

User's Manual

PLC
500 + Wi-Fi 300

LinkE Hy-Fi

800 Mbps Hy-Fi HD Booster



Table of Content

| | |
|--|-----------|
| 1. IMPORTANT INFORMATION | 1 |
| 1.1. IMPORTANT SAFETY NOTES..... | 1 |
| 2. INTRODUCTION..... | 2 |
| 2.1. PACKAGE CONTENT..... | 2 |
| 2.2. PRODUCT OVERVIEW | 3 |
| 2.3. BUTTONS AND LEDs | 4 |
| 3. HARDWARE INSTALLATION | 5 |
| 3.1. APPLICATION 1 – ESTABLISH HY-FI NETWORK..... | 5 |
| 3.2. APPLICATION 2 – EXPAND WI-FI NETWORK | 6 |
| 4. ENCRYPTED PLC NETWORK..... | 6 |
| 4.1. CREATE AN ENCRYPTED PLC NETWORK GROUP | 6 |
| 4.2. REMOVE DEVICE FROM AN EXISTING NETWORK GROUP | 7 |
| 4.3. CREATE ADDITIONAL ENCRYPTED NETWORK..... | 8 |
| 5. ADVANCED WI-FI SETTINGS VIA WEB BROWSER..... | 9 |
| 5.1. GETTING STARTED | 9 |
| 5.2. LOGIN TO SETTING PAGE | 11 |
| 5.3. HOME | 12 |
| 5.4. HY-FI NETWORKING SETTINGS | 15 |
| 5.5. INTERNET SETTINGS | 20 |
| 5.6. WIRELESS SETTINGS | 21 |
| 5.7. ADMINISTRATION | 30 |
| 5.8. CHANNEL NUMBER | 33 |
| 6. ENHANCE PLC PERFORMANCE | 35 |
| 7. SPECIFICATIONS | 37 |

1.Important Information

Important Safety Notes

The Device is intended for connection to the AC power line. For installation instructions, refer to the Installation section. The following precautions should be taken when using this product.

- Please read all instructions before installing and operating this product.
- Please keep all instructions for later reference.
- Please follow all warnings and instructions marked on the product.
- **For safety reason, when device is being powered on, this product should NOT be installed in any electric socket which makes the surface with venting holes on the product to face downward (facing the floor).**
- **Unplug the Powerline device from the wall outlet before cleaning. Use a dry cloth for cleaning. DO NOT use liquid cleaners or aerosol cleaners.**
- **DO NOT** operate this product near water.
- This product should **never** be placed near or over a radiator, or heat register.
- This product relies on the building's electrical installation for short-circuit (over current) protection.
- **DO NOT** allow anything to rest on the product interconnect plug. **DO NOT** locate this product where people may walk on the cords.
- Because this product sends data over the power line, it is recommended that you plug directly into a power outlet. Do not plug the Device into a UPS or power strip with surge protection. The product has its own power filter for protection against surges.
- **Only** a qualified technician should service this product. Opening or removing covers may result in exposure to dangerous voltage points or other risks.
- Unplug the product from the wall outlet and refer the product to qualified service personnel for the following conditions:
 - When the interconnect cords are damaged or frayed.
 - If liquid has been spilled into the product.
 - If the product has been exposed to rain or water.
 - If the product does not operate normally when the operating instructions are followed.
 - If the product exhibits a distinct change in performance.

2. Introduction


The **Hy-Fi HD Booster** is a wireless device with Powerline Communication (PLC) technology integrated. It takes advantage of wireless and powerline connections for providing more flexible and reliable bandwidth. That means it transmits at powerline or wireless interface, no matter which one your device use, they will automatically connect to the best available interface for the fast performance.

With Hy-Fi technology comes the intelligent “Path Switch”, it can re-assign traffic to the other connection if it experiences connection congested, without the user noticing the change has ever occurred.

This product is suitable for general users to operate in their homes/houses, while advanced configurations through web-browser described in later chapters are suitable for seasoned users to change and manage the **Hy-Fi HD Booster** product settings.

Package Content

Before starting the installation of the device, please make sure the package contains the following items:







| | Single pack | Dual pack |
|--------------------|---|--|
| Device |  <p>Hy-Fi HD Booster</p> | <p>错误!链接无效。 错误!链接无效。</p> <p>Hy-Fi HD Booster Hy-Fi HD Booster</p> |
| Accessories | <ul style="list-style-type: none"> ➤ RJ-45 Cable x 1 ➤ QIG x 1 | <ul style="list-style-type: none"> ➤ RJ-45 Cable x 2 ➤ QIG x 1 |

Product Overview

800Mbps Hy-Fi HD Booster



Buttons and LEDs

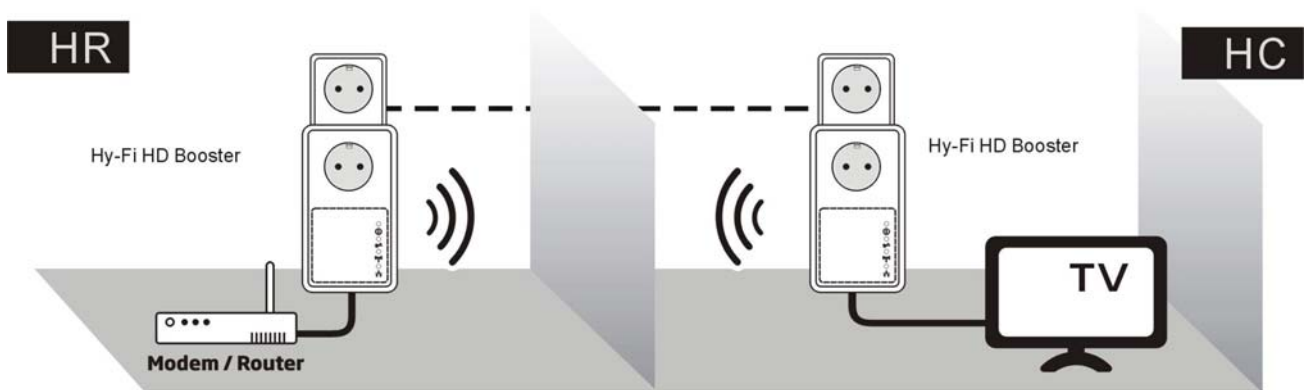
| LED | |
|---|--|
|  | <p><u>ON</u>: Power on and ready. <u>Blinking</u>: PLC group pairing. <u>OFF</u>: Power off.</p> |
|  | <p><u>ON</u>: PLC connection detected.</p> <p><u>Blinking</u>:</p> <ol style="list-style-type: none"> Fast: Powerline data rate > 60Mbps Normal: 60Mbps > Powerline data rate > 10Mbps Slow: 10Mbps > Powerline data rate <p><u>OFF</u>: No PLC connection detected. (They are too far to communicate or it is alone in its logical network).</p> |
|  | <p><u>Steady Green</u>: Wi-Fi network with security protection. <u>Flash Green</u>: Wi-Fi network traffic in transaction with security protection. <u>Steady Red</u>: Wi-Fi network without security protection. <u>Flash Red</u>: Wi-Fi network traffic in transaction without security protection. <u>Blinking Green</u> (0.5 sec ON / 0.5 sec OFF): WPS negotiation. <u>OFF</u> : Wi-Fi disabled.</p> |
|  | <p><u>ON</u>: Ethernet connection detected. <u>Blinking</u>: Network traffic in transaction. <u>OFF</u>: No Ethernet connection detected.</p> |
| Buttons | |
| Power Button | Push to power on/off the device. |
|  | AP Clone by default. The function follows Operation Mode setting in WPS configuration. |
|  | <p><u>Press 10 seconds</u>: Randomly generate a new PLC network group name.</p> <p><u>Press 1 to 3 seconds</u>: Start pairing with the other PLC device. Pairing procedure keeps for 2 minutes or ends automatically when they are paired. It can be stopped manually by pressing the button for 1 to 3 seconds again.</p> |
| Reset Button | <p><u>Press 1 second</u>: Reset to factory default setting. Press the button when the device is powered (not in standby mode)</p> |

3. Hardware Installation

Application 1 – Establish Hy-Fi Network

The Hy-Fi HD Booster takes advantage of wireless and powerline connections for providing stable and reliable home networking.

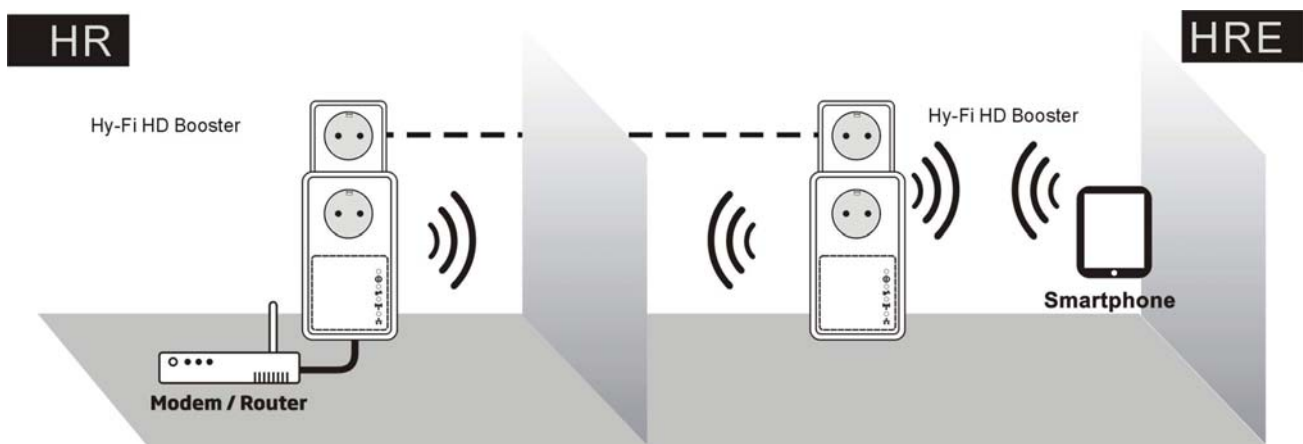
To establish Hy-Fi network, user needs at least 2 Hy-Fi HD Boosters. Once Hy-Fi HD Booster connects with a router, it will automatically turn into Hy-Fi router. Hy-Fi router will automatically detect and configure other Hy-Fi HD Boosters plugged in around the home on the network.



Application 2 – Expand Wi-Fi Network

To extend wireless AP coverage in different room or floor, user can place the Hy-Fi HD Boosters near the mobile devices such as iPad, Tablet, Smartphone and Notebook. The Hy-Fi HD Booster will turn itself into Hy-Fi extender. User can deploy multiple Hy-Fi extenders, using a single network name for all devices to eliminate the need to switch from one to one while moving around the house.

Once your Hy-Fi extenders are connected, any change to the wireless configuration of Hy-Fi router will automatically be applied to connected Hy-Fi extenders.



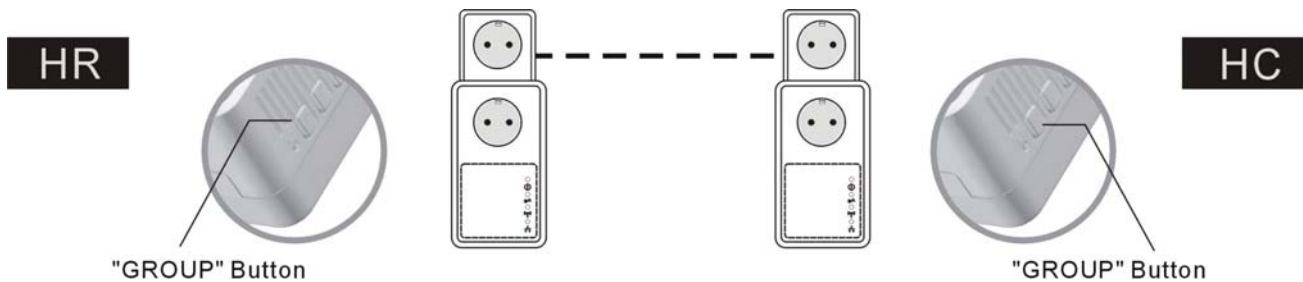
4. Encrypted PLC Network

Create an Encrypted PLC Network Group

The Powerline bridges are compliant with HomePlug AV specification. Every 'HomePlug AV' compliant PLC device that has the same default network name, "**HomePlug AV**", is capable of communicating with other "HomePlug AV" devices. This is the so called "**Public Network**". Two or more powerline devices under the same network can communicate with one another.

If you have a pair of powerline device, either one in the pair can be "device A" or "device B". By pressing the GROUP button more than 10 seconds; it will generate a random network group (different from HomePlug AV). Users can take the following two steps to change the public network group to the private network group to protect their data while transmitting over the powerline. Users also can create more than one private network groups by pressing GROUP button directly without software installation required.

*NOTE: Put the Devices side by side will be more convenient during the setting procedure. After network group is set, the Devices can be deployed anywhere at home.



Step I: Clear Group Attribute

Clear the original network group of device B by pressing its GROUP button more than 10 seconds until all LED lights simultaneously turns off and on once. At this moment, its network group name has been changed to a random name. It means that this device is **(1) ready to be assigned another network name** or **(2) to be used as a seed device so other PLC devices can join to a private network group.**

Step II: Join to Other Network Group

1. Press GROUP button of device A for 2 to 3 seconds (make sure POWER LED starts blinking).
2. Press GROUP button of device B for 2 to 3 seconds (make sure POWER LED starts blinking).

The Device B which has cleared its group attribute will join to the Device A which has not. This step makes device A and B are under the same encrypted network. Additional device C can be added into device A's logical network by taking same steps, thus all of the Device A, B, and C in the same encrypted network group. User can assign as many powerline devices into the logical network group as described in the SPECIFICATION section.

*NOTE: It does not matter which device's button is pressed first, but please press the second device's GROUP button **within two minutes** after pressing first device's GROUP button. After 10 seconds, device will start communicating with device A.

Remove Device from an Existing Network Group

If you would like to remove powerline device from an existing network group, you can generate a new group name (referring to Step I) to stop communication with an existing network group.

Create Additional Encrypted Network

If you want to create additional private network for your powerline devices that co-existence with your existing powerline private network group, please repeat the **Step 1 & 2** to generate new private network group for selected powerline devices.

P.S. Users can press the RESET button to reset the network name back to its factory default.

5. Advanced Wi-Fi Settings via WEB Browser

Getting Started

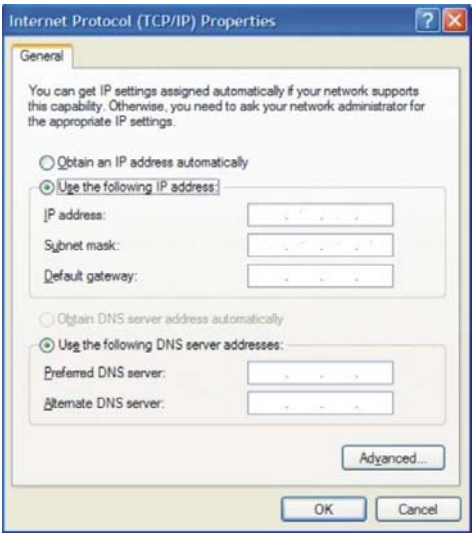
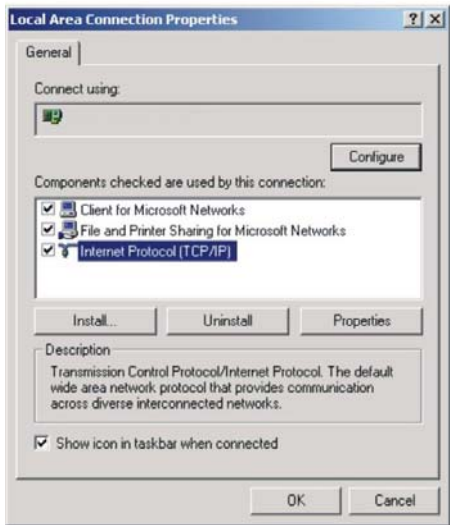
To set up advanced Wi-Fi features such as SSID or password, please connect to Hy-Fi HD Booster via Ethernet or wireless connection, and login to the setting page through web browser.

Default username: root
Default password: root

Before logging in to the setting page, PC or mobile device should be in the same subnet as this device. To do so, please manually change PC or mobile's IP address.

Go to "Network Connections" - "Local Area Connection" "Connection Status" and choose the **Internet Protocol (TCP/IP)** and click on **"Properties"**.

PC



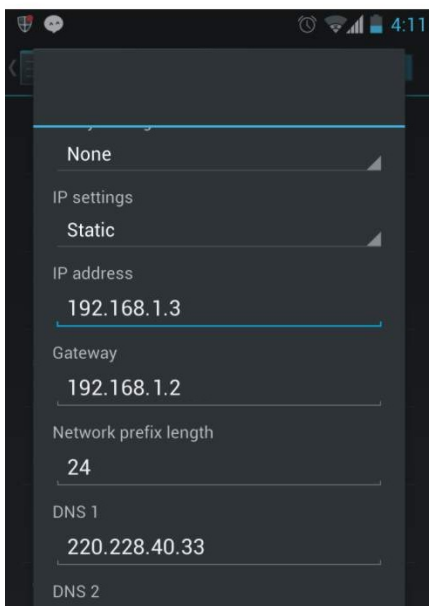
Enter IP address such as **192.168.1.XXX** (XXX can be set from 1-128) and click OK

Go to "Settings" - "Wi-Fi" - "Selected SSID" - "Advanced settings", then click on "Static" to enter IP address such as **192.168.1.XXX**. (XXX can be set from 1-128) and Subnet Mask **255.255.255.0**

Mobile device (iOS)



Mobile device (Android)



Go to "Settings" - "Wi-Fi" - press & hold "Selected SSID" to modify network - then click on "Show advanced options". Click "IP settings" to choose "Static" to enter address such as **192.168.1.XXX**. (XXX can be set from 1-128)

Log in to the Setting Page

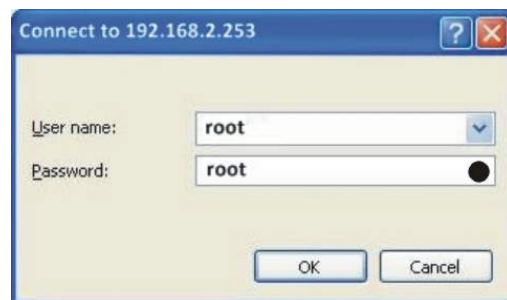
Step 1

Open the Web browser and type in IP address **192.168.1.2** (the IP of this device).



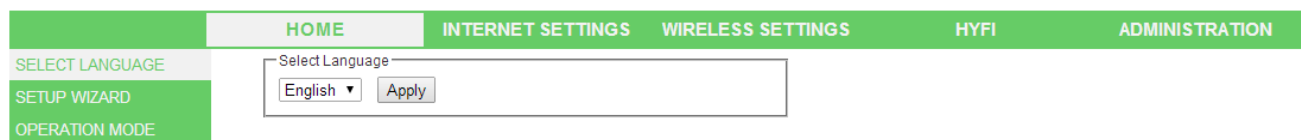
Step 2


When see the login window enter "root" in both user name and password fields. **Note:** you can change user name and password in **Administration** tab.

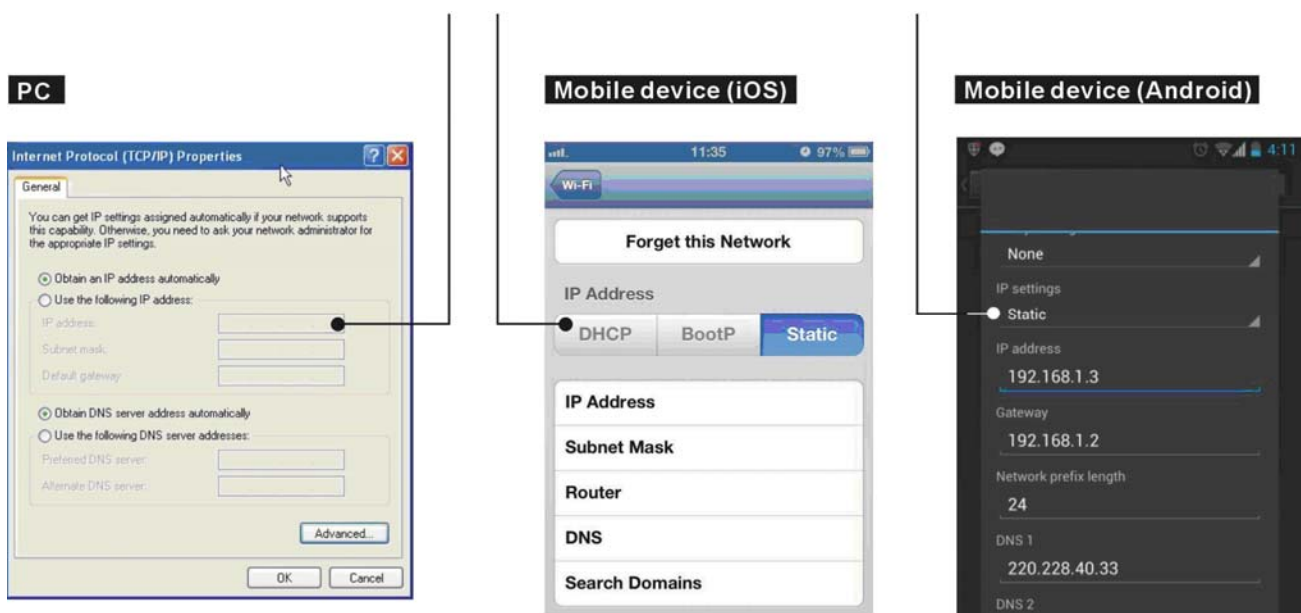


Step 3

The Hy-Fi HD Booster setting page will be displayed after successful login and you can start configuring all necessary settings from here.



 **Note:** After completing all necessary configurations, **DO NOT** forget to change the PC or mobile device's IP address back to your original setting.

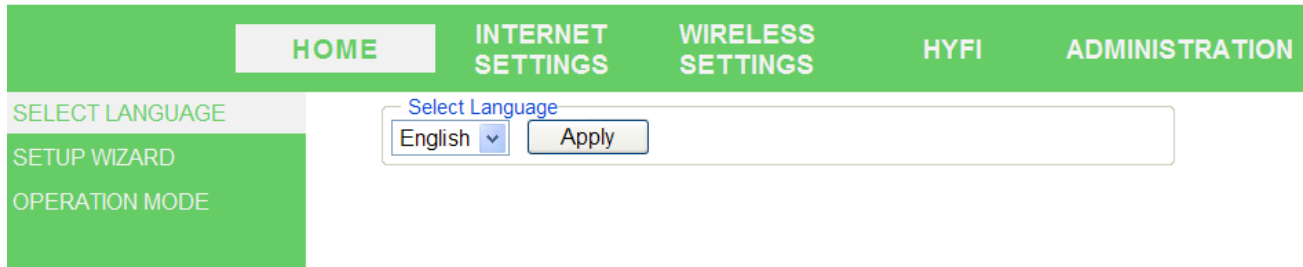


Home

Configuration details for Home section are explained as the following.

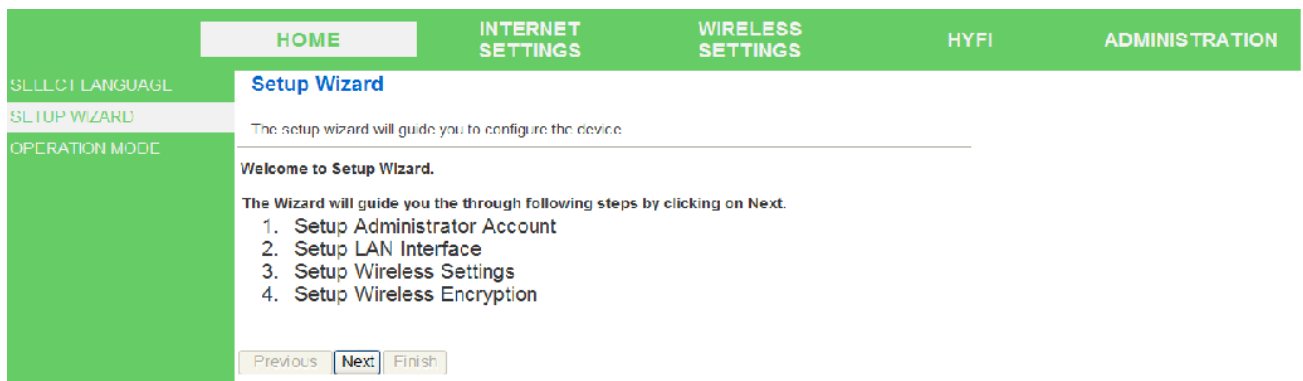
Select Language

Currently English is only the available option in the language setting.



Setup Wizard

The setup Wizard helps you to set up the device with minimum required settings. On the left panel click 'SETUP WIZARD' and then click the "Next" button. The wizard will guide you through required setting.



Step 1 : Set up account and password configuration for device login.

Step 2 : Set up LAN interface.

Step 3 : The page is for basic wireless setting to set network mode, SSID, etc.

Step 4 : Set up wireless security and encryption to prevent from unauthorized access.

Step 5 : Click "**Finish**" button and the device will reboot to apply the changes.

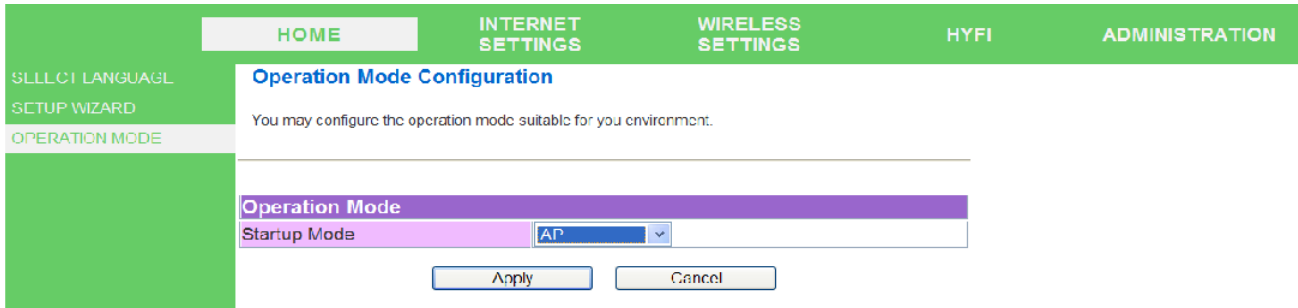


Operation Mode

This device supports five operation modes for the IP network. Click to select one from the following options and then click **Apply** button.

AP Mode

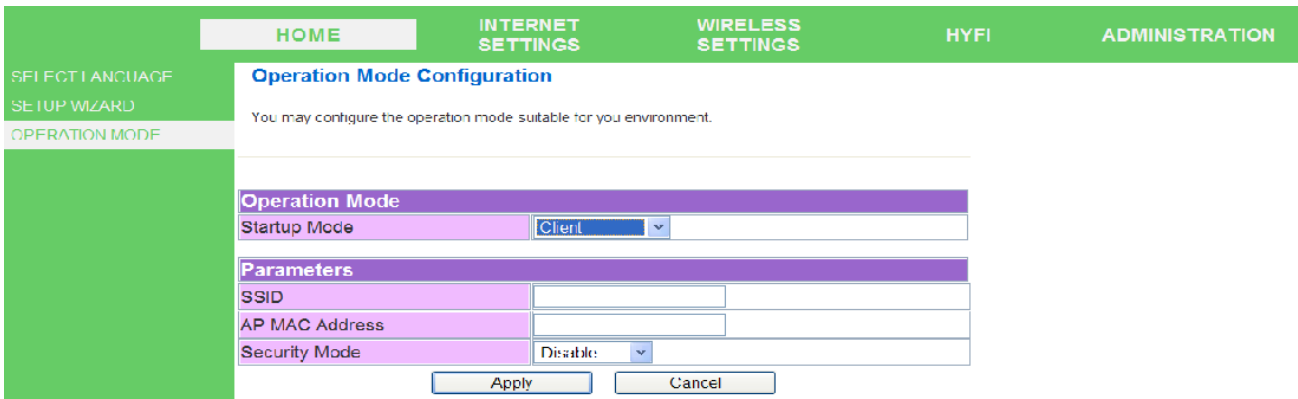
The device acts as Wireless Access Point (**AP**) for wireless clients and provides connections to Ethernet and PLC.



The screenshot shows the 'Operation Mode Configuration' page. The navigation bar includes 'HOME', 'INTERNET SETTINGS', 'WIRELESS SETTINGS', 'HYFI', and 'ADMINISTRATION'. The left sidebar has 'SELECT LANGUAGE', 'SETUP WIZARD', and 'OPERATION MODE'. The main content area has the title 'Operation Mode Configuration' and a subtitle 'You may configure the operation mode suitable for you environment.' Below this is a section titled 'Operation Mode' with a 'Startup Mode' dropdown menu set to 'AP'. At the bottom are 'Apply' and 'Cancel' buttons.

Client Mode

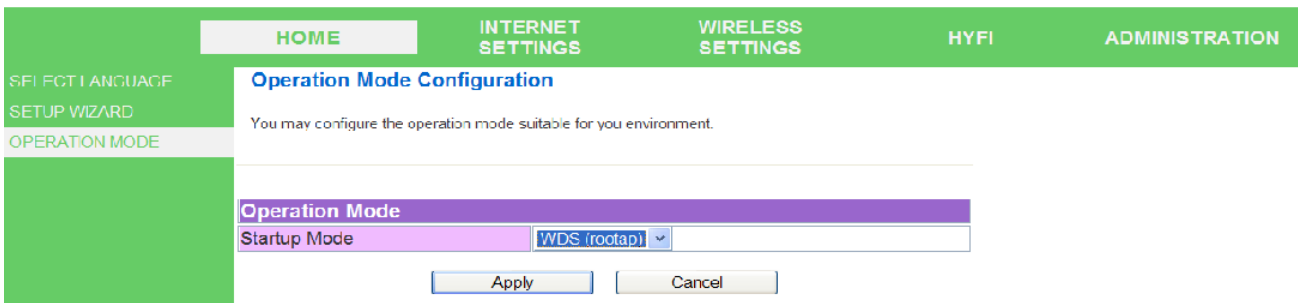
This mode enables the establishment of connection with the other AP using infrastructure /Ad-hoc networking types. With bridge operation mode, you can directly connect the wired Ethernet port to your PC and the device become a wireless adapter



The screenshot shows the 'Operation Mode Configuration' page. The navigation bar includes 'HOME', 'INTERNET SETTINGS', 'WIRELESS SETTINGS', 'HYFI', and 'ADMINISTRATION'. The left sidebar has 'SELECT LANGUAGE', 'SETUP WIZARD', and 'OPERATION MODE'. The main content area has the title 'Operation Mode Configuration' and a subtitle 'You may configure the operation mode suitable for you environment.' Below this is a section titled 'Operation Mode' with a 'Startup Mode' dropdown menu set to 'Client'. Underneath is a 'Parameters' section with input fields for 'SSID', 'AP MAC Address', and a 'Security Mode' dropdown menu set to 'Disable'. At the bottom are 'Apply' and 'Cancel' buttons.

WDS (Root AP)

The wireless radio of device serves for the other AP and provides a connection to a wired LAN (the other AP must use the same chipset as this device does).



The screenshot shows the 'Operation Mode Configuration' page. The navigation bar includes 'HOME', 'INTERNET SETTINGS', 'WIRELESS SETTINGS', 'HYFI', and 'ADMINISTRATION'. The left sidebar has 'SELECT LANGUAGE', 'SETUP WIZARD', and 'OPERATION MODE'. The main content area has the title 'Operation Mode Configuration' and a subtitle 'You may configure the operation mode suitable for you environment.' Below this is a section titled 'Operation Mode' with a 'Startup Mode' dropdown menu set to 'WDS (rootap)'. At the bottom are 'Apply' and 'Cancel' buttons.

WDS + AP Mode

This mode combines WDS mode with AP mode, and it not only allows WDS connections but also that the wireless clients can survey and associate to the device.

The screenshot shows a web interface for configuring the device's operation mode. The top navigation bar includes 'HOME', 'INTERNET SETTINGS', 'WIRELESS SETTINGS', 'HYFI', and 'ADMINISTRATION'. The left sidebar contains 'SELECT LANGUAGE', 'SETUP WIZARD', and 'OPERATION MODE'. The main content area is titled 'Operation Mode Configuration' and includes the following elements:

- A sub-header 'Operation Mode'.
- A 'Startup Mode' dropdown menu set to 'WDS+AP'.
- A 'Parameters' section with three rows:
 - 'Secondary SSID' with an empty text input field.
 - 'AP MAC Address' with an empty text input field.
 - 'Security Mode' with a dropdown menu set to 'Disable'.
- 'Apply' and 'Cancel' buttons at the bottom.

WDS Mode

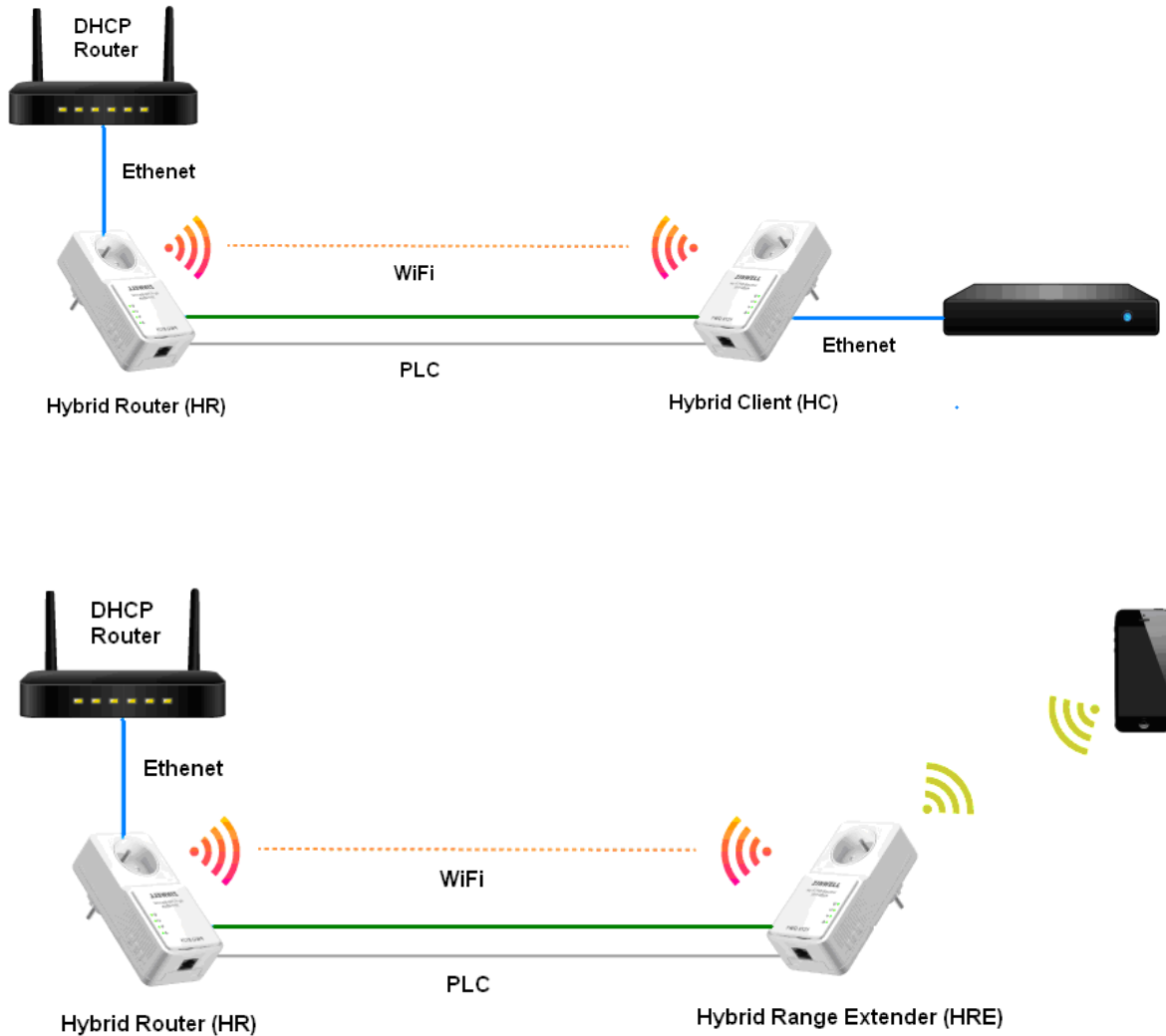
WDS is used to create a network of APs that can be used as a single “virtual” AP. The device forwards the packets to another AP with WDS function. When this mode is selected, all the wireless clients can't survey and connect to the device. The device only allows the WDS connection in WDS mode.

The screenshot shows a web interface for configuring the device's operation mode. The top navigation bar includes 'HOME', 'INTERNET SETTINGS', 'WIRELESS SETTINGS', 'HYFI', and 'ADMINISTRATION'. The left sidebar contains 'SELECT LANGUAGE', 'SETUP WIZARD', and 'OPERATION MODE'. The main content area is titled 'Operation Mode Configuration' and includes the following elements:

- A sub-header 'Operation Mode'.
- A 'Startup Mode' dropdown menu set to 'WDS'.
- A 'Parameters' section with three rows:
 - 'SSID' with an empty text input field.
 - 'AP MAC Address' with an empty text input field.
 - 'Security Mode' with a dropdown menu set to 'Disable'.
- 'Apply' and 'Cancel' buttons at the bottom.

Hy-Fi Networking Settings

Hybrid Network Setting



5.4.1.1. Hybrid Auto Configuration

Hybrid Auto Configuration is enabled by default. Under this mode, devices automatically configure themselves into an Hy-Fi Router(HR), Hy-Fi Client(HC) or Hy-Fi Range Extender (HRE) depending on network topology. Please refer to **Figure 5-1** for this Hybrid Auto Configuration setting. This can be explained in the following steps:

1. Device starts up as a HC by default.
2. If the device is directly connected to a gateway (detected through DHCP messages), it will convert itself to an HR.
3. If not in the above case, then the device (HC) detects whether any devices are connected to its Ethernet interface. If none, the device becomes a HRE. If yes, the

HC status remains.

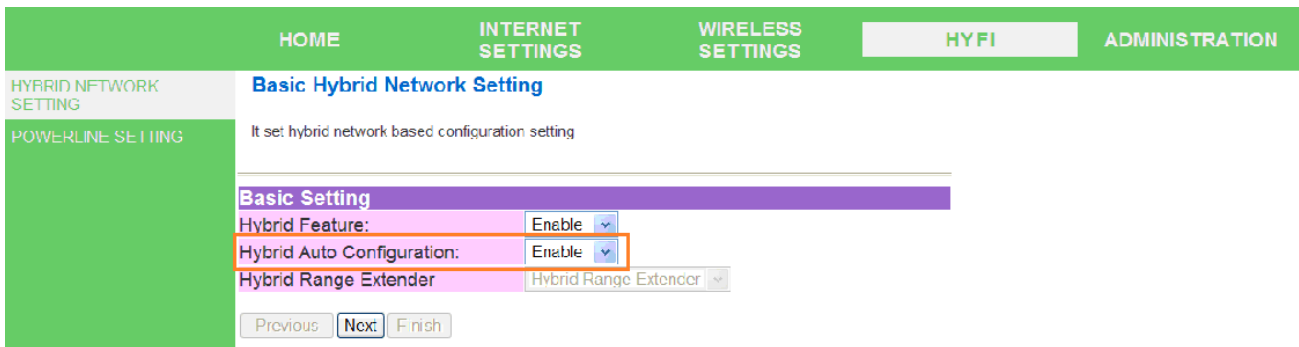


Figure 5-1: Hybrid Auto Configuration - Enable

5.4.1.2 Hybrid Manual Configuration

You can also assign the device as an HR, HC or HRE manually when Hybrid Auto Configuration mode is disabled by setting **Hybrid Auto Configuration** to **Disable**. Please refer to Figure 5-2 for the setting.

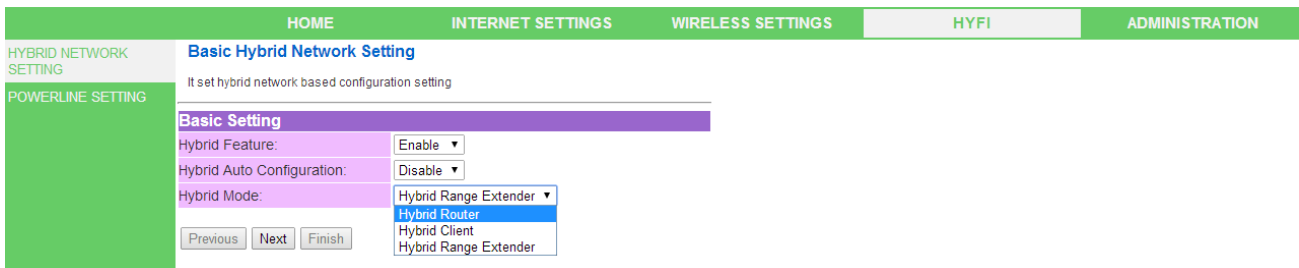


Figure 5-2: Hybrid Auto Configuration - Disable

After disabling Hybrid Auto Configuration, you can manually set the device to the options as shown from the dropdown list shown in Figure 5-2.

1. If the **Hybrid Router** option is selected, after clicking **Next**, you will be asked to do the following configurations as shown from Figure 5-3 to Figure 5-6. Once done, by clicking **Finish**, it will take around 40 seconds to reboot the device.

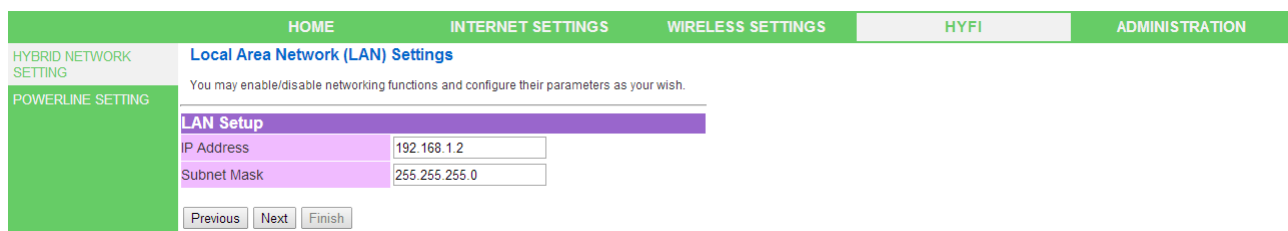


Figure 5-3: LAN Settings

| HOME | INTERNET SETTINGS | WIRELESS SETTINGS | HYFI | ADMINISTRATION |
|---|---|-------------------|------|----------------|
| HYBRID NETWORK SETTING | Basic Wireless Settings | | | |
| POWERLINE SETTING | You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items. | | | |
| Wireless Network | | | | |
| Network Mode | | 11a/n HT40 MINUS | | |
| Network Name(SSID) | | PWQ5121-J00001 | | |
| Frequency (Channel) | | Auto Selection | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> | | | | |

Figure 5-4: Basic Wireless Settings

| HOME | INTERNET SETTINGS | WIRELESS SETTINGS | HYFI | ADMINISTRATION |
|---|--|---|------|----------------|
| HYBRID NETWORK SETTING | Wireless Security/Encryption Settings | | | |
| POWERLINE SETTING | Setup the wireless security and encryption to prevent from unauthorized access and monitoring. | | | |
| Security Policy -- | | | | |
| Security Mode | | Disable Disable OPEN SHARED WEP/AUTO WPA-PSK WPA2-PSK WPA/WPA2 PSK | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> | | | | |

Figure 5-5: Wireless Security/Encryption Settings

| HOME | INTERNET SETTINGS | WIRELESS SETTINGS | HYFI | ADMINISTRATION |
|---|-------------------------------------|-------------------|------|----------------|
| HYBRID NETWORK SETTING | Powerline Settings | | | |
| POWERLINE SETTING | You can set the powerline you want. | | | |
| Powerline Setup | | | | |
| Network Password | | Test123456 | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> | | | | |

Figure 5-6: Powerline Settings

2. If the **Hybrid Client** option is selected, after clicking **Next**, you will be asked to do the following configurations as shown from Figure 5-7 to Figure 5-8. Once done, by clicking **Finish**, it will take around 40 seconds to reboot the device.

| HOME | INTERNET SETTINGS | WIRELESS SETTINGS | HYFI | ADMINISTRATION |
|---|--|-------------------|------|----------------|
| HYBRID NETWORK SETTING | Local Area Network (LAN) Settings | | | |
| POWERLINE SETTING | You may enable/disable networking functions and configure their parameters as your wish. | | | |
| LAN Setup | | | | |
| IP Address | | 192.168.1.2 | | |
| Subnet Mask | | 255.255.255.0 | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> | | | | |

Figure 5-7: LAN Settings

| HOME | INTERNET SETTINGS | WIRELESS SETTINGS | HYFI | ADMINISTRATION |
|---|-------------------------------------|-------------------|------|----------------|
| HYBRID NETWORK SETTING | Powerline Settings | | | |
| POWERLINE SETTING | You can set the powerline you want. | | | |
| Powerline Setup | | | | |
| Network Password | | Test123456 | | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> | | | | |

Figure 5-8: Powerline Settings

3. If the **Hybrid Range Extender** option is selected, after clicking **Next**, you will be asked to do the following configurations as shown from Figure 5-9 to Figure 5-11. Once done, by clicking **Finish**, it will take around 40 seconds to reboot the device.

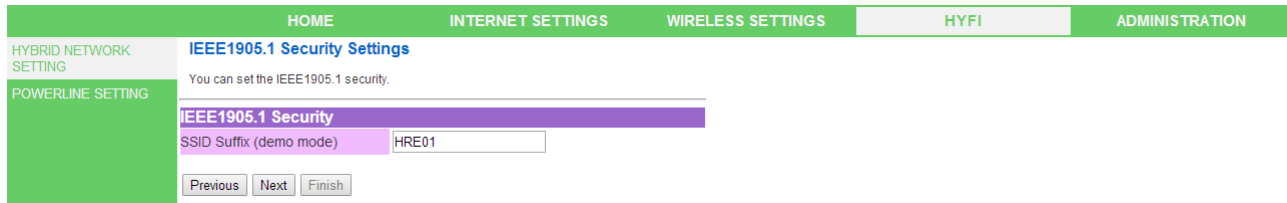


Figure 5-9: IEEE 1905.1 Security Settings

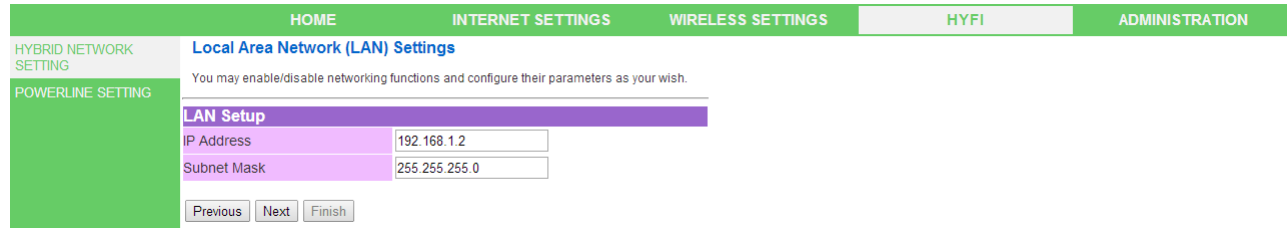


Figure 5-10: LAN Settings

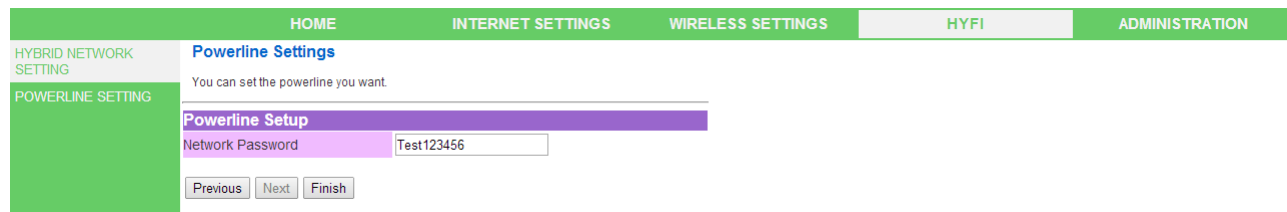


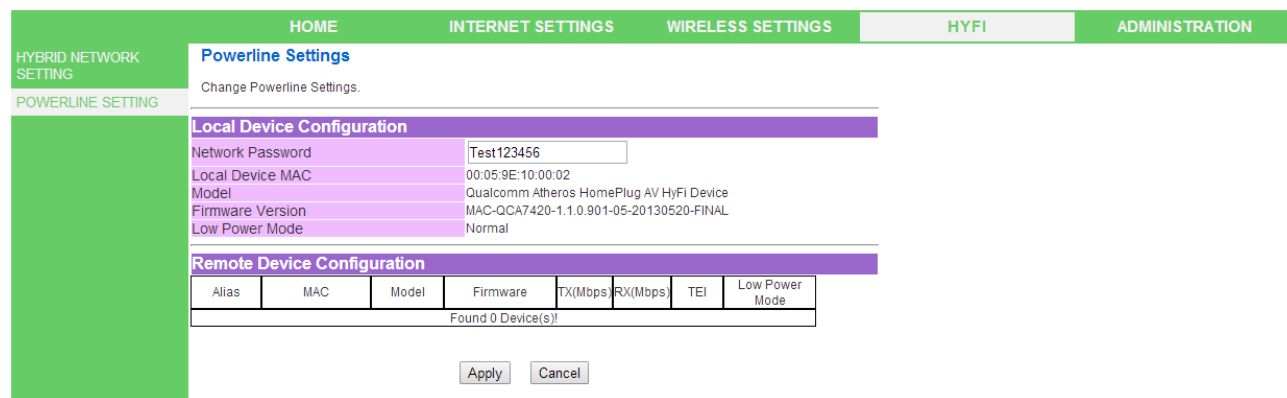
Figure 5-11: Powerline Settings

5.4.2 Powerline Settings

- Network Password: **HomePlugAV**.

You can specify a new value here if you want your powerline network to be separate from other powerline networks.

Save the configuration for it to take effect.



5.4.3 Hy-Fi Auto-Configuration

This feature, enabled by default, automatically conveys IEEE 802.11 parameters from a **registrar** to an **AP enrollee** to set up the initial configuration or renew an existing configuration of an IEEE 802.11 interface. IEEE 1905.1 AP Auto-Configuration is used to automatically configure multiple APs to share a single configuration (i.e. same SSID and Pass Phrase). This enables seamless roaming of wireless clients in the network.

Hy-Fi Auto-Configuration functions as follows:

- Devices start up as a HC.
- HR, HRE, HC all have the same firmware, but the one directly connected to gateway (i.e. home router running a DHCP server) via its Ethernet will turn itself into an HR, acting as the AP Auto-Configuration **registrar**.
- HC detects whether any devices are connected to its Ethernet internet. If none, it becomes an HRE (AP enabled, acting as the **enrollee**). Via web interface, the role of being an HRE can also be manually configured.
- When you plug in Hy-Fi **enrollee AP** devices (e.g. HRE or RE), security configuration (i.e. SSID, pass phrase) from the HR in the same group will be copied and configured automatically on the HRE or RE. This means security configuration on the HR (the registrar) will be propagated to the other APs (the enrollee APs) in the network.
- DHCP client is enabled by default on the device and the device automatically gets an IP address.

5.5 Internet Settings

5.5.1 LAN (Local Area Network Settings)

The screenshot shows a network management interface with a green header bar containing tabs for HOME, INTERNET SETTINGS, WIRELESS SETTINGS, HYFI, and ADMINISTRATION. The 'INTERNET SETTINGS' tab is active. Below the header, there is a 'LAN' section with the title 'Local Area Network (LAN) Settings'. A sub-header reads 'You could enable/disable networking functions and configure parameters.' Below this, a 'LAN Setup' section is highlighted in purple. It contains three input fields: 'IP Address' with the value '192.168.1.2', 'Subnet Mask' with the value '255.255.255.0', and 'MAC Address' with the value '00:0b:9e:11:20:28'. At the bottom of the setup section are two buttons: 'Apply' and 'Cancel'.

| LAN setup | |
|-------------|--|
| Item | Description |
| IP Address | The Internet Protocol (IP) address. |
| Subnet mask | The number used to identify the IP subnet network. |

Hybrid Auto-Configuration will run a DHCP client on all devices – that will override the manual IP settings. In particular, if no DHCP server is found, the default 192.168.1.2 IP address will be used.

5.6 Wireless Settings

5.6.1 Basic (Basic Wireless Settings)

| Wireless Network | |
|---------------------|---|
| Item | Description |
| Radio On/Off | Click to enable/disable wireless function. |
| Network Mode | Selectable Dual Band. The available options are 11a,11b,11g,11a/n HT20,11a/n HT40,11a/n HT40,11g/n HT20,11g/n HT40,11g/n HT40. |
| Network Name (SSID) | The SSID is a unique identifier that wireless networking devices use in order to establish and maintain wireless connectivity. SSID can contain up to 32 alphanumeric characters. |
| MAC 1 | MAC address |
| Frequency (Channel) | Click the drop down box to select the radio channel. Select the unused channel to prevent the radio overlapping. |

| HT Physical Mode | |
|----------------------|---|
| Item | Description |
| Operating Mode | Default: Mixed (Mixed, Green Field). Mixed mode: In this mode the device transmits the packets with preamble compatible legacy (802.11g), so they can be decoded by legacy devices. The Device receives and decodes both Mixed Mode packets and legacy packets. Green Field mode: the Device transmits HT packets without legacy compatible part. But the Device receives and decodes both Green Field and legacy packets. |
| Short Guard Interval | The 11n device inserts the Guard Interval into the signal. You |

| | |
|---------------------------|---|
| | can choose the interval between “Long” and “Short”. This option affects the Phy data rate of radio. Please refer to the table below. |
| MCS | It is Modulation Coding Scheme. The available options are “Auto, 0, 1-7”. It changes the modulation of this device and effect the maximum Phy data rate. We recommend “Auto” setting. For the details, please refer to the table below. |
| Aggregation MSDU (A-MSDU) | The multiple HT packets can be transmitted with single ACK reply packet. Enable it to apply this function and reduce the network congestion. |
| Auto Block ACK | It is another aggregation technique which prevents sending ACK in the communication to increase the throughput. If this option is enabled, the Device will activate this function when transmitting massive data. |

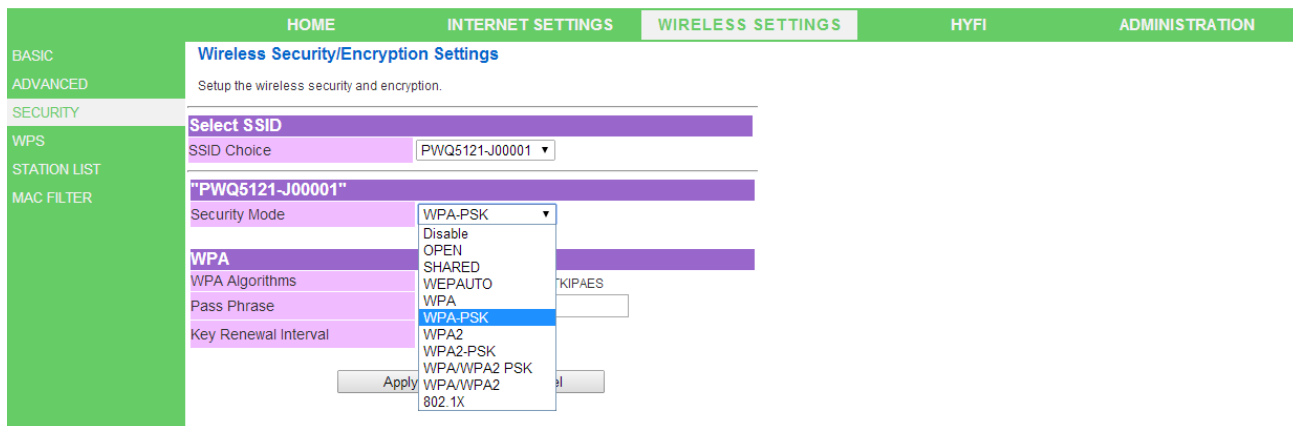
5.6.2 Advanced (Advance Wireless Settings)

| Advanced Wireless | |
|-------------------------|---|
| Item | Description |
| BG Protection Mode | You can select the other options including On and Off. The B/G protection technology is CTS-To-Self. It will try to reserve the throughput for 11g clients from 11b clients connecting to the Device as AP mode. |
| Beacon Interval | Beacons are the packets sending by Access point to synchronize the wireless network. The beacon interval is the time interval between beacons sending by this unit in AP or AP+WDS mode. The default and recommended beacon interval is 100 milliseconds. |
| Data Beacon Rate (DTIM) | This is the Delivery Traffic Indication Map. It is used to alert the clients that multicast and broadcast packets buffered at the AP will be transmitted immediately after the transmission of this beacon frame. |

| | |
|----------------|---|
| | You can change the value from 1 to 255. The AP will check the buffered data according to this value. For example, selecting “1” means to check the buffered data at every beacon. |
| Short Preamble | Default: Disable. It is a performance parameter for 802.11 b/g mode and not supported by some of very early stage of 802.11b station cards. If there is no such kind of stations associated to this AP, you can enable this function. |
| Tx Burst | The Device will try to send a serial of packages with single ACK reply from the clients. Enable this function to apply it. |

| Wi-Fi Multimedia | |
|------------------|---|
| Item | Description |
| WMM Capable | Choose “Enable” to enable WMM function. |
| APSD Capable | Turn on this feature so this device can detect whether the connecting wireless client device has turned on power saving feature. If yes, this device will send packets with power saving tag accordingly. |
| WMM Parameter | Click the button to edit the WMM parameter. |

5.6.3 Security (Wireless Security/Encryption Settings)



Security Mode: Choose one from the options.

| Wireless Security/Encryption Settings | |
|---------------------------------------|--|
| Item | Description |
| Security Mode | Disable, OPEN, SHARED, WEP/AUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 PSK, WPA/WPA2, 802.1X. |

Encryption Type: The options vary depending on the authentication mode. The corresponding options are listed below.

| Authentication | Encryption type | Key option |
|----------------|-----------------|------------|
| | | |

| | | |
|-------------------------------|---------------------|--|
| OPEN, SHARED, WEPAUTO | WEP | Default Key ID, WEP Keys 1/2/3/4 |
| WPA/WPA2 PSK (Pre-Shared Key) | TKIP, AES, TKIP/AES | Pass Phrase, Key Renewal Interval |
| WPA/WPA2 Enterprise | TKIP, AES, TKIP/AES | Radius Server: IP Address, Port, Shared Secret, Session Timeout |

WEP Encryption Setting

Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. The WEP setting must be the same as each client in your wireless network.

The screenshot shows the 'Wireless Security/Encryption Settings' page. It includes a sidebar with navigation options like HOME, INTERNET SETTINGS, WIRELESS SETTINGS, HYFI, and ADMINISTRATION. The main content area is titled 'Wireless Security/Encryption Settings' and contains the following fields:

- Select SSID:** SSID Choice dropdown set to 'PWQ5121-J00001'.
- Security Mode:** Dropdown set to 'WEPAUTO'.
- Wire Equivalence Protection (WEP):**
 - Default Key:** Key 1 dropdown.
 - WEP Keys:** Four text input fields for WEP Key 1 through WEP Key 4, each with a format dropdown (ASCII/Hex).

Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

- **Authentication Type:** OPEN, SHARED and WEPAUTO. When selecting “OPEN” or “SHARED”, all of the clients must select the same authentication to associate with this AP. If selecting “WEPAUTO”, the clients don’t have to use the same “OPEN” or “SHARED” authentication. They can choose either one for authentication.
- **Default Key:** Select the Key ID as the default Key.
- **WEP Key 1/2/3/4:** Select “ASCII” or “Hex” and then enter the key in the text field. Key options are listed as the following. The system will check the entered format and if not correct, a pop-up error message will be displayed.
 - Character input, 5 character (WEP64)
Enter 5 (case sensitive) alphanumeric characters.
 - Character input, 13 characters (WEP128)
Enter 13 (case sensitive) alphanumeric characters.
 - Hexadecimal number input, 10 digit (WEP64)
Enter a 10 digit HEX as an encryption key. You may use characters 0-9 and a-f.
 - Hexadecimal number input, 26 digit (WEP128)
Enter a 26 digit HEX as an encryption key. You may use characters 0-9 and a-f.

WPA Authentication

This device supports six WPA modes including WPA-PSK (pre-shared key), WPA, WPA2-PSK, WPA2 and additional WPA/WPA2 PSK and WPA/WPA2 mixed mode. For individual and residential user, it is recommended to select WPA-PSK or WPA2-PSK to encrypt the link without additional RADIUS server. This mode requires only an access point and client station that supports WPA-PSK. For WPA/WPA2, authentication is achieved via WPA RADIUS Server.

- **WPA/WPA2 with pre-shared key:**

- **Pass Phrase:**

A pre-shared key must be entered. If the same key is not entered into each wireless client in your wireless network, the communication will not be established. You can specify Pass Phrase with the key value containing 8-63 ACSII characters.

- **Key Renewal Interval:**

The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds and you can adjust the time interval.

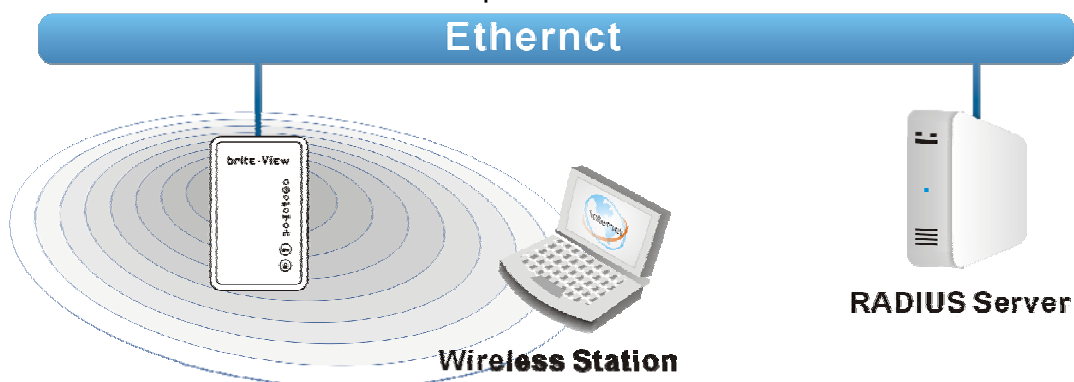
- **WPA/WPA2:**

When selecting WPA/WPA2, you have to add user accounts and the target device to the RADIUS Server. In the Device, you need to specify the RADIUS server address, server Port and server key of the target RADIUS server.

- WPA Algorithms: **TKIP, AES, TKIP/AES**. This is to set the encryption method. When selecting TKIP/AES, the client can use whether TKIP or AES for the authentication.

- **Radius Server Setting:**

- IP Address: Input the IP Address of the Radius server.
- Port: Input the port of the Radius server.
- Shared Secret: Input the Authentication Key.
- Session Timeout: Input the maximum idle time for this connection.

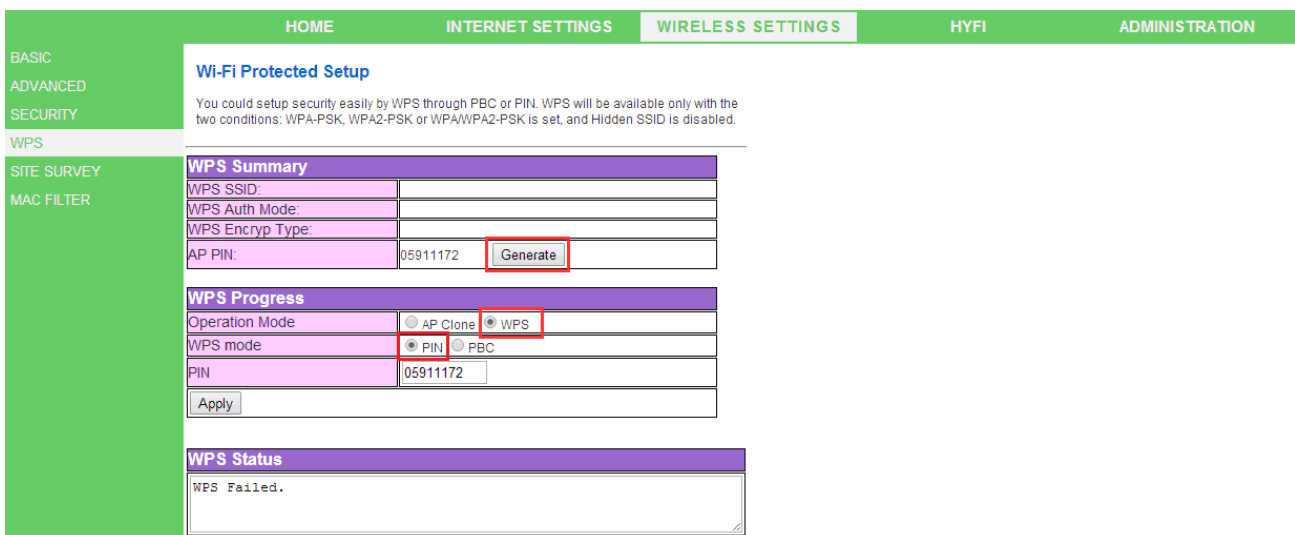


5.6.4 WPS (Wi-Fi Protected Setup)

This function helps establish the Wi-Fi security. WPS modes include **PIN** (Personal Identification Number) and **PBC** (Push Button Configuration). Before starting the WPS process, the WLAN security must be set up. Please first set up **Security Mode** with one value from the options of WPA-PSK, WPA2-PSK, WPA/WPA2-PSK and then start the WPS process.

PIN: From client's Web UI, you select WPS mode **PIN**, generate the PIN code and click **Apply** to start the WPS process. Then from AP's Web UI, you select WPS mode **PIN**, enter the generated PIN and click **Apply** to start the WPS process.

Client:



The screenshot shows the 'Wi-Fi Protected Setup' page in the Client Web UI. The navigation tabs are HOME, INTERNET SETTINGS, WIRELESS SETTINGS, HYFI, and ADMINISTRATION. The left sidebar includes BASIC, ADVANCED, SECURITY, WPS, SITE SURVEY, and MAC FILTER. The main content area has a purple header 'Wi-Fi Protected Setup' and a note: 'You could setup security easily by WPS through PBC or PIN. WPS will be available only with the two conditions: WPA-PSK, WPA2-PSK or WPA/WPA2-PSK is set, and Hidden SSID is disabled.'

WPS Summary

| | |
|------------------|--|
| WPS SSID: | |
| WPS Auth Mode: | |
| WPS Encryp Type: | |
| AP PIN: | 05911172 <input type="button" value="Generate"/> |

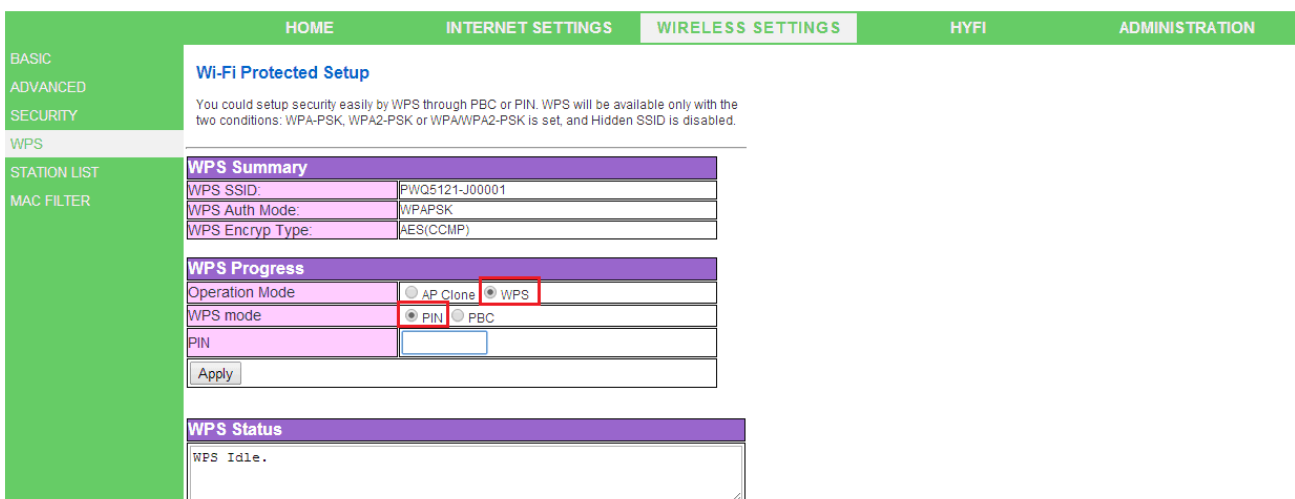
WPS Progress

| | |
|--------------------------------------|---|
| Operation Mode | <input type="radio"/> AP Clone <input checked="" type="radio"/> WPS |
| WPS mode | <input checked="" type="radio"/> PIN <input type="radio"/> PBC |
| PIN | 05911172 |
| <input type="button" value="Apply"/> | |

WPS Status

WPS Failed.

AP:



The screenshot shows the 'Wi-Fi Protected Setup' page in the AP Web UI. The navigation tabs are HOME, INTERNET SETTINGS, WIRELESS SETTINGS, HYFI, and ADMINISTRATION. The left sidebar includes BASIC, ADVANCED, SECURITY, WPS, STATION LIST, and MAC FILTER. The main content area has a purple header 'Wi-Fi Protected Setup' and a note: 'You could setup security easily by WPS through PBC or PIN. WPS will be available only with the two conditions: WPA-PSK, WPA2-PSK or WPA/WPA2-PSK is set, and Hidden SSID is disabled.'

WPS Summary

| | |
|------------------|----------------|
| WPS SSID: | PWQ5121-J00001 |
| WPS Auth Mode: | WPAPSK |
| WPS Encryp Type: | AES(CCMP) |

WPS Progress

| | |
|--------------------------------------|---|
| Operation Mode | <input type="radio"/> AP Clone <input checked="" type="radio"/> WPS |
| WPS mode | <input checked="" type="radio"/> PIN <input type="radio"/> PBC |
| PIN | |
| <input type="button" value="Apply"/> | |

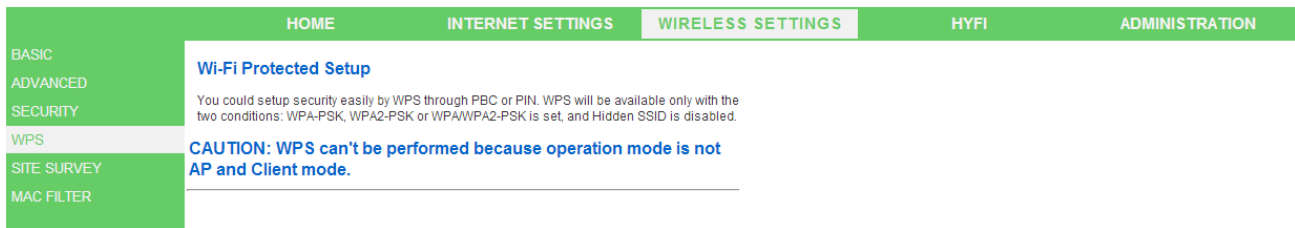
WPS Status

WPS Idle.

PBC: PBC can be done through either the Web UI or the physical WPS button.

- Press the physical WPS buttons both from the client and the AP to start and complete the WPS process.
- Or from both client's Web UI and AP's Web UI, you select WPS mode **PBC** and then click **Apply** to start and complete the WPS process.

WPS can only be performed between an AP and a client. If not the case, notification messages will be prompted while viewing WPS settings.



NOTE : WPS will be available only under the following conditions:

1. Security Mode, WPA-PSK, WPA2-PSK or WPA/WPA2-PSK, is set.
2. Hidden SSID is disabled.
3. The process is run between an AP and a client.

The function of the physical WPS button (default function is AP clone) follows the Operation Mode setting in WPS configuration, meaning that clicking this physical button will perform action as set in Operation Mode.

5.6.5 Station list

The list shows the associated clients.

5.6.6 Site Survey (AP Mode Site Survey)

Site survey shows information of available APs around and you may choose one AP from the list to make connection.

5.6.7 MAC Filter

MAC filtering allows the user to either limit specific MAC addresses from associating with the AP, or specifically indicates which MAC addresses can associate with the AP.

5.6.8 AP Clone

With this function, while **not in HyFi mode**, the security configuration (i.e. SSID, pass phrase) from a source AP will be copied and configured automatically on the target client – an AP or a client, helping to establish the Wi-Fi security on the target client. AP Clone can be done through either the Web UI or the physical WPS button. This enables seamless roaming of wireless clients in the network.

Physical WPS Button:

The AP Clone process can be performed by pressing the physical WPS buttons from both the source AP and the target client. After AP Clone, the target client will turn itself into an AP if it is a client before the process.

NOTE : The function of the physical WPS button (default function is AP clone) follows the Operation Mode setting in WPS configuration, meaning that clicking this physical button will perform action as set in Operation Mode.

Web UI:

Under WIRELESS SETTINGS > WPS, for Operation Mode, click on **AP Clone** option and then click **Apply** to start the process. Do this on both the source AP and the target client to complete the AP clone process.

The screenshot displays the 'WPS' configuration page within the 'WIRELESS SETTINGS' tab. The page is titled 'Wi-Fi Protected Setup' and includes a note about WPS availability conditions. It features three main sections: 'WPS Summary', 'WPS Progress', and 'WPS Status'. In the 'WPS Progress' section, the 'Operation Mode' is set to 'AP Clone', which is highlighted with a red box. The 'WPS Status' section shows 'WPS Processing ..', also highlighted with a red box. The 'WPS Summary' section contains fields for WPS SSID, WPS Auth Mode, WPS Encryp Type, and AP PIN (38028205), with a 'Generate' button next to the PIN field.

| WPS Summary | |
|------------------|--|
| WPS SSID: | |
| WPS Auth Mode: | |
| WPS Encryp Type: | |
| AP PIN: | 38028205 <input type="button" value="Generate"/> |

| WPS Progress | |
|--------------------------------------|---|
| Operation Mode | <input checked="" type="radio"/> AP Clone <input type="radio"/> WPS |
| <input type="button" value="Apply"/> | |

| WPS Status | |
|-------------------|--|
| WPS Processing .. | |

5.7 Administration

5.7.1 Management (System Management)

The screenshot shows the 'ADMINISTRATION' section of the web interface. The 'MANAGEMENT' menu is selected, and the 'System Management' page is displayed. The page contains a 'System Management' section with the instruction 'Set your account, password.' Below this is the 'Administrator Settings' section, which includes three input fields: 'Account' (with 'Admin' entered), 'Password' (with masked characters '...'), and 'Confirm Password'. There are 'Apply' and 'Cancel' buttons at the bottom of the settings section.

| Administrator Settings | |
|------------------------|---|
| Item | Description |
| Account | Enter the name for login. The default name is “root”. |
| Password | Enter the password for login. The default password is “root”. |
| Confirm Password | Enter the password again |

5.7.2 Upgrade firmware

This page provides the firmware upgrade function.

The screenshot shows the 'ADMINISTRATION' section of the web interface. The 'MANAGEMENT' menu is selected, and the 'Upgrade Firmware' page is displayed. The page contains a 'Upgrade Firmware' section with the instruction 'Upgrade firmware for the device. The upgrade process takes about 3 minute and DO NOT POWER OFF the device during the period. Please be noticed that a corrupted image will crash the system'. Below this is the 'Update Firmware' section, which includes a 'Location:' label, an input field, and a '浏览...' (Browse) button. There is an 'Apply' button at the bottom of the settings section.

Click the browse button to browse the file and click “open” button to select the file. The upgrade process takes about 1 minute and **DO NOT POWER OFF** the device during the process. In order to continue configuration, please refresh the PC web-browser to reflect new upgraded FW settings.

5.7.3 Settings management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

HOME INTERNET SETTINGS WIRELESS SETTINGS HYFI ADMINISTRATION

MANAGEMENT
 UPLOAD FIRMWARE
 SETTINGS MANAGEMENT
 STATUS
 STATISTICS
 SYSTEM LOG

Settings Management

You can do factory default value or export/import it, and Do system restart.

Export Settings

Export Button

Import Settings

Settings File Location

Load Factory Defaults

Load Default Button

Reboot System

Reboot Button

5.7.4 Status

The page shows system status information.

HOME INTERNET SETTINGS WIRELESS SETTINGS HYFI ADMINISTRATION

MANAGEMENT
 UPLOAD FIRMWARE
 SETTINGS MANAGEMENT
 STATUS
 STATISTICS
 SYSTEM LOG

Access Point Status

Display information of the device model, software version, local network, and wireless information

System Info

| | |
|---------------------|-------------------------------|
| Model Name | PWQ 6121 |
| System Version | PWQ612100139101 (Sep 10 2013) |
| System Time | Thu Jan 1 00:30:54 1970 |
| Boot Loader version | U-Boot 1.1.4 A |

Local Network

| | |
|------------------|-------------------|
| Local IP Address | 192.168.1.2 |
| Local Netmask | 255.255.255.0 |
| MAC Address | 00:05:9E:11:20:2B |

Wireless Information

| | |
|--------------------|-------------------|
| Mode | WDS (rcctap) |
| Band | 11NAHT40MINUS |
| SSID | PWQ5121-112029 |
| Channel | Auto |
| Encryption | None |
| MAC Address | 00:05:9E:11:20:2A |
| Associated Clients | 0 |

5.7.5 Statistics

Statistic

Show the statistic data of the device

Memory

| | |
|---------------|----------|
| Memory Total: | 62580 kB |
| Memory Left: | 45456 kB |

All interfaces

| Interfaces | Ethernet |
|------------|----------|
| Rx Packet: | 568 |
| Rx Byte: | 162651 |
| Tx Packet: | 1070 |
| Tx Byte: | 470018 |
| Interfaces | Wireless |
| Rx Packet: | 0 |
| Rx Byte: | 0 |
| Tx Packet: | 1980 |
| Tx Byte: | 848025 |

| Administrator Settings | |
|------------------------|--|
| Item | Description |
| Memory total | This is the total memory size for this device. |
| Memory left | This displays the available memory size. |

All interfaces

The “Rx Packet”, “Rx Byte”, “Tx Packet” and “Tx Byte” show the status of all interfaces, including “Ethernet and Wireless”.

5.7.6 System log

The system log displays in this window. For technical support, you may need to copy and save the log to text file and send it to the technical service. Click “**Refresh**” button to refresh the page or “**Clear**” button to clear the log.

System Log

You could check the system log below

System Log

```

1970-01-01 00:00:10 [Informational] syslogd started: BusyBox v1.15.0
1970-01-01 00:00:10 [Notice] kernel: klogd started: BusyBox v1.15.0 (2013-09-10)
1970-01-01 00:00:10 [Notice] kernel: Linux version 2.6.31--ESDR-9.3.2.43-svn6 ()
1970-01-01 00:00:10 [Warning] kernel: flash_size passed from bootloader = 16
1970-01-01 00:00:10 [Warning] kernel: arg 1: console=ttyS0,115200
1970 01 01 00:00:10 [Warning] kernel: arg 2: root=31:02
1970 01 01 00:00:10 [Warning] kernel: arg 3: rootfstype=jffs2
1970 01 01 00:00:10 [Warning] kernel: arg 4: init=/sbin/init
1970-01-01 00:00:10 [Warning] kernel: arg 5: mtdpart0=ath-nor0:256k(u-boot),64k(

```

5.8 Channel Number

5.8.1 The following table lists the available frequencies (in MHz) for the **2.4 GHz** radio.

| Channel No. | Frequency | Region Domain |
|-------------|-----------|--|
| 1 | 2412 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 2 | 2417 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 3 | 2422 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 4 | 2427 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 5 | 2432 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 6 | 2437 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 7 | 2442 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 8 | 2447 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 9 | 2452 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 10 | 2457 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 11 | 2462 | Americas, Taiwan, EMEA, Japan, Australia and China |
| 12 | 2467 | EMEA, Japan, Australia and China |
| 13 | 2472 | EMEA, Japan, Australia and China |
| 14 | 2484 | Japan, only in 802.11b mode |

*: EMEA (Europe, the Middle East and Africa).

The available channel is set by the factory according to the region of distribution and can't be changed by user. For example, the available channel of the American model is from ch1 to ch11.

5.8.2 The following table lists the available frequencies (in MHz) for the **5 GHz** radio.

802.11a (20MHz)

| Channel | Frequency | United States | Germany | France |
|---------|-----------|---------------|---------|--------|
| 36 | 5180 | Yes | Yes | Yes |
| 40 | 5200 | Yes | Yes | Yes |
| 44 | 5220 | Yes | Yes | Yes |
| 48 | 5240 | Yes | Yes | Yes |
| 149 | 5745 | Yes | No | No |
| 153 | 5760 | Yes | No | No |
| 157 | 5785 | Yes | No | No |
| 161 | 5805 | Yes | No | No |
| 165 | 5825 | Yes | No | No |

802.11a (40MHz)

| Channel | Frequency | United States | Germany | France |
|---------|-----------|---------------|---------|--------|
| 38 | 5190 | Yes | Yes | Yes |
| 46 | 5230 | Yes | Yes | Yes |
| 151 | 5755 | Yes | Yes | Yes |
| 159 | 5795 | Yes | Yes | Yes |

6 Enhance PLC Performance

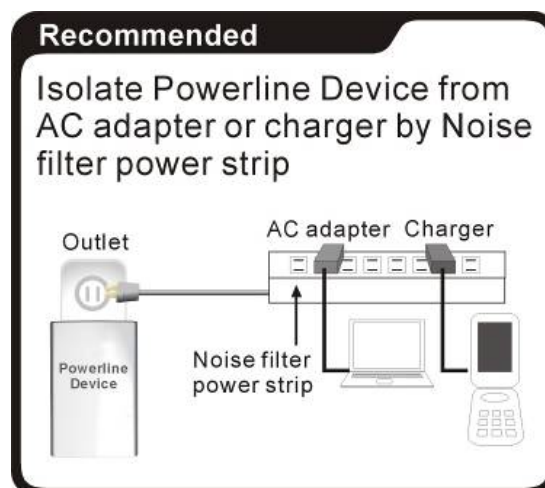
While Powerline device delivers data over the existing electrical wiring in the house, the actual performance may be affected by electrical noises or the length of the wiring. To improve PLC performance, please refer to below recommendations while placing the Powerline device.

AC outlets connection

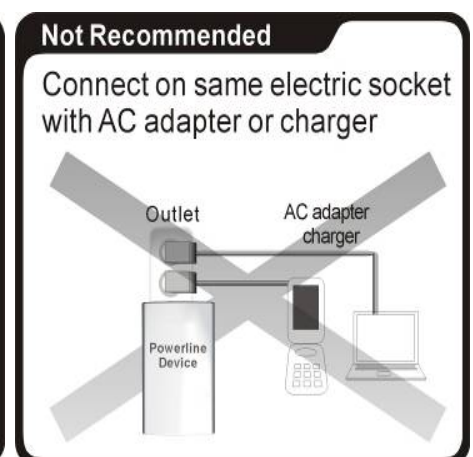
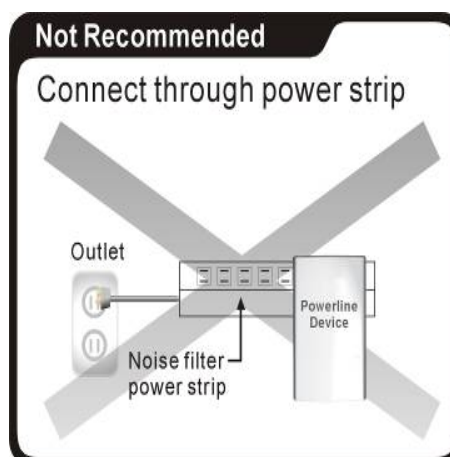
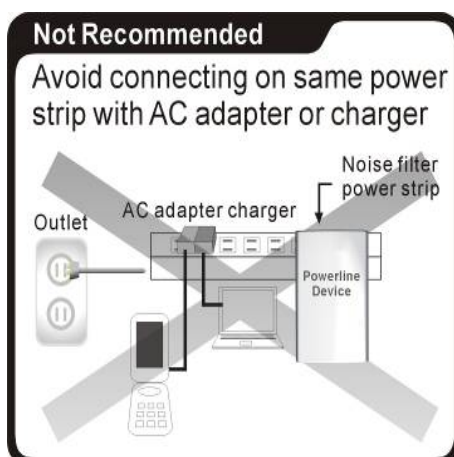
- Avoid connecting PLC device to an uninterruptible power supply (UPS) or backup power supply device. For best results, connect the adaptors directly to a wall outlet is recommended.
- Avoid connecting high-power consuming appliances to the same wall outlet.

See the following illustration:

For better performance, the following connection is recommended.



The following connections are **NOT** recommended.



Connection via Power Strip

If user intends to connect the PLC device via power strip, please follow below reference for better performance:

- Make sure the power strip does not support a noise filter or a surge protector.

Electrical Interference

Some household appliances may produce noise emission. If noise emission is spread over the electrical wiring it will affect PLC performance in the house. For the best results, we recommend to connect an electrical noise filter with the appliances such as:

- Battery chargers (including cell phone chargers)
- Hair dryers
- Power drills
- Halogen light
- Vacuum cleaner
- Lights or lamps with touch-sensitivity feature supported

Electrical Wiring

The PLC device delivers data over the existing electrical wiring in the house. Actual PLC data transfer rate might vary including the transmission distance between two PLC adapters..

7 Specifications

| 500Mbps Powerline Ethernet Bridge | |
|---|--|
| Supported Protocols | PLC: IEEE 1901 and HomePlug AV compliant Co-existence with HomePlug 1.0 nodes |
| Data Transfer Rate | PHY Rate: up to 500Mbps over powerline TCP Rate: up to 95Mbps UDP Rate: up to 95Mbps |
| Frequency Band | Support 2 MHz to 68 MHz operating frequency |
| Security | 128-bit AES Encryption with key management for secure powerline communications |
| PLC Modulation | Support OFDM 4096/1024/256/64/8-QAM, QPSK, BPSK, ROBO Modulation Schemes. |
| Transmission Distance | Up to 300 meters via AC wire |
| Max Supported Devices in a network Group | 8 Active/ 16 Total |

| 300Mbps Wireless N Extender | |
|-----------------------------|--|
| Standard | WLAN: IEEE 802.11 a/b/g/n |
| Maximum Throughput | WLAN to Ethernet: Up to 175 Mbps(2.4GHz) / 190 Mbps(5GHz) |
| | HyFi: Up to 180 Mbps |
| Frequency | Selectable Dual Band. 2.4GHz 2.412~2.484 GHz 5GHz 5.180 GHz ~ 5.240 GHz, 5.745 GHz ~ 5.825 GHz It varies in different countries or regions. |

| | | | |
|------------------------------|------------------|------------|----------|
| WLAN transceiver spec | RF Power: | | |
| | Standard | Data Rate | dBm |
| | IEEE 802.11a | 6 Mbps | 19 dBm |
| | IEEE 802.11b | 11 Mps | 17 dBm |
| | IEEE 802.11g | 6 Mbps | 17 dBm |
| | IEEE 802.11gn | HT20 MCS0 | 18 dBm |
| | | HT20 MCS7 | 14 dBm |
| | | HT40 MCS0 | 17 dBm |
| | | HT40 MCS7 | 14 dBm |
| | | HT20 MCS8 | 21 dBm |
| | | HT20 MCS15 | 17 dBm |
| | | HT40 MCS8 | 20 dBm |
| | | HT40 MCS15 | 17 dBm |
| | IEEE 802.11an | HT20 MCS0 | 16 dBm |
| | | HT20 MCS7 | 10.5 dBm |
| | | HT40 MCS0 | 13.5 dBm |
| | | HT40 MCS7 | 10 dBm |
| | | HT20 MCS8 | 19 dBm |
| | | HT20 MCS15 | 13 dBm |
| | | HT40 MCS8 | 16.5 dBm |
| HT40 MCS15 | | 12.5 dBm | |

| | | | | | | | |
|----------------------------|--|--|--------------|--|--------------|------------------------------------|---------------|
| | Sensitivity: | | | | | | |
| | The following table shows limit dBm values and all test results fall within the limits. | | | | | | |
| | Standard | | Data Rate | | Test Limit | | |
| | IEEE 802.11a | | 6 Mbps | | -84 dBm | | |
| | | | 54 Mbps | | -70 dBm | | |
| | IEEE 802.11b | | 11 Mbps | | -80 dBm | | |
| | IEEE 802.11g | | 6 Mbps | | -84 dBm | | |
| | | | 54 Mbps | | -70 dBm | | |
| | IEEE 802.11gn | | HT20 MCS0 | | -84 dBm | | |
| | | | HT20 MCS7 | | -66 dBm | | |
| | | | HT40 MCS0 | | -83 dBm | | |
| | | | HT40 MCS7 | | -64 dBm | | |
| | IEEE 802.11an | | HT20 MCS0 | | -84 dBm | | |
| | | | HT20 MCS7 | | -66 dBm | | |
| | | | HT40 MCS0 | | -83 dBm | | |
| HT40 MCS7 | | | -64 dBm | | | | |
| Physical Data Rate: | | | | | | | |
| 802.11a | | 6, 9, 12, 18, 24, 36, 48, 54Mbps | | | | | |
| 802.11b | | 1, 2, 5.5, 11Mbps | | | | | |
| 802.11g | | 6, 9, 12, 18, 24, 36, 48, 54Mbps | | | | | |
| 802.11n | | Up to 300 Mbps (2T2R) | | | | | |
| WPS | PIN (Personal Identification Number) and PBC (Push Button Configuration) | | | | | | |
| Security Mode | Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 PSK, WPA/WPA2, 802.1X | | | | | | |
| Wireless Modulation | OFDM: BPSK, QPSK, 16-QAM, 64-QAM DSSS: DBPSK, DQPSK, CCK | | | | | | |
| Antenna type | 2T2R | | | | | | |
| Power consumption | VCC=3.26 V | Continue Current by Current Meter (A) | | Continue Current by Current Probe (A) | | Power on Inrush Current (A) | |
| | Full run | 0.9 | 2.9 W | 1.27 | 4.1 W | 0.79 | 2.6 W |
| | Full run with AC loading | 0.93 | 3W | 1.32 | 4.3 W | 0.81 | 2.64 W |

| Other System Specifications | |
|------------------------------|---|
| Ethernet Interface | 1000BASE-T Ethernet RJ-45 port * 1 |
| AC Pass-through | Built-in |
| Operating Temperature | <u>Operating</u> : 0~40 °C |
| Relative Humidity | Operating: 10~85% Non-Condensing Storage: 5~90% Non-Condensing |
| Power Supply | 100 ~ 240 VAC 50/60Hz |
| Electric Plug Type | Available for Type B, E, F |
| Dimension | |
| LED Indicators | POWER (Green) |
| | PLC status (Green) |
| | Wireless status LED (Green/Red) |
| | Ethernet (Green) |
| Buttons | AP Clone(default) or WPS |
| | Grouping/Pairing |
| | Power on/off |
| | Reset |
| Quality of Service | <ul style="list-style-type: none"> - Priority-based CSMA/CA channel access schemes maximize Efficiency and throughput. - Integrated Quality of Service (QoS) enhancements. - Hardware Packet Classifiers for ToS, CoS and IP Port Number. - Supports IGMP managed multicast sessions. |

8 Statement and Notice

FCC Statement:

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

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

FCC Caution:

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

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.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted to indoor environments only.

Our products work well for channels 1-11 in the USA and Canada markets. It does not work well with other channels.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

IC statement:

This device complies with Industry Canada license-exempt RSS standard(s). 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.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux états-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.

Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;