EDIMAX
NETWORKING PEOPLE TOGETHER

BR-6258nL

User Manual

08-2012 / v1.0

EDIMAX
NETWORKING PEOPLE TOGETHER

COPYRIGHT

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

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

Edimax Technology Co., Ltd.
Add: No. 3, Wu-Chuan 3rd Rd., Wu-Ku Industrial Park, New Taipei City, Taiwan
Tel: +886-2-77396888
Email: sales@edimax.com.tw

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.

Contents

I. Product Information

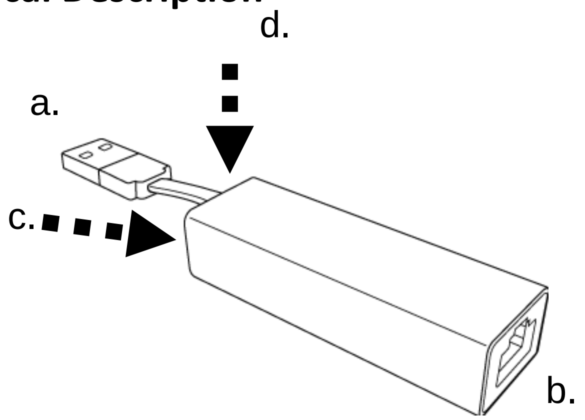
Thank you for purchasing the Edimax BR-6258nL Wireless Personal Hotspot and Travel Router! For someone constantly on the move, this tiny router is an essential companion. Its quick and easy installation process ensures that anybody can set up a network environment and share an Internet connection in a matter of minutes.

I-1. Package Contents

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

- Travel Router
- Quick installation guide
- CD with multi-language QIG and user manual
- Access Key Card

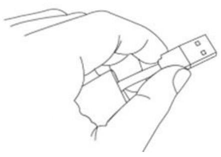
I-2. Physical Description



a. **USB connector and cable:** This connector can be plugged into a computer's USB port, or into a USB power adapter.

Note: The USB connector on this device transmits electrical power only, it does ***not*** transmit data. This device can only be configured by connecting to it wirelessly.

Note: To prevent damage to the device, when plugging and unplugging the USB connector, please hold the connector itself. Do not pull on the body of the travel router.



b. **Ethernet port:** This port is used to connect to a wired Internet connection.

> **Note**: Please do not connect this Ethernet port to your computer's Ethernet port, it will ***not*** work. This port should be connected to an access point or xDSL/cable modem.

c. **WPS/Reset button:** Press this button for 2 seconds to activate WPS mode, or 10 seconds to reset the device.

d. **LED indicator:** There are two visible LEDs underneath the device's casing, one blue and one green.

I-3. LED Status

LED	**Color**	**LED Status**	**Description**
Power	Blue	Blinking	Rapid: Device is initializing Slow: Device is resetting
		Steady On	Device is powered normally
		Off	Device is not powered
WPS	Green	Steady ON	When a WPS connection has been established, the LED will activate for 5 minutes
		Blinking	WPS is in progress
		Off	No power or no WPS in progress

> **Note**: When the WPS LED is blinking, that means WPS is in progress. Please do not press the WPS button again until the light stops blinking.

I-4. Safety Information

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

1. The travel router is designed for indoor use only; do not place the travel router outdoors.

2. Do not place the travel router 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 travel router.

4. Take care when moving and handling the travel router; accidental damage is not covered by the travel router’s warranty.

5. The device contains small parts which are a danger to small children under 3 years old. Please keep the travel router out of reach of children.

6. Do not place the travel router on paper, cloth, or other flammable materials. The travel router will become hot during use.

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

8. The travel router 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 travel router, then disconnect the travel router immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

I-5. System Requirements

- Wireless network card compatible with 802.11b/g/n wireless network standard.
- Web Browser for software configuration (Internet Explorer 7 or above, Google Chrome, Firefox, Safari).
- 1 available USB Type A port capable of supplying 500mA.
- Existing network with Internet connection.

II. Quick Installation: iQ Setup

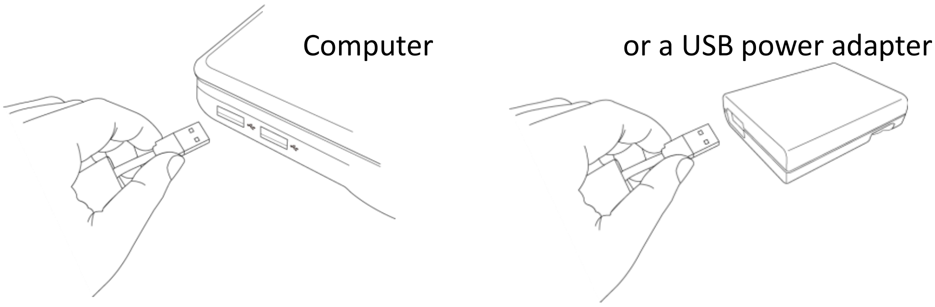
Your travel router can be up and running in a matter of minutes. Just follow these instructions to run the travel router's built-in quick installation program, known as "iQ Setup".

If you need to make more detailed configurations, you can refer to **III. Browser Based Configuration Interface.**

Note: Before you use this travel router, please make sure your computer is set to use a **dynamic IP address**. This is a simple procedure, and step by step instructions for how to do this, can be found in **IV-1. Appendix: Configuring your IP address**.

1. Remove the clear plastic wrapping from the device.

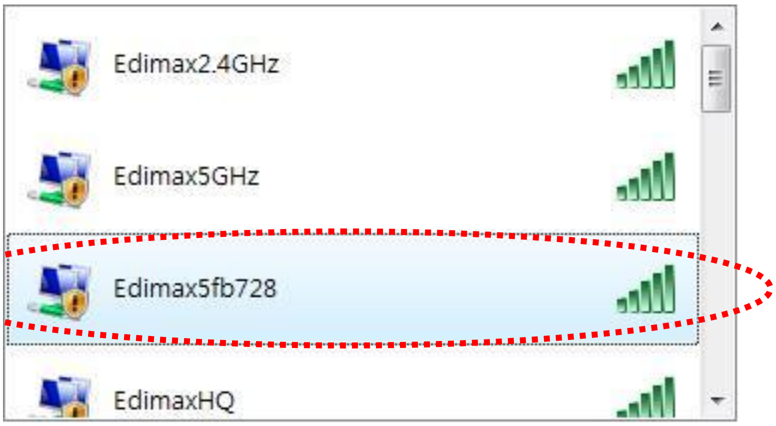
2. Insert the USB connector of the travel router into a USB port on your computer, **or** into a USB power adapter.



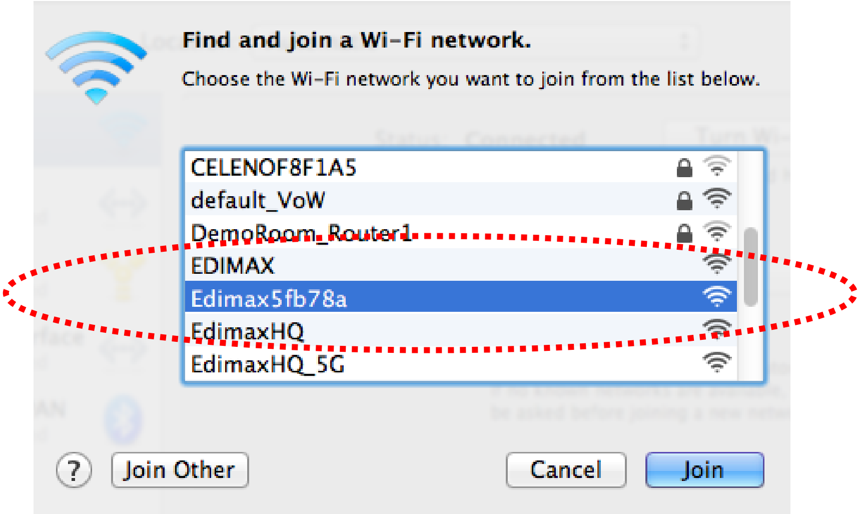
The **blue power LED** will light up for 10 to 15 seconds. The LED will then begin to flash rapidly for an additional 10 to 15 seconds, as the device initializes. When the **blue LED** remains lit without flashing, the device has completed its initialization.

3. Search nearby wireless connections for a network with an ID similar to **Edimax5fb728**, as in the figure below. The last six characters will be different for every individual travel router device, and will be based on the MAC address of your router.

Windows:

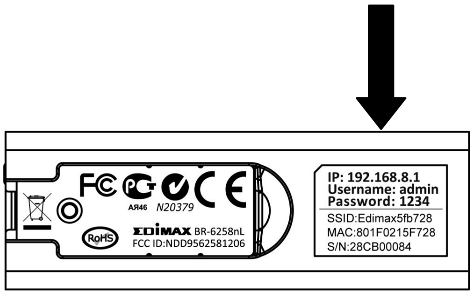


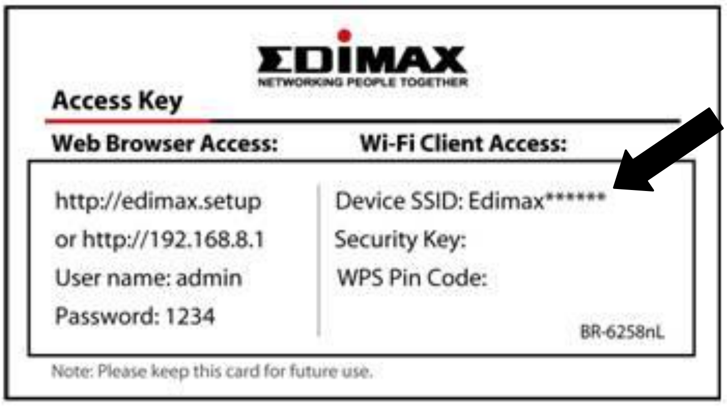
Mac:


Find and join a Wi-Fi network.

Choose the Wi-Fi network you want to join from the list below.

You may also find your device ID on the included Access Key card, or on the label on the travel router itself.




EDIMAX
NETWORKING PEOPLE TOGETHER

Access Key

Web Browser Access:
http://edimax.setup
or http://192.168.8.1
User name: admin
Password: 1234

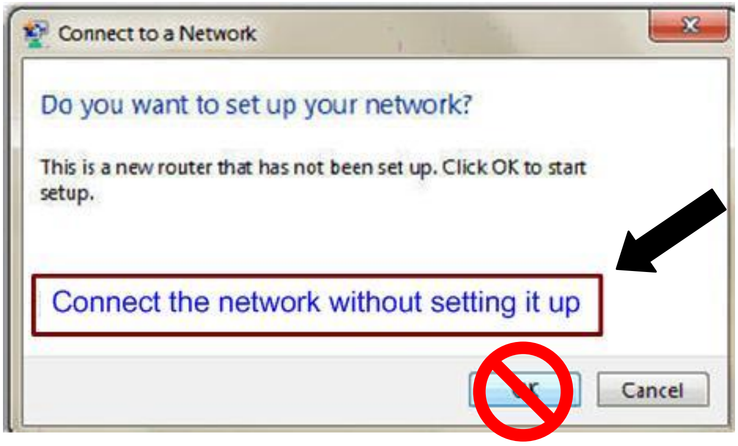
Wi-Fi Client Access:
Device SSID: Edimax******
Security Key:
WPS Pin Code:

BR-6258nL

Note: Please keep this card for future use.

Connect to this wireless network.

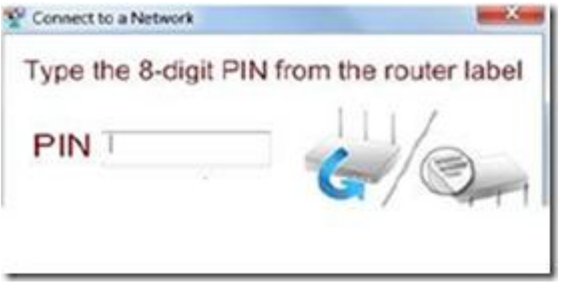
Note: If you are using Windows Vista or Windows 7 and the following appears, please click “Connect the network without setting it up”. Please do not click “OK”.


Connect to a Network

Do you want to set up your network?

This is a new router that has not been set up. Click OK to start setup.

If you have accidentally clicked "OK", you will see the following. Please click "Cancel" and try the previous step again.

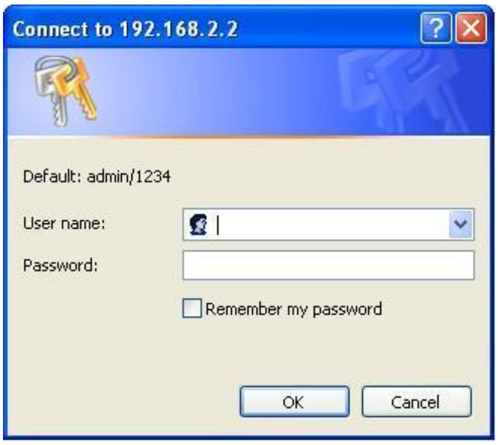

Connect to a Network

Type the 8-digit PIN from the router label

4. **Windows users**, open the Internet Explorer web browser. You will be prompted to enter a user name and password. **Mac users** will be prompted for a username and password automatically.

   The default user name is **admin**, and the default password is **1234**.

Windows:


Connect to 192.168.2.2

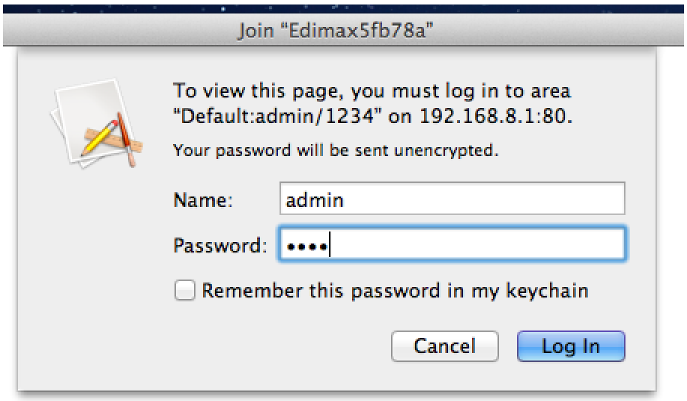
Default: admin/1234

User name:

Password:

□ Remember my password

Mac:



Join "Edimax5fb78a"

To view this page, you must log in to area "Default:admin/1234" on 192.168.8.1:80.

Your password will be sent unencrypted.

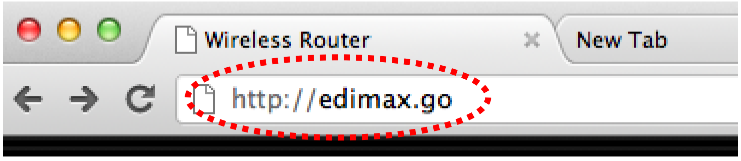
Name: admin

Password: ••••

☐ Remember this password in my keychain

Mac users then need to open a web browser, and enter the access key http://edimax.go or the default IP address 192.168.8.1 into the URL bar.

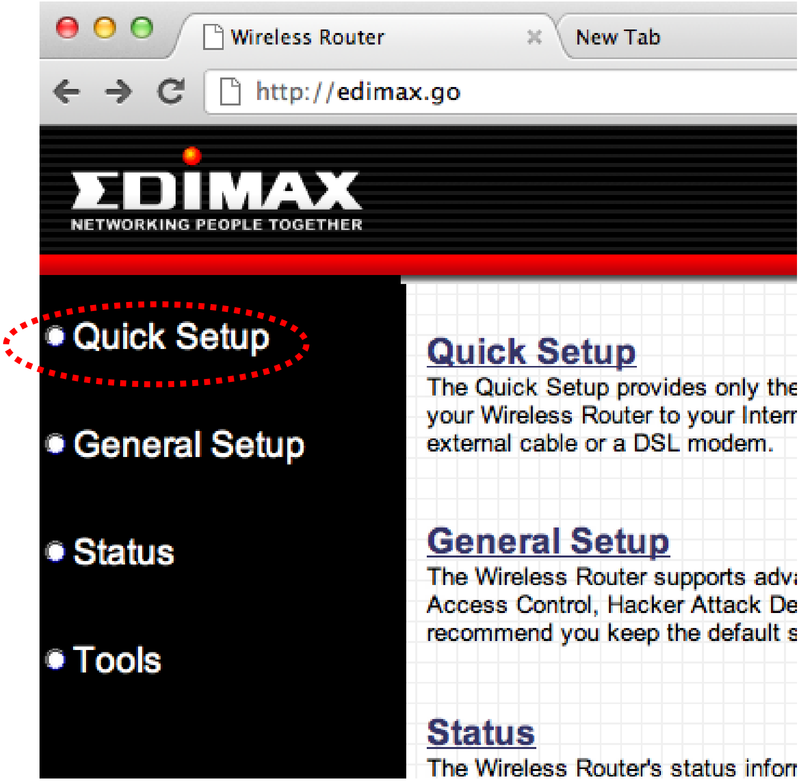
Mac:



http://edimax.go

5. **Windows users** will now arrive at the first iQ setup page. **Mac users** need to select "Quick Setup" from the menu on the left side, as shown below.

Mac:



Quick Setup

The Quick Setup provides only the your Wireless Router to your Interr external cable or a DSL modem.

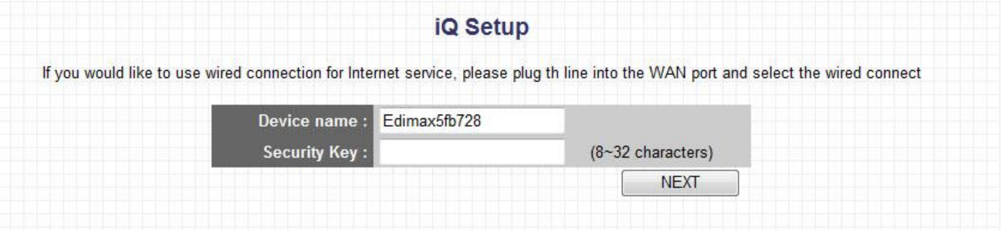
General Setup

The Wireless Router supports adv Access Control, Hacker Attack De recommend you keep the default s

Status

The Wireless Router's status infor

From this point, **both Windows and Mac users** continue iQ Setup in the same manner. The first step of the setup process is to name the router, and to give it a security key. The default name of the device is the device ID, while the security key must be between 8 and 32 characters. After both have been set, click ‘NEXT’ to continue.



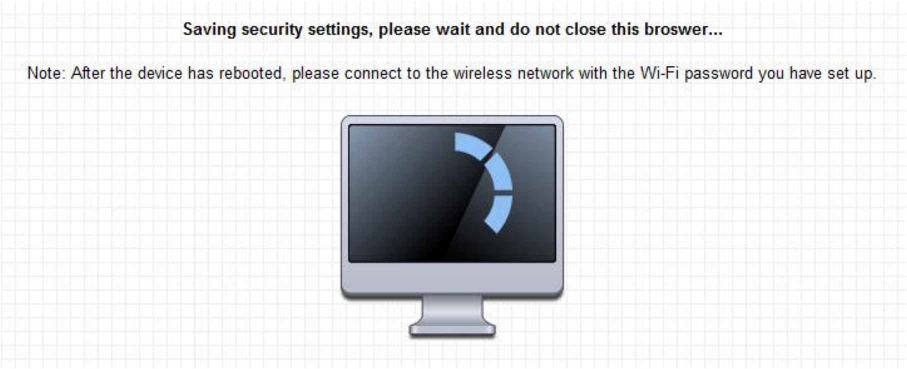
iQ Setup

If you would like to use wired connection for Internet service, please plug th line into the WAN port and select the wired connect

Device name : Edimax5fb728

Security Key : (8~32 characters)

6. The travel router will save settings and reboot. The device will automatically disconnect from your computer while it reboots.

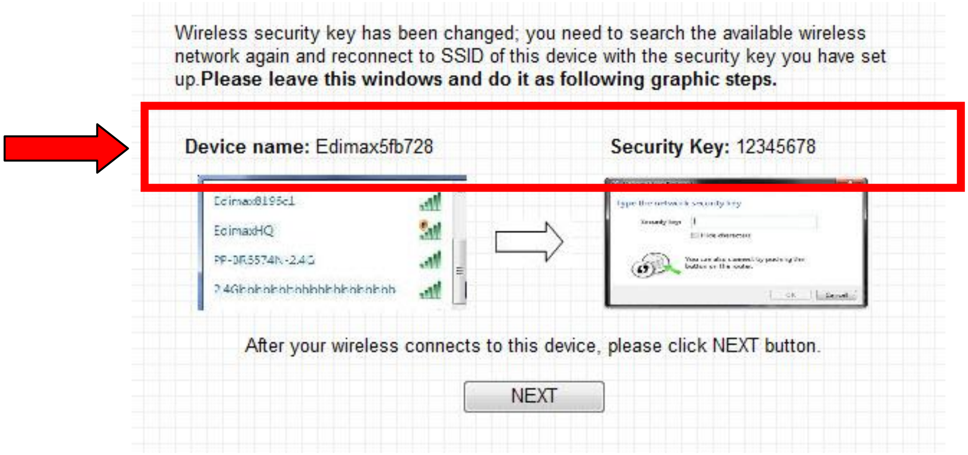


Saving security settings, please wait and do not close this browser...

Note: After the device has rebooted, please connect to the wireless network with the Wi-Fi password you have set up.

7. When the following screen appears, the device has completed its reboot. Reconnect to the travel router by searching available wireless networks for the device name you set in step 5. The device name and security key will also be displayed on screen, as shown below.

   Enter the 8 to 32 character security key you set. When your computer has successfully reconnected to the device, click “NEXT”.



Wireless security key has been changed; you need to search the available wireless network again and reconnect to SSID of this device with the security key you have set up.**Please leave this windows and do it as following graphic steps.**

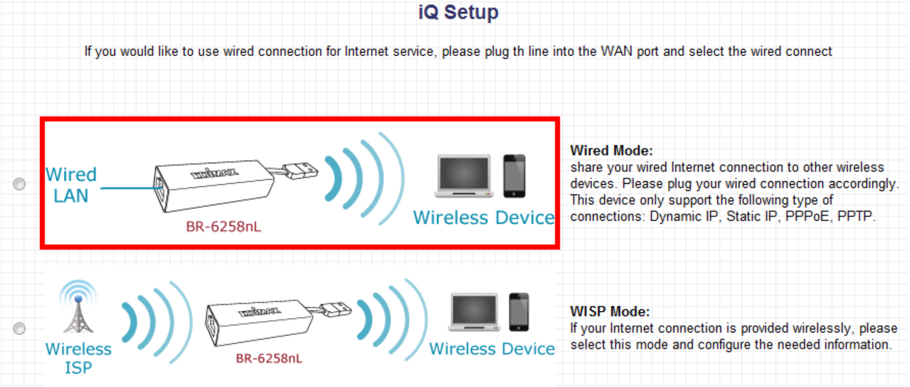
Device name: Edimax5fb728

Security Key: 12345678

After your wireless connects to this device, please click NEXT button.

Note: Please enter the security key you set in step 5. The security key in the screenshot is an example.

8. You will be prompted to choose between “Wired Mode” and “WISP Mode”.



iQ Setup

If you would like to use wired connection for Internet service, please plug th line into the WAN port and select the wired connect

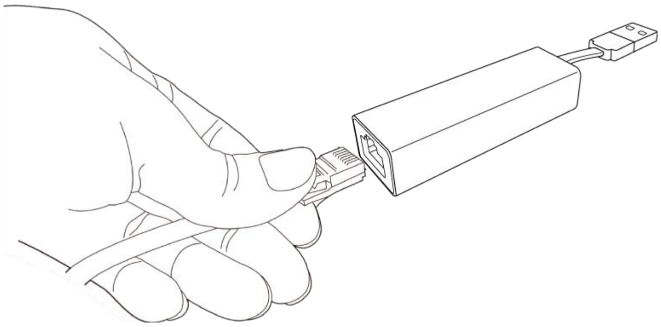
○ **Wired Mode:**
share your wired Internet connection to other wireless devices. Please plug your wired connection accordingly. This device only support the following type of connections: Dynamic IP, Static IP, PPPoE, PPTP.

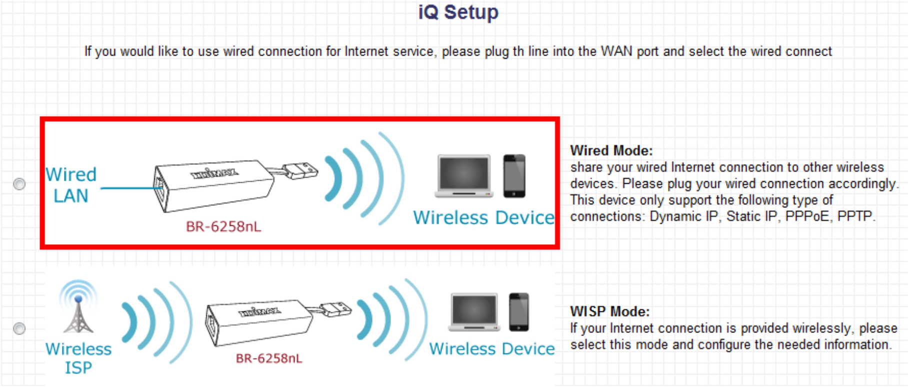
○ **WISP Mode:**
If your Internet connection is provided wirelessly, please select this mode and configure the needed information.

II-2. iQ Setup: Wired Connection Mode

Wired connection mode allows the travel router to receive a wired Internet connection via its Ethernet port, and broadcast that connection wirelessly.

1. Insert the Internet-connected LAN cable into the travel router’s Ethernet port, then select the Wired Mode option on the setup screen.





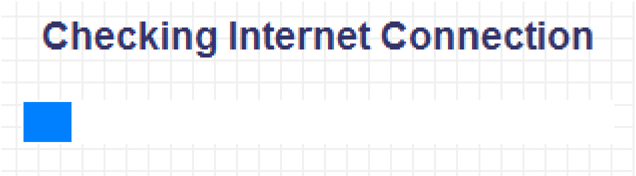
iQ Setup

If you would like to use wired connection for Internet service, please plug th line into the WAN port and select the wired connect

○ **Wired Mode:**
share your wired Internet connection to other wireless devices. Please plug your wired connection accordingly. This device only support the following type of connections: Dynamic IP, Static IP, PPPoE, PPTP.

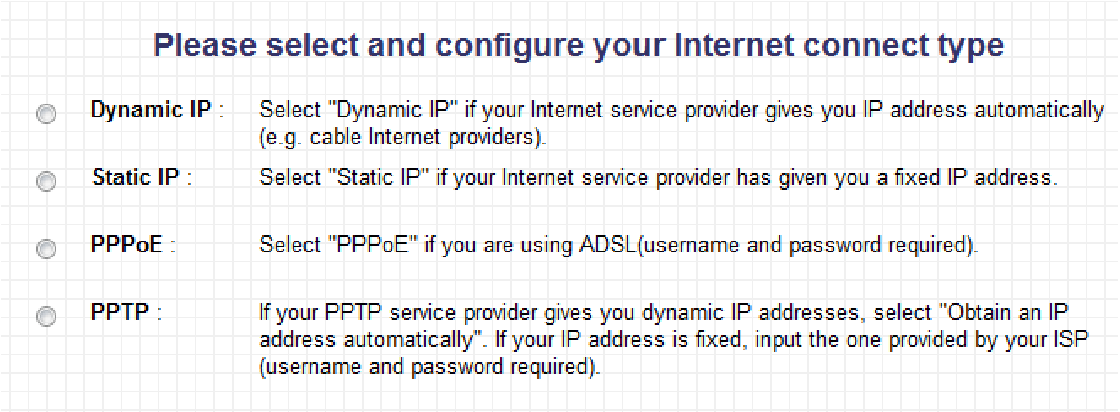
○ **WISP Mode:**
If your Internet connection is provided wirelessly, please select this mode and configure the needed information.

2. The travel router will detect your WAN (Wide Area Network) type and test the Internet connection.



Checking Internet Connection

3. If the WAN connection uses a dynamic IP and the connection is successful, you will see a final congratulation screen. If you see the following screen (shown below) “Please select and configure your Internet connect type”, then please follow the on-screen prompts and select your connection type. Enter your ISP information, user name, password, or DNS information as required.



Please select and configure your Internet connect type

○ **Dynamic IP** : Select "Dynamic IP" if your Internet service provider gives you IP address automatically (e.g. cable Internet providers).

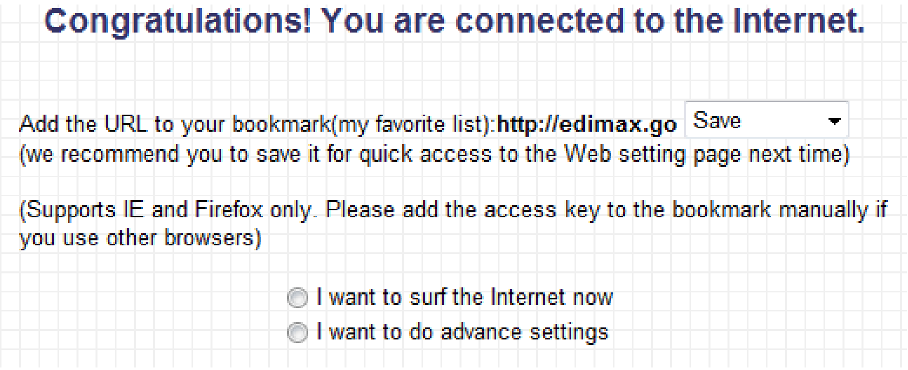
○ **Static IP** : Select "Static IP" if your Internet service provider has given you a fixed IP address.

○ **PPPoE** : Select "PPPoE" if you are using ADSL(username and password required).

○ **PPTP** : If your PPTP service provider gives you dynamic IP addresses, select "Obtain an IP address automatically". If your IP address is fixed, input the one provided by your ISP (username and password required).

Note: Please refer to **III-3-2.** WAN for more guidance on these parameters.

After the connection is successfully established, you may choose to start using the Internet immediately, or perform more advanced configuration. On this screen, you have the option of setting a bookmark to http://edimax.go, which will lead you directly to the travel router’s browser-based setup screen.



Congratulations! You are connected to the Internet.

Add the URL to your bookmark(my favorite list):**http://edimax.go** Save ▾
(we recommend you to save it for quick access to the Web setting page next time)

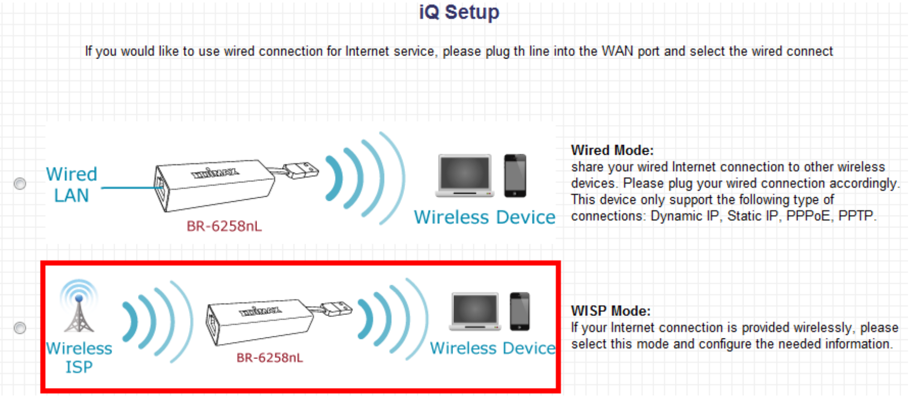
(Supports IE and Firefox only. Please add the access key to the bookmark manually if you use other browsers)

○ I want to surf the Internet now
○ I want to do advance settings

II-3. iQ Setup: WISP Mode

In WISP mode, the travel router receives a wireless signal and broadcasts it to multiple wireless devices.

1. Select WISP mode on the setup screen.



iQ Setup

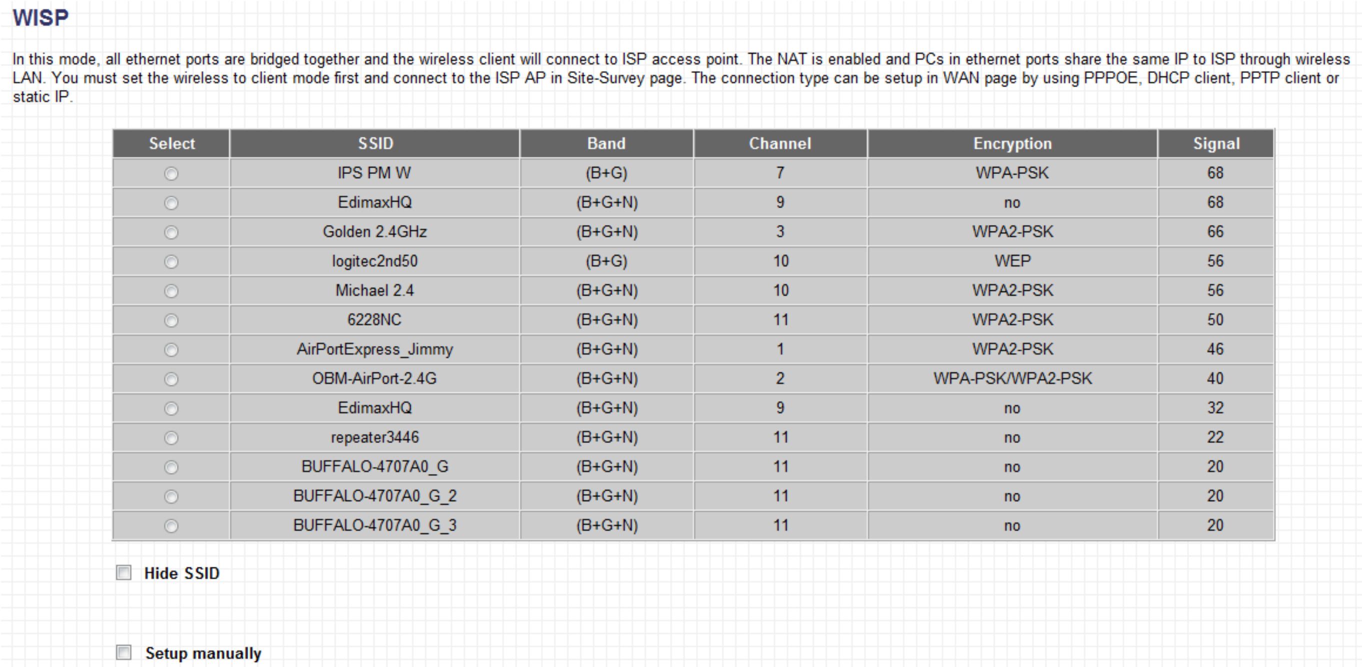
If you would like to use wired connection for Internet service, please plug th line into the WAN port and select the wired connect

○ **Wired Mode:**
share your wired Internet connection to other wireless devices. Please plug your wired connection accordingly. This device only support the following type of connections: Dynamic IP, Static IP, PPPoE, PPTP.

○ **WISP Mode:**
If your Internet connection is provided wirelessly, please select this mode and configure the needed information.

2. The travel router will automatically scan for available Wi-Fi networks. Select the network you wish to connect to. If the network requires a security key, enter it here. Please be careful when entering the security key, as an incorrect key will result in the travel router being unable to connect to the Wi-Fi network.

   If the network you wish to connect to does not appear, please try clicking on the “Refresh” button, or move the travel router closer to the root wireless access point.



WISP

In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

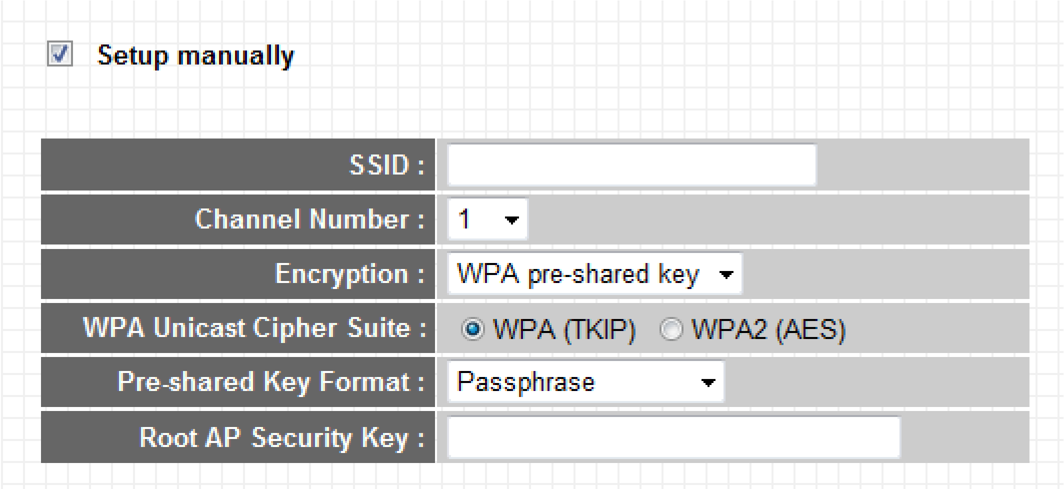
Select	SSID	Band	Channel	Encryption	Signal
○	IPS PM W	(B+G)	7	WPA-PSK	68
○	EdimaxHQ	(B+G+N)	9	no	68
○	Golden 2.4GHz	(B+G+N)	3	WPA2-PSK	66
○	logitec2nd50	(B+G)	10	WEP	56
○	Michael 2.4	(B+G+N)	10	WPA2-PSK	56
○	6228NC	(B+G+N)	11	WPA2-PSK	50
○	AirPortExpress_Jimmy	(B+G+N)	1	WPA2-PSK	46
○	OBM-AirPort-2.4G	(B+G+N)	2	WPA-PSK/WPA2-PSK	40
○	EdimaxHQ	(B+G+N)	9	no	32
○	repeater3446	(B+G+N)	11	no	22
○	BUFFALO-4707A0_G	(B+G+N)	11	no	20
○	BUFFALO-4707A0_G_2	(B+G+N)	11	no	20
○	BUFFALO-4707A0_G_3	(B+G+N)	11	no	20

□ Hide SSID

□ Setup manually

You may choose to Hide the SSID of the router's wireless network by checking the "Hide SSID" box.

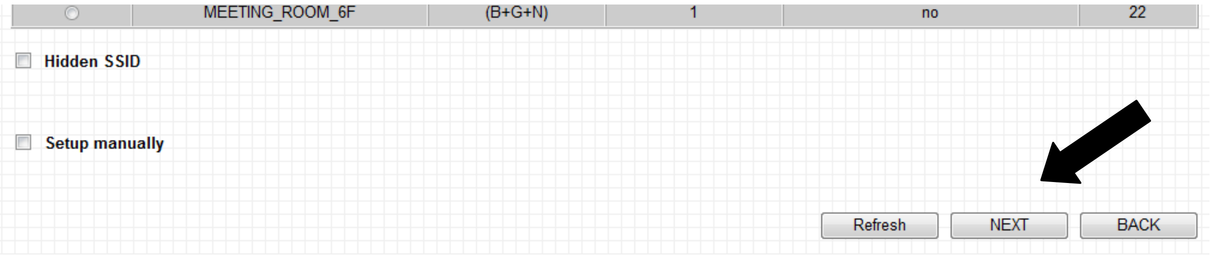
If the wireless network you wish to connect to is not broadcasting its SSID (i.e. it has chosen to hide its ID), you may connect to it manually if you know its SSID. To do so, please check the "Setup manually" box and input the SSID, channel number, and encryption information into the appropriate fields, as shown below. Please refer to **III-3-4-3.** Security Settings for more detailed information about encryption.



☑ Setup manually

SSID :	
Channel Number :	1
Encryption :	WPA pre-shared key
WPA Unicast Cipher Suite :	● WPA (TKIP) ○ WPA2 (AES)
Pre-shared Key Format :	Passphrase
Root AP Security Key :	

3. Press "NEXT" to continue, or press "BACK" to return to the previous step.

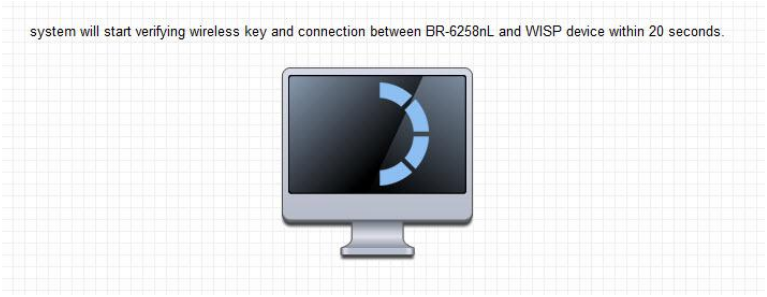


○	MEETING_ROOM_6F	(B+G+N)	1	no	22

☐ Hidden SSID

☐ Setup manually

4. The travel router will save the changed settings and may reboot. If it does, reconnect to the travel router by searching available wireless networks for the device name you set in step 5 of the **Quick Installation** section. Enter the 8 to 32 character security key you set.

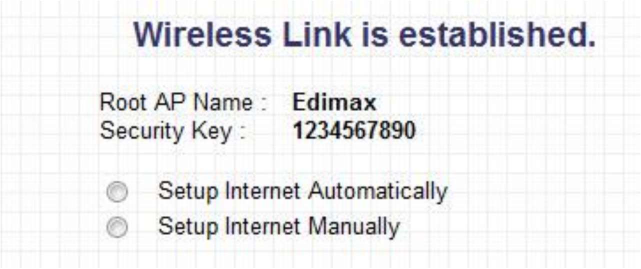


system will start verifying wireless key and connection between BR-6258nL and WISP device within 20 seconds.

5. After reconnecting, the travel router will verify the connection. If the connection is successful, the setup screen will tell you the ID of the wireless network it has connected to, as well as the security key.

   You will then be prompted to choose whether to "Setup Internet Automatically", or to "Setup Internet Manually". Selecting "Setup Internet Automatically" will work in most cases, and is recommended.

   If the router is unable to "Setup Internet Automatically", it will prompt you to "Setup Internet Manually". For details on how to set up the connection manually, please see **III-2. Quick Setup.**



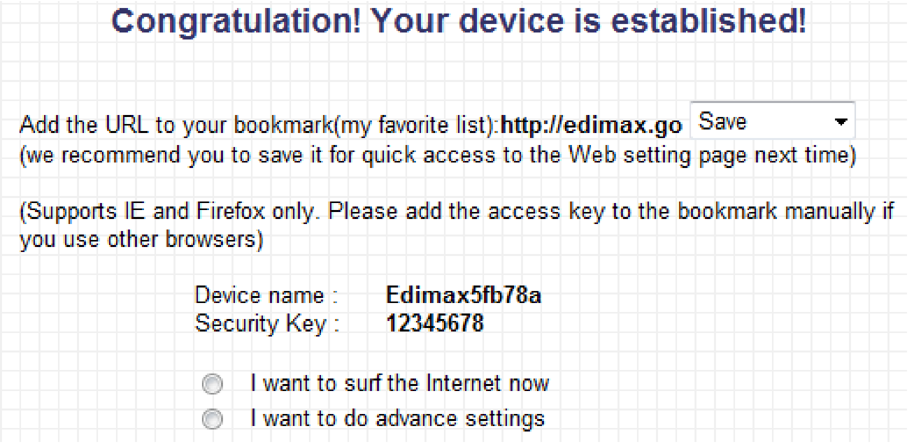
Wireless Link is established.

Root AP Name : **Edimax**
Security Key : **1234567890**

○ Setup Internet Automatically
○ Setup Internet Manually

6. After Internet settings are set up, you will see a final congratulation screen. On this screen, you have the option of setting a bookmark to http://edimax.go, which will lead you directly to the travel router's browser-based configuration interface (see **III.** **Browser Based Configuration Interface**). You will also see final confirmation of the travel router's name and security key.

   You may now start surfing the Internet immediately, or you may choose to perform more advanced configuration via the browser based configuration interface.



Congratulation! Your device is established!

Add the URL to your bookmark(my favorite list):**http://edimax.go** Save
(we recommend you to save it for quick access to the Web setting page next time)

(Supports IE and Firefox only. Please add the access key to the bookmark manually if you use other browsers)

Device name :	**Edimax5fb78a**
Security Key :	**12345678**

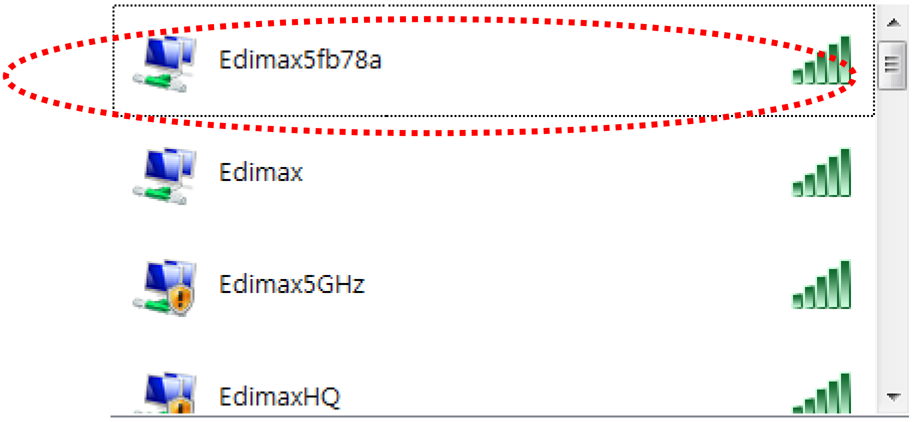
○ I want to surf the Internet now
○ I want to do advance settings

II-4. Connecting to the Travel Router

Once connected to the Internet, whether through a wired connection or through WISP mode, other wireless devices can connect to this travel router and access the Internet through it.

1. Search for available Wi-Fi networks on your other device, and select the ID of the travel router, such as in the example screenshot below. This simple procedure will vary slightly depending on your device.

Windows PC:



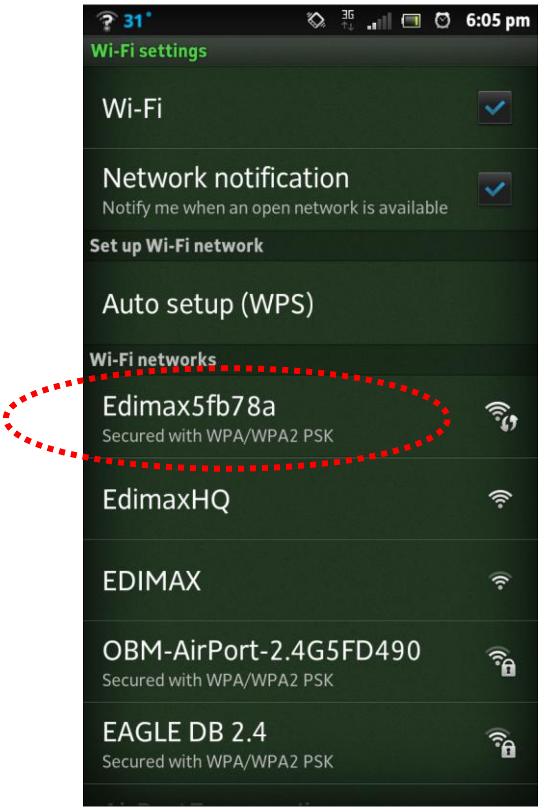
Edimax5fb78a

Edimax

Edimax5GHz

EdimaxHQ

Android Smartphone:



31° 6:05 pm

Wi-Fi settings

Wi-Fi ☑

Network notification ☑
Notify me when an open network is available

Set up Wi-Fi network

Auto setup (WPS)

Wi-Fi networks

Edimax5fb78a
Secured with WPA/WPA2 PSK

EdimaxHQ

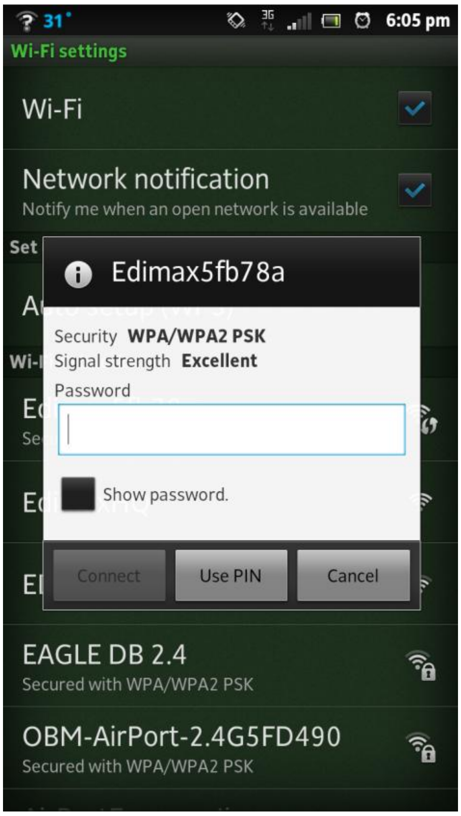
EDIMAX

OBM-AirPort-2.4G5FD490
Secured with WPA/WPA2 PSK

EAGLE DB 2.4
Secured with WPA/WPA2 PSK

2. Enter the wireless security key you set previously.

Android Smartphone:



31° 6:05 pm

Wi-Fi settings

Wi-Fi ☑

Network notification ☑
Notify me when an open network is available

Edimax5fb78a

Security **WPA/WPA2 PSK**
Signal strength **Excellent**
Password

□ Show password.

EAGLE DB 2.4
Secured with WPA/WPA2 PSK

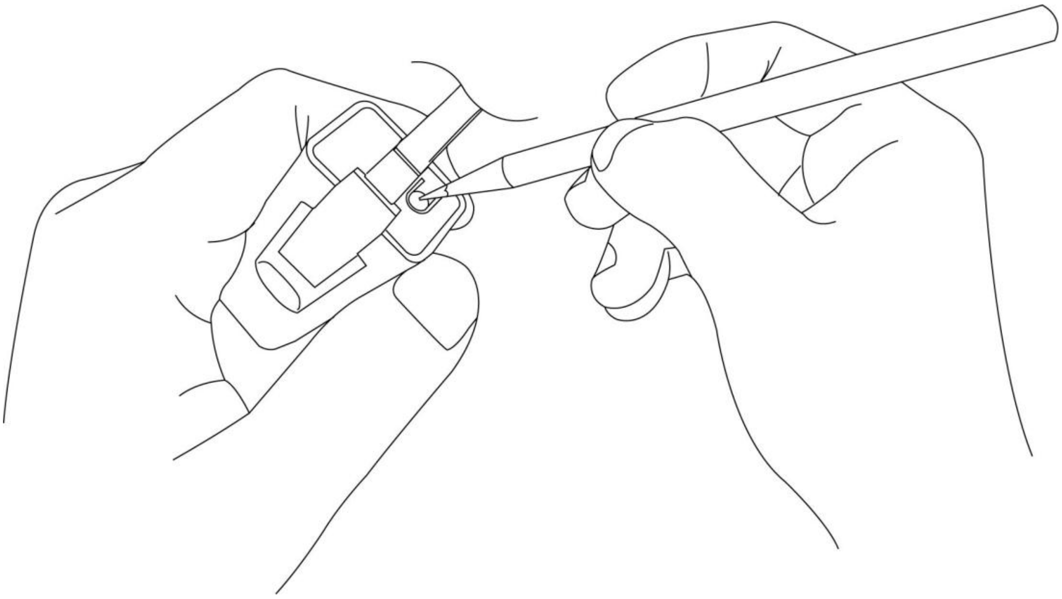
OBM-AirPort-2.4G5FD490
Secured with WPA/WPA2 PSK

3. Repeat for as many wireless devices as you wish to connect to the Internet. The travel router will broadcast the wireless Internet signal, making it a personal hotspot for you and your wireless devices.

II-5. Resetting the Travel Router

In the event the travel router is not properly functioning, or you wish to reset and remove all settings, you can reset the travel router to its factory default..

1. Make sure the device is powered (by plugging the USB connector to a computer or a USB power adapter).
2. Hold the body of the device with your hand, then press and hold the **WPS/Reset button** with the end of a paper clip or a pen nub for approximately 10 seconds, until the **blue LED indicator** begins to flash. When the LED begins to flash, you may release the button, and the device will begin to reset to factory default settings.



3. The LED will first stay steadily lit for approximately 10 to 15 seconds. The LED will then begin to flash rapidly for an additional 10 to 15 seconds, as the device reinitializes. When the blue LED remains lit without flashing, the device has completed its reset process, and is ready for further configuration.

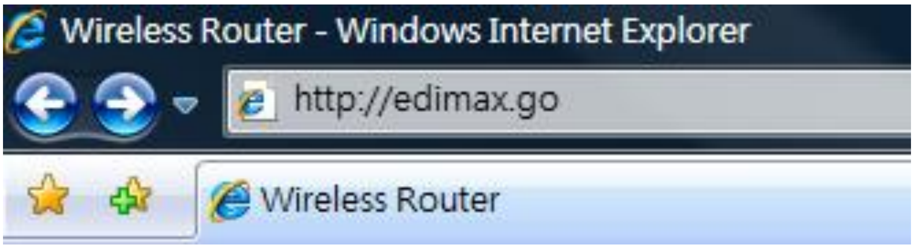
III. Browser Based Configuration Interface

Once you have set the travel router to its operating mode as detailed in **II. Quick Setup: iQ Setup**, you can further configure the settings of the travel router anytime using the browser based configuration interface.

Note: Before you use this travel router, please make sure your computer is set to use a **dynamic IP address**. This is a simple procedure, and step by step instructions for how to do this, can be found in Appendix.

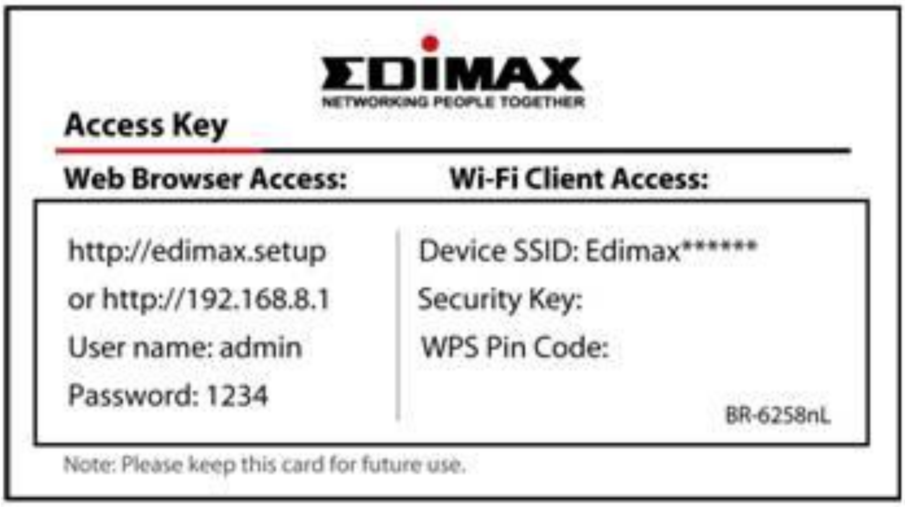
To access the browser based configuration interface, ensure that your travel router is still connected to your computer or power source via USB, and that you are connected to its wireless network, as detailed in **II. Quick Setup** steps 2 and 3.

You can access the browser based configuration interface by entering “**http://edimax.go**” into the URL bar of a web browser.



http://edimax.go

As an alternative, you can also enter the travel router’s default IP **http://192.168.8.1** into the URL bar of a web browser. This information, along with other useful factory default values, is displayed on the access key card which is included in the box with your travel router:



EDIMAX
NETWORKING PEOPLE TOGETHER

Access Key

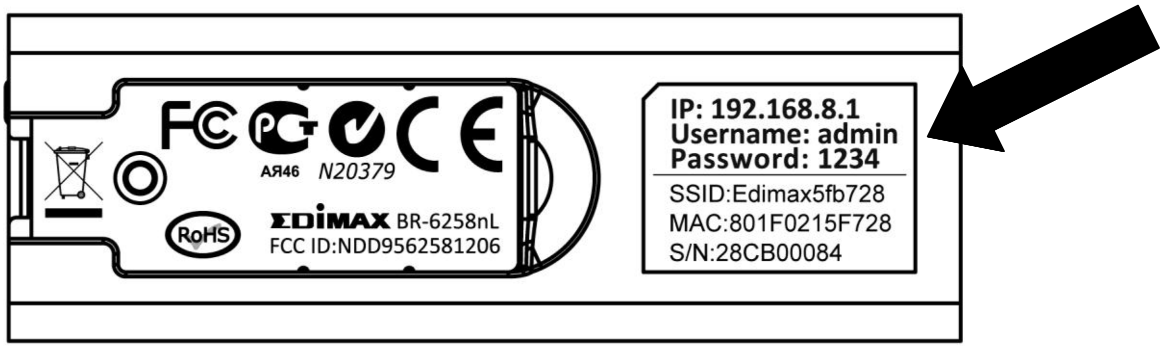
Web Browser Access:	Wi-Fi Client Access:
http://edimax.setup	Device SSID: Edimax******
or http://192.168.8.1	Security Key:
User name: admin	WPS Pin Code:
Password: 1234	

BR-6258nL

Note: Please keep this card for future use.

Web browser access	This is information necessary for you to login to the browser-based configuration interface.
Wi-Fi Client access	This is information necessary for your wireless client device (such as computer, smart phone or tablet) to connect to this device.

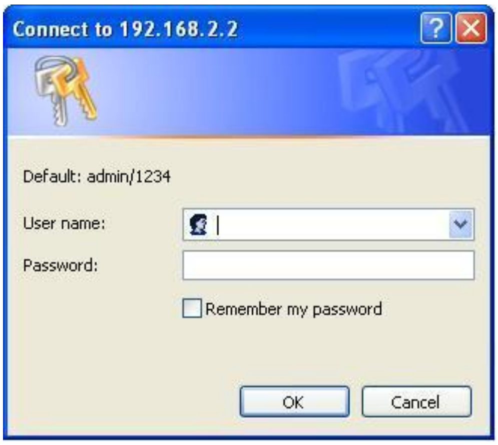
This information can also be found on the label of the device itself.



IP: 192.168.8.1
Username: admin
Password: 1234
SSID:Edimax5fb728
MAC:801F0215F728
S/N:28CB00084

You will then be prompted to enter the device's username and password. The default username is **admin** and the default password is **1234**.

Windows:



Connect to 192.168.2.2

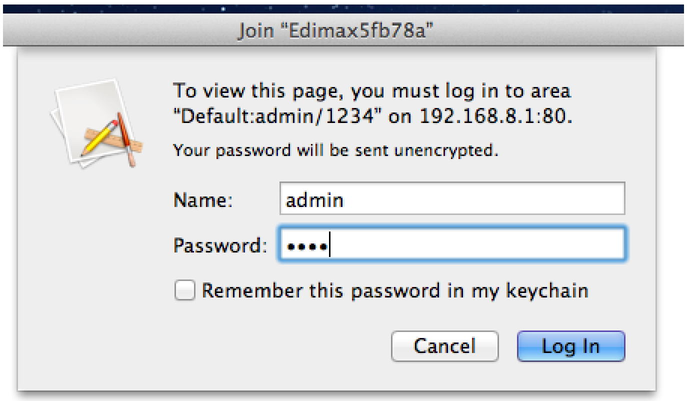
Default: admin/1234

User name:

Password:

□ Remember my password

Mac:



Join "Edimax5fb78a"

To view this page, you must log in to area "Default:admin/1234" on 192.168.8.1:80.

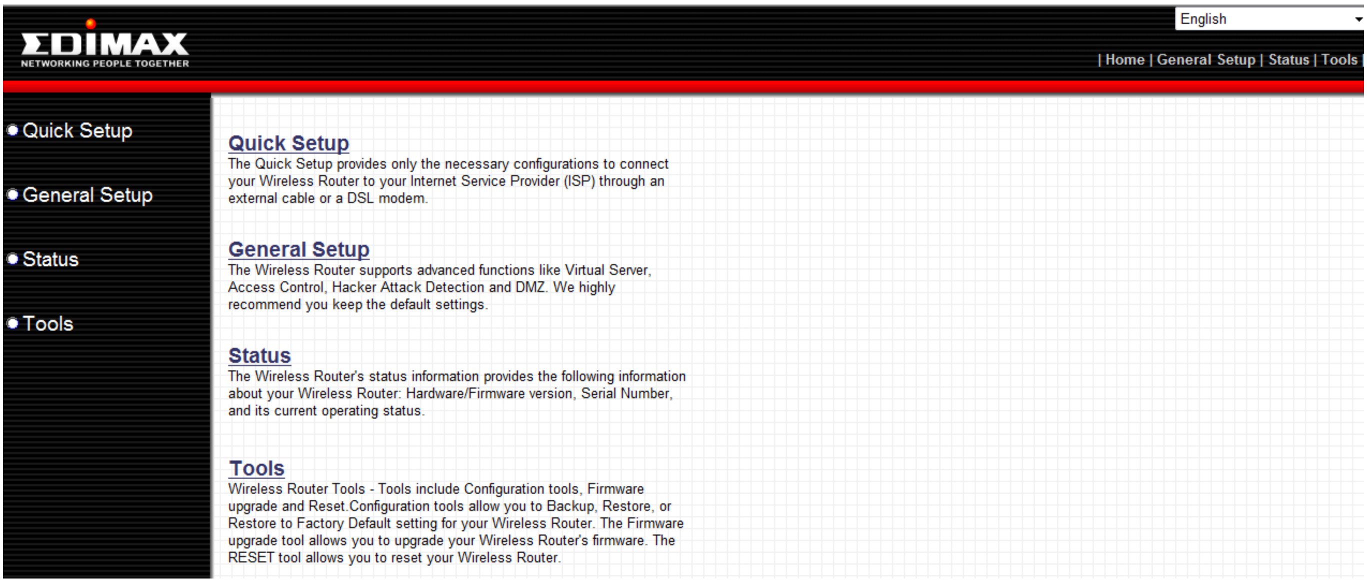
Your password will be sent unencrypted.

Name: admin

Password: ••••

□ Remember this password in my keychain

From here, you will see the browser based configuration interface home screen.


EDIMAX
NETWORKING PEOPLE TOGETHER
English
| Home | General Setup | Status | Tools |
Quick Setup
General Setup
Status
Tools

Quick Setup

The Quick Setup provides only the necessary configurations to connect your Wireless Router to your Internet Service Provider (ISP) through an external cable or a DSL modem.

General Setup

The Wireless Router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.

Status

The Wireless Router's status information provides the following information about your Wireless Router: Hardware/Firmware version, Serial Number, and its current operating status.

Tools

Wireless Router Tools - Tools include Configuration tools, Firmware upgrade and Reset.Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Wireless Router. The Firmware upgrade tool allows you to upgrade your Wireless Router's firmware. The RESET tool allows you to reset your Wireless Router.

III-1. Home

The Home page shows the four main menus into which you can navigate, and provides a brief description of each, those being:

- **III-2. Quick Setup**
- **III-3. General Setup**
- **III-4. Status**
- **III-5. Tools**

In the top right corner, there is a drop down menu to change the language of the browser based configuration interface, and shortcuts to each of the four main menus.

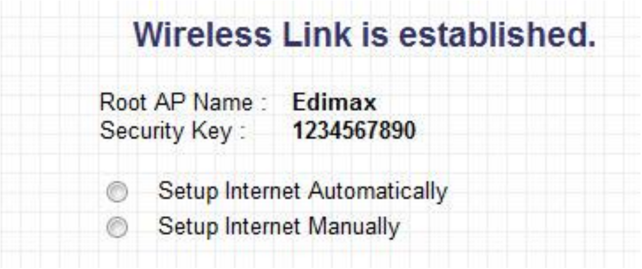
III-2. Quick Setup

If you wish to perform the initial setup process again, for example to change the operation mode of the device, select "**Quick Setup**" to restart the iQ Setup process.

You will be prompted to choose between "Wired Mode" and "WISP mode". For guidance on iQ Setup, please refer back to **II-1.** iQ Setup: Wired Connection Mode and **II-2.** iQ Setup: WISP Mode.

Note: During iQ Setup for WISP Mode, if you chose to setup your Internet connection manually, then please follow the instructions below.

When running iQ Setup for WISP mode, after you have established a connection with your wireless network, you can choose between "Setup Internet Automatically" and "Setup Internet Manually".

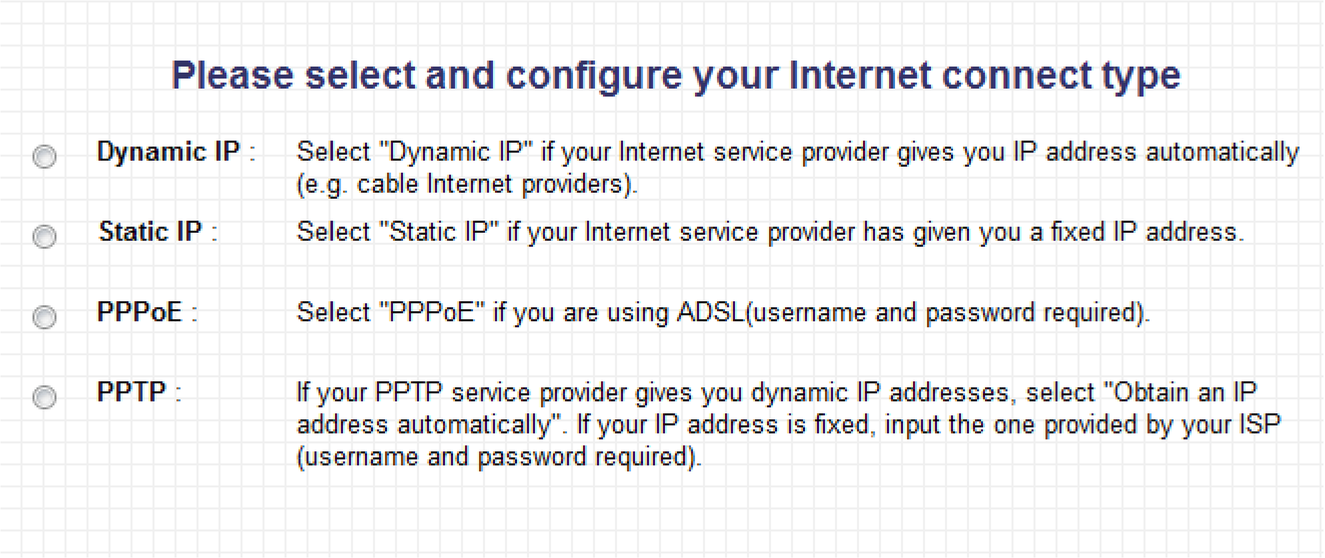


Wireless Link is established.

Root AP Name : Edimax
Security Key : 1234567890

○ Setup Internet Automatically
○ Setup Internet Manually

It is recommended that you choose "Setup Internet Automatically", as detailed in **II-2. iQ Setup: WISP Mode**. If you wish to “Setup Internet Manually”, or if the router is unable to “Setup Internet Automatically”, you will then be asked to select your connection type.



Please select and configure your Internet connect type

○ **Dynamic IP** : Select "Dynamic IP" if your Internet service provider gives you IP address automatically (e.g. cable Internet providers).

○ **Static IP** : Select "Static IP" if your Internet service provider has given you a fixed IP address.

○ **PPPoE** : Select "PPPoE" if you are using ADSL(username and password required).

○ **PPTP** : If your PPTP service provider gives you dynamic IP addresses, select "Obtain an IP address automatically". If your IP address is fixed, input the one provided by your ISP (username and password required).

Note: If you are not sure which connection type you should use, please contact your Internet Service Provider for help.

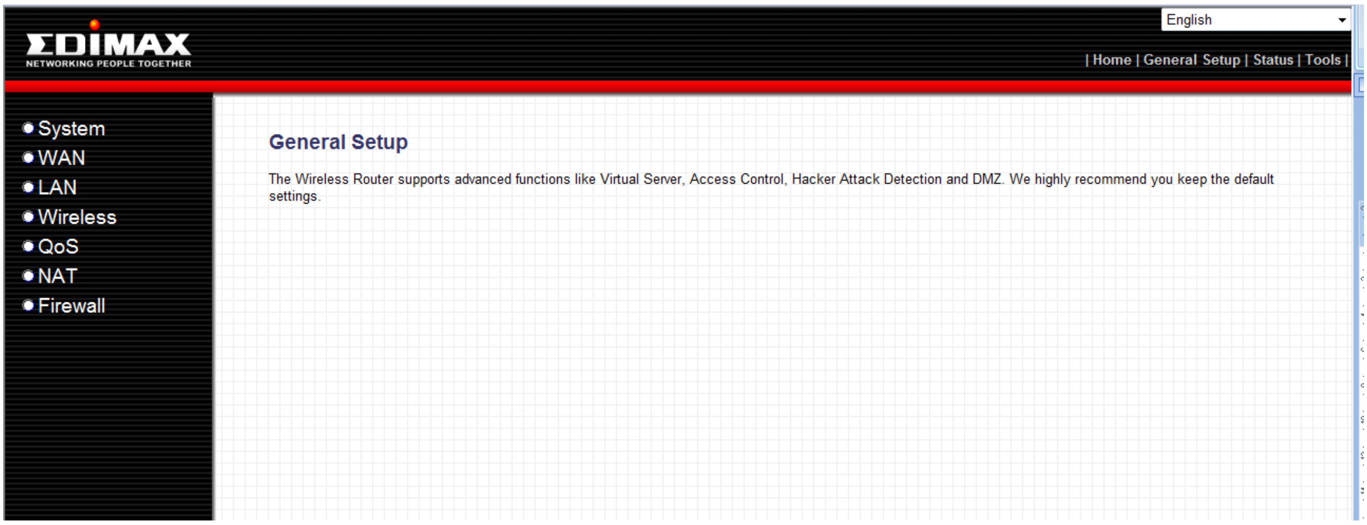
After you choose your connection type, please refer to the appropriate section of the user manual for more information, as detailed below:

- **III-3-2-1. Dynamic IP**
- **III-3-2-2. Static IP**
- **III-3-2-3. PPPoE**
- **III-3-2-4. PPTP**

III-3. General Setup

Various advanced functions can be configured under General Setup. It is highly recommended that you keep the default settings.

If you wish to proceed with configurations, use the menu displayed on the left side of the screen.

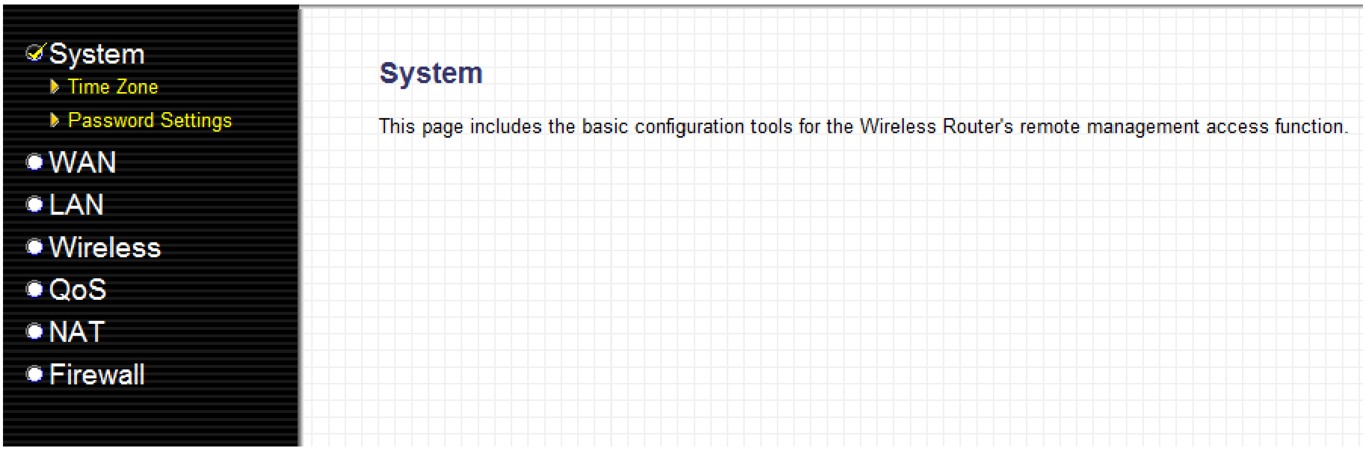

EDIMAX
NETWORKING PEOPLE TOGETHER
English
| Home | General Setup | Status | Tools |
System
WAN
LAN
Wireless
QoS
NAT
Firewall

General Setup

The Wireless Router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.

III-3-1. System

Under "System" you can modify basic parameters of the router, such as "Time Zone" and "Password Settings".

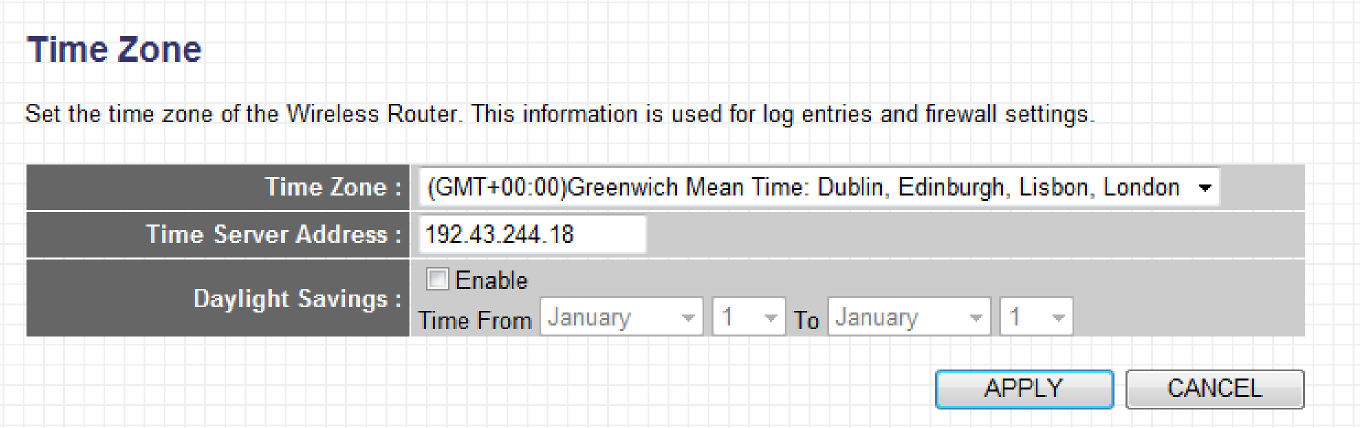


System

This page includes the basic configuration tools for the Wireless Router's remote management access function.

III-3-1-1. Time Zone

You can configure the time zone settings of your travel router here. The date and time of the device can be configured manually or can be synchronized with a time server.



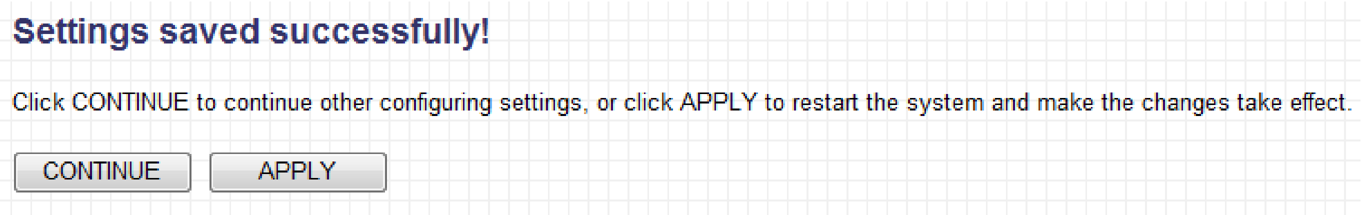
Time Zone

Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.

Time Zone :	(GMT+00:00)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time Server Address :	192.43.244.18
Daylight Savings :	□ Enable Time From January 1 To January 1

Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.
Time Server Address	The travel router supports NTP (Network Time Protocol) for automatic time and date setup. Input the host name or IP address of the IP server manually.
Daylight Savings	If your country/region uses daylight saving time, please check the "Enable Function" box and select the start and end date.

Click "APPLY" to make the changes take effect. The following message will appear:



Settings saved successfully!

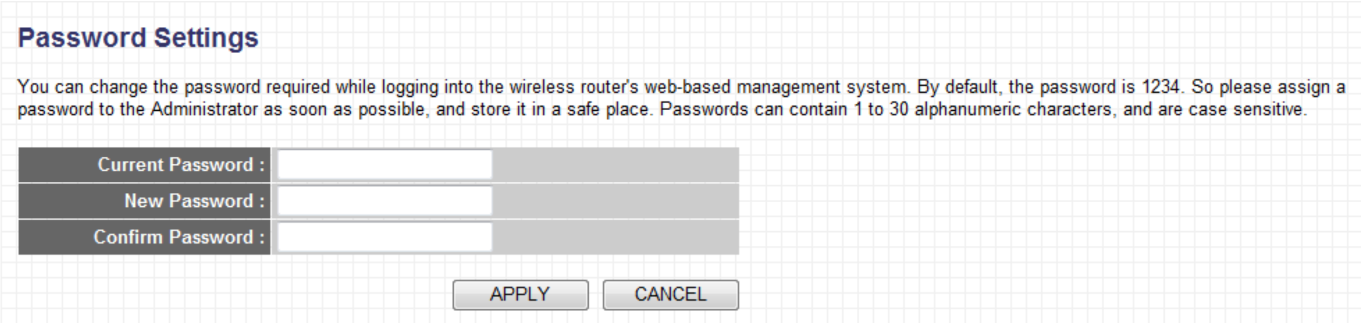
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click "APPLY" to restart the device and implement any changes. The device will restart itself.

III-3-1-2. Password Settings

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



Password Settings

You can change the password required while logging into the wireless router's web-based management system. By default, the password is 1234. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 1 to 30 alphanumeric characters, and are case sensitive.

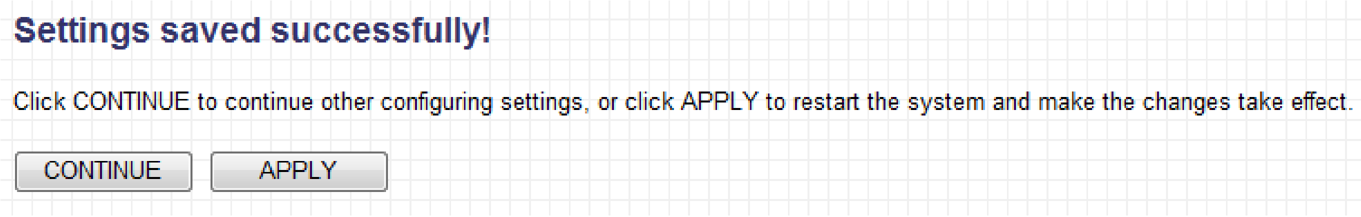
Current Password :

New Password :

Confirm Password :

Current Password	Enter your current password. The default password is **1234**.
New Password	Enter your desired new password here. You can use any combination of letters, numbers and symbols up to 20 characters.
Re-Enter Password	Confirm your new password.

Click "APPLY" to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

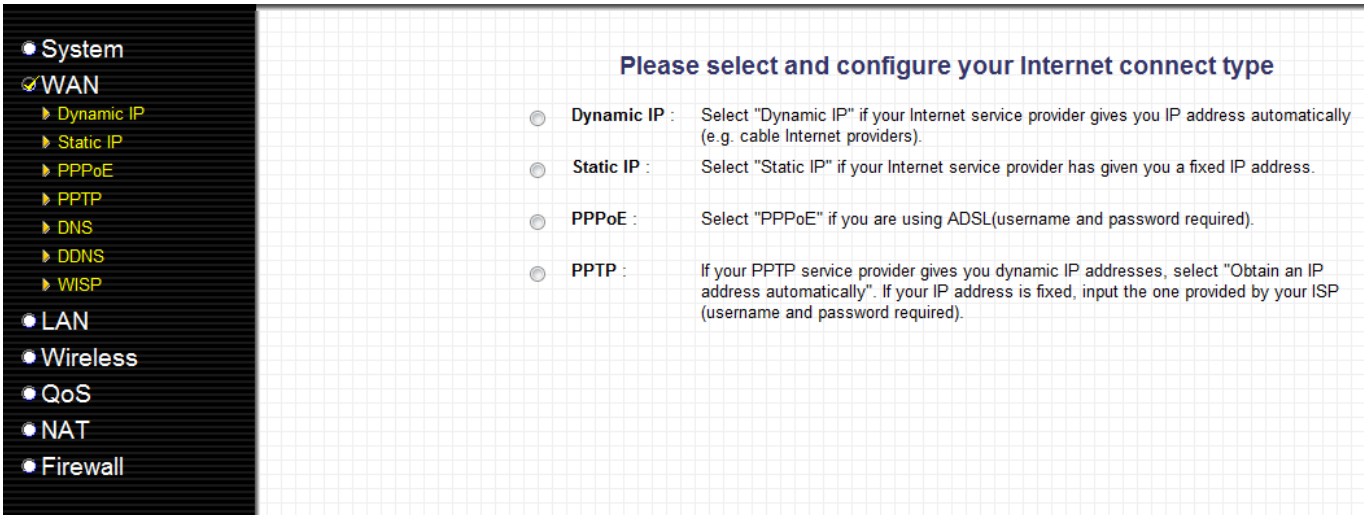
Click "APPLY" to restart the device and implement any changes. The device will restart itself.

III-3-2. WAN

Note: You will also arrive at this screen if you chose to setup your Internet connection manually, during iQ Setup for WISP Mode.

You can set up your Internet connection or WAN (Wide Area Network) under “WAN”. Select a connection type from the list.

Note: If you are not sure which connection type you should use, please contact your Internet Service Provider for help.



Please select and configure your Internet connect type

○ **Dynamic IP** : Select "Dynamic IP" if your Internet service provider gives you IP address automatically (e.g. cable Internet providers).

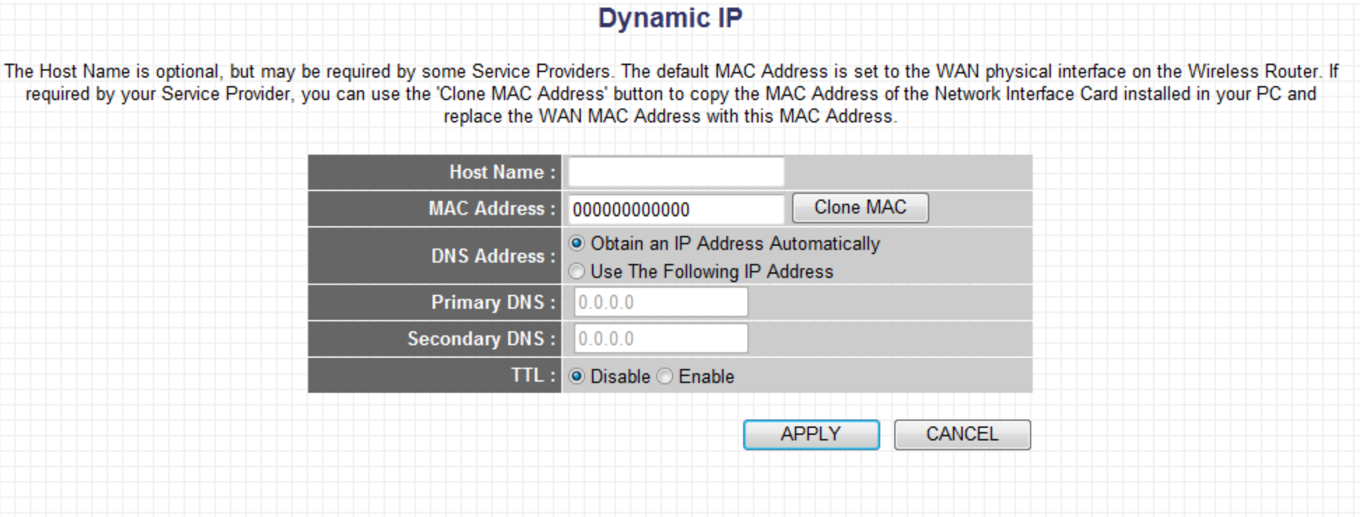
○ **Static IP** : Select "Static IP" if your Internet service provider has given you a fixed IP address.

○ **PPPoE** : Select "PPPoE" if you are using ADSL(username and password required).

○ **PPTP** : If your PPTP service provider gives you dynamic IP addresses, select "Obtain an IP address automatically". If your IP address is fixed, input the one provided by your ISP (username and password required).

III-3-2-1. Dynamic IP

If your Internet service provider assigns IP addresses to you automatically through DHCP (Dynamic Host Configuration Protocol), select “Dynamic IP”.



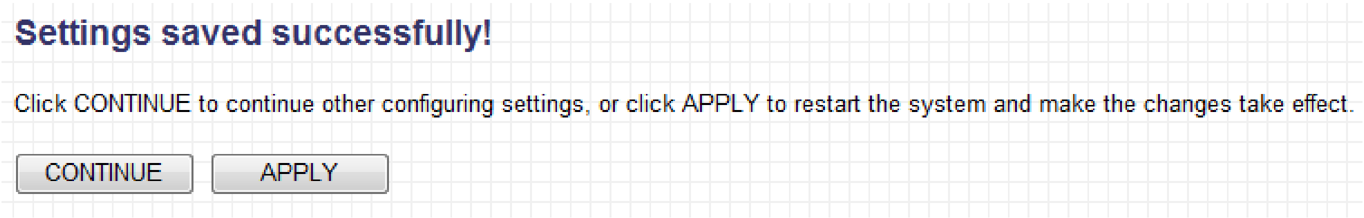
Dynamic IP

The Host Name is optional, but may be required by some Service Providers. The default MAC Address is set to the WAN physical interface on the Wireless Router. If required by your Service Provider, you can use the 'Clone MAC Address' button to copy the MAC Address of the Network Interface Card installed in your PC and replace the WAN MAC Address with this MAC Address.

Host Name :	
MAC Address :	000000000000 Clone MAC
DNS Address :	● Obtain an IP Address Automatically ○ Use The Following IP Address
Primary DNS :	0.0.0.0
Secondary DNS :	0.0.0.0
TTL :	● Disable ○ Enable

Host Name	Input the host name of your computer here. This is optional and only required if your ISP asks you to do so.
MAC Address	If your ISP only permits computers with certain MAC addresses to access the Internet, input your computer’s MAC address here. Press “Clone Mac address” to fill the MAC address field with your computer’s MAC address automatically.
DNS Address	Select “Use the following IP address” if your ISP requires that you do so.
DNS Address 1 and 2	Enter the primary and secondary DNS addresses assigned by your ISP here.
TTL	Enable the “TTL” function if your ISP requires you to do so.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

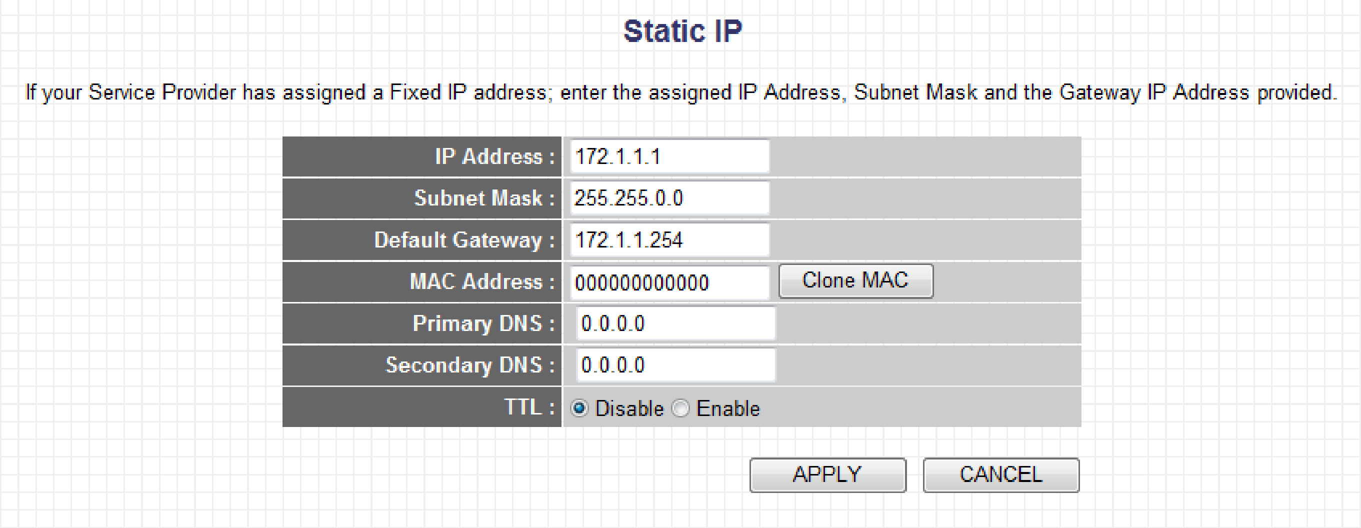
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-2-2. Static IP

If your ISP is providing you Internet access via a fixed IP address, select "Static IP". Generally, your ISP will provide you with such information as IP address, subnet mask, gateway address, and DNS address.



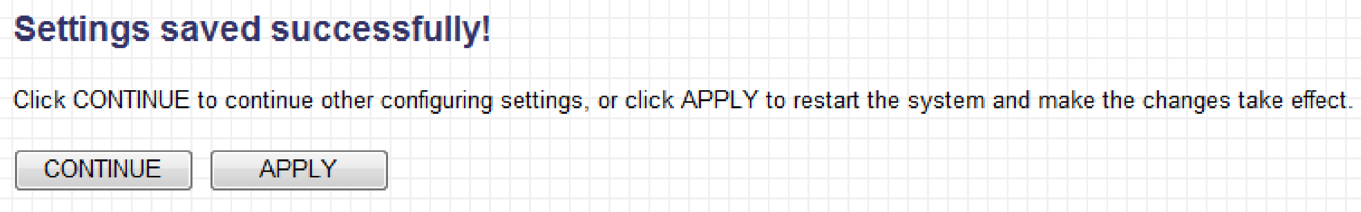
Static IP

If your Service Provider has assigned a Fixed IP address; enter the assigned IP Address, Subnet Mask and the Gateway IP Address provided.

IP Address :	172.1.1.1
Subnet Mask :	255.255.0.0
Default Gateway :	172.1.1.254
MAC Address :	000000000000
Primary DNS :	0.0.0.0
Secondary DNS :	0.0.0.0
TTL :	● Disable ○ Enable

IP Address	Input the IP address assigned by your ISP here.
Subnet Mask	Input the subnet mask assigned by your ISP here.
Default Gateway	Input the default gateway assigned by your ISP here. Some ISPs may call this "Default Route".
Mac Address	If your ISP only permits computers with certain MAC addresses to access the Internet, input your computer's MAC address here. Press "Clone Mac address" to fill the MAC address field with your computer's MAC address automatically.
DNS Address 1 and 2	Enter the primary and secondary DNS addresses assigned by your ISP here.
TTL	Enable the "TTL" function if your ISP requires you to do so.

Click "APPLY" to make the changes take effect. The following message will appear:



Settings saved successfully!

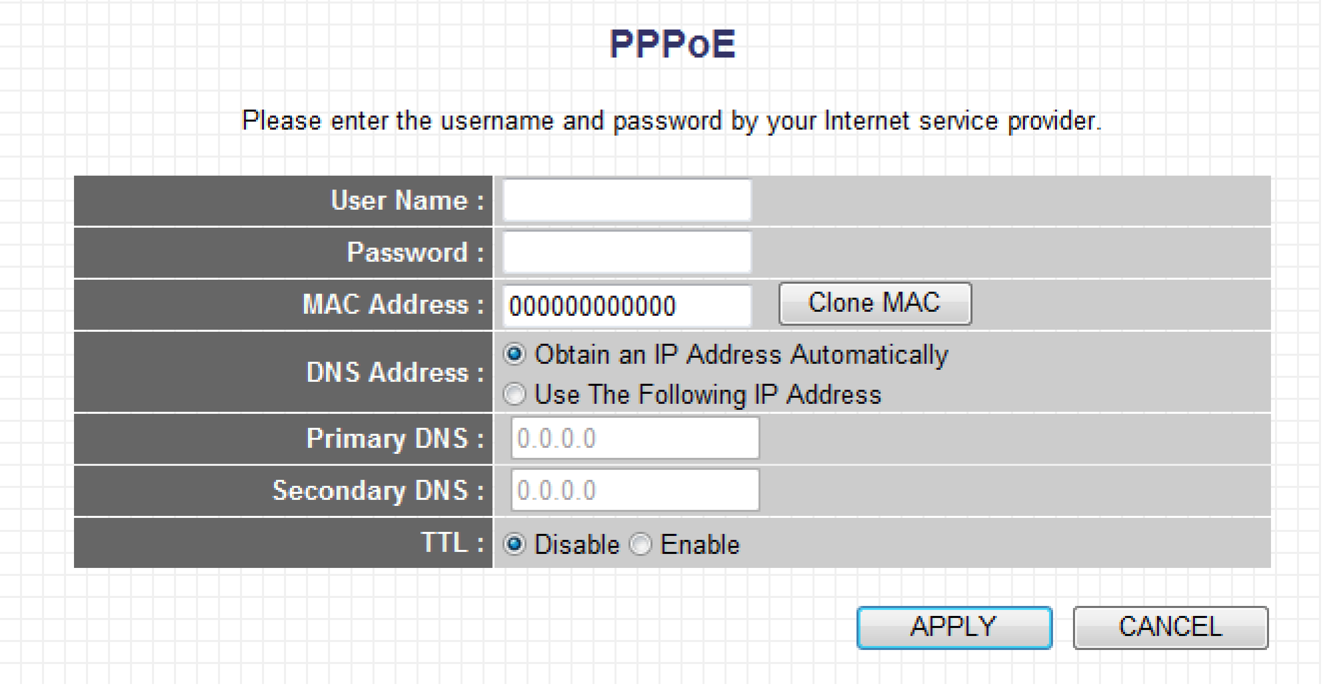
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-2-3. PPPoE

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



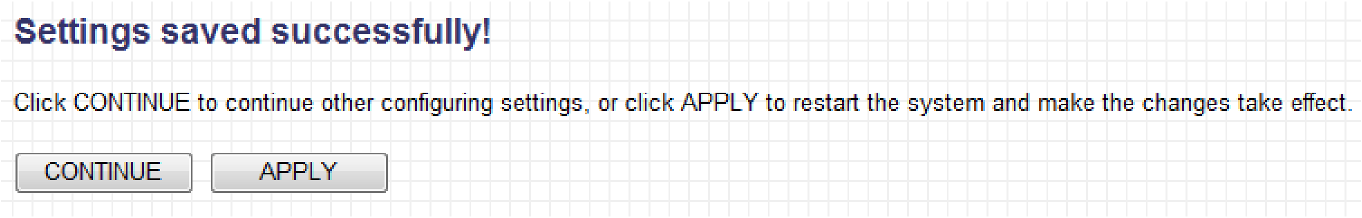
PPPoE

Please enter the username and password by your Internet service provider.

User Name :	
Password :	
MAC Address :	000000000000 Clone MAC
DNS Address :	● Obtain an IP Address Automatically ○ Use The Following IP Address
Primary DNS :	0.0.0.0
Secondary DNS :	0.0.0.0
TTL :	● Disable ○ Enable

User Name	Input the user name assigned by your ISP here.
Password	Input the password assigned by your ISP here.
MAC Address	If your ISP only permits computers with certain MAC addresses to access the Internet, input your computer’s MAC address here. Press “Clone Mac address” to fill the MAC address field with your computer’s MAC address automatically.
DNS Address	Select “Use the following IP address” if your ISP requires that you do so.
DNS Address 1 and 2	Enter the primary and secondary DNS addresses assigned by your ISP here.
TTL	Enable the “TTL” function if your ISP requires you to do so.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

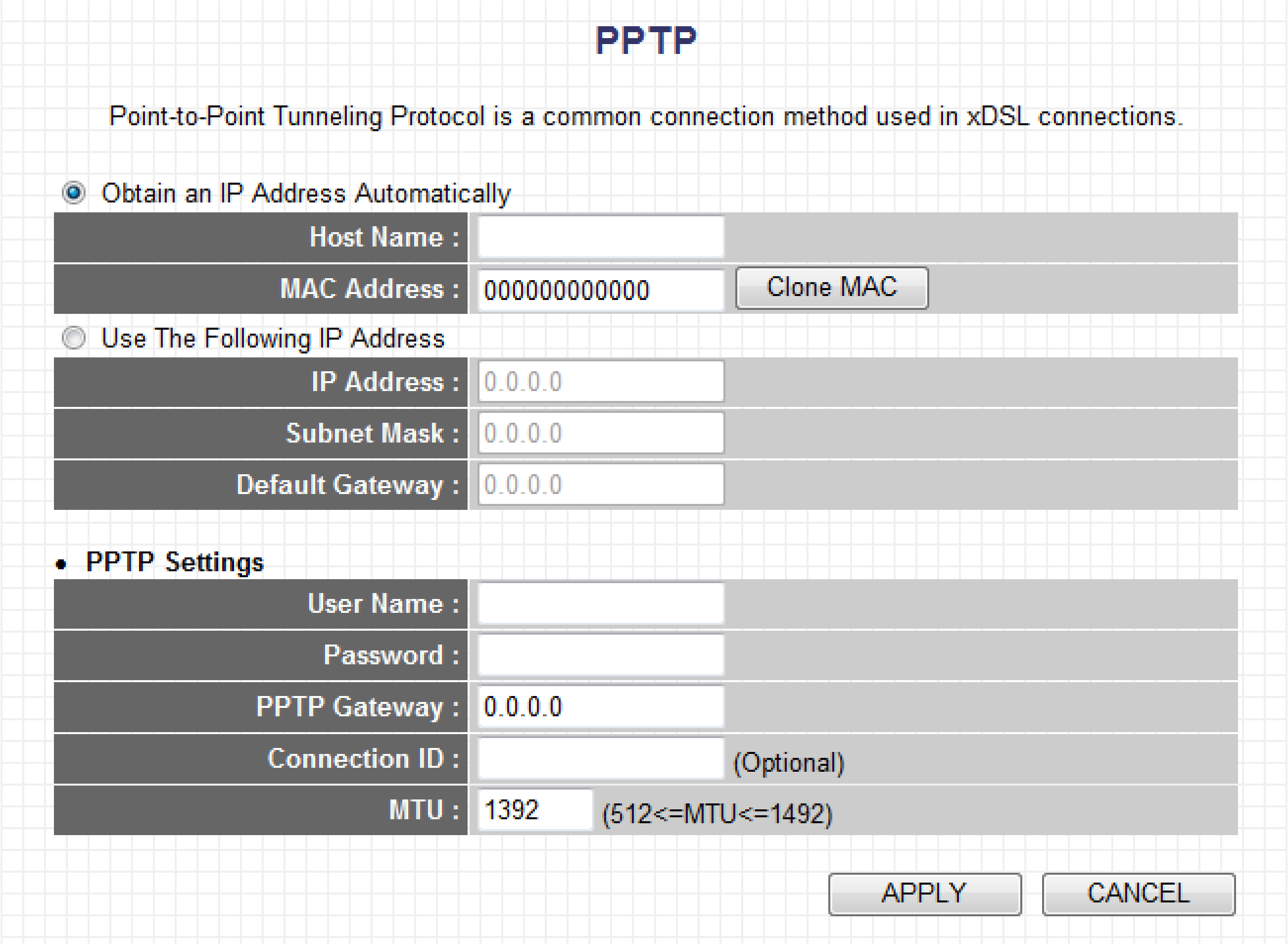
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-2-4. PPTP

Select “PPTP” if your ISP is providing you Internet access via PPTP (Point-to-Point Tunneling Protocol).
If your ISP is providing you dynamic IP addresses, select “Obtain an IP address automatically”. If your ISP is providing you a static IP address, select “Use the following IP address”.



PPTP

Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

● Obtain an IP Address Automatically

Host Name :	
MAC Address :	000000000000 Clone MAC

○ Use The Following IP Address

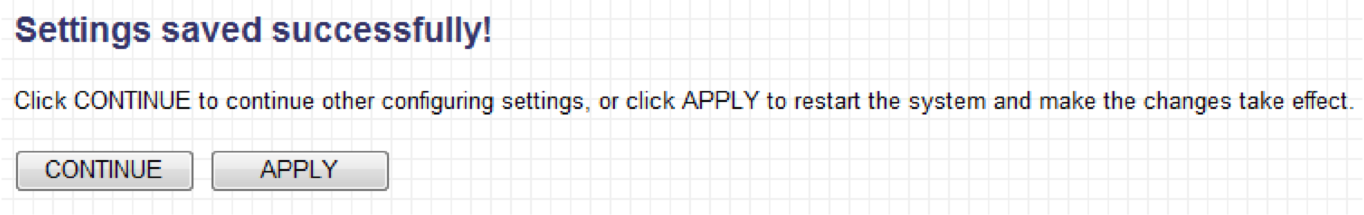
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0

- PPTP Settings

User Name :	
Password :	
PPTP Gateway :	0.0.0.0
Connection ID :	(Optional)
MTU :	1392 (512<=MTU<=1492)

Host Name	Input the host name of your computer here. This is optional and only required if your ISP asks you to do so.
MAC Address	If your ISP only permits computers with certain MAC addresses to access the Internet, input your computer’s MAC address here. Press “Clone Mac address” to fill the MAC address field with your computer’s MAC address automatically.
IP Address	Input the IP address assigned by your ISP here.
Subnet Mask	Input the subnet mask assigned by your ISP here.
Default Gateway	Input the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
User Name	Input the user name assigned by your ISP here.
Password	Input the password assigned by your ISP here.
PPTP Gateway	Input the PPTP gateway assigned by your ISP here.
Connection ID	Give this connection a name (optional).
MTU	Input the MTU value of your network connection here. If you do not know, use the default value.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

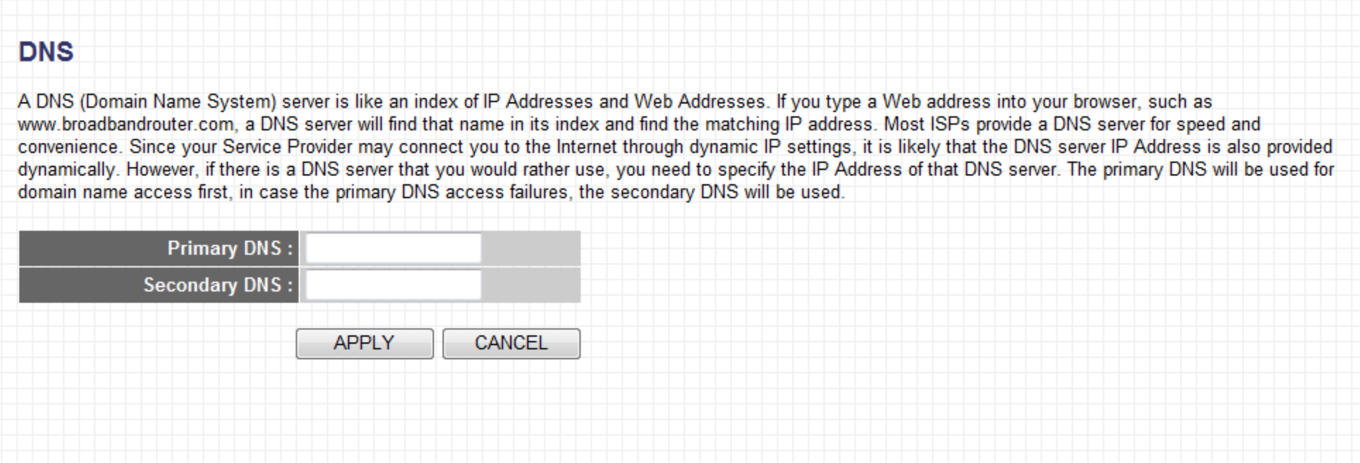
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-2-5. DNS

You can specify the IP address of a primary and secondary DNS server.

Note: In most cases, a DNS server IP address is provided dynamically by your ISP, and it is not necessary to enter a DNS server here.



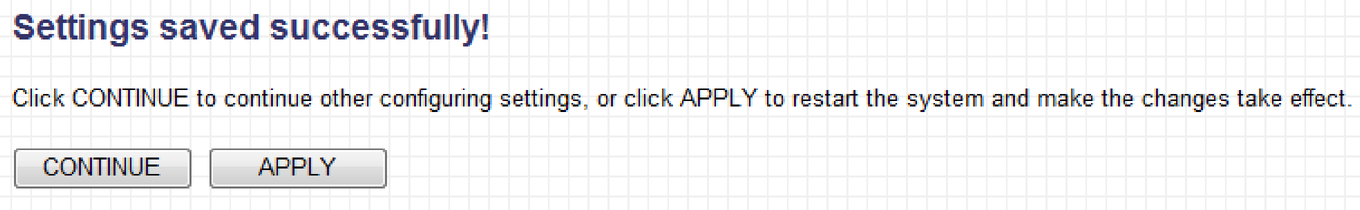
DNS

A DNS (Domain Name System) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

Primary DNS :	
Secondary DNS :	

Primary DNS	Input the primary DNS server IP address here.
Secondary DNS	Input the secondary DNS server IP address here.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

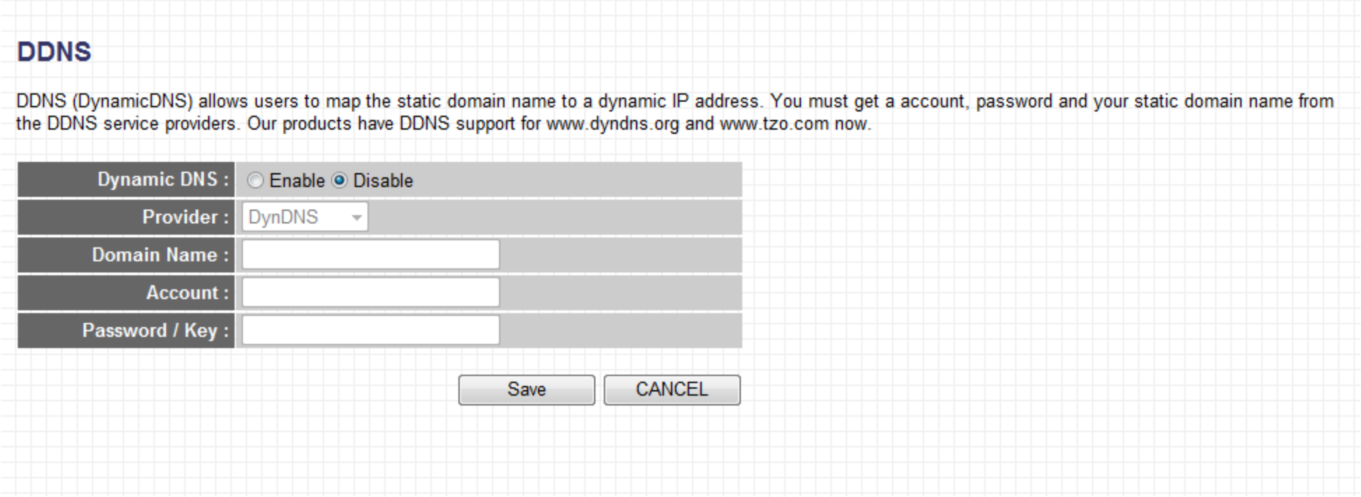
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-2-6. DDNS

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

Note: Dynamic IP users are those who will automatically be assigned a different IP address each time he or she connects to the Internet.



DDNS

DDNS (DynamicDNS) allows users to map the static domain name to a dynamic IP address. You must get a account, password and your static domain name from the DDNS service providers. Our products have DDNS support for www.dyndns.org and www.tzo.com now.

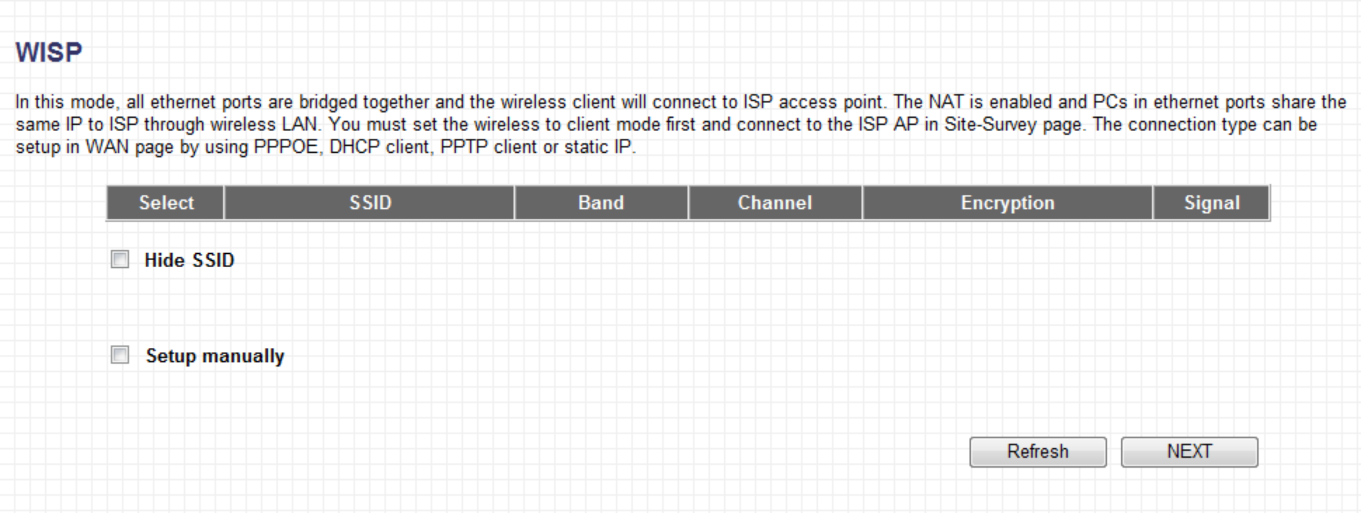
Dynamic DNS :	○ Enable ● Disable
Provider :	DynDNS
Domain Name :	
Account :	
Password / Key :	

Dynamic DNS	Select "Enable" or "Disable" to enable or disable DDNS function accordingly.
Provider	Select your DDNS service provider from the drop down menu.
Domain Name	Input the domain name you applied for or registered from a DDNS service provider (in the format xxx.xxx.xxx e.g. myrouter.homeip.net).
Account	Input the account (username or email address) that you used for DDNS registration.
Password / Key	Input DDNS service password or key.

Click "Save" to save the changes.

III-3-2-7. WISP

In WISP mode, the travel router receives a wireless signal and broadcasts it to multiple wireless devices. Please refer to **III-3. iQ Setup: WISP Mode** step 3 onwards, for guidance on configuring the travel router in WISP Mode.



WISP

In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client or static IP.

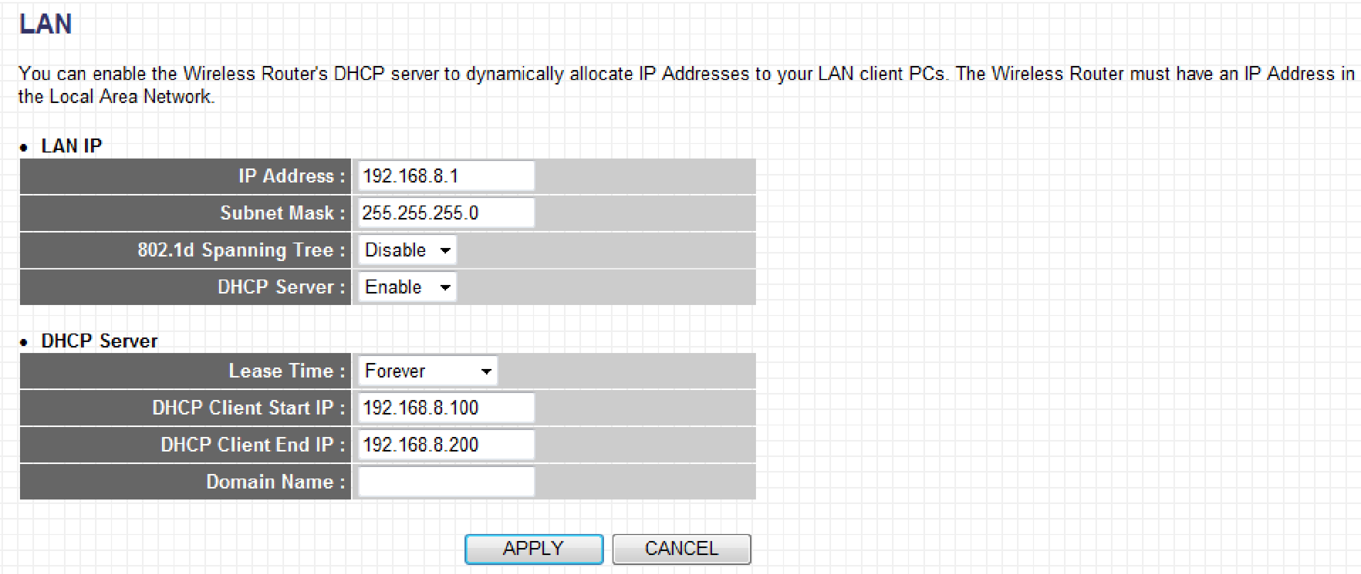
Select	SSID	Band	Channel	Encryption	Signal

□ Hide SSID

□ Setup manually

III-3-3. LAN

Here you can configure your LAN (Local Area Network). You can enable the travel router to dynamically allocate IP addresses to your LAN clients, and you can modify the IP address of the router.



LAN

You can enable the Wireless Router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The Wireless Router must have an IP Address in the Local Area Network.

- LAN IP

IP Address :	192.168.8.1
Subnet Mask :	255.255.255.0
802.1d Spanning Tree :	Disable
DHCP Server :	Enable

- DHCP Server

Lease Time :	Forever
DHCP Client Start IP :	192.168.8.100
DHCP Client End IP :	192.168.8.200
Domain Name :	

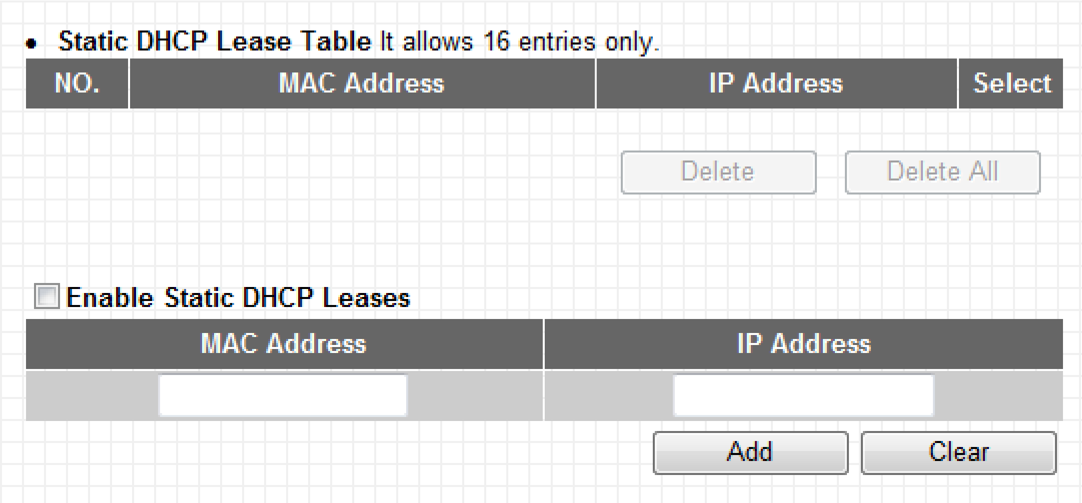
LAN IP	All LAN IP related information will be displayed here.
IP Address	Specify an IP address here. This IP address will be assigned to your access point, and will

	replace the default IP address 192.168.2.2.
Subnet Mask	Please input a subnet mask value for this network.
802.1d Spanning Tree	If you wish to activate the 802.1d spanning tree function, select “Enabled”.
DHCP Server	The device is active as a DHCP server for wireless devices to connect to. All DHCP Server related information will be displayed here.
Lease Time	Select a lease time for the DHCP leases here. The DHCP client will be forced to obtain a new IP address after the period expires. You can select “Forever” if you are using this broadband router with less than 30 computers.
DHCP Client Start IP	Enter the start IP address for the DHCP server’s IP assignment.
DHCP Client End IP	Enter the end IP address for the DHCP server’s IP assignment.
Domain Name	You can input a domain name for your network (optional).

Note: If you assigned a new IP address to the router, please make a note and remember it. If you forget this IP address, you may not be able to connect to the browser-based configuration interface in the future. If so, try using the default access key http://edimax.go.

Note: To reset the IP address back to its default value of 192.168.8.1, press and hold the **Reset/WPS** button on the router for 10 seconds. Be aware that doing so restores **all** settings and passwords back to factory defaults.

You can also set the router to assign a static IP address to specified computers or devices.



- **Static DHCP Lease Table** It allows 16 entries only.

NO.	MAC Address	IP Address	Select

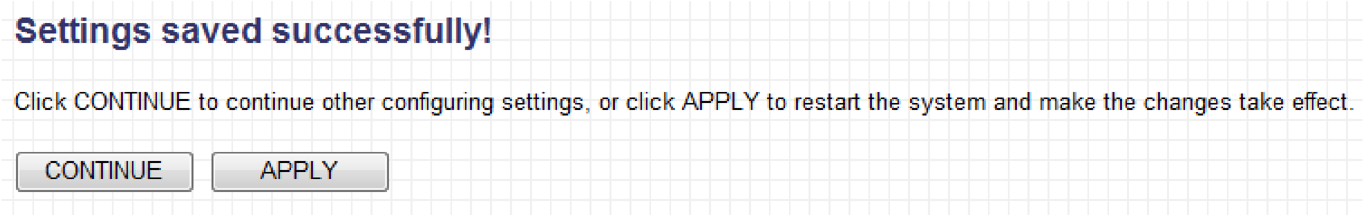
□ **Enable Static DHCP Leases**

MAC Address	IP Address

Enable Static DHCP Leases	Check this box to enable the function.
MAC Address	Input the specified computer’s MAC address here.
IP Address	Assign a fixed IP address for the specified computer here.
Add	After you have entered the MAC address and the IP address, click “Add” to add the information to the “Static DHCP Leases Table”.
Clear	Click “Clear” to clear the MAC address and IP address fields.

Check the box labeled “Enable Static DHCP Leases” to enable this function and then input the required values. Assigned entries will be listed in the table “Static DHCP Lease Table”. Up to 16 static DHCP leases can be assigned this way.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

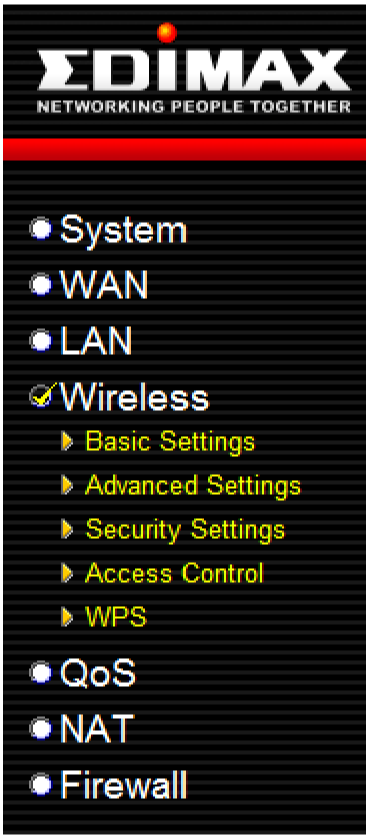
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

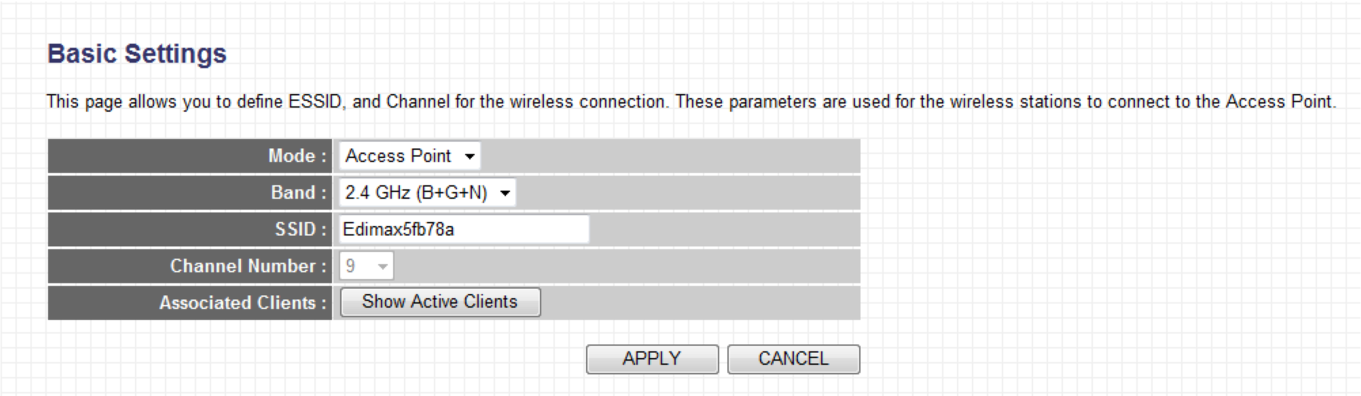
III-3-4. Wireless

You can configure wireless network settings using the sub menu under “Wireless” on the left side of the screen, as shown below.



III-3-4-1. Basic Settings

You can configure basic wireless settings here.



Basic Settings

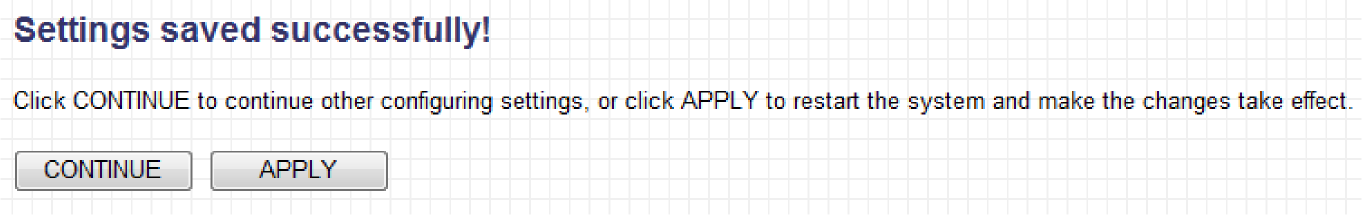
This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	Access Point
Band :	2.4 GHz (B+G+N)
SSID :	Edimax5fb78a
Channel Number :	9
Associated Clients :	Show Active Clients

Mode	The default mode of the router is “Access

	Point" and cannot be modified. Access Point mode means the device bridges an existing wired or wireless network with a wireless client.
Band	Select from one of the following options: 2.4GHz (B): Allows 802.11b wireless network clients to connect to this router (maximum transfer rate 11Mbps). 2.4GHz (N): Allows 802.11n wireless network clients to connect to this router (maximum transfer rate 450Mbps). 2.4GHz (B+G): Allows 802.11b and 802.11g wireless network clients to connect to this router (maximum transfer rate 11Mbps for 802.11b clients and 54Mbps for 802.11g clients). 2.4GHz (G): Allows 802.11g wireless network clients to connect to this router (maximum transfer rate 54Mbps). 2.4GHz (B+G+N): Allows 802.11b, 802.11g, and 802.11n wireless clients to connect to this router (recommended).
SSID	This is the name of your router. You can type any alphanumerical character here (maximum 32 characters).
Channel Number	Select a channel from the dropdown menu. You can select the channel of your preference (from 1 to 13, subject to local regulations).
Associated Clients	Click "Show Active Clients" for the list of all connected wireless clients. Click "Refresh" in the new window to renew the list, and click "Close" to close the window. Note: If you have a pop-up blocker installed, you may have to disable it, or set it to allow the pop-up window to show up.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

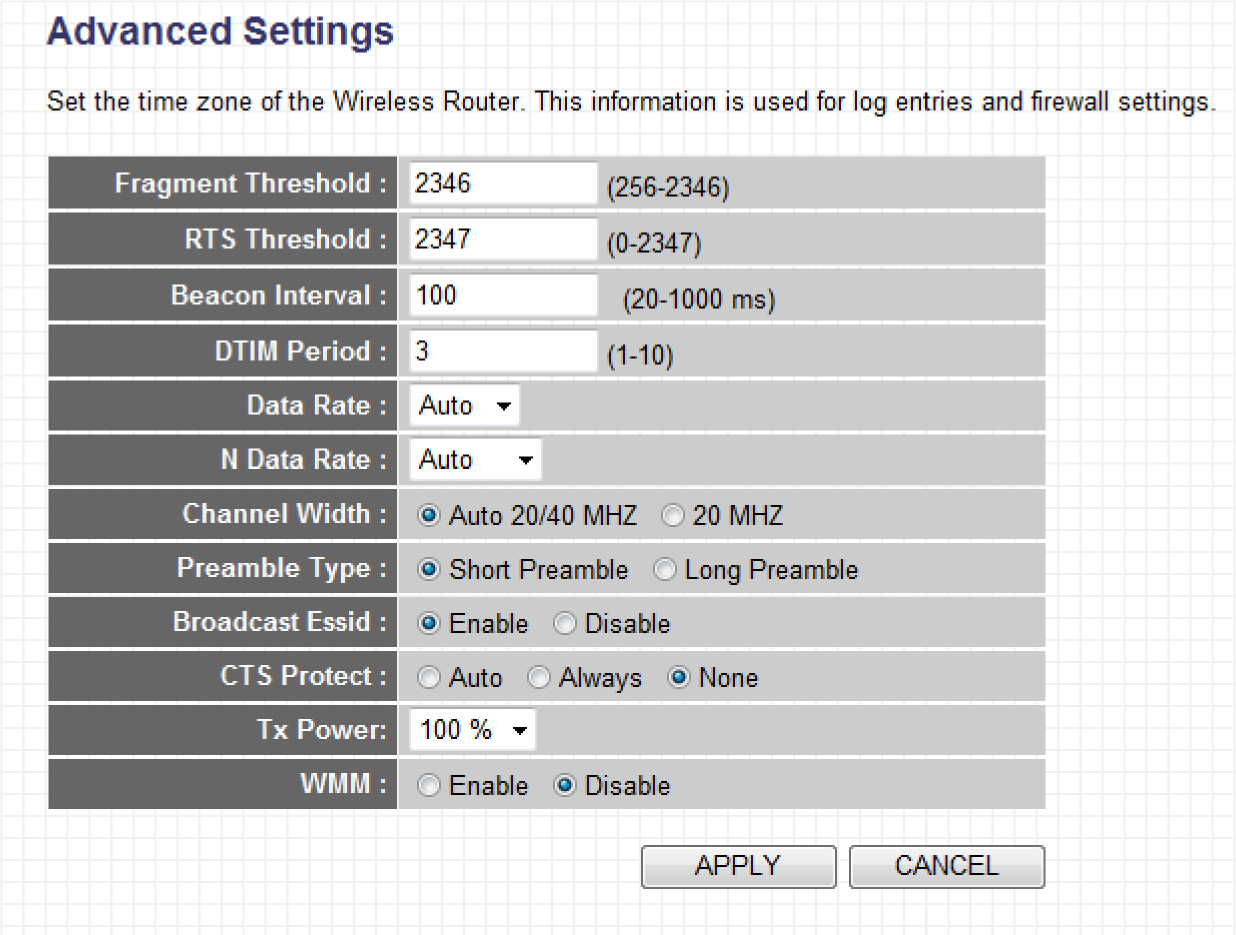
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-4-2. Advanced Settings

You can configure advanced wireless settings here.

Note: Advanced 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.



Advanced Settings

Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.

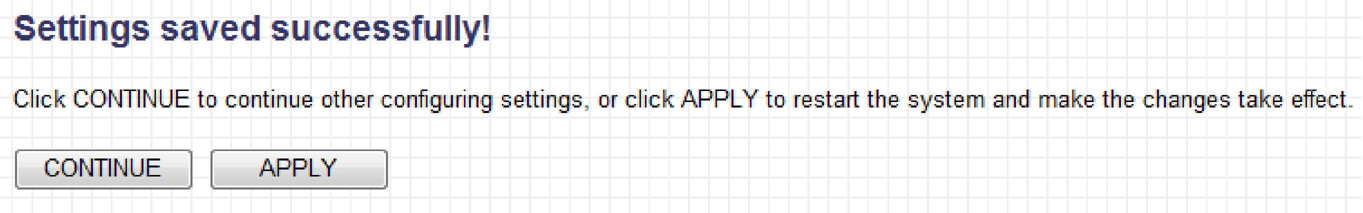
Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2347 (0-2347)
Beacon Interval :	100 (20-1000 ms)
DTIM Period :	3 (1-10)
Data Rate :	Auto
N Data Rate :	Auto
Channel Width :	● Auto 20/40 MHZ ○ 20 MHZ
Preamble Type :	● Short Preamble ○ Long Preamble
Broadcast Essid :	● Enable ○ Disable
CTS Protect :	○ Auto ○ Always ● None
Tx Power:	100 %
WMM :	○ Enable ● Disable

Fragment Threshold	Set the Fragment threshold of the wireless radio. **Please do not modify the default value if you don't know what this does, the default value is 2346**
RTS Threshold	Set the RTS threshold of the wireless radio. **Please do not modify the default value if you don't know what this does, the default value is 2347**
Beacon Interval	Set the beacon interval of the wireless

	radio. **Please do not modify the default value if you don't know what this does, the default value is 100**
DTIM Period	Set the DTIM period of wireless radio. **Please do not modify default value if you don't know what it is, the default value is 3**
Data Rate	Set the wireless data transfer rate. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.**
N Data Rate	Set the data rate of 802.11n clients, available options are MCS 0 to MCS 15. It's safe to set this option to "Auto" and **it's not necessary to change this value unless you know what will happen after modification.**
Channel Width	Select wireless channel width (bandwidth used by wireless signals from the travel router). It's suggested you select "Auto 20/40MHz". Do not change to "20 MHz" unless you know what that does.
Preamble Type	Set the wireless radio preamble type. **Please do not modify the default value if you don't know what this does, the default value is "Short Preamble".**
Broadcast ESSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your travel router (set the option to "Disable"), so only people who know the ESSID of your travel router can connect to it.
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	You can set the output power of the wireless radio. Unless you're using the travel router in a very large space, you may not require 100% output power. **This will enhance security (malicious/unknown users in distant areas will not be able to**

	reach your router).
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the travel router will define the priority of different kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

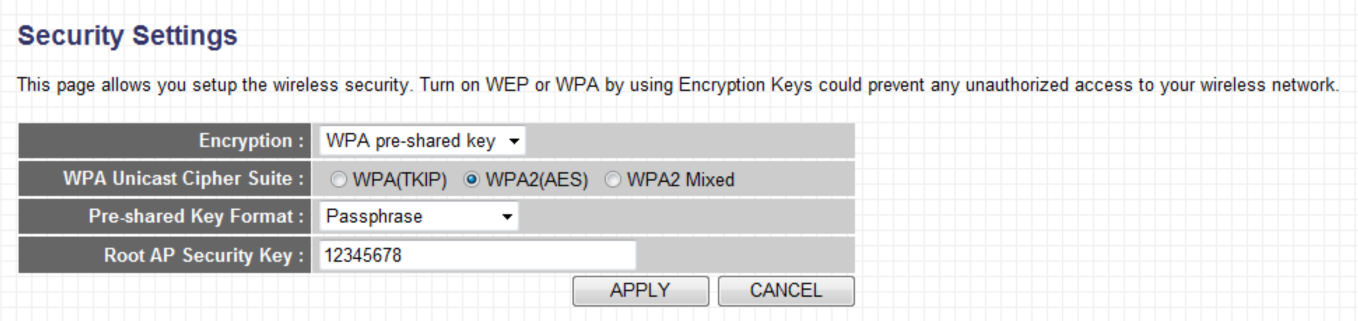
Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-4-3. Security Settings

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

Note: It is highly recommended that you set up wireless security. Without security enabled, intruders could gain access to your local network and cause damage to your computers and servers.

Security Tips:
- Use complicated, hard-to-guess phrases as your security password. Include random combinations of letters, numbers and symbols.
- Use WPA encryption if possible. It's more secure than WEP. WPA2(AES) is recommended.
- Change your security password regularly.



Security Settings

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

Encryption :	WPA pre-shared key ▾
WPA Unicast Cipher Suite :	○ WPA(TKIP) ● WPA2(AES) ○ WPA2 Mixed
Pre-shared Key Format :	Passphrase ▾
Root AP Security Key :	12345678

Select the type of encryption you wish to use from the drop down menu labeled "Encryption".

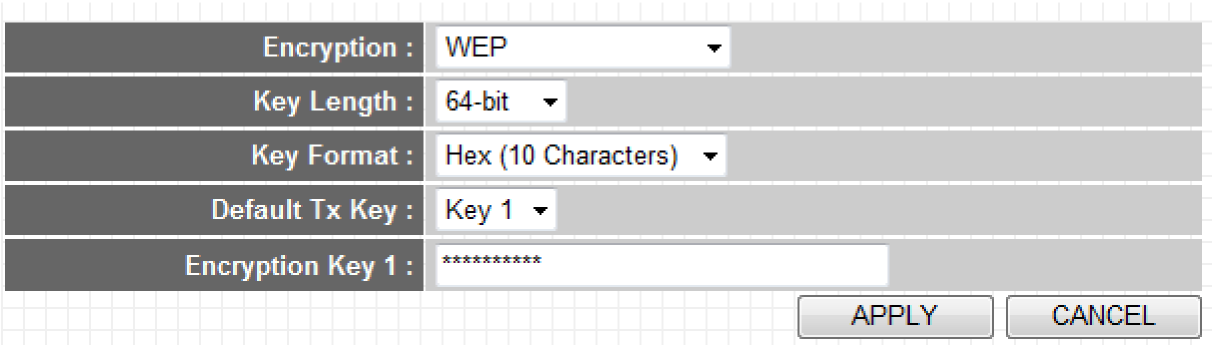
Disable

When you select "Disable", wireless encryption for the network is disabled. This means anyone who knows the device's SSID can connect to it, and is not recommended.

WEP

WEP (Wired Equivalent Privacy) is a simple encryption type. For a higher level of security, please consider using WPA encryption if possible.

Note: Most wireless devices support WPA encryption, though some legacy wireless devices only support WEP encryption.
WEP only supports up to 54Mbps transmission data rate.



Encryption : WEP

Key Length : 64-bit

Key Format : Hex (10 Characters)

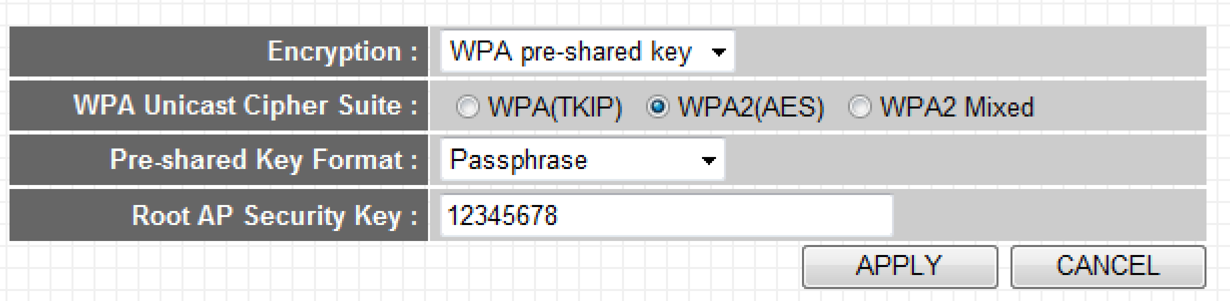
Default Tx Key : Key 1

Encryption Key 1 : **********

Key Length	There are two types of WEP key length: 64-bit and 128-bit. Using "128-bit" is safer than "64-bit", but will reduce some data transfer performance.
Key Format	There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of the key will be displayed. For example, if you select a "64-bit" key length, and "Hex" as the key format, you'll see the message "Hex (10 characters)" to the right, which means the length of the WEP key is 10 characters.
Default Tx Key	You can set up to four sets of WEP keys, and you can decide which key is used the default. **If you don't know which one you should use, select "Key 1".**
Encryption Key 1	Input WEP key characters here, the number of characters must be the same as the number displayed in the "Key Format" field. If you select the "ASCII" key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). If you select "Hex" as the key format, you can use the characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same as each other.

WPA pre-shared key

WPA pre-shared key is the safest encryption method, and it is recommended that you use this type of encryption.

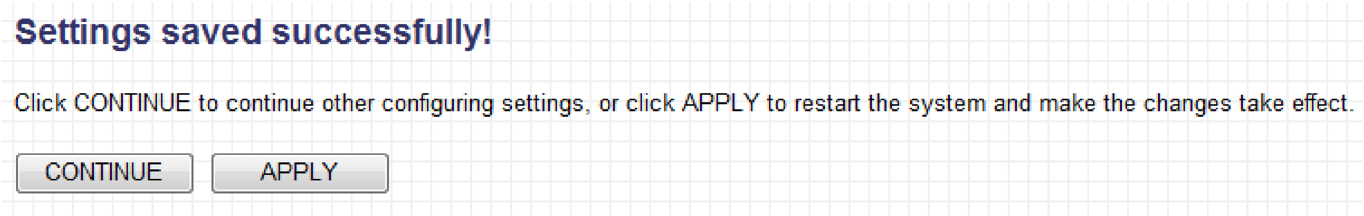


Encryption :	WPA pre-shared key
WPA Unicast Cipher Suite :	○ WPA(TKIP) ● WPA2(AES) ○ WPA2 Mixed
Pre-shared Key Format :	Passphrase
Root AP Security Key :	12345678

WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. AES is safer than TKIP, but not every wireless client supports it. Please make sure your wireless client supports the cipher you selected. **Our default is WPA2(AES), if your wireless device can not support AES, you can change to WPA2 Mixed.**
Pre-shared Key Format	Please select the format of the pre-shared key here, available options are "Passphrase" (8 to 63 alphanumerical characters) and "Hex (64 characters)" – 0 to 9 and a to f.
Root AP Security Key	Please enter the key according to the key format you selected above. For security reasons, it's best to use a complex, hard-to-guess key.

Note: TKIP only supports up to 54Mbps transmission data rate.

Click "APPLY" to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

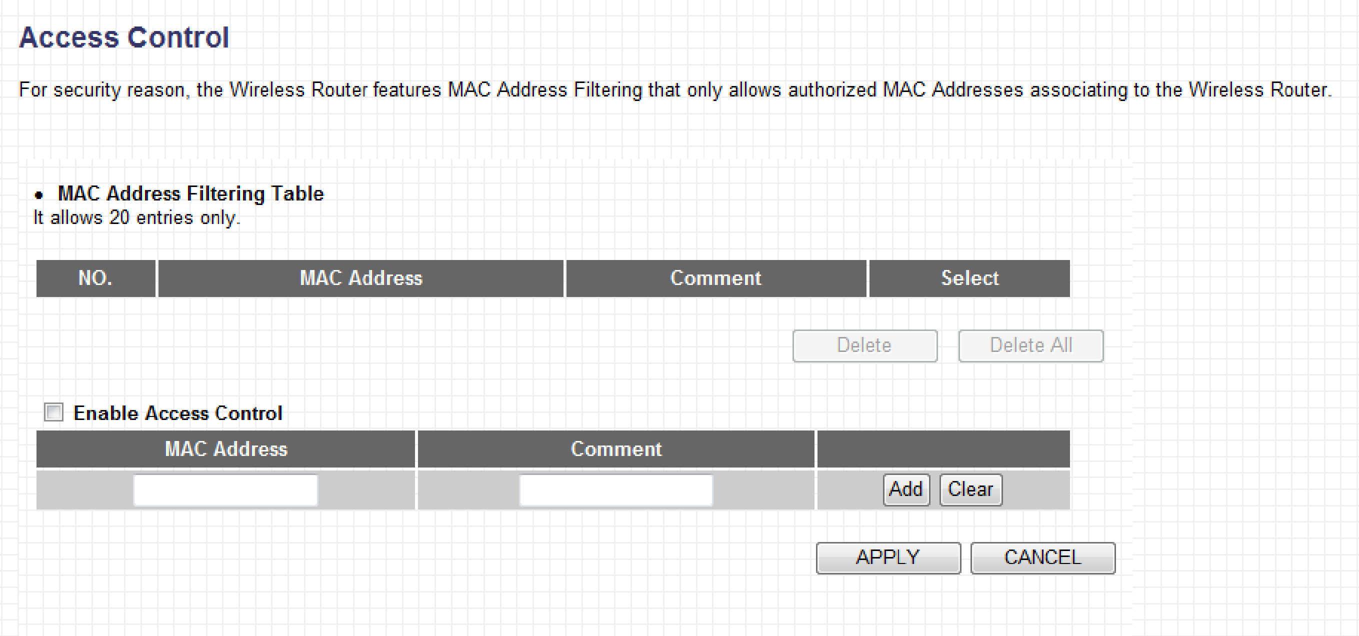
Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-4-4. Access Control

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

This function allows you to define a list of wireless devices permitted to connect to the travel router. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the travel router, it will be denied. Up to 20 MAC addresses can be assigned.

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



Access Control

For security reason, the Wireless Router features MAC Address Filtering that only allows authorized MAC Addresses associating to the Wireless Router.

- MAC Address Filtering Table

It allows 20 entries only.

NO.	MAC Address	Comment	Select

□ Enable Access Control

MAC Address	Comment	
		Add Clear

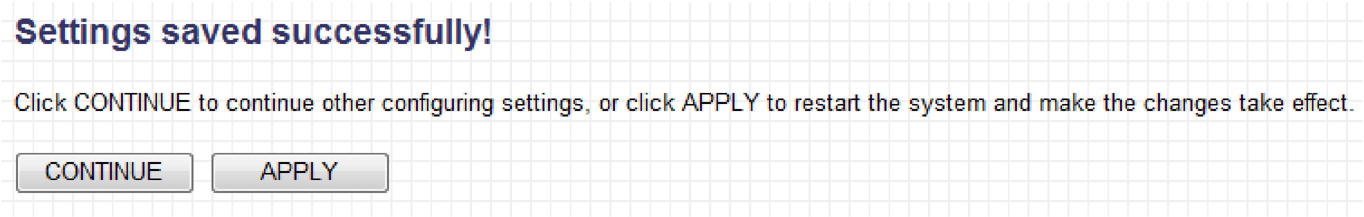
MAC addresses which have been added to the permitted list will be displayed in the table “MAC Address Filtering Table”. To delete one or more entries, please check the box of the corresponding entry (under “Select”), and click “Delete Selected”. If you wish to delete all the entries, click “Delete All”.

In the next table, you can add MAC addresses to the list.

MAC Address	Input the MAC address you wish to add here.
Comment	You can input up to 16 alphanumerical

	characters describing the MAC address here (optional).
Add	Click “Add” to add the MAC address and associated comment to the MAC address list.
Clear	Click “Clear” to remove everything in the MAC address and comment fields.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

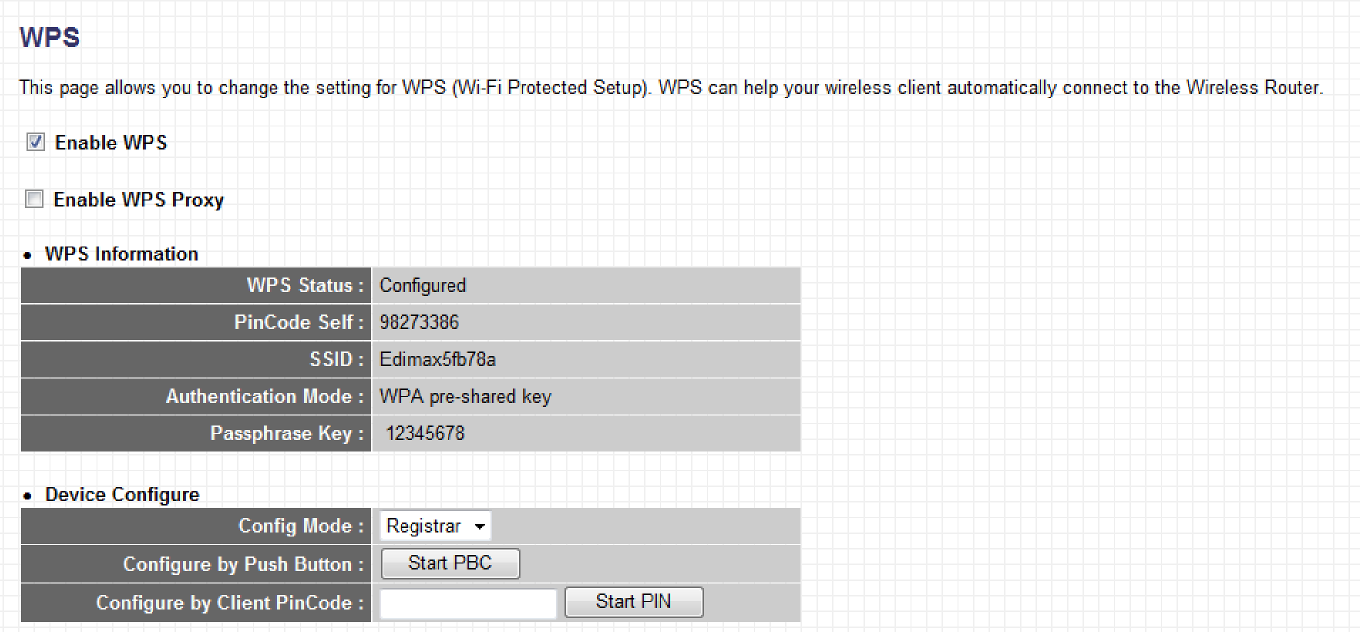
III-3-4-5. WPS

Wi-Fi Protected Setup (WPS) is a simple and convenient way to build a connection between the travel router and wireless network clients. This function eliminates the need to select an encryption mode and enter an encryption passphrase each time you want to set up a connection. You can build a connection simply by pressing a button on both the travel router and the wireless client.

This router supports two types of WPS: **Push-Button Configuration (PBC)** and **PIN code**.

To use **PBC** you will need to activate WPS by pushing the Reset/WPS button, or by clicking “Start PBC” in the “WPS” screen; and to activate WPS in the wireless client by pushing a WPS button.

To use **PIN code**, you will need to enter the PIN code of the wireless client you wish to connect to, and then activate WPS in the wireless client.



WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). WPS can help your wireless client automatically connect to the Wireless Router.

☑ Enable WPS

□ Enable WPS Proxy

- WPS Information

WPS Status :	Configured
PinCode Self :	98273386
SSID :	Edimax5fb78a
Authentication Mode :	WPA pre-shared key
Passphrase Key :	12345678

- Device Configure

Config Mode :	Registrar
Configure by Push Button :	Start PBC
Configure by Client PinCode :	Start PIN

Enable WPS	Check this box to enable or disable WPS
WPS Information	All information related to WPS will be displayed here.
WPS Status	Displays WPS status. If data encryption settings for the router have never been set, “unConfigured” will be shown here. If data encryption settings have been set, “Configured” will be shown here.
Device PIN Code	This is the WPS PIN code of travel router. It’s an 8-digit number, used when you need to build a wireless connection by WPS with other WPS-enabled wireless devices.
SSID	Displays the SSID (ESSID) of this router.
Authentication Mode	The wireless security authentication mode of this router will be shown here. If you don’t enable the security functions of the router before WPS is activated, the router will automatically set the security to WPA (AES) and generate a passphrase key for WPS connection.
Passphrase Key	Shows the WPA passphrase here, though all characters will be replaced by asterisks for security reasons. If encryption is not set on the router, this field will be blank.
Device Configuration	Configuration options for the device’s WPS settings can be found here.

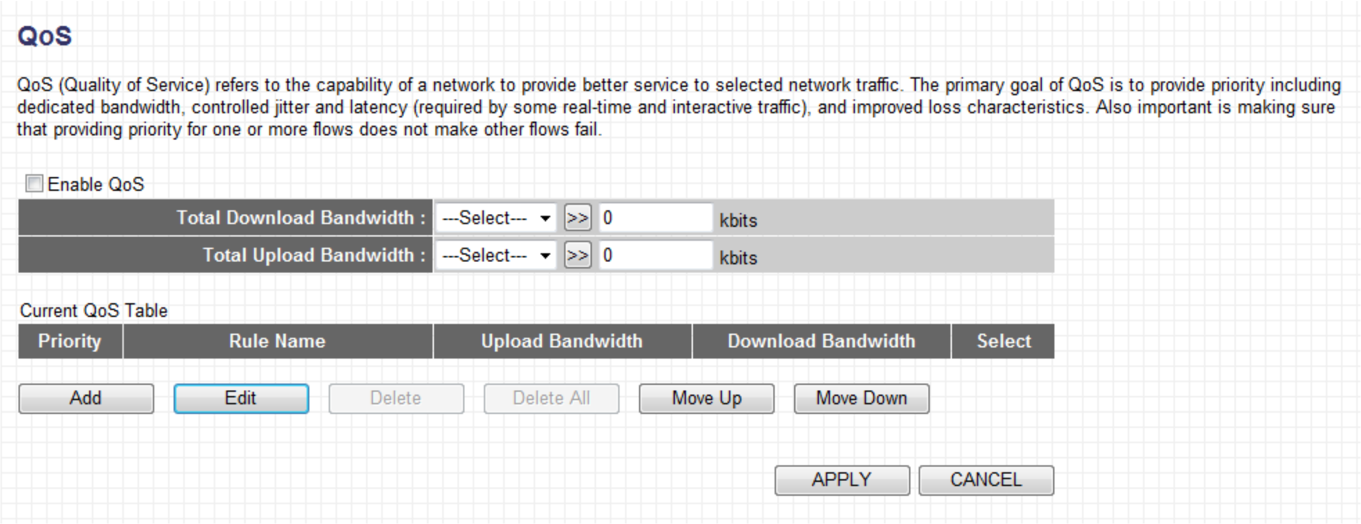
Config Mode	There are “Registrar” and “Enrollee” modes for the WPS connection. When “Registrar” is enabled, the wireless clients will follow the router’s wireless settings for WPS connections. When “Enrollee” mode is enabled, the router will follow the wireless settings of wireless client for WPS connections.
Configure via Push Button	Click “Start PBC” to start Push-Button style WPS setup. This router will wait for WPS requests from wireless clients for 2 minutes. The green WPS LED on the router will blink for 2 minutes while it waits for incoming WPS requests.
Configure by Client PIN Code	Please input the PIN code of the wireless client you wish to connect, and click the “Start PIN” button. The green WPS LED on the router will blink for 2 minutes while it waits for incoming WPS requests.

Note: When using PBC-type WPS setup, you must press the hardware or software WPS button on the wireless client within 120 seconds of doing so on the router. If you do not do so in time, you will need to activate WPS on the router again.

III-3-5. QoS

Quality of service (QoS) is a function which allows you to allocate a certain amount of bandwidth to specific computer. This can ensure that applications which require guaranteed bandwidth e.g. video conference or network telephone applications, are able to function properly and without interruption. Conversely, you can also limit the maximum bandwidth available to a specific computer or application.

Check the “Enable QoS” box to enable this function and then enter the desired values.



QoS

QoS (Quality of Service) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

□ Enable QoS

Total Download Bandwidth :	---Select--- >> 0 kbits
Total Upload Bandwidth :	---Select--- >> 0 kbits

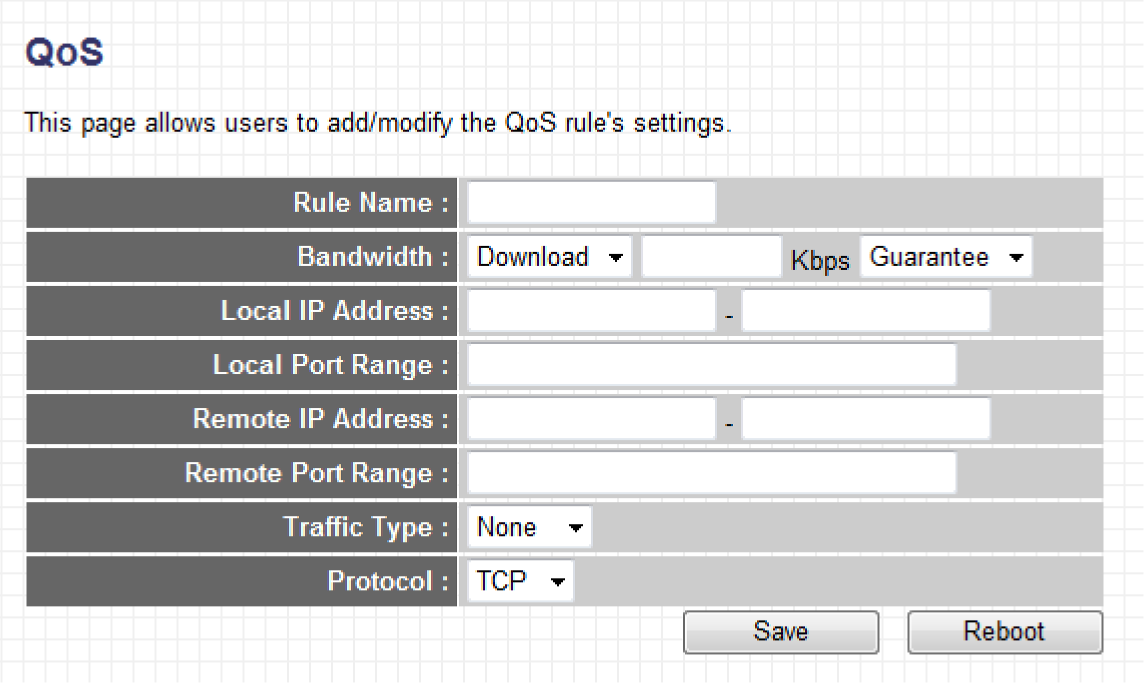
Current QoS Table

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select

Enable QoS	Check this box to enable QoS function, uncheck it to disable QoS.
Total Download Bandwidth	You can set the limit of total download bandwidth in kbits. To disable download bandwidth limitation, input '0' here.
Total Upload Bandwidth	You can set the limit of total upload bandwidth in kbits. To disable upload bandwidth limitation, input '0' here.

When you assign a particular bandwidth guarantee/limit to a specific computer, it is known as a rule. Existing rules will be listed in the table "Current QoS Table".

Add	Click "Add" to create a new QoS rule. This will open a new window, see below.
Edit	To edit an existing rule, please check the "Select" box of the corresponding rule, then click "Edit". **Please do not select more than one rule to edit at a time.**
Delete Selected	Delete one or more selected rules. If the QoS table is empty, this button will be grayed out.
Delete All	Deletes **all** rules currently listed in the QoS table. If the QoS table is empty, this button will be grayed out.
Move Up	Moves selected rule up, assigning it a higher priority.
Move Down	Moves selected rule down, assigning it a lower priority.



QoS

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

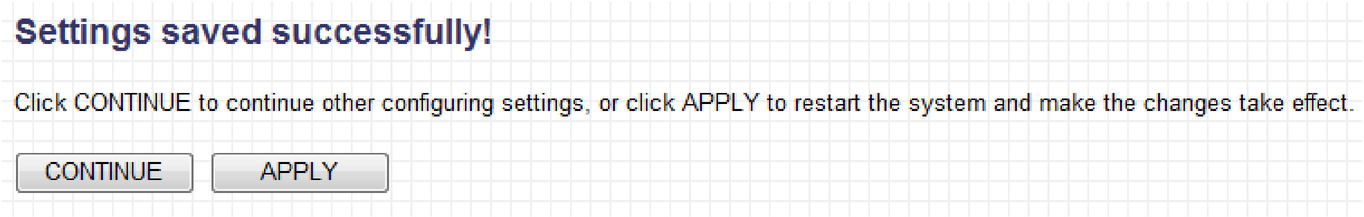
Rule Name :	
Bandwidth :	Download ▾ Kbps Guarantee ▾
Local IP Address :	-
Local Port Range :	
Remote IP Address :	-
Remote Port Range :	
Traffic Type :	None ▾
Protocol :	TCP ▾

Rule Name	Input a unique name for this QoS rule for reference.
Bandwidth	Set the bandwidth values for this QoS rule. Select “Download” or “Upload” for traffic type, and input the bandwidth in Kbps which will be assigned to this rule. Select “Guarantee” (minimum bandwidth allocated to this rule) or “Maximum” (maximum bandwidth assigned to this rule) as the type of rule.
Local IP Address	Set the IP address range that will be affected by this QoS rule. If only one IP address is involved, input the IP address in left field only.
Local Port Range	Set the port range that will activate this QoS rule. If only one port is involved, input a single number here (1 to 65535); if multiple ports are involved, input starting / ending port number in x-y format (like 10-20).
Remote IP Address	Set remote IP addresses that will trigger this QoS rule. If only one IP address is involved, input the IP address in left field only.

Remote Port Range	Set the port range that will activate this QoS rule. If only one port is involved, input a single number here (1 to 65535); if multiple ports are involved, input starting / ending port number in x-y format (like 10-20).
Traffic Type	If you’re creating a QoS rule for a specific type of traffic, you can select it from this menu and you don’t have to input port range above.
Protocol	Select the protocol type here (TCP or UDP).

Click “Save” to save the changes and return to the QoS page. Click “Reset” to clear all fields on this page.

Click “APPLY” to make the changes take effect. The following message will appear:



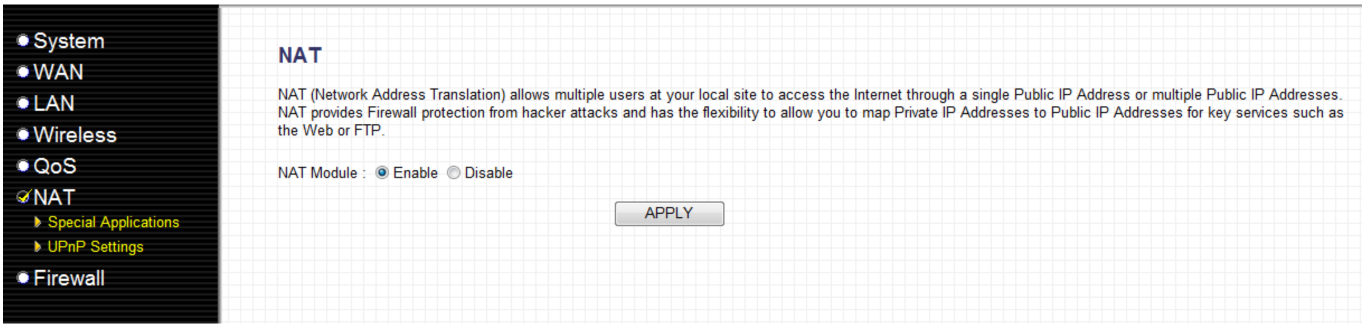
Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-6. NAT



NAT

NAT (Network Address Translation) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.

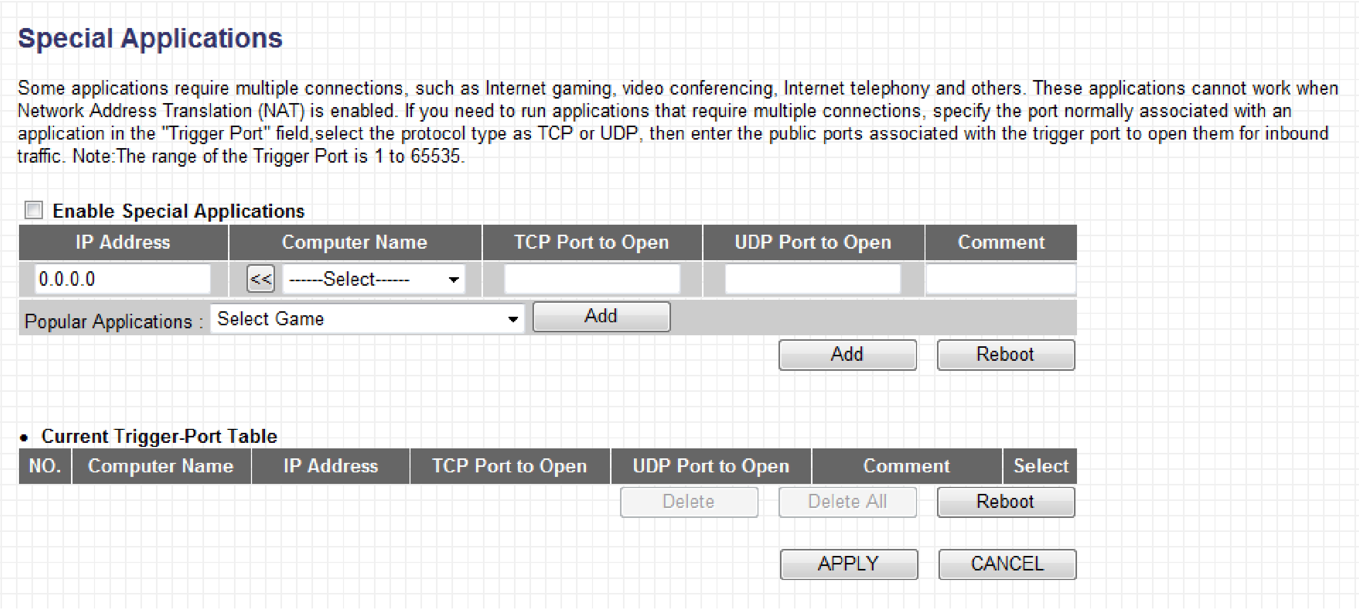
NAT Module : ● Enable ○ Disable

Network Address Translation (NAT) is a function which allows multiple users in a local network to share a single or multiple IP addresses. Click “Enable” or

"Disable" to enable or disable the NAT module accordingly. There are two headings under the "NAT" menu which you can choose from.

III-3-6-1. Special Applications

Some applications, such as video conferencing or network telephone applications, require multiple connections to function and so cannot work when NAT is enabled. In this case, you can configure NAT settings under "Special Applications" to allow multiple connections for specific applications.



Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field,select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic. Note:The range of the Trigger Port is 1 to 65535.

□ Enable Special Applications

IP Address	Computer Name	TCP Port to Open	UDP Port to Open	Comment
0.0.0.0	<< ------Select------			

Popular Applications : Select Game

- Current Trigger-Port Table

NO.	Computer Name	IP Address	TCP Port to Open	UDP Port to Open	Comment	Select

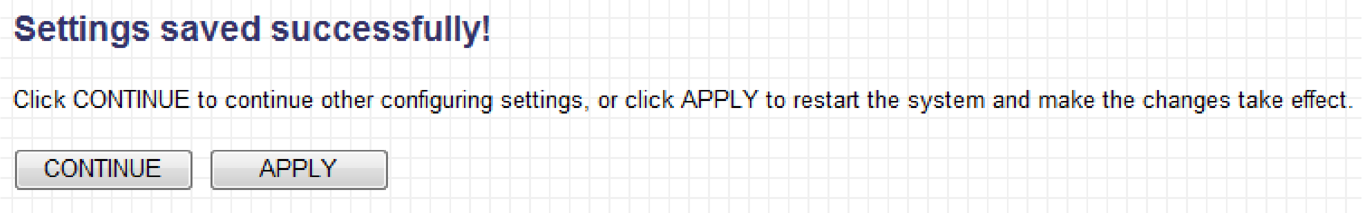
Enable Special Applications	Check this box to enable NAT for special applications.
IP Address	Input the IP address of the computer which is going to use the special application.
Computer name	Open the drop down menu and select the computer to which you will assign this rule. Click "<<" to add the selected computer's IP address to 'IP Address' field.
TCP Port to Open	Input the TCP port number to open (optional).
UDP Port to Open	Input the UDP port number to open (blank).
Comment	Input any comments here for reference. This is optional.

Select Game	This router is pre-loaded with the settings for many popular network games. Select a game from the drop down menu and click “Add” to add the connection parameters to all respective fields.
Add	Adds the new rule.
Reset	This will clear all text from the fields in this page.

Existing rules will be listed in the table “Current Trigger-Port Table”.

Select	Check the box to select an existing rule.
Delete	Delete selected rule(s).
Delete All	Delete all rules.
Reset	Unselect selected rule(s).

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

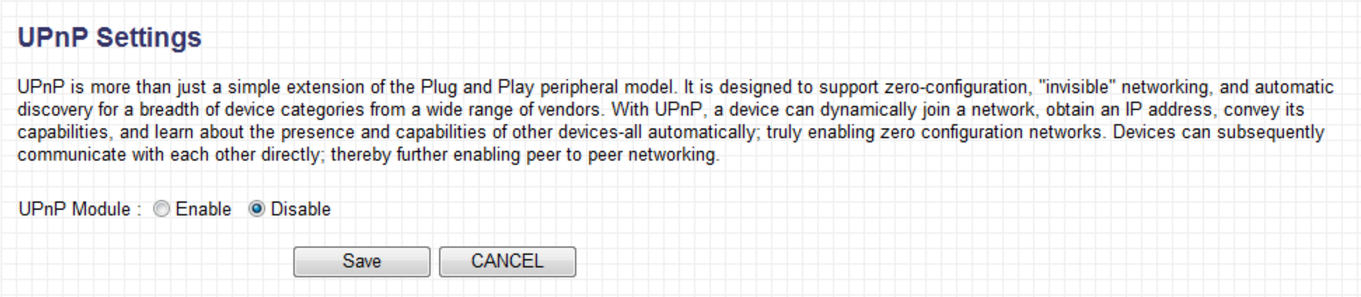
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-6-2. UPnP Settings

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

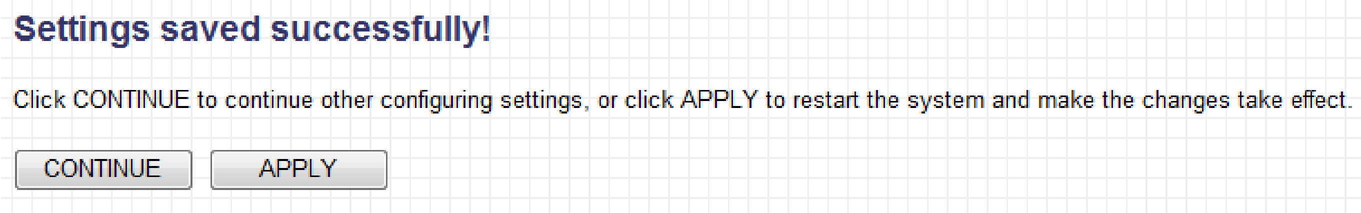


UPnP Settings

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

UPnP Module : ○ Enable ● Disable

To enable or disable this function, select “Enable” or “Disable” accordingly, and then click “Save”. The following message will appear:



Settings saved successfully!

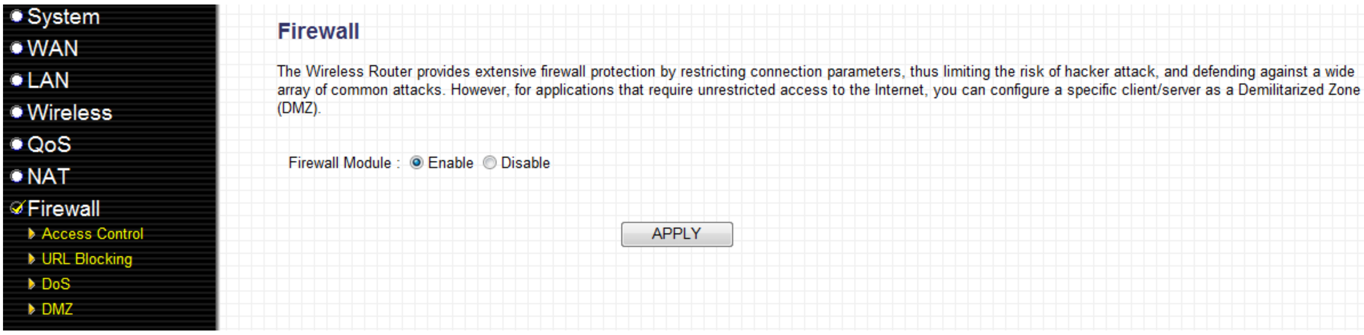
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-7. Firewall

The travel router supports firewall functions which can protect your network and computer from malicious intruders.



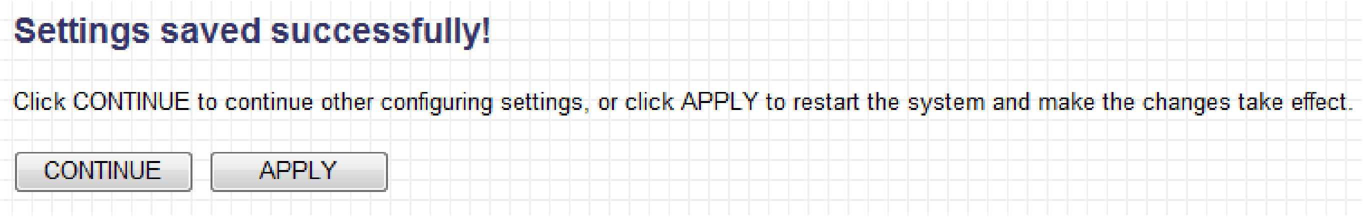
Firewall

The Wireless Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Firewall Module : ● Enable ○ Disable

Choose “Enable” or “Disable” to enable or disable the firewall module accordingly. Under the heading “Firewall” in the left menu, there are four options to choose from.

Click “APPLY” to make the changes take effect. The following message will appear:


Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

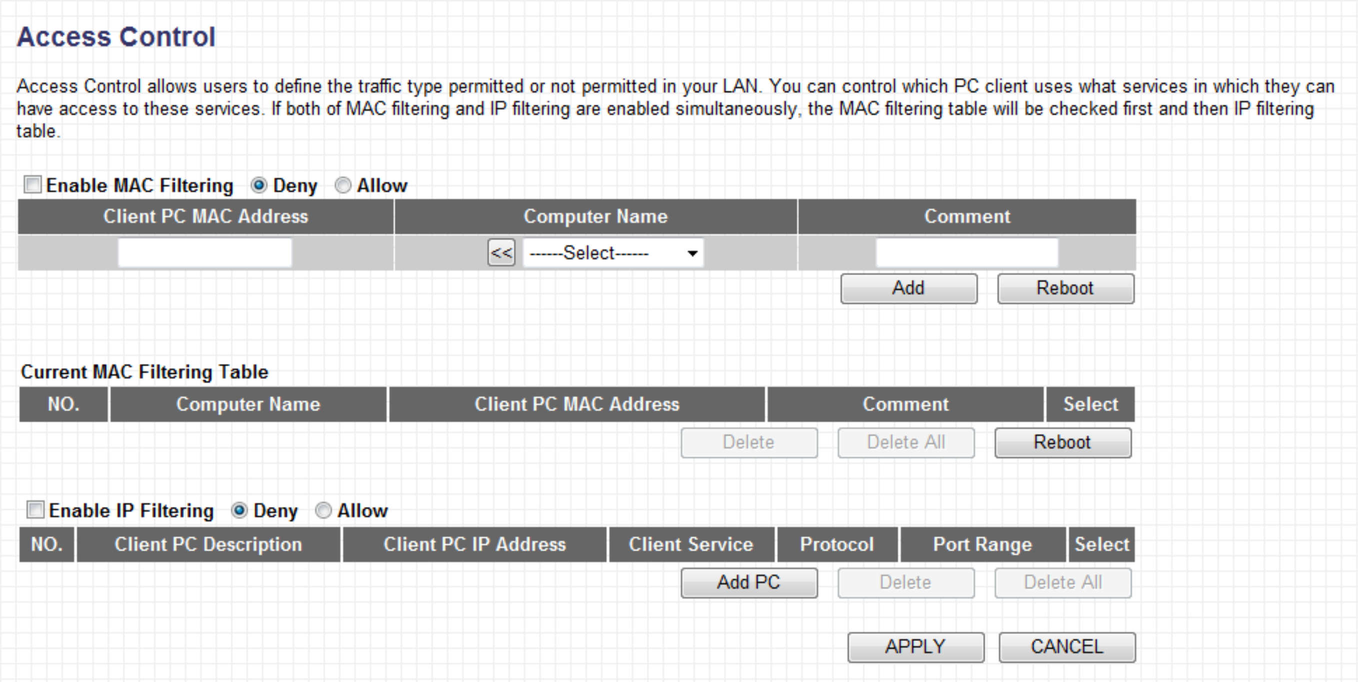
III-3-7-1. Access Control

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

This function allows you to define a list of wireless devices permitted or not permitted to connect to the travel router, identified by their unique MAC address or IP address. If a device which is not on the list of permitted MAC or IP addresses attempts to connect to the travel router, it will be denied.

To enable MAC filtering, check the box labeled “Enable Mac Filtering”.

To enable IP filtering, check the box labeled “Enable IP Filtering.”.



Access Control

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services. If both of MAC filtering and IP filtering are enabled simultaneously, the MAC filtering table will be checked first and then IP filtering table.

□ Enable MAC Filtering ● Deny ○ Allow

Client PC MAC Address	Computer Name	Comment
	<< ------Select------	

Current MAC Filtering Table

NO.	Computer Name	Client PC MAC Address	Comment	Select

□ Enable IP Filtering ● Deny ○ Allow

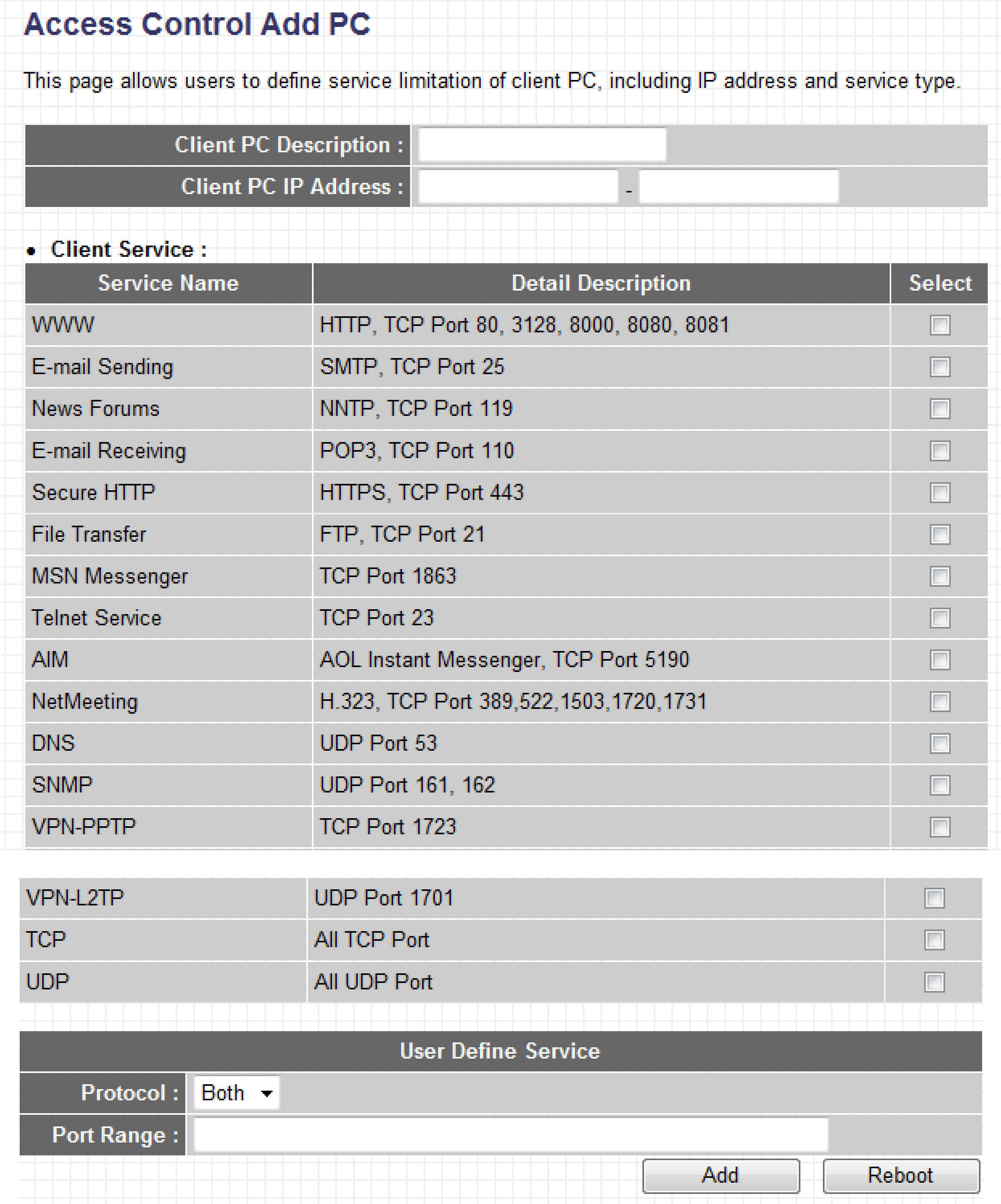
NO.	Client PC Description	Client PC IP Address	Client Service	Protocol	Port Range	Select

To add a MAC address to the list, choose “Deny” or “Allow” next to “Enable MAC Filtering”, to deny or allow a specific MAC address accordingly. Then input the information in the table below.

Client PC MAC Address	Input the MAC address you wish to add here.
Computer Name	Open the drop down menu and select the computer to which you will assign this rule. Click “<<” to add the selected computer’s MAC address to “MAC Address” field.
Comment	You can input up to 16 alphanumerical characters describing the MAC address here (optional).
Add	Click “Add” to add the MAC address and associated comment to the MAC address list.
Clear	Click “Clear” to remove everything in the MAC address and comment fields.

MAC addresses which have been added to the permitted list will be displayed in the table “Current MAC Filtering Table”. To delete one or more entries, please check the box of the corresponding entry (under “Select”), and click “Delete Selected”. If you wish to delete all the entries, click “Delete All”. Clicking “Reset” will unselect all MAC addresses.

To add an IP address to the list, choose “Deny” or “Allow” next to “Enable MAC Filtering”, to deny or allow a specific IP address accordingly. Then choose “Add PC” and you will see the following screen:



Access Control Add PC

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

Client PC Description :	
Client PC IP Address :	-

- **Client Service :**

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

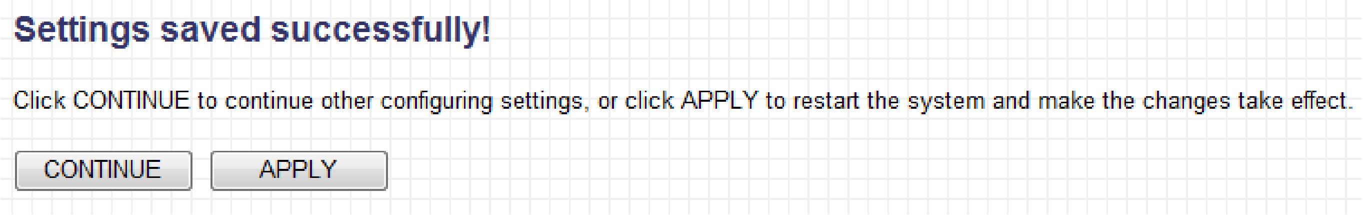
User Define Service	
Protocol :	Both
Port Range :	

Client PC Description	Enter a description of this computer for reference.
Client PC IP Address	Input the starting and ending IP address of the computers which will be subject to this rule. For a single computer, input only one IP address in the left field only.
Client Service	Check “Select” for any services which will be involved in this rule.

Protocol	Select the network protocol, “TCP”, “UDP” or “both”.
Port Range	Enter the port range. It can be a range such as “1-100”, specific ports such as “1,3,5,7,9” or a single port number.
Add	Click “Add” to add the IP address to the IP address list.
Reset	Click “Reset” to remove everything in all fields.

IP addresses which have been added to the permitted list will then be displayed on the “Access Control” page. To delete one or more entries, please check the box of the corresponding entry (labeled “Select”), and click “Delete Selected”. If you wish to delete all the entries, click “Delete All”.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

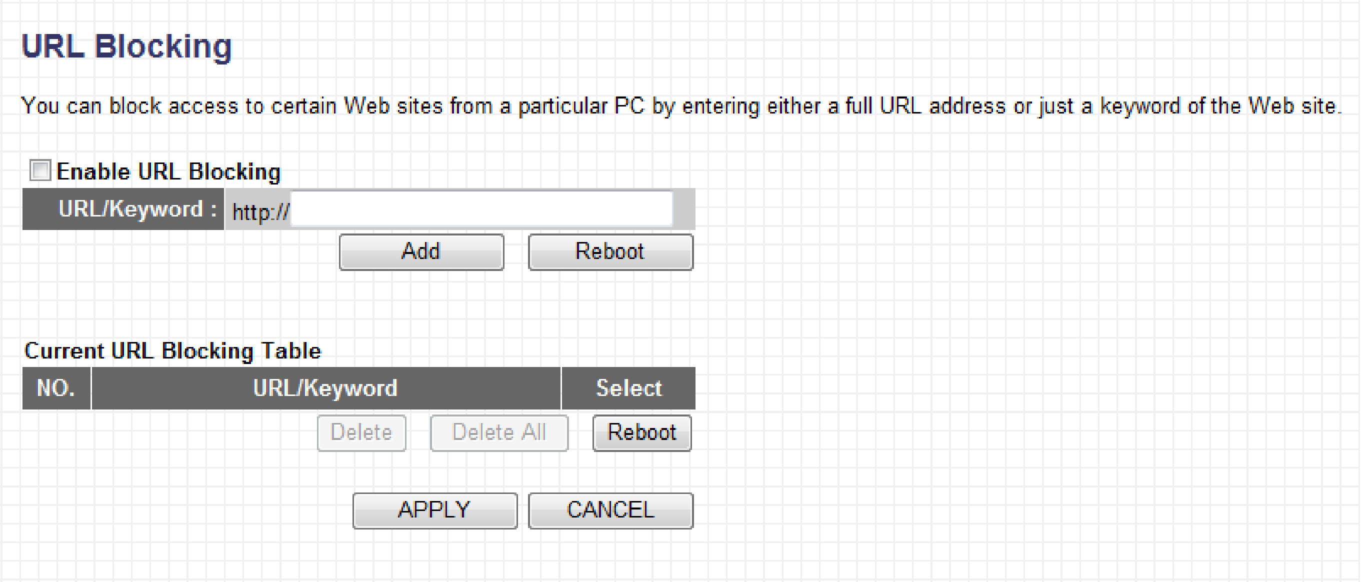
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-7-2. URL Blocking

URL Blocking is a function which enables access to specified websites to be blocked for users in the local network. Parents or company managers for example, may wish to utilize this function.



URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

□ Enable URL Blocking

URL/Keyword : http://

Add | Reboot

Current URL Blocking Table

NO.	URL/Keyword	Select

Delete | Delete All | Reboot

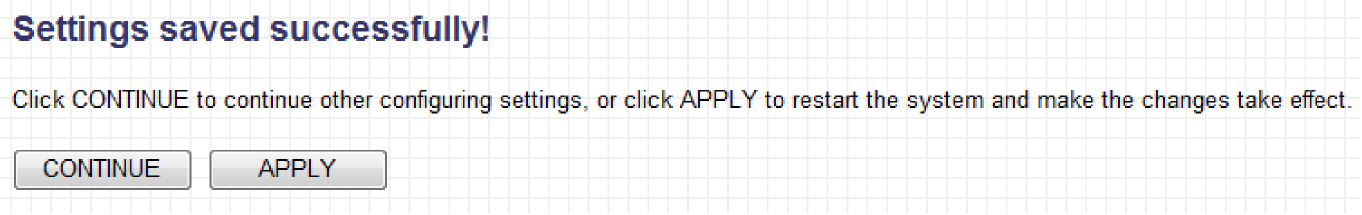
APPLY | CANCEL

Enable URL Blocking	Check this box to enable URL Blocking, uncheck it to disable URL Blocking.
URL/Keyword	Input the URL (host name or IP address) of the website to be blocked, or a keyword which is contained in URL.
Add	Click “Add” to add the URL / keyword to the “Current URL Blocking Table”.
Reset	Click “Reset” to clear the URL/Keyword field.

Existing URLs which have been blocked will be displayed in the “Current URL Blocking Table”.

To delete a specific URL/Keyword entry, check the “Select” box of the corresponding entry (or entries) and click “Delete Selected”. If you want to delete all URL/Keywords listed here, please click “Delete All”. Clicking “Reset” will unselect all URL/Keywords.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

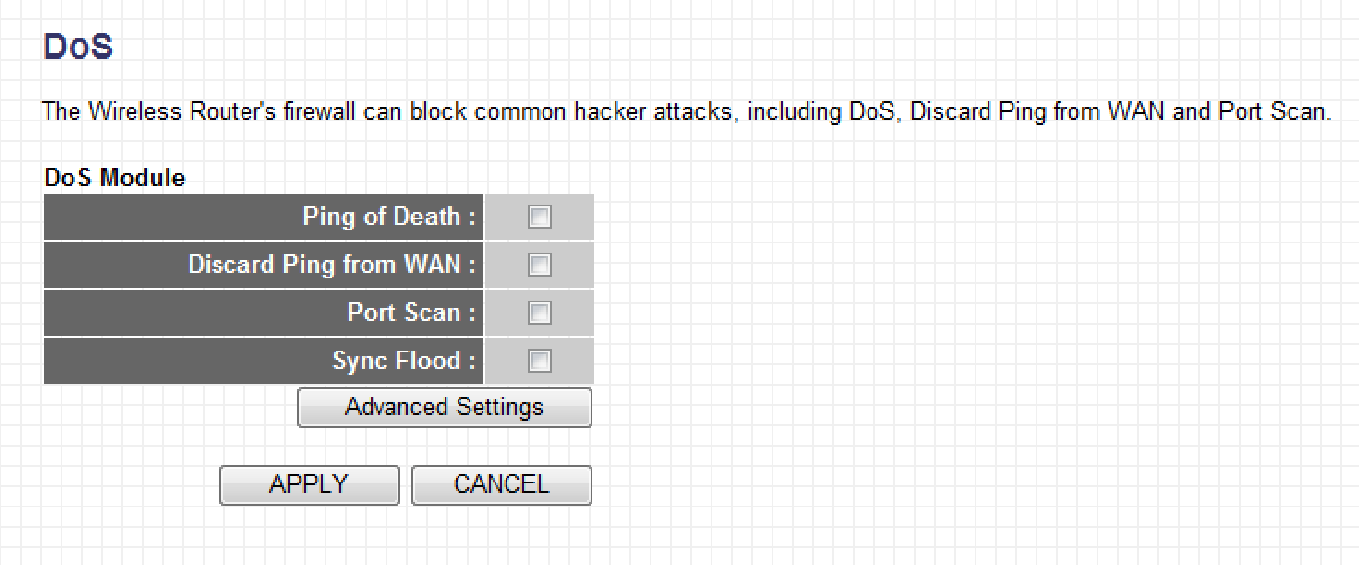
CONTINUE | APPLY

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-7-3. DoS

Denial-of-Service (DoS) is a common form of malicious attack against a network. The travel router’s firewall can protect against such attacks. When you click “DoS” in the menu on the left side, you will see the screen below.



DoS

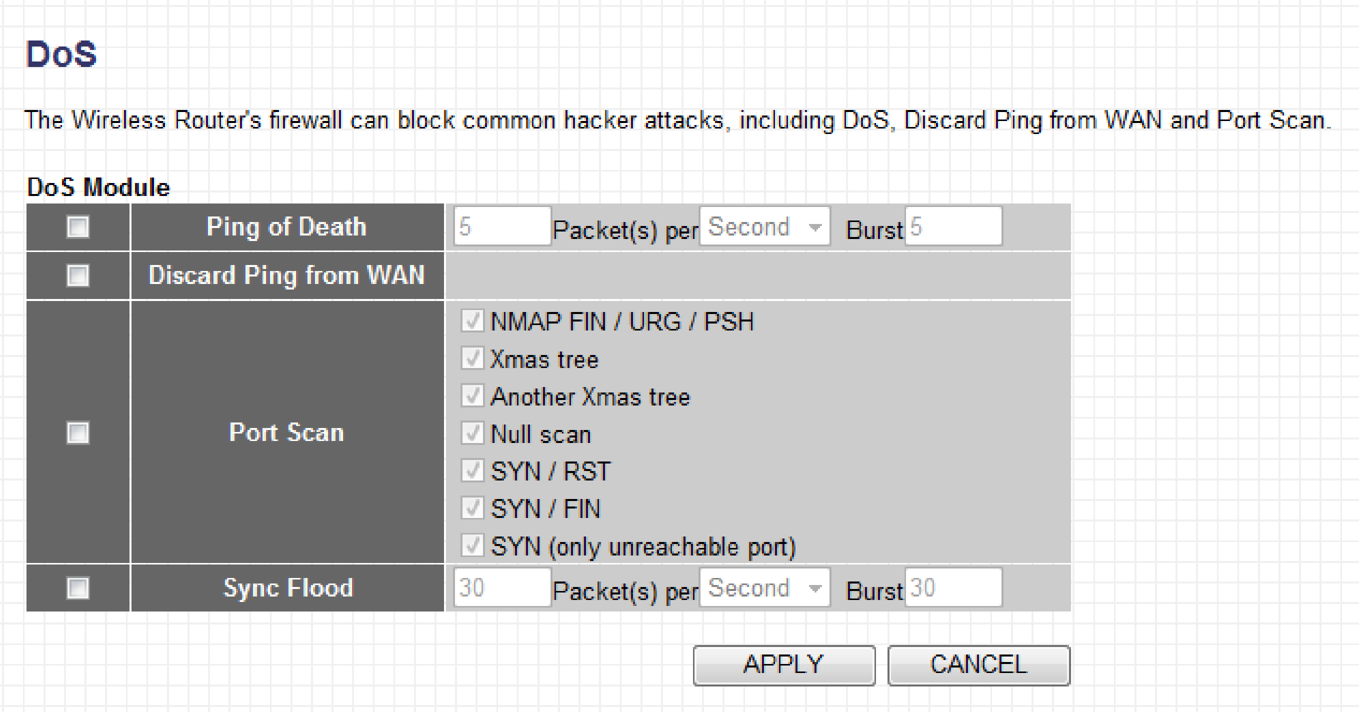
The Wireless Router's firewall can block common hacker attacks, including DoS, Discard Ping from WAN and Port Scan.

DoS Module

Ping of Death :	□
Discard Ping from WAN :	□
Port Scan :	□
Sync Flood :	□

DoS Module	Please check all boxes of the DoS function you wish to activate. If you don’t know which one you should use, you can select all without any problem.

Clicking “Advanced Settings” will open a new screen.



DoS

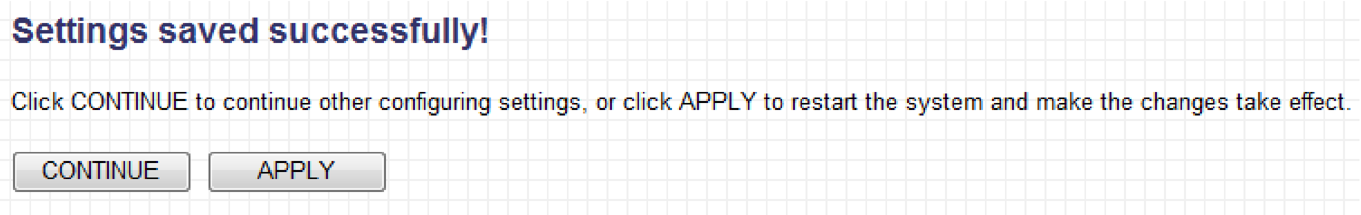
The Wireless Router's firewall can block common hacker attacks, including DoS, Discard Ping from WAN and Port Scan.

DoS Module

□	Ping of Death	5 Packet(s) per Second ▾ Burst 5
□	Discard Ping from WAN	
□	Port Scan	☑ NMAP FIN / URG / PSH ☑ Xmas tree ☑ Another Xmas tree ☑ Null scan ☑ SYN / RST ☑ SYN / FIN ☑ SYN (only unreachable port)
□	Sync Flood	30 Packet(s) per Second ▾ Burst 30

Ping of Death	You can specify the frequency of ping of death packets which will trigger this DoS function.
Discard Ping from WAN	Check this box and this travel router will not answer ping requests from Internet.
Port Scan	Check all types of port scan you want to prevent.
Sync Flood	Specify the frequency of sync flood packets which will trigger this DoS function.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

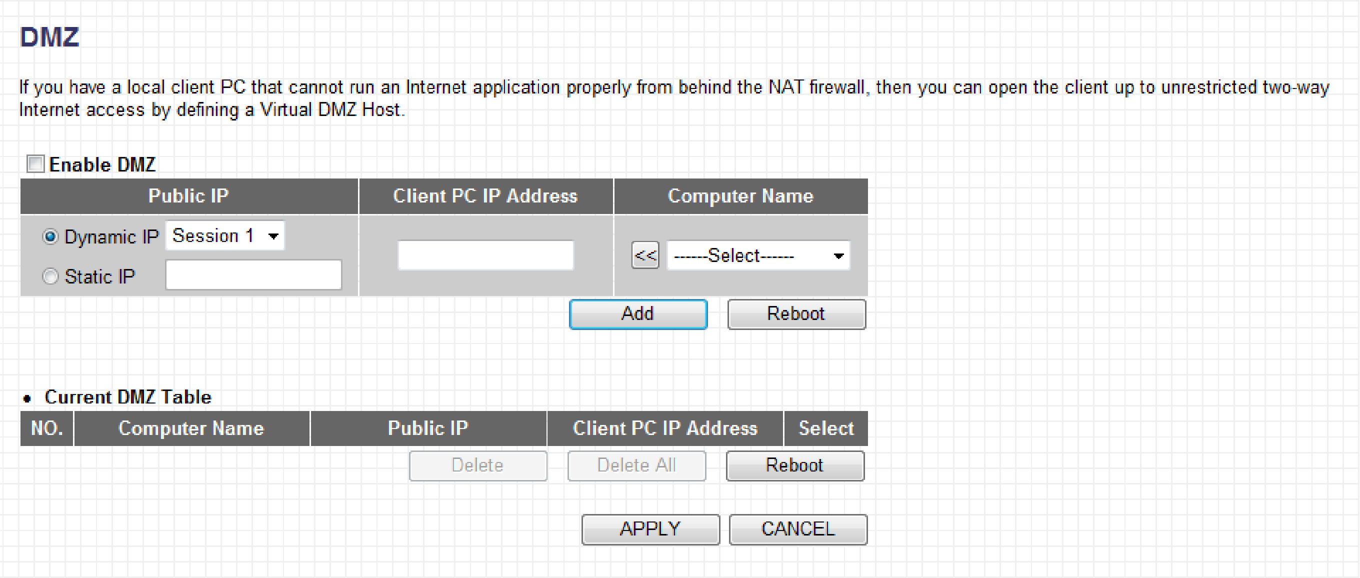
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-3-7-4. DMZ

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



DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

□ Enable DMZ

Public IP	Client PC IP Address	Computer Name
● Dynamic IP Session 1 ○ Static IP		<< ------Select------

- Current DMZ Table

NO.	Computer Name	Public IP	Client PC IP Address	Select

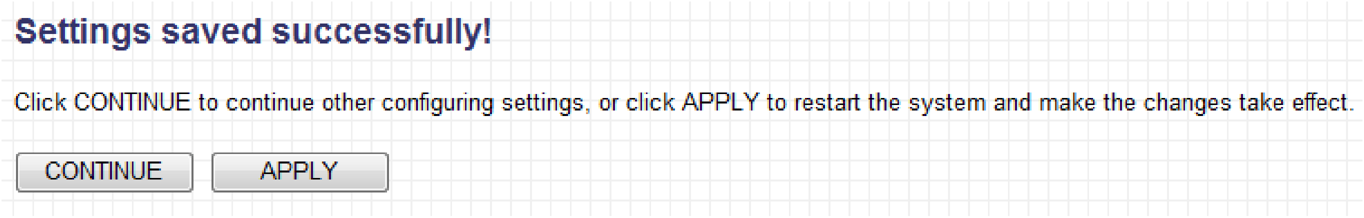
Enable DMZ	Check or uncheck “Enable DMZ” to enable or disable DMZ accordingly..
Public IP	Select ‘Dynamic IP’ or ‘Static IP’. If you select ‘Dynamic IP’, then select an Internet connection session from dropdown menu. If you select ‘Static IP’, please input the IP address that you want to map to a specific private IP address.
Client PC IP Address	Please input the private IP address that the Internet IP address will be mapped to.
Computer Name	Open the drop down menu and select the computer name of the client PC. Click “<<” to add the selected computer’s IP address to the “Client PC IP Address” field.
Add	Click “Add” to add the client to the “Current DMZ Table”.
Reset	Clicking “Reset” will clear all values.

Note: All public IP addresses can be mapped to a single client PC IP address only.

All existing DMZ entries will be displayed in the “Current DMZ Table”.

To delete a specific DMZ entry, check the “Select” box of the corresponding entry (or entries) and click “Delete Selected”. If you want to delete all DMZ entries listed here, please click “Delete All”. Clicking “Reset” will unselect all DMZ entries.

Click “APPLY” to make the changes take effect. The following message will appear:



Settings saved successfully!

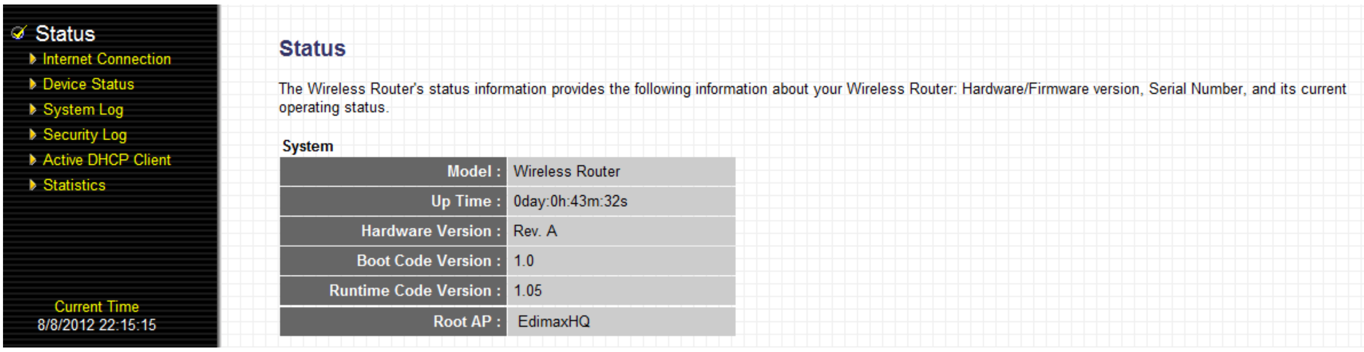
Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-4. Status

The "Status" page displays basic system information about the travel router. You can select from 6 further options listed down the left hand side under the "Status" menu.



Status

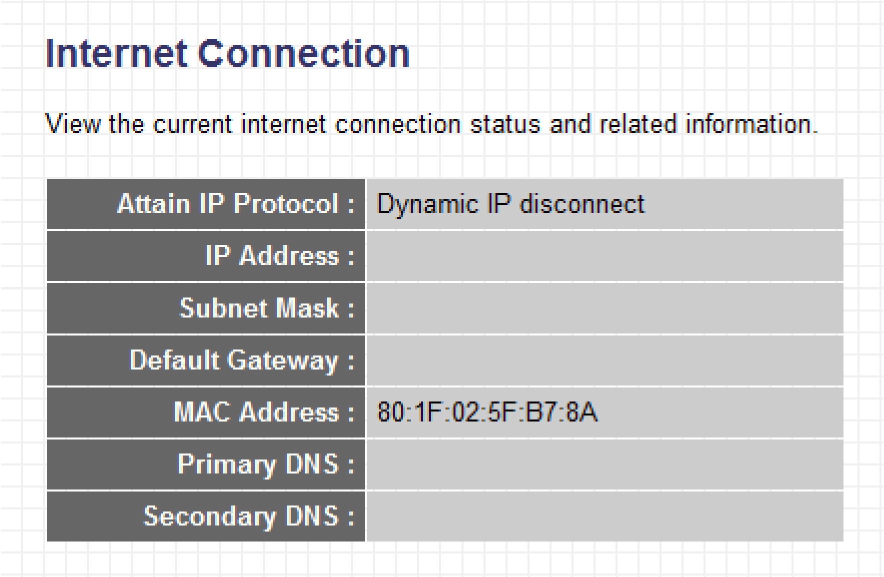
The Wireless Router's status information provides the following information about your Wireless Router: Hardware/Firmware version, Serial Number, and its current operating status.

System

Model :	Wireless Router
Up Time :	0day:0h:43m:32s
Hardware Version :	Rev. A
Boot Code Version :	1.0
Runtime Code Version :	1.05
Root AP :	EdimaxHQ

III-4-1. Internet Connection

Here you can view the status of your current Internet connection and other related information.



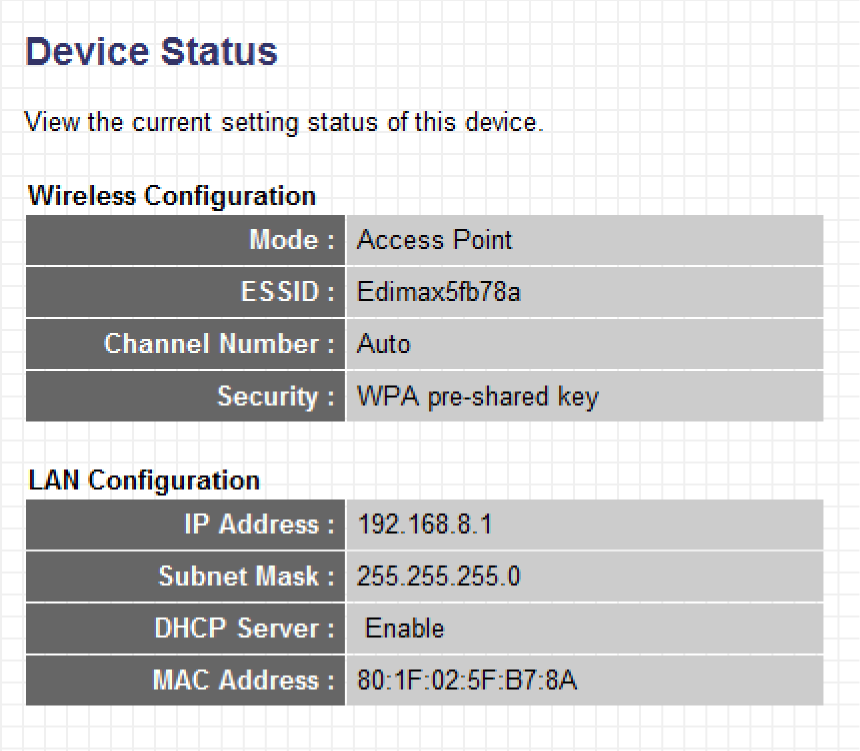
Internet Connection

View the current internet connection status and related information.

Attain IP Protocol :	Dynamic IP disconnect
IP Address :	
Subnet Mask :	
Default Gateway :	
MAC Address :	80:1F:02:5F:B7:8A
Primary DNS :	
Secondary DNS :	

III-4-2. Device Status

The statuses of the travel router's wireless and LAN configurations are displayed here.



Device Status

View the current setting status of this device.

Wireless Configuration

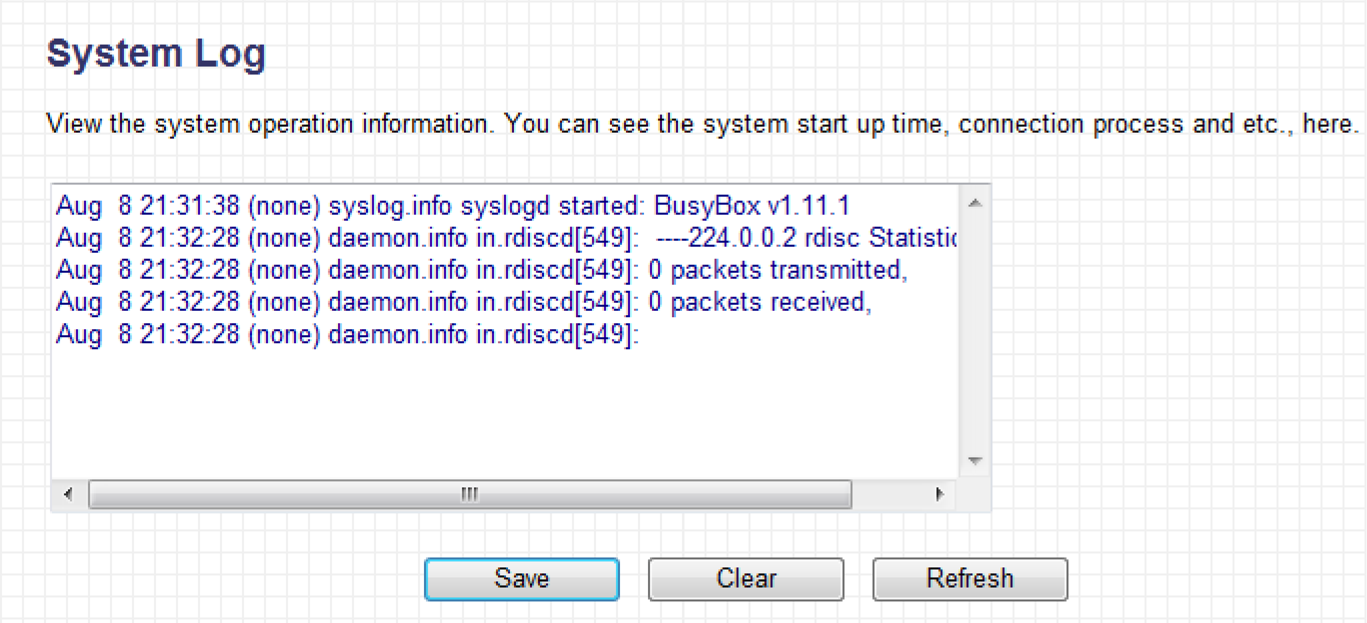
Mode :	Access Point
ESSID :	Edimax5fb78a
Channel Number :	Auto
Security :	WPA pre-shared key

LAN Configuration

IP Address :	192.168.8.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enable
MAC Address :	80:1F:02:5F:B7:8A

III-4-3. System Log

The system log of the travel router is displayed here. All logged system information since the device was last powered on is recorded here, and may be useful in the event of a problem with your travel router.



System Log

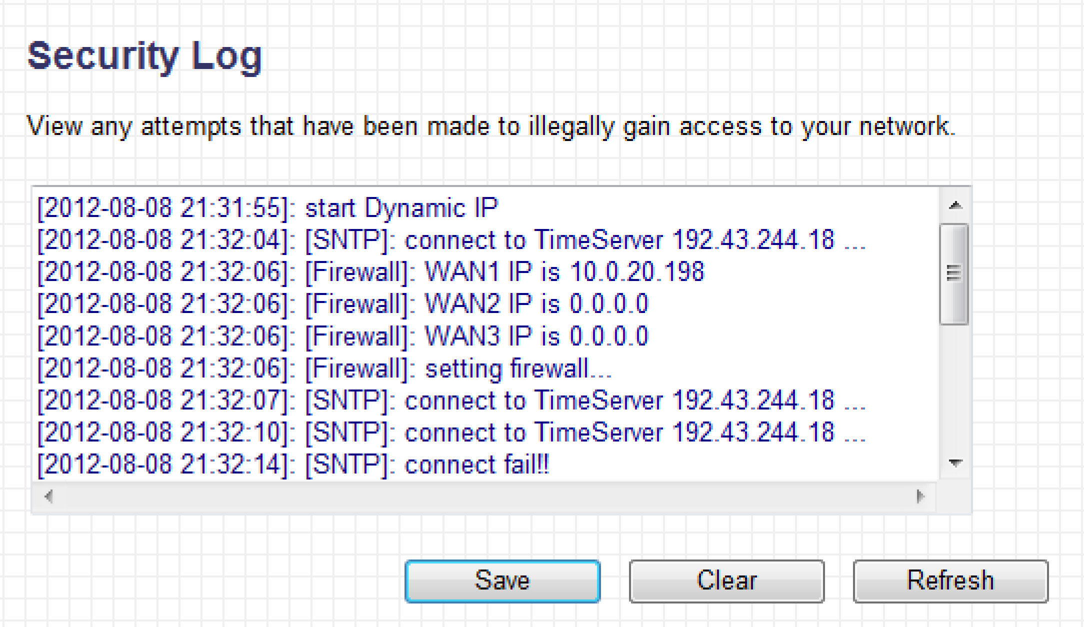
View the system operation information. You can see the system start up time, connection process and etc., here.

```
Aug  8 21:31:38 (none) syslog.info syslogd started: BusyBox v1.11.1
Aug  8 21:32:28 (none) daemon.info in.rdiscd[549]:  ----224.0.0.2 rdisc Statistic
Aug  8 21:32:28 (none) daemon.info in.rdiscd[549]: 0 packets transmitted,
Aug  8 21:32:28 (none) daemon.info in.rdiscd[549]: 0 packets received,
Aug  8 21:32:28 (none) daemon.info in.rdiscd[549]:
```

Save	This will save the system log as a text file in your computer.
Clear	This will clear the system log and erase all information.
Refresh	This will refresh the system log and display the latest messages, if they are not already displayed.

III-4-4. Security Log

The security log of the travel router is displayed here.



Security Log

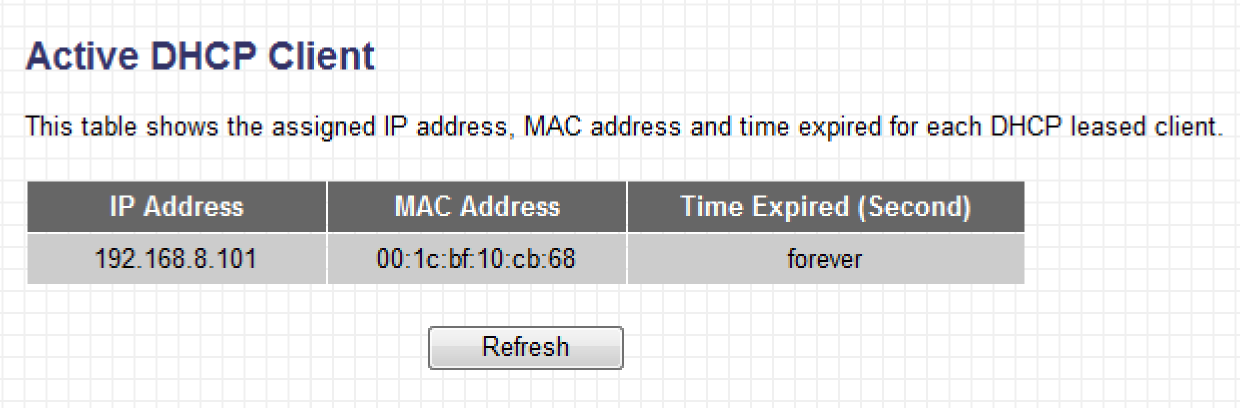
View any attempts that have been made to illegally gain access to your network.

```
[2012-08-08 21:31:55]: start Dynamic IP
[2012-08-08 21:32:04]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2012-08-08 21:32:06]: [Firewall]: WAN1 IP is 10.0.20.198
[2012-08-08 21:32:06]: [Firewall]: WAN2 IP is 0.0.0.0
[2012-08-08 21:32:06]: [Firewall]: WAN3 IP is 0.0.0.0
[2012-08-08 21:32:06]: [Firewall]: setting firewall...
[2012-08-08 21:32:07]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2012-08-08 21:32:10]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2012-08-08 21:32:14]: [SNTP]: connect fail!!
```

Save	This will save the security log as a text file in your computer.
Clear	This will clear the security log and erase all information.
Refresh	This will refresh the security log and display the latest messages, if they are not already displayed.

III-4-5. Active DHCP Client

This page lists and displays information on all active DHCP clients that connect to this travel router.



Active DHCP Client

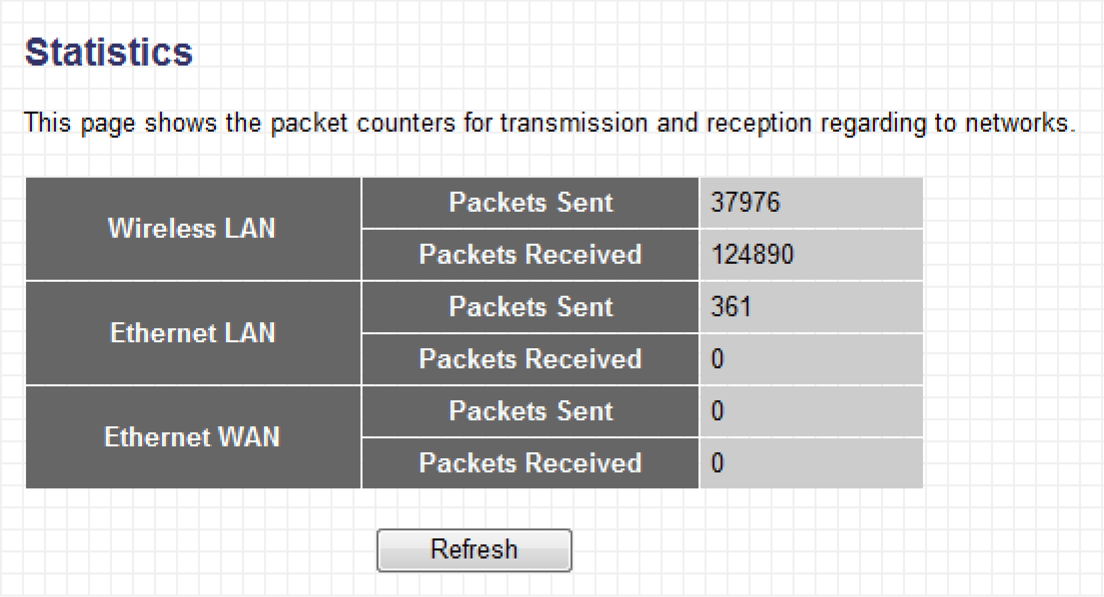
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired (Second)
192.168.8.101	00:1c:bf:10:cb:68	forever

Click “Refresh” to refresh the list and update the information.

III-4-6. Statistics

This page shows statistical information for each network interface.



Statistics

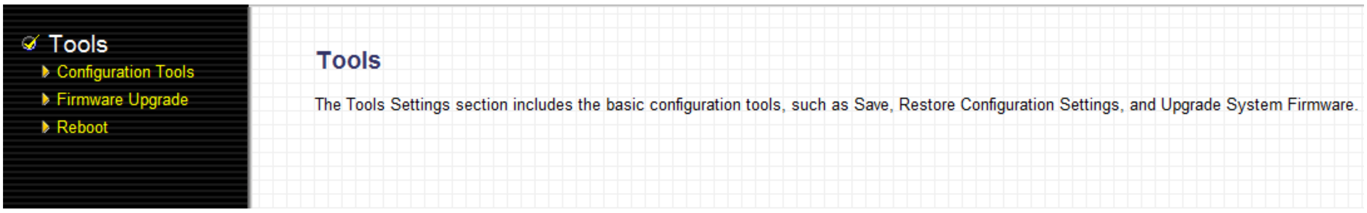
This page shows the packet counters for transmission and reception regarding to networks.

Wireless LAN	Packets Sent	37976
	Packets Received	124890
Ethernet LAN	Packets Sent	361
	Packets Received	0
Ethernet WAN	Packets Sent	0
	Packets Received	0

Click "Refresh" to update the information.

III-5. Tools

The "Tools" menu enables you to back up the current settings of the device, restore the settings back to a saved version or to factory defaults, upgrade the firmware and to reboot the device. Choose from the 3 options in the menu under "Tools" on the left side.

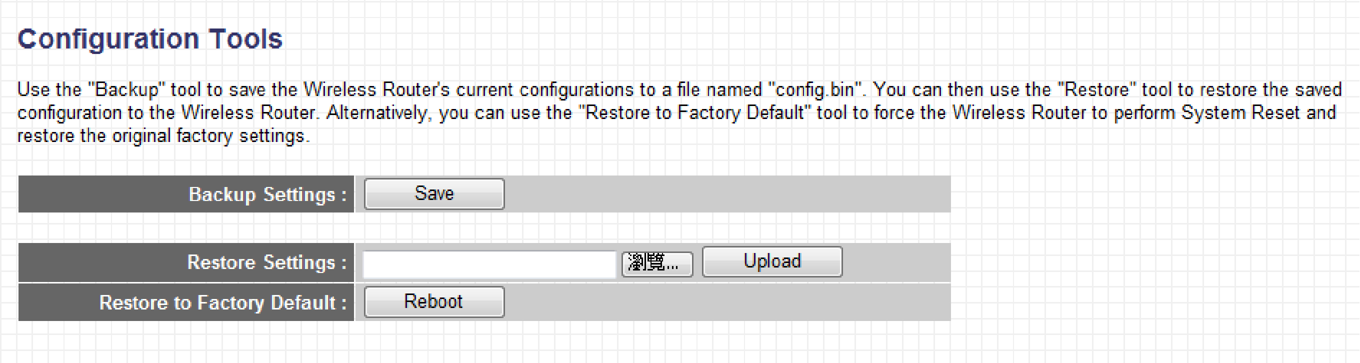


Tools

The Tools Settings section includes the basic configuration tools, such as Save, Restore Configuration Settings, and Upgrade System Firmware.

III-5-1. Configuration Tools

Here you can back up and restore the travel router's configuration.



Configuration Tools

Use the "Backup" tool to save the Wireless Router's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Wireless Router. Alternatively, you can use the "Restore to Factory Default" tool to force the Wireless Router to perform System Reset and restore the original factory settings.

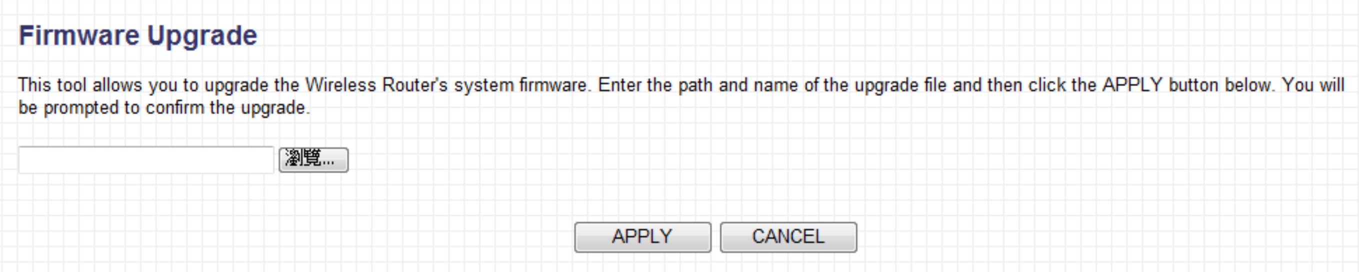
Backup Settings	Click "Save" to save the current settings on your computer as config.bin file.
Restore Settings	Click the browse button to find a previously saved config.bin file and then click "Upload" to replace your current settings.
Restore to Factory Defaults	Click "Reset" to restore settings to 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.

Note: Restoring to factory defaults will restore **all** settings, configurations and passwords back to the factory default.

Note: You can also reset the device to the factory default by pressing and holding the **Reset/WPS** button for 10 seconds, until the blue Power LED starts blinking slowly. See **I-2. Physical Description** for help finding the **Reset/WPS** button and **II-5. Resetting the Travel Router** for a description of the device's reset process.

III-5-2. Firmware Upgrade

Selecting "Firmware upgrade" from the "Tools" menu allows you to update the system firmware to a more recent version. You can download the latest firmware from the Edimax website.



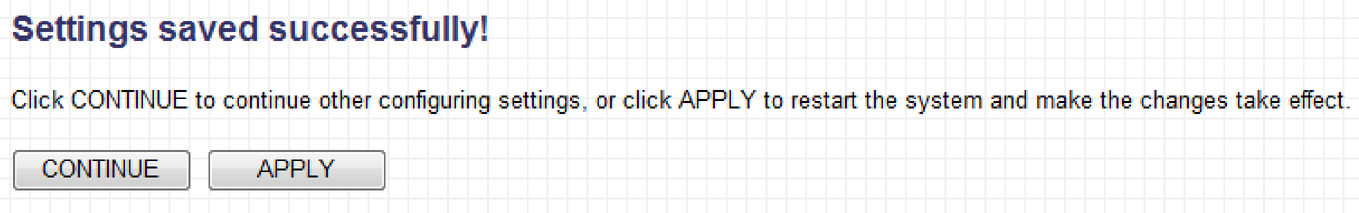
Firmware Upgrade

This tool allows you to upgrade the Wireless Router's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

Note: Do not turn off or disconnect the access point during a firmware upgrade, as this could damage the device.

Note: It is recommended that you use a wired Ethernet connection to upload the firmware file.

Click on the browse button to open a new window and locate the downloaded firmware file in your computer. Confirm your selection and click “APPLY” to make changes take effect. The following message will appear:



Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based configuration interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

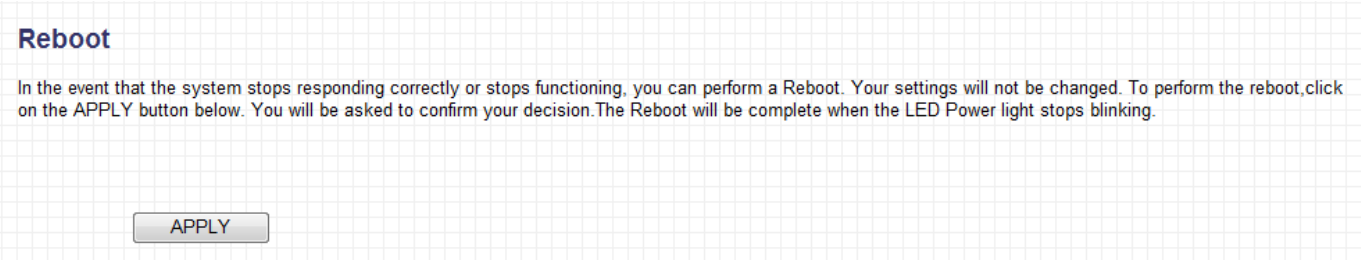
III-5-3. Reboot

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

Note: If the access point is still not responding after a reboot, switch off the device by unplugging the power supply. Plug it back in after 10 seconds.

Note: Rebooting the access point will not affect the current configuration of the device.

To reboot the device, please click "Reboot" from the "Tools" menu in the sidebar. The following screen will be displayed:

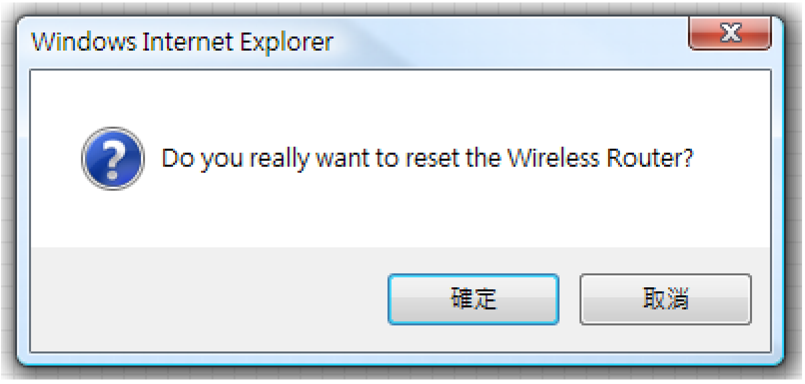


Reboot

In the event that the system stops responding correctly or stops functioning, you can perform a Reboot. Your settings will not be changed. To perform the reboot,click on the APPLY button below. You will be asked to confirm your decision.The Reboot will be complete when the LED Power light stops blinking.

Click "Apply" to reboot the device.

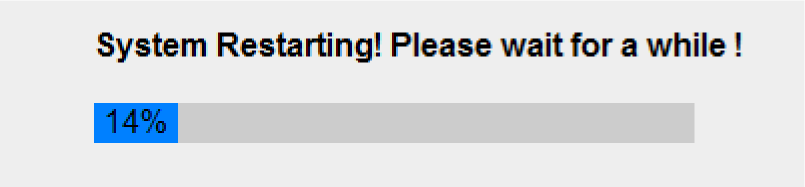
A pop up window will ask you to confirm, please click "Ok" to confirm or "Cancel" to abort. If you click "Ok" to continue, all connections between wireless client and access will be disconnected at this point.



Windows Internet Explorer

Do you really want to reset the Wireless Router?

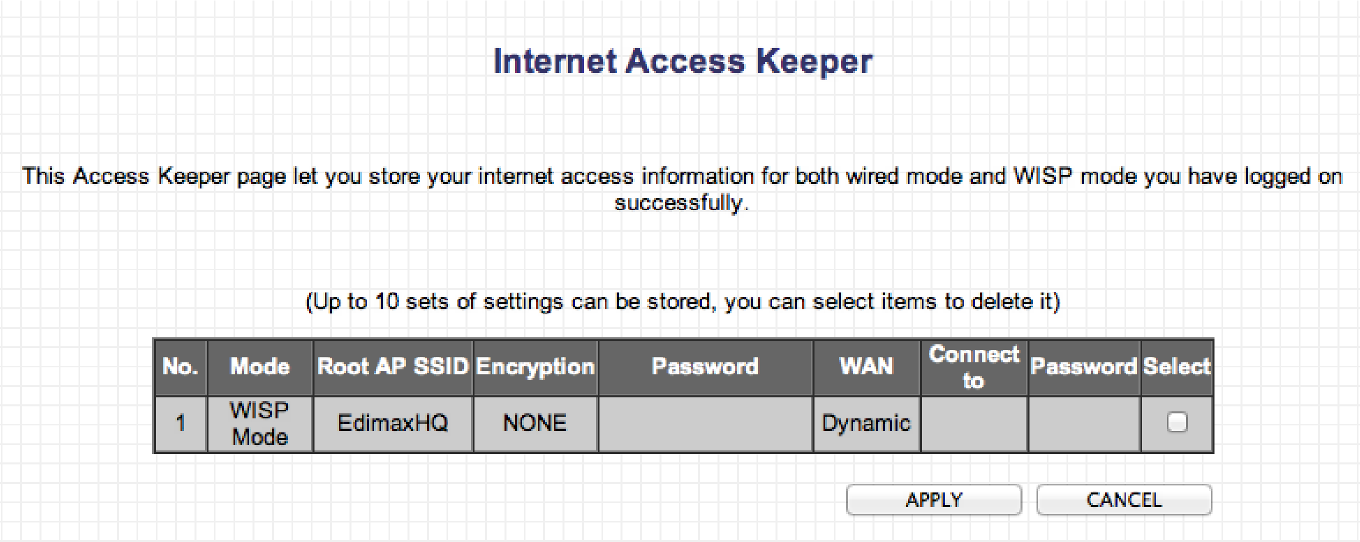
You will see the following screen. Please wait 1-2 minutes for the reboot to complete.



System Restarting! Please wait for a while !

III-5-4. Internet Access Keeper

The Internet Access Keeper stores information about the operating mode of the travel router, both currently and previously. Up to 10 records can be stored here for both wired and WISP modes.



Internet Access Keeper

This Access Keeper page let you store your internet access information for both wired mode and WISP mode you have logged on successfully.

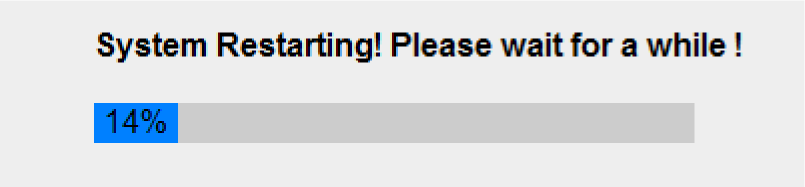
(Up to 10 sets of settings can be stored, you can select items to delete it)

No.	Mode	Root AP SSID	Encryption	Password	WAN	Connect to	Password	Select
1	WISP Mode	EdimaxHQ	NONE		Dynamic			□

No.	Items are ordered by number, which is displayed here.
Mode	The operating mode (wired or WISP) is displayed here.
Root AP SSID	The root AP SSID of the network is displayed here.
Encryption	If the root AP SSID uses encryption, the encryption type will be displayed here.
Password	If the root AP SSID uses encryption, the password will be displayed here.
WAN	Your WAN (Wide Area Network) type will be displayed here, “Dynamic”, “Static IP”, “PPPoE” or “PPTP”. See III-3-2. WAN for

	more information.
Connect to	In the case of a PPPoE or PPTP connection type, the username provided by your ISP will be displayed here. For a static IP connection, the IP address will be displayed. For a dynamic connection type, this field will be blank.
Password	In the case of a PPPoE or PPTP connection type, the password provided by your ISP will be displayed here. For a static IP connection and dynamic connection type, this field will be blank.
Select	Check the box to select one or more items for deletion.

Click “APPLY” to delete selected items. The system will restart, as shown below. Please 1-2 minutes for the restart to complete, after which you will be returned to the “Home” screen of the browser based configuration interface.



System Restarting! Please wait for a while !

IV. APPENDIX

IV-1. Configuring your IP address

Before you use this travel router, please make sure your computer is set to use a **dynamic IP address**. This means your computer can obtain an IP address automatically from a DHCP server. This is a simple procedure, which is explained step by step in **IV-1-1. How to configure your computer to use a dynamic IP address.**

Unfortunately, not all networks support DHCP capability. In this case, you need to use a static IP address for your PC or Macintosh. The router uses the default IP address 192.168.8.1, which may not be in the same IP address subnet of your network; meaning you are unable to access the browser based configuration interface. So, you need to modify the IP address of your PC or Macintosh to 192.168.8.10 in order to access the browser-based configuration interface.

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

> **Note**: For guidance on how to assign a new IP address to the **travel router**, so that it is within the same IP address subnet of your network, please refer to **III-3-3. LAN**. In the case where you need to modify the IP of your PC or Macintosh, if the default IP of the travel router remains unchanged, you may need to repeat this process and modify the IP of your PC or Macintosh every time you wish to configure the travel router.

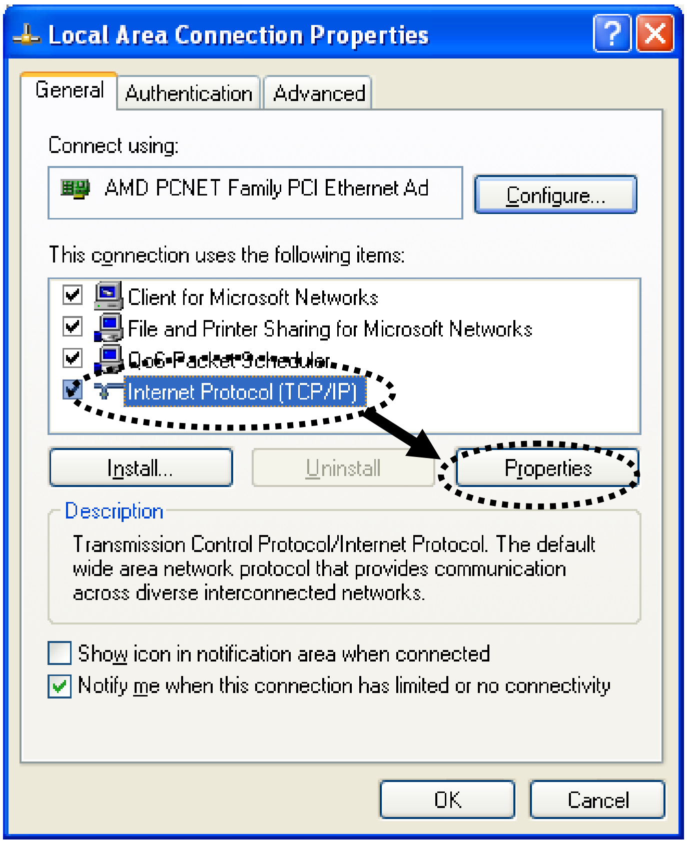
IV-1-1. How to configure your computer to use a dynamic IP address

Please follow the instructions appropriate for your operating system.

IV-1-1-1. Windows XP

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

Internet Connections" icon, click "Network Connections", and then double-click "Local Area Connection". The "Local Area Connection Status" window will then appear, click "Properties".



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

AMD PCNET Family PCI Ethernet Ad

Configure...

This connection uses the following items:

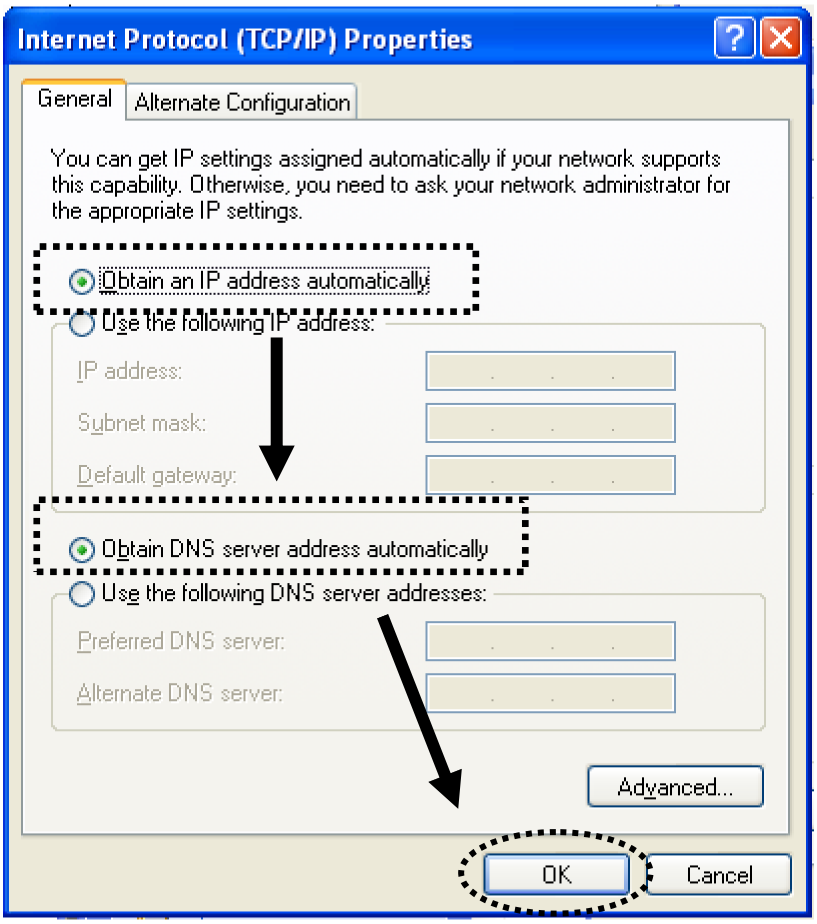
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically", then click "OK".



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

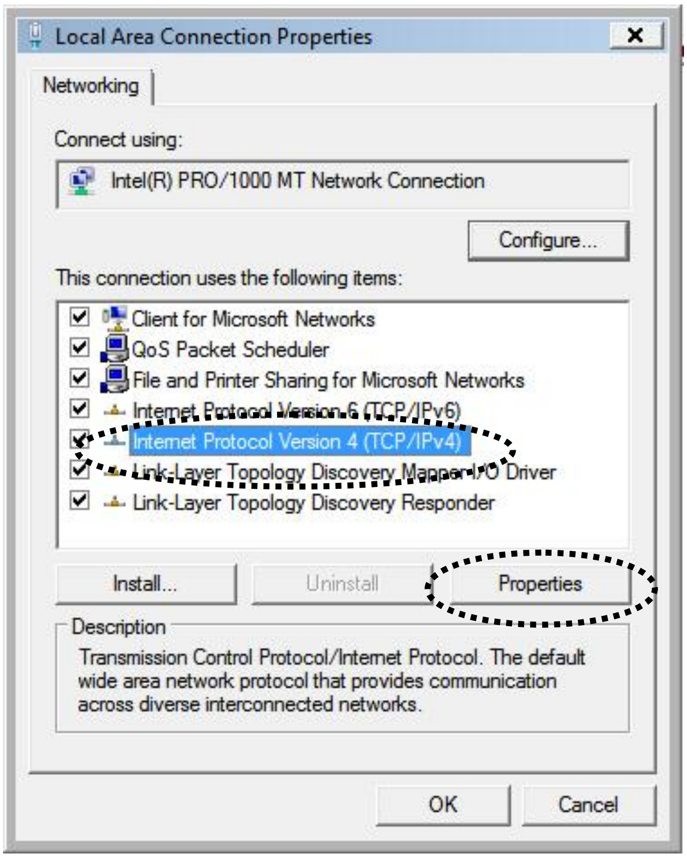
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

IV-1-1-2. Windows Vista

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

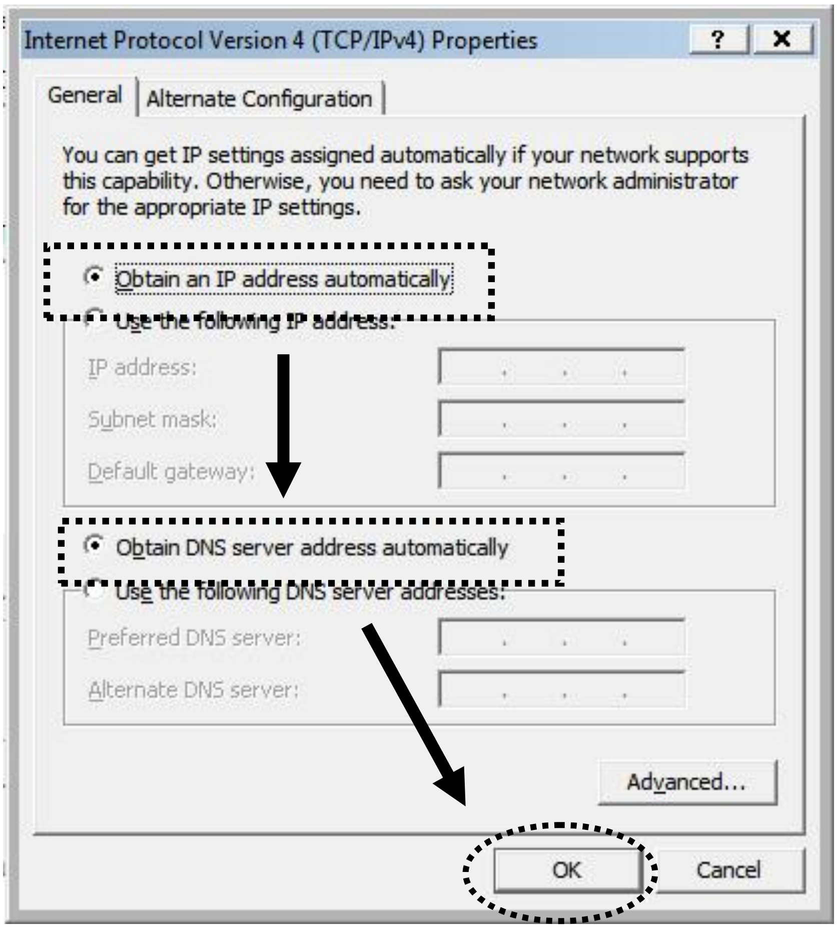
Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

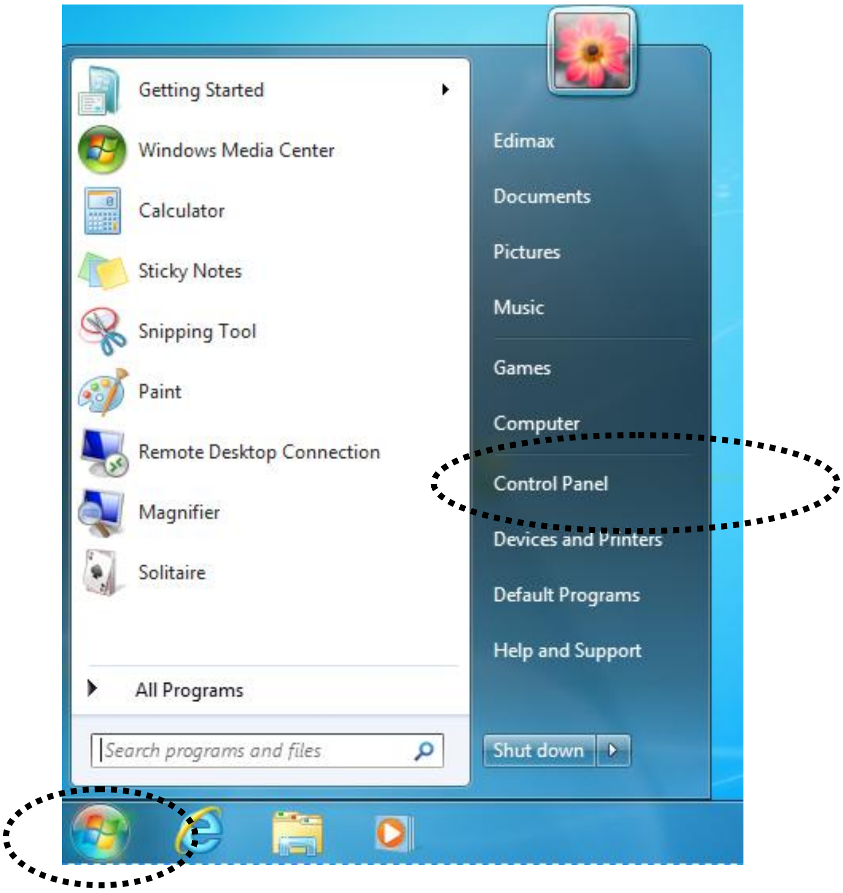
Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

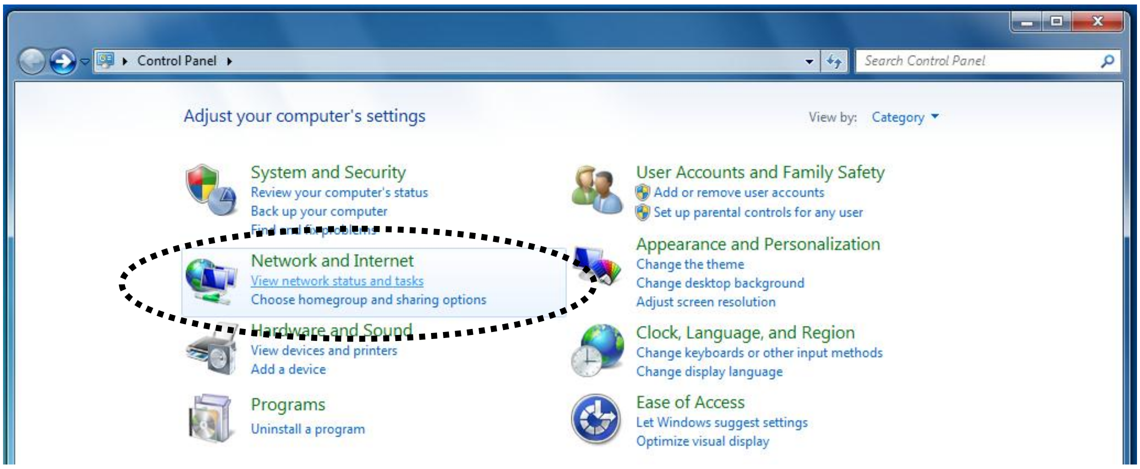
OK Cancel

IV-1-1-3. Windows 7

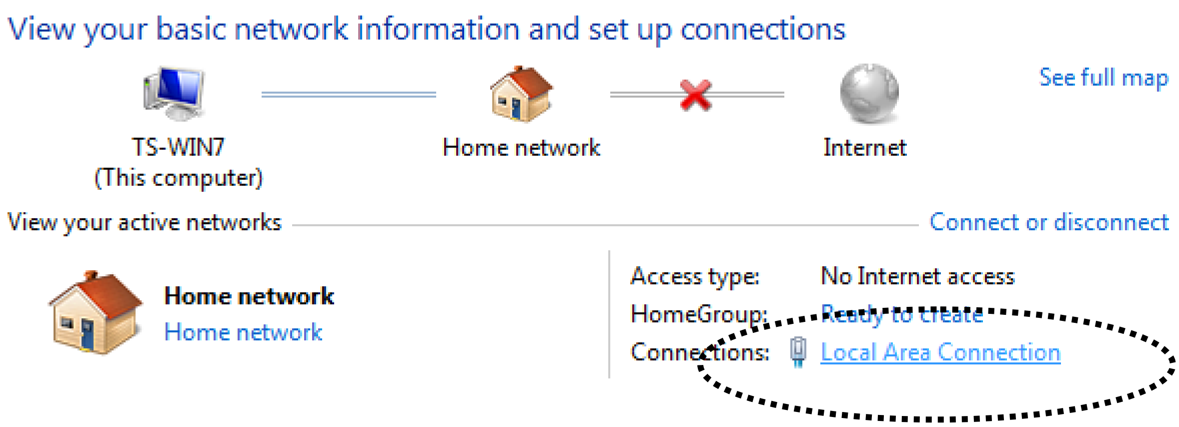
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



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


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click “Local Area Connection”.



View your basic network information and set up connections

See full map

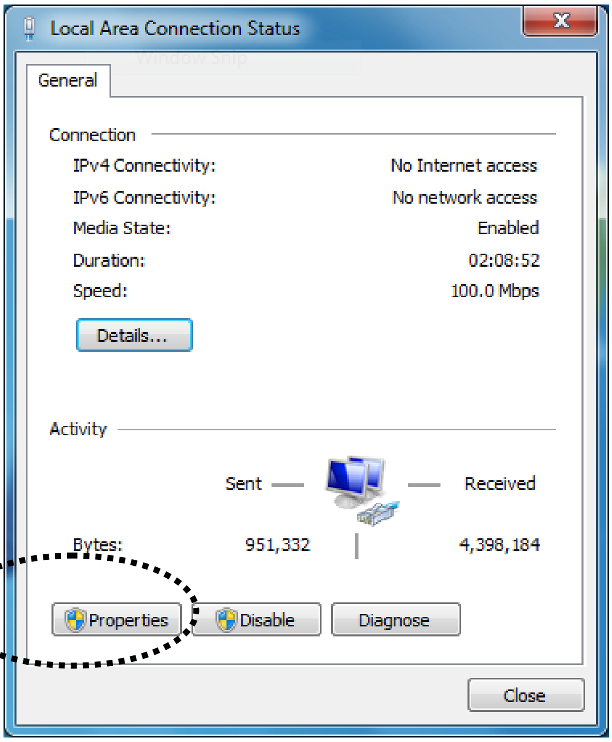
TS-WIN7 (This computer) — Home network — Internet

View your active networks — Connect or disconnect

Home network
Home network

Access type: No Internet access
HomeGroup: Ready to create
Connections: Local Area Connection

4. Click “Properties”.



Local Area Connection Status

General

Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	02:08:52
Speed:	100.0 Mbps

Details...

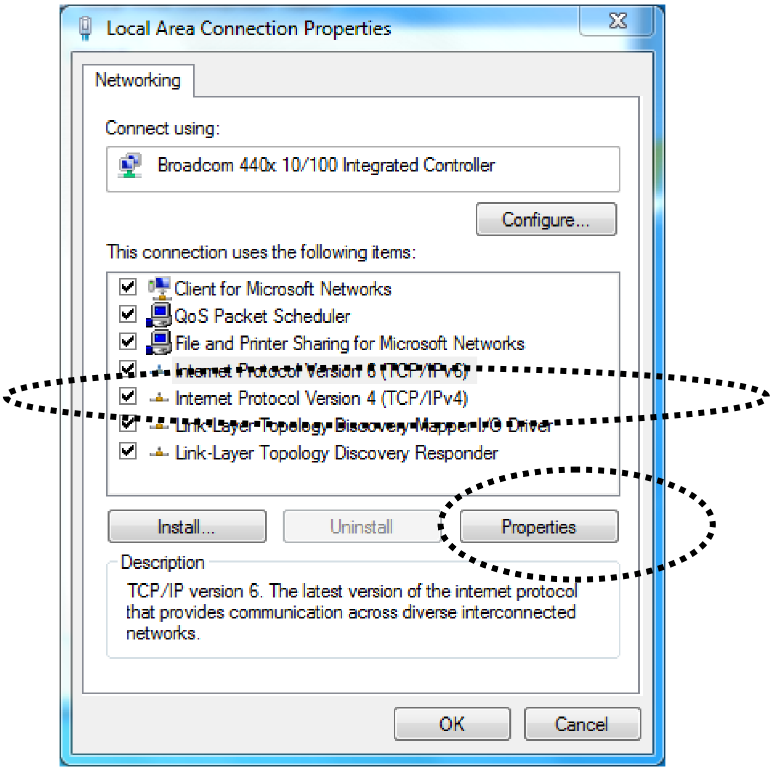
Activity

	Sent	Received
Bytes:	951,332	4,398,184

Properties Disable Diagnose

Close

5. Select “Internet Protocol Version 4 (TCP/IPv6) and then click “Properties”.



Local Area Connection Properties

Networking

Connect using:

Broadcom 440x 10/100 Integrated Controller

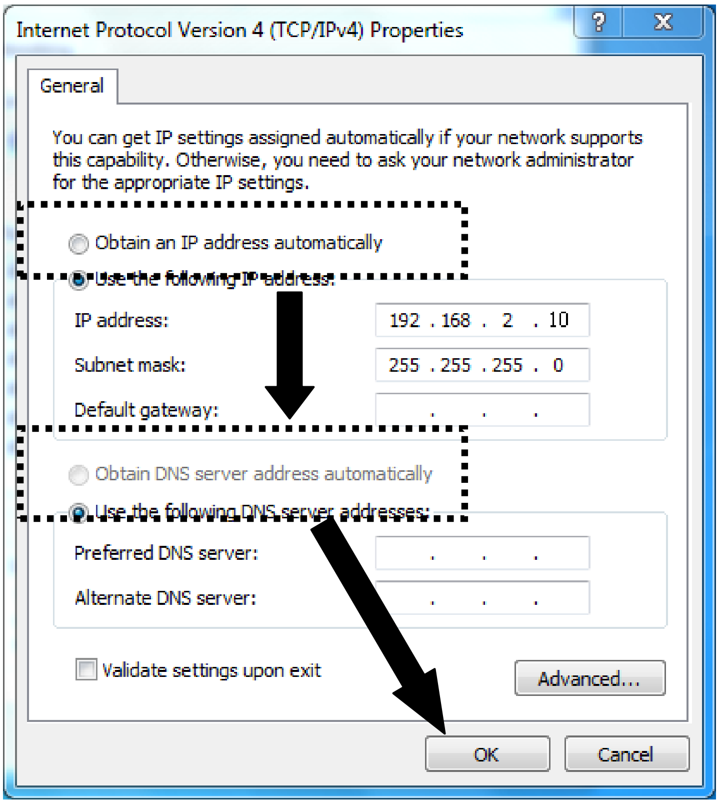
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

3. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”, then click “OK”.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

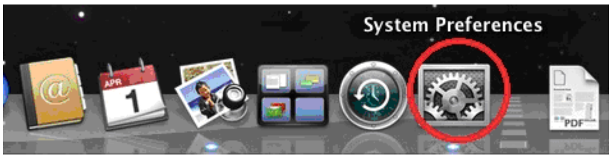
Preferred DNS server: . . .

Alternate DNS server: . . .

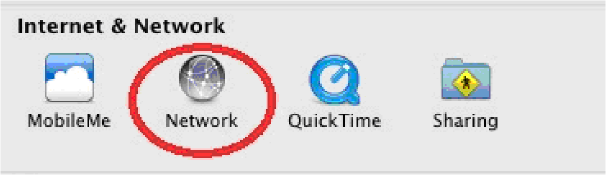
□ Validate settings upon exit

IV-1-1-4. Mac OS

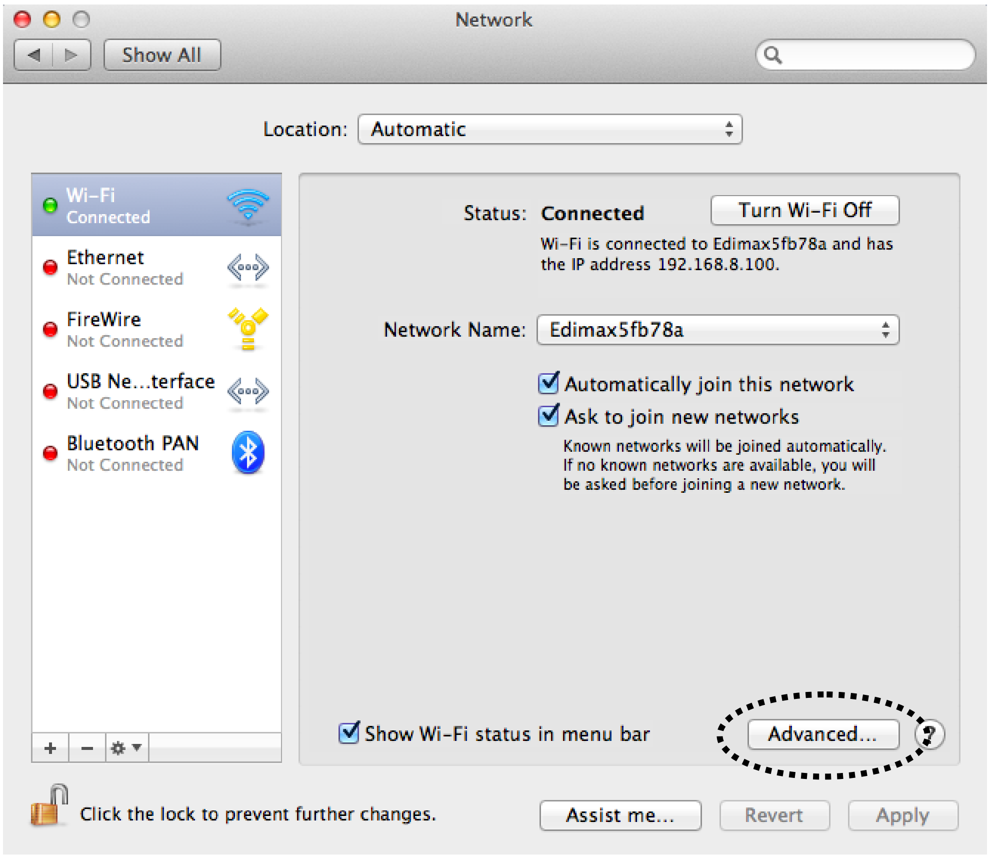
1. Have your Macintosh computer operate as usual, and click on “System Preferences”.



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



1. Here you will see all of your network connections. You need to remove any Ethernet cable that may be connected, so that the “Ethernet” status in the left panel displays “Not Connected”, as shown below. Choose “Wi-Fi” from the panel on the left side, and then click “Advanced” in the bottom right corner.



Location: Automatic

Wi-Fi
Connected

Ethernet
Not Connected

FireWire
Not Connected

USB Ne...terface
Not Connected

Bluetooth PAN
Not Connected

Status: Connected

Wi-Fi is connected to Edimax5fb78a and has the IP address 192.168.8.100.

Network Name: Edimax5fb78a

☑ Automatically join this network

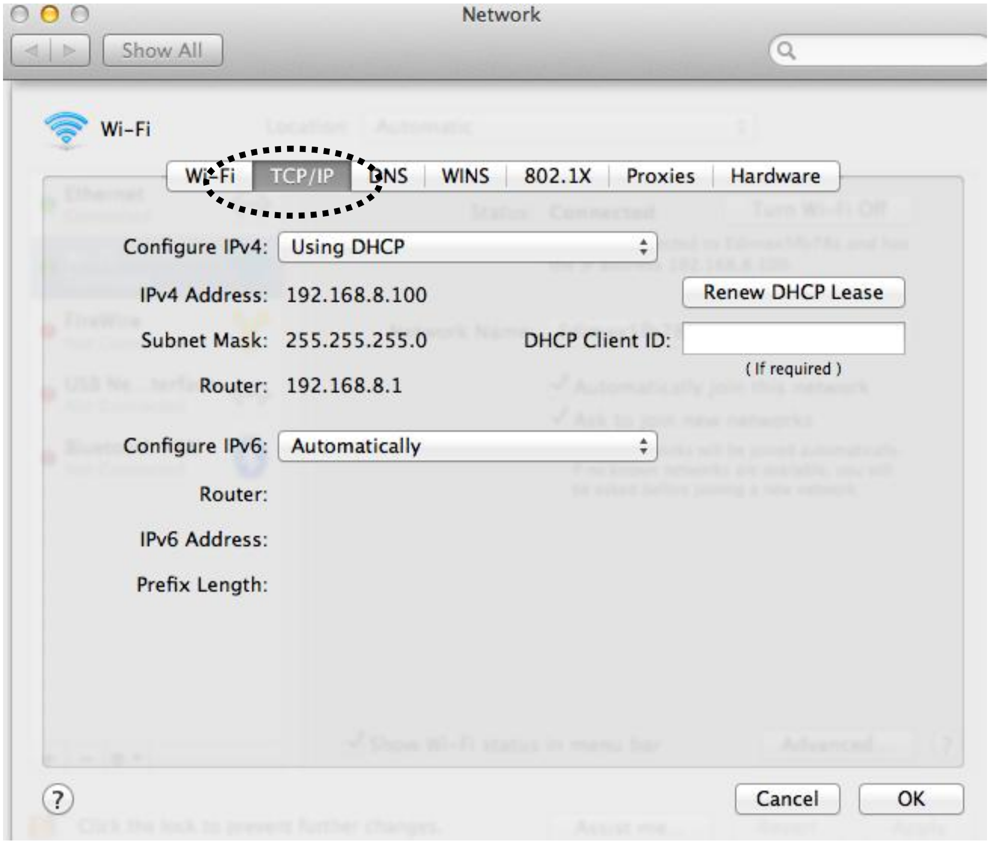
☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show Wi-Fi status in menu bar

Click the lock to prevent further changes.

3. Now select "TCP/IP" from the menu across the top of the screen.



Configure IPv4: Using DHCP

IPv4 Address: 192.168.8.100

Subnet Mask: 255.255.255.0

Router: 192.168.8.1

DHCP Client ID:

(If required)

Configure IPv6: Automatically

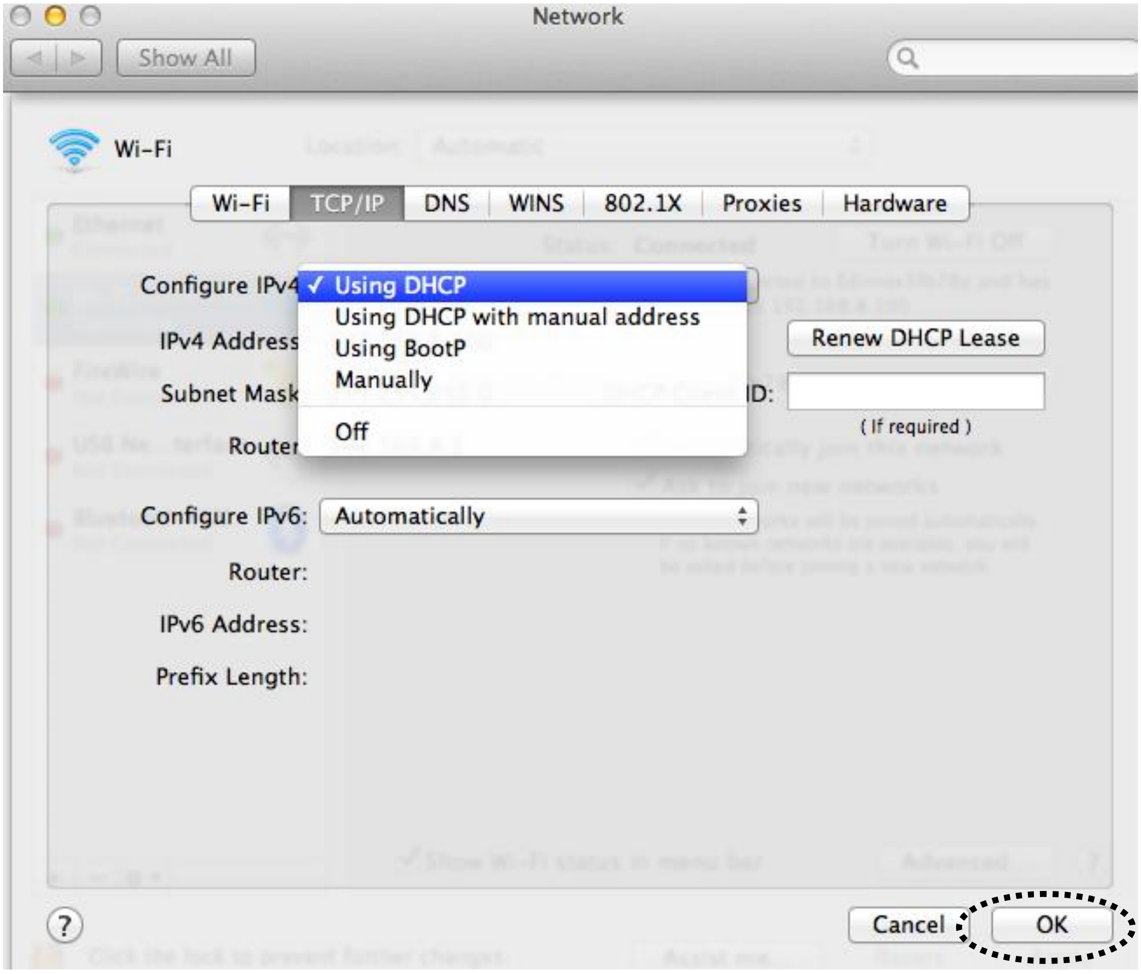
Router:

IPv6 Address:

Prefix Length:

4. Open the drop down menu labeled "Configure IPv4" and select "Using

DHCP”. Then click “OK” to save the setting and continue.



Configure IPv4: Using DHCP

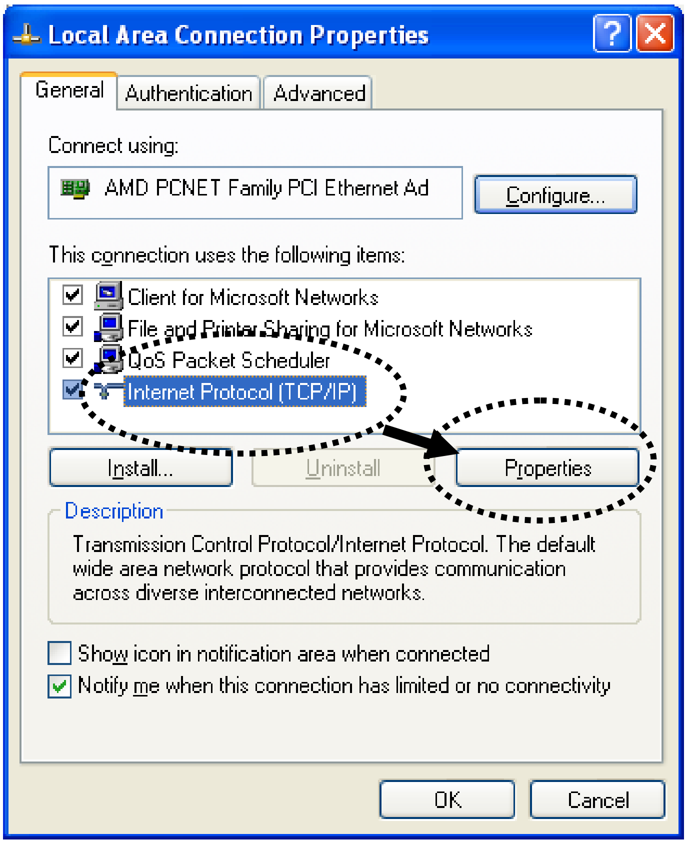
Configure IPv6: Automatically

IV-1-2. How to modify the IP address of your PC or Macintosh

Please follow the instructions appropriate for your operating system.

IV-1-2-1. Windows XP

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Double-click the “Network and Internet Connections” icon, click “Network Connections”, and then double-click “Local Area Connection”. The “Local Area Connection Status” window will then appear, click “Properties”.



Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

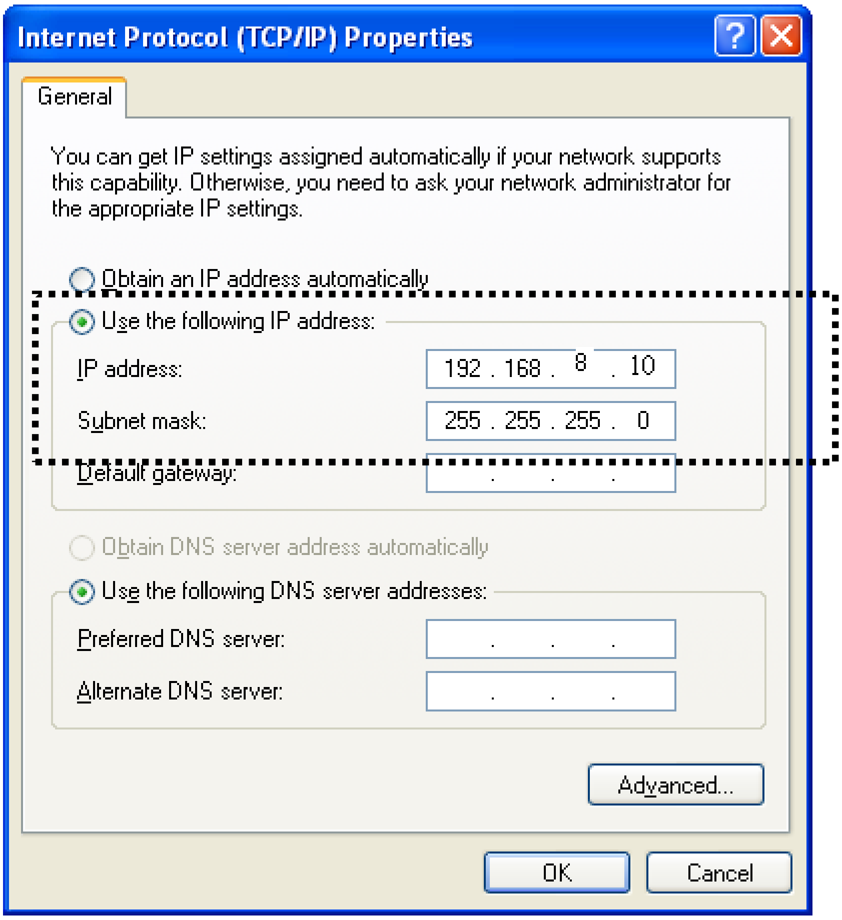
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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

   IP address: 192.168.8.10
   Subnet Mask: 255.255.255.0

   Click ‘OK’ when finished.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 8 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

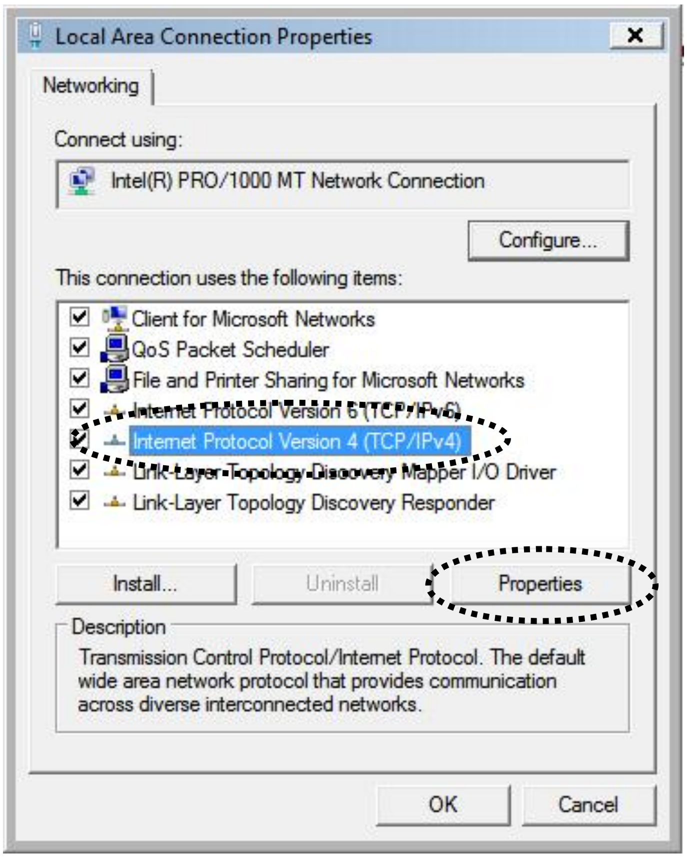
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

IV-1-2-2. Windows Vista

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

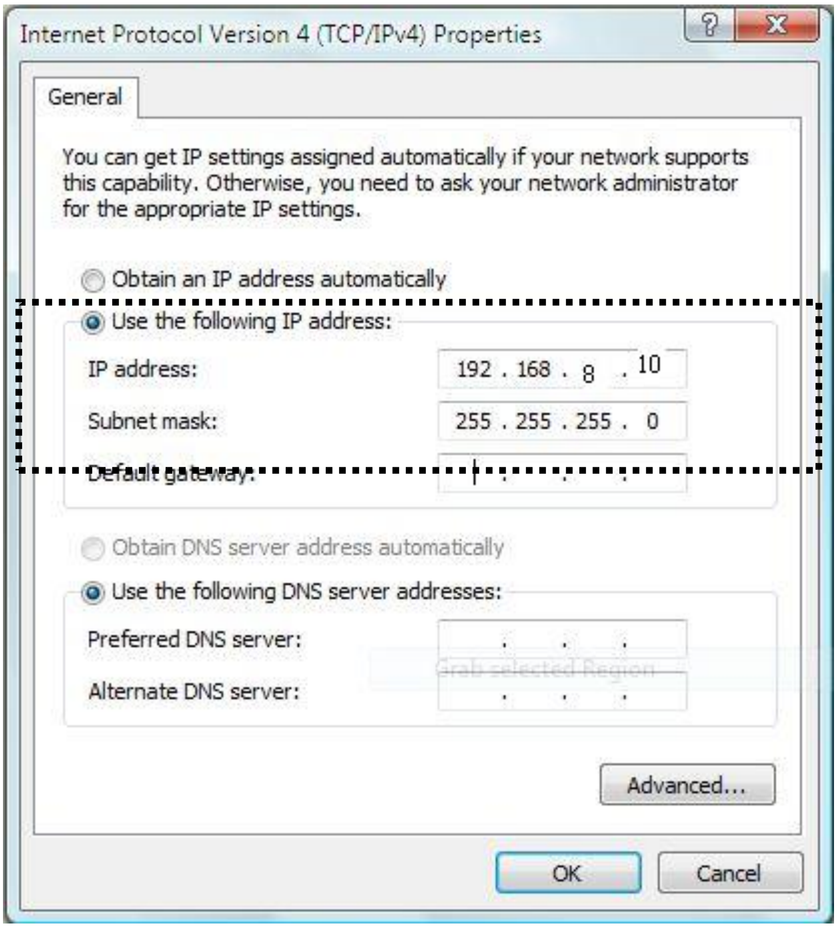
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

   IP address: 192.168.8.10
   Subnet Mask: 255.255.255.0

   Click 'OK' when finished.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 8 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

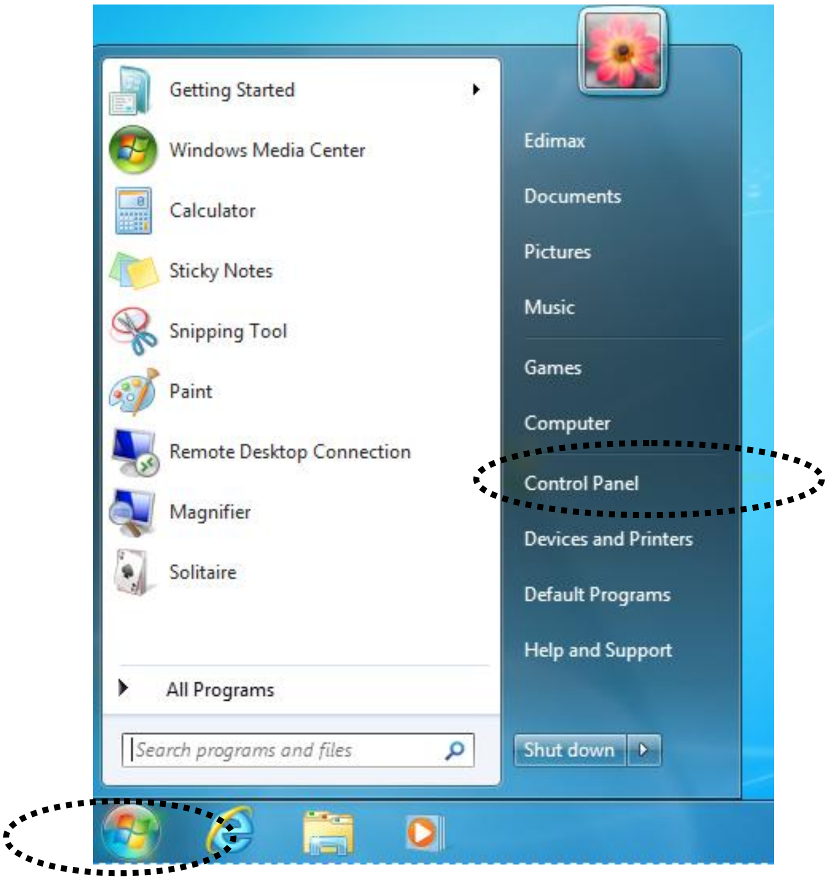
● Use the following DNS server addresses:

Preferred DNS server: . . .

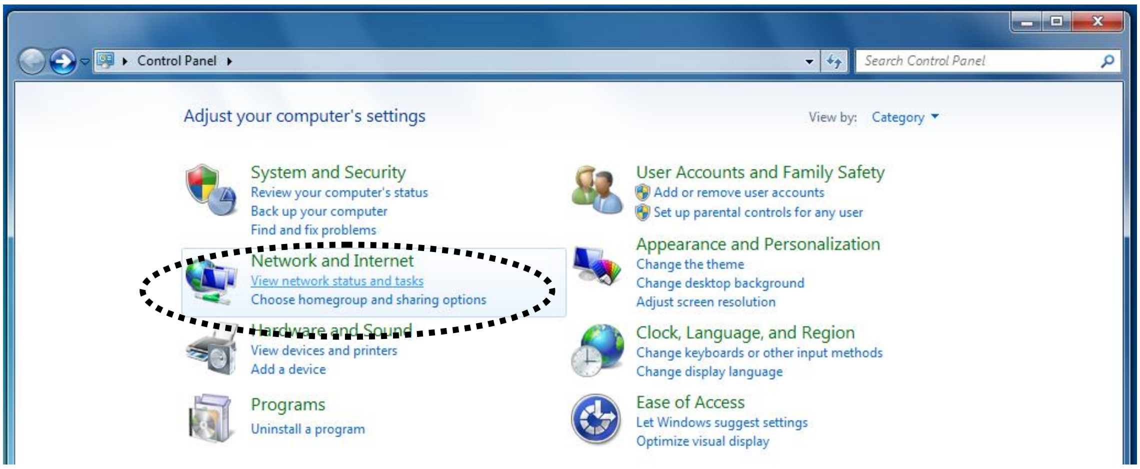
Alternate DNS server: . . .

IV-1-2-3. Windows 7

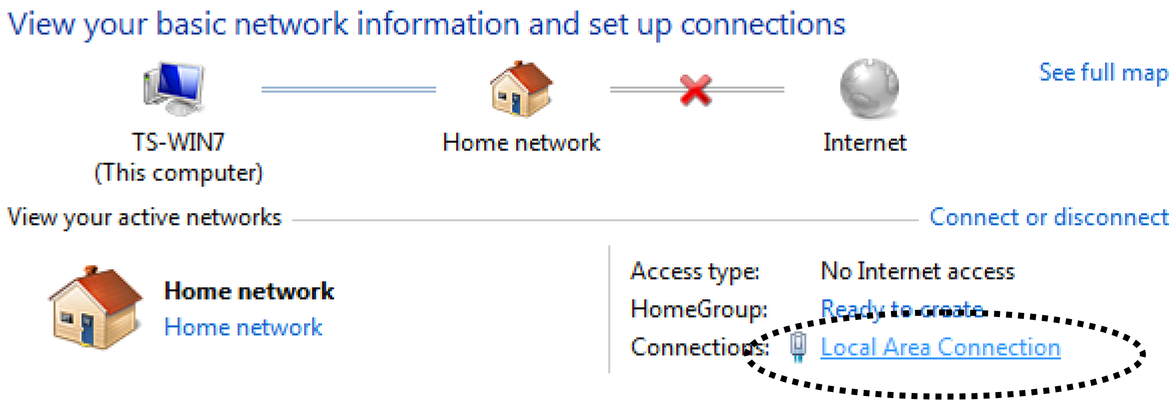
1. Click the "Start" button (it should be located in the lower-left corner of your computer), then click "Control Panel".



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


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click “Local Area Connection”.



View your basic network information and set up connections

TS-WIN7
(This computer)

Home network

Internet

See full map

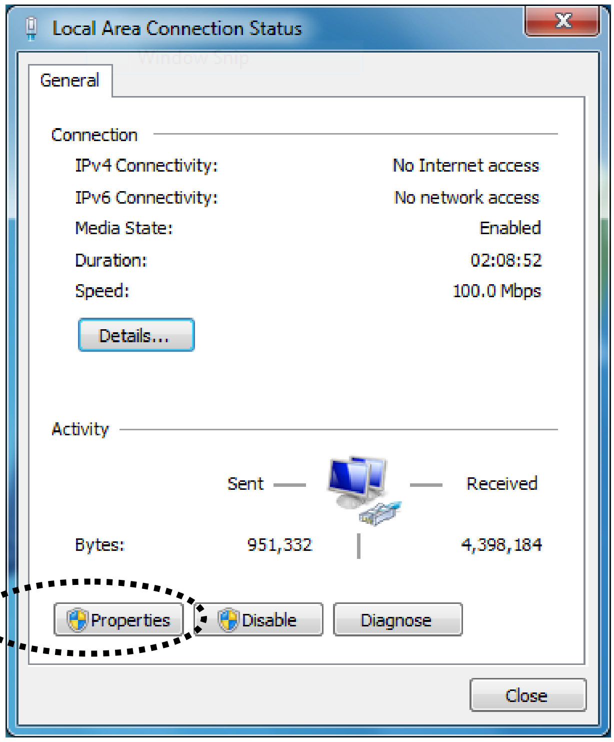
View your active networks

Connect or disconnect

Home network
Home network

Access type: No Internet access
HomeGroup: Ready to create
Connections: Local Area Connection

4. Click “Properties”.



Local Area Connection Status

General

Connection

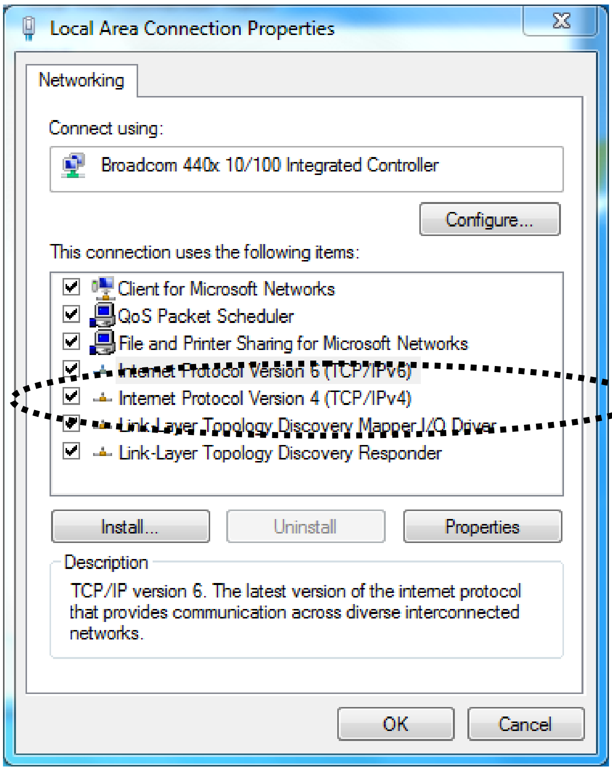
IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	02:08:52
Speed:	100.0 Mbps

Details...

Activity

	Sent	Received
Bytes:	951,332	4,398,184

5. Select “Internet Protocol Version 4 (TCP/IPv6) and then click “Properties”.



Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

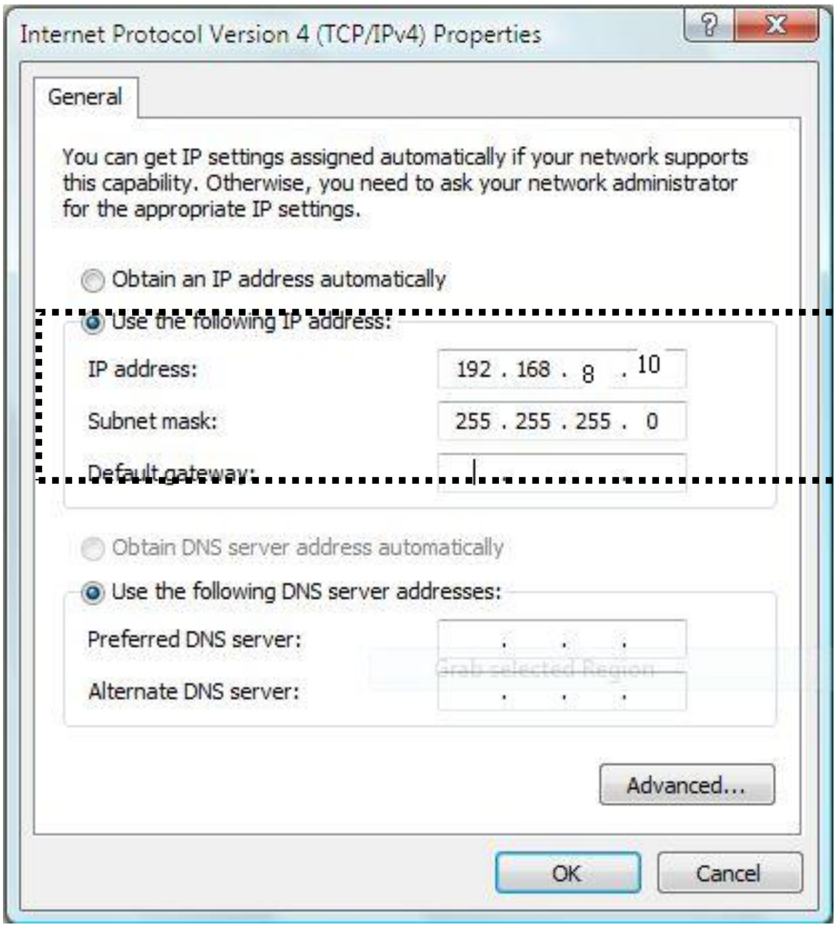
Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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

   IP address: 192.168.8.10
   Subnet Mask: 255.255.255.0

   Click ‘OK’ when finished.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 8 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

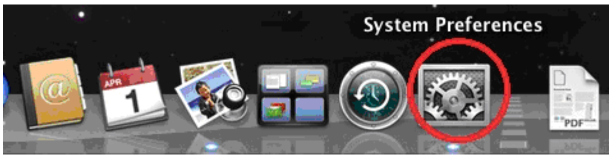
● Use the following DNS server addresses:

Preferred DNS server: . . .

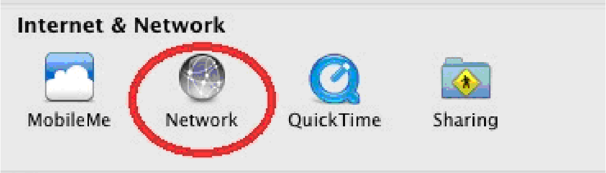
Alternate DNS server: . . .

IV-1-2-4. Mac OS

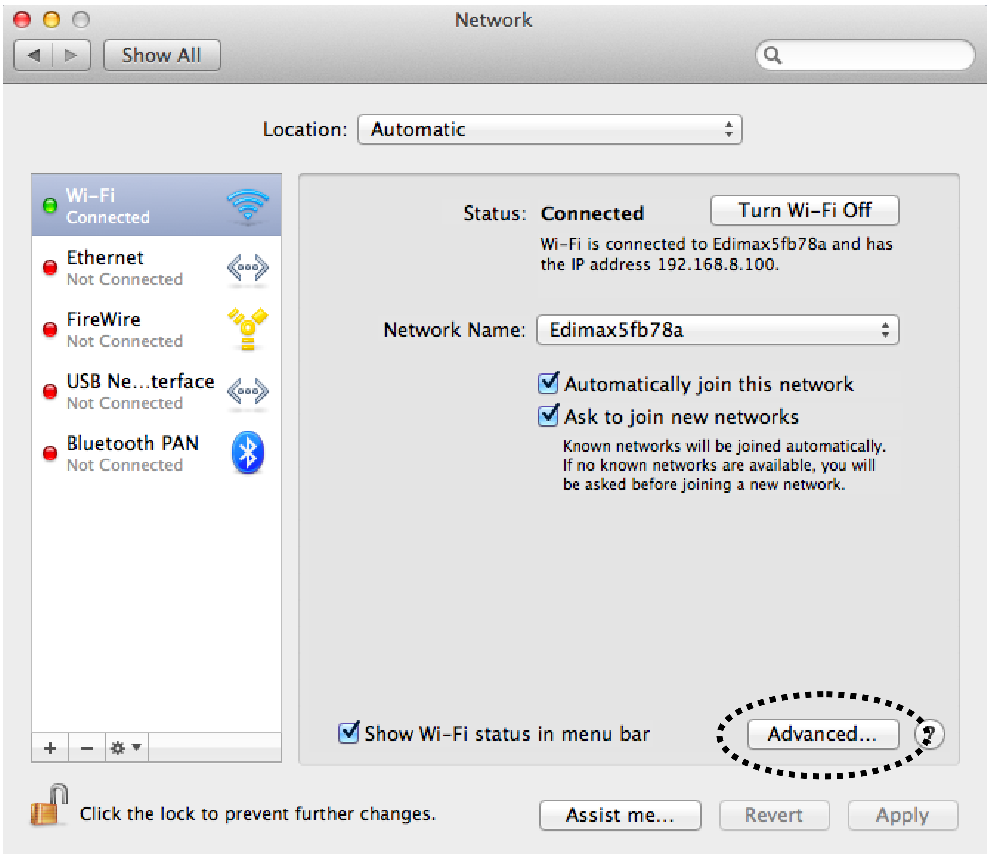
1. Have your Macintosh computer operate as usual, and click on “System Preferences”



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



3. Here you will see all of your network connections. You need to remove any Ethernet cable that may be connected, so that the “Ethernet” status in the left panel displays “Not Connected”, as shown below. Choose “Wi-Fi” from the panel on the left side, and then click “Advanced” in the bottom right corner.



Location: Automatic

Wi-Fi
Connected

Ethernet
Not Connected

FireWire
Not Connected

USB Ne...terface
Not Connected

Bluetooth PAN
Not Connected

Status: **Connected**

Wi-Fi is connected to Edimax5fb78a and has the IP address 192.168.8.100.

Network Name: Edimax5fb78a

☑ Automatically join this network

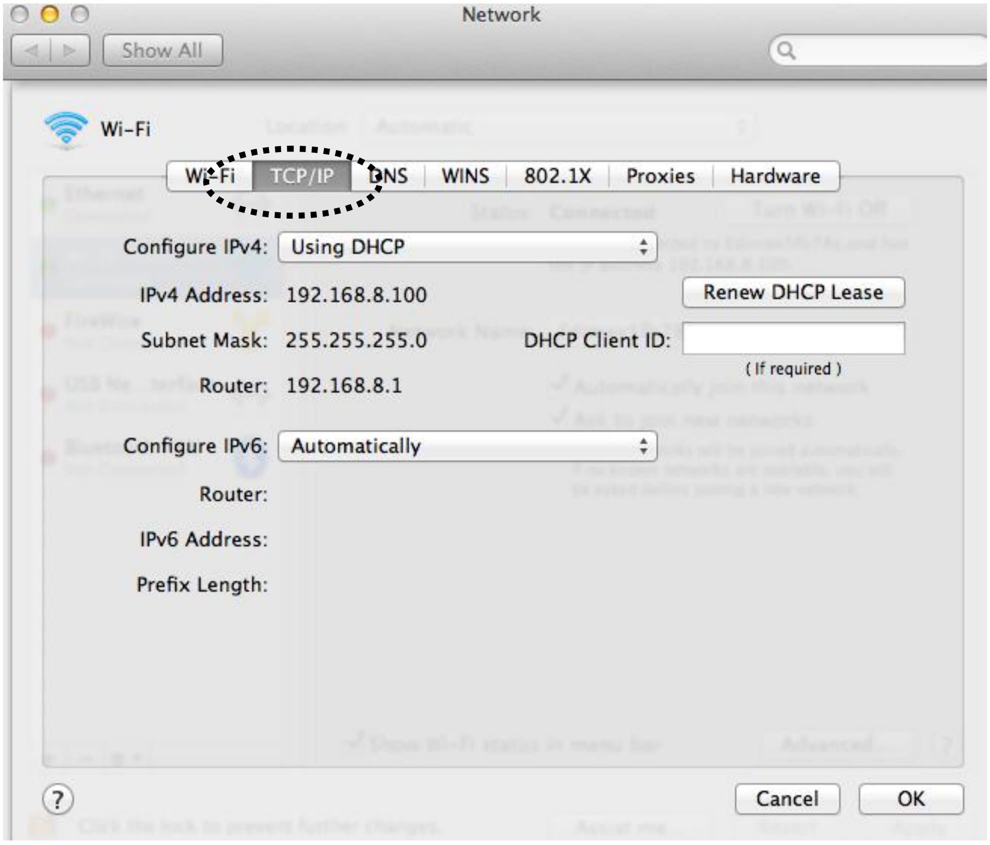
☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show Wi-Fi status in menu bar

Click the lock to prevent further changes.

4. Now select "TCP/IP" from the menu across the top of the screen.



Configure IPv4: Using DHCP

IPv4 Address: 192.168.8.100

Subnet Mask: 255.255.255.0

Router: 192.168.8.1

DHCP Client ID:

(If required)

Configure IPv6: Automatically

Router:

IPv6 Address:

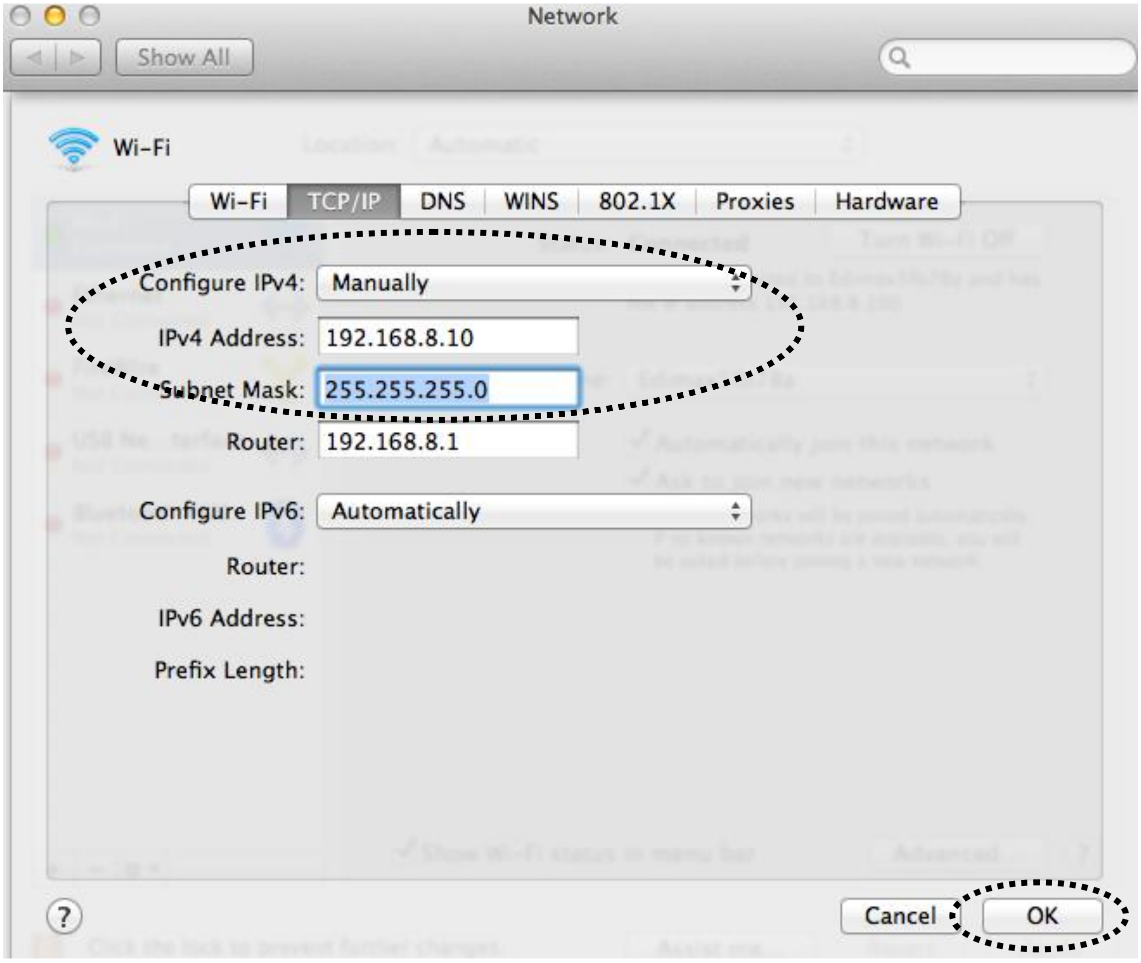
Prefix Length:

5. Open the drop down menu labeled "Configure IPv4" and select "Manually".

Then input the following values:

IPv4 address: 192.168.8.10
Subnet Mask: 255.255.255.0

Click “OK” to save the setting and continue.



Configure IPv4: Manually
IPv4 Address: 192.168.8.10
Subnet Mask: 255.255.255.0
Router: 192.168.8.1
Configure IPv6: Automatically
Router:
IPv6 Address:
Prefix Length:

IV-2. Troubleshooting

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

Scenario	Solution
My travel router can’t locate a wireless access point/wireless device when using the “Site Survey” function.	a. Click “Rescan” several more times and see if the wireless access point/device appears. b. Adjust the position of the travel router, or move closer to a known wireless access point. c. If the SSID of the access point you wish to connect to is hidden (nothing displayed in the “SSID” field in the “Site Survey” function), then you need to input the SSID manually. Ensure that you input the correct SSID.
My travel router can’t establish a connection with a particular wireless access point.	a. Click “Connect” several more times and see if you can establish a connection. b. Ensure that you input the correct passphrase/security key if connecting to an access point with encryption. c. It is possible that the access point you wish to connect to only allows network cards with specific MAC address’s to establish connections. Request that the owner/administrator of the access point add your MAC address to the list.
I can’t log onto the browser-based configuration interface: the access point is not responding.	a. Make sure travel router is powered on. Check the LED on the front panel. If the LED is out, then check the USB connection. b. Use your wireless device connects to this travel router wirelessly. c. Make sure you are using the correct IP address. d. If you are using a MAC or IP address

	filter, try to connect the access point to another computer. e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can obtain an IP address. f. If you are experiencing problems after a firmware upgrade, please contact your dealer of purchase for help.
I can't locate the travel router with my wireless client.	a. Check if "Broadcast ESSID" (in the "Wireless Advanced" section of the browser-based configuration interface) is "Enabled" or "Disabled". If "Disabled" you need to input the ESSID into your wireless client manually. b. Try moving closer to the travel router.
File transfers are slow or frequently interrupted.	a. Try to move closer to where the wireless access point is located. b. Try again later. Your local network may be experiencing technical difficulties or very high usage. c. Change channel number.
I can't log onto the browser-based configuration interface: incorrect password.	a. Password is case-sensitive. Make sure the "Caps Lock" light is not illuminated. b. If you do not know your password, restore the device to factory settings.
The travel router is extremely hot.	a. It is normal for the travel router to heat up during frequent use. If you can safely place your hand on the travel router, the temperature of the device is at a normal level. b. If you smell burning or see smoke coming from travel router or A/C power adapter, then disconnect the travel router and A/C power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.
When I launch a	a. Ensure that the router is powered on

web browser, it doesn't automatically redirect to the browser based configuration interface.	correctly. If you recently rebooted the device, please remember that the router will be unresponsive for up to 1.5 minutes after a reboot. b. Try the following URL's: - http://edimax.go - http://edimax.setup - http://192.168.8.1 Please remember to include http:// in the URL. c. Ensure that your wireless client is connected to the travel router's SSID. d. Try using an alternative web browser.
I can't save connection information to the "Access Keeper".	a. Connection information will only be saved to the "Access Keeper" when using iQ Setup. Manual configurations made using the browser based configuration interface will not be saved in the "Access Keeper".
"Access Keeper" has deleted my connection information.	a. "Access Keeper" can only store 10 sets of connection information. When 10 sets have been saved, any additional connections will replace the 1st, and then the 2nd (and so on) stored sets of information. If you wish keep a particular set of settings, please delete any other stored sets of information which are not used frequently, so that the "Access Keeper" has enough available space to save new connections.

IV-3. Glossary

1. **What is the IEEE 802.11g standard?**

   802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

   802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

   The standard specifically calls for:

   A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

   B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard?**

   The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support?**

   The product supports the following IEEE 802.11 functions:

   - CSMA/CA plus Acknowledge Protocol
   - Multi-Channel Roaming
   - Automatic Rate Selection
   - RTS/CTS Feature
   - Fragmentation
   - Power Management

4. **What is Ad-hoc?**

   An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN card, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. **What is Infrastructure?**

   An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. **What is BSS ID?**

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. **What is WEP?**

   WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. **What is TKIP?**

   TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. **What is AES?**

   AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. **Can Wireless products support printer sharing?**

    Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. **Would the information be intercepted while transmitting on air?**

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. **What is DSSS? What is FHSS? And what are their differences?**

    Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. **What is Spread Spectrum?**

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. What is WPS?

WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access point automatically. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.

IV-4. Technical Support

Support documentation is available on the enclosed CD and on our global websites.

Headquarters
Tel: +886-2-77396888
Fax: +886-2-77396887
Support: support@edimax.com.tw

European Headquarters
Tel: +31-499-377344
Fax: +31-499-372647
Support: support@edimax.nl

French Office
Tel: +33-160535680
Fax: +33-160535689
Support: support@edimax.fr

German Office
Tel: +49-215488-77334
Fax: +49-215488-77339
Support: support@edimax-de.eu

Poland Office
Tel: +48-22-6079480
Fax: +48-22-6079481
Support: support@edimax.pl

Romania Office
Tel: +40-31-4250126
Fax: +40-31-4250125
Support: support@edimax.ro

Russia Office
Tel: +7-499-7266678
Email: sales@edimax.ru
Support: support@edimax.ru

Ukraine Office

Tel: +38 (044) 4983091, +38 (044) 4983092
Fax: +38 (044) 4983093
Support: support@edimax.ua

United Kingdom Office

Tel: +44-845-1238307
Fax: +44-845-1238306
Support: support@edimax.co.uk

USA Office

Tel: +1-408-4961105
Fax: +1-408-9801530
Support: support@edimax.com

Australia Office

Tel: +61-3-95431888
Fax: +61-3-98992746
Tech Support: 1300 540 833
Email: sales@edimax-au.com
Support: support@edimax-au.com

China Office

Tel: +8610-82665815
Fax: +8610-82665795
Support: service@edimax.com.cn

Hong Kong Office

Tel: +852-2169 6311
Fax: +852-2169 6300
Support: service@edimax.com.cn

India Office

Technical & RMA Support: +91 9867520529 / 9888060206
Bulk & Corporate Enquiries: +91 9818029555
Working Hours: 10am ~ 7pm (IST) Monday ~ Saturday (except national holidays)
Email: support_india@edimax.com.tw

MEA Office

Tel: +971-4-804-1888
Support: +971 800 334629 [800-EDIMAX]
Fax: +971-4-883-4079

Support: technical.support@edimax-me.com

South East Asia Office

Singapore Authorized Service Centre
Tel: +65 6334 2298 (11am ~ 8pm, Monday ~ Sunday)
Technical Support Hotline: 31062273
(9am~6pm, Monday ~ Friday except national holidays)
Support: support@edimax.com.sg

Cambodia Service Centre

Sales & Technical Hotline: +855 (23) 996 638
(9am ~ 5:30pm, Monday ~ Friday except national holidays)
(9am ~ 12:30pm Saturday)
Support: service@i-qlick.com

Malaysia - Kuala Lumpur Authorized Service Centre

Technical Hotline: 03 2052 4288; 03 9130 7728
(11am ~ 8pm, Monday ~ Friday except national holidays)
Email: sales@edimax.com.sg
Support: support@edimax.com.sg

Indonesia - Jakarta Authorized Service Centre

Sales & Technical Hotline: 021 70777 629
(9am ~ 6pm, Monday ~ Sunday except national holidays)
Support: idsupport@edimax.com.sg

EDIMAX
NETWORKING PEOPLE TOGETHER

Edimax Technology co., Ltd
6F., No.3, Wu-Chuan 3rd Road, Wu-Gu,
New Taipei

Edimax Technology Europe B.V.
Nijverheidsweg 25 5683 CJ Best
The Netherlands

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

www.edimax.com