N300 Wireless LAN 11n

Ceiling-Mount Access Point

User’s Manual

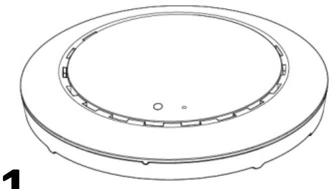
Version: 1.0

(October, 2014)

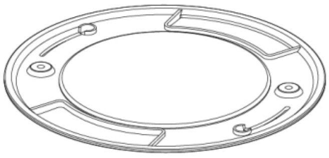
CONTENTS

I. Product Information

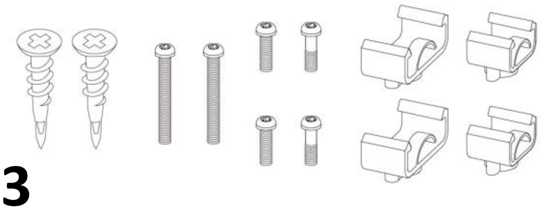
I-1. Package Contents



1



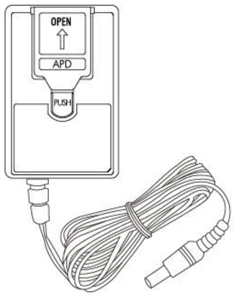
2



3

4

5

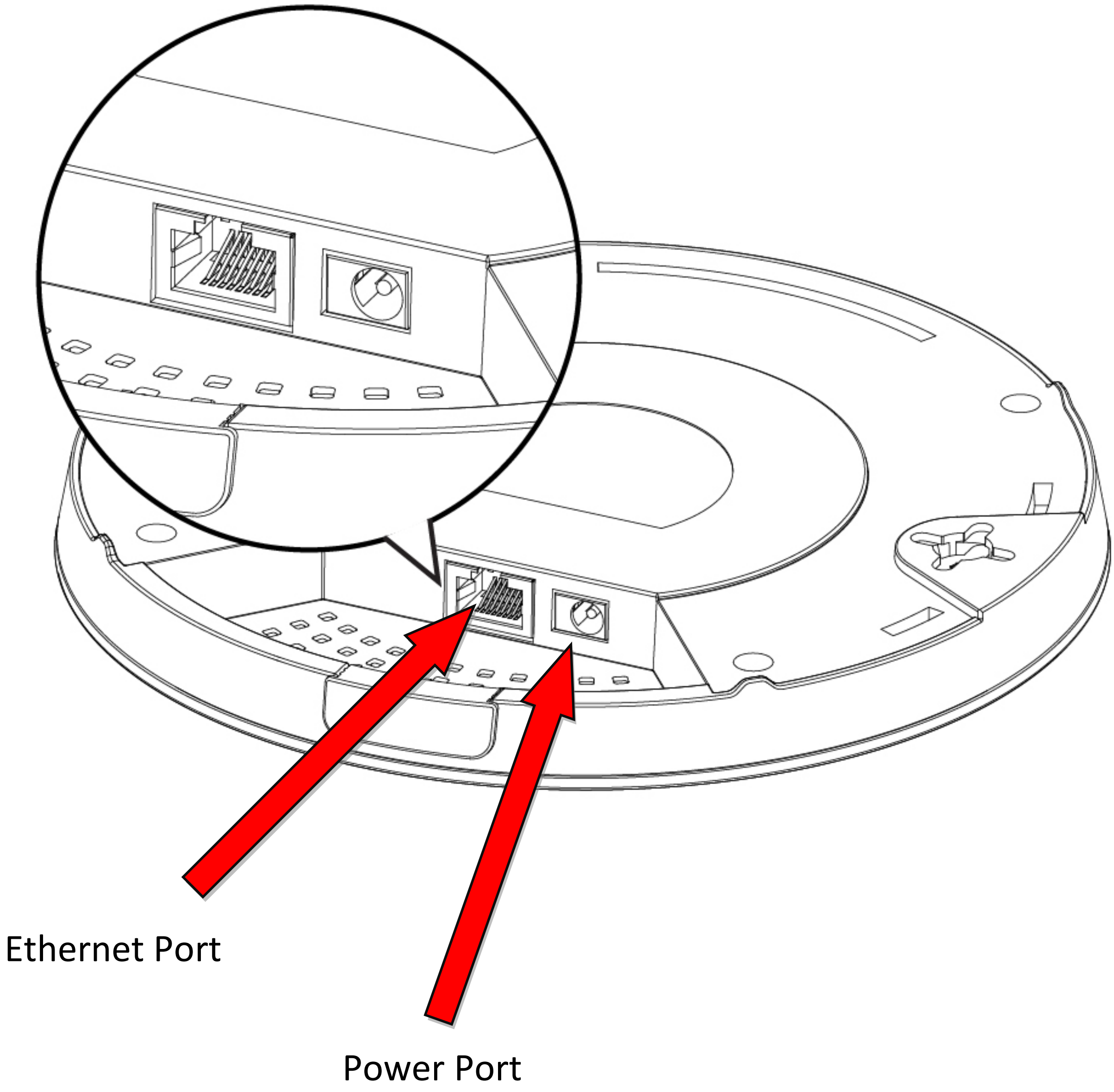


1. Access Point
2. Ceiling Mount Bracket
3. T-Rail Mounting Kit & Screws
4. Quick Installation Guide
5. Power Adapter (see **I-6. Multi-Region Power Adapter**)

I-2. System Requirements

- Existing cable/DSL modem & router
- Computer with web browser for access point configuration

I-3. Hardware Overview



I-4. LED Status

Blue	Amber	Status
Off	Off	AP is off
On	On	Booting up, Going to Reboot
On	Off	AP is up and every function working properly
Long Flashing	OFF	Firmware upgrading
Short Flashing	Off	Ready to reset to factory default
Off	Flashing	Error

I-5. Reset

If you experience problems with your access point, you can reset the device back to its factory settings. This resets **all** settings back to default.

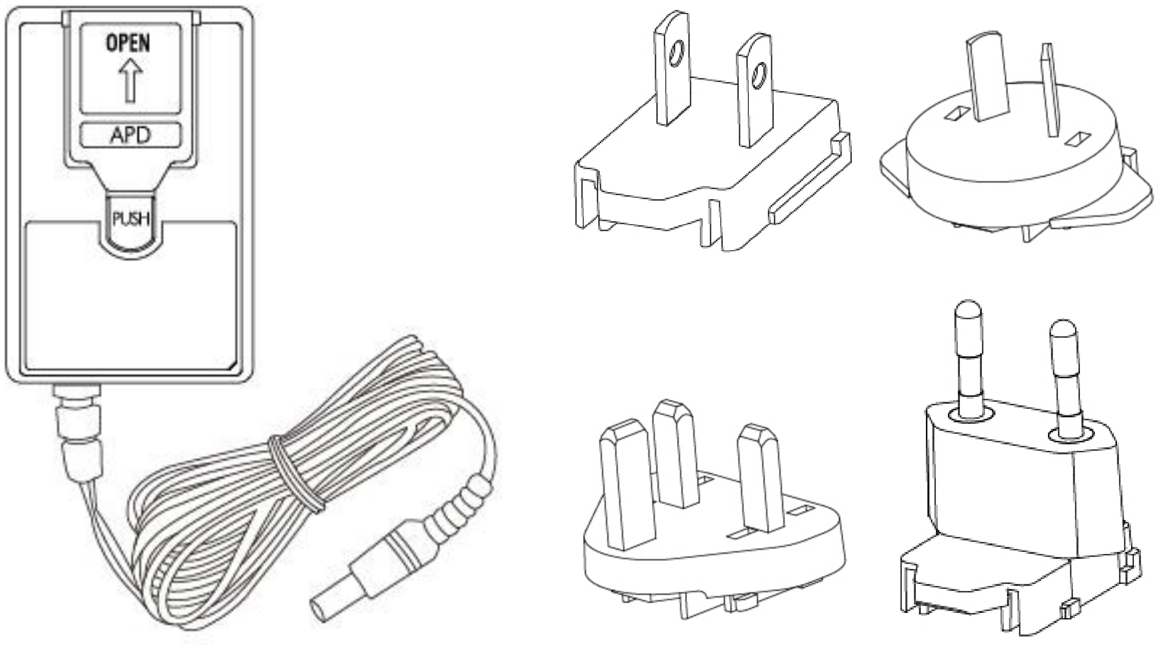
1. Press and hold the reset button on the access point for at least 10 seconds then release the button.

⚠ ***You may need to use a pencil or similar sharp object to push the reset button.***

2. Wait for the access point to restart. The access point is ready for setup when the LED is **blue**.

I-6. Multi-Region Power Adapter

The included power adapter has four changeable heads for different AC sockets according to your region.



I-7. Safety Information

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

1. The access point is designed for indoor use only; do not place the access point outdoors.

2. Do not place the access point 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 access point.

4. Handle the access point with care. Accidental damage will void the warranty of the access point.

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

6. Do not place the access point on paper, cloth, or other flammable materials. The access point may become hot during use.

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

8. The access point 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 access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

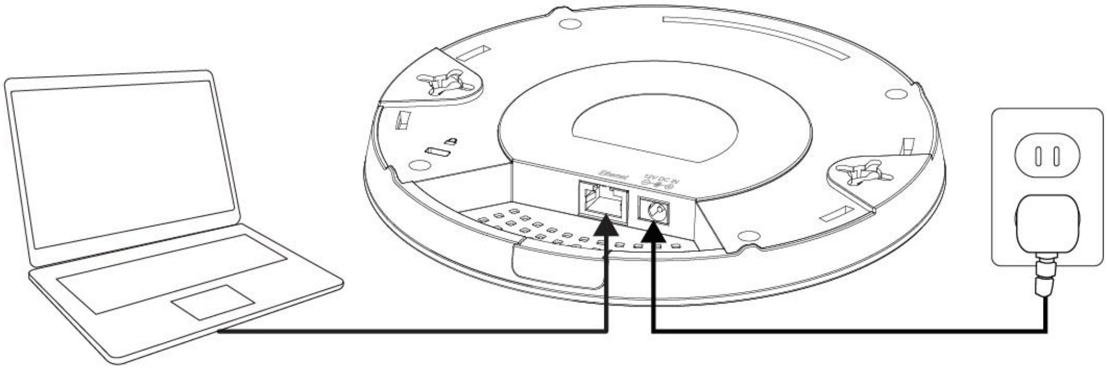
I. Quick Setup

Please follow the instructions in the chapters below to setup your access point and then configure its basic settings.

II-1. Initial Setup

1. Connect the access point to a computer via Ethernet cable.

2. Connect the power adapter to the access point’s 12V DC port and plug the power adapter into a power supply.

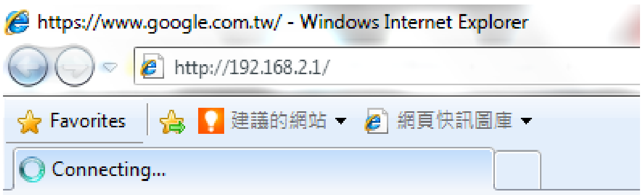


3. Please wait a moment for the access point to start up. The access point is ready when the LED is **blue**.

4. Set your computer’s IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, please refer to **IV-1. Configuring your IP address** for more information.

> ***Please ensure there are no other active network connections on your computer (disconnect Wi-Fi connections and Ethernet cables).***

5. Enter the access point’s default IP address **192.168.2.1** into the URL bar of a web browser.

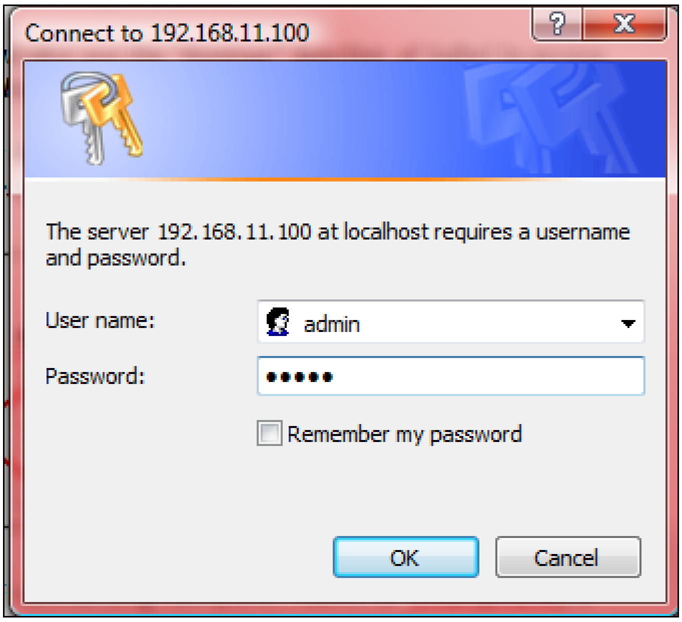


https://www.google.com.tw/ - Windows Internet Explorer

http://192.168.2.1/

Connecting...

6. You will be prompted for a username and password. Enter the default username “admin” and the default password “admin”.



Connect to 192.168.11.100

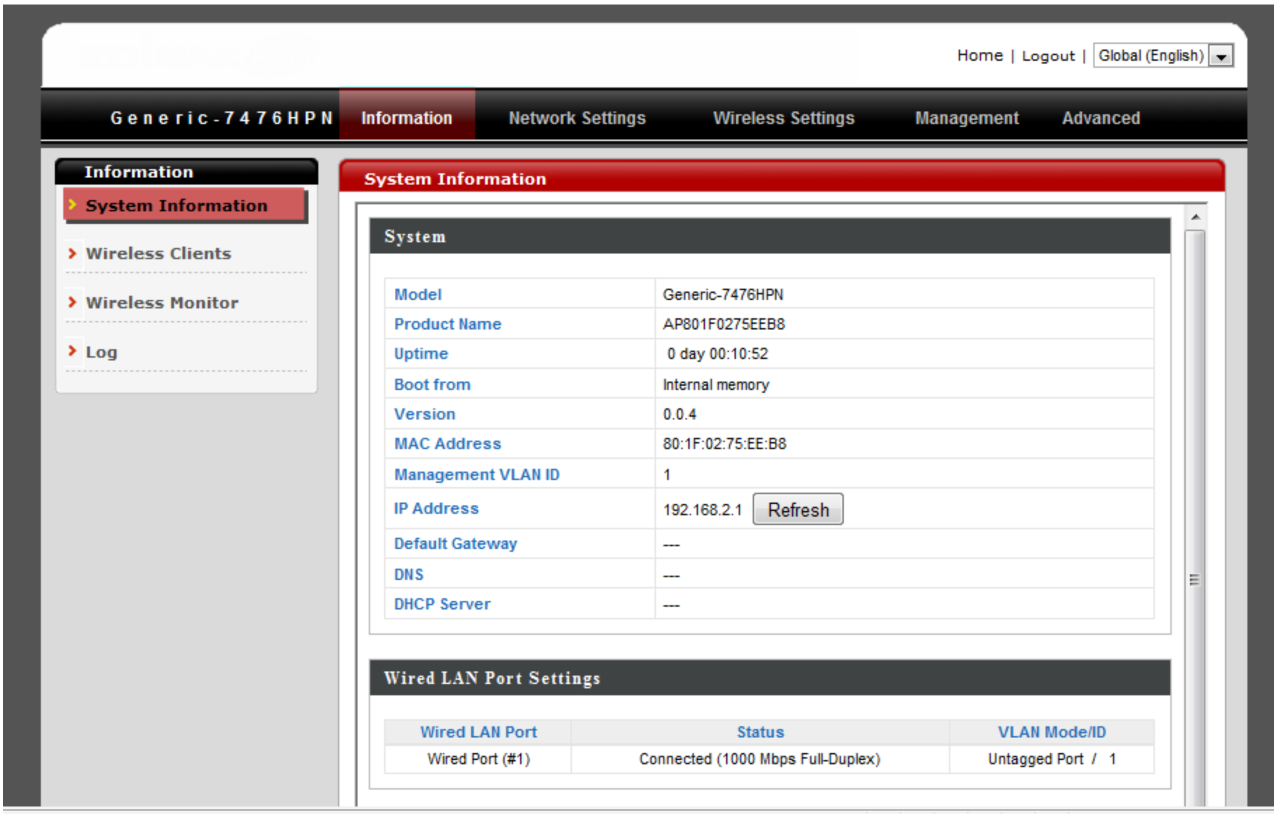
The server 192.168.11.100 at localhost requires a username and password.

User name: admin

Password: ●●●●●

□ Remember my password

7. You will arrive the “System Information” screen shown below.



System Information

System

Model	Generic-7476HPN
Product Name	AP801F0275EEB8
Uptime	0 day 00:10:52
Boot from	Internal memory
Version	0.0.4
MAC Address	80:1F:02:75:EE:B8
Management VLAN ID	1
IP Address	192.168.2.1
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
Wired Port (#1)	Connected (1000 Mbps Full-Duplex)	Untagged Port / 1

8. Next, please follow the instructions below in **II-1. Basic Settings** to configure the access point’s basic settings.

For more advanced configurations, please refer to IV. Browser Based Configuration Interface.

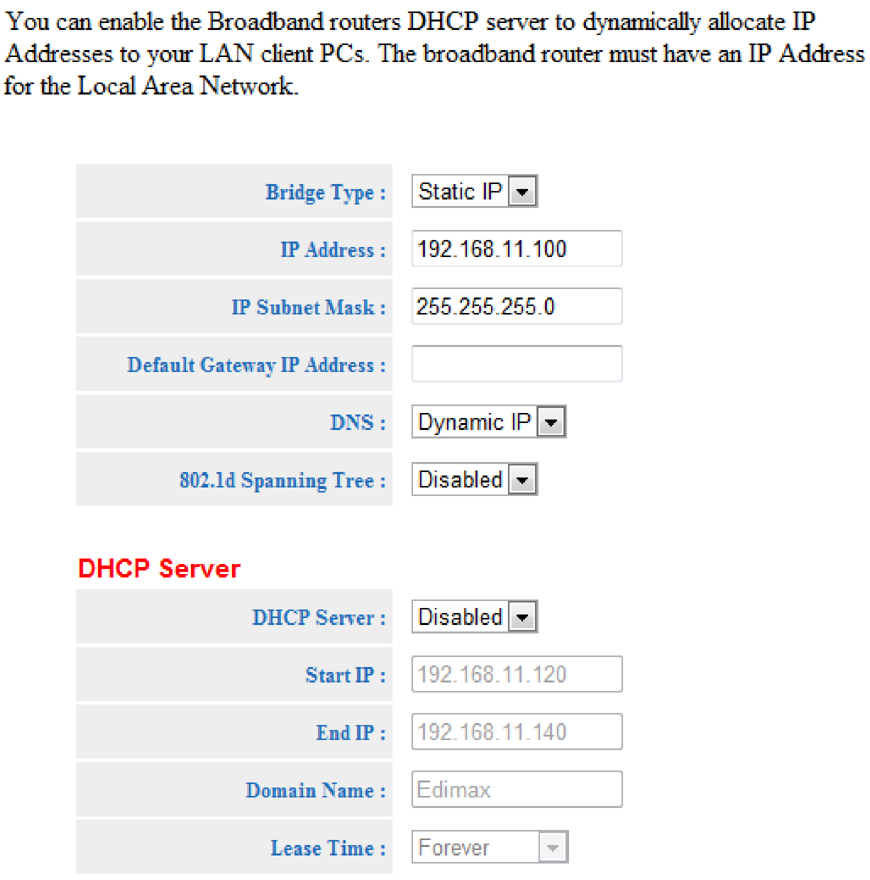
II-2. Basic Settings

The instructions below will help you to configure the following basic settings of the access point:

It is recommended you configure these settings before using the access point.

- ***LAN IP Address***
- ***2.4GHz SSID & Security***
- ***Login Password***
- ***Time & Date***

1. To change the access point's LAN IP address, go to **"Network Settings" > "LAN-side IP Address"** and you will see the screen below.



You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

Bridge Type :	Static IP
IP Address :	192.168.11.100
IP Subnet Mask :	255.255.255.0
Default Gateway IP Address :	
DNS :	Dynamic IP
802.1d Spanning Tree :	Disabled

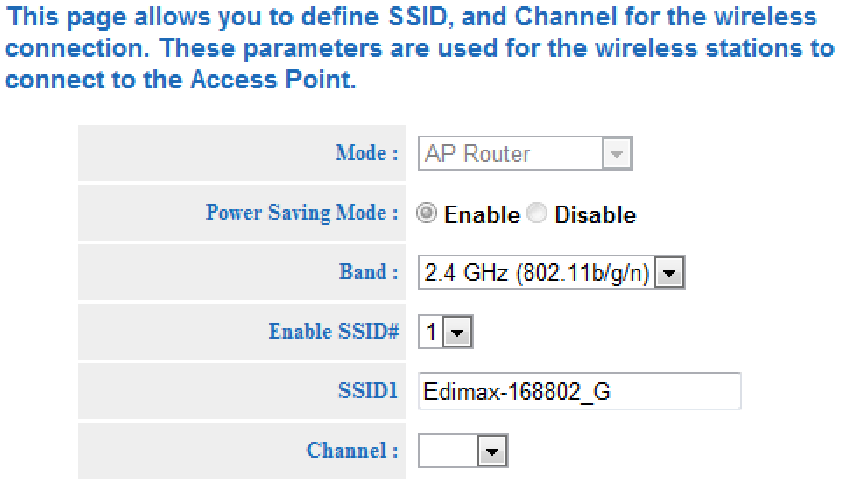
DHCP Server

DHCP Server :	Disabled
Start IP :	192.168.11.120
End IP :	192.168.11.140
Domain Name :	Edimax
Lease Time :	Forever

2. Enter the IP address settings you wish to use for your access point. Click "Apply" to save the changes the wait a few moments for the access point to reload.

⚠ ***When you change your access point's IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP*** *192.168.2.1.*

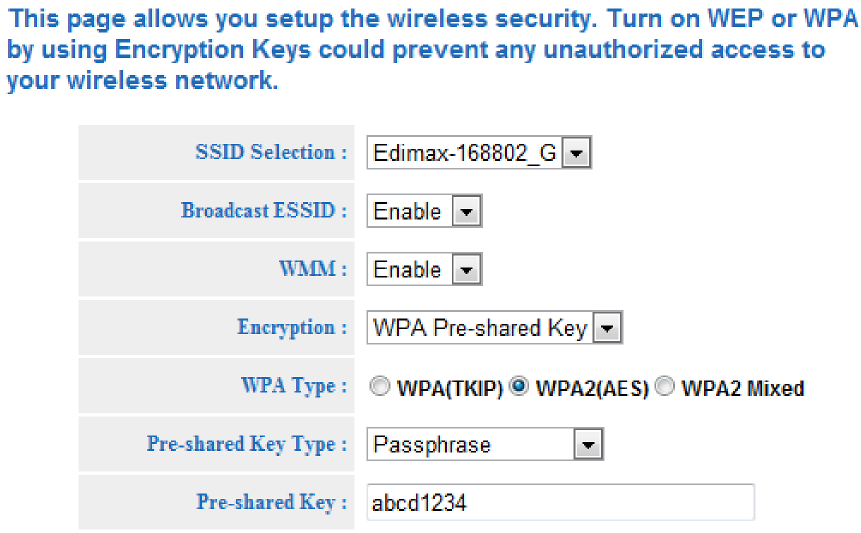
3. To change the SSID and password of your access point's wireless network(s), go to **"Wireless Setting" > "2.4GHz" > "Basic"**. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".



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

Mode :	AP Router
Power Saving Mode :	● Enable ○ Disable
Band :	2.4 GHz (802.11b/g/n)
Enable SSID#	1
SSID1	Edimax-168802_G
Channel :	

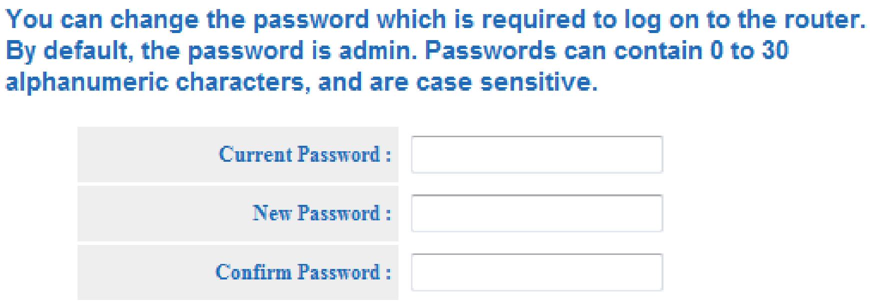
4. Go to **"Wireless Setting" > "2.4GHz" > "Security"**. Enter a new password for your 2.4GHz wireless network in the "SSID1" field and click "Apply".



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.

SSID Selection :	Edimax-168802_G
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WPA Pre-shared Key
WPA Type :	○ WPA(TKIP) ● WPA2(AES) ○ WPA2 Mixed
Pre-shared Key Type :	Passphrase
Pre-shared Key :	abcd1234

5. To change the login password for the browser based configuration interface, go to **“Toolbox” > “Admin”**.

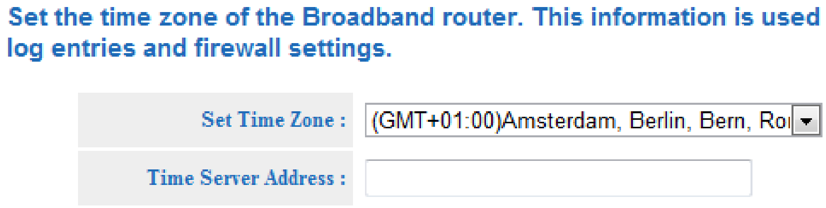


You can change the password which is required to log on to the router. By default, the password is admin. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.

Current Password :	
New Password :	
Confirm Password :	

6. Complete the “Current Password”, “New Password” and “Confirm Password” fields and click “Apply”.

7. To set the correct time for your access point, go to **“Toolbox” > “Time Setting”**.



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

Set Time Zone :	(GMT+01:00)Amsterdam, Berlin, Bern, Ro
Time Server Address :	

8. Select the correct time zone for your access point from the drop down list. The access point also supports NTP (Network Time Protocol) so alternatively you can enter the host name or IP address of a time server. Click “Apply” when you are finished.

9.The basic settings of your access point are now configured. Please refer to **III. Hardware Installation** for guidance on connecting your access point to a router or PoE switch and/or fixing your access point to a ceiling. Or refer to **IV. Browser Based Configuration Interface** for help with advanced configurations.

II-3. Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices.

After you have set up the access point as explained in **II. Installation** you can use the WPS button to establish a connection between the access point and a WPS-compatible wireless device/client.

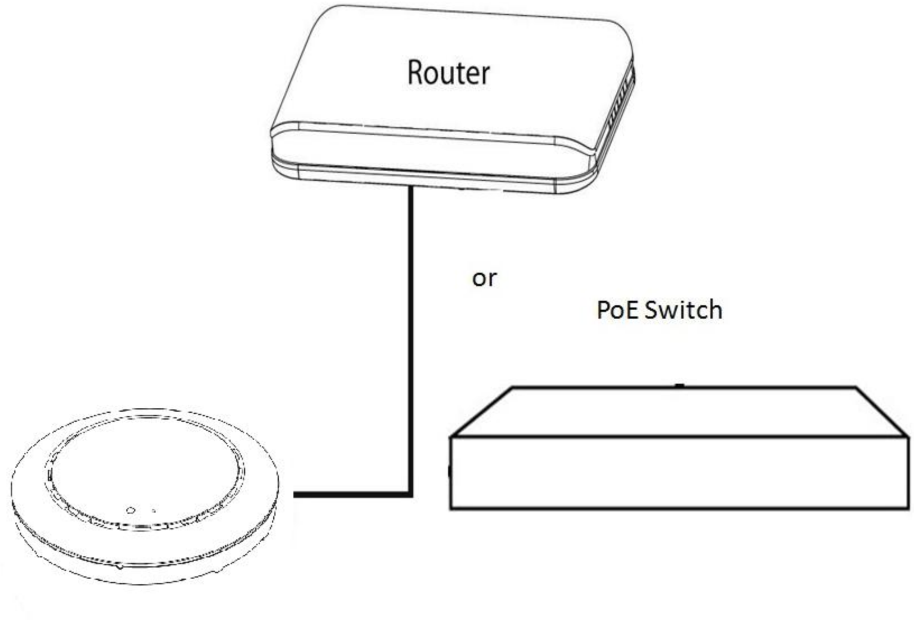
1. Press and hold the WPS/Reset button on the front of the access point for 2 seconds.

2. Within two minutes, activate WPS on your WPS-compatible wireless device. Please check the documentation for your wireless device for information regarding its WPS function.

3. The devices will establish a connection.

III-1. Connecting the access point to a router or PoE switch

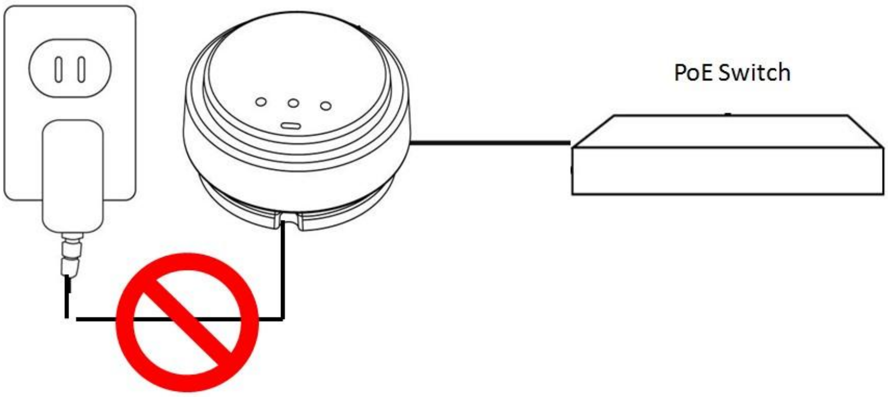
1. Connect the access point to a router or PoE switch via Ethernet cable.



2. If you are using a router, then connect the power adapter to the access point’s 12V DC port and plug the power adapter into a power supply.

3. If you are using a PoE (Power over Ethernet) switch then it is not necessary to use the included power adapter, the access point will be powered by the PoE switch.

⚠ ***Do not use the power adapter if you are using a PoE switch.***


PoE Switch

III-2. Mounting the access point to a ceiling

To mount the access point to a ceiling, please follow the instructions below and refer to diagram **A** & **B**.

For Wooden Ceilings (refer to diagram A):

1. Place the ceiling mount bracket to a ceiling in your desired location and insert screw **iii** through hole **i** (x 2)and tighten to fix the bracket in place.

2. When the ceiling bracket is in place, inset screw **iv** into hole **v** (x 2) on the access point.

3. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

4. Lock the access point firmly into place when by twisting it to align screws **iv** with the grooves in the ceiling mount.

For Other Ceilings (refer to diagram B):

1. Place the ceiling mount bracket to a ceiling in your desired location and Insert screw **ii** through hole **i** (x 2) and tighten to fix the bracket in place, as shown in **A**.

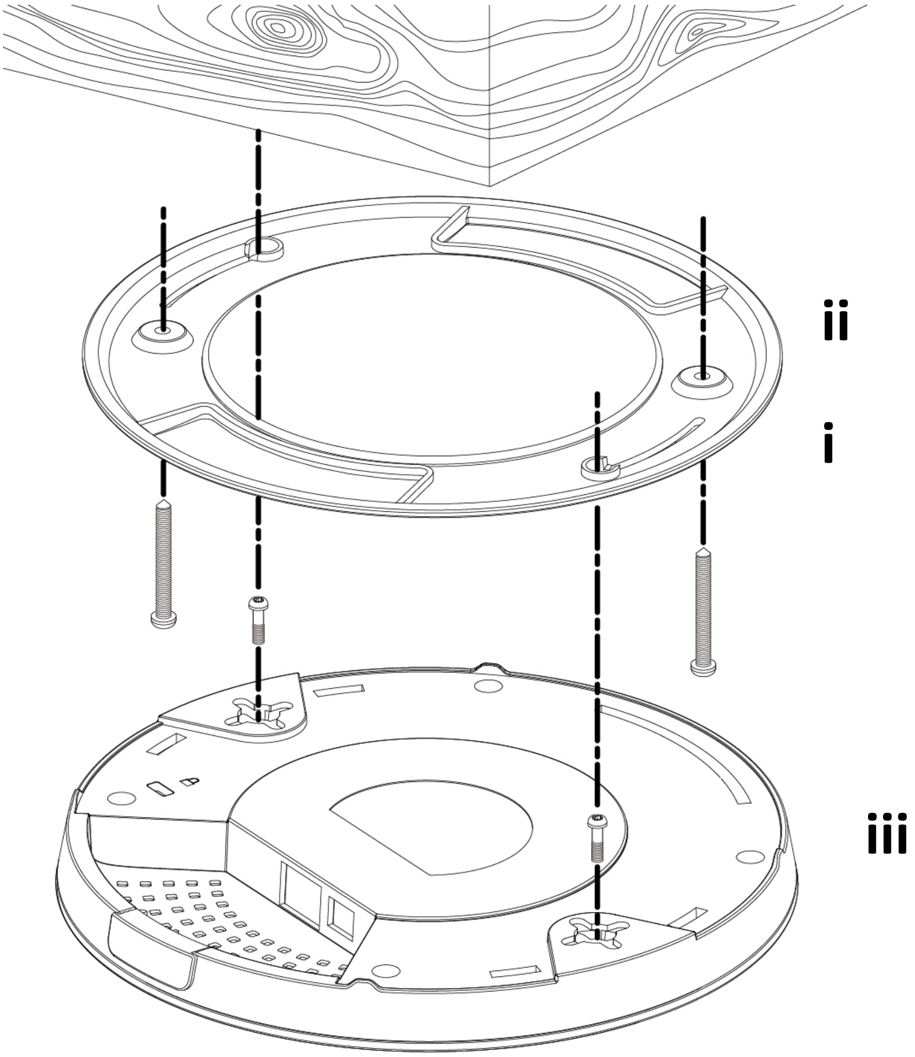
2. Insert screw **iii** through hole **i** and into the rear of screw ii and tighten to provide additional strength.

3. When the ceiling bracket is in place, insert screw **iv** into hole **v** (x 2) on the access point.

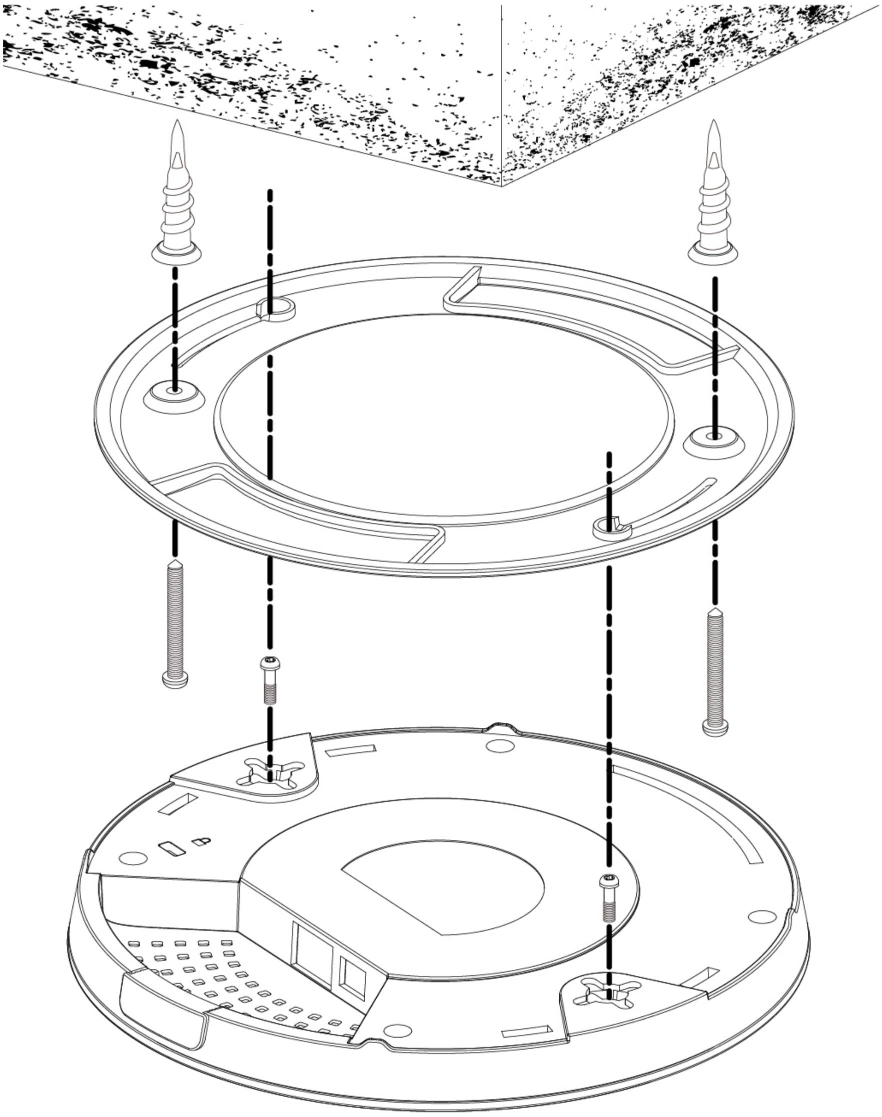
5. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

6. Lock the access point firmly into place by twisting it to align screws **iv** with the grooves in the ceiling mount.

A



B



III-3. T-Rail Mount

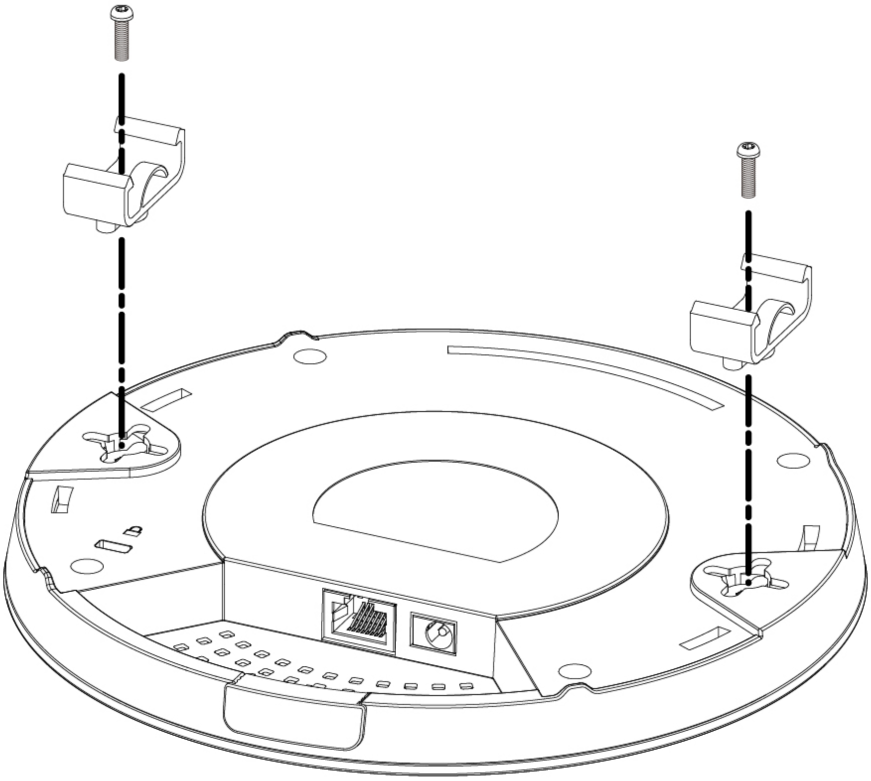
To mount the access point to a T-Rail, please follow the instructions below and refer to diagram **C, D** & **E**.

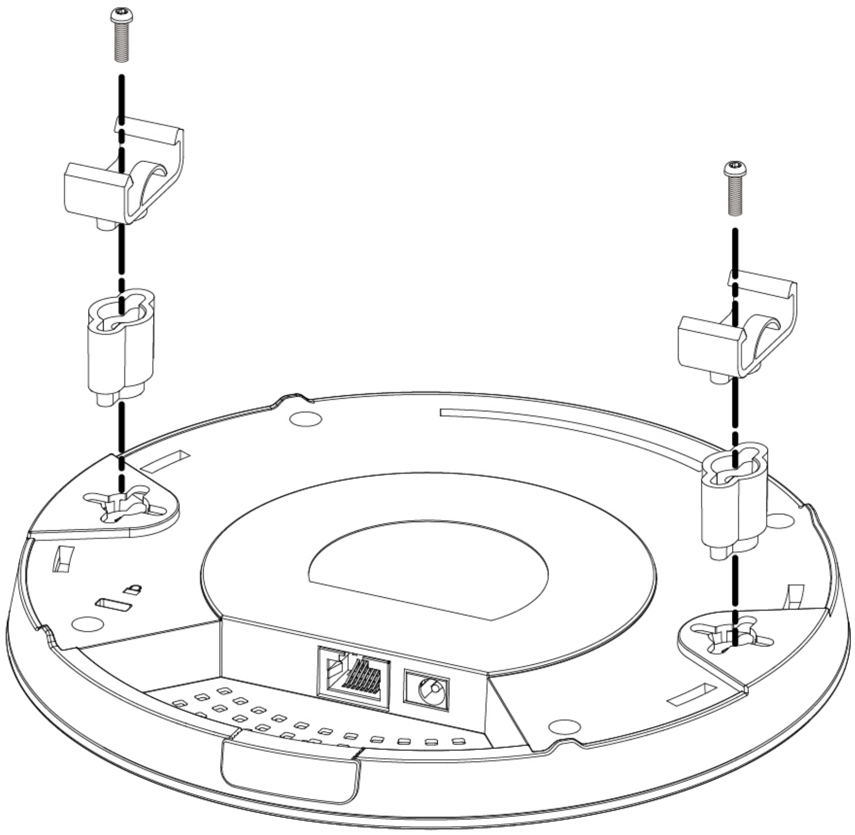
1. Select the correct size T-Rail bracket from the two sizes which are included in the package contents.

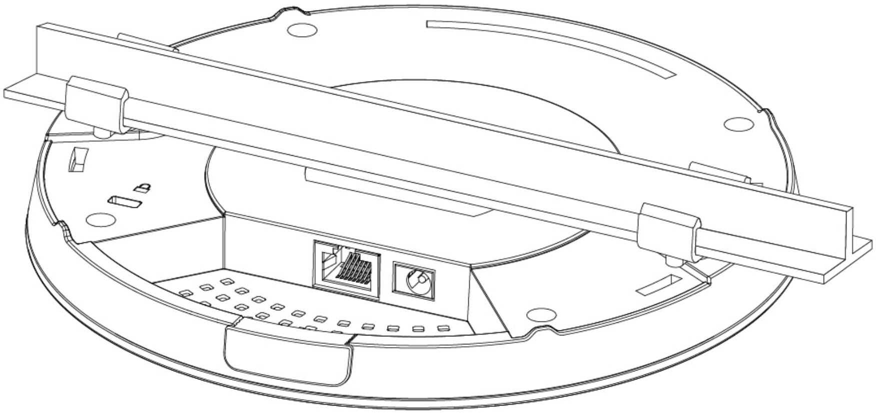
2. Attach the T-Rail bracket **i** to hole **ii** using screw **iii** (x 2) as shown in **C**.

⚠ ***If you need more space between the access point and the T-Rail, then additionally use bracket*** *iv* ***between bracket*** *i* ***and hole*** *ii (x 2),* ***and use the longer screws (x 2) included in the package contents.***

3. Clip the access point onto your T-Rail using the now attached T-Rail bracket.







IV. Browser Based Configuration Interface

You can use the browser-based configuration interface to configure advanced settings.

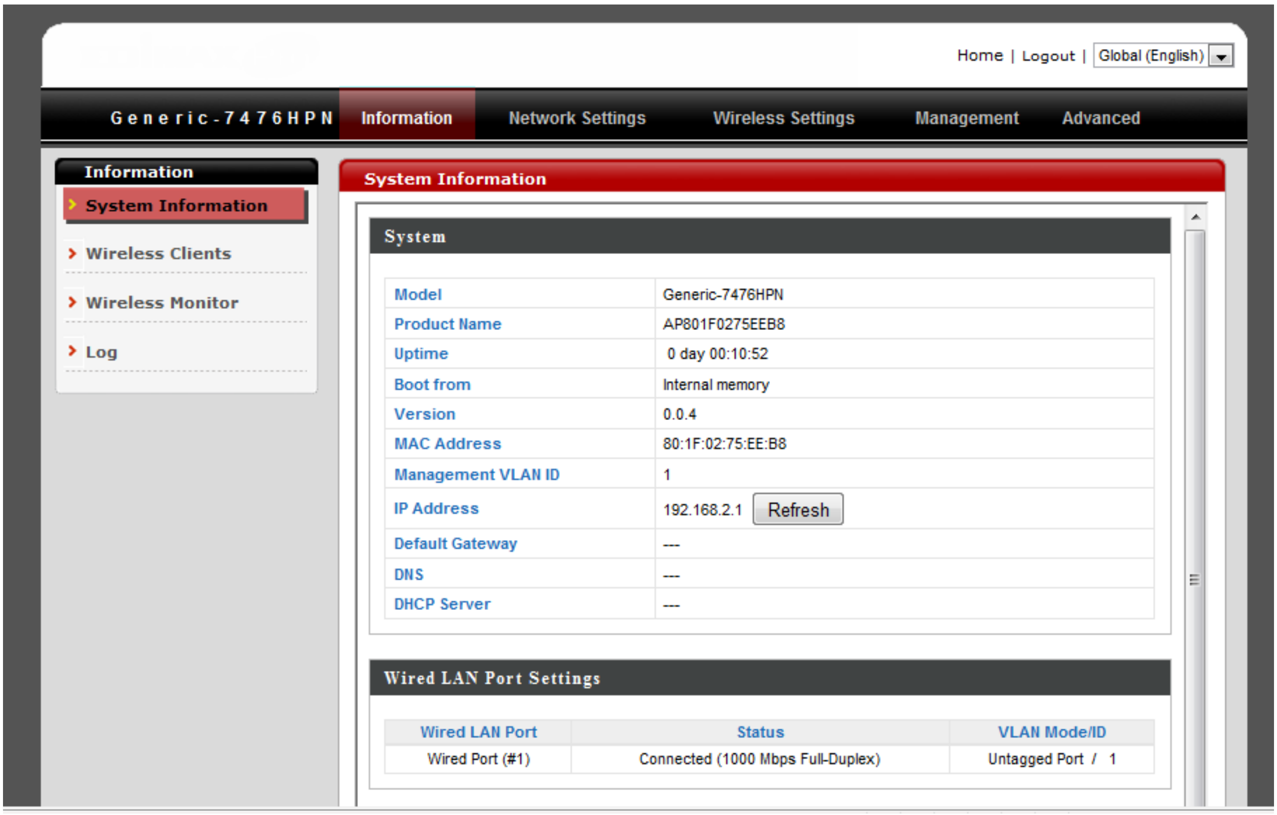
1. Connect a computer to your access point using an Ethernet cable.

2. Enter your access point's IP address in the URL bar of a web browser. The access point's default IP address is **192.169.2.2.**

3. You will be prompted for a username and password. The default username is "admin" and the default password is "admin", though it was recommended that you change the password during setup (see **II-2. Basic Settings**).

If you cannot remember your password, reset the access point back to its factory default settings. Refer to *I-5. Reset*

4. You will arrive at the "System Setup" screen shown below.



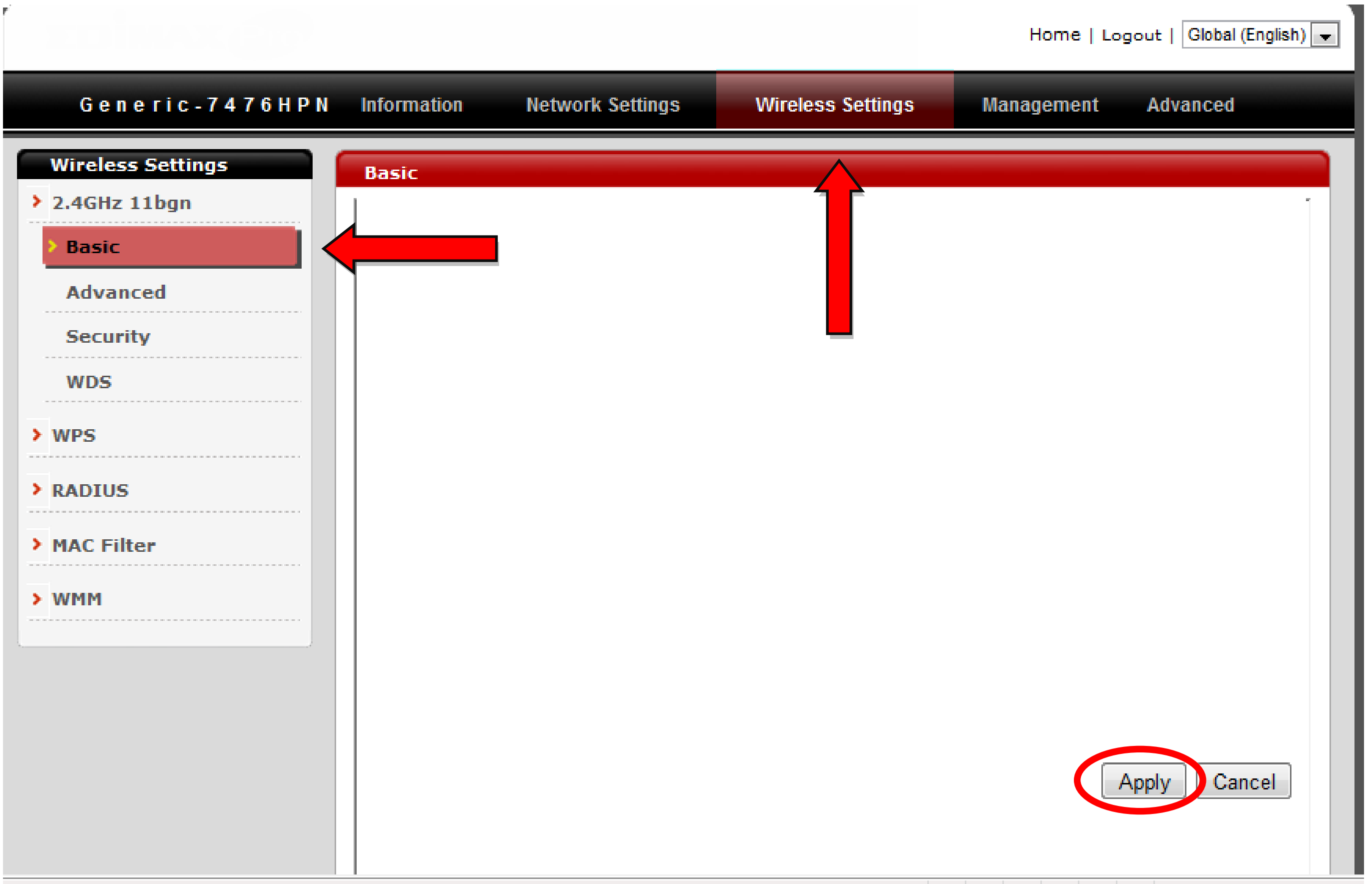
System

Model	Generic-7476HPN
Product Name	AP801F0275EEB8
Uptime	0 day 00:10:52
Boot from	Internal memory
Version	0.0.4
MAC Address	80:1F:02:75:EE:B8
Management VLAN ID	1
IP Address	192.168.2.1 Refresh
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

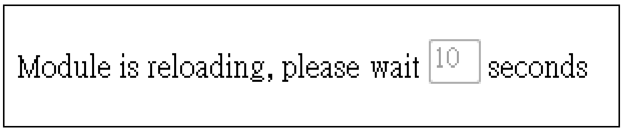
Wired LAN Port	Status	VLAN Mode/ID
Wired Port (#1)	Connected (1000 Mbps Full-Duplex)	Untagged Port / 1

5. Use the menu across the top and down the left side to navigate.



6. Click "Apply" to save changes and reload the access point, or "Cancel" to cancel changes.

Please wait a few seconds for the access point to reload after you "Apply" changes, as shown below.



Module is reloading, please wait 10 seconds

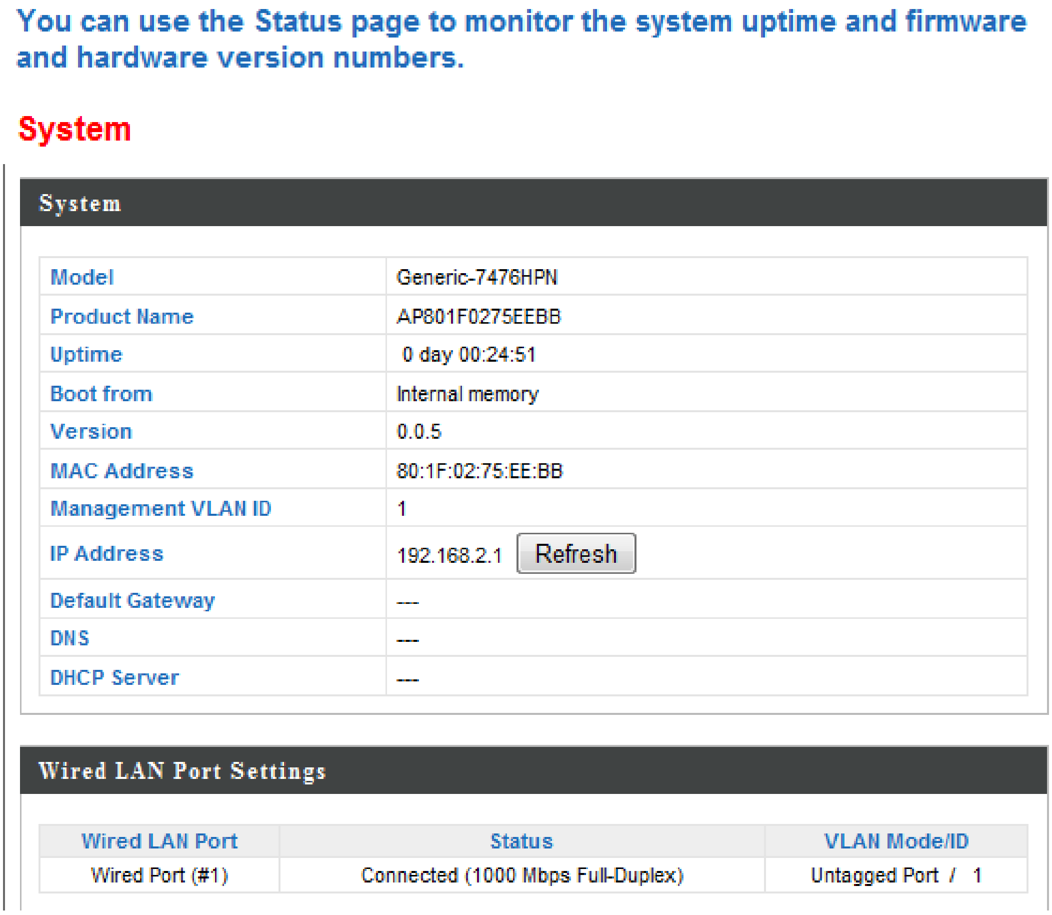
7. Please refer to the following chapters for full descriptions of the browser based configuration interface features.

IV-1. System Setup

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

IV-1-1. Status

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



You can use the Status page to monitor the system uptime and firmware and hardware version numbers.

System

System

Model	Generic-7476HPN
Product Name	AP801F0275EEBB
Uptime	0 day 00:24:51
Boot from	Internal memory
Version	0.0.5
MAC Address	80:1F:02:75:EE:BB
Management VLAN ID	1
IP Address	192.168.2.1 Refresh
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

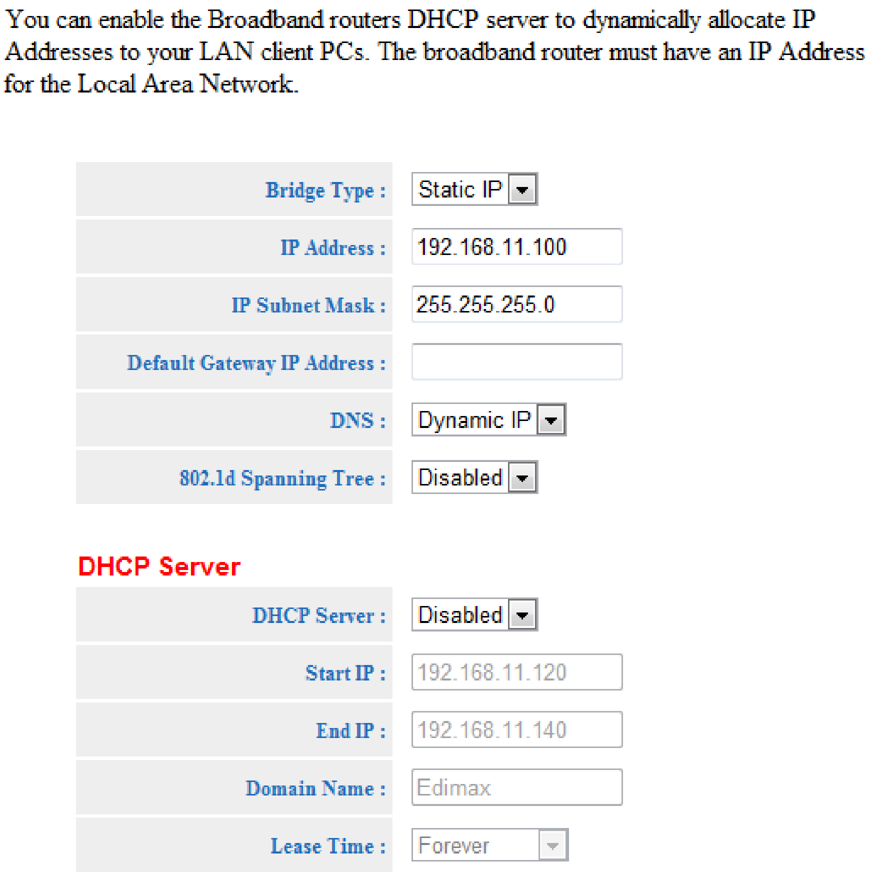
Wired LAN Port	Status	VLAN Mode/ID
Wired Port (#1)	Connected (1000 Mbps Full-Duplex)	Untagged Port / 1

Model	Displays the model number of the access point.
Uptime	Displays the total time since the device was turned on.
Firmware Version	Displays the firmware version.
Hardware Version	Displays the hardware version.
Serial Number	Displays the operating mode.
Boot Code Version	Displays the access point's ESSID, also known as SSID. The ESSID/SSID is the name used to identify a wireless network.
Runtime Code Version	Displays the current wireless channel number.
LAN IP Address	Displays the IP address of this device.
LAN Subnet Mask	Displays the subnet mask of the IP address.
LAN Default Gateway	Displays the IP address of the default gateway.
LAN MAC address	Displays the device's MAC address. The MAC address is a unique, fixed ID for this device, it cannot be modified.
DNS #1	IP address of DNS (Domain Name Server) #1.
DNS #2	IP address of DNS (Domain Name Server) #2.

IV-1-2. LAN Settings

LAN Settings

The “LAN Settings” page allows you to configure your Local Area Network (LAN). You can enable the access point to dynamically allocate IP addresses to your LAN clients, and you can modify the IP address of the access point.



You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

Bridge Type :	Static IP
IP Address :	192.168.11.100
IP Subnet Mask :	255.255.255.0
Default Gateway IP Address :	
DNS :	Dynamic IP
802.1d Spanning Tree :	Disabled

DHCP Server

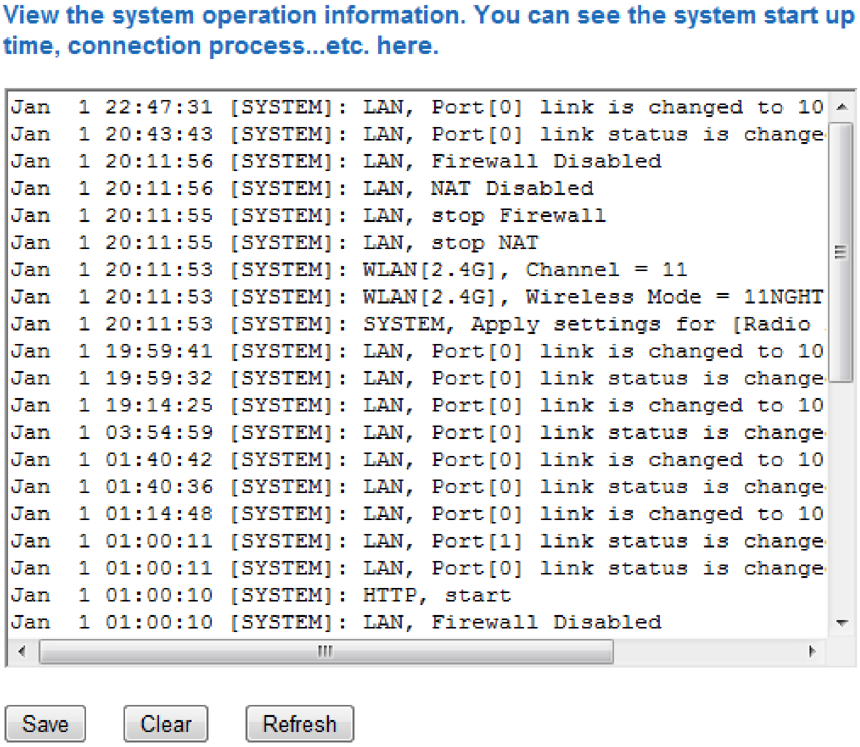
DHCP Server :	Disabled
Start IP :	192.168.11.120
End IP :	192.168.11.140
Domain Name :	Edimax
Lease Time :	Forever

Bridge Type	
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
IP Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway IP Address	Enter the default gateway assigned by your ISP here. Some ISPs may call this “Default Route”.
DNS	
802.1d Spanning Tree	Select “Enable” or “Disable” to enable/disable 802.1d Spanning Tree. This creates a tree of connected layer-2 bridges (typically Ethernet

	switches) within a mesh network, and disables those links that are not part of the tree, leaving a single active path between any two network nodes.
DHCP Server	Enable or disable the DHCP server.
Start IP	Enter the start IP address for the DHCP server’s IP address leases.
End IP	Enter the end IP address for the DHCP server’s IP address leases.
Domain Name	Enter a domain name for your network.
Lease Time	Select a lease time for the DHCP leases here. The DHCP client will obtain a new IP address after the period expires. If there are less than 30 computers connected to the router, you can select “Forever”.

IV-1-3. System Log

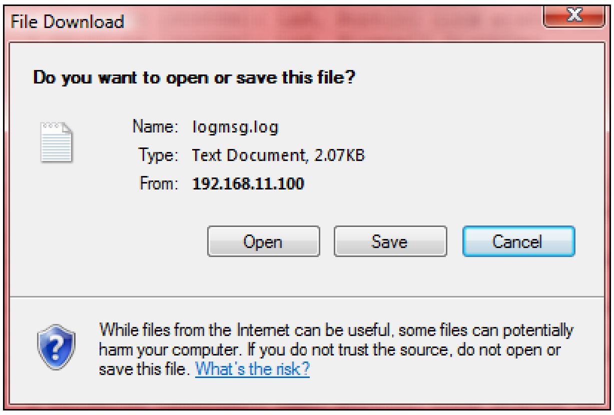
The system log displays system operation information such as up time and connection processes.



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

```
Jan  1 22:47:31 [SYSTEM]: LAN, Port[0] link is changed to 10
Jan  1 20:43:43 [SYSTEM]: LAN, Port[0] link status is change
Jan  1 20:11:56 [SYSTEM]: LAN, Firewall Disabled
Jan  1 20:11:56 [SYSTEM]: LAN, NAT Disabled
Jan  1 20:11:55 [SYSTEM]: LAN, stop Firewall
Jan  1 20:11:55 [SYSTEM]: LAN, stop NAT
Jan  1 20:11:53 [SYSTEM]: WLAN[2.4G], Channel = 11
Jan  1 20:11:53 [SYSTEM]: WLAN[2.4G], Wireless Mode = 11NGHT
Jan  1 20:11:53 [SYSTEM]: SYSTEM, Apply settings for [Radio
Jan  1 19:59:41 [SYSTEM]: LAN, Port[0] link is changed to 10
Jan  1 19:59:32 [SYSTEM]: LAN, Port[0] link status is change
Jan  1 19:14:25 [SYSTEM]: LAN, Port[0] link is changed to 10
Jan  1 03:54:59 [SYSTEM]: LAN, Port[0] link status is change
Jan  1 01:40:42 [SYSTEM]: LAN, Port[0] link is changed to 10
Jan  1 01:40:36 [SYSTEM]: LAN, Port[0] link status is change
Jan  1 01:14:48 [SYSTEM]: LAN, Port[0] link is changed to 10
Jan  1 01:00:11 [SYSTEM]: LAN, Port[1] link status is change
Jan  1 01:00:11 [SYSTEM]: LAN, Port[0] link status is change
Jan  1 01:00:10 [SYSTEM]: HTTP, start
Jan  1 01:00:10 [SYSTEM]: LAN, Firewall Disabled
```

Save	Click “Save” and you will be prompted (example shown below) to save the log on your computer as .txt file.
Clear	Click “Clear” to clear/erase the existing log.
Refresh	Click “Refresh” to refresh the log and update any activity.



File Download

Do you want to open or save this file?

Name: logmsg.log
Type: Text Document, 2.07KB
From: 192.168.11.100

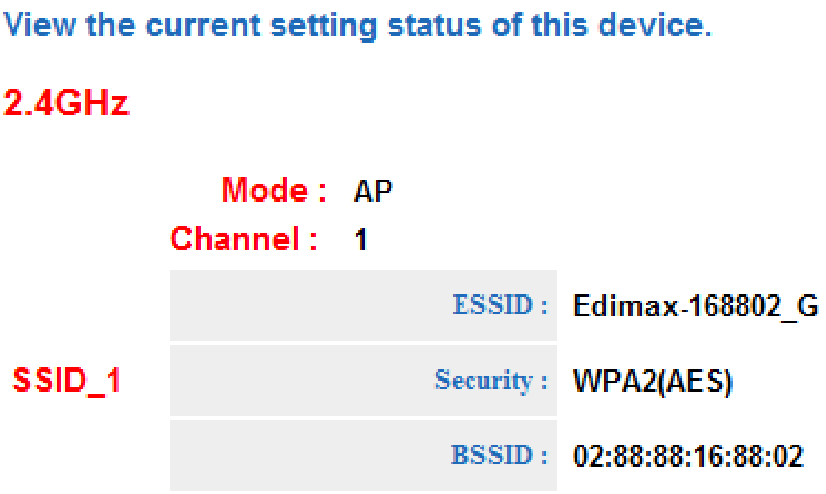
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

IV-2. Wireless Setting

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

IV-2-1. Status

The "Status" page displays a summary of key information about your access point's 2.4GHz wireless networks.



View the current setting status of this device.

2.4GHz

Mode : AP

Channel : 1

SSID_1

ESSID : Edimax-168802_G

Security : WPA2(AES)

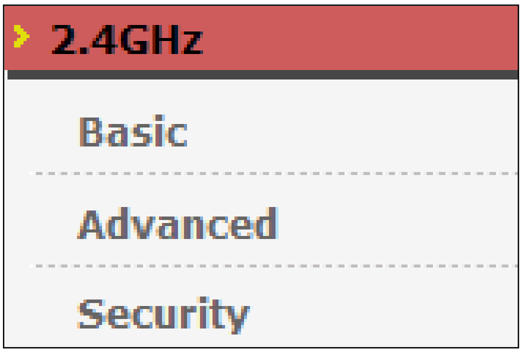
BSSID : 02:88:88:16:88:02

Mode	
Channel	Displays the wireless channel number used for the specified frequency (2.4GHz).
SSID1	Displays which SSID number the following "ESSID", "Security" and "BSSID" fields refer to.

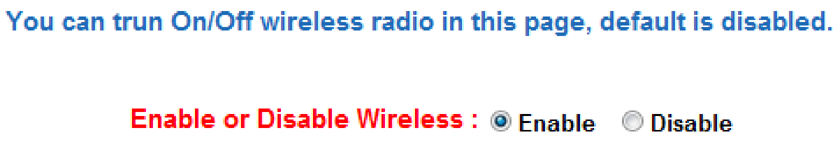
ESSID	Displays the ESSID (also referred to as SSID) for the access point's specified wireless network. The ESSID/SSID is the name used to identify a wireless network
Security	Displays the wireless security/encryption type for the specified wireless network.
BSSID	Displays the device's BSSID. The BSSID

	identifies this access point in the network, and is the same as the device’s MAC address.

IV-2-2. 2.4GHz



The "2.4GHz" menu allows you to access basic, advanced and security settings for your access point's 2.4GHz wireless networks. You can also enable or disable the access point's 2.4GHz wireless networks.



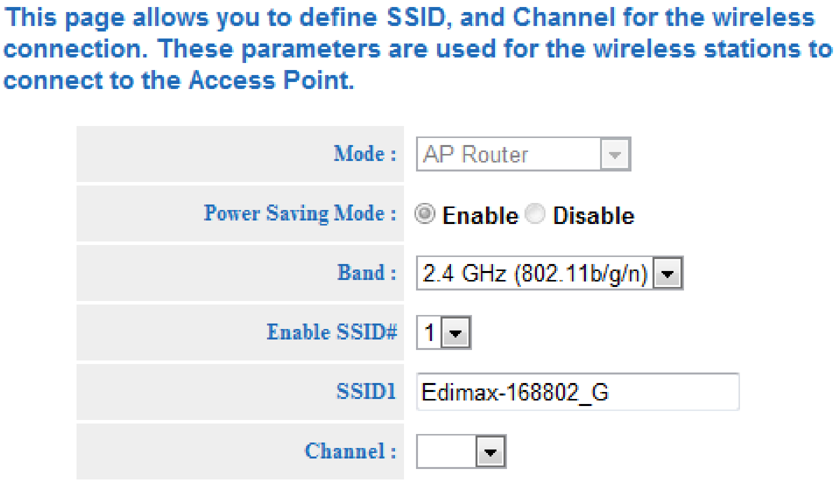
You can trun On/Off wireless radio in this page, default is disabled.

Enable or Disable Wireless : ● Enable ○ Disable

Enable/Disable	Enable or disable the access point's 2.4GHz wireless network.

IV-2-2-1. Basic

The "Basic" screen displays settings for your access point's 2.4GHz Wi-Fi network (s).



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

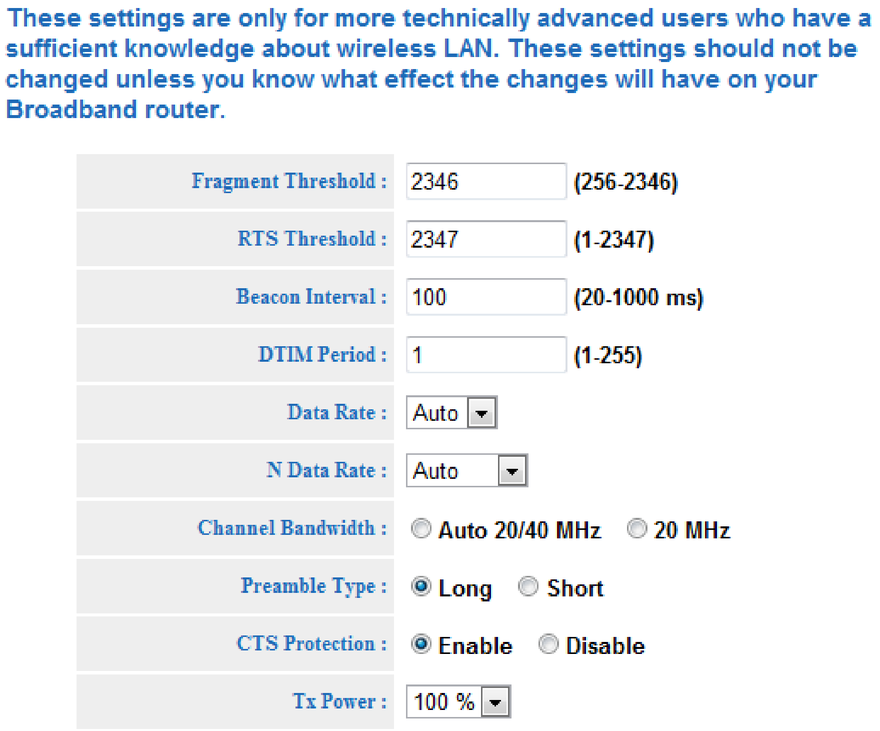
Mode :	AP Router
Power Saving Mode :	● Enable ○ Disable
Band :	2.4 GHz (802.11b/g/n)
Enable SSID#	1
SSID1	Edimax-168802_G
Channel :	

Mode	
Power Saving Mode	Enable or disable power saving mode on the access point.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID#	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of four can be enabled.
SSID1,2,3,4	Enter the SSID name for the specified SSID (1, 2, 3 or 4 depending on how many you have enabled). The SSID can consist of any combination of up to 32 alphanumeric characters.
Channel	Select a wireless radio channel or use the default “Auto” setting from the drop-down menu.

IV-2-2-2. Advanced

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

Changing these settings can adversely affect the performance of your access point.



These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2347 (1-2347)
Beacon Interval :	100 (20-1000 ms)
DTIM Period :	1 (1-255)
Data Rate :	Auto
N Data Rate :	Auto
Channel Bandwidth :	○ Auto 20/40 MHz ○ 20 MHz
Preamble Type :	● Long ○ Short
CTS Protection :	● Enable ○ Disable
Tx Power :	100 %

Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
Data Rate	Set the wireless data rate. The default is set to auto.
N Data Rate	Set the 802.11n wireless data rate. The default is set to auto.

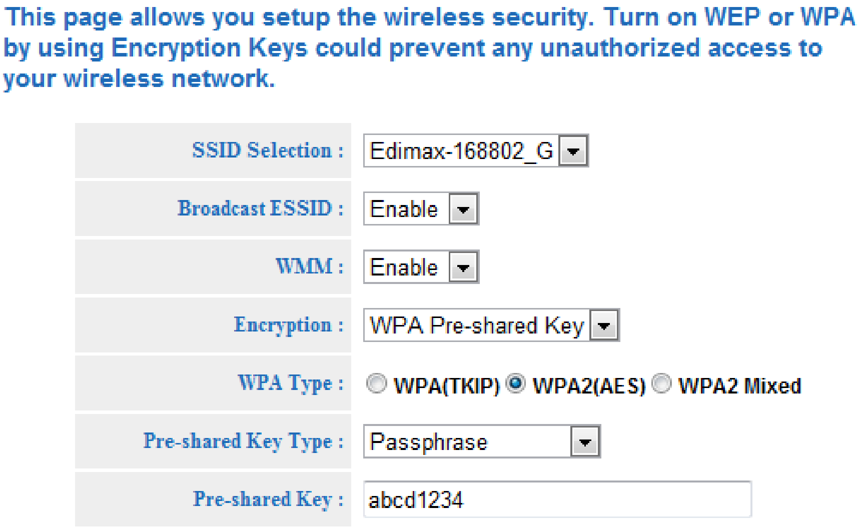
Channel Bandwidth	Select wireless channel width (analogue signal bandwidth used by wireless signals from the device) from “Auto 20/40Mhz” or “20Mhz” – the recommended value is Auto 20/40MHz.
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble”.
CTS Protection	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to “Auto”.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.

IV-2-2-3. Security

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

It's essential to configure wireless security in order to prevent unauthorised access to your network. "WPA Pre-shared Key" is the recommended security type.

Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.



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.

SSID Selection :	Edimax-168802_G
Broadcast ESSID :	Enable
WMM :	Enable
Encryption :	WPA Pre-shared Key
WPA Type :	○ WPA(TKIP) ● WPA2(AES) ○ WPA2 Mixed
Pre-shared Key Type :	Passphrase
Pre-shared Key :	abcd1234

SSID Selection	Select which SSID to configure security settings for.
Broadcast ESSID	Enable or disable ESSID broadcast. When enabled, the ESSID will be visible to clients as an available Wi-Fi network. When disabled, the ESSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the ESSID in order to connect. A hidden (disabled) ESSID is typically more secure than a visible (enabled) SSID.
WMM	Enable or disable WMM. WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP) and others. When WMM is enabled, the device will prioritize different kinds of data and give higher priority to applications which require instant responses for better performance.
Encryption	Select an encryption type from the drop-down menu and refer to the following chapters for more information. The recommended encryption type is “WPA Pre-shared Key”.

IV-2-2-3-1. Disable

Encryption is disabled and no password/key is required to connect to the BR-6428nS V2/nC.

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

IV-2-2-3-2. WEP

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

Authentication Type	Select "Open System", "Shared Key" or "Auto" authentication type.
Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from "ASCII" (any alphanumerical character 0-9, a-z and A-Z) or "Hex" (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

IV-2-2-3-3. WPA Pre-shared Key

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

WPA Type	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. WPA2 (AES) is safer than WPA (TKIP), but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2 (AES) is recommended followed by WPA2 Mixed if your client does not support WPA2 (AES).
Pre-shared Key Format	Choose from “Passphrase” (8 – 63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).
Pre-shared Key	Please enter a security key/password according to the format you selected above.

IV-2-2-3-4. WPA RADIUS

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

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

IV-2-2-3-5. 802.1x (WEP)

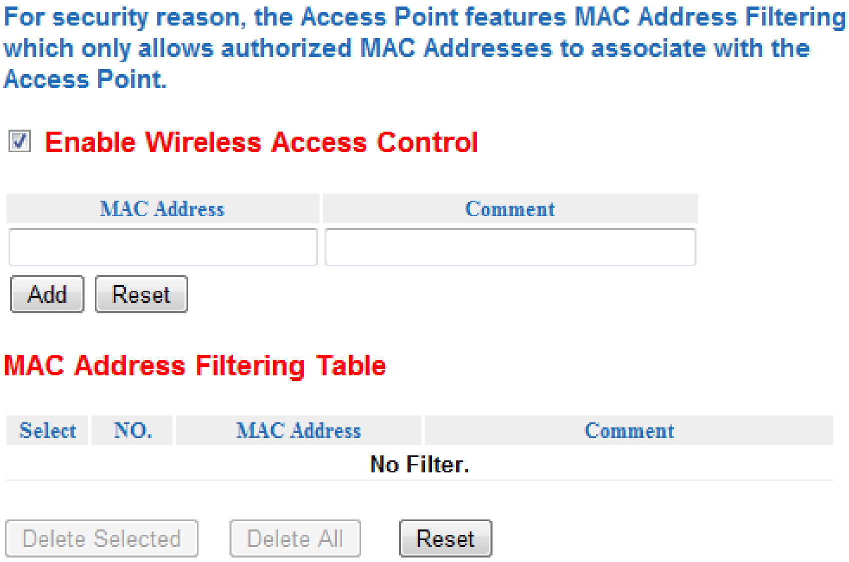
Enable 802.1x Authentication	Enable or disable the use of 802.1x user authentication.
RADIUS Server IP Address	Enter the IP address of the RADIUS authentication server here.
RADIUS Server Port	Enter the port number of the RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Enter the password of the RADIUS authentication server here.

IV-2-3. MAC Filter

Mac filtering is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the BR-6428nS V2/nC. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the BR-6428nS V2/nC, it will be denied.

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



For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point.

☑ Enable Wireless Access Control

MAC Address	Comment

MAC Address Filtering Table

Select	NO.	MAC Address	Comment
		No Filter.	

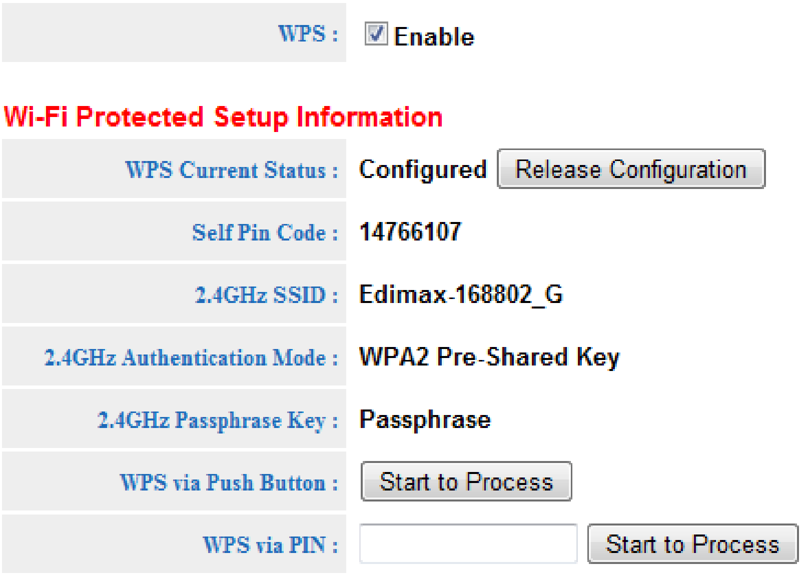
MAC address	Enter a MAC address of computer or network device manually without dashes or colons e.g. for MAC address ‘aa-bb-cc-dd-ee-ff’ enter ‘aabbccddeeff’.
Comment	Enter a comment for reference/identification consisting of up to 16 alphanumerical characters.
Add	Click “Add” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.

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

IV-2-4. WPS

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



WPS :	☑ Enable

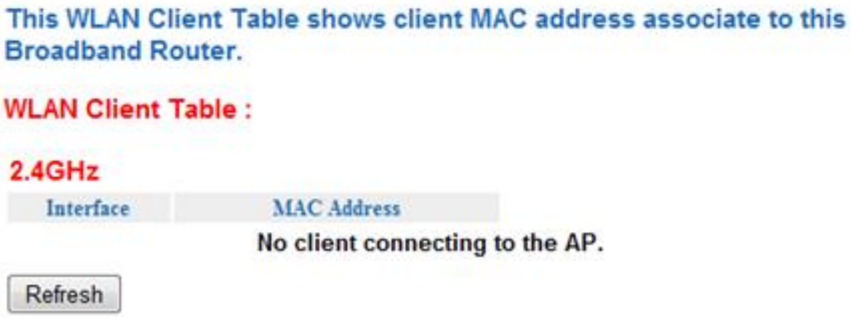
Wi-Fi Protected Setup Information

WPS Current Status :	Configured Release Configuration
Self Pin Code :	14766107
2.4GHz SSID :	Edimax-168802_G
2.4GHz Authentication Mode :	WPA2 Pre-Shared Key
2.4GHz Passphrase Key :	Passphrase
WPS via Push Button :	Start to Process
WPS via PIN :	Start to Process

Enable WPS	Check/uncheck this box to enable/disable WPS.
WPS Current Status	Displays “Configured” or “unConfigured” depending on whether WPS and security/encryption settings for the device have been configured or not, either manually or using the WPS button.
Self PIN Code	Displays the WPS PIN code of the device.
2.4 GHz SSID	Displays the SSID (ESSID) of the device.
2.4GHz Authentication Mode	Displays the wireless security authentication mode of the device.
2.4GHz Passphrase Key	Displays the wireless security authentication key type.
Configure via Push Button	Click “Start to Process” to activate WPS on the access point. WPS will be active for 2 minutes.
WPS via PIN	Enter the wireless client’s PIN code here and click “Start to Process” to activate PIN code WPS. Refer to your wireless client’s documentation if you are unsure of its PIN code.

IV-2-5. Client List

The “Client List” page displays a table of all clients which are connected to the access point.



This WLAN Client Table shows client MAC address associate to this Broadband Router.

WLAN Client Table :

2.4GHz

Interface	MAC Address
No client connecting to the AP.	

Interface	Interface of each client (2.4GHz) is displayed here.
MAC Address	The MAC address each client connected to the access point is displayed here.
Refresh	Click to refresh the list of connected clients.

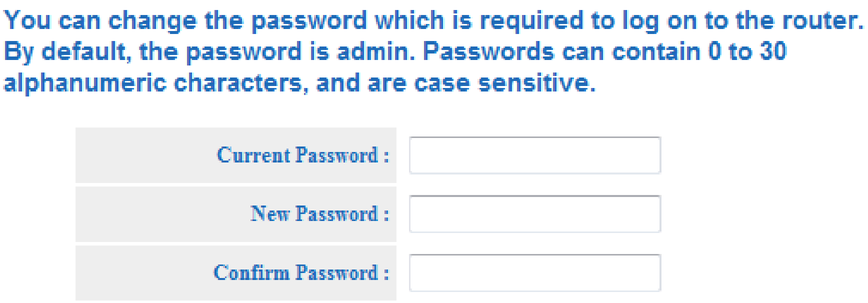
IV-3. Toolbox

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

IV-3-1. Admin

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

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see [II-2. Reset](#) for how to reset the access point.



You can change the password which is required to log on to the router. By default, the password is admin. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.

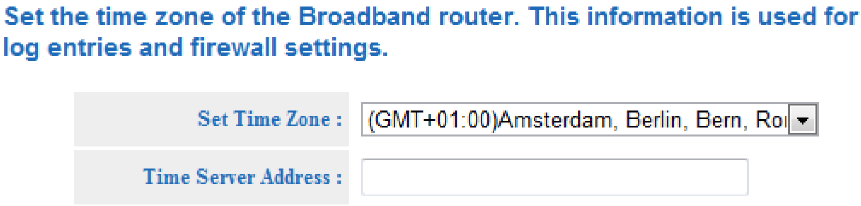
Current Password :	
New Password :	
Confirm Password :	

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.

IV-3-2. Time Setting

Time Setting

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


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

Set Time Zone : (GMT+01:00)Amsterdam, Berlin, Bern, Ro

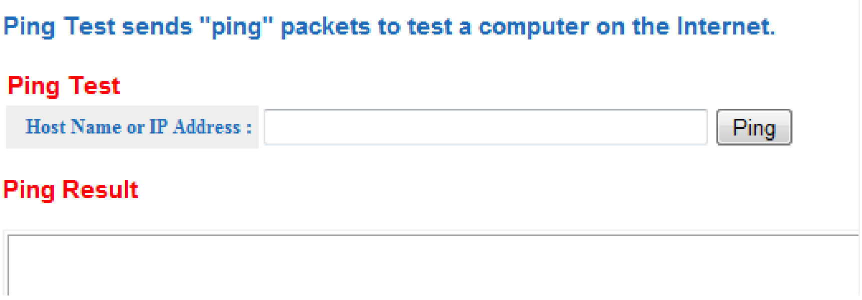
Time Server Address :

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 access point also supports NTP (Network Time Protocol) for automatic time and date setup. Enter the host name or IP address of the time server if you wish.

IV-3-3. Diagnosis

The diagnosis tool can ping a specific IP address and display the result in the box below.

A "ping" is a test packet of information sent to determine the reachability of a host on an IP network, and to measure the round-trip time for messages sent from the originating host to a destination computer.

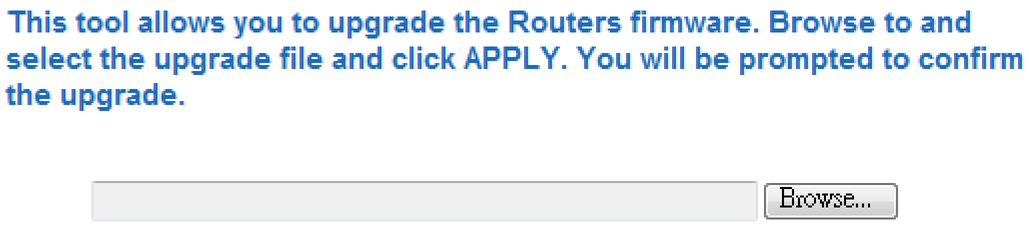

Ping Test sends "ping" packets to test a computer on the Internet.

Ping Address	Specify the host name or IP address to ping.
Ping	Click "Ping" to begin.

IV-3-4. Firmware

Firmware

The “Firmware” page allows you to update the system firmware to a more recent version. Updated firmware versions often offer increased performance and security, as well as bug fixes. You can download the latest firmware from the Edimax website.



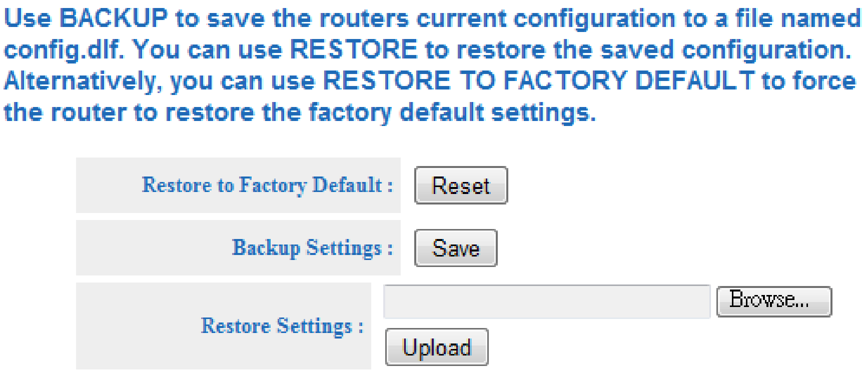
This tool allows you to upgrade the Routers firmware. Browse to and select the upgrade file and click APPLY. You will be prompted to confirm the upgrade.

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

Browse	Open a new window to locate and select the firmware file in your computer.

IV-3-5. System Setting

The access point’s “System Setting” page enables you to restore the device back to factory default settings, back up the current settings, or restore the device to previously saved settings.

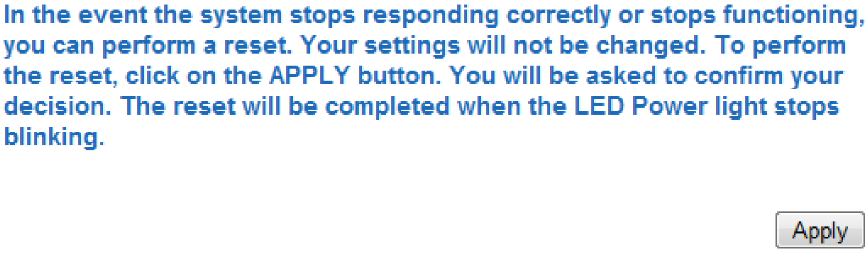


Use BACKUP to save the routers current configuration to a file named config.dlf. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings.

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.
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.

IV-3-6. Reboot

If the access point malfunctions or is not responding, then it is recommended that you reboot the device. You can reboot the access point remotely using this feature if the location of the access point is not convenient.



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

Apply	Click "Apply" to reboot the device. A countdown will indicate the progress of the reboot.

III. Appendix

IV-1. Configuring your IP address

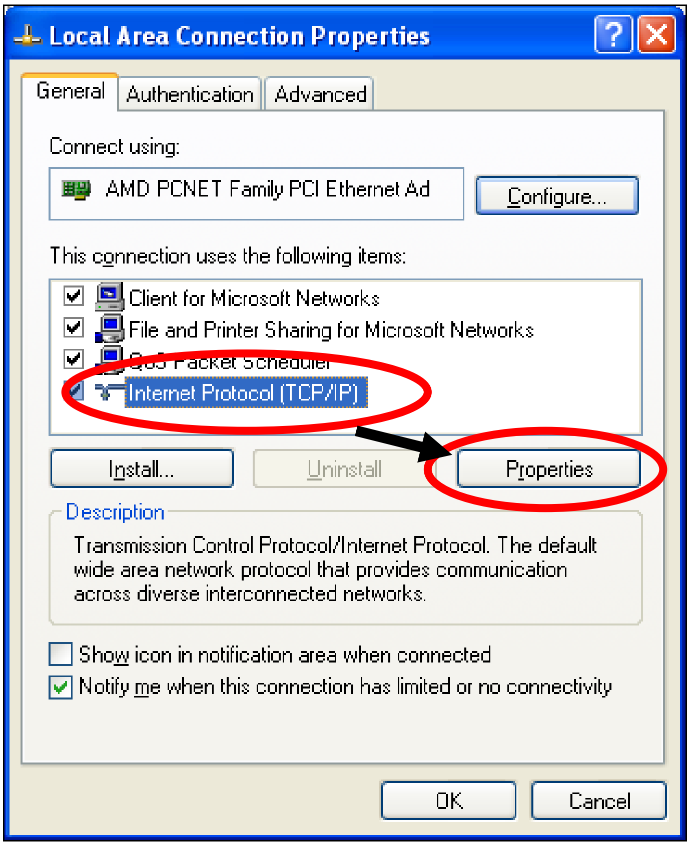
The access point uses the default IP address **192.168.2.2**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254).**

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system.

In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254).**

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

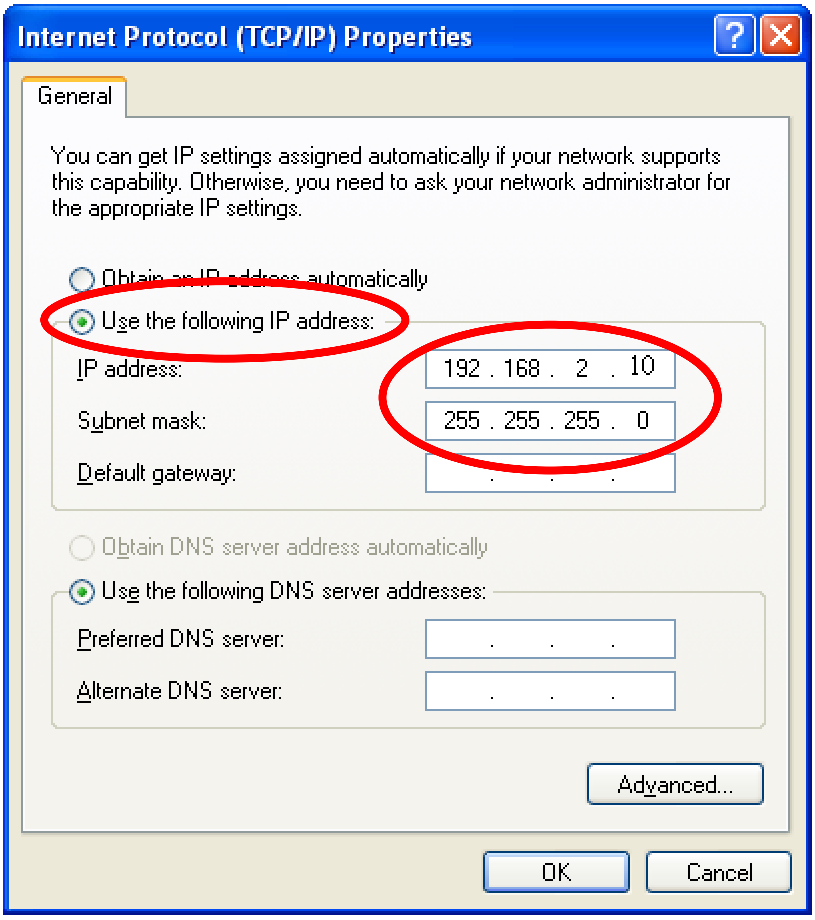
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ 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: 192.168.2.10
Subnet Mask: 255.255.255.0

Click 'OK' when finished.



Internet Protocol (TCP/IP) 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

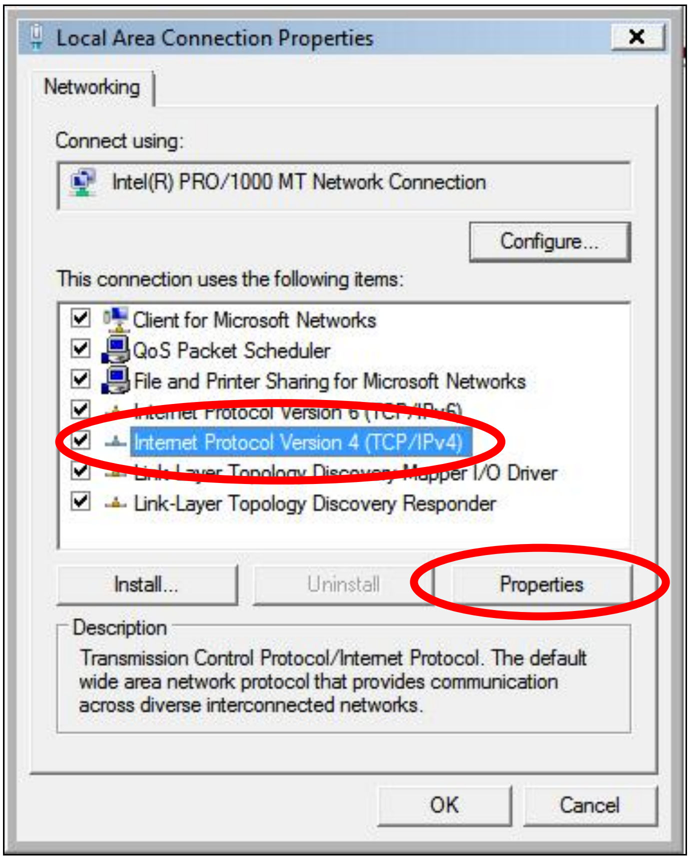
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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”.

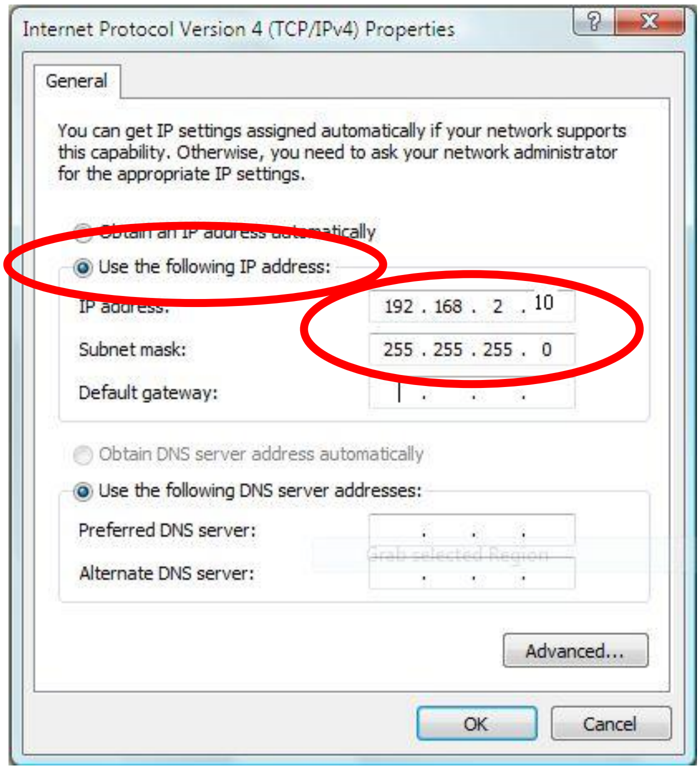


Local Area Connection Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Network Connection
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ 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 “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
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 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

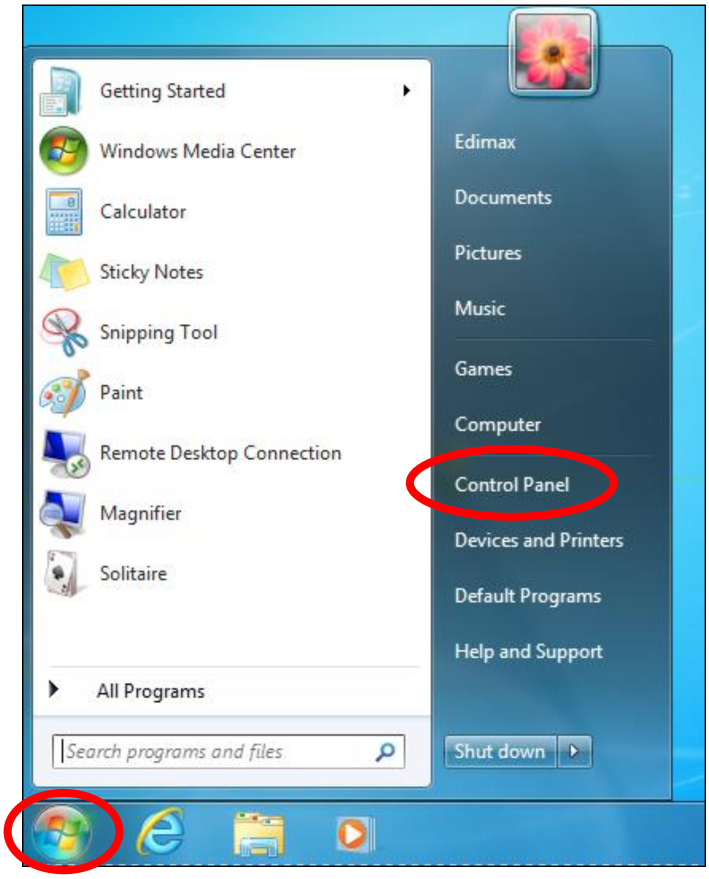
● Use the following DNS server addresses:

Preferred DNS server: . . .

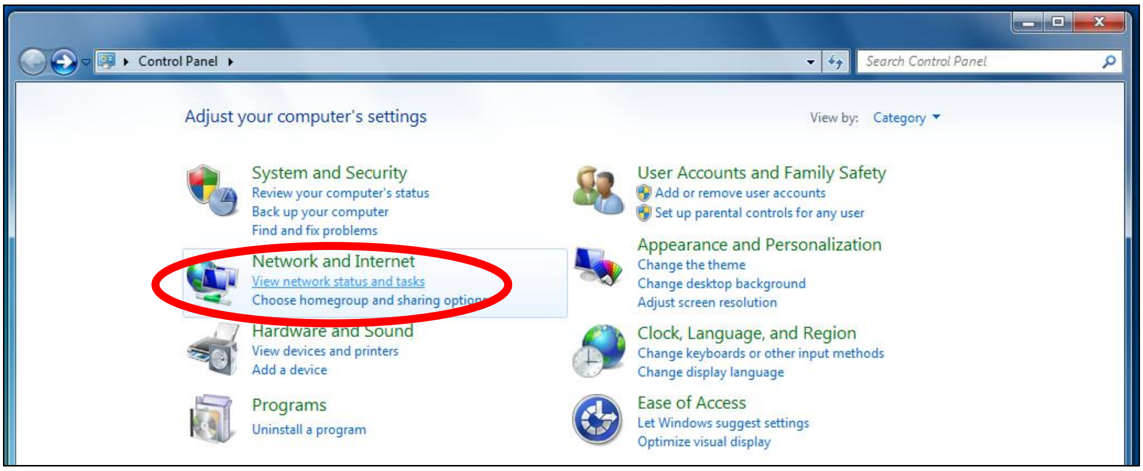
Alternate DNS server: . . .

IV-1-2-3. Windows 7

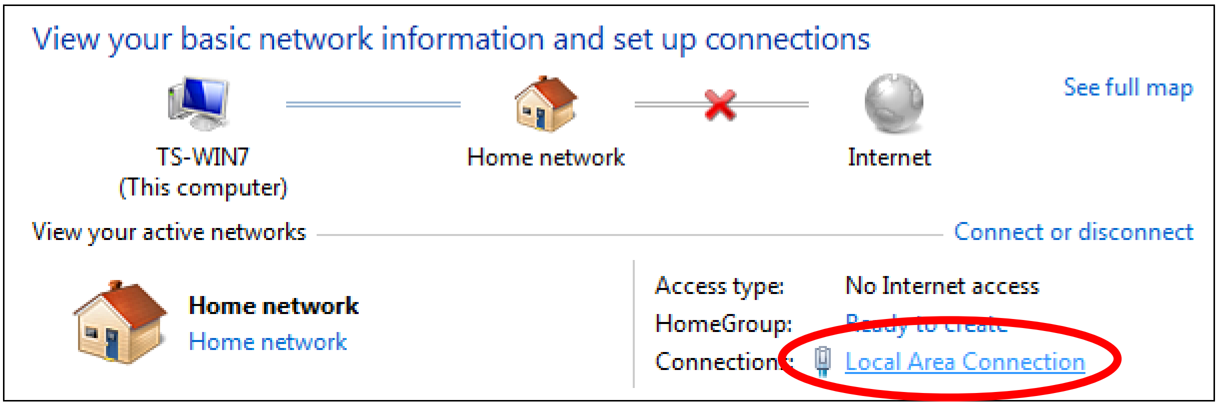
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



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

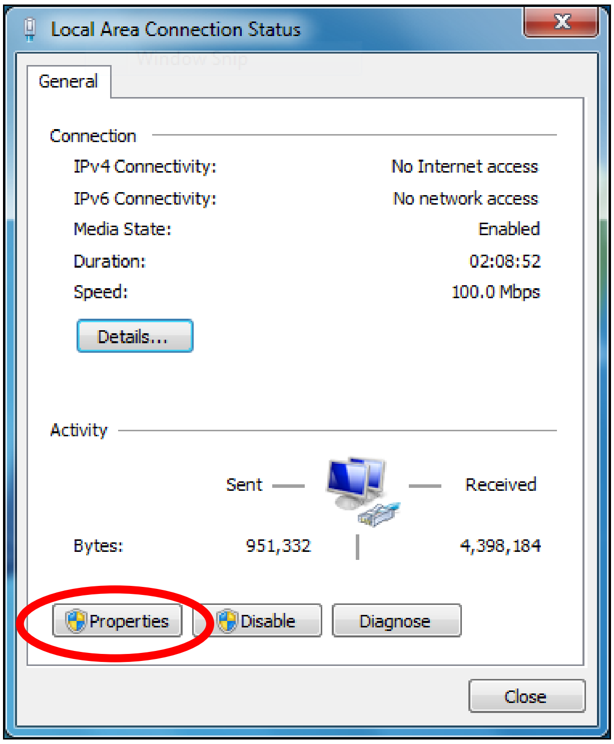
3. Click “Local Area Connection”.



View your basic network information and set up connections

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

4. Click "Properties".



Local Area Connection Status

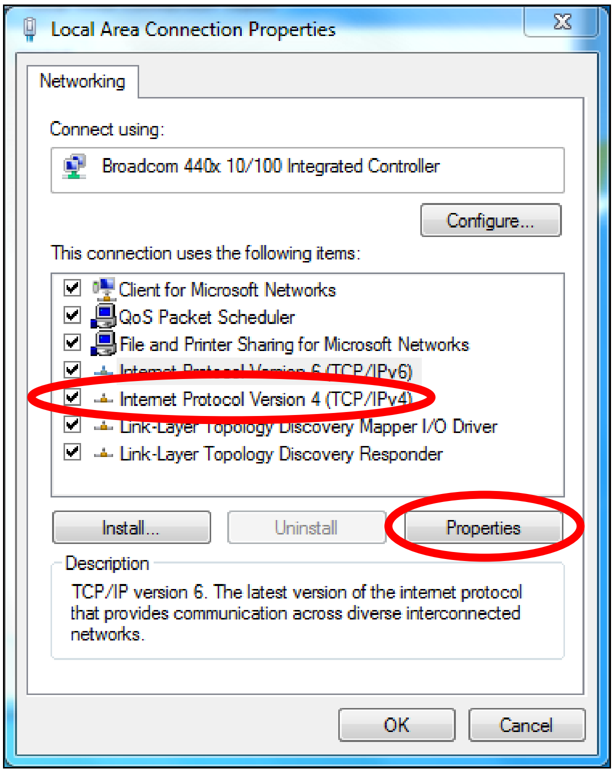
Connection

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

Activity

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

5. Select “Internet Protocol Version 4 (TCP/IPv4) 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

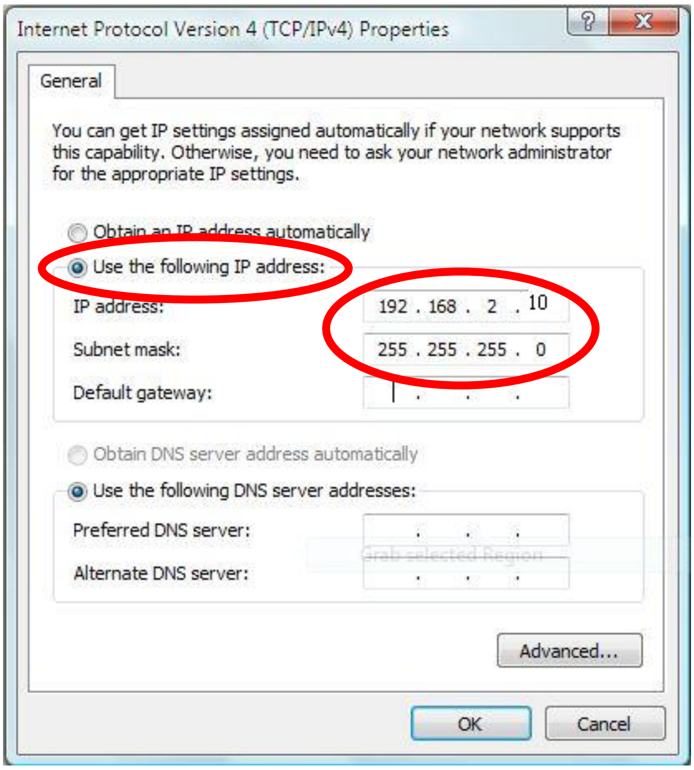
Description

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

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

IP address: 192.168.2.10
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 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

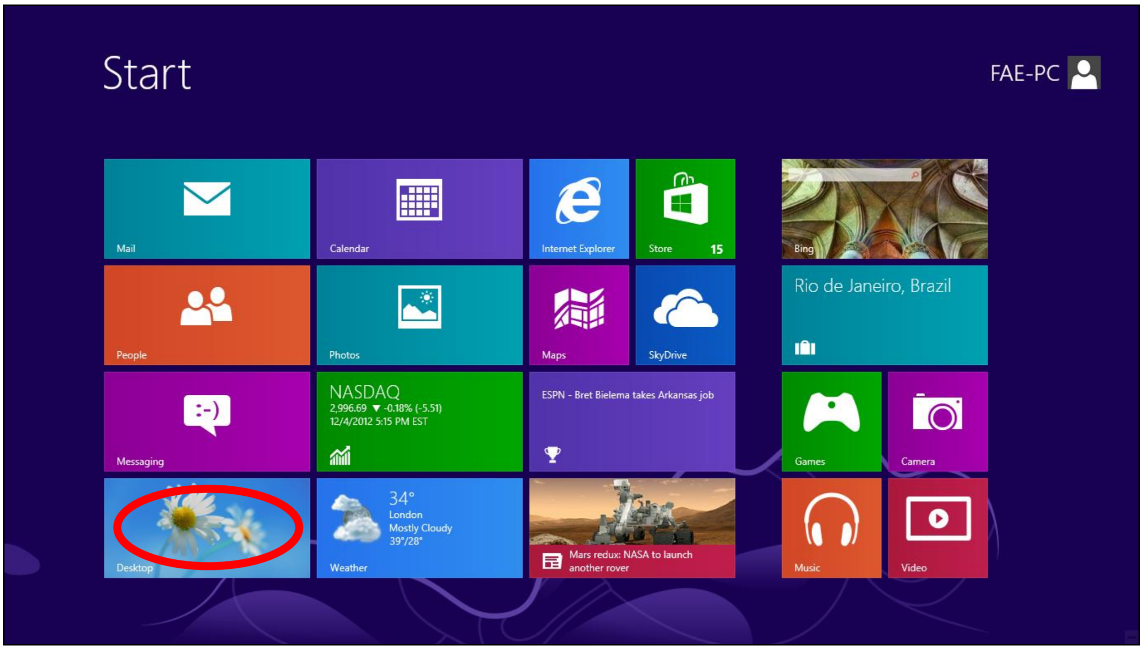
● Use the following DNS server addresses:

Preferred DNS server: . . .

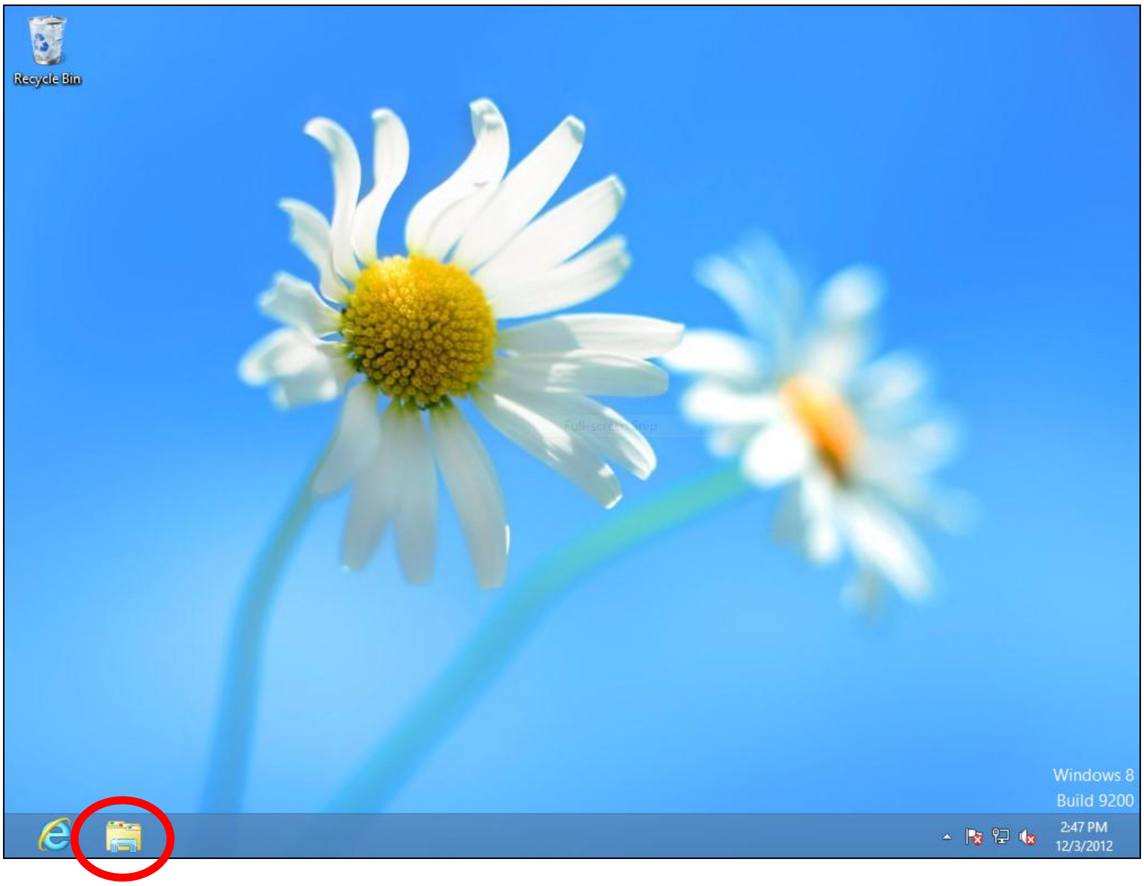
Alternate DNS server: . . .

IV-1-2-4. Windows 8

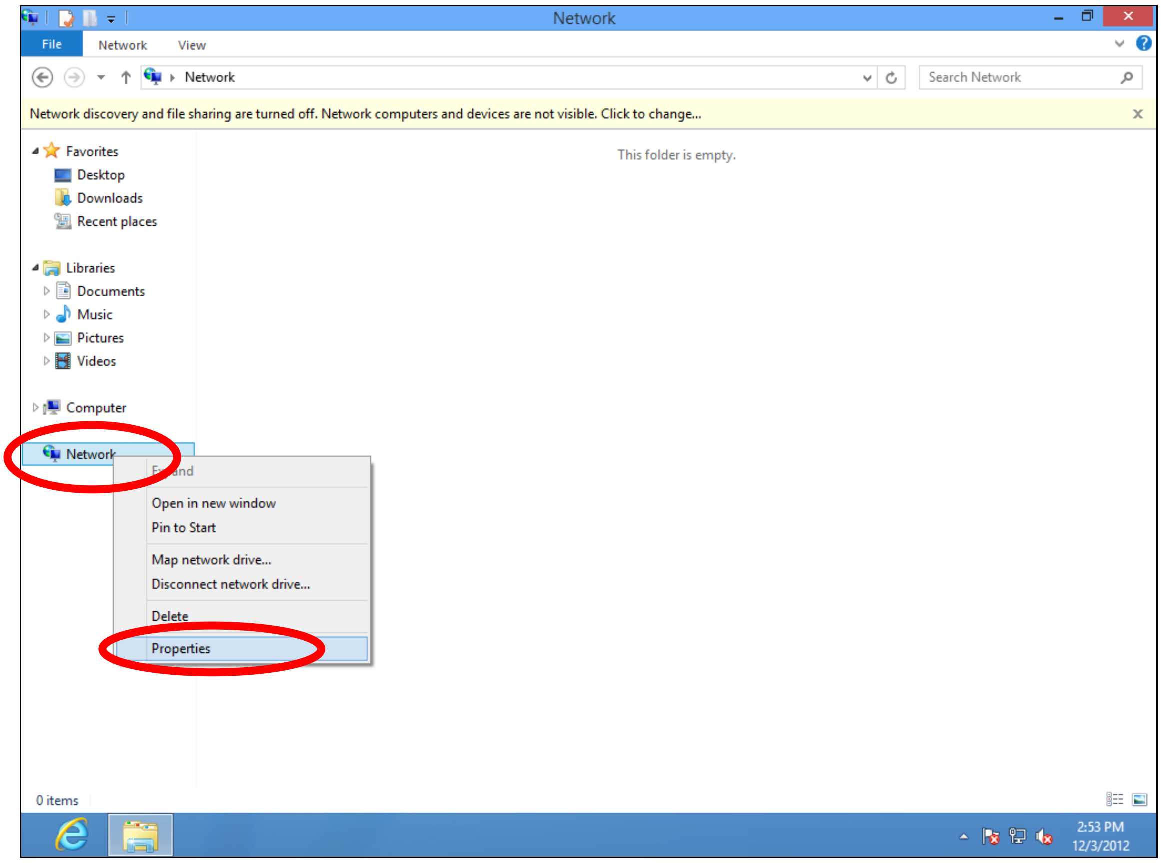
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



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

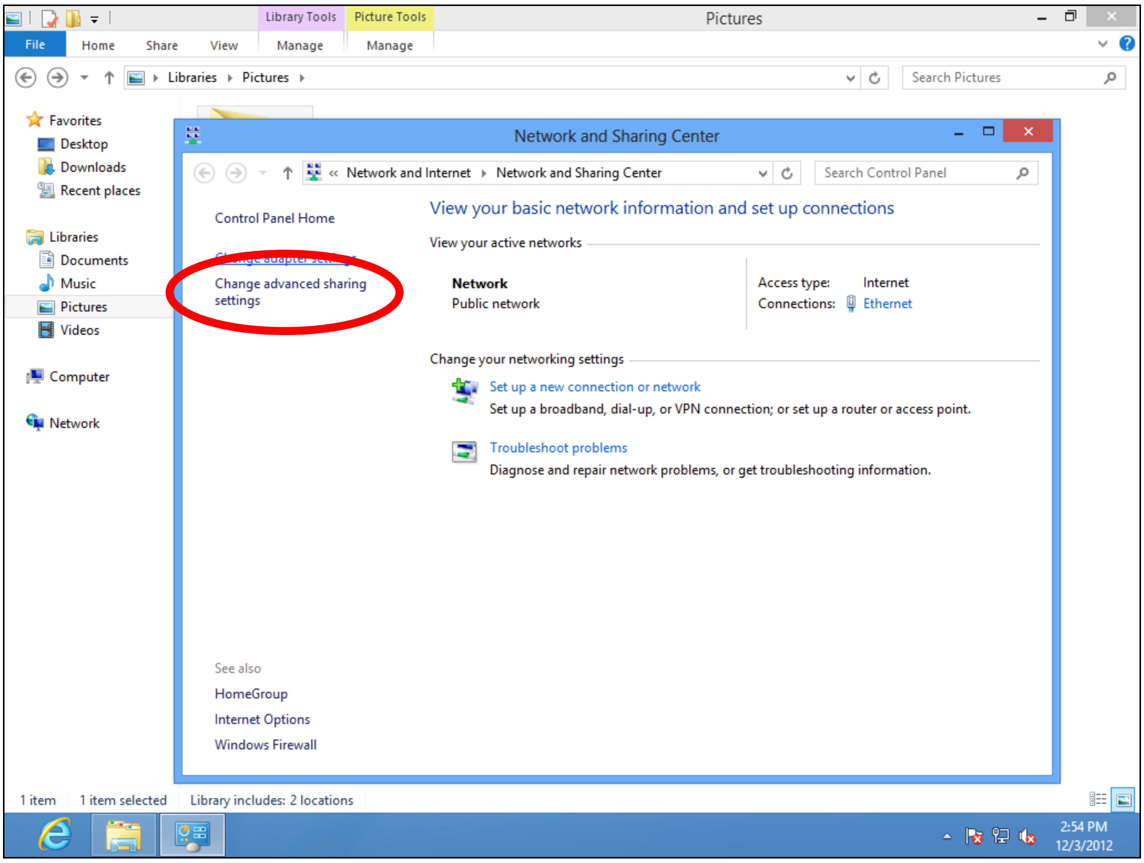


3. Right click “Network” and then select “Properties”.


Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

This folder is empty.

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



View your basic network information and set up connections

View your active networks

Network
Public network

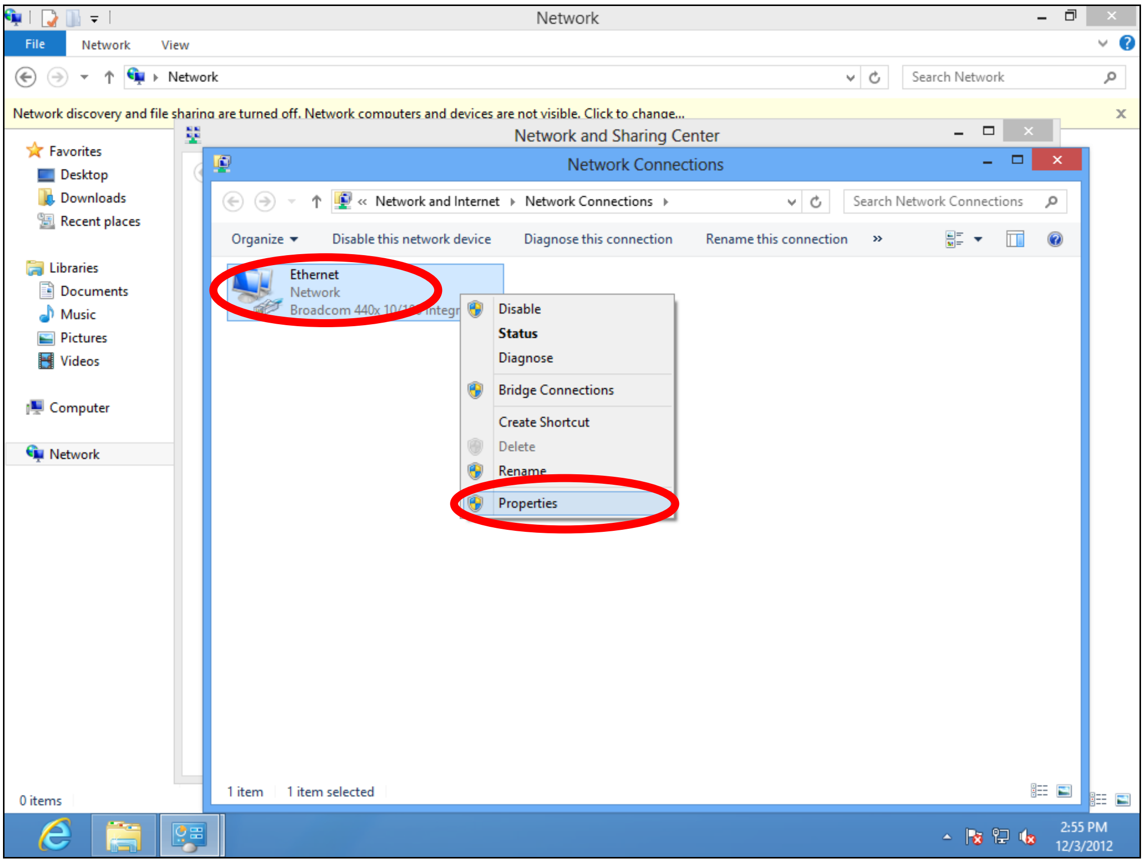
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

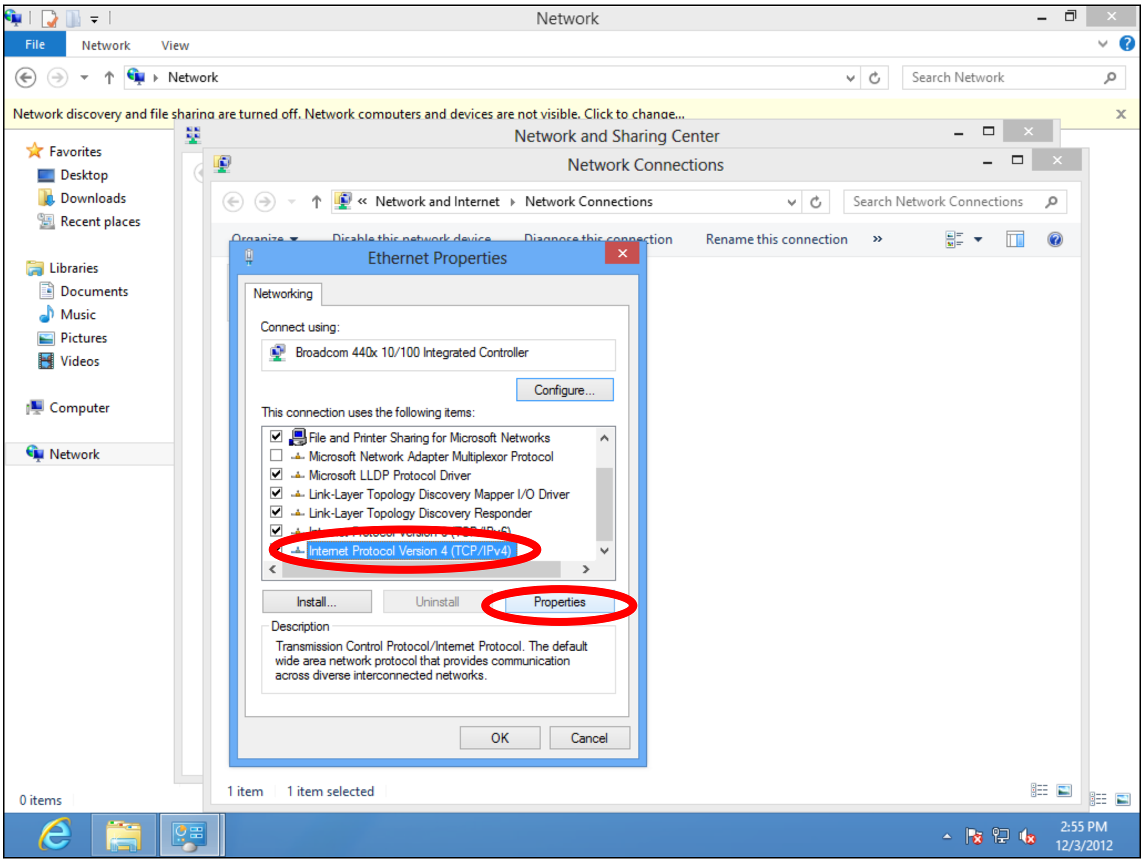
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

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



Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

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

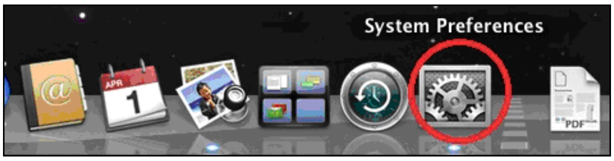
7. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

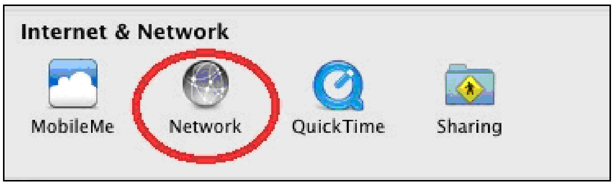
Click ‘OK’ when finished.

IV-1-2-5. Mac

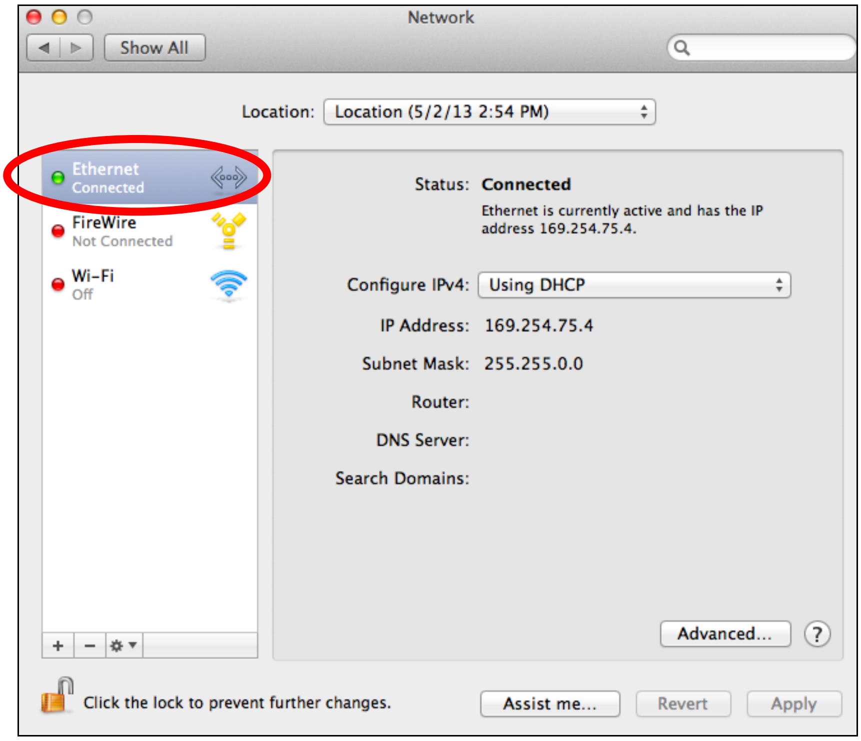
1. Have your Macintosh computer operate as usual, and click on "System Preferences"



2. In System Preferences, click on "Network".



3. Click on "Ethernet" in the left panel.



Location: Location (5/2/13 2:54 PM)

Status: **Connected**

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Using DHCP

IP Address: 169.254.75.4

Subnet Mask: 255.255.0.0

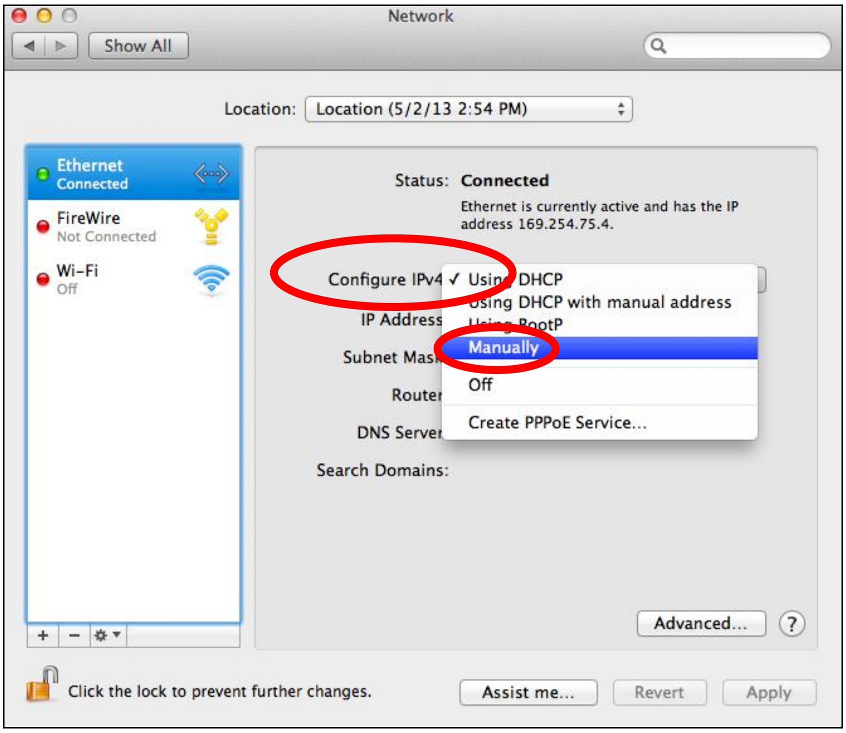
Router:

DNS Server:

Search Domains:

Click the lock to prevent further changes.

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



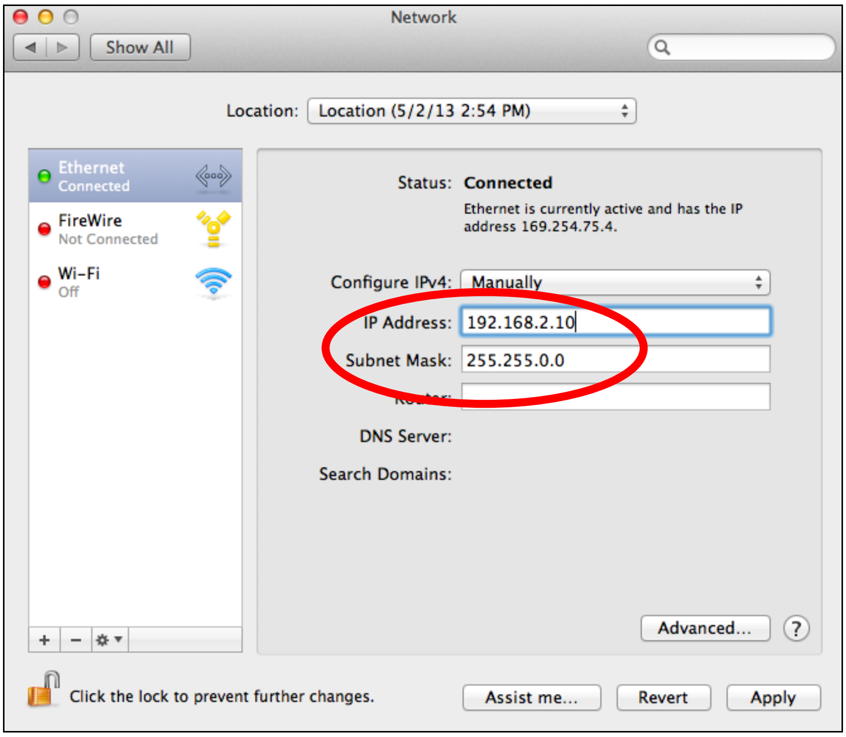
Location: Location (5/2/13 2:54 PM)

Status: Connected

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: ✓ Using DHCP

5. Enter the IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on “Apply” to save the changes.



Location: Location (5/2/13 2:54 PM)

Status: Connected

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Manually

IP Address: 192.168.2.10

Subnet Mask: 255.255.0.0

IV-1-5. Glossary

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

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

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandaccess point.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

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

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

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

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

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1’s followed by consecutive trailing 0’s, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as “x” number of leading 1’s.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1’s in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000

It means the device’s network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

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

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

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

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

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

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

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

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

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

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

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

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

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. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

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

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

FCC Caution

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

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

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

EU Countries Intended for Use

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

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 1999/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (1999/5/EK, 2009/125/EK, 2006/95/EK, 2011/65/EK).

Türkçe: Bu cihaz 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 1999/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1999/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Português: Este equipamento cumpre os requesitos essênciais da Directiva 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 1999/5/EG, 2009/125/EG, 2006/95/EG, 2011/65/EG.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 1999/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

suomen kieli: Tämä laite täyttää direktiivien 1999/5/EY, 2009/125/EY, 2006/95/EY, 2011/65/EY oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

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

CE FC N20379 АЯ46

WEEE Directive & Product Disposal

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

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directive 1999/5/EC, and 2009/125/EC, 2006/95/EC, 2011/65/EC .

Equipment: **N300 Wall-plug Access Point**
Model No.: **EW-7438APn**

The following European standards for essential requirements have been followed:

Spectrum: **ETSI EN 300 328 V1.7.1 (2006-10)**
EMC: **EN 301 489-1 V1.9.2 (2011-09);**
EN 301 489-17 V2.1.1 (2009-05)
EMF: **EN 50385:2002**
Safety (LVD): **IEC 60950-1:2005 (2nd Edition);**
EN-60950-1:2006+A11:2009+A1:2010+A12:2011

Edimax Technology Co., Ltd.
No. 3, Wu Chuan 3rd Road,
Wu-Ku Industrial Park,
New Taipei City, Taiwan

Date of Signature: November 15, 2011
Signature:

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

Notice According to GNU General Public License Version 2

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

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

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