



User Manual

BEC 6900 R21 / RidgeWave 6900 4G/LTE Outdoor Router

Copyright Notice

Copyright© 2019 BEC Technologies Inc. All rights reserved.

BEC Technologies reserves the right to change and make improvement to this manual at any time without prior notice.

No part of this document may be reproduced, copied, transmitted in any form or by any means without prior written permission from BEC Technologies, Inc.

Support Contact Information

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

Telephone: +1 972 422 0877

TABLE OF CONTENTS

COPYRIGHT NOTICE	1
SUPPORT CONTACT INFORMATION.....	1
CHAPTER 1: INTRODUCTION	1
INTRODUCTION TO YOUR ROUTER	1
FEATURES & SPECIFICATIONS	3
HARDWARE SPECIFICATIONS	5
APPLICATION DIAGRAM.....	5
CHAPTER 2: PRODUCT OVERVIEW	6
IMPORTANT NOTE FOR USING THIS ROUTER.....	6
PACKAGE CONTENTS.....	6
DEVICE DESCRIPTION	7
MOUNTING KIT INSTALLATION – USING LP2S MOUNTING KIT	9
MOUNTING KIT INSTALLATION – USING RT4R MOUNTING KIT	12
ROUTER INSTALLATION INSTRUCTIONS	19
SYSTEM RECOVERY PROCEDURES	22
CHAPTER 3: BASIC INSTALLATION	23
NETWORK CONFIGURATION – IPv4.....	24
Configuring PC in Windows 10 (IPv4)	24
Configuring PC in Windows 7/8 (IPv4).....	26
Configuring PC in Windows Vista (IPv4).....	28
NETWORK CONFIGURATION – IPv6.....	30
Configuring PC in Windows 10 (IPv6)	30
Configuring PC in Windows 7/8 (IPv6).....	32
Configuring PC in Windows Vista (IPv6).....	34
DEFAULT SETTINGS.....	36

CHAPTER 4: DEVICE CONFIGURATION.....37

LOGIN TO YOUR DEVICE 37

STATUS..... 39

Device Info	39
System Status	40
System Log	41
4G/LTE Status	42
Statistics	44
DHCP Table	46
ARP Table	46
VRRP Status	46

QUICK START 47

CONFIGURATION..... 49

Interface Setup.....	49
<i>Internet</i>	49
<i>LAN</i>	52
<i>Loopback</i>	56
Advanced Setup	57
<i>Firewall</i>	57
<i>Routing</i>	58
<i>Dynamic Routing</i>	59
<i>NAT</i>	61
<i>VRRP</i>	66
<i>Static DNS</i>	67
<i>QoS</i>	68
<i>Time Schedule</i>	70
<i>Mail Alert</i>	71
Access Management	72
<i>Device Management</i>	72
<i>SNMP</i>	73
<i>Syslog</i>	75
<i>Universal Plug & Play</i>	76
<i>Dynamic DNS (DDNS)</i>	77
<i>Access Control</i>	79
<i>Packet Filter</i>	81
<i>CWMP (TR-069)</i>	85
<i>Parental Control</i>	87
<i>BECentral Management</i>	88
Maintenance	89

<i>User Management</i>	89
<i>Time Zone</i>	91
<i>Firmware & Configuration</i>	92
<i>System Restart</i>	93
<i>Auto Reboot</i>	94
<i>Diagnostics Tool</i>	95

CHAPTER 5: TROUBLESHOOTING97

Problems with the Router	97
Problem with LAN Interface	97
Recovery Procedures.....	98

APPENDIX: PRODUCT SUPPORT & CONTACT99

FCC STATEMENT	100
PROFESSIONAL INSTALLATION INSTRUCTIONS (BEC 6900 R21)	101

CHAPTER 1: INTRODUCTION

Introduction to your Router

Congratulations on your purchase of the **BEC 6900 R21 / RidgeWave 6900 (Outdoor 4G/LTE Router)** known as BEC 4G/LTE ODU.

This unit is a lightweight, an industrial-grade outdoor fixed wireless router with an IP68 rated enclosure to withstand extreme weather conditions and harsh rugged deployments. With integrated IEEE802.3at power over Ethernet (PoE) support, the BEC 4G/LTE ODU provides an easy installation from eliminating the need for a separate power and data cable.

In addition to outdoor, it can be installed in environments such as: manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses or virtually any venue requiring a robust wireless solution. The BEC 4G/LTE ODU integrates a high-performance device with an embedded LTE module and advanced IP networking features enabling support of multiple high bandwidth applications.

Lightweight, Compact and unobtrusive Design

With multiple mounting options and a lightweight, it is easily to install the BEC 4G/LTE ODU by single person. The BEC 4G/LTE ODU also has a built-in passive Gigabit Power of Ethernet (GPoE) so both data and power can be sent from the unit.

Designed for Challenging / Rugged Deployments

The BEC 4G/LTE ODU is designed for the toughest industrial environments. With IP68 hardened enclosure with industrial-grade components, the BEC 4G/LTE ODU can be installed in manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses, etc.

4G/LTE Mobility

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

4G/LTE Management Center

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

IPv6 Supported

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

Quick Start Wizard

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

Firmware Upgradeable

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

Features & Specifications

- Outdoor 4G for high speed mobile connectivity
- 4G embedded with a built-in SIM card slot
- 4G Management Center for connection monitoring
- Firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ease of Use with Quick Installation Wizard
- Ideal for homes, businesses, rural areas and the underserved

Operational Mode

- Bridge or Routed mode

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)

Management

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

Hardware Specifications

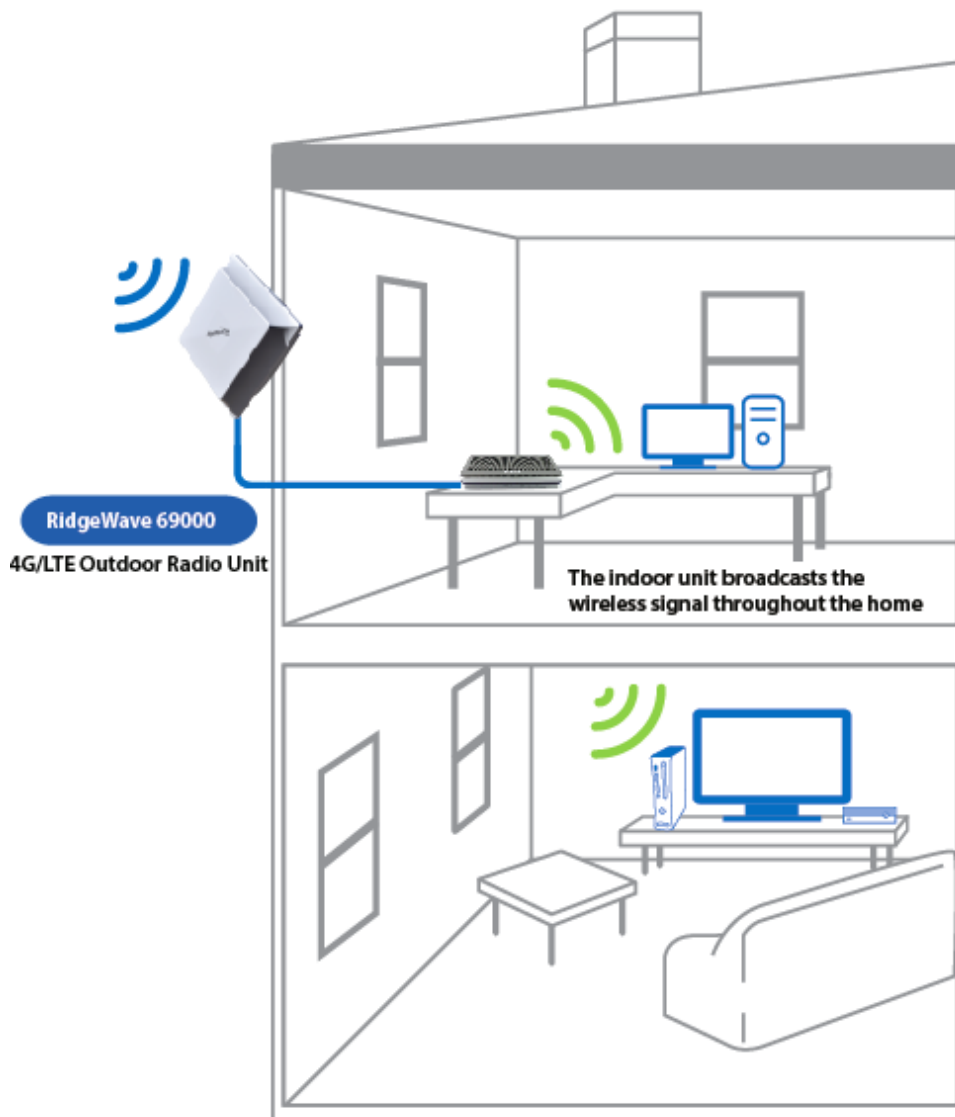
Physical Interface

- 10/100/1000 Gigabit Ethernet LAN with IEEE802.3at compliant Gigabit PoE PD
- SIM slot: (for the SIM card from Telco / ISP)
- LED Indicators: Power, LAN (PoE), LTE, and Internet

Physical Specifications

- Dimensions (W*H*D): 12.6" x 12.6" x 2.91" (320mm x 320mm x 74mm)
- Weight: < 1.5kg
- IP-68 Grade Enclosure

Application Diagram



CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router



Attention

- ✓ Do not remove, open or repair the case yourself. Contact with your Internet Service Provider or have it repaired at a qualified service center.
- ✓ Use the supplied PoE (Power-over-Ethernet) injector for indoor only or with any 802.3at capable PoE injectors to connect with the RidgeWave 6900
- ✓ It is mandatory to earth ground the BEC 4G/LTE ODU. Improper grounding not only could damage the unit but also all equipment connected to it.

Package Contents

- ✓ The 4G/LTE Outdoor Router
- ✓ M25 Cable Gland
- ✓ Quick Start Guide
- ✓ Gigabit Power-over-Ethernet (PoE) Injector
- ✓ Mounting Kit (#LP2S or #RT4R)

Device Description



4
1 2 3

CONNECTORS	DESCRIPTION
SIM / LED / Reset	Insert the SIM card into the SIM slot. Press the reset button to reset device or restore to factory default settings
Gigabit LAN(PoE)	Connect it to the supplied PoE injector, 802.3at compliant, using an Ethernet cable.

LED	STATUS	DESCRIPTION
1. Power	Orange	System is either in initial startup phase or has boot failure
	Green	System is up and ready
	Off	No input power
2. LAN(PoE)	Orange	Transmission speed is at 10/100Mbps
	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Blinking	Data being transmitted/received
	Off	No device is being connected
3. Internet	Orange	IP request failed or System is in initial booting phase
	Green	IP connected and traffic is passing thru the device
4. 3G/4G-LTE	Green	RSSI greater than -69 dBm. Excellent signal condition

(Received Signal Strength Indicator)	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. 4G/LTE module is still in connected mode
	Off	No 4G/LTE module or 4G/LTE module fails

Mounting Kit Installation – Using LP2S Mounting Kit

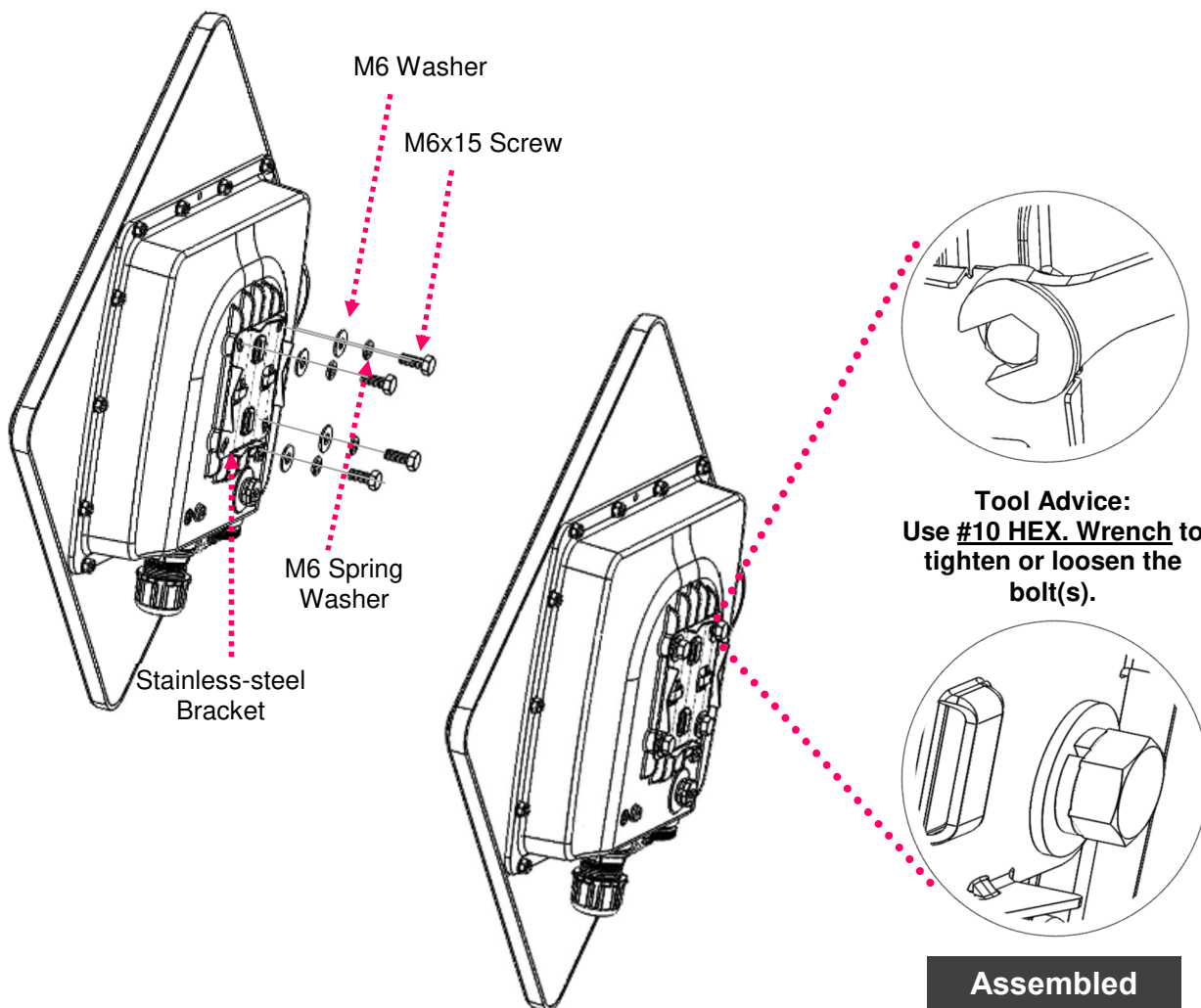
Mounting Kit includes:

- 1. Stainless Steel Bracket x 1
- 2. Hose Clamp x 2
- 3. M6x15 Screw x 4
- 4. M6 Washer x 4
- 5. Spring Washer x 4

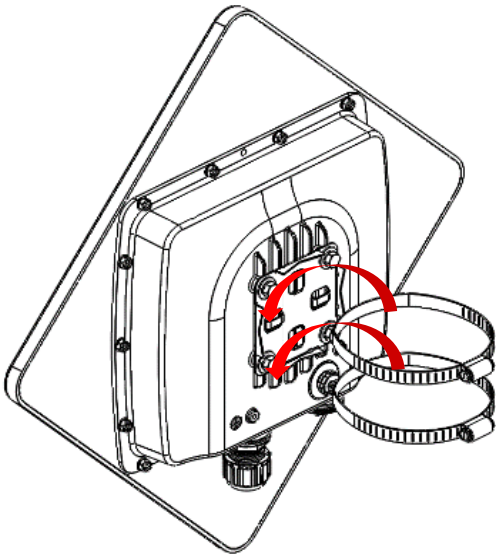


1. Attach the Stainless-Steel Bracket to the Enclosure

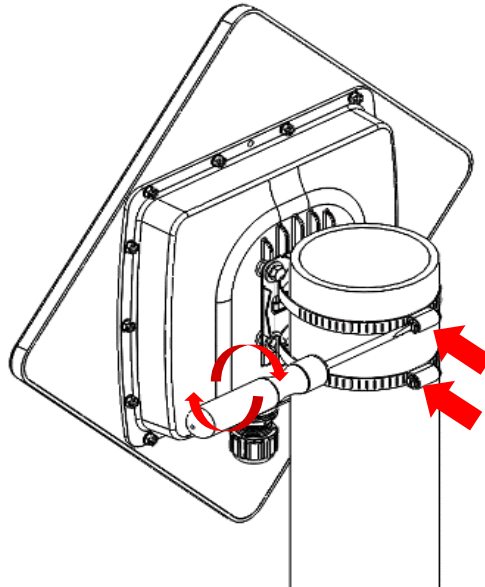
Attach the stainless-steel bracket to the back of the BEC 4G/LTE ODU enclosure then use the supplied M6 Washer, Spring Washer, and M6x15 screws in the mounting kit to screw the bracket tightly.



2. Pole Mounting for Pole 1" ~ 3" (25.4 ~ 76.2mm)

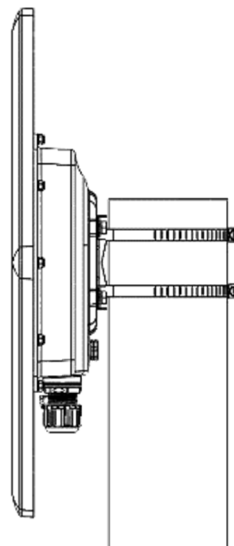


Use 1~3" hose clamps through the stainless-steel bracket.



Fix the stainless-steel bracket to the pole by using the supplied stainless hose clamps (1" ~ 3"). Use a flat-head screwdriver to turn the head of the screw clockwise to tighten it.

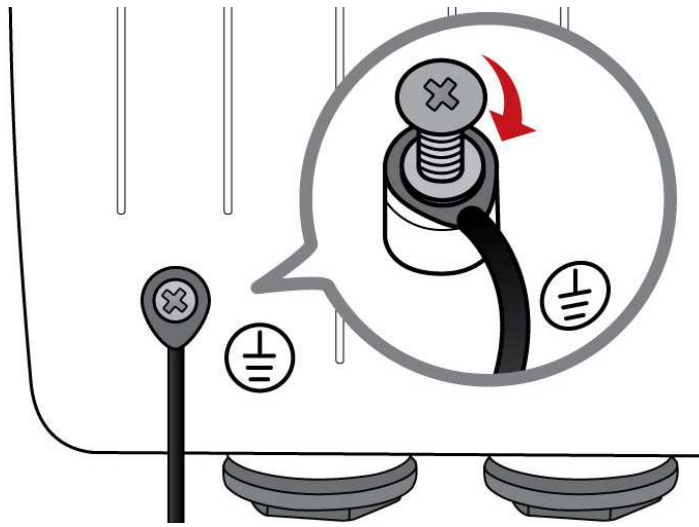
The BEC 4G/LTE ODU must be directed towards the nearest base station.



Completed

3. Proper Grounding to Complete the Installation

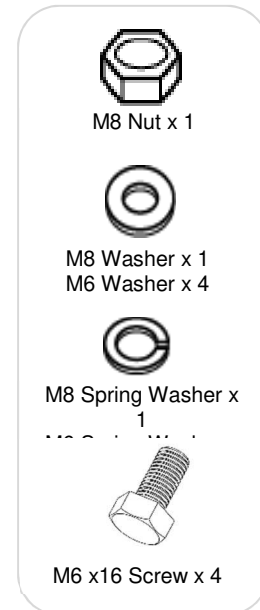
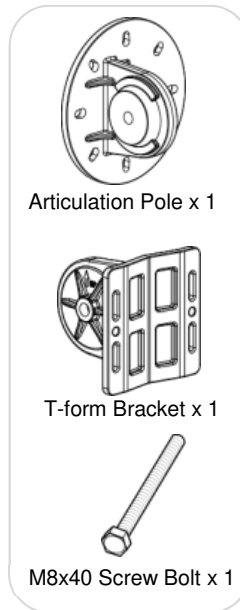
Attach the grounding wire to the BEC 4G/LTE ODU and tighten the screw.



Mounting Kit Installation – Using RT4R Mounting Kit

Mounting Kit includes:

1. Articulation Pole x 1
2. T-formed Bracket x 1
3. M8x40 Screw Bolt x 1
4. M8 Nut x 1
5. M8 Washer x 1
6. M6 Washer x 4
7. M8 Spring Washer x 1
8. M6 Spring Washer x 4
9. M6x16 Screw x 4



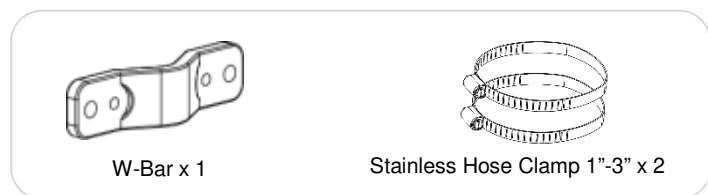
For **Wall Mount Installation**, you'll need:

10. Wood Screw x 4
11. Wood / Gyprock x 4



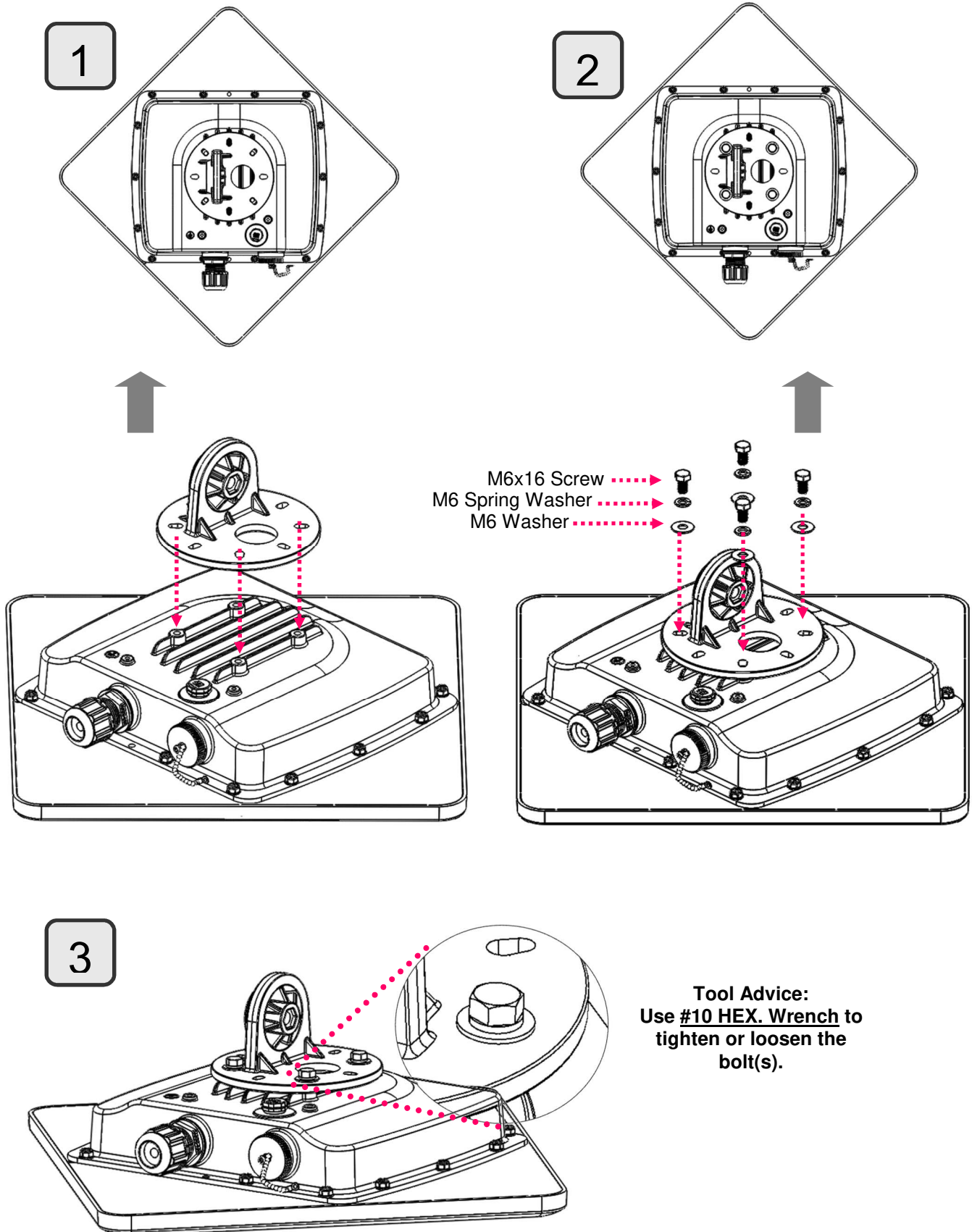
For **Pole Mount Installation**, you'll need:

12. W-Bar x 1
13. Stainless Hose Clamp x 2
14. M6x60 Screw Bolt x 2
15. M6 Washer x 2
16. M6 Spring Washer x 2

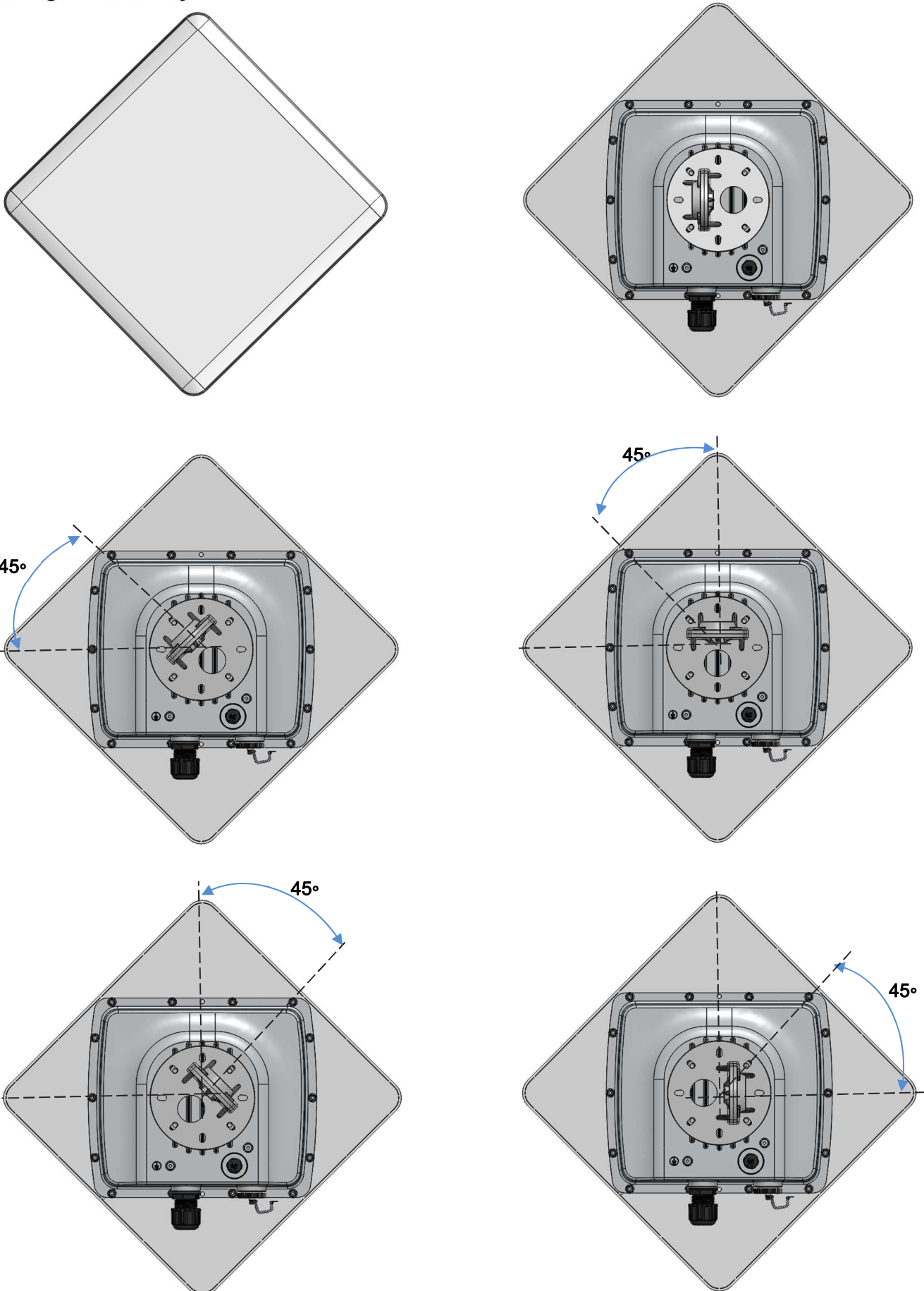


1. Attach the Articulation Pole to the Enclosure

Attach the articulation pole to the back of the BEC 4G/LTE ODU enclosure using the supplied **M6 screws**, **M6 spring washers** and **M6x16 screws** which are included in the mounting kit.



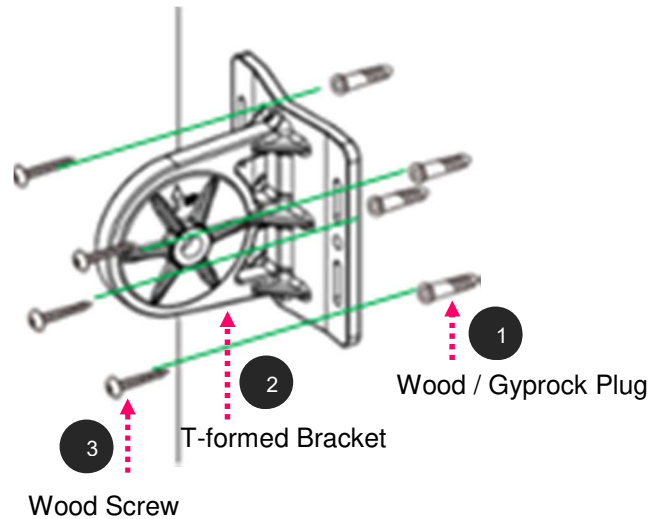
Note: The flexible mounting kit can be adjusted in multiple angles to align with the base station for higher efficiency.



2. Wall or Pole Mount Installation

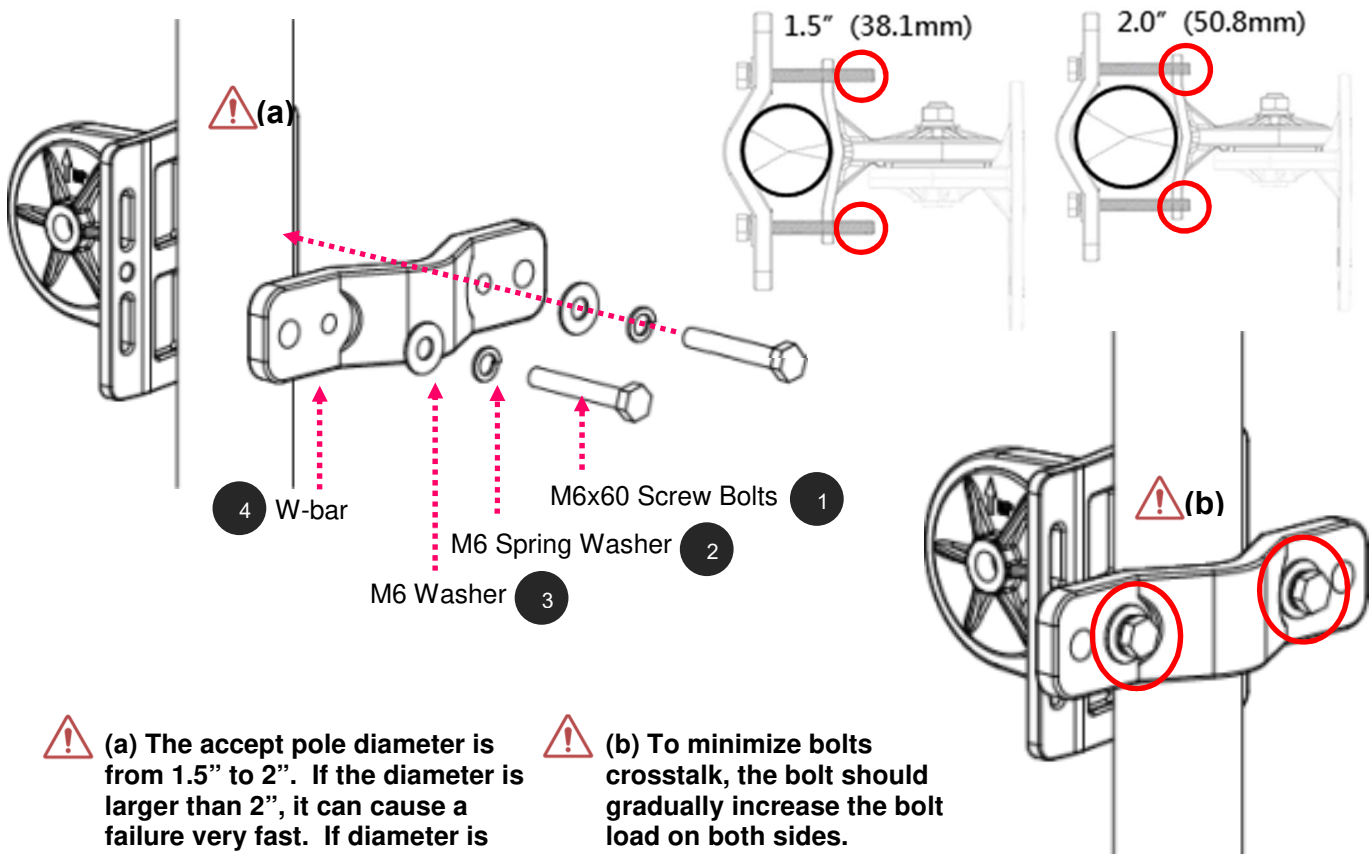
Mounting on Wall

Fix the T-formed Bracket to the wall by using **wood screws** and **Gyprock plugs**.

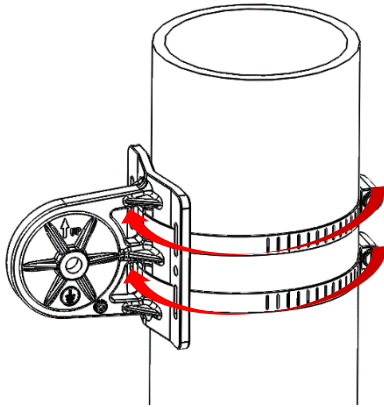


Mounting on a Pole between 1.5" to 2" (38.1~50.8mm)

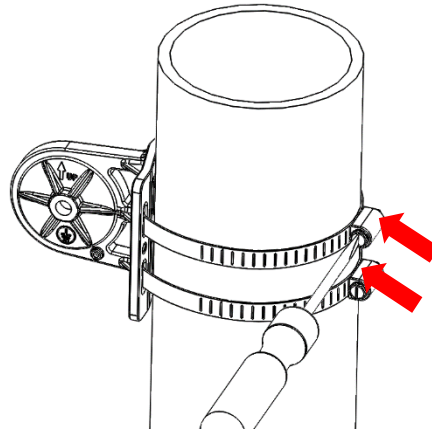
Attach the T-formed Bracket and the W-bar to the pole then use **M6x60 bolts**, **M6 spring washers** and **M6 washers** to fix the mounting kit onto the pole.



Mounting on a Pole between 1" to 3" (25.4~76.2mm)



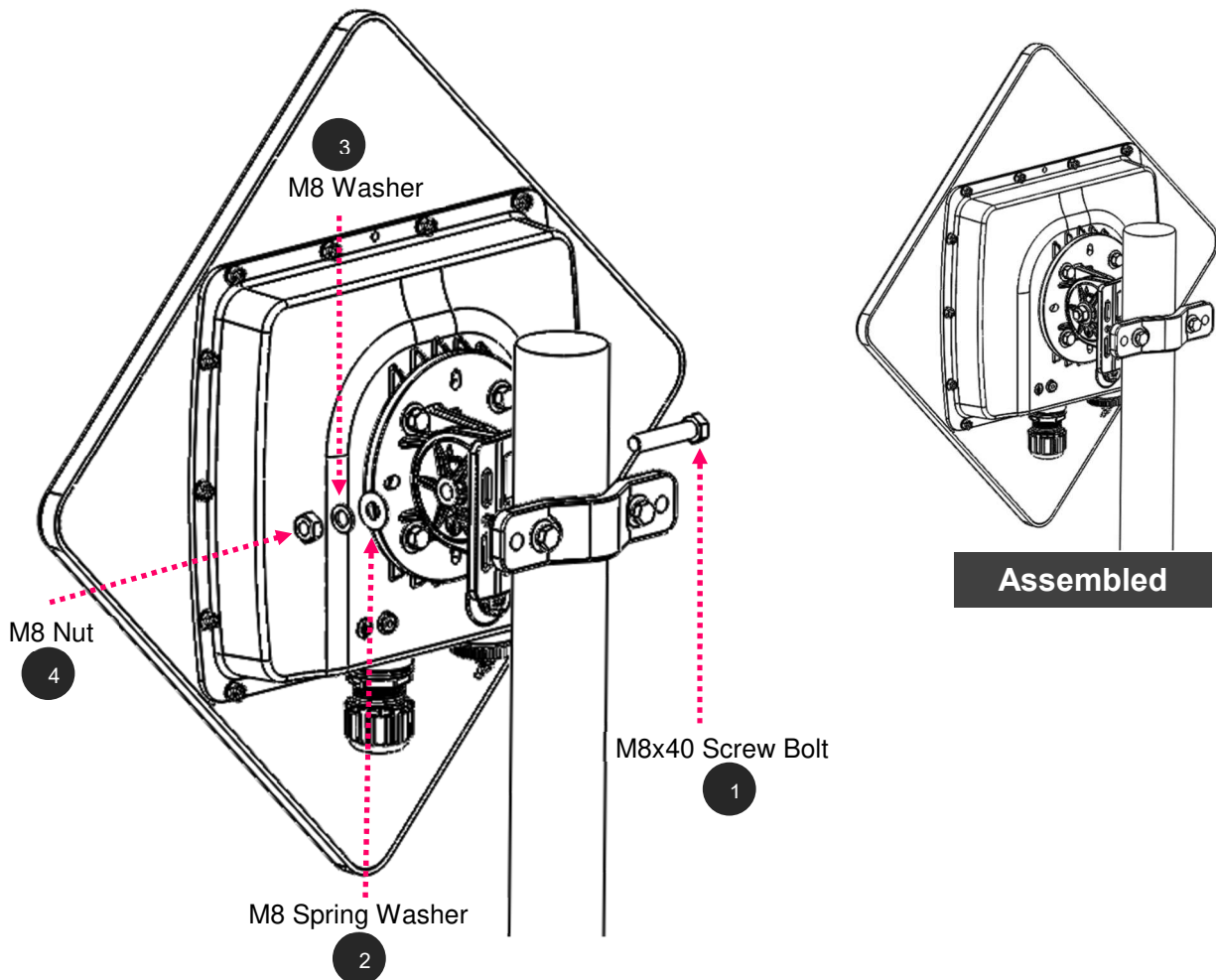
Use the stainless hose clamps through the T-formed Bracket.



Fix the T-formed Bracket to the pole by using the supplied stainless hose clamps. Use a flat-head screwdriver to turn the head of the screw clockwise to tighten it.

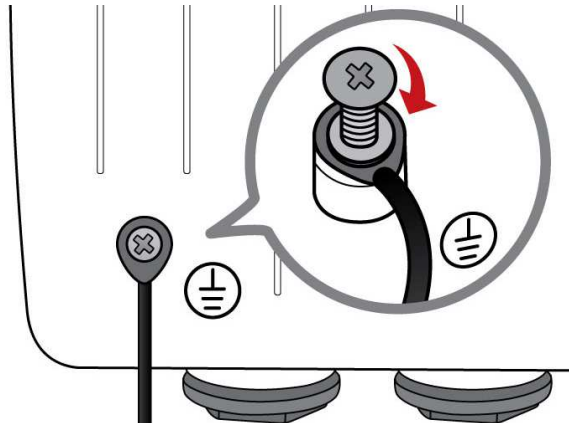
3. Attach the BEC 4G/LTE ODU Enclosure to the Pole

Attach the articulation pole (BEC 4G/LTE ODU enclosure) to the T-formed bracket using the supplied **M8 nut**, **M8 spring washer**, **M8 washer** and **M8x40 screw bolt**.



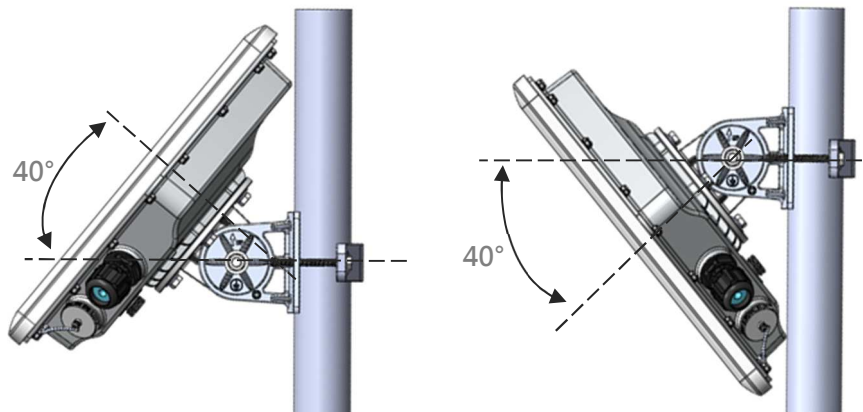
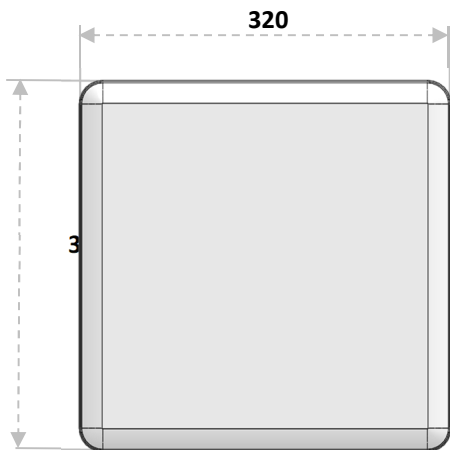
4. Proper Grounding to Complete the Installation

Attach the grounding wire to the BEC 4G/LTE ODU and tighten the screw.



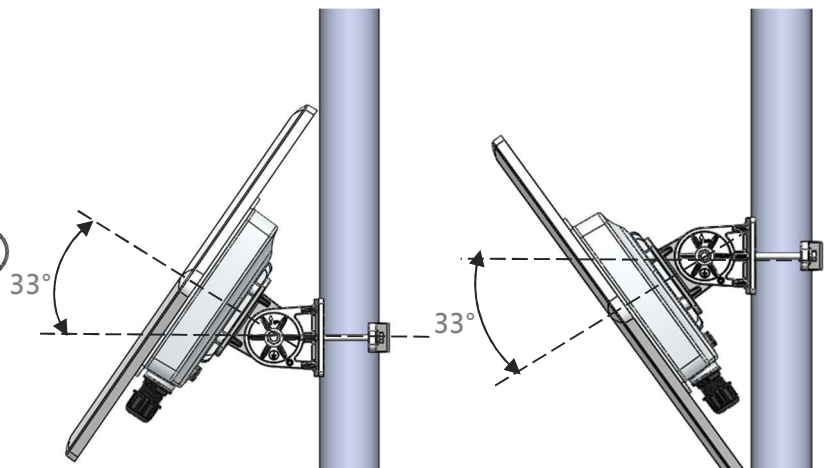
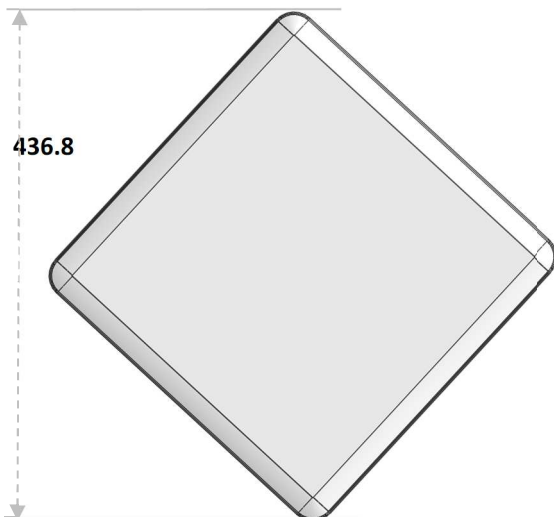
5. Position Adjustment

Adjust the BEC 4G/LTE ODU until it reaches the desire elevation and depression angle, then tight the **M8 nut** (see **Attach the BEC 4G/LTE ODU Enclosure to the Pole** for more information)



Max. upward angle: 40°
 Max. downward angle: 40°

Completed



Max. upward angle: 33°
 Max. downward angle: 33°

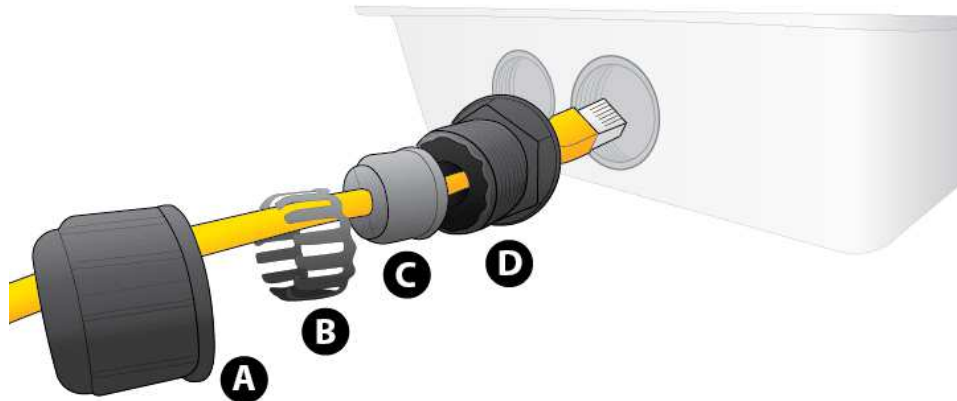
Router Installation Instructions

1. Power on your BEC 4G/LTE ODU

Step 1: Assemble M25 cable gland

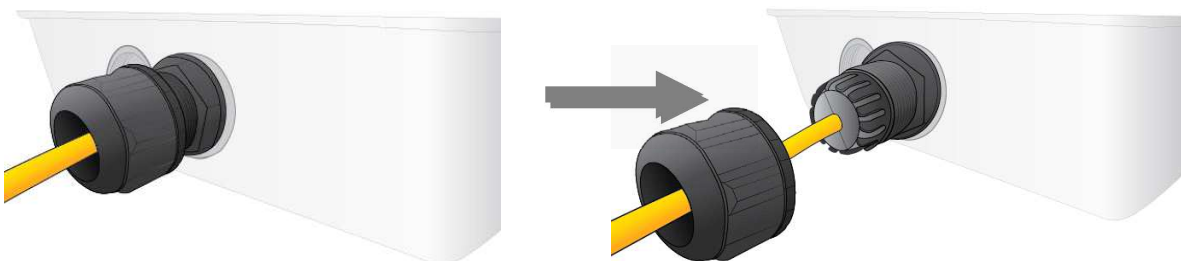


Step 2: Unscrew the LAN (PoE) cap then insert an outdoor Ethernet cable (RJ-45) through material A-D, and then connect the RJ-45 Ethernet cable into the LAN (PoE) port.



Step 3:

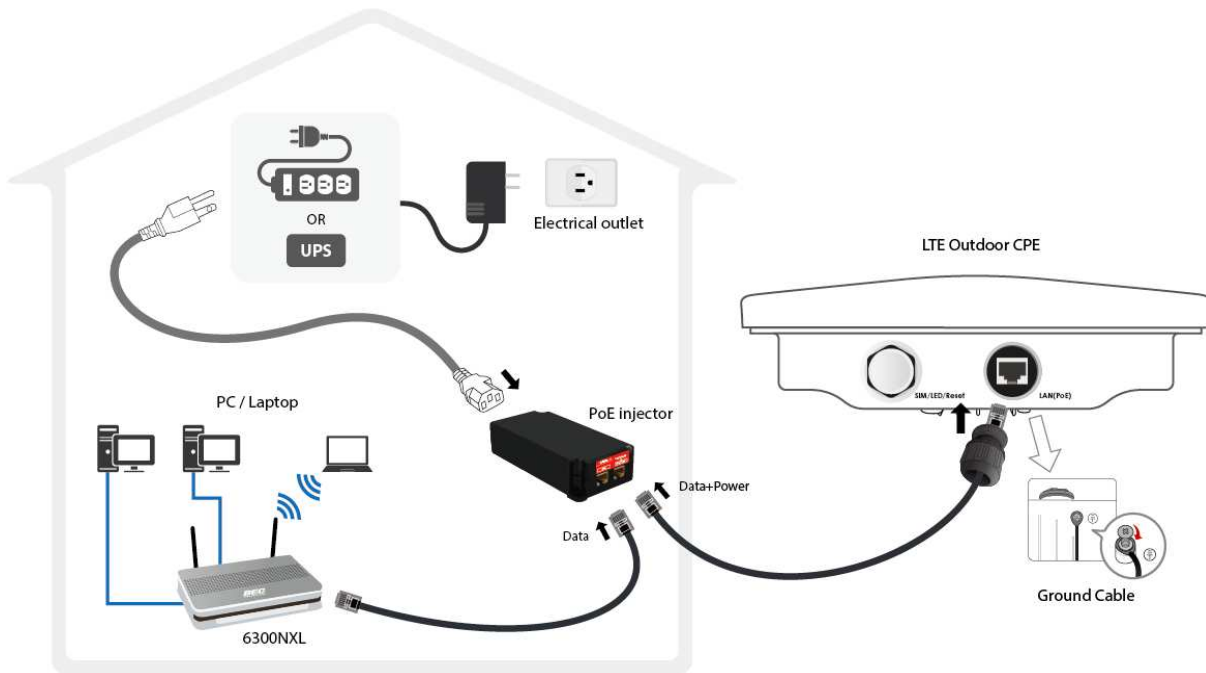
- 3.1: Insert (C) at the back end of (D)
- 3.2: clip (B) on (C)
- 3.3: keep (B) close to (D)
- 3.4: then tighten (A).



Step 4:

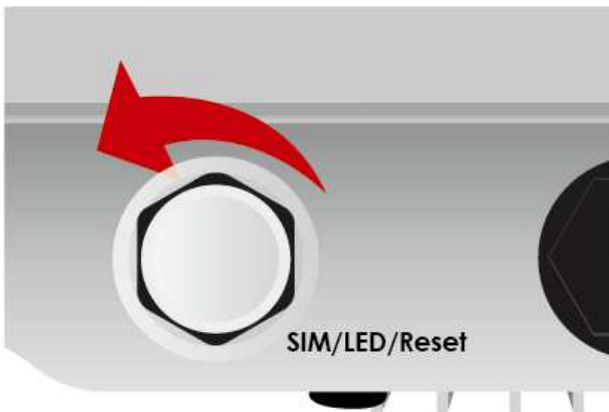
Insert the other end of outdoor Ethernet cable (RJ-45) to the supplied Gigabit PoE injector **Data+Power** port. Connect another Ethernet cable (RJ-45) directly to the **Data** port and the other end of cable to a switch or broadband router.

IMPORTANT: It is recommended to put the Gigabit PoE Injector on an UPS or Surge Protector. Use a grounding wire to ground your BEC 4G/LTE ODU is REQUIRED!



2. Set up your 4G/LTE Internet Connection

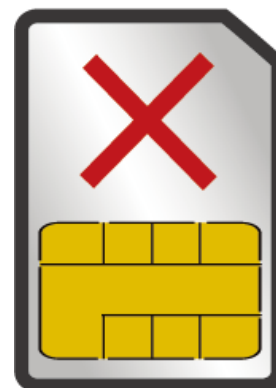
Step 1: Unscrew the cap of SIM card slot.



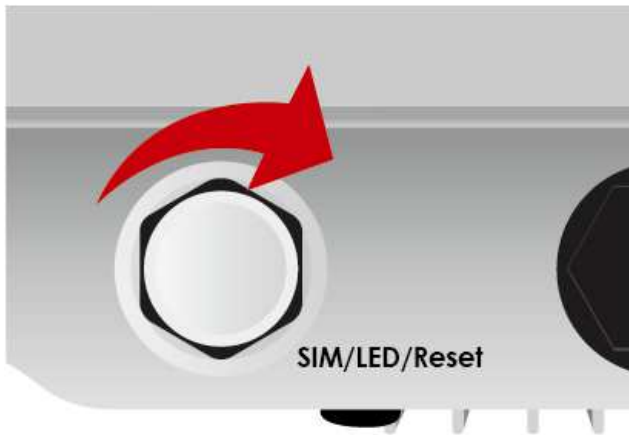
Step 2: Slide the SIM card with the metal contacts (gold plate) facing down to the SIM slot then push it all the way in until you hear the clicking sound.



It is recommended to use an industrial-grade SIM card.



Step 3: Screw the cap back tightly.



Please power off the device before inserting or removing the SIM card.

System Recovery Procedures

The purpose is to allow users to restore the BEC 4G/LTE ODU 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 BEC 4G/LTE ODU Device

- 2.1 Power off your BEC 4G/LTE ODU
- 2.2 Power on the BEC 4G/LTE ODU while pushing the RESET button with a small pointed object (such as paper clip, needle, toothpick, and etc.).
- 2.3 When the POWER LED turns RED, keep holding and pushing the RESET button for more 6 seconds then release it. The INTERNET LED will flash in GREEN afterward.

Step 3 – Restore your BEC 4G/LTE ODU Device

With INTERNET light flashes green, the BEC 4G/LTE ODU 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, your BEC 4G/LTE ODU will not respond to any PING or other requests.
- 3.2 Browse to the new Firmware image file then click Upload to start the upgrade process.
- 3.3 INTERNET LED turns red means the Firmware upgrade is in process.
DO NOT power off or reboot the device, it would permanently damage your BEC 4G/LTE ODU.
- 3.4 INTERNET LED turns green after the Firmware upgrade completed
- 3.5 Power cycle on & off to regain access to the BEC 4G/LTE ODU.

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 7 / 8 / 10, 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.

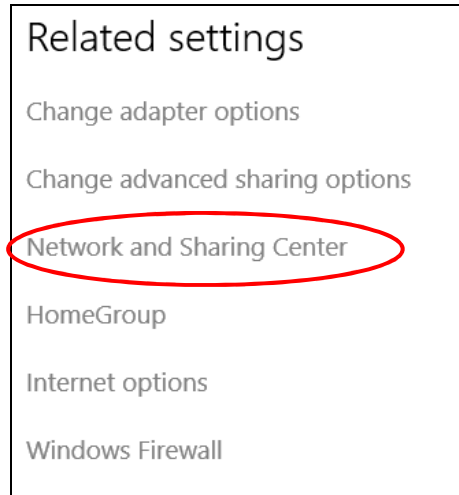


Any TCP/IP capable workstation can be used to communicate with or through the BEC 4G/LTE ODU. To configure other types of workstations, please consult the manufacturer's documentation.

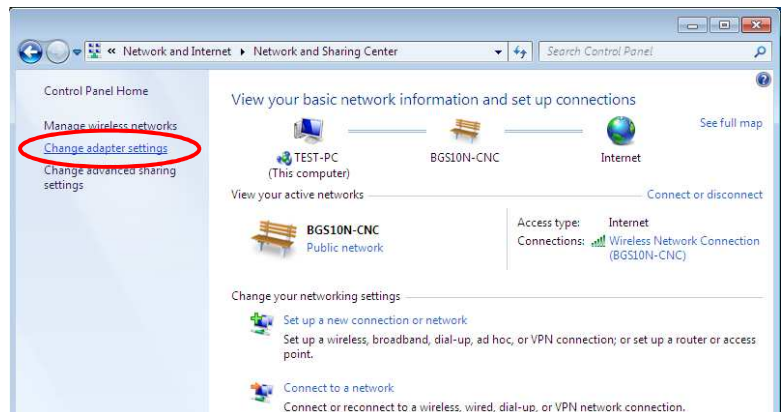
Network Configuration – IPv4

Configuring PC in Windows 10 (IPv4)

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

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



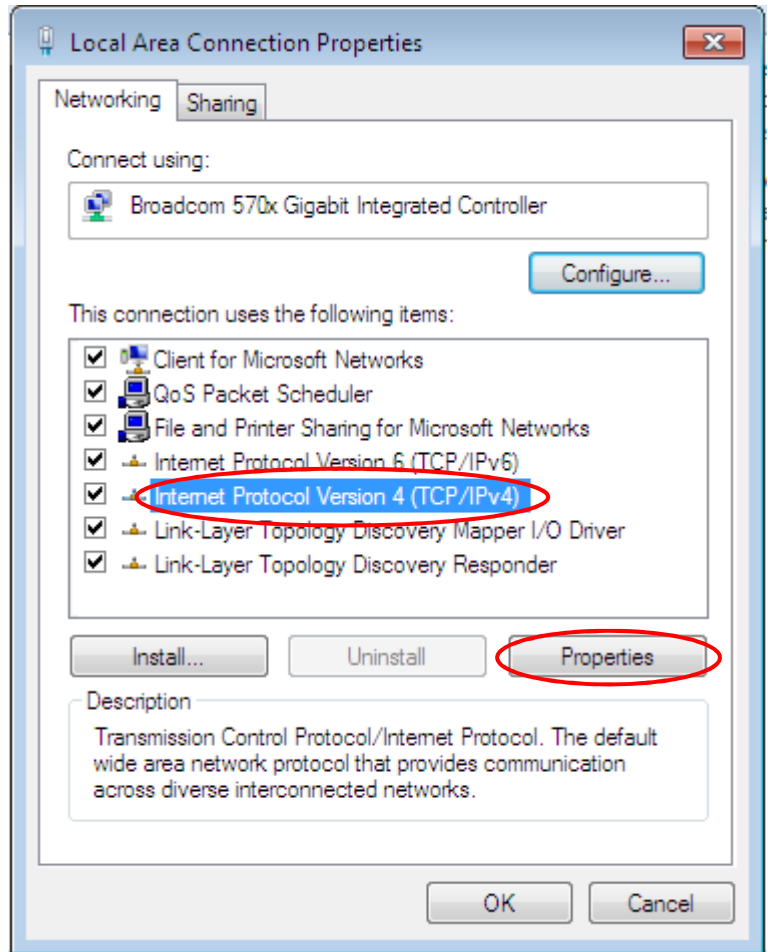
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

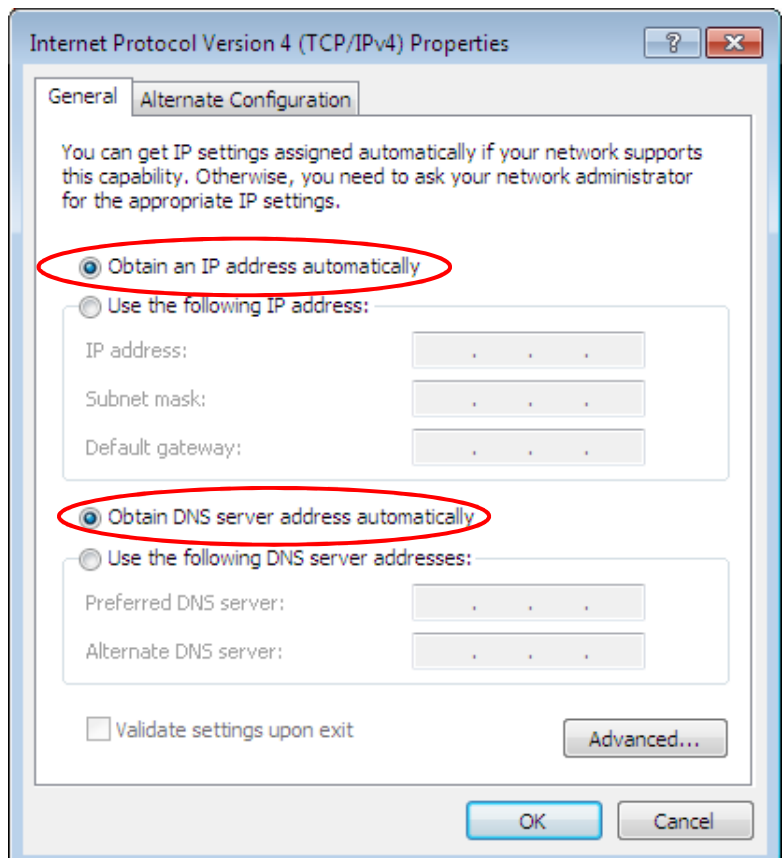


7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



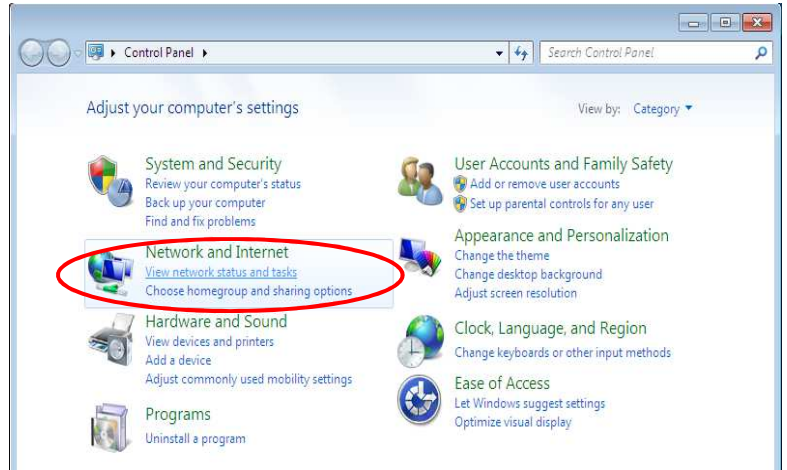
8. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

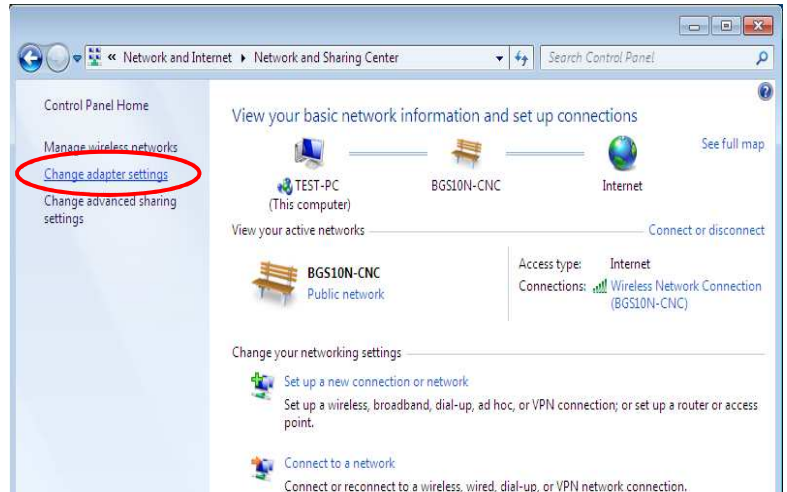


Configuring PC in Windows 7/8 (IPv4)

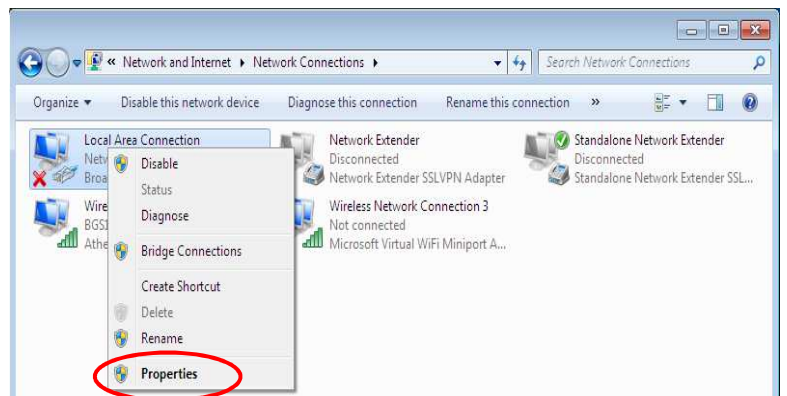
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



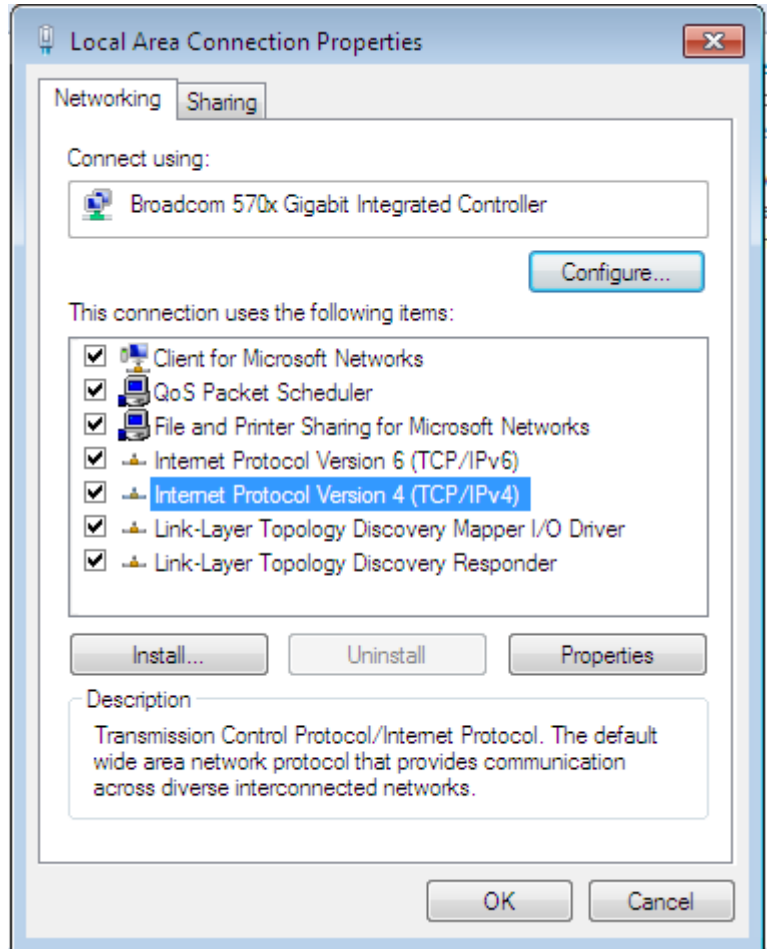
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



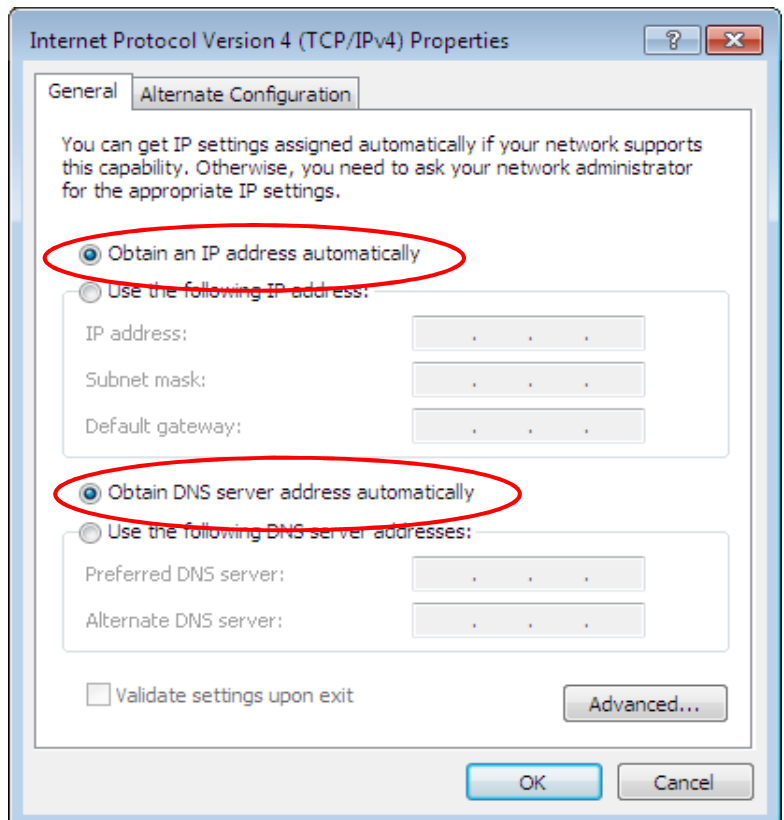
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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

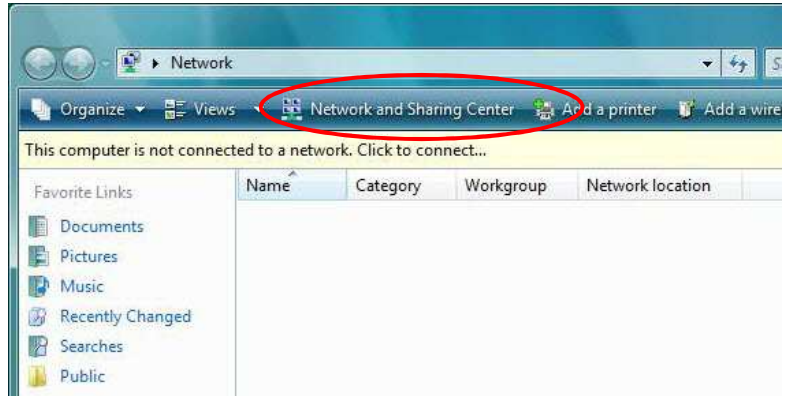


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

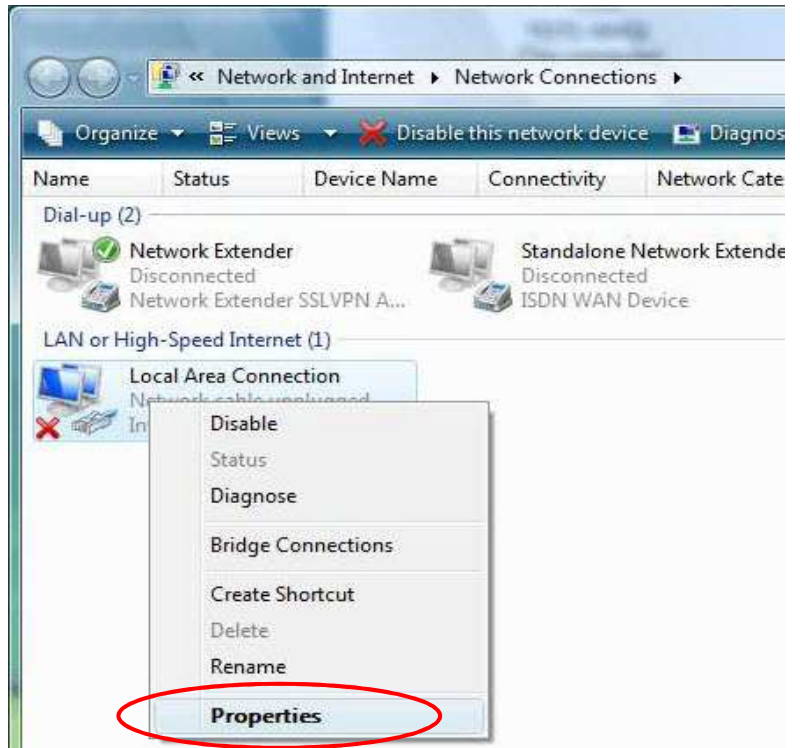
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



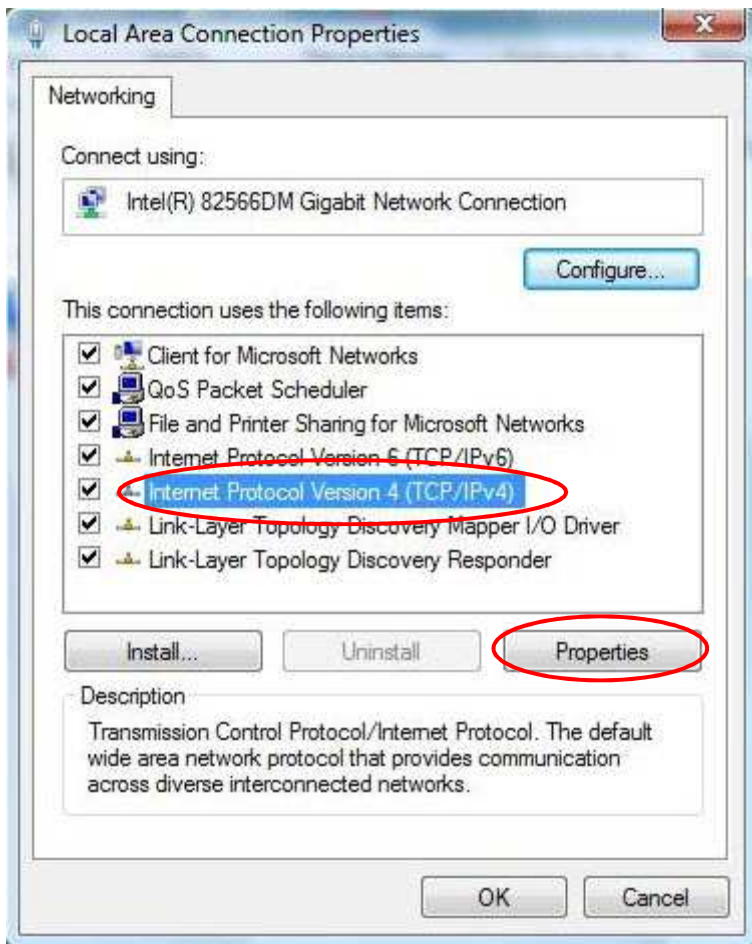
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left windowpane.



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

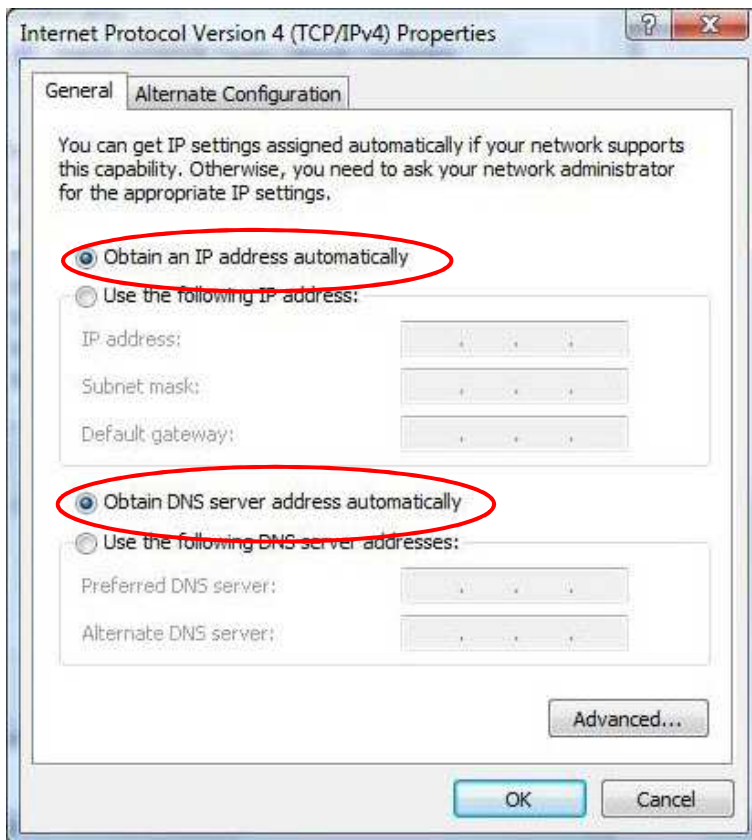


- 5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.






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

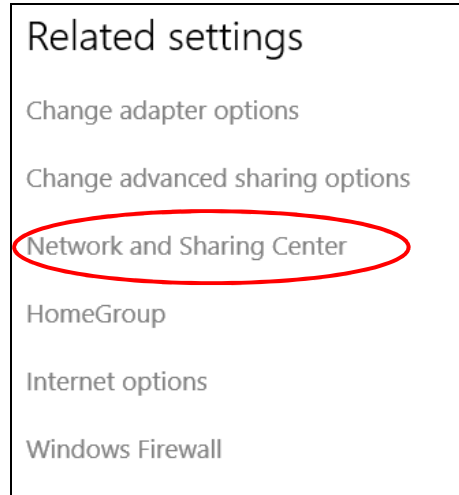
- 7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



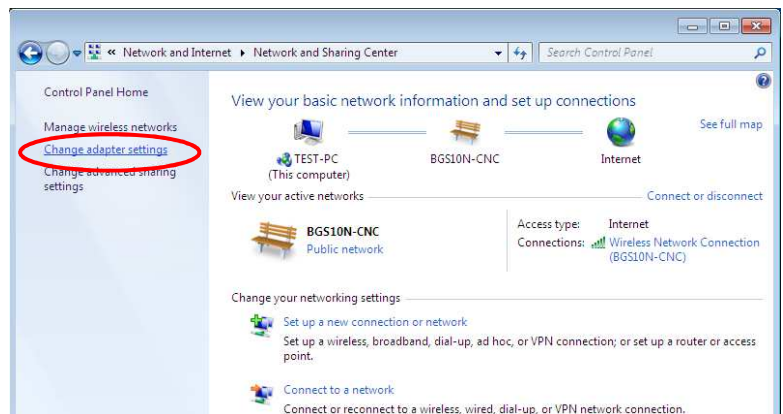
Network Configuration – IPv6

Configuring PC in Windows 10 (IPv6)

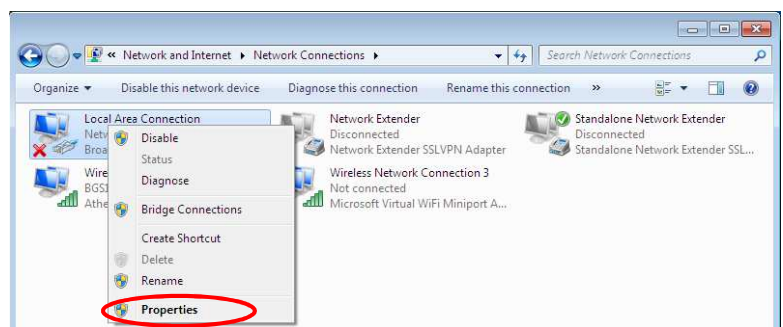
1. Click .
2. Click .
3. Then click on **Network and Internet**. 
4. Under **Related settings**, select **Network and Sharing Center**



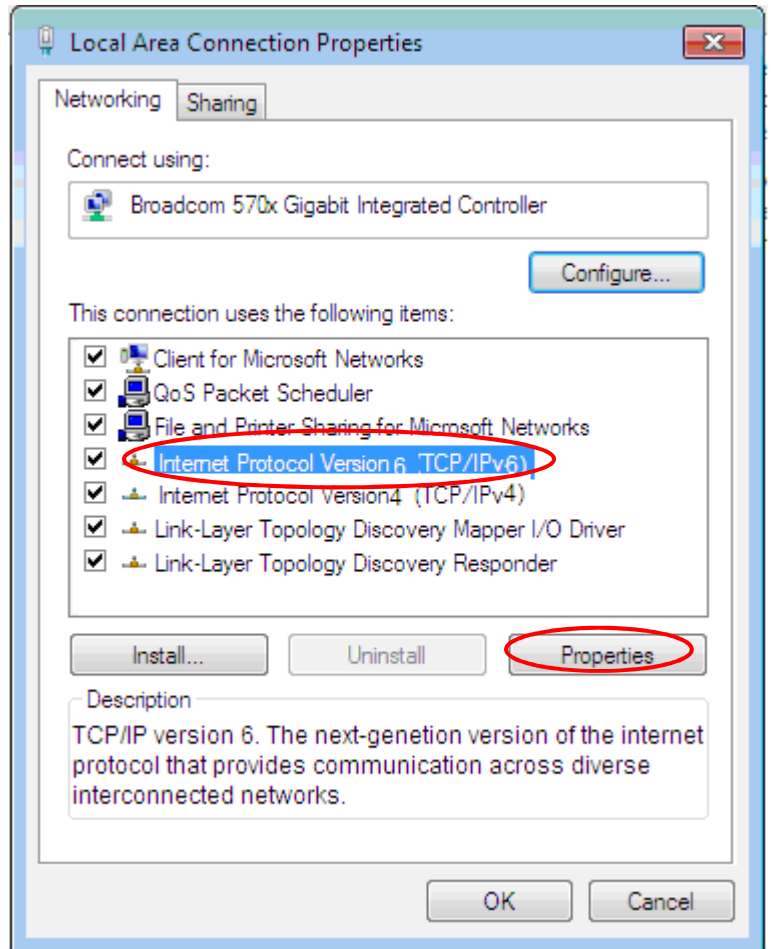
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

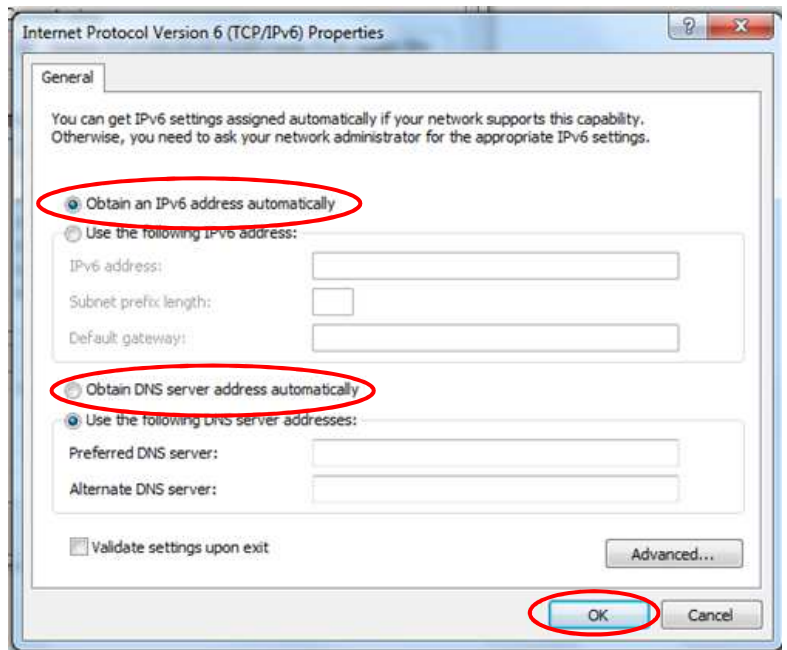


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



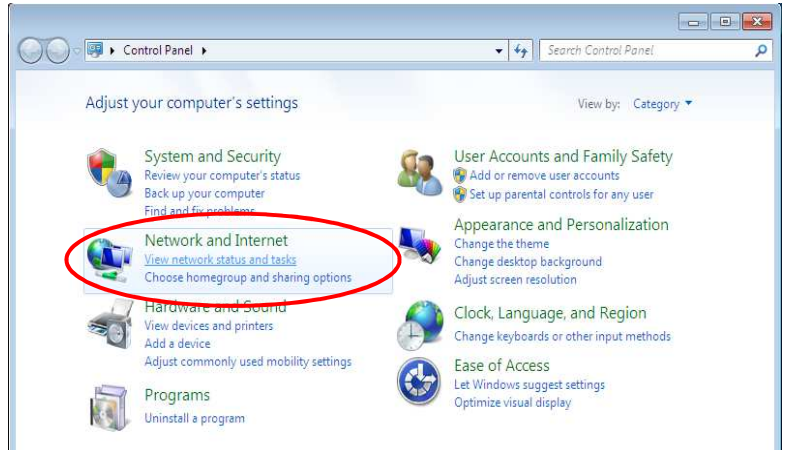
8. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

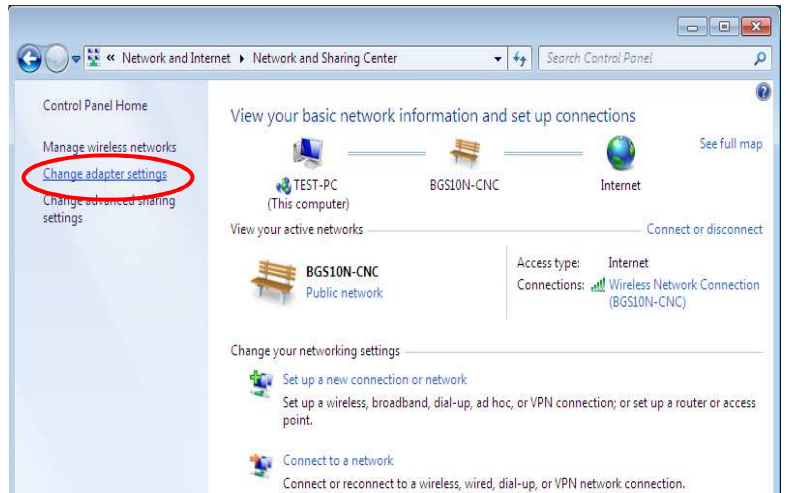


Configuring PC in Windows 7/8 (IPv6)

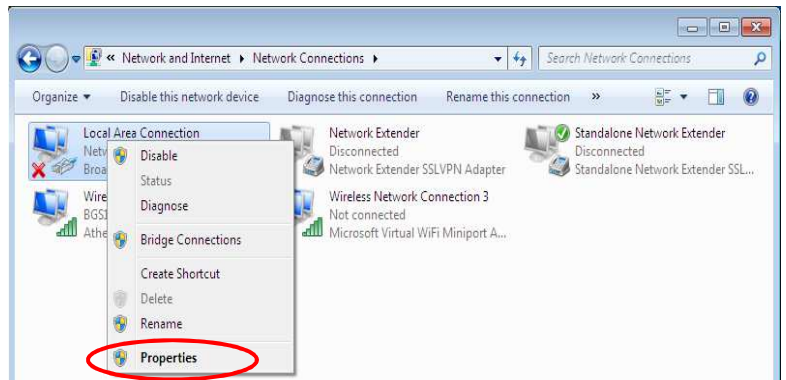
1. Go to **Start**. Click on **Control Panel**.
2. Then click on **Network and Internet**.



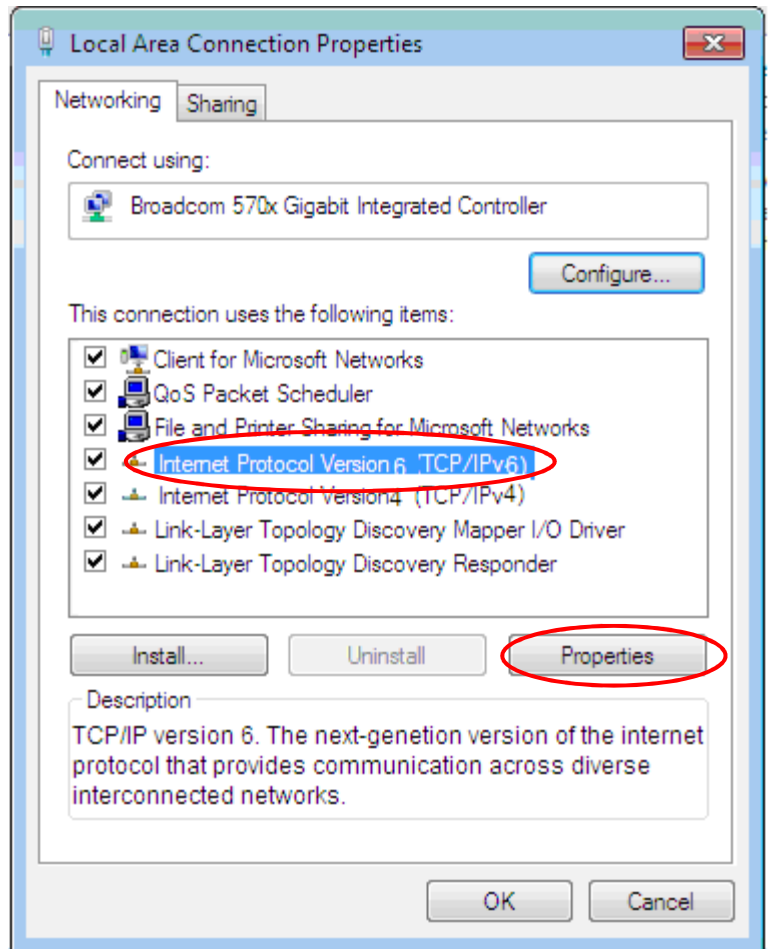
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

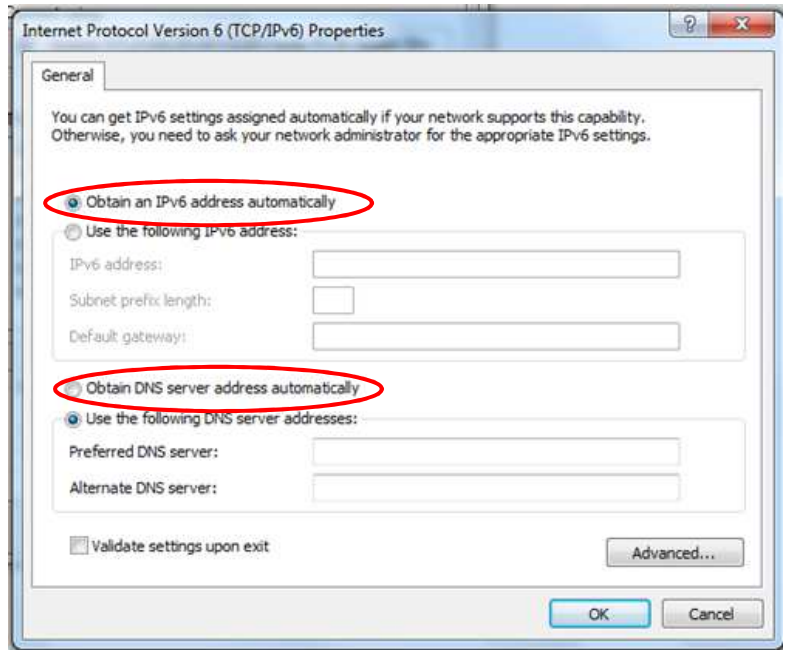


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



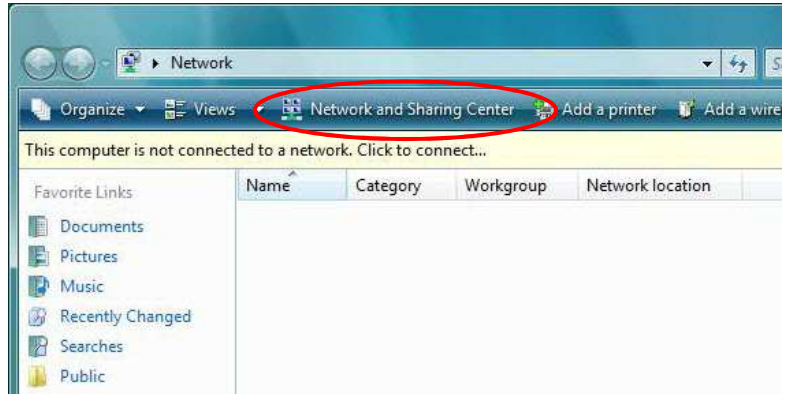
6. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



Configuring PC in Windows Vista (IPv6)

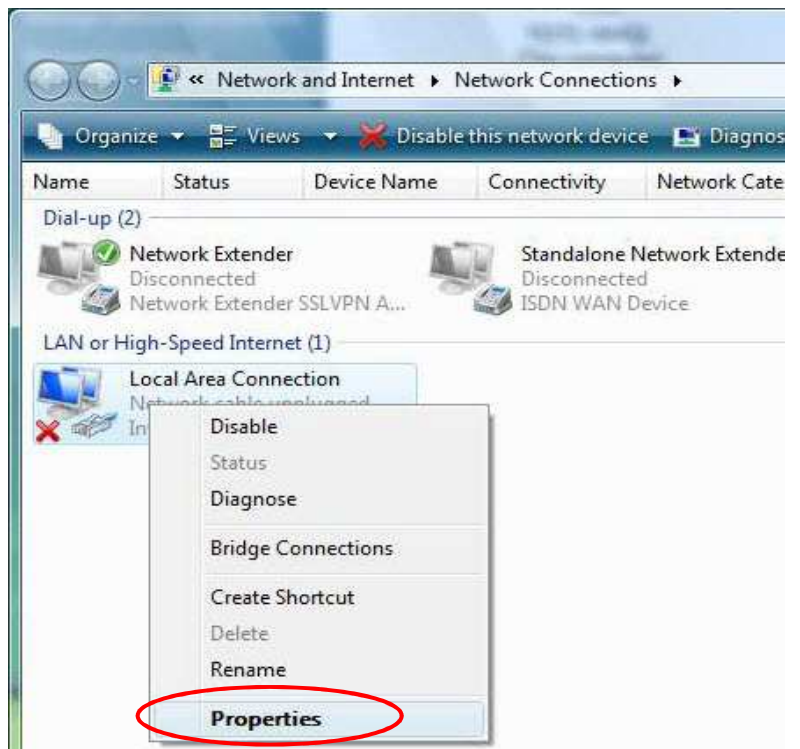
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



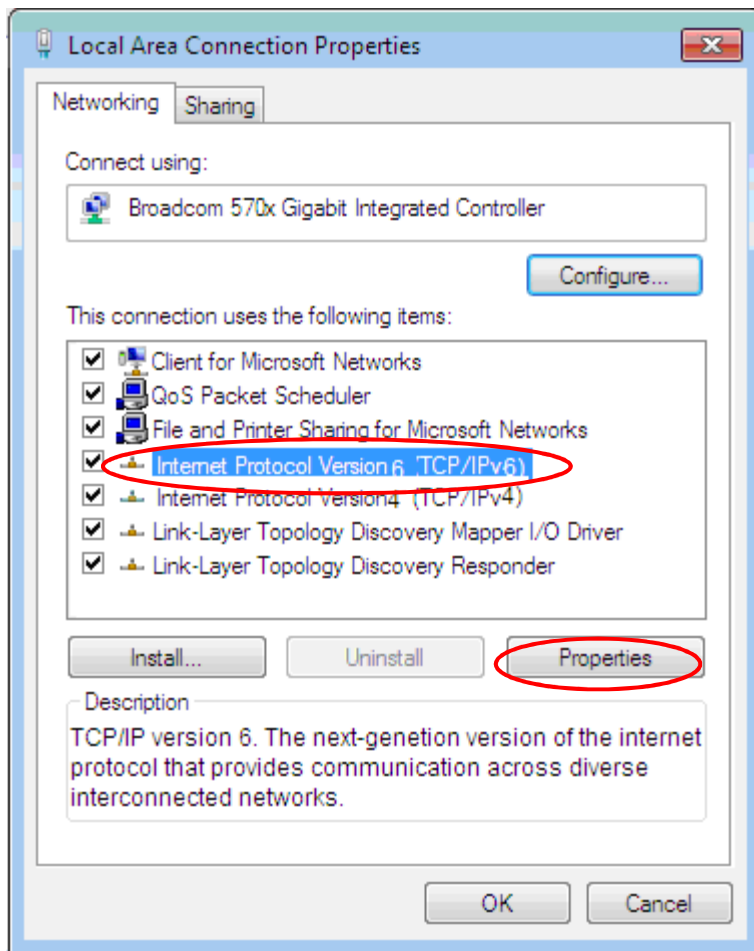
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left windowpane.



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

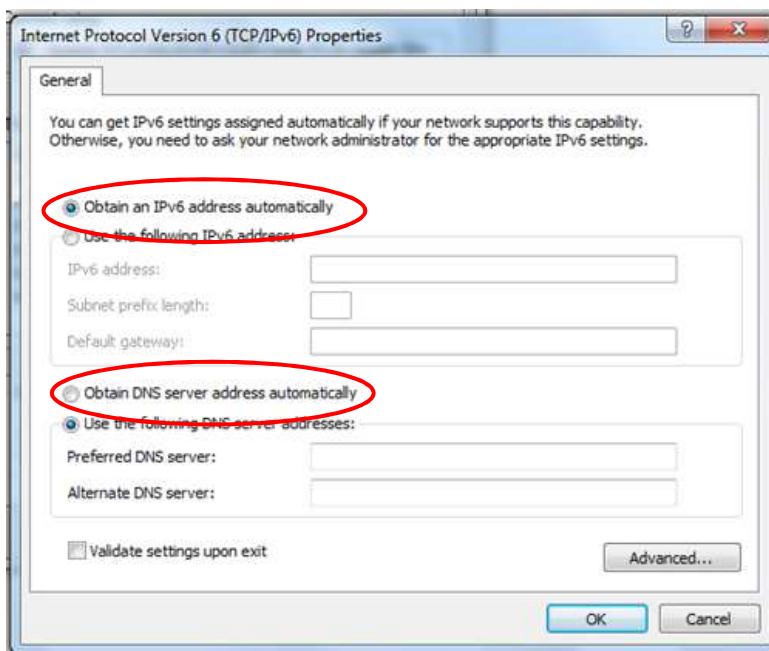


- 5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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

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



Default Settings

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

Web Interface: (Username and Password)

- ✓ 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

CHAPTER 4: DEVICE CONFIGURATION

Login to your Device

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

The default username and password are **“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 4G/LTE ODU

Once you have logged on to your BEC 4G/LTE ODU via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	Device Info		Interface Setup - Internet - LAN - Loopback
	System Status		
	System Log		Advanced Setup - Firewall - Routing - Dynamic Routing
	3G/4G-LTE Status		- NAT - VRRP - Static DNS
	Statistics		- QoS - Time Schedule - Mail Alert
	DHCP Table		Access Management - Device Management
	ARP Table		- SNMP - Syslog - Universal Plug & Play (UPnP)
	VRRP Status		- Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - BECentral Management
			Maintenance - User Management - Time Zone - Firmware & Configuration - System Restart - Auto Reboot - Diagnostic Tool

Please see the relevant sections of this manual for detailed instructions on how to configure your **BEC 4G/LTE ODU** router.

Status

In this section, you can check the router working status, including **Device Info**, **System Status**, **System Log**, **3G/4G-LTE Status**, **Statistics**, **DHCP Table**, **ARP Table** and **VRRP Table**

Device Info

It contains basic information of the device.

Device Information		Physical Port Status	
Model Name	RidgeWave 6900	3G/4G-LTE	✗
Firmware Version	1.04.1.146	Ethernet	✓
MAC Address	60:03:47:37:a8:d1		
Date-Time	Mon Apr 10 00:13:12 UTC 2017		
System Up Time	13 mins		

WAN				
Interface	Protocol	Connection	IP Address	Default Gateway
3G/4G-LTE	Dynamic IP	Not Connected	/	

LAN		
IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.5.254	255.255.255.0	Enable / 192.168.5.100~192.168.5.199 Enable / Stateless

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Data-Time: Setup correct time on the **BEC 4G/LTE ODU** with your PC. Check on [Time Zone](#) section for more configuration information.

System Uptime: Display how long the **BEC 4G/LTE ODU** has been powered on.

Physical Port Status

Physical Port Status : Display available connection interfaces, WAN (4G/LTE) and LAN, that are supported in the BEC 4G/LTE ODU.

WAN

Interface: List current available WAN connections.

Protocol: Display selected WAN connection protocol

Connection: The current connection status.

IP Address: WAN port IP address.

Default Gateway: The IP address of the default gateway.

LAN

IP Address: LAN port IPv4 address.

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

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

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

System Status

Display device CPU and memory usage information

System Status	
CPU	
Usage	1%
Memory	
Total	60520 kB
Free	32196 kB
Cached	9948 kB
<input type="button" value="Refresh"/>	

CPU

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

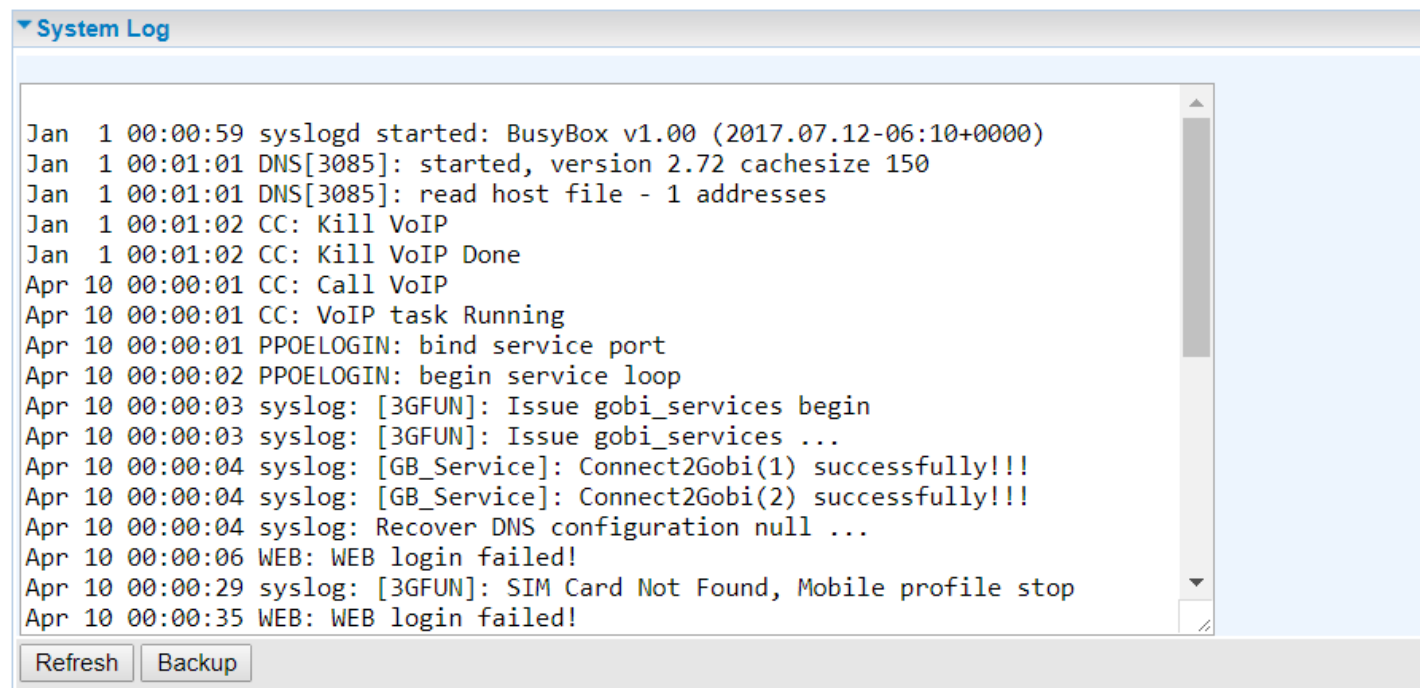
Memory

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

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

System Log

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



The screenshot displays a window titled "System Log" with a list of system events. The events are as follows:

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

At the bottom of the log window, there are two buttons: "Refresh" and "Backup".

Refresh: Press this button to refresh the statistics.

Backup: Press to save the System log, log.cfg, to your PC.

4G/LTE Status

This page contains 4G/LTE connection information.

4G/LTE Status	
Current SIM Slot in Use	SIM 1
Status	Down
SIM Status	SIM Card Not Found
Card Temperature	38°C
Signal Strength	
Network Name	
Cell ID	
Card IMEI	868323022552190
Card IMSI	ERROR
SIM Card Number (ICCID)	
Network Mode	
Network Band	
Auto Refresh	Disable ▼
<input type="button" value="Refresh"/> Neighbour Cell ▶	

Current SIM Slot in Use: Display which SIM slot is inserted with a SIM card.

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

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

Card Temperature: Display current operating temperature of the LTE module.

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

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

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

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

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

SIM Card Number (ICCID): It is a unique and specific serial number, consists of 19 or 20 characters, assigned to your SIM card.

Network Mode: Display current network operating mode.

Network Band: Indicated the current radio frequency band used.

Auto Refresh: Select **Disable** or **Enable** to reload the mobile status information.

Refresh: Click to refresh the statistics.

Neighbour Cell: Display lists of neighboring cell information in the area.

- ▶ **Index:** The numeric indicator of a cell tower.
- ▶ **Band:** Display the support operating LTE band

- ▶ **Earfcn (E-URTA Absolute Radio Frequency Channel Number):** Display the unique LTE band/carrier frequency.
- ▶ **PCI:** Display the Physical Cell ID (PCI) that the BEC 4G/LTE ODU is connected to for data service.
- ▶ **RSRQ (LTE signal parameters):** Reference Signal Receiving Quality measures the signal strength and is calculated based on both RSRP and RSSI.
- ▶ **RSSI (LTE signal parameters):** Received Signal Strength Indicator provides information about total received wide-band power (measure in all symbols) including all interference and thermal noise.

Usage Allowance

To enable this feature, please go to **Configuration >> Interface Setup >> Internet >> click “Usage Allowance” >> enable “Save the statistics to ROM”**

The screenshot shows a web-based configuration interface for 'Usage Allowance'. It features two main data rows: 'Amount used' with a progress bar and the text '0Hours of 720Hours', and 'Billing period' with a progress bar and the text 'Day:15'. At the bottom of the interface are two buttons: 'Clean' and 'Save'.

Amount Used: Display the amount of mobile data used and remaining in current billing cycle.

Billing Cycle: Display the start date and number of days remaining in current billing cycle.

Clean: Reset current saved mobile usage.

Save: Click to save current mobile status to ROM.

Statistics

❖ 4G/LTE Status

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

▼ Statistics			
Traffic Statistics			
Interface	<input checked="" type="radio"/> 3G/4G-LTE Status <input type="radio"/> EWAN(LAN2) <input type="radio"/> Ethernet		
Transmit Statistics		Receive Statistics	
Transmit Frames of Current Connection	0	Receive Frames of Current Connection	0
Transmit Bytes of Current Connection	0	Receive Bytes of Current Connection	0
Transmit Total Frames	0	Receive Total Frames	0
Transmit Total Bytes	0	Receive Total Bytes	0
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh <input type="text" value="None"/> ▼	

Traffic Statistics

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

Transmit Statistics

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

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

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

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

Transmit Speed: Display the data rate can be transferred to the server, the mobile Internet.

Receive Statistics

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

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

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

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

Receive Speed: Display the data rate receives from the mobile Internet.

Refresh: Click to manually refresh the data.

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

❖ Ethernet

Statistics			
Traffic Statistics			
Interface	<input type="radio"/> 3G/4G-LTE Status <input type="radio"/> EWAN(LAN2) <input checked="" type="radio"/> Ethernet		
Transmit Statistics		Receive Statistics	
Transmit Frames	1622	Receive Frames	693
Transmit Multicast Frames	1326	Receive Multicast Frame	432
Transmit Total Bytes	189066	Receive Total Bytes	118514
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh		Auto Refresh <input type="text" value="None"/>	

Traffic Statistics

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Traffic Speed

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

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

Refresh: Click to manually refresh the data.

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

DHCP Table

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

▼ DHCP Table				
Index	Host Name	IP	MAC Address	Expire Time
1	DESKTOP-PPUSERT	192.168.1.100	08:00:00:00:00:00	0days 22:29:22

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

Host Name: Display the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

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

ARP Table

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

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

#: The numeric table list indicator.

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

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

VRRP Status

▼ VRRP Status	
Current Status	N/A
Current Master	N/A

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

Current Master: Display the IP address of the Master

Quick Start

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

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.

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

Quick Start

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

Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your internet connection

Step 4. Confirm the configuration and save it

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 - Password

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

New Password

Confirm Password

Step 2 – Time Zone

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

Quick Start - Time Zone

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

Time Zone

Step 3 – ISP Connection Type

Set up your 4G/LTE Internet connection.

▼ Quick Start - ISP Connection Type

Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.

WAN Interface

Click **NEXT** to continue.

Input all relevant 3G/4G/LTE parameters from your cellular provider then click **Next** to continue.

▼ Quick Start - 4G/LTE

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

TEL No.

APN

PDN Type IPv4 IPv4/IPv6 IPv6

Authentication Protocol

Username

Password

PIN

Keep Alive Yes No

MTU (0 means use default:1500)

Step 4 – Quick Start Completed

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

▼ Quick Start - Quick Start Completed

Quick Start Completed !!

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

▼ Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

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

Configuration

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

These functions are described in the following sections.

Interface Setup

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

Internet

❖ 4G/LTE

WAN Interface: List all available WAN interfaces. (In this section, you have selected to use 4G/LTE)

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

LTE Settings

LTE Settings	
Usage Allowance ▶	<input type="checkbox"/> Enable
IP Pass-Through Mode	<input type="checkbox"/> Enable
LTE Antenna Diversity	Enabled
LTE PCI Lock	<input type="checkbox"/> Enable Earfcn <input type="text" value="0"/> Physical Cell ID <input type="text" value="0"/>
Network Mode	Automatic ▼
PLMN Selection	Operator Numeric <input type="text"/> RAT <input type="text"/> <input type="button" value="Scan"/>
TEL No.	<input type="text" value="*99***1#"/>
Dual APN	Single APN ▼

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

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

Period: Pick a period, **Month** or **Day**.

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

- ▶ **Volume-based** include “only Download”, “only Upload”, and “Download and Upload” to limit the flow.
- ▶ **Time-based** control the flow by providing specific hours per month.
 - **720 hours** if selected period **Month**
 - **12 hours** if selected period **Day**

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

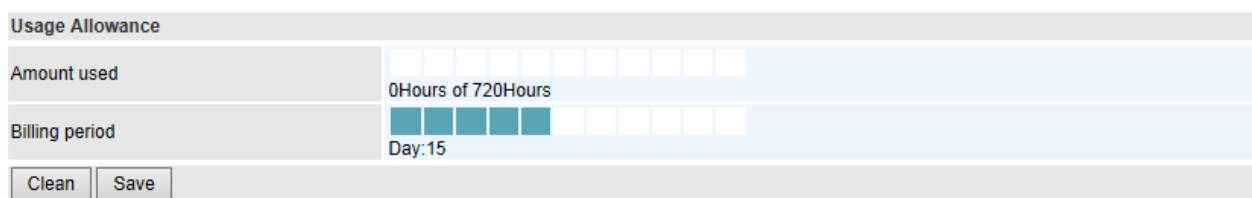
Over usage allowance action: Here are actions to perform when mobile data usage, defined in **Mode**, reached to its maximum.

- ▶ **None:** No action taken
- ▶ **Disconnect:** Disconnect mobile connection
- ▶ **Email Alert:** Send an e-mail alert and keep the mobile connection alive.
- ▶ **Email Alert and Disconnect:** Disconnect mobile connection after an alert e-mail is being sent.

Save the statistics to ROM:

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

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



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

- ▶ **Disable:** No action taken

LTE PCI Lock: Enable to force the BEC 4G/LTE ODU to connect with the specific **Earfcn** and **Physical Cell ID**.

Network Mode: Select a cellular mode. Select **Automatic** to auto detect the best mode for you.

LTE Band: Display a list of available LTE bands to choose from.

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

Dual APN: BEC 4G/LTE ODU can support up to two (2) APNs. Select **Single** or **Dual**.

APN: An APN is like a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider can 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.

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

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

Connection	
Connection	<input checked="" type="radio"/> Always On (Recommended)
Keep Alive	<input type="radio"/> Yes <input checked="" type="radio"/> No
Keep Alive IP	<input type="text"/> Check Interval 5 x <input type="text" value="1"/> Seconds
Background Ping	<input type="radio"/> Yes <input checked="" type="radio"/> No
Background Ping IP	<input type="text"/> Interval <input type="text"/> Seconds
Default Route	<input checked="" type="radio"/> Yes <input type="radio"/> No
NAT	Enable ▾
MTU	<input type="text" value="1428"/> (0 means use default:1500)

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

Keep Alive: Select **Yes** to ensure the 4G/LTE internet connection is always available.

- ▶ **Keep Alive IP:** Manually enter the Keep Alive IP Address to be used for ping operation to check if the connection is still on.
- ▶ **Check Interval 5 x ___ Seconds:** Default is set to 1 (5 seconds). Setup a timer to ping the keep alive IP.

Background Ping: Select **Yes** to keep the 4G/LTE active at all time, prevent BEC 4G/LTE ODU from entering idle state.

Background Ping IP: Enter the IP address that the BEC 4G/LTE ODU can ping the IP address.

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.

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

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface. **0** means to use default MTU size, 1500byte.

Click **Save** to apply settings.

LAN

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

LAN

IPv4 Parameters

IP Address: 192.168.1.254

IP Subnet Mask: 255.255.255.0

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

Alias IP Subnet Mask: 0.0.0.0

Snooping: Activated Deactivated

Dynamic Route: RIP1 Direction: None

DHCPv4 Server

DHCPv4 Server: Disabled Enabled Relay

Start IP: 192.168.1.100

IP Pool Count: 100

Lease Time: 86400 seconds (0 sets to default value of 259200)

DNS Relay: Automatically Manually

Primary DNS:

Secondary DNS:

Option 66:

Option 160:

Fixed Host

IP Address:

MAC Address:

IPv6 Parameters

Interface Address/Prefix Length: /

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

Save

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: Select the RIP version from RIP1 or RIP2.

DHCPv4 Server

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

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

DHCPv4 Server: If set to **Enabled**, your BEC 4G/LTE ODU 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 4G/LTE ODU acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- ▶ When DHCP is used, the following items need to be set.

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

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

Lease Time: The current lease time of client.

DNS Relay Select **Automatically** obtained or **Manually** set. If select **Manually**, please enter DNS IP addresses here.

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

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

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

Fixed Host

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

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

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

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

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

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

IPv6 parameters

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

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

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

DHCPv6 Server

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

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

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

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

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

DHCPv6 Server: Check whether to enable DHCPv6 server.

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

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

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

End interface ID: enter the end interface ID.

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

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

Click **Save** to apply settings.

Loopback

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

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

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

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

Click **Save** to apply settings.

Advanced Setup

Advanced configuration features provide advanced features, including [Firewall](#), [Routing](#), [Dynamic Routing](#), [NAT](#), [VRRP](#), [Static DNS](#), [QoS](#), [Time Schedule](#) and [Mail Alert](#) for advanced users.

Firewall

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

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

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.

Click **Save** to apply settings.

Routing

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

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

Add Route

Index #: The numeric route indicator.

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

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

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

Interface: Media/channel selected to append the route.

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

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

Add Route

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

Save Back

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

Destination Subnet Mask: The subnet mask of destination network.

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

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

Click **Save** to add this route

Dynamic Routing

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

Open Shortest Path First (OSPF)

▼ OSPF

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

Save Delete

OSPF Listing

Index	Interface	Area ID

OSPF: Enable to activate OSPF routing.

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

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

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

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

Click **Save** to apply the settings.

Border Gateway Protocol (BGP)

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

▼ BGP

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

BGP Listing

Index	Neighbor IP	Neighbor As Number	Allowas-in

BGP: Enable to activate BGP routing.

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

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

Neighbor IP: Enter the neighbor IP address.

Neighbor AS Number: Enter the neighbor AS number.

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

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

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 type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ / Virtual Server	
Interface	4G/LTE ▼
DMZ	▶ Edit
Virtual Server	▶ Edit

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

ALG

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

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

DMZ / Virtual Server

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

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

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

❖ DMZ

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

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

DMZ

DMZ for: Single IPs Account/ EWAN(LAN1)

DMZ: Enabled Disabled

DMZ Host IP Address:

Except Ports

Port:

Protocol:

Description:

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

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

DMZ:

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

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

Click **Save** to apply settings

Except Ports

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

Port: Enter port to be monitored.

Protocol: Enter the protocol to be monitored.

Description: Enter a description to this rule.

Example: Skip port 80 (UDP/TCP) in the list. All Incoming request to access to port 80 (Web GUI) will be forwarded to the embedded HTTP server of BEC 4G/LTE ODU instead of the DMZ host.

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

❖ Virtual Server

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

Virtual Server is also known as Port Forwarding that allows BEC 4G/LTE ODU to direct incoming traffic to a specific device in the network.

Configure a virtual rule in BEC 4G/LTE ODU for remote users accessing services such as Web or FTP services via the public (WAN) IP address that can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Virtual Server

Virtual Server for	4G/LTE
Protocol	TCP
Start Port Number	21
End Port Number	21
Local IP Address	192.168.1.110
Start Port Number (Local)	21
End Port Number(Local)	21

Save Back

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

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

Protocol: Choose the application protocol.

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

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

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

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

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

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

Well-known and Registered Ports

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



Attention

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

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

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

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

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

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

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

FTP server uses TCP protocol with port 21.

Enter “21” to Start and End Port Number. The BEC 4G/LTE ODU will accept port 21 requests from WAN side.

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

Enter “21” to Local Start and End Port number. The BEC 4G/LTE ODU will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.102) in the network.

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

Virtual Server

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

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

VRRP

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

VRRP	
VRRP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
VRID	<input type="text" value="1"/> (1~255)
Priority	<input type="text" value="100"/> (1~254)
Preempt Mode	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
VRIP	<input type="text" value="192.168.1.253"/>
Advertisement Period	<input type="text" value="1"/> (1~2147483647)
<input type="button" value="Save"/>	

VRRP: Click to activate the feature.

VRID: Virtual Router Identifier, range from 1-255 (decimal). A master or backup router running the VRRP protocol may participate in one VRID instance.

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

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

VRIP: An IP address which is associated with the virtual router.

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

Click **Save** to apply settings.

Static DNS

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

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

Static DNS

IP Address

Domain Name

Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete

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

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

Click **Save** to apply settings.

QoS

QoS helps you control the upload traffic of each application from LAN (Ethernet) to WAN (Internet). It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want give higher priority to, such as voice data packets given higher priority than web data packets.

Quality of Service

SW QoS Activated Deactivated

Bandwidth

LAN to WAN Bandwidth Kbps

WAN to LAN
 EWAN(LAN2) Bandwidth Kbps
 4G/LTE Bandwidth Kbps

Rule Index Wan Interfae Application

Direction Protocol DSCP Marking

Rate Type Rate Kbps Priority

Internal IP Address ~ * Internal Port ~ **

External IP Address ~ * External Port ~ **

Note * : 0.0.0.0 ~ 0.0.0.0 means all IPs
 Note * : 0 ~ 0 means all Ports

QOS Control Listing

Index	Application	Direction	Rate Type	Rate	Wan Interface
-------	-------------	-----------	-----------	------	---------------

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

LAN to WAN (Bandwidth): You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.

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

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

Click **Bandwidth Save** to save settings.

LAN Host Bandwidth:

LAN Host Bandwidth

Rule Index

MAC Address

Upload Mbps Download Mbps

LAN Host Bandwidth Listing

Index	MAC Address	Upload Bandwidth	Download Bandwidth
-------	-------------	------------------	--------------------

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

- ▶ **WAN Interface:** Select a WAN interface connection to allow external access to your internal network.
- ▶ **Application:** Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Select the direction mode of the QoS application

- ▶ **Protocol:** Select a protocol from the drop-down list
- ▶ **DSCP Marking:** Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

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

- ▶ **Rate:** Specify the data rate in Kbps.
- ▶ **Priority:** Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

- ▶ **Internal Port:** The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

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

Click **Save** to apply settings.

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

Time Schedule

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

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

Time Schedule							
Rule Index	1 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Save							

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

Name: User-defined identification for each time period.

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

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

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

Click **Save** to apply your settings.

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

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

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

Mail Alert

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

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

Server Information

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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

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

Port: the port, default is 25.

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

WAN IP Change Alert

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

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

Click **Apply** button to save settings.

Access Management

Access Management provides advanced users / administrators to grant accessibilities to authorized users or service systems. Features including [Device Management](#), [SNMP](#), [Syslog](#), [Universal Plug & Play](#), [Dynamic DNS](#), [Access Control](#), [Packet Filter](#), [CWMP \(TR-069\)](#), [Parental Control](#) and [BECentral Management](#).

Device Management

Device Management		
Device Host Name		
Host Name	<input type="text" value="home.gateway"/>	
<input type="button" value="Save"/>		
Embedded Web Server		
HTTP Port	<input type="text" value="80"/>	(The default HTTP port number is 80.)
HTTPS Port	<input type="text" value="443"/>	(The default HTTPS port number is 443.)
HTTPS Server Certificate Index	<input type="text" value="Default"/>	
<input type="button" value="Save"/>		

Device Host Name

Host Name: Enter the host name of the router. Default is **home.gateway**

Embedded Web Server

HTTP Port: It is the embedded web server (Web GUI) accessing port, default is **80**. It can be changed other port other than port 80, e.g. port **8080**.

HTTPS Port: Similar to HTTP which is an unencrypted communication using port 80. HTTPS is encrypted by SSL using port 443 instead.

Click **Save** to apply settings.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. The BEC 4G/LTE ODU serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.

SNMP	
SNMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Get Community	<input type="text"/>
Set Community	<input type="text"/>
Trap Manager IP	<input type="text" value="0.0.0.0"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Interface	<input type="text" value="ALL"/>
SNMPv3	
SNMPv3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Access Permissions	<input type="text" value="Read Only"/>
Authentication Protocol	<input type="text" value="MD5"/>
Authentication Key	<input type="text"/> (8~31 characters)
Privacy Protocol	<input type="text" value="DES"/>
Privacy Key	<input type="text"/> (8~31 characters)
<input type="button" value="Save"/>	

SNMP: Activate to enable SNMP.

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

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

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

System Name / Location / Contact: String descriptions of the SNMP agent.

Interface: Select the access interface. Choices are **LAN** or **ALL** (Both LAN and WAN).

SNMPv3

SNMPv3: Enable to activate the SNMPv3.

Username: Enter the name allowed to access the SNMP agent.

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

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

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

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

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

Click **Save** to apply settings.

Syslog

Use the Syslog to collect system event information to a remote log server.

▼ Syslog	
Remote System Log	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Server IP Address	<input type="text" value="0.0.0.0"/>
Server UDP Port	<input type="text" value="514"/>
<input type="button" value="Save"/>	

Remote System Log: Select **Activated** to enable this feature

Server IP Address: Assign the remote log server IP address.

Server UDP Port: Assign the remote log server port, 514 is commonly used.

Click **Save** to apply settings.

Universal Plug & Play

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

Both the user's Operating System and the relevant application must support UPnP in addition to the router.

Universal Plug & Play	
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)
<input type="button" value="Save"/>	

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration's login screen without entering the BEC 4G/LTE ODU's IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BEC 4G/LTE ODU so that they can communicate through the BEC 4G/LTE ODU, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Click **Save** to apply settings.

Dynamic DNS (DDNS)

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

Here users can register different WAN interfaces with different DNS Providers.

If you do not have a DDNS account, please choose a DDNS Service Provider from the list then go to their website to create an account first.

Dynamic DNS	
Dynamic DNS	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 <input type="text"/> Day(s) ▼
<input type="button" value="Save"/>	

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

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

My Host Name: Type the domain name assigned to your BEC 4G/LTE ODU by your Dynamic DNS provider.

Username / Password: Enter the username and password of the account you created with this service provider.

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

Period: Set the time period on how often the BEC 4G/LTE ODU will update the DDNS server with your current external IP address.

Example: How to register a DDNS account

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

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

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

Dynamic DNS	
Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	myhome.dyndns.org
Username	myhome-123
Password	*****
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼
<input type="button" value="Save"/>	

Access Control

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

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

Rule Index: The numeric rule indicator.

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

Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BEC 4G/LTE ODU. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the commonly used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **ALL**.

Click **Save** to apply settings.

By default, the “Access Control” has **two default rules**.

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

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 1

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application: ALL

Interface: LAN

Save Delete

Access Control Listing

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

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

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 1

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application: ALL

Interface: LAN

Save Delete

Access Control Listing

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

Packet Filter

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

❖ Packet Filter - IP & MAC Filter

Packet Filter

Filter Type: IP & MAC Filter ▼

IP & MAC Filter Editing

Action: Black List ▼

Rule Index: 1 ▼

Individual Active: Yes No

Interface: 4G/LTE ▼

Direction: Both ▼

Type: IPv4 ▼

Source IP Address: 0.0.0.0 (0.0.0.0 means Don't care)

Source Subnet Mask: 0.0.0.0

Source Port Number: 0 (0 means Don't care)

Destination IP Address: 0.0.0.0 (0.0.0.0 means Don't care)

Destination Subnet Mask: 0.0.0.0

Destination Port Number: 0 (0 means Don't care)

DSCP: 64 (Value Range:0-64, 64 means Don't care)

Protocol: Any ▼

Time Schedule: Always ▼

Save Delete

IP & MAC Filter List

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

IP & MAC Filter Editing

Rule Index: The numeric rule indicator.

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

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

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

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

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

► **IPv4**

Source IP Address	<input type="text" value="0.0.0.0"/>	<small>(0.0.0.0 means Don't care)</small>
Source Subnet Mask	<input type="text" value="0.0.0.0"/>	
Source Port Number	<input type="text" value="0"/>	<small>(0 means Don't care)</small>
Destination IP Address	<input type="text" value="0.0.0.0"/>	<small>(0.0.0.0 means Don't care)</small>
Destination Subnet Mask	<input type="text" value="0.0.0.0"/>	
Destination Port Number	<input type="text" value="0"/>	<small>(0 means Don't care)</small>
DSCP	<input type="text" value="0"/>	<small>(Value Range:0~64, 64 means Don't care)</small>
Protocol	<input type="text" value="TCP"/> ▼	

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

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

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

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

Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (E.g. HTTP is port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

► **IPv6**

Source IPv6 Address	<input type="text" value="0:0:0:0:0:0:0:0"/>	<small>(0:0:0:0:0:0:0:0 means Don't care)</small>
Source IPv6 Prefix	<input type="text" value="32"/>	
Source Port Number	<input type="text" value="0"/>	<small>(0 means Don't care)</small>
Destination IPv6 Address	<input type="text" value="0:0:0:0:0:0:0:0"/>	<small>(0:0:0:0:0:0:0:0 means Don't care)</small>
Destination IPv6 Prefix	<input type="text" value="32"/>	
Destination Port Number	<input type="text" value="0"/>	<small>(0 means Don't care)</small>
DSCP	<input type="text" value="0"/>	<small>(Value Range:0~64, 64 means Don't care)</small>
Protocol	<input type="text" value="TCP"/> ▼	

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

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

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

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

DSCP: show the set DSCP.

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

ICMP or ICMPv6

▶ MAC

Type	MAC ▼
Source MAC Address	<input type="text"/>

Source MAC Address: show the MAC address of the rule applied.

Time Schedule: Select a TimeSlot to activate the rule. Go to [Time Schedule](#) to configure a time control first.

Click **Save** to apply settings.

❖ Filter Type- URL Filter

Packet Filter	
Packet Filter	
Filter Type	URL Filter ▼
URL Filter Editing	
URL Filter Rule Index	1 ▼
Individual Active	<input type="radio"/> Yes <input checked="" type="radio"/> No
URL (Host)	<input type="text"/>
Time Schedule	Always ▼
<input type="button" value="Save"/> <input type="button" value="Delete"/>	
URL Filter Listing	
Index	Active
	URL

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

URL Filter Rule Index: The numeric rule indicator.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

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

Time Schedule: Select a TimeSlot to activate the rule. Go to [Time Schedule](#) to configure a time control first.

Click **Save** to apply settings.

CWMP (TR-069)

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

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

CWMP (TR-069)	
CWMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ACS Login Information	
URL	<input type="text" value="http://cpe.bectechnologies.com/comserver/node1/tr069"/>
Username	<input type="text" value="testcpe"/>
Password	<input type="text" value="ac5entry"/>
Connection Request Information	
Path	<input type="text"/>
Username	<input type="text" value="conexant"/>
Password	<input type="text" value="welcome"/>
Periodic Inform Config	
Periodic Inform	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Interval	<input type="text" value="870"/>
Bind Wan Interface	
Interface	<input type="text" value="Auto"/>
NATT Config	
NATT Server	<input type="text"/>
NATT Period	<input type="text"/>
<input type="button" value="Save"/>	

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

Username: Specify the ACS Username for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

Periodic Inform Config

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

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Bind WAN Interface

Interface: Specify any available or a single WAN interface to handle TR-069 requests.

NATT Config - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

NATT Server: By BEC administrator only.

NATT Period: By BEC administrator only.

Click **Save** to apply settings.

Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.

Parental Control	
Provider	www.opendns.com
Parental Control	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
**Parental Control provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.	
<input type="button" value="Save"/>	

To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Parent Control: Enable the feature by clicking the **Activated**

Host Name: It is the domain name of your OpenDNS. If you don't have one, please leave it blank.

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply settings.

BECentral Management

BECentral is a cloud-based device management platform that provides operators with a comprehensive suite of services to manage devices in real-time.

▼ BECentral Management	
BECentral Management	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
BECentral Management URL	<input type="text" value="becentral.becloud.io"/>
BECentral Management Port	<input type="text" value="48883"/>
Organization ID	<input type="text" value="DEFAULT"/>
Tag ID	<input type="text"/>
Device Report Interval	<input type="text" value="480"/>
Interface	<input type="text" value="ALL"/> ▼
<input type="button" value="Save"/>	

BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral.

BECentral Management Port: Port listened by the BECentral.

Organization ID: Customer ID (By BE C administrator only)

Tag ID: By BEC administrator only.

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

Interface: Specify any available or a single WAN interface to handle BECentral requests.

Click **Save** to apply settings.

Maintenance

Maintenance equips the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including [User Management](#), [Time Zone](#), [Firmware & Configuration](#), [System Restart](#), [Auto Reboot](#) and [Diagnostic Tool](#).

User Management

User Management provides the Administrator with the ability to grant access control and manage GUI login credentials for each user.

There are two access management levels, Administrator and User.

The default root account, Administrator (admin), has full access to all the features listed and ability to create other accounts with features to allow other users to access to. The User account is with limited access (specified by advanced users with admin account) to the GUI.

Total of **8** accounts can be created to grant access to manage the BEC 4G/LTE ODU via the web page.

❖ Administrator Account

admin/admin is the root/default account username and password.

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

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

The Administrator account cannot be deleted or removed.

▼ User Management

User Account

Index	1 ▼
Username	admin
New Password
Confirm Password

Save Delete

User Account Listing

Index	User Name
1	admin

Index: The numeric account indicator. The maximum entry is up to 8 accounts.

Username: Create account(s) username for GUI management.

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

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

❖ **Creating Other User Accounts**

User Management	
User Account	
Index	2 ▼
Username	user
New Password
Confirm Password
Web GUI Permission	
Guest Account	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Interface Setup	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Advanced Setup	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN Setup	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Access Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Maintenance	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Delete"/>	

User Account Setup

Index #: The numeric account indicator. The maximum entry is up to 7.

Username: Create account(s) username for GUI management.

New Password: Password for the user account.

Confirm Password: Re-enter the password.

Web GUI Permission

Guest Account: Enable to create this new guest account and select features to allow user account to access to.

When someone accesses to the BEC 4G/LTE ODU using this “user” account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account.

Click **Save** to apply settings.

Time Zone

With default, BEC 4G/LTE ODU does not contain the correct local time and date.

There are several options to setup, maintain, and configure current local time/date on the BEC 4G/LTE ODU. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.

Time Zone	
Current Date/Time	N/A (Can't find NTP server)
Time Synchronization	
Synchronize time with	<input checked="" type="radio"/> NTP Server <input type="radio"/> PC's Clock <input type="radio"/> Manually
Time Zone	(UTC-06:00) Central Time (US & Canada), Maxico City, Saskatchewan ▼
Daylight Saving	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)
<input type="button" value="Save"/>	

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

- ▶ **NTP Server automatically:** To synchronize time with the SNTP servers to get the current time from an SNTP server outside your network then choose your local time zone. After a successful connection to the Internet, BEC 4G/LTE ODU will retrieve the correct local time from the SNTP server this is specified.
- ▶ **PC's Clock:** To synchronize time with the PC's clock.
- ▶ **Manually:** Select this to enter the SNMP server IP address manually.
 - ◆ **Date:** Month / Date / Year. Month – 1 ~ 12 (January ~ December).
 - ◆ **Time:** Hour: Minute: Second

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

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

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

Click **Save** to apply settings.

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your BEC 4G/LTE ODU provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of the BEC 4G/LTE ODU, you should download or copy the firmware to your local environment first. Click “**Choose File**” to specify the path of the firmware file. Then, click “**Upgrade**” to start upgrading process. After completing the firmware upgrade, the BEC 4G/LTE ODU will automatically restart and run the new firmware.

Firmware & Configuraiton	
Upgrade	<input checked="" type="radio"/> Firmware <input type="radio"/> Configuration
System Restart with	<input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings
File	<input type="button" value="Choose File"/> No file chosen
Backup Configuration	<input type="button" value="Backup"/>
Status	
It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.	
<input type="button" value="Upgrade"/>	

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

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

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

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

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your BEC 4G/LTE ODU device when making false configurations and want to restore to the original settings.

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

Firmware Upgrade	
File upload succeeded, starting flash erasing and programming!!	
Progress	<div style="width: 15%; height: 10px; background-color: #0070C0;"></div>
Percent	15 %

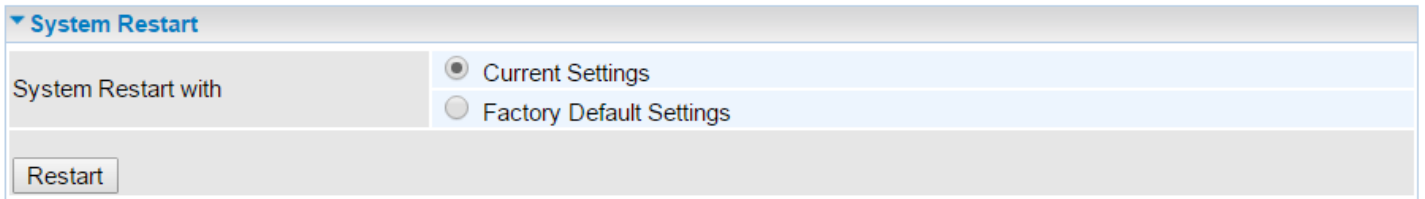


DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your RidgeWave 6900.

System Restart

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



The screenshot shows a web interface for the 'System Restart' section. At the top, there is a dropdown menu labeled 'System Restart'. Below it, there is a form with the label 'System Restart with'. There are two radio button options: 'Current Settings' (which is selected) and 'Factory Default Settings'. At the bottom of the form, there is a 'Restart' button.

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

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

Auto Reboot

Schedule an automatic reboot for your BEC 4G/LTE ODU 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 settings

Example: Schedule BEC 4G/LTE ODU 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 type="checkbox"/> Sat.	<input 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.

4G/LTE

Diagnostic Tool	
WAN Interface	4G-LTE ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address or Domain <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
Start	
Speed Test ▶	Download N/A Upload N/A Latency N/A
Trace Route	<input type="radio"/> Yes <input checked="" type="radio"/> No
Start Trace Route	

Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

Click **START** to begin to diagnose the connection.

Diagnostic Tool	
WAN Interface	4G/LTE ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A
Start	

Speed Time: Measure the current uplink and downlink speed rate.

- ▶ Take less than a minute to run the test.

Speed Test	
Testing	<div style="width: 10%; height: 10px; background-color: #0070C0;"></div>

- ▶ Result in Uplink / Downlink

Speed Test	
Result	NA NA
Back	

Click **Back** to go back to the Diagnostic Tool

Trace Route is to display how many hops (also view the exact hops) required to get to the destination.

Click **Yes**, enter the IP address or domain then **Start Trace Route**.

Trace Route <input checked="" type="radio"/> Yes <input type="radio"/> No	
IP Address or Domain	<input type="text"/>
Max TTL Value	<input type="text" value="16"/> [2-30]
<input type="button" value="Start Trace Route"/>	

IP Address or Domain: Set the destination host (IP, domain name) to be traced.

Max TTL value: Set the max Time to live (TTL) value.

Shown as we “trace” www.billion.com below.

```

Trace www.billion.com

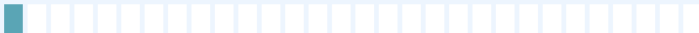
tracert to www.billion.com (125.227.205.188), 16 hops max, 60 byte packets
 1 172.16.1.254 (172.16.1.254)  0.472 ms  0.488 ms  0.643 ms
 2 122.96.153.233 (122.96.153.233)  7.354 ms  7.517 ms  7.704 ms
 3 221.6.12.69 (221.6.12.69)  7.921 ms  8.108 ms  8.256 ms
 4 221.6.1.253 (221.6.1.253)  8.392 ms  8.544 ms *
 5 219.158.99.245 (219.158.99.245)  36.110 ms  36.839 ms  37.001 ms
 6 * * *
 7 * * 219.158.103.26 (219.158.103.26)  40.731 ms
 8 211.72.233.194 (211.72.233.194)  65.969 ms  66.040 ms  66.019 ms
 9 220.128.6.126 (220.128.6.126)  61.726 ms  61.831 ms  61.960 ms
10 220.128.11.170 (220.128.11.170)  61.543 ms  61.583 ms  65.127 ms
11 220.128.17.85 (220.128.17.85)  63.436 ms  62.133 ms  65.862 ms
12 220.128.17.229 (220.128.17.229)  64.695 ms  64.849 ms  65.063 ms
13 168.95.229.145 (168.95.229.145)  61.915 ms  60.715 ms  60.825 ms
14 * * *
15 * * *
16 * * *
    
```

LAN

Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

Speed Time: Measure the current uplink and downlink speed rate.

- ▶ Take less than a minute to run the test.

Speed Test
Testing 

- ▶ Result in Uplink / Downlink

Speed Test
Result <input type="text" value="NA"/> <input type="text" value="NA"/>
<input type="button" value="Back"/>

Click **Back** to go back to the Diagnostic Tool

Click **START** to begin to diagnose the connection.

Chapter 5: Troubleshooting

If your **BEC 4G/LTE ODU** is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

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

Problem with LAN Interface

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

Recovery Procedures

Problem	Suggested Action
<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 another small pointed object immediately. 2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

APPENDIX: PRODUCT SUPPORT & CONTACT

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

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

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

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

FCC Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to FCC 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 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 FCC Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (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.

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 25cm between the radiator & your body.

Professional Installation Instructions (BEC 6900 R21)

1. **Installation Personal**

This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. **Installation Location**

The product shall be installed at a location where the radiating antenna can be kept 25 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. **External Antenna**

Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.

4. **Installation Procedure**

Please refer to user's manual for the detail.

5. **Warning**

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.