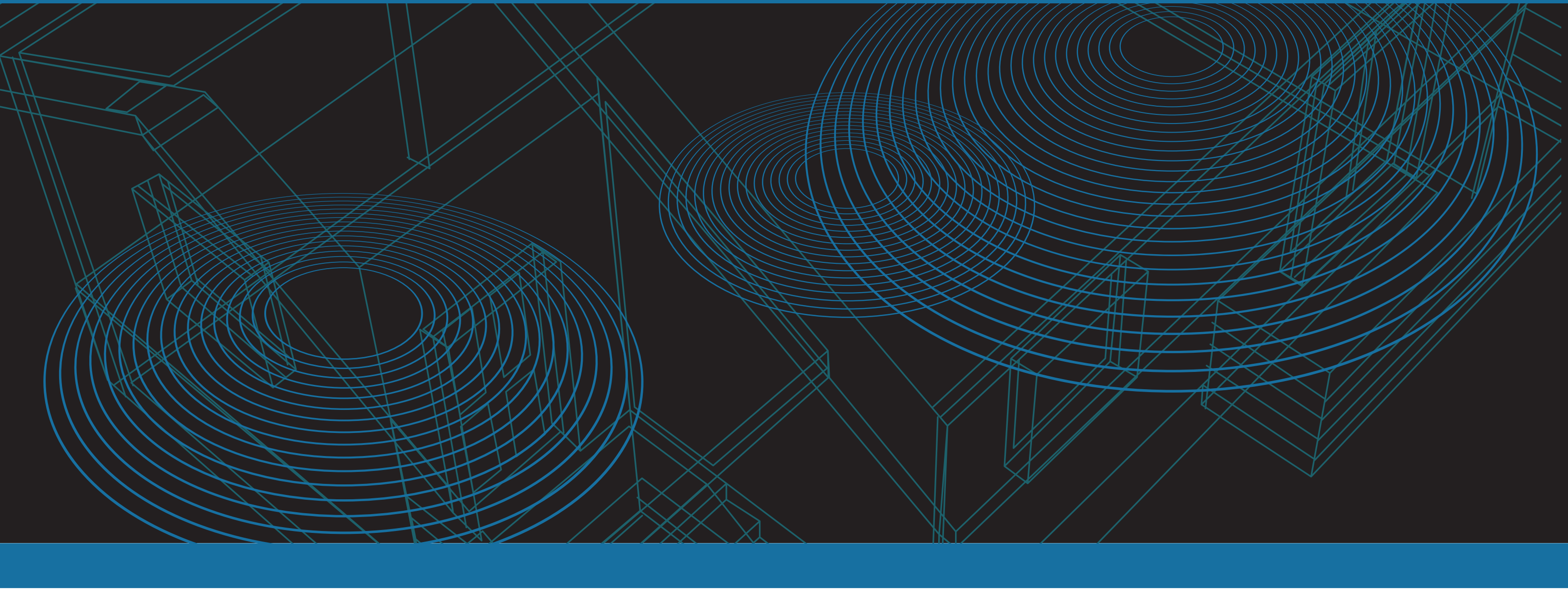
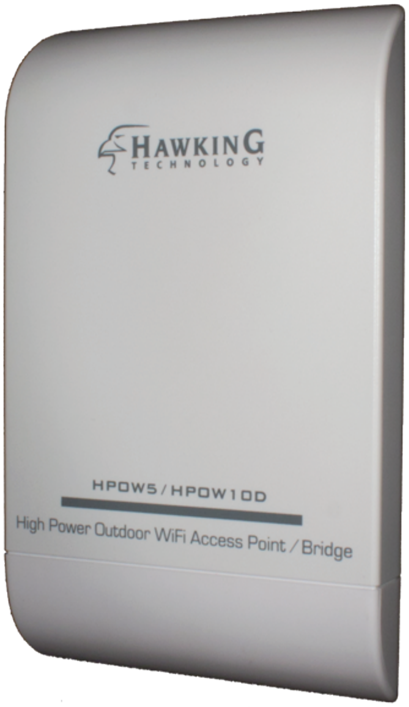
HAWKING®
TECHNOLOGY

High Power Outdoor WiFi Access Point/Bridge

HPOW5/HPOW10D





website www.hawkingtech.com
e-mail techsupport@hawkingtech.com

USER'S MANUAL ▶▶

COPYRIGHT

LIMITED WARRANTY

Hawking Technology guarantees that every HPOW5 Hawking High Power Outdoor WiFi Access Point/Bridge and HPOW10D Hawking High Power Outdoor WiFi Directional Access Point/Bridge is free from physical defects in material and workmanship under normal use for one (1) year from the date of purchase. If the product proves defective during this one-year warranty period, call Hawking Customer Service in order to obtain a Return Authorization number. Warranty is for repair or replacement only. Hawking Technology does not issue any refunds. BE SURE TO HAVE YOUR PROOF OF PURCHASE. RETURN REQUESTS CAN NOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization number clearly on the outside of the package and include your original proof of purchase.

IN NO EVENT SHALL HAWKING TECHNOLOGY'S LIABILTY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE OR ITS DOCUMENTATION. Hawking Technology makes no warranty or representation, expressed, implied or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Hawking Technology reserves the right to revise or updates its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to: techsupport@hawkingtech.com

Federal Communication Commission

Interference Statement

FCC Part 15

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

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

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person’s body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Table of Contents

Chapter I: Product Information

1-1 Introduction

Thank you for purchasing the HPOW5/HPOW10D Hawking High Power Outdoor WiFi Access Point/Bridge. This highly efficient access point is the best choice for ***Small office / Home office*** users. It allows computers and network devices to gain wireless access in several modes throughout their network. Easy install procedures allow any computer user to setup a network environment in a very short time.

This access point supports IEEE 802.11b/g/n. Using its internal 5dBi Omnidirectional Antennas (10dBi directional in the HPOW10D model), all computers and wireless-enabled network devices (including PDA, cellular phone, game console, etc.) can connect to this outdoor wireless access point without additional cabling. 802.11N wireless capability also gives you the highest wireless speeds and the 800mW high power gives you the greatest range and flexibility.

Other features of the HPOW5/HPOW10D include:

- Supports 2.4GHz wireless standard
- Provides IEEE 802.11b/g/n wireless
- 800mW max 2.4GHz wireless transmission power
- 2x 5dBi Omnidirectional Antennas (HPOW5) or 2x 10dBi Directional Antennas (HPOW10D)
- 6 different Wireless Modes: Access Point, Router, WDS, Wireless Client, AP Repeater, WISP Client Router
- IEEE 802.11N 2T/2R, Bandwidth up to 300Mbps (Tx and Rx)
- Supports 802.1X, 64/128-bit WEP, WPA, and WPA2 wireless data encryption.
- QoS & WMM
- Integrated Dual Ethernet – 2x 10/100Mbps Ethernet Ports - Power over Ethernet (PoE) & PoE Passthrough
- Multiple Virtual AP
- Business Class WLAN Security and Client Authentication
- Web Management and SNMP MIB II
- Client Isolation through Layer 2 VLAN
- Bandwidth traffic Shaping

Networking

- Support Static IP, Dynamic IP(DHCP Client) and PPPoE on WiFi WAN Connection
- Support MPPE-64 and MPPE-128 Encryption on PPTP Connection
- PPPoE and PPTP Reconnect – Always On , On demand, Manual
- Support PPTP/L2TP Pass Through
- MAC Cloning
- DHCP Server
- 802.3 Bridging
- NAT
- Proxy DNS
- Dynamic DNS
- NTP Client

- DMZ
- Virtual Server (Port Forwarding)
- Support MAC Filter
- Support IP Filter
- Support Layer-7 Protocol Filter and Content Filter
- Support Static Routing
- Support RIP and OSPF Dynamic Routing
- Bandwidth traffic Shaping

Wireless Feature

- Transmission power control : 3%, 6%, 12.5%, 25%, 50%, 100%
- Channel selection : Manual or Auto
- Associated clients limitation : 64
- No. of ESSID (Virtual AP): 8
- No. of Max. WDS setting: 8
- Preamble setting: Short/ Long
- Setting for 802.11b only, 802.11b/g mix, 802.11b/g/n mix or 802.11n only
- Setting for transmission speed
- Dynamic Wireless re-transmission
- IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- IEEE 802.11i Preauth (PMKSA Cache)
- IEEE 802.11d -Multi country roaming
- Wireless Site Survey
- Channel Bandwidth setting : 20MHz or 20/40MHz
- HT Tx/Rx Stream selection : 1 or 2
- A-MSDU and A-MPDU support
- Maximal MPDU density for TX aggregation setting
- Short Slot support
- RTS Threshold and Fragment Threshold support
- IGMP Snooping v1, v2 and v3

Authentication/ Encryption (Wireless Security)

- Layer2 User Isolation
- Blocks client to client discovery within a specified VLAN
- WEP 64/ 128 /152 Bits
- EAP-TLS + Dynamic WEP
- EAP-TTLS + Dynamic WEP
- PEAP/ MS-PEAP+Dynamic WEP
- WPA (PSK +TKIP)
- WPA (802.1x certification + TKIP)
- 802.11i WPA2 (PSK + CCMP/ AES)
- 802.11i WPA2 (802.1x certification + CCMP/ AES)
- Setting for TKIP/ CCMP/ AES key’s refreshing period
- Hidden ESSID support
- Setting for “Deny ANY “ connection request
- MAC ACL
- No. of registered RADIUS servers : 2
- VLAN assignment on ESSID
- VLAN tag over WDS

- Support WEP and AES data encryption over WDS link

Quality of Service

- Download and Upload traffic control
- IEEE802.11e WMM

System Administration

- Intuitive Web Management Interface
- Password Protected Access
- Firmware upgrade via Web
- Reset to Factory Defaults
- Profiles Configuration Backup and Restore
- One-button-click to reset factory default
- Two administrator accounts
- Remote Link Test – Display connect statistics
- Full Statistics and Status Reporting
- NTP Time Synchronization
- Even Log
- Support SNMP v1, v2c, v3
- SNMP Traps to a list of IP Address
- Support MIB II
- Ping Watchdog
- CLI access via Telnet and SSH
- Administrative Access : HTTP and HTTPS
- UPnP (Universal Plug and Play)

1-2 Safety Information

In order to keep the safety of users and property, please follow these safety instructions:

1. This access point is designed for outdoor use and is weather resistant.

2. DO NOT put this access point at or near hot or humid places, like kitchens or bathrooms. Also, do not leave this access point in the car in summer.

3. DO NOT pull any connected cable with force; disconnect them from the access point first.

4. If you want to place this access point in a high place or hang on the wall, please make sure the access point is firmly secured. Falling can damage the access point and its accessories and the warranty will be void.

5. Accessories of this access point, like antennas and power supply, are a danger to small children under 3 years old. KEEP THIS ACCESS POINT OUT OF THE REACH OF CHILDREN!

6. The access point will become warm when used for a long period of time (***This is normal and is not a malfunction).*** DO NOT put this access point on paper, cloth, or other flammable materials.

7. There are no user-serviceable parts inside the access point. If you have found that the access point is not working properly, please contact technical support or your place of purchase and ask for help. DO NOT disassemble the access point, or warranty will be void.

8. If the access point falls into water when it's powered on, DO NOT use your hands to pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.

9. If you smell something strange, or see smoke coming out from the access point or power supply, remove the power supply or switch the electrical power off immediately, and call techsupport or your place of purchase for help.

1-3 System Requirements

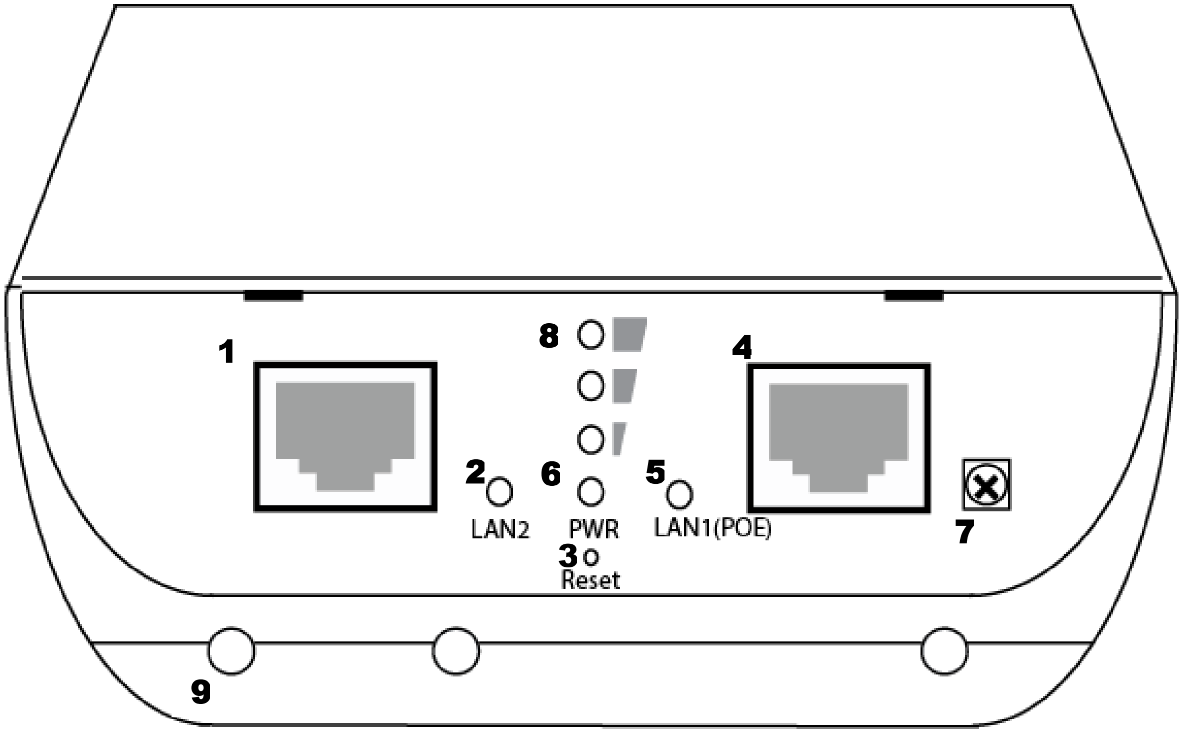
- One computer (Mac or PC).
- Internet Web Browser (Internet Explorer, Safari, etc.)
- A Wired or Wireless network adapter (e.g. Airport card, built-in Ethernet adapter, etc.)

1-4 Package Contents

Before you start to use this access point, please check if there's anything missing in the package, and contact your place of purchase or contact Hawking Technologies.

- 1x HPOW5/HPOW10D
- 1x RJ45 Cable
- 1x Power Adapter (Power Supply)
- 1x Power Over Ethernet (PoE) Adapter
- 1x Wall Mounting Kit
- 2x Cable Ties for Stand/Pole mounting
- 1x Setup CD (includes Manual/QIG)
- 1x Quick Installation Guide (QIG)

1-5 Product Overview



(1) LAN2's Ethernet port
(2) LED Indicator for LAN2

(3) Reset Button. Press and hold the reset button for at least 15 seconds to factory reset the device.

(4) LAN1 (PoE) Ethernet port

(5) LED indicator for LAN1

(6) Power LED

(7) Grounding Connection: Grounding cable can protect this device from lightning strikes and buildup of static electricity. Grounding cable not included in the package. We suggest 16-18 AWG grounding cable.

(8) LED for strong/weak WiFi Signal Indicator for Client Bridge, Repeater AP, WISP + Repeater AP modes

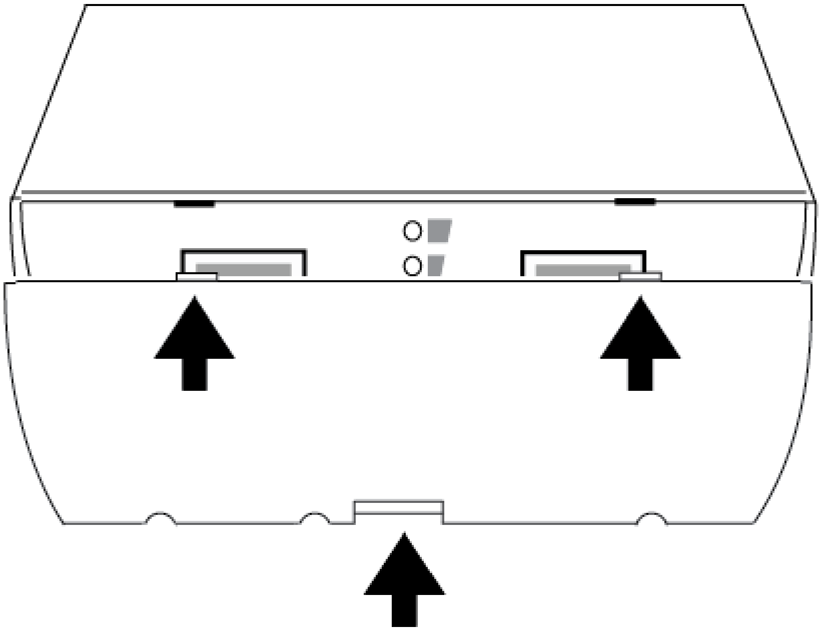
(9) Ethernet cable guide ports. These can be popped out to guide your Ethernet cables out of the device. Guide your Ethernet cables through here so you can close the outside latch.

Chapter II: System and Network Setup

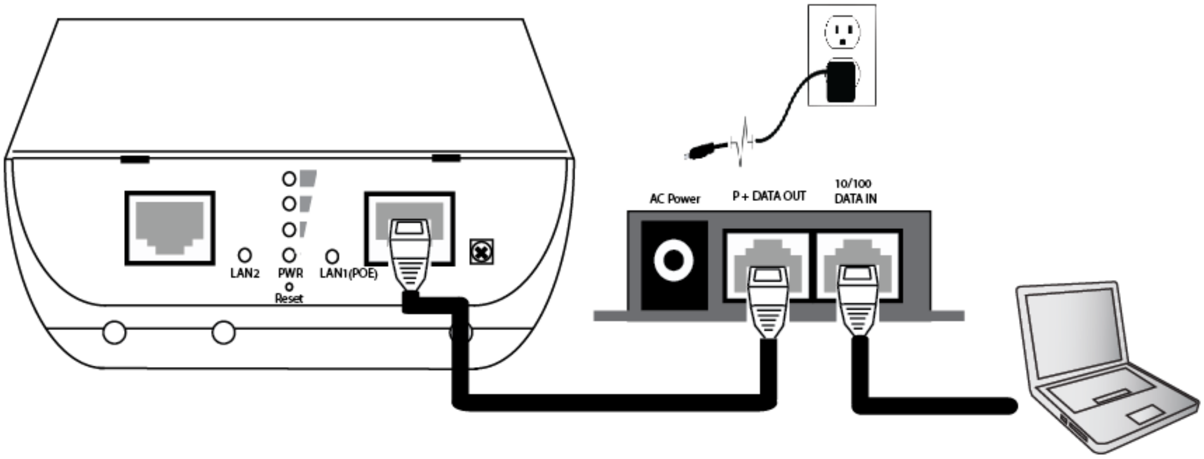
2-1 Build Network Connection

Please follow the following instructions to build the network connection between your new HPOW5/HPOW10D access point and your computers and other network devices:

1. Remove cover from device. Press the center tab (you may need a flathead screwdriver) and the cover should be able to be removed with a small amount of force.



2. Connect the A/C power adapter to the wall socket, and then connect it to the ‘Power’ socket of the PoE injector. Connect a Ethernet cable from the “P + Data Out” port on the PoE injector into the HPOW5/HPOW10D LAN1(POE) Port.
3. Connect your HPOW5/HPOW10D from the “10/100 Data in” on the PoE injector to your computer/network.



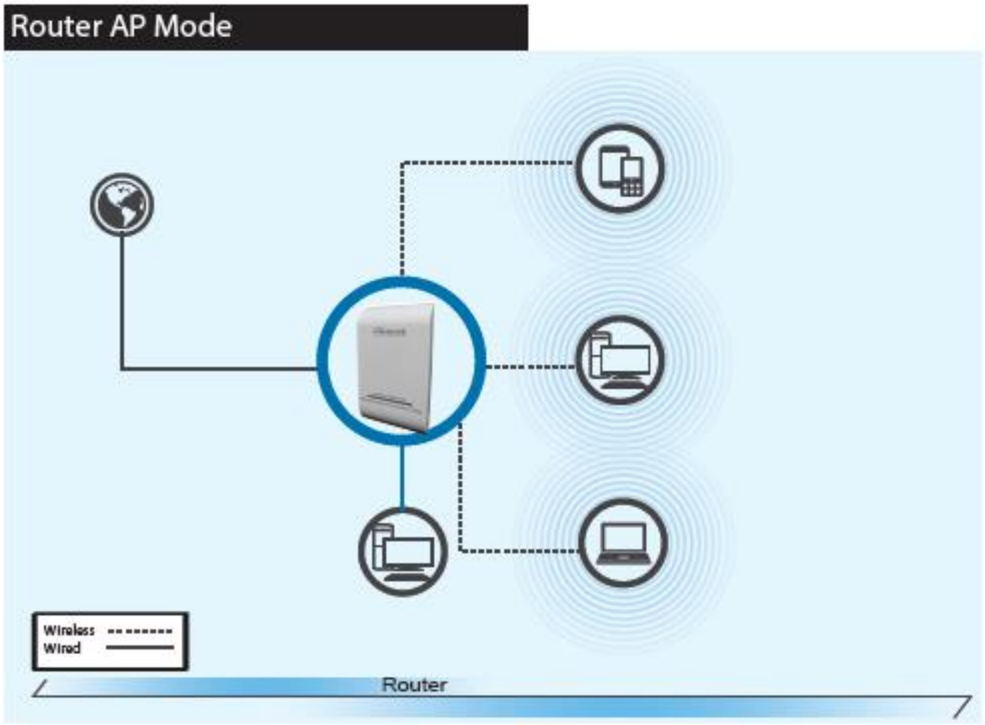
4. Configure the IP Address of your computer to be in the same range as the HPOW5/HPOW10D (see section 2-3)

Log into the setup page to configure the HPOW5/HPOW10D

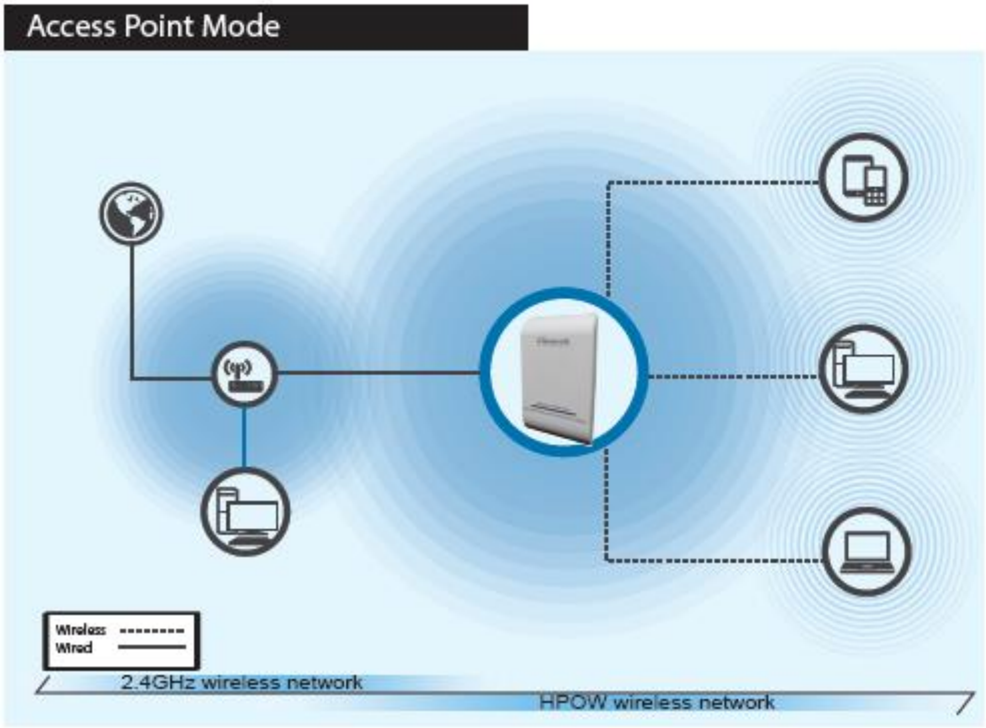
2-2 Definitions of HPOW5/HPOW10D Supported Modes

Modes

The HPOW5/HPOW10D supports 6 different modes.

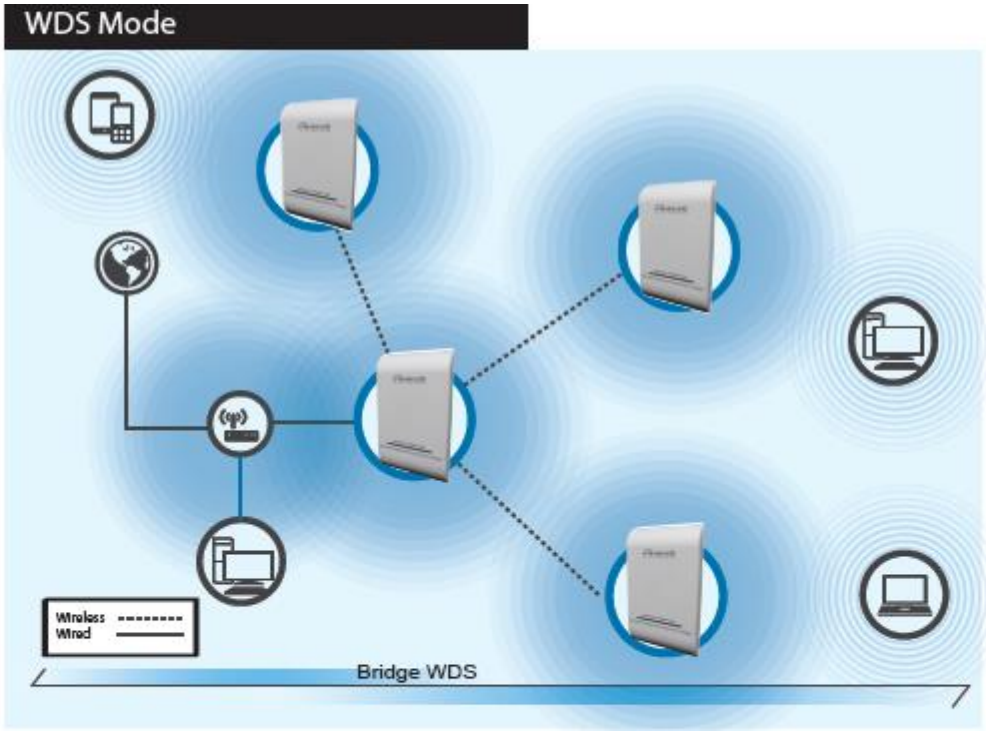


When Router AP mode is chosen, the system can be configured as a Wireless Router. In this mode, the device is supposed to be connected to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN/WLAN port share the same IP to ISP through the WAN port. The connection type can be setup in WAN page by using static IP, Dynamic IP, PPPoE or PPTP client.   Go to section 3-1



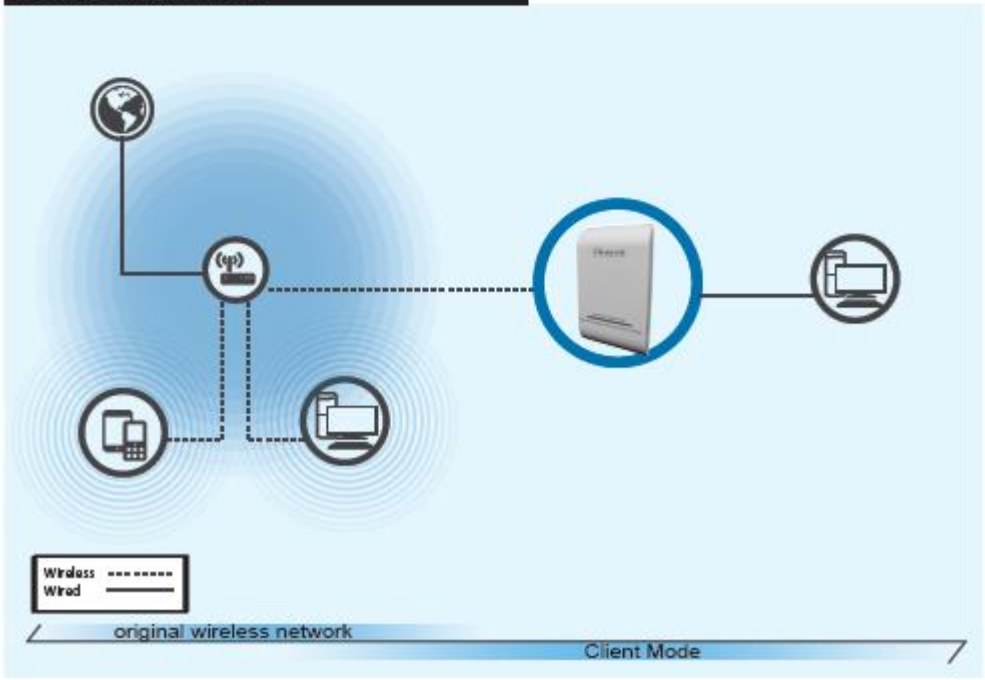
When AP mode is chosen, the system can be configured as a standard wireless access point. In this mode, the device can be used as an Access Point for wireless client connection. All Ethernet ports wand wireless interfaces are bridged together. Go to section 3-2

WDS Mode

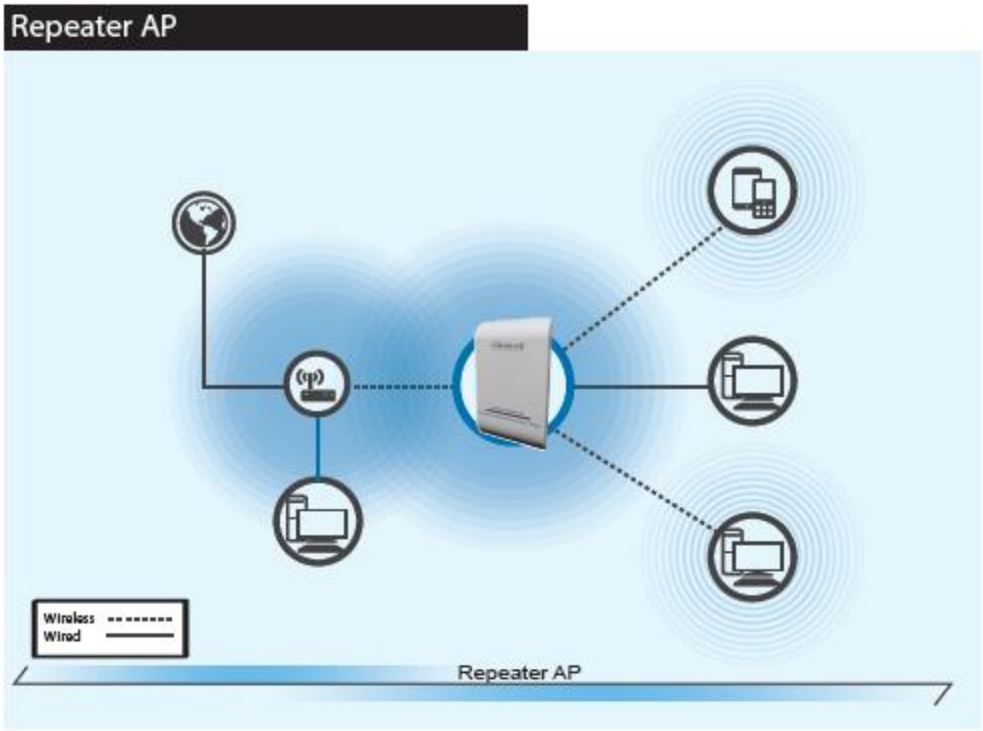


When WDS mode is chosen, the system can be configured in WDS Mode. In this mode, WDS (Wireless Distribution Service, creates a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them. ***We can only guarantee WDS will only work with the HPOW5 and the HPOW10D devices.*** Do not use other devices to set up a WDS network. Go to section 3-3

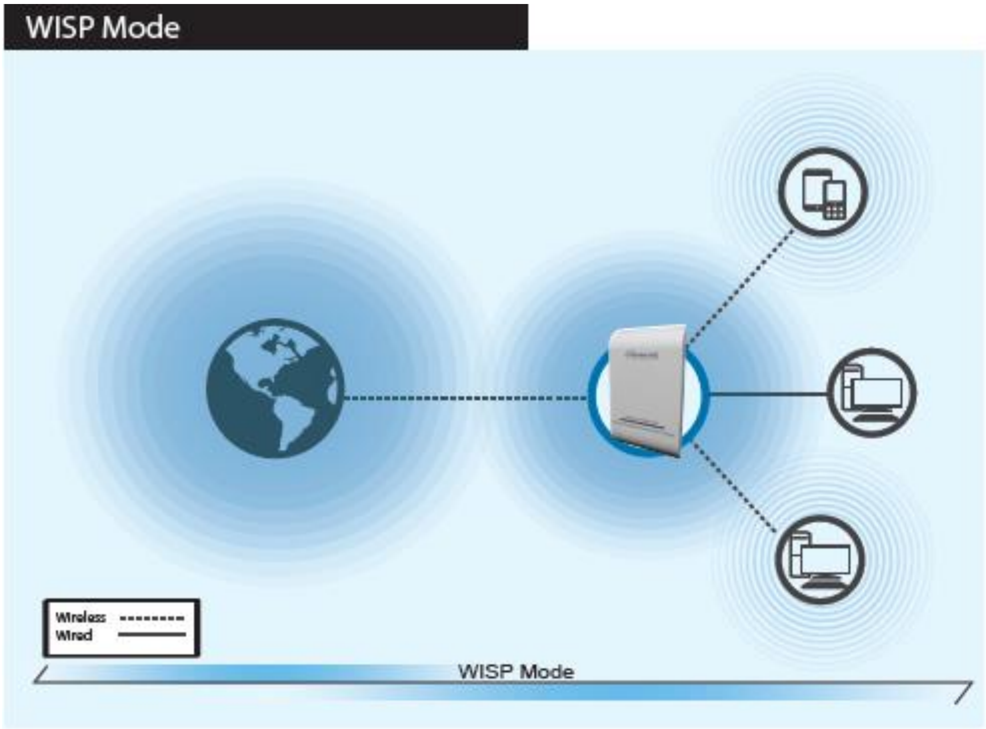
Client Bridge Mode



When Client Bridge + Repeater AP Mode is chosen, the system can be configured in bridged mode. In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network. Go to section 3-4



In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network and work as a wireless repeater for wireless devices. All Ethernet ports and repeater access points are bridged together. Go to section 3-4



When CPE + Repeater AP Mode is chosen, the system can be configured in Wireless repeater mode. In this mode, the device can wirelessly connect to a WISP (wireless internet service provider), ie. Another wireless AP, HotSpot, etc. It can then wirelessly repeat the signal and can even act as a router for these signals. NAT is enabled and wired and wireless computers can share the same IP range. Go to section 3-5

2-3 Connecting to the HPOW5/HPOW10D via Web Browser

After the network connection is built, the next step you should do is setup the access point with proper network parameters, so it can work properly in your network environment.

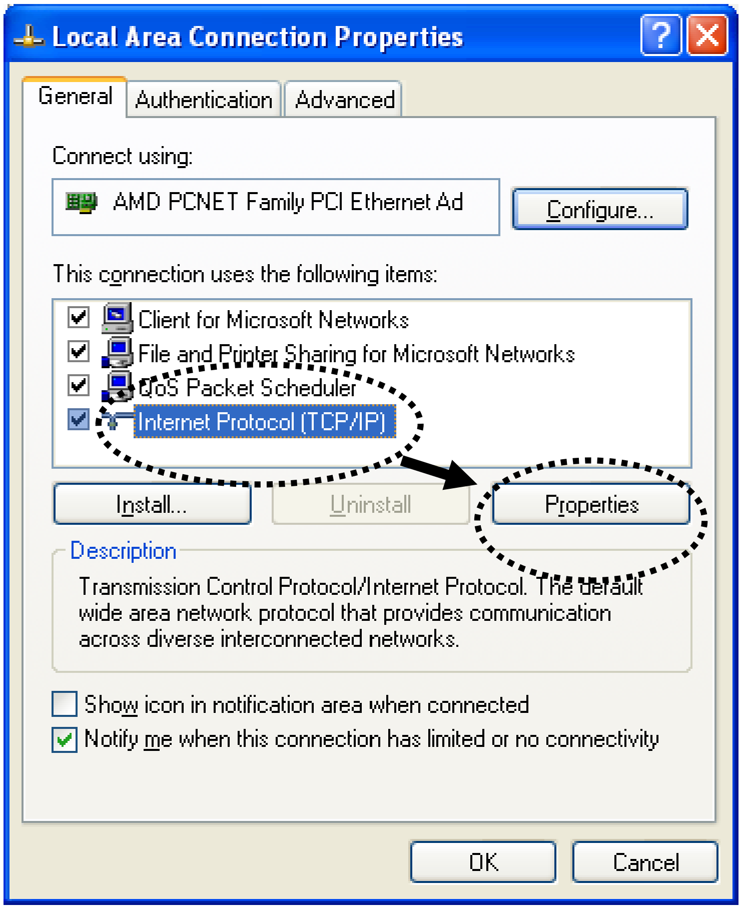
Before you can connect to the access point and start configuration procedures, your computer must be set to static IP. Please follow the following instructions to configure your computer to use a static IP address:

If the operating system of your computer is….

Windows XP	**- please go to section 2-3-1**
Windows Vista/7	**- please go to section 2-3-2**
Mac OS	**- please go to section 2-3-3**

2-3-1 Windows XP IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Double-click ***Network and Internet Connections*** icon, click ***Network Connections,*** and then double-click ***Local Area Connection, Local Area Connection Status*** window will appear, and then click 'Properties'



Connect using: AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

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

Description

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

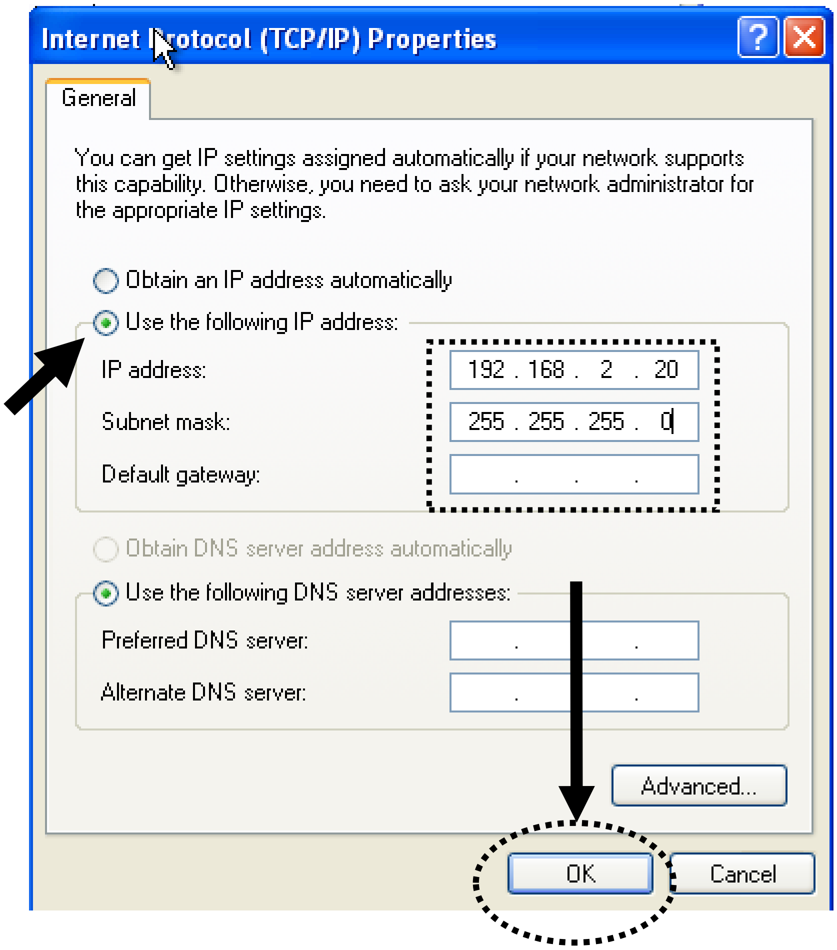
☐ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.20

Subnet Mask: 255.255.255.0



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

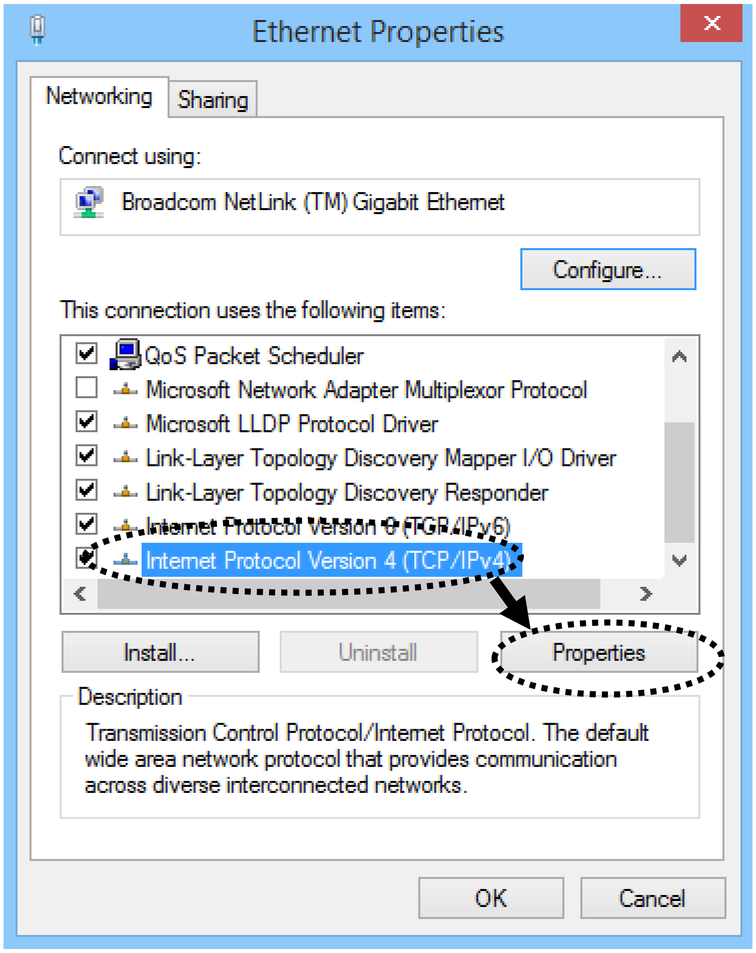
Preferred DNS server: . . .

Alternate DNS server: . . .

click ‘OK’ when finished.

2-3-2 Windows 7/8 IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Click ***View Network Status and Tasks***, then click ***Change Adapter Settings.*** Right-click ***Local Area Network, then select 'Properties'. Local Area Connection Properties*** window will appear, select 'Internet Protocol Version 4 (TCP / IPv4), and then click 'Properties'



Ethernet Properties

Networking | Sharing

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

This connection uses the following items:

- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

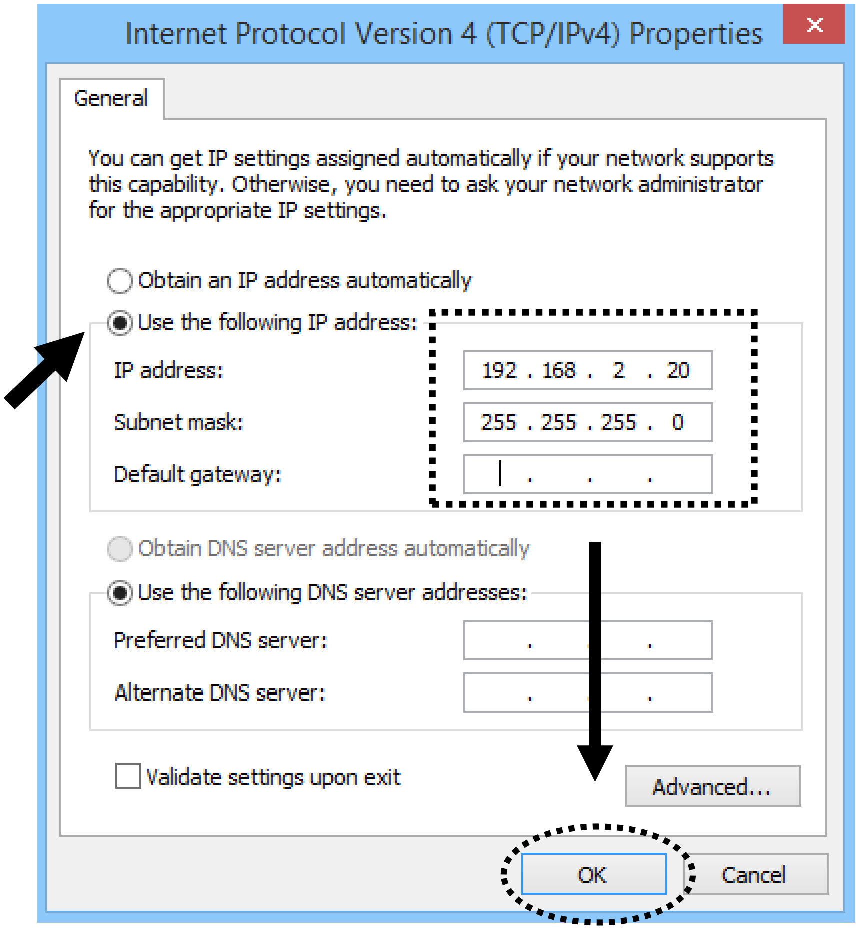
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.20

Subnet Mask: 255.255.255.0

click 'OK' when finish.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

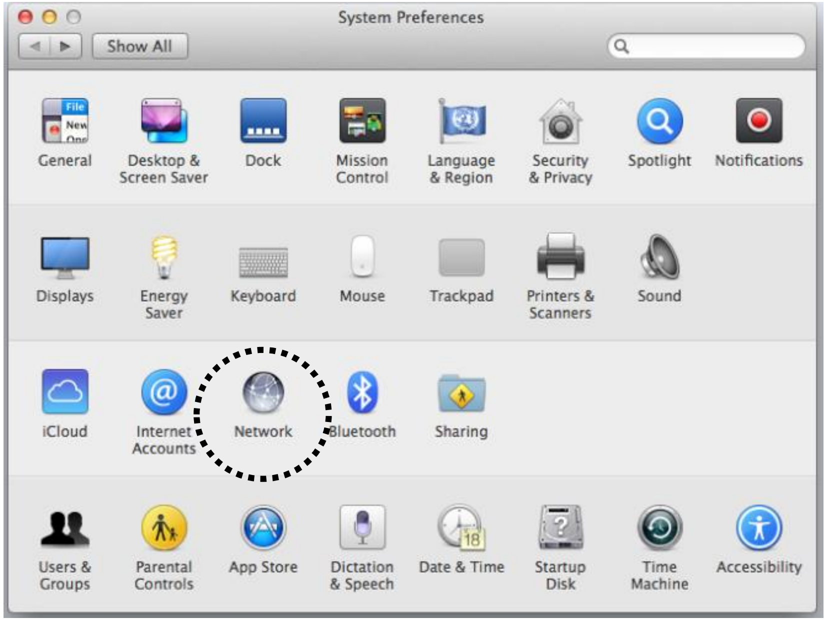
Preferred DNS server: . . .

Alternate DNS server: . . .

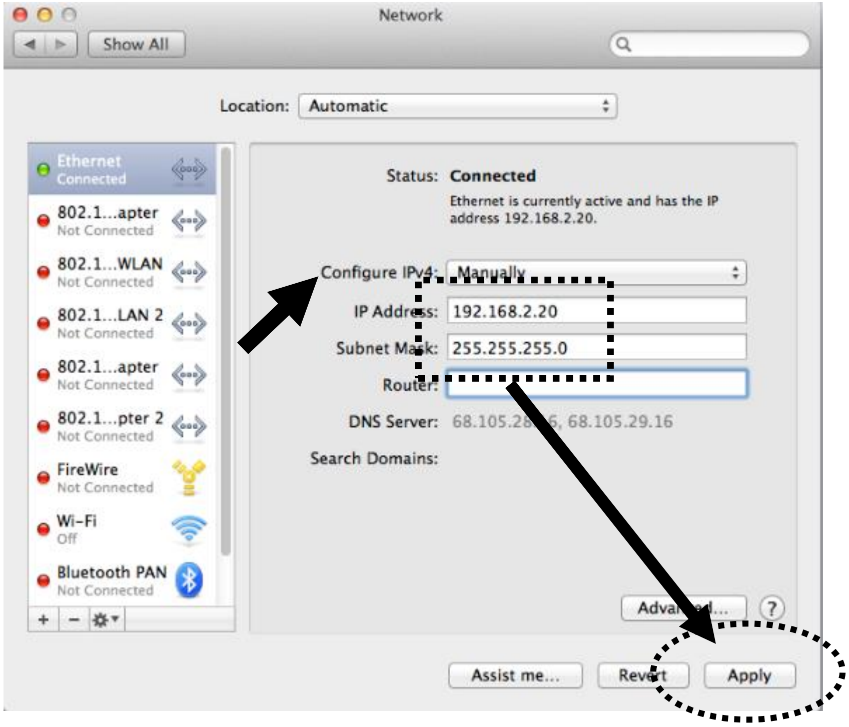
□ Validate settings upon exit

2-3-3 Mac OS X IP Address Setup

1) Go to your system preferences, go to network.



2) Select your Ethernet adapter. Make sure next to “Configure IPv4”, you have it set under “Manually”
IP Address 192.168.2.20
Subnet Mask: 255.255.255.0
Click ‘Apply’ when finished



Location: Automatic

Status: Connected

Ethernet is currently active and has the IP address 192.168.2.20.

Configure IPv4: Manually

IP Address: 192.168.2.20

Subnet Mask: 255.255.255.0

Router:

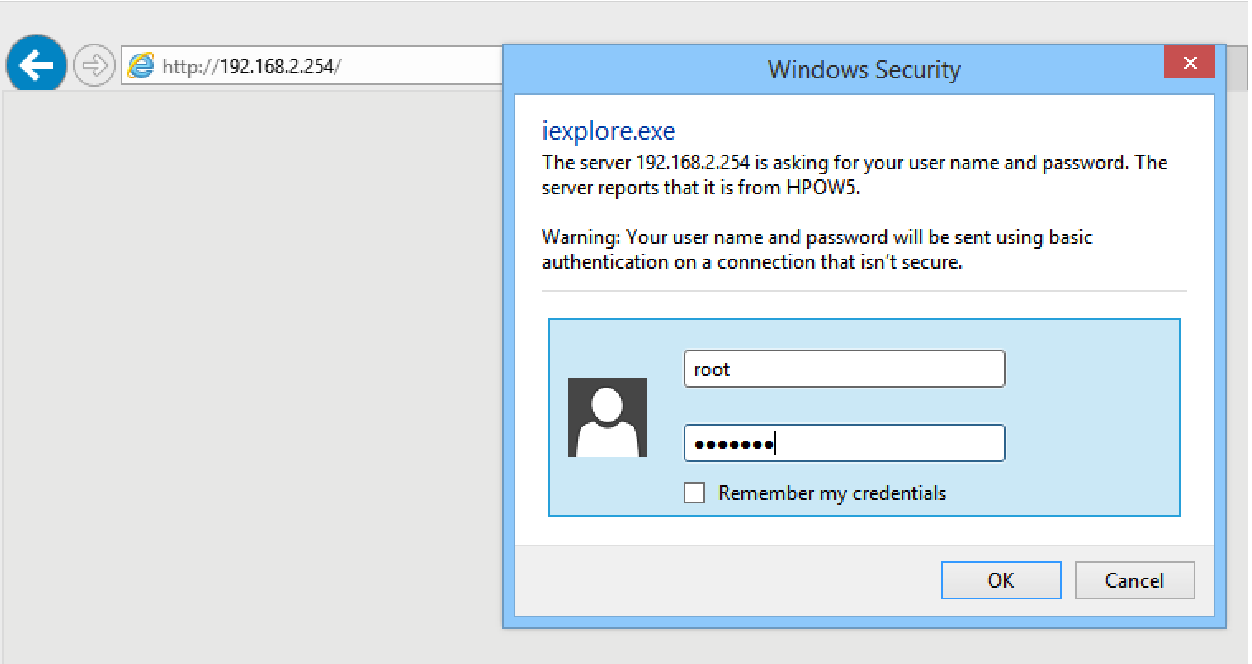
DNS Server: 68.105.28.16, 68.105.29.16

Search Domains:

2-3-4 Accessing the Web Page User Interface

After the IP address setup is complete, please open your web browser.
In the address field, please type: ‘192.168.2.254’ and press enter.

The following message should be shown:



The server 192.168.2.254 is asking for your user name and password. The server reports that it is from HPOW5.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

root

•••••••

□ Remember my credentials

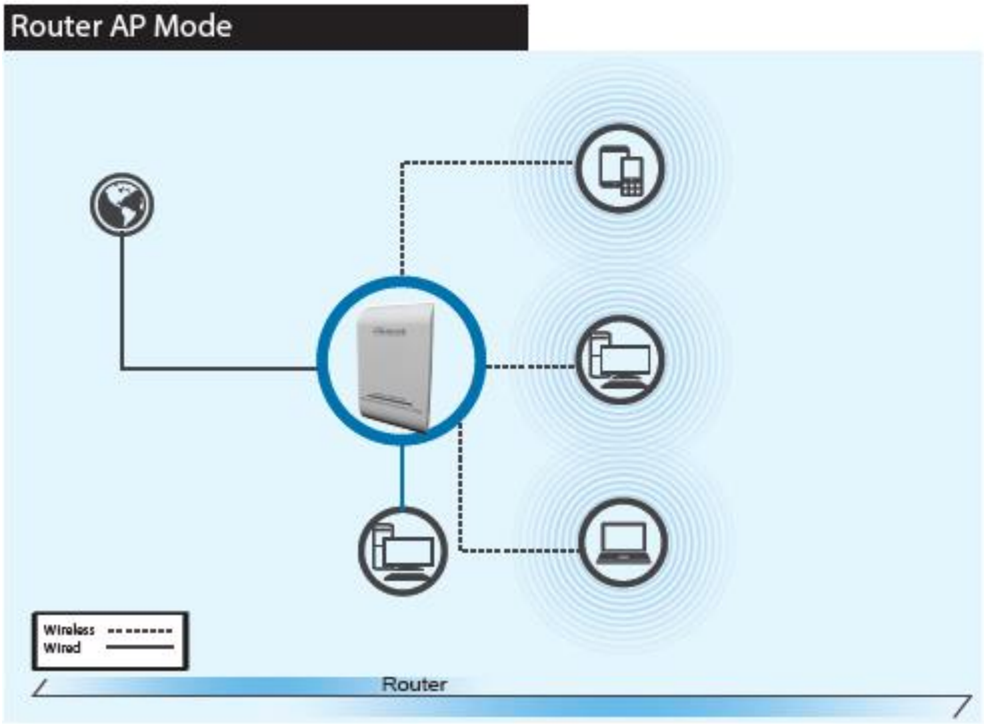
For username and passwords, see the table below:

	Root Account	Admin Account
Username:	root	admin
Password:	default	admin

Chapter III: Setup Wizard

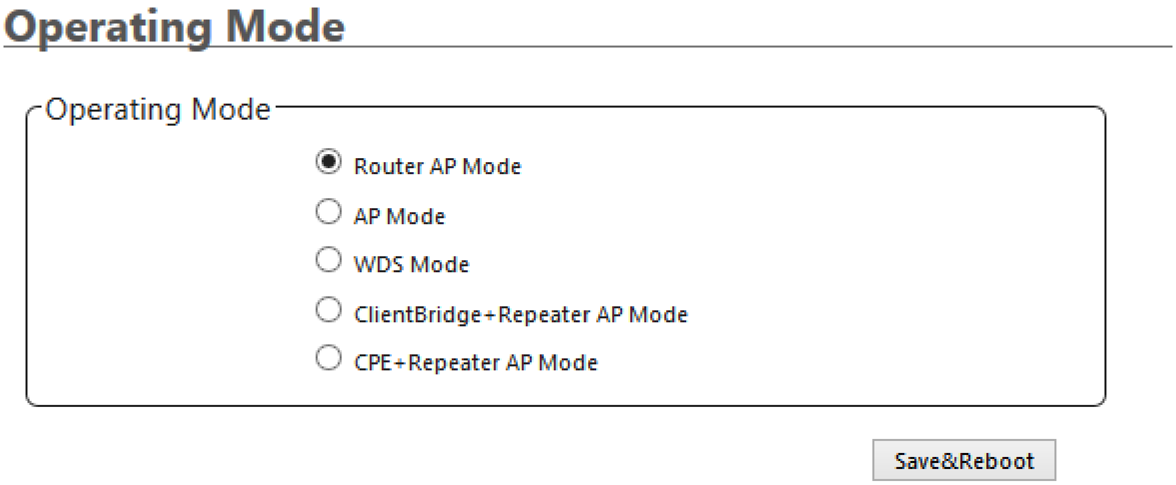
This section will outline how to access the setup wizard for each of the modes in the HPOW5/HPOW10D

3-1 Router AP Setup



When Router AP mode is chosen, the system can be configured as a Wireless Router. In this mode, the device is supposed to be connected to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN/WLAN port share the same IP to ISP through the WAN port. The connection type can be setup in WAN page by using static IP, Dynamic IP, PPPoE or PPTP client. This section provides a detailed explanation for users on how to configure Router AP mode.

Log into the settings page, go to system and select "Operating Mode"



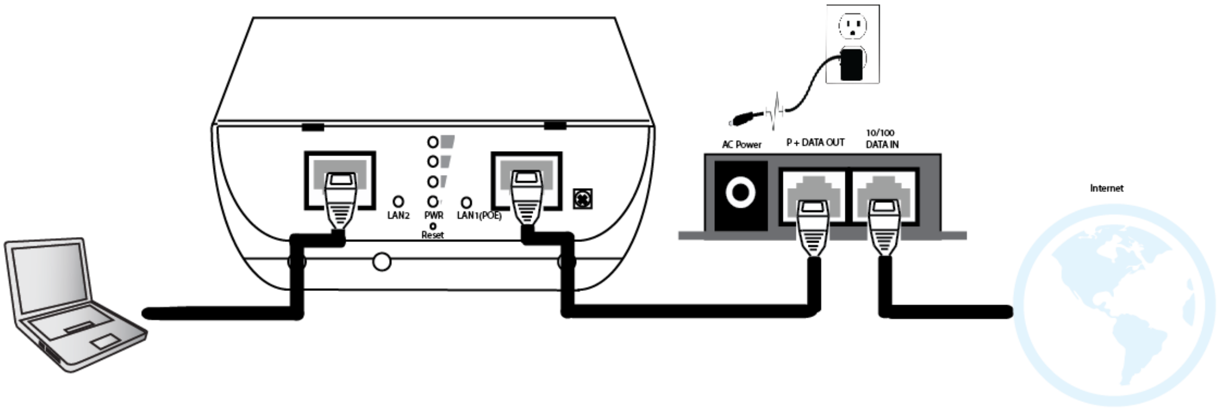
Operating Mode

Operating Mode

● Router AP Mode
○ AP Mode
○ WDS Mode
○ ClientBridge+Repeater AP Mode
○ CPE+Repeater AP Mode

Choose Router AP Mode and click save & reboot. The device will now reboot. After the device has finished rebooting, you will have to make changes to your computer's physical connection. See below.

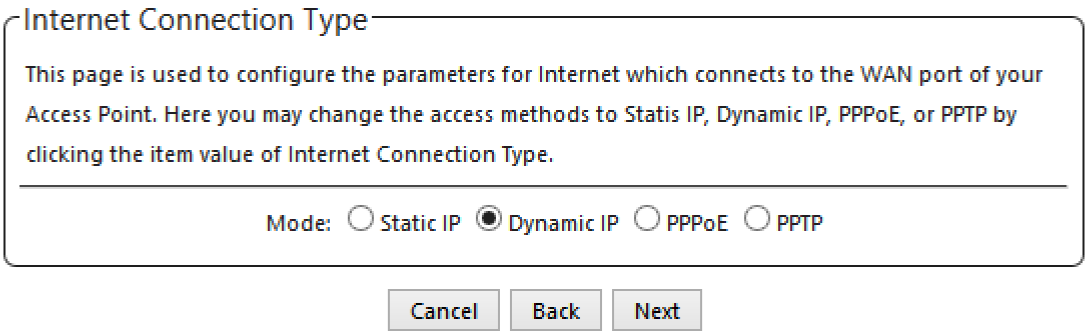
The physical setup is slightly different than the standard setup. Plug your computer into LAN2 on the access point. Plug your ISP's modem into the PoE '10/100 data in' port.



Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select "Setup Wizard".   Click "Next"

3-1-1 Internet Connection Type

Choose your mode. Most ISPs use "Dynamic IP". If you are unsure, please contact your ISP. Refer to Section 4-1 for a more in-depth explanation of these settings.



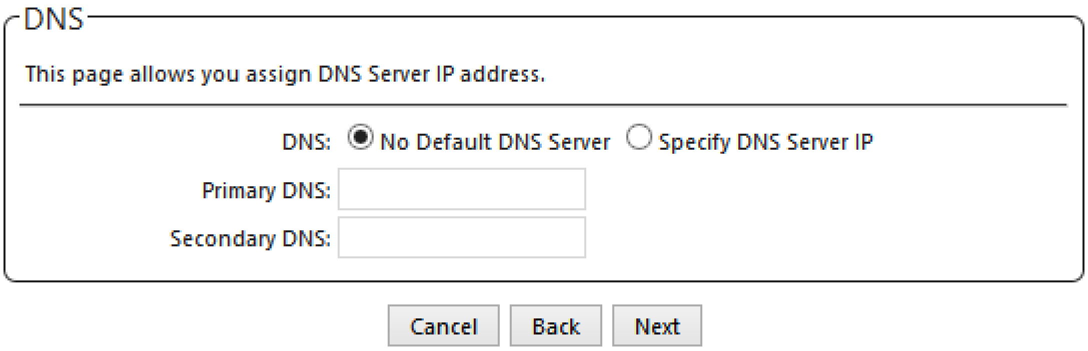
Internet Connection Type

This page is used to configure the parameters for Internet which connects to the WAN port of your Access Point. Here you may change the access methods to Statis IP, Dynamic IP, PPPoE, or PPTP by clicking the item value of Internet Connection Type.

Mode: ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP

3-1-2 DNS

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose "specify" and enter in your values.



DNS

This page allows you assign DNS Server IP address.

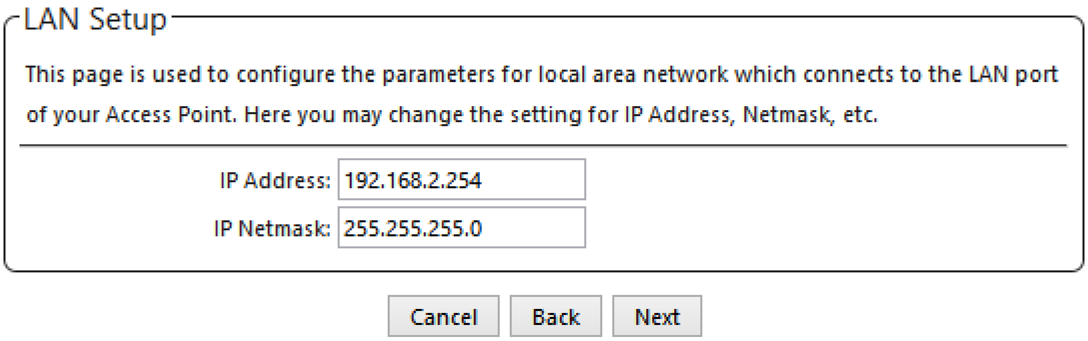
DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

Secondary DNS:

3-1-3 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254



LAN Setup

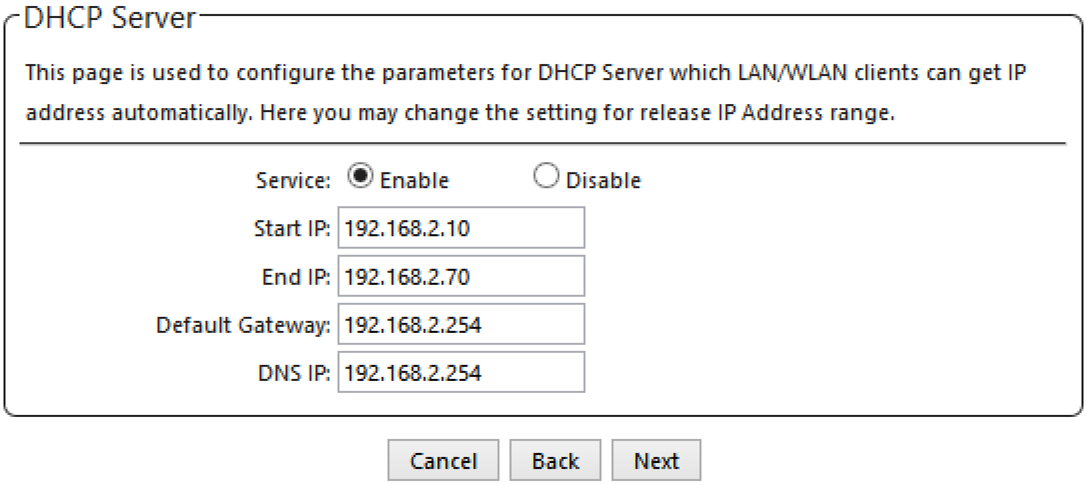
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP Address, Netmask, etc.

IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

3-1-4 DHCP Server

In router mode, by default, IP addresses will be assigned to any LAN/WLAN clients that are connected to the device. You can disable this feature. By default, DHCP is enabled and the IP range is 192.168.2.10 – 192.168.2.70



DHCP Server

This page is used to configure the parameters for DHCP Server which LAN/WLAN clients can get IP address automatically. Here you may change the setting for release IP Address range.

Service: ● Enable ○ Disable

Start IP: 192.168.2.10

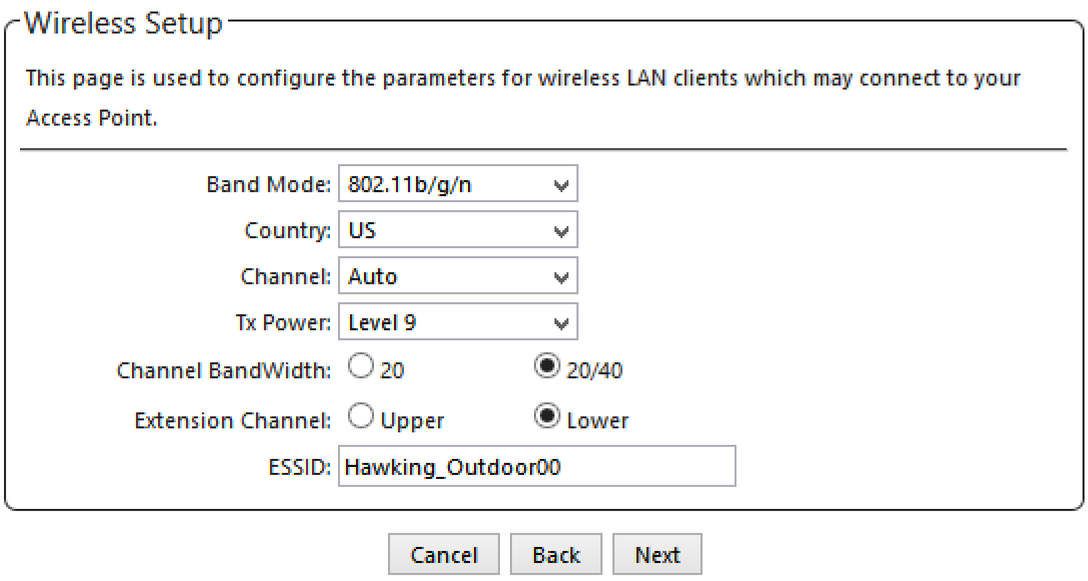
End IP: 192.168.2.70

Default Gateway: 192.168.2.254

DNS IP: 192.168.2.254

3-1-5 Wireless Setup

This page is used to define the parameters for the wireless LAN clients



Wireless Setup

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band Mode: 802.11b/g/n

Country: US

Channel: Auto

Tx Power: Level 9

Channel BandWidth: ○ 20 ● 20/40

Extension Channel: ○ Upper ● Lower

ESSID: Hawking_Outdoor00

Band: *Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.*

*If you select 802.11b only wireless clients using the wireless band you select 802.11b will be able to connect to this access point. (*Maximum transfer rate 11Mbps)

*If you select 802.11b/g, then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. (M*aximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients)

If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 802.11b/g/n (Maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*) (Default).*

*If you select 802.11n, the only wireless clients using 802.11n band will be able to connect to this access point. (M*aximum 300Mbps for 802.11n clients)

Country: *This device only supports United States WiFi channels.*

Channel: *Please select a channel from the dropdown list of 'Channel Number', You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there are radio communication conflicts*

By default, it is on AUTO but if you have a specific channel you wish to use, you can select it here.

Tx Power: *You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Specify power levels between level 1 and level 9. Level 9 is the maximum setting.*

Channel Bandwidth: *Set channel width of wireless radio.* ***Do not modify the default value if you do not understand the function, default setting is '20/40 MHz'***

Extension Channel: *Only for Channel Bandwidth 20/40. Select the desired channel bonding for control*

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_Outdoor' but you can change it to whatever you want.*

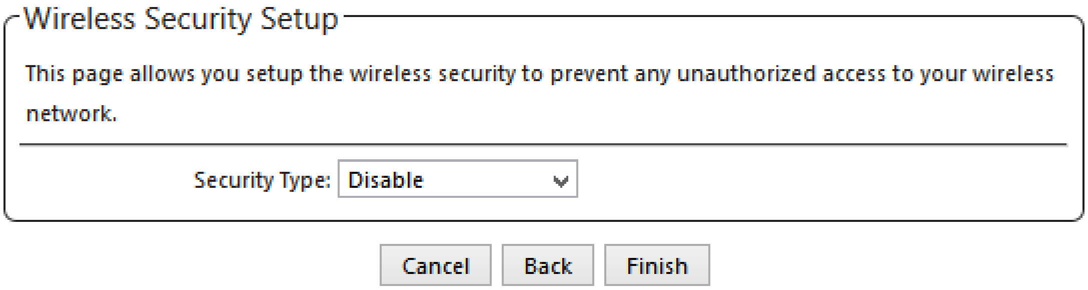
3-1-6 Wireless Security

This page allows you to set up wireless security to prevent any unauthorized access to your wireless network.

Next to security type, choose your type of security (Hawking recommends WPA-2PSK)

3-1-6-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled



Wireless Security Setup

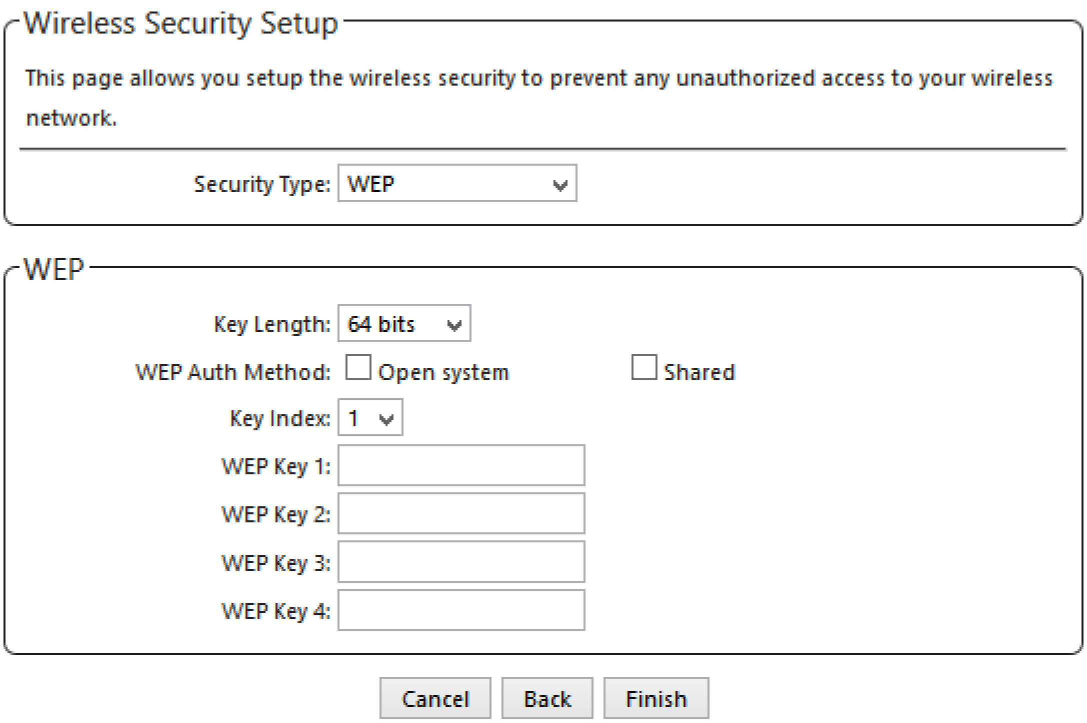
This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: Disable

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

3-1-6-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless access point will use WEP encryption, and the following setup menu will be shown on your web browser:



Wireless Security Setup

This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: WEP

WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

Key Length: *There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

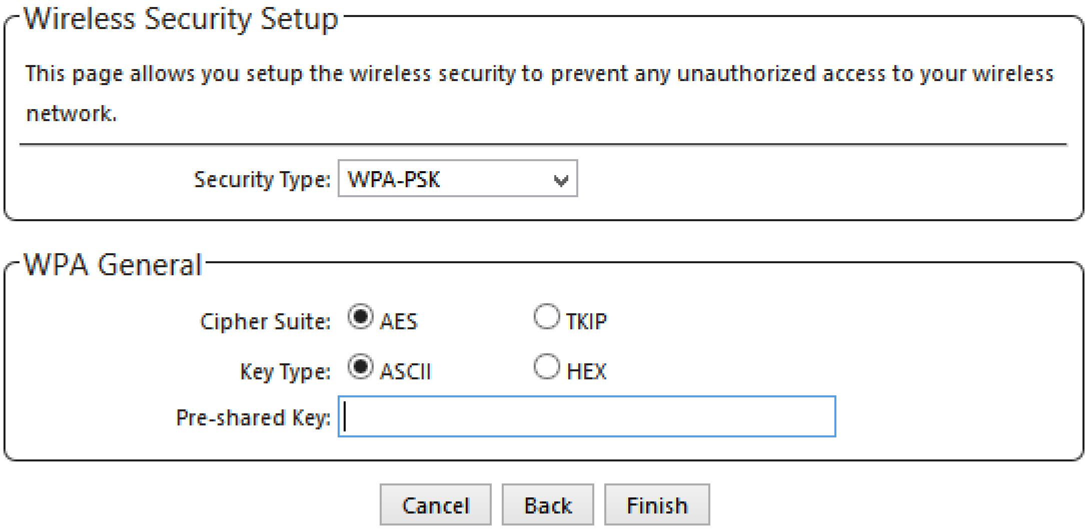
Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-1-6-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:


Wireless Security Setup

This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: WPA-PSK

WPA General

Cipher Suite: ● AES ○ TKIP

Key Type: ● ASCII ○ HEX

Pre-shared Key:

Cipher Suite: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

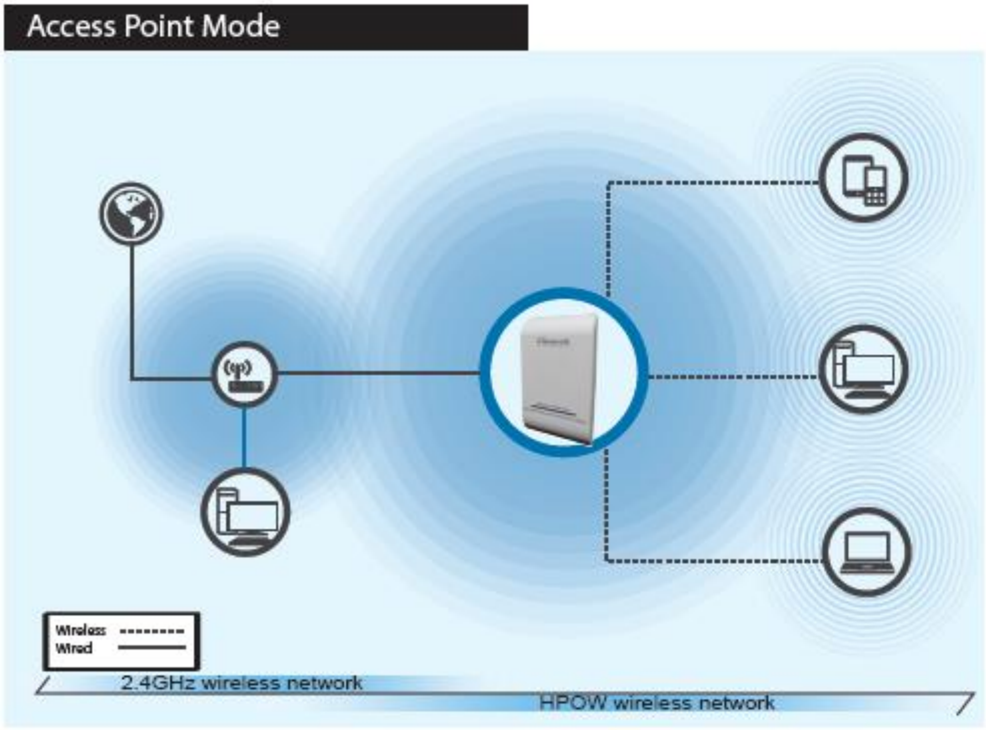
Key Type *Select the type of pre-shared key, you can select ASCII (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher suite as your default level of security.

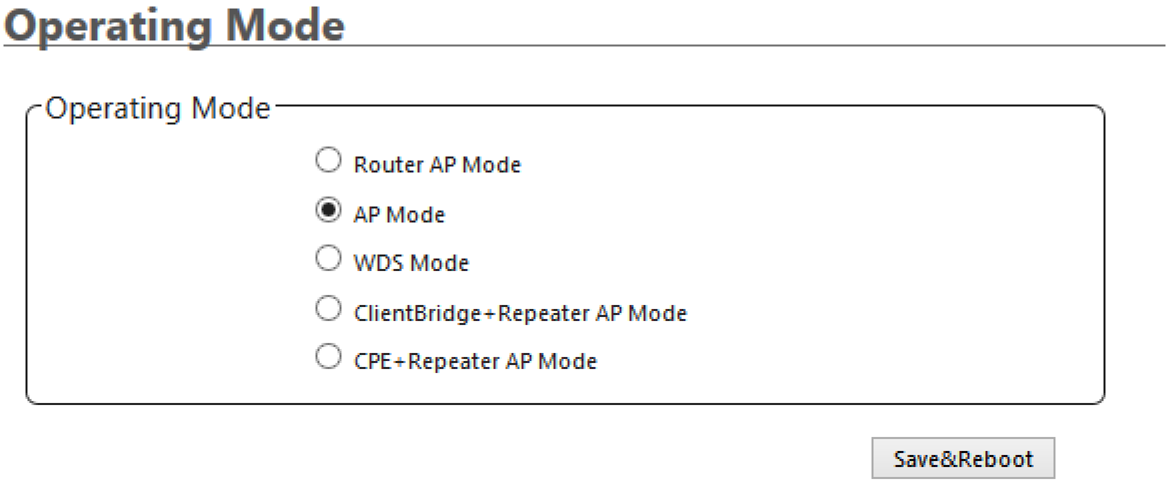
Click Finish and the device will automatically restart and save your settings. After you have finished, you can connect the device to your network via LAN2 to use this as a Router AP. You can add a network switch to LAN2 if you need more Ethernet ports. Please change your computer IP address back to "Obtain an IP automatically".

3-2 AP Mode Setup



When AP mode is chosen, the system can be configured as a standard wireless access point. In this mode, the device can be used as an Access Point for wireless client connection. All Ethernet ports wand wireless interfaces are bridged together. This section provides a detailed explanation for users on how to configure AP mode.

Log into the settings page, go to system and select “Operating Mode”



Operating Mode

Operating Mode

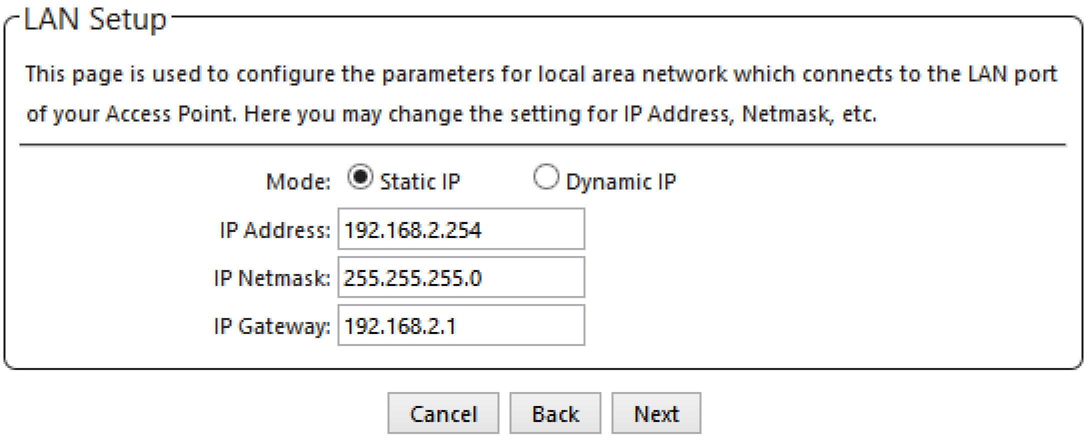
○ Router AP Mode
● AP Mode
○ WDS Mode
○ ClientBridge+Repeater AP Mode
○ CPE+Repeater AP Mode

Choose AP Mode and click save & reboot. The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select “Setup Wizard”. Click “Next”

3-2-1 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254



LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP Address, Netmask, etc.

Mode: ● Static IP ○ Dynamic IP

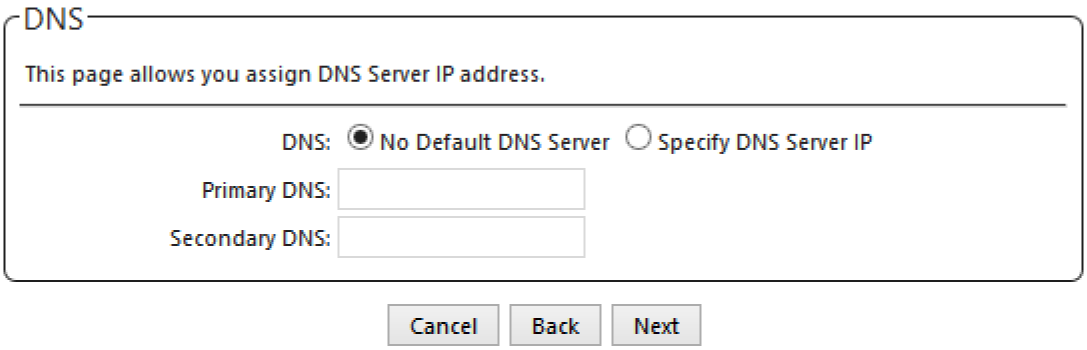
IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

IP Gateway: 192.168.2.1

3-2-2 DNS

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose "specify" and enter in your values.



DNS

This page allows you assign DNS Server IP address.

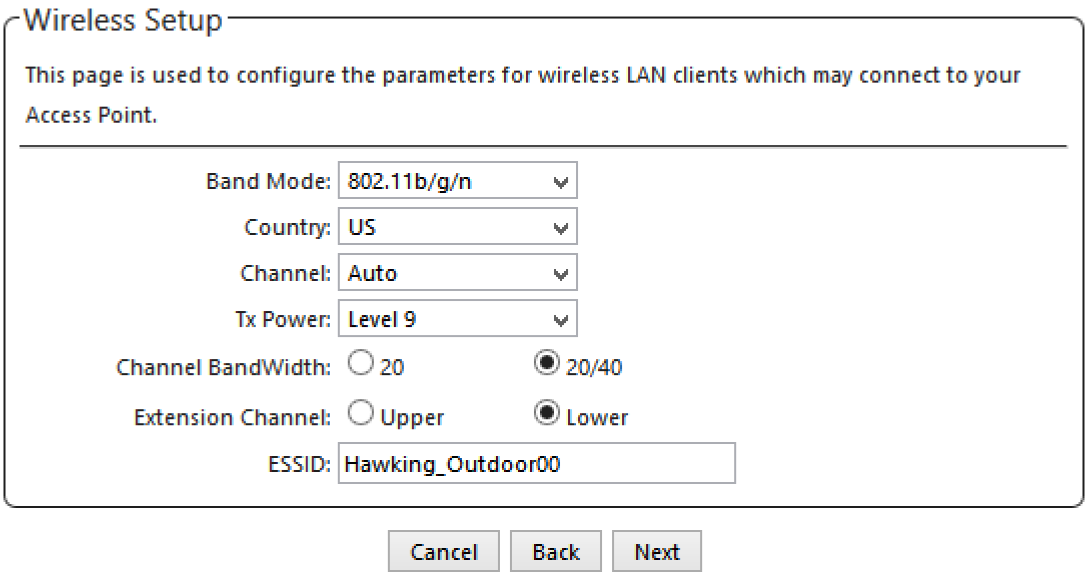
DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

Secondary DNS:

3-2-3 Wireless Setup

This page is used to define the parameters for the wireless LAN clients



Wireless Setup

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band Mode:	802.11b/g/n
Country:	US
Channel:	Auto
Tx Power:	Level 9
Channel BandWidth:	○ 20 ● 20/40
Extension Channel:	○ Upper ● Lower
ESSID:	Hawking_Outdoor00

Band: *Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.*

*If you select 802.11b only wireless clients using the wireless band you select 802.11b will be able to connect to this access point. (*Maximum transfer rate 11Mbps)

*If you select 802.11b/g, then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. (M*aximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients)

If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 802.11b/g/n (Maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*) (Default).*

*If you select 802.11n, the only wireless clients using 802.11n band will be able to connect to this access point. (M*aximum 300Mbps for 802.11n clients)

Country: *This device only supports United States WiFi channels.*

Channel: *Please select a channel from the dropdown list of 'Channel Number', You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there are radio communication conflicts*

By default, it is on AUTO but if you have a specific channel you wish to use, you can select it here.

Tx Power: *You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Specify power levels between level 1 and level 9. Level 9 is the maximum setting.*

Channel Bandwidth: *Set channel width of wireless radio.* ***Do not modify the default value if you do not understand the function, default setting is '20/40 MHz'***

Extension Channel: *Only for Channel Bandwidth 20/40. Select the desired channel bonding for control*

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_Outdoor' but you can change it to whatever you want.*

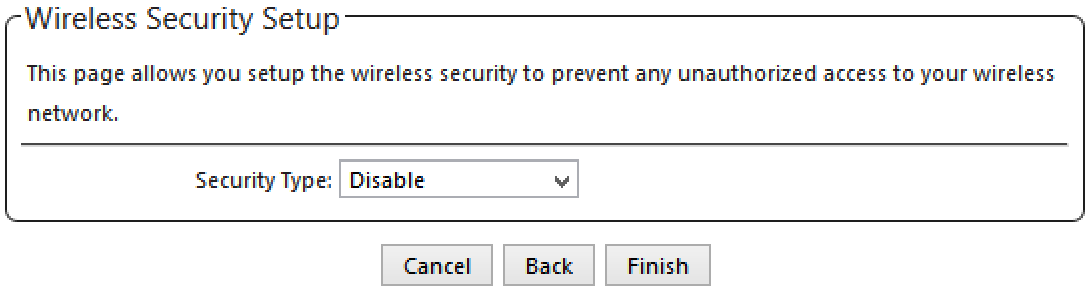
3-2-4 Wireless Security

This page allows you to set up wireless security to prevent any unauthorized access to your wireless network.

Next to security type, choose your type of security (Hawking recommends WPA-2PSK)

3-2-4-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled



Wireless Security Setup

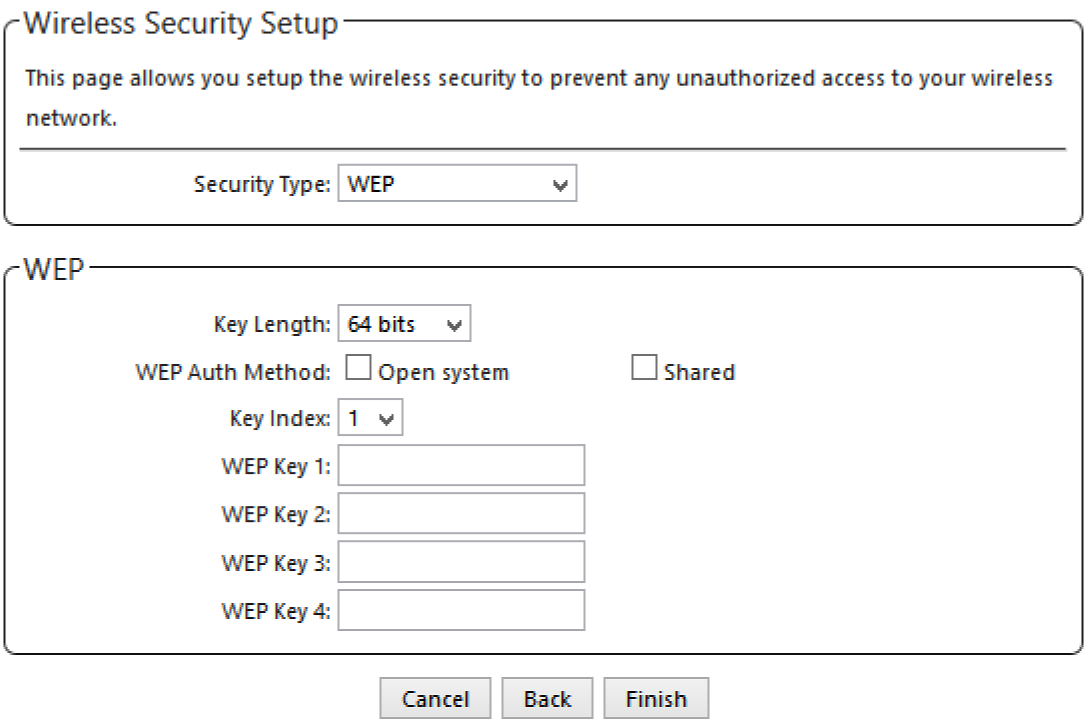
This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: Disable

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

3-2-4-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless access point will use WEP encryption, and the following setup menu will be shown on your web browser:



Wireless Security Setup

This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: WEP

WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

Key Length: *There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

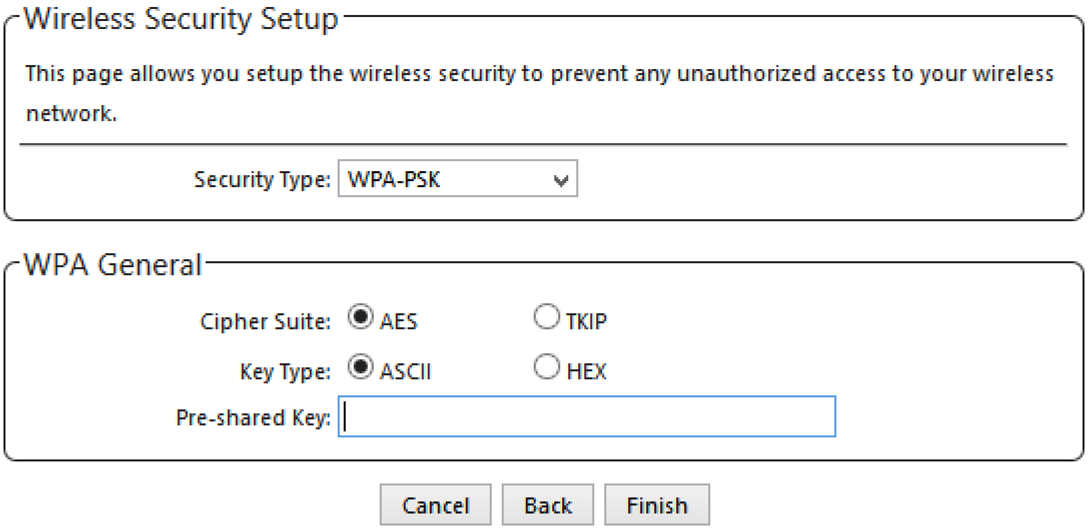
Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-2-4-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Wireless Security Setup

This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: WPA-PSK

WPA General

Cipher Suite: ● AES ○ TKIP

Key Type: ● ASCII ○ HEX

Pre-shared Key:

Cipher Suite: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

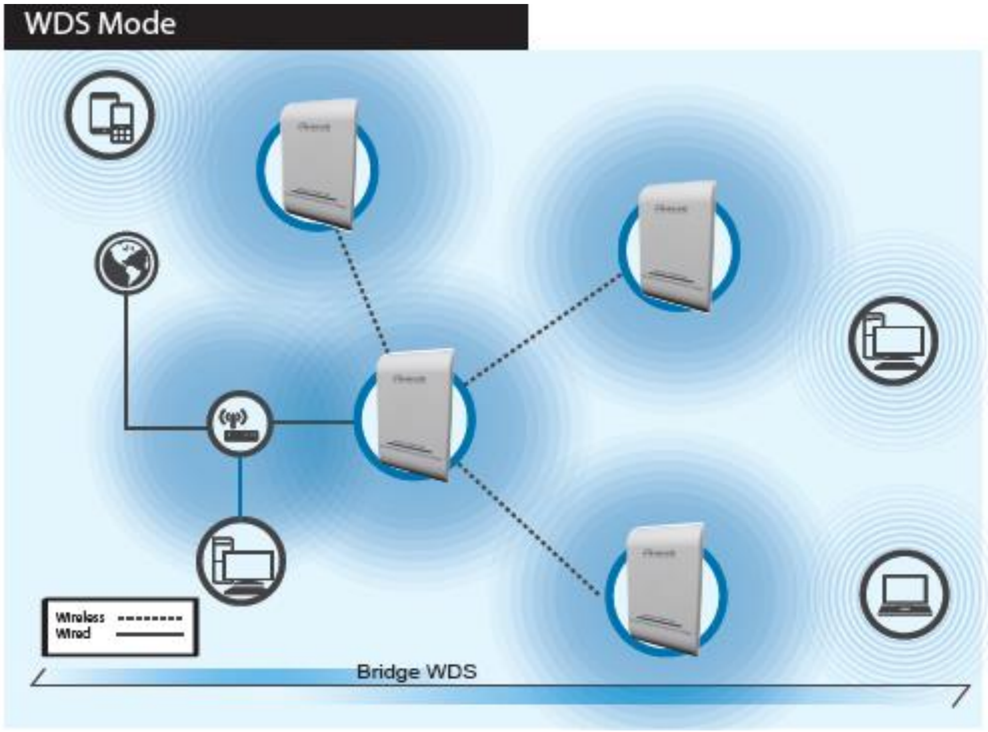
Key Type *Select the type of pre-shared key, you can select ASCII (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher suite as your default level of security.

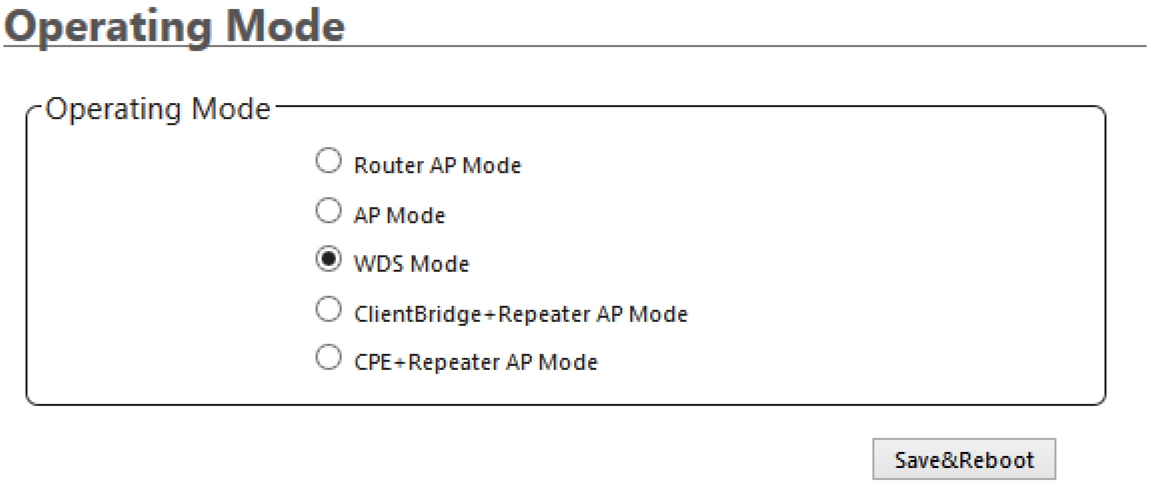
Click Finish and the device will automatically restart and save your settings. After you have finished, you can connect the device to your network via the 10/100 Data IN port on the PoE adapter or the LAN2 port to add this access point to your network. Please change your computer IP address back to "Obtain an IP automatically".

3-3 WDS Mode Setup



When WDS mode is chosen, the system can be configured in WDS Mode. In this mode, WDS (Wireless Distribution Service, creates a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them. ***We can only guarantee WDS will only work with the HPOW5 and the HPOW10D devices.*** Do not use other devices to set up a WDS network. This section provides a detailed explanation for users on how to configure this mode.

Log into the settings page, go to system and select "Operating Mode"



Operating Mode

Operating Mode

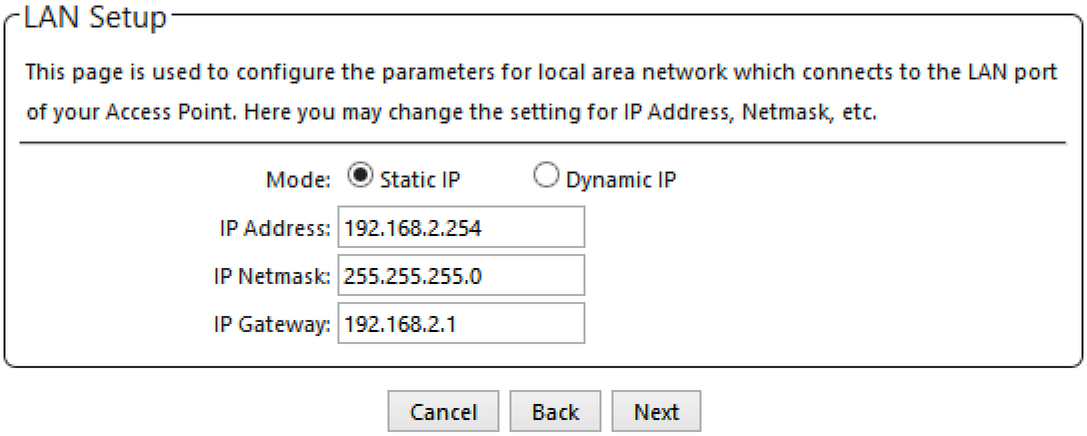
○ Router AP Mode
○ AP Mode
● WDS Mode
○ ClientBridge+Repeater AP Mode
○ CPE+Repeater AP Mode

Choose WDS Mode and click save & reboot. The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select “Setup Wizard”. Click “Next”

3-3-1 LAN Setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254. Note: The IP address of each remote WDS peer must be unique.



LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP Address, Netmask, etc.

Mode: ● Static IP ○ Dynamic IP

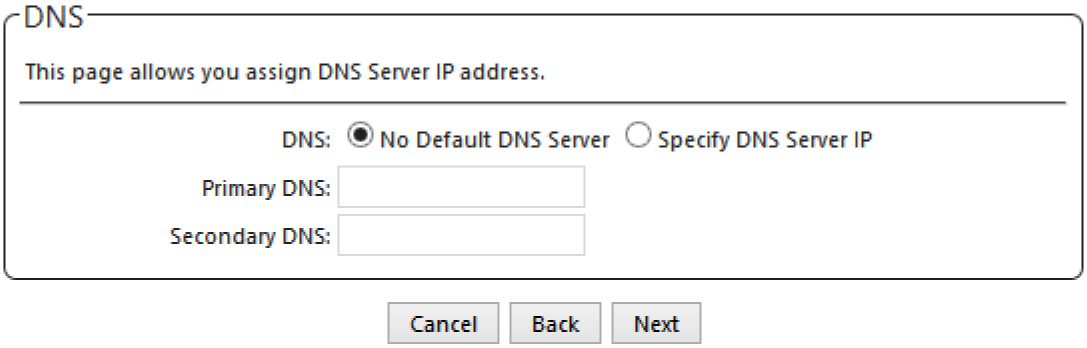
IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

IP Gateway: 192.168.2.1

3-3-2 DNS

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose “specify” and enter in your values.



DNS

This page allows you assign DNS Server IP address.

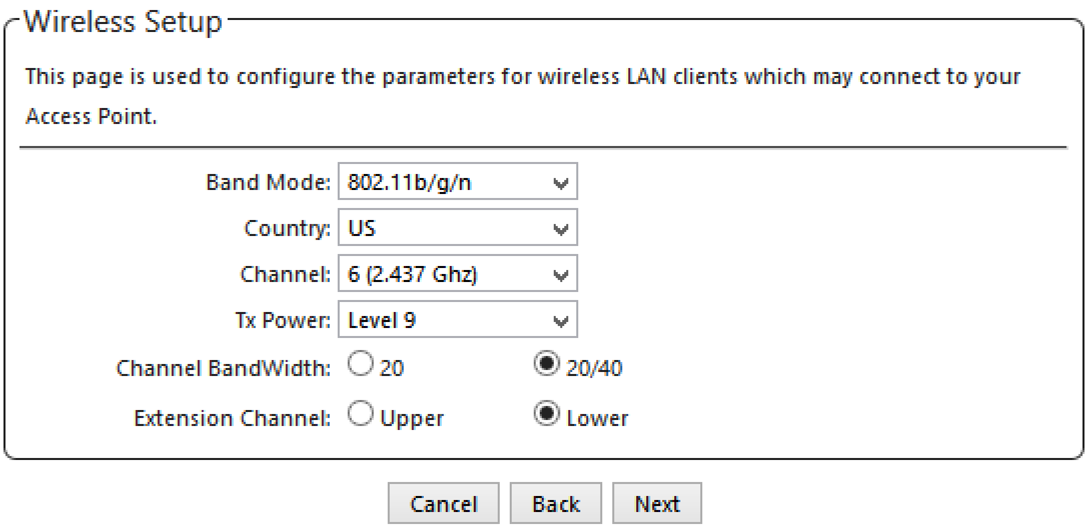
DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

Secondary DNS:

3-3-3 Wireless Setup

This page is used to define the parameters for the wireless LAN clients. These settings should match the remote WDS peer devices



Wireless Setup

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band Mode: 802.11b/g/n

Country: US

Channel: 6 (2.437 Ghz)

Tx Power: Level 9

Channel BandWidth: ○ 20 ● 20/40

Extension Channel: ○ Upper ● Lower

Band: *Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.*

*If you select 802.11b only wireless clients using the wireless band you select 802.11b will be able to connect to this access point. (*Maximum transfer rate 11Mbps)

*If you select 802.11b/g, then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. (*Maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients)

If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 802.11b/g/n (Maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*) (Default).*

*If you select 802.11n, the only wireless clients using 802.11n band will be able to connect to this access point. (*Maximum 300Mbps for 802.11n clients)

Country: *This device only supports United States WiFi channels.*

Channel: *Please select a channel from the dropdown list of 'Channel Number', You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there are radio communication conflicts*

By default, it is on AUTO but if you have a specific channel you wish to use, you can select it here.

Tx Power: *You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Specify power levels between level 1 and level 9. Level 9 is the maximum setting.*

Channel Bandwidth: *Set channel width of wireless radio.* ***Do not modify the default value if you do not understand the function, default setting is '20/40 MHz'***

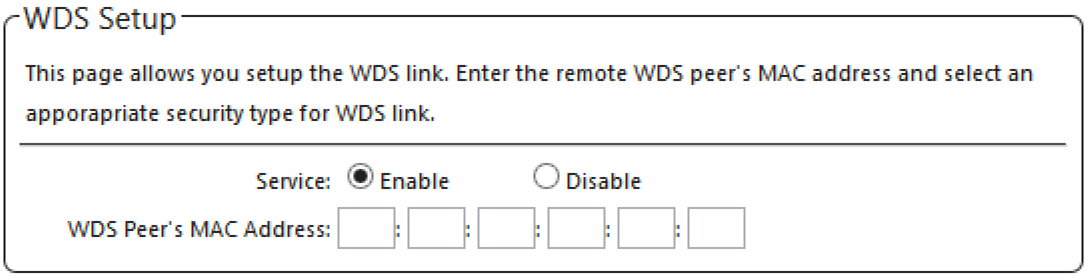
Extension Channel: *Only for Channel Bandwidth 20/40. Select the desired channel bonding for control*

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_Outdoor' but you can change it to whatever you want.*

3-3-4 WDS Setup/Wireless Security

3-3-4-1 WDS Setup

This page allows you to setup the WDS Link. Enter the Remote WDS peer's MAC Address and select an appropriate security type for WDS Link. Note that the remote WDS peer should also be using this device's MAC address. Reference Status, Overview to get the wireless MAC Address.



WDS Setup

This page allows you setup the WDS link. Enter the remote WDS peer's MAC address and select an apporapriate security type for WDS link.

Service: ● Enable ○ Disable

WDS Peer's MAC Address: ▢ : ▢ : ▢ : ▢ : ▢ : ▢

Service: *Enable/disable to turn on/off WDS mode*

WDS Peer's MAC Address: Enter the MAC address of the WDS Peer (aa.bb.cc.dd.ee.ff)

3-3-4-2 Wireless Security

This page allows you to set up wireless security to prevent any unauthorized access to your wireless network.

Next to security type, choose your type of security (Hawking recommends WPA-2PSK)

3-3-4-2-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

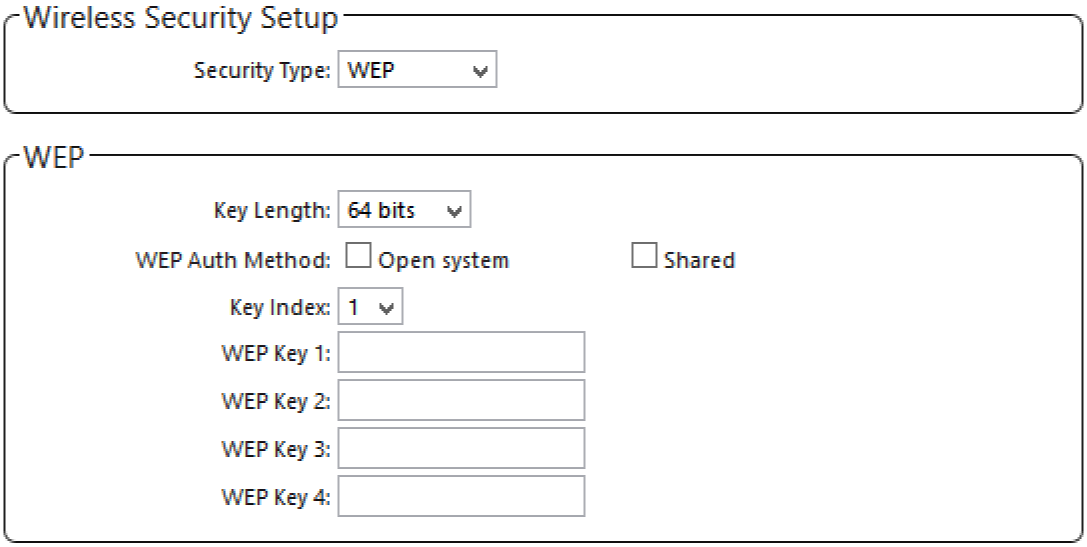
Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

Wireless Security Setup

Security Type: Disable

3-3-4-2-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless access point will use WEP encryption, and the following setup menu will be shown on your web browser:



Wireless Security Setup

Security Type: WEP

WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

Key Length: *There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-3-4-2-3 AES

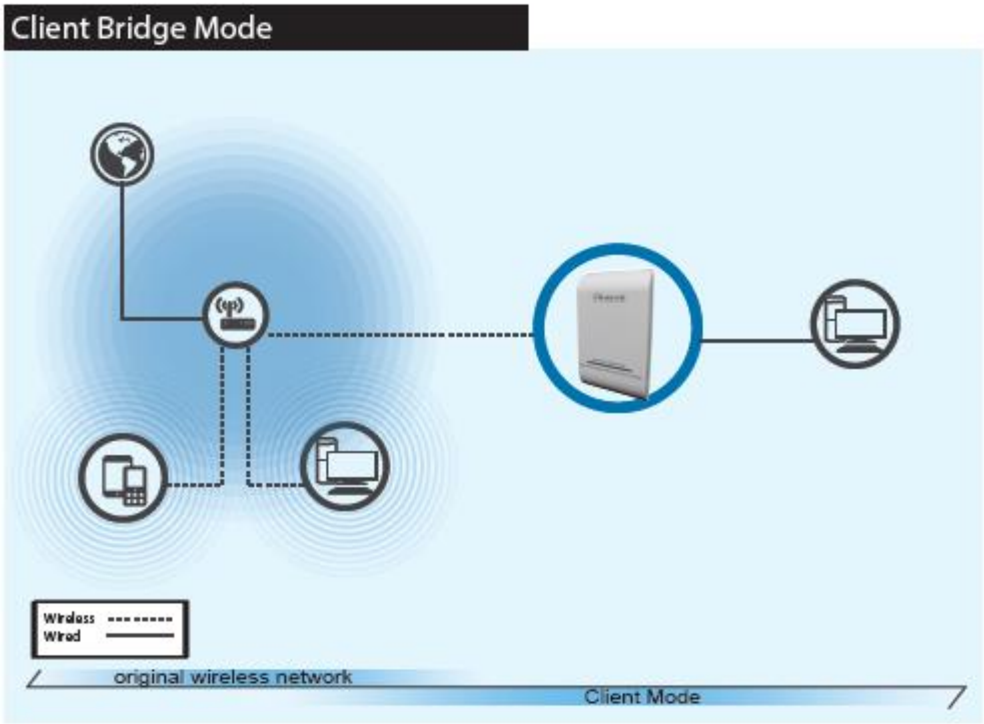
When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:

AES is short for **Advanced Encryption Standard**, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

AES Key *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

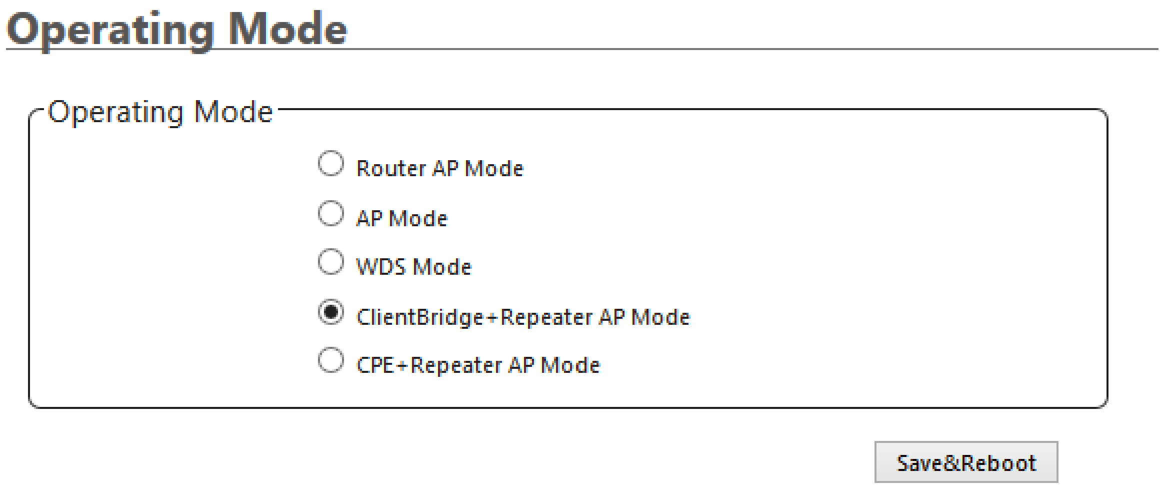
Click Finish and the device will automatically restart and save your settings. After you have finished, at least one of the WDS devices must be connected to your network via the 10/100 Data In port on the PoE adapter or the LAN2 port to add this WDS device to your network. The other WDS peers just need to be powered on via the P-Data Out port on the PoE adapter and can be stand alone. Please change your computer IP address back to "Obtain an IP automatically".

3-4 Client Bridge + Repeater AP Mode



When Client Bridge + Repeater AP Mode is chosen, the system can be configured in bridged mode. In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network. It can also act as a wireless repeater. All Ethernet ports and repeater access points are bridged together. This section provides a detailed explanation for users on how to configure this mode.

Log into the settings page, go to system and select “Operating Mode”



Operating Mode

Operating Mode

○ Router AP Mode
○ AP Mode
○ WDS Mode
● ClientBridge+Repeater AP Mode
○ CPE+Repeater AP Mode

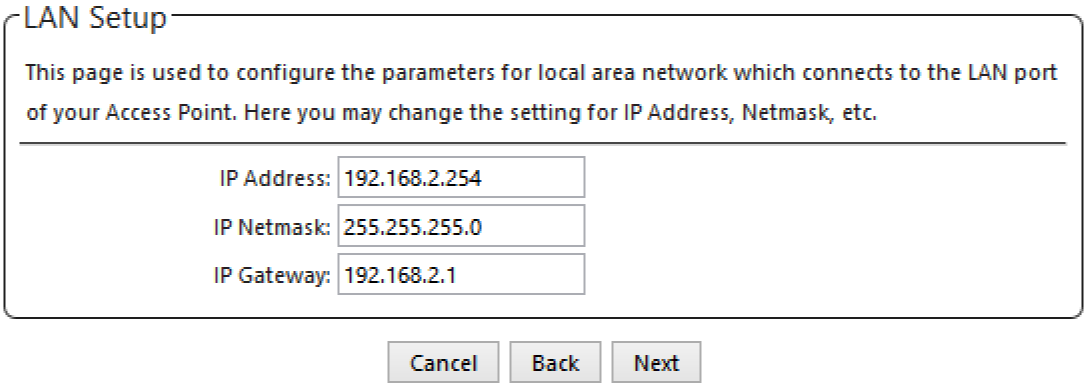
Save&Reboot

Choose Client Bridge + Repeater AP Mode and click save & reboot. The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select “Setup Wizard”. Click “Next”

3-4-1 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254



LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP Address, Netmask, etc.

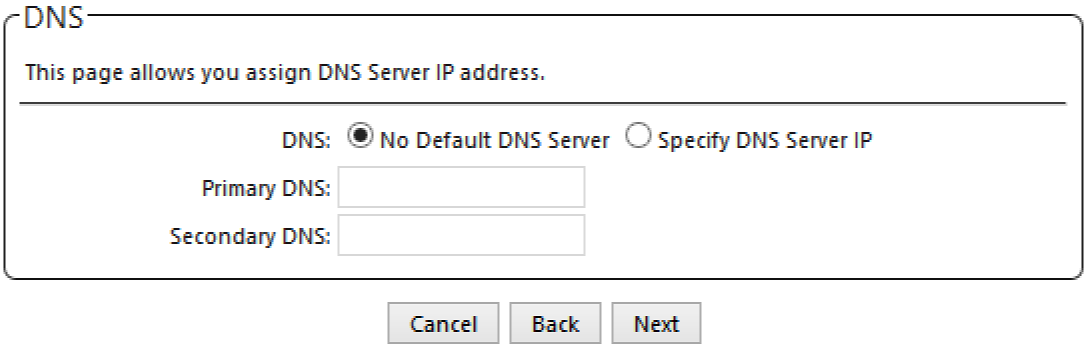
IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

IP Gateway: 192.168.2.1

3-4-2 DNS

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose “specify” and enter in your values.



DNS

This page allows you assign DNS Server IP address.

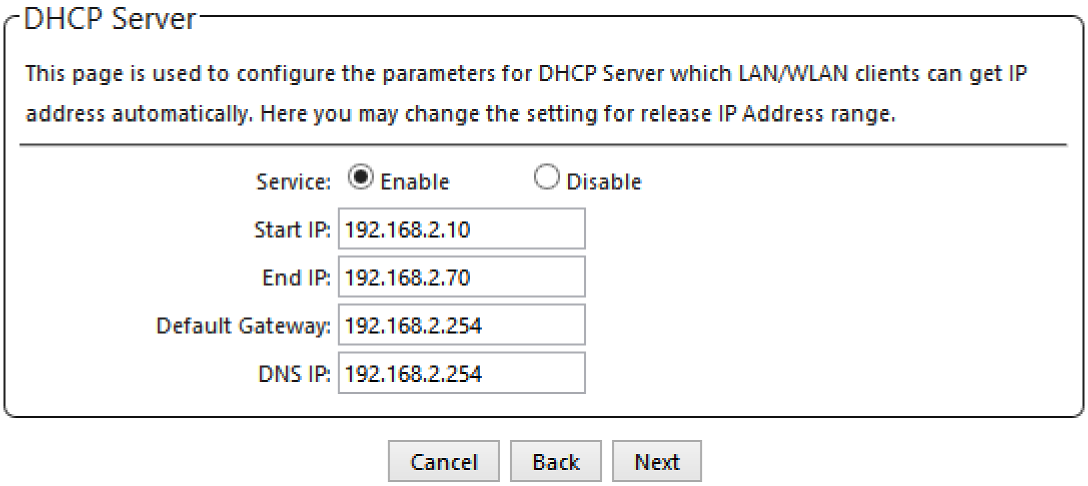
DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

Secondary DNS:

3-4-3 DHCP Server

In router mode, by default, IP addresses will be assigned to any LAN/WLAN clients that are connected to the device. You can disable this feature. By default, DHCP is enabled and the IP range is 192.168.2.10 – 192.168.2.70. If you want to use this device as a simple client bridge and/or a standard wireless repeater, you should disable this service.



DHCP Server

This page is used to configure the parameters for DHCP Server which LAN/WLAN clients can get IP address automatically. Here you may change the setting for release IP Address range.

Service: ● Enable ○ Disable

Start IP: 192.168.2.10

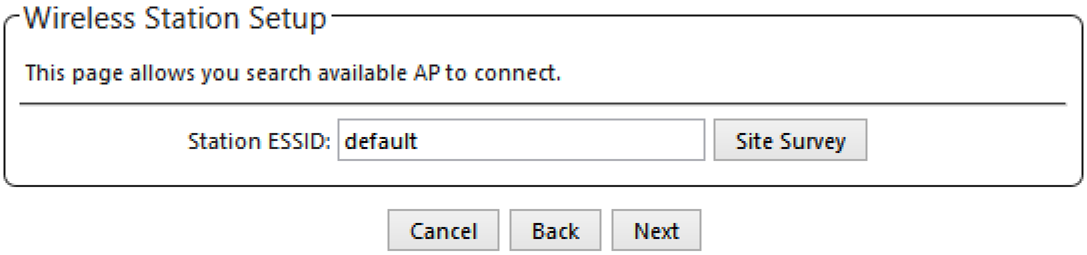
End IP: 192.168.2.70

Default Gateway: 192.168.2.254

DNS IP: 192.168.2.254

3-4-4 Wireless Station Setup

This page allows you to search for an available Access Point to Connect



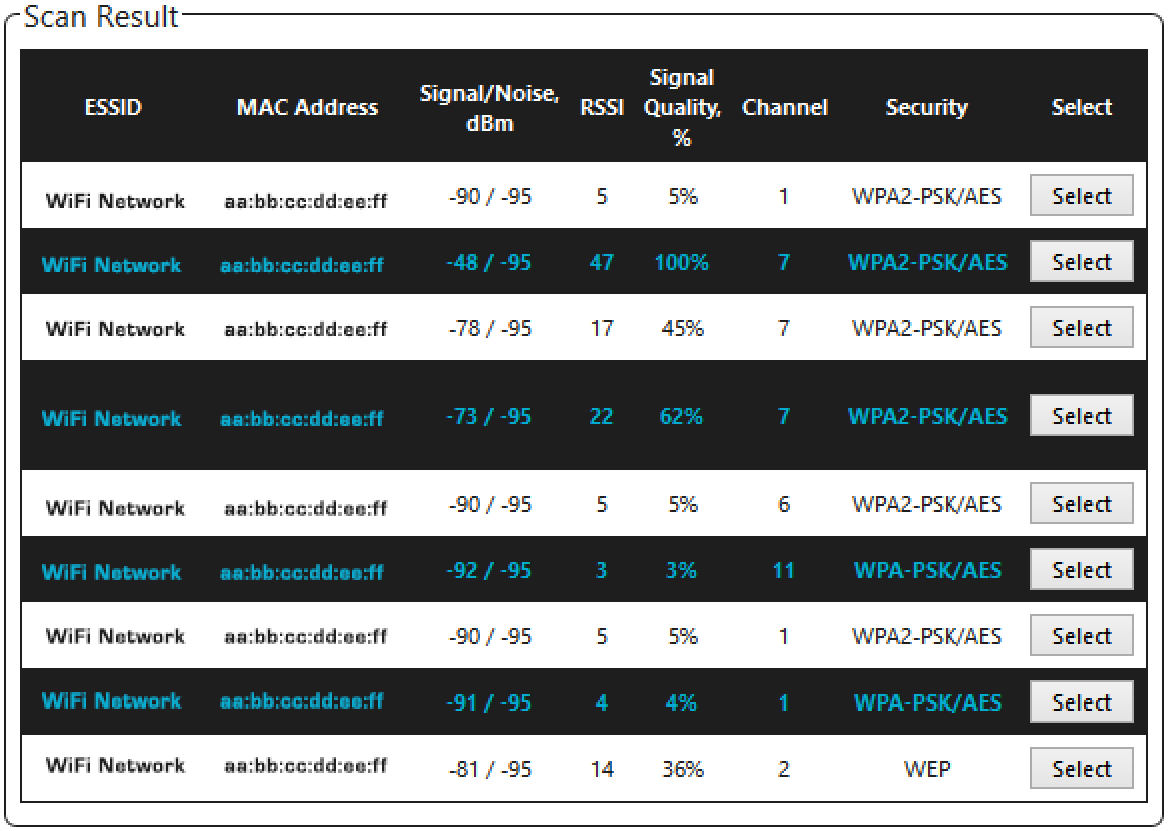
Wireless Station Setup

This page allows you search available AP to connect.

Station ESSID: default

Station ESSID: *Wireless Name of the network you wish to connect to. You can manually enter the name or click on "Site Survey" for the device to scan for wireless networks.*

Site Survey: *Press this button for the device to automatically scan for wireless networks*



Scan Result

ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-48 / -95	47	100%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-78 / -95	17	45%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-73 / -95	22	62%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	6	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-92 / -95	3	3%	11	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-91 / -95	4	4%	1	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-81 / -95	14	36%	2	WEP	Select

Site Survey Results

ESSID: Available Extend Service Set ID (wireless name) of surrounding Access Points.

MAC Address: MAC addresses of surrounding Access Points.

Signal/Noise dBm: Received signal strength of all found Access Points.

RSSI: Indicate the RSSI of the respective client's association.

Signal Quality (%): Received signal strength of all found Access Points.

Channel: Channel numbers used by all found Access Points.

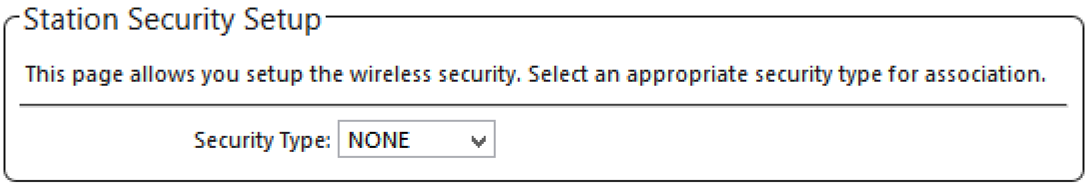
Security: Security type by all found Access Points.

3-4-5 Wireless Security

This page allows you to set up wireless security to the access point you are attempting to connect to. Make sure you use the exact same setting as the access point you are attempting to connect to.

3-4-5-1 Disable wireless security

This means the network you are choosing has no security enabled at all. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



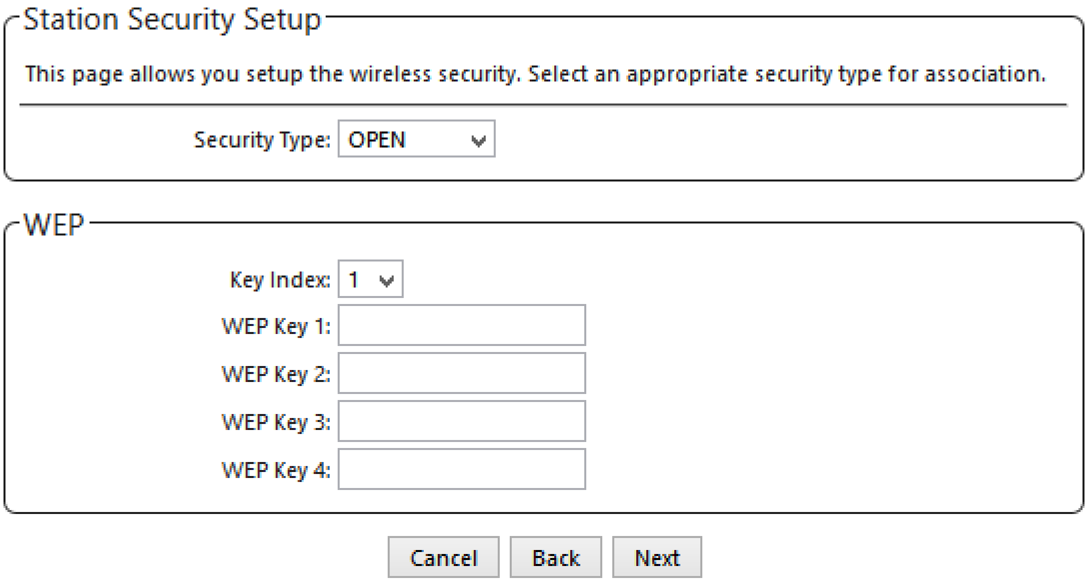
Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: NONE

3-4-5-2 WEP - Wired Equivalent Privacy (Open/Shared)

When you select this mode, the wireless access point you are connecting to is using WEP encryption. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: OPEN

WEP

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

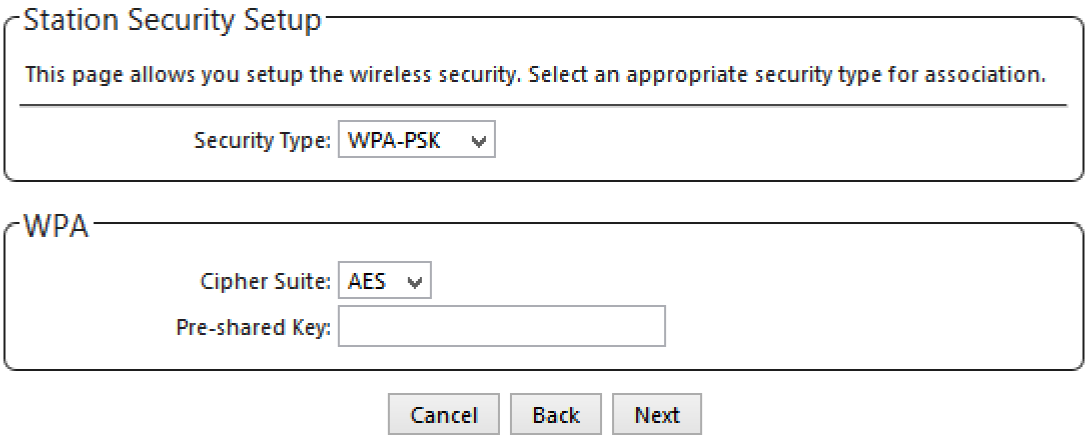
Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-4-5-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point you are connecting to is using WPA encryption. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: WPA-PSK

WPA

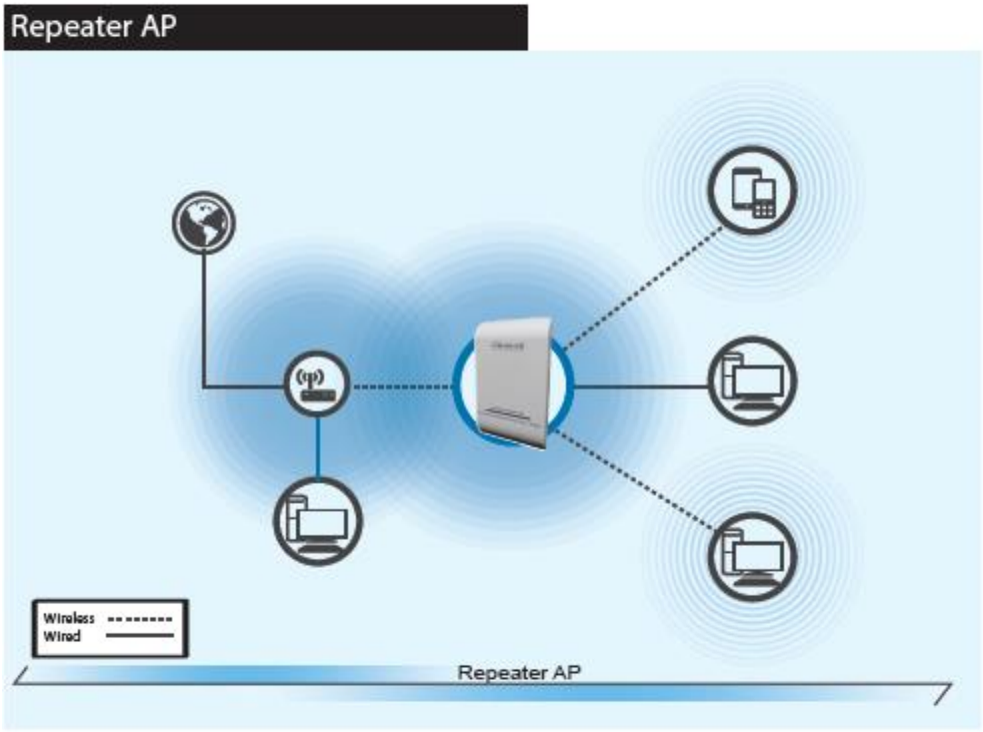
Cipher Suite: AES

Pre-shared Key:

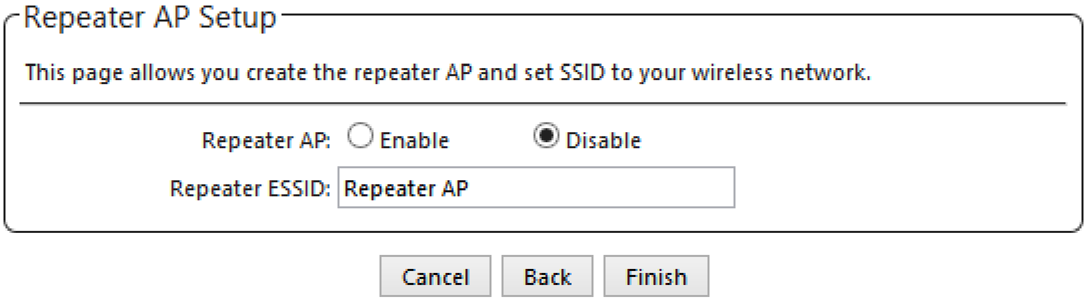
Cipher Suite: ***AES** is short for **Advanced Encryption Standard**, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. **TKIP** is short for **Temporal Key Integrity Protocol**, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Pre-shared Keyu\ Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters

3-4-6 Repeater AP Setup



This allows you to create a repeater AP and set SSID to your wireless network. Enable this if you want the device to act as a wireless repeater. If your choose disable, the device will be configured ONLY as a client bridge. If you click enable, you can set the settings for the repeater.



Repeater AP Setup

This page allows you create the repeater AP and set SSID to your wireless network.

Repeater AP: ○ Enable ● Disable

Repeater ESSID: Repeater AP

Repeater AP: Enable if you wish to use the repeater function, disable if you wish to use the device ONLY in client-bridge mode.

Repeater ESSID: Extended Service Set ID. When users are browsing for available wireless networks, this is the SSID that will appear in the list.

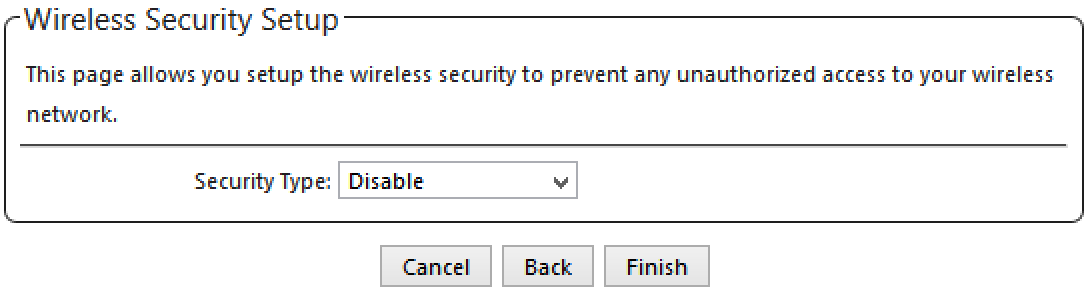
3-4-7 Repeater Wireless Security

This page allows you to set up wireless security to prevent any unauthorized access to your wireless network.

Next to security type, choose your type of security (Hawking recommends WPA-2PSK)

3-4-7-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled



Wireless Security Setup

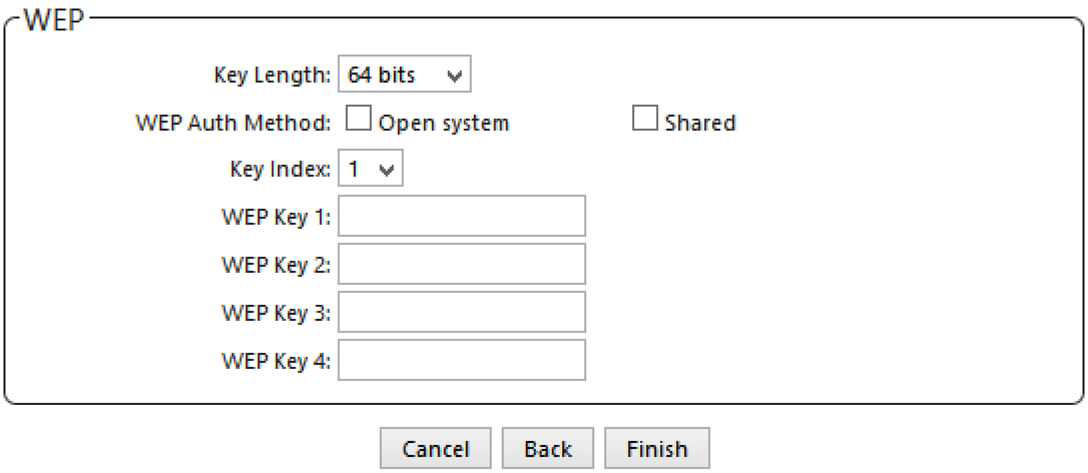
This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: Disable

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

3-4-7-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless access point will use WEP encryption, and the following setup menu will be shown on your web browser:



WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

Key Length: *There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

Shared - only those with the same key with the AP can connect to it.

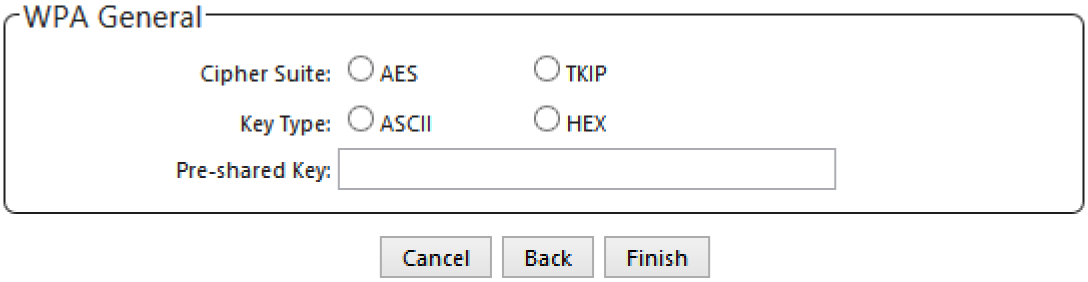
Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for*

ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)

3-4-7-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



WPA General

Cipher Suite: ○ AES ○ TKIP

Key Type: ○ ASCII ○ HEX

Pre-shared Key: □

Cipher Suite: ***AES** is short for **Advanced Encryption Standard**, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. **TKIP** is short for **Temporal Key Integrity Protocol**, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

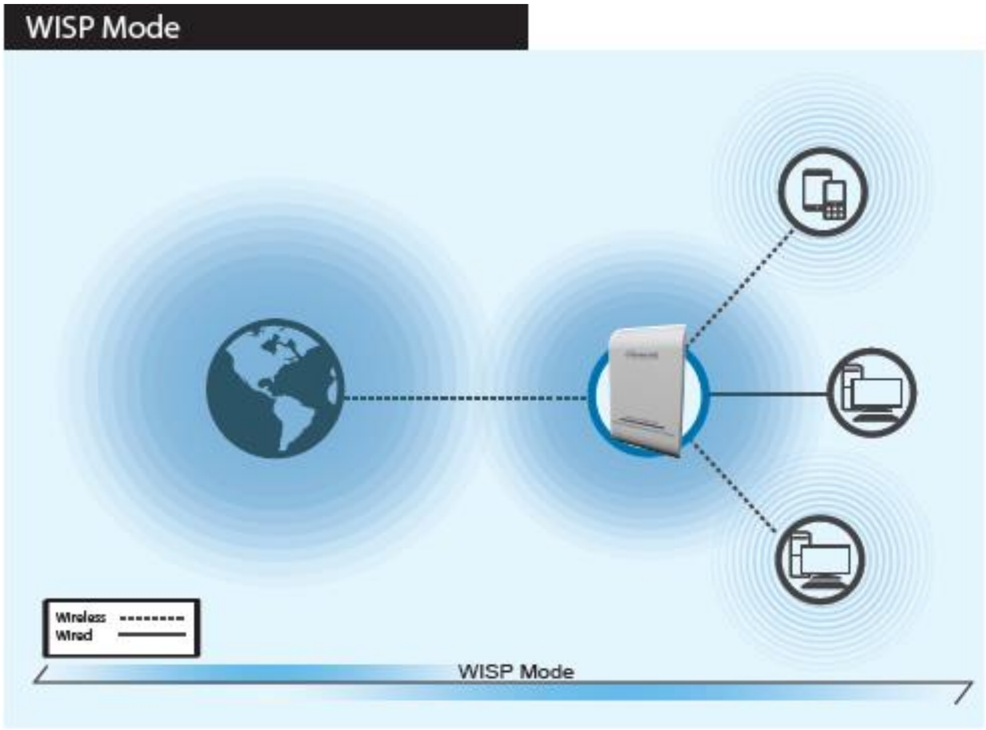
Key Type *Select the type of pre-shared key, you can select ASCII (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher suite as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, a network device must be connected to your network via the 10/100 Data In port on the PoE adapter or the LAN2 port to add this client device to your network. It should not be plugged back into the main network (should be remote). If using as a Repeater, the device just needs to be powered on via the P-Data Out port on the PoE adapter and can be standalone (you can also connect any wired client computers to the 10/100 Data In Port or LAN2). Please change your computer IP address back to "Obtain an IP automatically".

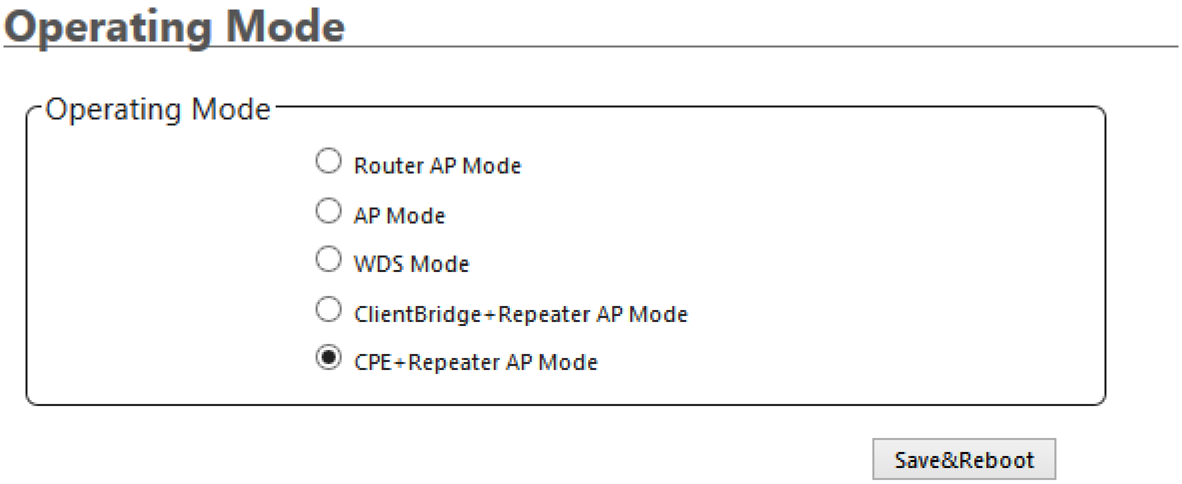
3-5 CPE + Repeater AP Mode (WISP)



When CPE + Repeater AP Mode is chosen, the system can be configured in Wireless Internet repeater mode. In this mode, the device can wirelessly connect to a WISP (wireless internet service provider), ie. Another wireless AP, HotSpot, etc. It can then wirelessly repeat the signal and can even act as a router for these signals. NAT is enabled and wired and wireless computers can share the same IP range. This section provides a detailed explanation for users on how to configure this mode.

Choose CPE+Repeater AP Mode

Log into the settings page, go to system and select “Operating Mode”



Operating Mode

Operating Mode

○ Router AP Mode

○ AP Mode

○ WDS Mode

○ ClientBridge+Repeater AP Mode

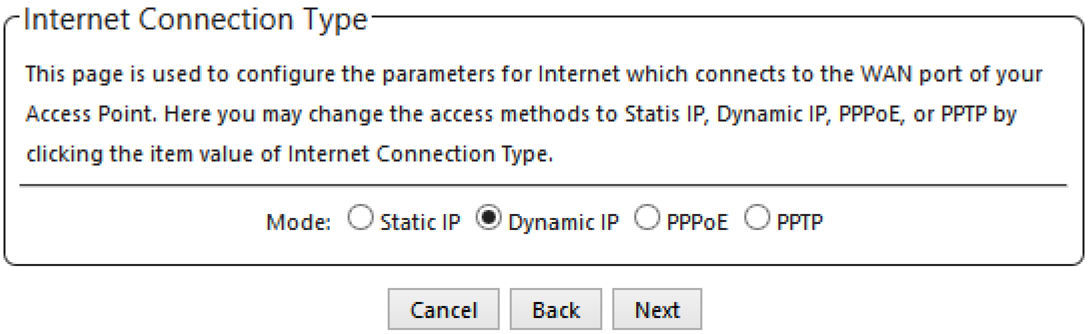
● CPE+Repeater AP Mode

Choose CPE + Repeater AP Mode and click save & reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select "Setup Wizard". Click "Next"

3-5-1 Internet Connection Type

Choose your mode. Most ISPs use "Dynamic IP". If you are unsure, please contact your ISP. Refer to Section 4-2 for a more in-depth explanation of these settings.



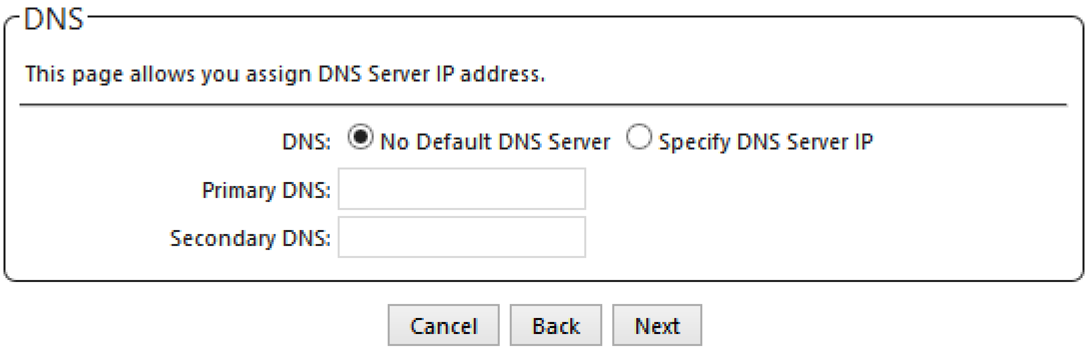
Internet Connection Type

This page is used to configure the parameters for Internet which connects to the WAN port of your Access Point. Here you may change the access methods to Statis IP, Dynamic IP, PPPoE, or PPTP by clicking the item value of Internet Connection Type.

Mode: ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP

3-5-2 DNS

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose "specify" and enter in your values.



DNS

This page allows you assign DNS Server IP address.

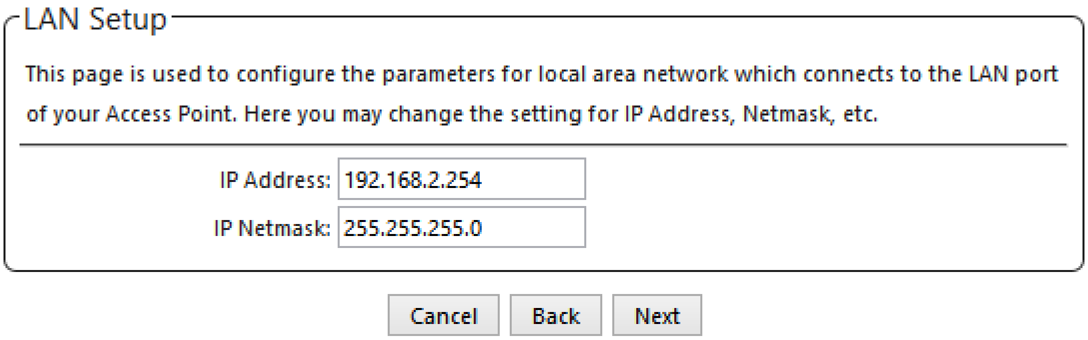
DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

Secondary DNS:

3-5-3 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254



LAN Setup

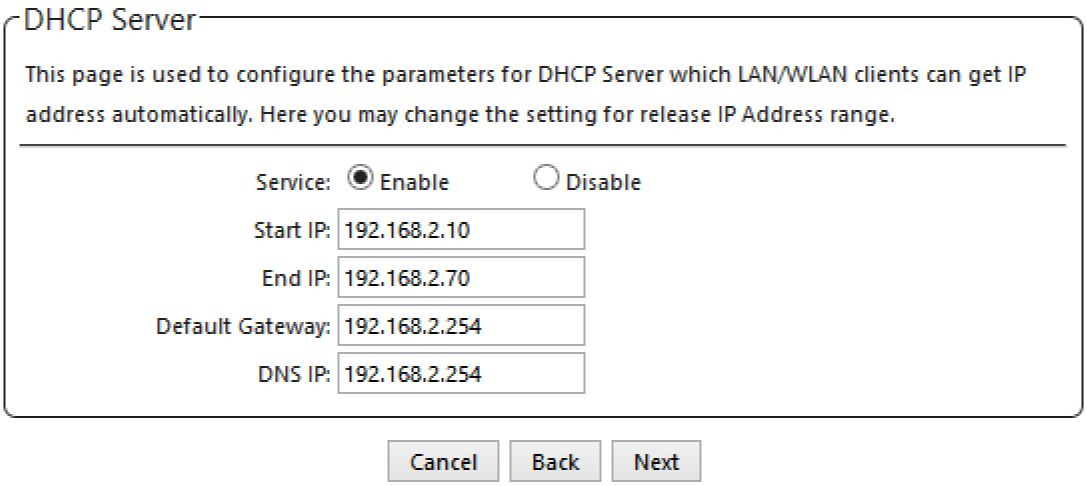
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP Address, Netmask, etc.

IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

3-5-4 DHCP Server

In this mode, by default, IP addresses will be assigned to any LAN/WLAN clients that are connected to the device. You can disable this feature. By default, DHCP is enabled and the IP range is 192.168.2.10 – 192.168.2.70



DHCP Server

This page is used to configure the parameters for DHCP Server which LAN/WLAN clients can get IP address automatically. Here you may change the setting for release IP Address range.

Service: ● Enable ○ Disable

Start IP: 192.168.2.10

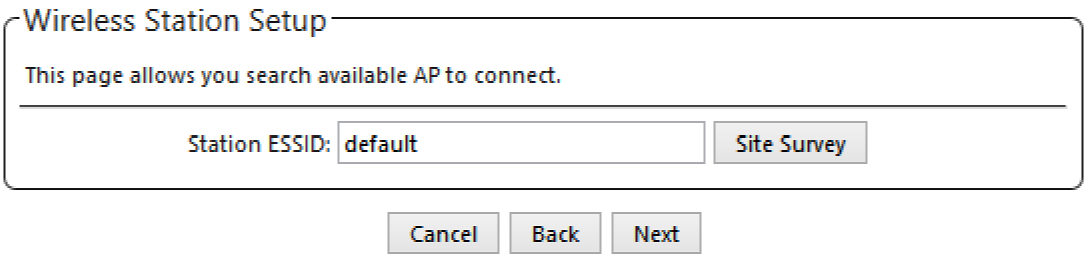
End IP: 192.168.2.70

Default Gateway: 192.168.2.254

DNS IP: 192.168.2.254

3-5-5 Wireless Station Setup

This page allows you to search for an available Wireless Network to Connect



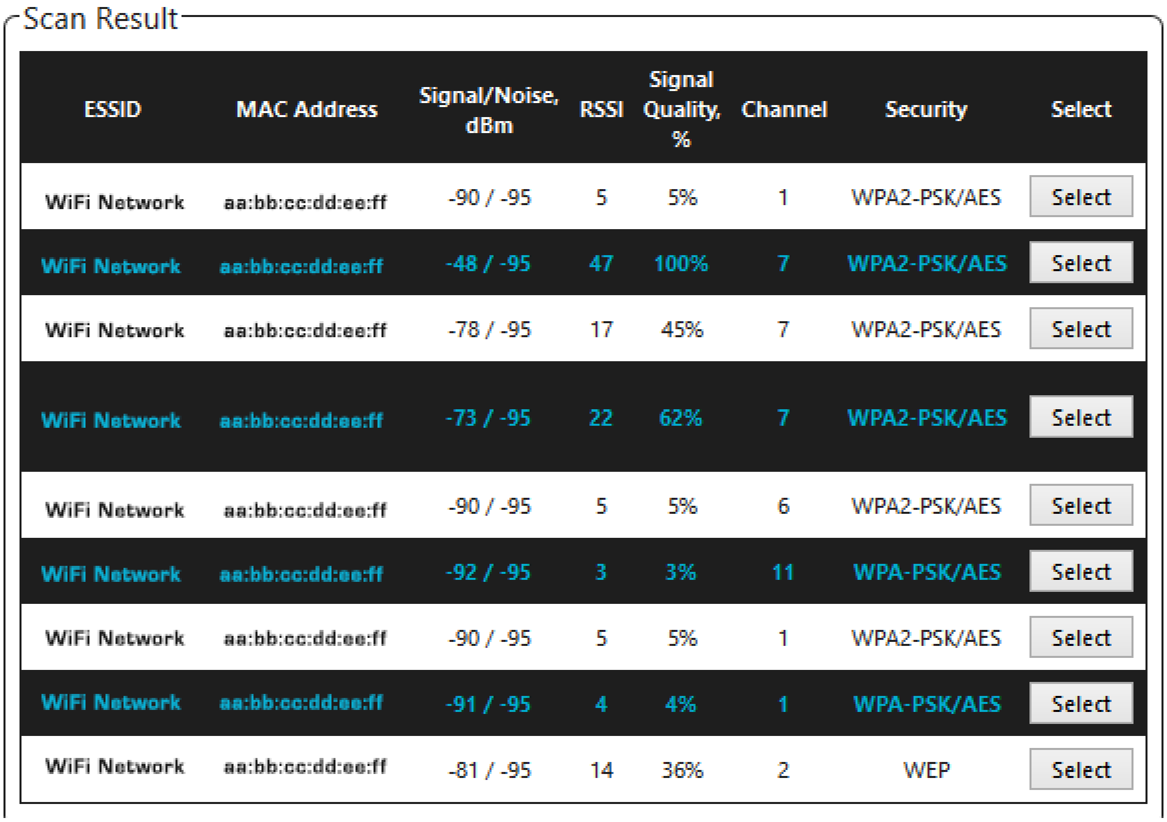
Wireless Station Setup

This page allows you search available AP to connect.

Station ESSID: default

Station ESSID: *Wireless Name of the network you wish to connect to. You can manually enter the name or click on "Site Survey" for the device to scan for wireless networks.*

Site Survey: *Press this button for the device to automatically scan for wireless networks*



Scan Result

ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-48 / -95	47	100%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-78 / -95	17	45%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-73 / -95	22	62%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	6	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-92 / -95	3	3%	11	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-91 / -95	4	4%	1	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-81 / -95	14	36%	2	WEP	Select

Site Survey Results

ESSID: Available Extend Service Set ID (wireless name) of surrounding Access Points.

MAC Address: MAC addresses of surrounding Access Points.

Signal/Noise dBm: Received signal strength of all found Access Points.

RSSI: Indicate the RSSI of the respective client's association.

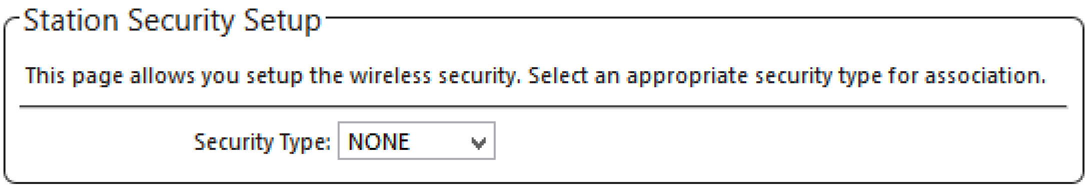
Signal Quality (%): Received signal strength of all found Access Points.

Channel: Channel numbers used by all found Access Points.

Security: Security type by all found Access Points.

3-5-5-1 Disable wireless security

This means the network you are choosing has no security enabled at all. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



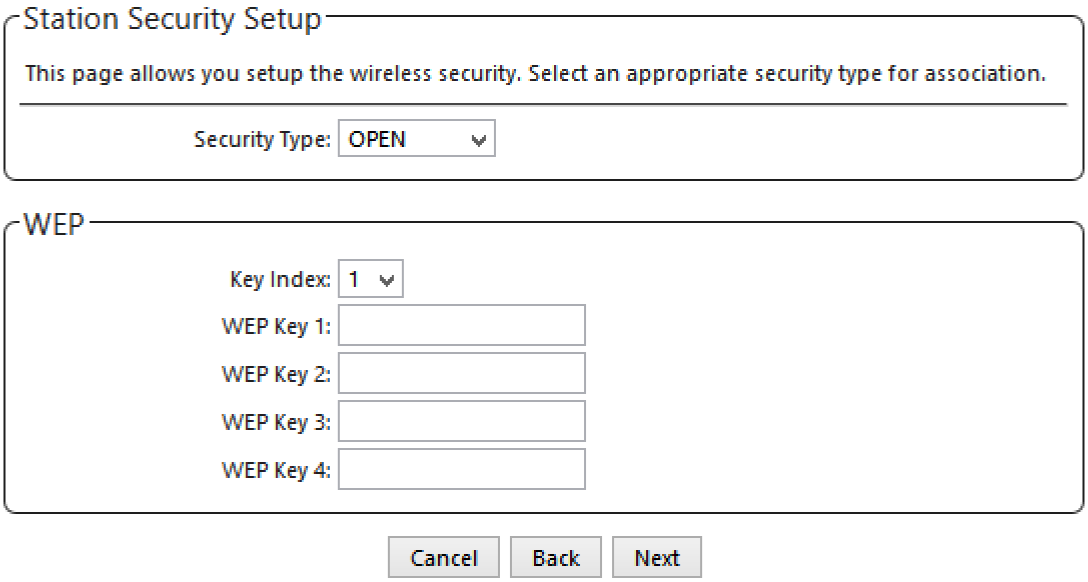
Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: NONE

3-5-5-2 WEP - Wired Equivalent Privacy (Open/Shared)

When you select this mode, the wireless access point you are connecting to is using WEP encryption. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: OPEN

WEP

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

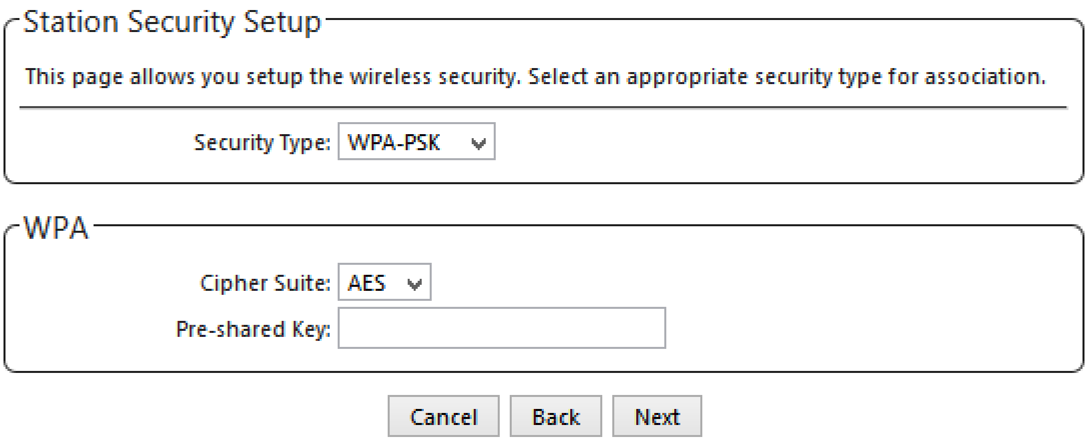
Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-5-5-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point you are connecting to is using WPA encryption. If you are unsure what kind of security the remote network is using, please contact the site administrator since this is unique to that network.



Station Security Setup

This page allows you setup the wireless security. Select an appropriate security type for association.

Security Type: WPA-PSK

WPA

Cipher Suite: AES

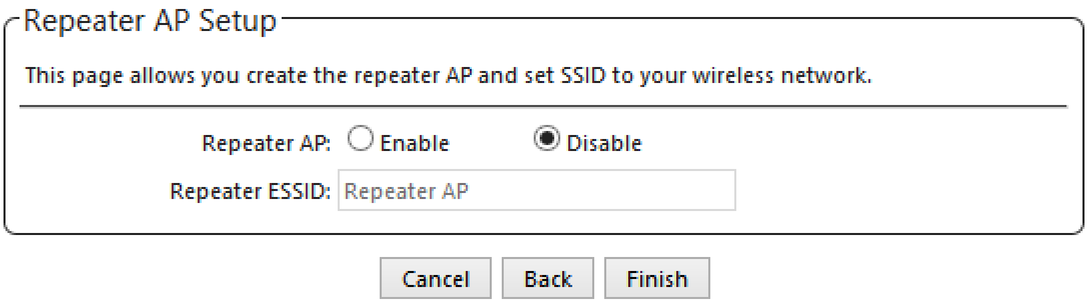
Pre-shared Key:

Cipher Suite: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Pre-shared Keyu\ Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters

3-5-7 Repeater AP Setup

This allows you to create a repeater AP and set SSID to your wireless network. Enable this if you want the device to act as a wireless repeater. If your choose disable, the device will be configured as a client bridge. If you click enable, you can set the settings for the repeater.



Repeater AP Setup

This page allows you create the repeater AP and set SSID to your wireless network.

Repeater AP: ○ Enable ● Disable

Repeater ESSID: Repeater AP

Repeater AP: Enable if you wish to use the repeater function, disable if you wish to use the device in client-bridge mode.

Repeater ESSID: Extended Service Set ID. When users are browsing for available wireless networks, this is the SSID that will appear in the list.

3-5-8 Wireless Security

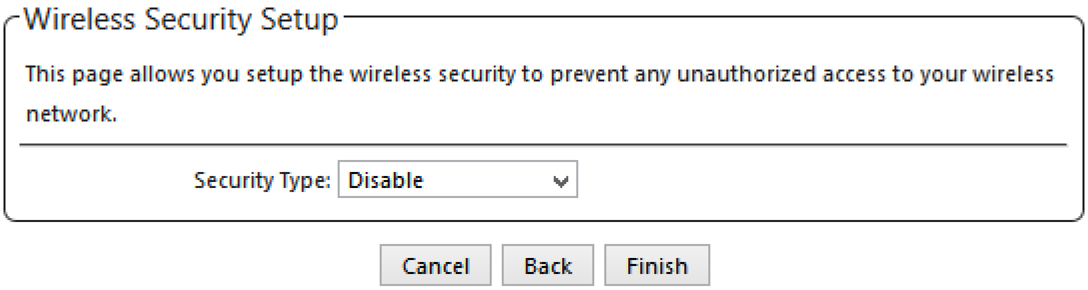
This page allows you to set up wireless security to prevent any unauthorized access to your wireless network.

Next to security type, choose your type of security (Hawking recommends WPA-2PSK)

3-5-8-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.



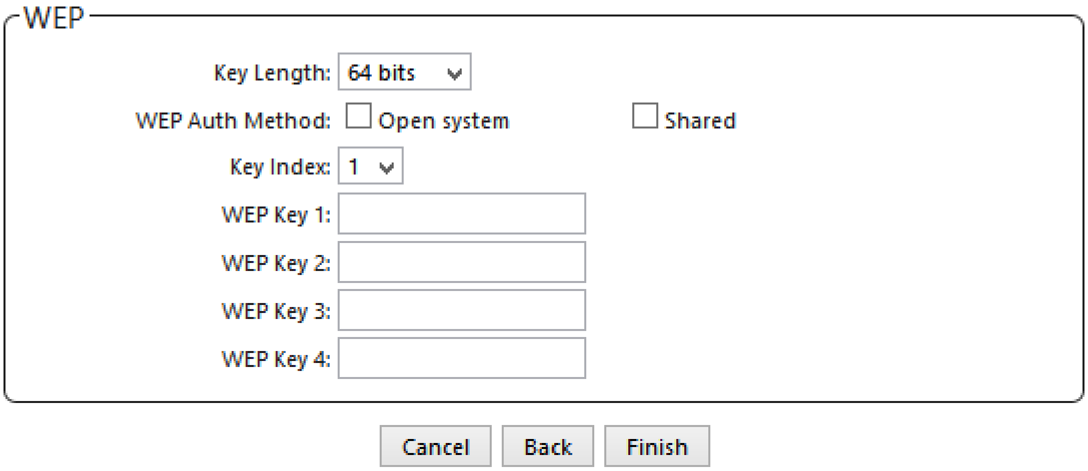
Wireless Security Setup

This page allows you setup the wireless security to prevent any unauthorized access to your wireless network.

Security Type: Disable

3-5-8-2 WEP - Wired Equivalent Privacy

When you select this mode, the wireless access point will use WEP encryption, and the following setup menu will be shown on your web browser:



WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

Key Length: *There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.*

WEP Auth Method: *Open system - there is no authentication to access AP or wireless NIC*

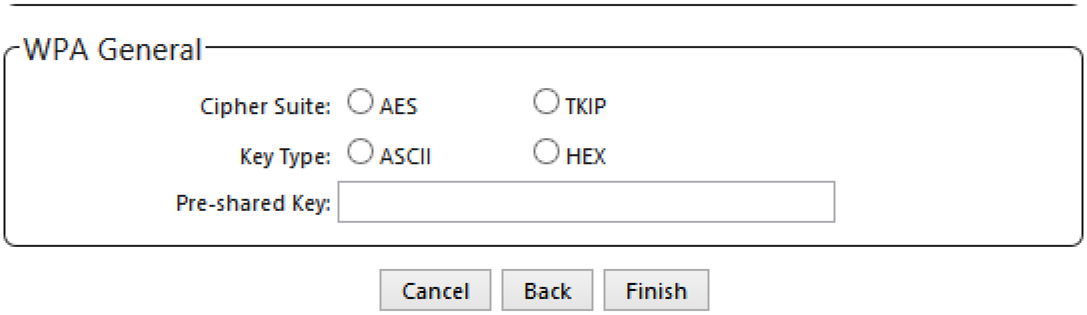
Shared - only those with the same key with the AP can connect to it.

Key Index: *You can set up to four sets of WEP key, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select 'Key 1'.***

WEP Key 1-4: *You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

3-5-8-3 Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



WPA General

Cipher Suite: ○ AES ○ TKIP

Key Type: ○ ASCII ○ HEX

Pre-shared Key:

Cipher Suite: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Key Type *Select the type of pre-shared key, you can select ASCII (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher suite as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, this device will act as a Wireless Internet Service Provider. The device just needs to be powered on via the P-Data Out port on the PoE adapter and can be standalone (you can also connect any wired clients to the 10/100 Data In Port or LAN2). Please change your computer IP address back to "Obtain an IP automatically".

Chapter IV: System Settings

Under this heading, several settings can be changed to configure this device

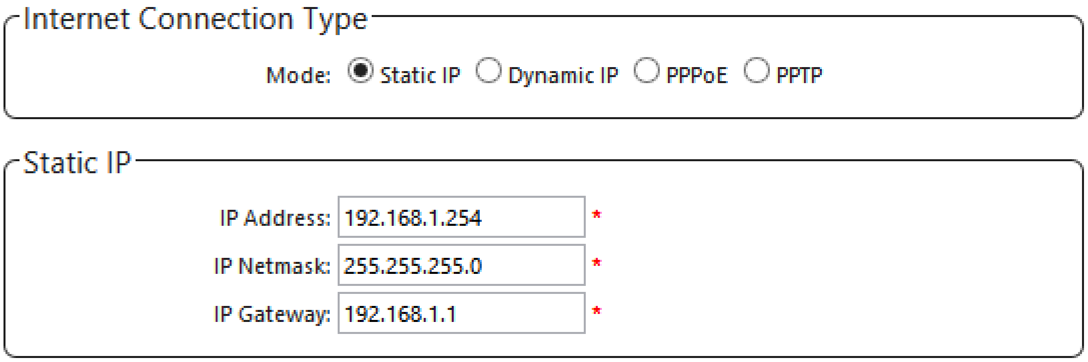
4-1 WAN Setup

Click under system, WAN setup. (This feature is only available under Router AP mode)

4-1-1 Internet Connection Type: Static IP

Static IP users can manually setup the WAN IP w/ a static IP provided by the Internet Service Provider (ISP).

IP Address, IP Netmask (subnet mask), IP Gateway are all provided by the ISP. Contact them if you are not sure.



Internet Connection Type

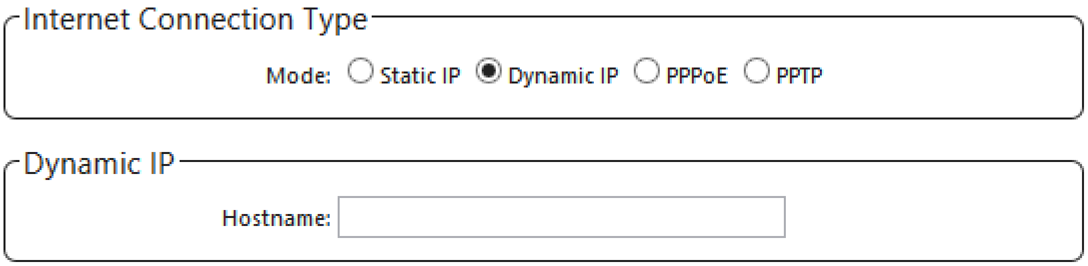
Mode: ● Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

Static IP

IP Address:	192.168.1.254 *
IP Netmask:	255.255.255.0 *
IP Gateway:	192.168.1.1 *

4-1-2 Internet Connection Type: Dynamic IP (Default)

Dynamic IP users receive all their IP, Subnet, Gateway and DNS settings from their ISP. This is the most common setting used.



Internet Connection Type

Mode: ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP

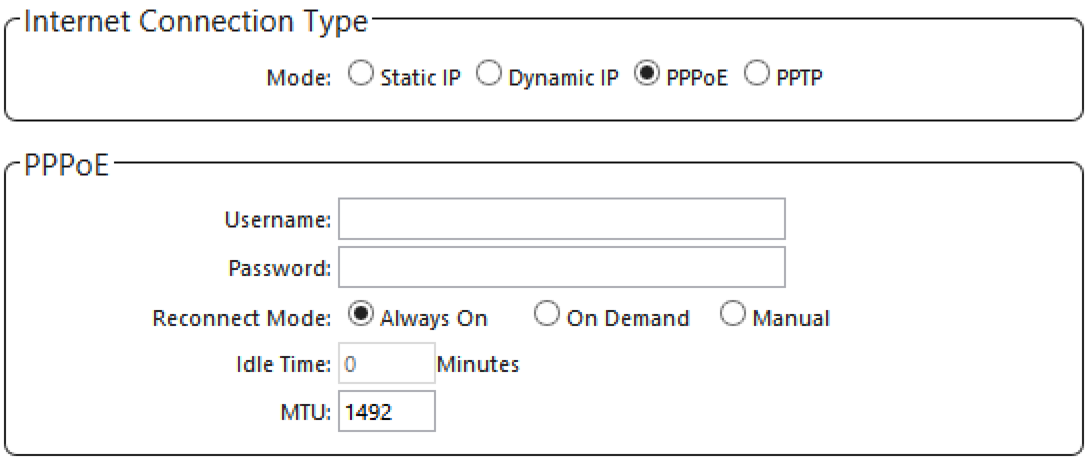
Dynamic IP

Hostname:

Hostname: (optional). If your ISP uses dynamic IP addresses, you may need to enter a hostname provided by the ISP.

4-1-3 Internet Connection Type: PPPoE

PPPoE users need to manually enter their ISP provided username/password. Please contact them if you are not sure.



Internet Connection Type

Mode: ○ Static IP ○ Dynamic IP ● PPPoE ○ PPTP

PPPoE

Username:

Password:

Reconnect Mode: ● Always On ○ On Demand ○ Manual

Idle Time: 0 Minutes

MTU: 1492

Username: *Enter user name for PPPoE connection*

Password: *Enter user name for PPPoE connection.*

Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

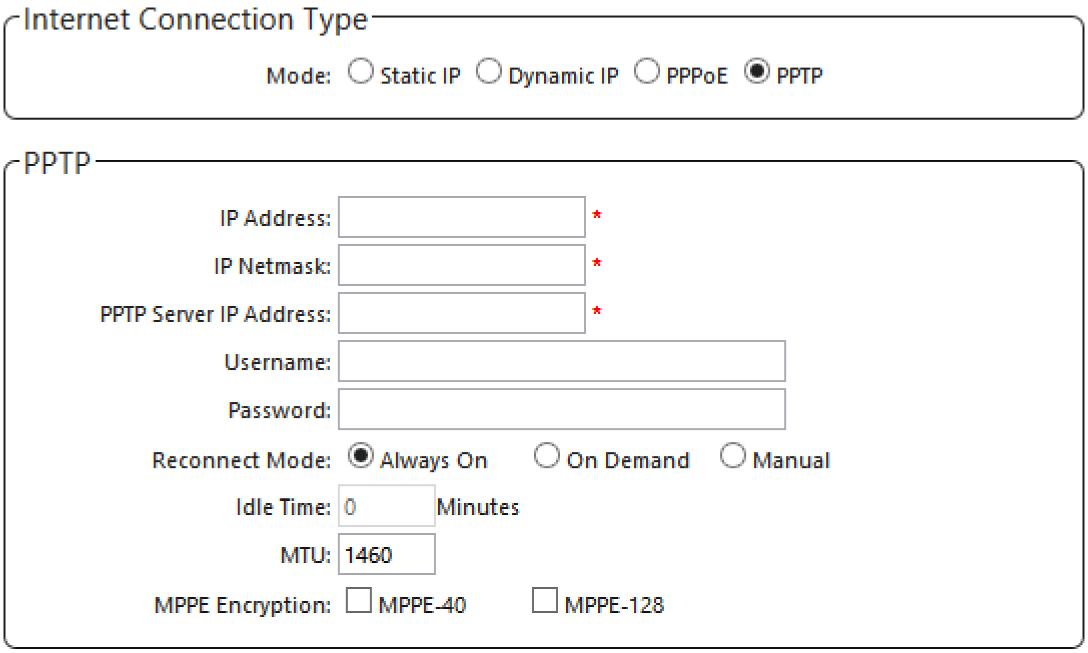
Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

Idle Time: *Time to last before disconnecting PPPoE session when it is idle. Enter preferred idle time in minutes. Default is '0'. When idle time is disabled, the reconnect mode will be set to "Always on"*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

4-1-4 Internet Connection Type: PPTP

The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPN) through public networks.



Internet Connection Type

Mode: ○ Static IP ○ Dynamic IP ○ PPPoE ● PPTP

PPTP

IP Address: *

IP Netmask: *

PPTP Server IP Address: *

Username:

Password:

Reconnect Mode: ● Always On ○ On Demand ○ Manual

Idle Time: 0 Minutes

MTU: 1460

MPPE Encryption: □ MPPE-40 □ MPPE-128

IP Address: *The IP address of the WAN port*

IP Netmask (Subnet): *The subnet mask of the WAN port*

PPTP Server IP address: *The IP address of the PPTP server*

Username: *Username of the PPTP connection*

Password: *Password of the PPTP connection*

Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

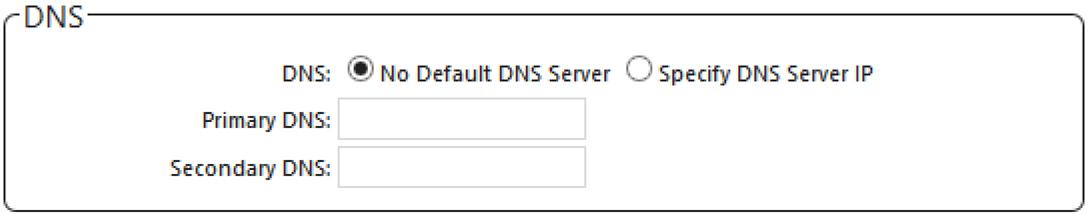
Idle Time: *Time to last before disconnecting PPPoE session when it is idle. Enter preferred idle time in minutes. Default is '0'. When idle time is disabled, the reconnect mode will be set to "Always on"*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

MPPE Encryption: *Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections.* ***128-bit*** *key (strong) and* ***40-bit*** *key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.*

4-1-5 DNS

Check “No default DNS server” (default) or “Specify a DNS server IP” to setup a system DNS.



DNS

DNS: ● No Default DNS Server ○ Specify DNS Server IP

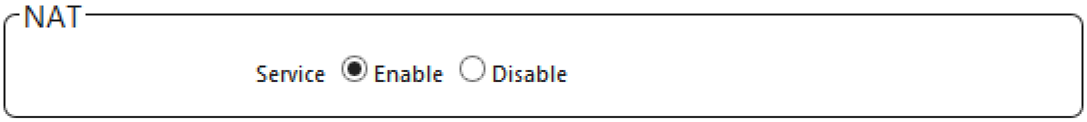
Primary DNS:

Secondary DNS:

Primary: *The IP Address of the Primary DNS server*

Secondary: *The IP address of the secondary DNS server*

4-1-6 NAT



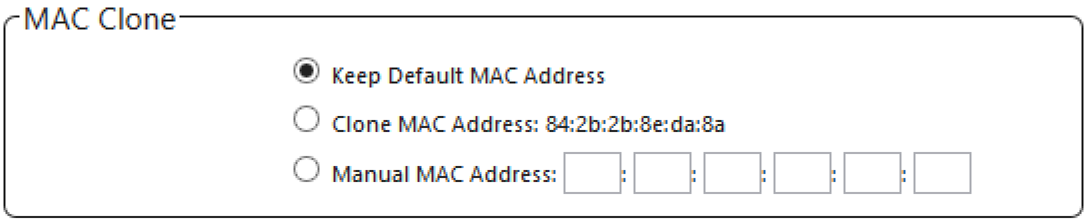
NAT

Service ● Enable ○ Disable

NAT support enabled/disabled. By default, enabled

4-1-7 MAC Clone

The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



MAC Clone

● Keep Default MAC Address

○ Clone MAC Address: 84:2b:2b:8e:da:8a

○ Manual MAC Address: __ : __ : __ : __ : __ : __

Keep Default MAC Address: *Keep the default MAC address of WAN port on the system.*

Clone MAC Address: *If you want to clone the MAC address of the PC, then click the Clone MAC Address button. The system will automatically detect your PC's MAC address.*

Manual MAC Address: *Enter the MAC address registered with your ISP.*

The Clone MAC Address field will display MAC address of the PC connected to system. Click “Save” button can make clone MAC effective.

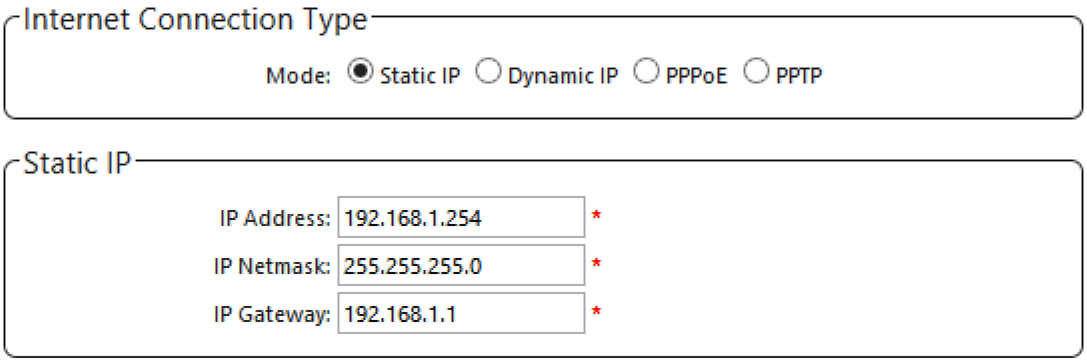
4-2 CPE (WISP) Setup

Click under system, CPE Setup. (This feature is only available under CPE + Repeater AP mode)

4-2-1 Internet Connection Type: Static IP

Static IP users can manually setup the WAN IP w/ a static IP provided by the Internet Service Provider (ISP).

IP Address, IP Netmask (subnet mask), IP Gateway are all provided by the ISP. Contact them if you are not sure



Internet Connection Type

Mode: ● Static IP ○ Dynamic IP ○ PPPoE ○ PPTP

Static IP

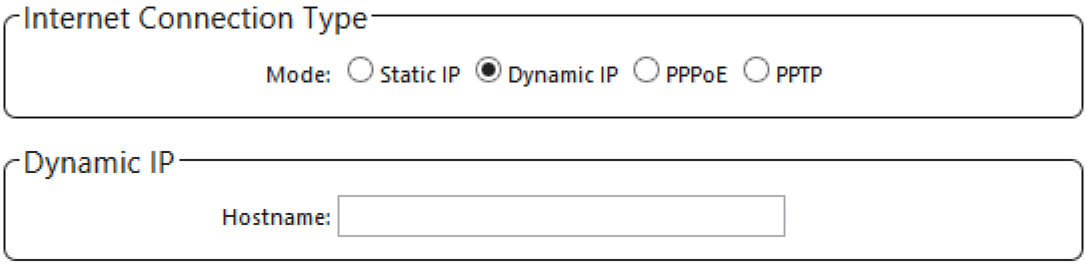
IP Address: 192.168.1.254 *

IP Netmask: 255.255.255.0 *

IP Gateway: 192.168.1.1 *

4-2-2 Internet Connection Type: Dynamic IP (Default)

Dynamic IP users receive all their IP, subnet, gateway and DNS settings from their ISP. This is the most common setting used.



Internet Connection Type

Mode: ○ Static IP ● Dynamic IP ○ PPPoE ○ PPTP

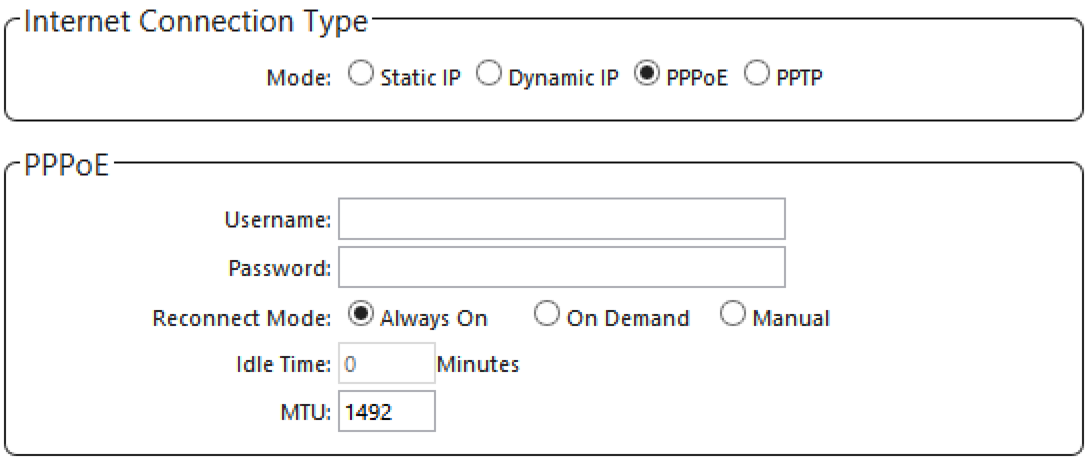
Dynamic IP

Hostname:

Hostname: (optional). If your ISP uses dynamic IP addresses, you may need to enter a hostname provided by the ISP)

4-2-3 Internet Connection Type: PPPoE

PPPoE users need to manually enter their ISP provided username/password. Please contact them if you are not sure.



Internet Connection Type

Mode: ○ Static IP ○ Dynamic IP ● PPPoE ○ PPTP

PPPoE

Username:

Password:

Reconnect Mode: ● Always On ○ On Demand ○ Manual

Idle Time: 0 Minutes

MTU: 1492

Username: *Enter user name for PPPoE connection*

Password: *Enter user name for PPPoE connection.*

Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

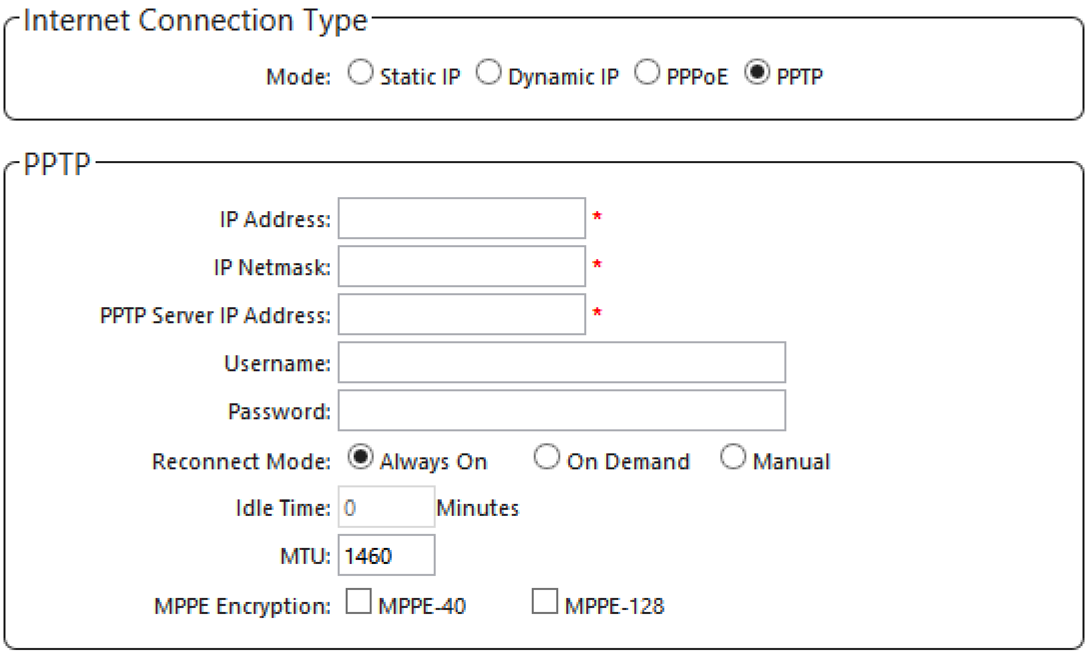
Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

Idle Time: *Time to last before disconnecting PPPoE session when it is idle. Enter preferred idle time in minutes. Default is '0'. When idle time is disabled, the reconnect mode will be set to "Always on"*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

4-2-4 Internet Connection Type: PPTP

The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPN) through public networks.



Internet Connection Type

Mode: ○ Static IP ○ Dynamic IP ○ PPPoE ● PPTP

PPTP

IP Address: *

IP Netmask: *

PPTP Server IP Address: *

Username:

Password:

Reconnect Mode: ● Always On ○ On Demand ○ Manual

Idle Time: 0 Minutes

MTU: 1460

MPPE Encryption: □ MPPE-40 □ MPPE-128

IP Address: *The IP address of the WAN port*

IP Netmask (Subnet): *The subnet mask of the WAN port*

PPTP Server IP address: *The IP address of the PPTP server*

Username: *Username of the PPTP connection*

Password: *Password of the PPTP connection*

Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

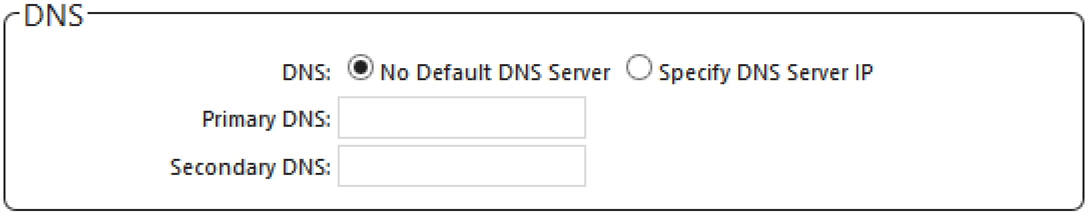
Idle Time: *Time to last before disconnecting PPPoE session when it is idle. Enter preferred idle time in minutes. Default is '0'. When idle time is disabled, the reconnect mode will be set to "Always on"*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

MPPE Encryption: *Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections.* ***128-bit*** *key (strong) and* ***40-bit*** *key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.*

4-2-5 DNS

Check “No default DNS server” (default) or “Specify a DNS server IP” to setup a system DNS.



DNS

DNS: ● No Default DNS Server ○ Specify DNS Server IP

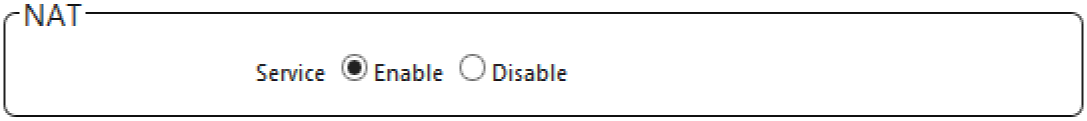
Primary DNS:

Secondary DNS:

Primary:	*The IP Address of the Primary DNS server*
Secondary:	*The IP address of the secondary DNS server*

4-2-6 NAT

NAT support enabled/disabled. By default, enabled

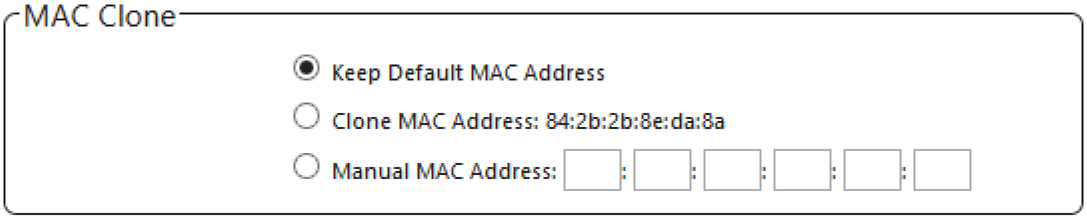


NAT

Service ● Enable ○ Disable

4-2-7 MAC Clone

The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



MAC Clone

● Keep Default MAC Address

○ Clone MAC Address: 84:2b:2b:8e:da:8a

○ Manual MAC Address: : : : : :

Keep Default MAC Address:	*Keep the default MAC address of WAN port on the system.*
Clone MAC Address:	*If you want to clone the MAC address of the PC, then click the Clone MAC Address button. The system will automatically detect your PC's MAC address.*
Manual MAC Address:	*Enter the MAC address registered with your ISP.*

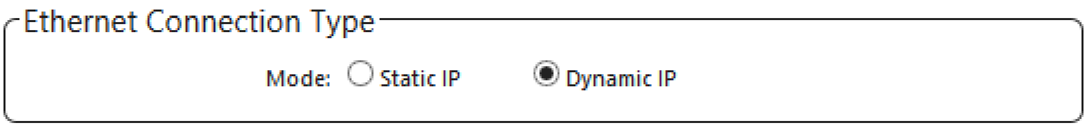
The Clone MAC Address field will display MAC address of the PC connected to system. Click “Save” button can make clone MAC effective.

4-3 LAN Setup

Click under system, LAN Setup

4-3-1 LAN IP Setup

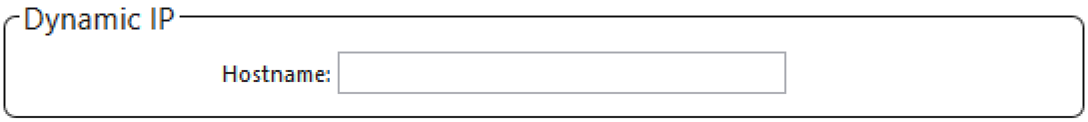
The administrator can set it to obtain (Dynamic IP) an IP automatically or manually setup (Static IP) the LAN IP address of the device.



Ethernet Connection Type

Mode: ○ Static IP ● Dynamic IP

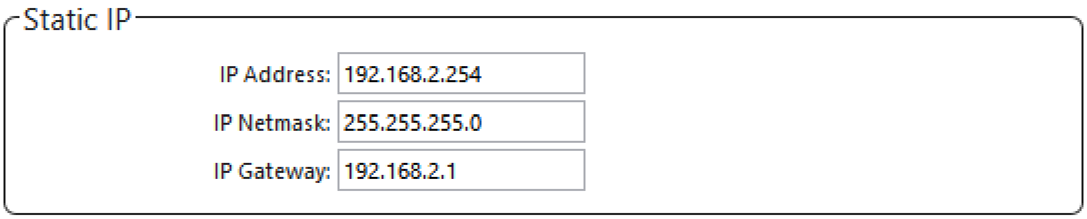
If you select Dynamic IP, you can input your host name (if required)



Dynamic IP

Hostname:

If you Static IP, you can enter in your settings here:



Static IP

IP Address: 192.168.2.254

IP Netmask: 255.255.255.0

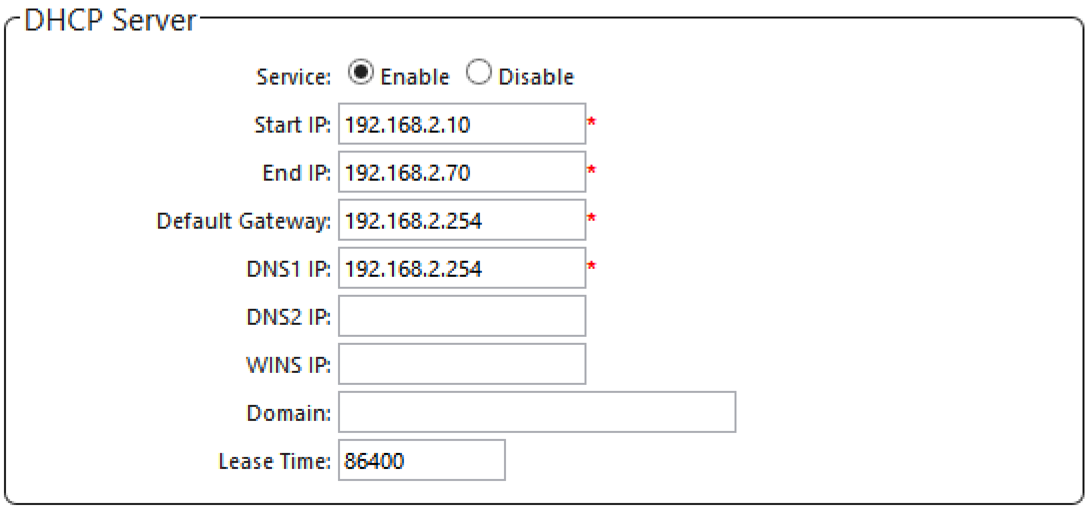
IP Gateway: 192.168.2.1

IP Address: *The IP address of the LAN port; default IP address is 192.168.2.254*

IP Netmask: *The Subnet mask of the LAN port; default Netmask is 255.255.255.0*

4-3-2 DHCP Setup

Devices connected to the system can obtain an IP address automatically when this service is enabled. (This feature is only available in Router AP, ClientBridge + Repeater AP and CPE + Repeater AP Modes)



DHCP Server

Service: ● Enable ○ Disable

Start IP: 192.168.2.10 *

End IP: 192.168.2.70 *

Default Gateway: 192.168.2.254 *

DNS1 IP: 192.168.2.254 *

DNS2 IP:

WINS IP:

Domain:

Lease Time: 86400

DHCP: *Check Enable button to activate this function or Disable to deactivate this service.*

Start IP / End IP: *Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0*

DNS1 IP: *Enter IP address of the first DNS server; this field is required.*

DNS2 IP: *Enter IP address of the second DNS server; this is optional.*

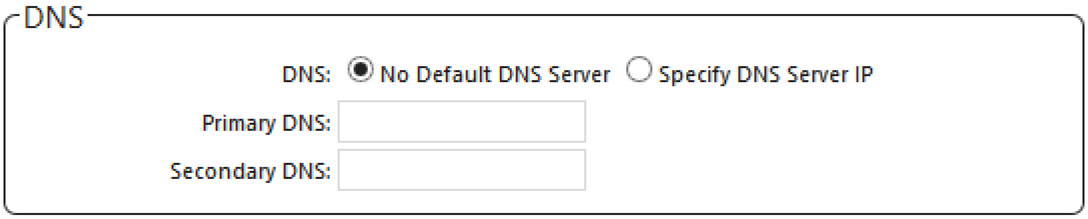
WINS IP: *Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.*

Domain: *Enter the domain name for this network.*

Lease Time: *The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is 86400 seconds*

4-3-3 DNS

Check "No default DNS server" (default) or "Specify a DNS server IP" to setup a system DNS. (This feature is only available in AP Mode, WDS Mode and ClientBridge + Repeater AP Mode)



DNS

DNS: ● No Default DNS Server ○ Specify DNS Server IP

Primary DNS:

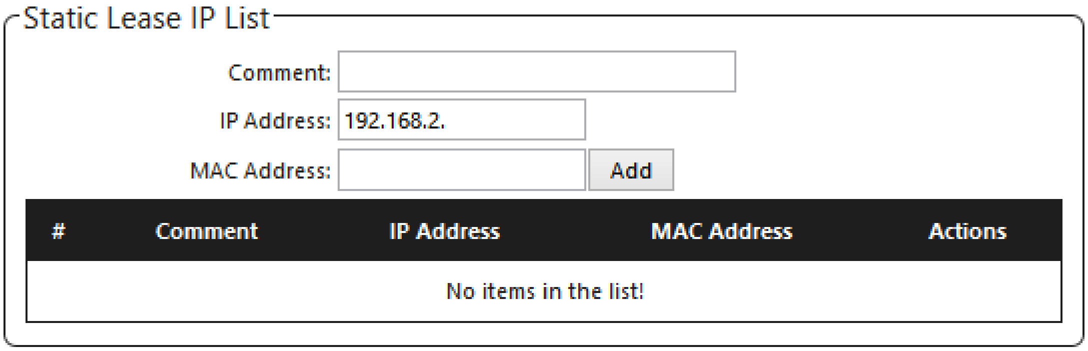
Secondary DNS:

Primary: *The IP Address of the Primary DNS server*

Secondary: *The IP address of the secondary DNS server*

4-3-4 Static Lease IP List

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still enjoy the benefit of using DHCP server. (This feature is only available in Router AP, ClientBridge + Repeater AP and CPE + Repeater AP Modes)



Static Lease IP List

Comment:

IP Address: 192.168.2.

MAC Address:

#	Comment	IP Address	MAC Address	Actions
No items in the list!				

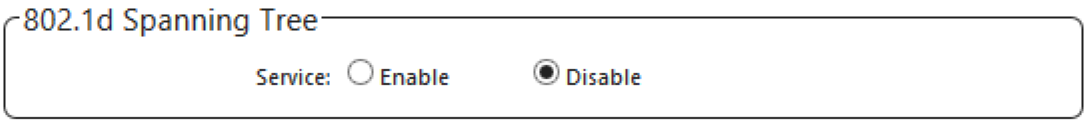
Comment: *You can enter a comment, for reference to the IP address you assigned. Ie "work computer, Living Room, etc.*

IP Address: *Input the IP address you want to assign to this computer or network device*

Mac Address: *Input the MAC address of the computer or network device (total 12 characters, with character from 0 to 9, and from a to f, like '001122aabbcc') Click "Add" to add the IP list to the table below.*

4-3-5 802.1d Spinning Tree

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. (This feature is only available in AP Mode, WDS Mode and ClientBridge + Repeater AP Mode, CPE + Repeater AP Mode)

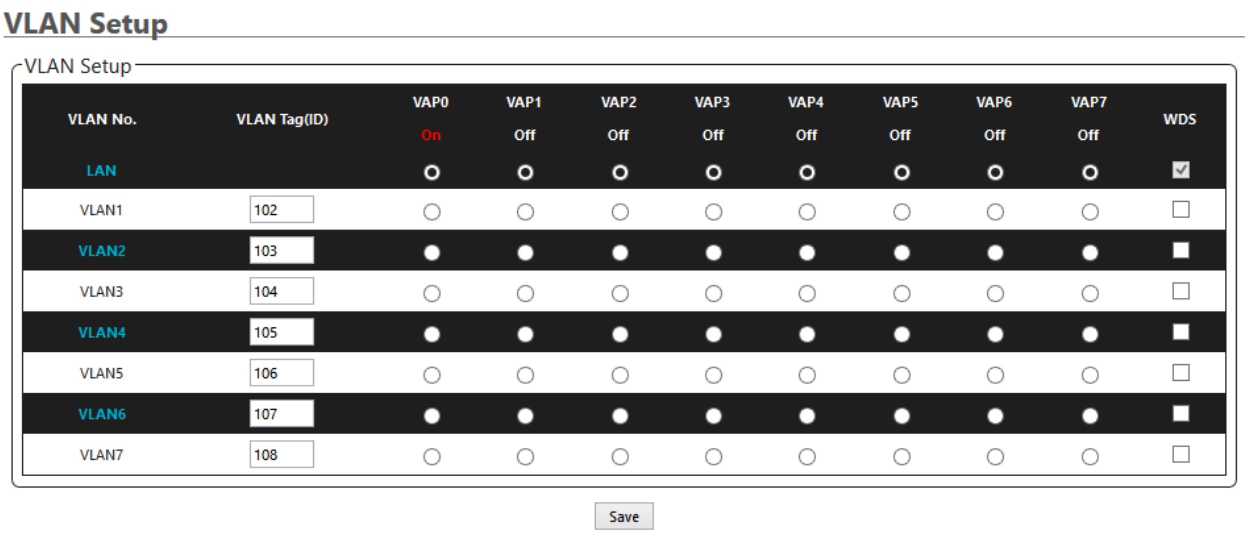


802.1d Spanning Tree

Service: ○ Enable ● Disable

4-4 VLAN Setup

The VLAN setup is used to configure VLANs. Click under System, LAN Setup. (This feature is only available in Router AP, AP and WDS Modes)



VLAN Setup

VLAN Setup

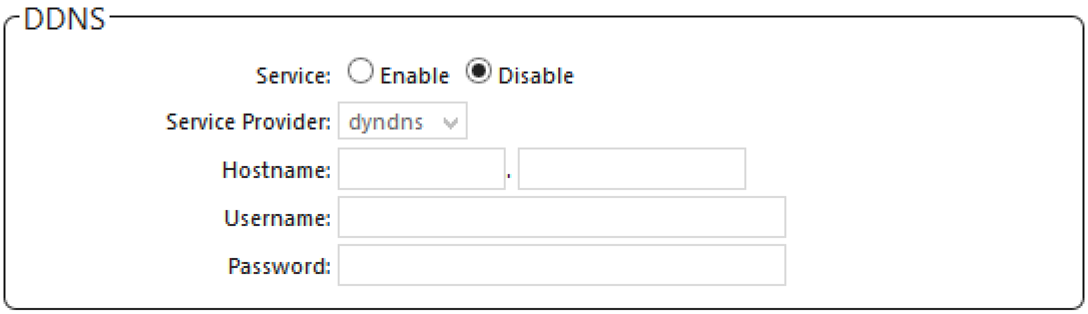
VLAN No.	VLAN Tag(ID)	VAP0 On	VAP1 Off	VAP2 Off	VAP3 Off	VAP4 Off	VAP5 Off	VAP6 Off	VAP7 Off	WDS
LAN		●	●	●	●	●	●	●	●	☑
VLAN1	102	○	○	○	○	○	○	○	○	□
VLAN2	103	○	○	○	○	○	○	○	○	□
VLAN3	104	○	○	○	○	○	○	○	○	□
VLAN4	105	○	○	○	○	○	○	○	○	□
VLAN5	106	○	○	○	○	○	○	○	○	□
VLAN6	107	○	○	○	○	○	○	○	○	□
VLAN7	108	○	○	○	○	○	○	○	○	□

VLAN No: *Number of VLANs (8 supported)*

VLAN Tag (ID): *Provide a number between 1 and 4094 for internal VLAN*

4-5 DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address. Click under Setup, DDNS. (This feature is only available in Router AP and CPE + Repeater AP Modes)



DDNS

Service: ○ Enable ● Disable

Service Provider: dyndns

Hostname: .

Username:

Password:

Enabled/Disabled: *By default, it is set to Disabled. The mapping domain name will not change when dynamic IP changes.*

Service Provider: *Select the preferred Service Provider from the drop-down list including dyndns, dhs, ods and tzo*

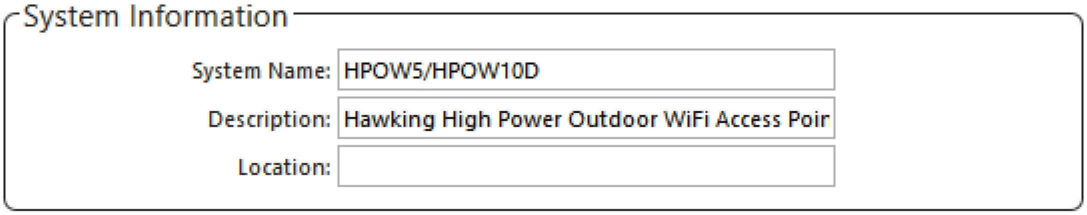
Hostname: *Host Name that you register to Dynamic-DNS service and export.*

User Name & Password: *User Name and Password of the DDNS service.*

4-6 Management Setup

Administrators can setup system info, passwords and login methods. Click under System, Management

4-6-1 System Information System



System Information

System Name: HPOW5/HPOW10D

Description: Hawking High Power Outdoor WiFi Access Poir

Location:

Name: *Enter a desired name or use the default one.*

Description: *Provide description of the system.*

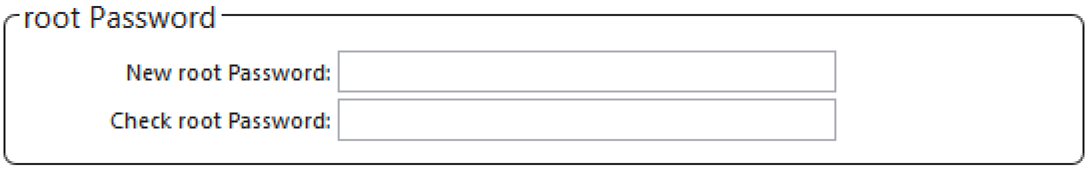
Location: *Enter geographical location information of the system.*

4-6-2 Passwords

The system supports two management accounts, root and admin. Root accounts are assigned full administrative privileges to manage the system in all aspects. While logging in as an admin user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own.

4-6-2-1 Root Password:

Full administrative rights and access to all aspects of the configuration



root Password

New root Password:

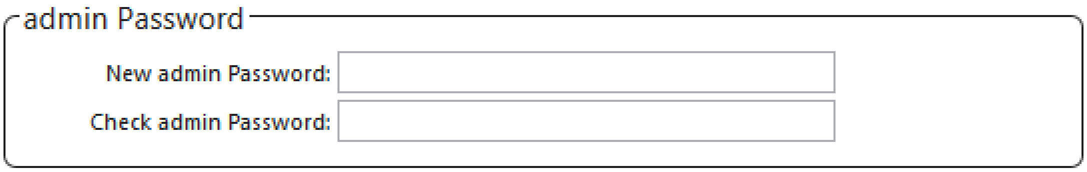
Check root Password:

New Password: *Enter a new password if desired*

Check New Password: *Enter the same new password again*

4-6-2-2 Admin Password:

Basic access to the settings



admin Password

New admin Password:

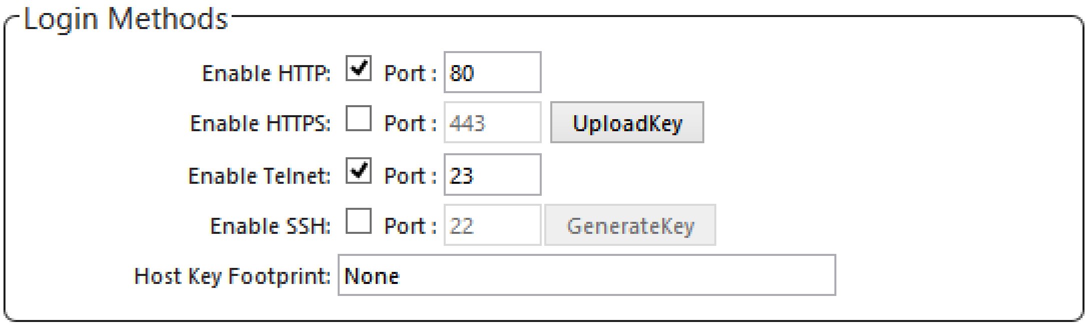
Check admin Password:

New Password: *Enter a new password if desired*

Check New Password: *Enter the same new password again*

4-6-3 Admin Login Methods:

Only root user can enable or disable system login methods and change services port.



Login Methods

Enable HTTP: ☑ Port : 80

Enable HTTPS: □ Port : 443

Enable Telnet: ☑ Port : 23

Enable SSH: □ Port : 22

Host Key Footprint: None

Enable HTTP: *Check to select HTTP Service.*

Enable HTTPS: *Check to select HTTPS Service*

HTTPS Port: *The default is 443 and the range is between 1 ~ 65535.*

If you already have an SSL Certificate, please click "Upload Key" button to select the file and upload it.

Enable Telnet: *Check to select Telnet Service*

Telnet Port : *The default is 23 and the range is between 1 ~ 65535*

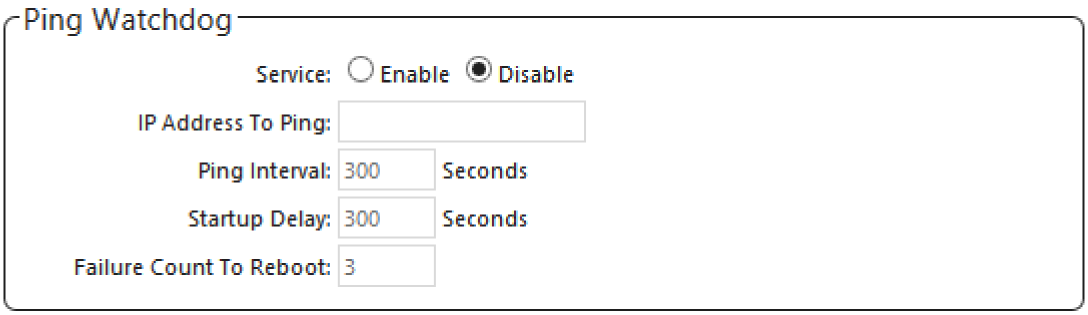
Enable SSH: *Check to select SSH Service*

SSH Port : *Please The default is 22 and the range is between 1 ~ 65535.*

Click "Generate Key" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.

4-6-4 Ping Watchdog

The ping watchdog feature continuously pings a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the device will automatically reboot. This option creates a "fail-proof" mechanism. Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.



Ping Watchdog

Service: ○ Enable ● Disable

IP Address To Ping:

Ping Interval: 300 Seconds

Startup Delay: 300 Seconds

Failure Count To Reboot: 3

Enable Ping Watchdog: *Control will enable Ping Watchdog Tool.*

IP Address To Ping: *Specify an IP address of the target host which will be monitored by Ping Watchdog Tool.*

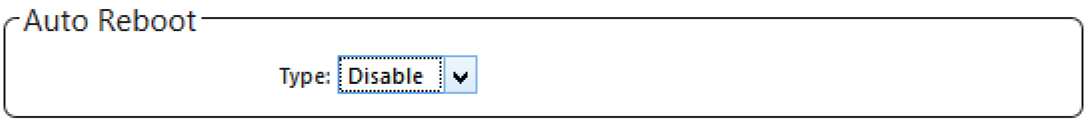
Ping Interval: *Specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is 300 seconds.*

Startup Delay: *Specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is 300 seconds.*

Failure Count To Reboot: *Specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.*

4-6-5 Auto Reboot

The device can be set to auto reboot in a daily, weekly, or monthly setting.

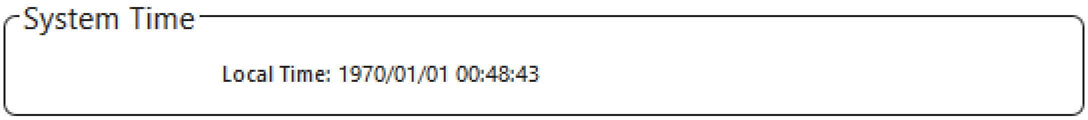


Auto Reboot

Type: Disable

4-7 Time Server Setup

System time can be configured via this page, and manual setting or via a NTP server is supported. Please go to System, Time Server



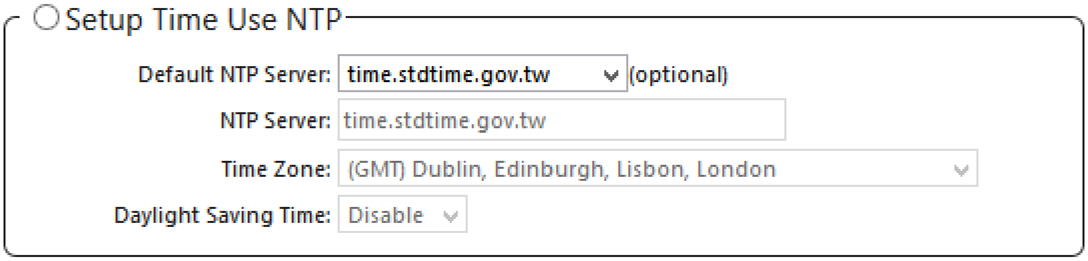
System Time

Local Time: 1970/01/01 00:48:43

Local Time: Display the current system time.

Setup Time Use NTP

Synchronize the system time with NTP server.



○ Setup Time Use NTP

Default NTP Server: time.stdtime.gov.tw (optional)

NTP Server: time.stdtime.gov.tw

Time Zone: (GMT) Dublin, Edinburgh, Lisbon, London

Daylight Saving Time: Disable

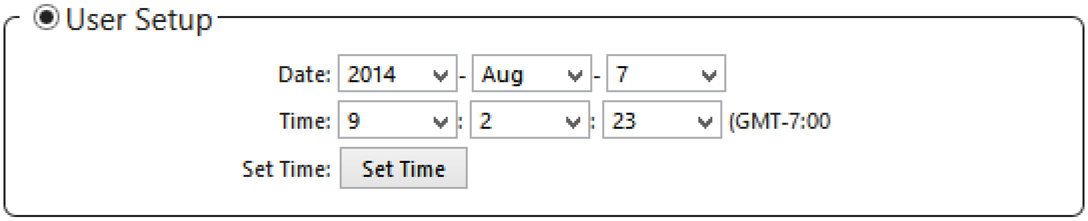
Default NTP Server / NTP Server: *Select the NTP Server from the drop-down list.*

Time Zone: *Select a desired time zone from the drop-down list.*

Daylight saving time: *Enable or disable Daylight saving.*

User Setup

The user can manually set time/date



● User Setup

Date: 2014 - Aug - 7

Time: 9 : 2 : 23 (GMT-7:00

Set Time: Set Time

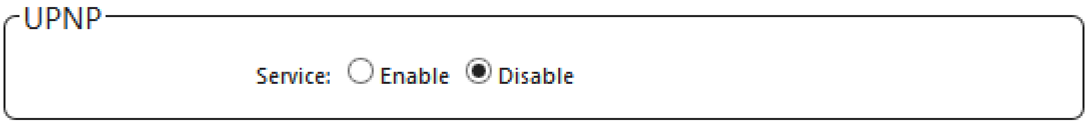
Date: *Set the date for system.*

Time: *Set the time for system.*

4-8 UPNP Setup

Universal Plug and Play (UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on a TCP/IP network to enable UPnP devices to connect and access to each other. You can access the settings by going to System, UPNP. (This feature is only available in Router AP and CPE + Repeater AP Modes)

UPnP is disabled by default. You can enable/disable it on the settings here



UPNP

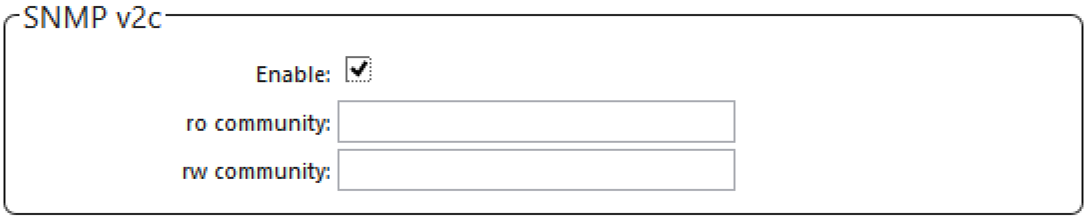
Service: ○ Enable ● Disable

4-9 SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. You can access the settings by going to System, SNMP

SNMP v2c Enable

Check to enable SNMP v2c.



SNMP v2c

Enable: ☑

ro community:

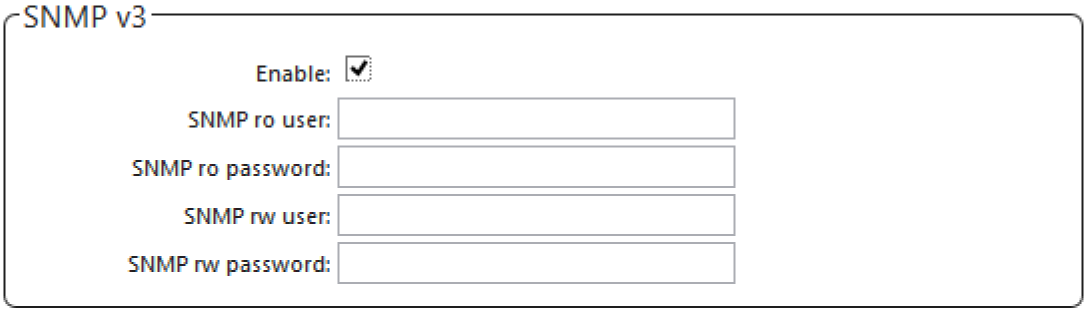
rw community:

ro community: *Set a community string to authorize read-only access.*

rw community: *Set a community string to authorize read/write access.*

SNMP v3 Enable

Check to enable SNMP v3. SNMPv3 supports the highest level SNMP security.



SNMP v3

Enable: ☑

SNMP ro user:

SNMP ro password:

SNMP rw user:

SNMP rw password:

SNMP ro user: *Set a community string to authorize read-only access.*

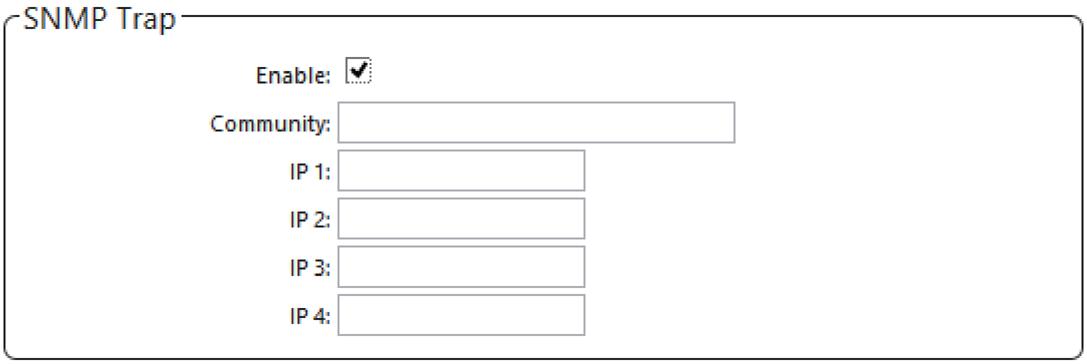
SNMP ro password: *Set a password to authorize read-only access.*

SNMP rw user: *Set a community string to authorize read/write access.*

SNMP rw password: *Set a password to authorize read/write access.*

SNMP Trap

Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Enable: ☑

Community:

IP 1:

IP 2:

IP 3:

IP 4:

Community: *Set a community string required by the remote host computer that will receive trap messages or notices send by the system.*

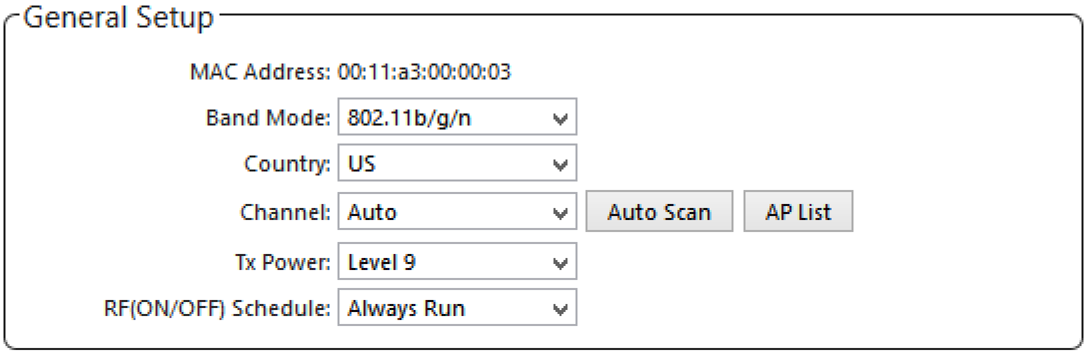
IP (1~4): *Enter the IP addresses of the remote hosts to receive trap messages.*

Chapter V: Wireless Setup

5-1 General Setup

This section allows you to set the data transmission, channel and output power for the system

5-1-1 General Settings



General Setup

MAC Address: 00:11:a3:00:00:03

Band Mode: 802.11b/g/n

Country: US

Channel: Auto

Tx Power: Level 9

RF(ON/OFF) Schedule: Always Run

MAC Address: *The MAC address of the Wireless interface is displayed here.*

Band: *Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.*

*If you select 802.11b only wireless clients using the wireless band you select 802.11b will be able to connect to this access point. (*Maximum transfer rate 11Mbps)

*If you select 802.11b/g, then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. (*Maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients)

If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 802.11b/g/n (Maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*) (Default).*

*If you select 802.11n, the only wireless clients using 802.11n band will be able to connect to this access point. (*Maximum 300Mbps for 802.11n clients)

Country: *This device only supports United States WiFi channels.*

Channel: *Please select a channel from the dropdown list of 'Channel Number', You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there are radio communication conflicts*

By default, it is on AUTO but if you have a specific channel you wish to use, you can select it here.

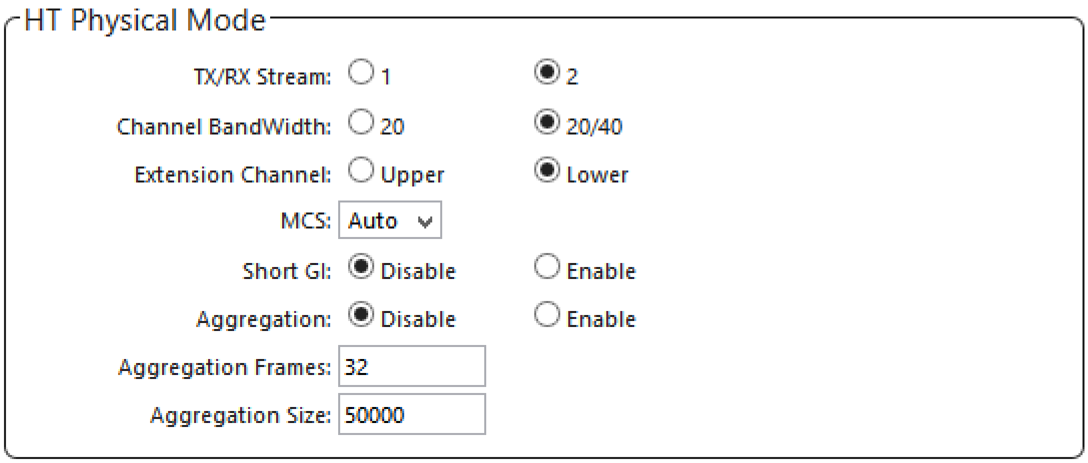
Auto Scan: This function can auto choose the best Channel

AP List: This will show you all wireless networks in the same range as this device.

Tx Power: *You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Specify power levels between level 1 and level 9. Level 9 is the maximum setting.*

RF (ON/OFF) Schedule: *You can set when you want the RF to be on/off according to a Time Policy you set up.*

5-1-2 HT Physical Mode



HT Physical Mode

TX/RX Stream: ○ 1 ● 2

Channel BandWidth: ○ 20 ● 20/40

Extension Channel: ○ Upper ● Lower

MCS: Auto

Short GI: ● Disable ○ Enable

Aggregation: ● Disable ○ Enable

Aggregation Frames: 32

Aggregation Size: 50000

Tx/Rx Stream: *2 is the default setting. Using 1 will halve your speed.*

Channel Bandwidth: *The "20/40" MHz option is usually best. The other option is available for special circumstances.*

Extension Channel: *Only for Channel Bandwidth "40" MHz. Select the desired channel bonding for control.*

MCS: *This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.*

Shout GI: *Short Guard Interval, by default, it's "Enabled" so throughput can be increased. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.*

Aggregation: *By default, it's "Enable". It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.*

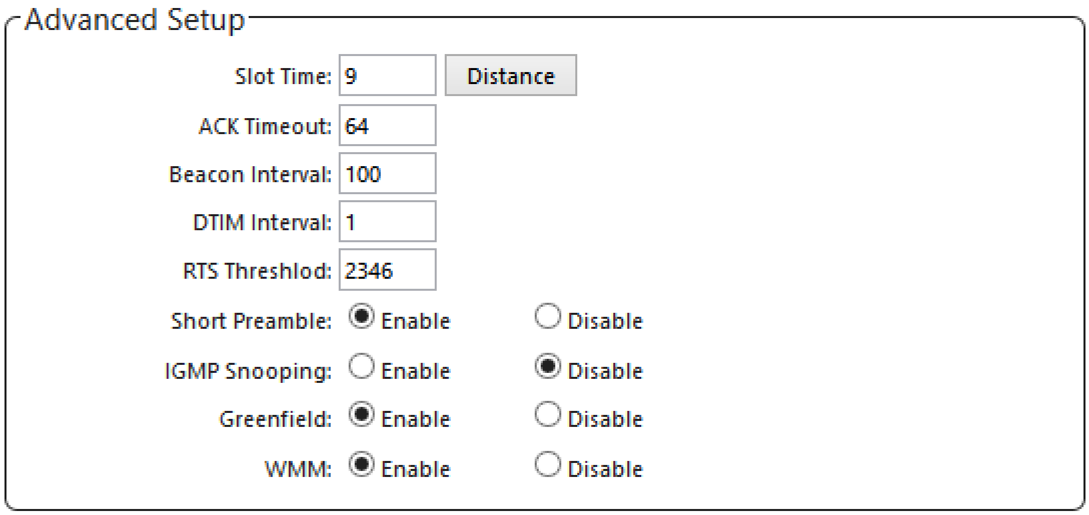
Aggregation Frames: *The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.*

Aggregation Size: *The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.*

5-2 Advanced Settings

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system

5-2-1 Advanced Setup



Advanced Setup

Slot Time: 9 Distance

ACK Timeout: 64

Beacon Interval: 100

DTIM Interval: 1

RTS Threshlod: 2346

Short Preamble: ● Enable ○ Disable

IGMP Snooping: ○ Enable ● Disable

Greenfield: ● Enable ○ Disable

WMM: ● Enable ○ Disable

Slot Time: *Slot time is in the range of 9~1489 and set in units of microsecond. The default value is 9 microsecond. Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN.*

ACK Timeout: *ACK timeout is in the range of 1~372 and set in unit of microsecond. The default value is 64 microsecond. All data transmission in 802.11b/g request an "Acknowledgement" (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as "ACK Timeout". ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to "Resend" packets before ACK is received, and throughput become low due to excessively high re-transmission. ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, If experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.*

Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

Beacon Interval: *Beacon Interval is in the range of 40~3500 and set in unit of millisecond. The default value is 100 msec. Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence* *of such AP, and may proceed to the next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis. The time interval can be adjusted. By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.*

DTIM Interval: *The DTIM interval is in the range of 1~255. The default is 1. DTIM is defined as Delivery Traffic Indication Message. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.*

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

RTS Threshold: *RTS Threshold is in the range of 1~2347 byte. The default is 2347 byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.*

Short Preamble: *By default, its set to "Enabled". If Disabled, the device will use Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.*

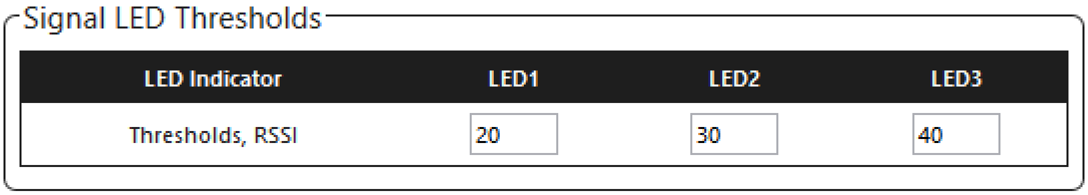
IGMP Snooping: *The process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.*

Greenfield: *In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.*

WMM: *WiFi Multi-Media (WMM) will enhance the data transfer performance of multimedia contents when they are being transferred over a wireless network*

5-2-2 Signal LED Thresholds

(This feature is only available in Client Bridge + Repeater AP and CPE + Repeater AP Modes)


Signal LED Thresholds

LED Indicator	LED1	LED2	LED3
Thresholds, RSSI	20	30	40

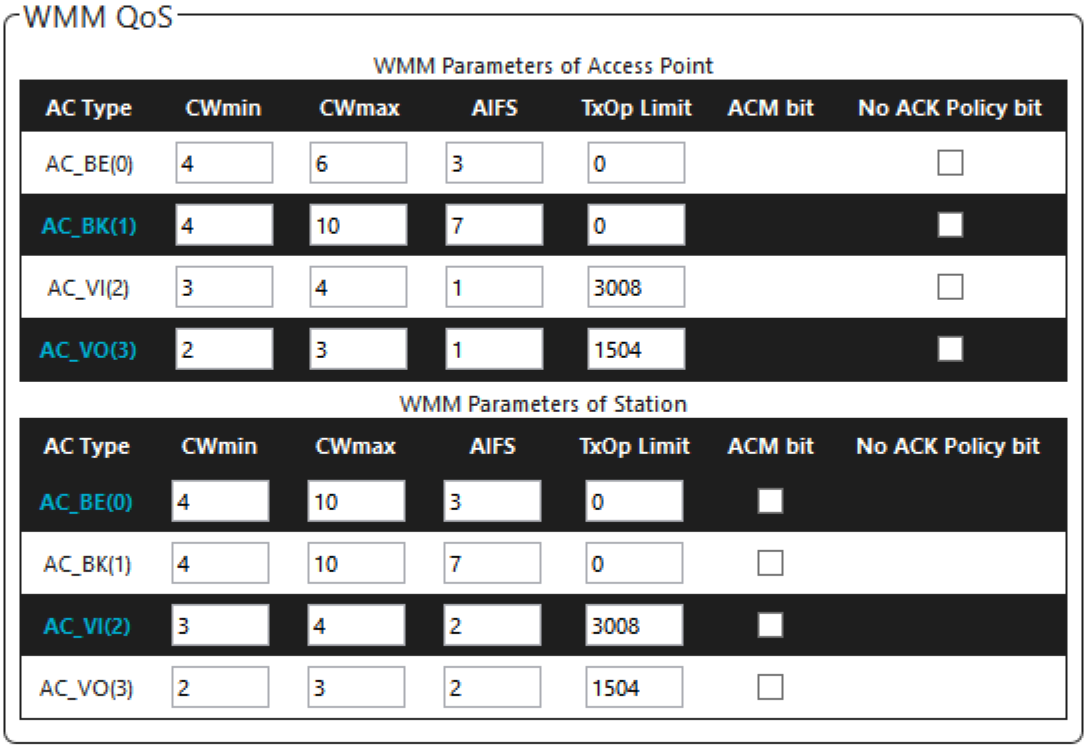
Signal LED Thresholds: *This function can set the RSSI number (1~99) to control the signal LEDs. These will light up the LEDs to show signal strength*

5-2-3 WMM QoS

This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). Medium throughput and delay. Most traditional IP data is sent to this queue. Minimum delay. Time-sensitive video data is automatically sent to this queue. Time-sensitive data like VoIP and streaming media are automatically sent to this queue.



WMM QoS

WMM Parameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	6	3	0		□
AC_BK(1)	4	10	7	0		□
AC_VI(2)	3	4	1	3008		□
AC_VO(3)	2	3	1	1504		□

WMM Parameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit	No ACK Policy bit
AC_BE(0)	4	10	3	0	□	
AC_BK(1)	4	10	7	0	□	
AC_VI(2)	3	4	2	3008	□	
AC_VO(3)	2	3	2	1504	□	

CWmin: *Determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.*

CWmax: *Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".*

AIFS *The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames*

TxOP Limit *Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.*

ACM bit: *Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge*

No ACK policy bit: *Acknowledgment Policy, WMM defines two ACK policies: Normal ACK and No ACK. Click “Checkbox” indicates “No ACK”*

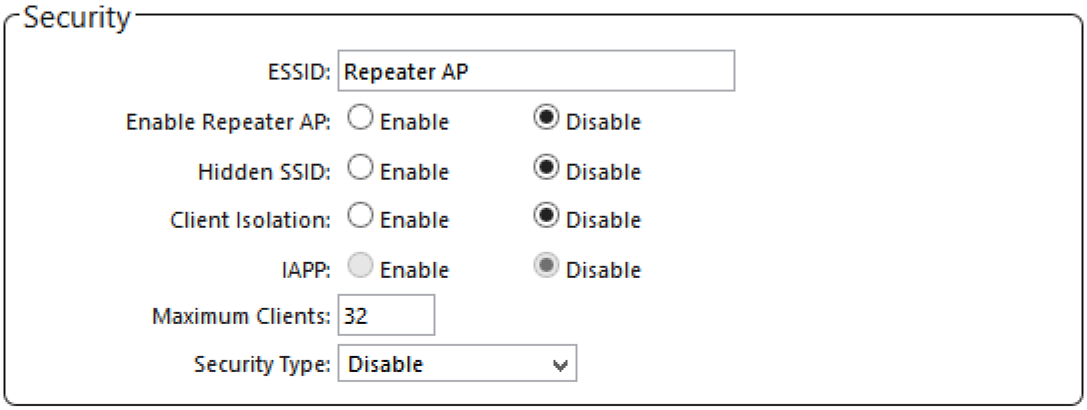
When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received uncast packet.

5-3 Repeater AP setup

The network manager can configure related wireless settings, **AP Setup**, **Security Settings**, and **Access Control Settings**.

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings. (This feature is only available in Client Bridge + Repeater AP and CPE + Repeater AP Modes)

5-3-1 Repeater AP Basic Setup



Security

ESSID: Repeater AP

Enable Repeater AP: ○ Enable ● Disable

Hidden SSID: ○ Enable ● Disable

Client Isolation: ○ Enable ● Disable

IAPP: ○ Enable ● Disable

Maximum Clients: 32

Security Type: Disable

ESSID: *Extended Service Set ID. When users are browsing for available wireless networks, this is the SSID that will appear in the list..*

Enable Repeater AP: *Choose Enable or Disable Repeater AP function, the default is Disable*

Hidden SSID: *By default, it is “Disable”. Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced.*

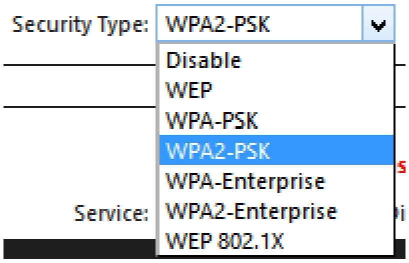
Client Isolation: *By default, it is “Disable”. Select “Enable”, all clients will be isolated from each other, which means they cannot reach each other.*

IAPP: *Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period.*

Maximum Clients: *The default value is 32. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.*

5-3-2 Repeater Security Settings

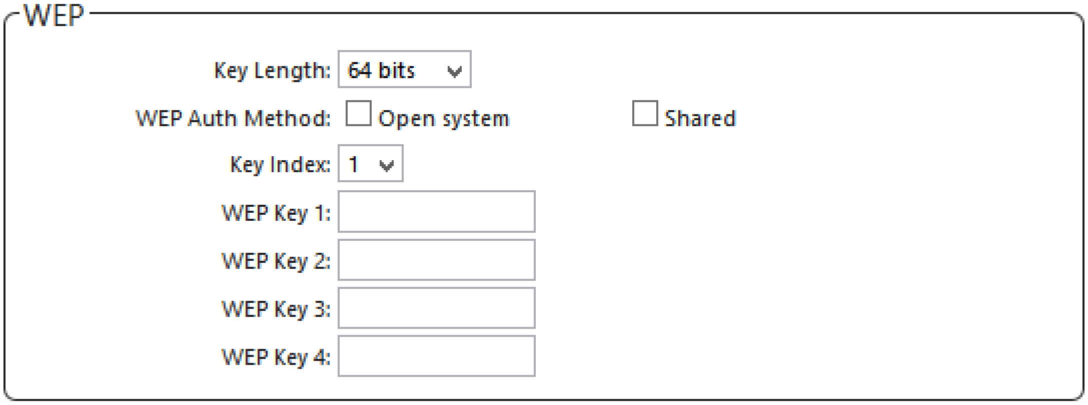
Security Type: *Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and WEP 802.1X.*



Security Type: WPA2-PSK

Disable: Data are unencrypted during transmission when this option is selected.

WEP: WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select WEP as the security type from the drop down list as desired.



WEP

Key Length: 64 bits

WEP Auth Method: □ Open system □ Shared

Key Index: 1

WEP Key 1:

WEP Key 2:

WEP Key 3:

WEP Key 4:

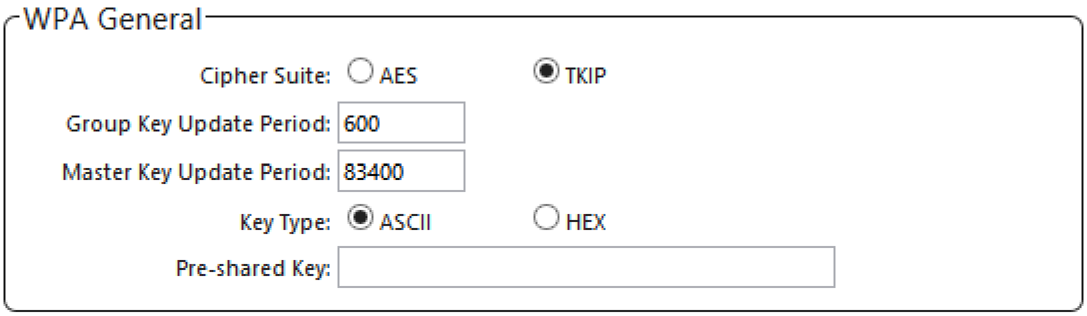
Key Length: The key size of WEP encryption can be 64bit, 128bit or 152bit.

WEP auth method: You can select the appropriate value: Open system (If enabling this mode, there is no need authentication to access AP or Wireless NIC) or Shared (Only those who are sharing the same key with the AP can connect with it).

Key Index: You can select the Key which you want to use. Other wireless station must have the same key value to connect with the device, 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3 or 4.

WEP Key #: You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)

WPA-PSK (or WPA2-PSK): WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.



WPA General

Cipher Suite: ○ AES ● TKIP

Group Key Update Period: 600

Master Key Update Period: 83400

Key Type: ● ASCII ○ HEX

Pre-shared Key:

Cipher Suite: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

AES is short for Advanced Encryption Standard. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

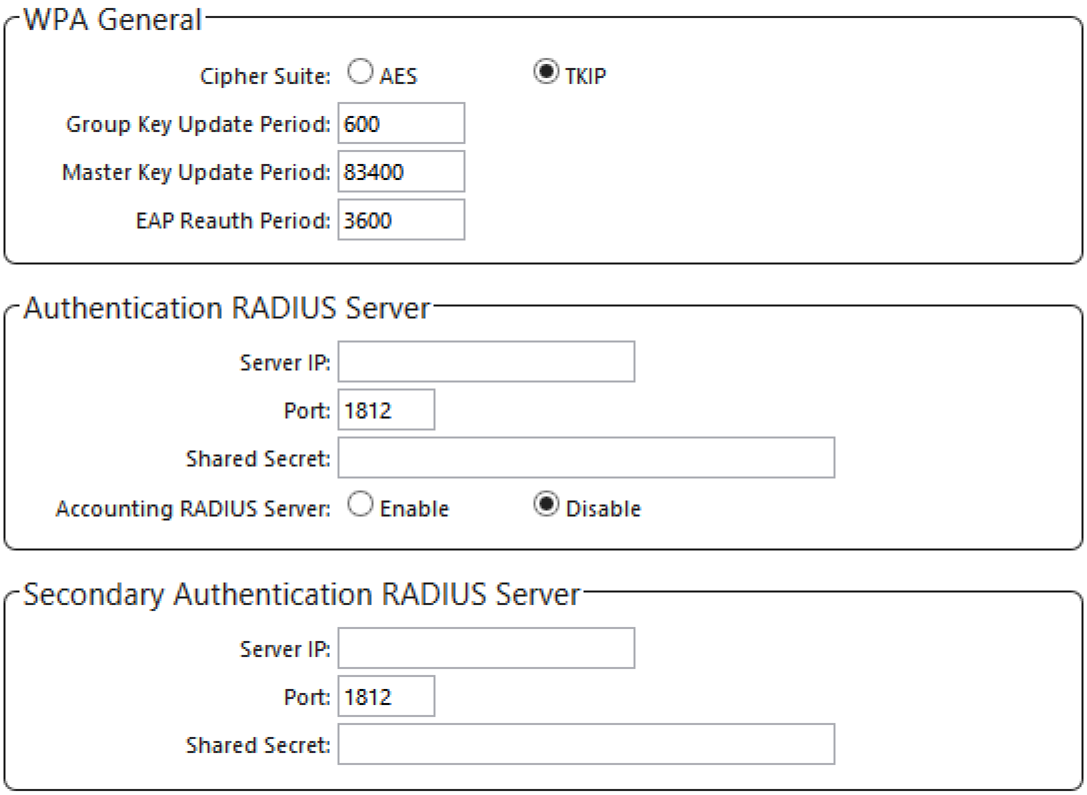
Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

Master Key Update Period: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.

Key Type: Check on the respected button to enable either ASCII or HEX format for the Pre-shared Key.

Pre-Shared Key: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

WPA-Enterprise (or WPA2-Enterprise) General Setting The RADIUS authentication and encryption will be both enabled if this selected.



WPA General

Cipher Suite: ○ AES ● TKIP

Group Key Update Period: 600

Master Key Update Period: 83400

EAP Reauth Period: 3600

Authentication RADIUS Server

Server IP:

Port: 1812

Shared Secret:

Accounting RADIUS Server: ○ Enable ● Disable

Secondary Authentication RADIUS Server

Server IP:

Port: 1812

Shared Secret:

General Setting:

Cipher Suite: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

AES is short for "Advanced Encryption Standard", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

Master Key Update Period: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.

EAP Reauth Period: This time interval for re- authentication in seconds. Enter the time-length required; the default time is 3600 seconds; 0 = disable re-authentication.

Authentication RADIUS Server Settings

Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Accounting Server: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

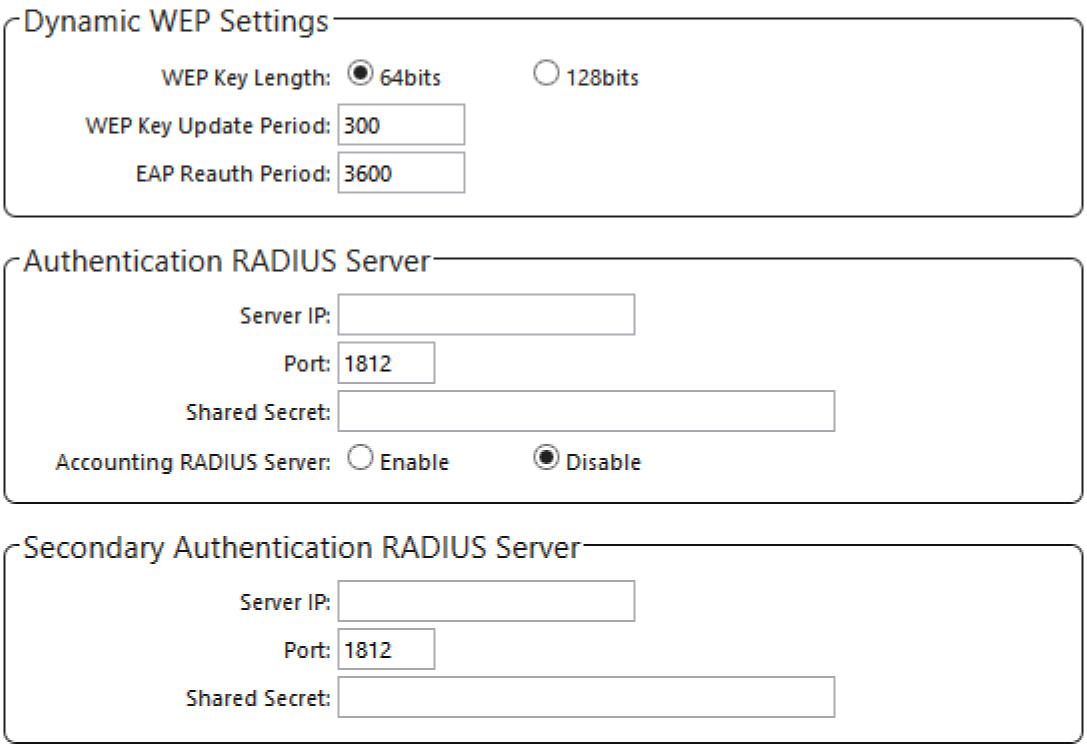
Secondary Authentication RADIUS Server

Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

WEP 802.1x: When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



Dynamic WEP Settings

WEP Key Length: ● 64bits ○ 128bits

WEP Key Update Period: 300

EAP Reauth Period: 3600

Authentication RADIUS Server

Server IP:

Port: 1812

Shared Secret:

Accounting RADIUS Server: ○ Enable ● Disable

Secondary Authentication RADIUS Server

Server IP:

Port: 1812

Shared Secret:

Dynamic WEP Settings WEP Key length: Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.

WEP Key Update Period: The time interval WEP will then be updated; the unit is in seconds; default is 300 seconds; 0 = do not rekey.

EAP Reauth Period: EAP re-authentication period in seconds; default is 3600; 0 = disable re-authentication.

Authentication RADIUS Server Settings Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Accounting Server: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

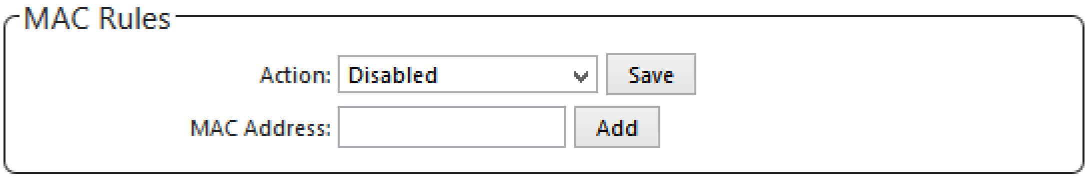
Secondary Authentication RADIUS Server Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

5-4 Repeater AP MAC Filter

For each Repeater AP, users can allow or reject clients based on their MAC address. Click on Wireless, Repeater AP MAC Filter Setup. (This feature is only available in Client Bridge + Repeater AP and CPE + Repeater AP Modes)



MAC Rules

Action: Disabled

MAC Address:

Action: *Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.*

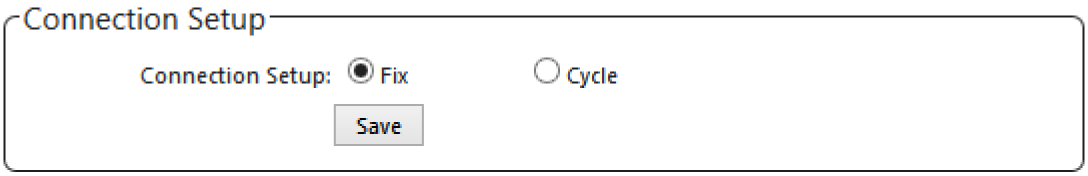
Only Allow List MAC: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "Only Allow List MAC".

Only Deny List MAC: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "Only Deny List MAC". MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

Mac Address: *Type in the Mac address of the client you wish to add under the Mac filter.*

5-5 Station Profile

Settings for Client Bridge. (This feature is only available in Client Bridge + Repeater AP and CPE + Repeater AP Modes)

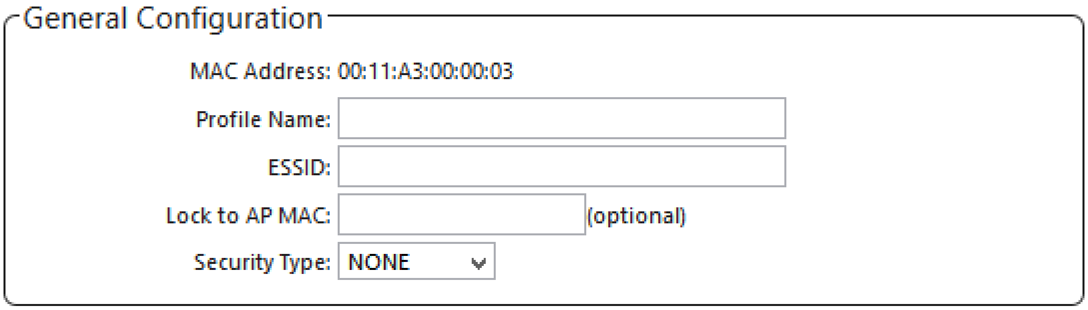


Connection Setup

Connection Setup: ● Fix ○ Cycle

Connection Setup: *Choose Fix or cycle*

General Configuration:



General Configuration

MAC Address: 00:11:A3:00:00:03

Profile Name:

ESSID:

Lock to AP MAC: (optional)

Security Type: NONE

MAC address: *The remote AP MAC Address*

Profile Name: *Set different profiles for quick connection uses.*

ESSID: *Assign Service Set ID for the wireless system. This should be the ESSID fo the remote AP*

Lock to AP MAC: *the function will lock remote AP MAC Address.*

Security Type: *Select an appropriate security type for association, the Security Type can be selected in "NONE", "OPEN", "SHARED", "WPA-PSK", or "WPA2-PSK" from drop-down list. T**he security type must be the same as the associated access point.***

OPEN / SHARED: OPEN and SHARED require the user to set a WEP key to exchange data.

Key Index: key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.

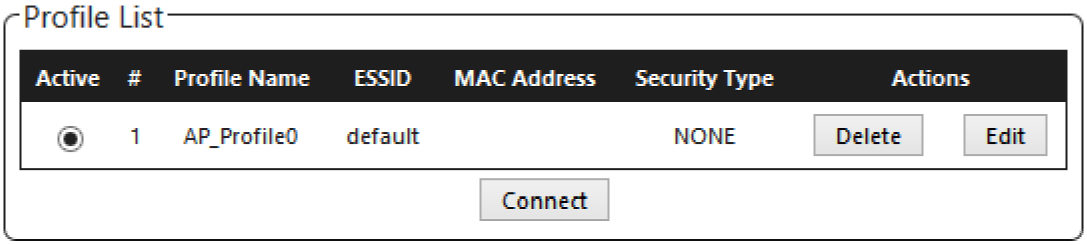
WEP Key #: Enter HEX or ASCII format WEP key value; the system supports up to 4 sets of WEP keys. Key Length Hex ASCII 64-bit 10 Characters 5 Characters 128-bit 26 Characters 13 Characters

WPA-PSK (or WPA2-PSK): WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

Cipher Suite: Select the desired cipher suite from the drop-down list; the options are AES and TKIP.

Pre-shared Key: Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

Profile List: *The user can manage the created profiles for home, work or public areas.*



Profile List

Active	#	Profile Name	ESSID	MAC Address	Security Type	Actions	
●	1	AP_Profile0	default		NONE	Delete	Edit

Click “”Edit” to edit an existing profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “Save” button to save the profile.

Click “Delete” to remove profile.

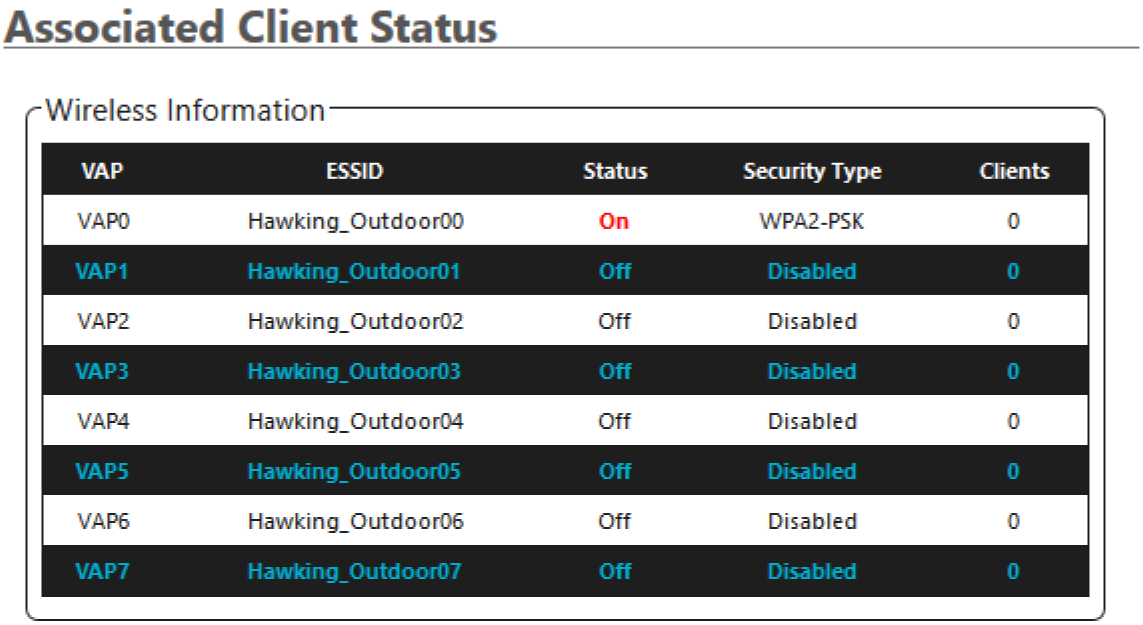
Click and Select a profile from list, then click the “Connect” button to connect to the wireless network with the profile setting.

Before you click “Connect” button for connection, Please double check the “Channel” setting of “Wireless General Setup” as it must be the same with associated AP channel setting

If you only click “Connect” button and do not click “Save”, the profile will not be saved.

5-6 Associated Clients

This page shows detailed wireless information and all associated client status. This page will show different information depending on the Mode you are in.



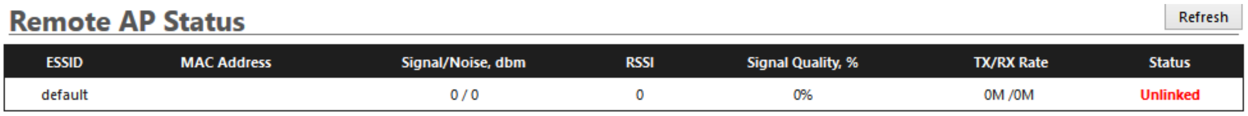
Associated Client Status

Wireless Information

VAP	ESSID	Status	Security Type	Clients
VAP0	Hawking_Outdoor00	On	WPA2-PSK	0
VAP1	Hawking_Outdoor01	Off	Disabled	0
VAP2	Hawking_Outdoor02	Off	Disabled	0
VAP3	Hawking_Outdoor03	Off	Disabled	0
VAP4	Hawking_Outdoor04	Off	Disabled	0
VAP5	Hawking_Outdoor05	Off	Disabled	0
VAP6	Hawking_Outdoor06	Off	Disabled	0
VAP7	Hawking_Outdoor07	Off	Disabled	0

5-7 Remote AP Status

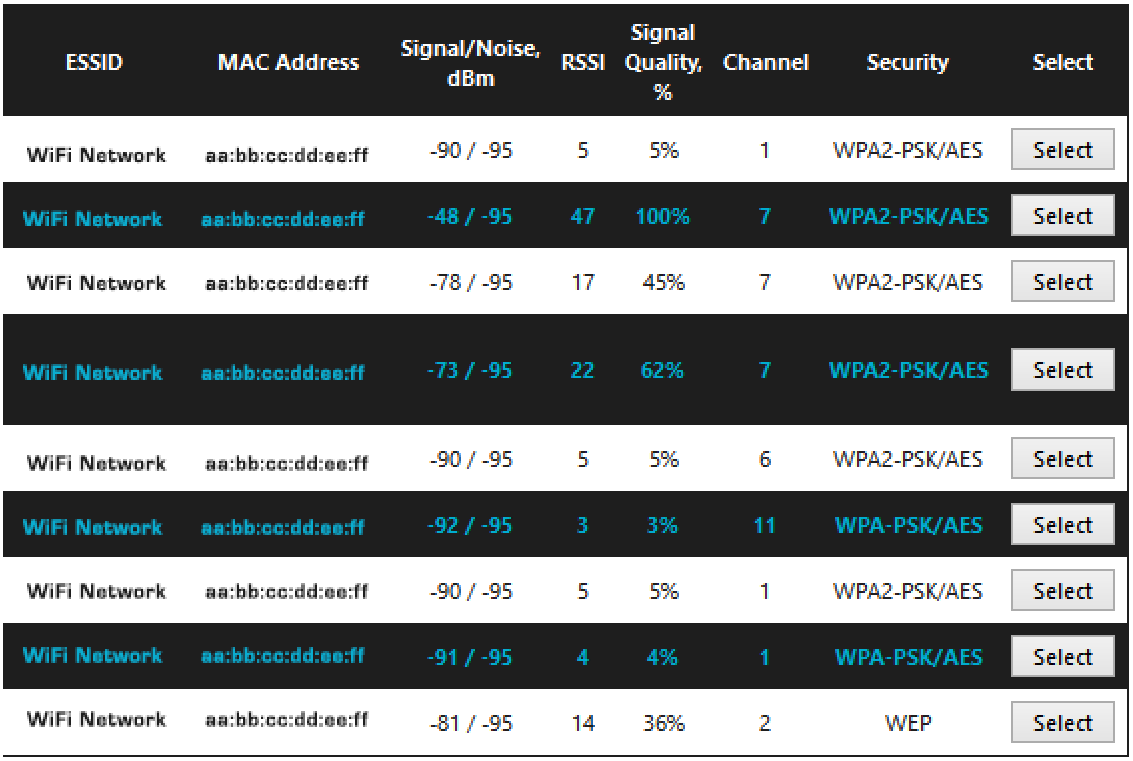
Show the remote bridge AP whether is link or unlinked. (This feature is only available in Client Bridge and CPE + Repeater AP Modes)



ESSID	MAC Address	Signal/Noise, dbm	RSSI	Signal Quality, %	TX/RX Rate	Status
default		0 / 0	0	0%	0M /0M	Unlinked

5-8 Site survey

Use this tool to scan and locate Access Points and select one to associate with. (This feature is only available in Client Bridge + Repeater AP and CPE + Repeater AP Modes)



ESSID	MAC Address	Signal/Noise, dBm	RSSI	Signal Quality, %	Channel	Security	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-48 / -95	47	100%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-78 / -95	17	45%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-73 / -95	22	62%	7	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	6	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-92 / -95	3	3%	11	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-90 / -95	5	5%	1	WPA2-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-91 / -95	4	4%	1	WPA-PSK/AES	Select
WiFi Network	aa:bb:cc:dd:ee:ff	-81 / -95	14	36%	2	WEP	Select

ESSID: *Available Extend Service Set ID of surrounding Access Points.*

MAC Address: *MAC addresses of surrounding Access Points.*

Signal/Noise dBm: *Received signal strength of all found Access Points.*

RSSI: *Indicate the RSSI of the respective client's association.*

Signal Quality (%): *Received signal strength of all found Access Points.*

Channel: *Channel numbers used by all found Access Points.*

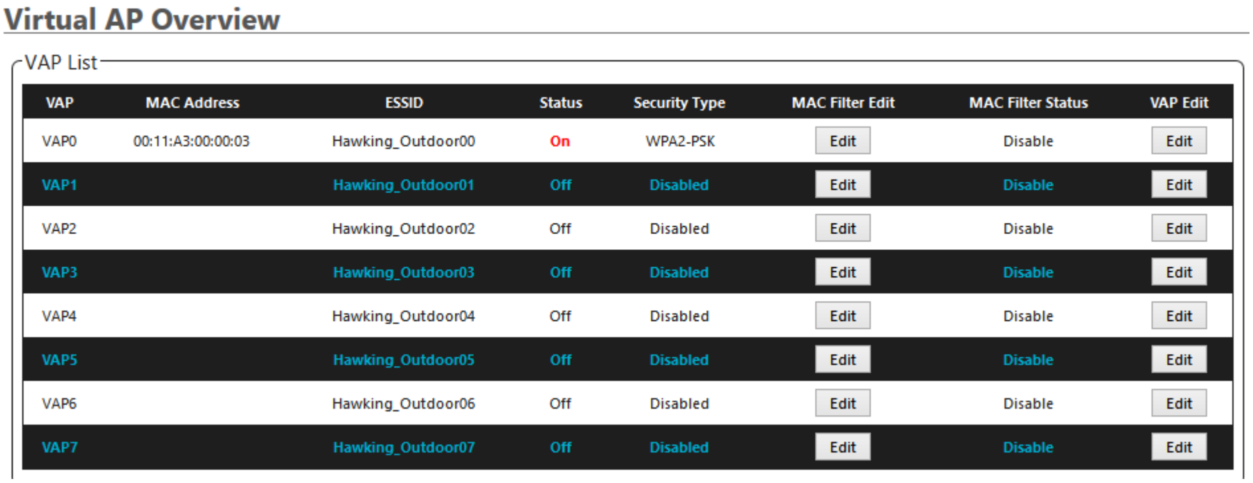
Security: *Security type by all found Access Points.*

Select: *Click “Select” to configure settings and associate with chosen AP.*

While clicking “Select” button in the Site Survey Table, the “ESSID” and “Security Type” will apply in the Wireless General Setup. However, more settings are needed including Security Key.

5-9 Virtual AP Setup

The administrator can create Virtual APs on this page. (This feature is only available in Router AP and AP Modes)



Virtual AP Overview

VAP List

VAP	MAC Address	ESSID	Status	Security Type	MAC Filter Edit	MAC Filter Status	VAP Edit
VAP0	00:11:A3:00:00:03	Hawking_Outdoor00	On	WPA2-PSK	Edit	Disable	Edit
VAP1		Hawking_Outdoor01	Off	Disabled	Edit	Disable	Edit
VAP2		Hawking_Outdoor02	Off	Disabled	Edit	Disable	Edit
VAP3		Hawking_Outdoor03	Off	Disabled	Edit	Disable	Edit
VAP4		Hawking_Outdoor04	Off	Disabled	Edit	Disable	Edit
VAP5		Hawking_Outdoor05	Off	Disabled	Edit	Disable	Edit
VAP6		Hawking_Outdoor06	Off	Disabled	Edit	Disable	Edit
VAP7		Hawking_Outdoor07	Off	Disabled	Edit	Disable	Edit

VAP: Display number of system's Virtual AP.

MAC Address: The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here

ESSID: Display Virtual AP's ESSID; default is AP00~AP07.

Status: Display VAP status; default VAP0 is always on and only VAP0 can support WPS function.

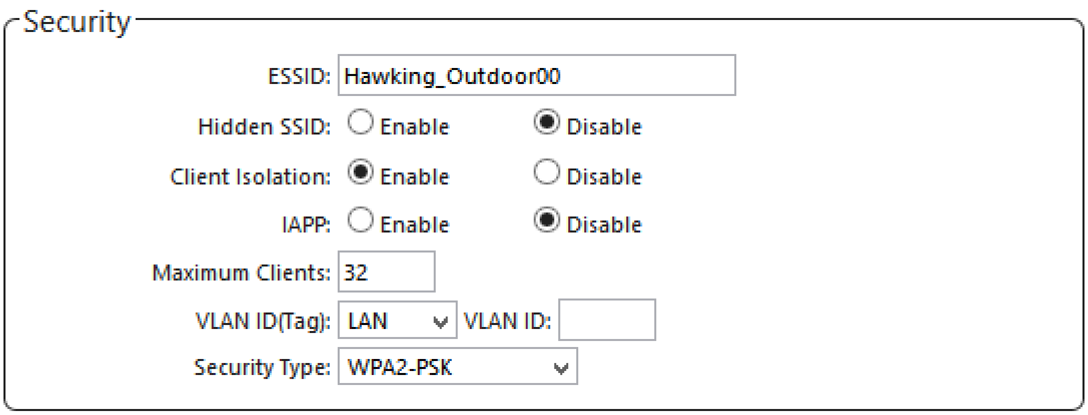
Security Type: Display Virtual AP's Security Type; default is disabled.

MAC Filter Setup: Click “Setup” button for configuring Virtual AP's Access Control List.

VAP Edit: Click “Edit” button for configuring Virtual AP's settings and security type.

5-9-1 Virtual AP General Configuration

For each Virtual AP, users can configure general settings and security. Click “edit” on the Virtual AP you wish to edit.



Security

ESSID: Hawking_Outdoor00

Hidden SSID: ○ Enable ● Disable

Client Isolation: ● Enable ○ Disable

IAPP: ○ Enable ● Disable

Maximum Clients: 32

VLAN ID(Tag): LAN VLAN ID:

Security Type: WPA2-PSK

ESSID: *Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.*

Hidden SSID: *Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.*

Client Isolation: *Select Enable, all clients will be isolated from each other. That means all clients cannot reach to other clients.*

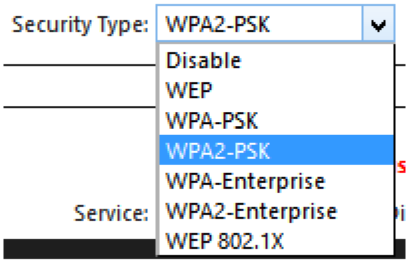
IAPP: *Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off period. Notice: IAPP only used on WPA-PSK and WPA2-PSK security type. Only one of VAPs can be enabled.*

Maximum Clients: *Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.*

VLAN Tag(ID): *Virtual LAN, the system supports tagged VLAN. To enable VLAN function; valid values are from 0 to 4094.*

5-9-2 Virtual AP Security Settings

Security Type: *Select the desired security type from the drop-down list; the options are WEP, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise and WEP 802.1X.*



Security Type: WPA2-PSK

Disable: Data are unencrypted during transmission when this option is selected.

WEP: WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, 128-bit or 152-bit shared key. Select WEP as the security type from the drop down list as desired.

> *Key Length: The key size of WEP encryption can be 64bit, 128bit or 152bit.*
>
> *WEP auth method: You can select the appropriate value: Open system (If enabling this mode, there is no need authentication to access AP or Wireless NIC) or Shared (Only those who are sharing the same key with the AP can connect with it).*
>
> *Key Index: You can select the Key which you want to use. Other wireless station must have the same key value to connect with this device, 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3 or 4.*
>
> *WEP Key #: You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)*

WPA-PSK (or WPA2-PSK): WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.

> *Cipher Suite: You can chose use AES or TKIP with your WPA / WPA2 encryption method,*
>
> *AES is short for Advanced Encryption Standard. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.*
>
> *TKIP is short for "Temporal Key Integrity Protocol. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*
>
> *Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.*

Master Key Update Period: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.

Key Type: Check on the respected button to enable either ASCII or HEX format for the Pre-shared Key.

Pre-Shared Key: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

WPA-Enterprise (or WPA2-Enterprise) General Setting. The RADIUS authentication and encryption will be both enabled if this selected.

General Setting:

Cipher Suite: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

AES is short for "Advanced Encryption Standard", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

Master Key Update Period: This time interval for re-keying GMK (master key used internally to generate GTKs) in seconds. Enter the time-length required; the default time is 83400 seconds.

EAP Reauth Period: This time interval for re- authentication in seconds. Enter the time-length required; the default time is 3600 seconds; 0 = disable re-authentication.

Authentication RADIUS Server Settings

Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Accounting Server: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

Secondary Authentication RADIUS Server

Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

WEP 802.1x: When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.

Dynamic WEP Settings WEP Key length: Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.

WEP Key Update Period: The time interval WEP will then be updated; the unit is in seconds; default is 300 seconds; 0 = do not rekey.

EAP Reauth Period: EAP re-authentication period in seconds; default is 3600; 0 = disable re-authentication.

Authentication RADIUS Server Settings Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

Accounting Server: Check on the respected button to enable either Enable or Disable accounting RADIUS server.

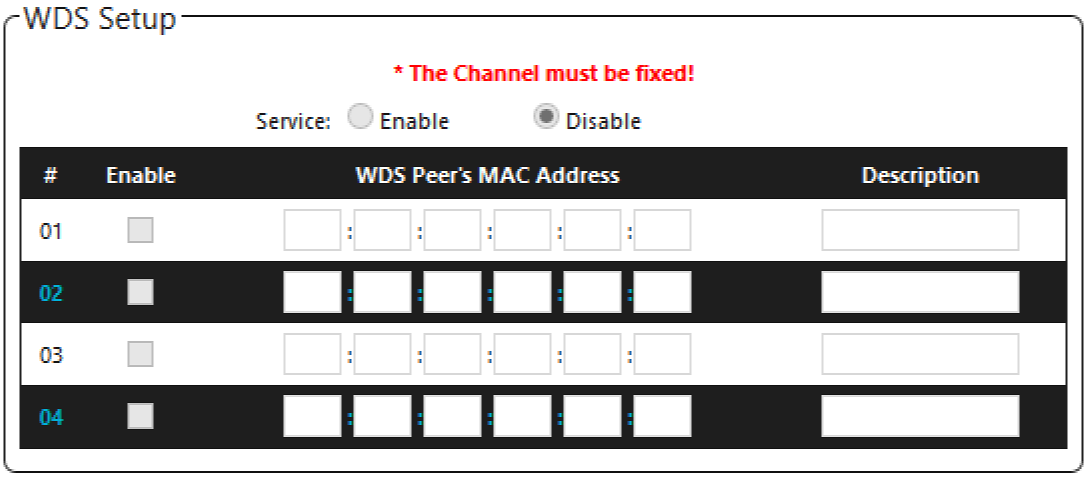
Secondary Authentication RADIUS Server Authentication Server: Enter the IP address of the Authentication RADIUS server.

Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Shared secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

5-9-3 Virtual AP WDS Setup

When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.**



WDS Setup

* The Channel must be fixed!

Service: ○ Enable ● Disable

#	Enable	WDS Peer's MAC Address	Description
01	□	: : : : :	
02	□	: : : : :	
03	□	: : : : :	
04	□	: : : : :	

WDS MAC List Enable: *Check "Enable" to create WDS link.*

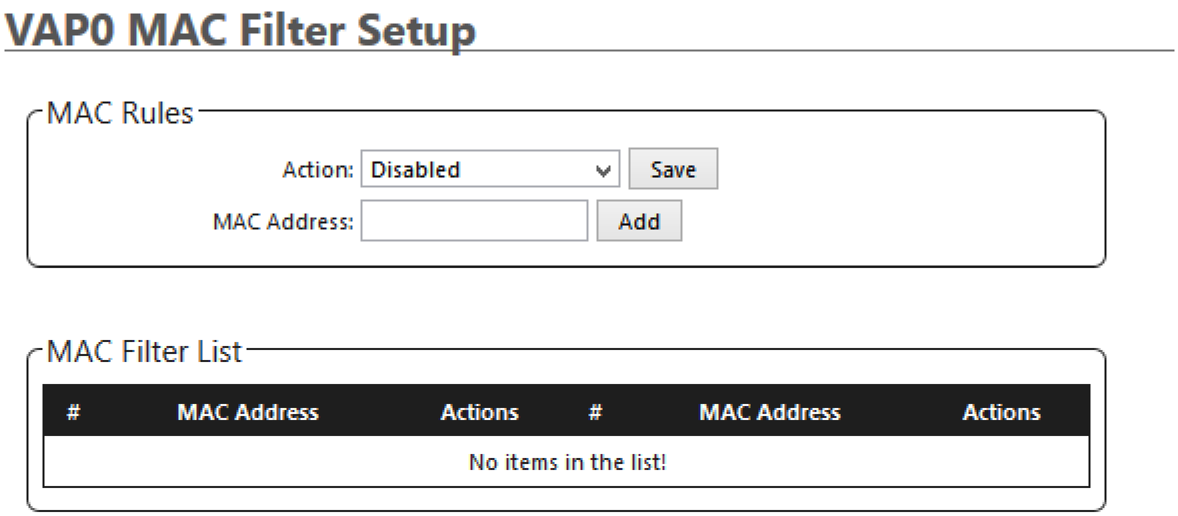
WDS Peer's MAC Address: *Enter the MAC address of WDS peer.*

Description: *Description of WDS peer*

Note: All WDS peers need to have same WiFi Channel and same Security Type.

5-9-4 VAP Mac Filter Setup

For each Virtual AP, users can allow or reject clients based on their MAC address. Click on Wireless, Virtual AP setup, Next to the VAP you wish to change, click on VAP MAC Filter Edit to configure these settings.


VAP0 MAC Filter Setup

MAC Rules

Action: Disabled

MAC Address:

MAC Filter List

#	MAC Address	Actions	#	MAC Address	Actions
No items in the list!					

Action: *Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.*

Only Allow List MAC: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "Only Allow List MAC".

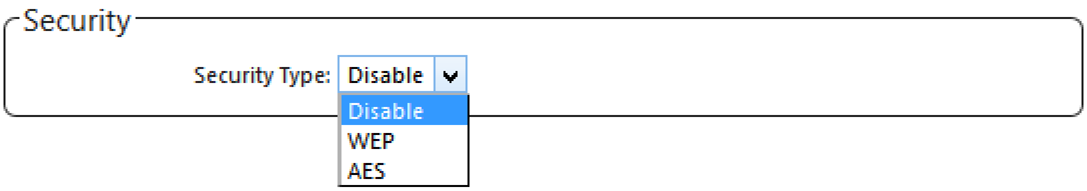
Only Deny List MAC: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "Only Deny List MAC". MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

Mac Address: *Type in the Mac address of the client you wish to add under the Mac filter.*

5-10 WDS Setup

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.** (This feature is only available in WDS Mode)

Security Type: *Option is "Disable", "WEP", "TKIP" or "AES" from drop-down list.*



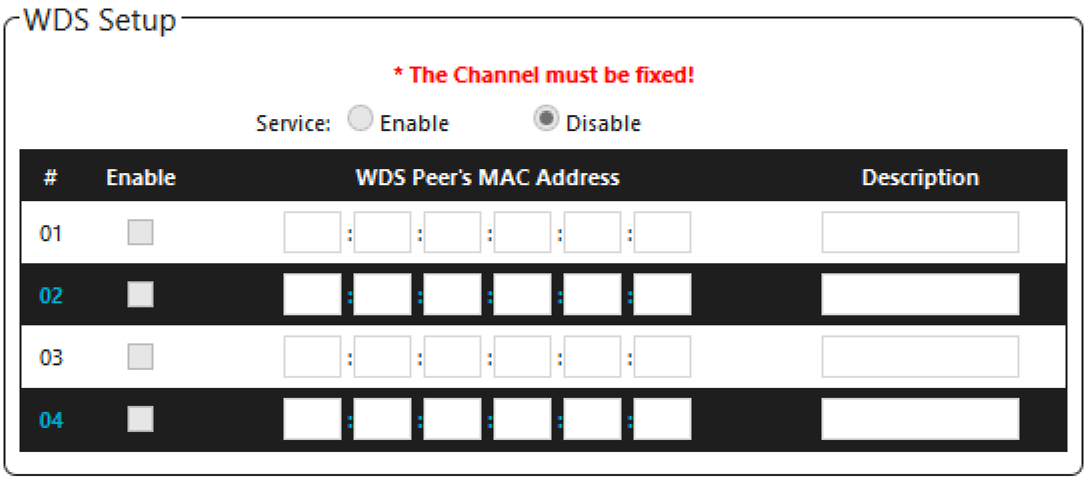
Security

Security Type: Disable

WEP Key: *Enter 5 / 13 ASCII or 10 / 26 HEX format WEP key.*

AES Key: *Enter 8 to 63 ASCII or 64 HEX format AES key.*

Note that the security key must be the same on all WDS Peer Devices in order to build WDS links. Security type takes effect when WDS is enabled.



WDS Setup

* The Channel must be fixed!

Service: ○ Enable ● Disable

#	Enable	WDS Peer's MAC Address	Description
01	□	: : : : :	
02	□	: : : : :	
03	□	: : : : :	
04	□	: : : : :	

WDS MAC List Enable: *Check "Enable" to create WDS link.*

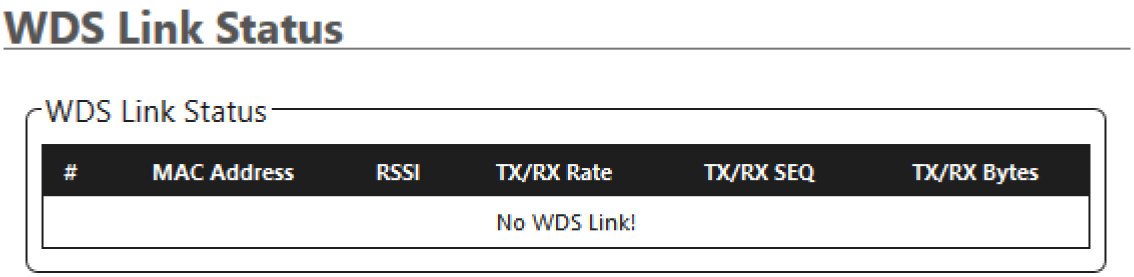
WDS Peer's MAC Address: *Enter the MAC address of WDS peer.*

Description: *Description of WDS peer*

Note: All WDS peers need to have same WiFi Channel and same Security Type.

5-11 WDS Status

This page shows the status of each WDS enabled device on the network. (This feature is only available in Router AP, AP and WDS Modes)



WDS Link Status

WDS Link Status

#	MAC Address	RSSI	TX/RX Rate	TX/RX SEQ	TX/RX Bytes
No WDS Link!					

MAC Address: *Display MAC address of WDS devices.*

RSSI: *Indicate the RSSI of the respective WDS's link.*

TX/RX Rate: *Indicate the TX/RX Rate of the respective WDS's link*

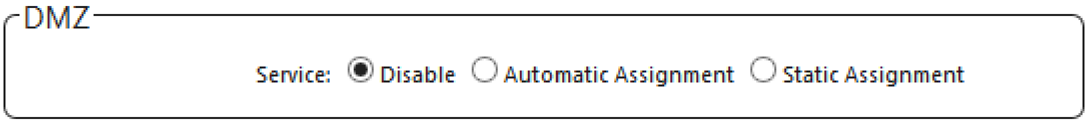
TX/RX SEQ: *Indicate the TX/RX sequence of the respective WDS's link*

Disconnect: *Administrator can kick out a specific client, click "Delete" button to kick out specific WDS's link.*

Chapter VI: Advanced Settings

6-1 DMZ

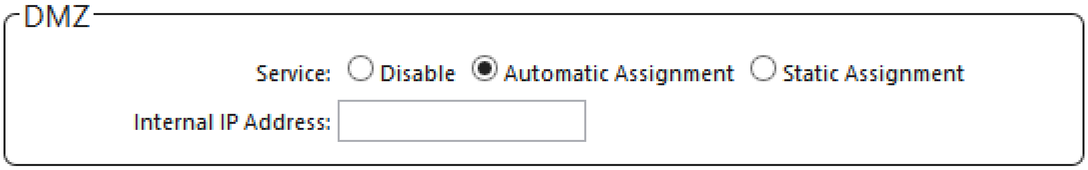
DMZ is a setting associated with NAT functionality and is an alternative to setting up a Virtual Server (Port Forwarding). This feature opens all ports of DMZ host to internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to different internal hosts, Virtual Server rules should be used. (This feature is only available in Router AP and CPE + Repeater AP Modes)



DMZ

Service: ● Disable ○ Automatic Assignment ○ Static Assignment

Service: *The DMZ is disabled by default. Chose an option to enable DMZ.*

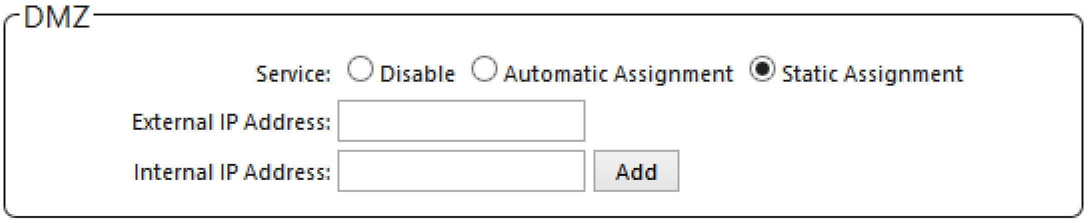


DMZ

Service: ○ Disable ● Automatic Assignment ○ Static Assignment

Internal IP Address:

Automatic Assignment: *Enter Internal IP address of DMZ host. Only one DMZ host is supported.*

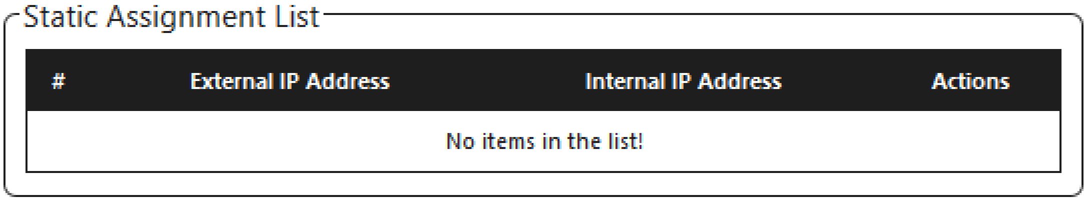


DMZ

Service: ○ Disable ○ Automatic Assignment ● Static Assignment

External IP Address:

Internal IP Address:



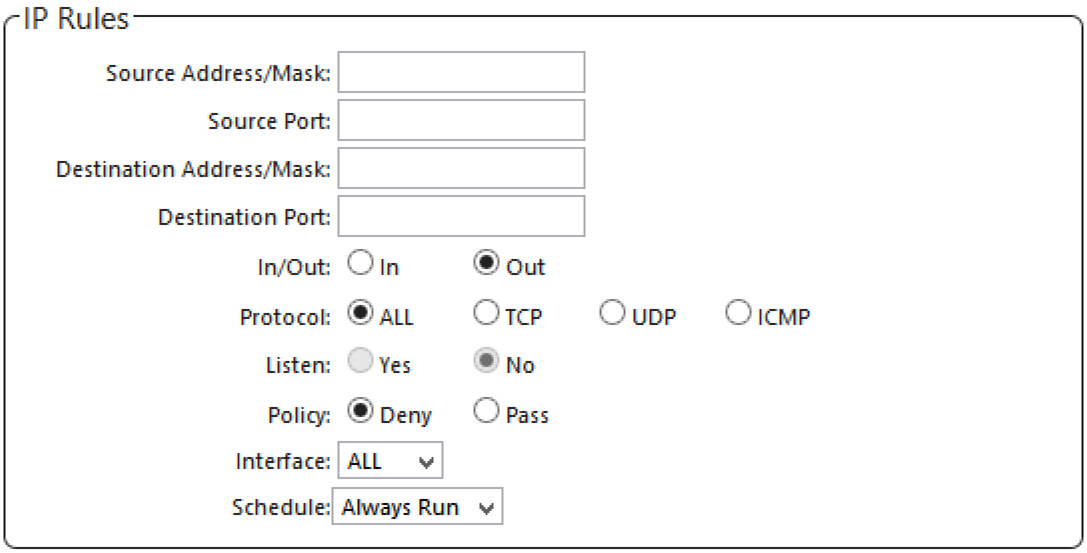
Static Assignment List

#	External IP Address	Internal IP Address	Actions
No items in the list!			

Static Assignment: *Enter external and internal IP address of DMZ host. This will map one external IP to one internal IP of the DMZ host.*

6-2 IP Filter

Allows users to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules. (This feature is only available in Router AP and CPE + Repeater AP Modes)



IP Rules

Source Address/Mask:

Source Port:

Destination Address/Mask:

Destination Port:

In/Out: ○ In ● Out

Protocol: ● ALL ○ TCP ○ UDP ○ ICMP

Listen: ○ Yes ● No

Policy: ● Deny ○ Pass

Interface: ALL

Schedule: Always Run

Source Address/Mask: *Enter desired source IP address and netmask. i.e. 192.168.2.10/32.*

Source Port: *Enter a port or a range of ports as start:end. i.e. port 20:80*

Destination Address/Mask: *Enter desired destination IP address and netmask. i.e. 192.168.1.10/32*

Destination Port: *Enter a port or a range of ports as start:end. i.e. port 20:80*

In/Out: *Applies to Ingress or egress packets.*

Protocol: *Supports TCP, UDP or ICMP.*

Listen: *Click Yes radial button to match TCP packets only with the SYN flag.*

Policy: *Deny to drop and Pass to allow per filter rules*

Interface: *The interface that a filter rule applies*

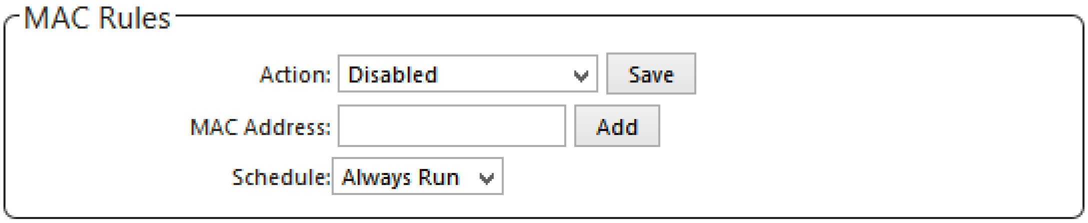
Schedule: *Can choose to use rule by "Time Policy"*

All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules.

6-3 MAC Filter

Allows users to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. That MAC filter rules have precedence over IP Filter rules. (This feature is only available in Router AP and CPE + Repeater AP Modes)



MAC Rules

Action: Disabled

MAC Address:

Schedule: Always Run

MAC Filter Rule: *Disable is the default setting. Options are Disabled, Only Deny List MAC or Only Allow List MAC.*

Only Allow List MAC: The wireless clients in the MAC Filter List will be allowed to access to Access Point; All others will be denied.

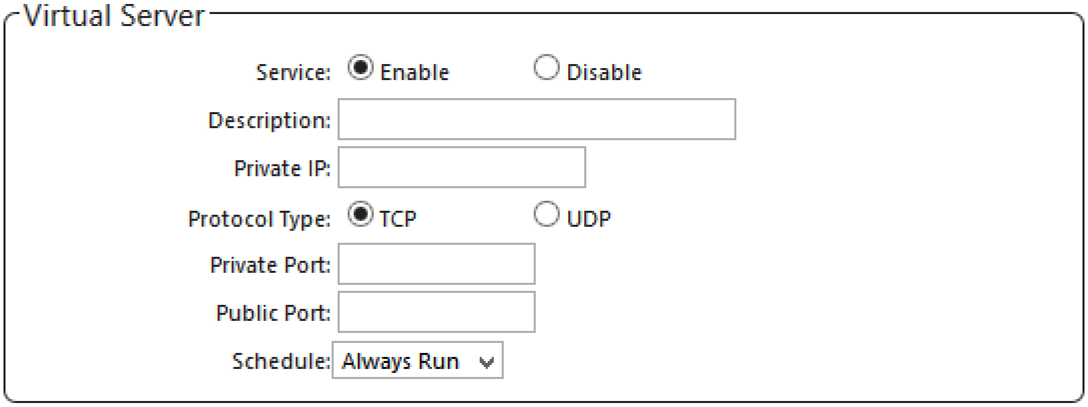
Only Deny List MAC The wireless clients in the MAC Filter List will be denied to access to Access Point; All others will be allowed.

MAC Address: *Enter MAC address (e.g. aa:bb:cc:dd:ee:ff) and click "Add". The MAC address should display in the MAC Filter List. There are a maximum of 20 clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the Add and Delete buttons.*

Schedule: *Can choose to use rule by "Time Policy"*

6-4 Virtual Server

This function allows you to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on local network, so you can setup an Internet service on the computer on local network, without exposing it on Internet directly. It is also referred to as "Port Forwarding". You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address. (This feature is only available in Router AP and CPE + Repeater AP Modes)



Virtual Server

Service: ● Enable ○ Disable

Description:

Private IP:

Protocol Type: ● TCP ○ UDP

Private Port:

Public Port:

Schedule: Always Run

Service: *By Default, the service is disabled. Check Enable radial button to enable Virtual Server.*

Description: *Enter appropriate message for resource sharing via Virtual Server.*

Private IP: *Enter corresponding IP address of internal resource to share.*

Protocol Type: *Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.*

Private Port: *A port or a range of ports may be specified as start:end; i.e. port 20:80*

Public Port: *A port or a range of ports may be specified as start:end; i.e. port 20:80*

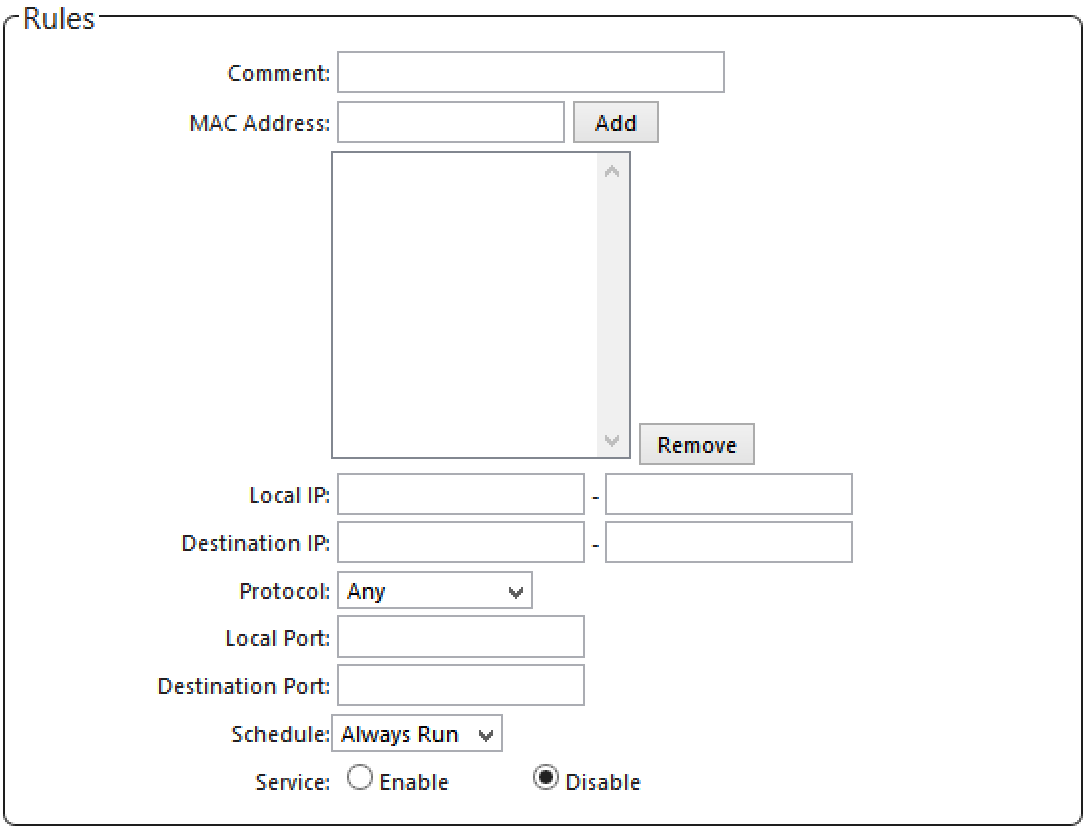
Schedule: *Can choose to use rule by "Time Policy"*

Click "Save" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List.

When creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ rules when both rules exist.

6-5 Parental Control

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites. (This feature is only available in Router AP and CPE + Repeater AP Modes)



Rules

Comment:

MAC Address: Add

Remove

Local IP: -

Destination IP: -

Protocol: Any

Local Port:

Destination Port:

Schedule: Always Run

Service: ○ Enable ● Disable

Comment: *Enter a descriptive name for this rule for identifying purposes.*

MAC Address: *Enter MAC address in valid MAC address format (aa.bb.cc.dd.ee.ff) and click "Add" button to add in the MAC group of each rule. Click "Remove" button can remove MAC address in the group of each rule. There are 10 MAC address maximum allowed in each rule.*

Local/Destination IP: *Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.*

Protocol: *Select Any or specify a protocol (TCP, UDP, ICMP, Content Filter and Application) from drop-down list. When you select ICMP or Layer 7 Application, the Local(LAN)/ Destination Port cannot be used.*

Content Filter: If you want to block websites with specific URL address or using specific keywords, enter each URL or keywords in the "Content Filter" field and click "Add" button to add in the Content Filter list of each rule. Click "Remove" button can remove URL or keywords.

TCP/UDP: Local Port: Specify local port(LAN port) range required for this rule Destination Port : Specify destination port range required for this rule

Application: Choose the application you wish to block. A small list of presets are available

Schedule: *Can choose to use rule by "Time Policy"*

Service: *Check Enable button to activate this rule, and Disable to deactivate.*

Click "**Add"** button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the list.

6-6 QoS

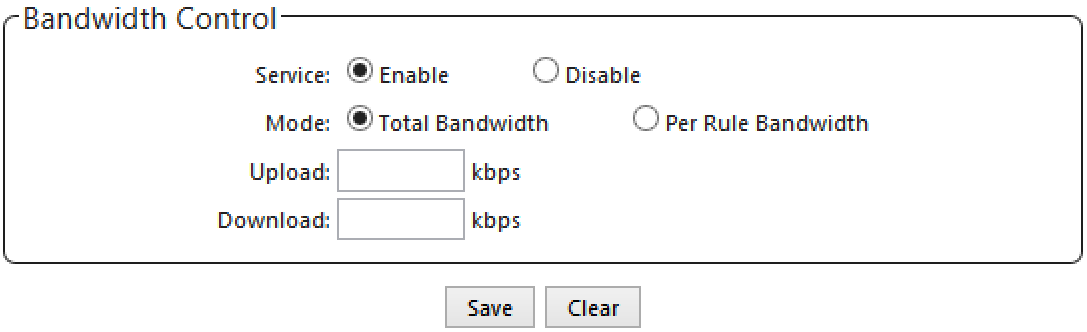
Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

Bandwidth Control Service

The default is Disable, **Click "**Enable" to enable QoS Service.

Mode: Can choose a total Bandwidth control or Per Rule Bandwidth control.

Total Bandwidth: the function is all customers use a total bandwidth.



Bandwidth Control

Service: ● Enable ○ Disable

Mode: ● Total Bandwidth ○ Per Rule Bandwidth

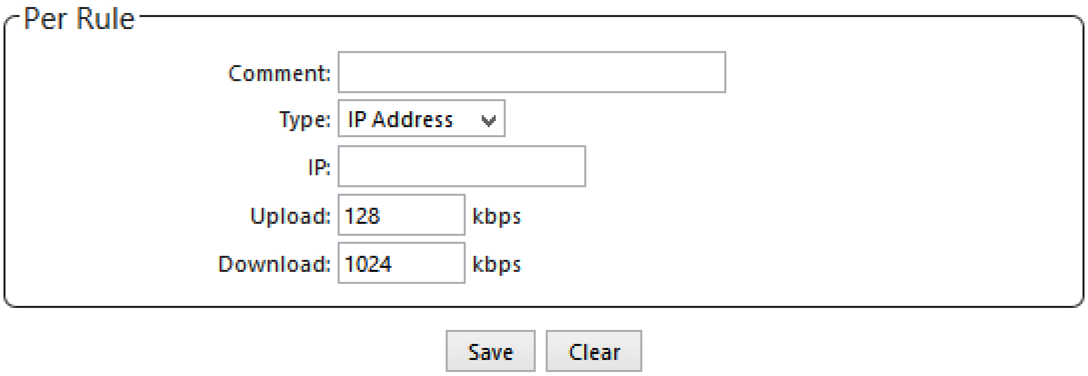
Upload: kbps

Download: kbps

Upload: Setting use upload control by total bandwidth

Download: Setting use download control by total bandwidth

Per Rule Bandwidth: Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules



Per Rule

Comment:

Type: IP Address

IP:

Upload: 128 kbps

Download: 1024 kbps

Comment: Enter a descriptive name for this rule for identifying purposes.

Type:

> *IP Address / IP segment: Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.1.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.1.254.*
>
> *Port: Specify local port(LAN port) range required for this rule.*
>
> *MAC: Enter MAC address in valid MAC address format (aa.bb.cc.dd.ee.ff) and click "Save"*
>
> *Application: Bittorrent, eDonkey2000, FTP and HTTP*

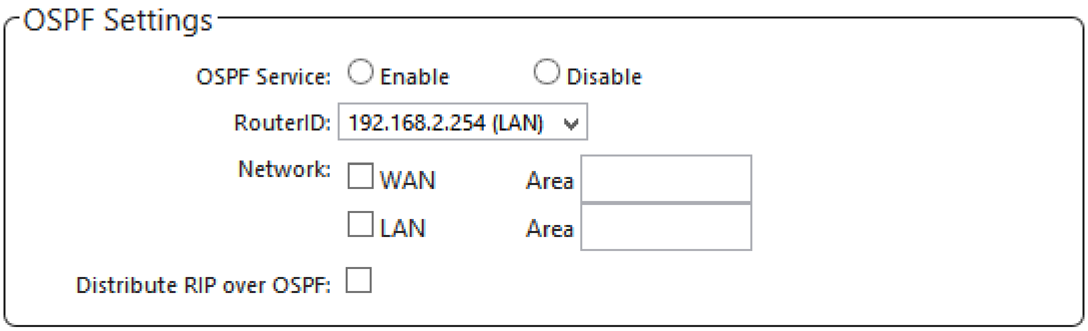
Upload: Setting use upload control by total bandwidth

Download: Setting use download control by total bandwidth

6-7 IP Routing

The IP Routing Settings allows you to configure routing feature in the gateway. The system supports RIP(Routing Information Protocol) and OSPF(Open Shortest Path First) dynamic routing and allows you to manually configure static network routes. (This feature is only available in Router AP and CPE + Repeater AP Modes)

OSPF Settings



OSPF Settings

OSPF Service: ○ Enable ○ Disable

RouterID: 192.168.2.254 (LAN)

Network: □ WAN Area

□ LAN Area

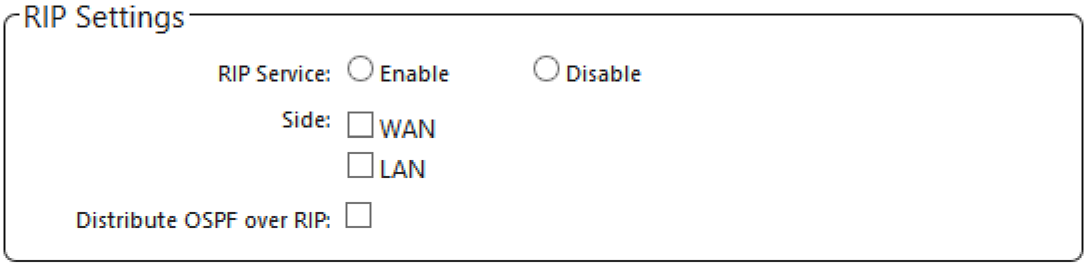
Distribute RIP over OSPF: □

OSPF Service: *By default, it is disabled.*

Router ID: *The router ID is typically derived by each router from its interface IP address.*

Distribute RIP over OSPF: *Allow RIP routes will redistributed into OSPF.*

RIP Settings



RIP Settings

RIP Service: ○ Enable ○ Disable

Side: □ WAN
□ LAN

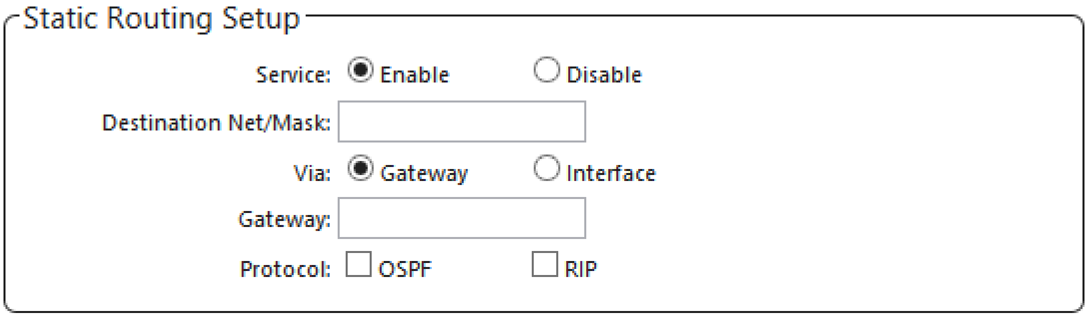
Distribute OSPF over RIP: □

RIP Service: *By default, it is disabled.*

Side: *Specify desired interface WAN, LAN for sending and receiving of RIP packets.*

Distribute OSPF over RIP: *Allow OSPF routes redistributed into RIP.*

Static Routing Setup



Static Routing Setup

Service: ● Enable ○ Disable

Destination Net/Mask:

Via: ● Gateway ○ Interface

Gateway:

Protocol: □ OSPF □ RIP

Service: *Click Enable to activate static routing.*

Destination Net/Mask: *Specify desired destination IP network address with format of A.B.C.D/M*

Via: *Select a next hop of Gateway or Interface to the destination IP network.*

Gateway: Enter gateway IP address

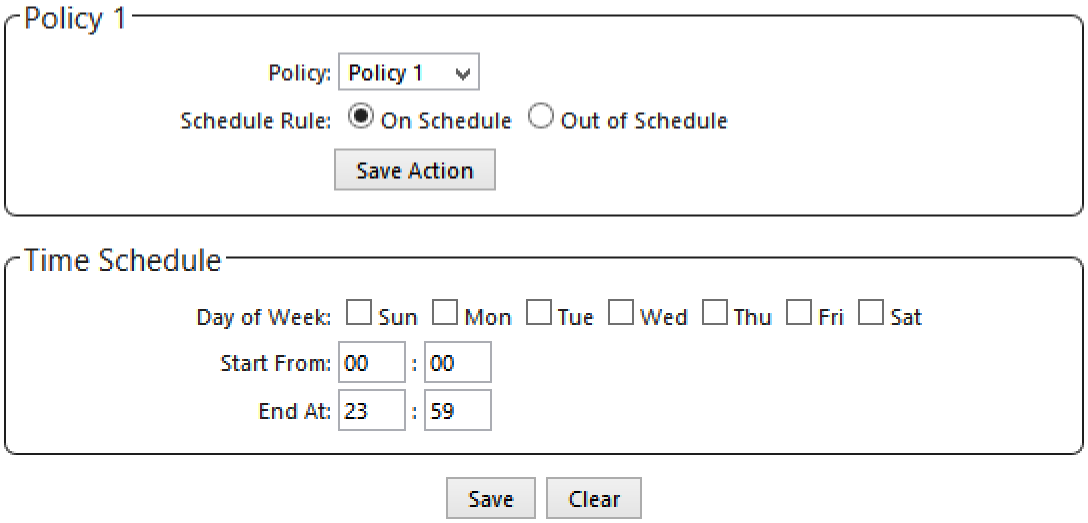
Interface: Choose the interface via LAN or WAN

Protocol: *Set static routing rule to RIP or OSPF network. Select RIP to associate specific network on RIP routing process. Select OSPF to associate specific network with the specified area on OSPF routing process*

Click “Save” button to add Routing rule to List. There are maximum 20 rules allowed in this List. All rules can be edited or removed on the List.

6-8 Time Policy

Users can define time policy for Service Domain, IP Filtering, MAC Filtering and Virtual Server. There are 10 policies that can be defined.



Policy 1

Policy: Policy 1

Schedule Rule: ● On Schedule ○ Out of Schedule

Time Schedule

Day of Week: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Start From: 00 : 00

End At: 23 : 59

Policy: *10 Policies can be selected.*

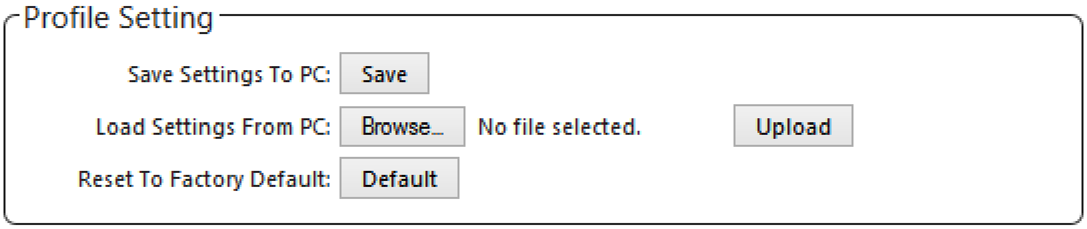
Schedule Rule: *Select desired schedule for this policy.*

Time Schedule: *Select desired day of week and time period for this policy.*

Chapter VII: Utilities

7-1 Profile Setting

In this page you can save your current configuration, restore a previous saved configuration or restore all the settings in the system to the factory default settings.



No file selected.

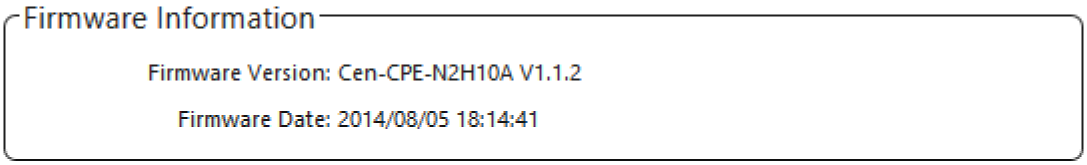
Save Settings to PC: *Click Save button to save the current configuration to a local disk.*

Load Settings from PC: *Click Browse button to locate a configuration file to restore, and then click Upload button to upload.*

Reset To Factory Default: *Click Default button to reset back to the factory default settings and expect Successful loading message. Then, click Reboot button to activate.*

7-2 Firmware Upgrade

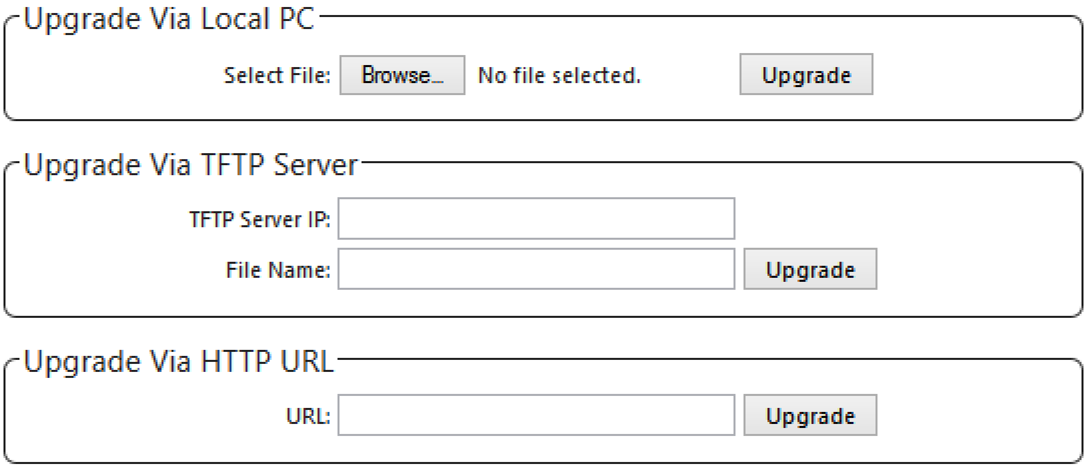
Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or a bug fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.



Firmware Version: Cen-CPE-N2H10A V1.1.2

Firmware Date: 2014/08/05 18:14:41

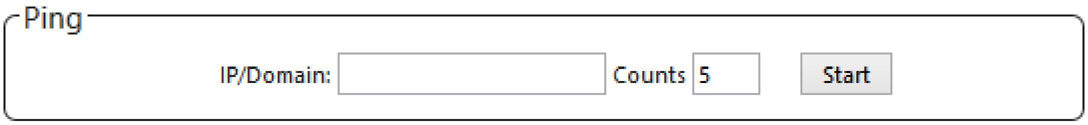
Firmware Information: *Shows current system software version and software date*



Upgrade Firmware: *Upgrade firmware will support via Local PC, TFTP Server and HTTP URL upgrade*

7-3 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility.

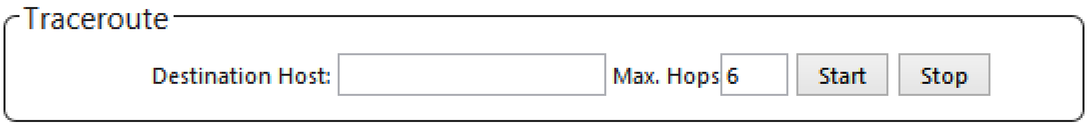


Counts 5

Ping: *This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the Result field while running the PING test.*

IP/Domain: Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.

Count: The default setting is 5 and the range is from 1 to 50. It indicates number of connectivity test.



Max. Hops 6

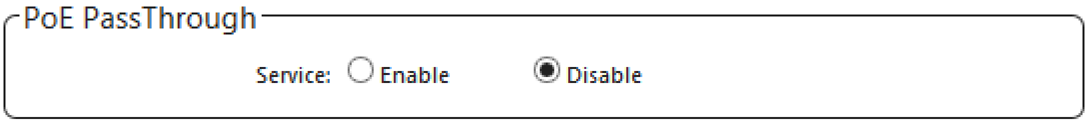
Traceroute: *Allows tracing the hops from the device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the Start button, click Stop button to stopped test.*

Destination Host: Specifies the Destination Host for the finding the route taken by ICMP packets across the network.

MAX Hop: Specifies the maximum number of hops (max time-to-live value) trace route will probe.

7-4 PoE PassThrough

This device supports PoE Bridge function. If this is enabled, the Ethernet port LAN2 will allow other PoE devices to be powered through the secondary LAN port



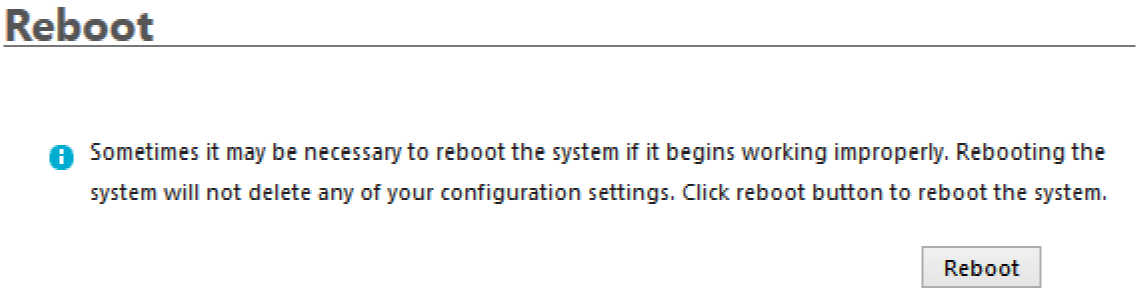
PoE PassThrough

Service: ○ Enable ● Disable

Service: the default is disabled but user can enable the feature here

7-5 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



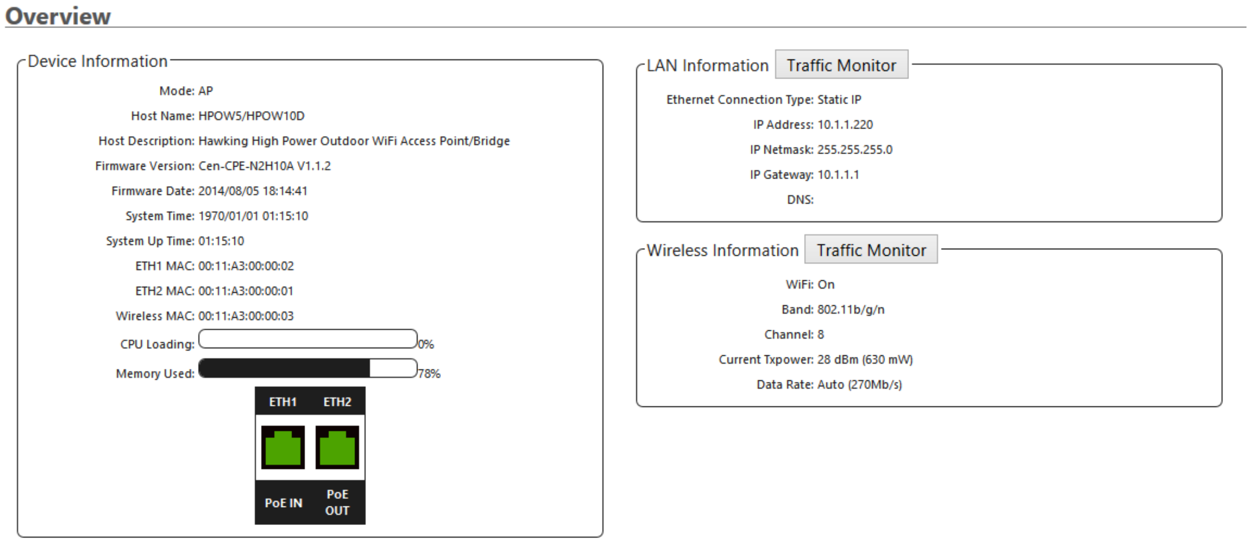
Reboot

Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Chapter VIII: Status

8-1 Overview

Detailed information on the Device and Network can be viewed on this page.



Overview

Device Information

Mode: AP
Host Name: HPOW5/HPOW10D
Host Description: Hawking High Power Outdoor WiFi Access Point/Bridge
Firmware Version: Cen-CPE-N2H10A V1.1.2
Firmware Date: 2014/08/05 18:14:41
System Time: 1970/01/01 01:15:10
System Up Time: 01:15:10
ETH1 MAC: 00:11:A3:00:00:02
ETH2 MAC: 00:11:A3:00:00:01
Wireless MAC: 00:11:A3:00:00:03
CPU Loading: 0%
Memory Used: 78%

LAN Information

Ethernet Connection Type: Static IP
IP Address: 10.1.1.220
IP Netmask: 255.255.255.0
IP Gateway: 10.1.1.1
DNS:

Wireless Information

WiFi: On
Band: 802.11b/g/n
Channel: 8
Current Txpower: 28 dBm (630 mW)
Data Rate: Auto (270Mb/s)

Device Information: *Display the information of the device, modes, firmware version, times, System Up Time, MAC address, CPU/memory use.*

LAN Information: *Gives current IP/Netmask of the device*

Traffic Monitor: Shows total transmit/receive LAN traffic on device

WAN Information: *(This feature is only available in Router AP and CPE + Repeater AP Modes) shows current Internet Connection Type, WAN IP address/NetMask/Gateway/DNS*

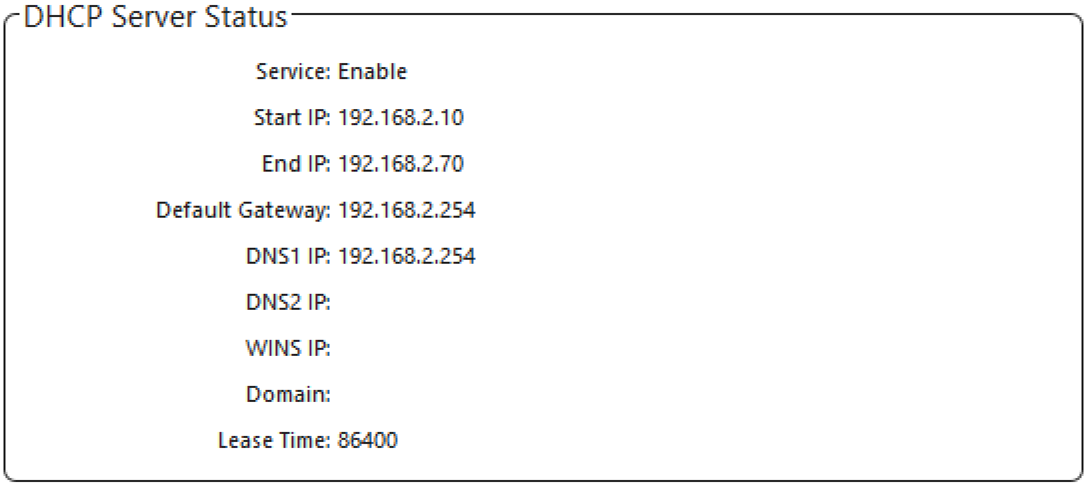
Traffic Monitor: Shows total transmit/receive LAN traffic on device

Wireless Information: *Shows current Wireless information, band, channel, output power and data rate*

Traffic Monitor: Shows total transmit/receive LAN traffic on device

8-2 DHCP Client

Administrators can view the status of all DHCP client users on each DHCP server. (This feature is only available in Router AP, ClientBridge + Repeater AP and CPE + Repeater AP Modes)



DHCP Server Status

Service: Enable

Start IP: 192.168.2.10

End IP: 192.168.2.70

Default Gateway: 192.168.2.254

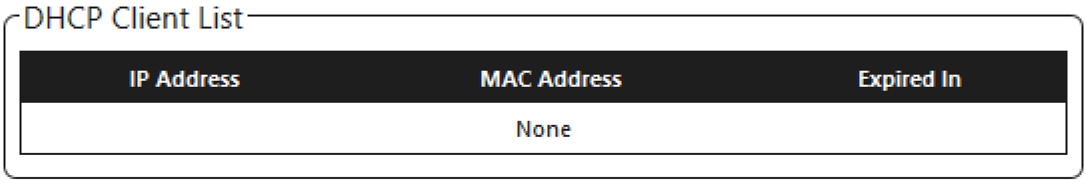
DNS1 IP: 192.168.2.254

DNS2 IP:

WINS IP:

Domain:

Lease Time: 86400



DHCP Client List

IP Address	MAC Address	Expired In
	None	

DHCP Server Status: *Display the information of the DHCP Server.*

DHCP Client List: *Display the information of the DHCP Client users.*

8-3 Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The **"Refresh"** button is used to retrieve latest table information.

Netstat Information: *This will show all connection track on the system, the information include Protocol, Live Time, Status, Source/Destination IP address and Port.*

Route Information: *This displays Route Information. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, its capable of being a gateway to route packets inward and outward.*

ARP Table Information: *ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.*

Bridge table information: *Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0~ra7 and wds0~wds3).*

Bridge MACs Information: *This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or* *wireless interfaces. Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.*

Bridge STP Information: *This table displays a list of bridge STP information.*

8-4 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

Time: *The date and time when the event occurred.*

Facility: *Identify source of events such as "System" or "User"*

Severity: *Severity level that a specific event is associated such as "info", "error", "warning", etc.*

Message: *Description of the event.*

Click **"Refresh"** button to renew the log

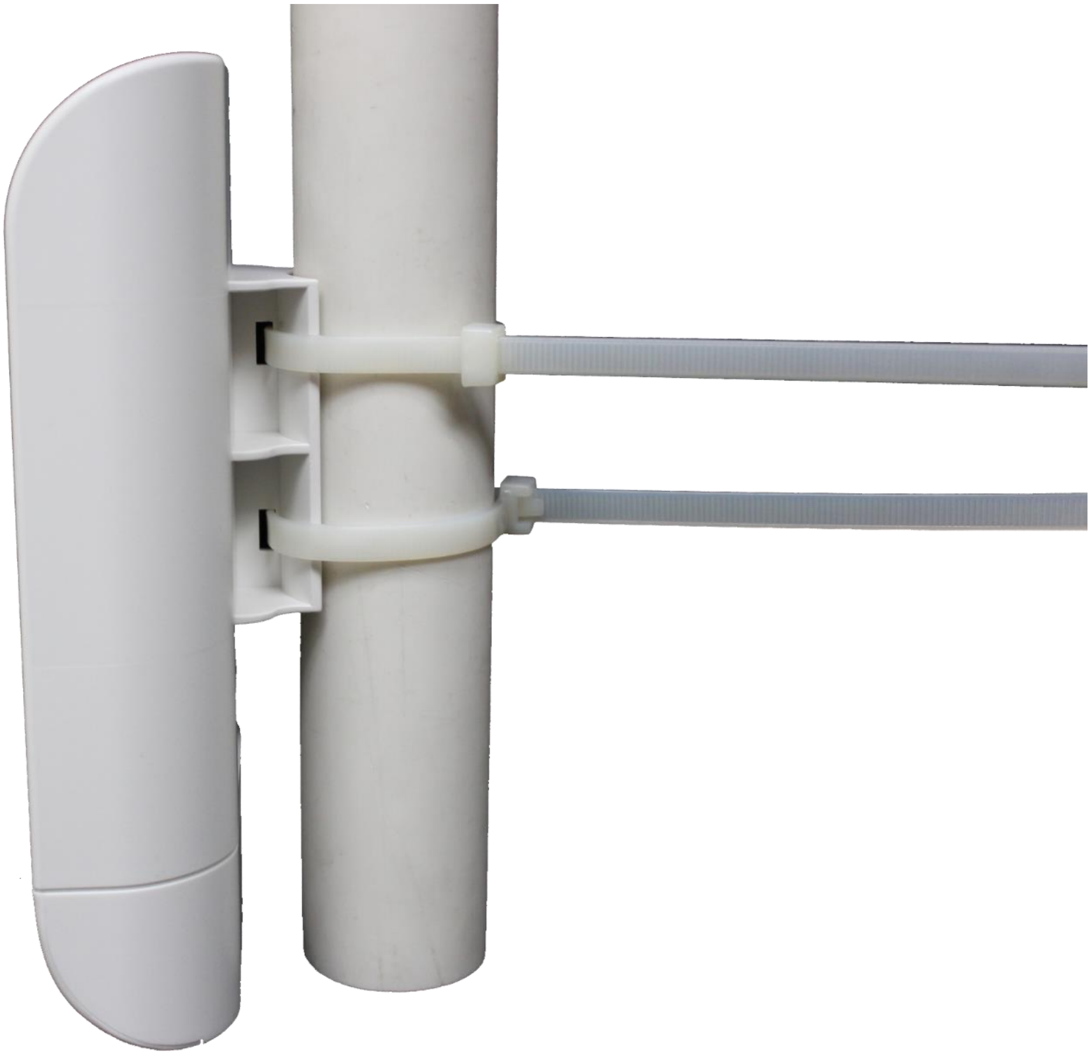
Click "**Clear"** button to clear all the records.

Chapter IX: Hardware Install

The HPOW5/HPOW10D are designed with wall mounts and pole mounts for exterior installations.

9-1 Pole Mount

Using the provided zip ties, secure the HPOW5/HPOW10D through the holes on the back of the device. Make sure they are tight and secure. Make sure the pole itself is secure.

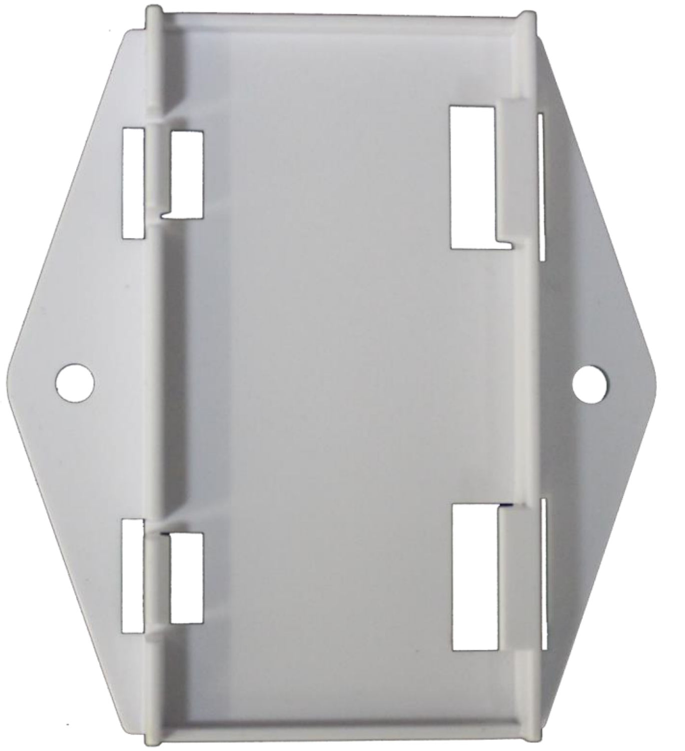


Note: you will need an Ethernet cable long enough to go from the device to the PoE injector. The PoE injector is not weather proofed. We do not recommend any cabling over 100 feet in length.

Note2: Make sure you also use a long enough grounding cable (not included) to mount to your grounding point. We recommend 16-18 AWG grounding cable

9-2 Wall Mount

Using the optional wall mount kit, first mount the wall mounting kit on a secure wall.



Screw it in using the provided screws. Once secure, simply snap the HPOW5/HPOW10D into the wall mount kit.

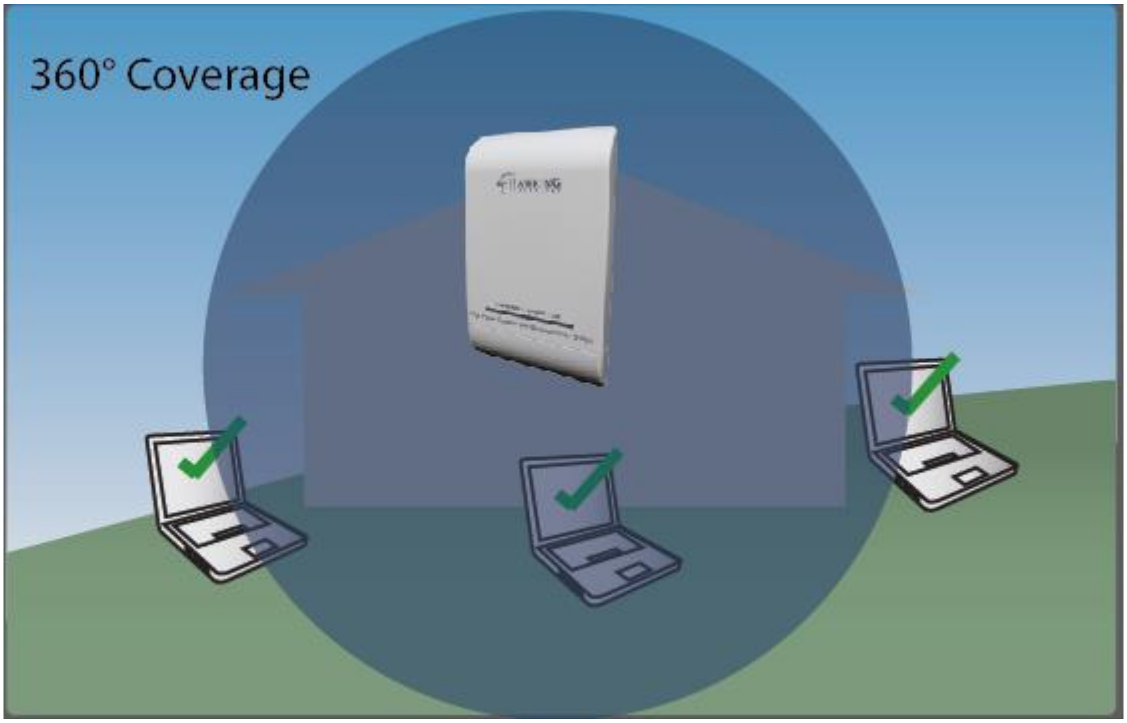
Note: you will need an Ethernet cable long enough to go from the device to the PoE injector. The PoE injector is not weather proofed. We do not recommend any cabling over 100 feet in length.

Note2: Make sure you also use a long enough grounding cable (not included) to mount to your grounding point. We recommend 16-18 AWG grounding cable

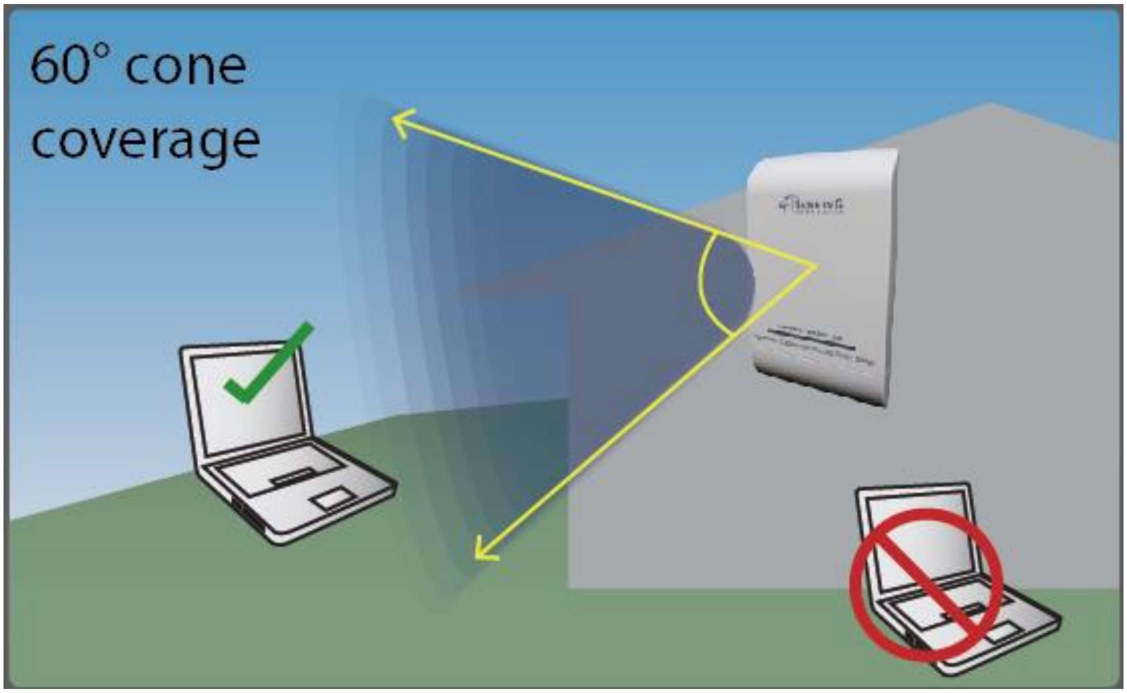
9-3 Antenna Orientation

Once you have mounted and connected HPOW5/HPOW10D, be sure to note the signal pattern of the antenna. Only devices within the transmission cone are guaranteed to get a good signal. You will receive optimal wireless signal by placing your wi-fi enabled device within the designated area. Adjust the antenna as needed.

The HPOW5 has a 360 degree coverage radius. As seen in the diagram below, the signal will be transmitted in a sphere around the HPOW5. All devices within the range of the device should get a signal.



The HPOW10D has a directional antenna that transmits in a 60 degree cone. As indicated by the diagram, the directional antenna does not give off a strong signal directly below or directly behind the product. The directional antenna allows you to aim your signal towards a specific source so you can better optimize your network needs.



Note: Your wireless coverage may vary depending on the receiving power of your wireless adapter. For example, if your wireless device only has a range of 100 feet and the HPOW5 has a range of 500 feet, your maximum range for your wireless device will be 100 feet. The weakest antenna determines the maximum range for that device.

Chapter X: Appendix

10-1 Specifications

Hardware Specification	
Base Platform	AR9341 **(AR1321)**
CPU Clock Speed	535 MHz
Wireless Radio	IEEE 802.11b/g/n
Serial Port	1 * Console (Internal)
Reset Switch Built-in	Push-button momentary contact switch
Standards Conformance	IEEE 802.3 / IEEE 802.3u
Ethernet Ports	• 2 x 10/100Mbps Ethernet ports (PoE Pass Through) • IEEE 802.3, 802.3u compliant • CSMA/CD 10/100 auto sense • Power over Ethernet (PoE)
Flash	On board : 8MB
SDRAM	On board : 32MB
Built-In LED Indicators	1 x Power, 2 x LAN, 4 x WLAN (Signal LED Indicator)
Wireless Specification	
Network Standards Conformance	IEEE802.11 b/g/n compliant
Data Transfer Rate	IEEE802.11b : 1 / 2 / 5.5 / 11Mbps (auto sensing) IEEE802.11g : 6/ 9/ 12/ 18/ 24/ 36/ 48/ 54Mbps (auto sensing) IEEE801.11n : 300Mbps (Tx), 300Mbps (Rx)
Frequency Range	2.412 ~ 2.462GHz (USA)
Channel Spacing	IEEE802.11b/g : 20MHz IEEE802.11n : 20/40MHz
Media Access Protocol	CSMA/ CA with ACK
Modulation Method	IEEE 802.11b: DSSS (DBPK,DQPSK,CCK) IEEE 802.11g/n : OFDM(64-QAM,16-QAM,QPSK,BPSK)
RF Output Power	800mW (±2dB dBm)
Frequency Response Flatness	±1dB over operating range
Receive Sensitivity	-96dBm (±2dB dBm)

Environmental & Mechanical Characteristics	
Operating Temperature	-20 °C ~ 60 °C
Storage Temperature	-20 °C ~ 85 °C
Operating Humidity	100% Non-Condensing
Storage Humidity	100% Non-Condensing
Built-in Antenna	HPOW5: 5dBi, 2.4GHz Omni Antenna (H-Plane: 360, E-Plane: 60) HPOW10D: 10dBi, 2.4GHz Dual Polarization Directional Antenna (H-Plane: 60, E-Plane: 60)
Input Power	48 VDC
Ethernet Connector	2 * Ethernet Connector
Power Supply	AC Input : 110 – 220V AV Power DC Output : 48 VDC, 0.5A input (PoE Power Injector, support up to 1A)
Unit Weight	0.35KG
Unit Dimensions	165(H) *96(L)*48(W) (mm)