

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

USER'S MANUAL 

COPYRIGHT

Copyright ©2012 by Hawking Technologies. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

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

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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

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

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

Table of Contents

Chapter I: Product Information	1
1-1 Introduction and safety information	1
1-2 Safety Information	4
1-3 System Requirements	5
1-4 Package Contents	6
1-5 Product Overview	7
CHAPTER II: Repeater Mode	10
2-1 Repeater Quick Installation Guide	10
2-1-1 Hardware WPS button setup	12
2-2 Repeater Quick Setup	15
2-3 General Setup	20
2-3-1 System	20
2-3-2 Local Network	22
2-3-3 Wireless Network	27
3-3-3-1 Basic Wireless Settings	28
3-3-3-2 Advanced Wireless Settings	30
3-3-3-3 Security Settings	33
3-3-3-4 Wireless Access Control	39
3-3-3-5 Wi-Fi Protected Setup (WPS)	42
2-4 Status	45
2-5 Configuration Tools	48
2-6 Firmware Upgrade	50
2-7 System Reset	52
CHAPTER III: Bridge Mode	53

3-1 Bridge Quick Installation Guide.....	53
3-1-1 Hardware WPS button setup	55
3-2 Bridge Mode Quick Setup	58
3-3 General Setup	62
3-3-1 System	62
3-3-2 Local Network.....	64
3-3-3 Wireless Network	68
3-3-3-1 Basic Wireless Settings	69
3-3-3-2 Advanced Wireless Settings	71
3-3-3-3 Security Settings	74
3-3-3-4 Wireless Access Control	80
3-3-3-5 Wi-Fi Protected Setup (WPS)	83
3-4 Status	86
3-5 Configuration Tools	89
3-6 Firmware Upgrade.....	91
3-7 System Reset.....	93
CHAPTER IV: Access Point Mode	94
4-1 AP mode Quick Installation Guide.....	94
4-1-1 Hardware WPS button setup	95
4-2 Access Mode Quick Setup.....	97
4-3 General Setup	102
4-3-1 System	103
4-3-2 Local Network.....	106
4-3-3 Wireless Network	110
4-3-3-1 Basic Wireless Settings	111
4-3-3-2 Advanced Wireless Settings	114
4-3-3-3 Security Settings	117
4-3-3-4 Wireless Access Control	123
4-3-3-5 Wi-Fi Protected Setup (WPS)	126
4-3-3-6 Security Tips for Wireless Network.....	129
4-4 Status	133
4-5 Configuration Tools	136
4-6 Firmware Upgrade.....	138
4-7 System Reset.....	140
Chapter V: Appendix.....	141

5-1 Configuring TCP/IP on PC	141
5-1-1 Windows XP IP address setup	141
5-1-2 Windows Vista/7 IP address setup	143
5-1-3 Mac OS X IP Address Setup	145
5-2 Specification	146
5-3 Glossary	147

Chapter I: Product Information

1-1 Introduction and safety information

Thank you for purchasing the HWREN25 Hi-Gain™ Wireless-300N Wall Plug Multi-Function HWREN25!

The ultra-compact design and built-in power adapter allows you to install this HWREN25 everywhere, and still provide excellent network performance to extend the Wi-Fi signal and wireless coverage.

Other features of this Multi-Function HWREN25:

- Extend the wireless signal inside your home or office.
- Ultra-compact design while maintaining excellent network performance.
- LED signal indicator to easily recognize the best location placement to extend Wireless signal and secure better wireless performance.
- The device supports Repeater mode, Access Point mode and Bridge mode
- Hardware switch button lets user change operation modes without logging into web firmware.
- WPS (Wi-Fi Protected Setup) hardware button for easy installation and secure wireless security.

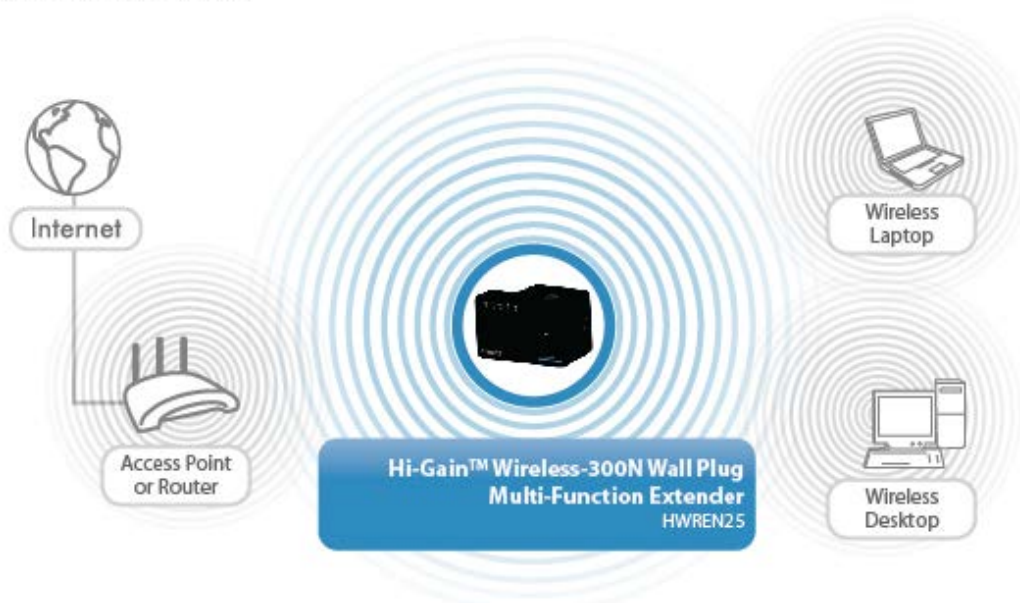
1-2 Definition of Supported Modes

Modes

The HWREN25 supports 3 different modes.

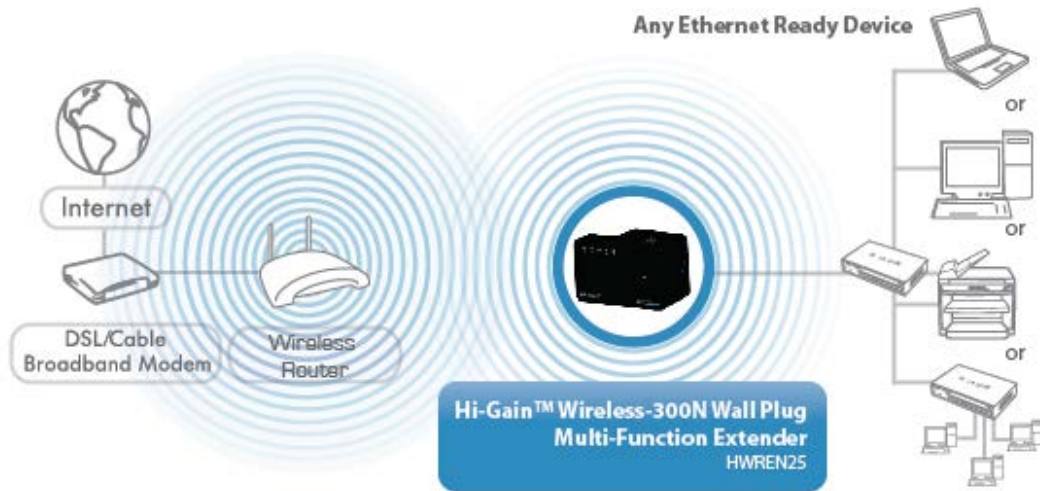
Repeater: Also known as range extender, this mode will allow you to repeat a selected wireless signal so you can extend the coverage of the existing wireless network. After setup, the device is standalone. Computers or other networked devices can also be wired into the network port on the unit.

UNIVERSAL REPEATER



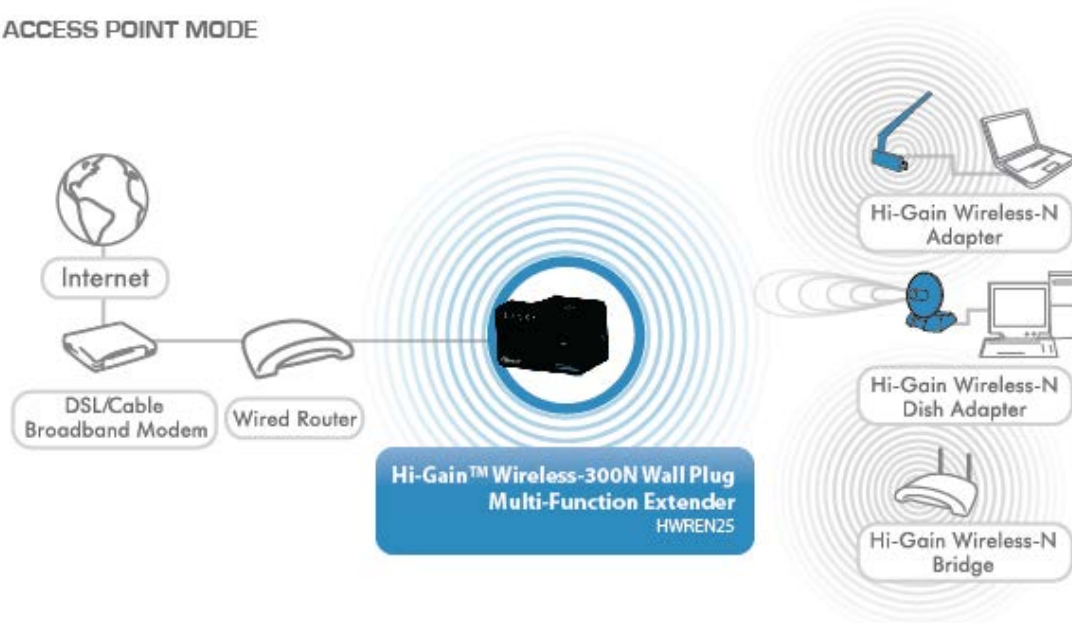
Bridge Mode: The HWREN25 will allow you to connect wired devices wirelessly to an existing wireless router or access point. It will “bridge” these devices wirelessly with your network. It will not broadcast any Wireless signal. It will only make a wireless connection between the Access Point and the HWREN25 and allow devices that are only wired to connect to the wireless network.

Station - Infrastructure (Bridge Mode)



Access Point: The HWREN25 will broadcast a Wireless signal for other computers and devices to connect to. Must be plugged into the router or network after setup.

ACCESS POINT MODE



1-3 Safety Information

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

1. This wireless HWREN25 is designed for indoor use only. **DO NOT** expose this device to direct sun light, rain, or snow.
2. **DO NOT** put this at or near hot or humid places, like kitchen or bathroom. Also, do not leave this Wireless HWREN25 in the car in summer.
3. Do not allow children to put any parts of this wireless HWREN25 in their mouths. It could cause serious injury or could be fatal. If they throw this wireless HWREN25, it will be damaged. **PLEASE KEEP THIS WIRELESS HWREN25 OUT OF THE REACH OF CHILDREN!**
4. This Wireless HWREN25 will become hot when being used for long time (***This is normal and is not a malfunction***). **DO NOT** put the Wireless HWREN25 on paper, cloth, or other flammable objects.
5. There's no user-serviceable part inside the Wireless HWREN25. If you find that the Wireless HWREN25 is not working properly, please contact your place of purchase and ask for help. **DO NOT** disassemble the Wireless HWREN25 by yourself, warranty will be void.
6. If the Wireless HWREN25 falls into water, **DO NOT USE IT**. Please contact your place of purchase and ask for help or for Warranty Return.

1-4 System Requirements

- Computer or network device(s) with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, Mozilla Firefox web browser or Safari web browser*).
- An available AC power socket (100 – 240 V, 50/60Hz)

1-5 Package Contents

Before you start to use this Wireless HWREN25, please check if there's anything missing in the package. If so, please contact your place of purchase to claim missing items:

1x - Hi-Gain™ Wireless-300N Wall Plug Multi-Function HWREN25

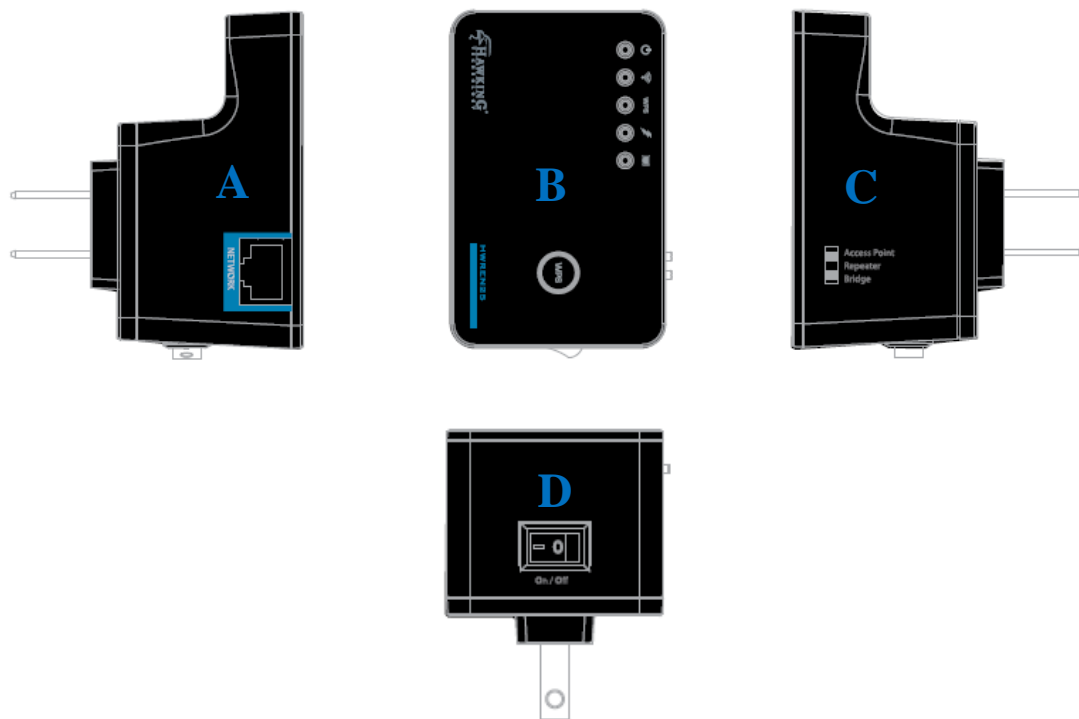
1x - Quick Installation Guide

1x - Ethernet cord

1x – CD containing user manual and product registration.

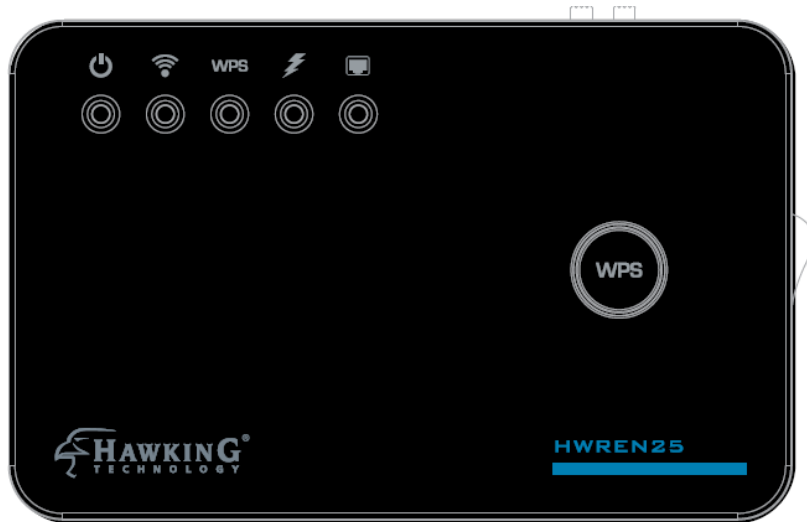
1-6 Product Overview





Interface Descriptions




Item	Item Name	Description
A	Network	10/100M Ethernet LAN Port with Auto-MDI/MDI-X. Connecting to computer, switch or hub for local network sharing.
B	Reset / WPS	Reset the HWREN25 to factory default settings (clear all settings) or start WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults. For WPS, press this button for less than 5 seconds to start WPS function.
C	Access Point/ HWREN25/ Bridge	Switch the button to change operating mode to Access Point or Range HWREN25 or Bridge mode.
D	ON/OFF	This is power on/off switch. If you want to switch off the HWREN25, switch it to Off mode.

LED Definitions



LED	Color	LED Status	Description
 Power	Green	Steady ON	Power is turned on.
		Slow Blinking	Ready for “Reset to factory default”, power LED is blinking.
		Off	Power is turned off.
 Wireless	Green	Blinking	Connected to wireless network. Wireless function is active (transferring or receiving data)
		Off	Wireless network is not connected or on.
 WPS	Green	Steady ON	When WPS connection is successful, turn on for 5 minutes.
		Blinking	WPS is in progress of waiting for WPS device’s connection, blinking (0.2 second on, 0.1 second off) for 2 minutes.
		Quick Blinking	WPS error, blinking (0.1 second on, 0.1 second off)
		Off	NO WPS is in progress/ LED off mode
 Signal	Amber	Steady ON	Excellent signal reception (signal strength 100%~67%).
		Blinking	Good signal reception Quick Blinking (66%~33%)

			Poor signal reception Slow blinking (<33%)
		Off	No Signal
 LAN	Green	Steady ON	LAN port is connected.
		Blinking	LAN port is active (transferring or receiving data)
		Off	LAN port is not connected

CHAPTER II: Repeater Mode

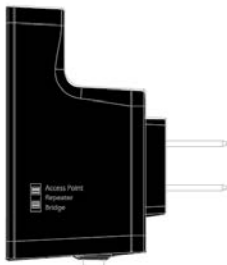
The HWREN25 is designed with the wireless repeater mode. This mode allows you to repeat your wireless signal and coverage and help you to solve wireless dead zones.

This chapter will show you how to quickly install this device by using quick setup and define the settings on the web based interface.

2-1 Repeater Quick Installation Guide

For first time setup and easy installation, you can move this device close to the Wireless Broadband Router or Access point you wish to connect to. After the installation is done and wireless connection is made, you can move this HWREN25 to the place you wish to use.

On the Top of the product, change the Switch mode selector to '**Repeater**'.



Insert this device into a power outlet in the wall, and switch the Wireless HWREN25's power switch to '**ON**'. You should see '**Power**' LED light up in a few seconds. If not, please check if the power outlet you're using is working.

There are two ways to set this up:

You can build wireless connection via 'Hardware WPS button' or 'Software web browser'.

If your wireless router or access point supports 'WPS', we recommend you use the WPS button to establish connection. It is the fast and secure

way without computer.

Using WPS button

- please go to section 2-1-1

Using Web browser

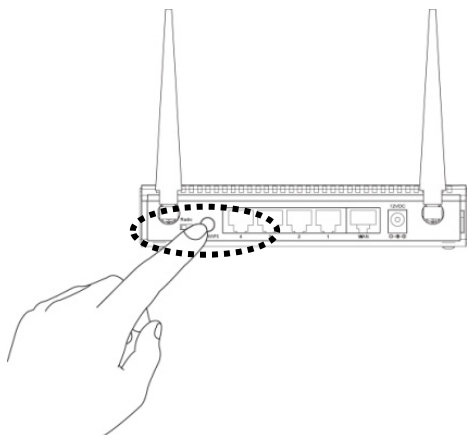
- please go to section 2-2

2-1-1 Hardware WPS button setup

(1) Press and hold **WPS button** on HWREN25 for 2 seconds, '**WPS**' LED will start flashing.



(2) Press **WPS button** on the wireless broadband router or access point you wish to connect within 2 minutes.



NOTE: this WPS button position on access point is an example. Different devices may have different WPS button position.

TIP: If the access point you wish to connect does not have hardware WPS button, you can also use its web configuration menu's WPS function to establish connection. You can also login to this HWREN25's web UI and do the setup there. (Refer to 2-1-2)

(3) If WPS connection is successfully established, '**WPS**' LED will light for 5 minutes; if '**WPS**' LED flashes fast, there's something wrong. Please wait for 2 minutes until '**WPS**' LED off, and try from step 1 again.



When WPS installation is successful, 'WLAN' LED will turn on.



(4) Please move the Wireless HWREN25 to the place you wish to use it (the best place would be a midpoint between your router and your wireless devices so the HWREN25 can relay the signal).

You can check the '*Signal*' LED status to understand signal reception level.

Steady light: Excellent, signal > 67%

Quick Flash: Good, signal < 66%

Slow Flash: Fair, signal < 33%

No Flash: no signal.

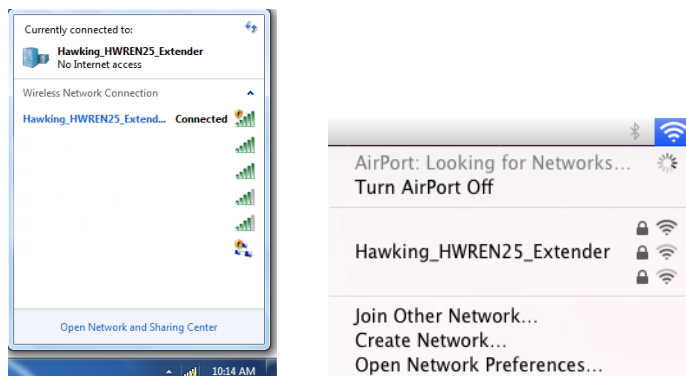
NOTE: If the Signal LED is off, it means the location is out of range of your wireless broadband router or access point. Please move this HWREN25 closer to the broadband router until the HWREN25 can receive signal from broadband router and repeat its signal.

2-2 Repeater Quick Setup

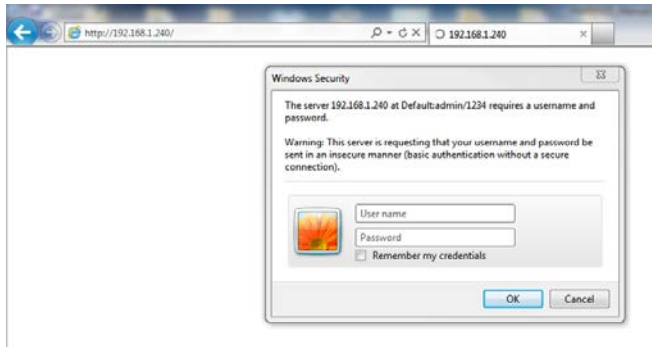
Before you can connect to the HWREN25 and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use a static IP address, please refer to '*Chapter V: Appendix, 5-1 Configuring TCP/IP on PC*' to set your computer to use dynamic IP address.

(1) Use Ethernet cable to connect your computer's Ethernet port and wireless HWREN25's Ethernet port.

Or use your computer's wireless configuration utility to search for a wireless network called '**Hawking_HWREN25_Extender**' and get connected. (The default wireless name of this HWREN25 device is: '**Hawking_HWREN25_Extender**')



(2) Open web browser and input '**http:// 192.168.1.240**' in address bar. A window will prompt you to input username and password. Default username is '**admin**' and password is '**1234**'. Click 'OK' button to continue.



(3) Once you are logged in, the HWREN25 setup page will appear.

Welcome to the Setup Wizard

This section allows you to set up your Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender in Range Extender Mode.

Basic Settings

You will need to first scan for an available wireless network (**Hot Spot**) to connect and redistribute within your current "**Home Network**" location.

Click **Scan** to begin a search for available networks.

By default, the HWREN25 will use the same SSID as your Home Wireless Connection.
 Note: To name the extended SSID with a different SSID, please uncheck the box below:

Wireless SSID:

Scan for a wireless network to extend your WiFi network:

Please choose your wireless network from the list below

Select	Band	Chan	SSID	Encry	Auth	Sign
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	68
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	32
<input type="radio"/>	(B)	10	HPC6F86E		no	6

4) By default, the HWREN25 will use the same Wireless Name as the network you are trying to extend. However, if you want to use your own unique name to identify the HWREN25, you can uncheck this box and type in your own name.

By default, the HWREN25 will use the same SSID as your Home Wireless Connection.
Note: To name the extended SSID with a different SSID, please uncheck the box below:

Wireless SSID:

5) The wireless networks available in your area will appear in this window

Please choose your wireless network from the list below

Select	Band	Chan	SSID	Encry	Auth	Sign
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	68
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	32
<input type="radio"/>	(B)	10	HPC6F86E		no	6

-OR- If you want to manually input your SSID:

Source AP ID: Enter the SSID and channel of your original access point:

SSID: Ch:

Please select your network that you wish to repeat. You may also manually enter in your wireless network's SSID and channel.

(6) Advanced IP address settings: This section allows you to set an IP Address and subnet mask to fit your network if needed. Uncheck the box to input. Otherwise, the default IP Address is 192.168.1.240
Note: It is recommended you give it an IP address in the same range of your network. Otherwise, once it is configured it will not be in the same range and you will not be able to access the setup page to view the general settings.

Advanced Settings

To input your own IP Address settings, Uncheck the box and enter it below.
Note: The default IP address of the HWREN25 is 192.168.1.240

IP Address:

Subnet Mask:

7) Click “Connect”

8) If your wireless network you hope to extend has wireless security, the next page will prompt you to enter in your security key. Please make sure you type in the exact key as the wireless network. If you are unsure what your key is, please contact the wireless router/access point’s manufacturer or your network administrator. Click Apply when you’re done.

Welcome to the Setup Wizard

This section allows you to set up your Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender’s security. The wireless network you are trying to connect has wireless security enabled. Please enter the security code below. If you do not know your security code, please contact the network administrator.

Wireless Security or Passphrase

Wireless Password:

Display characters

Save settings successfully!

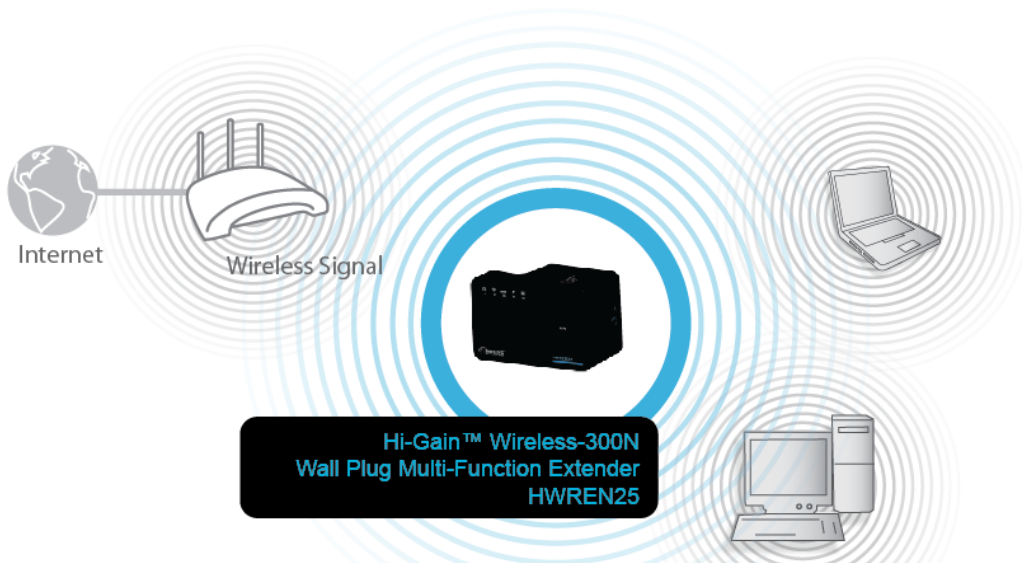
Please press APPLY button to restart the system to make the changes take effect.

System Restarting! Please wait for a while !

21%

(8) After reboot is complete, you can close the web browser to finish this quick setup. The HWREN25 will now be in extender mode. Please place the extender in an optimal location.

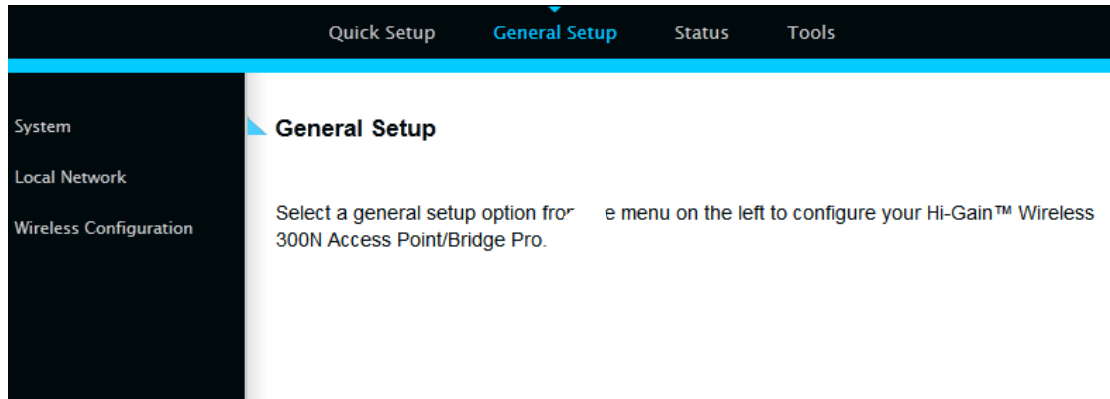
The HWREN25 should be placed in optimal location within the range of your wireless network.



Make sure the Extender is placed in a location where it can receive a strong signal from your desired wireless Internet connection. The Extender will not work without a signal it can repeat.

2-3 General Setup

In this chapter, you'll know how to change the major settings of the HWREN25. Log onto the device and click on 'General Setup'.



2-3-1 System

Change password

Default password of the HWREN25 is '1234', and it's displayed on the login prompt when accessed from the web browser. There's a security risk if you don't change the default password, since everyone can see it at the prompt. This is very important when you have wireless function enabled.

To change password, please follow the instructions:

Please click 'General Setup' at top of web management interface, select 'System' tab on the left hand column, and then click 'Password Settings', and the following message will be displayed on your web browser:

Password Settings

You can change the password required while logging into the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's web-based management system. By default, the password is 1234.

Passwords can contain 0 to 30 alphanumeric characters and are case sensitive.

Current Password: 1
New Password: 2
Confirm Password: 3

Current Password (1): Please input current password here.

New Password (2): Please input new password here.

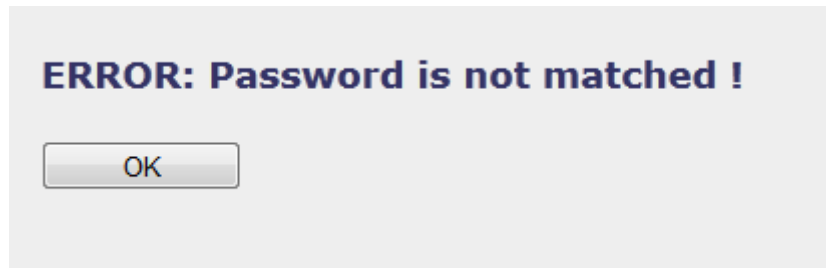
Confirm Password (3): Please input new password here again.

If the password you typed in 'New Password' (2) and 'Confirm Password' (3) field are not the same, you'll see the following message:

Password is not matched.

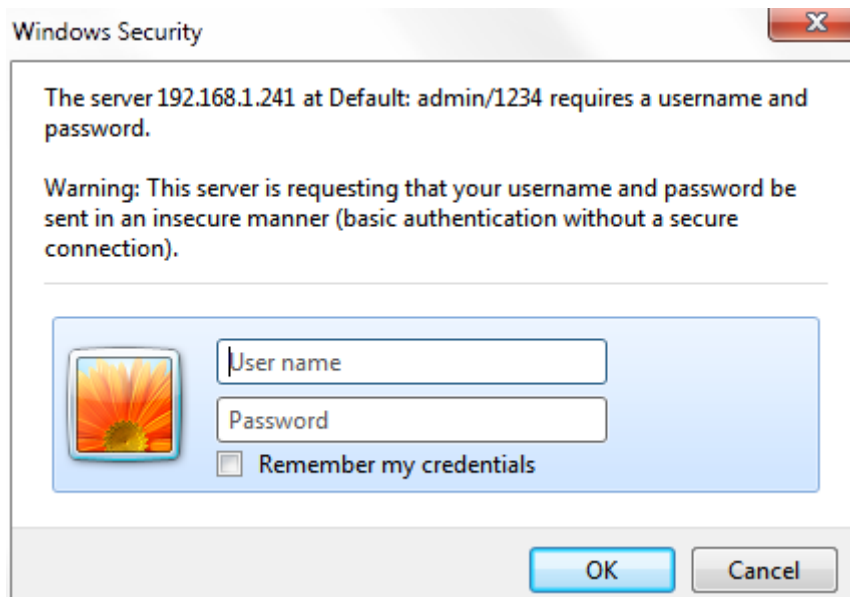
Please retype the new password again when you see above message.

If you see the following message:



It means the content in 'Current Password' field is wrong, please click 'OK' to go back to previous menu, and try to input current password again.

If the current and new passwords are correctly entered, after you click 'Apply', you'll be prompted to input your new password:



Please use new password to enter web management interface again, and you should be able to login with new password.

2-3-2 Local Network

Before all computers using wired Ethernet connection (i.e. those computers connected to this access point's LAN port 1 to 5 by Ethernet cable) can communicate with each other and access Internet, they must have a valid IP address.

There are two ways to assign IP addresses to computers: static IP address

(set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by access point automatically). It's recommended for most computers to use dynamic IP address, it will save a lot of time on setting IP addresses for every computer, especially when there are a lot of computers in your network; for servers and network devices which will provide services to other computers and users that come from the Internet, a static IP address should be used.

Suggestions on IP Address numbering plan:

If you have no idea on how to define an IP address plan for your network, here are some suggestions.

1. A valid IP address has 4 fields: a.b.c.d, for most of home and company users, it's suggested to use 192.168.c.d, where c is an integer between 0 and 254, and d is an integer between 1 and 254. This router is capable to work with up to 253 clients, so you can set 'd' field of IP address of router as 1 or 254 (or any number between 1 and 254), and pick a number between 0 and 254 for field 'c'.
2. In most cases, you should use '255.255.255.0' as subnet mask, which allows up to 253 clients (this also meets router's capability of working with up to 253 clients).
3. For all servers and network devices which will provide services to other people (like Internet service, print service, and file service), they should use static IP address. Give each of them a unique number between 1 and 253, and maintain a list, so everyone can locate those servers easily.
4. For computers which are not dedicated to provide specific service to others, they should use dynamic IP address.

Please click 'General Setup' at the top of web management interface and click 'Local Network' on the left hand column.

There are two setup groups here: 'LAN IP' and 'DHCP Server'

LAN IP	
IP Address:	<input type="text" value="192.168.1.241"/> 1
Subnet Mask:	<input type="text" value="255.255.255.0"/> 2
Gateway Address:	<input type="text"/> 3
DHCP Server:	<input type="text" value="Disable"/> 4

IP address (1): Please input the IP address of this access point.

Subnet Mask (2): Please input subnet mask for this network.

Gateway Address (3): Please input your gateway address for the network.

DHCP Server (4): If you want to activate DHCP server function of this access point, select 'Enabled', or set it to

'Disabled'.

Recommended Value if you don't know what to fill:

IP Address: 192.168.1.241

DNS Server: (leave it blank)

Subnet Mask: 255.255.255.0

DHCP Server: Disabled

Gateway Address: (leave it blank)

DHCP Server	
Lease Time:	Forever 1
DHCP Client Start IP:	192.168.1.100 2
DHCP Client End IP:	192.168.1.200 3
DHCP Client Gateway:	0.0.0.0 4
DHCP Client DNS:	0.0.0.0 5
Domain Name:	repeater.com 6

These settings are only available when ‘DHCP Server’ in ‘LAN IP’ section is ‘Enabled’.

Lease Time (1): Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this access point from dropdown menu.

DHCP Client Start IP (2): Please input the start IP address of the IP range.

DHCP Client End IP (3): Please input the end IP address of the IP range.

DHCP Client Gateway (4): Please input your default gateway address

DHCP Client DNS (5): Please input your DNS server address

Domain Name (6): If you wish, you can also optionally input the domain name for your network. This is optional.

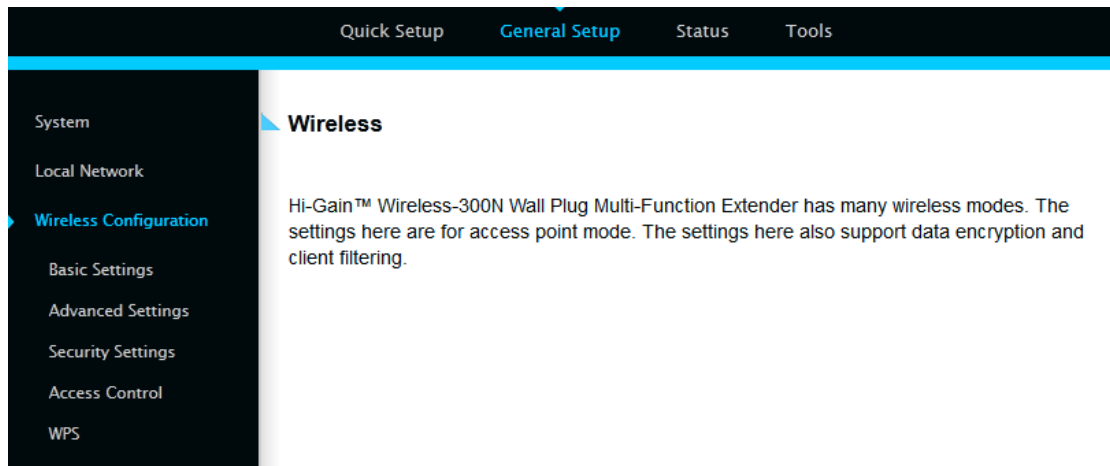
Recommended Value if you don't know what to fill:
 Lease Time: Two Weeks (or ‘Forever’, if you have less than 20 computers)
 Default Gateway: (leave it blank)
 Domain Server IP: (leave it blank)
 Start IP: 192.168.1.100
 End IP: 192.168.1.200
 Domain Name: (leave it blank)

NOTE:

1. The number of the last field (mentioned 'd' field) of 'End IP' must be greater than 'Start IP', and cannot be the same as router's IP address.
2. The former three fields of IP address of 'Start IP', 'End IP', and 'IP Address of 'LAN IP' section (mentioned 'a', 'b', and 'c' field) should be the same.
3. These settings will affect wireless clients too.

2-3-3 Wireless Network

Please click 'General Setup' tab at the top of web management interface, and then click 'Wireless Configuration' tab on the left hand column. The following message will be displayed on your web browser:



3-3-3-1 Basic Wireless Settings

Please click 'General Setup' menu at the top of web management interface, then click 'Wireless Configuration' on the left hand column. Choose 'Basic Settings'.

The HWREN25 will allow you connect wired devices wirelessly to an existing wireless router or access point. It will "bridge" these devices wirelessly with your network. It will not broadcast any WiFi signal. It will only make a wireless connection between the Access Point and the HWREN25.

Basic Settings

This page allows you to define the basic settings of the wireless access point.

Mode: Universal Repeater

Band: 2

SSID: 3

Channel Number: 4

Associated Clients: 5

Root AP SSID: 6

Wireless Network: 7

Band (2): Select the band you want to use. These should match the settings of your wireless network you are attempting to bridge.

SSID (3): This is the name of wireless network that the HWREN25 will broadcast.

Channel (4): This is the wireless channel that the HWREN25 will broadcast at. Please make sure it is the same channel of the existing network you hope to repeat.

Associated Clients (5): This button will show what wireless devices are currently connected to the HWREN25.

Root AP SSID (6): The network you are trying to repeat.

Select Wireless Network (7): Selecting this will allow you to choose a wireless network to extend. Select your network and click close. Click scan if your network does not appear.

Scan for a wireless network to extend your WiFi network:

Please choose your wireless network from the list below

Select	Band	Chan	SSID	Encry	Auth	Sign
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	68
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	32
<input type="radio"/>	(B)	10	HPC6F86E		no	6

After you finish these wireless settings, please click ‘Apply’ button, button, and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

Please click ‘Go Back’ to go back to previous setup menu; to continue on access point setup, or click ‘Apply’ to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

NOTE: If you don’t have special reason to limit the type of allowed wireless clients, it’s recommended to choose ‘2.4 GHz (B+G+N) to maximize wireless client compatibility.

3-3-3-2 Advanced Wireless Settings

This bridge provides some advanced control of wireless parameters, if you want to configure these settings, please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Choose "Advanced Settings".

Advanced Settings

Advanced wireless settings for your Wireless Network.

Fragment Threshold: (256 - 2346) 1
RTS Threshold: (0-2347) 2
Beacon Interval: (20-1000 ms) 3
DTIM Period: (0-2347) 4
Data Rate: 5
N Data Rate: 6
Channel Width: Auto 20/40 MHZ 20 MHZ 7
Preamble Type: Short Preamble Long Preamble 8
Broadcast ESSID: Enable Disable 9
CTS Protect: Auto Always None 10
Transmit Power: 11
WMM: Enable Disable 12

Cancel

Apply

Fragment Threshold(1): Set the Fragment threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2346'.

RTS Threshold(2): Set the RTS threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2347'.

Beacon Interval(3): Set the beacon interval of wireless radio. Do not modify the default value if you do not understand

the function, default value is '100'.

*DTIM Period(4): Set the DTIM period of wireless radio. **Do not modify the default value if you do not understand the function, default value is '3'.***

*Data Rate(5): Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically. **It is not necessary to change this value unless you know what will happen after modification.***

N Data Rate(6): Same as above, but only for 802.11n clients.

*Channel Width(7): Set channel width of wireless radio. **Do not modify the default value if you do not understand the function, default setting is 'Auto 20/40 MHz'.***

*Preamble Type(8): Set the type of preamble, **do not modify the default value if you do not know what it is, default setting is 'Short Preamble'.***

Broadcast ESSID(9): Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only those people who know the ESSID of your wireless access point can connect to the unit.

CTS Protect(10): Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. It is recommended to set this option to 'Auto' or 'Always'. However, if you set to 'None', your wireless access point should be able to function properly.

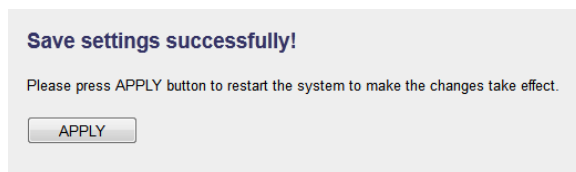
Transmit Power(11): You can set the output power of wireless radio.

*Unless you are using this wireless access point in a large open space, you may not have to set output power to 100%. **This will enhance security (malicious / unauthorized users in distance will not be able to reach your wireless access point).***

WMM(12):

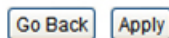
*Wi-Fi MultiMedia (WMM) will enhance the data transfer performance of multimedia contents when they are being transferred over a wireless network. **If you do not understand the function, then it is safe to set this option to 'Enable', however, default value is 'Disable'.***

After you finish these wireless settings, please click 'Apply' button, button, and the following message will be displayed on your web browser:



Settings Saved Successfully!

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.



Please click 'Go Back' to go back to previous setup menu; to continue on access point setup, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-3 Security Settings

It is important to set your wireless security settings properly! In bridge mode, the security settings must match the wireless network you are planning to connect to, otherwise, a connection cannot be established.

To set wireless security settings, please click 'General Setup' tab at the top of web management interface, then click 'Wireless Configuration' on the left hand column. Choose 'Security Settings'.

Please select an encryption method from the 'Encryption' dropdown menu, there are four options:

- Disable**
- WEP**
- WPA**
- WPA Radius**

Disable wireless security

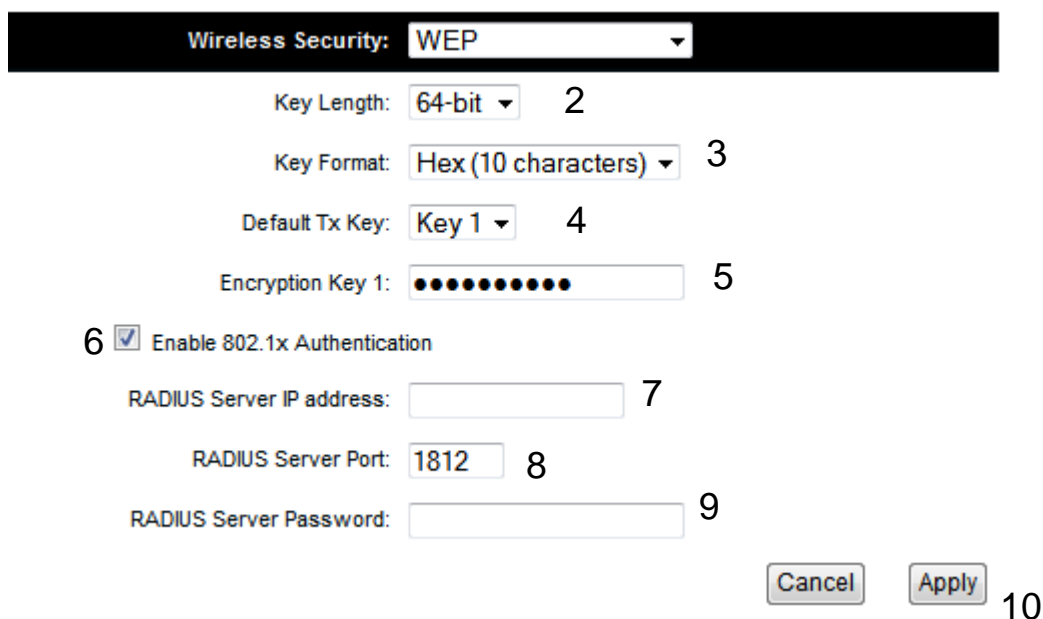
When you select this mode, data encryption is disabled.



Use this option only when there is no security set up on the original Wireless Signal.

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: WEP

Key Length: 64-bit 2

Key Format: Hex (10 characters) 3

Default Tx Key: Key 1 4

Encryption Key 1: ●●●●●●●●●● 5

6 Enable 802.1x Authentication

RADIUS Server IP address: 7

RADIUS Server Port: 1812 8

RADIUS Server Password: 9

Cancel Apply 10

Key Length (2): There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.

Key Format (3): There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key length, and 'Hex' as key format, you'll see the message at the right of 'Key Format' is 'Hex(10 characters)', which means the length of WEP key is 10 characters.

*Default Tx Key (4): **This device only supports one WEP Key 'Key 1'.***

Encryption Key (5) Input WEP key characters here, the number of characters must be the same as the number displayed at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be

same with each other.

Enable 802.1x Authentication (6): IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless access point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. If there is a RADIUS server in you environment, please enable this function. Check this box and another sub-menu will appear:

RADIUS Server IP address (7): Please input the IP address of RADIUS server here.

RADIUS Server Port (8): Please input the port number of RADIUS server here.

RADIUS Server Password (9): Please input the password here.

TIPS: Examples of WEP key

ASCII (5 characters): pilot phone 23561 2Hyux #@xml

ASCII (13 characters): digitalFAMILY 82Jh26xHy3m&n

Hex (10 characters): 287d2aa732 1152dabc85

Hex (26 characters): 9284bcda8427c9e036f7abcd84

To improve security level, do not use words that can be found in a dictionary or are easy to remember! Wireless clients will automatically remember the WEP key, so you only have to input the WEP key on wireless client once, and it is suggested that to use a complex WEP key to improve security level. Once you have chosen a password, write it down and keep it in a secure place.

After you finish WEP setting, please click ‘Apply’ (10) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

Wi-Fi Protected Access (WPA):

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 **WPA Pre-Shared Key** ▼

WPA Unicast Cipher Suite: WPA(TKIP) WPA(AES) WPA2(Mixed) 2

Pre-shared Key Format: Passphrase ▼ 3

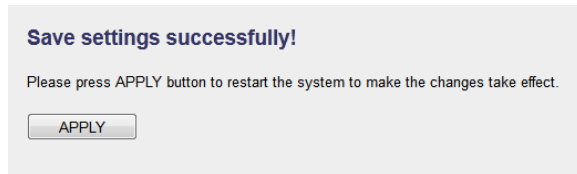
Pre-shared Key: 4

Cancel Apply 5

<i>WPA Unicast Cipher Suite (2):</i>	<i>Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.</i>
<i>Pre-shared Key Format (3):</i>	<i>Select the type of pre-shared key, you can select Passphrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).</i>
<i>Pre-shared Key (4):</i>	<i>Please input the WPA passphrase here. It's not recommended to use a word that can be found in a dictionary due to security reason.</i>

After you finish WPA Pre-shared key setting, please click 'Apply' button

(5) and the following message will be displayed on your web browser:

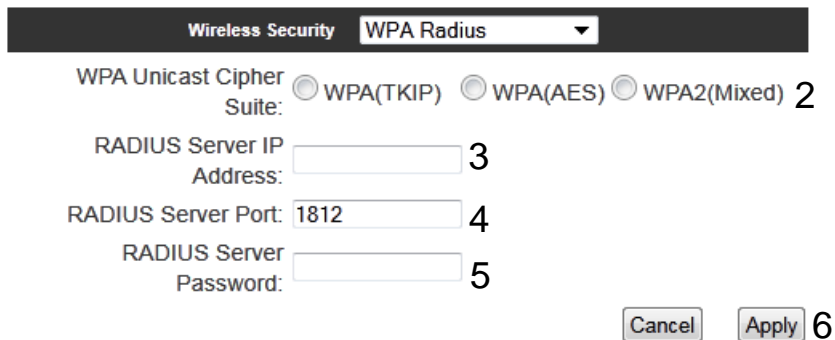


Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

NOTE: Some wireless clients (especially those manufactured before year 2003) only support WEP or WPA (TKIP) cipher. A driver upgrade would be needed for those clients to use WPA and WPA2 encryption.

WPA RADIUS:

If you have a RADIUS server, this access point can work with it and provide safer wireless authentication.



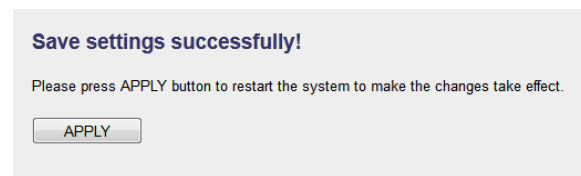
WPA Unicast Cipher Suite: Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.

RADIUS Server IP address (3): Please input the IP address of your Radius authentication server here.

RADIUS Server Port (4): *Please input the port number of your Radius authentication server here.*
Default setting is 1812.

RADIUS Server Password (5): *Please input the password of your Radius authentication server here.*

After you finish with all settings, please click ‘Apply’ (6) button and the following message will be displayed on your web browser:



Please click ‘Go Back’ to go back to previous setup menu, or click ‘Apply’ to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-4 Wireless Access Control

This function will help you prevent unauthorized users from connecting to your wireless access point; only those wireless devices who have a MAC address you assigned can gain access to your wireless access point. Use this function with other security measures described in previous section, to create a safer wireless environment.

You can add up to 20 MAC addresses by using this function. Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'Access Control'.

Access Control

For additional security, the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender features MAC Address Filtering that only allows authorized MAC Addresses to connect through the HWREN25.

MAC Address Filtering Table - up to 20 entries.

No.	MAC Address	Comment	Select
-----	-------------	---------	--------

6 Delete 7 Delete All

1 Enable Access Control

MAC Address	Comment
2 <input type="text"/>	3 <input type="text"/>

5 Clear 4 Add

8 APPLY CANCEL

All allowed MAC addresses will be displayed in 'MAC Address Filtering Table'.

Enable Wireless *To enforce MAC address filtering, you have to check*

Access Control (1): 'Enable Wireless Access Control'. When this item is unchecked, wireless access point will not enforce MAC address filtering of wireless clients.

MAC Address (2): Input the MAC address of your wireless devices here, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.

Comment (3): You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.

Add (4): Click 'Apply' button to add the MAC address and associated comment to the MAC address filtering table.

Clear (5): Click 'Clear' to remove the value you inputted in MAC address and comment field.

Delete Selected (6): If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete Selected' button. (You can select more than one MAC addresses).

Delete All (7): If you want to delete all MAC addresses listed here, please click 'Delete All' button.

After you finish with all settings, please click 'Apply' (8) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless access point. You don't have to select an encryption mode and input a long encryption passphrase every time when you need to set up a wireless client, you only have to press a button on the wireless client and this wireless access point, and the WPS will automatically configure for you.

This wireless access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless access point to WPS mode too. You can push Reset/WPS button of this wireless access point, or click 'Start PBC' button in the web configuration interface to do this; if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to this wireless access point. The detailed instructions are listed follow:

Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'WPS'.

Wi-Fi Protected Setup (WPS)

This section allows you to change the setting for Wi-Fi Protected Setup (WPS). Wi-Fi Protected Setup can help your wireless client automatically connect to the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender.

1 Enable WPS

WPS Information

WPS Status: Configured

2 PinCode Self: 87440386

SSID: Hawking_HWREN25_AP

Authentication Mode: WEP

Paraphrase Key:

Device Configure

Config Mode: Registrar 3

Configure by Push Button: Start PBC 4

Input client PIN code : Start PIN 5

Enable WPS (1) Check this box to enable WPS function, uncheck it to disable WPS.

WPS Information (2) WPS Status: If the wireless security (encryption) function of this wireless access point is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'Not configured'.

Self PIN code: This is the WPS PIN code of this wireless access point. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.

SSID: The SSID of this wireless access point will be displayed here.

Authentication Mode: The wireless security

authentication mode of this wireless access point will be displayed here. If you do not enable security function of the wireless access point before WPS is activated, the access point will auto set the security to WPA (AES) and generate a set passphrase key for WPS connection.

Passphrase Key: The wireless security key of the access point will be displayed here.

Config Mode (3) There are 'Registrar' and 'Enrollee' modes for the WPS connection. When 'Registrar' is enabled, the wireless clients will follow the access point's wireless settings for WPS connection. When 'Enrollee' mode is enabled, the access point will follow the wireless settings of wireless client for WPS connection.

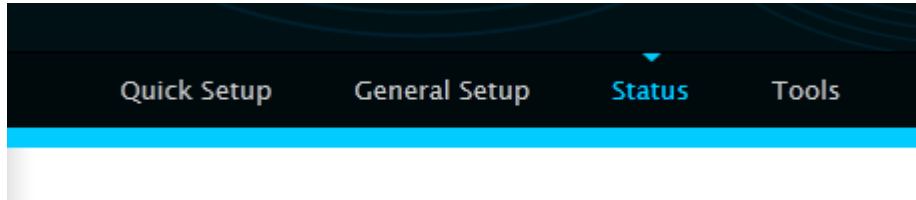
Configure by Push Button (4) Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless access point will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED light on the wireless access point will be steady for 2 minutes when this wireless access point is waiting for incoming WPS request.

Input client PinCode (5) Please input the PIN code of the wireless client you wish to connect, and click 'Start PIN' button. The 'WLAN' LED light on the wireless access point will be steady when this wireless access point is waiting for incoming WPS request.

2-4 Status

The status and information of the HWREN25 will be displayed here.

Click on the status tab on the top of web page.



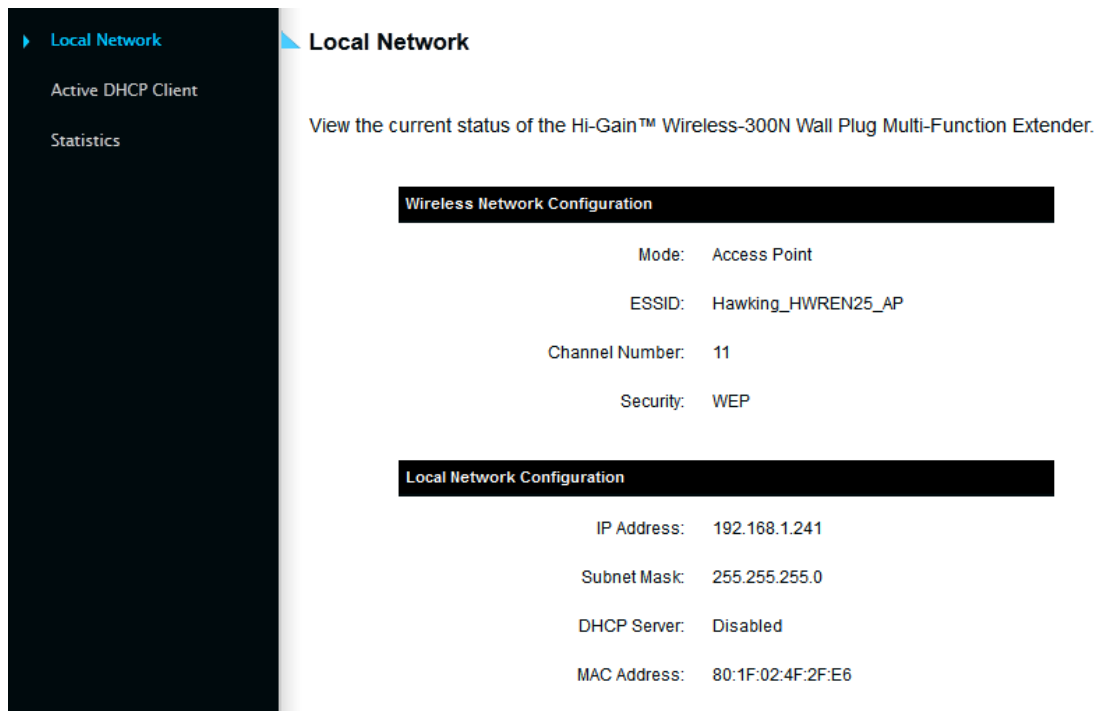
You should see the screen looks like this (the contents will vary depending on your current firmware):

Status

The Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's status information provides the following information: Hardware/Firmware version, Serial Number, and its current operating status.

System
Model: HWREN25
Up Time: 0day:1h:27m:58s
Hardware Version: Rev. A
Boot Code Version: 1.0
Firmware Version: 1.00

On the right hand column under status, click “Local Network”



Wireless Network Configuration: This section describes the current wireless settings of the HWREN25.

Mode: Current mode

ESSID: The broadcast name of the HWREN25

Channel: Current Wireless Channel

Security: The type of security the HWREN25 is using.

Local Network Configuration: This section describes the current network settings of the HWREN25

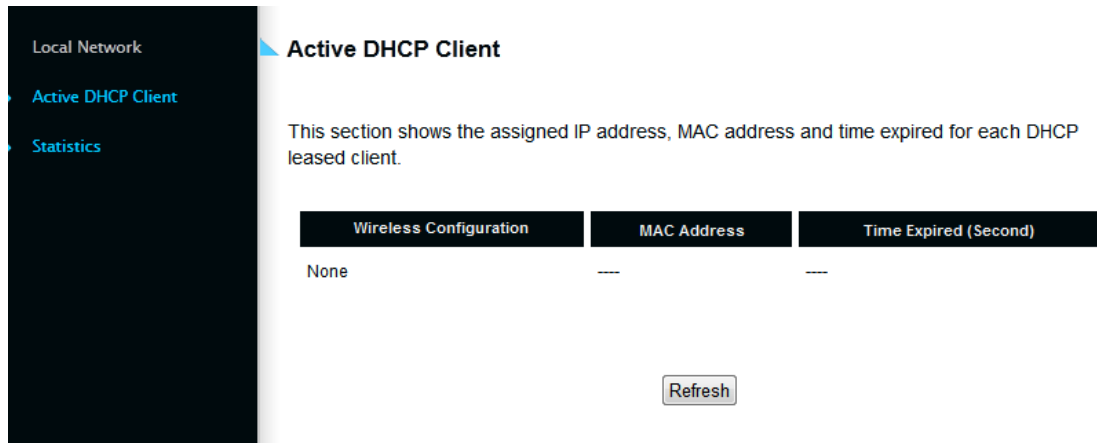
IP Address: Current IP address

Subnet Mask: Current subnet mask

DHCP Server: current status of the DHCP, enabled or disabled

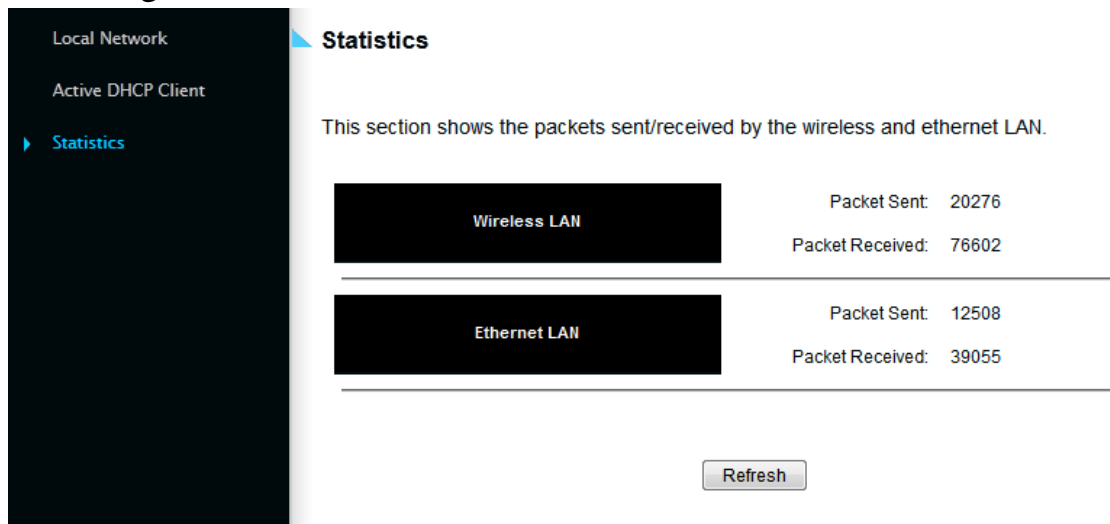
Mac Address: the Mac address of the HWREN25

On the right hand column, click Active DHCP Client



The Active DHCP Client describes clients that are current connected and receiving an IP address from the HWREN25. Only enabled if DHCP Server is enabled in the local network settings.

On the right hand column, click on Statistics



This section describes the amount of data sent/receive on both the wired and wireless connections.

2-5 Configuration Tools

You can back up all configurations of this access point to a file, so you can make several copies of the HWREN25's configuration for security reasons.

To backup or restore the HWREN25's configuration, please follow the instructions:

Please click 'Tools' menu at the top of web management interface, and then click 'Configuration Tools' on the left hand column.

Configuration Tools

Use the "Backup" tool to save the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Extender. Alternatively, you can use the "Restore to Factory Default" tool to force the Extender to perform System Reset and restore the original factory settings.

The screenshot shows a web interface with three sections. The first section is labeled 'Backup Settings' and contains a 'Save' button followed by the number '1'. A horizontal line separates this from the second section, 'Restore Settings', which includes a text input field, a 'Browse...' button, and an 'Upload' button, followed by the number '2'. The third section is 'Restore to Factory Default' with a 'Reset' button followed by the number '3'.

Backup Settings (1): Press 'Save...' button, and you'll be prompted to download the configuration as a file, default filename is 'default.bin', you can please save it as another filename for different versions, and keep it in a safe place.

Restore Settings (2): Press 'Browse...' to pick a previously-saved configuration file from your computer, and then click 'Upload' to transfer the configuration file to

access point. After the configuration is uploaded, the access point's configuration will be replaced by the file you just uploaded.

*Restore to
and*

Click this button to remove all settings you made,

Factory Default (3): restore the configuration of this access point back to factory default settings.

2-6 Firmware Upgrade

The system software used by this access point is known as ‘firmware’, just like any applications on your computer, when you replace the old application with a new one; your computer will be equipped with new function. You can also use this firmware upgrade function to add new functions to your access point, even fix the bugs of this access point.

To upgrade firmware, please follow the instructions:

Please click ‘Tools’ menu at the top of web management interface, and then click ‘Firmware Upgrade’ on the left hand column.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade. See below for the Extender's current firmware. You can go to www.hawkingtech.com for the latest firmware files.

The system will automatically reboot the after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the next step, you have to manually restart the Extender.

Firmware Version: 1.00

Next

Click ‘Next’ button if you wish to upgrade your firmware.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender. Enter the path and name of the upgrade file and then click the Apply button below. You will be prompted to confirm the upgrade.

Click 'Browse' button, and you'll be prompted to provide the filename of the firmware upgrade file. Please download the latest firmware file from the Hawking Technologies website at www.hawkingtech.com, and use it to upgrade your access point.

After a firmware upgrade file is selected, click 'Apply' button, and the access point will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnect your computer from router. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this router to the dealer of purchase to ask for help. Warranty is void if you interrupt the upgrade procedure.

2-7 System Reset

If you think your network performance is bad, or you find the behavior of the access point is strange, you can perform an access point reset. Sometimes it will solve the problem.

Please click 'Tools' menu at the top of the web management interface, and then click 'Reset' on the left-hand column.

Reset and Reboot

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

Reboot:

If resetting the Extender does not work, you may attempt to reset the Extender back to factory default settings. Note that all your current settings will be erased.

Reset to Factory Default Setting:

Please click 'Apply' to reset your access point, and it will be available again after a few minutes, please be patient.

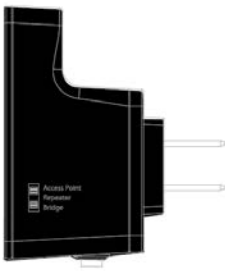
CHAPTER III: Bridge Mode

Client mode can let your networking device have wireless capability; it will become your device's wireless network card. You can connect this device to an Ethernet port on a TV or DVD player or game console device with Ethernet cable.

This chapter will show you how to quickly install this device by using quick setup and show you the each detailed setting on web UI page of client mode.

3-1 Bridge Quick Installation Guide

Switch mode selector to '**Bridge**'.



Insert this device into power outlet on the wall, and switch wireless HWREN25's power switch to '**ON**'. You should see '**Power**' LED light up in few seconds. If not, please check if the power outlet you're using is working.

Connect your wired networking device(wired PC, or internet TV, or game console..etc.) and this device by Ethernet cable.

NOTE: You must set your networking device as DHCP client (obtain IP automatically from DHCP server)

You can build wireless connection via 'Hardware WPS button' or 'Software web browser'.

If your wireless router or access point supports 'WPS', we recommend

you use the WPS button to establish connection. It is the fast and secure way without computer.

Using WPS button

- please go to section 3-1-1

Using Web browser

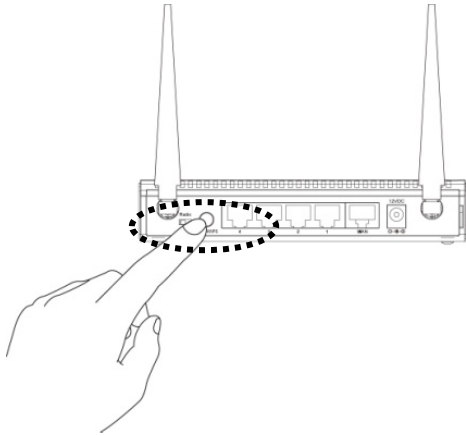
- please go to section 3-2

3-1-1 Hardware WPS button setup

(1) Press and hold **WPS button** on the HWREN25 for 2 seconds. The ‘**WPS**’ LED will start flashing.



(2) Press the **WPS button** on the wireless broadband router or access point you wish to connect within 2 minutes.



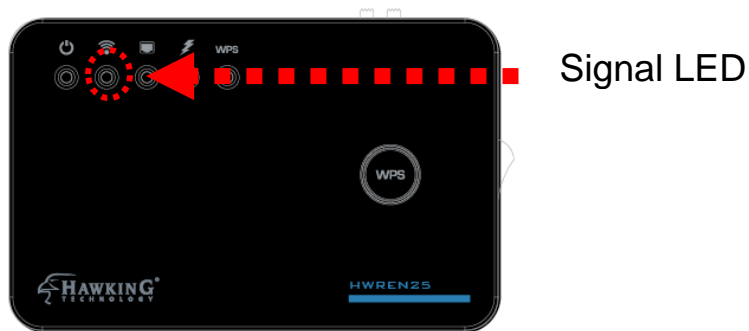
NOTE: Different devices will have different WPS button positions.

TIP: If the access point you wish to connect does not have hardware WPS button, you can also use its web configuration menu's WPS function to establish connection. You can also log into the HWREN25's web UI to do a quick setup. (refer. to section 3-2)

(3) If WPS connection is successfully established, the '**WPS**' LED will light for 5 minutes; if the '**WPS**' LED flashes fast, there's something wrong. Please wait for 2 minutes until '**WPS**' LED is off and try from step 1 again.



When WPS installation is successful, 'WLAN' LED will turn on.



You can check the '*Signal*' LED status to understand signal reception level.

Steady light: Excellent, signal > 67%

Quick Flash: Good, signal < 66%

Slow Flash: Fair, signal < 33%

No Flash: no signal.

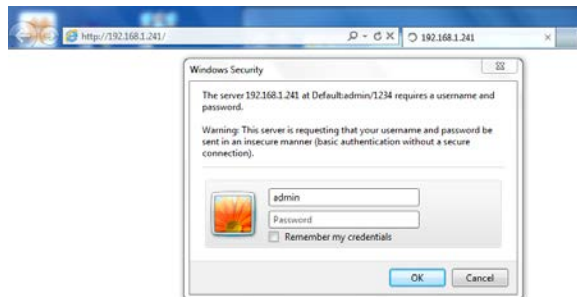
NOTE: If the Signal LED is off, it means the location is out of range of your wireless broadband router or access point. Please move this HWREN25 closer to the wireless signal until the HWREN25 can receive signal from broadband router and bridge the signal.

3-2 Bridge Mode Quick Setup

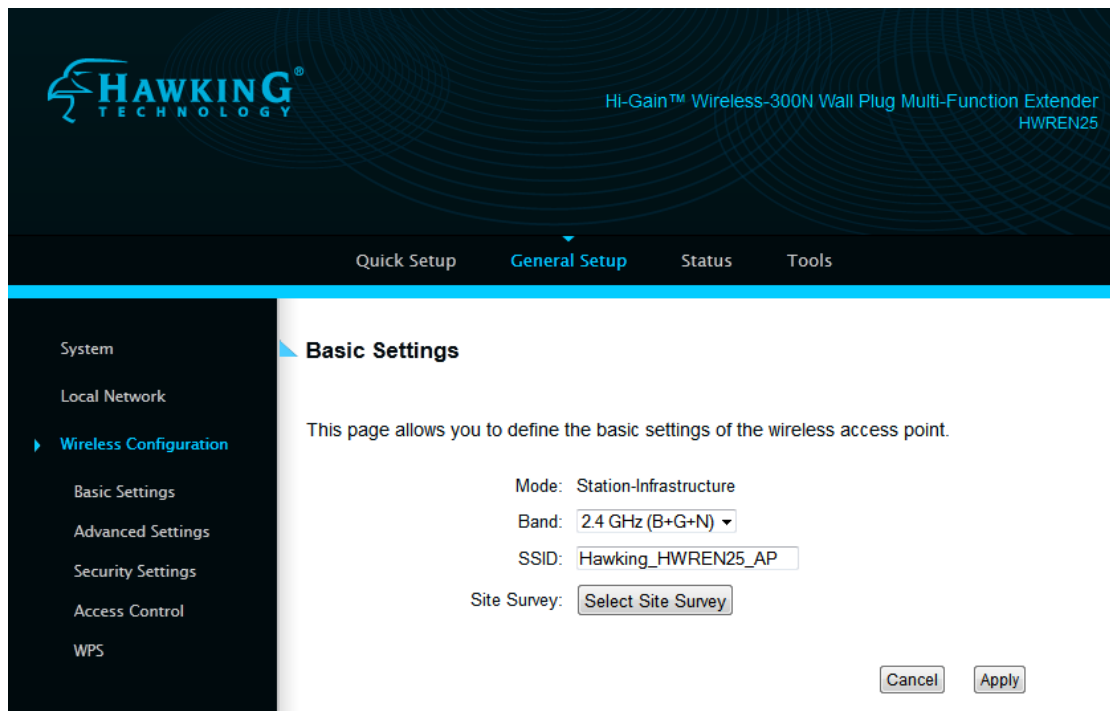
Before you connect to the HWREN25 and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please refer to '*Chapter 5-1 Configuring TCP/IP on PC*' to set your computer to use dynamic IP address.

(1) Use an Ethernet cable to connect your computer's Ethernet port and HWREN25's Ethernet port.

(2) Open web browser and input '**http:// 192.168.1.241**' in address bar. A window will prompt you to input username and password. Default username is '**admin**' and password is '**1234**'. Click 'OK' button to continue.



(3) Once you are logged in, the HWREN25 setup page will appear.



4) Click on “Select Site Survey” to choose the wireless network you wish to bridge to.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	Band	Channel	SSID	Encryption	Authentication	Signal
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	64
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	30
<input type="radio"/>	(B+G+N)	5	dlink		WEP	16

Select your network and click “Done”

The SSID field should be filled in with the network name you selected.

(5) Advanced IP address settings: This section allows you to set an IP Address and subnet mask to fit your network if needed. Uncheck the box to input. Otherwise, the default IP Address is 192.168.1.241
 Note: It is recommended you give it an IP address in the same range of your network. Otherwise, once it is configured it will not be in the same range and you will not be able to access the setup page to view the general settings.

Advanced Settings

To input your own IP Address settings, Uncheck the box and enter it below.

Note: The default IP address of the HWREN25 is 192.168.1.241

IP Address:

Subnet Mask:

6) After you have selected your wireless network and clicked apply, if your wireless network you hope to bridge has wireless security, the next page will prompt you to enter in your security key. Please make sure you type in the exact key as the wireless network. If you are unsure what your key is, please contact the wireless router/access point's manufacturer or your network administrator. Click Apply when you're done.

Welcome to the Setup Wizard

This section allows you to set up your Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's security. The wireless network you are trying to connect has wireless security enabled. Please enter the security code below. If you do not know your security code, please contact the network administrator.

Wireless Security or Passphrase

KEY :

Display characters

7) Click apply for your settings to take effect

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

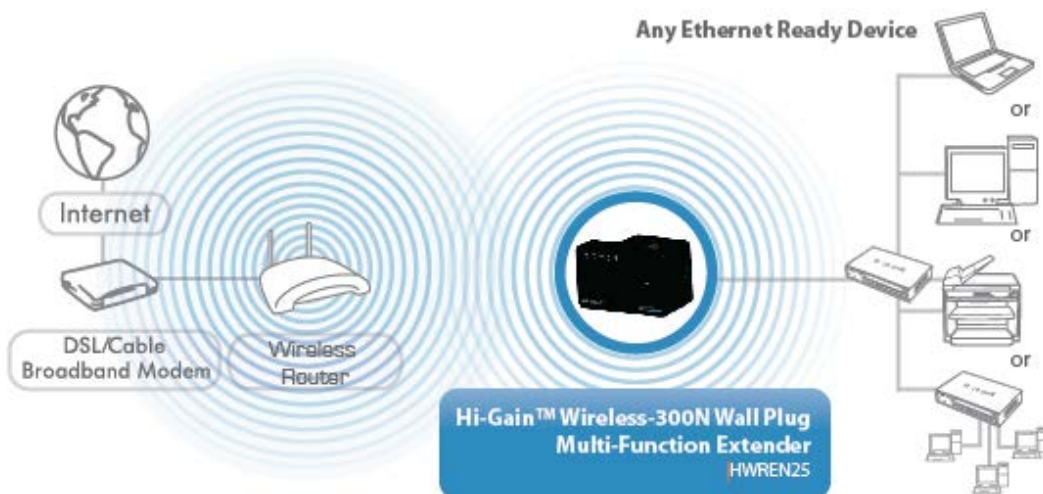
APPLY

System Restarting! Please wait for a while !

21%

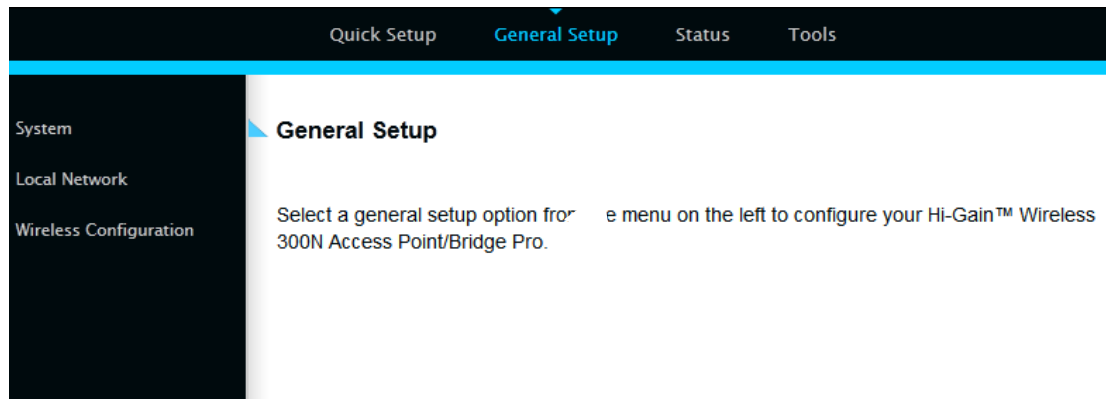
(8) After reboot complete, you can close the web browser to finish this quick setup. Connect the HWREN25 via Ethernet cable to the device you wish to bridge.

Station - Infrastructure (Bridge Mode)



3-3 General Setup

In this chapter, you'll know how to change the major settings of the HWREN25. Log onto the device and click on 'General Setup'.



3-3-1 System

Change password

Default password of the HWREN25 is '1234', and it's displayed on the login prompt when accessed from the web browser. There's a security risk if you don't change the default password, since everyone can see it at the prompt. This is very important when you have wireless function enabled.

To change password, please follow the instructions:

Please click 'General Setup' at top of web management interface, select 'System' tab on the left hand column, and then click 'Password Settings', and the following message will be displayed on your web browser:

Password Settings

You can change the password required while logging into the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's web-based management system. By default, the password is 1234.

Passwords can contain 0 to 30 alphanumeric characters and are case sensitive.

Current Password: 1
New Password: 2
Confirm Password: 3

Current Password (1): Please input current password here.

New Password (2): Please input new password here.

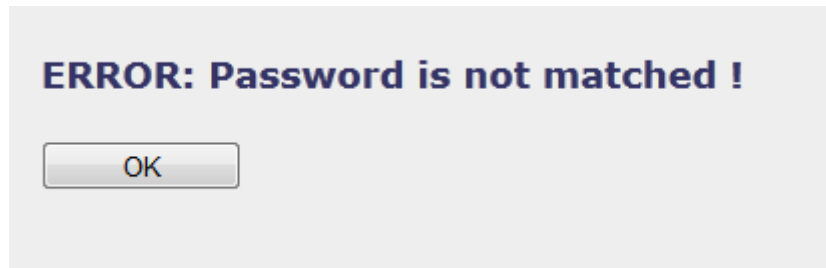
Confirm Password (3): Please input new password here again.

If the password you typed in 'New Password' (2) and 'Confirm Password' (3) field are not the same, you'll see the following message:

Password is not matched.

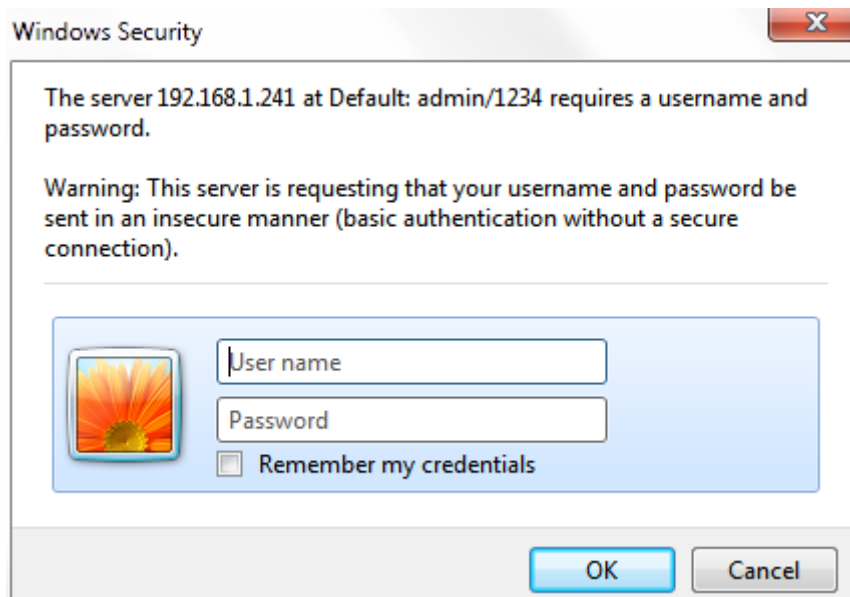
Please retype the new password again when you see above message.

If you see the following message:



It means the content in 'Current Password' field is wrong, please click 'OK' to go back to previous menu, and try to input current password again.

If the current and new passwords are correctly entered, after you click 'Apply', you'll be prompted to input your new password:



Please use new password to enter web management interface again, and you should be able to login with new password.

3-3-2 Local Network

Before all computers using wired Ethernet connection (i.e. those computers connected to this access point's LAN port 1 to 5 by Ethernet cable) can communicate with each other and access Internet, they must have a valid IP address.

There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by access point automatically). It's recommended for most computers to use dynamic IP address, it will save a lot of time on setting IP addresses for every computer, especially when there are a lot of computers in your network; for servers and network devices which will provide services to other computers and users that come from the Internet, a static IP address should be used.

Suggestions on IP Address numbering plan:

If you have no idea on how to define an IP address plan for your network, here are some suggestions.

- 5. A valid IP address has 4 fields: a.b.c.d, for most of home and company users, it's suggested to use 192.168.c.d, where c is an integer between 0 and 254, and d is an integer between 1 and 254. This router is capable to work with up to 253 clients, so you can set 'd' field of IP address of router as 1 or 254 (or any number between 1 and 254), and pick a number between 0 and 254 for field 'c'.**
- 6. In most cases, you should use '255.255.255.0' as subnet mask, which allows up to 253 clients (this also meets router's capability of working with up to 253 clients).**
- 7. For all servers and network devices which will provide services to other people (like Internet service, print service, and file service), they should use static IP address. Give each of them a unique number between 1 and 253, and maintain a list, so everyone can locate those servers easily.**
- 8. For computers which are not dedicated to provide specific service to others, they should use dynamic IP address.**

Please click 'General Setup' at the top of web management interface and click 'Local Network' on the left hand column.

There are two setup groups here: 'LAN IP' and 'DHCP Server'

LAN IP	
IP Address:	<input type="text" value="192.168.1.241"/> 1
Subnet Mask:	<input type="text" value="255.255.255.0"/> 2
Gateway Address:	<input type="text"/> 3
DHCP Server:	<input type="text" value="Disable"/> 4

IP address (1): Please input the IP address of this access point.

Subnet Mask (2): Please input subnet mask for this network.

Gateway Address (3): Please input your gateway address for the network.

DHCP Server (4): If you want to activate DHCP server function of this access point, select 'Enabled', or set it to 'Disabled'.

Recommended Value if you don't know what to fill:

IP Address: 192.168.1.241	DNS Server: (leave it blank)
Subnet Mask: 255.255.255.0	DHCP Server: Disabled
Gateway Address: (leave it blank)	

DHCP Server	
Lease Time:	Forever 1
DHCP Client Start IP:	192.168.1.100 2
DHCP Client End IP:	192.168.1.200 3
DHCP Client Gateway:	0.0.0.0 4
DHCP Client DNS:	0.0.0.0 5
Domain Name:	repeater.com 6

These settings are only available when 'DHCP Server' in 'LAN IP' section is 'Enabled'.

Lease Time (1): Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this access point from dropdown menu.

DHCP Client Start IP (2): Please input the start IP address of the IP range.

DHCP Client End IP (3): Please input the end IP address of the IP range.

DHCP Client Gateway (4): Please input your default gateway address

DHCP Client DNS (5): Please input your DNS server address

Domain Name (6): If you wish, you can also optionally input the domain name for your network. This is optional.

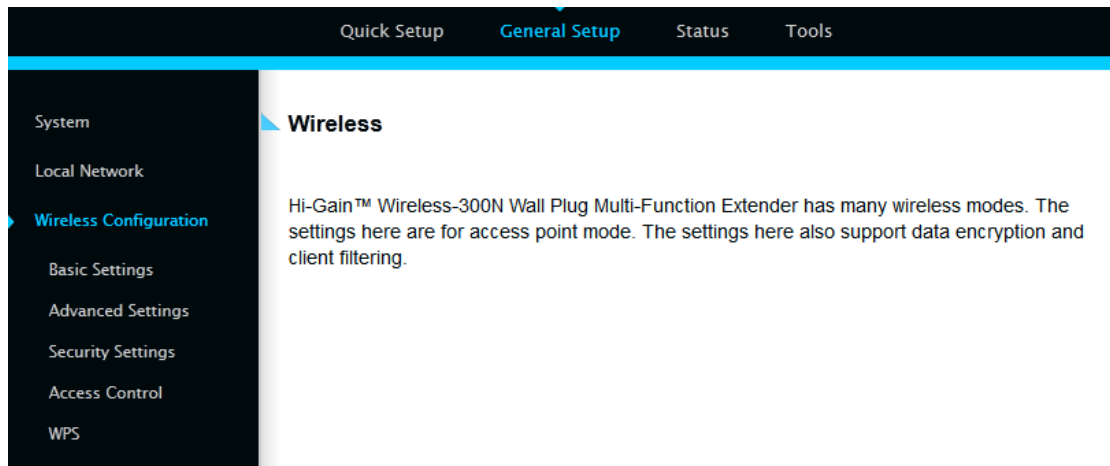
Recommended Value if you don't know what to fill:
 Lease Time: Two Weeks (or 'Forever', if you have less than 20 computers)
 Default Gateway: (leave it blank)
 Domain Server IP: (leave it blank)
 Start IP: 192.168.1.100
 End IP: 192.168.1.200
 Domain Name: (leave it blank)

NOTE:

1. The number of the last field (mentioned 'd' field) of 'End IP' must be greater than 'Start IP', and can not be the same as router's IP address.
2. The former three fields of IP address of 'Start IP', 'End IP', and 'IP Address of 'LAN IP' section (mentioned 'a', 'b', and 'c' field) should be the same.
3. These settings will affect wireless clients too.

3-3-3 Wireless Network

Please click 'General Setup' tab at the top of web management interface, and then click 'Wireless Configuration' tab on the left hand column. The following message will be displayed on your web browser:



3-3-3-1 Basic Wireless Settings

Please click ‘General Setup’ menu at the top of web management interface, then click ‘Wireless Configuration’ on the left hand column. Choose ‘Basic Settings’.

The HWREN25 will allow you connect wired devices wirelessly to an existing wireless router or access point. It will “bridge” these devices wirelessly with your network. It will not broadcast any WiFi signal. It will only make a wireless connection between the Access Point and the HWREN25.

Basic Settings

This page allows you to define the basic settings of the wireless access point.

Mode: Station-Infrastructure
Band: 2
SSID: 3
Site Survey: 4

Band (2): Select the band you want to use. These should match the settings of your wireless network you are attempting to bridge.

SSID (3): This is the name of wireless network you are attempting to connect to. Make sure it matches exactly with the wireless network you are attempting to connect to.

Site Survey (4): This allows you to select a wireless network to bridge to. ‘Select Site Survey’ button, then a “Wireless Site Survey Table” will pop up. It will list all available access points nearby. Please select the wireless network and click “Done” Click “Refresh” if you do not see your network.

Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	Band	Chan	SSID	Encry	Auth	Sign
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	64
<input type="radio"/>	(B+G+N)	3	HawkTech	AES	WPA2-PSK	30
<input type="radio"/>	(B+G+N)	5	dlink		WEP	16

After you finish these wireless settings, please click 'Apply' button, button, and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

Please click 'Go Back' to go back to previous setup menu; to continue on access point setup, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-2 Advanced Wireless Settings

This bridge provides some advanced control of wireless parameters, if you want to configure these settings, please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Choose "Advanced Settings".

Advanced Settings

Advanced wireless settings for your Wireless Network.

Fragment Threshold: (256 - 2346) 1
RTS Threshold: (0-2347) 2
Beacon Interval: (20-1000 ms) 3
DTIM Period: (0-2347) 4
Data Rate: 5
N Data Rate: 6
Channel Width: Auto 20/40 MHZ 20 MHZ 7
Preamble Type: Short Preamble Long Preamble 8
Broadcast ESSID: Enable Disable 9
CTS Protect: Auto Always None 10
Transmit Power: 11
WMM: Enable Disable 12

Cancel

Apply

Fragment Threshold(1): Set the Fragment threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2346'.

RTS Threshold(2): Set the RTS threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2347'.

Beacon Interval(3): Set the beacon interval of wireless radio. Do not modify the default value if you do not understand

the function, default value is '100'.

*DTIM Period(4): Set the DTIM period of wireless radio. **Do not modify the default value if you do not understand the function, default value is '3'.***

*Data Rate(5): Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically. **It is not necessary to change this value unless you know what will happen after modification.***

N Data Rate(6): Same as above, but only for 802.11n clients.

*Channel Width(7): Set channel width of wireless radio. **Do not modify the default value if you do not understand the function, default setting is 'Auto 20/40 MHz'.***

*Preamble Type(8): Set the type of preamble, **do not modify the default value if you do not know what it is, default setting is 'Short Preamble'.***

Broadcast ESSID(9): Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only those people who know the ESSID of your wireless access point can connect to the unit.

CTS Protect(10): Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. It is recommended to set this option to 'Auto' or 'Always'. However, if you set to 'None', your wireless access point should be able to function properly.

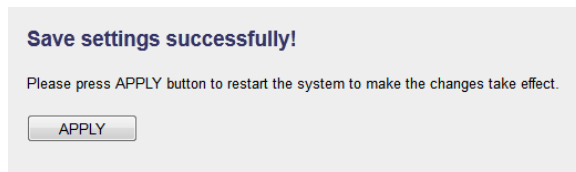
Transmit Power(11): You can set the output power of wireless radio.

*Unless you are using this wireless access point in a large open space, you may not have to set output power to 100%. **This will enhance security (malicious / unauthorized users in distance will not be able to reach your wireless access point).***

WMM(12):

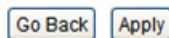
*Wi-Fi MultiMedia (WMM) will enhance the data transfer performance of multimedia contents when they are being transferred over a wireless network. **If you do not understand the function, then it is safe to set this option to 'Enable', however, default value is 'Disable'.***

After you finish these wireless settings, please click 'Apply' button, button, and the following message will be displayed on your web browser:



Settings Saved Successfully!

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.



Please click 'Go Back' to go back to previous setup menu; to continue on access point setup, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-3 Security Settings

It is important to set your wireless security settings properly! In bridge mode, the security settings must match the wireless network you are planning to connect to, otherwise, a connection cannot be established.

To set wireless security settings, please click 'General Setup' tab at the top of web management interface, then click 'Wireless Configuration' on the left hand column. Choose 'Security Settings'.

Please select an encryption method from the 'Encryption' dropdown menu, there are four options:

- Disable**
- WEP**
- WPA**
- WPA Radius**

Disable wireless security

When you select this mode, data encryption is disabled.



Use this option only when there is no security set up on the original Wireless Signal.

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: WEP

Key Length: 64-bit 2

Key Format: Hex (10 characters) 3

Default Tx Key: Key 1 4

Encryption Key 1: ●●●●●●●●●● 5

6 Enable 802.1x Authentication

RADIUS Server IP address: 7

RADIUS Server Port: 1812 8

RADIUS Server Password: 9

Cancel Apply 10

Key Length (2): There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.

Key Format (3): There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key length, and 'Hex' as key format, you'll see the message at the right of 'Key Format' is 'Hex(10 characters)', which means the length of WEP key is 10 characters.

*Default Tx Key (4): **This device only supports one WEP Key 'Key 1'.***

Encryption Key (5) Input WEP key characters here, the number of characters must be the same as the number displayed at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be

same with each other.

Enable 802.1x Authentication (6): IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless access point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. If there is a RADIUS server in you environment, please enable this function. Check this box and another sub-menu will appear:

RADIUS Server IP address (7): Please input the IP address of RADIUS server here.

RADIUS Server Port (8): Please input the port number of RADIUS server here.

RADIUS Server Password (9): Please input the password here.

TIPS: Examples of WEP key

ASCII (5 characters): pilot phone 23561 2Hyux #@xml

ASCII (13 characters): digitalFAMILY 82Jh26xHy3m&n

Hex (10 characters): 287d2aa732 1152dabc85

Hex (26 characters): 9284bcda8427c9e036f7abcd84

To improve security level, do not use words that can be found in a dictionary or are easy to remember! Wireless clients will automatically remember the WEP key, so you only have to input the WEP key on wireless client once, and it is suggested that to use a complex WEP key to improve security level. Once you have chosen a password, write it down and keep it in a secure place.

After you finish WEP setting, please click ‘Apply’ (10) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

Wi-Fi Protected Access (WPA):

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 **WPA Pre-Shared Key** ▼

WPA Unicast Cipher Suite: WPA(TKIP) WPA(AES) WPA2(Mixed) 2

Pre-shared Key Format: Passphrase ▼ 3

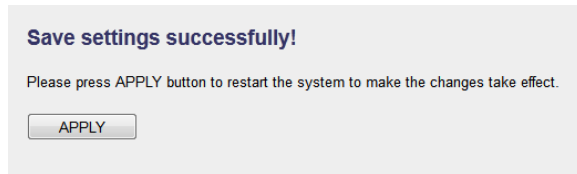
Pre-shared Key: 4

Cancel Apply 5

<i>WPA Unicast Cipher Suite (2):</i>	<i>Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.</i>
<i>Pre-shared Key Format (3):</i>	<i>Select the type of pre-shared key, you can select Passphrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).</i>
<i>Pre-shared Key (4):</i>	<i>Please input the WPA passphrase here. It's not recommended to use a word that can be found in a dictionary due to security reason.</i>

After you finish WPA Pre-shared key setting, please click 'Apply' button

(5) and the following message will be displayed on your web browser:

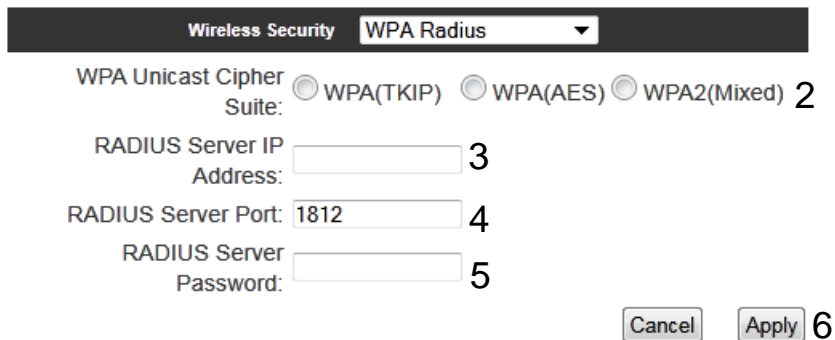


Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

NOTE: Some wireless clients (especially those manufactured before year 2003) only support WEP or WPA (TKIP) cipher. A driver upgrade would be needed for those clients to use WPA and WPA2 encryption.

WPA RADIUS:

If you have a RADIUS server, this access point can work with it and provide safer wireless authentication.



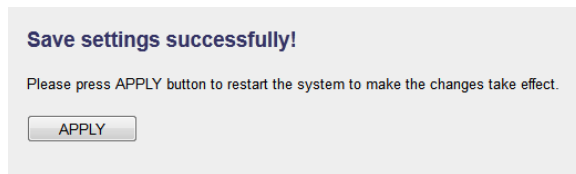
WPA Unicast Cipher Suite: Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.

RADIUS Server IP address (3): Please input the IP address of your Radius authentication server here.

RADIUS Server Port (4): *Please input the port number of your Radius authentication server here.*
Default setting is 1812.

RADIUS Server Password (5): *Please input the password of your Radius authentication server here.*

After you finish with all settings, please click ‘Apply’ (6) button and the following message will be displayed on your web browser:



Please click ‘Go Back’ to go back to previous setup menu, or click ‘Apply’ to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-4 Wireless Access Control

This function will help you prevent unauthorized users from connecting to your wireless access point; only those wireless devices who have a MAC address you assigned can gain access to your wireless access point. Use this function with other security measures described in previous section, to create a safer wireless environment.

You can add up to 20 MAC addresses by using this function. Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'Access Control'.

Access Control

For additional security, the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender features MAC Address Filtering that only allows authorized MAC Addresses to connect through the HWREN25.

MAC Address Filtering Table - up to 20 entries.

No.	MAC Address	Comment	Select
-----	-------------	---------	--------

6 7

1 Enable Access Control

MAC Address	Comment
2 <input type="text"/>	3 <input type="text"/>

5 4

8

All allowed MAC addresses will be displayed in 'MAC Address Filtering Table'.

Enable Wireless *To enforce MAC address filtering, you have to check*

Access Control (1): 'Enable Wireless Access Control'. When this item is unchecked, wireless access point will not enforce MAC address filtering of wireless clients.

MAC Address (2): Input the MAC address of your wireless devices here, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.

Comment (3): You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.

Add (4): Click 'Apply' button to add the MAC address and associated comment to the MAC address filtering table.

Clear (5): Click 'Clear' to remove the value you inputted in MAC address and comment field.

Delete Selected (6): If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete Selected' button. (You can select more than one MAC addresses).

Delete All (7): If you want to delete all MAC addresses listed here, please click 'Delete All' button.

After you finish with all settings, please click 'Apply' (8) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

3-3-3-5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless access point. You don't have to select an encryption mode and input a long encryption passphrase every time when you need to set up a wireless client, you only have to press a button on the wireless client and this wireless access point, and the WPS will automatically configure for you.

This wireless access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless access point to WPS mode too. You can push Reset/WPS button of this wireless access point, or click 'Start PBC' button in the web configuration interface to do this; if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to this wireless access point. The detailed instructions are listed follow:

Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'WPS'.

Wi-Fi Protected Setup (WPS)

This section allows you to change the setting for Wi-Fi Protected Setup (WPS). Wi-Fi Protected Setup can help your wireless client automatically connect to the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender.

1 Enable WPS

WPS Information

WPS Status: Configured

2 PinCode Self: 87440386

SSID: Hawking_HWREN25_AP

Authentication Mode: WEP

Paraphrase Key:

Device Configure

Config Mode: Registrar 3

Configure by Push Button: Start PBC 4

Input client PIN code : Start PIN 5

Enable WPS (1) Check this box to enable WPS function, uncheck it to disable WPS.

WPS Information (2) WPS Status: If the wireless security (encryption) function of this wireless access point is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'Not configured'.

Self PIN code: This is the WPS PIN code of this wireless access point. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.

SSID: The SSID of this wireless access point will be displayed here.

Authentication Mode: The wireless security

authentication mode of this wireless access point will be displayed here. If you do not enable security function of the wireless access point before WPS is activated, the access point will auto set the security to WPA (AES) and generate a set passphrase key for WPS connection.

Passphrase Key: The wireless security key of the access point will be displayed here.

Config Mode (3) There are 'Registrar' and 'Enrollee' modes for the WPS connection. When 'Registrar' is enabled, the wireless clients will follow the access point's wireless settings for WPS connection. When 'Enrollee' mode is enabled, the access point will follow the wireless settings of wireless client for WPS connection.

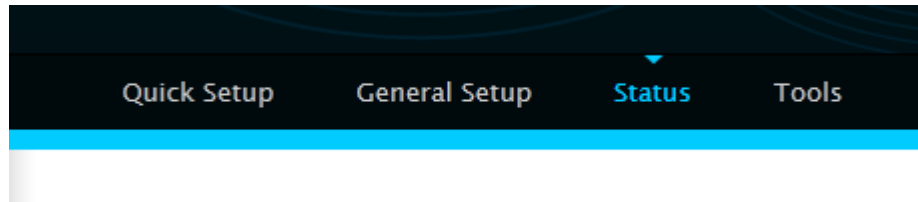
Configure by Push Button (4) Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless access point will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED light on the wireless access point will be steady for 2 minutes when this wireless access point is waiting for incoming WPS request.

Input client PinCode (5) Please input the PIN code of the wireless client you wish to connect, and click 'Start PIN' button. The 'WLAN' LED light on the wireless access point will be steady when this wireless access point is waiting for incoming WPS request.

3-4 Status

The status and information of the HWREN25 will be displayed here.

Click on the status tab on the top of web page.



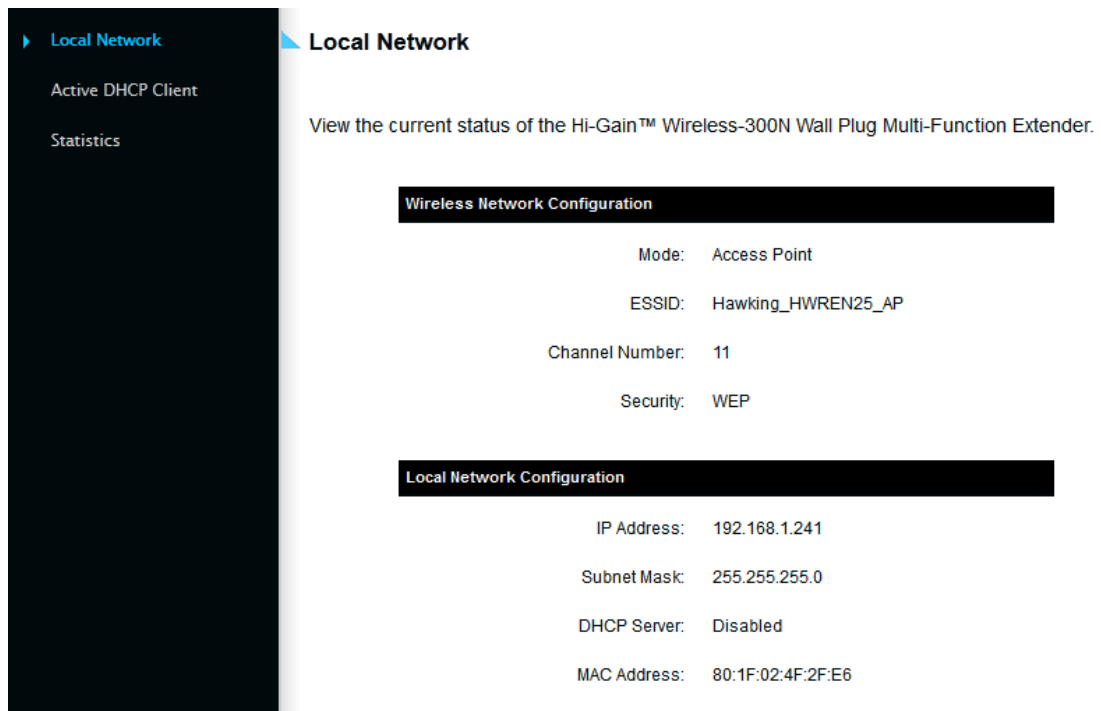
You should see the screen looks like this (the contents will vary depending on your current firmware):

Status

The Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's status information provides the following information: Hardware/Firmware version, Serial Number, and its current operating status.

System	
Model:	HWREN25
Up Time:	0day:1h:27m:58s
Hardware Version:	Rev. A
Boot Code Version:	1.0
Firmware Version:	1.00

On the right hand column under status, click “Local Network”



Wireless Network Configuration: This section describes the current wireless settings of the HWREN25.

Mode: Current mode

ESSID: The broadcast name of the HWREN25

Channel: Current Wireless Channel

Security: The type of security the HWREN25 is using.

Local Network Configuration: This section describes the current network settings of the HWREN25

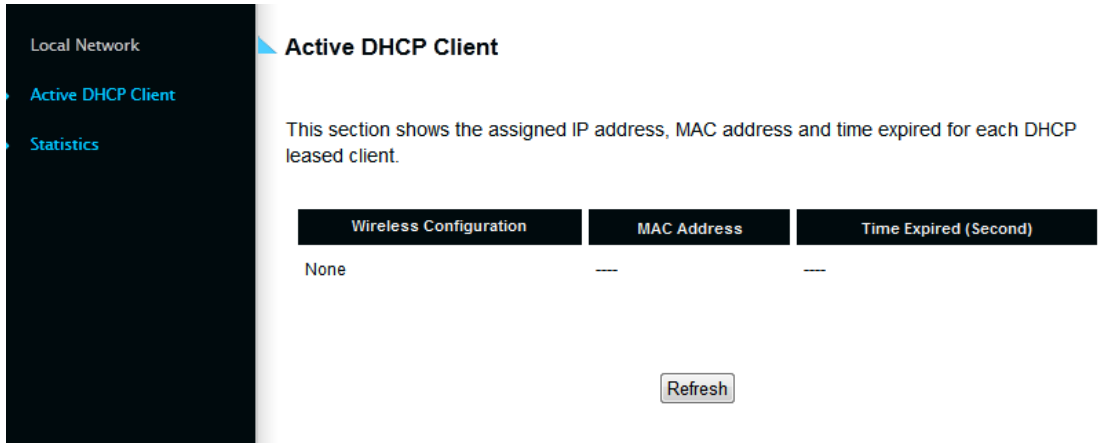
IP Address: Current IP address

Subnet Mask: Current subnet mask

DHCP Server: current status of the DHCP, enabled or disabled

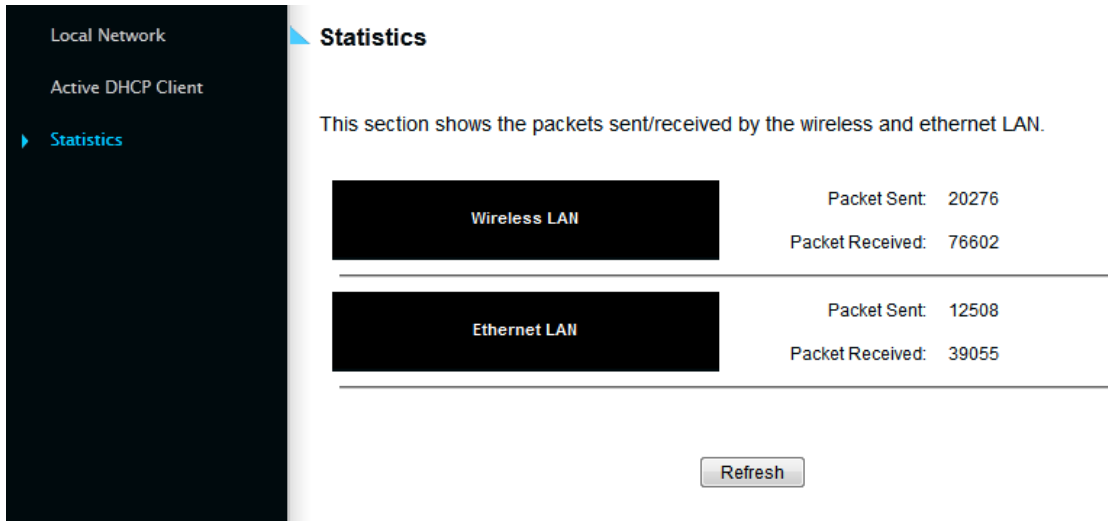
Mac Address: the Mac address of the HWREN25

On the right hand column, click Active DHCP Client



The Active DHCP Client describes clients that are current connected and receiving an IP address from the HWREN25. Only enabled if DHCP Server is enabled in the local network settings.

On the right hand column, click on Statistics



This section describes the amount of data sent/receive on both the wired and wireless connections.

3-5 Configuration Tools

You can back up all configurations of this access point to a file, so you can make several copies of the HWREN25's configuration for security reasons.

To backup or restore the HWREN25's configuration, please follow the instructions:

Please click 'Tools' menu at the top of web management interface, and then click 'Configuration Tools' on the left hand column.

Configuration Tools

Use the "Backup" tool to save the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Extender. Alternatively, you can use the "Restore to Factory Default" tool to force the Extender to perform System Reset and restore the original factory settings.



Backup Settings (1):

Press 'Save...' button, and you'll be prompted to download the configuration as a file, default filename is 'default.bin', you can please save it as another filename for different versions, and keep it in a safe place.

Restore Settings (2):

Press 'Browse...' to pick a previously-saved configuration file from your computer, and then click 'Upload' to transfer the configuration file to

access point. After the configuration is uploaded, the access point's configuration will be replaced by the file you just uploaded.

*Restore to
and*

Click this button to remove all settings you made,

Factory Default (3): restore the configuration of this access point back to factory default settings.

3-6 Firmware Upgrade

The system software used by this access point is known as ‘firmware’, just like any applications on your computer, when you replace the old application with a new one; your computer will be equipped with new function. You can also use this firmware upgrade function to add new functions to your access point, even fix the bugs of this access point.

To upgrade firmware, please follow the instructions:

Please click ‘Tools’ menu at the top of web management interface, and then click ‘Firmware Upgrade’ on the left hand column.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade. See below for the Extender's current firmware. You can go to www.hawkingtech.com for the latest firmware files.

The system will automatically reboot the after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the next step, you have to manually restart the Extender.

Firmware Version: 1.00

Next

Click ‘Next’ button if you wish to upgrade your firmware.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender. Enter the path and name of the upgrade file and then click the Apply button below. You will be prompted to confirm the upgrade.

Click 'Browse' button, and you'll be prompted to provide the filename of the firmware upgrade file. Please download the latest firmware file from the Hawking Technologies website at www.hawkingtech.com, and use it to upgrade your access point.

After a firmware upgrade file is selected, click 'Apply' button, and the access point will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnect your computer from router. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this router to the dealer of purchase to ask for help. Warranty is void if you interrupt the upgrade procedure.

3-7 System Reset

If you think your network performance is bad, or you find the behavior of the access point is strange, you can perform an access point reset. Sometimes it will solve the problem.

Please click 'Tools' menu at the top of the web management interface, and then click 'Reset' on the left-hand column.

Reset and Reboot

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

Reboot:

If resetting the Extender does not work, you may attempt to reset the Extender back to factory default settings. Note that all your current settings will be erased.

Reset to Factory Default Setting:

Please click 'Apply' to reset your access point, and it will be available again after a few minutes, please be patient.

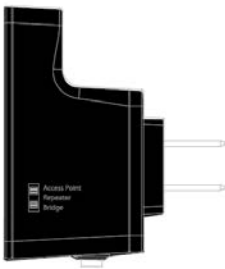
CHAPTER IV: Access Point Mode

You can build a wireless networking environment for home or small office, please switch this device to wireless access point mode and connect it to your wired router. Then your wireless client users can access internet by wirelessly connecting to this AP without wired cable burden.

This chapter will show you how to quickly install this device by using quick setup and show you the each detailed setting on web UI page of AP mode.

4-1 AP mode Quick Installation Guide

Switch mode selector to '**Access Point**'.



Insert this device into power outlet on the wall, and switch wireless HWREN25's power switch to '**ON**'. You should see '**Power**' LED light up in few seconds. If not, please check if the power outlet you're using is working.

You can build wireless connection via 'Hardware WPS button' or 'Software web browser'.

If your wireless router or access point supports 'WPS', we recommend you use the WPS button to establish connection. It is the fast and secure way without computer.

Using WPS button

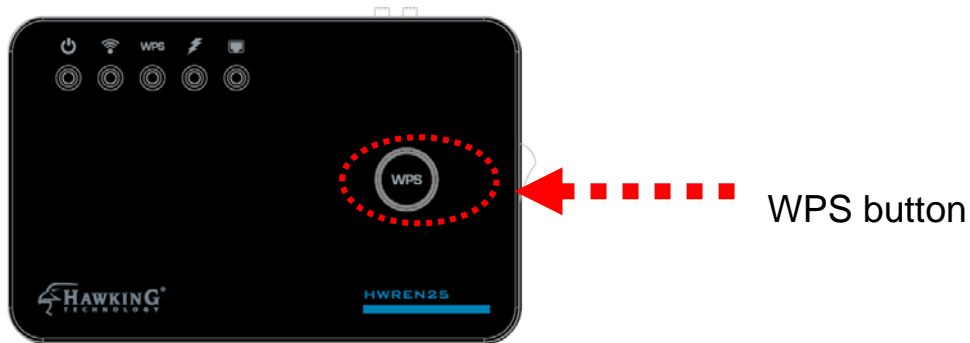
- please go to section 4-1-1

Using Web browser

- please go to section 4-2

4-1-1 Hardware WPS button setup

(1) Press **WPS button twice** on the HWREN25, '**WPS**' LED will start flashing.



(2) Press **WPS button** on the wireless client you wish to connect within 2 minutes.



NOTE: this WPS button position on wireless client is for example. Different device may have different WPS button position.

TIP: If your wireless client card does not have hardware WPS button, you can also use its web configuration menu's WPS function to establish connection. Otherwise you can login this Extender's web UI to do the quick setup (quick setup refers to '4-2 quick setup')

(3) If WPS connection is successfully established, the '**WPS**' LED will light for 5 minutes; if '**WPS**' LED flashes fast, there's something wrong. Please wait 2 minutes until '**WPS**' LED goes off, and try from step (1) again.



When quick installation is successfully done, the '**Wireless** LED will turn on.

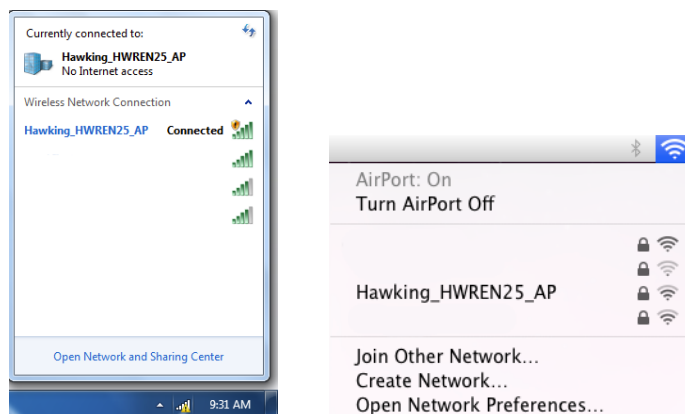
(4) Connect the HWREN25 to the ADSL modem, wired router, or switch/hub in your network through the LAN port by Ethernet cable.

4-2 Access Mode Quick Setup

Before you connect to the HWREN25 and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please refer to '[Chapter 5-1 Configuring TCP/IP on PC](#)' to set your computer to use dynamic IP address.

(1) Use Ethernet cable to connect your computer's Ethernet port and HWREN25's Ethernet port.

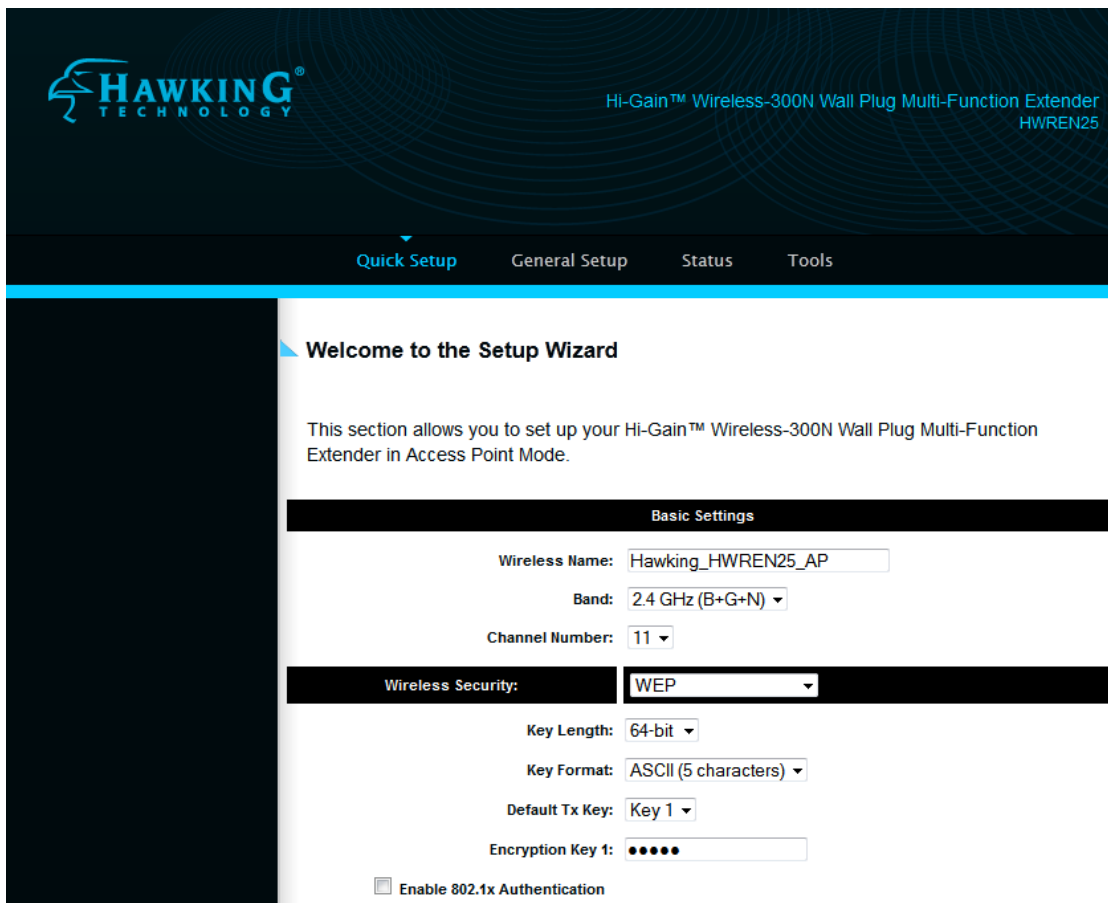
Or use your computer's wireless configuration utility to search for access point named '**Hawking_HWREN25_AP**' and get connected. (The default SSID of this Access Point mode is '**Hawking_HWREN25_AP**')



(2) Open web browser and input '**http:// 192.168.1.241**' in address bar. A window will prompt you to input username and password. Default username is '**admin**' and password is '**1234**'. Click 'OK' button to continue.



(3) Once you are logged in, the HWREN25 setup page will appear.



(4) Under the Quick Setup, Basic Settings, please input a wireless name you wish to use for the HWREN25.

Default Wireless Name is “Hawking_HWREN25_AP”

Basic Settings

Wireless Name:

Band:

Channel Number:

(5) Select the security type that you wish to use.
 The HWREN25 supports these functions: Disable (no security), WEP, WPA pre-shared key, or WPA RADIUS

Wireless Security:

WPA Unicast Cipher Suite: WPA(TKIP) WPA2(AES) WPA2 Mixed

Pre-shared Key Format:

Pre-shared Key:

Note: WEP encryption: Select key length (64 or 128bit), key format (Hex or ASCII characters), Default Tx Key (usually use 'Key 1'), and input key characters (refer to 'Key Format' you selected for number of characters)

WPA pre-shared key: Select one WPA Unicast Cipher Suite (usually use default setting 'WPA(TKIP)'), Pre-shared Key Format: Passphrase (alphanumeric characters) or Hex (64 Hex Characters), and input key characters in 'KEY' field.

WPA RADIUS: Only use this option if you have RADIUS authentication server on your LAN. You have to input RADIUS server's parameters (Server IP, port number, and password).

(6) Advanced IP address settings: This section allows you to set an IP Address and subnet mask to fit your network if needed. Uncheck the box to input. Otherwise, the default IP Address is 192.168.1.241
 Note: It is recommended you give it an IP address in the same range of your network. Otherwise, once it is configured it will not be in the same range and you will not be able to access the setup page to view the general settings.

Advanced Settings

To input your own IP Address settings, Uncheck the box and enter it below.

Note: The default IP address of the HWREN25 is 192.168.1.241

IP Address:

Subnet Mask:

Apply

7) Click apply for your settings to take effect

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

System Restarting! Please wait for a while !

21%



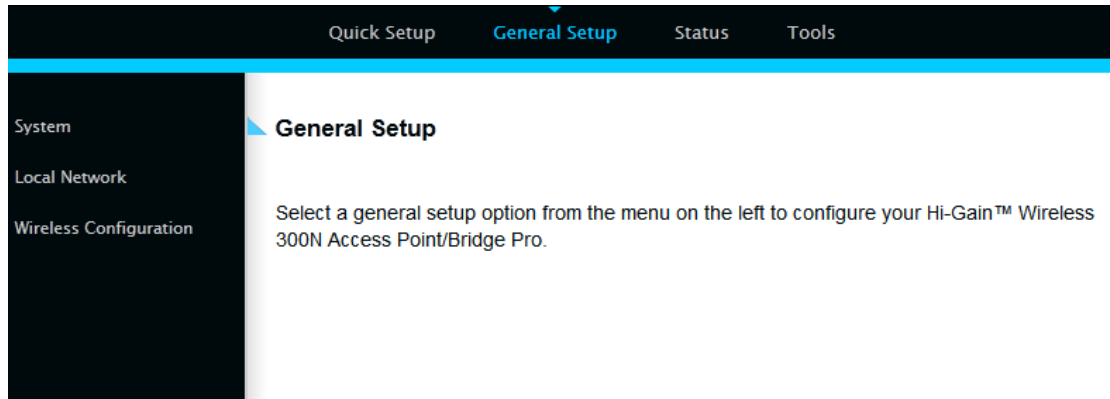
(8) After reboot complete, you can close the web browser to finish this quick setup. Connect the HWREN25 via Ethernet cable to an ADSL modem, wired router, or switch/hub in your network.

ACCESS POINT MODE



4-3 General Setup

In this chapter, you'll know how to change the major settings of the HWREN25. Log onto the device and click on 'General Setup'.



4-3-1 System

Change password

Default password of the HWREN25 is '1234', and it's displayed on the login prompt when accessed from the web browser. There's a security risk if you don't change the default password, since everyone can see it at the prompt. This is very important when you have wireless function enabled.

To change password, please follow the instructions:

Please click 'General Setup' at top of web management interface, select 'System' tab on the left hand column, and then click 'Password Settings', and the following message will be displayed on your web browser:

Password Settings

You can change the password required while logging into the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's web-based management system. By default, the password is 1234.

Passwords can contain 0 to 30 alphanumeric characters and are case sensitive.

Current Password: 1
New Password: 2
Confirm Password: 3

Current Password (1): Please input current password here.

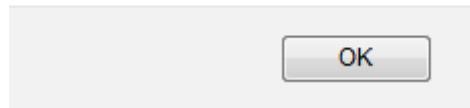
New Password (2): Please input new password here.

Confirm Password (3): Please input new password here again.

If the password you typed in 'New Password' (2) and 'Confirm Password'

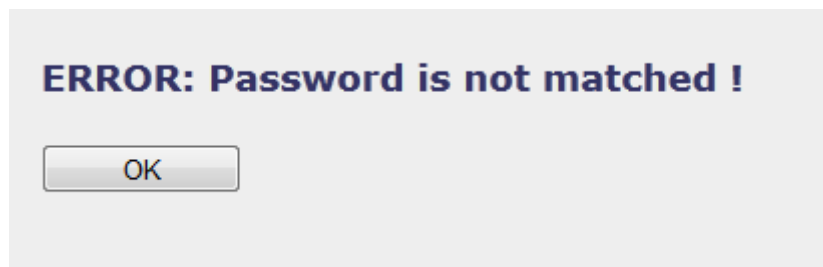
(3) field are not the same, you'll see the following message:

Password is not matched.



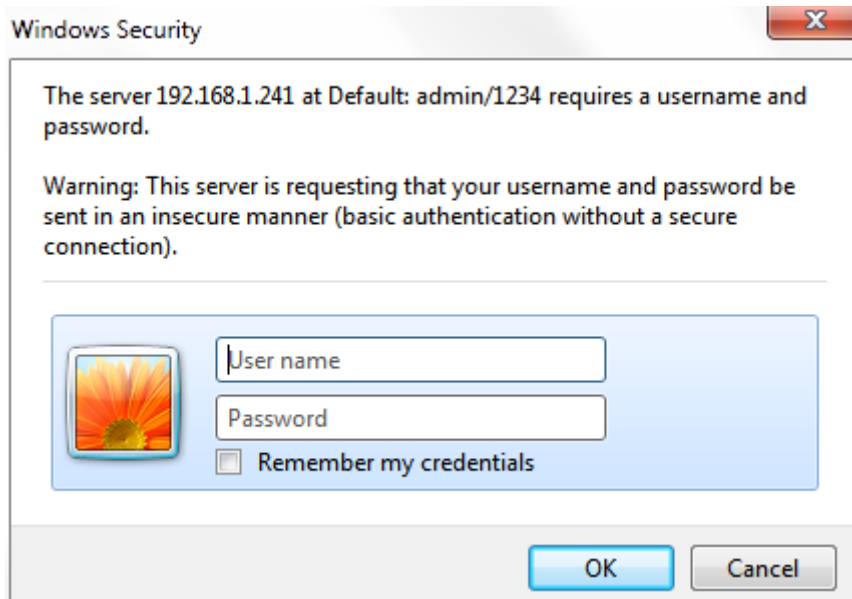
Please retype the new password again when you see above message.

If you see the following message:



It means the content in 'Current Password' field is wrong, please click 'OK' to go back to previous menu, and try to input current password again.

If the current and new passwords are correctly entered, after you click 'Apply', you'll be prompted to input your new password:



Please use new password to enter web management interface again, and you should be able to login with new password.

4-3-2 Local Network

Before all computers using wired Ethernet connection (i.e. those computers connected to this access point's LAN port 1 to 5 by Ethernet cable) can communicate with each other and access Internet, they must have a valid IP address.

There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by access point automatically). It's recommended for most computers to use dynamic IP address, it will save a lot of time on setting IP addresses for every computer, especially when there are a lot of computers in your network; for servers and network devices which will provide services to other computers and users that come from the Internet, a static IP address should be used.

Suggestions on IP Address numbering plan:

If you have no idea on how to define an IP address plan for your network, here are some suggestions.

- 9. A valid IP address has 4 fields: a.b.c.d, for most of home and company users, it's suggested to use 192.168.c.d, where c is an integer between 0 and 254, and d is an integer between 1 and 254. This router is capable to work with up to 253 clients, so you can set 'd' field of IP address of router as 1 or 254 (or any number between 1 and 254), and pick a number between 0 and 254 for field 'c'.**
- 10. In most cases, you should use '255.255.255.0' as subnet mask, which allows up to 253 clients (this also meets router's capability of working with up to 253 clients).**
- 11. For all servers and network devices which will provide services to other people (like Internet service, print service, and file service), they should use static IP address. Give each of them a unique number between 1 and 253, and maintain a list, so everyone can locate those servers easily.**
- 12. For computers which are not dedicated to provide specific service to others, they should use dynamic IP address.**

Please click 'General Setup' at the top of web management interface and click 'Local Network' on the left hand column.

There are two setup groups here: 'LAN IP' and 'DHCP Server'

LAN IP	
IP Address:	<input type="text" value="192.168.1.241"/> 1
Subnet Mask:	<input type="text" value="255.255.255.0"/> 2
Gateway Address:	<input type="text"/> 3
DHCP Server:	<input type="text" value="Disable"/> 4

IP address (1): Please input the IP address of this access point.

Subnet Mask (2): Please input subnet mask for this network.

Gateway Address (3): Please input your gateway address for the network.

DHCP Server (4): If you want to activate DHCP server function of this access point, select 'Enabled', or set it to 'Disabled'.

Recommended Value if you don't know what to fill:

IP Address: 192.168.1.241	DNS Server: (leave it blank)
Subnet Mask: 255.255.255.0	DHCP Server: Disabled
Gateway Address: (leave it blank)	

DHCP Server	
Lease Time:	Forever 1
DHCP Client Start IP:	192.168.1.100 2
DHCP Client End IP:	192.168.1.200 3
DHCP Client Gateway:	0.0.0.0 4
DHCP Client DNS:	0.0.0.0 5
Domain Name:	repeater.com 6

These settings are only available when ‘DHCP Server’ in ‘LAN IP’ section is ‘Enabled’.

Lease Time (1): Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this access point from dropdown menu.

DHCP Client Start IP (2): Please input the start IP address of the IP range.

DHCP Client End IP (3): Please input the end IP address of the IP range.

DHCP Client Gateway (4): Please input your default gateway address

DHCP Client DNS (5): Please input your DNS server address

Domain Name (6): If you wish, you can also optionally input the domain name for your network. This is optional.

Recommended Value if you don't know what to fill:
 Lease Time: Two Weeks (or ‘Forever’, if you have less than 20 computers)
 Default Gateway: (leave it blank)
 Domain Server IP: (leave it blank)
 Start IP: 192.168.1.100
 End IP: 192.168.1.200
 Domain Name: (leave it blank)

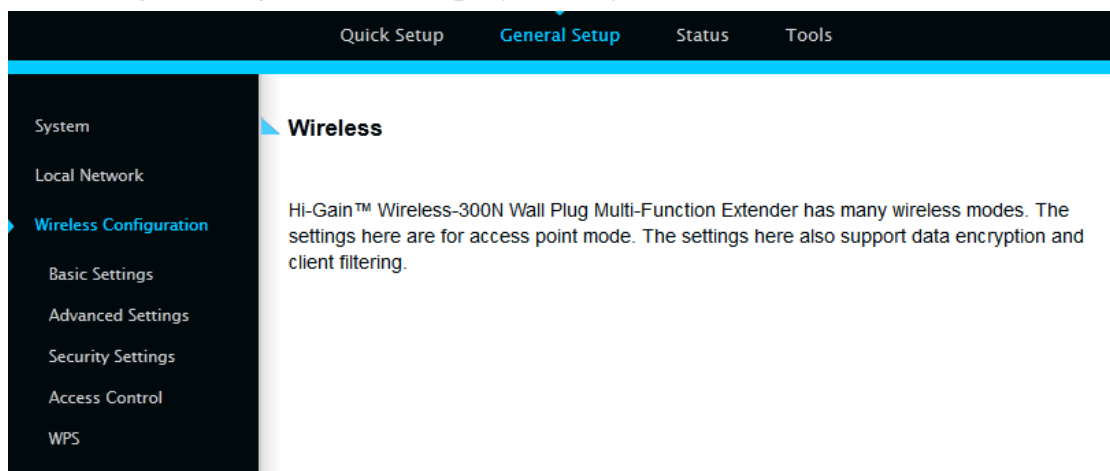
NOTE:

- 1. The number of the last field (mentioned 'd' field) of 'End IP' must be greater than 'Start IP', and cannot be the same as router's IP address.**
- 2. The former three fields of IP address of 'Start IP', 'End IP', and 'IP Address of 'LAN IP' section (mentioned 'a', 'b', and 'c' field) should be the same.**
- 3. These settings will affect wireless clients too.**

4-3-3 Wireless Network

If your computer, PDA, game console, or other network devices is equipped with a wireless network adapter, you can use the wireless function of this access point to let them connect to the Internet and share resources with other computers.

Please click 'General Setup' tab at the top of web management interface, and then click 'Wireless Configuration' tab on the left hand column. The following message will be displayed on your web browser:



4-3-3-1 Basic Wireless Settings

Please click 'General Setup' menu at the top of web management interface, then click 'Wireless Configuration' on the left hand column. Choose 'Basic Settings'. Next to the Mode option, please select your Mode.

Access Point Mode. The HWREN25 will broadcast a Wireless signal for other computers and devices to connect to. Must be plugged into the router or network after setup.

Basic Settings

This page allows you to define the basic settings of the wireless access point.

Mode: AP

Band: 1

SSID: 2

Channel Number: 3

Associated Clients: 4

Band (1): Please select the radio band from one of following options:

2.4 GHz (B)	2.4GHz band, only allows 802.11b wireless network clients to connect to this router (maximum transfer rate 11Mbps).
2.4 GHz (N)	2.4GHz band, only allows 802.11n wireless network clients to connect to this router (maximum transfer rate 300Mbps).
2.4 GHz (B+G)	2.4GHz band, only allows 802.11b and 802.11g wireless network clients to connect to this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).
2.4 GHz (G)	2.4GHz band, only allows 802.11g wireless network clients to connect to this router (maximum transfer rate 54Mbps).
2.4 GHz (B+G+N)	2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network clients to connect to this router (maximum transfer

NOTE: For 802.11b and 802.11g mode, the signals can be transmitted only by antenna 1 (The antenna on the right side of the rear panel).

For 802.11n mode: The router is operating in a 2T2R Spatial Multiplexing MIMO configuration. Two (2) antennas are for signal transmitting and two (2) antennas are for signal receiving.

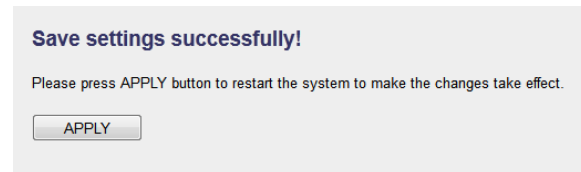
SSID (2): This is the name of wireless access point. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless access point from others when there are other wireless access points in the same area. Default SSID is 'Hawking_HWREN25_AP, It's recommended to change default SSID value to the one which is meaningful to you, such as, 'myhome', 'office_room1', etc.

Channel Number (3): Please select a channel from the dropdown list of 'Channel Number', 1 to 11. 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.

Associated Clients (4): Click 'Show Active Clients' button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are

connecting to the access point.

After you finish these wireless settings, please click ‘Apply’ button, button, and the following message will be displayed on your web browser:



Please click ‘Go Back’ to go back to previous setup menu; to continue on access point setup, or click ‘Apply’ to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

NOTE: If you don't have special reason to limit the type of allowed wireless clients, it's recommended to choose '2.4 GHz (B+G+N)' to maximize wireless client compatibility.

TIP: You can try to change channel number to another one if you think the data transfer rate is too slow. There could be some other wireless routers using the same channel, which will disturb the radio communication between wireless client and the wireless router.

4-3-3-2 Advanced Wireless Settings

This access point provides some advanced control of wireless parameters, if you want to configure these settings, please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Choose "Advanced Settings".

Advanced Settings

Advanced wireless settings for your Wireless Network.

Fragment Threshold: (256 - 2346) 1
RTS Threshold: (0-2347) 2
Beacon Interval: (20-1000 ms) 3
DTIM Period: (0-2347) 4
Data Rate: 5
N Data Rate: 6
Channel Width: Auto 20/40 MHZ 20 MHZ 7
Preamble Type: Short Preamble Long Preamble 8
Broadcast ESSID: Enable Disable 9
CTS Protect: Auto Always None 10
Transmit Power: 11
WMM: Enable Disable 12

Cancel

Apply

Fragment Threshold(1): Set the Fragment threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2346'.

RTS Threshold(2): Set the RTS threshold of wireless radio. Do not modify the default value if you do not understand the function, default value is '2347'.

Beacon Interval(3): Set the beacon interval of wireless radio. Do not modify the default value if you do not understand

the function, default value is '100'.

*DTIM Period(4): Set the DTIM period of wireless radio. **Do not modify the default value if you do not understand the function, default value is '3'.***

*Data Rate(5): Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically. **It is not necessary to change this value unless you know what will happen after modification.***

N Data Rate(6): Same as above, but only for 802.11n clients.

*Channel Width(7): Set channel width of wireless radio. **Do not modify the default value if you do not understand the function, default setting is 'Auto 20/40 MHz'.***

*Preamble Type(8): Set the type of preamble, **do not modify the default value if you do not know what it is, default setting is 'Short Preamble'.***

Broadcast ESSID(9): Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only those people who know the ESSID of your wireless access point can connect to the unit.

CTS Protect(10): Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. It is recommended to set this option to 'Auto' or 'Always'. However, if you set to 'None', your wireless access point should be able to function properly.

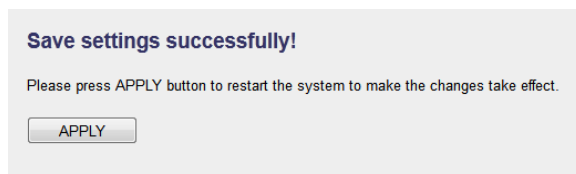
Transmit Power(11): You can set the output power of wireless radio.

*Unless you are using this wireless access point in a large open space, you may not have to set output power to 100%. **This will enhance security (malicious / unauthorized users in distance will not be able to reach your wireless access point).***

WMM(12):

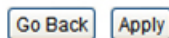
*Wi-Fi MultiMedia (WMM) will enhance the data transfer performance of multimedia contents when they are being transferred over a wireless network. **If you do not understand the function, then it is safe to set this option to 'Enable', however, default value is 'Disable'.***

After you finish these wireless settings, please click 'Apply' button, button, and the following message will be displayed on your web browser:



Settings Saved Successfully!

You may press Go Back button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.



Please click 'Go Back' to go back to previous setup menu; to continue on access point setup, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

4-3-3-3 Security Settings

It is important to set your wireless security settings properly! If you do not configure a wireless security setting, unauthorized users can use your network and/or obtain valuable data without your consent.

To set wireless security settings, please click 'General Setup' tab at the top of web management interface, then click 'Wireless Configuration' on the left hand column. Choose 'Security Settings'.

Please select an encryption method from the 'Encryption' dropdown menu, there are four options:

- Disable**
- WEP**
- WPA**
- WPA Radius**

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 (like MAC address access control - see section 3-4-4, or disable SSID broadcast).



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.

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:

Key Length (2): There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.

Key Format (3): There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key length, and 'Hex' as key format, you'll see the message at the right of 'Key Format' is 'Hex(10 characters)', which means the length of WEP key is 10 characters.

*Default Tx Key (4): **This device only supports one WEP Key 'Key 1'.***

Encryption Key (5) Input WEP key characters here, the number of characters must be the same as the number displayed at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be

same with each other.

Enable 802.1x Authentication (6): IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless access point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. If there is a RADIUS server in you environment, please enable this function. Check this box and another sub-menu will appear:

RADIUS Server IP address (7): Please input the IP address of RADIUS server here.

RADIUS Server Port (8): Please input the port number of RADIUS server here.

RADIUS Server Password (9): Please input the password here.

TIPS: Examples of WEP key

ASCII (5 characters): pilot phone 23561 2Hyux #@xml

ASCII (13 characters): digitalFAMILY 82Jh26xHy3m&n

Hex (10 characters): 287d2aa732 1152dabc85

Hex (26 characters): 9284bcda8427c9e036f7abcd84

To improve security level, do not use words that can be found in a dictionary or are easy to remember! Wireless clients will automatically remember the WEP key, so you only have to input the WEP key on wireless client once, and it is suggested that to use a complex WEP key to improve security level. Once you have chosen a password, write it down and keep it in a secure place.

After you finish WEP setting, please click ‘Apply’ (10) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

Wi-Fi Protected Access (WPA):

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 **WPA Pre-Shared Key** ▼

WPA Unicast Cipher Suite: WPA(TKIP) WPA(AES) WPA2(Mixed) 2

Pre-shared Key Format: Passphrase ▼ 3

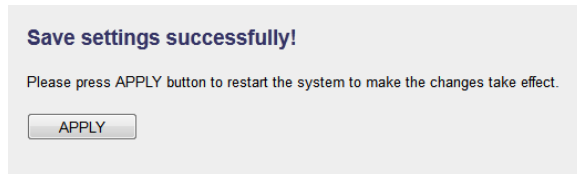
Pre-shared Key: 4

Cancel Apply 5

<i>WPA Unicast Cipher Suite (2):</i>	<i>Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.</i>
<i>Pre-shared Key Format (3):</i>	<i>Select the type of pre-shared key, you can select Passphrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).</i>
<i>Pre-shared Key (4):</i>	<i>Please input the WPA passphrase here. It's not recommended to use a word that can be found in a dictionary due to security reason.</i>

After you finish WPA Pre-shared key setting, please click 'Apply' button

(5) and the following message will be displayed on your web browser:

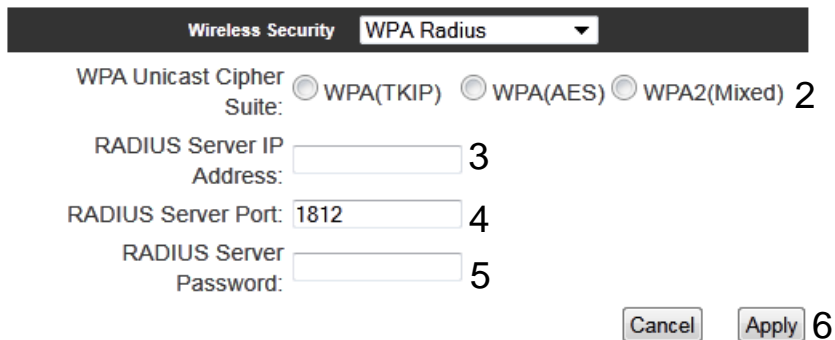


Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

NOTE: Some wireless clients (especially those manufactured before year 2003) only support WEP or WPA (TKIP) cipher. A driver upgrade would be needed for those clients to use WPA and WPA2 encryption.

WPA RADIUS:

If you have a RADIUS server, this access point can work with it and provide safer wireless authentication.



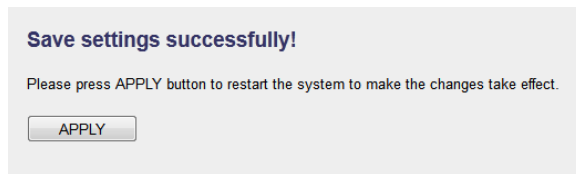
WPA Unicast Cipher Suite: Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.

RADIUS Server IP address (3): Please input the IP address of your Radius authentication server here.

RADIUS Server Port (4): *Please input the port number of your Radius authentication server here.*
Default setting is 1812.

RADIUS Server Password (5): *Please input the password of your Radius authentication server here.*

After you finish with all settings, please click ‘Apply’ (6) button and the following message will be displayed on your web browser:



Please click ‘Go Back’ to go back to previous setup menu, or click ‘Apply’ to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

4-3-3-4 Wireless Access Control

This function will help you prevent unauthorized users from connecting to your wireless access point; only those wireless devices who have a MAC address you assigned can gain access to your wireless access point. Use this function with other security measures described in previous section, to create a safer wireless environment.

You can add up to 20 MAC addresses by using this function. Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'Access Control'.

Access Control

For additional security, the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender features MAC Address Filtering that only allows authorized MAC Addresses to connect through the HWREN25.

MAC Address Filtering Table - up to 20 entries.

No.	MAC Address	Comment	Select
-----	-------------	---------	--------

6 7

1 Enable Access Control

MAC Address	Comment
2 <input type="text"/>	3 <input type="text"/>

5 4

8

All allowed MAC addresses will be displayed in 'MAC Address Filtering Table'.

Enable Wireless *To enforce MAC address filtering, you have to check*

Access Control (1): 'Enable Wireless Access Control'. When this item is unchecked, wireless access point will not enforce MAC address filtering of wireless clients.

MAC Address (2): Input the MAC address of your wireless devices here, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.

Comment (3): You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.

Add (4): Click 'Apply' button to add the MAC address and associated comment to the MAC address filtering table.

Clear (5): Click 'Clear' to remove the value you inputted in MAC address and comment field.

Delete Selected (6): If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete Selected' button. (You can select more than one MAC addresses).

Delete All (7): If you want to delete all MAC addresses listed here, please click 'Delete All' button.

After you finish with all settings, please click 'Apply' (8) button and the following message will be displayed on your web browser:

Save settings successfully!

Please press APPLY button to restart the system to make the changes take effect.

APPLY

Please click 'Go Back' to go back to previous setup menu, or click 'Apply' to reboot the access point so the settings will take effect. Please wait 30-60 seconds for the access point to reboot.

4-3-3-5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless access point. You don't have to select an encryption mode and input a long encryption passphrase every time when you need to set up a wireless client, you only have to press a button on the wireless client and this wireless access point, and the WPS will automatically configure for you.

This wireless access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless access point to WPS mode too. You can push Reset/WPS button of this wireless access point, or click 'Start PBC' button in the web configuration interface to do this; if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to this wireless access point. The detailed instructions are listed follow:

Please click 'General Setup' at the top of web management interface and click 'Wireless Configuration' on the left hand column. Select 'WPS'

Wi-Fi Protected Setup (WPS)

This section allows you to change the setting for Wi-Fi Protected Setup (WPS). Wi-Fi Protected Setup can help your wireless client automatically connect to the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender.

1 Enable WPS

WPS Information

WPS Status: Configured

2 PinCode Self: 87440386

SSID: Hawking_HWREN25_AP

Authentication Mode: WEP

Paraphrase Key:

Device Configure

Config Mode: Registrar 3

Configure by Push Button: Start PBC 4

Input client PIN code : Start PIN 5

Enable WPS (1) Check this box to enable WPS function, uncheck it to disable WPS.

WPS Information (2) WPS Status: If the wireless security (encryption) function of this wireless access point is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'Not configured'.

Self PIN code: This is the WPS PIN code of this wireless access point. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.

SSID: The SSID of this wireless access point will be displayed here.

Authentication Mode: The wireless security

authentication mode of this wireless access point will be displayed here. If you do not enable security function of the wireless access point before WPS is activated, the access point will auto set the security to WPA (AES) and generate a set passphrase key for WPS connection.

Passphrase Key: The wireless security key of the access point will be displayed here.

Config Mode (3) There are 'Registrar' and 'Enrollee' modes for the WPS connection. When 'Registrar' is enabled, the wireless clients will follow the access point's wireless settings for WPS connection. When 'Enrollee' mode is enabled, the access point will follow the wireless settings of wireless client for WPS connection.

Configure by Push Button (4) Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless access point will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED light on the wireless access point will be steady for 2 minutes when this wireless access point is waiting for incoming WPS request.

Input client PinCode (5) Please input the PIN code of the wireless client you wish to connect, and click 'Start PIN' button. The 'WLAN' LED light on the wireless access point will be steady when this wireless access point is waiting for incoming WPS request.

4-3-3-6 Security Tips for Wireless Network

Here are some quick tips to help you improve the security level of your wireless network:

1. Never use simple words for your password, such as “password” or “1234567890”.
2. A complicated (combination of numbers, alphabets, and even symbols) WEP key and WPA passphrase is more secure than simple and short words. Remember that the wireless client is capable of keeping the key or passphrase for you, so you only have to input the complicated key or passphrase once. Once you have chosen a password, write it down and keep it in a secure place.
3. You can hide the ESSID of this access point by setting the ‘Broadcast ESSID’ option to ‘Disable’. Your wireless access point will not be found by other people in proximity if they are using the Access Point scanning function of their wireless client, and this can reduce unauthorized access.
4. Use ‘Access Control’ function, described in section 4-3-3-4, to allow authorized users access to the wireless access point using their specific MAC address.

System

Local Network

Wireless Configuration

General Setup

Select a general setup option from the menu on the left to configure your Hi-Gain™ Wireless 300N Access Point/Bridge Pro.

The following setup page will appear:

The description of every setup item is listed as follow:

Item	Description
Enable WPS	You can enable or disable WPS function. Disabling WPS function is included hardware WPS button function. Default is 'enable WPS'.
WPS Status	Shows the security setting status of WPS. You must setup the security setting of this wireless HWREN25 manually and the WPS status will become 'Configured'. Currently only WPA encryption is supported, if you select other encryption method, WPS status will remain 'Unconfigured'.
Self PinCode	Here displays an 8-digit number for WPS PIN-style configuration. When other WPS-compatible device wish to connect to this wireless HWREN25 and supports Self-PIN type WPS, input this number to the wireless device to establish connection.
SSID	Shows the SSID of this wireless access point.
Authentication Mode	Shows the authentication mode of this wireless access point.
Passphrase Key	Here shows asterisks (*) to indicate wireless security is properly set.
Config Mode	There are 'Registrar' and 'Enrollee' modes for the WPS connection. When 'Registrar' is enabled, the wireless clients will follow the access point's wireless settings for WPS connection. When 'Enrollee' mode is enabled, the access point will follow the wireless settings of wireless router for WPS connection.
Start PBC	Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless HWREN25 will

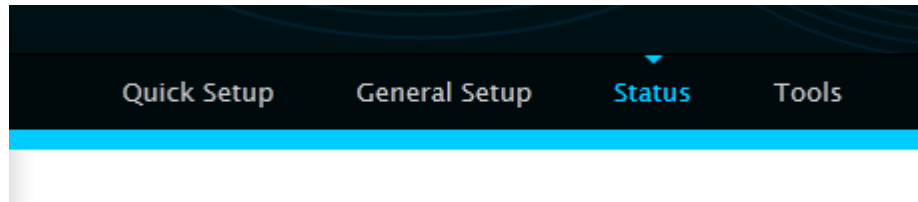
	<p>wait for WPS requests from another wireless device for 2 minutes.</p> <p>The 'WPS' LED on this device will be blinking for 2 minutes when this access point is waiting for incoming WPS request.</p>
Start PIN	<p>Please input the PIN code of the wireless client you wish to connect, and click 'Start PIN' button.</p> <p>The 'WPS' LED on the wireless HWREN25 will be blinking when this wireless HWREN25 is waiting for incoming WPS request.</p>

NOTE: For WPS2.0 compliance specification, WEP and WPA-PSK can't support WPS connection, some of wireless devices may follow this latest WPS2.0 specification, so we recommend you not to use WEP and WPA-PSK to avoid WPS interoperability problem.

4-4 Status

The status and information of the HWREN25 will be displayed here.

Click on the status tab on the top of web page.



You should see the screen looks like this (the contents will vary depending on your current firmware):

Status

The Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's status information provides the following information: Hardware/Firmware version, Serial Number, and its current operating status.

System	
Model:	HWREN25
Up Time:	0day:1h:27m:58s
Hardware Version:	Rev. A
Boot Code Version:	1.0
Firmware Version:	1.00

On the right hand column under status, click “Local Network”

Local Network

Active DHCP Client

Statistics

Local Network

View the current status of the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender.

Wireless Network Configuration

Mode: Access Point

ESSID: Hawking_HWREN25_AP

Channel Number: 11

Security: WEP

Local Network Configuration

IP Address: 192.168.1.241

Subnet Mask: 255.255.255.0

DHCP Server: Disabled

MAC Address: 80:1F:02:4F:2F:E6

Wireless Network Configuration: This section describes the current wireless settings of the HWREN25.

Mode: Current mode

ESSID: The broadcast name of the HWREN25

Channel: Current Wireless Channel

Security: The type of security the HWREN25 is using.

Local Network Configuration: This section describes the current network settings of the HWREN25

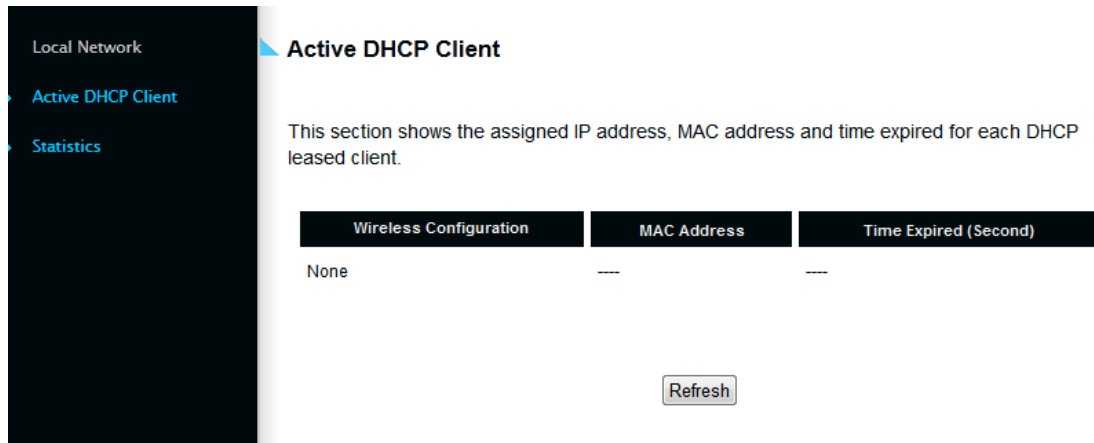
IP Address: Current IP address

Subnet Mask: Current subnet mask

DHCP Server: current status of the DHCP, enabled or disabled

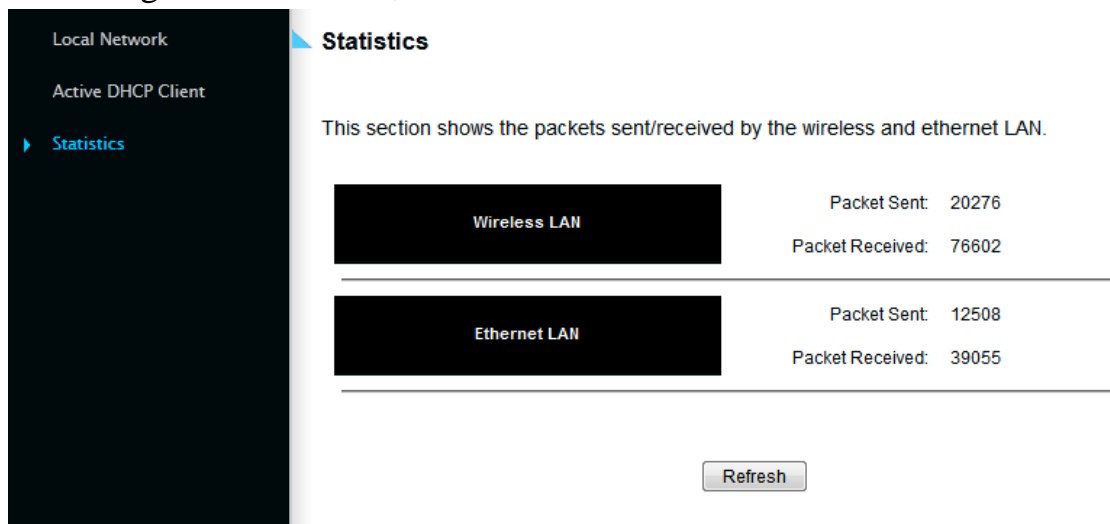
Mac Address: the Mac address of the HWREN25

On the right hand column, click Active DHCP Client



The Active DHCP Client describes clients that are current connected and receiving an IP address from the HWREN25. This is only enabled if DHCP Server is enabled in the local network settings.

On the right hand column, click on Statistics



This section describes the amount of data sent/receive on both the wired and wireless connections.

4-5 Configuration Tools

You can back up all configurations of this access point to a file, so you can make several copies of the HWREN25's configuration for security reasons.

To backup or restore the HWREN25's configuration, please follow the instructions:

Please click 'Tools' menu at the top of web management interface, and then click 'Configuration Tools' on the left hand column.

Configuration Tools

Use the "Backup" tool to save the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Extender. Alternatively, you can use the "Restore to Factory Default" tool to force the Extender to perform System Reset and restore the original factory settings.

The screenshot shows three sections of the Configuration Tools interface. The first section is 'Backup Settings' with a 'Save' button and a circled '1' next to it. The second section is 'Restore Settings' with a text input field, a 'Browse...' button, and an 'Upload' button, with a circled '2' next to the 'Upload' button. The third section is 'Restore to Factory Default' with a 'Reset' button and a circled '3' next to it.

Backup Settings (1):

Press 'Save...' button, and you'll be prompted to download the configuration as a file, default filename is 'default.bin', you can please save it as another filename for different versions, and keep it in a safe place.

Restore Settings (2):

Press 'Browse...' to pick a previously-saved configuration file from your computer, and then

click 'Upload' to transfer the configuration file to access point. After the configuration is uploaded, the access point's configuration will be replaced by the file you just uploaded.

*Restore to
and*

Click this button to remove all settings you made,

Factory Default (3): restore the configuration of this access point back to factory default settings.

4-6 Firmware Upgrade

The system software used by this access point is known as 'firmware', just like any applications on your computer, when you replace the old application with a new one; your computer will be equipped with new function. You can also use this firmware upgrade function to add new functions to your access point, even fix the bugs of this access point.

To upgrade firmware, please follow the instructions:

Please click 'Tools' menu at the top of web management interface, and then click 'Firmware Upgrade' on the left hand column.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade. See below for the Extender's current firmware. You can go to www.hawkingtech.com for the latest firmware files.

The system will automatically reboot the after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the next step, you have to manually restart the Extender.

Firmware Version: 1.00

Next

Click 'Next' button if you wish to upgrade your firmware.

Firmware Upgrade

This tool allows you to upgrade the Hi-Gain™ Wireless-300N Wall Plug Multi-Function Extender. Enter the path and name of the upgrade file and then click the Apply button below. You will be prompted to confirm the upgrade.

Click 'Browse' button, and you'll be prompted to provide the filename of the firmware upgrade file. Please download the latest firmware file from the Hawking Technologies website at www.hawkingtech.com, and use it to upgrade your access point.

After a firmware upgrade file is selected, click 'Apply' button, and the access point will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnect your computer from router. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this router to the dealer of purchase to ask for help. Warranty is void if you interrupt the upgrade procedure.

4-7 System Reset

If you think your network performance is bad, or you find the behavior of the access point is strange, you can perform an access point reset. Sometimes it will solve the problem.

Please click 'Tools' menu at the top of the web management interface, and then click 'Reset' on the left-hand column.

Reset and Reboot

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

Reboot:

If resetting the Extender does not work, you may attempt to reset the Extender back to factory default settings. Note that all your current settings will be erased.

Reset to Factory Default Setting:

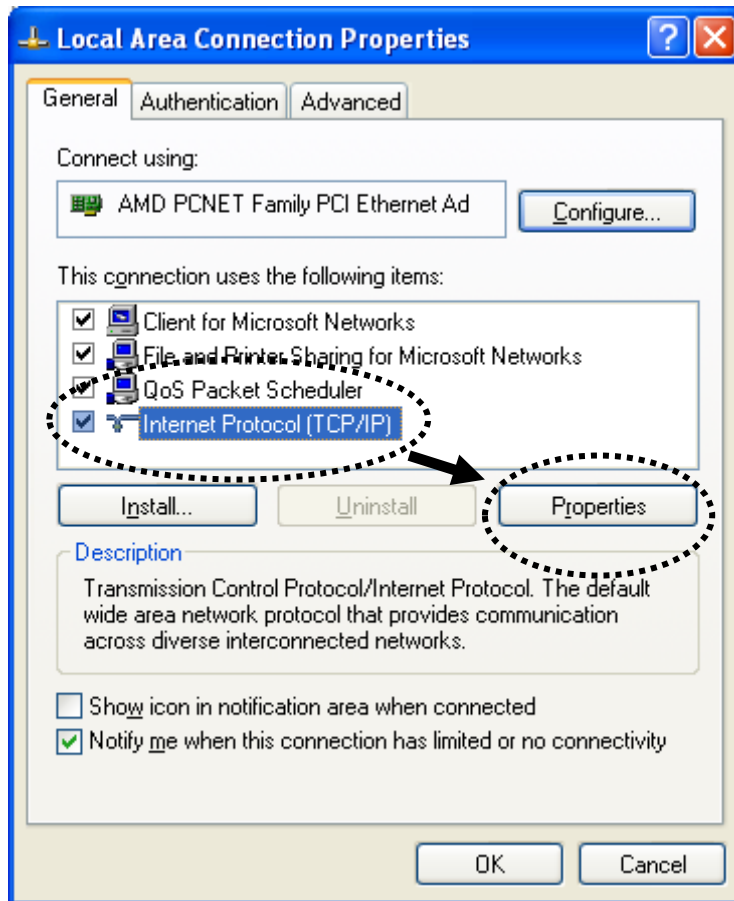
Please click 'Apply' to reset your access point, and it will be available again after a few minutes, please be patient.

Chapter V: Appendix

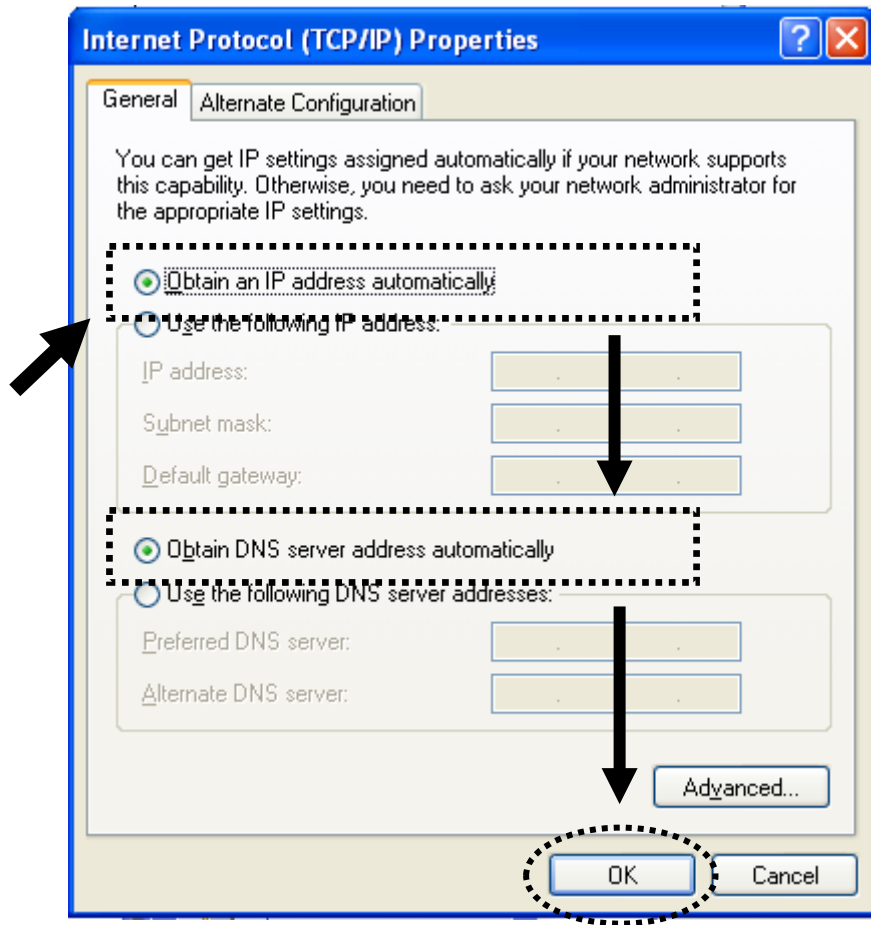
5-1 Configuring TCP/IP on PC

5-1-1 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'

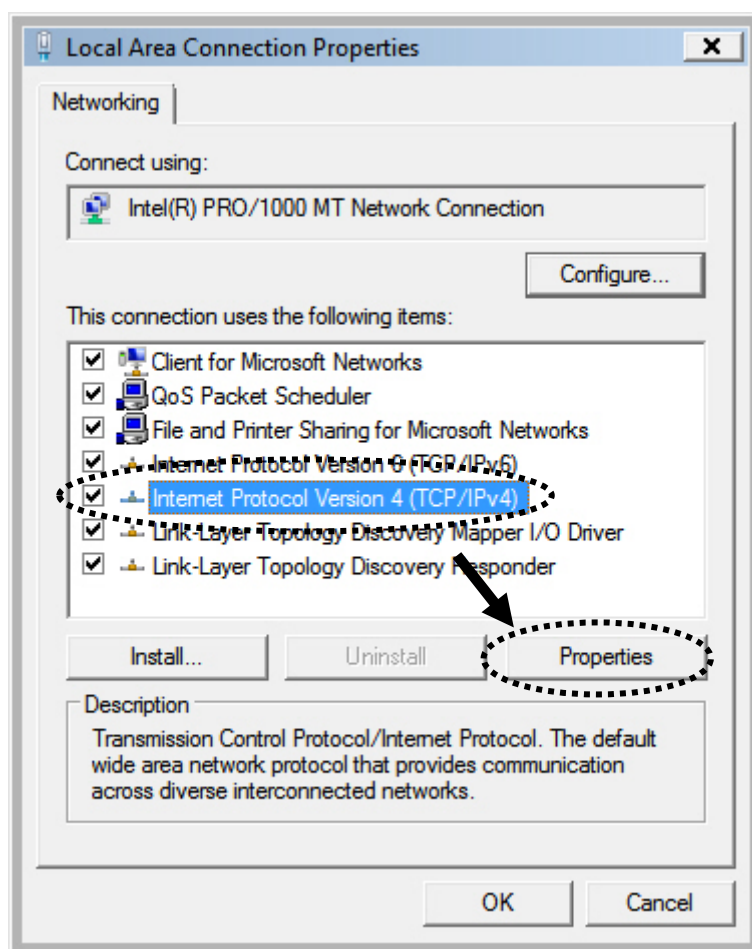


2. Select 'Obtain an IP address automatically' and 'Obtain DNS server address automatically', then click 'OK'.

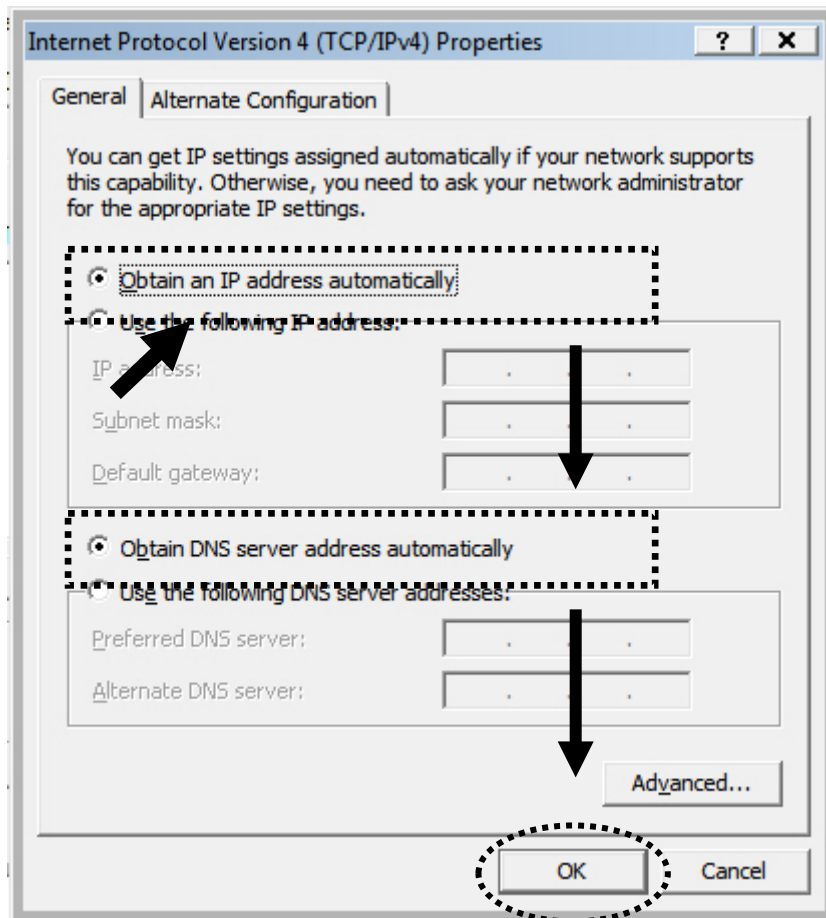


5-1-2 Windows Vista/7 IP address setup

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**, and then click **Manage Network Connections**. 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'

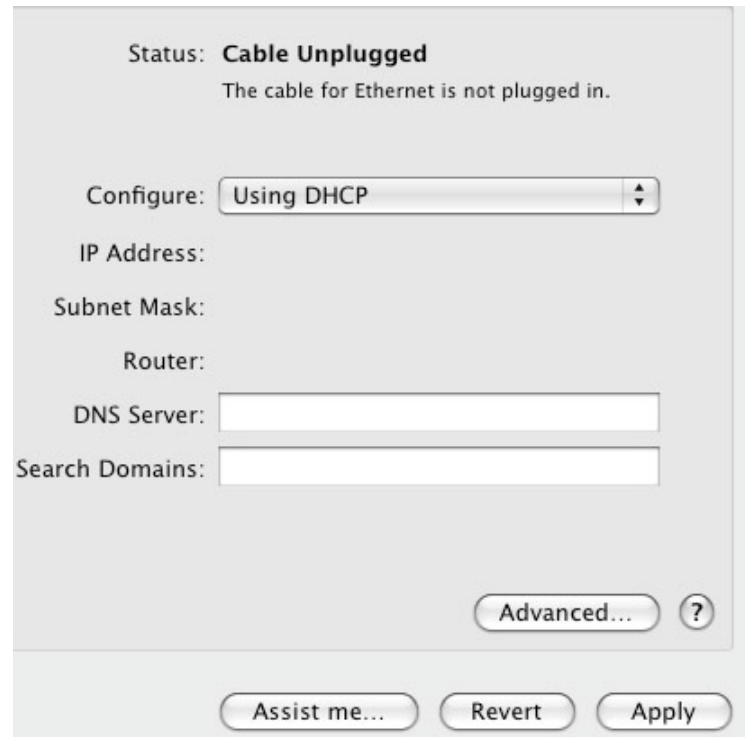


2. Select 'Obtain an IP address automatically' and 'Obtain DNS server address automatically', then click 'OK'.



5-1-3 Mac OS X IP Address Setup

- 1) Go to your system preferences, go to network. Make sure next to “Configure”, you have it set under “Using DHCP”



5-2 Specification

SoC + RF: Realtek RTL8196CS+ RTL8192CE

Flash: 2MB

SDRAM: 16MB

LAN Port: 10/100M UTP Port x 1

Power: 5VDC, 1A Switching Power Module Inside

Dimension: 46.5(W) x 73(H) x 41(D) mm excluding power plug

Transmit Power: 11n: 13dBm±1.5dBm, 11g: 14dBm±1.5dBm, 11b: 17dBm±1.5dBm

Temperature: 32~104°F (0 ~ 40°C)

Humidity: 10-90% (NonCondensing)

Certification: FCC, CE

5-3 Glossary

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

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

2. What is the IEEE 802.11b standard?

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

3. What does IEEE 802.11 feature support?

The product supports the following IEEE 802.11 functions:

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

4. What is Ad-hoc?

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

a branch or SOHO operation.

5. What is Infrastructure?

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

6. What is BSS ID?

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

7. What is WEP?

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

8. What is TKIP?

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

9. What is AES?

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

10. Can Wireless products support printer sharing?

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

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

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

their needs.

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

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

13. What is Spread Spectrum?

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

14. What is WPS?

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