



WAP-EN1750W
AC1750 Wireless Access Point
User Manual

Version 1.1.0, December 2016



FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the 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 instruction, may cause harmful interference to radio communication. 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:

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

The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Copyright

Copyright© 2016 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation. This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>

NOTE: This document is subject to change without notice.

Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling center and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law.

CONTENTS

- Overview 6**

- I. Product Information 7**
 - I-1. Package Contents 7
 - I-2. System Requirements..... 8
 - I-3. Hardware Overview..... 8
 - I-4. LED Status..... 9
 - I-5. Reset..... 9
 - I-6. Magnetic Wall Mount..... 10
 - I-7. Safety Information..... 11

- II. Quick Setup 12**
 - II-1. Initial Setup..... 12
 - II-2. Basic Settings..... 14
 - II-3. Wi-Fi Protected Setup (WPS)..... 18

- III. Hardware Installation..... 19**

- IV. Browser Based Configuration Interface..... 20**
 - IV-1. Information..... 22
 - IV-1-1. System Information 22
 - IV-1-2. Wireless Clients 26
 - IV-1-3. Wireless Monitor..... 28
 - IV-1-4. Log 30
 - IV-2. Network Settings 32
 - IV-2-1. LAN-Side IP Address 32
 - IV-2-2. LAN Port 35
 - IV-2-3. VLAN 36
 - IV-3. Wireless Settings 37
 - IV-3-1. 2.4GHz 11bgn 37
 - IV-3-1-1. Basic..... 37
 - IV-3-1-2. Advanced..... 40
 - IV-3-1-3. Security..... 42
 - IV-3-1-3-1. No Authentication 43
 - IV-3-1-3-2. WEP 44
 - IV-3-1-3-3. IEEE802.1x/EAP 44
 - IV-3-1-3-4. WPA-PSK..... 44
 - IV-3-1-3-5. WPA-EAP 45

IV-3-1-3-6.	Additional Authentication	45
IV-3-1-4.	WDS	46
IV-3-1-5.	Guest Network	47
IV-3-2.	5GHz 11ac 11an	49
IV-3-2-1.	Basic.....	49
IV-3-2-2.	Advanced	51
IV-3-2-3.	Security.....	53
IV-3-2-4.	WDS	54
IV-3-2-5.	Guest Network	56
IV-3-3.	WPS	56
IV-3-4.	RADIUS.....	59
IV-3-4-1.	RADIUS Settings.....	60
IV-3-4-2.	Internal Server	62
IV-3-4-3.	RADIUS Accounts.....	66
IV-3-6.	WMM	69
IV-3-7.	Schedule	71
IV-3-8.	Traffic Shaping.....	72
IV-4.	Management	73
IV-4-1.	Admin	73
IV-4-2.	Date and Time	76
IV-4-3.	Syslog Server.....	78
IV-4-4.	Ping Test	79
IV-4-5.	I'm Here	79
IV-4-6.	TR-069	80
IV-5.	Advanced	81
IV-5-1.	LED Settings	81
IV-5-2.	Update Firmware.....	82
IV-5-3.	Save/Restore Settings.....	83
IV-5-4.	Factory Default	84
IV-5-5.	Reboot	85
IV-5-6.	Operation	85

V. Appendix..... 86

V-1.	Configuring your IP address.....	86
V-1-1.	Windows XP.....	87
V-1-2.	Windows Vista	89
V-1-3.	Windows 7.....	91
V-1-4.	Windows 8.....	95
IV-1-5.	Mac.....	99
V-1-6.	Glossary	101

Overview

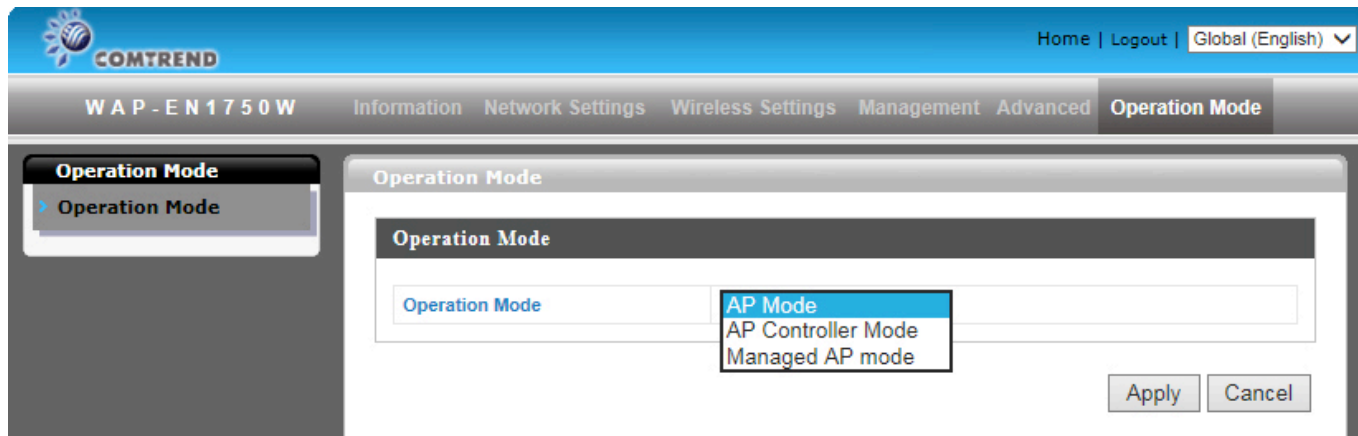
Your access point can function in three different modes.

The default mode for your access point is “AP Mode”.

AP Mode is a regular access point for your network.

AP Controller Mode acts as a designated “Master” for an array of “Slave” access points. (Group of linked access points)

Managed AP Mode acts like a “Slave” access point in an access point array. (Controlled by the AP Controller “Master”)

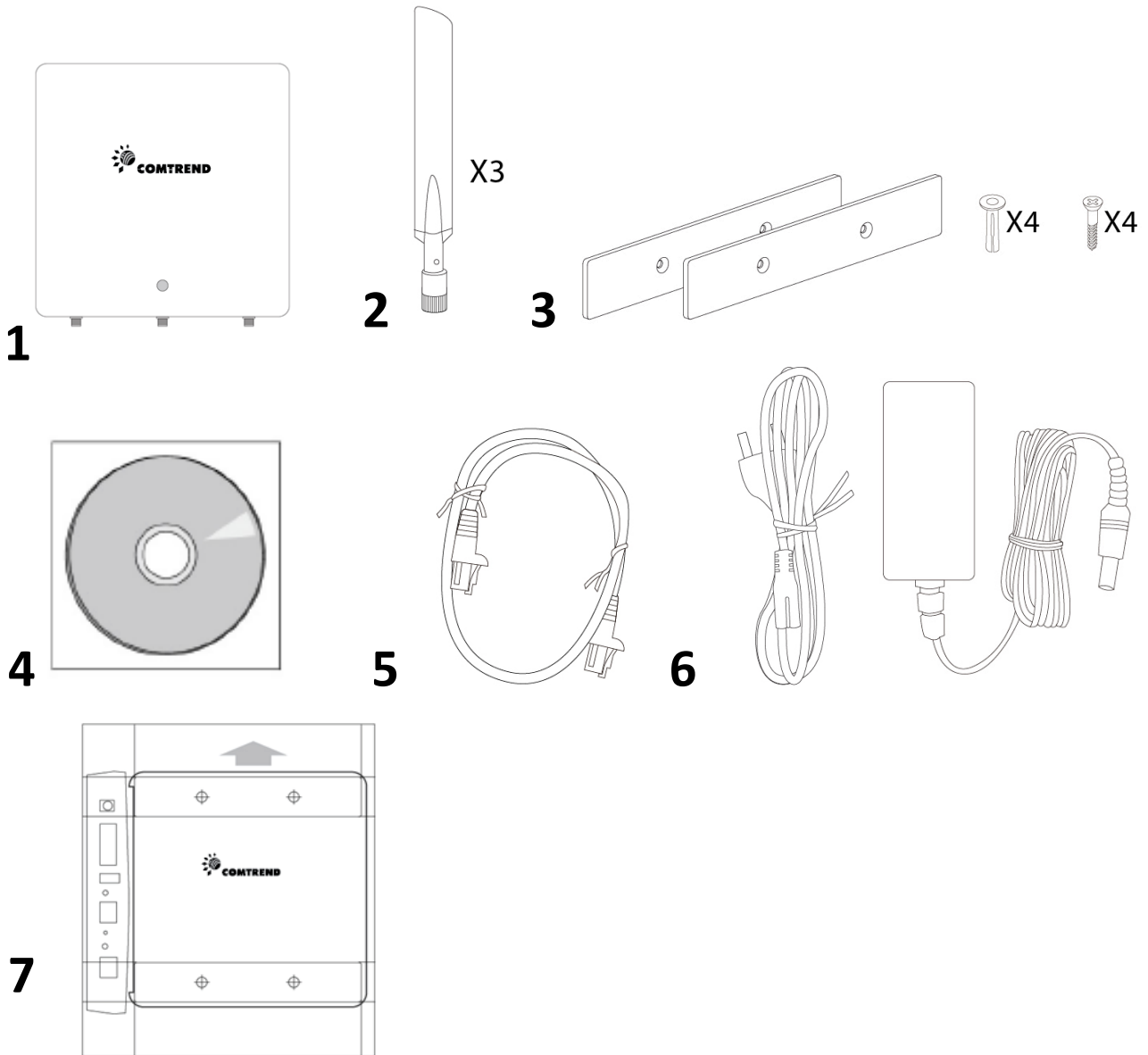


The user interface will change depending on which mode is selected.

This manual will cover the AP Mode functions.

I. Product Information

I-1. Package Contents



1. WAP-EN1750W Access Point

2. Antennas x 3

3. Magnetic Wall Mount x 2 &
Screws

4. CD

5. Ethernet Cable

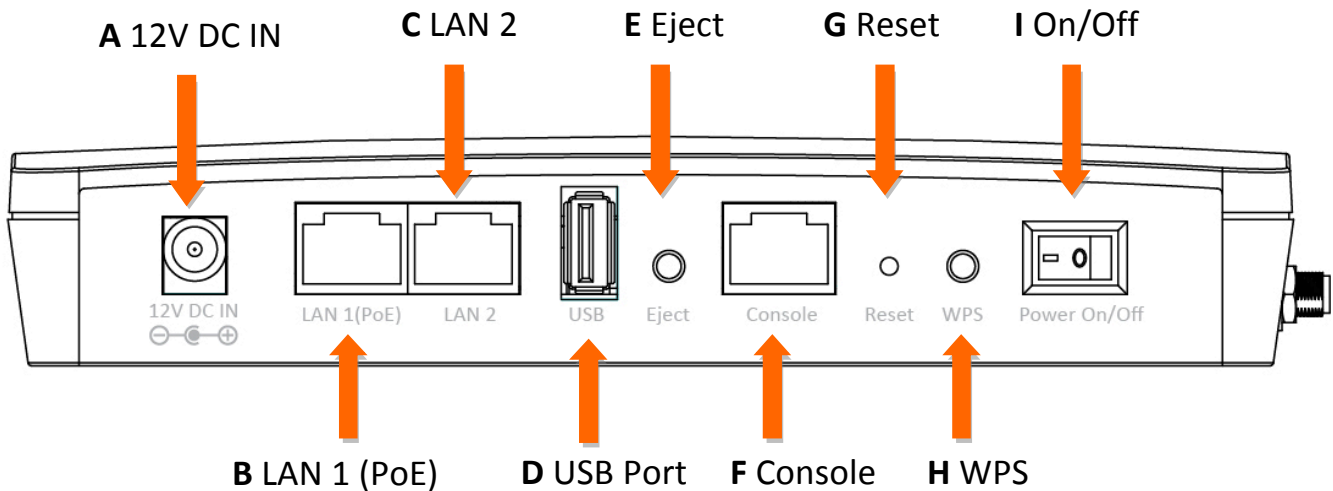
6. Power Adapter

7. Magnetic Wall Mount Screw
Template

I-2. System Requirements

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

I-3. Hardware Overview



- A.** 12V DC port to connect the power adapter
- B.** LAN port with Power over Ethernet (PoE) IN
- C.** LAN port with Power over Ethernet (PoE) OUT
- D.** USB Port for system log
- E.** Eject an attached USB device
- F.** Connect a management console
- G.** Reset the access point to factory default settings
- H.** Wi-Fi Protected Setup (WPS) button
- I.** Switch the access point on/off

I-4. LED Status

LED Status	Description
Off	The access point is off.
Blue	The access point is on.
Amber	The access point is starting up.
Flashing Amber	The access point cannot establish a connection to the network.
Flashing Amber and Blue	The access point experienced a problem starting up. The access point will restart.

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. Release the button when the LED is **flashing AMBER**.



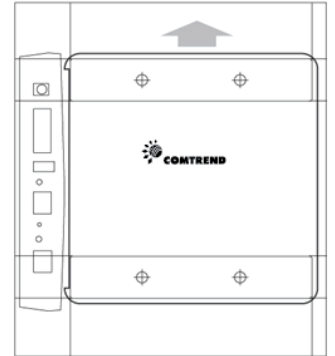
You may need to use a pencil or similar sharp object to push the reset button.

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

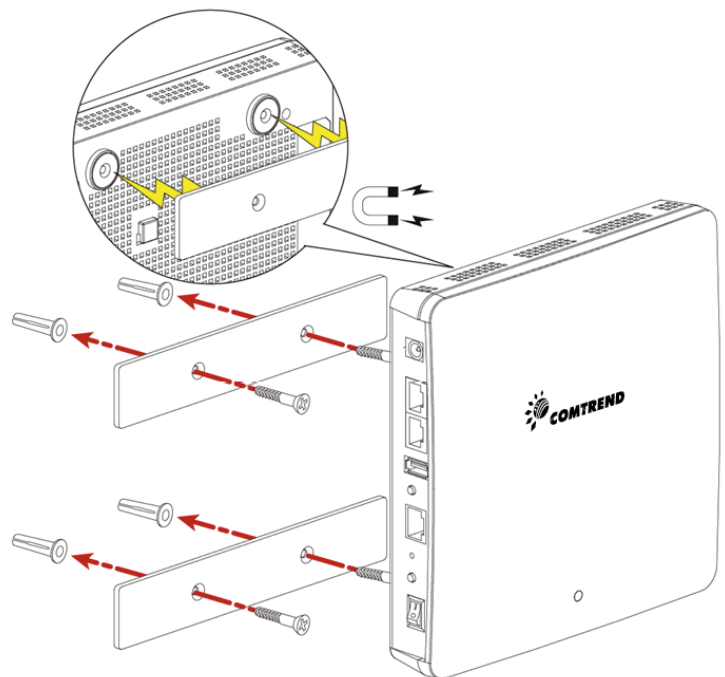
I-6. Magnetic Wall Mount

The access point includes a magnetic wall mount.

1. Use the included magnetic wall mount screw template to identify and mark correct screw positions on your selected wall.



2. Attach the two magnetic wall mount strips to your wall using the included screws, as shown below.



3. Press the back of your access point firmly against the two wall mounted magnetic strips, with the access point's Comtrend logo in the correct, upright orientation as displayed above.



Ensure your access point is securely attached to the magnetic strips.

I-7. Safety Information

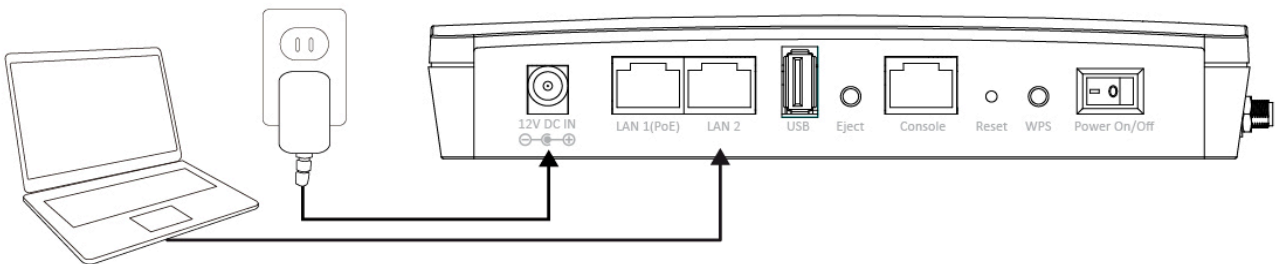
In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

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 Comtrend Customer Service for assistance.
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. Contact Comtrend Customer Service for assistance.


II. Quick Setup

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.



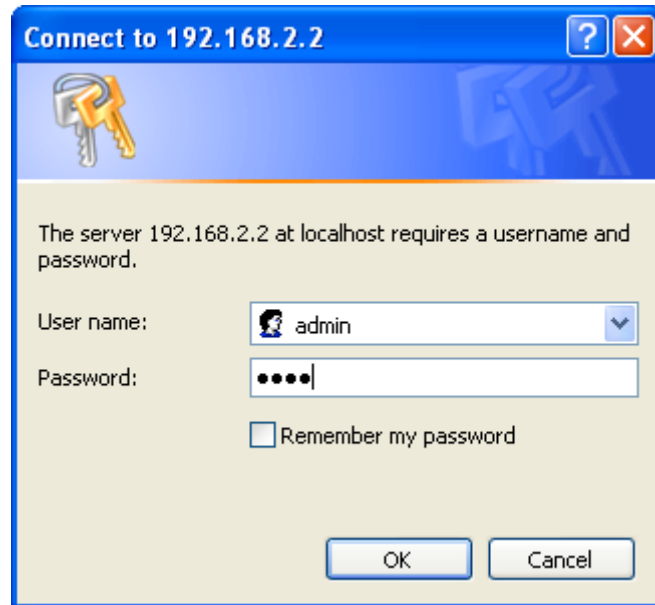
3. Please wait a moment for the access point to start up. The access point is ready when the LED is **blue**.
4. Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, please refer to Appendix **V-1. Configuring your IP address** for more information.

 ***DHCP is enabled on the access point by default. If no DHCP Service is found, the access point will default to IP address 192.168.2.2.***

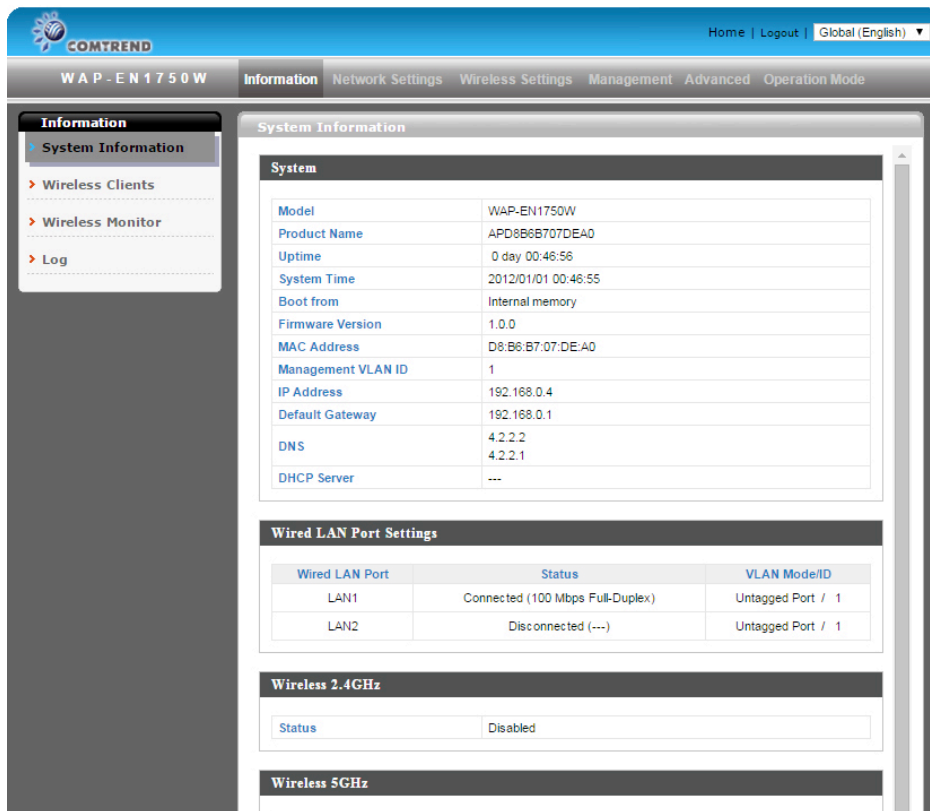
5. Enter the access point's default IP address **192.168.2.2** into the URL bar of a web browser.



6. You will be prompted for a username and password. Enter the default username "admin" and the default password "1234".



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



8. Next, please follow the instructions below in **II-2. 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:

- **LAN IP Address**
- **2.4GHz & 5GHz SSID & Security**
- **Administrator Name & Password**
- **Time & Date**



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

- 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.

LAN-side IP Address	
IP Address Assignment	DHCP Client <input type="button" value="v"/>
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP <input type="button" value="v"/> <input type="text"/>

DNS Servers	
Primary Address	From DHCP <input type="button" value="v"/> <input type="text"/>
Secondary Address	From DHCP <input type="button" value="v"/> <input type="text"/>

- 2.** Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and 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 192.168.2.2.

- 3.** To change the SSID of your access point's 2.4GHz wireless network(s), go to **"Wireless Setting" > "2.4GHz 11bgn" > "Basic"**. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".



To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled “Enable SSID number” and select how many SSIDs you require. Then enter a new SSID in the corresponding numbered fields below, before clicking “Apply”.

2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n
Enable SSID number	1
SSID1	WAP-5872u-FFC8E9_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 4.** To configure the security of your access point’s 2.4GHz wireless network(s), go to **“Wireless Setting” > “2.4GHz 11bgn” > “Security”**. Select an **“Authentication Method”** and enter a **“Pre-shared Key”** or **“Encryption Key”** depending on your choice, then click **“Apply”**.



If using multiple SSIDs, specify which SSID to configure using the “SSID” drop down menu.

2.4GHz Wireless Security Settings	
SSID	WAP-5872u-FFC8E9_G
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50
Authentication Method	No Authentication
Additional Authentication	No additional authentication

5. Go to **“Wireless Setting” > “5GHz 11ac 11an”** and repeat steps **3 & 4** for the access point’s 5GHz wireless network.
6. To change the administrator name and password for the browser based configuration interface, go to **“Management” > “Admin”**.

Account to Manage This Device

Administrator Name	admin
Administrator Password	••••• (4-32 Characters)
	••••• (Confirm)

Apply

7. Complete the **“Administrator Name”** and **“Administrator Password”** fields and click **“Apply”**.
8. To set the correct time for your access point, go to **“Management” > “Date and Time”**.

Date and Time Settings

Local Time

2012 Year Jan Month 1 Day

0 Hours 00 Minutes 00 Seconds

Acquire Current Time from Your PC

NTP Time Server

Use NTP Enable

Server Name

Update Interval 24 (Hours)

Time Zone

Time Zone (GMT-06:00) Central Time (US & Canada)

Apply Cancel

9. Set the correct time and time zone for your access point using the drop down menus. 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.



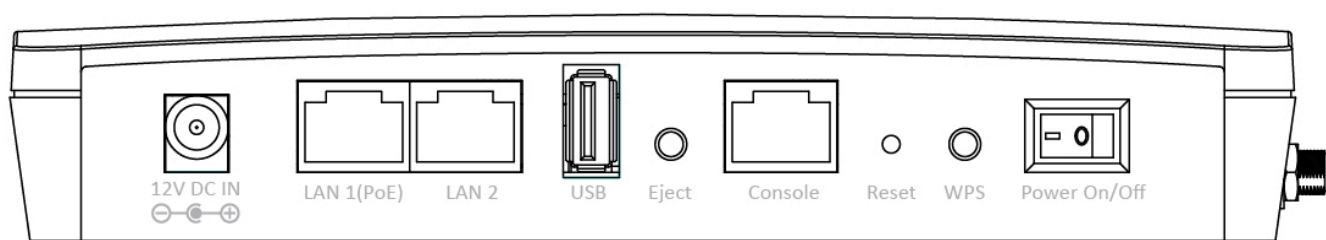
You can use the “Acquire Current Time from your PC” button if you wish to set the access point to the same time as your PC.

10. 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.

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

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. You can use the WPS button to establish a connection between the access point and a WPS-compatible wireless device/client.

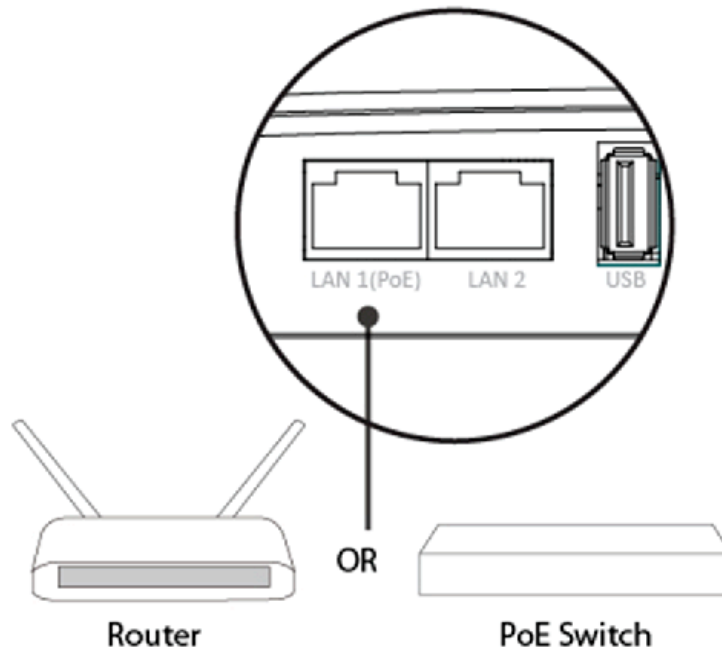
- 1.** Press and hold the Reset button on the front of the access point for 2 seconds.



- 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. Hardware Installation

1. Connect a router or switch to the access point's **LAN 1** port using an Ethernet cable. If powering the access point by PoE, the PoE switches **must** be connected to the access point's **LAN 1** port.

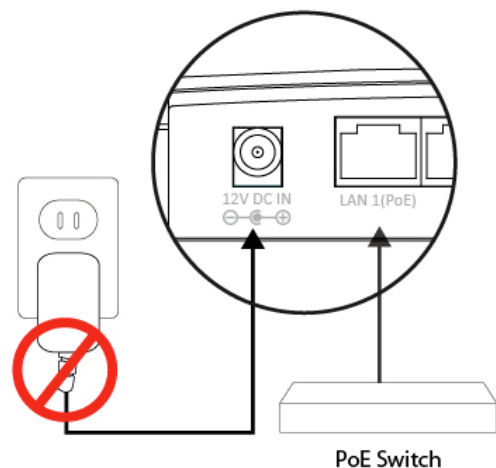


2. If you are not using a PoE switch, then connect the power adapter to the access point's 12V DC port and plug the power adapter into a power outlet.

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.



4. (Optional) Connect a local network device to the access point's **LAN 2** port.



The access point's LAN 2 port can support a PoE Powered Device. If powered by PoE, the LAN 2 port can provide 7.5w of PoE Power. If powered by the included 12v DC power adapter, a full 15.4w (IEEE 802.3af standard) of PoE Power is provided.

IV. Browser Based Configuration Interface

The browser-based configuration interface enables you to configure the access point's advanced features. The WAP-PC1750W features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, up to 16 SSIDs and many more. To access the browser based configuration interface:

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 "1234", 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 section I-5. Reset

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

The screenshot displays the Comtrend WAP-EN1750W web interface. The top navigation bar includes 'Home | Logout | Global (English)'. The main menu shows 'WAP-EN1750W' and 'Information' (selected), with other options like 'Network Settings', 'Wireless Settings', 'Management', 'Advanced', and 'Operation Mode'. The left sidebar lists 'Information' with sub-items: 'System Information' (selected), 'Wireless Clients', 'Wireless Monitor', and 'Log'. The main content area is titled 'System Information' and contains several sections:

- System Information Table:**

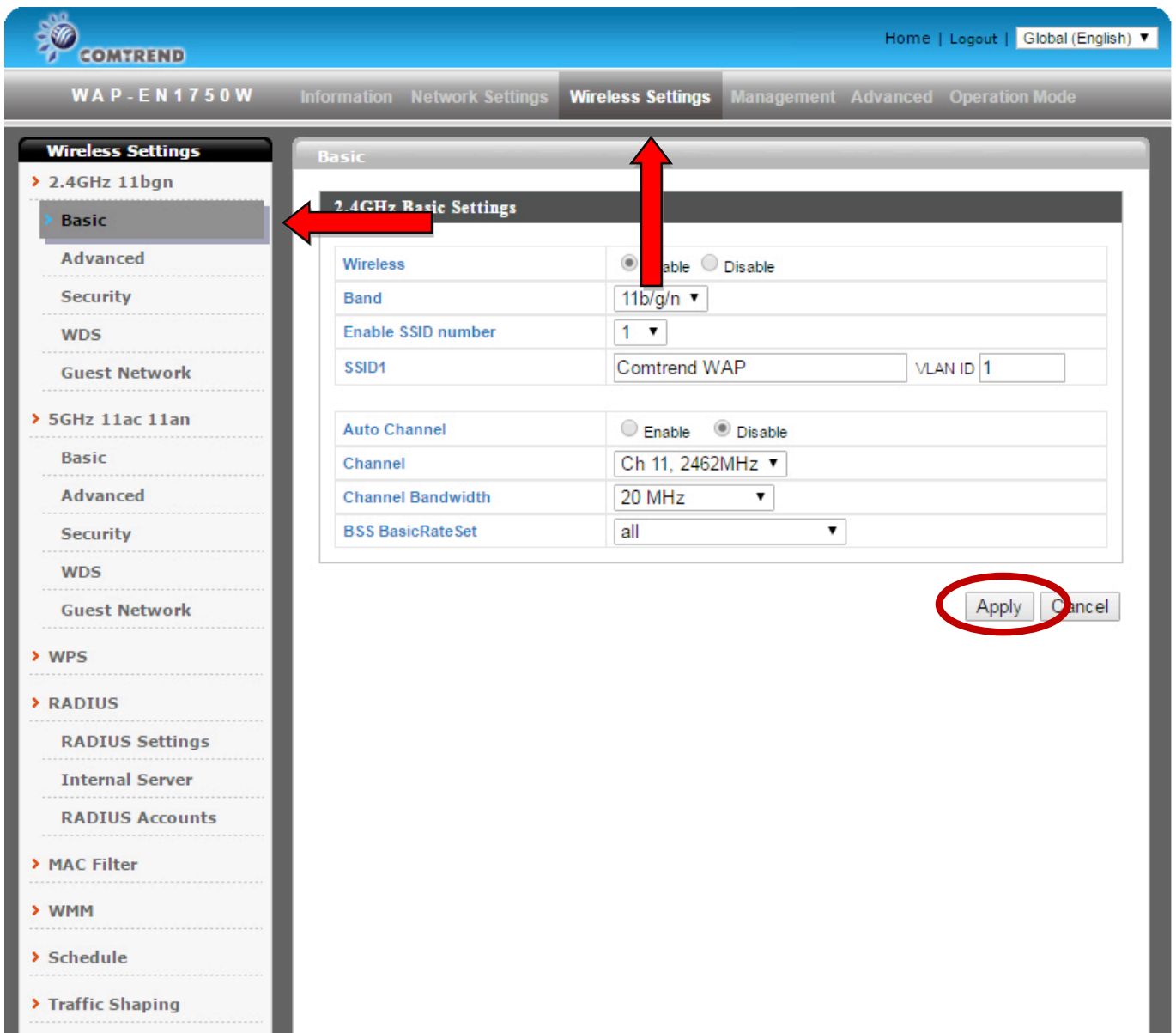
System	
Model	WAP-EN1750W
Product Name	APD8B6B707DEA0
Uptime	0 day 00:46:56
System Time	2012/01/01 00:46:55
Boot from	Internal memory
Firmware Version	1.0.0
MAC Address	D8:B6:B7:07:DE:A0
Management VLAN ID	1
IP Address	192.168.0.4
Default Gateway	192.168.0.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	---

- Wired LAN Port Settings Table:**


Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

- Wireless 2.4GHz:** Status: Disabled
- Wireless 5GHz:** (Section header visible, content partially obscured)

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.***

IV-1. Information

Information Network Settings Wireless Settings Management Advanced Operation Mode



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

IV-1-1. System Information

> System Information

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

System	
Model	
Product Name	COMTREND-AP
Uptime	9 days 05:42:15
Boot from	Internal memory
Version	1.0.5
MAC Address	00:1D:20:FF:C8:71
Management VLAN ID	1
IP Address	192.168.0.2 <input type="button" value="Refresh"/>
Default Gateway	192.168.0.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	192.168.0.1

Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
Wired Port (#1)	Connected (1000 Mbps Full-Duplex)	Untagged Port / 1
Wired Port (#2)	Disconnected (---)	Untagged Port / 1

Wireless 2.4GHz

Status	Enabled
MAC Address	00:1D:20:FF:C8:E9
Channel	Ch 4 (Auto)
Transmit Power	100%

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
WAP-5872u-FFC8E9_G	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Wireless 5GHz

Status	Enabled
MAC Address	00:1D:20:FF:C8:EA
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100%

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
WAP-5872u-FFC8E9_A	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 5GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Model	Displays the model number of the access point.
Product Name	Displays the product name for reference, which consists of “AP” plus the MAC address.
Uptime	Displays the total time since the device was turned on.
Boot From	Displays information for the booted hardware, booted from either USB or internal memory.
Version	Displays the software version of the access point.
MAC Address	Displays the access point’s MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. Click “Refresh” to update this value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of the DNS (Domain Name Server).
DHCP Server	IP address of the DHCP Server.

Wired LAN Port	Specifies which LAN port (1 or 2).
Status	Displays the status of the specified LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port. See IV-2-3. VLAN

Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point’s MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.

SSID	Displays the SSID name(s) for the specified frequency.
-------------	--

Authentication Method	Displays the authentication method for the specified SSID. See IV-3. Wireless Settings
Encryption Type	Displays the encryption type for the specified SSID. See IV-3. Wireless Settings
VLAN ID	Displays the VLAN ID for the specified SSID. See IV-2-3. VLAN
Additional Authentication	Displays the additional authentication type for the specified SSID. See IV-3. Wireless Settings
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See IV-2-3. VLAN
Refresh	Click to refresh all information.

IV-1-2. Wireless Clients

> Wireless Clients

The “Wireless Clients” page displays information about all wireless clients connected to the access point on the 2.4GHz or 5GHz frequency.

Refresh time

Auto Refresh time	<input checked="" type="radio"/> 5 seconds <input type="radio"/> 1 second <input type="radio"/> Disable
Manual Refresh	<input type="button" value="Refresh"/>

2.4GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
No wireless client								

5GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
No wireless client								

Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.

SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the access point.

Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client's wireless adapter is displayed here.

IV-1-3. Wireless Monitor

> Wireless Monitor

Wireless Monitor is a tool built into the access point to scan and monitor the surrounding wireless environment. Select a frequency and click “Scan” to display a list of all SSIDs within range along with relevant details for each SSID.

Wireless Monitor

Site Survey	<input checked="" type="radio"/> Wireless 2.4G/ 5G <input type="radio"/> 2.4G <input type="radio"/> 5G Scan
Channel Survey result	Export

Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

Wireless 5GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

Channel Survey	Select which frequency (or both) to scan, and click “Scan” to begin.
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage.

Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.

Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the specified SSID.

IV-1-4. Log

> Log

The system log displays system operation information such as up time and connection processes. This information is useful for network administrators.



When the log is full, old entries are overwritten.

```
Jan 1 00:01:18 [SYSTEM]: WLAN[2.4G], Best channel selection start, switch to channel 4
Jan 1 00:01:08 [SYSTEM]: WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
Jan 1 00:00:17 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan 1 00:00:17 [SYSTEM]: LAN, Port[0] link is changed to 1000Mbps-Full-Duplex
Jan 1 00:00:16 [SYSTEM]: HTTPS, start
Jan 1 00:00:16 [SYSTEM]: HTTP, start
Jan 1 00:00:16 [SYSTEM]: LAN, Firewall Disabled
Jan 1 00:00:16 [SYSTEM]: LAN, NAT Disabled
Jan 1 00:00:16 [SYSTEM]: NET, Firewall Disabled
Jan 1 00:00:16 [SYSTEM]: NET, NAT Disabled
Jan 1 00:00:16 [SYSTEM]: LEDs, light on specific LEDs
Jan 1 00:00:10 [SYSTEM]: WLAN[5G], Channel = AutoSelect
Jan 1 00:00:10 [SYSTEM]: WLAN[5G], Wireless Mode = 11ACVHT80
Jan 1 00:00:02 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan 1 00:00:02 [SYSTEM]: WLAN[2.4G], Wireless Mode = 11NGHT40MINUS
Jan 1 00:00:02 [SYSTEM]: DHCP, start
Jan 1 00:00:02 [SYSTEM]: LAN, start
Jan 1 00:00:02 [SYSTEM]: Bridge, start
Jan 1 00:00:02 [SYSTEM]: Bridge, start
Jan 1 00:00:00 [SYSTEM]: SYS, Model Name: Wireless Gigabit Router
Jan 1 00:00:00 [SYSTEM]: SYS, Application Version: 1.0.1
Jan 1 00:00:00 [SYSTEM]: BOOT, WAP-5872u
Jan 1 00:00:00 [RADIUS]: Start Log Message Service!
Jan 1 00:00:00 [USB]: Start Log Message Service!
Jan 1 00:00:00 [DHCP]: Start Log Message Service!
Jan 1 00:00:00 [SYSTEM]: Start Log Message Service!
```

Save Clear Refresh

Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:

USB

Mount & unmount

Wireless Client

Connected & disconnected

Key exchange success & fail

Authentication

Authentication fail or success

Association

Success or fail

WPS

M1 - M8 messages

WPS success

Change Settings

System Boot

Displays current model name

NTP Client

Wired Link

LAN Port link status and speed status

Proxy ARP

Proxy ARP module start & stop

Bridge

Bridge start & stop

SNMP

SNMP server start & stop

HTTP

HTTP start & stop

HTTPS

HTTPS start & stop

SSH

SSH-client server start & stop

Telnet

Telnet-client server start or stop

WLAN (2.4G)

WLAN (2.4G) channel status and country/region status

WLAN (5G)

WLAN (5G) channel status and country/region status

ADT

IV-2. Network Settings

Information **Network Settings** Wireless Settings Management Advanced Operation Mode

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

IV-2-1. LAN-Side IP Address

> LAN-side IP Address

The “LAN-side IP address” page allows you to configure your access point on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router’s DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers. You can also configure your Access Point to function as a DHCP Server on your LAN, to assign IP address to other devices.



If no IP address is provided a LAN DHCP Service, The access point’s default IP address is 192.168.2.2



It is recommended to Disable other DHCP servers on the LAN if using the AP as a DHCP Server.

LAN-side IP Address	
IP Address Assignment	Static IP Address ▾
IP Address	192.168.0.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
Primary DNS Address	4.2.2.2
Secondary DNS Address	4.2.2.1

IP Address Assignment

Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “Static IP” to manually specify a static/fixed IP address for your access point (below).

IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.

DHCP users can select to get DNS servers’ IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

Primary Address	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
Secondary Address	DHCP users can select “From DHCP” to get secondary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.

The screenshot shows a configuration window titled "LAN-side IP Address". It contains several fields:

- IP Address Assignment:** A dropdown menu set to "DHCP Client".
- IP Address:** A text field containing "192.168.222.220".
- Subnet Mask:** A text field containing "255.255.255.0".
- Default Gateway:** A dropdown menu set to "From DHCP" and a text field containing "192.168.222.1".
- Primary DNS Address:** A dropdown menu set to "From DHCP" and a text field containing "0.0.0.0".
- Secondary DNS Address:** A dropdown menu set to "From DHCP" and a text field containing "0.0.0.0".

DHCP Client	
IP Address	When “DHCP Client” is selected this value cannot be modified.
Subnet Mask	When “DHCP Client” is selected this value cannot be modified.
Default Gateway	Select “From DHCP” or select “User-Defined” and enter a default gateway.
Primary DNS Address	Select “From DHCP” or select “User-Defined” and enter a primary DNS address.
Secondary DNS Address	Select “From DHCP” or select “User-Defined” and enter a secondary DNS address.

LAN-side IP Address	
IP Address Assignment	DHCP Server
IP Address	192.168.222.220
Subnet Mask	255.255.255.0
IP Address Range	192.168.222.120 ~ 192.168.222.140
Domain Name	WAP1750
Lease Time	Forever
Default Gateway	192.168.222.1
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0

DHCP Server Static IP Address			
Index	MAC Address	IP Address	Action
1			Add

DHCP Client List			
Index	MAC Address	IP Address	Lease Time
No DHCP Client			

DHCP Server	
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
IP Address Range	Enter the start and end IP address of the IP address range which your access point's DHCP server will assign to devices on the network.
Domain Name	Enter a domain name.
Lease Time	Select a lease time from the drop down menu. IP addresses will be assigned for this period of time.
Default Gateway	Enter a default gateway.
Primary DNS Address	Enter a primary DNS address.
Secondary DNS Address	Enter a secondary DNS address.

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

DHCP Server Static IP Address	
MAC Address	Enter the MAC address of the network device to be assigned a static IP address.
IP Address	Specify the IP address to assign the device.
Add	Click to assign the IP address to the device.

IV-2-2. LAN Port

> LAN Port

The “LAN Port” page allows you to configure the settings for your access point’s two wired LAN (Ethernet) ports.

Wired LAN Port Settings				
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
Wired Port (#1)	Enabled <input type="button" value="v"/>	Auto <input type="button" value="v"/>	Enabled <input type="button" value="v"/>	Enabled <input type="button" value="v"/>
Wired Port (#2)	Enabled <input type="button" value="v"/>	Auto <input type="button" value="v"/>	Enabled <input type="button" value="v"/>	Enabled <input type="button" value="v"/>

Wired LAN Port	Identifies LAN port 1 or 2.
Enable	Enable/disable specified LAN port.
Speed & Duplex	Select a speed & duplex type for specified LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packet transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

IV-2-3. VLAN

> VLAN

The “VLAN” (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs 0 – 4094 are supported.



VLAN IDs in the range 0 – 4094 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port (#1)	Untagged Port ▼	1
Wired Port (#2)	Untagged Port ▼	1
Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [WAP-5872u-FFC8E9_G]	Untagged Port	1
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [WAP-5872u-FFC8E9_A]	Untagged Port	1

Management VLAN	
VLAN ID	1

Wired LAN Port/Wireless	Identifies LAN port 1 or 2, or wireless SSIDs (2.4GHz or 5GHz).
VLAN Mode	Select “Tagged Port” or “Untagged Port” for specified LAN/wireless interface.
VLAN ID	Set a VLAN ID for specified interface, if “Untagged Port” is selected.

VLAN ID	Specify the VLAN ID of the subnet. Hosts belonging to the subnet can only communicate with other hosts on the same subnet.
----------------	--

IV-3. Wireless Settings

Information Network Settings **Wireless Settings** Management Advanced Operation Mode



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

IV-3-1. 2.4GHz 11bgn

> 2.4GHz 11bgn

The “2.4GHz 11bgn” menu allows you to view and configure information for your access point’s 2.4GHz wireless network across four categories: Basic, Advanced, Security and WDS.

IV-3-1-1. Basic

> Basic

The “Basic” screen displays basic settings for your access point’s 2.4GHz Wi-Fi network (s).

2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n
Enable SSID number	1
SSID1	WAP-5872u-FFC8E9_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps

Wireless	Enable or disable the access point's 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 8 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 8). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for control communication frames for wireless clients.

When auto channel is disabled, select a wireless channel manually:

Channel Interval	Select a wireless channel from 1 – 13.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for control communication frames for wireless clients.

IV-3-1-2. Advanced

> 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.

2.4GHz Advanced Settings	
Contention Slot	Short ▾
Preamble Type	Short ▾
Guard Interval	Short GI ▾
802.11g Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Multicast Rate	Auto ▾
Tx Power	100% ▾
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM (see IV-3-6. WMM).
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble”.
Guard Interval	Set the guard interval.
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)

802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.
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.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Specifies the interval of the AP to probe for WLAN stations to verify if the station is still alive. The value ranges from 60 to 3600, in seconds. The default value is 60s.

IV-3-1-3. Security

> 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 is essential to configure wireless security in order to prevent unauthorised access to your network.



For optimal security, select a hard-to-guess password which include a combination of numbers, letters and symbols.

2.4GHz Wireless Security Settings	
SSID	WAP-5872u-FFC8E9_G ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

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.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below (IV-3-1-3-6.) appropriate for your method.

IV-3-1-3-1. No Authentication

Authentication is disabled and no password/key is required to connect to the access point.



Disabling wireless authentication is not recommended. When disabled, anybody within range can connect to your network.

IV-3-1-3-2. WEP

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

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit 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-3-1-3-3. IEEE802.1x/EAP

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
-------------------	--

IV-3-1-3-4. WPA-PSK

WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA only. WPA2 is safer than WPA only, but not supported by all wireless clients. Please make sure your wireless client supports your selection.
Encryption	Select "TKIP/AES Mixed Mode" or "AES" encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	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-3-1-3-5. WPA-EAP

WPA Type	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP.
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.



WPA-EAP must be disabled to use MAC-RADIUS authentication.

IV-3-1-3-6. Additional Authentication

Additional wireless authentication methods can also be used:

MAC Address Filter

Restrict wireless clients access based on MAC address specified in the MAC filter table.



See IV-3-5.MAC Filter to configure MAC filtering.

MAC Filter & MAC-RADIUS Authentication

Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

MAC-RADIUS Authentication

Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.



See IV-3-4.RADIUS to configure RADIUS servers.



WPS must be disabled to use MAC-RADIUS authentication. See IV-3-3. for WPS settings.

MAC RADIUS Password	<input checked="" type="radio"/> Use MAC address <input type="radio"/> Use the following password <input style="width: 150px; height: 20px;" type="text"/>
---------------------	---

MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select “Use the following password”, enter the password in the field below. The password should match the “Shared Secret” used in IV-3-4. RADIUS .
----------------------------	--

IV-3-1-4. WDS

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



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

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

2.4GHz	
WDS Functionality	<div style="border: 1px solid #ccc; padding: 2px;"> Disabled ▼ Disabled WDS with AP Dedicated WDS </div>
Local MAC Address	<input style="width: 100%;" type="text"/>
WDS Peer Settings	
WDS #1	MAC Address <input style="width: 100%;" type="text"/>
WDS #2	MAC Address <input style="width: 100%;" type="text"/>
WDS #3	MAC Address <input style="width: 100%;" type="text"/>
WDS #4	MAC Address <input style="width: 100%;" type="text"/>
WDS VLAN	
VLAN Mode	<div style="border: 1px solid #ccc; padding: 2px;"> Untagged Port ▼ (Enter at least one MAC address.) </div>
VLAN ID	<input style="width: 100%;" type="text" value="1"/>
WDS Encryption method	
Encryption	<div style="border: 1px solid #ccc; padding: 2px;"> None ▼ (Enter at least one MAC address.) </div>

2.4GHz	
WDS Functionality	Select “WDS with AP” to use WDS with access point or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption method	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters.

IV-3-1-5. Guest Network

The “Guest Network” page allows you to configure a guest network that will have a Layer-3 IP Filter applied to all traffic passing through the specific SSID.



When using a Guest Network, Traffic Shaping and IP Filter settings will be applied to all traffic passing through the Guest Network SSID.

Guest Network	
2.4GHz SSID	Comtrend-2.4g ▼
Guest Network	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Guest Access Policy			
Traffic Shaping Settings			
Traffic Shaping	Disable ▾		
Downlink	0 Mbps		
Uplink	0 Mbps		
Filtering Settings			
IP Filtering	Deny ▾		
Rules	<input type="checkbox"/>	IP/Subnet Mask	
	<input checked="" type="checkbox"/>	192.168.0.128	/255.255.255.128
	<input checked="" type="checkbox"/>	192.168.0.64	/255.255.255.192
	<input checked="" type="checkbox"/>	192.168.0.32	/255.255.255.224

Guest Network	
2.4GHz SSID	Select the SSID that you want to apply the Guest Network settings to.
Guest Network	Enable or Disable Guest Network settings.
Guest Access Policy	
Traffic Shaping	Select “Enable” to apply bandwidth limitations on the “Downlink” and “Uplink” performance on the Guest Network.
Filtering Settings	Select “Allow” or “Deny” to apply IP Filtering to the traffic on the Guest Network. Provide the IP and Subnet Mask you want to apply as a filter. Up to 3 IP Filters are supported.

IV-3-2. 5GHz 11ac 11an

> 5GHz 11ac 11an

The “5GHz 11ac 11an” menu allows you to view and configure information for your access point’s 2.4GHz wireless network across four categories: Basic, Advanced, Security and WDS.

IV-3-2-1. Basic

> Basic

The “Basic” screen displays basic settings for your access point’s 5GHz Wi-Fi network (s).

5GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11a/n/ac ▼
Enable SSID number	1 ▼
SSID1	WAP-5872u-FFC8E9_A <input type="text"/> VLAN ID <input type="text" value="1"/>
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	W52 ▼
Auto Channel Interval	One day ▼ <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz ▼
BSS BasicRateSet	6,12,24 Mbps ▼

Wireless	Enable or disable the access point’s 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11a, 802.11n & 802.11ac can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 5GHz frequency from the drop down menu. A maximum of 8 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 8). The SSID can consist of any combination of up to 32 alphanumeric characters.

VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for control communication frames for wireless clients.

When auto channel is disabled, select a wireless channel manually:

Channel Interval	Select a wireless channel.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for control communication frames for wireless clients.

IV-3-2-2. Advanced

> 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.

5GHz Advanced Settings	
Guard Interval	Short GI <input type="button" value="v"/>
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	<input type="text" value="1"/> (1-255)
RTS Threshold	<input type="text" value="2347"/> (1-2347)
Fragment Threshold	<input type="text" value="2346"/> (256-2346)
Multicast Rate	Auto <input type="button" value="v"/>
Tx Power	100% <input type="button" value="v"/>
Beacon Interval	<input type="text" value="100"/> (40-1000 ms)
Station idle timeout	<input type="text" value="60"/> (30-65535 seconds)

Guard Interval	Set the guard interval.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.

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.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Specifies the interval of the AP to probe for WLAN stations to verify if the station is still alive. The value ranges from 60 to 3600, in seconds. The default value is 60s.

IV-3-2-3. Security

> 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 is essential to configure wireless security in order to prevent unauthorised access to your network.***

 ***For optimal security, select a hard-to-guess password which include a combination of numbers, letters and symbols.***

5GHz Wireless Security Settings	
SSID	WAP-5872u-FFC8E9_A
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 / 50
Authentication Method	No Authentication
Additional Authentication	No additional authentication

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.

Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below appropriate for your method.

Please refer back to section **IV-3-1-3. Security** for more information on authentication and additional authentication types.

IV-3-2-4. WDS



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



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

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

5GHz WDS Mode	
WDS Functionality	Disabled ▼
Local MAC Address	Disabled WDS with AP Dedicated WDS

WDS Peer Settings	
WDS #1	MAC Address <input type="text"/>
WDS #2	MAC Address <input type="text"/>
WDS #3	MAC Address <input type="text"/>
WDS #4	MAC Address <input type="text"/>

WDS VLAN	
VLAN Mode	Untagged Port ▼ (Enter at least one MAC address.)
VLAN ID	1 <input type="text"/>

Encryption method	
Encryption	None ▼ (Enter at least one MAC address.)

5GHz WDS Mode	
WDS Functionality	Select “WDS with AP” to use WDS with access point or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDA devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES with 8-63 alphanumeric characters.

IV-3-2-5. Guest Network

The “Guest Network” page allows you to configure a guest network that will have a Layer-3 IP Filter applied to all traffic passing through the specific SSID.



When using a Guest Network, Traffic Shaping and IP Filter settings will be applied to all traffic passing through the Guest Network SSID.

Guest Network	
5GHz SSID	Comtrend-5g ▼
Guest Network	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Guest Access Policy													
Traffic Shaping Settings													
Traffic Shaping	Disable ▼												
Downlink	0 Mbps												
Uplink	0 Mbps												
Filtering Settings													
IP Filtering	Deny ▼												
Rules	<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th colspan="2">IP/Subnet Mask</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>192.168.0.128</td> <td>/255.255.255.128</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>192.168.0.64</td> <td>/255.255.255.192</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>192.168.0.32</td> <td>/255.255.255.224</td> </tr> </tbody> </table>	<input type="checkbox"/>	IP/Subnet Mask		<input checked="" type="checkbox"/>	192.168.0.128	/255.255.255.128	<input checked="" type="checkbox"/>	192.168.0.64	/255.255.255.192	<input checked="" type="checkbox"/>	192.168.0.32	/255.255.255.224
<input type="checkbox"/>	IP/Subnet Mask												
<input checked="" type="checkbox"/>	192.168.0.128	/255.255.255.128											
<input checked="" type="checkbox"/>	192.168.0.64	/255.255.255.192											
<input checked="" type="checkbox"/>	192.168.0.32	/255.255.255.224											

Guest Network	
5GHz SSID	Select the SSID that you want to apply the Guest Network settings to.
Guest Network	Enable or Disable Guest Network settings.
Guest Access Policy	
Traffic Shaping	Select “Enable” to apply bandwidth limitations on the “Downlink” and “Uplink” performance on the Guest Network.
Filtering Settings	Select “Allow” or “Deny” to apply IP Filtering to the traffic on the Guest Network. Provide the IP and Subnet Mask you want to apply as a filter. Up to 3 IP Filters are supported.

IV-3-3. WPS

> 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 (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.



Please refer to manufacturer's instructions for your other WPS device.

WPS	<input checked="" type="checkbox"/> Enable
-----	--

Apply

WPS	
Product PIN	58327524 <input type="button" value="Generate PIN"/>
Push-button WPS	<input type="button" value="Start"/>
WPS by PIN	<input type="text"/> <input type="button" value="Start"/>

WPS Security	
WPS Status	Not Configured <input type="button" value="Release"/>

WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication (see IV-3-1-3-6 & IV-3-4).
Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click "Generate PIN" to generate a new WPS PIN code.
Push-Button WPS	Click "Start" to activate WPS on the access point for approximately 2 minutes. This has the same effect as physically pushing the access point's WPS button.
WPS by PIN	Enter the PIN code of another WPS device and click "Start" to attempt to establish a WPS connection for approximately 2 minutes.
WPS Status	WPS security status is displayed here. Click "Release" to clear the existing status.

IV-3-4. RADIUS

> RADIUS

The RADIUS sub menu allows you to configure the access point's RADIUS server settings, categorized into three submenus: RADIUS settings, Internal Server and RADIUS accounts.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point's internal RADIUS server can be used.



To use RADIUS servers, go to “Wireless Settings” → “Security” and select the desired Authentication Method → “Additional Authentication” and select “MAC RADIUS Authentication” (see IV-3-1-3. & IV-3-2-3).



The “MAC RADIUS Authentication” feature works with an external RADIUS Server Only.

IV-3-4-1. RADIUS Settings

> RADIUS Settings

Configure the RADIUS server settings for 2.4GHz & 5GHz. Each frequency can use a primary and secondary (backup) RADIUS server.

RADIUS Server (2.4GHz)	
Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>
Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Server (5GHz)

Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in IV-3-1-3-6 or IV-3-2-3 .
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535.

IV-3-4-2. Internal Server

> Internal Server

The access point features a built-in RADIUS server which can be configured as shown below

To use the Internal Radius Server as an additional authentication, configure the “Authentication Method” in “Wireless Settings/Security” to “IEEE802.1x/EAP”. Leave “Additional Authentication” set to “No additional authentication”. Click “Apply” to save settings. (Example image below)

The screenshot shows the 'Security' configuration page for the 5GHz wireless network. The left sidebar shows the navigation menu with 'Security' selected under '5GHz 11ac 11an'. The main content area is titled '5GHz Wireless Security Settings' and contains the following fields:

SSID	Internal-Radius
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 / 50
Authentication Method	IEEE802.1x/EAP
Key Length	64-bit
Additional Authentication	No additional authentication

Buttons for 'Apply' and 'Cancel' are located at the bottom right of the configuration area.

Next, Under “Radius/Radius Settings”, Select “Internal” for Radius Type. Click “Apply” to save settings. (Example image below)

The screenshot shows the 'RADIUS Settings' configuration page. The left sidebar shows the navigation menu with 'RADIUS Settings' selected under 'RADIUS'. The main content area is titled 'RADIUS Settings' and contains two sections: 'RADIUS Server (2.4GHz)' and 'RADIUS Server (5GHz)'. Each section has a 'Primary RADIUS Server' and a 'Secondary RADIUS Server' configuration area.

RADIUS Server (2.4GHz) - Primary RADIUS Server:

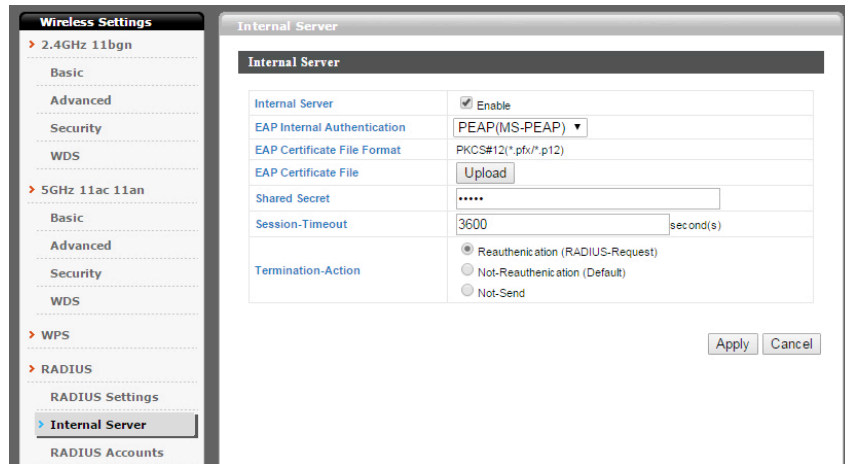
RADIUS Type	<input checked="" type="radio"/> Internal <input type="radio"/> External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	1813

RADIUS Server (5GHz) - Primary RADIUS Server:

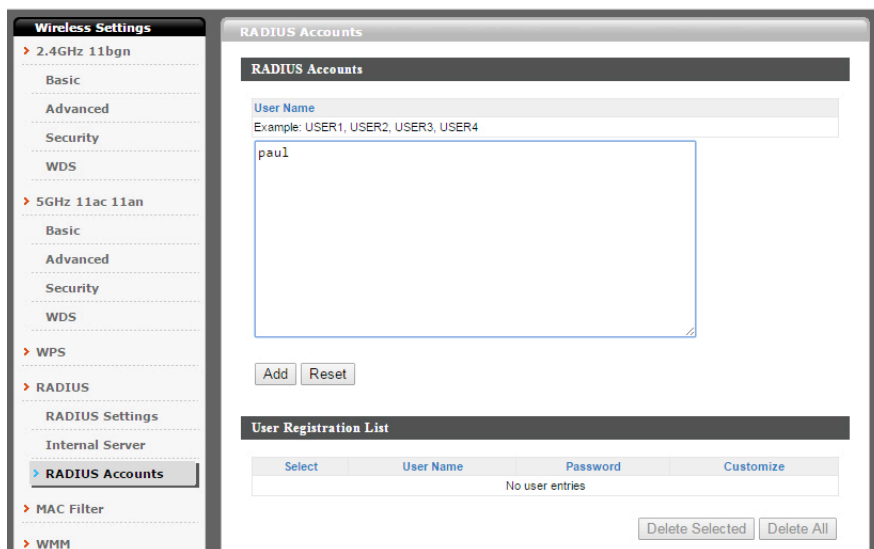
RADIUS Type	<input checked="" type="radio"/> Internal <input type="radio"/> External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	1813

Under “Radius/Internal Server”, check the “Enable” box next to “Internal Server”. Select “PEAP (MS-PEAP)” for “EAP Internal Authentication”. Enter numbers or

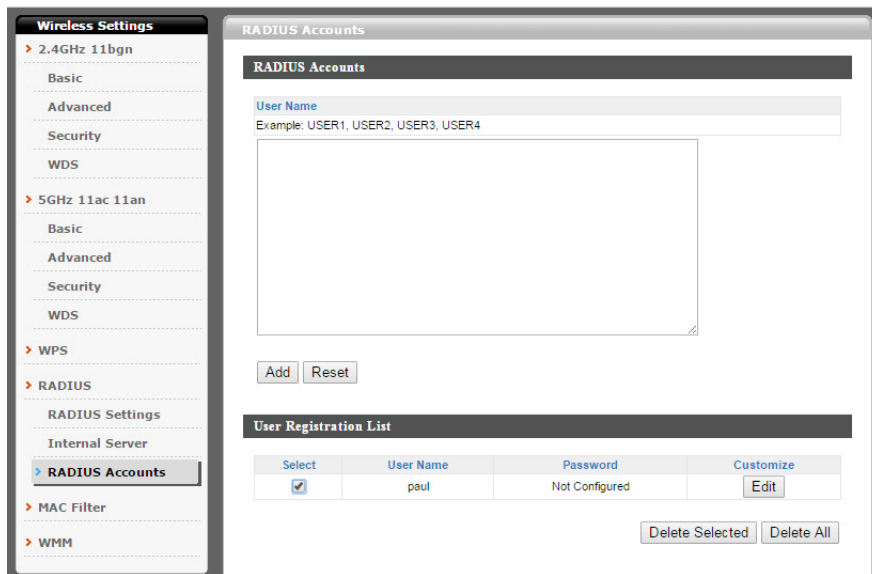
characters in the field “Shared Secret”. Set “Termination-Action” option to “Reauthentication (Radius-Request).” Click “Apply” to save changes. (Example image below)



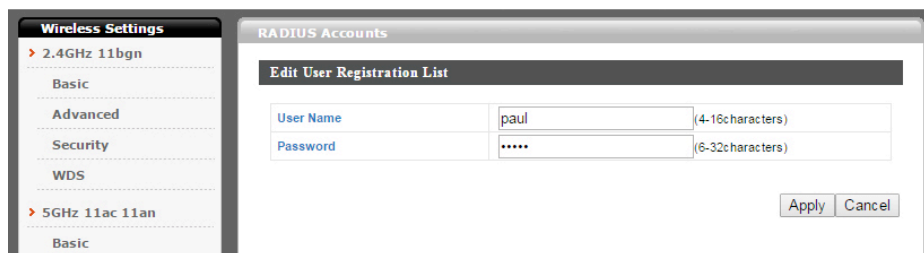
Do the following to add Radius User Names and configure passwords. Under “Radius/Radius Accounts”, enter a “User Name” in the window and click “Add”. (Example image below)



Select the “User Name” from the “User Registration List” and select “Edit”.
(Example image below)



Enter a password for the selected “User”. Click “Apply” to save changes.
(Example image below)



Your access point is now setup to authenticate Users with the Internal Radius Server.

Wireless Client Configuration for Radius Connection on Windows 7 (Example)

Go to "Control Panel/Network and Sharing Center/Manage Wireless Network".

Click "Add" on the "Manage wireless networks these use (Wireless Connection)" screen.

Click "Manually create a network profile".

Enter the "Network Name" which you want to connect to. The Network Name is the SSID for the Radius connection. In the examples above, the network name used is "Internal-Radius".

Adjust the "Security Type" to "802.1x". Click "Next".

Click "Change Connection Settings".

Click the "Security" tab and then "Settings".

Uncheck "Validate server certificate".

Click "Configure" next to "Secured password (EAP-MSCHAP v2)".

Uncheck "Automatically use my Windows Logon name and password".

Click "OK" to close all windows.

Select the Radius Network and Click "Connect".

You will receive a pop up message stating "Additional information is needed to connect".

Click on the message to continue.

Enter the Username and password you created in the "Windows Security" window.

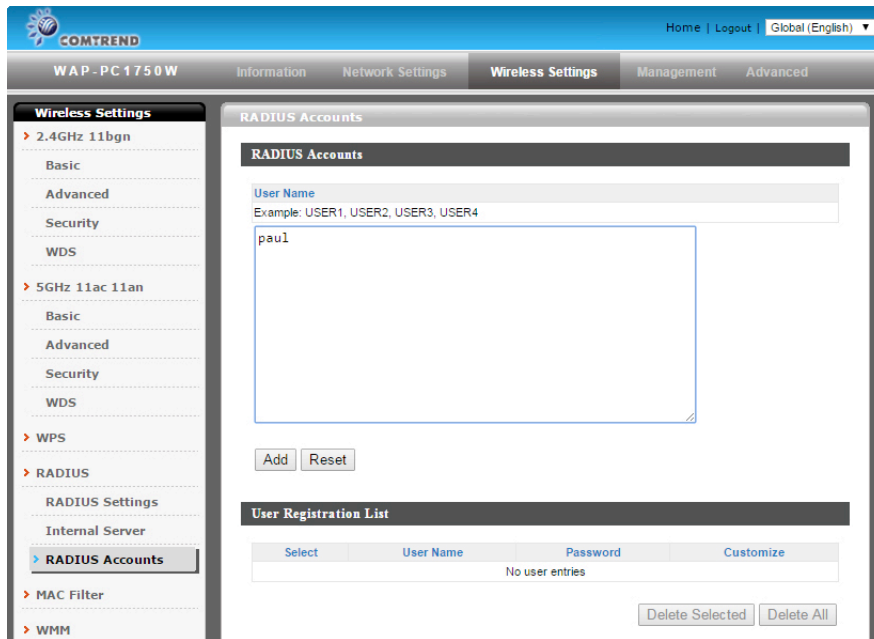
Click "OK".

Your connection to the SSID with Radius Authentication is now "Connected".

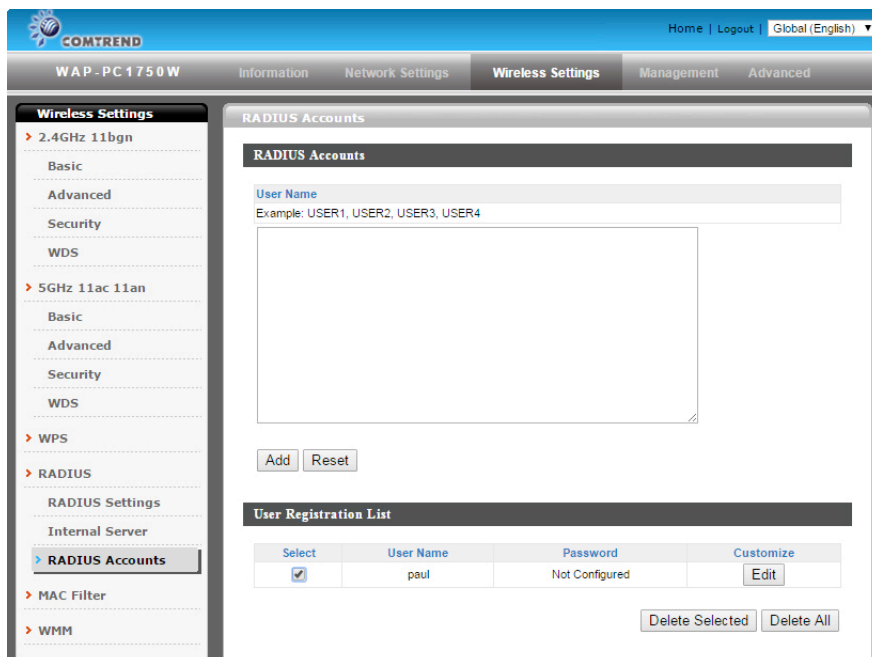
IV-3-4-3. RADIUS Accounts

> RADIUS Accounts

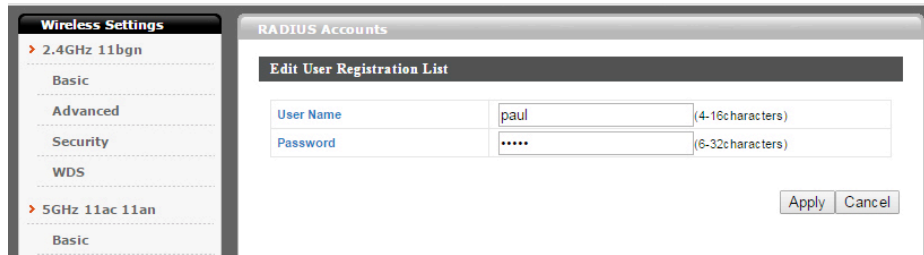
The internal RADIUS server can authenticate up to 256 user accounts. The “RADIUS Accounts” page allows you to configure and manage users. Do the following to add Radius User Names and configure passwords. Under “Radius/Radius Accounts”, enter a “User Name” in the window and click “Add”. (Example image below)



Select the “User Name” from the “User Registration List” and select “Edit”. (Example image below)



Enter a password for the selected “User”. Click “Apply” to save changes.
(Example image below)



IV-3-5. MAC Filter

> 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 access point. 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 access point, it will be denied.



To enable MAC filtering, go to “Wireless Settings” → “2.4GHz 11bgn/5GHz 11ac 11an” → “Security” → “Additional Authentication” and select “MAC Filter” (see IV-3-1-3. & IV-3-2-3).

The MAC address filtering table is displayed below:

Add MAC Addresses

Add
Reset

MAC Address Filtering Table

Select	MAC Address
<input type="checkbox"/>	00:1C:BF:10:CB:68

Delete Selected
Delete All
Export

Add 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'.
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.

Select	Delete selected or all entries from the table.
MAC Address	The MAC address is listed here.
Delete Selected	Delete the selected MAC address from the list.
Delete All	Delete all entries from the MAC address filtering table.
Export	Click "Export" to save MAC address filtering as a file to your local computer.

IV-3-6. WMM

> WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

WMM-EDCA Settings				
WMM Parameters of Access Point				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47
WMM Parameters of Station				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1024. The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above). Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511 or 1024.
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value effects higher priority.

IV-3-7. Schedule

Schedule allows an administrator to set specific hours of operation of the wireless access point. This feature is designed to provide wireless service during hours of operation and disables the wireless access point service during off hours. When “Enabled”, the wireless access point **will operate** in accordance with the specified schedule.

Schedule

Enable the wireless network during the following schedules.

Schedule Enable

Apply

Schedule List

#	SSID	Day of Week	Time	Select
No schedule entries				

Add Edit Delete Selected Delete All

Add/Edit a schedule by clicking the Add or Edit button. The schedule/Settings menu will allow you to schedule operational hours for each SSID for both the 2.4GHz and 5GHz Bands.

Schedule

Settings

2.4GHz SSID		5GHz SSID				
<input type="checkbox"/>	Comtrend WAP	<input type="checkbox"/>	Comtrend WAP 5g			
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00 ▾ : 00 ▾	End Time	00 ▾ : 00 ▾			

Apply Cancel

IV-3-8. Traffic Shaping

Traffic Shaping allows an administrator to limit the bandwidth available to each SSID. Providing a value between 0-1024Mbps. A value of “0” indicates unlimited bandwidth.

Traffic Shaping

Traffic Shaping for ssid(2.4GHz)

Enable

Unlimited : 0 Mbps

Down Link/Up Link Maximum : Mbps

SSID	Down Link	Up Link
WAP-EN1750W-07DEA0_G_1	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_2	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_3	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_4	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_5	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_6	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_7	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_8	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_9	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_10	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_11	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_12	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_13	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_14	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_15	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps
WAP-EN1750W-07DEA0_G_16	<input type="text" value="0"/> Mbps	<input type="text" value="0"/> Mbps

IV-4. Management

Information Network Settings Wireless Settings **Management** Advanced Operation Mode



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

IV-4-1. Admin

> 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 section I-5. Reset for how to reset the access point.

Account to Manage This Device	
Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="....."/> (4-32Characters)
	<input type="password" value="....."/> (Confirm)
<input type="button" value="Apply"/>	

Advanced Settings	
Product Name	<input type="text" value="WAP-EN1750W-2"/>
Management Protocol	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> TELNET <input type="checkbox"/> SSH <input type="checkbox"/> SNMP
Login Timeout	<input type="text" value="30"/> (mins)
SNMP Version	<input type="text" value="v1/v2c"/>
SNMP Get Community	<input type="text" value="public"/>
SNMP Set Community	<input type="text" value="private"/>
SNMP Trap	<input type="text" value="Disabled"/>
SNMP Trap Community	<input type="text" value="public"/>
SNMP Trap Manager	<input type="text" value=""/>
<input type="button" value="Apply"/>	

Administrator Name	Set the access point's administrator name. This is used to log in to the browser based configuration interface.
Administrator Password	Set the access point's administrator password. This is used to log in to the browser based configuration interface.

Product Name	Edit the product name according to your preference. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
Login Timeout	Change the Login Timeout from the 5 minute default. (Values include 5, 10, 15, 20 and 30 minutes)
SNMP Version	Select SNMP version appropriate for your

	SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (maximum 128 characters) of the SNMP manager.

HTTP

Internet browser HTTP protocol management interface

HTTPS

Internet browser HTTPS protocol management interface

TELNET

Client terminal with telnet protocol management interface

SSH

Client terminal with SSH protocol version 1 or 2 management interface

SNMP

Network management protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (UM) architecture.

IV-4-2. Date and Time

> Date and Time

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.

Date and Time Settings

Local Time

2012 ▼ Year Jan ▼ Month 1 ▼ Day

0 ▼ Hours 00 ▼ Minutes 00 ▼ Seconds

Acquire Current Time from Your PC

NTP Time Server

Use NTP Enable

Server Name

Update Interval (Hours)

Time Zone

Time Zone (GMT-06:00) Central Time (US & Canada) ▼

Local Time	Set the access point's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.

Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish. (ex. "time.windows.com")
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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.
------------------	--

IV-4-3. Syslog Server

> Syslog Server

The system log can be sent to a server, attached to USB storage or sent via email.

Syslog Server Settings	
Transfer Logs	<input type="checkbox"/> Enable Syslog Server <input type="text"/>
Copy Logs to Attached USB Device	<input type="checkbox"/> Enable

Syslog E-mail Settings	
E-mail Logs	<input checked="" type="checkbox"/>
E-mail Subject	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text"/>
Sender E-mail	<input type="text"/>
Receiver E-mail	<input type="text"/>
Authentication	<input type="text"/> <ul style="list-style-type: none"> SSL ▾ Disable SSL TLS
Account	<input type="text"/>
Password	<input type="text"/>

Syslog Server Settings	
Transfer Logs	Check/uncheck the box to enable/disable the use of a syslog server, and enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.
Copy Logs to Attached USB Device	Check/uncheck the box to enable/disable copying logs to attached USB storage.

Syslog Email Settings	
Email Logs	Check/uncheck the box to enable/disable email logs. When enabled, the log will be emailed according to the settings below.
Email Subject	Enter the subject line of the email which will be sent containing the log.
SMTP Server Address	Specify the SMTP server address for the sender email account.
SMTP Server Port	Specify the SMTP server port for the sender email account.
Sender Email	Enter the sender's email address.
Receiver Email	Specify the email recipient of the log.

Authentication	Select “Disable”, “SSL” or “TLS” according to your email authentication.
Account	When authentication is used above, enter the account name.
Password	When authentication is used above, enter the password.

IV-4-4. Ping Test

The access point includes a built-in ping test feature. Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.

IV-4-5. I’m Here

The access point features a built-in buzzer which can sound on command using the “I’m Here” page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

 ***The buzzer is loud!***

Duration of Sound	Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked.
Sound Buzzer	Activate the buzzer sound for the above specified duration of time.

IV-4-6. TR-069

TR-069 allows an administrator to establish a connection to an existing ACS System. These settings are unique to each ACS System.

ACS Settings	
URL	<input type="text" value="http://192.168.168.76:80"/>
Username	<input type="text" value="admin"/>
Password	<input type="text" value="12345"/>

Connection Request Account Information	
Username	<input type="text" value="admin"/>
Password	<input type="text" value="12345"/>

Connection Request URL	
CWMP Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Periodic Inform Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Periodic Inform Interval	<input type="text" value="30"/>
Periodic Inform Time	<input type="text" value="0000-00-00T00:00:00"/>

IV-5. Advanced

Information Network Settings Wireless Settings Management **Advanced** Operation Mode



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

IV-5-1. LED Settings

> LED Settings

The access point's LEDs can be manually enabled or disabled according to your preference.

LED Settings	
Power LED	<input checked="" type="radio"/> On <input type="radio"/> Off
Diag LED	<input checked="" type="radio"/> On <input type="radio"/> Off

Power LED	Select on or off.
Diag LED	Select on or off.

IV-5-2. Update Firmware

> Update 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.

Firmware Location

Update firmware from

a file on your PC
 a file on an attached USB device (No USB device connected.)

Update firmware from PC

Firmware Update File

Browse...

Update



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

Update Firmware From	Select to upload firmware from your local computer or from an attached USB device.
Firmware Update File	Click “Browse” to open a new window to locate and select the firmware file in your computer.
Update	Click “Update” to upload the specified firmware file to your access point.

IV-5-3. Save/Restore Settings

> Save/Restore Settings

The access point's "Save/Restore Settings" page enables you to save/backup the access point's current settings as a file to your local computer or a USB device attached to the access point, and restore the access point to previously saved settings.

The screenshot shows a web interface for saving and restoring settings. It is divided into three main sections:

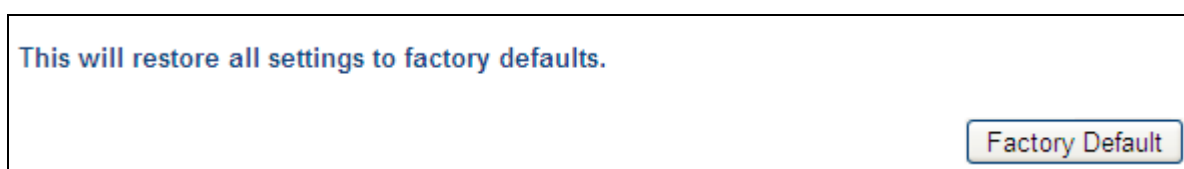
- Save/Restore Method:** Contains two radio buttons. "Using your PC" is selected with a green dot. "Using your USB device (No USB device connected.)" is unselected.
- Save Settings to PC:** Contains a "Save Settings" label, a checkbox for "Encrypt the configuration file with a password." (unchecked), and an empty text input field. Below this is a "Save" button.
- Restore Settings from PC:** Contains a "Restore Settings" label, a text input field with a "Browse..." button next to it, a checkbox for "Open file with password." (unchecked), and another empty text input field. Below this is a "Restore" button.

Using Device	Select to save the access point's settings to your local computer or to an attached USB device.
Save Settings	Click "Save" to save settings and a new window will open to specify a location to save the settings file. If saving settings to your computer, you can also check the "Encrypt the configuration file with a password" box and enter a password to protect the file in the field underneath, if you wish.

Restore Settings	Click the browse button to find a previously saved settings file and then click “Restore” to replace your current settings. If your settings file is encrypted with a password, check the “Open file with password” box and enter the password in the field underneath.
-------------------------	---

IV-5-4. Factory Default

> Factory Default If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **IV-5.5**) or reset the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the location of the access point is not convenient to access the reset button.



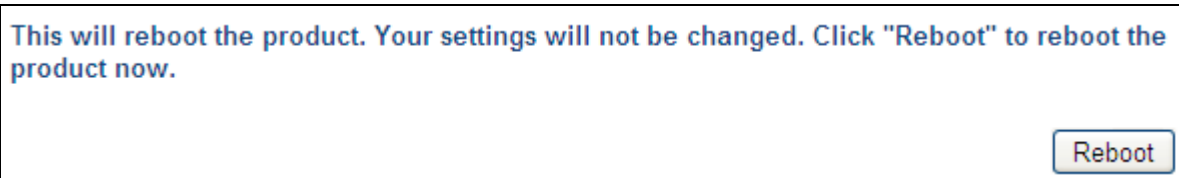
Factory Default	Click “Factory Default” to restore settings to the factory default. A pop-up window will appear and ask you to confirm.
------------------------	---



After resetting to factory defaults, please wait for the access point to reset and restart.

IV-5-5. Reboot

> Reboot If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings (see **IV-5-4**). You can reboot the access point remotely using this feature.



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

IV-5-6. Operation

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings (see **IV-5-4**). You can reboot the access point remotely using this feature.

V. Appendix

V-1. Configuring your IP address

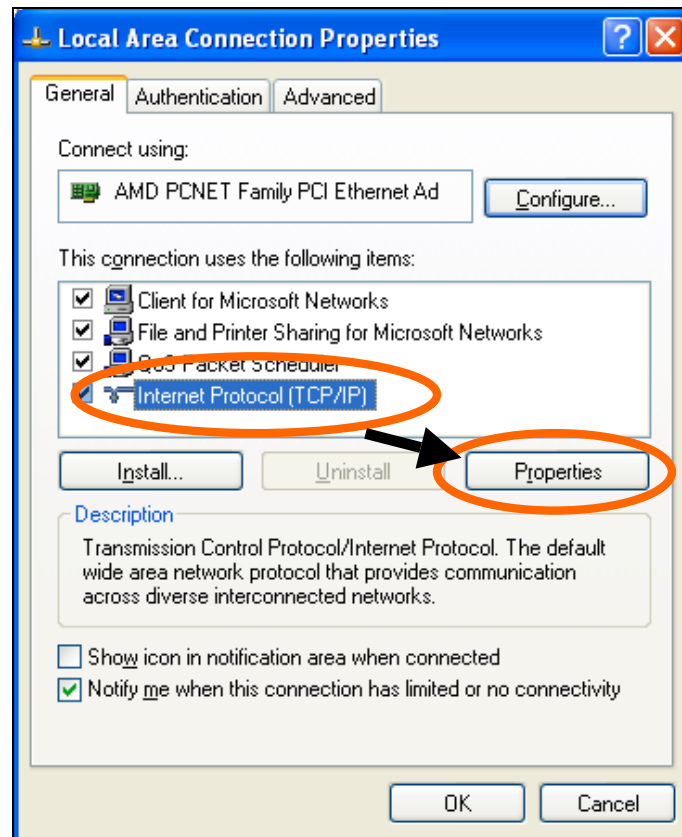
The access point uses the default IP address **192.168.2.2**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254)**.

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)**.

V-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”.

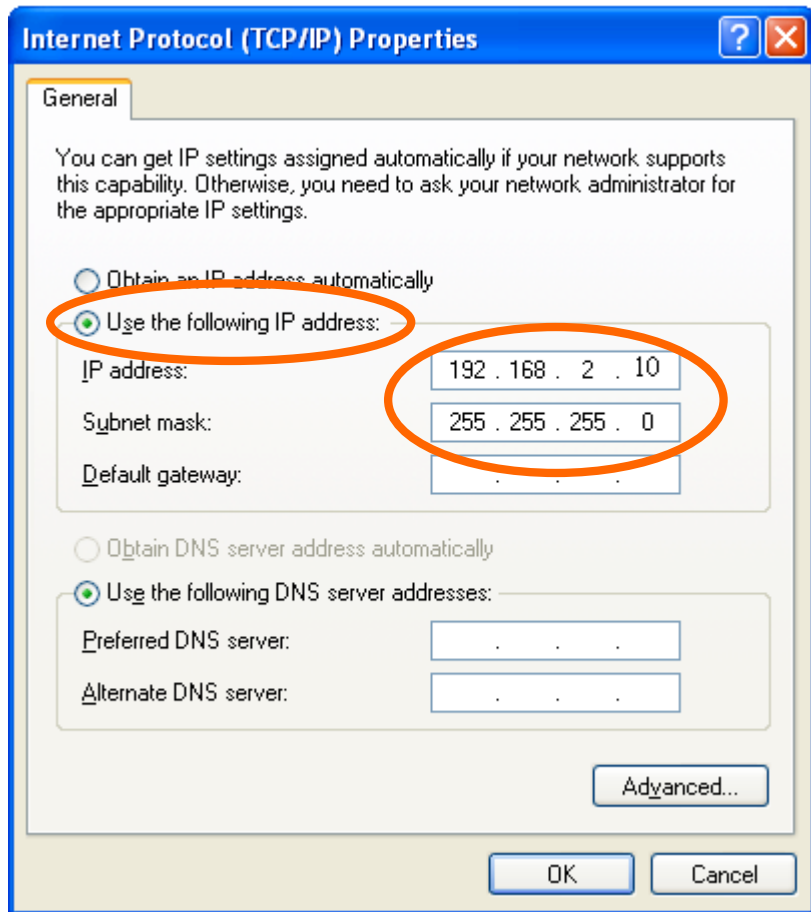


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

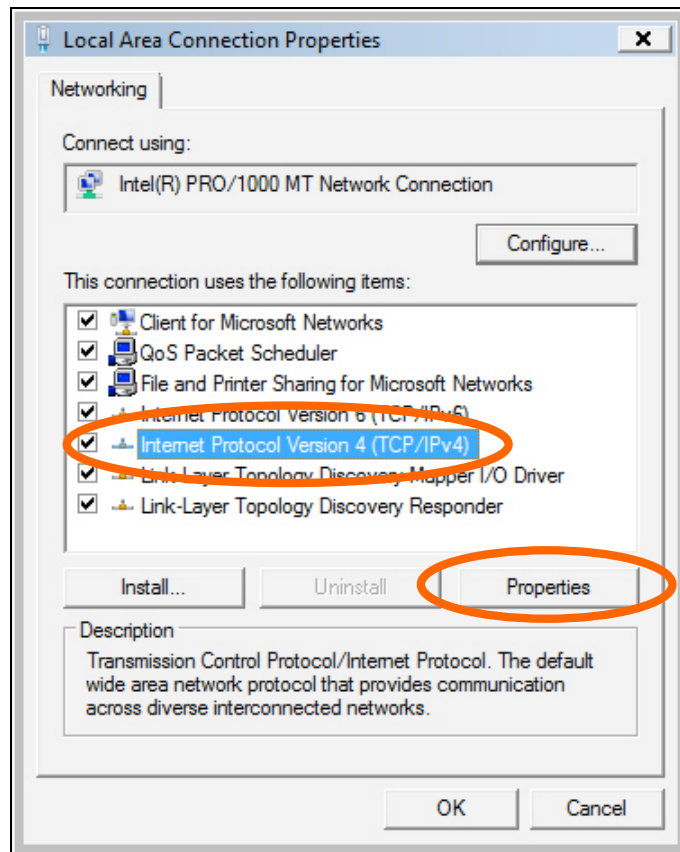
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



V-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”.

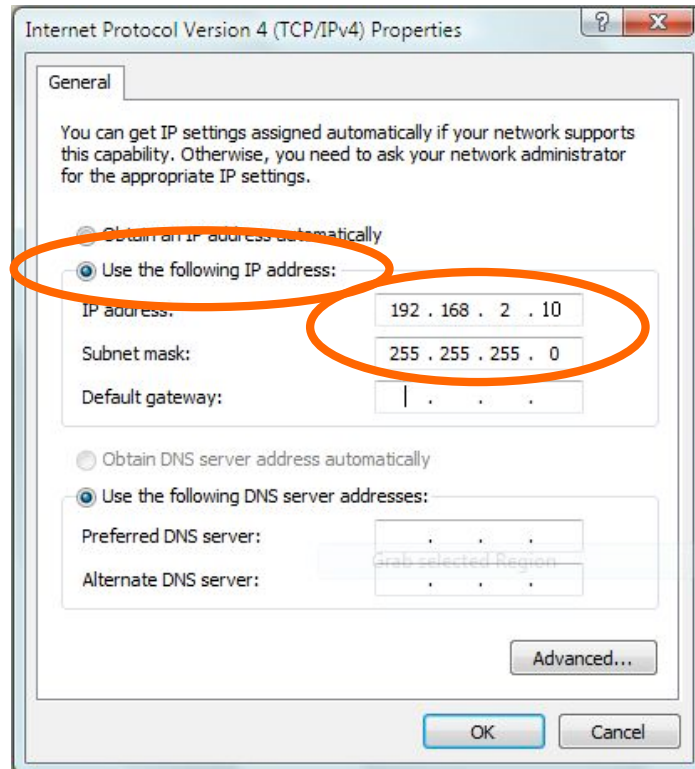


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

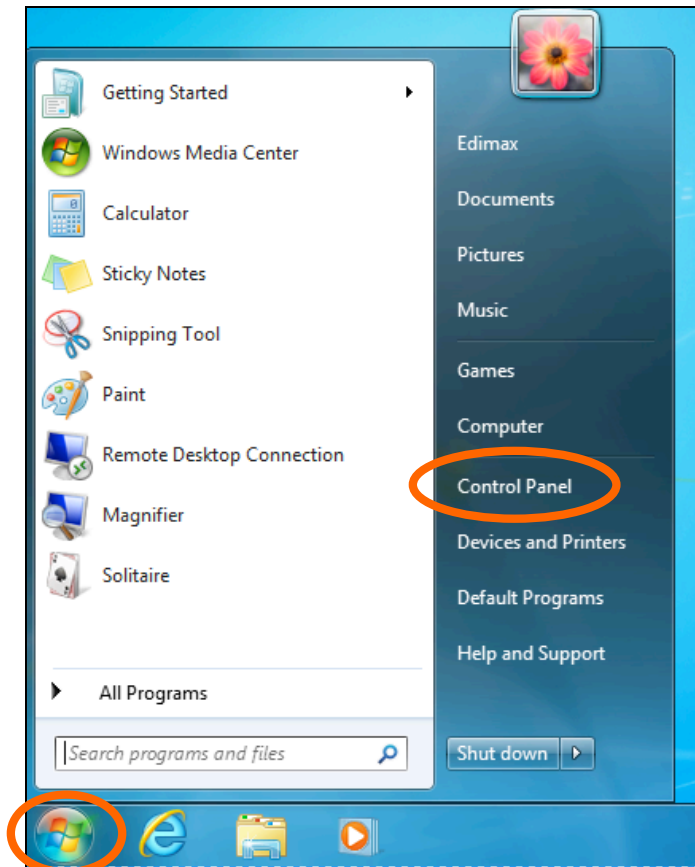
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

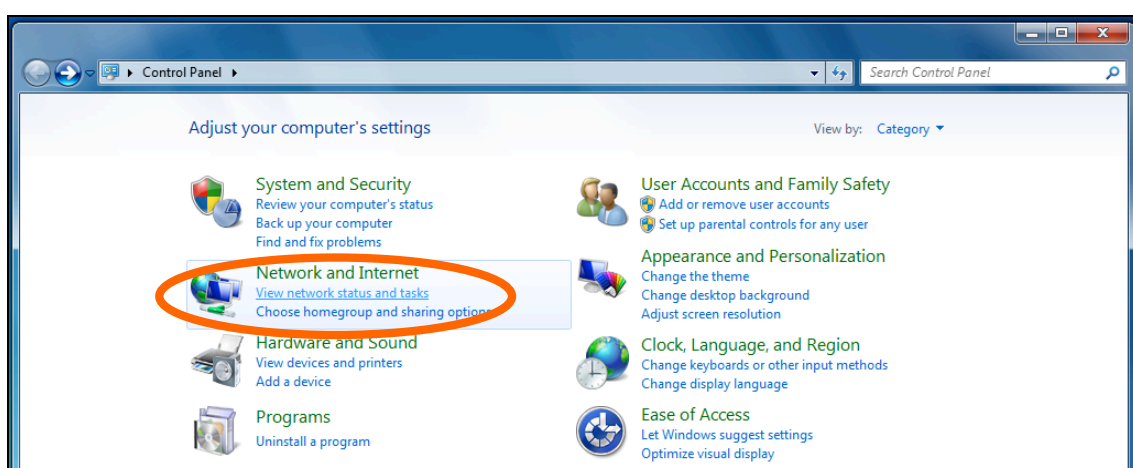


V-1-3. Windows 7

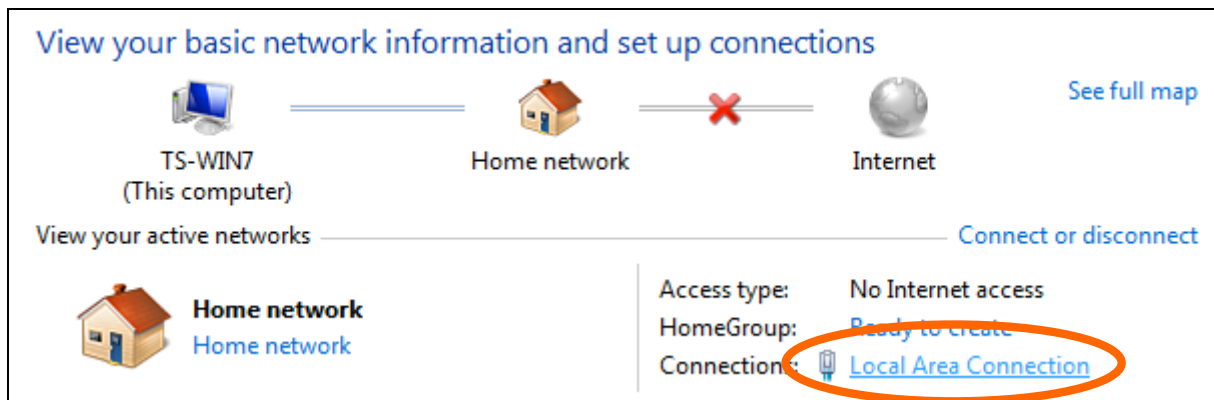
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



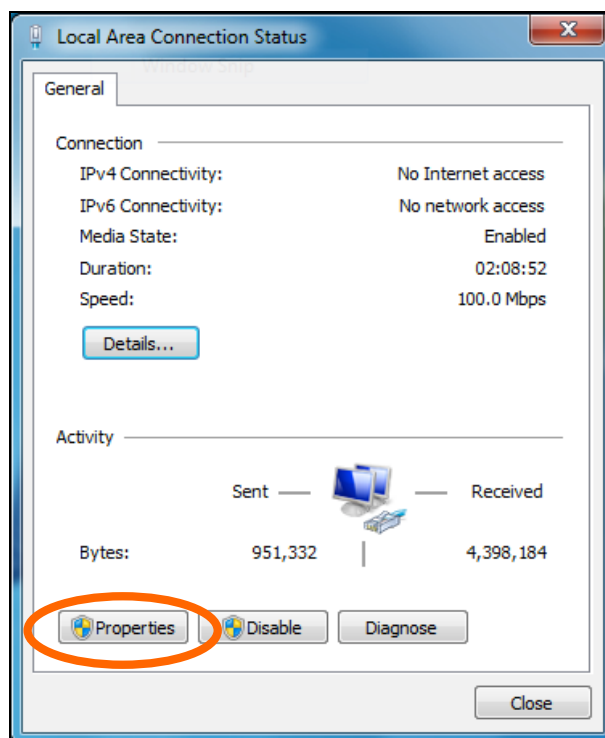
2. Under “Network and Internet” click “View network status and tasks”.



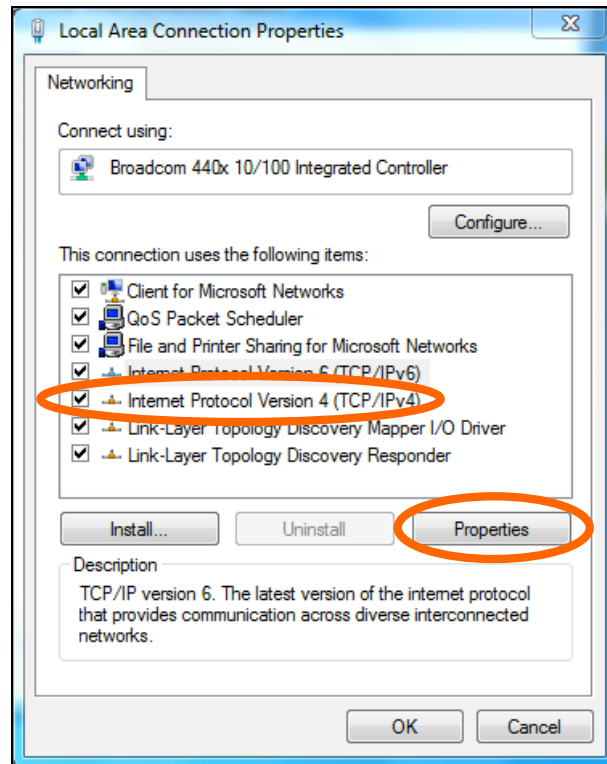
3. Click “Local Area Connection”.



4. Click “Properties”.



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

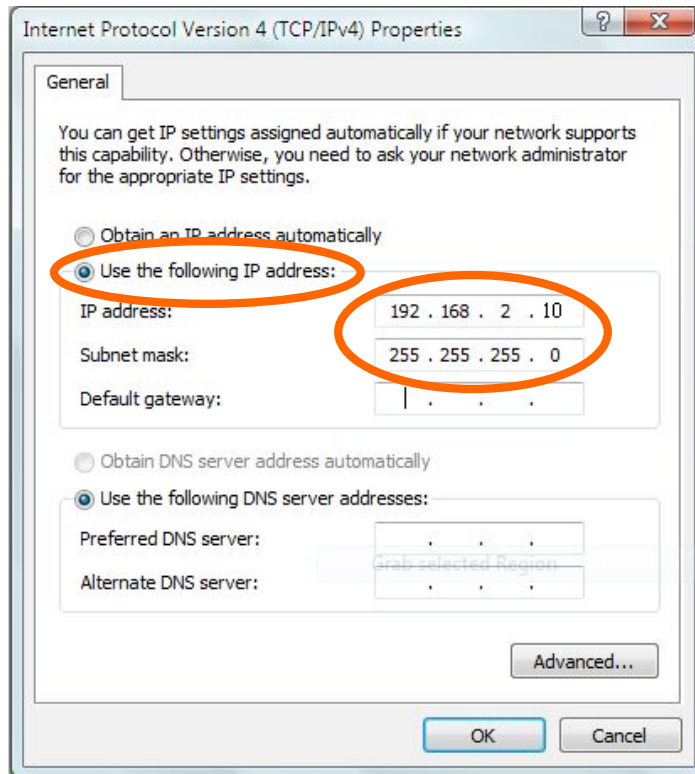


6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

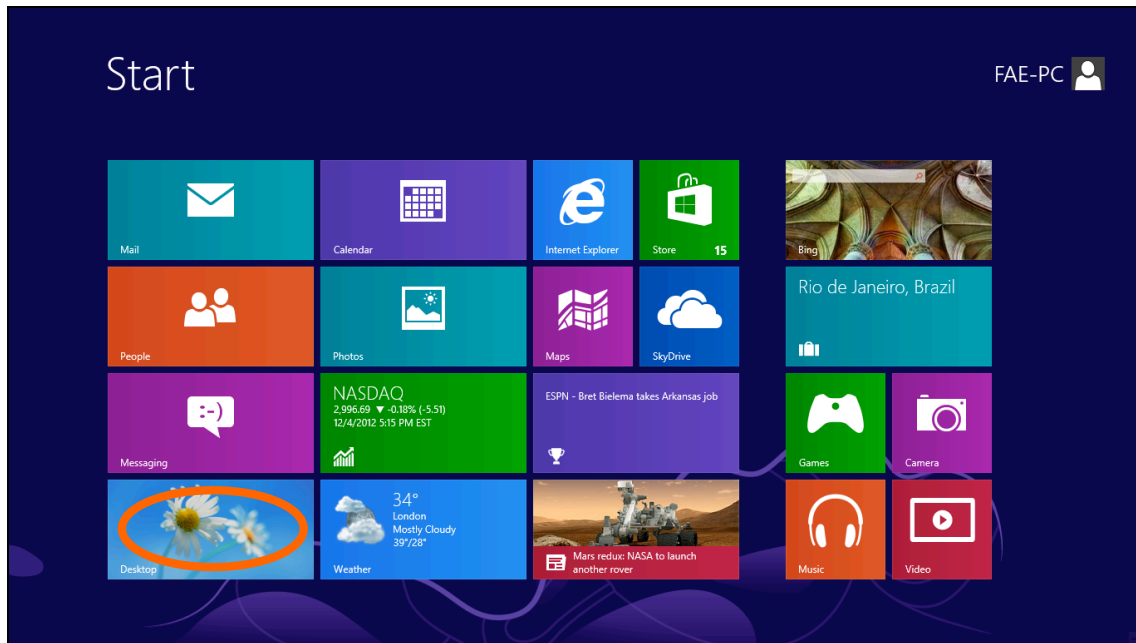
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

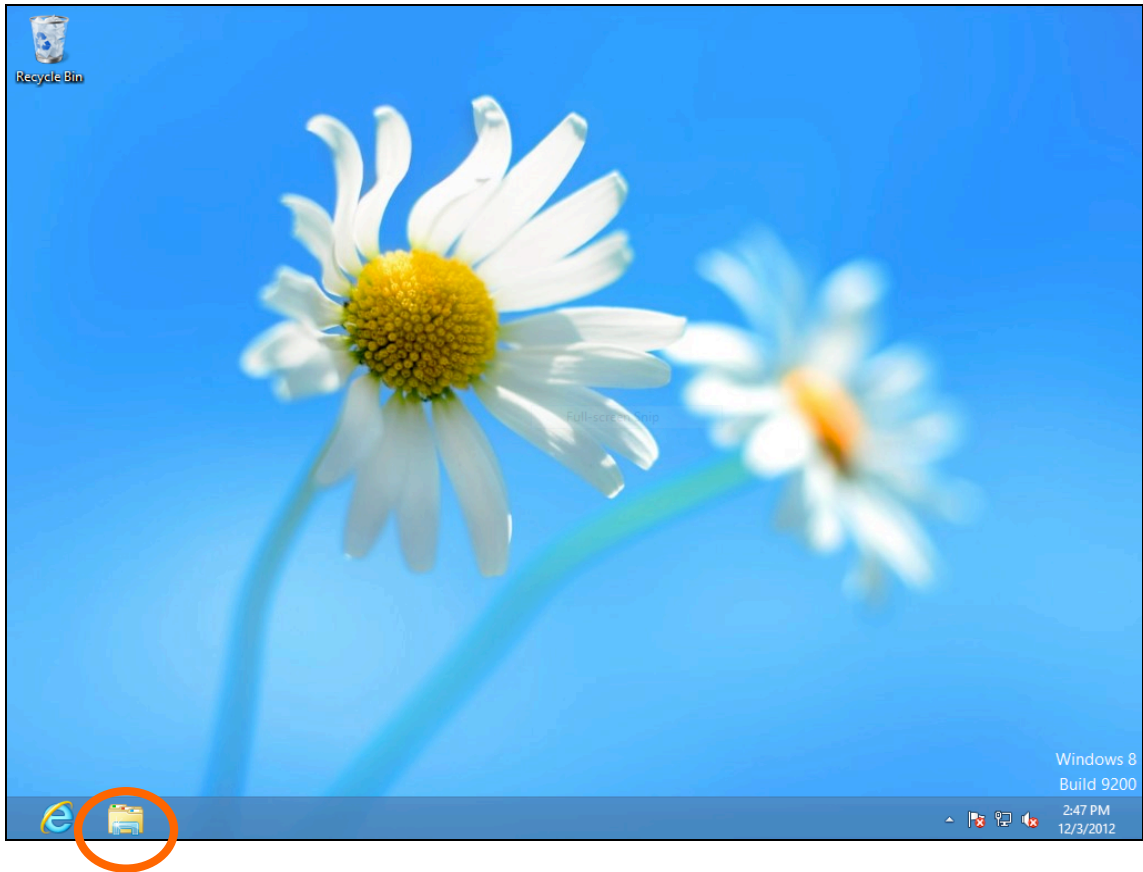


V-1-4. Windows 8

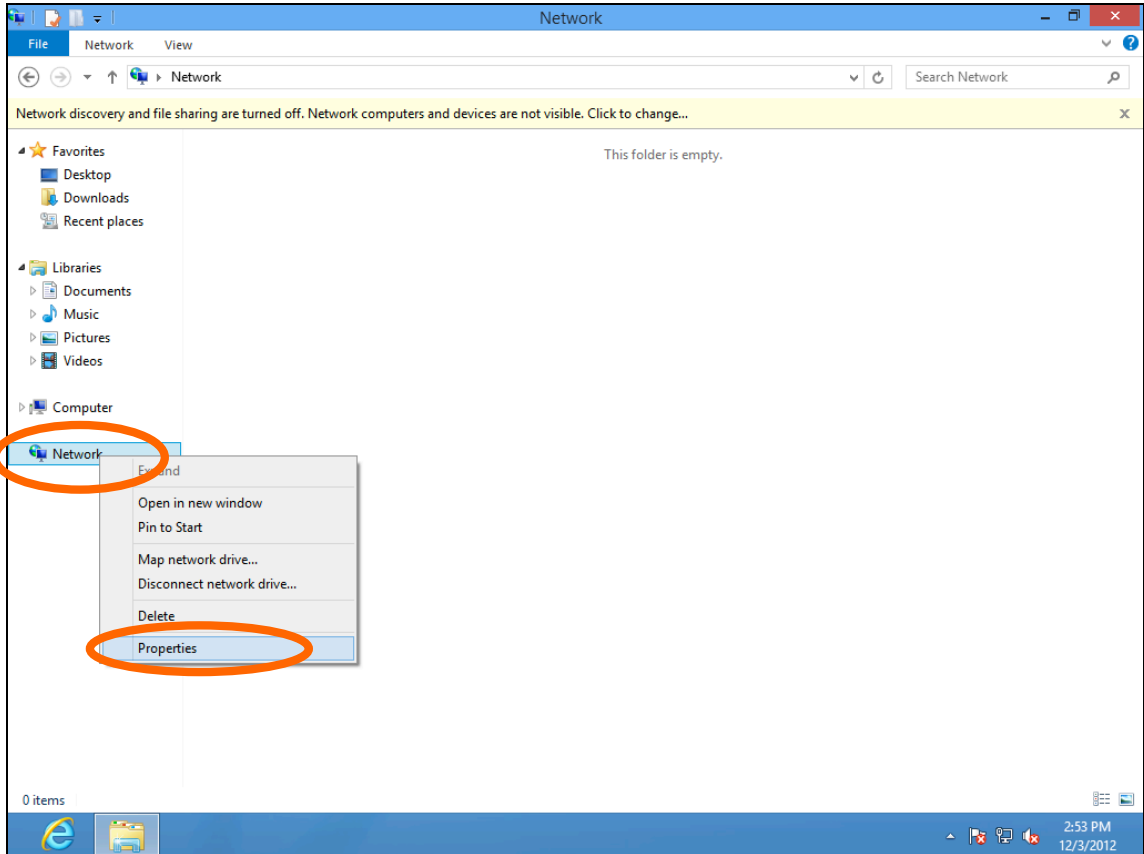
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your cursor to the bottom left of the screen and click.



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

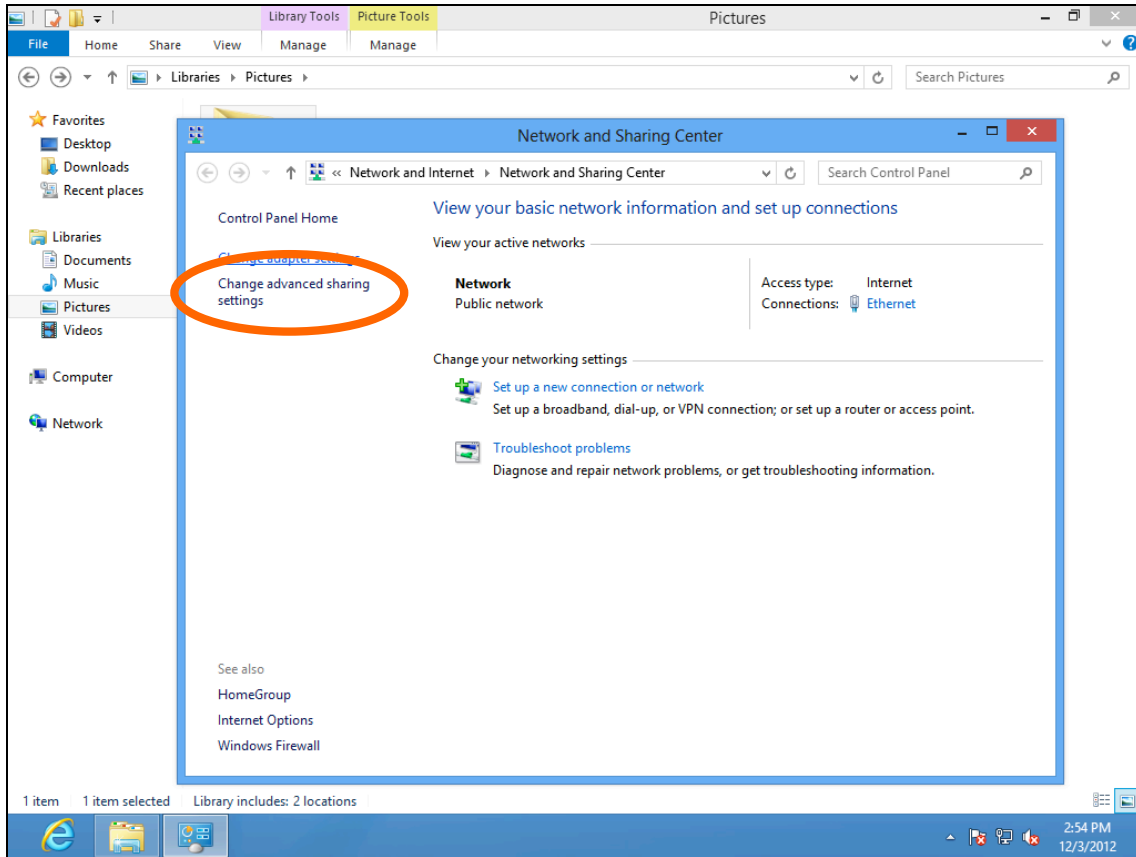


3. Right click “Network” and then select “Properties”.

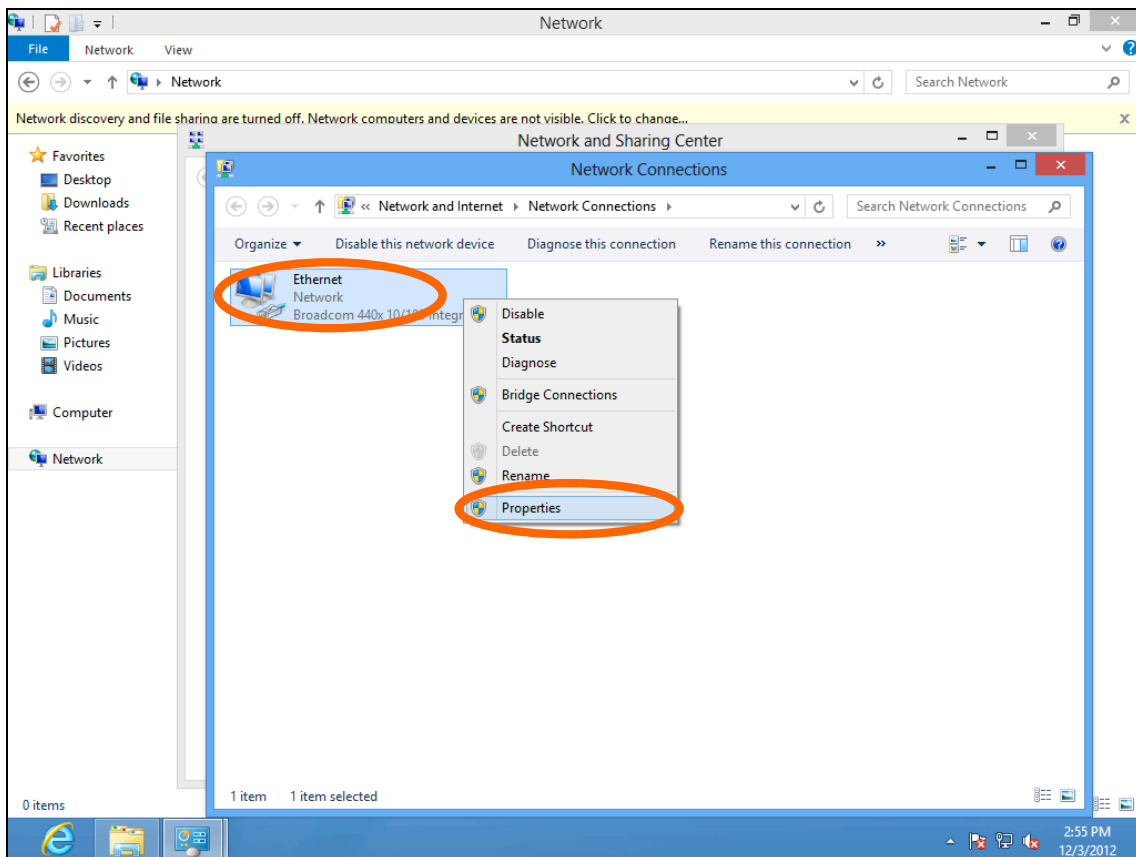


4. In the window that opens, select “Change adapter settings” from the left side.

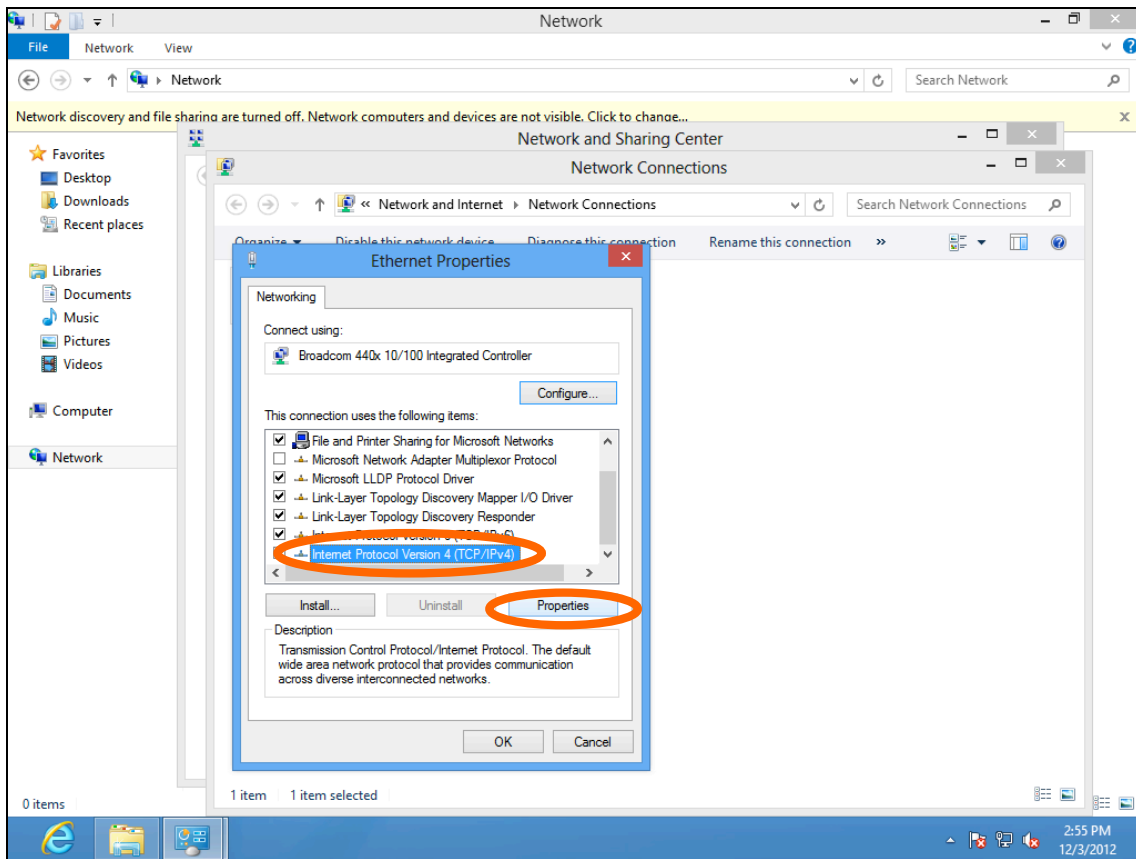
5.



6. Choose your connection and right click, then select "Properties".



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



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

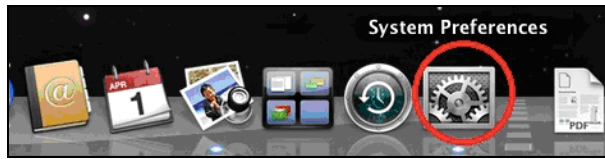
IP address: 192.168.2.10

Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

IV-1-5. Mac

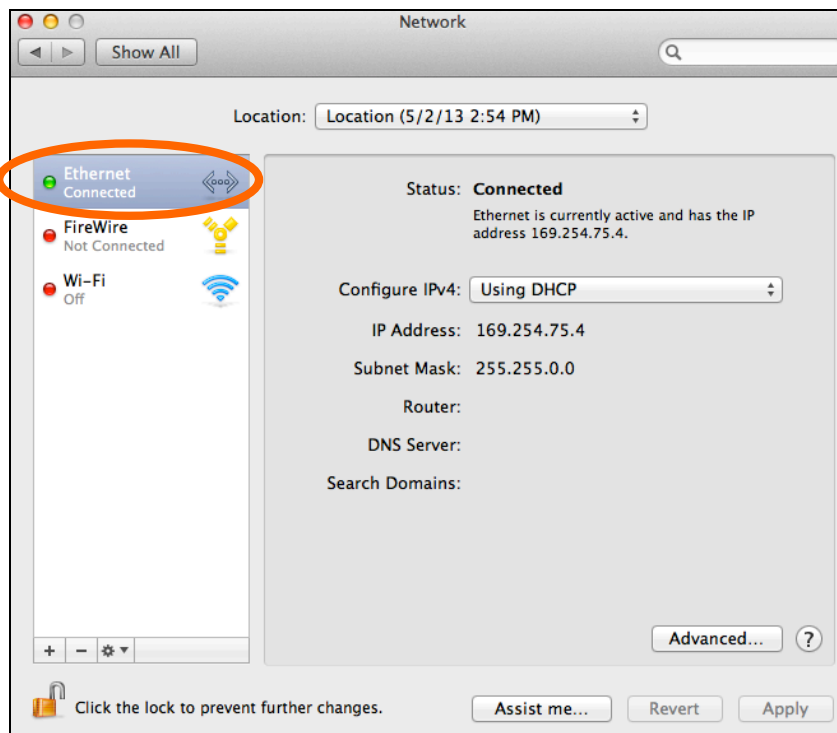
1. Have your Macintosh computer operate as usual, and click on “System Preferences”



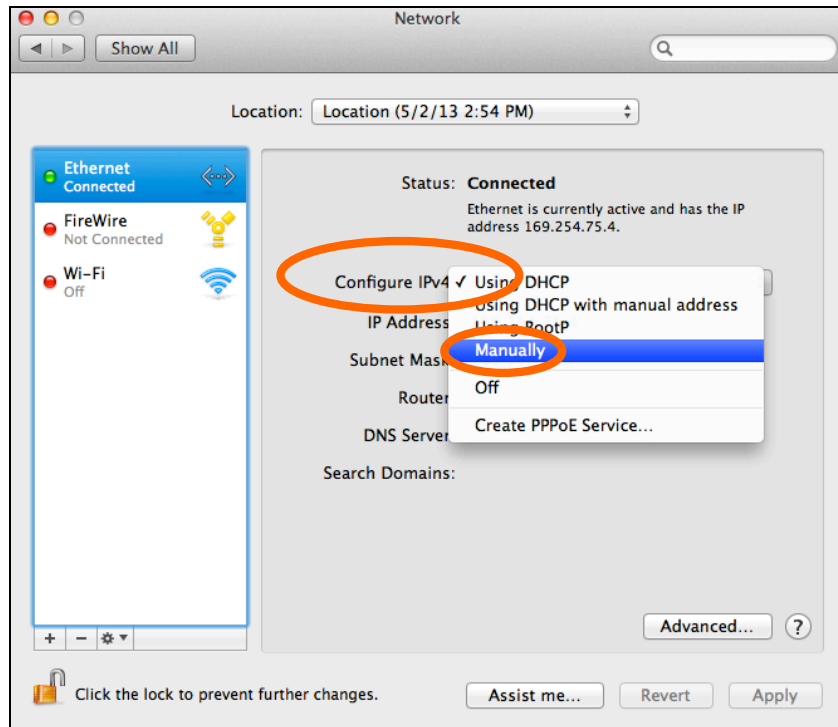
2. In System Preferences, click on “Network”.



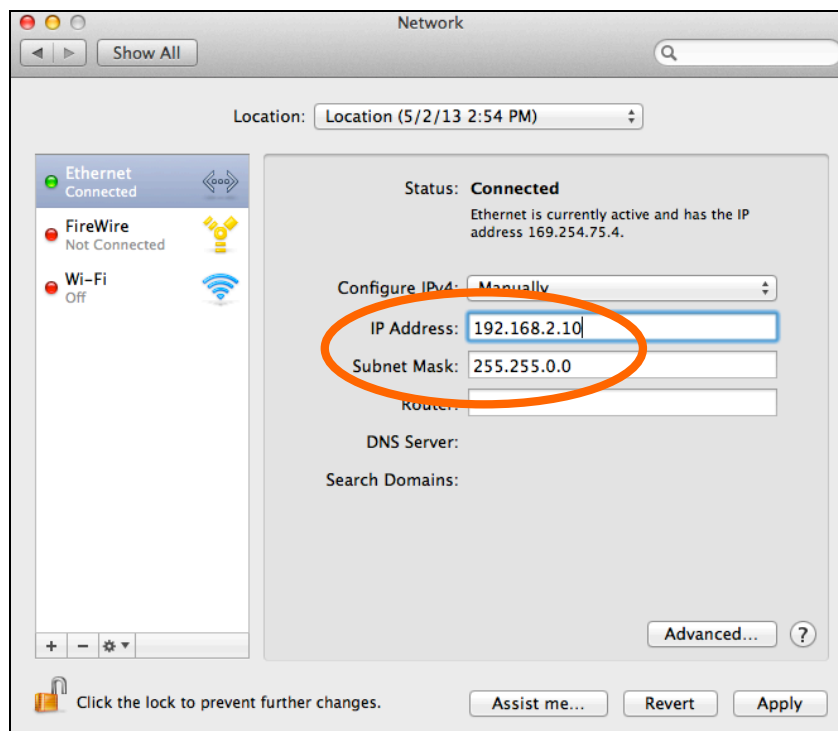
3. Click on “Ethernet” in the left panel.



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



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



V-1-6. 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.Broadbandaccesspoint.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "`Broadbandaccesspoint.com`" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

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

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 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: An access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

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

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

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

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