



BR-6478AC V3

User Manual

12-2018 / v1.0

Edimax Technology Co., Ltd.

No. 278, Xinhua 1st Rd., Neihu Dist., Taipei City, Taiwan

Email: support@edimax.com.tw

Edimax Technology Europe B.V.

Fijenhof 2, 5652 AE Eindhoven, The Netherlands

Email: support@edimax.nl

Edimax Computer Company

3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA

Live Tech Support: 1(800) 652-6776

Email: support@edimax.com

CONTENTS

| | |
|--|-----------|
| I. Product Information..... | 1 |
| I-1. Package Contents | 1 |
| I-2. LED Status | 2 |
| I-3. Back Panel..... | 3 |
| I-4. Safety Information..... | 4 |
| II. Installation..... | 5 |
| II-1. Wi-Fi Router Mode | 8 |
| II-2. Wireless Bridge Mode..... | 9 |
| II-3. WISP Mode | 10 |
| II-4. WPS Setup | 11 |
| II-5. Reset to Factory Default Settings..... | 12 |
| III. Browser Based Configuration Interface..... | 13 |
| III-1. Internet Status | 14 |
| III-2. Wizard Setup | 16 |
| III-3. WAN | 20 |
| III-3-1. Dynamic IP (DHCP) | 21 |
| III-3-2. PPPoE | 21 |
| III-3-3. Static IP..... | 22 |
| III-3-4. IPv6..... | 23 |
| III-3-5. Status | 24 |
| III-4. Operation Mode | 24 |
| III-5. Wi-Fi | 25 |
| III-5-1. Basic | 25 |
| III-5-2. Security | 27 |
| III-5-3. ACL | 28 |
| III-5-4. Site Survey..... | 28 |
| III-5-5. WPS | 29 |
| III-6. LAN | 29 |
| III-6-1. IPv4..... | 29 |
| III-6-2. IPv6..... | 30 |
| III-6-3. RADVD | 31 |
| III-6-4. TUNNEL 6 over 4..... | 33 |
| III-7. VPN | 33 |
| III-7-1. PPTP | 33 |
| III-7-2. L2TPv2 | 34 |
| III-7-3. L2TPv3 | 35 |

| | | |
|-------------|--------------------------|-----------|
| III-7-4. | Status..... | 36 |
| III-8. | USB..... | 36 |
| III-8-1. | Disk Information | 36 |
| III-8-2. | Account Management | 36 |
| III-8-3. | Share Folder | 37 |
| IV. | Features..... | 38 |
| IV-1. | QoS | 38 |
| IV-2. | Firewall | 39 |
| IV-2-1. | Advanced..... | 39 |
| IV-2-2. | DoS..... | 40 |
| IV-2-3. | IP Filtering | 41 |
| IV-2-4. | Port Filtering..... | 42 |
| IV-2-5. | MAC Filtering..... | 43 |
| IV-2-6. | Port Forwarding | 43 |
| IV-2-7. | URL Filter | 45 |
| IV-2-8. | Route..... | 45 |
| IV-2-8-1. | Default Route..... | 45 |
| IV-2-8-2. | Static Route | 45 |
| IV-2-8-3. | Dynamic DNS..... | 46 |
| V. | Management | 48 |
| V-1. | Time..... | 48 |
| V-1-1. | NTP Server..... | 48 |
| V-1-2. | Auto Reboot | 48 |
| V-2. | System Log | 49 |
| V-3. | System Settings | 50 |
| VI. | Logout..... | 55 |
| VII. | FAQ..... | 56 |

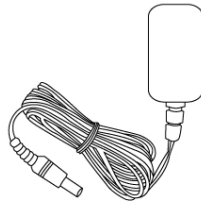
I. Product Information

I-1. Package Contents

Before you start using this product, please check if there is anything missing in the package, and contact your dealer to claim the missing item(s):



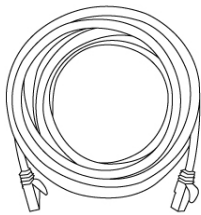
BR-6478AC V3



Power Adapter



CD-ROM

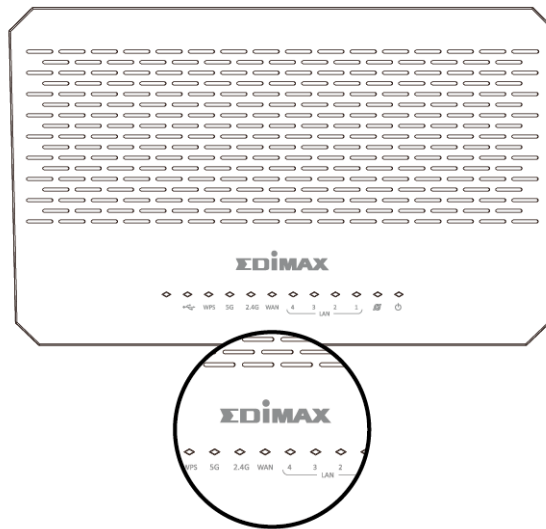






Ethernet Cable



Quick Installation Guide

I-2. LED Status

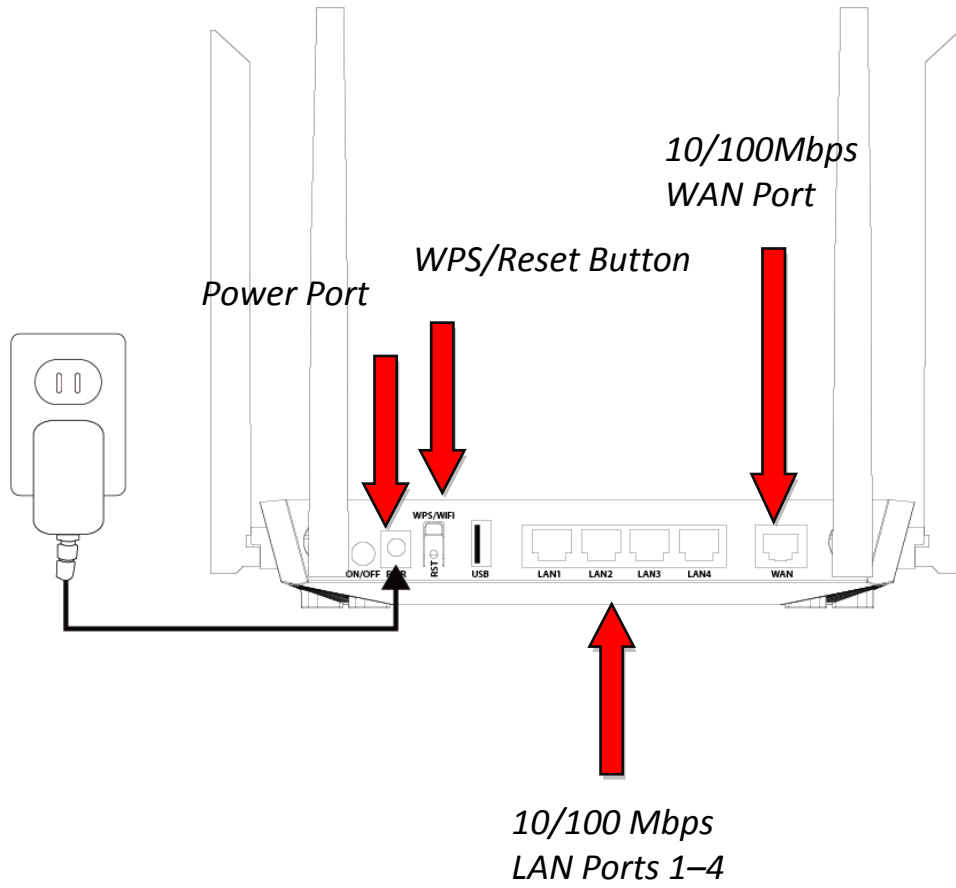


| LED | Color | LED Status | Description |
|--|-------|------------|---|
| Power  | Green | On | The device is on. |
| | | Off | The device is off. |
| Internet  | Green | On | Internet connection is ready. |
| | | Flashing | Restoring to factory default state, or Ethernet cable not connected, or no Internet connection. |
| 2.4G Wi-Fi  | Green | On | 2.4GHz Wi-Fi wireless activity. (Transferring/receiving data). |
| | | Flashing | 2.4GHz WPS is active. |
| | | Off | 2.4GHz Wi-Fi not active. |
| 5G Wi-Fi  | Green | On | 5GHz Wi-Fi wireless activity. (Transferring/receiving data). |
| | | Flashing | 5GHz WPS is active. |
| | | Off | 5GHz Wi-Fi not active. |
| USB | Green | On | USB connection is ready. |
| | | Flashing | A new USB device is being identified. |
| | | Off | USB is not active. |
| WPS | Green | On | Negotiation is in progress through Wi-Fi Protected Setup. |
| | | Off | WPS is disabled or connected. |
| LAN 1-4 | Green | On | Ethernet port is connected to a network device. |
| | | Off | Ethernet port is not connected to a network |



If indicator shows abnormal activity, please check the connection.

I-3. Back Panel



BR- 6478AC V3: 5dBi External Antenna x 4

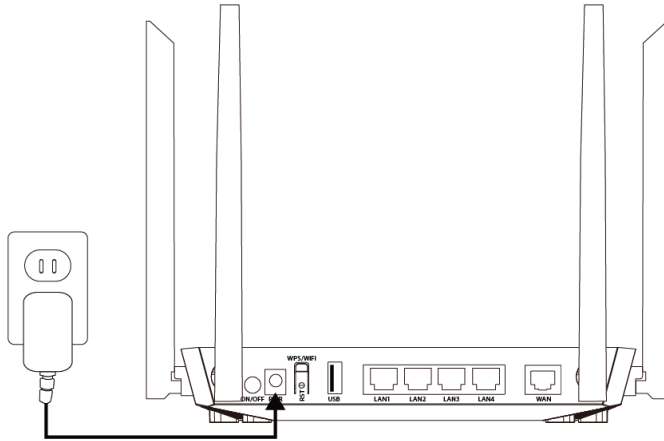
I-4. Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

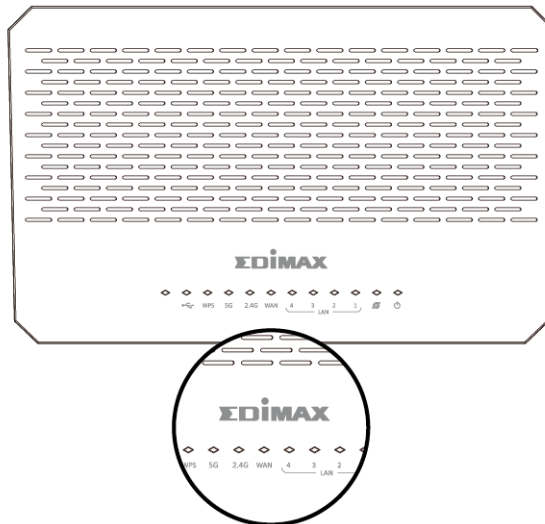
1. The device is designed for indoor use only; do not place it outdoors.
2. Do not place the device in or near hot/humid places, such as a kitchen or bathroom.
3. Do not pull any connected cable with force; carefully disconnect it from the BR-6478AC V3.
4. Handle the device with care. Accidental damage will void the warranty of the device.
5. The device contains small parts which are a danger to small children under 3 years old. Please keep the device out of reach of children.
6. Do not place the device on paper, cloth, or other flammable materials. The device may become hot during use.
7. There are no user-serviceable parts inside the device. If you experience problems with the device, please contact your dealer of purchase and ask for help.
8. The device is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.

II. Installation

1. Plug the included power adapter into the device's 5V DC power port and the other end into an electrical socket.



2. Ensure that the Wi-Fi On/Off switch is set to on and that five LEDs (power, Internet, 2.4GHz & 5GHz Wi-Fi & USB) display are on.



3. Plug the Ethernet cable to internet and the WAN port of the router.

4. Use a Wi-Fi device (e.g. computer, tablet, smartphone) to search for a Wi-Fi network with the SSID “edimax_2.4G_xx or edimax_5G_xx ” and connect to it.



iOS 4 or Android 4 and above are required for setup on a smartphone or tablet.



Please noted that BR-6478AC V3 is operated and set up as a Wi-Fi router by default. For complete set up of BR-6478AC V3 in other operation modes, please refer to the user manual.

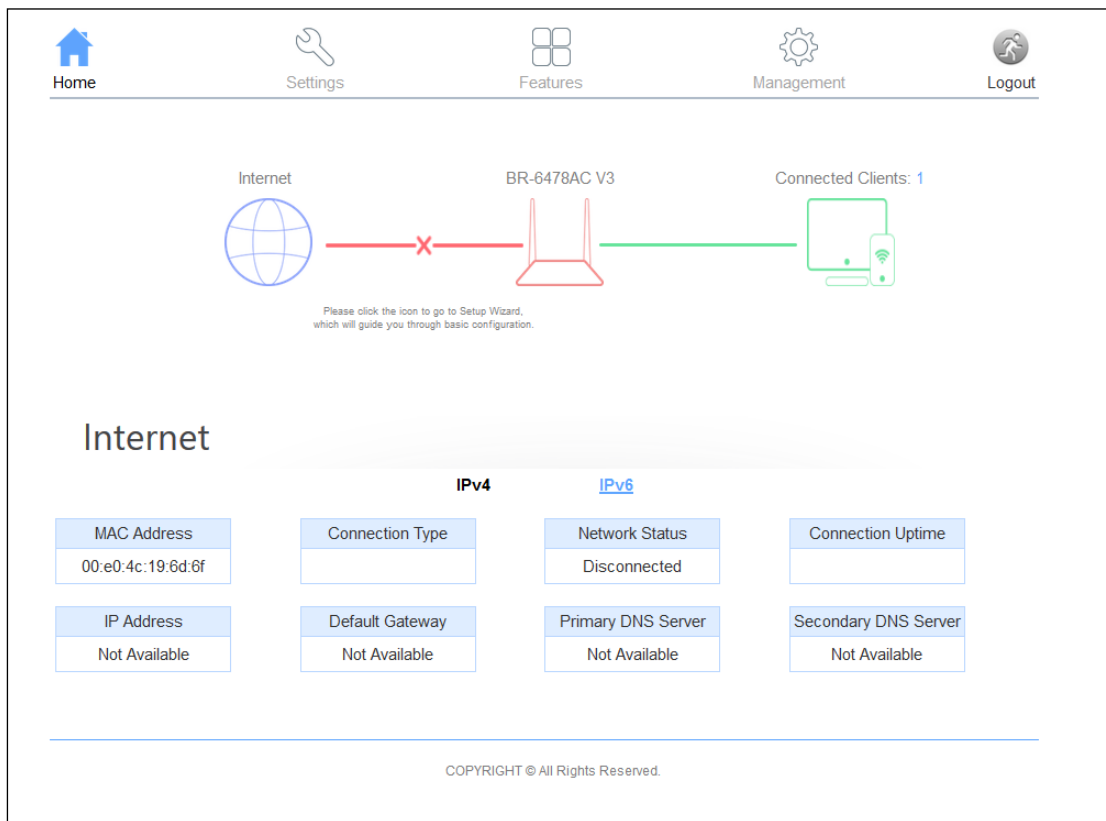
5. Open a web browser and enter the URL ***http://192.168.2.1*** and follow the instructions to begin the setup process. You will be prompted for a username and password. The default username is “**admin**” and the default password is “**1234**”.

The screenshot shows the Edimax web interface. At the top left is the Edimax logo with the tagline 'NETWORKING PEOPLE TOGETHER'. To the right of the logo, it says 'Model Name: BR-6478AC V3' and 'Language: English' with a dropdown arrow. In the center, there is a login form with two input fields: the top one is empty, and the bottom one is labeled 'Password'. Below the password field is a blue 'Login' button.



If you can not access 192.168.2.1, connect the BR-6478AC V3 to a computer using an Ethernet cable and try again.

6. When you login to the web UI of the router successfully. The following figure will appear, Click on “Settings” to set up:



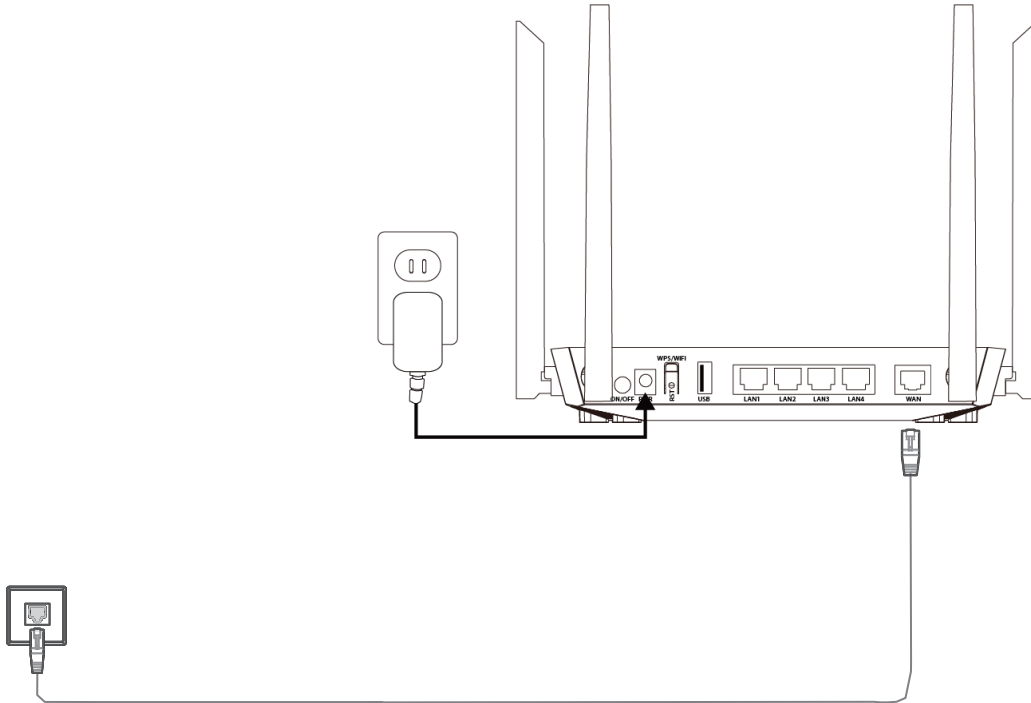
The BR-6478AC V3's three available modes are outlined below:

| | |
|--------------------------|--|
| Wi-Fi Router Mode | <i>The device connects to your modem and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.</i> |
| Wi-Fi Bridge Mode | <i>The device connects to a network device for example: TV, gaming console, or media player via Ethernet cable and acts as a Wi-Fi bridge, allowing the network device to join your Wi-Fi network.</i> |
| WISP Mode | <i>The device connects wirelessly to your Wireless Internet Service Provider and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.</i> |

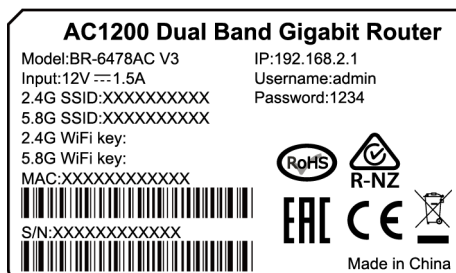
7. Follow the on-screen instructions to complete setup. For more information, please refer to the appropriate following chapter:

II-1. Wi-Fi Router Mode

1. Connect the blue WAN port of your BR-6478AC V3 to the LAN port of your modem using an Ethernet cable.



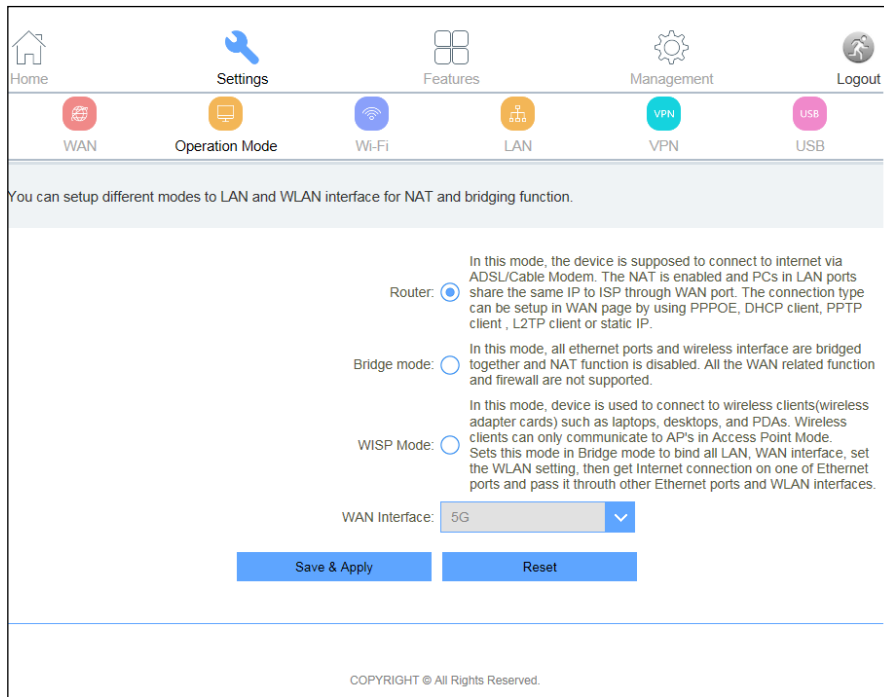
2. Log on to your 2.4GHz & 5GHz wireless networks. For first time use, please use the SSID and wireless password printed on the bottom of the router. Otherwise, enter a new SSID and password for your 2.4GHz & 5GHz wireless networks.



3. Please wait a moment until the device is ready
4. The BR-6478AC V3 is working and ready for use. You can now connect to the device's new SSID. Please refer to following chapters if you require more guidance.

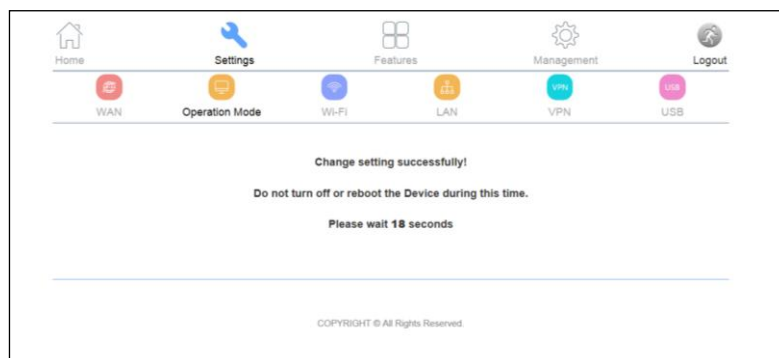
II-2. Wireless Bridge Mode

1. Please ensure your BR-6478AC V3 is within Wi-Fi range of your existing wireless router. Please log on ***http:// 192.168.2.1*** to set up.
2. In the top menu, click “Settings”, then click “Operation Mode”. Select “Bridge mode” to configure.



3. Click “Save & Apply”.

4. Please wait a moment until the BR-6478AC V3 is ready.



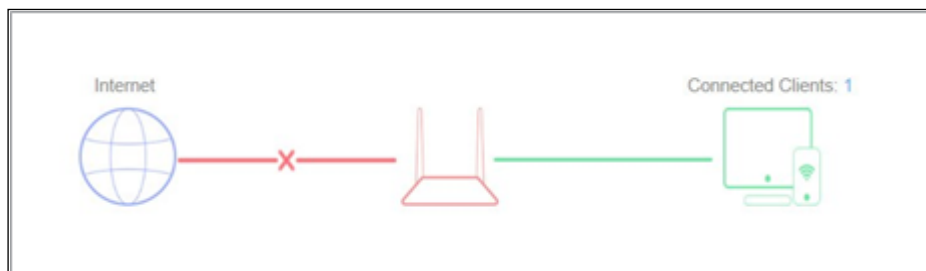
5. The BR-6478AC V3 is working and ready for use. You can now connect the BR-6478AC V3 to your network device using an Ethernet cable and connect to your network as usual.

II-3. WISP Mode

1. Please ensure your BR-6478AC V3 is within Wi-Fi range of your WISP network. Click “Next” to continue.

2. Please wait a moment until the BR-6478AC V3 is ready.

3. For first time use, log on [http:// 192.168.2.1](http://192.168.2.1). In the absence of an external network, the following interface appears.



4. Click the red “X”, the Wizard Setup page screen appears as below.

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

| | |
|----|---------------------------|
| 1. | Setup Operation Mode |
| 2. | Choose your Time Zone |
| 3. | Setup LAN Interface |
| 4. | Setup WAN Interface |
| 5. | Select Wireless Band |
| 6. | Wireless LAN Setting |
| 7. | Wireless Security Setting |

[Next>>](#)

[Cancel](#) [<<Back](#) [Next>>](#)

5. Click “Next”, select “Wireless ISP” to configure WISP mode.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Router : In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP client , L2TP client or static IP.

Bridge mode: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

WISP Mode: In this mode, device is used to connect to wireless clients(wireless adapter cards) such as laptops, desktops, and PDAs. Wireless clients can only communicate to AP's in Access Point Mode. Sets this mode in Bridge mode to bind all LAN, WAN interface, set the WLAN setting, then get Internet connection on one of Ethernet ports and pass it through other Ethernet ports and WLAN interfaces.

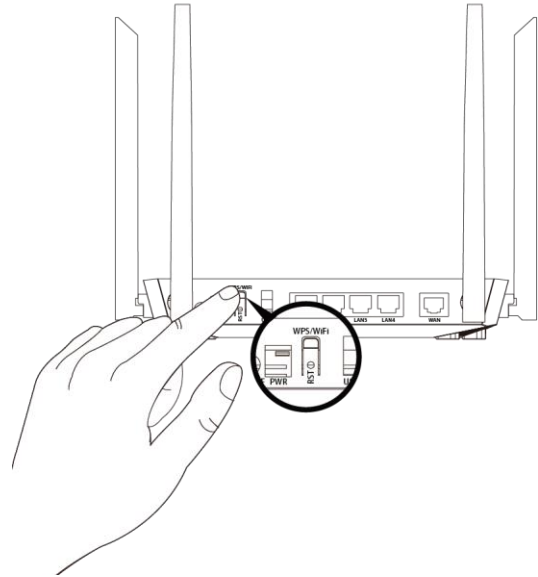
WAN Interface


[Cancel](#) [<<Back](#) [Next>>](#)

II-4. WPS Setup

If your wireless device supports WPS (Wi-Fi Protected Setup) then you can use this method to connect to the BR-6478AC V3's Wi-Fi network.

- 1.** Press the **WPS button** on the BR-6478AC V3 for 3 – 5 seconds to activate WPS.
- 2.** **Within two minutes**, press the WPS button on the **wireless device/client** to activate its WPS.
- 3.** The devices will establish a connection. Repeat for additional wireless devices.

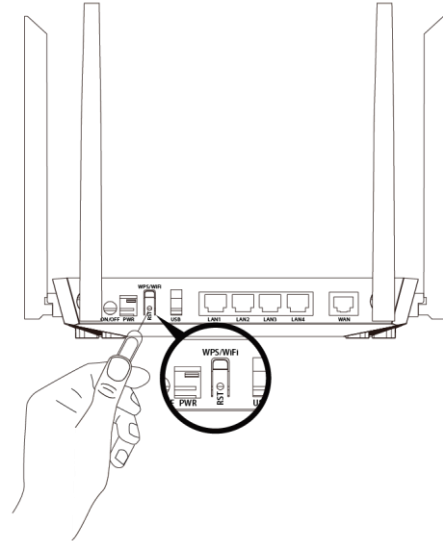


 ***Please check the instructions for your wireless device for how long you need to hold down its WPS button to activate WPS.***

II-5. Reset to Factory Default Settings

If you experience problems with your BR-6478AC V3, you can reset the device back to its factory settings. This resets **all** settings back to default.

- 1.** Press and hold RST button with a needle for about 5 seconds to reset the router to its factory default settings.
- 2.** Release the button when all the LED **blinks once**.
- 3.** Wait for the BR-6478AC V3 to restart. The BR-6478AC V3 is ready for setup when the power LED displays **on**.



III. Browser Based Configuration Interface

After setup you can access the browser based configuration interface to configure or change the settings of the BR-6478AC V3. To access the browser based configuration interface, enter ***http:// 192.168.2.1*** into the URL bar of a web browser on a network device which is connected to the BR-6478AC V3.



If you can not access 192.168.2.1, connects the BR-6478AC V3 to a computer using an Ethernet cable and try again.

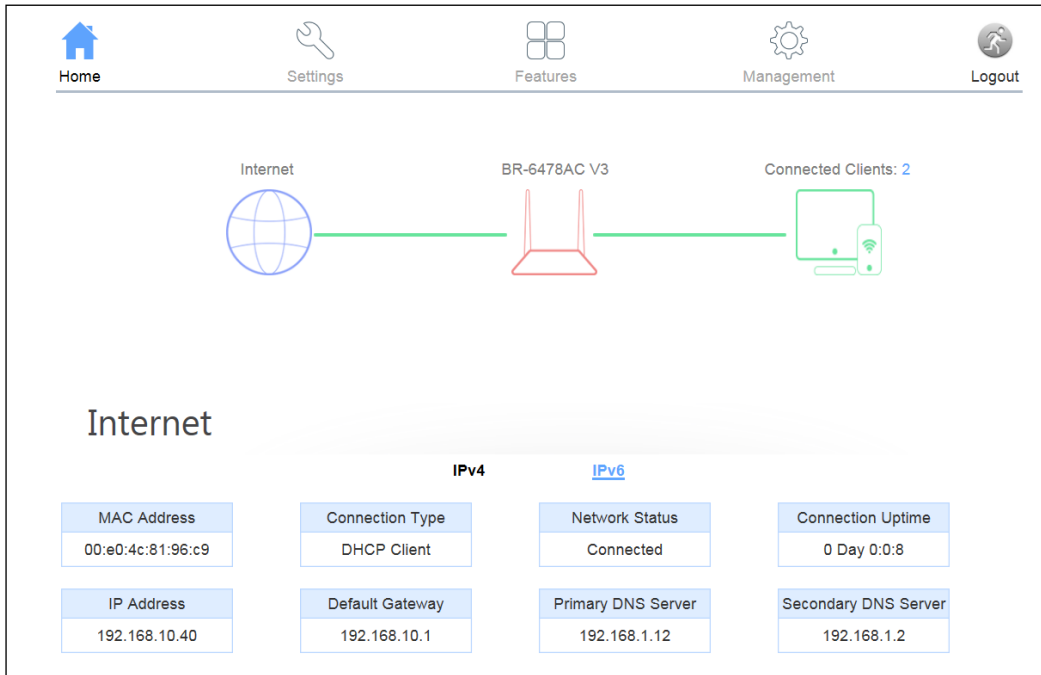
You will be prompted for a username and password. The default username is “admin” and the default password is “1234”.


You will arrive at the “Home” screen shown below. Use the top menu to navigate and click on “Settings” to select one of the three operation modes. For more information, refer to the user manual.

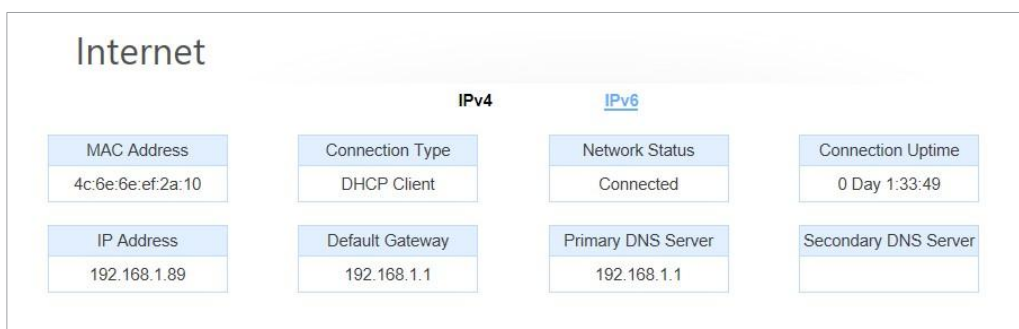
| IPv4 | | | |
|-------------------|-----------------|--------------------|----------------------|
| MAC Address | Connection Type | Network Status | Connection Uptime |
| 00:e0:4c:19:6d:6f | | Disconnected | |
| IP Address | Default Gateway | Primary DNS Server | Secondary DNS Server |
| Not Available | Not Available | Not Available | Not Available |


III-1. Internet Status

1. If you perform no operation within 2 minutes after your login, the router logs you out. In addition, click Logout on the upper right corner of the web UI also can log out.
2. Then Home page allows you to view the network status of the router, Wi-Fi information, online device and other status information



3. Click  icon to view the internet information. On this page, you can view information about the Internet status of the router, including MAC Address, Connection Type, Network Status, Connection Uptime, IP Address, Default Gateway, Primary DNS Server and Secondary DNS Server.



4. Click  icon to view the Wi-Fi information. You can view information about the current LAN and Wi-Fi status of the router.

| IPv4 Network | |
|--------------------|-------------------|
| MAC Address: | 4c:6e:6e:b0:ef:2e |
| Router IP Address: | 192.168.2.1 |
| Subnet Mask: | 255.255.255.0 |


| IPv6 Network | |
|----------------------|---------------------------|
| Link-Local Address: | fe80::4e6e:6eff:feb0:ef2e |
| Router IPv6 Address: | Not Available |

| System | |
|-------------|------------------------------|
| Uptime: | 0 Day 1:2:59 |
| Build Time: | Wed Oct 17 17:47:58 CST 2018 |

| CPU | |
|----------------------|--------------|
| CPU Usage: | 7.03% |
| Memory (Free/Total): | 76704/103296 |

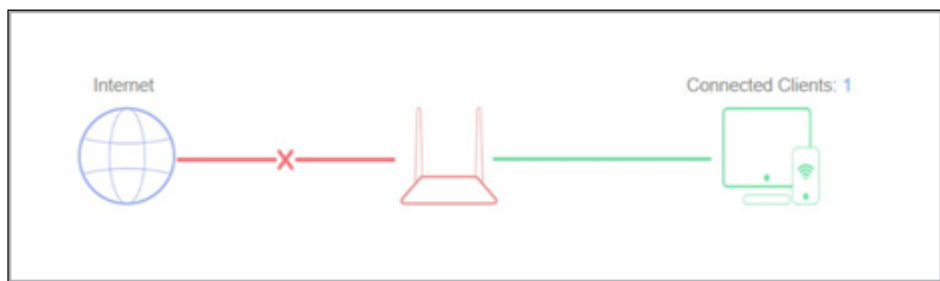
| Wi-Fi 2.4GHz | |
|--------------------|-------------------|
| Status: | Up |
| Wi-Fi Name (SSID): | edimax_2.4G_2e |
| Encryption: | WPA2 Mixed |
| BSSID: | 4c:6e:6e:0e:f2:e8 |

| Wi-Fi 5GHz | |
|--------------------|-------------------|
| Status: | Up |
| Wi-Fi Name (SSID): | edimax_5G_2e |
| Encryption: | WPA2 Mixed |
| BSSID: | 4c:6e:6e:0e:f2:e0 |

5. Click  icon to view the information of online device(s).

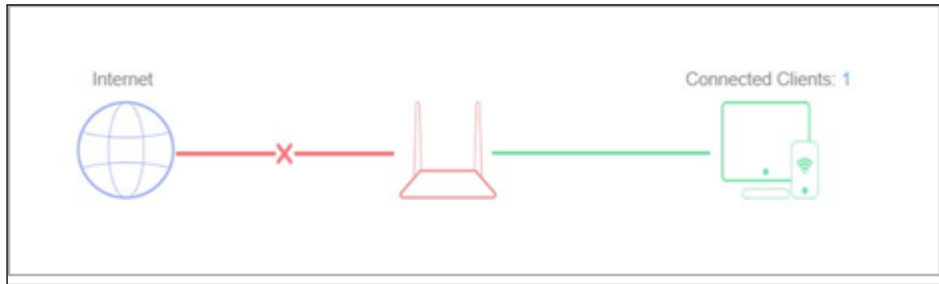
| Connected Clients | |
|-------------------|-------------------|
| IP Address | MAC Address |
| 192.168.0.100 | 9c:30:5b:ef:b8:8f |

6. When status below is displayed, it means the internet connection is unsuccessful. Please check the WAN connection.



III-2. Wizard Setup

1. In the absence of an external network, after entering the user name and password to login to the Web UI, it appears the following interface.



2. Click the red “X”, the Wizard Setup page screen appears as below.

Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Select Wireless Band
6. Wireless LAN Setting
7. Wireless Security Setting

[Next>>](#)

[Cancel](#) [<<Back](#) [Next>>](#)

3. Click **Next** and you can configure the router Operation Mode.

Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Router : In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

Bridge mode: In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

WISP Mode: In this mode, device is used to connect to wireless clients(wireless adapter cards) such as laptops, desktops, and PDAs. Wireless clients can only communicate to AP's in Access Point Mode. Sets this mode in Bridge mode to bind all LAN, WAN interface, set the WLAN setting, then get Internet connection on one of Ethernet ports and pass it through other Ethernet ports and WLAN interfaces.

WAN Interface: 5G ▼

[Cancel](#) [<<Back](#) [Next>>](#)

4. Click **Next** to configure Time Zone Setting.

The screenshot shows the 'Time Zone Setting' configuration page. At the top, it says 'Time Zone Setting' and 'You can maintain the system time by synchronizing with a public time server over the Internet.' Below this, there are two checkboxes: 'Enable NTP client update:' which is checked, and 'Automatically Adjust Daylight Saving:' which is unchecked. There are two dropdown menus: 'Time Zone Select:' with '(GMT+08:00)Taipei' selected, and 'NTP server:' with '131.188.3.220 - Europe' selected. At the bottom, there are three buttons: 'Cancel', '<<Back', and 'Next>>'.

5. Click **Next** and you can configure the LAN Interface Setup. This page is used to configure the **parameters for local area network which connects to the LAN port of your** Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.

The screenshot shows the 'LAN Interface Setup' configuration page. It starts with the title 'LAN Interface Setup' and a description: 'This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.' Below the description, there are two input fields: 'IP Address:' with '192.168.2.1' entered, and 'Subnet Mask:' with '255.255.255.0' entered. At the bottom, there are three buttons: 'Cancel', '<<Back', and 'Next>>'.

6. Click **Next** and you can configure the WAN Interface Setup. This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE by click the item value of WAN Access type.

The screenshot shows the 'WAN Interface Setup' configuration page. It starts with the title 'WAN Interface Setup' and a description: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE by click the item value of WAN Access type.' Below the description, there is a dropdown menu for 'WAN Access Type:' with 'DHCP Client' selected. A menu is open showing the options: 'Static IP', 'DHCP Client', and 'PPPoE'. At the bottom, there are three buttons: 'Cancel', '<<Back', and 'Next>>'.

7. Click **Next** and then the following page will pop up. Generally, the default selection is ok.

Select Wireless Band
You can select Wireless Band

Wireless Band: 2.4G+5G Concurrent

Cancel <<Back Next>>

8. Click **Next** and configure the 5 GHz wireless network parameters.

Wireless 5GHz Basic Settings
This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band: 5 GHz (A+N+AC)
Mode: AP
Network Type: Infrastructure
SSID: edimax_5G_c1
Channel Width: 80MHz
ControlSideband: Lower
Channel Number: Auto

Enable Mac Clone (Single Ethernet Client):
Add to Profile:

Cancel <<Back Next>>

9. Click **Next** and configure the 5 GHz wireless security. It should be set up at least 8 characters.

Wireless 5GHz Security Setup
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA Mixed
Pre-Shared Key Format: Passphrase
Pre-Shared Key: [Masked]

Cancel <<Back Next

10. Click **Next** and configure the 2.4GHz wireless network parameters.

Wireless 2.4GHz Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

Band: 2.4 GHz (B+G+N)

Mode: AP

Network Type: Infrastructure

SSID: edimax_2.4G_c1

Channel Width: 40MHz

ControlSideband: Upper

Channel Number: Auto

Enable Mac Clone (Single Ethernet Client):

Add to Profile:

11. Click **Next** and configure the 2.4GHz wireless security. It should be set up at least 8 characters. And then click Finish.

Wireless 2.4GHz Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption: WPA Mixed

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

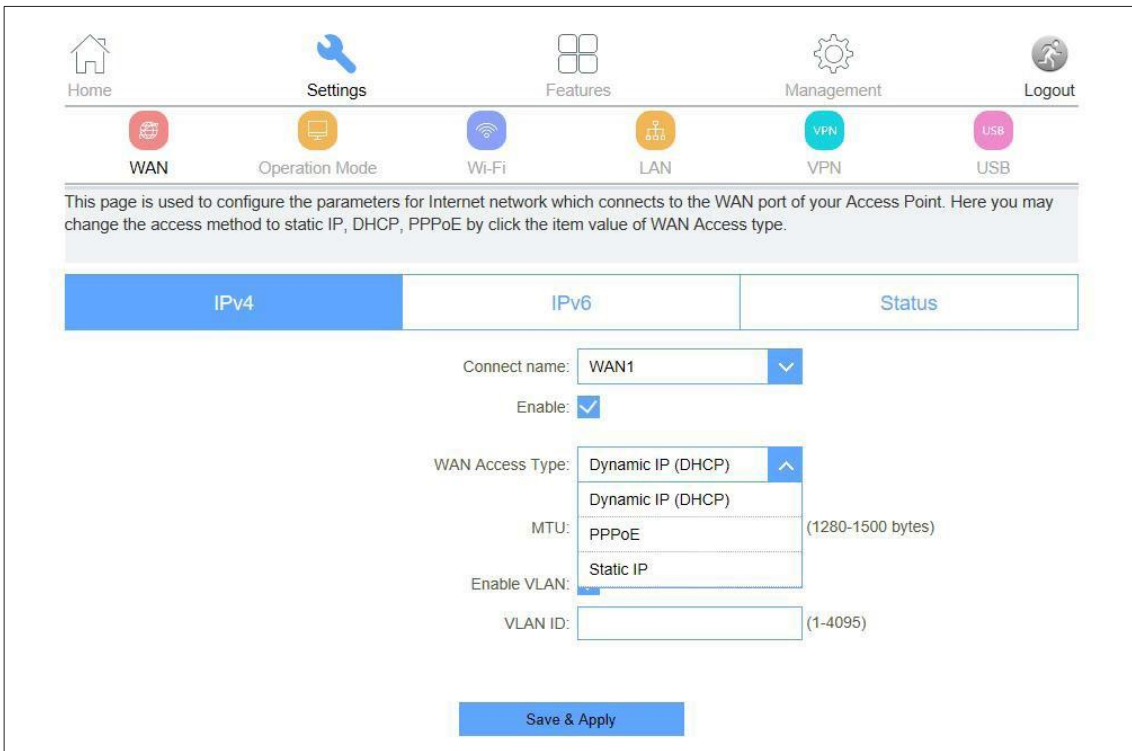


Users can select whether to set 5 GHz and 2.4GHz wireless security simultaneously according to their own demands.

III-3. WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Generally, the router detects your internet connection type automatically when you use the router for the first time or after you reset the router.

There are three WAN Connection type can be use, each WAN Connection type can be configured as difference mode, such as Dynamic IP (DHCP) router mode, PPPoE router mode, Static router mode, and each WAN connection can be configured to have VLAN tag, this will more helpful for user to meet different environment usage. The following table may help you understand your internet connection type. If you are still uncertain about your internet connection type, consult your ISP.



| | |
|--------------------------|--|
| Dynamic IP (DHCP) | Your ISP does not provide ISP user name, password or other information about IP address. |
| PPPoE | ISP user name and password are provided by your ISP |
| Static IP | Your ISP provides IP address, subnet mask, default gateway, DNS server(s). |

III-3-1. Dynamic IP (DHCP)

Choose “DHCP” and the router will automatically obtain IP addresses, subnet masks and gateway addresses from your ISP.

The screenshot shows the configuration page for Dynamic IP (DHCP) under the IPv4 tab. The 'Connect name' is set to 'WAN1'. The 'Enable' checkbox is checked. The 'WAN Access Type' is set to 'Dynamic IP (DHCP)'. The 'MTU' is set to '1500' (with a range of 1280-1500 bytes). The 'Enable VLAN' checkbox is checked, and the 'VLAN ID' field is empty (with a range of 1-4095). A 'Save & Apply' button is at the bottom.

| | |
|----------------|--|
| MTU | You can keep the maximum transmission unit (MTU) as default. |
| VLAN ID | Enter the VLAN ID value provided by your ISP |

III-3-2. PPPoE

Select PPPoE, if your ISP is using a PPPoE connection and provide you with PPPoE user name and password information.

The screenshot shows the configuration page for PPPoE under the IPv4 tab. The 'Connect name' is set to 'WAN1'. The 'Enable' checkbox is checked. The 'WAN Access Type' is set to 'PPPoE'. The 'User Name', 'Password', and 'Service Name' fields are empty. The 'MTU' is set to '1492' (with a range of 1360-1492 bytes). The 'Connection Type' is set to 'Continuous'. The 'Enable VLAN' checkbox is checked, and the 'VLAN ID' field is empty (with a range of 1-4095). A 'Save & Apply' button is at the bottom.

| | |
|---------------------|--|
| Username | Enter the User Name provided by your ISP |
| Password | Enter the password provided by your ISP |
| Service Name | Type the name of this router |
| MTU | You can keep the maximum transmission unit (MTU) as default. |
| VLAN ID | Enter the VLAN ID value provided by your ISP |

III-3-3. Static IP

If your ISP offers you static IP Internet connection type, select “Static IP” and then enter IP address, subnet mask, primary DNS and secondary DNS information provided by your ISP in the corresponding fields.

The screenshot shows a network configuration interface with three tabs: IPv4 (selected), IPv6, and Status. The IPv4 configuration includes the following fields and options:

- Connect name:** WAN1 (dropdown menu)
- Enable:**
- WAN Access Type:** Static IP (dropdown menu)
- IP Address:** 192.168.1.89
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 192.168.1.1
- MTU:** 1500 (1400-1500 bytes)
- DNS 1:** 192.168.1.1
- DNS 2:** (empty field)
- Enable VLAN:**
- VLAN ID:** (empty field) (1-4095)

A "Save & Apply" button is located at the bottom of the configuration area.

| | |
|------------------------|---|
| IP Address | Enter the WAN IP address provided by your ISP. Inquire your ISP if you are not clear. |
| Subnet Mask | Enter WAN Subnet Mask provided by your ISP. |
| Default Gateway | Enter the WAN Gateway address provided by your ISP. |
| DNS 1 | Enter the WAN Gateway address provided by your ISP. |
| DNS 2 | Enter the other DNS address if your ISP provides you with 2 such |
| MTU | You can keep the maximum transmission unit (MTU) as default. |

III-3-4. IPv6

If necessary to enable IPv6, please check the box below.

The screenshot shows a configuration interface with three tabs: IPv4, IPv6, and Status. The IPv6 tab is selected. Below the tabs, there is a checkbox labeled 'Enable IPv6:' which is currently unchecked. At the bottom, there are two buttons: 'Save & Apply' and 'Reset'.

And according to your actual situation to set the parameters below. In general, your ISP will set these if necessary.

The screenshot shows a more detailed IPv6 configuration interface. It has the same three tabs (IPv4, IPv6, Status) with IPv6 selected. The 'Enable IPv6:' checkbox is checked. Below it, 'Origin Type:' is set to 'AUTO'. A horizontal line separates the top section from the bottom section. In the bottom section, 'Address Mode:' is set to 'Stateless Address', and a dropdown menu is open showing 'Stateless Address' and 'Stateful Address'. Below that, 'DUID:' is set to 'Stateless Address' and 'PD Enable:' is set to 'Stateful Address'. 'Rapid-commit Enable:' is unchecked. The 'DNS:' field contains eight input boxes with the values: 0000, 0000, 0000, 0000, 0000, 0000, 0000, 0. At the bottom, 'Enable MLD Proxy:' is checked. There are 'Save & Apply' and 'Reset' buttons at the very bottom.

III-3-5. Status

This page will show all the status of the wan connections.

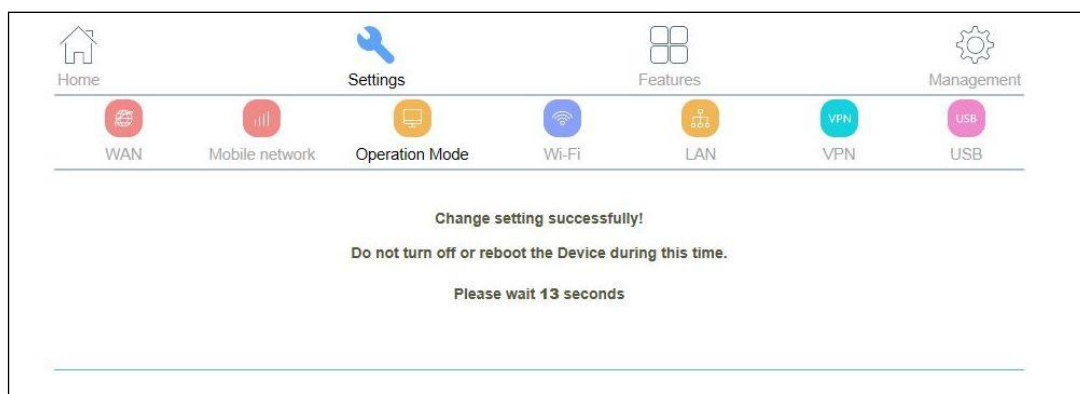
| IPv4 | | IPv6 | | | Status | | |
|--------------|----------|------|---------|-----------|--------------|-------------|-------------|
| Connect name | Enable | Type | Vlan ID | Status | IP Address | Gateway | DNS |
| WAN1 | Enabled | dhcp | --- | Connected | 192.168.1.89 | 192.168.1.1 | 192.168.1.1 |
| WAN2 | Disabled | | | | | | |
| WAN3 | Disabled | | | | | | |
| WAN4 | Disabled | | | | | | |

III-4. Operation Mode

Go to Settings > Operation Mode. If necessary, you can setup different modes.



Select the desired operation mode and click “Save& Apply”. Please wait for a moment for the change to take effect.



III-5. Wi-Fi

Go to Settings > WiFi. This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change 2.4G or 5G wireless encryption settings as well as other wireless network parameters.

III-5-1. Basic

Go to WiFi > Basic. This page is used to configure or check the basic parameters for wireless LAN clients which may connect to your Access Point.

| Basic | Security | ACL | Site Survey | WPS |
|--|----------|-----|-------------|-----|
| WLAN interface: 2.4G | | | | |
| Disable Wireless LAN Interface: <input type="checkbox"/> | | | | |
| Country or Region: UNITED STATES | | | | |
| Band: 2.4 GHz (B+G+N) | | | | |
| Mode: AP | | | | |
| Multiple AP | | | | |
| SSID: edimax_2.4G_01 | | | | |
| Channel Width: 40MHz | | | | |
| Control Sideband: Upper | | | | |
| Channel Number: Auto | | | | |
| BroadcastSSID: On | | | | |
| WMM: On | | | | |
| Data Rate: Auto | | | | |
| Associated Clients: Show Active Clients | | | | |

2.4GHz Wi-Fi Basic Settings

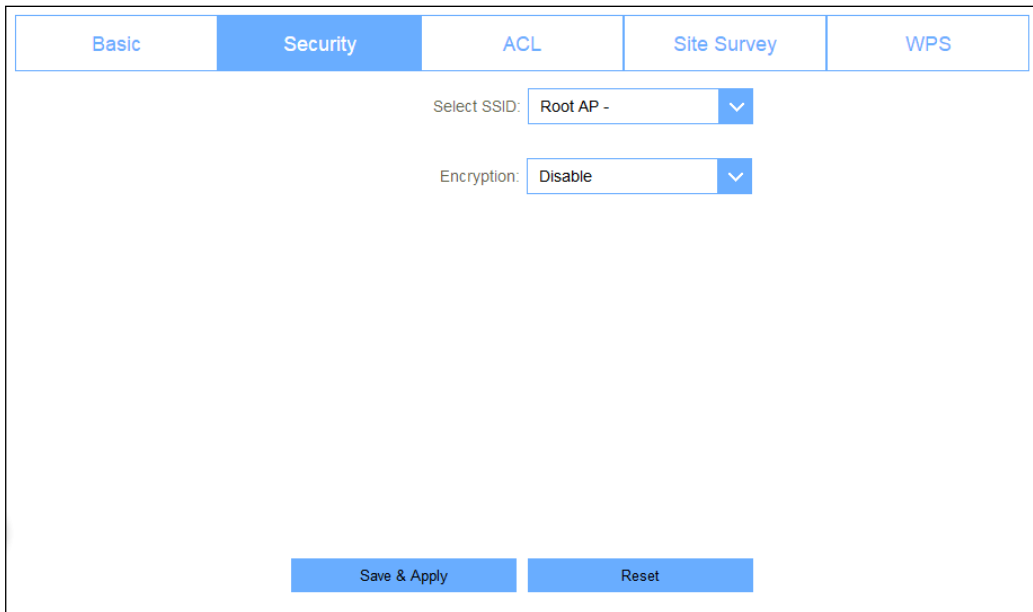
| Basic | Security | ACL | Site Survey | WPS |
|--|----------|-----|-------------|-----|
| WLAN interface: 5G | | | | |
| Disable Wireless LAN Interface: <input type="checkbox"/> | | | | |
| Country or Region: UNITED STATES | | | | |
| Band: 5 GHz (A+N+AC) | | | | |
| Mode: AP | | | | |
| Multiple AP | | | | |
| SSID: edimax_5G_c1 | | | | |
| Channel Width: 80MHz | | | | |
| Channel Number: Auto | | | | |
| BroadcastSSID: On | | | | |
| WMM: On | | | | |
| Data Rate: Auto | | | | |
| Associated Clients: Show Active Clients | | | | |

5GHz Wi-Fi Basic Settings

| | | |
|--------------------------|--|---|
| WAN interface | Select 2.4G to set parameters | |
| Country or Region | Check whether the name accords with your region | |
| Band | Select 2.4 GHz (B+G+N) or 5 GHz (A+N+AC) | |
| Mode | WLAN working mode, such AP, client, WDS and AP+ WDS | AP: this is the default mode that can be used as a routing pattern. The default is usually enough |
| | | Client: be used as a wireless network card |
| | | WDS: Wireless Bridge |
| | | AP+WDS: routing + Wireless Bridge mode |
| Multiple AP | You can set guest SSID from this button | |
| SSID | Set a name (SSID) for your wireless network. The ID of the wireless network. User can access the wireless network through it only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with. Default: edimax_2.4G_XXXX or edimax_5 G_XXXX. ("X" means the last 4 digits of the MAC address.) | |

III-5-2. Security

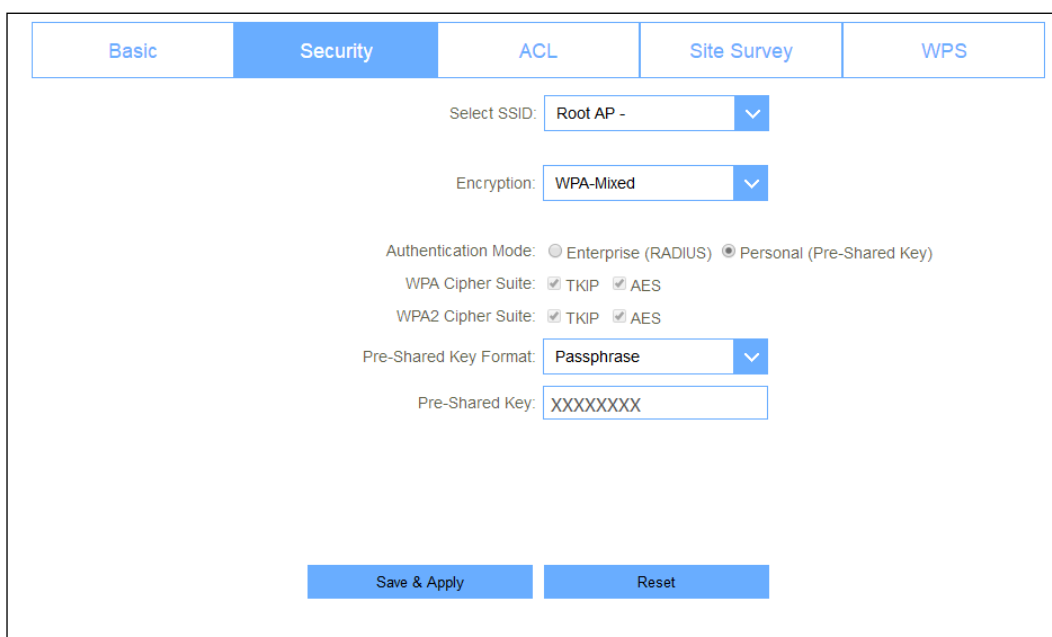
Go to WiFi > Security. This page allows you setup the wireless security. Using Encryption Keys could prevent any unauthorized access to your wireless network.



The screenshot shows the 'Security' tab selected in a navigation menu with options 'Basic', 'Security', 'ACL', 'Site Survey', and 'WPS'. Below the menu, there are two dropdown menus: 'Select SSID' with 'Root AP -' selected and 'Encryption' with 'Disable' selected. At the bottom, there are two buttons: 'Save & Apply' and 'Reset'.

It's worth mentioning that the default encryption is disabled. Select the security mode from the Encryption drop-down list. There are 4 options in the Security Mode drop-down list: Disable, WEP, WPA2, WPA- Mixed.

We strongly recommend you to set up WPA-Mixed encryption and enter 8 characters as the password for your wireless network.



The screenshot shows the 'Security' tab selected in a navigation menu with options 'Basic', 'Security', 'ACL', 'Site Survey', and 'WPS'. Below the menu, there are two dropdown menus: 'Select SSID' with 'Root AP -' selected and 'Encryption' with 'WPA-Mixed' selected. Below these are radio buttons for 'Authentication Mode' with 'Enterprise (RADIUS)' and 'Personal (Pre-Shared Key)' (selected). There are checkboxes for 'WPA Cipher Suite' (TKIP and AES, both checked) and 'WPA2 Cipher Suite' (TKIP and AES, both checked). Below these are a dropdown menu for 'Pre-Shared Key Format' with 'Passphrase' selected and a text input field for 'Pre-Shared Key' containing 'XXXXXXXX'. At the bottom, there are two buttons: 'Save & Apply' and 'Reset'.

III-5-3. ACL

Go to WiFi > ACL. There are 3 options in the Wireless ACL Mode drop-down list: Disable, Allowed Listed, Deny Listed. If you choose 'Allowed Listed', and enter the MAC Address, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point.

When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

The screenshot shows the ACL configuration page. At the top, there are five tabs: Basic, Security, ACL (selected), Site Survey, and WPS. Below the tabs, there is a form with the following fields:

- Wireless ACL Mode: A dropdown menu currently set to "Disable".
- MAC Address: An empty text input field.
- Comment: An empty text input field.

Below the form are two buttons: "Save & Apply" and "Reset".

Below the buttons is a section titled "Current ACL List". It contains a table with the following columns: "MAC Address", "Comment", and "Select". Below the table are three buttons: "Delete Selected", "Delete All", and "Reset".

III-5-4. Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

The screenshot shows the Site Survey page. At the top, there are five tabs: Basic, Security, ACL, Site Survey (selected), and WPS. Below the tabs, there is a single button labeled "Site Survey".

Below the button is a table with the following columns: "SSID", "BSSID", "Channel Number", "Type", "Encrypt", and "Signal".

III-5-5. WPS

This page allows you to change the settings for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

The screenshot shows the WPS configuration page with the following elements:

- Navigation tabs: Basic, Security, ACL, Site Survey, WPS (selected).
- Disable WPS:
- Buttons: Save & Apply, Reset
- WPS Status: Configured, UnConfigured
- Button: Reset to UnConfigured
- Auto-lock-down state: unlocked, Button: Unlock
- Self-PIN Number: 21595684
- Push Button Configuration: Button: Start PBC
- STOP WSC: Button: Stop WSC
- Connected State: Started
- Client PIN Number: Button: Start PIN

III-6. LAN

III-6-1. IPv4

Go to Settings > LAN > IPv4. This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc.

The screenshot shows the IPv4 configuration page with the following elements:

- Navigation tabs: IPv4 (selected), IPv6, RADVD, TUNNEL 6 over 4
- IP Address:
- Subnet Mask:
- Default Gateway:
- WORK MODE: (dropdown arrow)
- DHCP Client Range: - Button: Show Client
- Lease Time: (1 ~ 10080 minutes)
- Static DHCP: Button: Set Static DHCP
- Domain Name:
- 802.1d Spanning Tree: (dropdown arrow)
- Buttons: Save & Apply, Reset

| | |
|-----------------------------|--|
| LAN IP Address | Router's LAN IP. The default is 192.168.1.254. You can change it according to your needs. |
| Subnet Mask | Router's LAN subnet mask |
| WORK MODE | If it is selected, the router serves as the DHCP server and automatically assigns IP addresses to all computers in the LAN |
| DHCP Client Range | Enter the start and end IP address of all the available successive IPs. |
| Lease Time | Select the time for using one assigned IP from the dropdown list. After the lease time, the AP automatically assigns new IP addresses to all connected computers |
| Static DHCP | This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server |
| Domain Name | Set the domain name of the server |
| 802.1d Spanning Tree | Enable or disable spanning tree function |

III-6-2. IPv6

Go to Settings > LAN > IPv6. This page shows the information of IPv6.

The screenshot shows the IPv6 configuration interface. At the top, there are four tabs: 'IPv4', 'IPv6' (which is highlighted in blue), 'RADVD', and 'TUNNEL 6 over 4'. Below the tabs, the 'IP Address' field is displayed as a series of eight boxes, each containing '0000', followed by a final box containing '0'. Below the IP address field, there is a section titled 'Configuring DHCPv6 Server' with an 'Enable' checkbox that is currently unchecked. At the bottom of the page, there is a blue button labeled 'Save & Apply'.

III-6-3. RADVD

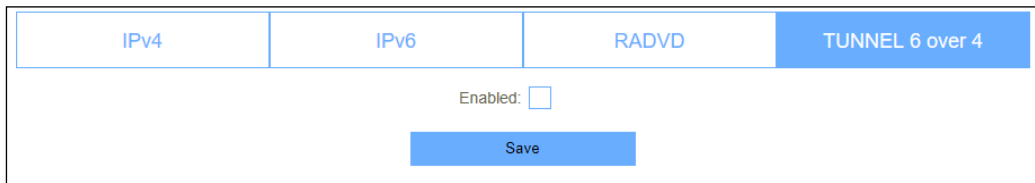
Go to Settings > LAN > RADVD. This page shows the information of RADVD.

| | |
|---------------------------|--|
| radvdinterfacename | Enter the interface name. |
| MaxRtrAdvInterval | Enter the max retry advertisement interval. |
| MinRtrAdvInterval | Enter the min retry advertisement interval. |
| MinDelayBetweenRAs | Enter the min delay between router advertisements. |

| | |
|-----------------------------|---|
| AdvManagedFlag | Enable or disable the advertisement managed |
| AdvOtherConfigFlag | Enable or disable the advertisement other |
| AdvLinkMTU | Enter the advertisement link MTU. |
| AdvReachableTime | Enter the advertisement reachable time. |
| AdvRetransTimer | Enter the advertisement retrains timer. |
| AdvCurHopLimit | Enter the advertisement current hop limit |
| AdvDefaultLifetime | Enter the advertisement default life time. |
| AdvDefaultPreference | Select from “high”, “medium” or “low” for |
| AdvSourceLLAddress | Enable or disable advertisement source link |
| UnicastOnly | Enable or disable unicast only. |
| Prefix1 Enabled | Enable or disable prefix. |
| prefix | Enter the prefix and prefix length. |
| AdvOnLinkFlag | Enable or disable advertisement on link flag. |
| AdvAutonomousFlag | Enable or disable advertisement autonomous |
| AdvValidLifetime | Enter advertisement valid life time. |
| AdvPreferredLifetime | Enter advertisement preferred life time. |
| AdvRouterAddr | Enable or disable advertisement router |
| If6to4 | Enter the interface 6to4. |

III-6-4. TUNNEL 6 over 4

Go to Settings > LAN > TUNNEL 6 over 4. This page is used for enable or disable Tunnel (6to4).



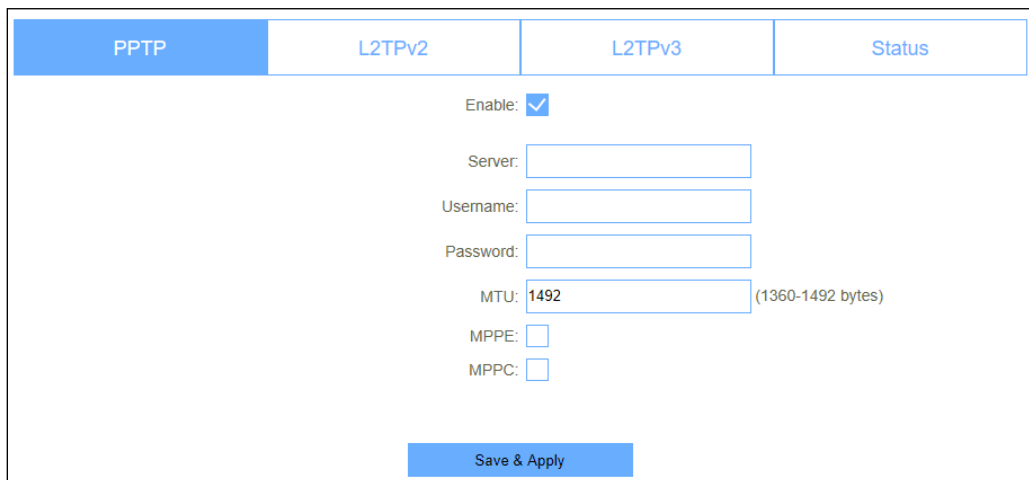
| IPv4 | IPv6 | RADVD | TUNNEL 6 over 4 |
|-----------------------------------|------|-------|-----------------|
| Enabled: <input type="checkbox"/> | | | |
| Save | | | |

III-7. VPN

Virtual Private Network (VPN) is the extension of enterprise Intranet. The virtual private network can help remote users, corporate branches, business partners and suppliers establish reliable and secure connections and ensure the security transmission of data. When you are on a business trip and need access to company data. To be secure, you need to connect to a VPN tunnel to establish communications.

III-7-1. PPTP

Go to Settings > VPN > PPTP. This page is used to configure the parameters for Internet network which connects to the PPTP server.



| PPTP | L2TPv2 | L2TPv3 | Status |
|--|--------|--------|--------|
| Enable: <input checked="" type="checkbox"/> | | | |
| Server: <input type="text"/> | | | |
| Username: <input type="text"/> | | | |
| Password: <input type="text"/> | | | |
| MTU: <input type="text" value="1492"/> (1360-1492 bytes) | | | |
| MPPE: <input type="checkbox"/> | | | |
| MPPC: <input type="checkbox"/> | | | |
| Save & Apply | | | |

| | |
|-----------------|--|
| Server | Type the name of PPTP Server. |
| Username | Enter the user name provided by your ISP. |
| Password | Enter the password provided by your ISP. |
| MTU | You can keep the maximum transmission unit (MTU) |

III-7-2. L2TPv2

Go to Settings > VPN > L2TPv2. This page is used to configure the parameters for Internet network which connects to the L2TPv2 server.

| | |
|-----------------|--|
| Server | Type the name of L2TP Server. |
| Username | Enter the user name provided by your ISP. |
| Password | Enter the password provided by your ISP. |
| MTU | You can keep the maximum transmission unit (MTU) as default. |

III-7-3. L2TPv3

Go to Settings > VPN > L2TPv3. This page is used to configure the parameters for Internet network which connects to peer by L2TPv3.

| PPTP | L2TPv2 | L2TPv3 | Status |
|---|--------|--------------------------------------|-------------------------|
| Enable: <input checked="" type="checkbox"/> | | | |
| Local Host Address: | | <input type="text" value="0.0.0.0"/> | (0.0.0.0 is autoconfig) |
| Remote Host Address: | | <input type="text"/> | |
| Local Udp Port: | | <input type="text"/> | (1 ~ 65535) |
| Remote Udp Port: | | <input type="text"/> | (1 ~ 65535) |
| Tunnel Address: | | <input type="text"/> | (172.10.12.1/24) |
| Remote Tunnel Address: | | <input type="text"/> | (172.10.13.1/24) |
| Tunnel Id: | | <input type="text"/> | (1 ~ 4294967295) |
| Remote Tunnel Id: | | <input type="text"/> | (1 ~ 4294967295) |
| Session Id: | | <input type="text"/> | (1 ~ 4294967295) |
| Remote session Id: | | <input type="text"/> | (1 ~ 4294967295) |
| MTU: | | <input type="text" value="1488"/> | (1360-1488 bytes) |
| <input type="button" value="Save & Apply"/> | | | |

| | |
|------------------------------|---|
| Local Host Address | The address of the LAN side device of local , eg: 192.168.2.1 |
| Remote Host Address | The address of the LAN side device of remote host , eg: 192.168.8.2 |
| Local Udp Port | LAN side device udp port. |
| Remote Udp Port | Remote device udp port |
| Tunnel Address | Wan interface IP address |
| Remote Tunnel Address | Remote device WAN interface IP address |
| Tunnel Id | Local device tunnel id |
| Remote Tunnel Id | Remote device tunnel id |
| Session Id | Local device session id |

| | |
|--------------------------|--|
| Remote session Id | Remote device session id |
| MTU | You can keep the maximum transmission unit (MTU) as default. |

III-7-4. Status

Go to Settings > VPN > Status. This page shows the status information for PPTP, L2TP and L2TPv3.

| PPTP | | L2TPv2 | | L2TPv3 | | Status |
|--------------|----------|-------------------|------------------|-------------------|--------|--------|
| Connect name | Enable | Server IP Address | Local IP Address | Remote IP Address | Status | |
| PPTP | Disabled | | | | | |
| L2TP | Disabled | | | | | |
| L2TPv3 | Disabled | | | | | |

III-8. USB

III-8-1. Disk Information

Go to Settings > USB > Disk Information. This page shows disk information.

| Disk Information | | Account Management | | Share Folder | |
|------------------|-------------|--------------------|----------|--------------|-------------|
| Disk Information | | | | | |
| Partition | Total Space | Available Space | had Used | Use per | System Type |
| | | | | | |

III-8-2. Account Management

Go to Settings > USB > Account Management. This page shows disk information. If enable anonymous access, can only access specific directory [public], the [public] directory located in the first partition of the first disk.

| Disk Information | Account Management | Share Folder | | | | |
|---|--------------------|--------------|-----------|--------|---|--|
| Enable Anonymous Access: <input type="checkbox"/> | | | | | | |
| <input type="button" value="Apply Changes"/> | | | | | | |
| Add a new samba account here | | | | | | |
| User Name: <input type="text"/> | | | | | | |
| Password: <input type="password"/> | | | | | | |
| Confirmed Password: <input type="password"/> | | | | | | |
| <input type="button" value="Apply Changes"/> | | | | | | |
| Current Account Table | | | | | | |
| <table border="1"> <thead> <tr> <th>User Name</th> <th>Select</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> </td> </tr> </tbody> </table> | | | User Name | Select | <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> | |
| User Name | Select | | | | | |
| <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> | | | | | | |

III-8-3. Share Folder

Go to Settings > USB > Share Folder. This page used for add/delete share folder. Enter the Folder Name and select the Folder Path and Permission.

| Disk Information | Account Management | Share Folder | | | | | | | | | | |
|---|--------------------|--------------|-------------|-------------|-------|------------|--------|---|--|--|--|--|
| Folder Name: <input type="text"/> | | | | | | | | | | | | |
| Folder Path: <input type="text"/> <input type="button" value="v"/> | | | | | | | | | | | | |
| Owner: No accounts available, please add account first | | | | | | | | | | | | |
| Permission: <input type="text" value="Read Only"/> <input type="button" value="v"/> | | | | | | | | | | | | |
| <input type="button" value="Apply Changes"/> | | | | | | | | | | | | |
| Current Share Folder Table | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Folder Name</th> <th>Folder Path</th> <th>Owner</th> <th>Permission</th> <th>Select</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="text-align: center;"> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> </td> </tr> </tbody> </table> | | | Folder Name | Folder Path | Owner | Permission | Select | <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> | | | | |
| Folder Name | Folder Path | Owner | Permission | Select | | | | | | | | |
| <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> | | | | | | | | | | | | |

IV. Features

IV-1. QoS

Go to Features > QoS. QoS (Quality of Service) refers to a network that can utilize various basic technologies to provide better service capability for designated network communication. It is a security mechanism of the network and a technology used to solve problems such as network delay and blocking. For example, users can improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic through setting QoS function. For example, I have several devices that are connected to my wireless network. I would like to set an intermediate speed on the Internet for my specified device.

There are two work modes for QoS function: Guaranteed minimum bandwidth and Restricted maximum bandwidth. Select any one of them in the mode drop-down list and then enter the corresponding information.

The screenshot displays a configuration page for Quality of Service (QoS). At the top, there are three checked checkboxes: "Enable QoS", "Automatic Uplink Speed", and "Automatic Downlink Speed". Below these are several input fields and dropdown menus. The "Name" field is empty. The "QoS Type" dropdown is set to "IPv4", and the "protocol" dropdown is set to "Both". There are four pairs of input fields for "Local IP Address", "Local Port", "Remot IP Address", and "Remote Port", all of which are currently empty. The "Mode" dropdown is set to "Guaranteed minimum". Below this are three more input fields: "Uplink Bandwidth (Kbps)", "Downlink Bandwidth (Kbps)", and "Remark DSCP" (with a range of 0-63). A "Comment" field is at the bottom. At the very bottom of the form are two buttons: "Save & Apply" and "Reset".

| | |
|-------------------------------------|--|
| Automatic Uplink Speed | Automatic uplink speed. |
| Automatic Downlink Speed | Automatic downlink speed. |
| Manual Downlink Speed (Kbps) | Set the upload speed of your Internet access |
| Name | QoS rule name. |

IV-2. Firewall

Firewall can prevent cyber attacks and validate the traffic that is passing through the router based on the protocol.

IV-2-1. Advanced

Go to Features > Firewall > Advanced. Your router's high-performance firewall feature continuously monitors Internet traffic, protecting your network and connected devices from malicious Internet attacks.

| Advanced | DoS | IP Filtering | Port Filtering | MAC Filtering |
|---|-----|--------------|----------------|---------------|
| Enable DMZ: <input type="checkbox"/> Enable UPNP: <input type="checkbox"/> Enable IGMP Proxy: <input type="checkbox"/> Enable Telnet Access on LAN: <input checked="" type="checkbox"/> Enable Telnet Access on WAN: <input type="checkbox"/> Enable Ping Access on WAN: <input type="checkbox"/> Enable Web Server Access on WAN: <input type="checkbox"/> Enable IPsec pass through on VPN connection: <input checked="" type="checkbox"/> Enable PPTP pass through on VPN connection: <input checked="" type="checkbox"/> Enable L2TP pass through on VPN connection: <input checked="" type="checkbox"/> | | | | |
| Save & Apply | | Reset | | |

| | |
|---|---|
| Enable DMZ | Enable or disable DMZ function. |
| Enable UPnP | Enable or disable UPnP function. |
| Enable IGMP Proxy | Enable or disable IGMP Proxy function. |
| Enable Telnet Access on LAN | Enable or disable Telnet by LAN access. |
| Enable Telnet Access on WAN | Enable or disable Telnet by wan access. |
| Enable Ping Access on WAN | Enable or disable Enable Ping Access on WAN function. |
| Enable Web Server Access on WAN | Enable or disable Enable Web Server Access on WAN function. |
| Enable IPsec pass through on VPN | Enable or disable IPSEC to pass through IPSEC communication data. |
| Enable PPTP pass through on VPN | Enable or disable PPTP to pass through PPTP communication data. |
| Enable L2TP pass through on VPN connection | Enable or disable L2TP to pass through L2TP communication data. |

IV-2-2. DoS

Go to Features > Firewall > DoS. A denial-of-service (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

| Advanced | DoS | IP Filtering | Port Filtering | MAC Filtering |
|---|-----|--|----------------|---------------|
| Enable DoS Prevention <input type="checkbox"/> | | | | |
| Whole System Flood: SYN <input type="checkbox"/> 0 Packets/Second | | | | |
| Whole System Flood: FIN <input type="checkbox"/> 0 Packets/Second | | | | |
| Whole System Flood: UDP <input type="checkbox"/> 0 Packets/Second | | | | |
| Whole System Flood: ICMP <input type="checkbox"/> 0 Packets/Second | | | | |
| Per-Source IP Flood: SYN <input type="checkbox"/> 0 Packets/Second | | | | |
| Per-Source IP Flood: FIN <input type="checkbox"/> 0 Packets/Second | | | | |
| Per-Source IP Flood: UDP <input type="checkbox"/> 0 Packets/Second | | | | |
| Per-Source IP Flood: ICMP <input type="checkbox"/> 0 Packets/Second | | | | |
| TCP/UDP PortScan: <input type="checkbox"/> Low Sensitivity <input type="button" value="v"/> | | | | |
| ICMP Smurf: <input type="checkbox"/> | | | | |
| IP Land: <input type="checkbox"/> | | | | |
| IP Spoof: <input type="checkbox"/> | | | | |
| IP TearDrop: <input type="checkbox"/> | | | | |
| PingOfDeath: <input type="checkbox"/> | | | | |
| TCP Scan: <input type="checkbox"/> | | | | |
| TCP SynWithData: <input type="checkbox"/> | | | | |
| UDP Bomb: <input type="checkbox"/> | | | | |
| UDP EchoChargen: <input type="checkbox"/> | | | | |
| <input type="button" value="Select ALL"/> | | <input type="button" value="Clear ALL"/> | | |
| Enable Source IP Blocking: <input type="checkbox"/> 0 Block time (sec) | | | | |
| <input type="button" value="Save & Apply"/> | | | | |

IV-2-3. IP Filtering

Go to Features > Firewall > IP Filtering. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

| Advanced | DoS | IP Filtering | Port Filtering | MAC Filtering |
|---|-----|--------------------------------------|----------------|---------------|
| Enable IP Filtering: <input type="checkbox"/> | | | | |
| Enable IPv4: <input type="checkbox"/> | | | | |
| Enable IPv6: <input type="checkbox"/> | | | | |
| Local IPv4 Address: <input type="text"/> | | | | |
| Local IPv6 Address: <input type="text"/> | | | | |
| Protocol: Both <input type="button" value="v"/> | | | | |
| Comment: <input type="text"/> | | | | |
| <input type="button" value="Save & Apply"/> | | <input type="button" value="Reset"/> | | |

| | |
|----------------------------|---|
| Enable IP Filtering | Enable or disable IP Filtering function. |
| Enable IPv4 | Enable or disable IPv4 Filtering feature. |
| Enable IPv6 | Enable or disable IPv6 Filtering feature. |
| Local IPv4 Address | Set LAN side source IPv4 address |
| Local IPv6 Address | Set LAN side source IPv6 address |
| Protocol | Select "TCP", "UDP" or "Both" |
| Comment | Comment for the rule. |

IV-2-4. Port Filtering

Go to Features > Firewall > Port Filtering. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

| | |
|------------------------------|--|
| Enable Port Filtering | Enable or disable IP Filtering function. |
| Enable IPv4 | Enable or disable IPv4 Port Filtering feature. |
| Enable IPv6 | Enable or disable IPv6 Port Filtering feature. |
| Port Range | Set the port range for port filtering |
| Protocol | Select "TCP", "UDP" or "Both" |

| | |
|----------------|-----------------------|
| Comment | Comment for the rule. |
|----------------|-----------------------|

IV-2-5. MAC Filtering

Go to Features > Firewall > MAC Filtering. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

| | |
|--------------------|--|
| Model | You can set working model here, Black and White. |
| MAC Address | Enter a MAC address. |
| Comment | Comment info. |
| Interface | WAN interface for the rule. |

IV-2-6. Port Forwarding

Go to Features > Port Forwarding. Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Enable Port Forwarding:

Local IP Address:

Local Port Start:

Local Port End:

Protocol:

Remote IP Address:

Remote Port Start:

Remote Port End:

Comment:

Current Port Forwarding Table

| Local IP Address | Local Port Range | Protocol | Remote IP Address | Remote Port Range | Status | Comment | Select |
|------------------|------------------|----------|-------------------|-------------------|----------|---------|--------------------------|
| 192.168.1.100 | 80 | TCP+UDP | ANY | --- | Disabled | 22 | <input type="checkbox"/> |

| | |
|-------------------------------|---|
| Enable Port Forwarding | Enable or disable Port Forwarding function. |
| Local IP Address | Enter a LAN IP address |
| Local Port Start | Enter LAN side start port. |
| Local Port End | Enter LAN side end port. |
| Protocol | Select "TCP", "UDP" or "Both". |
| Remote IP Address | Enter a WAN IP address |
| Remote Port Start | Enter the external start port |
| Remote Port End | Enter the external end port |
| Comment | Enter the port number |

IV-2-7. URL Filter

Go to Features > URL Filter. URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below. Please note: URL Filter cannot filter the HTTPS encrypted domain name.

Enable URL Filtering:

Deny URL address(black list):

Allow URL address(white list):

URL Address:

url Filter Table

| URL Address | Select |
|-------------|--------|
|-------------|--------|

| | |
|---------------------------------------|---|
| Enable URL Filtering | Enable or disable URL Filtering function. |
| Deny URL address (black list) | Blocking access to the URL list. |
| Allow URL address (white list) | Allowing access to the URL list. |
| URL Address | Block or allow access URL. |

IV-2-8. Route

IV-2-8-1. Default Route

It does not require you to make any settings in this option because there is only one wan port for BR-6478AC V3.

IV-2-8-2. Static Route

Go to Route > Static Route. Once connected to the Internet, your router automatically builds routing tables that determine where traffic should be sent. Static routes can override this process, allowing traffic to be directed to a specific client or location.

| | |
|----------------------------|---------------------------------|
| Enable Static Route | Enable or disable Static route. |
| IP Address | Enter the destination network |
| Subnet Mask | Enter the network mask |
| Gateway | Enter the network gateway |
| Metric | Enter the routing metric |
| Interface | Select the interface |

IV-2-8-3. Dynamic DNS

The Wireless Router supports Dynamic Domain Name Service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers.

Enable DDNS:

Service Provider: DynDNS ▼

Domain Name: host.dyndns.org

User Name/Email:

Password/Key:

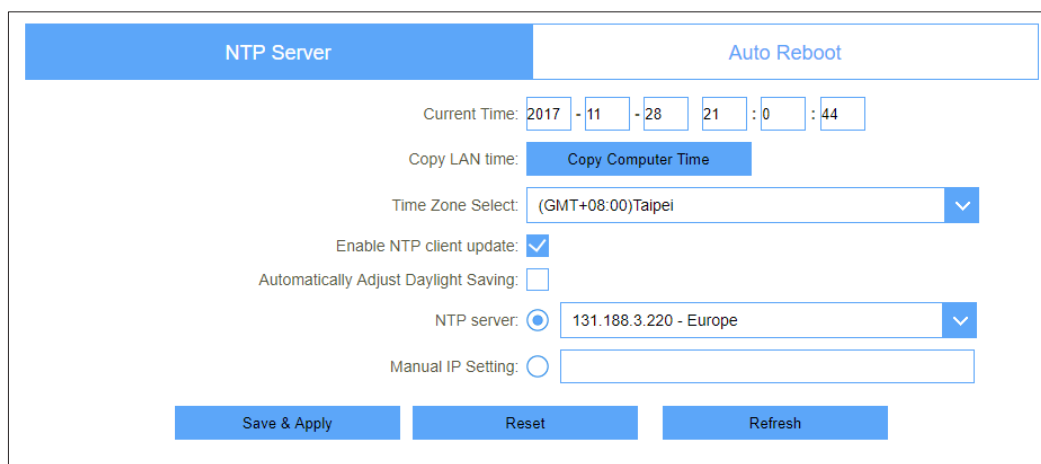
| | |
|------------------------|---|
| Server Provider | Select server from the drop-down list <ul style="list-style-type: none"> ● DynDNS ● TZO |
| Domain Name | Enter the host name |
| User Name/Email | Enter the user name |
| Password/Key | Enter the password |

V. Management

V-1. Time

V-1-1. NTP Server

Go to Management > Time > NTP Server. You can maintain the system time by synchronizing with a public time server over the Internet.



| | |
|---|--|
| Current Time | Select the time zone in your area. |
| Copy LAN time | Copy time from computer. |
| Time Zone Select | Select time zone from the drop box. |
| Enable NTP client | Enable or disable NTP client update. |
| Automatically Adjust Daylight Saving | Enable or disable daylight saving if you need this function. |
| NTP Server | Select the well know NTP Server. |
| Manual IP Setting | Enter the server manually. |

V-1-2. Auto Reboot

Go to Management > Time > Auto Reboot. This feature can do the Reboot automatically at a specified time. Please note: “Auto Reboot” depend on the “NTP Server”, you have to enable the 'NTP Server' when use this feature.

| NTP Server | Auto Reboot |
|--|-------------|
| Days: <input type="text" value="0"/> | |
| Hours Range: <input type="text" value="0"/> - <input type="text" value="0"/> | |
| Enable: <input type="button" value="Off"/> <input type="button" value="v"/> | |
| <input type="button" value="Save & Apply"/> | |

V-2. System Log

Go to Management > System Log. This page can be used to set remote log server and show the system log.

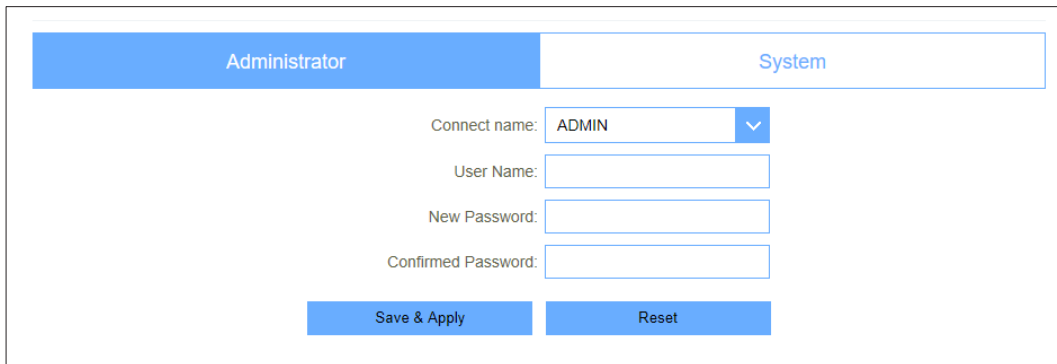
| | |
|--|--------------------------|
| Enable Log: | <input type="checkbox"/> |
| System All: | <input type="checkbox"/> |
| Wireless: | <input type="checkbox"/> |
| DoS: | <input type="checkbox"/> |
| Enable Remote Log: | <input type="checkbox"/> |
| Log Server IP Address: | <input type="text"/> |
| <input type="button" value="Apply Changes"/> | |
| <div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div> | |

| | |
|------------------------------|--|
| Enable Log | Enable or disable Log function. |
| System All | Print all log information. |
| Wireless | Print wireless log information. |
| DoS | Print DoS log information. |
| Enable Remote Log | Enable or disable “Logging to Syslog Server” |
| Log Server IP Address | Enter the Syslog server IP address |

V-3. System Settings

V-3-1. Administrator

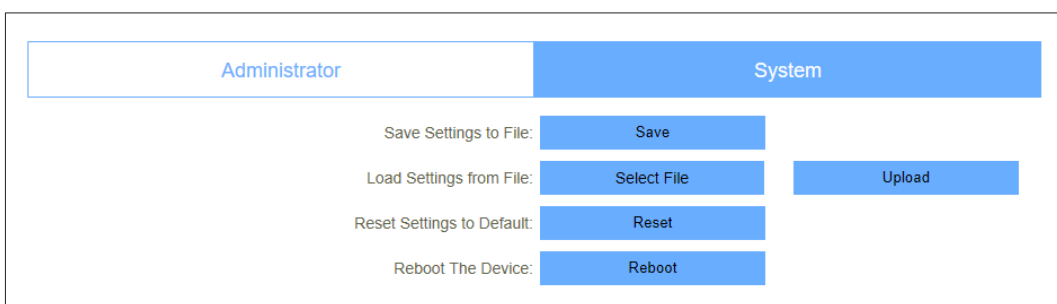
Go to Management > Administrator. This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.



| | |
|---------------------------|----------------------------------|
| Connect name | Select an account to be modified |
| Username | Enter the new username. |
| Password | Enter the new password. |
| Confirmed Password | Enter the new password again. |

V-3-2. System

Go to Management > System. This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.



| | |
|----------------------------------|---------------------------------------|
| Save settings to file | Save the setting to local PC |
| Load settings from File | Load the settings from local PC |
| Reset Settings to Default | Restore the device to factory default |
| Reboot the device | Press the button to reboot the device |



When you load new configuration, the original configuration will be lost. Please back up the current configuration before loading a new one. In this way, if the new configuration file has an error, you can load the backup file.



DO NOT shut down your router when loading a configuration file. Otherwise, the router may be damaged.

V-4. Statistics

V-4-1. User Statistics

Go to Management > Statistics > User Statistics. 'User Statistics' will show each user's total traffic statistics.

| User Statistics | | Interface Statistics | |
|-----------------|------------------|----------------------|--|
| IP Addr | Total Down | Total Up | |
| 192.168.0.1 | 25 084 013 Bytes | 5 255 176 Bytes | |
| 192.168.0.2 | 1 473 Bytes | 994 Bytes | |
| 192.168.0.3 | 0 Bytes | 0 Bytes | |
| 192.168.0.4 | 0 Bytes | 0 Bytes | |
| 192.168.0.5 | 0 Bytes | 0 Bytes | |
| 192.168.0.6 | 0 Bytes | 0 Bytes | |
| 192.168.0.7 | 77 722 Bytes | 5 544 Bytes | |

V-4-2. Interface Statistics

Go to Management > Statistics > Interface Statistics. This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

| User Statistics | Interface Statistics | |
|-----------------|----------------------|-----------|
| Wireless 1 LAN | Sent Bytes | 15067344 |
| | Received Bytes | 194910485 |
| Wireless 2 LAN | Sent Bytes | 558925796 |
| | Received Bytes | 157010398 |
| Ethernet LAN1 | Sent Bytes | 0 |
| | Received Bytes | 0 |
| Ethernet LAN2 | Sent Bytes | 0 |
| | Received Bytes | 0 |
| Ethernet LAN3 | Sent Bytes | 0 |
| | Received Bytes | 0 |
| Ethernet LAN4 | Sent Bytes | 0 |
| | Received Bytes | 0 |
| WAN | Sent Bytes | 24482344 |
| | Received Bytes | 502793254 |

[Refresh](#)

V-5. Diagnostics

V-5-1. Ping

Go to Management > Diagnostics > Ping. This page gives you various diagnostics about ping for IP connection.

[Ping](#) [Traceroute](#)

Host Name or Ip Address: [RUN](#)

V-5-2. Traceroute

Go to Management > Diagnostics > Traceroute. This page gives you various diagnostics about traceroute for IP connection.

V-6. TR069

Go to Management > TR069. ISP may use this function to remote management. User can configure the TR- 069 in this page. Here you may change the setting for the ACS's parameters.

| | |
|------------------|----------------------------------|
| TR069 | Enable or disable TR069. |
| ACS | ACS server domain or IP Address. |
| User Name | User name for connection to ACS. |
| Password | Password for connection to ACS. |

| | |
|-------------------------------------|---------------------------------------|
| Periodic Inform Enable | Enable or disable periodic inform. |
| Periodic Inform Interval | Periodic inform interval. |
| Connection Request User Name | User Name used form ACS connection to |
| Connection Request Password | Password used form ACS connection to |
| Path | Connection request path. |
| Port | Connection port. |

V-7. Upgrade

Go to Management > Upgrade. This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: EDIMAX_V1.0.4


Select File:

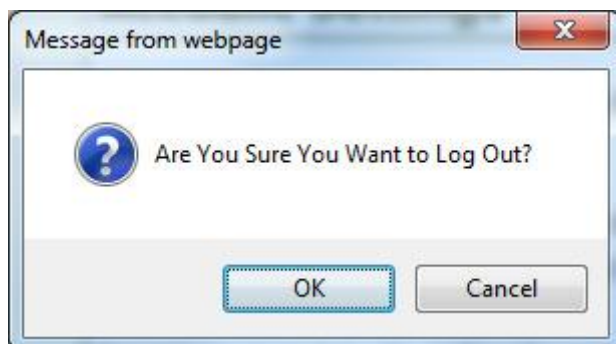
COPYRIGHT © All Rights Reserved.



DO NOT turns off the power or press the Reset button when updating the firmware. Otherwise, the router may be damaged.

VI. Logout

If you want to leave current interface, please  click icon to logout.



VII. FAQ


If you are experiencing problems with your BR-6478AC V3, please check below before contacting your dealer of purchase for help.



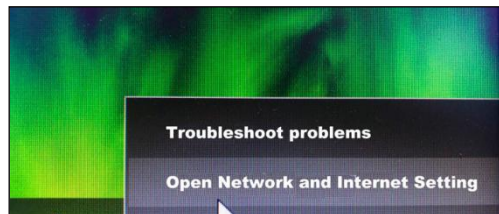
If you are experiencing problems immediately after a firmware upgrade, please contact your dealer of purchase for help.

1. How to set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer?

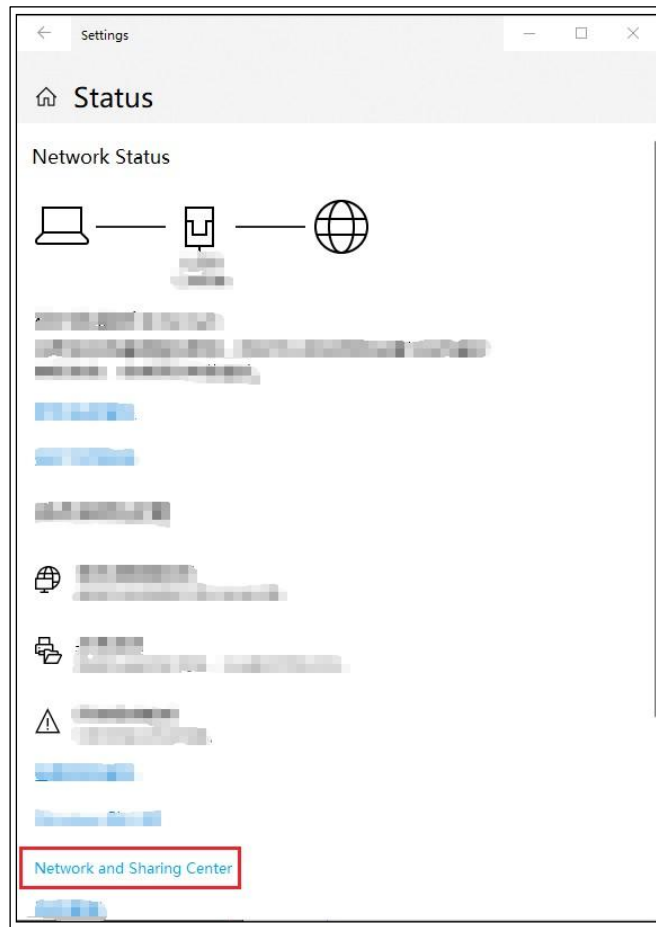
- a. A computer installed with a wired network adapter is used as an example here to describe the steps in **Win 10** and in similar steps for the other systems.

Step 1. Right-click  in the lower-right corner of the desktop and choose

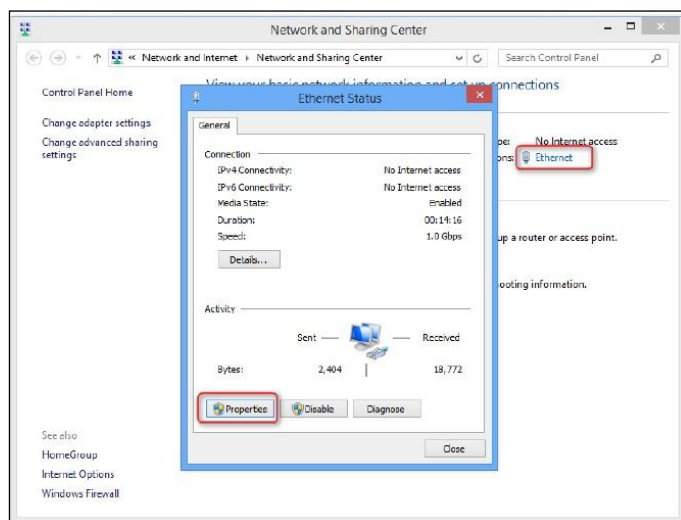
Open Network and Internet Setting.



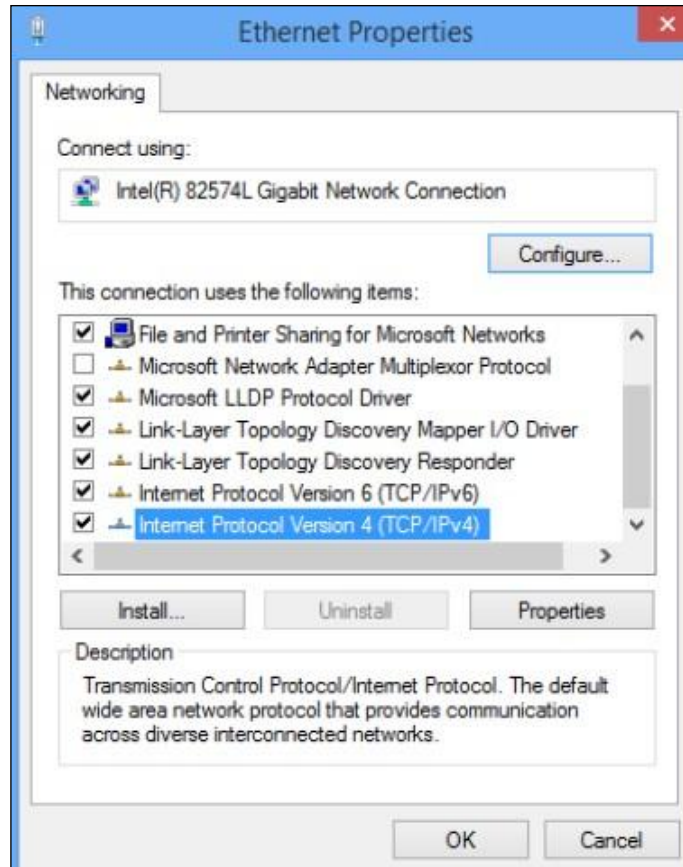
Step 2. Click **Network and Sharing Center**.



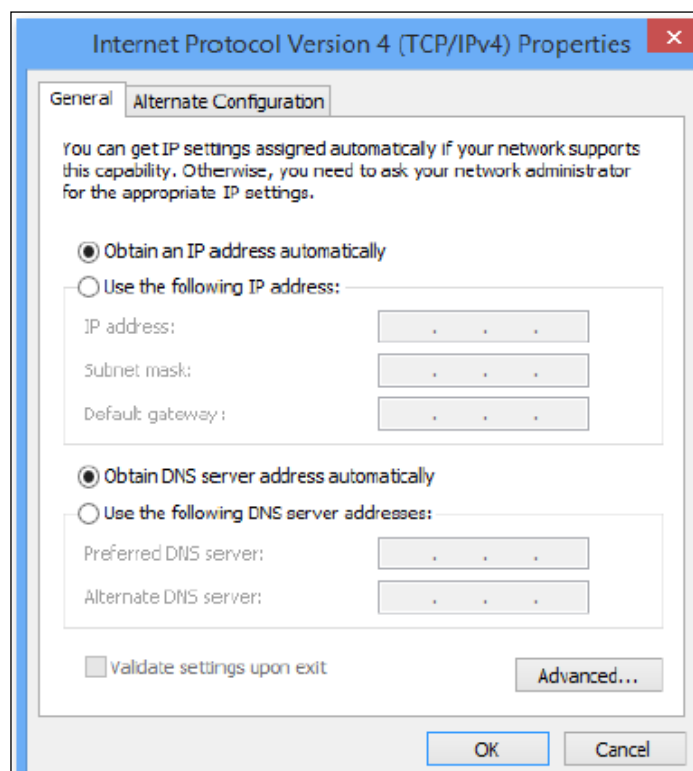
Step 3. Click **Ethernet and Properties**.



Step 4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Step 5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Step 6. You'll go back to the **Ethernet Properties** box, please click **OK**.

2. I can't open the browser based configuration interface.

- a. Make sure the connection of WAN and LAN port(s) is correct.
- b. Ensure that your Ethernet cable with internet connectivity is plugged into the WAN port of the router rather than a LAN port.
- c. Ensure that your wireless device is connected to the LAN port(s) of the router.
- d. Make sure you enter the correct IP address (192.168.2.1) to log in.
- e. Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.
- f. Use another web browser to log in again.
- g. Reset the router to factory default settings and try again.

3. How do I reset my device to factory default settings?

- a. To reset the device back to its factory default settings, press and hold the WPS/Reset button for over 10 seconds, until the power LED begins to flash. Please wait a few minutes for the product to restart. When the device restarts, all settings will be reset. Default settings are displayed on the product label on the back of the device.

| | |
|---------------------------|---|
| Router Login | Enter this URL in a web browser to run iQ Setup or configure advanced settings. You must be connected to the device by Wi-Fi or Ethernet cable. |
| Username/Password | This is the default username and password to access the browser based configuration interface when you go to the "Router Login" URL (above). |
| Wi-Fi Network Name | This is the default Wi-Fi network name for the device. Search for this name (SSID) and connect to it in order to access the "Router Login" URL (above). |
| MAC | A MAC address is unique to every device and is used for identification within a network. Your device's unique MAC addresses are displayed here. |
| PIN CODE | This is your device's PIN code for Wi-Fi Protected Setup (WPS) for each wireless frequency. |

4. I forgot my password.

- a. Reset the router to its factory default settings and use the default username **admin** and default password **1234**. Default settings are displayed on the product label on the back of the device, as shown above.

5. If An IP address conflict message appears after the computer is connected to the router, what should I do?

- a. Ensure that there is no other DHCP server in your LAN or the other DHCP server is disabled.
- b. Make sure the IP address of your router is not used by another device in your LAN. The default IP address of the router is 192.168.2.1.
- c. Ensure that the static IP address assigned to the computer in your LAN is not used by other devices.

COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

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

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such as PDAs or lap pads is not authorized. This transmitter is restricted for use with the specific antenna tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

| Frequency range (MHz) | Max. Transmit Power (dBm) |
|-----------------------|---------------------------|
| 2412-2472 | 17.87 dBm |
| 5150-5240 | 21.09 dBm |

A simplified DoC shall be provided as follows: Article 10(9)

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type **AC1200 Wireless Router** is in compliance with Directive 2014/53/EU

The full text of the EU declaration of conformity is available at the following internet address: <http://www.edimax.com/edimax/global/>

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical

equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

- English:** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/35/EU.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU.
- Polski:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU.
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/35/EU.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/35/EU).
- Türkçe:** Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/35/EU.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU.
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 2014/53/EU, 2014/35/EU.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/35/EU.
- suomen kieli:** Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN 



WEEE Directive & Product Disposal



At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European Radio Equipment directives.

Equipment: AC1200 Wireless router
Model No.: BR-6478AC V3

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

Spectrum : EN 300 328 V2.1.1:2016
EN 301 893 V2.1.1:2017
EMC : EN 301 489-1 V2.2.0:2017
EN 301 489-17 V3.2.0:2017
EMF : EN 62311:2008

Directives 2014/35/EU

Safety (LVD) : IEC 60950-1:2005 (2nd Edition)+Am 1:2009+Am 2:2013
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

a company of :
Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd.,
Neihu Dist., Taipei City,
Taiwan

Signature:

Printed Name: David Huang
Title: Director
Edimax Technology Europe B.V.



Date of Signature: Nov., 2018

Signature:

Printed Name:

Albert Chang

Title:

Director

Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.