User Manual

AirConnect® 8355P 5G CPE

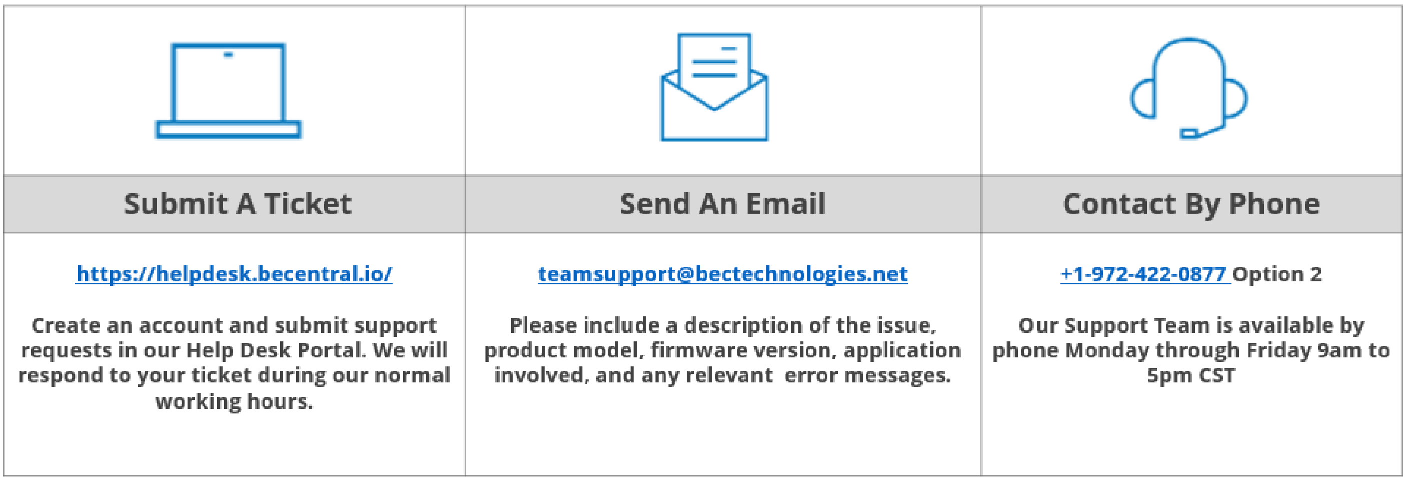
Last revised: April 2024

Version release: v1.34

Copyright Notice

Support Contact Information

If you come across any problems, please get in touch with the dealer from where you have purchased the product or contact BEC directly via the following methods:



Submit A Ticket	Send An Email	Contact By Phone
https://helpdesk.becentral.io/ Create an account and submit support requests in our Help Desk Portal. We will respond to your ticket during our normal working hours.	teamsupport@bectechnologies.net Please include a description of the issue, product model, firmware version, application involved, and any relevant error messages.	+1-972-422-0877 Option 2 Our Support Team is available by phone Monday through Friday 9am to 5pm CST

Last revised: April 2024
Version release: v1.34

TABLE OF CONTENTS

Chapter 1: Introduction

Introduction to your Router

Congratulations on your purchase of the **AirConnect® 8355P 5G CPE.**

The BEC AirConnect® 8355P 5G CPE boasts a versatile design suitable for indoor and outdoor installation, ensuring optimal signal reception regardless of placement. The 8355P 5G CPE offers exceptional performance with an industry-leading MIMO antenna design architecture, providing reliable capacity and extensive coverage.

Equipped with a robust multi-core CPU and sub-6 GHz carrier aggregation up to 4CA DL and 2CA UL, the 8355P delivers ultra-high data rates and lower latency. Additionally, it features 802.11ax Wi-Fi 6 Technology for faster speeds, greater capacity, and reduced network congestion, offering a transformative Wi-Fi experience.

Redefining Fixed Wireless Access

The AirConnect® 8335P supports 5G Sub-6 GHz and 4G/LTE with dual connectivity modes, standalone access (SA) fully bene-ting from all the 5G capabilities and non-standalone access (NSA) attached to a 4G network up to a gigabit speed to ensure a quick and flexible deployment to any 5G NR or LTE network.

Subscriber Self-Installable

Many subscribers prefer the convenience and Flexibility of self-installation over waiting for a technician to come, and operators' benefit from reduced operational costs and faster deployments. Our mobile app makes the setup of the 8355P 5G CPE simple and straightforward. Customers are guided through where best to position the 8355P 5G CPE, activation and connecting to the network.

Advanced MIMO Antenna Technology

Operators need antenna technology to meet capacity and throughput demands in challenging deployment scenarios such as Fixed Wireless Access (FWA). The high-gain embedded 4X4 MIMO directional antenna ensures increased capacity, maximum bandwidth, and extended coverage.

BECentral® CloudEdge Services

BECentral® CloudEdge is an Industry-leading cloud-based service platform designed to accelerate LTE and 5G Wireless WAN connectivity for deployments of any scale. The platform enables zero-touch provisioning and provides visual dashboards with real-time analytics, detailed reporting, historical analysis, performance monitoring, proactive alerts/notifications, and API extensibility for 3rd party integration

Features & Specifications

5G sub-6 GHz SA, 3GPP Release 16 Compliant

- Supports Frequency Range 1 Bands (SA): n2
- Carrier Aggregation: sub-6 GHz (FDD+FDD, 4CA)
- Channel Bandwidth: Up to 300 MHz
- Modulation: 256QAM DL / 256QAM UL

BEC SX High-Gain MIMO Antenna

- 4×4 MIMO DL / 2×2 MIMO UL
- 2T4R Antenna Chain
- Omni-Directional (617-2700MHz) - Maximum Peak Gain: 5 dBi
- Directional (3300-4200MHz) - Maximum Peak Gain: 10 dBi

Wi-Fi 6 (802.11ax)

- IEEE 802.11ax/ac/n/a 5 GHz
- IEEE 802.11ax/n/b/g 2.4 GHz
- Maximum PHY-Data Transmission Rates:
  5 GHz: 1201 Mbps (802.11ax)
  2.4 GHz: 574 Mbps (802.11ax)

Operational Modes

- Router or Bridge

Network Protocols and Features

- IPv4, IPv6 or IPv4 / IPv6 Dual Stack
- Pv6 in IPv4 (6RD) / IPv4 in IPv6 (DS-Lite) / IPv6-464XLAT
- NAT, static (v4/v6) routing and RIP-1 / 2
- DHCPv4 / v6
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS proxy
- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy

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

Quality of Service Control

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

Secured VPN

- IPSec VPN Tunneling (up to 8 tunnels)
- PPTP VPN Tunneling (up to 4 dial-in/dial-out tunnels)
- L2TP over IPSec VPN Tunneling (up to 4 dial-in / dial-out tunnel)
- GRE (up to 8 tunnels)
- Embedded PPTP / L2TP / IPSec Client and Server
- IKE Key Management
- MPPE Encryption for PPTP
- IPsec DES, 3DES, and AES encryption
- OpenVPN: 1 server for up to 4 clients

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 v1, v2, v3, MIB-I and MIB-II
- TR-069 supports remote management.
- BECentral® CloudEdge Remote Management
- Syslog monitoring

Dynamic Routing

- BGP and OSPF

Hardware Specifications

Physical interface

- 2.5 Gigabit Ethernet IEEE 802.3bt compliant PD interface
- Physical SIM Card Slot (2FF Size)
- Reset Button port configurable LAN/WAN
- LED indicators (Power, Internet, Signal Strength, Ethernet)

Physical Specifications

- Dimensions: 8.5" (D) x 1.5" (H) (215mm x 38 mm)
- Weight: 1.1 lbs.(460g)

Power Requirement

- Power over Ethernet (IEE 802.3bt compliant)

Operating Temperature

- Operating temperature: -40° to 140°F (-40° to 60°C)
- Humidity: 20 ~ 95% non-condensing

IP Rating

- IP65

CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

✓ 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.

✓ Use the supplied Poe (Power-over-Ethernet) injector for indoor only or with any IEEE 803bt capable PoE injector to connect with the AirConnect® 8355P 5G CPE.

What's in the Box

✓ AirConnect® 8355P 5G CPE x 1

✓ Quick Installation Guide x 1

✓ 8355P Desktop Stand x 1

✓ 8355P Mount Plate x 1

✓ Stainless Hose Clamp x 2

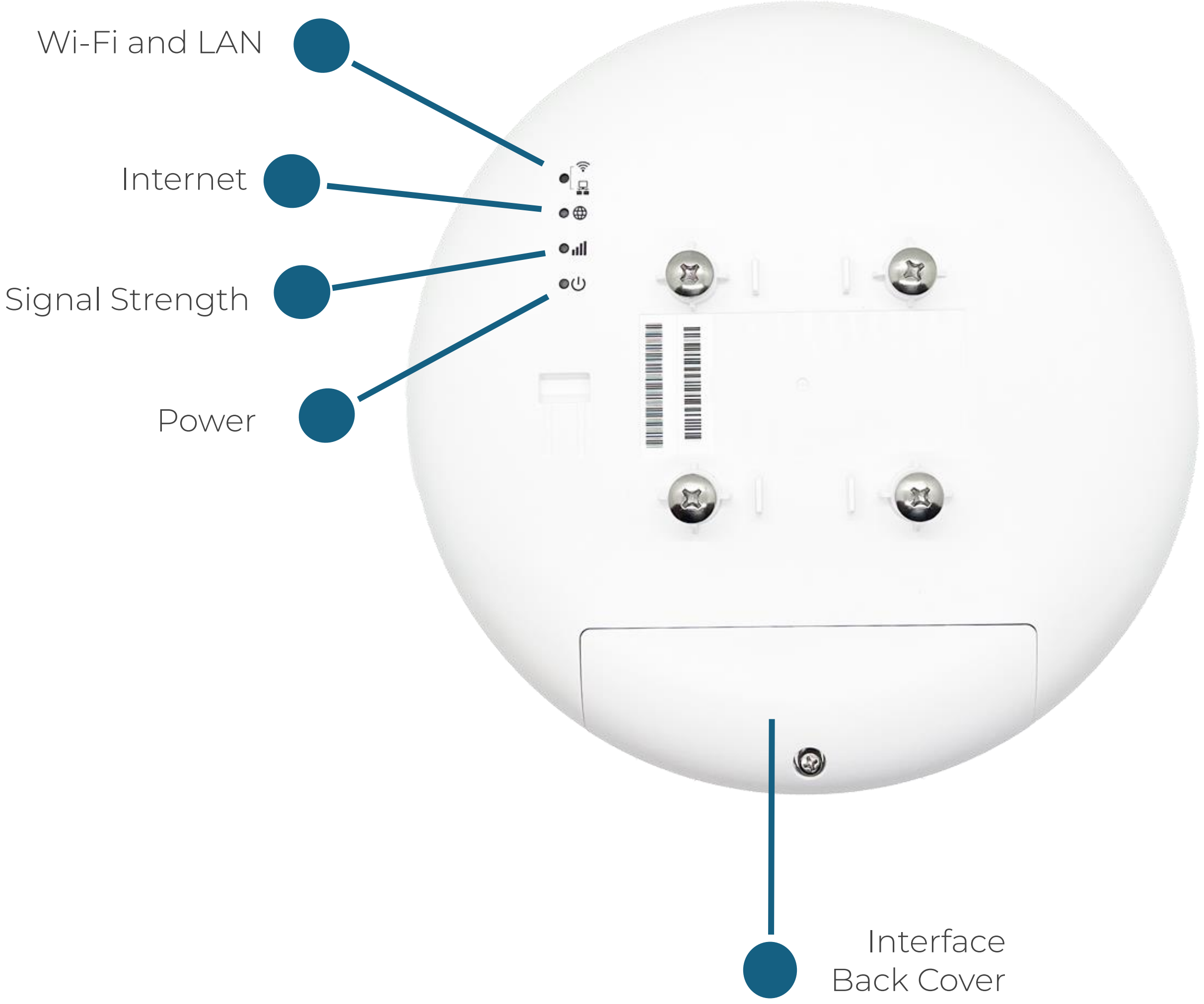
✓ Screw Set (SUS304 x 4 and Platis Nylon x 4)

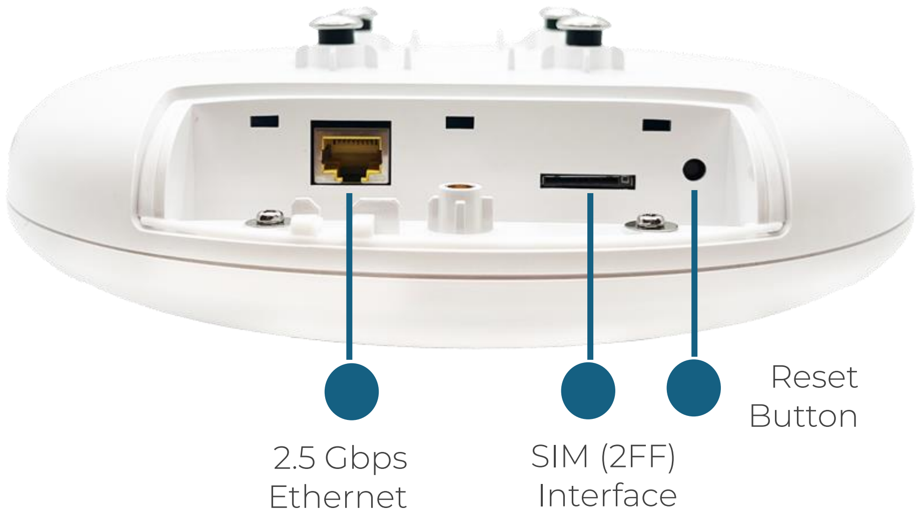
✓ Flat Ethernet (RJ-45) Cable x 1

✓ 2.5 Gigabit Poe Injector x 1

Device Description

Hardware Interfaces





LED Indicators

LED	STATUS	DESCRIPTION
Power ⏻	Green	System is up and ready
	Red	Boot failure
Wi-Fi and LAN	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
5G 📶 **(Received Signal Strength Indicator)**	Green	RSSI greater than -69 dBm. Excellent signal condition
	Green Flashing Quickly	RSSI from -81 to -69 dBm. Good signal condition
	Orange Flashing Quickly	RSSI from -99 to -81 dBm. Fair signal condition
	Orange Flashing Slowly	RSSI less than -99 dBm. Poor signal condition
	Orange	No signal and the 5G module is in service
	Off	No 5G module or 5G module fails
Internet 🌐	Green	WAN IP is received, and traffic is passing thru the device
	Red	Cannot get a WAN/public IP address
	Off	The device is either in bridged mode or WAN connection not ready.

System Recovery Procedures

The purpose is to allow users to restore the AirConnect® 8355P 5G CPE 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 AirConnect® 8355P 5G CPE

2.1 Power off your AirConnect® 8355P 5G CPE

2.2 Power on the AirConnect® 8355P 5G CPE while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, and etc.).

2.3 When the POWER LED turns RED, keep holding and pushing the RESET button for more 6 seconds then release it. The INTERNET LED will flash in GREEN afterward.

Step 3 – Restore your 8355P 5G CPE

With INTERNET light flashes green, AirConnect® 8355P 5G CPE 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, 8355P 5G CPE 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 8355P 5G.

3.4 INTERNET LED turns green after the Firmware upgrade completed.

3.5 Power cycle on & off to regain access to your AirConnect® 8355P 5G CPE.

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 XP / 7 / 8 / 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.

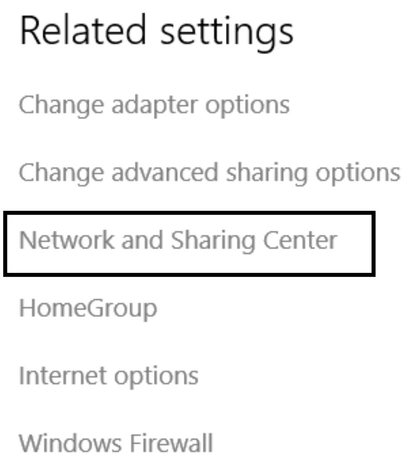
Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

NOTE!

Any TCP/IP capable workstation can be used to communicate with or through the AirConnect® **8355P 5G CPE.**To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

Configuring PC in Windows 10 (IPv4)



Related settings

Change adapter options

Change advanced sharing options

Network and Sharing Center

HomeGroup

Internet options

Windows Firewall

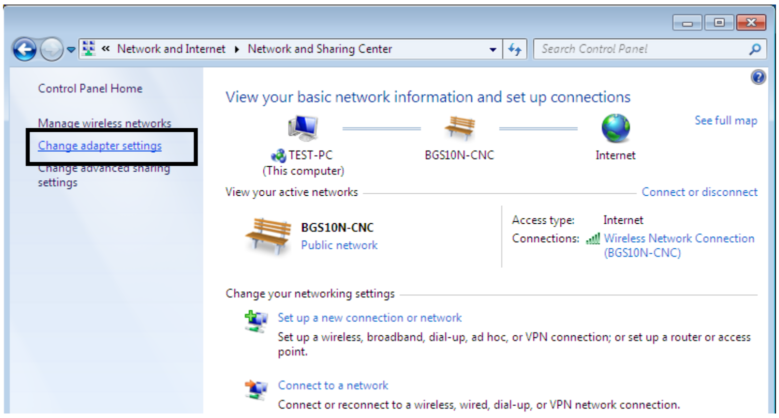
1. Click ⊞.

2. Click Settings

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.



View your basic network information and set up connections

View your active networks

BGS10N-CNC
Public network

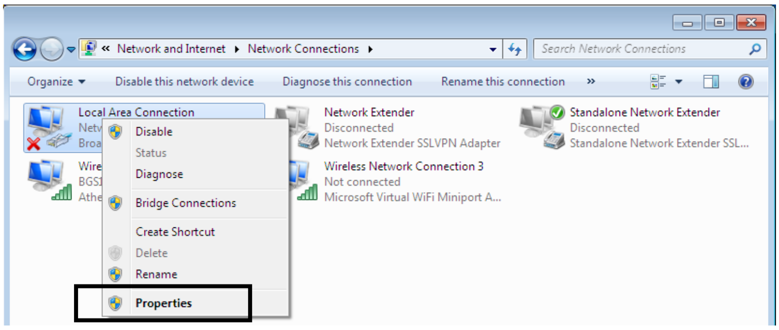
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

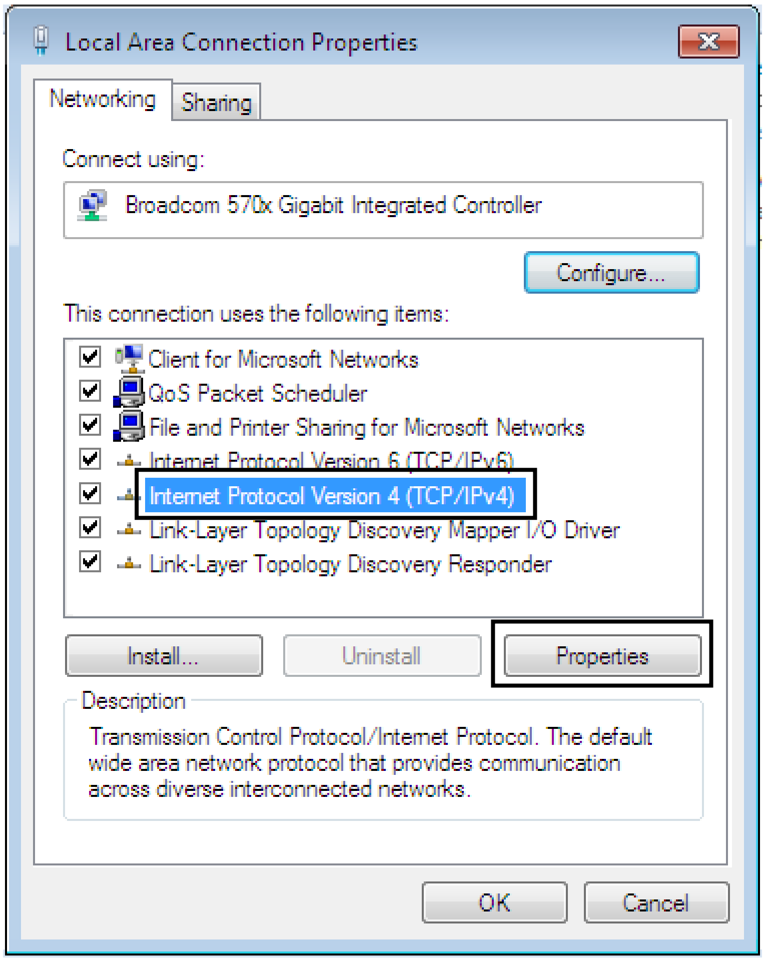
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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



« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
»
Local Area Connection
Netw
Broa
Wire
BGS1
Athe
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

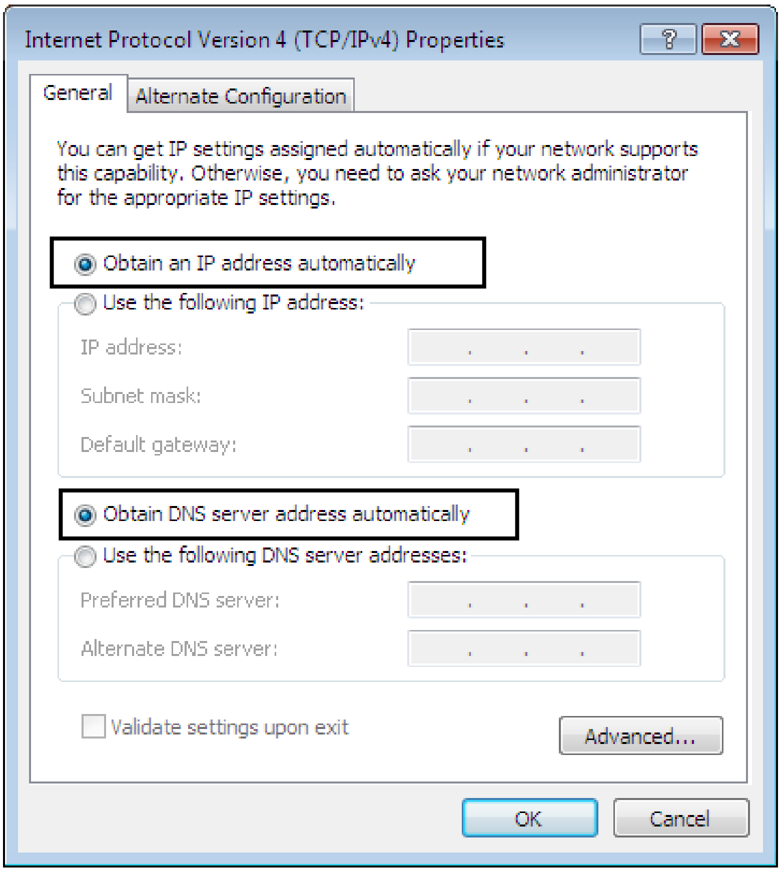
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

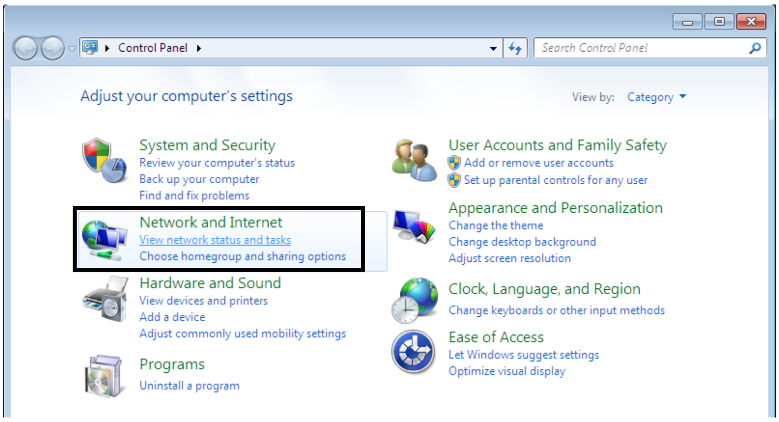
- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address: . . .
  - Subnet mask: . . .
  - Default gateway: . . .
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .

☐ Validate settings upon exit

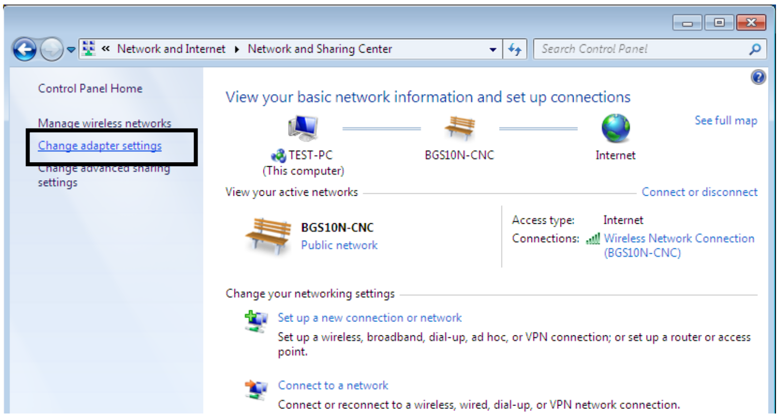
Configuring PC in Windows 7/8 (IPv4)

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

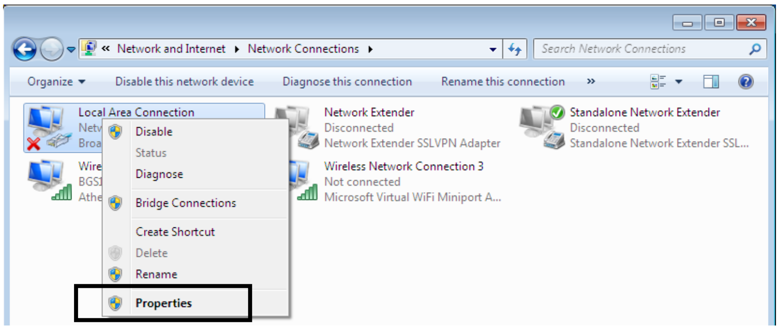
2. Then click on **Network and Internet**.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

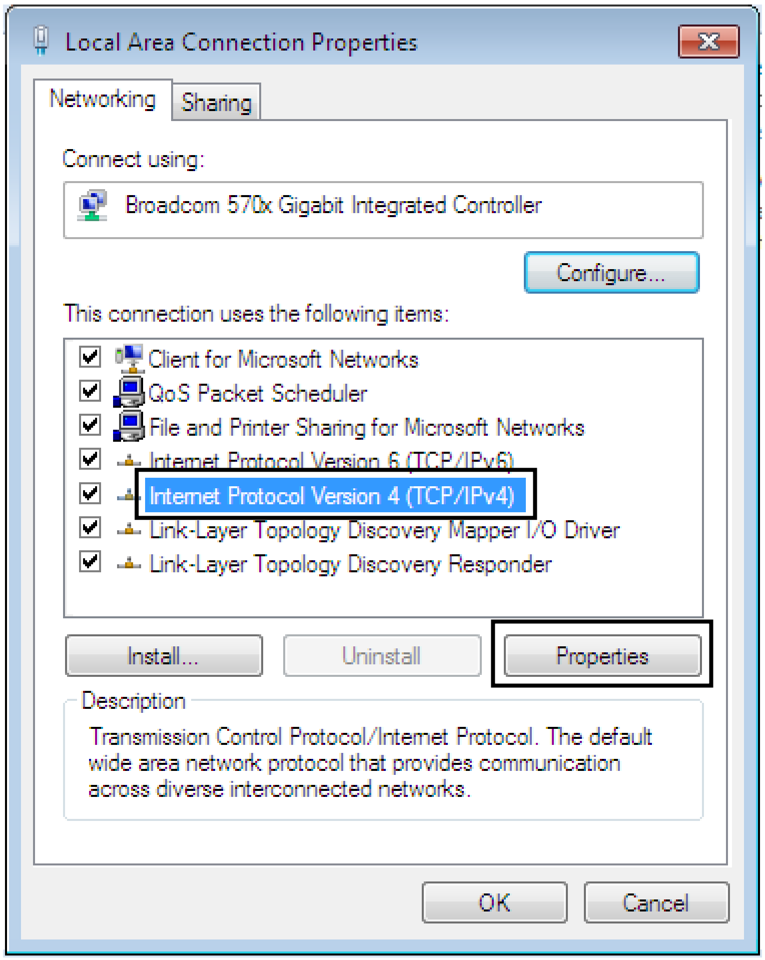
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet
Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

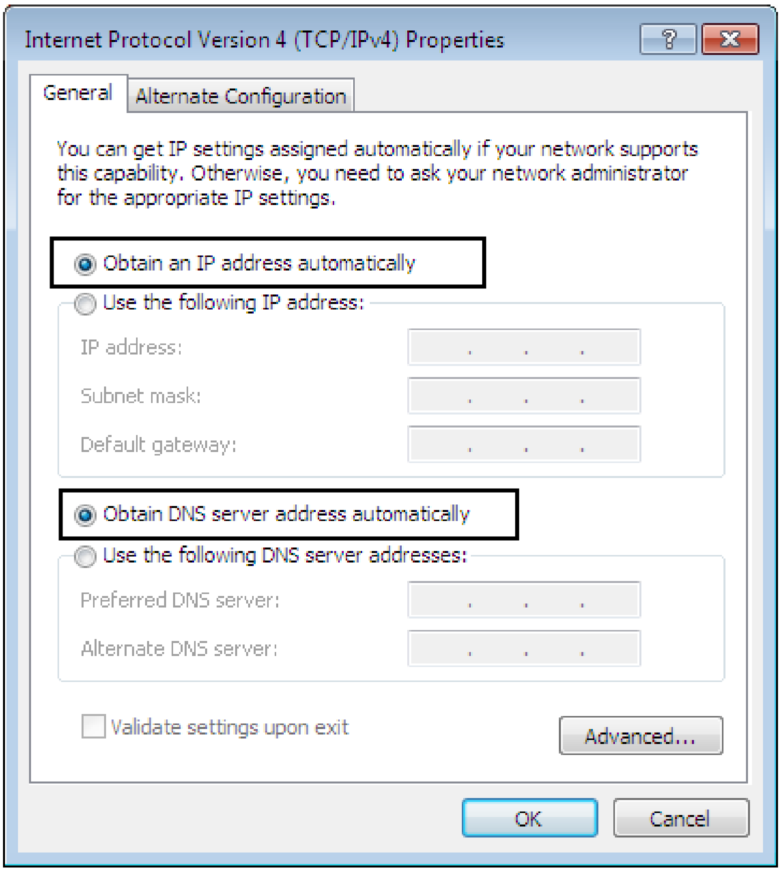
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

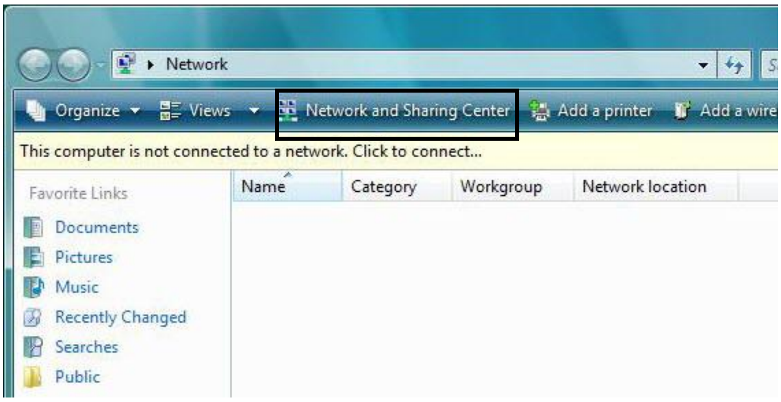
Advanced...

OK | Cancel

Configuring PC in Windows Vista (IPv4)

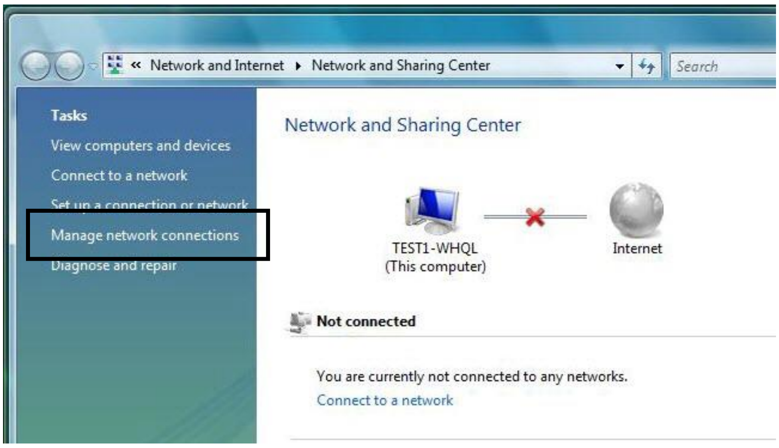
1. Go to **Start**. Click on **Network**.

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



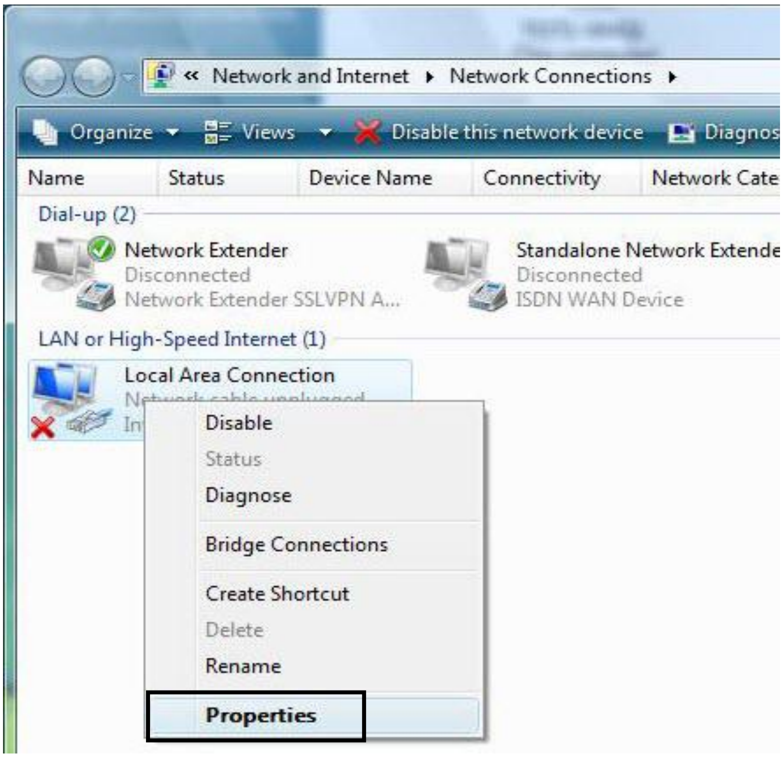
This computer is not connected to a network. Click to connect...

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

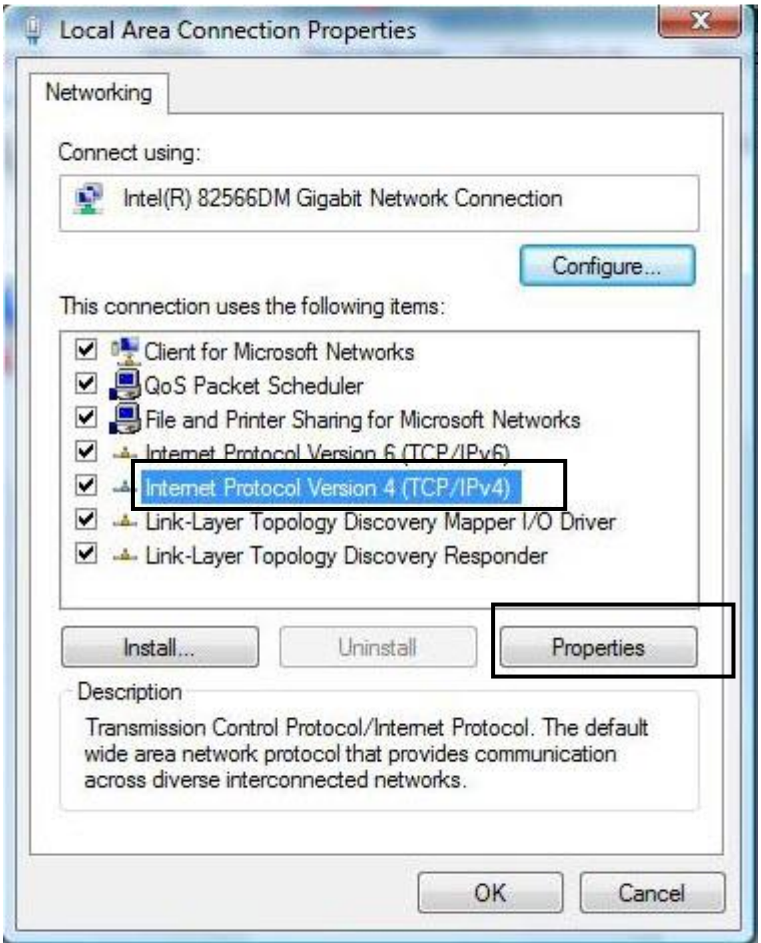


You are currently not connected to any networks.

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**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DM Gigabit Network Connection

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

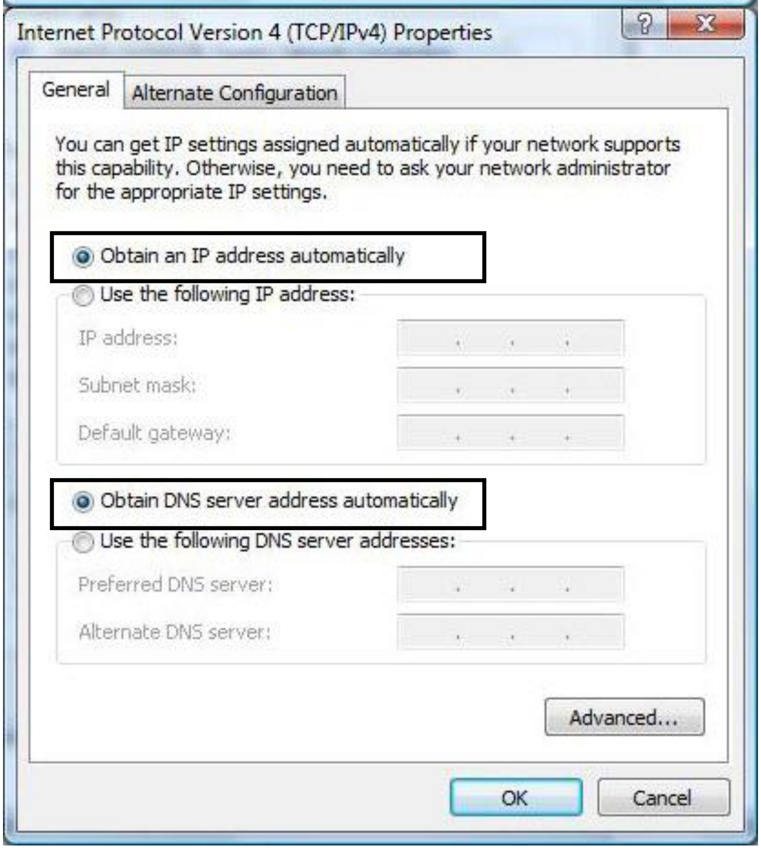
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Advanced...

OK Cancel

Network Configuration – IPv6

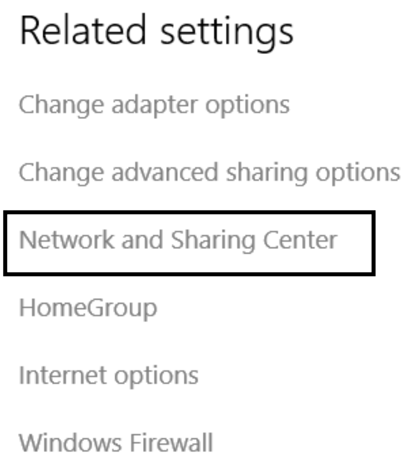
Configuring PC in Windows 10 (IPv6)

1. Click ⊞.

2. Click ⚙ Settings

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

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



Related settings

Change adapter options

Change advanced sharing options

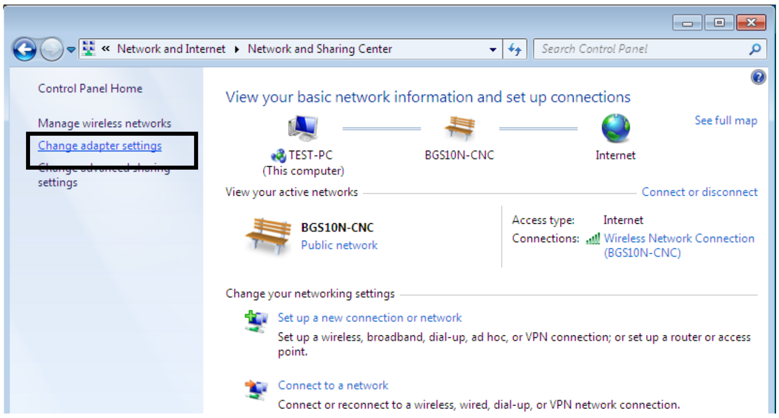
Network and Sharing Center

HomeGroup

Internet options

Windows Firewall

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



View your basic network information and set up connections

View your active networks

Access type: Internet

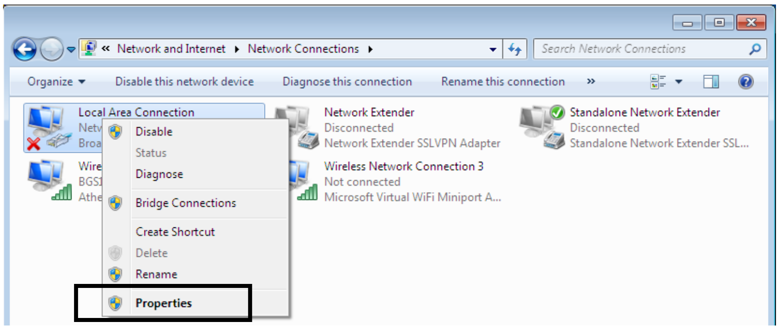
Connections: Wireless Network Connection (BGS10N-CNC)

Change your networking settings

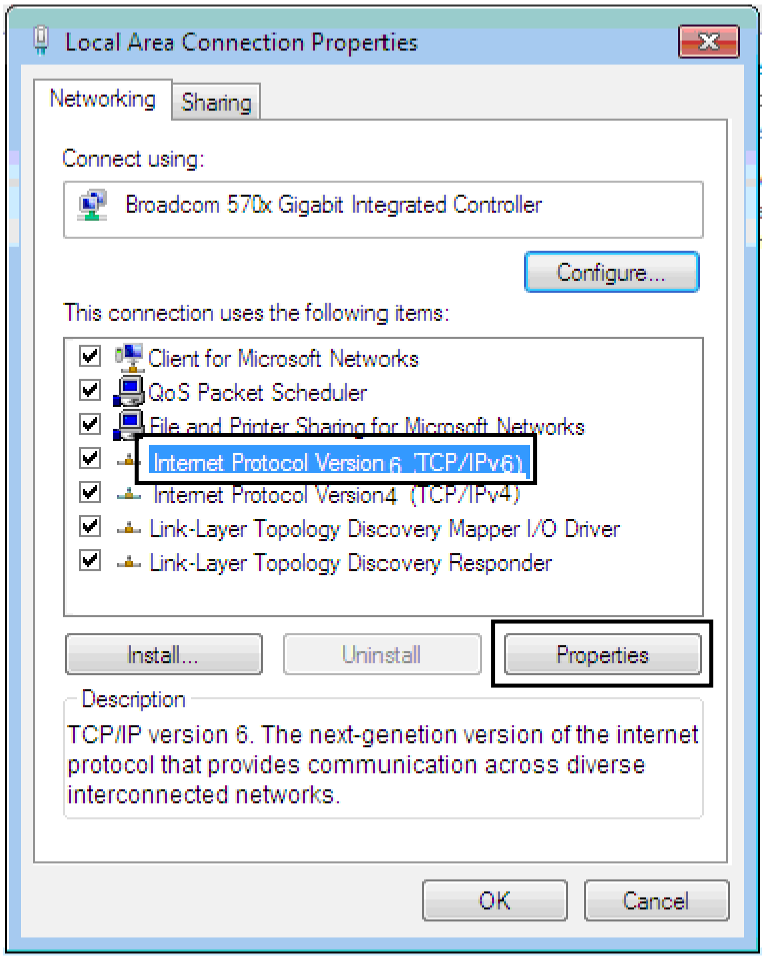
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
»
Local Area Connection
Netw
Broa
Wire
BGS1
Athe
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

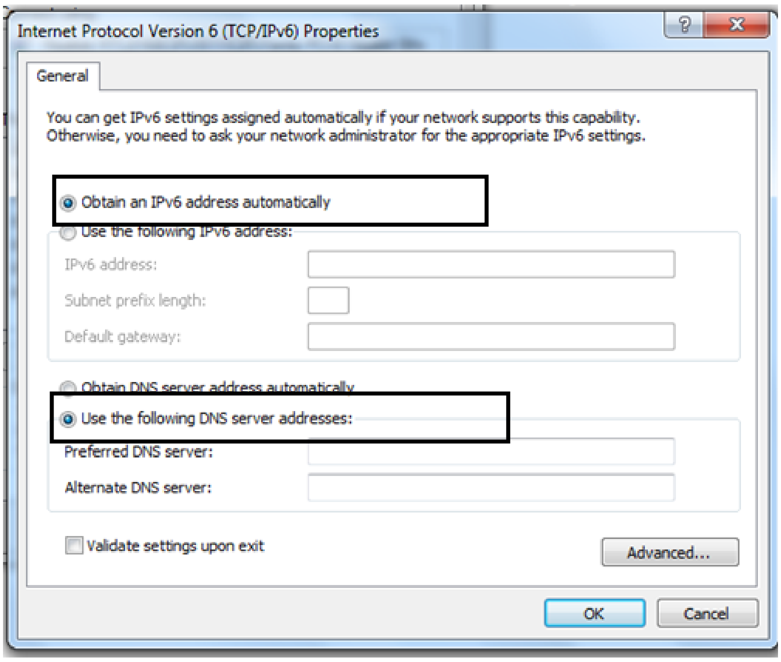
Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

OK | Cancel

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.



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

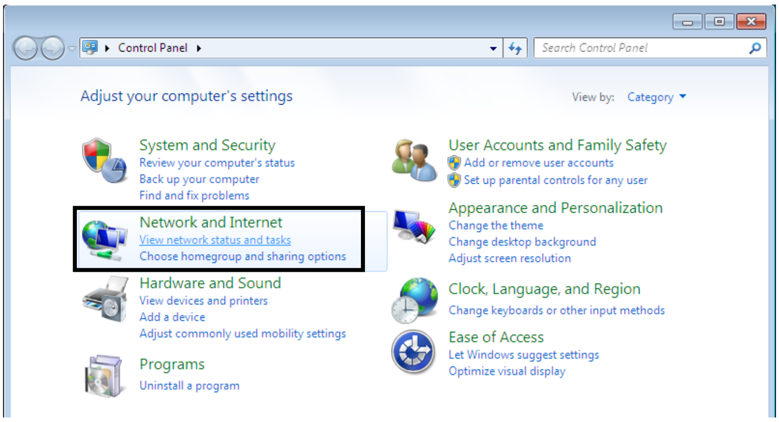
Advanced...

OK | Cancel

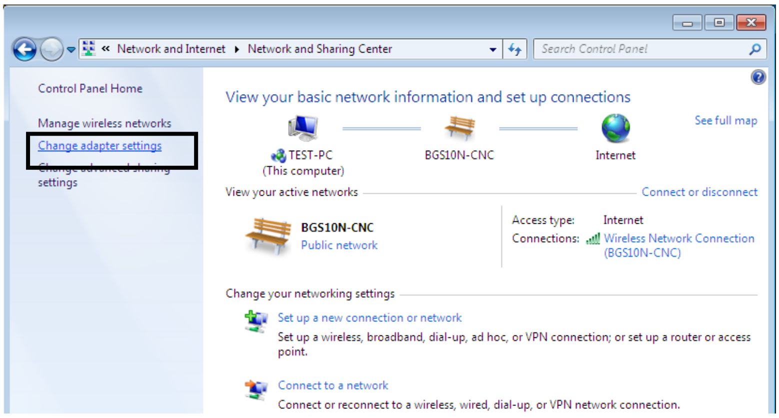
Configuring PC in Windows 7/8 (IPv6)

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

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


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

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



View your basic network information and set up connections

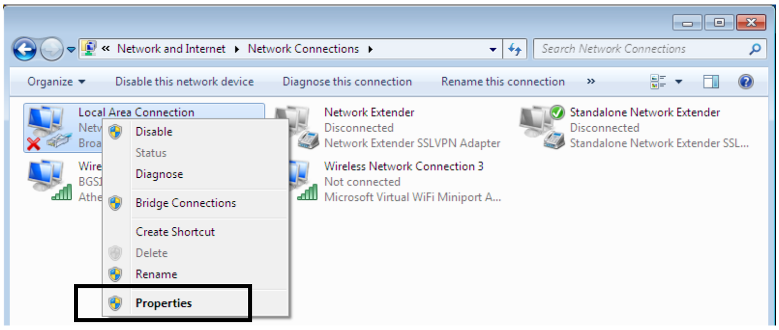
View your active networks

Change your networking settings

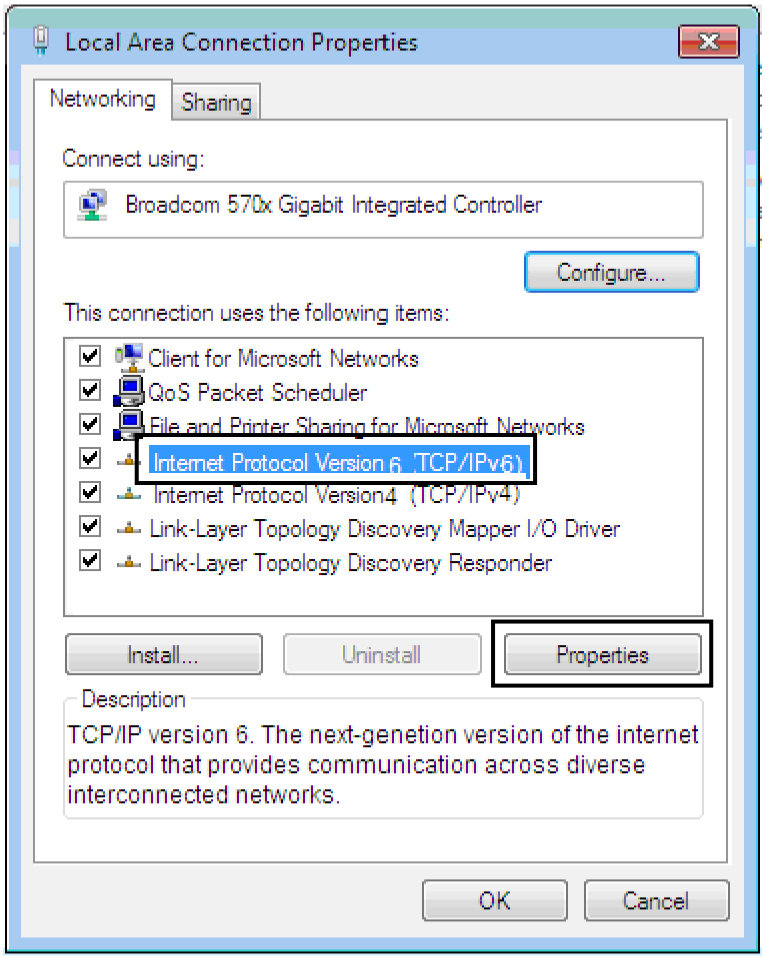
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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**.



Local Area Connection Properties

Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

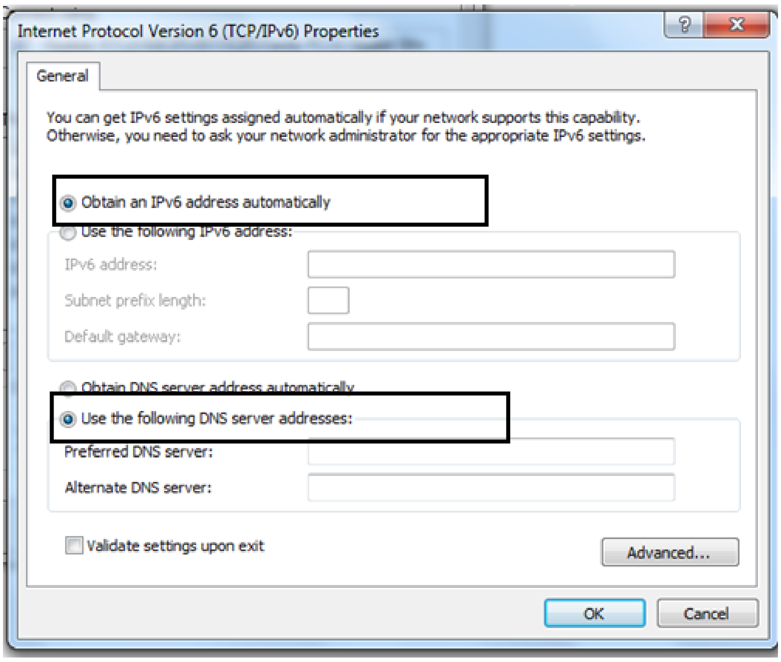
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 6 (TCP/IPv6) Properties

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:

IPv6 address:
Subnet prefix length:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

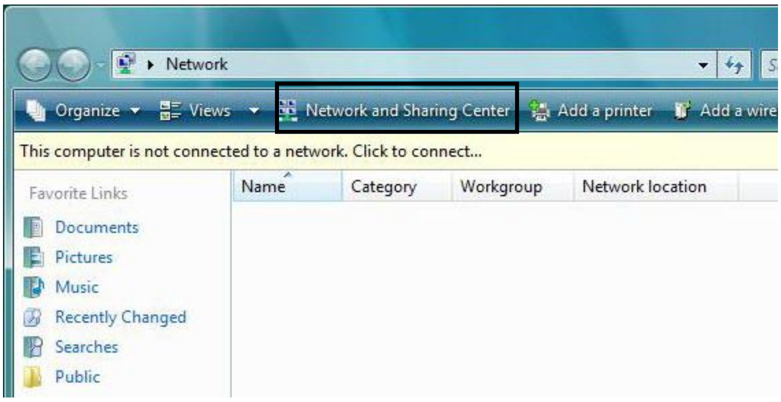
Preferred DNS server:
Alternate DNS server:

□ Validate settings upon exit

Configuring PC in Windows Vista (IPv6)

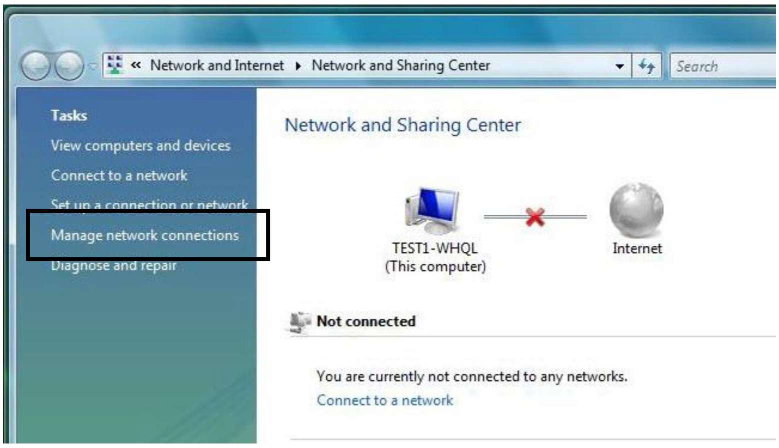
1. Go to **Start**. Click on **Network**.

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



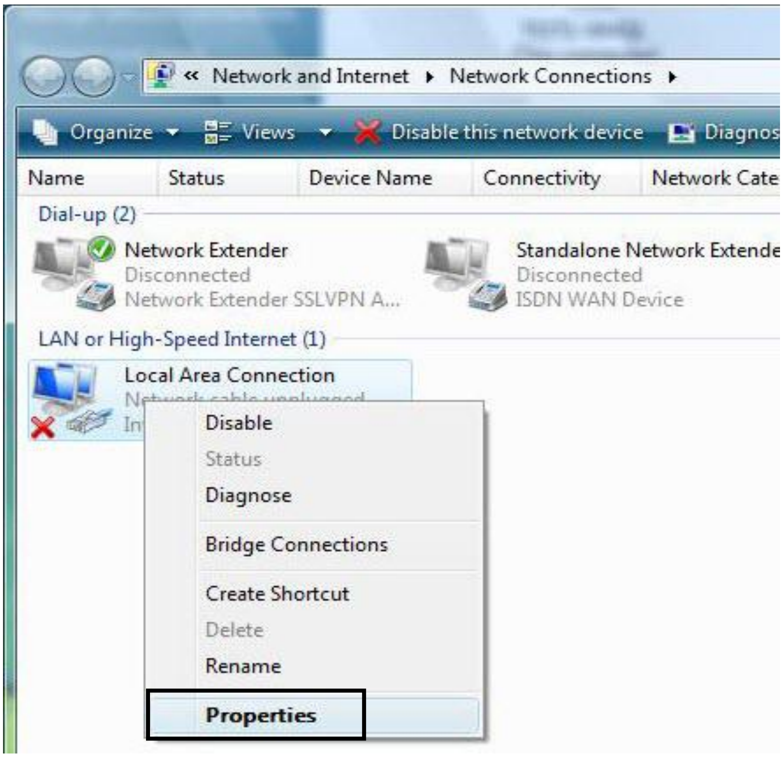
This computer is not connected to a network. Click to connect...

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

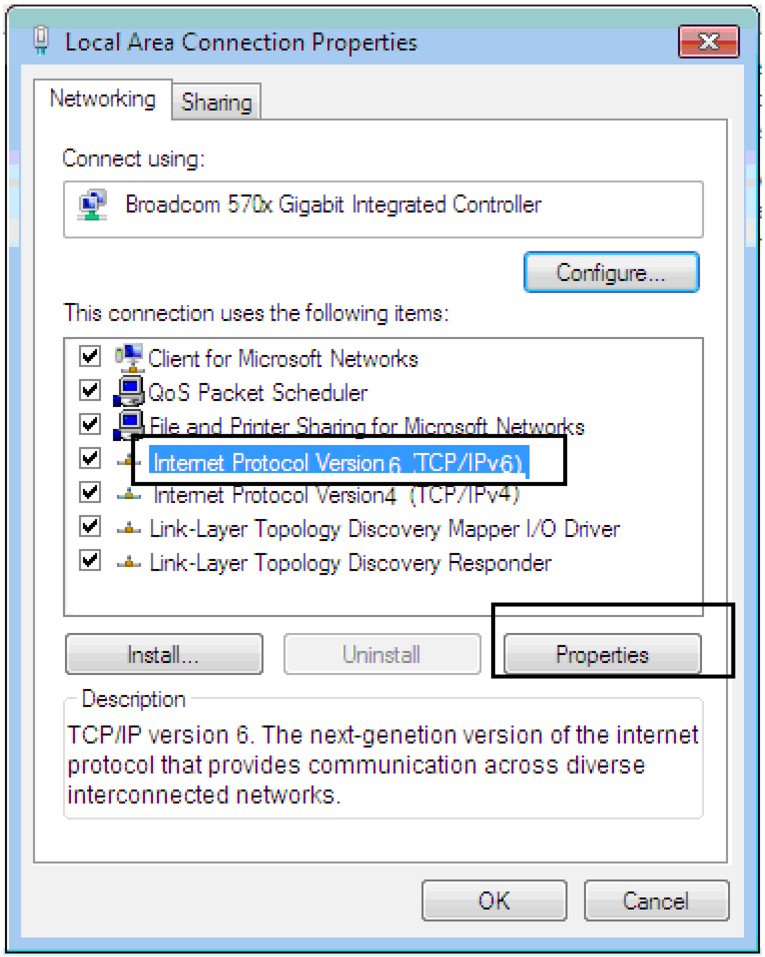


You are currently not connected to any networks.

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**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

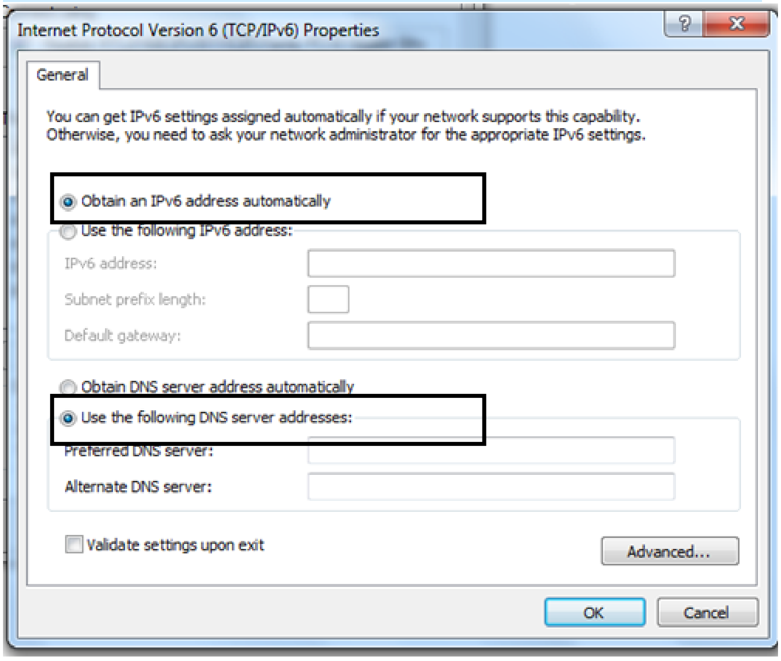
Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

OK | Cancel

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.



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK | Cancel

Default Settings

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

Web Interface: (Username and Password)

- ✔ Username: admin
- ✔ Password: admin **or** a unique 12-digit password can be found on the device label.

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 provided such as **EWAN** ((Dynamic IP address, Static IP address, PPPoE, 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

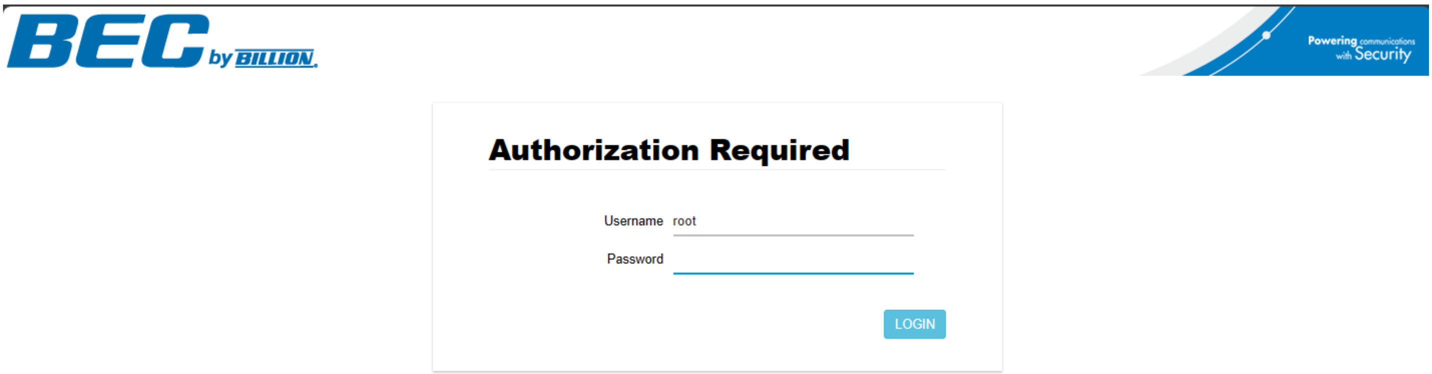
CHAPTER 4: DEVICE CONFIGURATION

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.

Default username is **“root”** and the password is **a unique 12-digit can be found on the device label** for **Administrator** account**.**

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



Authorization Required

Username root

Password

Congratulations! You have successfully logged on to your AirConnect® 8355P 5G.

Once you have logged on to your AirConnect® 8355P 5G CPE 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		Configuration
Sub-Items	**Overview** - System - Memory - WAN - LAN **Firewall Status** - IPv4 Firewall - IPv6 Firewall - Table: Filter - Chain: Forward - Chain: Output - Table: NAT - Hide Empty Chains - Show Raw Counters - Reset Counters - Restart Firewall **Routes** - ARP - Active IPv4 Routes - IPv6 Neighbors - Active IPv6 Routes **VPN** - PPTP Servers - L2TP Servers - OpenVPN Server **System Log** **Realtime Status** - Load - Traffic - Connections		**System** - System - Administration - Backup / Flash Firmware - Reboot **Modem** - Connection Profile - Miscellaneous - 5G NR Status - Neighbor Cell - Debug Manager **Network** - Interfaces - Wireless 2.4G - Wireless 5G - DHCP and DNS - Hostnames - Static Routes - Speedtest - Firewall - Diagnostics - TR-069 - BECentral Management **VPN** - VPN Account - PPTP Server - PPTP Client - L2TP Server - L2TP Client - IPSec - OpenVPN Server - OpenVPN Client - **GRE**

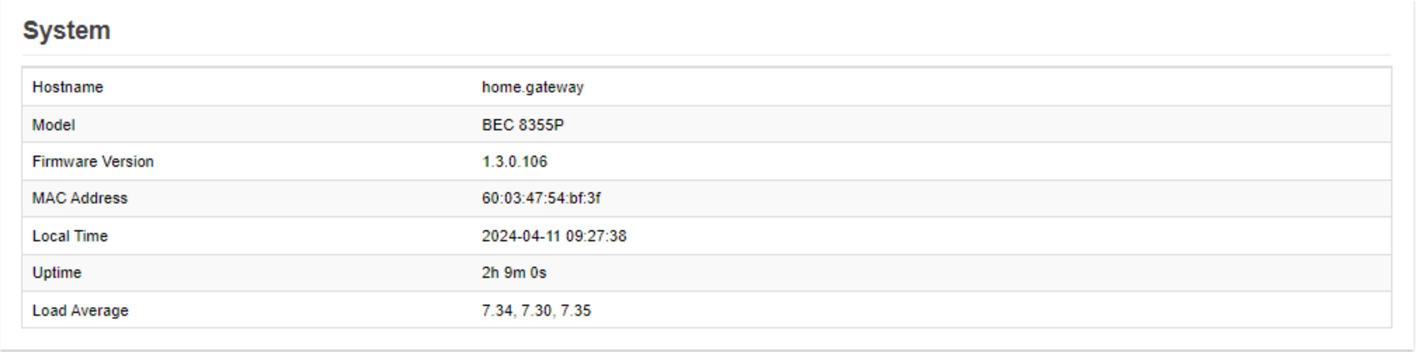
Refer to the relevant sections of this manual for detailed instructions on how to configure your device.

Status

In this section, you can check the router's working status, including Overview, Firewall Status, Routes, VPN, System Log, and Realtime Status.

Overview

The Overview Status summarizes various systems and network-related information about the router. It gives users a quick snapshot of the router's current state and configuration. It gives users a convenient way to monitor the key parameters and functionality of their 8355P 5G CPE at a glance.



System

Hostname	home.gateway
Model	BEC 8355P
Firmware Version	1.3.0.106
MAC Address	60:03:47:54:bf:3f
Local Time	2024-04-11 09:27:38
Uptime	2h 9m 0s
Load Average	7.34, 7.30, 7.35

System Information

Hostname: Displays the device hostname for use on local network instead of ip address

Model: Display the device model.

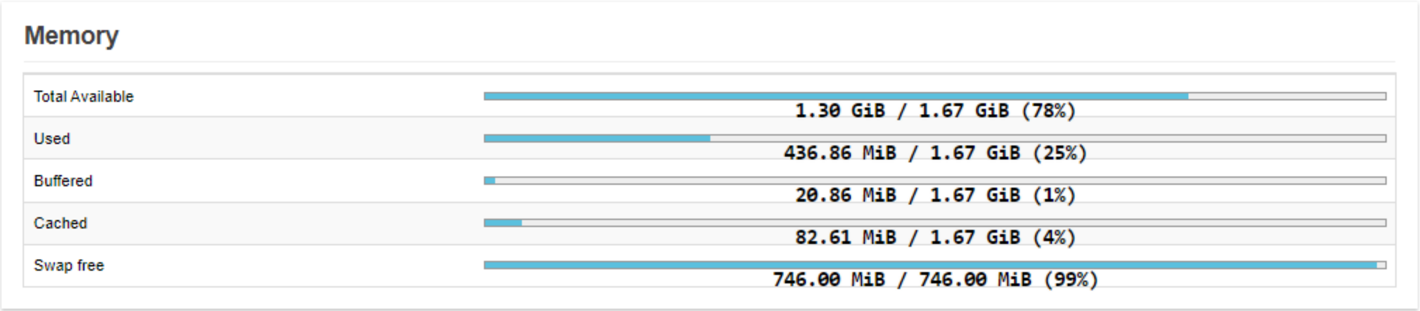
Firmware Version: Displays the device firmware version.

MAC Address: Displays the unique device MAC address.

Local Time: Displays the local time and date.

Uptime: Displays the amount of time the device has been up and operational.

Load Average: Display the average system load over a period of time.



Memory

Total Available	1.30 GiB / 1.67 GiB (78%)
Used	436.86 MiB / 1.67 GiB (25%)
Buffered	20.86 MiB / 1.67 GiB (1%)
Cached	82.61 MiB / 1.67 GiB (4%)
Swap free	746.00 MiB / 746.00 MiB (99%)

Memory Status

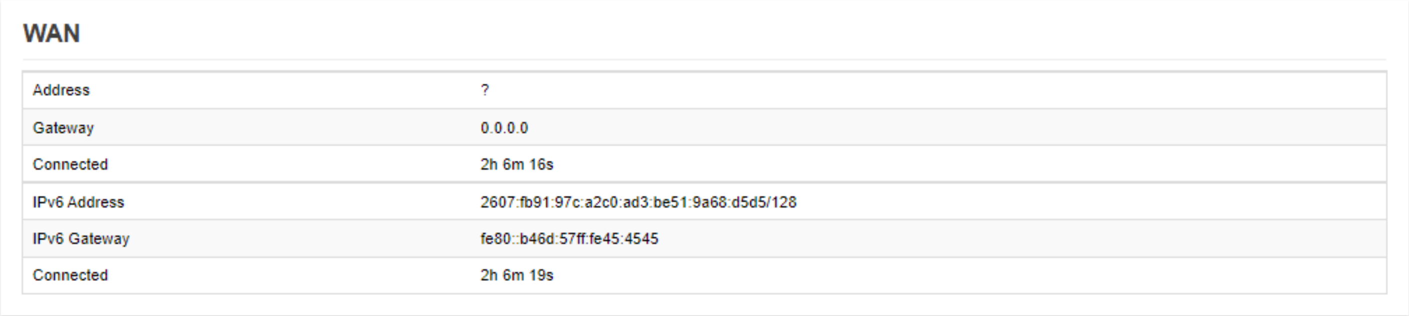
Total Available：Displays an estimate of RAM available to applications.

Used：Displays the amount of RAM used or unavailable.

Buffered：Displays the amount of RAM used for disk buffering.

Cached：Displays the amount of RAM used for filesystem caching

Swap Free：Display available connection interfaces supported in the 8355P 5G CPE.



WAN

Address	?
Gateway	0.0.0.0
Connected	2h 6m 16s
IPv6 Address	2607:fb91:97c:a2c0:ad3:be51:9a68:d5d5/128
IPv6 Gateway	fe80::b46d:57ff:fe45:4545
Connected	2h 6m 19s

WAN Interface

Address: Displays the current WAN IP address

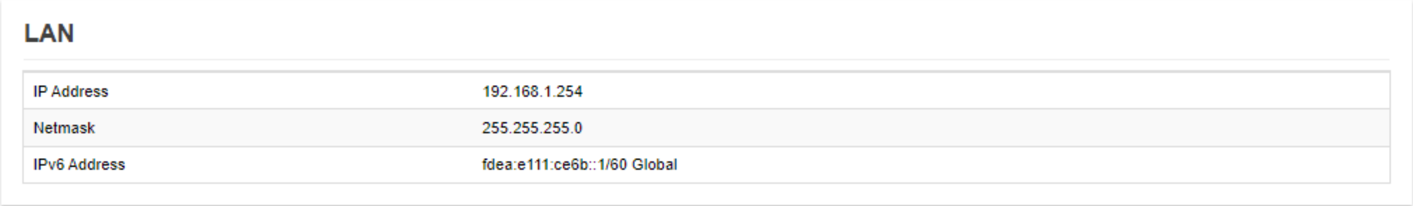
Gateway: Displays the IP address of the default gateway

Connected: Displays the current connected status in time

IPv6 Address: Displays the current IPv6 IP address

IPv4 Address: Displays the current IPv4 IP address

Connected: Displays the current connected status in time



LAN

IP Address	192.168.1.254
Netmask	255.255.255.0
IPv6 Address	fdea:e111:ce6b::1/60 Global

LAN Interface

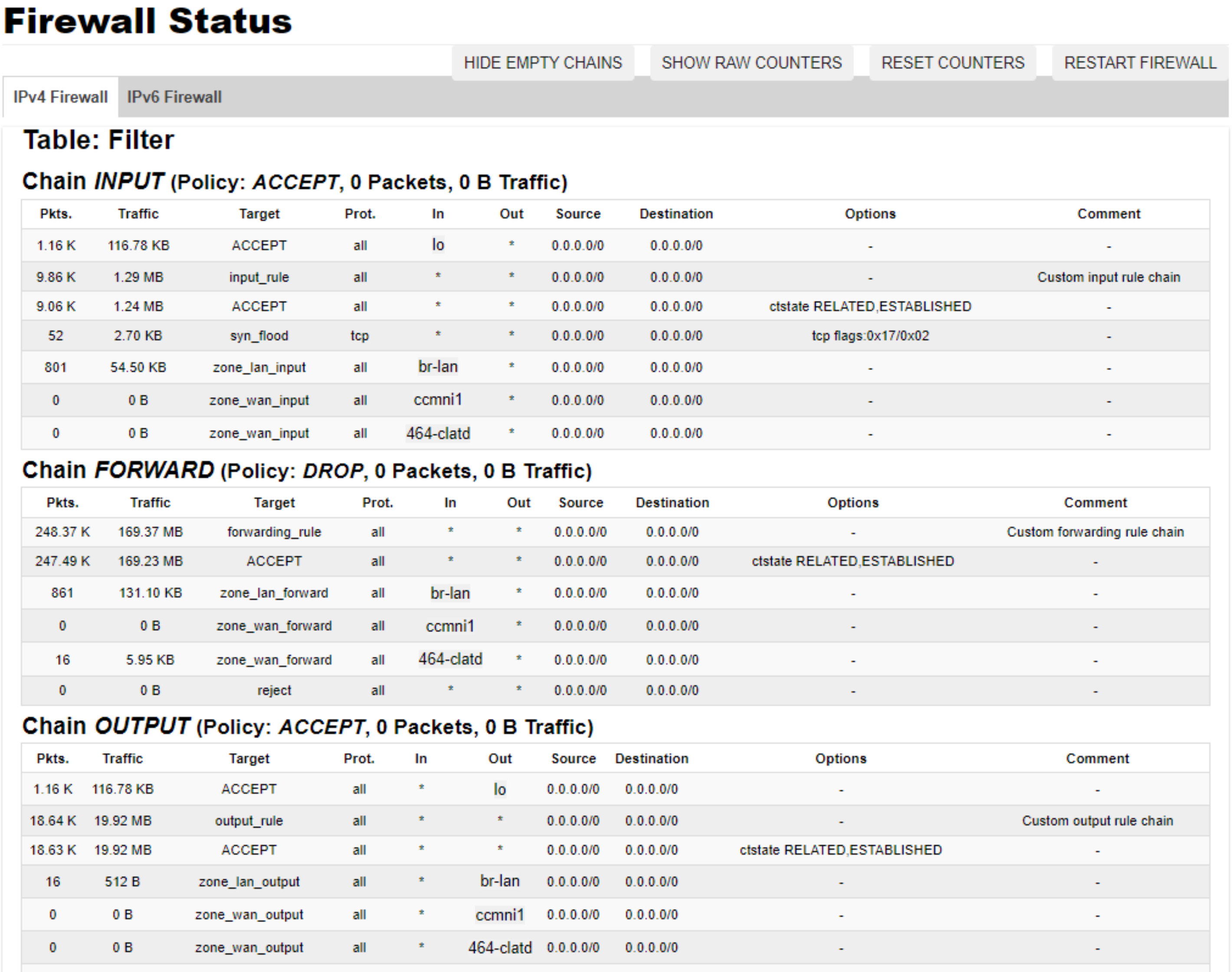
IP Address: Displays the IPv4 IP address of the LAN interface.

Netmask: Display the subnet mask of the LAN.

IPv6 Address: Display the IPv6 IP address of the LAN interface.

Firewall Status

The firewall status and chains refer to the current state and configuration of the firewall rules and chains that are applied to control network traffic on the router. A chain is a sequence of rules that are applied to packets as they traverse the firewall. The 8355P 5G CPE uses several predefined chains to control incoming and outgoing traffic, including input, output, forward, and NAT.



Firewall Status

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.16 K	116.78 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
9.86 K	1.29 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
9.06 K	1.24 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
52	2.70 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
801	54.50 KB	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	ccmni1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	464-clatd	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *FORWARD* (Policy: *DROP*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
248.37 K	169.37 MB	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
247.49 K	169.23 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
861	131.10 KB	zone_lan_forward	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_forward	all	ccmni1	*	0.0.0.0/0	0.0.0.0/0	-	-
16	5.95 KB	zone_wan_forward	all	464-clatd	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	reject	all	*	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *OUTPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1.16 K	116.78 KB	ACCEPT	all	*	lo	0.0.0.0/0	0.0.0.0/0	-	-
18.64 K	19.92 MB	output_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom output rule chain
18.63 K	19.92 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
16	512 B	zone_lan_output	all	*	br-lan	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_output	all	*	ccmni1	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_output	all	*	464-clatd	0.0.0.0/0	0.0.0.0/0	-	-

Here's an explanation of the key concepts related to the 8355P 5G CPE firewall status and chains:

Input Chain: This chain is applied to packets destined for the router. It controls traffic targeting router services SSH, DNS, DHCP, and web services.

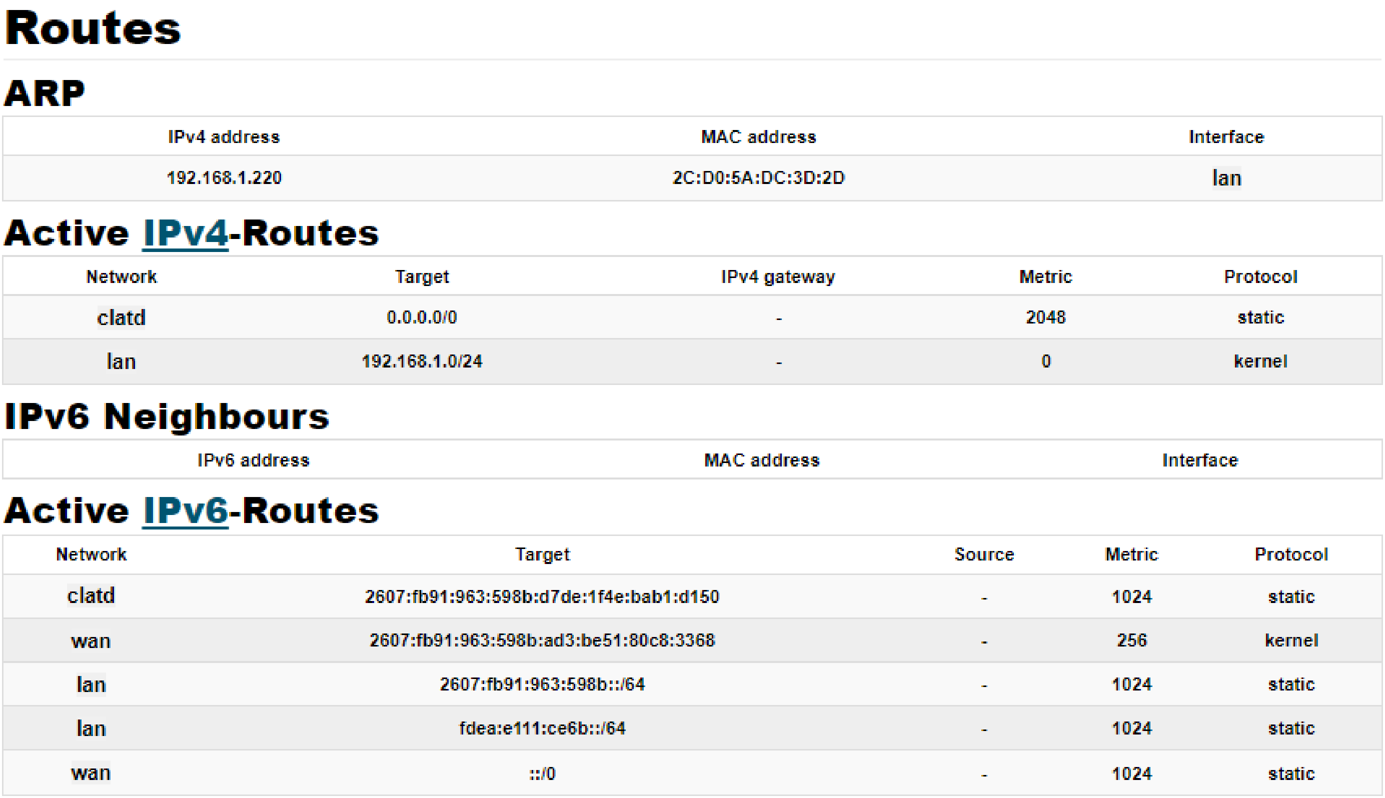
Output Chain: This chain is applied to packets originating from the router. It controls traffic router generated responses to incoming requests or locally generated traffic.

Forward Chain: This chain applies to packets being forwarded through the router. It controls traffic passing between network interfaces on the router, such as packets being routed between LAN and WAN interfaces.

NAT Chain: This chain is applied to packets as they are received by the router before any routing decisions are made. It can be used for advanced packet manipulation, such as destination NAT (DNAT) or port forwarding.

Routes

The Routes Status refers to the current state and configuration of the routing table, which contains information about how network traffic should be routed within the router and to external networks.



Routes

ARP

IPv4 address	MAC address	Interface
192.168.1.220	2C:D0:5A:DC:3D:2D	lan

Active IPv4-Routes

Network	Target	IPv4 gateway	Metric	Protocol
clatd	0.0.0.0/0	-	2048	static
lan	192.168.1.0/24	-	0	kernel

IPv6 Neighbours

IPv6 address	MAC address	Interface

Active IPv6-Routes

Network	Target	Source	Metric	Protocol
clatd	2607:fb91:963:598b:d7de:1f4e:bab1:d150	-	1024	static
wan	2607:fb91:963:598b:ad3:be51:80c8:3368	-	256	kernel
lan	2607:fb91:963:598b::/64	-	1024	static
lan	fdea:e111:ce6b::/64	-	1024	static
wan	::/0	-	1024	static

ARP: Address Resolution Protocol is used in IPv4 networks to map an IP address to a physical hardware address (such as an MAC address). The ARP table displays the list of IP address and MAC address pairs along with the associated interface.

Active IPv4-Routes: Displays the IPv4 routing table and active IPv4 routes across interfaces. It includes information such as the target IP, IP Gateway, metric, and protocol.

IPv6 Neighbor: The IPv6 neighbor table lists neighbors' IPv6 addresses on the same network and their corresponding MAC addresses along with the associated interface.

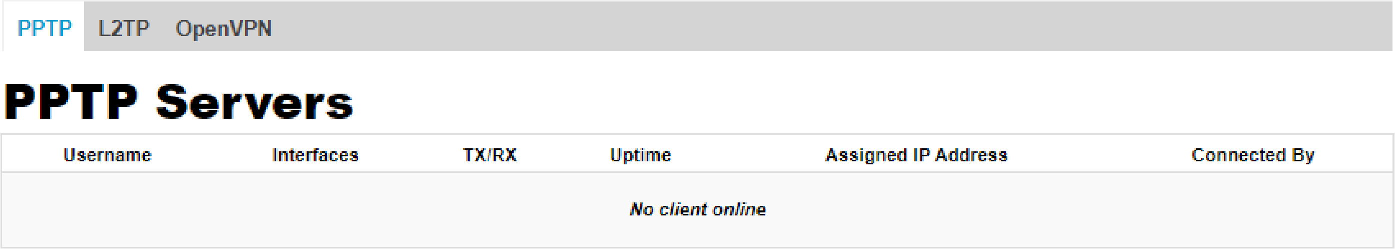
Active IPv6-Routes: Displays the IPv6 routing table and active IPv6 routes across interfaces. It includes information such as the target IP, source IP, metric, and protocol.

Table Definitions

Network: The network interface through which the traffic will be routed.
Target: The destination IPv6 address to which packets are being routed. IPv4 Gateway: This is the gateway's IP address where packets should be forwarded to reach the destination network.
Source: The IPv6 address of the originating device that sends the packet.
Metric: A value the routing algorithm uses to determine the best path to the destination network. It represents the route's cost, with lower metrics indicating preferred routes.
Protocol: Displays the protocol responsible for adding the route to the table.

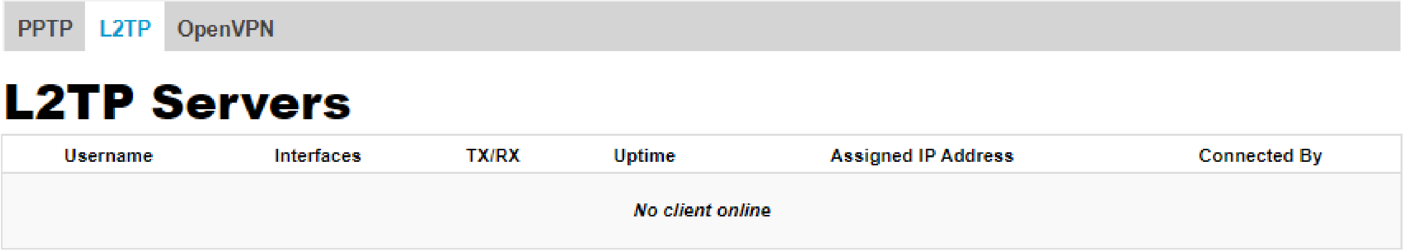
VPN

The VPN status provides information about the current state and configuration of VPN connections established on the 8355P 5G CPE. The specific information and status indicators can vary depending on the VPN protocol (e.g., PPTP, L2TP, OpenVPN) and the VPN client or server configuration.



PPTP Servers

Username	Interfaces	TX/RX	Uptime	Assigned IP Address	Connected By
No client online					

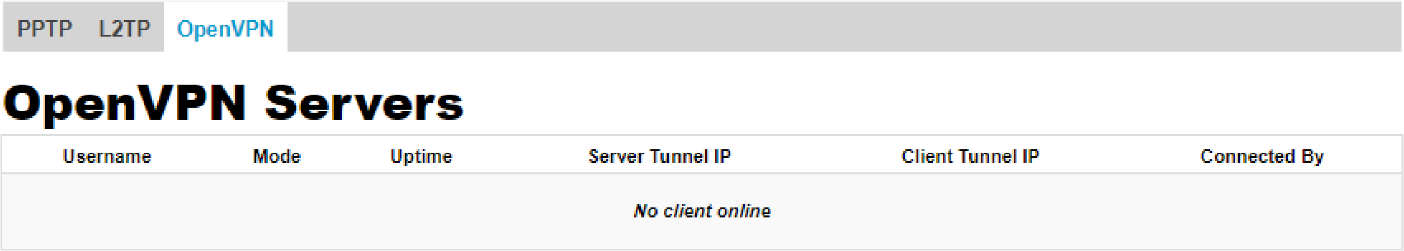


L2TP Servers

Username	Interfaces	TX/RX	Uptime	Assigned IP Address	Connected By
No client online					

PPTP and LT2P will include information such as:

Username: The username used for authentication will be displayed.
Interface: The network interface associated with the VPN connection.
TX/RX: The amount of data transmitted (TX) and received (RX) over the VPN connection.
Uptime: The duration of the VPN connection has been active since the last establishment.
Assigned IP: The IP address assigned to the router's VPN interface.
Connected By: Information (IP or Hostname) about the device or client connected to the VPN.



OpenVPN Servers

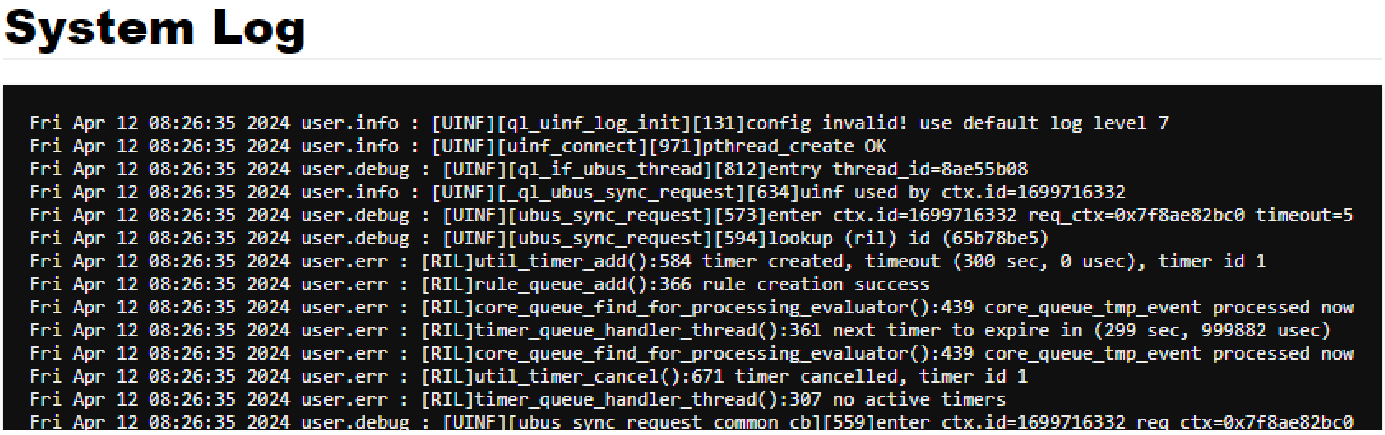
Username	Mode	Uptime	Server Tunnel IP	Client Tunnel IP	Connected By
No client online					

OpenVPN status will include information such as:

Username: The username used for authentication will be displayed.
Mode: Displays whether the OpenVPN connection is running in server mode or client mode.
Uptime: The duration of the VPN connection has been active since the last establishment.
Server Tunnel IP: This is the IP address assigned to the server side of the OpenVPN tunnel.
Client Tunnel IP: This is the IP address assigned to the client side of the OpenVPN tunnel.
Connected By: Information (IP or Hostname) about the device or client connected to the VPN.

System Logs

The system log contains various types of messages and information about system events, services, and network activity. These logs are invaluable for monitoring the health and performance of your 8355P 5G CPE, troubleshooting issues, and analyzing security events.



System Log

```
Fri Apr 12 08:26:35 2024 user.info : [UINF][ql_uinf_log_init][131]config invalid! use default log level 7
Fri Apr 12 08:26:35 2024 user.info : [UINF][uinf_connect][971]pthread_create OK
Fri Apr 12 08:26:35 2024 user.debug : [UINF][ql_if_ubus_thread][812]entry thread_id=8ae55b08
Fri Apr 12 08:26:35 2024 user.info : [UINF][_ql_ubus_sync_request][634]uinf used by ctx.id=1699716332
Fri Apr 12 08:26:35 2024 user.debug : [UINF][ubus_sync_request][573]enter ctx.id=1699716332 req_ctx=0x7f8ae82bc0 timeout=5
Fri Apr 12 08:26:35 2024 user.debug : [UINF][ubus_sync_request][594]lookup (ril) id (65b78be5)
Fri Apr 12 08:26:35 2024 user.err : [RIL]util_timer_add():584 timer created, timeout (300 sec, 0 usec), timer id 1
Fri Apr 12 08:26:35 2024 user.err : [RIL]rule_queue_add():366 rule creation success
Fri Apr 12 08:26:35 2024 user.err : [RIL]core_queue_find_for_processing_evaluator():439 core_queue_tmp_event processed now
Fri Apr 12 08:26:35 2024 user.err : [RIL]timer_queue_handler_thread():361 next timer to expire in (299 sec, 999882 usec)
Fri Apr 12 08:26:35 2024 user.err : [RIL]core_queue_find_for_processing_evaluator():439 core_queue_tmp_event processed now
Fri Apr 12 08:26:35 2024 user.err : [RIL]util_timer_cancel():671 timer cancelled, timer id 1
Fri Apr 12 08:26:35 2024 user.err : [RIL]timer_queue_handler_thread():307 no active timers
Fri Apr 12 08:26:35 2024 user.debug : [UINF][ubus_sync_request_common_cb][559]enter ctx.id=1699716332 req_ctx=0x7f8ae82bc0
```

Here are some common types of messages you might see in the 8355P 5G CPE system log:

Kernel Messages: These messages come directly from the Linux kernel and provide information about system hardware, device drivers, and kernel-level events. Examples include device initialization messages, hardware error notifications, and network interface status changes.

Service Messages: These messages come from various services running on the router, such as DHCP, DNS, NTP, and firewall services. They provide information about service startup, configuration changes, errors, and service-specific events.

Network Messages: These messages pertain to network activity and events, such as interface link status changes, DHCP lease assignments, DNS queries, NAT translations, and firewall rule matches.

Security Messages: These messages relate to security events and activities on the router, such as failed login attempts, firewall rule violations, port scans, and intrusion detection system (IDS) alerts.

System Events: These messages cover general system events and activities, such as system reboots, software package installations or updates, file system mounts, and system resource usage.

User Activity: These messages capture user-initiated actions and commands executed on the router, such as login/logout events, configuration changes made via the web interface or command line, and system commands executed by users with administrative privileges.

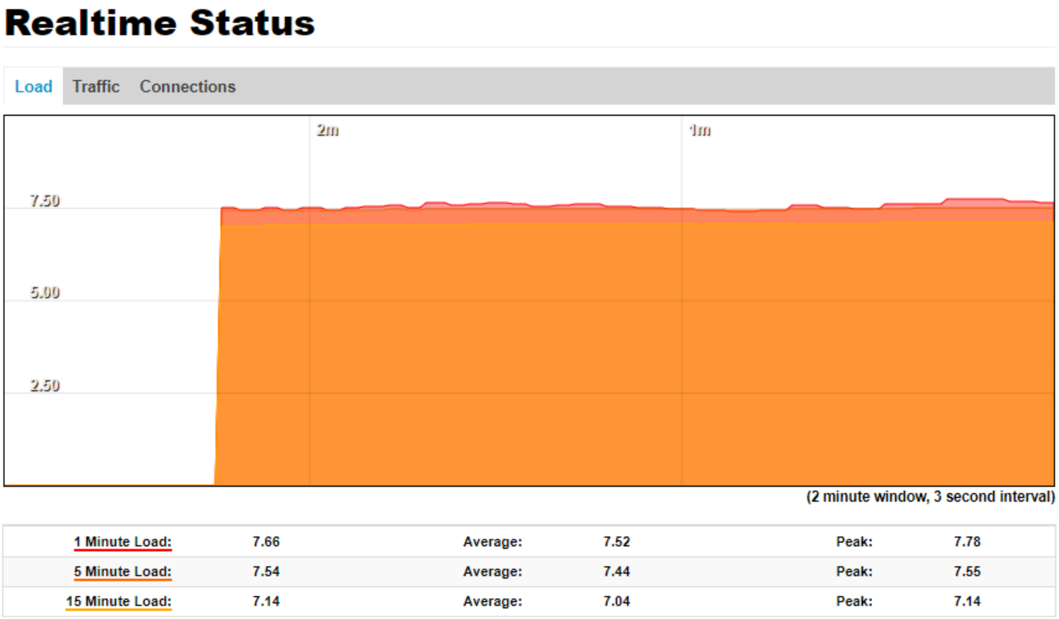
Warnings and Errors: These messages indicate warnings or errors encountered during system operation, such as configuration errors, failed service startups, hardware failures, and critical system errors.

Realtime Status

Realtime Status refers to dynamic and up-to-date information about various system and network parameters that are continuously updated in real time. This information provides users with a live view of the 8355P 5G CPE current state and activity.

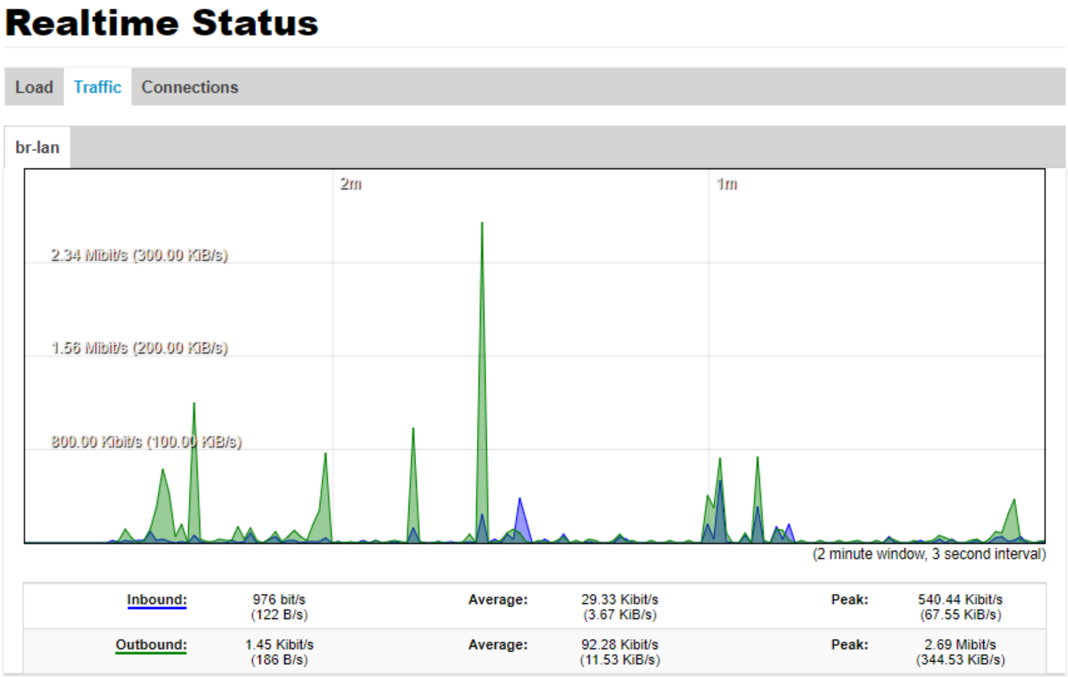
Below are examples of real-time status provided by the 8355P 5G CPE

System Load: The current system load, represented by the average number of processes in the system's run queue over the last 1, 5, and 15 minutes. This provides an indication of how busy the router's CPU is at any given moment.



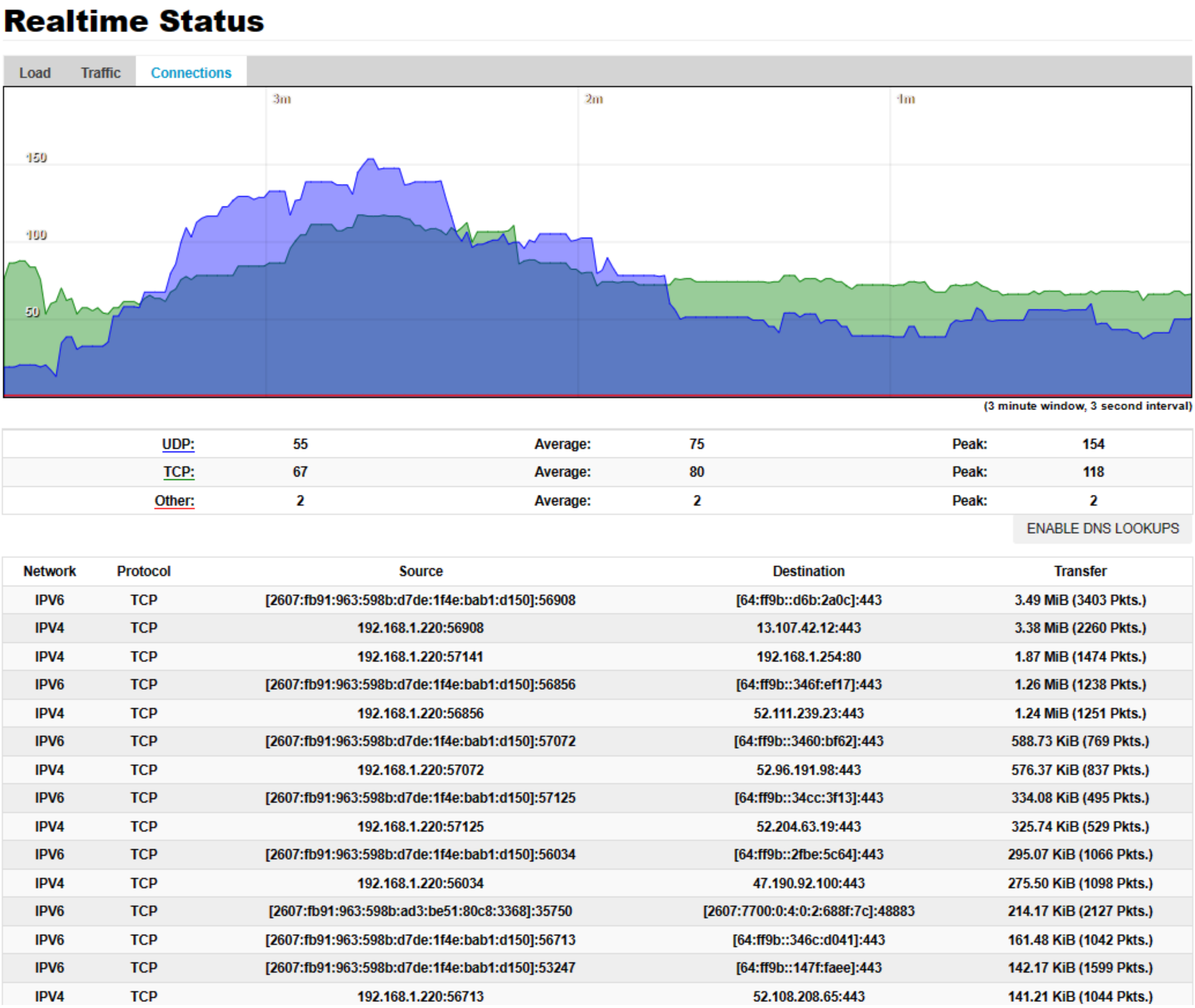
1 Minute Load:	7.66	Average:	7.52	Peak:	7.78
5 Minute Load:	7.54	Average:	7.44	Peak:	7.55
15 Minute Load:	7.14	Average:	7.04	Peak:	7.14

Traffic: Real-time statistics about network traffic, including the amount of data transmitted and received on each network interface, as well as the overall network throughput.


Realtime Status
Load
Traffic
Connections
br-lan
2m
1m
2.34 Mibit/s (300.00 KiB/s)
1.56 Mibit/s (200.00 KiB/s)
800.00 Kibit/s (100.00 KiB/s)
(2 minute window, 3 second interval)

Inbound:	976 bit/s (122 B/s)	Average:	29.33 Kibit/s (3.67 KiB/s)	Peak:	540.44 Kibit/s (67.55 KiB/s)
Outbound:	1.45 Kibit/s (186 B/s)	Average:	92.28 Kibit/s (11.53 KiB/s)	Peak:	2.69 Mibit/s (344.53 KiB/s)

Connections: Real-time status information about connections typically includes details about the current active network connections passing through the router. This information gives users a live view of the connections being established, maintained, or terminated on the router.



UDP:	55	Average:	75	Peak:	154
TCP:	67	Average:	80	Peak:	118
Other:	2	Average:	2	Peak:	2

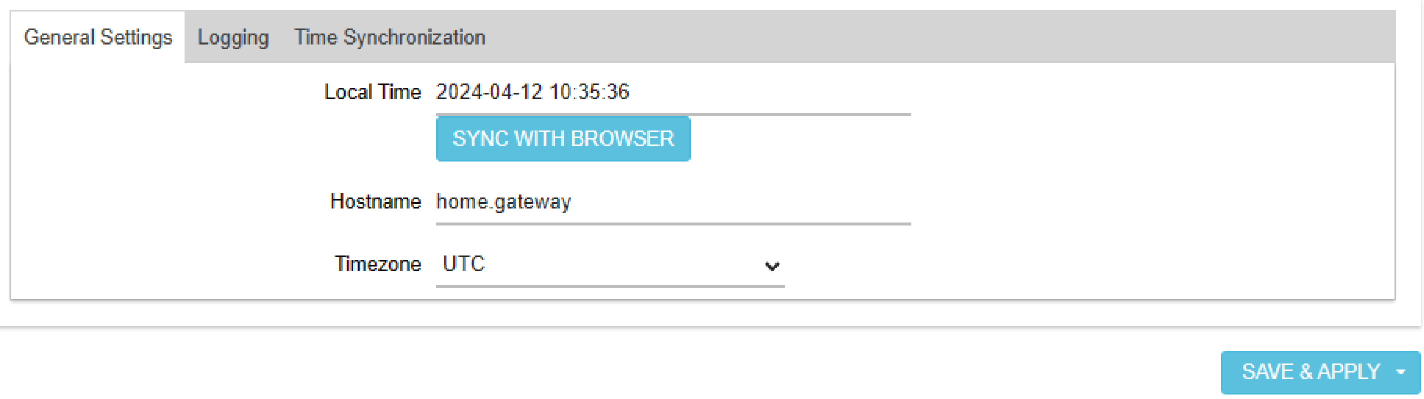
Network	Protocol	Source	Destination	Transfer
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:56908	[64:ff9b::d6b:2a0c]:443	3.49 MiB (3403 Pkts.)
IPV4	TCP	192.168.1.220:56908	13.107.42.12:443	3.38 MiB (2260 Pkts.)
IPV4	TCP	192.168.1.220:57141	192.168.1.254:80	1.87 MiB (1474 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:56856	[64:ff9b::346f:ef17]:443	1.26 MiB (1238 Pkts.)
IPV4	TCP	192.168.1.220:56856	52.111.239.23:443	1.24 MiB (1251 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:57072	[64:ff9b::3460:bf62]:443	588.73 KiB (769 Pkts.)
IPV4	TCP	192.168.1.220:57072	52.96.191.98:443	576.37 KiB (837 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:57125	[64:ff9b::34cc:3f13]:443	334.08 KiB (495 Pkts.)
IPV4	TCP	192.168.1.220:57125	52.204.63.19:443	325.74 KiB (529 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:56034	[64:ff9b::2fbe:5c64]:443	295.07 KiB (1066 Pkts.)
IPV4	TCP	192.168.1.220:56034	47.190.92.100:443	275.50 KiB (1098 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:ad3:be51:80c8:3368]:35750	[2607:7700:0:4:0:2:688f:7c]:48883	214.17 KiB (2127 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:56713	[64:ff9b::346c:d041]:443	161.48 KiB (1042 Pkts.)
IPV6	TCP	[2607:fb91:963:598b:d7de:1f4e:bab1:d150]:53247	[64:ff9b::147f:faee]:443	142.17 KiB (1599 Pkts.)
IPV4	TCP	192.168.1.220:56713	52.108.208.65:443	141.21 KiB (1044 Pkts.)

Device Configuration - System

System properties refer to various attributes and essential configurations of the 8355P 5G CPE, such as: System Properties, Administration, Backup / Flash Firmware, and Reboot. These functions are described in the following sections.

System Properties - General Settings

Allows the configuration of the local time, hostname, and time zone.



Local Time 2024-04-12 10:35:36

Hostname home.gateway

Timezone UTC

Local Time: You can enter the current date and time manually or select sync with Browser.

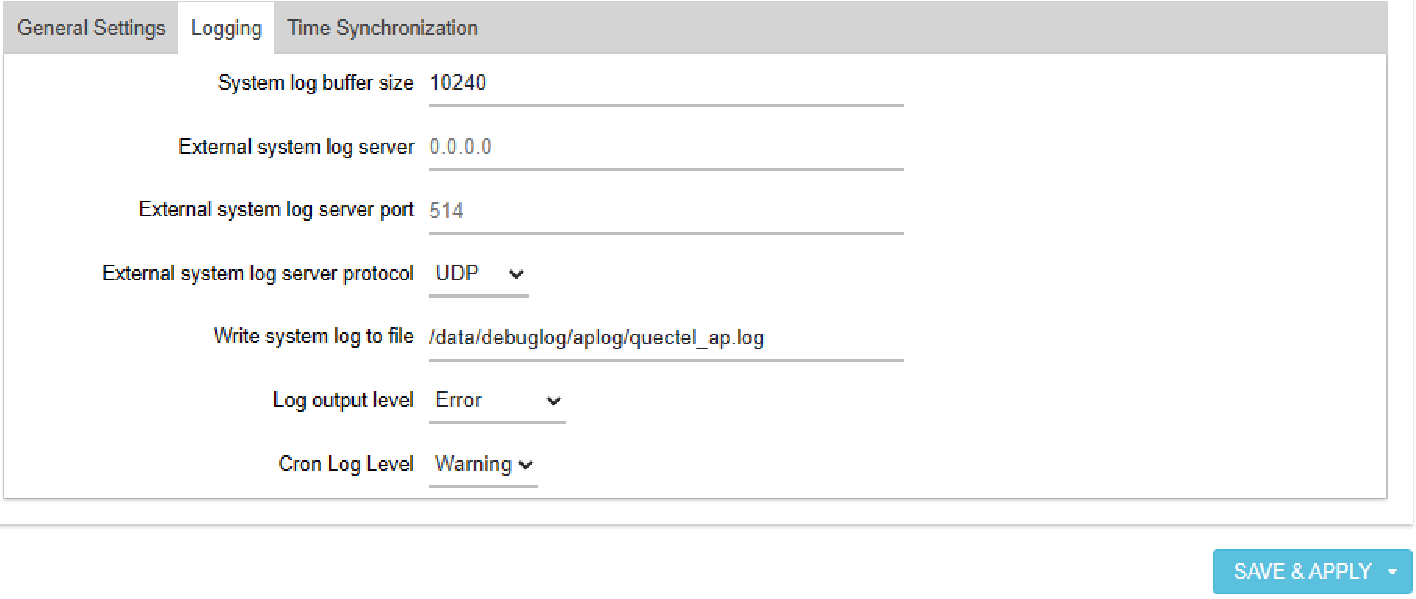
Hostname: Enter the desired hostname

Timezone: Select your geographic region and the corresponding time zone from the dropdown menu.

Click "Save & Apply" to save changes to any settings.

System Properties - Logging

Logging: Allows the configuration of how and where to write logging information.



System log buffer size 10240

External system log server 0.0.0.0

External system log server port 514

External system log server protocol UDP

Write system log to file /data/debuglog/aplog/quectel_ap.log

Log output level Error

Cron Log Level Warning

System log buffer size: This setting determines the size of the system log buffer, which is the amount of memory allocated for storing log messages before they are written to disk or sent to a remote syslog server.

External system log server: This setting specifies the IP address or hostname of the external syslog server where log messages will be sent for remote logging.

External system log server port: This setting specifies the port number used for communication with the external syslog server. By default, syslog servers listen on port 514 for incoming log messages, but you can specify a different port if needed.

External system log server protocol: This setting specifies the protocol used for communication with the external syslog server. The two common protocols used for syslog communication are UDP and TCP. UDP is typically used for its simplicity and efficiency, while TCP provides reliability and ensures that log messages are not lost in transit.

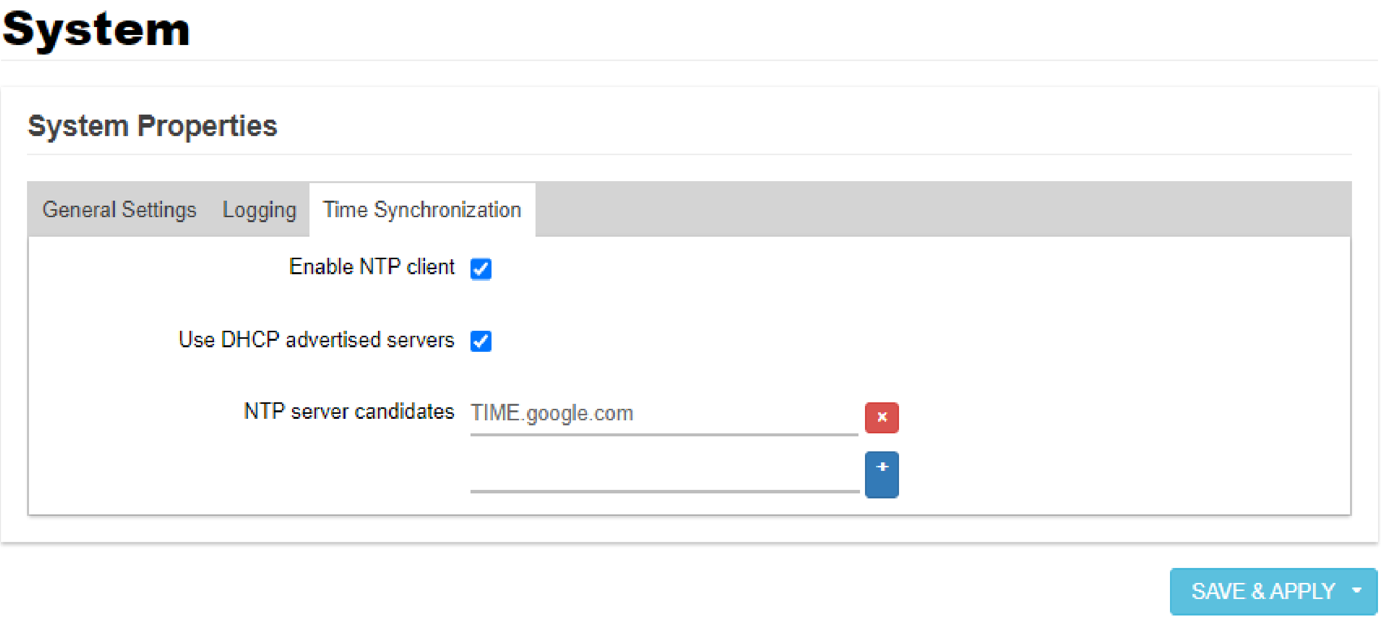
Write system log to file: This setting determines whether log messages should be written to local log files on the router's filesystem in addition to being sent to a remote syslog server. Enabling this option allows you to retain a local copy of log messages for offline analysis or archival purposes.

Log output level: This setting determines the verbosity level of log messages that are generated by various system components and services. The log output level specifies which types of log messages should be captured and sent to the syslog server or written to local log files. Common log levels include DEBUG, INFO, NOTICE, WARNING, ERROR, CRITiCAL, ALERT, and EMERGENCY.

Cron Log Level: This setting specifies the verbosity level of log messages generated by the cron daemon, which is responsible for scheduling and executing periodic tasks (cron jobs). You can configure the cron log level to control the amount of detail included in cron-related log messages. Common log levels include DEBUG, NORMAL, and WARNING.

System Properties – Time Synchronization

Time synchronization ensures that the system clock of the 8355P 5G CPE is accurate and synchronized with a reliable time source. This is important for various reasons, including logging, scheduling tasks, and maintaining consistency in network communications. The 8355P 5G CPE supports time synchronization through the Network Time Protocol (NTP), which allows automatic synchronization of the clocks with NTP servers on the internet.



System

System Properties

Enable NTP client ☑

Use DHCP advertised servers ☑

NTP server candidates: TIME.google.com

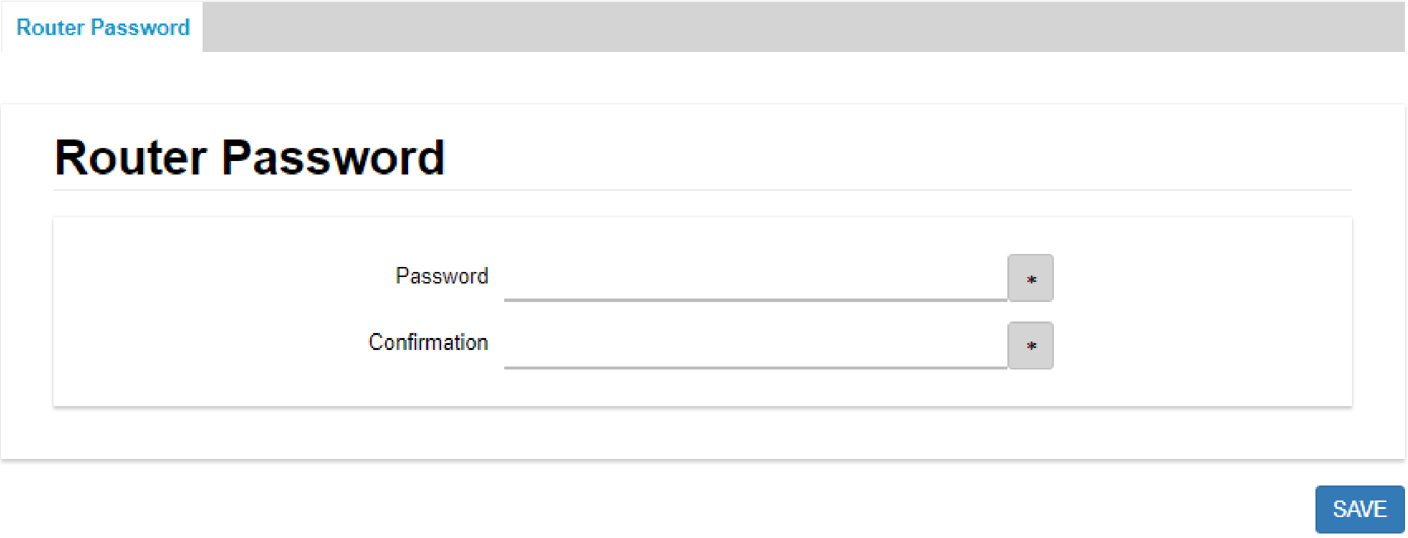
Enable NTP Client: This allows the 8355P 5G CPE's clock to synchronize with NTP servers.

Use DHCP Advertised Servers: This allows the 8355P 5G CPE to automatically obtain NTP server information from the DHCP server on your network.

NTP Server Candidates: Specifying server candidates allows the router to select the best available servers to synchronize its clock.

Administration

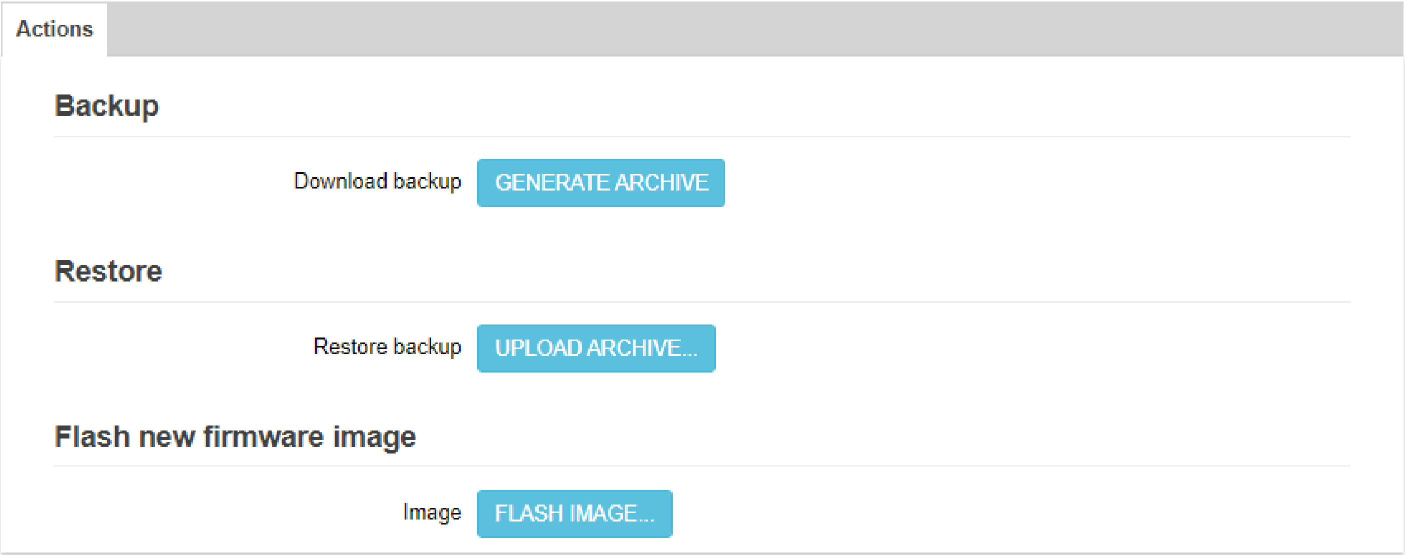
To set or change the administrator password for the 8355P 5G CPE.



After setting or changing the administrator password, remember to log out and log back in to the router using the new password to ensure that it has been successfully applied. Additionally, it's essential to keep your password secure and avoid using easily guessable passwords to protect your router from unauthorized access.

Backup / Flash Firmware

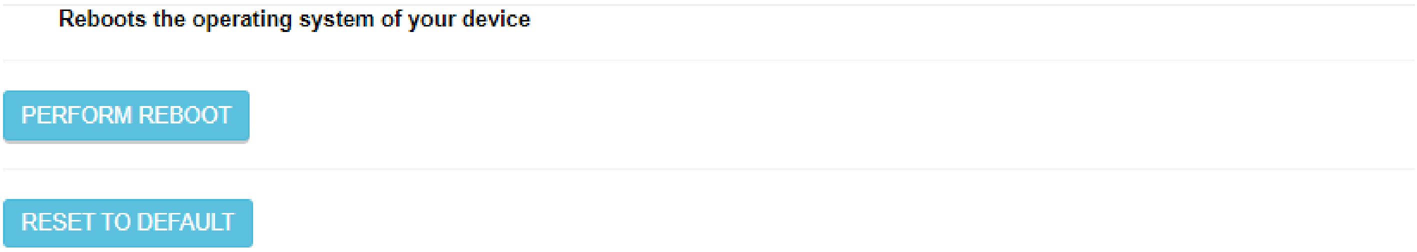
To backup, restore and flash new firmware image for the 8355P 5G CPE.


Actions
Backup
Download backup GENERATE ARCHIVE
Restore
Restore backup UPLOAD ARCHIVE...
Flash new firmware image
Image FLASH IMAGE...

By performing regular backups of your 8355P 5G CPE configuration and firmware, you can ensure that you have a copy of your settings and system files in case of accidental configuration changes or hardware failures.

Reboot

To perform a reboot or reset configuration to default for your 8355P 5G CPE.



Reboots the operating system of your device

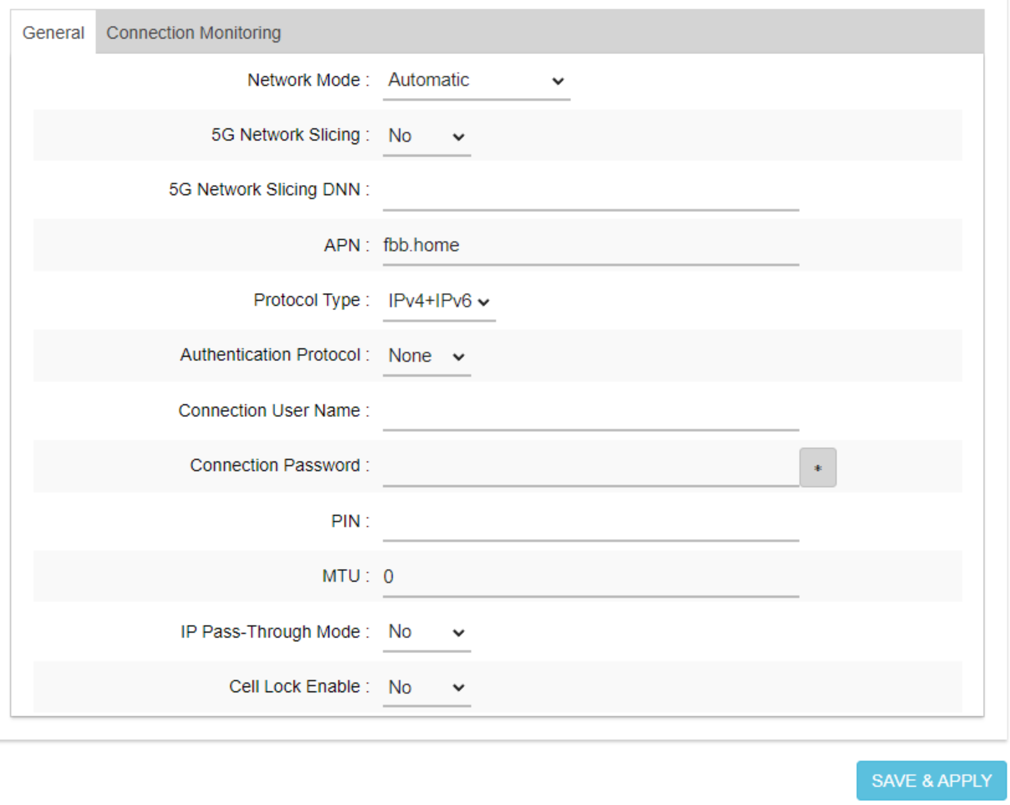
Regardless of the method you choose, initiating a reboot will restart your 8355P 5G CPE, allowing any configuration changes or updates to take effect. Make sure to save any unsaved work or configurations before rebooting to avoid data loss or interruptions in network services.

Device Configuration – Modem

Modem Settings refer to various attributes, configuration, management and monitoring of the 8355P 5G CPE modem's connection, such as: Connection Profile, Miscellaneous, 5G NR Status, Neighbor Cell, and Debug Manager. These functions are described in the following sections.

Connection Profile - General

Allows configuration of settings to manage the data connection. You can configure profiles for different networks or purposes, such as setting APNs (Access Point Names), choosing between static or dynamic IP addressing, and other network-specific settings that affect how your modem connects to the internet.



Network Mode :	Automatic
5G Network Slicing :	No
5G Network Slicing DNN :	
APN :	fbb.home
Protocol Type :	IPv4+IPv6
Authentication Protocol :	None
Connection User Name :	
Connection Password :	
PIN :	
MTU :	0
IP Pass-Through Mode :	No
Cell Lock Enable :	No

Network Mode: Generally, it's set to "Router" or similar. For cellular, it could be configured to pass through or act as a NAT gateway.

5G Network Slicing: This is not typically configured in default profiles as it requires integration with specific 5G network capabilities and service provider configurations. Network slicing allows multiple virtual networks to be created atop a common physical infrastructure.

5G Network Slicing DNN (Data Network Name): This setting specifies the name of the data network within a 5G slice. It's a part of advanced 5G network configurations and is specific to the carrier and service agreement.

APN (Access Point Name): Essential for cellular networks, the APN defines the network path for all cellular-data connectivity. Default settings would be carrier specific.

Protocol Type: This would be set to IPv4, IPv6, or both, depending on the network requirements.

Authentication Protocol: Select from options PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

Connection Username and Connection Password: These fields are used for PPP (Point-to-Point Protocol) connections over cellular networks, requiring authentication details provided by the network operator.

PIN: This would be the SIM card's PIN needed to access the cellular network if SIM security is enabled.

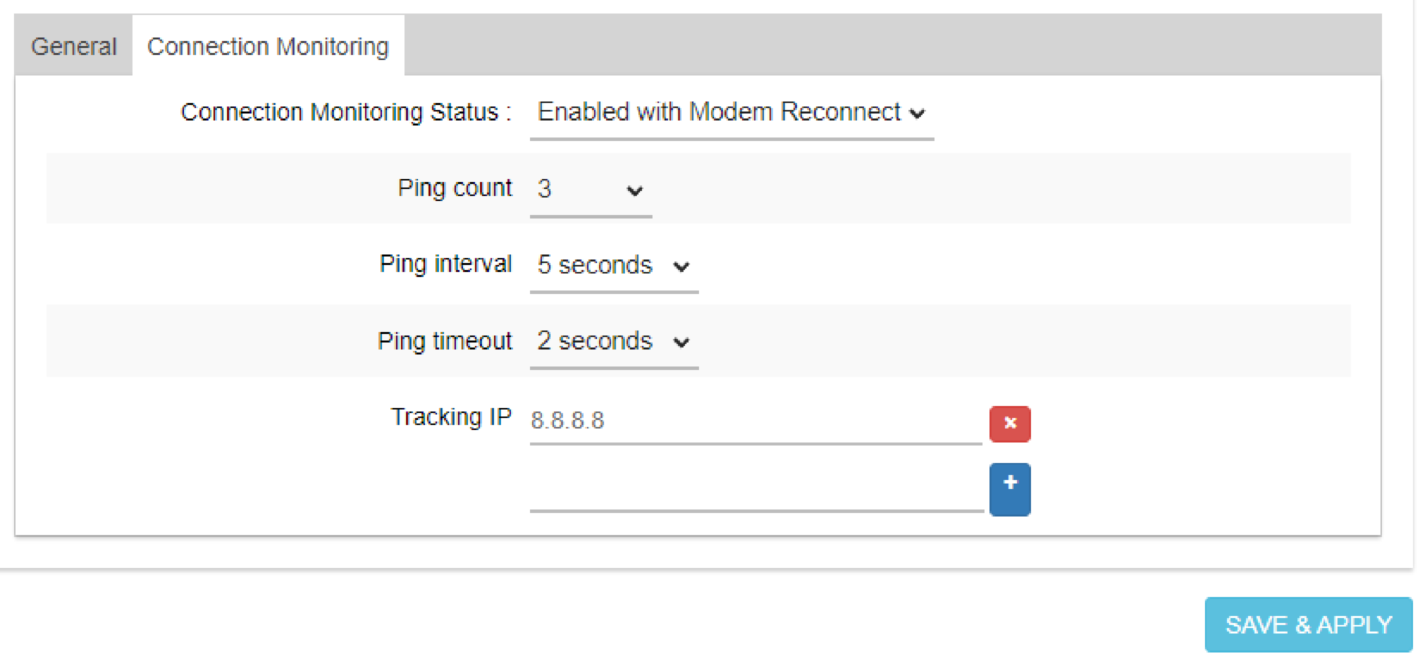
MTU (Maximum Transmission Unit): This is the largest packet that can be sent in a network transaction. For most internet usage, the default is typically 1500 bytes. However, this is typically automatically set dependent on your carrier/cellular connection.

IP Pass-Through Mode: This mode allows one device connected to the router to receive the public IP address directly from the ISP, bypassing NAT**.**

Cell Lock Enable: This setting would lock the 8355P 5G CPE to a specific cellular tower or frequency band, used to optimize connectivity or performance in certain situations.

Connection Profile – Connection Monitoring

Connection monitoring can help maintain a stable internet connection by monitoring the status and possibly taking actions like reconnecting automatically if the connection drops. This could be crucial for maintaining connectivity in environments where network reliability is critical.



Connection Monitoring Status : Enabled with Modem Reconnect

Ping count 3

Ping interval 5 seconds

Ping timeout 2 seconds

Tracking IP 8.8.8.8

Connection monitoring using parameters such as:

Ping Count: The number of ping packets sent during each check.

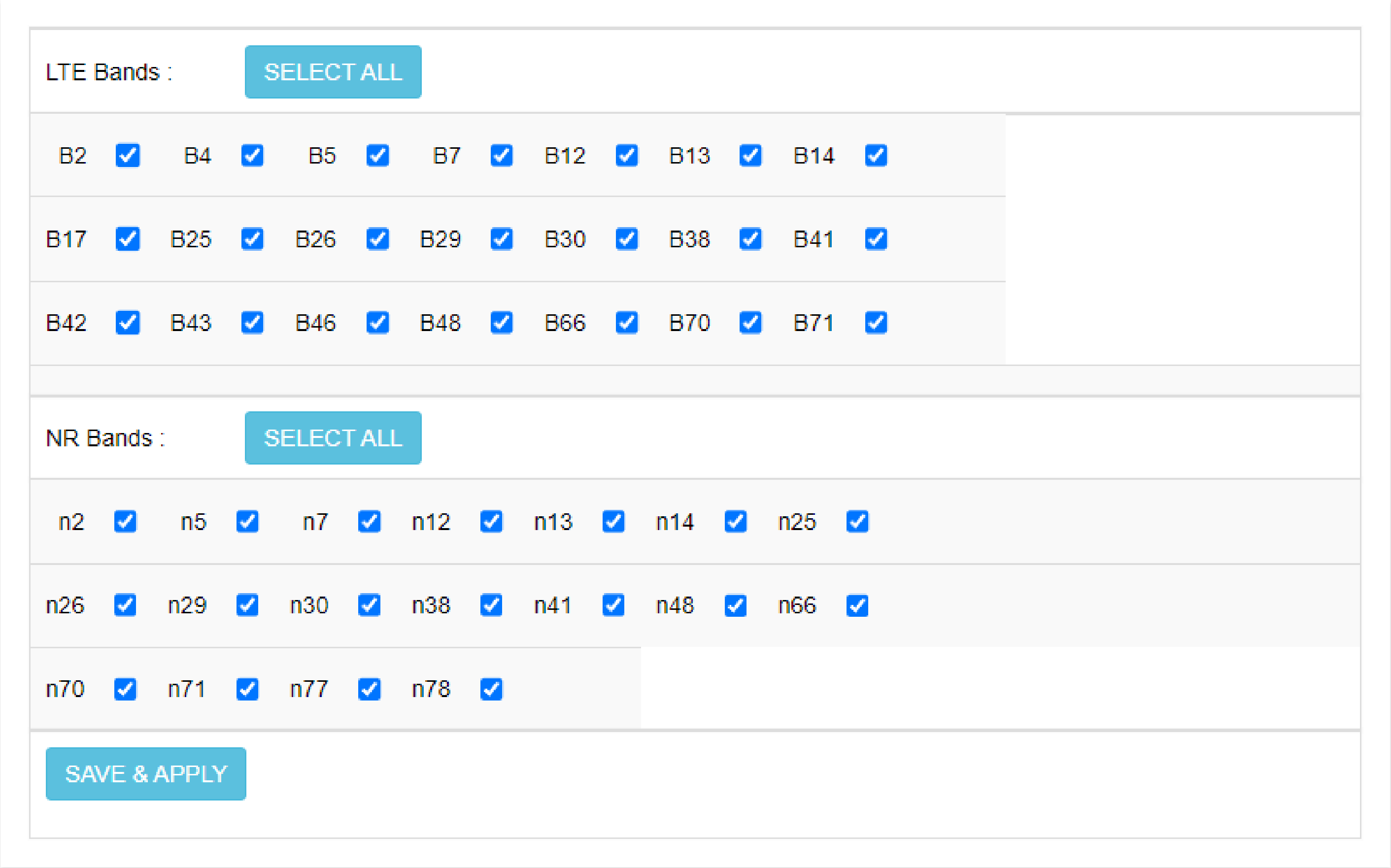
Ping Interval: This sets the interval between ping checks. Here, it’s set to 5 seconds.

Ping Timeout: The timeout for each individual ping response.

Tracking IP: This is the IP address used to check the connection. It’s often set to a reliable server like Google's DNS (8.8.8.8). You may add multiple.

Miscellaneous – Modem Features

This allows the selection or deselection of specific LTE and 5G NR bands, especially in environments where network conditions and operator capabilities vary significantly, users can fine-tune which bands the 8355P 5G CPE uses to ensure that their devices are not only operational but also optimized for their specific environment and use case.



LTE Bands : SELECT ALL

B2 ☑	B4 ☑	B5 ☑	B7 ☑	B12 ☑	B13 ☑	B14 ☑
B17 ☑	B25 ☑	B26 ☑	B29 ☑	B30 ☑	B38 ☑	B41 ☑
B42 ☑	B43 ☑	B46 ☑	B48 ☑	B66 ☑	B70 ☑	B71 ☑

NR Bands : SELECT ALL

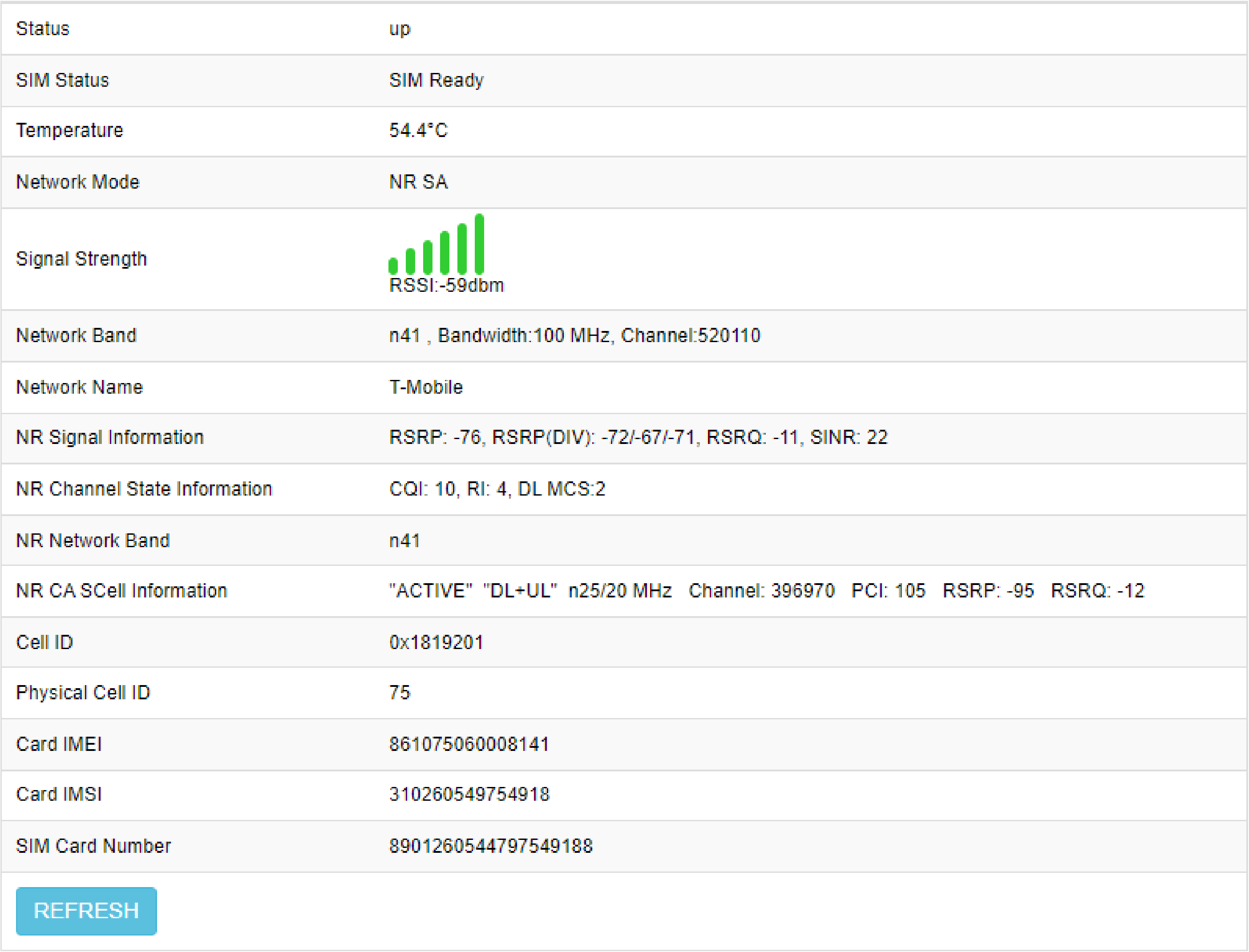
n2 ☑	n5 ☑	n7 ☑	n12 ☑	n13 ☑	n14 ☑	n25 ☑
n26 ☑	n29 ☑	n30 ☑	n38 ☑	n41 ☑	n48 ☑	n66 ☑
n70 ☑	n71 ☑	n77 ☑	n78 ☑			

SAVE & APPLY

TIP: Clicking “SELECT ALL” will display “SELECT NONE” to quickly deselect all bands, allowing you to easily select the desired bands. Click Save & Apply to save any changes.

5G NR Status

Displays several key parameters that provide insights into the performance and configuration of your 8355P 5G CPE.



Status	up
SIM Status	SIM Ready
Temperature	54.4°C
Network Mode	NR SA
Signal Strength	RSSI:-59dbm
Network Band	n41 , Bandwidth:100 MHz, Channel:520110
Network Name	T-Mobile
NR Signal Information	RSRP: -76, RSRP(DIV): -72/-67/-71, RSRQ: -11, SINR: 22
NR Channel State Information	CQI: 10, RI: 4, DL MCS:2
NR Network Band	n41
NR CA SCell Information	"ACTIVE" "DL+UL" n25/20 MHz Channel: 396970 PCI: 105 RSRP: -95 RSRQ: -12
Cell ID	0x1819201
Physical Cell ID	75
Card IMEI	861075060008141
Card IMSI	310260549754918
SIM Card Number	8901260544797549188

Status: Indicates whether the modem is connected, trying to establish a connection, or disconnected.

Temperature: This shows the operating temperature of the modem, which is critical for assessing device health and avoiding overheating issues.

Network Mode: This indicates the modem's current network technology (e.g., LTE, EN-DC, 5G SA).

Signal Strength: This displays signal strength in dBm, which helps determine the network connection quality.

Network Band: Specifies the LTE or NR band the modem is using along with the amount of bandwidth and channel.

Network Name: Shows the name of the connected network provider.

NR Signal Information: Provides detailed signal information for NR, such as RSRP (Reference Signal Received Power), RSRP-DIV (Reference Signal Received Power Diversity), RSRQ (Reference Signal Received Quality), SINR (Signal to Noise plus Interference Ratio)

NR Channel State Information: This section includes information about the state of the NR channels, which helps in understanding channel conditions and performance such as: CQI (Channel Quality Indicator), RI (Rank Indicator), DL MCS (Modulation and Coding Scheme).

NR Network Band: Specific to 5G, it details which NR band(s) are currently being used.

NR CA Scell Information: Details about Carrier Aggregation on 5G NR, including secondary cell configurations and their status.

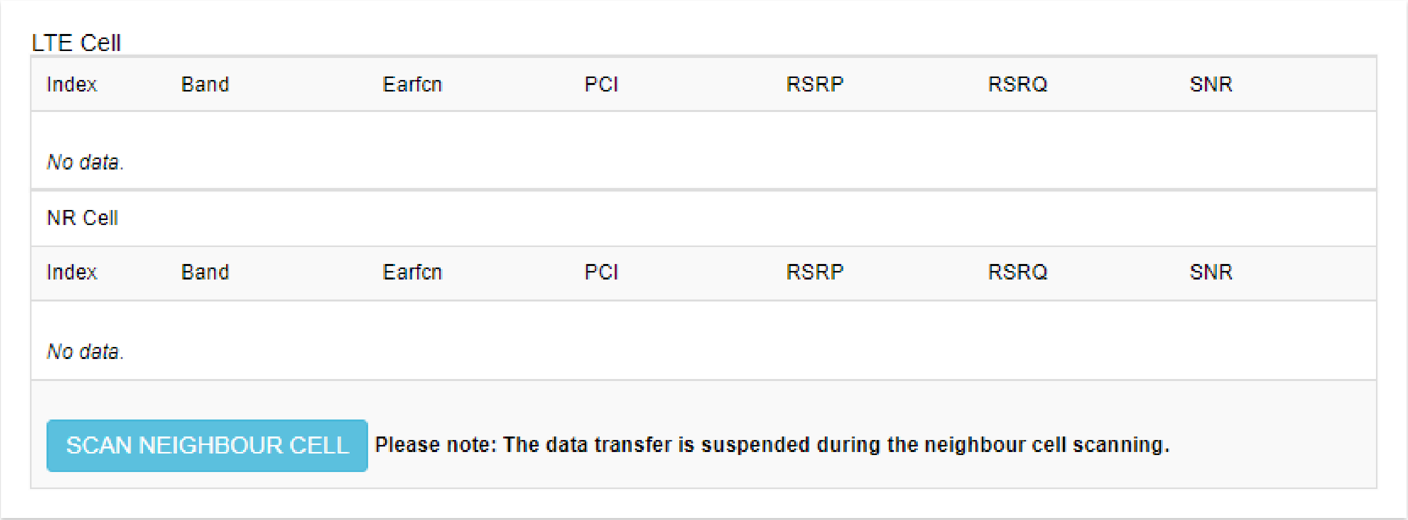
Cell ID: The unique identifier for the cell to which the modem is currently connected.

Physical Cell ID: This is a physical layer identifier that is part of the cell identity in the network and is important for network operations and troubleshooting.

Card IMEI: Displays the unique 15-digit serial number assigned to every cellular device that can access a cellular network. The IMEI (International Mobile Equipment Identity) is an identifier for the device on cellular networks, allowing networks to authenticate and distinguish it from other devices.

Neighbor Cell

Neighbor Cell information includes details about nearby cellular towers “Neighbors”, other than the one to which the 8355P 5G CPE is currently connected.



LTE Cell

Index	Band	Earfcn	PCI	RSRP	RSRQ	SNR
No data.						

NR Cell

Index	Band	Earfcn	PCI	RSRP	RSRQ	SNR
No data.						

Please note: The data transfer is suspended during the neighbour cell scanning.

Select "SCAN NEIGHBOR CELL" to provide detailed information such as:

Index: A numeric identifier assigned to each neighboring cell to distinguish them in the list.

Band: The specific frequency band on which the neighboring cell operates is important for understanding the cell’s coverage characteristics.

EarFCN (E-UTRA Absolute Radio Frequency Channel Number): This number corresponds to the frequency of the LTE band that the neighboring cell is using. It is specific to LTE technology and helps identify the exact downlink and uplink frequencies being used.

PCI (Physical Cell ID): A unique identifier used in cellular networks to identify cells. Each cell in a network is assigned a PCI, which is critical for the operation of cell-specific functions and handovers.

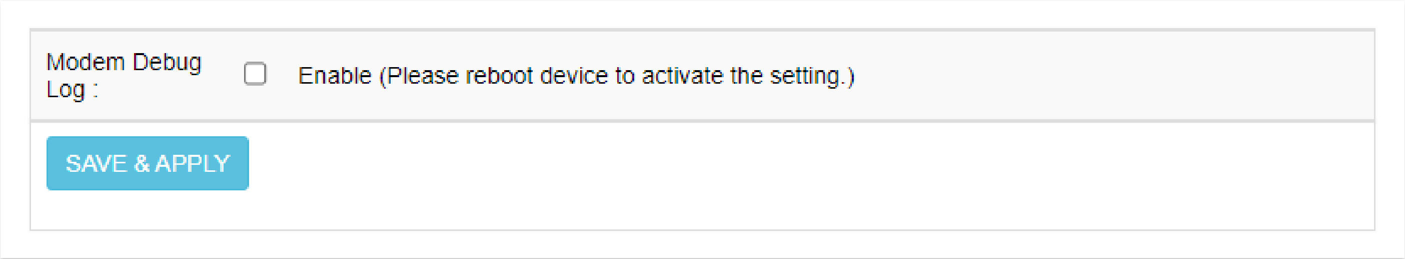
RSRQ (Reference Signal Received Quality): A key performance indicator in cellular networks used to assess the quality of the received signal relative to the interference and noise present in the channel. It is a critical measurement for determining the overall condition of a cellular connection.

RSRP (Reference Signal Received Power): A measure of the power level of the cellular Reference Signals within the cell. It is the most important metric for measuring signal strength from a neighboring cell.

SINR (Signal-to-interference plus Noise Ratio): Measures the quality of the cellular signal. It is a ratio of the signal power to the interference and noise power and is critical for assessing the usability of a radio channel in the presence of interference.

Debug Manager

The modem debug manager will allow the examination of logs specific to the modem's activities. This is useful in troubleshooting connectivity problems, understanding modem behavior, and optimizing configurations.



Modem Debug Log : □ Enable (Please reboot device to activate the setting.)

Modem Debug Log: Select the radio button to enable.

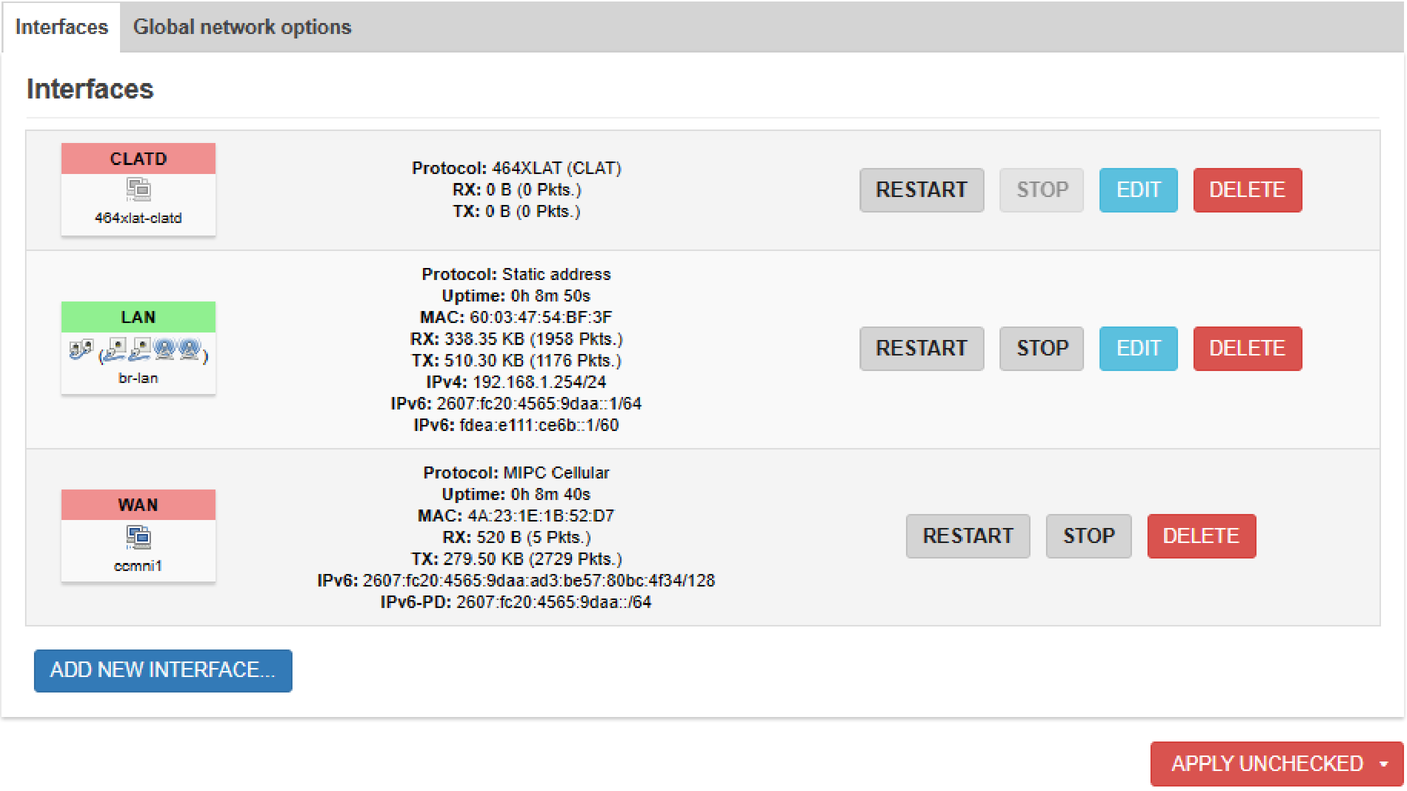
Click **Save** & **Apply to** save settings. Reboot 8355P 5G CPE.

Device Configuration – Network

Network Settings refer to various attributes, management, and monitoring of the 8355P 5G CPE network configuration, such as Interfaces, Wireless 2.4G, Wireless 5G, DHCP and DNS, Hostnames, Static Routes, Speedtest, Firewall, Diagnostics, TR069, and BECentral Management. These functions are described in the following sections.

Interfaces

Allows monitoring and the management of network interfaces involving common operations such as adding, restarting, stopping, editing, and deleting interfaces.



Interfaces

CLATD
464xlat-clatd
Protocol: 464XLAT (CLAT)
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

LAN
br-lan
Protocol: Static address
Uptime: 0h 8m 50s
MAC: 60:03:47:54:BF:3F
RX: 338.35 KB (1958 Pkts.)
TX: 510.30 KB (1176 Pkts.)
IPv4: 192.168.1.254/24
IPv6: 2607:fc20:4565:9daa::1/64
IPv6: fdea:e111:ce6b::1/60

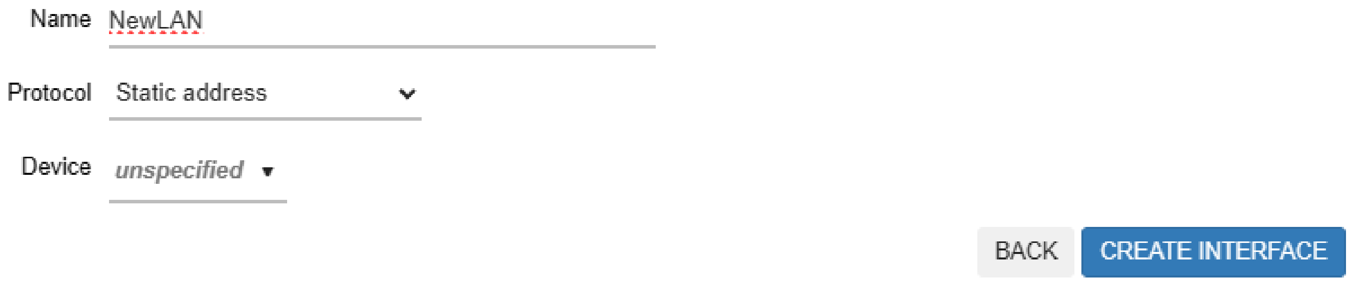
WAN
ccmni1
Protocol: MIPC Cellular
Uptime: 0h 8m 40s
MAC: 4A:23:1E:1B:52:D7
RX: 520 B (5 Pkts.)
TX: 279.50 KB (2729 Pkts.)
IPv6: 2607:fc20:4565:9daa:ad3:be57:80bc:4f34/128
IPv6-PD: 2607:fc20:4565:9daa::/64

Add New Interface

Click on Add new interface.... You will need to provide details for the new interface:

Name: Enter a name for your new interface, such as NewLAN.
Protocol: Select the protocol (e.g., static IP, DHCP client, DHCPV6 client, etc..).
Device: Choose the physical interface (a specific Ethernet port or VLAN) from the drop-down menu.

Select Create Interface



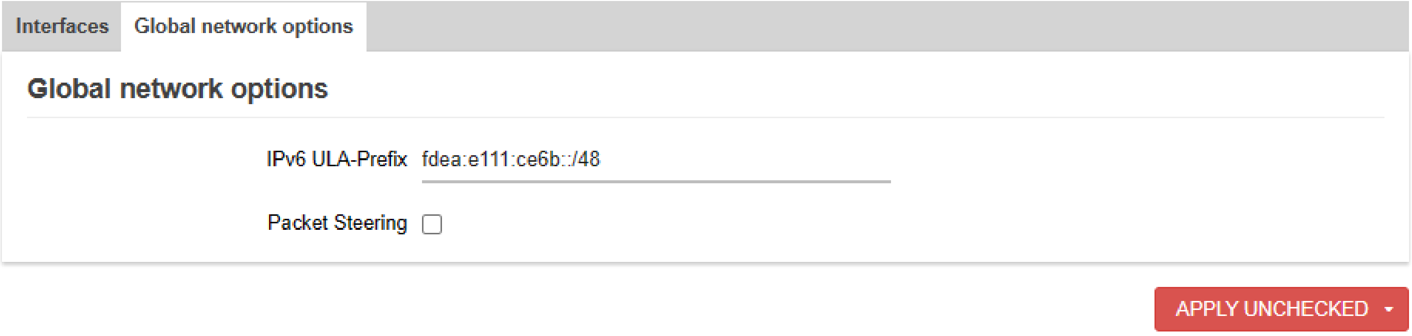
Name NewLAN

Protocol Static address

Device *unspecified*

Global Network Options

Global Network Options provide powerful ways to control and fine-tune network behavior. Configuring advanced network features like IPv6 ULA-Prefix and Packet Steering can greatly enhance your network's functionality and performance.
Note: These option are not typically needed,



Global network options

IPv6 ULA-Prefix fdea:e111:ce6b::/48

Packet Steering ☐

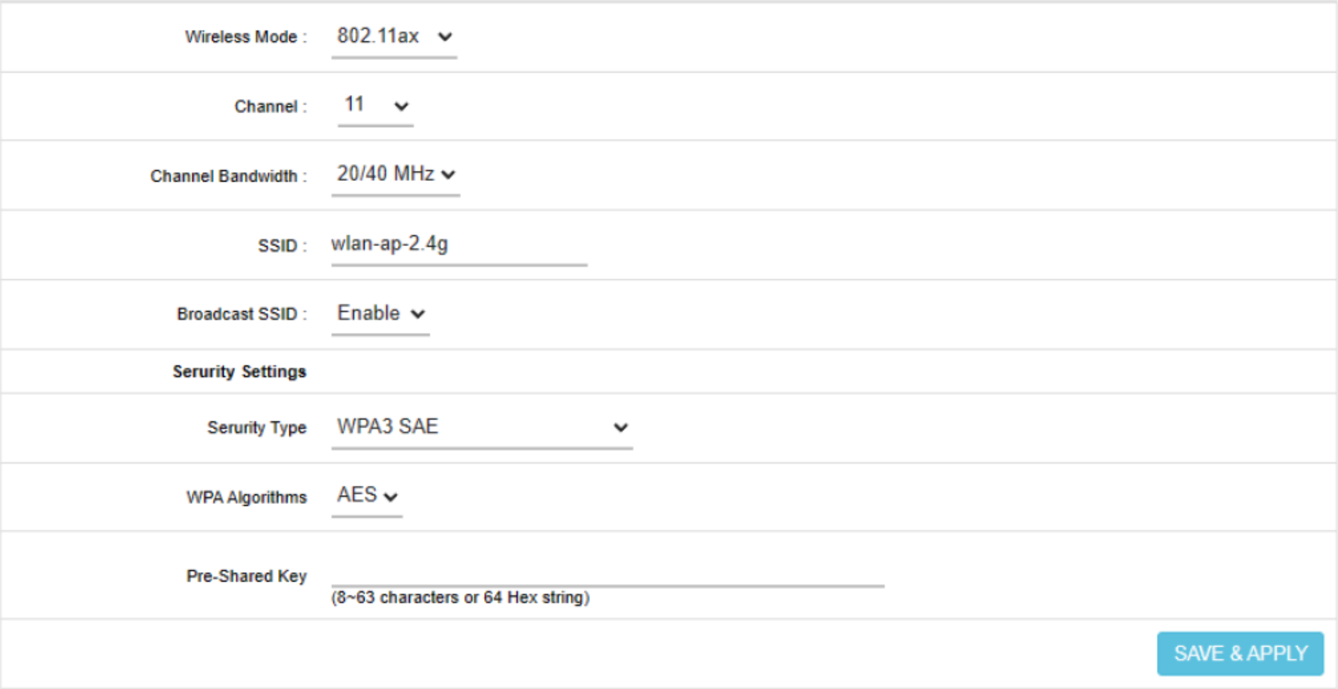
IPv6 ULA-Prefix: This prefix is used in IPv6 networking for local communications within a site (private network) and is not routable on the global internet. Generating a unique ULA prefix is important to avoid conflicts in larger network scenarios where multiple networks might interconnect.

Packet Steering: This feature is more beneficial on routers with multi-core CPUs where network traffic is heavy. It can improve performance by steering traffic to specific cores, making processing more efficient on multi-core devices.

Always make sure to back up your configurations before making significant changes.

Wireless 2.4G

Configuring wireless settings on the 8355P 5G CPE involves setting the wireless mode, selecting the channel and bandwidth, configuring the SSID (Service Set Identifier), and applying security settings.



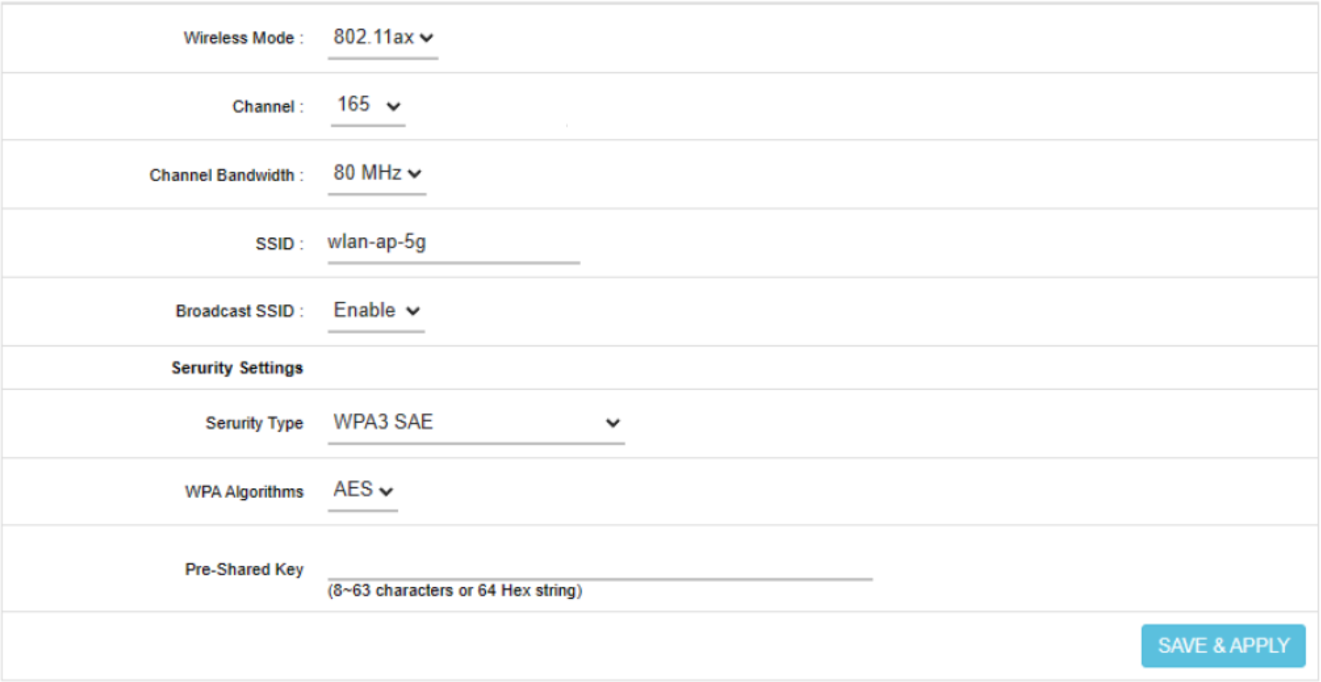
Wireless Mode :	802.11ax
Channel :	11
Channel Bandwidth :	20/40 MHz
SSID :	wlan-ap-2.4g
Broadcast SSID :	Enable
Serurity Settings	
Serurity Type	WPA3 SAE
WPA Algorithms	AES
Pre-Shared Key	(8~63 characters or 64 Hex string)

Wireless Mode: Select the wireless operation mode **(802.11ax (default)**
Channel: Choose the appropriate channel to avoid interference
Channel Bandwidth: Set the channel bandwidth (20 MHz or 20/40 MHz).
SSID (Service Set Identifier): Enter the SSID for your network.
Broadcast SSID: Select Enable to Broadcast SSID or Disable to Hide SSID
Security Settings
Security Type: Select the encryption method **(WPA3-SAE recommended)**

Click on Save & Apply to make the changes effective.

Wireless 5G

Configuring wireless settings on the 8355P 5G CPE involves setting the wireless mode, selecting the channel and bandwidth, configuring the SSID (Service Set Identifier), and applying security settings.



Wireless Mode :	802.11ax
Channel :	165
Channel Bandwidth :	80 MHz
SSID :	wlan-ap-5g
Broadcast SSID :	Enable
Serurity Settings	
Serurity Type	WPA3 SAE
WPA Algorithms	AES
Pre-Shared Key	(8~63 characters or 64 Hex string)

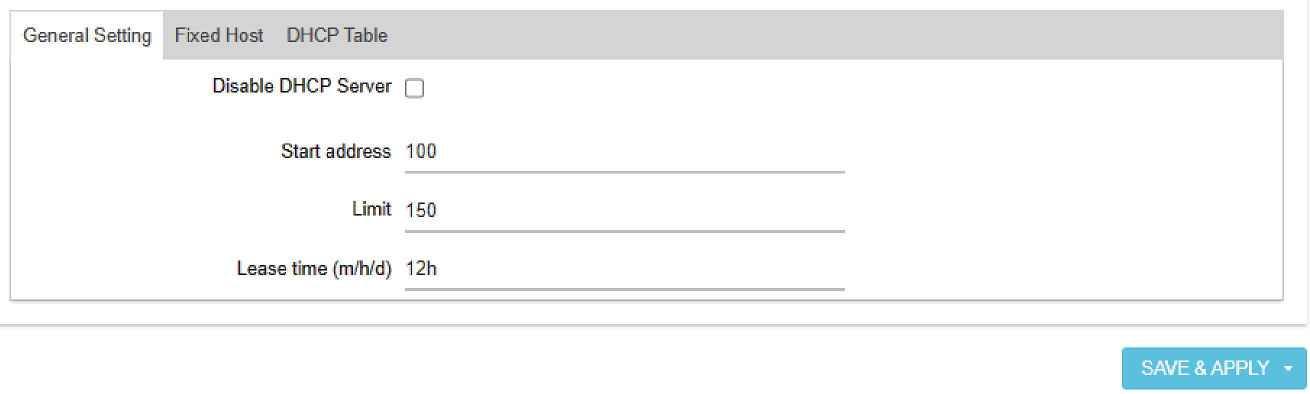
Wireless Mode: Select the wireless operation mode **(802.11ax (default)**
Channel: Choose the appropriate channel to avoid interference
Channel Bandwidth: Set the channel bandwidth (20 MHz, 40 MHz or 80 MHz).
SSID (Service Set Identifier): Enter the SSID for your network.
Broadcast SSID: Select Enable to Broadcast SSID or Disable to Hide SSID
Security Settings
Security Type: Select the encryption method **(WPA3-SAE recommended)**

Click on Save & Apply to make the changes effective.

DHCP and DNS

Dynamic Host Configuration Protocol (DHCP) settings are crucial for managing the distribution of IP addresses within your network. The DHCP server component handles these settings and assigns IP addresses to clients based on the configuration specified below.

General Setting



Disable DHCP Server ☐

Start address 100

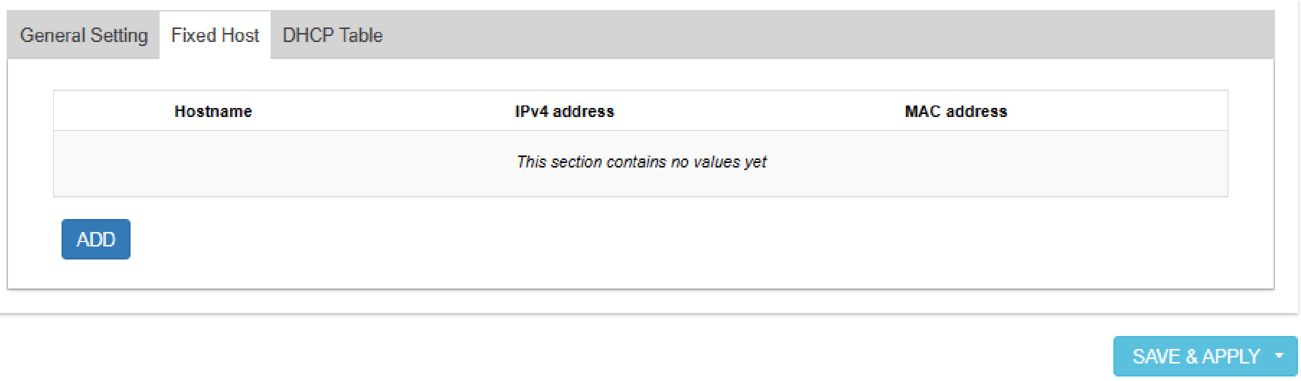
Limit 150

Lease time (m/h/d) 12h

Disable DHCP Server: Select this option to disable DHCP server.
NOTE: When disabling DHCP on an interface, ensure that another DHCP server is available on your network (if needed) or that static IPs are configured on all devices to maintain network connectivity. Disabling DHCP without an alternative can lead to connectivity issues for new or unconfigured devices on the network.
Start Address: The starting IP address relative to the network's subnet (not the absolute IP).
Limit: Maximum number of clients that can get an IP from the DHCP.
Lease time (m/h/d): Duration an IP address is leased to a client.

Fixed Host

A fixed host refers to a device on the network for which you have assigned a static IP address through DHCP reservation. By defining a fixed host, you ensure that the device always receives the same IP address every time it connects to the network, regardless of the state of the DHCP server or the order in which devices connect.



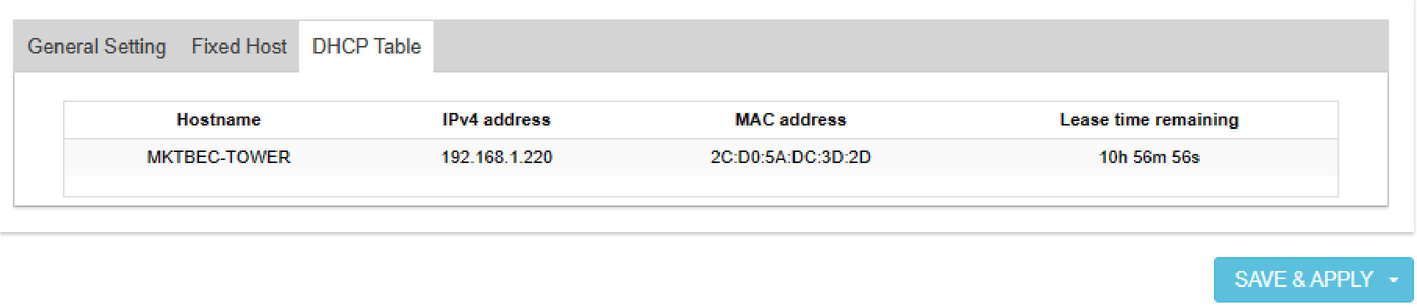
Hostname	IPv4 address	MAC address
	This section contains no values yet	

To add a fixed host, Select ADD
Hostname: Enter the Hostname of the new device for easy identification.
IPv4 Address: Specify the IPv4-Address that you want to reserve.
MAC Address: Type or the MAC Address of the device from the pull down**.**

After filling out the details, click on Save and then Save & Apply to update the settings.

DHCP Table

The DHCP table shows a list of all devices that have been assigned IP addresses by the DHCP server. This table includes information such as the hostname, IP address, MAC address, and lease expiration time for each connected device. This is particularly useful for monitoring who is connected to your network and managing network resources.

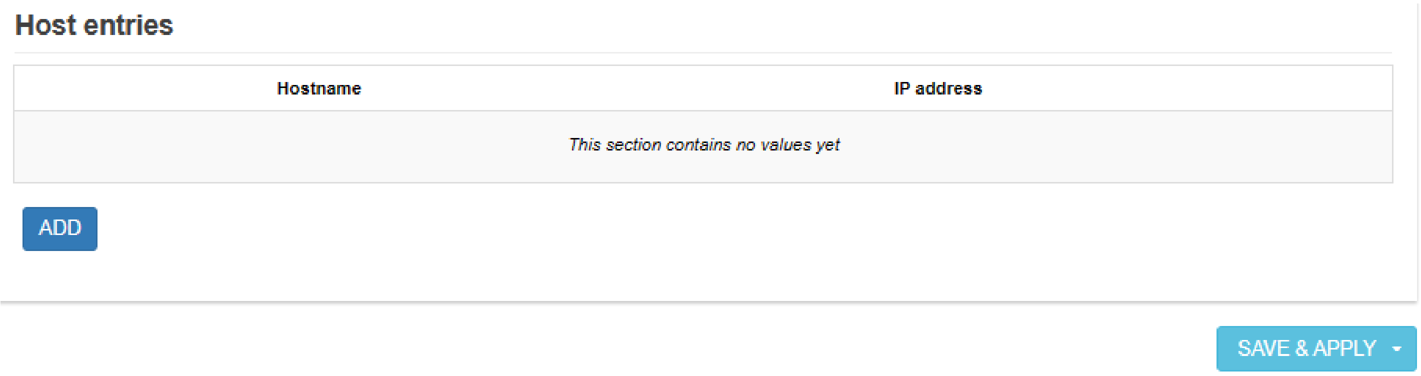


Hostname	IPv4 address	MAC address	Lease time remaining
MKTBEC-TOWER	192.168.1.220	2C:D0:5A:DC:3D:2D	10h 56m 56s

Hostnames: Hostname of device displayed if available.
IP Addresses: Shows the assigned IP address for each device.
MAC Addresses: Shows the MAC address for each device.
Lease Time Remaining: This shows when the DHCP lease will expire.

Hostnames

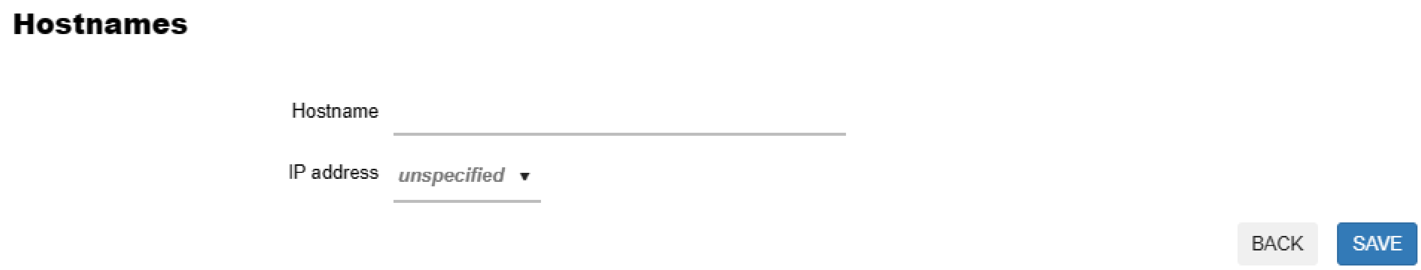
A hostname is a unique label given to a device that's connected to a network, and it's a human-readable way to distinguish that device from other devices on the network. Configured devices with hostnames will appear in the list.



Host entries

Hostname	IP address
This section contains no values yet	

To add Hostname, Select ADD



Hostnames

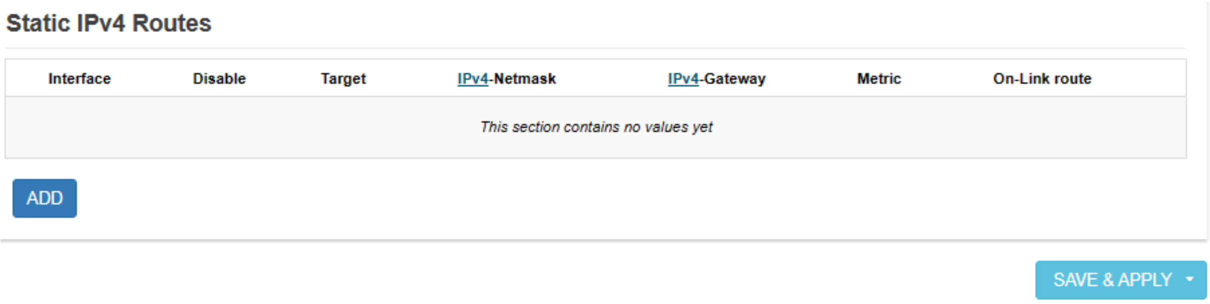
Hostname	
IP address	*unspecified* ▾

Hostname: Enter the Hostname of the new device for easy identification.
IP Address: Select the IP address from the pull down.

After filling out the details, click on Save and then Save & Apply to update the settings.

Static Routes

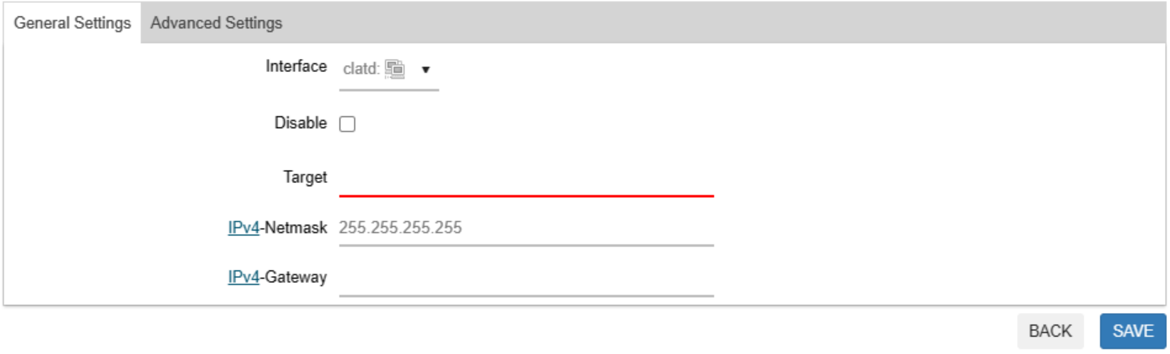
Static routes are used to define specific paths that network traffic should follow to reach a particular destination. This can be necessary for routing traffic between different subnets, directing traffic through a VPN, or managing multiple gateways in a complex network setup.



Static IPv4 Routes

Interface	Disable	Target	IPv4-Netmask	IPv4-Gateway	Metric	On-Link route
This section contains no values yet						

To add a new Static Route, Select ADD



Interface: clatd:

Disable: □

Target:

IPv4-Netmask: 255.255.255.255

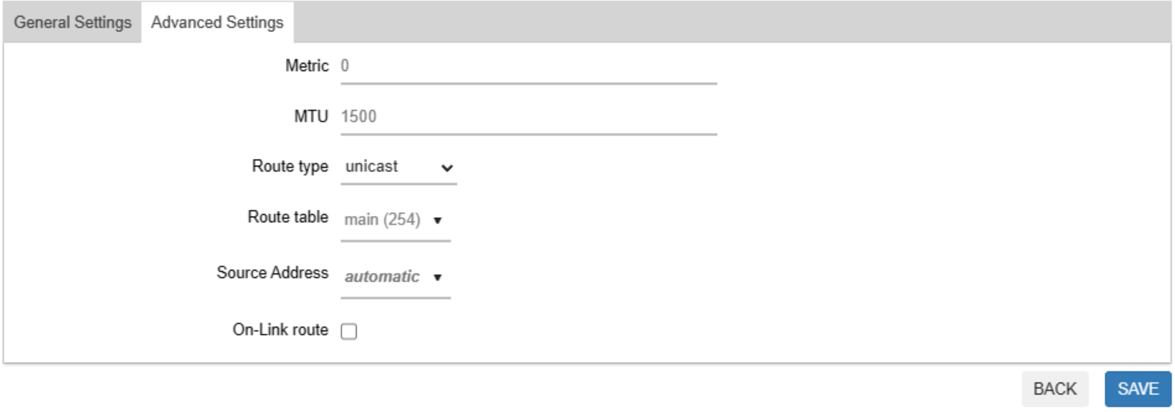
IPv4-Gateway:

Interface: Select the network interface to be used.
Target: Enter the destination network or IP.
IPv4-Netmask: Select the netmask for the target network.
IPv4-Gateway: Specify the gateway IP address.

After entering the details, click Save and then “Save and Apply” to implement the new route.

Advanced Settings

Configuring advanced settings for static routes can enhance flexibility and control over how traffic is handled within your network. These settings can be crucial for network scenarios that require specific routing behaviors or more complex configurations.



Metric 0
MTU 1500
Route type unicast
Route table main (254)
Source Address *automatic*
On-Link route □

Metric: The metric determines a route's priority. Lower values have higher priority. This is useful in environments where multiple routes to the same destination exist, and you need to specify which route should be preferred.

MTU: This specifies the Maximum Transmission Unit size for the route. It is useful when different segments of your network have different MTU requirements.

Route Type: It can be "unicast" (the default), "broadcast" (for broadcast traffic on a network segment), or "local" (for routes to local interfaces).

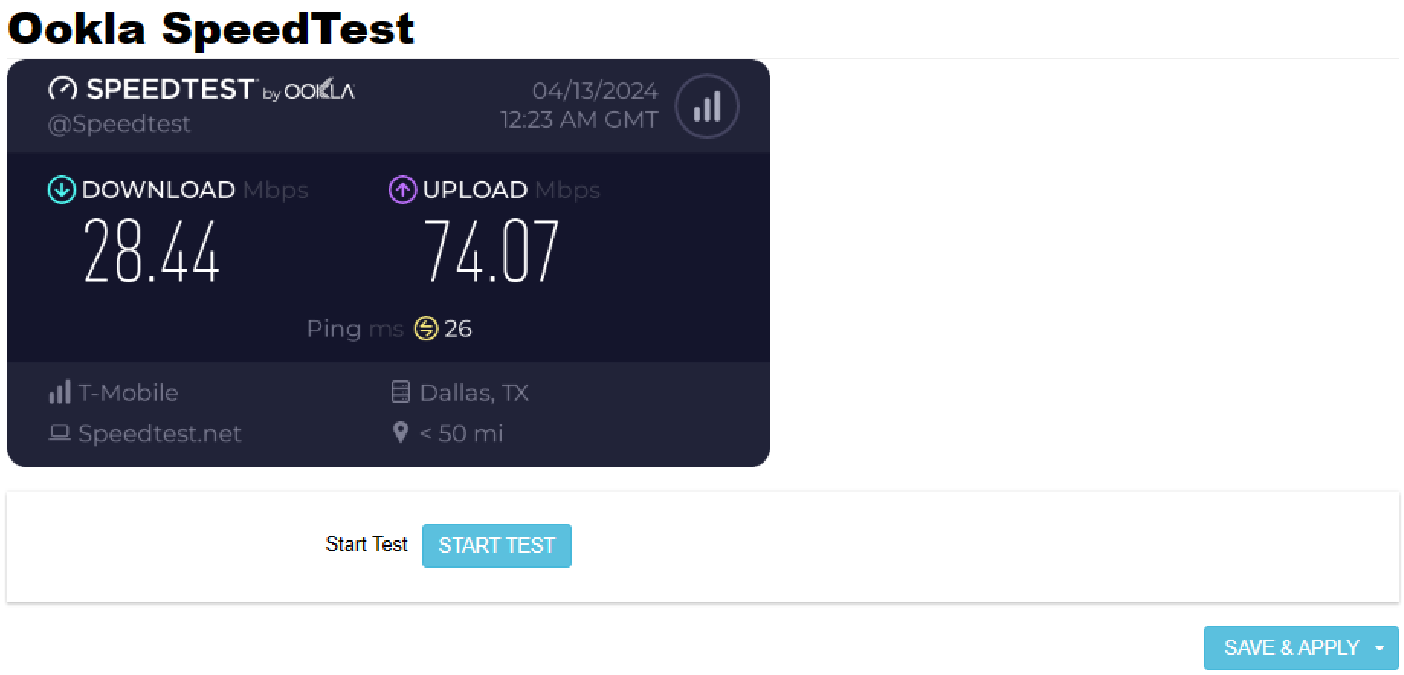
Routing Table: Specifies the routing table to which the route should be added. This allows for complex routing scenarios, such as policy-based routing, where different rules apply based on various criteria.

Source Address: Used for source-based routing, allowing routing decisions based on the source address of packets.

On-link Route: Indicates that the next hop is directly attached to the network and doesn't require a gateway.

SpeedTest

The 8355P 5G CPE integrates an Ookla Speedtest client into the system, allowing you to measure internet speeds directly from your router. This can be particularly useful for monitoring your connection without needing a separate device.



Ookla SpeedTest

SPEEDTEST by OOKLA
@Speedtest
04/13/2024
12:23 AM GMT

DOWNLOAD Mbps 28.44
UPLOAD Mbps 74.07
Ping ms 26

T-Mobile
Speedtest.net
Dallas, TX
< 50 mi

Start Test

Firewall

The 8355P 5G CPE firewall is a powerful tool for managing network traffic in and out of a router. It is based on netfilter/iptables (Linux kernel's networking and firewalling subsystem) and provides extensive capabilities for packet filtering, network address translation (NAT), and port forwarding. The firewall is highly configurable, allowing users to tailor it to their specific security needs and network configurations, suitable for both home and advanced enterprise environments.

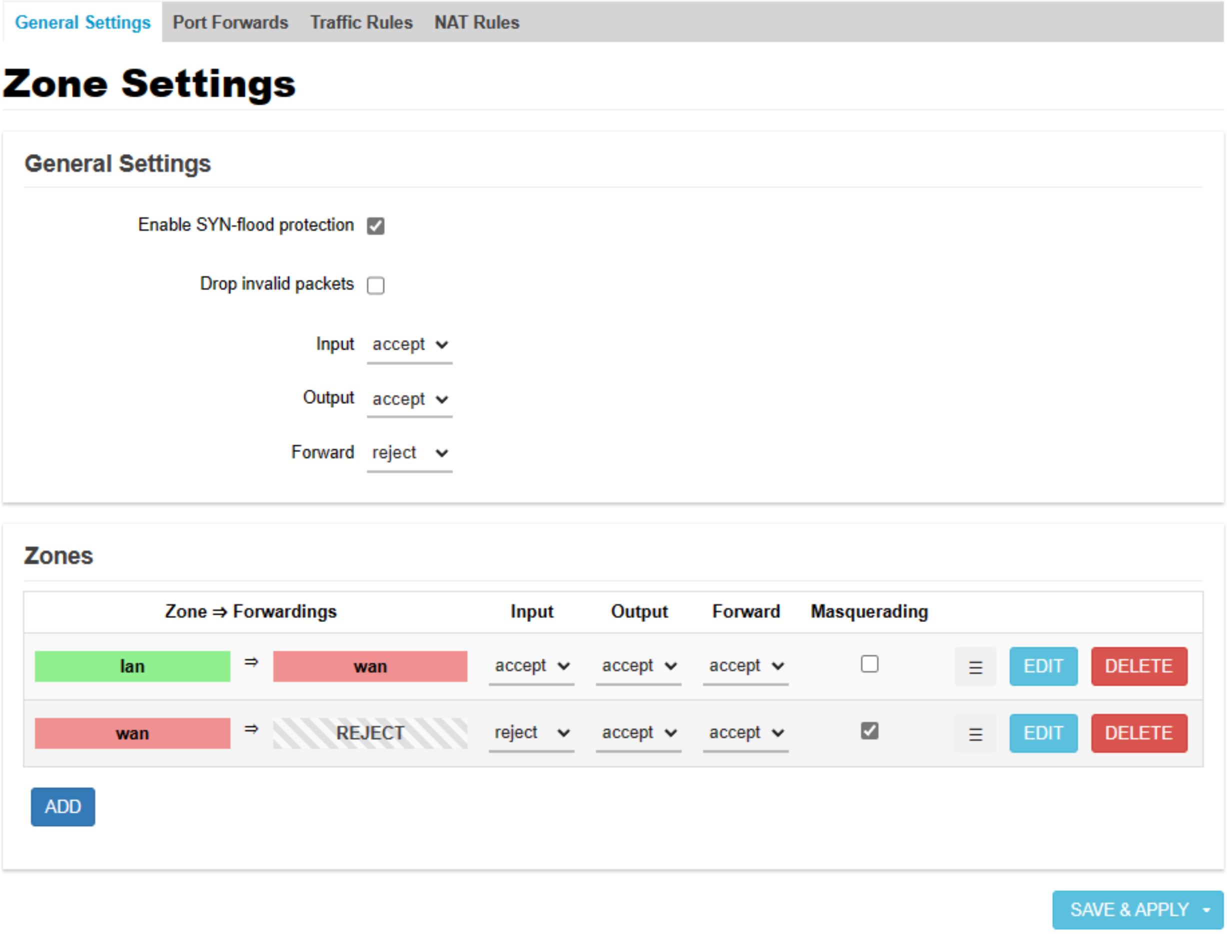
Key Components of 8355P 5G CPE Firewall

Zones: Organized interfaces into zones to manage how traffic is treated between different networks. Common zones include LAN (local area network), WAN (wide area network), and sometimes DMZ (demilitarized zone). Rules can specify what traffic is allowed between zones.

Port Forwards: A form of DNAT, this allows external devices to connect to a specific service within the LAN by forwarding the required ports.

Traffic Rules: These are specific instructions that dictate how packets should be handled. Rules can allow or block certain types of traffic based on various criteria like IP addresses, port numbers, protocols, and more.

NAT Rules (Network Address Translation): This is crucial for routers to allow multiple devices to share a single public IP address. NAT rules dictate how addresses and ports are translated, with SNAT (Source NAT) and DNAT (Destination NAT) being commonly used configurations.



Zone Settings

General Settings

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

Output: accept

Forward: reject

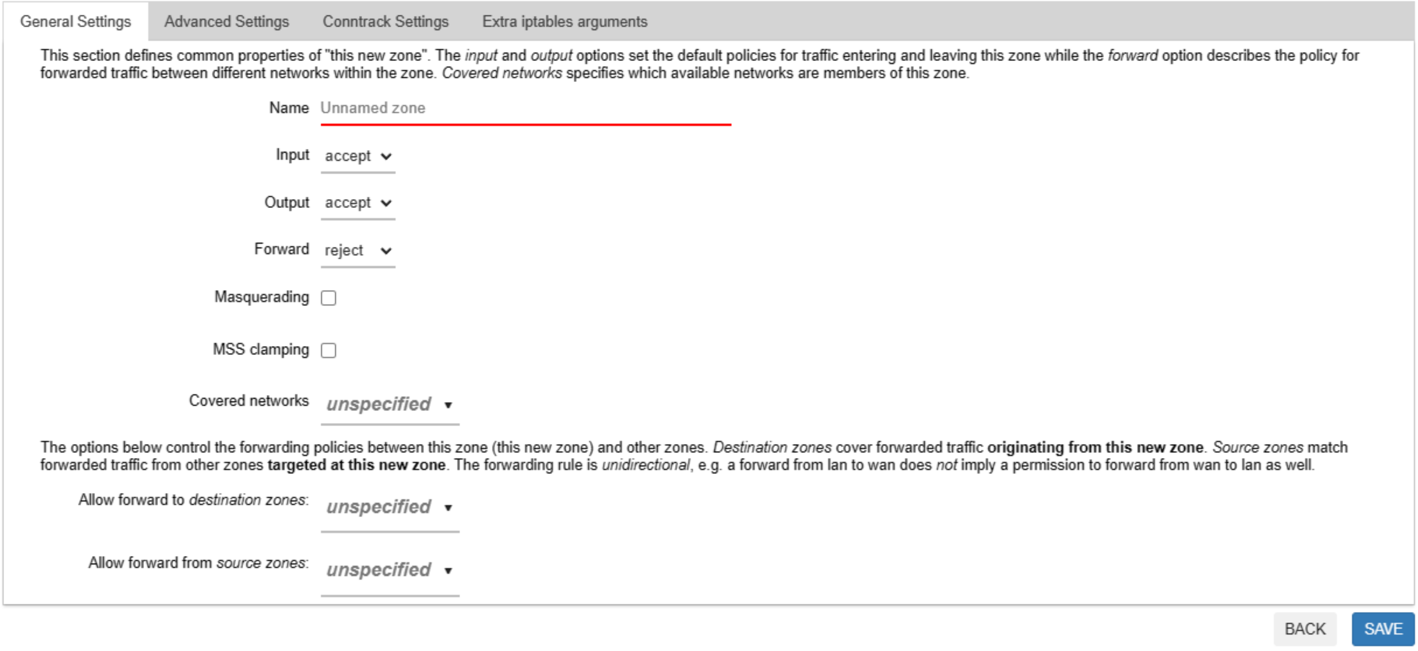
Zones

Zone ⇒ Forwardings			Input	Output	Forward	Masquerading			
lan	⇒	wan	accept	accept	accept	☐	≡	EDIT	DELETE
wan	⇒	REJECT	reject	accept	accept	☑	≡	EDIT	DELETE

To add a new zone, select the ADD button.

General Settings

This section defines common properties of "this new zone". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specify which available networks are members of this zone.



This section defines common properties of "this new zone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name: Unnamed zone

Input: accept

Output: accept

Forward: reject

Masquerading □

MSS clamping □

Covered networks: *unspecified*

The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic **originating from this new zone**. *Source zones* match forwarded traffic from other zones **targeted at this new zone**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*: *unspecified*

Allow forward from *source zones*: *unspecified*

Name: This is the identifier used for a firewall zone or rule. It helps in managing and referencing specific sections within the firewall configuration. Each zone or rule should have a unique name that describes its function or the interfaces it covers (e.g., LAN, WAN, DMZ).

Input: Controls how incoming traffic to the firewall itself is handled. This setting is crucial for protecting the router from unauthorized access. Options typically include:

- **Accept**: The firewall will accept incoming packets.
- **Reject:** The firewall will refuse incoming packets and send an error response to the sender.
- **Drop:** The firewall will silently ignore incoming packets.

Output: Controls how traffic originating from the router itself is handled.

Forward: Determines how the firewall handles traffic passing between different interfaces within the router.

Masquerading (SNAT): Dynamically assigns the router's external IP address to outgoing traffic from the internal network. It is typically used on the WAN interface to allow multiple devices on a private network to share a single public IP address.

MSS Clamping: Adjusts the "maximum segment size" of TCP packets to prevent fragmentation.

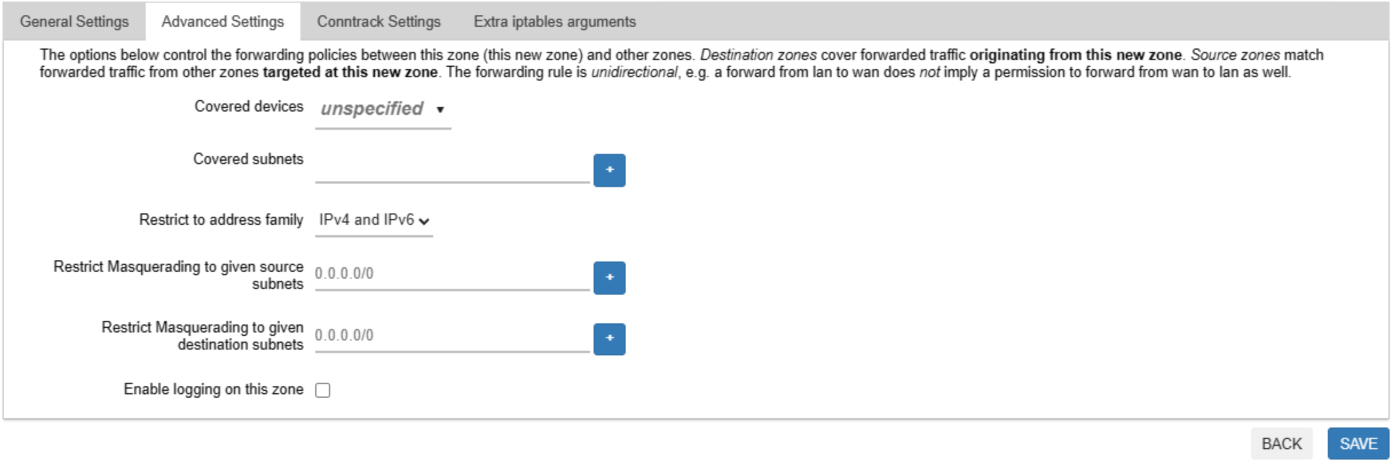
Covered Networks: This setting specifies which network interfaces are included in a particular firewall zone:

Allow Forward to Destination: Specifies which destinations (zones) can be reached from the current zone. For instance, you might allow traffic to flow from the LAN to the WAN but not to the DMZ.

Allow Forward from Source: Specifies from which sources (zones) the current zone can accept forwarded traffic. This setting is used to control incoming traffic to a zone based on its origin.

Advanced Settings

The options below control the forwarding policies between this zone (this new zone) and other zones. Destination zones cover forwarded traffic originating from this new zone. Source zones match forwarded traffic from other zones targeted at this new zone. The forwarding rule is unidirectional, e.g. a forward from LAN to WAN does not imply a permission to forward from WAN to LAN as well.



The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic **originating from this new zone**. *Source zones* match forwarded traffic from other zones **targeted at this new zone**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Covered devices: *unspecified* ▾

Covered subnets: +

Restrict to address family: IPv4 and IPv6 ⌄

Restrict Masquerading to given source subnets: 0.0.0.0/0 +

Restrict Masquerading to given destination subnets: 0.0.0.0/0 +

Enable logging on this zone: □

Covered Devices: This setting specifies which network interfaces (devices) are included in a firewall zone. For example, you might include eth0 or wlan0 as part of your LAN zone. This helps in defining the scope of the zone's rules and how they apply to the network.

Covered Subnets: While covered devices specify interfaces, covered subnets specifically relate to the IP ranges that are included within a zone. Defining covered subnets allows the firewall to apply rules to all traffic originating from or destined for these IP addresses, further refining the traffic control within zones.

Restrict to Address Family: This option allows you to specify whether the rules in a firewall zone should apply only to IPv4 or IPv6 traffic. This is useful in dual-stack environments where you might need different rules based on the type of IP traffic.

Restrict Masquerading to Given Source Subnets: Masquerading is typically used to allow machines on a private network to communicate with the external internet via a shared public IP address. This setting allows you to specify which internal IP ranges (source subnets) are allowed to use masquerading, providing a way to limit who can go out to the internet under the guise of the public IP.

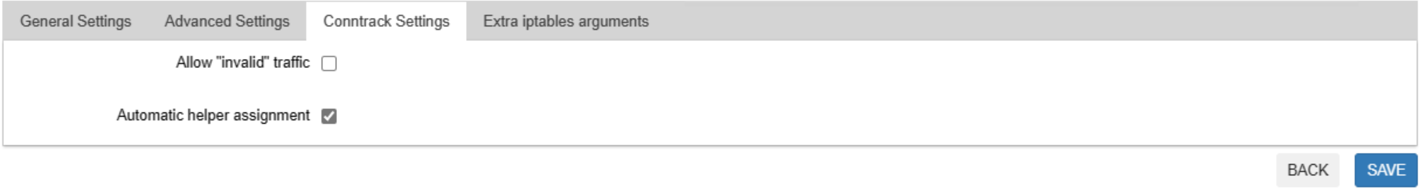
Restrict Masquerading to Given Destination Subnets: This limits masquerading to traffic directed towards specific external IP ranges (destination subnets). It’s useful for scenarios where only certain outbound traffic should appear as originating from the router’s external IP, such as directed traffic to specific external services or APIs.

Enable Logging on This Zone: Enabling this option will cause the firewall to log packets that are handled by this zone. Logging is crucial for troubleshooting and monitoring the firewall’s actions, helping administrators understand traffic flows and identify potential security issues.

Conntrack Settings

Connection tracking (conntrack) settings are part of the firewall's configuration that manage how the router tracks the state of network connections. Connection tracking is crucial for stateful packet inspection, which allows the firewall to inspect and make decisions about packets based on the context of established connections. This is used to enhance security and manage network resources more efficiently.

Connection tracking works by maintaining a table where details of each ongoing network connection are stored. This table includes information about the state of connections, such as established, new, related, or invalid. By tracking the state of connections, the firewall can apply different rules based on the connection state, such as allowing returning traffic for already established connections while blocking unwanted or unsolicited incoming connections.



Allow "invalid" traffic □

Automatic helper assignment ☑

Allow Invalid Traffic: is a setting in the firewall's configuration that determines whether packets classified as "invalid" by the connection tracking system should be allowed through the firewall.

Here's what you need to know:

- **Invalid Packets:** These are packets that the connection tracking system cannot reliably associate with any known connection. This might be due to several reasons, such as arriving out of sequence (beyond the TCP window), failing checksum tests, or simply not matching any existing connection tracking entries.

- **Security Implications**: Generally, allowing invalid packets can pose a security risk, as it could potentially allow malformed or malicious packets designed to exploit networking or application vulnerabilities. By default, most firewalls are configured to drop invalid packets.

- **Use Case**: There are some scenarios where you might need to allow invalid packets, such as when dealing with certain types of complex connections that include multi-path routing or certain VPN configurations that can lead to packet reordering or duplication.

Automatic Helper Assignment: is related to the connection tracking helpers, which are used to handle complex protocols such as FTP, TFTP, and some VoIP protocols, which require special handling because they negotiate dynamic ports within the application layer data.

- **Connection Tracking Helpers:** These are modules in the netfilter framework that inspect the application layer data to extract dynamic port information and other necessary data to maintain effective tracking and NAT traversal.

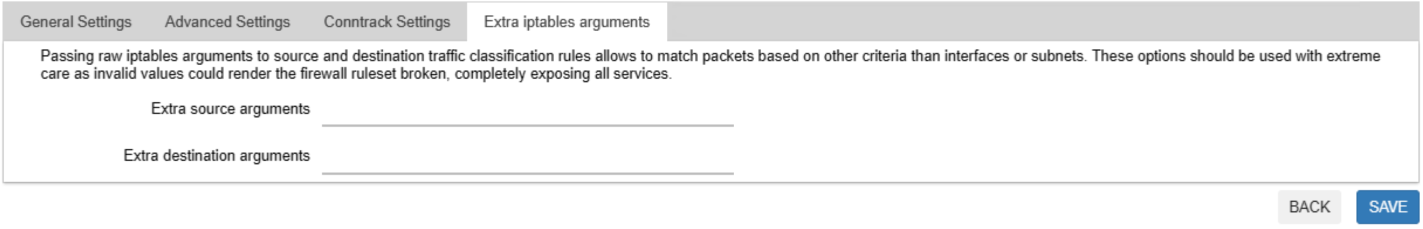
- **Automatic Helper Assignment:** In previous Linux kernels, helpers could automatically associate with connections based on inspection of the traffic (e.g., detecting an FTP connection and automatically applying the FTP helper). However, due to security concerns, newer kernel versions (since around 4.7) require explicit assignment of helpers to specific connections.

Extra iptables Arguments

Passing raw iptables arguments to source and destination traffic classification rules allows to match packets based on other criteria than interfaces or subnets. **These options should be used with extreme care as invalid values could render the firewall ruleset broken, completely exposing all services.**

Before diving into the specifics of extra arguments, it's important to understand what iptables is. Iptables is the user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel's firewall, implemented as different Netfilter modules. The rules are organized into different tables, which contain several built-in chains, and can also contain user-defined chains.

Each chain is a list of rules that can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which can be a jump to a user-defined chain or one of the special values like ACCEPT, DROP, REJECT, etc.



Passing raw iptables arguments to source and destination traffic classification rules allows to match packets based on other criteria than interfaces or subnets. These options should be used with extreme care as invalid values could render the firewall ruleset broken, completely exposing all services.

Extra source arguments

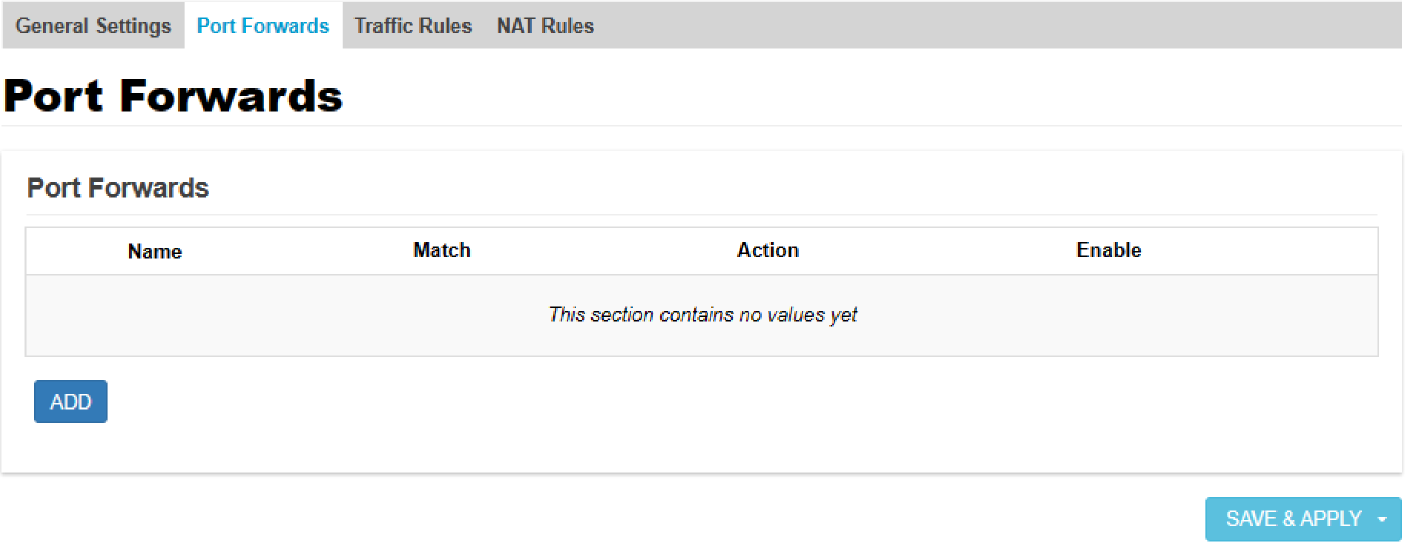
Extra destination arguments

Use Cases for Extra iptables Arguments.

Complex Matching Conditions: Such as matching packets based on specific byte counts, packet lengths, or time ranges.
Advanced NAT: Custom manipulations of packet headers.
Logging and Monitoring: Specifying custom logging options for matched packets that go beyond the basic logging provided by the 8355 5G CPE.
Rate Limiting: Implementing detailed rate limiting rules that require precise control over the match criteria.

Port Forwards

Port Forwards are rules used to redirect network traffic from one IP address and port number to another IP address and port number. This is particularly useful in NAT (Network Address Translation) configurations, which are common in home and small office network setups where multiple devices share a single public IP address. Port forwarding is essential for allowing external devices to access services hosted on your private network.



Port Forwards

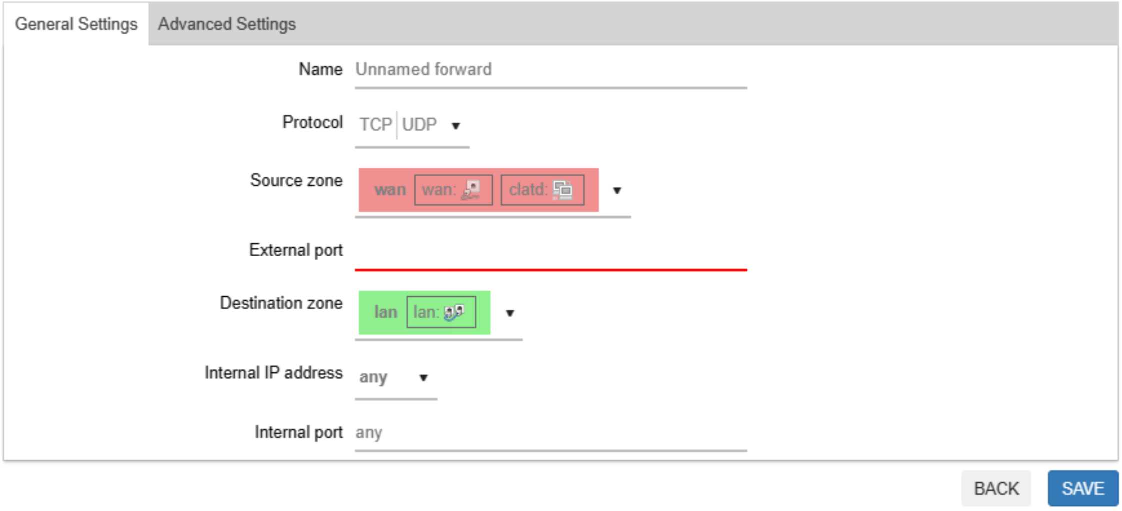
Port Forwards

Name	Match	Action	Enable
This section contains no values yet			

To add a new port forward, Click ADD

General Settings

General Setting focuses on the most common port forward configuration.



Name: Unnamed forward
Protocol: TCP UDP
Source zone: wan wan: clatd:
External port:
Destination zone: lan lan:
Internal IP address: any
Internal port: any

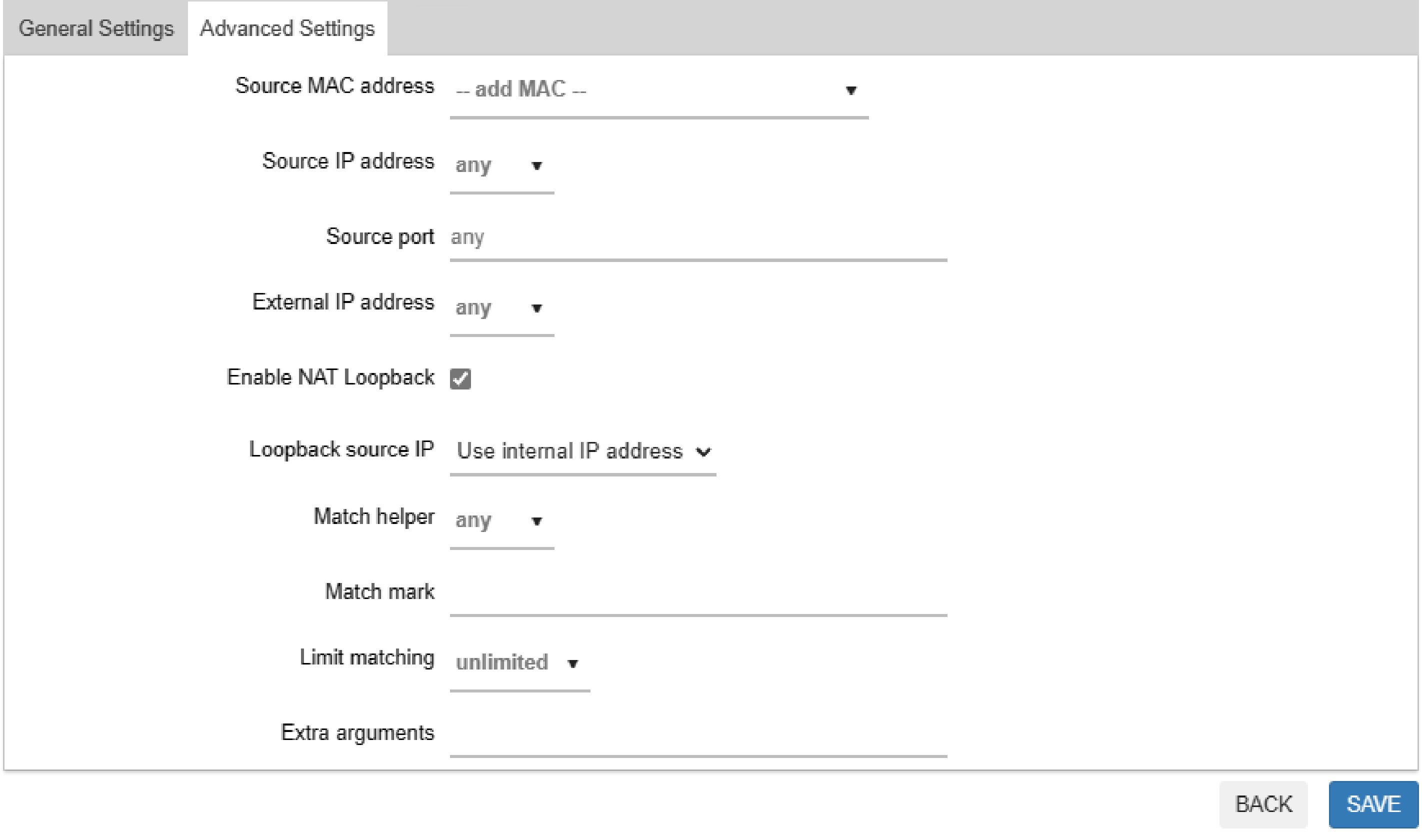
To configure General Settings:

Name: Give your rule a name that describes its purpose, such as "Web Server" or "Game Server".
Protocol: Choose the protocol (TCP, UDP, or TCP+UDP) depending on the application.
Source Zone: This is typically set to "WAN" as you are forwarding ports from the internet.
External Port: Enter the port number on the WAN side that you want to forward. This is the port that external users will connect to.
Destination Zone: Usually set to "LAN" since you are forwarding traffic to a device inside your network.
Internal IP Address: Specify the IP address of the device in your LAN that the traffic should be forwarded to. This is the device hosting the service.
Internal Port: Enter the port number on the internal device that will receive the traffic. This can be the same as the external port or different if the service is set to listen on a different port internally.

Click Save and then Save & Apply to activate the new rules.

Advanced Settings

Applying advanced settings for port forwarding rules allows you to specify a variety of parameters to fine-tune how incoming traffic is handled and directed within your network. This includes settings like Source MAC address, Source IP address, Source port, External IP address, NAT Loopback, and Loopback source IP.



Source MAC address: -- add MAC --
Source IP address: any
Source port: any
External IP address: any
Enable NAT Loopback: ☑
Loopback source IP: Use internal IP address
Match helper: any
Match mark:
Limit matching: unlimited
Extra arguments:

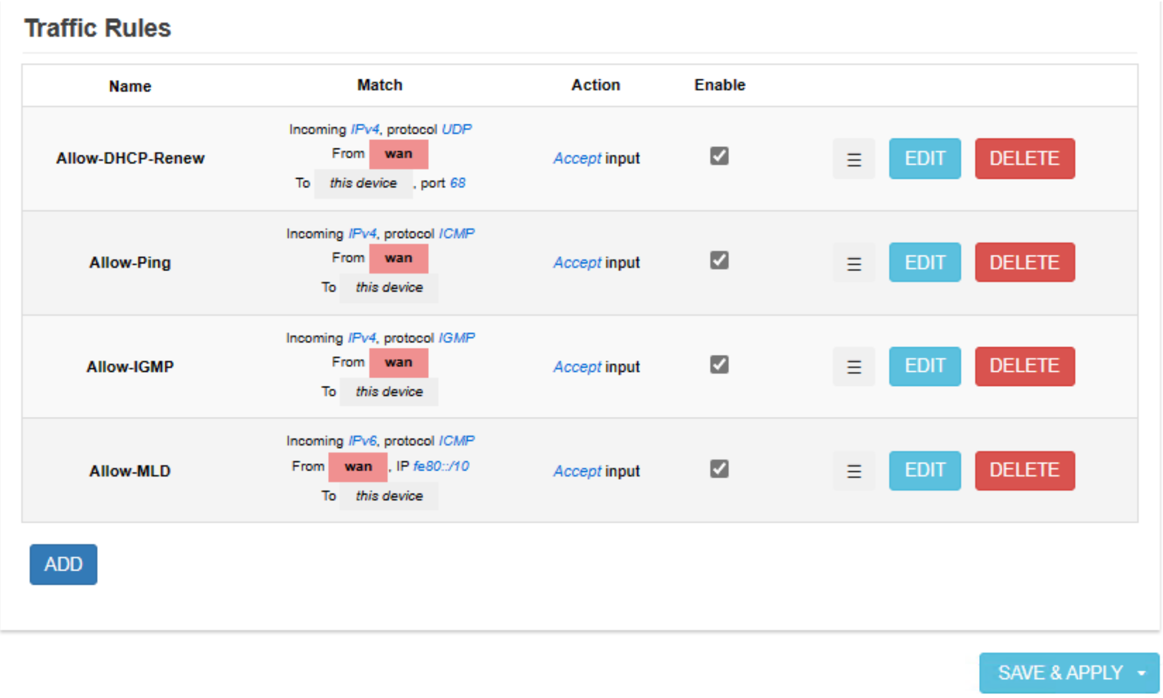
To configure Advanced Settings

Source MAC Address: Select MAC address from which incoming traffic originates.
Source IP Address: Select IP address that the incoming traffic must originate from.
Source Port: Specify the originating port on the external device.
External IP Address: If your WAN interface has multiple IP addresses, you can specify which IP address the rule should apply to.
Enable NAT Loopback: Enable this option to allow devices within your LAN to access the forwarded service using the WAN IP address.
Loopback Source IP: This setting specifies the source IP address that the internal clients will appear to come from when they are accessing the forwarded service via the WAN IP.
Match Helper: Select the specific types of connections traffic, such as FTP or PPTP, etc.
Match Mask: Specify a range of IP addresses based on a subnet mask.
Limit Matching: Limit the rate at which a rule can match (e.g., unlimited, sec, minute, custom)
Extra Arguments: Additional arguments for more complex matching or action behaviors.

Click Save and then Save & Apply to activate the advanced settings.

Traffic Rules

Traffic rules control how data packets are handled by the firewall, enabling you to specify which types of connections should be allowed or blocked based on criteria like IP addresses, ports, and protocols. These rules are pivotal for securing your network and optimizing its performance.



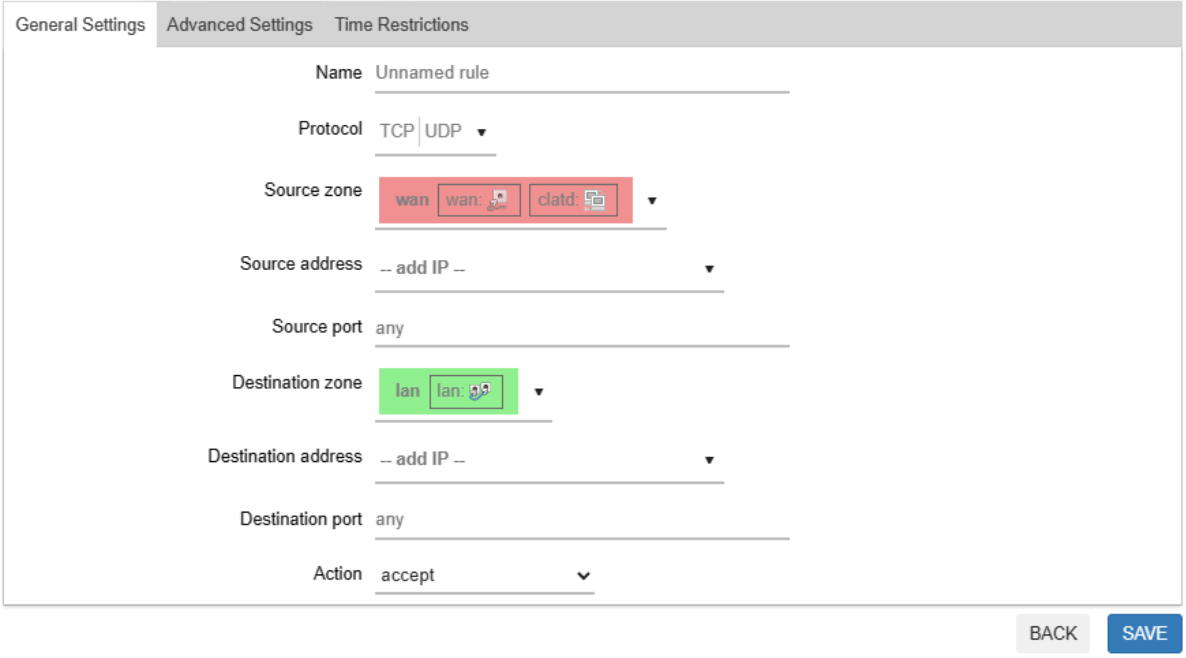
Traffic Rules

Name	Match	Action	Enable	
Allow-DHCP-Renew	Incoming *IPv4*, protocol *UDP* From wan To *this device*, port *68*	*Accept* input	☑	☰ EDIT DELETE
Allow-Ping	Incoming *IPv4*, protocol *ICMP* From wan To *this device*	*Accept* input	☑	☰ EDIT DELETE
Allow-IGMP	Incoming *IPv4*, protocol *IGMP* From wan To *this device*	*Accept* input	☑	☰ EDIT DELETE
Allow-MLD	Incoming *IPv6*, protocol *ICMP* From wan, IP *fe80::/10* To *this device*	*Accept* input	☑	☰ EDIT DELETE

To add a new traffic rule, Click ADD

General Settings

General Setting focus on the most common Traffic rules configuration:



Name: Unnamed rule
Protocol: TCP UDP
Source zone: wan wan: clatd:
Source address: -- add IP --
Source port: any
Destination zone: lan lan:
Destination address: -- add IP --
Destination port: any
Action: accept

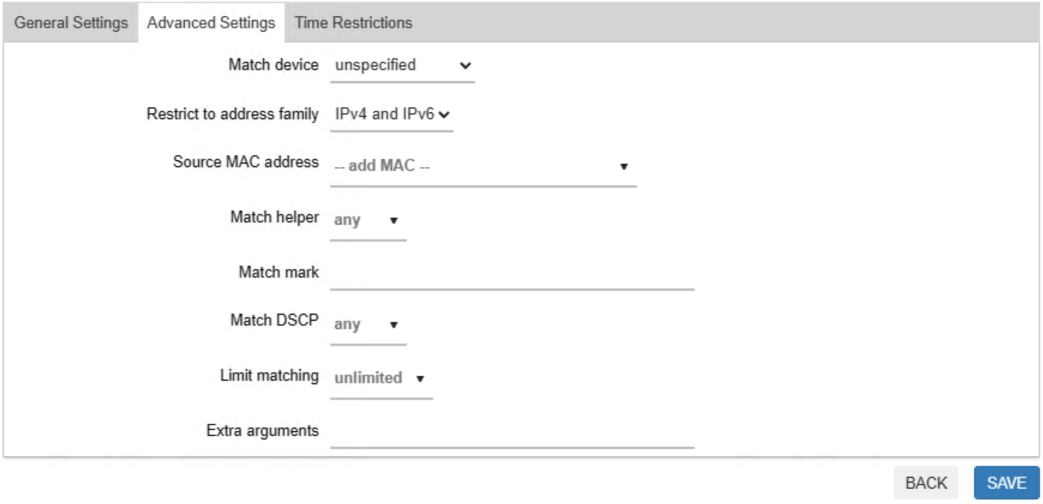
To configure General Settings:

Name: A descriptive name for the rule, which helps you identify it in the list.
Protocol: Specifies the protocol (TCP, UDP, ICMP, etc.) the rule will apply to.
Source Zone: Indicates the network zone from which the traffic originates, such as 'lan' or 'wan'.
Source Address/Port: Optionally specify an IP address and port number for the traffic originating source.
Destination Zone: Indicates the network zone where the traffic is going, such as 'wan', 'lan', or a specific VPN interface.
Destination Address/Port: Optionally specify an IP address and port number for the traffic destination.
Action: What to do when the conditions are met. Typical actions include 'Accept', 'Reject', or 'Drop'.

Click Save and then Save & Apply to activate the new traffic rules.

Advanced Settings

Applying advanced settings for traffic rules allows for granular control over the network traffic, enabling you to specify detailed conditions and actions that affect how packets are processed by the firewall.



Match device: unspecified
Restrict to address family: IPv4 and IPv6
Source MAC address: -- add MAC --
Match helper: any
Match mark
Match DSCP: any
Limit matching: unlimited
Extra arguments

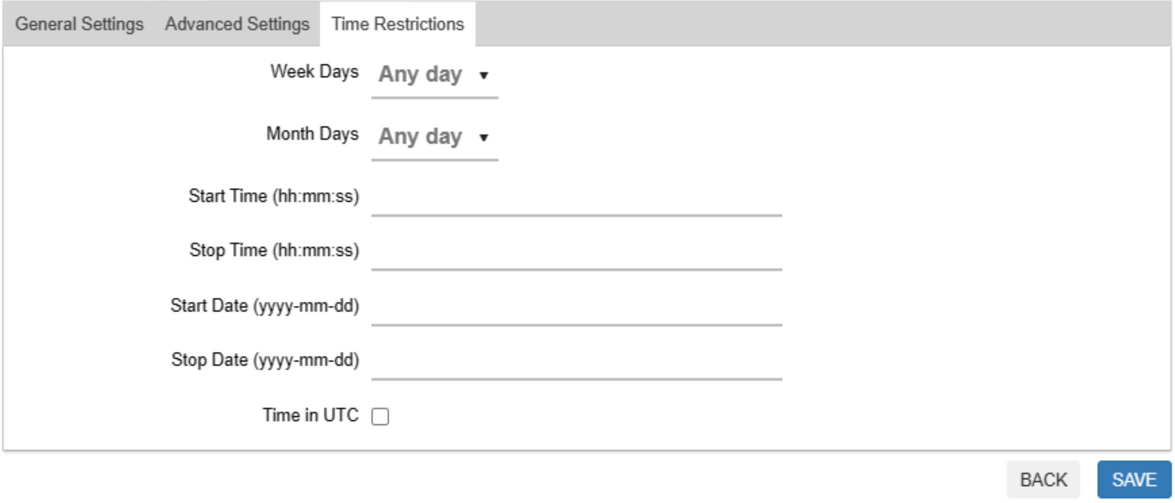
To configure Advanced Settings

Match Device: Apply traffic rules to packets coming to device inbound or outbound.
Restrict to Address Family: Restrict traffic rules to a specific address family: IPv4, IPv6 or both.
Source MAC Address: Select the MAC address of the device generating the traffic.
Match Helper: Select the specific types of connections traffic, such as FTP or PPTP, etc.
Match Mask: Specify a range of IP addresses based on a subnet mask.
Match DSCP: Match DSCP value to ensure useful for QoS and where traffic prioritized.
Limit Matching: Limit the rate at which a rule can match (e.g., unlimited, sec, minute, custom)
Extra Arguments: Additional arguments for more complex matching or action behaviors.

Click Save and then Save & Apply to activate the advanced settings.

Time Restrictions

Applying advanced settings for traffic rules allows for granular control over the network traffic, enabling you to specify detailed conditions and actions that affect how packets are processed by the firewall.



Week Days: Any day ▾
Month Days: Any day ▾
Start Time (hh:mm:ss)
Stop Time (hh:mm:ss)
Start Date (yyyy-mm-dd)
Stop Date (yyyy-mm-dd)
Time in UTC □

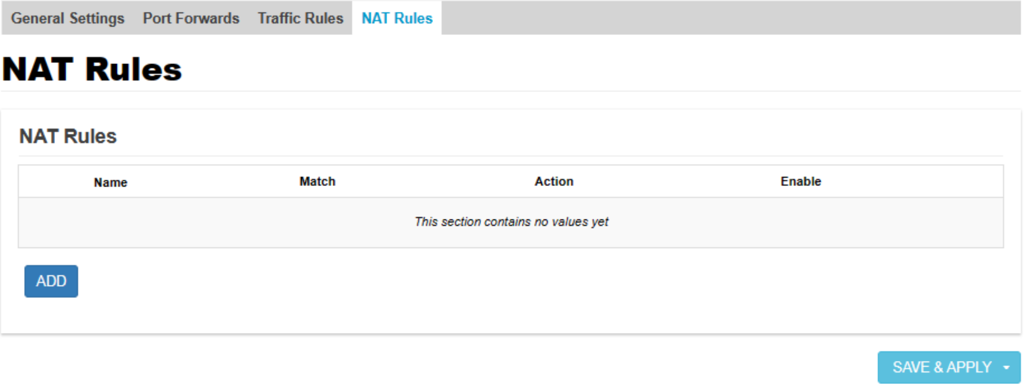
To configure Time Restrictions

Weekdays: Check the days of the week when the rule should be active.
Month Days: Enter specific days of the month (e.g., 1-15 for the first half of the month).
Start Time and Stop Time: Specify the time range during which the rule is active each day (e.g., 08:00-17:00).
Start Date and Stop Date: Enter start and end dates for the rule in the format YYYY-MM-DD.
Time in UTC: Ensure all time settings are in UTC if your system clock is set to UTC.

Click Save and then Save & Apply to activate the rules with the time constraints.

NAT Rules

Network Address Translation (NAT) rules are essential for managing how devices on your local network interact with the internet. NAT modifies the IP address information in IP packet headers while they are in transit across a traffic routing device. This is primarily used to enable multiple devices on a private network to access the internet using a single public IP address.



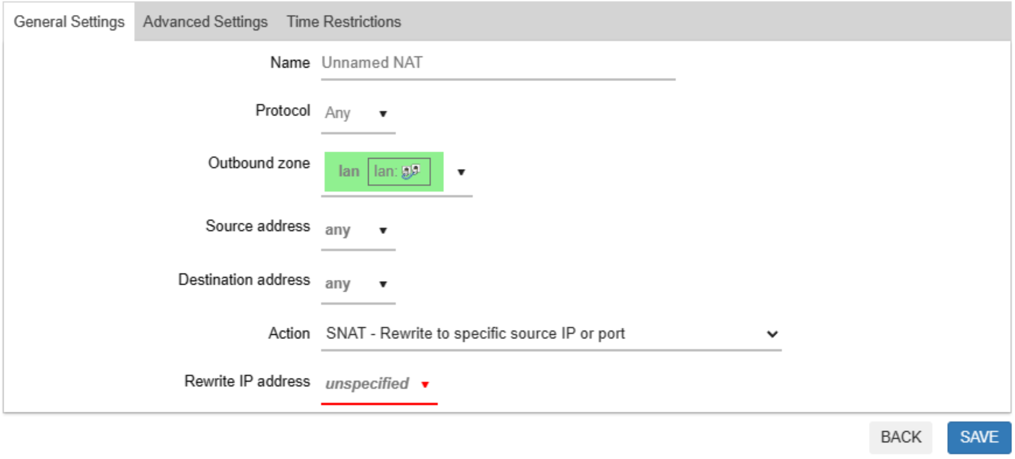
NAT Rules

NAT Rules

Name	Match	Action	Enable
This section contains no values yet			

General Settings

General Setting focus on the most common NAT configurations: Protocol, Zone, Source/Destination IP and Action.



Name	Unnamed NAT
Protocol	Any
Outbound zone	lan lan:
Source address	any
Destination address	any
Action	SNAT - Rewrite to specific source IP or port
Rewrite IP address	*unspecified*

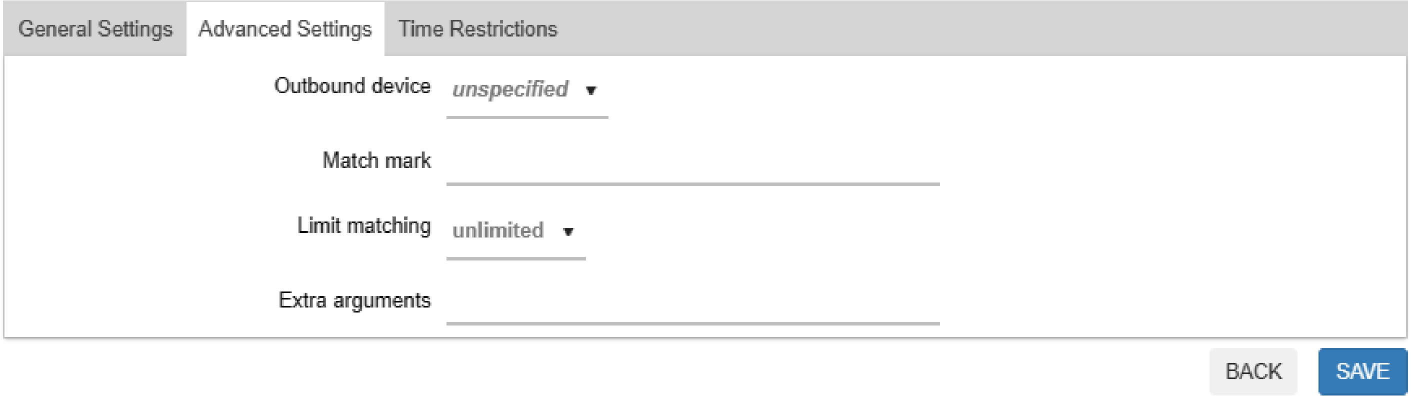
Click on Add to create a new NAT rule. Fill in the necessary fields:

Name: Give the rule a descriptive name.
Protocol: Typically, TCP or UDP depending on your application.
Outbound Zone: Usually set to 'WAN' for incoming internet connections.
Source/Destination Address: Define specific IPs if the rule should only apply to certain devices.
Action: Select desired action (SNAT, Masquerade or Accept)
SNAT: is useful for networks with multiple public IPs, where outbound traffic needs to appear to originate from a specific IP.
Masquerade: is particularly useful for networks with a dynamically changing external IP address.
Accept: simply allows specified traffic and does not involve rewriting IP addresses but is crucial for permitting certain traffic through the firewall.
Rewrite IP Address: Select IP address to rewrite.

Click Save and then Save & Apply to activate the rules.

Advanced Settings

Applying advanced setting allows for more precise control over how network traffic can access external resources or be accessible from the internet. These settings specify the outbound device, using a match mask, applying limit matching, and adding extra arguments to the rules.



Outbound device: *unspecified* ▾

Match mark:

Limit matching: unlimited ▾

Extra arguments:

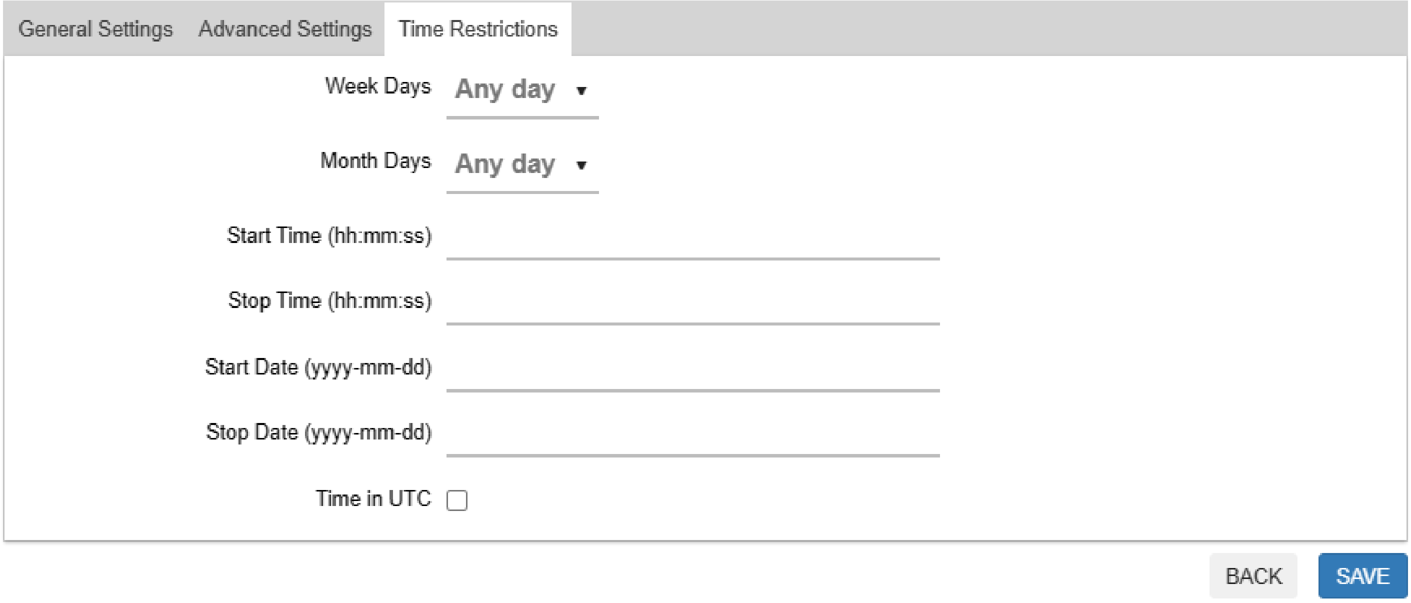
To configure Advanced Settings

Outbound Device: Specify network interface (e.g., eth0, wlan0) used for outbound traffic.
Match Mask: Specify a range of IP addresses based on a subnet mask.
Limit Matching: Limit the rate at which a rule can match (e.g., unlimited, sec, minute, custom)
Extra Arguments: Additional arguments for more complex matching or action behaviors.

Click Save and then Save & Apply to activate the advanced rules.

Time Restrictions

Applying time-based restrictions on NAT or firewall rules can be very useful for managing access control based on time criteria like specific days of the week, times of day, or even particular dates. This functionality is very helpful for implementing parental controls, business policies, or reducing network traffic during off-peak hours.



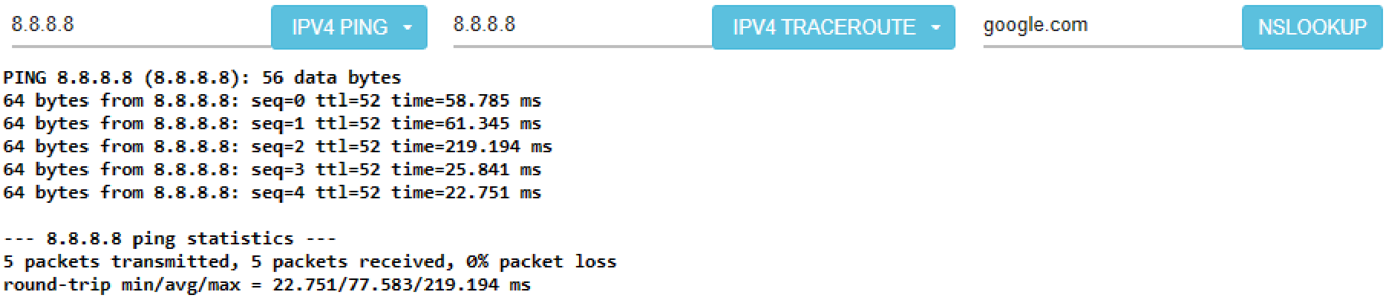
Week Days: Any day ▾
Month Days: Any day ▾
Start Time (hh:mm:ss)
Stop Time (hh:mm:ss)
Start Date (yyyy-mm-dd)
Stop Date (yyyy-mm-dd)
Time in UTC □

To configure Time Restrictions
Weekdays: Check the days of the week when the rule should be active.
Month Days: Enter specific days of the month (e.g., 1-15 for the first half of the month).
Start Time and Stop Time: Specify the time range during which the rule is active each day (e.g., 08:00-17:00).
Start Date and Stop Date: Enter start and end dates for the rule in the format YYYY-MM-DD.
Time in UTC: Ensures all time settings are in UTC if your system clock is set to UTC.

Click Save and then Save & Apply to activate the rules with the time constraints.

Diagnostics

The 8355P 5G CPE includes a range of diagnostic tools and capabilities that can help you troubleshoot network issues, monitor performance, and ensure your router and network are functioning optimally. Here’s an overview of common diagnostic tools.



```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=52 time=58.785 ms
64 bytes from 8.8.8.8: seq=1 ttl=52 time=61.345 ms
64 bytes from 8.8.8.8: seq=2 ttl=52 time=219.194 ms
64 bytes from 8.8.8.8: seq=3 ttl=52 time=25.841 ms
64 bytes from 8.8.8.8: seq=4 ttl=52 time=22.751 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 22.751/77.583/219.194 ms
```

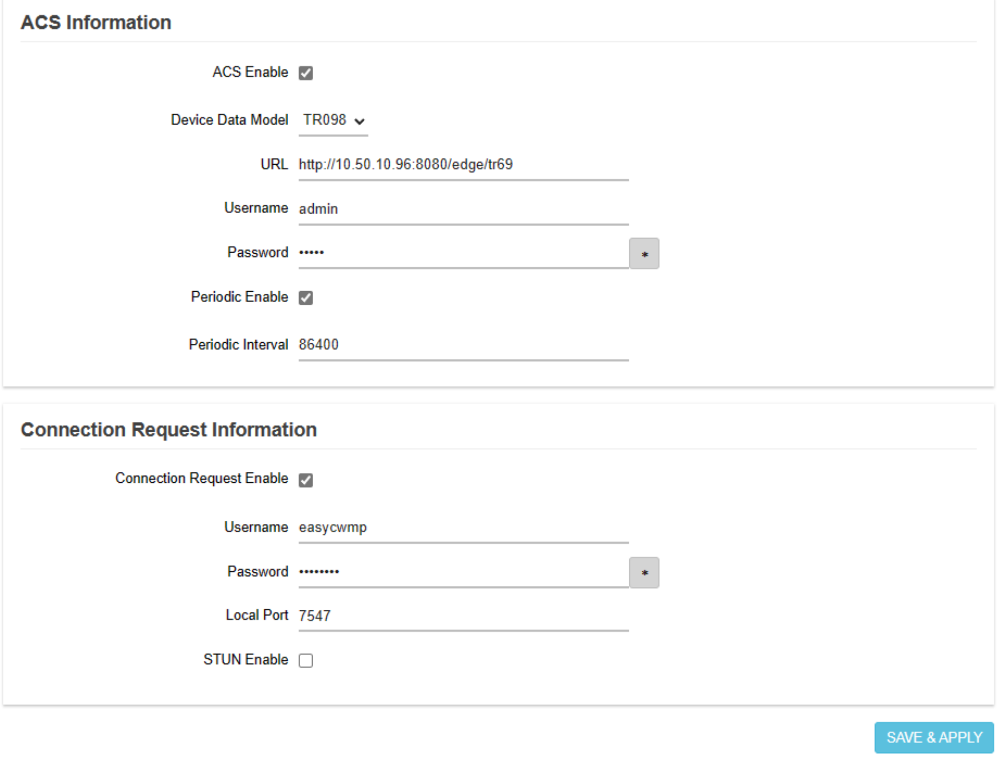
Ping: This tool allows you to test the reachability of a host on an IP network and measure the round-trip time for messages sent from your router to a destination computer. This is useful for checking if your network connection is active and how responsive it is.

Traceroute: Traceroute is used to identify the path traffic takes to reach a host. It can help diagnose routing problems and delays within the network.

NS Lookup: Tools for testing DNS resolution and latency can be crucial in diagnosing DNS-related issues affecting network connectivity.

TR-069

Technical Report 069 (TR-069) is a technical specification of the Broadband Forum that defines an application layer protocol for remote management and provisioning of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network. TR-069 uses the CPE WAN Management Protocol (CWMP) which provides support functions for auto-configuration, software or firmware image management, software management, status & performance managements, and diagnostics.



ACS Information

ACS Enable ☑
Device Data Model TR098
URL http://10.50.10.96:8080/edge/tr69
Username admin
Password •••••
Periodic Enable ☑
Periodic Interval 86400

Connection Request Information

Connection Request Enable ☑
Username easycwmp
Password ••••••••
Local Port 7547
STUN Enable □

ACS Information

ACS Enable: Select to enable.
Device Data Model: Select from TR-098 or TR-181
URL: Enter the ACS server login URL.
Username: Specify the ACS Username for ACS authentication
Password: Enter the ACS server login password.
Periodic Enable: Authorizes the 8355P 5G CPE to send an Inform message to the ACS server
Periodic Interval: Specify the inform interval time (sec) which the 8355P 5G CPE will use to periodically send inform messages to automatically connect to ACS. When the inform interval time arrives, the CPE will send an inform message to automatically connect to ACS.

Connection Request Information

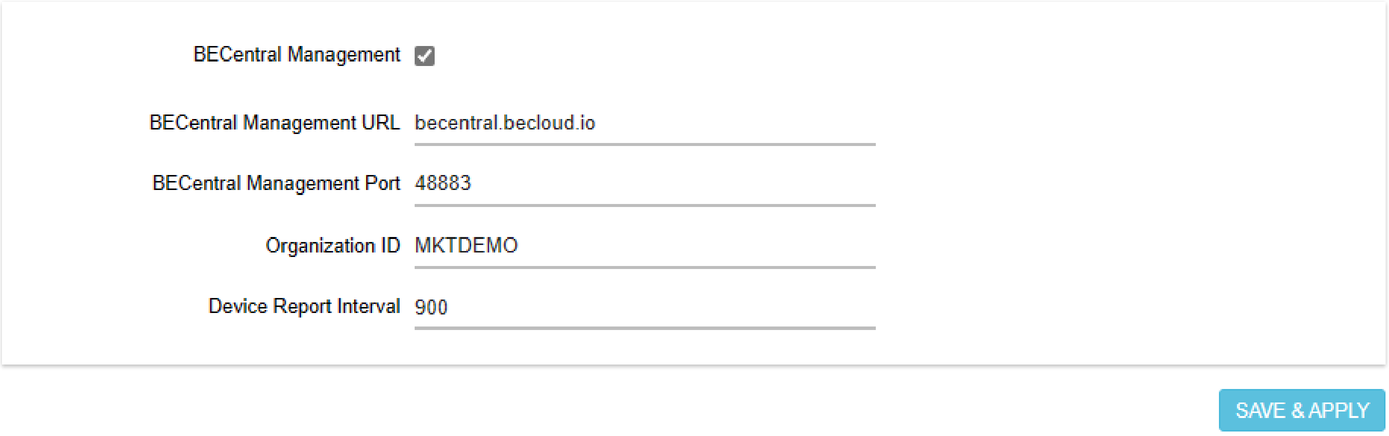
Connect Request Enable: Select to enable.
Username: Username used to authenticate an ACS making a Connection Request to the CPE.
Password: Password used to authenticate an ACS making a Connection Request to the CPE.
Local Port: Port configuration for access to server
STUN Enable: Select to enable STUN.

The STUN parameter in TR-069 indicates whether to enable the Simple Traversal of UDP through NAT (STUN) function. When this function is enabled, the endpoint can perform private-to-public network traversal using the STUN server on the TR-069 network.

Click Save & Apply to commit settings.

BECentral Management

BECentral® CloudEdge is an Industry-leading cloud-based service platform designed to accelerate LTE and 5G Wireless WAN connectivity for deployments of any scale. The platform enables zero-touch provisioning and provides visual dashboards with real-time analytics, detailed reporting, historical analysis, performance monitoring, proactive alerts/notifications, and API extensibility for 3rd party application integration. BECentral® CloudEdge is a powerful tool that provides valuable insights and essential network visibility at the edge.



BECentral Management ☑

BECentral Management URL becentral.becloud.io

BECentral Management Port 48883

Organization ID MKTDEMO

Device Report Interval 900

BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral Server

BECentral Management Port: Port listened to by the BECentral Server

Organization ID: Customer ID (for access to BECentral Server instance)

Device Report Interval: Enter the interval time in seconds to send inform message periodically to the BECentral Server

Click Save & Apply to commit 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.

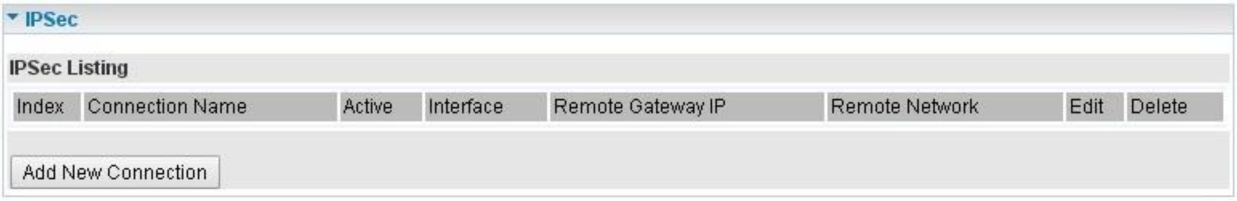
AirConnect® 8355P 5G CPE supports **IPSec, PPTP, L2TP** and **GRE**

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.



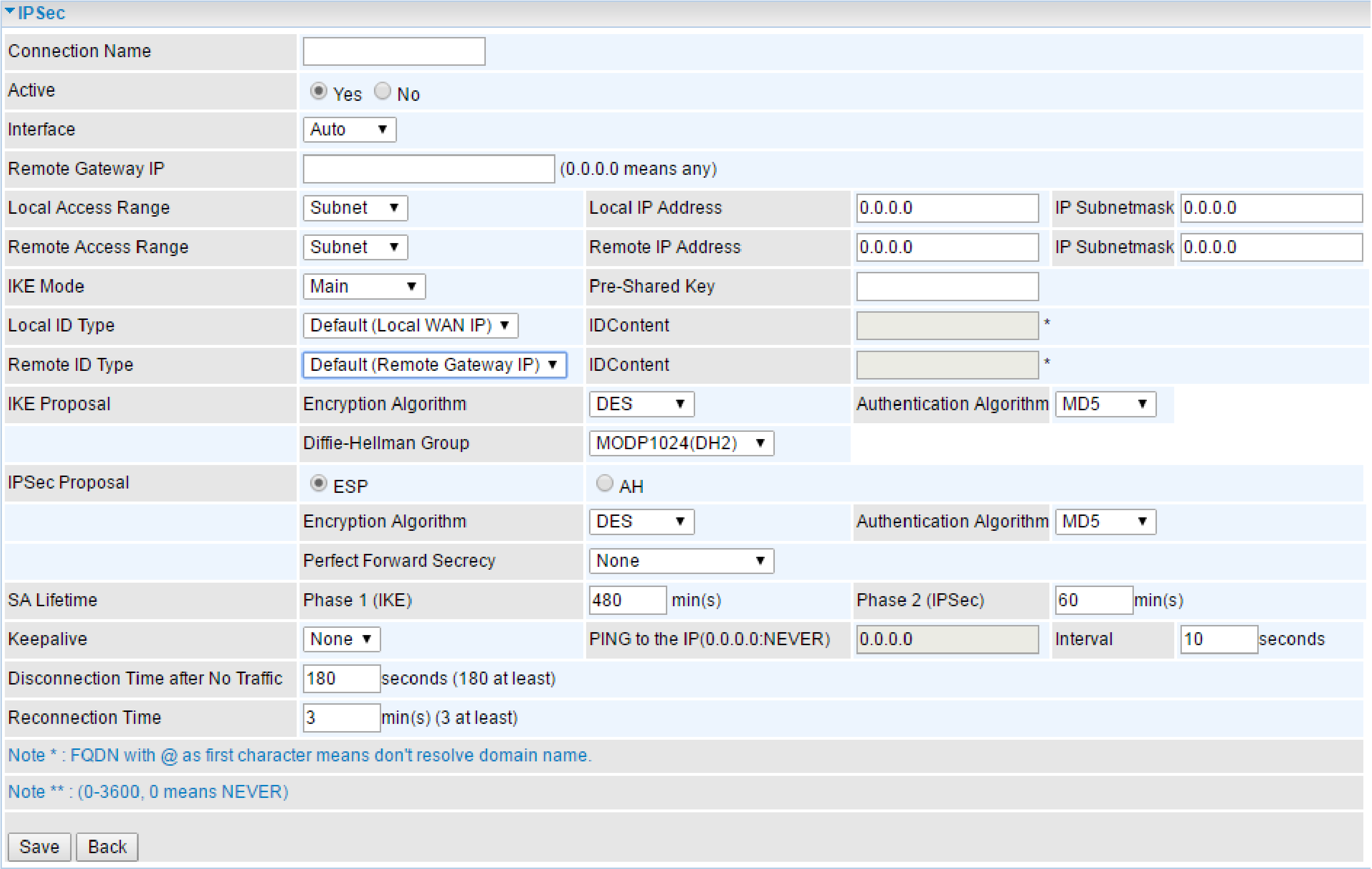
▾ IPSec

IPSec Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network	Edit	Delete

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

IPSec Connection Setting



▼IPSec

Connection Name					
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	(0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
Remote Access Range	Subnet ▼	Remote IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
IKE Mode	Main ▼	Pre-Shared Key			
Local ID Type	Default (Local WAN IP) ▼	IDContent	*		
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent	*		
IKE Proposal	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Diffie-Hellman Group	MODP1024(DH2) ▼			
IPSec Proposal	● ESP	○ AH			
	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Perfect Forward Secrecy	None ▼			
SA Lifetime	Phase 1 (IKE)	480 min(s)	Phase 2 (IPSec)	60 min(s)	
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

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

Connection Name: Enter a 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.

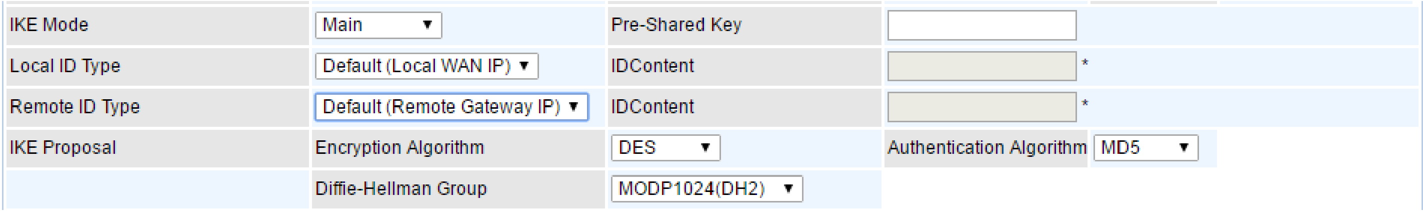
Local Access Range: Set the IP address or subnet of the local network.

- **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	Main ▾	Pre-Shared Key		
Local ID Type	Default (Local WAN IP) ▾	IDContent	*	
Remote ID Type	Default (Remote Gateway IP) ▾	IDContent	*	
IKE Proposal	Encryption Algorithm	DES ▾	Authentication Algorithm	MD5 ▾
	Diffie-Hellman Group	MODP1024(DH2) ▾		

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

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

Local ID Type / **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).

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.

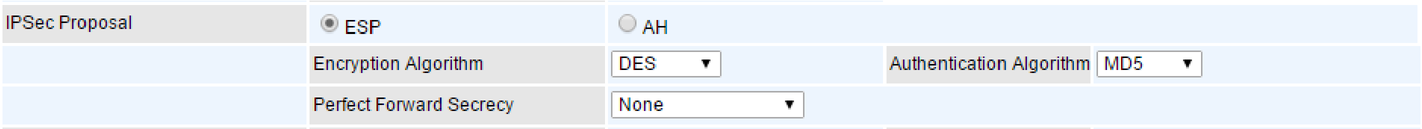
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

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	● ESP	○ AH		
	Encryption Algorithm	DES ▾	Authentication Algorithm	MD5 ▾
	Perfect Forward Secrecy	None ▾		

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.

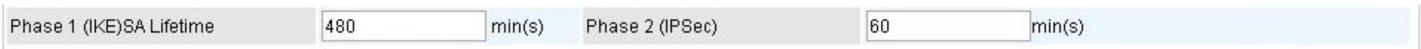
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

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

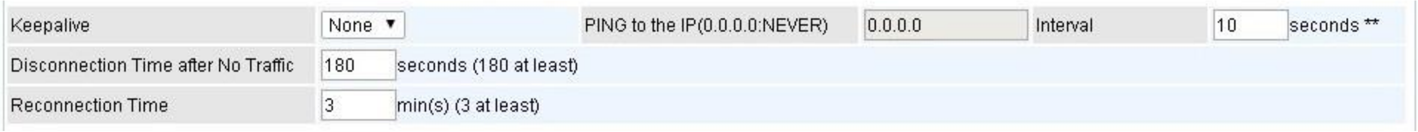


Phase 1 (IKE)SA Lifetime	480	min(s)	Phase 2 (IPSec)	60	min(s)

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



Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10	seconds **
Disconnection Time after No Traffic	180	seconds (180 at least)				
Reconnection Time	3	min(s) (3 at least)				

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.

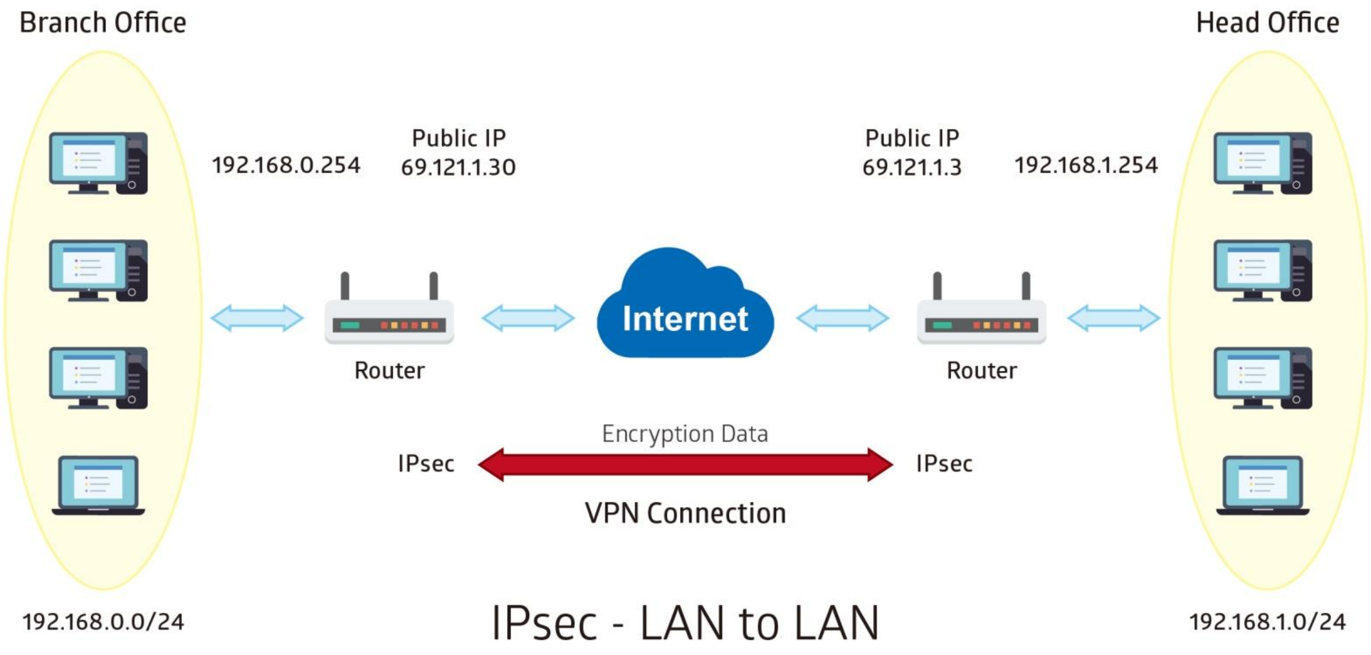
Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply settings.

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

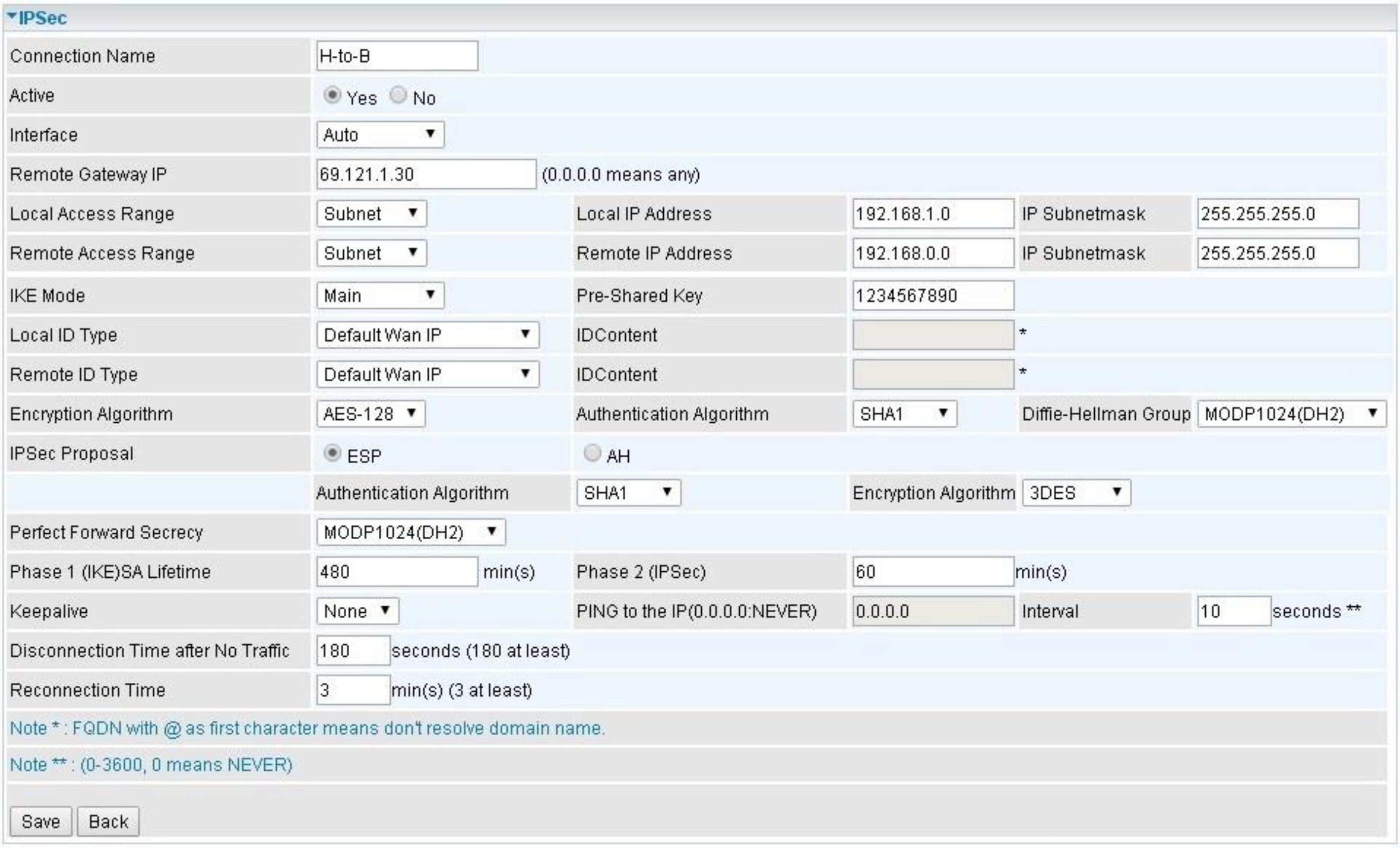
Two of the AirConnect® 8355P 5G CPE devices want to setup a secure IPSec VPN tunnel.

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)	



▾IPSec

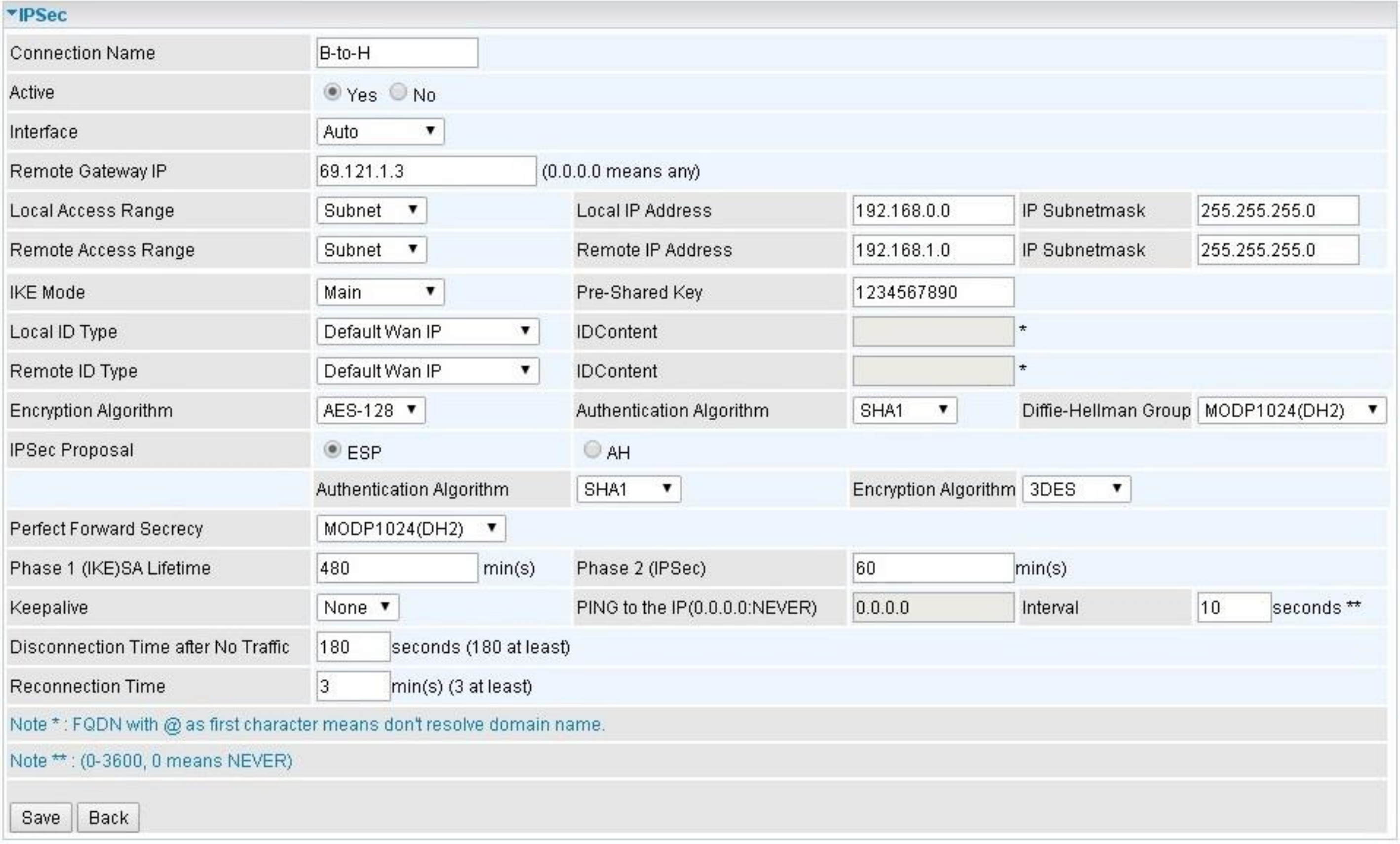
Connection Name	H-to-B				
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
Remote Access Range	Subnet ▼	Remote IP Address	192.168.0.0	IP Subnetmask	255.255.255.0
IKE Mode	Main ▼	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP ▼	IDContent	*		
Remote ID Type	Default Wan IP ▼	IDContent	*		
Encryption Algorithm	AES-128 ▼	Authentication Algorithm	SHA1 ▼	Diffie-Hellman Group	MODP1024(DH2) ▼
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1 ▼	Encryption Algorithm	3DES ▼	
Perfect Forward Secrecy	MODP1024(DH2) ▼				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

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

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)	



▾IPSec

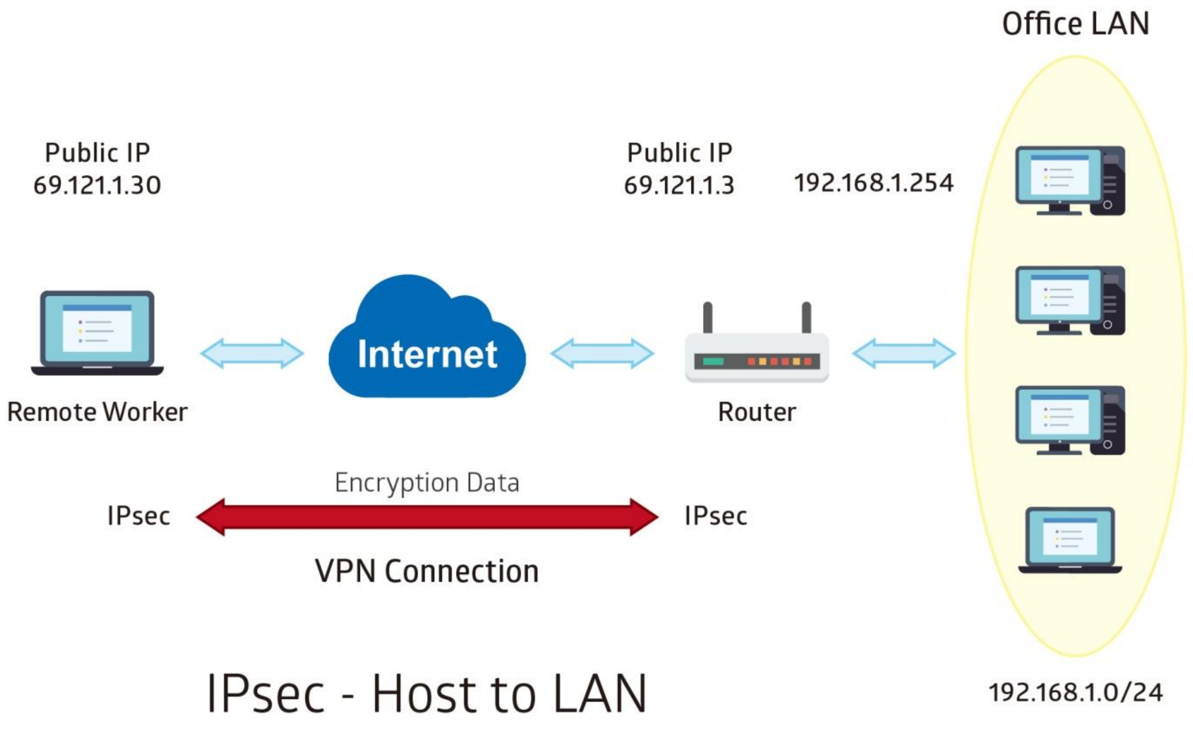
Connection Name	B-to-H				
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	69.121.1.3 (0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	192.168.0.0	IP Subnetmask	255.255.255.0
Remote Access Range	Subnet ▼	Remote IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
IKE Mode	Main ▼	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP ▼	IDContent	*		
Remote ID Type	Default Wan IP ▼	IDContent	*		
Encryption Algorithm	AES-128 ▼	Authentication Algorithm	SHA1 ▼	Diffie-Hellman Group	MODP1024(DH2) ▼
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1 ▼	Encryption Algorithm	3DES ▼	
Perfect Forward Secrecy	MODP1024(DH2) ▼				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

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

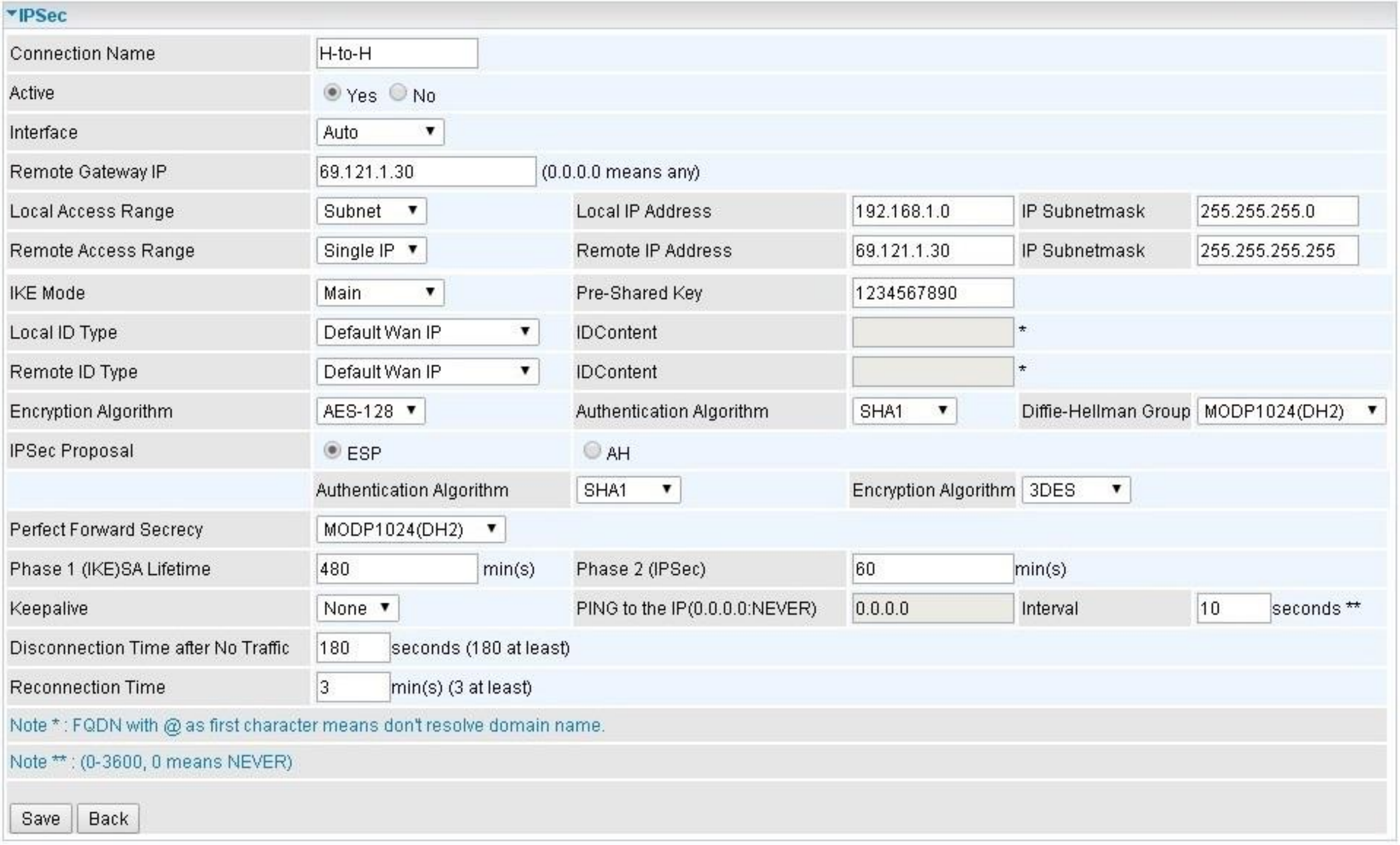
Examples: IPSec – Remote Employee to AirConnect® 8355P 5G CPEConnection

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)	



▾IPSec

Connection Name	H-to-H				
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
Remote Access Range	Single IP ▼	Remote IP Address	69.121.1.30	IP Subnetmask	255.255.255.255
IKE Mode	Main ▼	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP ▼	IDContent	*		
Remote ID Type	Default Wan IP ▼	IDContent	*		
Encryption Algorithm	AES-128 ▼	Authentication Algorithm	SHA1 ▼	Diffie-Hellman Group	MODP1024(DH2) ▼
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1 ▼	Encryption Algorithm	3DES ▼	
Perfect Forward Secrecy	MODP1024(DH2) ▼				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

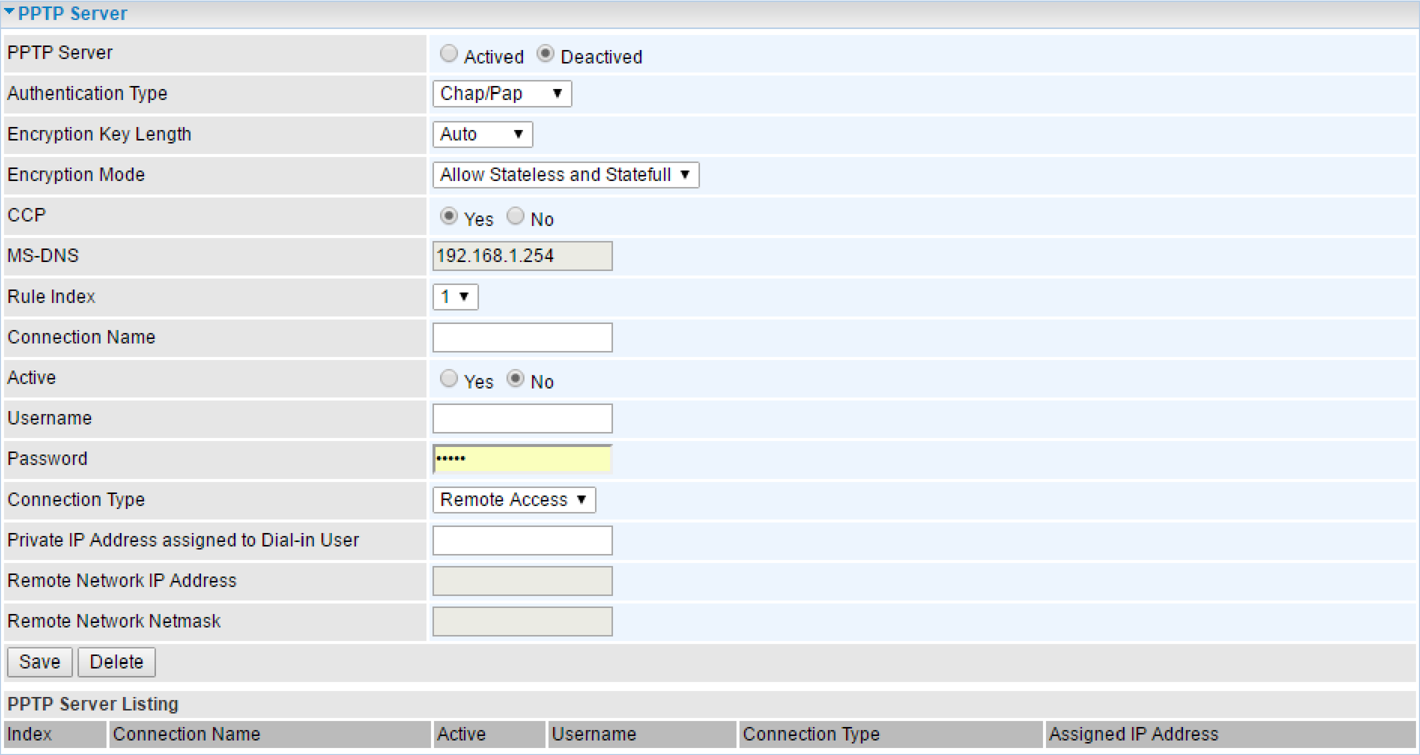
Note ** : (0-3600, 0 means NEVER)

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

PPTP Server	○ Actived ● Deactived
Authentication Type	Chap/Pap ▾
Encryption Key Length	Auto ▾
Encryption Mode	Allow Stateless and Statefull ▾
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1 ▾
Connection Name	
Active	○ Yes ● No
Username	
Password	•••••
Connection Type	Remote Access ▾
Private IP Address assigned to Dial-in User	
Remote Network IP Address	
Remote Network Netmask	

Save Delete

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address

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.

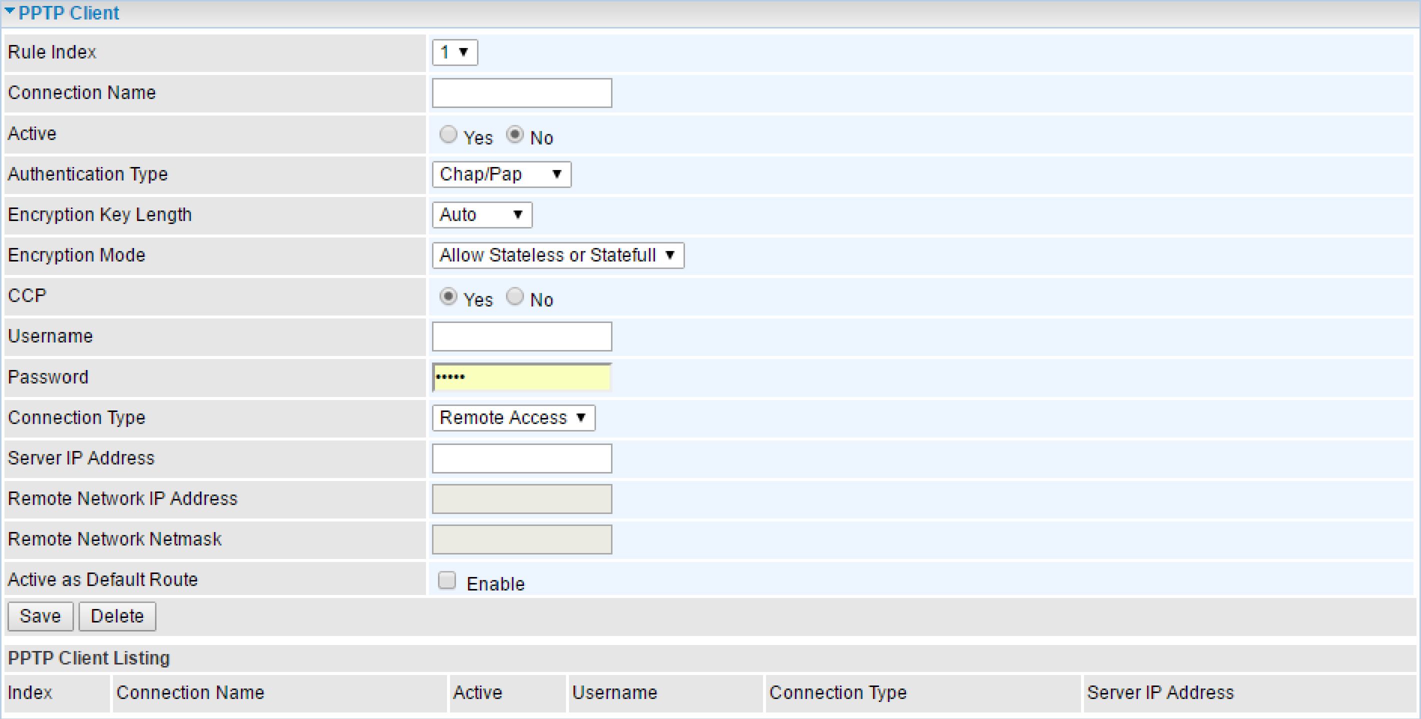
Remote Network Netmask: Enter the Netmask of the remote LAN network.

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.



PPTP Client

Rule Index	1 ▾
Connection Name	
Active	○ Yes ● No
Authentication Type	Chap/Pap ▾
Encryption Key Length	Auto ▾
Encryption Mode	Allow Stateless or Statefull ▾
CCP	● Yes ○ No
Username	
Password	•••••
Connection Type	Remote Access ▾
Server IP Address	
Remote Network IP Address	
Remote Network Netmask	
Active as Default Route	□ Enable

PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address

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.

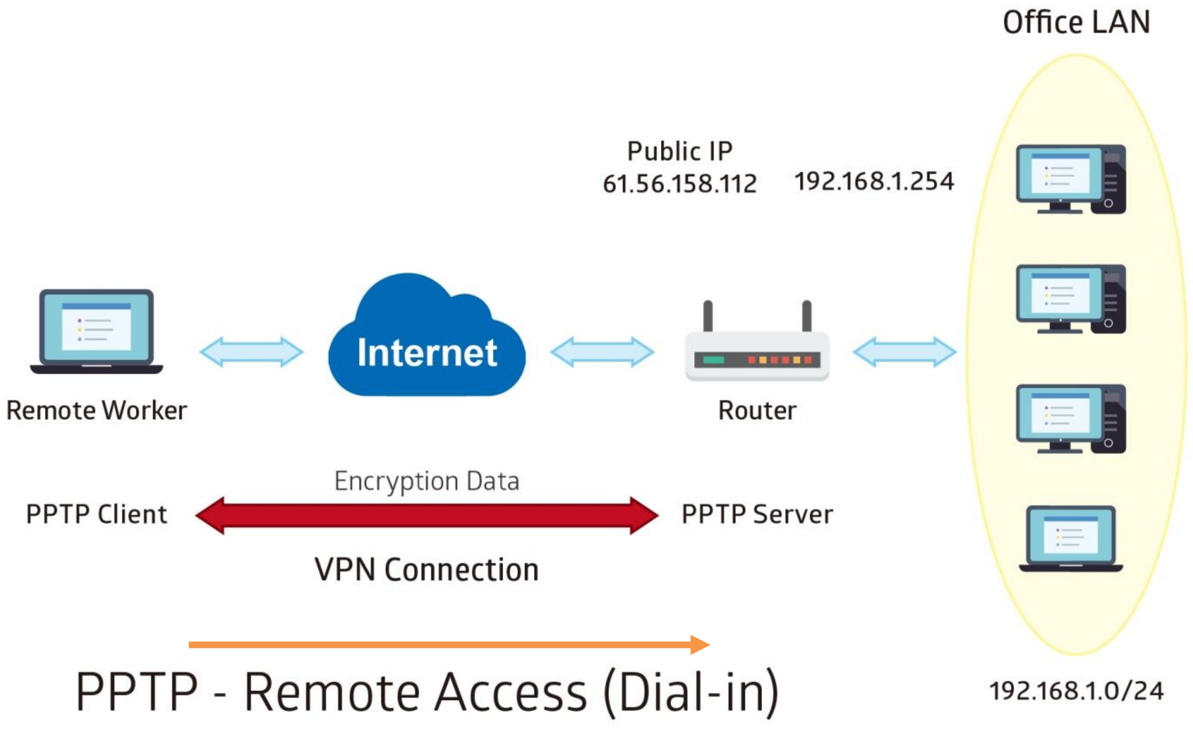
Server Address: Enter the WAN IP address of the PPTP server.

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.

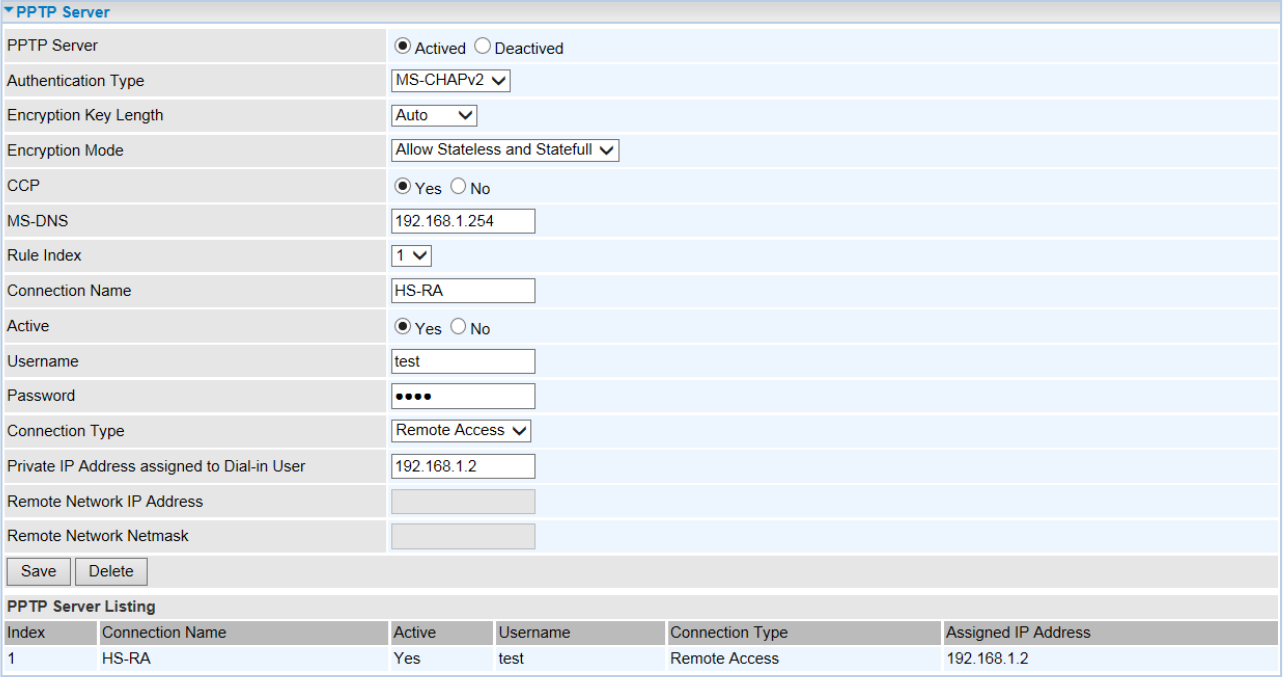
Click **Save** to apply settings.

Example: PPTP – Remote Employee Dial-in to AirConnect® 8355P 5G CPE



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



PPTP Server

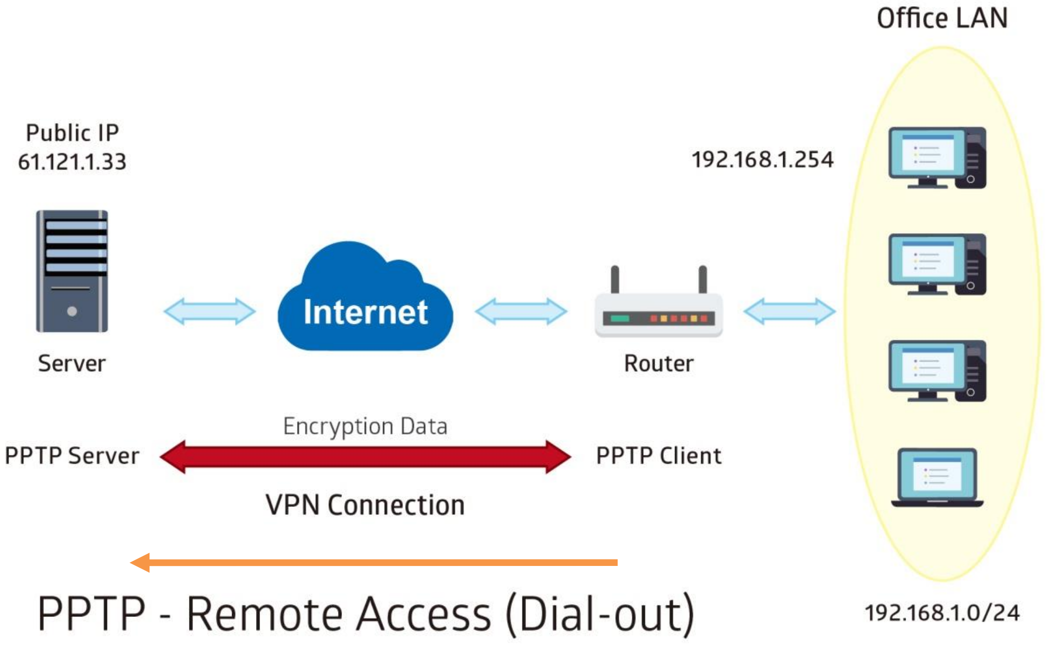
PPTP Server	● Actived ○ Deactived
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless and Statefull
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1
Connection Name	HS-RA
Active	● Yes ○ No
Username	test
Password	••••
Connection Type	Remote Access
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	
Remote Network Netmask	

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-RA	Yes	test	Remote Access	192.168.1.2

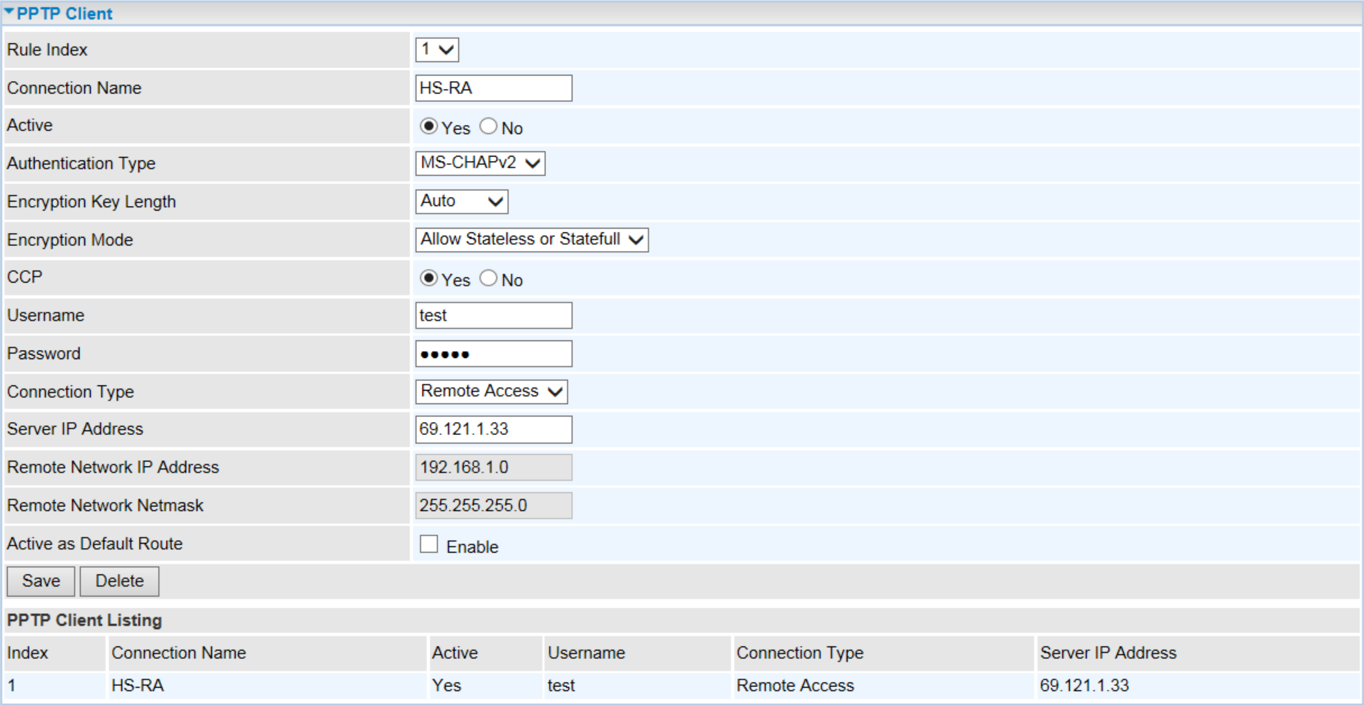
Example: PPTP – Remote Employee Dial-out to AirConnect® 8355P 5G CPE

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



PPTP Client

Rule Index	1
Connection Name	HS-RA
Active	● Yes ○ No
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless or Statefull
CCP	● Yes ○ No
Username	test
Password	•••••
Connection Type	Remote Access
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	□ Enable

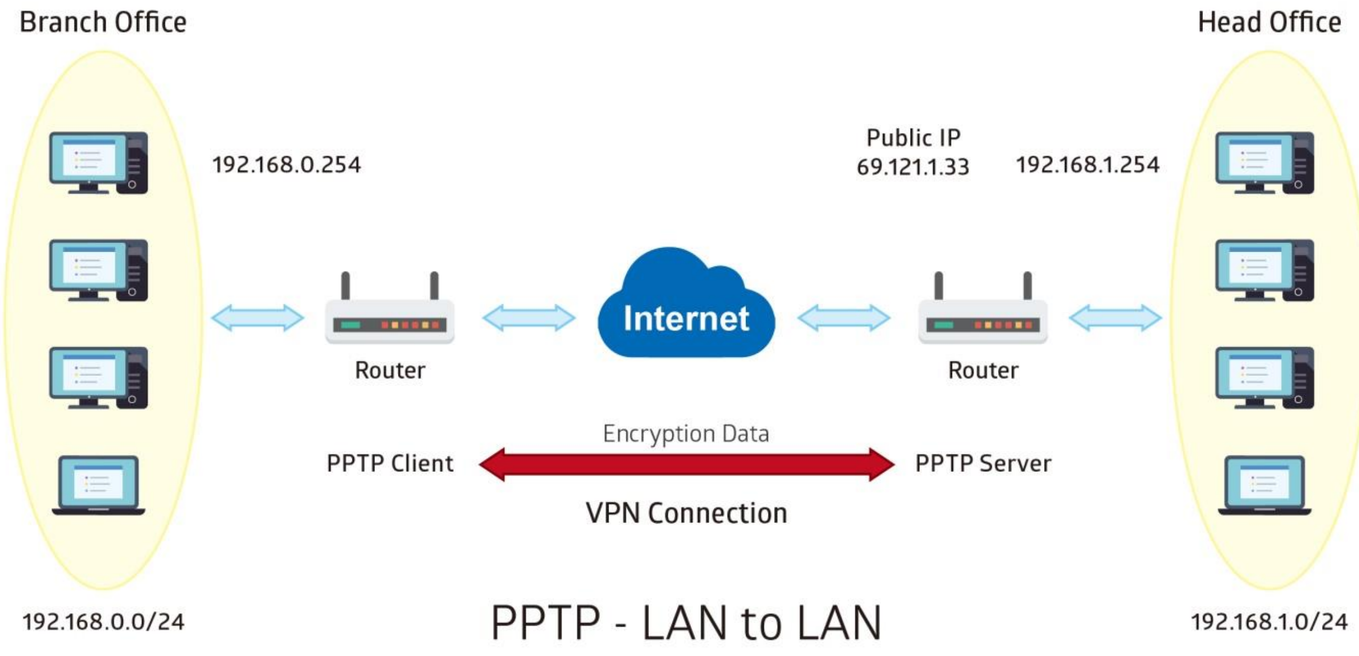
PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	HS-RA	Yes	test	Remote Access	69.121.1.33

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.

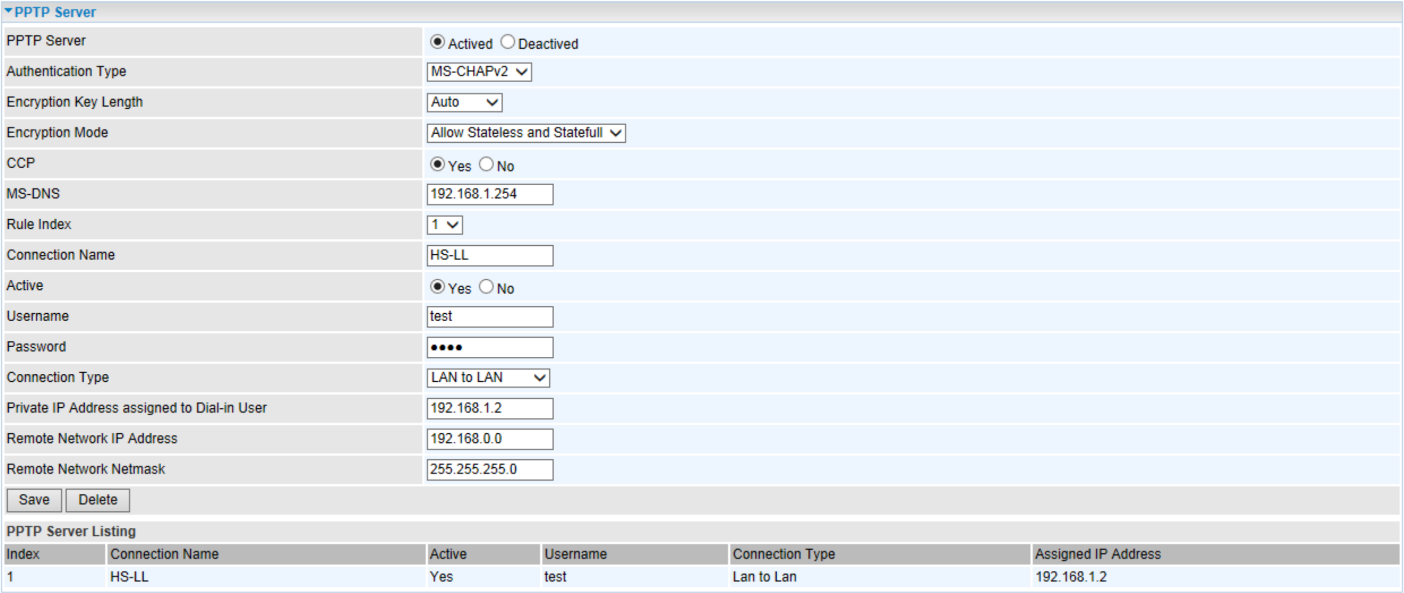
NOTE: Both office LAN networks must be in **different subnets** with the LAN-LAN application.



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	



▾PPTP Server

PPTP Server	● Actived ○ Deactived
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless and Statefull
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1
Connection Name	HS-LL
Active	● Yes ○ No
Username	test
Password	••••
Connection Type	LAN to LAN
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0

Save Delete

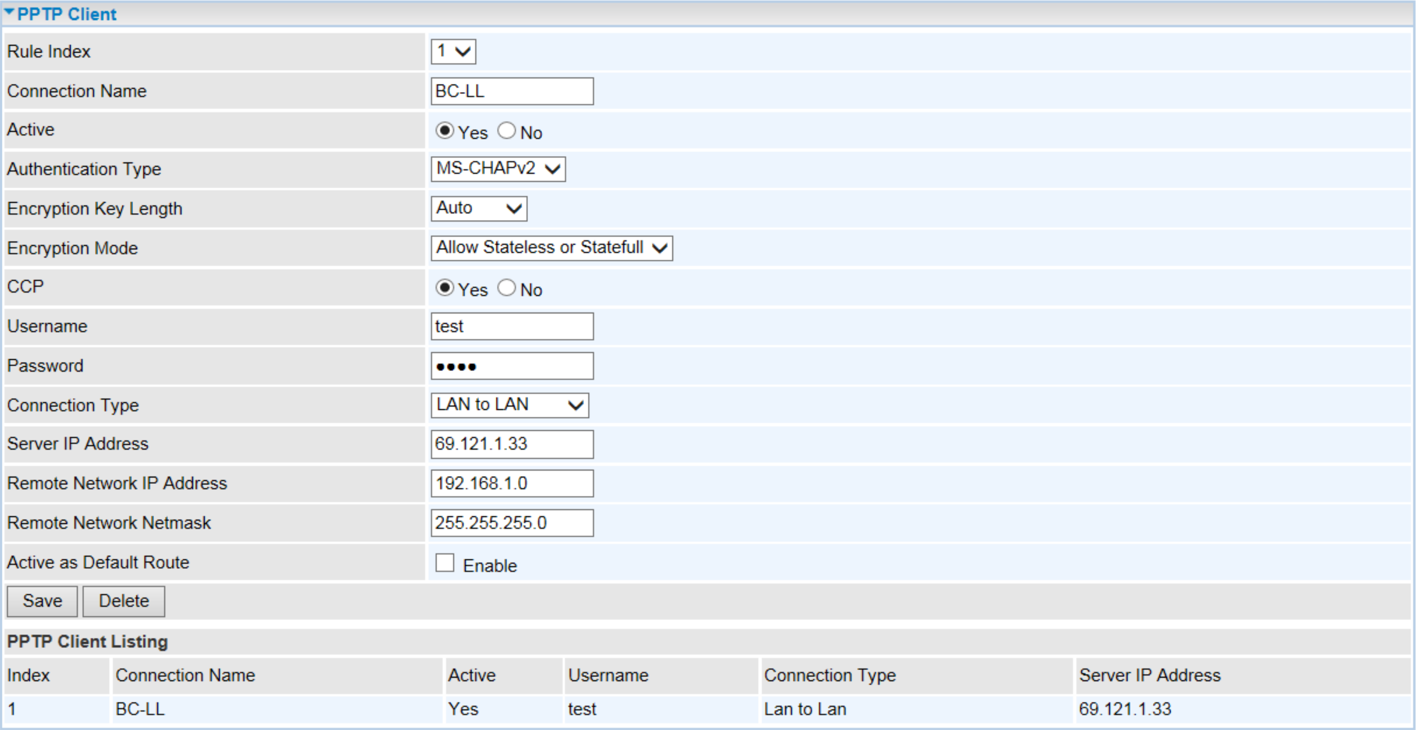
PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-LL	Yes	test	Lan to Lan	192.168.1.2

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	



▾PPTP Client

Rule Index	1
Connection Name	BC-LL
Active	● Yes ○ No
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless or Statefull
CCP	● Yes ○ No
Username	test
Password	••••
Connection Type	LAN to LAN
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	□ Enable

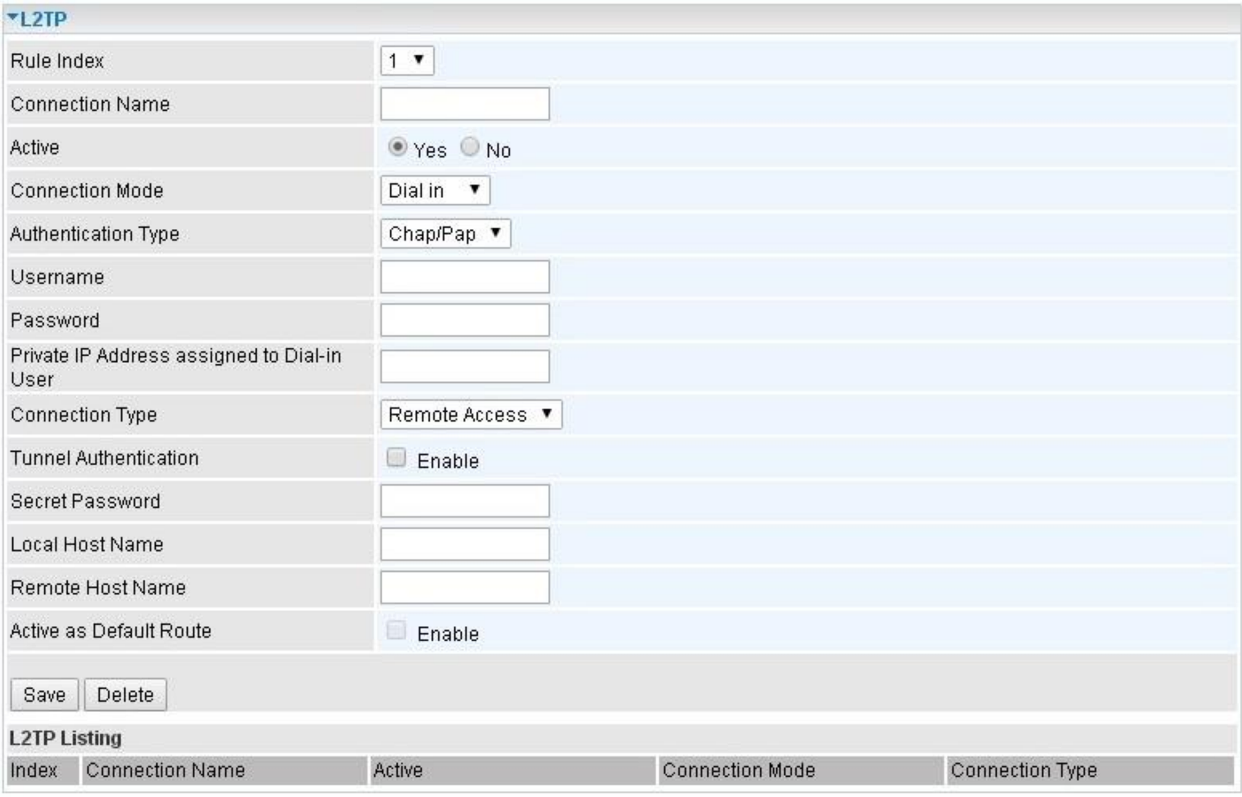
PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	BC-LL	Yes	test	Lan to Lan	69.121.1.33

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



▾L2TP

Rule Index	1 ▼
Connection Name	
Active	● Yes ○ No
Connection Mode	Dial in ▼
Authentication Type	Chap/Pap ▼
Username	
Password	
Private IP Address assigned to Dial-in User	
Connection Type	Remote Access ▼
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

L2TP Listing

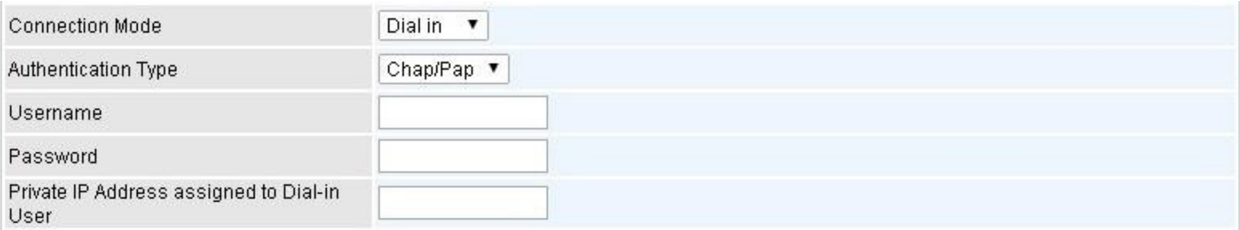
Index	Connection Name	Active	Connection Mode	Connection Type

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	Dial in ▼
Authentication Type	Chap/Pap ▼
Username	
Password	
Private IP Address assigned to Dial-in User	

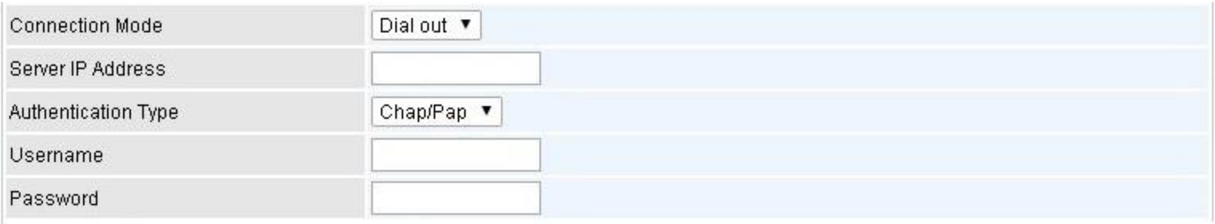
Connection Mode: Select Dial In to operate as a L2TP server.

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	Dial out ▼
Server IP Address	
Authentication Type	Chap/Pap ▼
Username	
Password	

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.

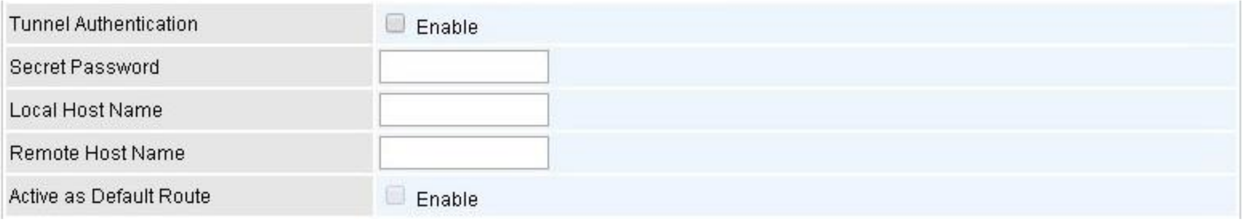
Authentication Type: Default is Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or 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	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

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.

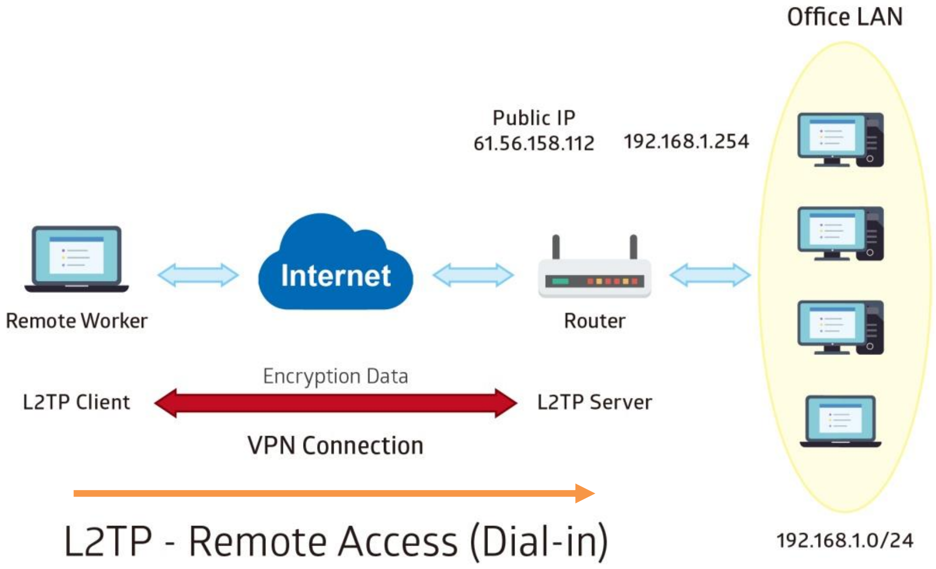
Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

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.

Click **Save** to apply settings.

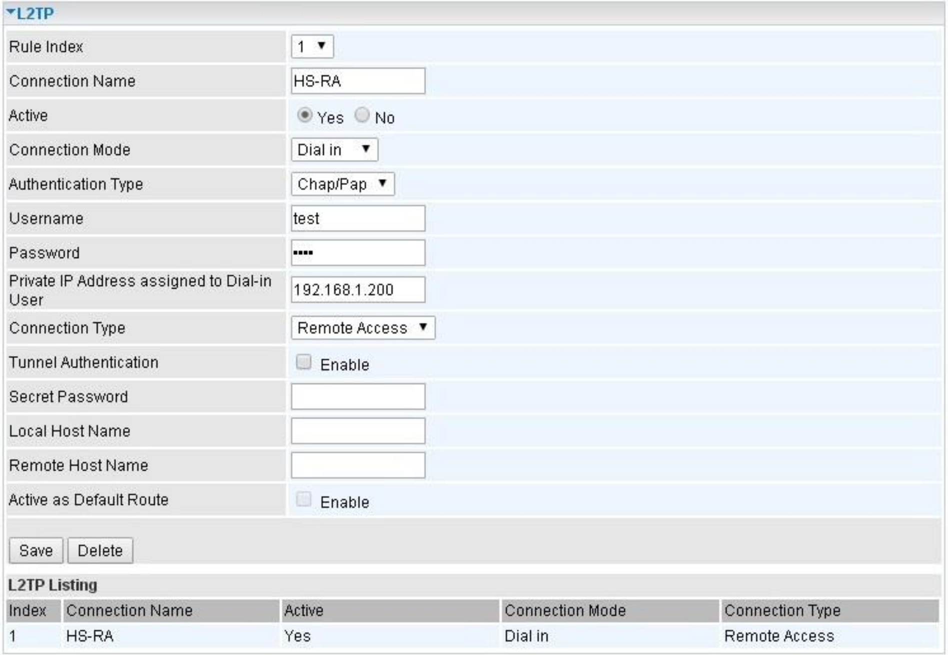
Example: L2TP VPN – Remote Employee Dial-in to AirConnect® 8355P 5G CPE

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



▾L2TP

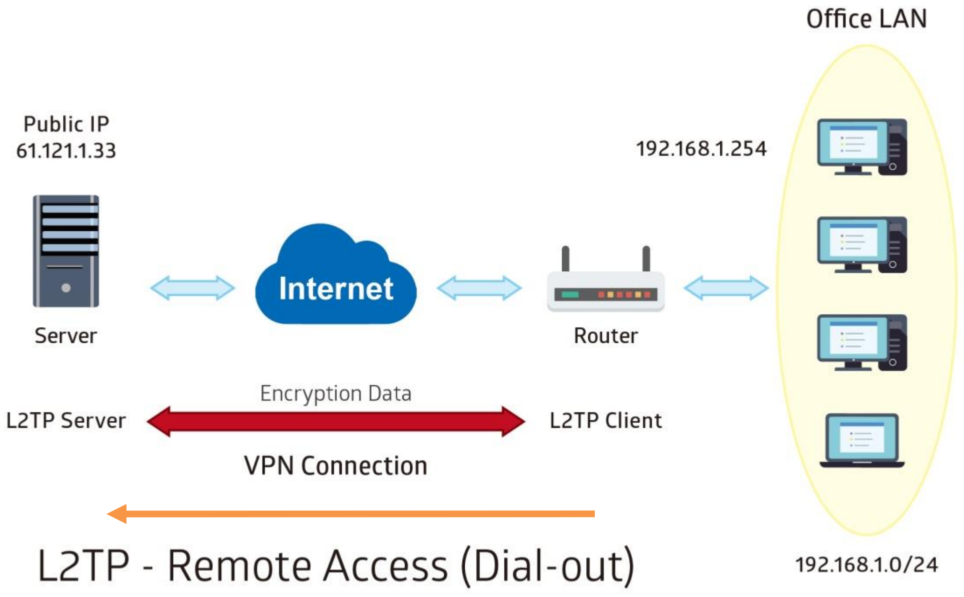
Rule Index	1 ▾
Connection Name	HS-RA
Active	● Yes ○ No
Connection Mode	Dial in ▾
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Private IP Address assigned to Dial-in User	192.168.1.200
Connection Type	Remote Access ▾
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

L2TP Listing

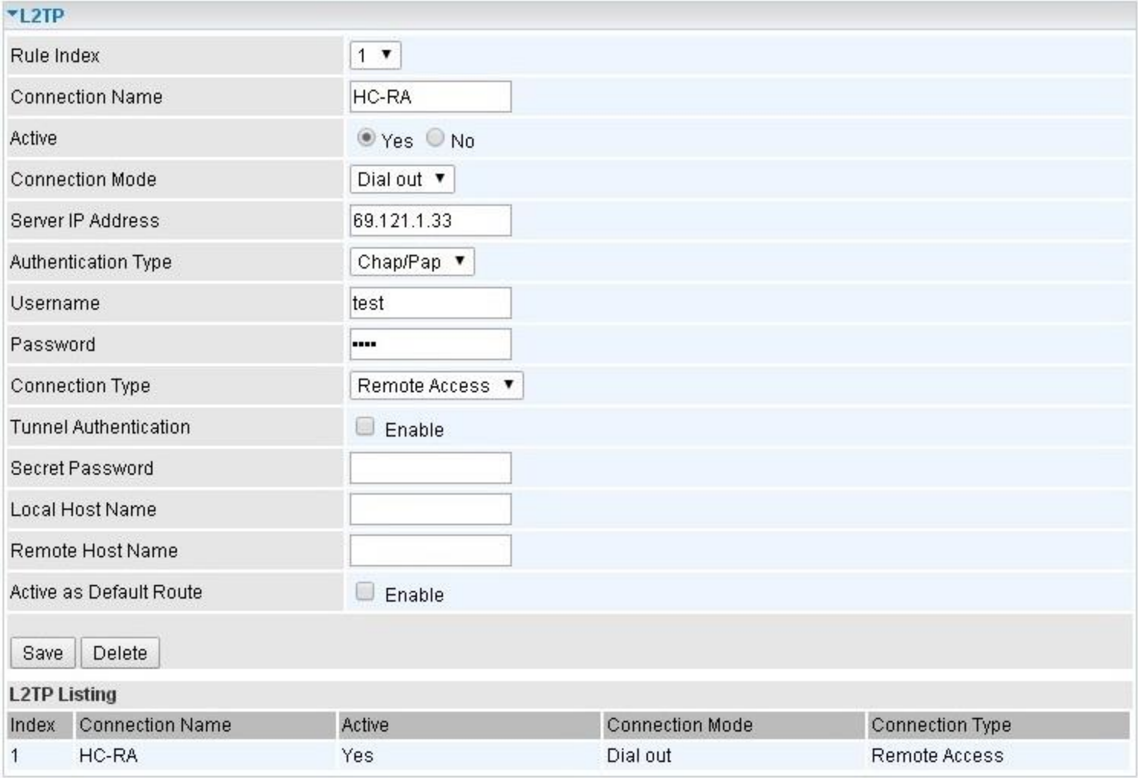
Index	Connection Name	Active	Connection Mode	Connection Type
1	HS-RA	Yes	Dial in	Remote Access

Example: L2TP VPN – AirConnect® 8355P 5G CPE 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



▾L2TP

Rule Index	1 ▾
Connection Name	HC-RA
Active	● Yes ○ No
Connection Mode	Dial out ▾
Server IP Address	69.121.1.33
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Connection Type	Remote Access ▾
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

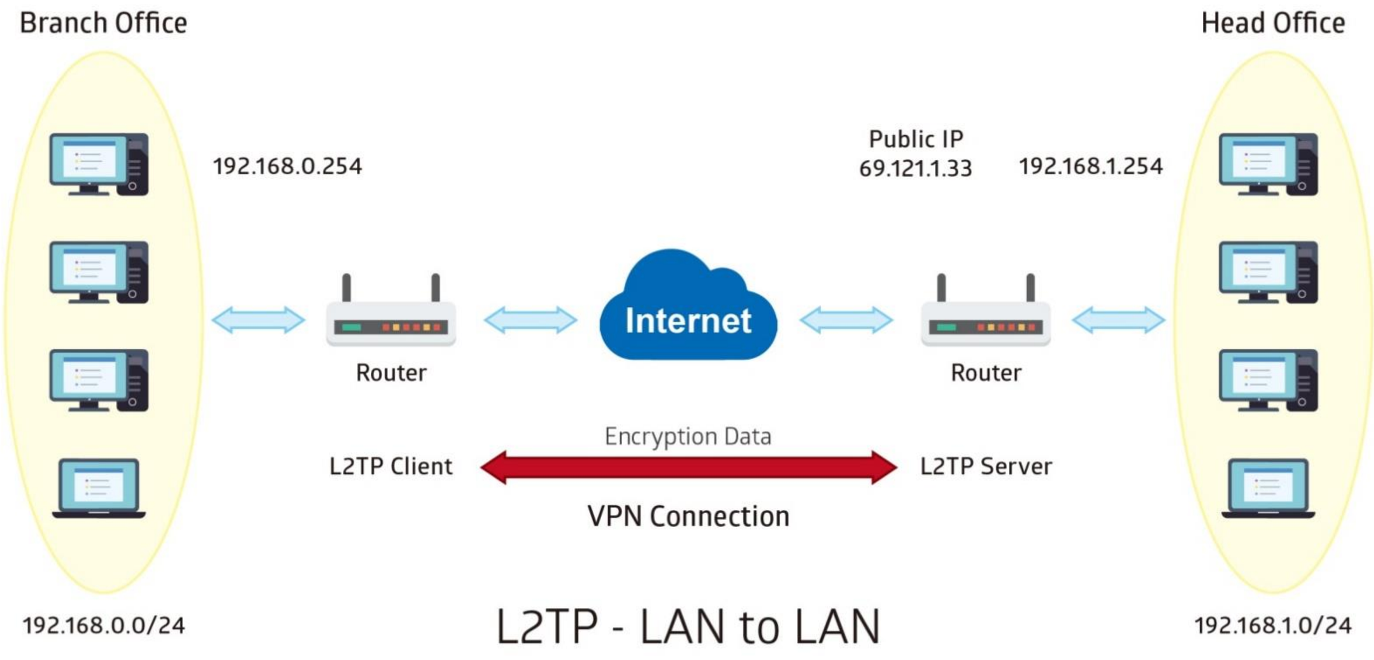
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	HC-RA	Yes	Dial out	Remote Access

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.

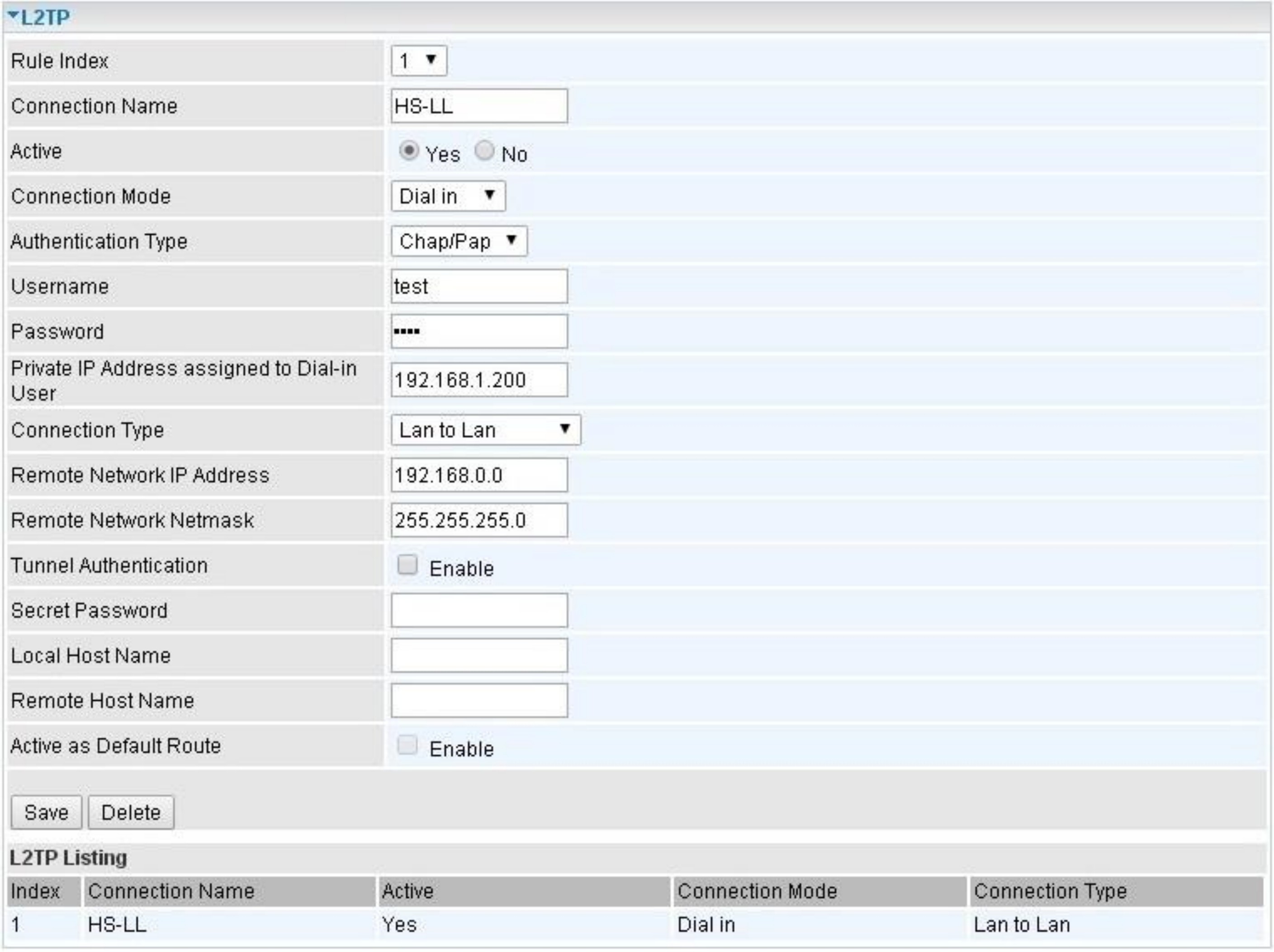
NOTE: Both office LAN networks must be in different subnets with the LAN-LAN application.



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	



L2TP

Rule Index	1
Connection Name	HS-LL
Active	● Yes ○ No
Connection Mode	Dial in
Authentication Type	Chap/Pap
Username	test
Password	••••
Private IP Address assigned to Dial-in User	192.168.1.200
Connection Type	Lan to Lan
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0
Tunnel Authentication	☐ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	☐ Enable

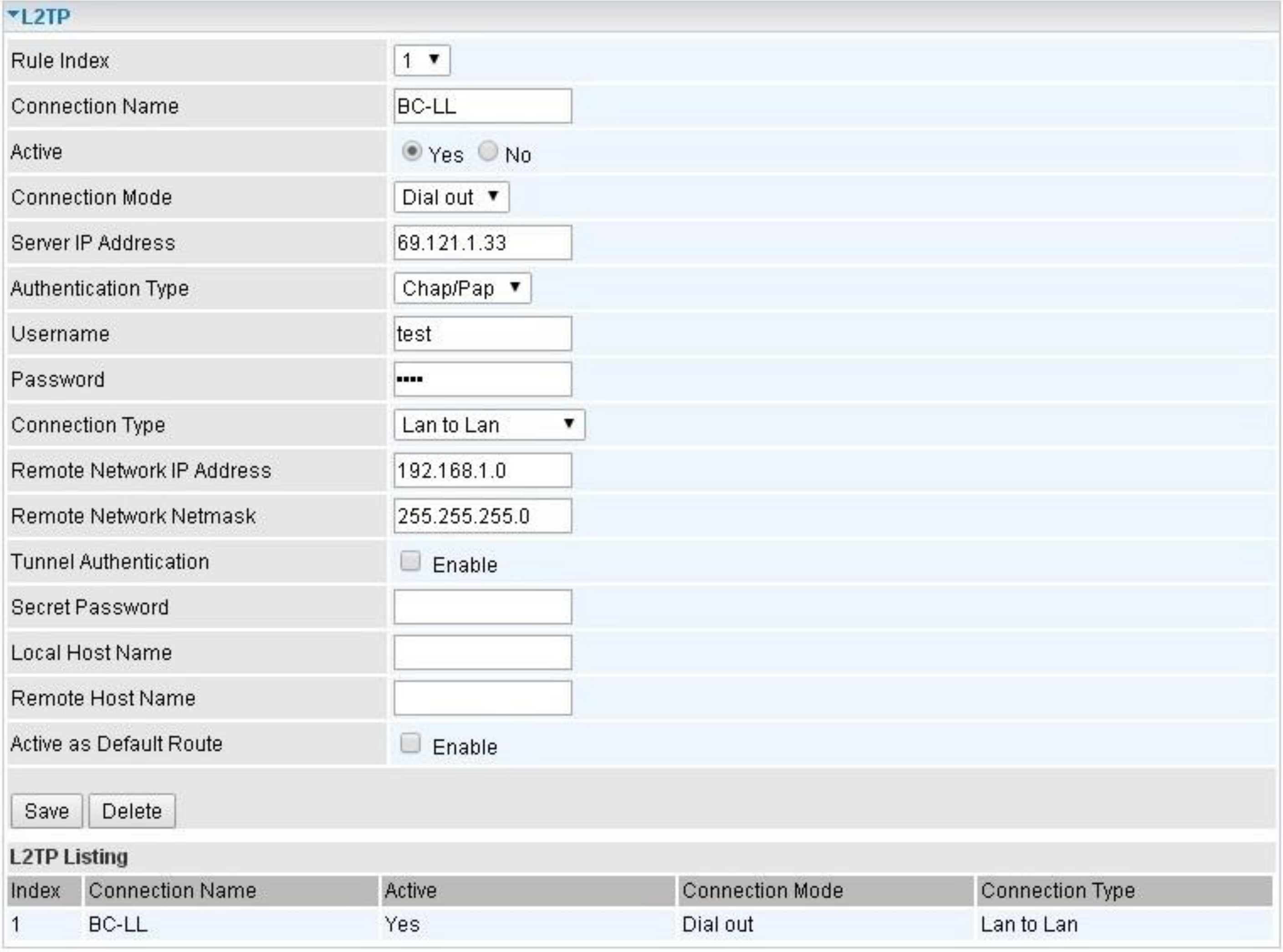
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	HS-LL	Yes	Dial in	Lan to Lan

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	



▾L2TP

Rule Index	1 ▾
Connection Name	BC-LL
Active	● Yes ○ No
Connection Mode	Dial out ▾
Server IP Address	69.121.1.33
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Connection Type	Lan to Lan ▾
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

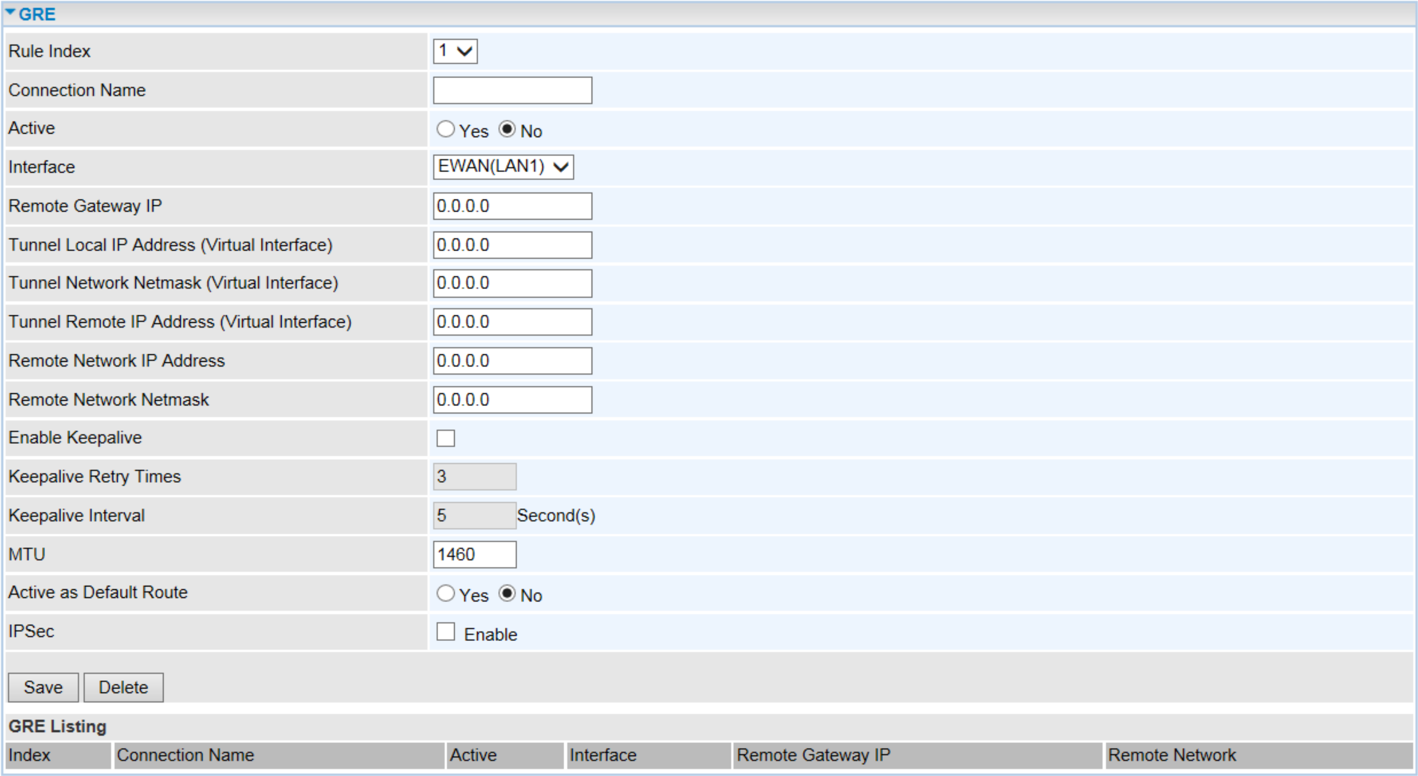
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	BC-LL	Yes	Dial out	Lan to Lan

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.



▾GRE

Rule Index	1
Connection Name	
Active	○ Yes ● No
Interface	EWAN(LAN1)
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
Active as Default Route	○ Yes ● No
IPSec	□ Enable

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network

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.

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

Remote Gateway: Enter the remote GRE WAN IP address.

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

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 Netmask: Enter remote LAN network IP address.

Remote Network Netmask: Enter remote LAN network Netmask.

Enable Keep-alive: Check the box to enable the keep-alive. 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.

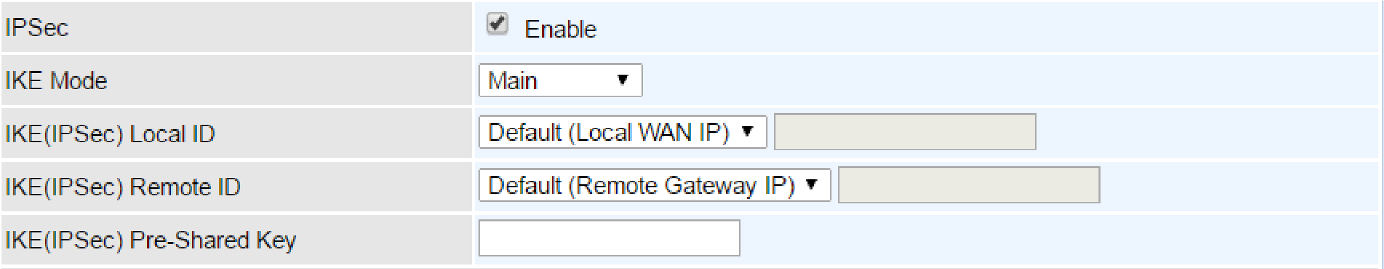
Keep-alive Interval: Set the keep-alive Interval, unit in seconds. Default is 5 seconds.

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.

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

IPSec: Click the checkbox to enable GRE tunnel over IPSec.



IPSec	☑ Enable
IKE Mode	Main ▼
IKE(IPSec) Local ID	Default (Local WAN IP) ▼
IKE(IPSec) Remote ID	Default (Remote Gateway IP) ▼
IKE(IPSec) Pre-Shared Key	

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.

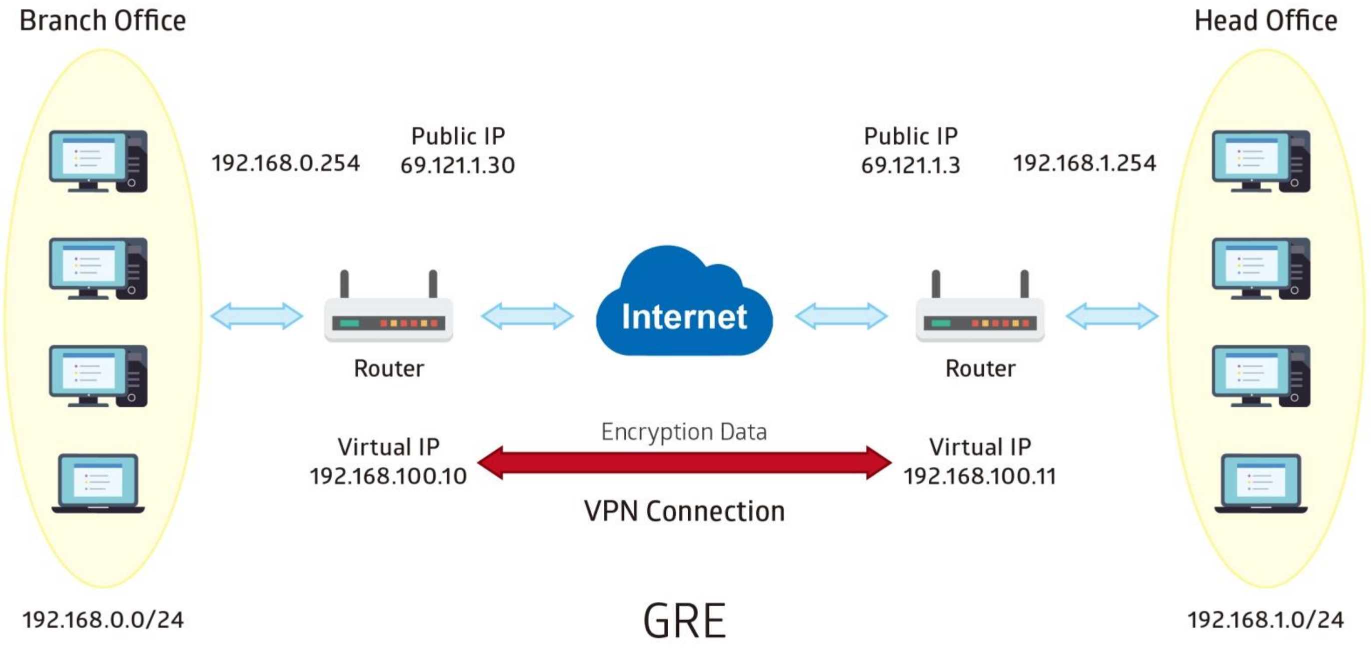
IKE (IPSec) Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can 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.

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.

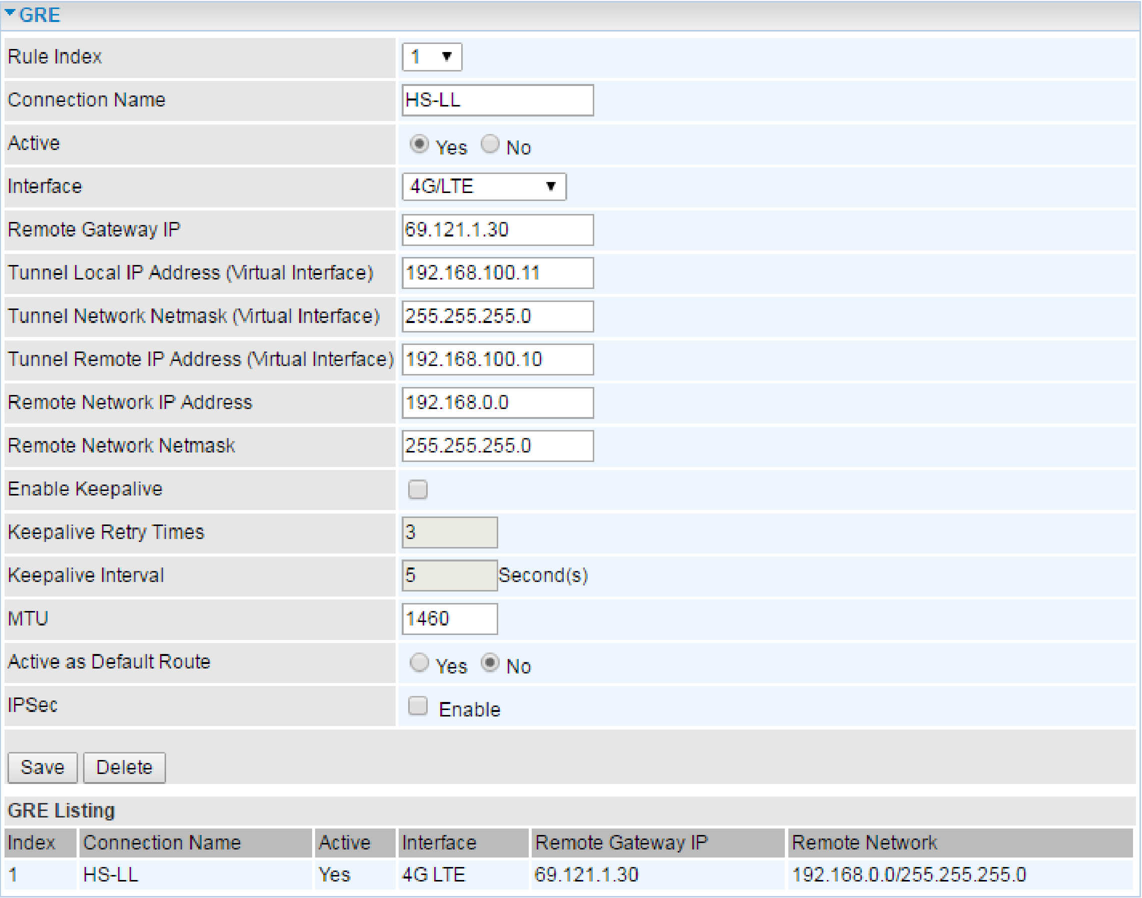
NOTE: Both office LAN networks must be in different subnets with the GRE VPN connection.



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.



▾GRE

Rule Index	1 ▾
Connection Name	HS-LL
Active	● Yes ○ No
Interface	4G/LTE ▾
Remote Gateway IP	69.121.1.30
Tunnel Local IP Address (Virtual Interface)	192.168.100.11
Tunnel Network Netmask (Virtual Interface)	255.255.255.0
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0
Enable Keepalive	□
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ● No
IPSec	□ Enable

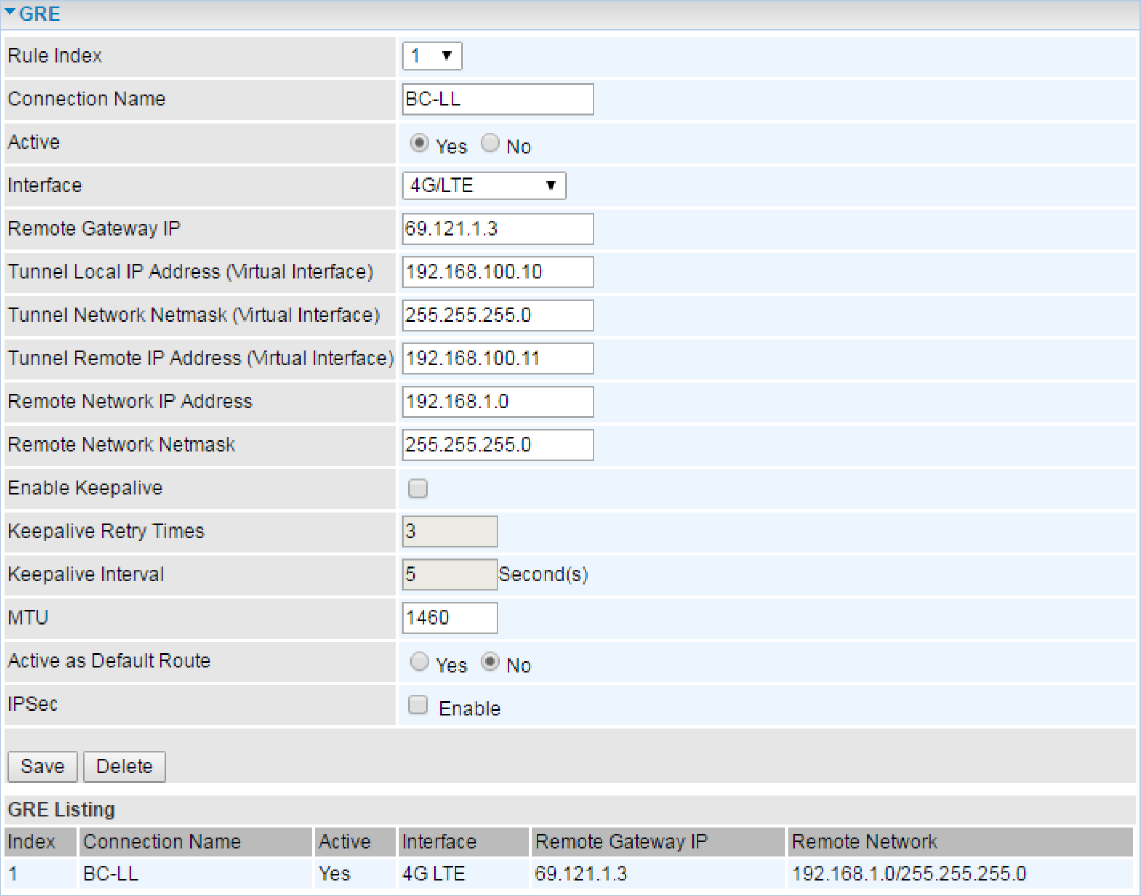
GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network
1	HS-LL	Yes	4G LTE	69.121.1.30	192.168.0.0/255.255.255.0

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.



▾GRE

Rule Index	1 ▾
Connection Name	BC-LL
Active	● Yes ○ No
Interface	4G/LTE ▾
Remote Gateway IP	69.121.1.3
Tunnel Local IP Address (Virtual Interface)	192.168.100.10
Tunnel Network Netmask (Virtual Interface)	255.255.255.0
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Enable Keepalive	□
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ● No
IPSec	□ Enable

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network
1	BC-LL	Yes	4G LTE	69.121.1.3	192.168.1.0/255.255.255.0

OpenVPN

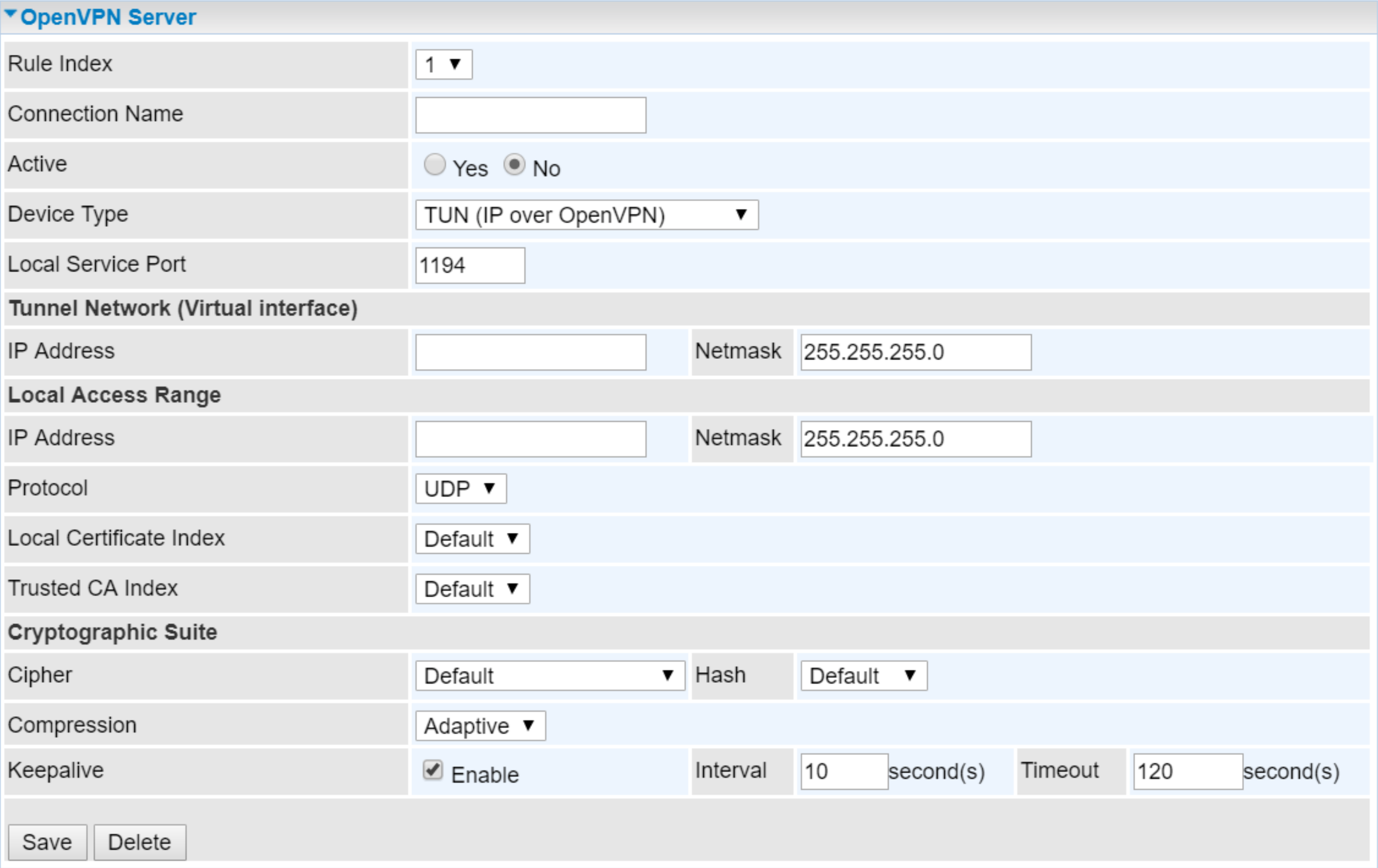
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.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



▾ OpenVPN Server

Rule Index	1 ▼				
Connection Name					
Active	○ Yes ● No				
Device Type	TUN (IP over OpenVPN) ▼				
Local Service Port	1194				
Tunnel Network (Virtual interface)					
IP Address		Netmask	255.255.255.0		
Local Access Range					
IP Address		Netmask	255.255.255.0		
Protocol	UDP ▼				
Local Certificate Index	Default ▼				
Trusted CA Index	Default ▼				
Cryptographic Suite					
Cipher	Default ▼	Hash	Default ▼		
Compression	Adaptive ▼				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

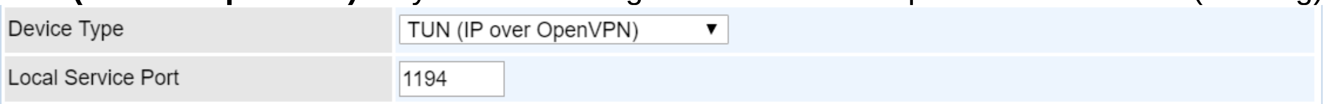
Rule Index: The numeric rule indicator for OpenVPN.

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

Active: Yes to activate this profile.

Device Type:

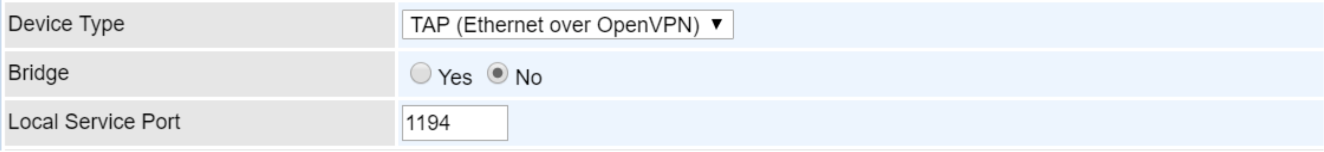
- **TUN (IP Over OpenVPN):** Layer 3 networking level which routes packets on the VPN (Routing).



Device Type	TUN (IP over OpenVPN) ▼
Local Service Port	1194

  - **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.



Device Type	TAP (Ethernet over OpenVPN) ▼
Bridge	○ Yes ● No
Local Service Port	1194

  - **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 keep-alive. The system will automatic 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.

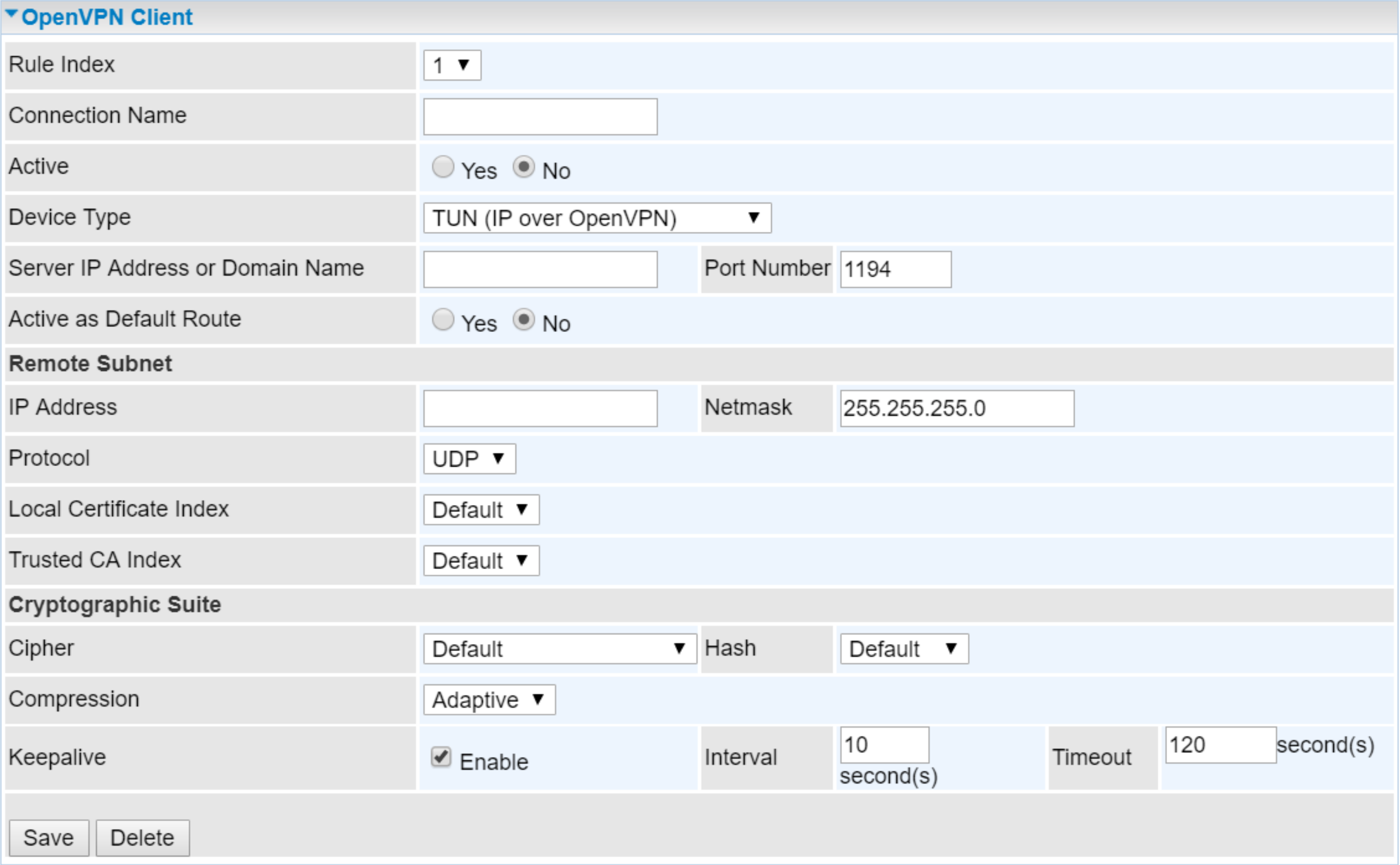
Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

OpenVPN Client

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

NOTE: Up to 4 tunnels supported.



▾OpenVPN Client

Rule Index	1 ▾				
Connection Name					
Active	○ Yes ● No				
Device Type	TUN (IP over OpenVPN) ▾				
Server IP Address or Domain Name		Port Number	1194		
Active as Default Route	○ Yes ● No				
Remote Subnet					
IP Address		Netmask	255.255.255.0		
Protocol	UDP ▾				
Local Certificate Index	Default ▾				
Trusted CA Index	Default ▾				
Cryptographic Suite					
Cipher	Default ▾	Hash	Default ▾		
Compression	Adaptive ▾				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

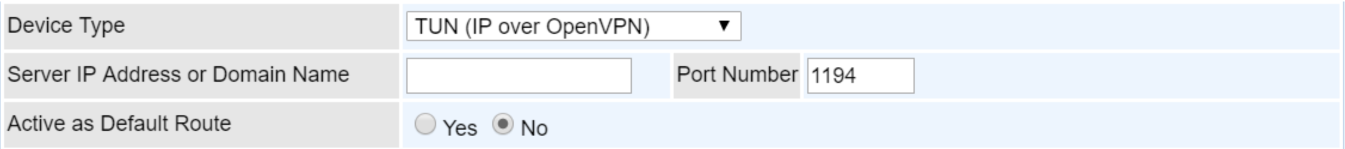
Rule Index: The numeric rule indicator for OpenVPN. Maximum up to 4 profile/tunnels

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

Active: Yes to activate this profile.

Device Type:

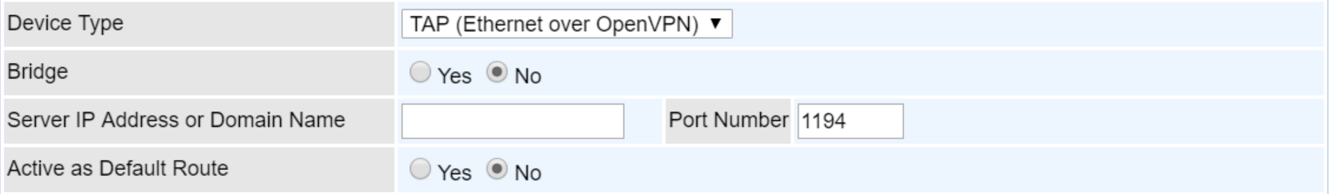
- **TUN (IP Over OpenVPN):** Works only in Layer 3 networking level which routes packets on the VPN.



Device Type	TUN (IP over OpenVPN) ▾		
Server IP Address or Domain Name		Port Number	1194
Active as Default Route	○ Yes ● No		

  - **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.
  - **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.

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



Device Type	TAP (Ethernet over OpenVPN) ▼		
Bridge	○ Yes ● No		
Server IP Address or Domain Name		Port Number	1194
Active as Default Route	○ Yes ● No		

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

Remote Subnet

IP Address / Netmask: Enter the LAN network IP address and Netmask of the OpenVPN Server.

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 keep-alive. The system will automatic 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.

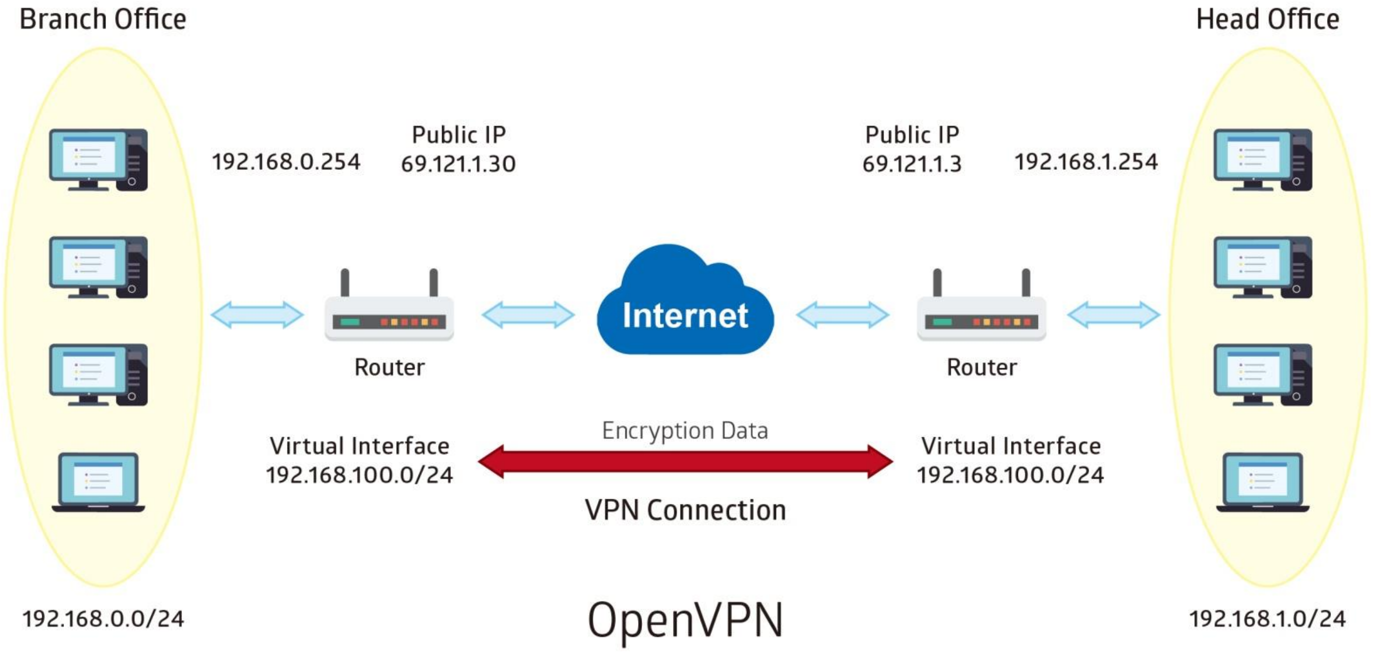
Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

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 with the GRE VPN connection.

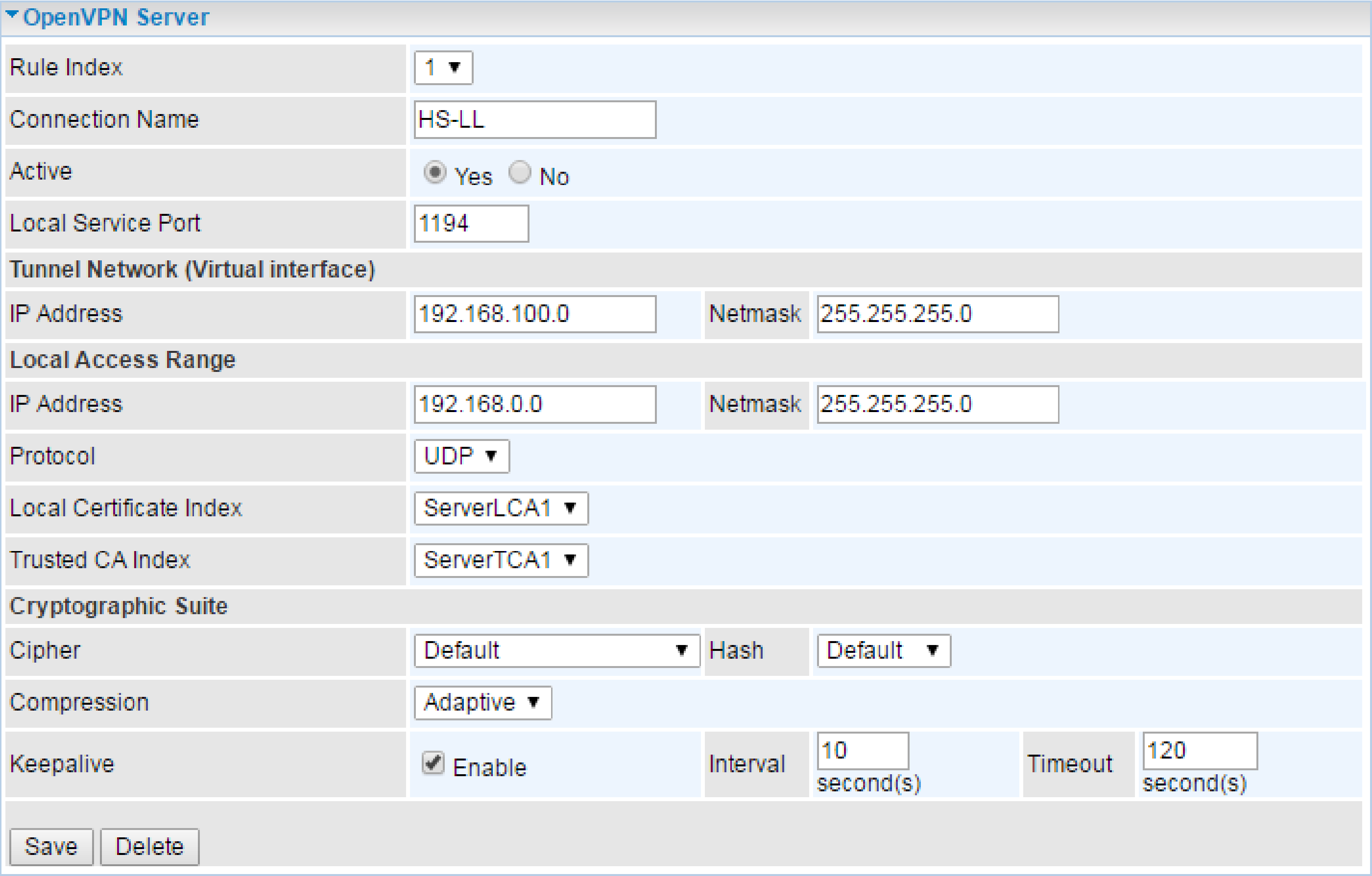


Configuring OpenVPN server in Headquarter office

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	192.168.0.0/ 255.255.255.0	OpenVPN Server's local LAN network.



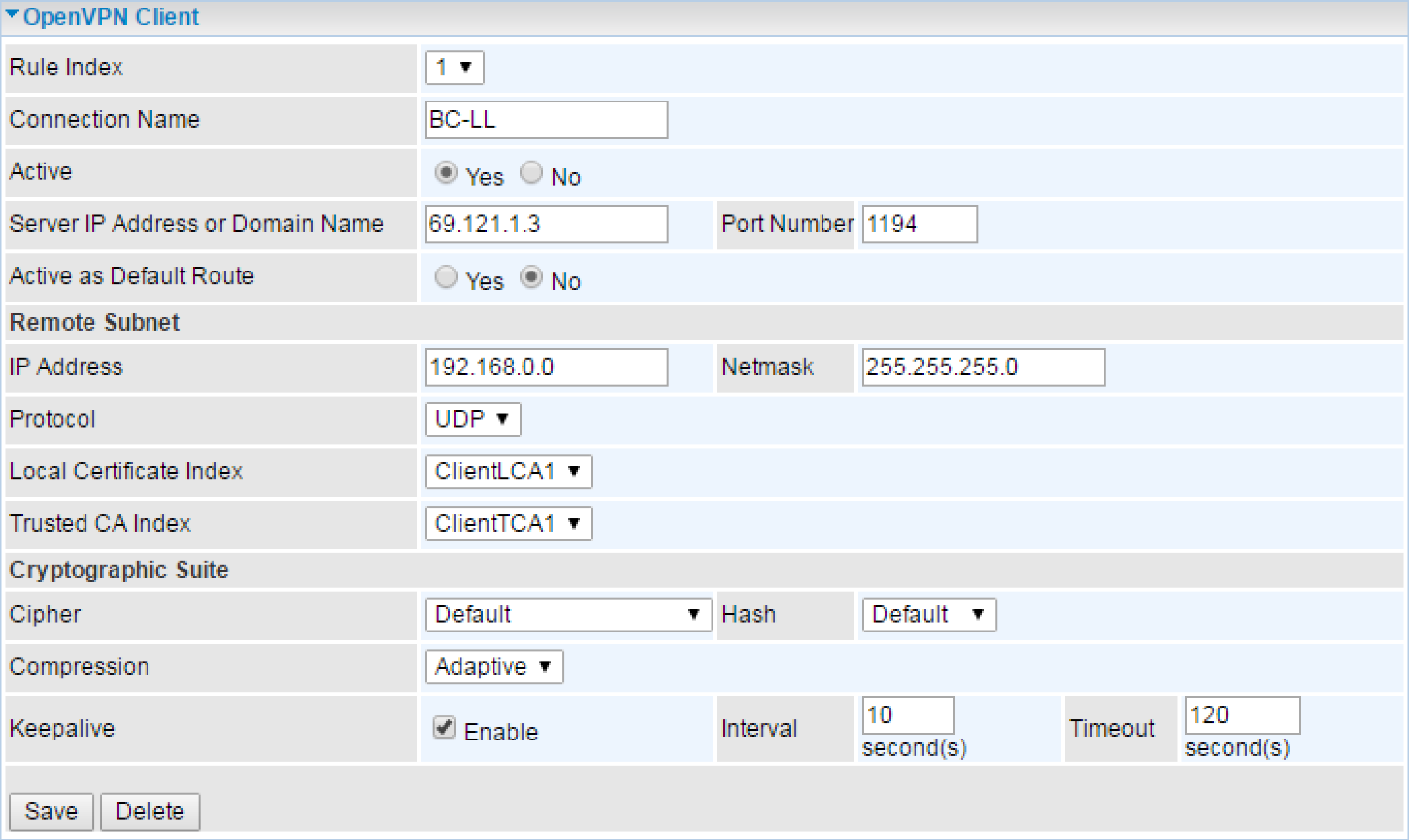
OpenVPN Server

Rule Index	1 ▾				
Connection Name	HS-LL				
Active	● Yes ○ No				
Local Service Port	1194				
Tunnel Network (Virtual interface)					
IP Address	192.168.100.0	Netmask	255.255.255.0		
Local Access Range					
IP Address	192.168.0.0	Netmask	255.255.255.0		
Protocol	UDP ▾				
Local Certificate Index	ServerLCA1 ▾				
Trusted CA Index	ServerTCA1 ▾				
Cryptographic Suite					
Cipher	Default ▾	Hash	Default ▾		
Compression	Adaptive ▾				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

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	192.168.0.0/ 255.255.255.0	Local LAN IP & Netmask of the Branch office



▾OpenVPN Client

Rule Index	1 ▾				
Connection Name	BC-LL				
Active	● Yes ○ No				
Server IP Address or Domain Name	69.121.1.3	Port Number	1194		
Active as Default Route	○ Yes ● No				
Remote Subnet					
IP Address	192.168.0.0	Netmask	255.255.255.0		
Protocol	UDP ▾				
Local Certificate Index	ClientLCA1 ▾				
Trusted CA Index	ClientTCA1 ▾				
Cryptographic Suite					
Cipher	Default ▾	Hash	Default ▾		
Compression	Adaptive ▾				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

CHAPTER 5: TROUBLESHOOTING

If your **AirConnect® 8355P 5G CPE** 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

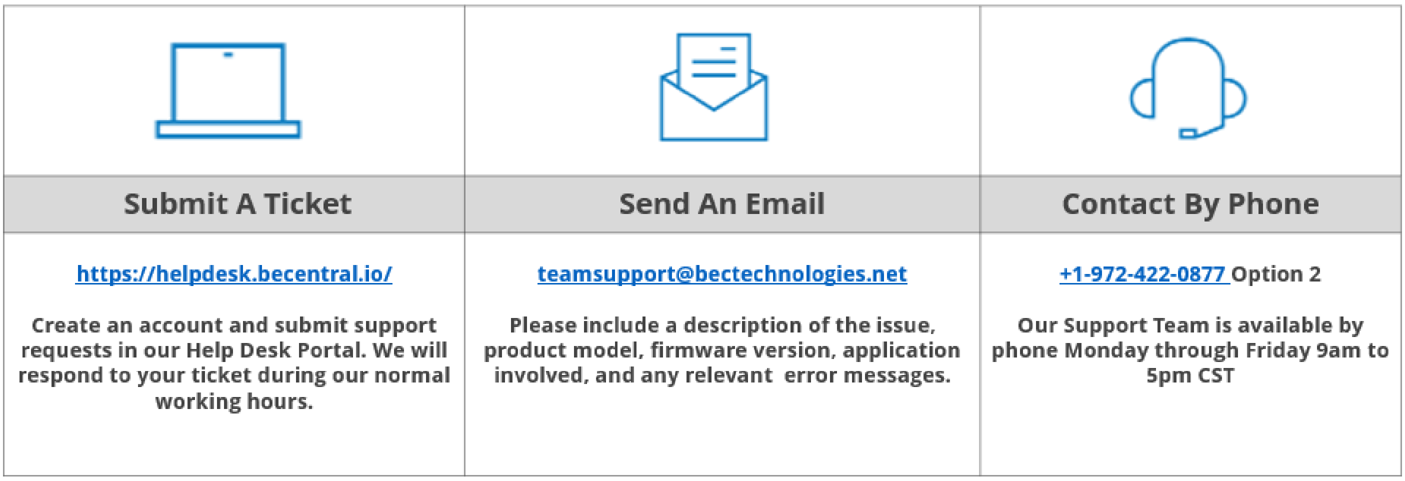
Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it was not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall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

Recovery Procedures

Problem	Suggested Action
- The front LEDs display incorrectly **- Still cannot access to the router management interface after pressing the RESET button.** **- Software / Firmware upgrade failure**	1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or another small pointed object immediately. 2. The router’s emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, please note that the router will only respond with its web interface at this address (192.168.1.1) and will not respond to ping request from your PC or other telnet operations.

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems, please contact the dealer from where you have purchased the product or contact BEC via one of the methods listed below:



Submit A Ticket	Send An Email	Contact By Phone
https://helpdesk.becentral.io/ Create an account and submit support requests in our Help Desk Portal. We will respond to your ticket during our normal working hours.	teamsupport@bectechnologies.net Please include a description of the issue, product model, firmware version, application involved, and any relevant error messages.	+1-972-422-0877 Option 2 Our Support Team is available by phone Monday through Friday 9am to 5pm CST

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 11/10/8/7 and Windows Vista are registered Trademarks of Microsoft Corporation.

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.

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 at a minimum distance 20cm between the radiator & your body.

This page is intentionally left blank.