Edimax Gemini
Home Roaming Wi-Fi Extender
RE23S

User Manual

10-2017 / v1.0

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

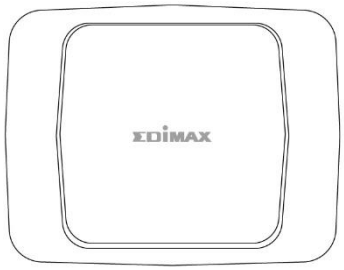
Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA
Live Tech Support: 1(800) 652-6776
Email: support@edimax.com

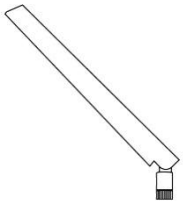
CONTENTS

I Product Information

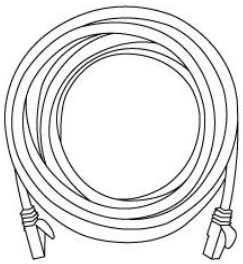
I-1 Package Contents



RE23S



Antenna (2pcs)



Ethernet Cable

Access Key Card

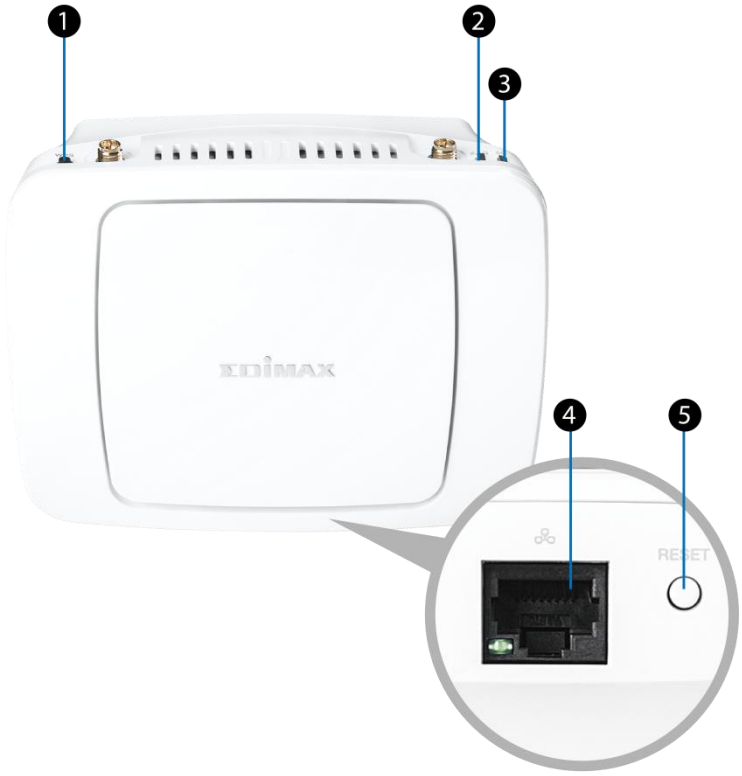
CD with multi-language QIG & user manual

Quick installation guide (QIG)

I-2 System Requirements

- Wi-Fi extender/Wi-Fi bridge mode: Existing 2.4GHz and/or 5GHz wireless network
- Access point mode: Cable/DSL modem router
- Computer with 802.11/b/g/n/a/ac Wi-Fi adapter, and web browser for software configuration (Internet Explorer, Google Chrome, Firefox, Opera or Safari latest version)
- Smartphone setup: iOS 6 or Android 4.x and above

I-3 Device Overview



① WPS Button
② LED: Power, WPS, Reset
③ LED: Wireless
④ LAN Port
(Gigabit Ethernet Port)
⑤ Reset Button

I-4 LED Status

Icon	LED	Status / Color	Indication
	Wireless	On / Green On / Yellow Flash / Red Off	Excellent Performance Good Performance Poor Performance No Signal
	Power WPS Reset	On / Green Slow Flash / Green Quick Flash / Green Off	System On WPS Mode Booting Up or Resetting to Factory Default Setting Power Off

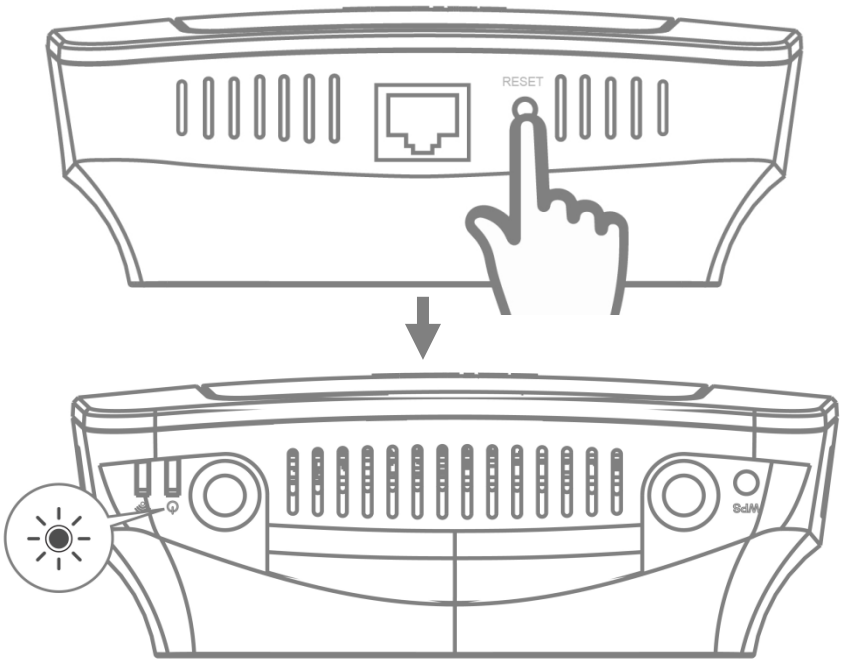
I-5 Hardware Explanation

Port / Button	Description
LAN Port	For "**Access Point Mode**", connect this port to the wireless broadband router During "**Extender Mode**", this port can be used for LAN-only devices
WPS Button	**WPS Function**: Press and hold this button for 1-3 seconds to activate WPS
Reset Button	**Factory Reset Function**: Press and hold this button for over 10 seconds

I-6 Reset to Factory Settings

If you experience problems with the device or if you want to change the device to a different operating mode, you can reset the device back to its factory settings. This resets **all** settings back to default.

1. Press and hold the Reset Button for at least 10 seconds and release when the **green** power LED is **flashing quickly**.



2. Wait for the device to restart. The device is ready for setup when the **green** power LED displays **on**.

I-7 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 RE23S.

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.

9. If you smell burning or see smoke coming from the RE23S then unplug the device immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

II Installation

The device can be configured into different modes. The table below explains the functions of each mode:

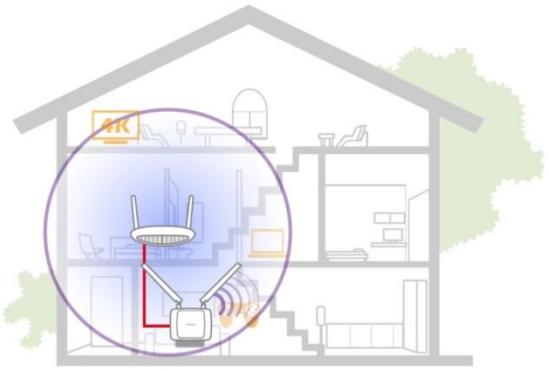
Wi-Fi Extender	*The device connects wirelessly to your existing network and repeats the wireless signal.* **Location:** The best location for your extender is roughly in the middle between your existing wireless router / master device and the dead zone. The extender needs to receive a good Wi-Fi signal from your router / master device.
Wi-Fi Access Point	*The device connects to an existing router via Ethernet cable and provides wireless Internet access for your network devices.* **Location:** Where your Ethernet cable reaches.
Wi-Fi Bridge (Wi-Fi Adapter)	*The device connects to an Ethernet device such as a games console or smart TV via Ethernet cable and provides wireless Internet access for that device.* **Location:** Within Wi-Fi coverage, close to your wired network device.

Roaming

The device supports roaming, meaning that after Wi-Fi devices are connected (smart phones, tablets, laptop computer etc.), these devices will automatically connect to the best available Wi-Fi signal as they move around.

II-1 Setup RE23S as an Access Point

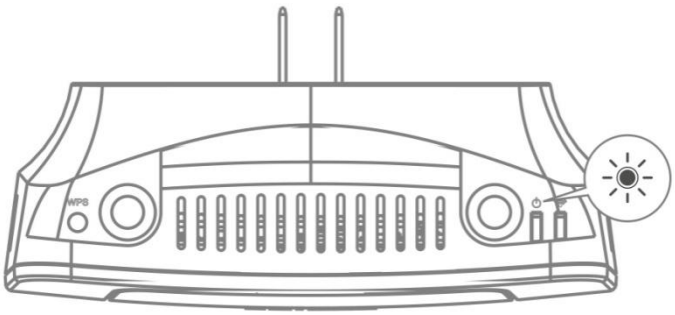
II-1-1 **Scenario 1:** You are using a ***General Router***



With this setup, users can enjoy extended coverage around the house. The Access Point has to be setup with a ***separate*** wireless name and connection password just like your router (original Wi-Fi SSID (network name) and password can be found on the Access Key Card).

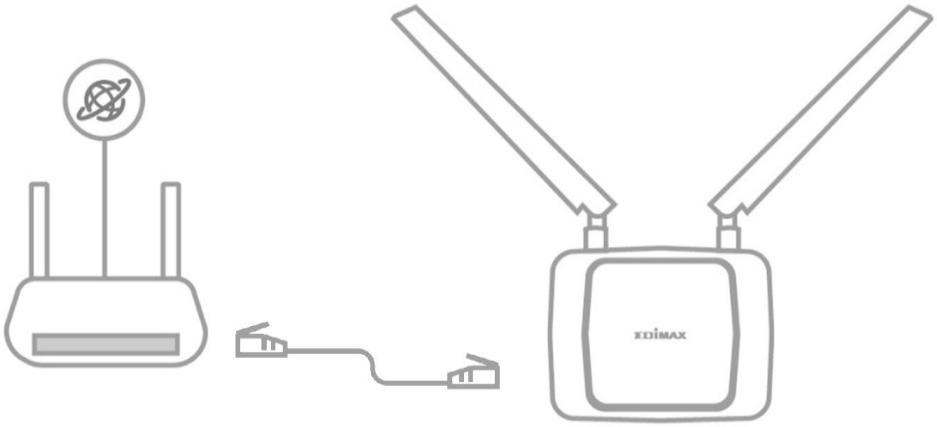
Step 1: Power up the device

Power up the device by plugging it into a power socket and wait for the Power LED to turn on.



Step 2: Set the device as an **Access Point**:

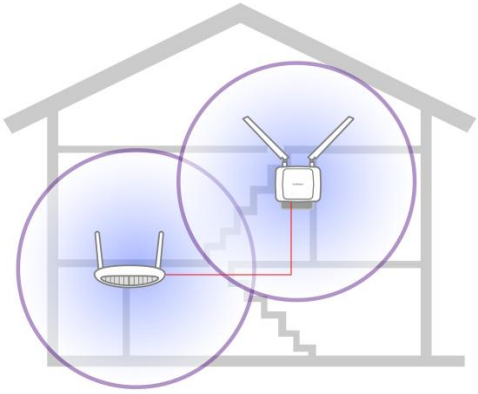
1. Connect the device to a LAN router using their respective LAN port.
2. The device will automatically link to your router
3. Connect a wireless device to confirm internet connectivity.



NOTE: The original Wi-Fi SSID (network name) and password for the device can be found on the Access Key Card in the package.

Example:

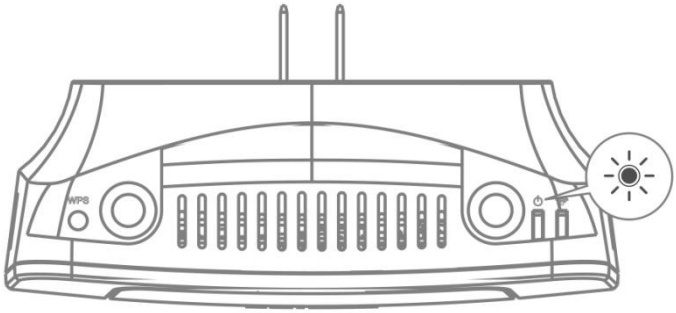
II-1-2 **Scenario 2:** You are using an ***Edimax Roaming Router***



Once the device is connected to the Edimax Roaming Router as an access point, devices using the internet connection can enjoy seamless connection within the wireless coverage with ***ONE network name and password***.

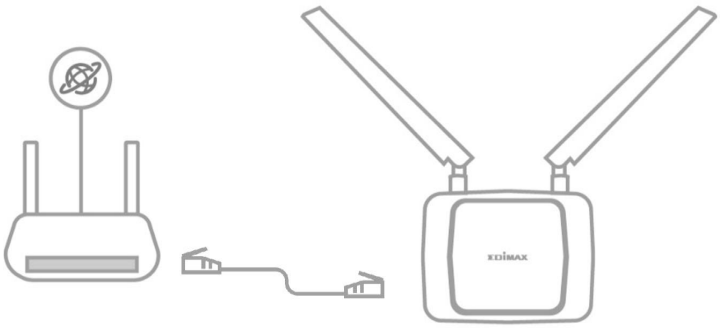
Step 1: Power up the device

Power up the device by plugging it into a power socket and wait for the Power LED to turn on.



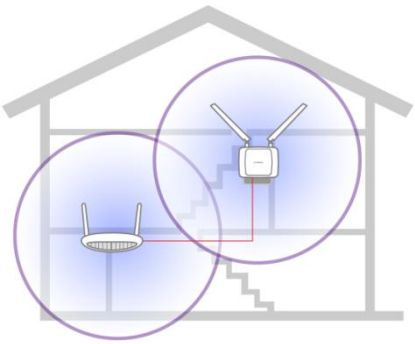
Step 2: Set the device as an **Access Point**:

1. Connect the device to the LAN router using their respective LAN port.
2. The device will automatically link to your router
3. Connect a wireless device to confirm internet connectivity.



Congratulations!

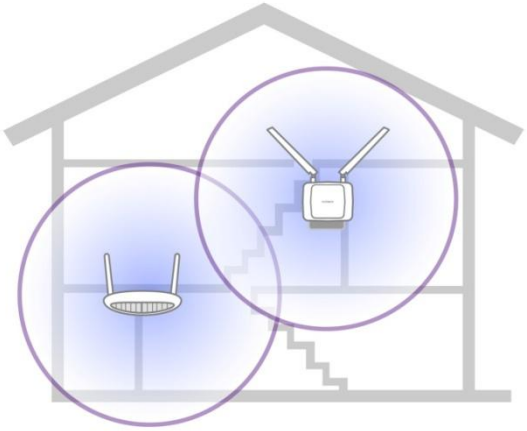
The Whole Home Wi-Fi system setup is completed! Each user will only require one Wi-Fi network name and password for your Wi-Fi system (The Wi-Fi network name and password of the roaming router).



II-2 Setup RE23S as an Extender

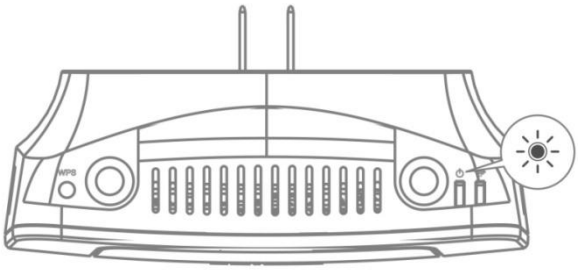
II-2-1 **Scenario 3:** You are using a ***General Router***

With this setup, users can enjoy extended coverage around the house. The Extender has to be setup with a ***separate*** wireless name and connection password just like your router (original Wi-Fi network name and password can be found on the Access Key Card)



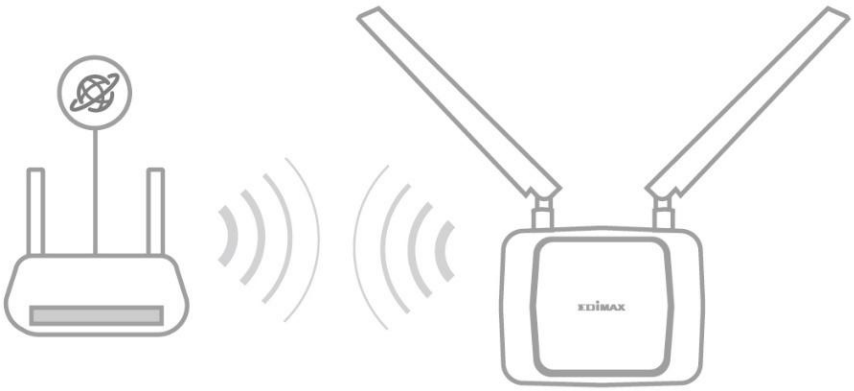
Step 1: Power up the device

Power up the device by plugging it into a power socket near the Wi-Fi router and wait for the Power LED to turn on.



Step 2 option A: Set the device as an Extender **using WPS**:

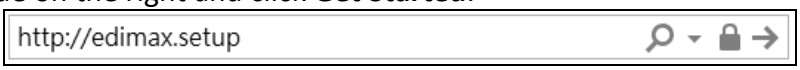
1. Turn on the WPS function on the router (e.g. pressing and holding the WPS button of the router).
2. Press and hold the WPS button of the device for 3 seconds. The Power LED should be flashing slowly.
3. Check the **Wi-Fi LED** of the device to make sure there's a signal. If the LED is **off**, move the extender closer to the router and retry.



Step 2 option B: Set the device as an Extender **using IQ setup**:

1. Connect a Wi-Fi capable device to the Extender:
   On your Wi-Fi capable device, search for the SSID **Edimax_xx_xx**, connect to it and enter the password when prompted. (The Wi-Fi SSID (network name) and password are printed on the Access Key Card).

2. Open a web browser and enter the URL ***http://edimax.setup*** or scan the QR-Code on the right and click **Get Started**.



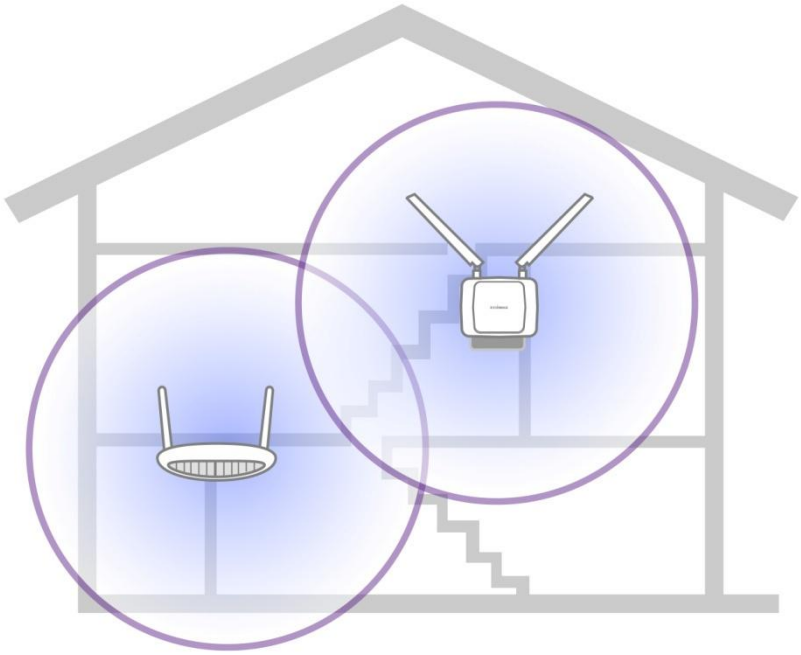
3. Select "**YES, I NEED A Wi-Fi EXTENDER"** to continue setup (shown below).

4. Follow the on-screen instructions to complete setup (Refer to ***II-4-1 Wi-Fi Extender Mode*** if you have any concern).
5. Check the **Wi-Fi LED** of the device to make sure there's a signal. If the LED is **off**, move the extender closer and retry.

Note: If you **cannot access** *http://edimax.setup*, please make sure your Wi-Fi capable device is set to use a **dynamic IP address.**

Step 3: Relocate the Extender

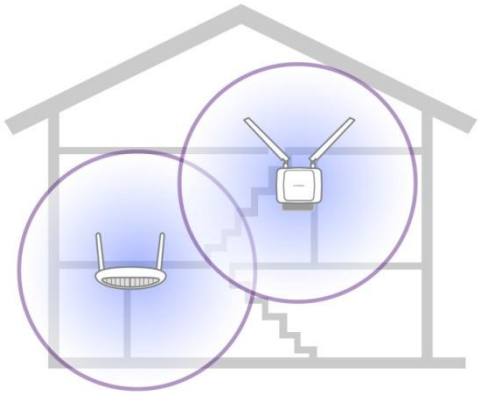
1. Please relocate the extender to achieve the desired coverage.
2. Observe the Wi-Fi LED behavior to determine whether the location is appropriate.
   For maximum coverage, relocate the extender to where signal strength is at Good Performance (where the signal coverage of both the extender and the Wi-Fi Router are less overlapped).



NOTE:

Wi-Fi LED	Connection Quality
On / Green	Excellent Performance
On / Yellow	Good Performance
Flash / Red	Poor Performance
Off	No Signal

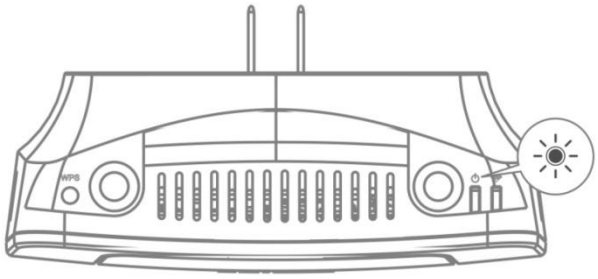
II-2-2 **Scenario 4:** You are using an ***Edimax Roaming Router***



Once the device is connected to the Edimax Roaming Router, devices can enjoy seamless connection within the wireless coverage with ***ONE network name and password***.

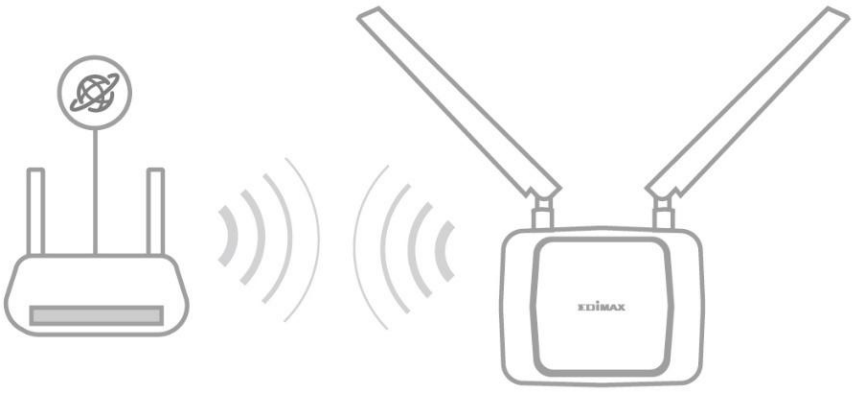
Step 1: Power up the device

Power up the device by plugging it into a power socket near the Wi-Fi router and wait for the Power LED to turn on.



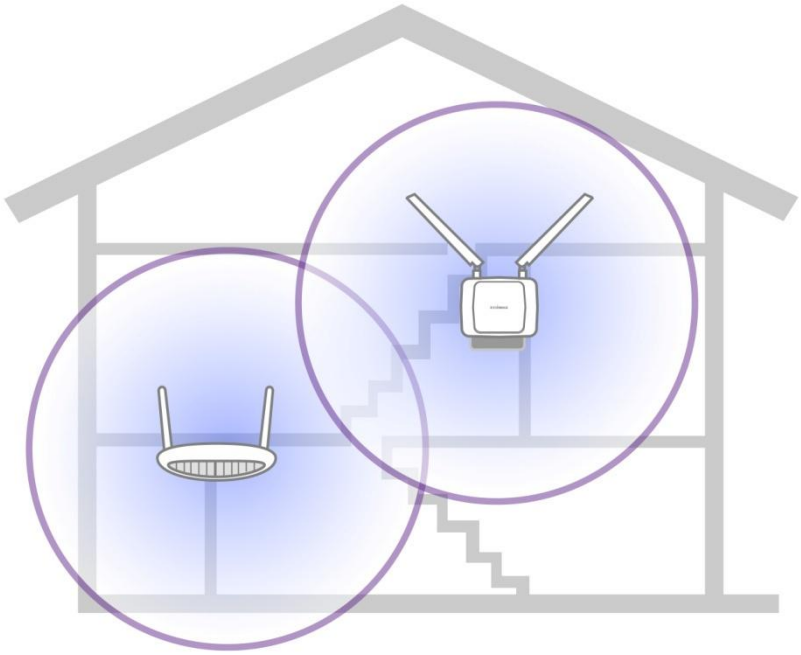
Step 2: Set the device as an Extender **using WPS**:

1. Turn on the WPS function on the Edimax Roaming Router (pressing and holding the WPS button for 3 seconds).
2. Within 2 minutes, press and hold the WPS button of the device for 3 seconds. The Power LED should be flashing slowly.
3. Check the **Wi-Fi LED** of the extender to make sure there's a signal. If the LED is **off**, move the extender closer to the router and retry.



Step 3: Relocate the device

1. Please relocate the device to achieve the desired coverage.
2. Observe the Wi-Fi LED behavior to determine whether the location is appropriate.
   For maximum coverage, relocate the device to where signal strength is at Good Performance (where the signal coverage of both the extender and the Wi-Fi Router are less overlapped).



NOTE:

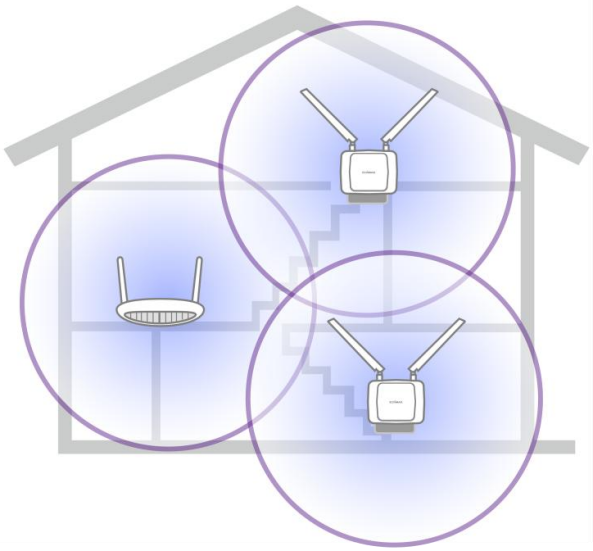
Wi-Fi LED	Connection Quality
On / Green	Excellent Performance
On / Yellow	Good Performance
Flash / Red	Poor Performance
Off	No Signal

Congratulations!

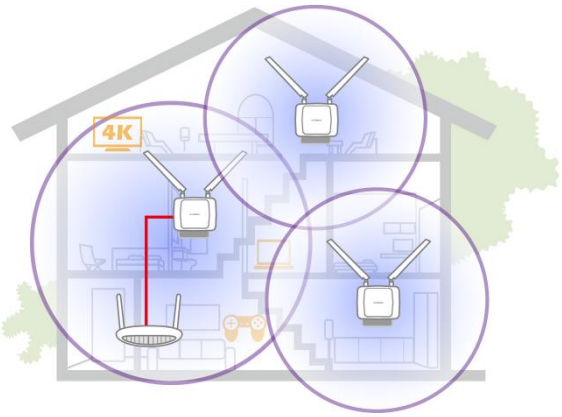
The Whole Home Wi-Fi system setup is completed! Each user will only require one network name and password for your Wi-Fi system.

More Coverage!

Should you feel some areas of your home require better coverage, additional Edimax extenders (available for purchase separately) can be installed! Go through *Steps 1 to 3* to setup extra extenders. An example coverage plan is shown below:



II-3 Special Scenario

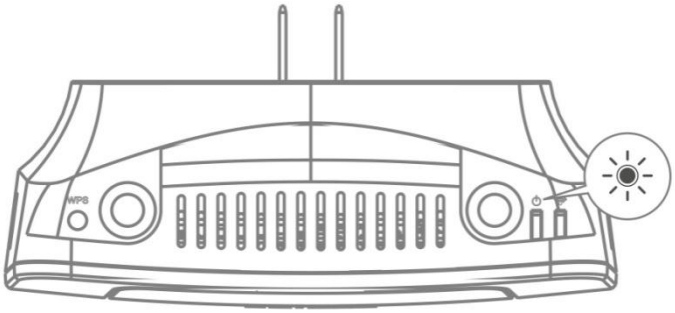


II-3-1 Scenario 5: using a ***General Router*** but also having ***Roaming Capability***

Like in Scenario 1, the Access Point has to be setup with a ***separate*** wireless name and connection password just like your router. However, if you still wish to have the roaming function, extra Extenders (available for purchase separately) can be setup to achieve it. Follow the instructions below:

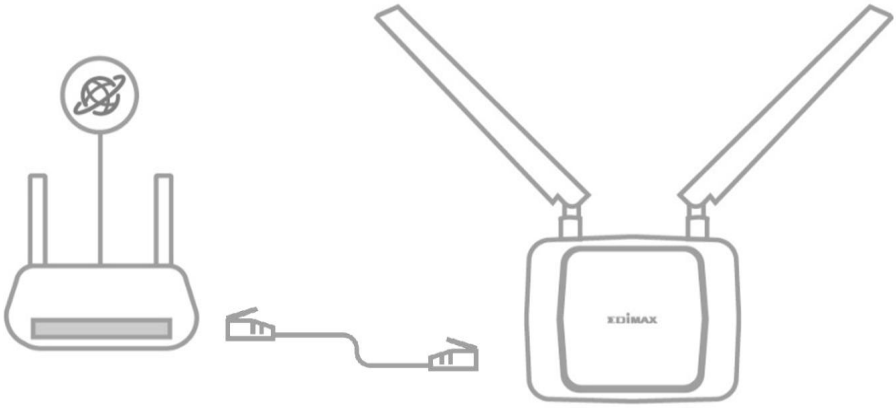
Step 1: Power up the master device

Power up the device by plugging it into a power socket and wait for the Power LED to turn on.



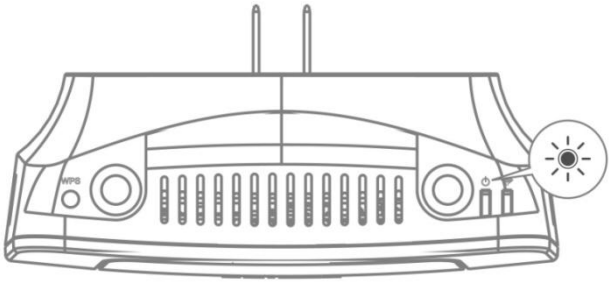
Step 2: Set the master device as an ***Access Point***:

1. Connect the master device to a LAN router using their respective LAN port.
2. The device will automatically link to your router
3. Connect a wireless device to confirm internet connectivity.



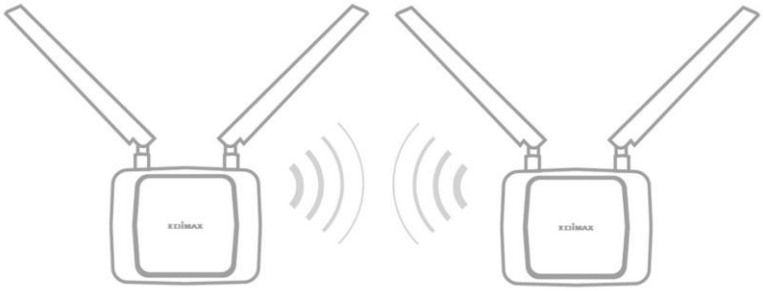
NOTE: The Wi-Fi SSID (network name) and password for the device can be found on the Access Key Card in the package. Example:

Step 3: Setup a slave device by powering up the device
Power up a second device near the Wi-Fi router and wait for the Power LED to turn on.



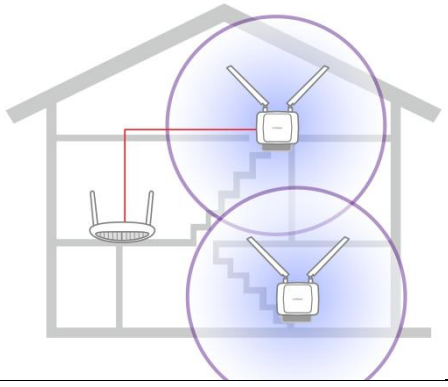
Step 4: Setup the slave device as an ***Extender*** **using WPS**:

1. Turn on the WPS function on the master device (pressing and holding the WPS button for 3 seconds).
2. Within 2 minutes, press and hold the WPS button of the slave device for 3 seconds. The Power LED should be flashing slowly.
3. Check the **Wi-Fi LED** of the slave device to make sure there's a signal. If the LED is **off**, move the extender closer and retry.



Step 5: Relocate the slave device (extender)

1. Please relocate the slave device to achieve the desired coverage.
2. Observe the Wi-Fi LED behavior to determine whether the location is appropriate.
   For maximum coverage, relocate the slave device to where signal strength is at Good Performance (where the signal coverage of both the master and slave devices are less overlapped).

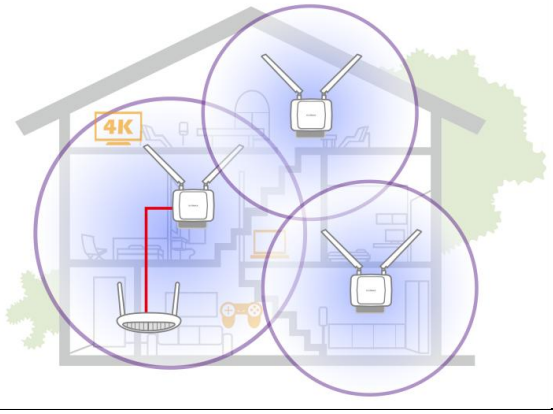


NOTE:

Wi-Fi LED	Connection Quality
On / Green	Excellent Performance
On / Yellow	Good Performance
Flash / Red	Poor Performance
Off	No Signal

More Coverage!

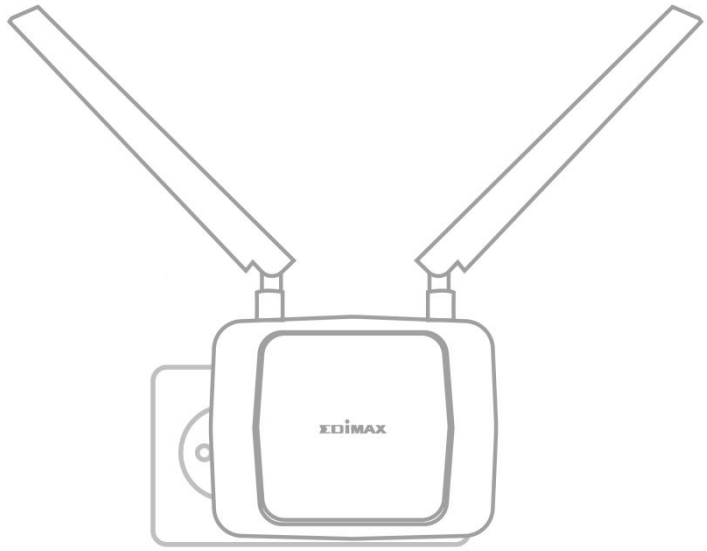
Should you feel some areas of your home require better coverage, additional Edimax extenders (available for purchase separately) can be installed! Go through *Steps 3 to 5* to setup extra extenders. An example floor plan is shown below:



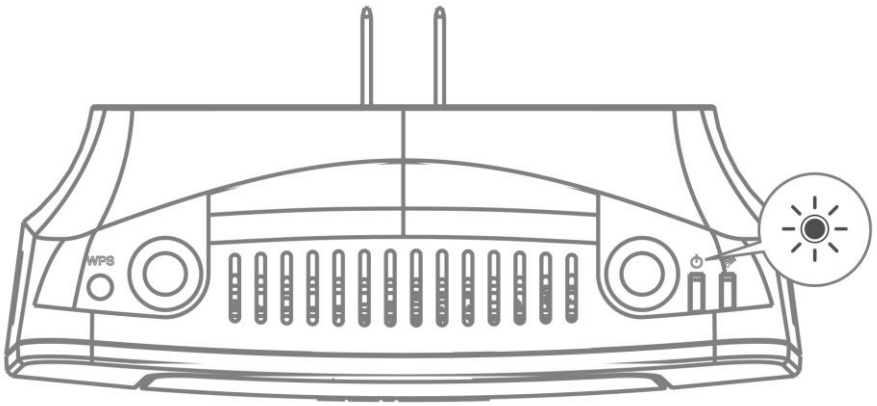
II-4 IQ Setup

Below outlines the steps to connect your device to your home Wi-Fi router using a Wi-Fi capable device (e.g. mobile phone, tablet, laptop computers, etc.)

1. Plug the extender device into a power socket.



2. The power LED will **flash quickly** in **green** color to indicate the device is starting up. The device is ready when the power LED is turned on in **solid green**.



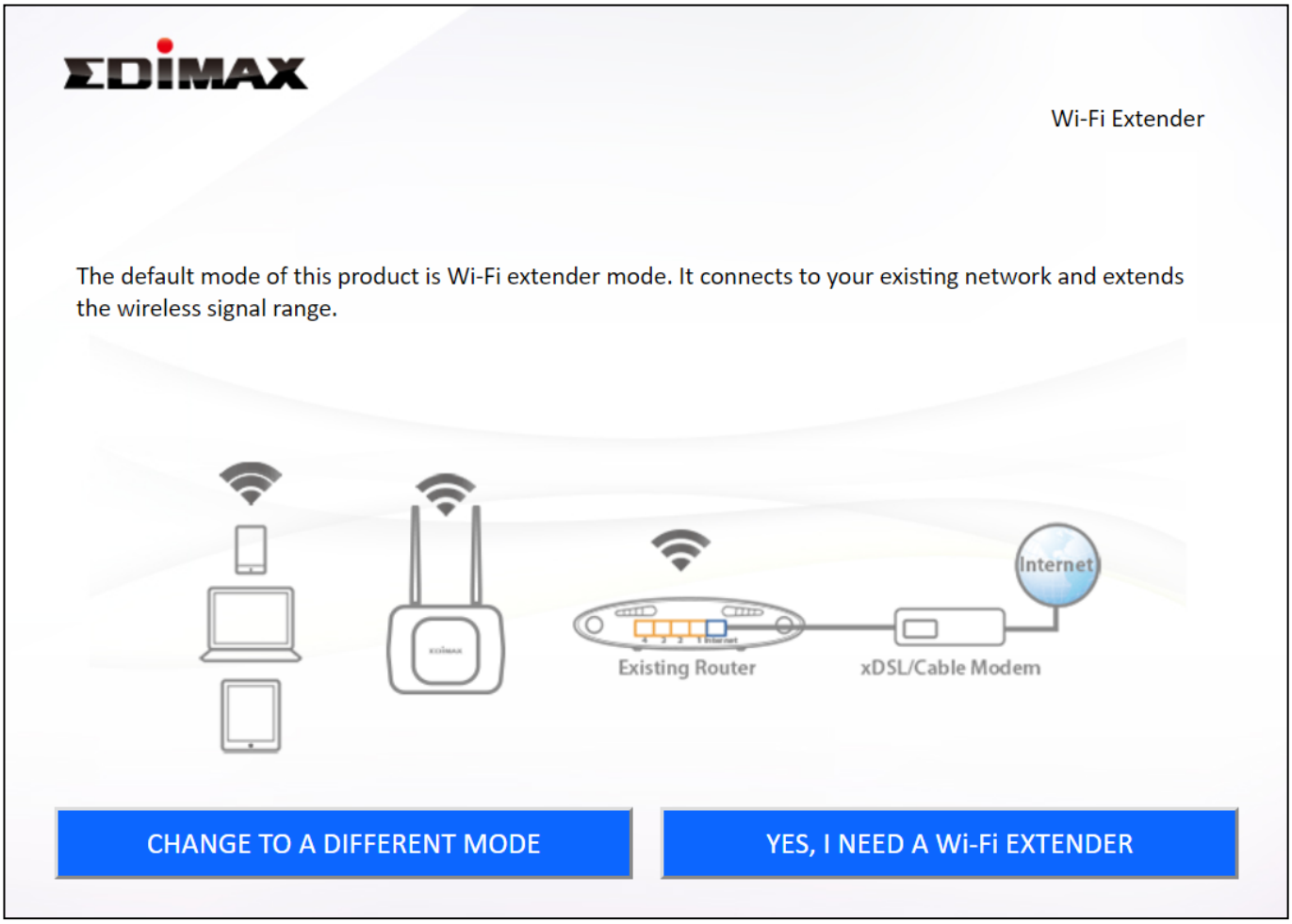
3. Use a Wi-Fi capable device (e.g. mobile phone, tablet, laptop computers, etc.), connect to the SSID "**Edimax_xx_xx**" and enter the password. The default Wi-Fi SSID and password is printed on the Access Key Card.

If you are using a computer, please disconnect any Ethernet cables.

4. Open a web browser on the Wi-Fi capable device to reach the page below (if you do not automatically arrive at the "Get Started" page shown below, enter the URL ***http://edimax.setup*** or scan the **QR-Code** below) and click **"Get Started"** to begin the setup process.

If you cannot access the webpage, please make sure your computer is set to use a dynamic IP address. For more information please refer to *IV-2 Checking if your computer is using a dynamic IP address.*

5. Refer to ***II-4-1***, ***10*** or ***II-4-3*** depending on how you wish to setup your RE23S.

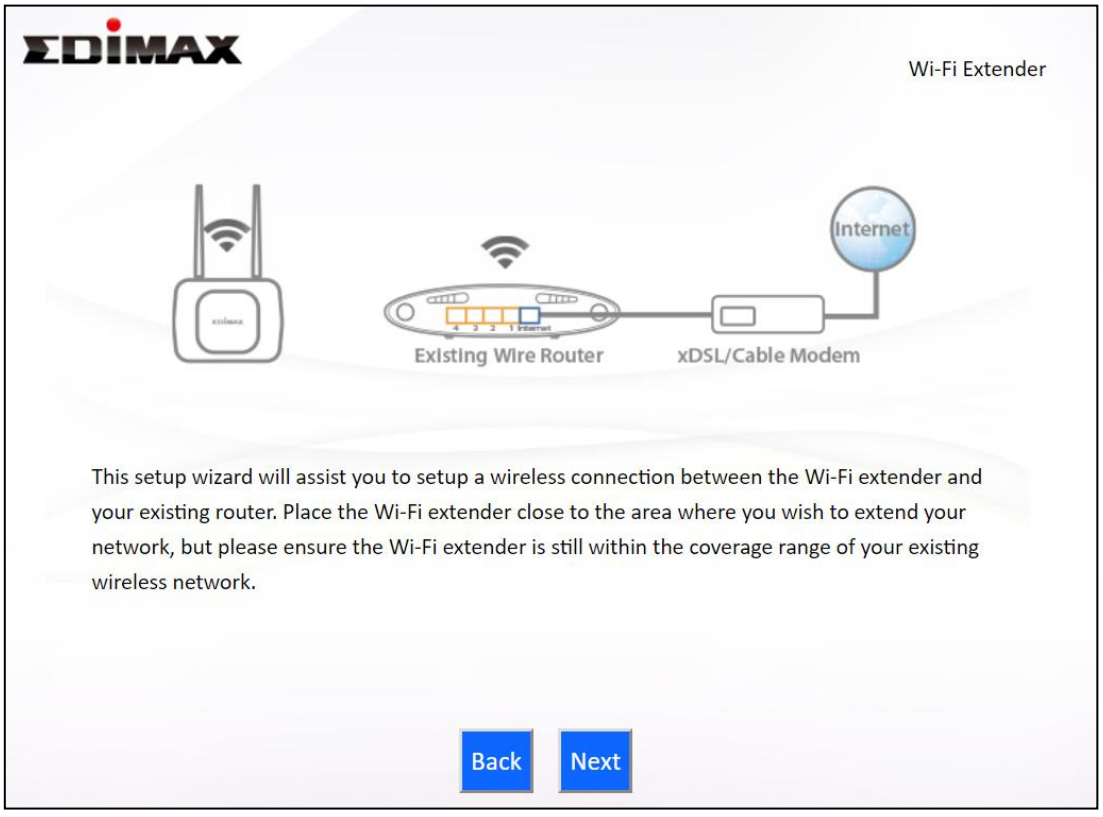


6. Select one of the options ("Change to a Different Mode" or "Yes, I need a Wi-Fi Extender") and go to the selected sections below to complete setup.

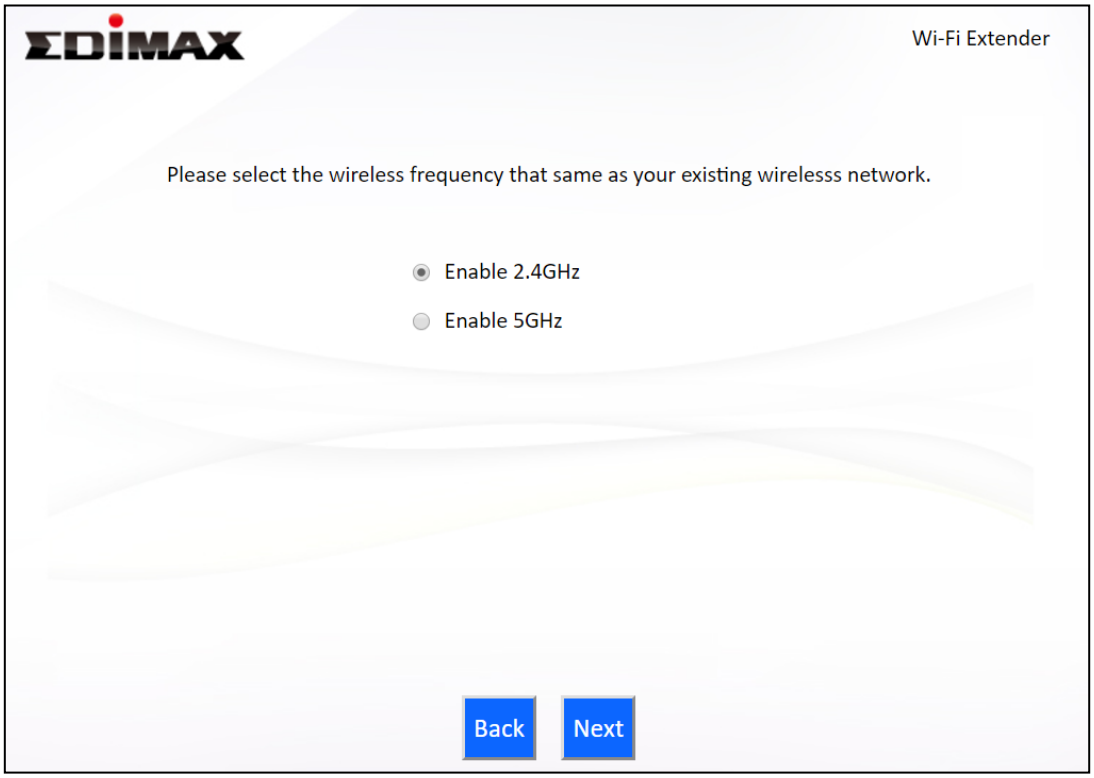
II-4-1 Wi-Fi Extender Mode

1. If you choose to set the device to extender mode, please select “Yes, I need a Wi-Fi Extender”.

2. Click “Next” to continue.
There is an on-screen demo showing how this mode is connected.

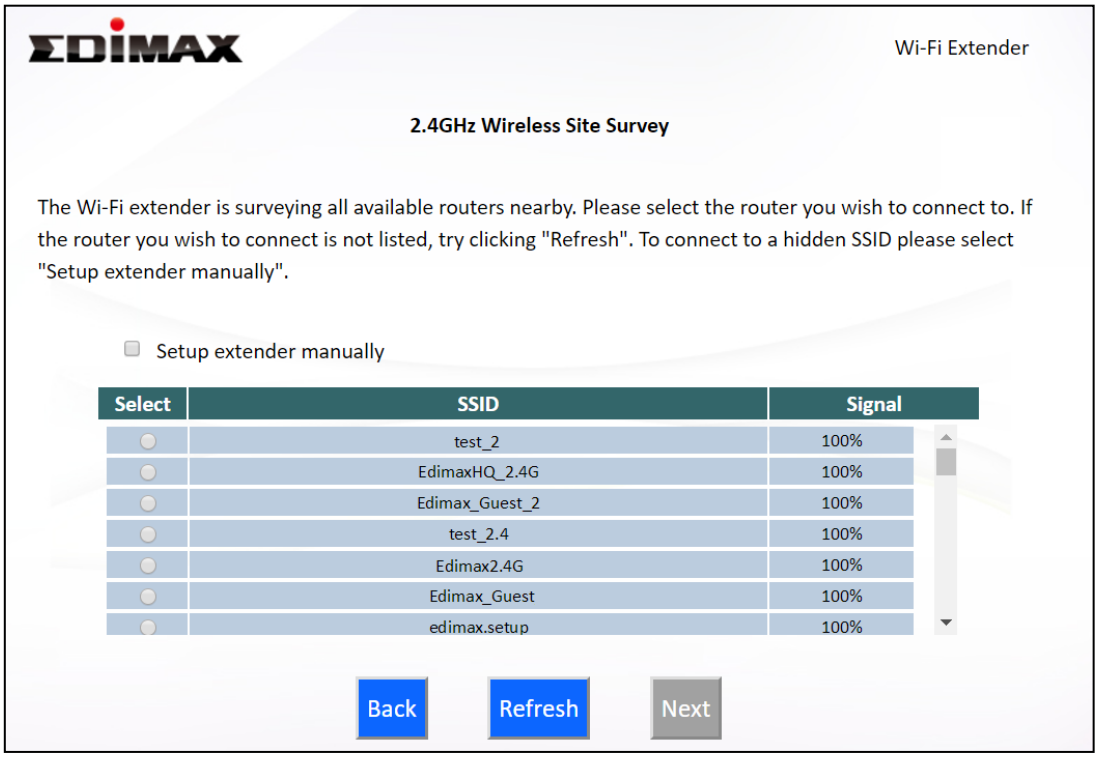


3. Select between 2.4GHz wireless frequency or 5GHz wireless frequency and click “Next”.

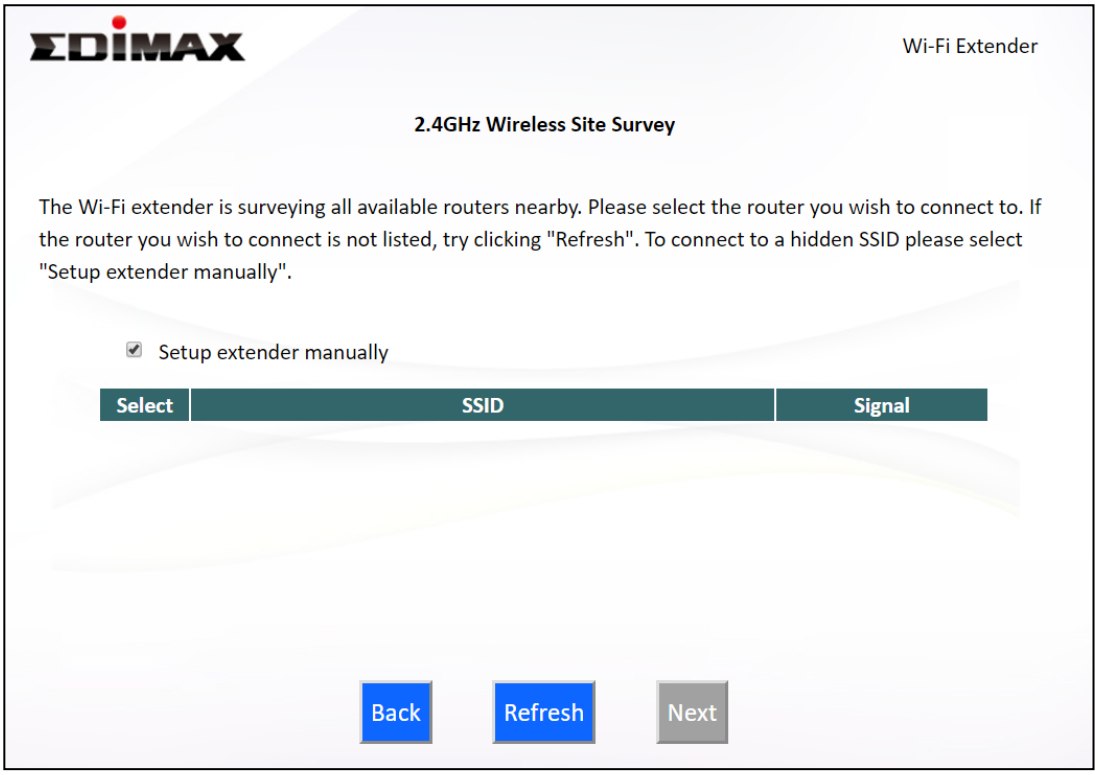


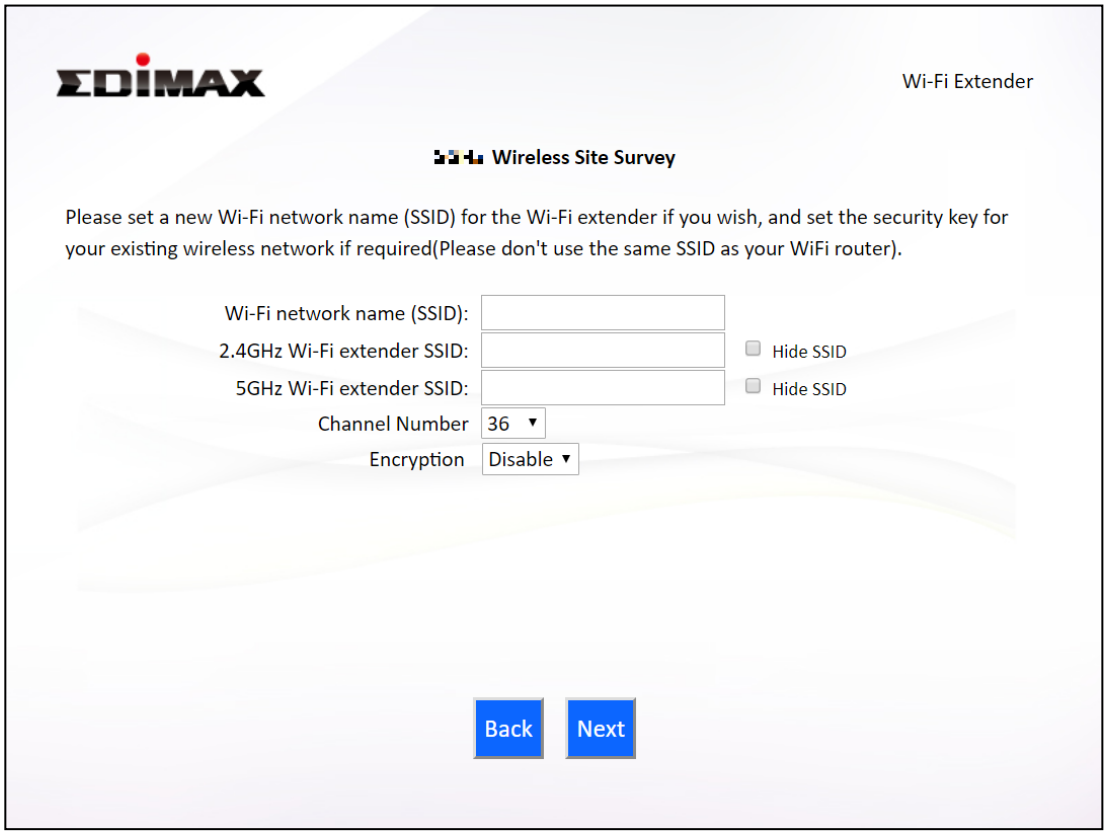
4. Select the Wi-Fi network name (SSID) which you wish to connect to and click “Next” to continue.

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

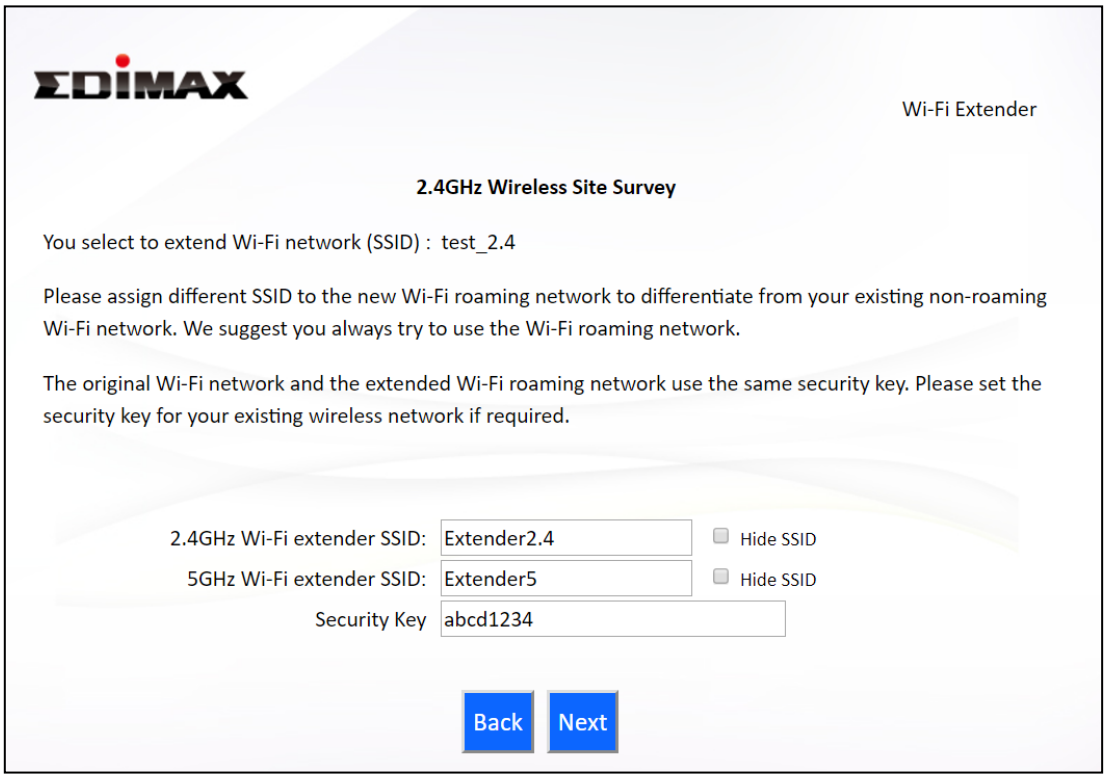


NOTE: If you wish to ***connect to a hidden SSID***, check the “Setup extender manually” box and enter the details manually on the next page, as shown below.



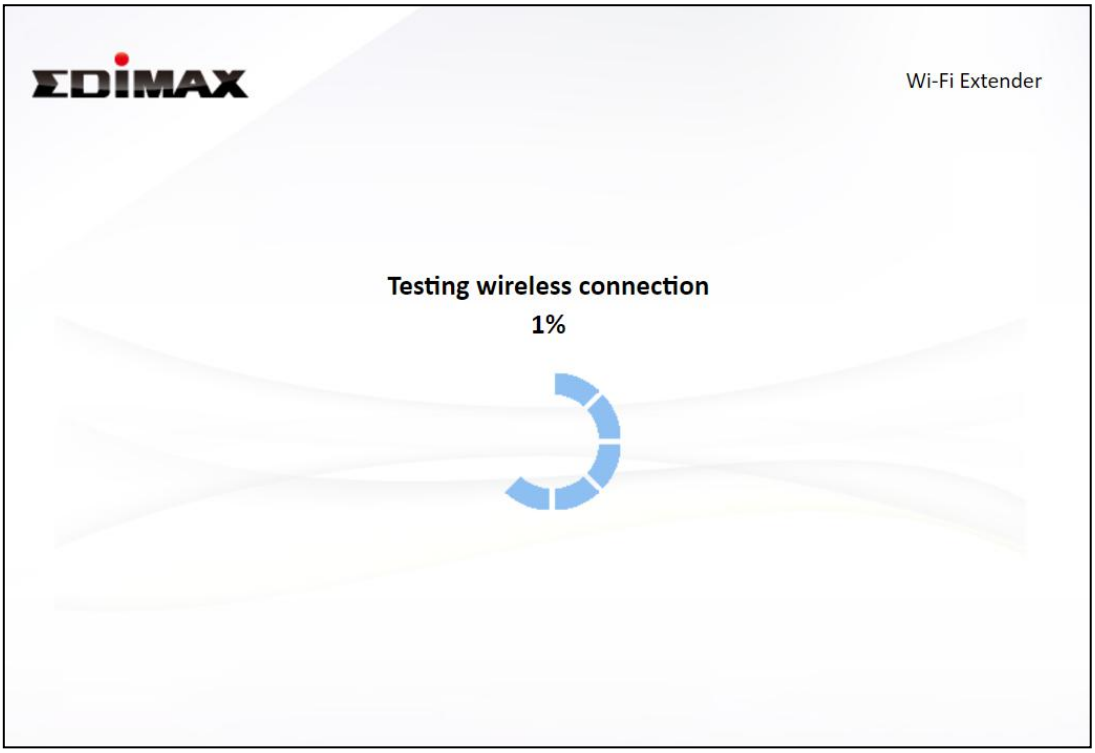


5. Enter the SSID (network name) you want to use for your extender and enter the security key of the selected wireless network (selected in **4.**) and click “Next” to continue.

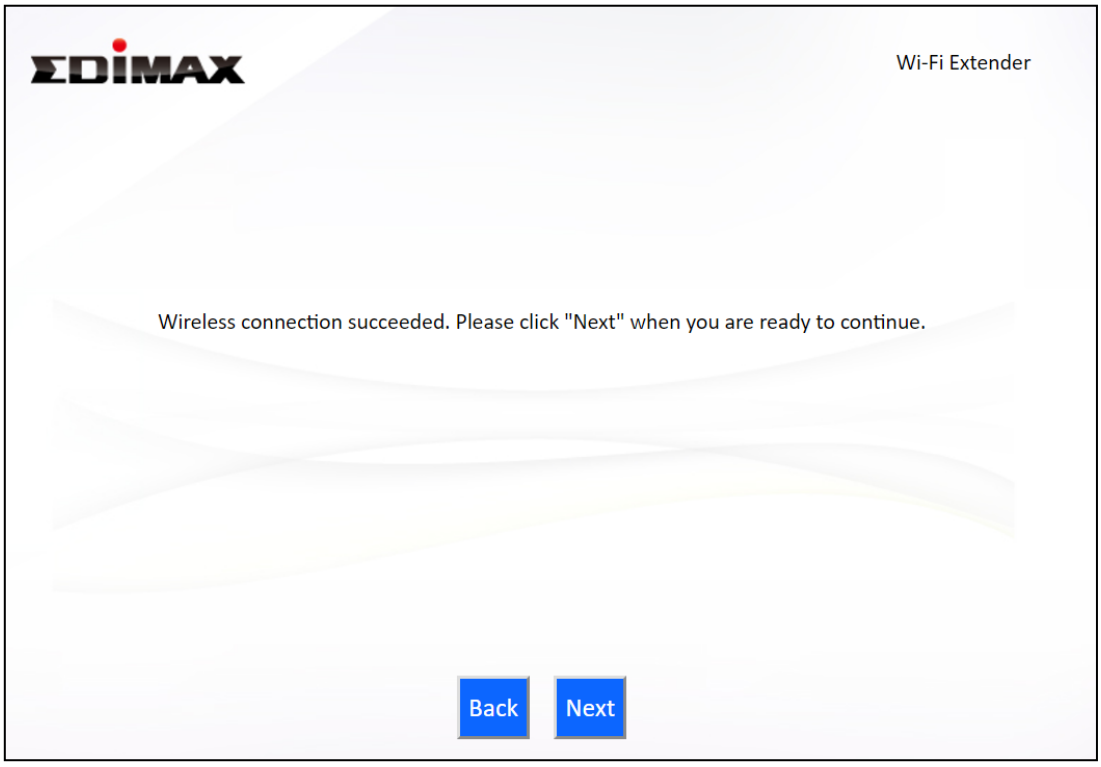


The Hide SSID boxes can be checked to make the SSID invisible in devices’ Wi-Fi settings. You can connect to hidden SSIDs with your Wi-Fi devices by manually entering the SSID name.

6. Wait a moment while the extender tests the wireless connection.

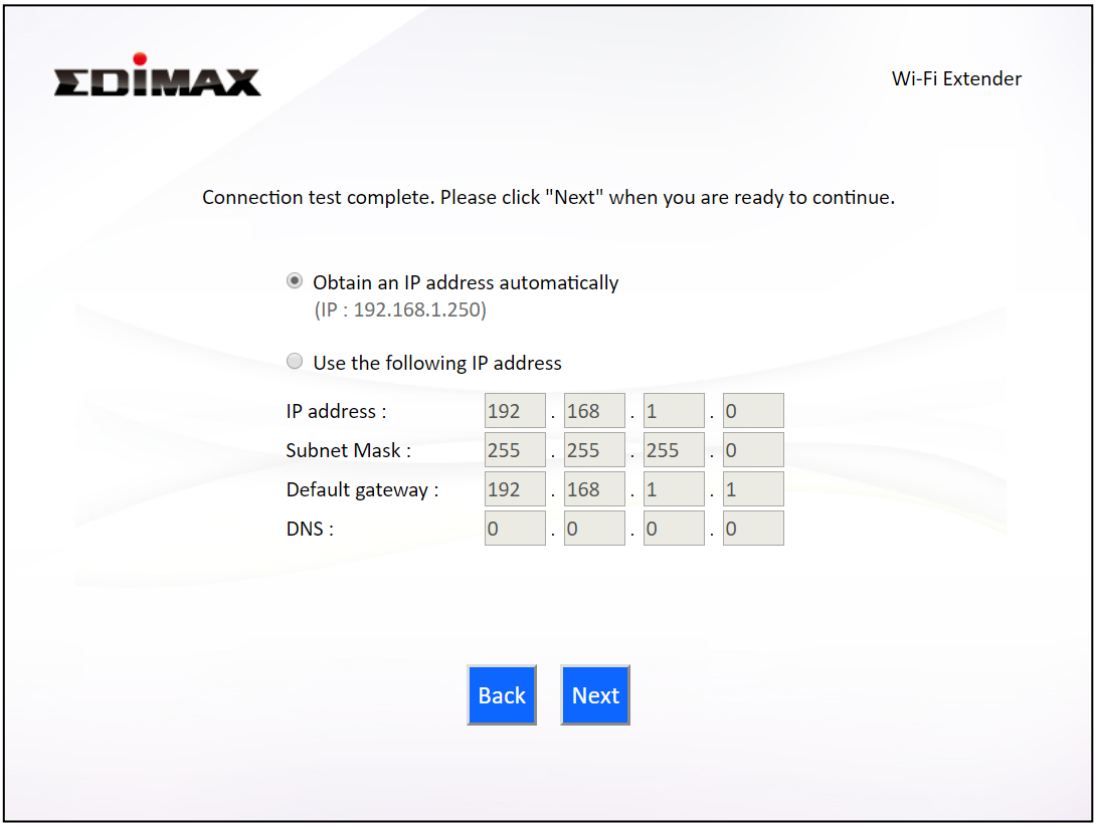


The message below is shown if wireless connection is successful. Click “Next” to continue.



7. Select “Obtain an IP address automatically” or “Use the following IP address”. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed.

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



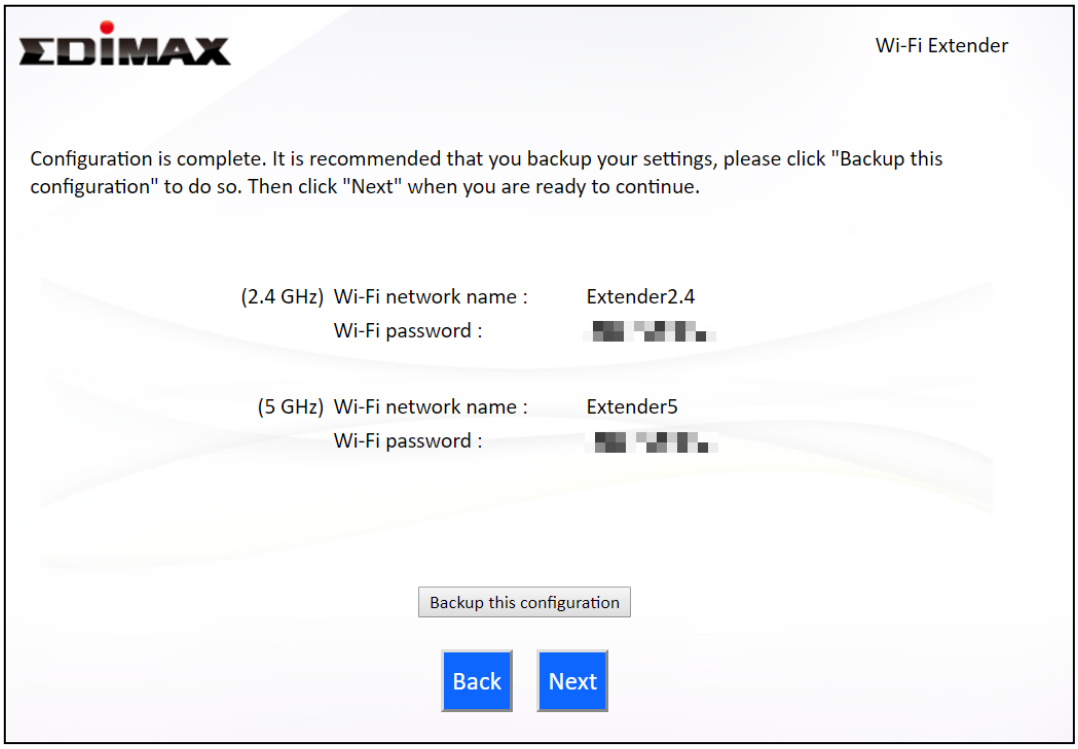
The system will start checking for updates and download where appropriate with the following indications:

If the firmware is already up-to-date, the following will be shown:

If update is required, update is automatically downloaded after the update-check.

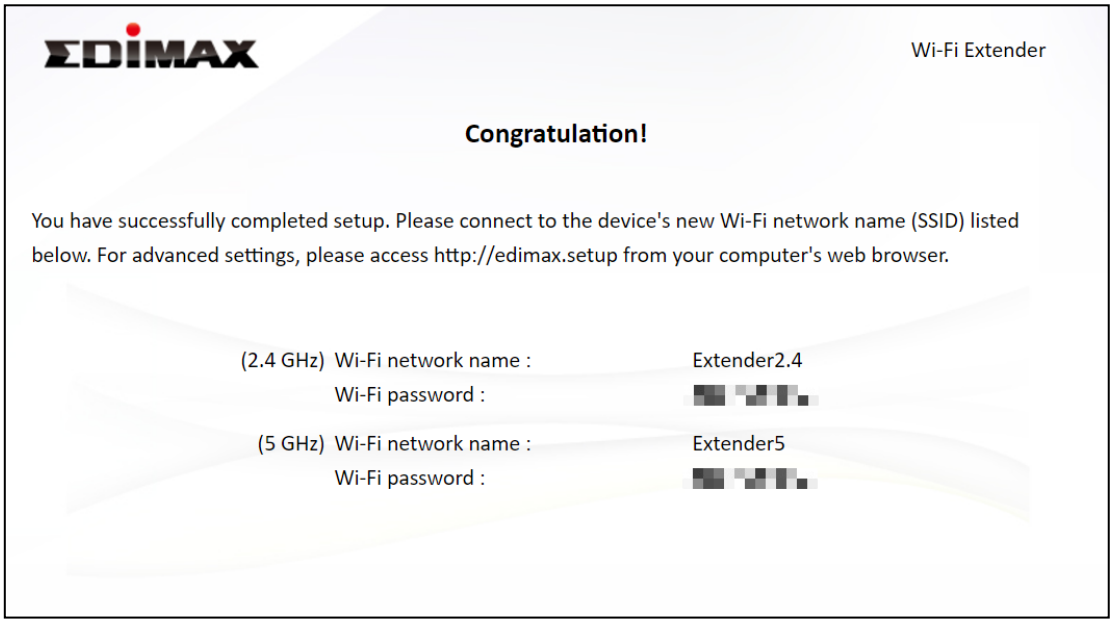
Followed by…

After the update, or if your system was already up-to-date, the following is displayed:



8. Click “Next” if you are satisfied with the configuration. Select “Backup this configuration” to backup this configuration.

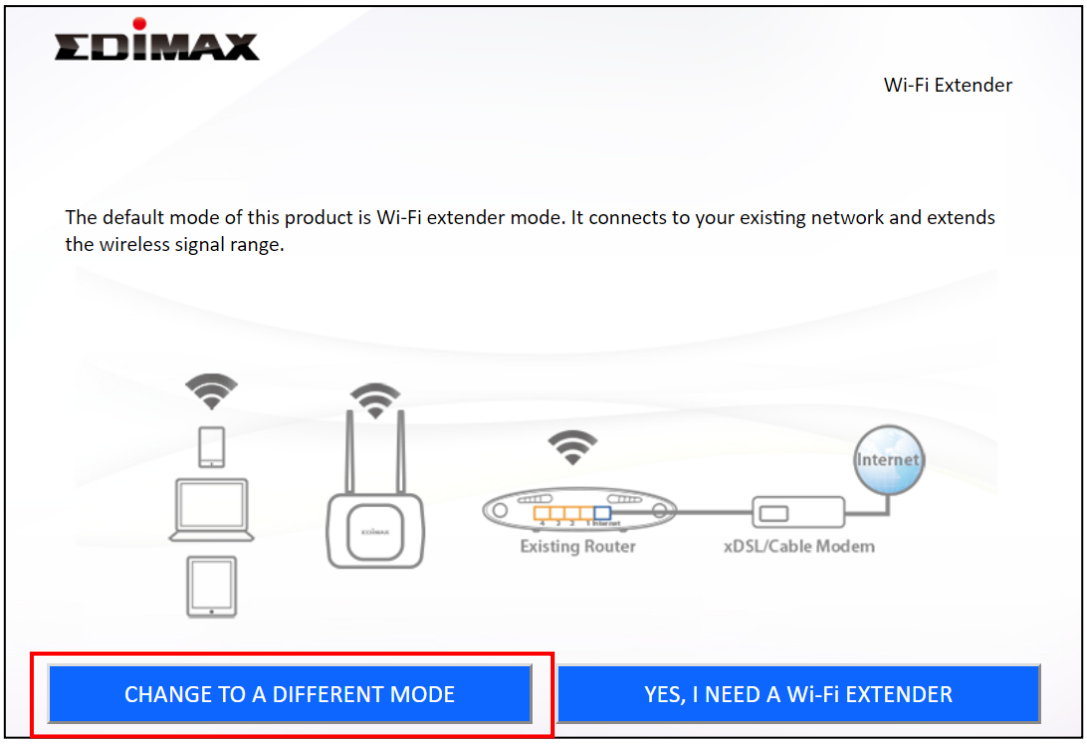
9. A final congratulations screen will indicate that setup is complete. You can now connect to the device’s new SSID(s) which are shown on the screen then close the browser window.



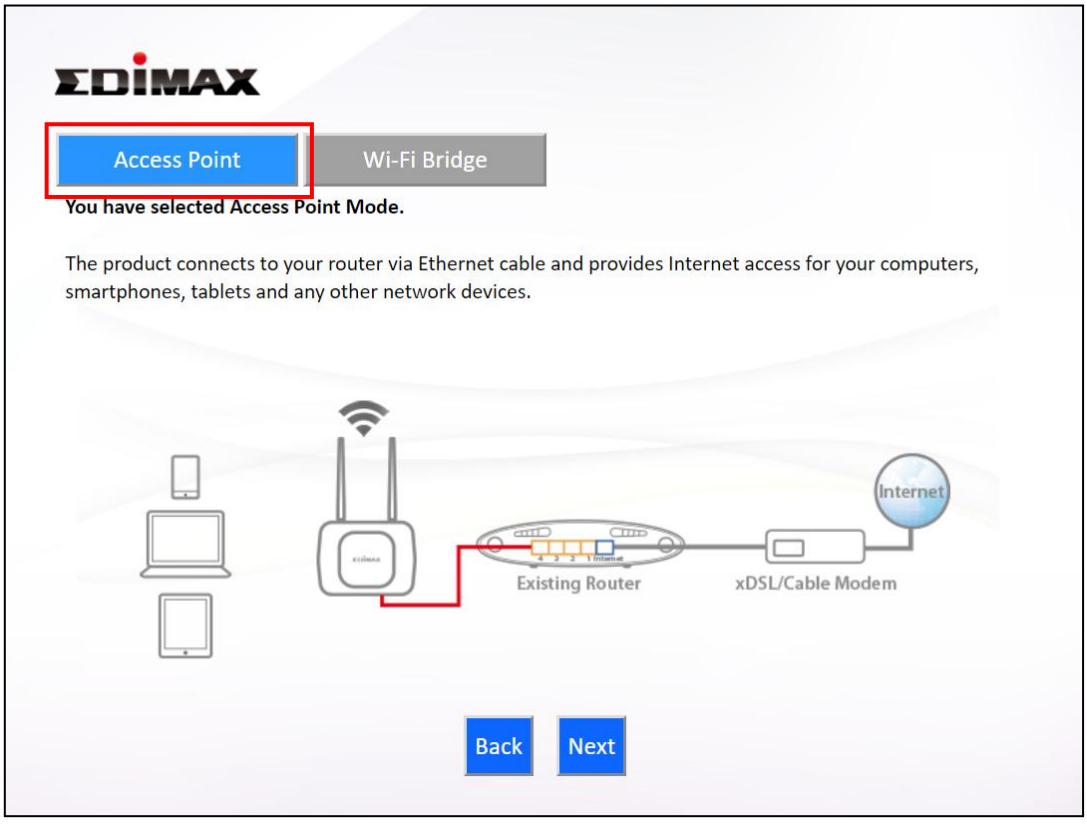
10. The extender is now working and ready for use.

II-4-2 Access Point Mode

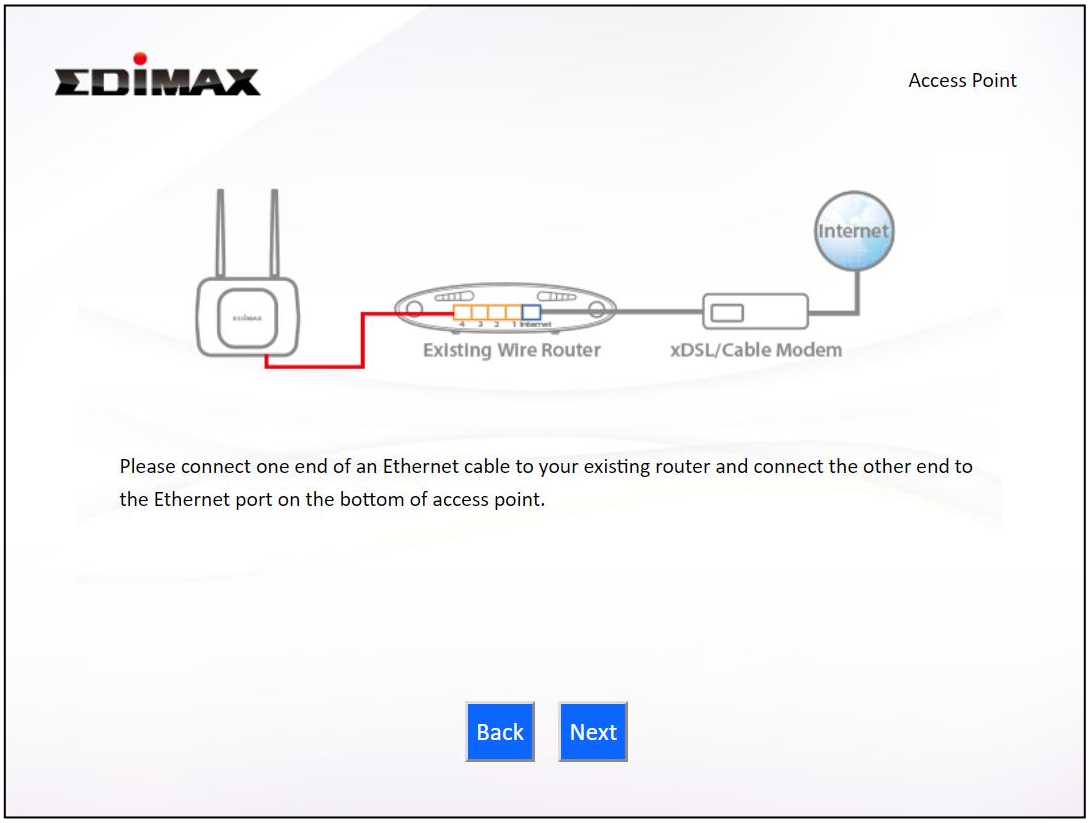
1. Choose “Change to a different mode”.



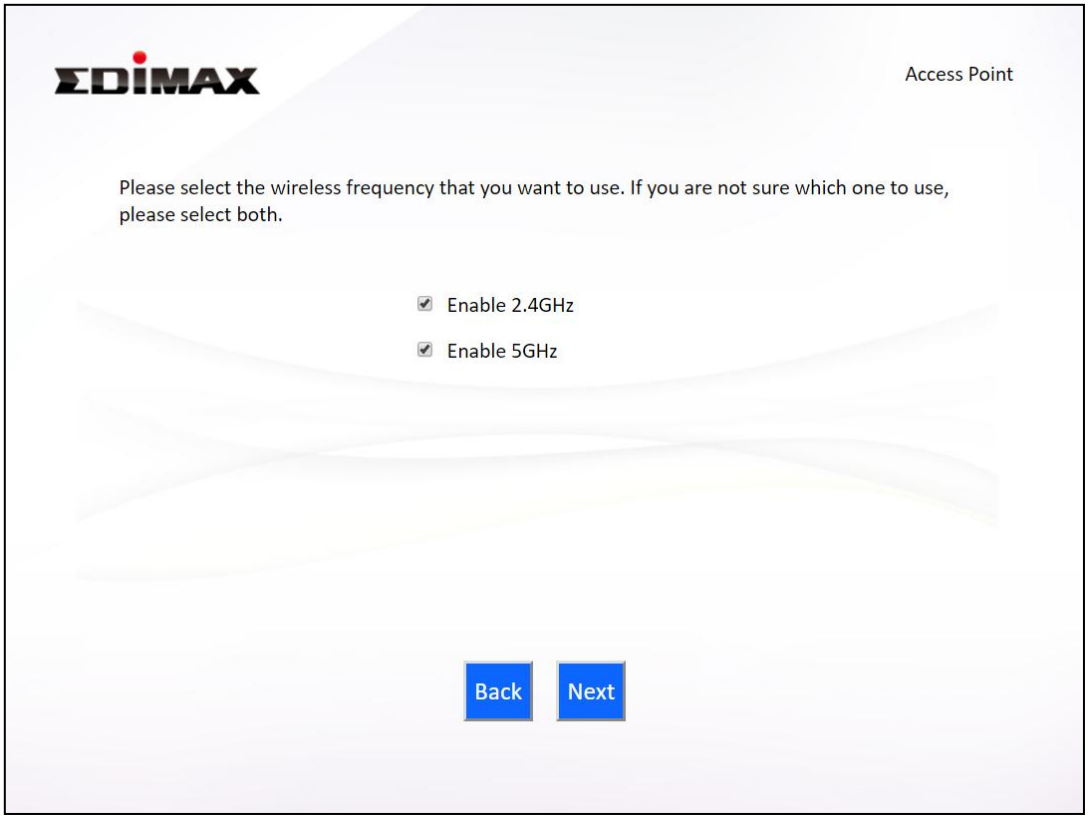
2. Select “Access Point” from the top menu and click “Next”.
There is an on-screen demo showing how this mode is connected.



3. If you have not already, connect the network port of your RE23S to the LAN port of your existing router using an Ethernet cable and click “Next”.

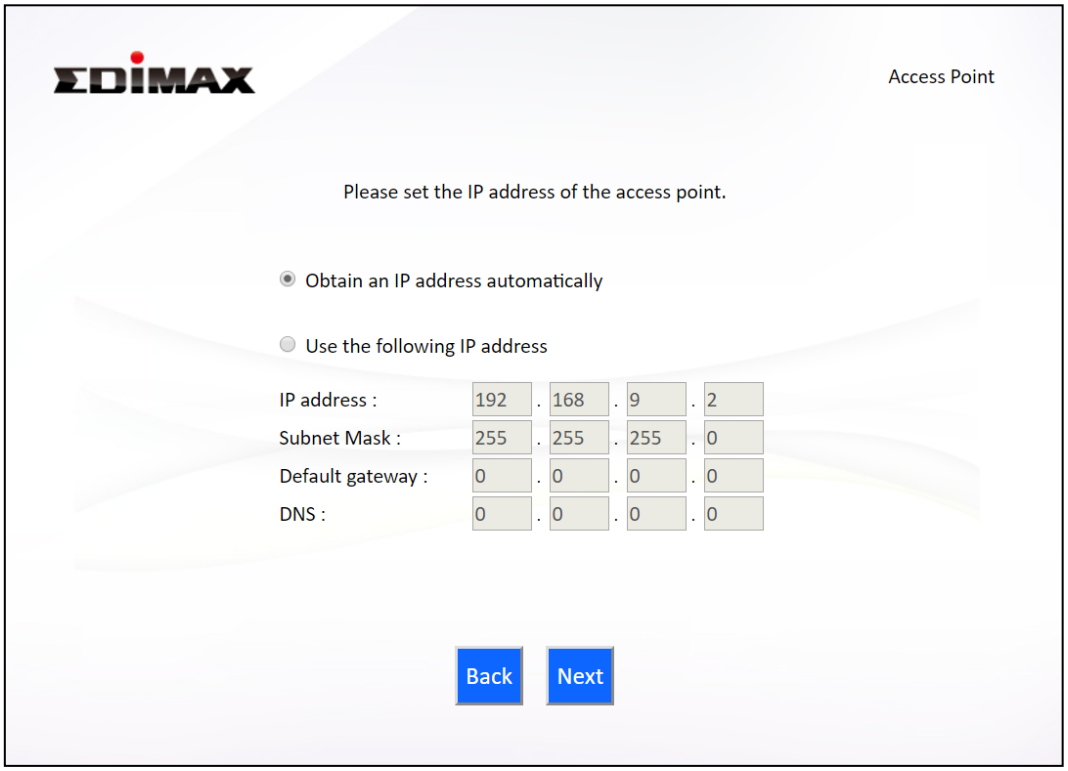


4. Select the wireless frequency you wish to use.

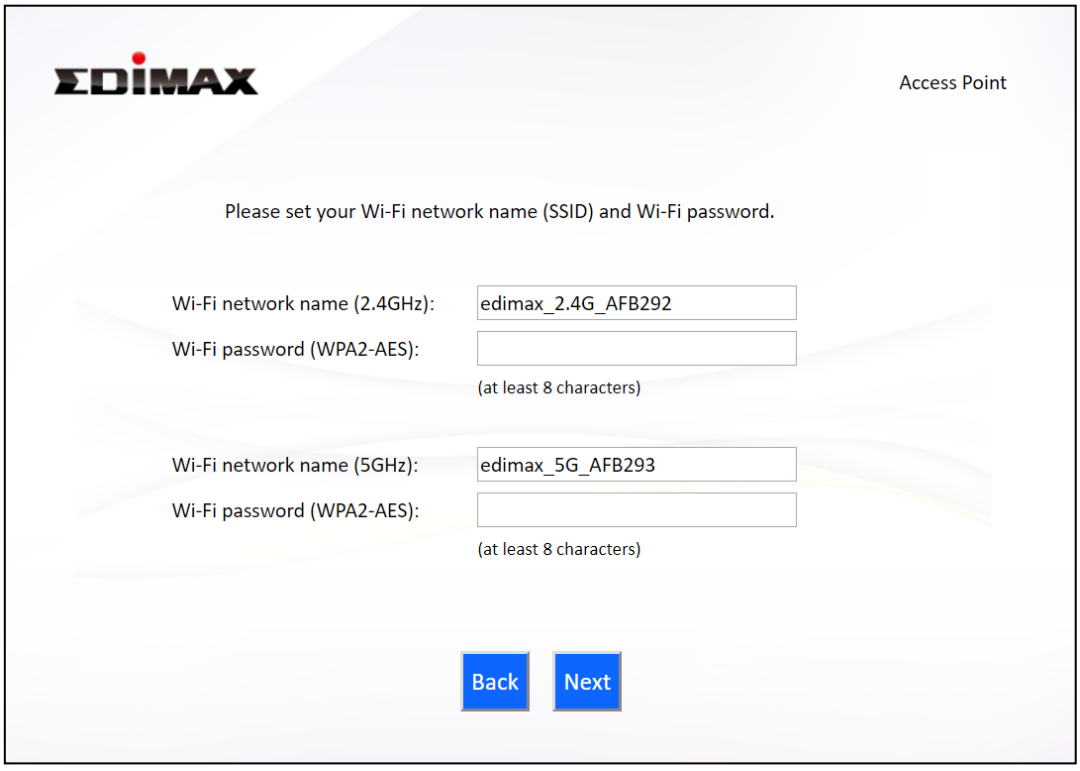


5. Select “Obtain an IP address automatically” or “Use the following IP address”. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

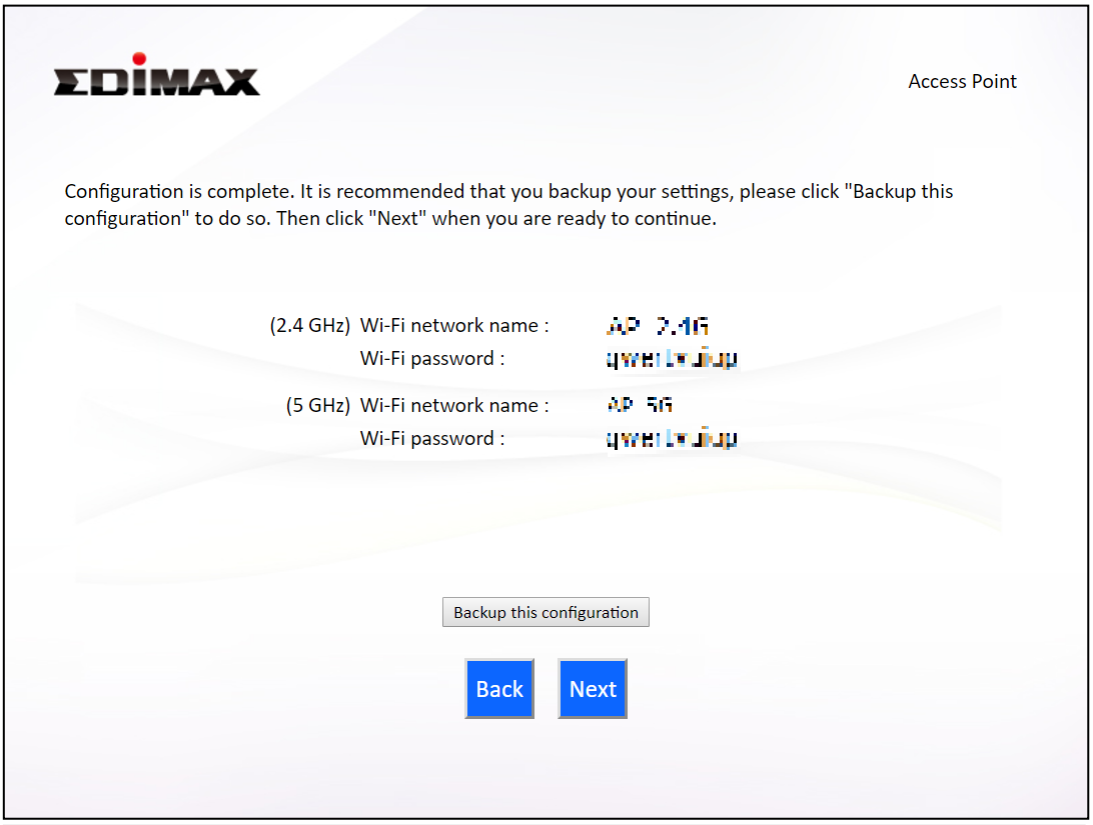
“Obtain an IP address automatically” is the recommended setting for most users.

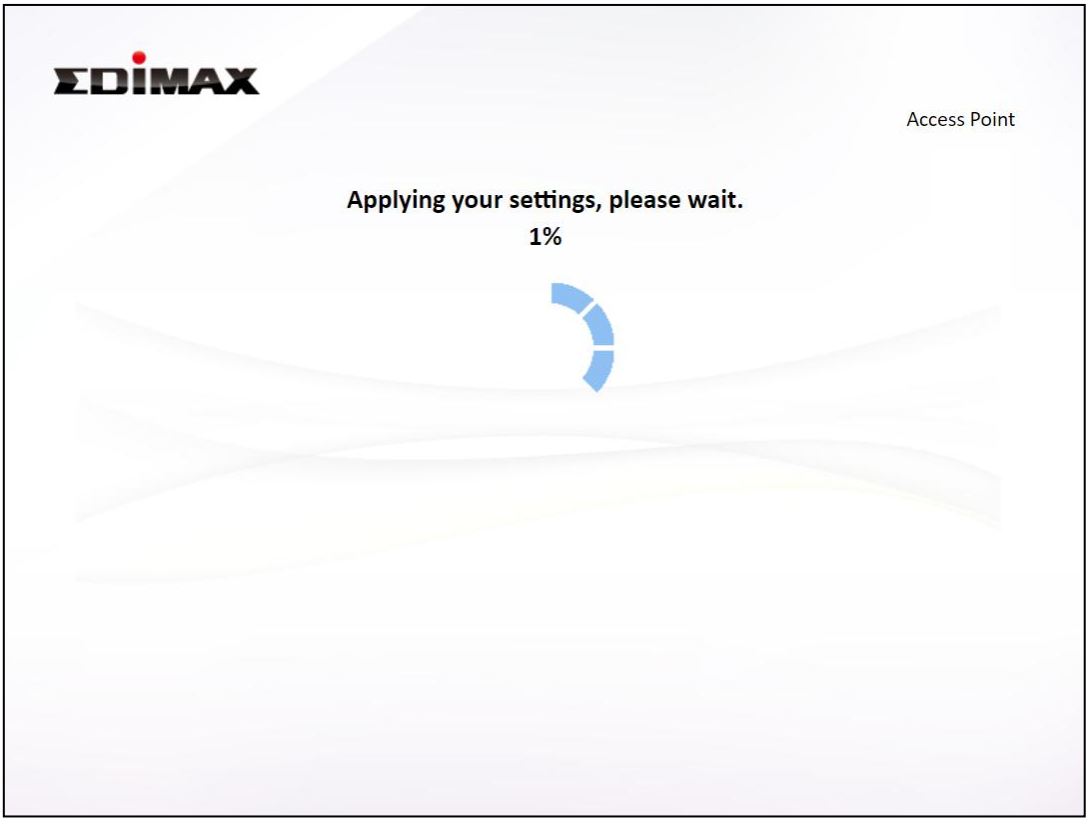


6. Enter a name and password for your 2.4GHz & 5GHz wireless networks, then click “Next” to continue.

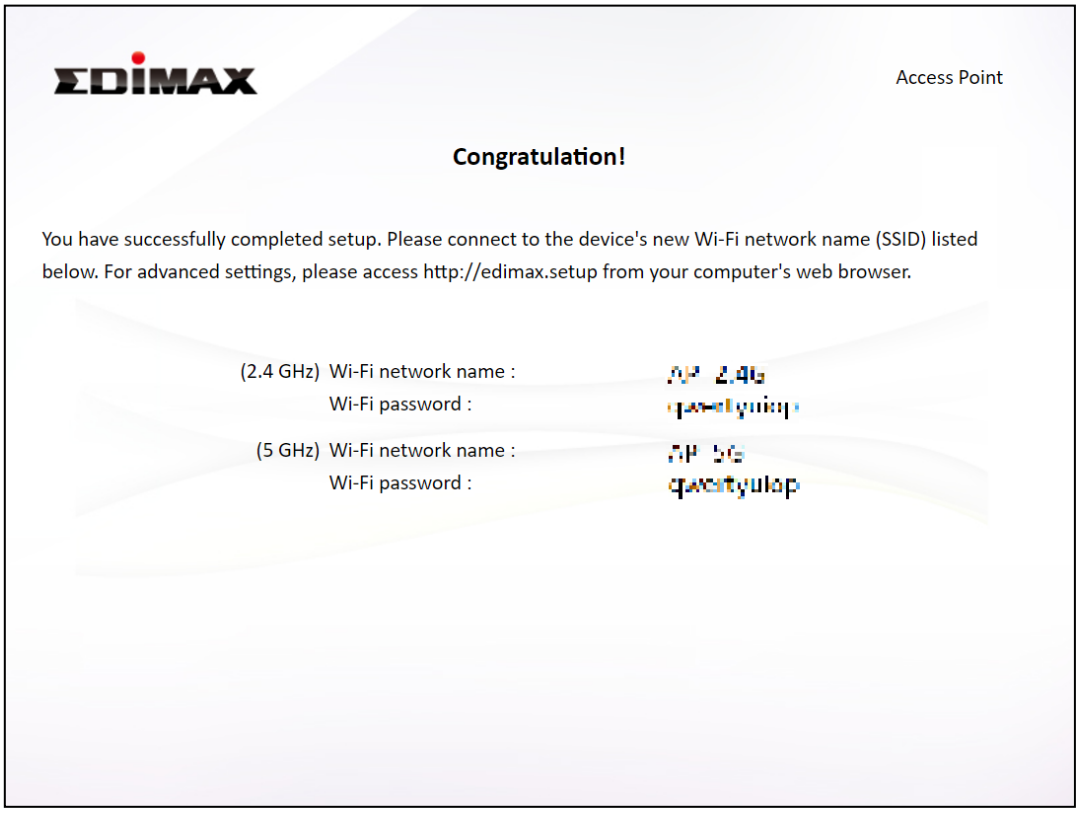


7. Click “Next” if you are satisfied with the configuration as the configurations are applied to the device. Select “Backup this configuration” to backup this configuration.



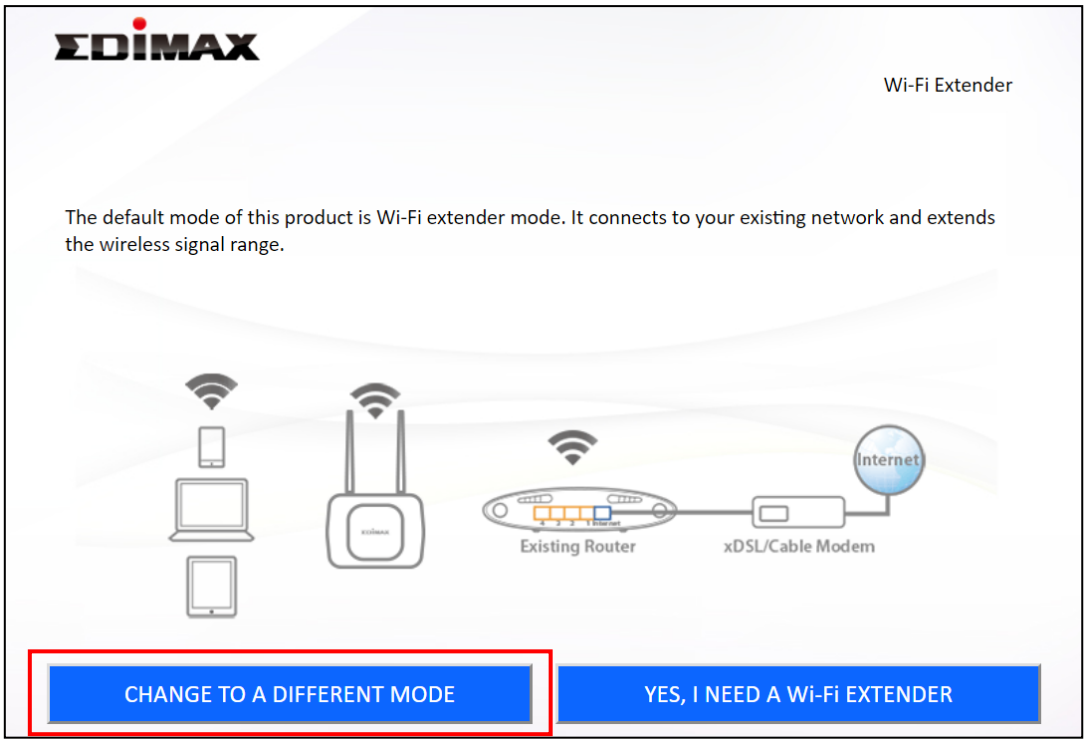


8. A final congratulations screen will indicate that setup is complete. You can now connect to the device's new SSID(s) shown below for the network connection.

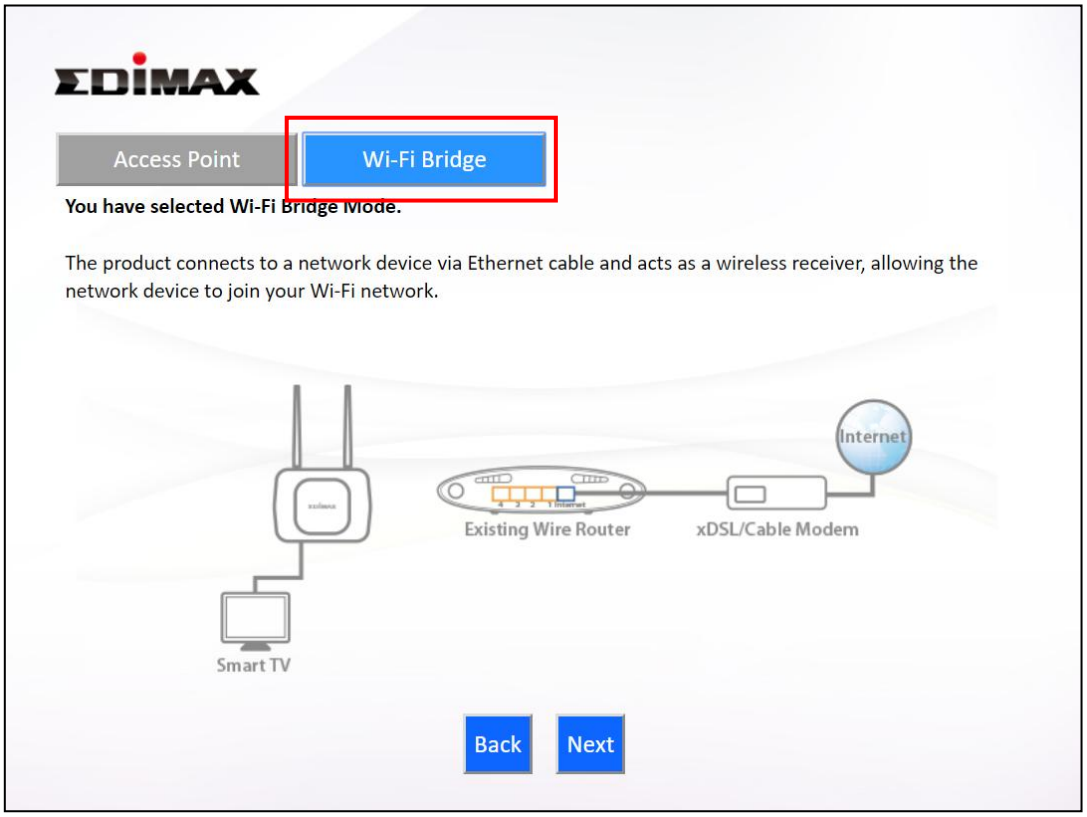


II-4-3 Wi-Fi Bridge Mode

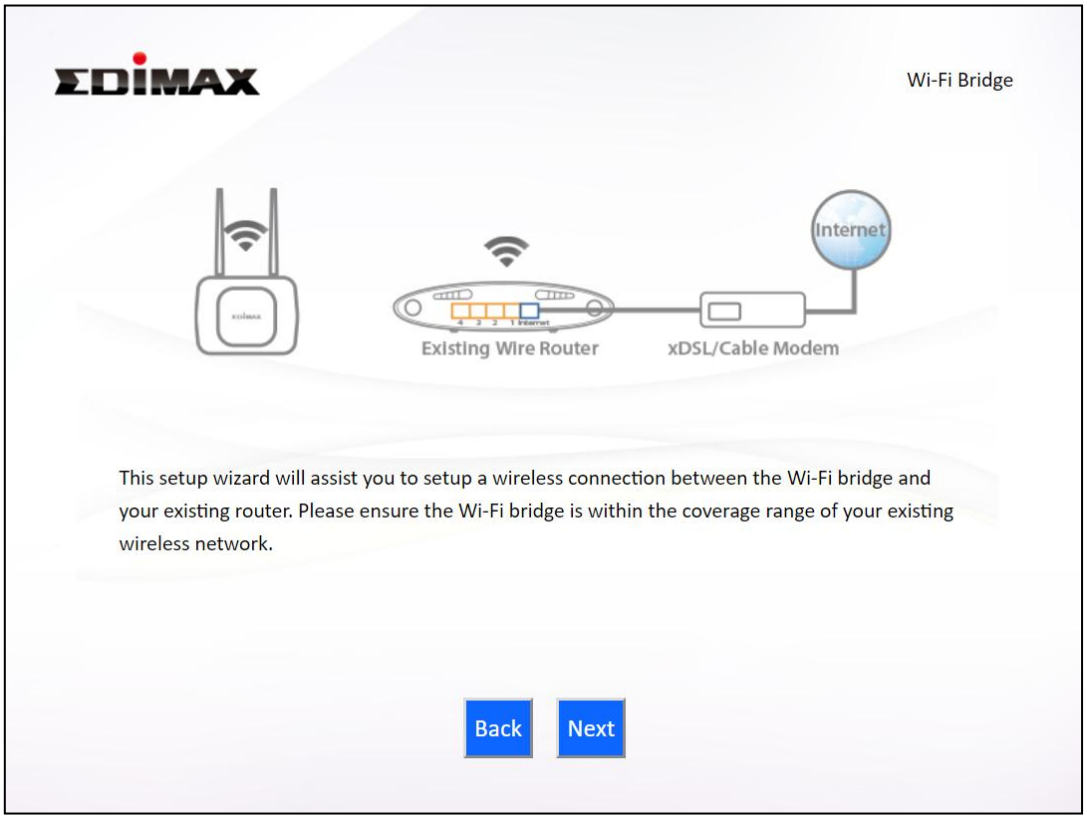
1. Choose “Change to a different mode”.



2. Select “Wireless Bridge” from the top menu and click “Next”. There is an on-screen demo showing how this mode is connected.

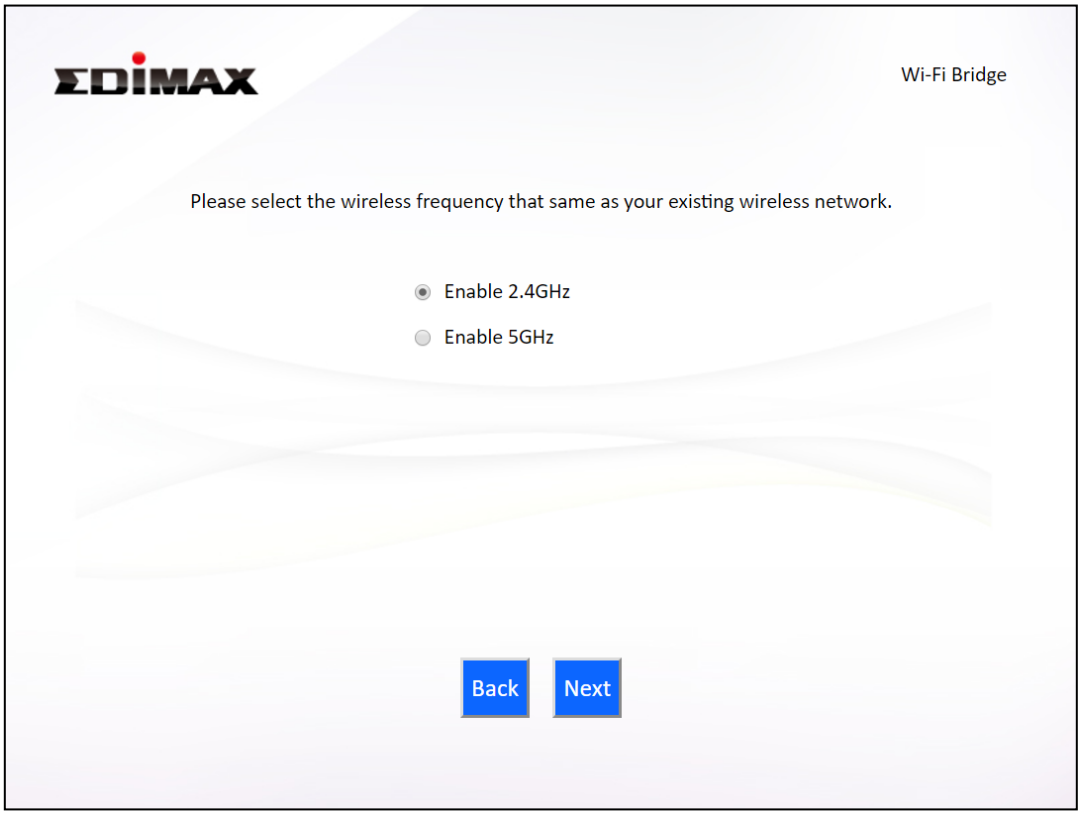


3. Please make sure the device is within Wi-Fi range of existing wireless router. Click “Next” to continue.



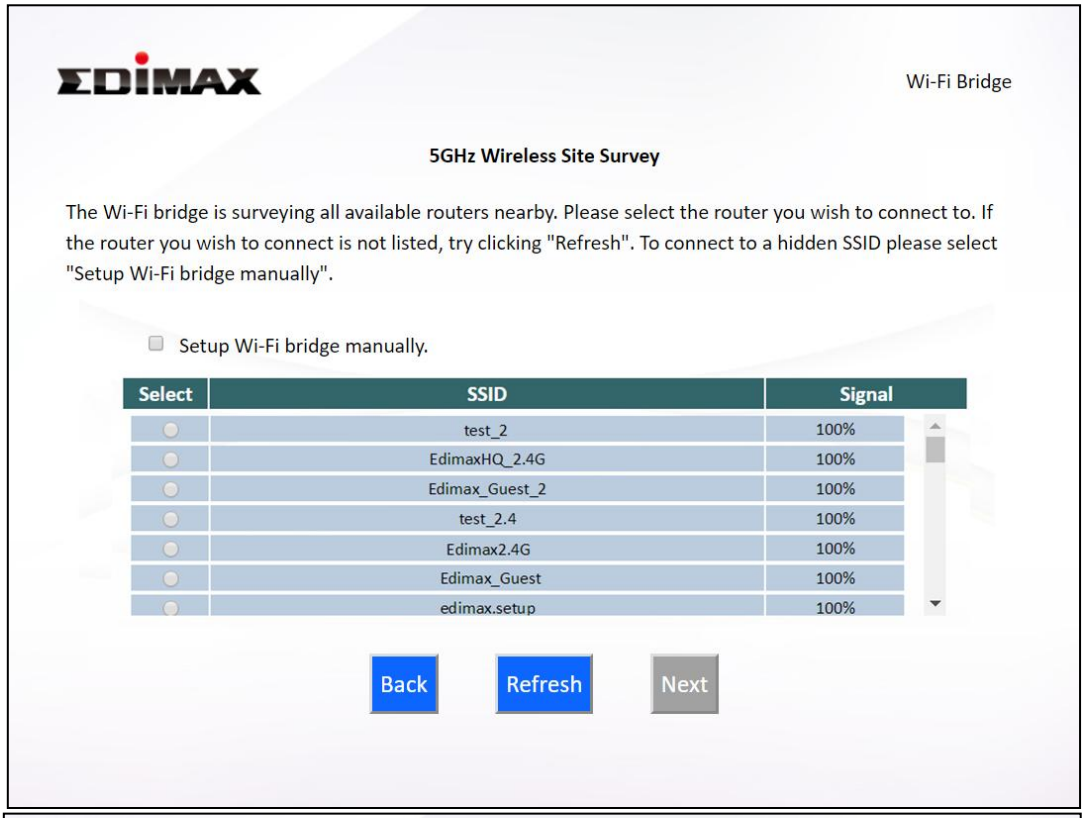
4. Select the frequency (2.4GHz or 5GHz) of your existing wireless network.

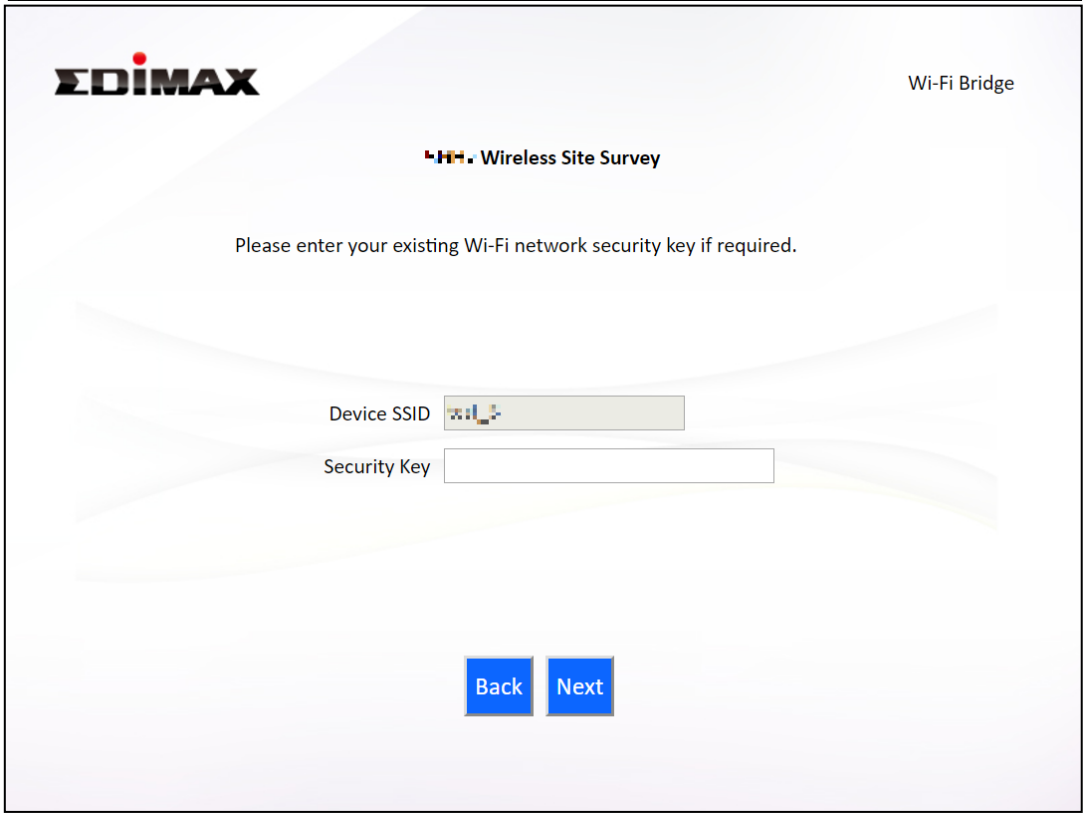
In wireless bridge mode, the RE23S can only connect to one wireless network / frequency (2.4GHz or 5GHz).



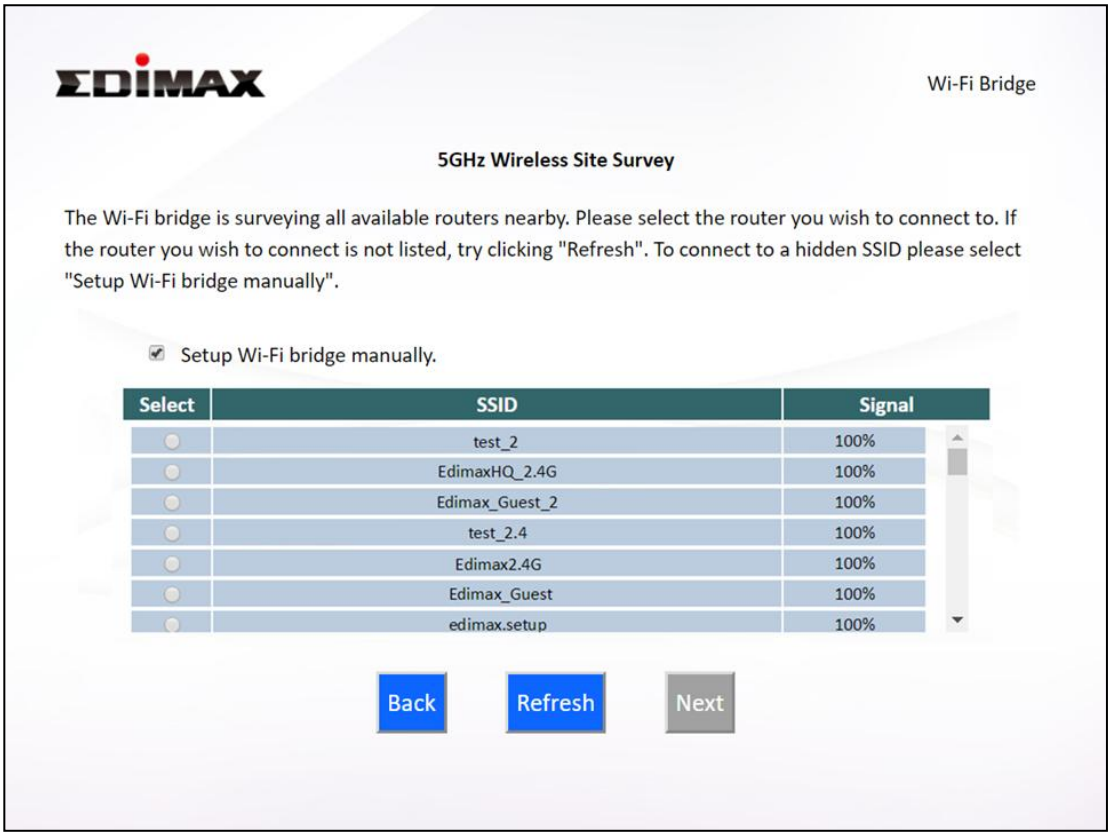
5. Select the Wi-Fi network name (SSID) which you wish to connect to and you will be directed to the next page to enter the security key of the network.

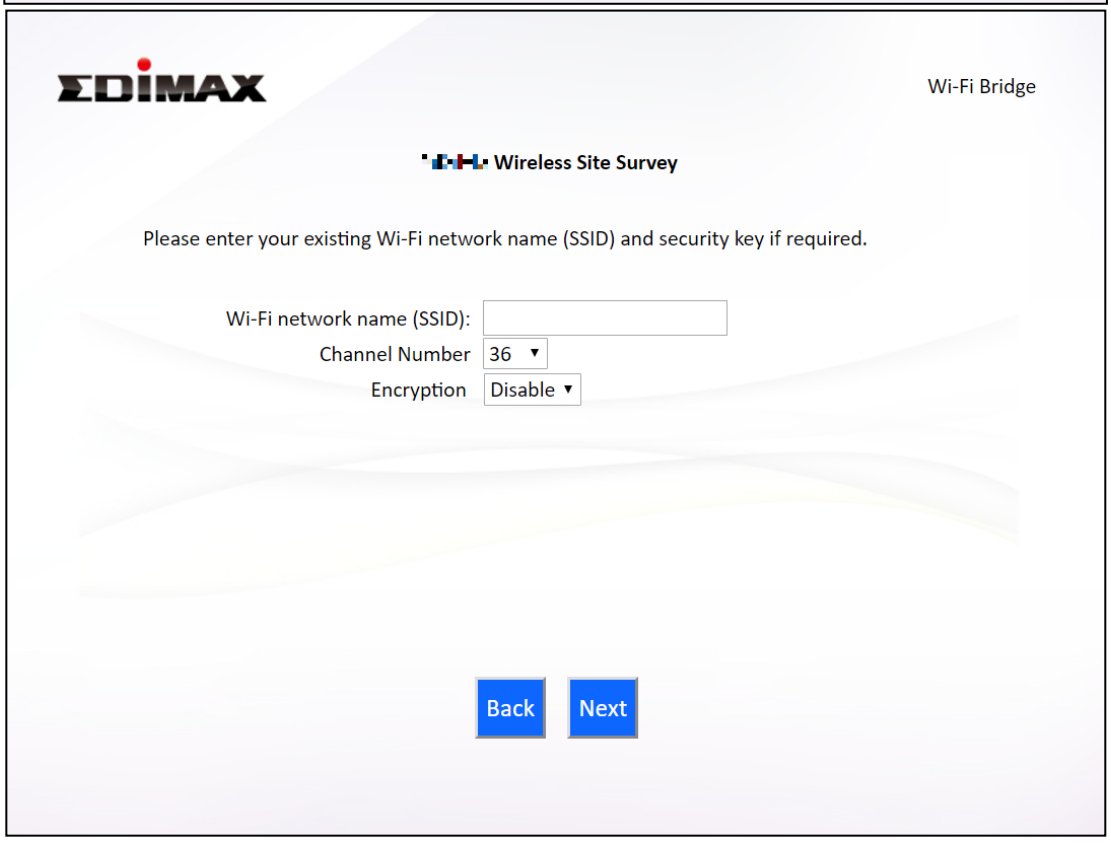
If the Wi-Fi network you wish to connect to does not appear, try clicking "Refresh".



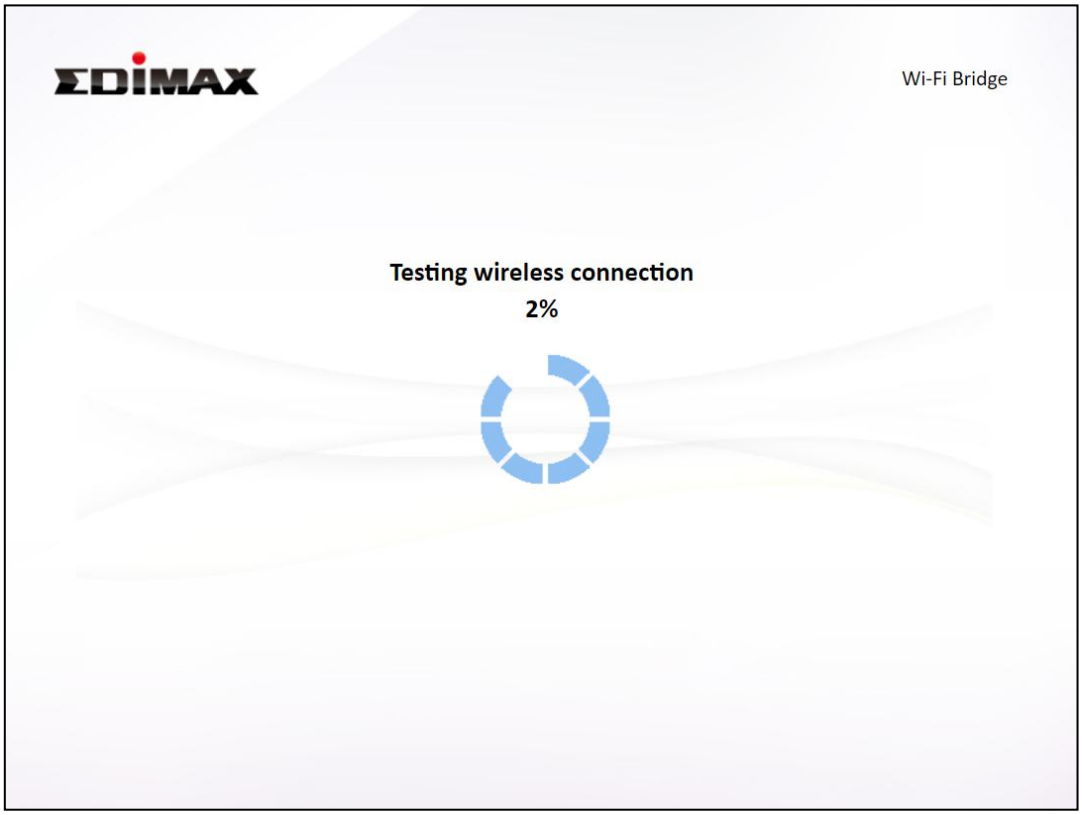


NOTE: If you wish to ***connect to a hidden SSID***, check the "Setup Wi-Fi bridge manually" box and enter the details manually on the next page, as shown below.

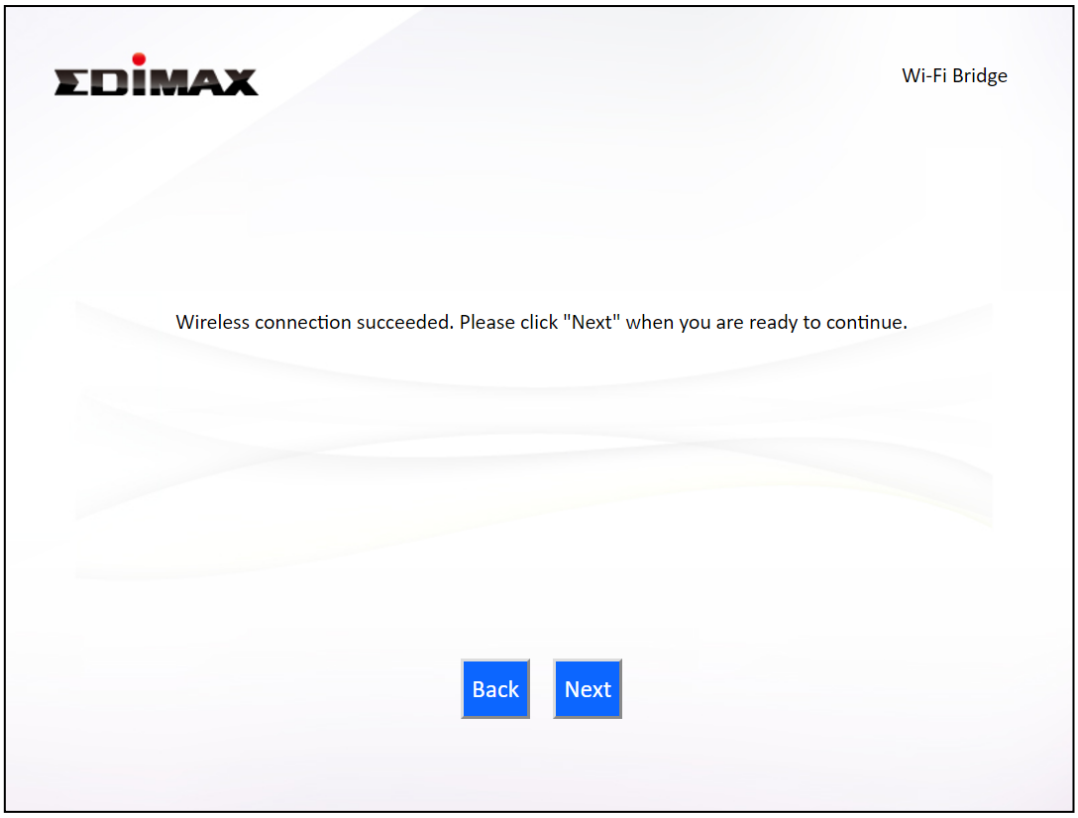




6. Wait a moment while the device tests the wireless connection.

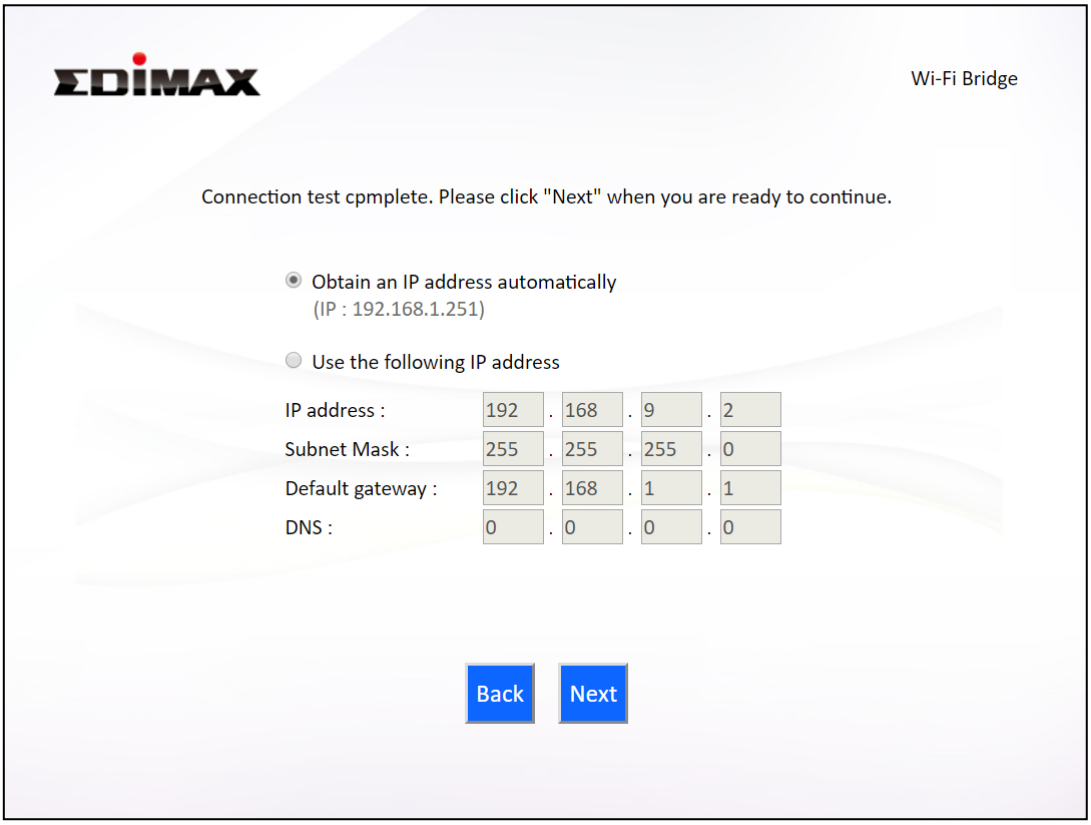


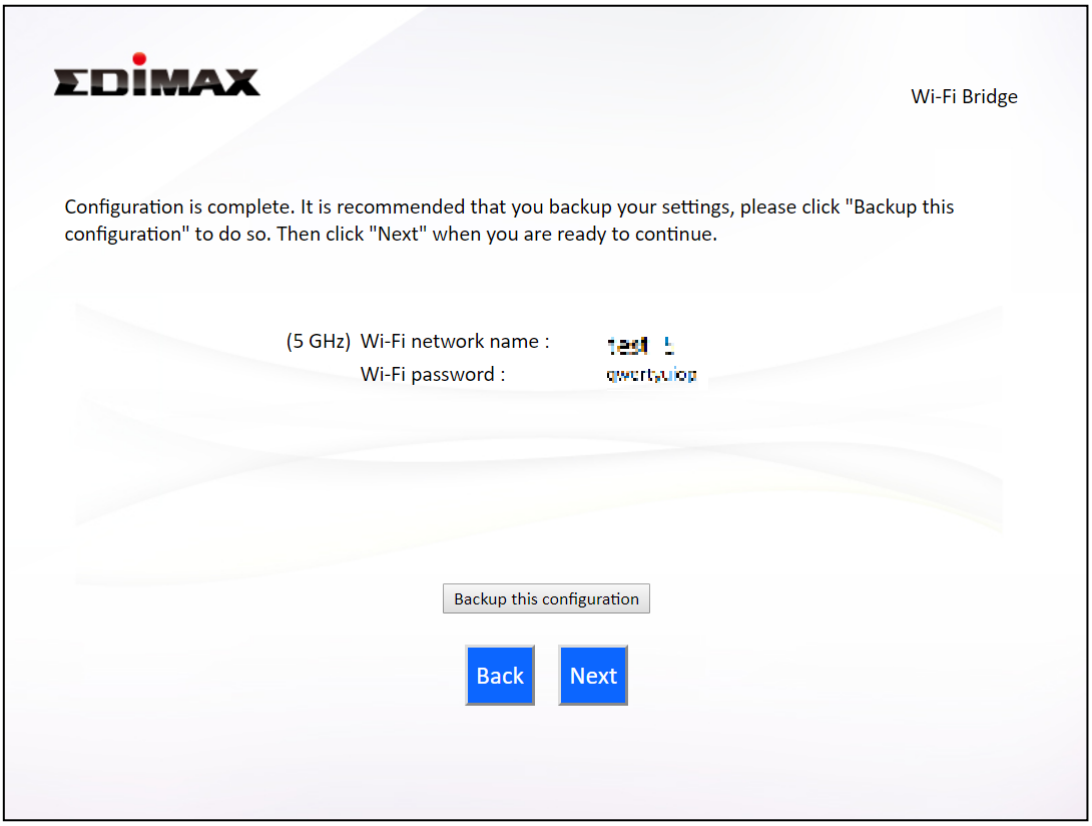
The message below is shown if wireless connection is successful. Click "Next" to continue.



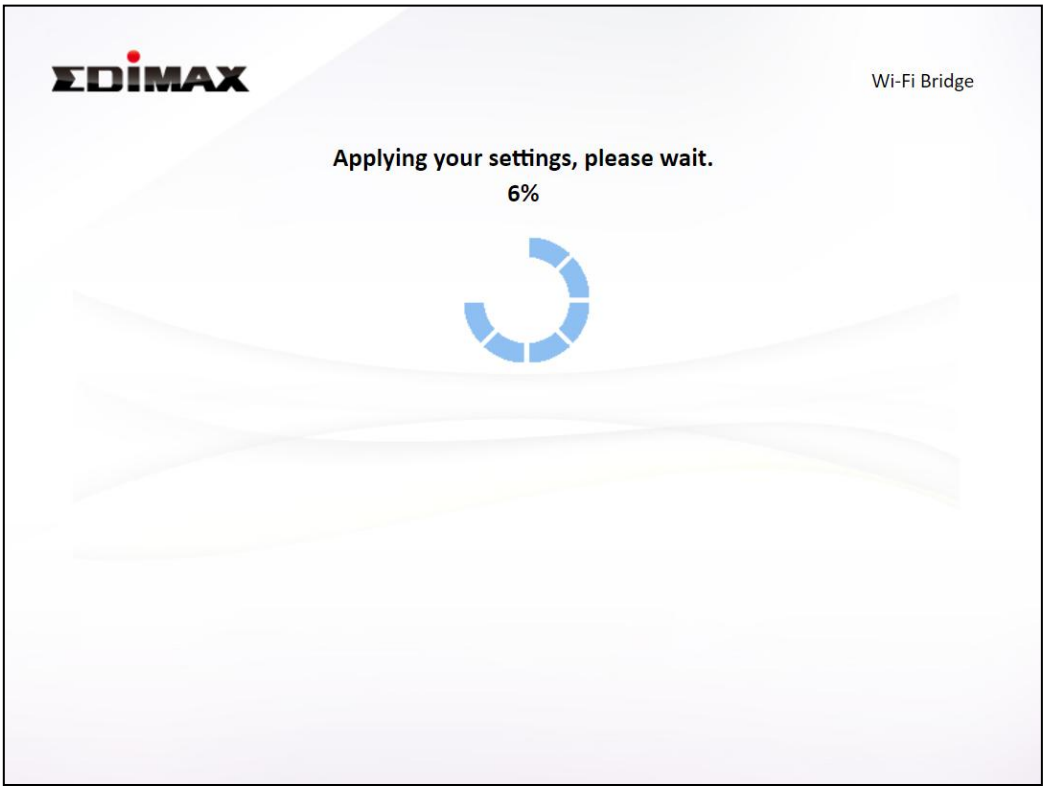
7. Select “Obtain an IP address automatically” or “Use the following IP address”. If you are using a static IP, enter the IP address, subnet mask and default gateway. Click “Next” to proceed to the next step.

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

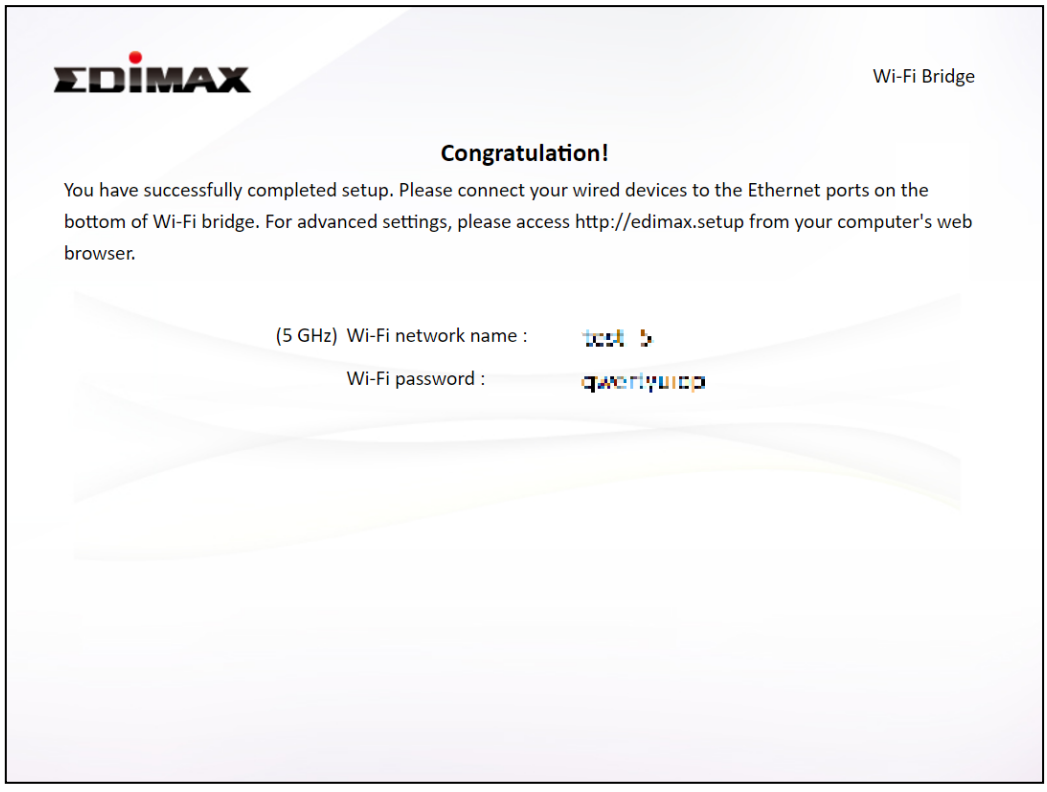




8. Click “Next” if you are satisfied with the configuration to apply the configuration to your device.
Select “Backup this configuration” to backup this configuration.



9. A final congratulations screen will indicate that setup is complete. You can now connect Ethernet cable between your Wi-Fi bridge and Ethernet-capable device for the network connection.



III Browser Based Configuration Interface

After setting up the device as detailed in ***II Installation*** or the included **Quick Installation Guide**, you can use the browser based configuration interface to configure advanced settings.

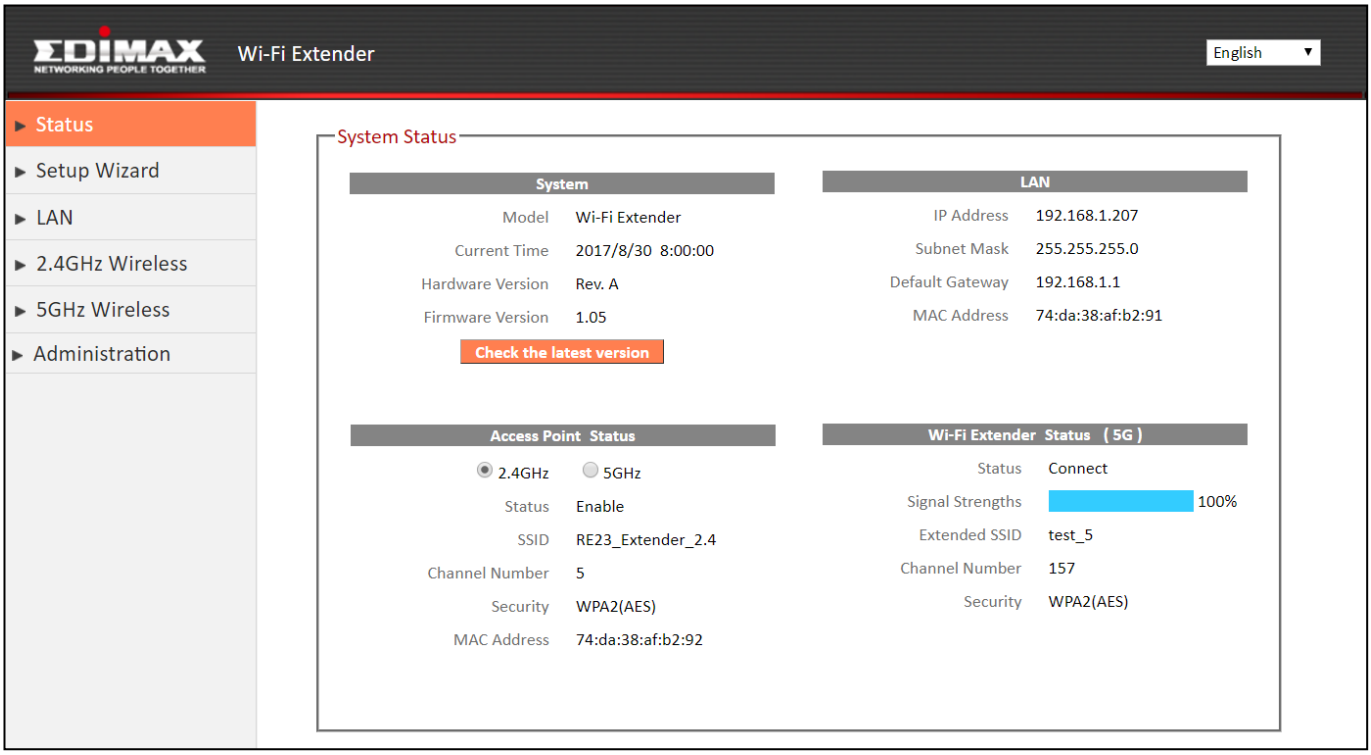
> ***Please ensure that your computer is set to use a dynamic IP address. Refer to*** *IV-2 Checking if your computer is using a dynamic IP address* ***for more information.***

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 RE23S.

2. The browser will prompt you for a username and password. The default username is “admin” and the default password is “1234”.

3. “Status and Information” screen will be shown by default. Use the menu on the left to navigate.



III-2 Save Settings

When settings are configured, click the “Save Settings” button on the configuration page to save the changes.

A message is shown below:

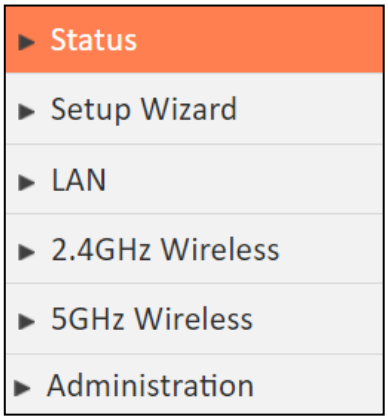
The device needs to restart in order to bring any changes into effect, click “Click here to restart” to do so.

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

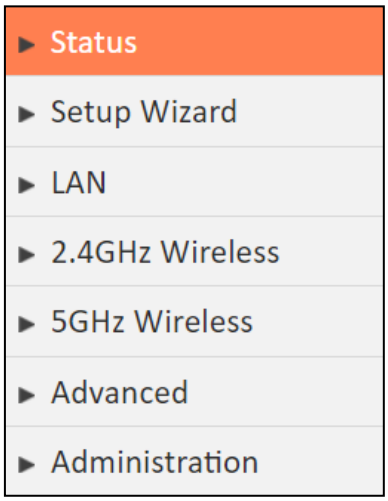
III-3 Main Menu

The main menu on the left panel will display differently according to the operation mode of the device.

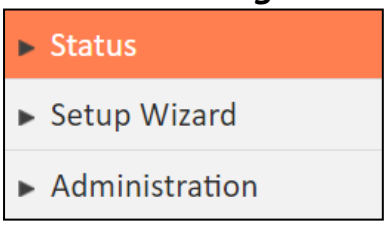
Wi-Fi Extender



Access Point



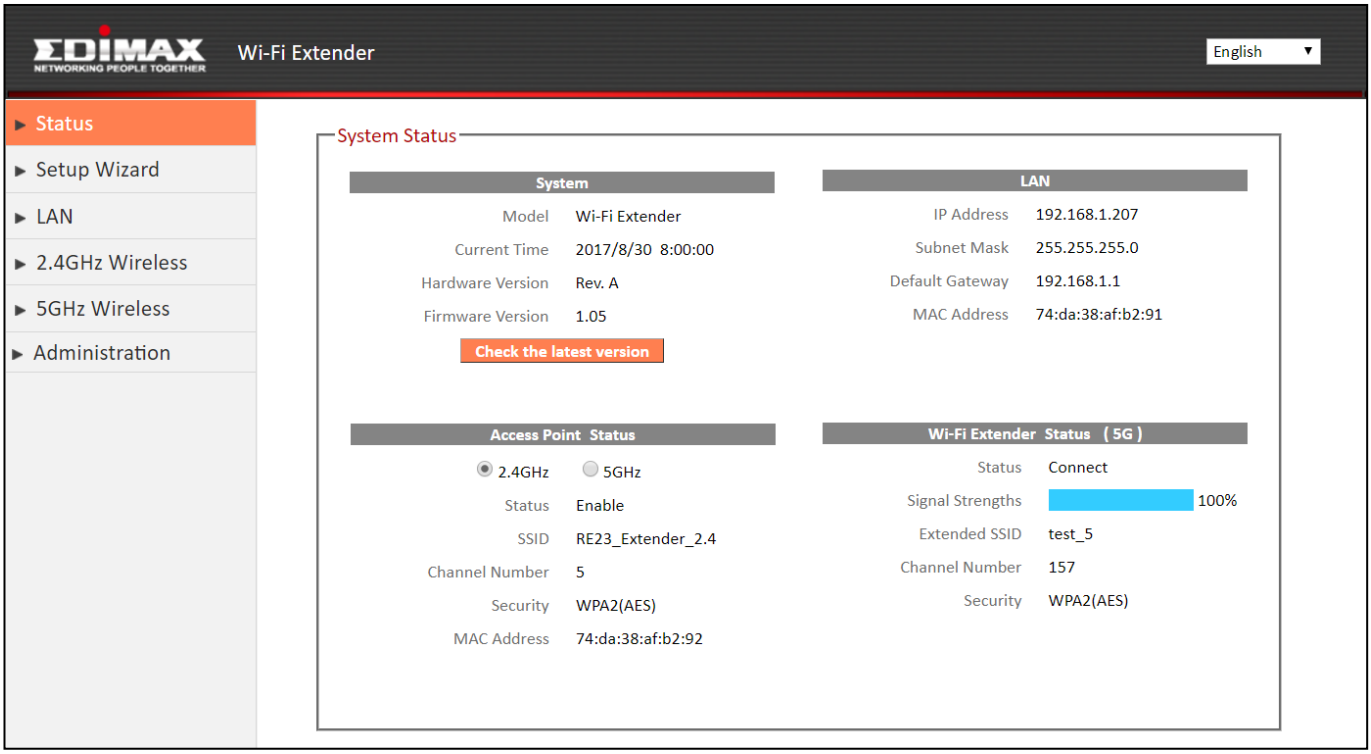
Wi-Fi Bridge



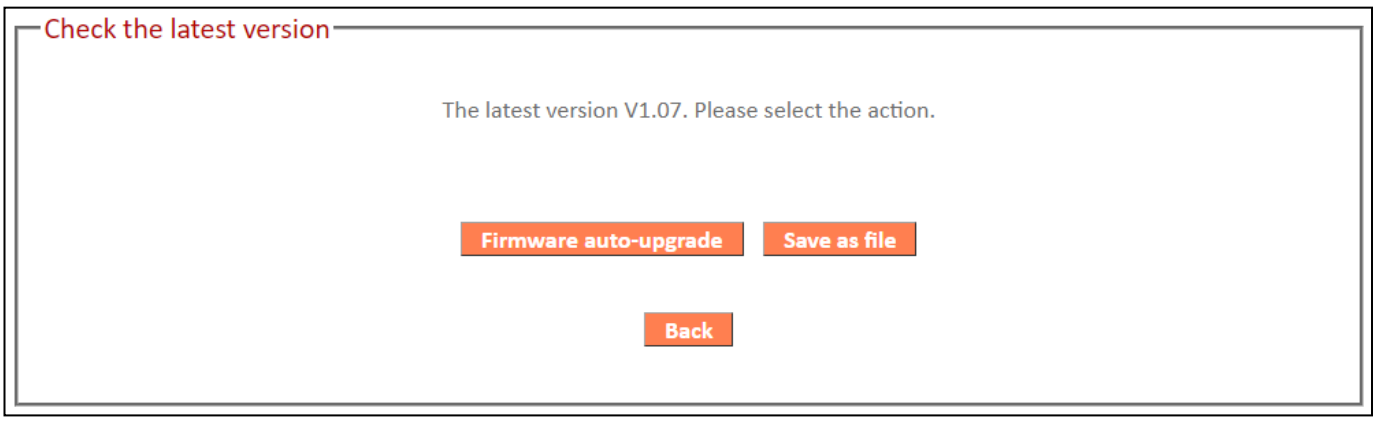
III-3-1 Status / Firmware Upgrade

The “Status” page displays basic system information about the device.

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

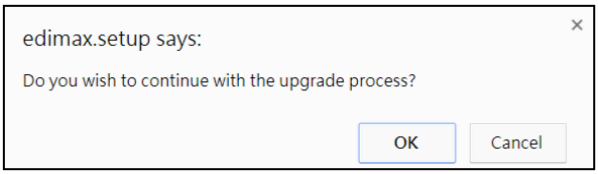


Click the orange **Check the latest version** button to check the latest version as shown below:



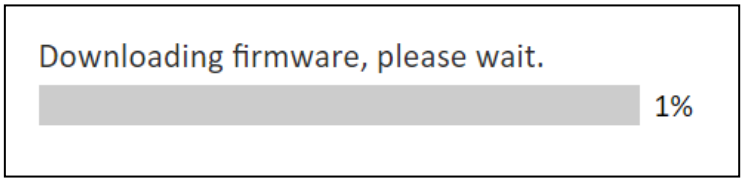
To backup the existing firmware version (recommended), click the **Save as File** button.

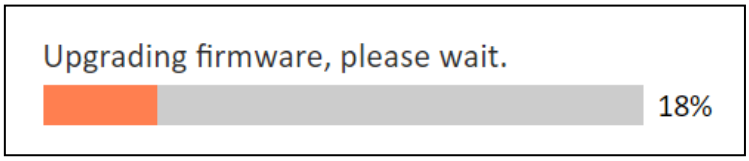
To upgrade firmware version, click **Firmware auto-upgrade**. The browser will ask you to confirm:



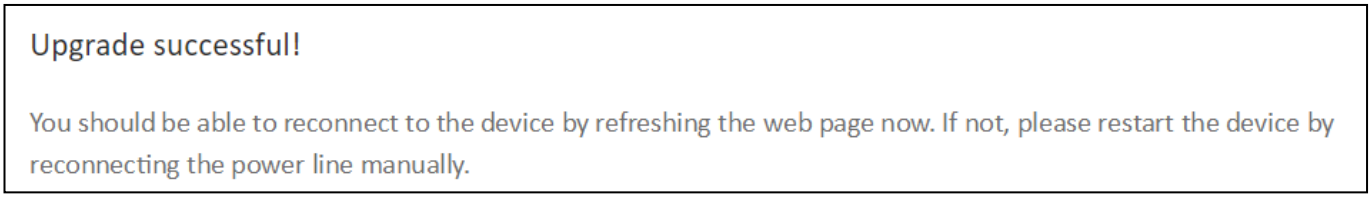
Click **OK** to continue the upgrade process.

Firmware will first be downloaded, followed by the actual upgrade:



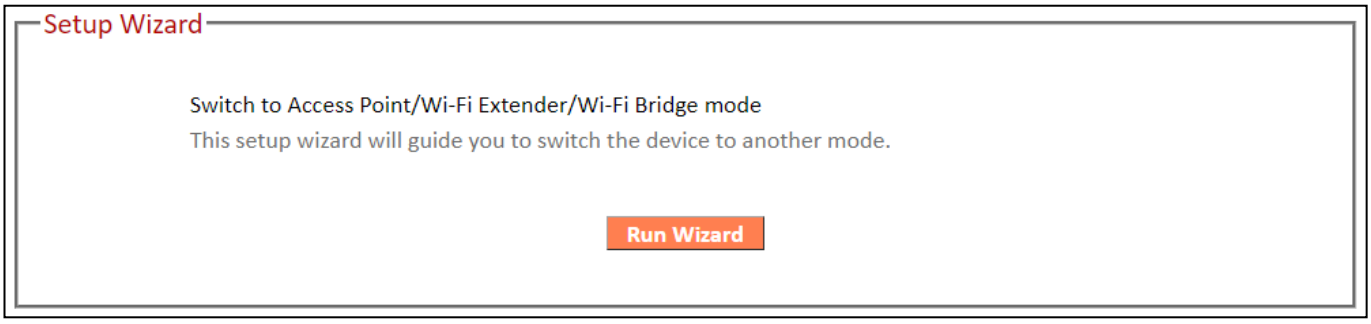


Firmware upgrade is successful!



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” and then click “Run Wizard” to begin.

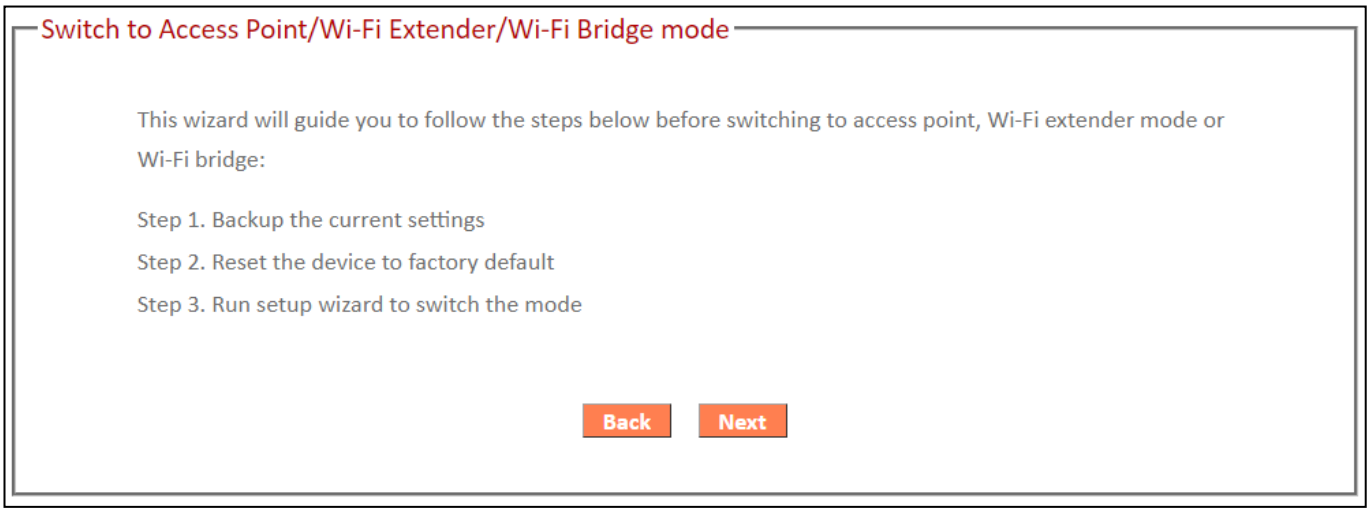


Switch to Access Point / Wi-Fi Extender / Wi-Fi Bridge mode	This wizard will help you to switch the device to a different operating mode: Access Point mode, Wi-Fi extender mode, Wi-Fi bridge mode (see below).

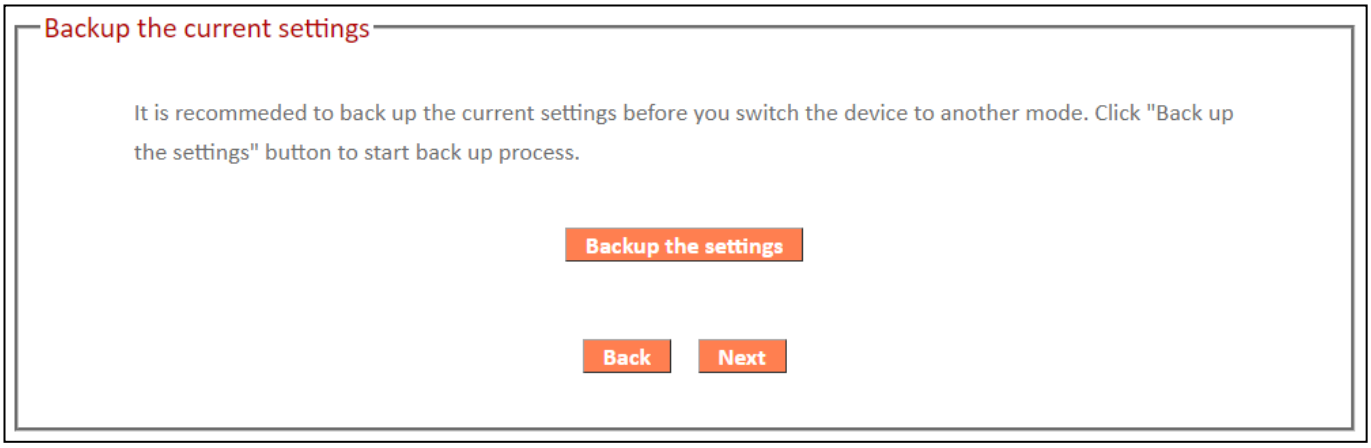
Switch to Access Point / Wi-Fi Extender / Wi-Fi Bridge mode:

Follow the on-screen instructions to run the wizard.

1. An introduction will be shown after clicking **Run Wizard**, click **Next** to proceed



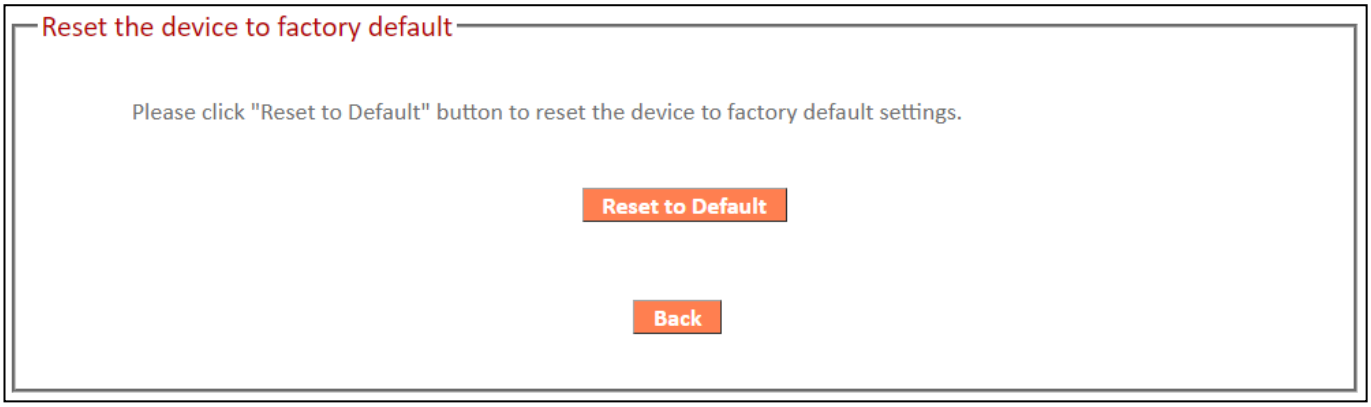
2. The wizard will ask you to back up current settings.



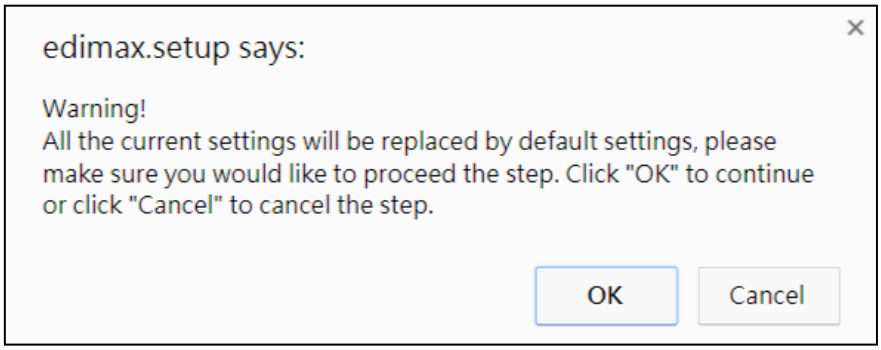
Click **Backup the settings** to back up. The file should have the name "config.bin"

Click **Next** to proceed to reset the device.

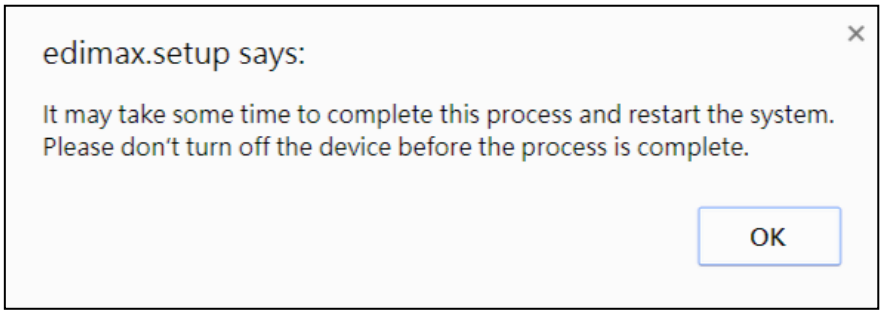
3. Click **Reset to Default** to proceed.



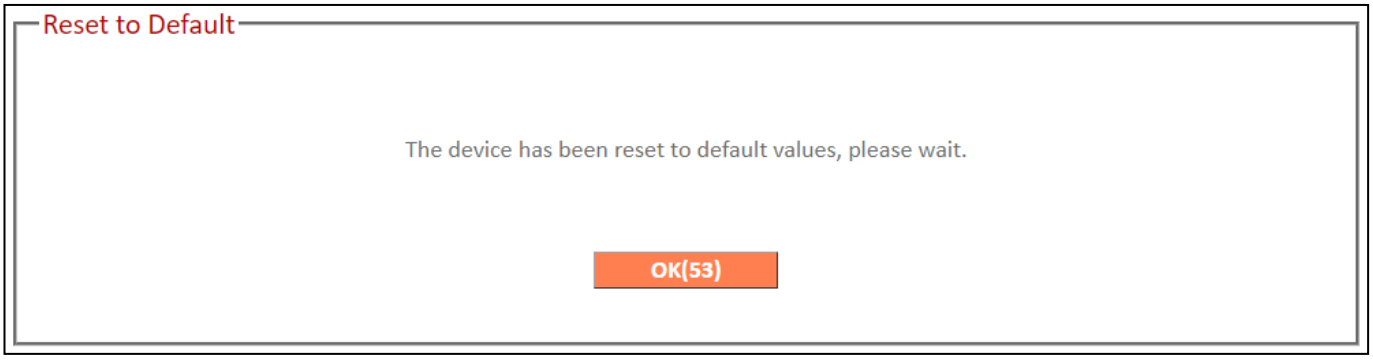
A reminder will be shown to indicate that all settings will be restored to default.



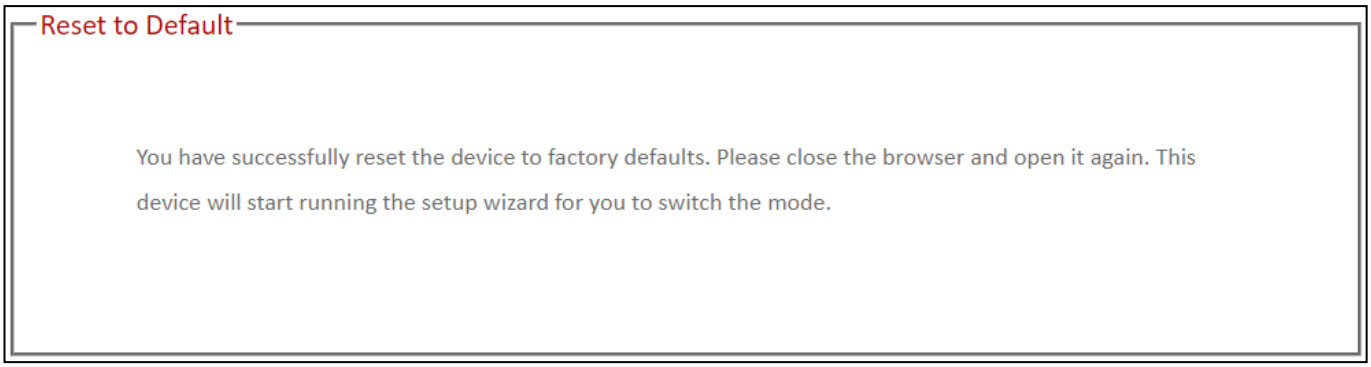
A second reminder will be shown to indicate that resetting the device may take some time.



4. The on-screen message will be shown below during the reset:



5. Close the browser (or the tab of the browser).



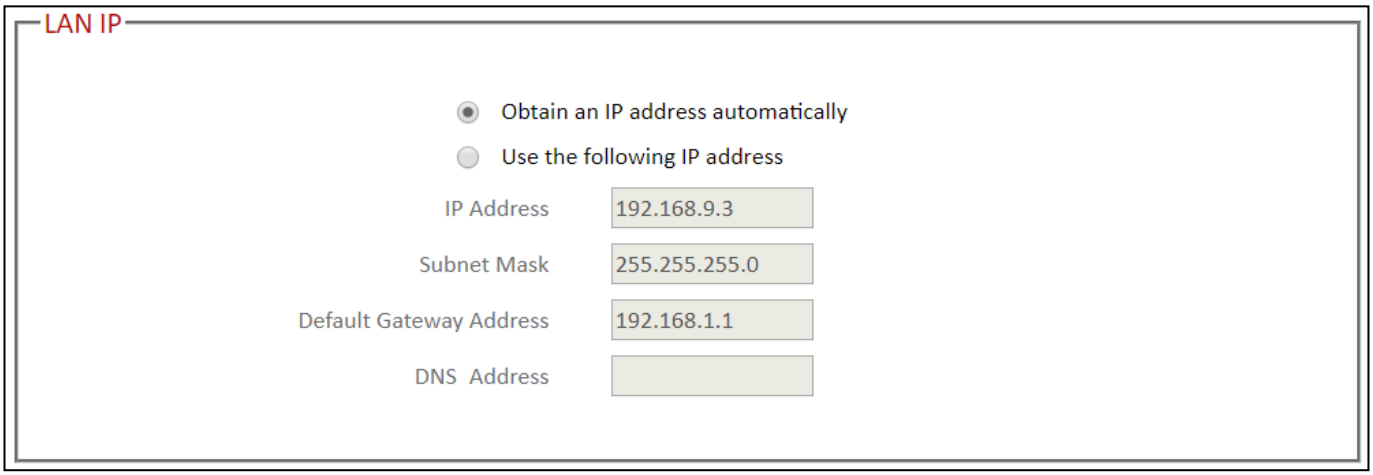
6. Go through the *steps 3 to 5* of ***II-4 IQ Setup*** and choose the desired "Operation Mode".

7. Follow the on-screen wizard to setup, or refer to the subsections in ***II-4 IQ Setup***.

III-3-3 LAN

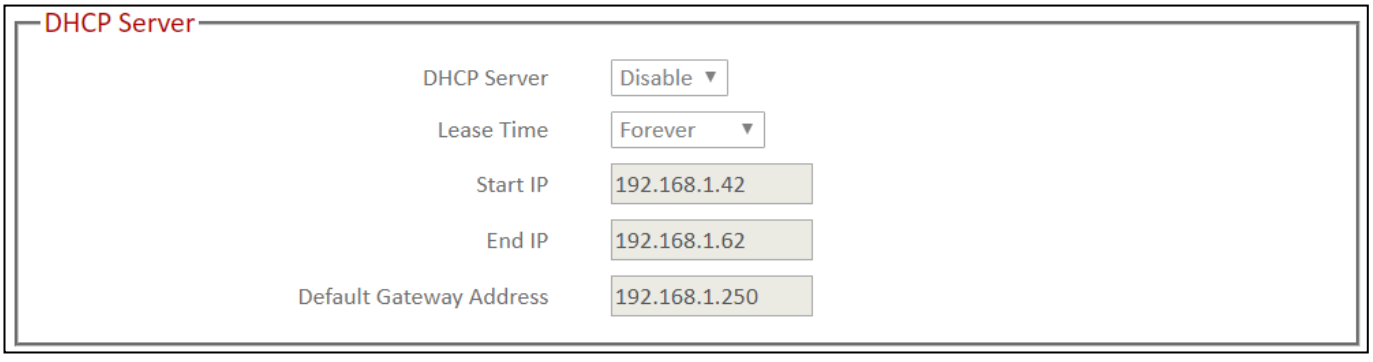
Wi-Fi Extender mode and Access Point mode only

You can configure your Local Area Network (LAN) on this page. Set the device to “Obtain an IP address automatically” or assign an IP address manually by selecting “Use the following IP address” and enter the necessary fields.



IP Address	Specify the IP address here. This IP address will be assigned to the device and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway Address	Enter a default gateway address. This is the node that forwards packets on to other networks.
DNS Address	Enter a DNS address.

If the network environment does not have a DHCP server, users can enable the DHCP server for the network and use the following configurations to setup the server.



DHCP Server	Enable or Disable DHCP server function.
Lease Time	Select a lease time for how long each device is assigned an IP address.
Start IP	Enter the starting IP address of the IP assignment range.
End IP	Enter the end IP address of the IP assignment range.
Default Gateway Address	Enter a default gateway address. This is the node that forwards packets on to other networks.

III-3-4 2.4GHz Wireless & 5GHz Wireless

Wi-Fi Extender mode and Access Point mode only

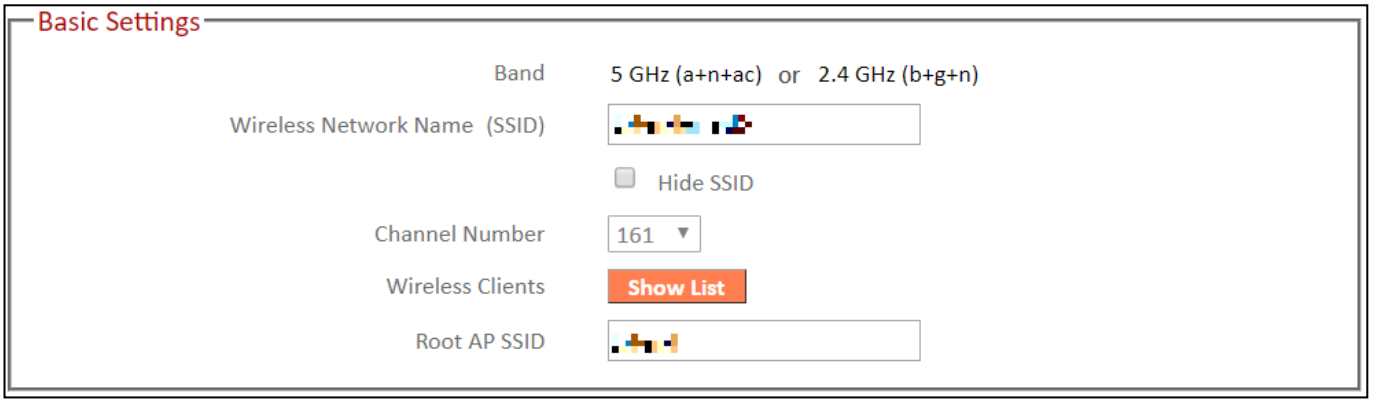
The “2.4GHz Wireless” & “5GHz Wireless” menu allows you to configure SSID and security settings for your Wi-Fi network, guest Wi-Fi network, WPS access control (in access point mode).

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

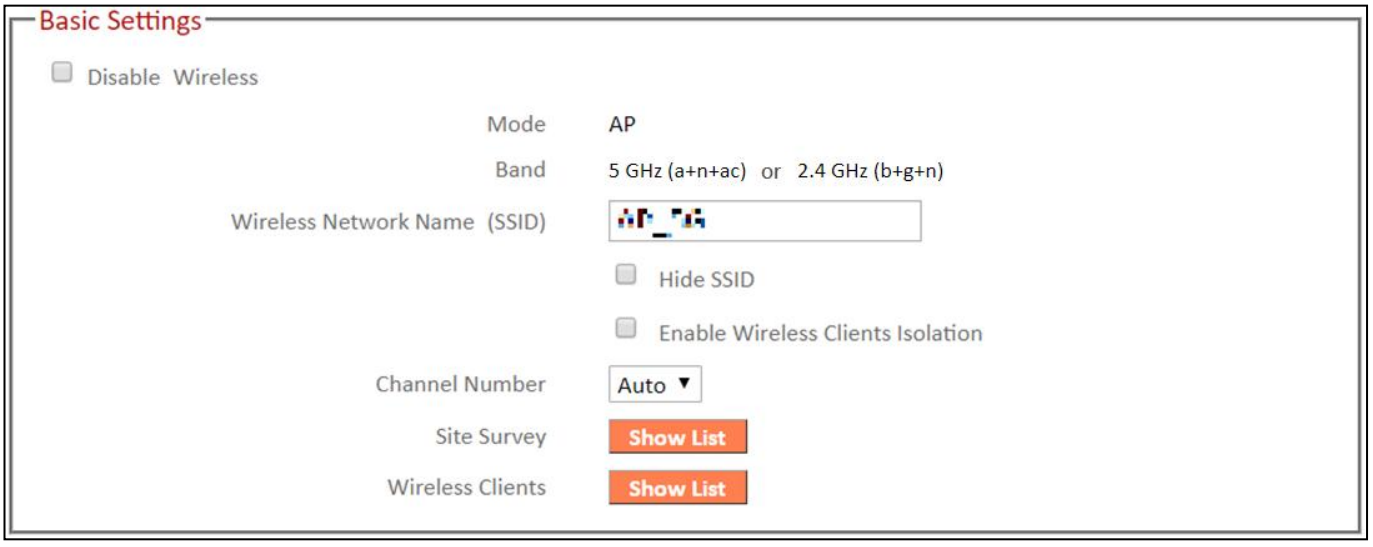
III-3-4-1 Basic

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

Wi-Fi Extender



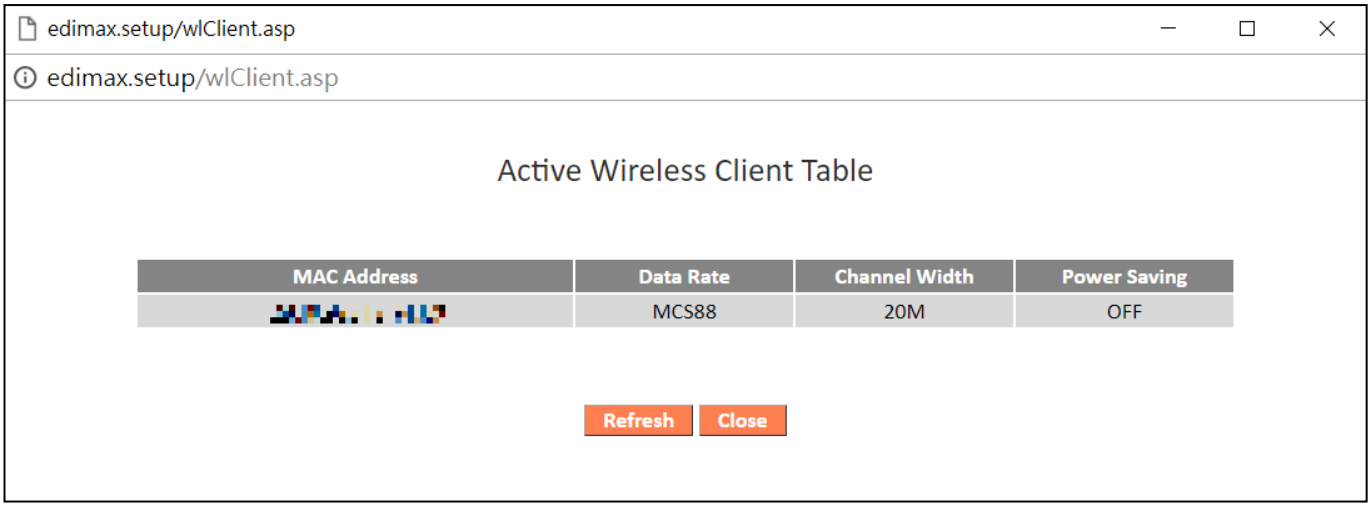
Access Point



Band	Displays the wireless standards used for the device. **2.4GHz (b+g+n)**: 802.11b, 802.11g, and 802.11n wireless standards. **5GHz (a+n+ac)**: 802.11a, 802.11n, and 802.11ac wireless standards.
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.
Hide SSID	When unchecked, the SSID will be visible to clients. When checked, the SSID will not be visible to clients. If SSID is not visible, clients must manually enter the SSID to connect. A hidden SSID is typically more secure.
Channel Number	(AP mode only) Select a wireless radio channel or use the default "Auto" setting from the drop-down menu.
Site Survey (AP mode only)	Click "Show List" to display a new window showing other wireless networks.
Wireless Clients	Click "Show List" to display a new window showing information about wireless clients. Please disable any pop-up blockers if the browser cannot display the list.
Root AP SSID (Extender only)	In extender mode, displays the SSID the extender is connected to (router or access point). This will only be displayed for the band the extender is extending the signal for (either 2.4GHz or 5GHz).

Wireless Clients

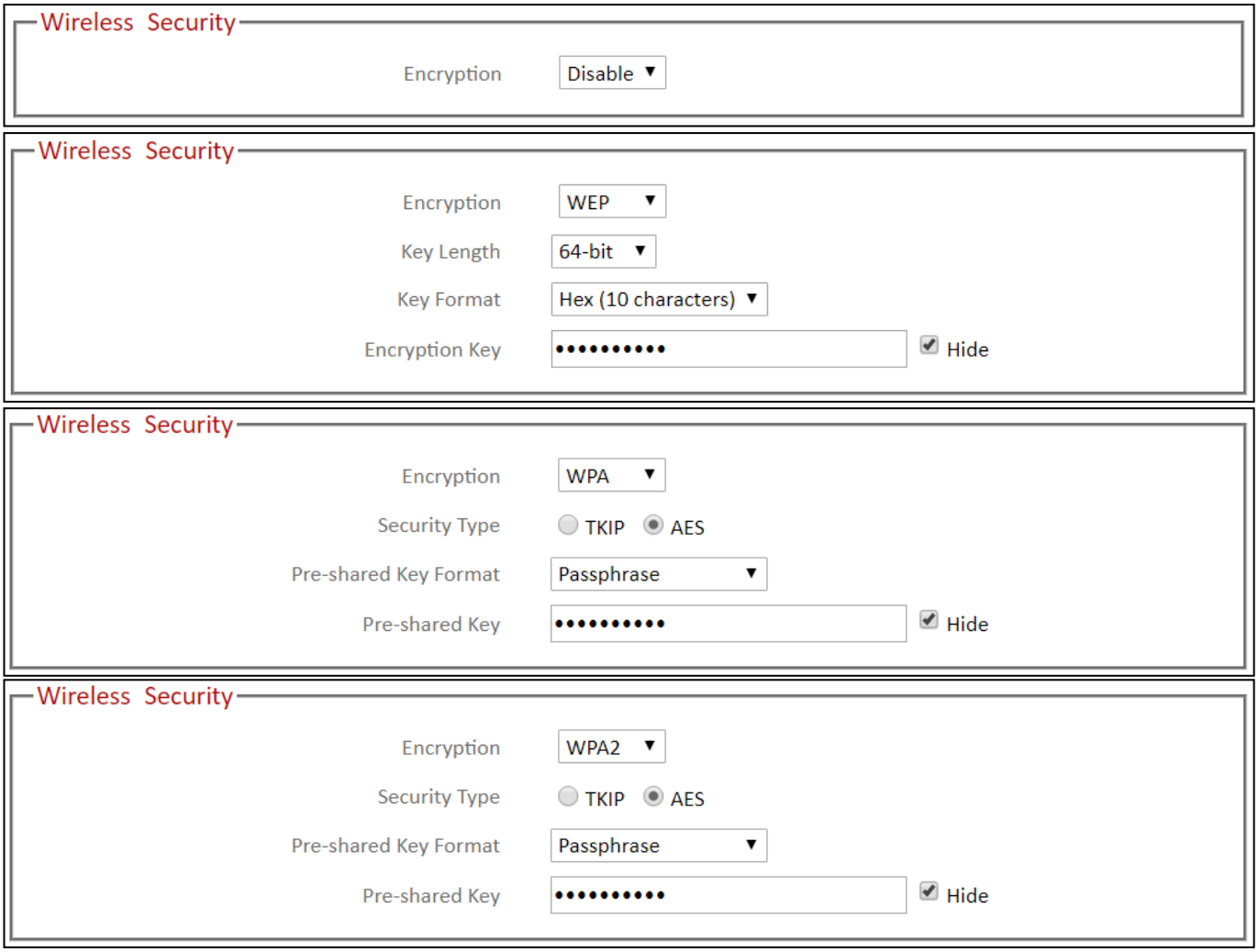
A window will pop-up when **Show List** is pressed, displaying the wireless clients as shown below:



Wireless Security

The device provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

You can choose the encryption type, or disable wireless security completely.



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

Encryption	If **Disable** is selected, no wireless security is implemented and no password/key is required to connect to the network **WEP**: WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security, consider using WPA encryption. **WPA**: WPA is a secure wireless encryption type with strong data protection and user authentication. **WPA2**: WPA2 is a secure wireless encryption type with

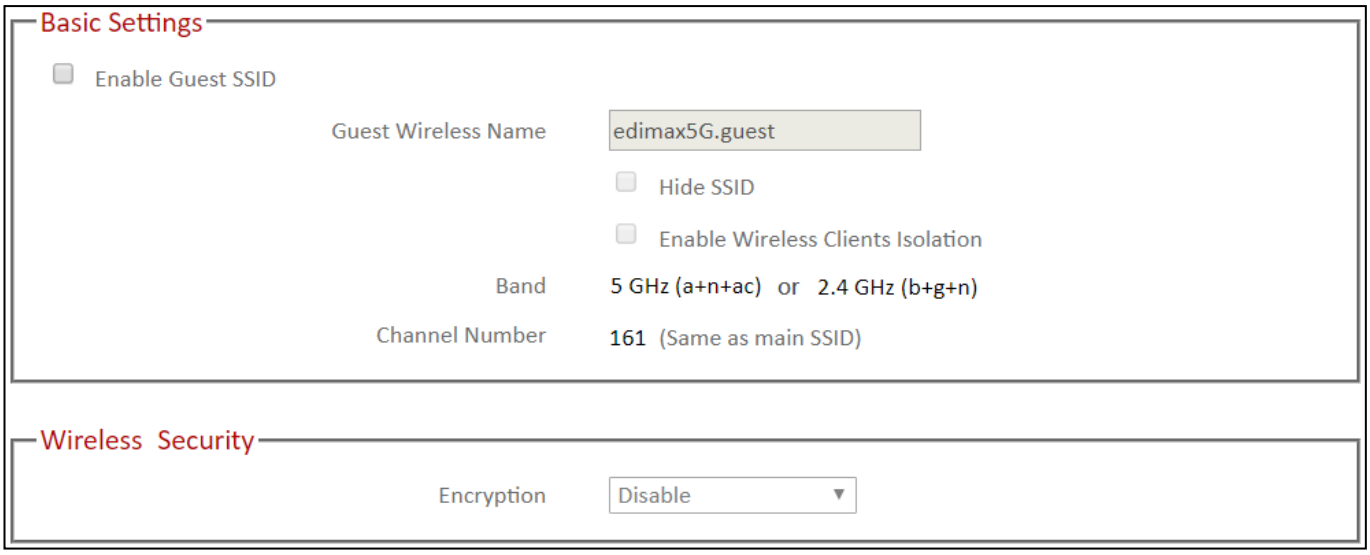
	strong data protection and user authentication. WPA2 is safer than WPA, but is not supported by all wireless clients. Please make sure your wireless client supports your selection.
Key Length (WEP)	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Format (WEP)	Choose from **ASCII (5 characters)** or **Hex (10 characters)** (any alphanumerical character 0-9, a-z and A-Z).
Security Type (WPA/WPA2)	Select **TKIP** or **AES** encryption type. AES is recommended.
Pre-shared Key Format (WPA/WPA2)	Choose from **Passphrase** (8 – 63 alphanumeric characters) or **Hex (64 characters)** (up to 64 characters from 0-9, a-f and A-F).
Encryption Key / Pre-Shared Key	Enter the security key according to the security type / key format. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.

III-3-4-2 Guest

Additional “Guest” Wi-Fi network can be setup for guest users to enjoy Wi-Fi connectivity without accessing your primary SSID. 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.

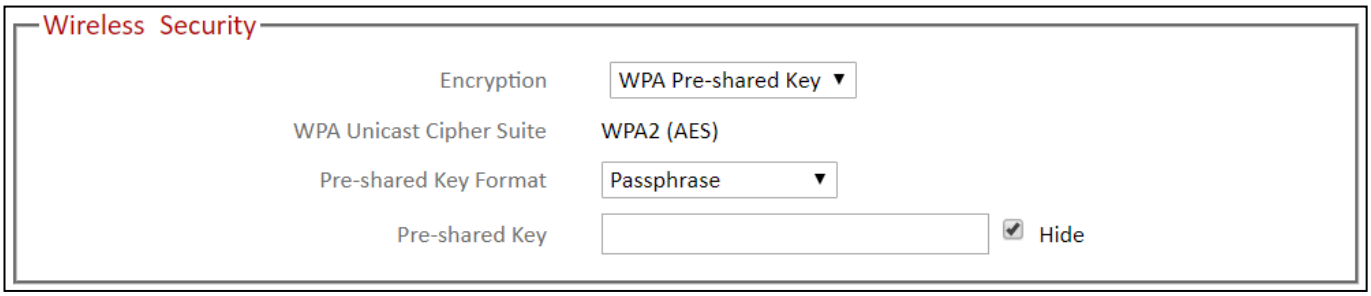
Not available in access point mode



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.
Hide SSID	Check the checkbox to hide the SSID. If unchecked, the SSID will be visible to clients as an available Wi-Fi network. If checked, the SSID will not be visible to anyone, but the clients can manually enter the SSID to connect to the network. Hidden SSID is typically more secure.
Enable Wireless Clients Isolation	Check the box to enable wireless clients isolation. This prevents wireless clients connected to the device 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 standards used for the device: **2.4GHz (b+g+n)**: 802.11b, 802.11g, and 802.11n wireless standards. **5GHz (a+n+ac)**: 802.11a, 802.11n, and 802.11ac wireless standards.
Channel Number	Channel number for the guest network is the same as the main SSID and cannot be adjusted independently.

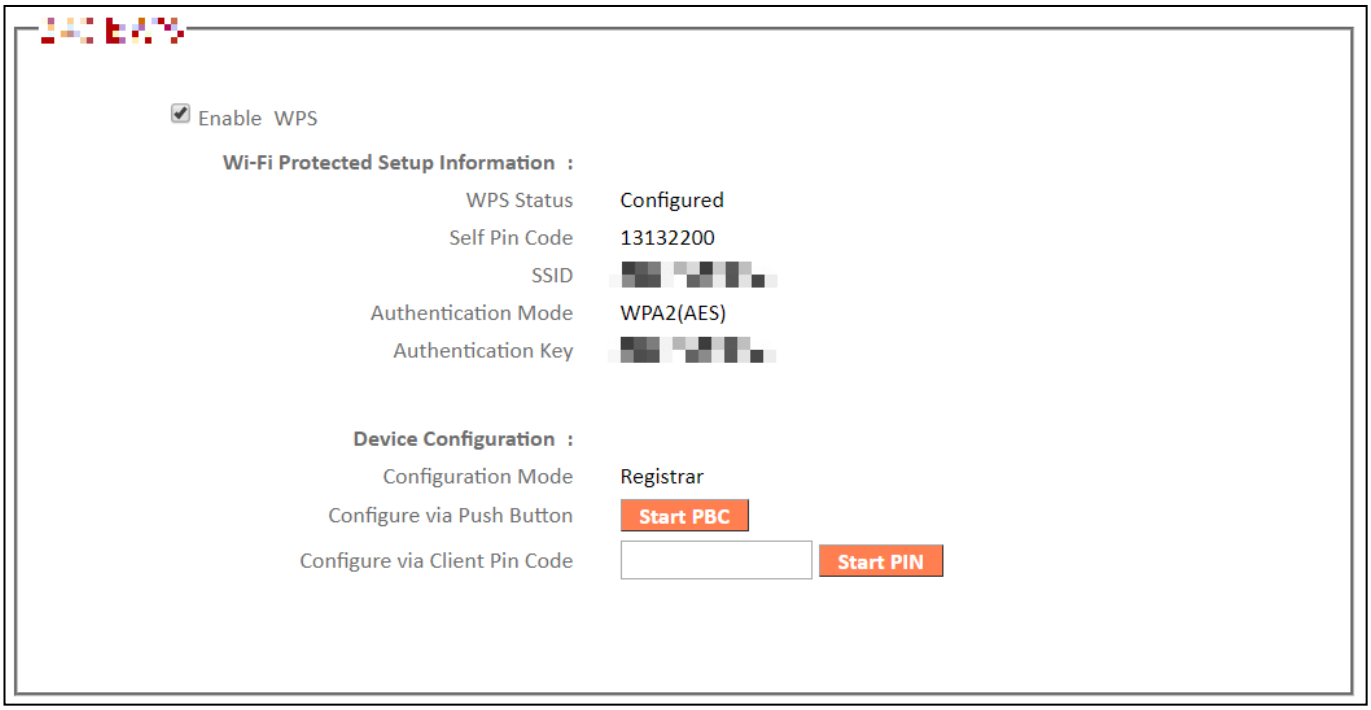
Wireless Security



Encryption	If **Disable** is selected, no wireless security is implemented and no password/key is required to connect to the network **WPA Pre-shared Key**: WPA is a secure wireless encryption type with strong data protection and user authentication.
Pre-shared Key Format	Choose from **Passphrase** (8 – 63 alphanumeric characters) or **Hex (64 characters)** (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared Key	Enter the security key according to the security type / key format. A complex, hard-to-guess key is recommended. Check the “Hide” box to hide your password from being displayed on-screen.

III-3-4-3 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.
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 device. 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-3-4-4 Access Control

Access Point mode only

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 access point. Devices are each identified by their unique MAC address. If a device, not on the list of permitted MAC addresses, attempts to connect to the access point, it will be denied.

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

Client PC	Select a PC name from the drop-down list and click “>>” to display the MAC address. Manually refresh the list by selecting “Refresh’ in the drop-down menu.
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’.
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. The list will refresh.

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

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

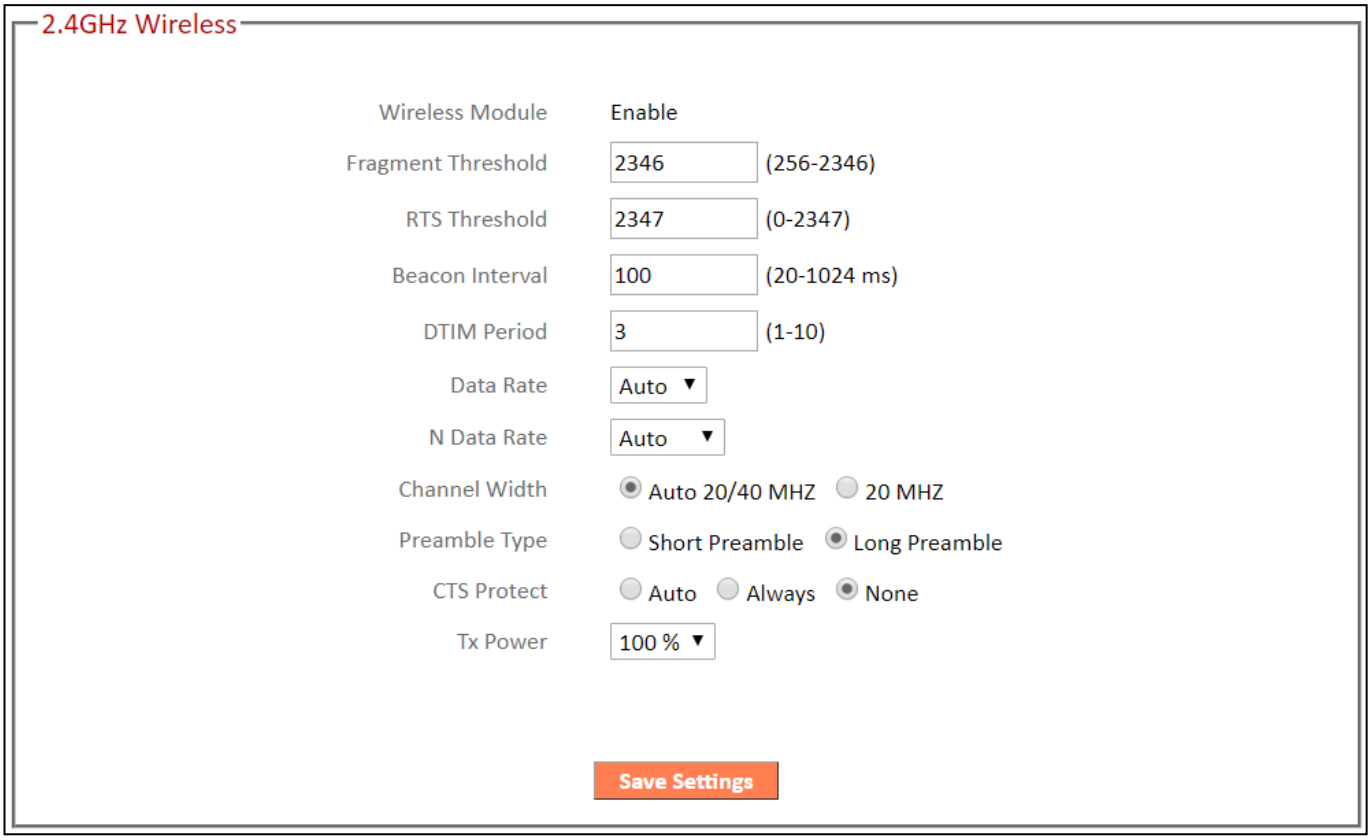
III-3-5 Advanced

Access Point mode only

Configure Advanced Features here:

III-3-5-1 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.

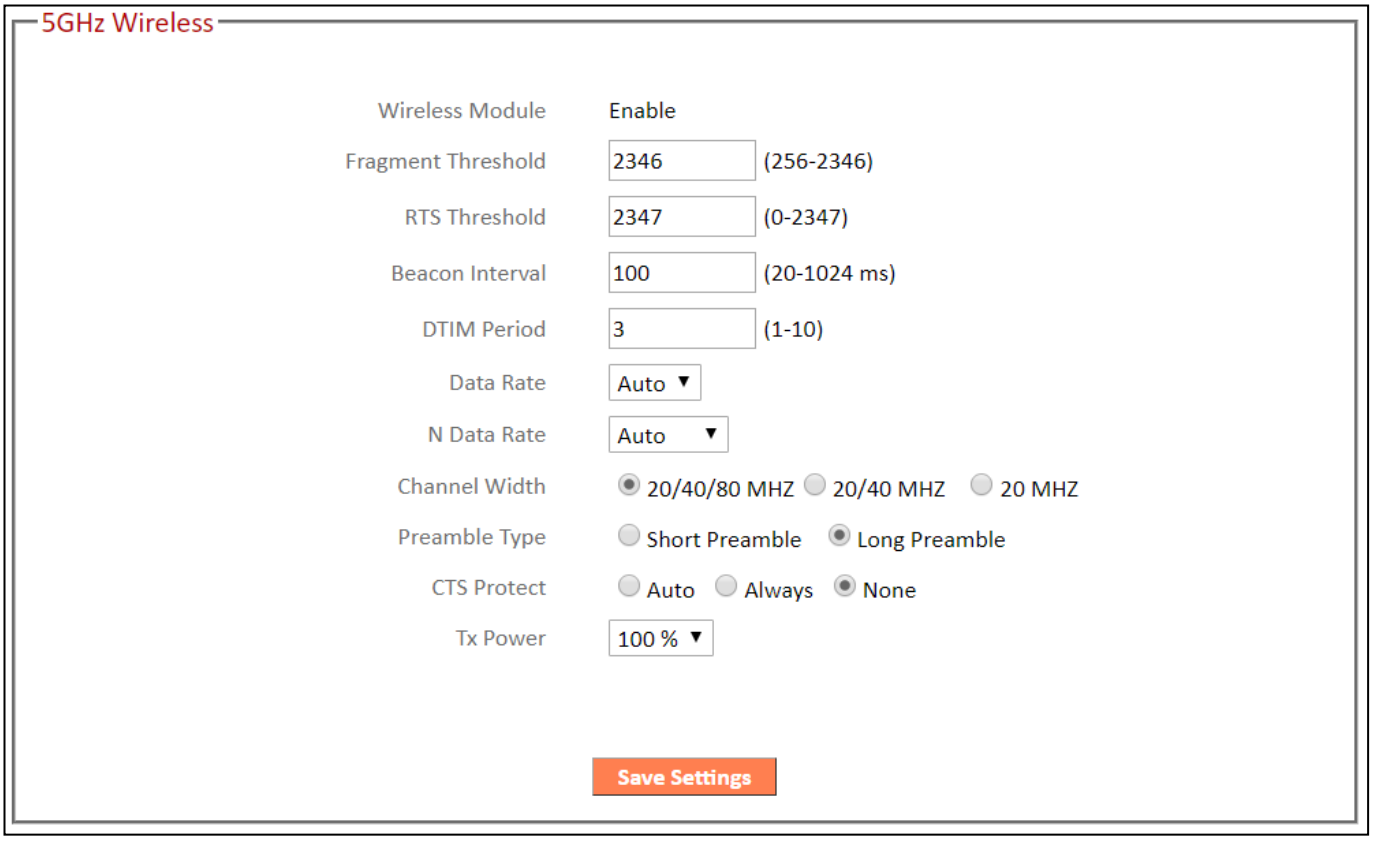


Fragment Threshold	Set the Fragment threshold of the wireless radio. The default value is 2346.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM period 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.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It is 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.

III-3-5-2 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.

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.

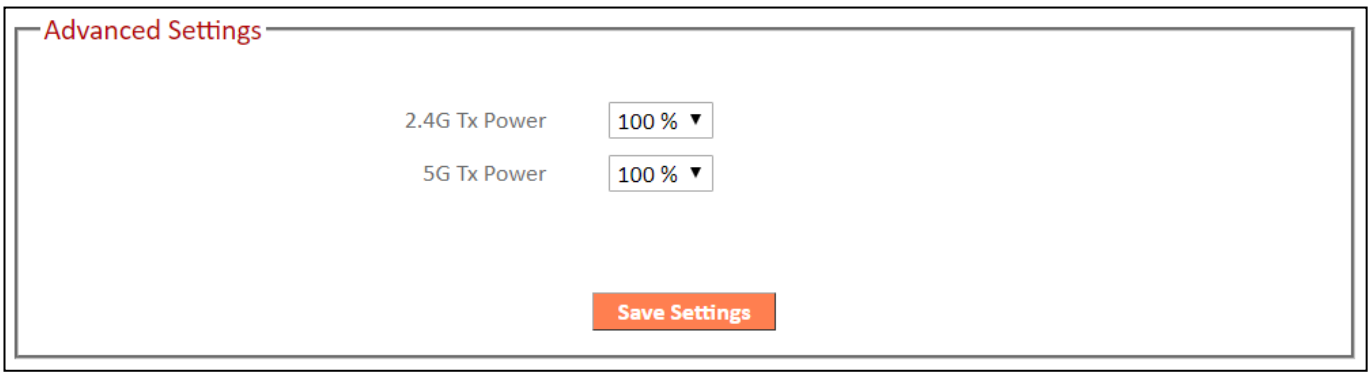
III-3-6 Administration

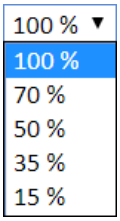
Various administrative functions can be accessed from the “Administration” menu.

III-3-6-1 Wireless

Wi-Fi Extender mode only

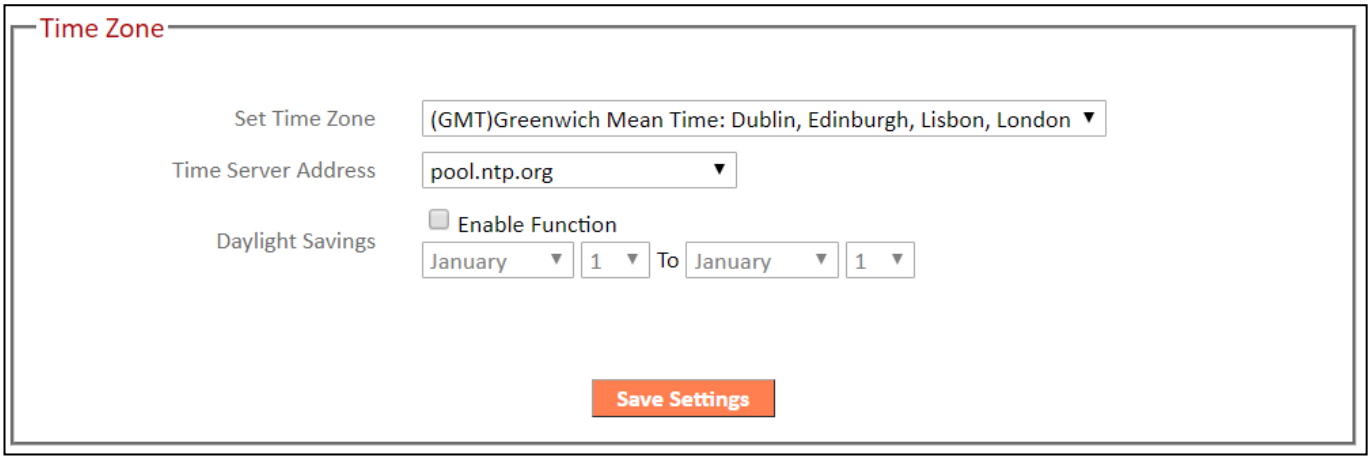
You can adjust the level of wireless output power as a percentage. Depending on the size of your location and required coverage, you may not require 100% output power. Reducing the output power can enhance security since your Wi-Fi signal will not extend to potential malicious/unknown users in distant areas.





2.4G Tx Power	Adjust the Wi-Fi output power for the 2.4GHz frequency.
5G Tx Power	Adjust the Wi-Fi output power for the 5GHz frequency.

III-3-6-2 Time Zone

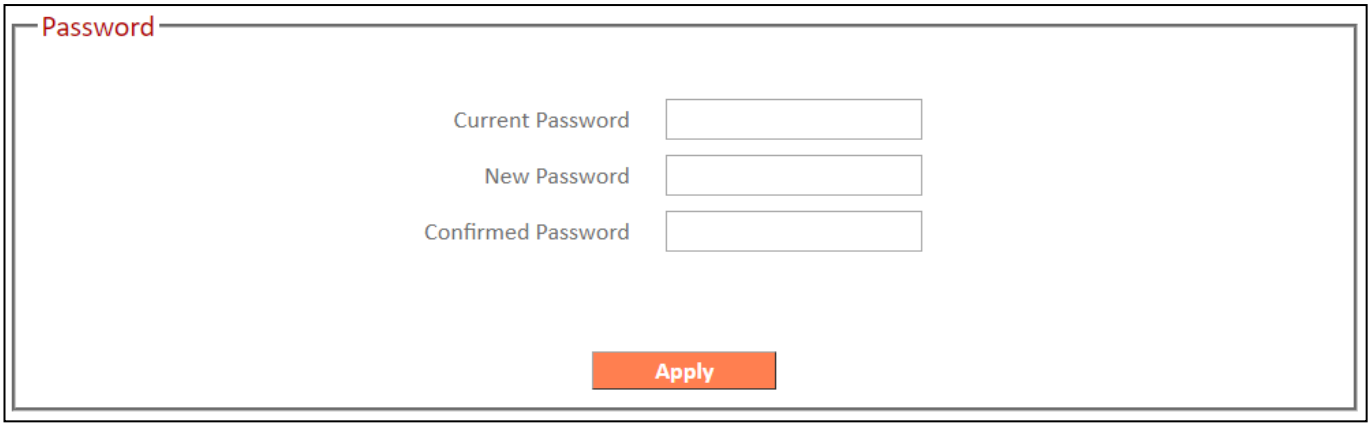


Set Time Zone	Select the time zone of your country or region.
Time Server Address	The travel router supports NTP (Network Time Protocol) for automatic time and date setup. Input the host name of the IP server manually.
Daylight Saving	If your country/region uses daylight saving time, please check the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

III-3-6-3 Password

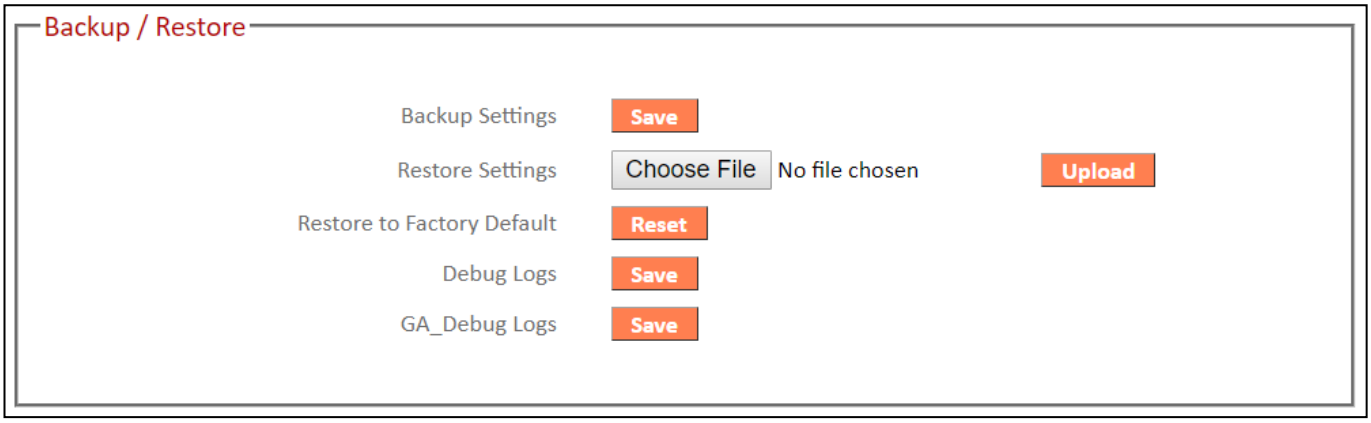
You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

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, you may have to reset it. See *I-6 Reset to Factory 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-3-6-4 Backup/Restore

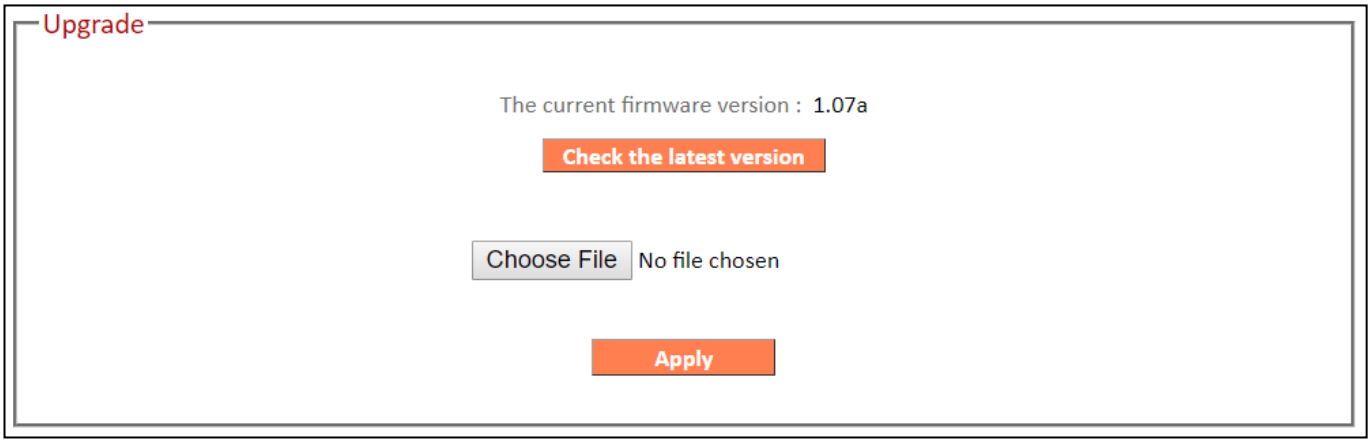


Backup Settings	Click “Save” to save the current settings on your computer as config.bin file.
Restore Settings	Click “Choose File” to find a previously saved config.bin file and then click “Upload” to replace your current settings.
Restore to Factory Default	Click “Reset” to restore settings to the 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.
Debug Logs	Click to save a log file of wireless information to your computer as a .txt file.

III-3-6-5 Upgrade

The upgrade page displays the current firmware version and allows you to upgrade the system firmware to a more recent version. You can download the latest firmware from the Edimax website and upgrade manually using the **Choose File** button or you can click the **Check the latest version** button to check your version and automatically upgrade if a newer version is available. 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 firmware upgrade and that you backup your existing firmware before upgrading.

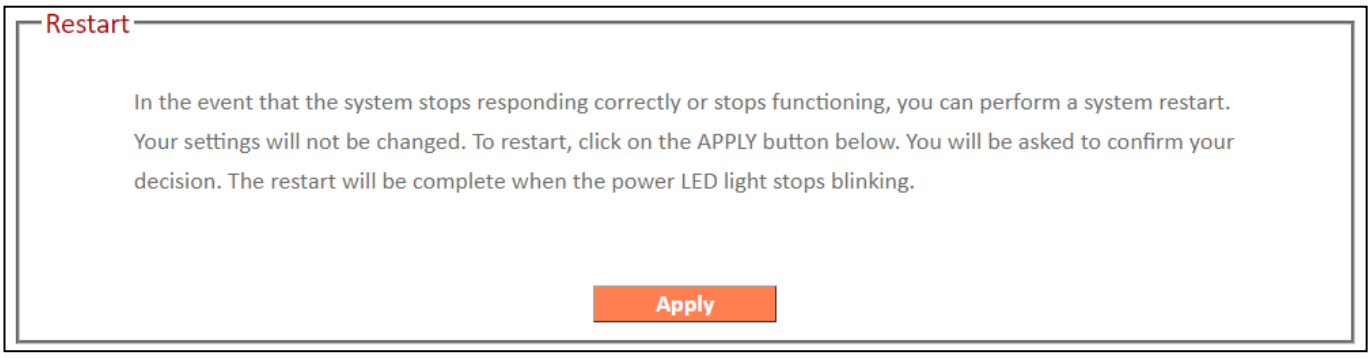


Manual Upgrade

If you have the firmware to upgrade, click “Choose File” and select your firmware file (.bin). Click “Apply” after the selection to upgrade.

III-3-6-6 Restart

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



IV Appendix

IV-1 Configuring your IP address

For the first time the URL ***http://edimax.setup*** is accessed, please ensure your computer is set to use a dynamic IP address. This allows your computer to automatically obtain an IP address from a DHCP server. You can check if your computer is set to use a dynamic IP address by following ***IV-2 Checking if your computer is using 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. **192.168.9.x (x = 3 – 254)**) as the RE23S in order to access ***http://edimax.setup***.

The RE23S's default IP address is 192.168.9.2.

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system in ***IV-3 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, so that you can access the URL ***http://edimax.setup*** in future without modifying your IP address.

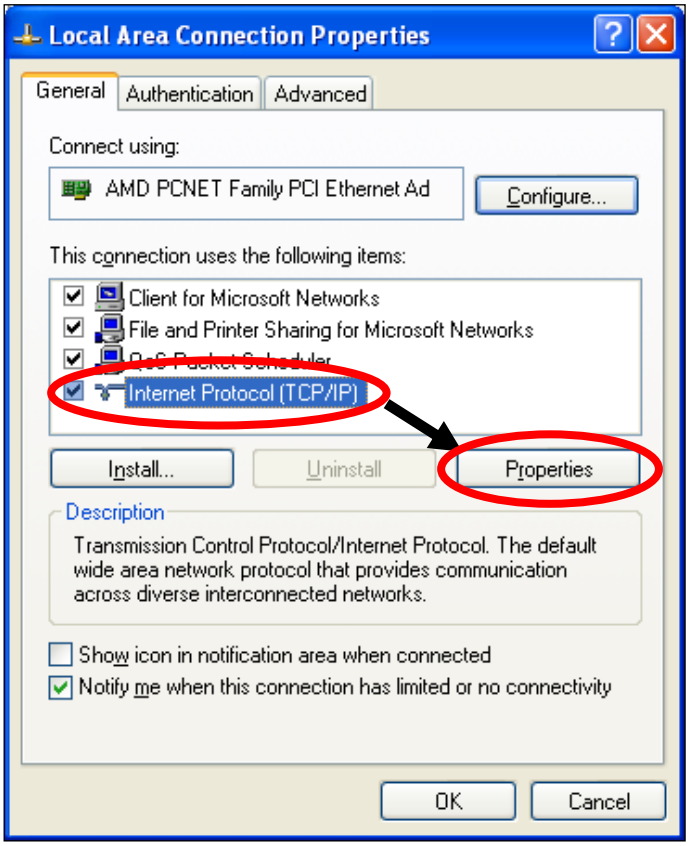
Please remember to change your IP address back to its original value after the device is properly configured.

IV-2 Checking if your computer is using a dynamic IP address

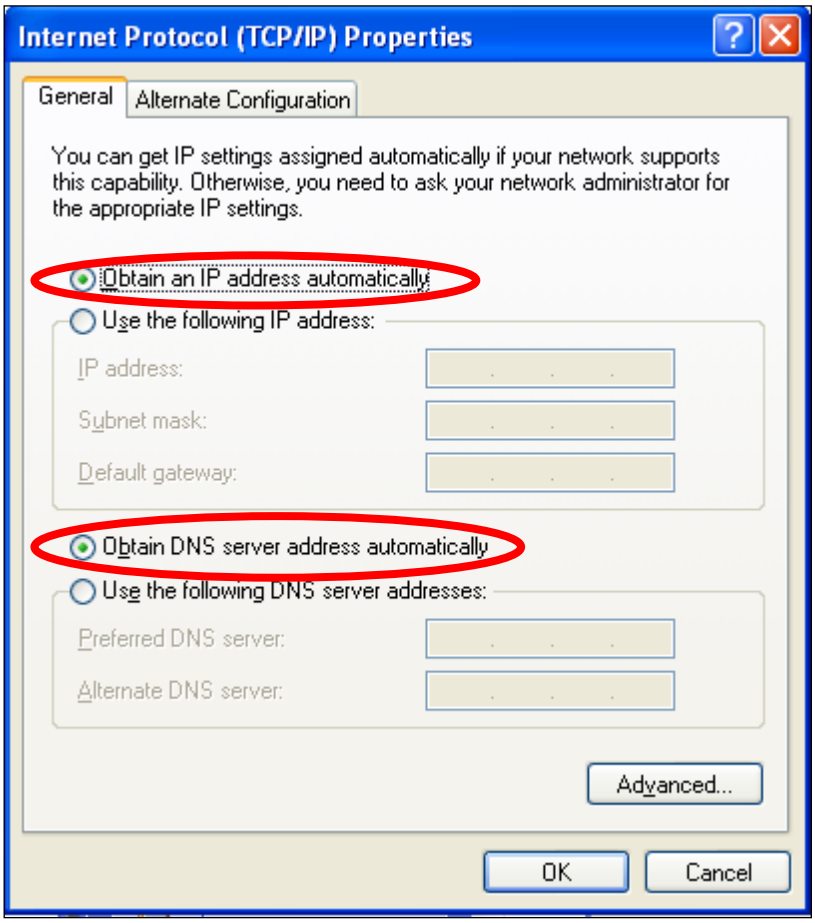
Please follow the instructions appropriate for your operating system.

IV-2-1 Windows XP

1. Click the “Start” button (it should be located in the lower-left corner of your computer) → “Control Panel” → “Network and Internet Connections” → “Network Connections” → “Local Area Connection” → “Internet Protocol (TCP/IP” → “Properties”.

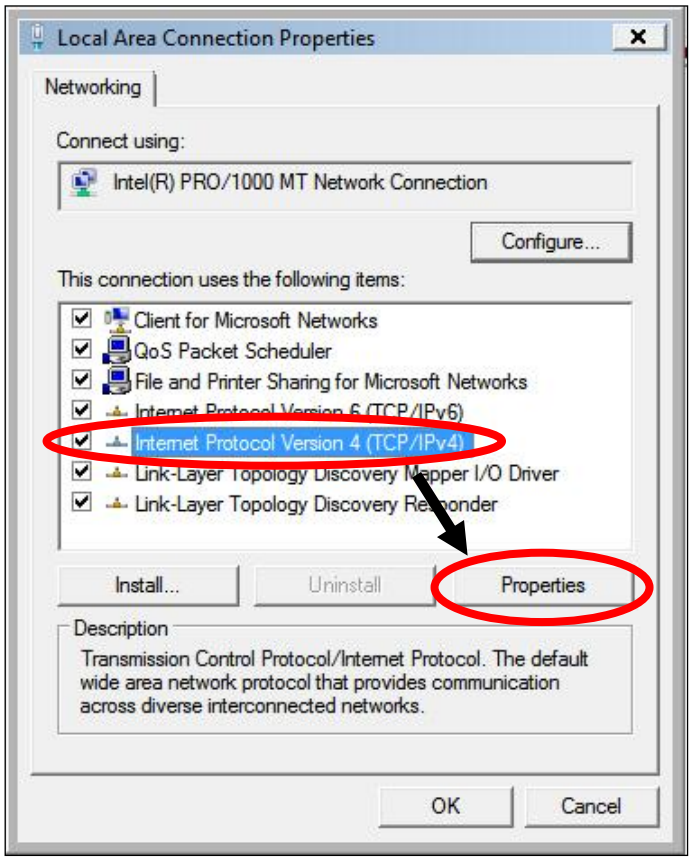


2. “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

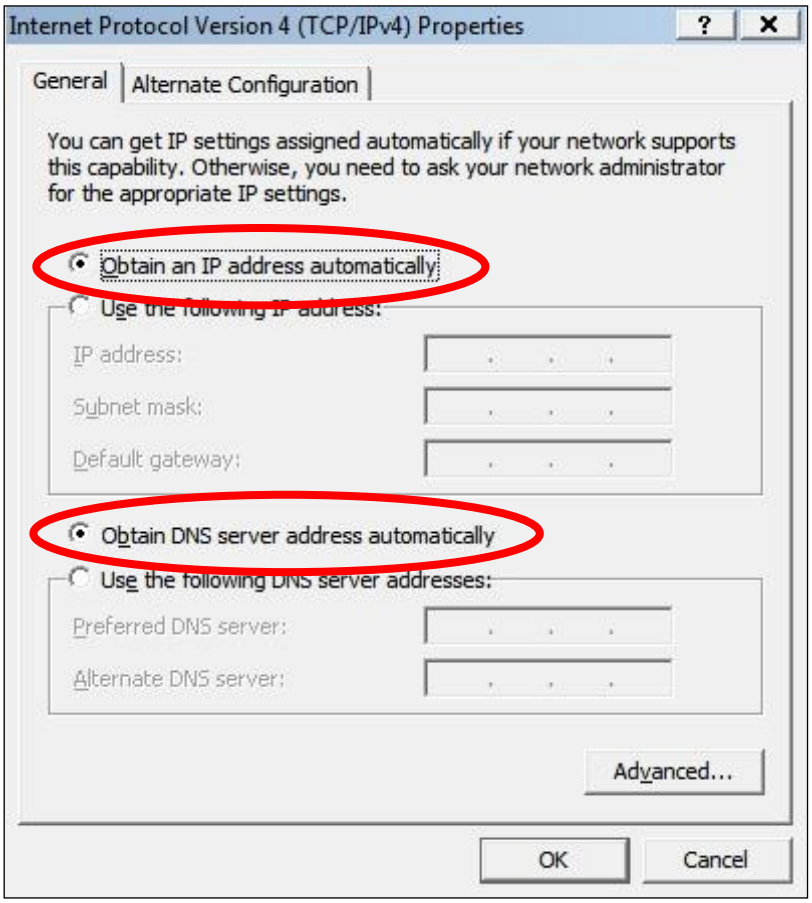


IV-2-2 Windows Vista

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

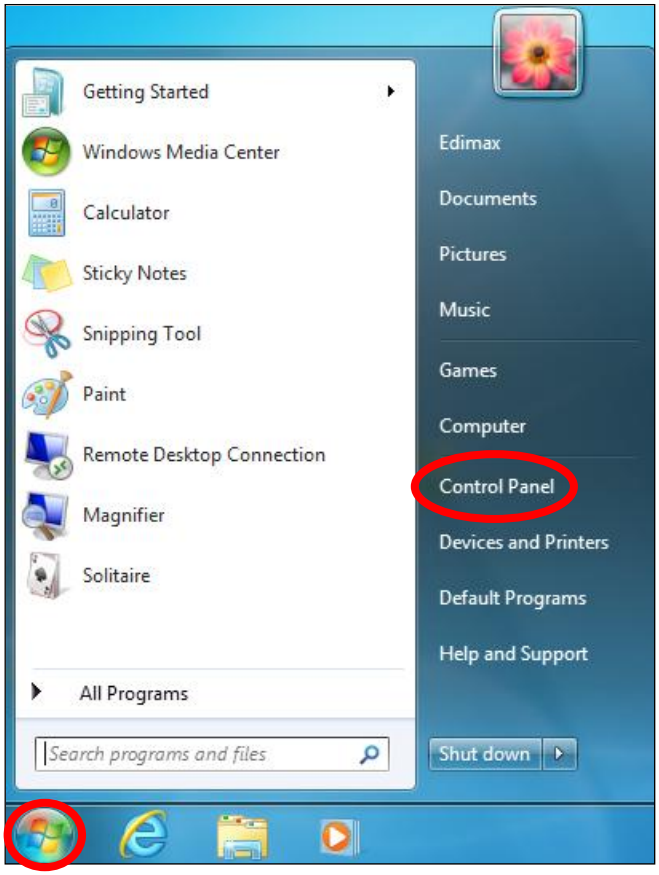


2. “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.



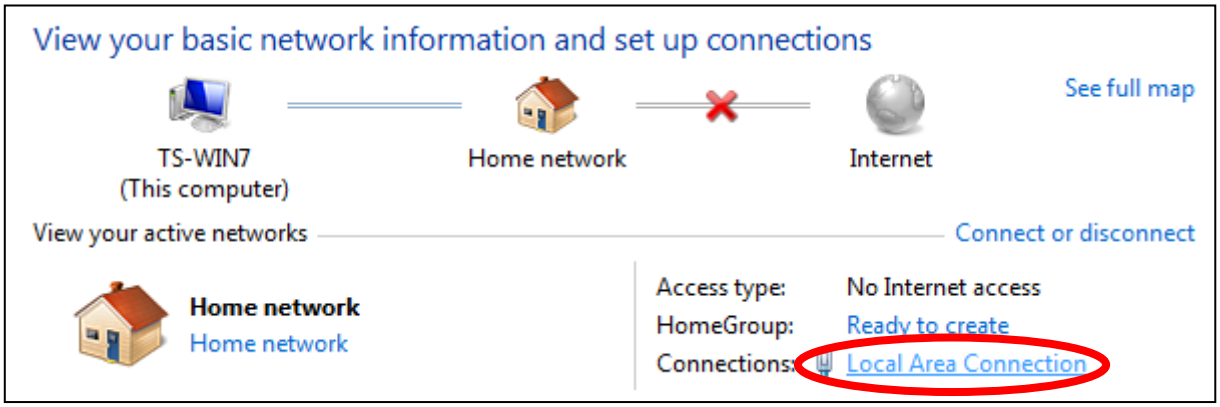
IV-2-3 Windows 7

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

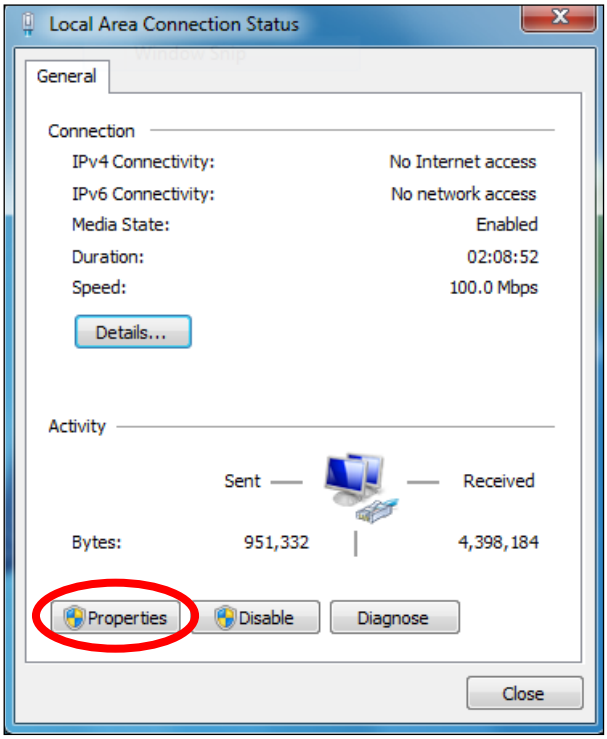


2. Under “Network and Internet” click “View network status and tasks”.

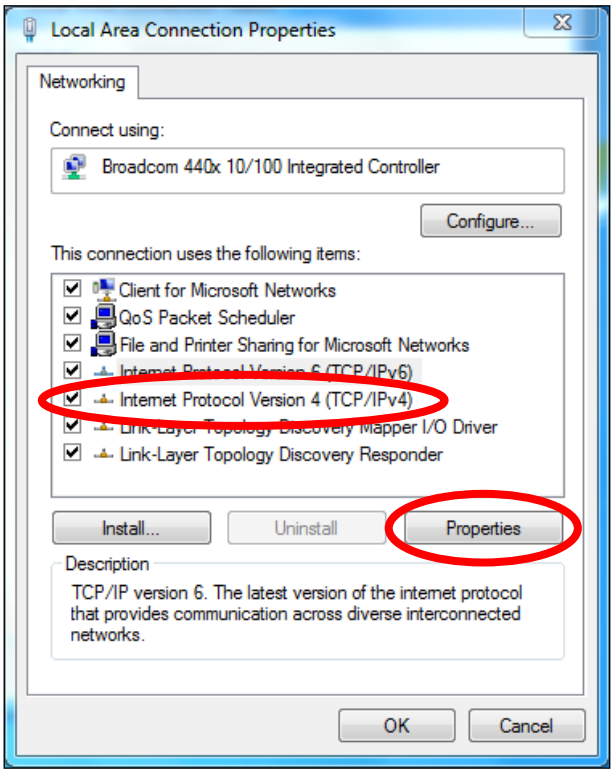
3. Click “Local Area Connection”.



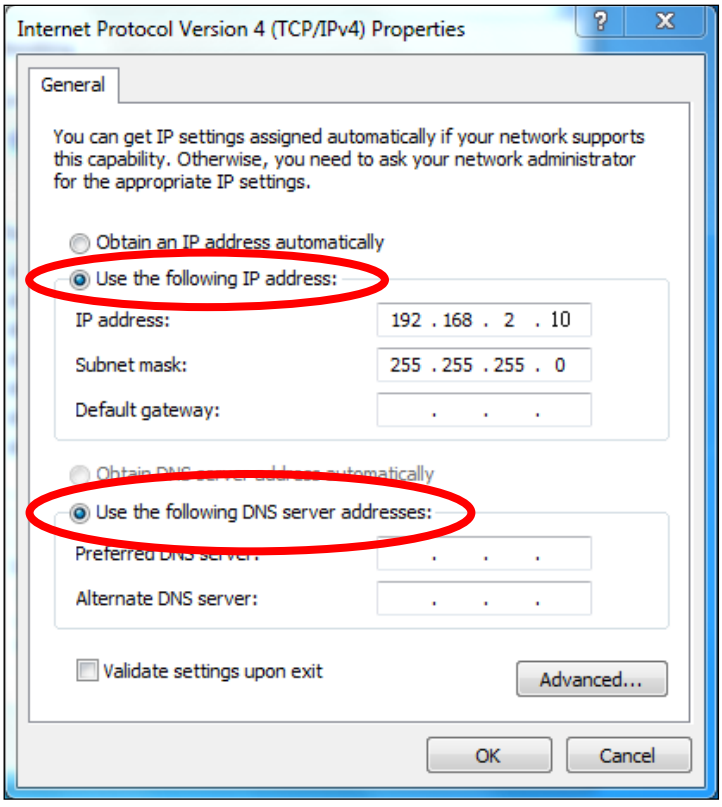
4. Click “Properties”.



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

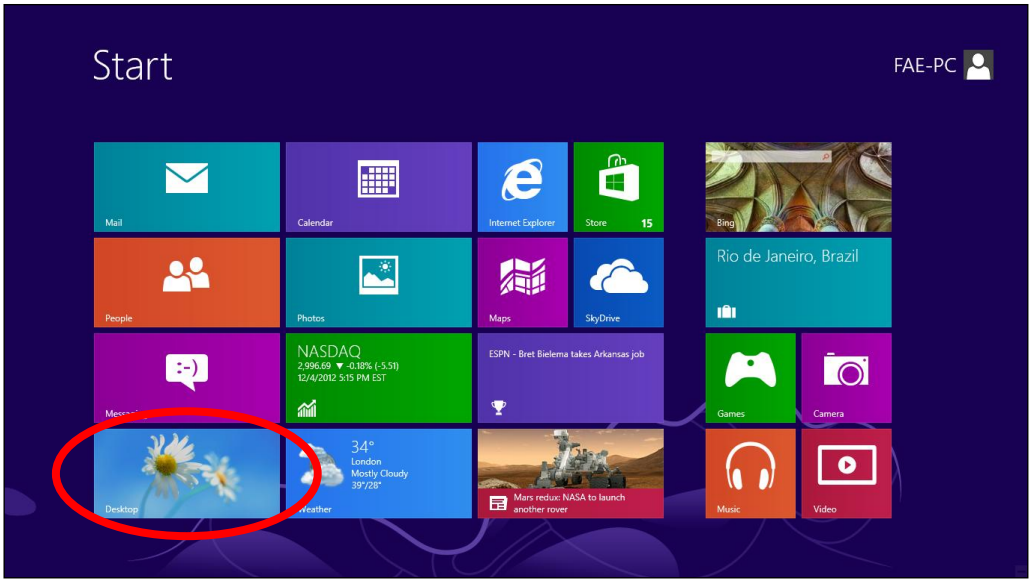


6. “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.

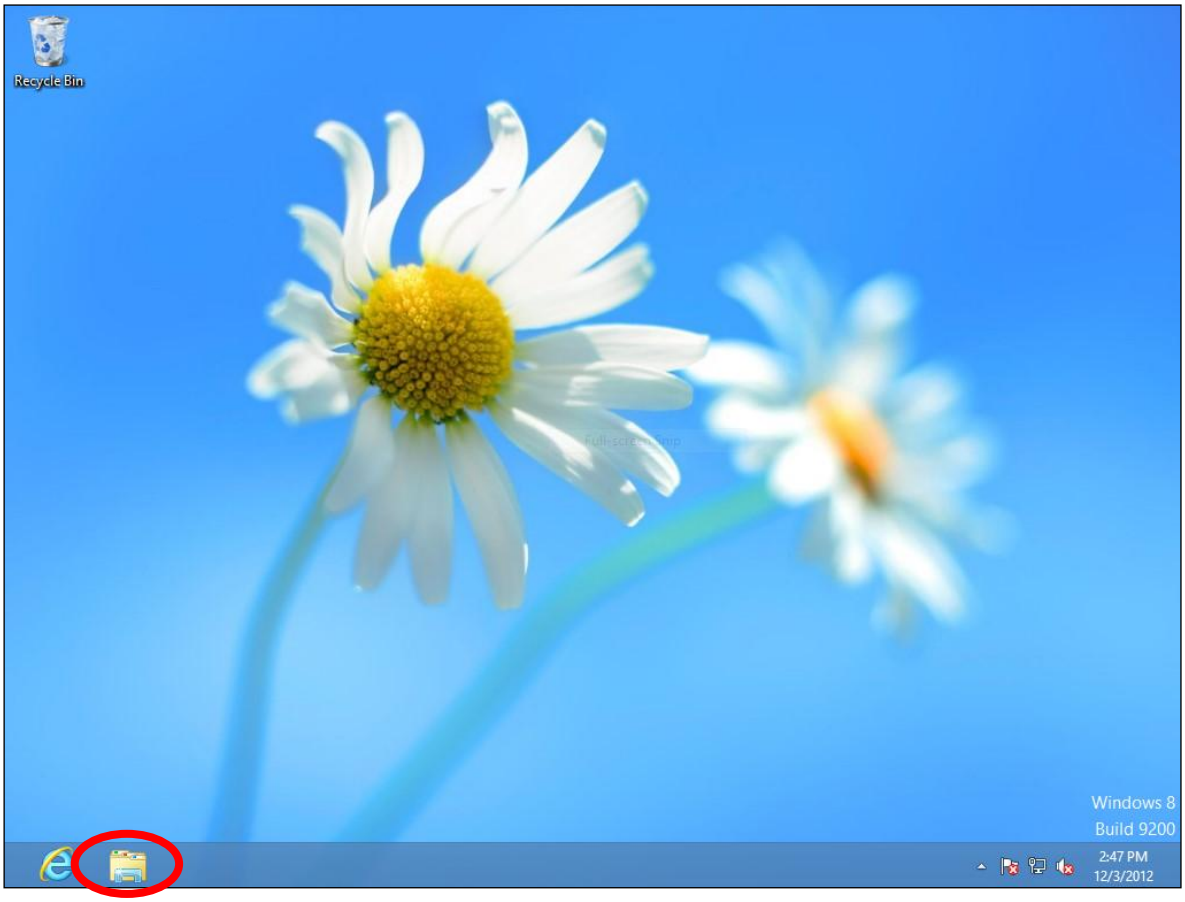


IV-2-4 Windows 8

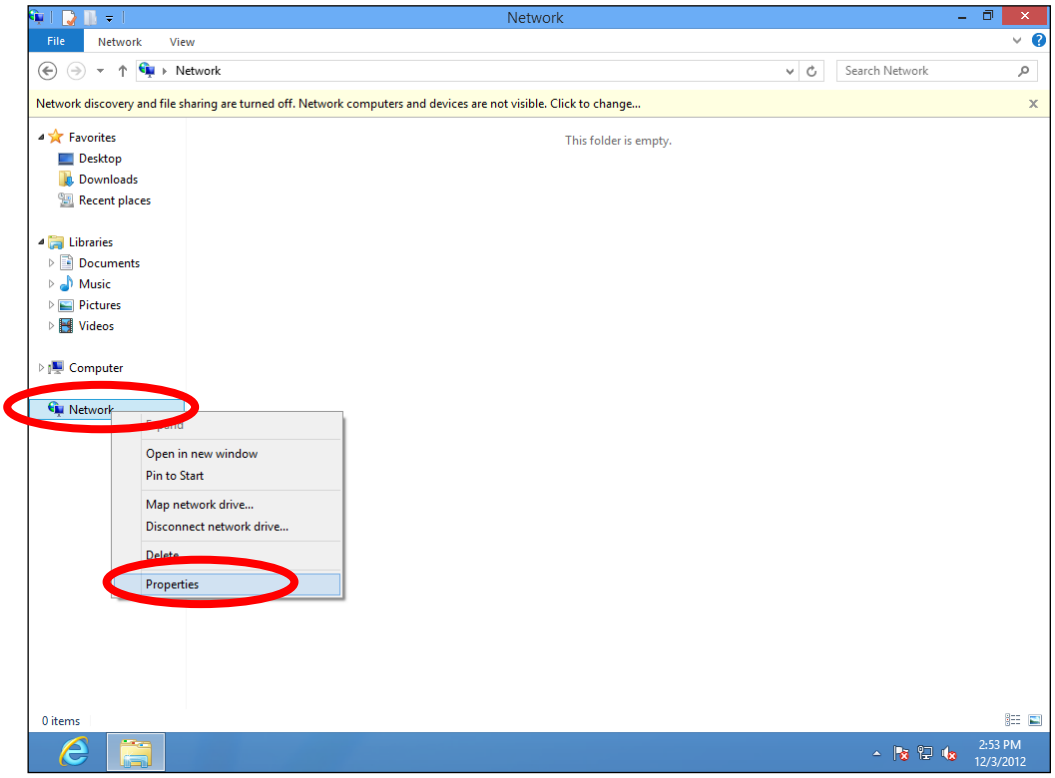
1. From the Windows 8 Start screen, switch to desktop mode by clicking the “Desktop” icon.



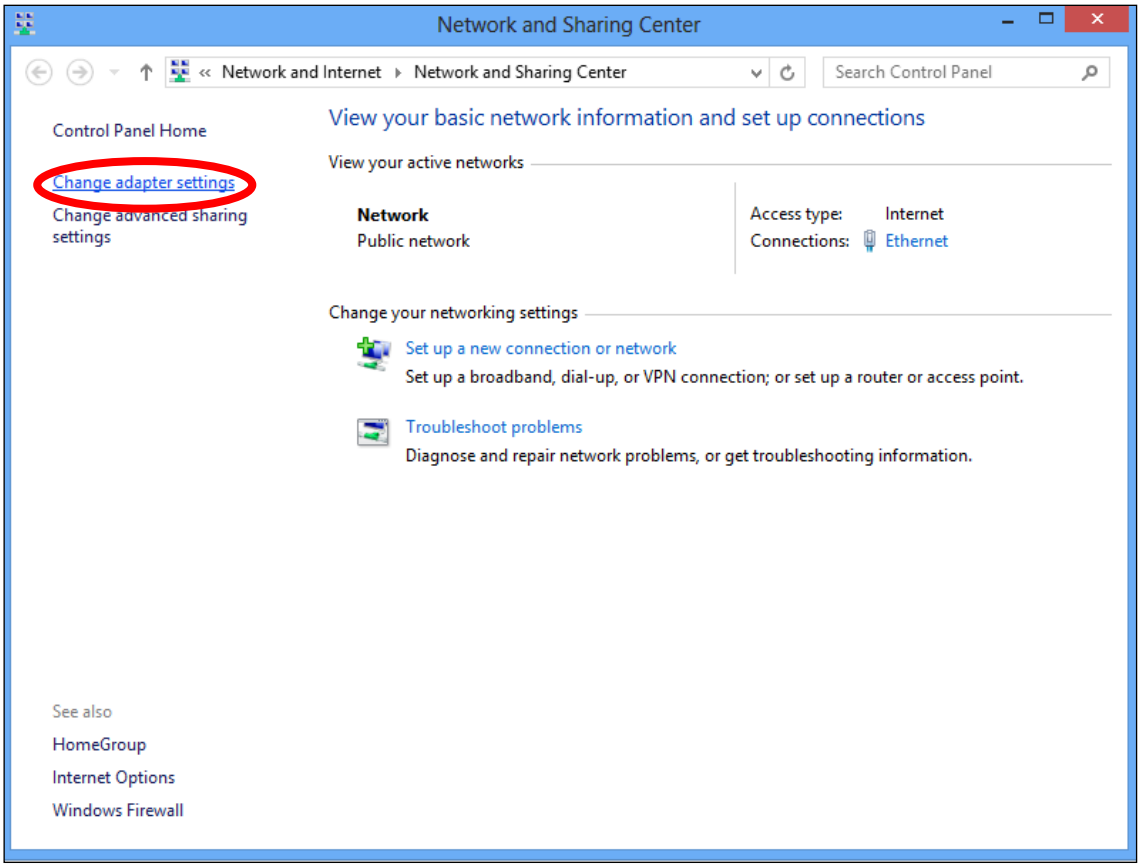
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



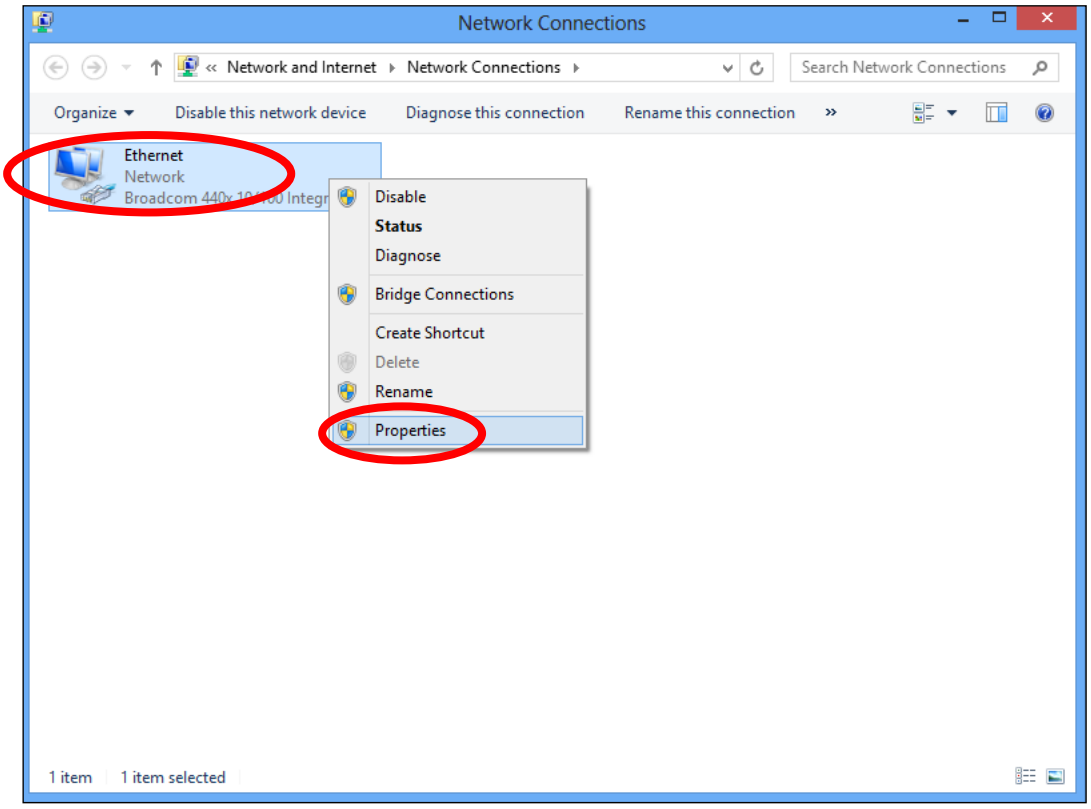
3. Right click “Network” and select “Properties”.



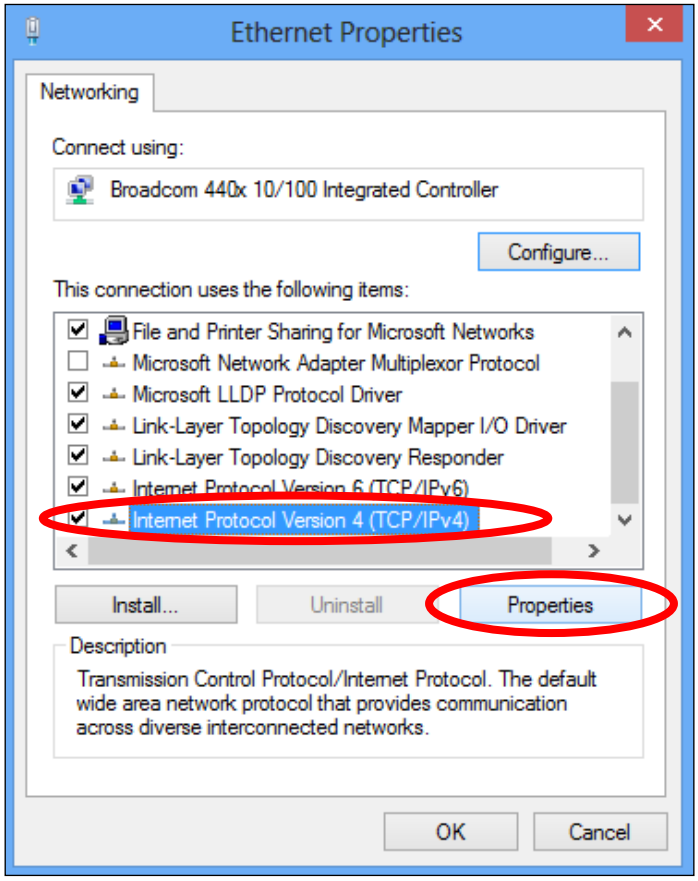
4. In the window that opens, select “Change adapter settings” from the left side.



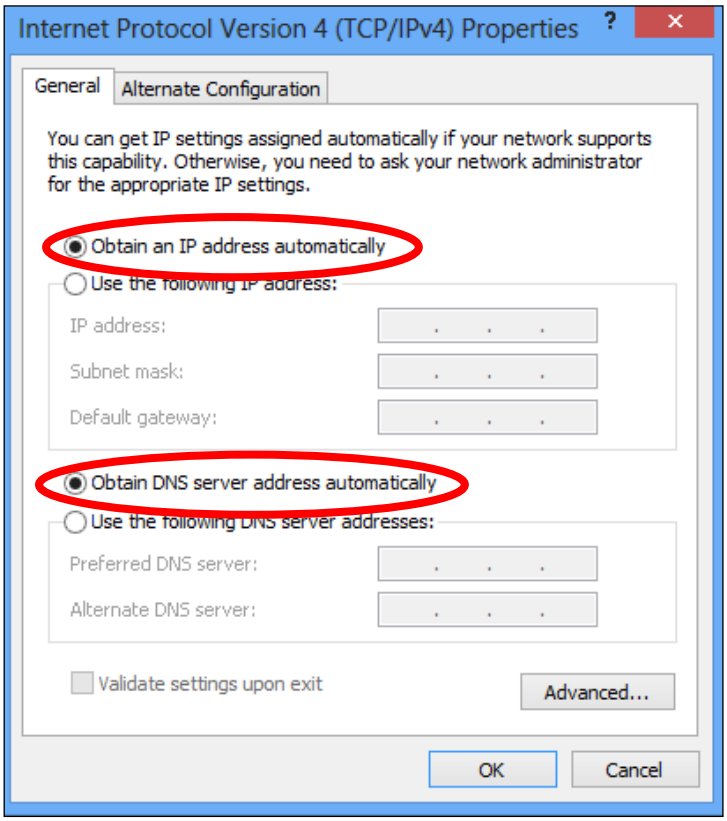
5. Choose your connection and right click, then select “Properties”.



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



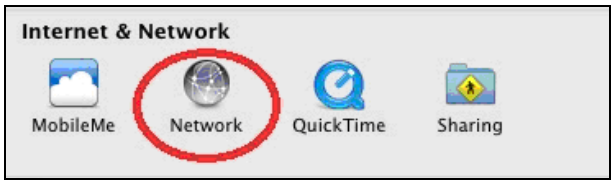
7. “Obtain an IP address automatically” and “Obtain DNS server address automatically” should be selected.



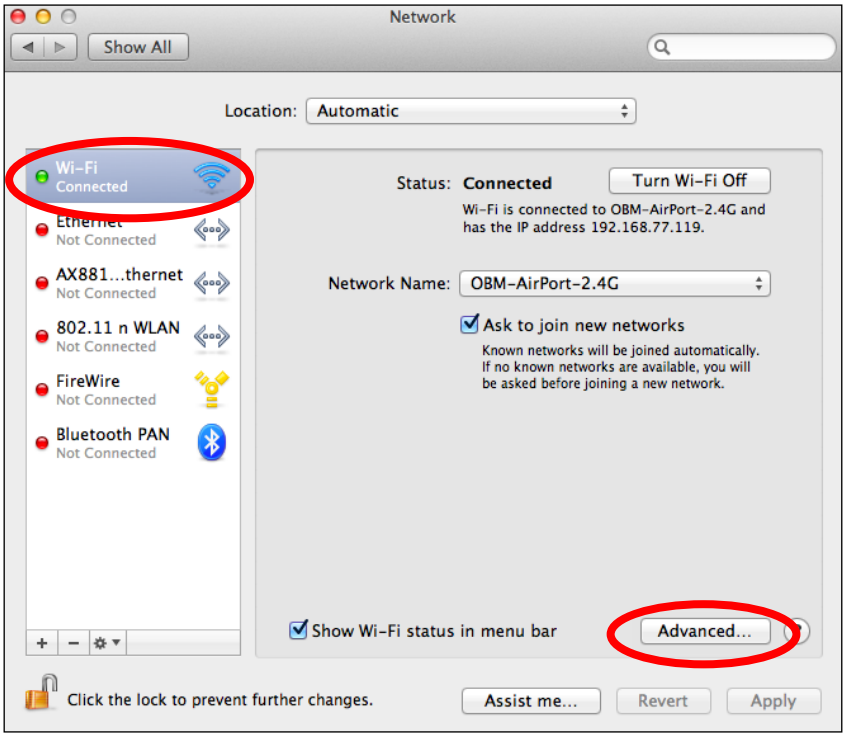
IV-2-5 Mac OS

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

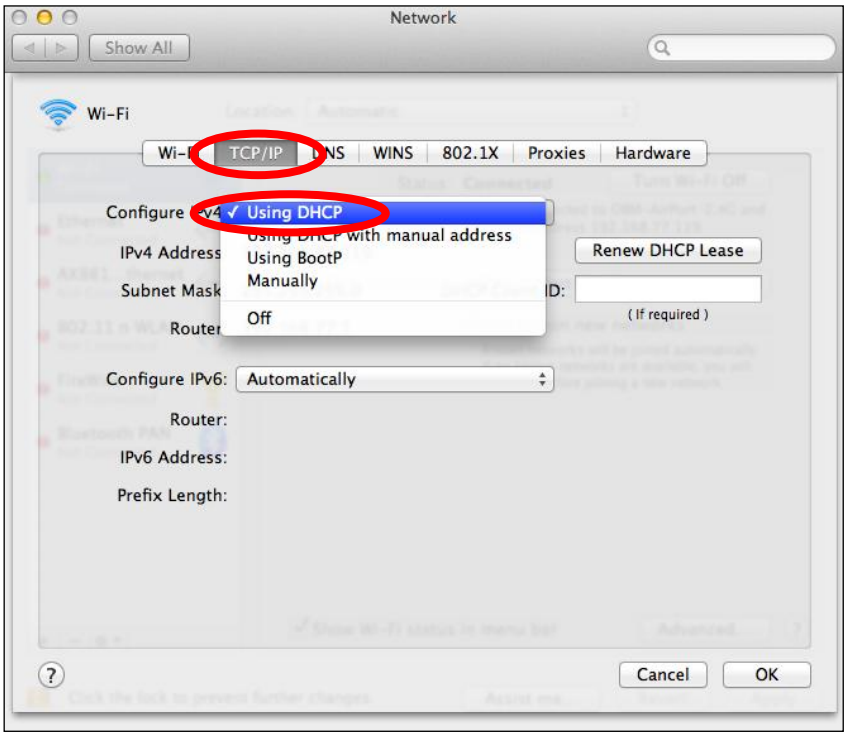
2. In System Preferences, click on “Network”.



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 “Using DHCP” in the “Configure IPv4” drop down menu.



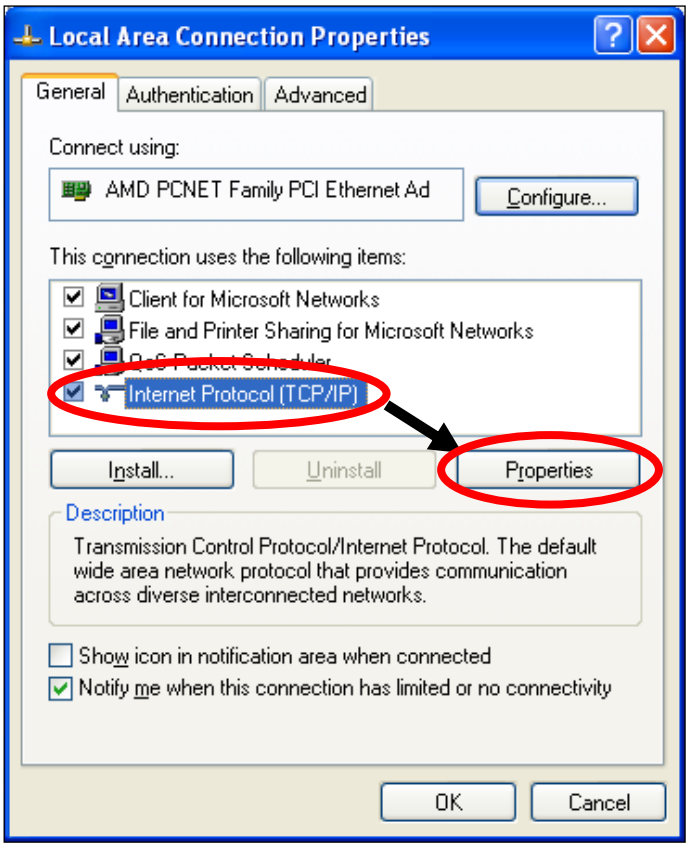
IV-3 How to modify the IP address of your computer

Please follow the instructions appropriate for your operating system. In the following examples we use the IP address **192.168.9.20** though you can use any IP address in the range **192.168.9.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-3-1 Windows XP

3. Click the "Start" button (it should be located in the lower-left corner of your computer) → "Control Panel" → "Network and Internet Connections" → "Network Connections" → "Local Area Connection" → "Internet Protocol (TCP/IP" → "Properties".

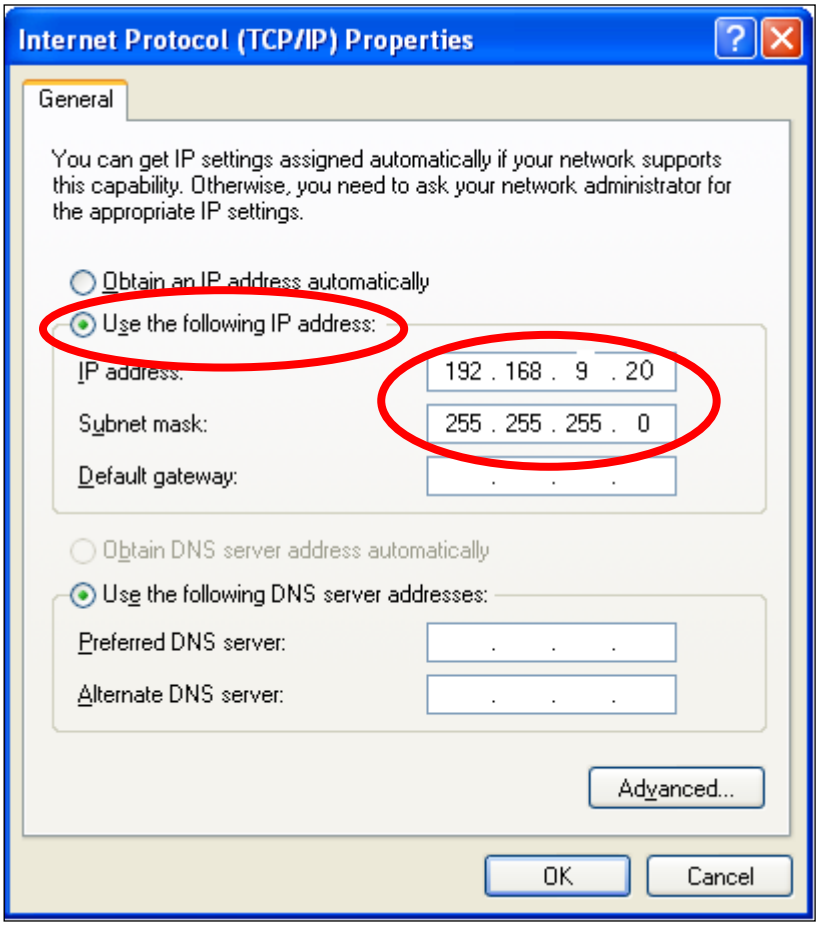


4. Select “Use the following IP address”, then input the following values:

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.

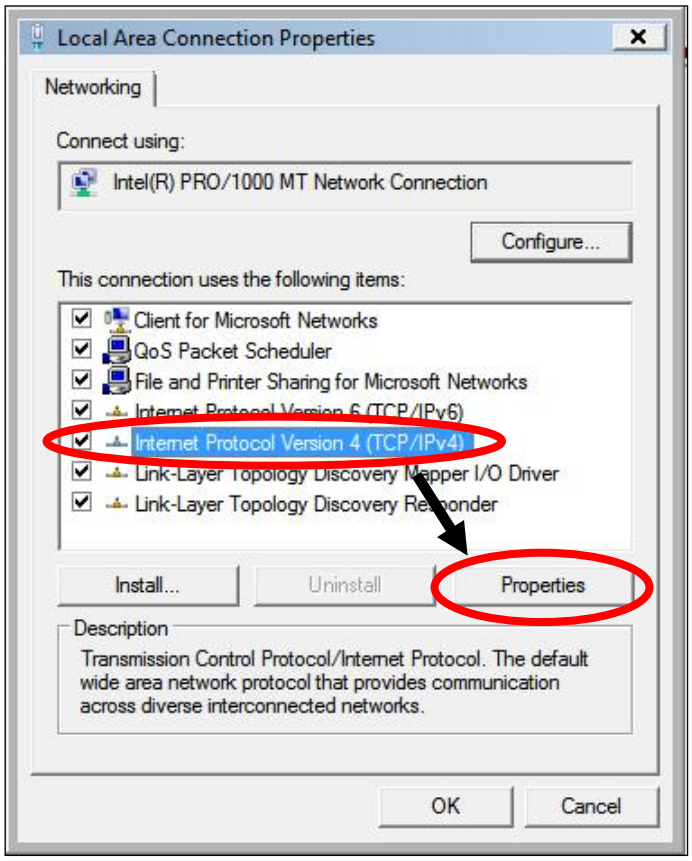
IP address: 192.168.9.20
Subnet Mask: 255.255.255.0

Click “OK” when finished.



IV-3-2 Windows Vista

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

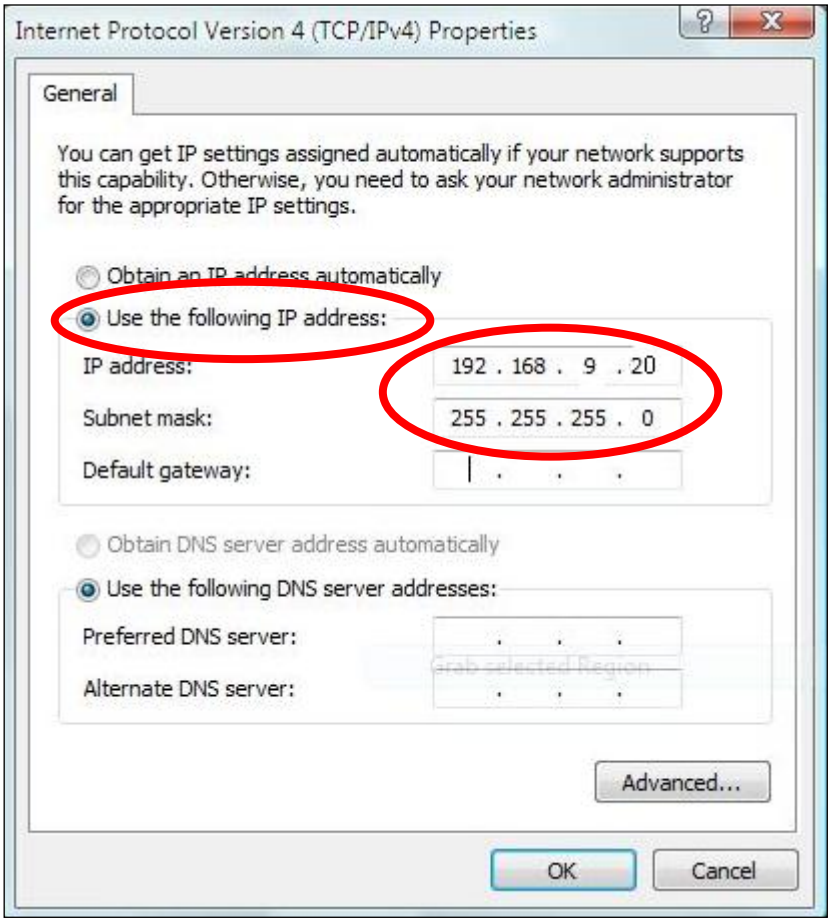


2. Select “Use the following IP address”, then input the following values:

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.

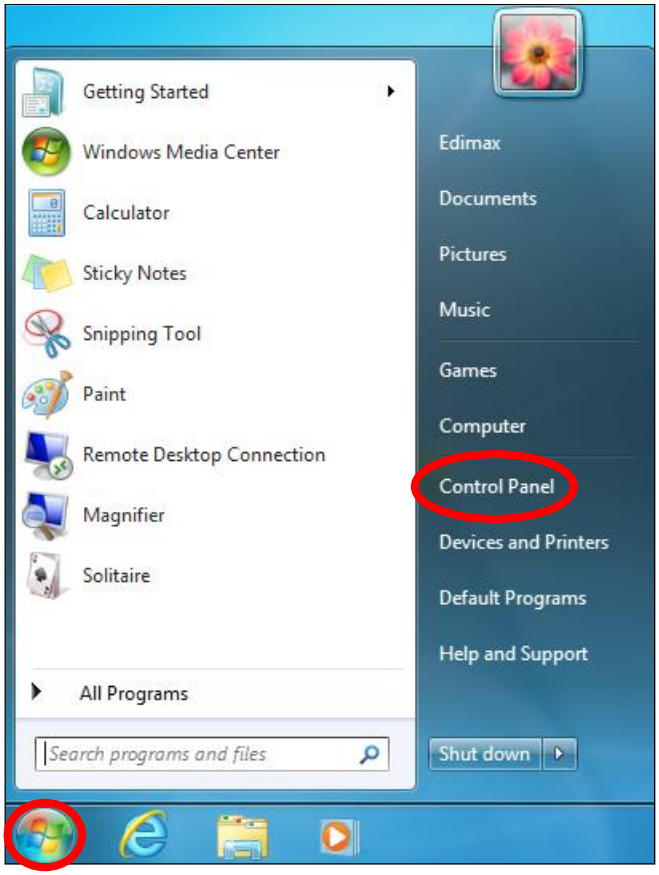
IP address: 192.168.9.20
Subnet Mask: 255.255.255.0

Click “OK” when finished.

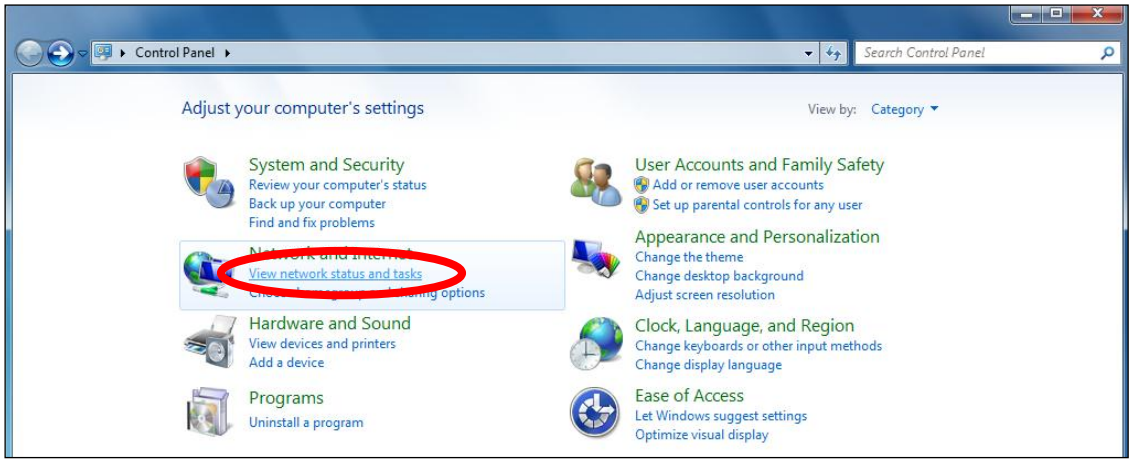


IV-3-3 Windows 7

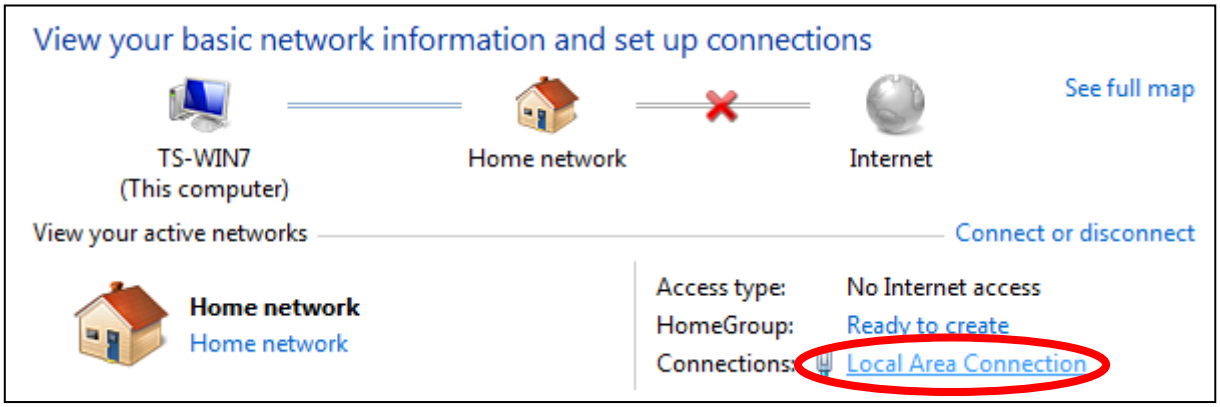
1. Click the “Start” button (it should be located in the lower-left corner of your computer) → “Control Panel”.



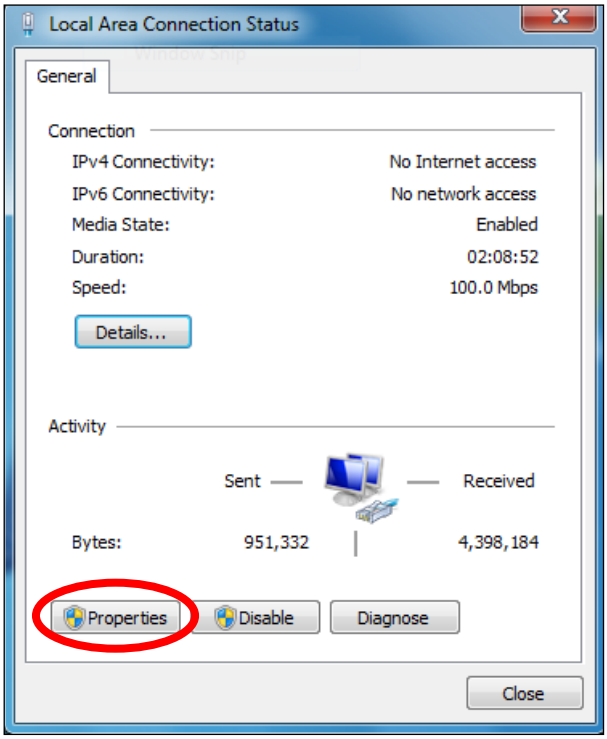
2. Under “Network and Internet” click “View network status and tasks”.



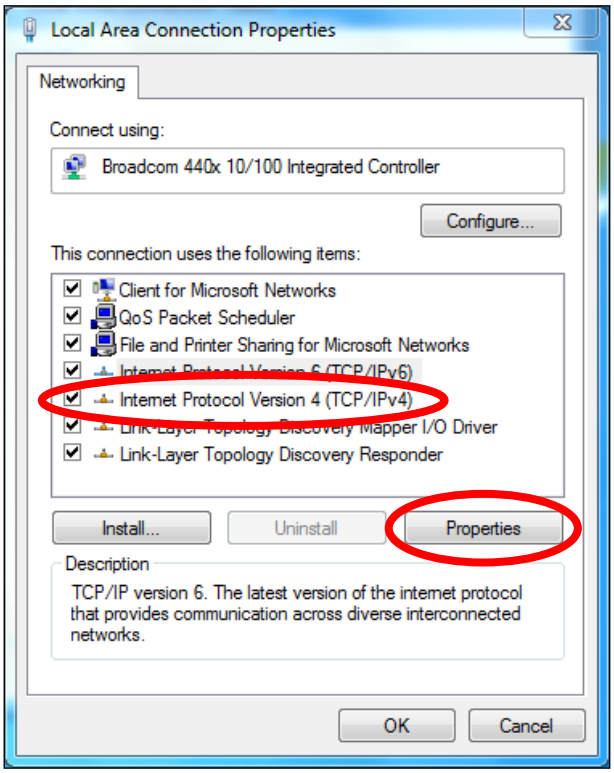
3. Click “Local Area Connection”.



4. Click “Properties”.



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

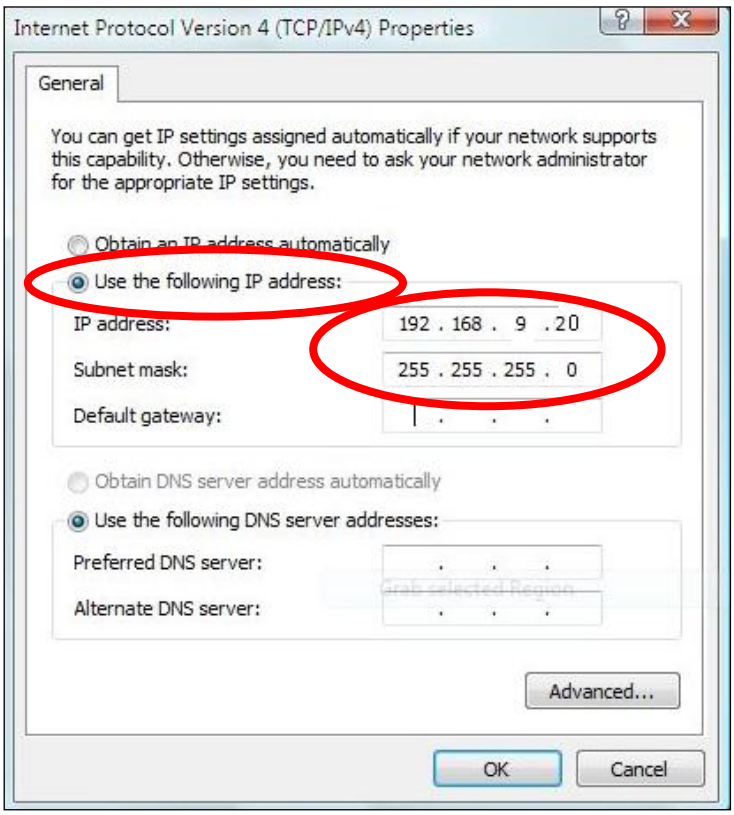


6. Select “Use the following IP address”, then input the following values:

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.

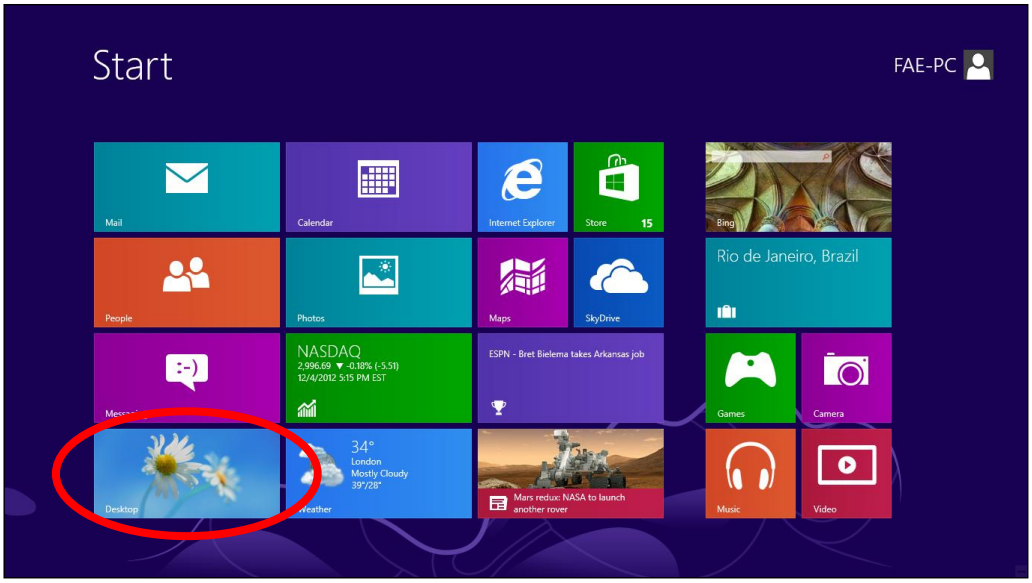
IP address: 192.168.9.20
Subnet Mask: 255.255.255.0

Click “OK” when finished.

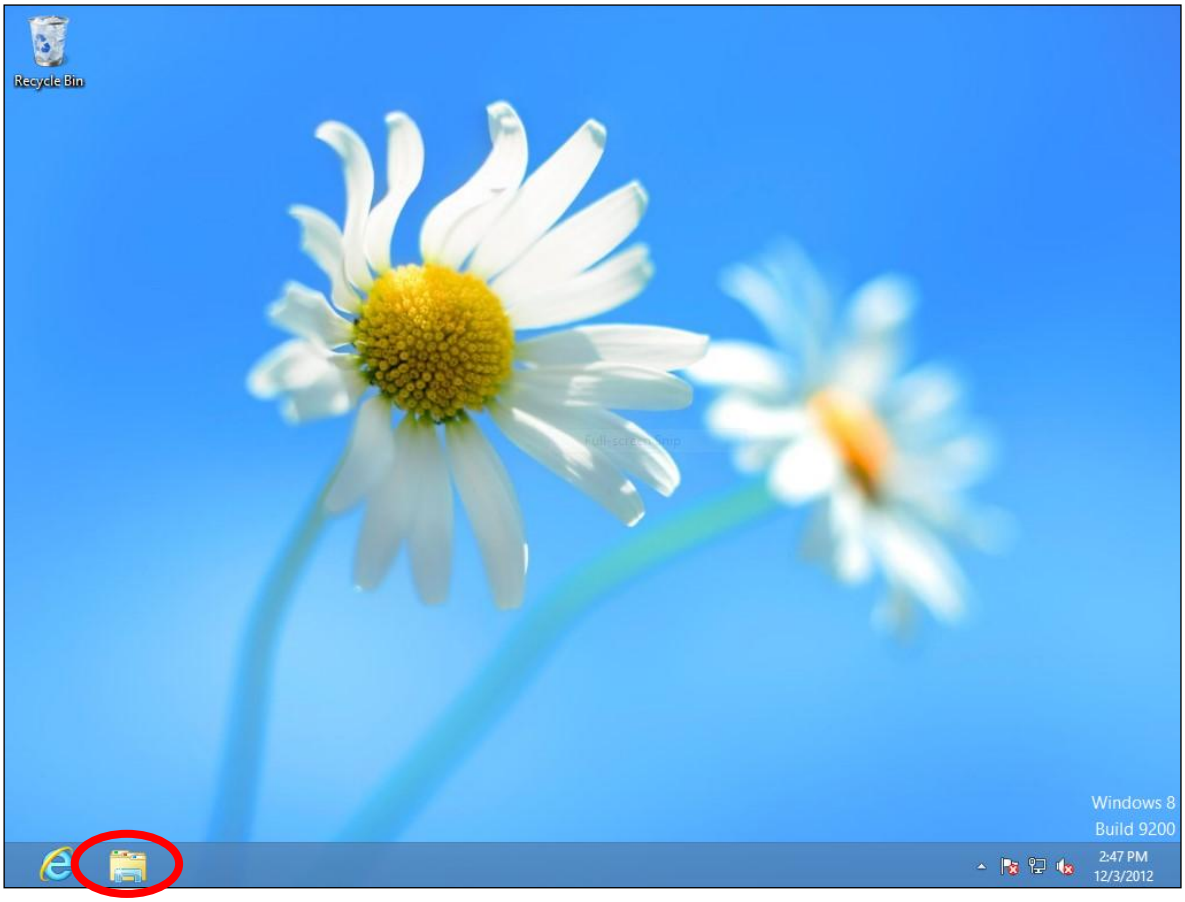


IV-3-4 Windows 8

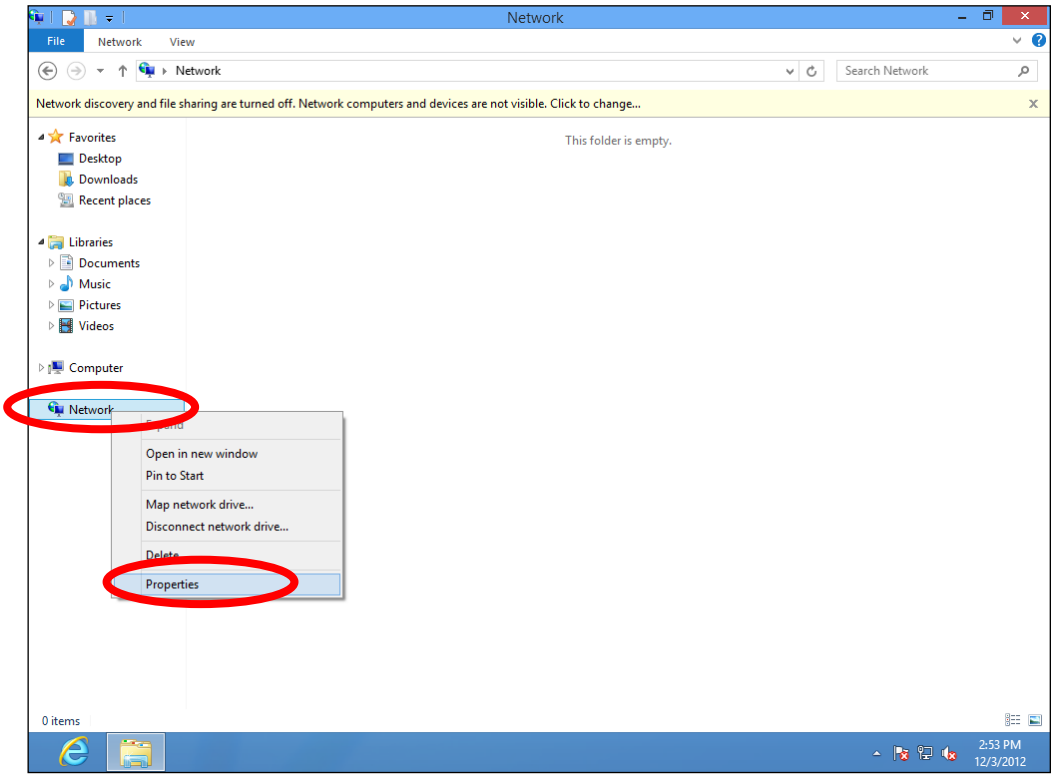
1. From the Windows 8 Start screen, switch to desktop mode by clicking the “Desktop” icon.



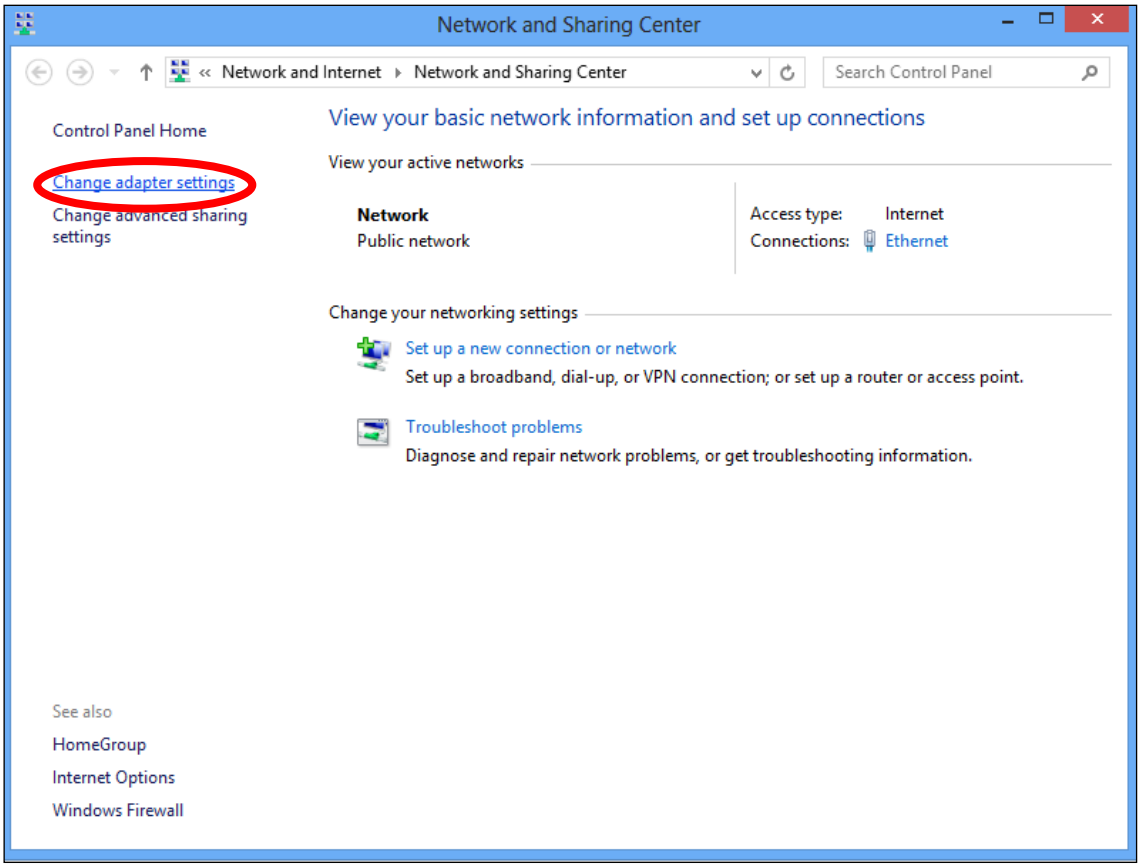
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



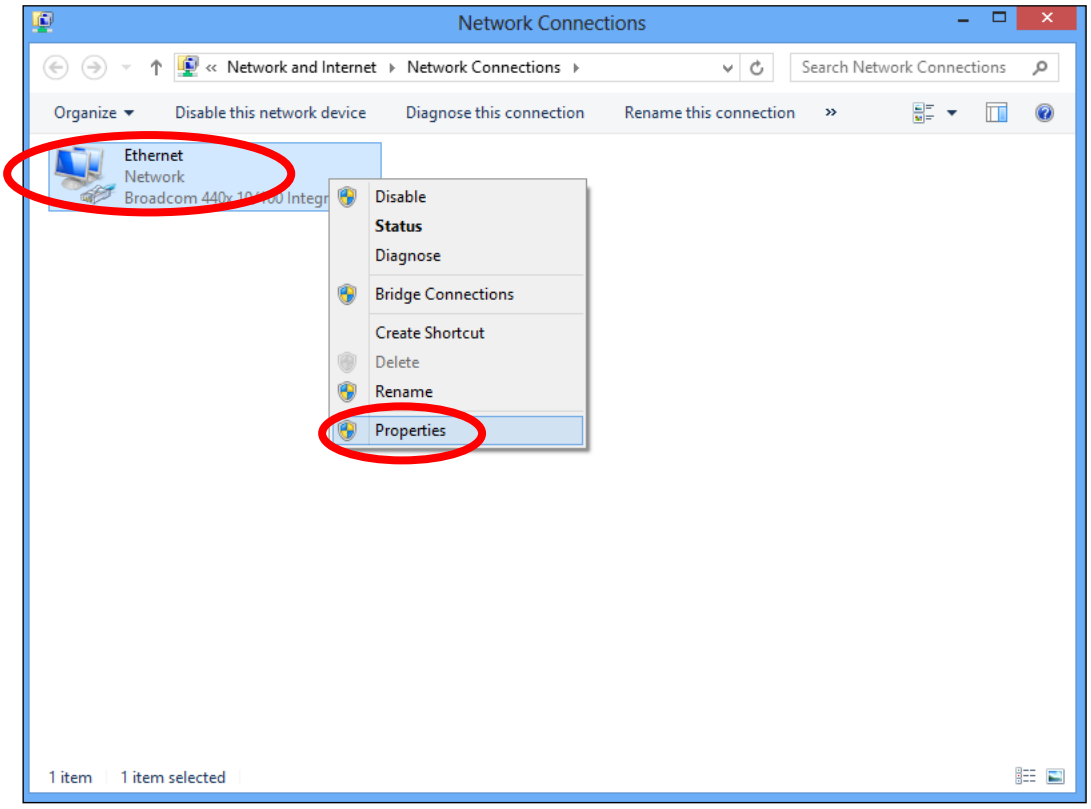
3. Right click “Network” and select “Properties”.



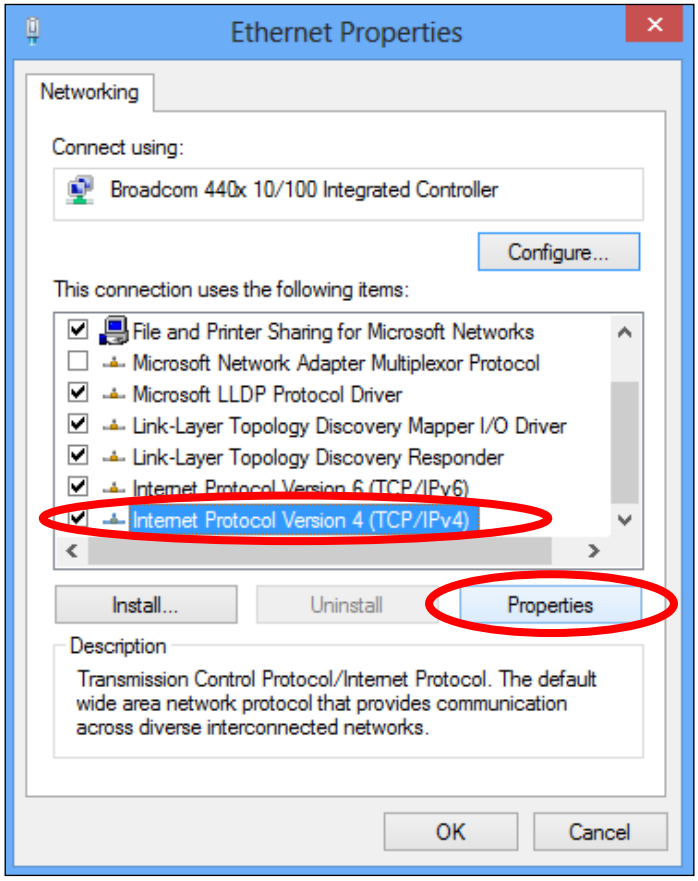
4. In the window that opens, select “Change adapter settings” from the left side.



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



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

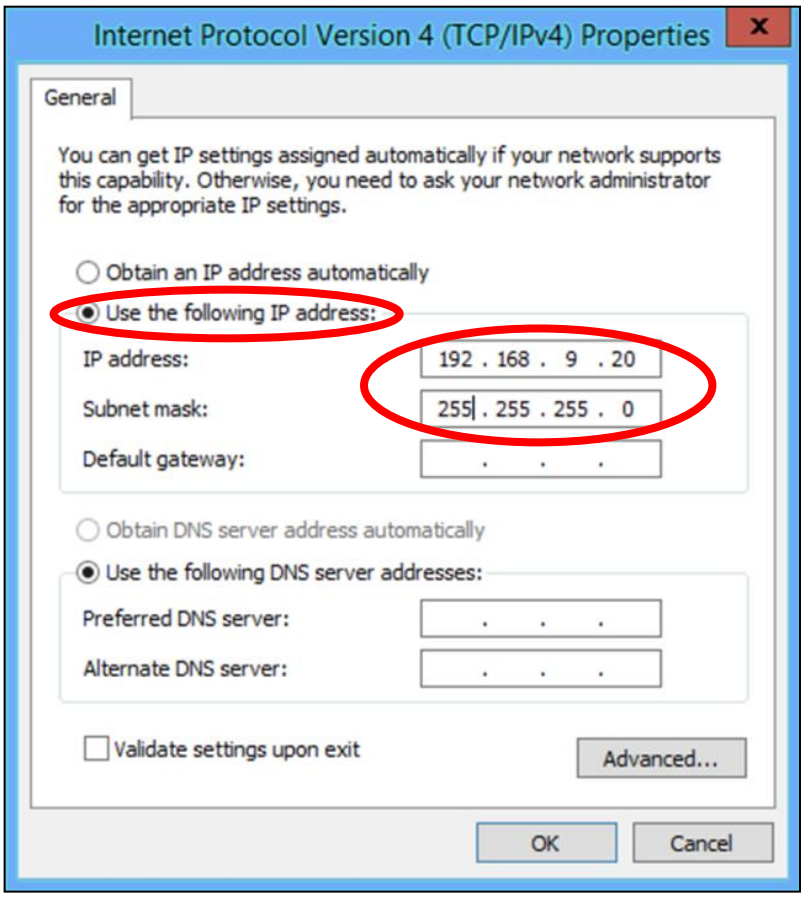


7. Select “Use the following IP address”, then input the following values:

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: 192.168.9.20
Subnet Mask: 255.255.255.0

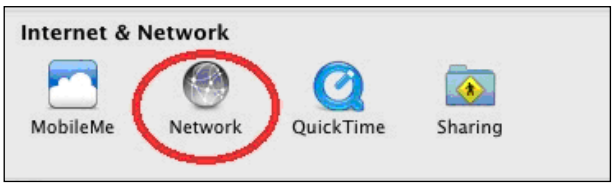
Click “OK” when finished.



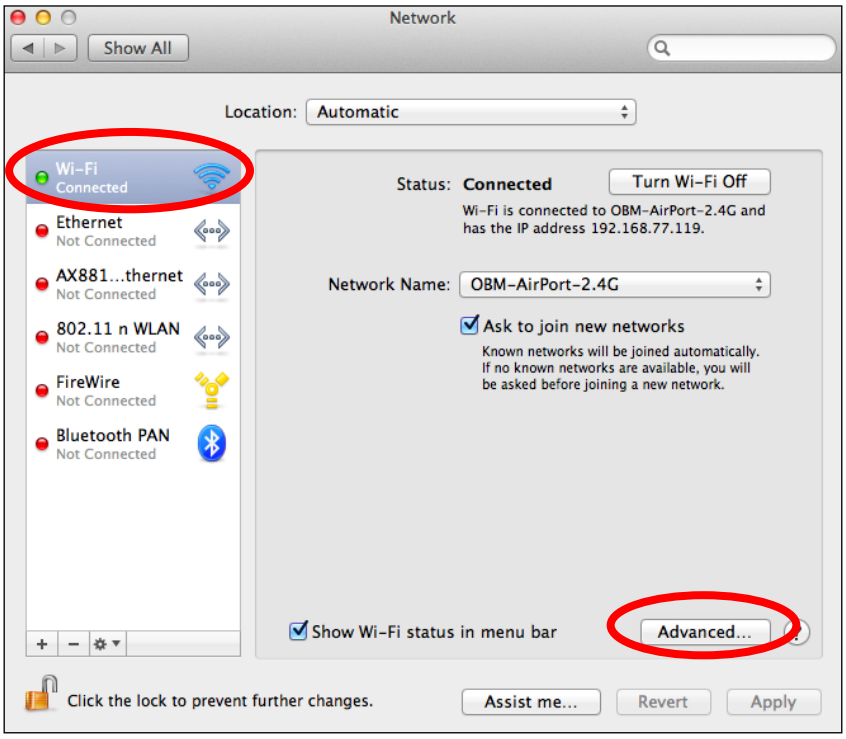
IV-3-5 Mac OS

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

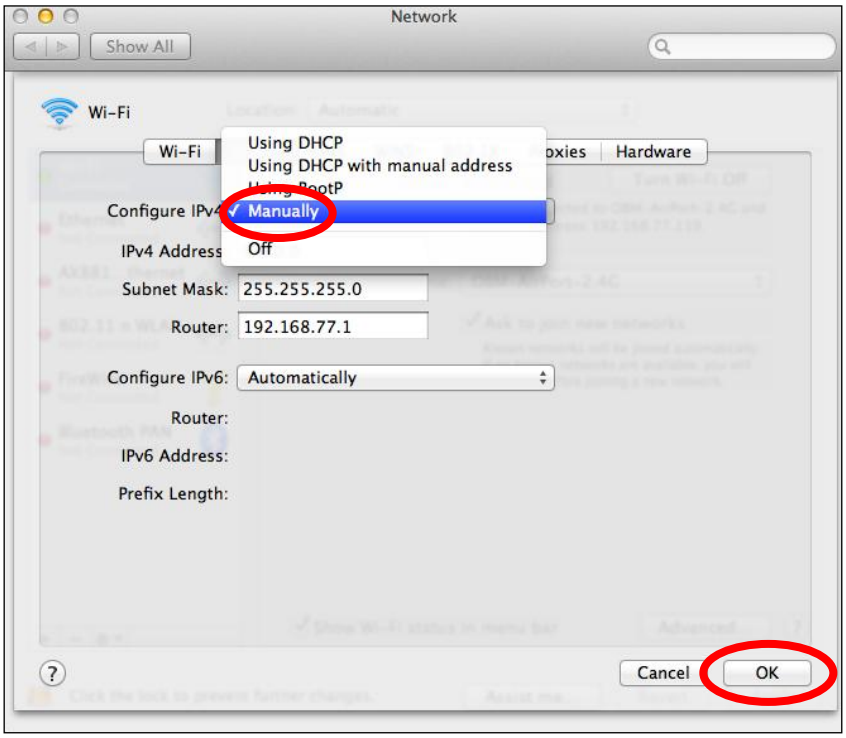
2. In System Preferences, click on “Network”.



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

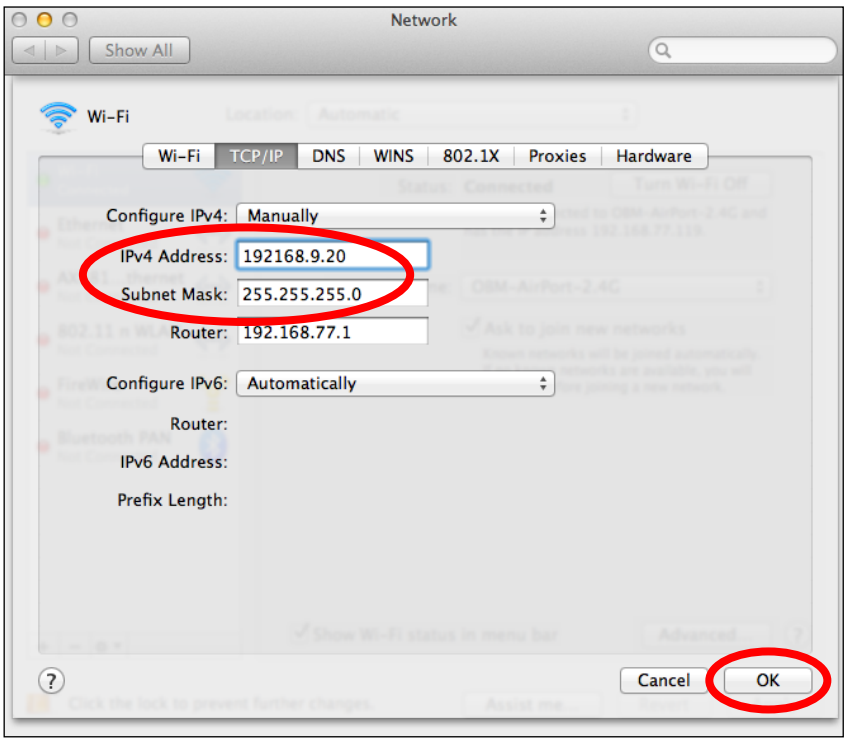


4. Select “TCP/IP” from the top menu, select “Manually” from the “Configure IPv4” drop down menu and click “OK”.

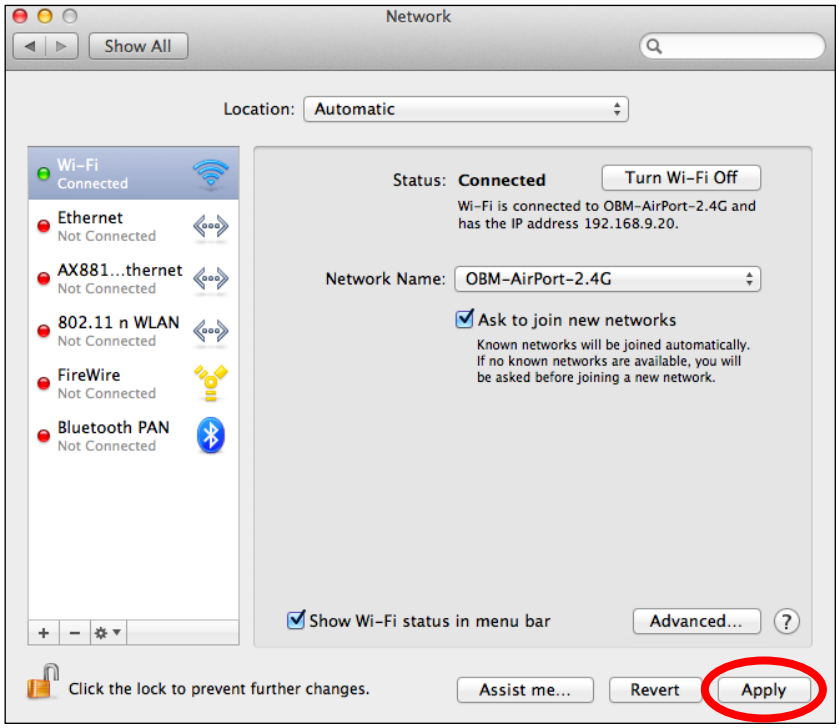


Your existing static IP address will be displayed in the “IP address” field before you replace it. Please make a note of this IP address, subnet mask, default gateway and DNS server addresses.

5. In the “IPv4 Address” and “Subnet Mask” fields, respectively enter IP address 192.168.9.20 and subnet mask 255.255.255.0.
Click “OK”.



6. Click “Apply” to save the changes.



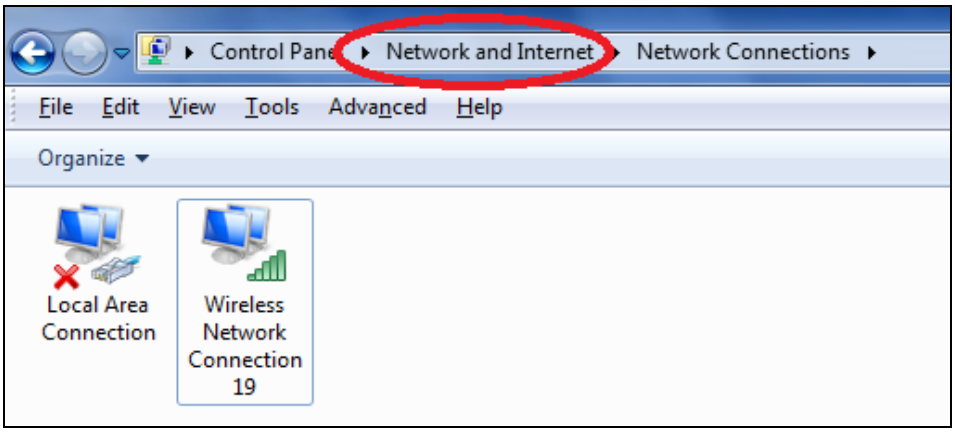
IV-4 How to Find Your Network Security Key

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

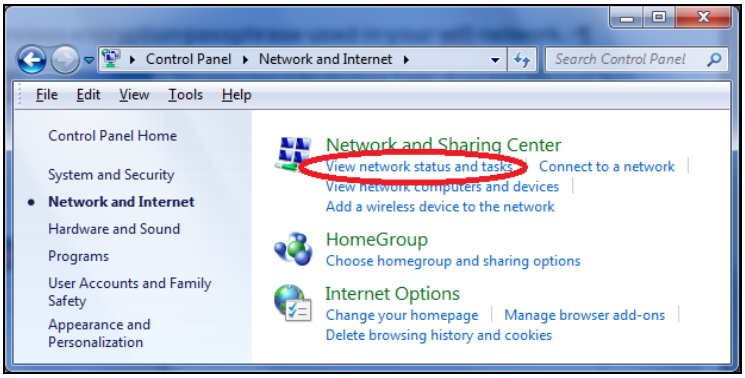
If you are using Windows XP or earlier, please contact your ISP or router manufacturer to find your network security key.

IV-4-1 Windows 7 & Vista

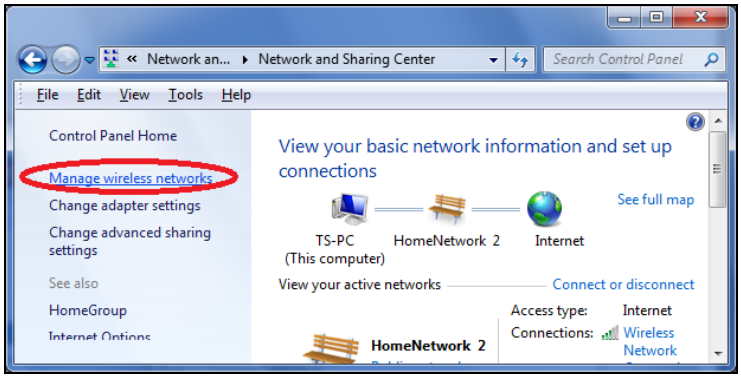
1. Open “Control Panel” and click on “Network and Internet” in the top menu.



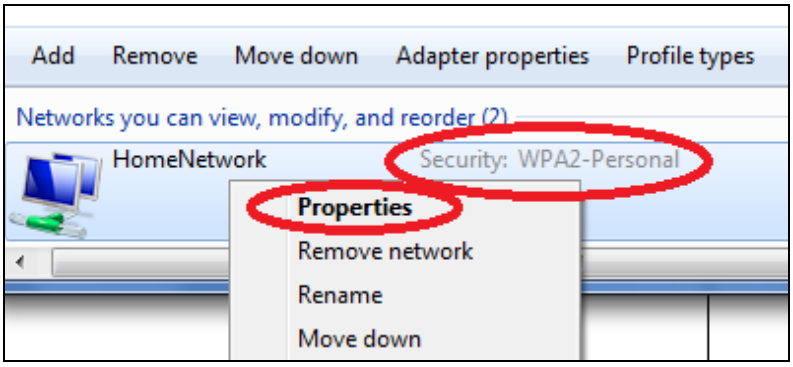
2. Click on “View network status and tasks” which is under the heading “Network and Sharing Center”.



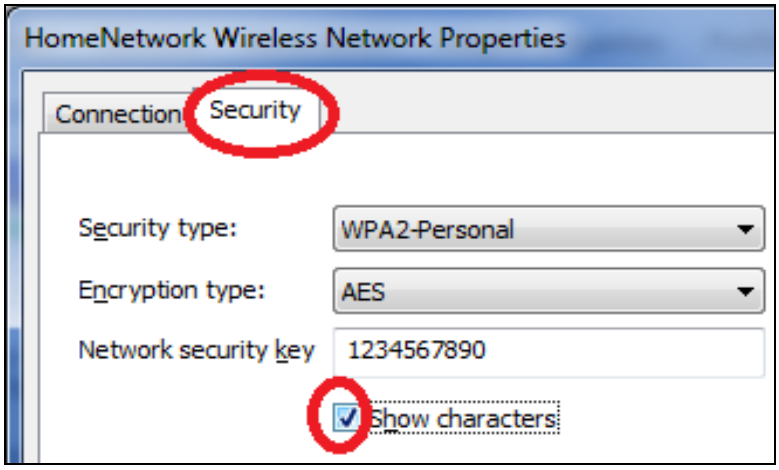
3. Click on “Manage wireless networks” in the left menu.



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

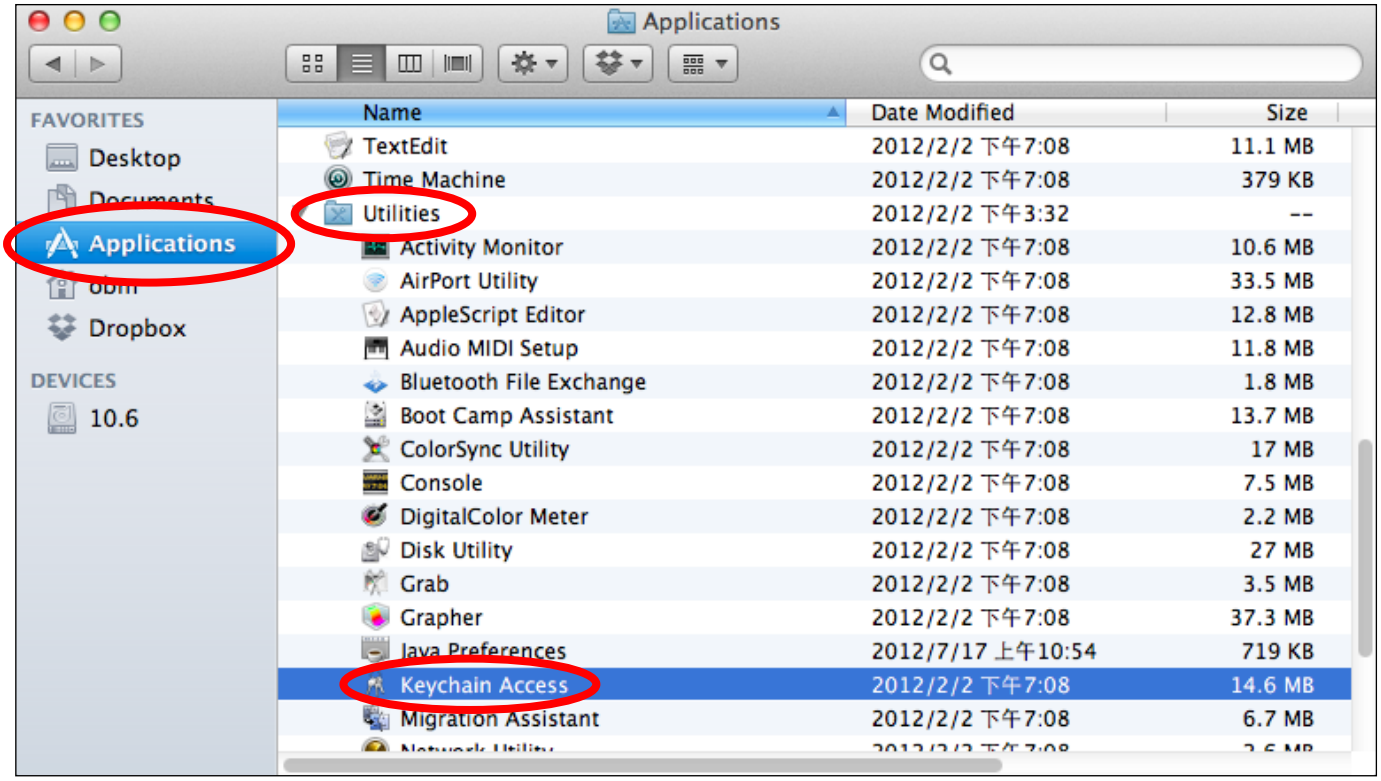


5. Click on the “Security” tab, and then check the box labeled “Show characters”. This will show your network security key. Click the “Cancel” button to close the window.

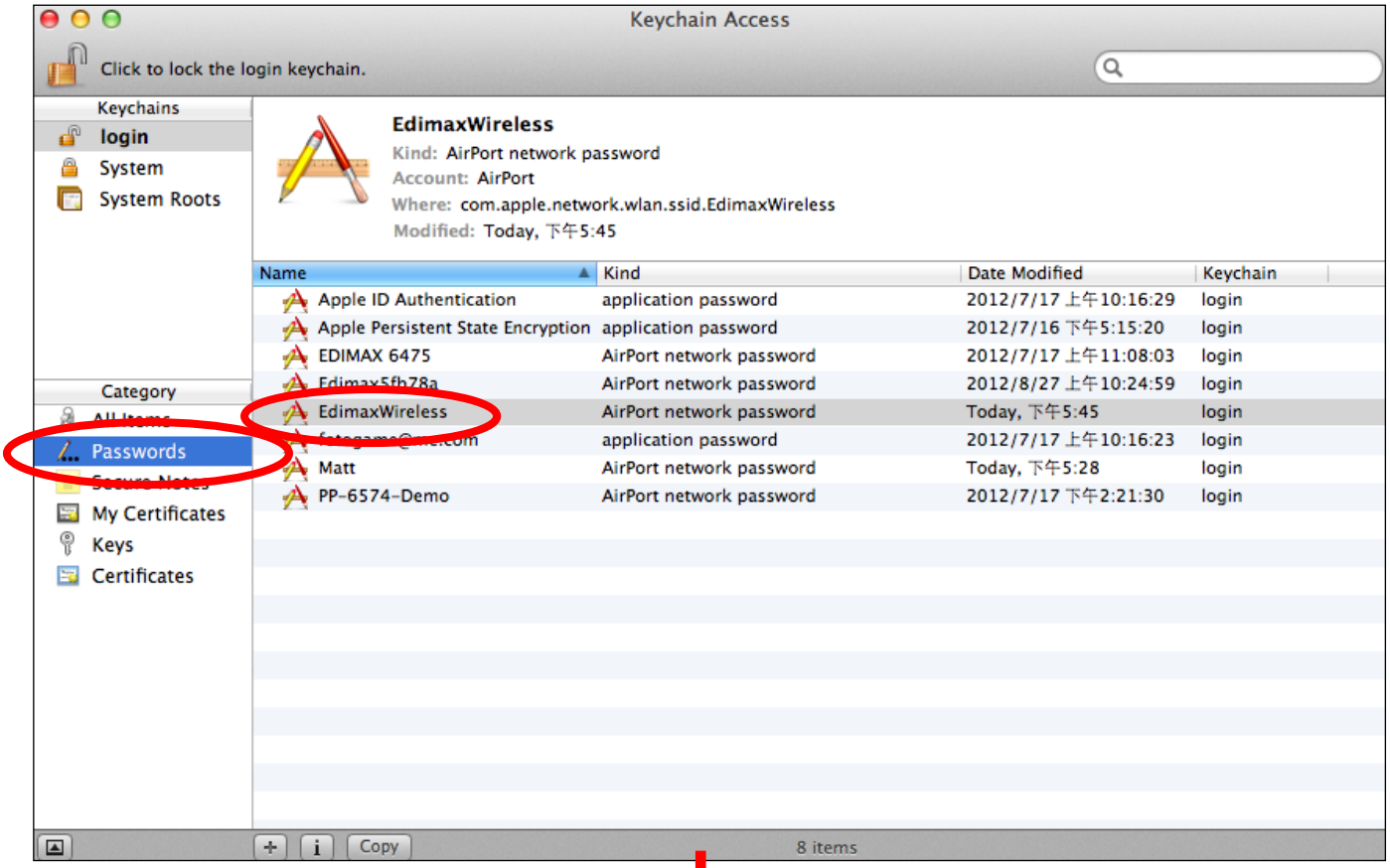


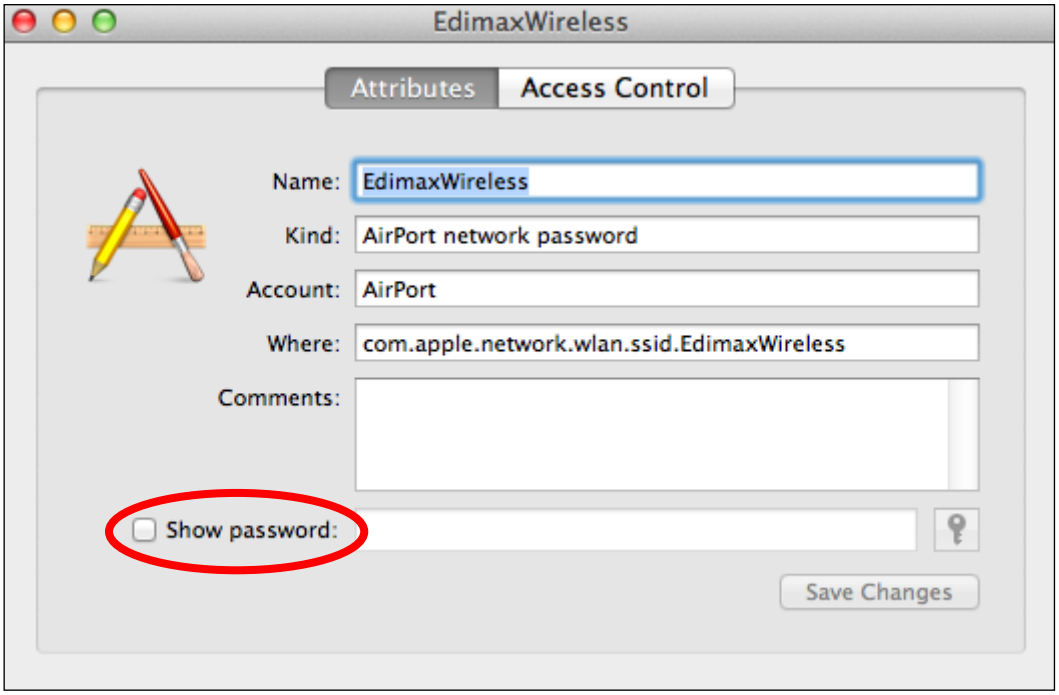
IV-4-2 Mac

1. Open a new Finder window, and select “Applications” → “Utilities” → “Keychain Access”.

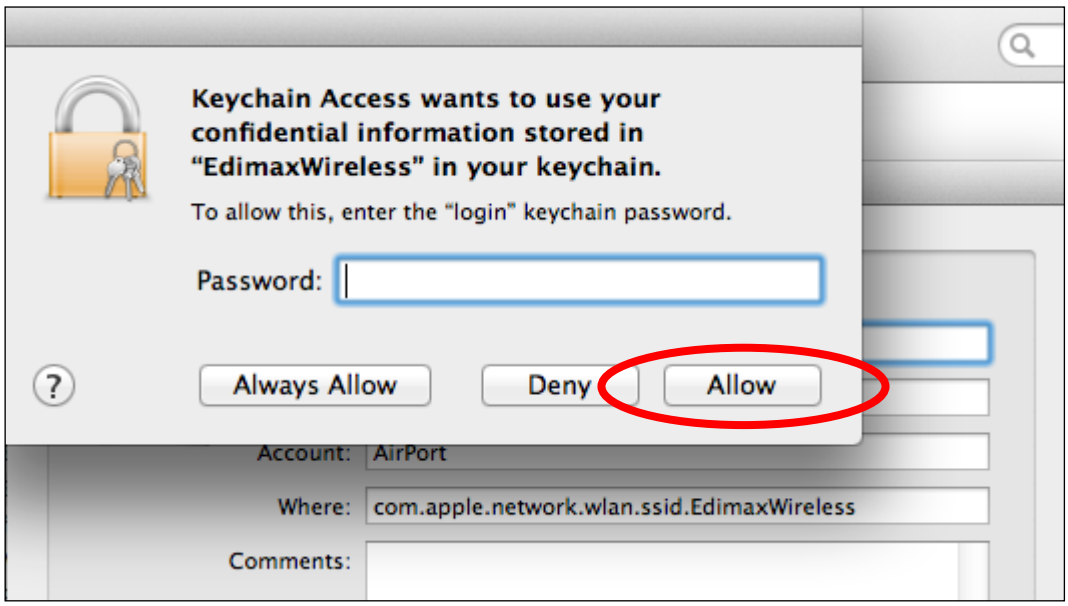


2. Select “Passwords” from the “Category” sub-menu on the left side. Search the list in the main panel for the SSID of your network. In this example, the SSID is “EdimaxWireless” – though your SSID will be unique to your network.
Double click the SSID of your network.





3. 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”.



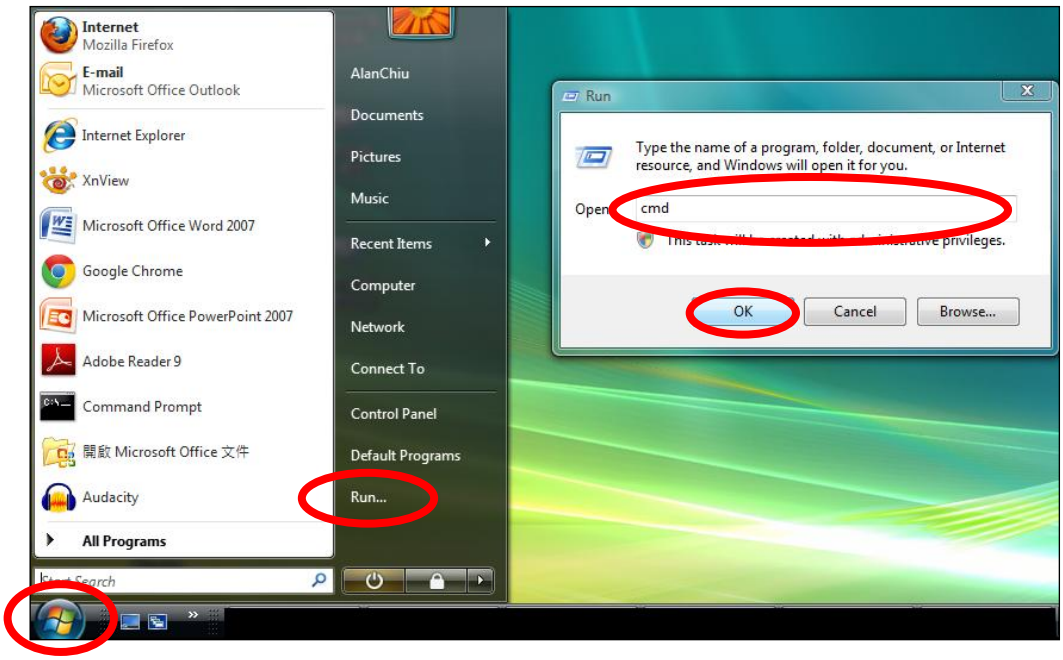
Your network security password will now be displayed in the field next to the box labeled “Show password”. In the example below, the network security password is “edimax1234”. Please make a note of your network security password.

IV-5 How to Find Your Router's IP Address

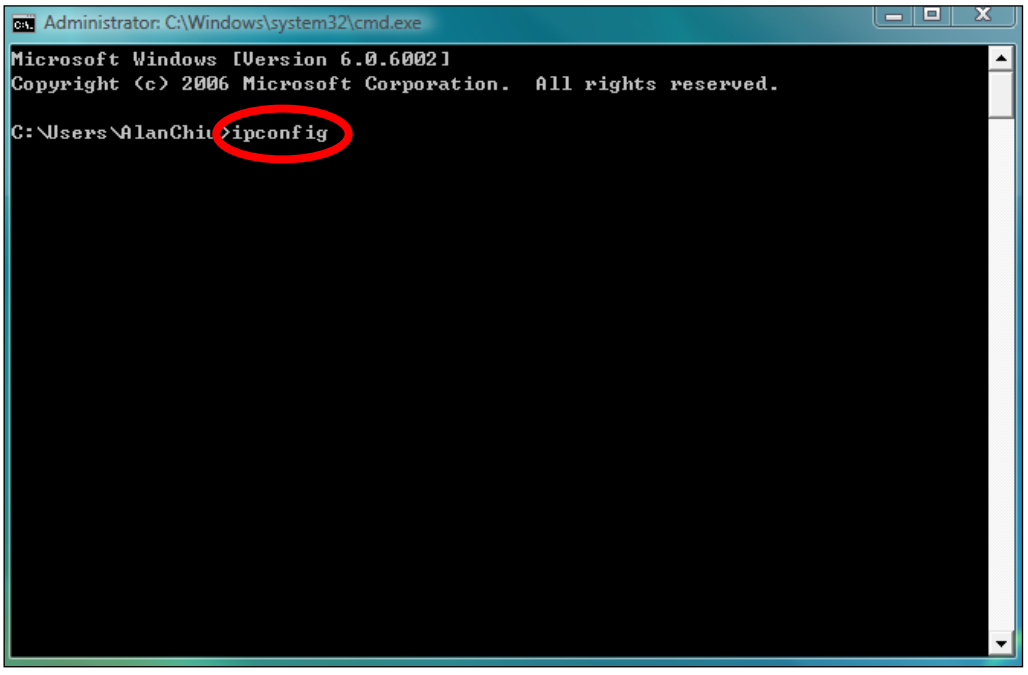
To find your router's IP address, please follow the instructions appropriate for your operating system.

IV-5-1 Windows XP, Vista & 7

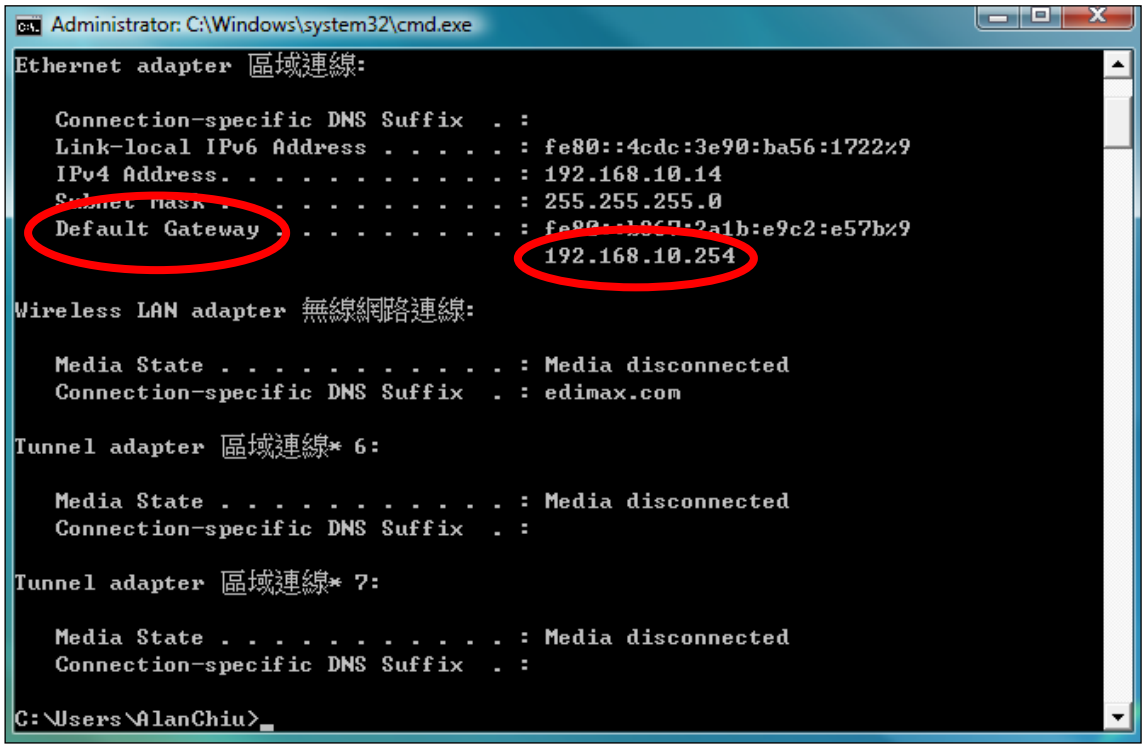
1. Go to "Start" → "Run" and type "cmd", then press Enter or click "OK".



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



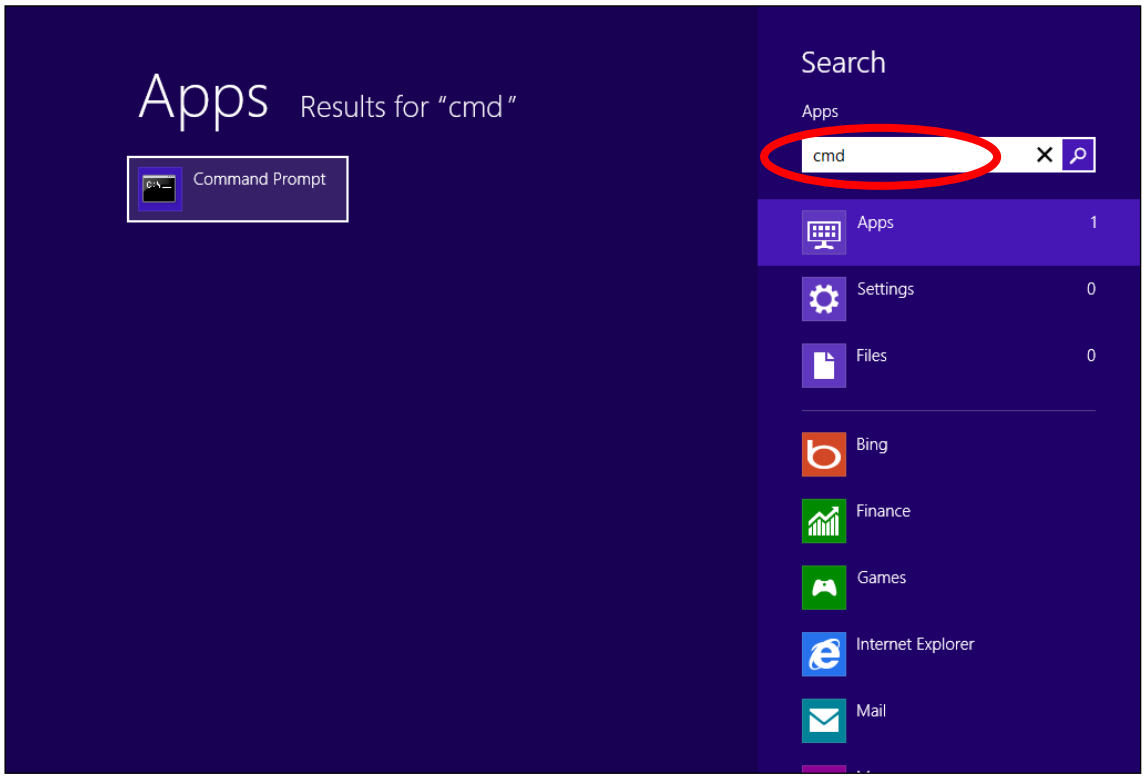
3. Your router's IP address will be displayed next to "Default Gateway".



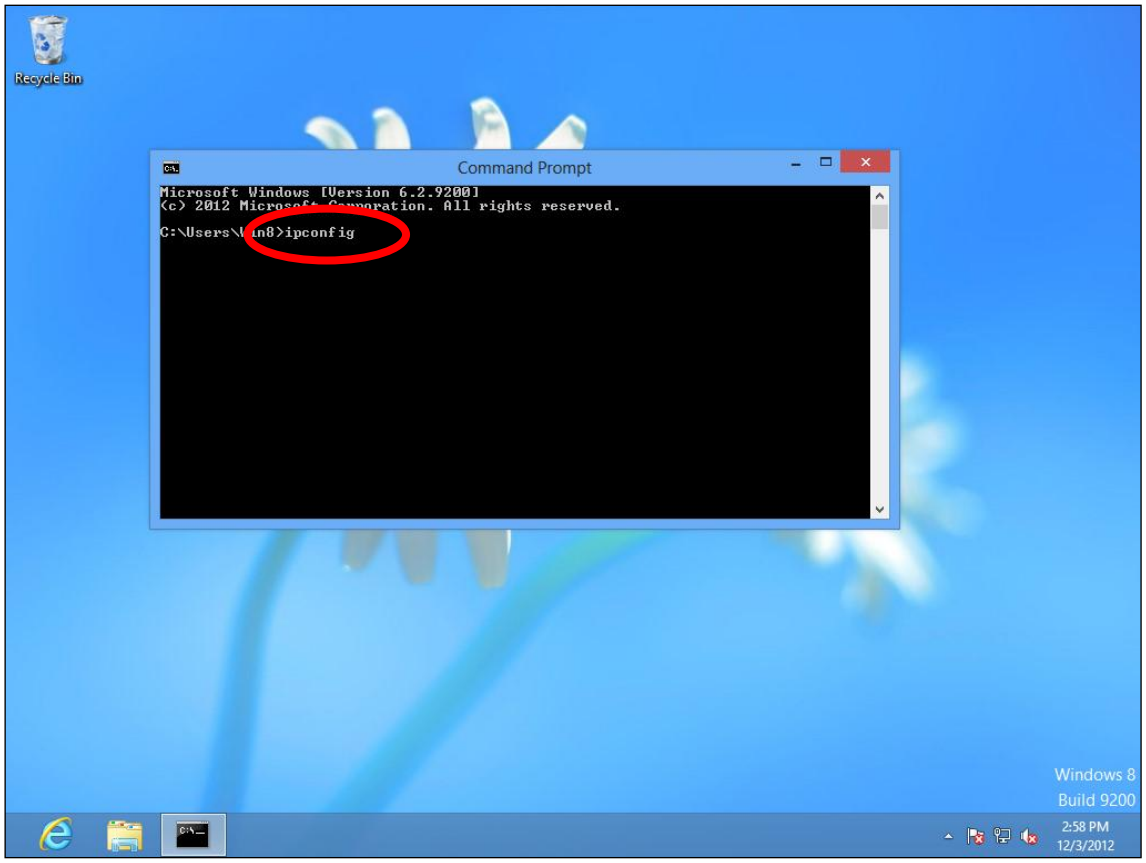
IV-5-2 Windows 8

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

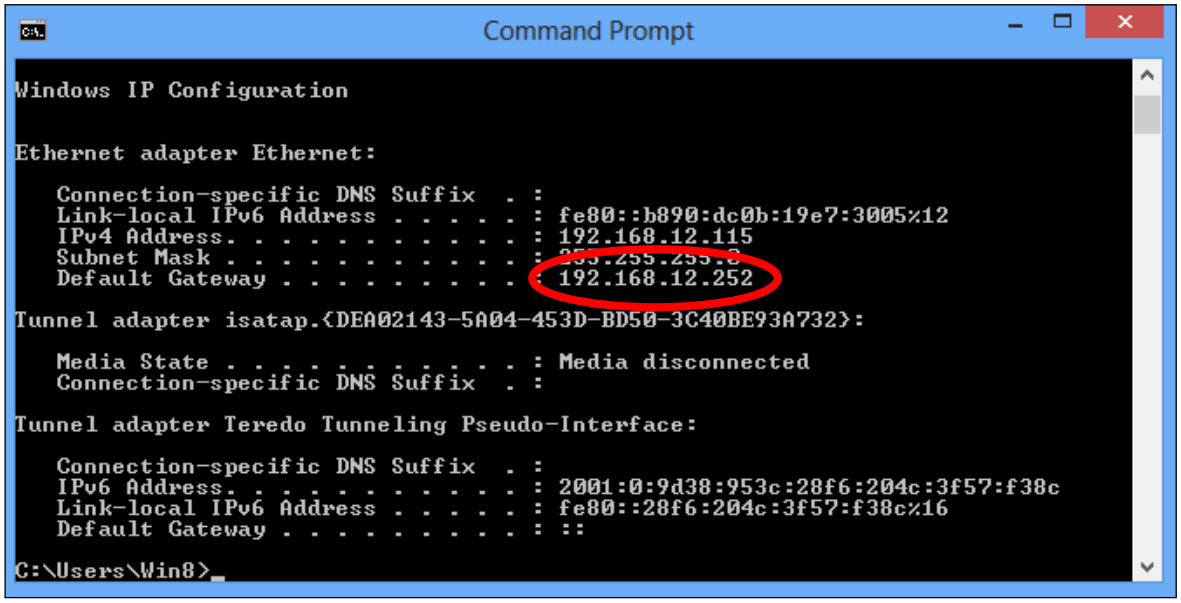
2. Click “Search” and enter “cmd” into the search bar. Click the “Command Prompt” app which be displayed on the left side.



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



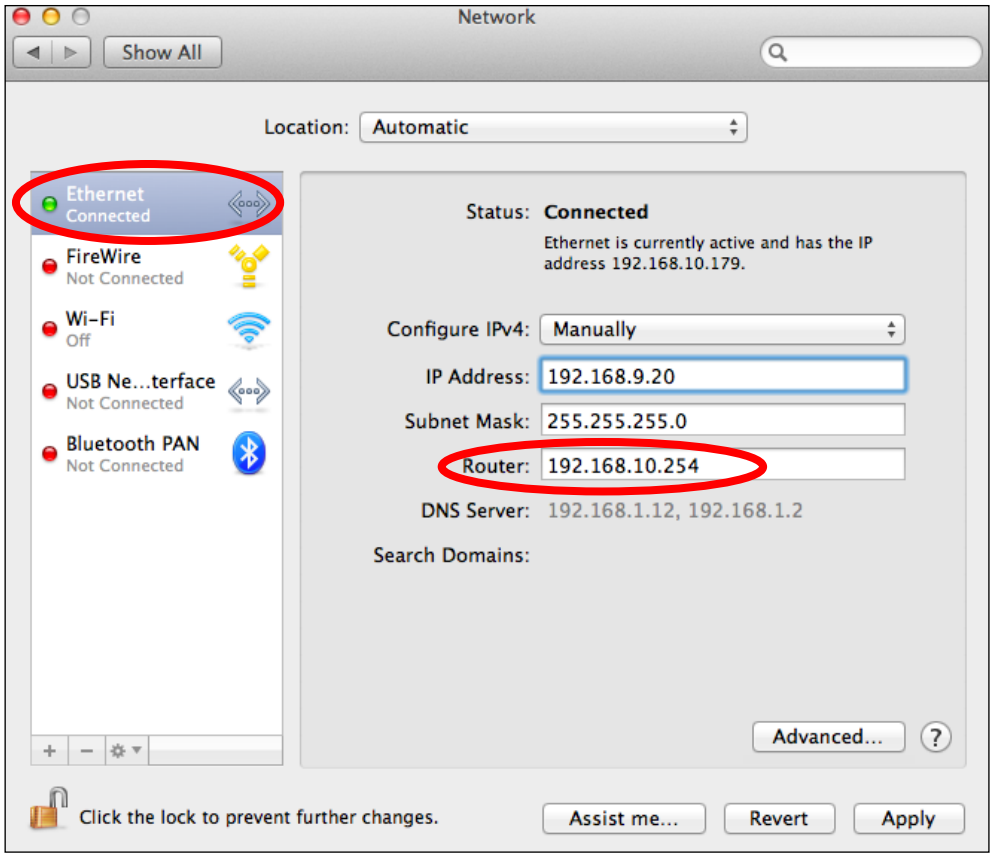
4. Your router's IP address will be displayed next to "Default Gateway".



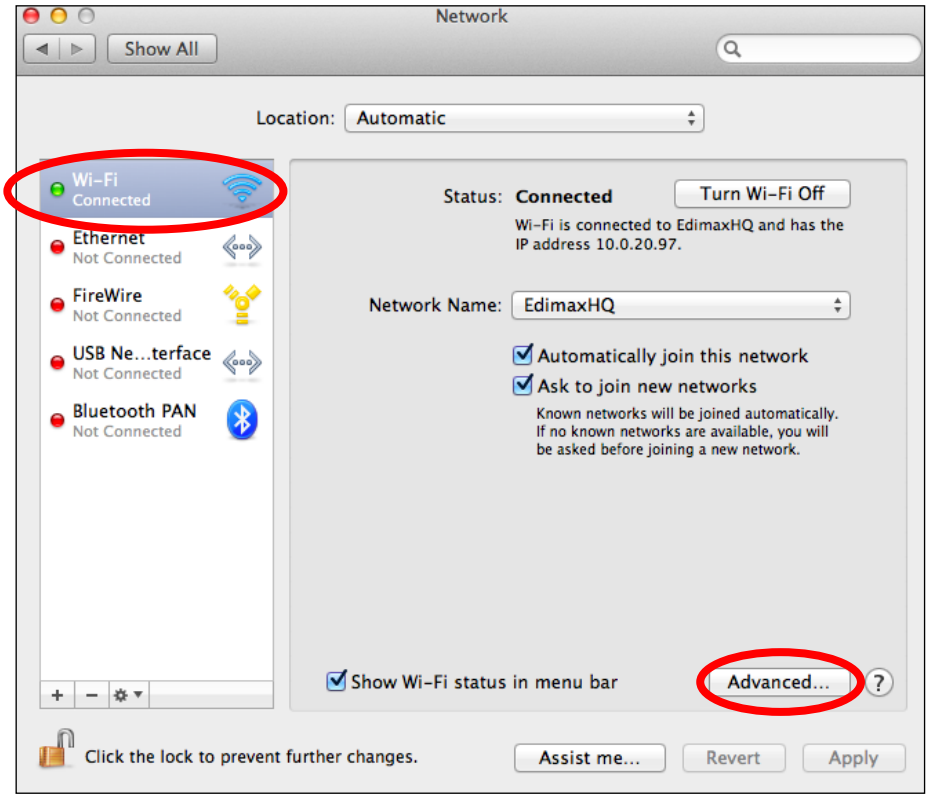
IV-5-3 Mac

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

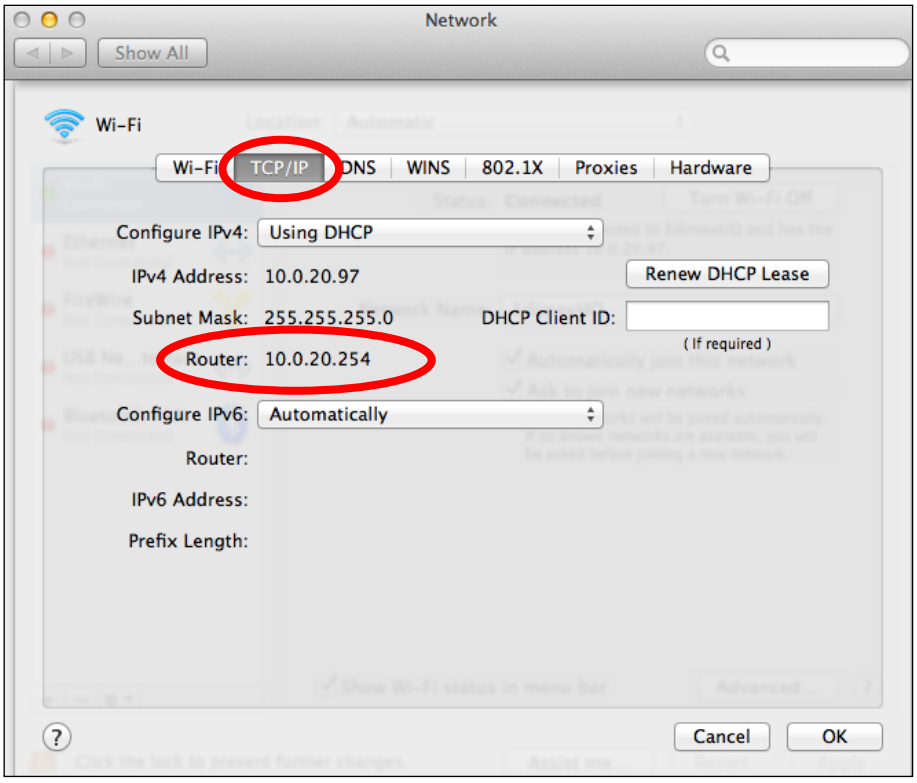
2. If you are using an Ethernet cable to connect to your network, your router’s IP address will be displayed next to “Router”.



3. If you are using Wi-Fi, click “Wi-Fi” → “Advanced”.



4. Click the “TCP/IP” tab and your router’s IP address will be displayed next to “Router”.

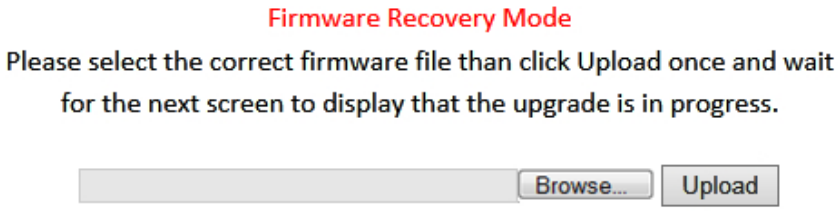


IV-6 Troubleshooting

If you are experiencing problems with your wireless extender, please refer to this troubleshooting guide before contacting your dealer of purchase for help.

Scenario	Solution
I can't log onto the browser-based configuration interface.	a. Please check that the extender is correctly inserted into a power socket and check the LEDs on the front panel. If the extender is initializing after being switched off or restarted, wait for a 2 minutes and try again. b. Make sure you are using the full, correct URL: **http://edimax.setup** c. If you are using a MAC or IP address filter, try to connect the wireless extender using a different computer. d. Set your computer to "Obtain an IP address automatically" (DHCP), and see if your computer can obtain an IP address. e. Make sure that all other Wi-Fi / Ethernet adapters are disabled or disconnected. f. Password is case-sensitive. Make sure you are not caps locked ("Caps Lock" light is not illuminated). g. If you do not know your password, restore the device to factory settings.
I can't establish a connection to my wireless extender.	a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client. The password is case-sensitive. Make sure you are not caps locked ("Caps Lock" light is not illuminated). b. Try moving closer to the wireless extender. c. Power off the extender (remove from plug) and power back on after 10 seconds (plug in the device). d. Please check that the extender is correctly inserted into a power socket and check the LEDs.

Files are downloading very slowly or the downloads are frequently interrupted.	a. Restart the wireless extender b. Try again later. Your local network may be experiencing technical difficulties or very high usage. c. Change channel number.
The wireless extender is extremely hot.	a. It is normal for the wireless extender to heat up during frequent use. If you can safely place your hand on the wireless extender, the temperature of the device is at a normal level. b. If you smell burning or see smoke coming from wireless extender, disconnect the extender immediately as far as it is safely possible to do so. Call your dealer of purchase for help.
My network device can't access the Internet.	a. Make sure that your broadband router is fully functional. b. Switch off both your network device and wireless extender and switch back on again. c. Make sure that the wireless extender is powered on (check the PWR LED). d. On the browser based configuration interface home page, check "Status" under "Wireless Configuration". It should be "Connected" – if "Disconnected" is shown, the wireless extender is not connected to your router/access point.
My wireless extender has a poor signal from my access point/router.	The best location to place the Wi-Fi extender is one which is an open space, roughly in the middle between your router and the Wi-Fi dead zone, and where the Wi-Fi extender LED displays "Excellent" signal strength. a. Keep the extender away from other radio devices such as microwaves or wireless telephones. b. Do not put the extender in the corner of a room or under/near metal. c. It is recommended to plug the extender directly into a wall socket. d. Make sure there are as few obstacles as possible between the extender and the access point/router.

Can I use the same SSID as my current gateway router for my Wi-Fi extender?	Yes, but it is not recommended as it will be difficult to distinguish between two SSIDs with the same name.
A firmware upgrade failed and the RE23S isn't working.	Firmware upgrade failures can happen occasionally due to power cuts or unstable connections. When this happens, follow the instructions below: 1. Connect a computer to one of the LAN ports on RE23S using an Ethernet cable. 2. Modify the IP address of the connected computer to ***192.168.9.x*** where ***x*** is any value between ***3*** and ***254*** (Refer to ***IV-3*** on how to modify the IP address of your computer). 3. Go to ***192.168.9.2*** in a web browser, and you will see the page below:  4. Click "Browse" to locate the firmware file on your computer and click "Upload" to upload the new firmware. It may take several minutes to complete, please wait and follow the instructions on screen.

IV-7 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.
http://192.168.168.254/ - top
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 192.34.45.8). 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 "Broadbandaccesspoint.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 mega 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: An 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 Unreliable 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 users can use their favorite browser to control, configure or monitor the managed device.

COPYRIGHT

Federal Communication Commission Interference Statement

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

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

FCC Caution

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

Federal Communications Commission (FCC) RF Exposure Requirements

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

RED Compliance Statement

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

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

Frequency range (MHz)	Max. Transmit Power (dBm)
WLAN Wi-FI 802.11b/g/n; 2, 4 GHz	19 bbm
WLAN Wi-FI 802.11 a/an/ac; 5 GHz	18 bbm

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

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type Home Roaming 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

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.
Operations in 5150-5250 MHz band is for indoor use only.

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 20cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

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

RED Compliance Statement

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

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

Frequency range (MHz)	Max. Transmit Power (dBm)
WLAN Wi-FI 802.11b/g/n; 2, 4 GHz	19 bbm
WLAN Wi-FI 802.11 a/an/ac; 5 GHz	18 bbm

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

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type Home Roaming 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, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU).

Türkçe: Bu cihaz 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 2006/95/EC, 2011/65/EC.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU.

suomen kieli: Tämä laite täyttää direktiivien 2014/53/EU, 2014/30/EU, 2014/35/EU, 2011/65/EU oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

	AT	BE	BG	HR	CY	CZ	DK
	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL
	PT	RO	SK	SI	ES	SE	UK

This device is restricted to indoor use.

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 Directive .

Equipment: **Home Roaming Wi-Fi Extender**
Model No.: **RE23S**

The following European standards for essential requirements have been followed:

Spectrum: **ETSI EN 300 328 V2.1.1**
ETSI EN 301 893 V2.1.1
EMC: **EN 301 489-1 V2.2.0**
EN 301 489-17 V3.2.0
EMF: **EN 62311:2008**
Safety (LVD): **IEC 60950-1:2005 (2nd Edition)+Am 1:2009+Am 2:2013 and/ or 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

Printed Name: Vivian Ma
Title: Director
Edimax Technology Europe B.V.

Date of Signature: Aug., 2017
Signature:

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

CE

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

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.


EDIMAX
NETWORKING PEOPLE TOGETHER