BR-6288ACL V2

User Manual

07-2019 / v1.0

Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd., Neihu Dist., Taipei City, Taiwan
Email: support@edimax.com.tw

Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3444 De La Cruz Blvd., Santa Clara, CA 95054, USA
Live Tech Support: 1(800) 652-6776
Email: support@edimax.com

CONTENTS

I. Product Information 1

I-1. Package Contents 1

I-2. LED Status 2

I-3. Back Panel 3

I-4. RJ-45 Splitter Cable 4

I-5. Wi-Fi Power Switch 5

I-6. Safety Information 6

II. Installation 7

II-1. Ranger Extender Mode 10

II-2. Access Point Mode 16

II-3. Wi-Fi Router Mode 21

II-4. Wireless Bridge Mode 26

II-5. WISP Mode 32

II-6. WPS Setup 40

II-7. Reset to Factory Default Settings 40

III. Browser Based Configuration Interface 41

III-1. Login 41

III-2. Save Settings 43

III-3. Main Menu 44

III-3-1. Status 45

III-3-2. Setup Wizard 46

III-3-3. Internet/WISP 48

III-3-3-1. WAN Setup 49

III-3-3-1-1. Dynamic IP 49

III-3-3-1-2. Static IP 51

III-3-3-1-3. PPPoE 53

III-3-3-1-4. PPTP 55

III-3-3-1-5. L2TP 58

III-3-3-2. DDNS 60

III-3-4. LAN 62

III-3-5. 2.4GHz Wireless & 5GHz Wireless 65

III-3-5-1. Basic 65

III-3-5-1-1. Disable 69

III-3-5-1-2. WEP 70

III-3-5-1-3. WPA Pre-Shared Key 71

III-3-5-1-4. WPA Radius 72

III-3-5-2. Guest/ Multiple SSID 73

III-3-5-3. WPS 76

III-3-5-4. Access Control 77

III-3-5-5. Schedule 79

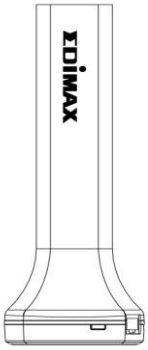
III-3-6. Firewall 81
III-3-6-1. URL Blocking 81
III-3-6-2. Access Control 83
III-3-6-3. DMZ 87
III-3-6-4. DoS 88
III-3-7. QoS (Quality of Service) 90
III-3-7-1. QoS 90
III-3-7-2. iQoS 93
III-3-8. Advanced 95
III-3-8-1. Static Routing 95
III-3-8-2. Port Forwarding 96
III-3-8-3. Virtual Server 98
III-3-8-4. 2.4GHz Wireless 99
III-3-8-5. 5GHz Wireless 101
III-3-8-6. IGMP 103
III-3-8-7. UPnP 103
III-3-9. Administration 104
III-3-9-1. Time Zone 104
III-3-9-2. Password 105
III-3-9-3. Remote Access 106
III-3-9-4. Backup/Restore 107
III-3-9-5. Upgrade 107
III-3-9-6. Restart 108
III-3-9-7. Logs 108
III-3-9-8. Active DHCP Client 109
III-3-9-9. Statistics 109
IV. Appendix 110
IV-1. Configuring your IP address 110
IV-1-1. How to check that your computer uses a dynamic IP address 111
IV-1-1-1. Windows Vista 111
IV-1-1-2. Windows 7 113
IV-1-1-3. Windows 8 116
IV-1-1-4. Mac OS 120
IV-1-2. How to modify the IP address of your computer 122
IV-1-2-1. Windows Vista 122
IV-1-2-2. Windows 7 124
IV-1-2-3. Windows 8 127
IV-1-2-4. Mac 131
IV-1-3. How to Find Your Network Security Key 134
IV-1-3-1. Windows 7 & Vista 134
IV-1-3-2. Mac 136
IV-1-4. How to Find Your Router's IP Address 139

IV-1-4-1. Windows Vista & 7 139
IV-1-4-2. Windows 8 141
IV-1-4-3. Mac 144
IV-2. Connecting to a Wi-Fi network 146
IV-3. Troubleshooting 148
V. Glossary 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):

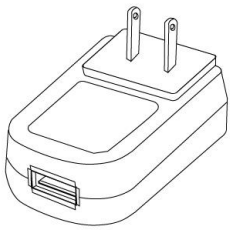


BR-6288ACL V2

RJ-45 Splitter Cable

USB Cable

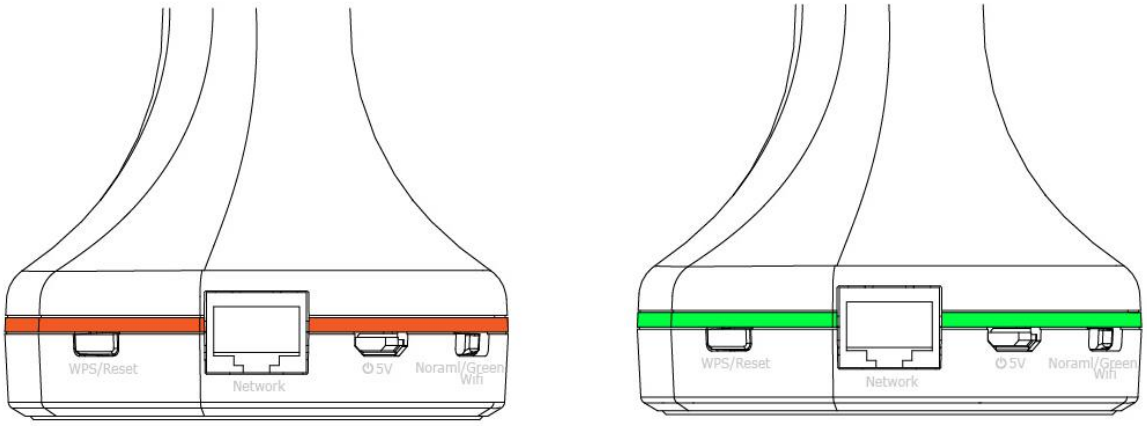
Quick Installation Guide



Power Adapter

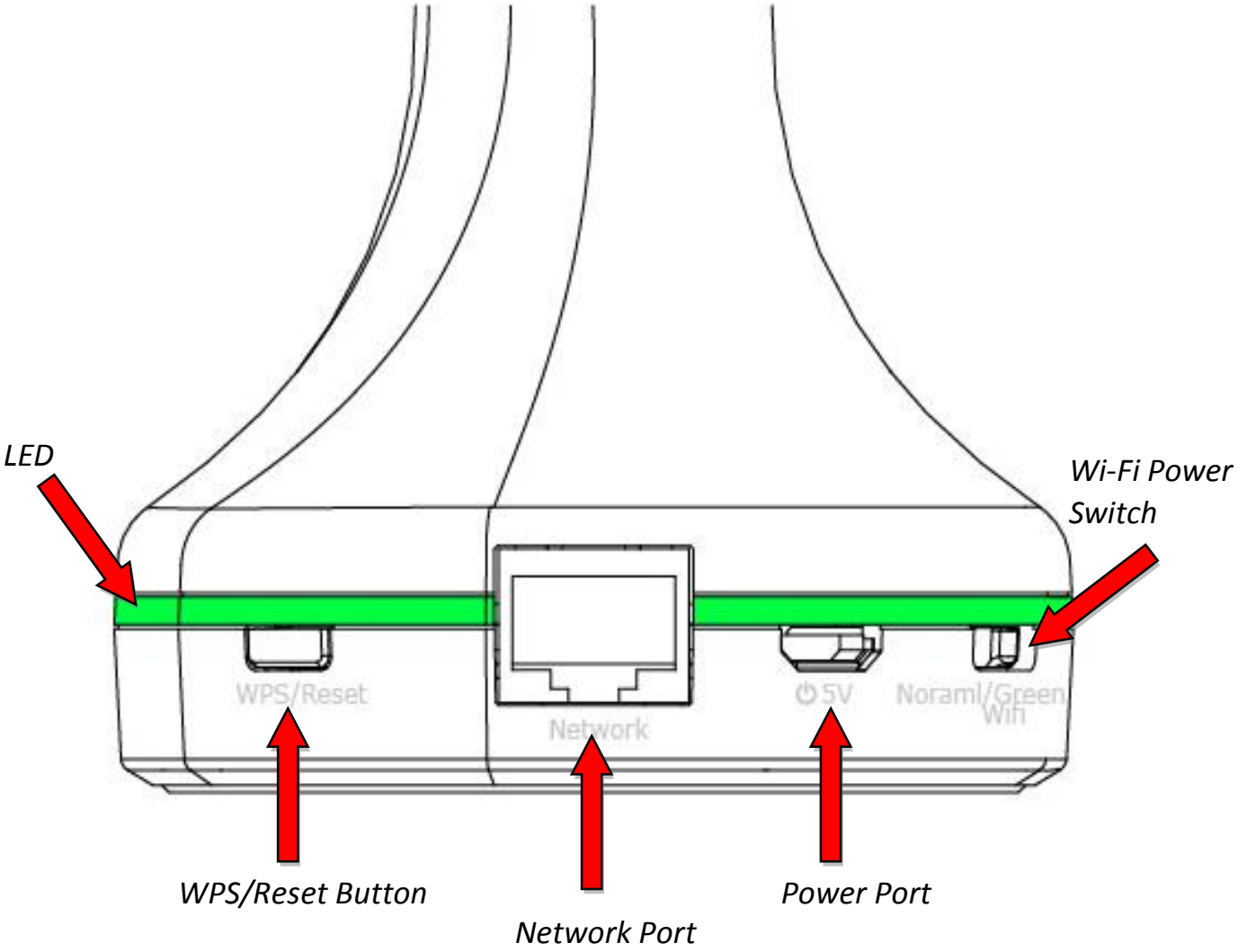
Download product material here
https://www.edimax.com/download/de

I-2. LED Status



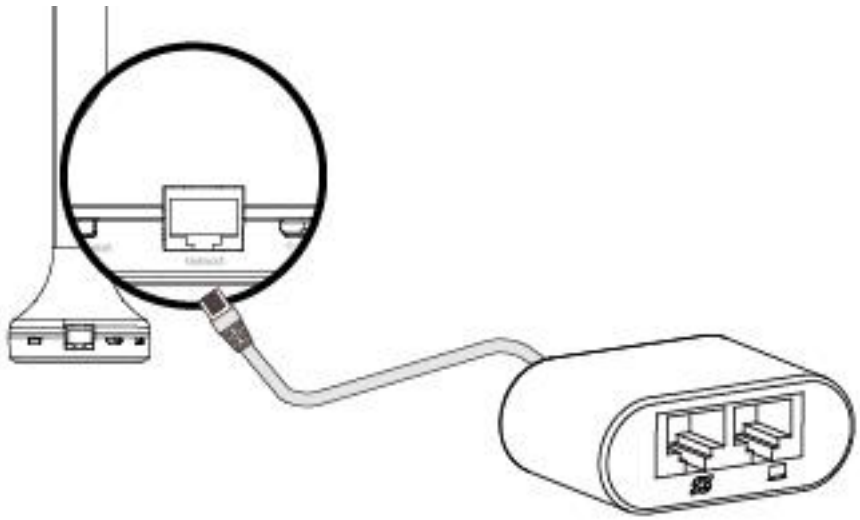
LED Color	LED Status	Description
Orange/Red	On	Product is starting up.
	Flashing (Slow)	No Internet connection.
	Flashing (Fast)	Resetting to factory default status or Wi-Fi Protected Setup (WPS) is active.
Light Green	On	Internet is connected and Wi-Fi is full power.
Dark Green	On	Internet is connected and Wi-Fi is in green mode (75% power).
Off	Off	BR-6288ACL V2 is off.

I-3. Back Panel



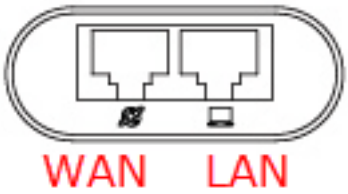
I-4. RJ-45 Splitter Cable

The BR-6288ACL V2 includes an RJ-45 splitter cable in the package contents. This plugs into the “Network” port of the BR-6288ACL V2 and splits the port into two separate Ethernet ports – providing two ports instead of one, as shown below.

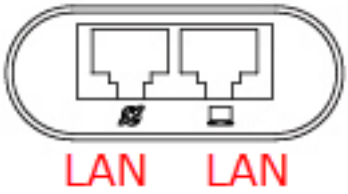


In **Wi-Fi router** mode, one port is the **WAN** (Network) port. The **WAN** port connects directly to your modem.

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).

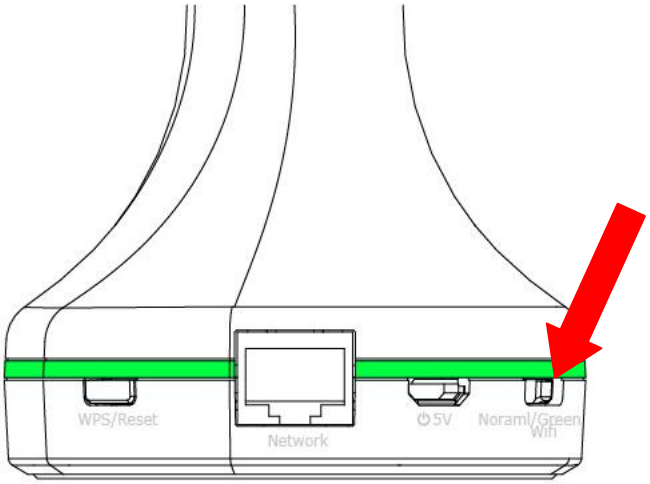


In **other** modes, both ports function as LAN ports for wired network devices (e.g. computers, games consoles etc.), and in **access point** mode also for connecting to your router.



I-5. Wi-Fi Power Switch

After setup you can use the Wi-Fi power switch to adjust the strength of the BR-6288ACL V2's wireless radio if you wish. Normal mode uses full 100% wireless power while green mode uses 75% 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 V2.

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.

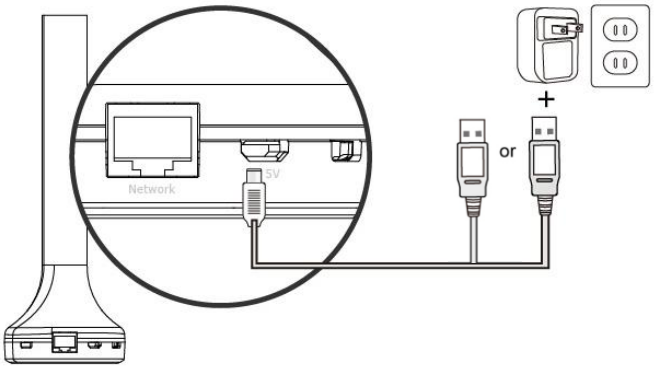
7. There are no user-serviceable parts inside the device. If you experience problems with the device, please contact your dealer of purchase and ask for help.

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.

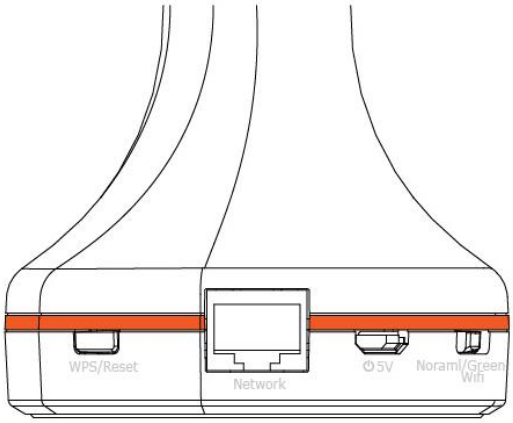
II. Installation

1. Plug in the BR-6288ACL V2 using the included power adapter and/or USB cable.

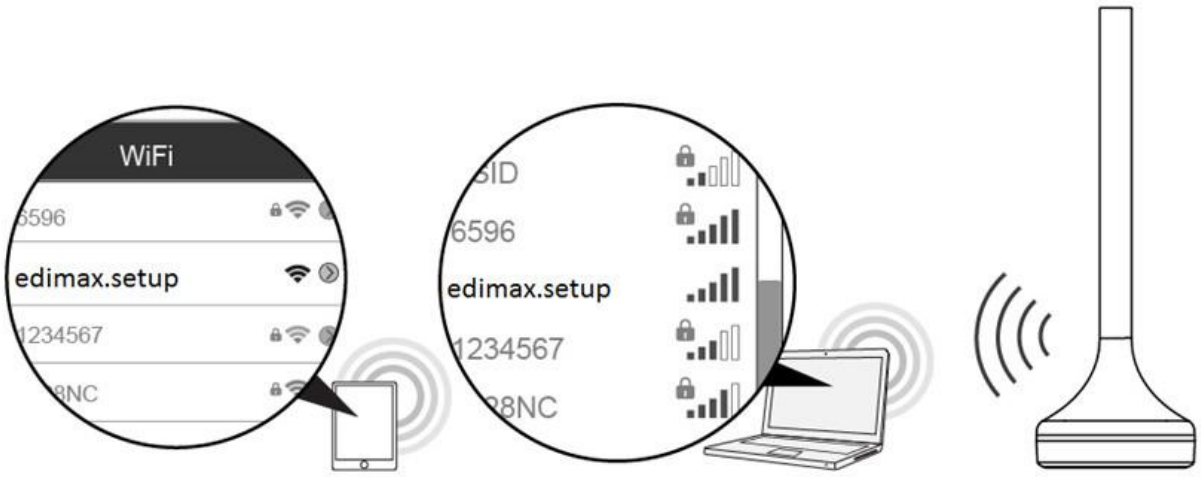
The BR-6288ACL V2 requires 1.2 A of current – please ensure that your USB port can provide sufficient power. If not, use the 5V DC adapter.



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



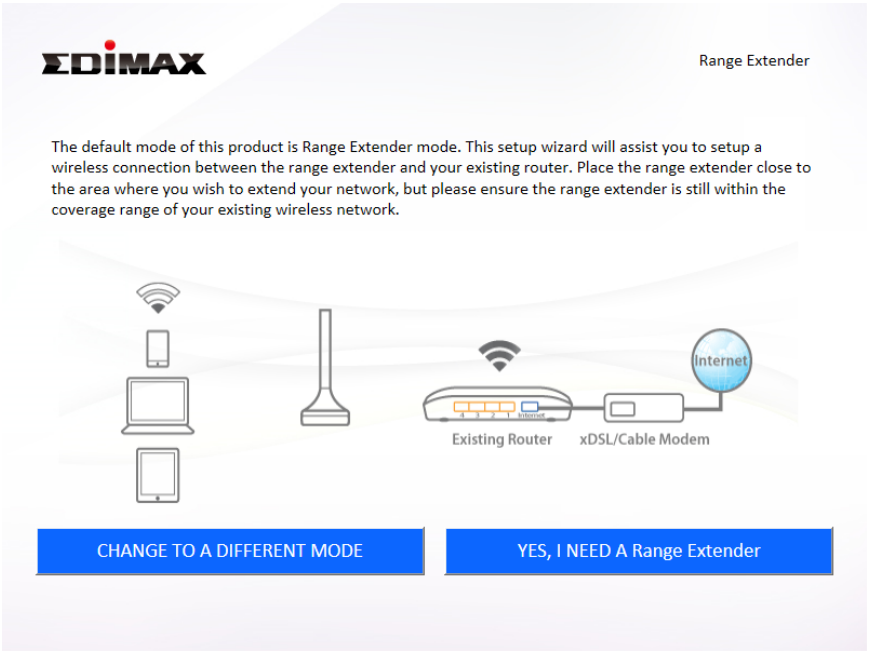
3. Use a Wi-Fi device (e.g. computer, tablet, smartphone) to search for a Wi-Fi network with the SSID “edimax.setup” and connect to it.



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 V2 in its default range extender mode or in a different mode.

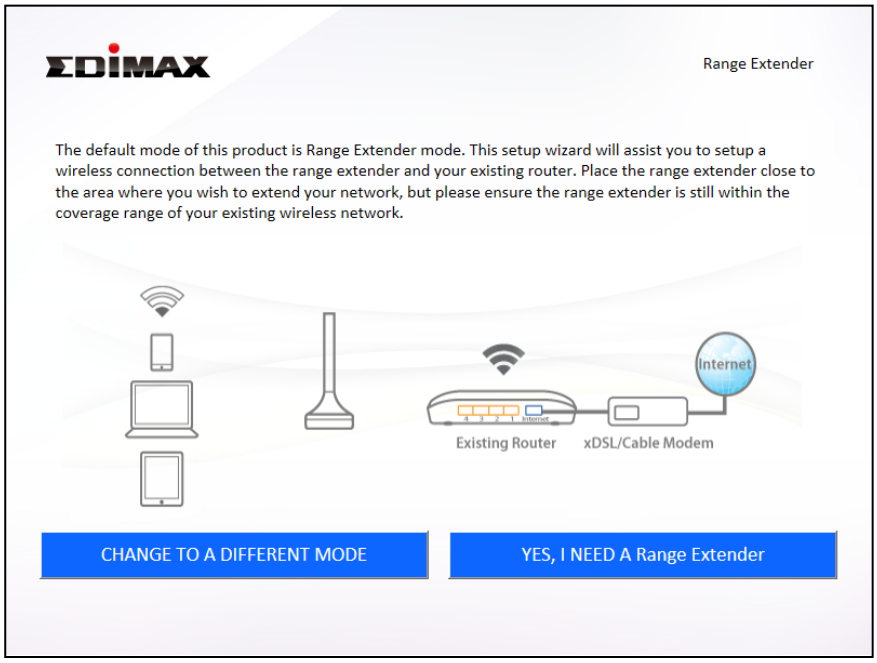


The BR-6288ACL V2's five available modes are outlined below:

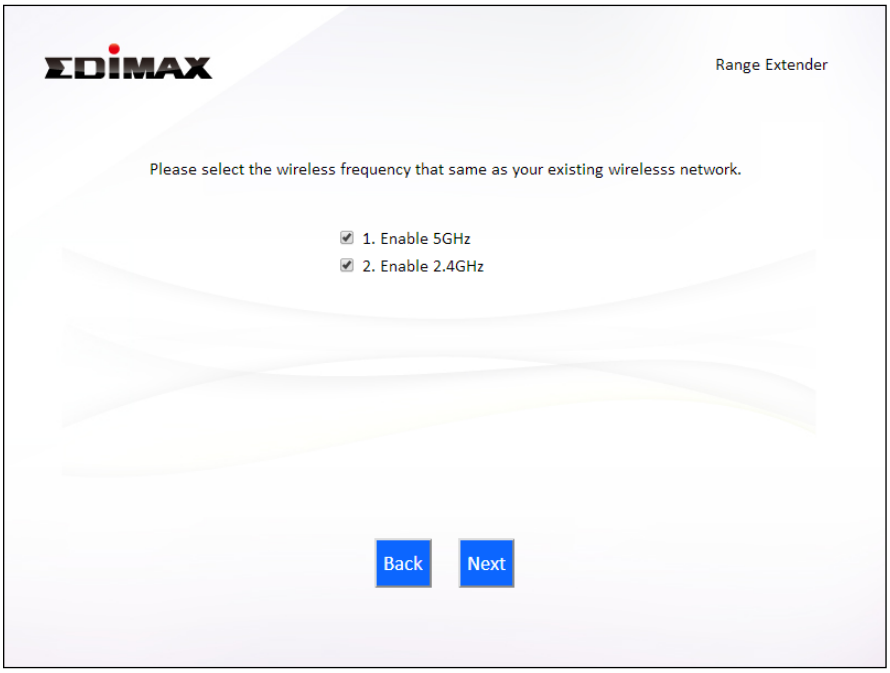
Range Extender Mode	*The device connects wirelessly to your existing 2.4GHz and/or 5GHz network and repeats the wireless signal(s).*
Wi-Fi Router Mode	*The device connects to your **modem** and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.*
Access Point Mode	*The device connects to an existing **router** via Ethernet cable and provides 2.4GHz and/or 5GHz Internet (wireless and Ethernet) access for your network devices.*
Wireless Bridge Mode	*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.*
WISP Mode	*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.*

II-1. Ranger Extender Mode

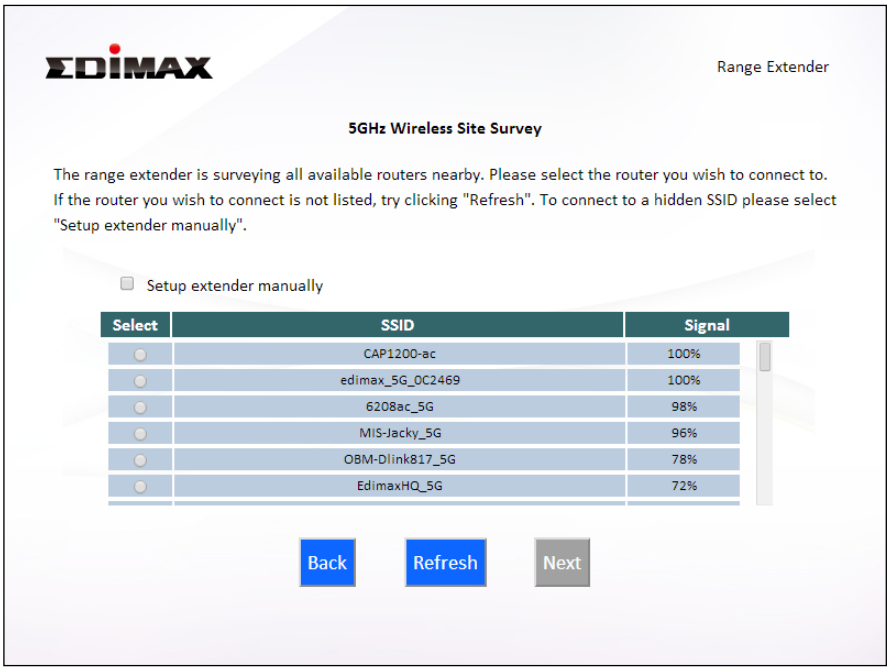
1. Please ensure your BR-6288ACL V2 is within Wi-Fi range of your existing wireless router. Click “Next” to continue.



2. 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”.

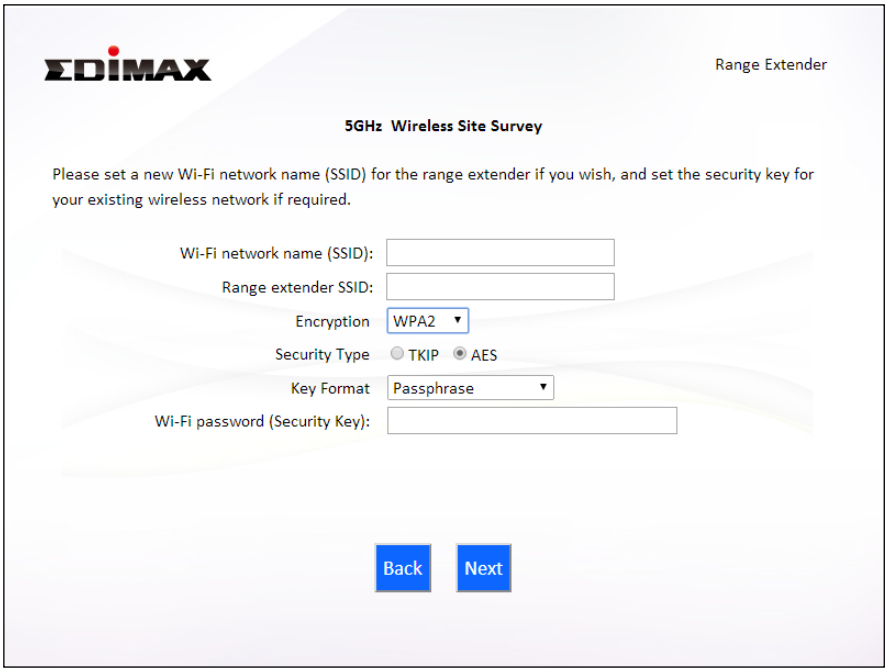


3. Select the Wi-Fi network name (SSID) which you wish to connect to for the specified frequency and click “Next” to continue.

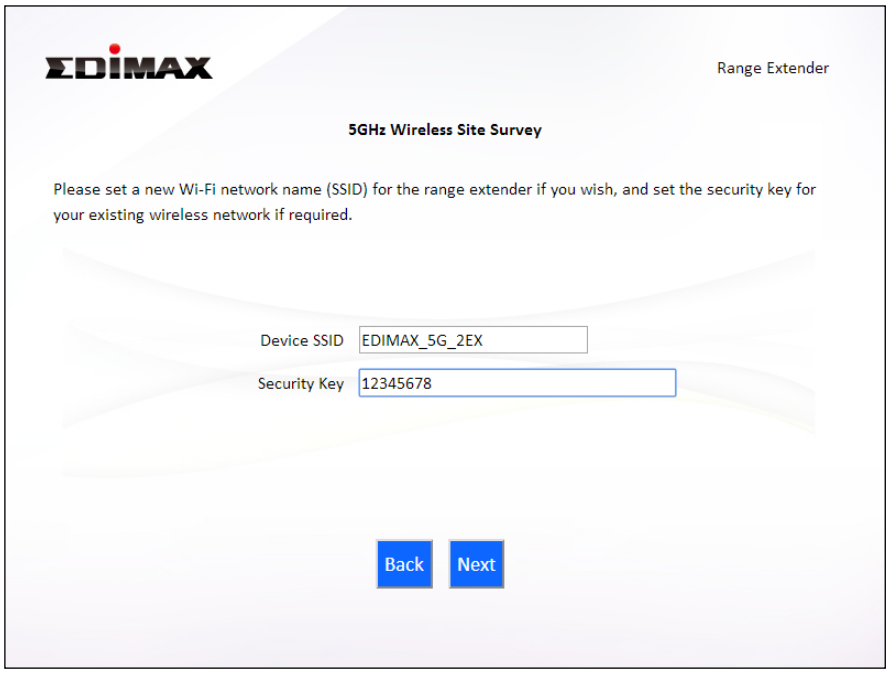


If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.

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

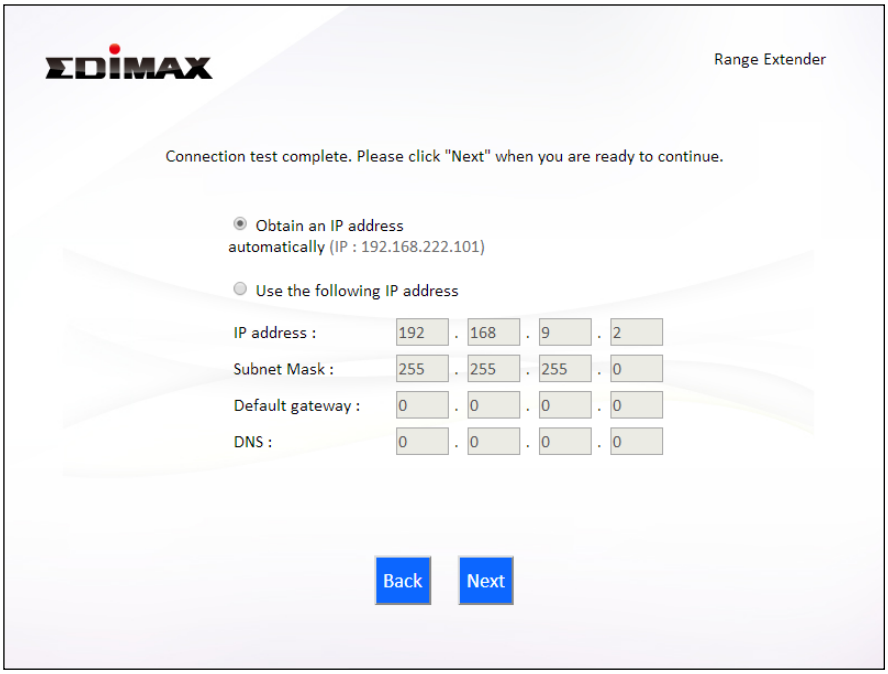


4. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.



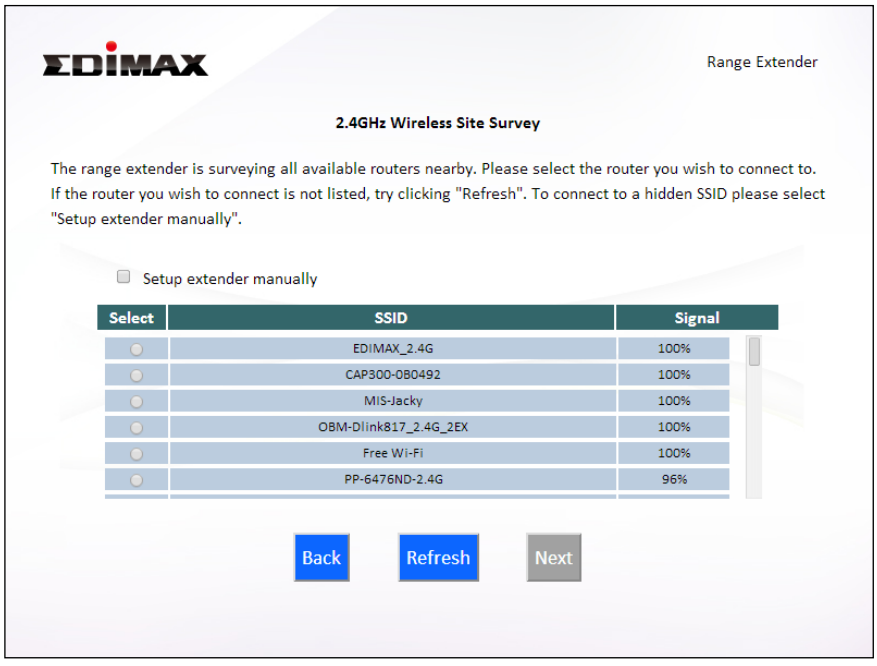
5. Wait a moment while the BR-6288ACL V2 tests the wireless connection.

6. Select “Obtain an IP address automatically” or “Use the following IP address” for your BR-6288ACL V2. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

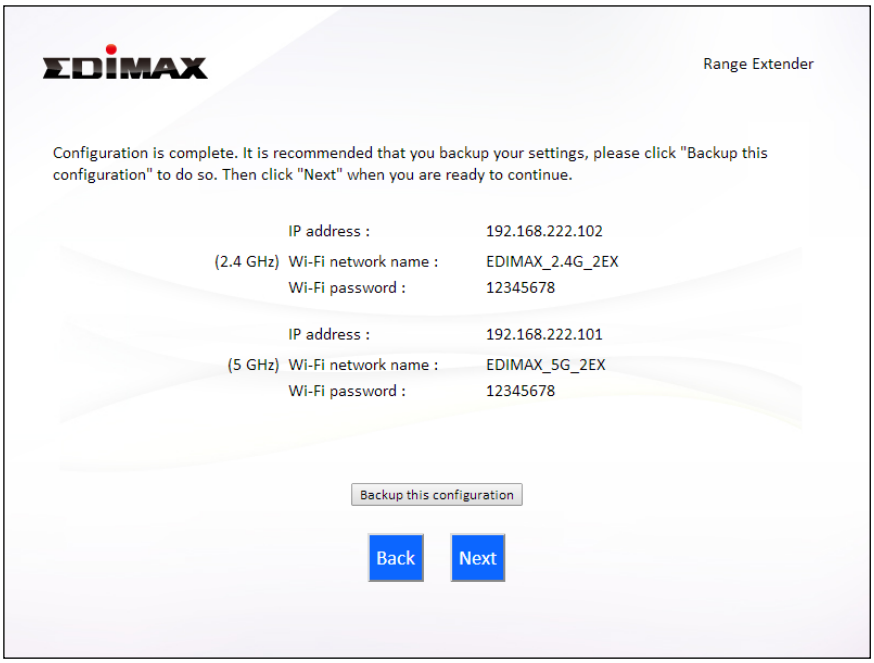


“Obtain an IP address automatically” is the recommended setting for most users. The IP address will be displayed in brackets.

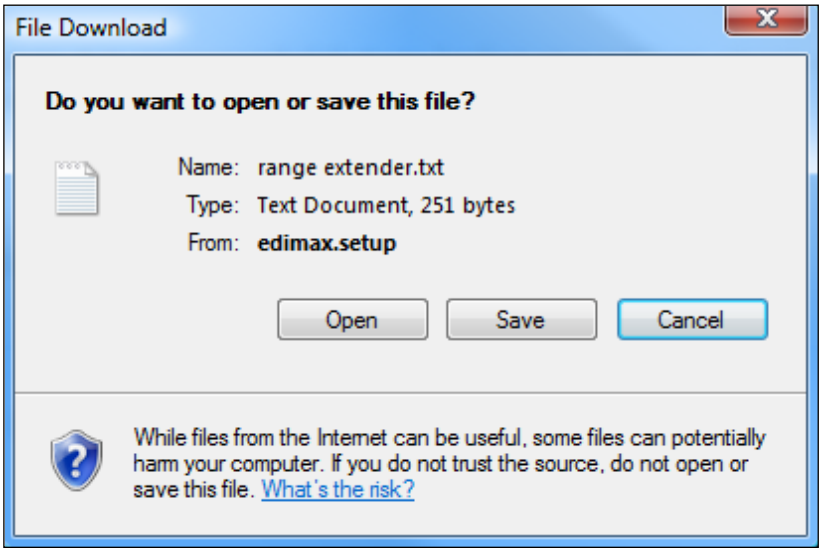
7. If you selected to use both 2.4GHz and 5GHz wireless frequencies in step 3, then repeat steps 4 – 7 for the 2.4GHz wireless frequency.



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.

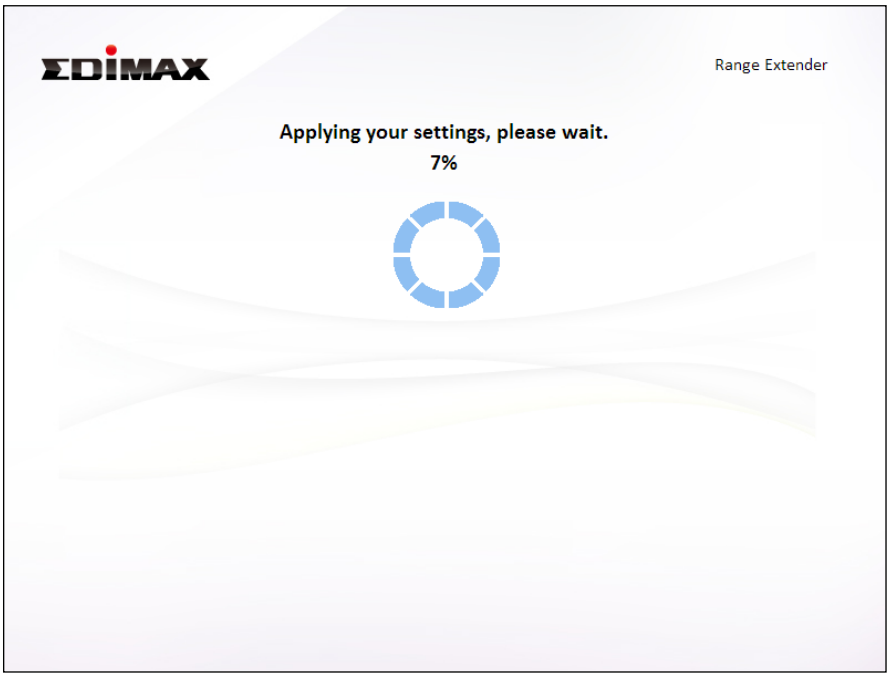


The device will use the same wireless password/security key as the existing wireless network.

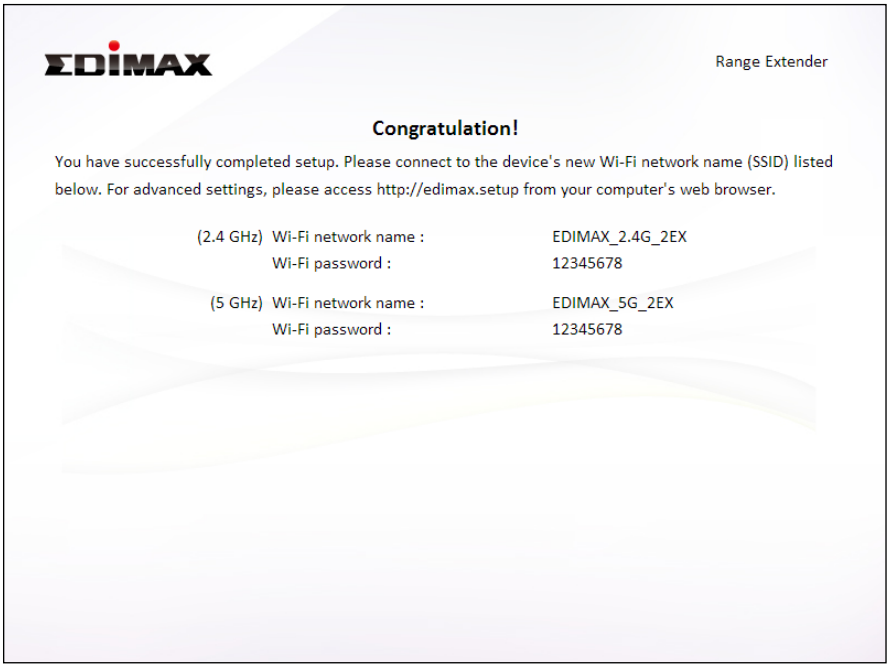


If you wish to backup the BR-6288ACL V2’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.

9. Please wait a moment until the BR-6288ACL V2 is ready.



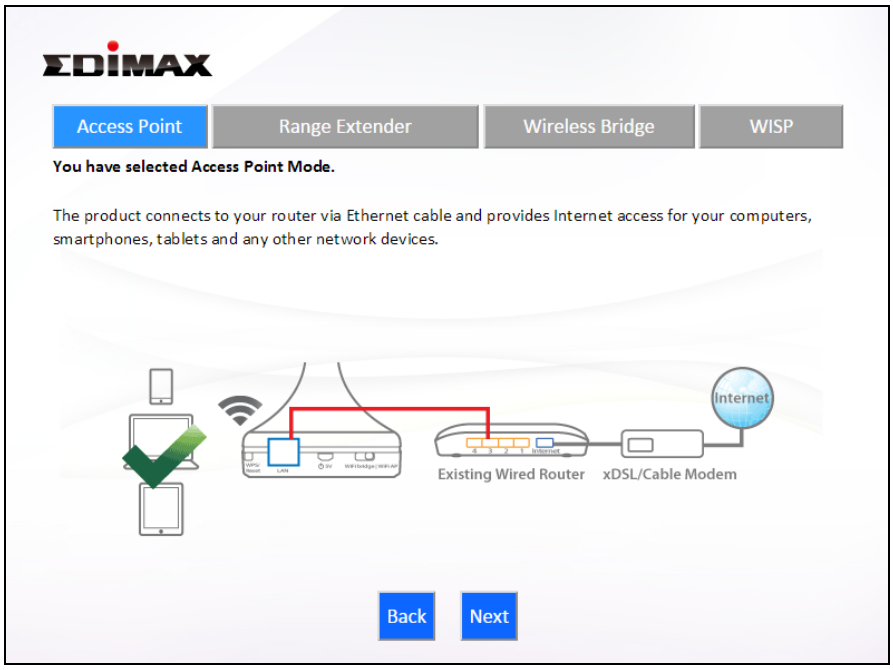
10. A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.



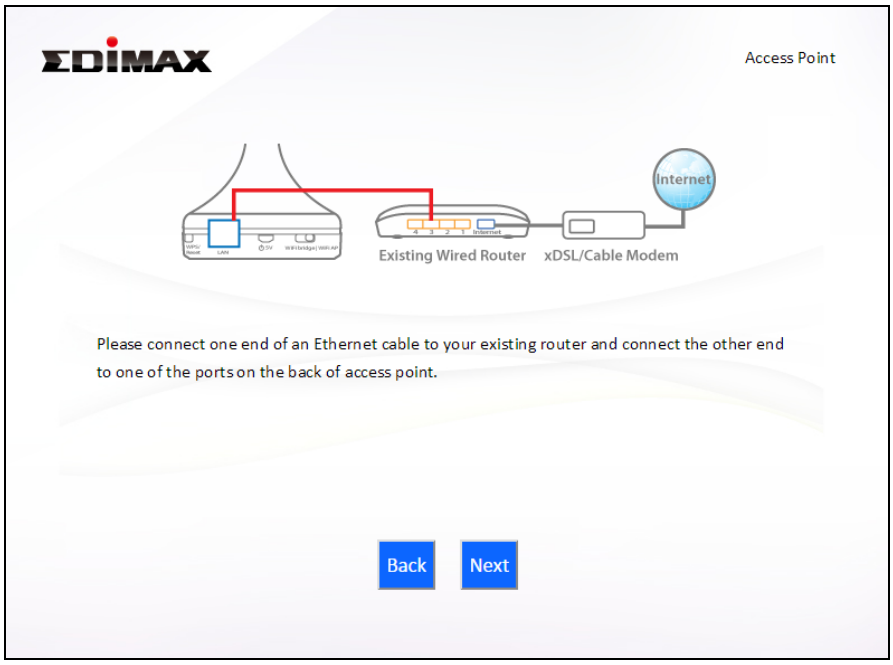
11. The BR-6288ACL V2 is working and ready for use. Refer to IV-2. Connecting to a Wi-Fi network if you require more guidance.

II-2. Access Point Mode

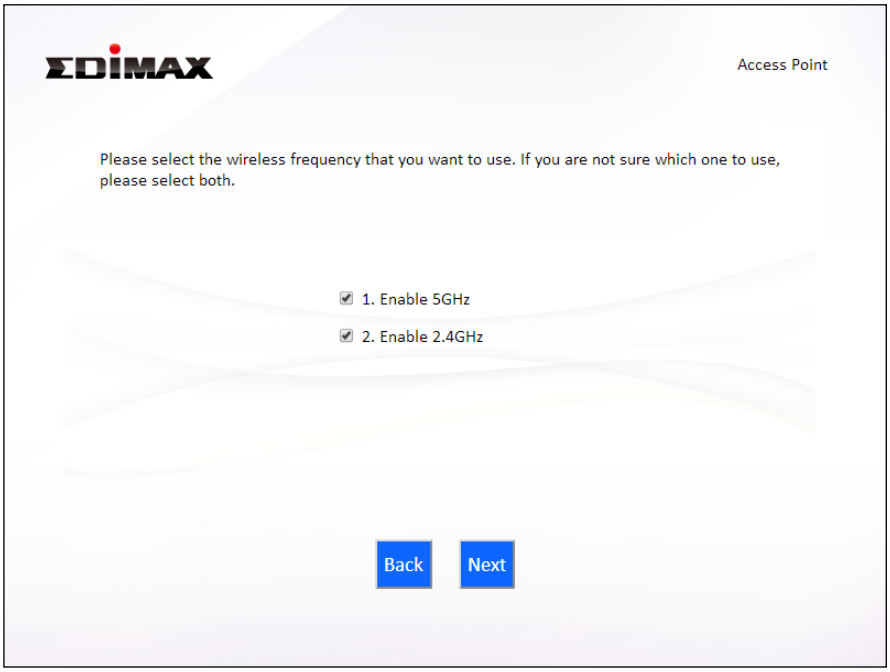
1. Select “Access Point” from the top menu and click “Next”.



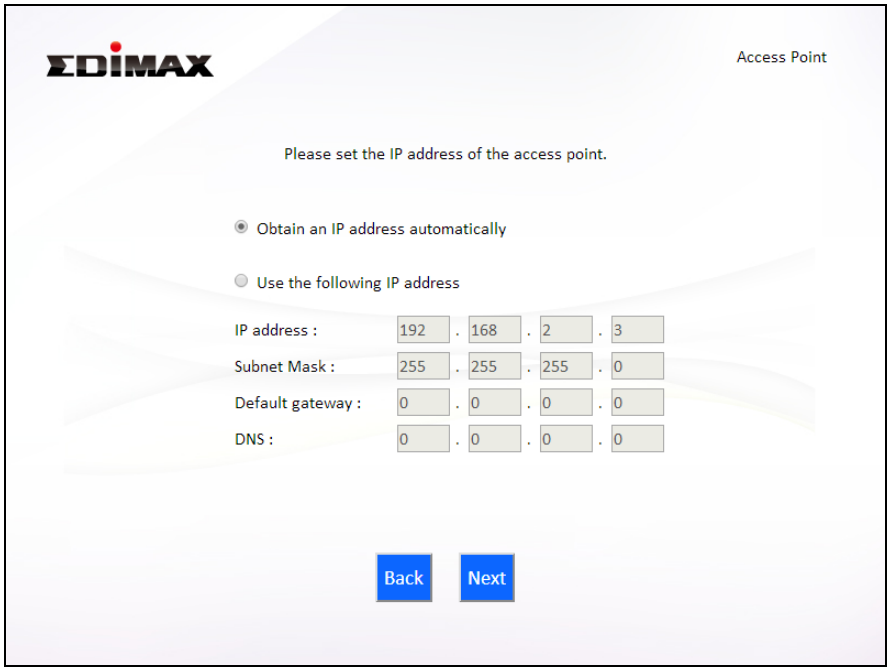
2. Connect the network port of your BR-6288ACL V2 to the LAN port of your existing router using an Ethernet cable, then click “Next”.



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

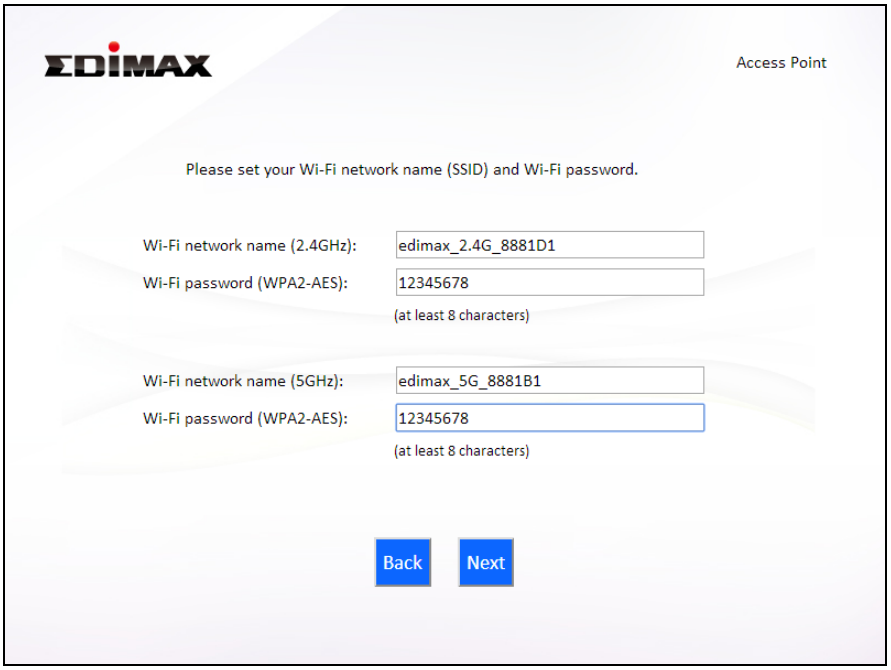


4. Select "Obtain an IP address automatically" or "Use the following IP address" for your BR-6288ACL V2. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click "Next" to proceed to the next step.

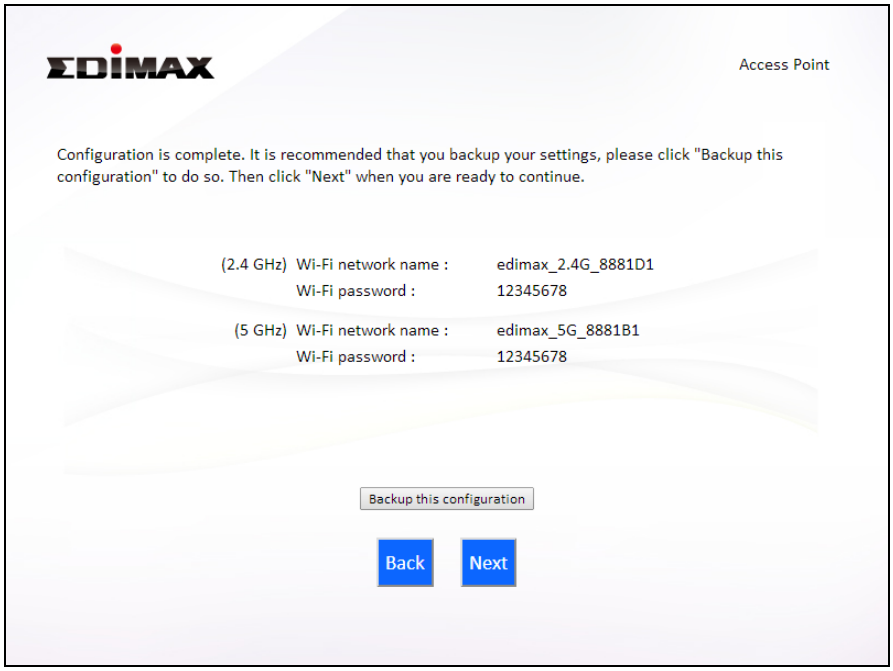


"Obtain an IP address automatically" is the recommended setting for most users. For more guidance on static IP addresses, please refer to IV-1. Configuring your IP address.

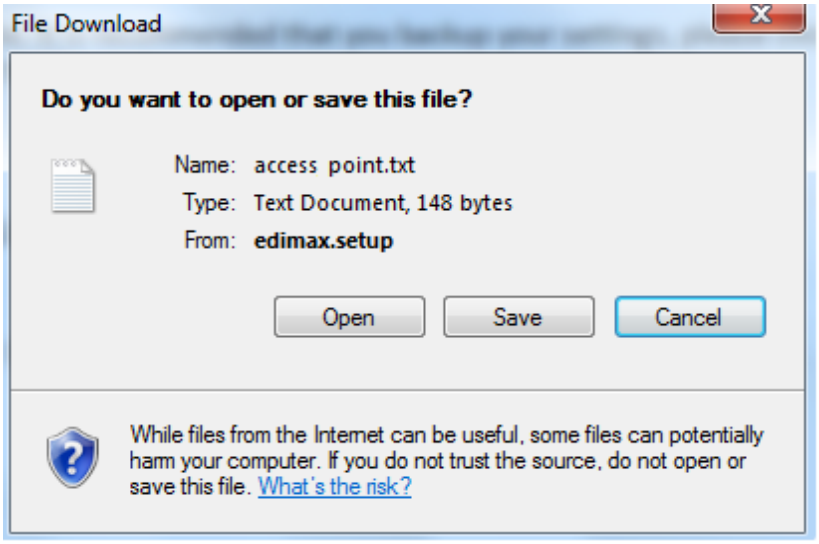
5. Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.



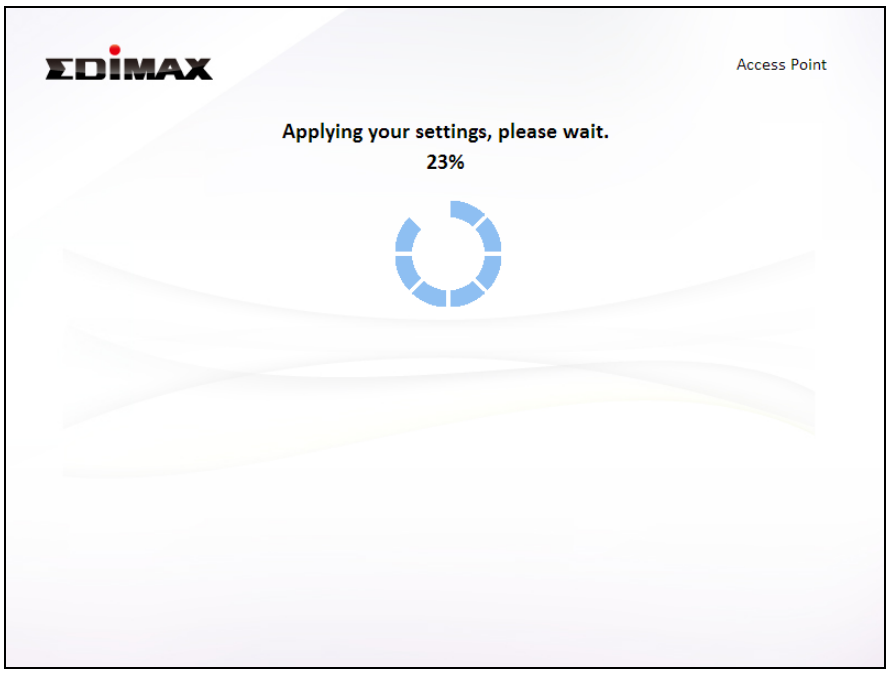
6. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



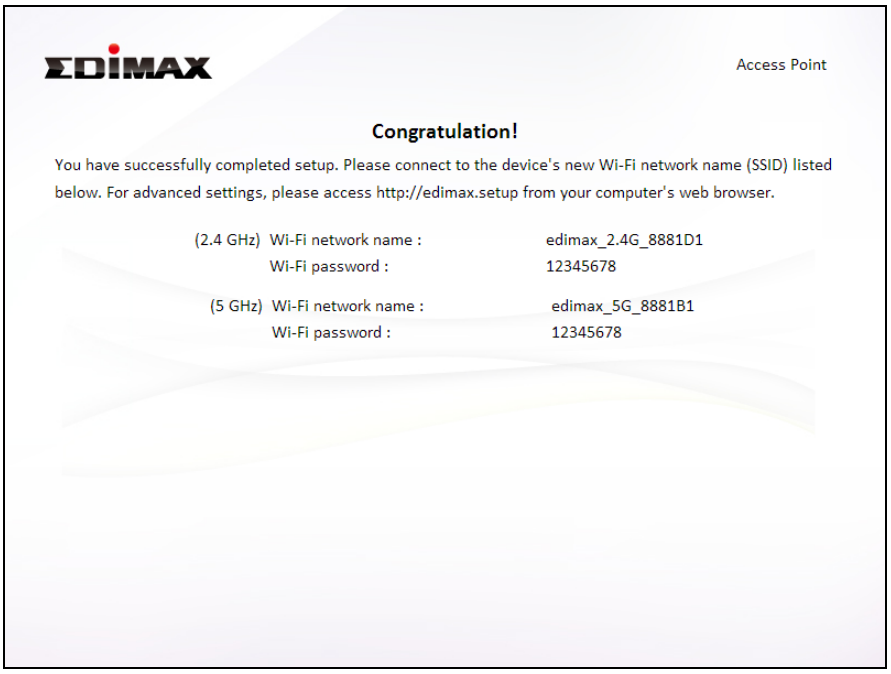
If you wish to backup the device’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.



7. Please wait a moment until the BR-6288ACL V2 is ready.



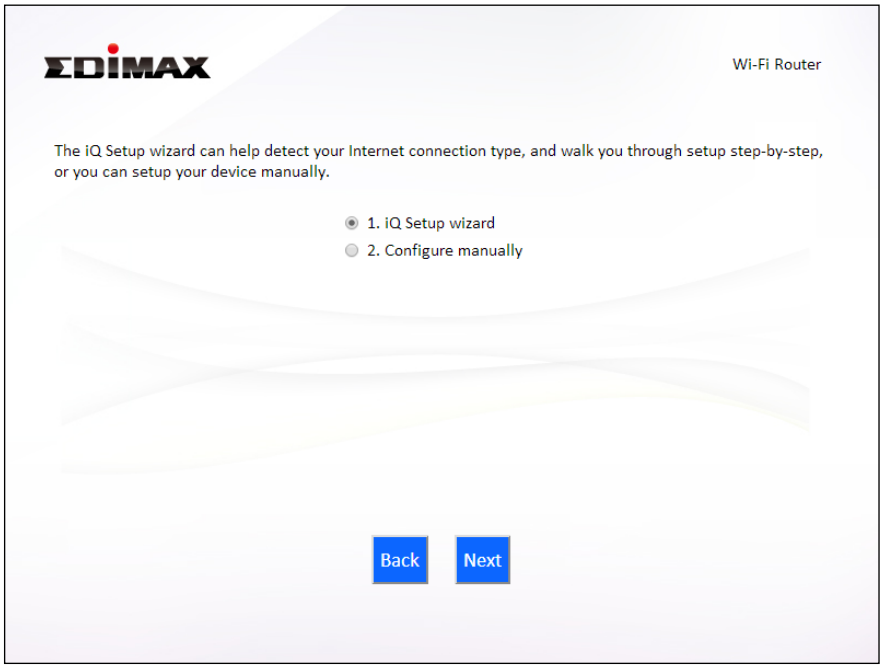
8. A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.



9. The BR-6288ACL V2 is working and ready for use. Refer to **IV-2. Connecting to a Wi-Fi network** if you require more guidance.

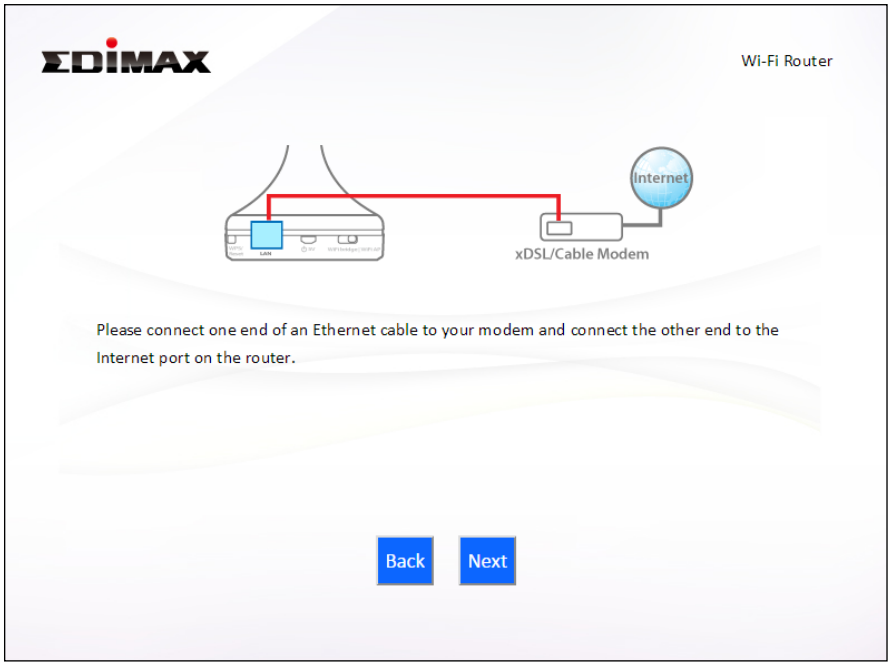
II-3. Wi-Fi Router Mode

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

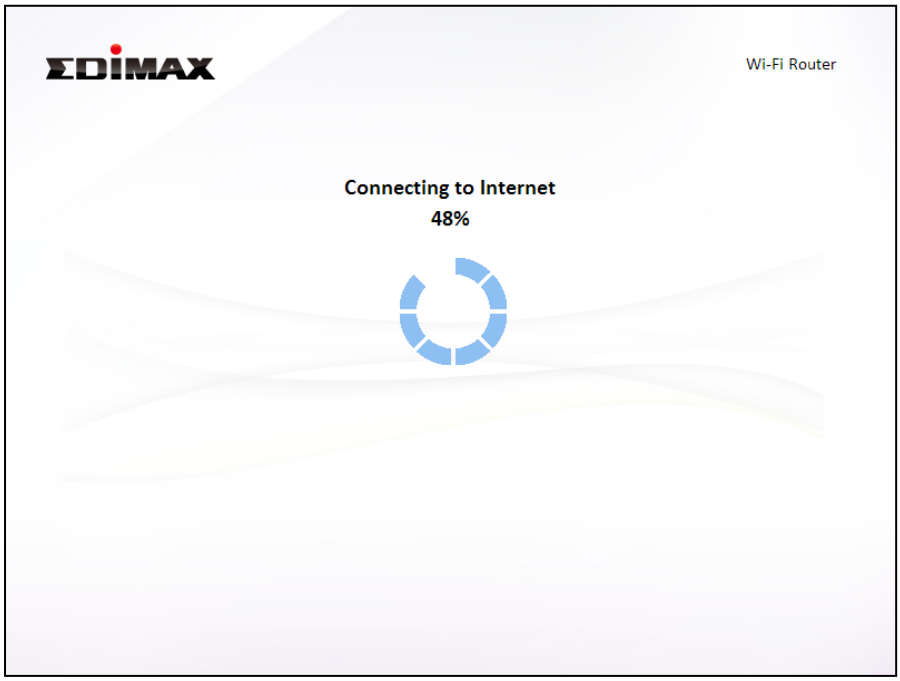


Manual configuration is only recommended for advanced users.

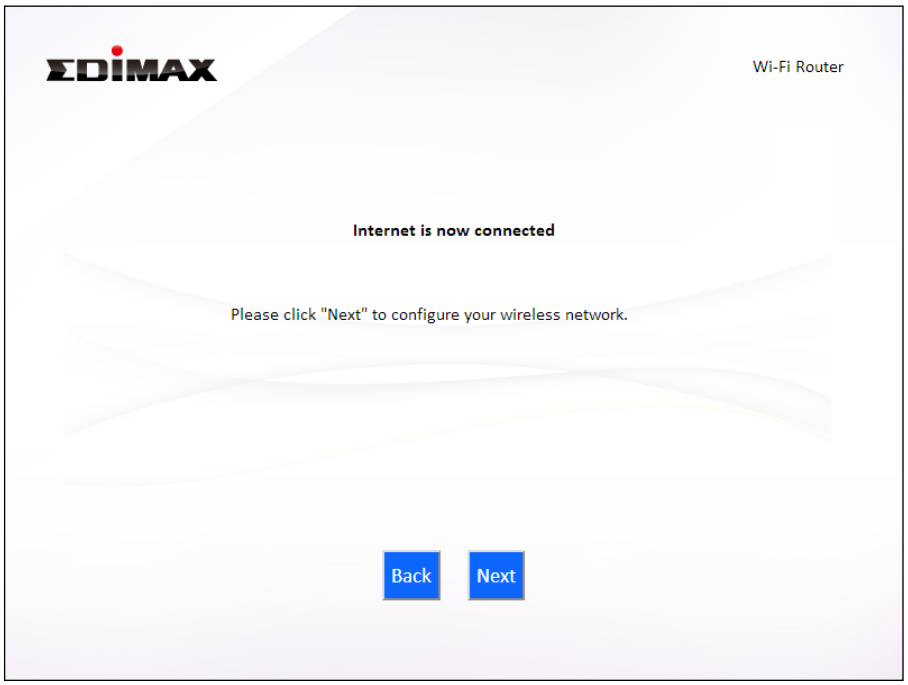
2. Connect the **blue** Internet port of your BR-6288ACL V2 to the LAN port of your modem using an Ethernet cable, and then click “Next”.



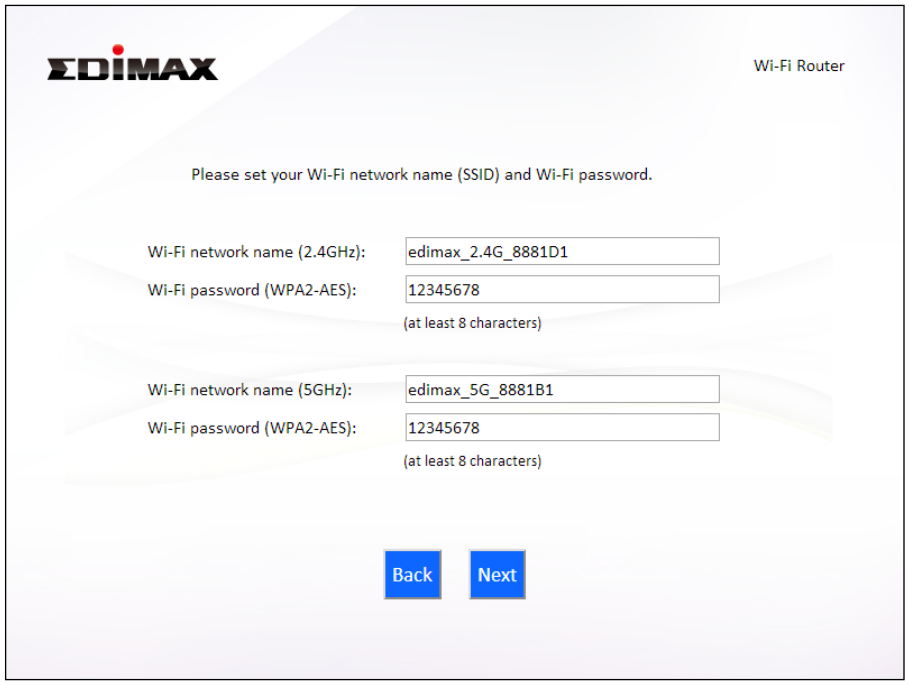
3. Please wait a moment while the BR-6288ACL V2 tests the connection.



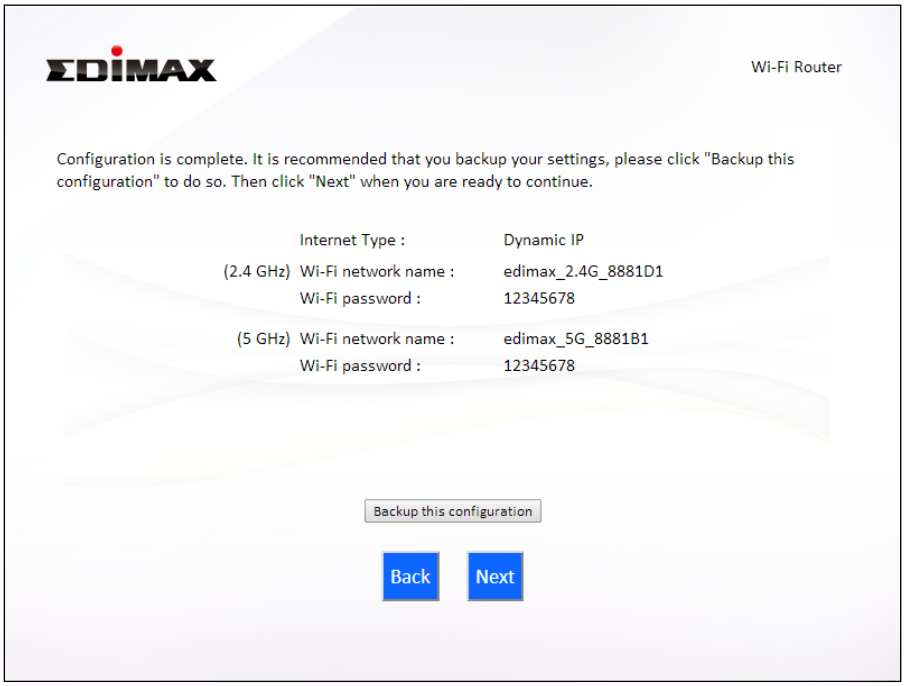
4. Click “Next” to continue and configure the device’s wireless network.



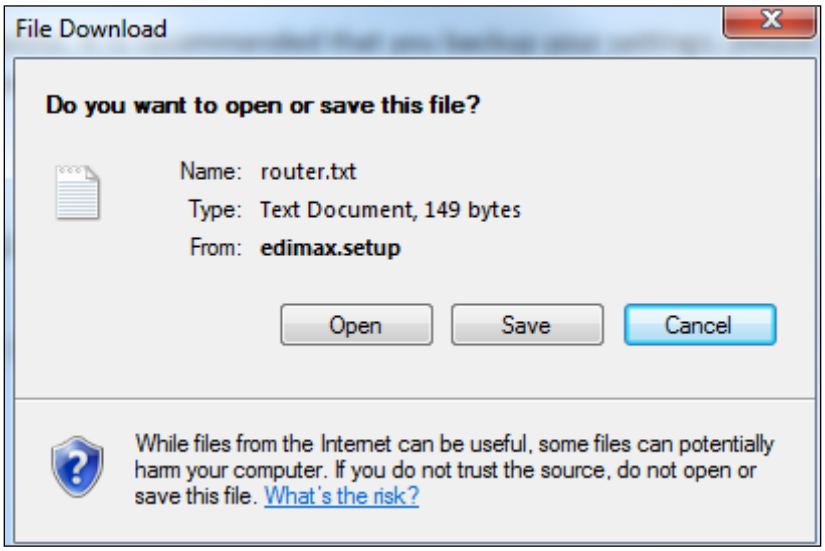
5. Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.



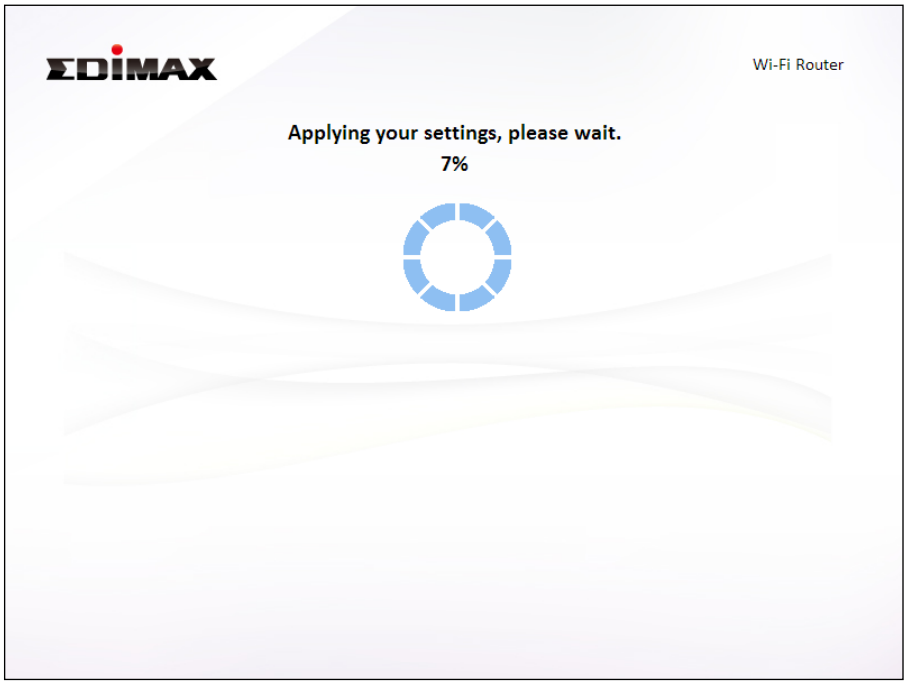
6. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



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 V2 applies your settings.

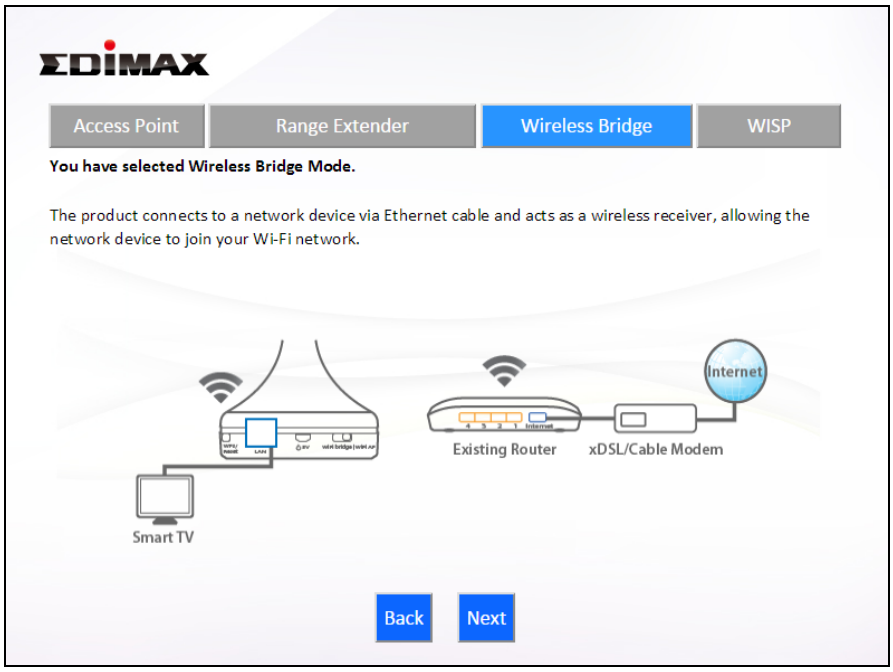


8. A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) which are shown on the screen then close the browser window.

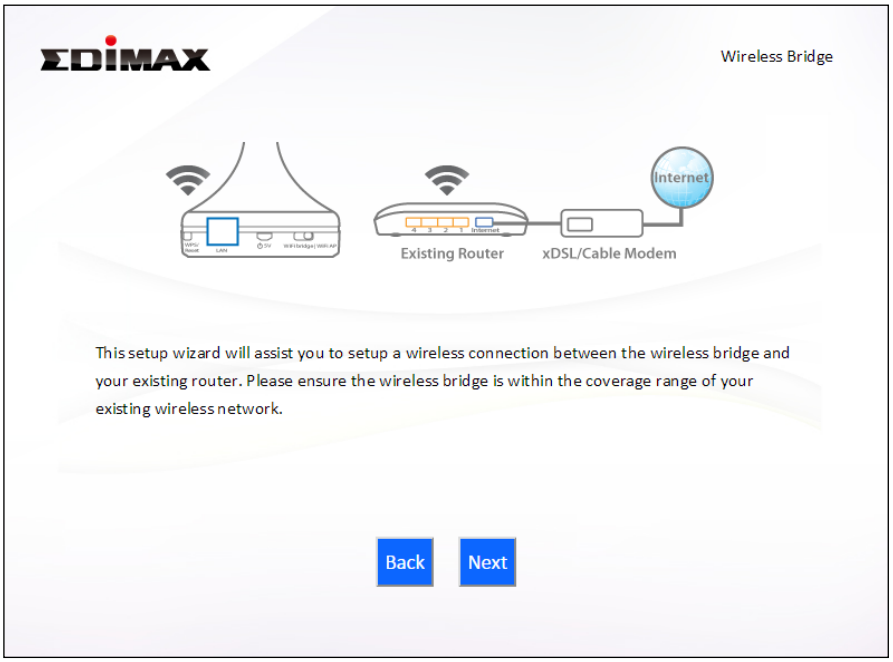
9. The BR-6288ACL V2 is working and ready for use. Refer to **IV-2. Connecting to a Wi-Fi network** if you require more guidance.

II-4. Wireless Bridge Mode

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

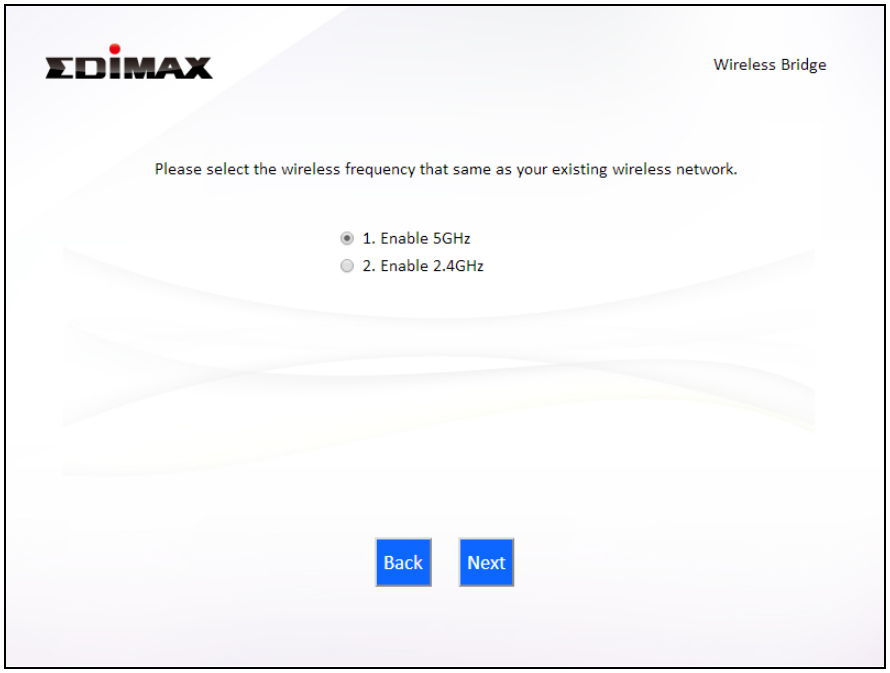


2. Please ensure your BR-6288ACL V2 is within Wi-Fi range of your existing wireless router. Click “Next” to continue.



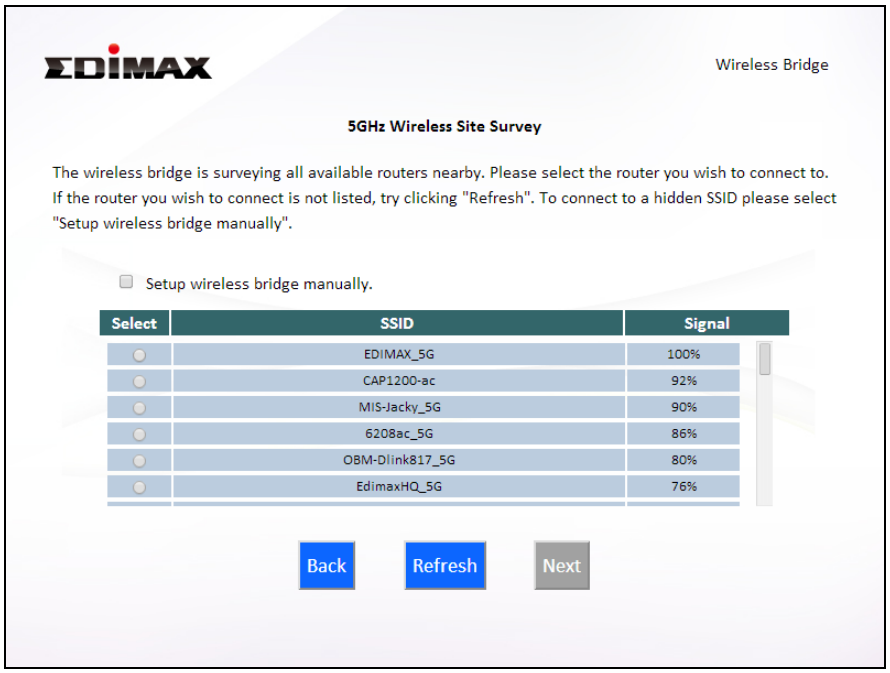
3. Select the frequency (2.4GHz or 5GHz) of your existing wireless network.

In wireless client mode, the BR-6288ACL V2 can only connect to one wireless network/frequency i.e. 2.4GHz or 5GHz.

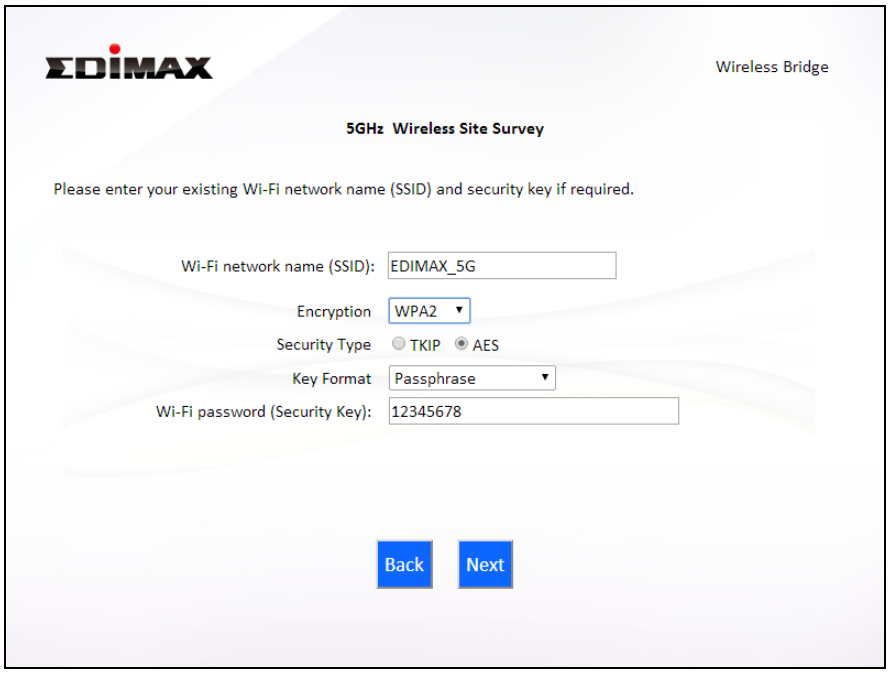


4. Select the Wi-Fi network name (SSID) which you wish to connect to and click “Next” to continue.

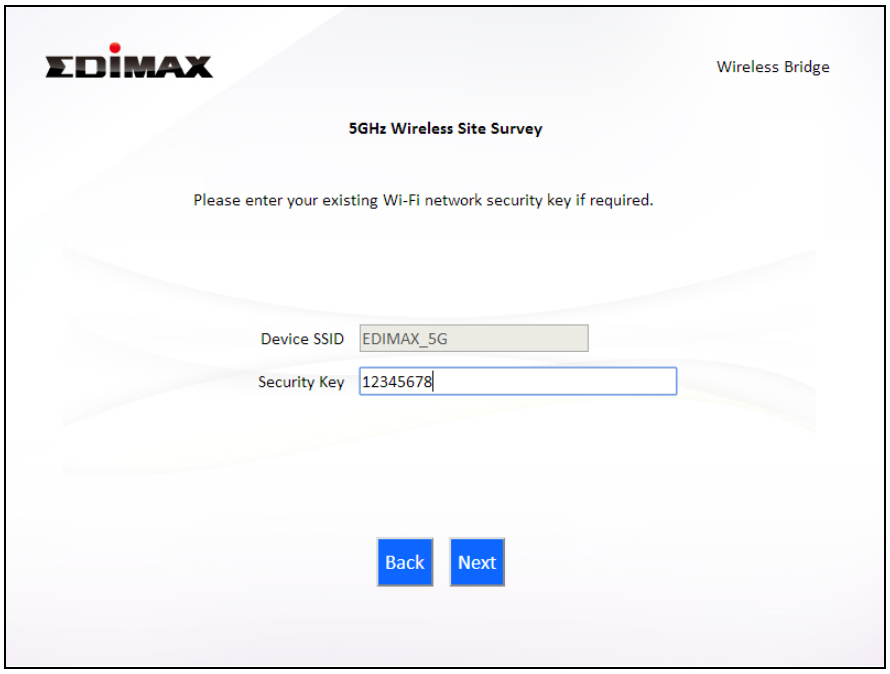
If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.



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



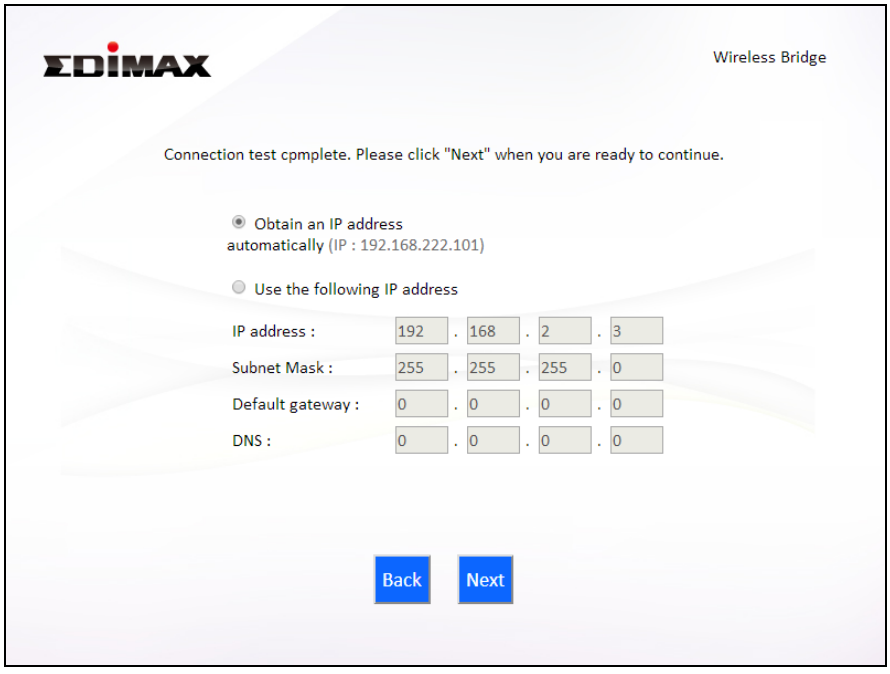
5. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.



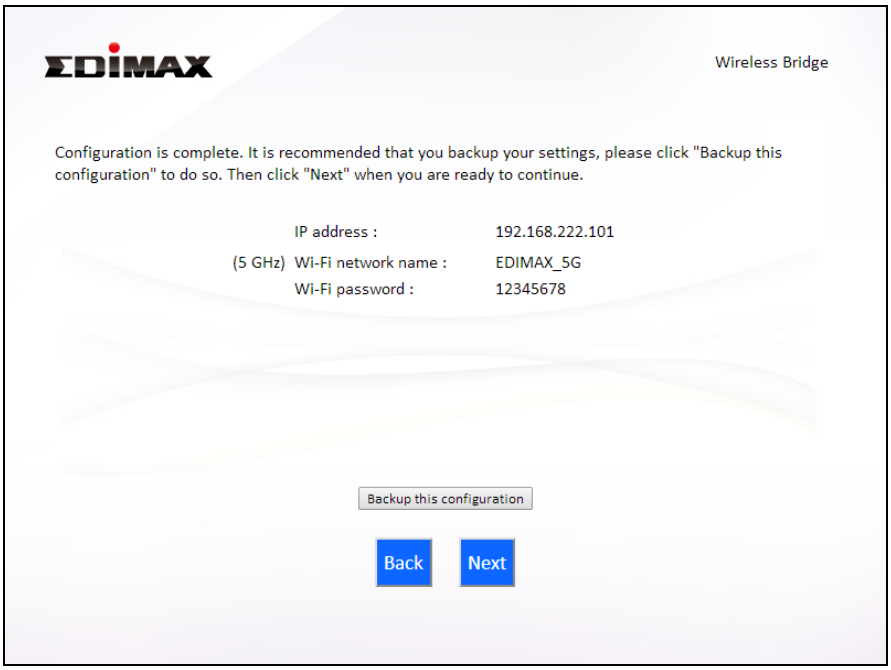
6. Wait a moment while the BR-6288ACL V2 tests the wireless connection.

7. Select “Obtain an IP address automatically” or “Use the following IP address” for your BR-6288ACL V2. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

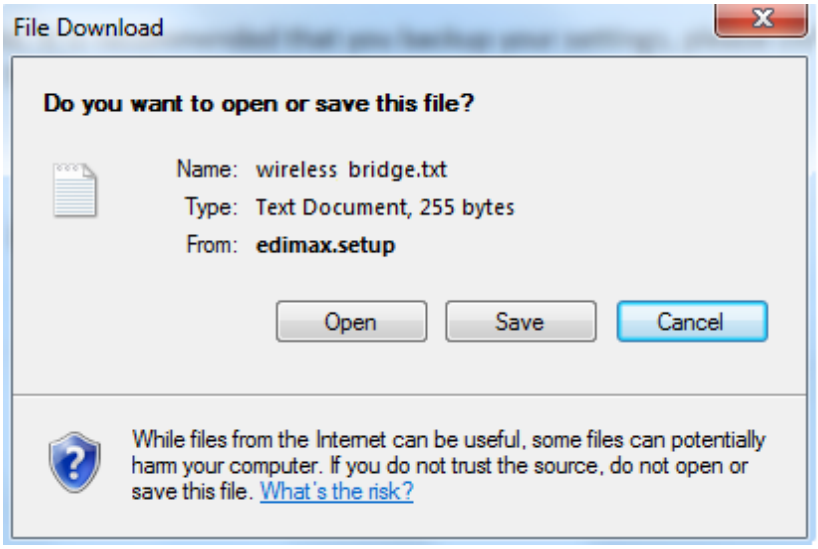
“Obtain an IP address automatically” is the recommended setting for most users. The IP address will be displayed in brackets.



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.

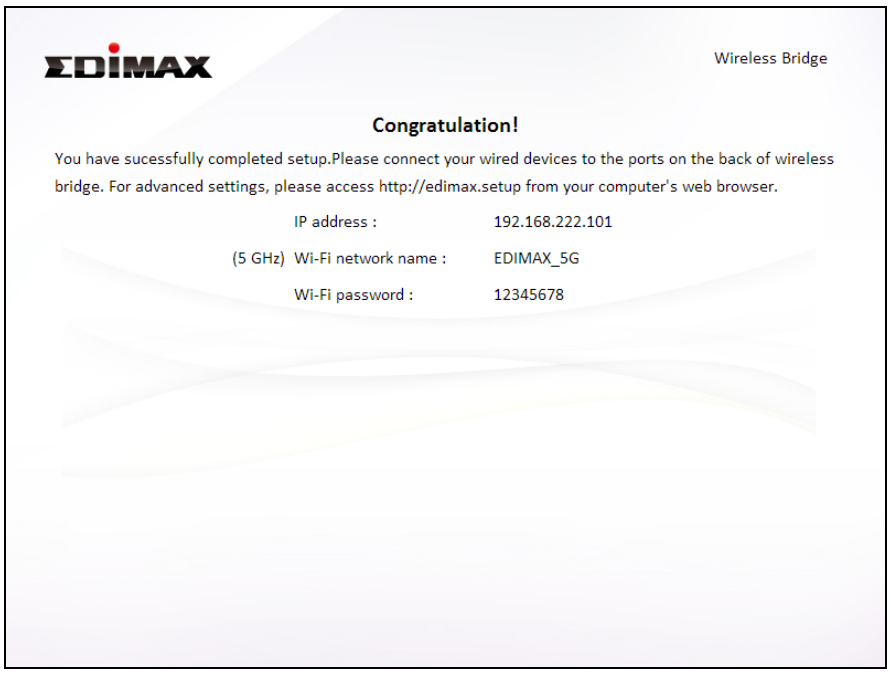


If you wish to backup the BR-6288ACL V2’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.



9. Please wait a moment until the BR-6288ACL V2 is ready.

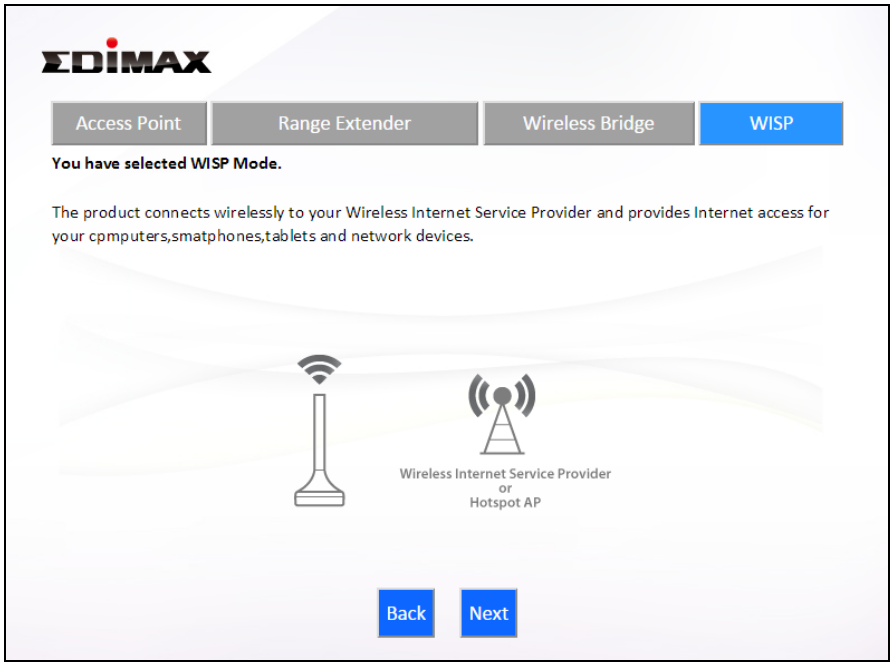
10. A final congratulations screen will indicate that setup is complete. Please close the browser window.



11. The BR-6288ACL V2 is working and ready for use. You can now connect the BR-6288ACL V2 to your network device using an Ethernet cable and connect to your network as usual.

II-5. WISP Mode

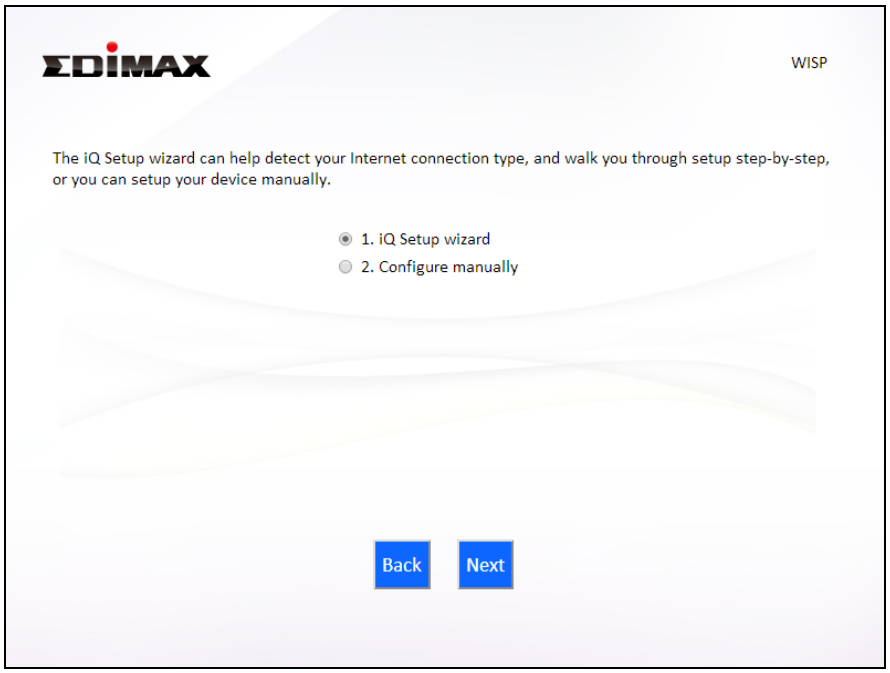
1. Select “WISP” from the top menu and click “Next”.



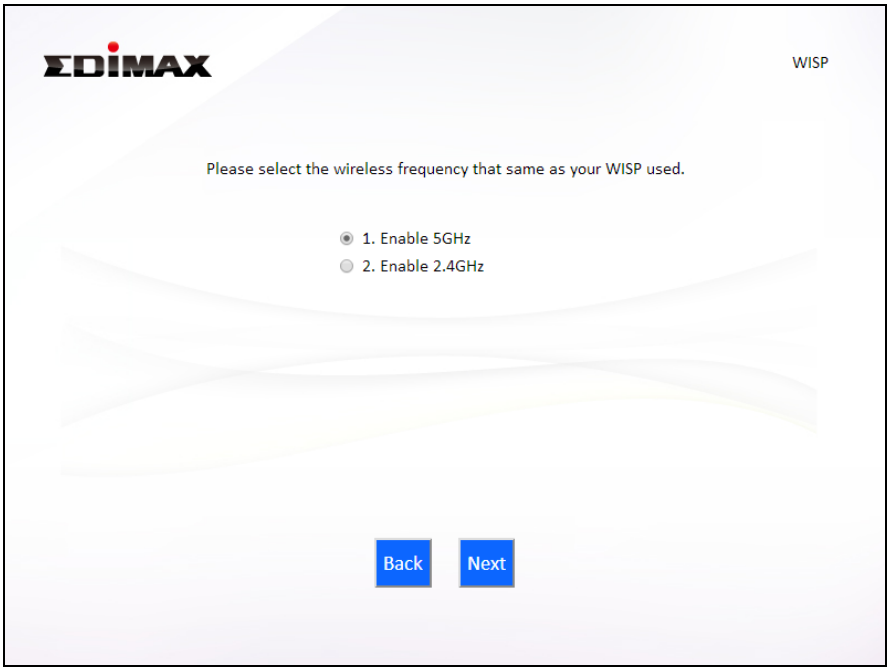
2. Please ensure your BR-6288ACL V2 is within Wi-Fi range of your WISP network and click “Next” to continue.

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.

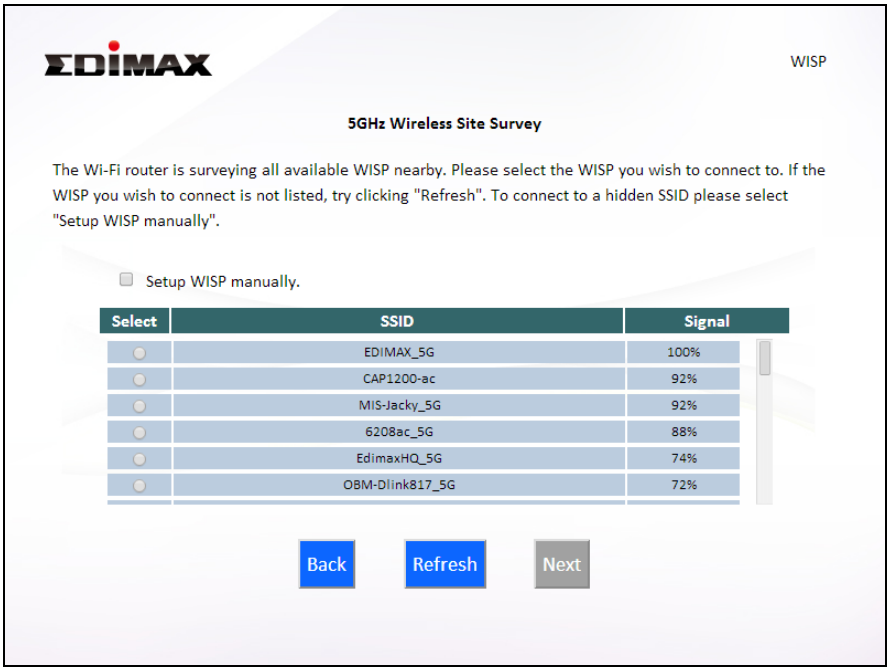


4. Select the wireless frequency (2.4GHz or 5GHz) of your WISP network.

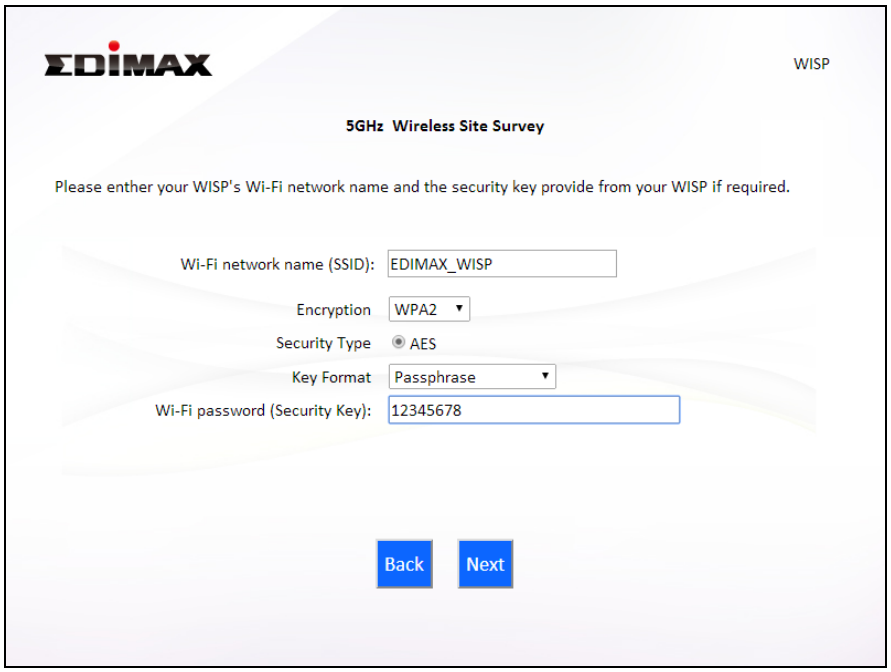


5. Select the WISP SSID which you wish to connect to and click “Next” to continue.

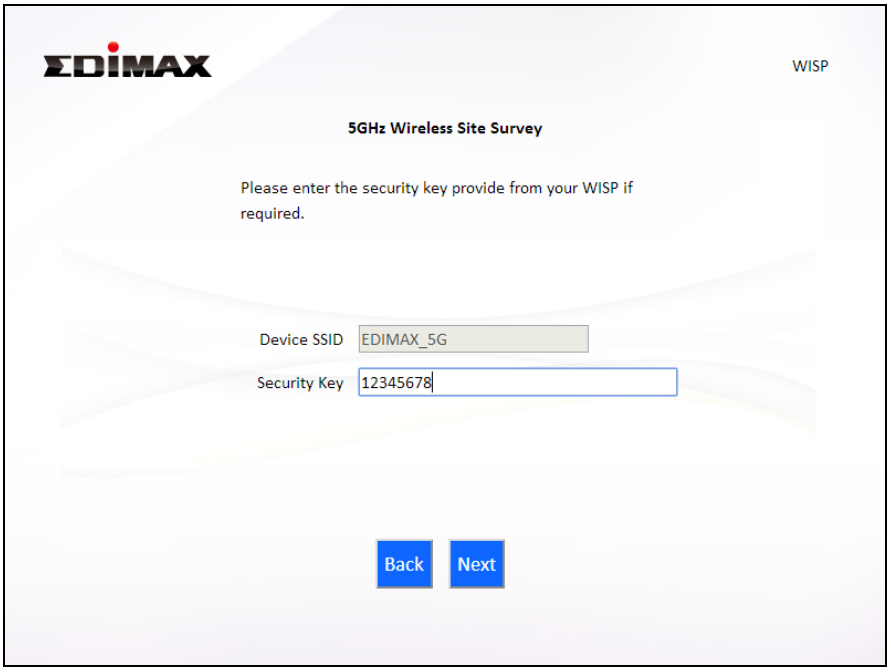
If the Wi-Fi network you wish to connect to does not appear, try clicking “Refresh”.



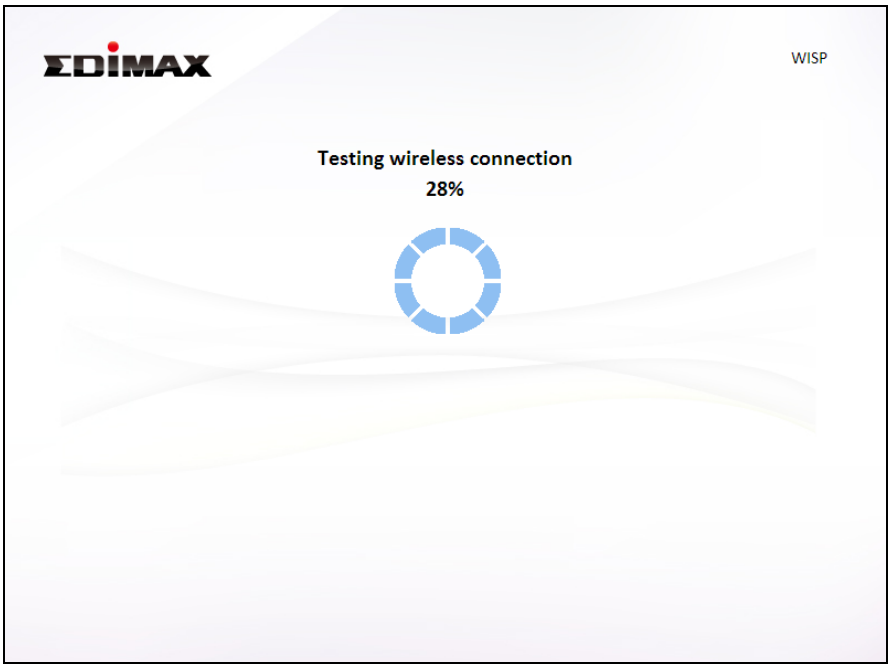
To connect to a hidden SSID, check the “Setup extender manually” box and enter the details manually on the next page, as shown below.



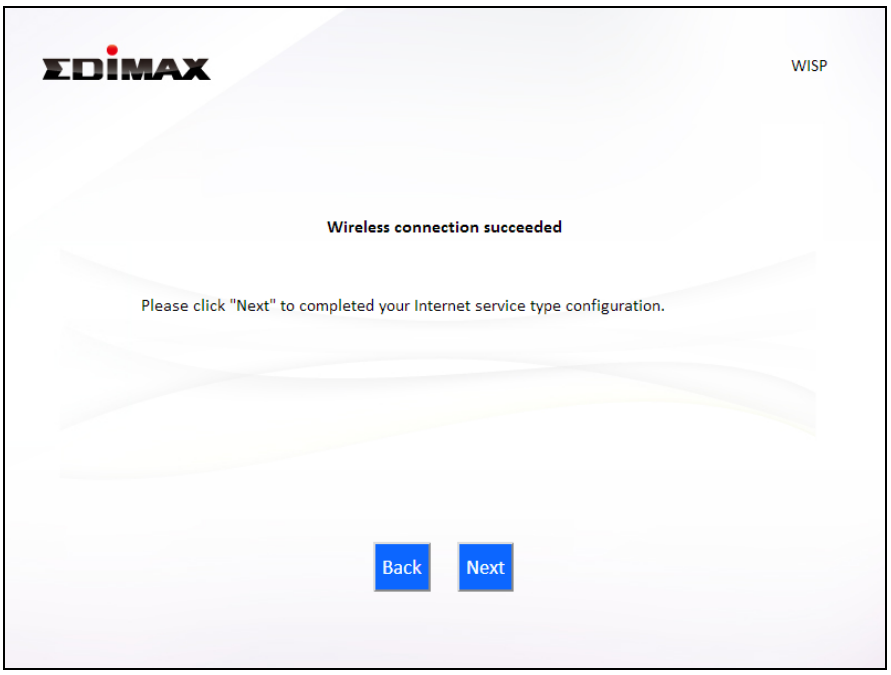
6. Enter your existing wireless network's security key/password in the "Security Key" field and click "Next" to continue.



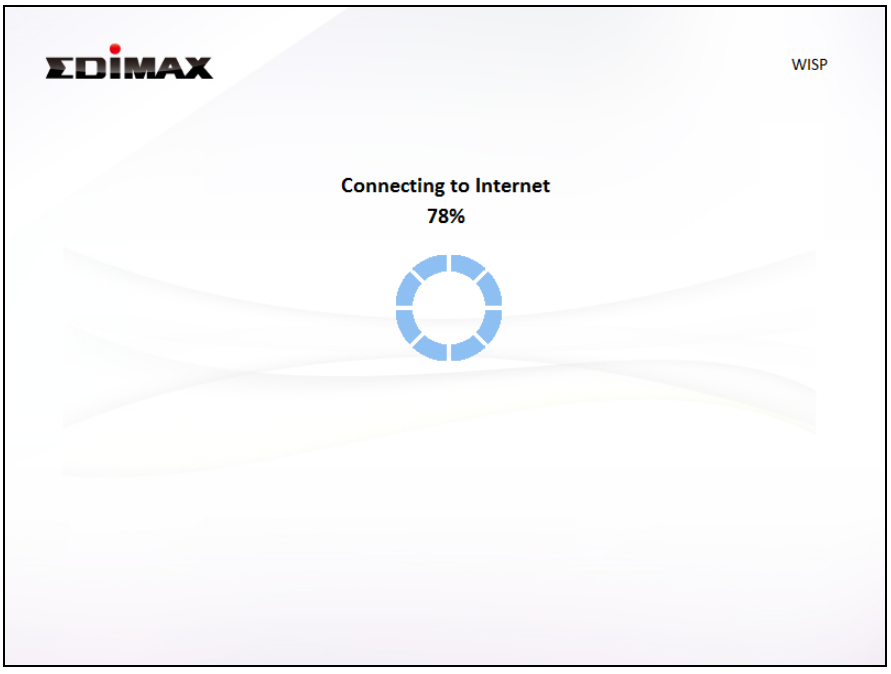
7. Wait a moment while the BR-6288ACL V2 tests the wireless connection.



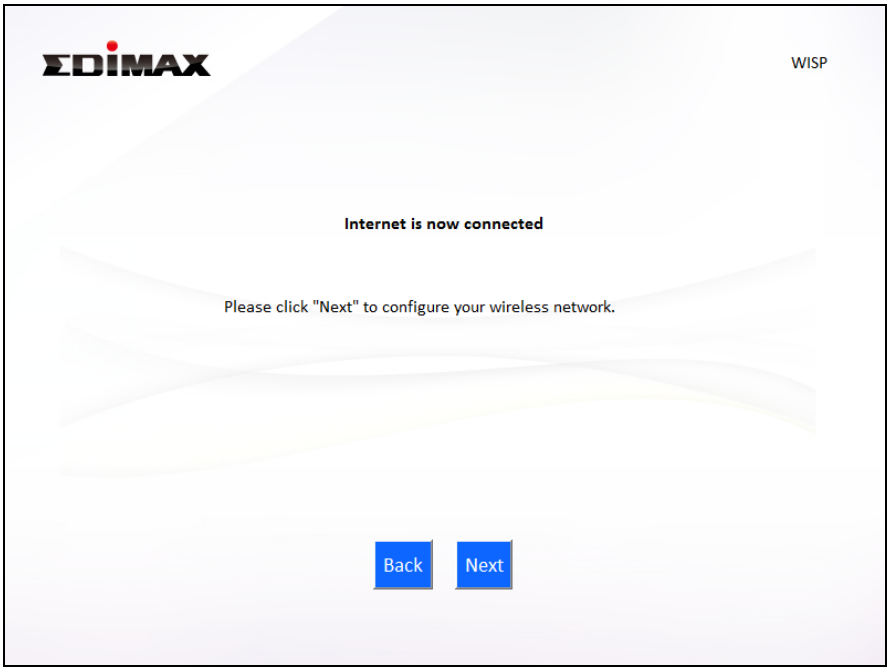
8. Click “Next” to continue your Internet service type configuration.



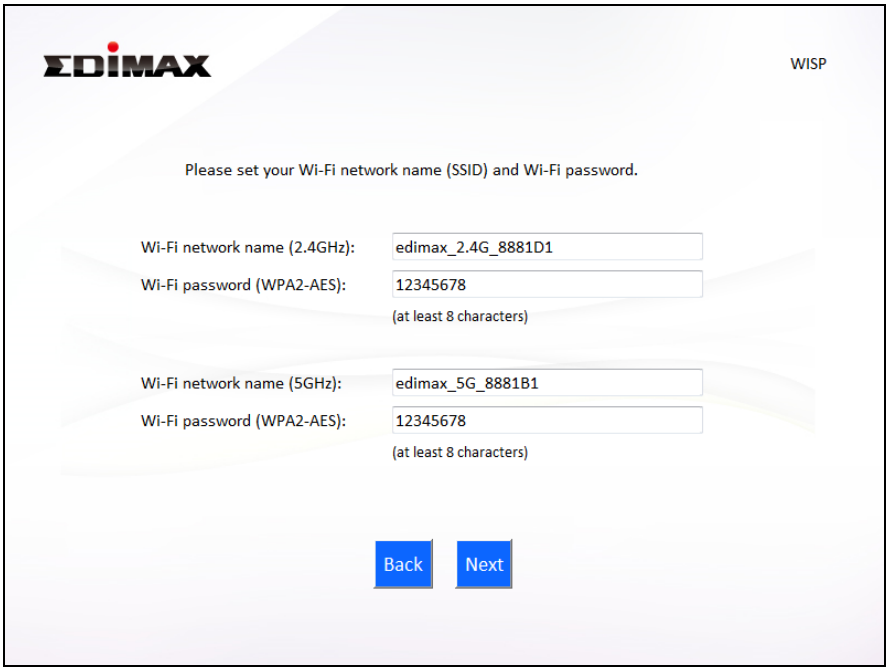
9. Wait a moment while the BR-6288ACL V2 connects to the Internet.



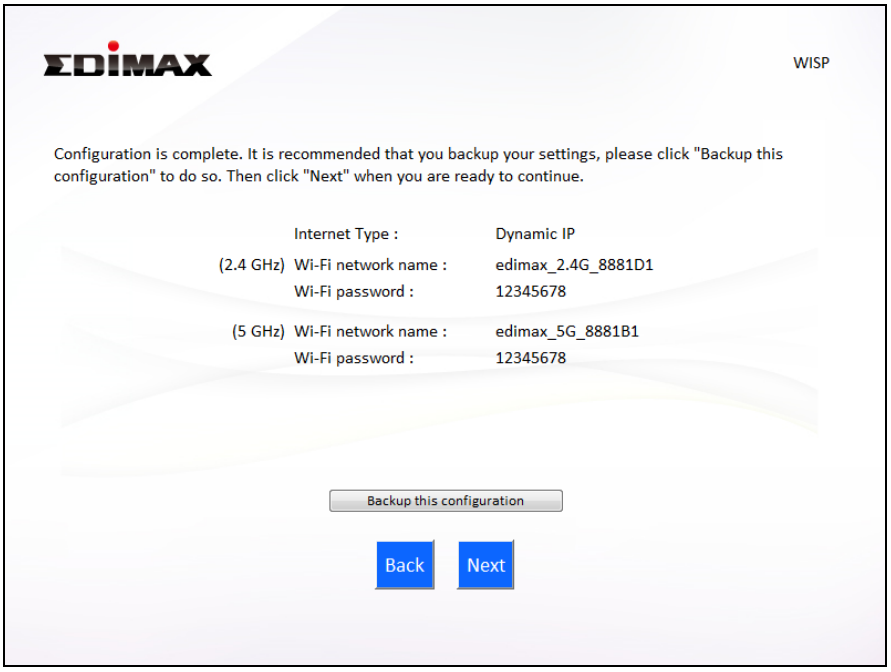
10. When the Internet is connected, click “Next” to configure your wireless network.



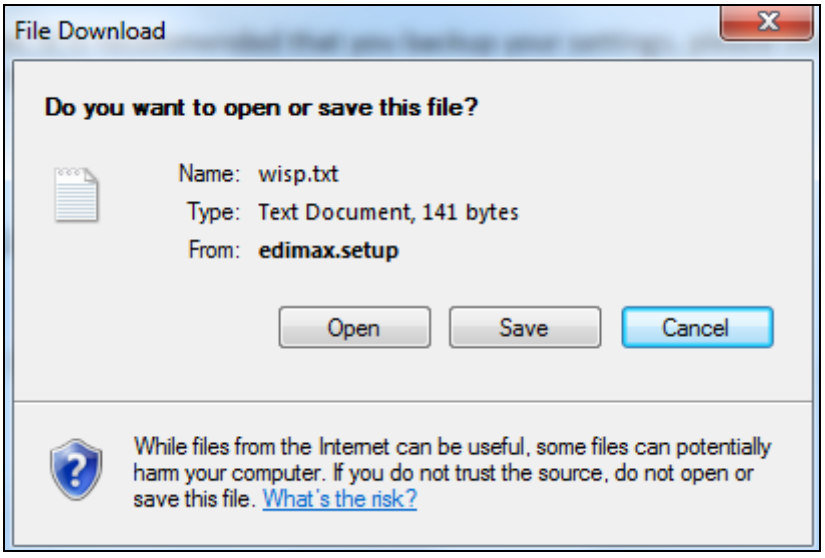
11. Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.



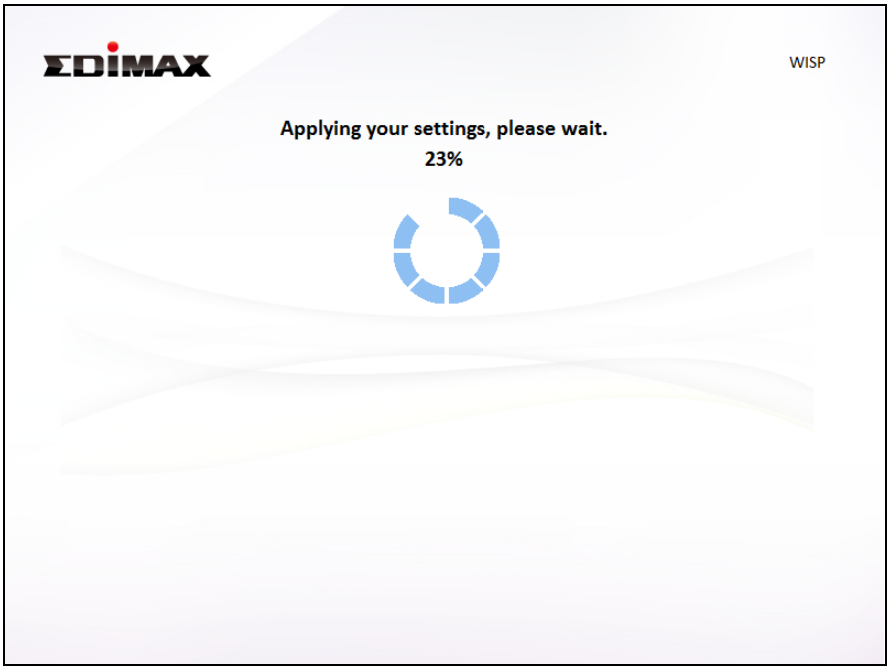
12. A summary of your configuration will be displayed, as shown below. Check that all of the details are correct and then click “Next” to proceed.



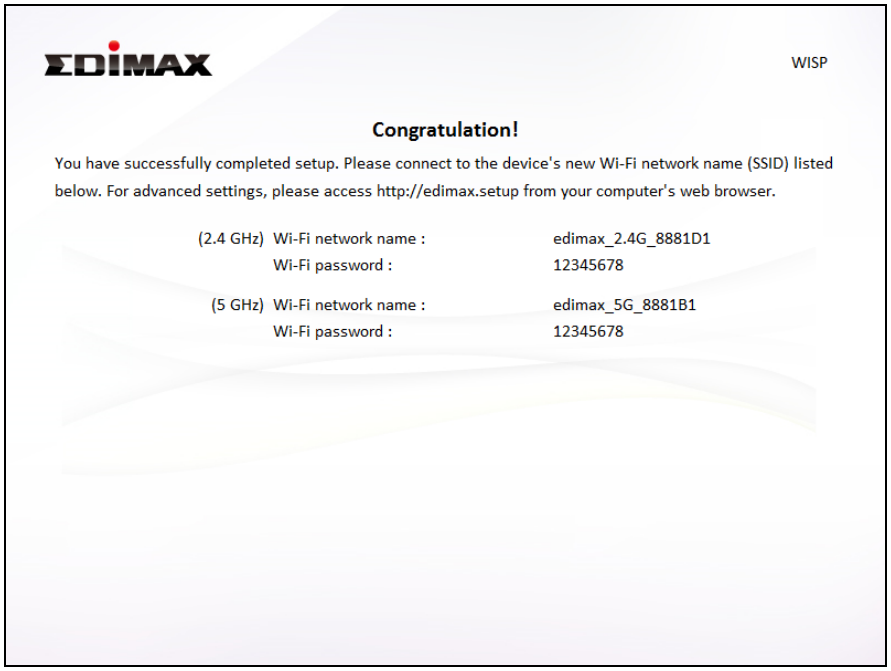
If you wish to backup the device’s settings, click “Backup this configuration” to open a new window and save your current configuration to a .txt file.



13. Please wait a moment until the BR-6288ACL V2 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.

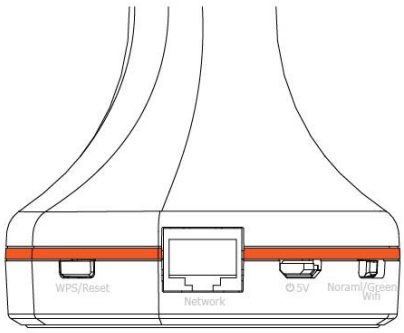


15. The BR-6288ACL V2 is working and ready for use. Refer to **IV-2. Connecting to a Wi-Fi network** if you require more guidance.

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 V2's Wi-Fi network.

1. Press the **WPS/Reset button** on the BR-6288ACL V2 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 V2, 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 V2 to restart.

III. Browser Based Configuration Interface

After you have setup the BR-6288ACL V2 as detailed in **II. Installation** or the included **Quick Installation Guide**, you can use the browser based configuration interface to configure advanced settings.

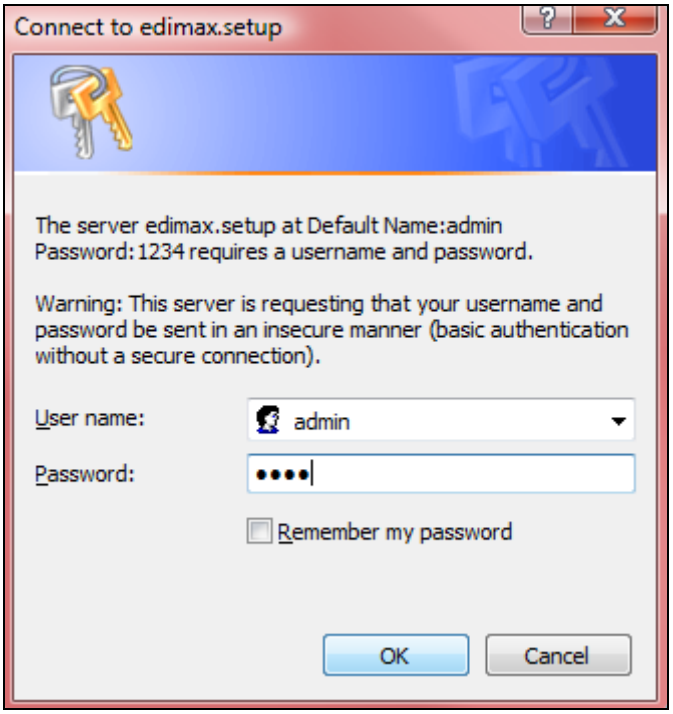
Please ensure that your computer is set to use a dynamic IP address. Refer to IV-1. Configuring your IP address for more information.

III-1. Login

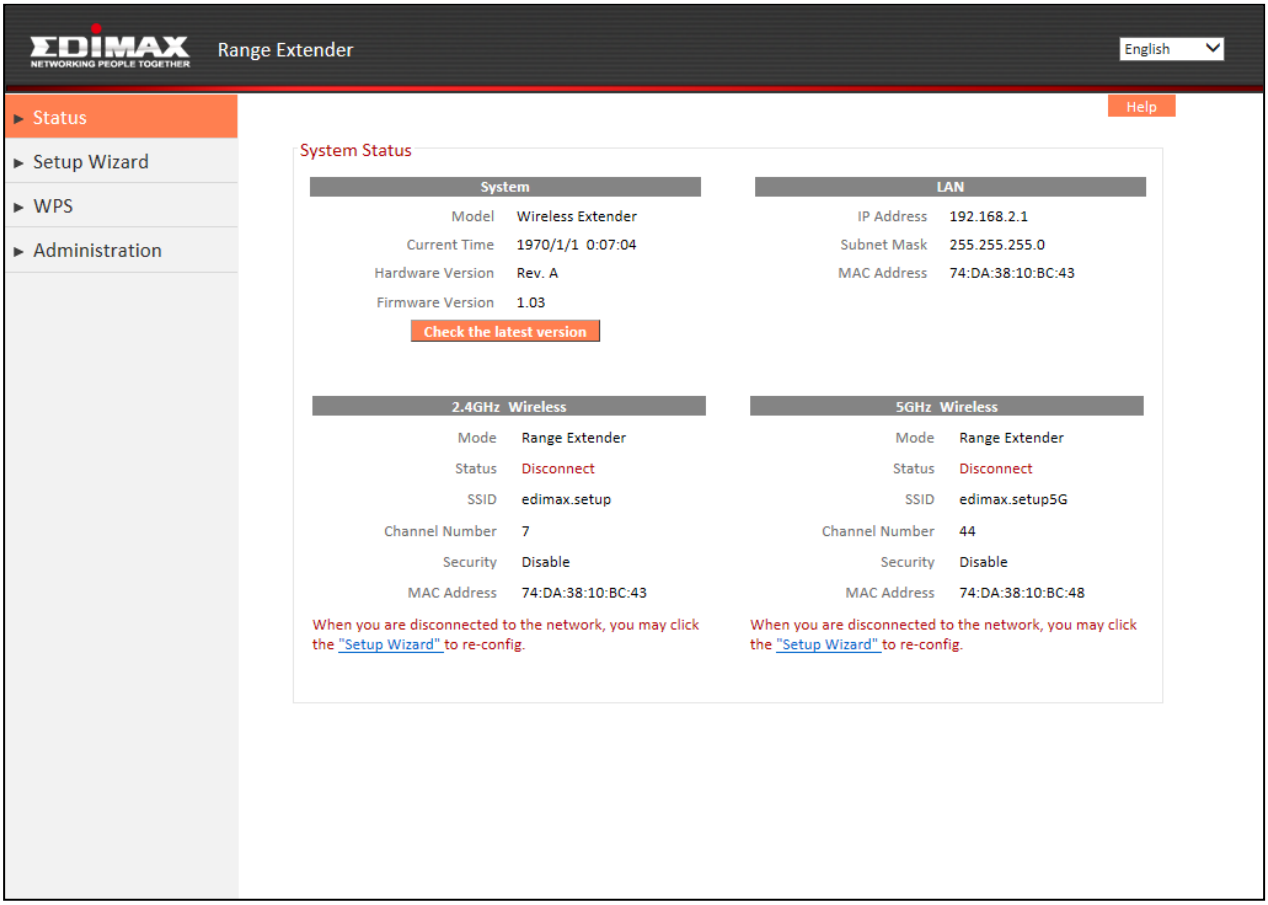
1. To access the browser based configuration interface enter ***http://edimax.setup*** into the URL bar of a browser on a network device connected to the same Wi-Fi network as the BR-6288ACL V2.

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.



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.

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*

Range Extender

- Status
- Setup Wizard
- WPS
- Administration

Access Point

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

Wi-Fi Router

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

WISP

- Status
- Setup Wizard
- Administration

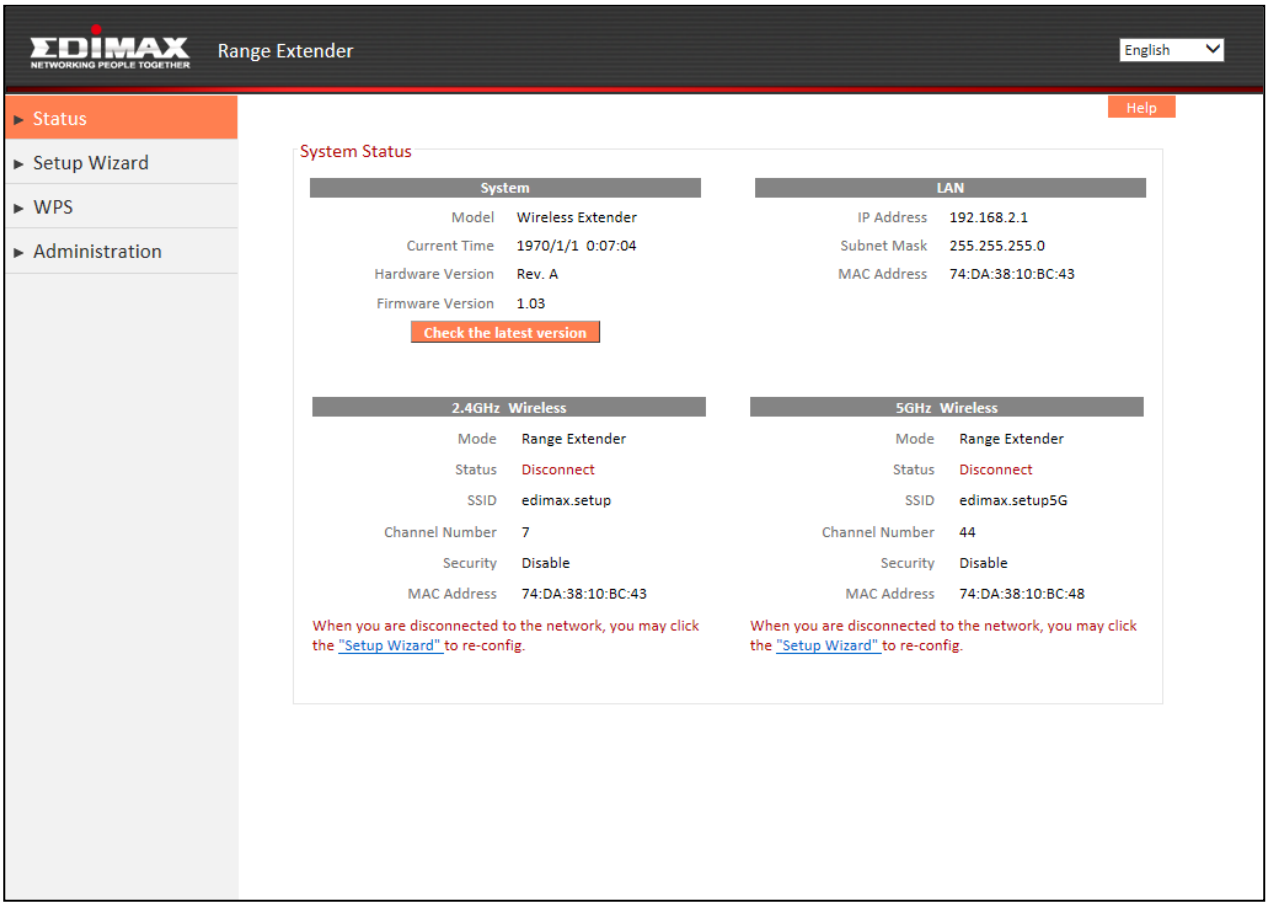
Wireless Bridge

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

III-3-1. Status

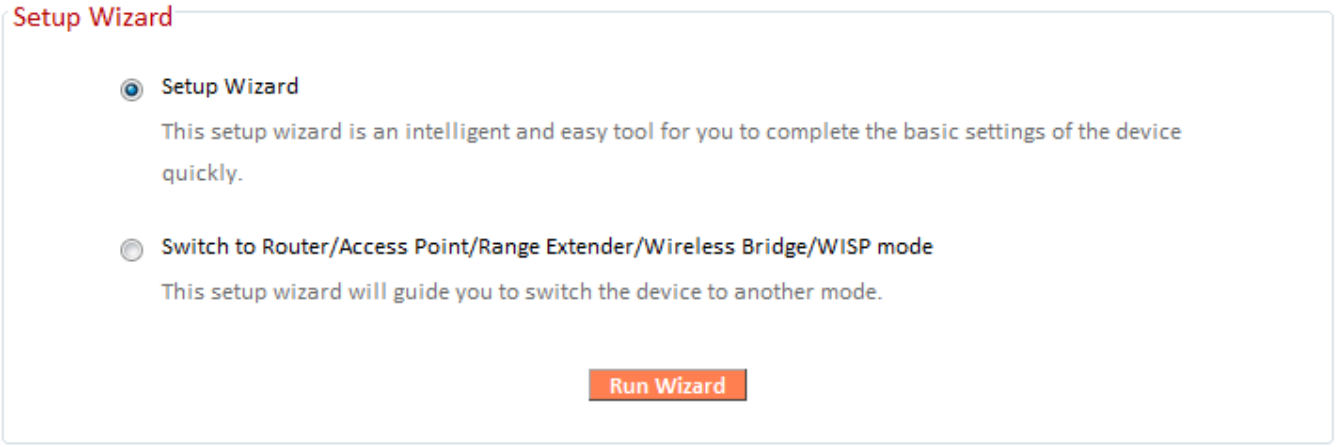
The “Status” page displays basic system information about the device, arranged into categories.

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



III-3-2. 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.

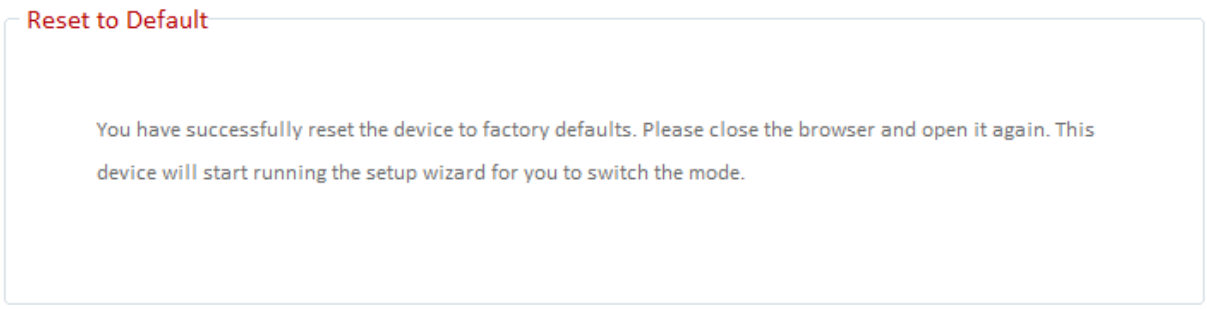


Setup Wizard	This wizard will help you to set up the basic functions and settings of the device. For guidance about using the setup wizard, please refer to **II. Installation**.
Switch to Router/Access Point/ Range Extender/ Wireless Bridge/ WISP mode	This wizard will help you to switch the device to 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.

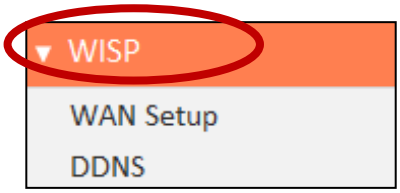


3. Follow the on-screen wizard to setup your device in a different mode. Refer to **II. Installation Step 3** onwards for help if needed.

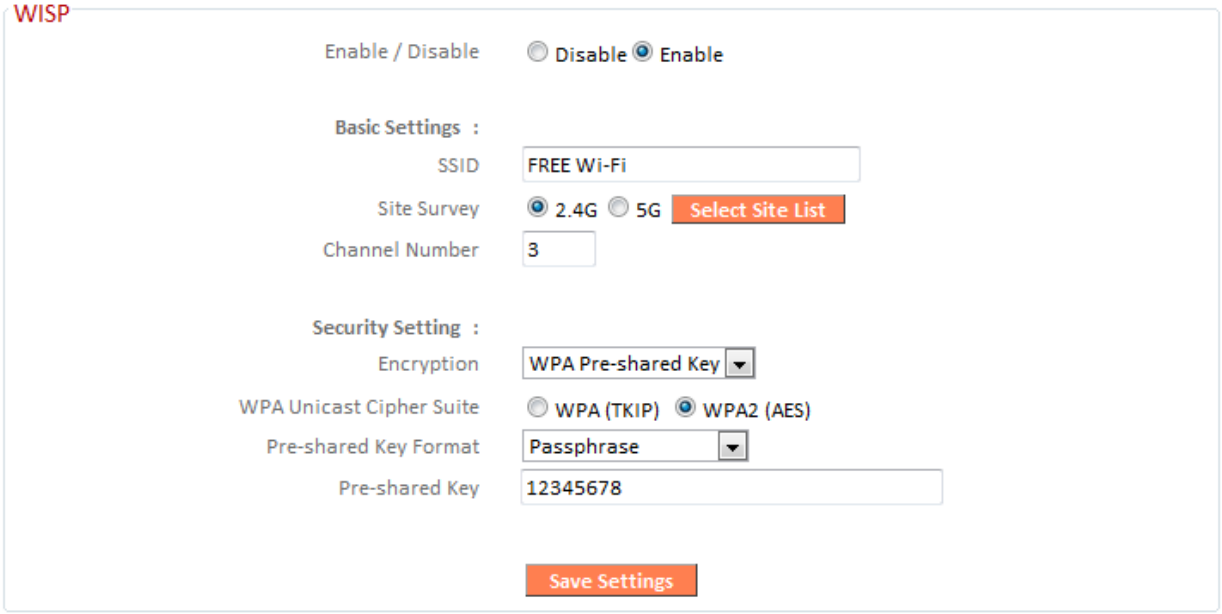
If you don't see the** "Get Started" **screen, try reconnecting to the** edimax.setup **SSID and go to** http://edimax.setup **in a web browser.

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:

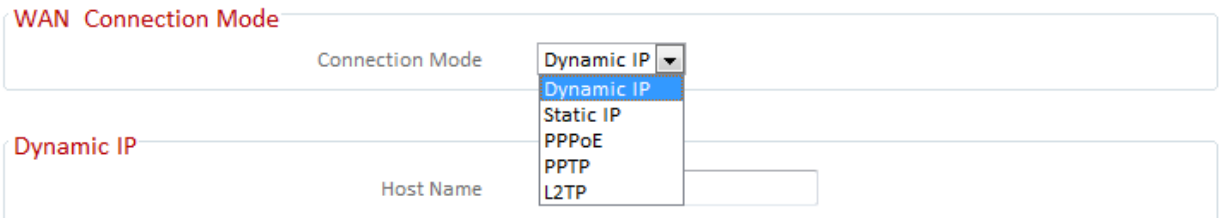


Enable / Disable	Enable or disable your WISP connection.
SSID	The name of the WISP network which your BR-6288ACL V2 is connected to. Manually enter an SSID if you wish or use “Site Survey” below.
Site Survey	Select wireless frequency and click “Show List” to open a new window and select your WISP network.
Security Setting	Please refer to **III-3-5-1. Basic** for a description of security settings.

III-3-3-1. WAN Setup

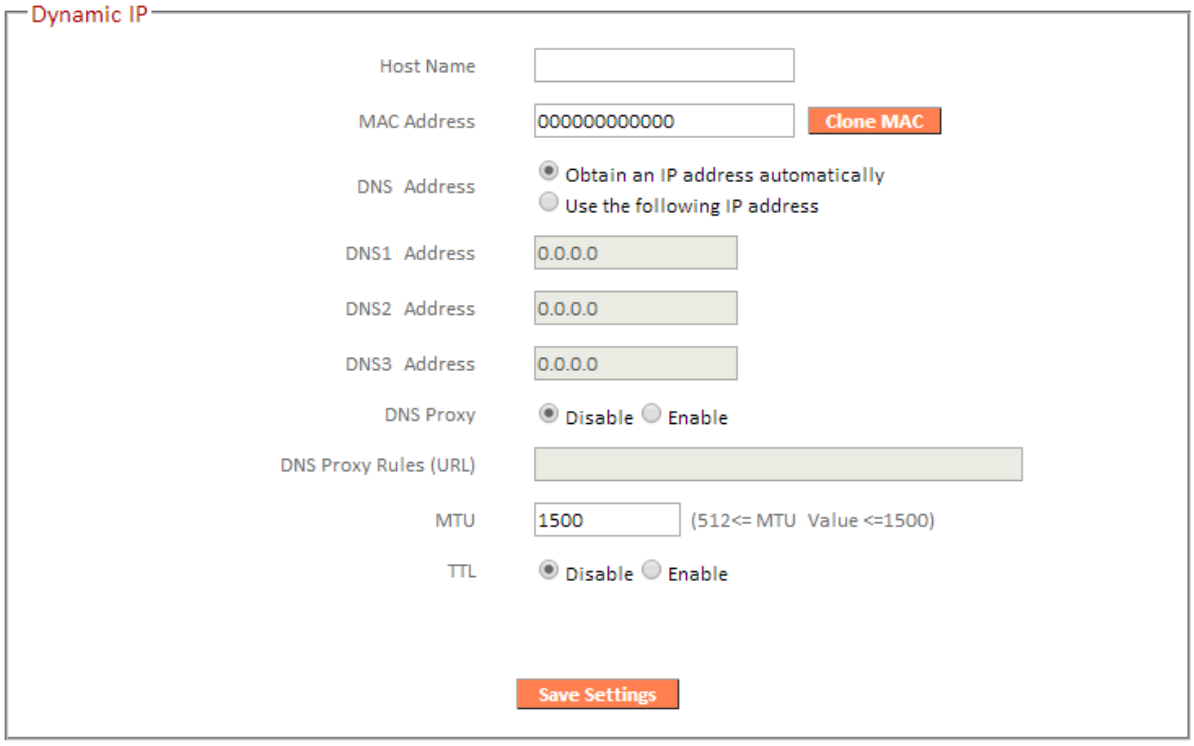
Select a Wide Area Network (WAN) connection mode and configure the settings. If you are unsure about your connection type, contact your ISP.

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



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

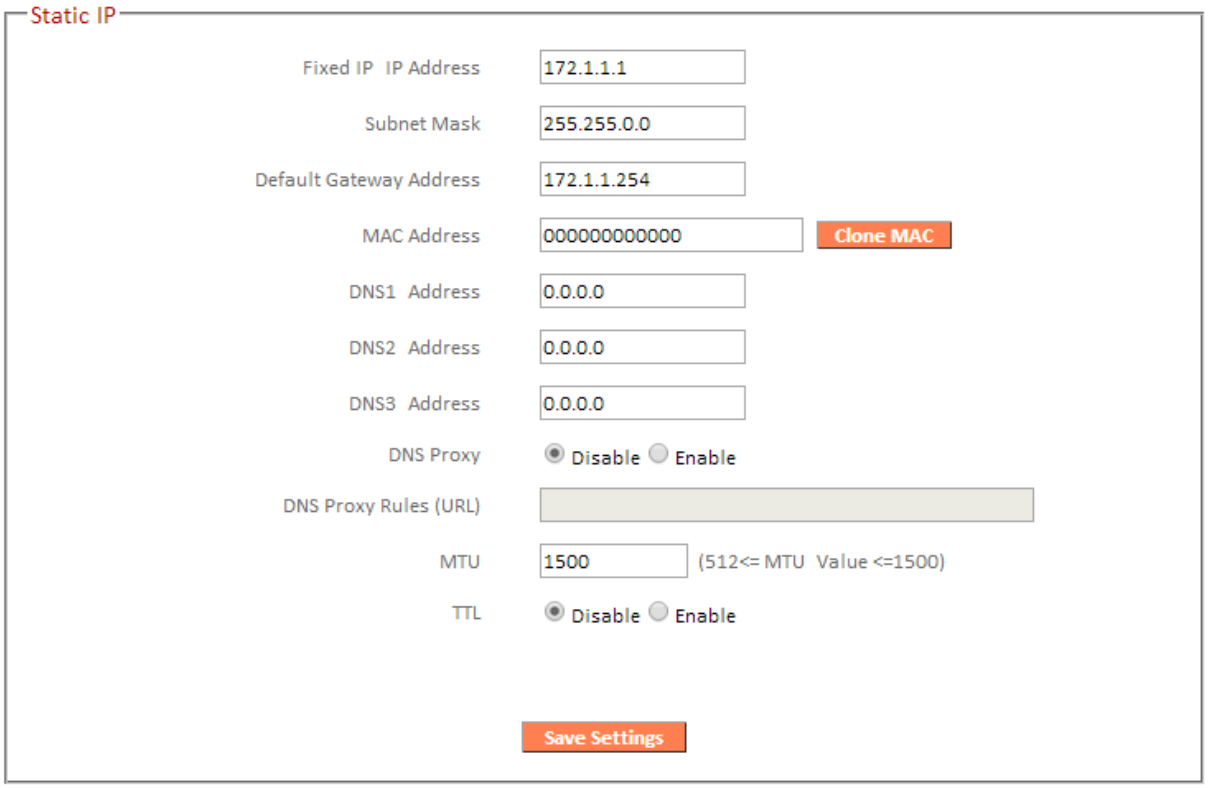
Select “Dynamic IP”. If your Internet service provider assigns IP address automatically using DHCP (Dynamic Host Configuration Protocol).



Host Name	Enter the host name of your computer.
MAC Address	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.
DNS Address	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
DNS Address 1,2 & 3	Enter the DNS address(es) assigned by your ISP here.
DNS Proxy	Enable or disable a DNS proxy server.
DNS Proxy Rules (URL)	When DNS proxy is enabled, enter the URL of a DNS proxy server.
MTU	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1500.
TTL	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.

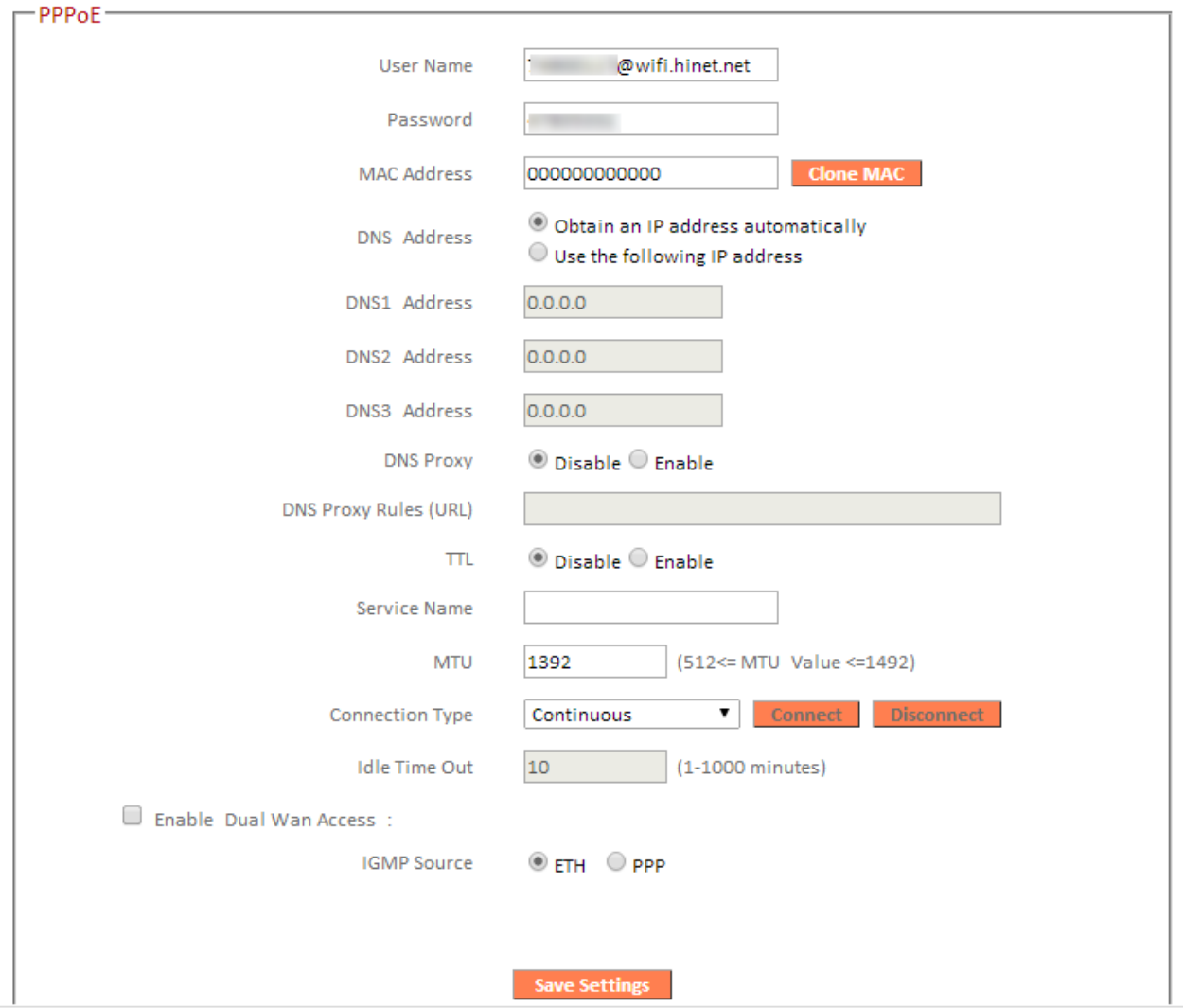


Fixed IP Address	Input the IP address assigned by your ISP here.
Subnet Mask	Input the subnet mask assigned by your ISP here.
Default Gateway Address	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
MAC Address	For some applications, you may need to designate 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.
DNS Address 1, 2 & 3	Enter the DNS address(es) assigned by your ISP here.
DNS Proxy	Enable or disable a DNS proxy server.
DNS Proxy Rules	When DNS proxy is enabled, enter the URL of a

(URL)	DNS proxy server.
TTL	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).

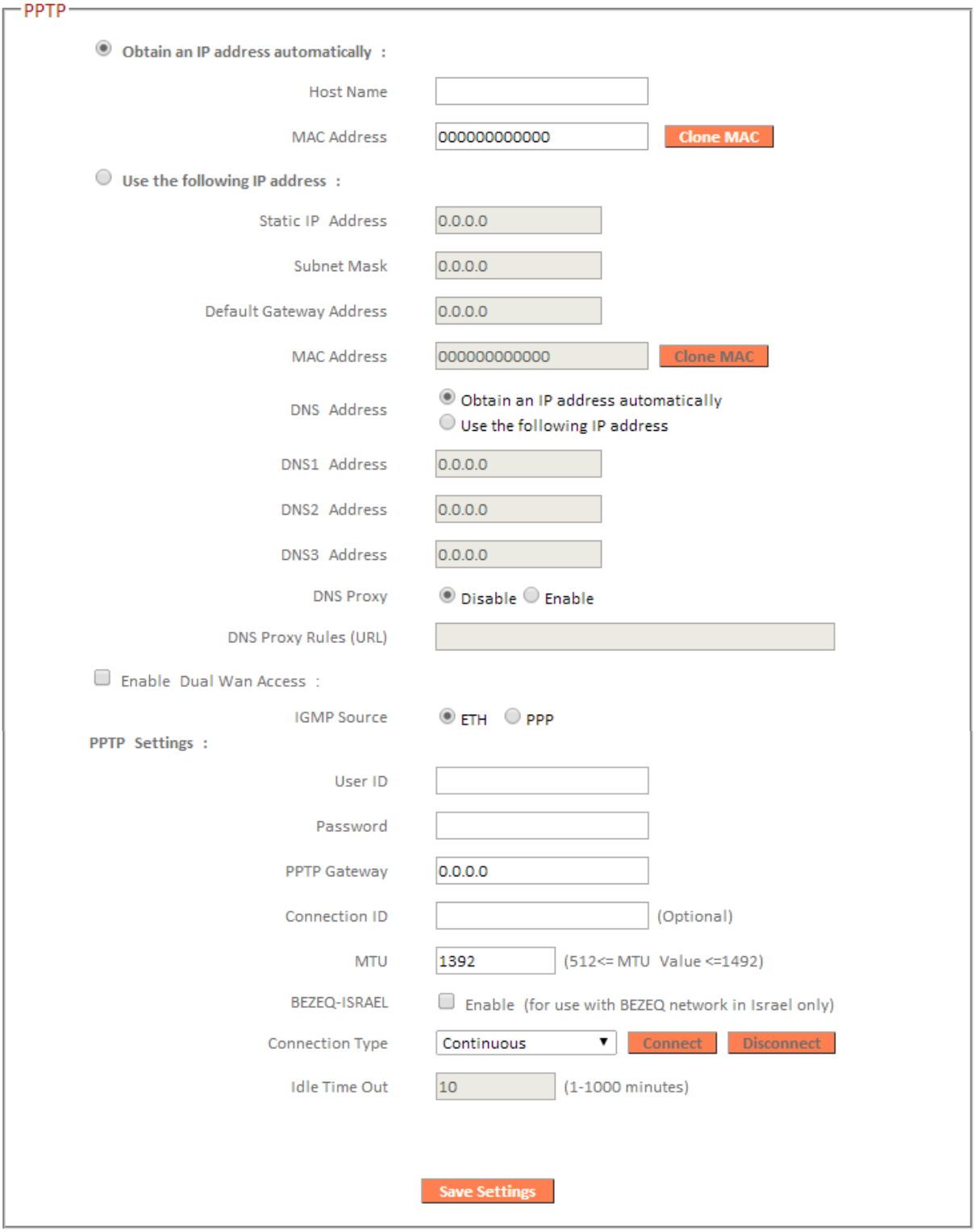


User Name	Enter the user name assigned by your ISP here.
Password	Enter the password assigned by your ISP here.
MAC Address	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press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

DNS Address	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
DNS Address 1, 2 & 3	Enter the DNS address(es) assigned by your ISP here.
DNS Proxy	Enable or disable a DNS proxy server.
DNS Proxy Rules (URL)	When DNS proxy is enabled, enter the URL of a DNS proxy server.
Service Name	Give this Internet service a name (optional).
MTU	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1392.
Connection Type	Specify a connection type: 1. “Continuous”: Connected all the time. 2. “Connect on Demand”: Connect when you initiate an Internet connection. 3. “Manual”: Connect/disconnect manually using the “Connect” and “Disconnect” buttons.
Idle Time Out	Specify the amount of time the router waits before shutting down an idle connection. Only available when “Connect on Demand” (above) is selected.
Enable Dual-WAN Access	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.

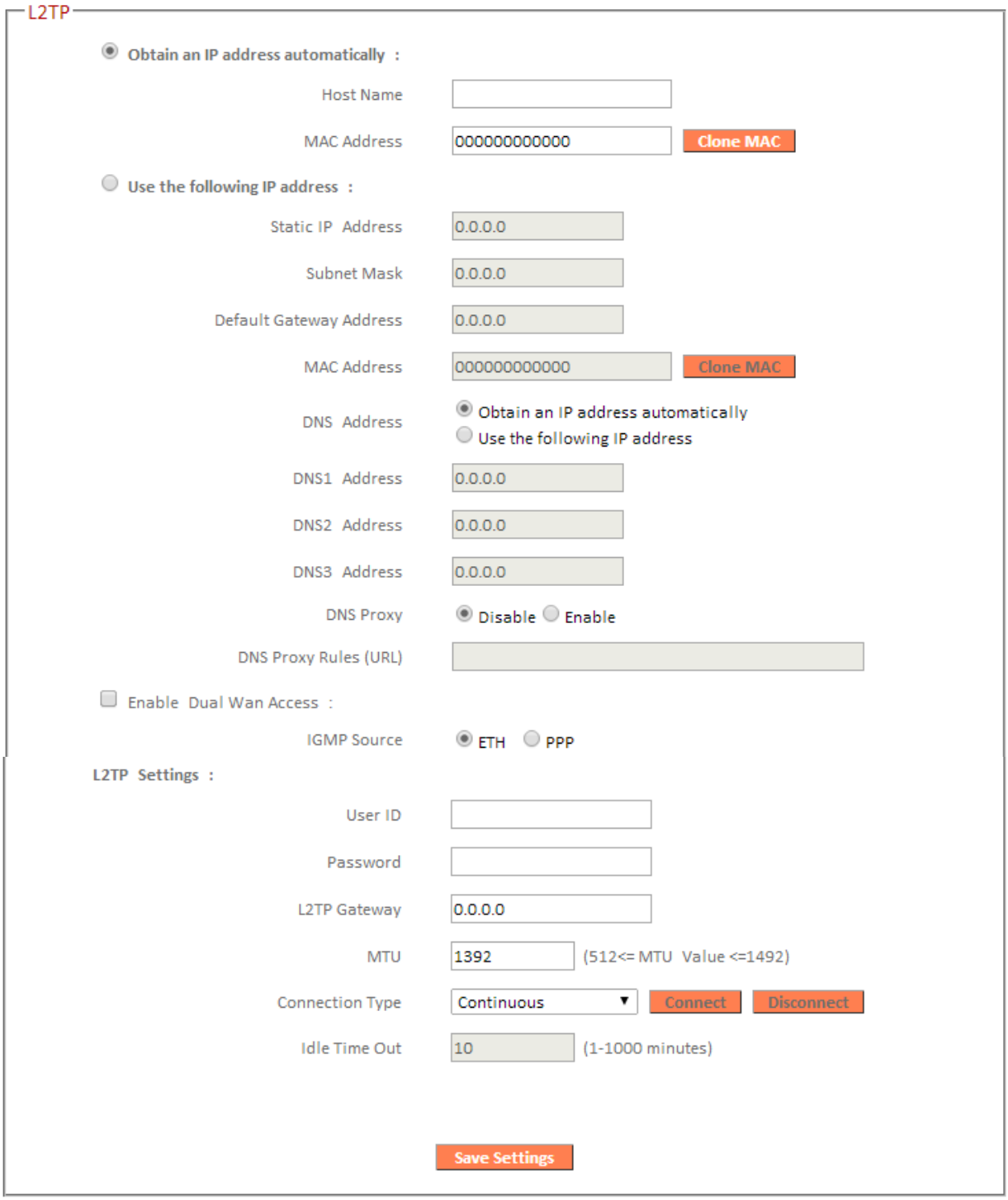


Host Name	Enter the host name of your computer here If required.
MAC Address	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, press “Clone Mac” to automatically enter your computer’s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

Connection Type	Specify a connection type: 1. “Continuous”: Connected all the time. 2. “Connect on Demand”: Connect when you initiate an Internet connection. 3. “Manual”: Connect/disconnect manually using the “Connect” and “Disconnect” buttons.
Idle Time Out	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).

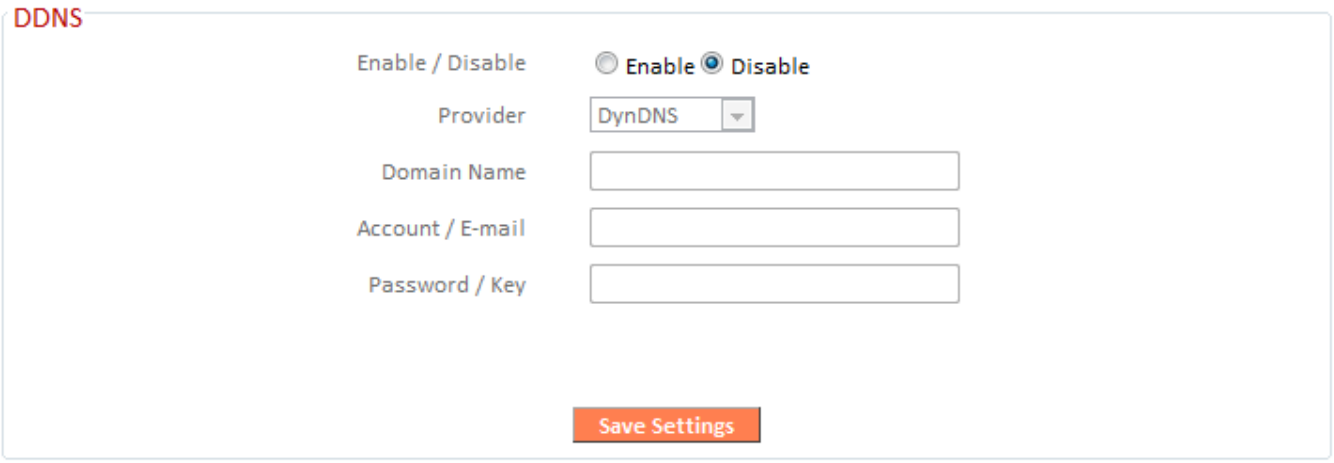


Host Name	Enter the host name of your computer here If required.
MAC Address	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to

	a computer, press “Clone Mac” to automatically enter your computer’s MAC address.
Static IP Address	Input the IP address assigned by your ISP here.
Subnet Mask	Input the subnet mask assigned by your ISP here.
Default Gateway Address	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
MAC Address	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.
DNS Address	Select “Obtain an IP address automatically” or “Use the following IP address”. Check with your ISP if you are unsure.
DNS 1,2 & 3	Enter the DNS address(es) assigned by your ISP here.
DNS Proxy	Enable or disable a DNS proxy server.
DNS Proxy Rules (URL)	When DNS proxy is enabled, enter the URL of a DNS proxy server.
User ID	Input the user name assigned by your ISP here.
Password	Input the password assigned by your ISP here.
L2TP Gateway	Input the L2TP gateway assigned by your ISP here.
Connection ID	Specify a reference name/ID for the connection.
MTU	Enter the maximum transmission unit (MTU) value of your network connection. The default value is 1392.
Connection Type	Specify a connection type: 1. “Continuous”: Connected all the time. 2. “Connect on Demand”: Connect when you initiate an Internet connection. 3. “Manual”: Connect/disconnect manually using the “Connect” and “Disconnect” buttons.
Idle Time Out	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.



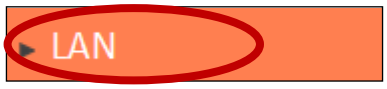
Enable/Disable	Enable or disable DDNS
Provider	Select DDNS service provider.
Domain Name	Enter the domain name provided by the DDNS provider.
Account/Email	Please enter the DDNS registration account/email.
Password/Key	Enter the DDNS service password/key.

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/*

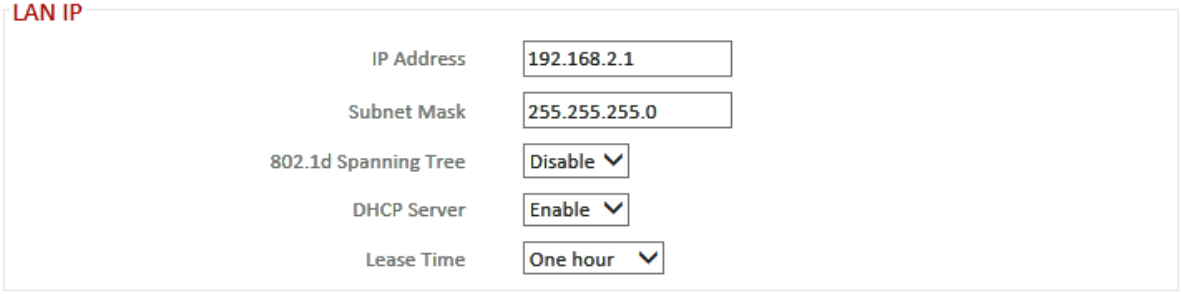
ZoneEdit	*http://www.zoneedit.com*
CyberGate	*http://cybergate.planex.co.jp/ddns/*
NS2GO	*http://www.ns2go.com/*
NO-IP	*http://www.noip.com/*

III-3-4. LAN



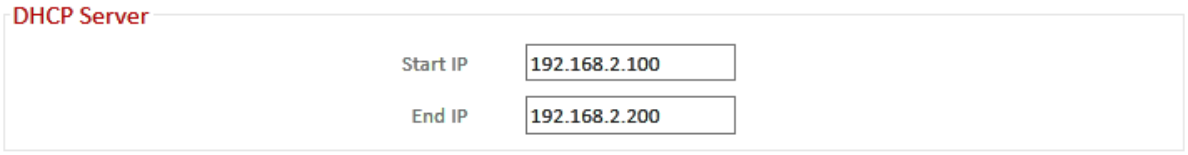
You can configure your Local Area Network (LAN) on this page. You can enable the router to dynamically allocate IP addresses to your LAN clients, and you can modify the IP address of the device. The device's default IP address is 192.168.2.1.

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



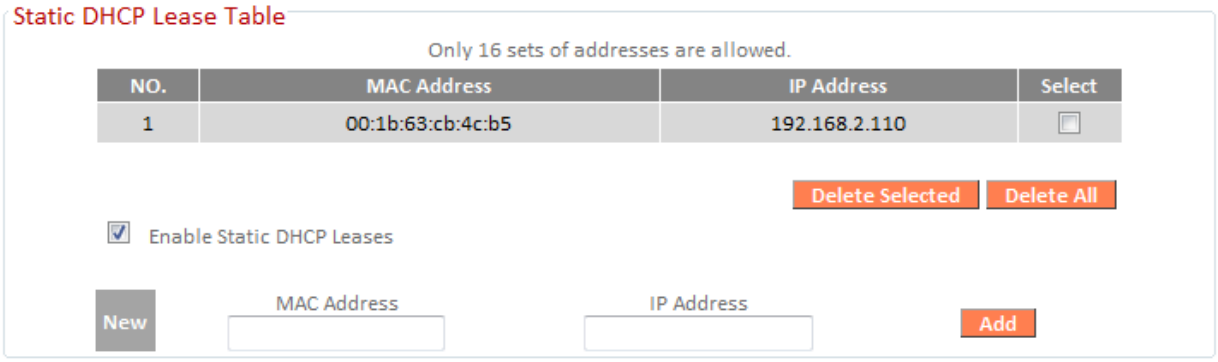
IP Address	Specify the IP address here. This IP address will be assigned to the BR-6288ACL V2 and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
802.1d Spanning Tree	Select "Enable" or "Disable" to enable/disable 802.1d Spanning Tree. This creates 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.
DHCP Server	Enable or disable the DHCP server.
Lease Time	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.



Start IP	Enter the start IP address for the DHCP server's IP address leases.
End IP	Enter the end IP address for the DHCP server's IP address leases.

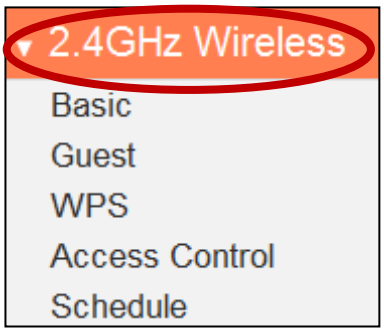
Your device's DHCP server can be configured to assign static (fixed) IP addresses to specified network devices, identified by their unique MAC address.

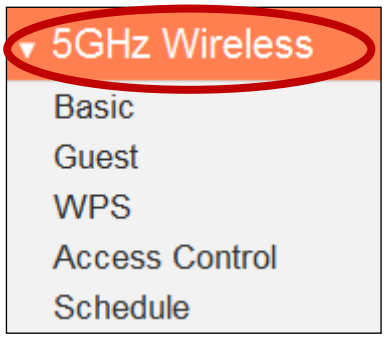


Enable Static DHCP Leases	Enable/disable static DHCP leases. This must be enabled in order to assign any network device a static IP address.
MAC Address	Enter the specified network device's MAC address here.
IP Address	Assign a fixed IP address for the specified network device here.
Add	Add the information to the "Static DHCP Leases Table".
Clear	Clear the MAC address and IP address fields.
Delete Selected / Delete All	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 theBR-6288ACL V2 to obtain an IP address automatically or you can specify an IP address.

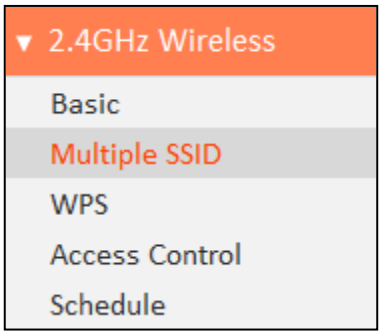
III-3-5. 2.4GHz Wireless & 5GHz Wireless

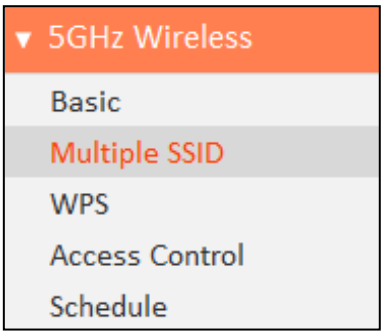




The "2.4GHz Wireless" & "5GHz Wireless" menu allows you to configure SSID and security settings for your Wi-Fi network along with a guest Wi-Fi network. WPS, access control and scheduling functions can also be managed from here.

Access Point Mode:

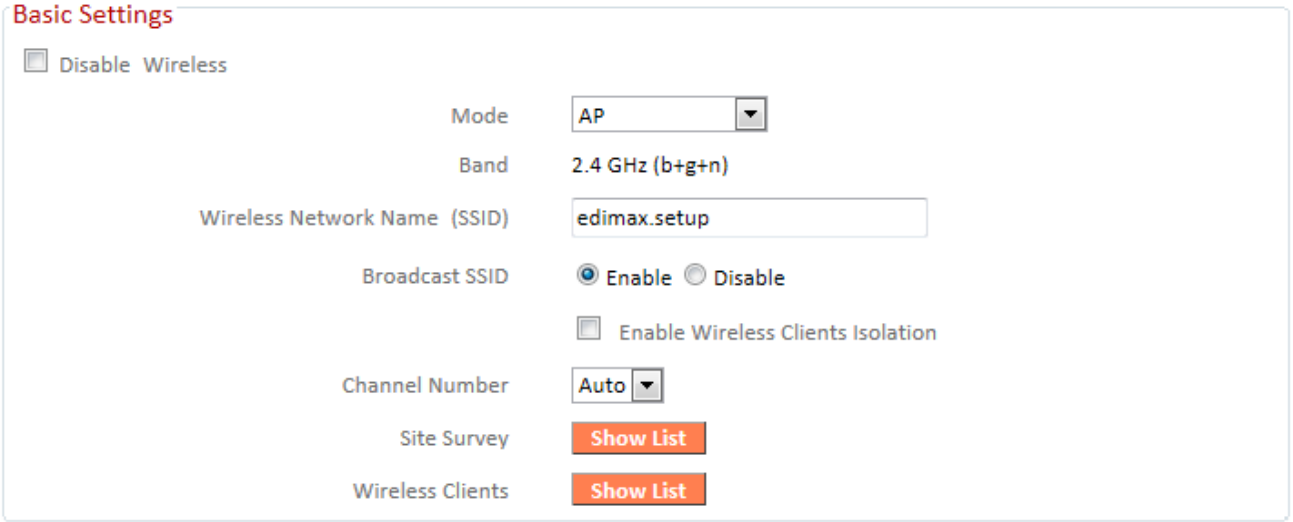




In Access Point mode, the "Guest" feature in the menu is replaced by "Multiple SSID".

III-3-5-1. Basic

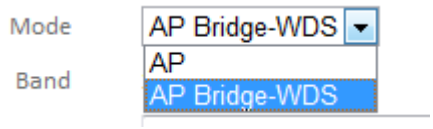
The "Basic" screen displays settings for your primary 2.4GHz or 5GHz Wi-Fi network.



Disable Wireless	Check the box to disable the wireless function of your device.
Mode	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).
Band	Displays the wireless standard used for the BR-6288ACL V2’s “2.4GHz (B+G+N)” means that 802.11b, 802.11g, and 802.11n wireless clients can connect to the BR-6288ACL V2.
Wireless Network Name (SSID)	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 alphanumerical characters.
Broadcast SSID	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.
Enable Wireless Clients Isolation	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL V2 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.
Channel Number	Select a wireless radio channel or use the default “Auto” setting from the drop-down menu.
Site Survey	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.
Wireless Clients	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.

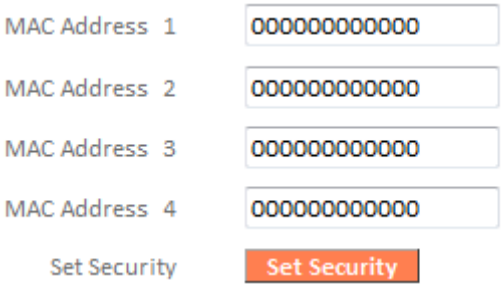
AP Bridge-WDS:



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

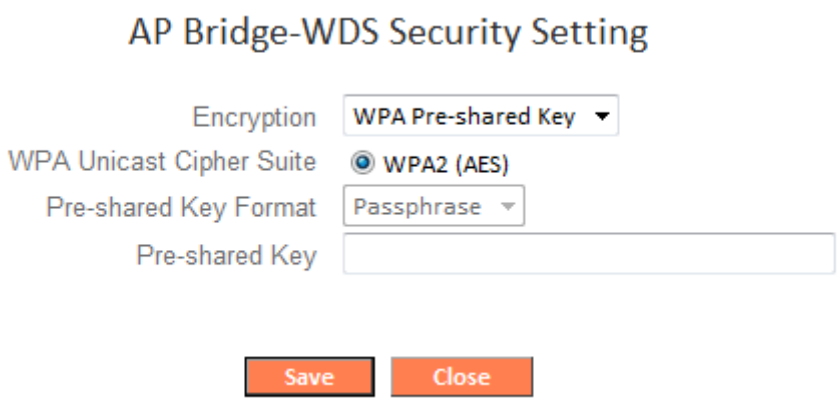
When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

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



MAC Address 1 - 4	Enter the correct MAC address for other access points in WDS mode.
Set Security	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.

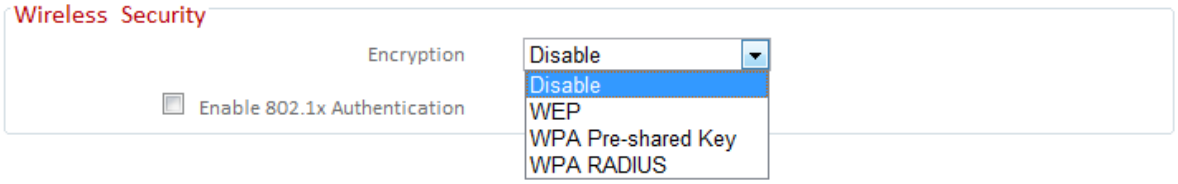


Wireless Security:

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.

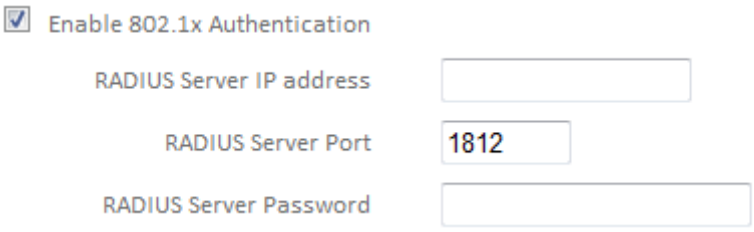


III-3-5-1-1. Disable

Encryption is disabled and no password/key is required to connect to the BR-6288ACL V2.

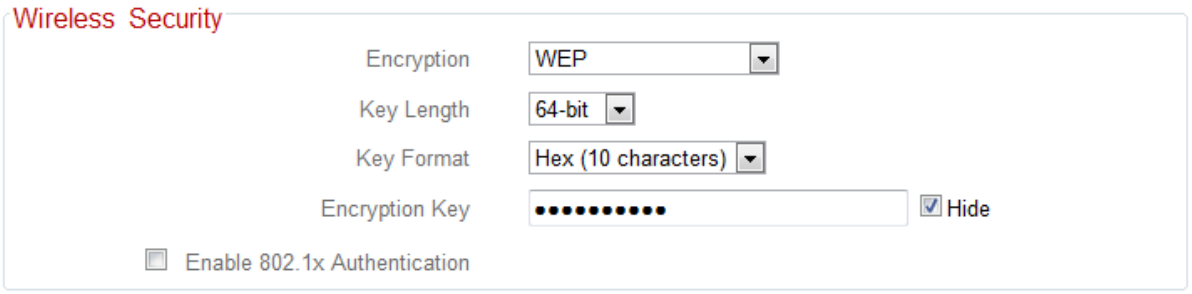
Disabling wireless encryption is not recommended. When disabled, anybody within range can connect to your device's SSID.

Enable 802.1x Authentication	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).

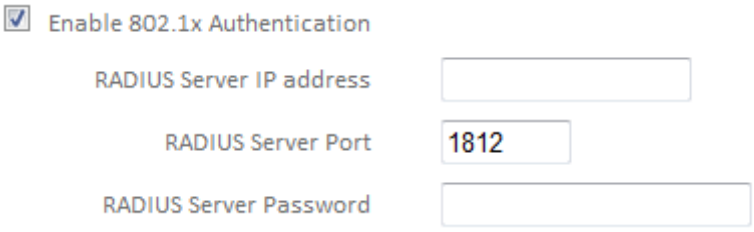


III-3-5-1-2. WEP

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

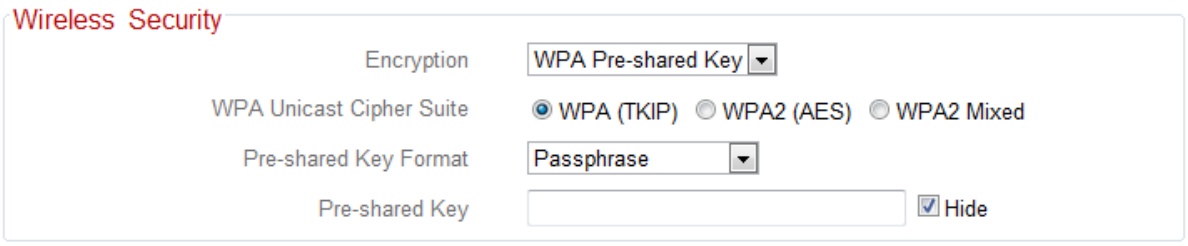


Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit.
Key Format	Choose from “ASCII” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Encryption Key	Enter your encryption key/password according to the format you selected above. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.
Enable 802.1x Authentication	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).



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

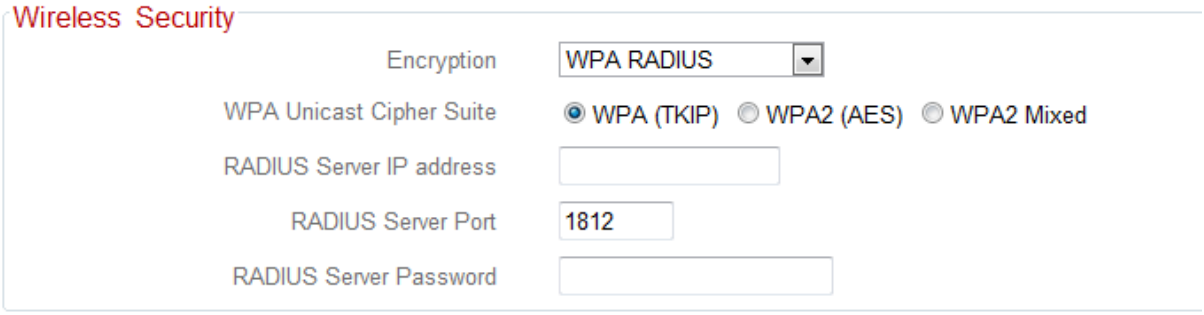
WPA pre-shared key is the recommended and most secure encryption type.



WPA Unicast Cipher Suite	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).
Pre-shared Key Format	Choose from “Passphrase” (8-63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).
Pre-shared Key	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.



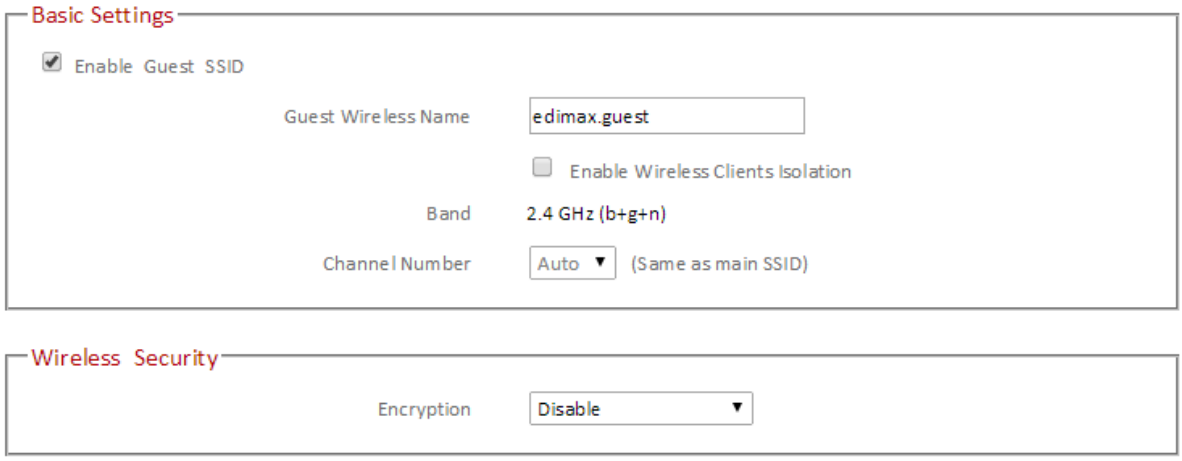
WPA Unicast Cipher Suite	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP), but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
RADIUS Server IP address	Input the IP address of the RADIUS authentication server here.
RADIUS Server Port	Input the port number of the RADIUS authentication server here. The default value is 1812.
RADIUS Server Password	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 V2 supports up to four additional SSIDs for each wireless band in access point mode.



Enable Guest SSID	Check/uncheck the box to enable/disable the guest Wi-Fi network.
Wireless Guest Name	Enter a reference/ID name for your guest wireless network.
Enable Wireless Clients Isolation	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL V2 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.
Band	Displays the wireless standard used for the BR-6288ACL V2’s frequency band: 2.4GHz (B+G+N): Allows 802.11b, 802.11g, and 802.11n wireless clients to connect to the

	BR-6288ACL V2.
Channel Number	Channel number for the guest network is the same as the main SSID and cannot be adjusted independently.

Encryption	Please refer to ***III-3-5-1. Basic: Wireless Security*** for details about security settings.

WPA RADIUS encyrption type is not available for the guest network.

MULTIPLE SSID:

The BR-6288ACL V2 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	☑	edimax.1	0	Disable	80:1F:02:ED:F2:D2
2	☑	edimax.2	0	WPA2 (AES)	80:1F:02:ED:F2:D3
3	☑	VLAN	1	WPA2 (AES)	80:1F:02:ED:F2:D4
4	☐	edimax.4	0	Disable	80:1F:02:ED:F2:D5

Multiple SSID Basic Settings

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

Wireless Network Name (SSID): edimax.1

☑ Enable Multiple SSID

☐ Enable Wireless Clients Isolation

Band: 2.4 GHz (b+g+n)

Channel Number: Auto (Same as main SSID)

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

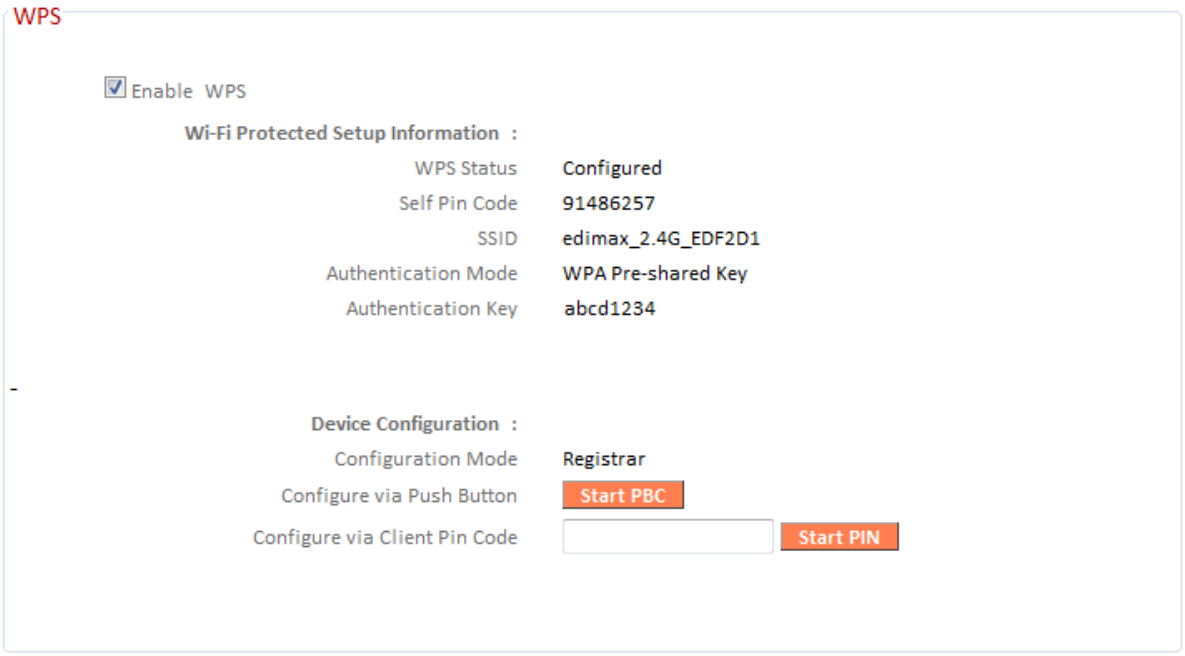
Multiple SSID	Use the drop down menu to select which SSID (numbered 1 – 4) to configure.
Wireless Network Name (SSID)	Enter a reference/ID name to separate your wireless network.

Enable Multiple SSID	Check/uncheck this box to enable/disable the specified SSID. Must be checked for the SSID to function.
Enable Wireless Clients Isolation	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the BR-6288ACL V2 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.
Band	Displays the wireless standard used for the BR-6288ACL V2's frequency band: 2.4GHz (B+G+N): Allows 802.11b, 802.11g, and 802.11n wireless clients to connect to the BR-6288ACL V2.
Channel Number	Channel number for the guest network is the same as the main SSID and cannot be adjusted independently.
VLAN ID	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.



Enable WPS	Check/uncheck this box to enable/disable WPS.
WPS Status	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.
Self PIN Code	Displays the WPS PIN code of the device.
SSID	Displays the SSID of the device.
Authentication Mode	Displays the wireless security authentication mode of the device.
Authentication Key	Displays the wireless security authentication key.
Configuration Mode	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

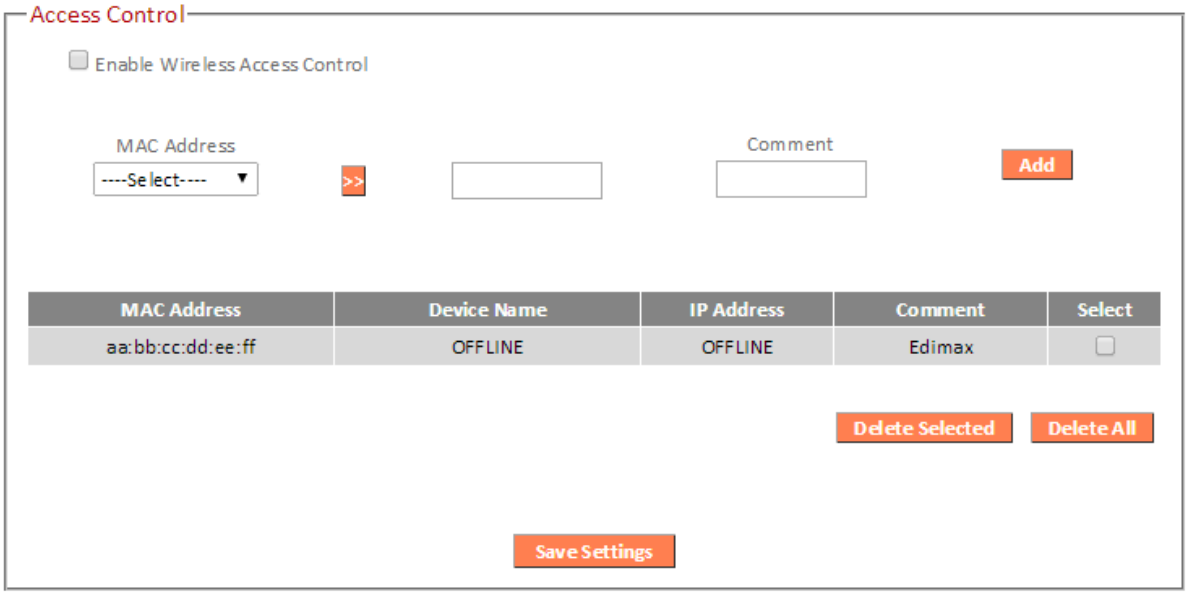
	to and the wireless client(s) will follow the device's wireless settings.
Configure via Push Button	Click "Start PBC" (Push-Button Configuration) to activate WPS on the access point. WPS will be active for 2 minutes.
Configure via Client PIN Code	Enter the wireless client's PIN code here and click "Start 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.

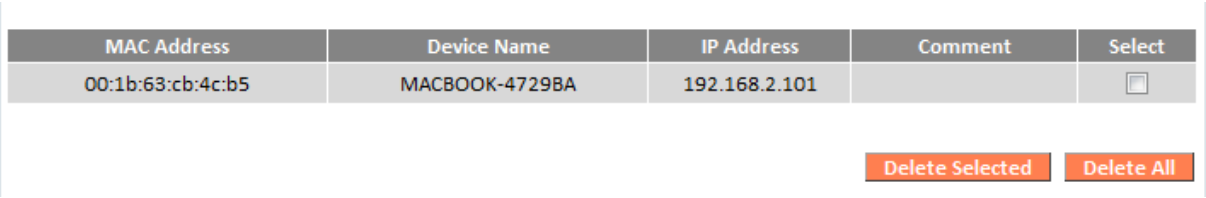
This function allows you to define a list of network devices permitted to connect to the BR-6288ACL V2. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the BR-6288ACL V2, it will be denied.

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



MAC address	Select a PC name from the drop-down list and click “>>” to add enter it into the blank field to the right. 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. 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’.
Comment	Enter a comment for reference/identification consisting of up to 16 alphanumerical characters.
Add	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.

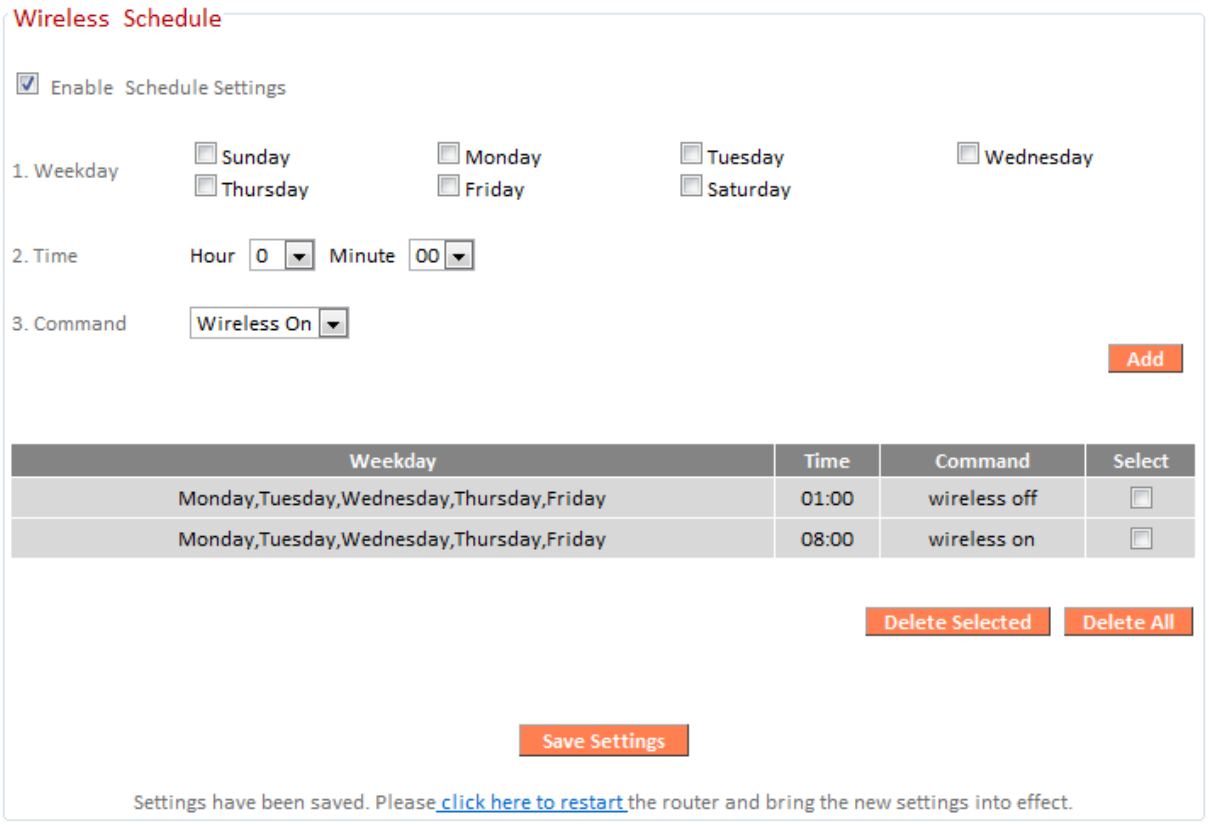


Delete Selected / Delete All	Delete selected or all entries from the table.

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 V2 must remain connected to the Internet and use an NTP server for the schedule feature to function correctly.



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

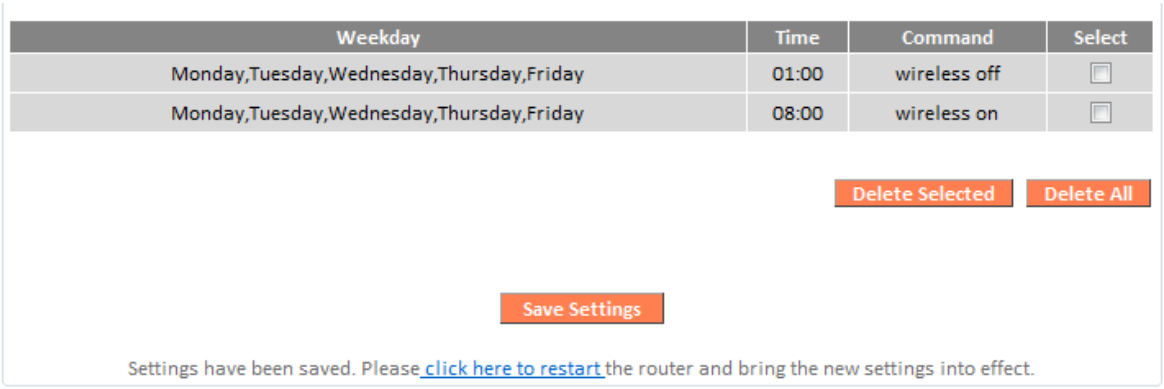
1. Use the checkboxes to select which day(s) to include in the schedule.

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”.

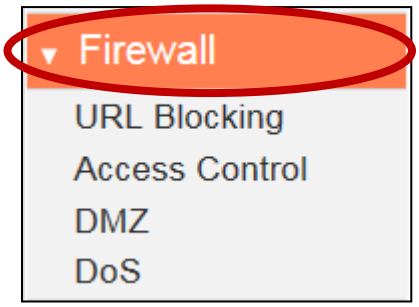
Add	Add the schedule to the table of active schedules.

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



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.

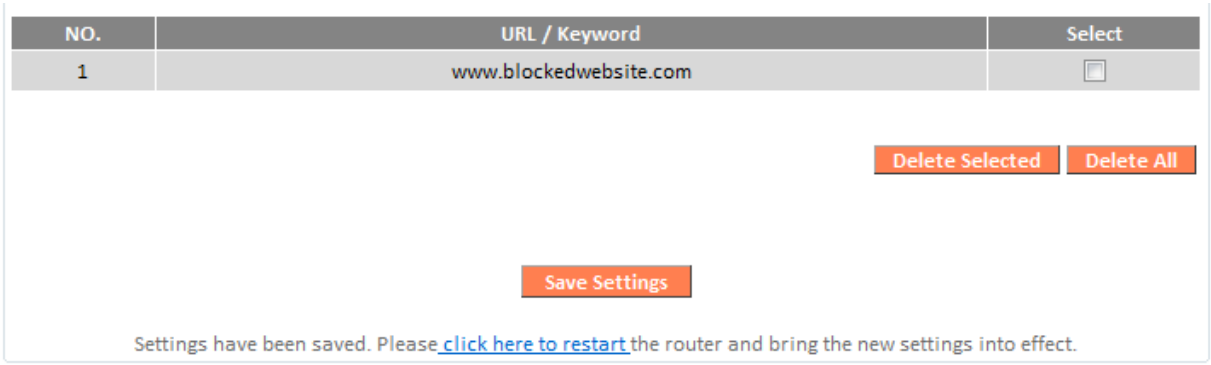
SPI firewall	Enable or disable the Stateful Packet Inspection (SPI) firewall.

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/Keyword	Enter the URL or keyword to be blocked.
Add	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.



Delete Selected / Delete All	Delete selected or all entries from the table.

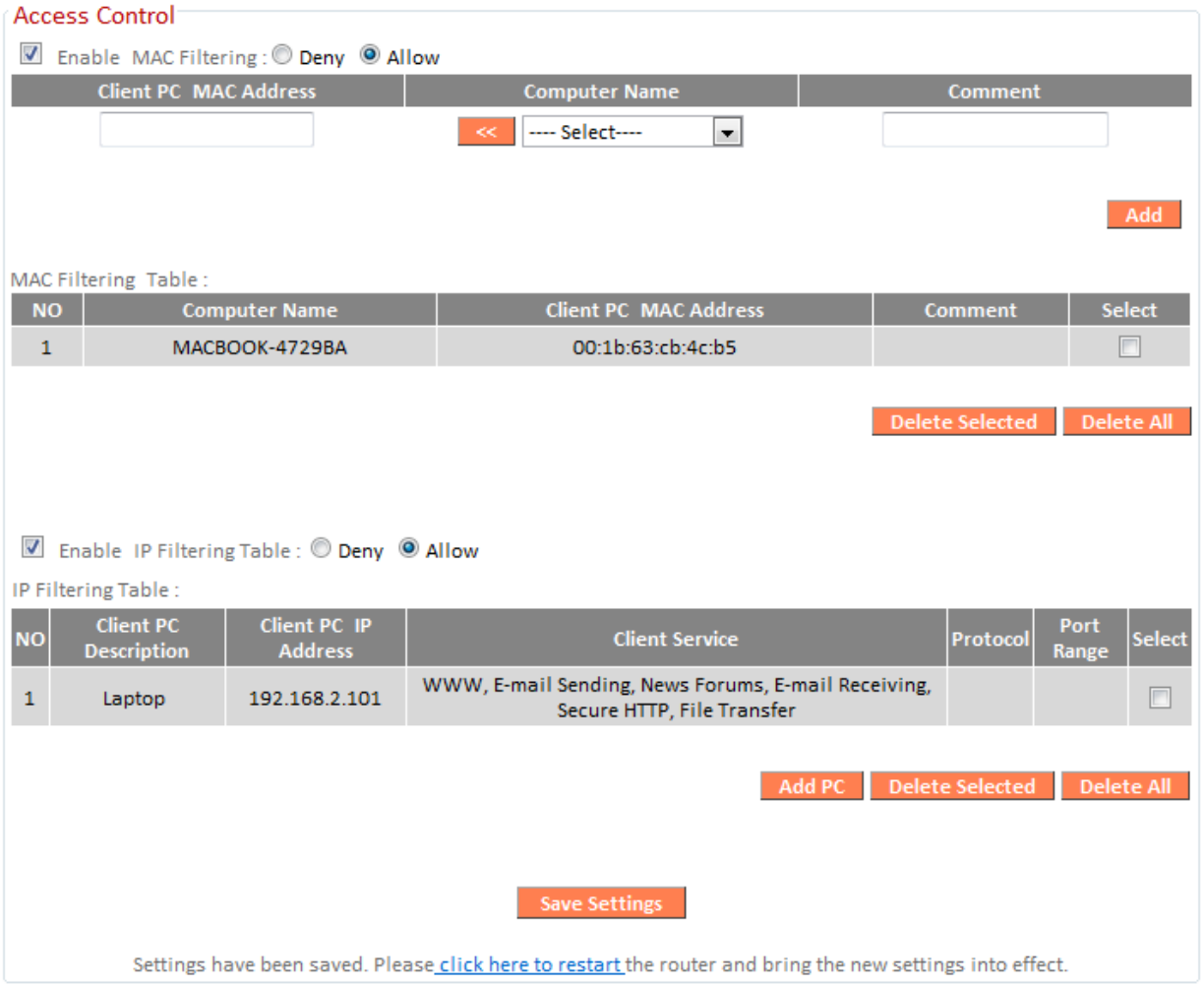
III-3-6-2. Access Control

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 V2. Devices are each identified by their unique MAC address or IP address. Specific services can also be allowed/denied for IP addresses.

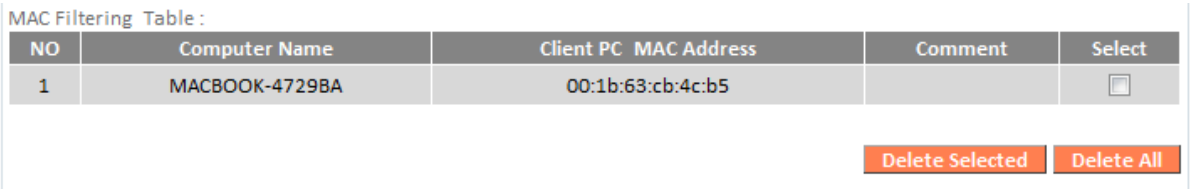
Check/uncheck the “Enable MAC Filtering” and/or “Enable IP Filtering” box to enable/disable MAC filtering and/or IP filtering.



MAC Filtering:

Enable MAC Filtering	Check the box to enable MAC filtering and select whether to “Deny” or “Allow” access for specified MAC address.
Client PC MAC Address	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’.
Computer Name	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.
Comment	Enter a comment for reference/identification consisting of up to 16 alphanumerical characters.
Add	Click “Add” to add the MAC address to the MAC address filtering table.

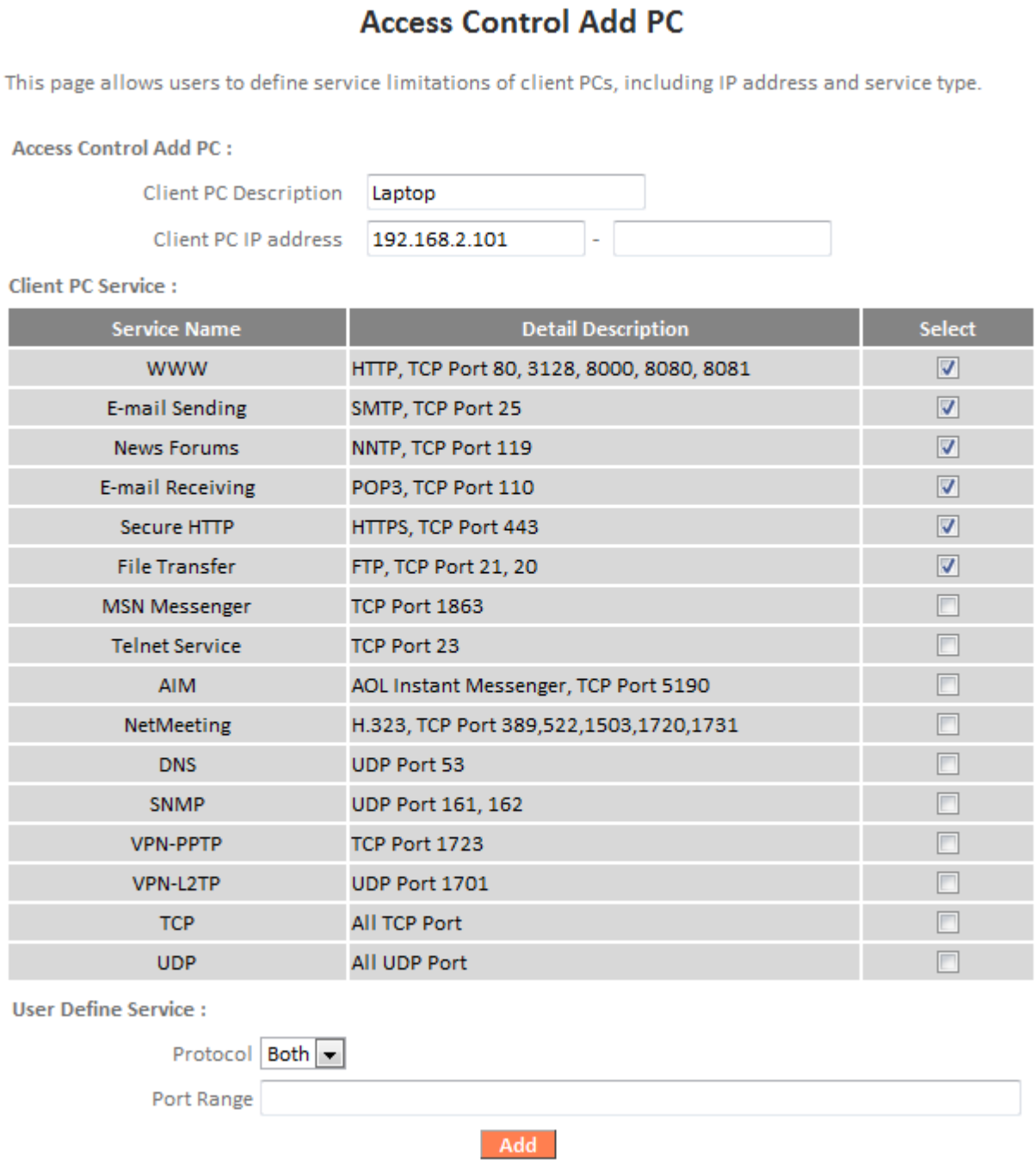
MAC address entries will be listed in the table as shown below. Select an entry using the “Select” checkbox.



Delete Selected / Delete All	Delete selected or all entries from the table.

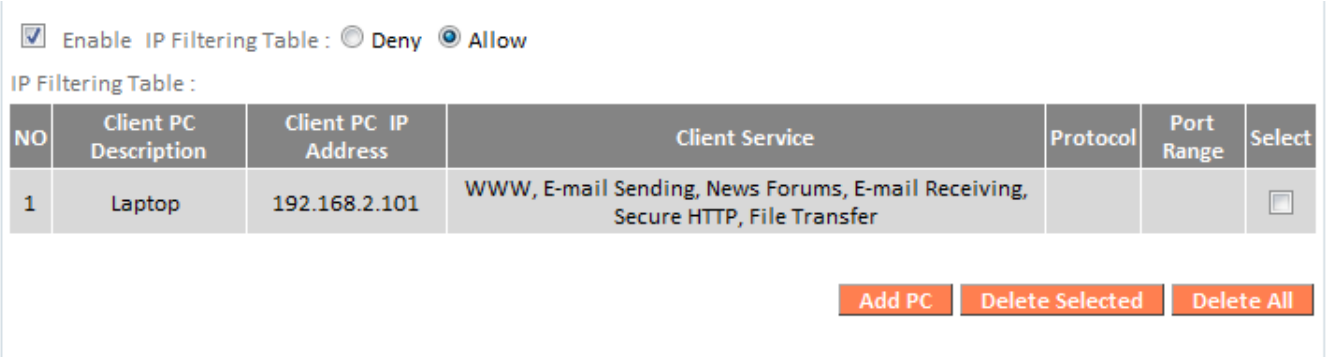
IP Filtering:

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



Client PC Description	Enter a description for reference/identification of up to 16 alphanumeric characters.
Client PC IP address	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.
Service Name	Various services are listed here with a short description. Check/uncheck the box for each service you wish to select.
Protocol	Select protocol “TCP” or “UDP” or “Both” for a service not included in the “Client PC Service” list.
Port Range	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.
Add	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.

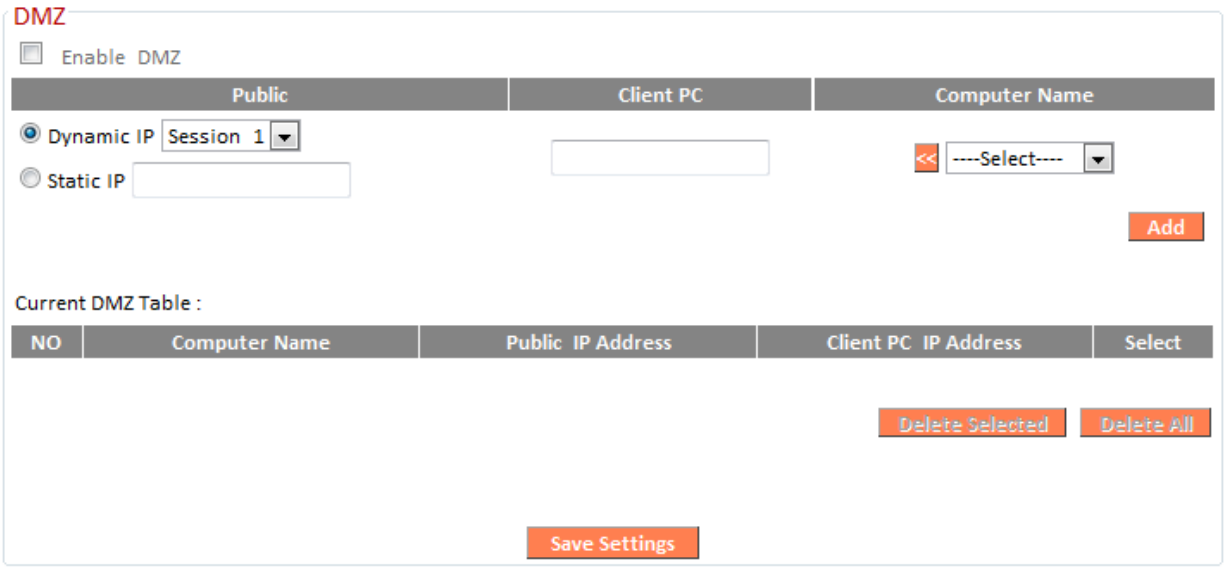


Delete Selected / Delete All	Delete selected or all entries from the table.

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.



Enable DMZ	Check/uncheck the box to enable/disable the device's DMZ function.
Public	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.
Client PC	Enter the private IP address that the internet IP address will be mapped to.
Computer Name	Select a computer name from the list and click "<<"

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

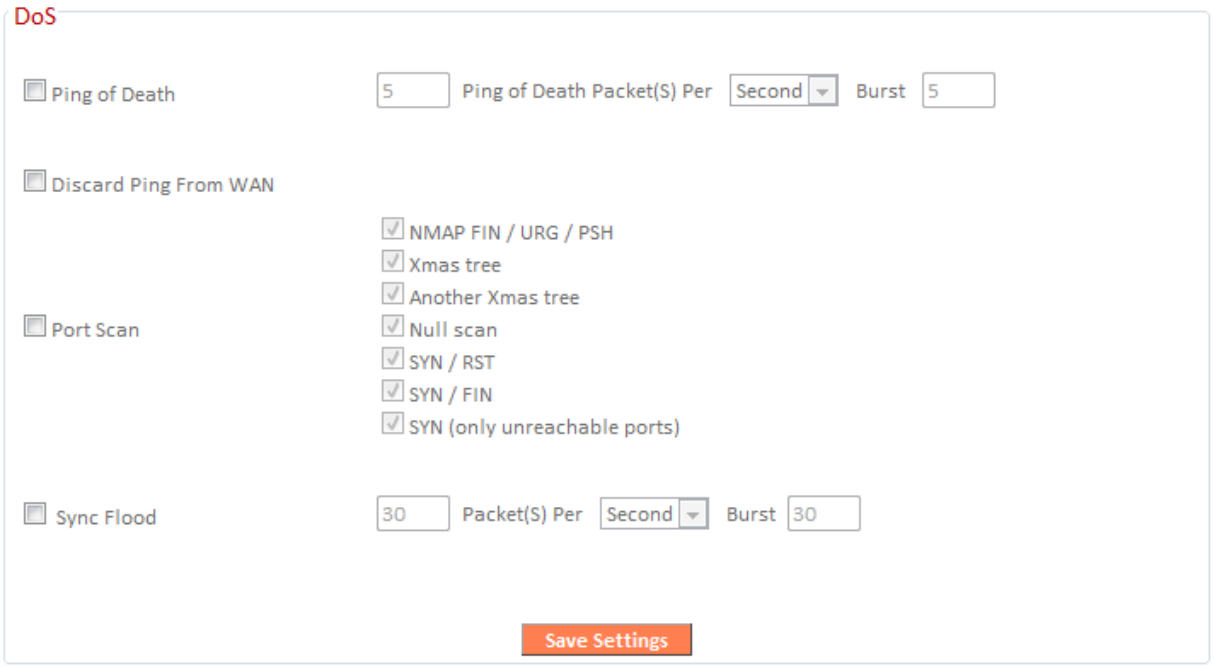
DMZ entries will be displayed in the table shown below:

Delete Selected / Delete All	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.



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

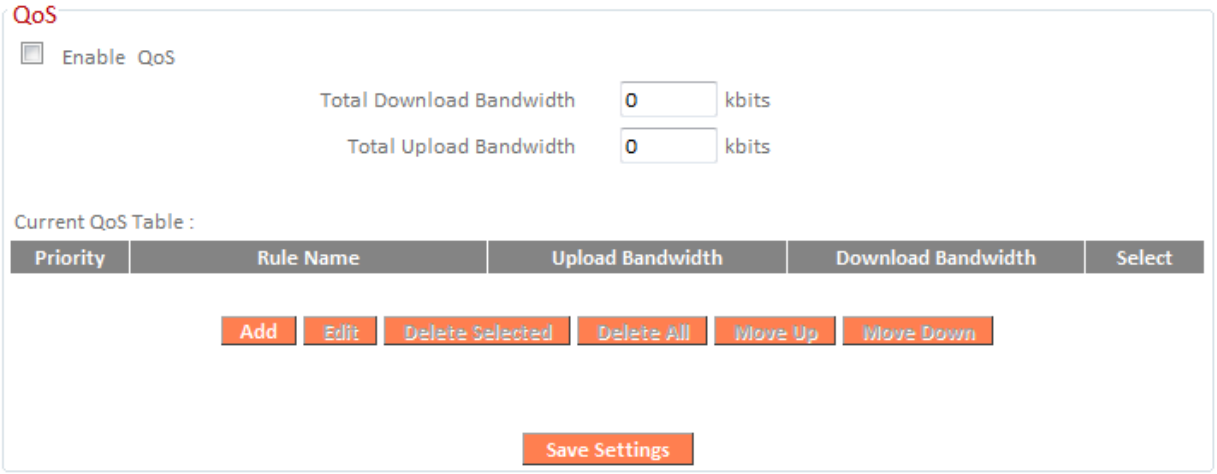
III-3-7. QoS (Quality of Service)

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.

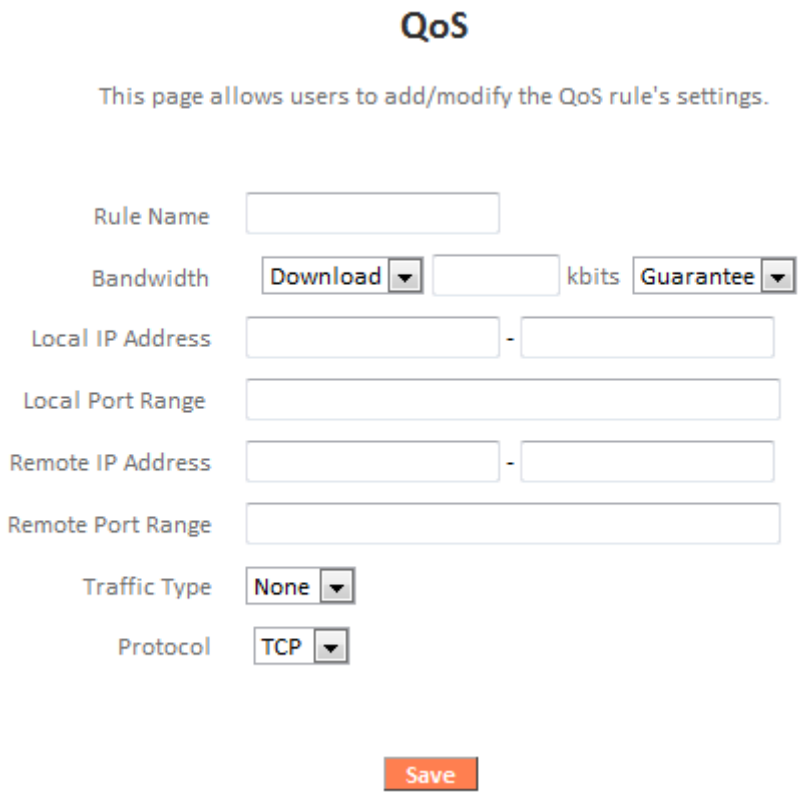
QoS can improve the BR-6288ACL V2's performance. QoS is recommended to optimize performance for online gaming.

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.



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



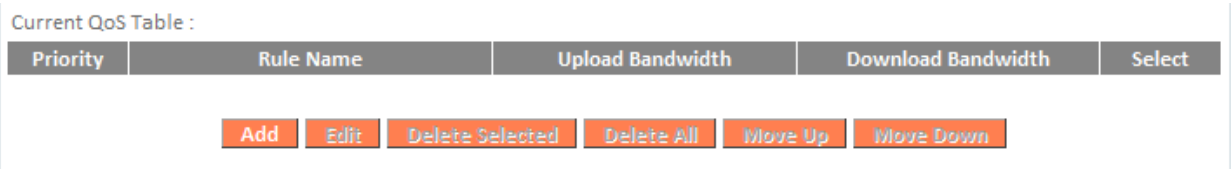
Rule Name	Enter a name for the QoS rule for reference/identification.
Bandwidth	Set the bandwidth limits for the QoS rule: (1) (2) (3) 1. Select “Download” or “Upload” for the QoS rule. 2. Enter the bandwidth limit. 3. Select whether the bandwidth is a “Guarantee” (minimum) or “Max” (maximum).
Local IP Address	Enter the IP address range to which the QoS rule will be applied. 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.

Local Port Range	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
Remote IP Address	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.
Remote Port Range	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
Traffic Type	Select traffic type as an alternative to specifying a port range above.
Protocol	Select a “TCP” or “UDP” protocol type.
Save	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.

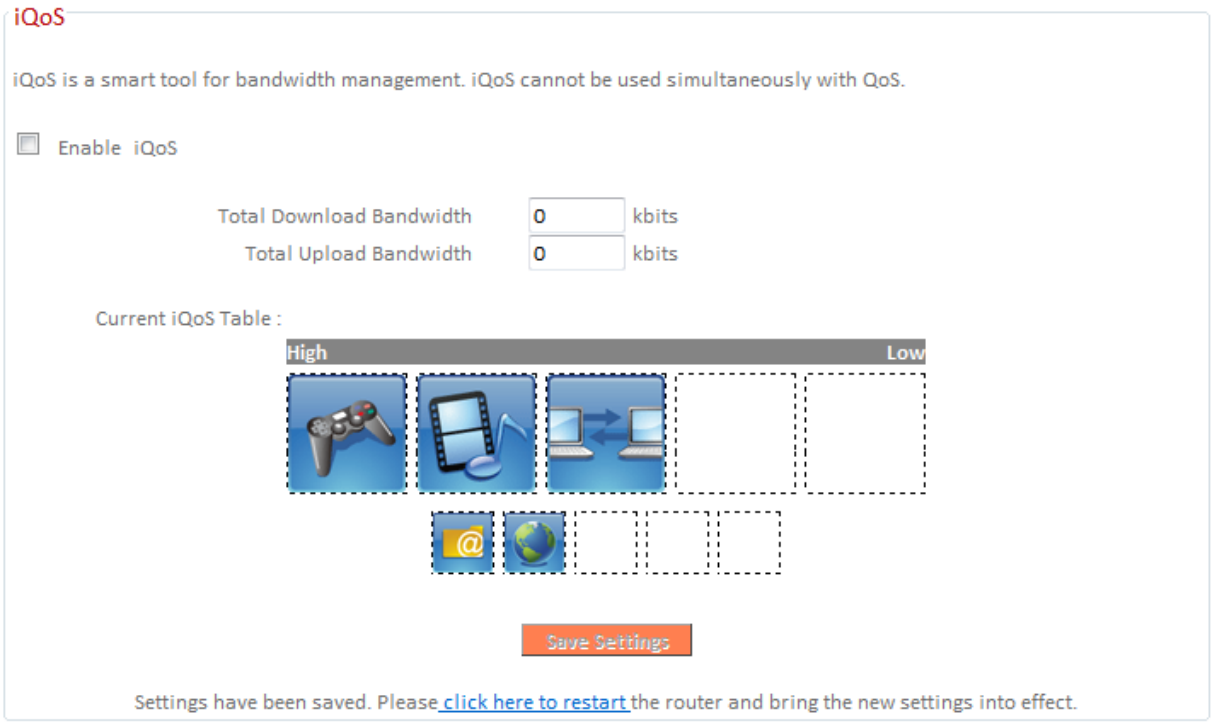


Edit	Edit a selected rule.
Delete Selected/ Delete All	Delete selected or all entries from the table.
Move Up/Down	Move selected rule up or down the list.

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.



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.

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

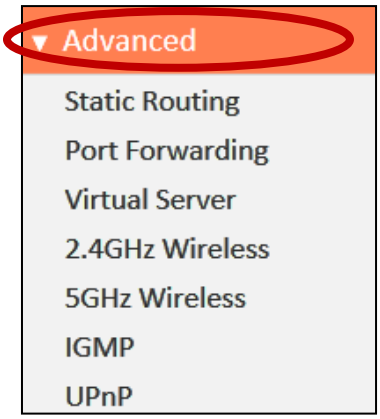
FTP

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

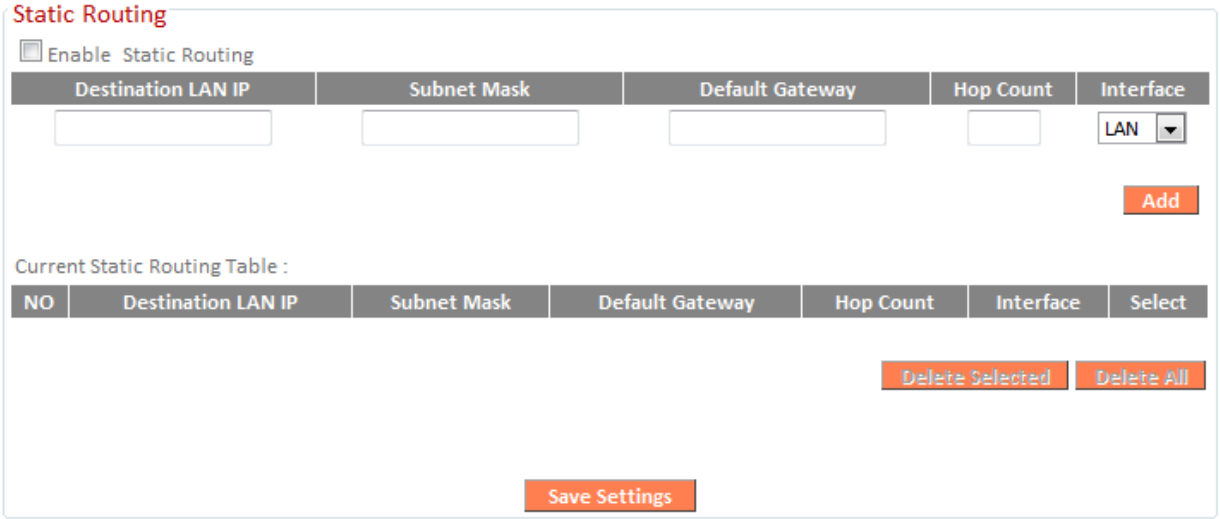


Advanced features of the BR-6288ACL V2 can be configured from the “Advanced” menu.

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.

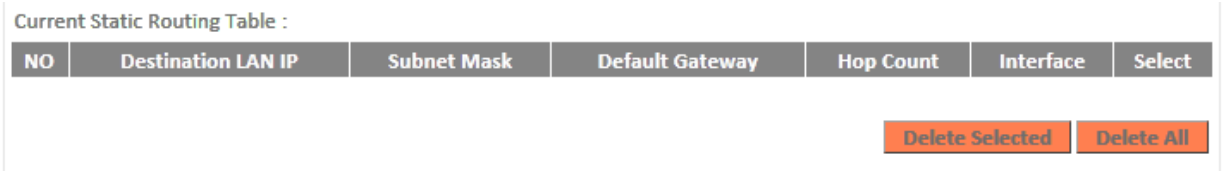
You can configure static routing and manually add routes to the routing table shown below.



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

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

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

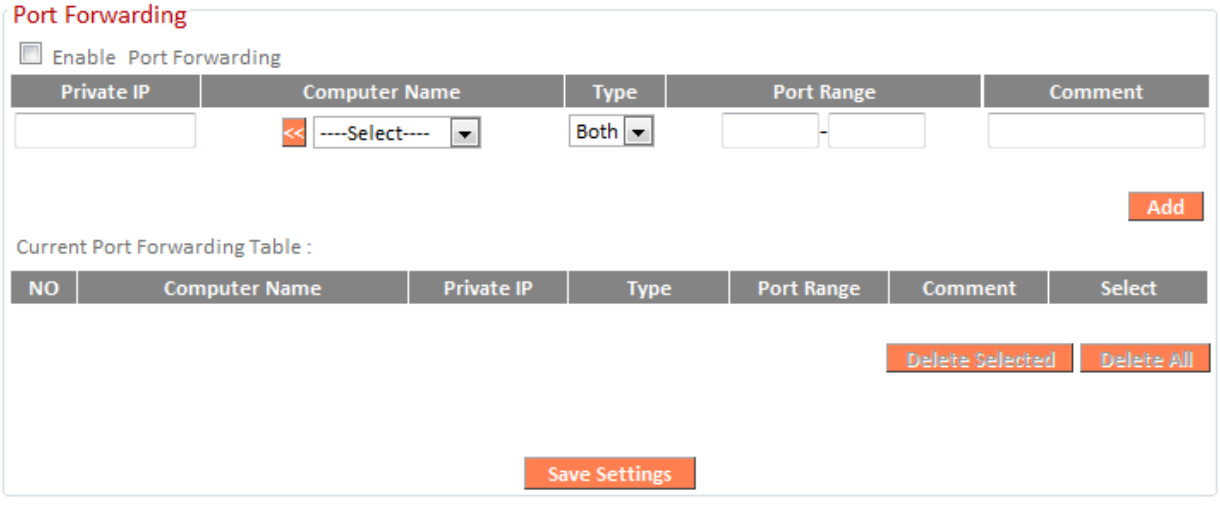


Delete Selected/ Delete All	Delete selected or all entries from the table.

III-3-8-2. Port Forwarding

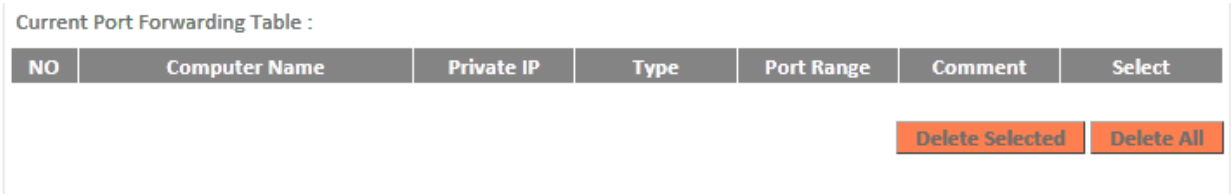
This function allows you to redirect a single port or consecutive ports of an Internet IP address to the same port of a local IP address. The port number(s) of the Internet IP address and local IP address must be the same.

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



Private IP	Enter the IP address of the computer on the local network.
Computer Name	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.
Type	Select the type of connection, “TCP”, “UDP” or “Both”.
Port Range	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.
Comment	Enter a comment for reference or identification.

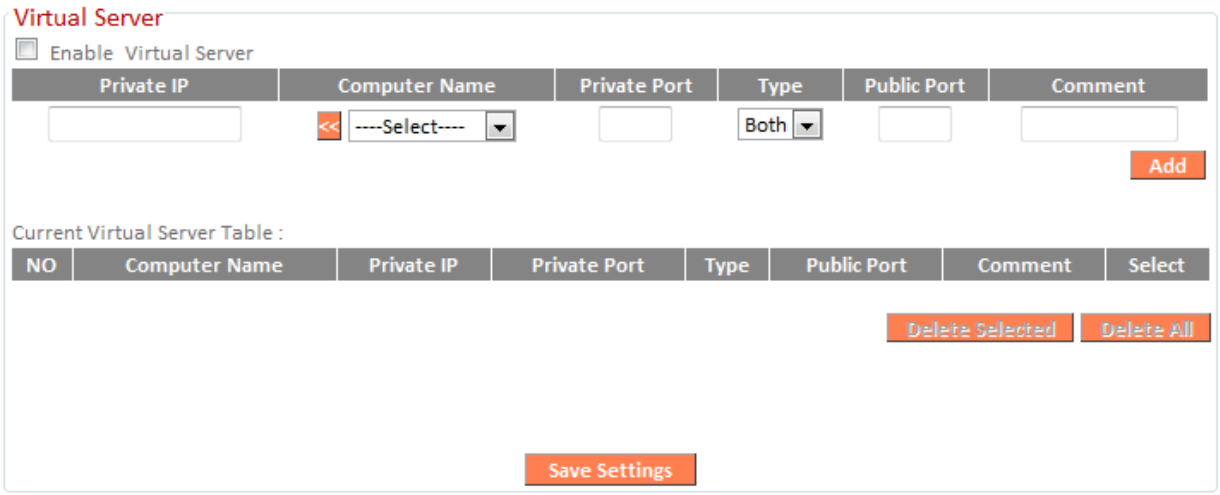
Port Forwarding Table entries will be displayed in the table shown below:



Delete Selected/ Delete All	Delete selected or all entries from the table.

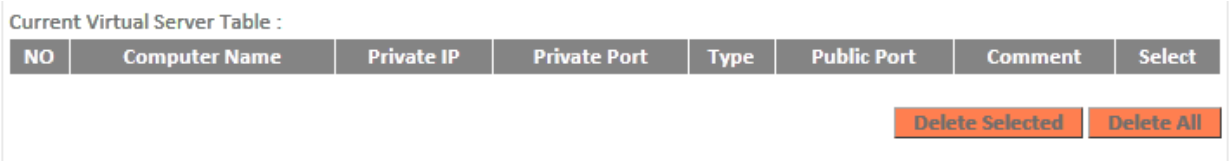
III-3-8-3. Virtual Server

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.



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

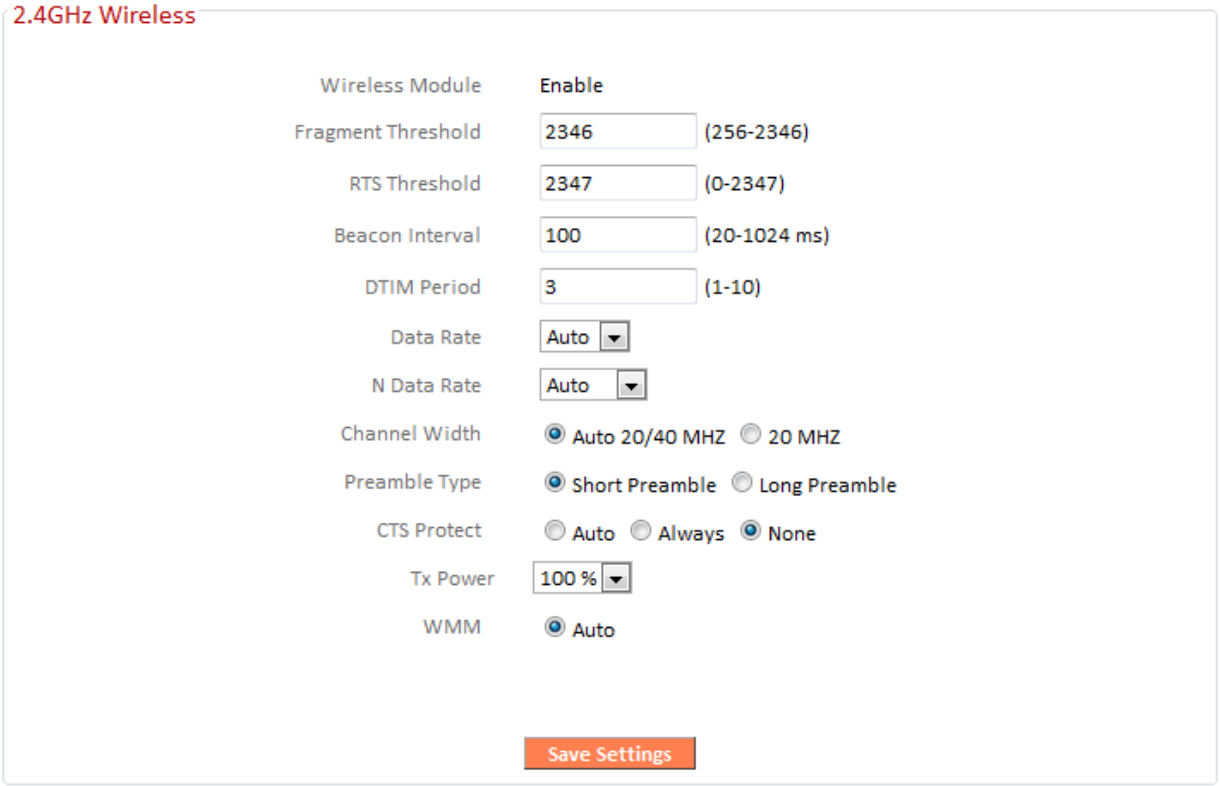
Current Virtual Table entries will be displayed in the table shown below:



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.

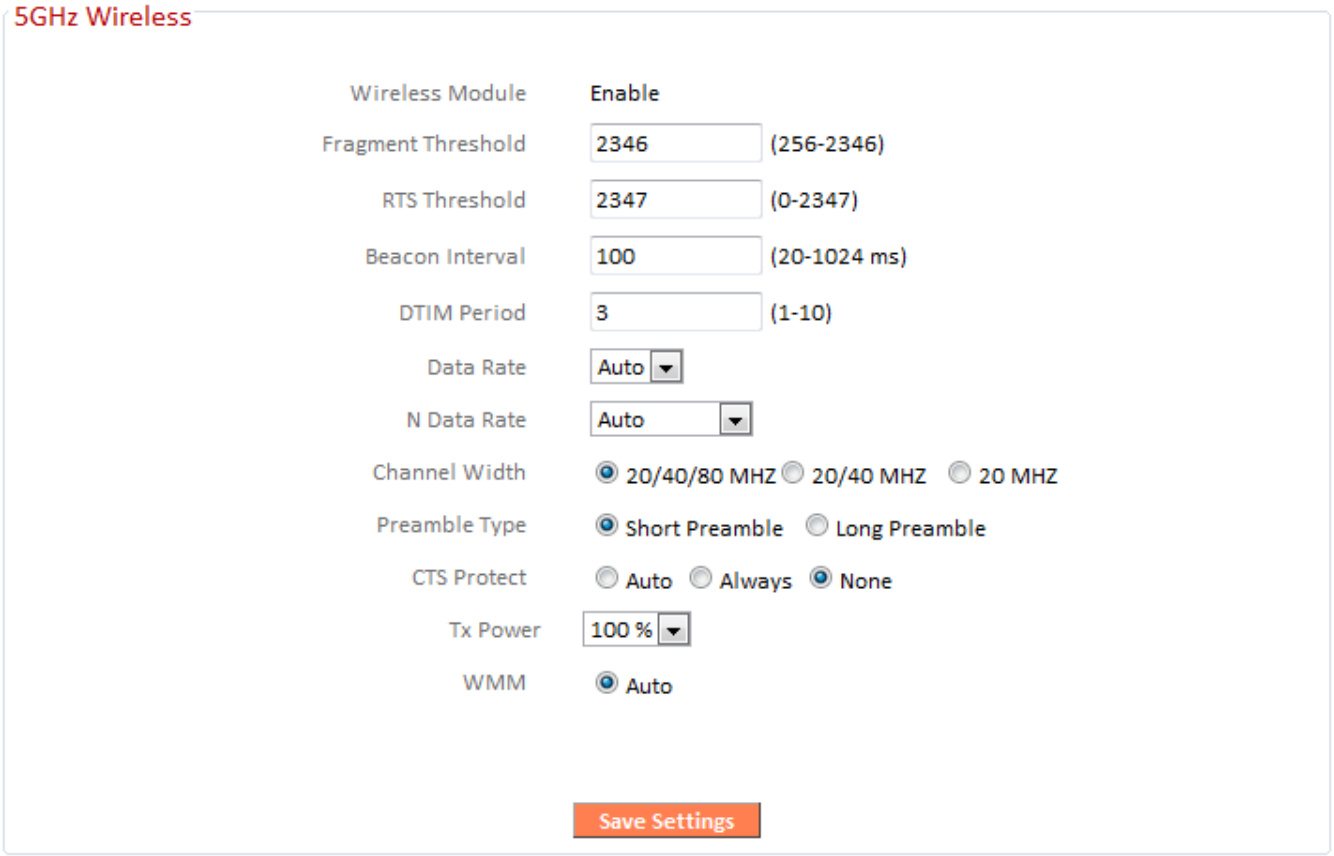


Fragment Threshold	Set the Fragment threshold of the wireless radio. The default value is 2346.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM period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

Channel Width	Select wireless channel width (bandwidth used by wireless signals from the device) – the recommended value is Auto 20/40MHz.
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble”.
CTS Protect	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”.
Tx Power	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.
WMM	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.

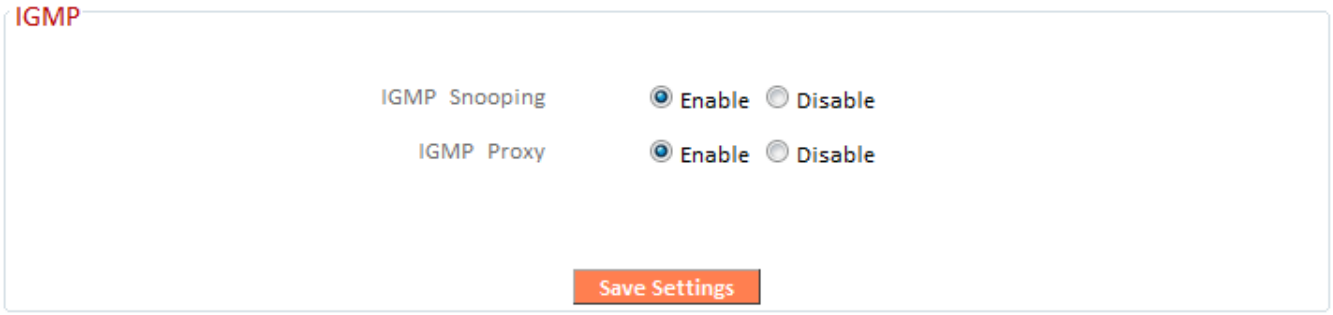


Fragment Threshold	Set the Fragment threshold of the wireless radio. The default value is 2346.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM period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

Channel Width	Select wireless channel width (bandwidth used by wireless signals from the device) – the recommended value is 20/40/80MHz.
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble”.
CTS Protect	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”.
Tx Power	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.
WMM	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.

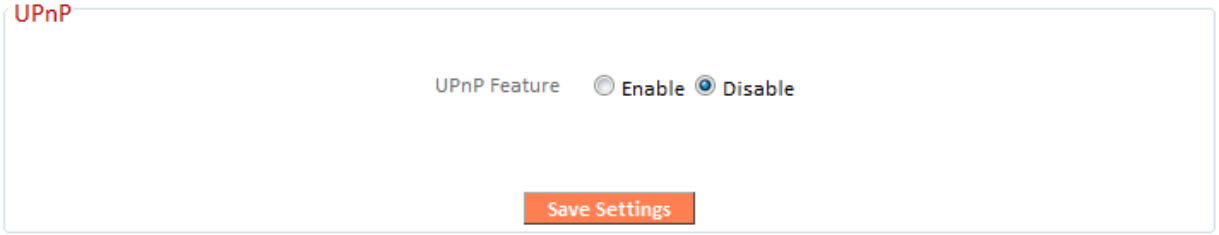


IGMP Snooping	IGMP snooping monitors traffic between hosts and multicast routers to facilitate bandwidth conservation. Select enable or disable.
IGMP Proxy	IGMP proxy enables intelligent multicast forwarding based on IGMP snooping information. Select enable or disable.

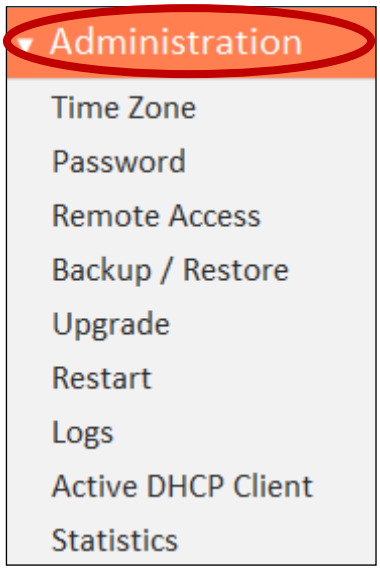
It is recommended to set "IGMP Snooping" and "IGMP Proxy" to "Enable".

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".

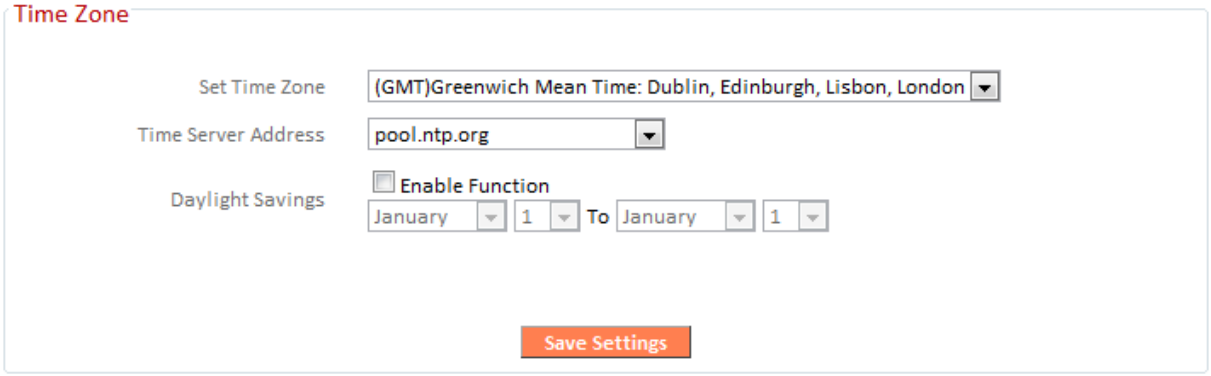


III-3-9. Administration



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

III-3-9-1. Time Zone

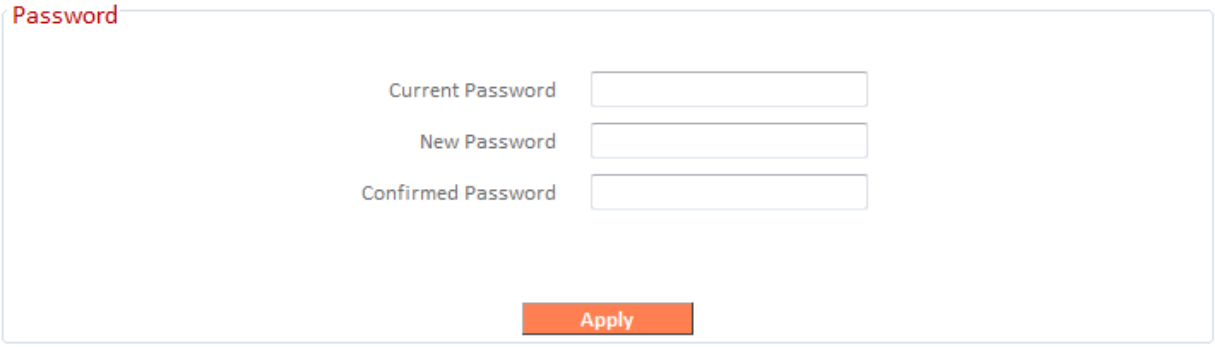


Set Time Zone	Select the time zone of your country or region.
Time Server Address	The travel router supports NTP (Network Time Protocol) for automatic time and date setup. Input the host name of the IP server manually.
Daylight Saving	If your country/region uses daylight saving time, please check the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

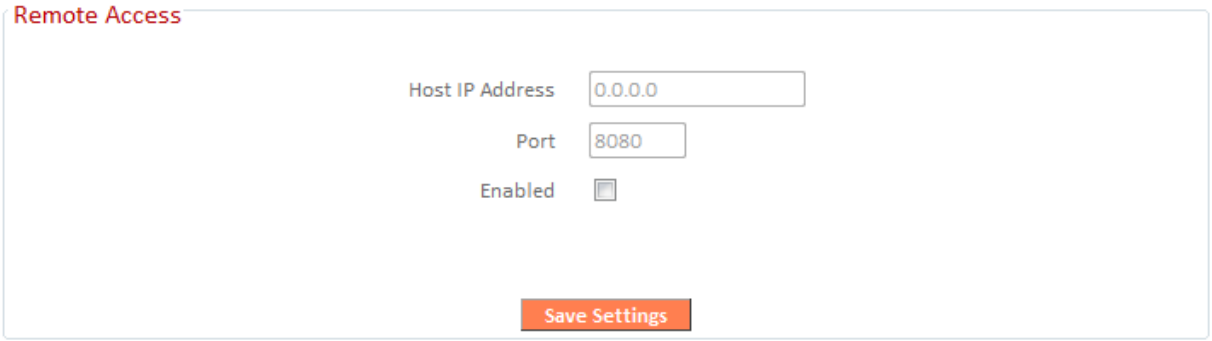
Please make a note of the new password. In the event that you forget the password and are unable to login to the browser based configuration interface, see II-7. Reset to factory default settings for how to reset the device.



Current Password	Enter your current password.
New Password	Enter your new password.
Confirmed Password	Confirm your new password.

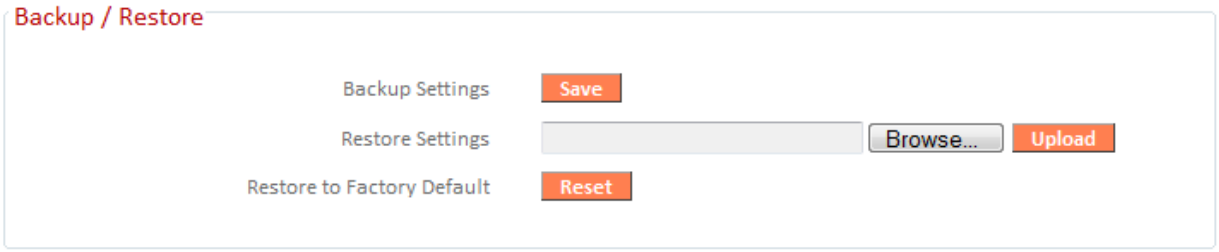
III-3-9-3. Remote Access

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



Host IP Address	Specify the IP address which is allowed remote access.
Port	Specify a port number used for remote ac cess.

III-3-9-4. Backup/Restore

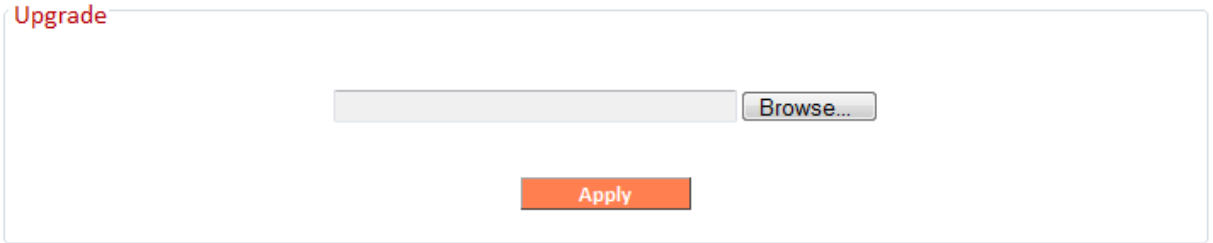


Backup Settings	Click “Save” to save the current settings on your computer as config.bin file.
Restore Settings	Click “Browse” to find a previously saved config.bin file and then click “Upload” to replace your current settings.
Restore to Factory Default	Click “Reset” to restore settings to the factory 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

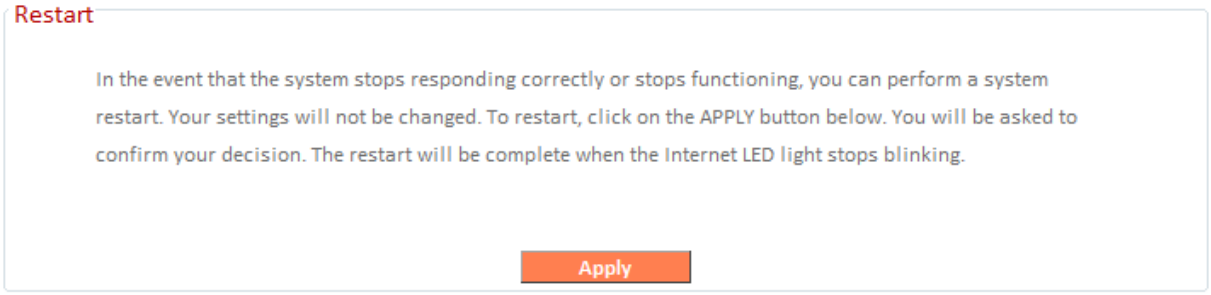
The upgrade page allows you to upgrade the system firmware to a more recent version. You can download the latest firmware from the Edimax website. After the upgrade, the system will restart.

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.



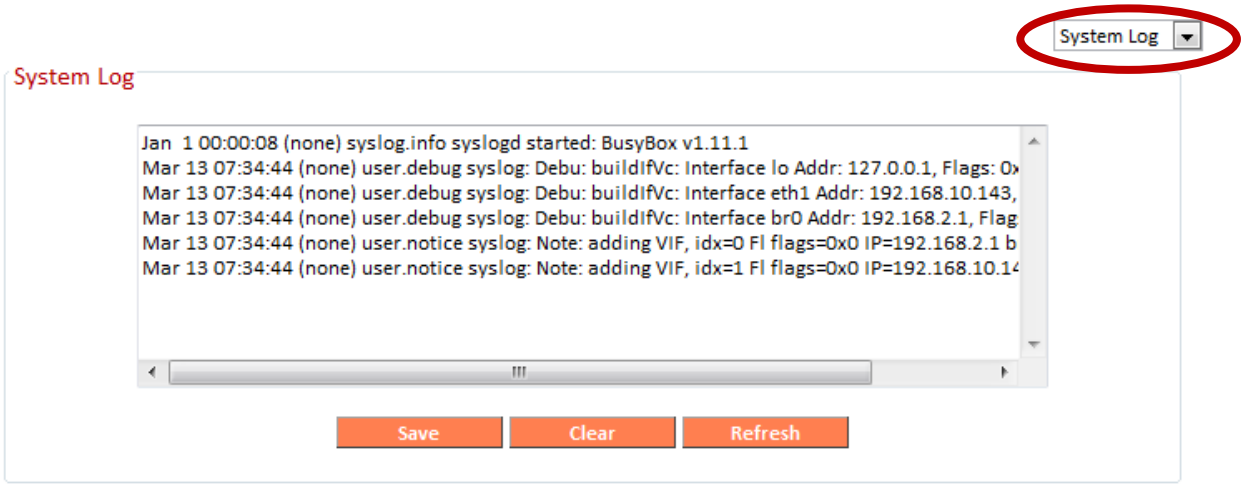
III-3-9-6. Restart

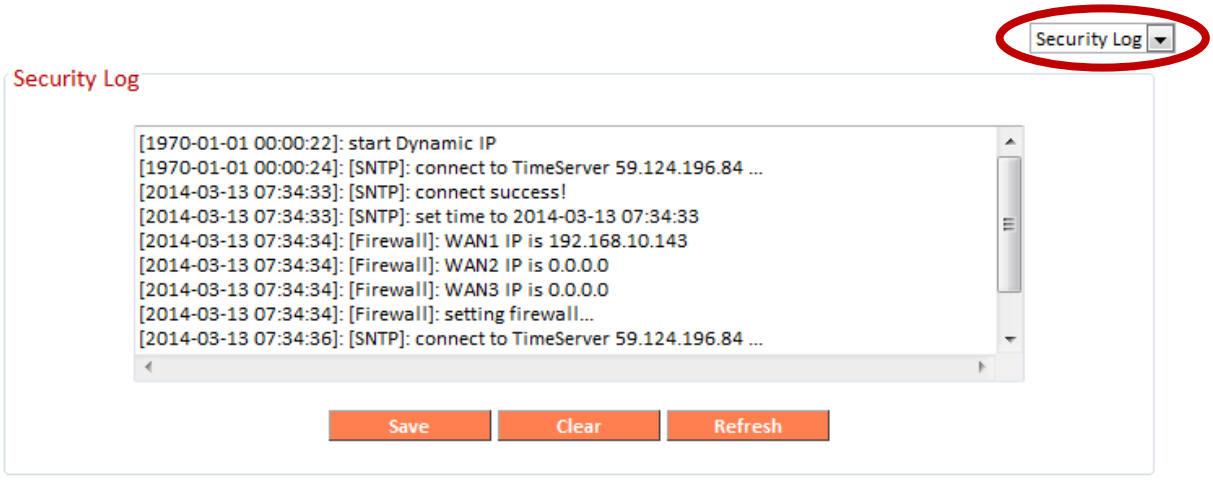
In the event that the router malfunctions or is not responding, then it is recommended that you restart the device.



III-3-9-7. Logs

You can view the system log and security log here. Use the drop down menu in the top-right corner to select which log to view.

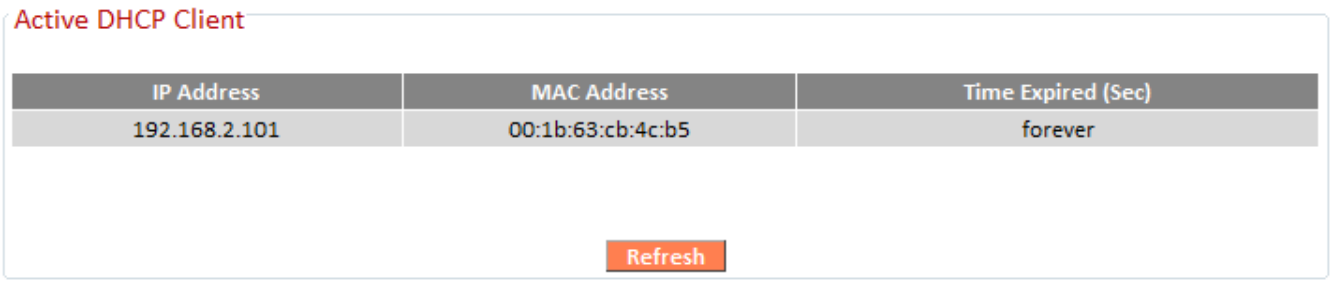




Save	Click “Save” to save the log on your computer as .txt file.
Clear	Click “Clear” to clear/erase the existing log.
Refresh	Click “Refresh” to refresh the log and update any activity.

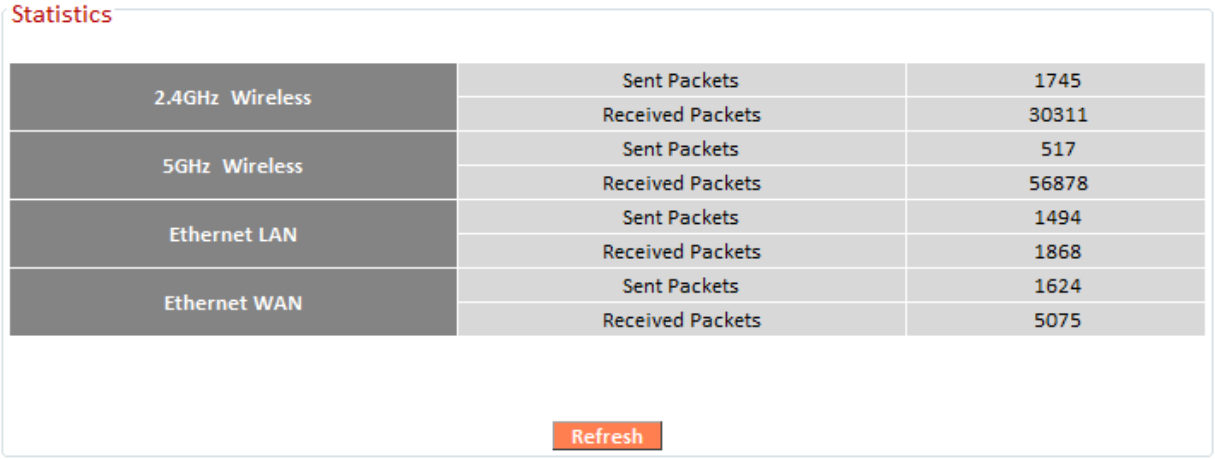
III-3-9-8. Active DHCP Client

Information about active DHCP clients is shown in the table, which displays the DHCP server assigned IP address, MAC address and time expired for each computer or device on the local network.



III-3-9-9. Statistics

Displays sent and received packet network statistics.



IV. Appendix

IV-1. Configuring your IP address

For first time access to the URL ***http://edimax.setup*** please ensure your computer is set to use a dynamic IP address. This means your computer can obtain an IP address automatically from a DHCP server. You can check if your computer is set to use a dynamic IP address by following **IV-1-1. How to check that your computer uses a dynamic IP address**.

Static IP users can also temporarily modify your computer's IP address to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254)** as the BR-6288ACL V2 in order to access ***http://edimax.setup***.

The BR-6288ACL V2's default IP address is 192.168.2.1.

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system in **IV-1-2. How to modify the IP address of your computer****.**

Static IP users please make a note of your static IP before you change it.

You can assign a new IP address to the device which is within the subnet of your network during setup or using the browser based configuration interface (refer to **III-3-4. LAN**). Then you can access the URL ***http://edimax.setup*** in future without modifying your IP address.

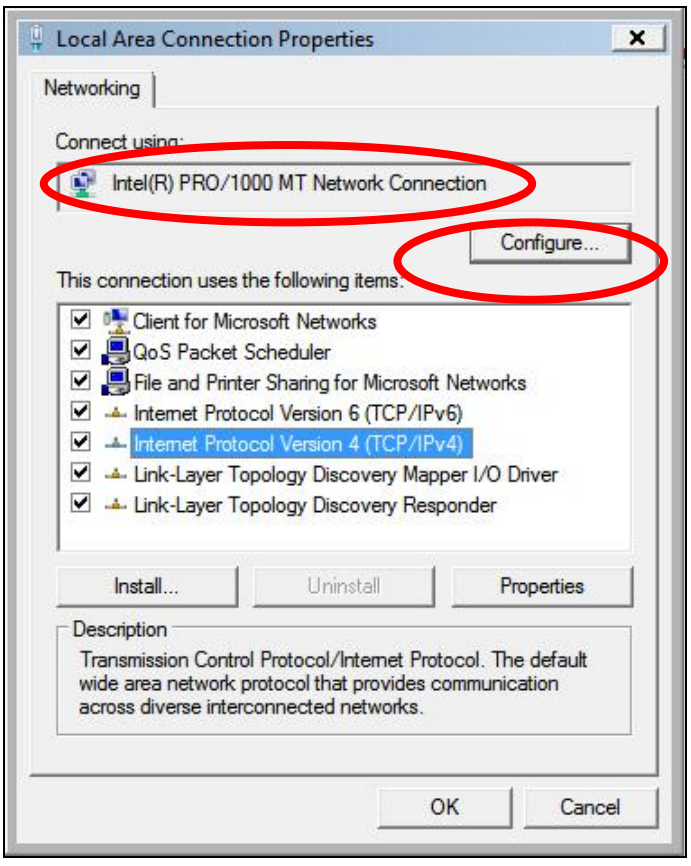
Please remember to change your IP address back to its original value after the device is properly configured.

IV-1-1. How to check that your computer uses a dynamic IP address

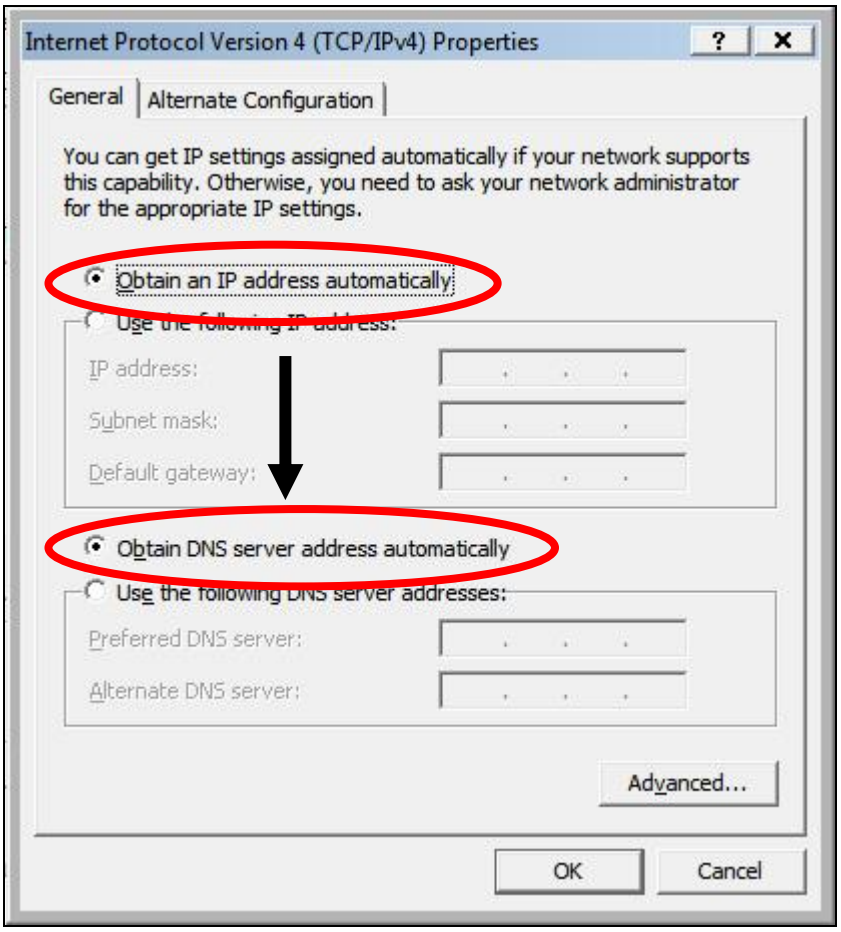
Please follow the instructions appropriate for your operating system.

IV-1-1-1. Windows Vista

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Click “View Network Status and Tasks”, then click “Manage Network Connections”. Right-click “Local Area Network”, then select “Properties”. The “Local Area Connection Properties” window will then appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.

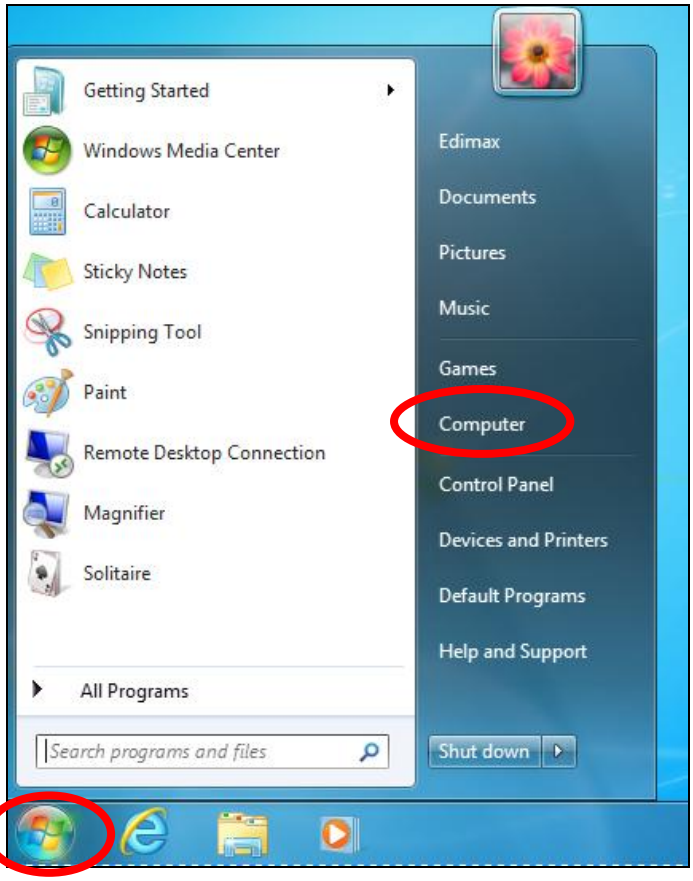


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

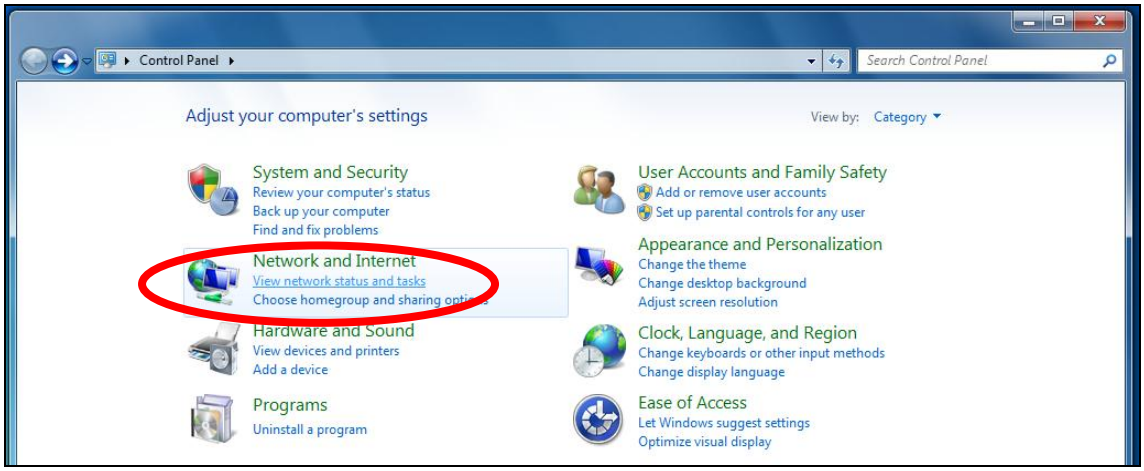

Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

IV-1-1-2. Windows 7

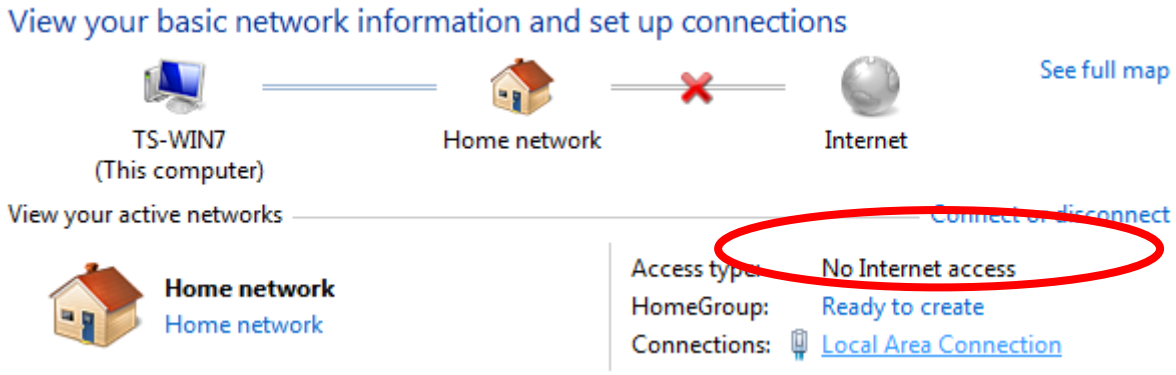
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



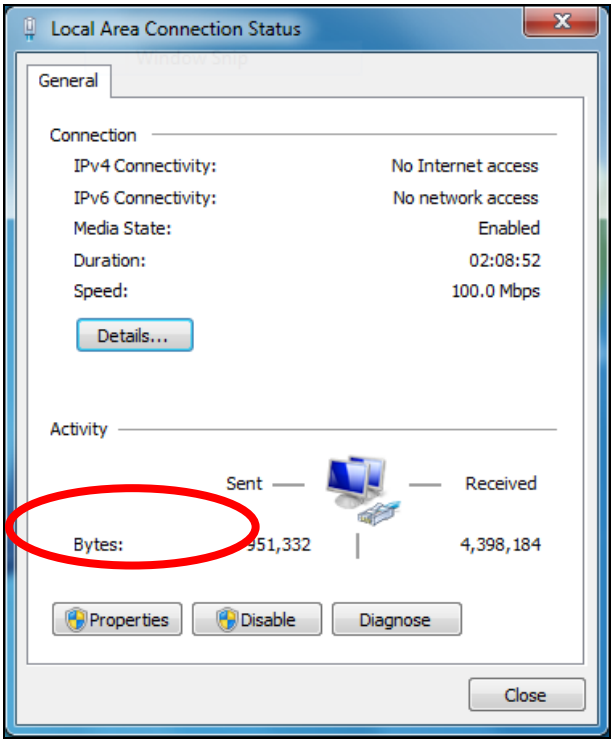
2. Under “Network and Internet” click “View network status and tasks”.



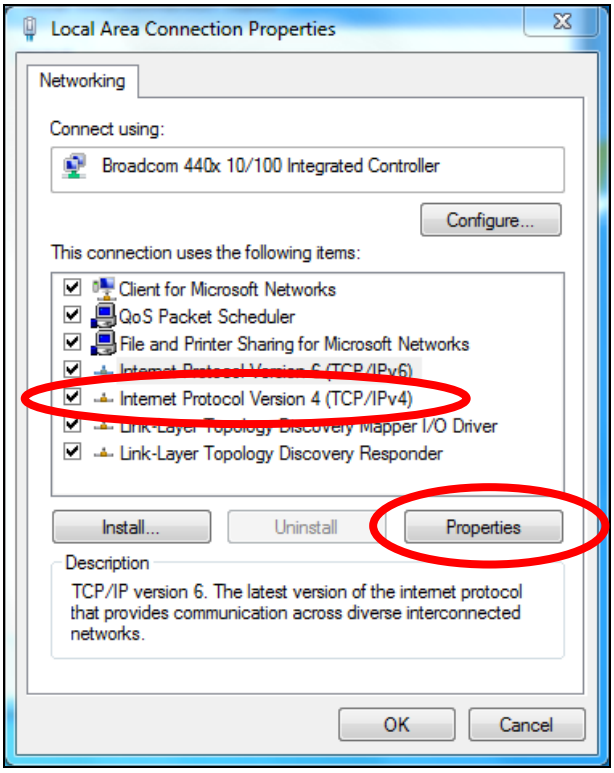
3. Click “Local Area Connection”.



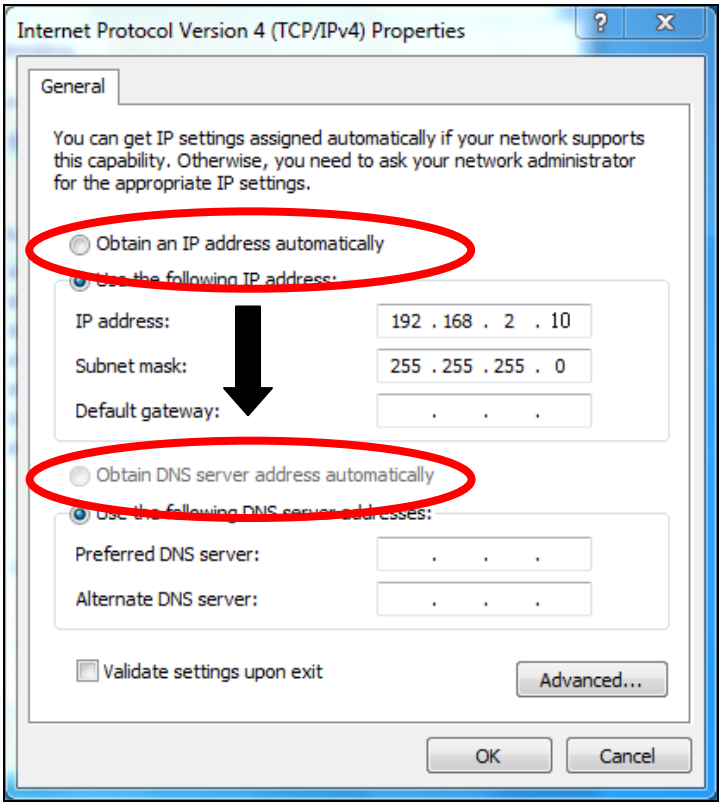
4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.

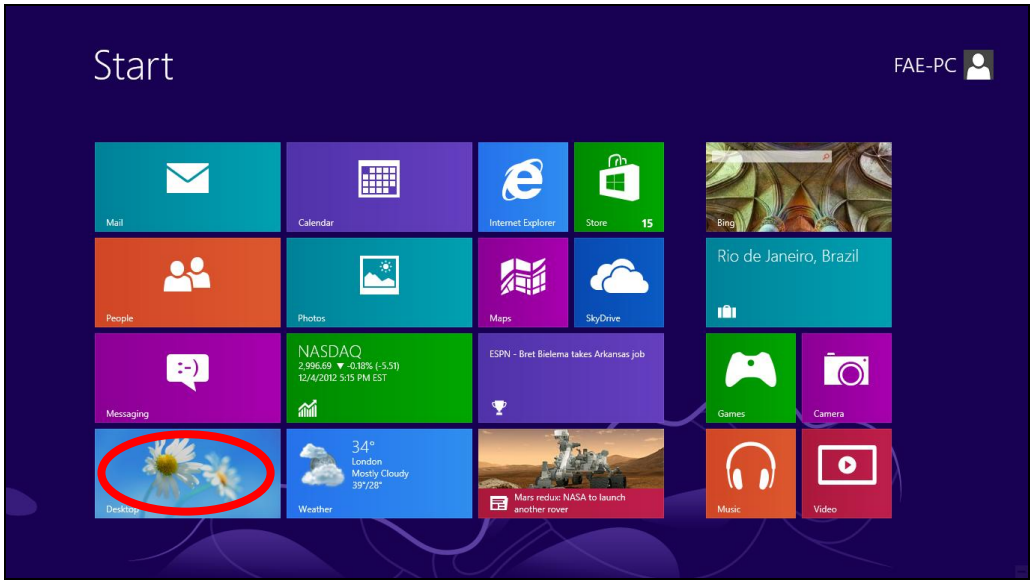


6. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

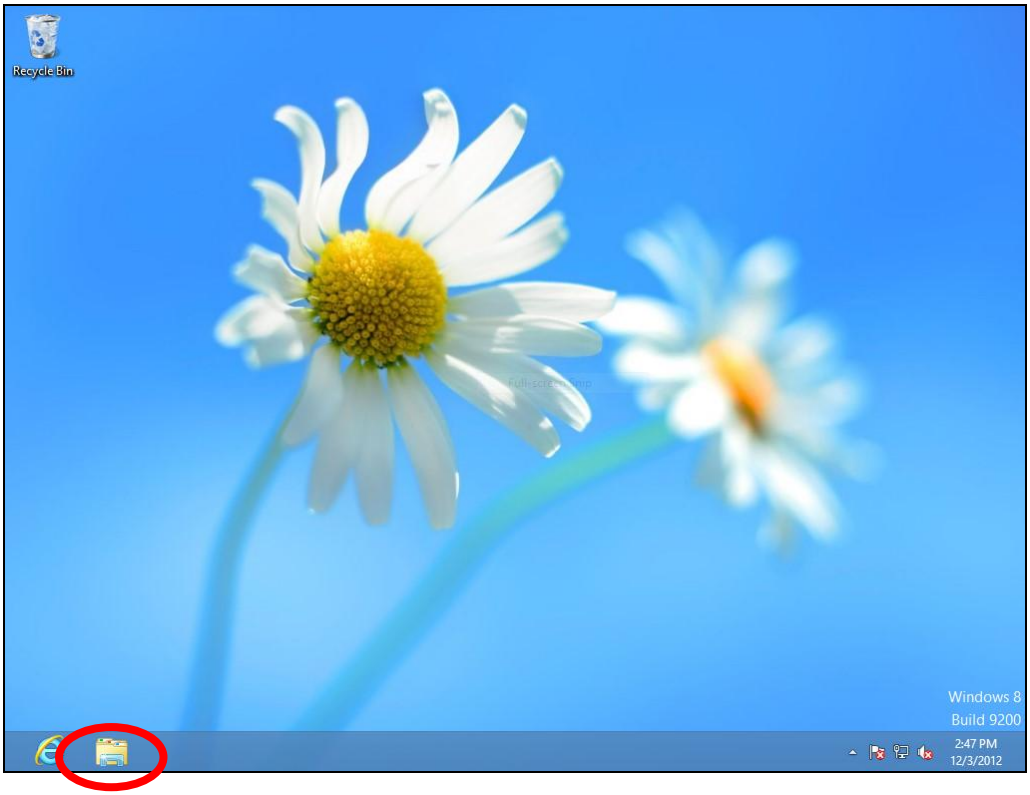


IV-1-1-3. Windows 8

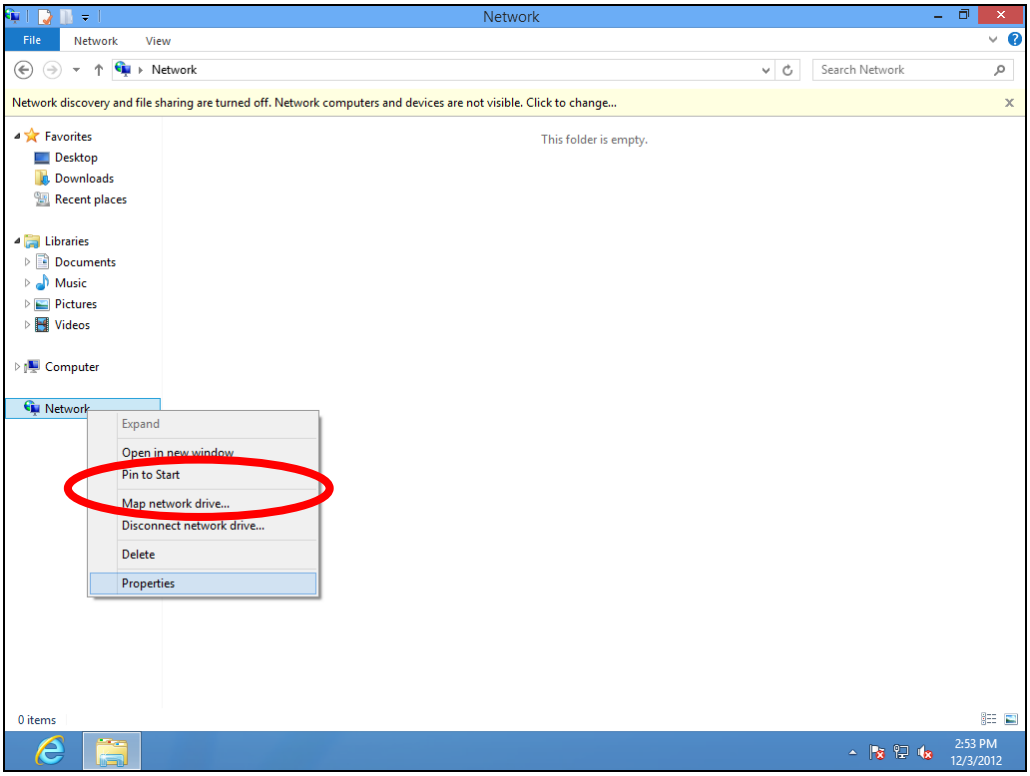
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



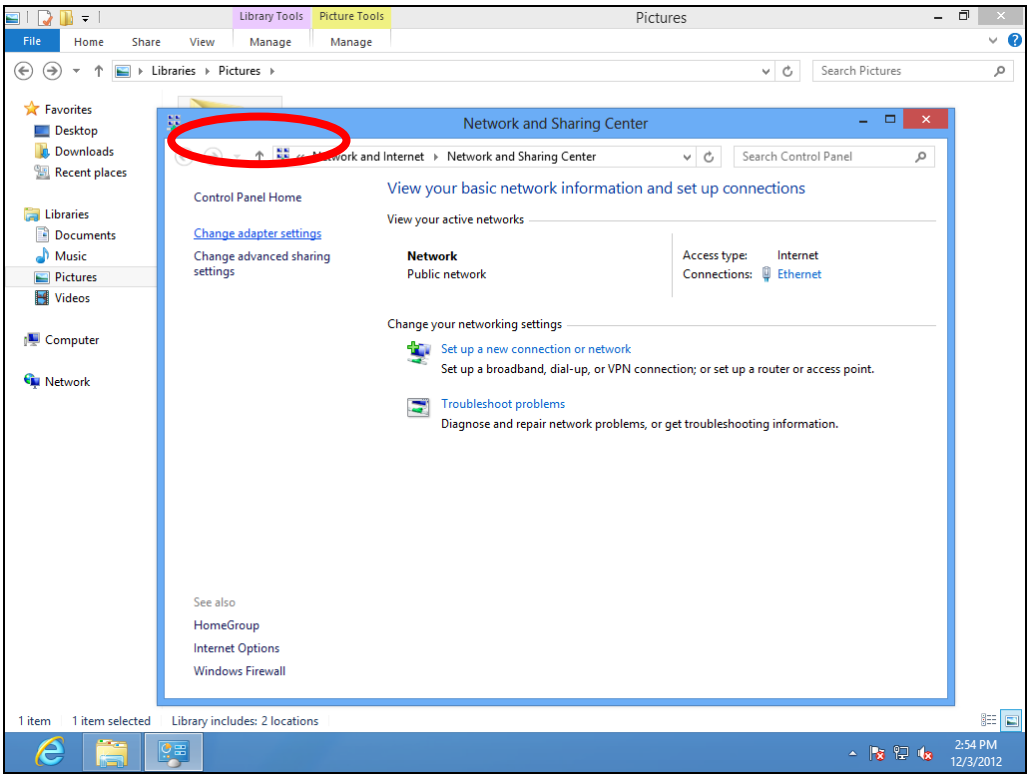
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



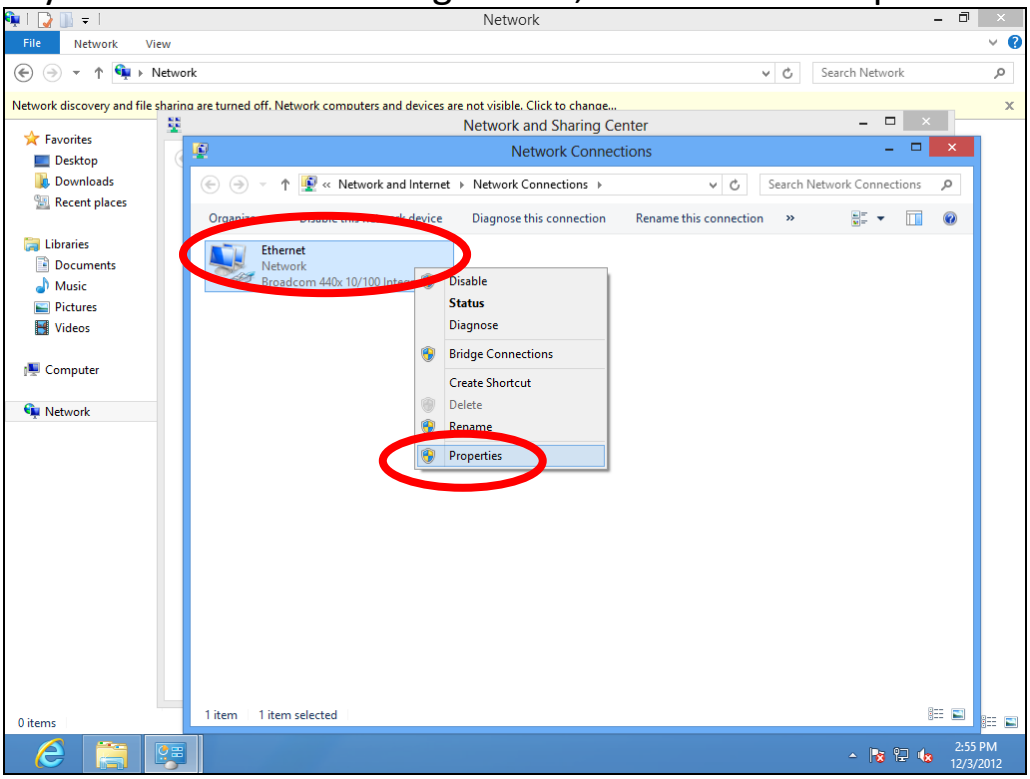
3. Right click “Network” and then select “Properties”.



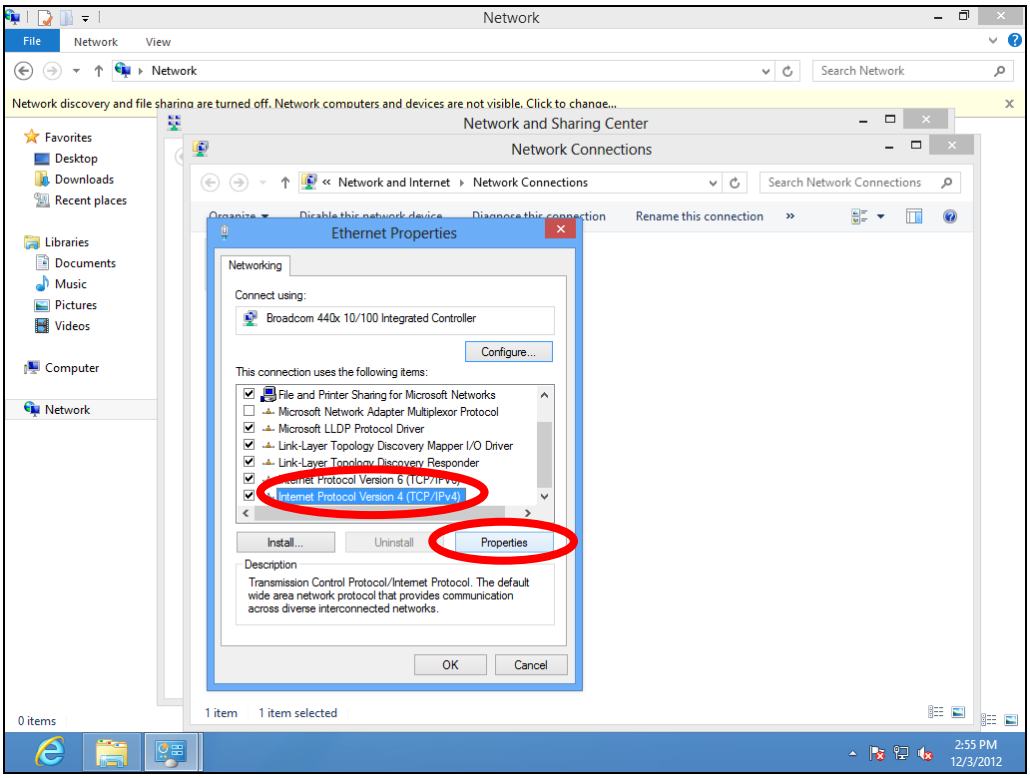
4. In the window that opens, select “Change adapter settings” from the left side.



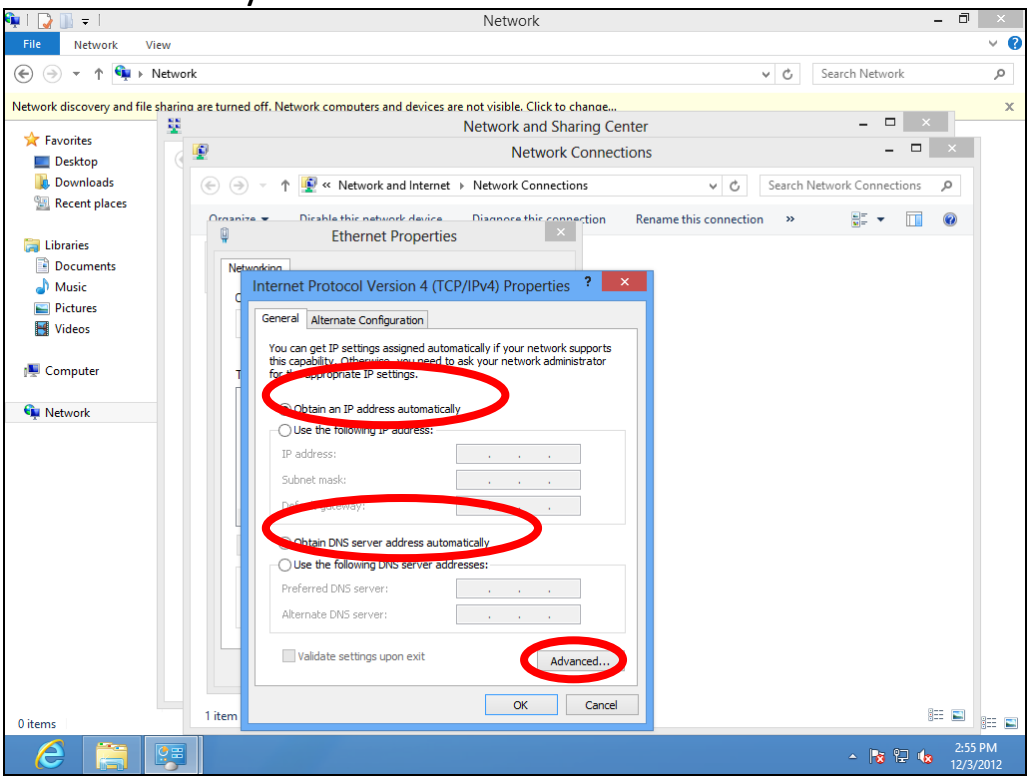
5. Choose your connection and right click, then select “Properties”.



6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



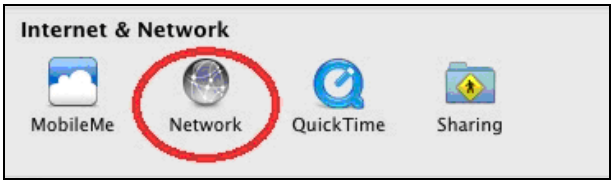
7. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.



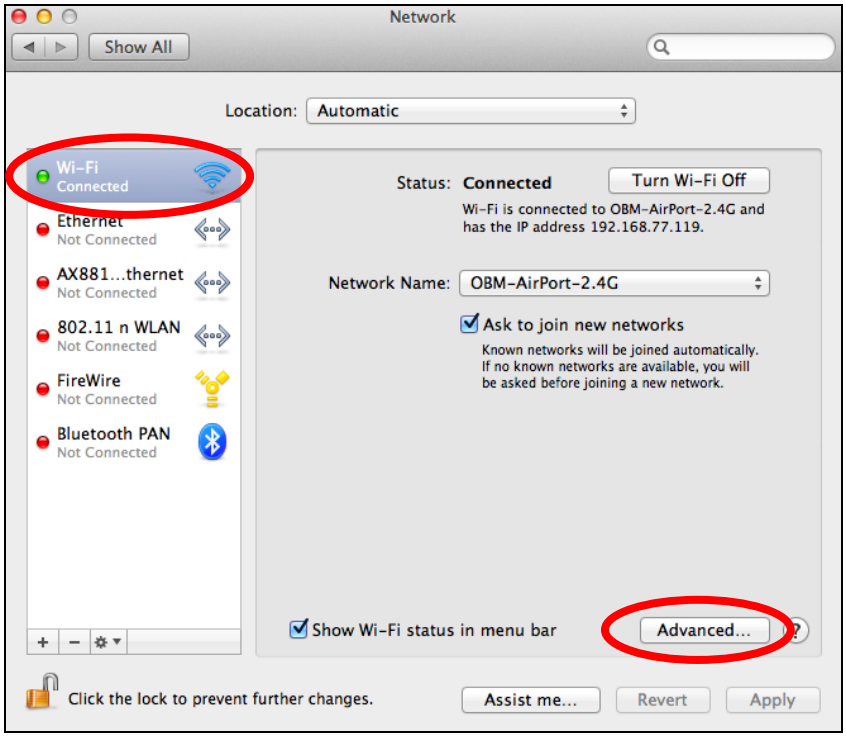
IV-1-1-4. Mac OS

1. Have your Mac computer operate as usual, and click on “System Preferences”.

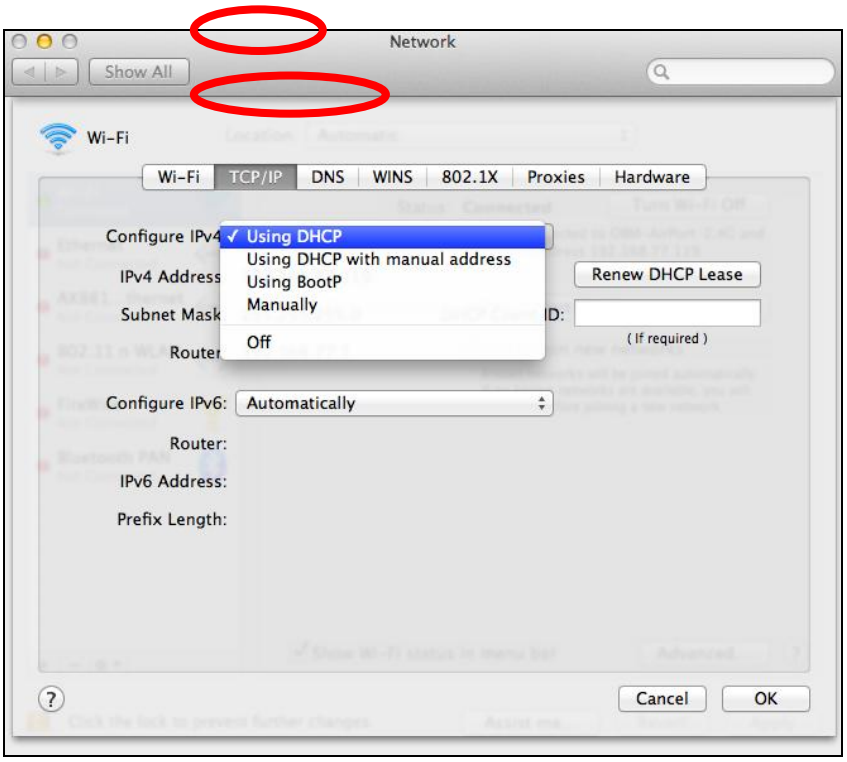
2. In System Preferences, click on “Network”.



3. Click on “Wi-Fi” in the left panel and then click “Advanced” in the lower right corner.



4. Select “TCP/IP” from the top menu and “Using DHCP” in the drop down menu labeled “Configure IPv4” should be selected.



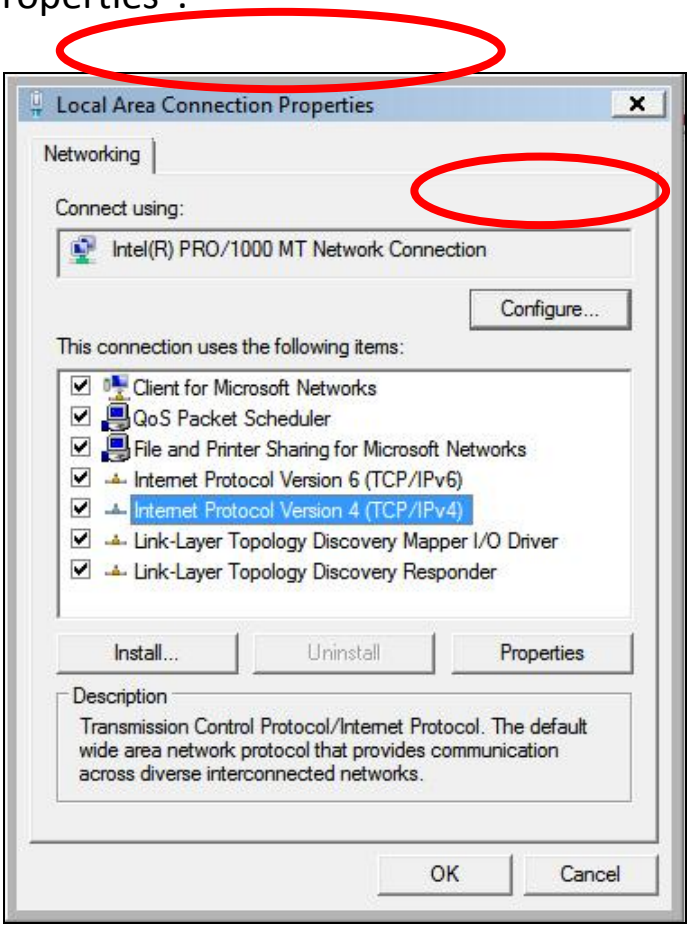
IV-1-2. How to modify the IP address of your computer

Please follow the instructions appropriate for your operating system. In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254)** in order to access iQ Setup/browser based configuration interface.

Please make a note of your static IP before you change it.

IV-1-2-1. Windows Vista

1. Click the "Start" button (it should be located in the lower-left corner of your computer), then click "Control Panel". Click "View Network Status and Tasks", then click "Manage Network Connections". Right-click "Local Area Network", then select "Properties". The "Local Area Connection Properties" window will then appear, select "Internet Protocol Version 4 (TCP / IPv4)", and then click "Properties".



2. Select "Use the following IP address" and "Use the following DNS server addresses", then input the following values:

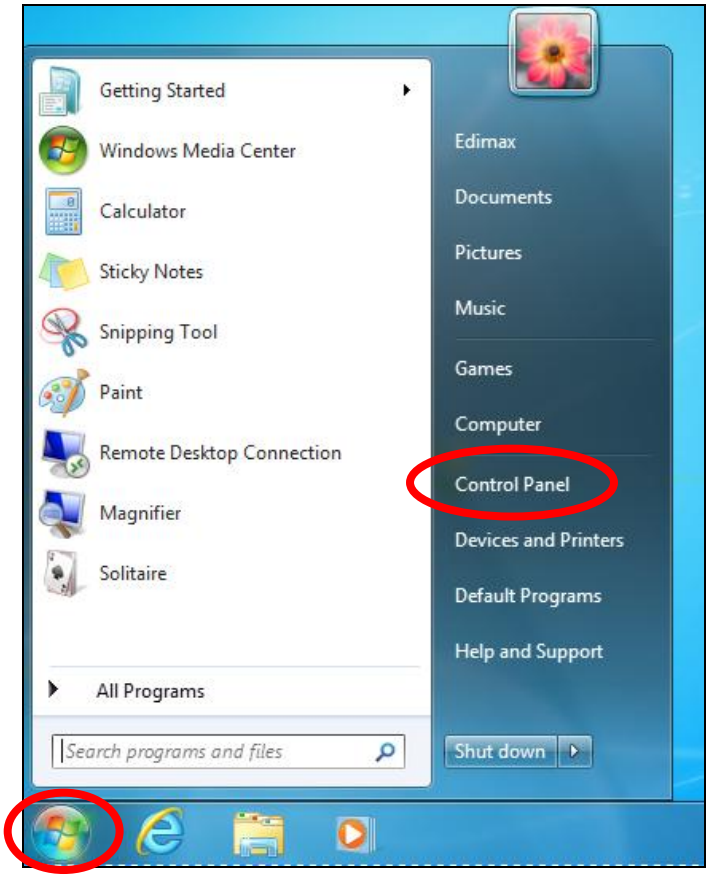
Your existing static IP address will be displayed in the "IP address" field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0
Preferred DNS Server: 192.168.2.1

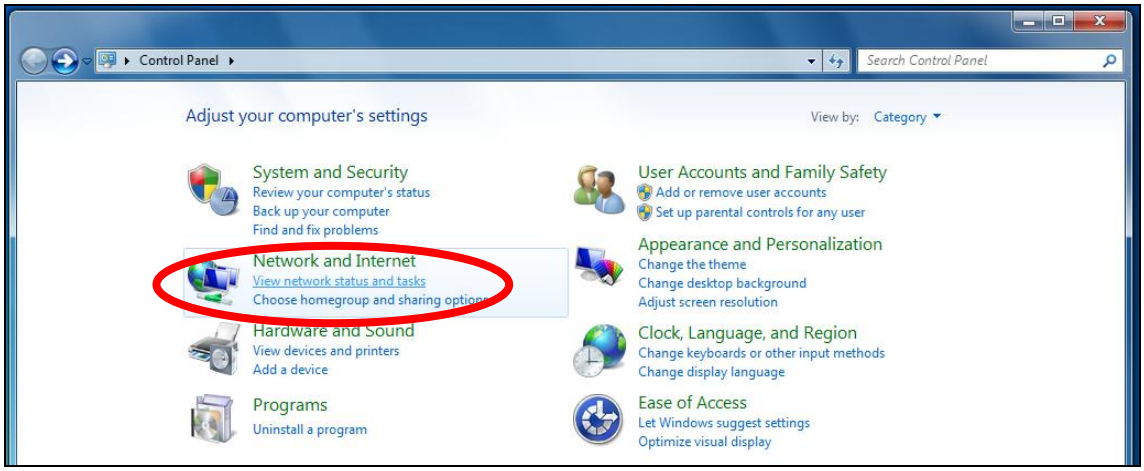
Click 'OK' when finished.

IV-1-2-2. Windows 7

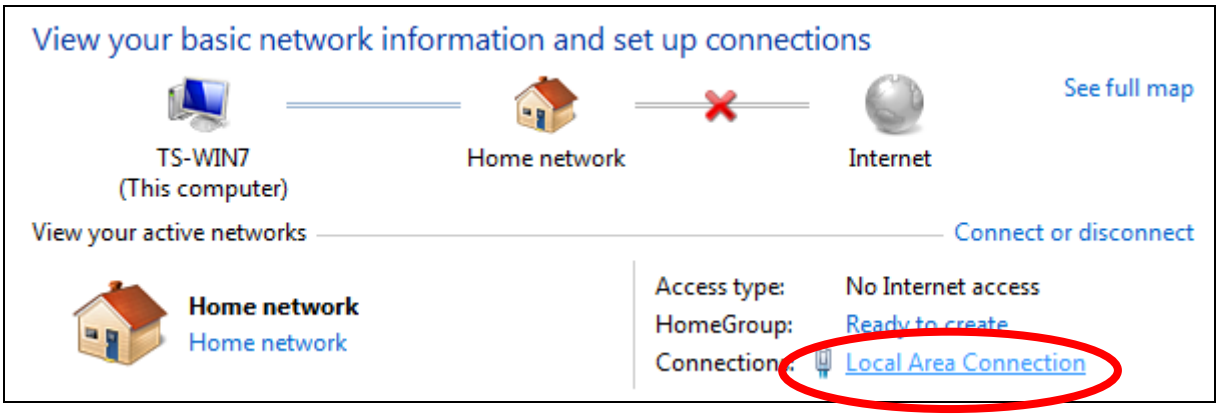
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



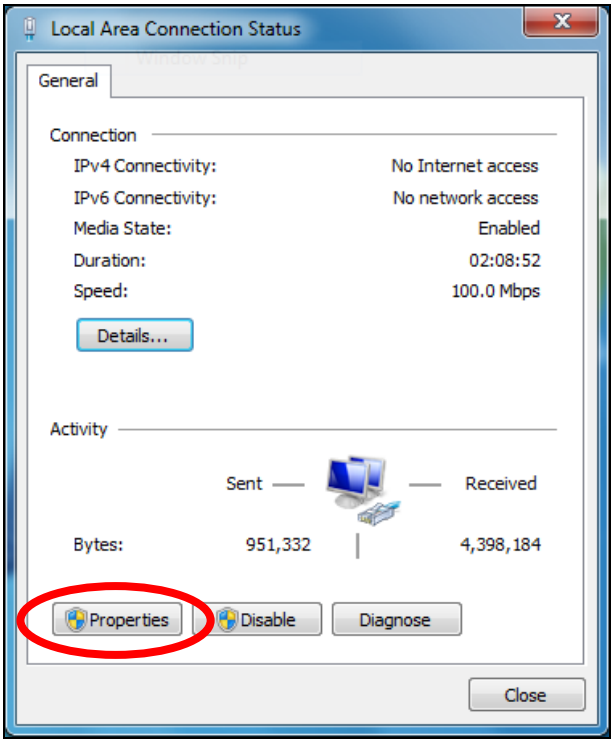
2. Under “Network and Internet” click “View network status and tasks”.



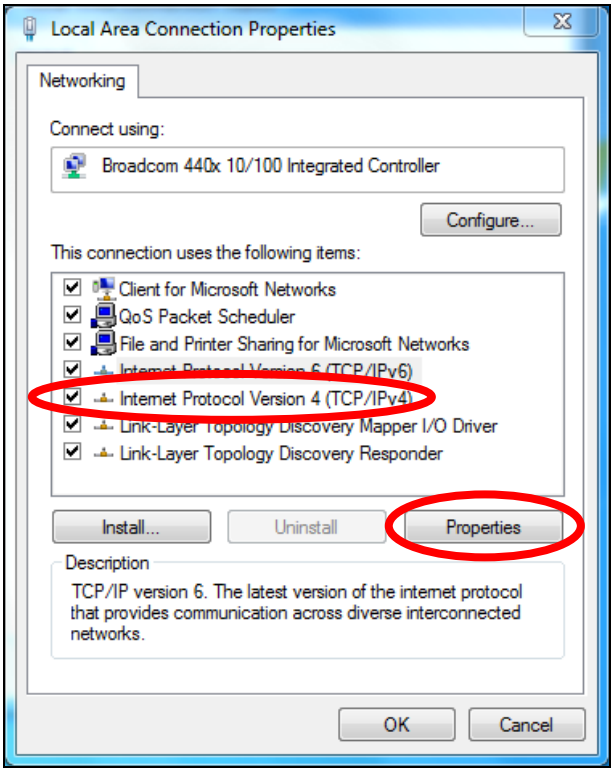
3. Click “Local Area Connection”.



4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



6. Select “Use the following IP address” and “Use the following DNS server addresses”, then input the following values:

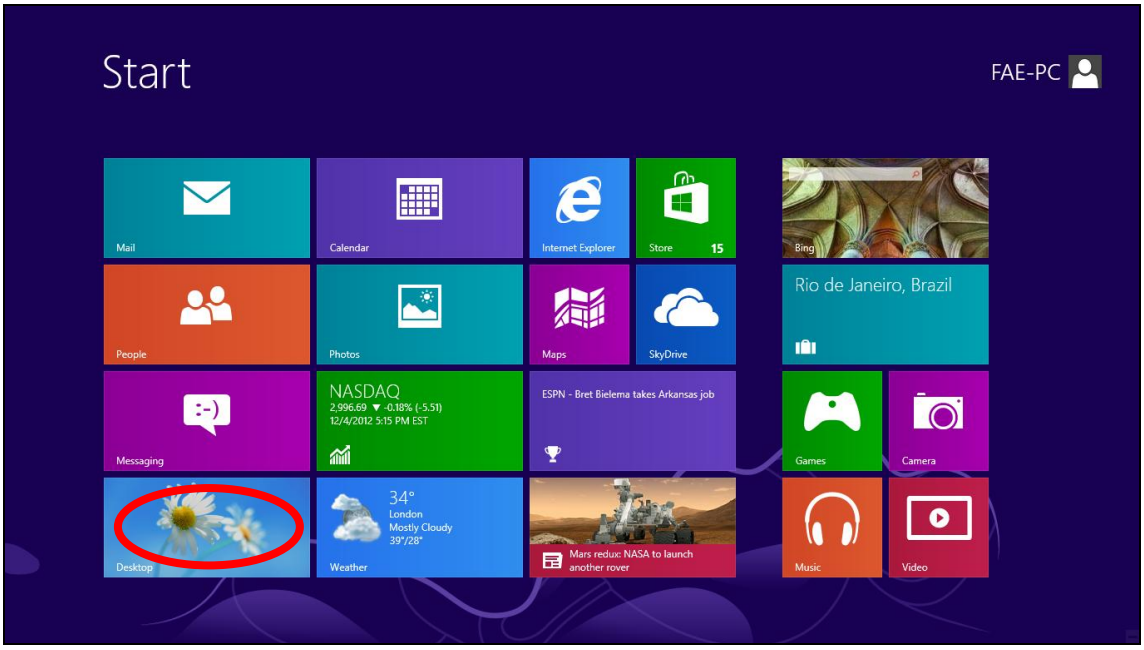
Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0
Preferred DNS Server: 192.168.2.1

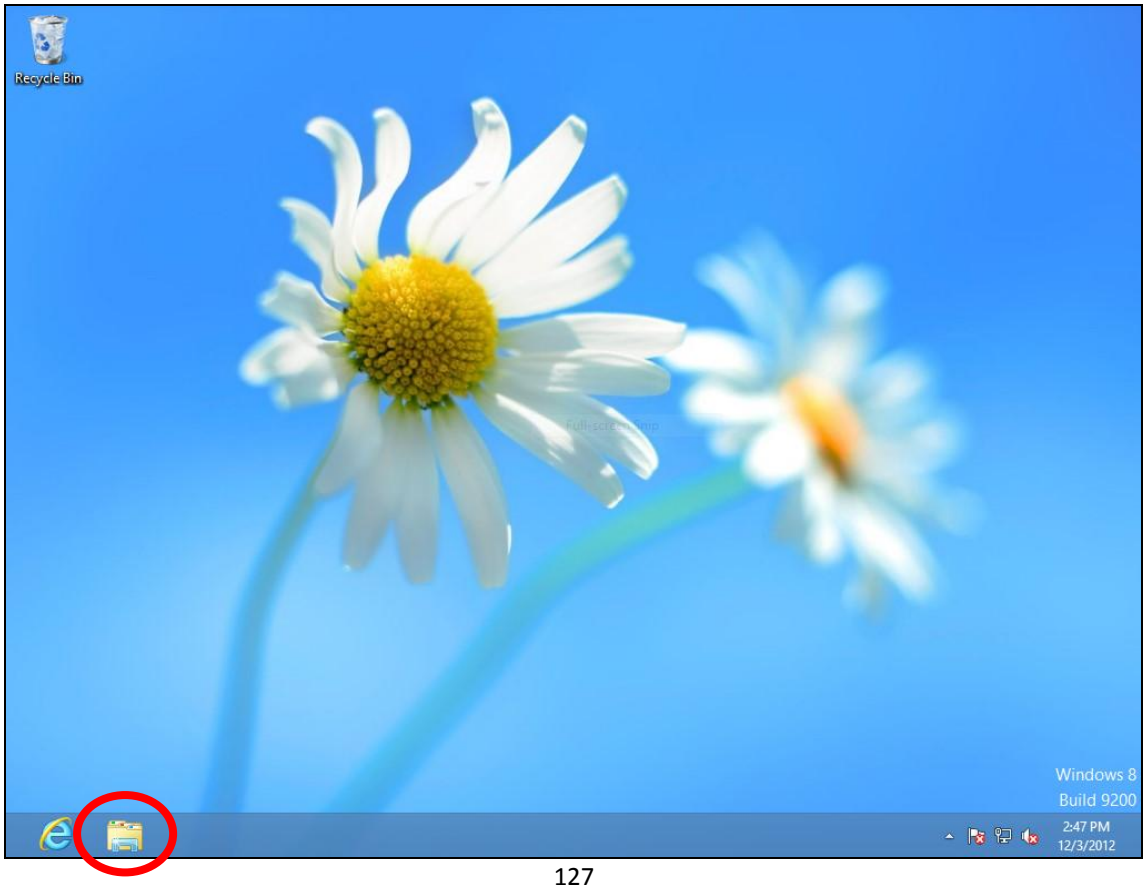
Click ‘OK’ when finished.

IV-1-2-3. Windows 8

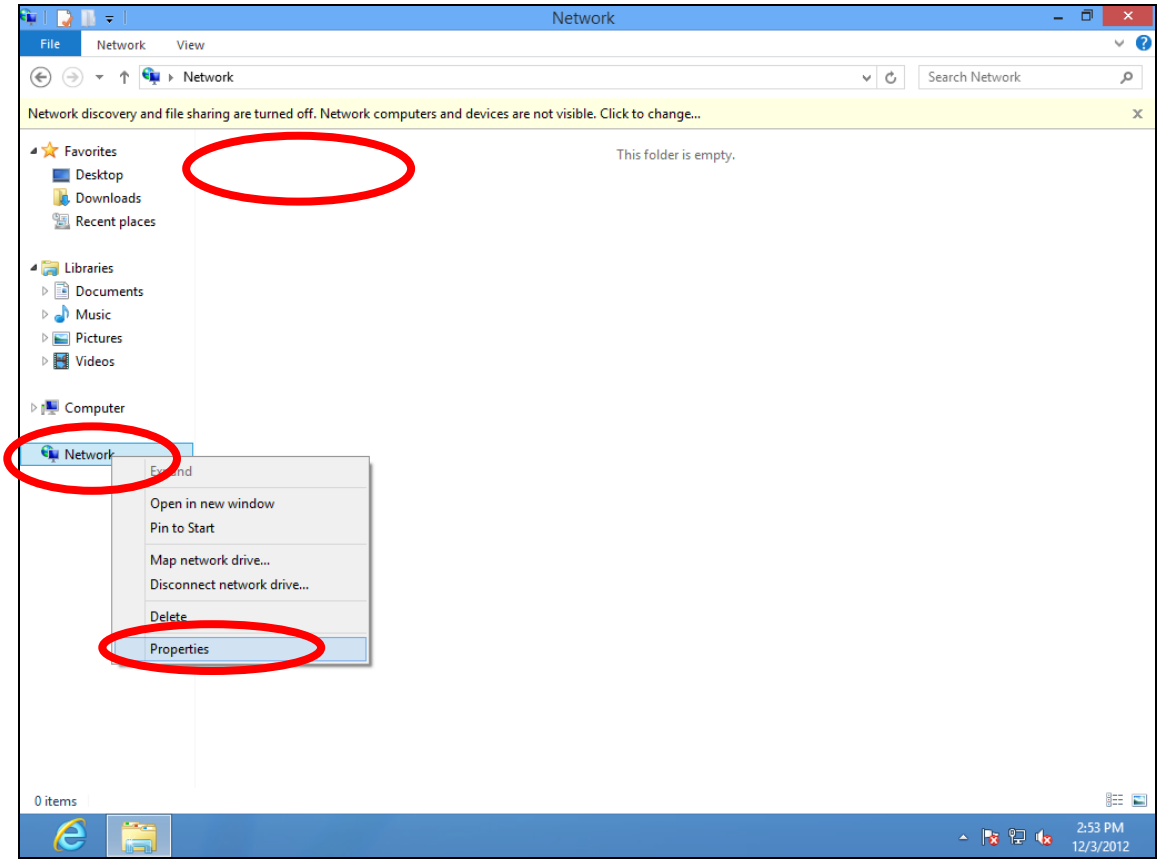
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



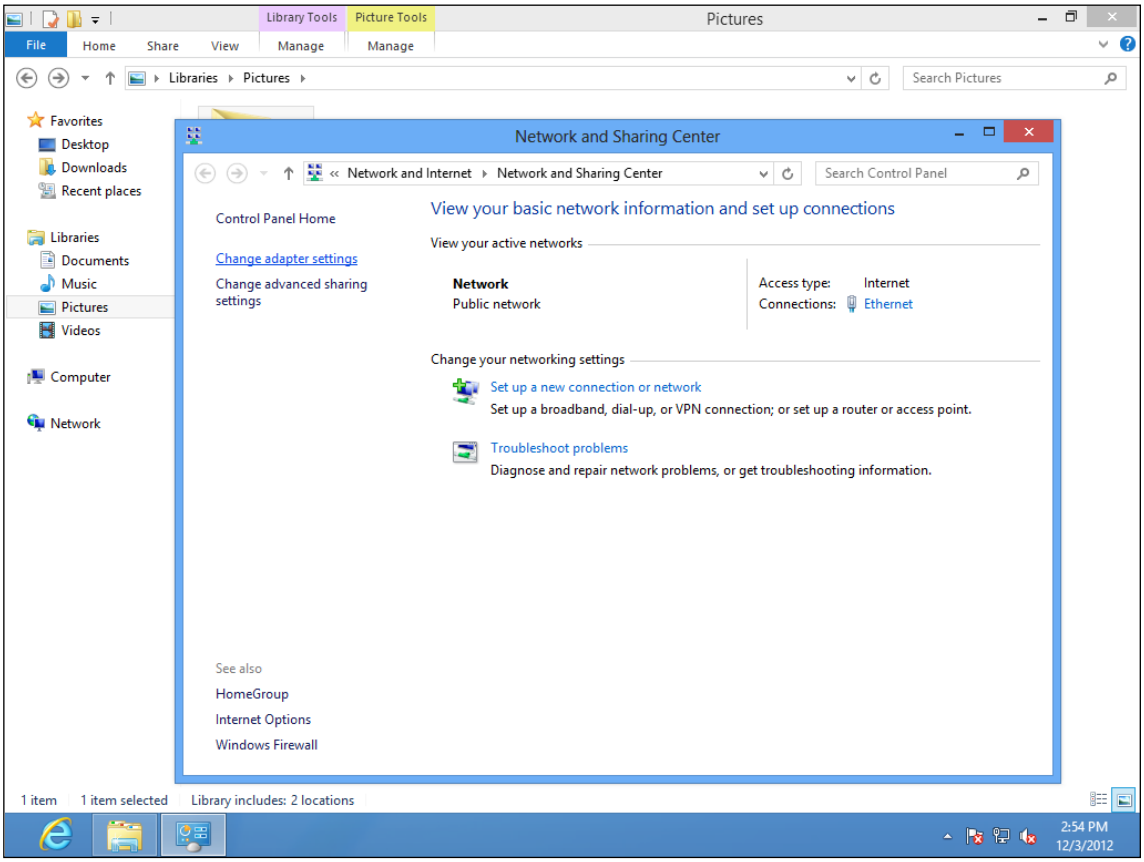
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



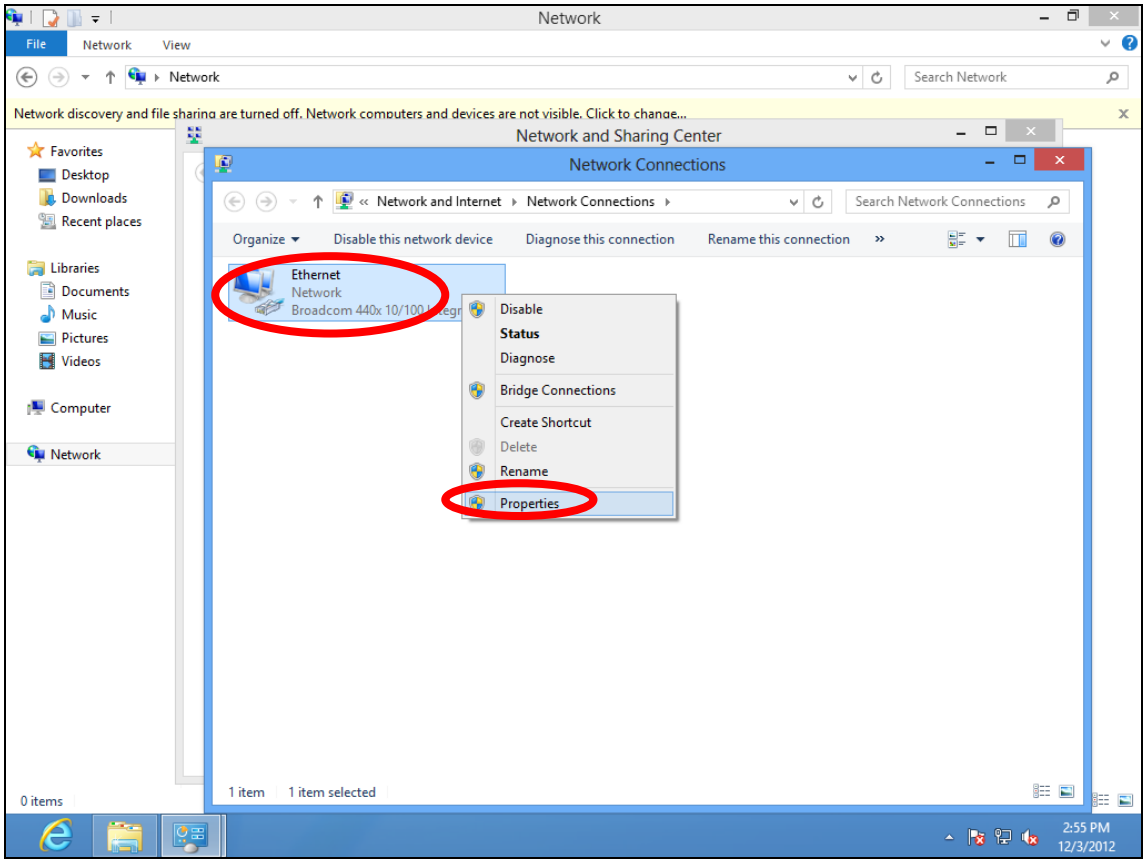
3. Right click “Network” and then select “Properties”.



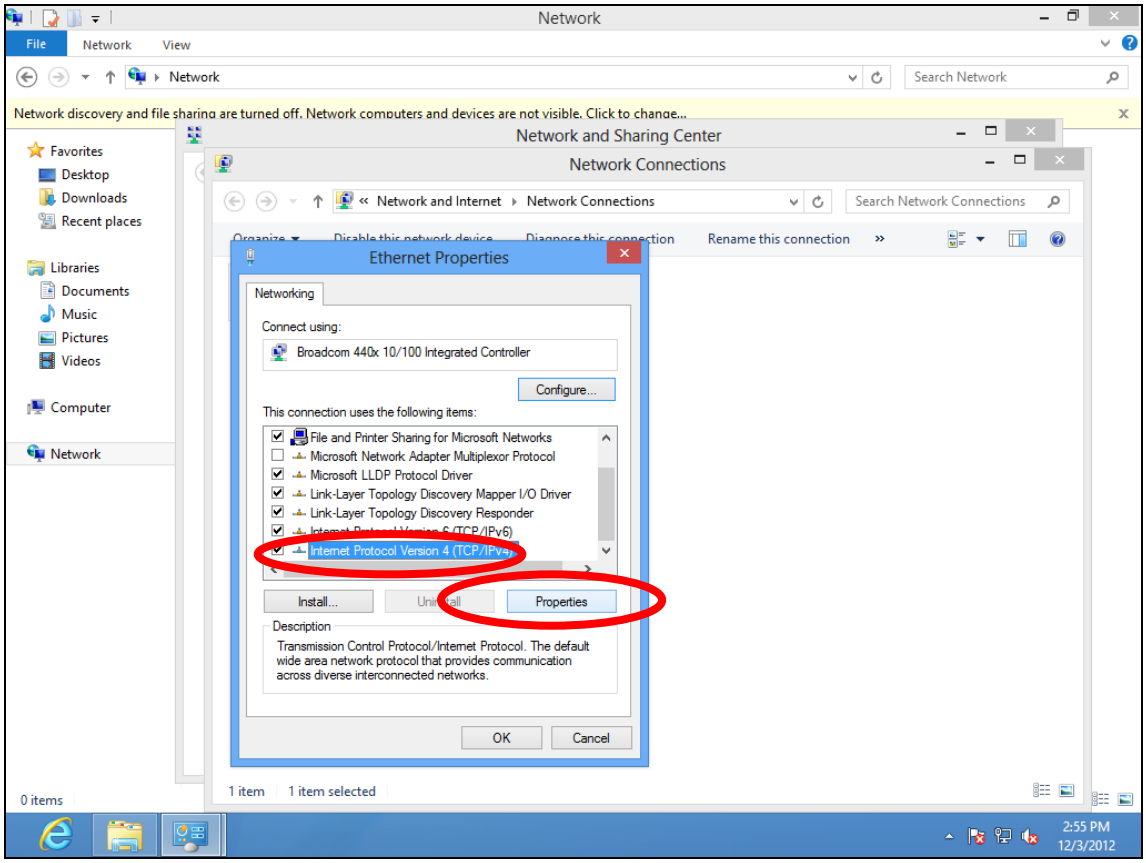
4. In the window that opens, select “Change adapter settings” from the left side.



5. Choose your connection and right click, then select “Properties”.



6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



7. Select “Use the following IP address” and “Use the following DNS server addresses”, then input the following values:

Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

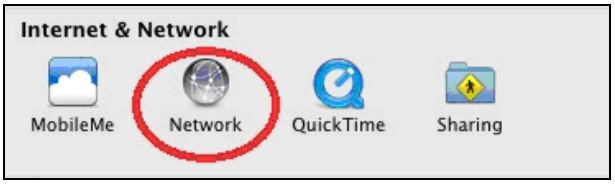
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0
Preferred DNS Server: 192.168.2.1

Click ‘OK’ when finished.

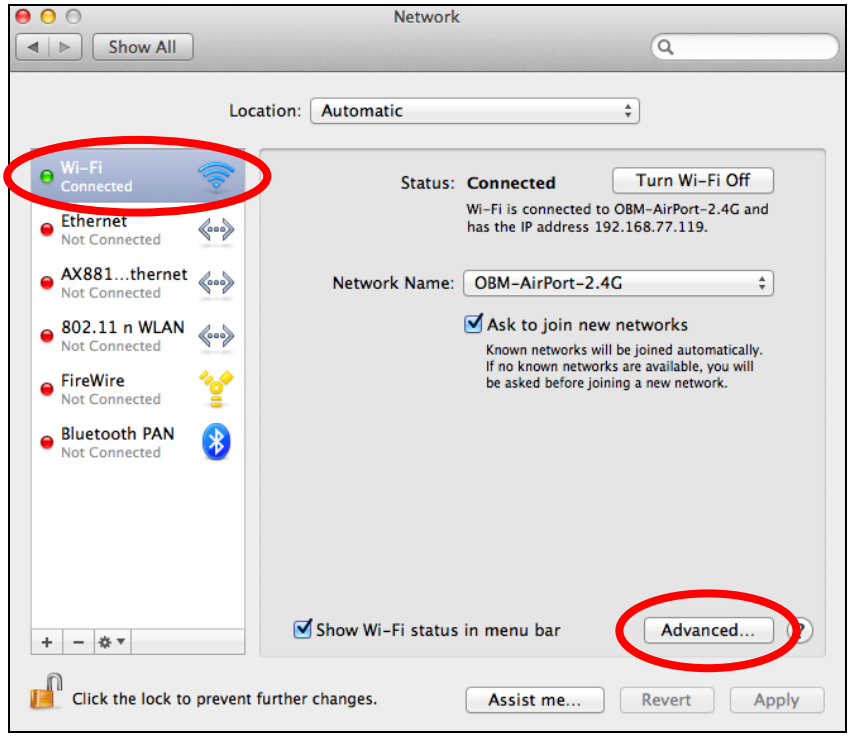
IV-1-2-4. Mac

1. Have your Mac computer operate as usual, and click on “System Preferences”.

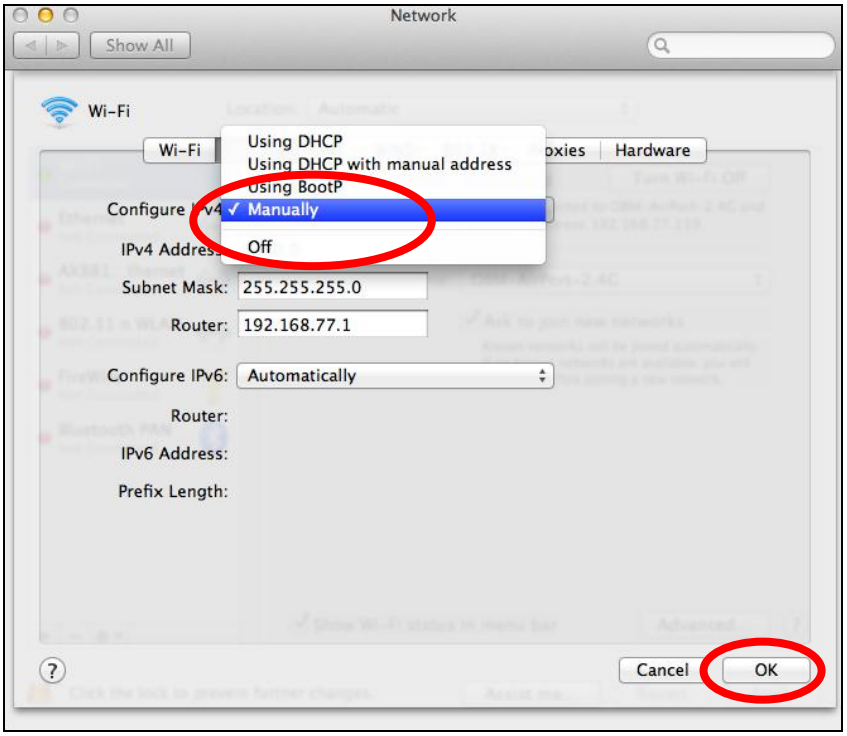
2. In System Preferences, click on “Network”.



3. Click on “Wi-Fi” in the left panel and then click “Advanced” in the lower right corner.

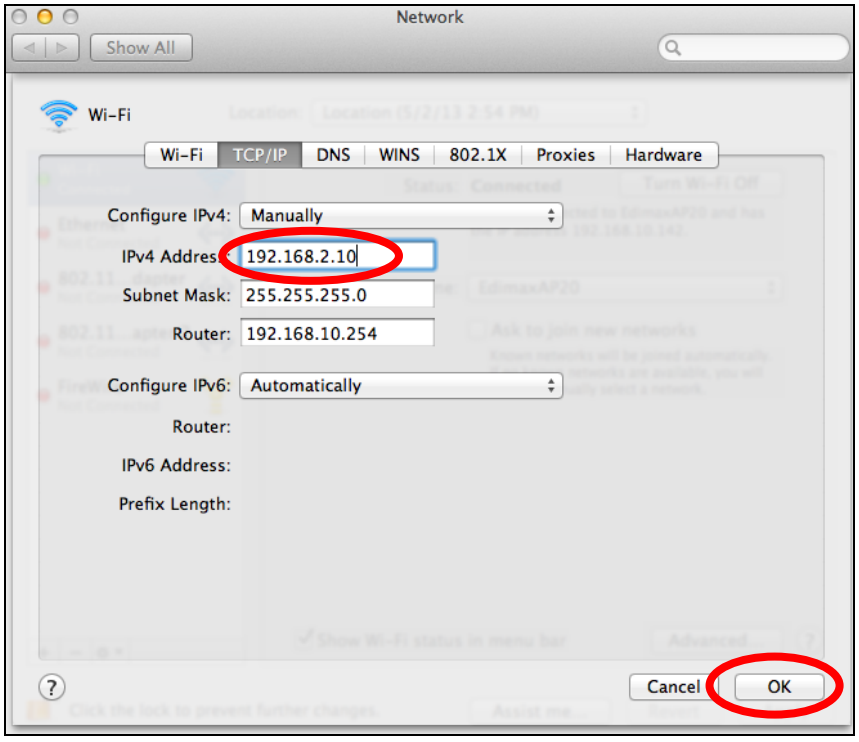


4. Select “TCP/IP” from the top menu and select “Manually” from the drop down menu labeled “Configure IPv4”, then click “OK”.

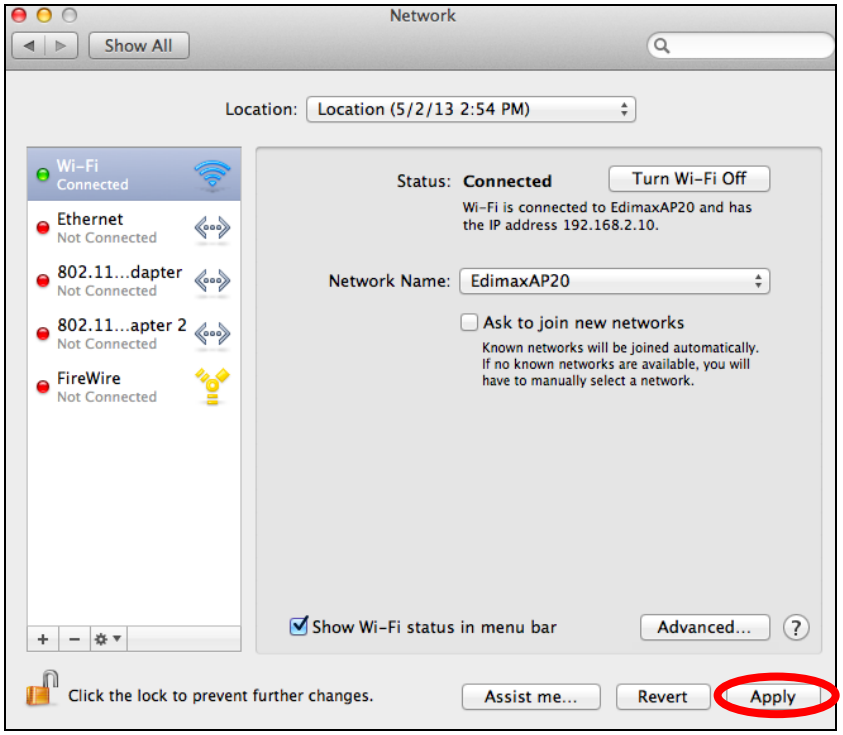


Your existing static IP address will be displayed in the "IP address" field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

5. In the "IPv4 Address" and "Subnet Mask" field enter IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on "OK".



6. Click “Apply” to save the changes.

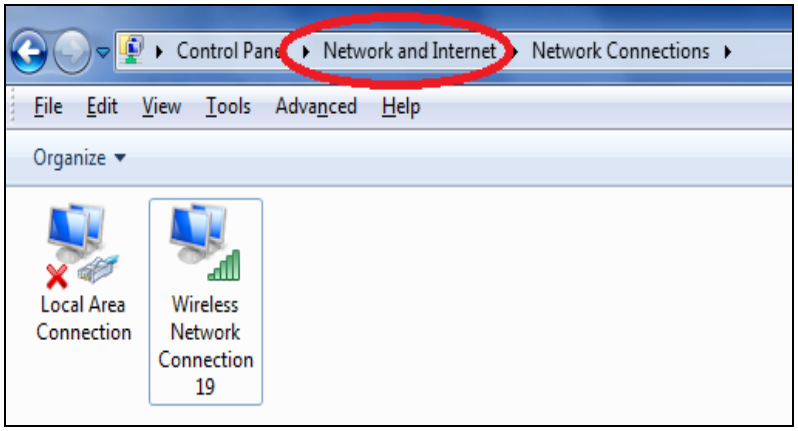


IV-1-3. How to Find Your Network Security Key

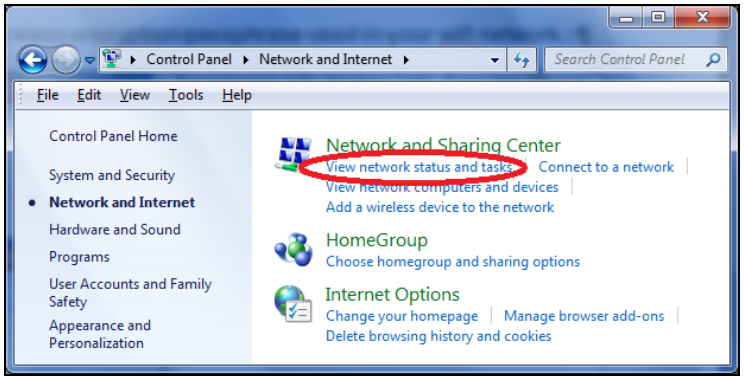
To find your network security key, please follow the instructions appropriate for your operating system.

IV-1-3-1. Windows 7 & Vista

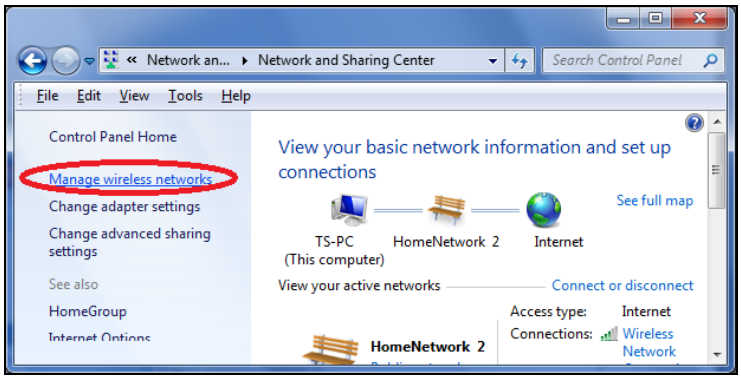
1. Open “Control Panel” and click on “Network and Internet” in the top menu.



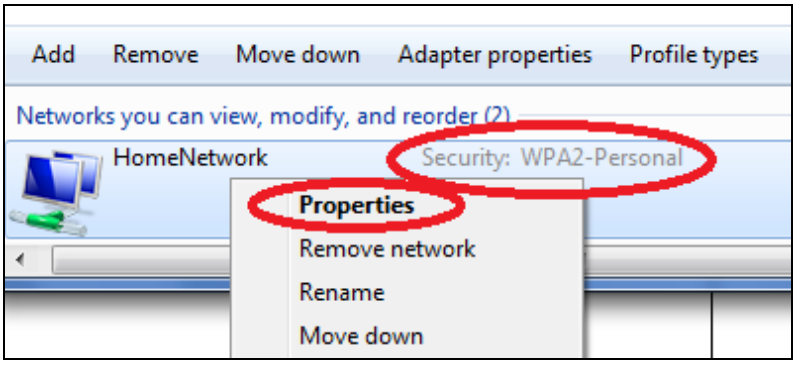
2. Click on “View network status and tasks” which is under the heading “Network and Sharing Center”.



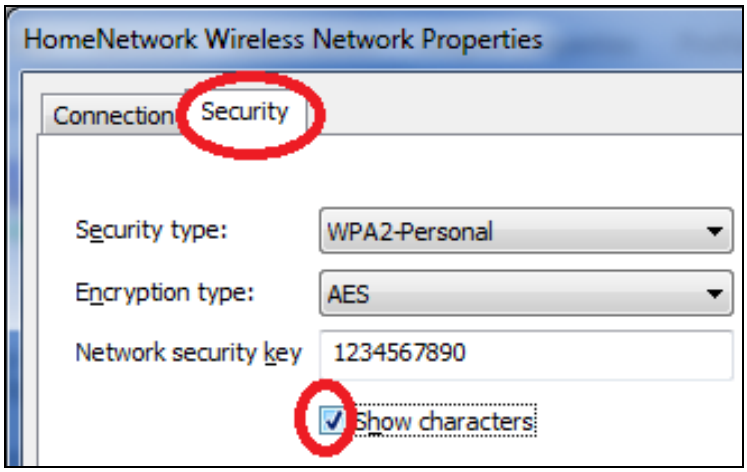
3. Click on “Manage wireless networks” in the left menu.



4. You should see the profile of your Wi-Fi network in the list. Right click on your Wi-Fi network and then click on “Properties”.

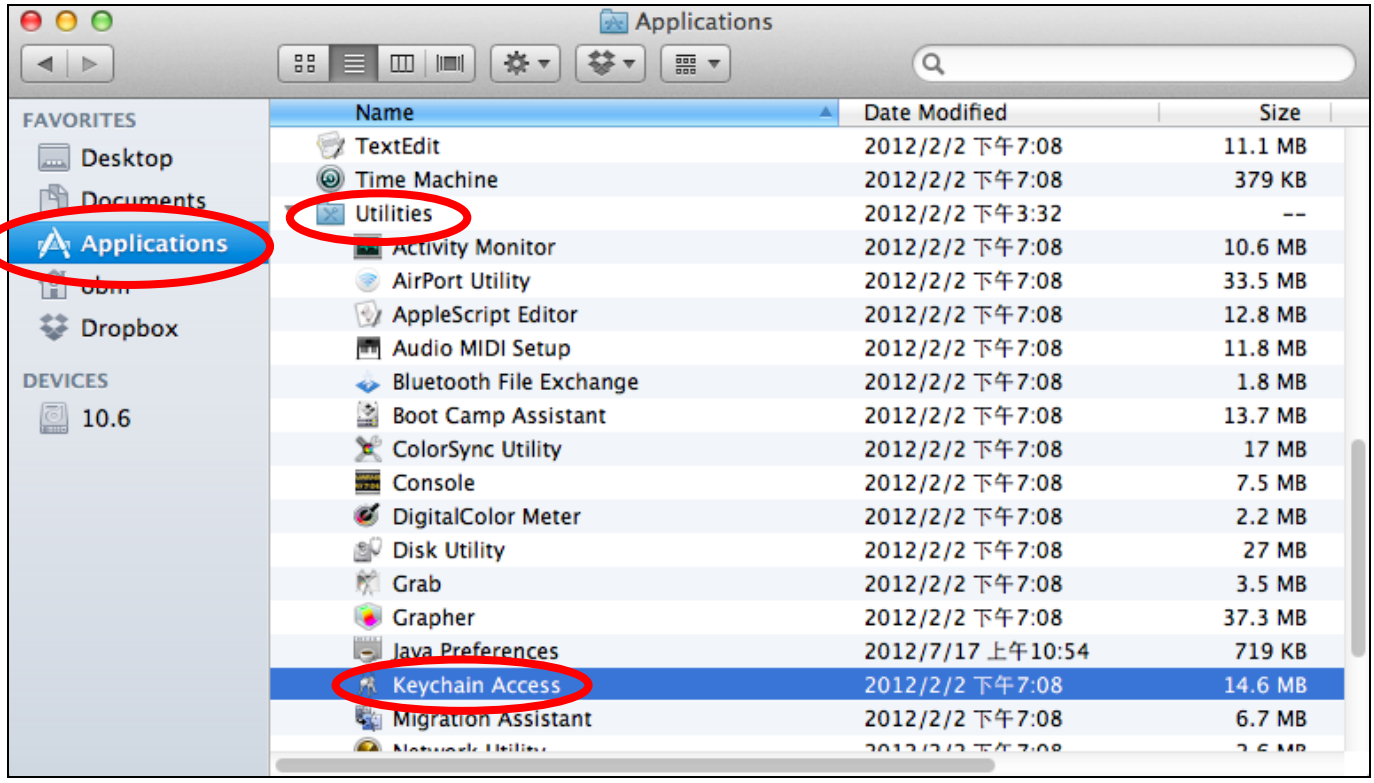


5. Click on the “Security” tab, and then check the box labeled “Show characters”. This will show your network security key. Click the “Cancel” button to close the window.

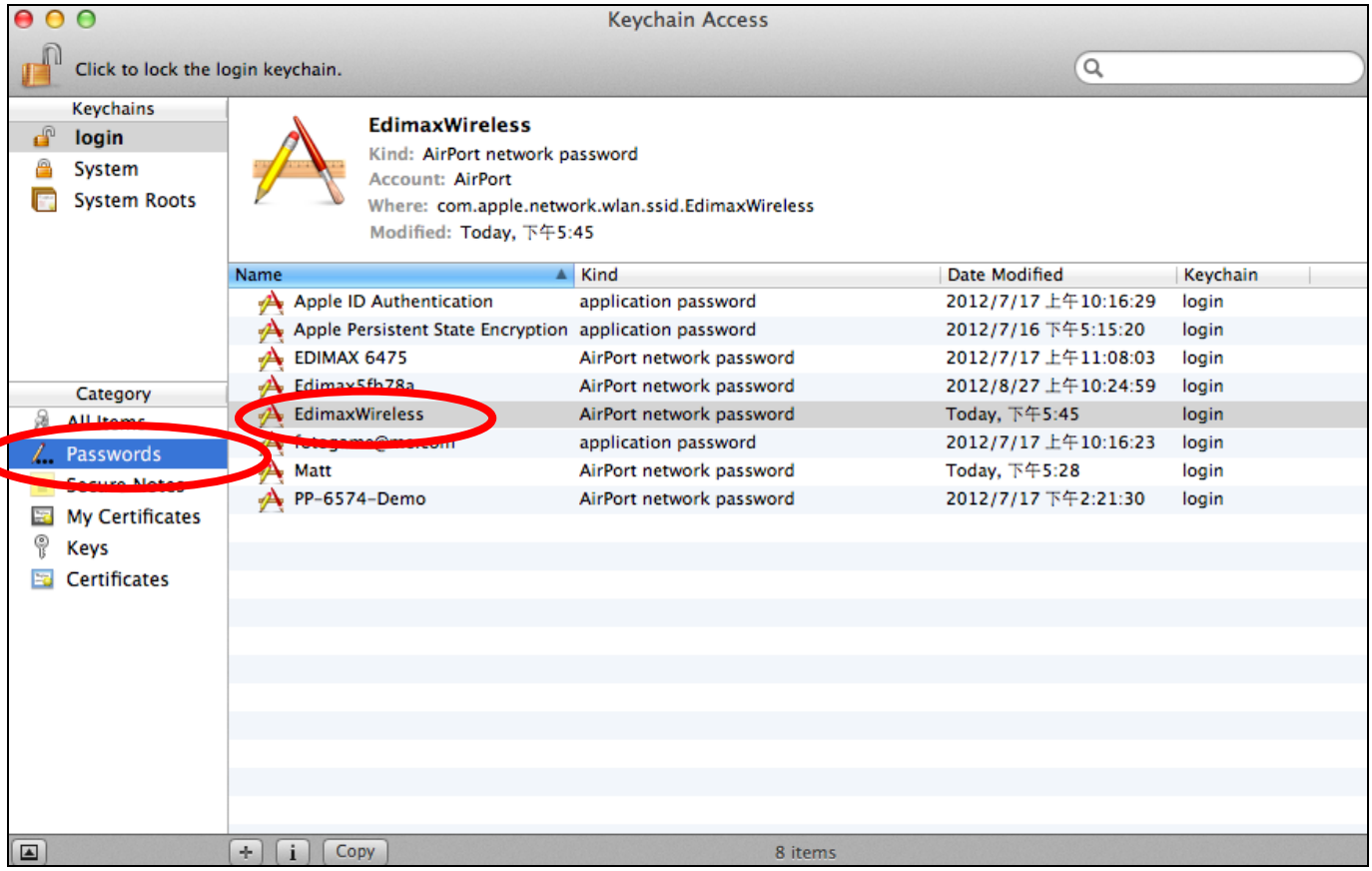


IV-1-3-2. Mac

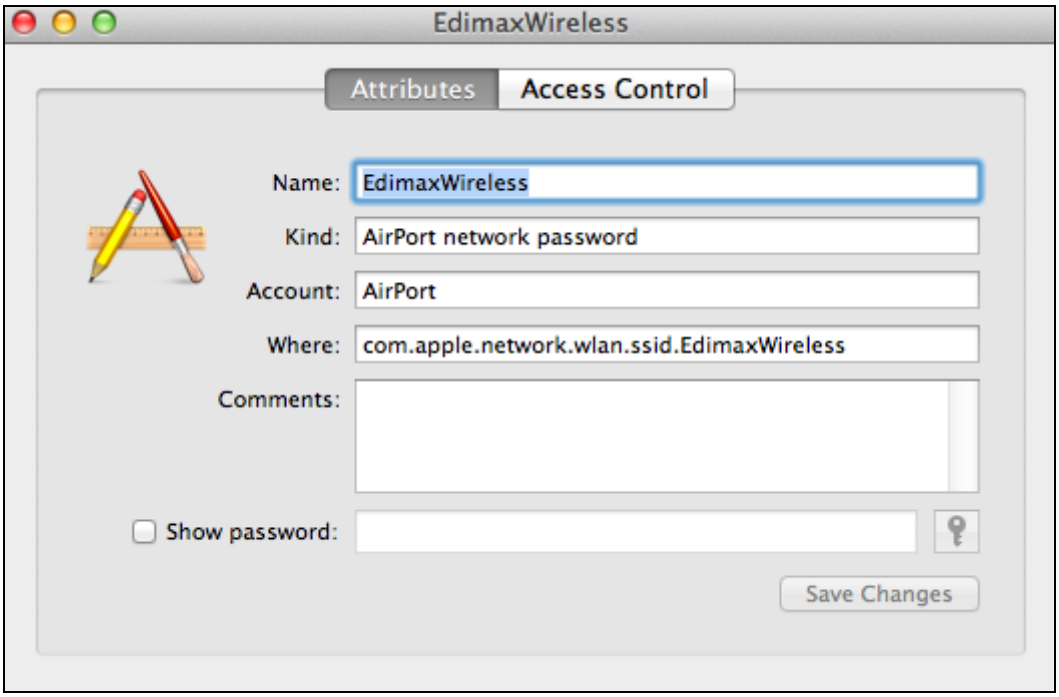
1. Open a new Finder window, and select “Applications” from the menu on the left side. Open the folder labeled “Utilities” and then open the application “Keychain Access”.



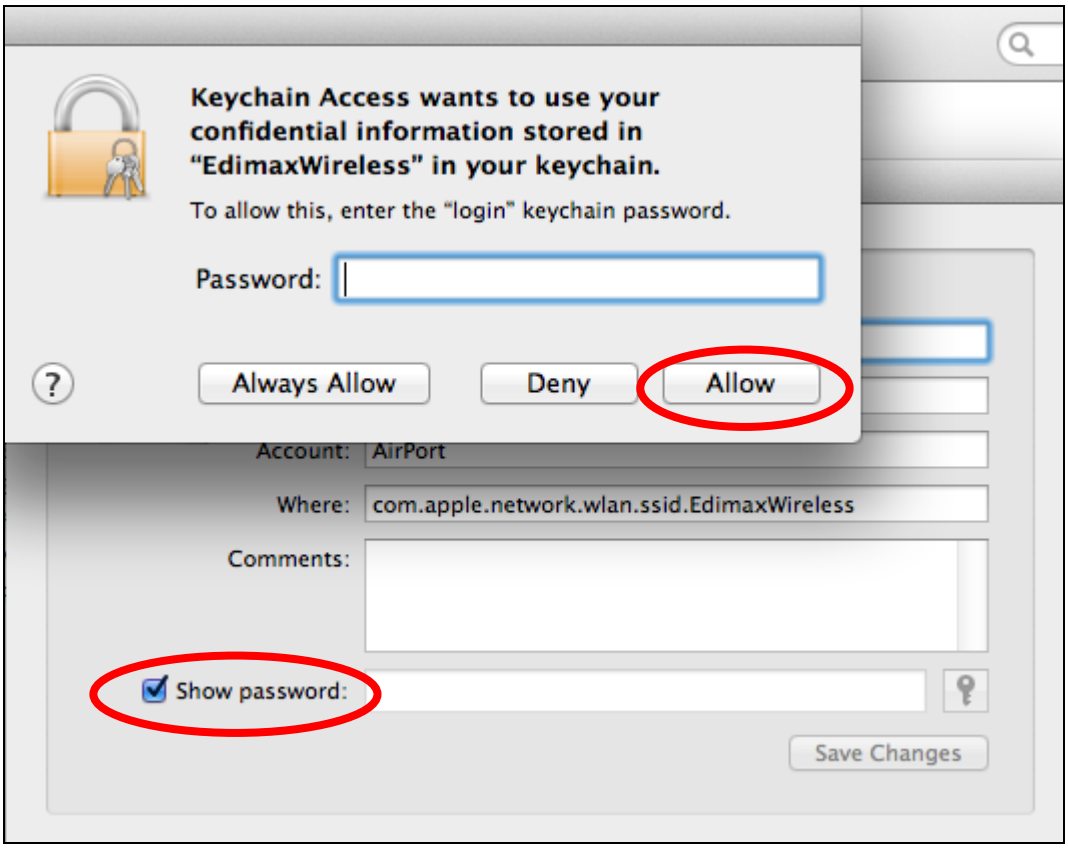
2. Select “Passwords” from the sub-menu labeled “Category” on the left side, as shown below. Then search the list in the main panel for the SSID of your network. In this example, the SSID is “EdimaxWireless” – though your SSID will be unique to your network.



3. Double click the SSID of your network and you will see the following window.



4. Check the box labeled “Show password” and you will be asked to enter your administrative password, which you use to log into your Mac. Enter your password and click “Allow”.



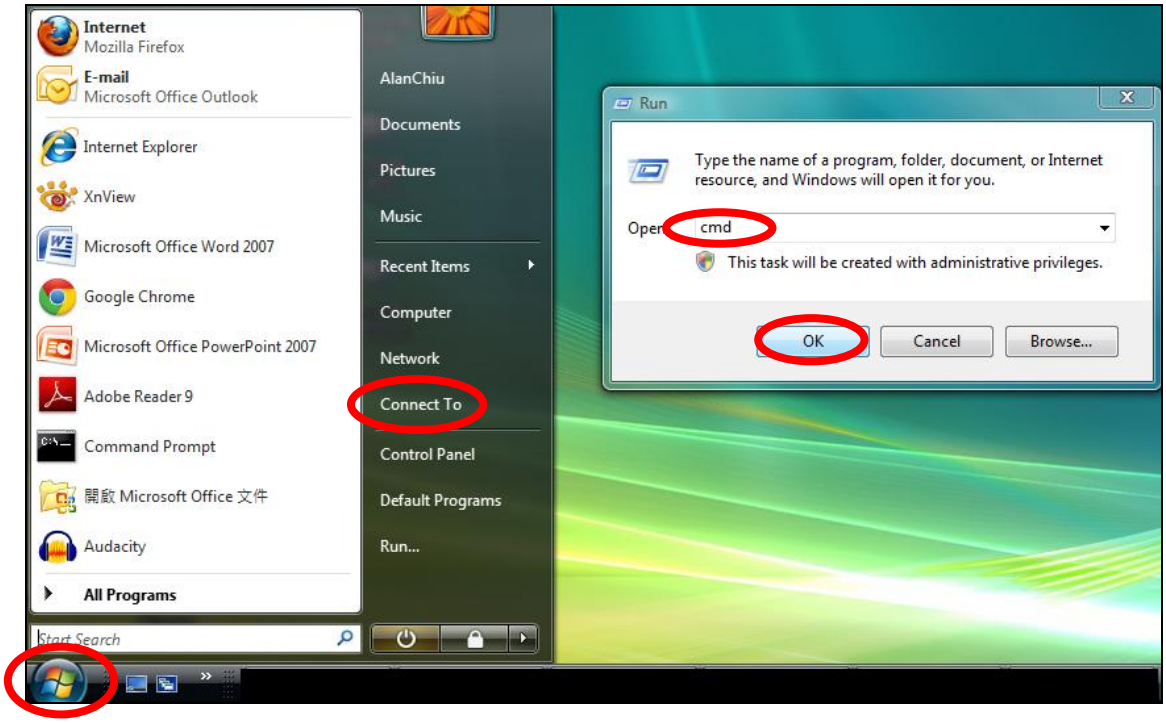
Your network security password will now be displayed in the field next to the box labeled “Show password”. In the example below, the network security password is “edimax1234”. Please make a note of your network security password.

IV-1-4. How to Find Your Router's IP Address

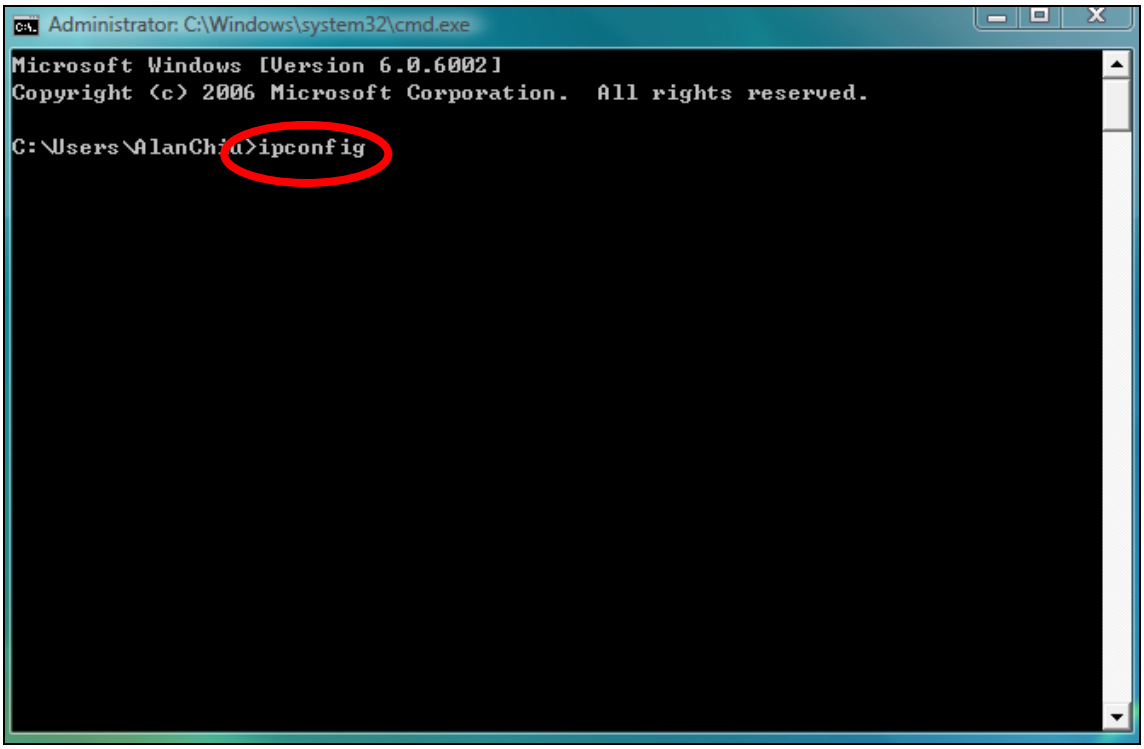
To find your router's IP address, please follow the instructions appropriate for your operating system.

IV-1-4-1. Windows Vista & 7

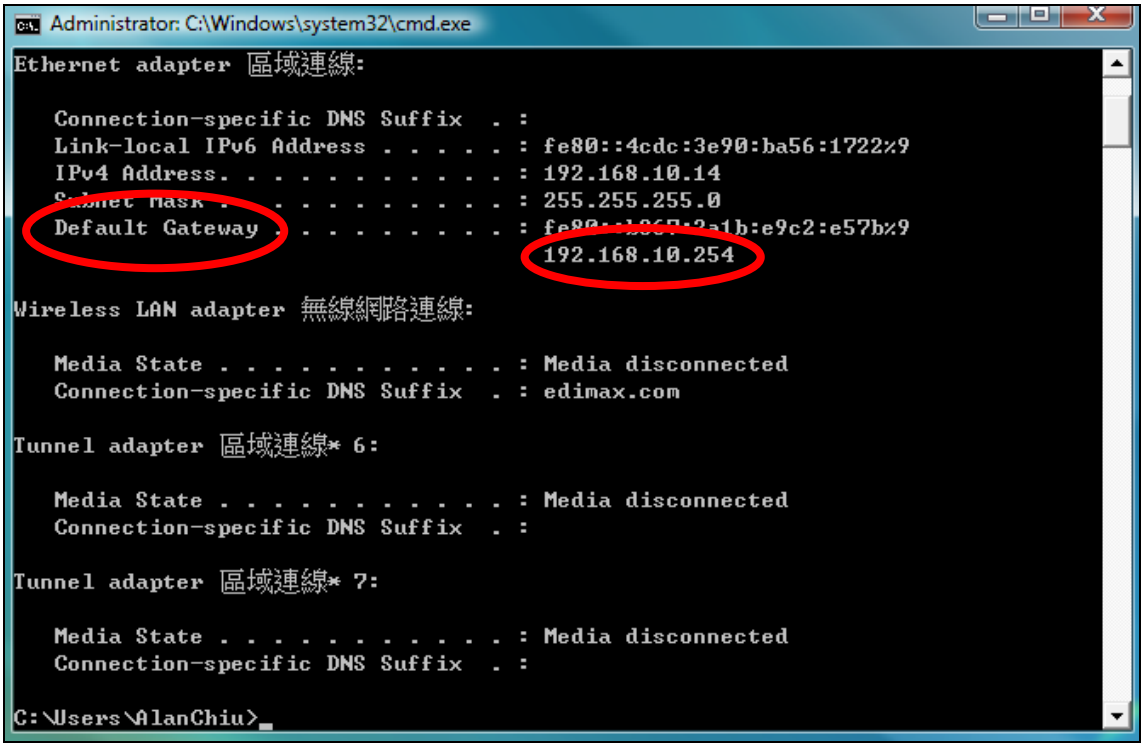
1. Go to "Start", select "Run" and type "cmd", then press Enter or click "OK".



2. A new window will open, type "ipconfig" and press Enter.



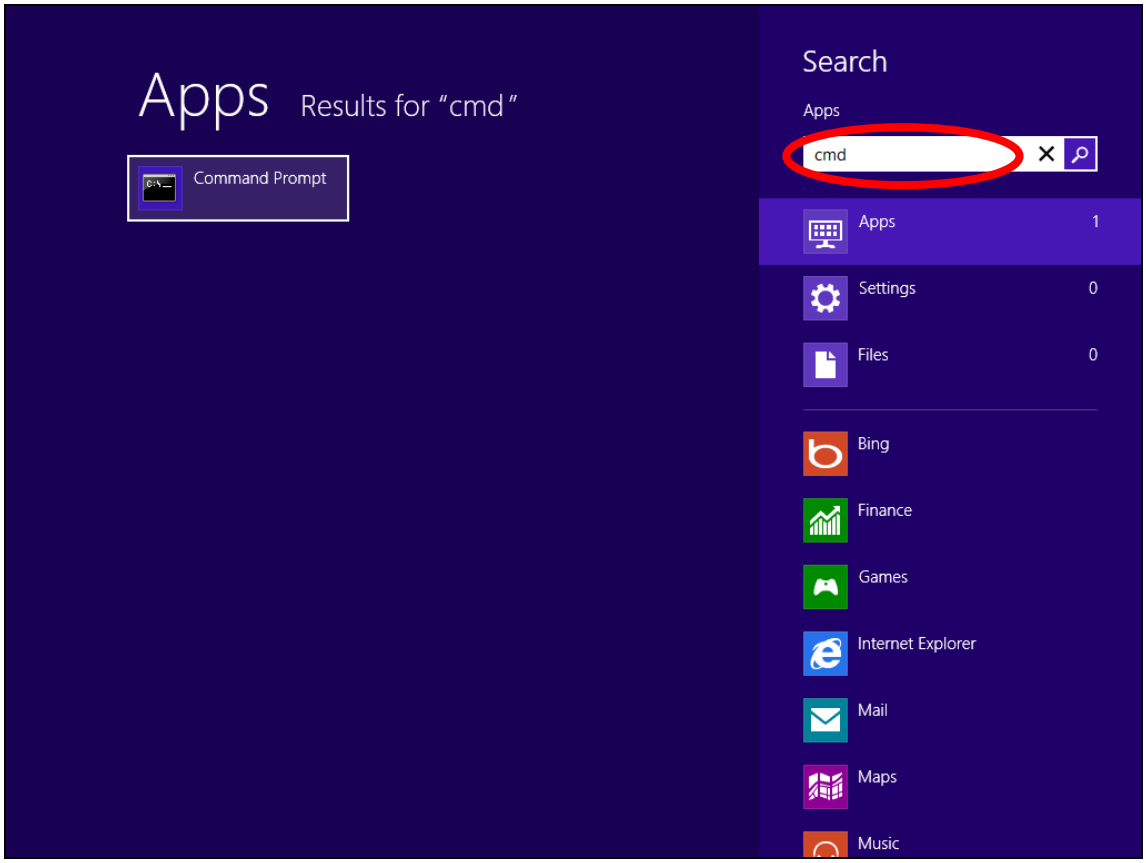
3. Your router's IP address will be displayed next to "Default Gateway".



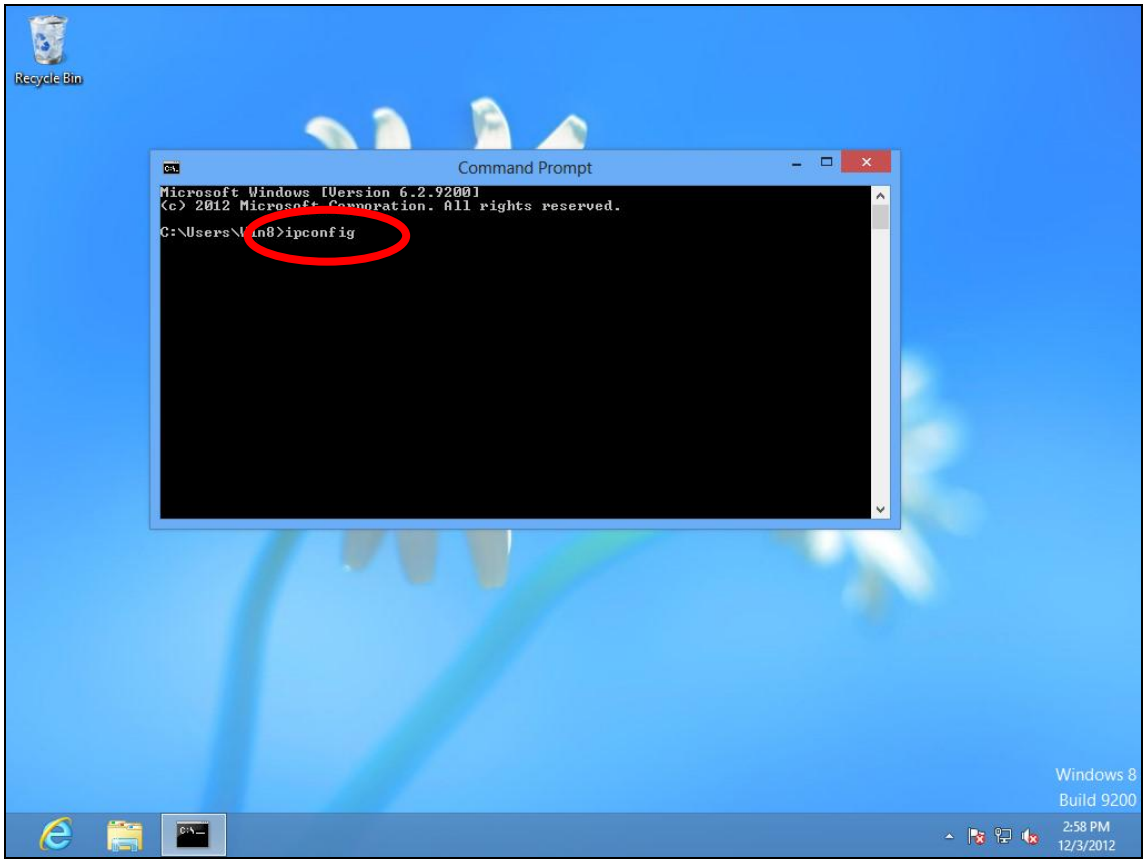
IV-1-4-2. Windows 8

1. From the Windows 8 Start screen, move your curser to the top right corner of the screen to display the Charms bar.

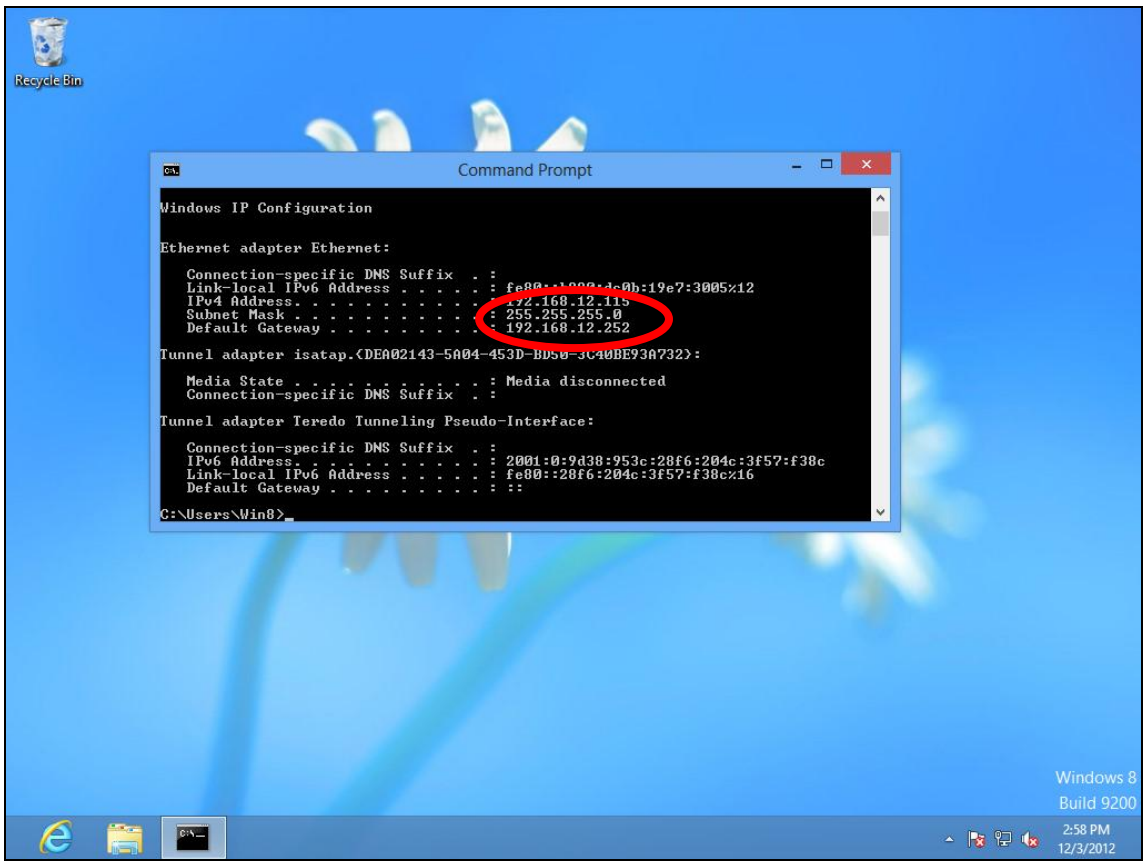
2. Click “Search” and enter “cmd” into the search bar. Click the “Command Prompt” app which be displayed on the left side.



3. A new window will open, type “ipconfig” and press Enter.



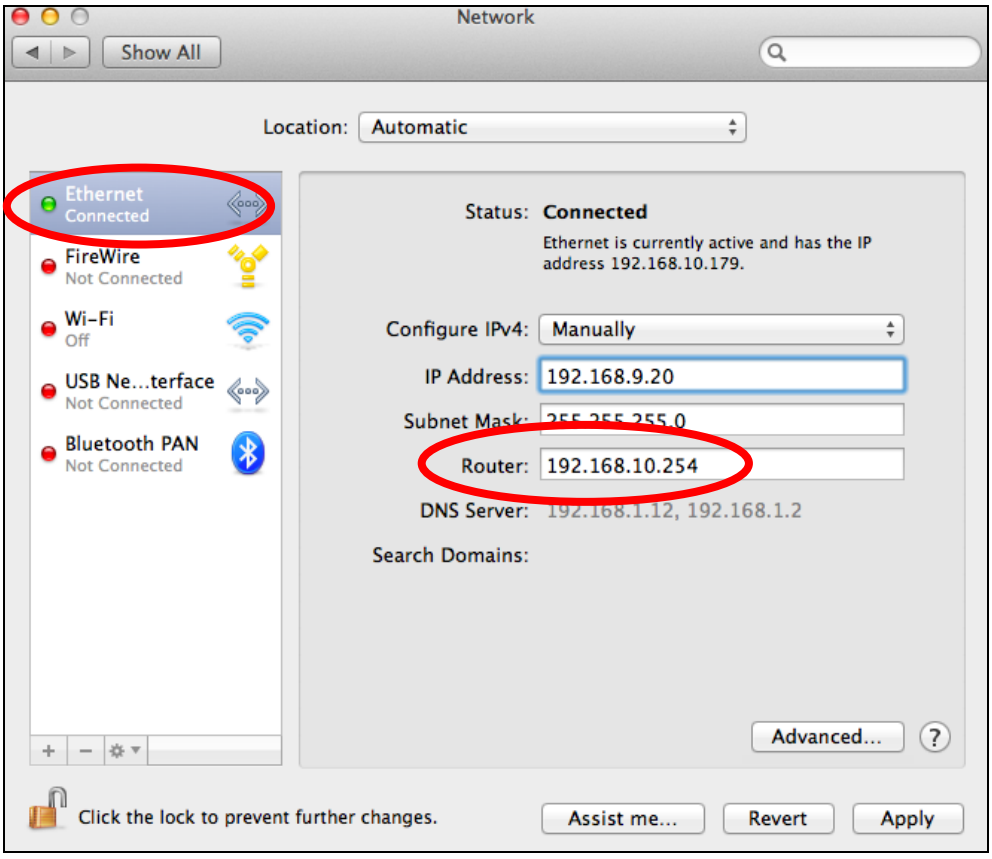
4. Your router's IP address will be displayed next to "Default Gateway".



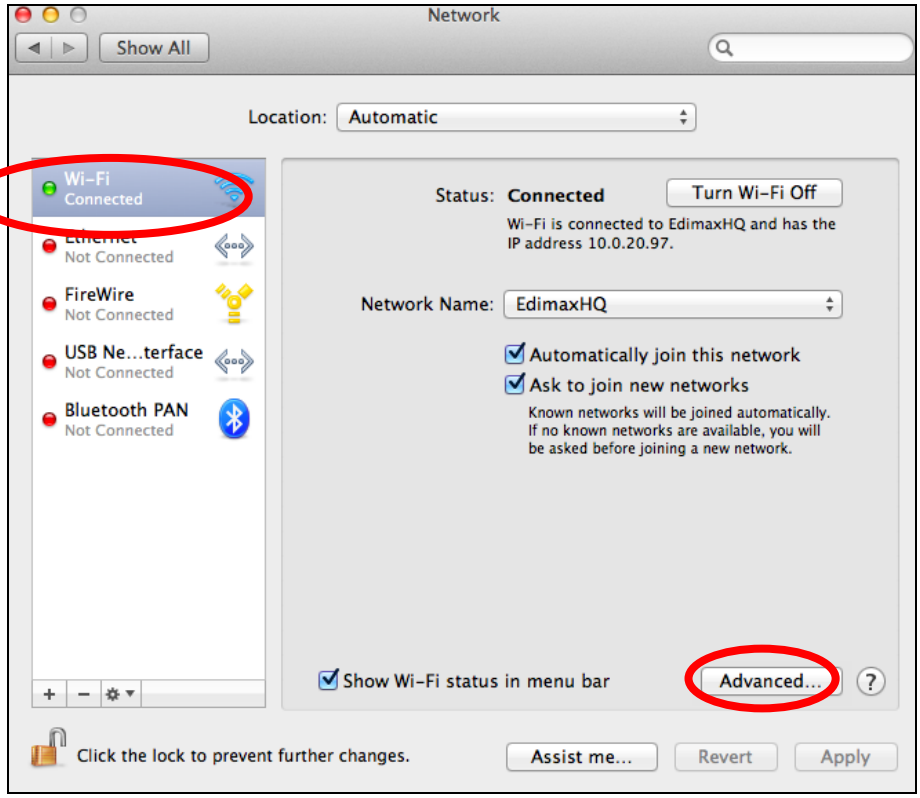
IV-1-4-3. Mac

1. Launch “System Preferences” and click on “Network”.

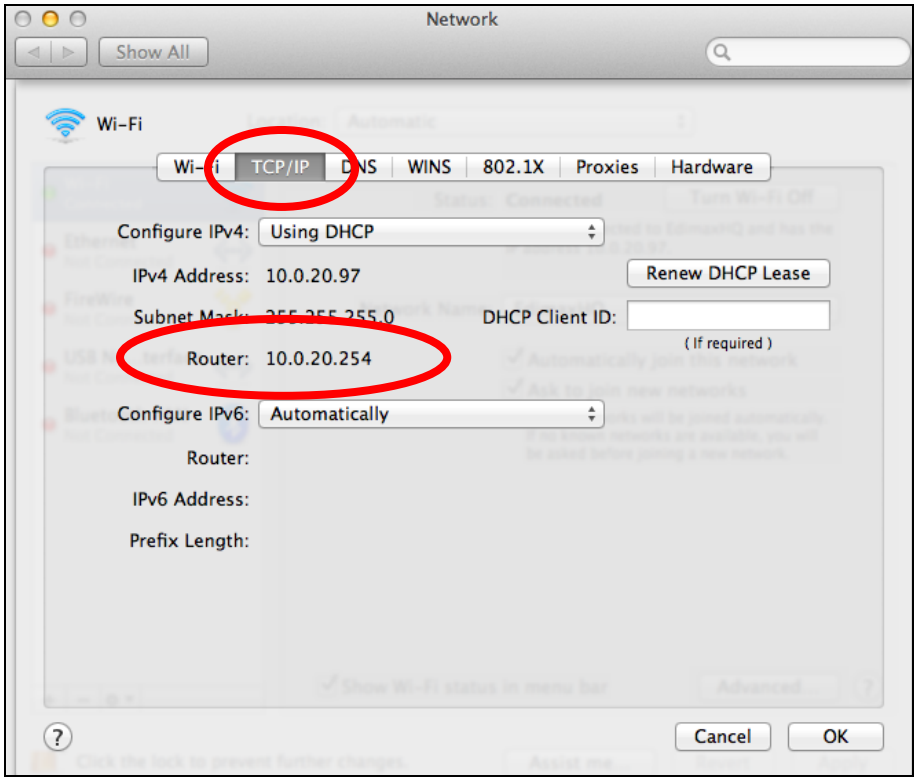
2. If you are using an Ethernet cable to connect to your network, your router’s IP address will be displayed next to “Router”.



3. If you are using Wi-Fi, click “Wi-Fi” in the left panel, and then “Advanced” in the bottom right corner.



4. Click the "TCP/IP" tab and your router's IP address will be displayed next to "Router".

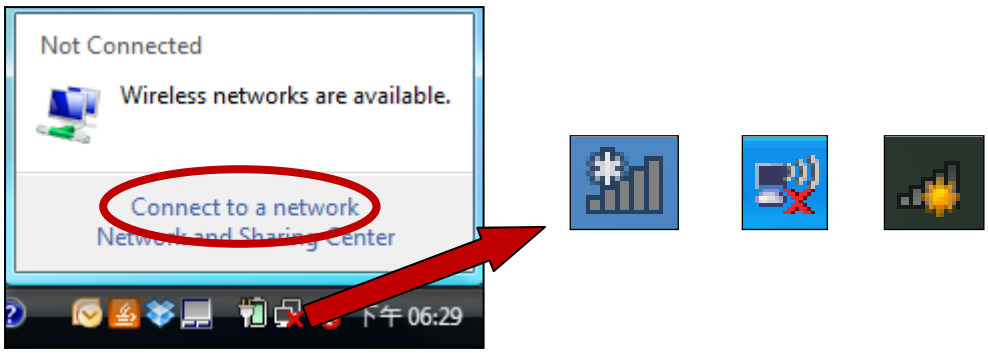


IV-2. Connecting to a Wi-Fi network

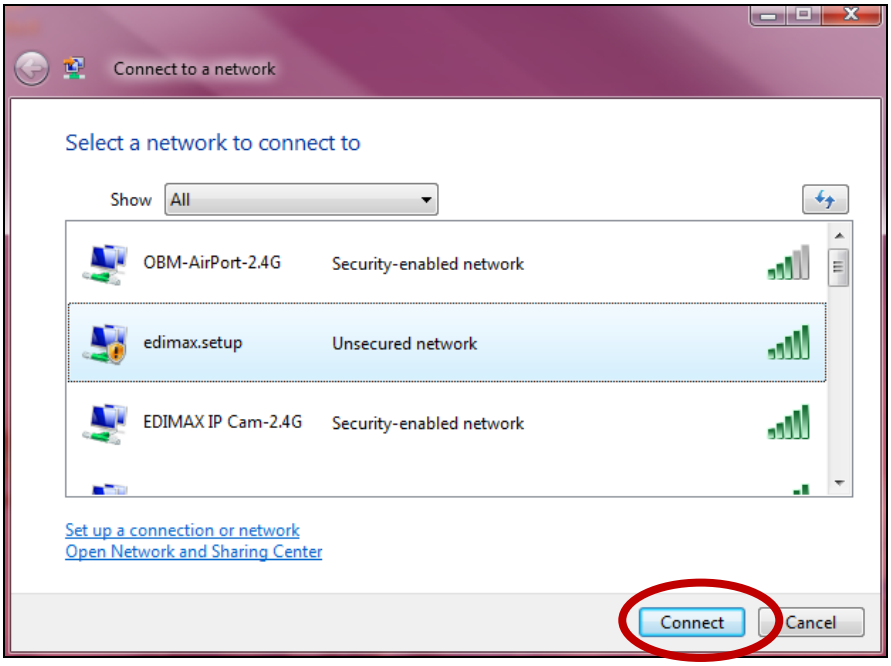
For help connecting to your device's ***Edimax.Setup*** SSID for initial setup, or to connect to your device's new Wi-Fi network (SSID) after setup is complete, follow the guide below:

> ***Below is an example of how to connect using Windows Vista – the process may vary slightly for other versions of Windows.***

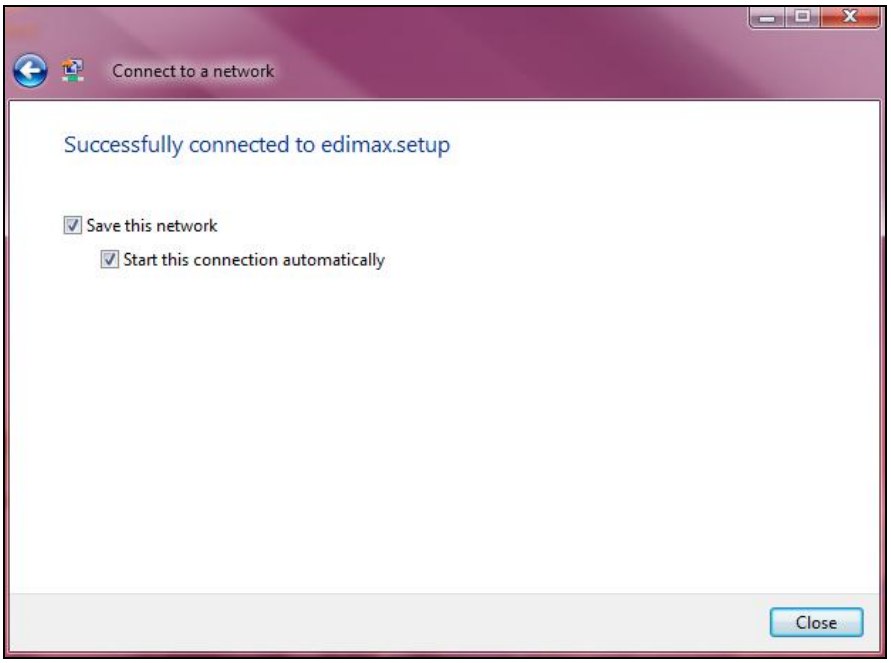
1. Click the network icon (, or) in the system tray and select **"Connect to a network"**.



2. Search for the SSID of your BR-6288ACL V2 and then click "Connect". If you set a password for your network, you will then be prompted to enter it.



3. After correctly entering your password, you will be successfully connected to the BR-6288ACL V2's wireless network.



IV-3. Troubleshooting

1. In range extender mode, is my BR-6288ACL V2 dual-band?

a. Yes. The BR-6288ACL V2 can extend 2.4GHz & 5GHz Wi-Fi signals concurrently, but you must connect your BR-6288ACL V2 to each (2.4GHz & 5GHz) network separately during iQ setup. During iQ Setup, you will be asked to select both a 2.4GHz & 5GHz Wi-Fi network to extend, as well as specify a new SSID (name) and password for each of the networks that your BR-6288ACL V2's will broadcast/extend.

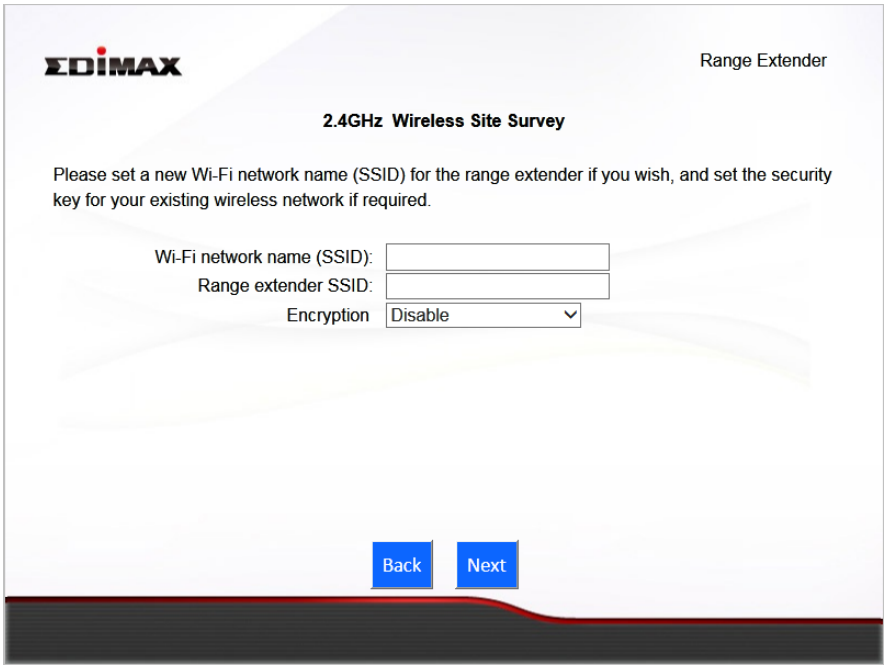
You can disable either 2.4GHz or 5GHz Wi-Fi during iQ setup if there is no appropriate source network available, or if you do not wish to use it. If either the 2.4GHz or 5GHz frequency band is disabled, wireless clients/devices on the same frequency band will be unable to connect to your range extender.

2. In range extender mode, if my BR-6288ACL V2 is set up as a dual-band extender, what happens when I connect a wired Ethernet client?

a. When you connect a network device to your BR-6288ACL V2 in range extender mode via Ethernet cable, by default the network device will connect to the 5GHz network. If there is no 5GHz network available, the network device will connect to the 2.4GHz network instead.

3. In range extender mode, how do I connect to a network which has a hidden SSID?

a. During iQ Setup, you can manually enter a SSID in the "Wi-Fi network name" field as shown below, for either/both 2.4GHz and 5GHz, along with the relevant encryption information.



Wi-Fi network name	Enter the SSID (network name) of your existing, hidden network.
Range extender SSID	Enter an SSID for the BR-6288ACL V2 or leave it blank to use a default which consists of your existing router's SSID (above) +"_2EX".
Encryption	Select and enter the encryption information for your existing, hidden network.

4. I can't access the Internet.

a. Ensure that all cables are connected properly. Try a different Ethernet cable.
b. Check if you can access the web based configuration interface. If not, please ensure your Wi-Fi device is set to use a dynamic IP address. If you are unsure how to do this, try using a computer and refer to the user manual for guidance.
c. Login to the web based configuration interface and go to **Internet > WAN Setup** and check that the connection type is correct. If you are unsure which internet connection type you have, please contact your Internet Service Provider (ISP).
d. Connect a computer directly to your modem and check if you can access the internet. If you can't, please contact your Internet service provider for assistance.

5. I can't open the web based configuration interface.

a. Please ensure your Wi-Fi device is set to use a dynamic IP address. If you are unsure how to do this, try using a computer and refer to **IV-1-1. How to check that your computer uses a dynamic IP address.**

6. I forgot my password.

a. Reset the router to its factory default settings and use the default username **admin** and default password **1234**.

7. My BR-6288ACL V2 has a weak wireless signal.

Weak signals are usually caused by interference from other devices or obstacles blocking the BR-6288ACL V2's wireless signal:

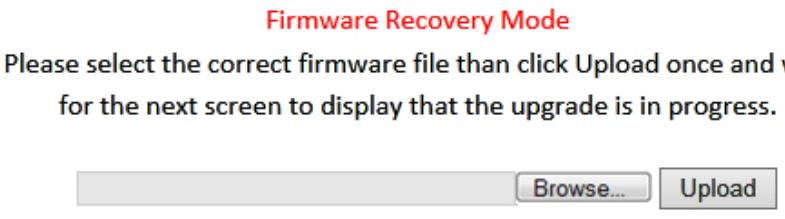
a. Keep the device away from other radio devices such as microwaves or cordless phones.
b. Do not put the device in the corner of a room or under/nearby metal.
c. Ensure there are as few obstacles as possible between the BR-6288ACL V2 and your wireless network device.

In range extender mode, the BR-6288ACL V2's weak wireless signal may be in turn caused by a weak signal from your existing router. It's important to choose a good location for the BR-6288ACL V2 *in relation to your existing wireless router*. The best location is roughly in the middle between your existing wireless router and the area you would like to be covered by the BR-6288ACL V2. If you are too far away from your existing router, then it is difficult for the BR-6288ACL V2 to receive a wireless signal.

8. A firmware upgrade failed and the BR-6288ACL V2 isn't working.

Firmware upgrade failures can happen occasionally due to power cuts or unstable connections. In this scenario, you need to first connect a computer to one of your BR-6288ACL V2's LAN ports using an Ethernet cable. Then you need to modify your computer's IP address to ***192.168.2.x*** where ***x*** is any value between ***3*** and ***254***. Refer to IV-1-2. How to modify the IP address of your computer if you need guidance to do so.

From there, you need to go to 192.168.2.1 in a web browser, and you will see the page below:



Click “Browse” to locate the firmware file on your computer and then click “Upload” to upload the new firmware. It may take several minutes to complete, please wait and follow the instructions on screen.

V. Glossary

Default Gateway (Wireless bridge): Every non-access point IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandaccess point.com) and one or more IP addresses (such as 74.125.128.104). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Access point: A access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

COPYRIGHT

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

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

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

Federal Communication Commission Interference Statement

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

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

FCC Caution

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

The equipment version marketed in US is restricted to usage of the channels 1-11 only. This equipment is restricted to ***indoor*** use when operated in the 5.15 to 5.25 GHz frequency range.

RED Compliance Statement

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

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

Frequency range (MHz)	Max. Transmit Power (dBm)
2400-2483.5	18.35 dBm
5150-5250	18.72 dBm

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

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type **AC600 Multi-Function Dual-Band Wi-Fi Extender** is in compliance with Directive 2014/53/EU

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

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

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

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/35/EU.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU.

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/35/EU.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/35/EU).

Türkçe: Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/35/EU.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU.

Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/53/EU, 2014/35/EU.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/35/EU.

suomen kieli: Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR DE GR HU
IE IT LV LT LU MT NL PL PT SK SI ES SE
GB IS LI NO CH BG RO RU TR UA

WEEE Directive & Product Disposal

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

Declaration of Conformity

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

Equipment: AC600 Multi-Function Dual-Band Wi-Fi Extender
Model No.: BR-6288ACL V2

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

Spectrum	:	EN 300 328 V2.1.1 (2016-11)
		EN 301 893 V2.1.1 (2017-05)
EMC	:	EN 301 489-1 V2.0.0 (2017-03)
		EN 301 489-17 V3.2.0 (2017-03)
EMF	:	EN 62311:2008
Safety (LVD)	:	IEC 60950-1:2005 (2nd Edition)+Am 1:2009+Am 2:2013
		EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

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

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

Signature:

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

CE

Date of Signature: July, 2017
Signature:

Printed Name: Albert Chang
Title: Director
Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

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

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

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

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

Preamble

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

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

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

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

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

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

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

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

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

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

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

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

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

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