

# BR-6288ACL

## User Manual

09-2014 / v1.0

---

### **Edimax Technology Co., Ltd.**

No.3, Wu-Chuan 3rd Road, Wu-Gu, New Taipei City 24891, Taiwan

Email: [support@edimax.com.tw](mailto:support@edimax.com.tw)

---

### **Edimax Technology Europe B.V.**

Fijenhof 2, 5652 AE Eindhoven, The Netherlands

Email: [support@edimax.nl](mailto: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](mailto:support@edimax.com)

# CONTENTS

<b>I. Product Information.....</b>	<b>1</b>
I-1. Package Contents .....	1
I-2. LED Status .....	2
I-3. Back Panel.....	3
I-4. RJ-45 Splitter Cable .....	4
I-5. Wi-Fi Power Switch .....	5
I-6. Safety Information .....	6
<b>II. Installation.....</b>	<b>7</b>
II-1. Wi-Fi Router Mode .....	10
II-2. Access Point Mode.....	15
II-3. Range Extender Mode .....	20
II-4. Wireless Bridge Mode.....	27
II-5. WISP Mode .....	33
II-6. WPS Setup.....	41
II-7. Reset to Factory Default Settings .....	41
<b>III. Browser Based Configuration Interface.....</b>	<b>42</b>
III-1. Login.....	42
III-2. Save Settings.....	44
III-3. Main Menu .....	45
III-3-1. Status .....	46
III-3-2. Setup Wizard.....	47
III-3-3. Internet/WISP .....	49
III-3-3-1. WAN Setup.....	50
III-3-3-1-1. Dynamic IP .....	50
III-3-3-1-2. Static IP .....	52
III-3-3-1-3. PPPoE .....	54
III-3-3-1-4. PPTP .....	56
III-3-3-1-5. L2TP.....	59
III-3-3-2. DDNS.....	61
III-3-4. LAN.....	63
III-3-5. 2.4GHz Wireless & 5GHz Wireless.....	66
III-3-5-1. Basic .....	66
III-3-5-1-1. Disable .....	70
III-3-5-1-2. WEP.....	71
III-3-5-1-3. WPA Pre-Shared Key.....	72
III-3-5-1-4. WPA Radius.....	73
III-3-5-2. Guest/ Multiple SSID.....	74

III-3-5-3.	WPS.....	77
III-3-5-4.	Access Control .....	78
III-3-5-5.	Schedule.....	80
III-3-6.	Firewall.....	82
III-3-6-1.	URL Blocking .....	82
III-3-6-2.	Access Control .....	84
III-3-6-3.	DMZ.....	88
III-3-6-4.	DoS.....	89
III-3-7.	QoS.....	91
III-3-7-1.	QoS.....	91
III-3-7-2.	iQoS.....	94
III-3-8.	Advanced .....	96
III-3-8-1.	Static Routing.....	96
III-3-8-2.	Port Forwarding .....	97
III-3-8-3.	Virtual Server .....	99
III-3-8-4.	2.4GHz Wireless.....	100
III-3-8-5.	5GHz Wireless .....	102
III-3-8-6.	IGMP .....	104
III-3-8-7.	UPnP.....	104
III-3-9.	Administration .....	105
III-3-9-1.	Time Zone .....	105
III-3-9-2.	Password.....	106
III-3-9-3.	Remote Access.....	107
III-3-9-4.	Backup/Restore .....	108
III-3-9-5.	Upgrade .....	108
III-3-9-6.	Restart.....	109
III-3-9-7.	Logs .....	109
III-3-9-8.	Active DHCP Client.....	110
III-3-9-9.	Statistics.....	110

## **IV. Appendix .....111**

IV-1.	Configuring your IP address.....	111
IV-1-1.	How to check that your computer uses a dynamic IP address .....	112
IV-1-1-1.	Windows XP .....	112
IV-1-1-2.	Windows Vista .....	114
IV-1-1-3.	Windows 7 .....	116
IV-1-1-4.	Windows 8 .....	119
IV-1-1-5.	Mac OS.....	123
IV-1-2.	How to modify the IP address of your computer .....	125
IV-1-2-1.	Windows XP .....	125
IV-1-2-2.	Windows Vista .....	127
IV-1-2-3.	Windows 7 .....	128

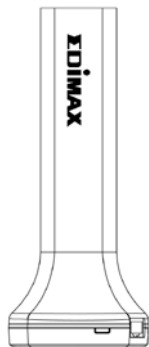
IV-1-2-4.	Windows 8 .....	131
IV-1-2-5.	Mac .....	135
IV-1-3.	How to Find Your Network Security Key .....	138
IV-1-3-1.	Windows 7 & Vista.....	138
IV-1-3-2.	Mac .....	140
IV-1-4.	How to Find Your Router's IP Address.....	143
IV-1-4-1.	Windows XP, Vista & 7.....	143
IV-1-4-2.	Windows 8 .....	145
IV-1-4-3.	Mac .....	148
IV-2.	Connecting to a Wi-Fi network.....	150
IV-3.	Troubleshooting.....	152

# ***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-6288ACL***



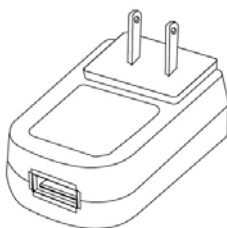
***CD-ROM***



***RJ-45 Splitter Cable***



***Quick Installation Guide***

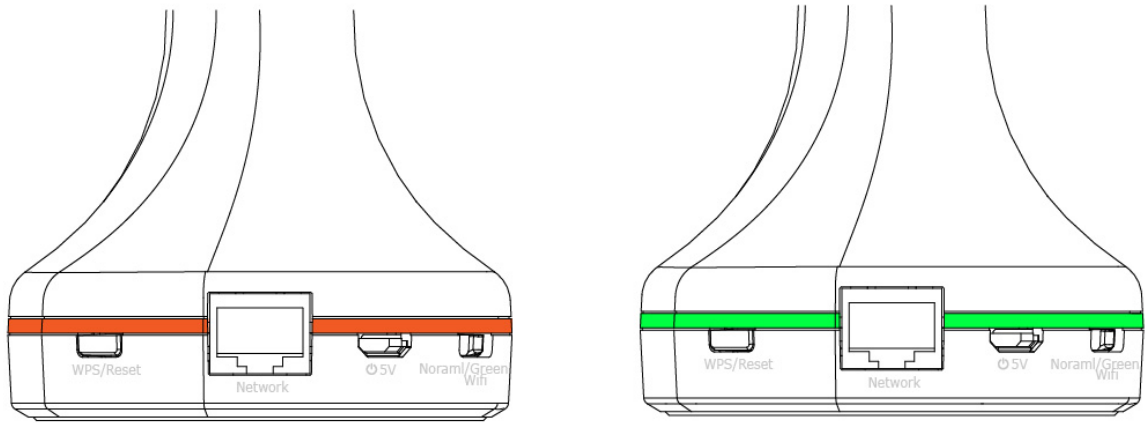


***Power Adapter***



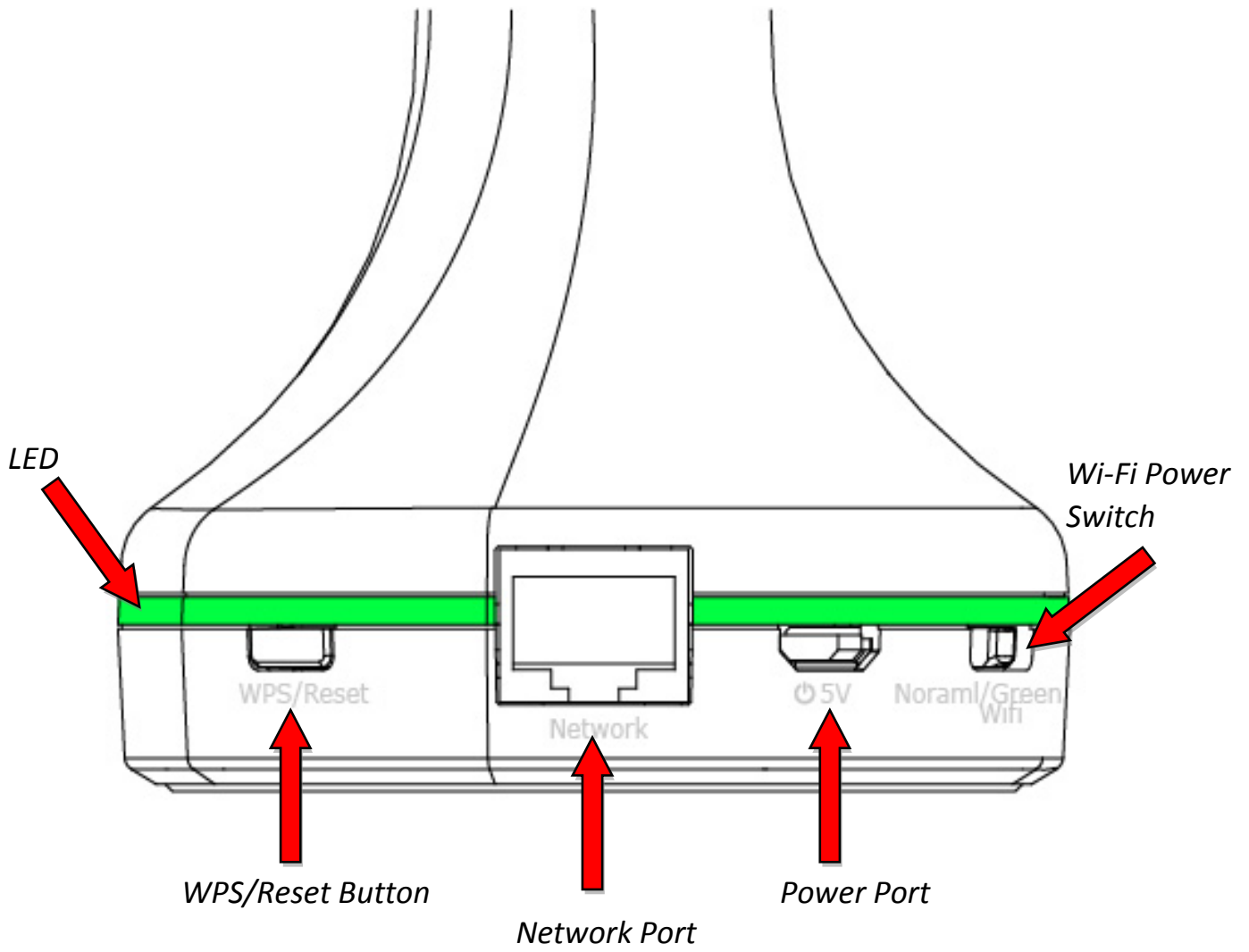
***USB Cable***

## I-2. LED Status



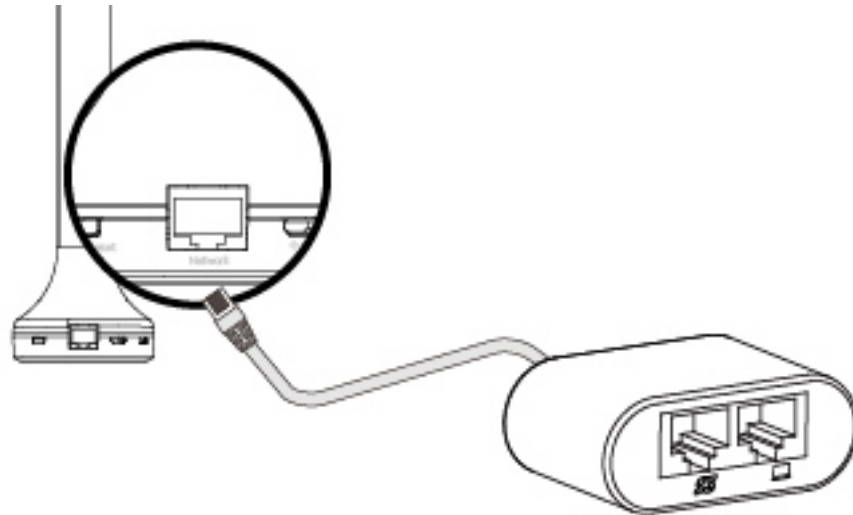
LED Color	LED Status	Description
<b>Orange/Red</b>	On	Product is starting up.
	Flashing (Slow)	No Internet connection.
	Flashing (Fast)	Resetting to factory default status or Wi-Fi Protected Setup (WPS) is active.
<b>Light Green</b>	On	Internet is connected and Wi-Fi is full power.
<b>Dark Green</b>	On	Internet is connected and Wi-Fi is in green mode (25% power).
<b>Off</b>	Off	BR-6288ACL is off.

### I-3. Back Panel



## I-4. RJ-45 Splitter Cable

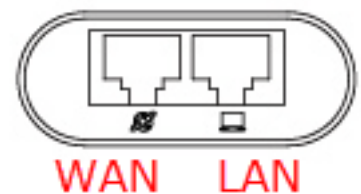
The BR-6288ACL includes an RJ-45 splitter cable in the package contents. This plugs into the “Network” port of the BR-6288ACL and splits the port into two separate Ethernet ports – providing two ports instead of one, as shown below.



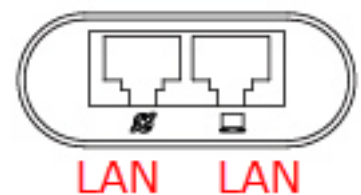
In **Wi-Fi router** mode, one port is the **WAN** (Network) port. The **WAN** port connects directly to your modem.



In **Wi-Fi router** mode, the other port is the **LAN** port. The **LAN** port is for wired connections to other network devices (e.g. computer).



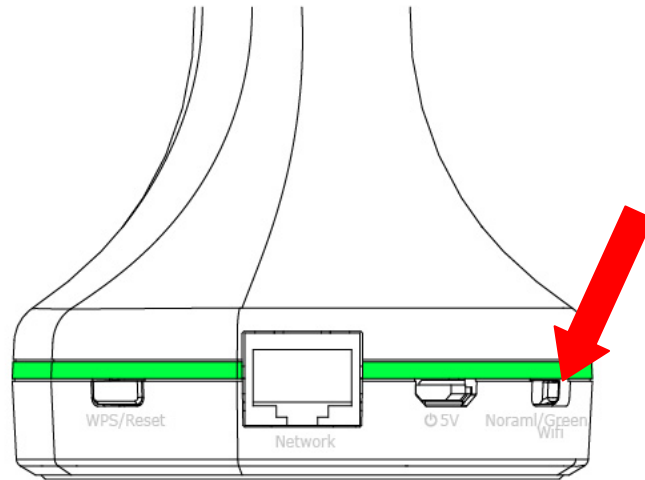
In **other** modes, both ports function as LAN ports for wired network devices (e.g. computers, games consoles etc.), and in **access point** mode also for connecting to your router.





## I-5. Wi-Fi Power Switch

After setup you can use the Wi-Fi power switch to adjust the strength of the BR-6288ACL's wireless radio if you wish. Normal mode uses full 100% wireless power while green mode uses 25% wireless power.




## **I-6. Safety Information**

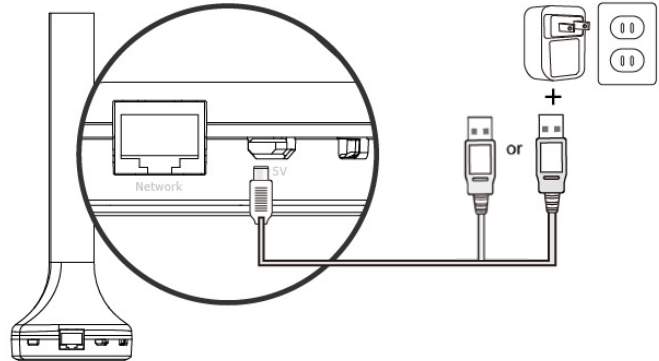
In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

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-6288ACL.
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.

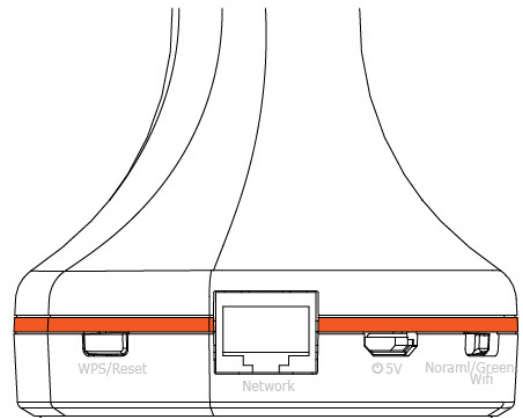
## II. Installation

1. Plug in the BR-6288ACL using the included power adapter and/or USB cable.

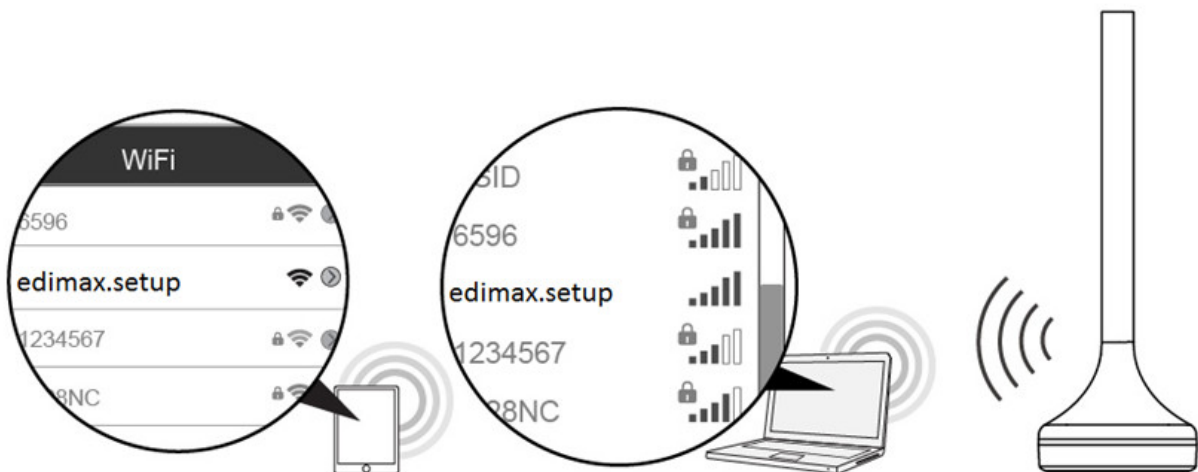
 **The BR-6288ACL requires 1 A of current – please ensure that your USB port can provide sufficient power. If not, use the 5V DC adapter.**



2. Wait until the circular LED at the base of the product is flashing "Orange/Red".




3. Use a Wi-Fi device (e.g. computer, tablet, smartphone) to search for a Wi-Fi network with the SSID "edimax.setup" and connect to it.

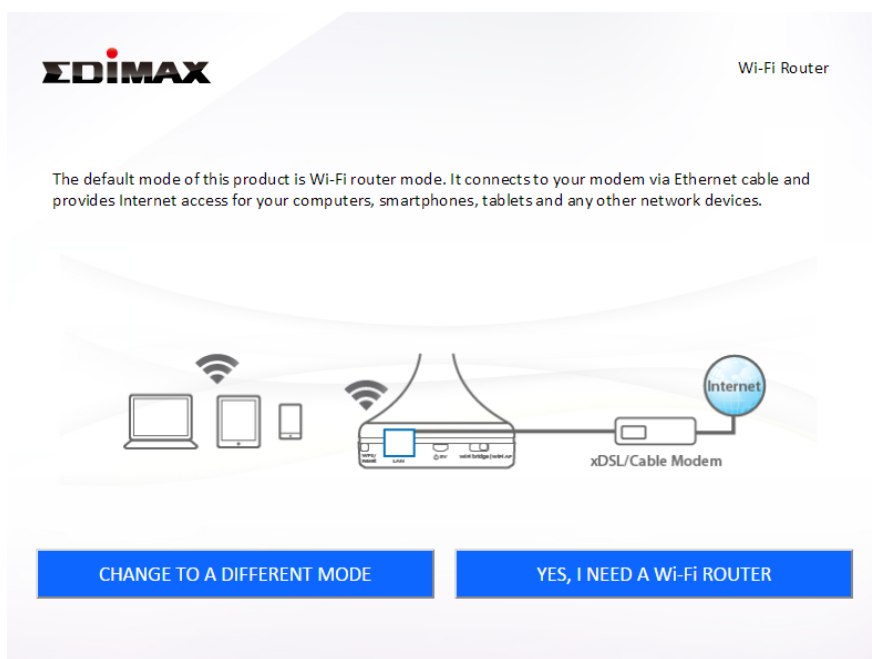


4. Open a web browser and if you do not automatically arrive at the “Get Started” screen shown below, enter the URL ***http://edimax.setup*** and click “Get Started” to begin.



 ***If you cannot access <http://edimax.setup>, please make sure your Wi-Fi device is set to use a dynamic IP address. This is a simple procedure and step-by-step instructions to do this on a computer can be found in the user manual.***

5. Choose if you want to use your BR-6288ACL in its default Wi-Fi router mode or in a different mode.



The BR-6288ACL's five available modes are outlined below:

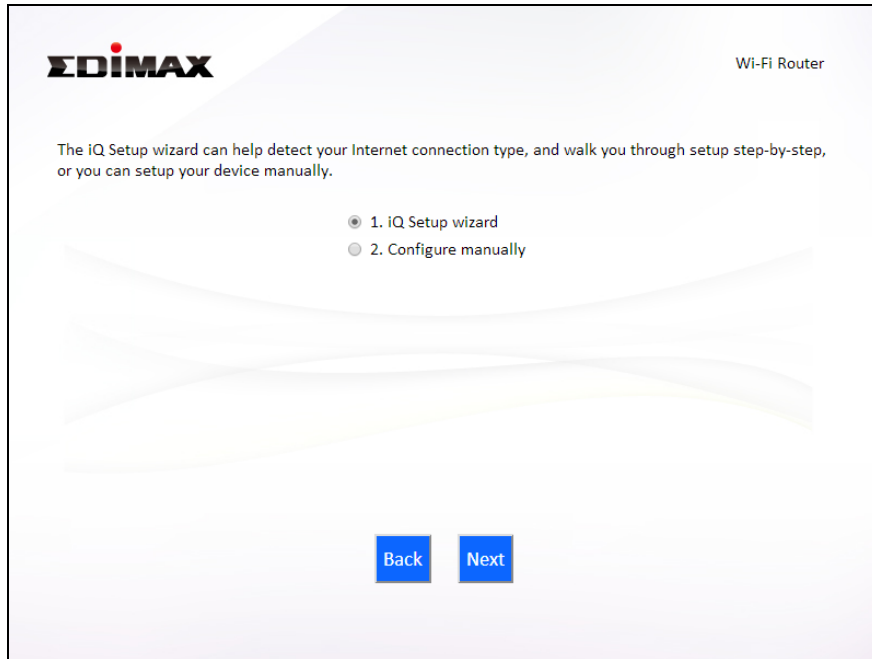
<b>Wi-Fi Router Mode</b>	<i>The device connects to your <b>modem</b> and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.</i>
<b>Access Point Mode</b>	<i>The device connects to an existing <b>router</b> via Ethernet cable and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.</i>
<b>Range Extender Mode</b>	<i>The device connects wirelessly to your existing 2.4GHz and/or 5GHz network and repeats the wireless signal(s).</i>
<b>Wireless Bridge Mode</b>	<i>The device connects to a network device for example: TV, gaming console, or media player via Ethernet cable and acts as a wireless receiver, allowing the network device to join your Wi-Fi network.</i>
<b>WISP Mode</b>	<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>

## II-1. Wi-Fi Router Mode

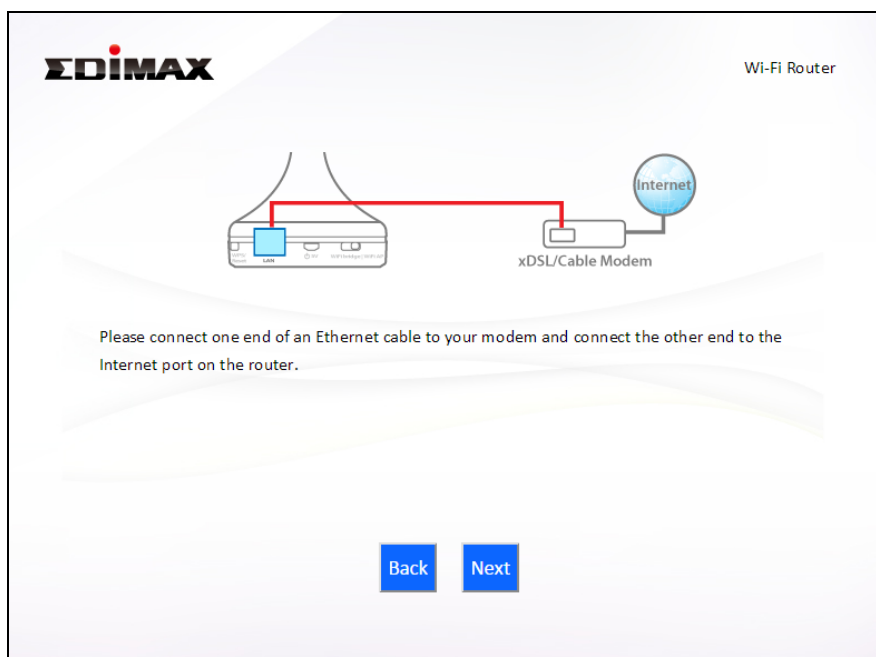
1. Select whether to use the iQ Setup wizard (recommended) to detect your Internet connection type, or enter the settings manually.



**Manual configuration is only recommended for advanced users.**



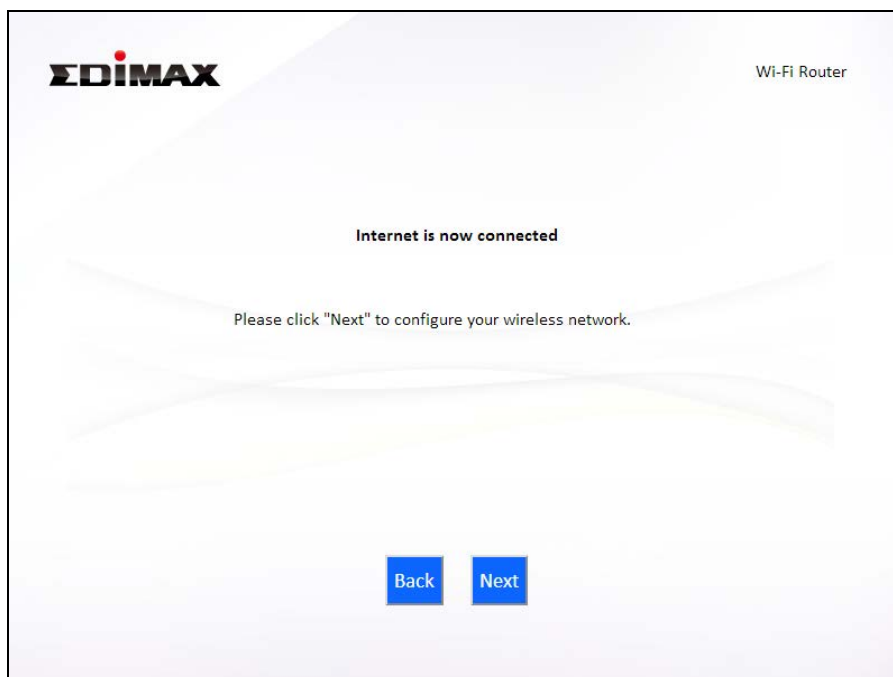
2. Connect the **blue** Internet port of your BR-6288ACL to the LAN port of your modem using an Ethernet cable, and then click “Next”.



**3.** Please wait a moment while the BR-6288ACL tests the connection.



**4.** Click “Next” to continue and configure the device’s wireless network.



**5.** Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.

**EDIMAX** Wi-Fi Router

Please set your Wi-Fi network name (SSID) and Wi-Fi password.

Wi-Fi network name (2.4GHz):

Wi-Fi password (WPA2-AES):   
(at least 8 characters)

Wi-Fi network name (5GHz):

Wi-Fi password (WPA2-AES):   
(at least 8 characters)

- 6.** A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.

**EDIMAX** Wi-Fi Router

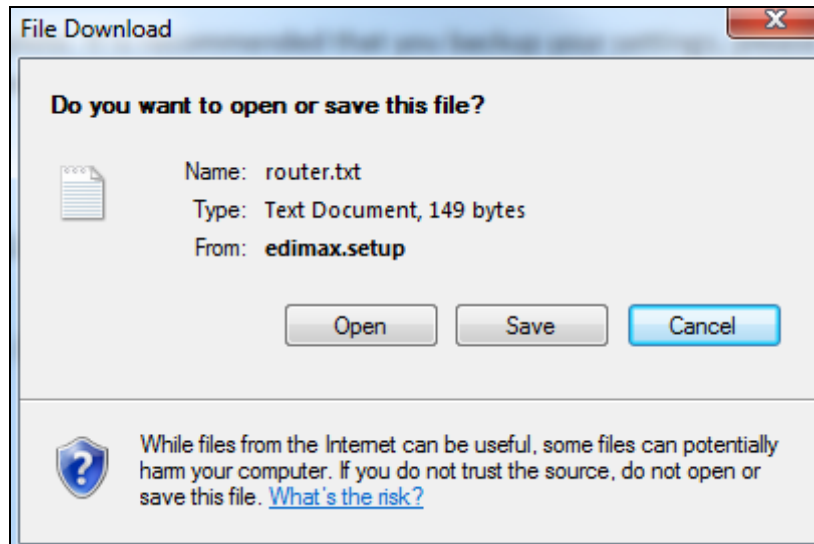
Configuration is complete. It is recommended that you backup your settings, please click "Backup this configuration" to do so. Then click "Next" when you are ready to continue.

Internet Type :	Dynamic IP
(2.4 GHz) Wi-Fi network name :	edimax_2.4G_8881D1
Wi-Fi password :	12345678
(5 GHz) Wi-Fi network name :	edimax_5G_8881B1
Wi-Fi password :	12345678

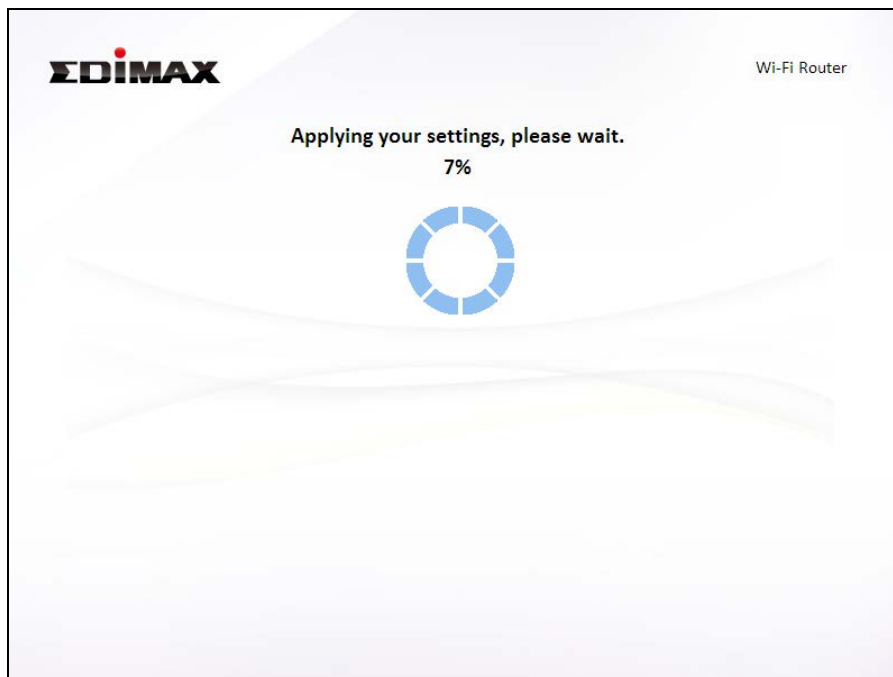


***If you wish to backup the device’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.***

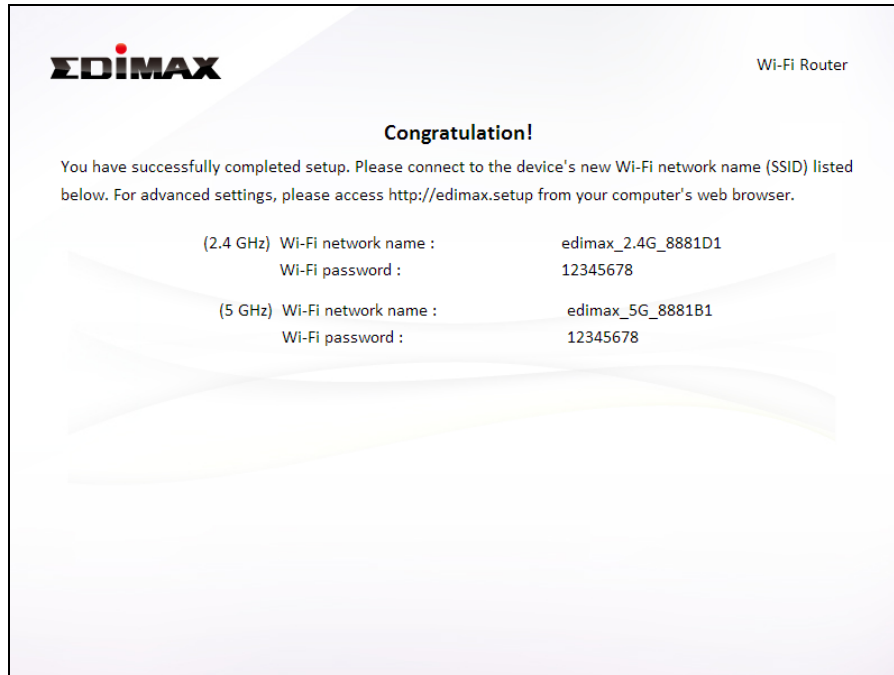




**7.** Please wait while the BR-6288ACL applies your settings.



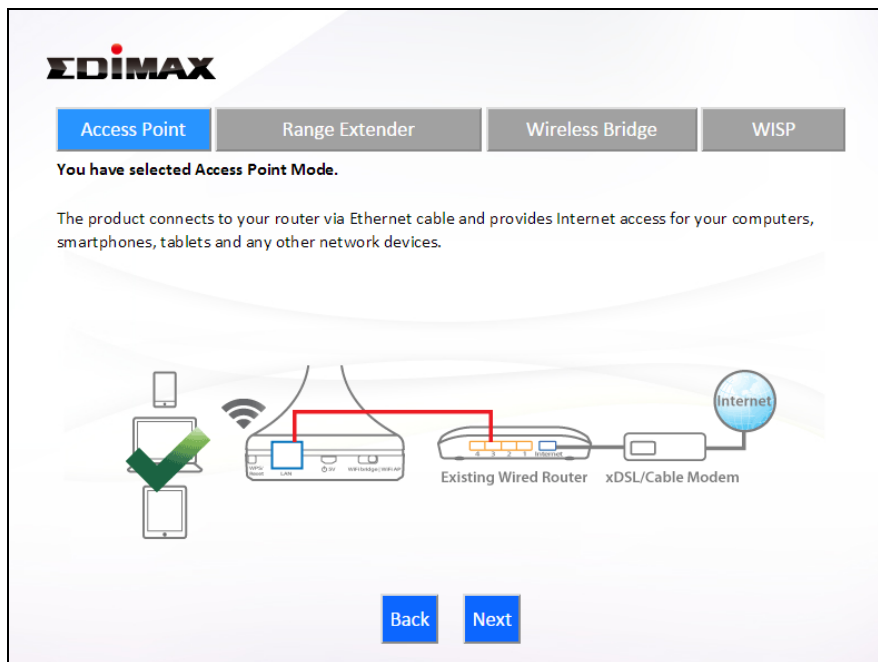
**8.** A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.



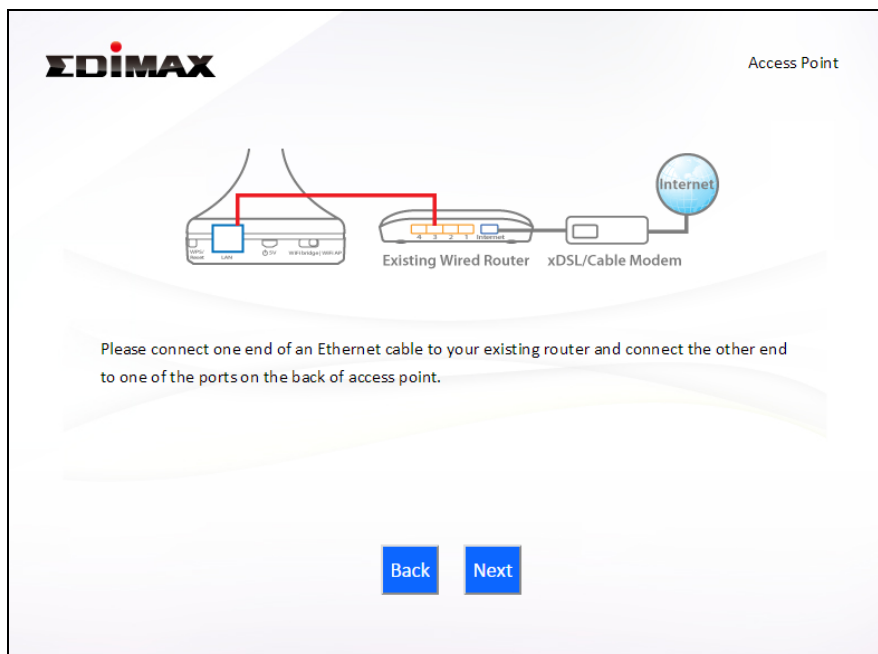
9. The BR-6288ACL is working and ready for use. Refer to [IV-2. Connecting to a Wi-Fi network](#) if you require more guidance.

## II-2. Access Point Mode

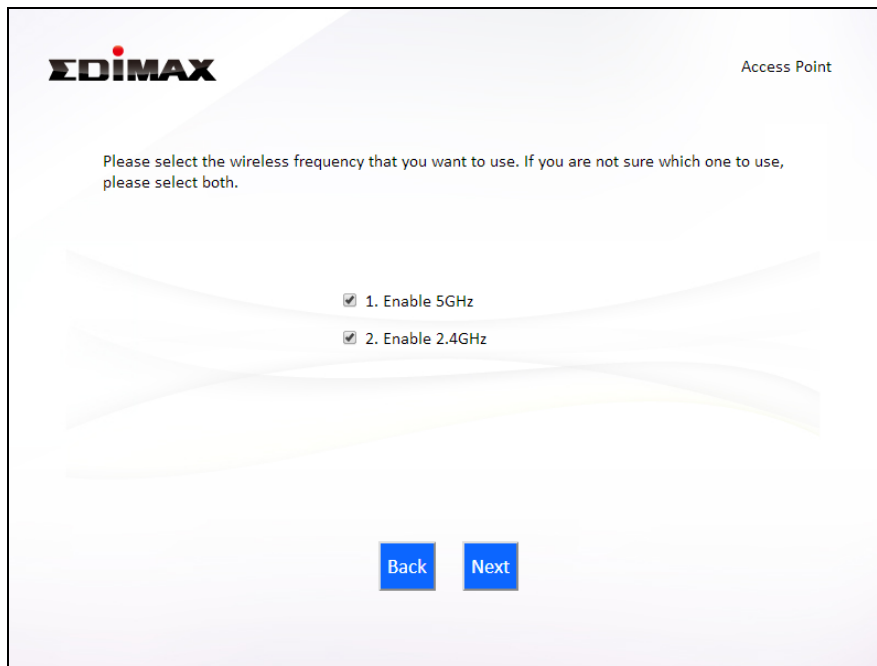
1. Select “Access Point” from the top menu and click “Next”.



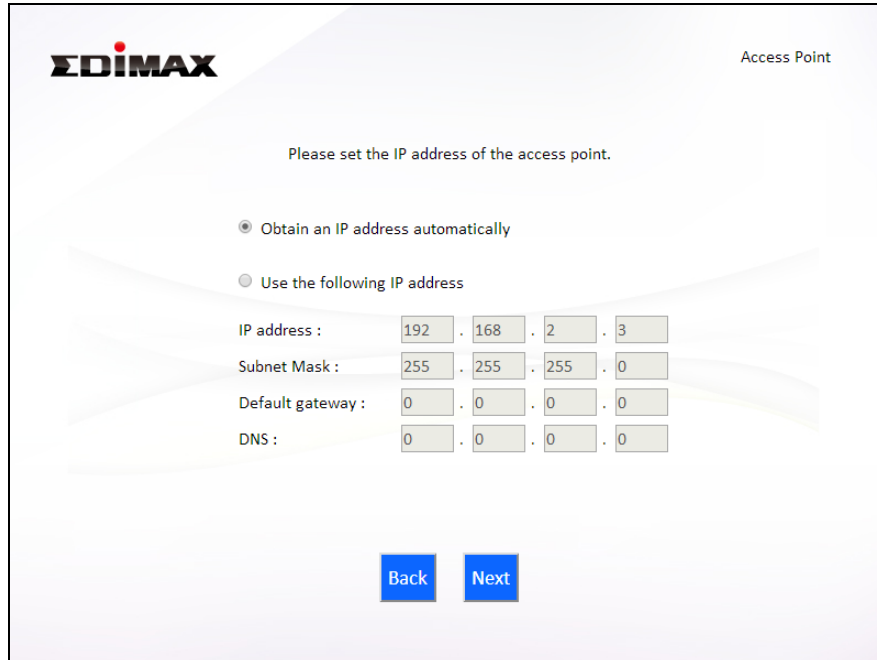
2. Connect the network port of your BR-6288ACL to the LAN port of your existing router using an Ethernet cable, then click “Next”.



3. Select whether to use the 5GHz wireless frequency, 2.4GHz wireless frequency or both. If you are not sure, select both.

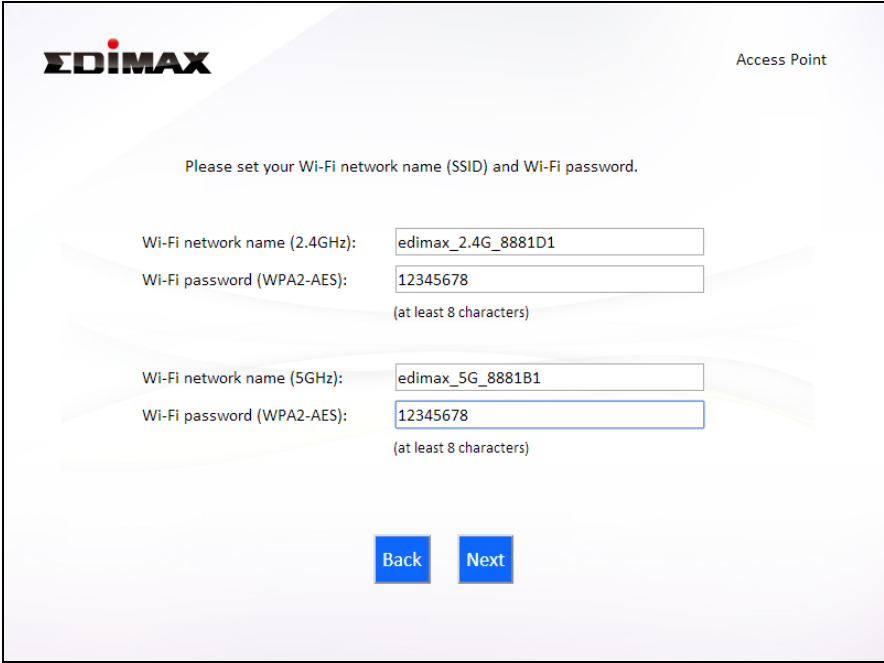


4. Select “Obtain an IP address automatically” or “Use the following IP address” for your BR-6288ACL. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.



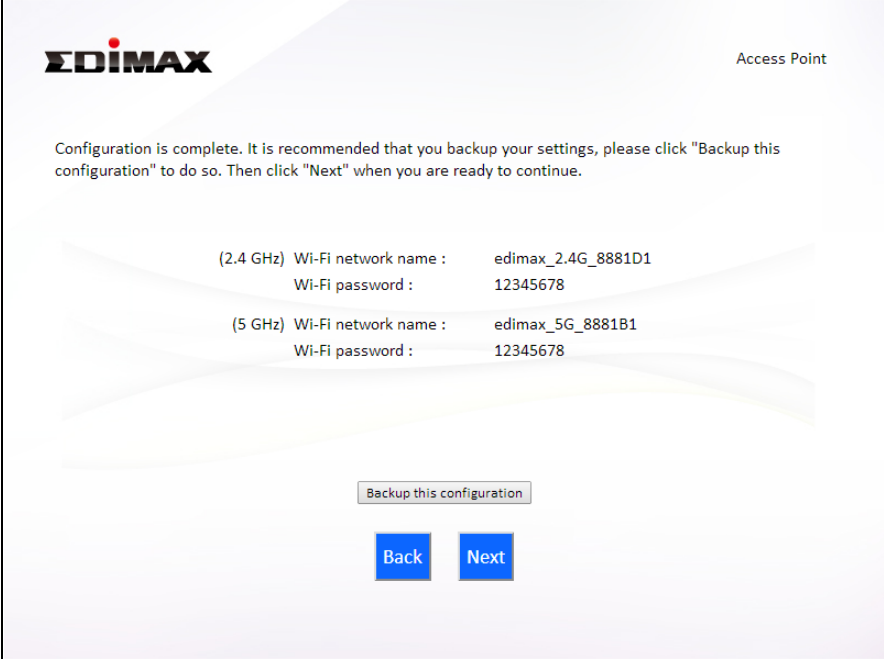
***“Obtain an IP address automatically” is the recommended setting for most users. For more guidance on static IP addresses, please refer to [IV-1. Configuring your IP address.](#)***

5. Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.



The screenshot shows the EDIMAX Access Point configuration interface. At the top left is the EDIMAX logo, and at the top right is the text "Access Point". Below the logo, a message reads: "Please set your Wi-Fi network name (SSID) and Wi-Fi password." There are two sets of input fields. The first set is for the 2.4GHz network, with the SSID field containing "edimax\_2.4G\_8881D1" and the WPA2-AES password field containing "12345678" (with a note "(at least 8 characters)"). The second set is for the 5GHz network, with the SSID field containing "edimax\_5G\_8881B1" and the WPA2-AES password field containing "12345678" (with a note "(at least 8 characters)"). At the bottom, there are two blue buttons: "Back" and "Next".

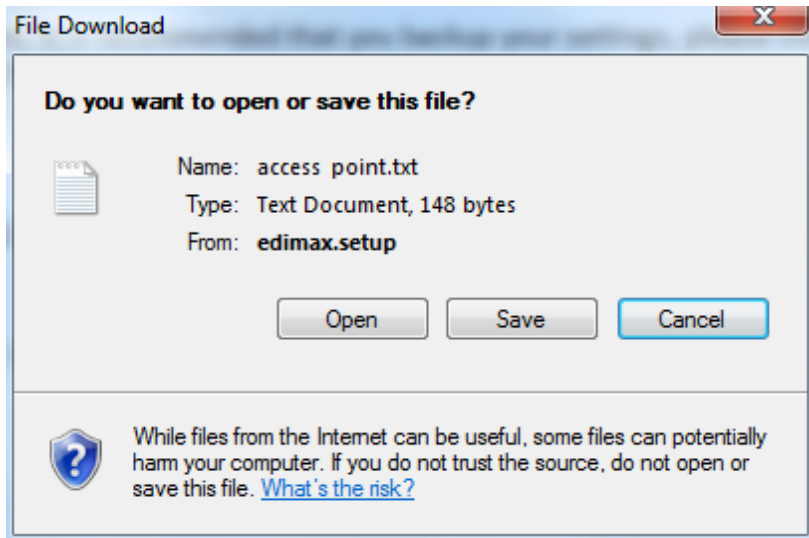
6. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



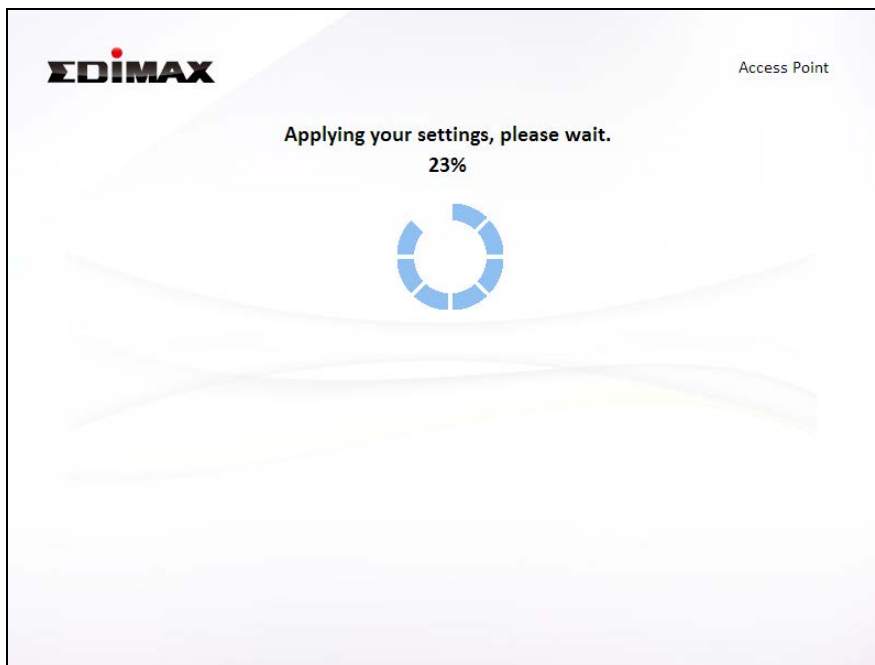
The screenshot shows the EDIMAX Access Point configuration interface displaying a summary of the configuration. At the top left is the EDIMAX logo, and at the top right is the text "Access Point". Below the logo, a message reads: "Configuration is complete. It is recommended that you backup your settings, please click "Backup this configuration" to do so. Then click "Next" when you are ready to continue." The summary lists the following details: (2.4 GHz) Wi-Fi network name : edimax\_2.4G\_8881D1, Wi-Fi password : 12345678; (5 GHz) Wi-Fi network name : edimax\_5G\_8881B1, Wi-Fi password : 12345678. Below the summary, there is a button labeled "Backup this configuration" and two blue buttons: "Back" and "Next".



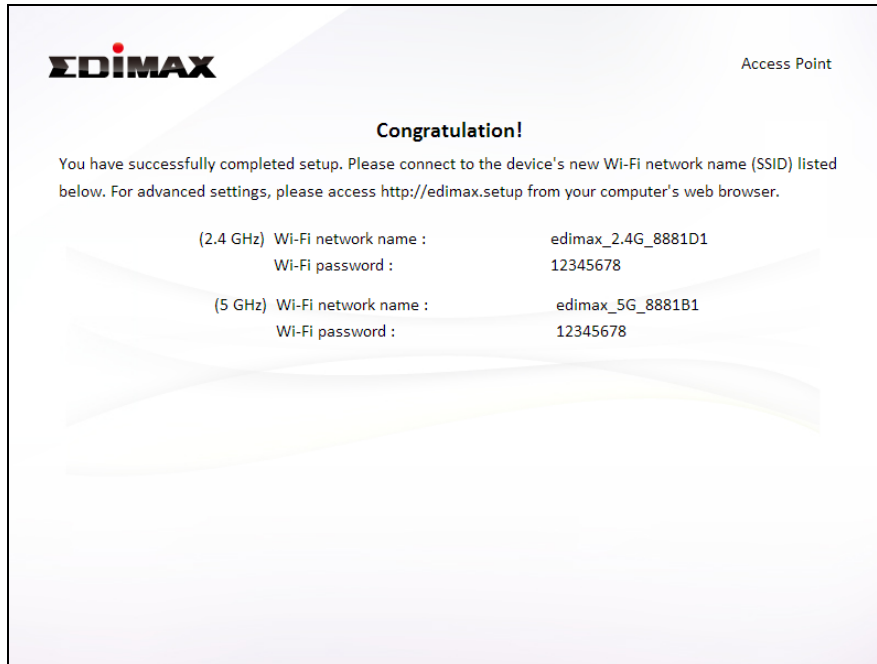
***If you wish to backup the device’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.***



**7.** Please wait a moment until the BR-6288ACL is ready.



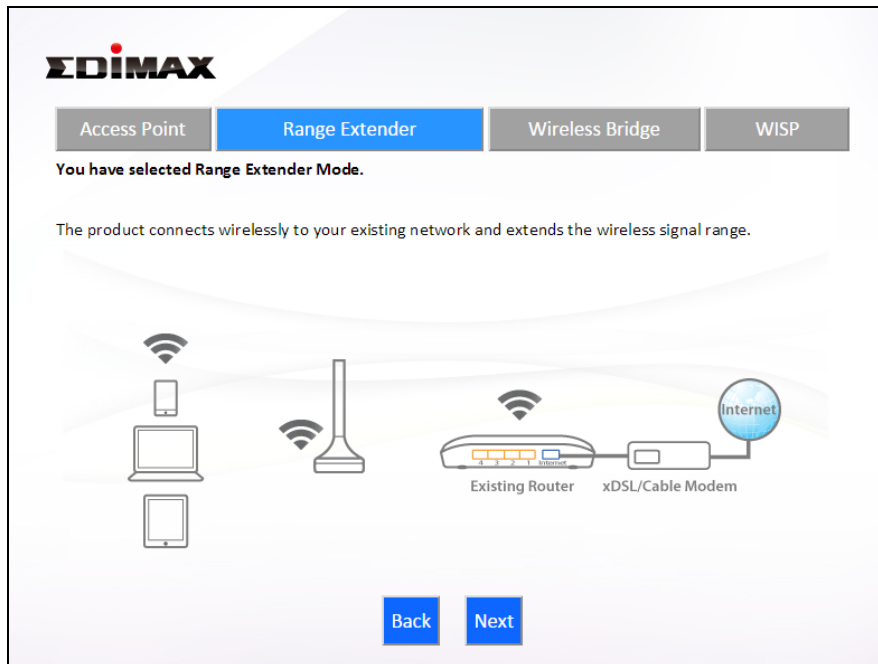
**8.** A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.



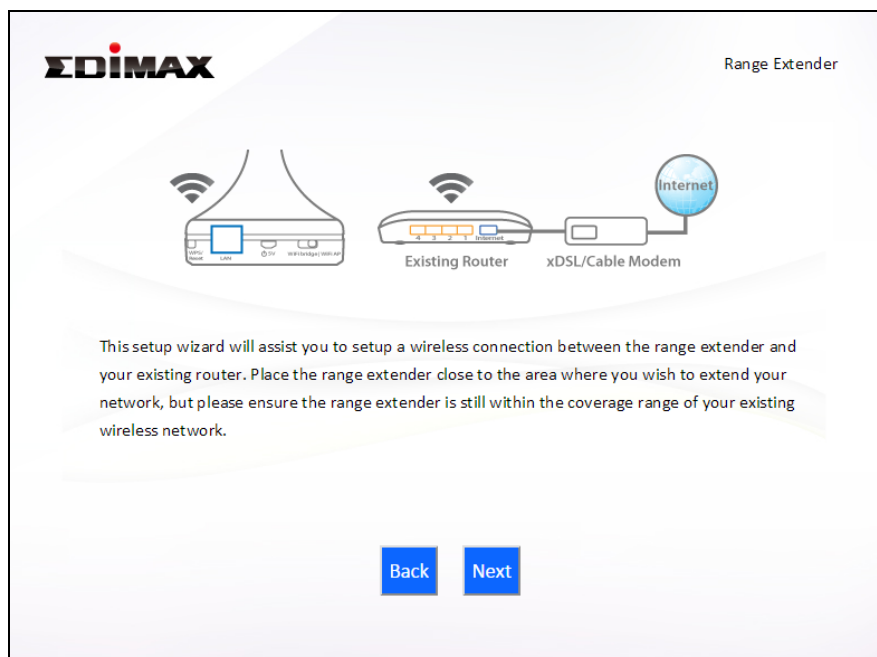
9. The BR-6288ACL is working and ready for use. Refer to [IV-2. Connecting to a Wi-Fi network](#) if you require more guidance.

## II-3. Range Extender Mode

1. Select “Range Extender” from the top menu and click “Next”.

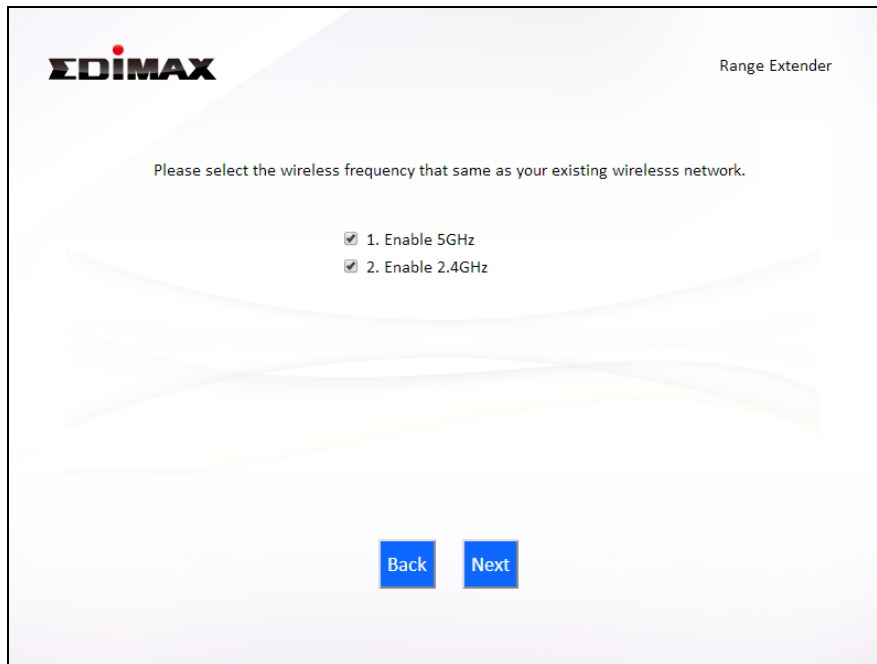


2. Please ensure your BR-6288ACL is within Wi-Fi range of your existing wireless router. Click “Next” to continue.





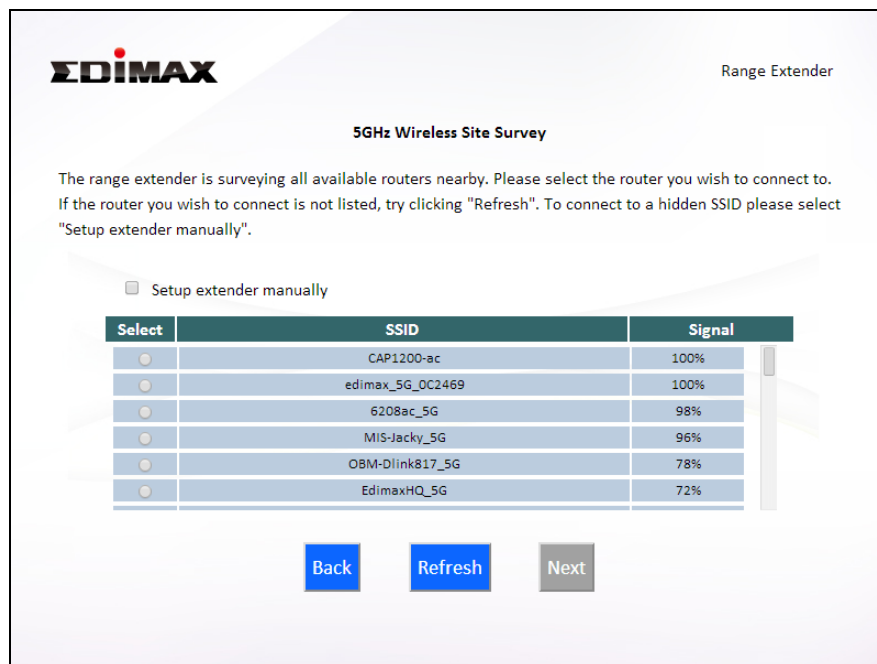
3. Select whether to use the 5GHz wireless frequency, 2.4GHz wireless frequency or both. If you are not sure, select both and then click “Next”.



The screenshot shows the EDIMAX Range Extender configuration interface. At the top left is the EDIMAX logo, and at the top right is the text "Range Extender". Below the logo, there is a heading "Please select the wireless frequency that same as your existing wireless network." followed by two checked radio button options: "1. Enable 5GHz" and "2. Enable 2.4GHz". At the bottom of the page, there are two blue buttons labeled "Back" and "Next".


4. Select the Wi-Fi network name (SSID) which you wish to connect to for the specified frequency and click “Next” to continue.

 ***If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.***



The screenshot shows the EDIMAX Range Extender configuration interface for a 5GHz Wireless Site Survey. At the top left is the EDIMAX logo, and at the top right is the text "Range Extender". Below the logo, there is a heading "5GHz Wireless Site Survey" and a paragraph: "The range extender is surveying all available routers nearby. Please select the router you wish to connect to. If the router you wish to connect is not listed, try clicking "Refresh". To connect to a hidden SSID please select "Setup extender manually"." Below this text is a checkbox labeled "Setup extender manually". Below the checkbox is a table with three columns: "Select", "SSID", and "Signal". The table contains six rows of data. At the bottom of the page, there are three buttons: "Back", "Refresh", and "Next".

Select	SSID	Signal
<input type="radio"/>	CAP1200-ac	100%
<input type="radio"/>	edimax_5G_OC2469	100%
<input type="radio"/>	6208ac_5G	98%
<input type="radio"/>	MIS-Jacky_5G	96%
<input type="radio"/>	OBM-Dlink817_5G	78%
<input type="radio"/>	EdimaxHQ_5G	72%

 ***To connect to a hidden SSID, check the “Setup extender manually” box and enter the details manually on the next page, as shown below.***

**EDIMAX** Range Extender

### 5GHz Wireless Site Survey

Please set a new Wi-Fi network name (SSID) for the range extender if you wish, and set the security key for your existing wireless network if required.

Wi-Fi network name (SSID):

Range extender SSID:

Encryption:

Security Type:  TKIP  AES

Key Format:

Wi-Fi password (Security Key):

5. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.

**EDIMAX** Range Extender

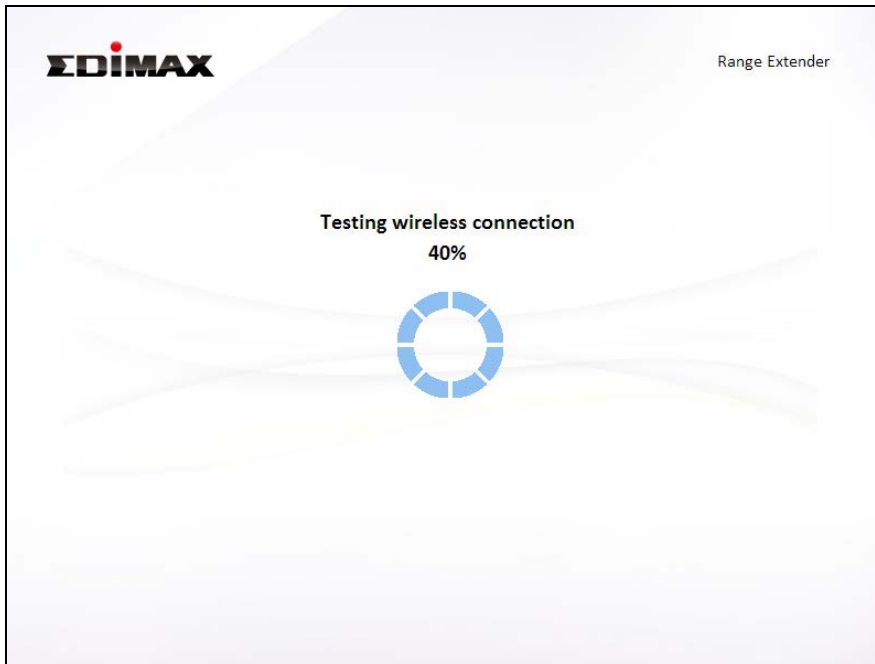
### 5GHz Wireless Site Survey

Please set a new Wi-Fi network name (SSID) for the range extender if you wish, and set the security key for your existing wireless network if required.


Device SSID:

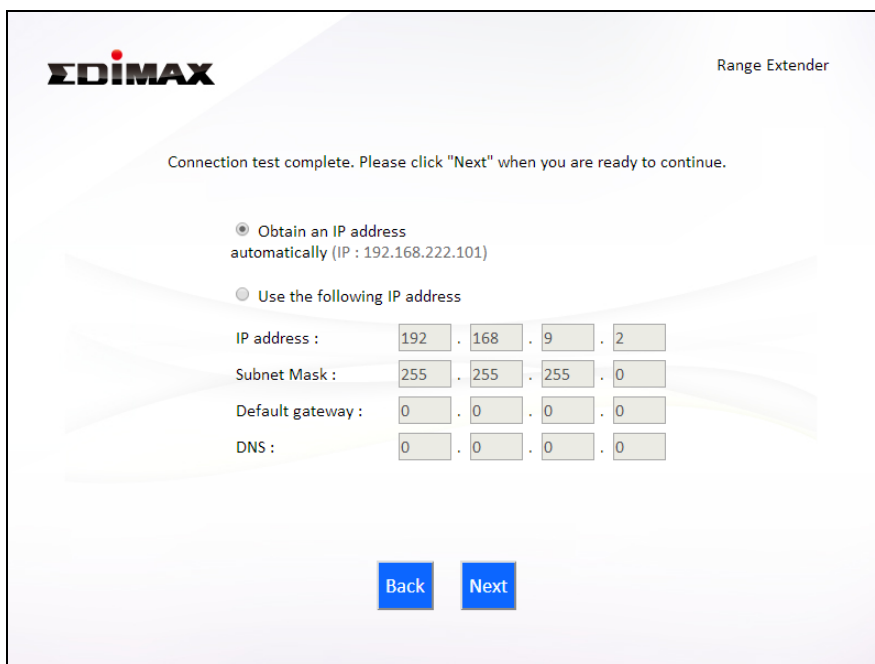
Security Key:

6. Wait a moment while the BR-6288ACL tests the wireless connection.



7. Select “Obtain an IP address automatically” or “Use the following IP address” for your BR-6288ACL. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

 ***“Obtain an IP address automatically” is the recommended setting for most users. The IP address will be displayed in brackets.***



8. If you selected to use both 2.4GHz and 5GHz wireless frequencies in step 3, then repeat **steps 4 – 7** for the 2.4GHz wireless frequency.

EDIMAX Range Extender

### 2.4GHz Wireless Site Survey

The range extender is surveying all available routers nearby. Please select the router you wish to connect to. If the router you wish to connect is not listed, try clicking "Refresh". To connect to a hidden SSID please select "Setup extender manually".

Setup extender manually

Select	SSID	Signal
<input type="radio"/>	EDIMAX_2.4G	100%
<input type="radio"/>	CAP300-0B0492	100%
<input type="radio"/>	MIS-Jacky	100%
<input type="radio"/>	OBM-Dlink817_2.4G_2EX	100%
<input type="radio"/>	Free Wi-Fi	100%
<input type="radio"/>	PP-6476ND-2.4G	96%

Back Refresh Next

9. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



***The device will use the same wireless password/security key as the existing wireless network.***

EDIMAX Range Extender

Configuration is complete. It is recommended that you backup your settings, please click "Backup this configuration" to do so. Then click "Next" when you are ready to continue.

IP address : 192.168.222.102  
 (2.4 GHz) Wi-Fi network name : EDIMAX\_2.4G\_2EX  
 Wi-Fi password : 12345678

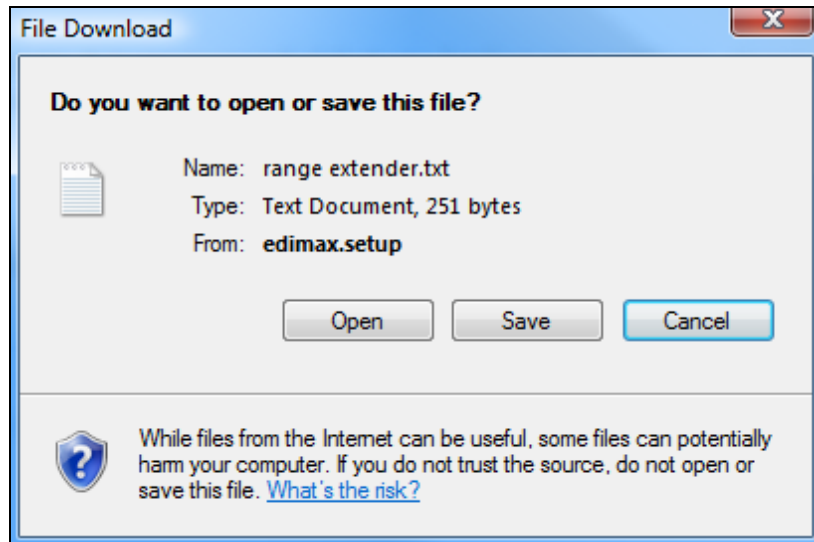
IP address : 192.168.222.101  
 (5 GHz) Wi-Fi network name : EDIMAX\_5G\_2EX  
 Wi-Fi password : 12345678

Backup this configuration

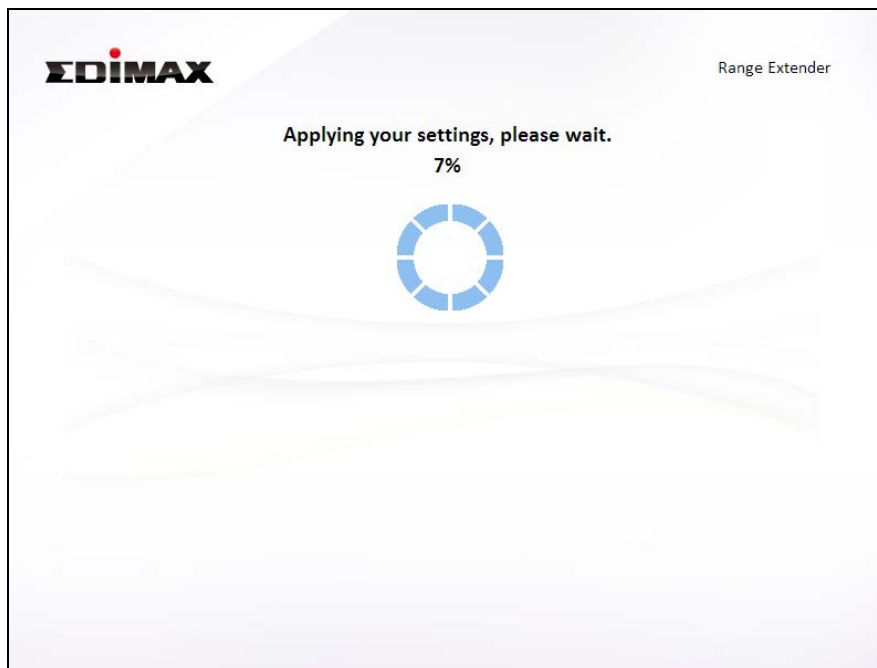
Back Next



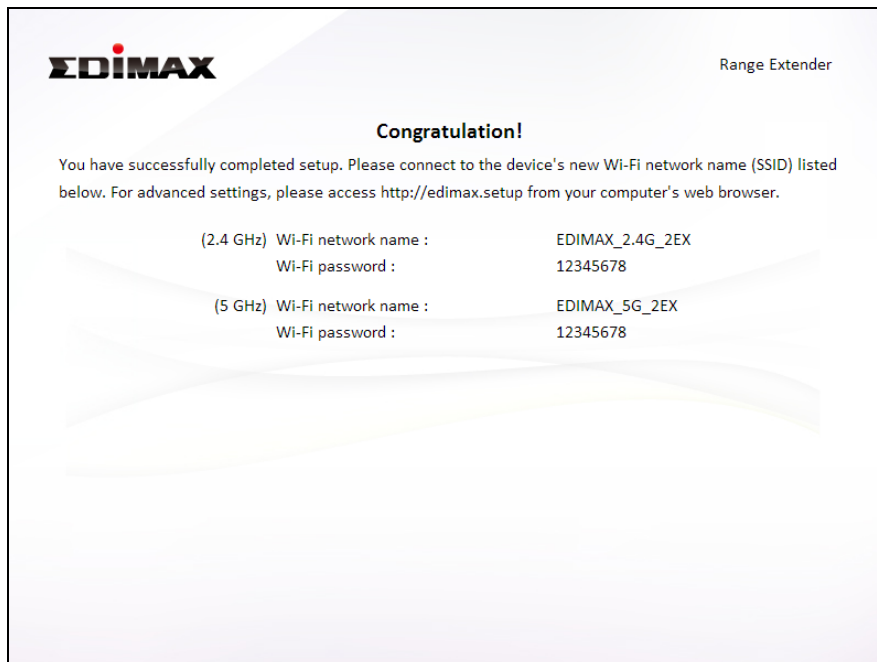
***If you wish to backup the BR-6288ACL’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.***



**10.** Please wait a moment until the BR-6288ACL is ready.



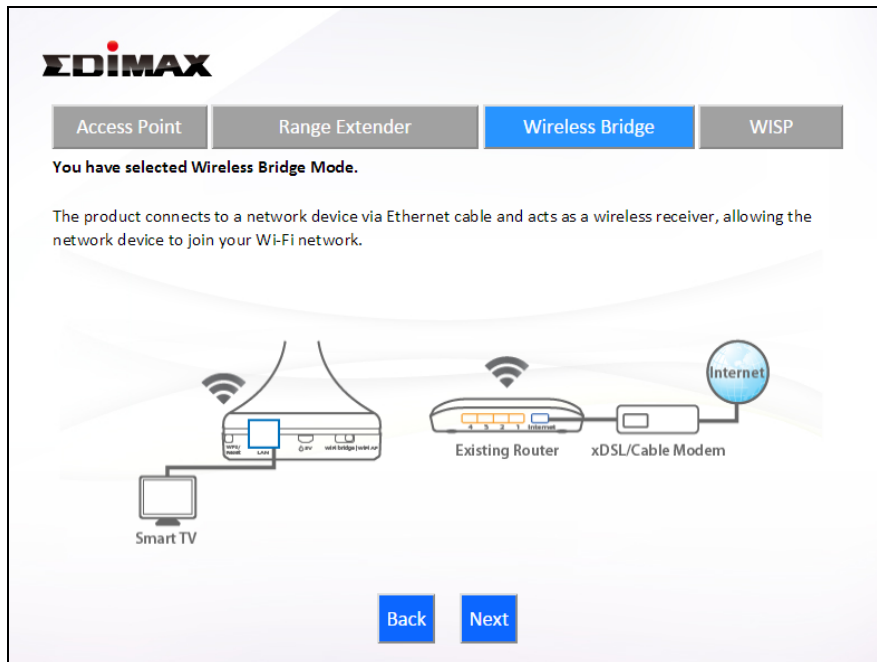
**11.** A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.



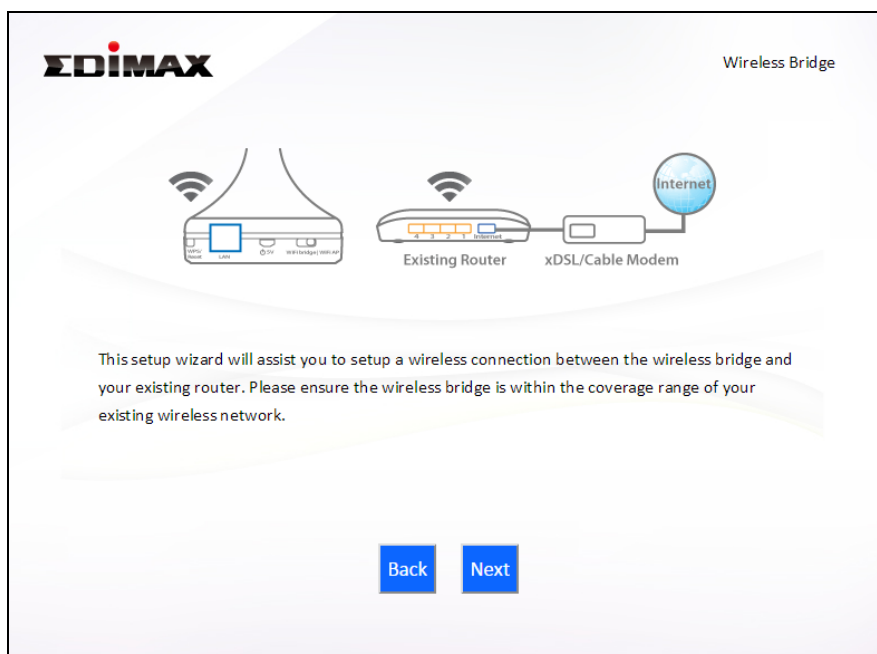
**12.** The BR-6288ACL is working and ready for use. Refer to [IV-2. Connecting to a Wi-Fi network](#) if you require more guidance.

## II-4. Wireless Bridge Mode

1. Select “Wireless Bridge” from the top menu and click “Next”.



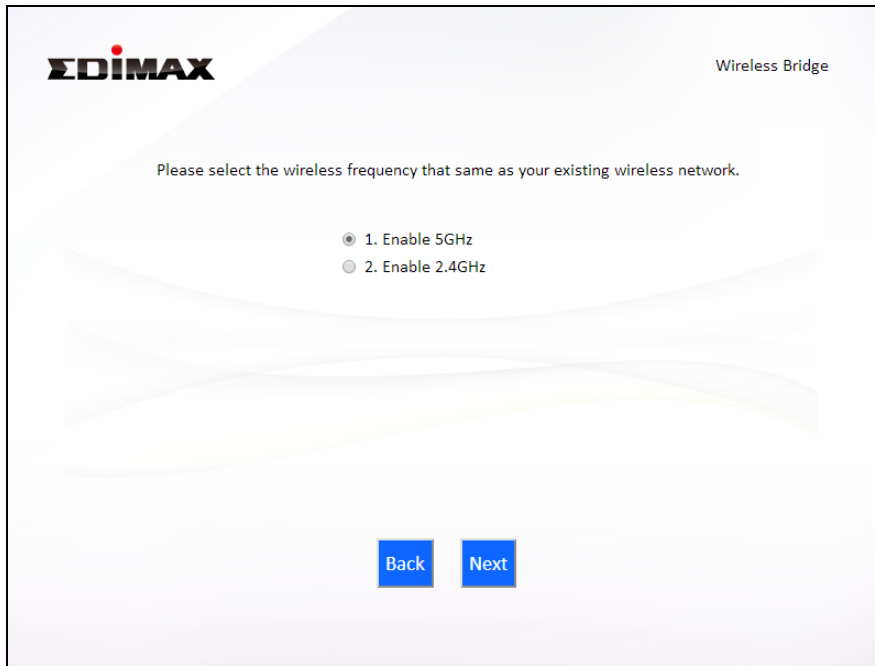
2. Please ensure your BR-6288ACL is within Wi-Fi range of your existing wireless router. Click “Next” to continue.



3. Select the frequency (2.4GHz or 5GHz) of your existing wireless network.



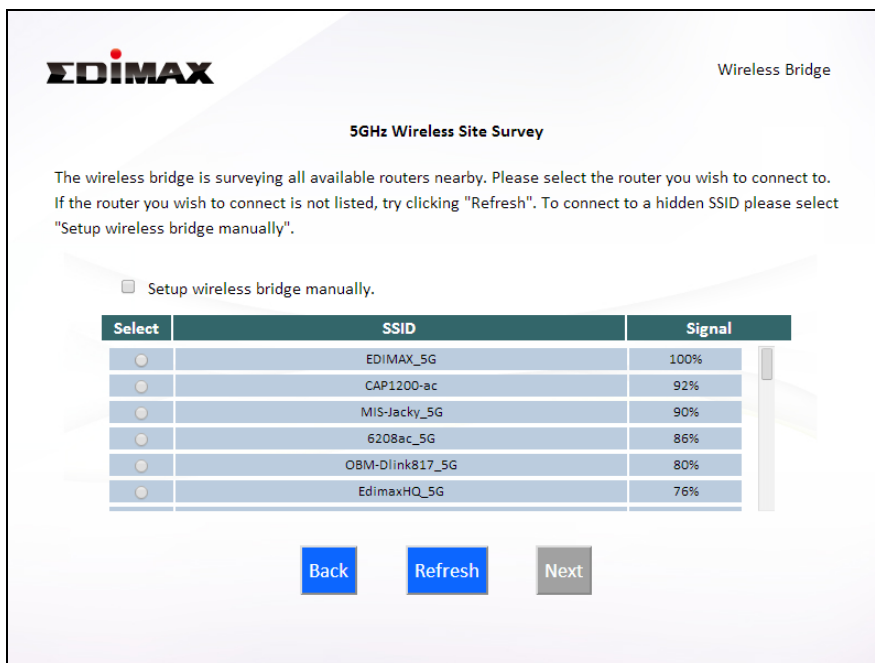
***In wireless client mode, the BR-6288ACL can only connect to one wireless network/frequency i.e. 2.4GHz or 5GHz.***



4. Select the Wi-Fi network name (SSID) which you wish to connect to and click “Next” to continue.



***If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.***



***To connect to a hidden SSID, check the “Setup extender manually” box and enter the details manually on the next page, as shown below.***



**EDIMAX** Wireless Bridge

**5GHz Wireless Site Survey**

Please enter your existing Wi-Fi network name (SSID) and security key if required.

Wi-Fi network name (SSID): EDIMAX\_5G

Encryption: WPA2

Security Type:  TKIP  AES

Key Format: Passphrase

Wi-Fi password (Security Key): 12345678

Back Next

5. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.

**EDIMAX** Wireless Bridge

**5GHz Wireless Site Survey**

Please enter your existing Wi-Fi network security key if required.

Device SSID: EDIMAX\_5G


Security Key: 12345678

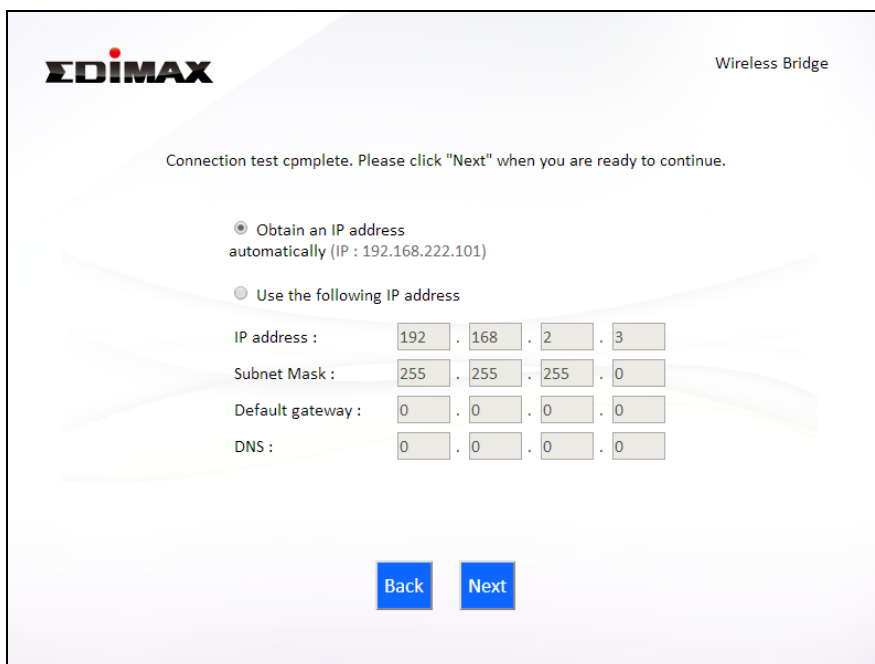
Back Next

6. Wait a moment while the BR-6288ACL tests the wireless connection.

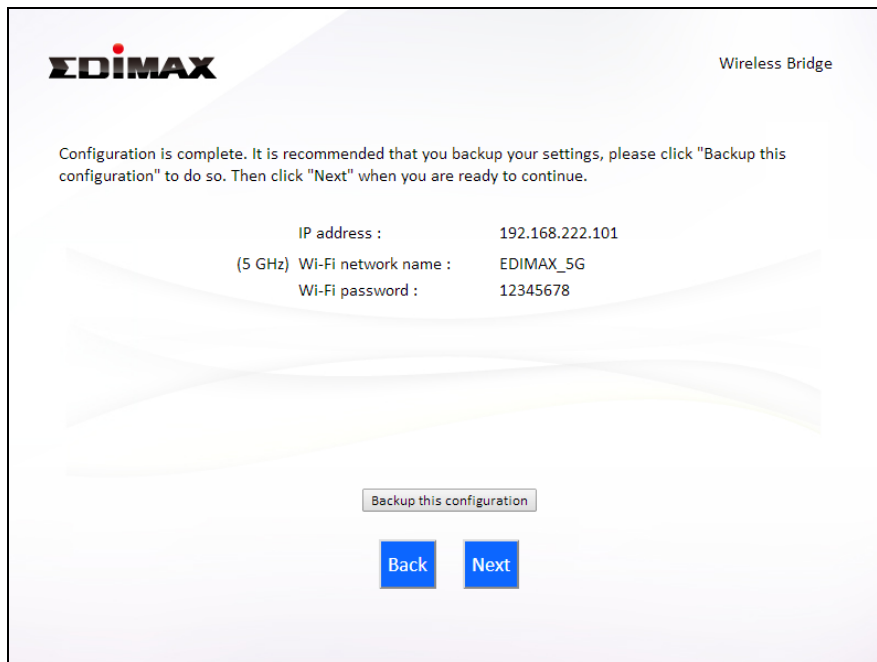



7. Select “Obtain an IP address automatically” or “Use the following IP address” for your BR-6288ACL. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

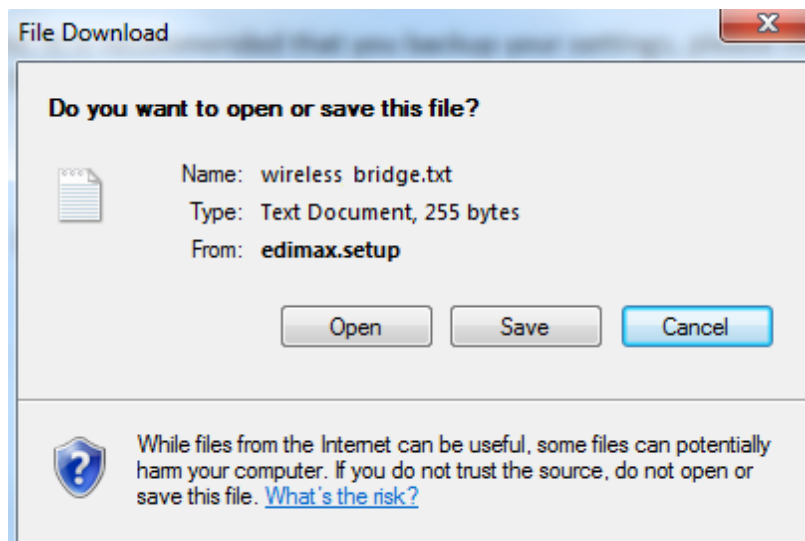
 **“Obtain an IP address automatically” is the recommended setting for most users. The IP address will be displayed in brackets.**



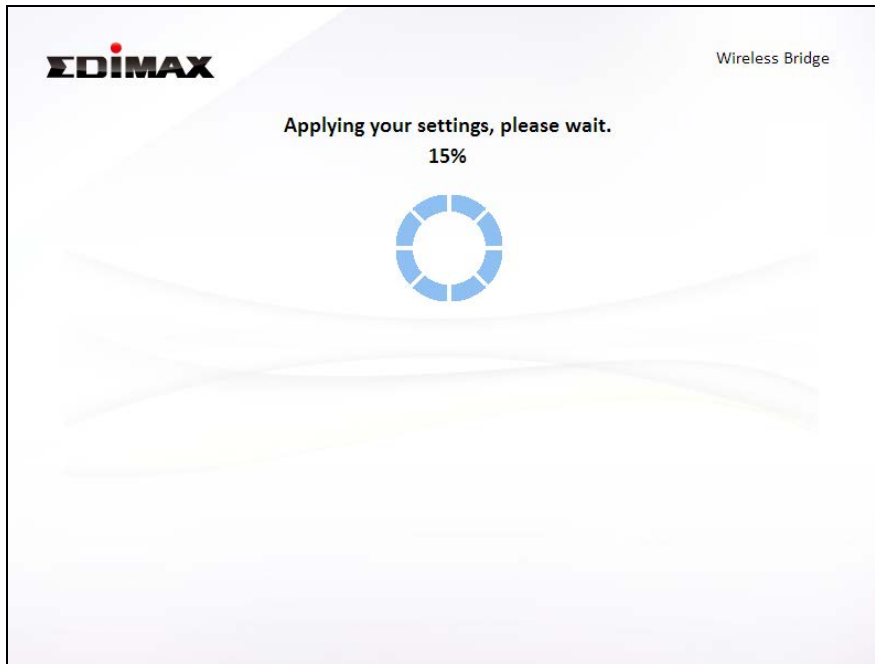
8. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



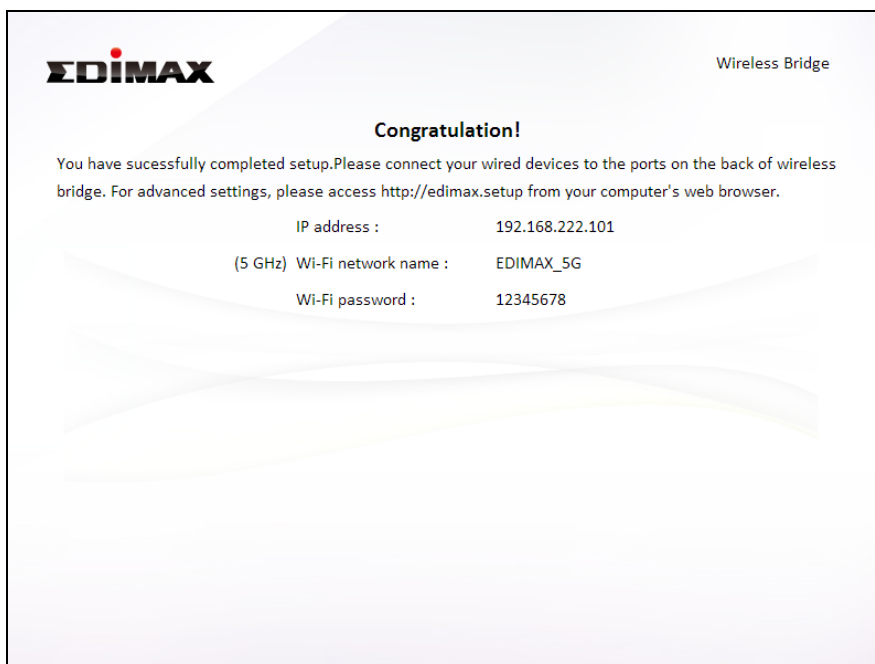
 ***If you wish to backup the BR-6288ACL's settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.***



**9.** Please wait a moment until the BR-6288ACL is ready.



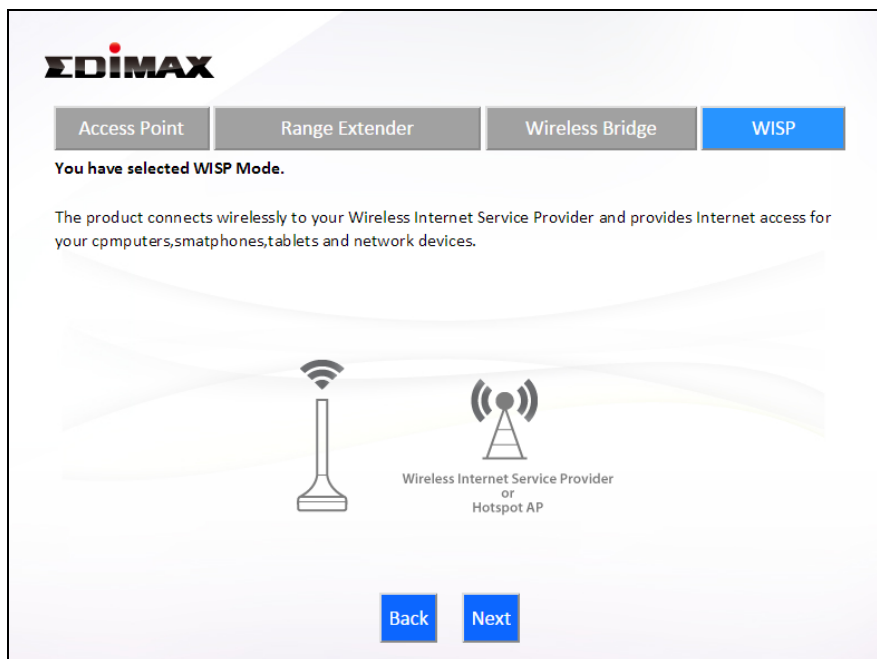
**10.** A final congratulations screen will indicate that setup is complete. Please close the browser window.



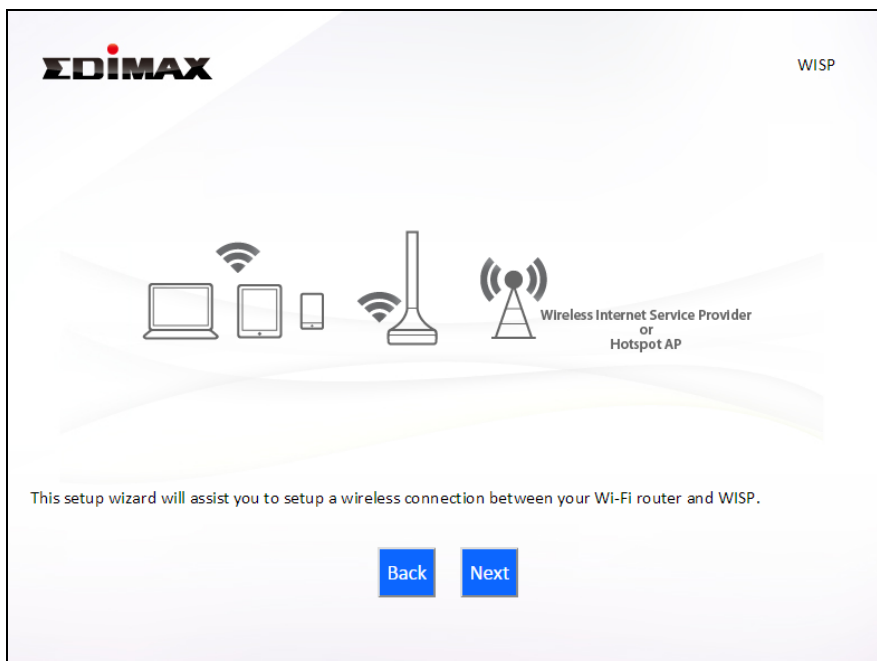
**11.** The BR-6288ACL is working and ready for use. You can now connect the BR-6288ACL to your network device using an Ethernet cable and connect to your network as usual.

## II-5. WISP Mode

1. Select “WISP” from the top menu and click “Next”.



2. Please ensure your BR-6288ACL is within Wi-Fi range of your WISP network and click “Next” to continue.



- 3.** Select whether to use the iQ Setup wizard (recommended) to detect your Internet connection type, or enter the settings manually.



***Manual configuration is only recommended for advanced users.***

**EDIMAX** WISP

The iQ Setup wizard can help detect your Internet connection type, and walk you through setup step-by-step, or you can setup your device manually.

- 1. iQ Setup wizard
- 2. Configure manually

Back Next

- 4.** Select the wireless frequency (2.4GHz or 5GHz) of your WISP network.

**EDIMAX** WISP

Please select the wireless frequency that same as your WISP used.

- 1. Enable 5GHz
- 2. Enable 2.4GHz

Back Next

5. Select the WISP SSID which you wish to connect to and click “Next” to continue.



***If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.***

**EDIMAX** WISP

**5GHz Wireless Site Survey**

The Wi-Fi router is surveying all available WISP nearby. Please select the WISP you wish to connect to. If the WISP you wish to connect is not listed, try clicking "Refresh". To connect to a hidden SSID please select "Setup WISP manually".

Setup WISP manually.

Select	SSID	Signal
<input type="radio"/>	EDIMAX_5G	100%
<input type="radio"/>	CAP1200-ac	92%
<input type="radio"/>	MIS-Jacky_5G	92%
<input type="radio"/>	6208ac_5G	88%
<input type="radio"/>	EdimaxHQ_5G	74%
<input type="radio"/>	OBM-Dlink817_5G	72%



***To connect to a hidden SSID, check the “Setup extender manually” box and enter the details manually on the next page, as shown below.***

**EDIMAX** WISP

**5GHz Wireless Site Survey**

Please enter your WISP's Wi-Fi network name and the security key provide from your WISP if required.

Wi-Fi network name (SSID):

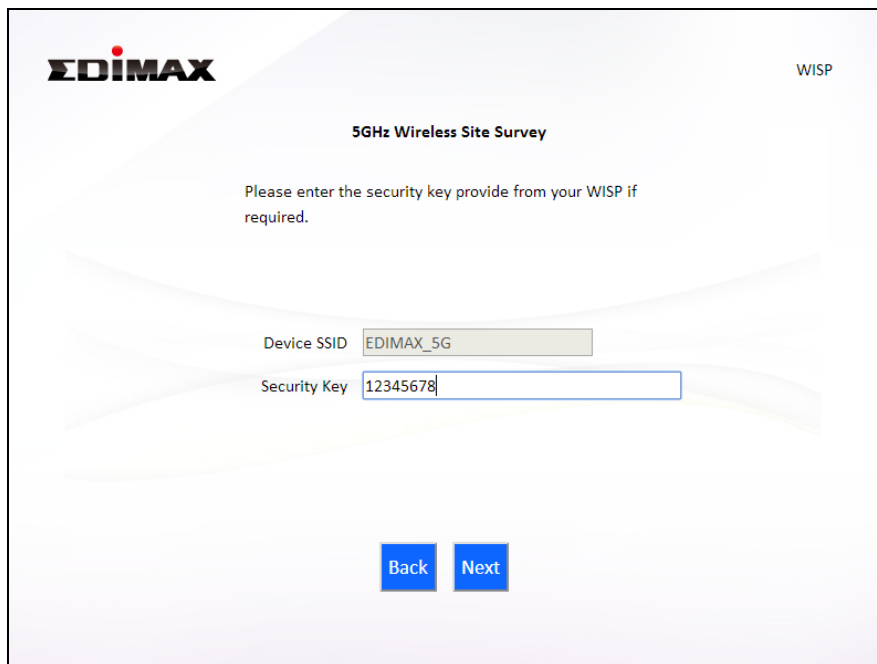
Encryption:

Security Type:  AES

Key Format:

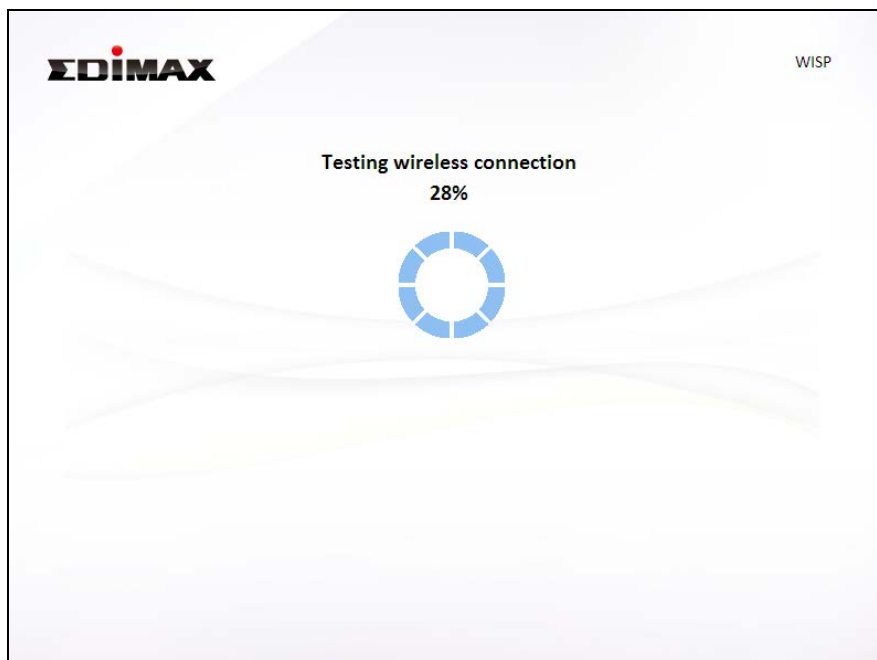
Wi-Fi password (Security Key):

6. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.



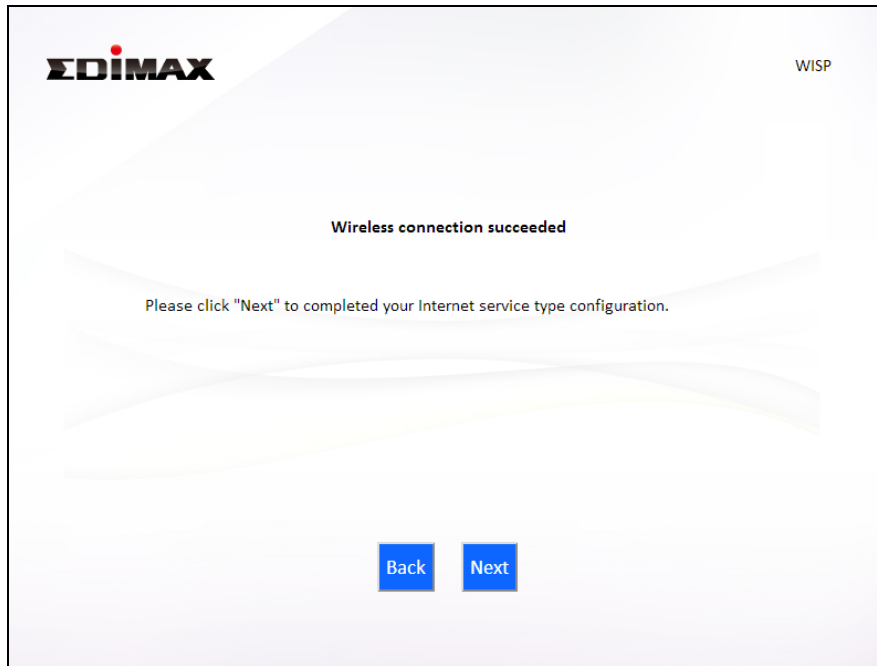
The screenshot shows the EDIMAX 5GHz Wireless Site Survey configuration interface. At the top left is the EDIMAX logo, and at the top right is the text "WISP". The main heading is "5GHz Wireless Site Survey". Below this, a message reads: "Please enter the security key provide from your WISP if required." There are two input fields: "Device SSID" with the value "EDIMAX\_5G" and "Security Key" with the value "12345678". At the bottom, there are two blue buttons labeled "Back" and "Next".

7. Wait a moment while the BR-6288ACL tests the wireless connection.

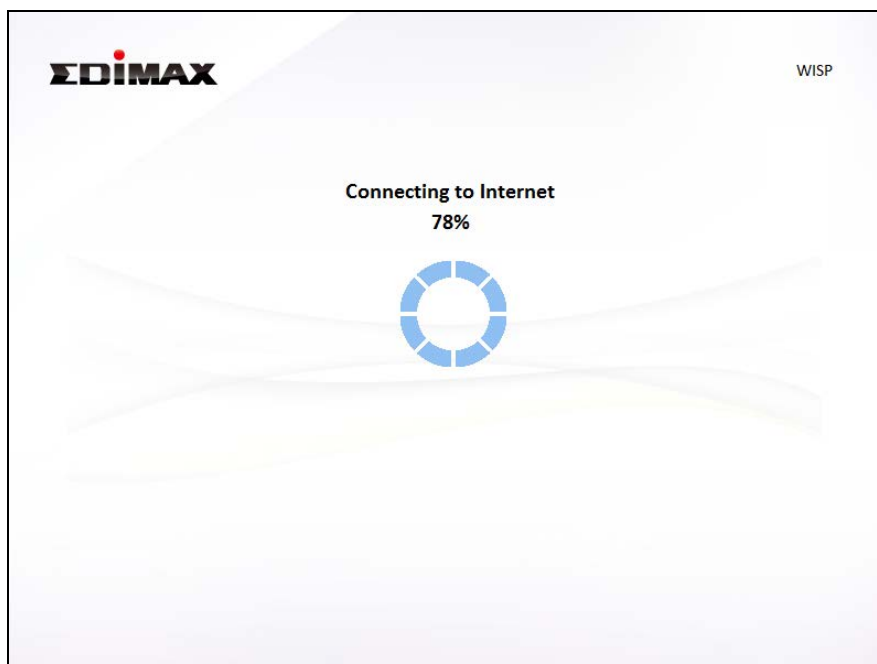




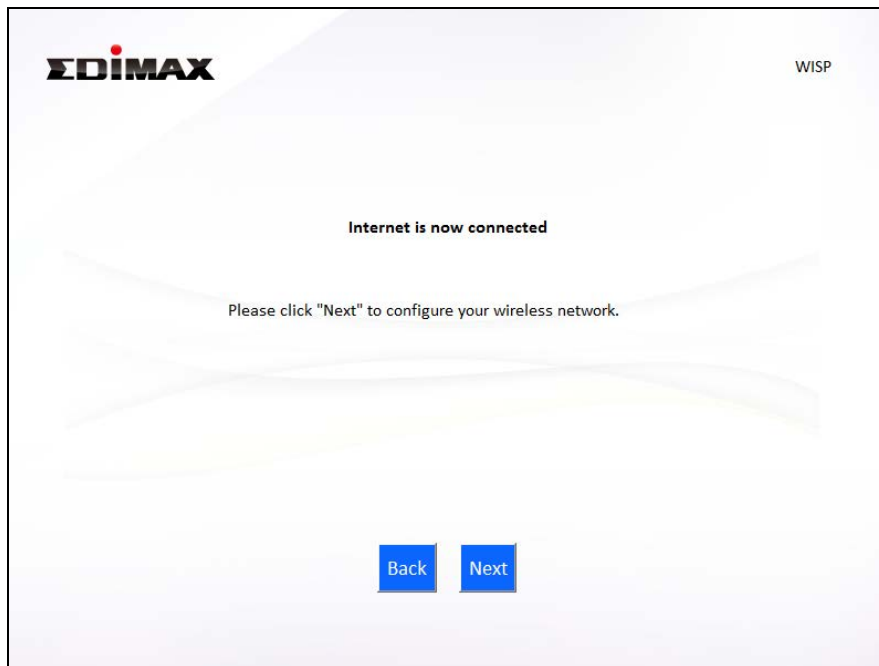
8. Click “Next” to continue your Internet service type configuration.



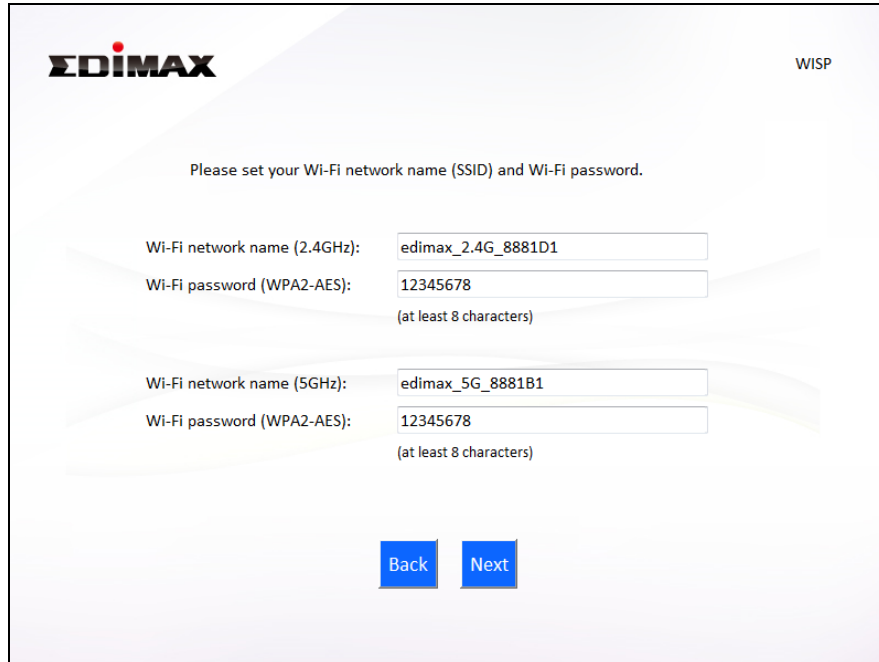
9. Wait a moment while the BR-6288ACL connects to the Internet.



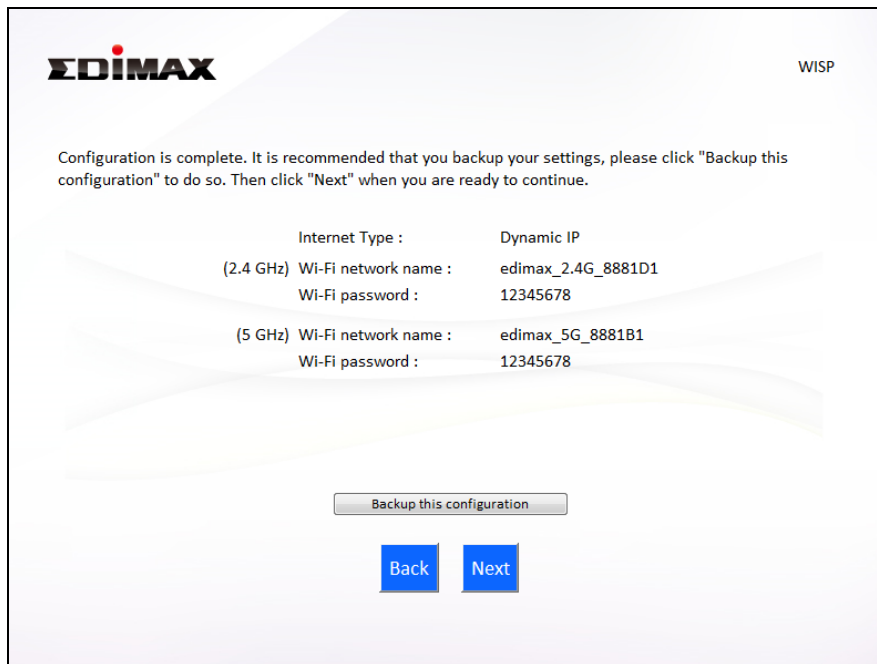
**10.** When the Internet is connected, click “Next” to configure your wireless network.



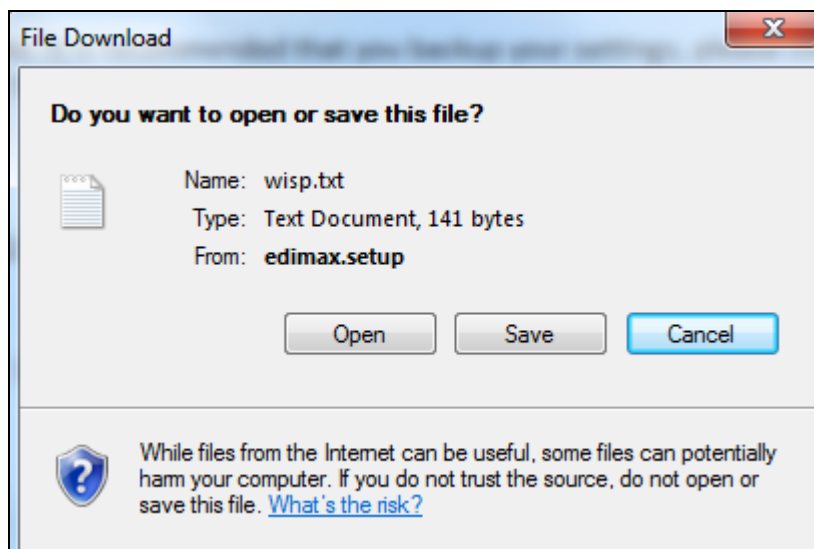
**11.** Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.



- 12.** A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



*If you wish to backup the device’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.*



**13.** Please wait a moment until the BR-6288ACL is ready.



**14.** A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.

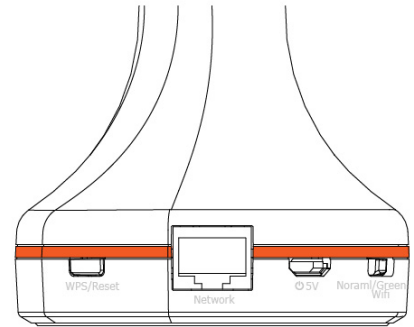


**15.** The BR-6288ACL is working and ready for use. Refer to [IV-2. Connecting to a Wi-Fi network](#) if you require more guidance.

## II-6. WPS Setup

If your wireless device supports WPS (Wi-Fi Protected Setup) then you can use this method to connect to the BR-6288ACL's Wi-Fi network.

- 1.** Press the **WPS/Reset button** on the BR-6288ACL for 2 seconds to activate WPS. The LED will then quickly flash orange/red to indicate that WPS is active.
- 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-7. Reset to Factory Default Settings


If you experience problems with your BR-6288ACL, you can reset the device back to its factory settings. This resets **all** settings back to default.

- 1.** Press and hold the **WPS/Reset button** found on the rear base of the product for at least 10 seconds.
- 2.** Release the button when the LED is quickly flashing orange/red.
- 3.** Wait for the BR-6288ACL to restart.

### III. Browser Based Configuration Interface

---


After you have setup the BR-6288ACL as detailed in **II. Installation** or the included **Quick Installation Guide**, you can use the browser based configuration interface to configure advanced settings.

 **Please ensure that your computer is set to use a dynamic IP address. Refer to [IV-1. Configuring your IP address](#) for more information.**

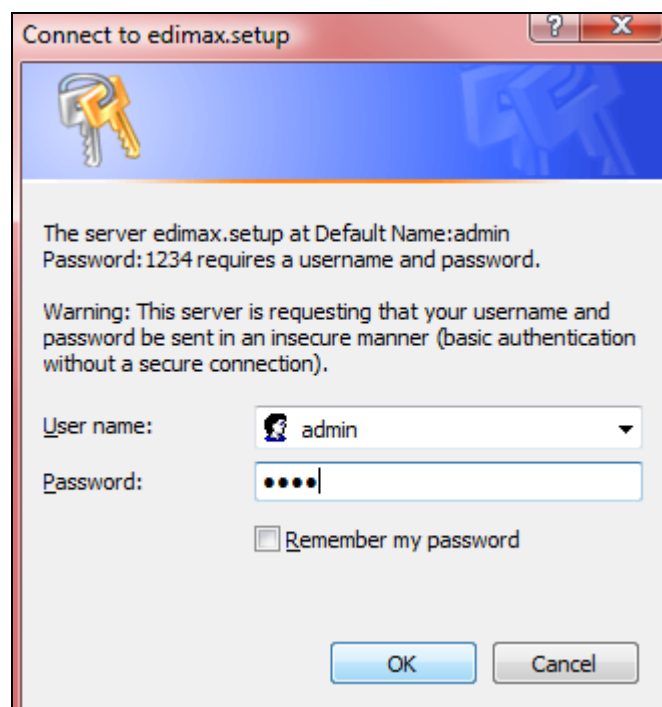
#### III-1. Login

1. To access the browser based configuration interface enter ***http://edimax.setup*** into the URL bar of a browser on a network device connected to the same Wi-Fi network as the BR-6288ACL.



 **If you can not access *http://edimax.setup*, connect the device to a computer using an Ethernet cable and try again.**

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



3. You will arrive at the “Status” screen. Use the menu down the left side to navigate.

The screenshot displays the EDIMAX Wi-Fi Router's Status page. The left sidebar contains a navigation menu with the following items: Status (selected), Setup Wizard, Internet, LAN, 2.4GHz Wireless, 5GHz Wireless, Firewall, QoS, Advanced, and Administration. The main content area is titled 'System Status' and is divided into several sections:

- System:**
  - Model: Wireless Router
  - Current Time: 1970/1/1 0:03:16
  - Hardware Version: Rev. A
  - Firmware Version: 1.03
  - [Check the latest version](#)
- LAN:**
  - IP Address: 192.168.2.1
  - Subnet Mask: 255.255.255.0
  - DHCP Server: Enable
  - MAC Address: 00:E0:4C:88:81:B1
- Internet:**
  - IP Address Mode: Dynamic IP Disconnect
  - IP Address:
  - Subnet Mask:
  - Default Gateway Address:
  - MAC Address: 00:E0:4C:88:81:B9
  - DNS 1:
  - DNS 2:
  - DNS 3:
- 2.4GHz Wireless:**
  - Mode: Access Point
  - SSID: edimax.setup
  - Channel Number: 2
  - Security: Disable
  - MAC Address: 00:E0:4C:88:81:D1
- 5GHz Wireless:**
  - Mode: Access Point
  - SSID: edimax.setup5G
  - Channel Number: 161
  - Security: Disable
  - MAC Address: 00:E0:4C:88:81:B1

## III-2. Save Settings

1. After you configure any settings, click the “Save Settings” button at the bottom of the screen to save your changes.



***The device needs to restart in order to bring any changes into effect.***

2. Then, click “Click here to restart” in order to restart the device and bring the changes into effect.

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.

3. To make several changes at once, use the “Save Settings” button after each change and then click “click here to restart” after your final change. Only one restart is necessary as long as each change is saved with the “Save Settings” button.



***After you click “click here to restart”, all saved changes will come into effect.***



### III-3. Main Menu

The main menu displays different options depending on your device's operating mode.



**For Range Extender mode: WPS please refer to 2.4GHz Wireless & 5GHz Wireless → WPS**

#### **Wi-Fi Router**

▶ Status
▶ Setup Wizard
▶ Internet
▶ LAN
▶ 2.4GHz Wireless
▶ 5GHz Wireless
▶ Firewall
▶ QoS
▶ Advanced
▶ Administration

#### **Access Point**

▶ Status
▶ Setup Wizard
▶ LAN
▶ 2.4GHz Wireless
▶ 5GHz Wireless
▶ Advanced
▶ Administration

#### **Range Extender**

▶ Status
▶ Setup Wizard
▶ WPS
▶ Administration

#### **Wireless Bridge**

▶ Status
▶ Setup Wizard
▶ Administration

#### **WISP**

▶ Status
▶ Setup Wizard
▶ WISP
▶ LAN
▶ 2.4GHz Wireless
▶ 5GHz Wireless
▶ Firewall
▶ QoS
▶ Advanced
▶ Administration

### III-3-1. Status



The “Status” page displays basic system information about the device, arranged into categories.



**Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.**

The screenshot shows the EDIMAX Wi-Fi Router Status page. The navigation menu on the left includes Status, Setup Wizard, Internet, LAN, 2.4GHz Wireless, 5GHz Wireless, Firewall, QoS, Advanced, and Administration. The main content area is titled "System Status" and is divided into four sections: System, LAN, Internet, and Wireless (2.4GHz and 5GHz).

System	
Model	Wireless Router
Current Time	2014/9/28 10:56:47
Hardware Version	Rev. A
Firmware Version	1.03
<a href="#">Check the latest version</a>	

LAN	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:E0:4C:82:98:C1

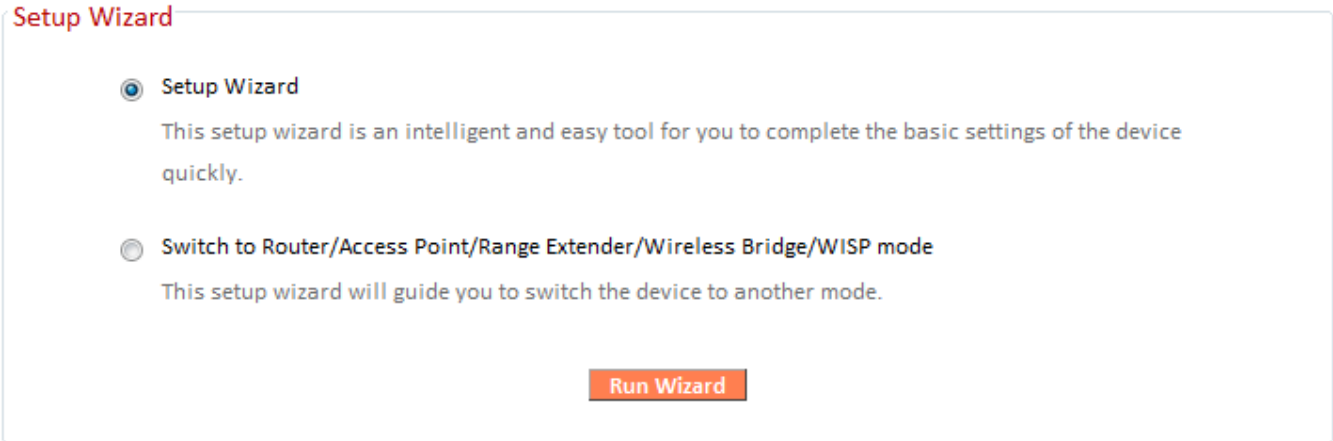
Internet	
IP Address Mode	PPPoE Connect
IP Address	118.165.189.118
Subnet Mask	255.255.255.255
Default Gateway Address	168.95.98.254
MAC Address	00:E0:4C:81:96:C9
DNS 1	168.95.192.1
DNS 2	168.95.1.1
DNS 3	168.95.1.1

2.4GHz Wireless	
Mode	Access Point
SSID	edimax_2.4G_8298D1
Channel Number	6
Security	WPA2 (AES)
MAC Address	00:E0:4C:82:98:D1

5GHz Wireless	
Mode	Access Point
SSID	edimax_5G_8298C1
Channel Number	44
Security	WPA2 (AES)
MAC Address	00:E0:4C:82:98:C1

### III-3-2. Setup Wizard

**Setup Wizard** You can run the setup wizard again to reconfigure the basic settings of the device, or you can run a wizard to help you switch the device to a different operating mode. Select “Setup Wizard” or “Switch to Router/Access Point/Range Extender/Wireless Bridge/WISP mode” and then click “Run Wizard” to begin.



<b>Setup Wizard</b>	This wizard will help you to set up the basic functions and settings of the device. For guidance about using the setup wizard, please refer to <a href="#">II. Installation</a> .
<b>Switch to Router/Access Point/ Range Extender/ Wireless Bridge/ WISP mode</b>	This wizard will help you to switch the device to a different operating mode: Wi-Fi router mode, access point mode, range extender, wireless bridge, or WISP mode (see below).

#### Switch to Router/Access Point/ Range Extender/ Wireless Bridge/ WISP mode:

1. Follow the on-screen instructions to back up your current settings and then reset the device back to its factory default settings.
2. After the device has reset you will see the screen below. Close your browser and open it again.

### Reset to Default

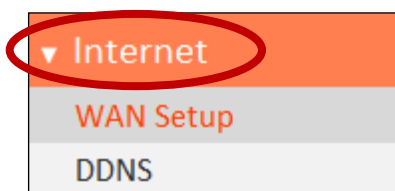
You have successfully reset the device to factory defaults. Please close the browser and open it again. This device will start running the setup wizard for you to switch the mode.

3. Follow the on-screen wizard to setup your device in a different mode. Refer to [II. Installation Step 3](#) onwards for help if needed.

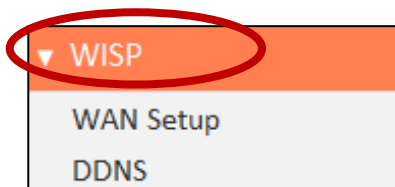


***If you don't see the "Get Started" screen, try reconnecting to the edimax.setup SSID and go to <http://edimax.setup> in a web browser.***

### III-3-3. Internet/WISP



The “Internet” menu provides access to WAN and DDNS settings. Click on an item from the submenu to view and/or configure the settings.



*In WISP mode, the screen below will be displayed:*

**WISP**

Enable / Disable     Disable  Enable

**Basic Settings :**

SSID   

Site Survey     2.4G  5G   

Channel Number   

**Security Setting :**

Encryption   

WPA Unicast Cipher Suite     WPA (TKIP)  WPA2 (AES)

Pre-shared Key Format   

Pre-shared Key

<b>Enable / Disable</b>	Enable or disable your WISP connection.
<b>SSID</b>	The name of the WISP network which your BR-6288ACL is connected to. Manually enter an SSID if you wish or use “Site Survey” below.
<b>Site Survey</b>	Select wireless frequency and click “Show List” to open a new window and select your WISP network.
<b>Security Setting</b>	Please refer to <b>III-3-5-1. Basic</b> for a description of security settings.

### III-3-3-1. WAN Setup

Select a Wide Area Network (WAN) connection mode and configure the settings. If you are unsure about your connection type, contact your ISP.



***In WISP mode, only Dynamic IP, Static IP & PPPoE are available for WAN Connection Mode.***

**WAN Connection Mode**

Connection Mode: Dynamic IP

**Dynamic IP**

Host Name:

Dynamic IP options: Dynamic IP, Static IP, PPPoE, PPTP, L2TP

#### III-3-3-1-1. Dynamic IP

Select “Dynamic IP”. If your Internet service provider assigns IP address automatically using DHCP (Dynamic Host Configuration Protocol).

**Dynamic IP**

Host Name:

MAC Address:  Clone MAC

DNS Address:  Obtain an IP address automatically  
 Use the following IP address

DNS1 Address:

DNS2 Address:

DNS3 Address:

DNS Proxy:  Disable  Enable

DNS Proxy Rules (URL):

MTU:  (512<= MTU Value <=1500)

TTL:  Disable  Enable

Save Settings

<b>Host Name</b>	Enter the host name of your computer.
<b>MAC Address</b>	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press “Clone Mac” to automatically enter your computer’s MAC address.
<b>DNS Address</b>	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
<b>DNS Address 1,2 &amp; 3</b>	Enter the DNS address(es) assigned by your ISP here.
<b>DNS Proxy</b>	Enable or disable a DNS proxy server.
<b>DNS Proxy Rules (URL)</b>	When DNS proxy is enabled, enter the URL of a DNS proxy server.
<b>MTU</b>	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1500.
<b>TTL</b>	Enable/Disable time to live (TTL) function which limits the lifespan of network data to improve performance.

### III-3-3-1-2. Static IP

Select “Static IP” if your ISP provides Internet access via a fixed IP address. Your ISP will provide you with such information as IP address, subnet mask, gateway address, and DNS address.

**Static IP**

Fixed IP IP Address

Subnet Mask

Default Gateway Address

MAC Address

DNS1 Address

DNS2 Address

DNS3 Address

DNS Proxy  Disable  Enable

DNS Proxy Rules (URL)

MTU  (512<= MTU Value <=1500)

TTL  Disable  Enable

<b>Fixed IP Address</b>	Input the IP address assigned by your ISP here.
<b>Subnet Mask</b>	Input the subnet mask assigned by your ISP here.
<b>Default Gateway Address</b>	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
<b>MAC Address</b>	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press “Clone Mac” to automatically enter your computer’s MAC address.
<b>DNS Address 1, 2 &amp; 3</b>	Enter the DNS address(es) assigned by your ISP here.
<b>DNS Proxy</b>	Enable or disable a DNS proxy server.
<b>DNS Proxy Rules</b>	When DNS proxy is enabled, enter the URL of a



<b>(URL)</b>	DNS proxy server.
<b>TTL</b>	Enable/Disable time to live (TTL) function which limits the lifespan of network data to improve performance.

### III-3-3-1-3. PPPoE

Select “PPPoE” if your ISP is providing you Internet access via PPPoE (Point-to-Point Protocol over Ethernet).

PPPoE

User Name: [ ] @wifi.hinet.net

Password: [ ]

MAC Address: [000000000000] Clone MAC

DNS Address:  Obtain an IP address automatically  
 Use the following IP address

DNS1 Address: [0.0.0.0]

DNS2 Address: [0.0.0.0]

DNS3 Address: [0.0.0.0]

DNS Proxy:  Disable  Enable

DNS Proxy Rules (URL): [ ]

TTL:  Disable  Enable

Service Name: [ ]

MTU: [1392] (512<= MTU Value <=1492)

Connection Type: [Continuous] Connect Disconnect

Idle Time Out: [10] (1-1000 minutes)

Enable Dual Wan Access :

IGMP Source:  ETH  PPP

Save Settings

<b>User Name</b>	Enter the user name assigned by your ISP here.
<b>Password</b>	Enter the password assigned by your ISP here.
<b>MAC Address</b>	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press “Clone Mac” to automatically enter your computer’s MAC address.

<b>DNS Address</b>	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
<b>DNS Address 1, 2 &amp; 3</b>	Enter the DNS address(es) assigned by your ISP here.
<b>DNS Proxy</b>	Enable or disable a DNS proxy server.
<b>DNS Proxy Rules (URL)</b>	When DNS proxy is enabled, enter the URL of a DNS proxy server.
<b>Service Name</b>	Give this Internet service a name (optional).
<b>MTU</b>	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1392.
<b>Connection Type</b>	Specify a connection type: <ol style="list-style-type: none"> <li>1. “Continuous”: Connected all the time.</li> <li>2. “Connect on Demand”: Connect when you initiate an Internet connection.</li> <li>3. “Manual”: Connect/disconnect manually using the “Connect” and “Disconnect” buttons.</li> </ol>
<b>Idle Time Out</b>	Specify the amount of time the router waits before shutting down an idle connection. Only available when “Connect on Demand” (above) is selected.
<b>Enable Dual-WAN Access</b>	Enable/disable dual WAN access. When you enable dual WAN access, select an IGMP source and enter a “Host Name” and “MAC Address”.

### III-3-3-1-4. PPTP

Select “PPTP” if your ISP is providing you Internet access via PPTP (Point-to-Point Tunneling Protocol). Then select “Obtain an IP address automatically” or “Use the following IP address” depending on your ISP.

**PPTP**

Obtain an IP address automatically :

Host Name

MAC Address  **Clone MAC**

Use the following IP address :

Static IP Address

Subnet Mask

Default Gateway Address

MAC Address  **Clone MAC**

DNS Address  Obtain an IP address automatically  
 Use the following IP address

DNS1 Address

DNS2 Address

DNS3 Address

DNS Proxy  Disable  Enable

DNS Proxy Rules (URL)

Enable Dual Wan Access :

IGMP Source  ETH  PPP

**PPTP Settings :**

User ID

Password

PPTP Gateway

Connection ID  (Optional)

MTU  (512<= MTU Value <=1492)

BEZEQ-ISRAEL  Enable (for use with BEZEQ network in Israel only)

Connection Type  **Connect** **Disconnect**

Idle Time Out  (1-1000 minutes)

**Save Settings**

<b>Host Name</b>	Enter the host name of your computer here If required.
<b>MAC Address</b>	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press “Clone Mac” to automatically enter your computer’s MAC address.
<b>Static IP Address</b>	Input the IP address assigned by your ISP here.
<b>Subnet Mask</b>	Input the subnet mask assigned by your ISP here.
<b>Default Gateway Address</b>	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
<b>MAC Address</b>	If your ISP filters access by MAC addresses, enter your computer’s MAC address here. Click “Clone MAC” to automatically enter your computer’s MAC address.
<b>DNS Address</b>	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
<b>DNS 1,2 &amp; 3</b>	Enter the DNS address(es) assigned by your ISP here.
<b>DNS Proxy</b>	Enable or disable a DNS proxy server.
<b>DNS Proxy Rules (URL)</b>	When DNS proxy is enabled, enter the URL of a DNS proxy server.
<b>User ID</b>	Input the user name assigned by your ISP here.
<b>Password</b>	Input the password assigned by your ISP here.
<b>PPTP Gateway</b>	Input the PPTP gateway assigned by your ISP here.
<b>Connection ID</b>	Specify a reference name/ID for the connection.
<b>MTU</b>	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1392.
<b>BEZEQ-ISRAEL</b>	Check the “Enable” box if you are using BEZEQ network services (Israel users only).

<b>Connection Type</b>	Specify a connection type: <ol style="list-style-type: none"><li>1. "Continuous": Connected all the time.</li><li>2. "Connect on Demand": Connect when you initiate an Internet connection.</li><li>3. "Manual": Connect/disconnect manually using the "Connect" and "Disconnect" buttons.</li></ol>
<b>Idle Time Out</b>	Specify the amount of time the router waits before shutting down an idle connection. Only available when "Connect on Demand" (above) is selected.

### III-3-3-1-5. L2TP

Select “L2TP” if your ISP is providing you Internet access via L2TP (Layer 2 Tunneling Protocol).

**L2TP**

Obtain an IP address automatically :

Host Name

MAC Address  **Clone MAC**

Use the following IP address :

Static IP Address

Subnet Mask

Default Gateway Address

MAC Address  **Clone MAC**

DNS Address  Obtain an IP address automatically  
 Use the following IP address

DNS1 Address

DNS2 Address

DNS3 Address

DNS Proxy  Disable  Enable

DNS Proxy Rules (URL)

Enable Dual Wan Access :

IGMP Source  ETH  PPP

**L2TP Settings :**

User ID

Password

L2TP Gateway

MTU  (512<= MTU Value <=1492)

Connection Type  **Connect** **Disconnect**

Idle Time Out  (1-1000 minutes)

**Save Settings**

<b>Host Name</b>	Enter the host name of your computer here If required.
<b>MAC Address</b>	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to

	a computer, press “Clone Mac” to automatically enter your computer’s MAC address.
<b>Static IP Address</b>	Input the IP address assigned by your ISP here.
<b>Subnet Mask</b>	Input the subnet mask assigned by your ISP here.
<b>Default Gateway Address</b>	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
<b>MAC Address</b>	If your ISP filters access by MAC addresses, enter your computer’s MAC address here. Click “Clone MAC” to automatically enter your computer’s MAC address.
<b>DNS Address</b>	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
<b>DNS 1,2 &amp; 3</b>	Enter the DNS address(es) assigned by your ISP here.
<b>DNS Proxy</b>	Enable or disable a DNS proxy server.
<b>DNS Proxy Rules (URL)</b>	When DNS proxy is enabled, enter the URL of a DNS proxy server.
<b>User ID</b>	Input the user name assigned by your ISP here.
<b>Password</b>	Input the password assigned by your ISP here.
<b>L2TP Gateway</b>	Input the L2TP gateway assigned by your ISP here.
<b>Connection ID</b>	Specify a reference name/ID for the connection.
<b>MTU</b>	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1392.
<b>Connection Type</b>	Specify a connection type: <ol style="list-style-type: none"> <li>1. “Continuous”: Connected all the time.</li> <li>2. “Connect on Demand”: Connect when you initiate an Internet connection.</li> <li>3. “Manual”: Connect/disconnect manually using the “Connect” and “Disconnect” buttons.</li> </ol>
<b>Idle Time Out</b>	Specify the amount of time the router waits before shutting down an idle connection. Only available when “Connect on Demand” (above) is selected.



### III-3-3-2. DDNS

Dynamic DNS (DDNS) is a service which provides a hostname-to-IP service for dynamic IP users. The changing nature of dynamic IPs means that it can be difficult to access a service provided by a dynamic IP user; a DDNS service though can map such dynamic IP addresses to a fixed hostname, for easier access. The router supports several DDNS service providers, for more details and to register for a DDNS account please visit the DDNS providers website(s), examples of which are listed below.

DDNS

Enable / Disable  Enable  Disable

Provider

Domain Name

Account / E-mail

Password / Key

Save Settings

<b>Enable/Disable</b>	Enable or disable DDNS
<b>Provider</b>	Select DDNS service provider.
<b>Domain Name</b>	Enter the domain name provided by the DDNS provider.
<b>Account/Email</b>	Please enter the DDNS registration account/email.
<b>Password/Key</b>	Enter the DDNS service password/key.

The following DDNS services are supported:

- 3322** <http://www.3322.org>
- DHS** <http://www.dhs.org>
- DynDNS** <http://www.dyndns.org>
- ODS** <http://ods.org>
- TZO** <http://www.tzo.com>
- GnuDIP** <http://gnudip2.sourceforge.net>
- DyNS** <http://www.dyns.cx/>

<b>ZoneEdit</b>	<i><a href="http://www.zoneedit.com">http://www.zoneedit.com</a></i>
<b>CyberGate</b>	<i><a href="http://cybergate.planex.co.jp/ddns/">http://cybergate.planex.co.jp/ddns/</a></i>
<b>NS2GO</b>	<i><a href="http://www.ns2go.com/">http://www.ns2go.com/</a></i>
<b>NO-IP</b>	<i><a href="http://www.noip.com/">http://www.noip.com/</a></i>

### III-3-4. LAN



You can configure your Local Area Network (LAN) on this page. You can enable the router to dynamically allocate IP addresses to your LAN clients, and you can modify the IP address of the device. The device’s default IP address is 192.168.2.1.



***You can access the browser based configuration interface using the device’s IP address instead of using the URL <http://edimax.setup>.***

**LAN IP**

IP Address	<input type="text" value="192.168.2.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
802.1d Spanning Tree	<input type="text" value="Disable"/> ▼
DHCP Server	<input type="text" value="Enable"/> ▼
Lease Time	<input type="text" value="One hour"/> ▼

<b>IP Address</b>	Specify the IP address here. This IP address will be assigned to the BR-6288ACL and will replace the default IP address.
<b>Subnet Mask</b>	Specify a subnet mask. The default value is 255.255.255.0
<b>802.1d Spanning Tree</b>	Select “Enable” or “Disable” to enable/disable 802.1d Spanning Tree. This creates a tree of connected layer-2 bridges (typically Ethernet switches) within a mesh network, and disables those links that are not part of the tree, leaving a single active path between any two network nodes.
<b>DHCP Server</b>	Enable or disable the DHCP server.
<b>Lease Time</b>	Select a lease time for the DHCP leases here. The DHCP client will obtain a new IP address after the period expires.

Your device's DHCP server automatically assigns IP addresses to computers on its network, between a defined range of numbers.

**DHCP Server**

Start IP

End IP

<b>Start IP</b>	Enter the start IP address for the DHCP server's IP address leases.
<b>End IP</b>	Enter the end IP address for the DHCP server's IP address leases.

Your device's DHCP server can be configured to assign static (fixed) IP addresses to specified network devices, identified by their unique MAC address.

**Static DHCP Lease Table**

Only 16 sets of addresses are allowed.

NO.	MAC Address	IP Address	Select
1	00:1b:63:cb:4c:b5	192.168.2.110	<input type="checkbox"/>

Enable Static DHCP Leases

<b>Enable Static DHCP Leases</b>	Enable/disable static DHCP leases. This must be enabled in order to assign any network device a static IP address.
<b>MAC Address</b>	Enter the specified network device's MAC address here.
<b>IP Address</b>	Assign a fixed IP address for the specified network device here.
<b>Add</b>	Add the information to the "Static DHCP Leases Table".
<b>Clear</b>	Clear the MAC address and IP address fields.
<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.



***The LAN IP page will be displayed as below when your device is set to access point mode. You can set the BR-6288ACL to obtain an IP address automatically or you can specify an IP address.***

LAN IP

Obtain an IP address automatically

Use the following IP address

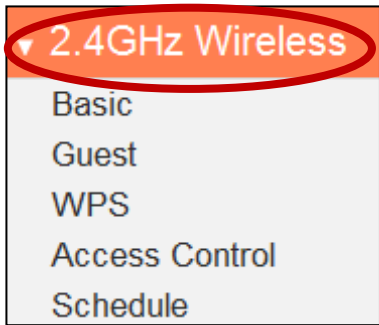
IP Address

Subnet Mask

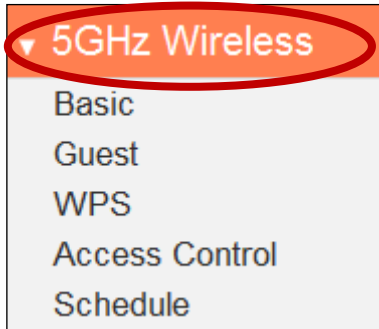
Default Gateway Address

DNS Address

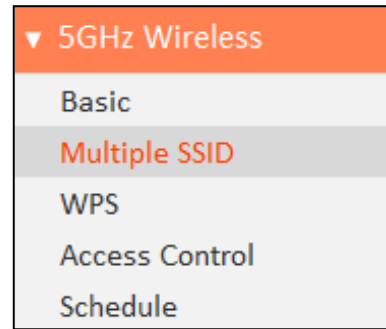
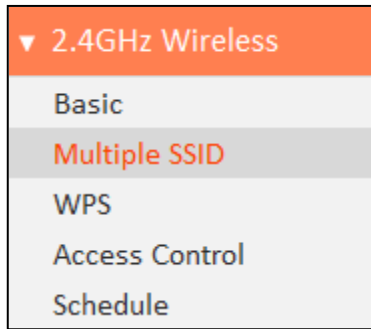
### III-3-5. 2.4GHz Wireless & 5GHz Wireless



The “2.4GHz Wireless” & “5GHz Wireless” menu allows you to configure SSID and security settings for your Wi-Fi network along with a guest Wi-Fi network. WPS, access control and scheduling functions can also be managed from here.



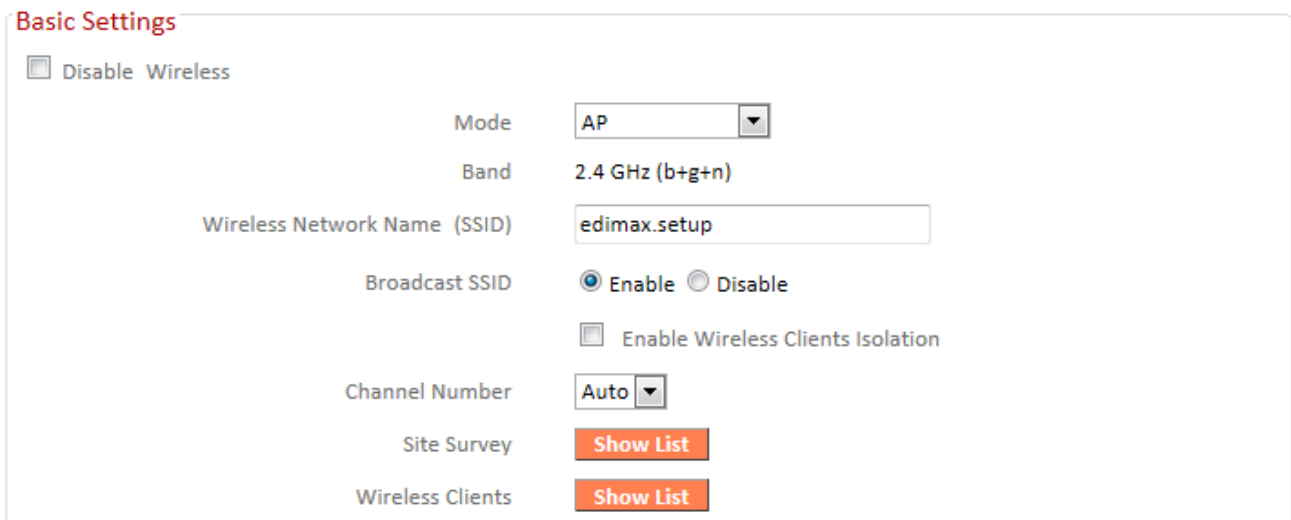
#### Access Point Mode:



*In Access Point mode, the “Guest” feature in the menu is replaced by “Multiple SSID”.*

#### III-3-5-1. Basic


The “Basic” screen displays settings for your primary 2.4GHz or 5GHz Wi-Fi network.




<b>Disable Wireless</b>	Check the box to disable the wireless function of your device.
<b>Mode</b>	Keep the default “AP” value for the device to act as a standard wireless access point, or select “AP Bridge-WDS” for the device to function in WDS mode (see below).
<b>Band</b>	Displays the wireless standard used for the BR-6288ACL’s “2.4GHz (B+G+N)” means that 802.11b, 802.11g, and 802.11n wireless clients can connect to the BR-6288ACL.
<b>Wireless Network Name (SSID)</b>	This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumeric characters.
<b>Broadcast SSID</b>	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
<b>Enable Wireless Clients Isolation</b>	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients’ usernames and passwords.
<b>Channel Number</b>	Select a wireless radio channel or use the default “Auto” setting from the drop-down menu.
<b>Site Survey</b>	Click “Show List” to display a new window showing information about the surrounding wireless environment. This information is useful to select an effective wireless channel number.
<b>Wireless Clients</b>	Click “Show List” to display a new window showing

	information about wireless clients. Please disable any pop-up blockers if you have difficulty using this function.
--	--

**AP Bridge-WDS:**

Mode    
 Band

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

 **When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.**

WDS must be configured on each access point, using correct MAC addresses. All access points should use the same wireless channel.

MAC Address 1   
 MAC Address 2   
 MAC Address 3   
 MAC Address 4   
 Set Security

<b>MAC Address 1 - 4</b>	Enter the correct MAC address for other access points in WDS mode.
<b>Set Security</b>	Click “Set Security” to open a new window and enter the security settings for WDS (shown below). Click “Save” when finished.

 **Please ensure you setup and save wireless security settings before you click “Set Security” to set WDS security settings.**



## AP Bridge-WDS Security Setting

Encryption

WPA Unicast Cipher Suite  WPA2 (AES)

Pre-shared Key Format

Pre-shared Key

### Wireless Security:

Wireless Security

Encryption

Key Length

Key Format

Encryption Key   Hide

Enable 802.1x Authentication

Select an encryption type from the drop-down menu:



***“WPA Pre-shared Key” is the recommended and most secure encryption type.***



***In WISP mode, WPA RADIUS is unavailable for the wireless band that is used to connect to WISP’s AP.***

Wireless Security

Encryption

Enable 802.1x Authentication

- Disable
- WEP
- WPA Pre-shared Key
- WPA RADIUS

### III-3-5-1-1. Disable

Encryption is disabled and no password/key is required to connect to the BR-6288ACL.



***Disabling wireless encryption is not recommended. When disabled, anybody within range can connect to your device's SSID.***

<b>Enable 802.1x Authentication</b>	Check the box to enable the 802.1x authentication. A RADIUS server is required to perform 802.1x authentication: enter the RADIUS server's information in the relevant fields (below).
-------------------------------------	--

Enable 802.1x Authentication

RADIUS Server IP address

RADIUS Server Port

RADIUS Server Password

### III-3-5-1-2. WEP

WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security consider using WPA encryption.

**Wireless Security**

Encryption:

Key Length:

Key Format:

Encryption Key:   Hide

Enable 802.1x Authentication

<b>Key Length</b>	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit.
<b>Key Format</b>	Choose from “ASCII” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
<b>Encryption Key</b>	Enter your encryption key/password according to the format you selected above. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.
<b>Enable 802.1x Authentication</b>	Check the box to enable the 802.1x authentication. A RADIUS server is required to perform 802.1x authentication: enter the RADIUS server’s information in the relevant fields (below).

Enable 802.1x Authentication

RADIUS Server IP address:

RADIUS Server Port:

RADIUS Server Password:

### III-3-5-1-3. WPA Pre-Shared Key

WPA pre-shared key is the recommended and most secure encryption type.

**Wireless Security**

Encryption: WPA Pre-shared Key

WPA Unicast Cipher Suite:  WPA (TKIP)  WPA2 (AES)  WPA2 Mixed

Pre-shared Key Format: Passphrase

Pre-shared Key:   Hide

<b>WPA Unicast Cipher Suite</b>	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP), but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
<b>Pre-shared Key Format</b>	Choose from “Passphrase” (8-63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).
<b>Pre-shared Key</b>	Please enter a key according to the format you selected above. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.

### III-3-5-1-4. WPA Radius

WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can authenticate the identity of every wireless client against a user database.

**Wireless Security**

Encryption:

WPA Unicast Cipher Suite:  WPA (TKIP)  WPA2 (AES)  WPA2 Mixed

RADIUS Server IP address:

RADIUS Server Port:

RADIUS Server Password:

<b>WPA Unicast Cipher Suite</b>	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP), but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
<b>RADIUS Server IP address</b>	Input the IP address of the RADIUS authentication server here.
<b>RADIUS Server Port</b>	Input the port number of the RADIUS authentication server here. The default value is 1812.
<b>RADIUS Server Password</b>	Input the password of the RADIUS authentication server here.

### III-3-5-2. Guest/ Multiple SSID

You can setup an additional “Guest” Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary network. The “Guest” screen displays settings for your guest Wi-Fi network.



***The guest network is separate from your primary network. The settings for your primary network can be found in the “Basic” menu.***



***In access point mode, the “Guest” feature in the menu is replaced by “Multiple SSID”. The BR-6288ACL supports up to four additional SSIDs for each wireless band in access point mode.***

**Basic Settings**

Enable Guest SSID

Guest Wireless Name:

Enable Wireless Clients Isolation

Band: 2.4 GHz (b+g+n)

Channel Number:  (Same as main SSID)

---

**Wireless Security**

Encryption:

<b>Enable Guest SSID</b>	Check/uncheck the box to enable/disable the guest Wi-Fi network.
<b>Wireless Guest Name</b>	Enter a reference/ID name for your guest wireless network.
<b>Enable Wireless Clients Isolation</b>	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients’ usernames and passwords.
<b>Band</b>	Displays the wireless standard used for the BR-6288ACL’s frequency band: 2.4GHz (B+G+N): Allows 802.11b, 802.11g, and 802.11n wireless clients to connect to the

	BR-6288ACL.
<b>Channel Number</b>	Channel number for the guest network is the same as the main SSID and cannot be adjusted independently.

<b>Encryption</b>	Please refer to <a href="#">III-3-5-1. Basic: Wireless Security</a> for details about security settings.
-------------------	--



**WPA RADIUS encryption type is not available for the guest network.**

### MULTIPLE SSID:

The BR-6288ACL supports up to four additional SSIDs for each wireless band in access point mode. Once configured, these SSIDs are displayed in the “Multiple SSID Status” table as shown below. Use the “Multiple SSID Basic Settings” box to configure additional SSIDs.

#### Multiple SSID Status

NO.	Enable	SSID	VLAN ID	Encryption	MAC Address
1	<input checked="" type="checkbox"/>	edimax.1	0	Disable	80:1F:02:ED:F2:D2
2	<input checked="" type="checkbox"/>	edimax.2	0	WPA2 (AES)	80:1F:02:ED:F2:D3
3	<input checked="" type="checkbox"/>	VLAN	1	WPA2 (AES)	80:1F:02:ED:F2:D4
4	<input type="checkbox"/>	edimax.4	0	Disable	80:1F:02:ED:F2:D5

#### Multiple SSID Basic Settings

Multiple SSID:  ( MAC Address : 80:1F:02:ED:F2:D2 )

Wireless Network Name (SSID):

Enable Multiple SSID

Enable Wireless Clients Isolation

Band: 2.4 GHz (b+g+n)

Channel Number:  (Same as main SSID)

VLAN ID:  (Untagged:0, Tagged:1~4094)

<b>Multiple SSID</b>	Use the drop down menu to select which SSID (numbered 1 – 4) to configure.
<b>Wireless Network Name (SSID)</b>	Enter a reference/ID name to separate your wireless network.

<b>Enable Multiple SSID</b>	Check/uncheck this box to enable/disable the specified SSID. Must be checked for the SSID to function.
<b>Enable Wireless Clients Isolation</b>	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
<b>Band</b>	Displays the wireless standard used for the BR-6288ACL's frequency band: 2.4GHz (B+G+N): Allows 802.11b, 802.11g, and 802.11n wireless clients to connect to the BR-6288ACL.
<b>Channel Number</b>	Channel number for the guest network is the same as the main SSID and cannot be adjusted independently.
<b>VLAN ID</b>	Set a VLAN ID for the specified SSID (see below).

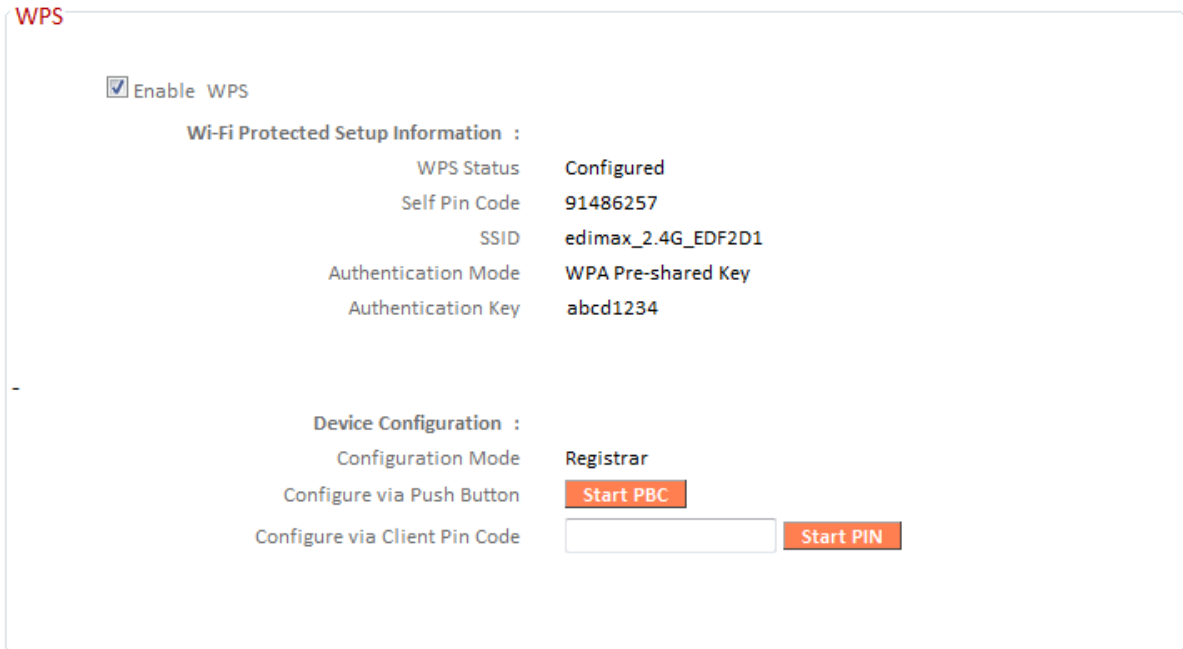


***A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs 0 – 4094 are supported.***



### III-3-5-3. WPS

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device’s firmware/configuration interface. When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. PIN code WPS includes the use of a PIN code between the two devices for verification.



<b>Enable WPS</b>	Check/uncheck this box to enable/disable WPS.
<b>WPS Status</b>	Displays “Configured” or “unConfigured” depending on whether WPS and SSID/security settings for the device have been configured or not, either manually or using the WPS button.
<b>Self PIN Code</b>	Displays the WPS PIN code of the device.
<b>SSID</b>	Displays the SSID of the device.
<b>Authentication Mode</b>	Displays the wireless security authentication mode of the device.
<b>Authentication Key</b>	Displays the wireless security authentication key.
<b>Configuration Mode</b>	The configuration mode of the device’s WPS setting is displayed here. “Registrar” means the device acts as an access point for a wireless client to connect

	to and the wireless client(s) will follow the device's wireless settings.
<b>Configure via Push Button</b>	Click "Start PBC" (Push-Button Configuration) to activate WPS on the access point. WPS will be active for 2 minutes.
<b>Configure via Client PIN Code</b>	Enter the wireless client's PIN code here and click "Start PIN" to activate PIN code WPS. Refer to your wireless client's documentation if you are unsure of its PIN code.

### III-3-5-4. Access Control

Access Control is a security feature that can help to prevent unauthorized users from connecting to your wireless router.

This function allows you to define a list of network devices permitted to connect to the BR-6288ACL. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the BR-6288ACL, it will be denied.

To enable this function, check the box labeled "Enable Wireless Access Control".

**Access Control**

Enable Wireless Access Control

MAC Address:    Comment:

MAC Address	Device Name	IP Address	Comment	Select
aa:bb:cc:dd:ee:ff	OFFLINE	OFFLINE	Edimax	<input type="checkbox"/>

<b>MAC address</b>	<p>Select a PC name from the drop-down list and click “&gt;&gt;” to add enter it into the blank field to the right.</p> <p>Click “Refresh’ in the drop-down menu to refresh the list of available MAC addresses. If the address you wish to add is not listed, enter it manually.</p> <p>Enter a MAC address of computer or network device manually without dashes or colons e.g. for MAC address ‘aa-bb-cc-dd-ee-ff’ enter ‘aabbccddeeff’.</p>
<b>Comment</b>	Enter a comment for reference/identification consisting of up to 16 alphanumerical characters.
<b>Add</b>	Click “Add” to add the MAC address to the MAC address filtering table.

MAC address entries will be listed in the table as shown below. Select an entry using the “Select” checkbox.

MAC Address	Device Name	IP Address	Comment	Select
00:1b:63:cb:4c:b5	MACBOOK-4729BA	192.168.2.101		<input type="checkbox"/>

Delete Selected Delete All

<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.
-------------------------------------	--

### III-3-5-5. Schedule

The schedule feature allows you to automate the wireless radio to switch on/off at specified times. Multiple schedules can be configured. Check/uncheck the box “Enable Schedule Settings” to enable/disable the wireless on/off scheduling function.



***The BR-6288ACL must remain connected to the Internet and use an NTP server for the schedule feature to function correctly.***

**Wireless Schedule**

Enable Schedule Settings

1. Weekday  Sunday  Monday  Tuesday  Wednesday  
 Thursday  Friday  Saturday

2. Time Hour  Minute

3. Command

Weekday	Time	Command	Select
Monday,Tuesday,Wednesday,Thursday,Friday	01:00	wireless off	<input type="checkbox"/>
Monday,Tuesday,Wednesday,Thursday,Friday	08:00	wireless on	<input type="checkbox"/>

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.



***Wireless scheduling can save energy and increase the security of your network.***

- 1.** Use the checkboxes to select which day(s) to include in the schedule.
- 2.** Specify a time (hour and minute) for the schedule using the drop-down menu.
- 3.** Select which command applies to this schedule from the drop-down menu, either “Wireless On” or “Wireless Off”.

**Add**

Add the schedule to the table of active schedules.

Active schedules will be displayed in the table as shown below. Select an entry using the “Select” checkbox.

Weekday	Time	Command	Select
Monday,Tuesday,Wednesday,Thursday,Friday	01:00	wireless off	<input type="checkbox"/>
Monday,Tuesday,Wednesday,Thursday,Friday	08:00	wireless on	<input type="checkbox"/>

[Delete Selected](#) [Delete All](#)

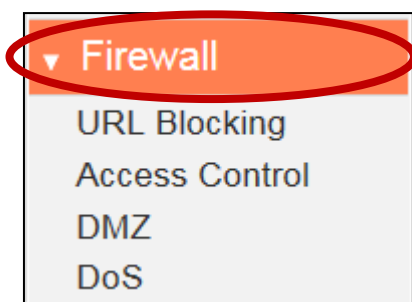
[Save Settings](#)

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.

**Delete Selected /  
Delete All**

Delete selected or all entries from the table.

### III-3-6. Firewall



The “Firewall” menu provides access to URL blocking, access control, DMZ and DoS functions to improve the security of your wireless network.

**Firewall**

The router provides stateful packet inspection (SPI) firewall protection. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.

SPI firewall  Enable  Disable

<b>SPI firewall</b>	Enable or disable the Stateful Packet Inspection (SPI) firewall.
---------------------	--

#### III-3-6-1. URL Blocking

This function can block Internet access by either specific URLs or keywords. Check/uncheck the “Enable URL Blocking” box to enable/disable URL blocking.

**URL Blocking**

Enable URL Blocking

URL / Keyword :

NO.	URL / Keyword	Select
1	www.blockedwebsite.com	<input type="checkbox"/>

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.

<b>URL/Keyword</b>	Enter the URL or keyword to be blocked.
<b>Add</b>	Add the URL or keyword to the blocked table.

Blocked URLs/keywords entries will be listed in the table as shown below. Select an entry using the “Select” checkbox.

NO.	URL / Keyword	Select
1	www.blockedwebsite.com	<input type="checkbox"/>

Delete Selected Delete All

Save Settings

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.

<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.
-------------------------------------	--

### III-3-6-2. Access Control



**Access Control (MAC filtering) can also be configured from [III-3-5-4. Access Control](#).**

Access Control is a security feature that can help to prevent unauthorized users from connecting to your wireless router.

This function allows you to define a list of network devices permitted or denied to connect to the BR-6288ACL. Devices are each identified by their unique MAC address or IP address. Specific services can also be allowed/denied for IP addresses.

Check/uncheck the “Enable MAC Filtering” and/or “Enable IP Filtering” box to enable/disable MAC filtering and/or IP filtering.

**Access Control**

Enable MAC Filtering :  Deny  Allow

Client PC	MAC Address	Computer Name	Comment
<input type="text"/>	<input type="text"/>	<< ---- Select----	<input type="text"/>

MAC Filtering Table :

NO	Computer Name	Client PC MAC Address	Comment	Select
1	MACBOOK-4729BA	00:1b:63:cb:4c:b5		<input type="checkbox"/>

Enable IP Filtering Table :  Deny  Allow

IP Filtering Table :

NO	Client PC Description	Client PC IP Address	Client Service	Protocol	Port Range	Select
1	Laptop	192.168.2.101	WWW, E-mail Sending, News Forums, E-mail Receiving, Secure HTTP, File Transfer			<input type="checkbox"/>

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.



## MAC Filtering:

<b>Enable MAC Filtering</b>	Check the box to enable MAC filtering and select whether to “Deny” or “Allow” access for specified MAC address.
<b>Client PC MAC Address</b>	Enter a MAC address of computer or network device manually without dashes or colons e.g. for MAC address ‘aa-bb-cc-dd-ee-ff’ enter ‘aabbccddeeff’.
<b>Computer Name</b>	Select a computer name from the drop-down list and click “<<” to add its MAC address into the “Client PC Mac Address” field.  Click “Refresh’ in the drop-down menu to refresh the list of available MAC addresses. If the address you wish to add is not listed, enter it manually.
<b>Comment</b>	Enter a comment for reference/identification consisting of up to 16 alphanumeric characters.
<b>Add</b>	Click “Add” to add the MAC address to the MAC address filtering table.

MAC address entries will be listed in the table as shown below. Select an entry using the “Select” checkbox.

MAC Filtering Table :

NO	Computer Name	Client PC MAC Address	Comment	Select
1	MACBOOK-4729BA	00:1b:63:cb:4c:b5		<input type="checkbox"/>

Delete Selected Delete All

<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.
-------------------------------------	--

## IP Filtering:

<b>Enable IP Filtering</b>	Check the box to enable IP filtering and select whether to “Deny” or “Allow” access for specified IP address.
<b>Add PC</b>	Opens a new window to add a new IP to the list, to deny or allow access/services according to above.

### Access Control Add PC

This page allows users to define service limitations of client PCs, including IP address and service type.

#### Access Control Add PC :

Client PC Description   
Client PC IP address  -

#### Client PC Service :

Service Name	Detail Description	Select
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input checked="" type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input checked="" type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input checked="" type="checkbox"/>
File Transfer	FTP, TCP Port 21, 20	<input checked="" type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 389,522,1503,1720,1731	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

#### User Define Service :

Protocol    
Port Range

<b>Client PC Description</b>	Enter a description for reference/identification of up to 16 alphanumeric characters.
<b>Client PC IP address</b>	Enter a starting IP address in the left field and the end IP address in the right field to define a range of IP addresses; or enter an IP address in the left field only to define a single IP address.
<b>Service Name</b>	Various services are listed here with a short description. Check/uncheck the box for each service you wish to select.
<b>Protocol</b>	Select protocol "TCP" or "UDP" or "Both" for a service not included in the "Client PC Service" list.
<b>Port Range</b>	Enter the port range for the service not included in the "Client PC Service" list.  Enter a single port number e.g. 110, a range of port numbers e.g. 110-120, or multiple port numbers separated by a comma e.g. 110,115,120.
<b>Add</b>	Click "Add" to add selected services or a user defined service to the IP filtering table.

IP filtering entries will be listed in the IP filtering table shown below.

Enable IP Filtering Table :  Deny  Allow

IP Filtering Table :

NO	Client PC Description	Client PC IP Address	Client Service	Protocol	Port Range	Select
1	Laptop	192.168.2.101	WWW, E-mail Sending, News Forums, E-mail Receiving, Secure HTTP, File Transfer			<input type="checkbox"/>

<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.
-------------------------------------	--

### III-3-6-3. DMZ

A Demilitarized Zone (DMZ) is an isolated area in your local network where private IP addresses are mapped to specified Internet IP addresses, allowing unrestricted access to the private IP addresses but not to the wider local network.

You can define a virtual DMZ host here. This is useful for example, if a network client PC cannot run an application properly from behind an NAT firewall, since it opens the client up to unrestricted two-way access.

The screenshot shows a web-based configuration page for DMZ. At the top, there is a checkbox labeled 'Enable DMZ'. Below it is a table with three columns: 'Public', 'Client PC', and 'Computer Name'. The 'Public' column has two radio buttons: 'Dynamic IP' (selected) and 'Static IP'. The 'Dynamic IP' option has a dropdown menu showing 'Session 1'. The 'Client PC' column has an empty text input field. The 'Computer Name' column has a dropdown menu with '<< ----Select---- >>' and an 'Add' button to its right. Below the table is a section titled 'Current DMZ Table :'. It contains a table with five columns: 'NO', 'Computer Name', 'Public IP Address', 'Client PC IP Address', and 'Select'. Below this table are two buttons: 'Delete Selected' and 'Delete All'. At the bottom center of the form is a 'Save Settings' button.

<b>Enable DMZ</b>	Check/uncheck the box to enable/disable the device’s DMZ function.
<b>Public</b>	Select “Dynamic IP” or “Static IP” here.  For “Dynamic IP” select an Internet connection session from dropdown menu.  For “Static IP” enter the IP address that you want to map to a specific private IP address.
<b>Client PC</b>	Enter the private IP address that the internet IP address will be mapped to.
<b>Computer Name</b>	Select a computer name from the list and click “<<”

	to enter its IP address into the “Client PC” field (above).
<b>Add</b>	Click “Add” to add the client to the “Current DMZ Table”.

DMZ entries will be displayed in the table shown below:

Current DMZ Table :

NO	Computer Name	Public IP Address	Client PC IP Address	Select
				<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>

<b>Delete Selected / Delete All</b>	Delete selected or all entries from the table.
-------------------------------------	--

#### III-3-6-4. DoS

Denial-of-Service (DoS) is a common form of malicious attack against a network. The router’s firewall can protect against such attacks.

If you are not familiar with these functions, it is recommended you keep the default settings.

**DoS**

Ping of Death      5      Ping of Death Packet(S) Per      Second      Burst      5

Discard Ping From WAN

NMAP FIN / URG / PSH

Xmas tree

Another Xmas tree

Port Scan       Null scan

SYN / RST

SYN / FIN

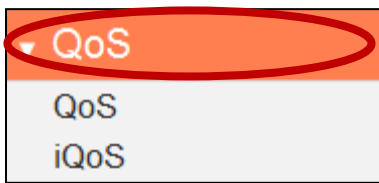
SYN (only unreachable ports)

Sync Flood      30      Packet(S) Per      Second      Burst      30

**Save Settings**

<b>Ping of Death</b>	Specify the frequency of ping of death packets which will trigger the router's DoS protection function.
<b>Discard Ping from WAN</b>	Check this box and the router will not answer ping requests from the Internet.
<b>Port Scan</b>	Intruders use "port scanners" to detect open Internet IP address ports. Check each type of port scan to prevent.
<b>Sync Flood</b>	Specify the frequency of sync flood packets which will trigger the DoS protection function.

### III-3-7. QoS



Quality of Service (QoS) is a feature to manage Internet bandwidth efficiently. Some applications require more bandwidth than others to function properly, and QoS allows you to ensure that sufficient bandwidth is available. Minimum or maximum bandwidth can be guaranteed for a specified application.



***QoS can improve the BR-6288ACL's performance. QoS is recommended to optimize performance for online gaming.***

#### III-3-7-1. QoS

Check/uncheck the box “Enable QoS” to enable/disable the QoS function. Click “Add” to open a new window and setup a QoS rule. The “Current QoS Table” displays all QoS rules.

A screenshot of the QoS configuration page. At the top left, the title 'QoS' is displayed. Below it is a checkbox labeled 'Enable QoS'. To the right, there are two input fields: 'Total Download Bandwidth' and 'Total Upload Bandwidth', both with a value of '0' and the unit 'kbits'. Below these fields is a section titled 'Current QoS Table :'. This section contains a table with five columns: 'Priority', 'Rule Name', 'Upload Bandwidth', 'Download Bandwidth', and 'Select'. Below the table are several buttons: 'Add', 'Edit', 'Delete Selected', 'Delete All', 'Move Up', and 'Move Down'. At the bottom center of the page is a 'Save Settings' button.

<b>Total Download Bandwidth</b>	Enter your total download bandwidth limit from your Internet service provider (ISP) in kbits.
<b>Total Upload Bandwidth</b>	Enter your total upload bandwidth limit from your Internet service provider (ISP) in kbits.
<b>Add</b>	Opens a new window to add a new QoS rule to the current QoS table.

## QoS

This page allows users to add/modify the QoS rule's settings.

Rule Name

Bandwidth   kbits

Local IP Address  -

Local Port Range

Remote IP Address  -

Remote Port Range

Traffic Type

Protocol


<b>Rule Name</b>	Enter a name for the QoS rule for reference/identification.
<b>Bandwidth</b>	<p>Set the bandwidth limits for the QoS rule:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">             Bandwidth : <input type="text" value="Download"/> <input type="text"/> Kbps <input type="text" value="guarantee"/> </div> <p style="text-align: center;">(1)                      (2)                      (3)</p> <ol style="list-style-type: none"> <li>1. Select "Download" or "Upload" for the QoS rule.</li> <li>2. Enter the bandwidth limit.</li> <li>3. Select whether the bandwidth is a "Guarantee" (minimum) or "Max" (maximum).</li> </ol>
<b>Local IP Address</b>	<p>Enter the IP address range to which the QoS rule will be applied.</p> <p>Enter a starting IP address in the left field and the end IP address in the right field to define a range of IP addresses; or enter an IP address in the left field only to define a single IP address.</p>



<b>Local Port Range</b>	Enter the port range to activate the QoS rule. Enter a single port number e.g. 110 or a range of port numbers e.g. 110-120
<b>Remote IP Address</b>	Enter the remote IP address range which will activate the QoS rule. Enter a starting IP address in the left field and the end IP address in the right field to define a range of IP addresses; or enter an IP address in the left field only to define a single IP address.
<b>Remote Port Range</b>	Enter the remote port range to activate the QoS rule. Enter a single port number e.g. 110 or a range of port numbers e.g. 110-120
<b>Traffic Type</b>	Select traffic type as an alternative to specifying a port range above.
<b>Protocol</b>	Select a "TCP" or "UDP" protocol type.
<b>Save</b>	Click 'add' button to add a new QoS rule (detailed instructions will be given below).

QoS rule entries will be listed in the "Current QoS Table" as shown below. Select a rule using the "Select" checkbox.

 **When using the "Edit" button only one rule can be selected each time.**

 **QoS rules will be processed in the order that they are listed i.e. the rule at the top of the list will be applied first, and then the second rule etc. The order can be adjusted using the "Move Up/Down" buttons.**


Current QoS Table :

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select
<span>Add</span> <span>Edit</span> <span>Delete Selected</span> <span>Delete All</span> <span>Move Up</span> <span>Move Down</span>				

<b>Edit</b>	Edit a selected rule.
<b>Delete Selected/ Delete All</b>	Delete selected or all entries from the table.
<b>Move Up/Down</b>	Move selected rule up or down the list.

### III-3-7-2. iQoS

iQoS is a more intuitive and automated tool to manage internet bandwidth than manually configuring the settings using QoS. For online gamers or users with bandwidth requirements for audio/video, iQoS is a useful function.

 ***iQoS cannot be used in conjunction with QoS and vice-versa. When one is enabled, the other is automatically disabled.***






**iQoS**

iQoS is a smart tool for bandwidth management. iQoS cannot be used simultaneously with QoS.

Enable iQoS

Total Download Bandwidth  kbits  
Total Upload Bandwidth  kbits

Current iQoS Table :

High		Low		
				
				

Settings have been saved. Please [click here to restart](#) the router and bring the new settings into effect.

Check/uncheck the box “Enable iQoS” to enable/disable the iQoS function, and then enter your bandwidth limits and arrange the network application icons in priority order in the “Current iQoS Table”. Icons with higher priority will be assigned bandwidth more efficiently for better performance.

<b>Total Download Bandwidth</b>	Enter your total download bandwidth limit from your Internet service provider (ISP) in kbits.
<b>Total Upload Bandwidth</b>	Enter your total upload bandwidth limit from your Internet service provider (ISP) in kbits.

The icons represent the following categories:



Internet Browsing



P2P/BT Downloads



FTP



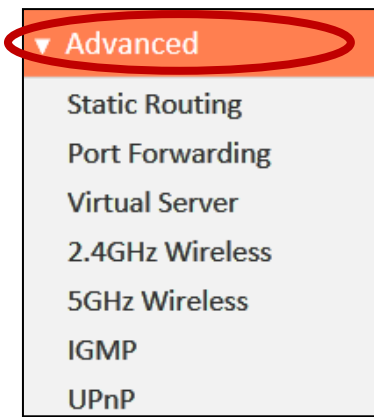
Multimedia



Online Gaming

The iQoS table is ordered left to right, high to low priority. Click a small icon below the table to insert it into the table, and click a large icon in the table to remove it. All spaces in the priority table must be filled.

### III-3-8. Advanced



Advanced features of the BR-6288ACL can be configured from the “Advanced” menu.

#### III-3-8-1. Static Routing

Static routing is a method of configuring path selection of routers, characterized by the absence of communication between routers regarding the current topology of the network. The opposite of static routing is dynamic routing, sometimes also referred to as adaptive routing.

You can configure static routing and manually add routes to the routing table shown below.

**Static Routing**

Enable Static Routing

Destination LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	LAN <span style="font-size: small;">▼</span>

Current Static Routing Table :

NO	Destination LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface	Select

<b>Enable Static Routing</b>	Check/uncheck the box to enable/disable static routing.
<b>Destination LAN IP</b>	Enter the destination network’s IP address.
<b>Subnet Mask</b>	Enter the subnet mask of the destination network.

<b>Default Gateway</b>	Enter the default gateway of the destination network.
<b>Hop Count</b>	Enter the hop count (the distance between destination network and this broadband router) here.
<b>Interface</b>	Enter the interface which leads to destination network.
<b>Add</b>	Add the route to the current static routing table.

Static Routing Table entries will be displayed in the table shown below:

Current Static Routing Table :

NO	Destination LAN IP	Subnet Mask	Default Gateway	Hop Count	Interface	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>						

<b>Delete Selected/ Delete All</b>	Delete selected or all entries from the table.
--	--

### III-3-8-2. Port Forwarding

This function allows you to redirect a single port or consecutive ports of an Internet IP address to the same port of a local IP address. The port number(s) of the Internet IP address and local IP address must be the same.

If the port number of the Internet IP address and local IP address is different, please use the “Virtual Server” function instead.

**Port Forwarding**

Enable Port Forwarding

Private IP	Computer Name	Type	Port Range	Comment
<input type="text"/>	<input type="button" value="←"/> <input type="text" value="---Select---"/> <input type="button" value="▼"/>	<input type="text" value="Both"/> <input type="button" value="▼"/>	<input type="text"/> - <input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>				

Current Port Forwarding Table :

NO	Computer Name	Private IP	Type	Port Range	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>						

<b>Private IP</b>	Enter the IP address of the computer on the local network.
<b>Computer Name</b>	Windows computers on the local network will be listed here – select a computer from the list and click << to automatically add the IP address to the “Private IP” field.
<b>Type</b>	Select the type of connection, “TCP”, “UDP” or “Both”.
<b>Port Range</b>	Input the starting port number in the left field, and input the ending port number in the right field. If you only want to redirect a single port number, only enter a port number in the left field.
<b>Comment</b>	Enter a comment for reference or identification.

Port Forwarding Table entries will be displayed in the table shown below:

Current Port Forwarding Table :

NO	Computer Name	Private IP	Type	Port Range	Comment	Select
						<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>

<b>Delete Selected/ Delete All</b>	Delete selected or all entries from the table.
--	--

### III-3-8-3. Virtual Server

This function allows you to set up an internet service on a local computer, without exposing the local computer to the internet. You can also build various sets of port redirection, to provide various internet services on different local computers via a single internet IP address.

**Virtual Server**

Enable Virtual Server

Private IP	Computer Name	Private Port	Type	Public Port	Comment
<input type="text"/>	<input type="button" value="⏪"/> <span style="border: 1px solid #ccc; padding: 2px;">----Select----</span> <input type="button" value="▼"/>	<input type="text"/>	<span style="border: 1px solid #ccc; padding: 2px;">Both</span> <input type="button" value="▼"/>	<input type="text"/>	<input type="text"/>

Current Virtual Server Table :

NO	Computer Name	Private IP	Private Port	Type	Public Port	Comment	Select

<b>Private IP</b>	Specify the IP address of the computer on your local network.
<b>Computer Name</b>	Select the name of a Windows computer from the drop-down menu and click <input type="button" value="⏪"/> to auto-input its IP address in the "Private IP" field.
<b>Private Port</b>	Specify the private port you wish to use on the computer in your local network.
<b>Type</b>	Select the type of Internet Protocol.
<b>Public Port</b>	Specify a public port to access the computer on your local network.
<b>Comment</b>	Enter a comment for reference or identification.

Current Virtual Table entries will be displayed in the table shown below:

Current Virtual Server Table :

NO	Computer Name	Private IP	Private Port	Type	Public Port	Comment	Select

**Delete Selected/  
Delete All**

Delete selected or all entries from the table.

### III-3-8-4. 2.4GHz Wireless

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

**2.4GHz Wireless**

Wireless Module	Enable
Fragment Threshold	<input type="text" value="2346"/> (256-2346)
RTS Threshold	<input type="text" value="2347"/> (0-2347)
Beacon Interval	<input type="text" value="100"/> (20-1024 ms)
DTIM Period	<input type="text" value="3"/> (1-10)
Data Rate	Auto ▾
N Data Rate	Auto ▾
Channel Width	<input checked="" type="radio"/> Auto 20/40 MHz <input type="radio"/> 20 MHz
Preamble Type	<input checked="" type="radio"/> Short Preamble <input type="radio"/> Long Preamble
CTS Protect	<input type="radio"/> Auto <input type="radio"/> Always <input checked="" type="radio"/> None
Tx Power	<input type="text" value="100 %"/> ▾
WMM	<input checked="" type="radio"/> Auto

[Save Settings](#)

<b>Fragment Threshold</b>	Set the Fragment threshold of the wireless radio. The default value is 2346.
<b>RTS Threshold</b>	Set the RTS threshold of the wireless radio. The default value is 2347.
<b>Beacon Interval</b>	Set the beacon interval of the wireless radio. The default value is 100.
<b>DTIM Period</b>	Set the DTIM period of wireless radio. The default value is 3.
<b>Data Rate</b>	Set the wireless data transfer rate. The default is set to Auto.
<b>N Data Rate</b>	Set the data rate of 802.11n. The default is set to Auto.



<b>Channel Width</b>	Select wireless channel width (bandwidth used by wireless signals from the device) – the recommended value is Auto 20/40MHz.
<b>Preamble Type</b>	Set the wireless radio preamble type. The default value is “Short Preamble”.
<b>CTS Protect</b>	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to “Auto”.
<b>Tx Power</b>	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
<b>WMM</b>	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP) and others. When WMM is enabled, the device will prioritize different kinds of data and give higher priority to applications which require instant responses for better performance.

### III-3-8-5. 5GHz Wireless

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

**5GHz Wireless**

Wireless Module  Enable

Fragment Threshold  (256-2346)

RTS Threshold  (0-2347)

Beacon Interval  (20-1024 ms)

DTIM Period  (1-10)

Data Rate

N Data Rate

Channel Width  20/40/80 MHz  20/40 MHz  20 MHz

Preamble Type  Short Preamble  Long Preamble

CTS Protect  Auto  Always  None

Tx Power

WMM  Auto

[Save Settings](#)

<b>Fragment Threshold</b>	Set the Fragment threshold of the wireless radio. The default value is 2346.
<b>RTS Threshold</b>	Set the RTS threshold of the wireless radio. The default value is 2347.
<b>Beacon Interval</b>	Set the beacon interval of the wireless radio. The default value is 100.
<b>DTIM Period</b>	Set the DTIM period of wireless radio. The default value is 3.
<b>Data Rate</b>	Set the wireless data transfer rate. The default is set to Auto.
<b>N Data Rate</b>	Set the data rate of 802.11n. The default is set to Auto.

<b>Channel Width</b>	Select wireless channel width (bandwidth used by wireless signals from the device) – the recommended value is 20/40/80MHz.
<b>Preamble Type</b>	Set the wireless radio preamble type. The default value is “Short Preamble”.
<b>CTS Protect</b>	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to “Auto”.
<b>Tx Power</b>	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
<b>WMM</b>	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP) and others. When WMM is enabled, the device will prioritize different kinds of data and give higher priority to applications which require instant responses for better performance.

### III-3-8-6. IGMP

IGMP is a communications protocol used to establish multicast group memberships. It allows for a more efficient use of resources and better performance for applications such as IPTV video streaming.

IGMP

IGMP Snooping  Enable  Disable

IGMP Proxy  Enable  Disable

Save Settings

<b>IGMP Snooping</b>	IGMP snooping monitors traffic between hosts and multicast routers to facilitate bandwidth conservation. Select enable or disable.
<b>IGMP Proxy</b>	IGMP proxy enables intelligent multicast forwarding based on IGMP snooping information. Select enable or disable.



***It is recommended to set “IGMP Snooping” and “IGMP Proxy” to “Enable”.***

### III-3-8-7. UPnP

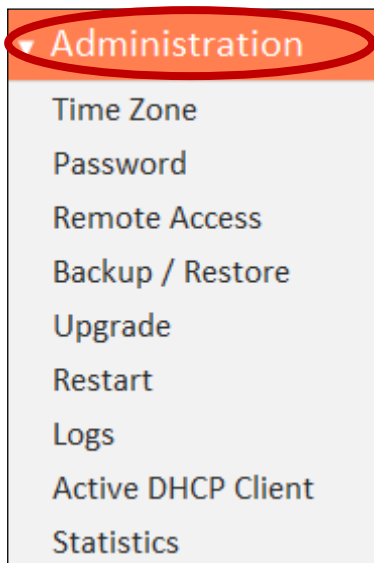
Universal plug-and-play (UPnP) is a set of networking protocols which enables network devices to communicate and automatically establish working configurations with each other. Select “Enable” or “Disable”.

UPnP

UPnP Feature  Enable  Disable

Save Settings

### III-3-9. Administration



Various administrative functions can be accessed from the “Administration” menu.

#### III-3-9-1. Time Zone

<b>Set Time Zone</b>	Select the time zone of your country or region.
<b>Time Server Address</b>	The travel router supports NTP (Network Time Protocol) for automatic time and date setup. Input the host name of the IP server manually.
<b>Daylight Saving</b>	If your country/region uses daylight saving time, please check the “Enable Function” box, and select the start and end date.

### III-3-9-2. Password

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.



***Please make a note of the new password. In the event that you forget the password and are unable to login to the browser based configuration interface, see [II-7. Reset to factory default settings](#) for how to reset the device.***

Password

Current Password

New Password

Confirmed Password

<b>Current Password</b>	Enter your current password.
<b>New Password</b>	Enter your new password.
<b>Confirmed Password</b>	Confirm your new password.

### III-3-9-3. Remote Access

Check “Enabled” to enable the remote access feature and then enter the appropriate values.

Remote Access

Host IP Address

Port

Enabled

[Save Settings](#)

<b>Host IP Address</b>	Specify the IP address which is allowed remote access.
<b>Port</b>	Specify a port number (0–65535) used for remote access.

### III-3-9-4. Backup/Restore

Backup / Restore

Backup Settings

Restore Settings

Restore to Factory Default

<b>Backup Settings</b>	Click "Save" to save the current settings on your computer as config.bin file.
<b>Restore Settings</b>	Click "Browse" to find a previously saved config.bin file and then click "Upload" to replace your current settings.
<b>Restore to Factory Default</b>	Click "Reset" to restore settings to the factory default. A pop-up window will appear and ask you to confirm and enter your log in details. Enter your username and password and click "Ok". See below for more information.

### III-3-9-5. Upgrade

The upgrade page allows you to upgrade the system firmware to a more recent version. You can download the latest firmware from the Edimax website. After the upgrade, the system will restart.



***Do not switch off or disconnect the device during a firmware upgrade, as this could damage the device. It is recommended that you use a wired Ethernet connection for a firmware upgrade.***

Upgrade