



BEC 6300VNL

GigaConnect[®] 4G/LTE VoIP Wireless Broadband Router

User Manual

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
INTRODUCTION TO YOUR ROUTER.....	1
FEATURES & SPECIFICATIONS.....	3
HARDWARE SPECIFICATIONS.....	6
APPLICATION DIAGRAMS	7
CHAPTER 2: PRODUCT OVERVIEW.....	8
IMPORTANT NOTE FOR USING THIS ROUTER	8
DEVICE DESCRIPTION	9
Front Panel LEDs.....	9
Rear Panel Connectors	10
POWER SOURCE	11
SYSTEM RECOVERY PROCEDURES.....	13
CABLING	14
CHAPTER 3: BASIC INSTALLATION.....	15
NETWORK CONFIGURATION – IPv4	16
Configuring PC in Windows 10 (IPv4)	16
Configuring PC in Windows 7/8 (IPv4).....	18
Configuring PC in Windows Vista (IPv4).....	20
Configuring PC in Windows XP (IPv4)	22
NETWORK CONFIGURATION – IPv6	23
Configuring PC in Windows 10 (IPv6)	23
Configuring PC in Windows 7/8 (IPv6).....	25
Configuring PC in Windows Vista (IPv6).....	27
Configuring PC in Windows XP (IPv6)	29
DEFAULT SETTINGS.....	30
INFORMATION FROM YOUR ISP	31
CHAPTER 4: DEVICE CONFIGURATION	32

LOGIN TO YOUR DEVICE	32
STATUS.....	34
Device Info	34
System Status	36
System Log	36
3G/4G-LTE Status	37
Statistics	38
DHCP Table.....	43
Disk Status.....	43
IPSec Status.....	44
PPTP Status	45
L2TP Status.....	46
GRE Status.....	46
VoIP Status	47
ARP Table	48
QUICK START	49
CONFIGURATION.....	52
Interface Setup.....	52
<i>Internet</i>	52
<i>LAN</i>	63
<i>Wireless</i>	67
<i>Wireless MAC Filter</i>	79
<i>Loopback</i>	80
Dual WAN.....	81
<i>General Setting</i>	81
Advanced Setup	84
<i>Firewall</i>	84
<i>Static Routing</i>	86
<i>Dynamic Routing</i>	87
<i>NAT</i>	89
<i>Static DNS</i>	94
<i>QoS</i>	95
<i>Interface Grouping</i>	96
<i>Port Isolation</i>	98
<i>Time Schedule</i>	99
<i>Mail Alert</i>	100
VPN	101
<i>IPSec</i>	101
<i>PPTP Server</i>	111

<i>PPTP Client</i>	113
<i>L2TP</i>	119
<i>GRE Tunnel</i>	126
VoIP	131
<i>Basic</i>	131
<i>Media</i>	133
<i>Advanced</i>	134
<i>Speed Dial</i>	135
<i>Dial Plan</i>	137
<i>Call Features</i>	141
<i>NAT Traversal for VoIP</i>	144
Access Management	146
<i>Device Management</i>	146
<i>SNMP</i>	147
<i>Syslog</i>	149
<i>Universal Plug & Play</i>	150
<i>Dynamic DNS</i>	151
<i>Access Control</i>	153
<i>Packet Filter</i>	155
<i>CWMP (TR-069)</i>	159
<i>Parental Control</i>	161
<i>SAMBA & FTP Server</i>	162
<i>BECentral Management</i>	165
Maintenance	166
<i>User Management</i>	166
<i>Time Zone</i>	170
<i>License</i>	171
<i>Firmware & Configuration</i>	172
<i>System Restart</i>	173
<i>Auto Reboot</i>	174
<i>Diagnostics Tool</i>	175

CHAPTER 5: TROUBLESHOOTING 177

Problems with the Router	177
Problem with LAN Interface	177
Recovery Procedures.....	178

APPENDIX: PRODUCT SUPPORT & CONTACT 179

FCC STATEMENT	180
----------------------------	------------

IC REGULATIONS.....	181
IC Warning	181
Detachable Antenna Usage.....	182

CHAPTER 1: INTRODUCTION

Introduction to your Router

Congratulations on your purchase of the **BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router)**. This router is a compact and advanced broadband router that offers flexible and multiple Internet connection options, EWAN and embedded 4G/LTE interfaces, for home, SOHO, and office users to enjoy high-speed, high-level security Internet connection via cellular wireless and/or Ethernet WAN. With an integrated 802.11n wireless access point and 4-port Gigabit Ethernet LAN, this router enables faster wireless speed of up to 300Mbps and LAN connection 10 times faster than regular 10/100Mbps Ethernet LAN. **BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router)** provides a unique Management Center enabling users to monitor 4G/LTE signal strength, bandwidth, download speed, and many more. Users can choose the most economical rate of VoIP calls provided by different providers. The device integrates two FXS ports which allows for simultaneous VoIP calls.

Cost Saving

Making VoIP calls is extremely simple; just connect the router with your existing analog telephones. **BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router)** complies with the most popularly adopted VoIP standard and SIP protocol to ensure interoperability with SIP devices and major VoIP Gateways. This router also supports a wider range of telephony features, such as Call Waiting, Conference, Speed Dial, Return Call, Redial, etc.

4G/LTE Mobility

With 4G/LTE-based Internet connection (4G/LTE embedded module, requires an additional SIM card), you can access to the Internet through 4G/LTE whether you are seated at your desk or taking a cross-country trip.

Wireless Mobility and Security

With an integrated 802.11n Wireless Access Point, this router delivers up to 3 times the wireless coverage of a 802.11b/g network device, so that wireless access is available everywhere in the house or office. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) allows you to expand your wireless network without additional wires or cables. **BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router)** also supports the Wi-Fi Protected Setup (WPS) standard and allows users to establish a secure wireless network just by pressing a button. Multiple SSIDs allow users to access different networks through a single access point. Network managers can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure.

4G/LTE Management Center

BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router) Mobile Management Center visually displays its current 4G/LTE signal status also calculates the total amount of hours or data traffic used per month, allowing you to manage your 4G/LTE monthly subscriptions.

IPv6 Supported

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

Quick Start Wizard

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

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Features & Specifications

- 4G/LTE for high speed mobile broadband connectivity
- Gigabit Ethernet WAN (GbE WAN) for Cable/Fiber/xDSL high WAN throughput
- Gigabit Ethernet LAN
- IPv6 ready (IPv4/IPv6 dual stack)
- Multiple wireless SSIDs with wireless guest access and client isolation
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP)
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization management
- Universal Plug and Play (UPnP) Compliance
- Voice over IP compliant with SIP standard
- Two FXS ports for connecting to regular analog telephones
- Call Waiting, Conference Call
- Speed Dial, Return Call, Redial
- Don't Disturb
- Ease of Use with Quick Installation Wizard
- One USB port for NAS (FTP/ SAMBA server)
- Ideal for SOHO, office, and home users

Network Protocols and Features

- IPv4, IPv6 or IPv4 / IPv6 Dual Stack
- 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)

Wireless LAN

- Compliant with IEEE 802.11 b/ g/ n standards
- 2.4 GHz - 2.484GHz radio band for wireless
- Up to 300 Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support

USB Application Server

- Storage/NAS: SAMBA Server, FTP Server
- 3G/4G LTE Mobile Internet Connection

VoIP

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

- FAX Relay: T.38
- Call Detailed Records (CDR)

Management

- Quick Installation wizard
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server / client / relay
- Supports SNMP v1, v2, v3, MIB-I and MIB-II
- TR-069 supports remote management

Hardware Specifications

Physical interface

- 4G LTE antenna: 2 external antennas
- SIM card slot: Mini SIM card (2FF) slot for mobile broadband connectivity
- VoIP phone port: 2 RJ-11 FXS phone ports to connect with 2 regular analog phones.
- USB: USB 2.0 port for storage service
- Ethernet: 4-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: RJ-45 Gigabit Ethernet port for connecting to Cable/Fiber/xDSL modem for Broadband connectivity.
- Factory default reset button
- Wireless on/off and WPS push button
- DC Power jack
- UPS Power with 4-pin connectors
- Power switch to switch between DC power and UPS power.

Physical Specifications

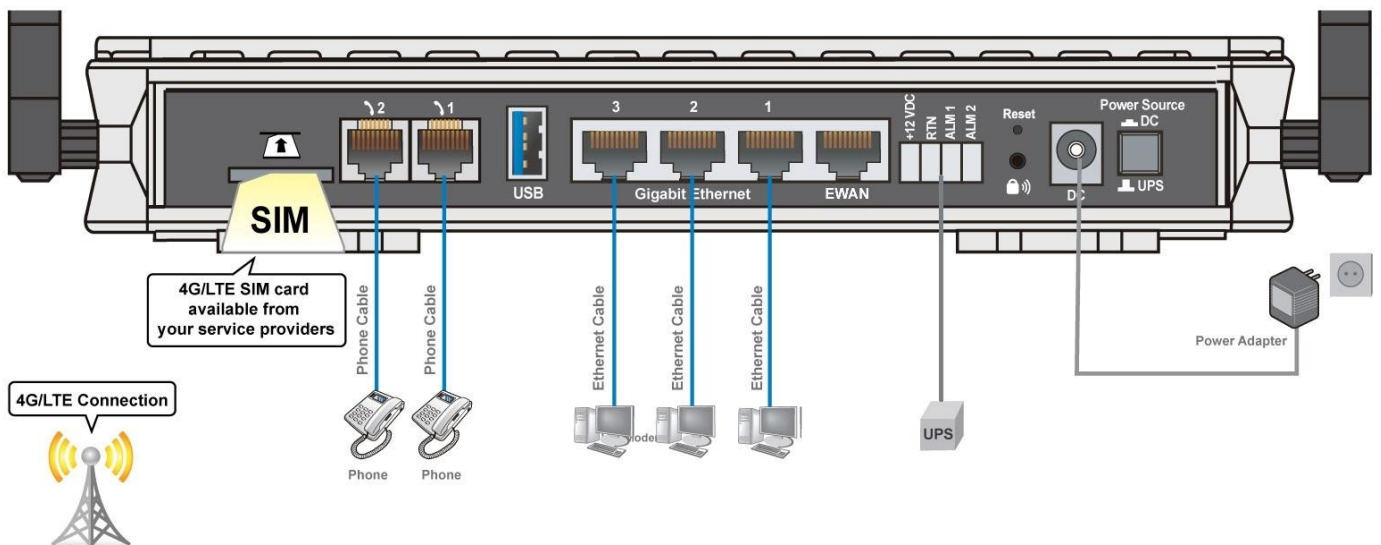
- Dimensions (W*H*D): 9.04" x 6.10" x 1.27"(229.5mm x 155mm x 32.24mm)

Application Diagrams

BEC 6300VNL (4G/LTE VoIP Wireless Broadband Router) is an all-in-one router, supporting 2 connection options (4/LTE and EWAN) to connect to the Internet.

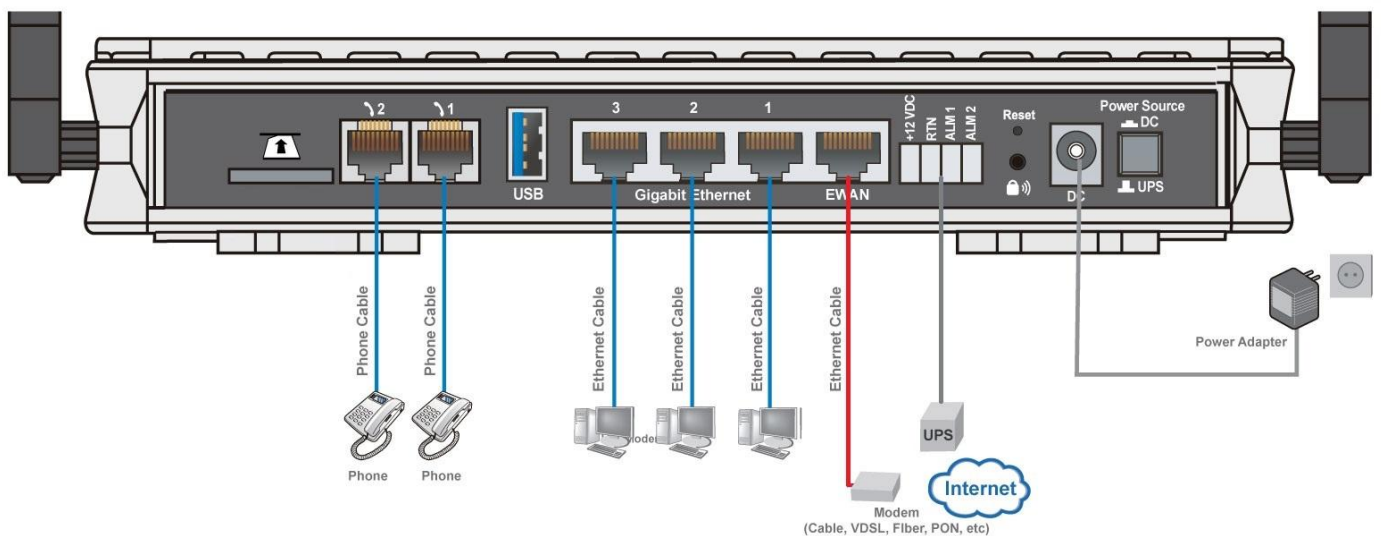
4G/LTE router mode

With an embedded 4G/LTE module, the router can be used to connect to high speed mobile fixed wireless connection.



Broadband Router Mode

This router also has a Gigabits Ethernet WAN port (EWAN) to connect with your Fiber / Cable/ xDSL modem.



CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router



Warning

- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not use the same power source for the BEC 6300VNL on other equipment.
- ✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

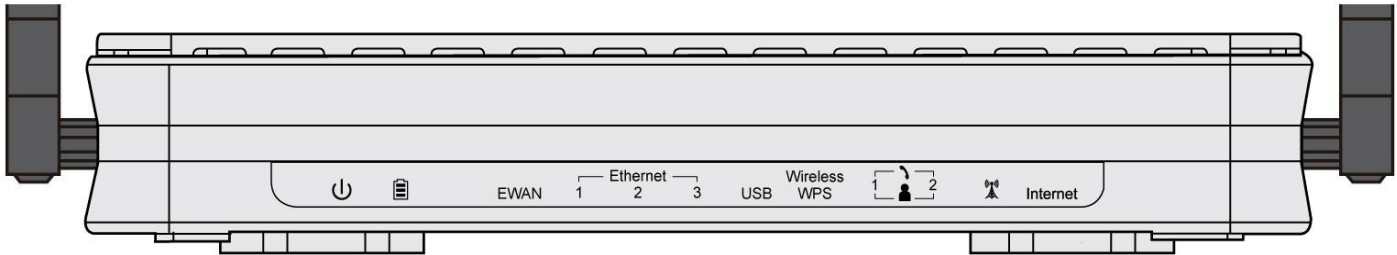






Attention

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

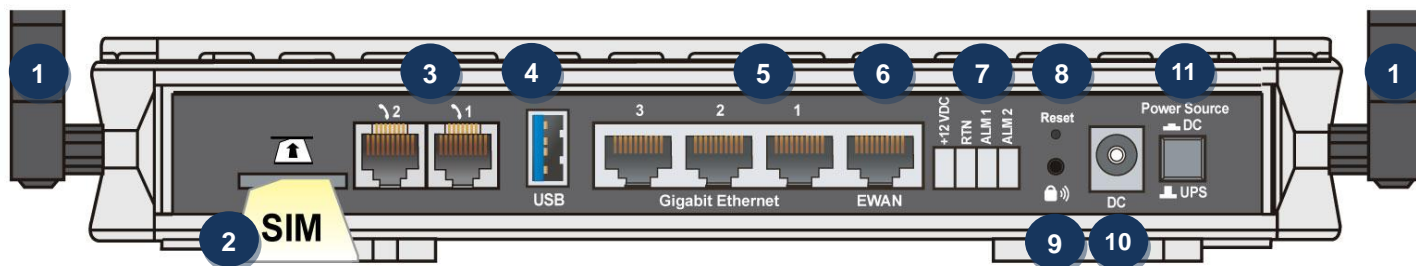
Device Description

Front Panel LEDs



LED	STATUS	DESCRIPTION
Power 	Green	System is up and ready
	Red	Boot failure
Battery 	Green	UPS is functional properly
	Orange	UPS battery failure. Need a new battery replacement
	Orange blinking	UPS AC power failure and battery functional properly
	Off	Device powered by the DC power adapter
EWAN	Lit up	BEC 6300VNL is successfully connected with a broadband connection device.
	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
Ethernet Port LAN 1 ~ 3	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
USB 2.0	Green	Connecting to a USB dongle or a hard drive.
Wireless/WPS	Green	Wireless connection established
	Green blinking	Data being transmitted / received
	Orange	WPS configuration is in progress
Phone 	Green	Successfully registered and ready to be used.
	Orange	Phone is off-hook, in-use
LTE  (Received Signal Strength Indicator)	Green	RSSI greater than -69 dBm. Excellent signal condition
	Green Flashing quickly	RSSI from -81 to -69 dBm. Good signal condition
	Orange Flashing quickly	RSSI from -99 to -81 dBm. Fair signal condition.
	Orange Flashing slowly	RSSI less than -99 dBm. Poor signal condition.
	Orange	No signal and the 4G_LTE module is in service
	Off	No LTE module or LTE module fails
Internet	Green	IP connected and traffic is passing thru the device.
	Red	IP request failed.
	Off	BEC 6300VNL is either in bridged mode or WAN connection not ready.

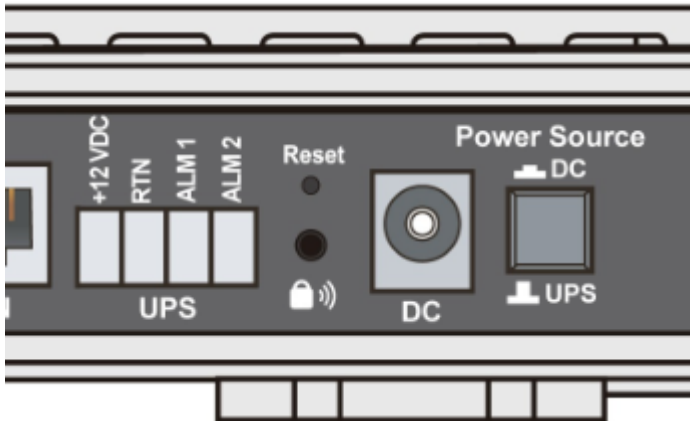
Rear Panel Connectors



PORT		MEANING
1	LTE Antenna	Screw the supplied LTE antennas onto the antenna connectors on both sides.
2	SIM Card Slot	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it
3	Phone (1X-2X)	Connect your analog phone to this port with a RJ-11 cable.
4	USB	The USB can either setup for 3G/4G LTE internet access or storage/file sharing. (1) For File Sharing: Connect an external USB dongle / hard drive for storage, network sharing, etc (2) For 3G/4G LTE Internet Connection: Connect with an external USB 3G/4G LTE modem or dongle with an activate data plan (Internet access).
5	Gigabit LAN Ethernet (1~3)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps /1000Mbps
6	Gigabit EWAN	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable
7	UPS Jack	The 4-pin connectors are used to power the device with an external UPS battery backup.
8	Reset	After the device is powered on, press it 6 seconds or above : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
9	WPS & Wireless On/Off	By controlling the pressing time, users can achieve two different effects: (1) WPS : Press &hold the button for less than 6 seconds to trigger WPS function. (2) Wireless ON/OFF button : Press & hold the button for more than 6 seconds to On/Off the wireless. * Please refer to the WPS section in the User Manual.
10	Power Jack (DC)	Connect the supplied Power Adapter to this jack.
11	Power Source	Power ON/OFF switch (1) with Power Switch ON : power up by the supplied DC power adapter (2) with Power Switch OFF : power up by the UPS battery unit

Power Source

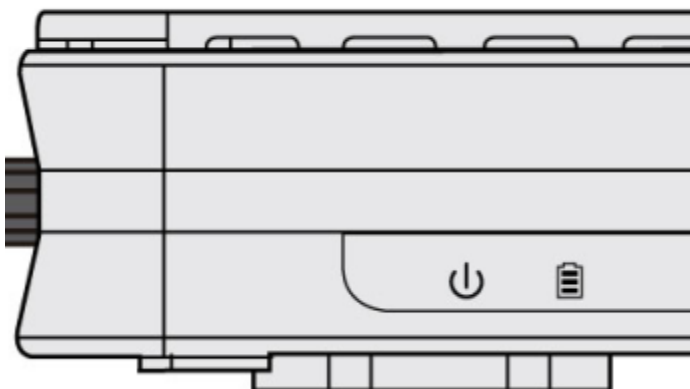
BEC 6300VNL offers two kinds of power input, namely, **DC power Adapter** and **DC UPS** (or BBU).
BEC 6300VNL can take the advantage of UPS (Uninterruptible Power Supply) to keep working even if the power outage hit your router when the router is working in DC UPS mode.



(A picture of the rear focusing on the power source)

UPS Port Assignment:

- ▶ +12VDC: VCC (DC + 12V) Power supply
- ▶ RTN: GND (Ground)
- ▶ ALM 1: Active high – replace battery
- ▶ ALM 2: Active high – on battery



(A shot from the front panel, with second icon being identified as the **Battery** LED)

How to switch between the two (2) power sources, DC power adapter and external UPS battery

Pressed "Power Source" button, the button is visually being pressed down. The power source is from the DC power adapter supplied in the package.

"Power Source" button in the un-pressed state, the power source is from the UPS. The router can continue to operate for a period of time after AC power failure, due to uninterrupted power system features of UPS.

UPS LED:

A Battery LED indicates if a DC UPS is in-use or not. When the router is operating via the DC power adapter this LED will be off.

Battery LED Definition:

- ▶ Green LED: UPS AC power is working; UPS battery is also working well
- ▶ Orange LED Only UPS AC power is working. Battery failure- need a new battery replacement
- ▶ Orange LED: UPS AC power failure; UPS battery is working

System Recovery Procedures

The purpose is to allow users to restore the BEC 6300VNL 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 6300VNL Device

- 2.1 Power off your 6300VNL
- 2.2 Power on the 6300VNL 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 until the INTERNET LED flashes in GREEN

Step 3 – Restore your 6300VNL Device

With INTERNET light flashes green, 6300VNL 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, 6300VNL 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 6300VNL.
- 3.4 INTERNET LED turns green after the Firmware upgrade completed
- 3.5 Power cycle on & off to regain access to the 6300VNL.

Cabling

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

Make sure that all other devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your BEC router have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If the line filter is not correctly installed and connected, it may cause problems to your connection or may result in frequent disconnections.

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.



Any TCP/IP capable workstation can be used to communicate with or through the **BEC 6300VNL**. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

Configuring PC in Windows 10 (IPv4)

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

Related settings

Change adapter options

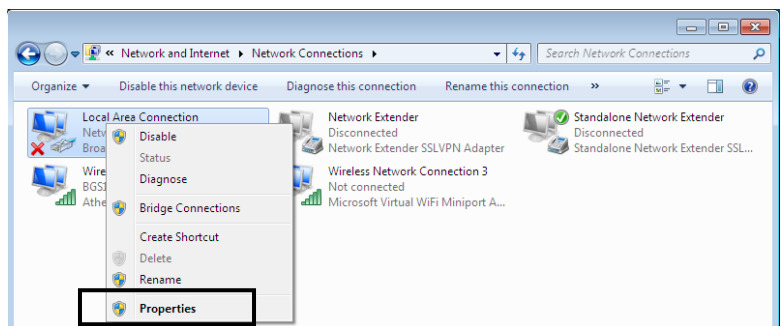
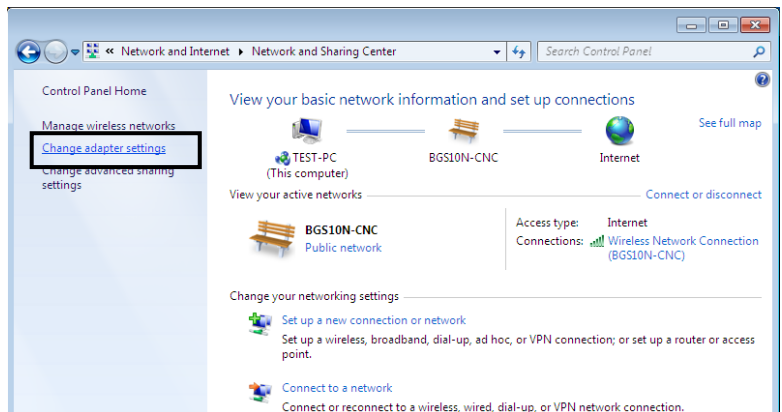
Change advanced sharing options

Network and Sharing Center

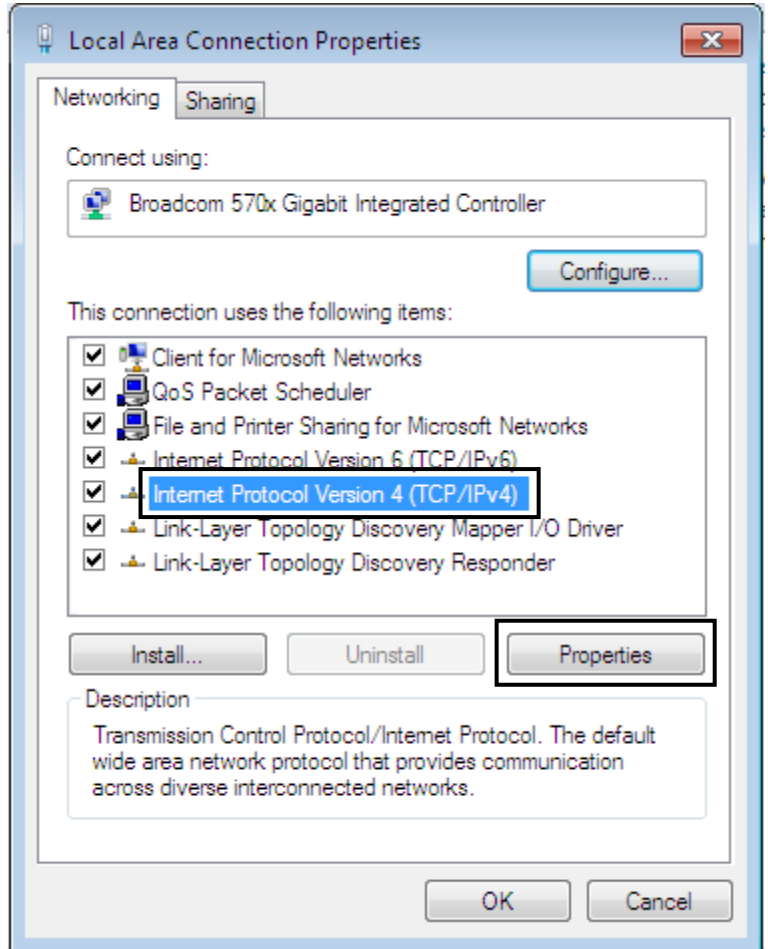
HomeGroup

Internet options

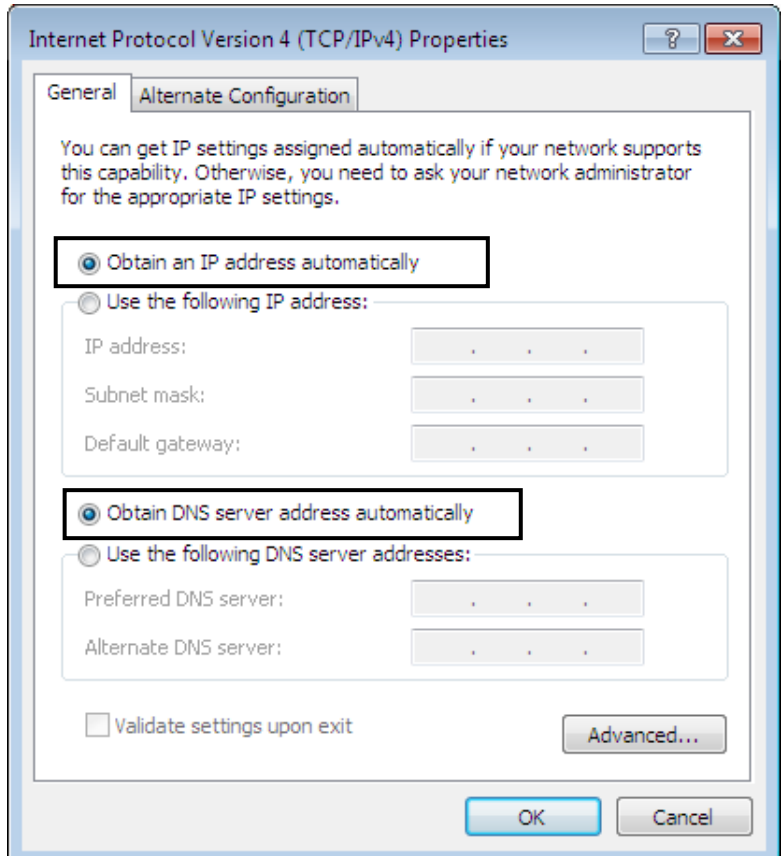
Windows Firewall



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

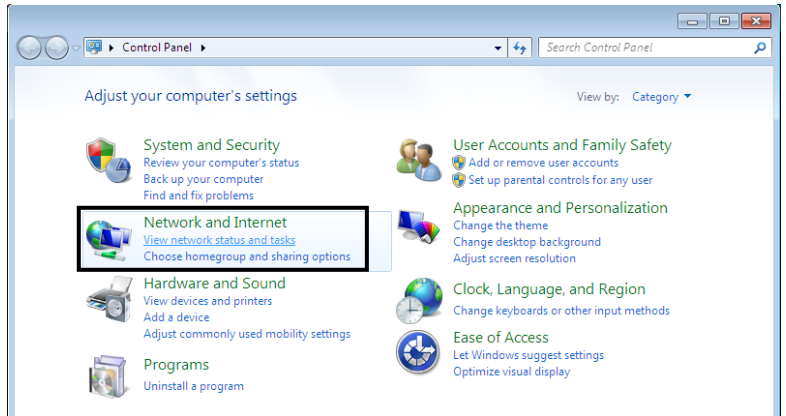


8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

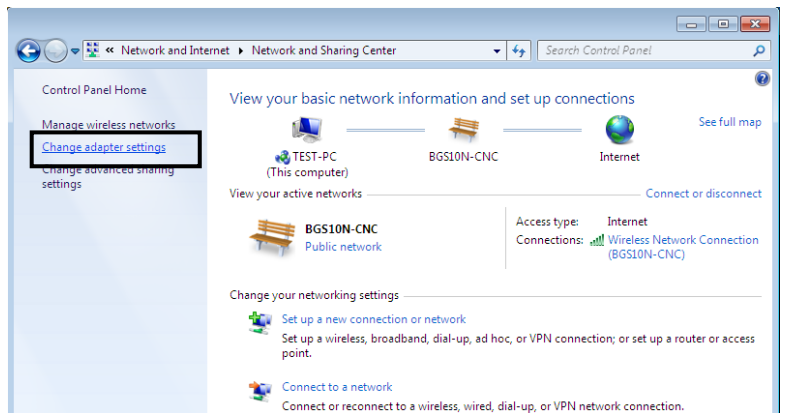


Configuring PC in Windows 7/8 (IPv4)

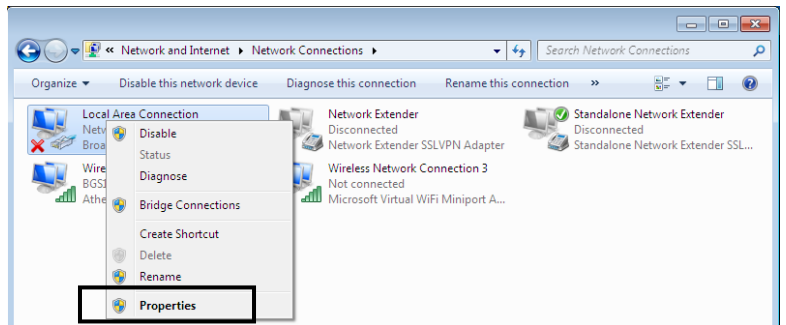
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



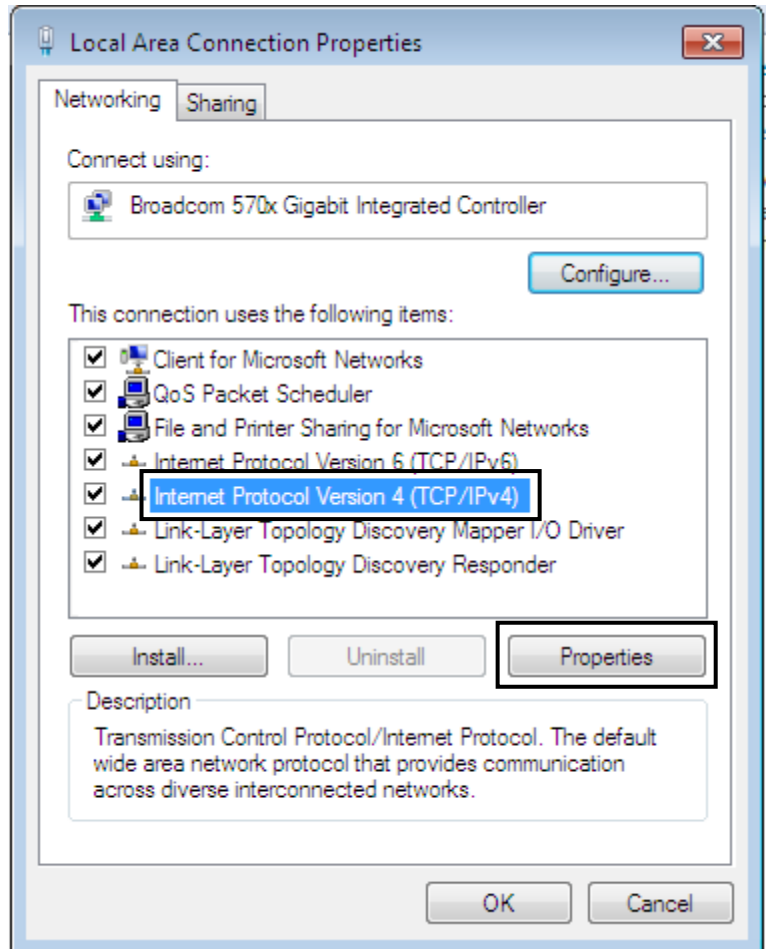
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



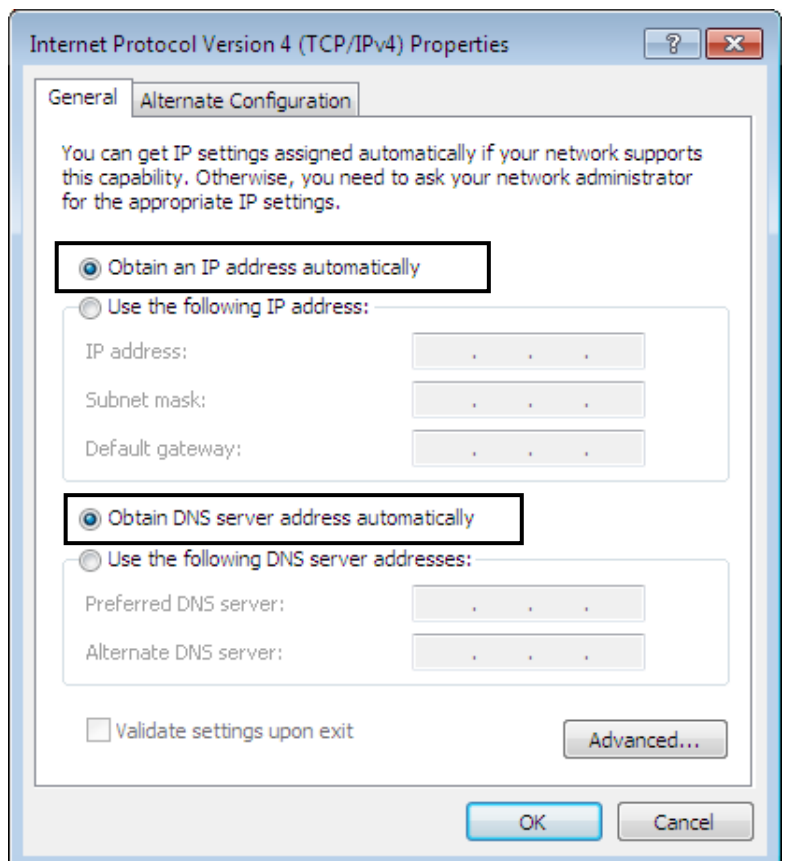
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

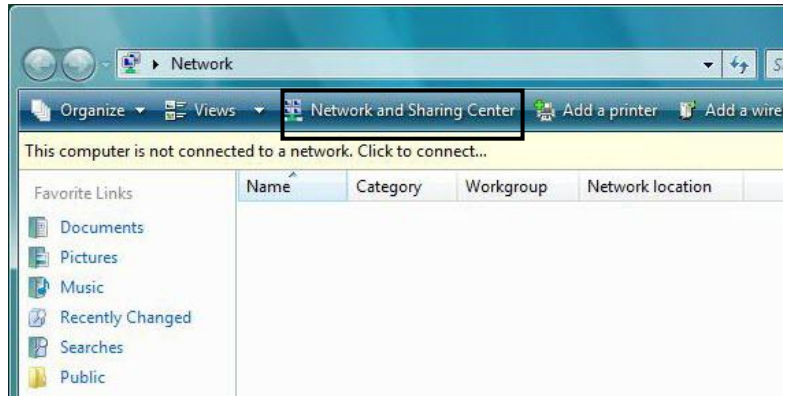


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

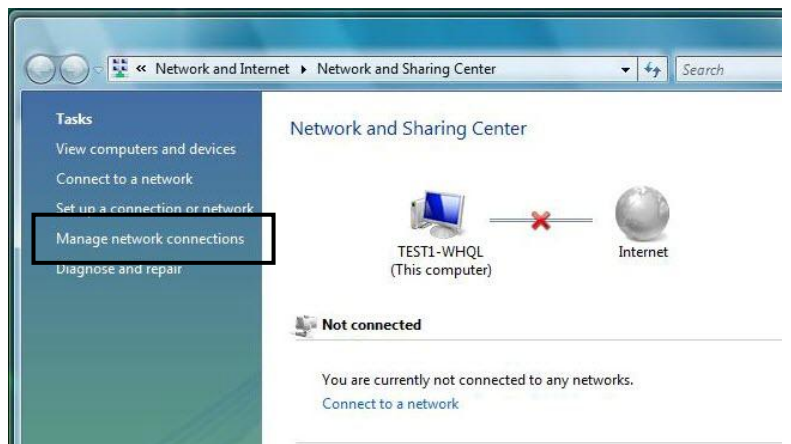


Configuring PC in Windows Vista (IPv4)

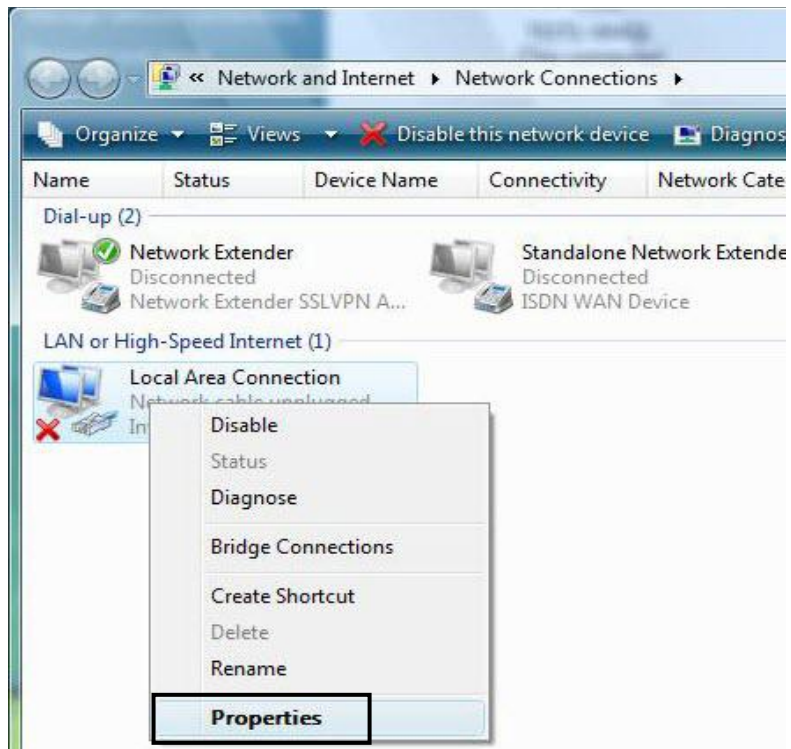
- 1. Go to **Start**. Click on **Network**.
- 2. Then click on **Network and Sharing Center** at the top bar.



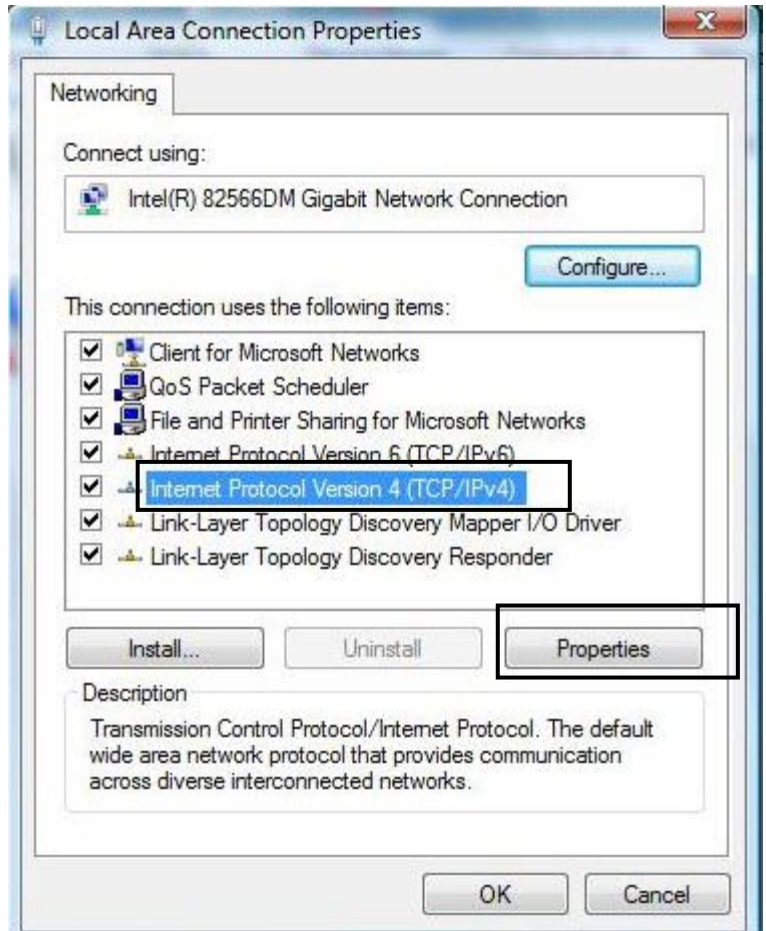
- 3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



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

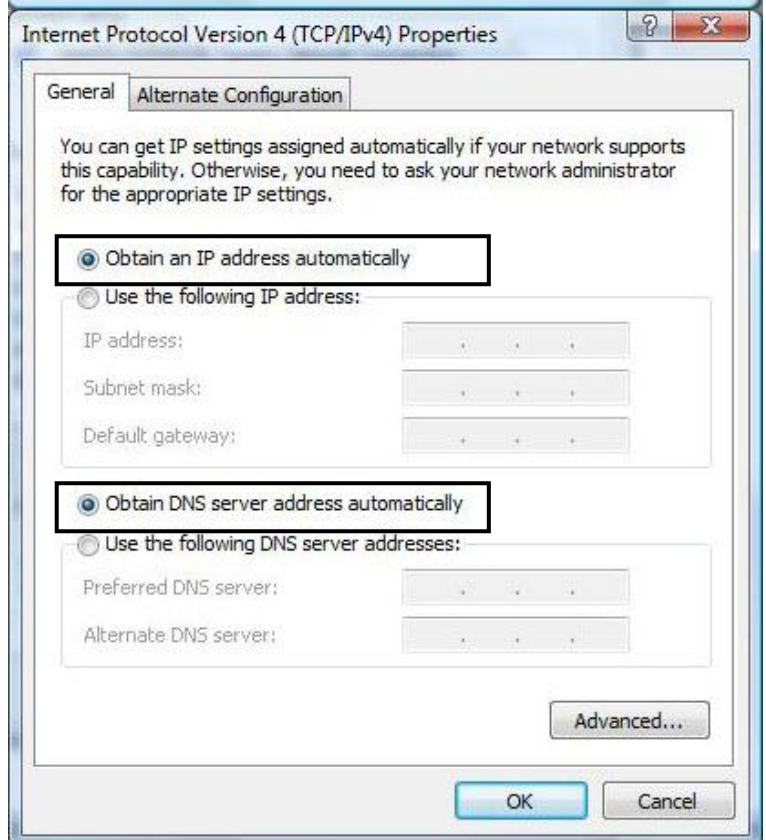


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



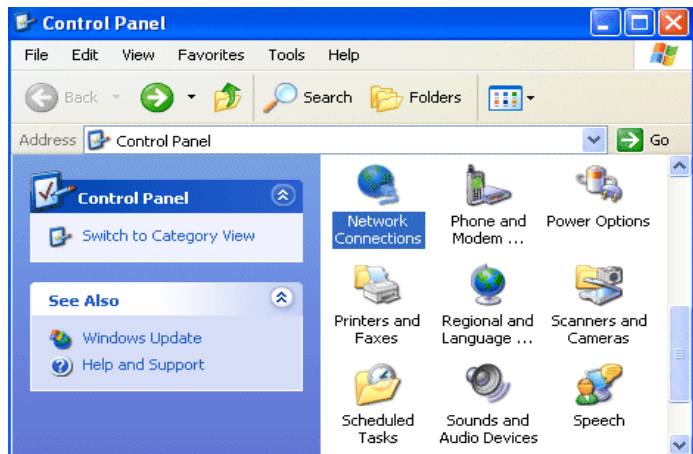
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

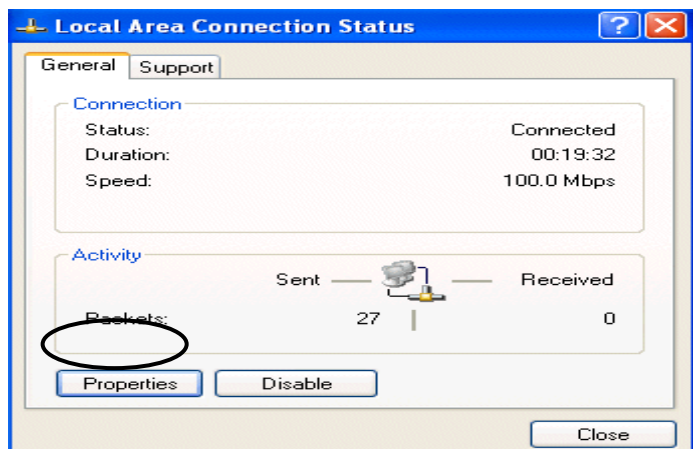


Configuring PC in Windows XP (IPv4)

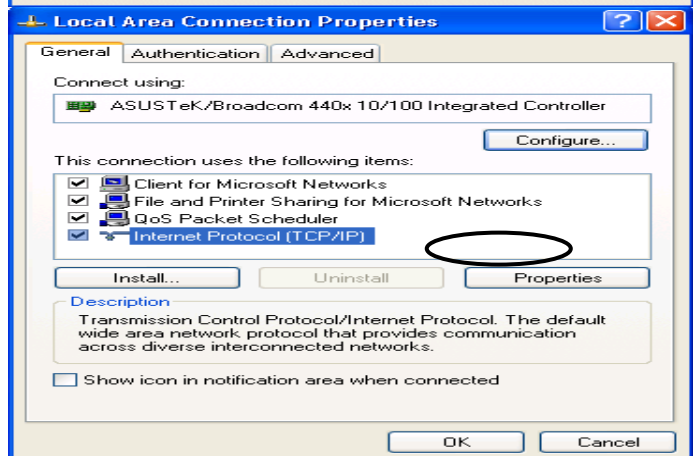
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



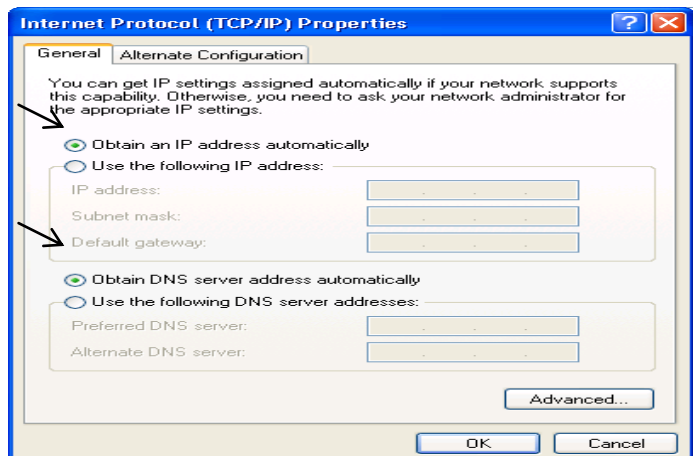
3. In the **Local Area Connection Status** window, click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.






5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.



6. Click **OK** to finish the configuration.

Network Configuration – IPv6

Configuring PC in Windows 10 (IPv6)

1. Click .
2. Click .
3. Then click on **Network and Internet**.

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

Related settings

Change adapter options

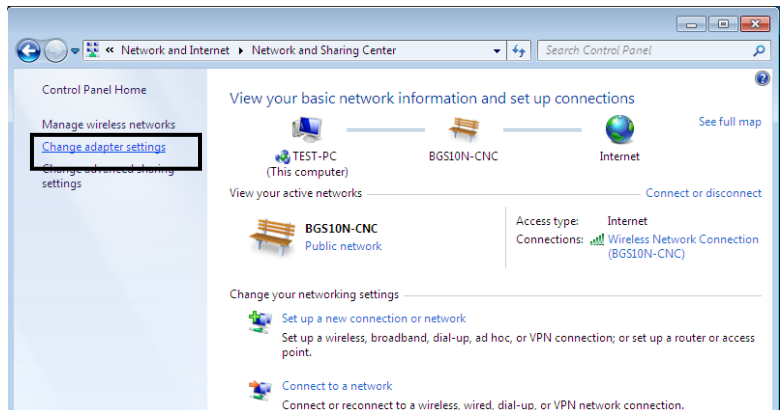
Change advanced sharing options

Network and Sharing Center

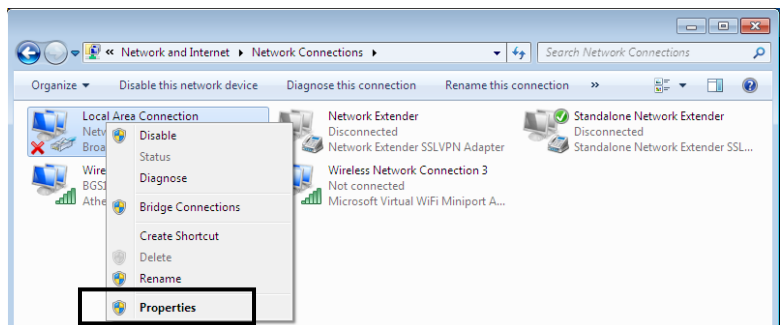
HomeGroup

Internet options

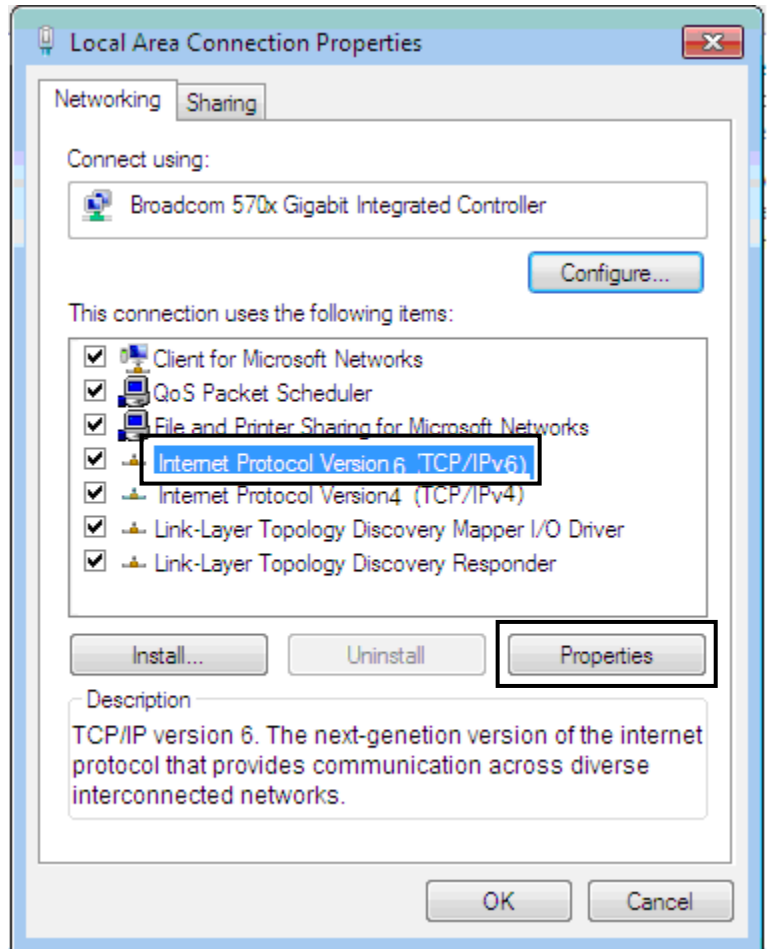
Windows Firewall



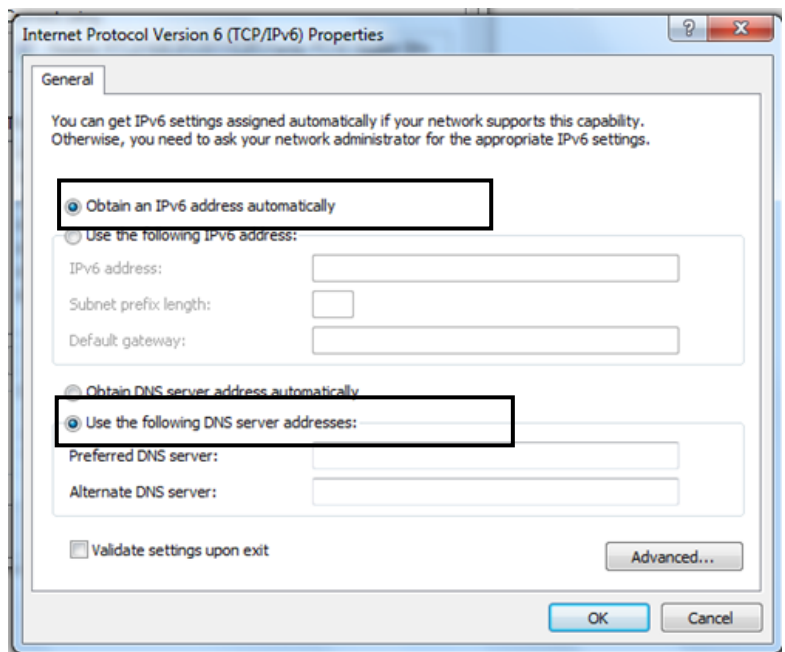
6. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

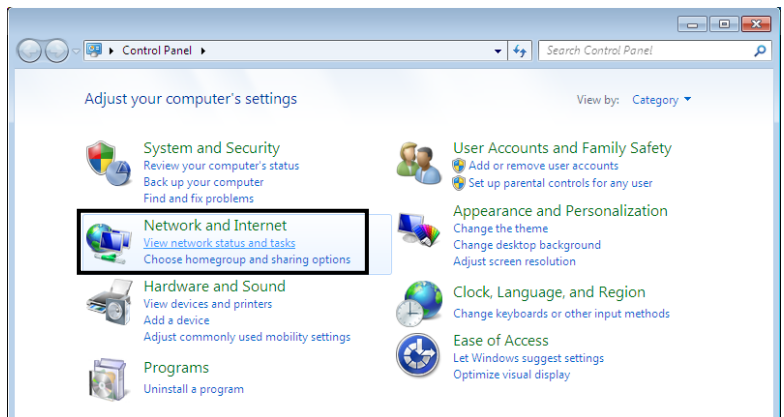


- 8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
- 9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

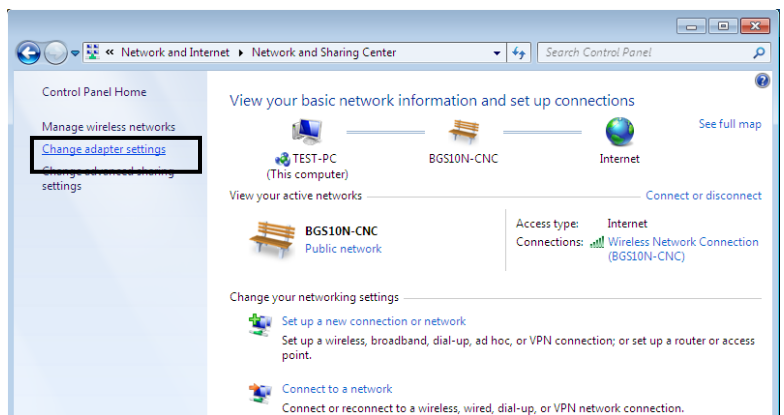


Configuring PC in Windows 7/8 (IPv6)

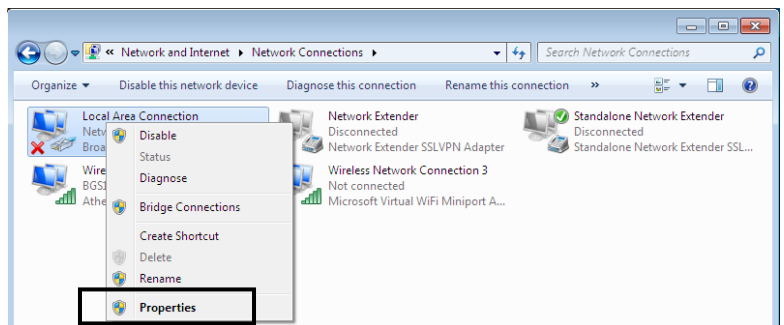
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



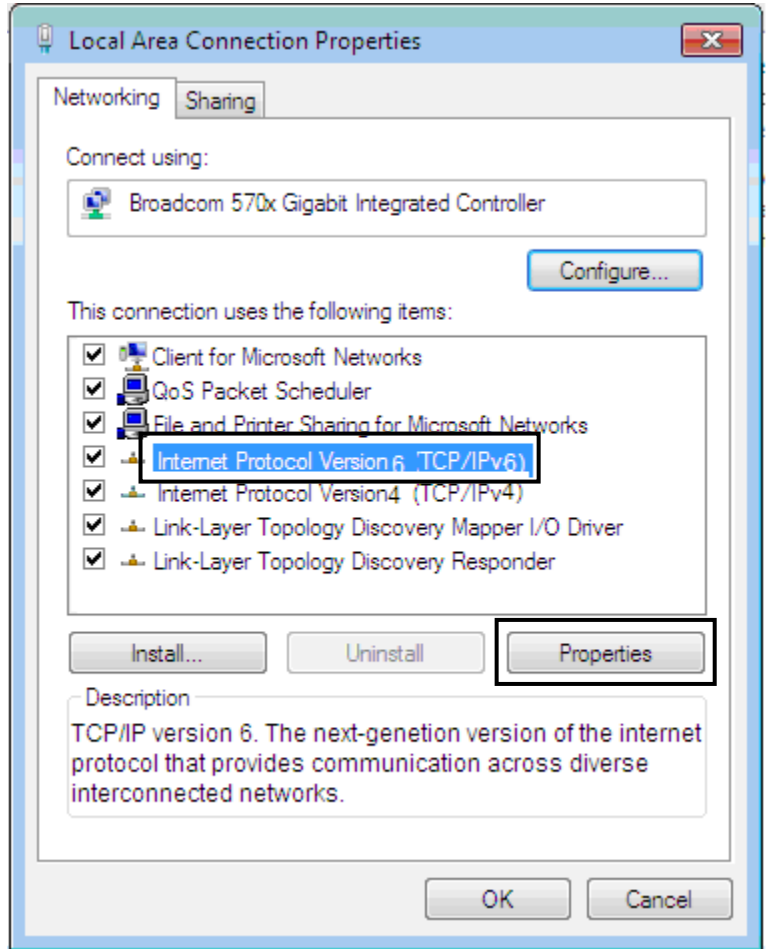
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



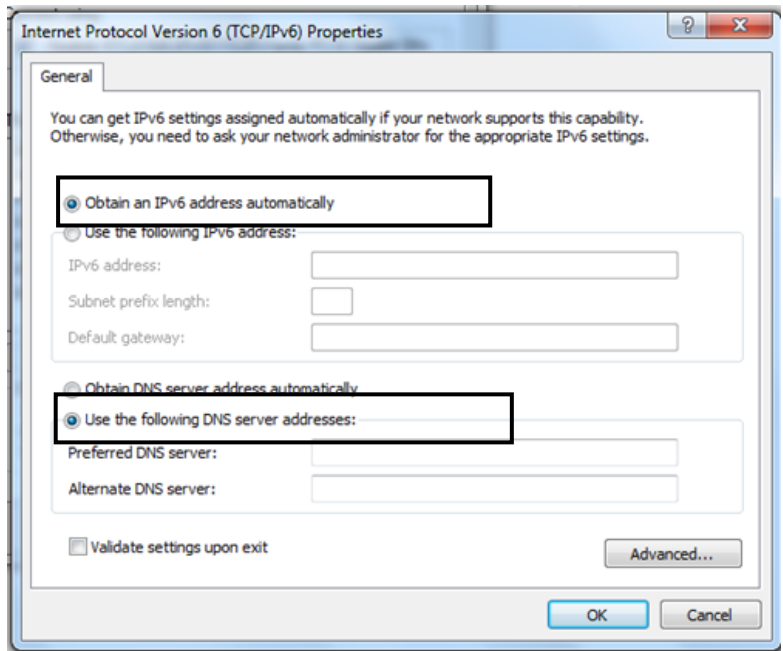
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

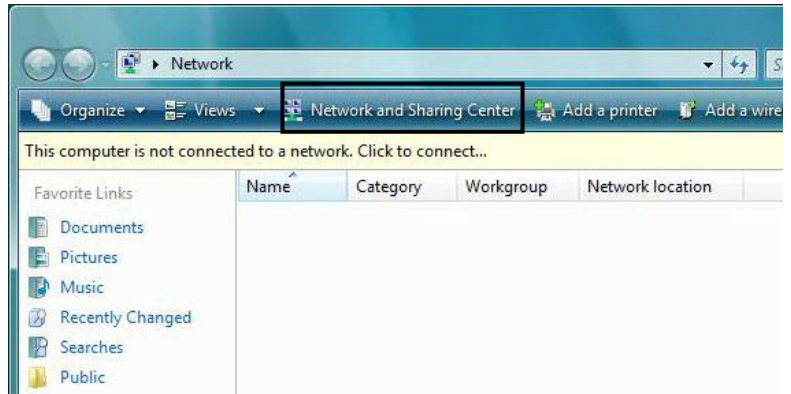


- 6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
- 7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv6)

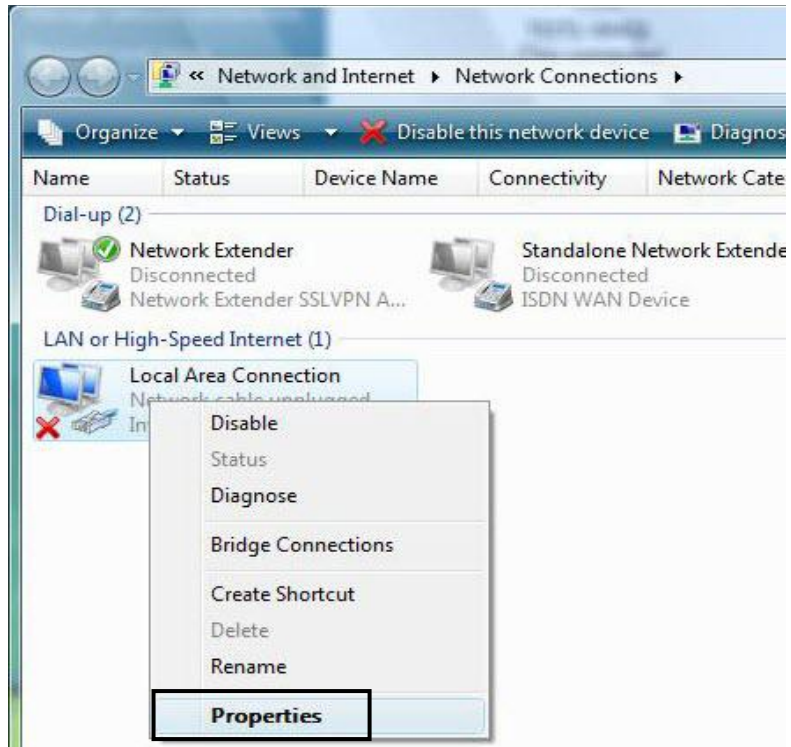
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



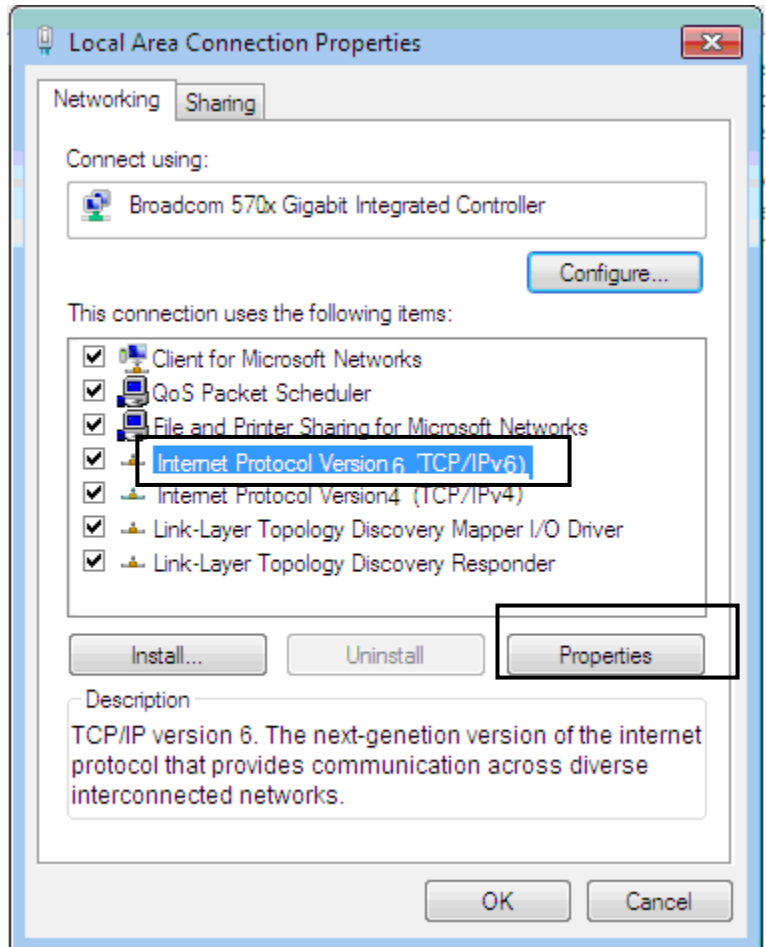
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



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

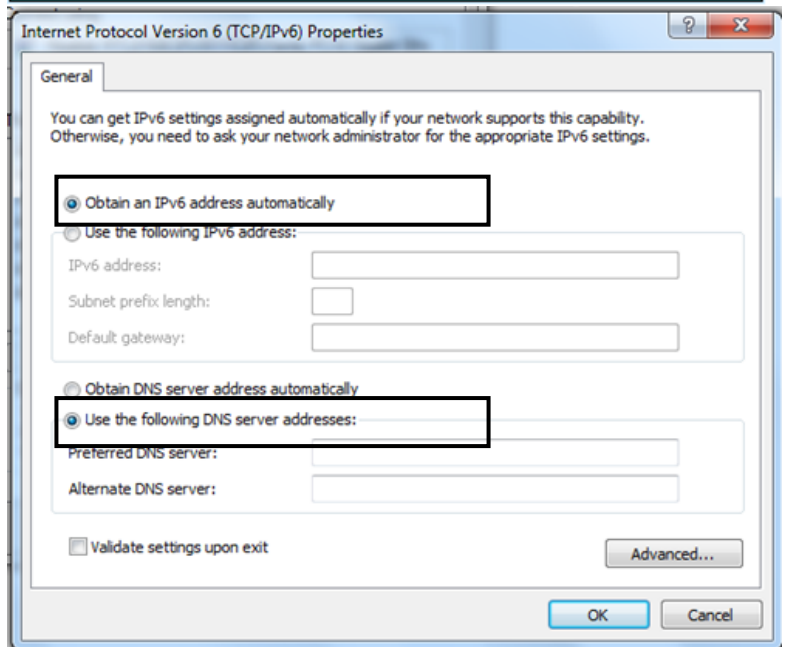


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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

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

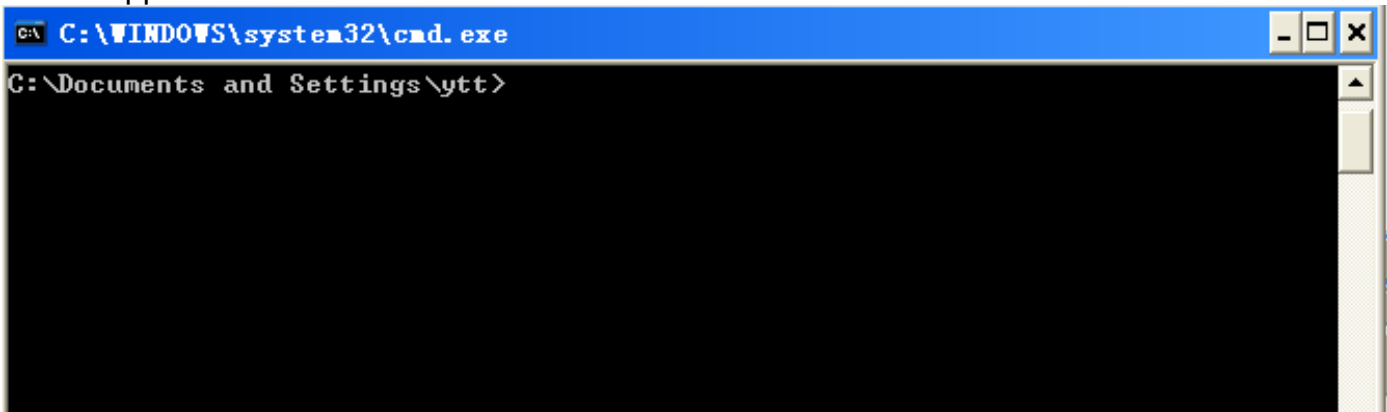


Configuring PC in Windows XP (IPv6)

IPv6 is supported by Windows XP, but you need to install it first.

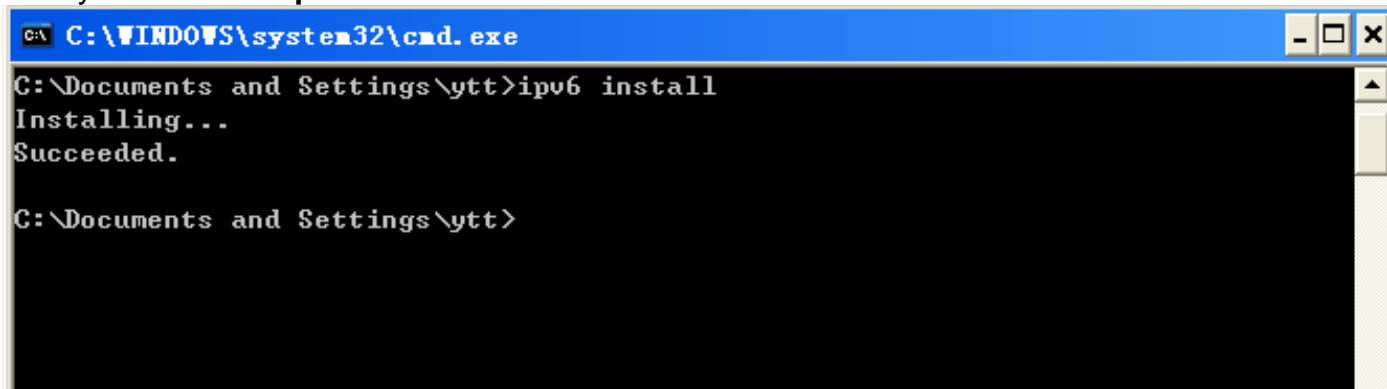
Please follow the steps to install IPv6:

1. On the Desktop, Click **Start > Run**, type **cmd**, then press **Enter** key in the keyboard, the following screen appears.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

Installation of IPv6 is now completed. Please test it to see if it works or not. .

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.

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



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

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

Device LAN IP Settings

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

DHCP Server:

- ✓ DHCP server is enabled.
- ✓ Start IP Address: 192.168.1.100
- ✓ IP pool counts: 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 user name and password window prompt appears.

Default username is **admin** and password is **admin** or 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.



Congratulations! You have successfully logged on to your BEC 6300VNL.

Once you have logged on to your 6300VNL via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	Device Info		Interface Setup
	System Status		- Internet
	System Log		- LAN
	3G/4G-LTE Status		- Wireless
	Statistics		- Wireless MAC Filter
	DHCP Table		- Loopback
	IPSEC Status		Dual WAN
	PPTP Status		- General Setting
	L2TP Status		Advanced Setup
	GRE Status		- Firewall
	OpenVPN Status		- Routing
	Disk Status		- Dynamic Routing
	VoIP Status		- NAT
	- VoIP Status		- Static DNS
	- VoIP Call Log		- QoS
ARP Table		- Interface Grouping	
		- Port Isolation	
		- Time Schedule	
		- Mail Alert	
		VPN	
		- IPSec	
		- PPTP Server & Client	
		- L2TP	
		- GRE	
		VoIP	
		- Basic	
		- Media	
		- Advanced	
		- Speed Dial	
		- Dial Plan	
		- Call Features	
		- NAT Traversal	
		Access Management	
		- Device Management	
		- SNMP	
		- Syslog	
		- Universal Plug & Play (UPnP)	
		- Dynamic DNS	
		- Access Control	
		- Packet Filter	
		- CWMP (TR-069)	
		- Parental Control	
		- SAMBA & FTP Server	
		- BECentral Management	
		Maintenance	
		- User Management	
		- Time Zone	
		- License	
		- Firmware & Configuration	
		- System Restart	
		- Auto Reboot	
		- Diagnostic Tool	


Please see the relevant sections of this manual for detailed instructions on how to configure your **BEC 6300VNL** gateway.

Status

In this section, you can check the router working status, including **Device Info**, **System Status**, **System Log**, **3G/4G-LTE Status**, **Statistics**, **DHCP Table**, **IPSec Status**, **PPTP Status**, **L2TP Status**, **GRE Status**, **Disk Status**, **VoIP Status** and **ARP Table**.

Device Info

It contains basic information of the device.

Device Information	
Model Name	BEC 6300VNL
Firmware Version	1.02b.rc6.dt10
MAC Address	00:04:ED:01:23:45
LAN	
IPv4	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Server	Enable
IPv6	
IP Address	
Prefix Length	
DHCPv6 Server	Enable Stateless
WAN	
Interface	3G/4G-LTE
Connection Time	0d: 1h:13m:22s
IPv4	
Status	Connected
IP Address	100.101.33.242
Subnet Mask	255.255.255.252
Default Gateway	100.101.33.241
DNS Server	168.95.1.1
3G/4G-LTE	
Signal Strength	 -72.00dbm
Network Name	"Chunghwa Telecom"
Card IMEI
Card IMSI

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

LAN

▶ **IPv4:**

IP Address: LAN port IPv4 address.

Subnet Mask: LAN port IP subnet mask.

DHCPv4 Server: LAN port DHCP role - Enabled, Relay or Disabled.

▶ **IPv6:**

IP Address: LAN port IPv6 address.

Prefix Length: The prefix length

DHCPv6 Server: The DHCP status.

WAN

Interface: WAN connection options, "EWAN" or "3G/4G-LTE".

Service: The WAN interface service index.

PPP Connection Time: the uptime of the PPP connection.

▶ **IPv4:**

Status: The connection status, either being connected or not in connected.

IP Address: WAN port IP address.

Subnet Mask: WAN port IP subnet mask.

Default Gateway: The IP address of the default gateway.

DNS Server: DNS information.

▶ **IPv6:**

Status: The IPv6 connection status.

IP Address: WAN port IPv6 address.

Prefix Length: The prefix length of IPv6 address.

Default Gateway: The IP address of the default gateway.

DNS Server: DNS information.

▶ **3G/4G-LTE:**

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

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

Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE module.

System Status

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

System Status	
CPU	
Usage	16%
Memory	
Total	61092 kB
Free	21304 kB
Cached	16072 kB
Refresh	

CPU

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

Memory

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

System Log

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

System Log	
<pre> Jan 1 00:00:59 syslogd started: BusyBox v1.00 (2017.07.12-06:10+0000) Jan 1 00:01:01 DNS[3085]: started, version 2.72 cachesize 150 Jan 1 00:01:01 DNS[3085]: read host file - 1 addresses Jan 1 00:01:02 CC: Kill VoIP Jan 1 00:01:02 CC: Kill VoIP Done Apr 10 00:00:01 CC: Call VoIP Apr 10 00:00:01 CC: VoIP task Running Apr 10 00:00:01 PPOELOGIN: bind service port Apr 10 00:00:02 PPOELOGIN: begin service loop Apr 10 00:00:03 syslog: [3GFUN]: Issue gobi_services begin Apr 10 00:00:03 syslog: [3GFUN]: Issue gobi_services ... Apr 10 00:00:04 syslog: [GB_Service]: Connect2Gobi(1) successfully!!! Apr 10 00:00:04 syslog: [GB_Service]: Connect2Gobi(2) successfully!!! Apr 10 00:00:04 syslog: Recover DNS configuration null ... Apr 10 00:00:06 WEB: WEB login failed! Apr 10 00:00:29 syslog: [3GFUN]: SIM Card Not Found, Mobile profile stop Apr 10 00:00:35 WEB: WEB login failed! </pre>	
Refresh Backup	

Refresh: Press this button to refresh the statistics.

3G/4G-LTE Status

This page contains 3G/4G-LTE connection information.

3G/4G-LTE Status	
WAN	3G/4G-LTE ▼
Status	Up
SIM Status	SIM Card Not Found
Signal Strength	
Network Name	
Cell ID	
Card IMEI	359225054110101
Card IMSI	
Network Mode	
Network Band	
Refresh	

Status: The current status of the 3G/4G-LTE connection.

SIM Status: Identify current status of the SIM, Activate or SIM Card Not Found.

Signal Strength: The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G-LTE Signal Strength LED indicates the signal strength as well.

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

- ▶ RSRP (Reference Signal Receiving Power): is the average power of all resource elements which carry cell-specified reference signals over the entire bandwidth.
- ▶ RSRQ (Reference Signal Receiving Quality): measures the signal strength and is calculated based on both RSRP and RSSI.
- ▶ RSSI (Received Signal Strength Indicator): parameter which provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise.
- ▶ SNR (Signal Noise Ratio): is also a measure of signal quality as well. It is widely used by the operators as it provides a clear relationship between RF conditions and throughput.

Note: Some LTE modules do not provide this information.

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

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

Card IMEI: The unique identification number that is used to identify the 3G/4G-LTE module.

Card IMSI: The international mobile subscriber identity used to uniquely identify the 3G/4G-LTE module.

Network Mode: Display current network operating mode.

Network Band: Indicated the current radio frequency band used.

Refresh: Press this button to refresh the statistics.

Statistics

❖ EWAN

Statistics			
Traffic Statistics			
Interface	<input checked="" type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input type="radio"/> 3G/4G-LTE USB <input type="radio"/> Ethernet <input type="radio"/> Wireless		
Transmit Statistics		Receive Statistics	
Transmit Frames	5	Receive Frames	0
Transmit Multicast Frames	5	Receive Multicast Frame	0
Transmit Total Bytes	478	Receive Total Bytes	0
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh	None ▼

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Traffic Speed

Transmit / Receive Speed: Display current transmit and receive speeds of the interface.

Auto Refresh: Automatic recheck transmit and receive speed in every 10-second, 30-seconds, or no check.

Refresh: Click button to refresh the statistics manually.

❖ 3G/4G-LTE

Take 3G/4G-LTE as an example to describe the following connection transmission information.

Statistics			
Traffic Statistics			
Interface	<input type="radio"/> EWAN <input checked="" type="radio"/> 3G/4G-LTE <input type="radio"/> 3G/4G-LTE USB <input type="radio"/> Ethernet <input type="radio"/> Wireless		
Transmit Statistics		Receive Statistics	
Transmit Frames of Current Connection	0	Receive Frames of Current Connection	0
Transmit Bytes of Current Connection	0	Receive Bytes of Current Connection	0
Transmit Total Frames	0	Receive Total Frames	0
Transmit Total Bytes	0	Receive Total Bytes	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh			Auto Refresh <input type="text" value="None"/>

Interface: List all available network interfaces in the router. You are currently checking on the physical status of **3G/4G-LTE** interface.

Transmit Statistics

Transmit Frames of Current Connection: This field displays the total number of 3G/4G-LTE frames transmitted until the latest second for the current connection.

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

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

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

Receive Statistics

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

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

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

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

Traffic Speed

Transmit / Receive Speed: Display current transmit and receive speeds of the interface.

Auto Refresh: Automatic recheck transmit and receive speed in every 10-second, 30-seconds, or no check.

Refresh: Click button to refresh the statistics manually.

❖ **3G/4G_LTE via USB port**

Take 3G/4G-LTE USB as an example to describe the following connection transmission information.

Statistics		
Traffic Statistics		
Interface	<input type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input checked="" type="radio"/> 3G/4G-LTE USB <input type="radio"/> Ethernet <input type="radio"/> Wireless	
Transmit Statistics	Receive Statistics	
Transmit Frames of Current Connection	0	Receive Frames of Current Connection 0
Transmit Bytes of Current Connection	0	Receive Bytes of Current Connection 0
Transmit Total Frames	0	Receive Total Frames 0
Transmit Total Bytes	0	Receive Total Bytes 0
<input type="button" value="Refresh"/>		Auto Refresh <input type="button" value="None"/> ▾

Interface: List all available network interfaces in the router. You are currently checking on the physical status of **3G/4G-LTE** interface.

Transmit Statistics

Transmit Frames of Current Connection: This field displays the total number of 3G/4G-LTE frames transmitted until the latest second for the current connection.

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

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

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

Receive Statistics

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

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

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

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

Auto Refresh: Automatic recheck transmit and receive speed in every 10-second, 30-seconds, or no check.

Refresh: Click button to refresh the statistics manually.

❖ Ethernet

Statistics			
Traffic Statistics			
Interface	<input type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input type="radio"/> 3G/4G-LTE USB <input checked="" type="radio"/> Ethernet <input type="radio"/> Wireless		
Transmit Statistics		Receive Statistics	
Transmit Frames	5165	Receive Frames	2629
Transmit Multicast Frames	3410	Receive Multicast Frame	1109
Transmit Total Bytes	2713989	Receive Total Bytes	770531
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.40KBps	Receive Speed	0.16KBps
Refresh		Auto Refresh <input type="text" value="None"/> ▼	

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Traffic Speed

Transmit / Receive Speed: Display current transmit and receive speeds of the interface.

Auto Refresh: Automatic recheck transmit and receive speed in every 10-second, 30-seconds, or no check.

Refresh: Click button to refresh the statistics manually.

❖ Wireless

Statistics			
Traffic Statistics			
Interface	<input type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input type="radio"/> 3G/4G-LTE USB <input type="radio"/> Ethernet <input checked="" type="radio"/> Wireless		
Transmit Statistics		Receive Statistics	
Transmit Frames	11364	Receive Frames	84885
Transmit Error Frames	0	Receive Error Frames	102956
Transmit Drop Frames	0	Receive Drop Frames	102956
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh <input type="text" value="None"/>	

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

Transmit Statistics

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

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

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

Receive Statistics

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

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

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

Refresh: Press this button to refresh the statistics.

Traffic Speed

Transmit / Receive Speed: Display current transmit and receive speeds of the interface.

Auto Refresh: Automatic recheck transmit and receive speed in every 10-second, 30-seconds, or no check.

Refresh: Click button to refresh the statistics manually.

DHCP Table

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

▼ DHCP Table				
Index	Host Name	IP Address	MAC Address	Expire Time
1	Billion-HC-ee	192.168.1.101	00:C0:9F:D1:E1:CA	0days 23:36:1

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

Host Name: Display the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

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

Disk Status

▼ Disk status		
Partition	Disk Space(KB)	Free Space(KB)
usb1_1	1953988	1732288

Partition: Display the USB storage partition.

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

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

IPsec Status

IPsec Status								
Index	Action	Connection Name	Active	Connection State	Statistics	Remote Gateway	Remote Network	Local Network
0	<input type="button" value="Connect"/> <input type="button" value="Drop"/>	H-to-B	Yes	Phase1 Established Phase2 Established	191408/43308	69.121.1.30	192.168.0.0/24	192.168.1.0/24
<input type="button" value="Refresh"/>								

Index #: The numeric IPsec VPN tunnel/ rule.

Action: Display Connect or Drop the connection.

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

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

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

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

Remote Gateway: Display remote gateway IP address.

Remote Network: Display remote local IP address and Netmask.

Local Network: Display local IP address and Netmask.

Refresh: Click to refresh the page.

PPTP Status

❖ PPTP Server

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

Index #: The numeric PPTP VPN tunnel/ rule.

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

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

Connection State: Display the VPN connection status.

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

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

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

Refresh: Click to refresh the page.

❖ PPTP Client

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

Index #: The numeric PPTP VPN tunnel/ rule.

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

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

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

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

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

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

Refresh: Click to refresh the page.

L2TP Status

L2TP Status						
Index	Connection Name	Active	Connection State	Connection Mode	Connection Type	Tunnel Remote IP Address
1	HS-LL	Yes	Connected	Dial in	Lan to Lan	192.168.1.200

Refresh

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

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

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

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

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

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

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

Refresh: Click to refresh the page.

GRE Status

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

Index #: The numerical GRE tunnel/rule indication.

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

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

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

Remote Gateway IP: Display the remote gateway IP address.

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

VoIP Status

❖ VoIP Status

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

VoIP Status			
Phone Number	Host	Status	Registered Time
7154500000	metaprosyehibordun.net:5060	Registered	Fri, 06 Sep 2013 08:10:28
7154500100	metaprosyehibordun.net:5060	Registered	Fri, 06 Sep 2013 08:10:27

Refresh

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

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

Status: The status of the registered SIP account.

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

❖ VoIP Call Log

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

VoIP Call Log						
Phone	1					
Incoming Call Log	Outgoing Call Log	Missed Call Log				
Incoming Call Log						
Start-Time	Caller Name	Caller Number	Answer Time	End Time	Talk Duration	Status

Refresh

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

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

Start-Time: The start time of the call

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

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

Answer Time: The answer time of phone call

End Time: The end time of the call

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

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

ARP Table

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

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

#: The numeric table list indicator.

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

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

Quick Start

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

▼ Quick Start

The 'Quick Start' wizard will guide you to configure the device to connect to your ISP(Internet Service Provider).
Please follow the 'Quick Start' wizard step by step to configure the device. It will allow you to have Internet access within minutes.

Run Wizard

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

▼ Quick Start

The Wizard will guide you through these five quick steps. Begin by clicking on NEXT.

Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your wireless connection

Step 4. Set your internet connection

Step 5. Confirm the configuration and save it

Next

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

Step 1 – Password

Set new password of the “admin” account to access for router management. The default is “admin” or a unique 12-digit password can be found on the device label.

Once changed, please use this new password next time when accessing to the router. Click **NEXT** to continue.

▼ Quick Start - Password

You may change the admin account password by entering in a new password. Click NEXT to continue.

New Password

Confirm Password

Back Next

Step 2 – Time Zone

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

▼ Quick Start - Time Zone

Select the appropriate time zone for your location and click NEXT to continue.

Time Zone

Back Next

Step 3 – Wireless

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

Quick Start - Wireless

Configure your wireless network, authentication type and click NEXT to continue.

Access Point	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated	
SSID	BEC223	
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Channel	UNITED STATES ▼	06 ▼
Security Type	Mixed WPA2/WPA-PSK ▼	
WPA Algorithms	TKIP+AES ▼	
Pre-Shared Key	14F812CE	(8-63 characters or 64 Hex string)
Key Renewal Interval	600	seconds (10 ~ 4194303)

Back Next

Step 4 – ISP Connection Type

Set up your Internet connection.

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

Quick Start - ISP Connection Type

Dynamic IP Address

WAN Interface	EWAN ▼
Service	0 ▼
ISP	<input type="radio"/> Dynamic IP Address (Dynamic IP Address) <input type="radio"/> Static IP Address (Choose this option to set static IP information provided to you by your ISP.) <input checked="" type="radio"/> PPPoE (Choose this option if your ISP uses PPPoE.) <input type="radio"/> Bridge Mode (Choose this option if your ISP uses Bridge Mode.)

Back Next

4.2 If selected **3G/4G-LTE or 3G/4G-LTE USB** (for example).

Quick Start - ISP Connection Type

Dynamic IP Address

WAN Interface	3G/4G-LTE ▼
---------------	-------------

Back Next

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

Quick Start - 3G/4G-LTE

Enter the 3G information provided to you by your ISP. Click NEXT to continue.

TEL No.	*99***1#
APN	internet
Username	
Password	
PIN	

Back Next

Click Next to save changes.

4.2 If selected **EWAN / PPPoE**, please enter PPPoE account information provided by your ISP. Click **NEXT** to continue.

▼ Quick Start - PPPoE

Provide the PPPoE information. Click NEXT to continue.

Username

Password

Step 5 – Quick Start Completed

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

▼ Quick Start - Quick Start Completed

Quick Start Completed !!

The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click NEXT to exit the Setup Wizard.

▼ Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

Switch to **Status > Device Info** to view the status.

Configuration

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

These functions are described in the following sections.

Interface Setup

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

Internet

❖ **EWAN**

❖ EWAN (Cont.)

Internet	
WAN Interface	EWAN
Multi Service	
Service Index	0 Services Summary
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
IPv4/IPv6	
IP Version	<input type="radio"/> IPv4 <input checked="" type="radio"/> IPv4/IPv6 <input type="radio"/> IPv6
ISP Connection Type	
ISP	<input type="radio"/> Dynamic IP Address <input type="radio"/> Static IP Address <input checked="" type="radio"/> PPPoE <input type="radio"/> Bridge Mode
802.1q Options	
802.1q	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
VLAN ID	0 (range: 0~4095)
PPPoE	
Username	<input type="text"/>
Password	<input type="text"/>
Bridge Interface for PPPoE	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Connection Setting	
Connection	<input checked="" type="radio"/> Always On (Recommended) <input type="radio"/> Connect Manually
TCP MSS Option	TCP MSS 0 bytes(0 means use default)
IP Options	
IP Common Options	
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
TCP MTU Option	TCP MTU 0 bytes(0 means use default: 1492)
IPv4 Options	
Get IP Address	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable
Dynamic Route	RIP1 Direction None
IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPv6 Options	
Obtain IPv6 DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
MLD Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC Spoofing	
MAC Spoofing	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/>	

Multi Service

Service Index: The index marks the EWAN interface of different ISP type, ranging from 0-7.

Service Summary: The overall service information.

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

Status: Select whether to enable the service.

IPv4/IPv6

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

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

- ▶ **Dynamic IP:** Select this option if your ISP provides you an IP address automatically.
- ▶ **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form. IP address from by four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.
- ▶ **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.
- ▶ **Bridge:** Select this mode if you want to use this device as an OSI Layer 2 device like a switch.

802.1q Options

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

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

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

Username: Enter the user name provided by your ISP.

Password: Enter the password provided by your ISP.

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

Connection Setting

Connection:

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

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

IP Common Options

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

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

IPv4 Options

Get IP Address: Choose Static or Dynamic

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

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

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

NAT: Select Enable if you use this router to hold a group of PCs to get access to the internet.

Dynamic Route:

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

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

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

IPv6 Address: Type the WAN IPv6 address from your ISP.

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

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

MLD Proxy: MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a

Multicast Management protocol for IPv6 multicast packets.

MAC Spoofing

MAC Spoofing: Use it to change factory-default MAC temporarily.

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

When router's Internet configuration is finished successfully, go to status to review connection status.

❖ 3G/4G-LTE

Internet	
WAN Interface	3G/4G-LTE ▾
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Usage Allowance ▶	<input type="checkbox"/> Enable
IP Pass-Through Mode	<input type="checkbox"/> Enable
Network Mode	Automatic ▾
PLMN Selection	Operator Numeric <input type="text"/> RAT <input type="text"/> <input type="button" value="Scan"/>
TEL No.	*99***1#
Dual APN	Single APN ▾
APN	internet
Username	<input type="text"/>
Password	<input type="text"/>
PIN	<input type="text"/>
Connection	<input checked="" type="radio"/> Always On (Recommended)
Keep Alive	<input type="radio"/> Yes <input checked="" type="radio"/> No
Keep Alive IP	<input type="text"/>
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
NAT	Enable ▾
SMS Control ▶	Disabled
<input type="button" value="Save"/>	

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

IP Pass-Through Mode: When **enabled**, BEC 6300VNL is in bridge mode and will not obtain a WAN IP address, features such as routing capabilities, NAT, firewall, etc, will be disabled by default. However, the client router behind the BEC 6300VNL can get a WAN IP address instead.

When **disabled**, BEC 6300VNL is in router mode that it handles a WAN IP address and all routing-related features become available.

LTE Mode (This feature is not supported in some LTE modules): Display current selected LTE frequency band. To change the band, please click “**LTE Band**” to access to the band selection page.

LTE Band

LTE Band: A list of available LTE bands to choose from.

LTE Mode	
Parameters	
LTE Band	B12 ▾
***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.	
<input type="button" value="Apply"/>	<input type="button" value="Save Config & Restart"/>

LTE Antenna Diversity (This feature is not supported in some LTE modules): When **enabled**, the auxiliary antenna will be activated. With **disabled**, only the primary antenna is receiving and transmitting data.

To change it, please click “**LTE Antenna Diversity**” to access to the LTE antenna diversity selection page.

NOTE: When using Yagi antenna, please **DISABLE** the Antenna Diversity feature for utmost performance.

LTE Antenna Diversity

To enable or disable the LTE antenna diversity feature.

The screenshot shows a configuration window titled 'LTE Mode'. Under the 'Parameters' section, there is a dropdown menu for 'LTE Antenna Diversity'. Below the dropdown, a blue message reads: '***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.' At the bottom, there are two buttons: 'Apply' and 'Save Config & Restart'.

PLMN (Public Land Mobile Network) Selection: Either manually enter the information or click **Scan** button to scanning all closest base stations in the area.

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

Dual APN*(This feature is not supported in some LTE modules): BEC 6300VNL can support up to two (2) APNs. Select **Single / Dual** or a **different LTE/3G APN**.

- ▶ **APN (3G):** If select **LTE/3G with different APN**, enter the APN here.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN 'internet' for their portal. The default value is "internet".

PDN Type: The IP type for PDN connections. Available types are **IPv4**, **IPv6**, and **IPv4v6**.

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

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

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

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

Keep Alive IP: Enter the IP address that the router can ping the IP to find whether the connection is on or not, if not, router will recover the connection.

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

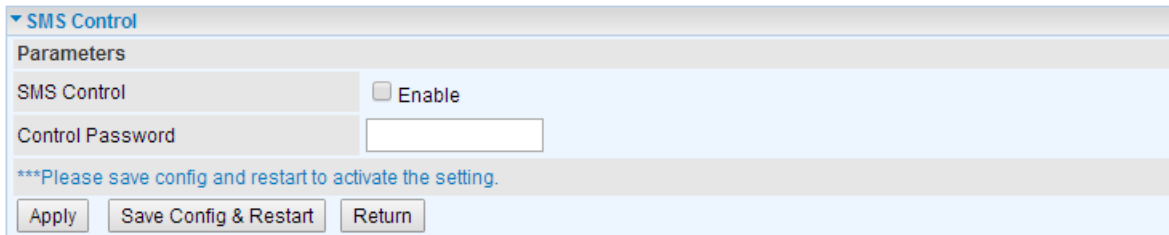
NAT: Select this option to Disabled/Enable the NAT (Network Address Translation) function. Enable NAT to grant multiples devices in LAN to access to the Internet through a single WAN IP.

MTU: Enter the maximum packet that can be transmitted. Default MTU **0** means it is set to 1500 bytes.

SMS Control: Enable to send a SMS message to reboot or get the current 3G/ 4G LTE status information from the 6300VNL.

NOTE: You must obtain the phone number on the SIM card. Please contact with your network / service provider for more information.

SMS Control



The screenshot shows a configuration window titled "SMS Control". Under the "Parameters" section, there is a checkbox labeled "SMS Control" which is currently unchecked, with the text "Enable" next to it. Below this is a text input field labeled "Control Password" which is empty. A blue italicized note below the input field reads: "***Please save config and restart to activate the setting." At the bottom of the window, there are three buttons: "Apply", "Save Config & Restart", and "Return".

SMS Control: Check to enable this feature.

Control Password: Preconfig a password to automatically reboot 6300VNL via a SMS message. Password length is up to 10 characters. (Valid characters: 0~9, A~Z and a~z)

Example:

6300VNL obtains the phone number, +513 123 4567, on the SIM card

1. Send a text message, **reboot#<password>**, to device (513 123 4567). 6300VNL will reboot the system once receiving this message.
2. Send ***60**, will get 3G/ 4G LTE status message. It includes IMEI number, System up time, Network mode, Signal strength, WAN IP, Connection time.

When router's Internet configuration is finished successfully, you can go to the **Status** to check connection information.

❖ 3G/4G-LTE via USB

▼ Internet	
WAN Interface	3G/4G-LTE USB ▼
Status	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Usage Allowance ▶	<input type="checkbox"/> Enable
IP Pass-Through Mode	<input type="checkbox"/> Enable
Network Mode	Automatic ▼
TEL No.	*99***1#
Dual APN	Single APN ▼
APN	internet
Authentication Protocol	Disable ▼
Username	<input type="text"/>
Password	<input type="text"/>
PIN	<input type="text"/>
Connection	<input checked="" type="radio"/> Always On (Recommended)
Keep Alive	<input type="radio"/> Yes <input checked="" type="radio"/> No
Keep Alive IP	<input type="text"/>
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
NAT	Enable ▼
MTU	1428 (0 means use default:1500)
<input type="button" value="Save"/>	

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

Usage Allowance: Enable and click “**Usage Allowance**” for further setting configuration of your 4G/LTE data usage.

Usage Allowance

▼ Usage Allowance	
Parameters	
Mode	<input type="radio"/> Volume-based Only Download ▼ <input type="text" value=""/> MB data volume per month included <input checked="" type="radio"/> Time-based 720 <input type="text" value=""/> hours per month included The billing period always begins on day 1 <input type="text" value=""/> of a month.
Over usage allowance action	None ▼
Save the statistics to ROM	Disable ▼
<input type="button" value="Save"/> <input type="button" value="Back"/>	

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

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

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

Over usage allowance action: Here are actions to perform when mobile data usage, defined in **Mode**, reached to its maximum.

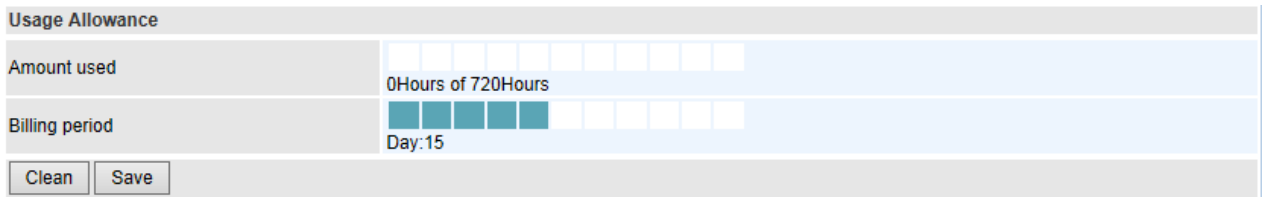
- ▶ **None:** No action taken
- ▶ **Disconnect:** Disconnect mobile connection

- ▶ **Email Alert:** Send an e-mail alert and keep the mobile connection alive.
- ▶ **Email Alert and Disconnect:** Disconnect mobile connection after an alert e-mail is being sent.

Save the statistics to ROM:

- ▶ **Every one hour:** Activate the 3G/4G-LTE statistics on data usage and this info will get updated and saved to the internal memory (ROM) in every hour.

Once the feature is turned on, you can see the amount of data used and how many days left before next billing cycle starts. Go to **Status >> 3G/4G-LTE Status** page for details.



NOTE: This statistic information will get deleted after a factory reset.

- ▶ **Disable:** No action taken

IP Pass-Through Mode: When **enabled**, BEC 6300VNL is in bridge mode and will not obtain a WAN IP address, features such as routing capabilities, NAT, firewall, etc, will be disabled by default. However, the client router behind the BEC 6300VNL can get a WAN IP address instead.

When **disabled**, BEC 6300VNL is in router mode that it handles a WAN IP address and all routing-related features become available.

Network Mode: There are 8 options of service standards: “Automatic”, “UMTS 3G only”, “GSM 2G Only”, “UMTS 3G Preferred”, “GSM 2G Preferred”, “GSM and UMTS Only”, “LTE Only”, “GSM, UMTS, LTE”. If you are not sure which mode to use, you may select **Automatic** to auto detect the best mode for you.

PLMN (Public Land Mobile Network) Selection: Either manually enter the information or click **Scan** button to scanning all closest base stations in the area.

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

Dual APN: Check with the dongle module vendor to see if dual APNs can be supported.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some 3G operators use the APN ‘internet’ for their portal. The default value is “internet”.

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

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

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

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

Interface Setup – Internet (3G/4G_LTE via USB Port)

Keep Alive IP: Enter the IP address that the router can ping the IP to find whether the connection is on or not, if not, router will recover the connection.

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

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

MTU: Enter the maximum packet that can be transmitted. Default MTU **0** means it is set to 1500 bytes.

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

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

When router's Internet configuration is finished successfully, go to status to review connection status.

LAN

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

LAN

IPv4 Parameters

IP Address	<input type="text" value="192.168.1.254"/>
IP Subnet Mask	<input type="text" value="255.255.255.0"/>
Alias IP Address	<input type="text" value="0.0.0.0"/> (0.0.0.0 means to close the alias ip)
Alias IP Subnet Mask	<input type="text" value="0.0.0.0"/>
IGMP Snooping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Dynamic Route	RIP1 <input type="text"/> Direction <input type="text" value="None"/>

DHCPv4 Server

DHCPv4 Server	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay
Start IP	<input type="text" value="192.168.1.100"/>
IP Pool Count	<input type="text" value="100"/>
Lease Time	<input type="text" value="86400"/> seconds (0 sets to default value of 259200)
Physical Ports	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3
DNS Relay	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Option 66	<input type="text"/>
Option 160	<input type="text"/>

Fixed Host

IP Address	<input type="text"/>
MAC Address	<input type="text"/>

IPv6 Parameters

Interface Address/Prefix Length	<input type="text"/> / <input type="text"/>
MLD Snooping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated

DHCPv6 Server

DHCPv6 Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start Interface ID	<input type="text"/>
End Interface ID	<input type="text"/>
Lease Time	<input type="text"/> seconds(0 sets to default value of 4800)
Router Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

Fixed Host List

Index	IP Address	MAC Address	Delete
-------	------------	-------------	--------

IPv4 Parameters

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

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

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

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

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

Dynamic Route:

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

DHCPv4 Server

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

DHCPv4 Server	
DHCPv4 Server	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay
Start IP	<input type="text" value="192.168.1.100"/>
IP Pool Count	<input type="text" value="20"/>
Lease Time	<input type="text" value="86400"/> seconds (0 sets to default value of 259200)
Physical Ports	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input checked="" type="checkbox"/> WLAN1
DNS Relay	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

DHCPv4 Server: If set to **Enabled**, your BEC 6300VNL can assign IP addresses, default gateway and DNS servers to the DHCP client.

- ▶ If set to **Disabled**, the DHCP server will be disabled.
- ▶ If set to **Relay**, the BEC 6300VNL acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- ▶ When DHCP is used, the following items need to be set.

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

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

Lease Time: The current lease time of client.

Physical Ports: Select to determine if the DHCPv4 server is applicable to the specific port or ports. By

default, all ports can obtain local IP from DHCPv4 server.

DNS Relay:

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

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

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

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

Fixed Host


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

Fixed Host	
IP Address	<input type="text"/>
MAC Address	<input type="text"/>

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

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

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

Fixed Host Listing			
Index	IP	MAC	Drop
1	192.168.1.102	23:24:5B:4B:22:33	

IPv6 parameters

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

IPv6 Parameters	
Interface Address/Prefix Length	<input type="text"/> / <input type="text"/>

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

MLD Snooping: Similar to IGMP Snooping, but applicable for IPv6.

DHCPv6 Server

DHCPv6 Server	
DHCPv6 Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start Interface ID	<input type="text"/>
End Interface ID	<input type="text"/>
Lease Time	<input type="text"/> seconds(0 sets to default value of 4800)
Router Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

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

Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

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

DHCPv6 Server: Check whether to enable DHCPv6 server.

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

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

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

End interface ID: enter the end interface ID.

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

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

Click **Save** to apply settings.

Wireless

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

Wireless	
Access Point Settings	
Access Point	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
AP MAC Address	60:03:47:23:F2:00
Wireless Mode	802.11b+g+n ▼
Channel	UNITED STATES ▼ 06 ▼ Current Channel : 6
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
TX Power	100 (range: 1~100)
IGMP Snooping	<input checked="" type="radio"/> Yes <input type="radio"/> No
11n Settings	
Channel Bandwidth	20 MHz ▼
Guard Interval	Auto ▼
MCS	Auto ▼
SSID Settings	
Available SSID	1 ▼
SSID Index	<input checked="" type="radio"/> SSID1
SSID	BEC223
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Clients Isolation	<input type="radio"/> Yes <input checked="" type="radio"/> No
SSID Activated	Always ▼
WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> PBC
Security Settings	
Security Type	Mixed WPA2/WPA-PSK ▼
WPA Algorithms	TKIP+AES ▼
Pre-Shared Key	14F812CE (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)
WDS Settings	
AP MAC Address	60:03:47:23:F2:00
WDS Mode	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00
Save	

Access Point Settings

Access Point Settings	
Access Point	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
AP MAC Address	60:03:47:23:F2:00
Wireless Mode	802.11b+g+n ▼
Channel	UNITED STATES ▼ 06 ▼ Current Channel : 6
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
TX Power	100 (range: 1~100)
IGMP Snooping	<input checked="" type="radio"/> Yes <input type="radio"/> No

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

AP MAC Address: The MAC address of wireless AP.

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

Channel: The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. There are Regulation Domains and Channel ID in this field. The Channel ID will be different based on Regulation Domains. Select a channel from the drop-down list box.

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

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

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

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

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

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

11n Settings

11n Settings	
Channel Bandwidth	20 MHz ▼
Guard Interval	Auto ▼
MCS	Auto ▼

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

Extension Channel: This is for the 20/40MHz clients to use and is predefined to **Auto** by default.

Guard Interval: Select either **400nsec** or **800nsec** for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other. It also prevents propagation delays, echoing and reflections. The shorter the Guard Interval, the better the performance will be. We recommend users to select Auto.

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

SSID Settings

SSID Settings	
Available SSID	1 ▼
SSID Index	<input checked="" type="radio"/> SSID1
SSID	BEC223
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Clients Isolation	<input type="radio"/> Yes <input checked="" type="radio"/> No
SSID Activated	Always ▼

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

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

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

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

Client Isolation: (Known as AP Isolation) After enabling this feature, all Wi-Fi clients connect to the same Access Point, in the same local wireless network, cannot interact with each another.

SSID Activated: Select the time period during which the SSID is active. Default is always which means the SSID will be active all the time without time control. See [Time Schedule](#) to set the timeslot to flexibly control when the SSID functions.

WPS Settings

WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> PBC

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

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

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

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

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

Security Settings

Security Settings	
Security Type	Mixed WPA2/WPA-PSK ▼
WPA Algorithms	TKIP+AES ▼
Pre-Shared Key	14F812CE (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)

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

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

There are five alternatives to select from: WEP 64-bit, WEP 128-bit, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. If you require high security for transmissions, please select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK.

▶ Security Type - WEP

Security Settings	
Security Type	WEP 64-bit ▼
WEP Authentication Method	Both ▼
WEP 64-bit	For each key, please enter either (1) 5 characters, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
<input checked="" type="radio"/> Key#1	<input type="text"/>
<input type="radio"/> Key#2	<input type="text"/>
<input type="radio"/> Key#3	<input type="text"/>
<input type="radio"/> Key#4	<input type="text"/>

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

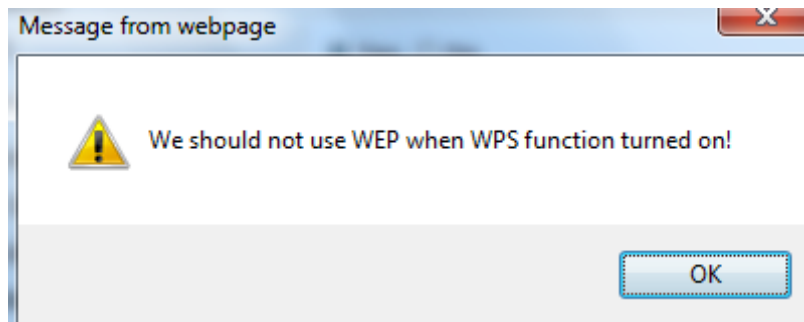
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bit WEP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

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

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

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

NOTE: When you enable WPS function, this WEP function will be invalid. And if you select one of WEP-64Bits/WEP-128Bits, the following prompt box will appear to notice you.



▶ **Security Type - WPA-PSK & WPA2-PSK**

Security Type	WPA-PSK
WPA Algorithms	AES
Pre-Shared Key	0004ED596230 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

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

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

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

WDS Settings

WDS Settings	
AP MAC Address	60:03:47:23:F2:00
WDS Mode	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00

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

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

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

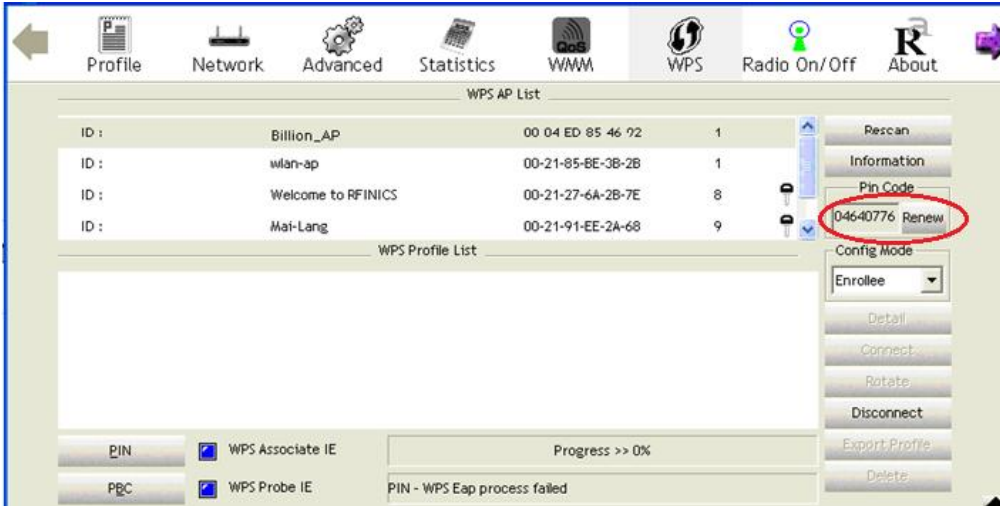
WDS Settings	
WDS Mode	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
WDS Peer MAC #1	<input type="text" value="00:00:00:00:00:00"/>
WDS Peer MAC #2	<input type="text" value="00:00:00:00:00:00"/>
WDS Peer MAC #3	<input type="text" value="00:00:00:00:00:00"/>
WDS Peer MAC #4	<input type="text" value="00:00:00:00:00:00"/>

Click **Save** to apply settings.

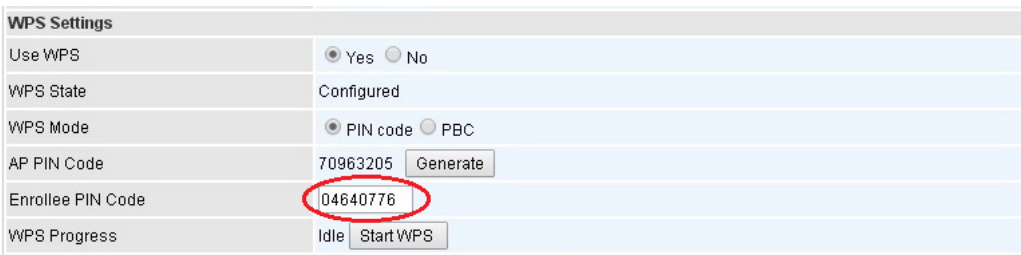
Example: WPS using PIN Method (Personal Information Number)

PIN Method – Configure 6300VNL as a Registrar

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

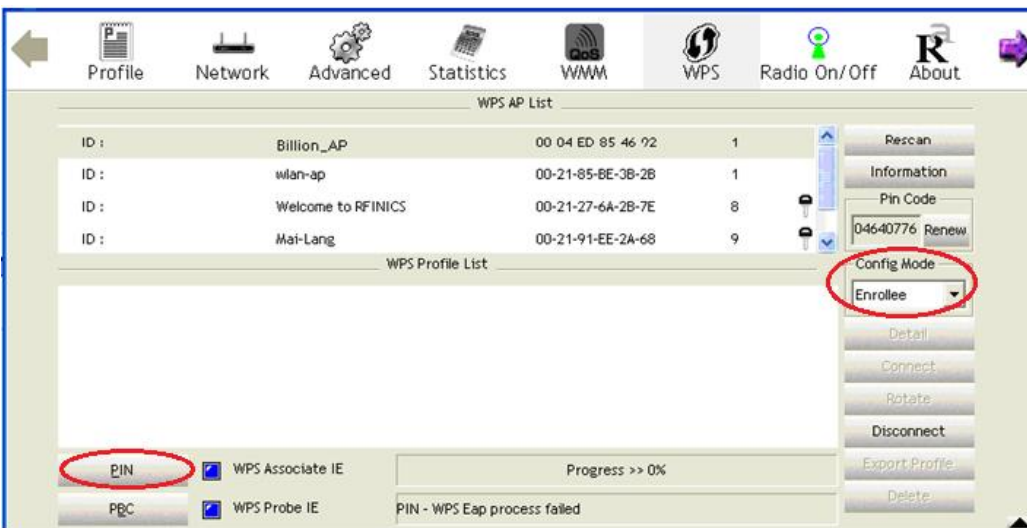


2. Enter the Enrollee (Client) PIN code and then press **Start WPS**.



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

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



4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar, the 6300VNL router.

The screenshot displays the configuration interface for a wireless device. At the top, there are navigation tabs: Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About, and Help. The main area is divided into several sections:

- WPS AP List:** A table showing discovered access points. The first entry, 'Billion_AP' with MAC address '00-04-ED-85-46-92', is circled in red.
- WPS Profile List:** Shows a profile named 'Billion_AP'.
- WPS Status:** Shows 'WPS Associate IE' and 'WPS Probe IE' are checked, with a progress bar at 100% and the message 'WPS status is connected successfully'.
- Link Quality:** A summary of connection metrics: Link Quality >> 100%, Signal Strength 1 >> 41%, Signal Strength 2 >> 44%, and Noise Strength >> 26%.
- Transmit/Receive:** Graphs showing link speed and throughput for both directions.
- SSID Settings:** A form where 'Billion-AP' is entered in the SSID field, circled in red.
- WPS Settings:** Shows 'Use WPS' is checked, 'WPS State' is 'Configured', and 'WPS Mode' is 'PIN code'.
- Security Settings:** Shows 'Security Type' is 'WPA2-PSK', circled in red, and 'WPA Algorithms' is 'AES'.

PIN Method – Configure 6300VNL as an Enrollee

1. Jot down the AP PIN Code (e.g. 03454435) from the BEC 6300VNL. Press **Start WPS**.

WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input checked="" type="radio"/> PIN code <input type="radio"/> PBC
AP PIN Code	03454435 <input type="button" value="Generate"/>
Enrollee PIN Code	<input type="text"/>
WPS Progress	In progress <input type="button" value="Stop WPS"/>

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

The screenshot shows the Ralink Utility WPS interface. At the top, there is a menu bar with icons for Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About, and Help. The main area is titled 'WPS AP List' and contains a table with the following data:

ID	SSID	BSSID	Channel	Key Icon
ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1	
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8	
ID :	Mai-Lang	00-21-91-EE-2A-68	9	

Below the AP list is the 'WPS Profile List' section, which shows 'Billion_AP' selected. To the right of the AP list, there are several controls: a 'Rescan' button, an 'Information' button, a 'Pin Code' input field containing 03454435, a 'Renew' button, a 'Config Mode' dropdown menu set to Registrar, and buttons for 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.

At the bottom left, there are two radio buttons: 'PIN' (selected and circled in red) and 'PBC'. Below them are checkboxes for 'WPS Associate IE' and 'WPS Probe IE'. A progress bar shows 'Progress >> 100%' and a status message reads 'WPS status is connected successfully'.

The bottom section displays network statistics for the selected AP (Billion_AP):

- Status >> Billion_AP <-> 00-04-ED-85-46-92
- Extra Info >> Link is Up [TxPower: 100%]
- Channel >> 1 <-> 2412 MHz; central channel : 6
- Authentication >> WPA2-PSK
- Encryption >> AES
- Network Type >> Infrastructure
- IP Address >> 192.168.1.101
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.1.254

Performance metrics are shown on the right:

- Link Quality >> 100%
- Signal Strength 1 >> 24%
- Signal Strength 2 >> 65%
- Noise Strength >> 26%
- Transmit: Link Speed >> 150.0 Mbps, Throughput >> 0.000 Kbps
- Receive: Link Speed >> 1.0 Mbps, Throughput >> 118.144 Kbps

Interface Setup – Wireless (Example on WPS using PIN)

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

ID	AP Name	BSSID	Channel	Security
0x0000	Billion_AP	00-04-ED-85-46-92	1	WPA2-PSK
	Welcome to RFINICS	00-21-27-6A-2B-7E	8	WPA2-PSK
	Mai-Lang	00-21-91-EE-2A-68	9	WPA2-PSK

Profile Name
Billion_AP

WPS status is connected successfully

Link Quality >> 100%
Signal Strength 1 >> 24%
Signal Strength 2 >> 65%
Noise Strength >> 26%

Transmit: Link Speed >> 150.0 Mbps, Throughput >> 0.000 Kbps
Receive: Link Speed >> 1.0 Mbps, Throughput >> 118.144 Kbps

SSID Settings

SSID Num: 1
SSID Index: SSID 1
SSID: Billion_AP
Broadcast SSID: Yes
SSID Activated: Always

WPS Settings

Use WPS: Yes
WPS State: Configured
WPS Mode: PIN code
AP PIN Code: 03454435
Enrollee PIN Code:
WPS Progress: In progress

Security Settings

Security Type: WPA2-PSK
WPA Algorithms: AES
Pre-Shared Key: 12345678
Key Renewal Interval: 3600 seconds

Interface Setup – Wireless (Example on WPS using PBC)

Example: WPS using PBC Method (Push Button Configuration)

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

The screenshot shows a configuration page with two main sections: SSID Settings and WPS Settings. In the SSID Settings section, the SSID field is set to "Billion_AP" and is circled in red. In the WPS Settings section, the "Use WPS" option is selected as "Yes", the "WPS State" is "Configured", and the "WPS Mode" is set to "PBC", which is also circled in red.

SSID Settings	
SSID Num	1
SSID Index	SSID1
SSID	Billion_AP
Broadcast SSID	Yes
SSID Activated	Always
WPS Settings	
Use WPS	Yes
WPS State	Configured
WPS Mode	PBC

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

The screenshot shows the WPS Utility interface. At the top, the "WPS" button is circled in red. Below it, the "WPS AP List" table is visible, with "Billion_AP" circled in red. On the right side, the "Config Mode" dropdown menu is set to "Enrollee" and is also circled in red. At the bottom left, the "PBC" button is circled in red. The interface also shows a "PIN" button and checkboxes for "WPS Associate IE" and "WPS Probe IE".

WPS AP List				
ID :	Billion_AP	00 04 ED 85 46 92	1	
ID :	wlan-ap	00-21-85-BE-3B-2B	1	
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8	
ID :	Mai-Lang	00-21-91-EE-2A-68	9	

Interface Setup – Wireless (Example on WPS using PBC)

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

The screenshot shows the WPS configuration interface. At the top, there are navigation tabs: Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About, and Help. The main area is divided into 'WPS AP List' and 'WPS Profile List'. The 'WPS AP List' shows three entries: 'Billion_AP' (ID: 00-04-ED-85-46-92), 'wlan-ap' (ID: 00-21-85-BE-3B-2B), and 'Welcome to RFINICS' (ID: 00-21-27-6A-2B-7E). The 'WPS Profile List' shows a profile for 'Billion_AP'. Below this, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A 'PBC' button is highlighted with a red circle. A progress bar indicates 'Progress >> 100%' and a message states 'WPS status is connected successfully'. On the right side, there are buttons for 'Rescan', 'Information', 'Pin Code' (04c40776), 'Renew', 'Config Mode' (Enrollee), 'Detail', 'Connect', 'Rotate', 'Disconnect', 'Export Profile', and 'Delete'. At the bottom, there are status indicators for 'Link Quality >> 100%', 'Signal Strength 1 >> 41%', 'Signal Strength 2 >> 44%', and 'Noise Strength >> 26%'. There are also graphs for 'Transmit' and 'Receive' link speeds and throughput.

The screenshot shows the wireless settings page. It is divided into three sections: 'SSID Settings', 'WPS Settings', and 'Security Settings'. In the 'SSID Settings' section, 'SSID Num' is set to 1, 'SSID Index' is set to SSID1, and the 'SSID' field contains 'Billion_AP', which is circled in red. 'Broadcast SSID' is set to Yes, and 'SSID Activated' is set to Always. In the 'WPS Settings' section, 'Use WPS' is set to Yes, 'WPS State' is Configured, and 'WPS Mode' is set to PBC. In the 'Security Settings' section, 'Security Type' is set to WPA2-PSK, 'WPA Algorithms' is set to AES, and 'Pre-Shared Key' is set to 12345678, which is circled in red. 'Key Renewal Interval' is set to 3600 seconds.

Wireless MAC Filter

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

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

Wireless MAC Address Filter

SSID Index	<input checked="" type="radio"/> SSID1
Active	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Action	Allow ▾ the follow Wireless LAN station(s) association.
MAC Address	<input style="width: 100%;" type="text"/>

Wireless MAC Address Filter Listing

Index	MAC Address	Edit	Delete
-------	-------------	------	--------

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

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

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

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

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

Click **Save** to apply settings.

Loopback

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

▼ Loopback	
Loopback interface	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
IP Address	<input type="text" value="127.0.0.1"/>
IP Subnet Mask	<input type="text" value="255.0.0.0"/>
<input type="button" value="Save"/>	

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

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

Click **Save** to apply settings.

Dual WAN

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

General Setting

▼ General Setting	
Dual WAN Mode	
Mode	Disable ▼
<input type="button" value="Save"/>	

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

Failover

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

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

General Setting	
Dual WAN Mode	
Mode	Failover ▼
WAN Port Service Detection Policy	
WAN1	EWAN_0 ▼
WAN2	3G/4G-LTE ▼
Keep Backup Interface Connected	<input type="checkbox"/> Enabled
Connectivity Decision	Not in service when probing failed after <input type="text" value="3"/> consecutive times
Probe Cycle	Every <input type="text" value="30"/> seconds.
Probe WAN1	<input checked="" type="radio"/> Gateway <input type="radio"/> Host <input type="text" value="0.0.0.0"/>
<input type="button" value="Save"/>	

WAN Port Service Detection Policy

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

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

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

- ▶ **Disable:** Inactivate this feature.
- ▶ **Always:** Keep the backup WAN (WAN2) interface always connected to the Internet
- ▶ **By Signal Strength:** Enable and initiate automatic backup WAN to connect to the Internet at all time until the RSRP / RSSI of primary WAN is greater than the Minimum RSRP / RSSI.
 - **Minimum RSRP / RSSI:** Set a minimum requirement for RSRP and RSSI for the primary WAN. Value range from -111 ~ -5. 0 means don't care/no need to check this value.

NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

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

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

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

Failover/Fallback Rule Decisions:

1. **Probe by Ping:** Enable Ping to the gateway or an IP address
 - ▶ **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.
 - ▶ **Host:** Internal system will wait for responses to the pings from a fixed IP address.
2. **Probe by Signal Strength:** Enable to measure the LTE signal strength

- ▶ **Minimum RSRP / RSSI:** Set a minimum requirement for RSRP and RSSI for initiating automatic WAN failback or failover procedures.

The valid range is from -111 ~ -5. 0 means don't care/no need to check this value.

NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

Click **Save** to apply settings.

Advanced Setup

Advanced Step provides advanced features including **Firewall, Routing, Dynamic Routing, NAT, Static DNS, QoS, Interface Grouping, Port Isolation, Time Schedule** and **Mail Alert** for advanced users.

Firewall

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

Firewall	
IPv4 Firewall	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IPv4 SPI	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IPv6 Firewall	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IPv6 SPI	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="button" value="Exception List"/>
<small>(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)</small>	
<input type="button" value="Save"/>	

Firewall (IPv4 or IPv6): To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

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

SPI (IPv4 or IPv6): If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- ▶ **Enabled:** It activates your SPI function.
- ▶ **Disabled:** It disables the SPI function.
- ▶ **Exception List (IPv6 Only): (next page)**

Click **Save** to apply and save settings

- ▶ **Exception List (IPv6 Only):** Click to add an IPv6 address / source to skip the check.

IPv6 SPI Exception List

Rule Index	1	
Individual Active	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Interface	EWAN	
Source IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Source IPv6 Prefix	32	
Source Port Number	0	(0 means Don't care)
Destination IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Destination IPv6 Prefix	32	
Destination Port Number	0	(0 means Don't care)
DSCP	0	(Value Range:0~64, 64 means Don't care)
Protocol	ALL	
Time Schedule	Always	

Save Back

Exception List				
Index	Source IPv6 Address/Prefix	Destination IPv6 Address/Prefix	Edit	Delete

Rule Index: The numeric rule indicator.

Individual Active: Click **Yes** to activate the rule

Interface: The WAN interface is handling the request.

Source IP (IPv6) Address/ Prefix: The source IP address or range of packets to be monitored.

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

Destination IP (IPv6) Address/ Prefix: The destination subnet IP address.

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

DSCP: show the set DSCP.

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

Time Schedule: Select an active scedule of the rule, always allow or at a specifcy times of day and time. Use [Time Schedule](#) to predefine a schedule.

Click **Save** to apply and save settings

Static Routing

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

▼ Routing Table							
Index	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	127.0.0.0	255.255.0.0	0.0.0.0	0	loopback		

Add Route

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

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

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

Interface: Media/channel selected to append the route.

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

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

Add Route

▼ Static Route	
Destination IP Address	<input type="text" value="0.0.0.0"/>
Destination Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway IP Address / Interface	<input type="radio"/> <input type="text" value="0.0.0.0"/> <input checked="" type="radio"/> <input type="text" value="4G/LTE"/>
Metric	<input type="text" value="1"/>

Save Back

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

Destination Subnet Mask: The subnet mask of destination network.

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

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

Click **Save** to apply and save settings

Dynamic Routing

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

Open Shortest Path First (OSPF)

▼ OSPF

OSPF	<input type="checkbox"/> Enable
Rule Index	0 ▼
Interface	EWAN(LAN1) ▼
Area ID	<input style="width: 100%;" type="text"/>

OSPF Listing

Index	Interface	Area ID

OSPF: Enable to activate OSPF routing.

Rule Index: The numeric route indicator. The maximum entry is up to 10, ranging from 0 to 9.

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

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

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

Border Gateway Protocol (BGP)

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

▼ **BGP**

BGP	<input type="checkbox"/> Enable
As Number	<input style="width: 100%;" type="text"/>
Rule Index	1 ▼
Neighbor IP	<input style="width: 100%;" type="text"/>
Neighbor As Number	<input style="width: 100%;" type="text"/>
Allowas-in	<input type="checkbox"/> Enable
Next-Hop-Self	<input type="checkbox"/> Enable

BGP Listing

Index	Neighbor IP	Neighbor As Number	Allowas-in

BGP: Enable to activate BGP routing.

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

Rule Index: The numeric route indicator. The maximum entry is up to 10, ranging from 0 to 9.

Neighbor IP: Enter the neighbor IP address.

Neighbor AS Number: Enter the neighbor AS number.

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

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

NAT

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

NAT	
NAT Status	Enable
ALG	
VPN Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DMZ / Virtual Server	
Interface	4G/LTE ▼
DMZ	▶ Edit
Virtual Server	▶ Edit

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

ALG

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

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

DMZ / Virtual Server

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

Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** [▶ Edit](#) or **Virtual Server** [▶ Edit](#) to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

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

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

▼ DMZ

DMZ for: Single IPs Account/ EWAN(LAN1)

DMZ: Enabled Disabled

DMZ Host IP Address:

Except Ports

Port:

Protocol: ▼

Description:

DMZ Export Ports Listing						
Index	Description	Protocol	Port	Edit	Delete	
1	N/A	N/A	N/A			
2	N/A	N/A	N/A			
3	N/A	N/A	N/A			
4	N/A	N/A	N/A			
5	N/A	N/A	N/A			
6	N/A	N/A	N/A			

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

DMZ:

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

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

Click **Save** to apply settings

Except Ports

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

Port: Enter port to be monitored.

Protocol: Enter the protocol to be monitored.

Description: Enter a description to this rule.

Example: Skip port 80 (UDP/TCP) in the list. All Incoming request to access to port 80 (Web GUI) will be forwarded to the embedded HTTP server of BEC 6300VNL instead of the DMZ host.

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

Virtual Server

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

Virtual Server is also known as Port Forwarding that allows BEC 6300VNL to direct incoming traffic to a specific device in the network.

Configure a virtual rule in BEC 6300VNL for remote users accessing services such as Web or FTP services via the public (WAN) IP address that can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Virtual Server

Virtual Server for	4G/LTE
Protocol	TCP ▼
Start Port Number	<input style="width: 80%;" type="text" value="21"/>
End Port Number	<input style="width: 80%;" type="text" value="21"/>
Local IP Address	<input style="width: 80%;" type="text" value="192.168.1.110"/>
Start Port Number (Local)	<input style="width: 80%;" type="text" value="21"/>
End Port Number(Local)	<input style="width: 80%;" type="text" value="21"/>

Virtual Server Listing								
Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.110	21	21		
1	N/A	N/A	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A	N/A	N/A		
10	N/A	N/A	N/A	N/A	N/A	N/A		

Virtual Server for: Indicate the related WAN interface to allow outside network to communicate with the internal LAN device.

Protocol: Choose the application protocol.

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

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

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

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

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

Examples of well-known and registered port numbers are shown below. For further information, please

see IANA's website at <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

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



Attention

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

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

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

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

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

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

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

FTP server uses TCP protocol with port 21.

Enter "21" to Start and End Port Number. The BEC 6300VNL will accept port 21 requests from WAN side.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.102

Enter "21" to Local Start and End Port number. The BEC 6300VNL will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.102) in the network.

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

Virtual Server

Virtual Server for	4G/LTE
Protocol	TCP ▼
Start Port Number	<input type="text" value="21"/>
End Port Number	<input type="text" value="21"/>
Local IP Address	<input type="text" value="192.168.1.110"/>
Start Port Number (Local)	<input type="text" value="21"/>
End Port Number(Local)	<input type="text" value="21"/>

Virtual Server Listing								
Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.110	21	21		
1	N/A	N/A	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A	N/A	N/A		
10	N/A	N/A	N/A	N/A	N/A	N/A		

Static DNS

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

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

Static DNS

IP Address

Domain Name

Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete
-------	------------	-------------	------	--------

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

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

Click **Save** to apply settings.

QoS

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

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

Quality of Service	
QoS	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
<input type="button" value="Save"/> <input type="button" value="Rules Summary"/>	
Rule	
Rule Index	0 ▼
Active	<input type="radio"/> Yes <input checked="" type="radio"/> No
Destination IPv4/IPv6 Address	<input type="text"/>
Destination Subnet Mask / IPv6 Prefix	<input type="text"/>
Destination Port Range	<input type="text"/> ~ <input type="text"/>
Source IPv4/IPv6 Address	<input type="text"/>
Source Subnet Mask / IPv6 Prefix	<input type="text"/>
Source Port Range	<input type="text"/> ~ <input type="text"/>
Protocol ID	<input type="text"/> ▼
Priority	<input type="text"/> ▼
<input type="button" value="Save"/> <input type="button" value="Delete"/>	

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

Click **Rule Summary** to review all created QoS rules.

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

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

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

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

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

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

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

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

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

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

Click **Save** to apply settings.

Interface Grouping

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

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

▼ Interface Grouping	
Interface Grouping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Group Index	0 ▼
EWAN Service	<input type="checkbox"/> EWAN0 <input type="checkbox"/> EWAN1
3G/4G-LTE	<input type="checkbox"/> 3G/4G-LTE <input type="checkbox"/> 3G/4G-LTE USB
Ethernet LAN	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3
Wireless LAN	<input type="checkbox"/> WLAN1
Group Summary	<input type="button" value="Group Summary"/>
<input type="button" value="Save"/> <input type="button" value="Delete"/>	

Interface Grouping: Select **Activated** to enable the feature.

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

EWAN Service: Available EWAN interface. Go to [Interface Setup](#) to add more WAN interfaces.

3G/4G-LTE: Available 3G/4G-LTE interfaces.

Ethernet LAN: Available Ethernet interfaces.

Wireless LAN: Go to **Interface Setup / Wireless** to enable the Wi-Fi service.

Group Summary: Click **Group Summary** to review current group information.

Click **Save** to apply settings.

Example: Create two EWAN services, Service0 (PPPoE) and Service1 (Bridge).

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

Group Index	Group Port
0	EWAN0,LAN1, LAN2, WLAN1
1	EWAN1, LAN3

▼ Interface Grouping

Interface Grouping Activated Deactivated

Group Index

EWAN Service EWAN0 EWAN1

3G/4G-LTE 3G/4G-LTE 3G/4G-LTE USB

Ethernet LAN LAN1 LAN2 LAN3

Wireless LAN WLAN1

Group Summary

▼ Interface Grouping

Interface Grouping Activated Deactivated

Group Index

EWAN Service EWAN0 EWAN1

3G/4G-LTE 3G/4G-LTE 3G/4G-LTE USB

Ethernet LAN LAN1 LAN2 LAN3

Wireless LAN WLAN1

Group Summary

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

▼ Interface Grouping

Group ID	Group port
0	,EWAM0,LAN1,LAN2,WLAN1
1	,EWAM1,LAN3

Port Isolation

Port isolation is also known as Private VLAN or a Private Port. Port(s) assigned in a group will be restricted, no communicate with one another.

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

Save

Click and group port(s), either from LAN or Wireless, to be separate from others.

Click **Save** to create and apply settings.

Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router’s time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.

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

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

Name: User-defined identification for each time period.

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

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

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

Click **Save** to apply your settings.

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

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

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

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

Mail Alert

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

Mail Alert	
Server Information	
SMTP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="*****"/>
Sender's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
SSL/TLS	<input type="checkbox"/> Enable
Port	<input type="text" value="25"/> (1~65535)
<input type="button" value="Account Test"/>	
WAN IP Change Alert	
Recipient's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
4G/LTE Usage Allowance	
Recipient's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
<input type="button" value="Apply"/>	

Server Information

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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

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

Port: the port, default is 25.

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

WAN IP Change Alert

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

Recipient's Email (3G/4G-LTE Usage Allowance): Enter a valid e-mail address to receive an alert message when the 3G or 4G/LTE over Usage Allowance occurs.

Click **Apply** button to save settings.

VPN

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

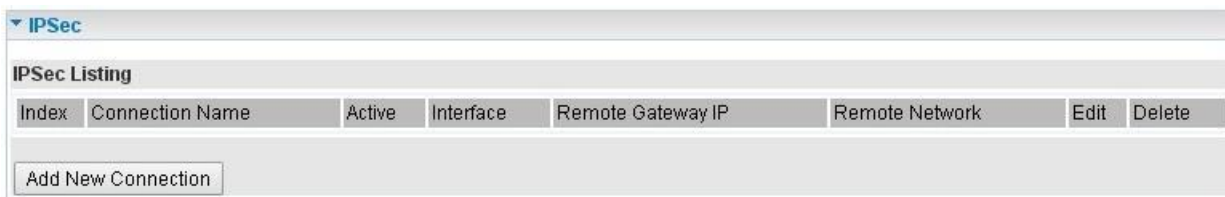
BEC 6300VNL supports **IPSec**, **PPTP**, **L2TP** and **GRE**

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.



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

IPSec Connection Setting

IPSec					
Connection Name	<input type="text"/>				
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Interface	Auto ▼				
Remote Gateway IP	<input type="text"/> (0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	<input type="text"/> 0.0.0.0	IP Subnetmask	<input type="text"/> 0.0.0.0
Remote Access Range	Subnet ▼	Remote IP Address	<input type="text"/> 0.0.0.0	IP Subnetmask	<input type="text"/> 0.0.0.0
IKE Mode	Main ▼	Pre-Shared Key	<input type="text"/>		
Local ID Type	Default (Local WAN IP) ▼	IDContent	<input type="text"/> *		
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent	<input type="text"/> *		
IKE Proposal	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Diffie-Hellman Group	MODP1024(DH2) ▼			
IPSec Proposal	<input checked="" type="radio"/> ESP		<input type="radio"/> AH		
	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Perfect Forward Secrecy	None ▼			
SA Lifetime	Phase 1 (IKE)	<input type="text"/> 480 min(s)	Phase 2 (IPSec)	<input type="text"/> 60 min(s)	
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	<input type="text"/> 0.0.0.0	Interval	<input type="text"/> 10 seconds
Disconnection Time after No Traffic	<input type="text"/> 180 seconds (180 at least)				
Reconnection Time	<input type="text"/> 3 min(s) (3 at least)				
Note * : FQDN with @ as first character means don't resolve domain name.					
Note ** : (0-3600, 0 means NEVER)					
<input type="button" value="Save"/> <input type="button" value="Back"/>					

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	<input type="text"/>
Local ID Type	Default (Local WAN IP) ▼	IDContent	<input type="text"/> *
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent	<input type="text"/> *
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	<input checked="" type="radio"/> ESP <input type="radio"/> 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.

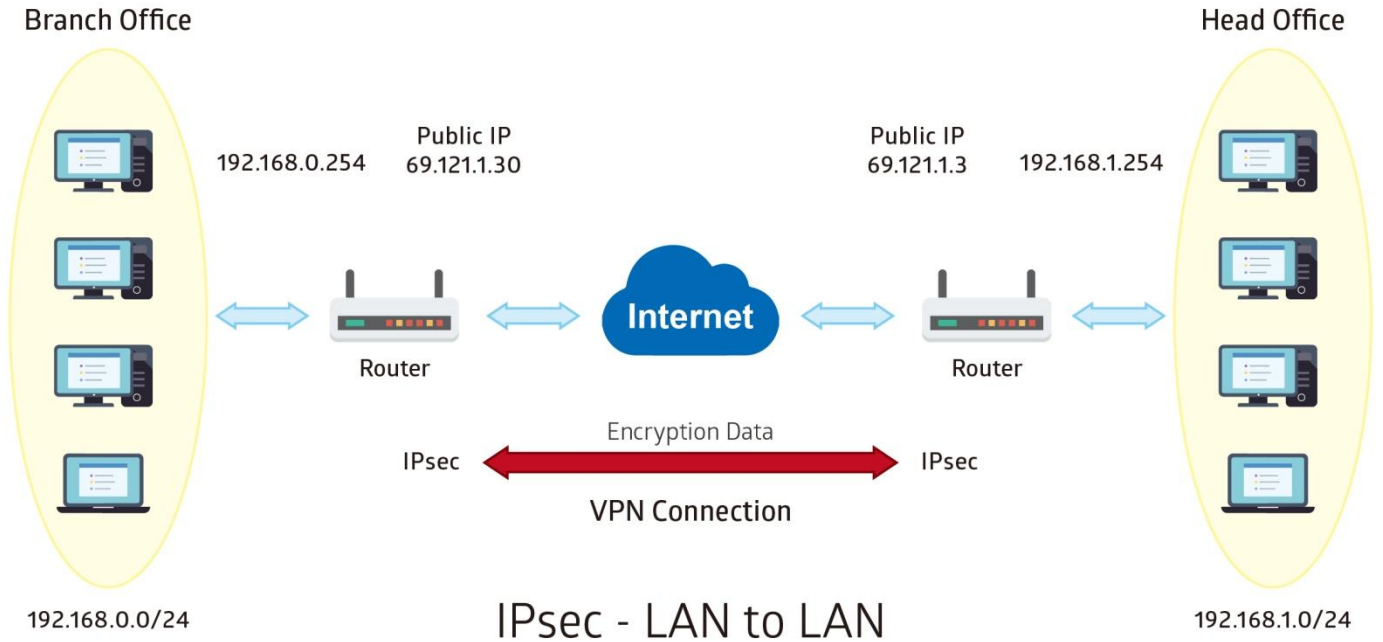
Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply settings.

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

Two of the BEC 6300VNL 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	<input type="text" value="H-to-B"/>			
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Interface	<input type="text" value="Auto"/>			
Remote Gateway IP	<input type="text" value="69.121.1.30"/> (0.0.0.0 means any)			
Local Access Range	<input type="text" value="Subnet"/>	Local IP Address	<input type="text" value="192.168.1.0"/>	
		IP Subnetmask	<input type="text" value="255.255.255.0"/>	
Remote Access Range	<input type="text" value="Subnet"/>	Remote IP Address	<input type="text" value="192.168.0.0"/>	
		IP Subnetmask	<input type="text" value="255.255.255.0"/>	
IKE Mode	<input type="text" value="Main"/>	Pre-Shared Key	<input type="text" value="1234567890"/>	
Local ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *	
Remote ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *	
Encryption Algorithm	<input type="text" value="AES-128"/>	Authentication Algorithm	<input type="text" value="SHA1"/>	
		Diffie-Hellman Group	<input type="text" value="MODP1024(DH2)"/>	
IPsec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH			
	Authentication Algorithm	<input type="text" value="SHA1"/>	Encryption Algorithm	<input type="text" value="3DES"/>
Perfect Forward Secrecy	<input type="text" value="MODP1024(DH2)"/>			
Phase 1 (IKE)SA Lifetime	<input type="text" value="480"/> min(s)	Phase 2 (IPsec)	<input type="text" value="60"/> min(s)	
Keepalive	<input type="text" value="None"/>	PING to the IP(0.0.0.0:NEVER)	<input type="text" value="0.0.0.0"/> Interval <input type="text" value="10"/> seconds **	
Disconnection Time after No Traffic	<input type="text" value="180"/> seconds (180 at least)			
Reconnection Time	<input type="text" value="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	<input type="text" value="B-to-H"/>				
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Interface	Auto				
Remote Gateway IP	<input type="text" value="69.121.1.3"/> (0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	<input type="text" value="192.168.0.0"/>	IP Subnetmask	<input type="text" value="255.255.255.0"/>
Remote Access Range	Subnet	Remote IP Address	<input type="text" value="192.168.1.0"/>	IP Subnetmask	<input type="text" value="255.255.255.0"/>
IKE Mode	Main	Pre-Shared Key	<input type="text" value="1234567890"/>		
Local ID Type	Default Wan IP	IDContent	<input type="text"/> *		
Remote ID Type	Default Wan IP	IDContent	<input type="text"/> *		
Encryption Algorithm	AES-128	Authentication Algorithm	SHA1	Diffie-Hellman Group	MODP1024(DH2)
IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH				
	Authentication Algorithm	SHA1	Encryption Algorithm	3DES	
Perfect Forward Security	MODP1024(DH2)				
Phase 1 (IKE)SA Lifetime	<input type="text" value="480"/> min(s)	Phase 2 (IPSec)	<input type="text" value="60"/> min(s)		
Keepalive	None	PING to the IP(0.0.0.0:NEVER)	<input type="text" value="0.0.0.0"/>	Interval	<input type="text" value="10"/> seconds **
Disconnection Time after No Traffic	<input type="text" value="180"/> seconds (180 at least)				
Reconnection Time	<input type="text" value="3"/> min(s) (3 at least)				

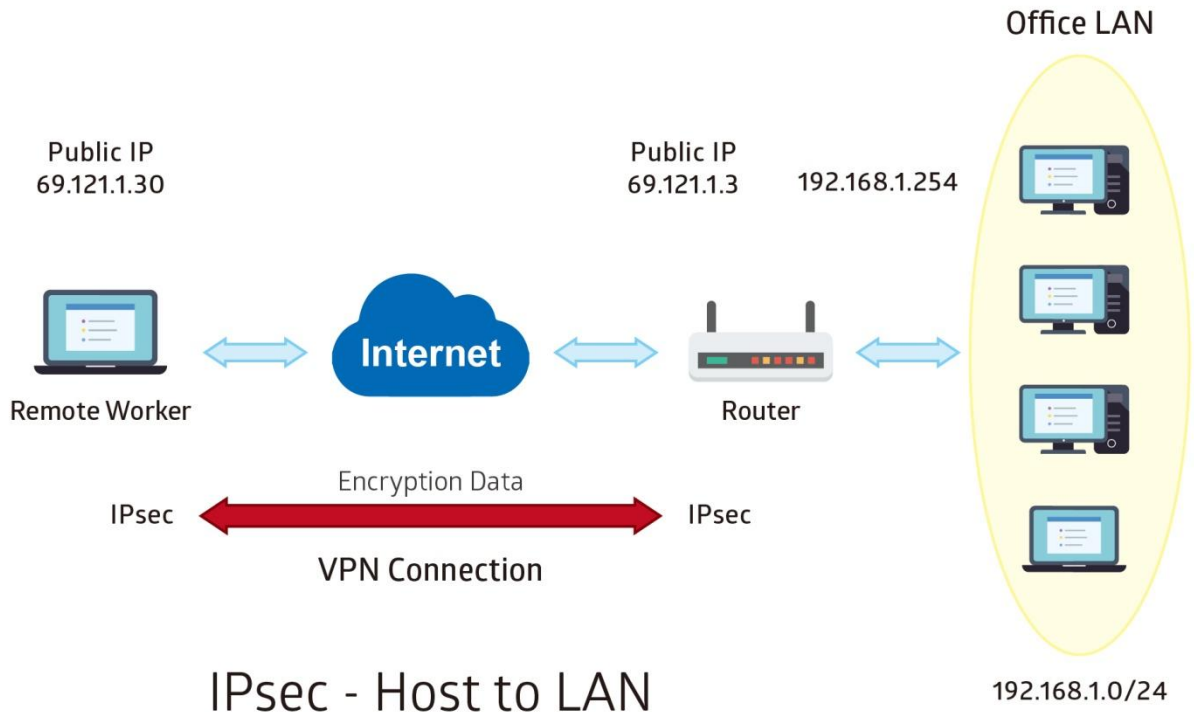
Note *: FQDN with @ as first character means don't resolve domain name.

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

Save Back

Examples: IPsec – Remote Employee to BEC 6300VNL Connection

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



Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office LAN network information
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Single 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	<input type="text" value="H-to-H"/>		
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Interface	<input type="text" value="Auto"/>		
Remote Gateway IP	<input type="text" value="69.121.1.30"/> (0.0.0.0 means any)		
Local Access Range	<input type="text" value="Subnet"/>	Local IP Address	<input type="text" value="192.168.1.0"/>
		IP Subnetmask	<input type="text" value="255.255.255.0"/>
Remote Access Range	<input type="text" value="Single IP"/>	Remote IP Address	<input type="text" value="69.121.1.30"/>
		IP Subnetmask	<input type="text" value="255.255.255.255"/>
IKE Mode	<input type="text" value="Main"/>	Pre-Shared Key	<input type="text" value="1234567890"/>
Local ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *
Remote ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *
Encryption Algorithm	<input type="text" value="AES-128"/>	Authentication Algorithm	<input type="text" value="SHA1"/>
		Diffie-Hellman Group	<input type="text" value="MODP1024(DH2)"/>
IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
	Authentication Algorithm	<input type="text" value="SHA1"/>	Encryption Algorithm
		<input type="text" value="3DES"/>	
Perfect Forward Secrecy	<input type="text" value="MODP1024(DH2)"/>		
Phase 1 (IKE)SA Lifetime	<input type="text" value="480"/> min(s)	Phase 2 (IPSec)	<input type="text" value="60"/> min(s)
Keepalive	<input type="text" value="None"/>	PING to the IP(0.0.0.0:NEVER)	<input type="text" value="0.0.0.0"/> Interval <input type="text" value="10"/> seconds **
Disconnection Time after No Traffic	<input type="text" value="180"/> seconds (180 at least)		
Reconnection Time	<input type="text" value="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	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated				
Authentication Type	Chap/Pap ▼				
Encryption Key Length	Auto ▼				
Encryption Mode	Allow Stateless and Statefull ▼				
CCP	<input checked="" type="radio"/> Yes <input type="radio"/> No				
MS-DNS	192.168.1.254				
Rule Index	1 ▼				
Connection Name	<input type="text"/>				
Active	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Username	<input type="text"/>				
Password	*****				
Connection Type	Remote Access ▼				
Private IP Address assigned to Dial-in User	<input type="text"/>				
Remote Network IP Address	<input type="text"/>				
Remote Network Netmask	<input type="text"/>				
<input type="button" value="Save"/> <input type="button" value="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	<input type="text"/>				
Active	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Authentication Type	Chap/Pap ▼				
Encryption Key Length	Auto ▼				
Encryption Mode	Allow Stateless or Statefull ▼				
CCP	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Username	<input type="text"/>				
Password	*****				
Connection Type	Remote Access ▼				
Server IP Address	<input type="text"/>				
Remote Network IP Address	<input type="text"/>				
Remote Network Netmask	<input type="text"/>				
Active as Default Route	<input type="checkbox"/> Enable				
<input type="button" value="Save"/> <input type="button" value="Delete"/>					
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.

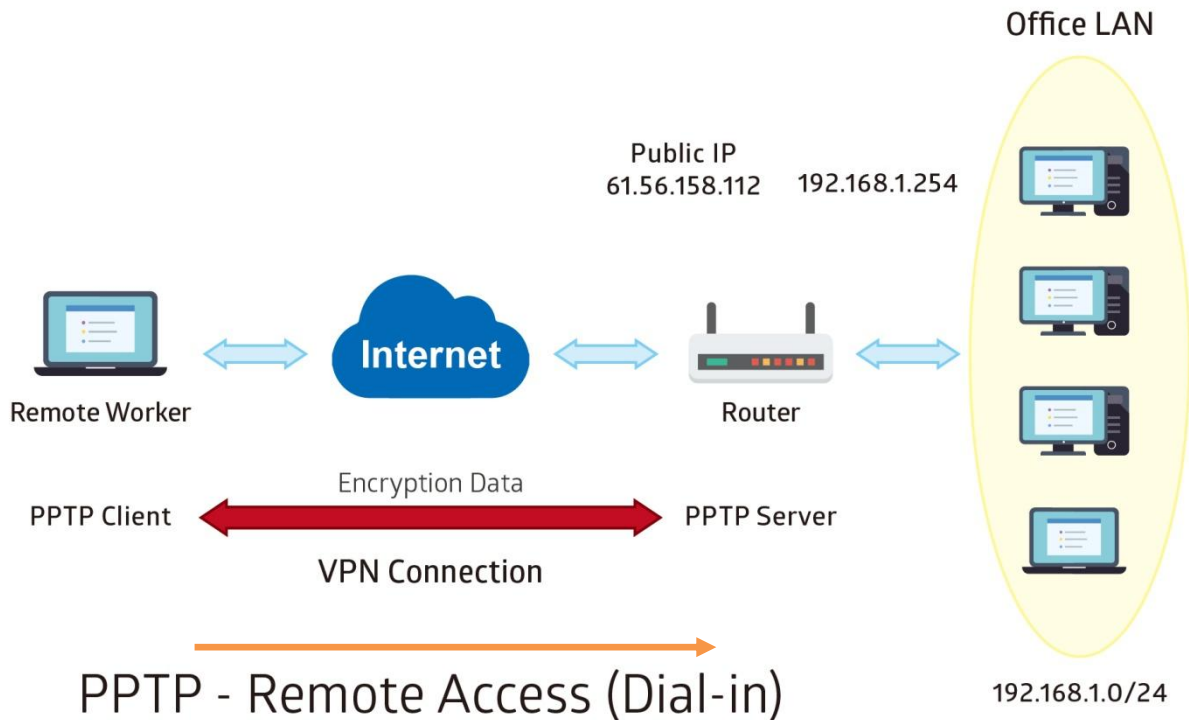
Server Address: Enter the WAN IP address of the PPTP server.

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 BEC 6300VNL



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 Activated Deactivated

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:

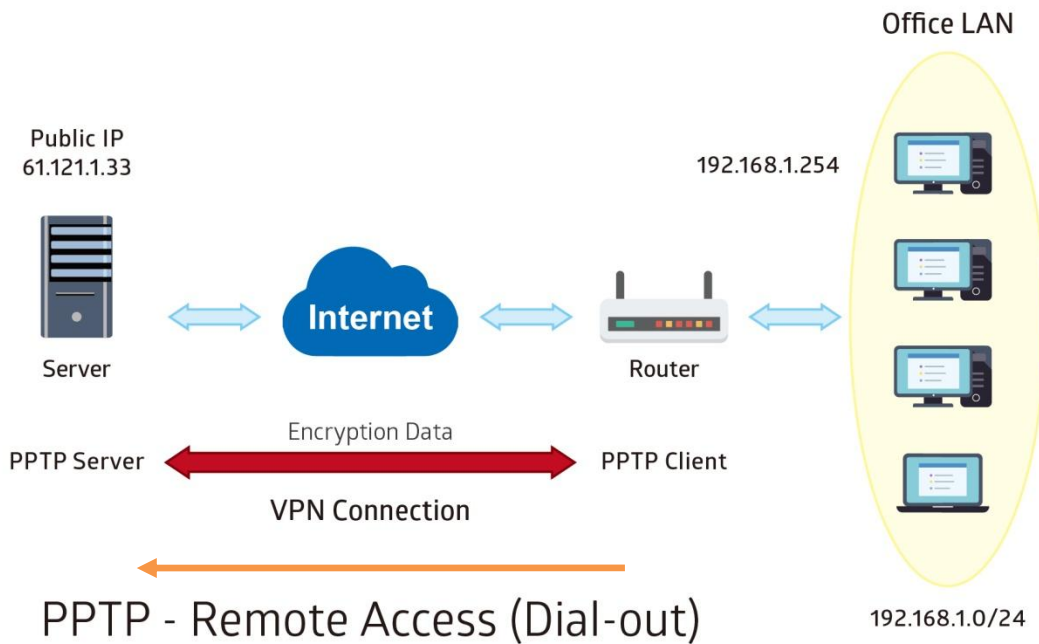
Save Delete

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 BEC 6300VNL

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

Save Delete

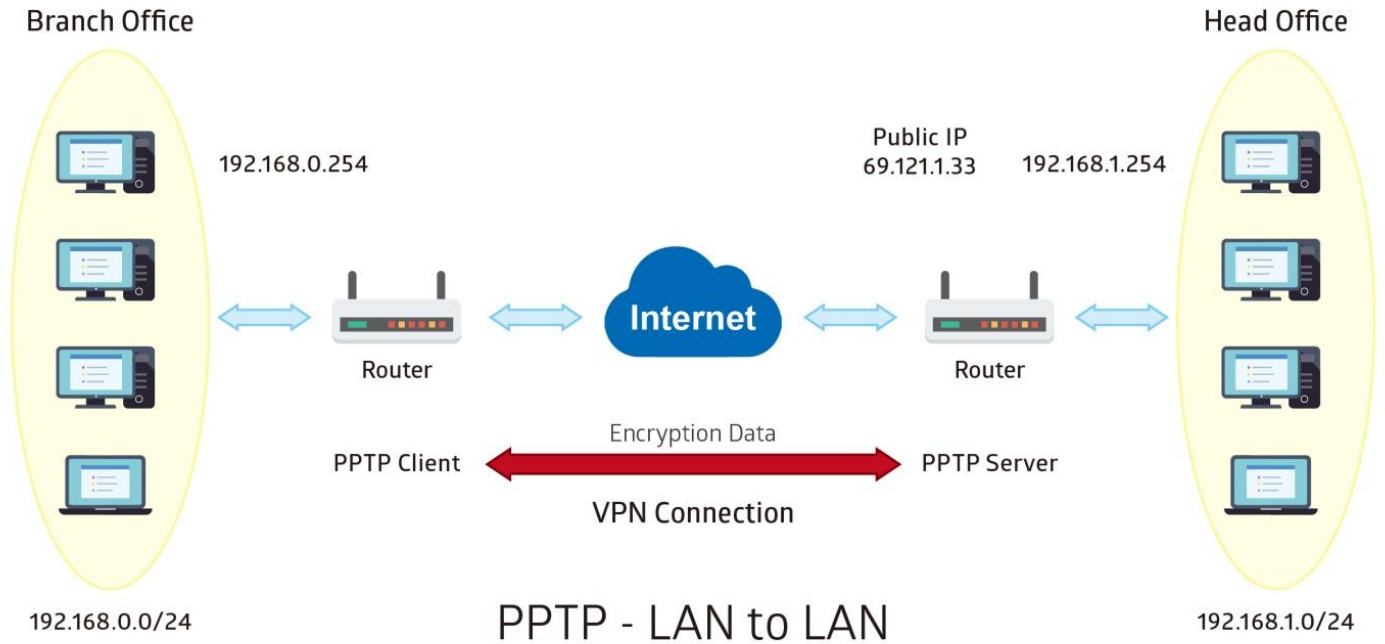
PPTP Client Listing

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
Authentication Type	MS-CHAPv2
Username	test
Password	test
Connection Type	LAN to LAN
Assigned IP	192.168.1.2
Remote Network IP	129.168.0.0
Remote Network Netmask	255.255.255.0

▼ PPTP Server

PPTP Server Activated Deactivated

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

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
Authentication Type	MS-CHAPv2
Username	test
Password	test
Connection Type	LAN to LAN
Server IP	69.121.1.33
Remote Network IP	129.168.1.0
Remote Network Netmask	255.255.255.0

▼ PPTP Client

Rule Index	1 ▼
Connection Name	BC-LL
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authentication Type	MS-CHAPv2 ▼
Encryption Key Length	Auto ▼
Encryption Mode	Allow Stateless or Statefull ▼
CCP	<input checked="" type="radio"/> Yes <input type="radio"/> 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	<input type="checkbox"/> 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	<input type="text"/>
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Connection Mode	Dial in ▼
Authentication Type	Chap/Pap ▼
Username	<input type="text"/>
Password	<input type="text"/>
Private IP Address assigned to Dial-in User	<input type="text"/>
Connection Type	Remote Access ▼
Tunnel Authentication	<input type="checkbox"/> Enable
Secret Password	<input type="text"/>
Local Host Name	<input type="text"/>
Remote Host Name	<input type="text"/>
Active as Default Route	<input type="checkbox"/> Enable

Save Delete

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	<input type="text"/>
Password	<input type="text"/>
Private IP Address assigned to Dial-in User	<input type="text"/>

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	<input type="text"/>
Authentication Type	Chap/Pap ▼
Username	<input type="text"/>
Password	<input type="text"/>

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	<input type="checkbox"/> Enable
Secret Password	<input type="text"/>
Local Host Name	<input type="text"/>
Remote Host Name	<input type="text"/>
Active as Default Route	<input type="checkbox"/> 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.

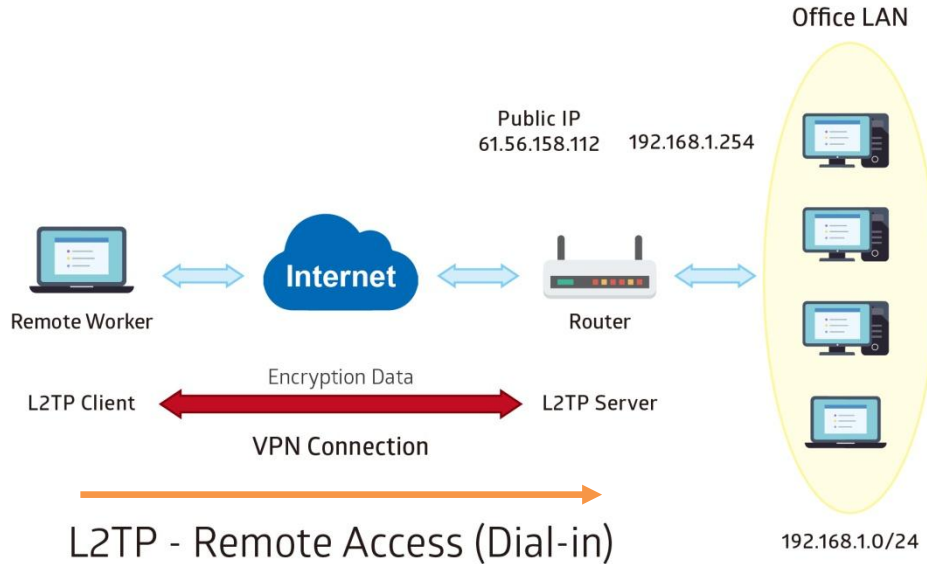
Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

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 BEC 6300VNL

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:

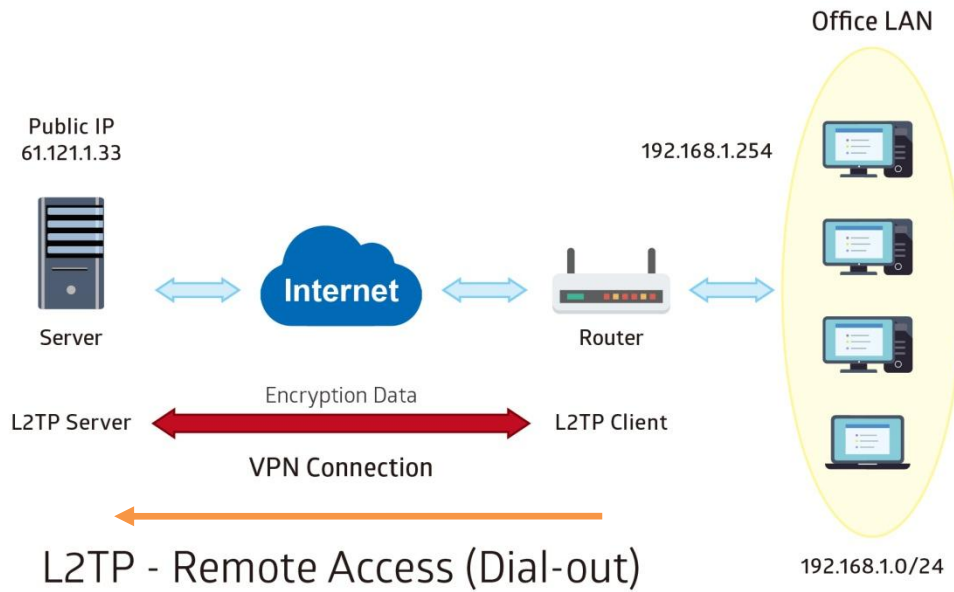
Active as Default Route: Enable

Save Delete

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

Example: L2TP VPN – BEC 6300VNL 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

Save Delete

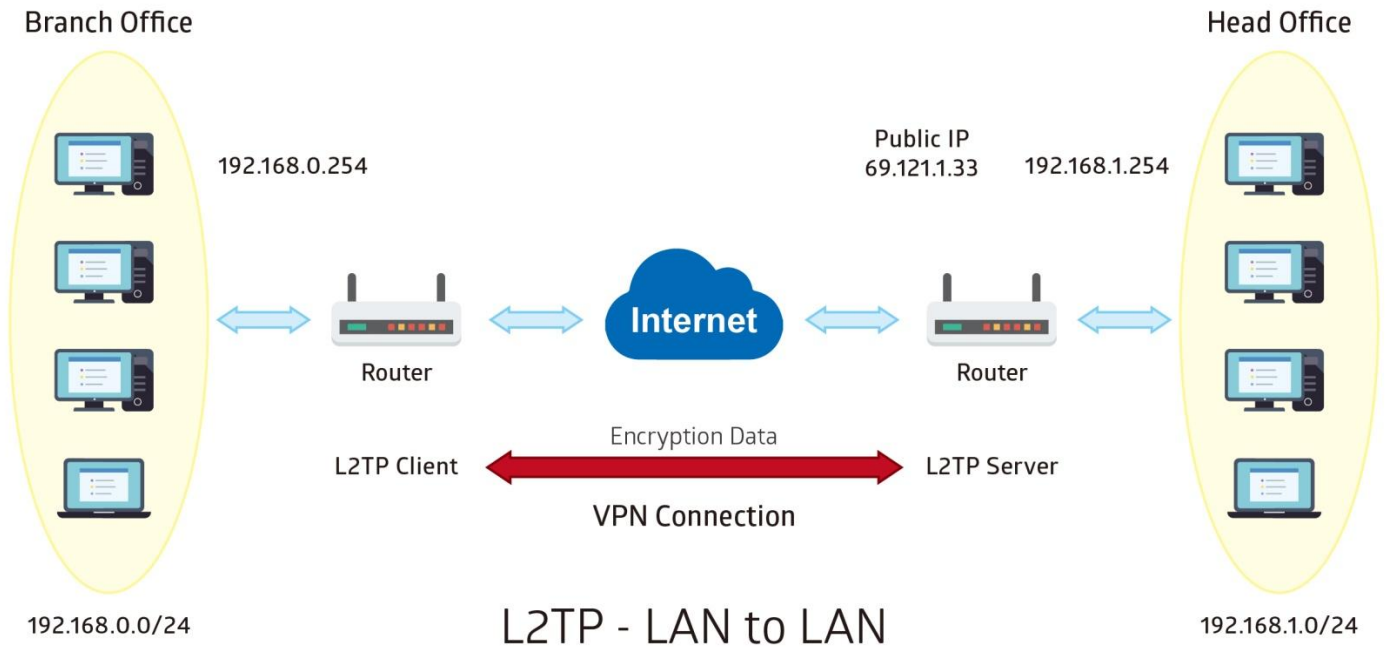
L2TP Listing

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	<input checked="" type="radio"/> Yes <input type="radio"/> 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	<input type="checkbox"/> Enable
Secret Password	<input type="text"/>
Local Host Name	<input type="text"/>
Remote Host Name	<input type="text"/>
Active as Default Route	<input type="checkbox"/> 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	<input checked="" type="radio"/> Yes <input type="radio"/> 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	<input type="checkbox"/> Enable
Secret Password	<input type="text"/>
Local Host Name	<input type="text"/>
Remote Host Name	<input type="text"/>
Active as Default Route	<input type="checkbox"/> 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	<input type="radio"/> Yes <input checked="" type="radio"/> 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	<input type="checkbox"/>				
Keepalive Retry Times	3				
Keepalive Interval	5 Second(s)				
MTU	1460				
Active as Default Route	<input type="radio"/> Yes <input checked="" type="radio"/> No				
IPSec	<input type="checkbox"/> Enable				
<input type="button" value="Save"/> <input type="button" value="Delete"/>					
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	<input checked="" type="checkbox"/> Enable
IKE Mode	Main ▾
IKE(IPSec) Local ID	Default (Local WAN IP) ▾ <input type="text"/>
IKE(IPSec) Remote ID	Default (Remote Gateway IP) ▾ <input type="text"/>
IKE(IPSec) Pre-Shared Key	<input type="text"/>

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.

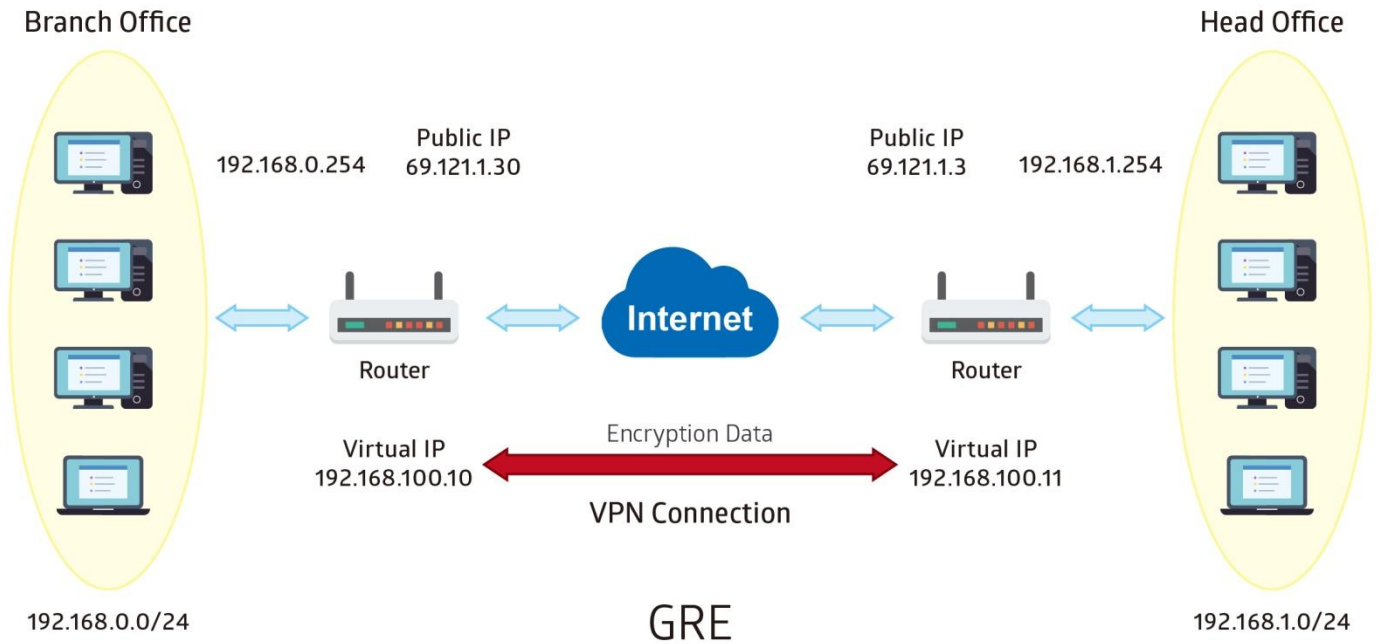
IKE (IPSec) Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can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

Save Delete

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	<input checked="" type="radio"/> Yes <input type="radio"/> 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	<input type="checkbox"/>
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	<input type="radio"/> Yes <input checked="" type="radio"/> No
IPSec	<input type="checkbox"/> 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

VoIP

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

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

Basic

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

VoIP Basic	
Local SIP Port	<input type="text" value="5060"/>
Local RTP (voice) Port	<input type="text" value="4000"/> ~ <input type="text" value="4020"/>
Voice QoS DSCP Marking	<input type="text" value="Premium"/>
Interface	<input type="text" value="Auto"/>
Phone	<input type="text" value="1"/>
Phone Number	<input type="text"/>
Display Name	<input type="text"/>
Authentication Name	<input type="text"/> <input type="checkbox"/> The same as Phone Number
Password	<input type="password" value="....."/>
User Domain	<input type="text"/>
SIP Registrar	<input type="text"/> : <input type="text" value="5060"/>
SIP Registration Expire	<input type="text" value="3600"/> sec.
SIP Proxy	<input type="text"/> : <input type="text" value="5060"/>
SIP Outbound Proxy	<input type="text"/> : <input type="text" value="5060"/>
<input type="button" value="Save"/>	

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

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

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

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

Phone: Select “1”, the following parameters will be applicable to Phone1. In BEC 6300VNL, Phone_1 and Phone_2 are allowed to be of different characteristics, including different SIP registrar. You need to configure individually for phone1 and phone 2 and can have up to 2 different VoIP accounts.

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

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

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

Password: Set the registering account password.

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

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

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

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

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

Media

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

VoIP Media			
Phone	1 ▼		
T.38	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Supported codec			
Priority 1	G.711 u-law ▼	Packetization Time	20 ▼
Priority 2	G.711 A-law ▼	Packetization Time	20 ▼
Priority 3	G.729 ▼	Packetization Time	20 ▼
Priority 4	G.726 ▼	Packetization Time	20 ▼
Save			

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

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

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

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

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

Advanced

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

VoIP Advanced	
Region	USA-United States ▼
Dial Delay Time	3000 ms
Phone	1 ▼
Silence Suppression(VAD)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Echo Cancellation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTMF Transport Mode	RFC2833 ▼
Listening Volume	0 db (-6~6)
Speaking Volume	0 db (-6~6)
Save	

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

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

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

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

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

DTMF Transport Mode: Select the DTMF mode.

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

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





















Speed Dial

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

▼ Speed Dial

Index	0
Phone	1 ▼
Speed Dial Number	<input type="text"/>
Phone Number	<input type="text"/>

Speed Dial Listing

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

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

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

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

Phone Number: The complete destination number





















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

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

▼ Speed Dial

Index	0
Phone	1 ▼
Speed Dial Number	<input type="text"/>
Phone Number	<input type="text"/>

Speed Dial Listing

Index	Phone	Speed Dial Number	Phone Number	Edit	Delete
0	1	301#	5135555555		
1		N/A			
2		N/A			
3		N/A			
4		N/A			
5		N/A			
6		N/A			
7		N/A			
8		N/A			
9		N/A			

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

Dial Plan

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

▼ Dial Plan Rule

Phone	1 ▼
Prefix Processing	<input type="radio"/> Prepend <input type="text"/> unconditionally
	<input type="radio"/> If prefix is <input type="text"/> , delete it
	<input type="radio"/> If prefix is <input type="text"/> , replace with <input type="text"/>
	<input checked="" type="radio"/> No prefix
Main Digit Sequence	<input type="text"/> @ <input type="text"/>
<input type="button" value="Save"/>	

Current Digit Map : N/A

Index	Rule Name	Delete
0	x.	

Digit Sequence Example:

- x. x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length at least 2. Maximum length is 32.*
- xxx Any sequence of digits in fixed length. Total length is 3.*
- xx. Any sequence of digits in variable length at least 3 digits. Maximum Length is 32.*
- 123 Squence of digits 123.*
- 123. Any sequence of digits starting with 123 and with variable length at least 4. Maximum length is 32.*
- 123x. Any sequence of digits starting with 123 and with variable length at least 5. Maximum length is 32.*
- [124]x. Any sequence of digits starting with 1 or 2 or 4. Minimal length is 3, maximum length is 32.*
- [1-3]x. Any sequence of digits starting with 1 to 3 and with variable length. Maximum length is 32.*
- 9[4-6]8x. Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.*

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

Prefix Processing <:xx>

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

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

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

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

Main Digit Sequence

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

x: Any numeric number between 0 and 9.

. [period]: Repeat numeric number(s) between 0 and 9.

*** [asterisk]:** It is normal character '*' on phone key pad. Please check if special service(s) is provided

by your VoIP Service Provider or your Local Telephone Service Provider.

[pound]: It is normal character '#' on phone key pad. Please check if it is provided by your VoIP Service Provider or Local Telephone Service Provider for special service(s).

<@ Current Profile>: Referring to the VoIP accounts registered for Port 1 / 2.

Dial-Plan Examples:	Description
x.	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3 digit number only between 0 and 9. Total length is 3. NOTE: No period is needed (.)
xxxx.	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length is 16.
123x.	Any number (0-9) starting with 123. Maximum length is 16.
[x...x]x. Example: [124]x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[x-x]x. Example: [1-3]x.	Any number (0-9) starting with number 1 to 3. Maximum length is 16.
x[x-x]x. Example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.
Special Dial Plan Examples:	Description
*xx*x.	Starting with '* sign' + any two digit numbers + any number (0-9) in variable length. Maximum length is 16.
xx	Starting with ' sign' + any 2 digit numbers between 0 and 9. Total length including the * is 3. NOTE: No period is needed (.)
xx*x	Starting with ' sign' + any two digit numbers between 0 + any number (0-9) in variable length. Maximum length is 16.
#xx.	Starting with '# sign' + any digit number (0-9) in variable length but no shorter than 1 digits. Maximum length is 16.
##xx*x.	Starting with '## sign' + any two digit numbers + '* sign' + any number (0-9) in variable length. Maximum length is 16.

Example: < @ Current Profile > / Call Routing

Current registered VoIP/SIP providers are localcheap.com and longdischeap.com. Each provider has its price for different type of calls

1) Phone 1: For Local calls: I set a dial rule, <:3>[123]x.T, for Phone_1.

Localcheap.com is the default VoIP provider I set on phone port 1. When I call out any number start with 1 or 2 or 3 and plus rest of the phone number for local call, 03 is always to add in front of the dialed number. If 1234567 is dialed, 513-1234567 is the actual phone number called out via localcheap.com provider.

Dial Plan Rule

Phone: 1

Prefix Processing:

- Prepend 513 unconditionally
- If prefix is [], delete it
- If prefix is [], replace with []
- No prefix

Main Digit Sequence: [123]x. @ phone_1

Save

Current Digit Map : x.<:513>[123]x.@phone_1

Index	Rule Name	Delete
0	x.	
1	<:513>[123]x.@phone_1	

2) Phone 1: For International calls: I set a dial rule, 0[2456]x.T, on my phone port 1.

Localcheap.com is the default VoIP provider I set on phone port 1. No prefix is attached to the dialed number when I call out number 0 plus any following number 2 or 4 or 5 or 6 and plus rest of the phone number for an international call. If 02016148513295 are dialed, 0-2-016148513295 is the actual phone number called out via phone_1; otherwise, the call will get dropped.

Dial Plan Rule

Phone: 1

Prefix Processing:

- Prepend [] unconditionally
- If prefix is [], delete it
- If prefix is [], replace with []
- No prefix

Main Digit Sequence: 0[2456]x. @ phone_1

Save

Current Digit Map : 0[2456]x.@phone_1

Index	Rule Name	Delete
0	0[2456]x.@phone_1	

3) Phone 2: For Weekend Local calls: I set a dial rule, 0[2456]x.T, on my phone port 2.

Mobilecheap.com is the default VoIP provider I set on Phone_2. When I call out 123-39-45678 for a mobile call, 123 is replaced with 614. Therefore, 614-394-5678 is the actual phone number called out via Mobilecheap.com provider.

▼ Dial Plan Rule

Phone	2 ▼	
Prefix Processing	<input type="radio"/>	Prepend <input type="text"/> unconditionally
	<input type="radio"/>	If prefix is <input type="text"/> , delete it
	<input checked="" type="radio"/>	If prefix is <input type="text" value="123"/> , replace with <input type="text" value="614"/>
	<input type="radio"/>	No prefix
Main Digit Sequence	<input type="text" value="39x."/> @ <input type="text" value="phone_2"/>	
<input type="button" value="Save"/>		

Current Digit Map : x.|<123:614>39x.@phone_2

Index	Rule Name	Delete
0	<123:614>39x.@phone_2	

Call Features

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

▼ Call Features	
Phone	1 ▼
Hot-line/Warm-line	<input type="checkbox"/> Dial to <input type="text"/> Delay Time: <input type="text" value="0"/> seconds (0 ~ 15)
Call Forwarding	<input type="checkbox"/> Unconditional forwarding to <input type="text"/>
	<input type="checkbox"/> On Busy forwarding to <input type="text"/>
	<input type="checkbox"/> On No Answer forwarding to <input type="text"/> No Answer Time: <input type="text" value="30"/> seconds
Blind Call Transfer (Flash: *21 + number)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Attended Call Transfer (Flash: *22 + number)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Call Waiting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Conference Call	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MWI (Message Waiting Indicator)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Anonymous Call	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block Anonymous Call	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Distinctive Ring	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Phone number +"#".Immediate Call Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Vertical service code (VSC)	
Pass VSC to Softswitch	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Return Call (Dial number: *69)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Redial (Dial number: *68)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Don't Disturb (Enable: *78, Disable: *79)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

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

Hot-line: Pre-selected a phone number and set the delay time to **0** to activate the Hot-line feature. When taking the telephone off hook, this outgoing call will route to the pre-selected number without dialing the number.

- ▶ **To make an outgoing call:** Not allowed! Once the Hot-line is being turned ON, no any other outgoing calls are allowed except the hot-line number.
- ▶ **Receive Incoming Call:** Yes. No affected by this feature.

Warm-line: Pre-selected a phone number and pre-configure the delay time **between 1~15 seconds** to activate the Warm-line feature. When the time delay has elapsed after taking the phone off hook, this outgoing call will route to the pre-selected number, no dialing is required.

- ▶ **To make an outgoing call:** Allowed! Replace a call before the delay time has elapsed.
- ▶ **Receive Incoming Call:** Yes. No affected by this feature.

Call Forwarding: All incoming can redirect to any phone number, a mobile number or landline telephone number, to get picked up.

- ▶ **Unconditional forwarding to:** Forward all incoming calls to a pre-selected phone number automatically. Input a phone number in the given space.
- ▶ **On Busy forwarding to:** Forward incoming calls to a pre-selected phone number when the line is busy. Input a phone number in the given space
- ▶ **On No Answer forwarding to ... No Answer Time (Seconds):** Forward incoming calls to a pre-selected phone number when calls are not answered within a certain time in seconds. Input a phone number and time in seconds in the given spaces.

Blind Call Transfer (Flash: *21 + number): A direct call transfer to the second party without speaking to the party. Enable to activate the feature.

1. Hold the original call
2. Press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone until you hear the dial tone
3. Then dial *21 and the number of the second party.

Attended Call Transfer (Flash: *22 + number): Need to consult with the second party before transferring the call. Enable to activate the feature.

1. Hold the original call
2. Press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone until you hear the dial tone
3. Dial *22 and the number of the second party.
4. After speaking with the second party
5. Then press the “Transfer” or “hook flash” button, or quickly tap the on-hook sensor on the phone again to complete the transfer.

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

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

MWI (Message Waiting Indicator): After enabling this feature, users will be able to see light flashing on their phones to indicate the presence of a new voice message.

Anonymous Call: This feature enables you to restrict your phone number from displaying to the called party. When enabled, your phone number will be withheld and not be revealing to the called party.

Block Anonymous Call: All calls from people who have withheld their phone number can get rejected. After enabling this feature, BEC 6300VNL will reject calls with no phone number.

Distinctive Ring: This call feature is only available from a VoIP Service Provider which enables each telephone number to have a distinctive ring sound.

Note: Before enabling this feature, please consult with your VoIP Service Provider to be sure it can be supported.

There is a ringtone list available in the BEC 6300VNL, after enabling this feature, your BEC 6300VNL will adapt a specific ring pattern on the list requested by your VoIP Service Provider for a specific telephone number.

When it is being disabled, all incoming calls will adapt the default ringtone for all telephone lines.

Phone number + “#” Immediate Call Out: Enable to call out immediately after pressing the #.

Pass VSC to Softswitch:

- ▶ **Enable** to pass VSC(Vertical Service Code) to the SIP server of ITSP which allows the SIP server to handle all its unique calling features such as Return Call, Call Redial, Don't Disturb, etc. Under this circumstance, users need to pay for such service, please ensure you check with your SIP provider for more information.
- ▶ **Disable** to let the BEC 6300VNL to handle all available call features.

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

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

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

NAT Traversal for VoIP

BEC 6300VNL VoIP adapts SIP technology as main telephony protocol to provide voice call services over the Internet. This NAT Traversal of SIP feature resolves common NAT / firewall problem when 6300VNL VoIP is behind the NAT / another router to ensure all incoming calls (anyone from outside to place calls) can get picked up and protect the SIP network as well.

NOTE: Use this feature if your BEC 6300VNL is behind another router on a private network and does not obtain a public IP address.

VoIP NAT Traversal	
STUN Server	<input type="text"/> : 3478
External IP	<input type="text"/>
Phone	1 ▼
NAT Traversal method	<input checked="" type="radio"/> None (use local IP address) <input type="radio"/> STUN <input type="radio"/> Use External IP
<input type="button" value="Save"/>	

STUN (Simple Traversal of UDP through NATs) Server: Input STUN server IP address and port number in the given space. STUN server not only checks and discovers the Public WAN IP and port of an external router but also determine the kind of NAT the BEC 6300VNL is behind.

Note: STUN server normally operates on port 3478. If your STUN server uses other port than 3478, make sure you update this information.

External IP: Input a Public WAN IP address of the router in front of the BEC 6300VNL in the given space.

Note: If router's WAN / Public IP changes all the time, it is ideal to use STUN server or consult with your Service Provider if getting a static IP address is feasible; otherwise, manual updating your external router IP address would be required.

Phone: Choose which phone to use NAT traversal when behind another router on a private network.

NAT Traversal Method:

- ▶ **None** to disable the feature
- ▶ Use **STUN server** to do resolve NAT/firewall issue and ensure you input the STUN server IP address in the given space above.
- ▶ Use External IP of the router which is in front of the BEC 6300VNL. Please make sure this external router obtains a public WAN IP address then input this IP address in the given space above.

Example: Making 3-way Calling



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Access Management

Device Management

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

Device Management	
Device Host Name	
Host Name	<input type="text" value="home.gateway"/>
<input type="button" value="Save"/>	
Embedded Web Server	
HTTP Port	<input type="text" value="80"/> (The default HTTP port number is 80.)
HTTPS Port	<input type="text" value="443"/> (The default HTTPS port number is 443.)
TACACS+ (WAN Access)	
TACACS+	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Server Host	<input type="text"/>
Server Port	<input type="text" value="49"/> (The default port number is 49.)
Server Key	<input type="text"/>
<input type="button" value="Save"/>	

Device Host Name

Host Name: Enter the host name of the router. Default is **home.gateway**

Click **Save** to apply settings.

Embedded Web Server

HTTP Port: It is the embedded web server (Web GUI) accessing port, default is **80**. It can be changed other port other than port 80, e.g. port **8080**.

HTTPS Port: Similar to HTTP which is an unencrypted communication using port 80. HTTPS is encrypted by SSL using port 443 instead.

TACACS+ (WAN Access)

TACACS+ (Terminal Access Controller Access Control Service Plus): Click **Activated** to enable the feature. It is an older authentication protocol and used

Server Host: Specify TACACS+ host IP address.

Server Port: Used port 49 (default) to communicate with the TACACS+ client and server.

Server Key: Enter the Preshared key for the TACACS+ host.

Click **Save** to apply settings

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BEC 6300VNL serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.

SNMP	
SNMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Get Community	<input type="text"/>
Set Community	<input type="text"/>
Trap Manager IP	<input type="text" value="0.0.0.0"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
SNMPv3	
SNMPv3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Access Permissions	Read Only ▾
Authentication Protocol	MD5 ▾
Authentication Key	<input type="text"/> (8~31 characters)
Privacy Protocol	DES ▾
Privacy Key	<input type="text"/> (8~31 characters)
<input type="button" value="Save"/>	

SNMP: Activate to enable SNMP.

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

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

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

System Name / Location / Contact: String descriptions of the SNMP agent.

SNMPv3

SNMPv3: Enable to activate the SNMPv3.

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

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

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

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

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

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

Click **Save** to apply settings.

Syslog

Use the Syslog to collect system event information to a remote log server.

▼ Syslog	
Remote System Log	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Server IP Address	<input type="text" value="0.0.0.0"/>
Server UDP Port	<input type="text" value="514"/>
<input type="button" value="Save"/>	

Remote System Log: Select **Activated** to enable this feature

Server IP Address: Assign the remote log server IP address.

Server UDP Port: Assign the remote log server port, 514 is commonly used.

Click **Save** to apply settings.

Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router.

Universal Plug & Play	
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)
<input type="button" value="Save"/>	

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BEC 6300VNL' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BEC 6300VNL so that they can communicate through the BEC 6300VNL, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Click **Save** to apply settings.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS Providers.

If you do not have a DDNS account, please choose a DDNS Service Provider from the list then go to their website to create an account first.

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

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

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

My Host Name: Type the domain name assigned to your BEC 6300VNL by your Dynamic DNS provider.

Username / Password: Enter the user name and password of the account you created with this service provider.

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

Period: Set the time period on how often the BEC 6300VNL will update the DDNS server with your current external IP address.

Click **Save** to apply settings.

Example: How to register a DDNS account

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

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

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

Dynamic DNS	
Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	<input type="text" value="www.dyndns.org (dynamic)"/>
My Host Name	<input type="text" value="myhome.dyndns.org"/>
Username	<input type="text" value="myhome-123"/>
Password	<input type="password" value="*****"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	<input type="text" value="25"/> <input type="text" value="Day(s)"/>
<input type="button" value="Save"/>	

Access Control

Access Control Listing allows you to determine which services/protocols can access BEC 6300VNL interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is **16**.

▼ Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: ▼

Active: Yes No

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

Application: ▼

Interface: ▼

Access Control Listing

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

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

Rule Index: The numeric rule indicator.

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

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BEC 6300VNL. Type an IP address range to restrict access to the client(s) without a matching IP address.

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

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

Click **Save** to apply settings.

By default, the “Access Control” has **two default rules**.

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

▼ Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index:

Active: Yes No

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

Application:

Interface:

Access Control Listing

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

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

▼ Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index:

Active: Yes No

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

Application:

Interface:

Access Control Listing

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

Packet Filter

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

❖ Packet Filter - IP & MAC Filter

Packet Filter

Filter Type: IP & MAC Filter ▼

IP & MAC Filter Editing

Rule Index: 1 ▼

Individual Active: Yes No

Action: Black List ▼

Interface: 4G LTE -1 ▼

Direction: Both ▼

Type: IPv4 ▼

Source IP Address: (0.0.0.0 means Don't care)

Source Subnet Mask:

Source Port Number: (0 means Don't care)

Destination IP Address: (0.0.0.0 means Don't care)

Destination Subnet Mask:

Destination Port Number: (0 means Don't care)

DSCP: (Value Range:0~64, 64 means Don't care)

Protocol: TCP ▼

IP & MAC Filter List

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

IP & MAC Filter Editing

Rule Index: The numeric rule indicator.

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

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

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

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

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

▶ IPv4

► **IPv4 (Cont.)**

Source IP Address	<input type="text" value="0.0.0.0"/>	(0.0.0.0 means Don't care)
Source Subnet Mask	<input type="text" value="0.0.0.0"/>	
Source Port Number	<input type="text" value="0"/>	(0 means Don't care)
Destination IP Address	<input type="text" value="0.0.0.0"/>	(0.0.0.0 means Don't care)
Destination Subnet Mask	<input type="text" value="0.0.0.0"/>	
Destination Port Number	<input type="text" value="0"/>	(0 means Don't care)
DSCP	<input type="text" value="0"/>	(Value Range:0~64, 64 means Don't care)
Protocol	<input type="text" value="TCP"/>	▼

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

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

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

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

Destination Subnet Mask: Enter the subnet mask of the destination network.

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

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

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

► **IPv6**

Source IPv6 Address	<input type="text" value="0:0:0:0:0:0:0:0"/>	(0:0:0:0:0:0:0:0 means Don't care)
Source IPv6 Prefix	<input type="text" value="32"/>	
Source Port Number	<input type="text" value="0"/>	(0 means Don't care)
Destination IPv6 Address	<input type="text" value="0:0:0:0:0:0:0:0"/>	(0:0:0:0:0:0:0:0 means Don't care)
Destination IPv6 Prefix	<input type="text" value="32"/>	
Destination Port Number	<input type="text" value="0"/>	(0 means Don't care)
DSCP	<input type="text" value="0"/>	(Value Range:0~64, 64 means Don't care)
Protocol	<input type="text" value="TCP"/>	▼

Source IP (IPv6) Address/ Prefix: The source IP address or range of packets to be monitored.

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

Destination IP (IPv6) Address/ Prefix: The destination subnet IP address.

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

DSCP: show the set DSCP.

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

▶ **MAC**

Type	MAC ▼
Source MAC Address	<input type="text"/>

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

Click **Save** to apply settings.

❖ Filter Type- URL Filter

Packet Filter

Packet Filter

Filter Type:

URL Filter Editing

URL Filter: Activated Deactivated

URL Filter Rule Index:

Individual Active: Yes No

URL (Host):

URL Filter Listing

Index	Active	URL
-------	--------	-----

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

URL Filter Rule Index: The numeric rule indicator.

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

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

Click **Save** to apply settings.

CWMP (TR-069)

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

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

CWMP (TR-069)	
CWMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ACS Login Information	
URL	<input type="text" value="http://cpe.bectechnologies.com/comserver/node1/tr069"/>
Username	<input type="text" value="testcpe"/>
Password	<input type="text" value="ac5entry"/>
Connection Request Information	
Path	<input type="text"/>
Username	<input type="text" value="conexant"/>
Password	<input type="text" value="welcome"/>
Periodic Inform Config	
Periodic Inform	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Interval	<input type="text" value="870"/>
Bind Wan Interface	
Interface	<input type="text" value="Auto"/>
NATT Config	
NATT Server	<input type="text"/>
NATT Period	<input type="text"/>
<input type="button" value="Save"/>	

ACS Login Information

URL: Enter the ACS server login URL.

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

Password: Enter the ACS server login password.

Connection Request Information

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

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

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

Periodic Inform Config

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

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Bind WAN Interface

Interface: Specify any available or a single WAN interface to handle TR-069 requests.

NATT Config - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

NATT Server: By BEC administrator only.

NATT Period: By BEC administrator only.

Click **Save** to apply settings.

Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.

Parental Control	
Provider	www.opendns.com
Parental Control	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
<p>**Parental Control provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.</p>	
<input type="button" value="Save"/>	

To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Parent Control: Enable the feature by clicking the **Activated**

Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blank.

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply settings.

SAMBA & FTP Server

Samba and FTP are served as network sharing.

SAMBA & FTP Server	
SAMBA	
SAMBA Server	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Work Group	<input type="text" value="MyGroup"/>
Net BIOS Name	<input type="text" value="SambaSvr"/>
FTP	
FTP Server	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
FTP Server Port	<input type="text" value="21"/>
<input type="button" value="Save"/>	

SAMBA:

SAMBA Server: Activated to enable SAMBA sharing.

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

NetBIOS Name: The sharing NetBIOS name.

FTP:

FTP Server: Activated to enable FTP sharing.

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

SAMBA/FTP Login Account: See [User Management](#) for more information.

- ▶ **Default user:** admin/admin, it is the administrative user and a super user; it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.
- ▶ **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

Example: How to setup Samba

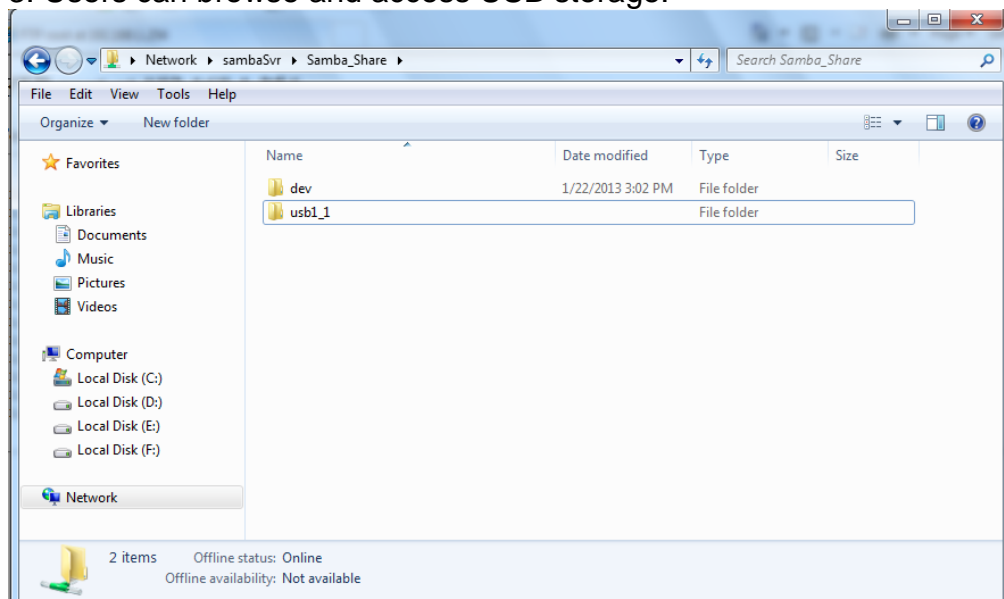
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.

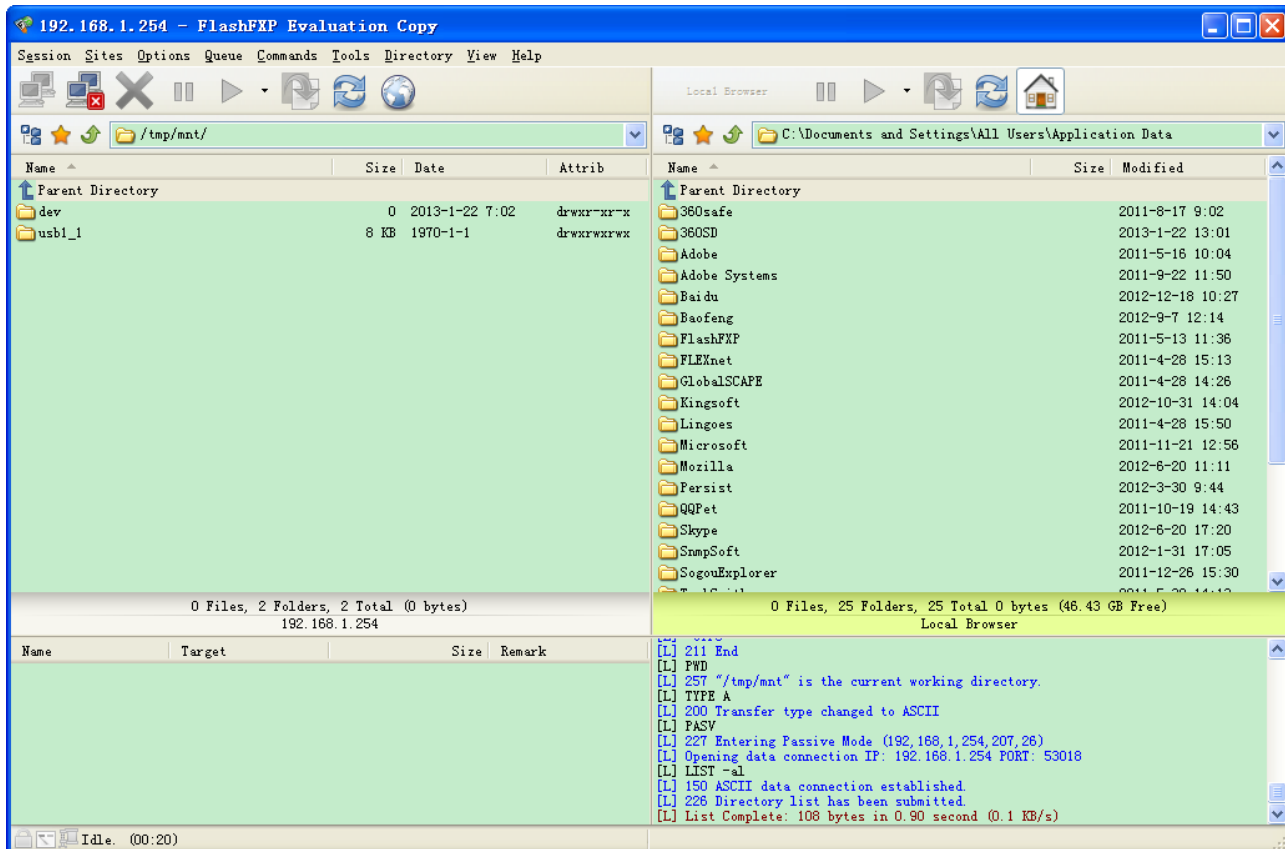


Example: How to setup FTP :

1. Access via FTP tools

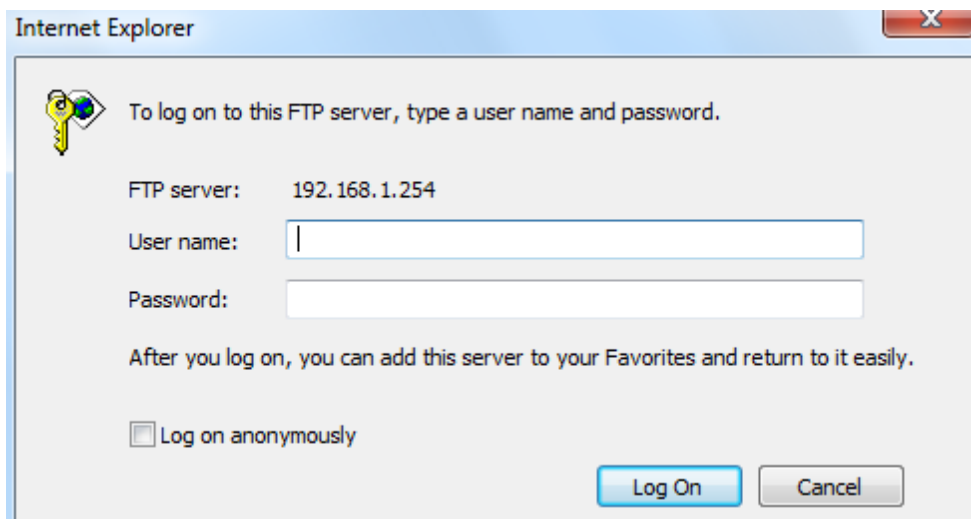
Take popular FTP tool of FlashFXP for example:

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



2. Web FTP access

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



BECentral Management

BECentral is a cloud based device management platform that provides operators with a comprehensive suite of services to manage devices in real-time.

▼ BECentral Management	
BECentral Management	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
BECentral Management URL	<input type="text" value="becentral.becloud.io"/>
BECentral Management Port	<input type="text" value="48883"/>
Organization ID	<input type="text" value="DEFAULT"/>
Device Report Interval	<input type="text" value="480"/>
Interface	<input type="text" value="ALL"/> ▼
<input type="button" value="Save"/>	

BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral.

BECentral Management Port: Port listened by the BECentral.

Organization ID: Customer ID

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

Interface: Specify any available or a single WAN interface to handle BECentral requests.

Maintenance – User Management (Administrator Account)

Maintenance

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

User Management

User Management controls the Router Web GUI permission, FTP/SAMBA access to the specific account.

In factory setting, the default accounts are **admin/admin** and **user/user**. The default root account admin has been authorized to web access of router, Samba access, and FTP access. **user/user** is equipment with limited access (specified by advanced users with admin account) to router web, and FTP/SAMBA . A total of **6** other accounts can be created to grant access to the access of Samba and FTP and web page (need to be specified).

Note: Please go to [SAMBA & FTP Server](#) to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.

❖ Administrator Account

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

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

The screenshot displays the 'User Management' configuration page in the router's web interface. It includes a 'User Account' section with a dropdown for 'Index' (set to 1), text boxes for 'Username' (admin), 'New Password', and 'Confirm Password'. Below this are 'FTP Authority Setup' and 'SAMBA Authority Setup' sections, each with radio buttons for 'Enable' and 'Disable', and another set of radio buttons for 'Read/Write' and 'Read' permissions. A note at the bottom of the form says '**Please restart the Storage server after config changed**'. At the bottom of the page, there is a 'User Account List' table with the following data:

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

User Setup

Index: The numeric account indicator. The maximum entry is up to 8 accounts.

User Name: Create account(s) user name for GUI management.

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

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

FTP Authority Setup

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

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

SAMBA Authority

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

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

❖ **User Account (Adding additional user accounts)**

user/user is the default user account username and password

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

User Management

User Account

Index: 2

Username: user

New Password: [masked]

Confirm Password: [masked]

FTP Authority Setup

FTP Access: Enable Disable

Permission: Read/Write Read

SAMBA Authority Setup

SAMBA Access: Enable Disable

Permission: Read/Write Read

Web GUI Permission

Guest Account: Enable Disable

Interface Setup: Enable Disable

Advanced Setup: Enable Disable

VOIP Setup: Enable Disable

Access Management: Enable Disable

Maintenance: Enable Disable

Please restart the Storage server after config changed

Save Delete

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

User Setup

Index #: The numeric account indicator. The maximum entry is up to 8.

User Name: Create account(s) user name for GUI management.

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

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

FTP Authority Setup

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

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

SAMBA Authority

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

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

Web GUI Permission

Guest Account: Enable to create this new guest account.

Interface Setup / Advanced Setup / VPN Setup / Access Management / Maintenance: Enable to grant this user access to these features.

When someone accesses to the BEC 6300VNL using this “user” account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account.

Click **Save** to apply settings.

Click **Save** to apply the settings.

Time Zone

With default, 6300VNL does not contain the correct local time and date.

There are several options to setup, maintain, and configure current local time/date on the 6300VNL. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.

Time Zone	
Current Date/Time	N/A (Can't find NTP server)
Time Synchronization	
Synchronize time with	<input checked="" type="radio"/> NTP Server <input type="radio"/> PC's Clock <input type="radio"/> Manually
Time Zone	(GMT-06:00) Central Time (US & Canada), Maxico City, Saskatchewan ▼
Daylight Saving	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
NTP Server Address	<input type="text" value="0.0.0.0"/> (0.0.0.0: Default Value)
<input type="button" value="Save"/>	

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

- ▶ **NTP Server automatically:** To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, BEC 6300VNL will retrieve the correct local time from the SNTP server this is specified.
- ▶ **PC's Clock:** To synchronize time with the PC's clock.
- ▶ **Manually:** Select this to enter the SNMP server IP address manually.
 - ◆ **Date:** Month / Date / Year. Month – 1 ~ 12 (January ~ December).
 - ◆ **Time:** Hour: Minute: Second

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

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

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

Click **Save** to apply settings.

License

Some of the advanced features are required for a license. For more information, please contact with Billion/BEC for more information.

Input your license key here and click “Upgrade” to enable the features.

NOTE: Device will reboot after the upgrade.

▼ License	
License	<input type="text"/>
Status	
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade	
<input type="button" value="Upgrade"/>	

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your BEC 6300VNL provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of BEC 6300VNL, you should download or copy the firmware to your local environment first. Press the “**Browse...**” button to specify the path of the firmware file. Then, click “**Upgrade**” to start upgrading. When the procedure is completed, BEC 6300VNL will reset automatically to make the new firmware work.

Firmware & Configuraiton	
Upgrade	<input checked="" type="radio"/> Firmware <input type="radio"/> Configuration
System Restart with	<input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings
File	<input type="button" value="Choose File"/> No file chosen
Backup Configuration	<input type="button" value="Backup"/>
Status	
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.	
<input type="button" value="Upgrade"/>	

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

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

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

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

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your BEC 6300VNL device when making false configurations and want to restore to the original settings.

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

Firmware Upgrade	
File upload succeeded, starting flash erasing and programming!!	
Progress	<div style="width: 15%; height: 10px; background-color: #0070C0;"></div>
Percent	15 %

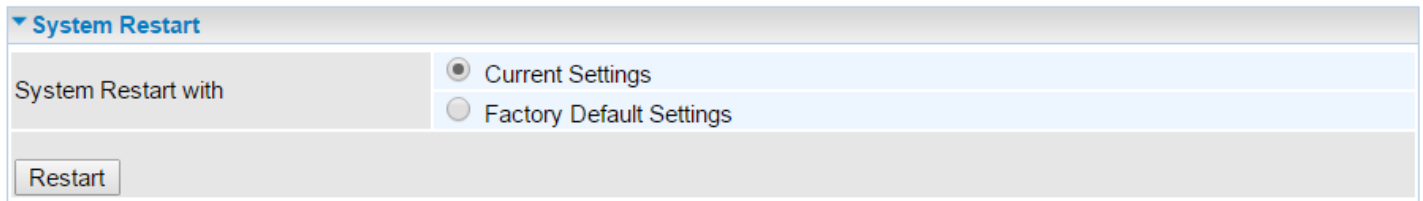


DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your RidgeWave 6900.

System Restart

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



The screenshot shows a web interface for system restart. At the top, there is a dropdown menu labeled "System Restart". Below it, there is a section titled "System Restart with" containing two radio button options: "Current Settings" (which is selected) and "Factory Default Settings". At the bottom of this section, there is a "Restart" button.

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

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

Auto Reboot

Schedule an automatic reboot for your BEC 6300VNL to ensure proper operation and best performance.

This reboot will only reboot with current configuration settings and not overwrite any existing settings.

▼ Auto Reboot										
Schedule	1.	<input type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time <input type="text" value="00"/> : <input type="text" value="00"/>
	2.	<input type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time <input type="text" value="00"/> : <input type="text" value="00"/>
<input type="button" value="Save"/>										

Click **Save** to apply settings

Example: Schedule BEC 6300VNL to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.

▼ Auto Reboot										
Schedule	1.	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Mon.	<input checked="" type="checkbox"/> Tues.	<input checked="" type="checkbox"/> Wed.	<input checked="" type="checkbox"/> Thur.	<input checked="" type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time <input type="text" value="22"/> : <input type="text" value="00"/>
	2.	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Mon.	<input type="checkbox"/> Tues.	<input type="checkbox"/> Wed.	<input type="checkbox"/> Thur.	<input type="checkbox"/> Fri.	<input type="checkbox"/> Sat.	<input type="checkbox"/> Sun.	Time <input type="text" value="09"/> : <input type="text" value="00"/>
<input type="button" value="Save"/>										

Diagnostics Tool

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

3G/4G-LTE / 3G/4G-LTE USB / EWAN

Diagnostic Tool	
WAN Interface	EWAN(LAN1) ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address or Domain <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
<input type="button" value="Start"/>	
Trace Route <input type="radio"/> Yes <input checked="" type="radio"/> No	
<input type="button" value="Start Trace Route"/>	

Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

Click **START** to begin to diagnose the connection.

Diagnostic Tool	
WAN Interface	4G/LTE ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
<input type="button" value="Start"/>	

Trace Route is to display how many hops (also view the exact hops) the packet of data has to take to get to the destination.

Click **Yes**, enter the IP address or domain then **Start Trace Route**.

Trace Route <input checked="" type="radio"/> Yes <input type="radio"/> No	
IP Address or Domain	<input type="text"/>
Max TTL Value	16 [2-30]
<input type="button" value="Start Trace Route"/>	

IP Address or Domain: Set the destination host (IP, domain name) to be traced.

Max TTL value: Set the max Time to live (TTL) value.

Shown as we “trace” www.billion.com below.

```

Trace www.billion.com

tracert to www.billion.com (125.227.205.188), 16 hops max, 60 byte packets
 1  172.16.1.254 (172.16.1.254)  0.472 ms  0.488 ms  0.643 ms
 2  122.96.153.233 (122.96.153.233)  7.354 ms  7.517 ms  7.704 ms
 3  221.6.12.69 (221.6.12.69)  7.921 ms  8.108 ms  8.256 ms
 4  221.6.1.253 (221.6.1.253)  8.392 ms  8.544 ms  *
 5  219.158.99.245 (219.158.99.245)  36.110 ms  36.839 ms  37.001 ms
 6  * * *
 7  * * 219.158.103.26 (219.158.103.26)  40.731 ms
 8  211.72.233.194 (211.72.233.194)  65.969 ms  66.040 ms  66.019 ms
 9  220.128.6.126 (220.128.6.126)  61.726 ms  61.831 ms  61.960 ms
10  220.128.11.170 (220.128.11.170)  61.543 ms  61.583 ms  65.127 ms
11  220.128.17.85 (220.128.17.85)  63.436 ms  62.133 ms  65.862 ms
12  220.128.17.229 (220.128.17.229)  64.695 ms  64.849 ms  65.063 ms
13  168.95.229.145 (168.95.229.145)  61.915 ms  60.715 ms  60.825 ms
14  * * *
15  * * *
16  * * *
    
```

LAN

Diagnostic Tool

WAN Interface	LAN
Testing Ethernet LAN Connection	PASS
Ping other IP Address or Domain <input checked="" type="radio"/> Yes <input type="radio"/> No	Skipped
IP Address or Domain	N/A

Start

Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

Click **START** to begin to diagnose the connection.

CHAPTER 5: TROUBLESHOOTING

If your **BEC 6300VNL** is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

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

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not 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
<ul style="list-style-type: none">- The front LEDs display incorrectly- Still cannot access to the router management interface after pressing the RESET button.- Software / Firmware upgrade failure	<ol style="list-style-type: none">1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately.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.

FCC Statement

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

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

FCC Caution:

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

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

Co-location statement

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

FCC Radiation Exposure Statement

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

IC Regulations

IC Warning

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (identifier le dispositif par son numéro de certification ou son numéro de modèle s'il fait partie du matériel de catégorie I) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Detachable Antenna Usage

This device has been designed to operate with an antenna having a maximum gain of 2.5dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (IC: 5315A- 6300VNOZ / Model: BEC 6300VNL ; BEC 6300 ; RidgeWave 6300VNL ; BEC 6300NEL ; RidgeWave 6300NEL) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated.

Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de dB 2.5. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent émetteur radio (IC: 5315A-6300VNOZ / Model: BEC 6300VNL ; BEC 6300 ; RidgeWave 6300VNL ; BEC 6300NEL ; RidgeWave 6300NEL) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Approved antennas list

Type	Gain	Brand	Manufacture
Dipole	1.5dBi	BEC	INVAX System Technology Corp.
Dipole	2.5dBi	BEC	INVAX System Technology Corp.