# PLC Wireless Extender User Manual V1.0



### Contents

Abou	ut Use	r Manua	۱	1		
Orga	anizati	on		1		
1	Over	rview				
2	Hardware Description					
	2.1	2.1 LED Status				
	2.2	Interf	ace Description	7		
		2.2.1	The Ethernet Interface	7		
		2.2.2	The Adapter's Buttons	8		
	2.3	Hard	ware Installation	9		
		2.3.1	System Requirements	9		
		2.3.2	Before You Begin	9		
	2.4	Operation Range				
	2.5	How to Improve the Transmission Capacity10				
	2.6	2.6 Wireless Roaming				
3	Wireless Network Configuration					
	3.1	3.1 TCP/IP Settings				
	3.2 Log In to the Web Page					
4	Web Configuration					
	4.1	Interr	net Settings			
		4.1.1	LAN			
		4.1.2	DHCP Clients			
	4.2	Wirel	less Settings			
		4.2.1	Basic			
		4.2.2	Advanced			
		4.2.3	Security			
		4.2.4	WPS			
		4.2.5	Station List			
	4.3	Admi	nistration			
		4.3.1	Management	51		
		4.3.2	Upload Firmware	53		
		4.3.3	Settings Management	53		

	4	4.3.4	Status	54
	4	4.3.5	Statistic	55
	4	4.3.6	System Command	56
	4	4.3.7	System Log	57
5	Install	the Pov	verLine Utility	59
6	How to	o Use T	he Utility Software	61
	6.1	Main <sup>-</sup>	Tab	61
	6.2	Privac	cy Tab	63
	6.3	Diagn	ostics Tab	64
	6.4	About	Tab	66
7	How to	o use th	e NMK Pushbutton	67
	7.1	Formi	ng a HomePlug AV logical network	67
	7.2	Joinin	g a Network	68
	7.3	Leavir	ng a Network	68
8	About PowerLine QoS			70
9	Parameter and Specification71			71

# **About User Manual**

This user manual mainly describes how to install and configure the NL-HPW200 wireless extender.

# Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1 : Overview	Provides a general overview of the NL-HPW200
	wireless router, and the package list.
Chapter 2 : Hardware	Mainly describes the front panel and the rear
Description	panel of the NL-HPW200 and the procedure for
	hardware installation.
Chapter 3: Wireless	Describes how to configure network settings of
Network Configuration	your PC, then connect to the NL-HPW200.
Chapter 4 : Web	Mainly describes how to navigate through the
Configuration	Web pages and how to configure the
	parameters.
Chapter 5 : Install the	Introduce installation of the PowerLine Utility
PowerLine Utility	
Chapter 6 : How to use the	Describes how to view the PowerLine
Utility Software	parameter, modify NMK, device name
Chapter7 : How to use the	Introduce how to form, join and leave a
NMK pushbutton	HomePlug AV local network
Chapter8 : About PowerLine	Introduce how to setup the QoS parameter in
QoS	PowerLine function
Chapter9 : Parameter and	Introduce the product system specification
Specification	

# Features

# **PowerLine Feature**

- Power supply range of 100 ~ 240VAC 50/60Hz
- Comply with HomePlug AV, and Co-existence with HomePlug 1.0 Nodes
- PowerLine phy rate up to 200 Mbps
- Support QAM 1024/256/64/16/8, QPSK, BPSK, and ROBO modulation schemes
- 128-bit AES Link Encryption with key management for secure power line communications
- Windowed OFDM with noise mitigation based on patented line synchronization techniques improves data integrity in noisy conditions
- Dynamic channel adaptation and channel estimation maximizes throughput in harsh channel conditions
- Priority-based CSMA/CA channel access schemes maximize efficiency and throughput
- Integrated Quality of Service (QoS) Enhancements: contention-free access, four-level priority based contention access, and multi segment bursting
- ToS and CoS Packet Classifiers
- Supports IGMP managed multicast sessions

# **Wireless Feature**

- Support IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i, and IEEE802.11e
- Support 1T1R mode and transmission data rate is up to 150 Mbps
- Support WEP and WPA for data transmission security
- Support DHCP Server and Client
- Support firmware version upgrade via Web page
- Support restoring factory default settings
- Support wireless security authentication modes, including OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA1WPA2, and 802.1X.

- Support system status display
- Support cross-over cable detection and also support auto modification and polarity modification
- Support system log

# 1 Overview

Thank you for choosing NL-HPW200.

NL-HPW200 (also called PLC Wireless Extender) is fully compatible with HomePlugAV, and can co-exist with HomePlug 1.0. Meanwhile, it is also compatible with 802.11b/g/n standards. NL-HPW200 supports CCK and OFDM and its PowerLine phy rate is up to 200Mbps, wireless phy rate is up to 150 Mbps under 11n mode.

NL-HPW200 provides 128-bit AES encryption in PowerLine communication, 64-bit and 128-bit WEP encryption, WPA encryption in wireless communication, associating with IEEE 802.1X authentication, which insures the security of wireless communication.

# Package list

Please check whether your package list includes the following items:

- NL-HPW200 x 1
- CD-ROM x 1
- RJ45 x 1
- Quid installation Guide x 1

# **Security Notes**

This device is intended for connection to the AC power line. For installation instructions, please refer to the installation section of this guide. The following precautions should be taken when using this product.

- Read all instructions before installing and operating this product.
- Follow all warnings and instructions marked on the product.
- Unplug the device from the wall outlet before cleaning. Use a damp 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.
- Do not use an extension cord between the device and the AC power source.
- 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 device from the wall outlet and refer the product to qualified service personnel for the following conditions:
  - 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 Hardware Description

# 2.1 LED Status

There are 5 LED indicators on the front panel of NL-HPW200. By observing their status, you can judge whether the device runs normally.



LED Indicator	Color	Status	Description
PWR	Red	On	Power is on.
	Green	On	The device runs normally.
	-	Off	Power is off or the device is down.
WLAN	Green	On	Radio switch is turned on.
	Green	Blink	Data is being transmitted.
	-	Off	Radio switch is shut off.
WPS	Green	On	Connection succeeds under Wi-Fi Protected
			Setup.
	Green	Blink	Negotiation is in progress under Wi-Fi
			Protected Setup.
	-	Off	Wi-Fi Protected Setup is disabled.
PLC	Green	On/Blink	When PLC rate > 100Mbps, see note 1
	Orange	On/Blink	When PLC rate in 80-100Mbps, see note 1
	Red	On/Blink	When PLC rate < 100Mbps, see note 1
LAN	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No LAN connection.

The following table describes the status of LED indicators on the front panel.

Note: The PLC LED indicator turns "ON" when powerline link is detected. If the device is serving as a STATION, the LED indicator will blink to indicate transmit or receive powerline activity. If the device is serving as a CCO, the LED indicator will light steadily ON, even in the presence of powerline activity

# 2.2 Interface Description

### 2.2.1 The Ethernet Interface

Ethernet : The Ethernet port connects to an Ethernet network cable. The other end of the cable will connect to

your computer or other Ethernet-enabled network device.

### 2.2.2 The Adapter's Buttons

RST:	The RST button can restore the factory defaults.
NMK:	The button is used to synchronous the private
	network name.
WPS:	This button is used for enabling WPS PBC mode.
	If WPS is enabled, press this button, and then the
	extender starts to accept the negotiation of PBC
	mode

Note: Do not press the Reset button unless you want to clear the current settings. The Reset button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the Reset button gently for 3 seconds with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

# 2.3 Hardware Installation

### 2.3.1 System Requirements

Before installing the device, please make sure that the following items are ready.

- At least one Ethernet RJ45 cable (10Base-T/100Base-T)
- One NL-HPW200
- One PLC device for PowerLine communication
- A PC has been installed PCP/IP protocol and it can access the Internet.

### 2.3.2 Before You Begin

Before you install the device, please pay attention to the following items:

- When connecting the device to a computer, a hub, a router or a switch, the Ethernet cable should be less than 100 meters.
- Do not place this device on an unstable surface or support. Do not put this device on the ground.
- Keep the device clean. Avoid the device from direct sunshine. Avoid any metal in the device.
- Place the device in the center of the area, and try to optimize the wireless coverage.
- Install Powerline Utility when you want to see the quality of PLC communication

# 2.4 Operation Range

The operation range of NL-HPW200 depends on the actual environment. When the device is placed in the house or in the office, the overall arrangements are different. So the path and effect for signal transmission are different. For PLC network the typical coverage Up to 5000 square foot, but the actual Coverage will vary with the power grid and the number of PLC terminal device. For wireless, the outdoor straight transmission distance for some devices in the open air is up to 300 meters, and the indoor straight transmission distance is up to 100 meters.

# 2.5 How to Improve the Transmission Capacity

It is important to use the PLC product complying with the following "correct rules", because it can significantly improve the transmission capacity of the network.

For the PLC device no female socket, it is recommended to plug the device directly into a wall socket, not to power stripe.



Note: Please don't plug the device in horizontal.

# 2.6 Wireless Roaming

Suppose that one NL-HPW200 and several APs run in the same network. The NL-HPW200 or AP acts as one BSS, and has its coverage range. One wireless client terminal (e.g. notebook PC or PDA), can realize roaming from one AP to another AP correctly. In that case, the wireless client terminal can communicate with the other devices within the NL-HPW200 and APs' coverage.

In order to realize the wireless client roaming among different APs, you need to set the NL-HPW200 and APs properly. Do as follows:

- Set the same SSID for NL-HPW200 and all APs.
- The SSIDs of all the computers and PDAs should be consistent with the APs.
- All the BSSs must use the same wireless channel.
- If the encryption function is enabled, all the NL-HPW200 and APs should configure the same encryption mode and the encryption key for establishing connection.
- The NL-HPW200 and APs must keep the wireless signal covering the whole operation environment and the wireless signal should be continuous. Please put the APs to the appropriate places for a better network coverage.

# 3 Wireless Network Configuration

Web management tool allows you to configure wireless function of NL-HPW200, but not PLC function, the PLC function should install the PowerLine Utility to configure and will introduce in back chapter. The web management only for wireless function, the recommended browser is IE 5.0 or above.

The following sections describe how to set the Internet connection, local Ethernet connection, and wireless connection, and how to access the Web page of the NL-HPW200.

# 3.1 TCP/IP Settings

By default, the IP address of LAN interface of the NL-HPW200 is 192.168.1.1.The subnet mask is 255.255.255.0. The DHCP Server is enabled.

It is recommended you set the network adapter to be **Obtain an IP address automatically**. Your PC acquires IP address, subnet mask, gateway, and DNS address automatically via the extender. If you know the setting of the current LAN interface, you can manually set the TCP/IP properties of the network adapter, so that your PC can communicate with the extender.

You may manually set the network adapter by following the steps below:

Step 1 Right click the icon of **My Network Places** (e.g., Windows XP) and select **Properties** in the menu. The **Network Connections** page appears.



Step 2 Right click the network adapter icon and select **Properties** in the menu. The Local Area Connections Properties appears. (Note: If there are several

network cards on your PC, it may not display the **Local Area Connections Properties** page. It may display other dialog boxes.)



Step 3 Double click the Internet Protocol (TCP/IP) to display the Internet Protocol (TCP/IP) Properties page.



Step 4 Select **Use the following IP address** and enter the IP address of the network adapter. The IP address should belong to the IP network segment 192.168. 1.X (X is a number between 2 and 254).

r'ou can get IP settings assigned this capability. Otherwise, you ne the appropriate IP settings.	l automatically if your network supports ed to ask your network administrator for
O Obtain an IP address auton	natically
Use the following IP address	: London Longitud
JP address:	192.168.1.123
Sybnet mask:	255.255.255.0
Default gateway:	192.168.1.1
O Obtain DNS server address	automatically
Use the following DNS server	er addresses:
Preferred DNS server:	2 K K
Alternate DNS server:	<u> </u>
	Advanced

NL-HPW200 User Manual

- Step 5 Set the subnet mask and then click the OK button to finish manual setting.
- Step 6 After finishing setting, you may ping the default IP address of the the extender, to check whether the current connection between PC and the extender is normal. Click RUN... in the lower left corner on the desktop, and then enter ping 192.168.1.1 in the dialog box. See the following figure:



Note: 192.168.1.1 is the default IP address of the LAN interface. If this IP address is changed and you need to ping the IP address of the extender, you should enter the current IP address in the dialog box above.

Step 7 If PC can ping through the default IP address of the extender and the following page appears, it indicates that the connection between PC and AP is normal.



# 3.2 Log In to the Web Page

Open the browser, and enter the http://192.168.1.1/in the IE address bar.



Enter the user name (*admin*, by default) and the password (*admin.* by default) on the login page.

Connect to 192.168.1.1		
	GP	
GoAhead		
User name:	🖸 admin 🛛 🔽	
Password:	•••••	
	Remember my password	
	OK Cancel	

After clicking the OK button on the login page, you can log in to the Web page of the NL-HPW200.

# 4 Web Configuration

# 4.1 Internet Settings

The following figure shows the navigation menu of the Internet Settings:



The sub-menus of the Internet Settings include LAN, and DHCP clients.

### 4.1.1 LAN

Click Internet Settings --> LAN to display Local Area Network (LAN) Settings page.

#### <u>open all</u> <u>close all</u>

#### Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup			
IP Address	192.168.1.1		
Subnet Mask	255.255.255.0		
LAN 2	C Enable 💿 Disable		
LAN2 IP Address			
LAN2 Subnet Mask			
MAC Address	00:0C:43:30:52:77		
DHCP Type	Server 💌		
Start IP Address	192.168.1.100		
End IP Address	192.168.1.200		
Subnet Mask	255.255.255.0		
Primary DNS Server	192.168.1.1		
Secondary DNS Server	192.168.1.1		
Default Gateway	192.168.1.1		
Lease Time	86400		
Statically Assigned	MAC:		
Statically Assigned	MAC:		
Statically Assigned	MAC:		
802.1d Spanning Tree	Disable 💌		
LLTD	Disable 💌		
IGMP Proxy	Disable 💌		
UPNP	Disable 💌		
App	Apply Cancel		

This page is used to configure the LAN parameters. This page allows you to configure LAN interface properties, DHCP server properties, and other parameters related to LAN.

The parameters on this page are described as follows:

Field	Description			
IP Address	The IP address of LAN interface. The default IP address is			
	192.168.1.1.			
Subnet Mask	The subnet mask of the IP address of the LAN interface.			
	The default subnet mask is 255.255.255.0.			
LAN 2	Enable or disable the second IP address of the LAN			
	interface. The default setting is <b>Disable</b> .			
LAN 2 IP	The second IP address of the LAN interface. This IP			
Address	address should not collide with the IP address of the			
	interior network.			
LAN 2 Subnet	The subnet mask of the second IP address of the LAN			
Mask	interface.			
MAC Address	Display the current MAC address that LAN interface uses.			
DHCP Type	Enable or disable DHCP service. The default setting is			
	Server, it indicates DHCP service is enabled.			
	After enabling DHCP service, you can configure the			
	following parameters of the DHCP server:			
	<ul> <li>Start IP Address: The start IP address of the DHCP</li> </ul>			
	address pool.			
	<ul> <li>End IP Address: The end IP address of the DHCP</li> </ul>			
	address pool.			
	<ul> <li>Subnet Mask: The subnet mask that DHCP server</li> </ul>			
	assigns.			
	<ul> <li>Primary DNS Server: The primary DNS server that</li> </ul>			
	DHCP server assigns.			
	<ul> <li>Secondary DNS Server: The secondary DNS server</li> </ul>			
	that DHCP server assigns.			
	<ul> <li>Default Gateway: The gateway that DHCP server</li> </ul>			
	assigns.			
	• Lease Time: The lease time of the IP address.			
	<ul> <li>Statically Assigned: For binding MAC and IP.</li> </ul>			
802.1d	It can provide redundant link and prevent network from			

#### NL-HPW200 User Manual

Field	Description
Spanning Tree	generating loop. You may select Enable or Disable.
LLTD	After enabling LLTD (Link Layer Topology Discovery),
	Windows Vista automatically discovers other devices's link
	topology, and these devices are also compatible with
	LLTD. You may select Enable or Disable.
IGMP Proxy	Enable or disable IGMP Proxy.
IGMP Snooping	Enable or disable IGMP Snooping. After enabling this
	function, the packets of the IGMP broadcast will not sent
	to the LAN interface that does not belong to that group.
UPNP	Enable or disable the UPnP function. After enabling this
	function, AP will provide automatic port-mapping for P2P
	software on the interior network.

### 4.1.2 DHCP Clients

Click Internet Settings --> DHCP Clients to display the DHCP Client List page.

TaW TaW LAN HCP Clients Comparison	You could monitor DHCP clients here.				
	DHCP Clients				
	MAC Address	IP Address	Expires in		
	00:1C:25:93:DB:4A	192.168.1.100	21:11:06		
	00:16:6F:48:97:45	192.168.1.101	21:30:24		

On this page, you can view the clients's information assigned by the DHCP server, including the MAC address, the IP address, the lease time of the IP address and so on.

### 4.2 Wireless Settings

In the gateway mode, the following figure shows the navigation menu of the **Wireless Settings**:



In the gateway mode, the sub-menus of the **Wireless Settings** include **Basic**, **Advanced**, **Security**, **WPS**, and **Station List**.

### 4.2.1 Basic

Click Wireless Settings --> Basic to display the Basic Wireless Settings page.

#### <u>open all | close all</u>



#### **Basic Wireless Settings**

You could configure the minimum number of Wireless settings for communication, such as Network Name (SBID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network			
Radio On/Off	RADIO OFF		
Network Mode	11b/g/n mixed mode 💌		
Network Name(SSID)	default		
Multiple SSID1			
Multiple SSID2			
Multiple SSID3			
Multiple SSID4			
Multiple SSID5			
Multiple SSID6			
Multiple SSID7			
Broadcast Network Name (SSID)	● Enable O Disable		
AP Isolation	O Enable      O Disable		
MBSSID AP Isolation	C Enable © Disable		
BSSID	00:0C:43:30:62:98		
Frequency (Channel)	2437MHz (Channel 6) 💌		
Wireless Distribution System(WDS)			
WDS Mode	Disable		
HT Physical Mode			
Operating Mode	Mixed Mode C Green Field		
Channel BandWidth	C 20 € 20/40		
Guard Interval	C Long   Auto		
MCS	Auto 💌		
Reverse Direction Grant(RDG)	O Disable 💿 Enable		
Extension Channel	2457MHz (Channel 10) 💌		
Aggregation MSDU(A-MSDU)	⊙ Disable O Enable		
Auto Block ACK	O Disable 💿 Enable		
Decline BA Request			
Other			
HT TxStream	2 •		
HT RxStream	2 •		
Annis	Cancel		

On this page, you may set the parameters of wireless network, WDS, and HT Physical mode.

### • Wireless Network

145reless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode 💌
Network Name(SSID)	default
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	• Enable C Disable
AP Isolation	C Enable C Disable
MBSSID AP Isolation	C Enable  C Disable
BSSID	00:0C:43:30:52:98
Frequency (Channel)	2437MHz (Channel 6) 💌

### The parameters of Wireless Network are described as follows:

Field	Description	
Radio On/Off	Enable or disable wireless LAN interface.	
Network Mode	You may select a proper network mode in the drop down list. <ul> <li>11b/g mixed mode</li> <li>11b only</li> <li>11g only</li> <li>11b/g/n mixed mode (default)</li> </ul>	
Network Name (SSID)	The maximum character number for SSID is 32 characters. The legal characters include letter, number underline or the combination of these characters.	
Multiple SSID1~7	Accessional network SSID. Each SSID can use wireless security setting independently.	

Field	Description
Broadcast	Whether to broadcast SSID. After enabling this
Network Name	function, AP will broadcast its SSID.
(SSID)	
AP Isolation	Enable or disable the isolation among AP clients.
	After enabling this function, the client terminals that
	connect to the same AP can not communicate each
	other.
MBSSID AP	Enable or disable the isolation among different
Isolation	SSIDs. After enabling this function, the client
	terminals with different SSIDs can not communicate
	each other.
BSSID	The MAC address of the wireless interface.
Frequency	You may select a proper channel in the drop down
(Channel)	list. The default channel is Channel 6.

### • Wireless Distribution System (WDS)

WDS modes include Lazy Mode, Bridge Mode, and Repeater Mode. You can also enable WDS.

### 1) Lazy Mode

In the lazy mode, AP automatically connects to the WDS devices that use the same SSID, channel, encryption mode, and the physical mode. You do not need to manually enter other MAC addresses of peer APs.

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode
Phy Mode	GREENFIELD -
EncrypType	WEP -
Encryp Key	

The parameters of Lazy Mode are described as follows:

Field	Description	
WDS Mode	Select the Lazy Mode in the drop down list.	
Phy Mode	The physical modes in the drop down list include CCK,	

Field	Description	
	OFDM, HTMIX, and GREENFIELD.	
Encryp Type	The encryption types you can select include NONE, WEP, TKIP, and AES. If selecting WEP, TKIP, or AES, you need to set the encryption key.	
Encryp Key	Set the encryption key.	

- Step 1 On the **Basic Wireless Settings** page, set the WDS mode to be **Lazy Mode**, set the same phy mode and encryp type with the peer AP, and then enter the MAC address of the peer AP. After finishing the settings, click the **Apply** button to apply the settings.
- Step 2 Enter the **Wireless Security/Encryption Settings** page, set the security mode of the NL-HPW200 to accord with the peer AP.

#### 2) Bridge Mode

In the bridge mode, you can use the NL-HPW200 to connect to your router, for extending wireless coverage. Meanwhile, it can also decrease the working load of the AP that accesses the Internet. In that case, the wireless card does not directly communicate with the wireless device that accesses the Internet, but it directly communicates with the NL-HPW200.



#### Step 1 On the **Basic Wireless Settings** page, select the WDS mode to be **Bridge** Mode.

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode
Phy Mode	ССК
EncrypType	WEP 💌
Encryp Key	
AP MAC Address	00:0C:43:28:60:E8
AP MAC Addres	
AP MAC Address	
AP MAC Address	

Field	Description
WDS Mode	Select the Bridge Mode.
Phy Mode	The physical modes in the drop down list include CCK,
	OFDM, HTMIX, and GREENFIELD.
Encryp Type	The encryption types you can select include NONE,
	WEP, TKIP, and AES. If selecting WEP, TKIP, or AES,
	you need to set the encryption key.
Encryp Key	Set the encryption key.
AP MAC	The MAC address of another AP that connects to the
Address	NL-HPW200 by WDS.

- Step 2 On the **Basic Wireless Settings** page, set the same physical mode and encryption type with the peer AP, and then enter the MAC address of the peer AP. After finishing the settings, click the **Apply** button to apply the settings. The NL-HPW200 will work in the **Bridge** mode.
- Step 3 Enter the **Wireless Security/Encryption Settings** page, set the security mode of the NL-HPW200 to accord with the peer AP.

#### NL-HPW200 User Manual

<u>open all   close all</u>	Wireless Security/Enc	ryption Settings	
₹ T&W Operation Mode □ Operation Kode	Setup the wireless security and encry	ption to prevent from unauth	orized access and monitoring.
Wireless Settings     Basic     Advanced	Select SSID	default V	
Security     Security     Security     Station List     Station List     MAC/DP/Port Filtering     Dir2     Dir2     System Security     Content Filtering     usb     Administration	"default"		
	Security Mode	Disable Disable OPEN	
	Access Policy	SHARED	
	Policy	WPA WPA-PSK	
	Add a station Mac:	WPA2 WPA2-PSK WPAPSKWPA2PSK WPA1WPA2 802.1X	

#### 3) Repeater Mode

In the **Repeater** mode, you can use the NL-HPW200 to connect to the primary router, for extending the wireless coverage.



Step 1 Click Wireless Settings --> Basic to display Basic Wireless Settings page.

Wireless Network	
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode 💌
Network Name(SSID)	default
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Multiple SSID7	
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	C Enable © Disable
MBSSID AP Isolation	○ Enable . O Disable
BSSID	00:0C:43:30:52:98
Frequency (Channel)	2437MHz (Channel 6) 💌

#### NL-HPW200 User Manual

- Step 2 Set the **Frequency(channel)** according with the peer AP (An AP that wants to connect to the NL-HPW200 by WDS).
- Step 3 On the **Basic Wireless Settings** page, set the WDS mode to be **Repeater Mode**, set the same physical mode and encryption type with the peer AP, and then enter the MAC address of the peer AP. After finishing the settings, click the **Apply** button to apply the settings. The NL-HPW200 will work in the **Repeater** Mode.

Wireless Distribution System(WDS)		
WDS Mode	Bridge Mode 💌	
Phy Mode	ССК	
ЕпстурТуре	WEP 💌	
Encryp Key		
AP MAC Address	00:0C:43:28:60:E8	
AP MAC Addres		
AP MAC Address		
AP MAC Address		

Step 4	Click Wireles	s Settings> Security to display the Wireless
	Security/Enc	ryption Settings page.
	open all   close all	Wireless Security/Encryption Settings
	TSW	

Operation Mode	,	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
🖲 🧰 Internet Settings		
🖯 😋 Wireless Settings		
Basic	Select SSID	
- Advanced	COID at all a	
- Security	SSID choice	detault 💌
- Station List	"default"	
🖹 😋 Firewall	Coourity Mode	Disable
MAC/IP/Port Filtering	Security Mode	Disable
Port Forwarding		Disable
DMZ		OPEN
System Security	Access Policy	SHARED
Content Filtering		WEPAUTO
1 C Administration	Policy	WPA WBA DOL
E C Nominisciación	And a station black	WPA-PSK WDA0
	Add a station wac.	WPA2.PSK
		Amply WPAPSKAPA2PSK
		WPA1WPA2
		802 1X

Step 5 On this page, set the security mode of the NL-HPW200 to accord with the peer AP.

Note: In the WDS mode, don't set any mixed modes, for example, WPA-PSK/WPA2-PSK. Do not set all the WDS APs to be Lazy mode, please ensure that at least one WDS AP acts as Root Bridge, and enter the MAC addresses in the WDS table on the Basic Wireless Settings page

### • HT Physical Mode

HT Physical Mode			
Operating Mode	Mixed Mode ⊂ Green Field		
Channel BandWidth	C 20 © 20/40		
Guard Interval	C Long   Auto		
MCS	Auto 💌		
Reverse Direction Grant(RDG)	C Disable 💿 Enable		
Extension Channel	2457MHz (Channel 10) 💌		
Aggregation MSDU(A-MSDU)	© Disable C Enable		
Auto Block ACK	C Disable 💿 Enable		
Decline BA Request	⊙ Disable C Enable		

The I	parameters	of HT	Phy	vsical	Mode	are	described	as	follows:
	04.14.1.0101010	•••••				<b>~</b>		~~	

Field	Description
Operation Mode	You may select Mixed Mode or Green Field. The
	default operation mode is Mixed Mode.
Channel	You may select 20 or 20/40. The default channel
BandWidth	bandwidth is <b>20/40</b> .
Guard Interval	You may select Long or Auto. The default guard
	interval is Auto.
MCS	You may select the MCS value from 0 to 32. The
	default MCS is Auto.
<b>Reverse Direction</b>	You may select <b>Disable</b> or <b>Enable</b> . The default
Grant (RDG)	RDG setting is <b>Enable</b> .
Extension	When the channel bandwidth is set to be 20/40
Channel	MHz, the extension channel will provide a channel
	that is adjacent to the primary channel but not
	overlaps. The wireless network will acquire diploid
	bandwidth by this extension channel, that is, 20MHz
	bandwidth.
	Note: IEEE 802.11n can bind two adjacent 20 MHz bandwidths together to form a 40MHz bandwidth. Actually, the 40MHz bandwidth can act as two 20 MHz bandwidths. One is primary bandwidth, the other is secondary bandwidth. When data is being transmitted, it can act as 40MHz bandwidth, and it can also acts as 20 MHz bandwidth independently. In this way, the data rate is doubled.
Aggregation	Enable or disable A-MSDU.
MSDU	MSDU is the aggregation of multiple MSDUs by
(A-MSDU)	using certain method and the multiple MSDUs forms
	a greater load. MSDU can be considered as
	Ethernet message. Usually, when AP or wireless
	client receives MSDUs from protocol stack, the
	MSDUs will be marked with the Ethernet message

#### NL-HPW200 User Manual

Field	Description
	header (also called A-MSDU Subframes). Before
	sending them out, the A-MSDU Subframes need to
	be transformed into the message format of 802.11
	one by one.
	A-MSDU aggregates multiple A-MSDU Subframes
	and encapsulates them to be an 802.11 message. In
	this way, PLCP Preamble, PLCP Header, and
	802.11 MAC overhead that are needed to send an
	802.11 message decrease. At the same time, the
	acknowledge frames also decrease, and the
	efficiency for sending message is improved.
Auto Block ACK	Enable or disable Auto Block ACK.
	In order to insure the security of the data
	transmission, 802.11n protocol requires that if client
	receives a uincast frame, it should immediately send
	back an ACK frame. After the receiver of A-MPDU
	receives A-MPDU, it needs to process every MPDU.
	In that case, it sends out ACK frames to every
	MPDU. Block Acknowledgement is used to reduce
	the number of the ACK frames by using an ACK
	frame.
Decline BA	Enable or disable Decline BA Request.
Request	

### • Other

Other			
HT TxStream	2 -		
HT RxStream	2 -		
	Apply	Cancel	

The parameters of HT TxStream and HT RxStream are described as follows:

Field	Description
HT TxStream	The stream number that wireless antenna transmits.
HT RxStream	The stream number that wireless antenna receives.

### 4.2.2 Advanced

Click Wireless Settings --> Advanced to display the Advanced Wireless Settings page.

#### open all | close all



#### **Advanced Wireless Settings**

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon interval, Control Tx Rates and Basic Data Rates.

DO Bustantina Maria	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	50 (range 1 - 100, default 100)
Short Preamble	C Enable  O Disable
Short Slot	© Enable C Disable
Tx Burst	C Enable C Disable
Pkt_Aggregate	C Enable C Disable
IEEE 802.11H Support	C Enable O Disable(only in A band)
Country Code	HK (Hong Kong)
Wi-Fi Multimedia	
WMM Capable	C Enable C Disable
APSD Capable	C Enable O Disable
DLS Capable	C Enable O Disable
WMM Parameters	WMM Configuration
Multicast-to-Unicast Conve	rter
Multicast-to-Unicast	C Enable  O Disable

On this page, you may configure advanced wireless parameters, such as beacon interval, data beacon rate, and Tx power.

*Note: The advanced wireless setting is only for advanced user. For the common user, do not change any setting on this page.* 

### Advanced Wireless

The parameters of <b>Advanced Wireless</b> are described as f
---

Field	Description
BG Protection	You may select On, Off, or Auto. The default BG
Mode	protection mode is Auto.
Beacon Interval	By default, wireless beacon signal sends data to
	station every other 100 ms. The range is 20~999.
Data Beacon Rate	The default DTIM is 1ms. The range is 1~255.
(DTIM)	
Fragment	The default fragment threshold is 2346. The range is
Threshold	256~2346.
RTS Threshold	The default RTS threshold is 2347. The range is
	1~2347.
TX Power	Set the Tx power. 100% indicates full power.
Short Preamble	Enable or disable short preamble. The default
	setting is <b>Disable</b> .
	Preamble defines the length of CRC correction
	block for wireless devices. Short preamble adopts
	56-bit synchronization field. The network whose
	network stream is dense should use shorter
	preambles.
	Short Preamble is mainly applied to improvement
	the efficiency of real- time applications, such as
	streaming video, and Voice-Over-IP telephony.
Short Slot	Enable or disable short slot.
Tx Burst	Tx Burst can be used to improve the efficiency of
	data transmission. It can make system transmit
	more data during a period of time.
Pkt_Aggregate	Pkt_Aggregate can aggregate multiple data packets
	together for improving the transmission efficiency
Country Code	Select a proper country code in the drop down list.

### • Wi-Fi Multimedia

#### The parameters of WMM are described as follows:

Field	Description
WMM Capable	Enable or disable WMM. After enabling WMM, AP
	can process different types of wireless data
	according to their priority levels.
APSD Capable	Enable or disable APSD. After enabling APSD, it
	can decrease the consumption of the power supply
	device.
DLS Capable	Enable or disable DLS
WMM Parameters	Click the WMM Configuration button to display
	WMM parameters configuration page.

#### 1) WMM Access Categories

At present, WMM defines traffic into 4 access categories.

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest priority	7,6
	Allows multiple concurrent VoIP calls, with low latency and toll voice quality	
WMM Video Priority	Prioritize video traffic above other data traffic	5, 4
	One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities	0, 3
	Traffic less sensitive to latency, but affected by long delays, such as Internet surfing	
WMM Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2, 1

AC\_VO: Voice (highest priority)

AC\_VI: Video (high priority)

AC\_BE: Best effort (medium priority)

AC\_BK: Background (low priority)

802.11 uses DCF (Distributed Coordination Function) scheme of the CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) protocol to reduce the chances of packets collision while one more devices access the wireless media at the same
time. A client wishing to transmit has to first listen to the channel for a predetermined amount of time so as to check for any activity on the channel. If the channel is sensed "idle" then the client is permitted to transmit. If the channel is sensed as "busy" the station has to defer its transmission. The random interval provides a fair transmission chance for all the devices.

When each priority queue waits for sending packets, it has to wait a fixed time AIFSN and a random time CW. They define time values by multiple time slots. For 802.11b, its time slot is 20ms. The time slot of 802.11a and 802.11g is 9 ms. CW insures the random delay time of DCF, so that the packets collision among the devices with the same access category can be avoided. If collision occurs, CW is doubled until exceeds its maximum value. After every successful transmission, CW returns to the minimum value.

The priority queue that succeeds in the competition of sending packets, it will acquire Txop time to send packets. If the txop value is 0, it is limited to be a MSDC (MAC Service Data Unit).

#### 2) Set WMM Parameters

Click the WMM Configuration button, the following page appears.

	WMM Parameters of Access Point								
	Aifsn	CWMin	CW	Max	Тхор		ACM	Ac	kPolicy
AC_BE	3	15 💌	63	-	0				
AC_BK	7	15 💌	102	3 💌	D				
AC_VI	1	7 💌	15	-	94				
AC_VO	1	3 💌	7	•	47				
	WMM Parameters of Station								
	Aifsn	CV	VMin	C1	VMax		Тхор		ACM
AC_BE	3	1	5 💌	10	23 💌	0			
AC_BK	7	15	5 💌	10	23 💌	O			
AC_VI	2	7	•	1	5 💌	9	4		
AC_VO	2	3	•	7		4	7		
	Apply		Ca	ncel		Close			

On this page, you can configure WMM parameters of access point and station. The parameters are described as follows:

Field	Description

Field	Description
Aifsn	Aifsn (Arbitrary Inter-Frame Space Number). This
	parameter influences the delay time of WMM access
	category. If you use voice or video service, you'd
	better set this parameter to be smaller in the fields of
	AC_VI and AC_VO. If it is E-mail or Web service,
	you should set a bigger value in the fields of AC_BE
	and AC_BK.
Cwmin	Cwmin (Mini. Contention Window) also influences
	the delay time of WMM access category. The
	difference between AC_VI and AC_VO should be
	smaller, but the difference between AC_BE and
	AC_BK should be bigger.
Cwmax	Cwmax (Max.Contention Window)
Тхор	Txop (Opportunity to Transmit) may optimize the
	WMM access. Compared to the WMM access that
	needs a higher priority, such as AC_VI and AC_VO,
	this value should be bigger.
ACM	ACM (Admission Control Mandatory) parameter
	only reacts on AC_VI and AC_VO. If you set this
	value to be 0, it indicates that AP is in the charge of
	the access commands. If this value is 1, it means
	the client is in the charge of the access commands.
Ackpolicy	When WMM packets are transmitting, AP will
	receive an echo request. If you set this value is 0, it
	means AP does not send back an echo request,
	which will brings positive effect for WMM. If this
	value is 1, AP generates the response to the
	request.

Note: NL-HPW200 provides standard WMM settings. If you want to modify the parameters above, please refer to the WMM settings of your WMM products.

#### 3) DLS (Direct Link Setup)

NL-HPW200 provides DLS function. Suppose that there are two WMM devices. Enter the MAC address of a WMM device in the DLS setting of the other device, and then connect the two WMM devices to the NL-HPW200. In this way, the two WMM devices can transmit message directly.

If you want to configure WMM DLS, do as follows:

Step 1 Prepare two wireless network cards (A and B) and one NL-HPW200.

Step 2 Enable the DLS function on the Advanced Wireless Settings page.

Wi-Fi Multimedia	
VVMM Capable	€ Enable
APSD Capable	C Enable    Disable
DLS Capable	€nable ○ Disable
WMM Parameters	WMM Configuration

Step 3 Enable the DLS function of wireless network cards. Enter the MAC address of wireless card A on the **WMM** page of the wireless network card B, and then click the **Apply** button.

🔀 RaUI										
Prot	ile Ne	twork	Advanc	} :ed S	atistics		<b>Ø</b> WPS	Radio on/of	f About	٩
WMM Setup	itatus									_
WM	A >> Enabled		Power !	Save >> Dis	abled			Direct Link >> Ena	abled	
	WAWA Enab	le l								
	WMW -	Power Save	Enable							
		IC_BK	AC	_BE	AC_V	T 🗖 A				
	Direct	Link Setup E	nable							
	MAC A	Address >> 0	0 18	6e 39	ca 81	Timeout V	alue >> 60	sec		
									Apply	
								T	ar Down	
								and the second se		
										-

Step 4 If DLS succeeds, you can view the MAC address of wireless card A on the **WMM** page of wireless card B, and vice versa.

NL-HPW200 User Manual

Profile	Network	Advanced	Statistics	Cos WMM	<b>Ø</b> WPS	Radio on/off	About
WMM Setup Status WMM >> E	nabled	Power Save >	> Disabled			Direct Link >> Enable	ed
<b>2</b> w	MM Enable						
L	WMM - Power Sav	Ve Enable	AC_VI	AC,			
2	Direct Link Setup	p Enable					
	MAC Address >>	00 18 6e	39 ca 81	Timeout Val	ue >> 60	sec	
	00-1E-E3-00-	-61-8A		60		<b></b> Ap	ply
						Tear	Down

### Multicast-to-Unicast Converter

Multicast-to-Unicast Converter					
Multicast-to-Unicast	O Enable	Oisable			
	Apply	Cancel			

Enable or disable Multicast-to-Unicast. After enabling this function, the transmission quality of wireless multicast stream can be improved.

# 4.2.3 Security

Click Wireless Settings --> Security to display the Wireless Security/Encryption Settings page.

#### <u>open all</u> <u>close all</u>



#### Wireless Security/Encryption Settings

Select SSID				
SSID choice		default 🖌		
"default"				
Security Mode		Disable	*	
Access Policy				
Policy		Disable 👻		
Add a station Mac:				
	Apply		Cancel	1

This page allows you to configure wireless security modes and set the encryption keys, to prevent unauthorized access and monitoring.

#### Select SSID •

Select SSID	
SSID choice	default

SSID choice: select SSID that you want to configure.

#### Security Mode •

This page provides 10 types of security modes, including OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSKWPA2PSK, WPA1WPA2, and 8021.X.

#### 1) **OPEN**

"default"				
Security Mode		OF	PEN 🔽	
Wire Equivalence	Protection (WEP)			
Default Key			Key 1 💌	
	WEP Key 1 :			Hex 💌
	WEP Key 2 :			Hex 💌
WEP KBys	WEP Key 3 :			Hex 💌
	WEP Key 4 :			Hex 💌

The parameters of **OPEN** mode are described as follows:

Field	Description
Security Mode	Select OPEN.
Default Key	Select a key as the default key.
WEP Keys (WEP	Set 64-bit or 128-bit key. The key format is Hex or
Key1/2/3/4)	ASCII.

#### 2) SHARED

"default"	
Security Mode	SHARED
Encrypt Type	WEP

Wire Equivalence Protection (WEP)				
	Default Key		Кеу 1 💌	
		WEP Key 1 :		Hex 💌
	WEP Keys	WEP Key 2 :		Hex 💌
		WEP Key 3 :		Hex 💌
		WEP Key 4 :		Hex 💌

The parameters of **SHARED** mode are described as follows:

Field	Description
Security Mode	Select SHARED.
Encrypt Type	You may select WEP or None.
Default Key	Select a key as the default key.

Field	Description
WEP Keys (WEP	Set 64-bit or 128-bit key. The key format is Hex or
Key1/2/3/4)	ASCII.

### 3) WEPAUTO

"default"				
Security Mode		VVE	EPAUTO	
Wire Equivalence	Protection (WEP)			
Default Key			Key 1 💌	
	WEP Key 1 :			Hex
WED Keye	WEP Key 2 :			Hex 💌
WEP Keys	WEP Key 3 :			Hex 💌
	WEP Key 4 :			Hex 💌

The parameters' description of WEPAUTO mode, please refer to OPEN mode.

4)	WPA

"default"	
Security Mode	WPA
WPA	
WPA Algorithms	OTKIP OAES CTKIPAES
Key Renewal Interval	3600 seconds
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	
Idle Timeout	

The parameters of **WPA** mode are described as follows:

Field	Description
Security Mode	Select WPA.

Field	Description		
WPA Algorithms	You may select TKIP or AES.		
Key Renewal	Set the key renewal interval.		
Interval			
WEP Keys (WEP	Set 64-bit or 128-bit key. The key format is Hex or		
Key1/2/3/4)	ASCII.		
IP Address	The IP address of RADIUS server.		
Port	The default port number is 1812. You may change it		
	according to the server setting.		
Shared Secret	The shared key that RADIUS server needs to		
	authenticate.		
Session Timeout	If this value is 0, it indicates that there is no session		
	time limit.		
Idle Timeout	Set the idle timeout.		

#### 5) WPA-PSK

"default"	
Security Mode	WPA-PSK
	л
WPA	
WPA Algorithms	
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

#### The parameters of **WPA-PSK** mode are described as follows:

Field	Description	
Security Mode	Select WPA-PSK.	
WPA Algorithms	Select <b>TKIP</b> or <b>AES</b> .	
Pass Phrase	Set 8-bit to 64-bit key.	
Key Renewal	Set the key renewal interval.	
Interval		

#### 6) **WPA2**

"default"	
Security Mode	WPA2
IN/D.R	
WPA Algorithms	© TKIP IC AES IC TKIPAES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	O Disable      C Enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	
Idle Timeout	

### The parameters of **WPA2** are described as follows:

Field	Description
Security Mode	Select WPA2.
WPA Algorithms	You may select TKIP, AES, or TKIPAES
Key Renewal	Set the key renewal interval.
Interval	
PMK Cache	Set the PMK (Pairwise Master Key) cache period.
Period	PMK scheme allows the roaming users that pass
	through the 802.11X/EAP handshake protocol roam
	to the previous AP again. PMK can decrease the
	roaming delay and improve the roaming speed.
Pre-Authentication	Enable or disable pre-authentication.
WEP Keys (WEP	Set 64-bit or 128-bit key. The key format is Hex or
Key1/2/3/4)	ASCII.
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it
	according to the server setting.
Shared Secret	The shared key that RADIUS server needs to

Field	Description
	authenticate.
Session Timeout	If this value is 0, it indicates that there is no session
	time limit.
Idle Timeout	Set the idle timeout.

### 7) WPA2-PSK

"default"	
Security Mode	WPA2-PSK
WPA	
WPA Algorithms	O TKIP @ AES O TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

### The parameters of **WPA2-PSK** mode are described as follows:

Field	Description
Security	Select WPA2-PSK.
Mode	
WPA	You may select TKIP, AES, or TKIPAES.
Algorithms	
Pass	Set 8-bit to 64-bit key.
Phrase	
Key	Set the key renewal interval.
Renewal	
Interval	

### 8) WPAPSKWPA2PSK

"default"	
Security Mode	WPAPSKWPA2PSK -
VVPA	
WPA Algorithms	OTKIP © AES OTKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

The parameters' description of WPAPSKWPA2PSK mode, please refer to **WPA2-PSK**.

#### 9) WPA1WPA2

"default"	
Security Mode	WPA1WPA2
WPA	
WPA Algorithms	O TKIP I AES O TKIPAES
Key Renewal Interval	3600 seconds
	JL
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	D
Idle Timeout	

#### The parameters of **WPA1WPA2** are described as follows:

Field	Description
Security Mode	Select WPA1WPA2.
WPA Algorithms	You may select TKIP, AES, or TKIPAES.
Key Renewal	Set the key renewal interval.
Interval	
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it
	according to the server setting.

Field	Description
Shared Secret	The shared key that RADIUS server needs to
	authenticate.
Session Timeout	If this value is 0, it indicates that there is no session
	time limit.
Idle Timeout	Set the idle timeout.

# 10) **802.1X**

"default"	
Security Mode	802.1X
802.1x WEP	
WEP	O Disable O Enable
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	
Idle Timeout	

The parameters of 802.1X mode are described as follows:

Field	Description
Security Mode	Select 802.1X.
IP Address	The IP address of RADIUS server.
Port	The default port number is 1812. You may change it
	according to the server setting.
Shared Secret	The shared key that RADIUS server needs to
	authenticate.
Session Timeout	If this value is 0, it indicates that there is no session
	time limit.
Idle Timeout	Set the idle timeout.

# Access Policy

Policy	Allow
Del 00:14:78:3F:2F:3B	Disable Allow 78:3F:2F:3C
Del 00:14:78:3F:2F:3D	Reject Del 00:14:78:3F:2F:3E
Add a station Mac:	

The parameters of Access Policy are described as follows:

Field	Description
Policy	• <b>Disable:</b> Stop the access control to the wireless
	devices in the MAC list.
	Allow: Allow the access control to the wireless
	devices in the MAC list.
	Reject: Reject the access control to the wireless
	devices in the MAC list.
Add a	Enter the MAC address of wireless device that you want to
station Mac	allow or reject.

After finishing the settings, click the **Apply** button to apply the settings.

# 4.2.4 WPS

Click Wireless Settings --> WPS to display the Wi-Fi Protected Setup page.

#### open all close all



#### Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

Enable 💌	
Idle	
Yes	
default	
WPA2-PSK	
AES	
2	
sdfasdfasfadf	
31668729	
● PIN O PBC	
][	_
	Idle       Yes       default       WPA2-PSK       AES       2       sdfasdfasfadf       31668729

On this page, you can modify the WPS settings. WPS can make your client automatically synchronize with the AP setting, and establish connection.

# WPS Config

WPS Config		
WPS:	Enable 💌	
Apply		

WPS: enable or disable WPS.

After enabling WPS, you can configure the parameters related to WPS.

#### • WPS Summary

WPS Summary			
WPS Current Status:	Idle		
WPS Configured:	Yes		
WPS SSID:	default		
WPS Auth Mode:	WPA2-PSK		
WPS Encryp Type:	AES		
WPS Default Key Index:	2		
WPS Key(ASCII)	sdfasdfasfadf		
AP PIN:	31668729		
Reset OOB			

WPS summary displays the preset WPS information, such as WPS current status, WPS authentication mode, and WPS encryption type.

Click the Reset OOB button to display the WPS default settings.

### WPS Progress

WPS modes include PIN and PBC modes, At present, WPS supports three operation modes, including **Enrollee** mode, **Registrar** mode, and **PBC** mode. **Enrollee** and **Registrar** modes need to apply PIN code negotiation.

- 1) Enrollee Mode
- Step 1 Select **Enrollee** mode on the wireless client, the software of wireless client will generate a random PIN code, for example, 12345678.
- Step 2 On the **Wi-Fi Protected Setup** page, enter the PIN code of wireless client, for example, 12345678.
- Step 3 Click the **Apply** button on the **Wi-Fi Protected Setup** page to submit setting.

WPS Progress		
WPS mode	● PIN O PBC	
PIN	12345678	
Apply		

2) Registrar Mode

# Step 1 View the AP PIN on the **Wi-Fi Protected Setup** page, for example, 31668729.

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	RalinkInitAP_305298
WPS Auth Mode:	WPA-PSK
WPS Encryp Type:	TKIP
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	31668729
Reset OOB	

Step 2 Select **Registrar** mode on the wireless client and enter the PIN code of the NL-HPW200. See the following figure:

Profile	Network Adv	anced Statistics	WWW	<b>Ø</b> WPS	Radio On/Of	f About
		WPS AP List				
ID :	default		00-E0-4C-81-86-D1	I 1		Information Pin Code
		WPS Profile List				31668729 Retress Config Mode
ExRegIVW27700	1			٩		Registrar 🔹
•					• • •	Connect
EIN	WPS Associate IE		Progress >> 0%			Rotate
PBC	WPS Probe IE	WPS status is disconne	scted			Disconnect
	Auto					Export Profile

- 3) PBC Mode
- Step 1 On the **Wi-Fi Protected Setup** page, select the **PBC** mode, and then click the **Apply** button. You may also press the **WPS** button on the rear panel.

WPS Progress		
WPS mode	O PIN O PBC	
Apply		

- Step 2 Enable the PBC function on the wireless client. In that case, NL-HPW200 and wireless client will automatically establish connection.
- WPS Status

WPS Status		
WSC:Idle		*
		Ψ.
	►	

The figure above displays WPS current status.

# 4.2.5 Station List

Click Wireless Settings --> Station List to display the Station List page.

☑ T&W ☑ ☐ ☐ Internet Settings ☐ ☐ Wireless Settings	You could monitor stations w	/hich a:	ssociated	I to this AP here				
Basic	Miroloss Notwork							
Advanced	WITCIESS NELWORK	1	1	16		1	1	
Security	MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
WPS	00:1E:4C:39:E4:46	1	1	0	1	20M	0	0
Station List	00:1B:77:03:7D:FB	2	1	0	5	20M	0	0

On this page, you can view the wireless networks that connect to the NL-HPW200. If there is any wireless network connects to NL-HPW200, refresh this page and the connection information of the wireless network is displayed.

# 4.3 Administration

The following figure shows the navigation menu of the Administration:



The sub-menus of the Administration include Management, Upload Firmware, Settings Management, Status, Statistics, System Command and System Log.

#### 4.3.1 Management

#### Click Administration --> Management to display the System Management page.

<u>open all   close all</u>	System Managemen	t			
T&W	You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.				
E G Firewall					
🖲 🧰 usb	Language Settings				
Administration	Select Language	English -			
Upload Firmware     Settings Management     Status	Âρ	ply Cancel			
- 🚺 Statistics	Adminstrator Settings				
System Command D System Log	Account	admin			
	Password	•••••			
	Ân	nly Cancel			
		eaner.			
	NTP Settings				
	Current Time	Sat Jan 1 01:09:17 UTC 2000 Sync with host			
	Time Zone:	(GMT-11:00) Midway Island, Samoa 💌			
	NTP Server	ex time nist gov ntp0.broad.mit.edu time.stdfime.gov.tw			
	NTP synchronization(hours)				
	Αp	ply Cancel			
	DDNS Settings				
	Dynamic DNS Provider	None			
	Account				
	Password				
	DDNS				
	A	Cancel			

This page provides administration settings, NTP settings, and DDNS settings.

### Language Settings

Language Settings			
Select Language	English	-	
	Apply	Cancel	

Select Language: Only provide English.

**Administrator Settings** 

Adminstrator Settings		
Account	admin	
Password		
	Apply	Cancel

The parameters of Administrator Settings are described as follows:

Field	Description
Account	Enter the account that you want to change.
Password	Enter the password for the new username.

Note: If you forget the account and the password, please press the Reset button. The system will return to the factory default settings. The default account and the password are Admin.

### NTP Settings

You may set the AP time to synchronize the time with your PC or the NTP server.

NTP Settings	
Current Time	Sat Jan 1 01:31:44 UTC 2000 Sync with host
Time Zone:	(GMT-11:00) Midway Island, Samoa 💌
NTP Server	ex time.nist.gov nip0.broad.mit.edu time.stidline.gov.tw
NTP synchronization(hours)	
Арр	ly Cancel

The parameters of the NTP Settings are described as follows:

Field	Description
Current Time	Display the current system time. Click the
	Sync with Host button, and then AP can
	synchronize its time with your PC.
Time Zone	Select your proper time zone.
NTP Server	Enter the URL of the time server.
NTP synchronization	Set the interval for synchronizing with the time

Field	Description
(hours)	server.

# 4.3.2 Upload Firmware

Click Administration --> Upload Firmware to display the Upload Firmware page.

및 T&W B- ☐ Internet Settings B- ☐ Wireless Settings	Upgrade the Ralink SoC firmware to obtain new functionality. It takes about 1 minute to uploa upgrade flash and be patient please. Caution! A corrupted image will hang up the system.
🖃 🔄 Administration	Update Firmware
Management     Upload Firmware     Settings Management     Status	Location: Browse Apply
Statistics	Update Bootloader
System Command	Location: Browse
	Apply

If you want to upload the firmware of the NL-HPW200, click the **Browse...** button to choose the correct new firmware, and then click the **Apply** button. System begins to upgrade firmware.

After upgrading, system reboots and automatically enters the Web page.

The procedure for upgrading Bootloader is similar to that of the firmware upgrade.

Note: Upgrading firmware will make the AP return to the factory defaults. In order to avoid the settings loss, please save the settings before upgrading firmware. During upgrading, do not cut off the power or press the **Reset** button.

# 4.3.3 Settings Management

Click Administration --> Settings Management to display the Settings Management page.

<u>open all   close all</u>	Settings Management	t
G T&W B ← Internet Settings B ← Wireless Settings E ← Administration	You might save system settings by e importing the file, or reset them to fa	exporting them to a configuration file, restore them by ctory default.
Management		
Upload Firmware	Export Settings	
Settings Management     Status	Export Button	Export
Statistics System Command		
System Log	Import Settings	
	Settings file location	Browse
	Imp	ort Cancel
	Load Factory Defaults	
	Load Default Button	Load Default

The parameters on this page are described as follows:

Field	Description
Export Settings	Click the Export button to save the settings
	on your local PC.
Import Settings	Click the Browse button to choose the
	settings on your PC, and then click the Import
	button to import the settings to AP.
Load Factory Defaults	Click the Load Default button, the system
	returns to the factory default settings.

# 4.3.4 Status

Click Administration --> Status to display the Access Point Status page.

#### <u>open all</u> | <u>close all</u>

😨 т&w	
🕂 🗀 Int	ernet Settings
🗄 🚞 Wi	reless Settings
🗄 😑 🗚	ministration
	Management
🗋	Upload Firmware
	Settings Management
	Status
- 🗋	Statistics
	System Command
- 0	System Log

#### **Access Point Status**

Let's take a look at the status of Ralink SoC Platform.

System Info	
SDK Version	3.2.0.0 (Aug 18 2009)
System Up Time	3 hours, 43 mins, 6 secs
System Platform	RT3052 embedded switch
Operation Mode	Bridge Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Primary Domain Name Server	192.168.1.5
Secondary Domain Name Server	168.95.1.1
MAC Address	00:0C:43:30:52:11
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:0C:43:30:52:11

This page displays system information, Internet configuration, and local network settings.

# 4.3.5 Statistic

Click the Administration --> Statistics to display the Statistic page.

#### <u>open all | close all</u>

#### Statistic

🥃 T&W ⊞ 🛅 Internet Settings	Take a look at the Ralink SoC statistics	
🗄 📋 Wireless Settings	Метогу	
Management	Memory total:	29224 kB
📋 Upload Firmware	Memory left:	18568 kB
Settings Management	WAN/LAN	
Status	LAN Rx packets:	9072
System Command	LAN Rx bytes:	644400
System Log	LAN Tx packets:	2423
	LAN Tx bytes:	1437584
	All interfaces	
	Name	eth2
	Rx Packet	40963
	Rx Byte	3515667
	Tx Packet	4770
	Tx Byte	2198164
	Name	lo
	Rx Packet	17
	Rx Byte	2878
	Tx Packet	17
	Tx Byte	2878

This page displays the memory status, the numbers of transmitted and received data packets of the WLAN, LAN, and WAN.

# 4.3.6 System Command

Click Administration --> System Command to display the System Command page.

<u>open all   close all</u>	System Command	
😼 T&W 🖻 🦳 Internet Settings	Run a system command as root.	
🖽 🧰 Wireless Settings	System command	
Administration     Management     Oload Firmware     Settings Management     Status     Statistics     Statistics     System Command     System Log	Command:	
		~
	Apply Cancel	

On this page, you can run 4 types of commands, including ls, ps, reboot, and ping.

# 4.3.7 System Log

Click Administration --> System Log to display the System Log page.

#### <u>open all</u> | <u>close all</u>

#### System Log

T&W     Tay     Internet Settings     Wireless Settings     Administration	Syslog: Refresh Clear	
	System Log	
<ul> <li>Status</li> <li>Status</li> <li>Status</li> <li>Status</li> <li>Statistics</li> <li>System Command</li> <li>System Loc</li> </ul>	Jan 1 03:09:48 (none) syslog.info syslogd started: BusyBox v1.12 Jan 1 03:09:48 (none) user.notice kernel: klogd started: BusyBox Jan 1 03:09:58 (none) user.info kernel: br0: topology change det Jan 1 03:09:58 (none) user.info kernel: br0: port 9(ra7) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 8(ra6) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 8(ra6) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 7(ra5) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 7(ra5) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 7(ra5) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 7(ra5) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 5(ra3) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 5(ra3) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 5(ra3) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.info kernel: br0: port 4(ra2) enterir Jan 1 03:09:58 (none) user.i	1 : v1.2.1 (2009- ected, propagat g forwarding st ected, propagat ig forwarding st ected, propagat
	Jan 1 03:09:58 (none) user.info kernel: br0: topology change det Jan 1 03:09:58 (none) user.info kernel: br0: port 1(ra0) enterir Jan 1 03:00:20 (none) user.info syslog: Password for 'admin' cha Jan 1 03:30:33 (none) user.info syslog: Password for 'admin' cha	ected, propagat ig forwarding st inged anged

On this page, you are allowed to set the log server and view the system log. After enabling the remote log server and entering the IP address of the server, click the Apply button, and then the log information can be sent to the remote log server.

# 5 Install the PowerLine Utility

First step, you need to verify that there is no any other Powerline Utility installed on your computer before installing this utility. If there is another utility installed, please uninstall it and restart your computer.

Second step, please insert the Utility CD-ROM into the computer's CD-ROM drive. then select the "PowerLine Utility Installation" folder and clicks the setup.exe. Follow the steps to install the Utility Program. No password or CD-Key is needed.

The installation utility similar to the one shown in below figure. Click the Next button to continue.



Power Packet5.0 _x86Setup		
Select Installation Fold	ler	
The installer will install Power Packet5.(	0_x86Setup to the following folde	er.
To install in this folder, click "Next". To	install to a different folder, enter i	t below or click "Browse".
<u>F</u> older:		
C:\Program Files\Intellon\Po	wer Packet5.0 _x86Setup\	Browse
		Disk Cost
Install Power Packet5.0_x86Setup f	ior yourself, or for anyone who us	es this computer:
Evenione		
C Lutur		
U Just me		
U Just me		
t Just me	Cancel < Ba	ack
C Just <u>m</u> e	Cancel < Ba	ack Next>
Power Packet5.0 _x86Setup	Cancel < <u>B</u> a	sck
Pover Packet5.0 _x86Setup Installation Complete	Cancel < <u>8</u> 2	ack <u>Next&gt;</u>
Pover Packet5.0 _x865etup Pover Packet5.0 _x865etup Power Packet5.0 _x685etup has been	Cancel <u>Se</u>	sck <u>Next&gt;</u>
Pover Packet5.0z005setup Installation Complete Power Packet5.0x065etup has been Cick "Diose" to ext.	Cancel <u>Se</u>	ack <u>Next&gt;</u>
Pover Packet5.01055etup Installation Complete Pover Packet5.0_x655etup has been Click "Doe" to ext.	Cancel < Ba	sck Next>
Pover Packet5.0x865etup Installation Complete Pover Packet5.0_x665etup has been Click "Dore" to ext.	Cancel < Ba	sck <u>Nest</u>
Power Packet5, 0x865etup Installation Complete Power Packet5, 0 _x665etup has been Click "Close" to ext.	Cancel	sck <u>Nest</u>
Pover Packet5, 0x865etup Installation Complete Power Packet5, 0 _x665etup has been Click "Close" to exit.	Cancel	eck Next>
Pover Packet5 0x865etup Installation Complete Power Packet5 0_x665etup has been Click "Close" to exit.	Cancel	sck <u>Rest</u>
Suit ge  Pover Tacket5, 0x86Setup Installation Complete Power Packet5, 0 _x66Setup has been Click "Close" to exit.	Cancel	eck Next>
Power Packet5, 0x0055etup Installation Complete Power Packet5, 0_x665etup has been Click "Dose" to exit.	Cancel	sck Next>

Click "Close" to complete installation.

# 6 How to Use The Utility Software

# 6.1 Main Tab

The **Main** screen provides a list of all powerline devices logically connected to the computer when the utility is running.

The **top panel** shows local HomePlug devices connected to the computer's NIC (Network Interface Card). the user can click the Connect button to its right. Once connected to the local device, the utility will automatically scan the power line periodically for any other HomePlug devices. If no local HomePlug devices are discovered, the status area above the connect button will indicate with a message 'NO HOMEPLUG ADAPTERS DETECTED'.

evice Type	MAC Address 00:1E:E3:00:26:06	Connecte	ed on Powerline	device.
Powerline Devices dete Device Name	cted: Network Typ Password	e: Public Quality	Rate (Mbps)	Autoscan On MAC Address
Device 3			125.00	00:1E:E3:00:26:C9
Device 2			92.00	00.1E:E3:00.26:CA
Device 1			98.00	00.1E:E3:00.26:CD
Device 5			120.00	00:1E:E3:00:26:CE

The **lower panel** displays all the HomePlug remote devices, discovered on the current logical network. The total number of remote devices connected on the same network can be found on top of the Remote device panel. The Network type (Public or Private) is also displayed based on the network status of the local device. The scan status option is displayed on the top right corner above the Remote devices panel showing whether the Autoscan functionality is turned ON or OFF. The following information is displayed for all devices that appear in the lower panel.

#### Device Name

This column shows the default device name, which may be user re-defined. A user can change the name by either using the rename button or by clicking on the name and editing in-place.

#### MAC Address

This column shows the Remote device's MAC address.

#### Password

This column by default is blank and "Enter Password" button can be used to enter it. To set the Password of the device (required when creating a private network), first select the device by clicking on its name in the lower panel and then click on the enter Password button. A dialog box will appear as shown in below figure to type the password. The selected device name is shown above the password field and the password can be verified by hitting the OK button. The Password field accepts the Device password in any case formats, with or without dashed between them.

A confirmation box will appear if the password was entered correctly. If a device was not found, the user will be notified along with the suggestions to resolve common problems. This process might take a few seconds to get completed.



### • Add

This button is used to add a remote device to the existing network by entering the device password of the device. A dialog box will appear as shown in below figure. The dialog box allows the user to enter both a device name and the password.

A confirmation box will appear if the password was entered correctly and if the device was found in the powerline network. If a device was not found, the user will be notified and suggestions to resolve common problems will be presented.



Note: The device must be present on the power line (plugged in) in order for the password to be confirmed and added to the network. If the device could not be located, a warning message will be shown.

### • Scan

This button is used to perform an immediate search of the HomePlug devices connected to the Powerline network. By default, the utility automatically scans every few seconds and updates the display screen.

# 6.2 Privacy Tab

The **Privacy** screen provides the user with an option to maintain security for their logical network and also to select the devices that has to be included in the network. The appearance is shown in below figure.

All HomePlug devices are shipped using a default logical network (network name), which is normally "**HomePlug**". The **Privacy** dialog screen allows user to change to a private network by changing the network name (network password) of devices.

The user can always reset to the HomePlug network (Public) by entering "HomePlug" as the network name or by clicking on the Use **Default** button.

Power Packet5.0 _x86	×
Main Privacy Diagnostics About	
Use this scient to create a Private Network that provides you with extra secur Private Network Name ScientFugAN Do not share the network name with others you do not want to be pat of th	ity. twork] iis network.
After setting the name above, choose how it will be applied below: Place On This Network: Only the device attached to this computer (the Local Device) Isolates this computer (the Incold Device)	Set Local Device Only
ALL devices whore Password has been entered. (They communicate together but are isolated from devices with a different network name)	OR Set All Devices
	Close Cancel

*Note: Changing the network name to anything other than HomePlug will show the network type on the main screen as Private.* 

### Set Local Device Only

This button can be used to change the network name (network password) of the local device. If a new network password is entered, all the devices seen on the Main panel prior to this will be no longer present in the new network, effectively making the local devices not to communicate to the devices who were in the old logical network. Devices previously set up with the same logical network (same network name) will appear in the device list afterward selecting this option.

### Set All Devices

This button is used to change the logical network of all devices that appear on the Main panel whose Device's Password had been entered for the same logical network. A dialog window will appear to report the success of this operation. For devices whose device password's were not entered, this operation will fail and will report a failure message.

# 6.3 Diagnostics Tab

The **Diagnostics** screen shows System information and a history of all remote devices seen over a period of time. The appearance is shown in below figure.

The **Upper panel** shows technical data concerning software and hardware present on the host computer which were used to communicate over HomePlug on the Powerline network. It shall include the following:

- Operating System Platform/Version
- Host Network Name
- User Name
- MAC Address of all NICs (Network interface card) connected to the host
- Identify versions of all Driver DLLs and Libraries used (NDIS) and optionally
- HomePlug chipset manufacturer name (Turbo Only devices)
- MAC Firmware Version (Turbo Only devices)
- MAC addresses of all devices connected locally to the host
- Version of the Configuration Utility
- Vendor name

in   Privac	y Diagnostics About	1			
System Informa	ation				-
On NIC #1 MA	C = 00:1A:A0:3A:26:F7				
HomePlug D	evice #1 MAC = 00:1E:E3:0	0:26:06			
Network nam	e:HomePlugAV				
Vendor: Intell	on				
Firmware: HF	1.0				
Reads: IIII.	29 (UKB), Writes: 34840 (UI ila = 0, Hisbart = 0,00 Mbar	KBJ Lawrad - 0.00 Mbr			-1
Drops = 0, Pa	ils = 0, Highest = 0.00 Mbps	: Lowest = 0.00 Mbp	08		<u> </u>
lemote Device	History (Log)				
Device	MAC Address	Password	Rate (Mbps)	Network	Last Seen
Device 1	001E:E3:00:26:CD	not entered -	98.00	HomePlug	May 09 11:41
Device 2	00:1E:E3:00:26:CA	<ul> <li>not entered -</li> </ul>	92.00	HomePlug	May 09 11:41
Device 3	00:1E:E3:00:26:C9	<ul> <li>not entered -</li> </ul>	125.00	HomePlug	May 09 11:41
Device 5	00.1E:E3.00.26.CE	<ul> <li>not entered -</li> </ul>	120.00	HomePlug	May 09 11:41
4 Í					•
			1	D110	- 4
Delete	Email Report		Save Report	Fint Hep	ort I
Delete	Email Report	_	Save Report	Print Hep	ort
Delete	Email Report	_	Save Report	Print Hep	or

The **Lower panel** contains a history of all remote devices seen on the computer over a certain period of time. All devices that were on the powerline network are listed here along with a few other parameters. Devices that are active on the current logical network will show a transfer rate in the Rate column; devices on other networks, or devices that may no longer exist are shown with a "?" in the Rate column. The following remote device information is available from the diagnostics screen:

Device Alias Name

- Device MAC Address
- Device Password
- Device Last known rate
- Device Last Known Network name
- HomePlug chipset manufacturer name
- Date device last seen on the network
- MAC Firmware Version

The diagnostics information displayed may be saved to a text file for later use, or can be printed for reference for a technical support call. Devices, which are not part of the network anymore, can be deleted using the delete button. A dialog window pops up with a confirmation message if we try to delete a device whose password has been entered.

# 6.4 About Tab

The **About** screen shows the software version and provides a html link to a website, such as www.PowerPacket.com. Clicking on the web address field will open a web browser and take the user directly to the web site.

fais Privacy Dispositics About PowePacketUNity Version V5.0.Build 1.6 Copyright 2008. Healon Cop. All Pights Reserved http://www.PowePacket.com Released.June 30, 2008	lain   Priv		a second second second second second second		2 -
PowerPacket Unity Version, V50, Build 1.6 Copyright 2008, Intelian Corp. All Rights Reserved. http://www.PowerPacket.com. Released. June 30, 2008		acy Diagnostics Abo	ut		
http://www.PowerPacket.com Released. June 30, 2008		PowerPacket Utility	Version. V5.0, Build 1.6		
Preferences	Preferences	http://www.PowerPacke	st.com	Released: June 30, 2008	

### • Preferences

The lower part of the panel may display options for turning the auto-scan feature on or off.

# 7 How to use the NMK Pushbutton

This section describes how to add new devices to, or remove old devices from a HomePlug AV logical network(AVLN) , both can be accomplished using a NMK pushbutton press.

Operation progress and outcome can be monitored by observing the behavior of the Power LED.

# 7.1 Forming a HomePlug AV logical network

When two devices with different NMK values are connected to the same powerline, and wants them to form a logical network.

- 1) Press the NMK button on the first device A for less than 3 seconds.
- Press the NMK button on the second device B for less than 3 seconds. The button on B must be pressed within 1 minute
- 3) Wait for connection to complete.

The Power LED on both devices will flash evenly at 1-second intervals until the operation succeeds or fails. It will illuminate steadily on successful completion. If an error occurs, the Power LED on the 'adder' will flash unevenly until the pushbutton on the 'adder' is pressed again or the 'joiner' is reset by holding the pushbuttons down for more than 10 seconds.



# 7.2 Joining a Network

In this scenario a network exists, a new device, the 'joiner', wants to join the network. Any device on the existing network can become the 'adder'.

- 1) Press the pushbutton on the 'joiner' for at least 3 seconds.
- Press the pushbutton on any network device for less than 3 seconds, making it the 'adder'. Please press this pushbutton within 1 minute.
- 3) Wait for connection to complete.

The Power LED on both devices will flash at 1-second intervals until the process succeeds or fails. It will illuminate steadily on success. If an error occurs, the Power LED on the 'adder' will flash unevenly until the pushbutton on the 'adder' is pressed again or the 'joiner' is reset by pressing the pushbutton for more than 10 seconds.



# 7.3 Leaving a Network

A network exists. The user wants to remove one device, the 'leaver', from that network, for whatever reason. He may want to remove the device from service altogether or have it join another logical network.

- Press the pushbutton on the 'leaver' for at least 10 seconds. The device will reset and restart with a random NMK.
- 2) Wait for reset to complete.

The Power LED on the 'leaver' will momentarily extinguish during reset, flash during restart then illuminate steadily. No errors can occur.

Once the process completes, the user may disconnect the device from the medium or join it to another logical network on the same medium.

NL-HPW200 User Manual


## 8 About PowerLine QoS

The NL-HPW200 allows for 4 levels of Channel Access Priority (CAP (0 - 3)). The 8 levels of VLAN Ethernet tags must be mapped to the 4 levels of CAP priority, where CAP 3 is the highest priority and CAP 0 is the lowest. CAP 3 priority might be used for voice and network management frames, CAP 2 is used for streaming video and music while CAP 1 and CAP 0 are used for data.

## **Default CAP**

The 'Default CAP' group allows for default priority mapping of packets that do not have a VLAN TAG. Settings are available for Unicast (directed to a host).

- IGMP (default CAP 3) sets the channel access priority for IGMP frames
  these are the group management frames, not the stream data
- Unicast (default CAP 1) sets the default channel access priority for unicast frames not matching any other classification or mapping.
- IGMP managed Multicast Stream (Fixed to CAP 2) sets the default channel access priority for stream data belonging to a snooped IGMP multicast group.
- Multicast/Broadcast sets the default CAP for multicast frames not in a snooped group and for broadcast frames.

VLAN Tag	Default CAP Priority	TOS Bit	Default CAP Priority
User riority		User Priority	-
0	CAP1	0	CAP1
1	CAP0	1	CAP0
2	CAP0	2	CAP0
3	CAP1	3	CAP1
4	CAP2	4	CAP2
5	CAP2	5	CAP2
6	CAP3	6	CAP3
7	CAP3	7	CAP3

The following are the factory default settings for VLAN Tags and TOS Bits:

## 9 Parameter and Specification

PLC Module SPEC		
Chipset	Intellon INT6400/INT1400	
Serial Flash	16Mbits	
SDRAM:	128Mbits	
Firmware	Support North America/Europe/APAC/Japan	
Protocol	HomePlug AV	
	IEEE 802.3 10/100 Ethernet (100Mbps)	
	IEEE 802.3u Fast Ethernet	
	Co-exists with existing HomePlug 1.0	
PLC Rate	200Mbit/s	
Data Rate - TCP/UDP	65Mbps TCP, 90Mbps UDP	
Modulation Band	2-30MHz	
Modulation Schemes	Supports 1024/256/64/16/8-QAM, QPSK, BPSK and ROBO	
Encryption	128-bit AES	
QoS	Support contention-free access, four-level priority based	
	contention access, and multi segment bursting	
	Support VLAN Priority	
	Support ToS and CoS Packet Classifier	
Work Mode	TDMA and priority based CSMA/CA	
Multicast Support	Supports IGMP managed multicast sessions	
WiFi Module SPEC		
Chipset	Ralink RT3050	
Protocol	IEEE 802.11b/g/n	
	IEEE 802.3/3x/3u	
Wireless Frequency	2.4GHz to 2.484GHz	
Range		
Wireless Signal Rates	11b: 11/5.5/2/1 Mbps	
With Automatic Fallback	11g: 54/48/36/24/18/12/9/6 Mbps	
	11n: 150Mbps in 20MHz mode	
Transmit Output Power	11n: 18dBm	
	11g: 21.5dBm	
	11b: 26dBm	
Receiver Sensitivity	11n: 150Mbps/-69dbM	
	11g: 54Mbps/-75dBm	
	11b: 11Mbps/-88dBM	
Work mode	1Tx/1Rx	
multi-BSSID	Up to 8 BSSIDs	
Security	WPA, WPA2, 64/128/152-bit WEP, SSID hide,	
	MAC Address Access Control List	

NL-HPW200 Us	er Manual
--------------	-----------

System SPEC				
System Support	Windows 98SE, 2000, ME, XP 32/64 bit and Vista 32/64bit			
LED's	Power/run: double color			
	PLC: double color, indicator PLC Link and Activity			
	WLAN: indicator Wireless Link and Activity			
	WPS: indicator the status of WPS Authenticator.			
	LAN: indicator the Ethernet Link and Activity			
Power Socket	Support British, Euro, Japan, US and China power connector			
Ethernet Interface	1 x RJ45 for 10/100 Ethernet (Auto MDI/MDI-X)			
Antenna interface	R/SMA x 1			
Push Button	Reset: reset system or restore default setup			
	NMK: use to synchronized network password in PLC			
	WPS: use to authenticated for wireless provide service			
Software update	Support software update from WEB			
Consumption	7.5W (Typed)			
Environment Requirement				
Operating Temperature	0° to 40° C			
Storage Temperature	-20 ° to 70 ° C			
Operating Humidity	10% to 85% Non-condensing			
Storage Humidity	5% to 90% Non-Condensing			
Input Rating	100-240 VAC, 50/60Hz			
EMC and Safety				
Regulatory Compliance	FCC Part 15 Class B, CE			
Safety Regulations	UL			
Green Standard	RoHS			
Physical Feature				
Physical Characteristics	L×W×H: 170mm×147mm×36.5mm			
Weight	291g			