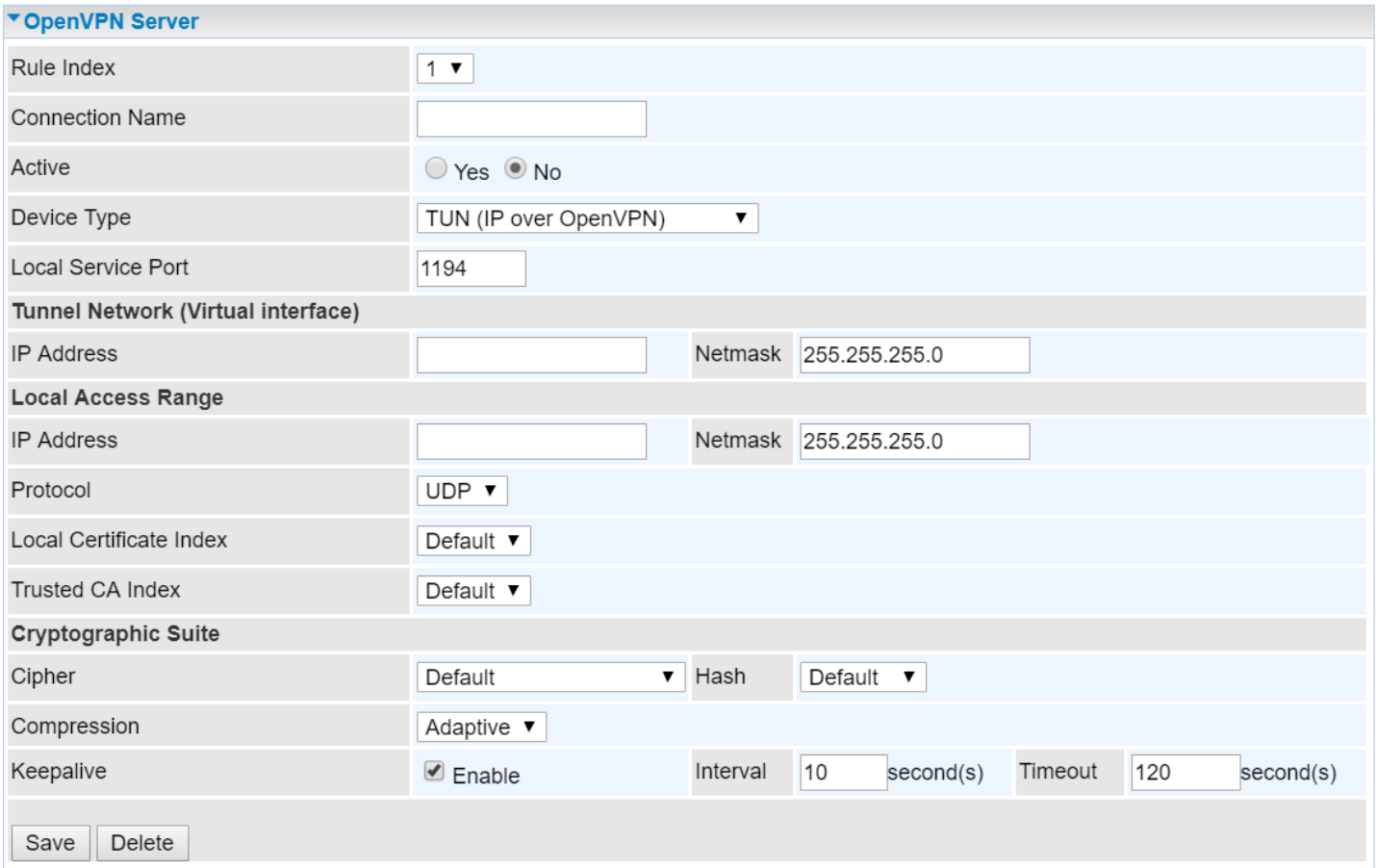
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.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

NOTE: Up to 1 profile.



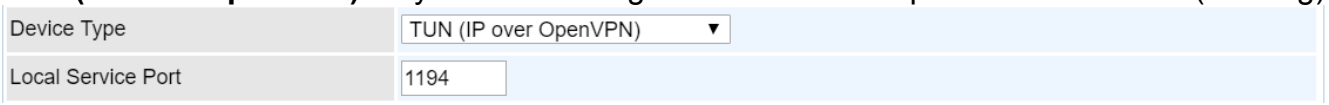
Rule Index: The numeric rule indicator for OpenVPN.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

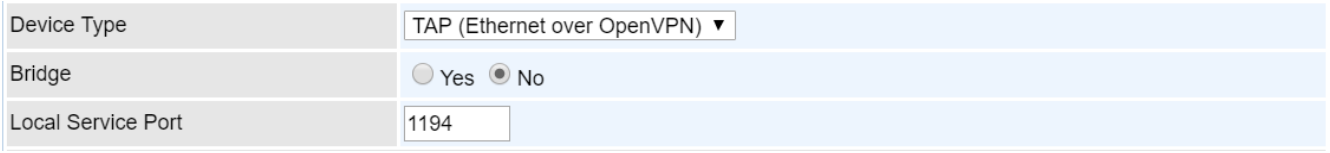
Device Type:

- **TUN (IP Over OpenVPN):** Layer 3 networking level which routes packets on the VPN (Routing).



  - **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.

- **TAP (Ethernet Over OpenVPN):** Works in layer 2 to pass Ethernet frame over the VPN tunnel.



  - **Bridge: Yes** if used in bridge.
  - **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.

Tunnel Network (Virtual Interface)

IP Address / Netmask: Enter a virtual IP address and Netmask for this tunnel.

NOTE: The virtual IP addresses **cannot be existed or used** in both networks.

Local Access Range

IP Address / Netmask: Enter local LAN network IP address and Netmask.

Protocol: OpenVPN can run over either UDP or TCP transports. Select the protocol.

Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Cryptographic Suite

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an 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: Check the box to enable the keepalive feature. The system will automatically send ping packet to remote peer to keep the tunnel active.

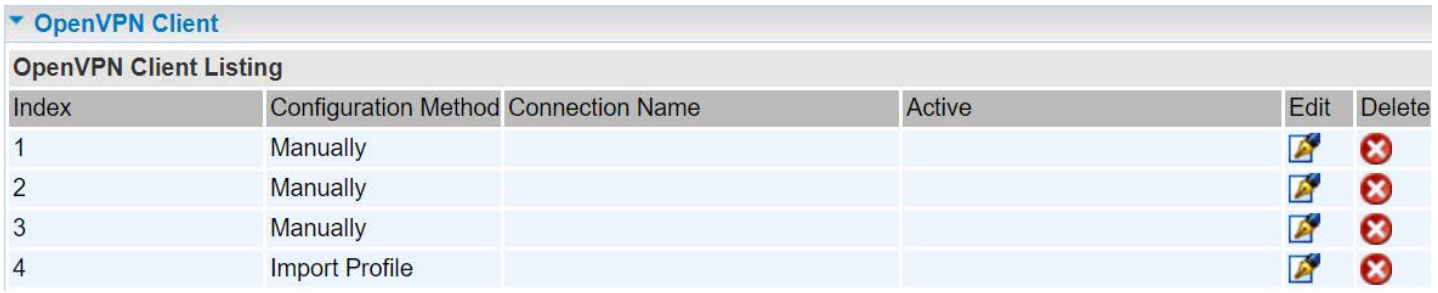
Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

OpenVPN Client

OpenVPN client must match the VPN information / settings with the OpenVPN Server.



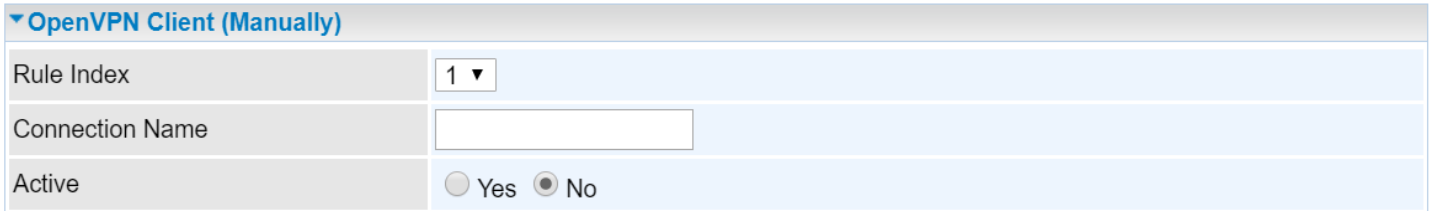
Rule Index: The indication of the rule number. Maximum up to 4 profile/tunnels

Configuration Method: OpenVPN client profiles can be manually entered or imported a pre-configured client profile.

Connection Name: Display the name of the connection or profile.

Active: Display whether the connection or profile is set to active or not.

Manual Input Client Information



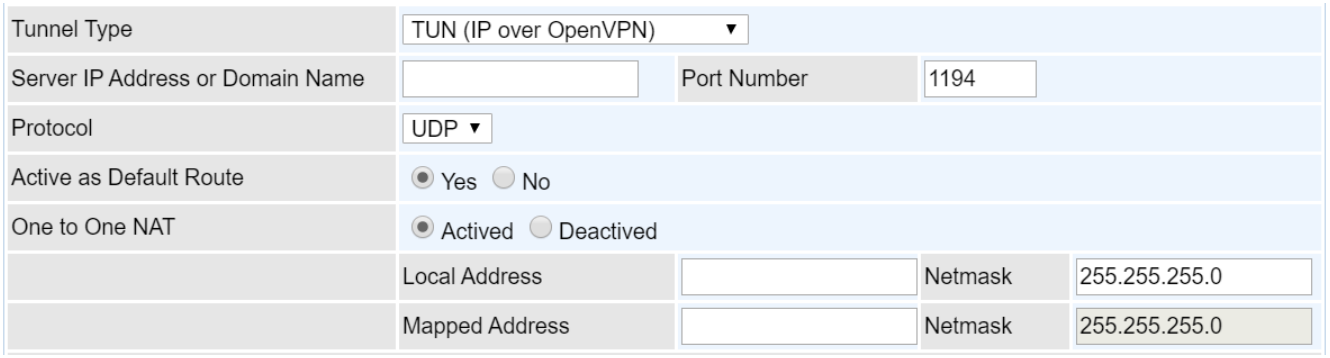
Rule Index: The indication of the rule number. Maximum up to 3 profile/tunnels

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Device Type:

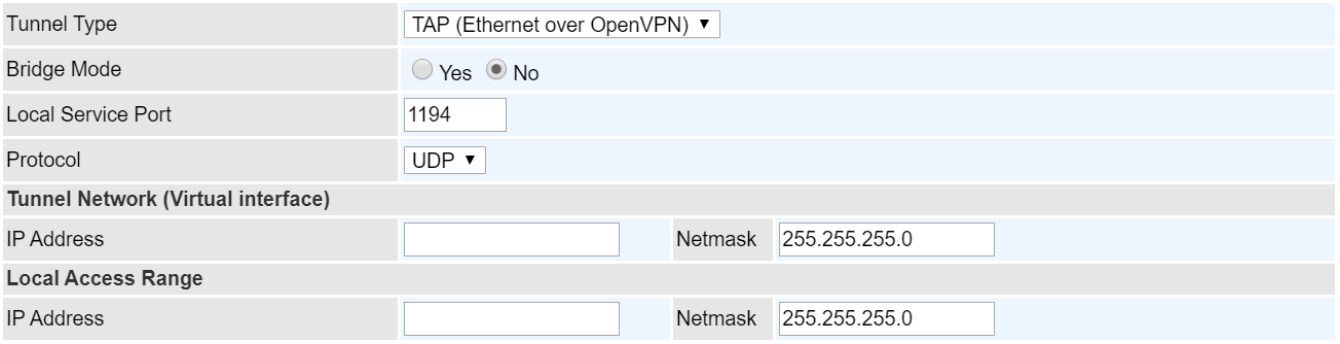
- **TUN (IP Over OpenVPN):** Works only in Layer 3 networking level which routes packets on the VPN.



  - **Server IP Address or Domain Name:** Enter OpenVPN Server's WAN IP address or Domain name.
  - **Service Port:** Port 1194 is the official assigned port number for OpenVPN.
  - **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

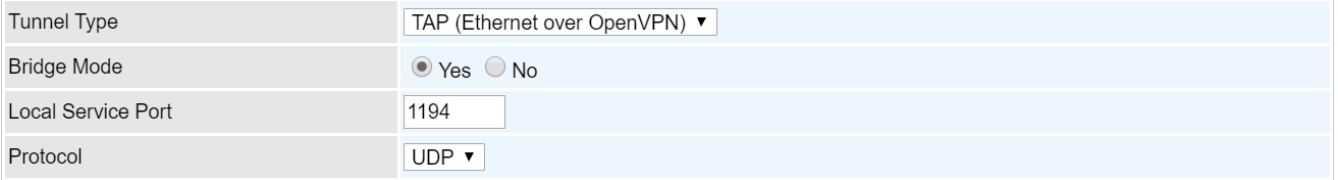
- **Active as Default Route:** Choose **Yes** to let the OpenVPN tunnel/connection be the default route for traffic, under this circumstance, all outgoing packets will be forwarded to this tunnel and routed to the next hop.
- **Remote Network IP Address / Netmask:** Enter the LAN network IP address and Netmask of the OpenVPN Server.
- **One-to-One NAT:** Create a one-to-one mapping for a specific or a range of internal LAN IP address of the OpenVPN client to the VPN tunnel.
  - **Local IP Address / Netmask:** This is the internal LAN network IP address & netmask of the OpenVPN client.
  - **Mapped Tunnel IP Address / Netmask:** This is the IP address & netmask of the OpenVPN tunnel.

TAP (Ethernet Over OpenVPN) in Server-Bridge Mode



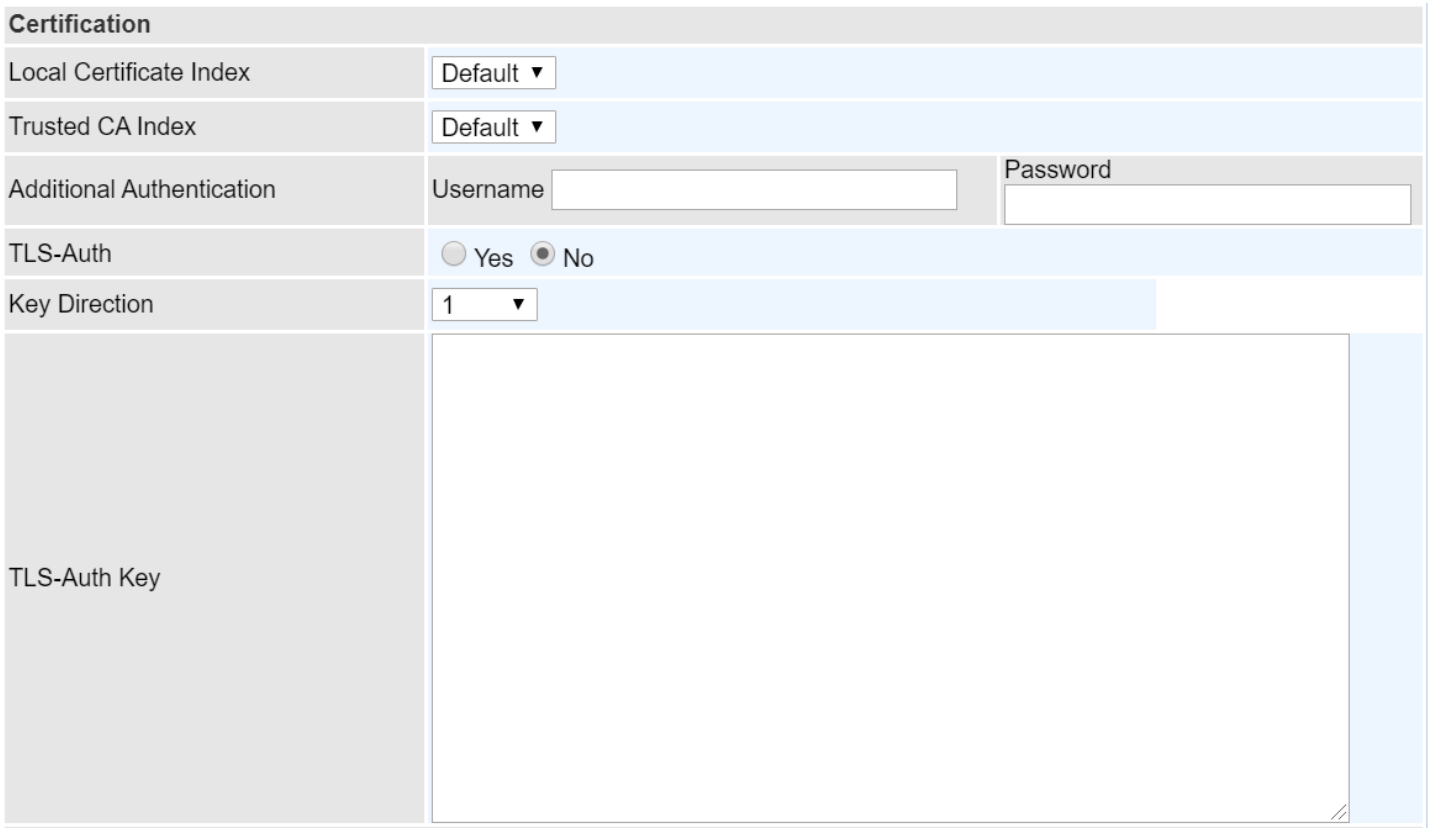
- **Bridge: No** – Using its own client IP address.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.
- **Tunnel Network IP Address / Netmask:** Enter a virtual IP address and Netmask for this tunnel. **NOTE:** The virtual IP addresses **cannot be existed or used** in both networks.
- **Local IP Address / Netmask:** Enter local LAN network IP address and Netmask.
- **Server IP Address or Domain Name:** Enter OpenVPN Server's WAN IP address or Domain name.
- **Bridge: No** – Using its own client IP address.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

TAP (Ethernet Over OpenVPN) in Bridge Mode



- **Bridge: Yes** if used in bridge.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

Certification



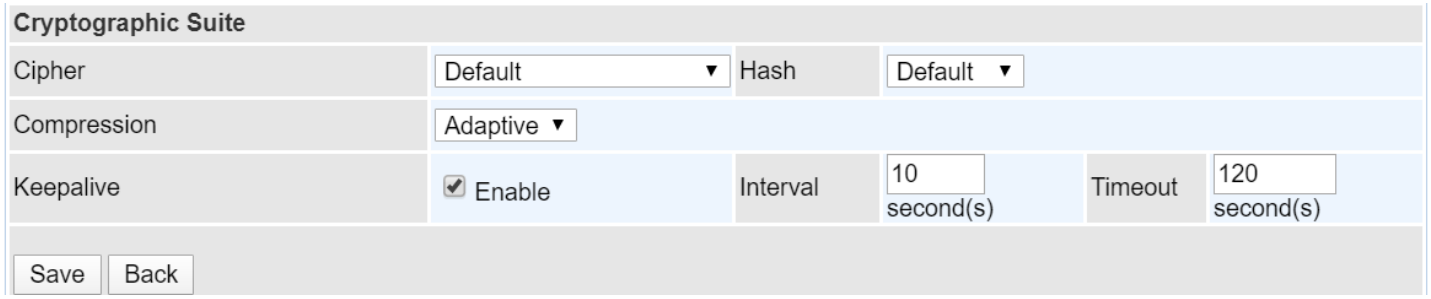
Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Additional Authentication: Enter the extra credential requested by the OpenVPN server.

TLS-Auth / Key Direction / TLS-Auth Key: These are optional functions which must be activated on the server side.

Cryptographic Suite



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

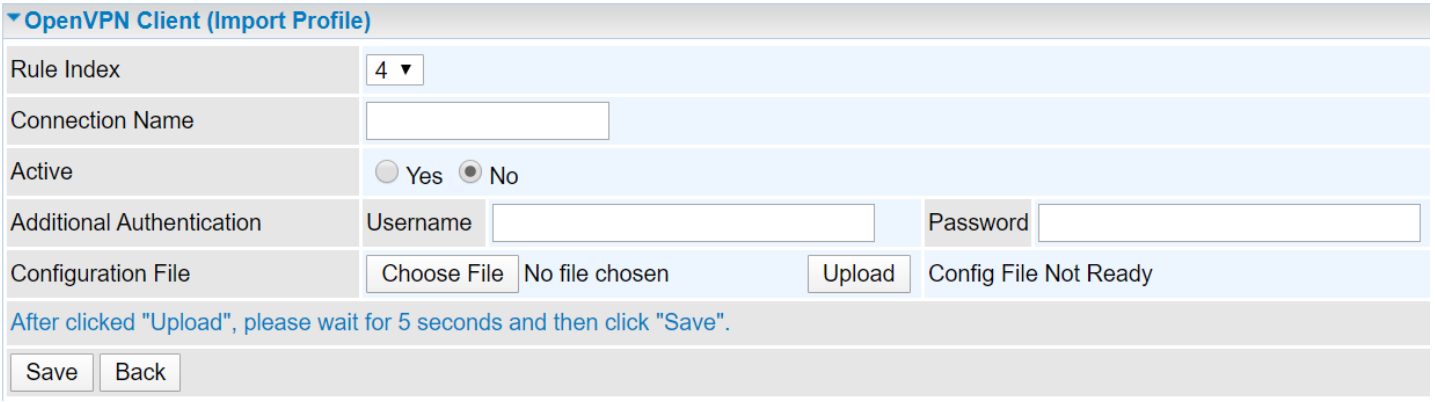
Keepalive: Check the box to enable the keepalive feature. The system will automatically send ping packet to remote peer to keep the tunnel active.

Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

Import an OpenVPN Client Profile



Rule Index: The indication of the rule number.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Additional Authentication: Enter the extra credential requested by the OpenVPN server.

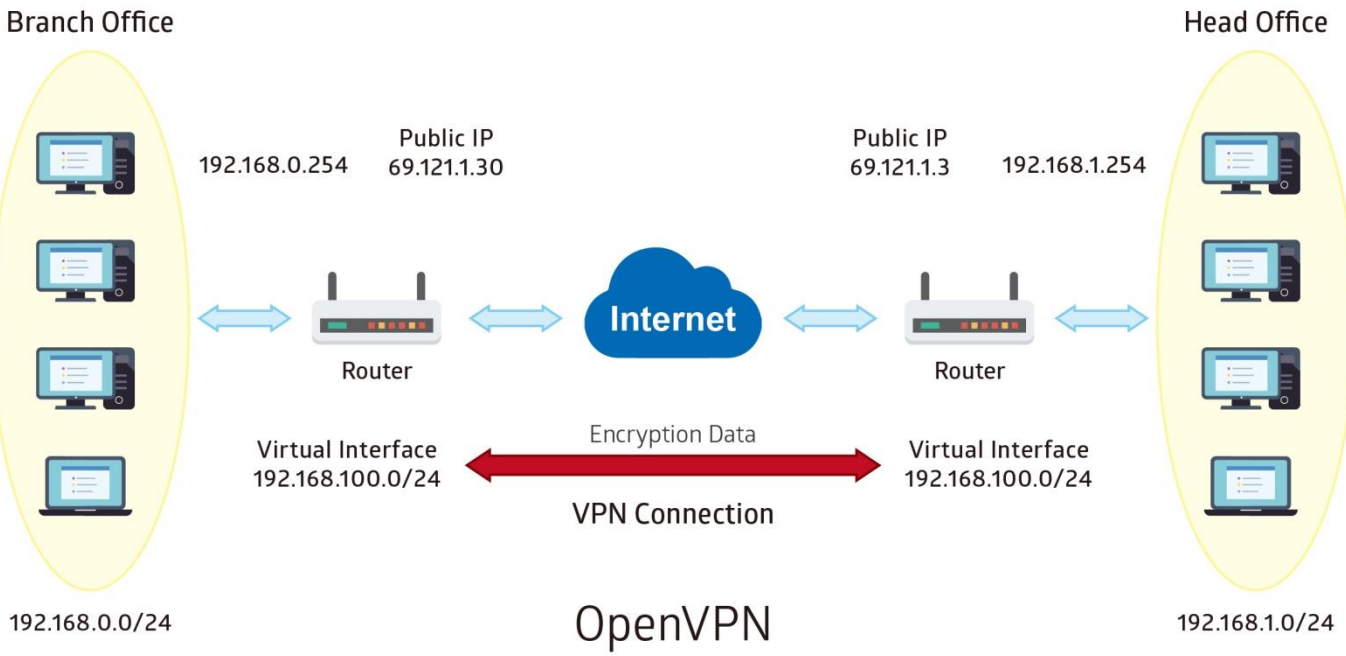
Configuration File: Click **"Choose File"** to find the OpenVPN client profile you want to upload. If the .ovpn file is in zip format, you must extract / decompress / unzip the file prior to the upload.

Upload: Click **Upload** to begin the upload process.

Example: OpenVPN – Network (LAN) to Network (LAN) Connection

The Branch office establishes a tunnel with Headquarter office to connect two private networks over the OpenVPN.

NOTE: Both office LAN networks must be in different subnets.

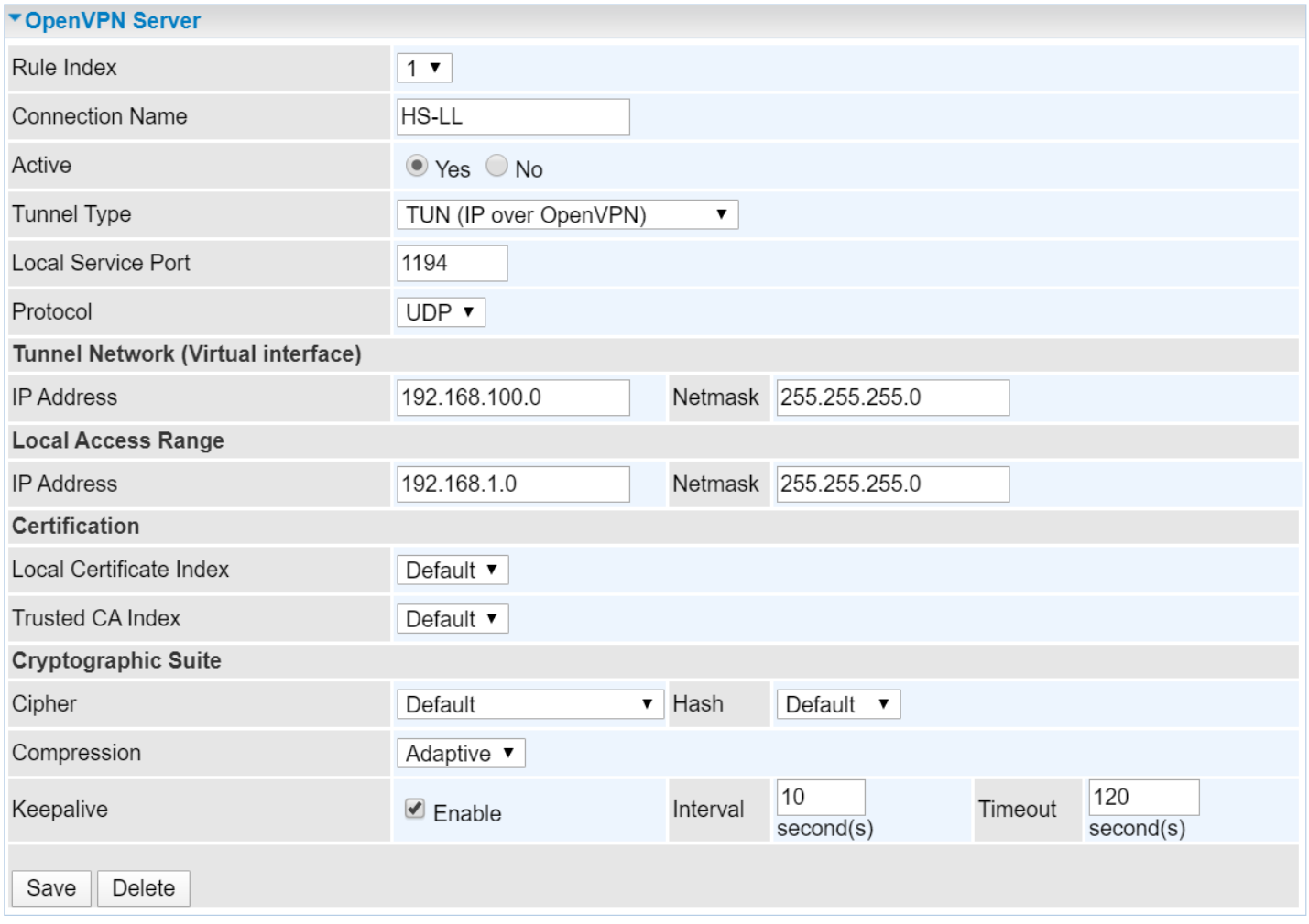


Configuring OpenVPN server in Headquarter office

The IP address 69.1.121.30 is the WAN IP address of the router located in the Branch office.

The OpenVPN tunnel network virtual interface is set to 192.168.100.0/24.

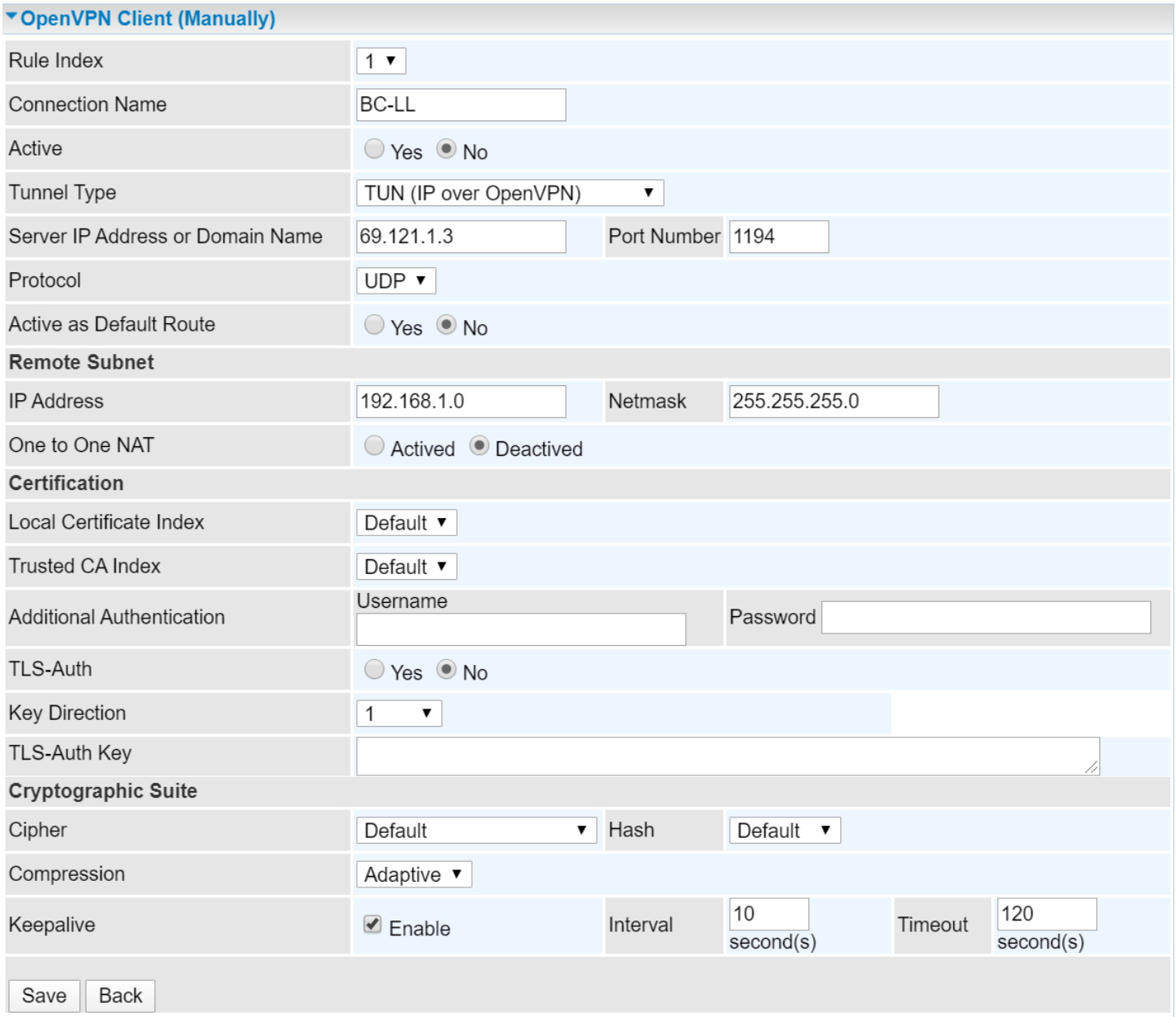
Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Tunnel Network (Virtual Interface)	192.168.100.0/ 255.255.255.0	IP address & Netmask of the virtual tunnel.
Local Access Range	192.168.1.0/ 255.255.255.0	OpenVPN Server's local LAN network.



Configuring OpenVPN client in Branch office

The IP address 69.1.121.3 is the WAN IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Server IP Address	69.121.1.3	The WAN IP address of OpenVPN server.
Remote Subnet	192.168.1.0/ 255.255.255.0	Local LAN IP & Netmask of the Server office



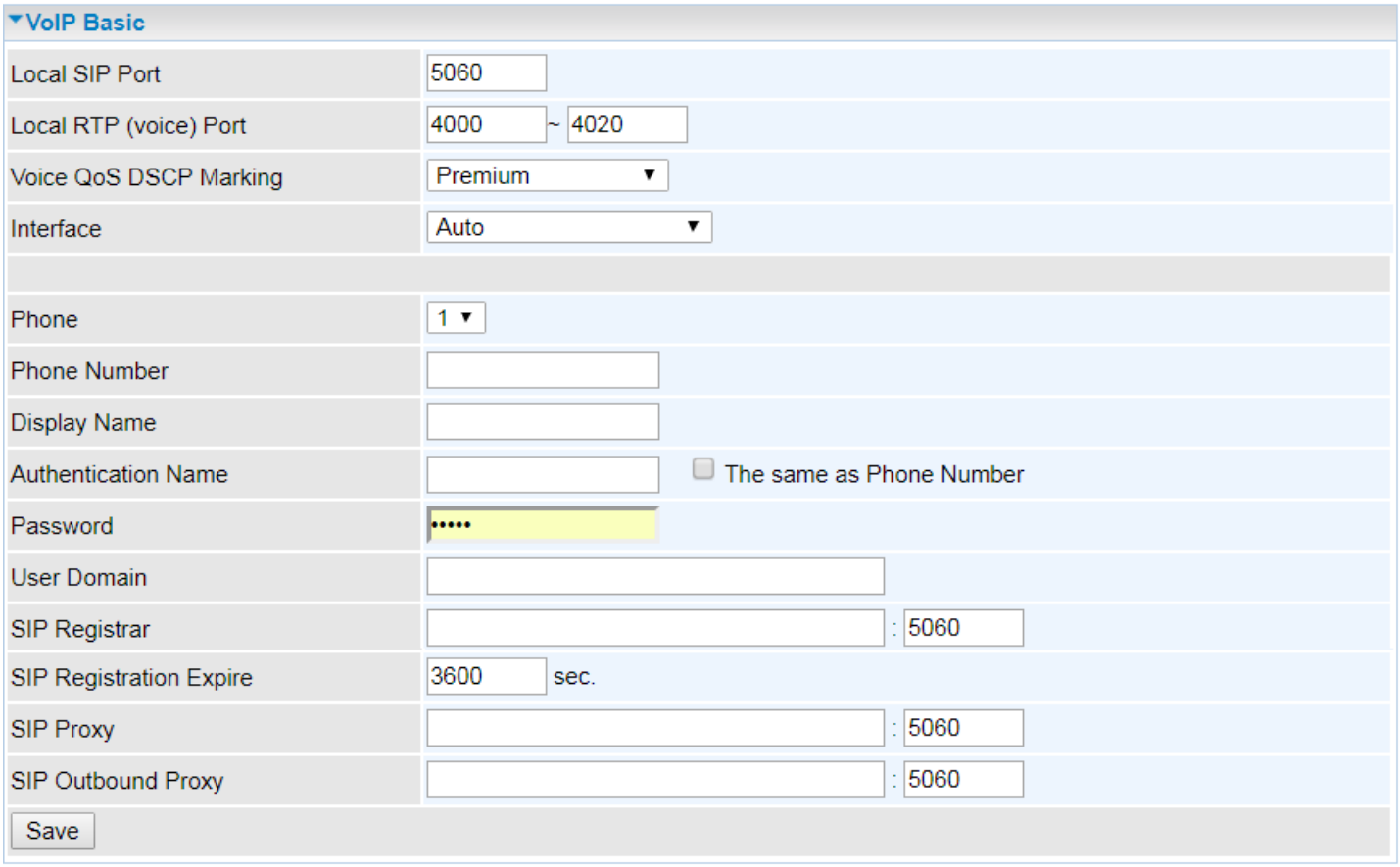
VoIP

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

This section covers Basic, Media, Advanced, Speed Dial, Dial Plan, Call Features, and NAT Traversal.

Basic

Register to a SIP/VoIP service provider is an essential step before making the VoIP call. You can find out this information from your SIP/VoIP service provider.



Local SIP Port: Common port used for VoIP is 5060. Consult with your SIP provide for more information.

Local RTP Port: Set the local RTP port range used to receive voice packet. This setting applies to both the phone ports, Phone_1 and Phone_2, and these phone ports share the same local RTP port.

Voice QoS DSCP Marking: Mark DSCP for outgoing SIP and RTP. VoIP flow to control VoIP QoS.

Interface: Select a WAN interface, any or a specific WAN, to establish voice call.

Phone: Select "1", the following parameters will be applicable to Phone1. In your BEC 9900VA, Phone_1 and Phone_2 are allowed to be of different characteristics, including different SIP registrar. You need to configure individually for phone1 and phone 2 and can have up to 2 different VoIP accounts.

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

from.

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

Authentication Name: Enter a valid name for account authentication purpose. It is usually the Phone Number received from the VoIP service provider. If you have concerns, please contact your SIP/VoIP service provider for more information. Checkmark **The same as Phone Number** box if Authentication Name is identical as the phone number.

Password: Set the registering account password.

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

SIP Registrar: Port: Enter the SIP registrar address where offers the service of registering the VoIP account and the SIP port which will listen to register requests from VoIP devices.

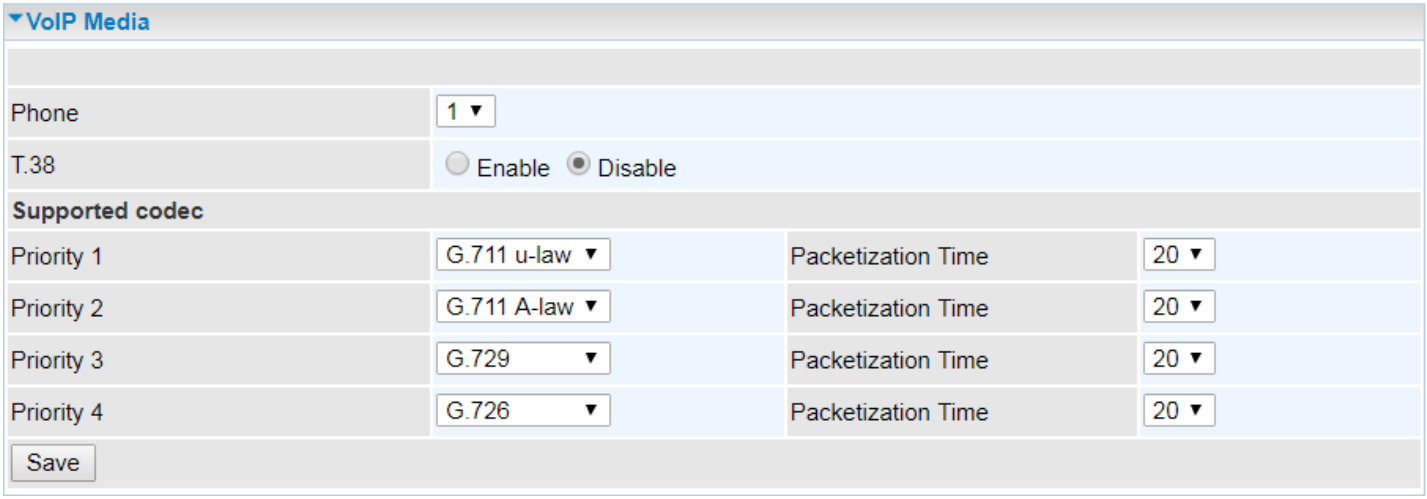
SIP Registration Expire: Set the time interval. The device can update (usually re-login the account) the VoIP account information with the SIP server very the time interval.

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

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

Media

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



Phone: Select to set the following configurations for Phone_1 or Phone_2. When phone1 is selected, the following set media codec will be applied to phone_1.

T.38: T.38 relay is a way to permit faxes to be transported across IP networks between existing fax terminals. Click Enable to allow transmission of fax over IP network between two fax machines. If T.38 is disabled, the analog fax signal is transmitted as the normal audio data. If T.38 relay is enabled, the fax signal is converted to T.38 signal.

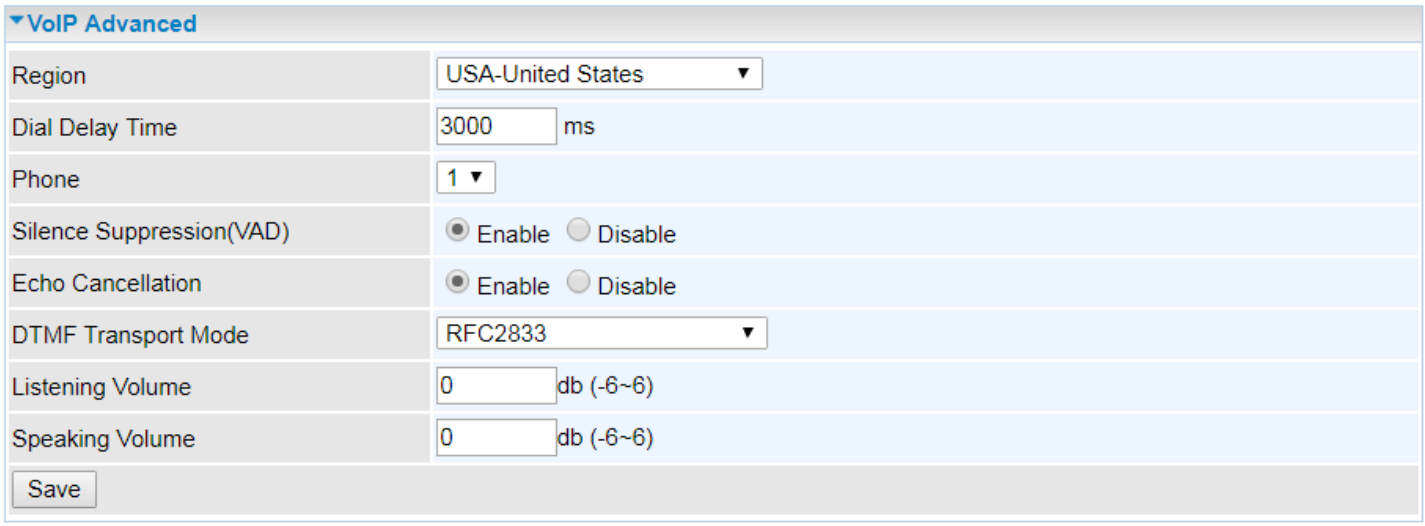
Supported Codec: Codec, Coder-Decoder, is used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority

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

Packetization Time (pTime): Default in 20ms. It indicates how many milliseconds the Voice packets will be queued and sent out.

Advanced

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



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

Dial Delay Time: Default in 3000ms (3 seconds). Time to wait after finished dialing before placing a call.

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

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

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

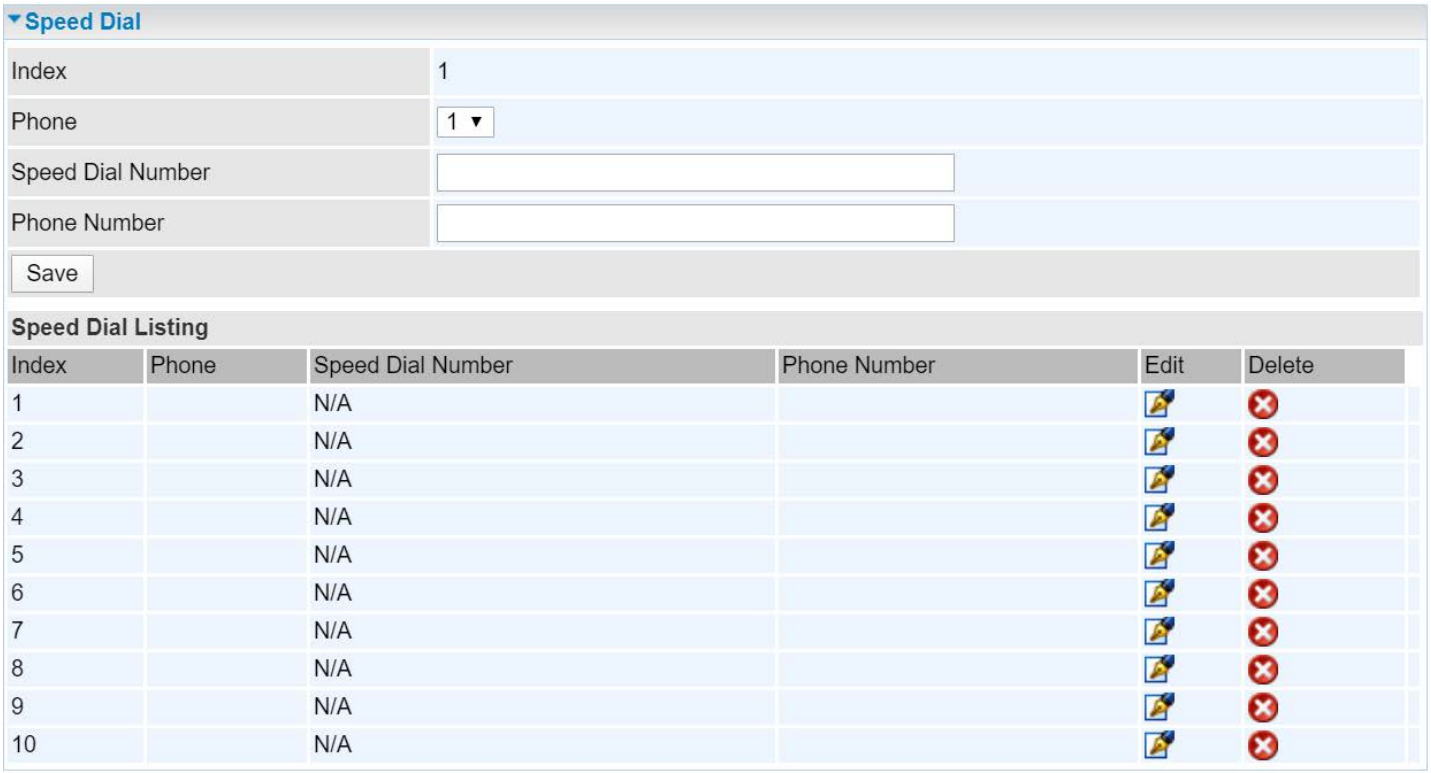
DTMF Transport Mode: Select the DTMF mode.

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

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

Speed Dial

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



Index: The index to mark the speed dial number mapping, 1-10.

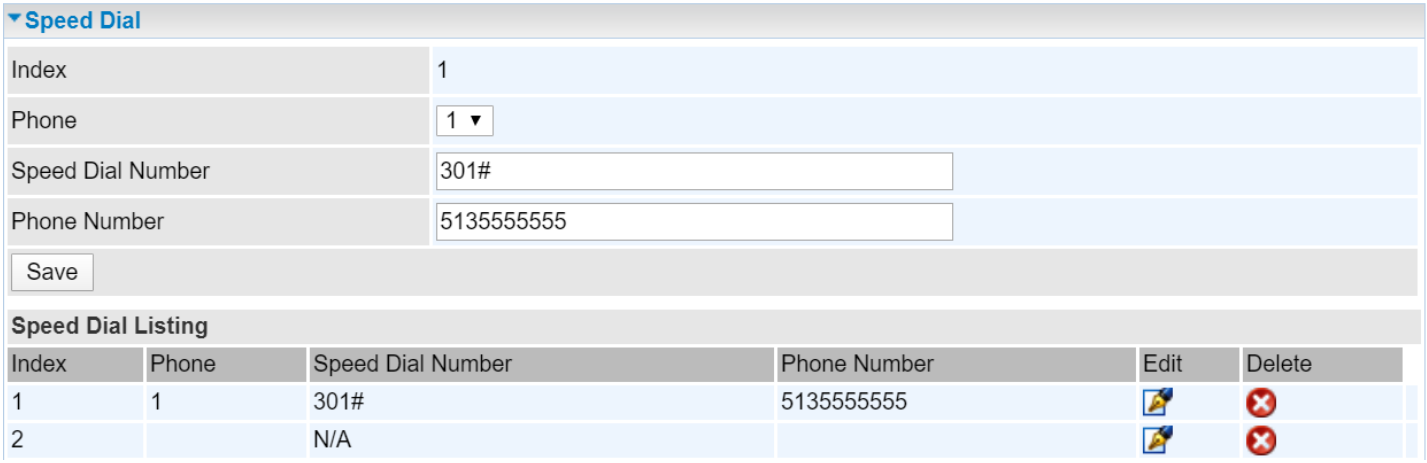
Phone: Select Phone 1 or Phone 2 to have your set speed dial number applied to the phone. If Phone_1 is selected, your set speed dial number is about to be applied to Phone_1.

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

Phone Number: The complete destination number

Click **Save** to save and apply the settings.

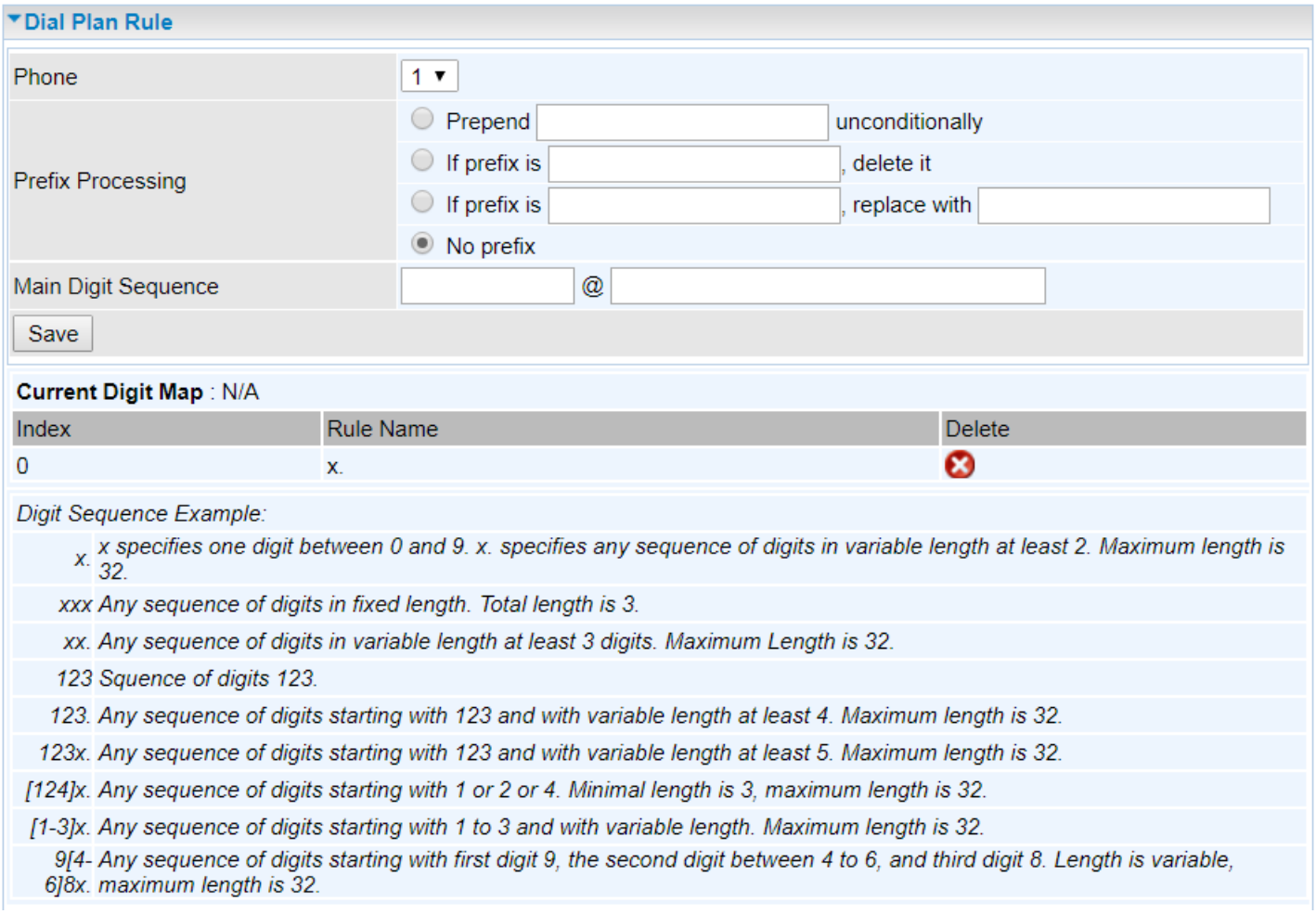
Example: Save phone number 83455301 to the speed dial list.



When you want call 5135555555 through phone 1, you can simply dial 301# to make your desired call.

Dial Plan

Dial plan provides greater flexibility and is an easy-to-use feature allowing users to place call without memorizing the long string of phone numbers.



Phone #: Apply define rules for a specific phone, Phone_1 or Phone_2.

Prefix Processing <:xx>

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

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

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

No prefix: Default – no prefix in front of the dialing numbers.

Main Digit Sequence

It is known as the *Call Routing*; digits dialed that match with the rule will be called via the specific SIP account.

x: Any numeric number between 0 and 9.

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

*** [asterisk]:** It is normal character '*' on phone key pad. Please check if special service(s) is provided

by your VoIP Service Provider or your Local Telephone Service Provider.

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

<@ Current Profile>: Referring to the VoIP accounts registered for Port 1 / 2.

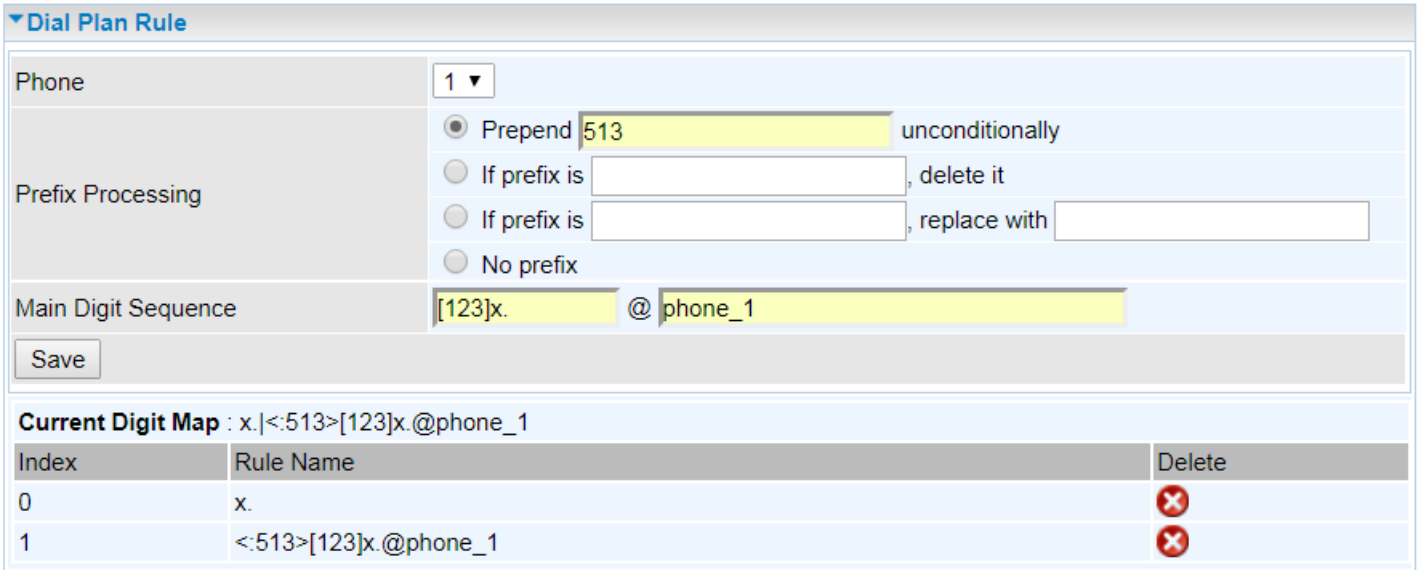
Dial-Plan Examples:	**Description**
x.	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3-digit number between 0 and 9. Total length is 3. **NOTE:** No period is needed (.)
xxxx.	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length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

Example: < @ Current Profile > / Call Routing

Current registered VoIP/SIP providers are localcheap.com and longdischeap.com. Each provider has its price for different type of calls

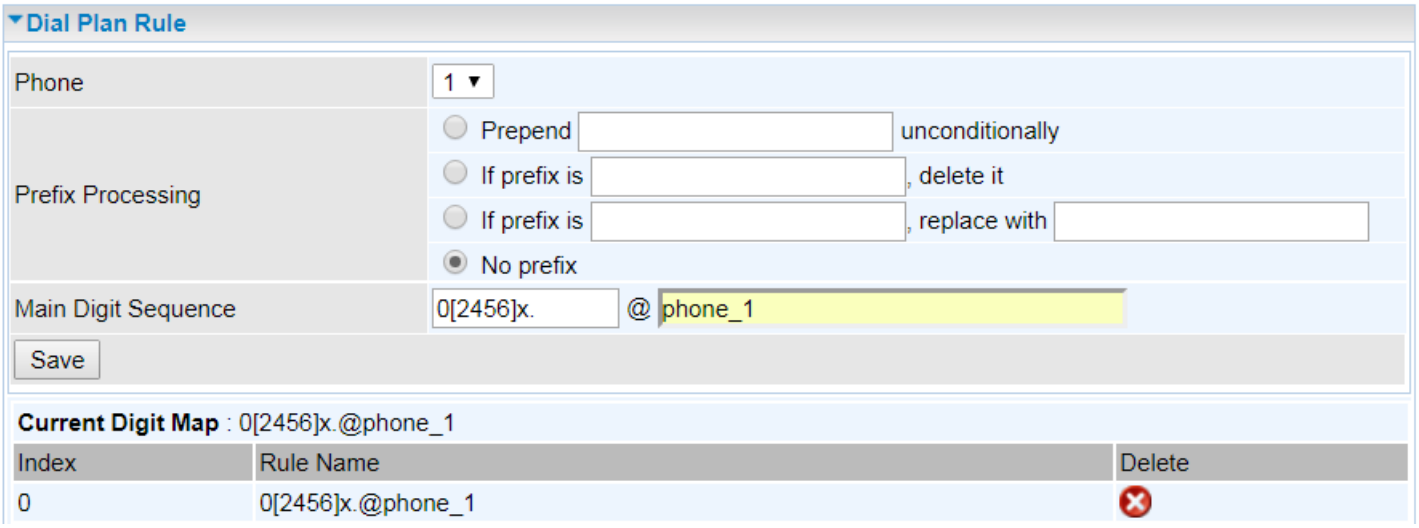
1) Phone 1: For Local calls: I set a dial rule, **<:3>[123]x.T**, for Phone_1.

Localcheap.com is the default VoIP provider I set on phone port 1. When I call out any number start with 1 or 2 or 3 and plus rest of the phone number for local call, 03 is always to add in front of the dialed number. If 1234567 is dialed, 513-1234567 is the actual phone number called out via localcheap.com provider.



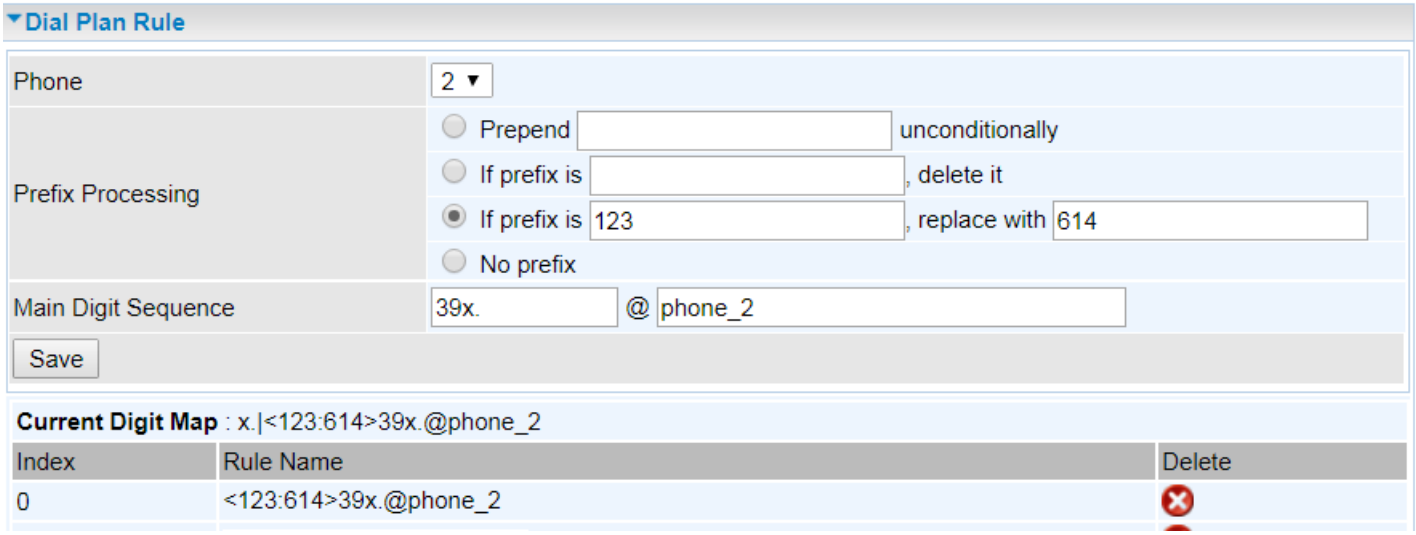
2) Phone 1: For International calls: I set a dial rule, 0[2456]x.T, on my phone port 1.

Localcheap.com is the default VoIP provider I set on phone port 1. No prefix is attached to the dialed number when I call out number 0 plus any following number 2 or 4 or 5 or 6 and plus rest of the phone number for an international call. If 02016148513295 are dialed, 0-2-016148513295 is the actual phone number called out via phone_1; otherwise, the call will get dropped.



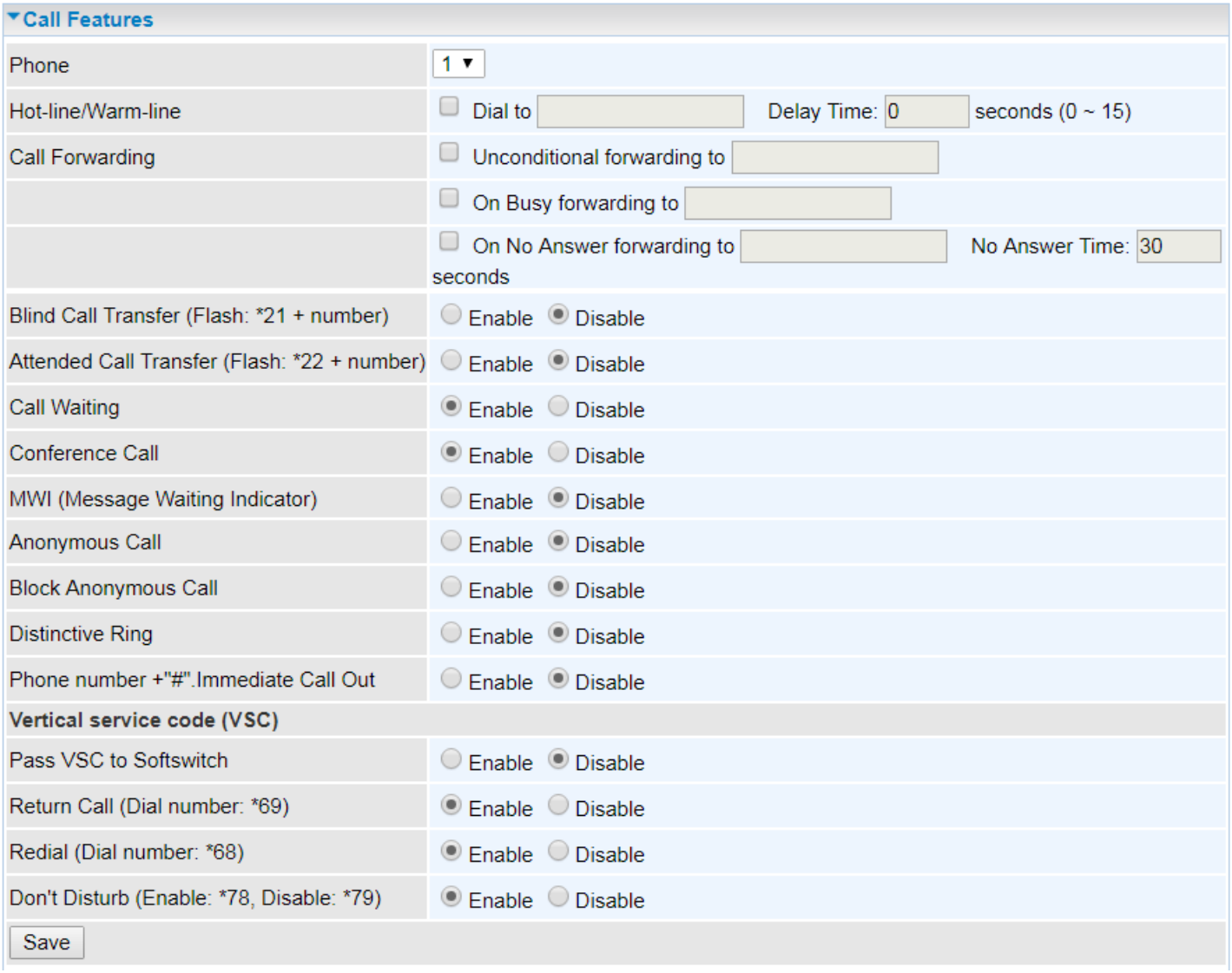
3) Phone 2: For Weekend Local calls: I set a dial rule, 0[2456]x.T, on my phone port 2.

Mobilecheap.com is the default VoIP provider I set on Phone_2. When I call out 123-39-45678 for a mobile call, 123 is replaced with 614. Therefore, 614-394-5678 is the actual phone number called out via Mobilecheap.com provider.



Call Features

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



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

Hot-line: Pre-selected a phone number and set the delay time to **0** to active the Hot-line feature. When taking the telephone off hook, this outgoing call will route to the pre-selected number without dialing the number.

- **To make an outgoing call:** Not allowed! Once the Hot-line is being turned ON, no other outgoing calls are allowed except the hot-line number.
- **Receive Incoming Call:** Yes. No affected by this feature.

Warm-line: Pre-selected a phone number and pre-configure the delay time **between 1~15 seconds** to active the Warm-line feature. When the time delay has elapsed after taking the phone off hook, this outgoing call will route to the pre-selected number, no dialing is required.

- **To make an outgoing call:** Allowed! Replace a call before the delay time has elapsed.
- **Receive Incoming Call:** Yes. No affected by this feature.

Call Forwarding: All incoming can redirect to any phone number, a mobile number or landline

telephone number, to get picked up.

- **Unconditional forwarding to:** Forward all incoming calls to a pre-selected phone number automatically. Input a phone number in the given space.
- **On Busy forwarding to:** Forward incoming calls to a pre-selected phone number when the line is busy. Input a phone number in the given space
- **On No Answer forwarding to … No Answer Time (Seconds):** Forward incoming calls to a pre-selected t phone number when calls are not answered within a certain time in seconds. Input a phone number and time in seconds in the given spaces.

Blind Call Transfer (Flash: *21 + number): A direct call transfer to the second party without speaking to the party. Enable to activate the feature.

1. Hold the original call
2. Press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone until you hear the dial tone
3. Then dial *21 and the number of the second party.

Attended Call Transfer (Flash: *22 + number): Need to consult with the second party before transferring the call. Enable to activate the feature.

1. Hold the original call
2. Press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone until you hear the dial tone
3. Dial *22 and the number of the second party.
4. After speaking with the second party
5. Then press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone again to complete the transfer.

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

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

MWI (Message Waiting Indicator): After enabling this feature, users will be able to see light flashing on their phones to indicate the presence of a new voice message.

Anonymous Call: This feature enables you to restrict your phone number from displaying to the called party. When enabled, your phone number will be withheld and not be revealing to the called party.

Block Anonymous Call: All calls from people who have withheld their phone number can get rejected. After enabling this feature, your BEC 9900VA will reject calls with no phone number.

Distinctive Ring: This call feature is only available from a VoIP Service Provider which enables each telephone number to have a distinctive ring sound.

Note: Before enabling this feature, please consult with your VoIP Service Provide to be sure it can be supported.

There is a ringtone list available in the BEC 9900VA, after enabling this feature, your BEC 9900VA will adapt a specific ring pattern on the list requested by your VoIP Service Provider for a specific telephone number.

When it is being disabled, all income calls will adapt the default ringtone for all telephone lines.

Phone number + "#" Immediate Call Out: Enable to call out immediately after pressing the #.

Pass VSC to Softswitch:

- **Enable** to pass VSC(Vertical Service Code) to the SIP server of ITSP which allows the SIP server to handle all its unique calling features such as Return Call, Call Redial, Don't Disturb, etc. Under this circumstance, users need to pay for such service, please ensure you check with your SIP provider for more information.
- **Disable** to let the BEC 9900VA to handle all available call features.

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

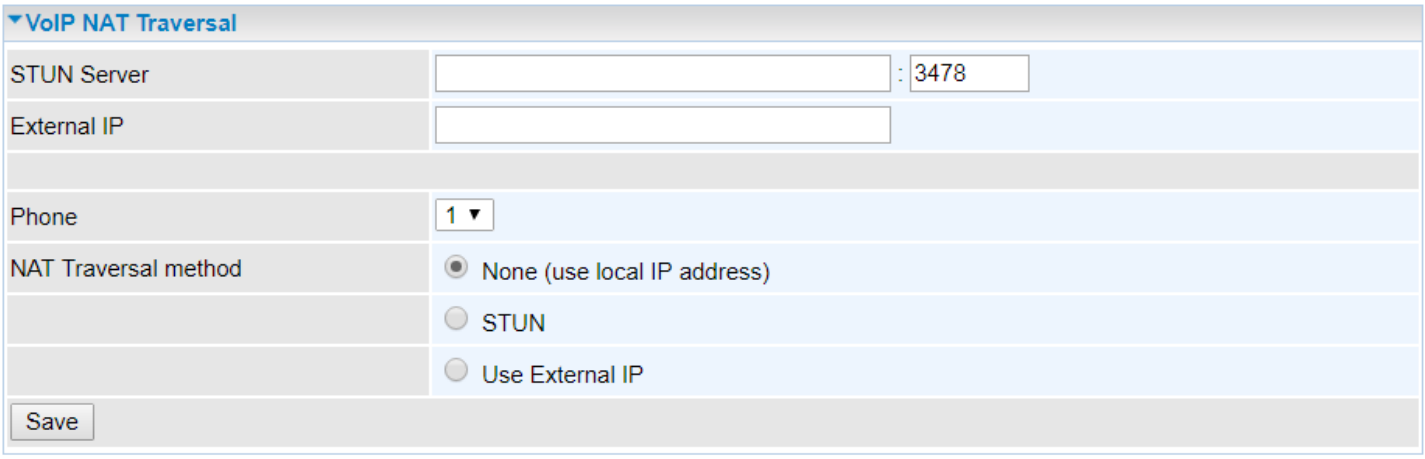
Redial (Dial number: *68): Dial *68 to redial the latest outgoing call number.

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

NAT Traversal for VoIP

BEC 9900VA VoIP adapts SIP technology as main telephony protocol to provide voice call services over the Internet. This NAT Transversal of SIP feature resolves common NAT / firewall problem when your BEC 9900VA VoIP is behind the NAT / another router to ensure all incoming calls (anyone from outside to place calls) can get picked up and protect the SIP network as well.

NOTE: Use this feature if your BEC 9900VA is behind another router on a private network and does not obtain a public IP address.



STUN (Simple Traversal of UDP through NATs) Server: Input STUN server IP address and port number in the given space. STUN server not only checks and discovers the Public WAN IP and port of an external router but also determine the kind of NAT the BEC 9900VA is behind.

Note: STUN server normally operates on port 3478. If your STUN server uses other port than 3478, make sure you update this information.

External IP: Input a Public WAN IP address of the router in front of the BEC 9900VA in the given space.

Note: If router's WAN / Public IP changes all the time, it is ideal to use STUN server or consult with your Service Provide if getting a static IP address if feasible; otherwise, manual updating your external router IP address would be required.

Phone: Choose which phone to use NAT traversal when behind another router on a private network.

NAT Traversal Method:

- **None** to disable the feature
- Use **STUN server** to do resolve NAT/firewall issue and ensure you input the STUN server IP address in the given space above.
- Use External IP of the router which is in front of the BEC 9900VA. Please make sure this external router obtains a public WAN IP address then input this IP address in the given space above.

Example: Making 3-way Calling

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

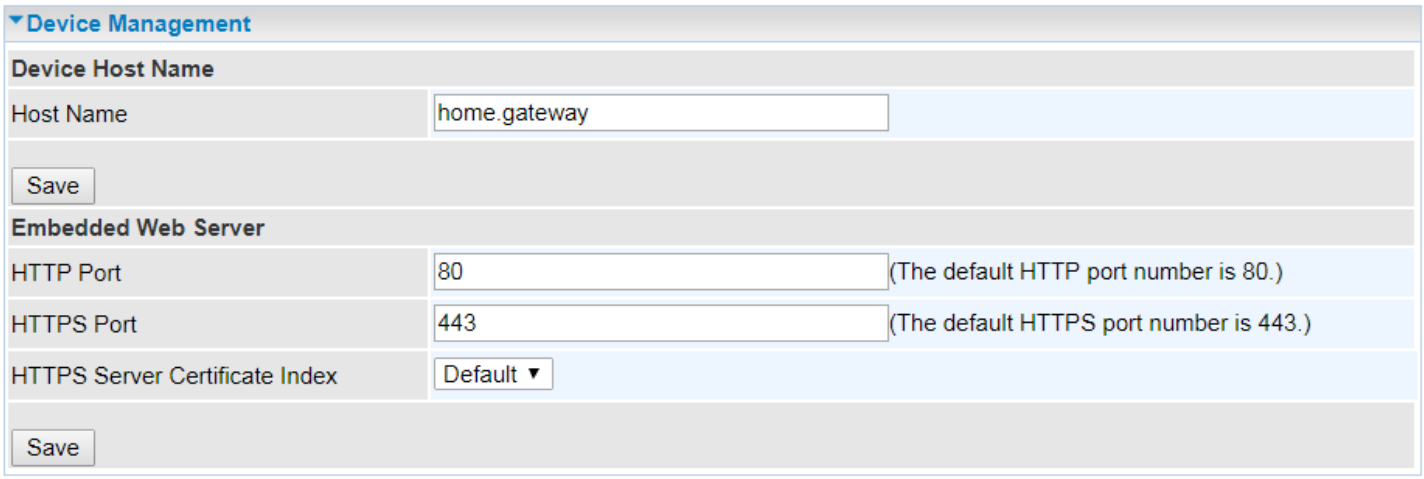
Step – 6: Bill presses flash again to merge all 3 calls.

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

Access Management

Here are the features in **Access Management:** Device Management, SNMP, Syslog, Universal Plug & Play, Dynamic DNS, Access Control, Packet Filter, CWMP (TR-069), Parental Control, SAMBA & FTP Server and BECentral Management.

Device Management



Device Host Name

Host Name: Enter the host name of the router. Default is **home.gateway**

Embedded Web Server

HTTP Port: It is the embedded web server (Web GUI) accessing port, default is **80**. It can be changed other port other than port 80, e.g. port 8080.

HTTPS Port: Similar to HTTP which is an unencrypted communication using port 80. HTTPS is encrypted by SSL using port 443 instead.

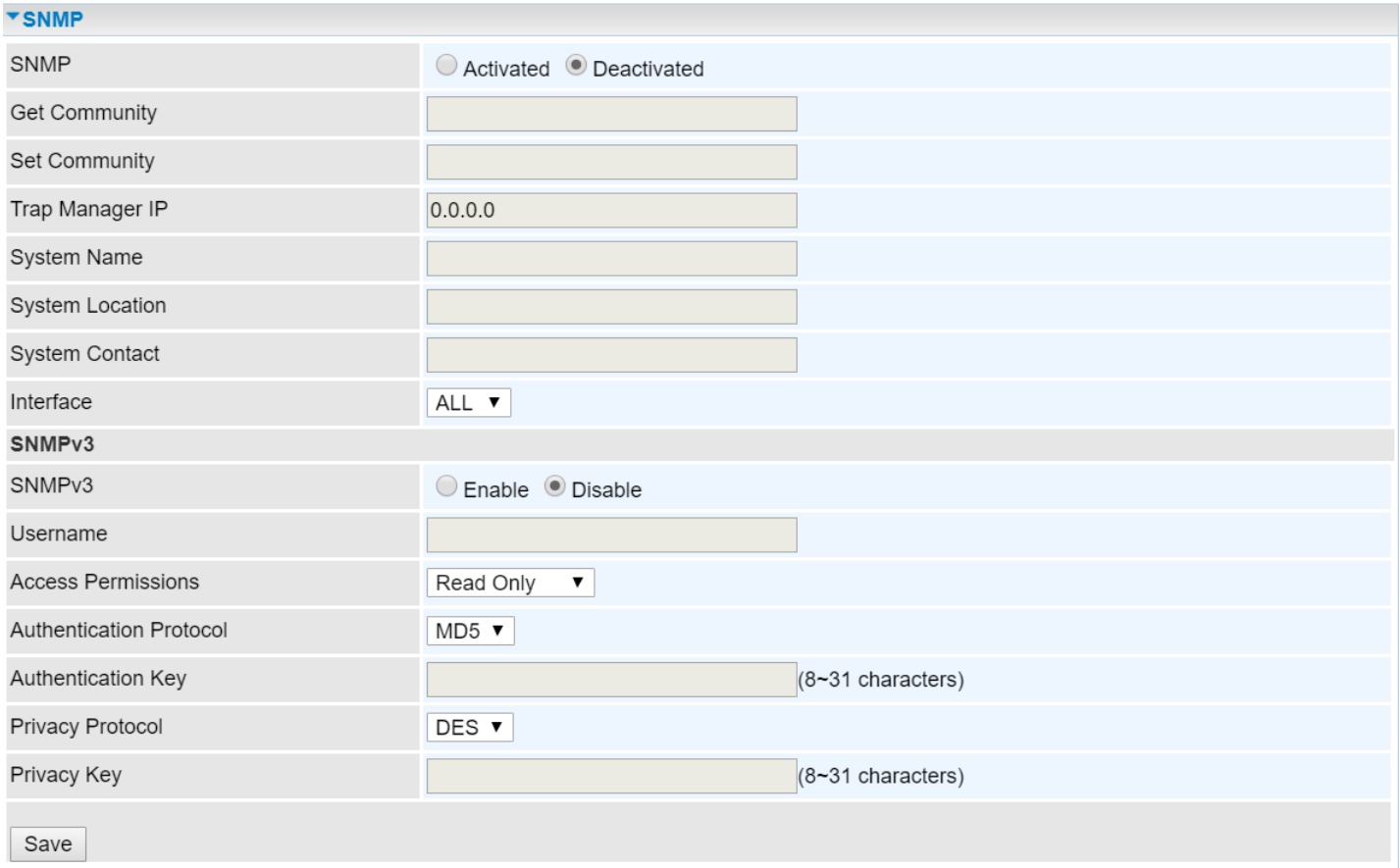
HTTPS Server Certificate Index: *HTTPS* known as HTTP-over-SSL tunnel protocol. Select a certificate to identify the system web server. When accessing to the web server (Web GUI), the browser will issue a warning page.

To import certificates, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Click **Save** to apply settings.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. The 9900VA serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.



SNMP: Activate to enable SNMP.

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.

System Name / Location / Contact: String descriptions of the SNMP agent.

Interface: Select the access interface. Choices are **LAN** or **ALL** (Both LAN and WAN).

SNMPv3

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.

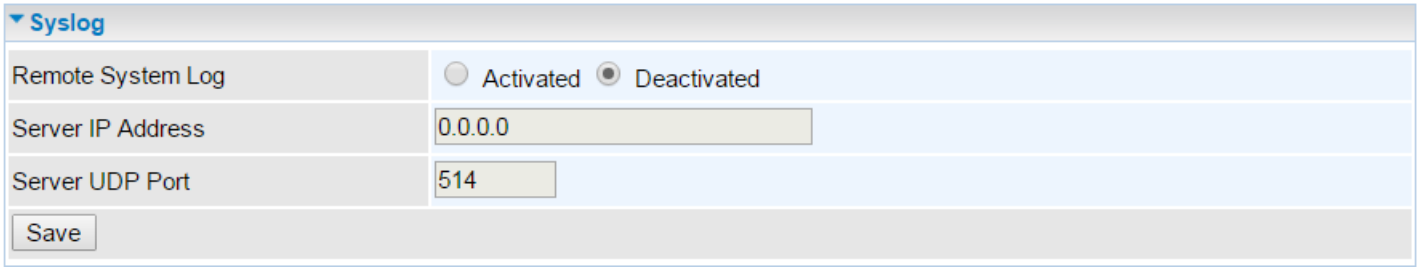
Privacy Protocol: Select the privacy mode, DES and AES.

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

Click **Save** to apply settings.

Syslog

Use the Syslog to collect system event information to a remote log server.



Remote System Log: Select **Activated** to enable this feature

Server IP Address: Assign the remote log server IP address.

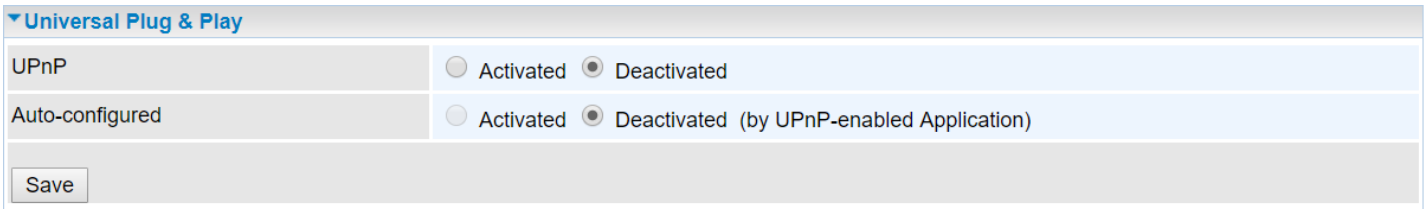
Server UDP Port: Assign the remote log server port, 514 is commonly used.

Click **Save** to apply settings.

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.



UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration's login screen without entering the 9900VA's IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the 9900VA so that they can communicate through the 9900VA, 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.

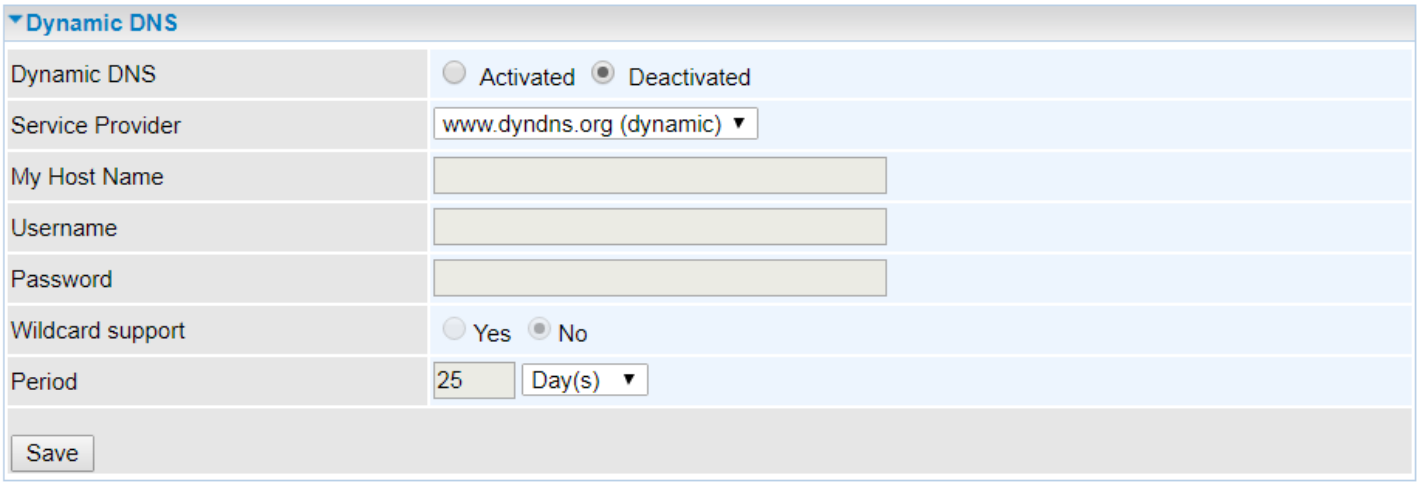
Click **Save** to apply settings.

Dynamic DNS (DDNS)

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

Here users can register different WAN interfaces with different DNS Providers.

If you do not have a DDNS account, please choose a DDNS Service Provider from the list then go to their website to create an account first.



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 9900VA by your Dynamic DNS provider.

Username / Password: Enter the username and password of the account you created with this service provider.

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

Period: Setup a time on how often the 9900VA will update the DDNS server with your current external IP address.

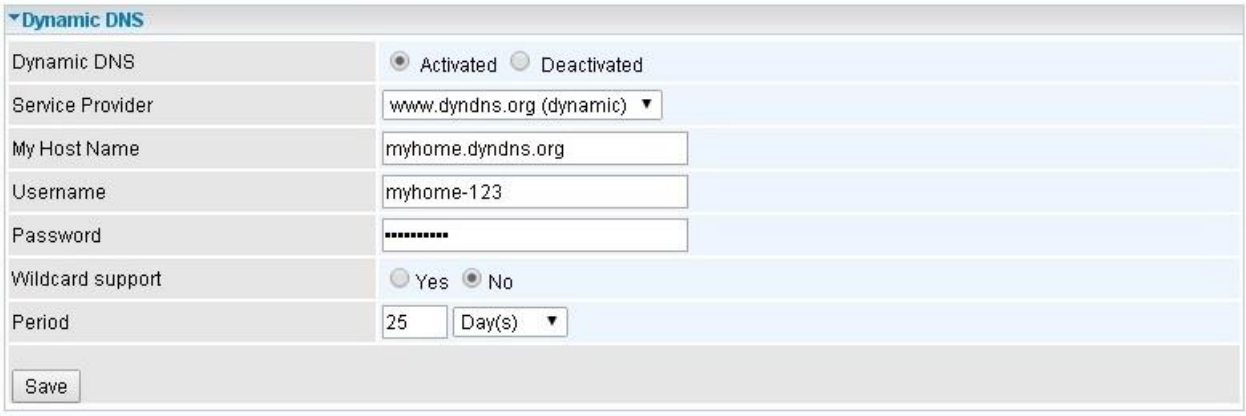
Click **Save** to apply settings.

Example: How to register a DDNS account

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

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

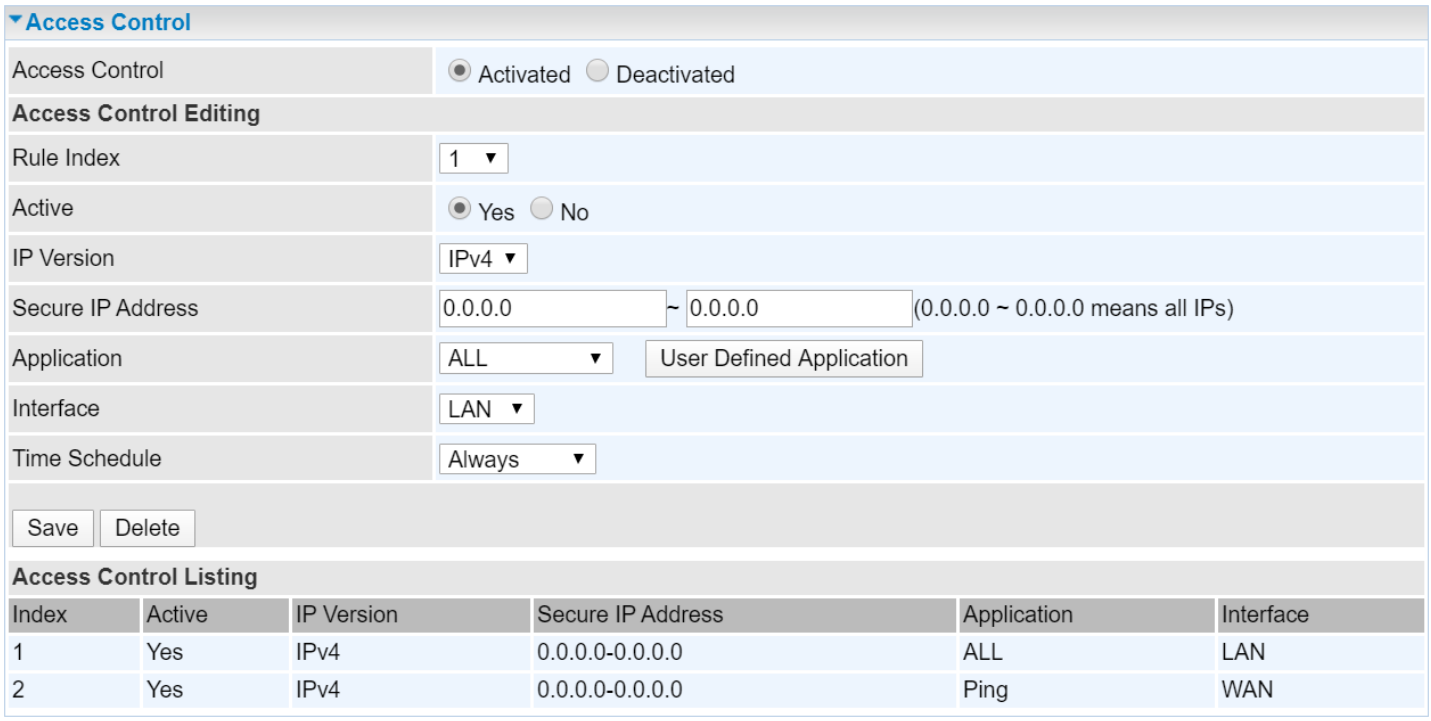
DDNS: www.hometest.com using username/password test/test



Access Control

Access Control Listing allows you to determine which services/protocols can access the 9900VA 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: Click **Activate** to enable the Access Control function.

Rule Index: The numeric rule indicator.

Active: Yes to activate the rule.

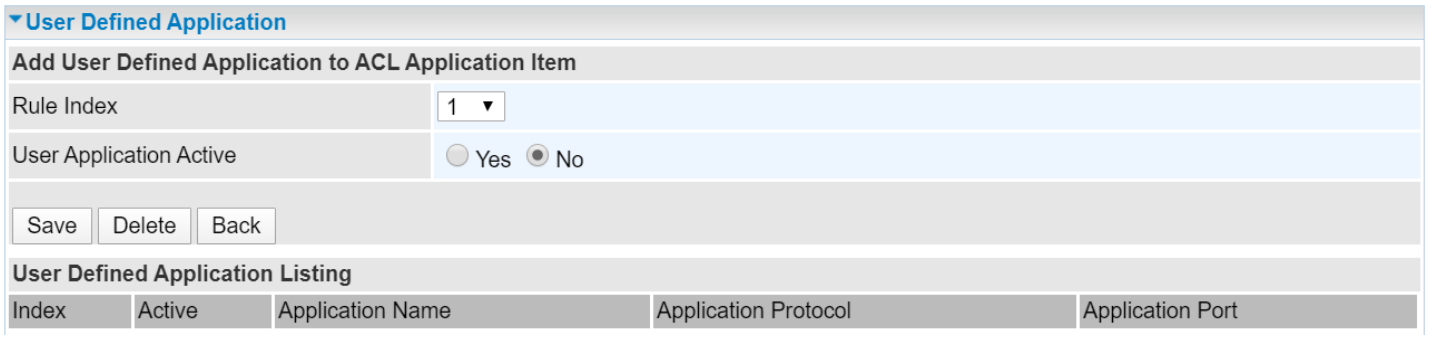
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the 9900VA. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the commonly used applications or manually create an application.

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

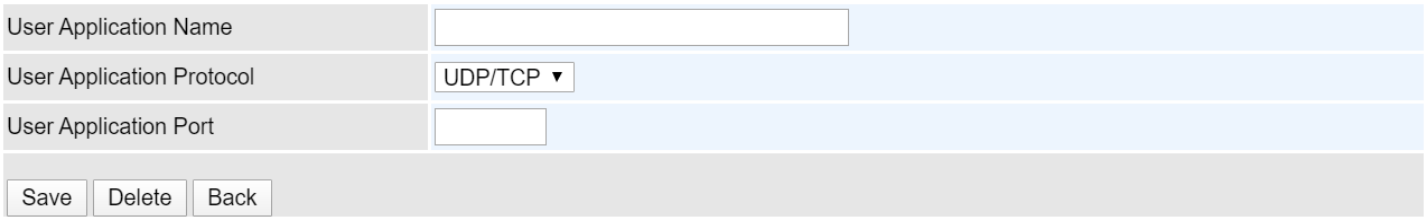
Click **Save** to apply settings.

User Defined Application



Rule Index: The numeric rule indicator.

User Application Active: Yes to add a new rule.



User Application Name: A self-define name to identify the application.

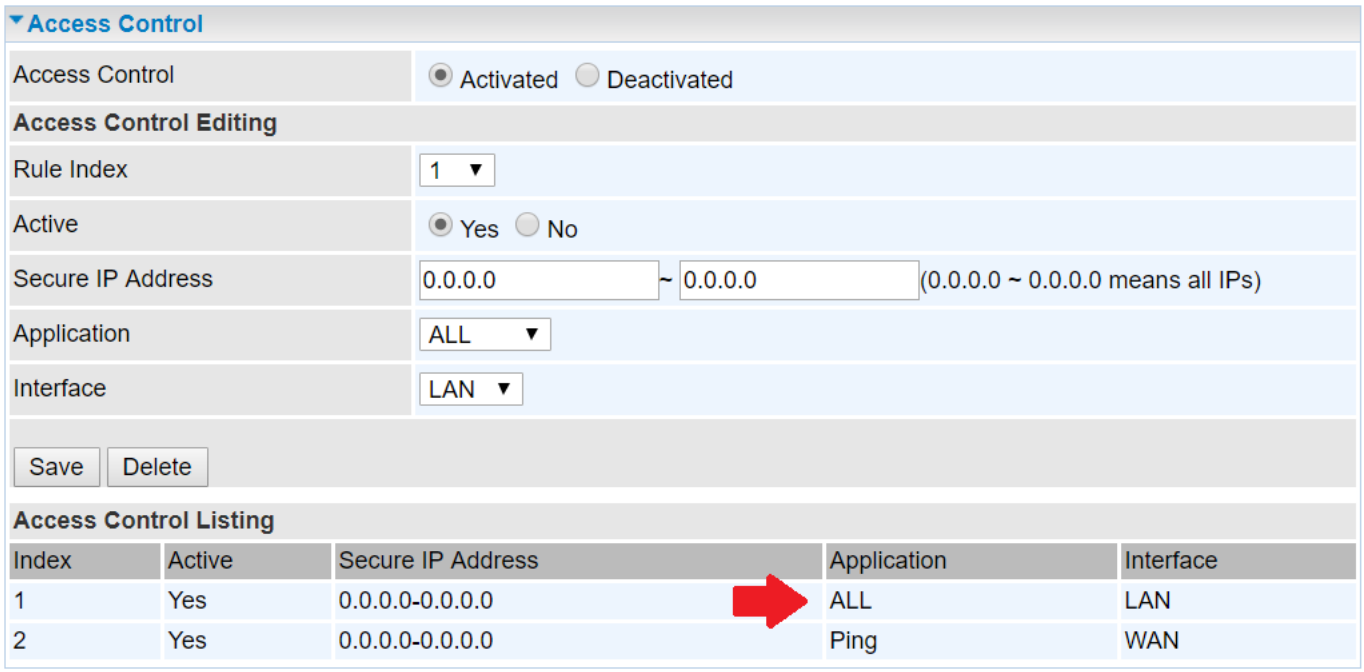
User Application Protocol: Enter a protocol, TCP, UDP, UDP/TCP, to use for this application.

User Application Port: Enter the port number which defines the application.

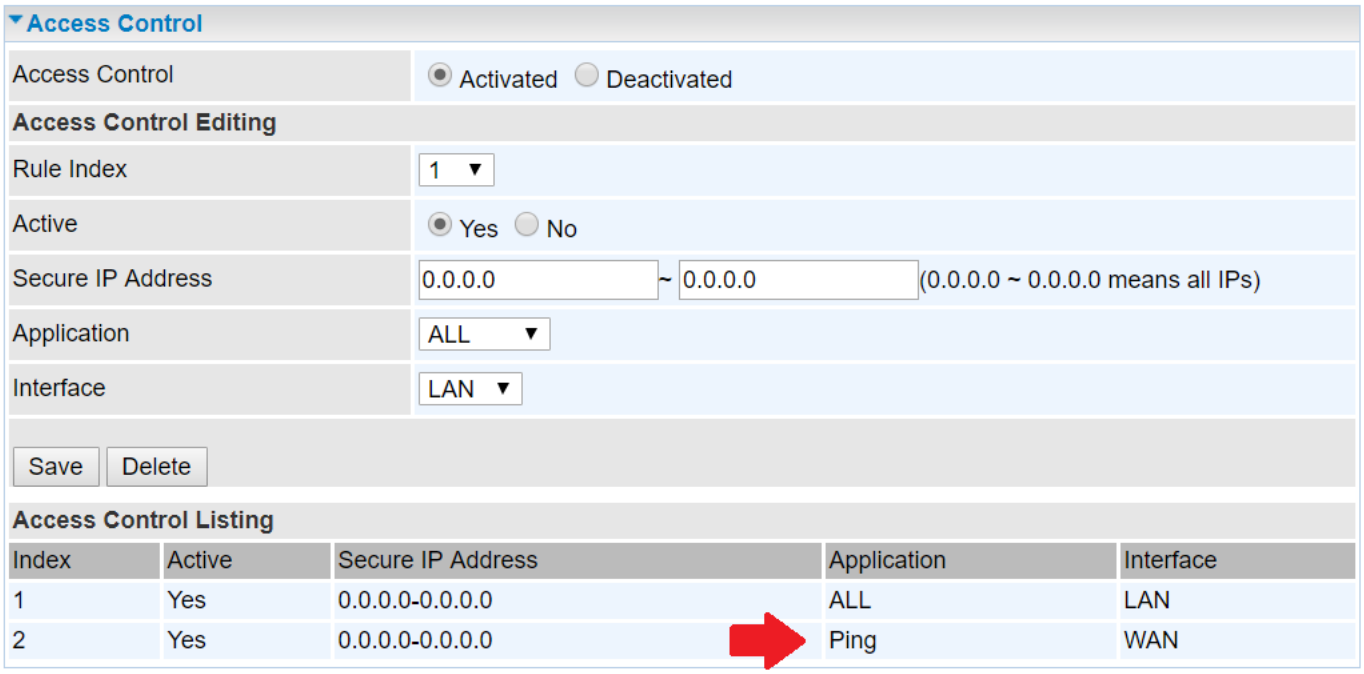
Click **Save** to save the rule.

By default, the “Access Control” has **two default rules**.

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



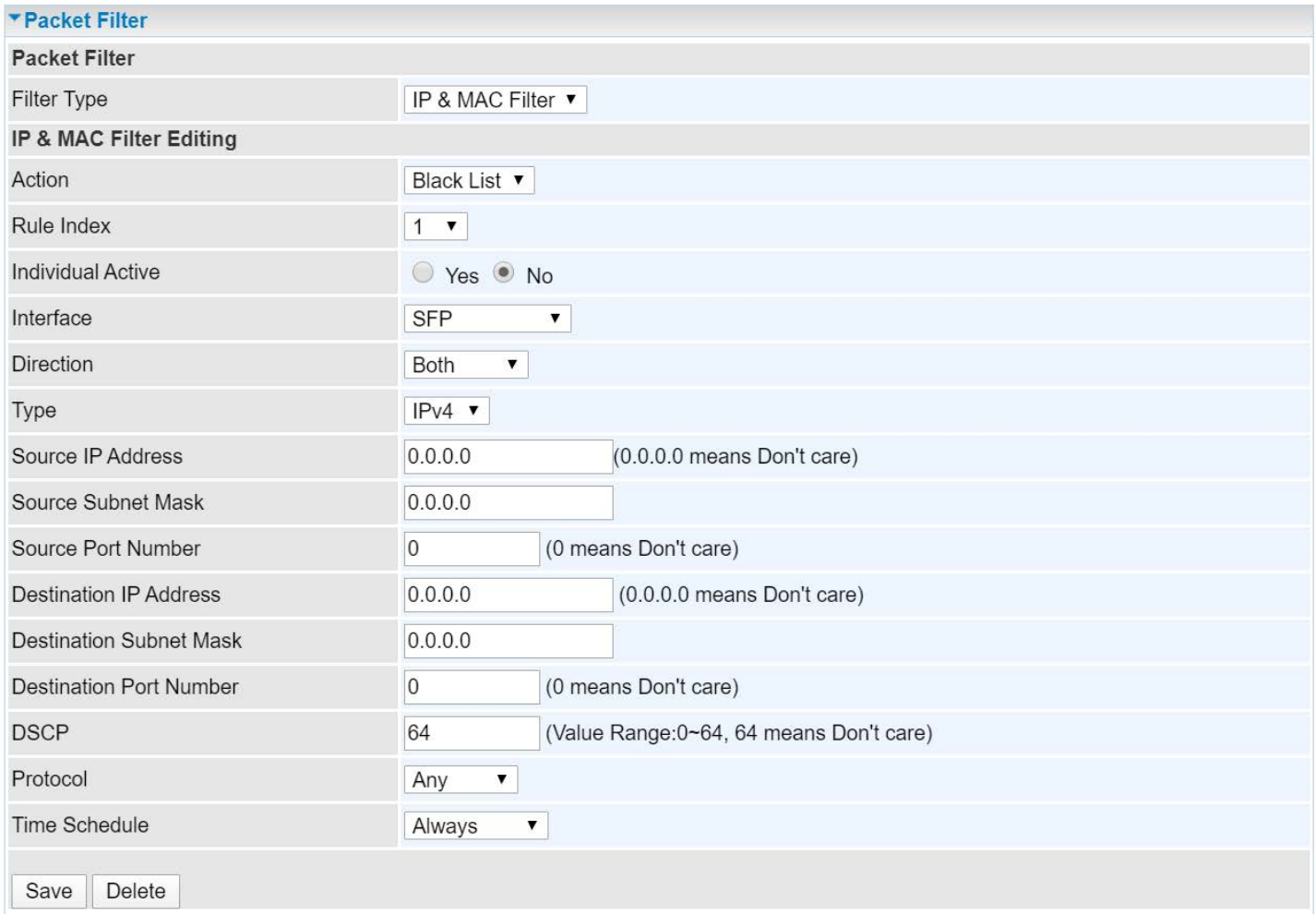
Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.



Packet Filter

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

❖ Filter Type - IP & MAC Filter



IP & MAC Filter Editing

Rule Index: The numeric rule indicator.

Individual Active: Yes to enable the rule.

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

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

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

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

- **IPv4**

Type	IPv4 ▼
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0
Source Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0
Destination Port Number	0 (0 means Don't care)
DSCP	64 (Value Range:0~64, 64 means Don't care)
Protocol	Any ▼
Time Schedule	Always ▼

Save Delete

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: Select a TimeSlot to activate this rule at a certain time, if not select **Always** to enable the rule at all times. Go to **Time Schedule** to setup a time.

- **IPv6**

Type	IPv6 ▼
Source IPv6 Address	0:0:0:0:0:0:0:0 (0:0:0:0:0:0:0:0 means Don't care)
Source IPv6 Prefix	32
Source Port Number	0 (0 means Don't care)
Destination IPv6 Address	0:0:0:0:0:0:0:0 (0:0:0:0:0:0:0:0 means Don't care)
Destination IPv6 Prefix	32
Destination Port Number	0 (0 means Don't care)
DSCP	64 (Value Range:0~64, 64 means Don't care)
Protocol	Any ▼
Time Schedule	Always ▼

Source IP (IPv6) Address/ Prefix: The source IP address or range of packets to be monitored.

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

Destination IP (IPv6) Address/ Prefix: The destination subnet IP address.

Destination Port Number: 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**

Time Schedule: Select a TimeSlot to activate this rule at a certain time, if not select **Always** to enable the rule at all times. Go to **Time Schedule** to setup a time.

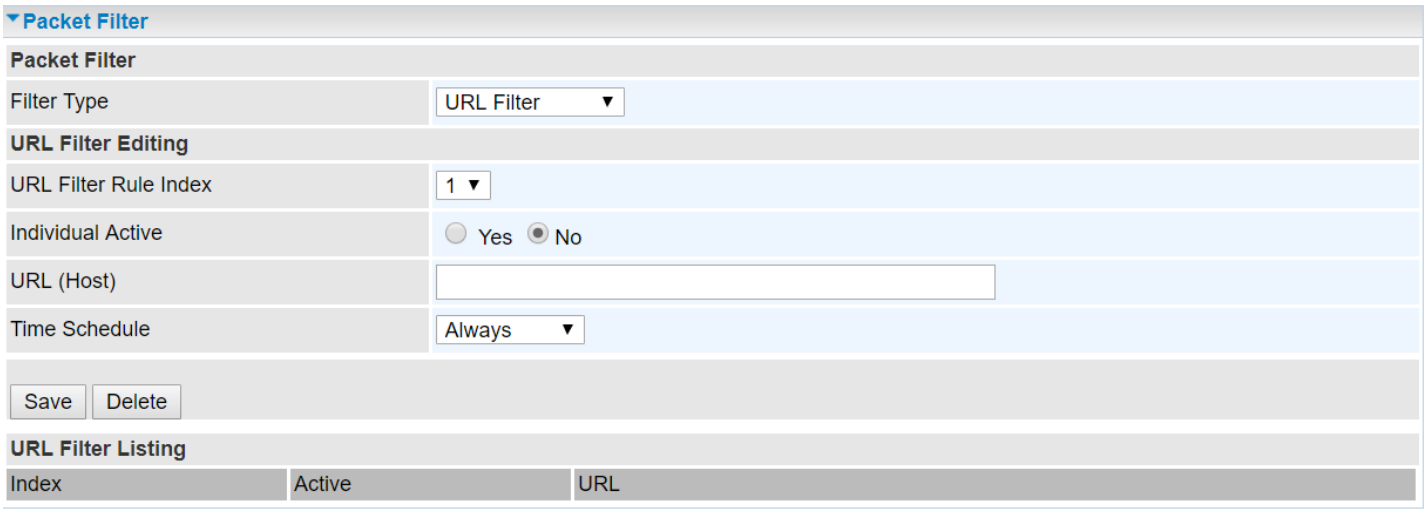
- **MAC**

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

Time Schedule: Select a TimeSlot to activate this rule at a certain time, if not select **Always** to enable the rule at all times. Go to **Time Schedule** to setup a time.

Click **Save** to apply settings.

❖ Filter Type - URL Filter



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

URL Filter Rule Index: The numeric rule indicator.

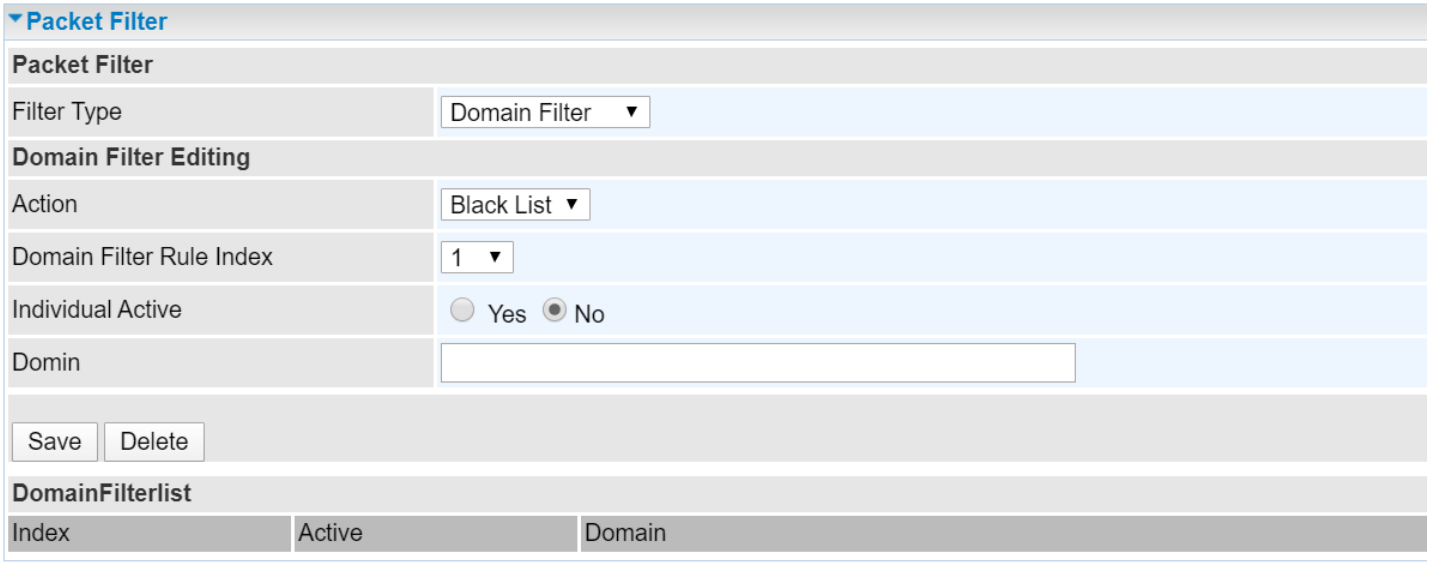
Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No 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: Select a TimeSlot to activate the rule. Go to **Time Schedule** to configure a time control first.

Click **Save** to apply settings.

❖ Filter Type - Domain Filter



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

Domain Filter Rule Index: The indication of the rule number.

Individual Active: Click **Yes** to enable this rule/policy.

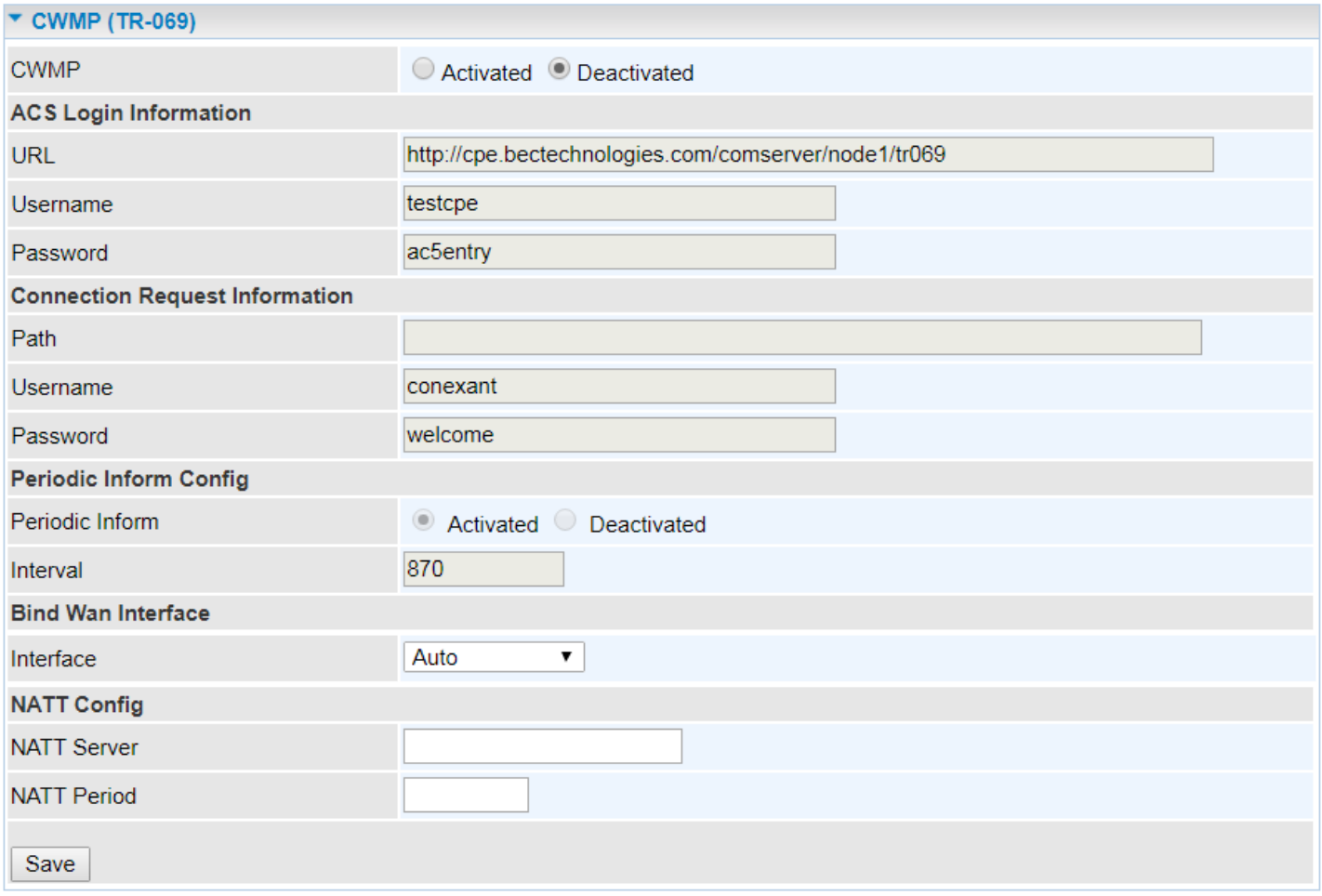
Domain: Enter the domain name in the blank field to be allowed or prohibited.

Click **Save** to apply settings.

CWMP (TR-069)

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

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



CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

Username: Specify the ACS Username 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.

Bind WAN Interface

Interface: Specify any available or a single WAN interface to handle TR-069 requests.

NATT Config - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

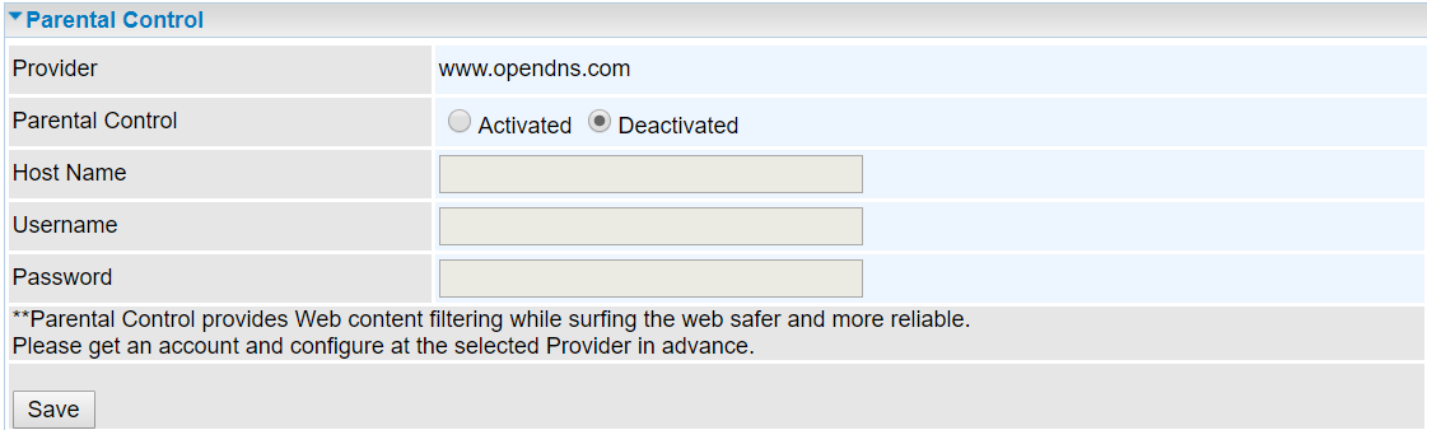
NATT Server: By BEC administrator only.

NATT Period: By BEC administrator only.

Click **Save** to apply settings.

Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.



To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Parent Control: Enable the feature by clicking the **Activate**d

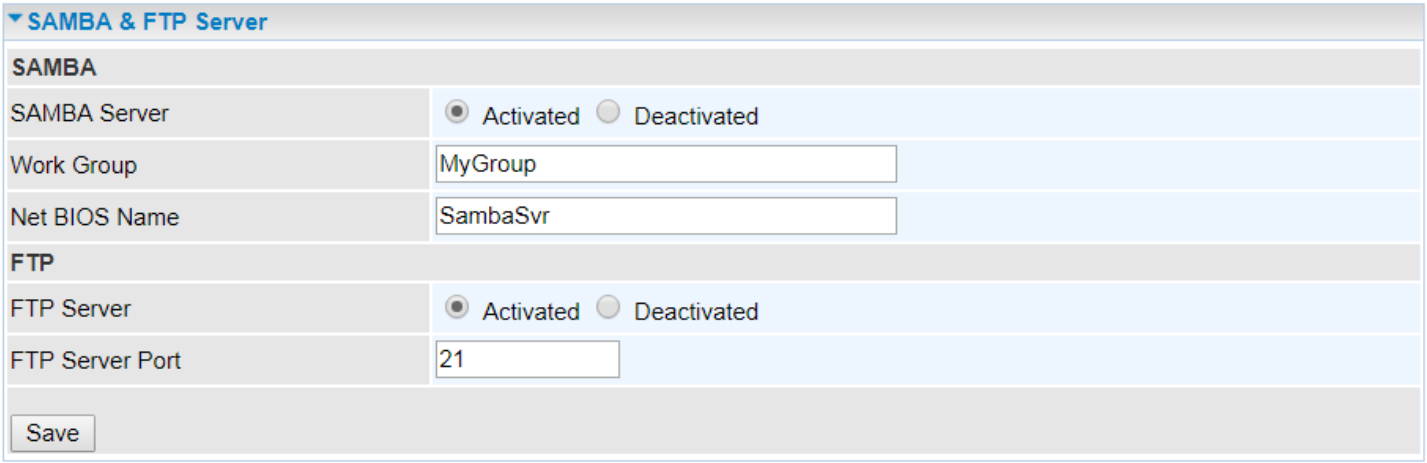
Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blink.

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply settings.

SAMBA & FTP Server

Samba and FTP are served as network sharing.



SAMBA

SAMBA Server: Activated to enable SAMBA sharing.

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

NetBIOS Name: The sharing NetBIOS name.

FTP

FTP Server: Activated to enable FTP sharing.

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

SAMBA/FTP Login Account

See User Management for more information.

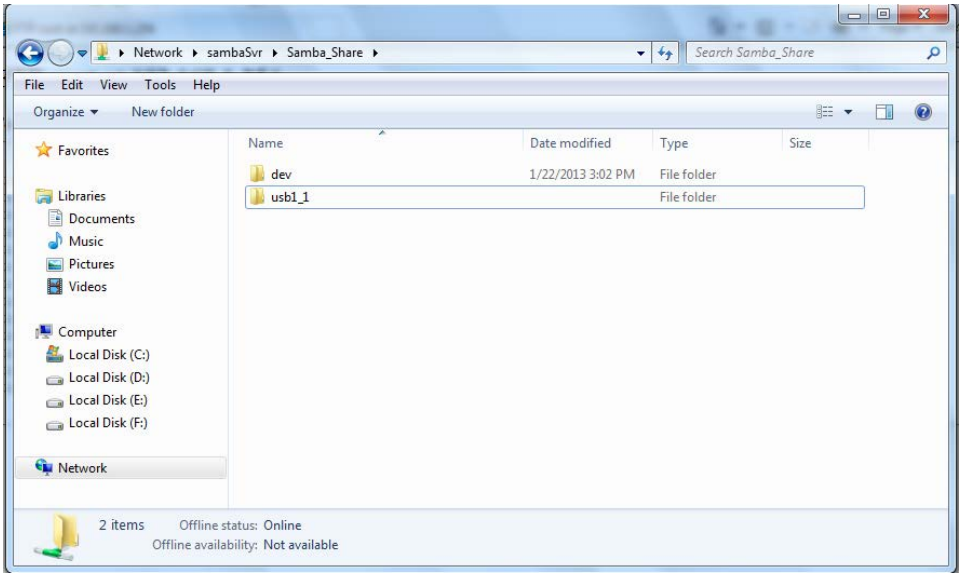
- **Default user:** admin/admin, it is the administrative user and a super user; it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.
- **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

Example: How to setup Samba

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

2. Enter the Username and password.

3. Users can browse and access USB storage.



Example: How to setup FTP：

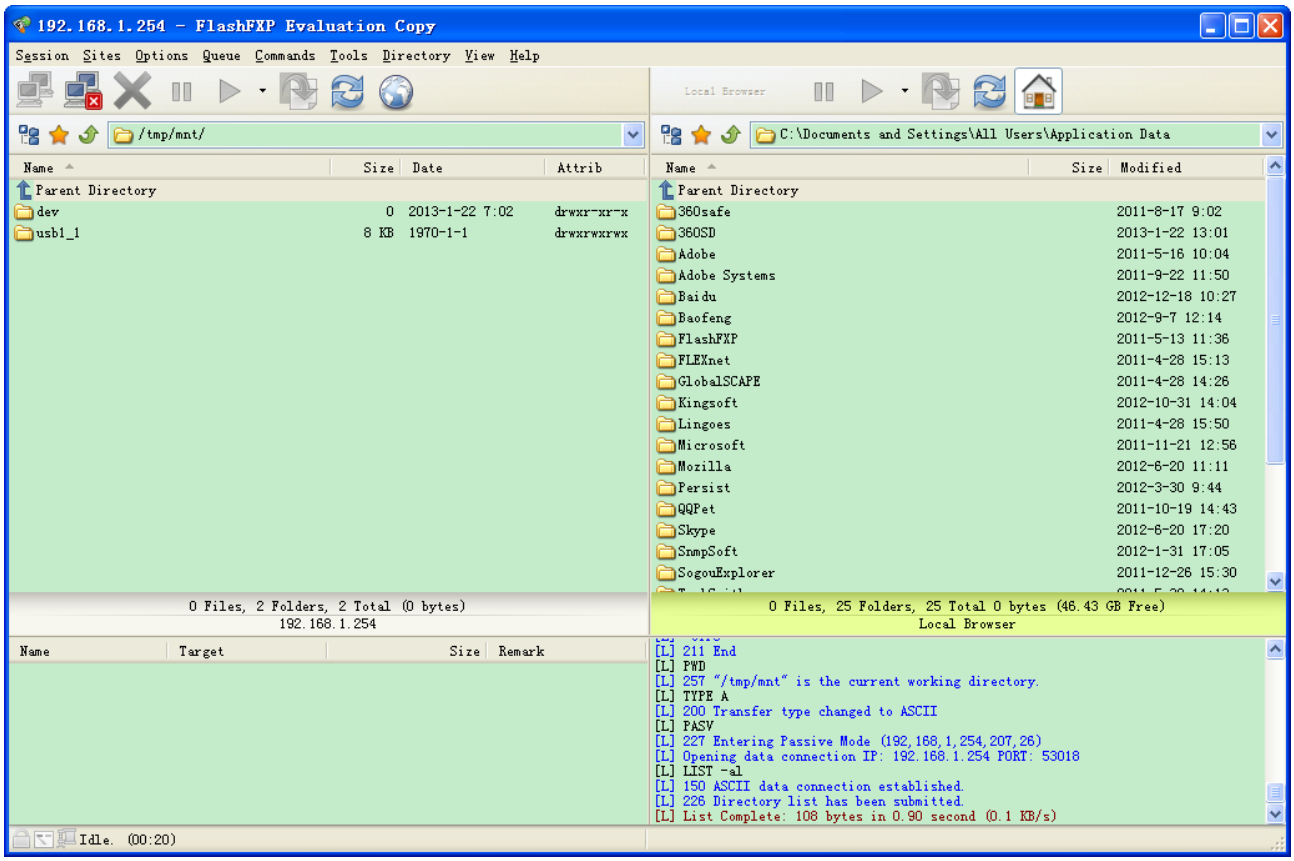
1. **Access via FTP tools**

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP

2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).

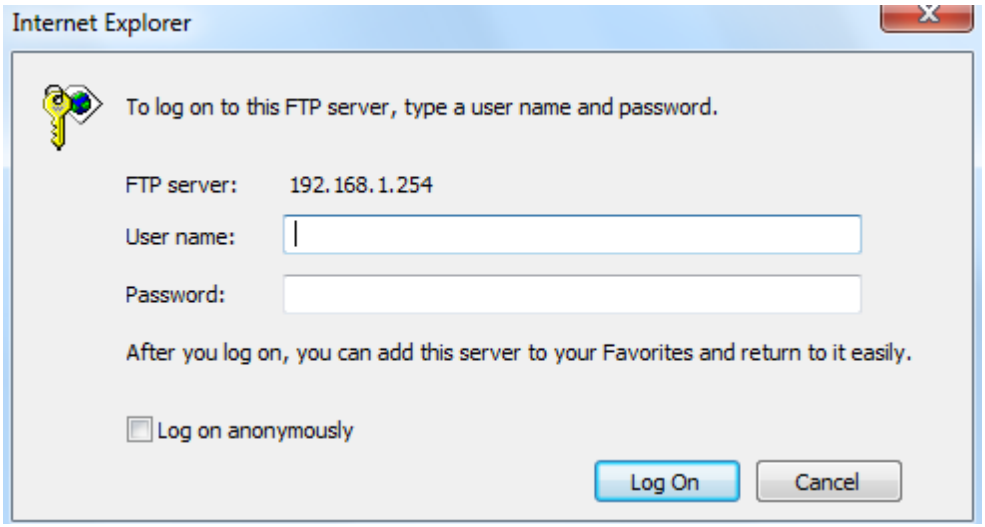
3) Connect to the ftp site.



2. **Web FTP access**

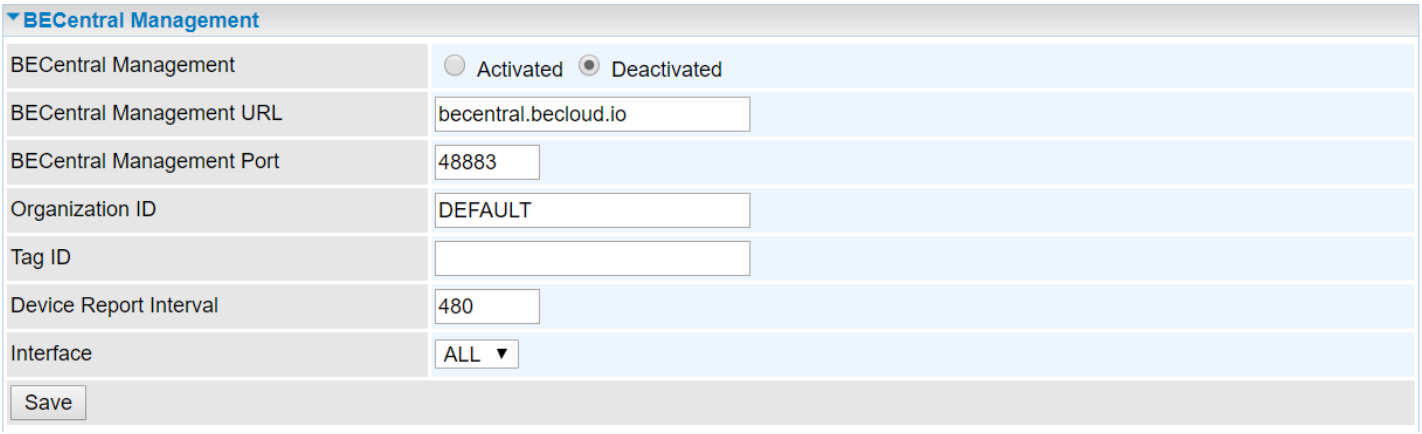
1) Enter ftp://192.168.1.254 at the address bar of the web page.

2) Enter the account's username and password.



BECentral Management

BECentral is a cloud-based device management platform that provides operators with a comprehensive suite of services to manage devices in real-time.



BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral.

BECentral Management Port: Port listened by the BECentral.

Organization ID: Customer ID (By BE C administrator only)

Tag ID: By BEC administrator only.

Device Report Interval: Enter the interval time in seconds to send inform message periodically to the BECentral.

Interface: Specify any available or a single WAN interface to handle BECentral requests.

Click **Save** to apply settings.

Maintenance

Here are the features in **Maintenance:** User Management, Certificate Management, Time Zone, Firmware & Configuration, System Restart, Auto Reboot and Diagnostic Tool.

User Management

User Management provides the Administrator with the ability to grant access control and manage GUI login credentials for each user.

There are two access management levels, Administrator and User.

The default root account, Administrator (admin), has full access to all the features listed and ability to create other accounts with features to allow other users to access to. The User account is with limited access (specified by advanced users with admin account) to the GUI.

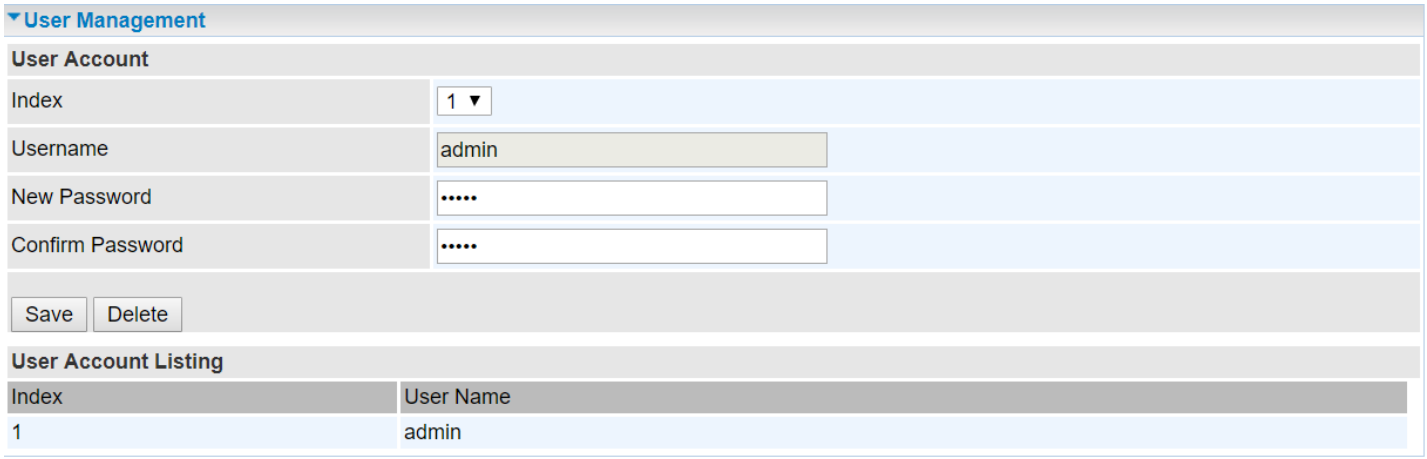
Total of **8** accounts can be created to grant access to manage the 9900VA via the web page.

❖ Administrator Account

admin/admin is the root/default account username and password.

NOTE: This username / password may vary by different Internet Service Providers.

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 Account

Index: The numeric account indicator. The maximum entry is up to 8 accounts.

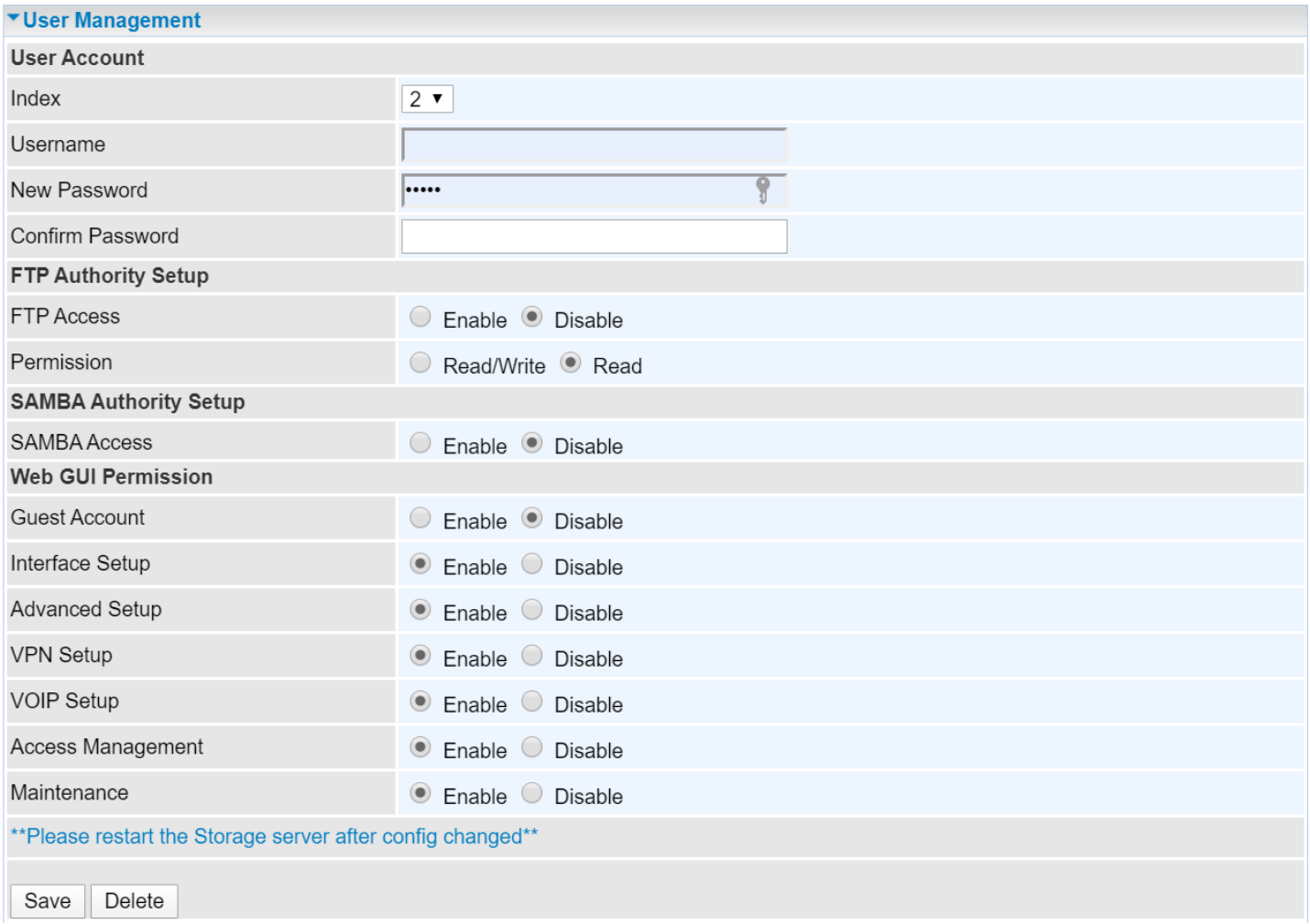
Username: Create account(s) username for GUI management.

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.

Click **Save** to apply settings.

❖ Other Accounts



User Account Setup

Index #: The numeric account indicator. The maximum entry is up to 8.

Username: Create account(s) username for GUI management.

New Password: Password for the user account.

Confirm Password: Re-enter the password.

Web GUI Permission

Guest Account: Enable to create this new guest account.

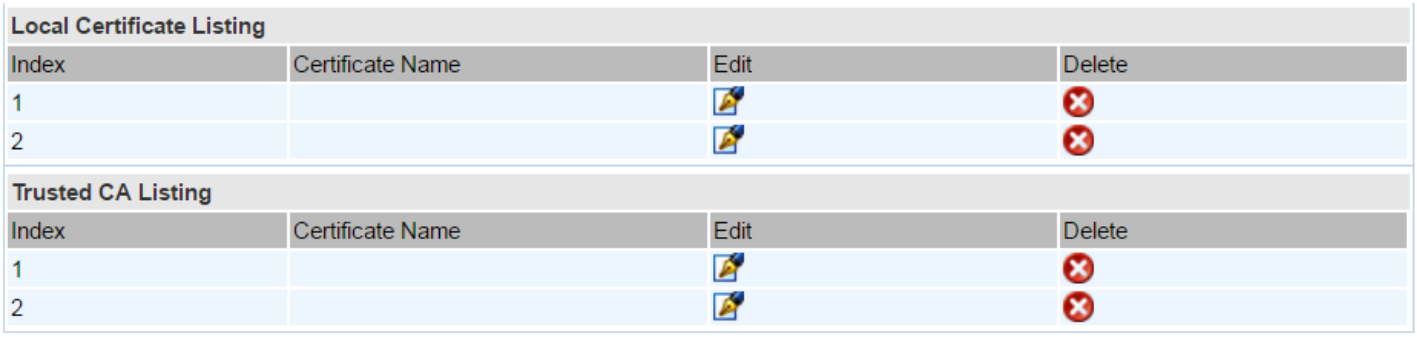
Interface Setup / Advanced Setup / VPN Setup / VoIP Setup / Access Management / Maintenance: Enable to grant this user access to these features.

When someone accesses to the 9900VA using this “user” account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account.

Click **Save** to apply settings.

Certificate Management

This feature is used for OpenVPN and HTTS Server authentication of the device using certificate. If the imported certificate doesn't match the authorized certificate with the Server, then no access is allowed.

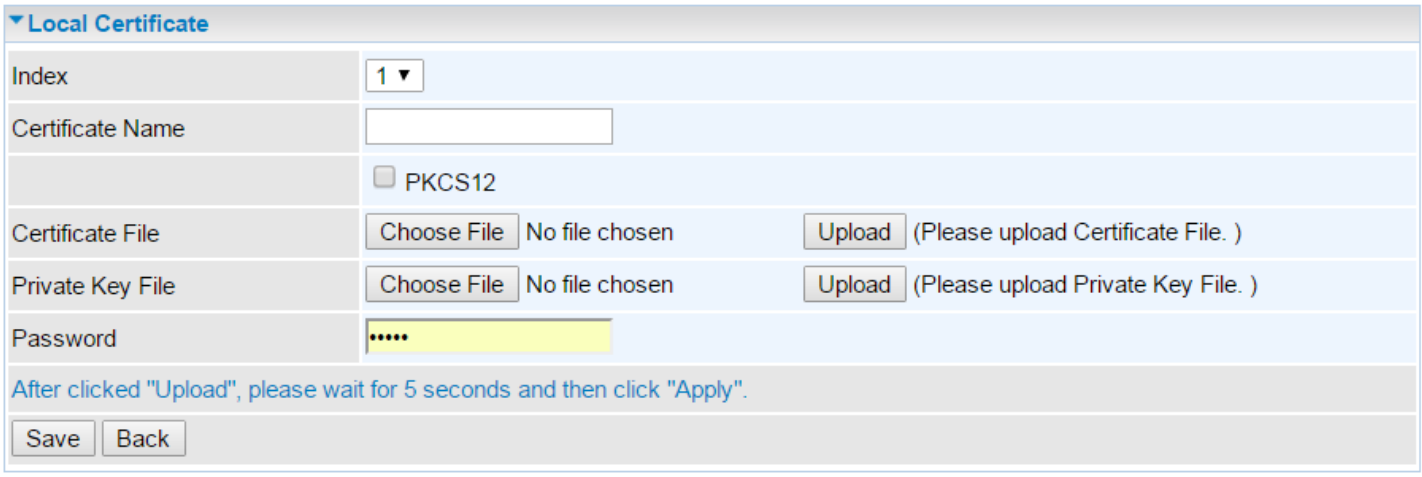


Local Certificate Listing			
Index	Certificate Name	Edit	Delete
1			
2			
Trusted CA Listing			
Index	Certificate Name	Edit	Delete
1			
2			

Edit: Click (Edit) to import a certificate.

Delete: Click (Delete) to remove the certificate from the list.

Local Certificate Listing



Local Certificate		
Index	1	
Certificate Name		
	PKCS12	
Certificate File	Choose File No file chosen	Upload (Please upload Certificate File.)
Private Key File	Choose File No file chosen	Upload (Please upload Private Key File.)
Password	•••••	
After clicked "Upload", please wait for 5 seconds and then click "Apply".		
Save Back		

Index #: The numeric account indicator. The maximum entry is up to 2.

Certificate Name: Description of the certificate.

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.

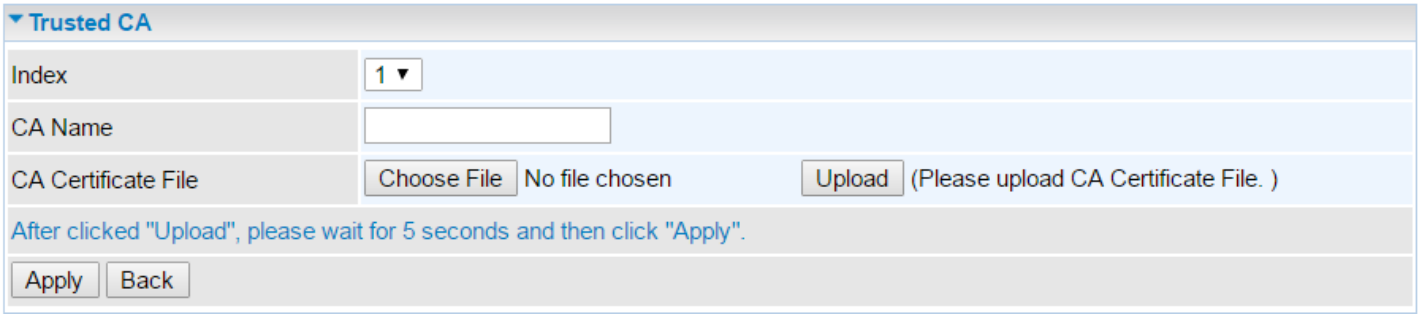
Certificate File: Browse to locate the target certificate file on PC before uploading it.

Private Key File: Browse to locate the target file on PC before uploading it. If PKCS enabled, please ignore this setting.

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

Click **Apply** to save settings.

Trusted CA Listing



Index #: The numeric account indicator. The maximum entry is up to 2.

CA Name: Description of the CA.

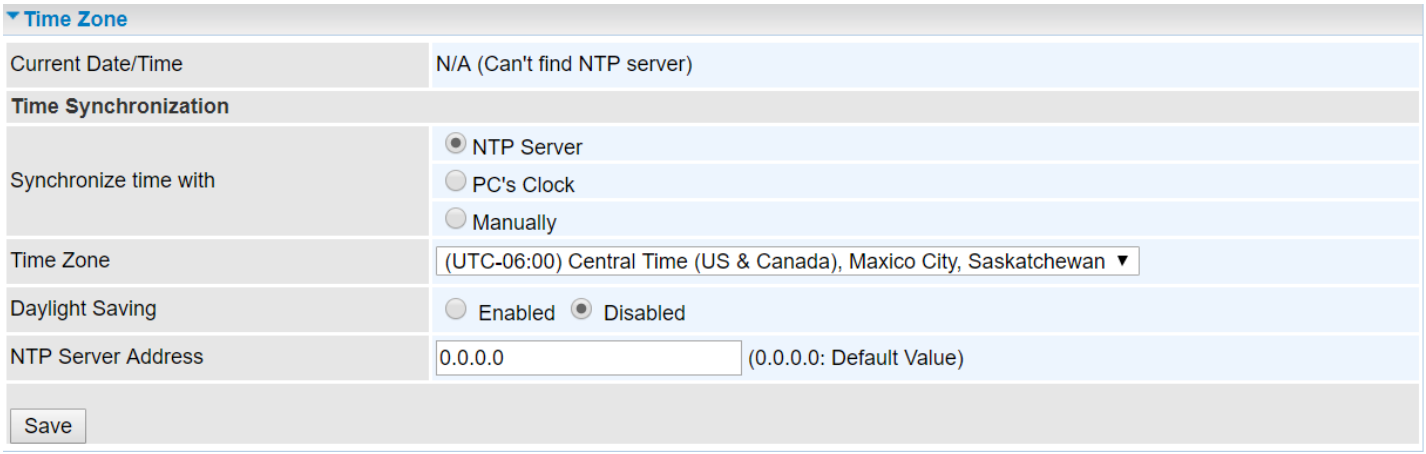
CA Certificate File: Browse to locate the target certificate file on PC before uploading it.

Click **Apply** to save settings.

Time Zone

With default, 9900VA does not contain the correct local time and date.

There are several options to setup, maintain, and configure current local time/date on the 9900VA. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.



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

- **NTP Server automatically:** To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, 9900VA will retrieve the correct local time from the SNTP server this is specified.
- **PC's Clock:** To synchronize time with the PC's clock.
- **Manually:** Select this to enter the SNMP server IP address manually.
  - **Date:** Month / Date / Year. Month – 1 ~ 12 (January ~ December).
  - **Time:** Hour: Minute: Second

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.

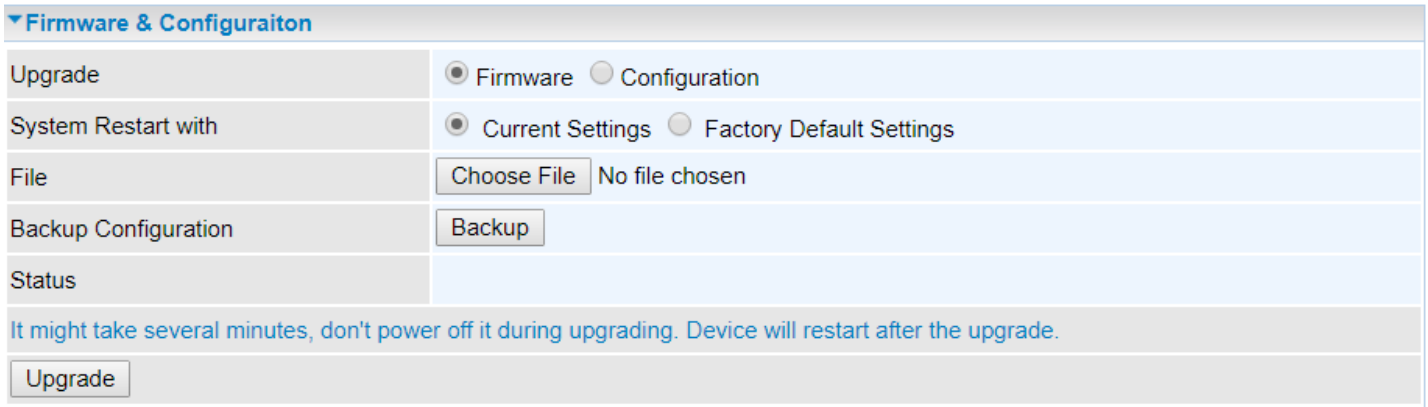
NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Click **Save** to apply settings.

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 9900VA provides an effortless way to update the code to take advantage of the changes.

To upgrade the firmware of the 9900VA, you should download or copy the firmware to your local environment first. Click **"Choose File"** to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading process. After completing the firmware upgrade, the 9900VA will automatically restart and run the new firmware.



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 **Browse** 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 if you need this configuration file to be restored back to your 9900VA device when making false configurations and want to restore to the original settings.

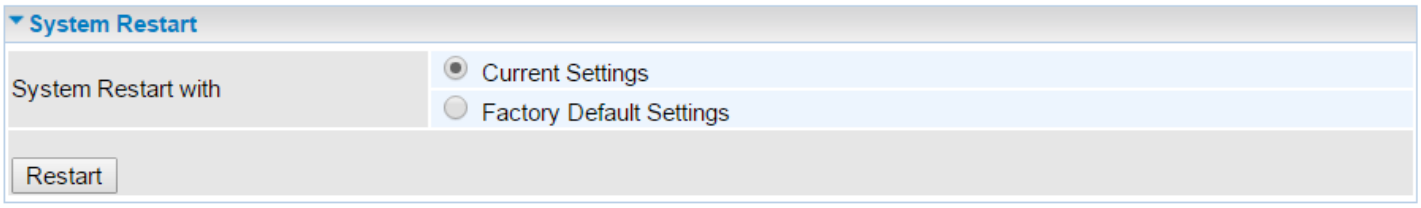
Upgrade: Click **"Upgrade"** to begin the upload process. This process may take up to two minutes.

DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your 9900VA.

System Restart

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



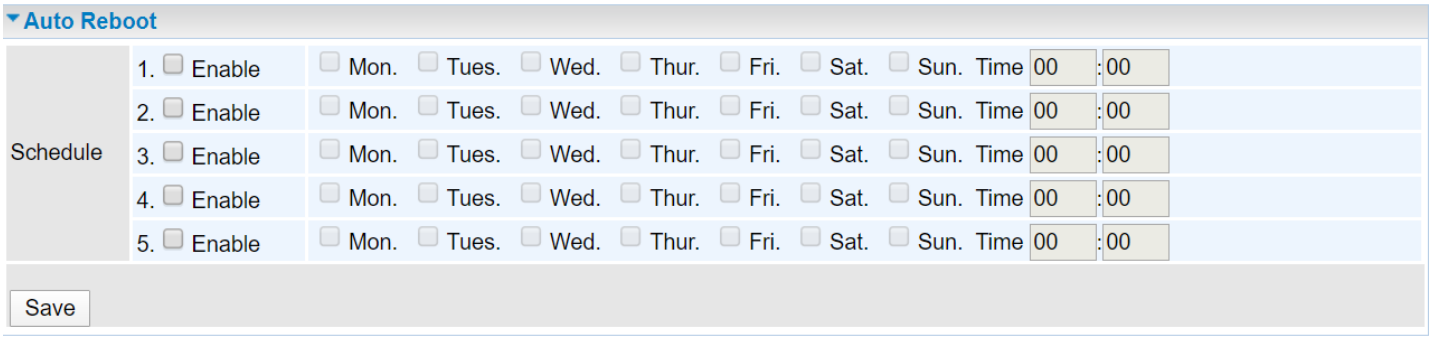
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

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

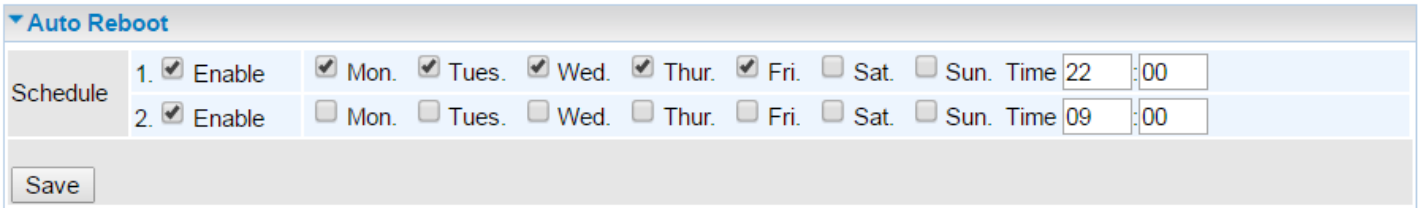
Schedule an automatic reboot for your 9900VA to ensure proper operation and best performance.

This reboot will only reboot with current configuration settings and not overwrite any existing settings.



Click **Save** to apply settings

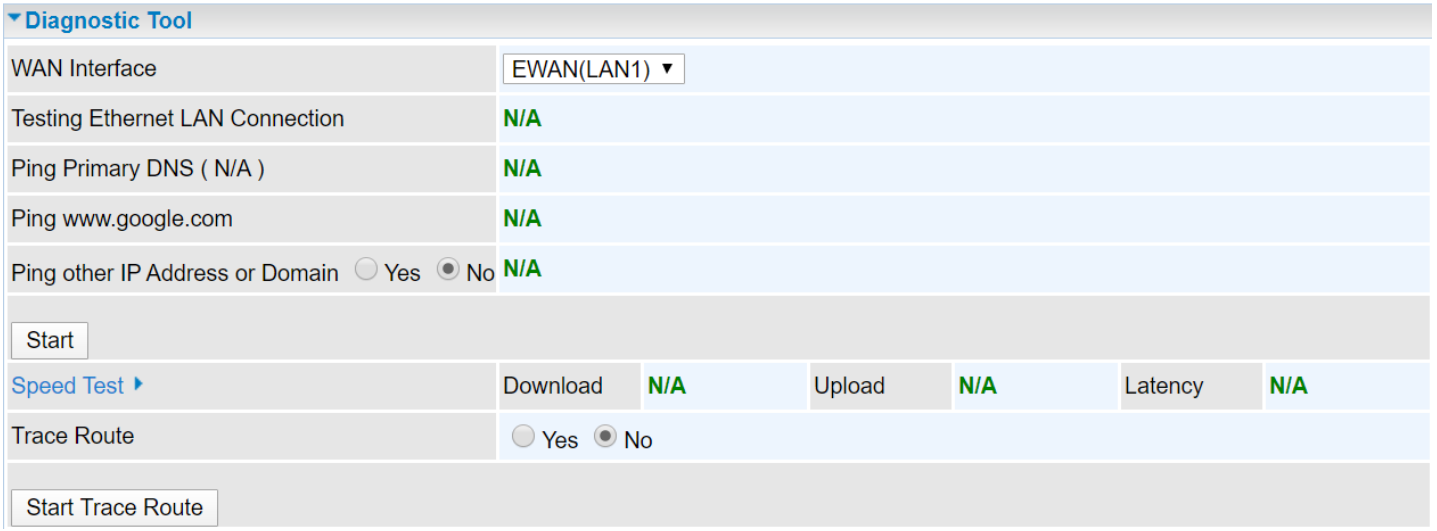
Example: Schedule 9900VA to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.



Diagnostics Tool

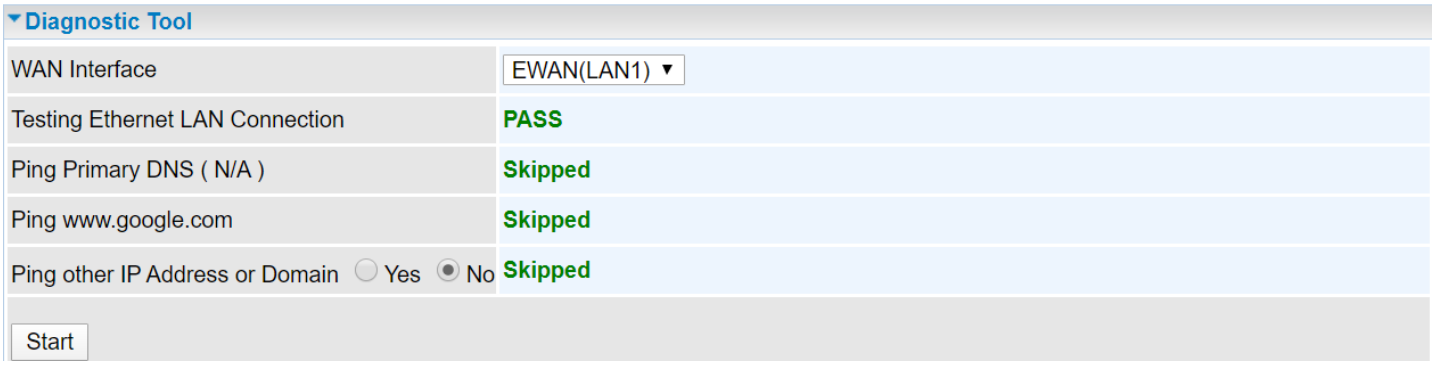
The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

EWAN (LAN1) / SPF WAN



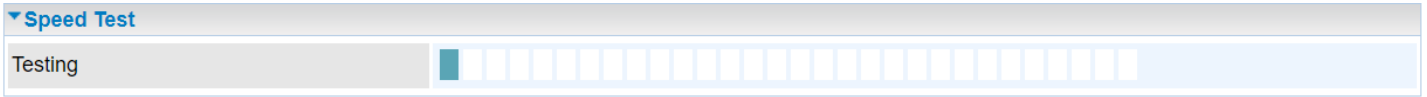
Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

Click **START** to begin to diagnose the connection.

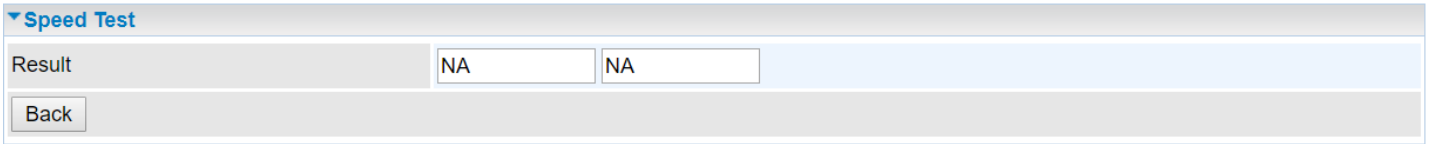


Speed Time: Measure the current uplink and downlink speed rate.

- Take less than a minute to run the test.



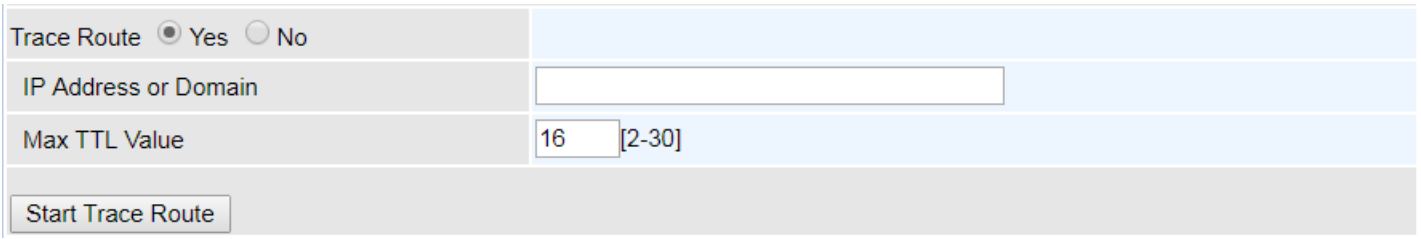
- Result in Uplink / Downlink



Click **Back** to go back to the Diagnostic Tool

Trace Route is to display how many hops (also view the exact hops) required to get to the destination.

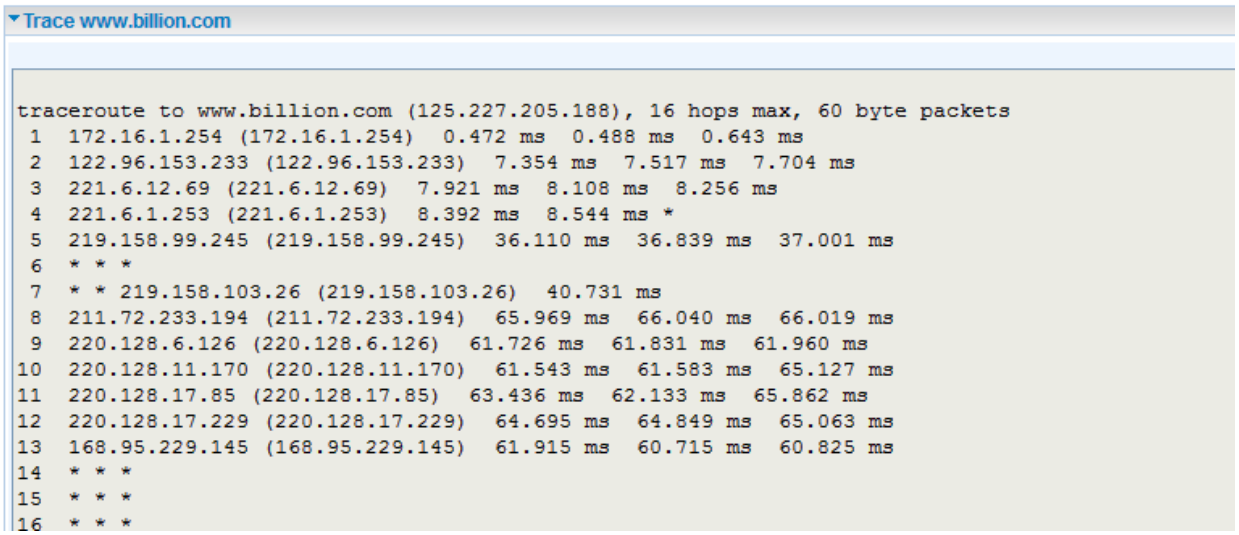
Click **Yes**, enter the IP address or domain then **Start Trace Route**.



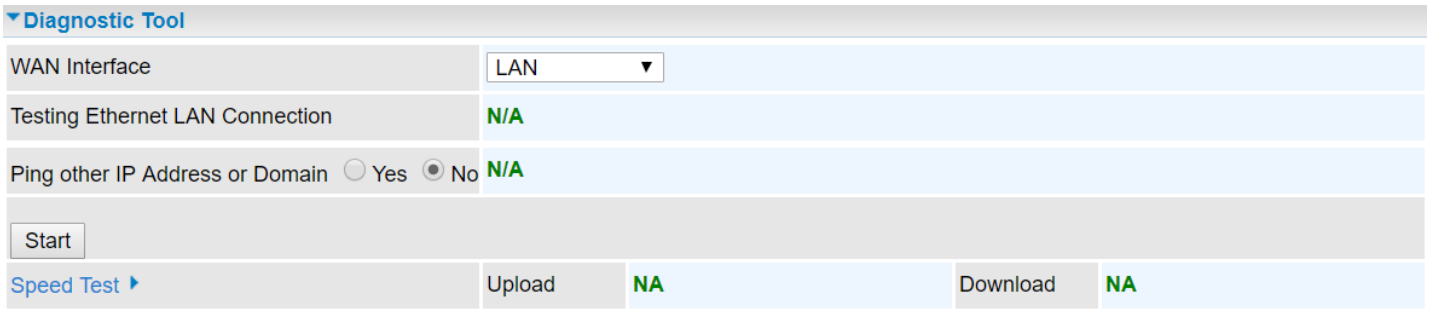
IP Address or Domain: Set the destination host (IP, domain name) to be traced.

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

Shown as we "trace" www.billion.com below.



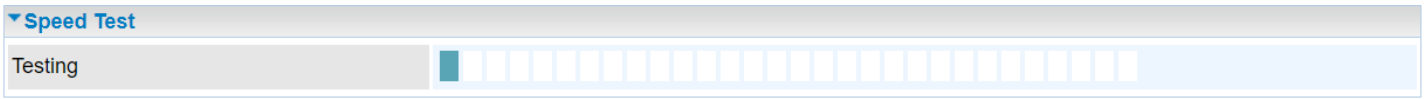
LAN



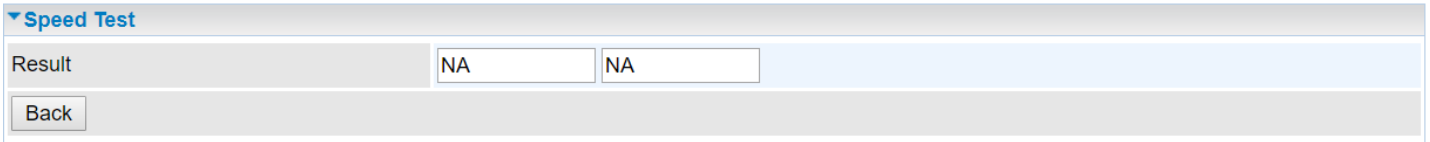
Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

Speed Time: Measure the current uplink and downlink speed rate.

- Take less than a minute to run the test.



- Result in Uplink / Downlink



Click **Back** to go back to the Diagnostic Tool

Click **START** to begin to diagnose the connection.

Chapter 5: Troubleshooting

If your 9900VA 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 or BEC 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 light, 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
1. The front LEDs display incorrectly upgrade **2. Still cannot access to the router management interface after pressing the RESET button.** **3. 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 Lights Red, keeping press reset button over 6 seconds. 3. Internet LED flashes Green, 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 cycle off/on the 9900VA

APPENDIX: PRODUCT SUPPORT & CONTACT

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

Contact BEC @ http://www.bectechnologies.net

FCC Statement

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

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

FCC Caution:

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.