



BEC 6300VNL

GigaConnect[®] Wireless Broadband Router

User Manual

TABLE OF CONTENTS

TABLE OF CONTENTS	2
CHAPTER 1: INTRODUCTION	1
INTRODUCTION TO YOUR ROUTER	1
FEATURES & SPECIFICATIONS	3
HARDWARE SPECIFICATIONS	5
APPLICATION DIAGRAMS	6
CHAPTER 2: PRODUCT OVERVIEW	7
IMPORTANT NOTE FOR USING THIS ROUTER	7
PACKAGE CONTENTS	7
DEVICE DESCRIPTION	8
Front Panel LEDs	8
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	24
Configuring PC in Windows 10 (IPv6)	24
Configuring PC in Windows 7/8 (IPv6)	26
Configuring PC in Windows Vista (IPv6)	28
Configuring PC in Windows XP (IPv6)	30

DEFAULT SETTINGS.....	31
INFORMATION FROM YOUR ISP	32
CHAPTER 4: DEVICE CONFIGURATION.....	33
LOGIN TO YOUR DEVICE	33
STATUS.....	35
Device Info	36
System Status	38
System Log	38
3G/4G-LTE Status.....	39
Statistics	40
DHCP Table.....	44
Disk Status.....	44
IPSec Status	45
PPTP Status	46
L2TP Status.....	47
GRE Status.....	47
VoIP Status	48
QUICK START	49
CONFIGURATION.....	52
Interface Setup.....	52
<i>Internet</i>	53
<i>LAN</i>	60
<i>Wireless</i>	64
<i>Wireless MAC Filter</i>	75
Advanced Setup	76
<i>Firewall</i>	76
<i>Routing</i>	77
<i>NAT</i>	78
<i>Static DNS</i>	83
<i>QoS</i>	84
<i>Interface Grouping</i>	85
<i>Time Schedule</i>	87
<i>Mail Alert</i>	88
VPN	89
<i>IPSec</i>	89
<i>PPTP Server</i>	99
<i>PPTP Client</i>	100

<i>L2TP</i>	104
<i>GRE Tunnel</i>	112
Access Management	114
<i>Device Management</i>	114
<i>SNMP</i>	115
<i>Remote Syslog</i>	116
<i>Universal Plug & Play</i>	116
<i>Dynamic DNS</i>	117
<i>Access Control</i>	119
<i>Packet Filter</i>	121
<i>Parental Control</i>	124
<i>SAMBA & FTP Server</i>	125
Maintenance	128
<i>User Management</i>	128
<i>Time Zone</i>	132
<i>Firmware & Configuration</i>	133
<i>System Restart</i>	134
<i>Auto Reboot</i>	135
<i>Diagnostics Tool</i>	136

CHAPTER 5: TROUBLESHOOTING 138

Problems with the Router	138
Problem with LAN Interface	138
Recovery Procedures.....	139

APPENDIX: PRODUCT SUPPORT & CONTACT 140

FCC STATEMENT	141
IC REGULATIONS	142
IC Warning.....	142
Detachable Antenna Usage	143

CHAPTER 1: INTRODUCTION

Introduction to your Router

Congratulations on your purchase of the **BEC 6300VNL (Wireless Broadband Router)**. This router is a compact and advanced broadband router that offers flexible and multiple Internet connection options, EWAN and embedded 3G/EVDO 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 (3G/EVDO Wireless Broadband Router)** provides a unique Management Center enabling users to monitor 3G/EVDO signal strength, bandwidth, download speed, and many more.

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 (3G/EVDO 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.

3G/EVDO Management Center

BEC 6300VNL (3G/EVDO VoIP Wireless Broadband Router) Mobile Management Center visually displays its current 3G/EVDO signal status also calculates the total amount of hours or data traffic used per month, allowing you to manage your 3G/EVDO 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

- 3G/EVDO for 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
- 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

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

Hardware Specifications

Physical interface

- Cellular antenna: 2 external antennas
- SIM card slot: Mini SIM card (2FF) slot for mobile broadband connectivity
- 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

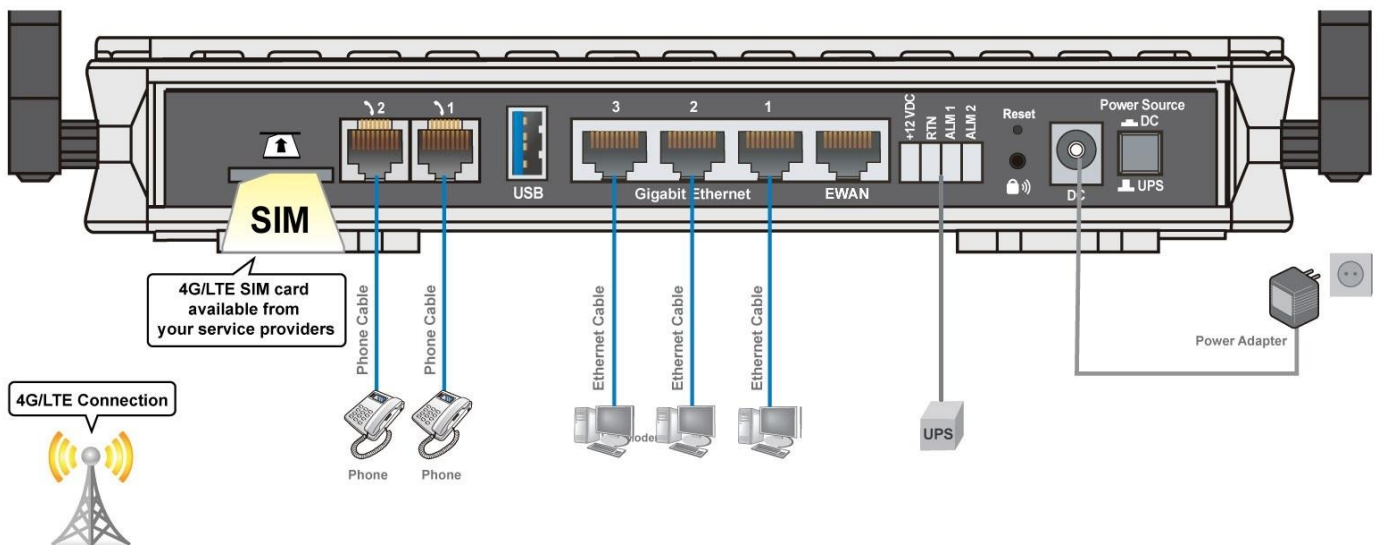
- Dimensions (W*H*D): 9.04" x 6.10" x 1.27"(229.5mm x 155mm x 32.24mm)

Application Diagrams

BEC 6300VNL (3G/EVDO VoIP Wireless Broadband Router) is an all-in-one router, supporting 2 connection options (3G/EVDO and EWAN) to connect to the Internet.

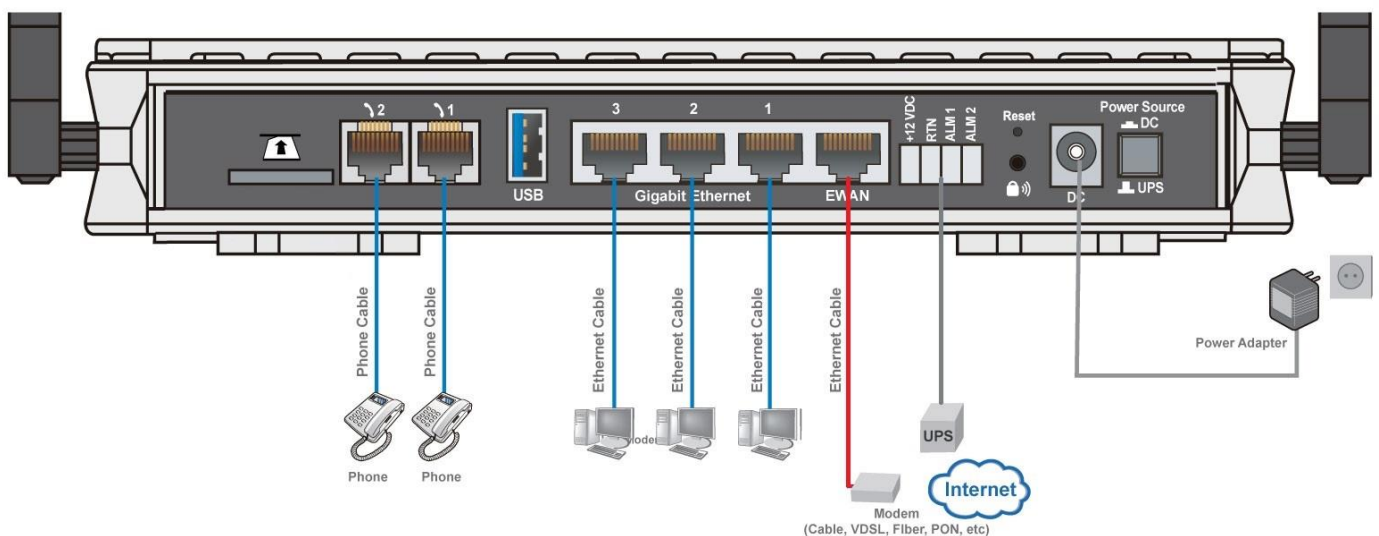
3G/EVDO router mode

With an embedded 3G/EVDO 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

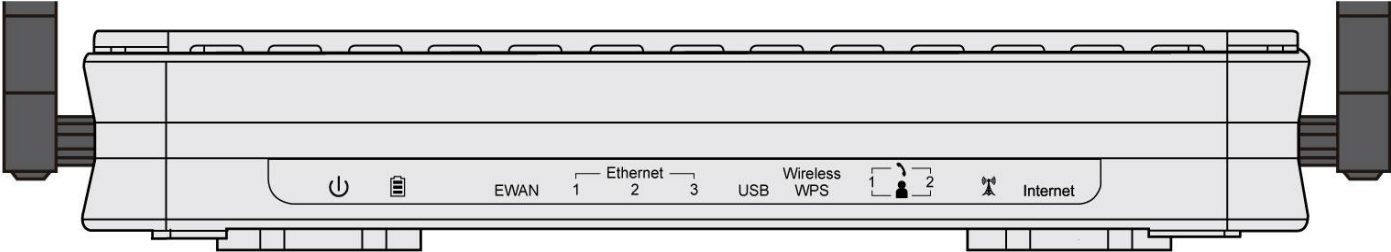
- ✓ Place the router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.





Package Contents

- ✓ BEC 6300VNL 3G/EVDO VoIP Wireless Broadband Router x 1
- ✓ Quick Start Guide x 1
- ✓ RJ-45 Ethernet cable x 1
- ✓ 3G/EVDO detachable antennas x 2
- ✓ DC Power adapter x 1

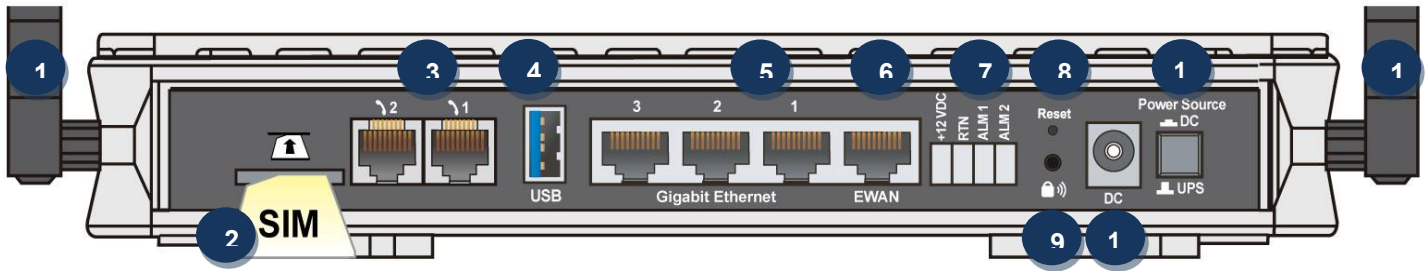
Device Description

Front Panel LEDs



LED	STATUS	DESCRIPTION
Power 	Green	System is up and ready
	Red	Boot failure
Battery 	Green	UPS is functioning properly
	Orange	UPS battery failure. Need a new battery replacement
	Orange blinking	UPS AC power failure and battery functioning properly
	Off	Device powered by the DC power adaptor
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 3G/EVDO module is in service
	Off	No 3G/EVDO module or 3G/EVDO module fails
Internet	Green	IP connected and traffic is passing through the device.
	Red	IP request failed.
	Off	BEC 6300VNL is either in bridged mode or WAN connection not ready.

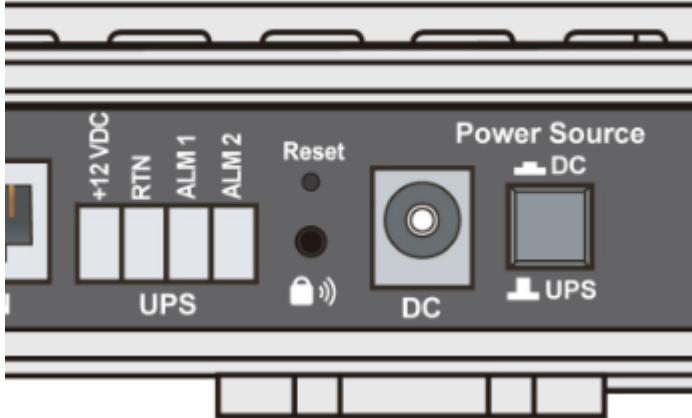
Rear Panel Connectors



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	Connect an external USB dongle / hard drive for storage, network sharing, etc.
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 the reset button for 10 seconds 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 a few seconds to trigger WPS function. (2) Wireless ON/OFF button : Press & hold the button for 10 seconds to turn On/Off 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 adaptor (2) with Power Switch OFF : power up by the UPS battery unit

Power Source

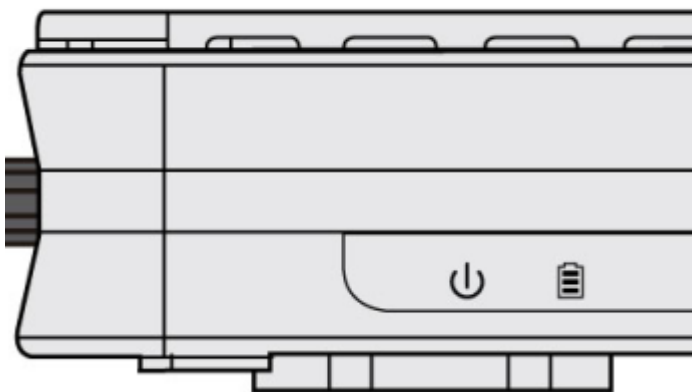
BEC 6300VNL offers two kinds of power input, namely, **DC power Adapter** and **DC UPS** (or BBU). BEC 6300VNL can take the advantage of UPS (Uninterruptible Power Supply) to keep working even if the power outage hit your router when the router is working in DC UPS mode.



(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 adaptor and external UPS battery

Pressed "Power Source" button, the button is visually being pressed down. The power source is from the DC power adaptor 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 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, 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

When the 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 When the Internet LED turns red, the firmware upgrade is in process.
DO NOT power off or reboot the device, it would permanently damage your 6300VNL.
- 3.4 When the Internet LED turns green, the firmware upgrade is complete.
- 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.

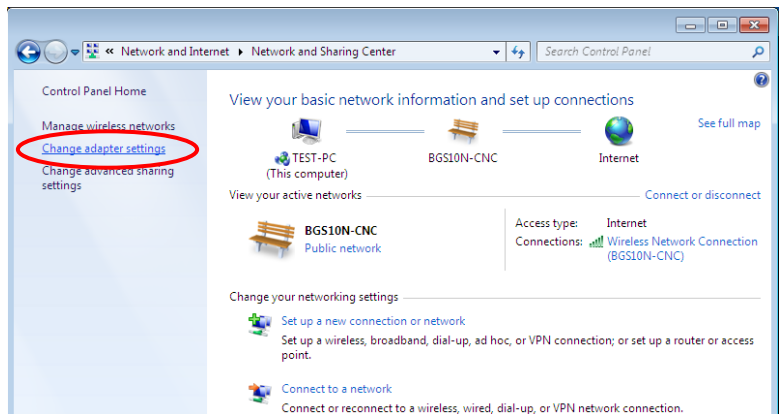
Network Configuration – IPv4

Configuring PC in Windows 10 (IPv4)

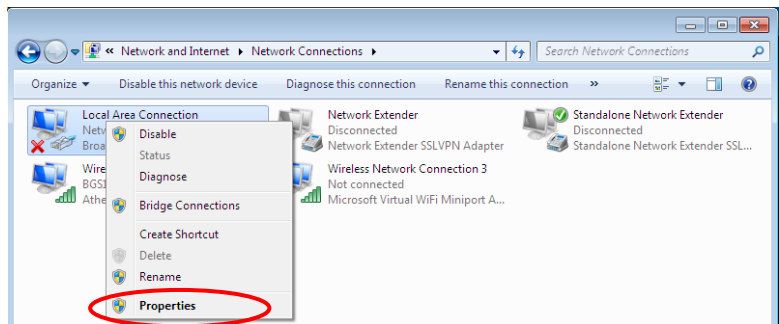
1. Click .
2. Click  Settings
3. Then click on **Network and Internet**. 
4. Under **Related settings**, select **Network and Sharing Center**

- Related settings
- Change adapter options
- Change advanced sharing options
- Network and Sharing Center**
- HomeGroup
- Internet options
- Windows Firewall

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

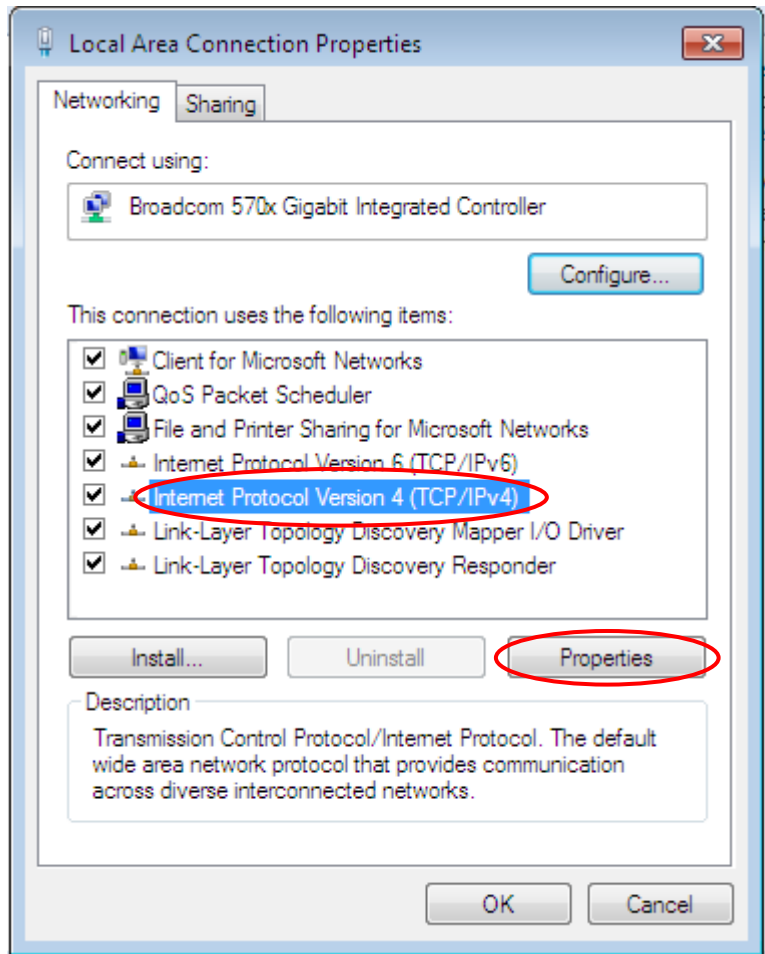


6. Select the **Local Area Connection**, and right click the icon to select **Properties**.



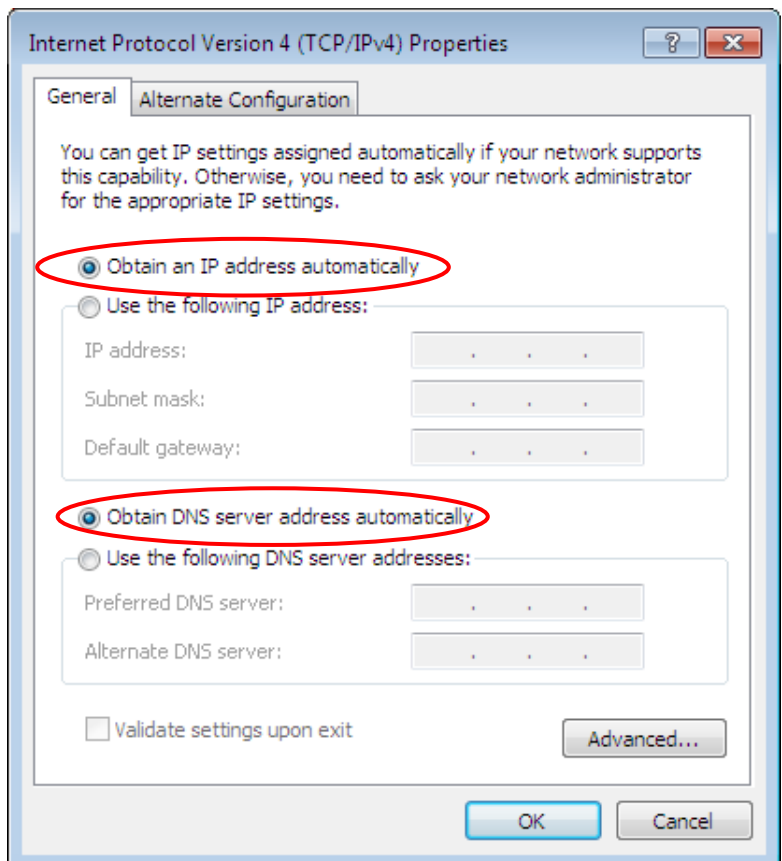
Network Configuration – Windows 10 (IPv4)

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



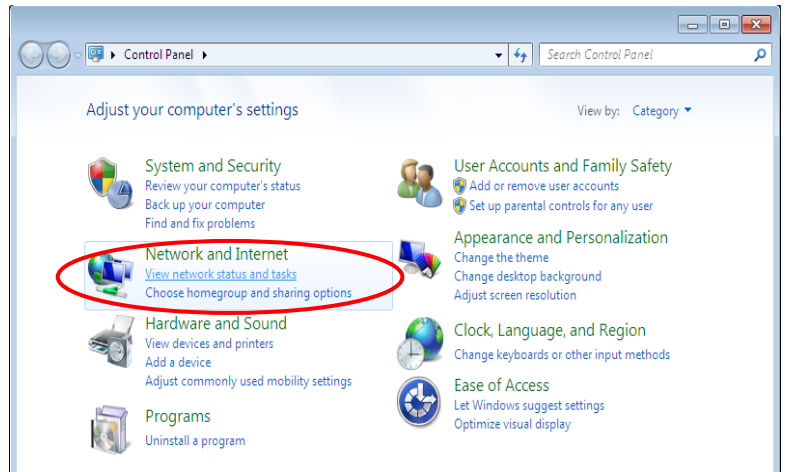
8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

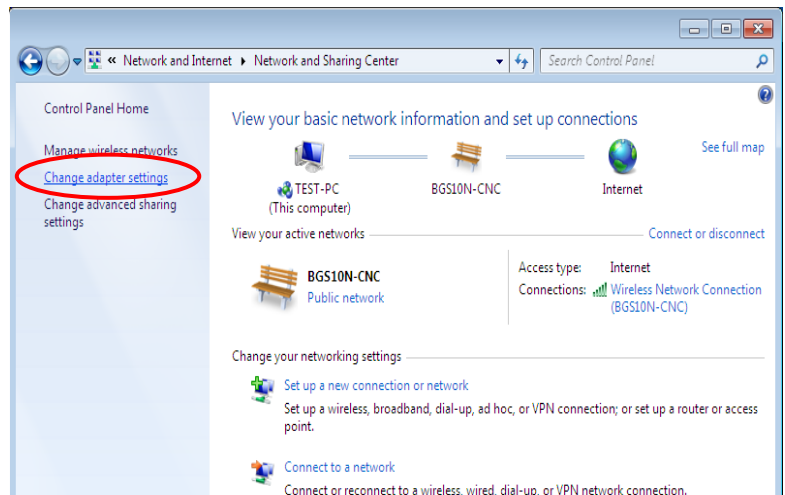


Configuring PC in Windows 7/8 (IPv4)

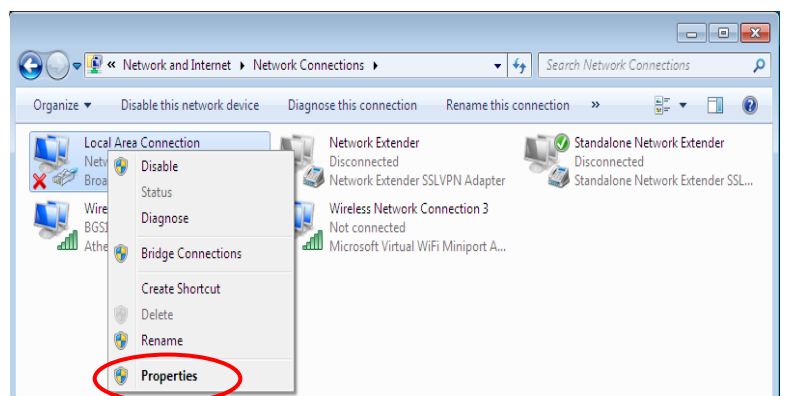
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



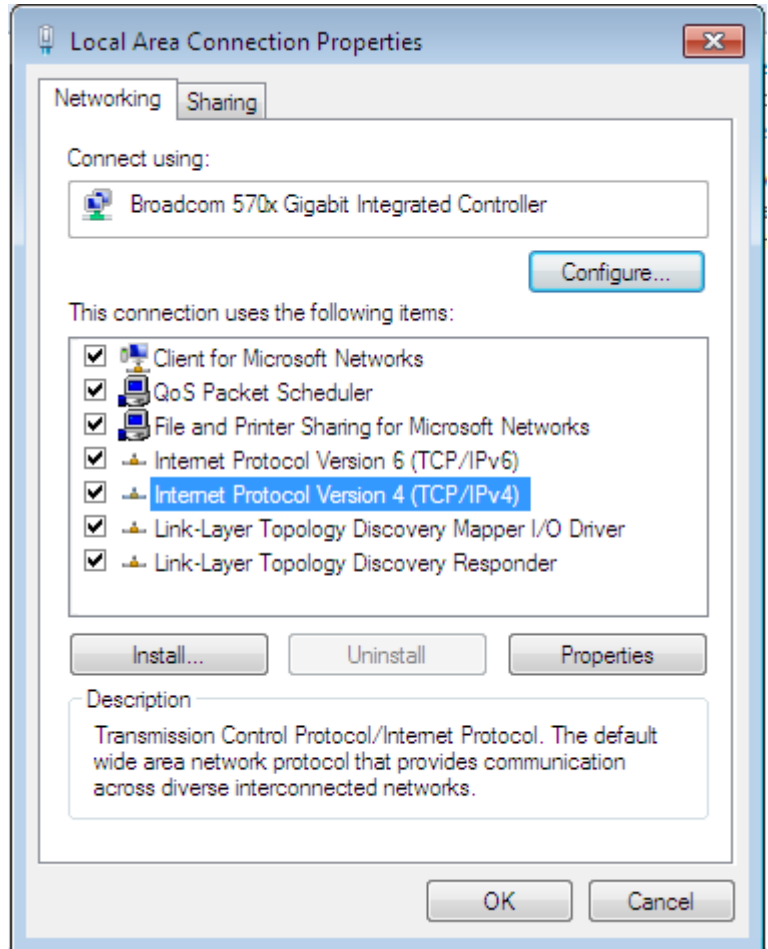
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



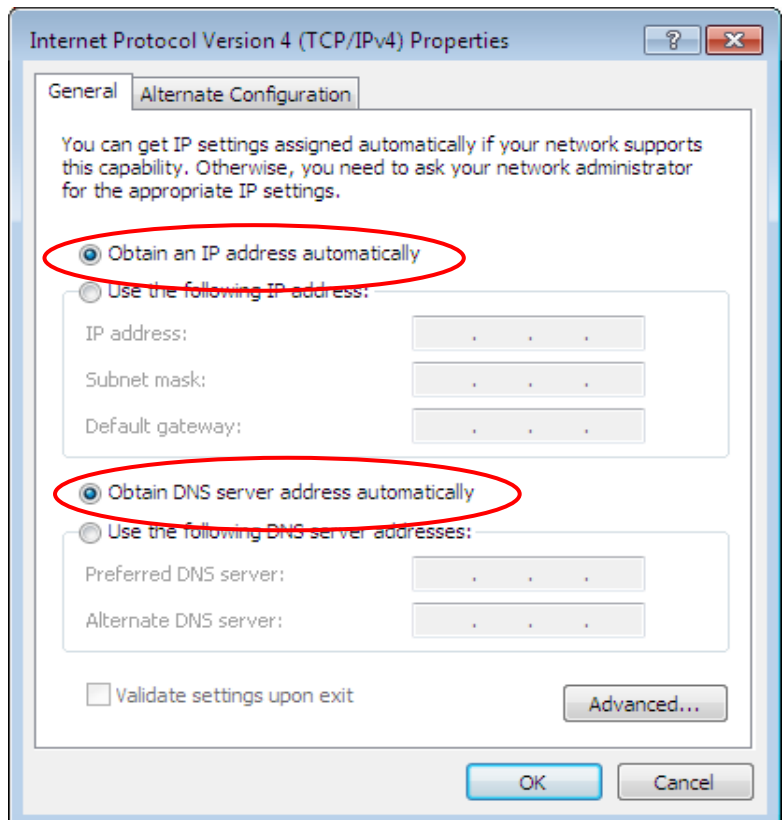
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

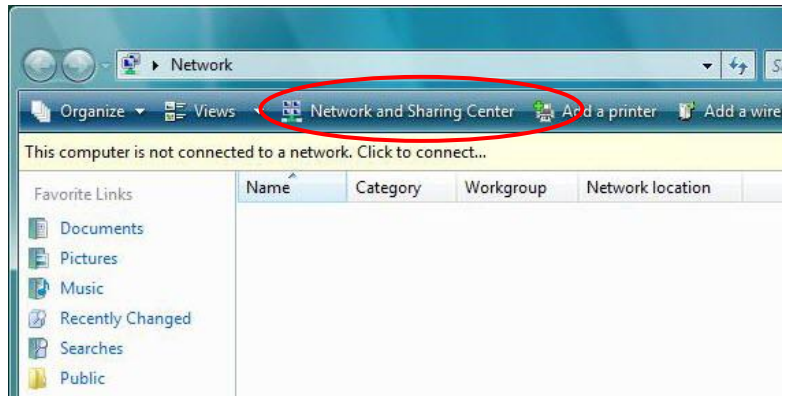


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

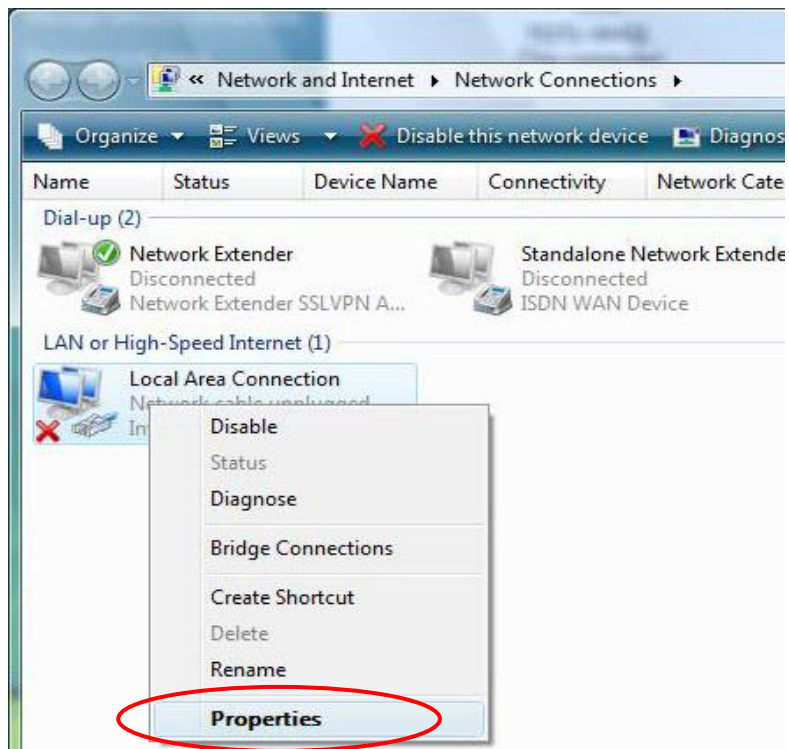
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



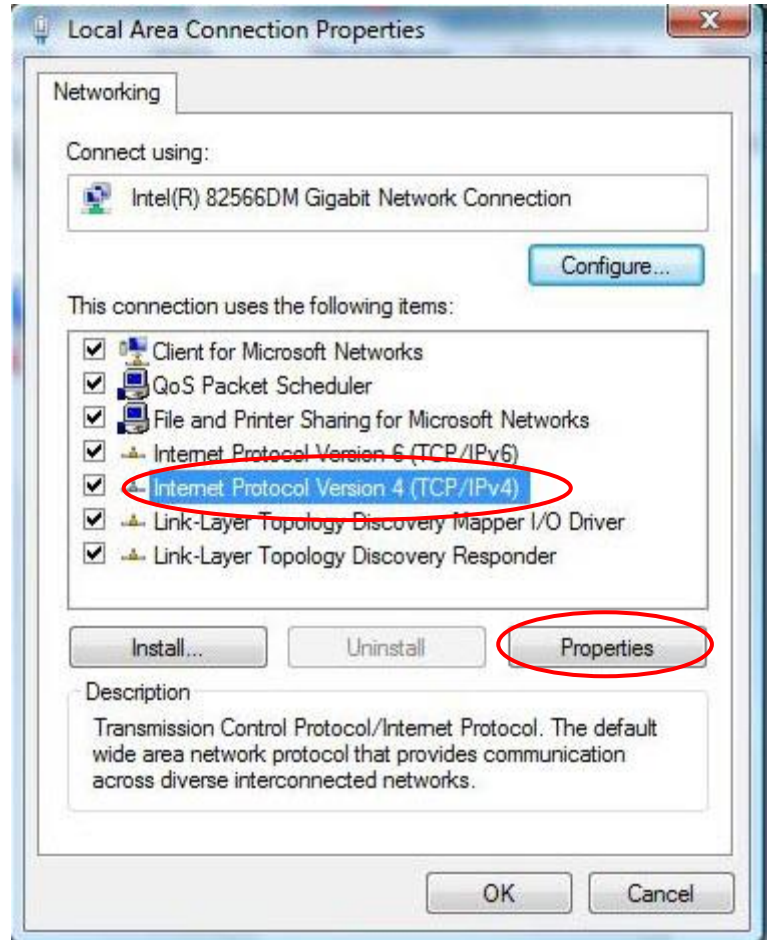
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



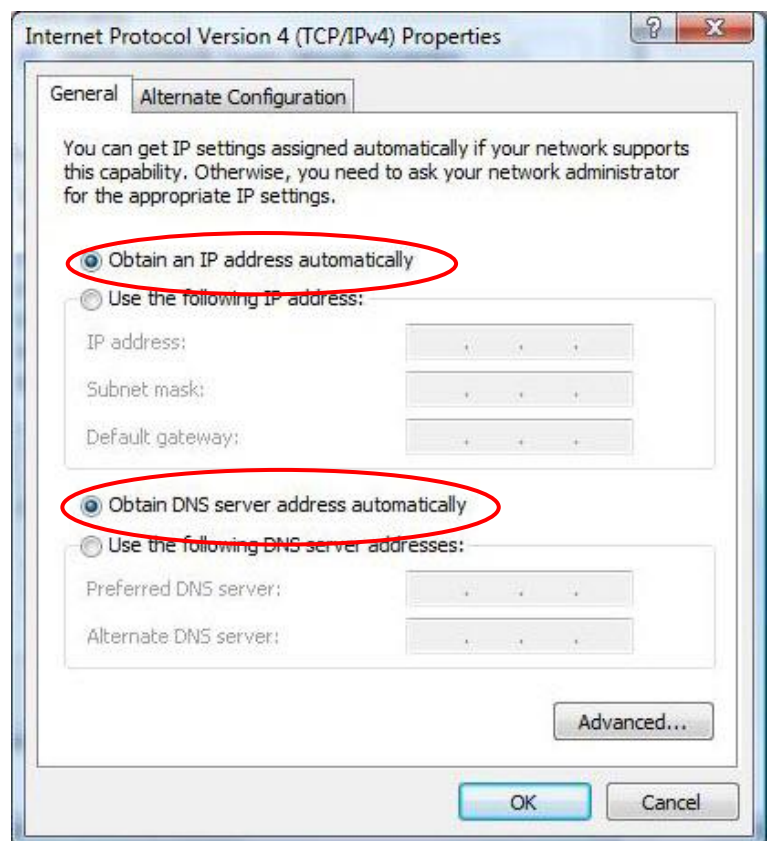
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

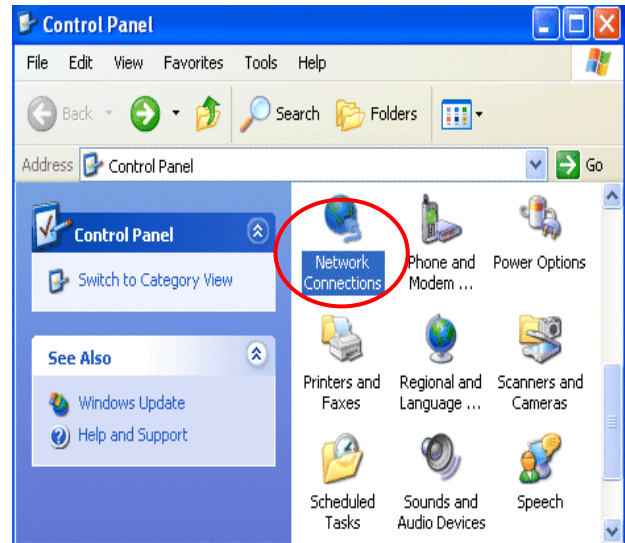


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

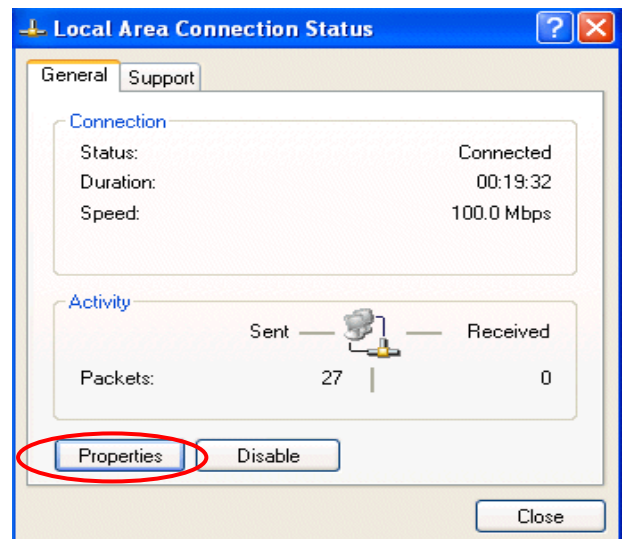


Configuring PC in Windows XP (IPv4)

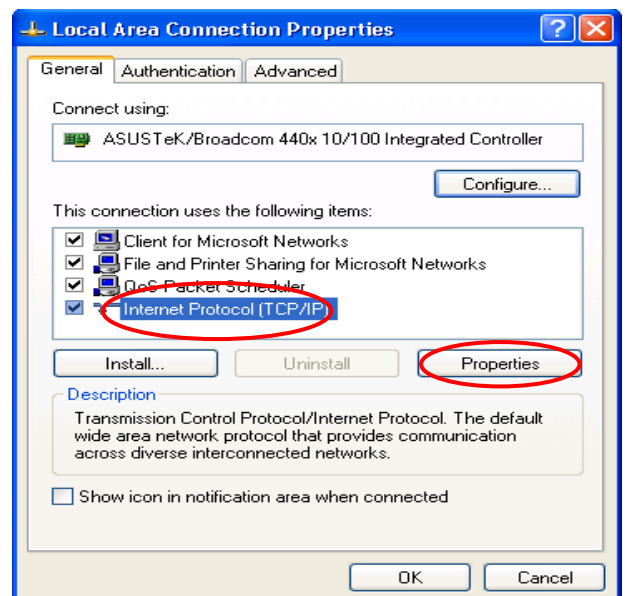
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



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

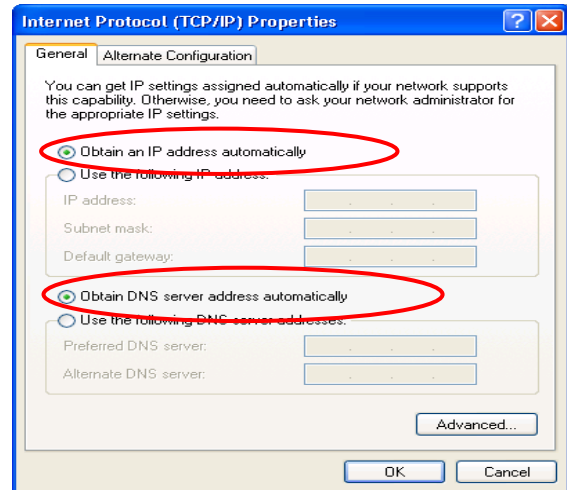


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.






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  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.

Related settings

Change adapter options

Change advanced sharing options

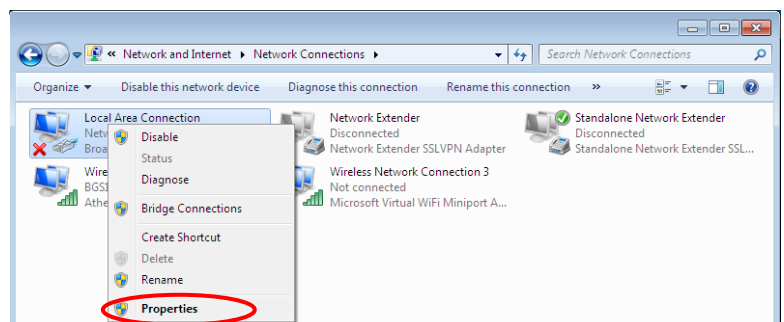
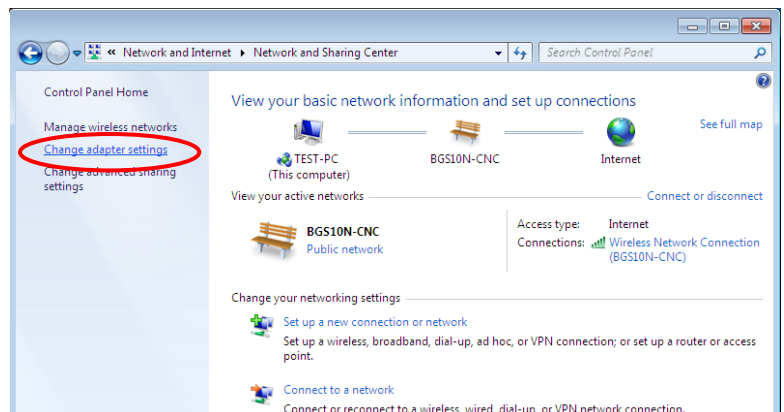
Network and Sharing Center

HomeGroup

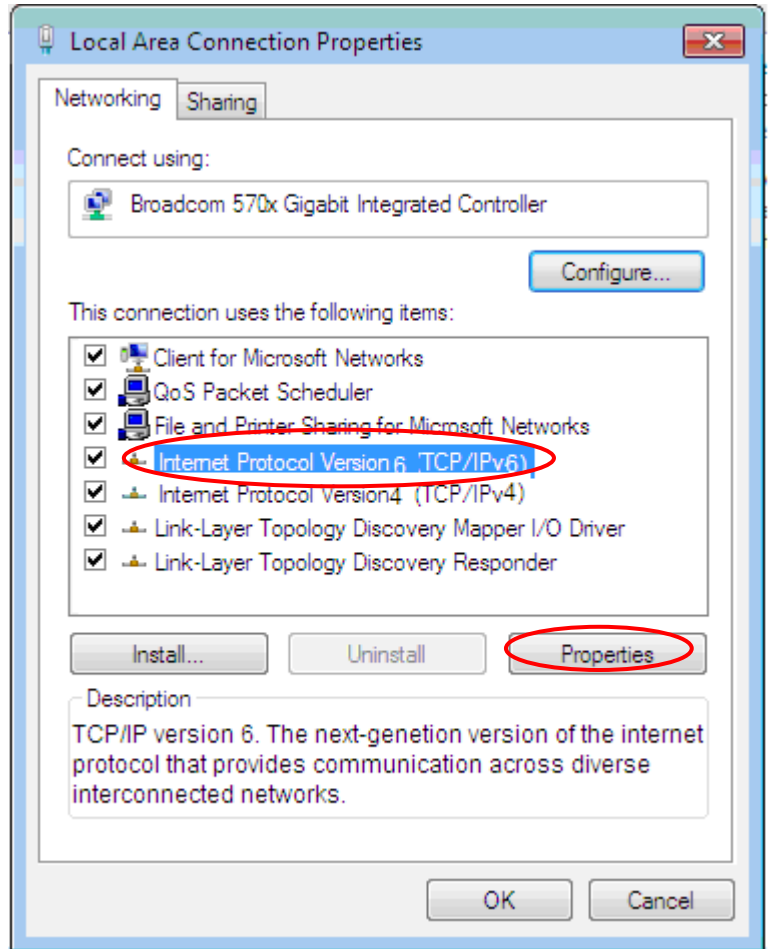
Internet options

Windows Firewall

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

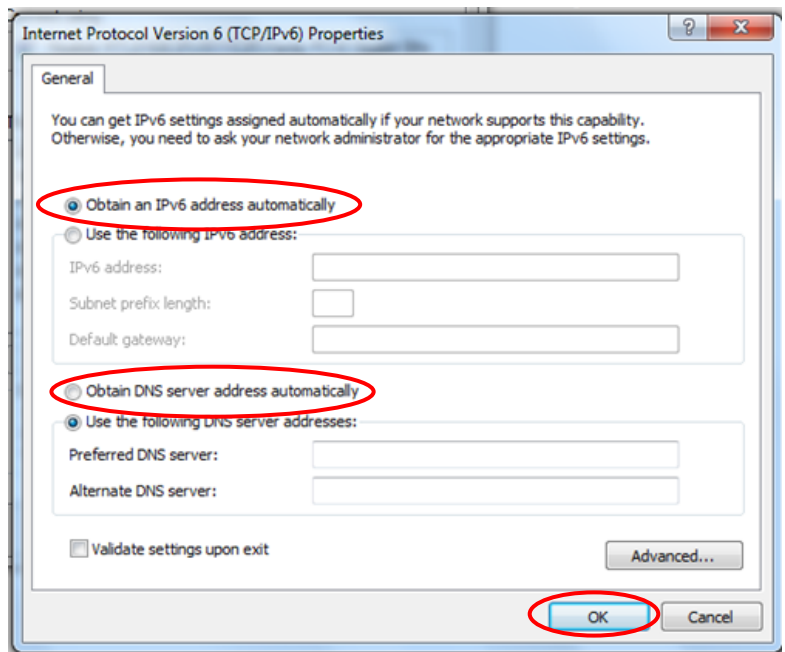


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



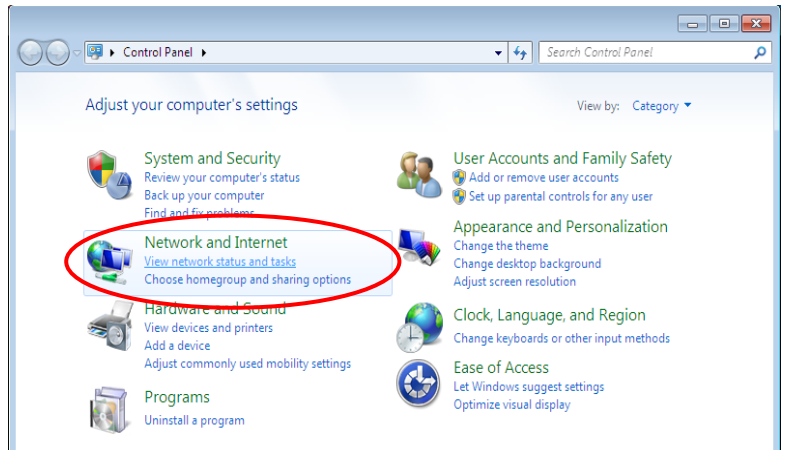
8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

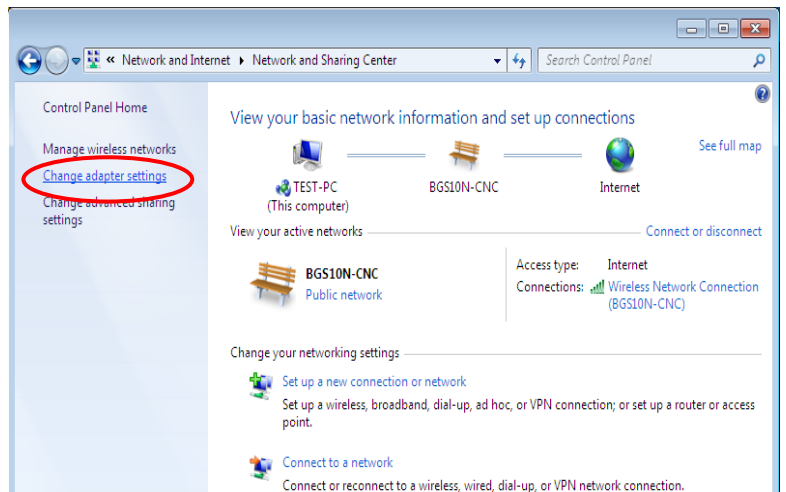


Configuring PC in Windows 7/8 (IPv6)

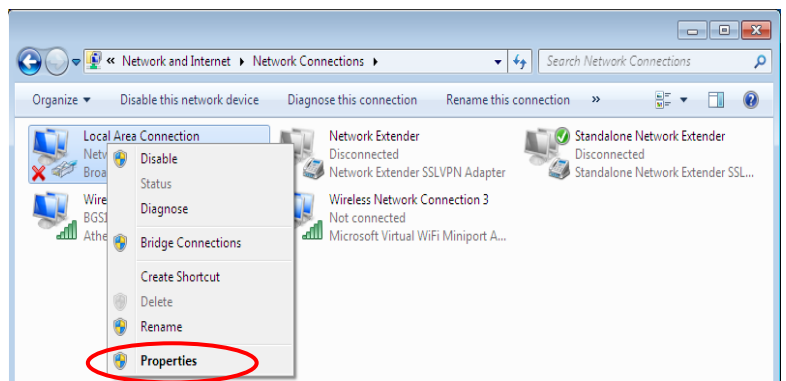
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



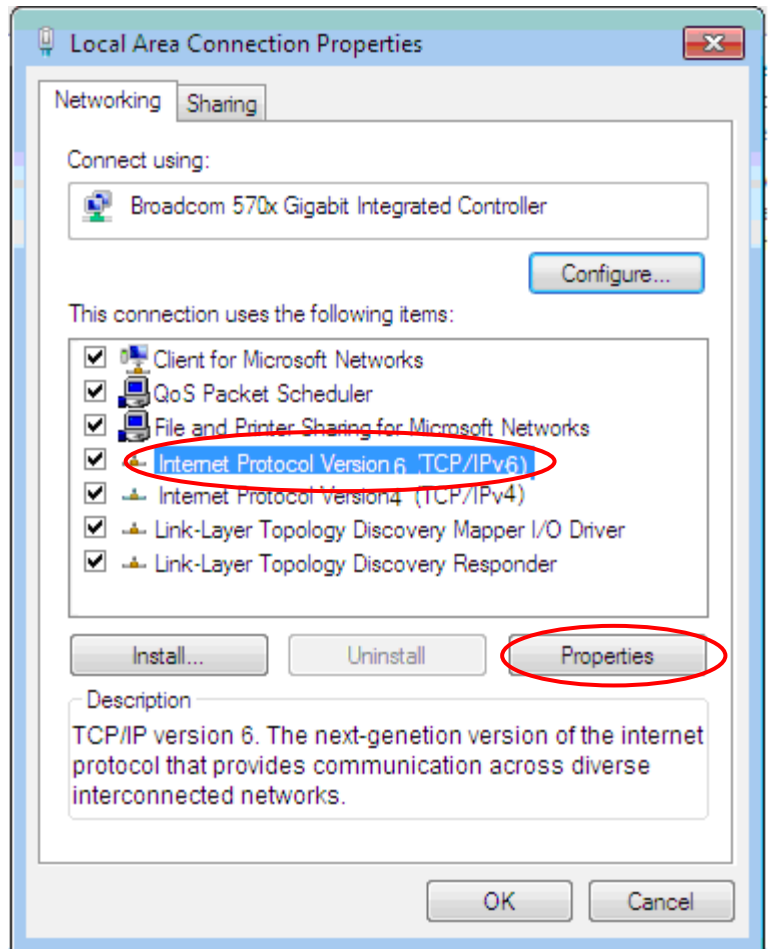
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

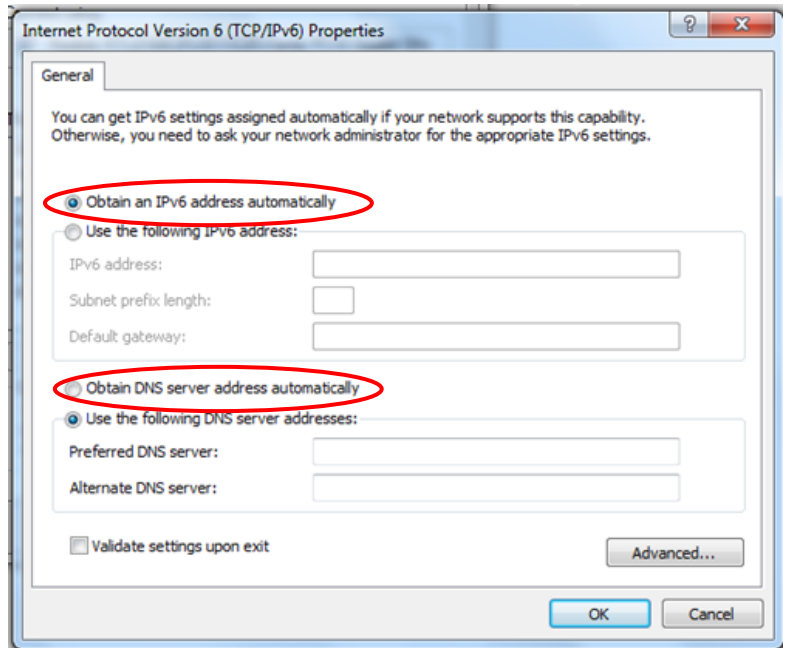


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



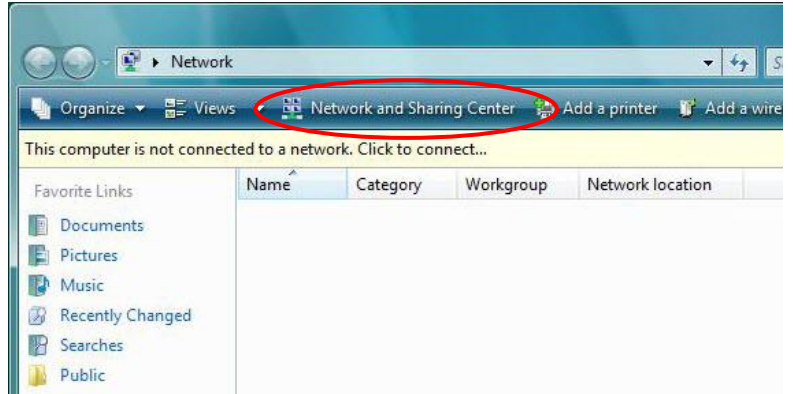
6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



Configuring PC in Windows Vista (IPv6)

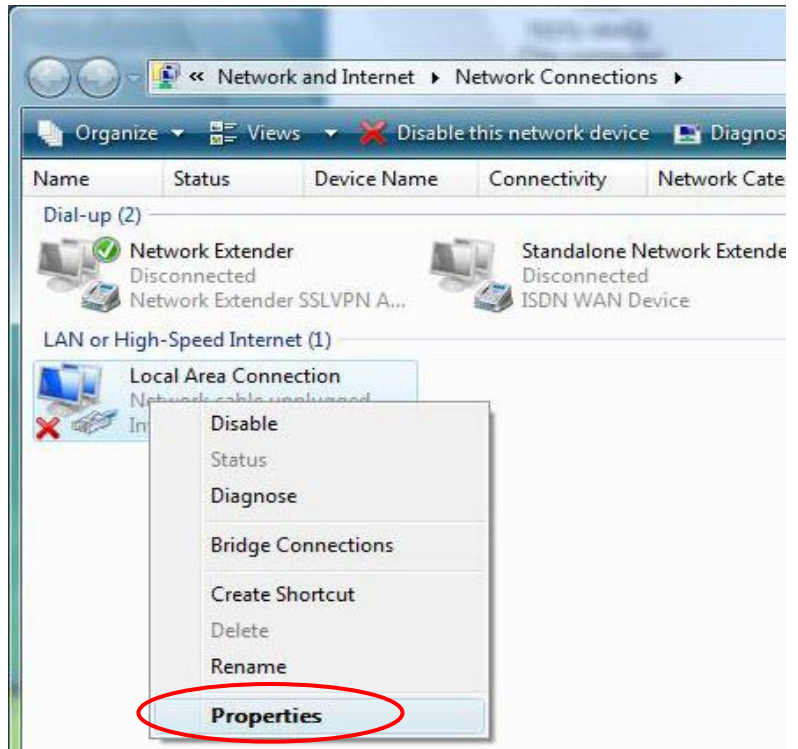
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



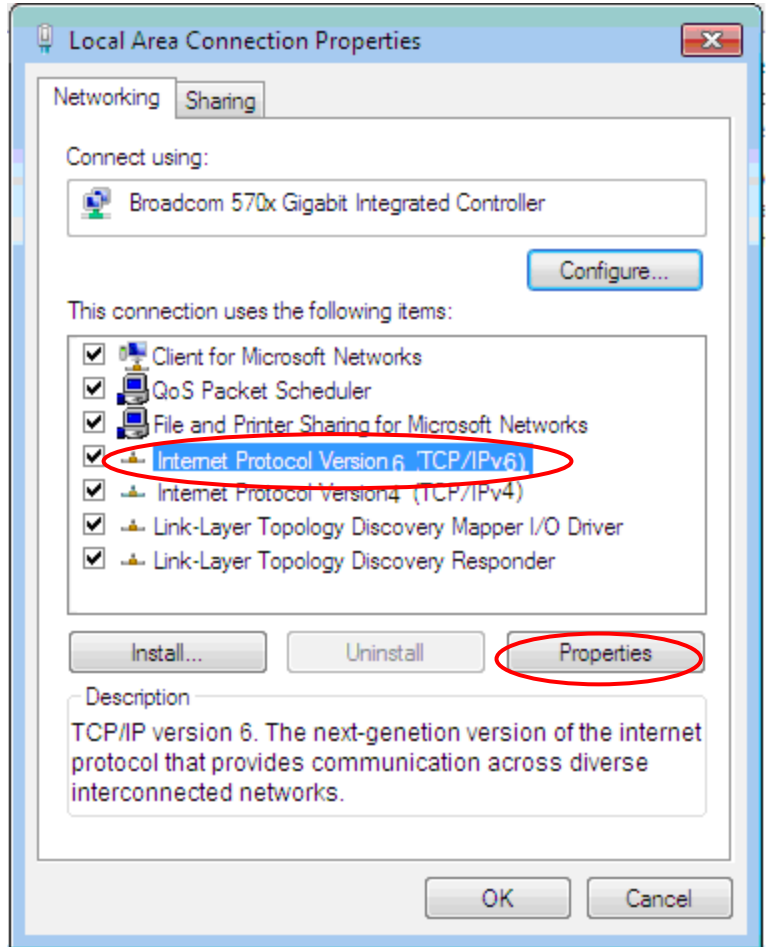
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.



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

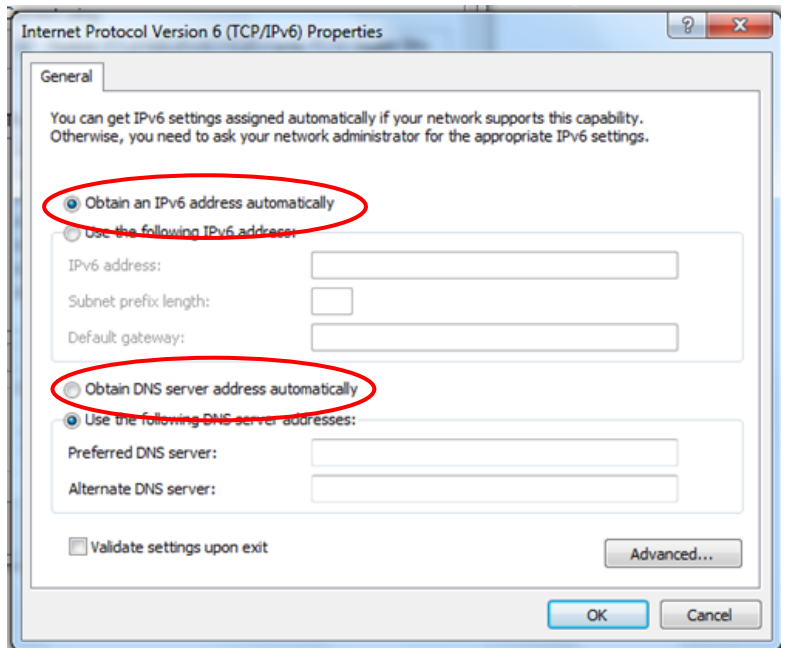


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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.

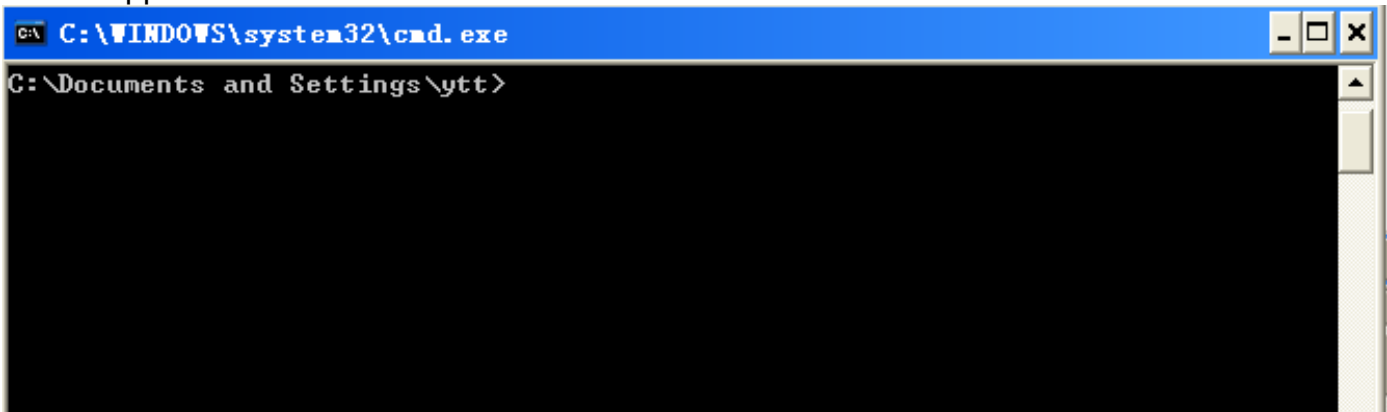


Configuring PC in Windows XP (IPv6)

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

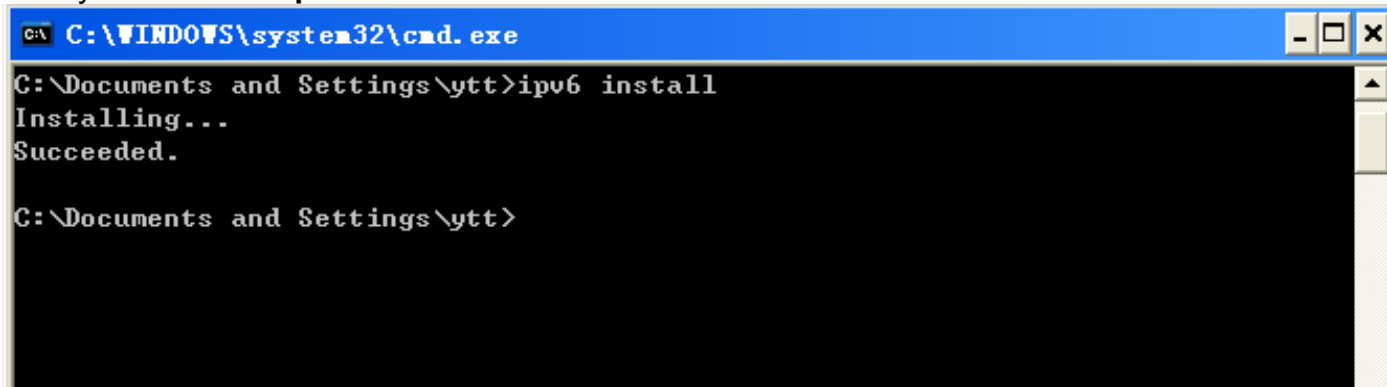
Please follow the steps to install IPv6:

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. Test it to see if it can work.

Default Settings

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

Web Interface: (Username and Password)

- ✓ Username: admin
- ✓ Password: admin

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



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

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

Device LAN IP Settings

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

DHCP Server:

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

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

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	Language
Sub-Items	Device Info		Interface Setup <ul style="list-style-type: none"> - Internet - LAN - Wireless - Wireless MAC Filter 	
	System Status		Advanced Setup <ul style="list-style-type: none"> - Firewall - Routing - NAT - Static DNS - QoS - Interface Grouping - Time Schedule 	
	System Log		VoIP <ul style="list-style-type: none"> - Basic - Media - Advanced - Speed Dial - Dial Plan - Call Features - NAT Traversal 	
	3G/4G-LTE Status		Access Management <ul style="list-style-type: none"> - Device Management - SNMP - Remote Syslog - Universal Plug & Play (UPnP) - Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - SAMBA & FTP Server 	
	Statistics		Maintenance <ul style="list-style-type: none"> - User Management - Time Zone - Firmware & Configuration - System Restart - Auto Reboot - Diagnostic Tool 	
	DHCP Table			
	Disk Status			
	VoIP Status		<ul style="list-style-type: none"> - VoIP Status - VoIP Call Log 	

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 Log**, **3G/4G-LTE Status**, **Statistics**, **DHCP Table**, **Disk Status**, and **VoIP Status**.

The screenshot displays the 'Status' page for a BEC 4G/LTE VoIP Gigabit Wireless Router. The page is divided into a left sidebar with navigation options and a main content area showing configuration details for the LAN and WAN interfaces.

Navigation Sidebar:

- ▼ Status
 - Device Info
 - System Log
 - 3G/4G-LTE Status
 - Statistics
 - DHCP Table
 - Disk Status
 - ▶ VoIP Status
- Quick Start
- ▶ Configuration
- ▶ Language

Main Content Area:

Status

▼ 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	EWAN	
Service	0	
Connection Type	Dynamic IP	
IPv4		
Status	Connected	
IP Address	172.16.1.216	<input type="button" value="Renew IP Address"/> <input type="button" value="Release IP Address"/>
Subnet Mask	255.255.255.0	
Default Gateway	172.16.1.254	
DNS Server	172.16.1.254	

Restart

Copyright © BEC Technologies, Ltd. All rights reserved.

Device Info

It contains basic information of the device.

Status

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
-----------------	---

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
<input type="button" value="Refresh"/>	

System Log

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

Status

System Log

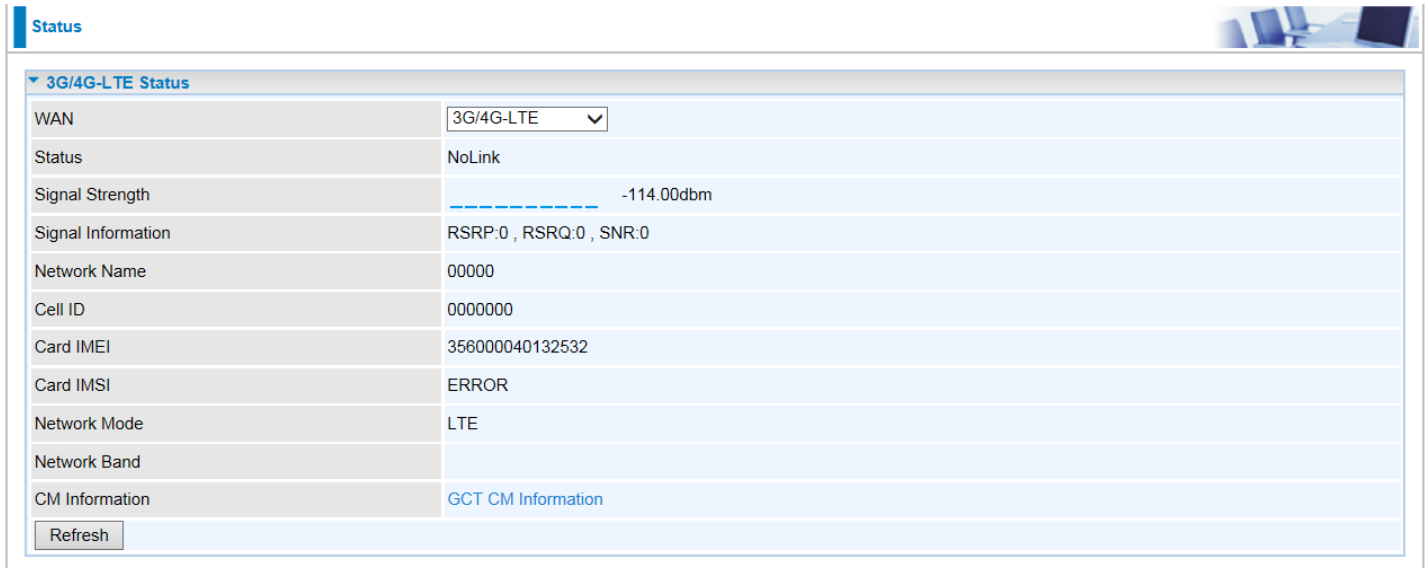
```

Jan  1 00:00:30 syslogd started: BusyBox v1.00 (2013.08.16-04:45+0000)
Jan  1 00:00:32 dnsmasq[1241]: started, version 2.52 cachesize 150
Jan  1 00:00:32 dnsmasq[1241]: compile time options: IPv6 GNU-getopt no-RTC no-
DBus no-I18N no-DHCP no-TFTP
Jan  1 00:00:32 dnsmasq[1241]: reading /etc/resolv.conf
Jan  1 00:00:32 dnsmasq[1241]: ignoring nameserver ::1 - local interface
Jan  1 00:00:32 dnsmasq[1241]: ignoring nameserver 127.0.0.1 - local interface
Jan  1 00:00:32 dnsmasq[1241]: read /etc/hosts - 0 addresses
Dec 20 18:00:00 PPOELOGIN: bind service port
Dec 20 18:00:00 PPOELOGIN: begin service loop
Dec 20 18:00:30 dnsmasq[1775]: started, version 2.52 cachesize 150
Dec 20 18:00:30 dnsmasq[1775]: compile time options: IPv6 GNU-getopt no-RTC no-
DBus no-I18N no-DHCP no-TFTP
Dec 20 18:00:30 dnsmasq[1775]: reading /etc/resolv.conf
Dec 20 18:00:30 dnsmasq[1775]: ignoring nameserver ::1 - local interface
Dec 20 18:00:30 dnsmasq[1775]: ignoring nameserver 127.0.0.1 - local interface
Dec 20 18:00:30 dnsmasq[1775]: read /etc/hosts - 0 addresses
                    
```

Refresh: Press this button to refresh the statistics.

3G/4G-LTE Status

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



The screenshot shows a web interface for '3G/4G-LTE Status'. It includes a 'WAN' dropdown menu set to '3G/4G-LTE', a 'Status' field showing 'NoLink', and a 'Signal Strength' field with a bar graph and '-114.00dbm'. Other fields include 'Signal Information' (RSRP:0, RSRQ:0, SNR:0), 'Network Name' (00000), 'Cell ID' (0000000), 'Card IMEI' (356000040132532), 'Card IMSI' (ERROR), 'Network Mode' (LTE), and 'Network Band'. A 'CM Information' link points to 'GCT CM Information' and a 'Refresh' button is at the bottom.

3G/4G-LTE Status	
WAN	3G/4G-LTE
Status	NoLink
Signal Strength	-114.00dbm
Signal Information	RSRP:0, RSRQ:0, SNR:0
Network Name	00000
Cell ID	0000000
Card IMEI	356000040132532
Card IMSI	ERROR
Network Mode	LTE
Network Band	
CM Information	GCT CM Information
<input type="button" value="Refresh"/>	

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

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

The screenshot shows the 'Status' page of a router. At the top, there is a 'Status' tab and a small image of a desk with a laptop. Below this is a 'Statistics' section with a dropdown arrow. Underneath, there is a 'Traffic Statistics' section with a radio button selection for the interface: EWAN (selected), 3G/4G-LTE, Ethernet, and Wireless. This is followed by 'Transmit Statistics' and 'Receive Statistics' sections, each containing a table of metrics and their values. A 'Refresh' button is located at the bottom of the statistics section.

Traffic Statistics	
Interface	<input checked="" type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input type="radio"/> Ethernet <input type="radio"/> Wireless
Transmit Statistics	
Transmit Frames	73852
Transmit Multicast Frames	817
Transmit Total Bytes	15977177
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	153578
Receive Multicast Frame	79037
Receive Total Bytes	14342348
Receive CRC Errors	0
Receive Under-size Frames	0

Refresh

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

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 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.

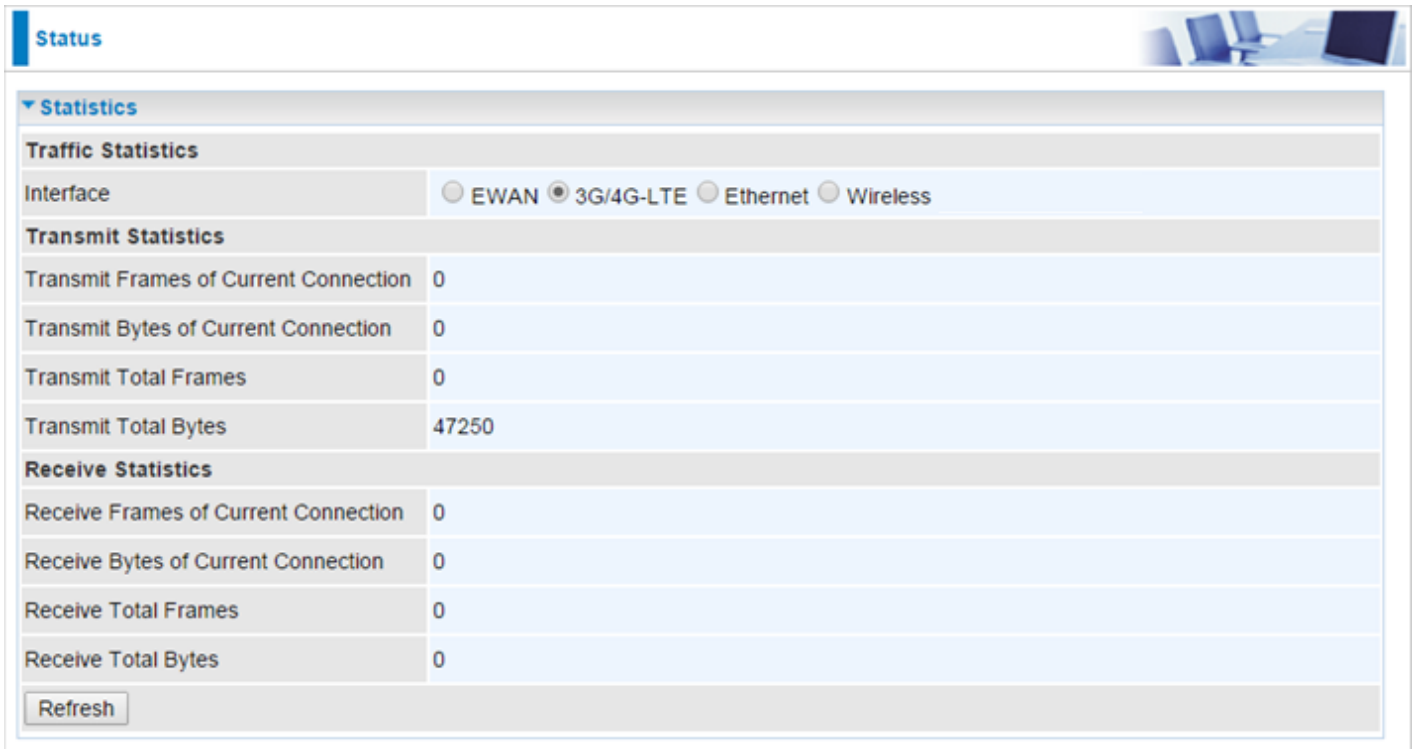
Receive CRC Errors: This field displays the number of error packets on this port.

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

Refresh: Press this button to refresh the statistics.

❖ 3G/4G-LTE

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



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

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 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.

❖ Ethernet

Status

▼ **Statistics**

Traffic Statistics

Interface EWAN 3G/4G-LTE Ethernet Wireless

Transmit Statistics

Transmit Frames	157600
Transmit Multicast Frames	157600
Transmit Total Bytes	55934140
Transmit Collision	0
Transmit Error Frames	0

Receive Statistics

Receive Frames	153519
Receive Multicast Frame	79023
Receive Total Bytes	14334604
Receive CRC Errors	0
Receive Under-size Frames	0

Refresh

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

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

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

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

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

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

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

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

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

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

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

Refresh: Press this button to refresh the statistics.

❖ Wireless

The screenshot displays the 'Status' page for the router's wireless interface. It features a 'Statistics' section with a dropdown menu. The 'Interface' is currently set to 'Wireless'. The statistics are divided into 'Transmit Statistics' and 'Receive Statistics'. The 'Transmit Statistics' section shows 76131 Transmit Frames, 1954 Transmit Error Frames, and 1954 Transmit Drop Frames. The 'Receive Statistics' section shows 1534449 Receive Frames, 18319981 Receive Error Frames, and 18319981 Receive Drop Frames. A 'Refresh' button is located at the bottom of the statistics section.

Traffic Statistics	
Interface	<input type="radio"/> EWAN <input type="radio"/> 3G/4G-LTE <input type="radio"/> Ethernet <input checked="" type="radio"/> Wireless
Transmit Statistics	
Transmit Frames	76131
Transmit Error Frames	1954
Transmit Drop Frames	1954
Receive Statistics	
Receive Frames	1534449
Receive Error Frames	18319981
Receive Drop Frames	18319981

Refresh

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

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 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.

DHCP Table

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

Status				
DHCP Table List				
#	Host Name	IP Address	MAC Address	Expire Time
1	billion-17bc6f1	192.168.1.104	18:A9:05:38:04:03	0days 23:37:51

Index #: The index identifying the connected devices.

Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

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

Disk Status

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 tunnel indicator.

Action: Connect or Drop the connection.

Connection Name: User-defined IPsec VPN connection name.

Active: Show if the tunnel is active for connection.

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

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

Remote Gateway: The IP of the remote IPsec gateway.

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

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

PPTP Status

❖ 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 connection indicator.

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

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

Connection Type: Remote Access or LAN to LAN.

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

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

Refresh: Click this button to refresh the connection status.

❖ 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 connection indicator.

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

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

Connection Type: Remote Access or LAN to LAN.

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

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

Refresh: Click this button to refresh the connection status.

L2TP Status

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 tunnel indicator.

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

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

Connection Mode: The L2TP mode is dial-in or dial-out.

Connection Type: Remote Access or LAN to LAN.

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

Refresh: Click this button to refresh the connection status.

GRE Status

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 indication.

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

Active: Show if the tunnel is active for connection.

Connection State: Show the connecting status.

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

Remote Network: Display the remote network.

VoIP Status

❖ VoIP Status

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

Phone Number	Host	Status	Registered Time
7154000000	metaproxy.vohibardun.net:5060	Registered	Fri, 06 Sep 2013 08:10:28
7154000104	metaproxy.vohibardun.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.

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

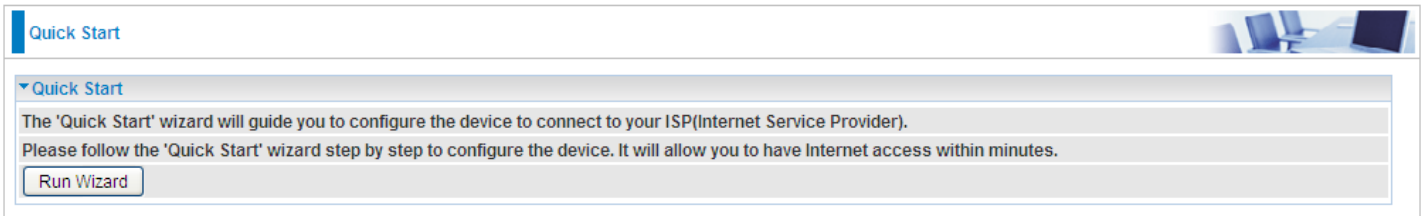
End Time: The end time of the call

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.

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.



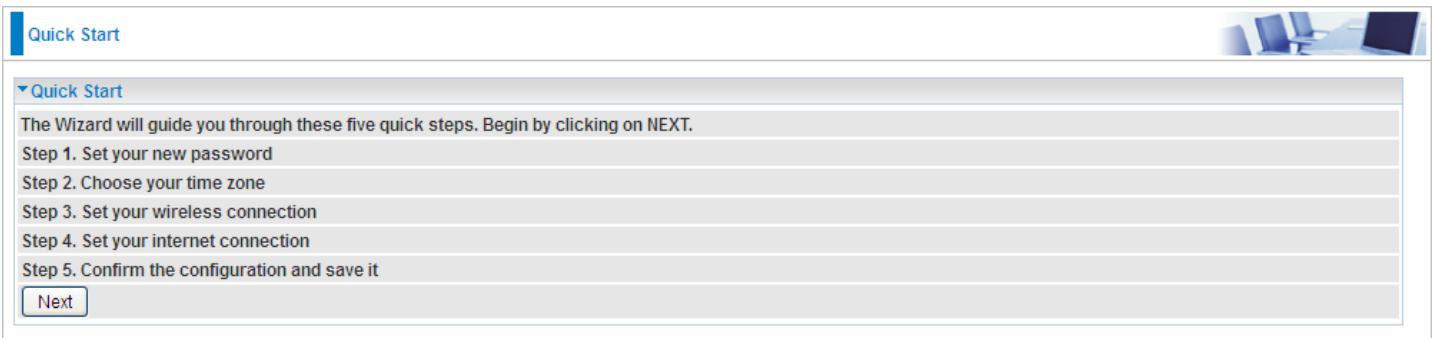
Quick Start

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

Quick Start

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

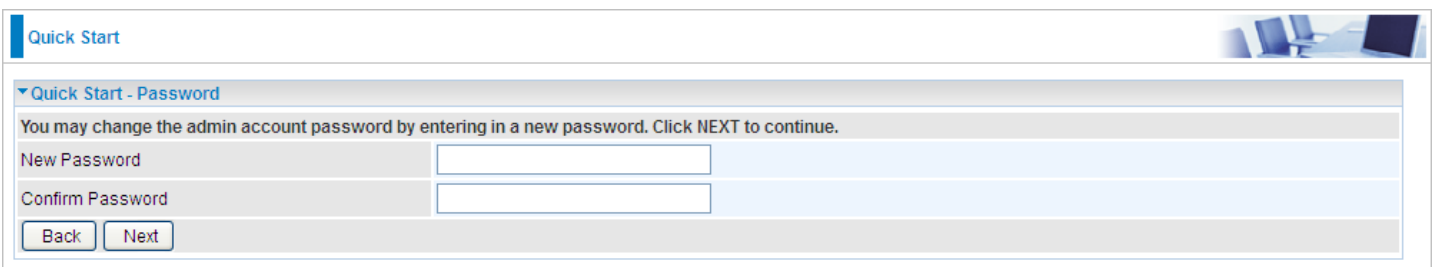
- Step 1. Set your new password
- Step 2. Choose your time zone
- Step 3. Set your wireless connection
- Step 4. Set your internet connection
- Step 5. Confirm the configuration and save it

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



Quick Start

Quick Start - Password

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

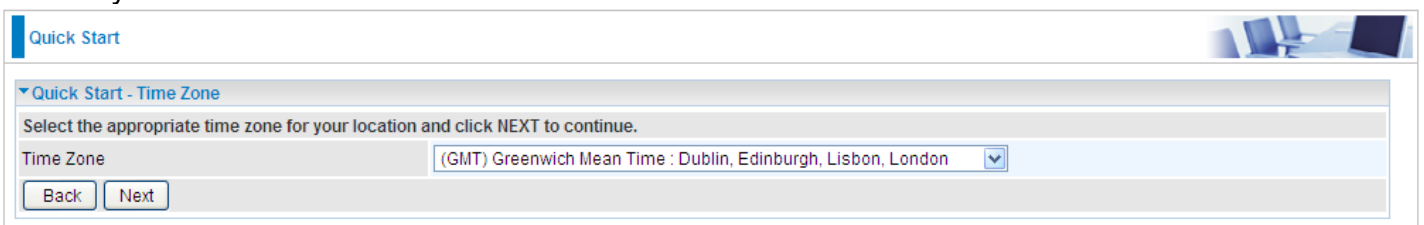
New Password

Confirm Password

Back Next

Step 2 – Time Zone

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



Quick Start

Quick Start - Time Zone

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

Time Zone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

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.

Step 4 – ISP Connection Type

Set up your Internet connection.

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

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

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

Quick Start

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.

Quick Start

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.

Back Next

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

Quick Start

Quick Start - PPPoE

Provide the PPPoE information. Click NEXT to continue.

Username	
Password	

Back Next

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 - 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.

Back Next

Quick Start

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, 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 and Wireless MAC Filter.**

The screenshot shows the configuration interface for a BEC 4G/LTE VoIP Gigabit Wireless Router. The page is titled "4G/LTE VoIP Gigabit Wireless Router" and is part of the "Configuration" section. A left-hand navigation menu includes options for Status, Quick Start, Configuration (selected), Interface Setup, Advanced Setup, VoIP, Access Management, Maintenance, and Language. The main content area is titled "Internet" and contains the following settings:

- WAN Interface: 3G/4G-LTE
- Status: Activated Deactivated
- Network Mode: Automatic
- TEL No.: *99***1#
- APN: internet
- Username: [Empty field]
- Password: [Empty field]
- PIN: [Empty field]
- Connection: Always On (Recommended)
- Keep Alive: Yes No
- Default Route: Yes No
- NAT: Enable

A "Save" button is located at the bottom of the configuration area. At the bottom right of the page, there are "Restart" and "Logout" buttons. The footer contains the text "Copyright © BEC Technologies Inc. All rights reserved."

Internet

❖ EWAN

Configuration

Internet

WAN Interface: EWAN

Multi Service

Service Index: 0 Services Summary

Status: Activated Deactivated

IPv4/IPv6

IP Version: IPv4 IPv4/IPv6 IPv6

ISP Connection Type

ISP: Dynamic IP Address Static IP Address PPPoE Bridge Mode

802.1q Options

802.1q: Activated Deactivated

VLAN ID: 0 (range: 0~4095)

PPPoE

Username:

Password:

Bridge Interface for PPPoE: Activated Deactivated

Connection Setting

Connection: Always On (Recommended) Connect Manually

TCP MSS Option: TCP MSS 0 bytes(0 means use default)

IP Options

IP Common Options

Default Route: Yes No

IPv4 Options

Get IP Address: Static Dynamic

Static IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

NAT: Enable

Dynamic Route: RIP1 Direction: None

TCP MTU Option: TCP MTU 0 bytes(0 means use default:1492)

IGMP Proxy: Enable Disable

IPv6 Options

IPv6 Address: /

Obtain IPv6 DNS: Enable Disable

Primary DNS:


Secondary DNS:

MLD Proxy: Enable Disable

Multi Service

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

Service Summary: The overall service information.

Status 

▼ Service Information Summary

WAN 0	Active	ISP	IP Address
0	Yes	PPPoE	Dynamic
1	Yes	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.

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

❖ 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 ▾
APN	vzwinternet
Connection	<input checked="" type="radio"/> Always On (Recommended)
Keep Alive	<input type="radio"/> Yes <input checked="" type="radio"/> No
Keep Alive IP	
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
NAT	Enable ▾
MTU	0 (0 means use default:1500)
<input type="button" value="Save"/>	

Status: Choose Activated to enable the 3G/EVDO service.

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 ▾
<p>***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.</p>	
<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.

▼ LTE Mode

Parameters

LTE Antenna Diversity

***Please save config and restart to activate the setting. Please make sure device had get WAN IP, then config this feature.

PLMN (Public Land Mobile Network) Selection:

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: BEC 6300VNL can support up to two (2) APNs. Select Single or Dual.

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

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.

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

▼ SMS Control

Parameters

SMS Control Enable

Control Password

***Please save config and restart to activate the setting.

SMS Control: Check to enable this feature.

Control Password: Pre-config 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 +513 123 4567. 6300VNL will reboot the system upon receiving of this text message.
2. Send a text message, ***60**, to +513 123 4567. 6300VNL will send the current 3G/ 4G status information back including IMEI number, System up time, Network mode, Signal strength, WAN IP, and Connection time.

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

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.

Configuration

LAN

IPv4 Parameters

IP Address:

IP Subnet Mask:

Alias IP Address: (0.0.0.0 means to close the alias ip)

Alias IP Subnet Mask:

IGMP Snooping: Activated Deactivated

Dynamic Route: Direction:

DHCPv4 Server

DHCPv4 Server: Disabled Enabled Relay

Start IP:

IP Pool Count:

Lease Time: seconds (0 sets to default value of 259200)

Physical Ports: LAN1 LAN2 LAN3 WLAN1

DNS Relay: Automatically Manually

Primary DNS:

Secondary DNS:

Fixed Host

IP Address:

MAC Address:

IPv6 Parameters

Interface Address/Prefix Length: /

MLD Snooping: Activated Deactivated

DHCPv6 Server

DHCPv6 Server: Disable Enable

DHCPv6 Server Type: Stateless Stateful

Start Interface ID:

End Interface ID:

Lease Time: seconds (0 sets to default value of 4800)

Router Advertisements: Disable Enable

Fixed Host List

Index	IP	MAC	Drop

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.

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"/>
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

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

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 do not need to configure anything on the client.

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

DHCPv6 Server: Check whether to enable DHCPv6 server.

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

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

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

End interface ID: enter the end interface ID.

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

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

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.

Configuration

Wireless

Access Point Settings

Access Point Activated Deactivated

AP MAC Address 00:04:ED:15:07:00

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 Yes No

11n Settings

Channel Bandwidth 40 MHz

Guard Interval Auto

MCS Auto

SSID Settings

Available SSID 1

SSID Index SSID1

SSID wlan-ap_715

Broadcast SSID Yes No

SSID Activated Always

WPS Settings

Use WPS Yes No

WPS State Configured

WPS Mode PIN code PBC

Security Settings

Security Type Mixed WPA2/WPA-PSK

WPA Algorithms TKIP+AES

Pre-Shared Key E5C7EB09 (8~63 characters or 64 Hex string)

Key Renewal Interval 600 seconds (10 ~ 4194303)

WDS Settings

AP MAC Address 00:04:ED:15:07:00

WDS Mode Activated Deactivated

WDS Peer MAC #1 00:00:00:00:00:00

WDS Peer MAC #2 00:00:00:00:00:00

WDS Peer MAC #3 00:00:00:00:00:00

WDS Peer MAC #4 00:00:00:00:00:00

Access Point Settings

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

AP MAC Address: The MAC address of wireless AP.

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

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

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

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

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

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

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

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

11n Settings

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

Extension Channel: This is for the 40MHz clients to use and is predefined to “**Above the control channel**”, not configurable.

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

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 (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 “YES” radio button.

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

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

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

Security Settings

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

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

There are 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.

► **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.

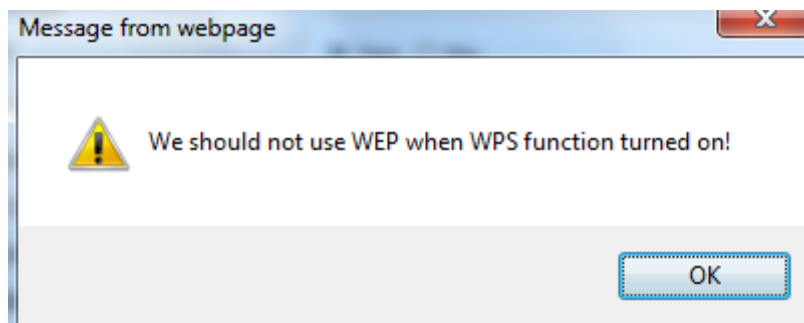
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP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



► **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 ASKII characters or 64 hexadecimal characters

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

WDS Settings

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

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

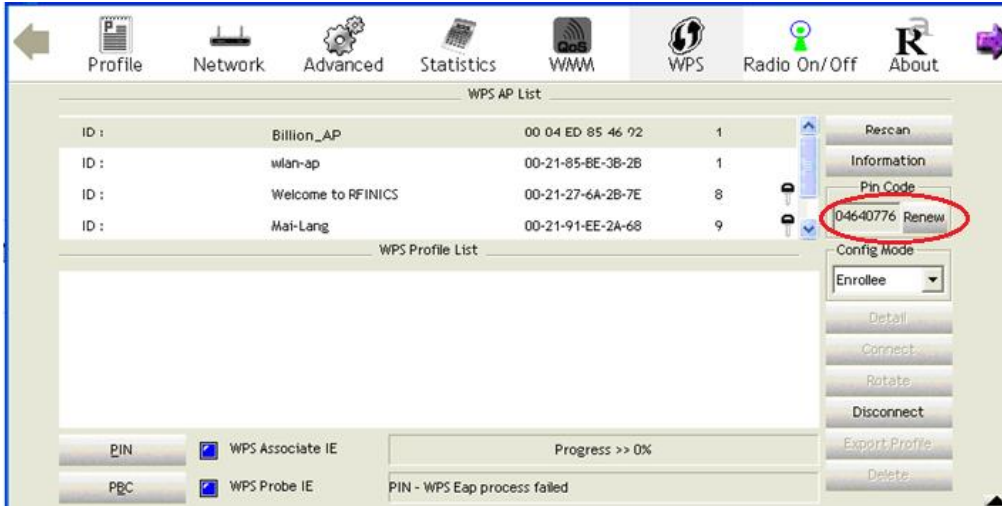
MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.

WDS Settings	
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"/>

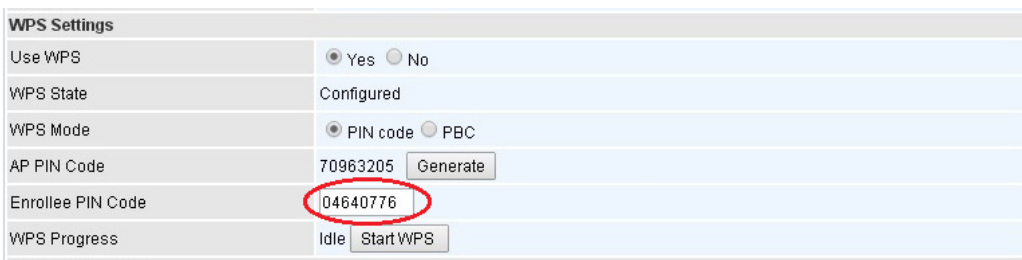
Example: WPS using PIN Method (Personal Information Number)

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)

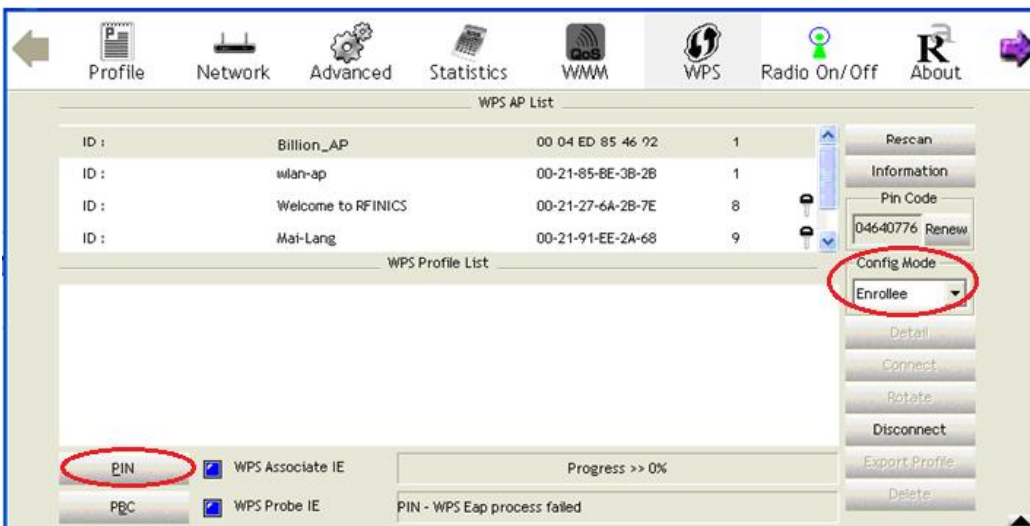


2. Enter the Enrollee (Client) PIN code and then press **Start WPS**.



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 wireless 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 several sections:

- WPS AP List:** A table showing discovered APs. The first entry, 'Billion_AP' with MAC address '00-04-ED-85-46-92', is circled in red.
- WPS Profile List:** Shows the selected profile 'Billion_AP'.
- WPS Configuration:** Includes checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both checked. A progress bar shows 'Progress >> 100%' and a message 'WPS status is connected successfully'.
- Link Quality:** A bar chart showing 'Link Quality >> 100%', 'Signal Strength 1 >> 41%', 'Signal Strength 2 >> 44%', and 'Noise Strength >> 26%'.
- Transmit/Receive:** Graphs showing 'Link Speed >> 108.0 Mbps' and 'Throughput >> 0.000 Kbps' for transmit, and 'Link Speed >> 1.0 Mbps' and 'Throughput >> 109.204 Kbps' for receive.
- Status:** A detailed status section for 'Billion_AP' showing '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', and 'Default Gateway >> 192.168.1.254'. This section is also circled in red.

Below the main interface is the configuration form:

- SSID Settings:** 'Available SSID' is set to 1. 'SSID Index' is 'SSID1'. The 'SSID' field contains 'Billion-AP', which is circled in red.
- WPS Settings:** 'Use WPS' is 'Yes'. 'WPS State' is 'Configured'. 'WPS Mode' is 'PIN code'. 'AP PIN Code' is '70963205'. 'Enrollee PIN Code' is '04640776'.
- Security Settings:** 'Security Type' is 'WPA2-PSK', circled in red. 'WPA Algorithms' is 'AES'. 'Pre-Shared Key' is 'billion00486c'. 'Key Renewal Interval' is '600' seconds.

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 are navigation icons for Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About, and Help. The main area is divided into several sections:

- WPS AP List:** A table with columns for ID, Name, MAC Address, and Signal Strength. The first entry is "Billion_AP" with MAC address "00-04-ED-85-46-92" and signal strength "1". It is circled in red.
- WPS Profile List:** Shows "Billion_AP" selected.
- Configuration:** Includes a "PIN Code" field with "03454435" entered (circled in red), a "Config Mode" dropdown set to "Registrar" (circled in red), and a "PIN" button (circled in red).
- Status:** Shows "Progress >> 100%" and "WPS status is connected successfully".
- Network Details:**
 - 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:**
 - 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).

WPS AP List

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	

WPS Profile List

- Billion_AP

WPS status is connected successfully

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

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

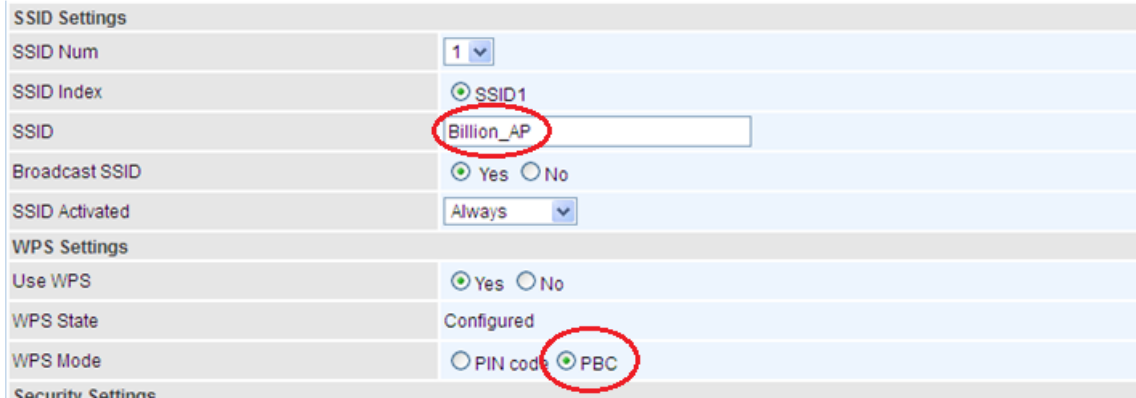
Security Settings

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

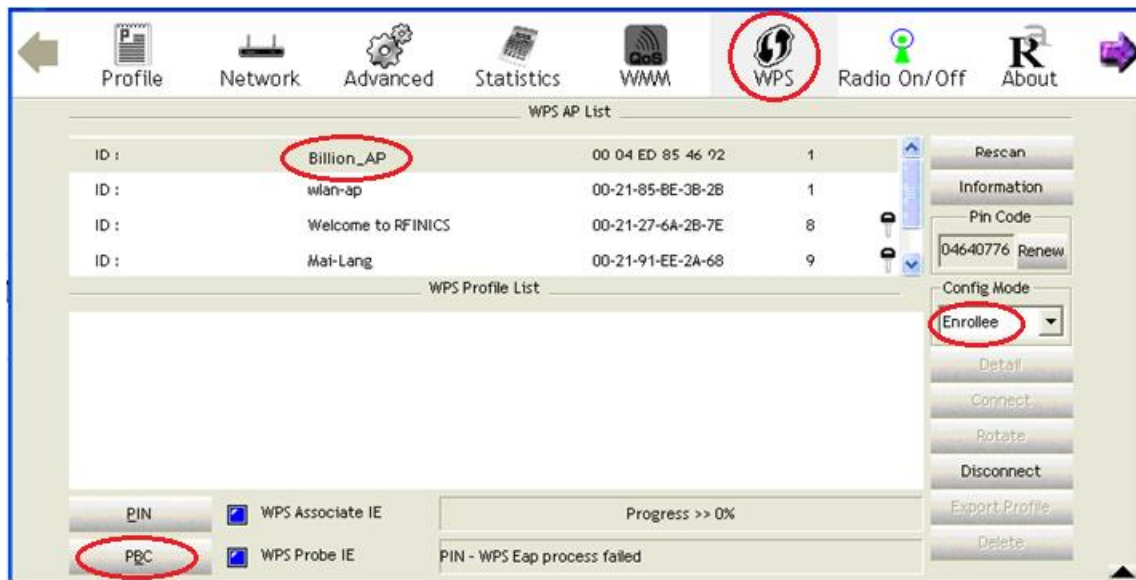
Interface Setup – Wireless (Example on WPS using PBC)

Example: WPS using PBC Method (Push Button Configuration)

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



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.



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 displays the WPS configuration interface. At the top, there are navigation tabs: Network, Advanced, Statistics, WMM, WPS, Radio On/Off, About, and Help. The main content area is divided into two sections: 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 Billion_AP selected. Below the profile list, there are buttons for PIN, PBC, WPS Associate IE, and WPS Probe IE. The PBC button is circled in red. 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. The bottom section shows status details: 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, HT, BW >> 40, GI >> long, MCS >> 5, SNR0 >> 30, SNR1 >> 20102206, Link Quality >> 100%, Signal Strength 1 >> 41%, Signal Strength 2 >> 44%, Noise Strength >> 26%, Transmit Link Speed >> 108.0 Mbps, Throughput >> 0.000 Kbps, and Receive Link Speed >> 1.0 Mbps, Throughput >> 109.204 Kbps.

The screenshot shows the SSID Settings and Security Settings sections. The SSID Settings section includes: SSID Num (1), SSID Index (SSID1), SSID (Billion_AP), Broadcast SSID (Yes), SSID Activated (Always). The WPS Settings section includes: Use WPS (Yes), WPS State (Configured), WPS Mode (PIN code, PBC). The Security Settings section includes: Security Type (WPA2-PSK), WPA Algorithms (AES), Pre-Shared Key (12345678), and Key Renewal Interval (3600 seconds). The SSID field and Security Type dropdown are circled in red.

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.

The screenshot shows the 'Wireless MAC Address Filter' configuration page. The 'SSID Index' is set to 'SSID1'. The 'Active' status is 'Deactivated'. The 'Action' is set to 'Allow', with a dropdown menu showing 'the follow Wireless LAN station(s) association.'. There is an empty text box for 'MAC Address'. A 'Save' button is located below the form. Below the form is a table titled 'Wireless MAC Address Filter Listing' with columns for 'Index', 'MAC Address', 'Edit', and '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.

Advanced Setup

Advanced Step provides advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **QoS**, **Internet Grouping**, and **Time Schedule** 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.

Configuration

▼ Firewall

Firewall Enabled Disabled

SPI Enabled Disabled

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

SAVE CANCEL

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

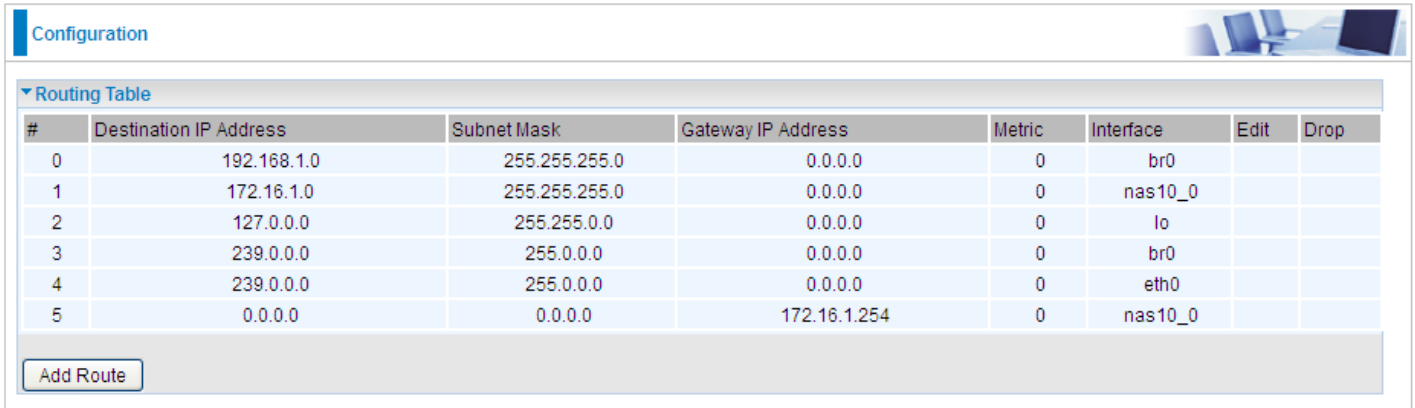
- ▶ **Enabled:** It activates your firewall function.
- ▶ **Disabled:** It disables the firewall function.

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

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

Routing

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



#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	172.16.1.0	255.255.255.0	0.0.0.0	0	nas10_0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	eth0		
5	0.0.0.0	0.0.0.0	172.16.1.254	0	nas10_0		

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

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

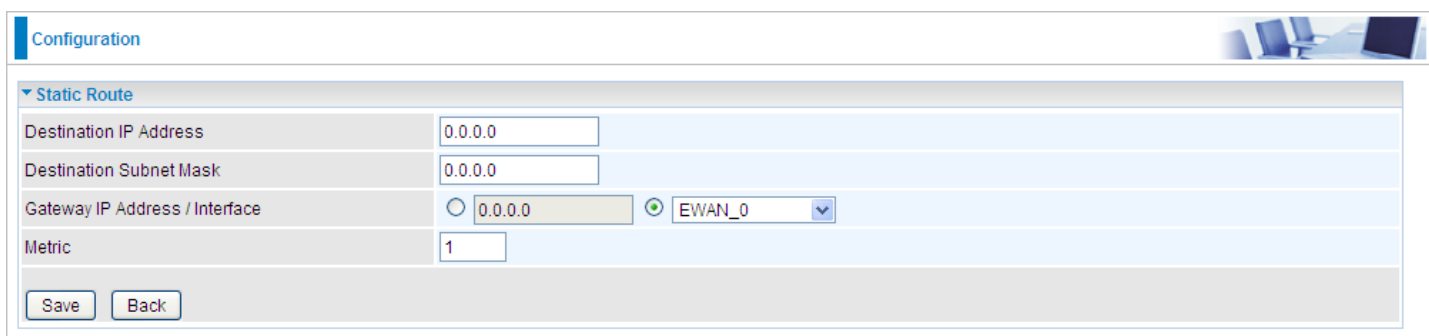
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

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

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

Add Route



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

Destination Subnet Mask: The subnet mask of destination network.

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

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

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	EWAN
Service Index	0
DMZ	Edit
Virtual Server	Edit

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

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

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

Interface: Select 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.

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

The screenshot shows a web-based configuration interface for DMZ. The page is titled 'Configuration'. Under the 'DMZ' section, there are three rows of configuration options:

- DMZ for:** Multiple IPs Account/ EWAN Service ID 0
- DMZ:** Radio buttons for 'Enabled' and 'Disabled'.
- DMZ Host IP Address:** An empty text input field.

At the bottom of the configuration area, there are two buttons: 'Save' and 'Back'.

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

Note: Here you can see the Multiple IPs Account/EWAN Service ID 0. It is the interface set in the previous NAT page.

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.

Select the **Save** button to apply your changes.

Virtual Server

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

Virtual Server is also known as Port Forwarding that allows 6300VNL to direct all incoming traffic to the servers on the LAN.

Configure a virtual rule in 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.

The screenshot shows the configuration page for Virtual Servers. The 'Virtual Server' section includes the following fields:

- Virtual Server for: Multiple IPs Account/ EWAN
- Protocol: TCP
- Start Port Number: []
- End Port Number: []
- Local IP Address: []
- Start Port Number (Local): []
- End Port Number(Local): []

Buttons: Save, Back

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	N/A	N/A	N/A	N/A	N/A	N/A		
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		

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

Protocol: Choose the application protocol.

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

(Example: Start / End: 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 your server IP address in this field.

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

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

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



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



Attention

If you have disabled the NAT option in the 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. 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. BEC 6300VNL will forward port 21 request from WAN to the specific LAN PC (ex:192.168.1.102) in the network.

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

The screenshot shows the 'Virtual Server' configuration page. The form is filled with the following values:

- Virtual Server for: Multiple IPs Account/ EWAN
- Protocol: TCP
- Start Port Number: 21
- End Port Number: 21
- Local IP Address: 192.168.1.102
- Start Port Number (Local): 21
- End Port Number(Local): 21

Buttons for 'Save' and 'Back' are visible. Below the form is a 'Virtual Server Listing' table:

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.102	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		

Static DNS

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

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

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.

The screenshot displays a web-based configuration interface. At the top left, there is a 'Configuration' tab. Below it, a section titled 'Static DNS' is expanded. This section contains two input fields: 'IP Address' and 'Domain Name'. A 'Save' button is located below these fields. Underneath, there is a 'Static DNS Listing' table with the following columns: Index, IP Address, Domain Name, Edit, and Delete.

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

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

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

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.

The screenshot shows a web-based configuration interface for Quality of Service (QoS). At the top, there is a 'Configuration' tab and a 'Quality of Service' section. The 'QoS' section has radio buttons for 'Activated' (selected) and 'Deactivated'. Below this are 'Save' and 'Rules Summary' buttons. The 'Rule' section contains the following fields:

- Rule Index: A dropdown menu with '0' selected.
- Active: Radio buttons for 'Yes' and 'No' (selected).
- Destination IPv4/IPv6 Address: A text input field.
- Destination Subnet Mask / IPv6 Prefix: A text input field.
- Destination Port Range: Two text input fields separated by a tilde (~).
- Source IPv4/IPv6 Address: A text input field.
- Source Subnet Mask / IPv6 Prefix: A text input field.
- Source Port Range: Two text input fields separated by a tilde (~).
- Protocol ID: A dropdown menu.
- Priority: A dropdown menu.

At the bottom of the rule configuration area, there are 'Save' and 'Delete' buttons.

Click **SETTING** to add QoS rules (up to **16** QoS rules).

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

Active: Select whether 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.

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.

Configuration

Interface Grouping

Interface Grouping Activated Deactivated

Group Index 0

EWAN Service EWAN0

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

Ethernet LAN LAN1 LAN2 LAN3

Wireless LAN WLAN1

Group Summary

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

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

EWAN Service: The available EWAN interface. Move to [Interface Setup](#) to add other EWAN interface.

3G/4G-LTE: The available 3G/4G-LTE interfaces.

Ethernet LAN: The available Ethernet interfaces.

Wireless LAN: The available wireless interfaces.

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

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

Status

Service Information Summary

WAN 0	Active	ISP	IP Address
0	Yes	Dynamic	Dynamic
1	Yes	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

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

Configuration

Interface Grouping

Interface Grouping Activated Deactivated

Group Index: 0

EWAN Service: EWAN0 EWAN1

Ethernet LAN: LAN1 LAN2 LAN3

Wireless LAN: WLAN1

Group Summary: [Group Summary](#)

[Save](#) [Delete](#)

Configuration

Interface Grouping

Interface Grouping Activated Deactivated

Group Index: 1

EWAN Service: EWAN0 EWAN1

Ethernet LAN: LAN1 LAN2 LAN3

Wireless LAN: WLAN1

Group Summary: [Group Summary](#)

[Save](#) [Delete](#)

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

Group ID	Group port
0	wan0_0,e1,e2,w1
1	wan0_1,e3

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.

Configuration

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 index (0-15) for identifying each timeslot.

Name: User-defined identification for each time period.

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

Configuration

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 Friday

Configuration

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 type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	09:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	18:00	00:00	00:00

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="text"/>
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)
3G/LTE Usage Allowance	
Recipient's E-mail	<input type="text"/> (Must be XXX@yyy.zzz)
<input type="button" value="Apply"/>	

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.

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): E Enter a valid e-mail address to receive an alert message when the 3G over Usage Allowance occurs.

Click **Apply** button to save your 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 head office network through the public Internet.

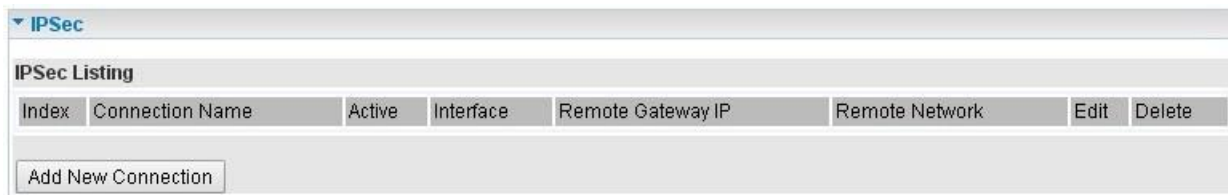
BEC 6300VNL supports **IPSec**, **PPTP**, **L2TP**, **GRE** for enterprise users.

IPSec

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

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

A total of 8 IPSec tunnels can be added.



Click **Add New Connection** to create an IPSec connection.

IPSec Connection Setting

IPSec						
Connection Name	<input type="text"/>					
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No					
Interface	Auto <input type="text"/>					
Remote Gateway IP	<input type="text"/> (0.0.0.0 means any)					
Local Access Range	Subnet <input type="text"/>	Local IP Address	<input type="text"/> 0.0.0.0	IP Subnetmask	<input type="text"/> 0.0.0.0	
Remote Access Range	Subnet <input type="text"/>	Remote IP Address	<input type="text"/> 0.0.0.0	IP Subnetmask	<input type="text"/> 0.0.0.0	
IKE Mode	Main <input type="text"/>	Pre-Shared Key	<input type="text"/>			
Local ID Type	Default Wan IP <input type="text"/>	IDContent	<input type="text"/> *			
Remote ID Type	Default Wan IP <input type="text"/>	IDContent	<input type="text"/> *			
Encryption Algorithm	DES <input type="text"/>	Authentication Algorithm	MD5 <input type="text"/>	Diffie-Hellman Group	MODP1024(DH2) <input type="text"/>	
IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		Authentication Algorithm	MD5 <input type="text"/>	Encryption Algorithm	DES <input type="text"/>
Perfect Forward Secrecy	None <input type="text"/>					
Phase 1 (IKE)SA Lifetime	480 <input type="text"/> min(s)	Phase 2 (IPSec)	60 <input type="text"/> min(s)			
Keepalive	None <input type="text"/>	PING to the IP(0.0.0.0:NEVER)	<input type="text"/> 0.0.0.0	Interval	10 <input type="text"/> seconds **	
Disconnection Time after No Traffic	180 <input type="text"/> seconds (180 at least)					
Reconnection Time	3 <input type="text"/> 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: Assign a name for this connection. Example: connection to office.

Active: **Yes** to activate the connection.

Interface: Select the set used interface for the IPSec connection, when you select 3G/4G-LTE interface, the IPSec tunnel would via this interface to connect to the remote peer.

Remote Gateway IP: The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.

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

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

Remote Access Range: Set the IP address or subnet of the remote network.

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

IPSec Phase 1(IKE)

IKE Mode	Main ▼	Pre-Shared Key	<input type="text"/>
Local ID Type	Default Wan IP ▼	IDContent	<input type="text"/> *
Remote ID Type	Default Wan IP ▼	IDContent	<input type="text"/> *
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 and Remote ID Type: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

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

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

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

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

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

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

IPSec Phase 2(IPSec)

IPSec Proposal	<input checked="" type="radio"/> ESP	<input type="radio"/> AH
	Authentication Algorithm	MD5 ▼
	Encryption Algorithm	DES ▼
Perfect Forward Security	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.

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

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

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

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

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, an IKE SA is used by IKE.

- ▶ **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
- ▶ **Phase 2 (IPsec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

IPsec 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.

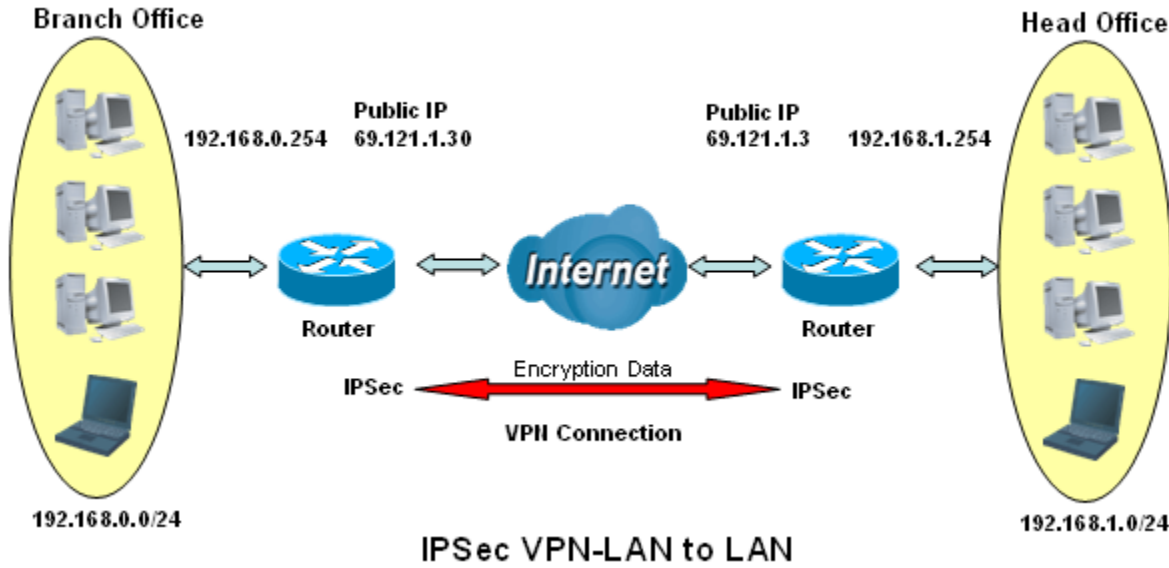
Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply the settings.

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

Two of the 6300VNL devices want to setup a secure IPsec VPN tunnel

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



Head Office Side:

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

▼ IPSec

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

Note *: FQDN with @ as first character means don't resolve domain name.
Note **: (0-3600, 0 means NEVER)

Save Back

Branch Office Side:

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

▼ IPSec

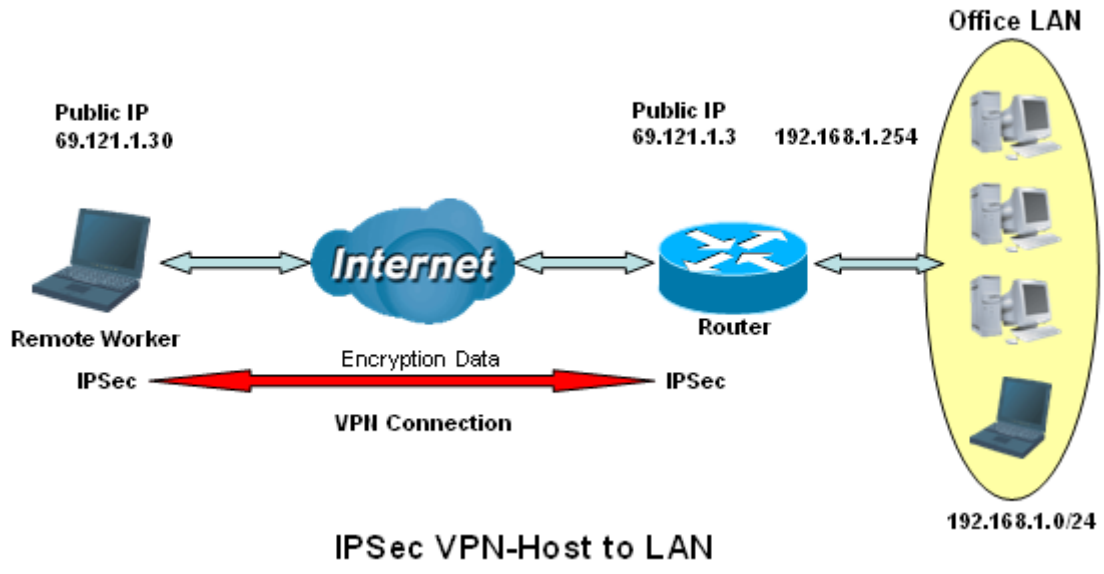
Connection Name	B-to-H				
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Interface	Auto				
Remote Gateway IP	69.121.1.3 (0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	192.168.0.0	IP Subnetmask	255.255.255.0
Remote Access Range	Subnet	Remote IP Address	192.168.1.0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

Note *: FQDN with @ as first character means don't resolve domain name.
Note **: (0-3600, 0 means NEVER)

Save Back

Examples: IPSec – Remote Employee to 6300VNL Connection

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



Head Office Side:

Configuration Settings		Description
Connection Name	H-to-H	Name for IPSec tunnel
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Head Office network
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Single IP	Host
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"/>	<small>(0.0.0.0 means any)</small>	
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 Activated Deactivated

Authentication Type: Chap/Pap

MS-DNS: 192.168.1.254

Rule Index: 1

Connection Name: []

Active: Yes No

Username: []

Password: []

Connection Type: Remote Access

Private IP Address assigned to Dial-in User: []

Remote Network IP Address: []

Remote Network Netmask: []

[Save] [Delete]

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
-------	-----------------	--------	----------	-----------------	---------------------

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

Authentication Type: The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

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: User-defined name for the PPTP connection.

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

Username: Please input the username for this account.

Password: Please input the password for this account.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Private IP Address Assigned to Dial-in User: Specify the private IP address to be assigned to dial-in clients, and the IP should be in the same subnet as local LAN, but not occupied.

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

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

Click **Save** to apply your settings.

PPTP Client

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

▼PPTP Client

Rule Index: 1 ▼

Connection Name:

Active: Yes No

Authentication Type: Chap/Pap ▼

Username:

Password:

Connection Type: Remote Access ▼

Server IP Address:

Remote Network IP Address:

Remote Network Netmask:

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: User-defined name for the PPTP connection.

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

Authentication Type: The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Username: Please input the username for this account.

Password: Please input the password for this account.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

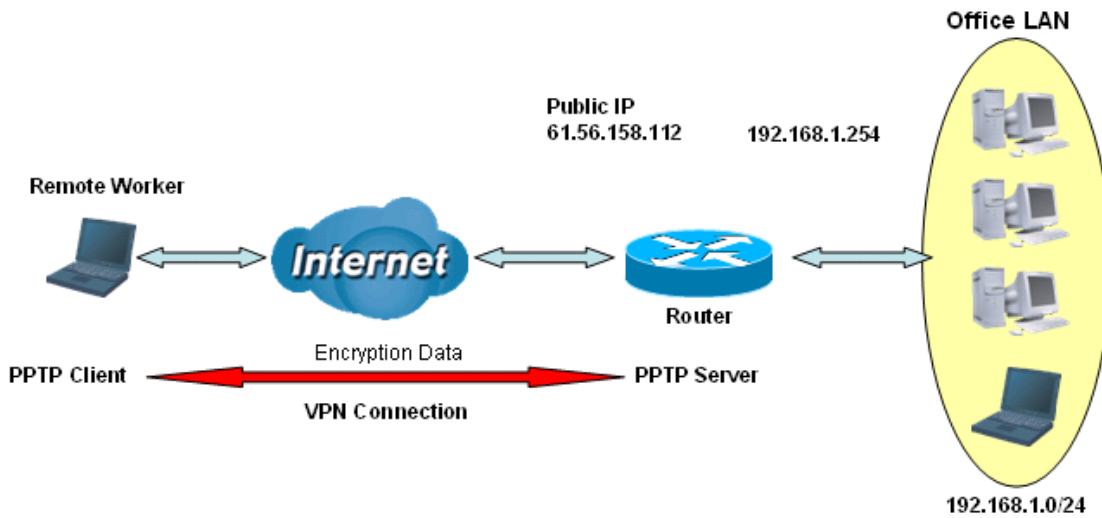
Server Address: Enter the WAN IP address of the PPTP server.

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

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

Click **Save** to apply the settings.

Example: PPTP – Remote Employee Dial-in to 6300VNL



PPTP VPN-Remote Access (Dial-in)

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	Give a name of L2TP connection
Authentication Type	MPPE 128bit	Authentication type
Username	test	Dial in authenticate user name
Password	test	Dial in authenticate user password
Connection Type	Remote Access	Remote access for dial in
Assigned IP	192.168.1.2	An IP assigned to the dial in client

▼ PPTP Server

PPTP Server Activated Deactivated

Authentication Type: MPPE 128bit Encryption ▼

MS-DNS: 192.168.1.254

Rule Index: 1 ▼

Connection Name: HS-RA

Active: Yes No

Username: test

Password: ****

Connection Type: Remote Access ▼

Private IP Address assigned to Dial-in User: 192.168.1.2

Remote Network IP Address:

Remote Network Netmask:

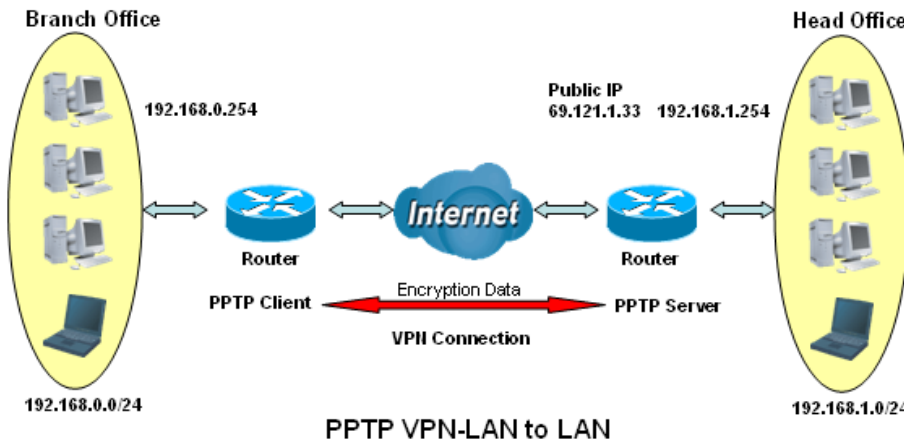
PPTP Server Listing

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

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

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

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



Configuring PPTP Server in the Head office

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

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

PPTP Server

PPTP Server Activated Deactivated

Authentication Type: MPPE 128bit Encryption

MS-DNS: 192.168.1.254

Rule Index: 1

Connection Name: HS-LL

Active: Yes No

Username: test

Password: ****

Connection Type: LAN to LAN

Private IP Address assigned to Dial-in User: 192.168.1.2

Remote Network IP Address: 192.168.0.0

Remote Network Netmask: 255.255.255.0

Save Delete

PPTP Server Listing

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

Configuring PPTP Client in the Branch office

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

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

▼ PPTP Client

Rule Index	1 ▼
Connection Name	BC-LL
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Authentication Type	MPPE 128bit Encryption ▼
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

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.

Connection Name: User-defined name for the connection.

Active: To enable or disable the tunnel.

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

Username: Please input the username for this account.

Password: Please input the password for this account.

Private IP Address Assigned to Dial-in User: The private IP to be assigned to 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: Please input the username for this account.

Password: Please input the password for this account.

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 / establishes a VPN tunnel.

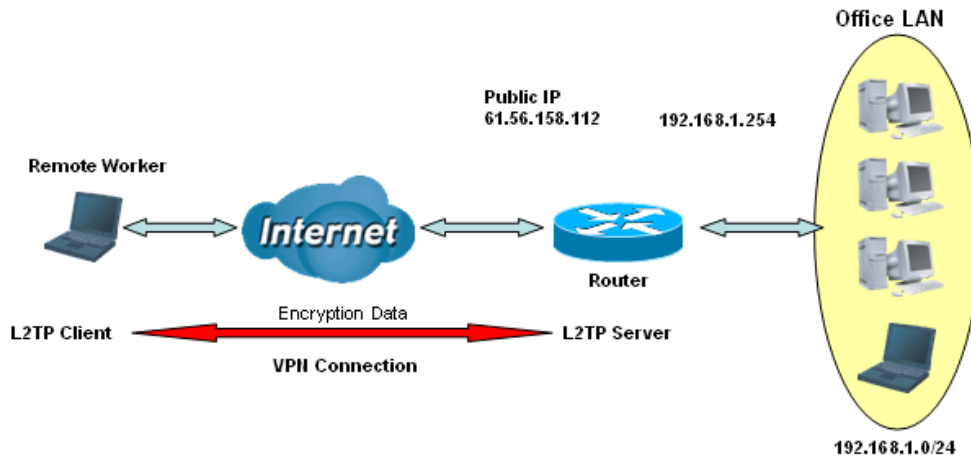
Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

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

Click **Save** to apply the settings.

Example: L2TP VPN – Remote Employee Dial-in to 6300VNL

A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-in)

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	Give a name of L2TP connection
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	test	Dial in authenticate user name
Password	test	Dial in authenticate user password
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

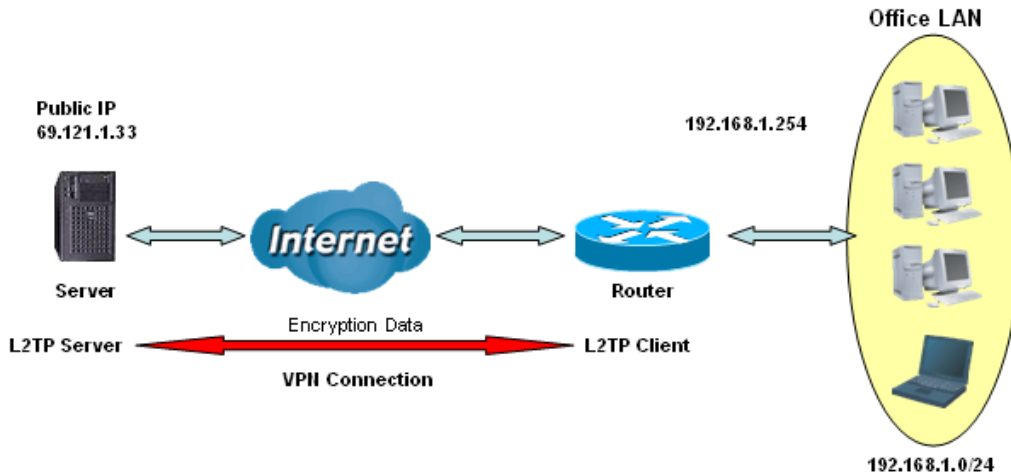
Save Delete

L2TP Listing

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

Example: L2TP VPN – 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.



L2TP VPN-Remote Access (Dial-out)

Item		Description
Connection Name	HC-RA	Give a name of L2TP connection
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	Dialed server IP address
Authentication Type	Chap/Pap	Authentication type
Username	test	Dial out authenticate user name
Password	test	Dial out authenticate user password
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

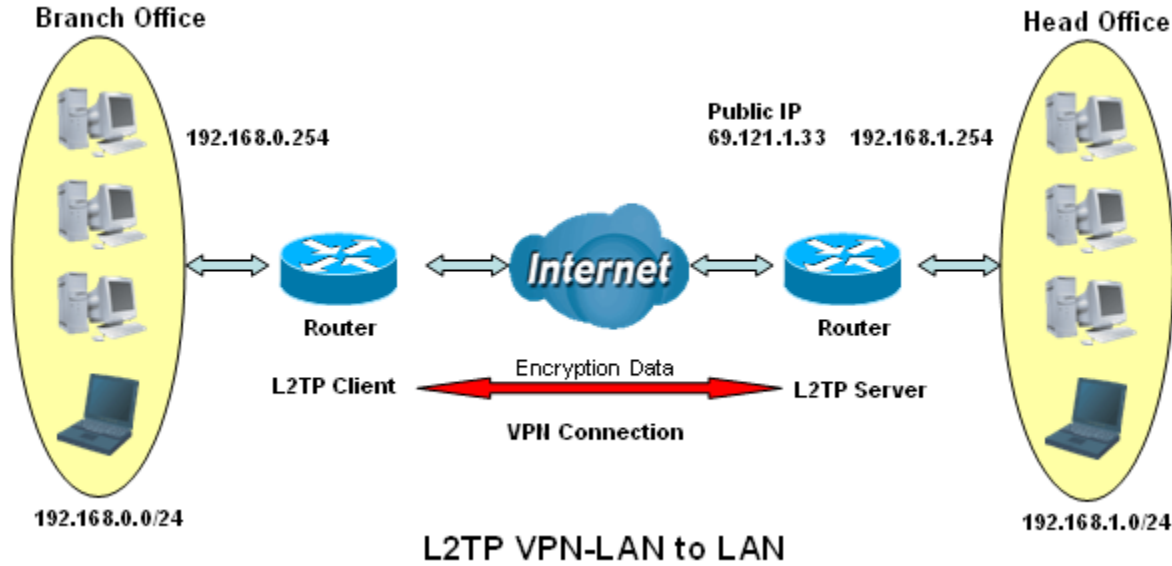
L2TP Listing

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 head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

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



Configuring L2TP VPN Dial-in in the Head office

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

Item	Description	
Connection Name	HS-LL	Give a name of L2TP connection
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	Test	Dial in authenticate user name
Password	Test	Dial in authenticate user password
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 access network
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	
Local Host Name	
Remote Host Name	
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 head office.

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

▼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	
Local Host Name	
Remote Host Name	
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 tunnels can be added.

GRE					
Rule Index	1 ▼				
Connection Name	<input type="text"/>				
Active	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Interface	4G LTE -1 ▼				
Remote Gateway IP	<input type="text" value="0.0.0.0"/>				
Tunnel Local IP Address	<input type="text" value="0.0.0.0"/>				
Tunnel Local Netmask	<input type="text" value="0.0.0.0"/>				
Tunnel Remote IP Address	<input type="text" value="0.0.0.0"/>				
Remote Network IP Address	<input type="text" value="0.0.0.0"/>				
Remote Network Netmask	<input type="text" value="0.0.0.0"/>				
Enable Keepalive	<input type="checkbox"/>				
Keepalive Retry Times	<input type="text" value="3"/>				
Keepalive Interval	<input type="text" value="5"/> Second(s)				
MTU	<input type="text" value="1460"/>				
Active as Default Route	<input type="radio"/> Yes <input checked="" type="radio"/> No				
<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: User-defined name for the connection.

Active: Select Yes to activate the GRE tunnel.

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

Remote Gateway: The remote GRE gateway IP.

Tunnel Local IP: Please set the source IP for the local tunnel.

Tunnel Local Netmask: Please set the Netmask for the local tunnel.

Tunnel Remote IP Address: Set the peer IP address of the tunnel.

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

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

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

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.

MTU: Maximum Transmission Unit.

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

Click **Save** to apply the settings.

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.)
<input type="button" value="Save"/>	

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.

The screenshot shows a web-based configuration interface for SNMP. It is organized into two main sections: 'SNMP' and 'SNMPv3'. In the 'SNMP' section, the 'SNMP' feature is currently 'Deactivated'. There are three input fields: 'Get Community', 'Set Community', and 'Trap Manager IP' (set to 0.0.0.0). The 'SNMPv3' section has 'SNMPv3' set to 'Disable'. It includes fields for 'Username', 'Access Permissions' (set to 'Read Only'), 'Authentication Protocol' (set to 'MD5'), 'Authentication Key' (8-31 characters), 'Privacy Protocol' (set to 'DES'), and 'Privacy Key' (8-31 characters). A 'Save' button is located at the bottom left of the configuration area.

SNMP: Select to enable SNMP feature.

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

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

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

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

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

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

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

Remote Syslog

Remote Syslog allows users to set up an isolated external syslog server to receive system logs from the router for convenient view.

Syslog	
Syslog	<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 Log: Select whether to activate to use remote syslog service.

Server IP Address: Enter your syslog server IP address.

Server UDP Port: The syslog service UDP port, default is 514.

Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Configuration	
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.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es). But note that first users have to go to the Dynamic DNS registration service provider to register an account.

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your BEC 6300VNL by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

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

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

Example: How to register a DDNS account

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

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

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

Configuration

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="www.hometest.com"/>
Username	<input type="text" value="test1"/>
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)"/>

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**.

The screenshot shows the 'Access Control' configuration page. At the top, there is a 'Configuration' tab. Below it, the 'Access Control' section is expanded, showing a form with the following fields:

- Access Control:** Activated Deactivated
- Access Control Editing:**
 - Rule Index:** 1 (dropdown)
 - Active:** Yes No
 - Secure IP Address:** 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
 - Application:** ALL (dropdown)
 - Interface:** LAN (dropdown)
- Buttons:** Save, Delete

Below the form is the 'Access Control Listing' table:

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

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

Rule Index: The numerical indication of the rules

Active: Select to activate the rule.

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the 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**.

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.

This is an identical screenshot of the configuration interface shown above, displaying the 'Access Control' settings and the 'Access Control Listing' table.

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

Configuration

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

The screenshot shows the configuration page for a Packet Filter. The 'Filter Type' is set to 'IP & MAC Filter'. The 'Rule Index' is 1. The 'Action' is 'Black List'. The 'Interface' is 'LAN' and the 'Direction' is 'Both'. The 'Type' is 'IPv4'. The 'Source IP Address' is '0.0.0.0', 'Source Subnet Mask' is '0.0.0.0', 'Source Port Number' is '0', 'Destination IP Address' is '0.0.0.0', 'Destination Subnet Mask' is '0.0.0.0', 'Destination Port Number' is '0', 'DSCP' is '0', and 'Protocol' is 'TCP'. There are 'Save' and 'Delete' buttons at the bottom of the configuration area.

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

Packet Filter

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

IP & MAC Filter Editing

Rule Index: The numerical indication of the rules.

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

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

Interface: Select which interface the rule will be applied to.

Direction: Select if the rule applies to outgoing packets, incoming packets or both directions.

Type: Choose type of field you want to specify to monitor. Select “IPv4” for IPv4 address, port number and protocol. Select “IPv6” for IPv6 address, port number and protocol. Select “MAC” for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.

- Source Port Number:** The source port number of packets to be monitored. 0 means “Don’t care”.
- Destination IP Address:** The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.
- Destination Subnet Mask:** Enter the subnet mask of the destination network.
- Destination Port Number:** This is the Port that defines the application. (E.g. HTTP is port 80.)
- DSCP:** DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)
- Protocol:** Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

IP/MAC Filter Listing

- #:** Item number.
- Active:** Whether the connection is currently active.
- Interface:** show the interface the rule applied to.
- Direction:** show the direction the rule applied to.
- Source IP (IPv6) Address/Mask (Prefix):** The source IP address or range of packets to be monitored.
- Destination IP (IPv6) Address/Mask (Prefix):** This is the destination subnet IP address.
- Source MAC Address:** show the MAC address of the rule applied.
- Source Port:** The source port number of packets to be monitored.
- Destination Port:** This is the Port or Port Ranges that defines the application.
- DSCP:** show the set DSCP.
- Protocol:** It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP** or **ICMPv6**

Access Management – Packet Filter (Application & URL Filters)

❖ Packet Filter - Application Filter

Configuration

Packet Filter

Packet Filter

Filter Type

Application Filter Editing

Application Filter Activated Deactivated

ICQ Allow Deny

MSN Allow Deny

YMSG Allow Deny

Real Audio/Video(RTSP) Allow Deny

Application Filter: Select this option to Activated/Deactivated the Application filter.

ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video (RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

❖ Packet Filter - URL Filter

Configuration

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
1	Yes	www.yahoo.com

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

URL Filter Rule Index: The numerical indication of the rules.

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.

Parental Control

With this feature, router can reject to provide **Internet** services to the specified computer during some specified time interval. This can be very useful for parents to give control to children using computer without restraint.

Configuration

Parental Control

Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

Save

Parent Control: Select Activated to enable this feature.

MAC Address: Type the MAC address(es) you want to block to access the internet (access to the router is sustained). The format of MAC address could be: xx:xx:xx:xx:xx:xx . If you want to set restriction to the Browser PC, you can directly check the checkbox of Browser's MAC Address.

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

Configuration

Parental Control

Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

SAVE

Timeslot1 at Time Schedule:

Configuration

Time Schedule

Time Index

Name

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

Save

SAMBA & FTP Server

Samba and FTP are served as network sharing.

The screenshot shows a configuration interface with the following fields and values:

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 Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

SAMBA/FTP login account:

- ▶ **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.

Please see [User Management](#).

Example: How to setup Samba

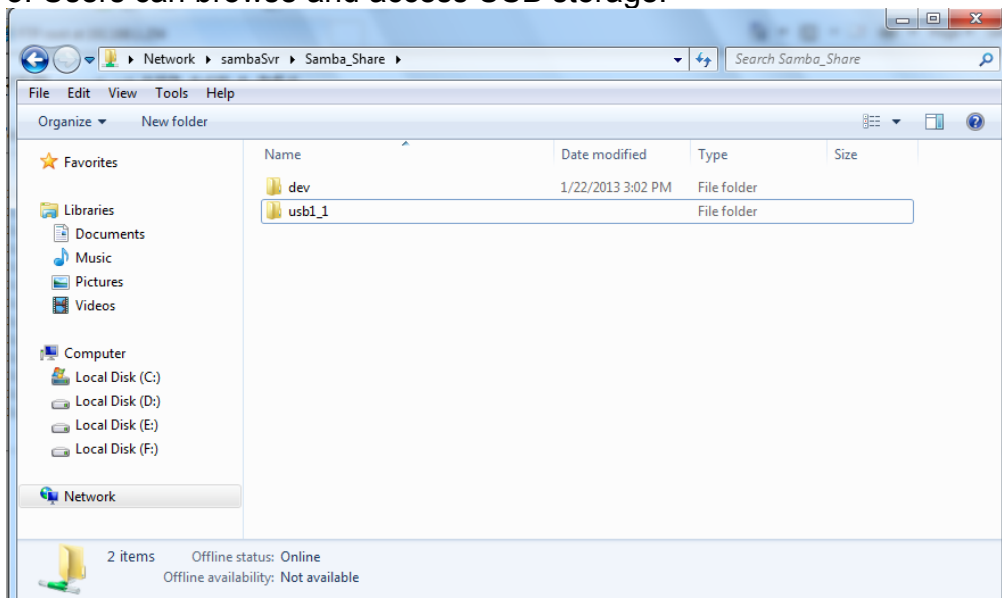
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.

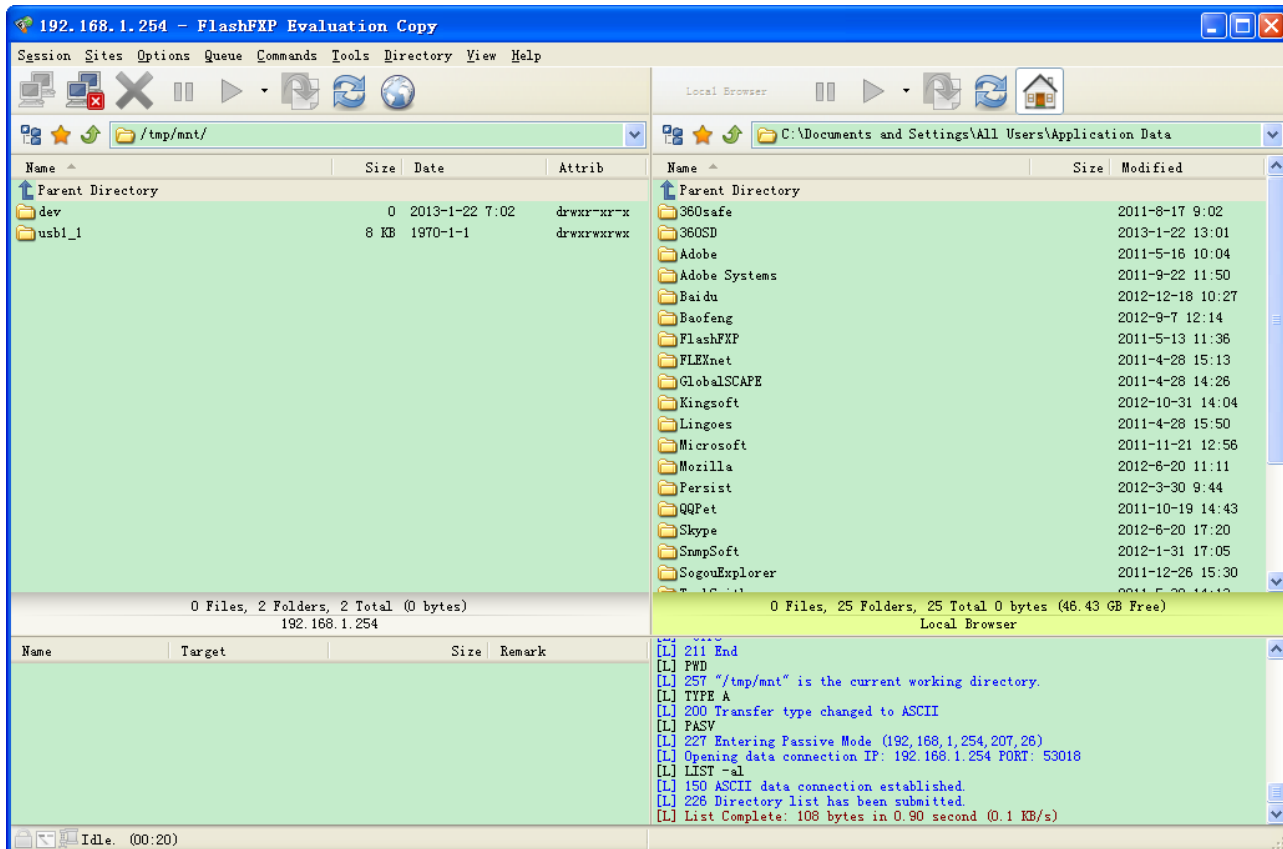


Example: How to setup FTP :

1. Access via FTP tools

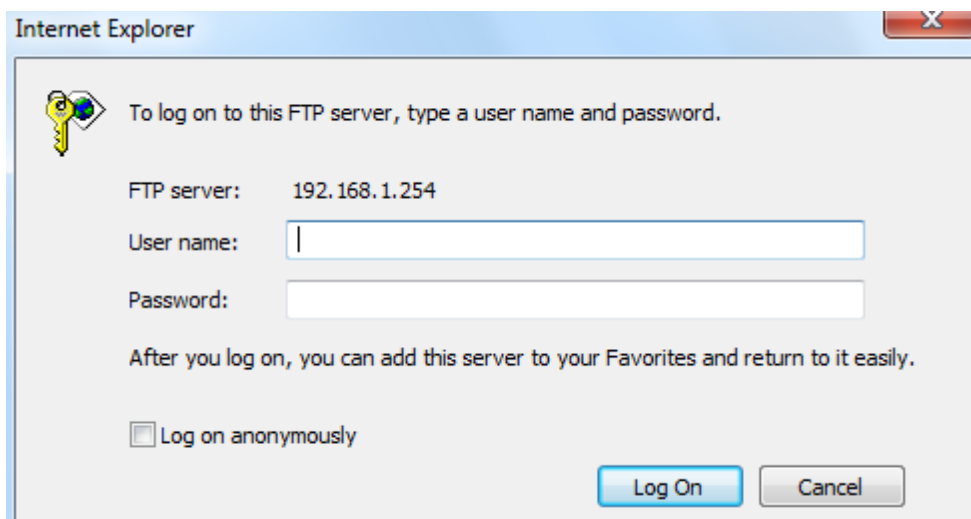
Take popular FTP tool of FlashFXP for example:

- 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.



Maintenance – User Management (Administrator Account)

Maintenance

Maintenance gives users the ability to maintain the device as well as examine 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.

Configuration

▼ User Management

User Account

Index: 1

Username: admin

New Password: ●●●●

Confirm Password: ●●●●

FTP Authority Setup

FTP Access: Enable Disable

Permission: Read/Write Read

SAMBA Authority Setup

SAMBA Access: Enable Disable

Permission: Read/Write Read

Please restart the Storage server after config changed

Save Delete

User Account List

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

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.

Web GUI Permission

Login using the Administrator account, you will have the full accessibility to manage & control your BEC 6300VNL device and can also create user accounts for others to control some of the open configuration settings.

❖ **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.

The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' header. Below it, a 'User Management' section is expanded. The 'User Account' section includes fields for 'Index' (set to 2), 'Username' (set to 'user'), 'New Password' (masked with dots), and 'Confirm Password' (masked with dots). Below this are sections for 'FTP Authority Setup', 'SAMBA Authority Setup', and 'Web GUI Permission', each with 'Enable' and 'Disable' radio buttons. For FTP and SAMBA, 'Disable' is selected. For Web GUI Permission, 'Interface Setup', 'Advanced Setup', and 'Access Management' are enabled, while 'Guest Account' and 'Maintenance' are disabled. A note at the bottom of the form says '**Please restart the Storage server after config changed**'. There are 'Save' and 'Delete' buttons. Below the form is a 'User Account List' table.

#	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 / Access Management Setup / Maintenances: Enable to grant this user access to these features.

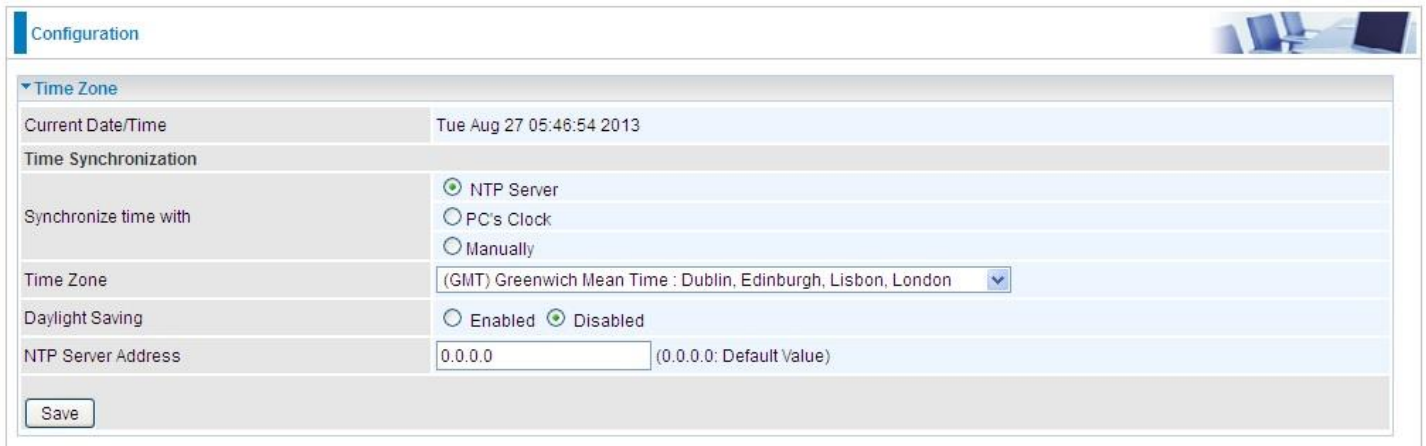
When someone accesses to the 6300VNL using this “user” account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account..

Click **Save** to apply 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.



The screenshot shows the 'Configuration' page with the 'Time Zone' section expanded. The 'Current Date/Time' is 'Tue Aug 27 05:46:54 2013'. Under 'Time Synchronization', 'Synchronize time with' has three radio button options: 'NTP Server' (selected), 'PC's Clock', and 'Manually'. The 'Time Zone' dropdown is set to '(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London'. 'Daylight Saving' has 'Enabled' and 'Disabled' radio buttons, with 'Disabled' selected. The 'NTP Server Address' is '0.0.0.0' with a note '(0.0.0.0: Default Value)'. A 'Save' button is at the bottom left.

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, 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.

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

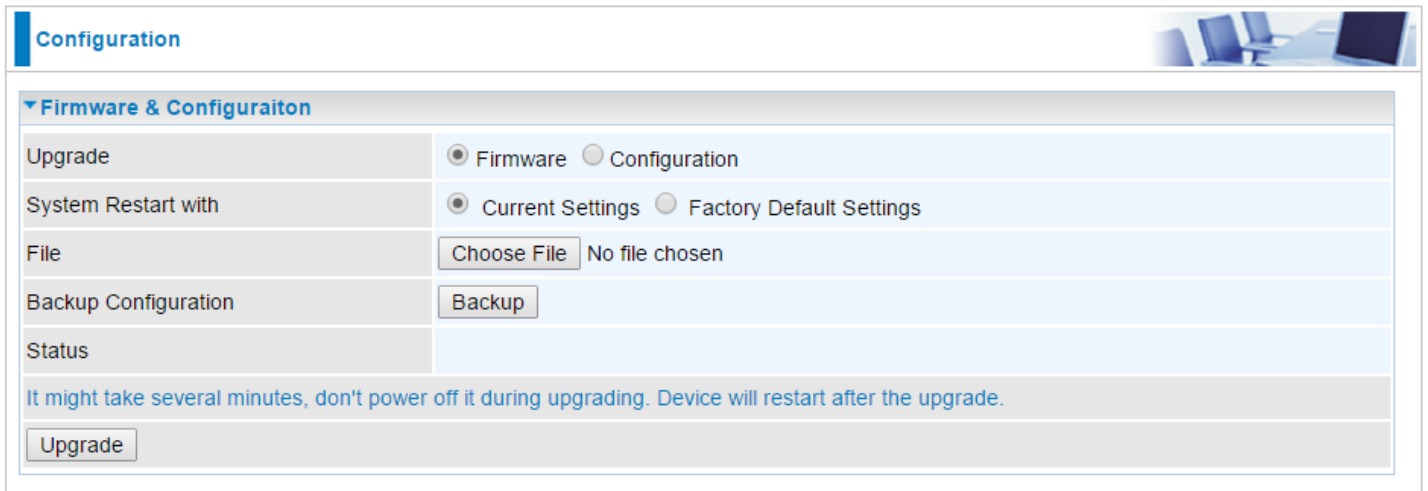
Daylight Saving: Select this option if you use daylight savings time.

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

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your 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.



The screenshot shows the 'Configuration' page with a sub-section for 'Firmware & Configuration'. It includes several settings:

- Upgrade:** Radio buttons for 'Firmware' (selected) and 'Configuration'.
- System Restart with:** Radio buttons for 'Current Settings' (selected) and 'Factory Default Settings'.
- File:** A 'Choose File' button and the text 'No file chosen'.
- Backup Configuration:** A 'Backup' button.
- Status:** A text area.

Below the settings, there is a warning message: "It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade." and an 'Upgrade' button.

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

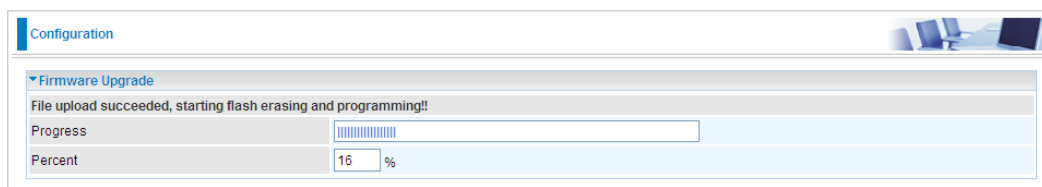
- ▶ **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- ▶ **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Browse: Click **Browse...** 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.



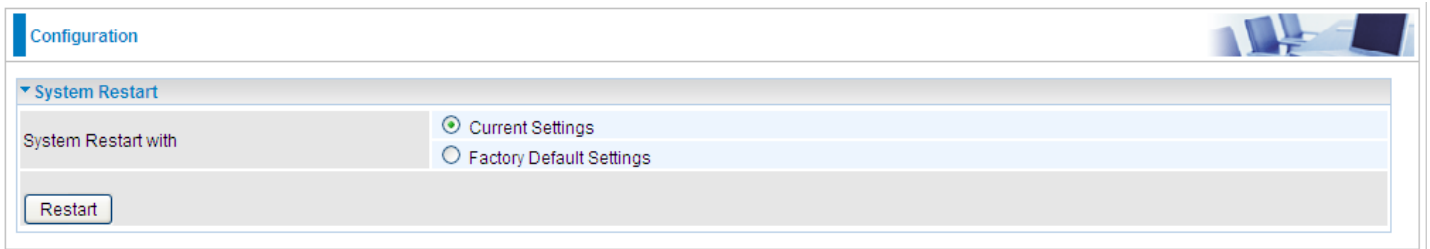
The screenshot shows the 'Firmware Upgrade' section with a progress bar. The progress bar is partially filled, and the text below it indicates '16 %'.



DO NOT turn off / power off the device or interrupt the firmware upgrading while it is still in process. Improper operation could damage your BEC 6300VNL.

System Restart

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



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

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

Auto Reboot

Schedule an automatic reboot for your 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 00 : 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 00 : 00
Save										

Click **Save** to apply the settings

Example: Schedule 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 22 : 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 checked="" type="checkbox"/> Sat.	<input checked="" type="checkbox"/> Sun.	Time 09 : 00
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

Configuration	
▼ Diagnostic Tool	
WAN Interface	3G/4G-LTE
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (221.6.4.66)	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"/>	

Click START to begin to diagnose the connection.

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

EWAN

Configuration 

▼ Diagnostic Tool

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

Start

Click START to begin to diagnose the connection.

Configuration 

▼ Diagnostic Tool

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

Start

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.

APPENDIX: PRODUCT SUPPORT & CONTACT

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

Contact BEC @ <http://www.bectechnologies.net>

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

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

FCC Statement

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

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

FCC Caution:

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

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . 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.

