User Manual

BEC 4700A/AZ

(4G/LTE) Wireless Outdoor Router

Last revised: July 2020
Version release: v2.1

Copyright Notice

Copyright@ 2020 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 6

APPLICATION DIAGRAM..... 7

CHAPTER 2: PRODUCT OVERVIEW.....8

IMPORTANT NOTE FOR USING THIS ROUTER..... 8

PACKAGE CONTENTS 8

DEVICE DESCRIPTION 9

Hardware Overiew (BEC 4700AZ) 9

Hardware Overiew (BEC 4700A) 11

.....11

MOUNTING KIT INSTALLATION 13

ROUTER INSTALLATION INSTRUCTIONS 19

SYSTEM RECOVERY PROCEDURES 23

CHAPTER 3: BASIC INSTALLATION 24

NETWORK CONFIGURATION – IPV4..... 25

Configuring PC in Windows 10 (IPv4) 25

Configuring PC in Windows 7/8 (IPv4).....27

Configuring PC in Windows Vista (IPv4).....29

NETWORK CONFIGURATION – IPV6..... 31

Configuring PC in Windows 10 (IPv6) 31

Configuring PC in Windows 7/8 (IPv6).....33

Configuring PC in Windows Vista (IPv6).....35

DEFAULT SETTINGS 37
INFORMATION FROM YOUR ISP 38
CHAPTER 4: DEVICE CONFIGURATION 39
LOGIN TO YOUR DEVICE 39
STATUS 42
Device Info 42
System Status 44
System Log 44
4G/LTE Status 45
Wireless Status 47
Hotspot Status 48
Statistics 49
DHCP Table 53
IPSec Status 53
PPTP Status 54
L2TP Status 55
GRE Status 55
OpenVPN Status 56
ARP Table 57
VRRP Status 57
QUICK START 58
CONFIGURATION 61
Interface Setup 61
Internet 61
LAN 71
Wireless 2.4GHz 75
Wireless MAC Filter 80
Wireless 5GHz 81
Wireless 5G MAC Filter 89
Wireless 5G Repeater 90
Loopback 91
Dual WAN 92
General Setting 92
Outbound Load Balance 96
Protocol Binding 97
Hotspot 99

General Setting *99*
Built-in User Account *102*
Authorized of Client *103*
Walled Garden *104*
Advertisement *105*
Hotspot Status Log *106*
Customization *107*
Advanced Setup 109
Firewall *109*
Static Routing *110*
Dynamic Routing *111*
NAT *113*
VRRP *118*
Static DNS *119*
QoS *120*
Interface Grouping *123*
Port Isolation *126*
Time Schedule *127*
Mail Alert *128*
VPN 129
IPSec *129*
PPTP Server *139*
PPTP Client *141*
L2TP *148*
GRE Tunnel *156*
OpenVPN *164*
OpenVPN Server *164*
OpenVPN Client *168*
Access Management 176
Device Management *176*
SNMP *177*
Syslog (System Log) *179*
Universal Plug & Play *180*
Dynamic DNS (DDNS) *181*
Access Control *183*
Packet Filter *186*
CWMP (TR-069) *191*
Parental Control *193*
BECentral Management *194*
Maintenance 195
User Management *195*
Certificate Management *197*

Time Zone *199*
License *200*
Firmware & Configuration *201*
System Restart *202*
Auto Reboot *203*
Diagnostics Tool *204*

CHAPTER 5: TROUBLESHOOTING 206

Problems with the Router 206
Problem with LAN Interface 206
Recovery Procedures 207

APPENDIX: PRODUCT SUPPORT & CONTACT 208

FCC STATEMENT 209

CHAPTER 1: INTRODUCTION

Introduction to your Router

Congratulations on your purchase of the **BEC 4700A / AZ ((4G/LTE) Wireless Outdoor Router)**.

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 4700A/AZ provides an easy installation from eliminating the need for a separate power and data cable.

Lightweight, Compact, and unobtrusive Design

With multiple mounting options and a lightweight, it is easily to install the BEC 4700 A/AZ by single person. The BEC 4700 A/AZ 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 4700 A/AZ is designed for the toughest industrial environments. With IP68 hardened enclosure with industrial-grade components, the BEC 4700 A/AZ can be installed in manufacturing plants, industrial automation, stadiums, convention halls, stadium facilities, school campuses, etc.

4G/LTE Mobility (BEC 4900AZ Only)

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 4900AZ Only)

BEC 4700AZ 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.

New Experience with Wi-Fi Speed and Coverage

With the next wireless generation, 802.11ac, integrated in the BEC 4700 A/AZ, the router delivers fast Wi-Fi speeds of up to 2000Mbps. The BEC 4700 A/AZ supports a link rate up to 300Mbps in 2.4GHz frequency range & 1700Mbps in 5GHz range and is also backward compatible with existing 802.11 a / b / g / n wireless equipment in the network. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over Wireless LAN. BEC 4700 A/AZ also supports the Wi-Fi Protected Setup (WPS) standard for easy and secure establishment of a wireless home network. If the user's network requires

wider coverage, the built-in Wireless Distribution System (WDS) repeater function expands the wireless network without needing any external wires or cables.

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

- High-speed 4G connection up to downlink 100/300Mbps and uplink 50Mbps data rate (4700AZ)
- Outdoor 4G for high speed mobile connectivity (4700AZ)
- 4G embedded with a built-in SIM card slot (4700AZ)
- 4G Management Center for connection monitoring (4700AZ)
- Concurrent 2.4GHz & 5GHz Wi-Fi Connections
- Firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ease of Use with Quick Installation Wizard
- Ideal for boat marina, campgrounds, RV parks, public parks, urban space, remote connectivity

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)

Carrier Grade Wireless LAN

- Compliant with IEEE 802.11 a/b/g/n/ac standards
- 2.4GHz & 5GHz frequency range
- 20/40-MHz channel bandwidth
- Up to 300Mbps (2.4GHz) & 1700Mbps (5GHz) wireless data phy rate
- 64/128 bits WEP supported for encryption
- Wireless security with WPA-PSK, WPA2-PSK, Mixed WPA/WAP2-PSK, 802.1x/Radius
- AP, Client Bridge and WDS Operational Modes
- Multiple SSID (4 SSIDs), BSSID
- Wireless MAC filtering
- Wireless Client Isolation
- Support up to 32 Connected Clients
- Wi-Fi client rate-limiting

Management

- Quick Installation wizard

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

Hardware Specifications

Physical interface

- (2) 10/100/1000 Gigabit Ethernet LAN with IEEE802.3at compliant Gigabit PoE PD
- IEEE 802.3at PD complaint (25.5W)
- (6) Wireless N-Type Connectors with arrester
- SIM slot (for the SIM from Telco / ISP) (4700AZ)
- Reset Button
- LED Indicators:

  (4700AZ) Power/Boot, LAN(PoE), EWAN, WI-FI(2.4GHz & 5GHz), LTE RSSI, and Internet

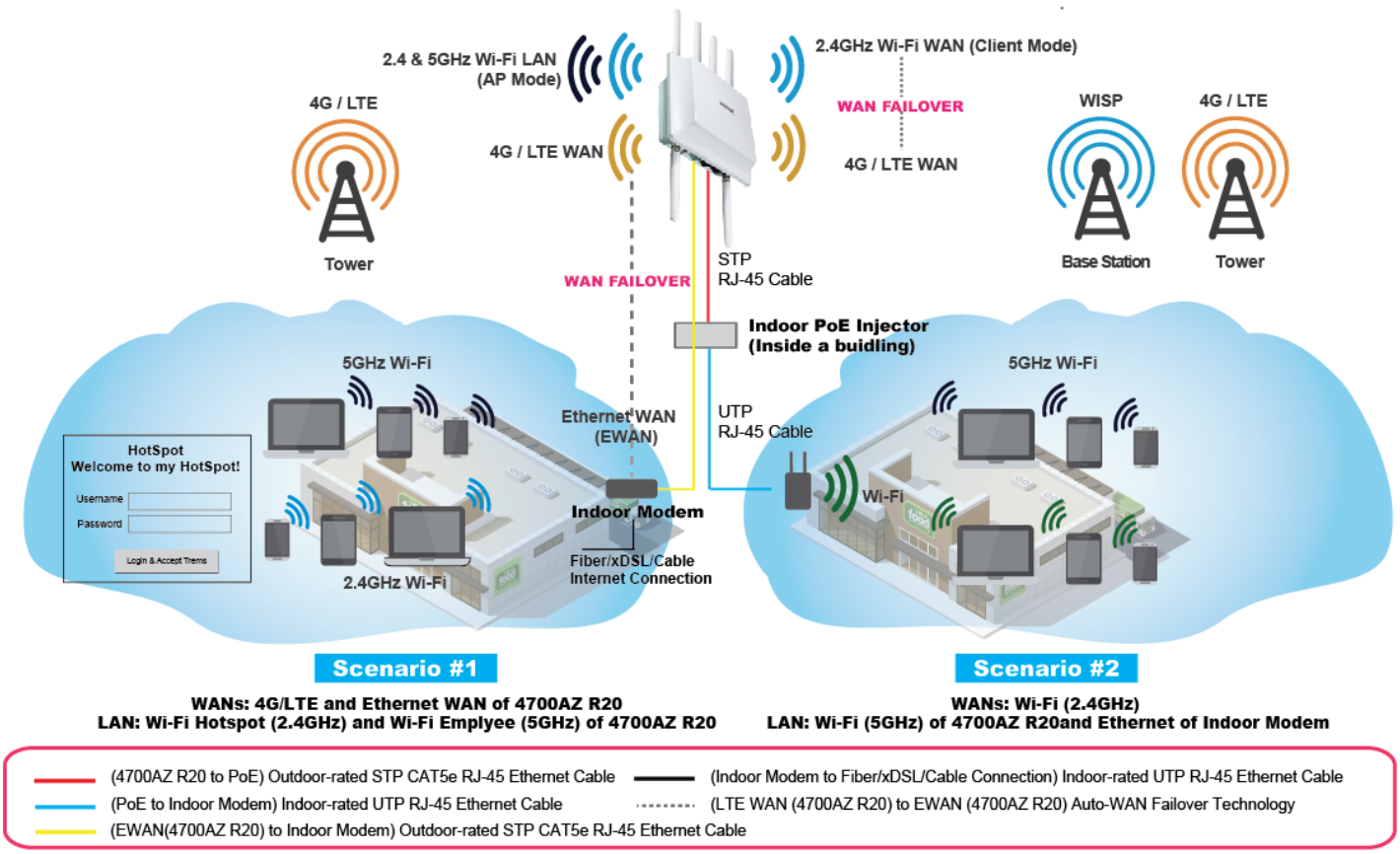
  (4700A) Power/Boot, LAN(PoE), WAN, Wi-Fi Internet

Physical Specifications

- Dimensions (W*H*D): 8.5" x 7.5" x 3"(257mm x 227mm x 91mm)
- Weight: 2kgs (4.4lbs) (Without Mount)
- Industrial-grade IP68 and Vent integration enclosure
- Top cover material UL-746C compliant for UV-resistant

Application Diagram

4700AZ



CHAPTER 2: PRODUCT OVERVIEW

Important Note for Using This Router

Attention

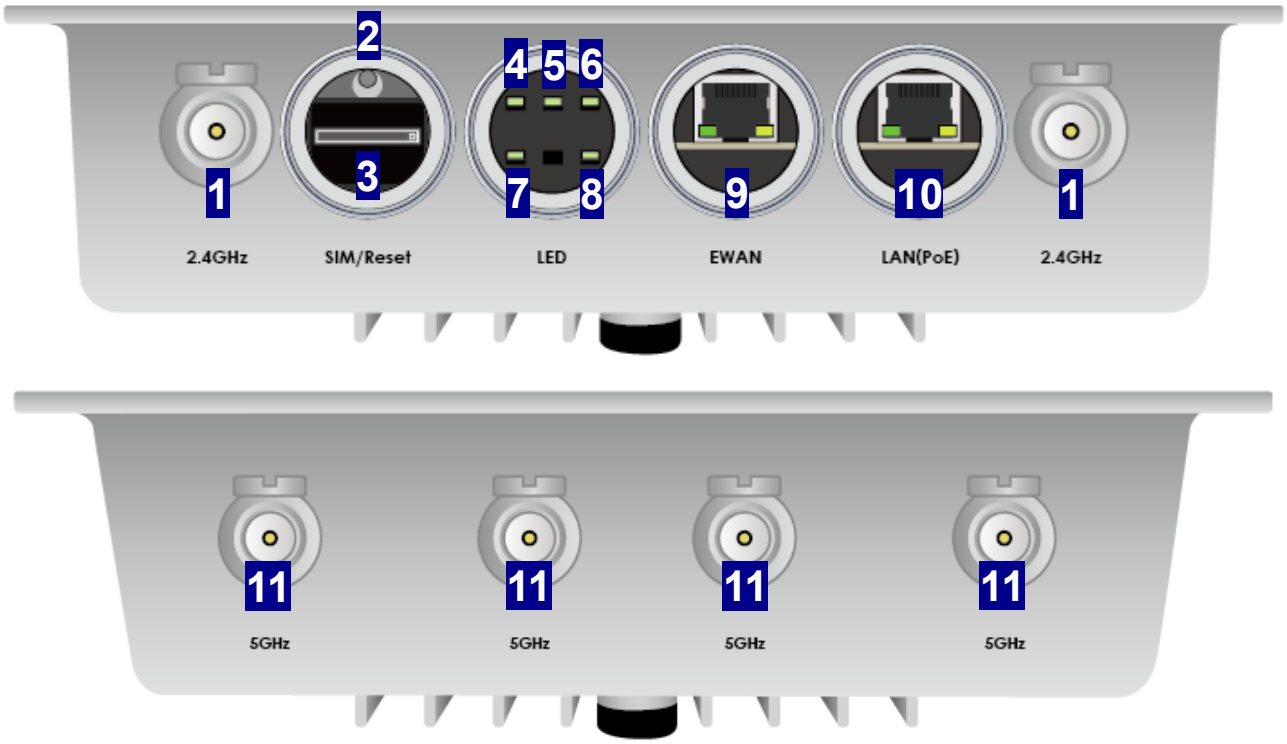
- ✓ Do not remove, open or repair the case yourself. Contact with your Internet Service Provider or have it repaired at a qualified service center.
- ✓ Use the supplied PoE (Power-over-Ethernet) injector for indoor only or with any 802.3at capable PoE injectors to connect with the BEC 4700A/AZ.
- ✓ It is mandatory to earth ground the BEC 4700A/AZ. Improper grounding not only could damage the unit but also all equipment connected to it.

Package Contents

- ✓ The BEC 4700A / AZ (4G/LTE) Wireless Outdoor Router x 1
- ✓ M25 Cable Gland x 2
- ✓ Quick Start Guide x 1
- ✓ Outdoor LAN Cable x 1
- ✓ Gigabit Power-over-Ethernet (PoE) Injector x 1
- ✓ Grounding Wire x 1
- ✓ 2.4GHz/5GHz Wi-Fi Antennas x 6
- ✓ Mounting Kit x 1

Device Description

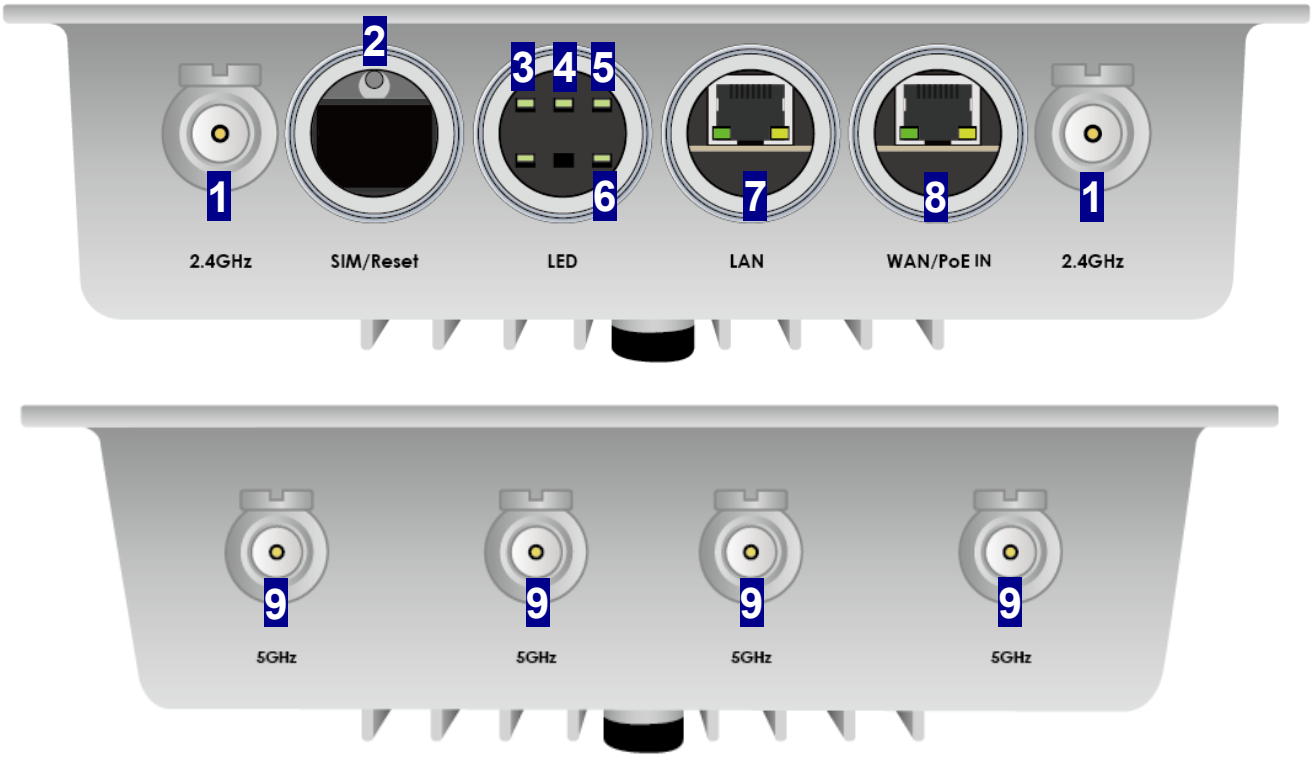
Hardware Overiew (BEC 4700AZ)



PORT & LED		MEANING	
1	**WIFI Antenna Connectors (2.4GHz)**	Screw the supplied 2.4GHz antennas onto the antenna connectors on both sides.	
2	**RESET**	After the device is powered on, press it **6 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)	
3	**SIM Card Slot**	Insert the mini SIM card (2FF) with the gold contact facing down. Push the mini SIM card (2FF) inwards to eject it * Power off the BEC 4700AZ before inserting or removing the SIM card(s)	
4	**2.4GHz WIFI LED**	Green	Wireless connection established
		Blinking	Data being transmitted / received
5	**5GHz WIFI LED**	Green	Wireless connection established
		Blinking	Data being transmitted / received

PORT & LED		MEANING	
6	**LTE LED (Received Signal Strength Indicator)**	Green	RSSI greater than -69 dBm. Excellent signal condition
		Green Flashing Quickly	RSSI from -81 to -69 dBm. Good signal condition
		Orange Flashing Quickly	RSSI from -99 to -81 dBm. Fair signal condition
		Orange Flashing Slowly	RSSI less than -99 dBm. Poor signal condition
		Orange	No signal and the 4G LTE module is in service
		Off	No LTE module or LTE module fails
7	**Power LED**	Green	System is up and ready
		Red	Boot failure
8	**Internet LED**	Green	IP connected; WAN connection is ready
		Red	IP request failed
		Off	Either in bridged mode or WAN connection is not available
9	**Gb Ethernet WAN**	Use an outdoor Ethernet cable to connect with to an internet device. **Note: The EWAN port is a configurable LAN/WAN port, which automatically becomes an EWAN port when EWAN internet interface is being selected in the GUI**.	
		Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
10	**Gb Ethernet LAN/PoE**	LAN & PoE interface. Connect to the supplied 802.3at Gb PoE injector to provide power & data	
		Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
11	**WIFI Antenna Connectors (5GHz)**	Screw the supplied Wi-Fi antennas onto those 4 antenna connectors.	

Hardware Overiew (BEC 4700A)



PORT & LED		MEANING	
1	**WIFI Antenna Connectors (2.4GHz)**	Screw the supplied 2.4GHz antennas onto the antenna connectors on both sides.	
2	**RESET**	After the device is powered on, press it **6 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)	
3	**2.4GHz WIFI LED**	Green	Wireless connection established
		Blinking	Data being transmitted / received
4	**5GHz WIFI LED**	Green	Wireless connection established
		Blinking	Data being transmitted / received

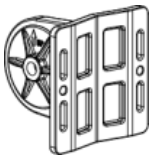
PORT & LED		MEANING	
5	**Power LED**	Green	System is up and ready
		Red	Boot failure
6	**Internet LED**	Green	IP connected; WAN connection is ready
		Red	IP request failed
		Off	Either in bridged mode or WAN connection is not available
7	**Gb Ethernet LAN**	Use an outdoor Ethernet cable to connect to any Ethernet equipment.	
		Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
8	**Gb Ethernet WAN/PoE IN**	WAN & PoE interface. Connect to the supplied 802.3at Gb PoE injector to provide power & data.	
		Green	Transmission speed is at Gigabit speed (1000Mbps)
		Orange	Transmission speed is at 10/100Mbps
		Blinking	Data being transmitted/received
9	**WIFI Antenna Connectors (5GHz)**	Screw the supplied Wi-Fi antennas onto those 4 antenna connectors.	

Mounting Kit Installation

Mounting Kit includes:

- ❖ Articulation Pole x 1
- ❖ T-formed Bracket x 1
- ❖ Stainless Hose Clamp x 2
- ❖ M8x40 Screw Bolt x 1
- ❖ M8 Nut x 1
- ❖ M8 Washer x 1
- ❖ M6 Washer x 4
- ❖ Spring Washer M8 x 1
- ❖ Spring Washer M6 x 4
- ❖ M6x16 Screw x 4

Articulation Pole x 1


T-form Bracket x 1

M8x40 Screw Bolt x 1

M8 Nut x 1

M8 Washer x 1
M6 Washer x 4

Spring Washer M8 x 1

M6 x 16 Screw x 4

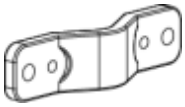
For **Wall Mount Installation**, you will need:

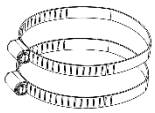
- ❖ Wood Screw x 4
- ❖ Wood / Gyprock x 4

Wood Screw x 4
Wood / Gyprock Plug x 4

For **Pole Mount Installation**, you will need:

- ❖ W-Bar x 1
- ❖ M6 x 60 Screw Bolts x 2
- ❖ M6 Washer x 2
- ❖ Spring Washer x 2
- ❖ Stainless Hose Clamp x 2


W-Bar x 1


Hose Clamp x 2

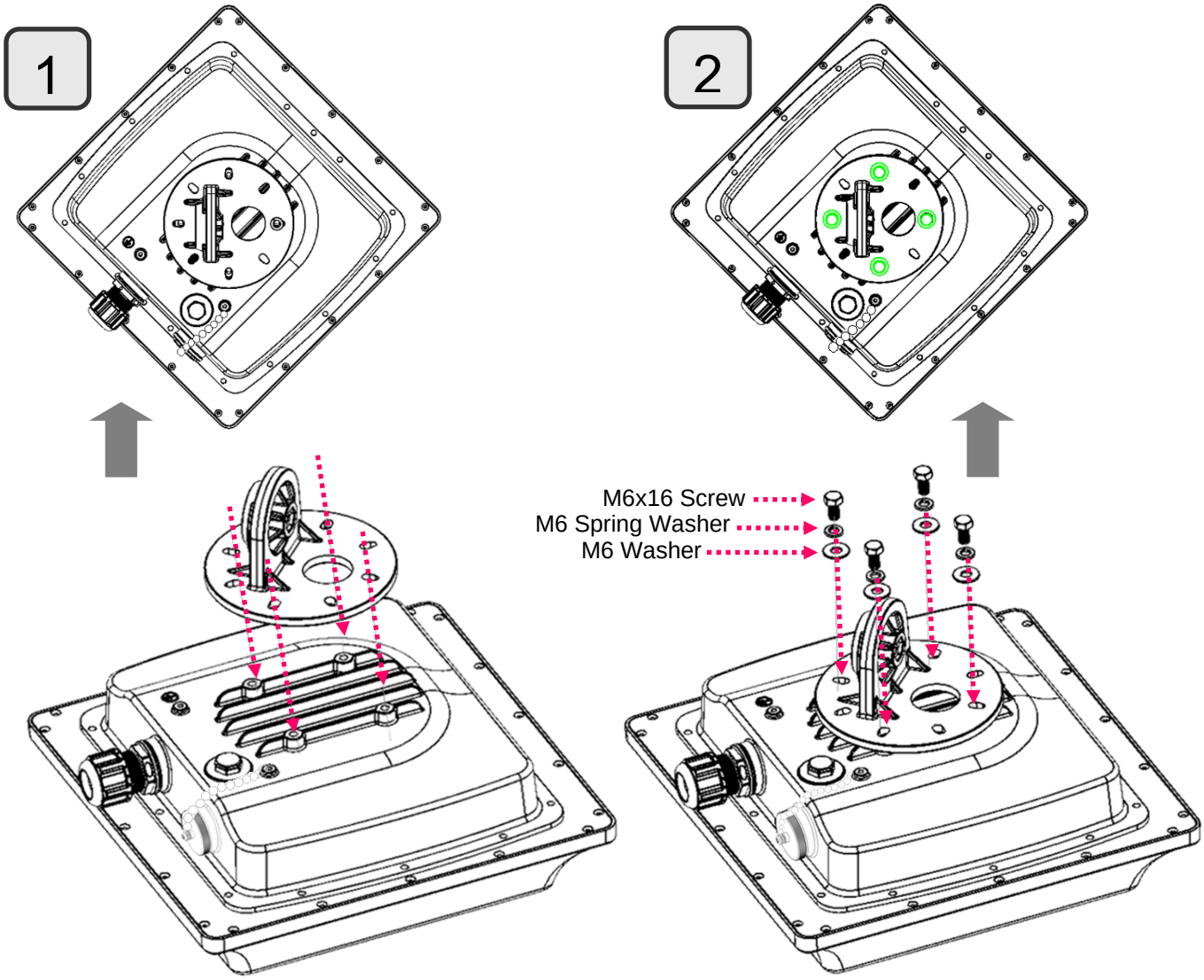
M6 x 60 Screw Bolt x 2

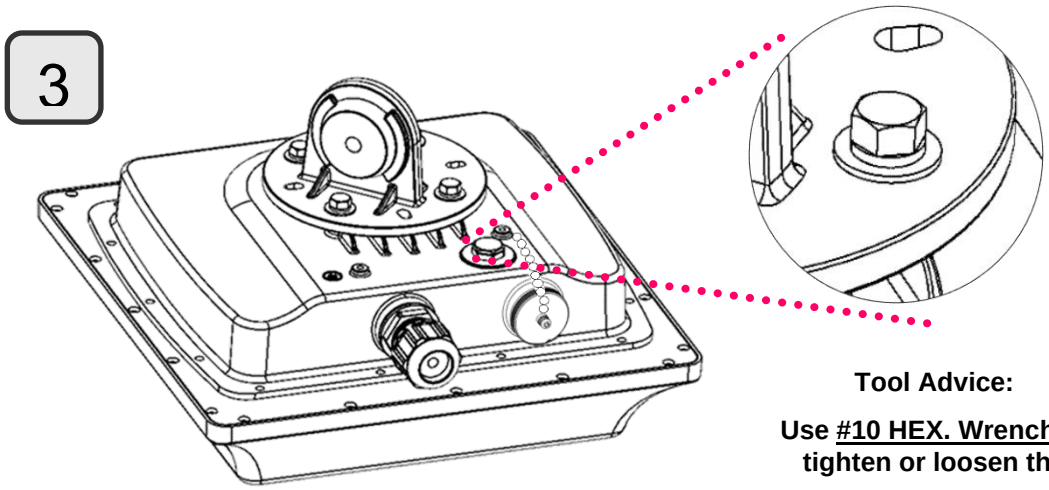
M6 Washer x 2

Spring Washer M6 x 2

1. Attach the Articulation Pole to the Enclosure

Attach the articulation pole to the back of the BEC 4700A/AZ enclosure using the supplied **M6 screws**, **M6 spring washers** and **M6x16 screws** which are included in the mounting kit.

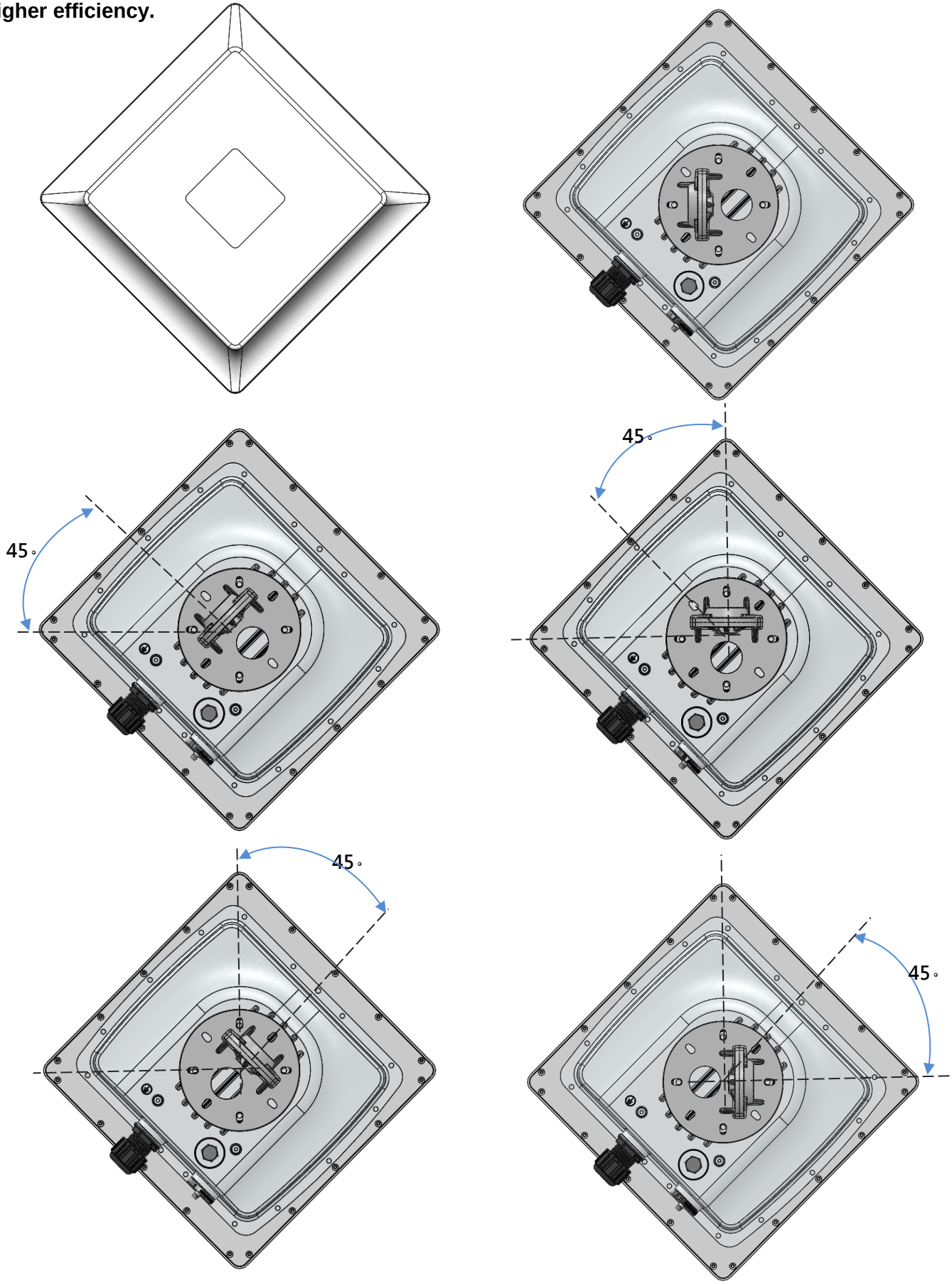




Tool Advice:

Use #10 HEX. Wrench to tighten or loosen the

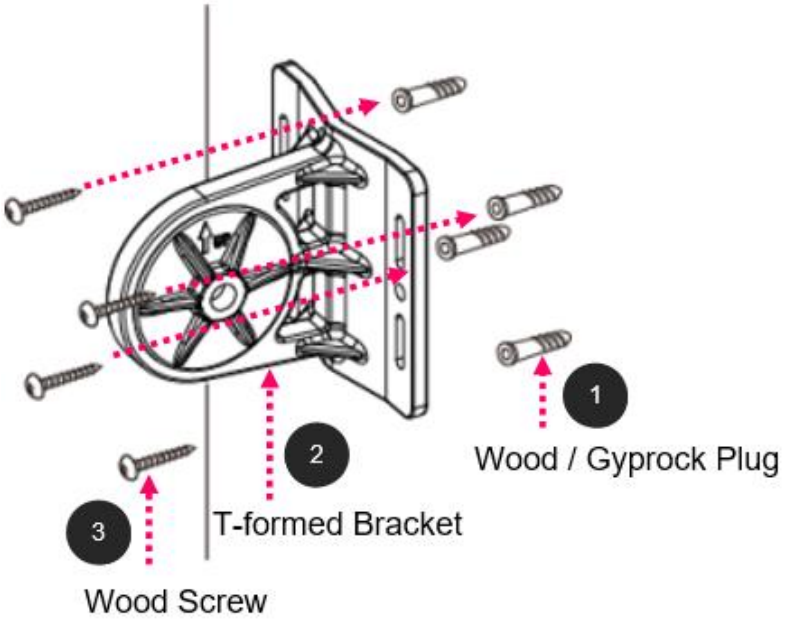
Note: The flexible mounting kit can be adjusted in multiple angles to align with the base station for higher efficiency.



2. Wall or Pole Mount Installation

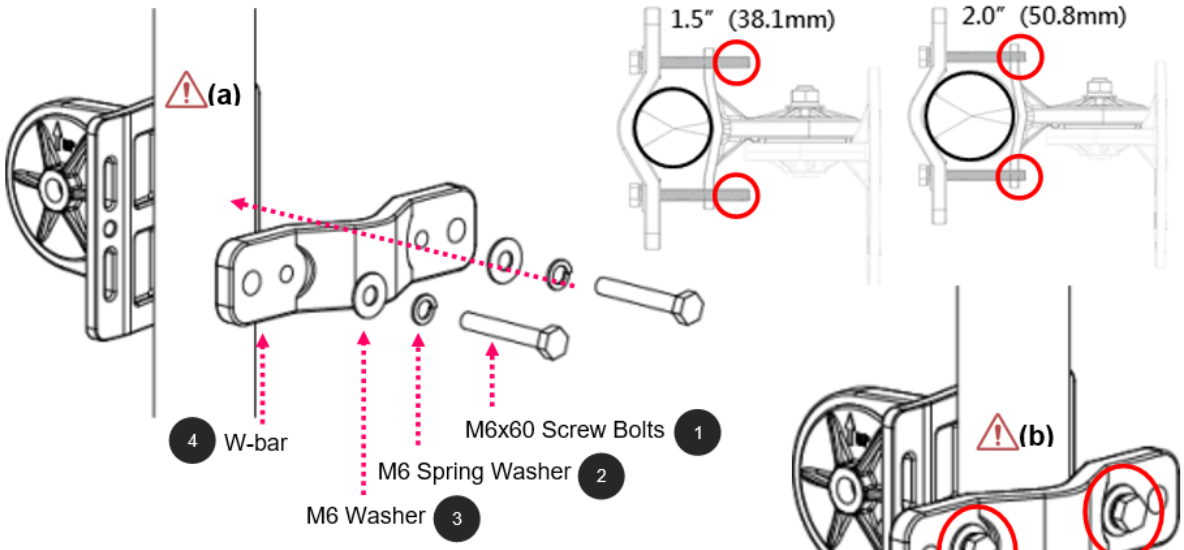
2.1 Mounting on Wall

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



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

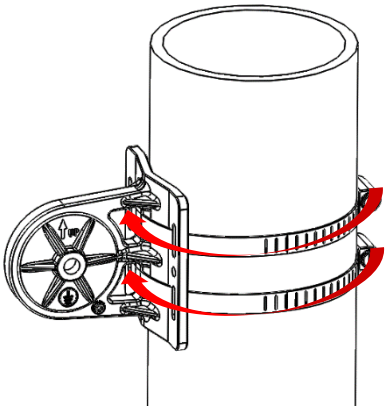
Attach the T-formed Bracket and the W-bar to the pole then use **M6x60 bolts**, **M6 spring washers** and **M6 washers** to fix the mounting kit onto the pole.



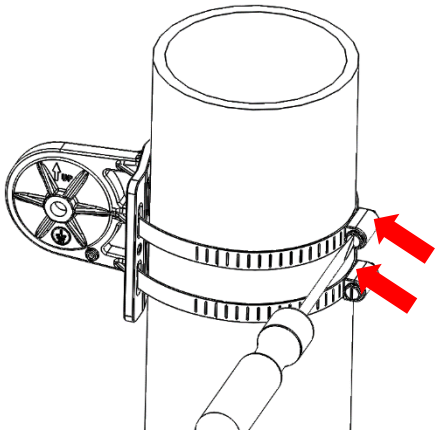
⚠ **(a) The accept pole diameter is from 1.5” to 2”. If the diameter is larger than 2”, it can cause a failure very fast. If diameter is smaller than 1.5”, the clamping force might be insufficient in holding the device to the pole.**

⚠ **(b) To minimize bolts crosstalk, the bolt should gradually increase the bolt load on both sides.**

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



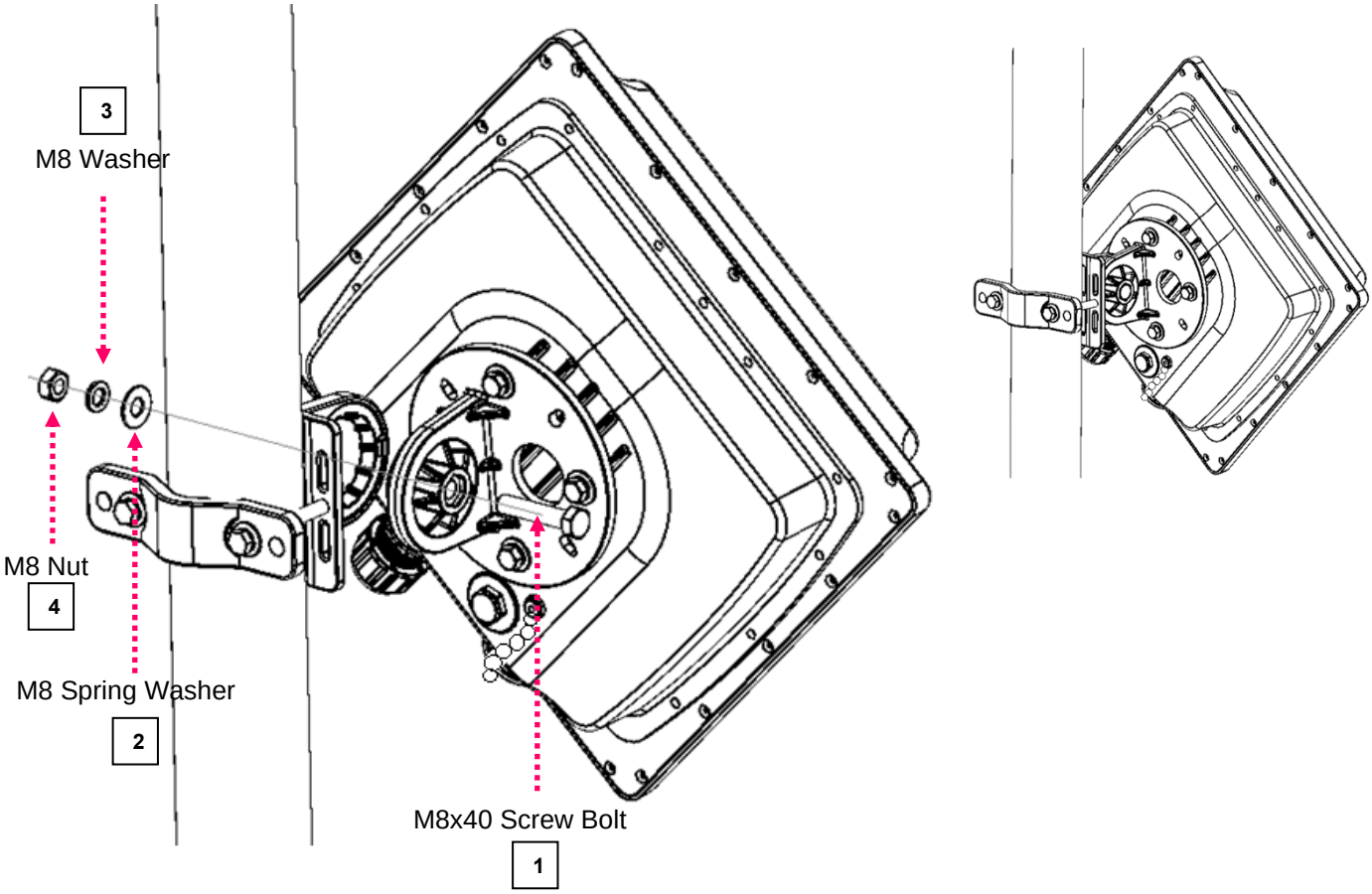
Use the stainless hose clamps through the T-formed Bracket.



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.

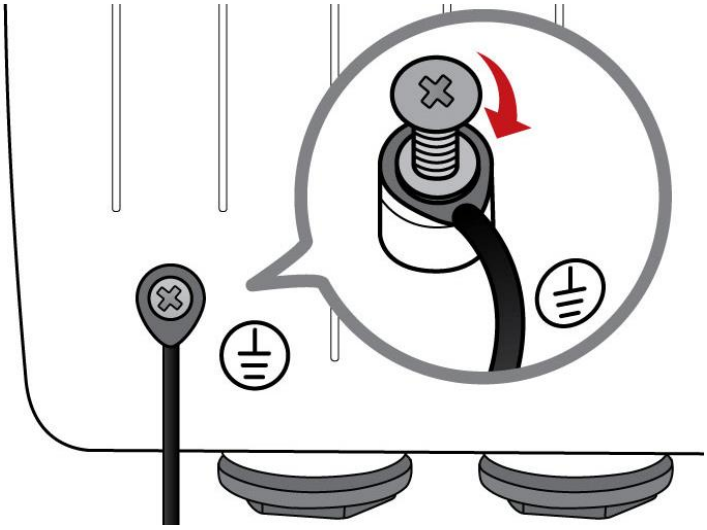
3. Install the Articulation Pole with the T-formed Bracket

Attach the articulation pole (BEC 4700A/AZ enclosure) to the T-formed bracket using the supplied **M8 nut**, **M8 spring washer**, **M8 washer** and **M8x40 screw bolt**.



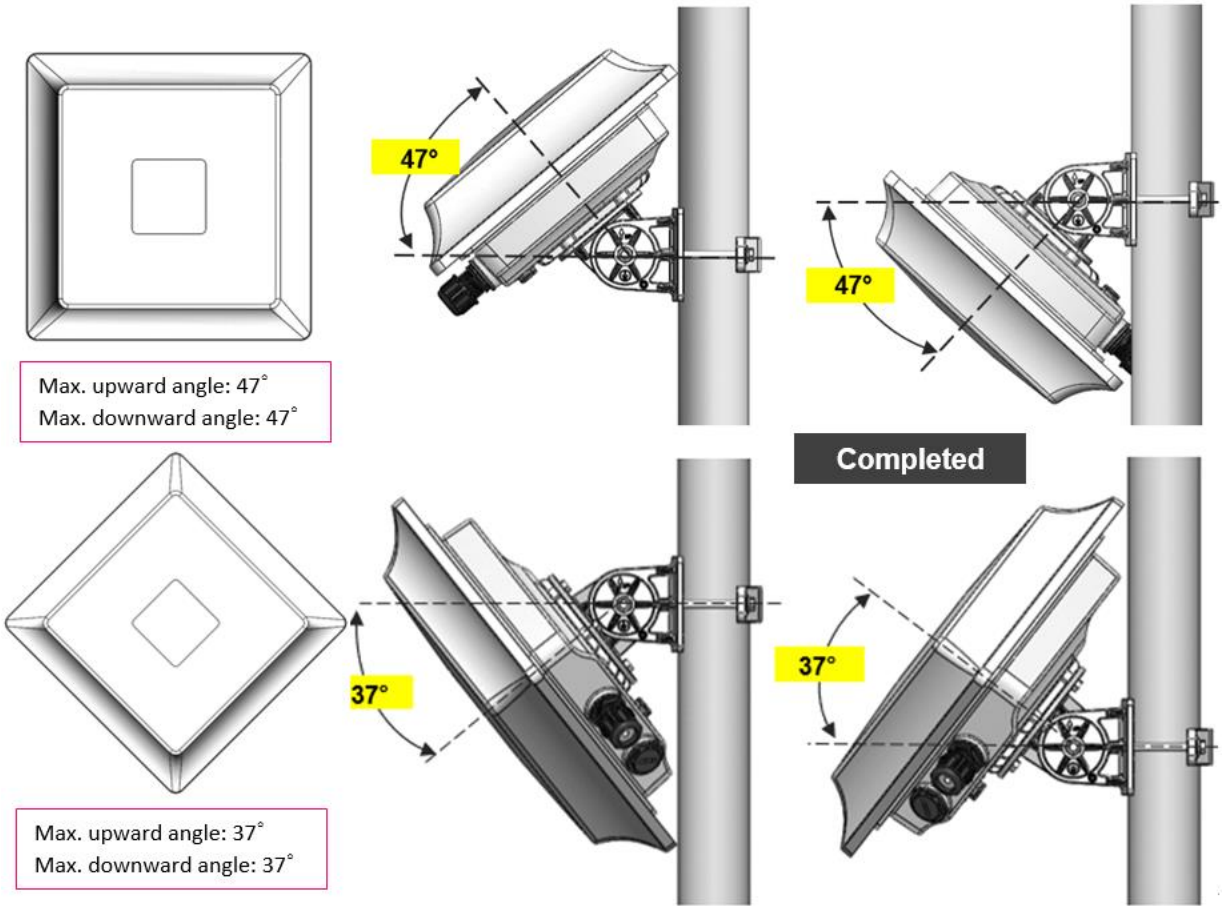
4. Grounding the BEC 4700A/AZ to Complete the Installation

Attach the grounding wire to the BEC 4700A/AZ and tighten the screw



5. Position Adjustment

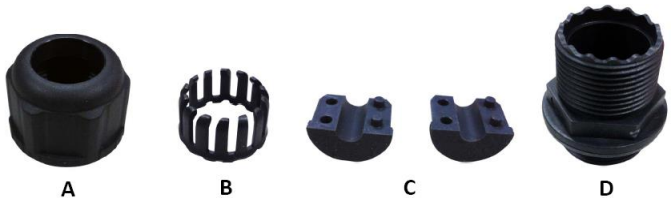
Adjust the 4700A/AZ until it reaches the desire elevation and depression angle, then tight the **M8 nut** (see **Install the Articulation Pole with the T-formed Bracket** for more information)



Router Installation Instructions

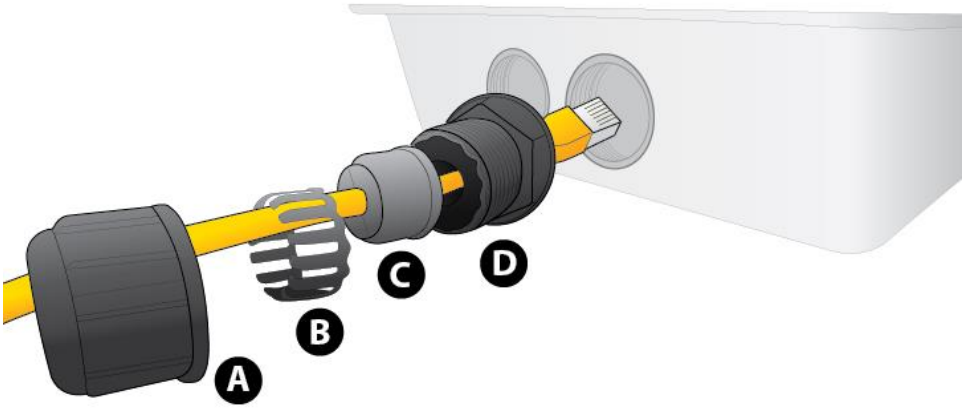
1. Power on your BEC 4700A/AZ

Step 1: Assemble M25 cable gland



Step 2:

Unscrew the WAN/PoE IN port and insert the supplied outdoor Ethernet cable (RJ-45) through material A-D, and then connect the RJ-45 Ethernet cable into the WAN/PoE IN port.



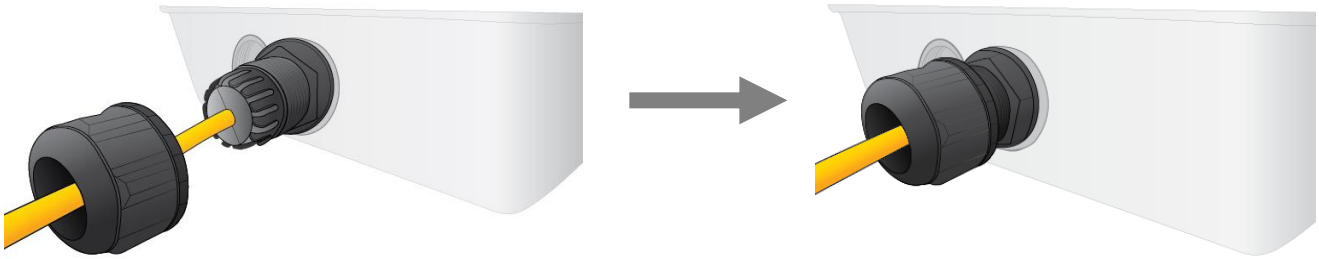
Step 3:

3.1: Insert Ⓒ at the back end of Ⓓ

3.2: clip Ⓑ on Ⓒ

3.3: keep Ⓑ close to Ⓓ

3.4: then tighten Ⓐ

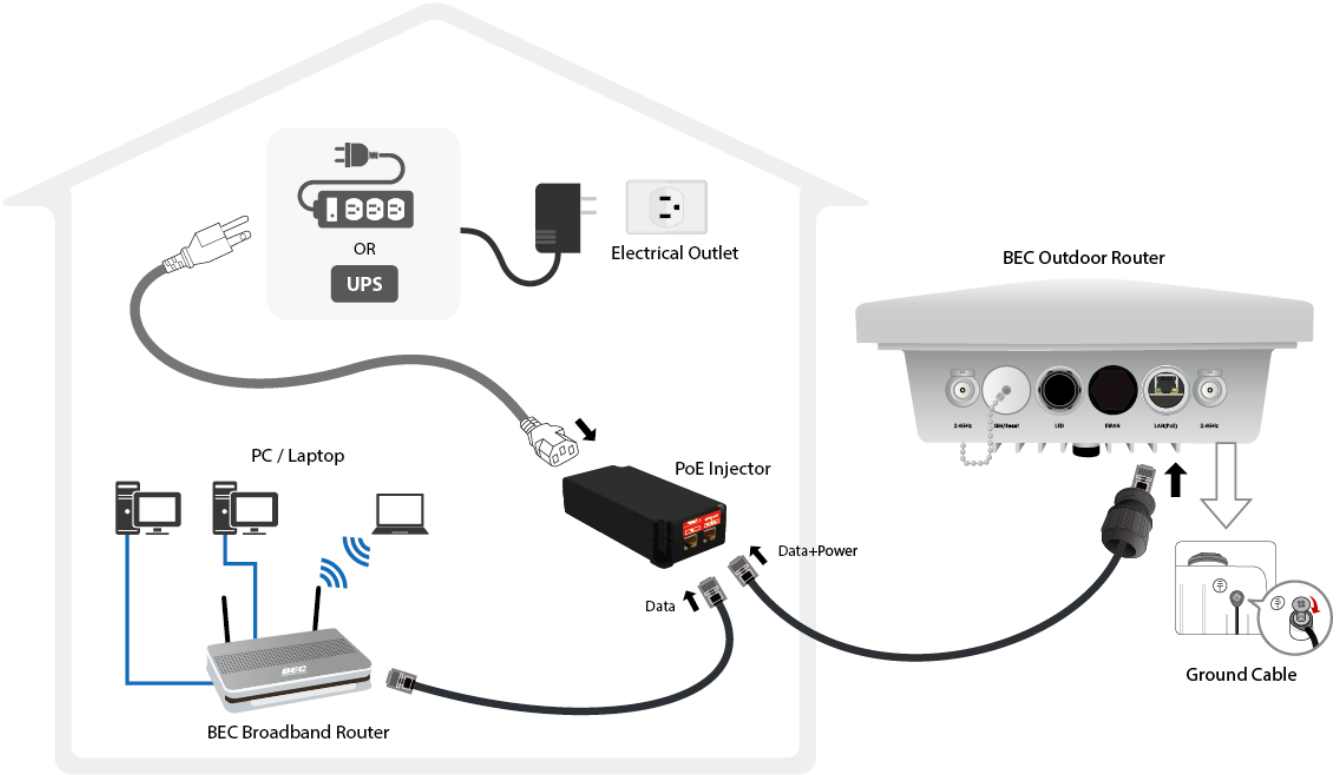


Step 4:

Powering via PoE Injector: 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.

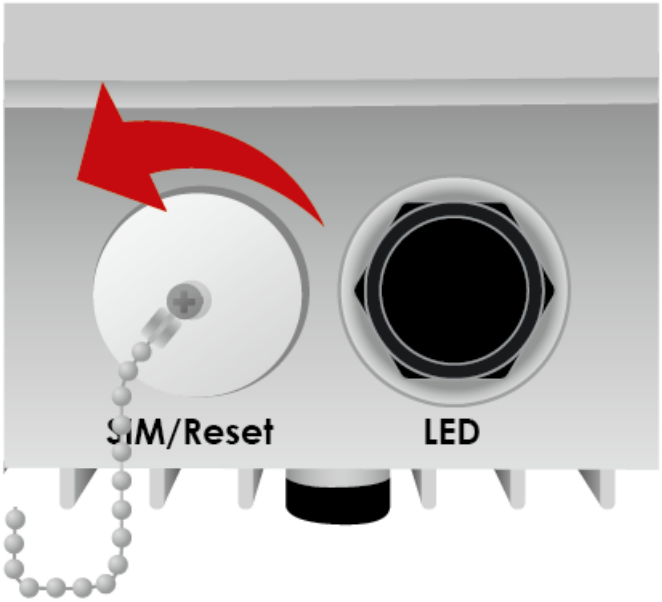
Powering via a PoE Switch: Connect the Ethernet cable (RJ-45) from the 4700A/AZ directly to a PoE port on the switch.

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!



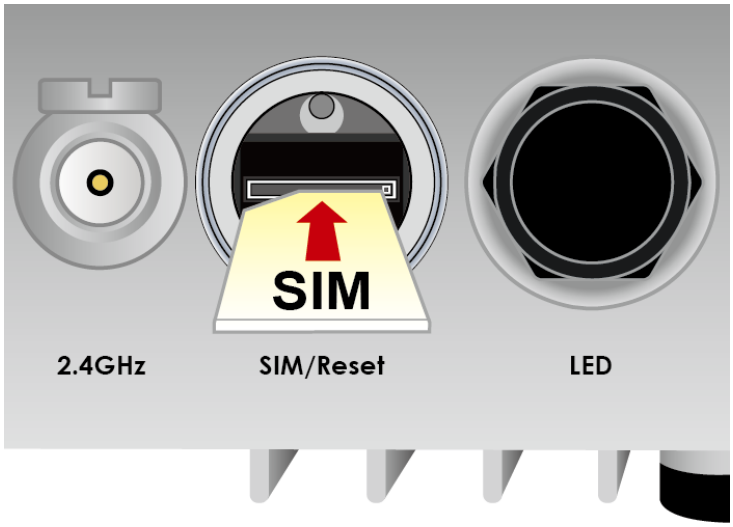
2. Set up Your Internet Connection

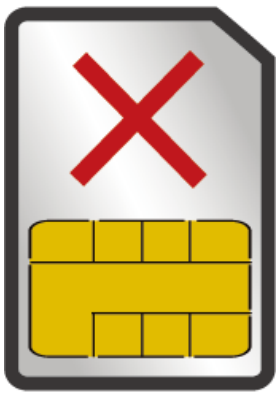
Step 1 (4700AZ Only): Unscrew the cap of SIM card slot.



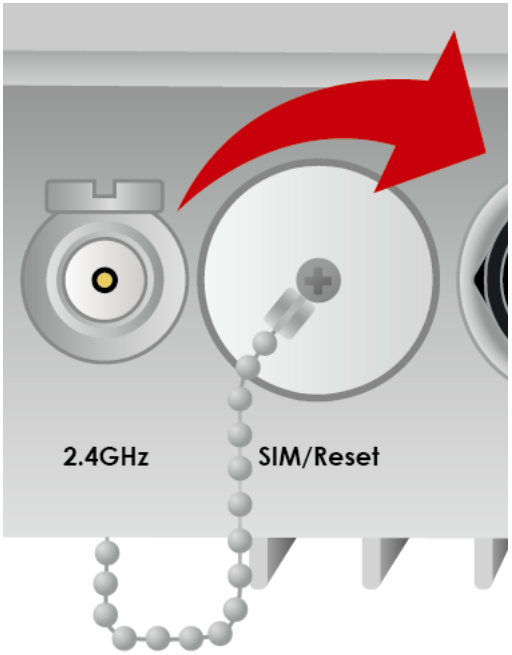
Step 2 (4700AZ Only): Slide the SIM card with the mental contacts (gold plate) facing down to the SIM slot then push it all the way in until you hear the clicking sound.

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





Step 3 (4700AZ Only): 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 4700A/AZ 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 4700A/AZ Device

2.1 Power off your BEC 4700A/AZ

2.2 Power on the BEC 4700A/AZ 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 4700A/AZ Device

With INTERNET light flashes green, BEC 4700A/AZ 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, BEC 4700A/AZ 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 4700A/AZ.

3.4 INTERNET LED turns green after the Firmware upgrade completed

3.5 Power cycle on & off to regain access to the BEC 4700A/AZ.

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.

Attention

Any TCP/IP capable workstation can be used to communicate with or through the BEC 4700A/AZ. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

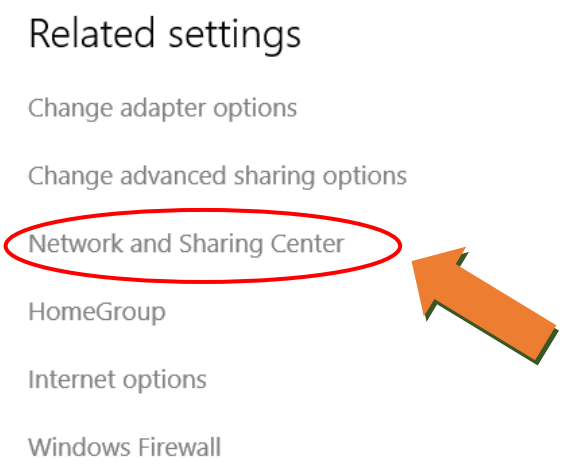
Configuring PC in Windows 10 (IPv4)

1. Click .

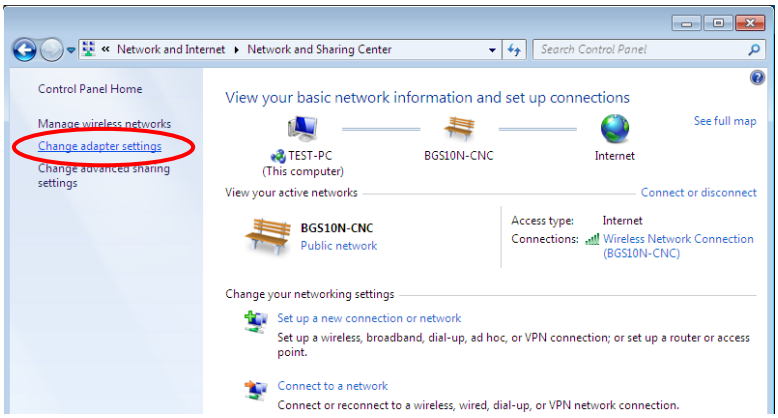
2. Click Settings

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

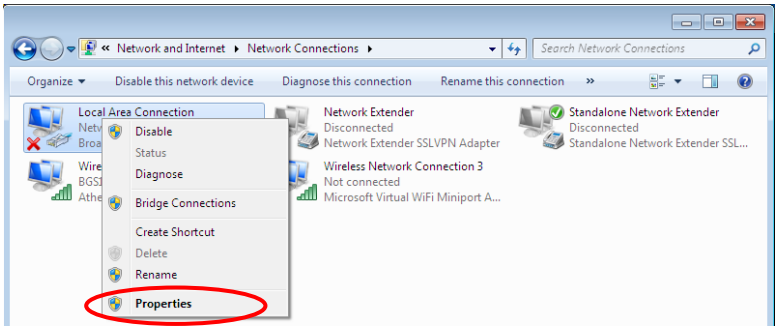
4. Under **Related settings,** select **Network and Sharing Center**



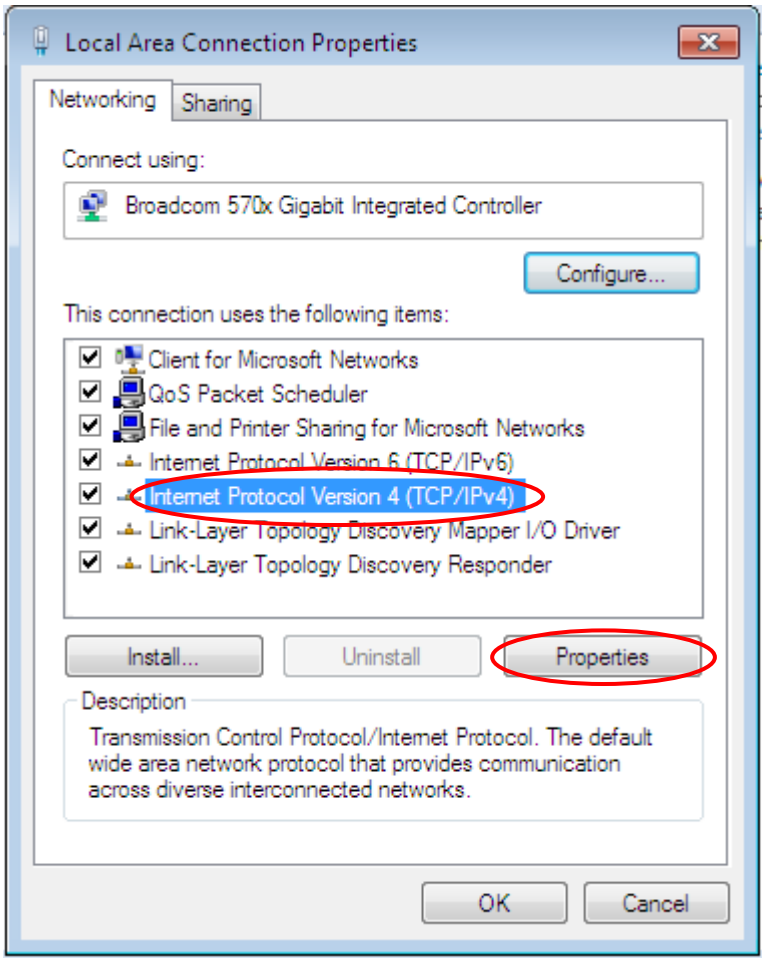
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

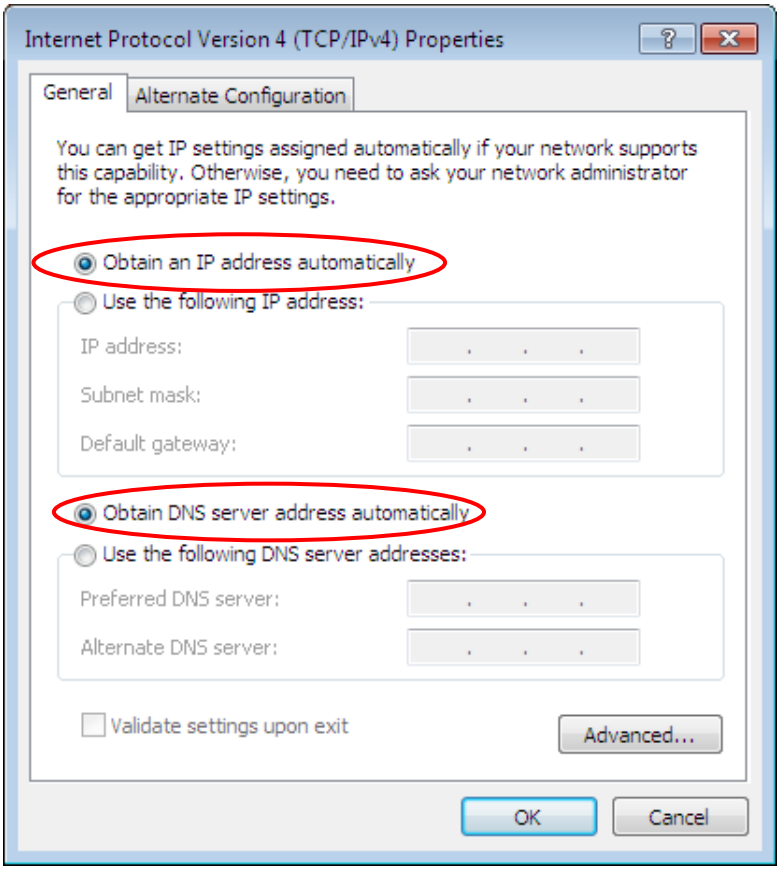


7. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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.

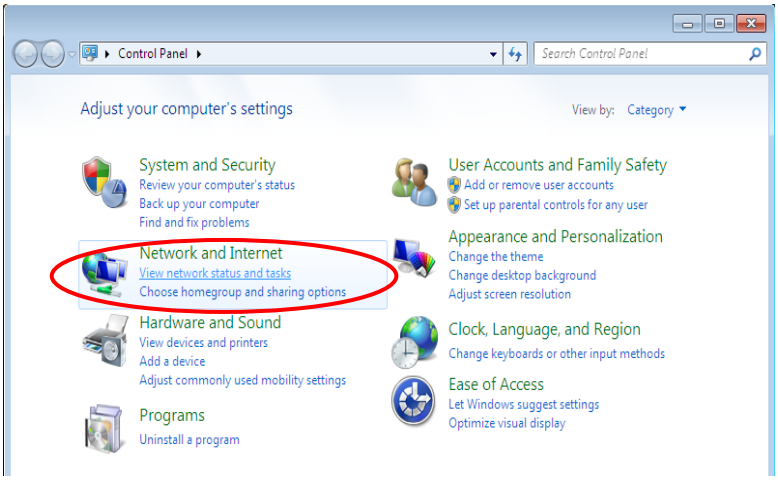
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



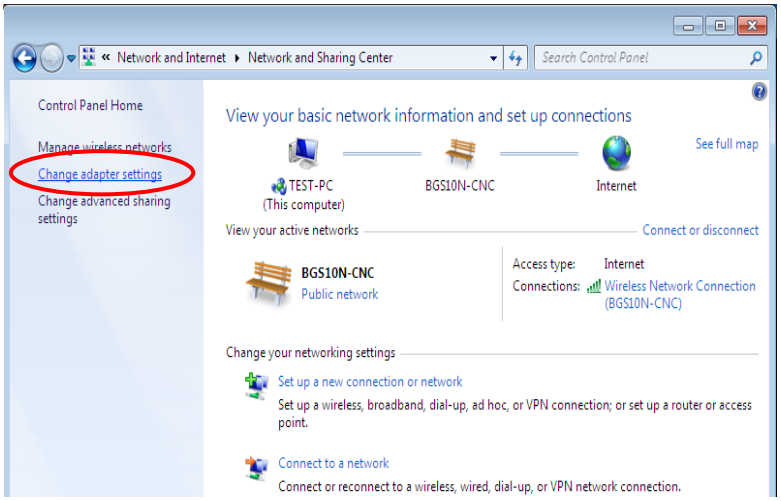
Configuring PC in Windows 7/8 (IPv4)

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

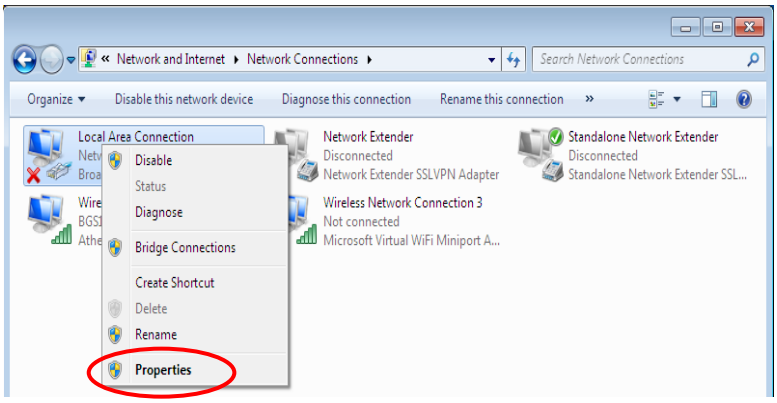
2. Then click on **Network and Internet**.



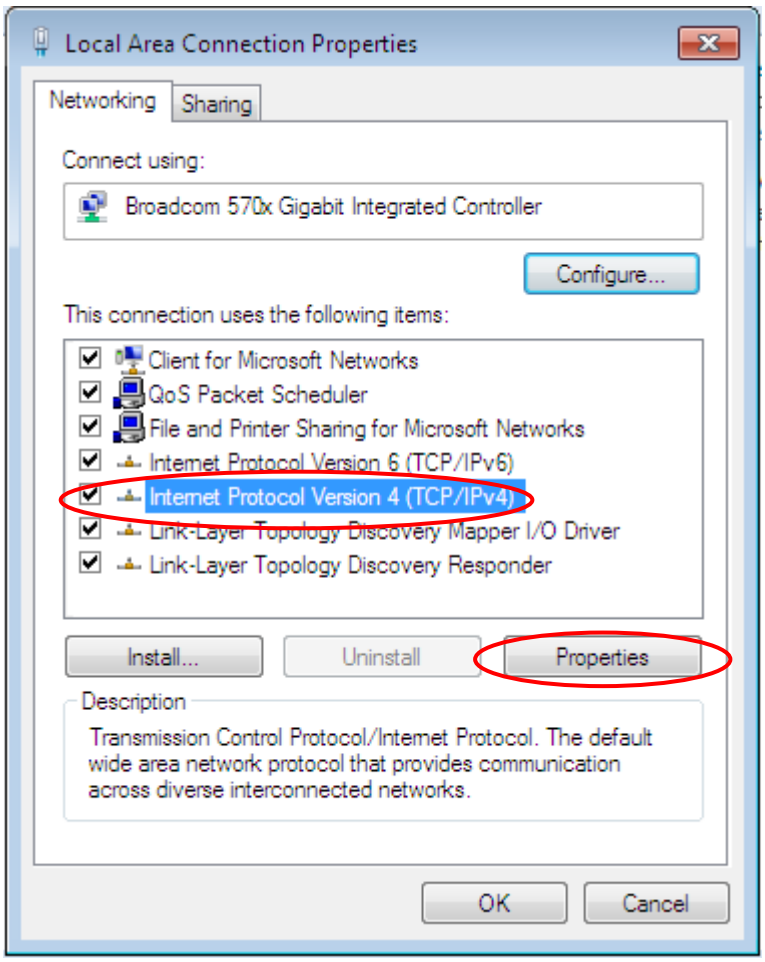
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



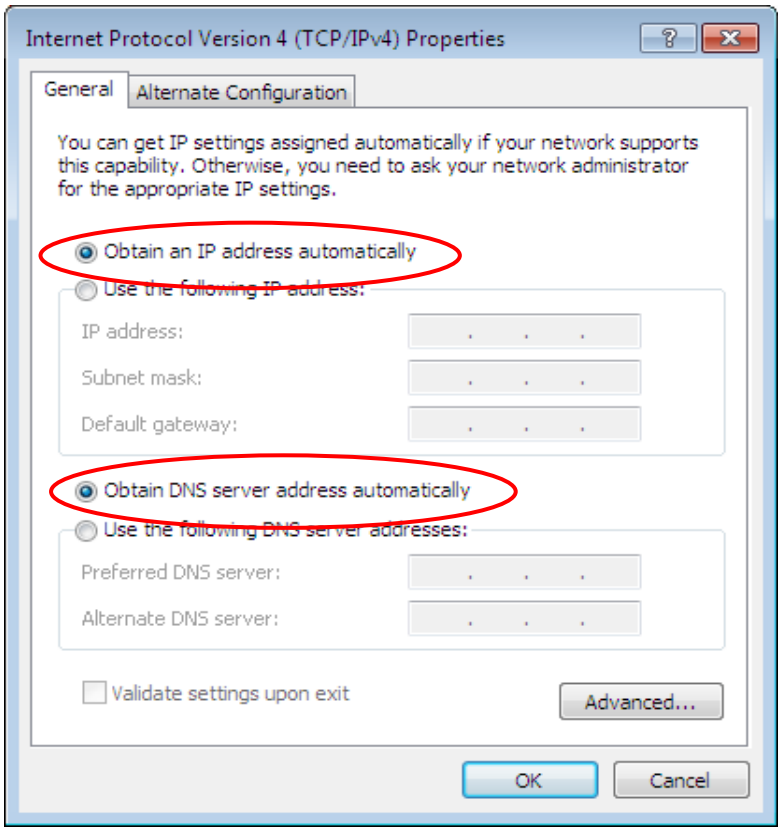
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



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



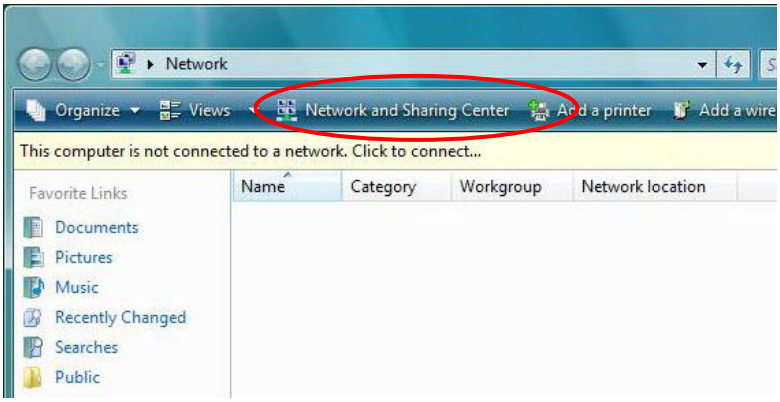
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring PC in Windows Vista (IPv4)

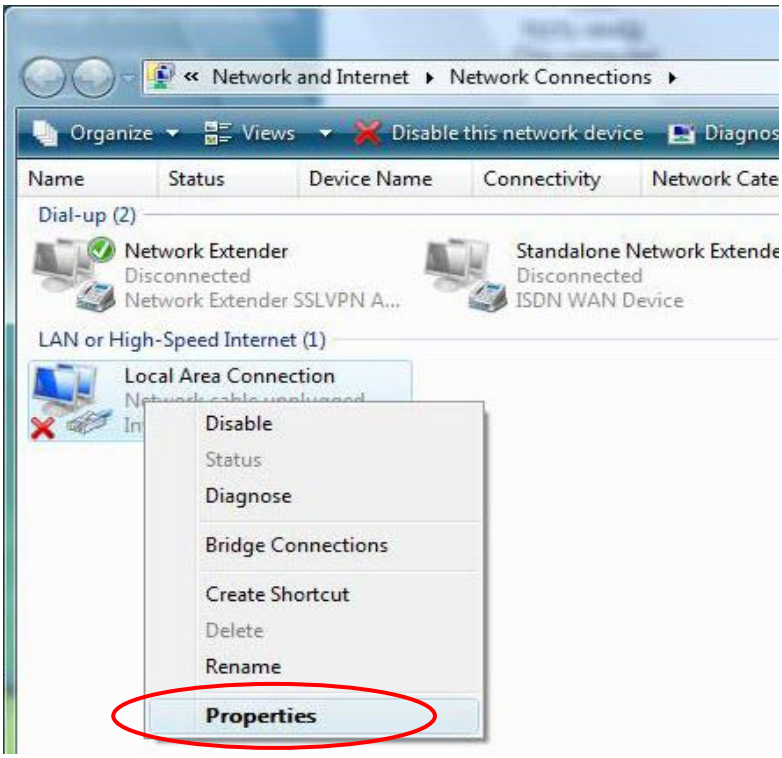
1. Go to **Start**. Click on **Network**.

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

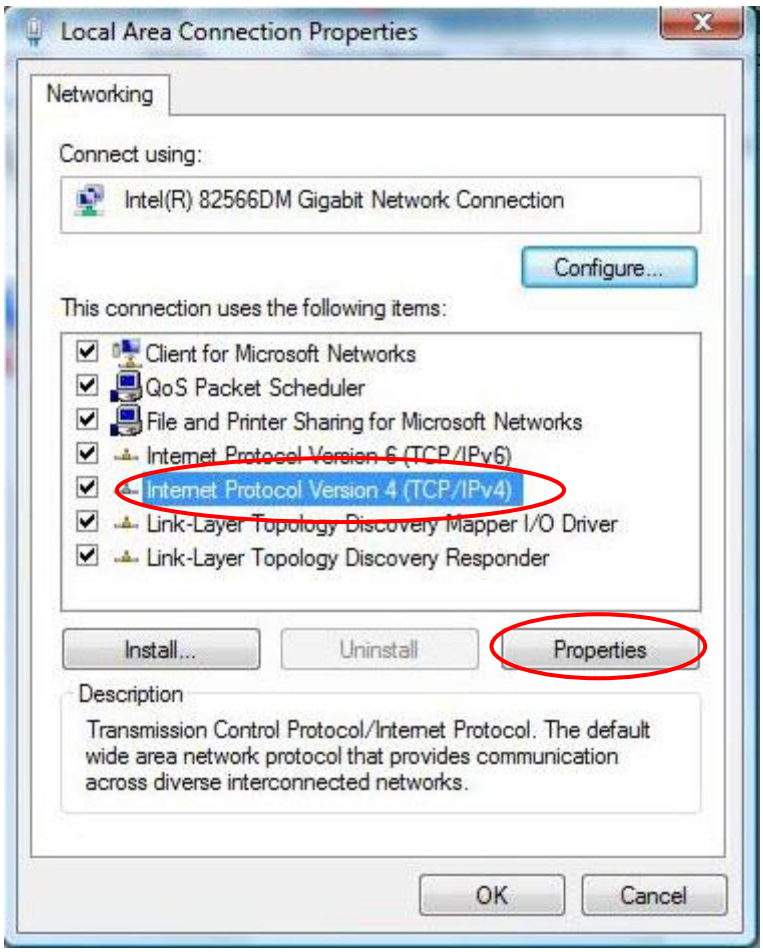


3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window panel.

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

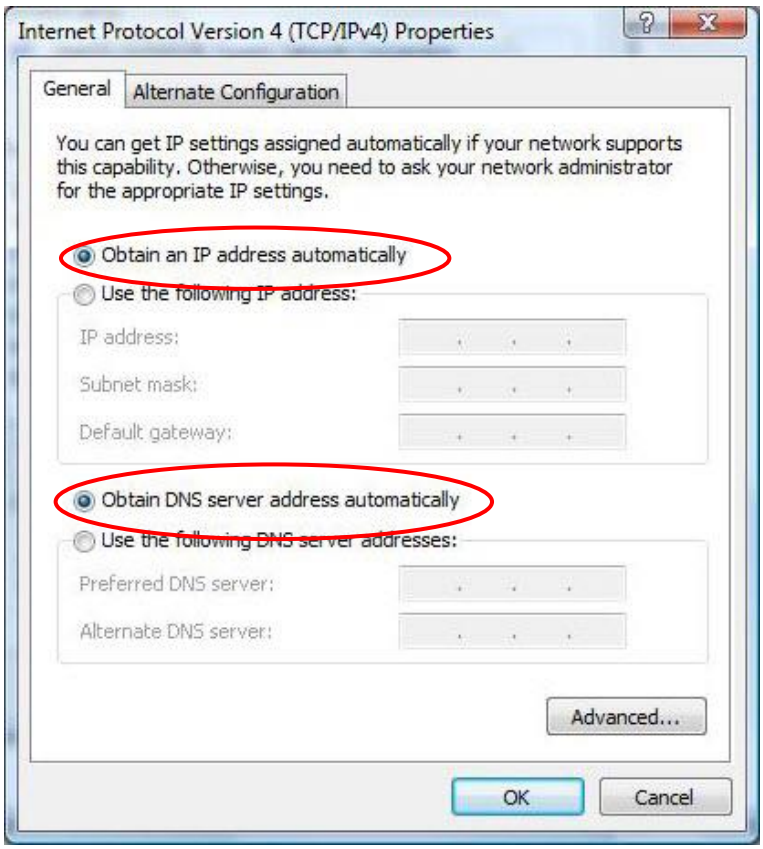


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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.



Network Configuration – IPv6

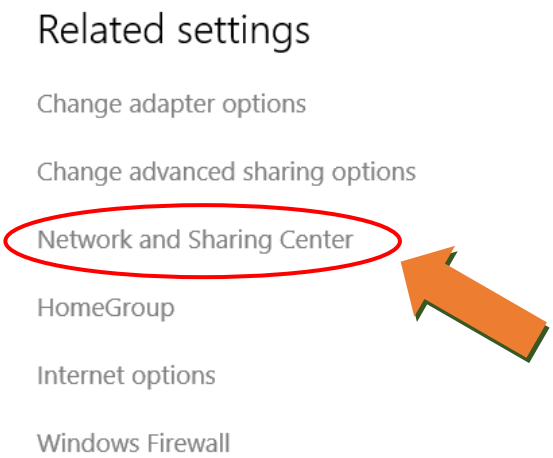
Configuring PC in Windows 10 (IPv6)

1. Click .

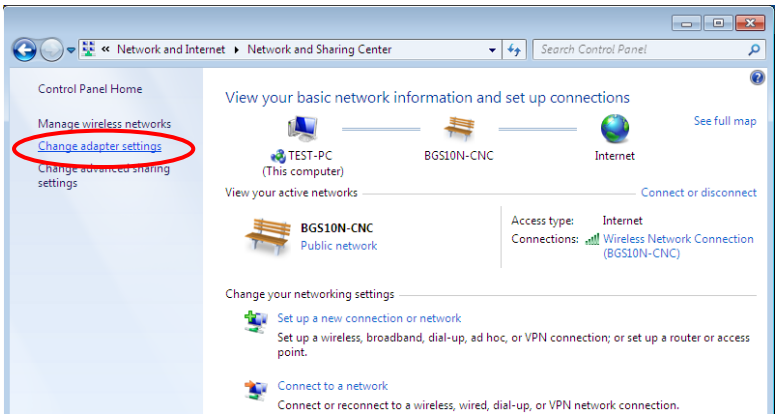
2. Click Settings

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

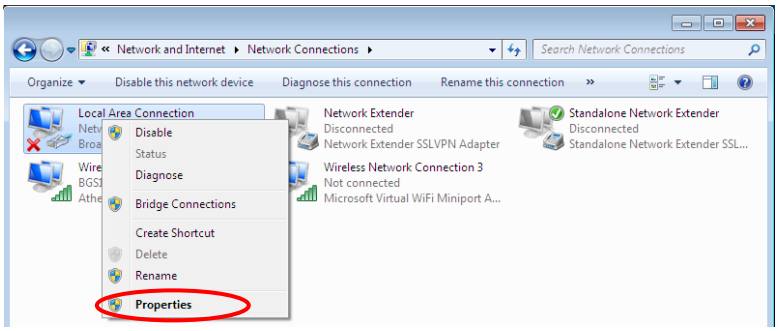
4. Under **Related settings,** select **Network and Sharing Center**



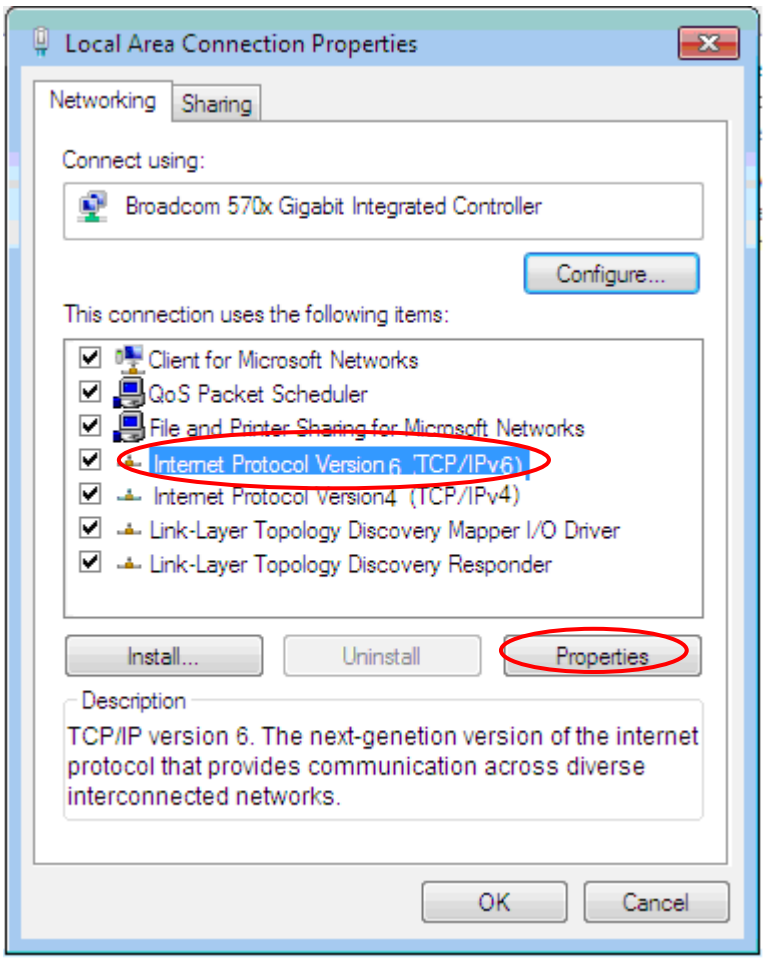
5. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

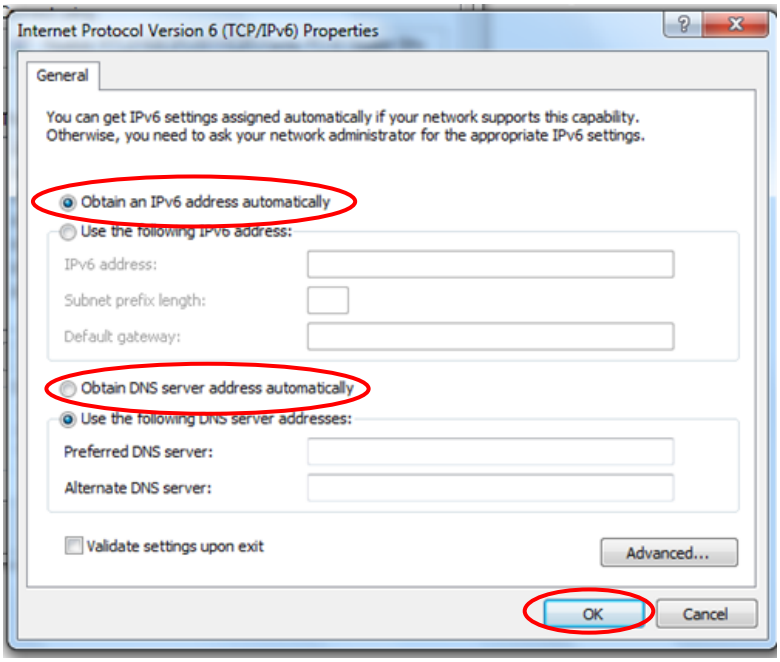


7. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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

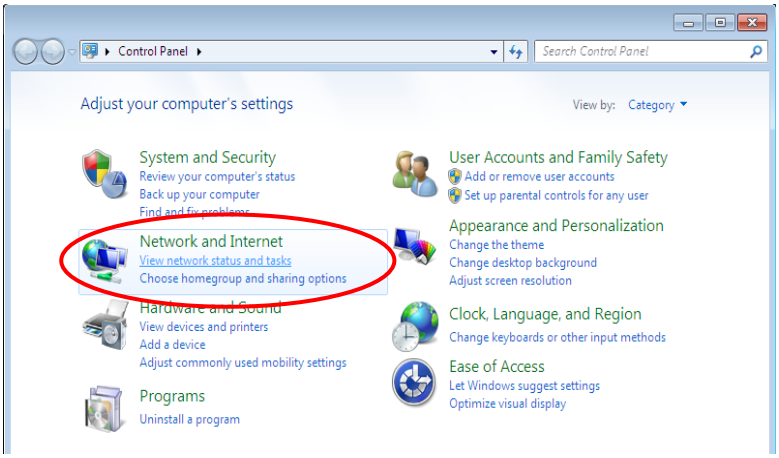
9. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



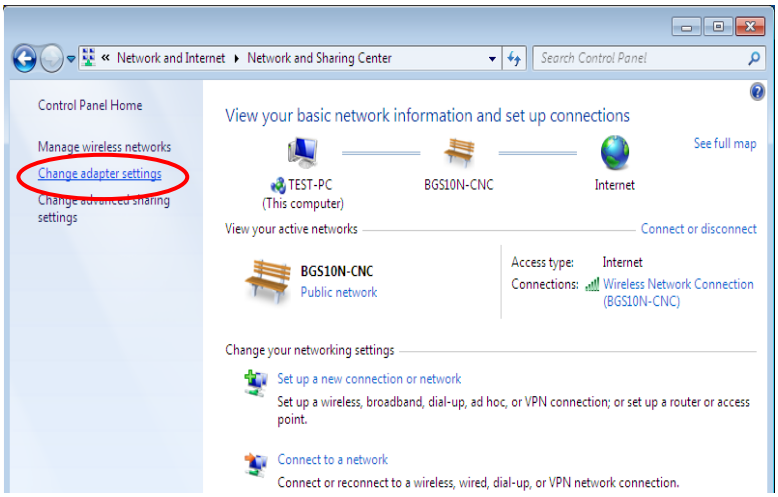
Configuring PC in Windows 7/8 (IPv6)

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

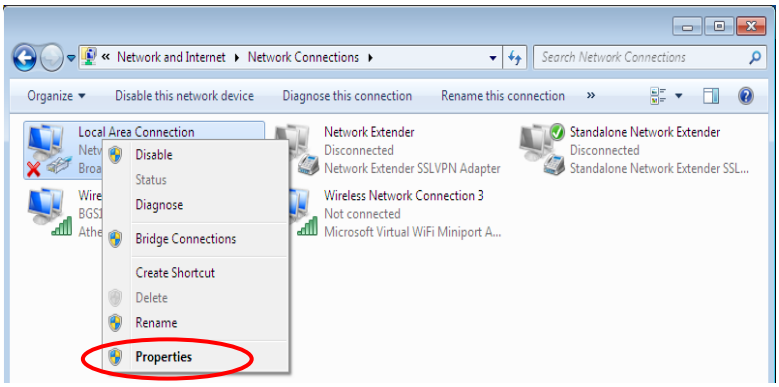
2. Then click on **Network and Internet**.



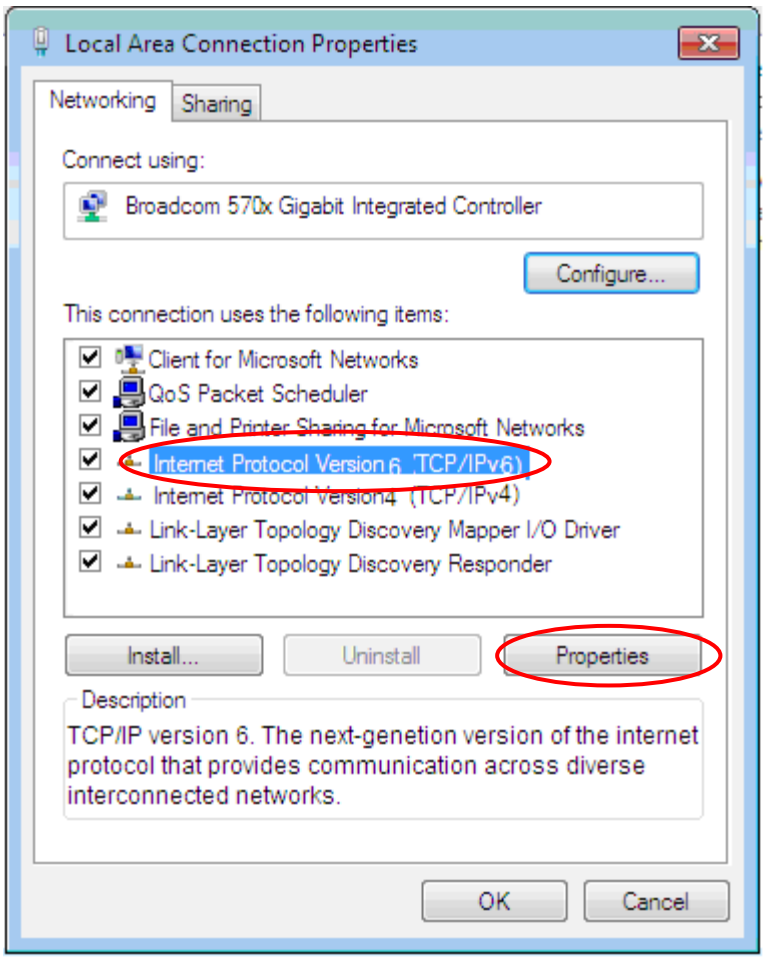
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

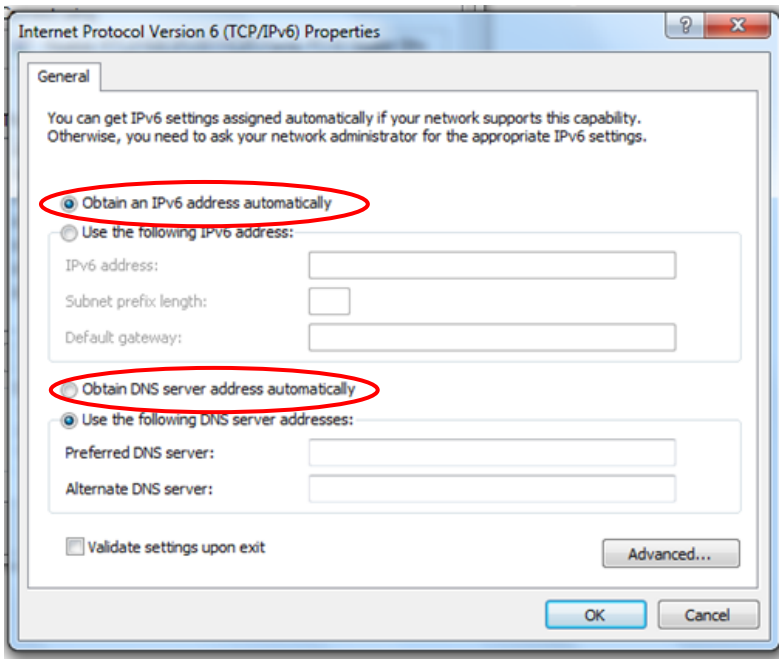


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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

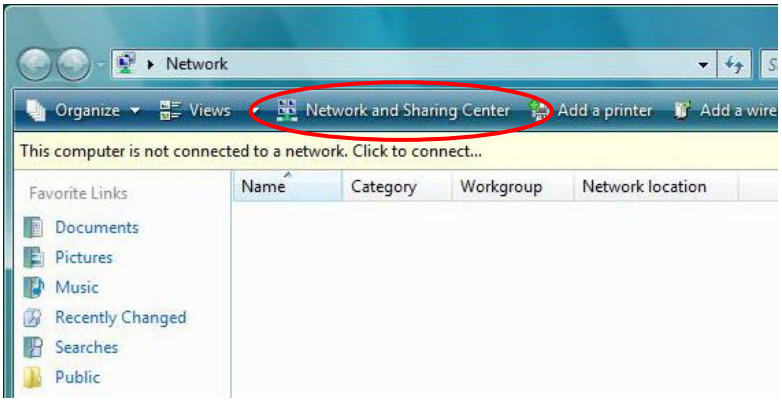
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



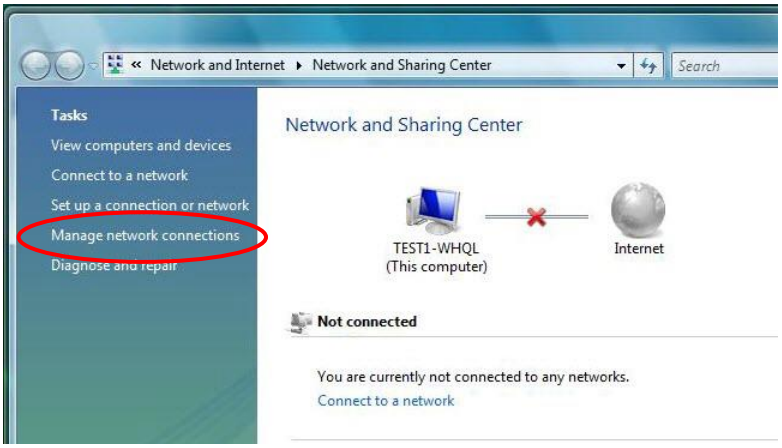
Configuring PC in Windows Vista (IPv6)

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

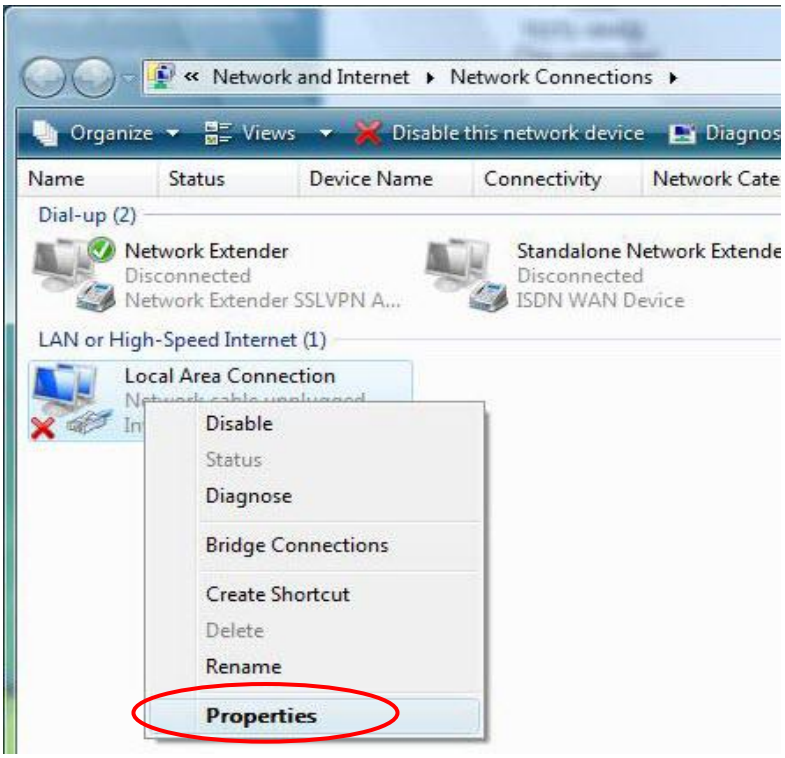
2. Then click on **Network and Sharing Center** at the top bar.



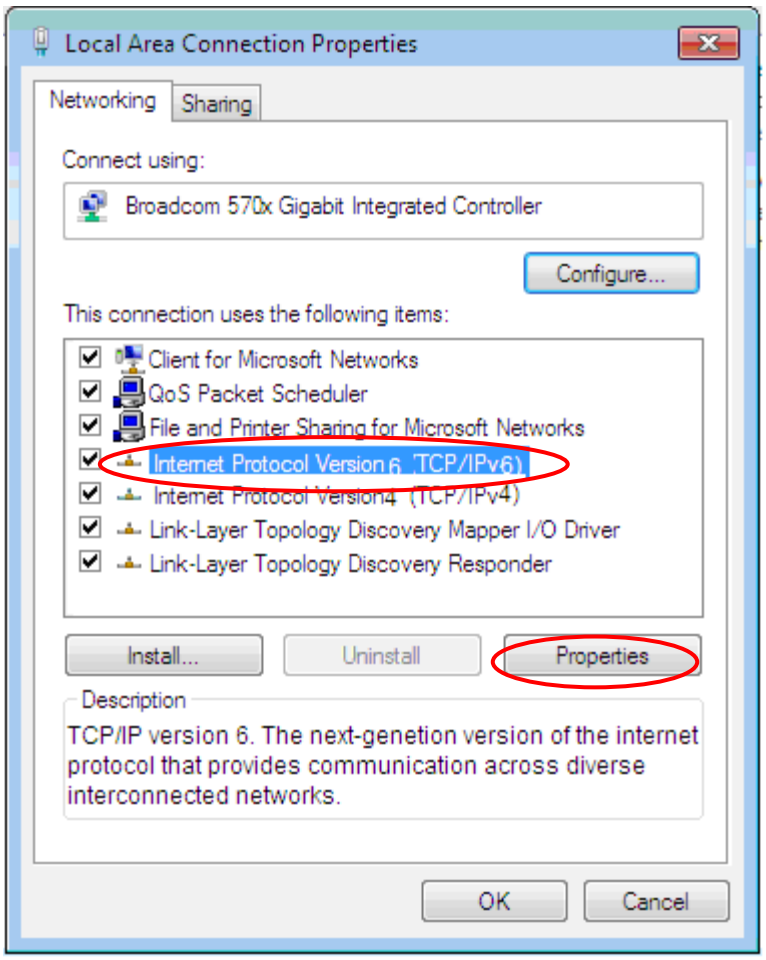
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window panel.



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

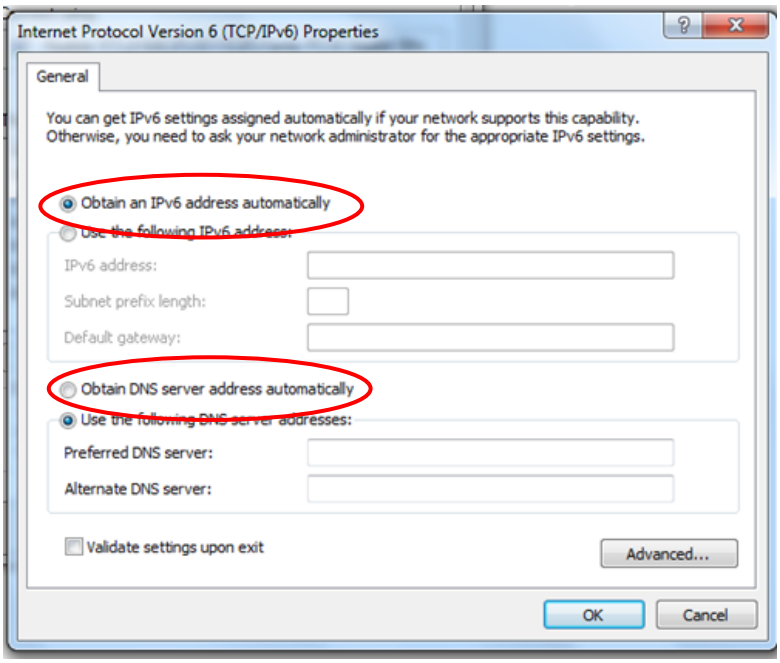


5. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



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

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



Default Settings

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

Web Interface: (Username and Password)

Administrator

- ✔ Username: admin
- ✔ Password: admin

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

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

Device LAN IP Settings

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

DHCP Server:

- ✔ DHCP server is enabled.
- ✔ Start IP Address: 192.168.1.100
- ✔ IP pool counts: 100

Information from Your ISP

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

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

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

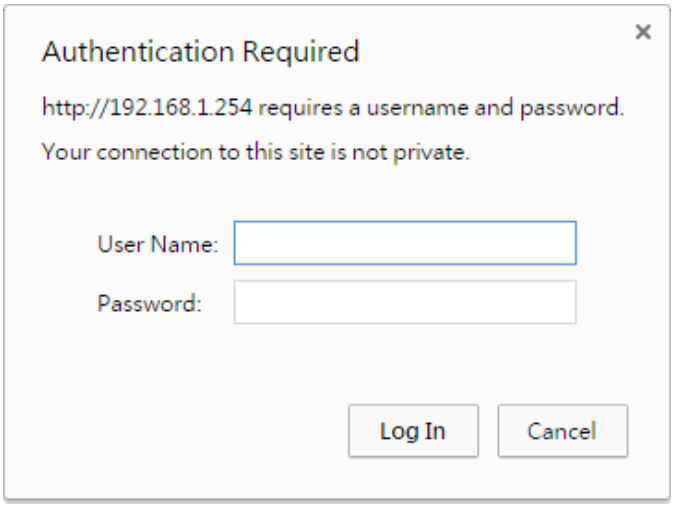
CHAPTER 4: DEVICE CONFIGURATION

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 & password is "**admin**" & "**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 4700A/AZ

Once you have logged on to your BEC 4700A/AZ via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration
Sub-Items	**Device Info** **System Status** **System Log** **4G-LTE Status (4700AZ)** **Wireless Status** **Hotspot Status** **Statistics** **DHCP Table** **IPSEC Status** **PPTP Status** **L2TP Status** **GRE Status** **OpenVPN Status** **ARP Table** **VRRP Status**		**Interface Setup** - Internet - LAN - Wireless 2.4G / 5G - Wireless 2.4G / 5G MAC Filter - Wireless 5G Repeater - Loopback **Dual WAN (4700AZ)** - General Setting - Outbound Load Balance - Protocol Binding **Hotspot** - General Setting - Built-in User Account - Authorized of Client - Walled Garden - Advertisement - Hotspot Status Log - Customization **Advanced Setup** - Firewall - Routing - Dynamic Routing - NAT - VRRP - Static DNS - QoS - Interface Grouping (4700AZ) - Port Isolation - Time Schedule - Mail Alert **VPN** - IPSec - PPTP Server & Client - L2TP - GRE - OpenVPN Server / Client **Access Management** - Device Management - SNMP - Syslog - Universal Plug & Play (UPnP) - Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - BECentral Management **Maintenance** - User Management - Certificate Management - Time Zone - License

			- Firmware & Configuration - System Restart - Auto Reboot - Diagnostic Tool

Please see the relevant sections of this manual for detailed instructions on how to configure your **BEC 4700A/AZ**.

Status

Device Info

It provides brief status summary of the device.

Device Information

Model Name	BEC 4700A
Firmware Version	1.04.1.348
MAC Address	00:04:ed:47:01:10
Date-Time	Mon Apr 10 01:41:22 2017
System Up Time	1 hour 41 mins

Physical Port Status

EWAN	✗
Ethernet	✓
Wireless 2.4G	✓
Wireless 5G	✓

WAN

Interface	Protocol	Connection	IP Address	Default Gateway
EWAN ▼	PPPoE	Not Connected	/	

LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.199 Enable / Stateless

Wireless 2.4G

Mode	SSID	Channel	Security
802.11b+g+n	BEC110	6	Mixed WPA2/WPA-PSK

Wireless 5G

Mode	SSID	Channel	Security
802.11ac	BEC111	153	Mixed WPA2/WPA-PSK

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router.

MAC Address: A unique number that identifies the router.

Data Time: Setup correct time on the **BEC 4700A/AZ** with your PC. Check on **Time Zone** section for more configuration information.

System Uptime: Display how long the **BEC 4700A/AZ** has been powered on.

Physical Port Status

Physical Port Status：Display available connection interfaces supported in the 4700A/AZ.

WAN

Interface: List current available WAN connections.

Protocol: Display selected WAN connection protocol

Connection: The current connection status.

IP Address: WAN port IP address.

Default Gateway: The IP address of the default gateway.

LAN

IP Address: LAN port IPv4 address.

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

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

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

Wireless

Mode: Display selected Wireless mode.

SSID: Display the name of the Wireless AP(s) to use.

Channel: Display radio frequency to be used for this wireless link.

Security: Display security method to be used for this wireless link.

System Status

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

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

CPU

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

System Log

```
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!
```

Refresh 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	
Status	Down
SIM Status	
Signal Strength	
Network Name	
Cell ID	
Card IMEI	
Card IMSI	
SIM Card Number (ICCID)	
Network Mode	
Network Band	
Auto Refresh	Disable ▼
Refresh	

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

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

Signal Strength: The signal strength bar and dBm value indicates the current 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.

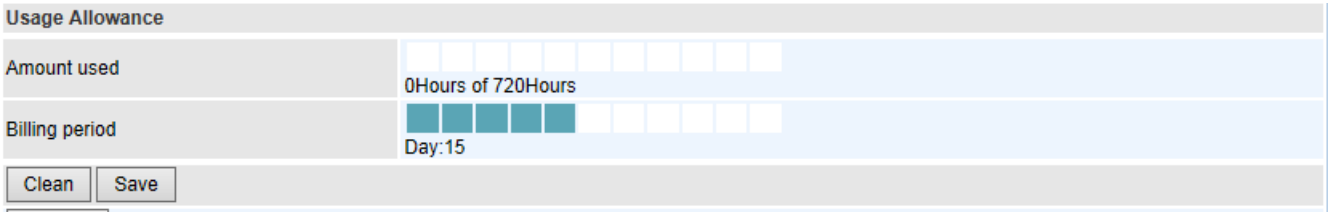
Network Band: Indicated the current radio frequency band used.

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

Refresh: Click to refresh the statistics.

Usage Allowance

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



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.

Wireless Status

Wireless Status

Wireless 2.4G Status

MAC	SSID	RSSI	Rx Rate	Tx Rate	Connected Time	Host Name	IP Address	Expire Time

Wireless 5G Status

MAC	SSID	RSSI	Rx Rate	Tx Rate	Connected Time	Host Name	IP Address	Expire Time
[redacted]:fe	BEC111	-69	325 Mbps, MCS:7, 80 MHz	260 Mbps, MCS:5, 80 MHz	00:00:9	[redacted]	192.168.1.100	0 days 23:59:50

Wireless 5G Repeater Status

MAC	SSID	RSSI	Connected Time

Refresh

MAC: The MAC of the connected wireless device.

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

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

RX / TX Rate: Display the current data reception (RX) and transmission (TX) rate, in Mbps, of the Wi-Fi client can use. Also display the MCS (Modulation and Coding Scheme) index and Channel Bandwidth are used.

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

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

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

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

Refresh: Click to refresh the statistics.

Hotspot Status

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

Hotspot Status

Action	MAC Address	IP Address	Authenticated	User Name	Duration Time	Idle Time	Upload Bandwidth	Download Bandwidth	Download Data Usage	Upload Data Usage	Total Data Usage
Drop	98:01:A7:5B:4D:1C	10.0.0.3	Not	-	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Drop	38:89:2C:17:4E:FE	10.0.0.2	Authorized	-	22/3600	2/180	0%/0	0%/0	0/0	0/0	0/0

Refresh

Action: Click **Drop** to terminate the Wi-Fi connection of the client to the wireless network.

MAC Address: The MAC of the connected wireless device.

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

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

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

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

Idle Time (current idle time / total idle timeout period): Display current idle time of the Wi-Fi device. If it reaches to total idle timeout period, the Internet connection will get disconnected immediately.

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

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

Refresh: Click to refresh the statistics.

Statistics

❖ 4G-LTE Status

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

Statistics			
Traffic Statistics			
Interface	◉ 3G/4G-LTE Status ○ EWAN ○ Ethernet ○ Wireless 5G		
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 None ▾

Traffic Statistics

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

Statistics			
Traffic Statistics			
Interface	◉ EWAN ○ Ethernet ○ Wireless 5G		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	0	Receive Frames	0
Transmit Multicast Frames	0	Receive Multicast Frame	0
Transmit Total Bytes	0	Receive Total Bytes	0
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.00KBps	Receive Speed	0.00KBps
Refresh			Auto Refresh None ▼

Traffic Statistics

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

Transmit Statistics

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

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

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

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

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

Receive Statistics

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

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

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

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

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

Traffic Speed

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

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

Refresh: Click to manually refresh the data.

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

❖ Ethernet

Statistics

Traffic Statistics			
Interface	○ EWAN ◉ Ethernet ○ Wireless 5G		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	9885	Receive Frames	7710
Transmit Multicast Frames	1896	Receive Multicast Frame	462
Transmit Total Bytes	8735356	Receive Total Bytes	829147
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0
Traffic Speed			
Transmit Speed	0.28KBps	Receive Speed	0.26KBps
Refresh			Auto Refresh 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 Broadband Internet Service Provider.

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

Refresh: Click to manually refresh the data.

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

❖ Wireless 2.4G/5G

Statistics			
Traffic Statistics			
Interface	○ EWAN ○ Ethernet ◉ Wireless 5G		
Transmit Statistics		**Receive Statistics**	
Transmit Frames	5315	Receive Frames	5235
Transmit Error Frames	0	Receive Error Frames	0
Transmit Drop Frames	0	Receive Drop Frames	0
Traffic Speed			
Transmit Speed	0.12KBps	Receive Speed	0.08KBps
Refresh		Auto Refresh	None ▼

Traffic Statistics

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

Transmit Statistics

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

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

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

Receive Statistics

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

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

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

Traffic Speed

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

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

Refresh: Click to manually refresh the data.

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

DHCP Table

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

DHCP Table

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

Index #: The indication of the rule number.

Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

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

IPSec Status

IPSec Status

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

Refresh

Index #: The numeric IPSec VPN tunnel/ rule.

Action: Display Connect or Drop the connection.

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

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

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

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

Remote Gateway: Display remote gateway IP address.

Remote Network: Display remote local IP address and Netmask.

Local Network: Display local IP address and Netmask.

Refresh: Click to refresh the page.

PPTP Status

❖ PPTP Server

PPTP Status

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

Refresh

Index #: The numeric PPTP VPN tunnel/ rule.

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

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

Connection State: Display the VPN connection status.

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

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

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

Refresh: Click to refresh the page.

❖ PPTP Client

PPTP Status

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

Refresh

Index #: The numeric PPTP VPN tunnel/ rule.

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

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

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

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

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

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

Refresh: Click to refresh the page.

L2TP Status

L2TP Status

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

Refresh

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

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

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

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

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

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

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

Refresh: Click to refresh the page.

GRE Status

GRE Status

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

Index #: The numerical GRE tunnel/rule indication.

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

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

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

Remote Gateway IP: Display the remote gateway IP address.

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

OpenVPN Status

❖ OpenVPN Server

OpenVPN Status

OpenVPN Server					
Index	Connection Name	Active	Service Port	Tunnel Network	Status
1	OpenVPN1	Yes	1194 /udp	192.168.100.0 /255.255.255.0	Ready
OpenVPN Client					
Index	Connection Name	Active	Remote Server	Status	Detail Info

Refresh

Index #: The numeric OpenVPN tunnel/ rule.

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

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

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

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

Status: Display the status of the profile/rule

Refresh: Click to refresh the page.

❖ OpenVPN Client

OpenVPN Status

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

Refresh

Index #: The numeric OpenVPN tunnel/ rule.

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

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

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

Status: Display the status of the profile/rule

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

Refresh: Click to refresh the page.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall - MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

ARP Table

#	IP	MAC Address
1	192.168.1.11	[redacted]

Index #: The indication of the APR table number.

IP Address: It is IP Address of internal host that join this network.

MAC Address: The MAC address of internal host.

VRRP Status

VRRP Status

Current Status	N/A
Current Master	N/A

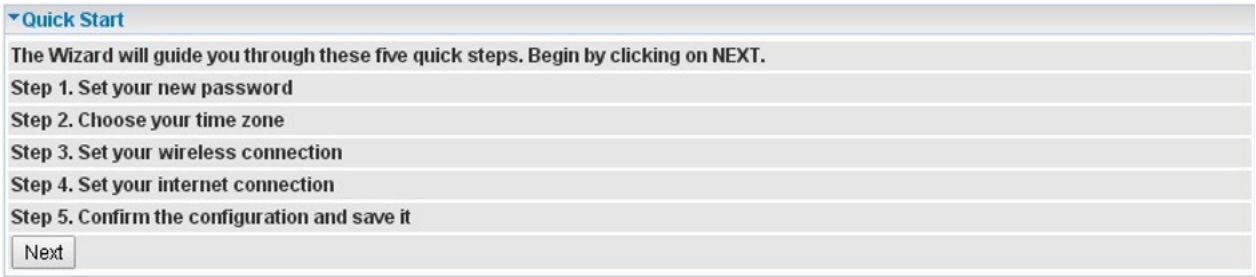
Current Status: Display current VRRP status, Master or Backup.

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, wireless, and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

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



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

Step 2 – Time Zone

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

Step 3 – Wireless

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

Quick Start - Wireless

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

Access Point	Activated / Deactivated
SSID	BEC345
Broadcast SSID	Yes / No
Channel	UNITED STATES / 06
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	TKIP+AES
Pre-Shared Key	842CFFDE (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)

Back Next

Step 4 – ISP Connection Type

Set up your WAN Internet connection.

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

Quick Start - ISP Connection Type

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

WAN Interface	4G/LTE

Back Next

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

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

Quick Start - 3G/4G-LTE

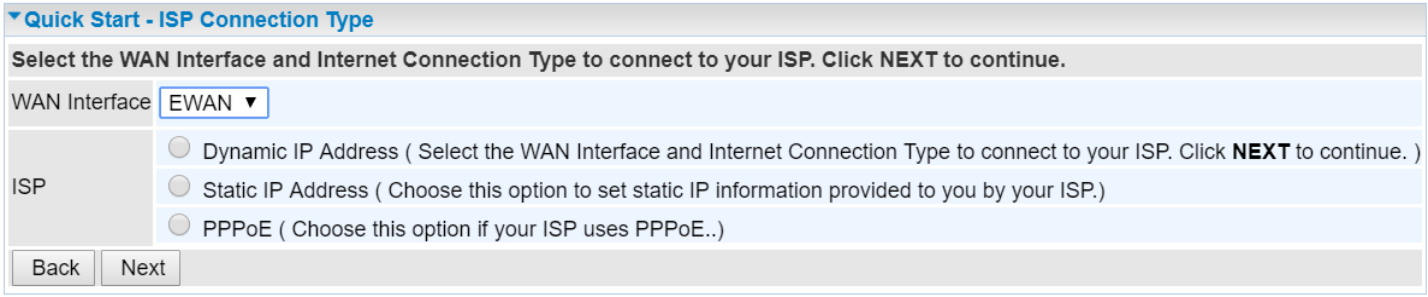
Enter the 3G information provided to you by your ISP. Click NEXT to continue.

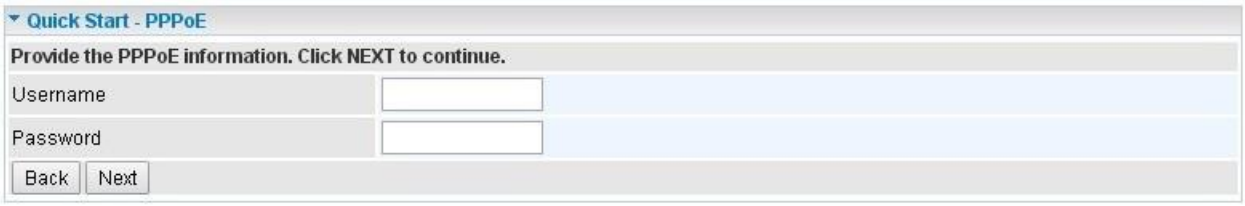
TEL No.	*99***1#
APN	internet
Username	
Password	
PIN	

Back Next

Click **Next** to save changes.

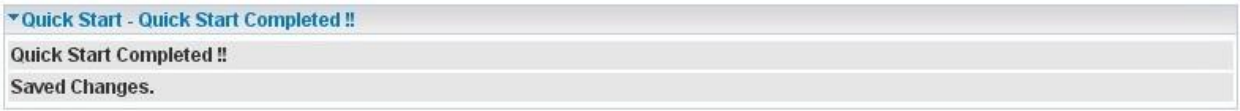
4.3 If selected **EWAN / PPPoE**, please enter PPPoE account information provided by your ISP. Click **NEXT** to continue.





Step 5 – Quick Start Completed

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



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

Configuration

Click to access and configure the available features in the following: **Interface Setup, Dual WAN (4700AZ), Hotspot, Advanced Setup, VPN, Access Management,** and **Maintenance.**

These functions are described in the following sections.

Interface Setup

Here are the features under **Interface Setup**: Internet, LAN, Wireless 2.4G, Wireless MAC Filter, Wireless 5G, Wireless 5G MAC Filter, Wireless 5G Repeater, and Loopback.

Internet

❖ **4G/LTE**

❖ **4G/LTE (Cont.)**

Internet

WAN Interface	4G/LTE
Status	Activated / Deactivated
Usage Allowance	Enable
IP Pass-Through Mode	Enable
Network Mode	Automatic
TEL No.	*99***1#
Dual APN	Single APN
APN	
Authentication Protocol	Disable
Username	
Password	
PIN	
Connection	Always On (Recommended)
Keep Alive	Yes / No
Keep Alive IP	Check Interval 5 x 1 Seconds
Background Ping	Yes / No
Background Ping IP	Interval Seconds
Default Route	Yes / No
Second APN as Default Route	Yes / No
NAT	Enable
MTU	1428 (0 means use default:1500)

Save

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

Usage Allowance: Click **Enable** to activate the feature. Click the link to setup the usage settings.

Usage Allowance

Parameters	
Period	Month / Day
Mode	Volume-based Only Download MB data volume per month/day included Time-based 720 hours per month/day included The billing period always begins on day/o'clock 1 of a month.
Over usage allowance action	None
Save the statistics to ROM	Disable

Save 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.

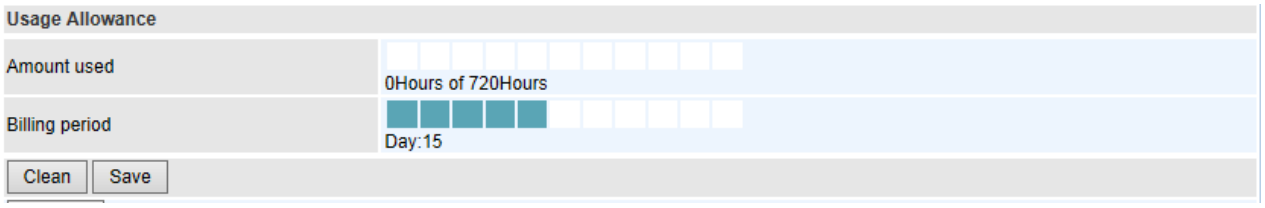
Over usage allowance action: Here are actions to perform when mobile data usage, defined in **Mode**, reached to its maximum.

- **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

IP Pass-Through Mode: When **enabled**, BEC 4700A/AZ is in bridge mode and will not obtain a WAN IP address, features such as routing capabilities, NAT, firewall, etc., will be disabled by default. However, the client router behind the BEC 4700A/AZ can get a WAN IP address instead.

When **disabled**, BEC 4700A/AZ is in router mode that it handles a WAN IP address and all routing-related features become available.

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

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

Dual APN: BEC 4700A/AZ can support up to two (2) APNs, **Single** or **Dual**.

APN: An APN is similar to a URL on the WWW; it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection, requirements for APNs varies between different service providers. Most service providers have an internet portal which they use to connect to a DHCP Server, thus giving you access to the internet i.e. some mobile/cellular operators use the APN 'internet' for their portal. The default value is "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: 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: Enter the IP address that the 4700A/AZ can ping the IP to find whether the connection is on or not, if not, router will recover the connection.

Background Ping: Select **Yes** to keep the 4G/LTE active at all time, prevent 4700A/AZ from entering idle state.

Background Ping IP: Enter the IP address that the 4700A/AZ 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.

MTU: Enter the maximum packet that can be transmitted. Use default 1500 bytes by entering MTU **0**.

❖ EWAN

Internet	
WAN Interface	EWAN ▾
Bandwidth	Upload 1000 Mbps Download 1000 Mbps
Status	◉ Activated ○ Deactivated

Bandwidth: Traffic/data control from WAN to LAN (Downstream) and LAN to WAN (Upload).

Status: Select **Activate** / **Deactivated** to enable / disable the WAN service.

IPv4/IPv6

IPv4/IPv6	
IP Version	○ IPv4 ◉ IPv4/IPv6 ○ IPv6

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

ISP Connection Type

ISP Connection Type	
ISP	○ Dynamic IP Address ○ Static IP Address ◉ PPPoE
802.1q Options	
802.1q	○ Activated ◉ Deactivated
VLAN ID	0 (range: 0~4095)

ISP: Select the encapsulation type your ISP uses.

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

802.1q Options

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

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

Dynamic IP Address (If selected as WAN Connection Type; otherwise, skip this part)

Dynamic IP Address	
IP Common Options	
Default Route	◉ Yes ○ No
TCP MTU Option	TCP MTU 0 bytes(0:default)
IPv4 Options	
NAT	Enable ▼
Client ID	
Vendor ID	
Dynamic Route	RIP1 ▼ Direction None ▼
IGMP Proxy	○ Enable ◉ Disable
IPv6 Options	
IPv6 Message Fetch Type	Dynamic Mode
Obtain IPv6 DNS	◉ Enable ○ Disable
Primary DNS	
Secondary DNS	
MLD Proxy	○ Enable ◉ Disable

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

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

IPv4 Options

NAT: Enable to allow BEC 4700A/AZ to assign private network IPs to all devices in the network for get Internet access.

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

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

Dynamic Route

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

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

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

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

- **Obtain IPv6 DNS:** Choose if you want to obtain DNS automatically.
- **Primary/Secondary:** if you choose Disable in the Obtain IPv6 DNS field, please type the exactly primary and secondary DNS.
- **MLD Proxy:** MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a Multicast Management protocol for IPv6 multicast packets.

Static IP Address (If selected as WAN Connection Type; otherwise, skip this part)

Static IP Address	
IP Common Options	
Default Route	◉ Yes ○ No
TCP MTU Option	TCP MTU 0 bytes(0:default)
IPv4 Options	
Static IP Address	
IP Subnet Mask	
Gateway	
Primary DNS	
Secondary DNS	
NAT	Enable ▼
Dynamic Route	RIP1 ▼ Direction None ▼
IGMP Proxy	○ Enable ◉ Disable
IPv6 Options	
IPv6 Message Fetch Type	Static Mode
IPv6 Address	/
IPv6 Default Gateway	
Obtain IPv6 DNS	○ Enable ◉ Disable
Primary DNS	
Secondary DNS	
MLD Proxy	○ Enable ◉ Disable

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

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

IPv4 Options

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

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

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

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

NAT: Enable to allow BEC 4700 to assign private network IPs to all devices in the network for get Internet access.

Dynamic Route

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

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

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

- **IPv6 Address/Default Gateway:** Type the WAN IPv6 address and gateway IP from your ISP.
- **Obtain IPv6 DNS:** Choose if you want to obtain DNS automatically.
- **Primary/Secondary:** if you choose Disable in the Obtain IPv6 DNS field, please type the exactly primary and secondary DNS.
- **MLD Proxy:** MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a Multicast Management protocol for IPv6 multicast packets.

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

IP Options	
IP Common Options	
Default Route	Yes No
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)
IPv4 Options	
Get IP Address	Static Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable
Dynamic Route	RIP1 Direction None
IGMP Proxy	Enable Disable
IPv6 Options	
IPv6 Address	/
Obtain IPv6 DNS	Enable Disable
Primary DNS	
Secondary DNS	
MLD Proxy	Enable Disable

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

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

IPv4 Options

Get IP Address: Choose Static or Dynamic

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

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

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

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

Dynamic Route

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

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish

membership in a Multicast group. Choose whether enable IGMP proxy.

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

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

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

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

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

Click **Save** to apply settings.

LAN

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

IPv4 Parameters

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 ▼

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

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

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

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

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

Dynamic Route:

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

DHCPv4 Server

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

DHCPv4 Server	
DHCPv4 Server	○ 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	

DHCPv4 Server: If set to **Enabled**, your BEC 4700A/AZ 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 4700A/AZ acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- When DHCP is used, the following items need to be set.

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

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

Lease Time: The current lease time of client.

DNS Relay:

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

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

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

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

Fixed Host

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

Fixed Host	
IP Address	
MAC Address	

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 Address	MAC Address	Delete
1	192.168.1.110	00:04:ED:01:01:10	

IPv6 Parameters

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

IPv6 Parameters	
Interface Address/Prefix Length	/
MLD Snooping	Activated Deactivated
DHCPv6 Server	
DHCPv6 Server	Disable Enable
DHCPv6 Server Type	Stateless Stateful
Start Interface ID	
End Interface ID	
Lease Time	seconds(0 sets to default value of 4800)
Router Advertisements	Disable Enable

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	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

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: Click **Enable** to activate the DHCPv6 server.

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

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

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

End interface ID: enter the end interface ID.

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

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

Click **Save** to apply settings.

Wireless 2.4GHz

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

NOTE: WLAN (or BEC)1 / 2 / 3 / 4 Interface refers to as SSID1 / 2 / 3 / 4 Wi-Fi networks.

Access Point Settings

Wireless 2.4G | Site Survey

Access Point Settings	
Access Point	(•) Activated ( ) Deactivated
AP MAC Address	00:04:ED:45:00:04
Wireless Mode	802.11b+g+n ▼
Channel	UNITED STATES ▼ 06 ▼ Current Channel : 6
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
TX Power	100 (range:1~100)
IGMP Snooping	(•) Yes ( ) No

Site Survey: Click to view all other available Wireless-AP devices near the BEC 4700A/AZ.

Wireless 2.4G

Site Survey

CH	SSID	BSSID	Security	Signal (%)
1	J M	[redacted]cc:28	WPA1PSK/WPA2PSK	0
4	DTS	[redacted]66:bb	WPA1PSK	0
5	wlan-ap	[redacted]ee:d4	WPA1PSK/WPA2PSK	100

Refresh | Back

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

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

AP MAC Address: The MAC address of wireless AP.

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

802.11b and if you only have 802.11n then select **802.11n**.

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

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

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

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

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

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

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

11n Settings

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

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

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

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

MCS (Modulation and Coding Scheme): There are options **0~7** and **AUTO** to select from. **AUTO** is most recommended.

SSID Settings

SSID Settings	
Available SSID	1 ▼
SSID Index	◉ SSID1
SSID	BEC223
Broadcast SSID	◉ Yes ○ No
Clients Isolation	○ Yes ◉ No
SSID Activated	Always ▼

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

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

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

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

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

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

Security Settings

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

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

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

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

Security Type - WEP

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

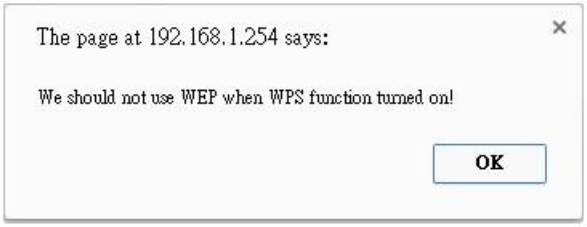
WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

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

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

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

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



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

Security Type - WPA-PSK / WPA2-PSK / Mixed WPA & WPA2

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

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

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

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

WDS Settings

WDS Settings	
AP MAC Address	60:03:47:23:F2:00
WDS Mode	Activated Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00

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

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

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

Click **Save** to apply settings.

Wireless MAC Filter

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

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

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

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

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

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

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

Click Save to apply settings.

Wireless 5GHz

Access Point Settings

Wireless 5G	Site Survey
Access Point	Activated / Deactivated
AP MAC Address	00:04:ED:47:01:11
Channel	UNITED STATES ▼ 153 ▼ Current Channel 153
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
Channel Bandwidth	20 MHz ▼

Site Survey: Click to view all other available Wireless-AP devices near the BEC 4700A/AZ.

Wireless 5G

Site Survey

CH	SSID	BSSID	Security	RSSI
153		[redacted]75	WPA2	6
153	wlan-ap_5G	[redacted]d5	WPA/WPA2	26

Refresh Back

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

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

AP MAC Address: The MAC address of wireless AP.

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

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

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

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

a value between 1500 and 2347.

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

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

Channel Bandwidth: Select **20 MHz, 40 MHz** or **80MHz** for the channel bandwidth. The wider the Channel bandwidth the better the performance will be.

SSID Settings

SSID Settings	
SSID index	1 ▼
SSID	BEC111
Broadcast SSID	◉ Yes ○ No
Clients Isolation	○ Yes ◉ No

SSID Index: 5GHz only support up to 1 SSID.

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

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

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

WPS Settings

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: PIN Method (Personal Information Number) & PBC Method (Push Button Configuration). BEC 4700A/AZ offers PIN Method only.

WPS Settings	
Use WPS	◉ Yes ○ No
WPS state	Configured
WPS mode	◉ PIN code
AP PIN code	40982205 Generate
Enrollee PIN code	
WPS progress	WPS_INITIAL Start WPS

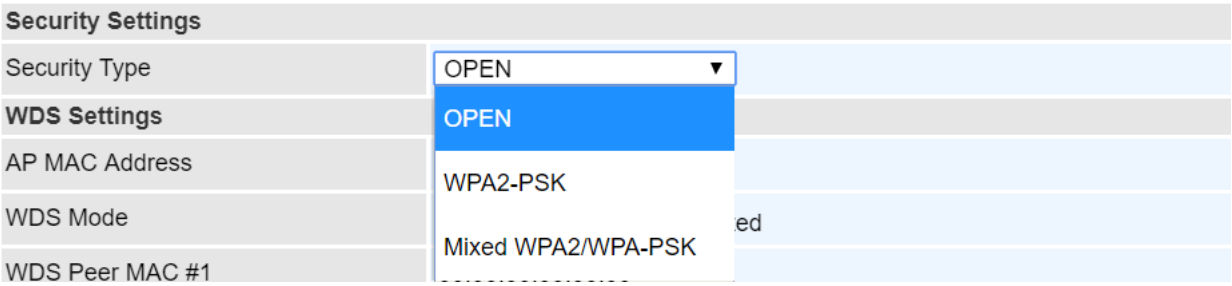
Use WPS: Yes to enable the WPS.

WPS State: Configured means Wi-Fi clients will use the default security setting of the SSID.

WPS Mode: Pin Code means enrollee PIN code is required.

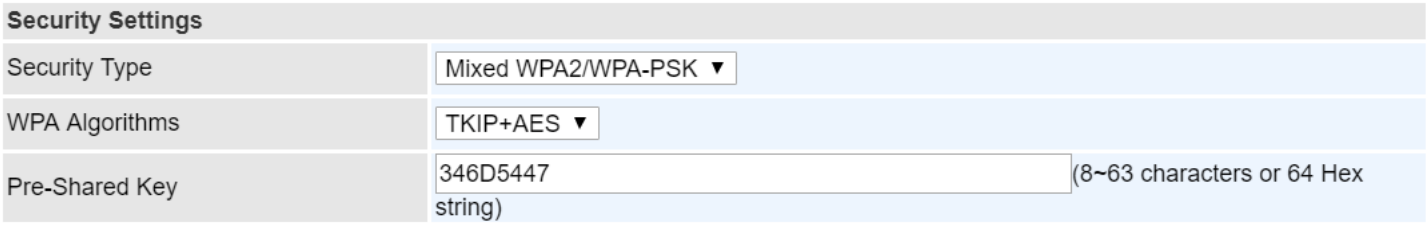
WPS Progress: Click **Start WPS** to begin the WPS pairing process.

Security Settings



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

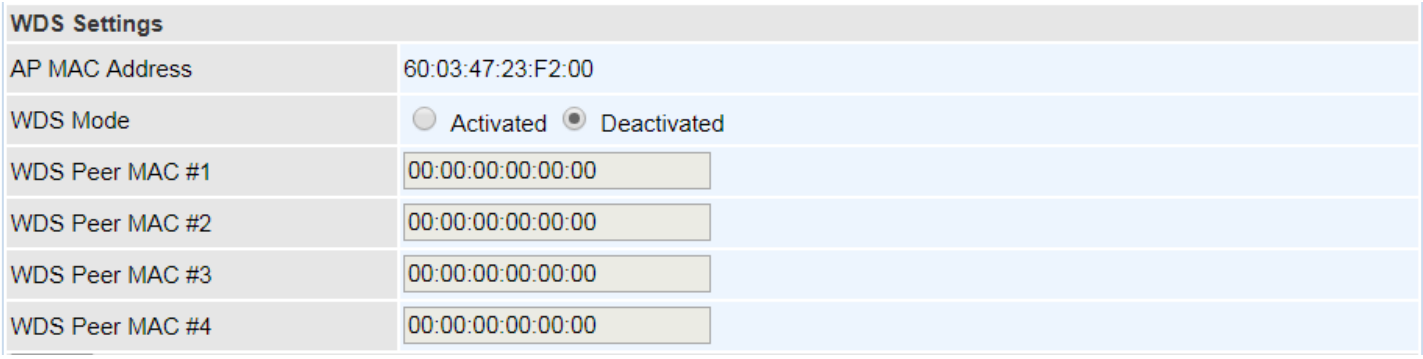
Security Type - WPA-PSK / WPA2-PSK / Mixed WPA & WPA2



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

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

WDS Settings



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

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

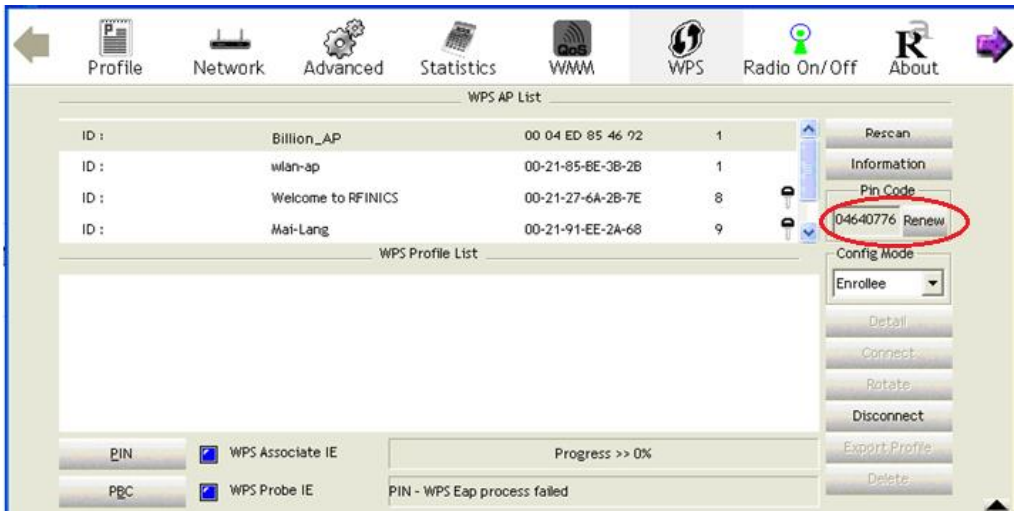
MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.

Click **Save** to apply settings.

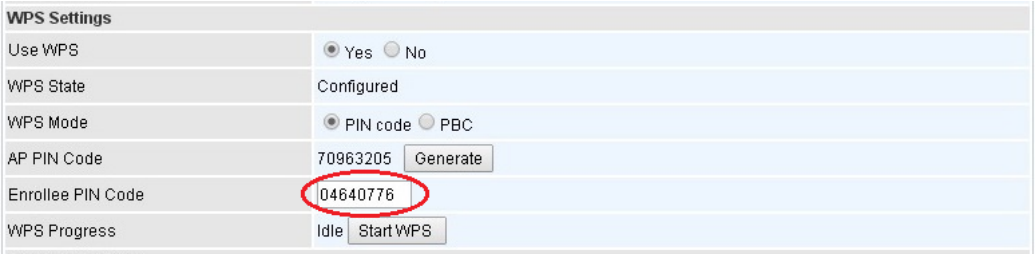
Example: WPS using PIN Method (Personal Information Number)

PIN Method – Configure BEC 4700A/AZ as a Registrar

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



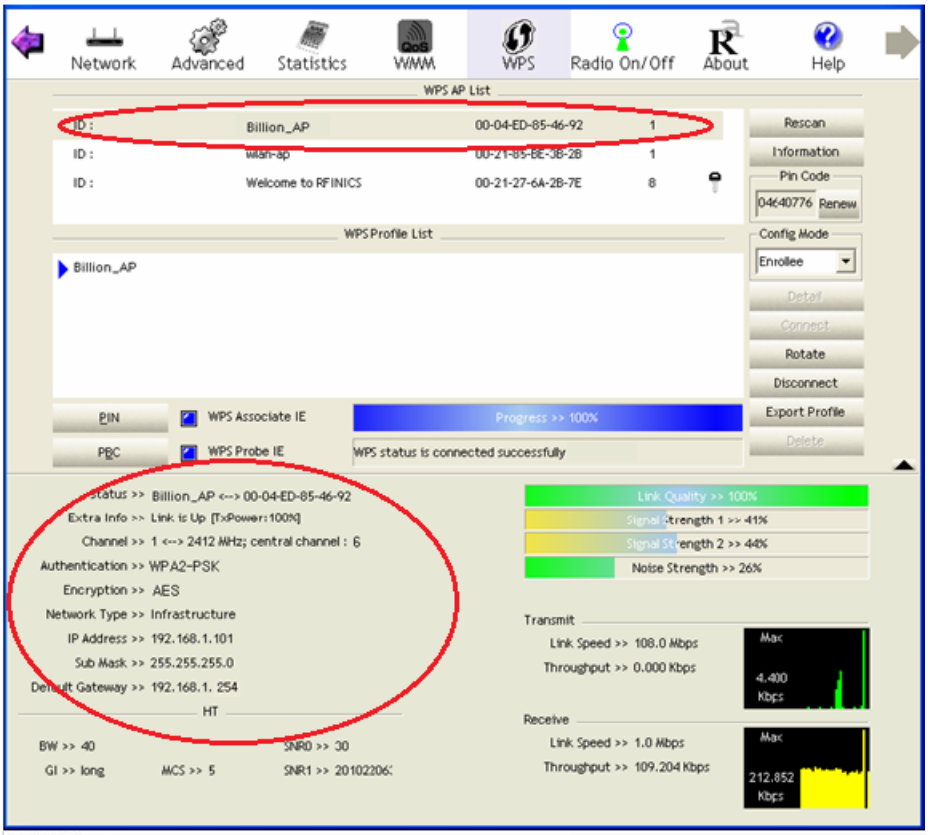
2. Enter the Enrollee (Client) PIN code and then press **Start WPS**.

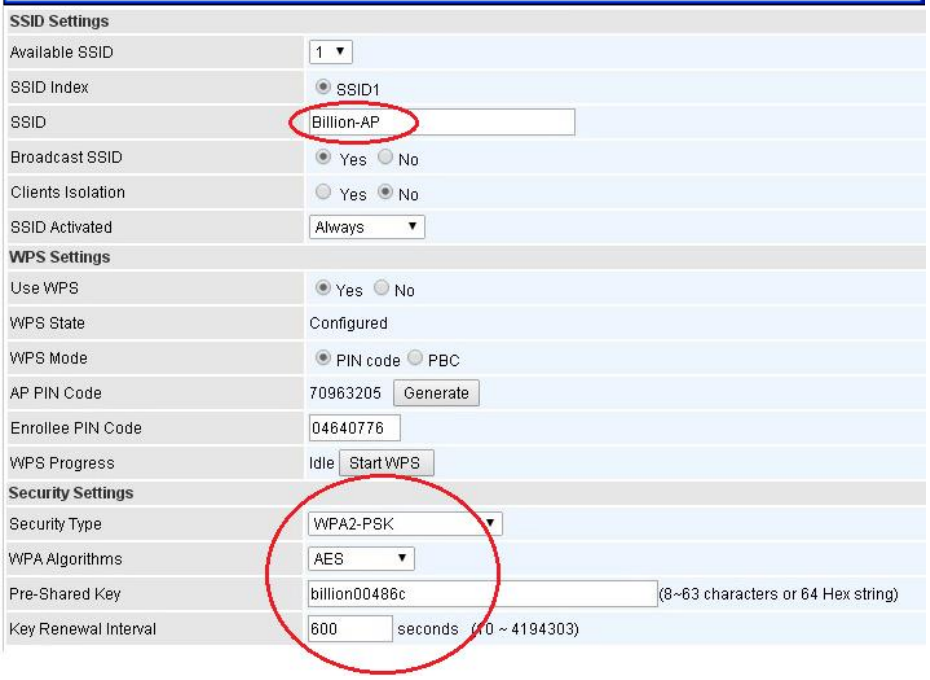


3. Go back to the wireless client's WPS utility (e.g. Ralink Utility).

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

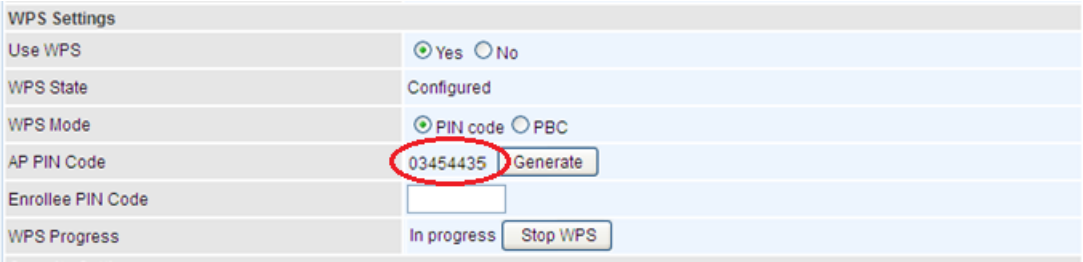
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar, the BEC 4700A/AZ router.



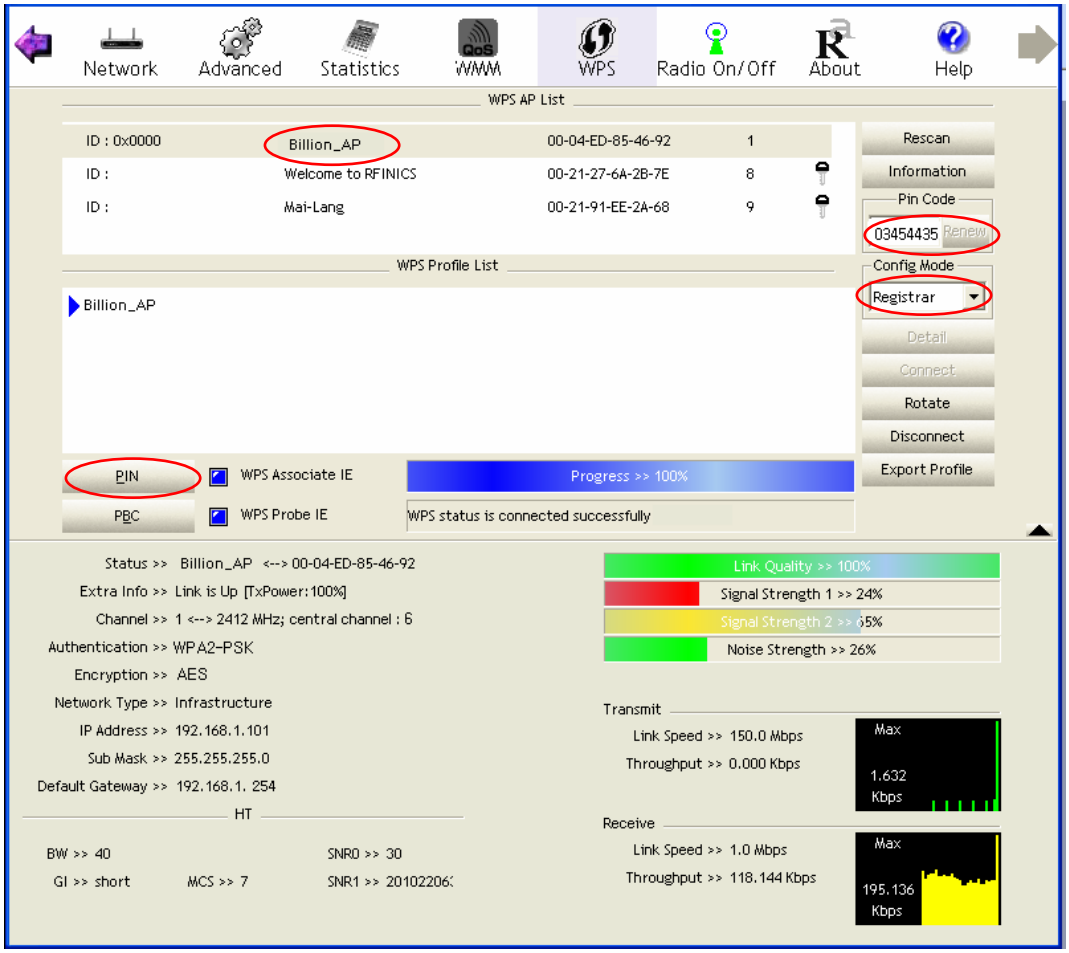


PIN Method – Configure BEC 4700A/AZ as an Enrollee

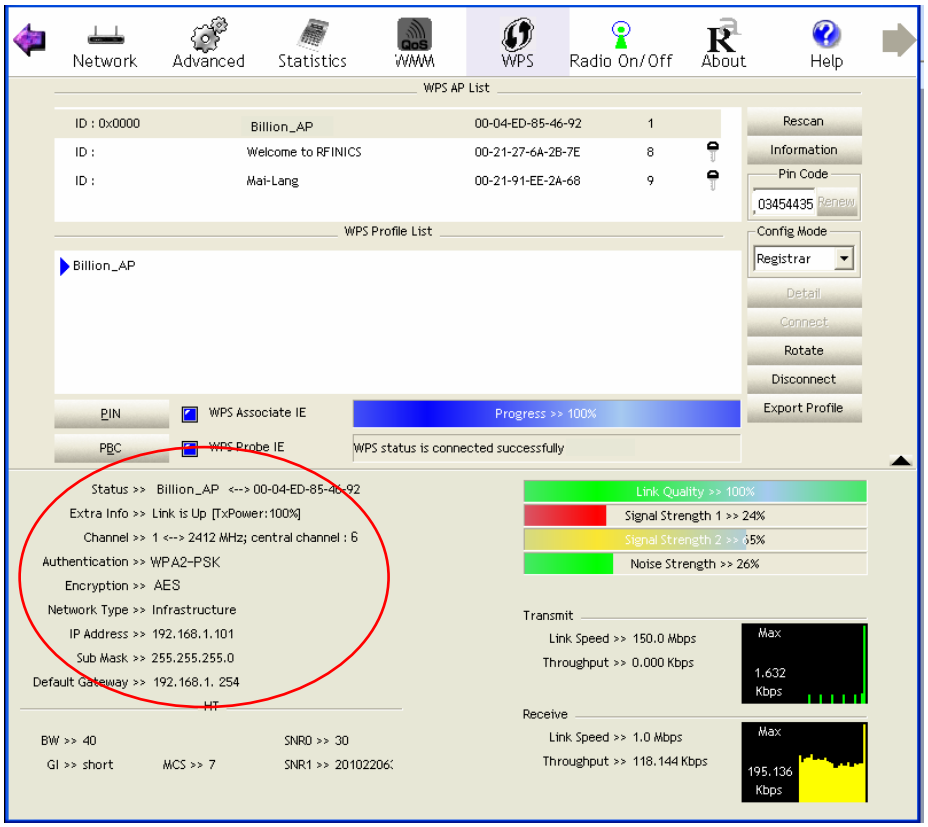
1. Jot down the AP PIN Code (e.g. 03454435) from the BEC 6300VNL. Press **Start** WPS.

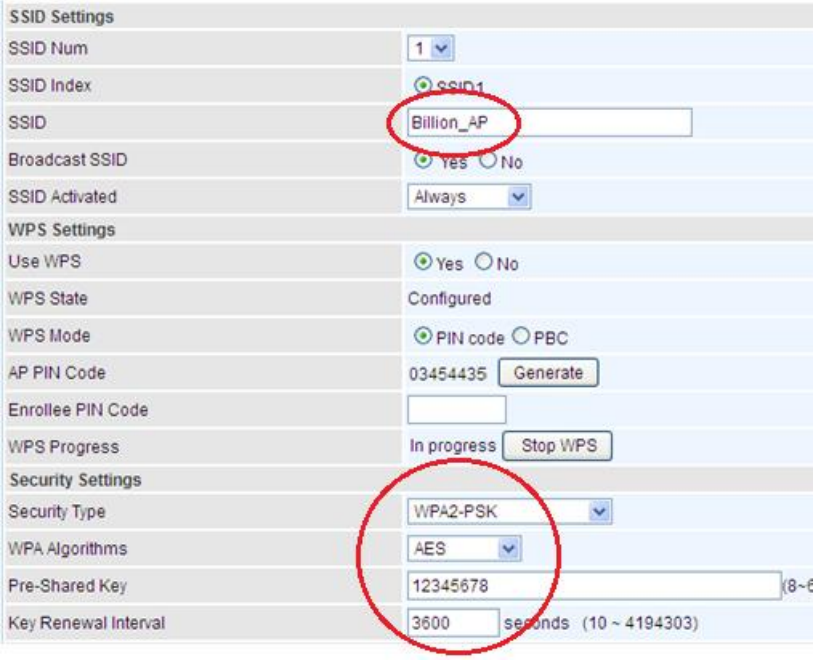


2. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code (e.g. 03454435) column then choose the correct AP (e.g. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.



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

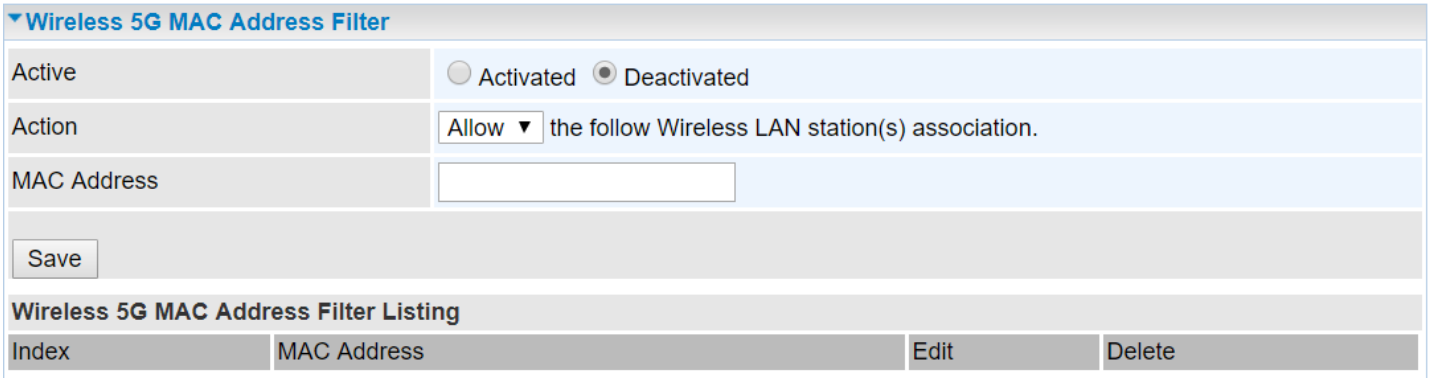




Wireless 5G MAC Filter

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

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



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

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

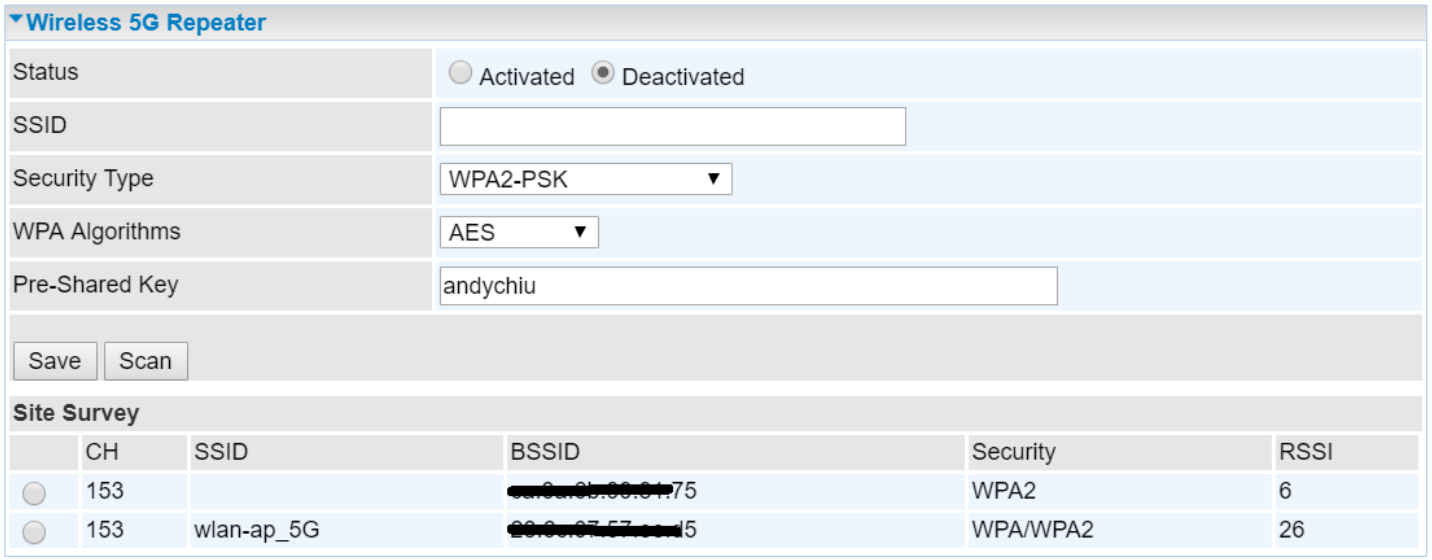
- Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router.
- Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

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

Click Save to apply settings.

Wireless 5G Repeater

Use the BEC 4700A/AZ as a repeater to extend the wi-fi signal of the primary AP.



Manually Fill-in

SSID: Enter the SSID of the primary AP.

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

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

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

Automatically

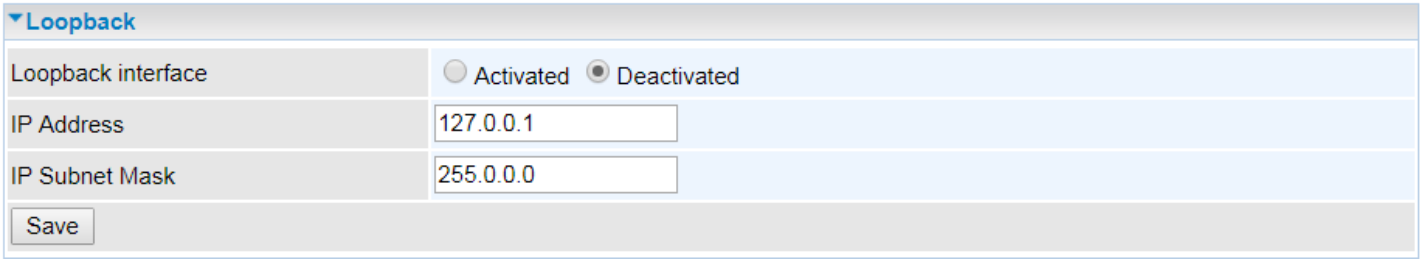
Scan: Click to view all other available Wireless-AP devices near the BEC 4700A/AZ. Select the desired AP you wish to extend the signal.

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

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.



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

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

Click **Save** to apply settings

Dual WAN

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

General Setting

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

❖ Failover & Failback

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

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

General Setting	
Dual WAN Mode	
Mode	Failover & Failback ▼
WAN Port Service Detection Policy	
WAN1	4G/LTE ▼
WAN2	EWAN(LAN1) ▼
Keep Backup Interface Connected	Disable ▼
Minimun RSRP/RSSI	-105 / -90 dbm(-111~ -5 , 0:disable)
Connectivity Decision	Auto failover takes place after straight 3 consecutive failure in every 30 seconds.
Probe By Ping	☑ Enable
Ping Setting	○ Gateway ◉ Host 8.8.8.8 Timeout 3 ▼ seconds
Probe By Signal Strength	☑ Enable
Minimum RSRP/RSSI	-105 / -90 dbm(-111~ -5 , 0:disable)
Save	

WAN Port Service Detection Policy

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

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

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

- **Disable:** Inactivate this feature.
- **Always:** Keep the backup WAN (WAN2) interface always connected to the Internet
- **By Signal Strength:** Enable and initiate automatic backup WAN to connect to the Internet at all time until the RSRP / RSSI of primary WAN is greater than the Minimum RSRP / RSSI.

Minimum RSRP / RSSI: Set a minimum requirement for RSRP and RSSI for the primary WAN. Value range from -111 ~ -5. 0 means don't care/no need to check this value.

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

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

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

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

Failover/Fallback Rule Decisions:

1. **Probe by Ping:** Enable Ping to the gateway or an IP address
   - **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.
   - **Host:** Internal system will wait for responses to the pings from a fixed IP address.
   - **Timeout X Seconds:** Ping response time for each reply. Maximum timeout up to **5** seconds.
2. **Probe by Signal Strength:** Enable to measure the LTE signal strength
   - **Minimum RSRP / RSSI:** Set a minimum requirement for RSRP and RSSI for initiating automatic WAN failback or failover procedures.

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

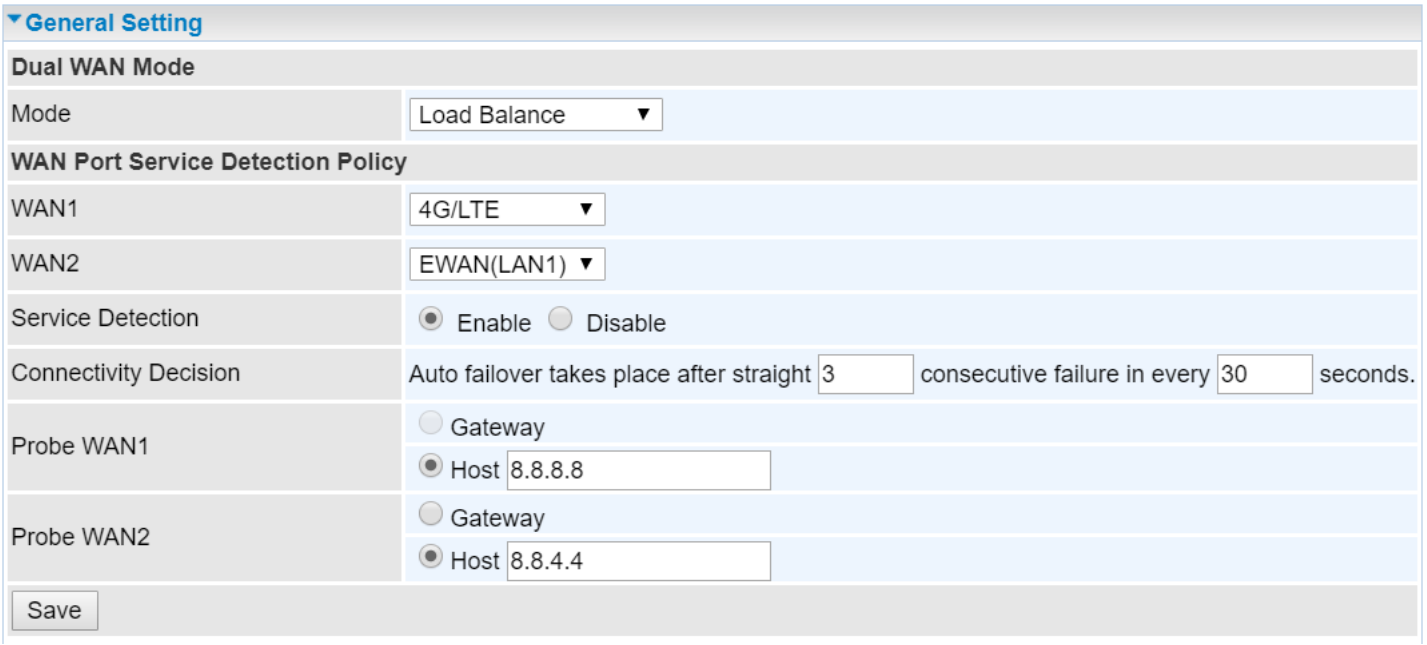
     NOTE: Both the RSRP and RSSI cannot be 0 at the same time.

Click **Save** to apply settings.

❖ Load Balance

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

NOTE: Go setup Outbound Load Balance mechanism after saving the settings.



WAN Port Service Detection Policy

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

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

Service Detection: Enable to detect WAN connectivity automatically.

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

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

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

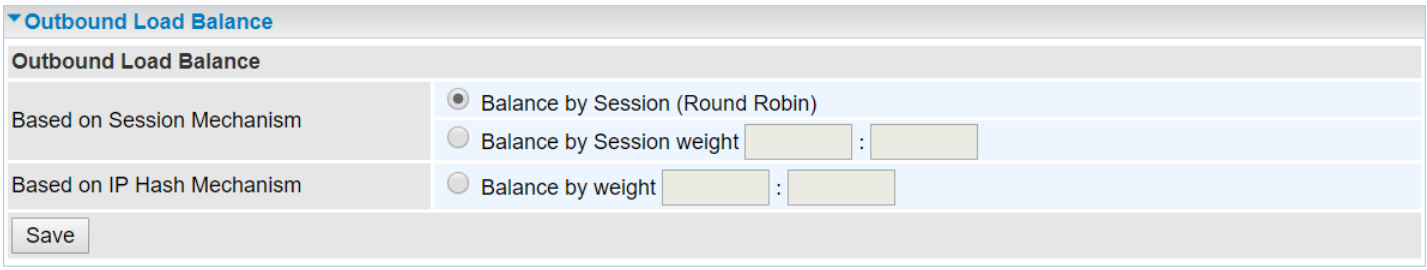
- **Gateway:** Internal system will wait for responses to the pings from the gateway of the WAN.
- **Host:** Internal system will wait for responses to the pings from a fixed IP address.

Click **Save** to apply settings

Outbound Load Balance

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

NOTE: Load Balancing must be enabled first.



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

Base on Session Mechanism:

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

OR

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

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

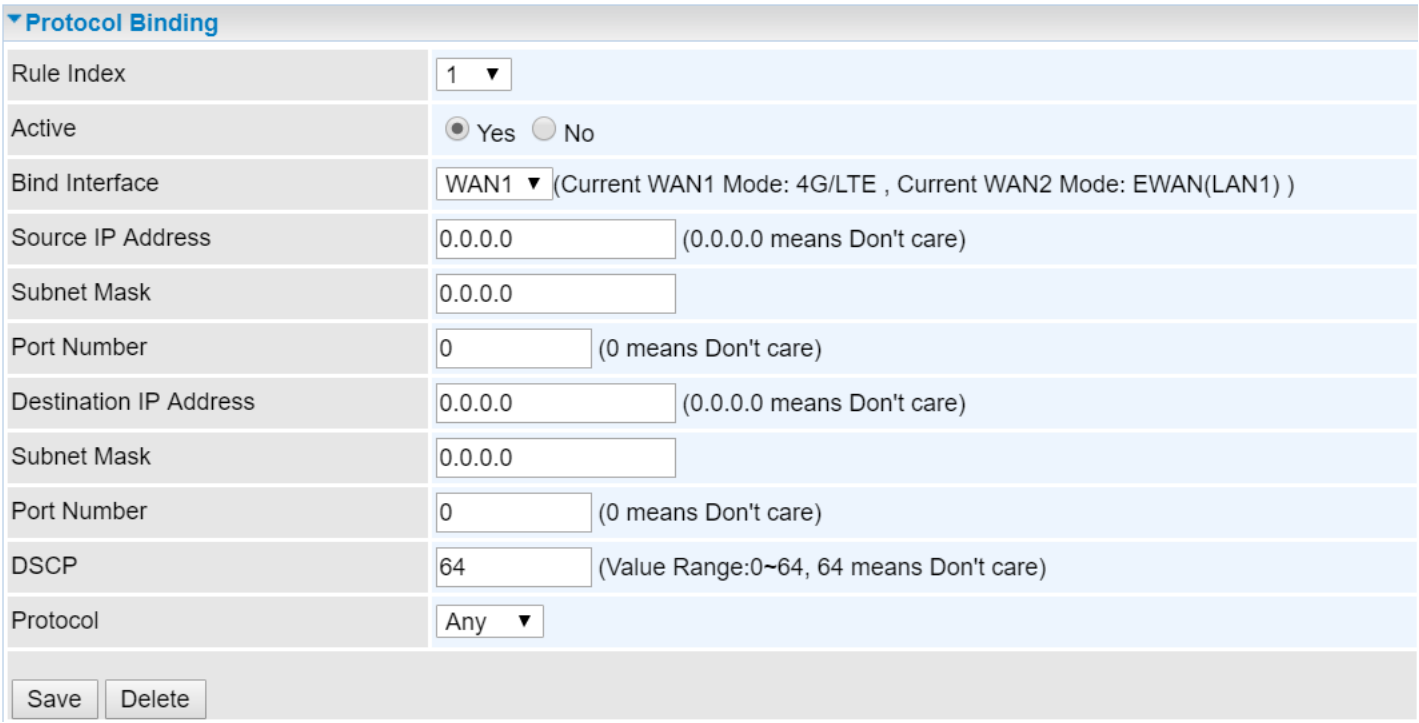
Base on IP Hash Mechanism:

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

Click **Save** to apply settings

Protocol Binding

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



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

Active: Click YES to activate the rule

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

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

Subnet Mask: Enter the subnet of the source network.

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

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

Subnet Mask: Enter the subnet of the designation network.

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

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

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

Click **Save** to apply settings

Example:

All traffics from IP 192.168.1.100/255.255.255.0 with port 8080 will go through WAN1 interface.

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

Protocol Binding List								
#	Active	Interface	Source IP Address/Mask	Destination IP Address/Mask	Source Port	Destination Port	DSCP	Protocol
1	Yes	WAN1	192.168.1.100/ 255.255.255.0	0.0.0.0/ 0.0.0.0	8080	0	0	TCP

Hotspot

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

General Setting

General Setting	
Hotspot	Activated Deactivated
Interface	BEC110 BEC2 BEC111
IP Address	10.0.0.1
IP Subnet Mask	255.255.255.0
Primary DNS	208.67.222.222 (Default:208.67.222.222)
Secondary DNS	208.67.222.220 (Default:208.67.222.220)
Login Mode	Authentication
Redirection On Successful Authentication To	(empty string: user intended to visit)

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

Interface: Select Wi-Fi interface(s), example: BEC110 (2.4GHz) to handles the hotspot traffic.

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

IP Subnet Mask: Enter the subnet of the network.

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

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

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

Redirect URL after Successful Login: Enter the URL (**http://** is not required). After Wi-Fi client is successful login to the network, the page will get redirected to this URL.

OR leave it blank to stay in current page.

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

Authentication

Authentication	
Authentication Method	◉ RADIUS ○ Built-in User Account
Primary RADIUS Server	
Secondary RADIUS Server	
Shared Secret Key	admin ☑ Show Character
Authentication Protocol	CHAP ▼

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

- **RADIUS (an external authentication server)**
  - **Primary RADIUS Server:** The main IP address of the server.
  - **Secondary RADIUS Server:** The backup IP address of the server, if any.
  - **Shared Secret Key:** Enter the shared Secret given by the server
- **Built-in User Account (local database handled by the BEC 4700A/AZ)**

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

Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) 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.

Session Settings

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

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

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

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

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