User's Manual

brite-View
vision accomplished

LinkE Air

BVH-5101C

BVH-5101

BVP-5100

Preface

BVH-5101 is a wireless AP device with **P**ower**L**ine **C**ommunication (PLC) capability. With the latest 500Mbps PLC technology (Homeplug AV), crossing-floor communication in a concrete building, which has been a big problem for wireless networking, is made as a extreme reliable product. Its cutting edge 802.11n wireless technology provides the highest wireless throughput for devices in the same floor. Embedded 1T1R MIMO antenna makes it easy for wall installation.

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 **Powerline Wireless N Extender** product settings. To use these chapters, you should have experience working with the TCP/IP configuration and be familiar with the concepts and terminology of local area networks.

Important Safety Notes

BVH-5101 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** operates 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** locates 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.

TABLET of CONTENT

Ch 1. Product Overview

Package Content

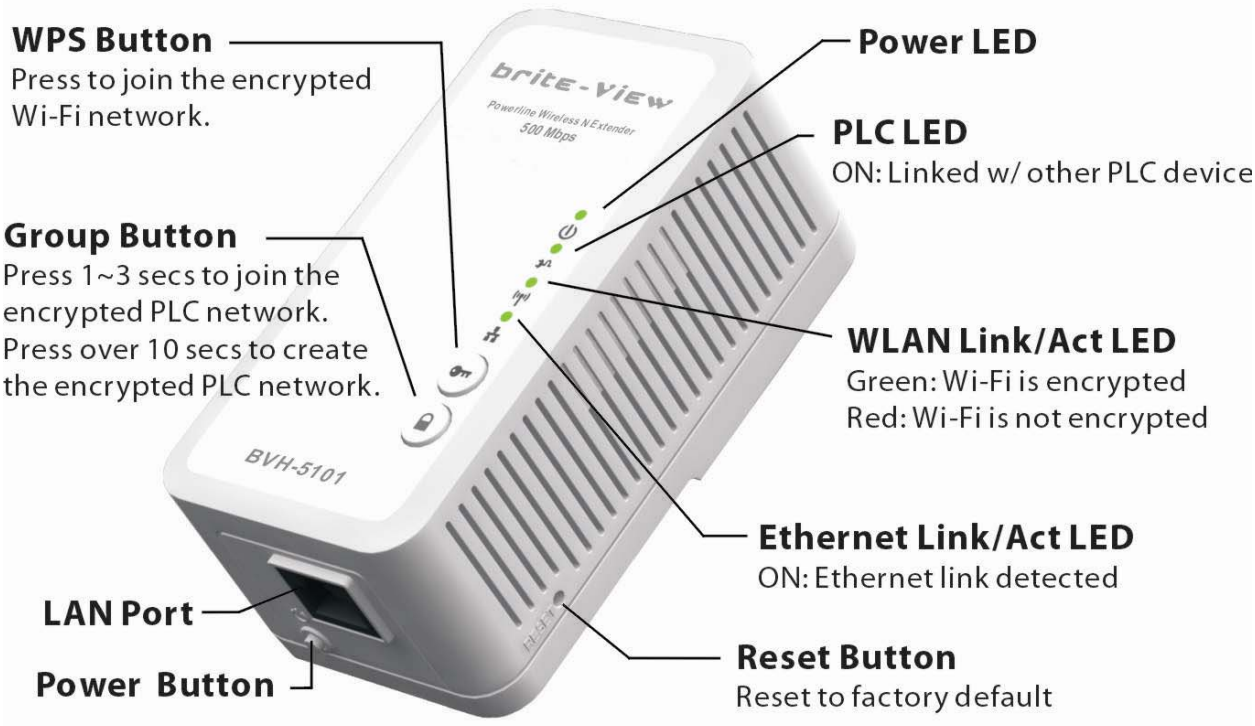
Before starting the installation of the device, please make sure the package contains the following items:

	Single pack	Combo pack
Device	 **Powerline Wireless N Extender**	 **Powerline Ethernet Bridge**  **Powerline Wireless N Extender**
Accessories	➢ RJ-45 Cable x 1	➢ RJ-45 Cable x2

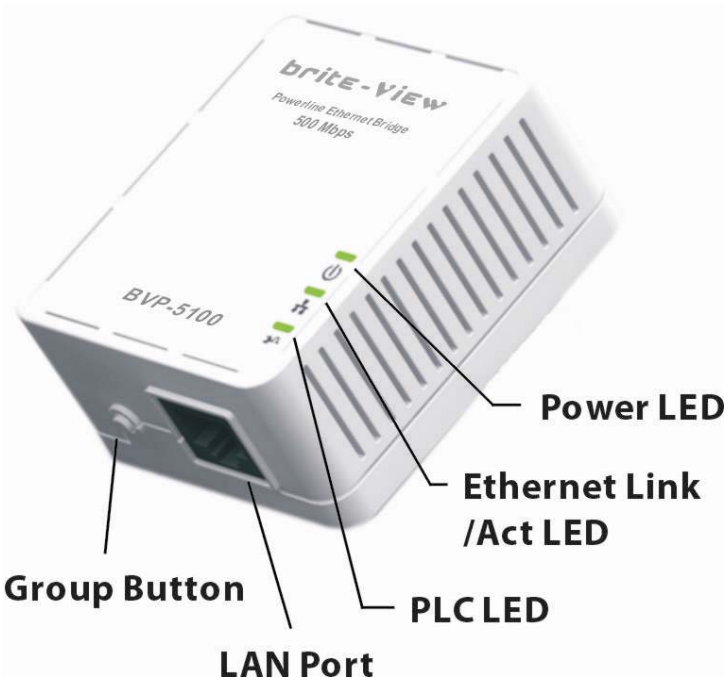
Buttons and LEDs

500 Mbps Powerline Wireless N Extender (BVH-5101)

1T1R antennas are embedded into the device



500 Mbps Powerline Bridge (BVP-5100)



LEDs	
Power LED **Green**	ON: Power on and ready. BLINKING: During **group pairing procedure (creating an encrypted PLC network)**. In this procedure, the device is creating or being joined into same logical network and will continue 2 minutes blinking, until the procedures succeed or canceled. To enter or cancel **group pairing procedure**, just press the group button 2~3 sec. OFF: Power off.
PLC LED **Green**	ON: Powerline link with other PLC device but no powerline traffic. BLINKING: 1. **Fast blinking**: Powerline data rate higher than 80Mbps. 2. **Normal blinking**: Powerline data rate between 40Mbps to 80Mbps. 3. **Slow blinking**: Powerline data rate slower than 40Mbps. OFF: Powerline link not detected (either other devices in same network is too far to communicate or it is alone in its logical network).
WLAN Link / Act LED **Green + Red**	Steady Green: Wi-Fi active under security protection Flash Green: Wi-Fi transmits packets under security protection, Steady Red: Wi-Fi active under NO security protection, Flash Red: Wi-Fi transmits packets under NO security protection, Blinking Green: WPS negotiation OFF：Wi-Fi off

Ethernet Link / Act LED 	ON: Ethernet Link Detected. BLINKING: Ethernet traffic detected. OFF: No Ethernet Link detected.
Buttons	
WPS Button 	Press it to enable PBC (Press Button Configuration) for WPS authentication. When WPS function is started, the WLAN Link / Act LED will be blinking.
Group Button 	Press 1 to 3 seconds (until the Power LED blinking) and release button: this will enter **group pairing procedure(creating an encrypted PLC network)**. In this procedure, the device starts joining into a logical network of other device or announcing its network group name for other devices to join. This maximum two-minute procedure automatically ends when it succeeds or is manually stopped. Press this button 2 to 3 seconds will manually stop the procedure. Press 10 seconds (until Power LED blink once and PLC LED off): clear the current and randomly generate a new network group name.
Power Button	Push to turn on and off the power of PWQ-5101
Reset Button (inside the needle pin hole)	Press the button when the device is powered on (not standby) to complete following functions: Pushing 1 second and release : will make both PLC and Wi-Fi FW settings back to factory default. NOTE: Every new PLC devices' factory default **PLC network group name** is **HomePlugAV**. During trouble shooting the powerline network group assignment, doing this to every PLC devices will make each device return to default network group, thus ensure their mutual communicability.

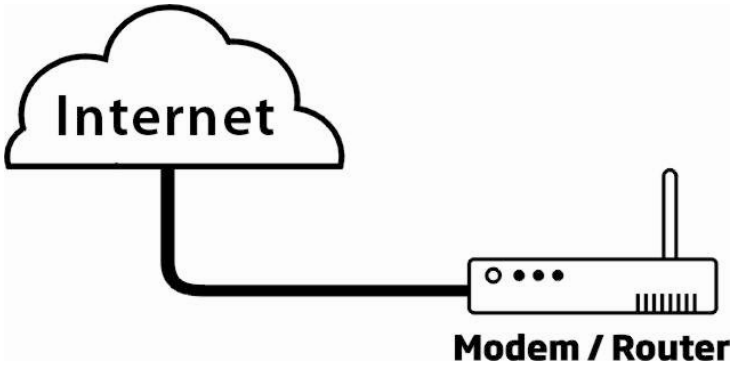
Ch 2. Hardware Installation

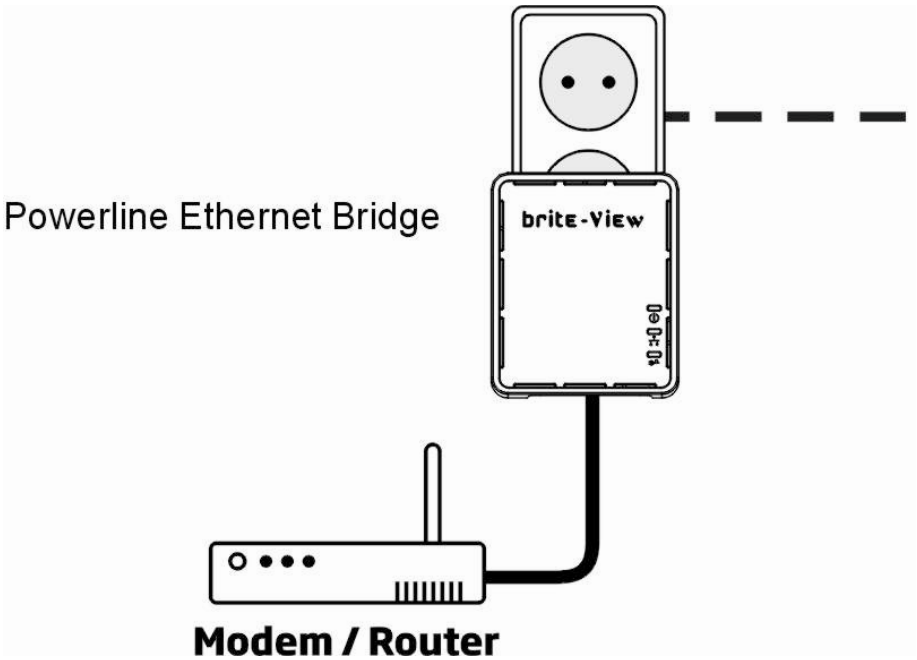
Once you check everything from the package, you can start to deploy the PLC devices. To connect this AP wirelessly need to search and connect the SSID (Wi-Fi name) of this device: **BVH-5101_XXXXXX** (factory default is no wireless security setting)

Please see the following application diagrams for different application connections of this device.

Application 1 – Link to Remote DSL via Powerline

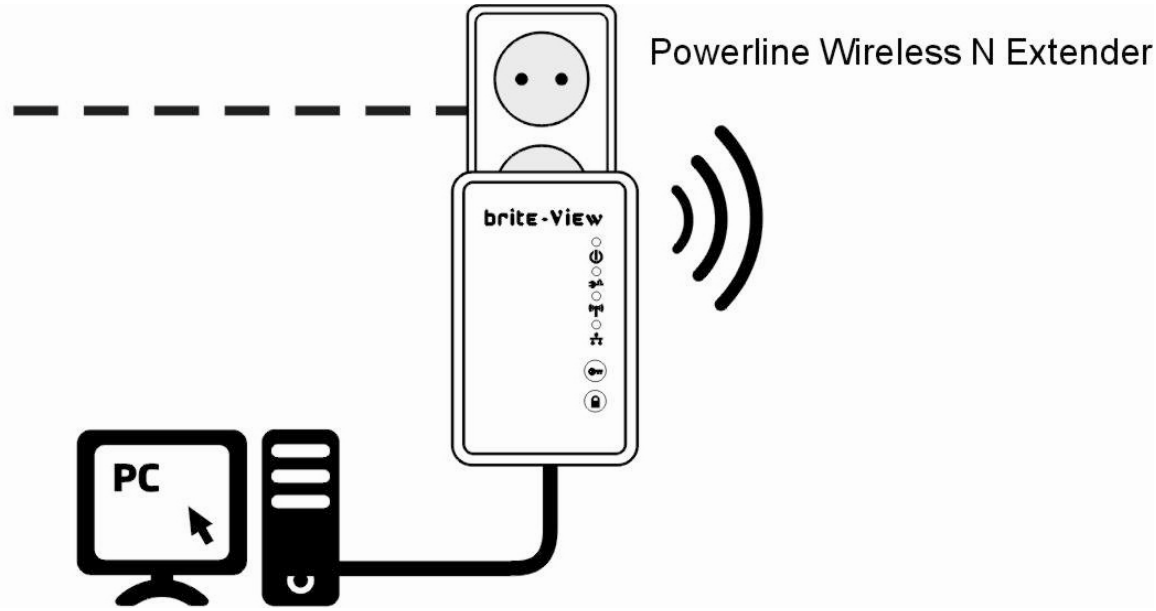
Via Powerline technology, the **Powerline Wireless N Extender** can access DSL modem at other floors for internet accesses. Note that this needs another **Powerline to Ethernet Bridge** device at other floor and is connected to internet, so that connection between **Powerline to Ethernet Bridge** and **Powerline to Ethernet Bridge** can be done through the embedded PLC technology.





Application 2 – Wireless AP

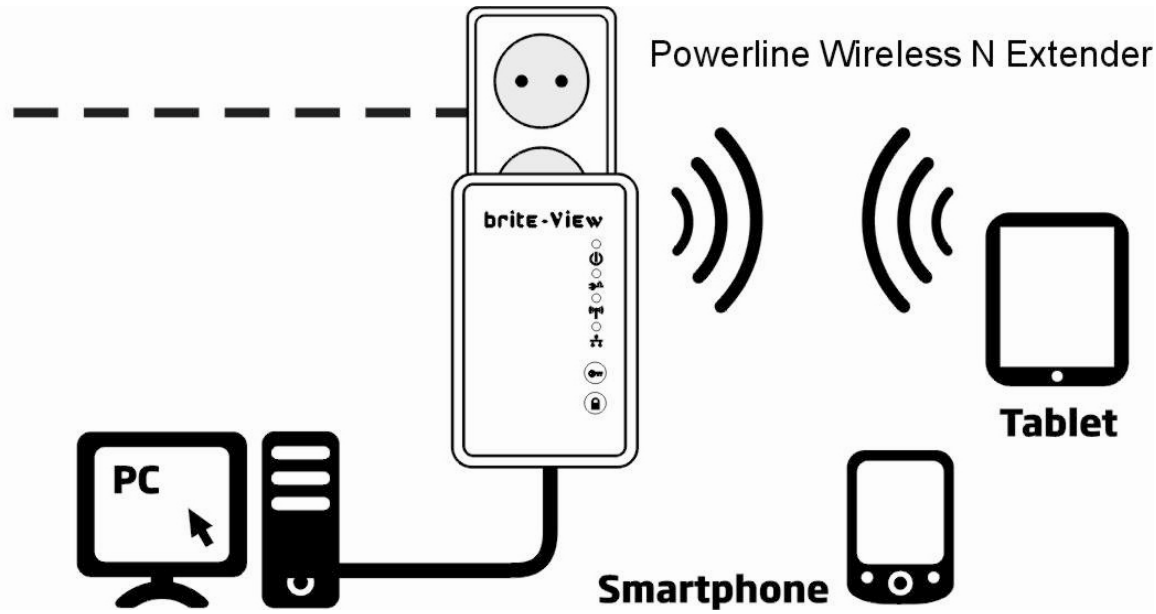
The **Powerline Wireless N Extender** can be a central 802.11n access point to for all WLAN devices to connect.



Application 3 – Multiple Floor Home Networking (1)

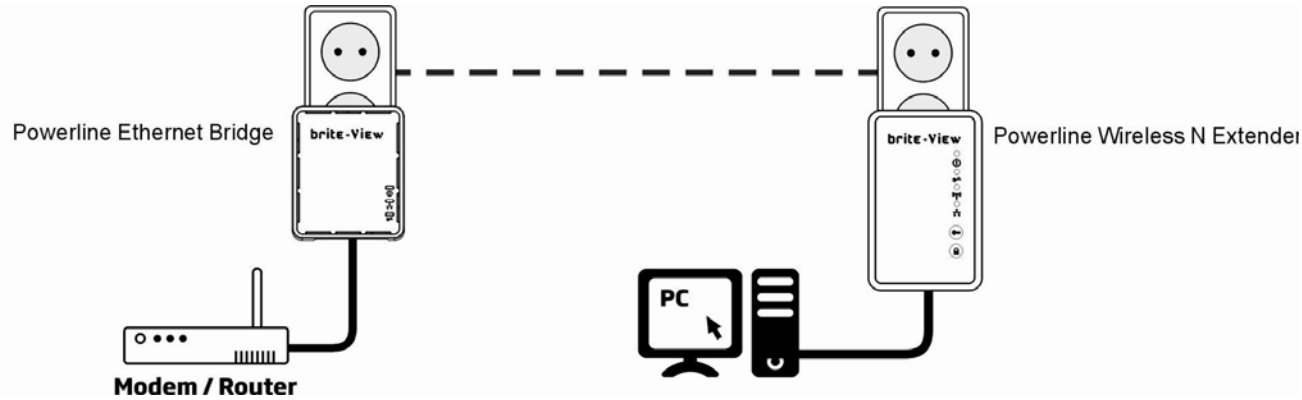
When Wi-Fi signal is not good for devices in different rooms to access, use Powerline technology powered by the **Powerline Wireless N Extender** to extend home networking range to other rooms.

While on the same floor, the Wi-Fi function can be used for tablet, Smartphone or laptop to access internet. Please see the diagram below and this allows other **Powerline to Ethernet Bridge** devices at other rooms to access network resources via the Powerline communication.



Application 3 – Multiple Floor Home Networking (2)

By turning off the **Wi-Fi** function (need to operate in the web page settings), **HomePlug AV Wireless N Extender** acts as **Powerline Ethernet Bridge**, which, when used together with other remote **Powerline Ethernet Bridge**, enables other remote Ethernet devices (ex. IP devices or PC) on the different floor to communicate via the embedded Powerline technology.



Fast Encryption by Buttons

The factory default wireless setting of this device is "**WPA-PSK**" mode and default with a set of Wi-Fi name and password on a sticker at back of the device. This section describes (1) quick wireless encryption set up using **WPS Button** and (2) quick encryption set up in a PLC network group using **Group Button**.

Setting Wireless Encryption by WPS Button

This button can be pressed for WPS PBC authentication. The default security mode is WPA-PSK, you may login the web configuration to set it to other modes. Then press the WPS button on this device and then press WPS button on the WLAN station/client card to start WPS process. It is also working if pressing WPS button on the WLAN station card first and then this device. The WPS process will be started and connected after a few seconds.

For those WLAN station card without physical WPS button, the software WPS button should be found in its utility software for this function.

Create Private Encrypted PLC Network Group (group pairing procedure)

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

If you have a pair of HomePlug AV 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 when transmit over the powerline. Users also can create more than one private network groups by pressing GROUP button directly without complicated software setup involved.

*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 it to form 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 B joins device A to become the same encrypted network. Users can add device C to device A's logical network with 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 a Network Group

If you would like to remove device from a network group, you can generate a new group name for the device that you would like to remove by following the Step I. This makes the device not able to communicate with the original network group.

Create Private Network

If users want to make devices become private or separate devices from one group to two or more network group, please follow **Step 1** on those devices, and after that, take **Step 2**. Then private network with random name is created.

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

Standby Mode

If no Ethernet cable is connected to the **Powerline Ethernet Bridge** within two minutes after powering it on, this device will go into standby mode automatically, in order to lower power consumption. Meanwhile, the POWER LED will blink ON and OFF at a slow rate. To exit the standby mode, insert the Ethernet cable or re-plug in this device to the electrical outlet.

Note:

1. Some computers support “Wake on LAN” and it may cause the Ethernet adapters to stay on without entering the standby mode.
2. **Powerline Ethernet Switch** does not go into standby mode.

Ch 3. Advanced Wi-Fi Setting – via Web Browser

Before Starting Configure

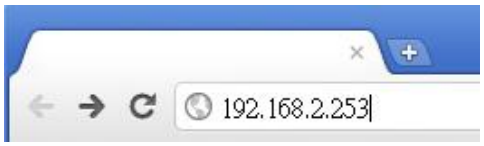
The configuration of this device is through web-browser on a PC. The default IP address of the device is **192.168.2.253**, and the subnet-mask is **255.255.255.0**. The DHCP server inside the device is default to “Off” (Disable).

1. Plug BVH-5101 into socket

2. Set your IP to the same IP domain of BVH-5101 manually (**Control panel** > **Network connections** > double click “**Local area connection**” > **Properties** > select “**Internet Protocol TCP/IP**” and click **Properties** > select "**Use the following IP address”**) ie. 192.168.2.xxx (you can set xxx from 1 – 128)

Then connect your computer to BVH-5101.

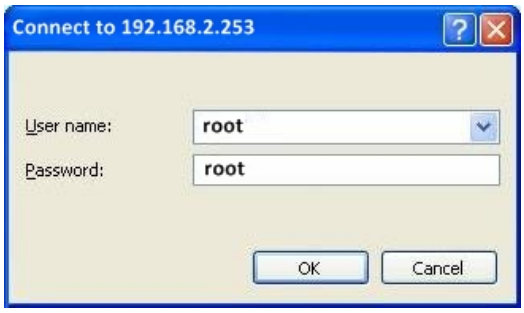
3. Running Web browser and type the IP address of this device (**192.168.2.253)** on the place you enter URL address, then you may link to BVH-5101 for further settings.



4. Login BVH-5101

User name: **root**

Password: **root**



➢ Remember changing back to “ Obtain an IP address automatically “ after all setting are done.

5. At first login, please select the language you would like to use. (**English, Traditional Chinese, Simple Chinese**)

Please ensure there is not multiple DHCP servers in your network environment, otherwise it will cause abnormal situation.

Select Language

The device provides 3 languages, English, Tradition Chinese and Simple Chinese for you to select one you want to use.

Setup Wizard

The setup Wizard can help you to finish settings in minutes. Open the page from the left panel and click “Next” button.

Step 1：Set up account and password for login BVH-5101 configuration in the future.

Step 2：Set up LAN interface.

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

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

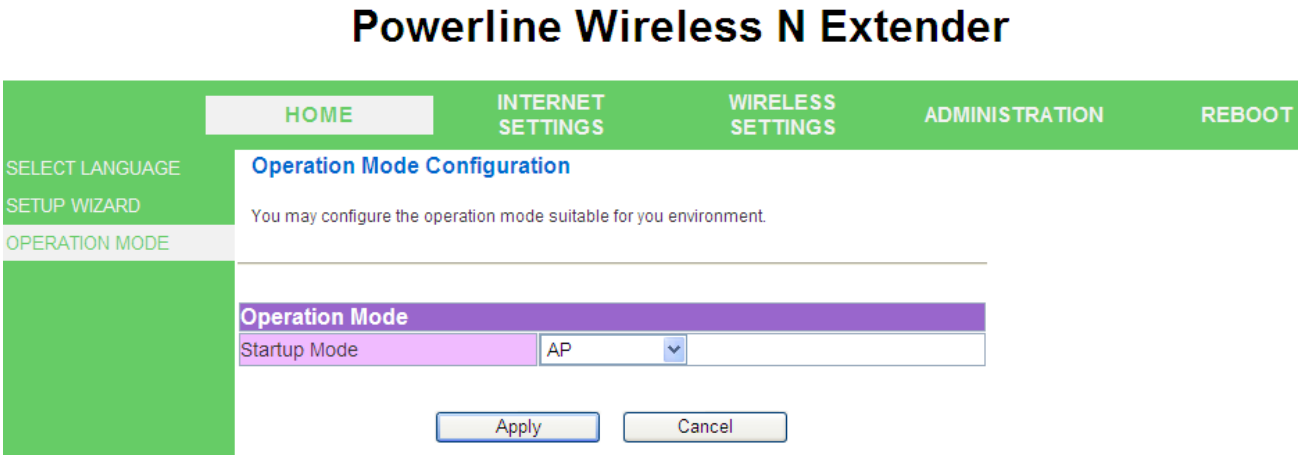
Step 5：Click “Finish” button and the device will reboot to apply the settings.

Operation Mode Configuration

This device supports five operation modes for the IP network. Click to select one between the following wireless operation modes, then click Apply button.

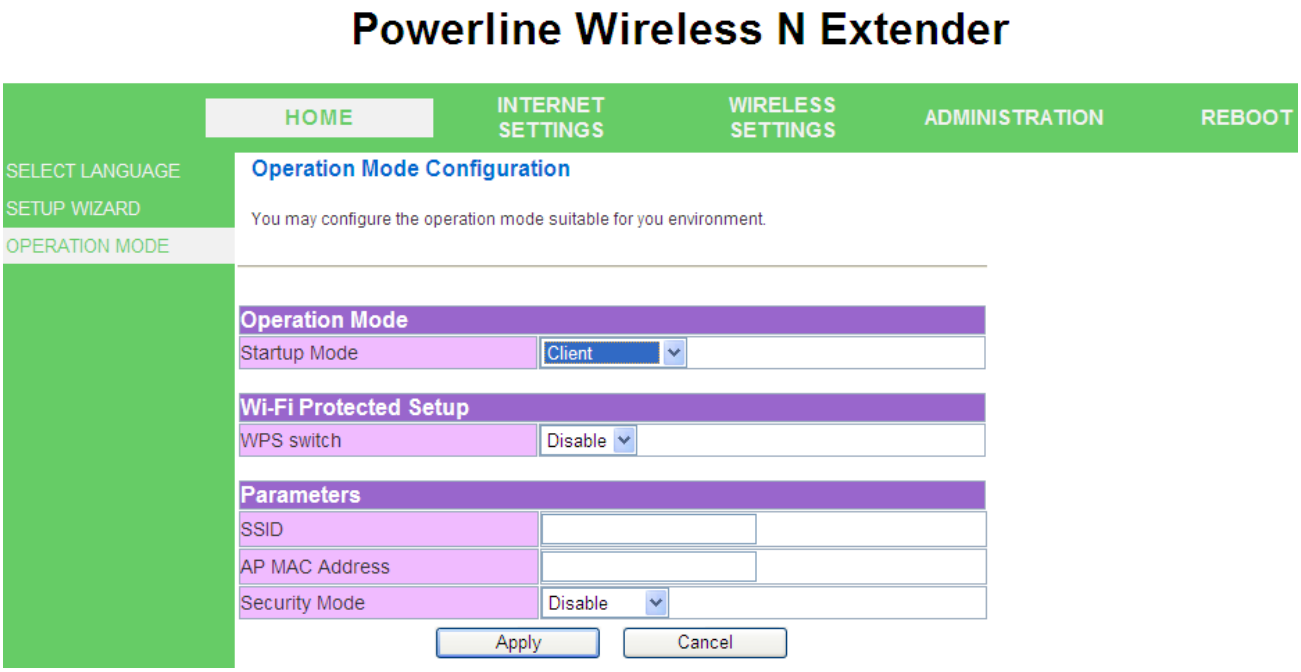
AP Mode

This device act as Wireless Access Point (**AP**) for wireless clients and provides a connection to Ethernet and PLC.



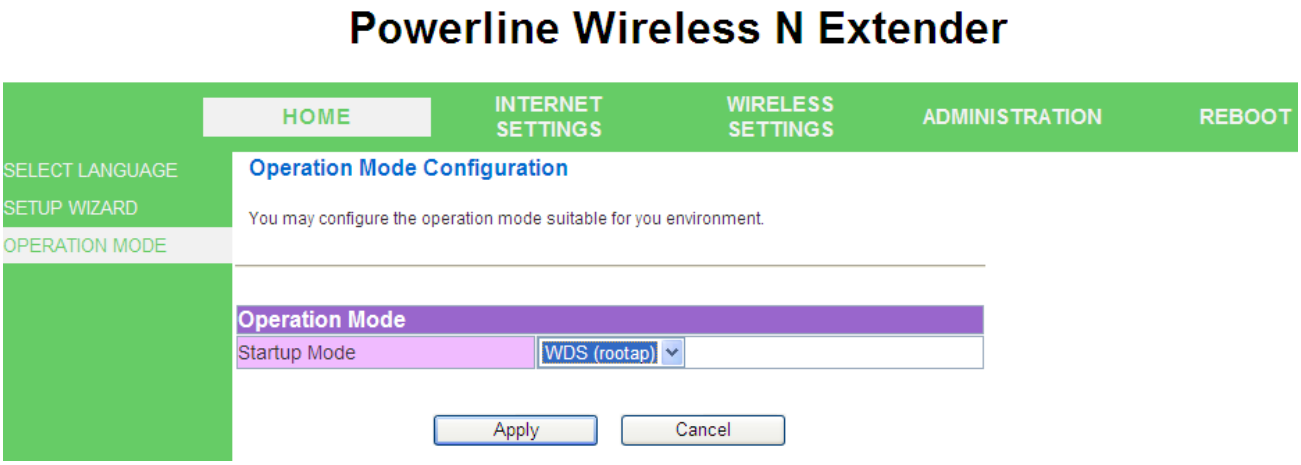
Client Mode

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 one of the wired Ethernet port to your PC and the device
become a wireless adapter



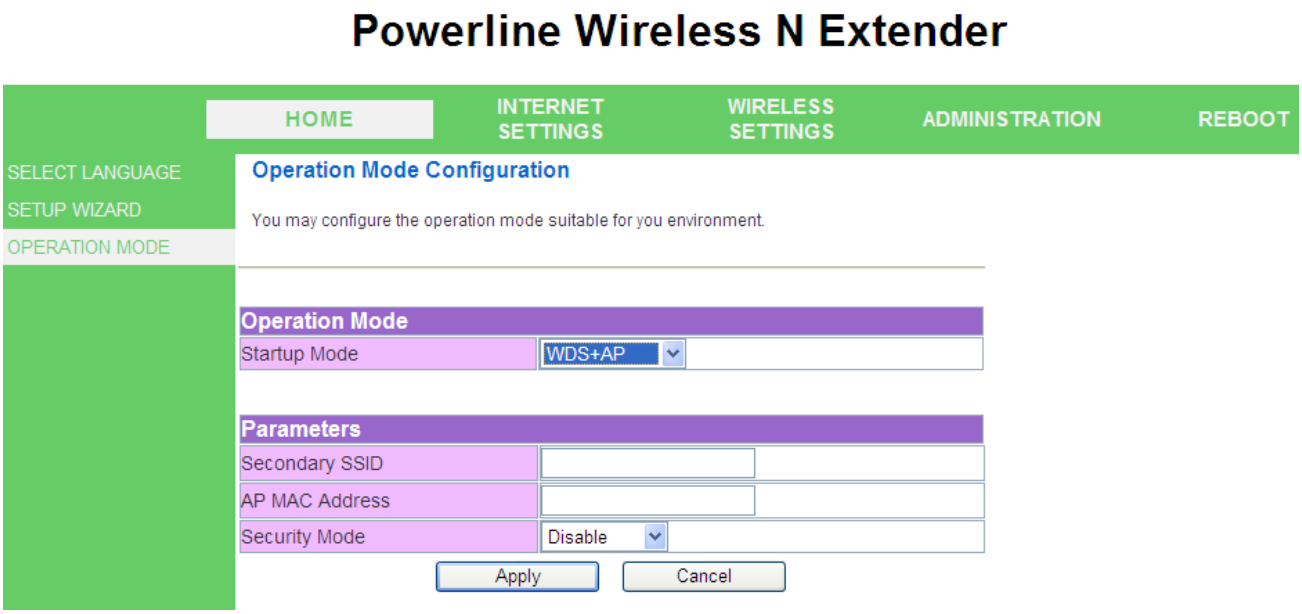
WDS (Root AP)

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 with this device)



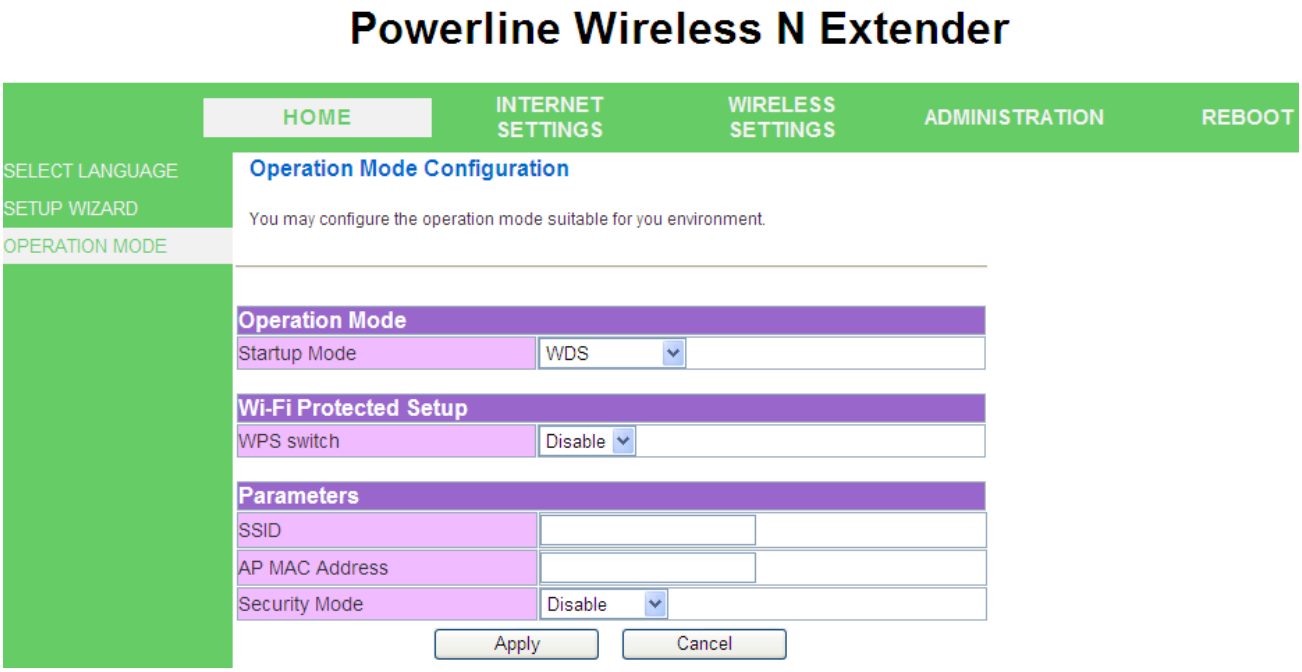
WDS + AP Mode

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

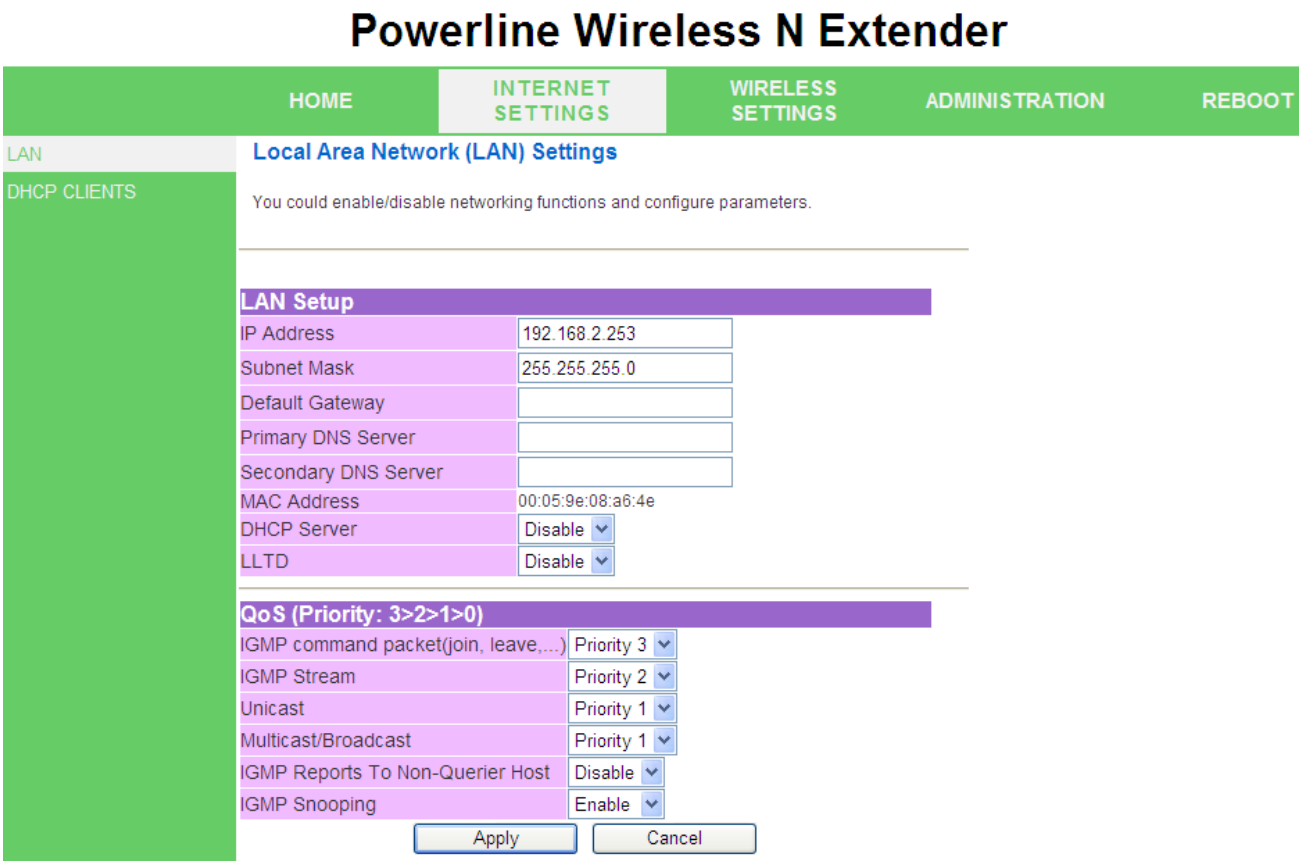


WDS Mode

The WDS system is used to create a network of AP's 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.



LAN (Local Area Network Settings)



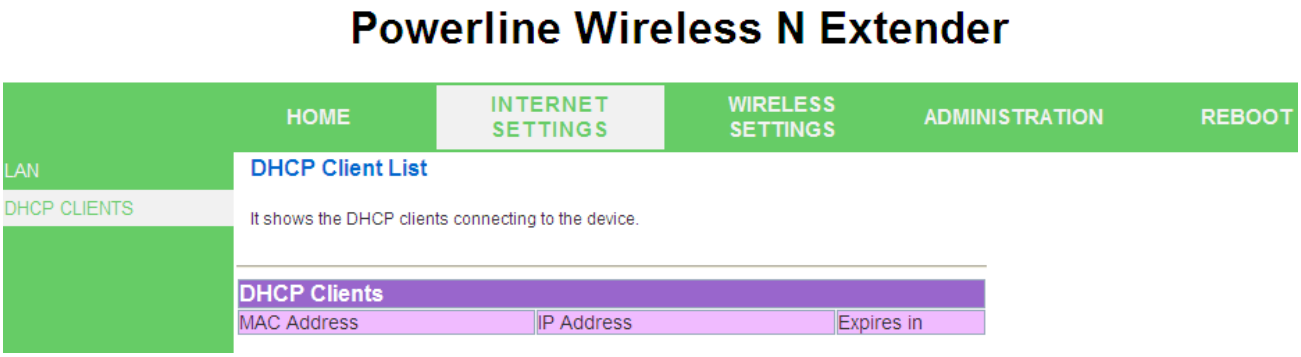
LAN setup	
Item	**Description**
IP Address	The Internet Protocol (IP) address.
Subnet mask	The number used to identify the IP subnet network.
Default Gateway	This is the default gateway for the LAN PCs.
Primary DNS Server	This is the primary DNS server for the LAN PCs which automatically get DNS IP address from this device.
Secondary DNS Server	This is the second DNS server for the LAN PCs which automatically get DNS IP address from this device.
DHCP Server	When enabling the DHCP server, there should be NO other DHCP server in this IP sub-domain, and you must setup the information below.
Start IP Address	This is the first IP Address of the IP pool from which the server assigns the IP Address to DHCP client PCs.
End IP Address	This is the last IP Address of the IP pool from which the server assigns the IP Address to DHCP client PCs.
Subnet mask	This is the subnet mask of this domain. The default value is “255.255.255.0”.

Primary DNS Server	This is the primary DNS server for the LAN PCs which automatically get DNS IP address from this device.
Secondary DNS Server	This is the second DNS server for the LAN PCs which automatically get DNS IP address from this device.
Default Gateway	This is the default gateway for the LAN PCs.
Lease Time	This is the DHCP lease time. When it is short, the IP release/renew of the LAN will be faster but the network congestion will be more.
Statically Assigned	You can manually assign the IP Address to the certain PCs. Enter the MAC Address and IP Address in the table.
LLTD	Enable this function to support LLTD (Link Layer Topology Discovery) for Windows Vista. It shows the status of connection in the Windows Vista.

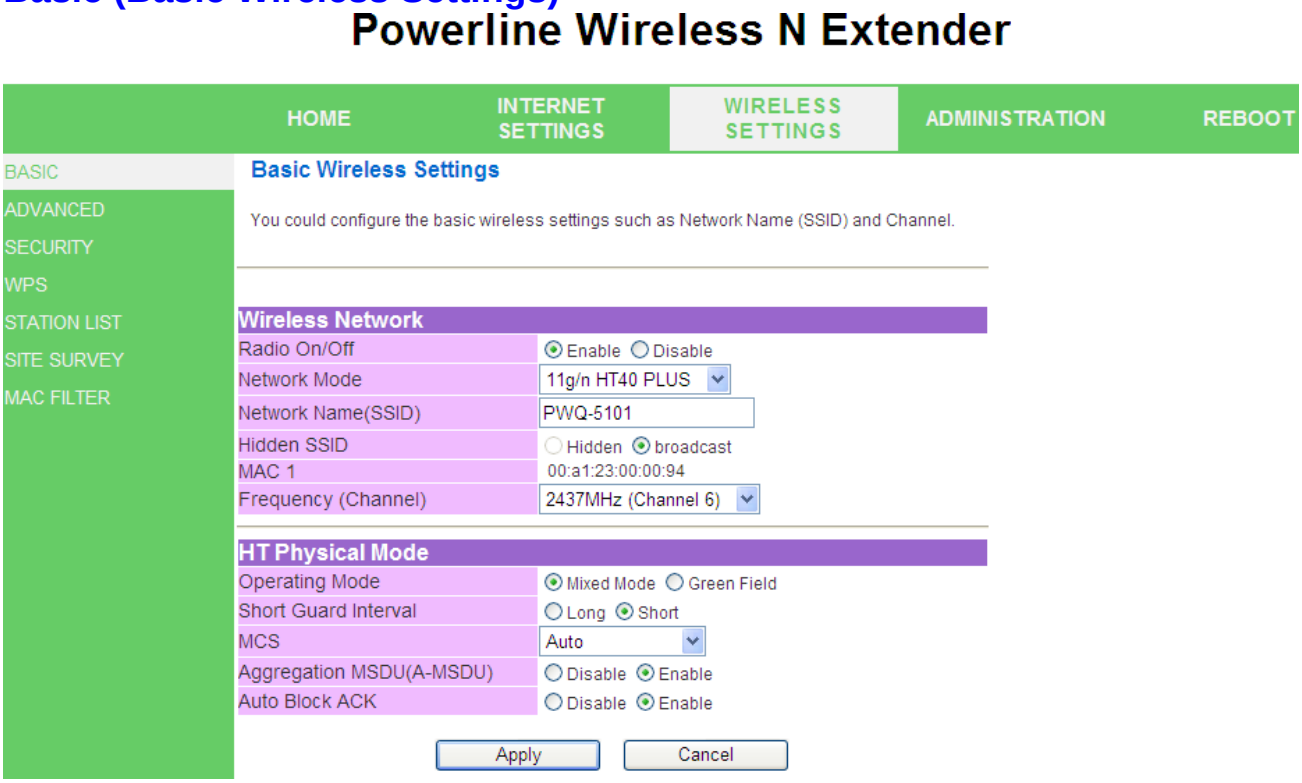
QoS	
Item	**Description**
IGMP command packet (join, leave..)	recommend to set the highest priority (3) to keep it work smoothly
IGMP Stream	recommend to set the higher priority (2) to make sure the good streaming video and audio quality
Unicast	recommend to set priority 1
Multicast/Broadcast	recommend to set priority 1
IGMP Reports To Non-Querier Host	default disable but recommend to turn on this function while using BVH-5101 in China
IGMP Snooping	default and also recommend to enable IGMP snooping

DHCP Clients

When DHCP server enable, you can monitor DHCP clients here.



Basic (Basic Wireless Settings)

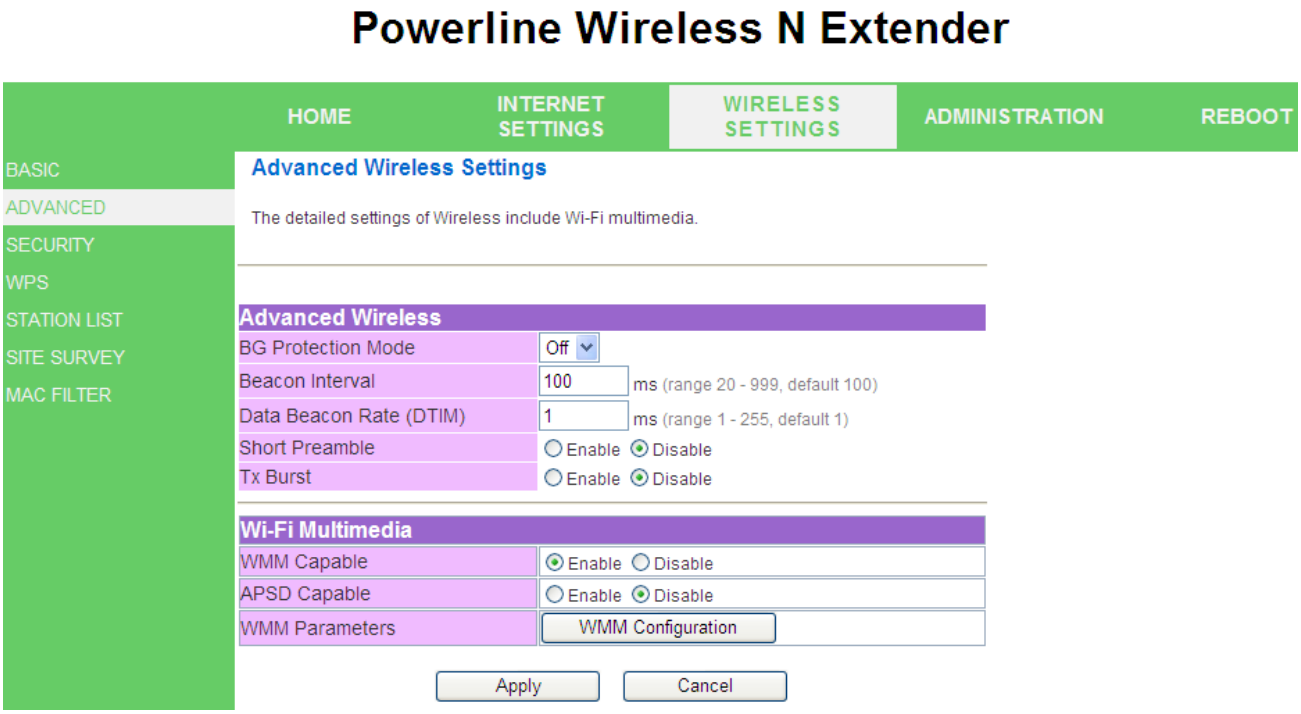


Wireless Network	
Item	**Description**
Radio On/Off	Click to enable/disable wireless function.
Network Mode	The available options are 11b, 11g, 11g/n HT20, 11g/n HT40 PLUS (default), 11 g/n HT40 MINUS
Network Name (SSID)	The SSID, which is also called ESSID is a unique identifier that wireless networking devices use in order to establish and maintain wireless connectivity. SSID can contain up to 32 alphanumeric characters.
Hidden SSID	Click to enable/disable, With hidden SSID, the AP can't be scanned and the wireless client must input SSID manually to associate this AP.
BSSID	The BSSID is displayed in this field.
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.

Advanced (Advance Wireless Settings)

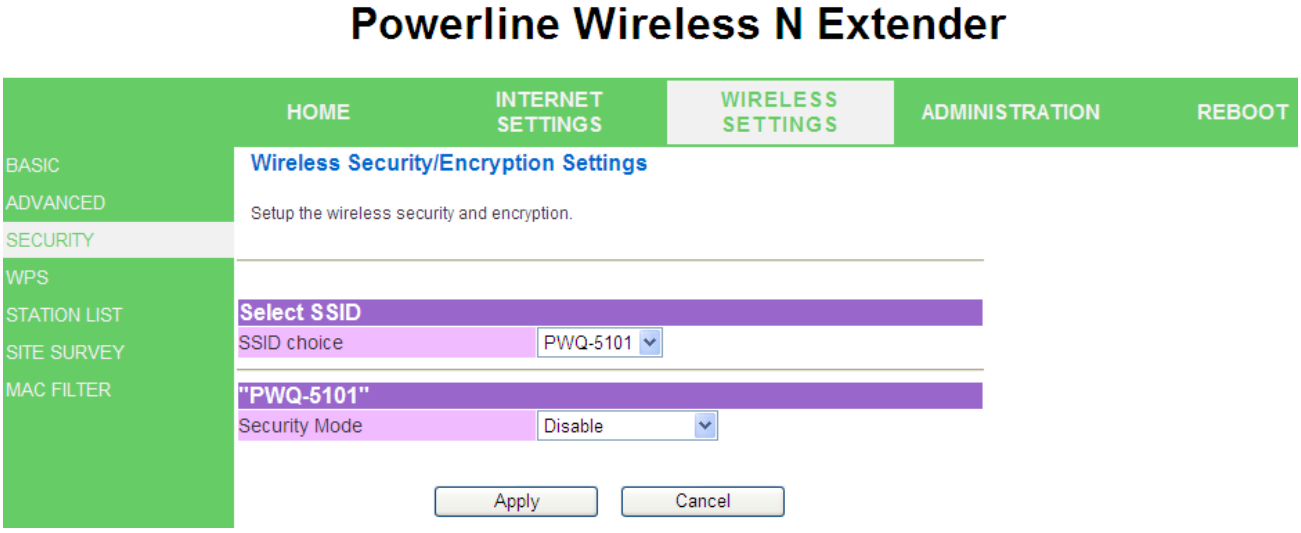


Advanced Wireless	
Item	**Description**
BG Protection Mode	You can select the other options including On and Off. The B/G protection technology is CTS-To-Self. It will try to reserve the throughput for 11g clients from 11b clients connecting to the device as AP mode.

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.

Security (Wireless Security/Encryption Settings)



The default SSID and Wi-Fi key

Wireless Security/Encryption Settings	
Item	**Description**
Security Mode	Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2 PSK, WPA/WPA2, 802.1X.

Security Mode: Choose one as the wireless authentication among the following types: Open, Shared, WEP Auto, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA/WPA2-PSK, WPA/WPA2, and 802.1 X.

- Encryption Type: Select one for the encryption type. The options vary depending on the Authentication mode. The corresponding options shows below.

Authentication	**Encryption type**	**Key option**
Open/Shared/WEP Auto	WEP	Default Key ID, Key content of Key 1/2/3/4
WPA/WPA2-PSK (Pre-Shared Key)	TKIP, AES, TKIP/AES	Pass Phrase (8-32 bytes), Key Renewal Interval
WPA/WPA2 Enterprise	TKIP, AES, TKIP/AES	Radius Server Network/Address/Port/Key/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 as same as each client in your wireless network.

- Authentication Type: Open, Shared and Auto. When choose “Open” or “Shared”, all of the clients must select the same authentication to associate this AP. If select “WEP Auto”, the clients don’t have to use the same “Open” or “Shared” authentication. They can choose any one to authenticate.
- Default Key ID: Select the Key ID as the default Key.
- Key 1/2/3/4: Select “ASCII” or “Hex” and then type the key in the text field. It will check whether the number of characters meet 10 or 26. If not, an error message is shown.
  - 64-bit WEP Encryption：64-bit WEP keys are as same as the encryption method of 40-bit WEP. When input 10 hexadecimal digits (0-9, a-f or A-F) or 5 ACSII chars as the key, it is using 64-bit WEP encryption.
  - 128-bit WEP Encryption：128-bit WEP keys are as same as the encryption method of 104-bit WEP. When input 26 hexadecimal digits (0-9, a-f or A-F) or 10 ACSII chars, it is using 128-bit WEP encryption.

WPA Authentication Mode

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-PSK:**
  - Pass Phrase:

  Option: Pass Phrase (8-32bytes). This mode requires only an access point and client station that supports WPA-PSK. The WPA-PSK settings include Key Format, Length and Value. They must be as same as each wireless client in your wireless network. When Key format is Passphrase, the key value should have 8-63 ACSII chars.
  - Key Renewal Interval:

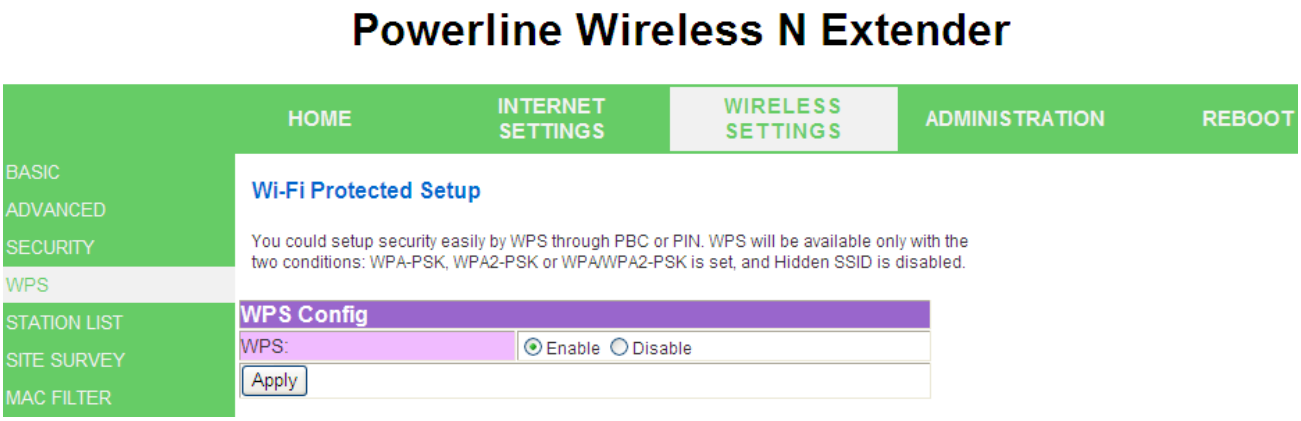
  The WPA Algorithm will regroup the key for a period. The default value is 3600 seconds and you can adjust the time interval.

- **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 Server Network, Server address, Server Port and Server Key of the target RADIUS server.

  - WPA Algorithms: TKIP, AES, TKIP/AES. Select the encryption type. When selecting TKIP/AES, the client can use whether TKIP or AES for the authentication.
  - Pre-Authentication Support option: This option only appears when selecting WPA2 or WPA/WPA2 as the authentication mode. Enable it to use this function.
- **Radius Server Setting:**
  - IP Address: Input the IP Address of the Radius server.
  - Port: Input the port of the Radius server. The default port is 1812.
  - Shared Secret: Input the Authentication Key.
  - Session Timeout: Input the maximum idle time for this connection.

WPS (Wi-Fi Protected Setup)



This function helps to establish the Wi-Fi security. For AP mode, it can be setup one WPS method including PIN (Personal Identification Number) and PBC (Push Button Certification).
To begin the WPS progress, the WLAN security must be setup first. Please setup one among WPAPSK, WPA2PSK, WPA/WPA2PSK and then apply WPS setting. WPS will only be available in these encryption types.

PIN: query the PIN code in the utility of the WLAN client connecting to this AP, and then enter it in the PIN field. The Wi-Fi link between the WLAN client and the device should be encrypted.

PBC: Select PBC, and then you can begin the PBC process. Press the PBC button in the front panel can also trigger this process. Press or click the PBC button on the WLAN client to finish the communication. You can press the PBC button on the WLAN client first and then click the PBC button on this device to establish the encryption.

The options and the information fields are showed below.

WPS Config	
Item	**Description**
WPS Capable	Select enable then press Apply button to start this function.

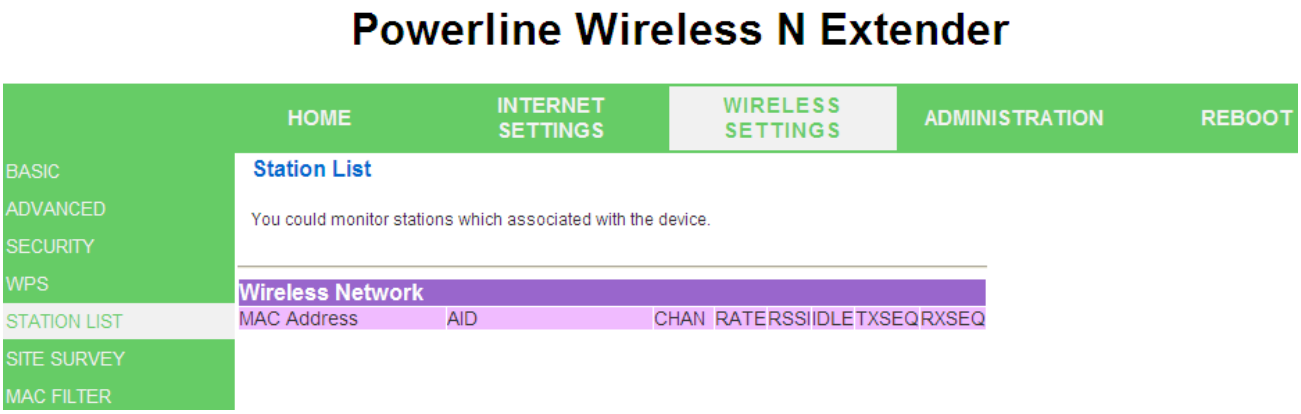
NOTE：WPS will be available only with the two conditions:

1、WPA-PSK, WPA2-PSK or WPA/WPA2-PSK is set

2、Hidden SSID is disabled.

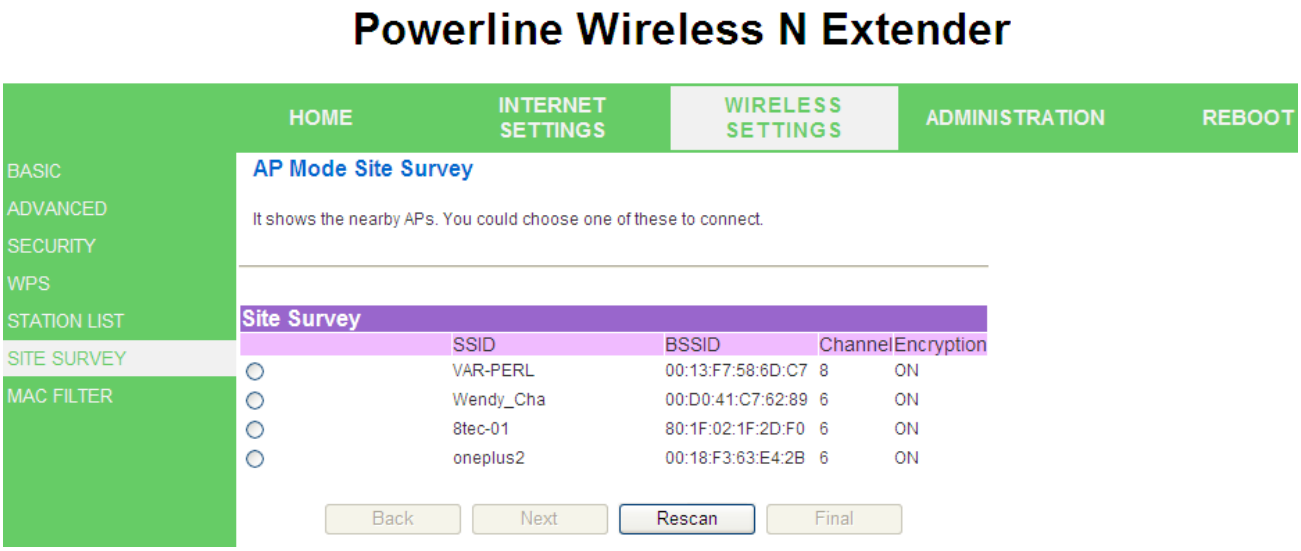
Station List

In the Station list, the information of associated clients is displayed.



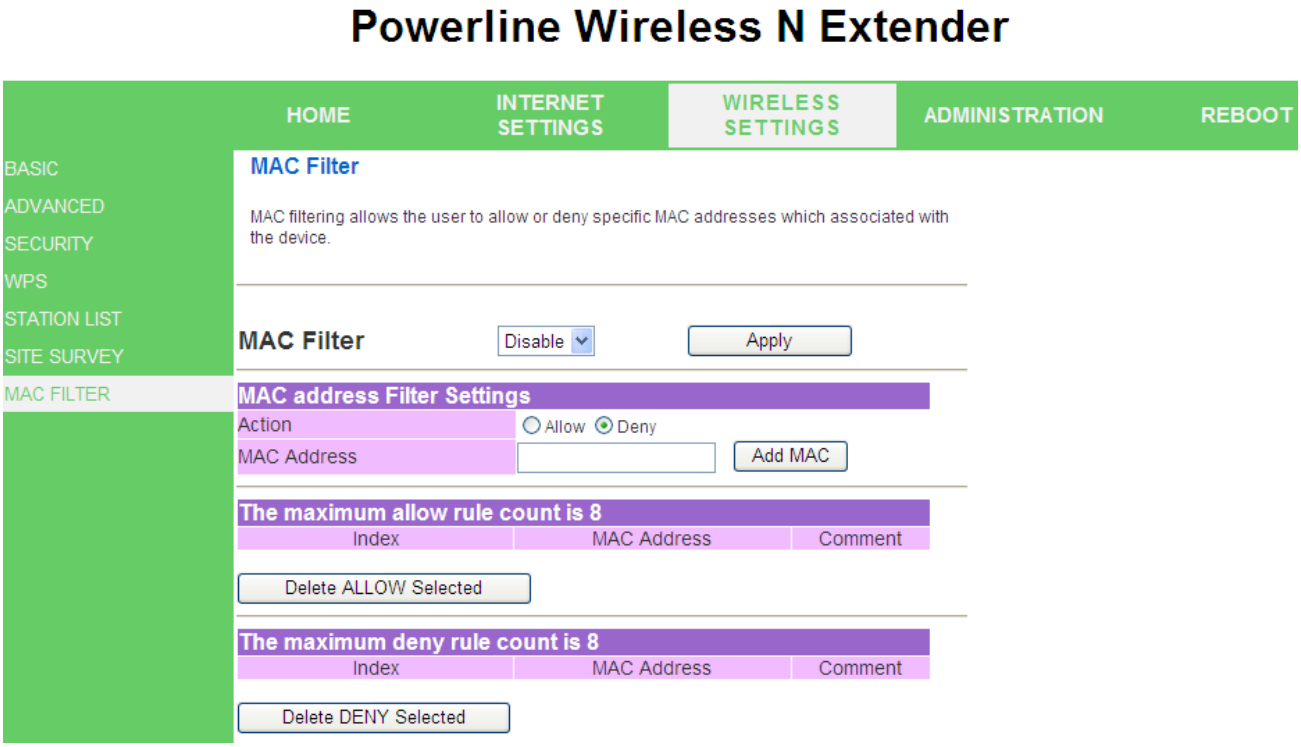
Site Survey (AP Mode Site Survey)

Site survey shows information of APs nearby; you may choose one of these APs connecting.



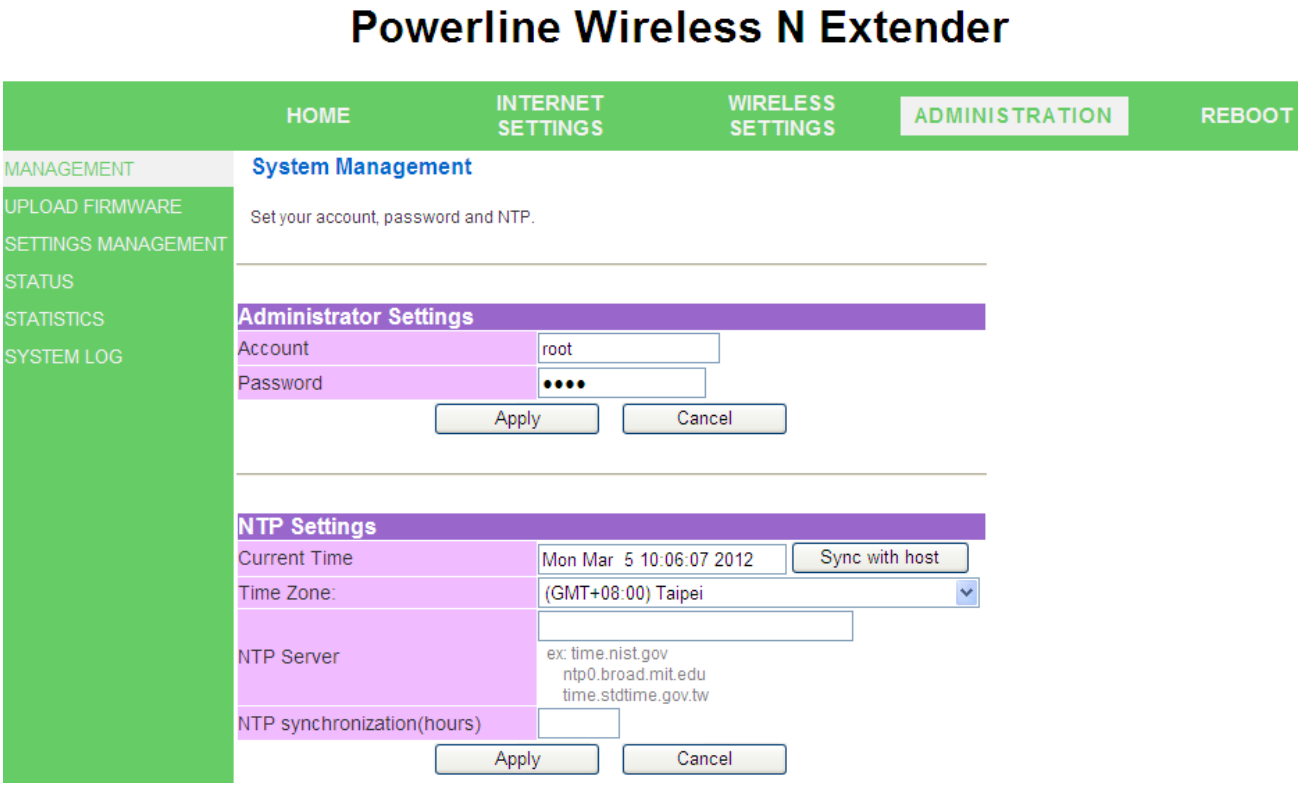
MAC Filter

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.



Administration

Management (System Management)

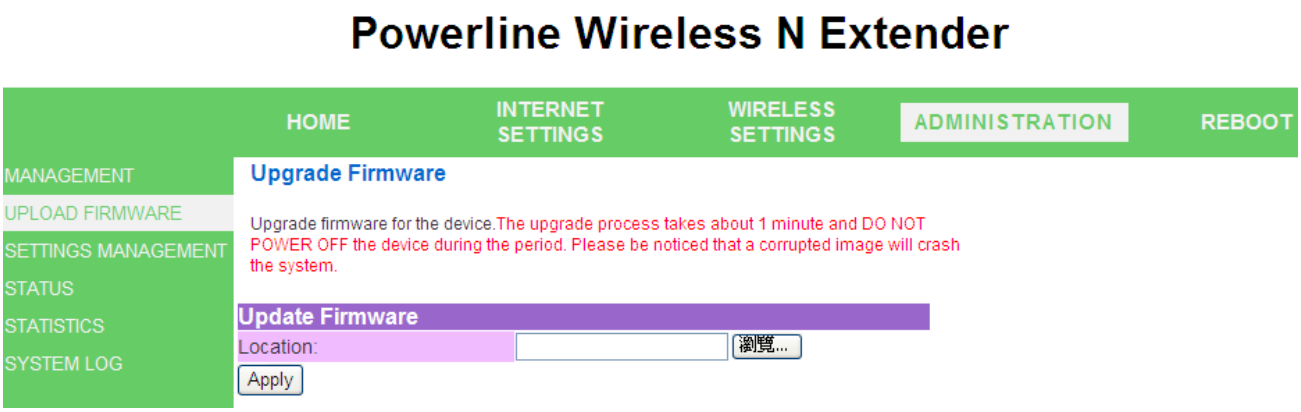


Administrator Settings	
Item	**Description**
Account	Enter the name for login. The default name is “root”.
Password	Enter the password for login. The default password is “root”.

NTP Settings	
Item	**Description**
Sync with host	Synchronizing current time with your PC
Time Zone	Select local time zone.
NTP server	Input the NTP server address. If you are not sure about the local NTP server address, you can input pool.ntp.org.
NTP Synchronization	This is the time interval of NTP synchronization. The range is 1-300 hours. It is the necessary field for NTP setting and please input it to apply.

Upgrade Firmware

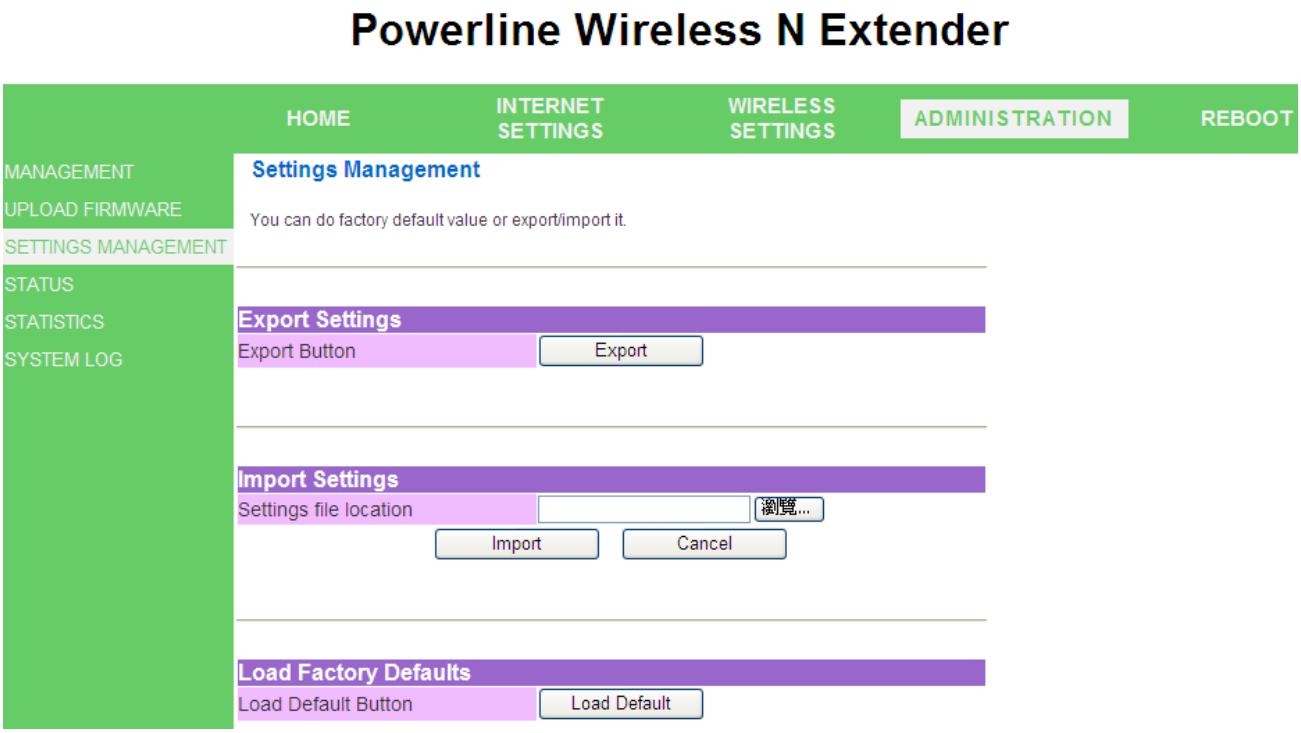
This page provides the firmware upgrade function.



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 this period. In order to continue configuration, please refresh the PC web-browser to reflect new upgraded FW settings.

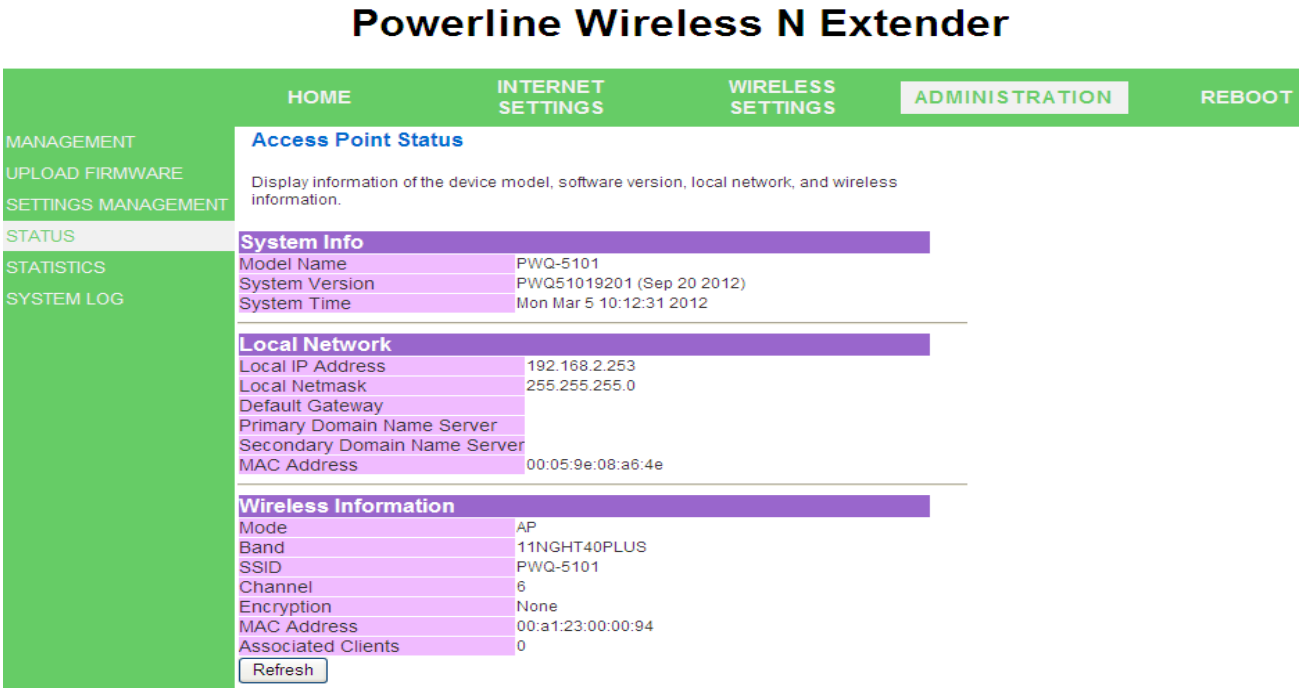
Settings Management

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

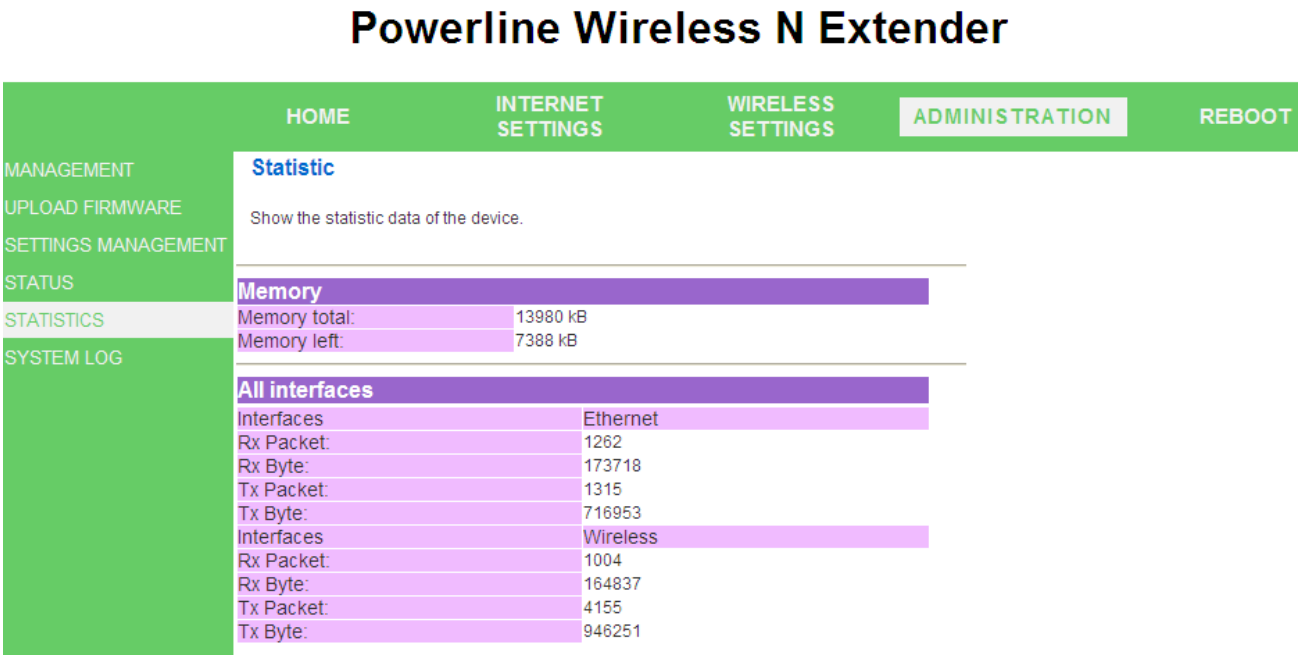


Status

The page shows system status information.



Statistics



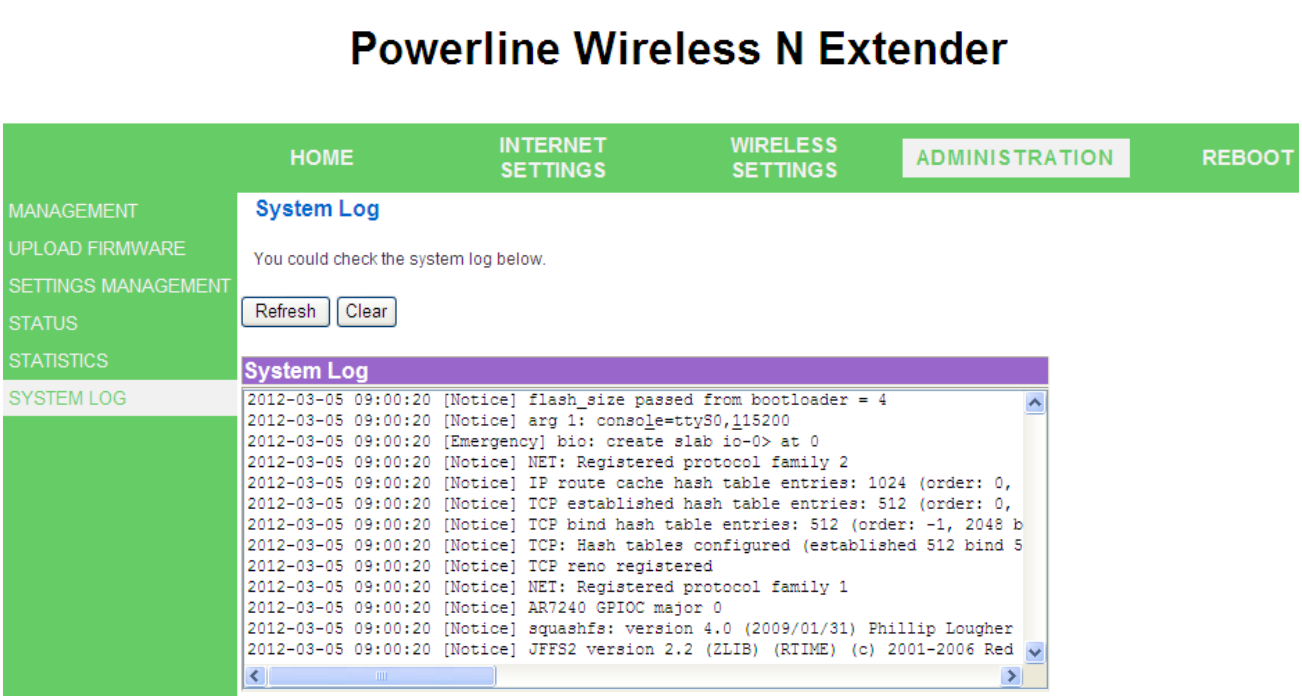
Administrator Settings	
Item	**Description**
Memory total	This is the total memory size for this device.
Memory left	The available memory size shows in this field.

All interfaces

The information likes “Rx Packet”, “Rx Byte”, “Tx Packet” and “Tx Byte” shows the status of all interface including “Ethernet and Wireless”.

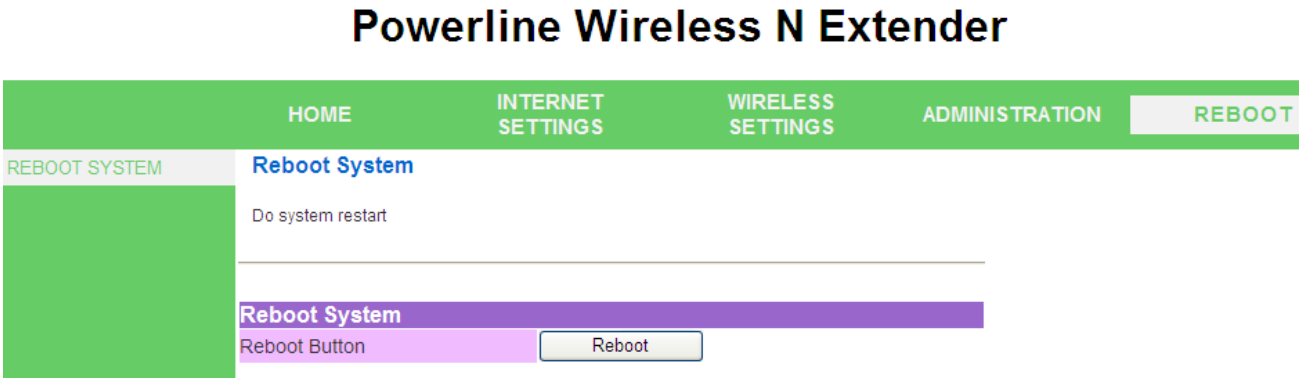
System Log

The system log shows 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.



Reboot

Reboot System



Channel Number

The following table is 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.

***FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of 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 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:

-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.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

Labeling Requirements

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.

RF Exposure Warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions. (antennas are greater than 20cm from a person's body).

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.
Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

Informations Concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l’appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l’appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.

Ce périphérique a également été évalué et démontré conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition à des appareils mobiles (les antennes se situent à moins de 20 cm du corps d'une personne).

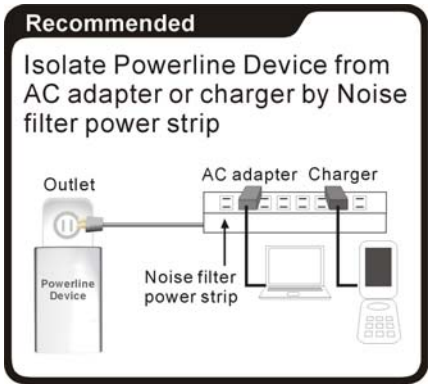
Ch 4 Enhance PLC Performance During Installation

This Powerline device sends data to remote device using WLAN or PLC technology. When it sends data to another remote Powerline device over the existing electrical wiring in your home, it may be affected by noises on the electric wire or the length of the wiring between transmitting and receiving devices. Keep the following in mind when placing this Powerline device at home.

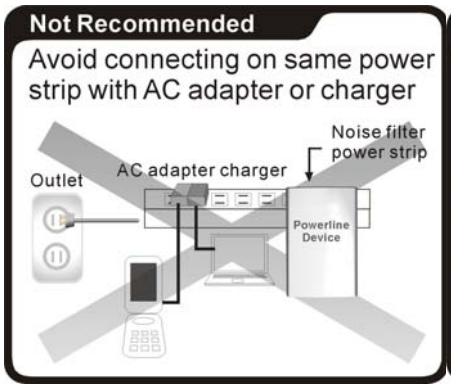
AC Outlets Connection

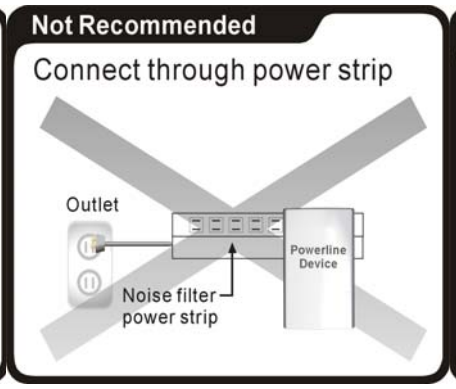
Avoid connecting this device to an uninterruptible power supply (UPS) or backup power supply device. For best results, we recommend connecting the adaptors directly to a wall outlet. Avoid connecting high power-consumption appliances to the same wall outlet. Plug these power consuming devices onto a noise filtering power strip to prevent these device interfere with this Powerline device. See the following illustration figure:

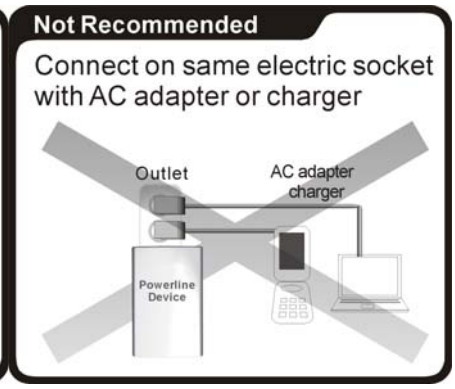
For better performance, the following connection is recommended, although not isolate with Noise filter power strip will still work OK.



The following connections are **NOT** recommended, although current PLC technology will overcome most noise interference from electronic devices' AC adapters or chargers.







Connection via Power Strip

If you must connect this device to a power strip, please keep the following recommendation in mind:

• Make sure the power strip does not have a noise filter or a surge protector, as these features may impair communication signaling of the Powerline device sent over the electric wiring, and its throughput or distance will be degraded.

• Use a power strip with an AC cord that is as short as possible.

• Do not connect the adaptor to a power strip that receives power from another power strip.

Electrical Interference

Certain electrical devices emit electrical noise. If this noise is spread over to the electrical wiring in your home, it may interfere with the performance, speed, and reliability of this device. For best results, we recommend connecting an electrical noise filter to noise emitting appliances.

The following appliances are more likely to produce noise:

- Battery chargers (including cell phone chargers)
- Hair dryers
- Power drills
- Halogen light
- vacuum cleaner

Additionally, this product may interfere with the following appliance:

- Lights or lamps which have a touch-sensitive on/off feature

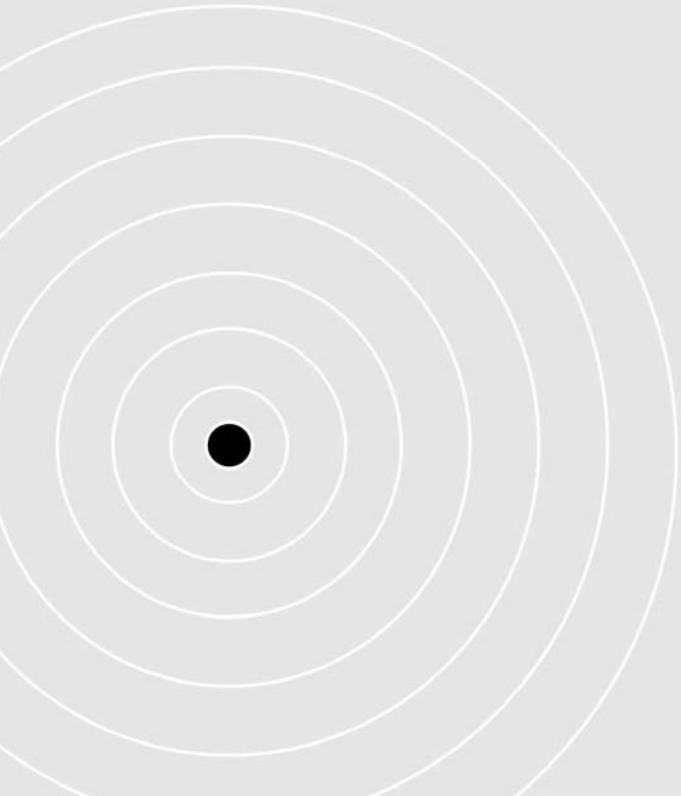
Electrical Wiring

This device sends data to and from each other over the existing electrical wiring of your house. If two wall outlets are separated by a great distance of electrical wiring, these devices may not communicate well with each other. For more information, refer to the troubleshooting section.

Ch 5 Specifications

Powerline Wireless N Extender	
Standards	WLAN: IEEE 802.11 b/g, IEEE 802.11n
	LAN: IEEE 802.3, IEEE 802.3u
	Powerline: HomePlug AV 1.0
Maximum Throughput	WLAN to Ethernet: up to 93 Mbps (Under 802.11n 40MHz)
	Powerline to Ethernet: TCP: 92 Mbps
Frequency band	WLAN: 2.4~2.4835GHz
	PLC: 2~ 68MHz
WLAN transceiver spec	RF Power:
	802.11b TX: 16 dBm +/- 1.5dB (typ.)@1Mbps
	802.11g TX : 16 dBm +/- 1.5dB (typ.)@6Mbps
	802.11n TX : 14 dBm +/- 1.5dB (typ.)@6.5Mbps 802.11n TX : 13 dBm +/- 1.5dB (typ.)@13.5Mbps
	Sensitivity:
	802.11b RX: -82 dBm(typ.)@11Mbps
	802.11g RX: -70 dBm(typ.)@54Mbps
	802.11n RX(20MHz): -67dBm(typ.)@ 72.2Mbps
	802.11n RX(40MHz): -64dBm(typ.)@ 150Mbps
	Physical Data Rate:
	802.11b: 1,2, 5.5, 11Mbps
	802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
	802.11n (20MHz): MCS0~7, Up to 72.2Mbps
	802.11n (40MHz): MCS0~7, Up to 150Mbps
Wi-Fi mode	Wireless AP+ Bridge mode (Default)
Security mode	WLAN WPS PBC / PIN code, WPA-PSK, and WPA2-PSK
	PLC 128-bit AES
Antenna type	1T1R
LAN port	1 port
AC input	100 - 240 V 50-60Hz

Power consumption	(Note: Ethernet and Wi-Fi is connected and running)
LEDs	POWER LED (Green);
	PLC Link/Activity LED (Green);
	Wireless & Security LED (dual color);
	Ethernet (Green)
Buttons	WPS
	GROUP/Pairing
	Power on/off
	RESET
PLC PHY Rate	500 Mbps
PLC Modulation	OFDM (QAM 8/16/64/256/1024/4096, BPSK, QPSK, ROBO)
PLC Distance	AC Wire : up to 300 meters
Max. dev in a PLC network Group	8/16 (Active/Total)
Temperature	Operating: 0~40 ℃; Storage: -20~60 ℃
Relative Humidity	Operating: 10~85% Non-Condensing , Storage: 5~90% Non-Condensing
Dimension	56 x 105 x 48(H) mm
Certification	FCC, CE, CE-LVD, RoHS, WEEE



IB04380599 Rev.0