

**200M Powerline Wallmount
Wireless 11n 1T1R 150M AP
GP-L200N
User Manual**



GOLDWEB

Contents

1	Overview	1
2	Hardware Description.....	3
2.1	LED Status.....	3
2.2	Interface Description.....	4
2.2.1	The Ethernet Interface	4
2.2.2	The Adapter's Buttons	4
2.3	Hardware Installation.....	6
2.3.1	System Requirements	6
2.3.2	Before You Begin	6
2.4	Operation Range	6
2.5	How to Improve the Transmission Capacity	7
2.6	Wireless Roaming	7
3	Wireless Network Configuration.....	8
3.1	TCP/IP Settings	8
3.2	Log In to the Web Page.....	11
4	Web Configuration	12
4.1	Internet Settings	12
4.1.1	LAN.....	12
4.1.2	DHCP Clients.....	15
4.2	Wireless Settings.....	15
4.2.1	Basic.....	16
4.2.2	Advanced.....	27
4.2.3	Security.....	35
4.2.4	WPS.....	43
4.2.5	Station List	47
4.3	Administration.....	47
4.3.1	Management.....	48
4.3.2	Upload Firmware	49
4.3.3	Settings Management.....	50
4.3.4	Status.....	50
4.3.5	Statistic	51

4.3.6	System Command	53
4.3.7	System Log	53
4.3.8	SDK History	55
5	Install the PowerLine Utility	56
6	How to Use the Utility Software	59
6.1	Main Tab	59
6.2	Privacy Tab	61
6.3	Diagnostics Tab	63
6.4	About Tab	64
7	How to use the NMK Pushbutton	66
7.1	Forming a HomePlug AV logical network	66
7.2	Joining a Network	67
7.3	Leaving a Network	67
8	About PowerLine QoS	69
9	Parameters and Specifications	70

About User Manual

This user manual mainly describes how to install and configure the GP-L200N wireless extender.

Organization

This user manual is organized as follows:

Chapter	Description
Chapter 1 : Overview	Provides a general overview of the GP-L200N wireless router and the package list.
Chapter 2 : Hardware Description	Mainly describes the front panel and the rear panel of the GP-L200N and the procedure for hardware installation.
Chapter 3 : Wireless Network Configuration	Describes how to configure network settings of your PC and how to connect to the GP-L200N.
Chapter 4 : Web Configuration	Mainly describes how to navigate through the Web pages and how to configure the parameters.
Chapter 5 : Install the PowerLine Utility	Describes installation of the PowerLine Utility.
Chapter 6 : How to Use the Utility Software	Describes how to view the PowerLine parameter, modify NMK, device name.
Chapter 7 : How to use the NMK Pushbutton	Describes how to form, join and leave a HomePlug AV local network.
Chapter 8 : About PowerLine QoS	Describes how to setup the QoS parameter in PowerLine function.
Chapter 9 : Parameters and Specifications	Describes the product system specifications.

GP-L200N Features

PowerLine Features

- 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 Features

- 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, WPAUTO, 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 the GP-L200N.

The GP-L200N (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. The GP-L200N supports CCK and OFDM and its PowerLine phy rate is up to 200Mbps, wireless phy rate is up to 150 Mbps under 11n mode.

The GP-L200N 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 ensures the security of wireless communication.

Package list

Please check whether your package list includes the following items:

- GP-L200N 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 the GP-L200N. By observing their status, you can know whether the device runs normally.



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

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 > 100 Mbps, see note.
	Orange	On/Blink	When PLC rate in 80-100 Mbps, see note.
	Red	On/Blink	When PLC rate < 100 Mbps, see note.
LAN	Green	On	Connection succeeds.
	Green	Blink	Data is being transmitted.
	-	Off	No LAN connection.

**Note:**

The PLC LED indicator turns “On” when powerline link is detected. If the device is serving as a STATION, the LED indicator blinks to indicate transmit or receive powerline activity. If the device is serving as a CCO, the LED indicator lights 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 connects 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 restores 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 GP-L200N
- One PLC device for PowerLine communication
- A PC has been installed TCP/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:

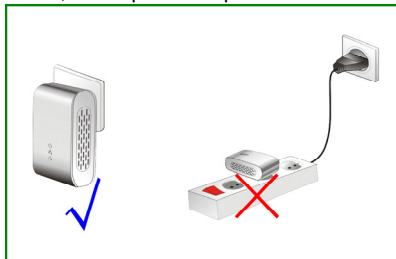
- When connecting the device to a computer, a hub, a router or a switch, the Ethernet cable should be less than 100 meters.
- Do not place this device on an unstable surface or support. Do not put this device on the ground.
- Keep the device clean. Avoid the device from direct sunshine. Avoid any metal 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 the GP-L200N 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 varies according to 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 without female socket, it is recommended to plug the device directly into a wall socket, not to power stripe.



2.6 Wireless Roaming

Suppose that one GP-L200N and several APs run in the same network. The GP-L200N or AP acts as one BSS, and has its coverage range. One wireless client terminal (for example, a 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 GP-L200N and APs' coverage.

In order to realize the wireless client roaming among different APs, you need to set the GP-L200N and APs properly. Do as follows:

- Set the same SSID for the GP-L200N 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 GP-L200N and APs should configure the same encryption mode and the encryption key for establishing connection.
- The GP-L200N 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

The Web management tool allows you to configure only the wireless function of the GP-L200N, but not PLC function. You need to install the PowerLine Utility to configure the PLC 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 GP-L200N.

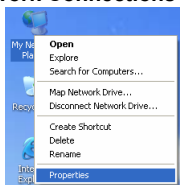
3.1 TCP/IP Settings

By default, the IP address of LAN interface of the GP-L200N is 192.168.1.1. The subnet mask is 255.255.255.0. The DHCP Server is enabled.

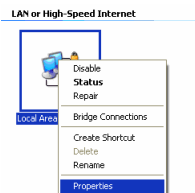
It is recommended that you set the network adapter to be **Obtain an IP address automatically**. Your PC obtains IP address, subnet mask, gateway, and DNS address automatically via the extender. If you know the setting of the current LAN interface, you can manually set the TCP/IP properties of the network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

To manually set the network adapter, do as follows:

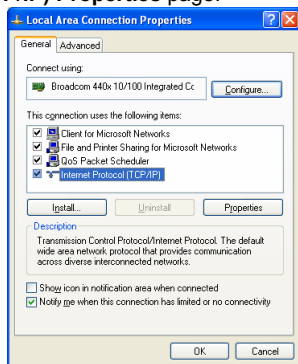
- Step 1** Right-click the icon of **My Network Places** and choose **Properties** from the menu. The **Network Connections** page appears.



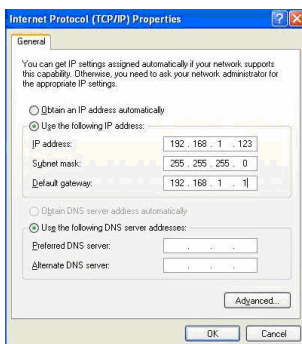
- Step 2** Right-click the network adapter icon and choose **Properties** from the menu. The **Local Area Connections Properties** window appears. **Note:** If there are several network cards on your PC, a window other than the **Local Area Connections Properties** may appear.



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

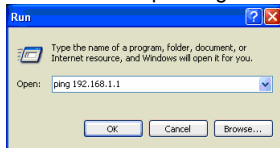


Step 4 Select **Use the following IP address** and enter the IP address of the network adapter. The IP address should belong to the IP network segment 192.168. 1.X (X is a number between 2 and 254).



Step 5 Set the subnet mask and click **OK** to finish manual setting.

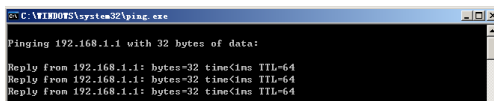
Step 6 After finishing setting, you can ping the default IP address of the extender, to check whether the current connection between PC and the extender is normal. Choose **Start > Run...** from the desktop and enter **ping 192.168.1.1** in the corresponding field. See the following figure:



Note:

The default IP address of the LAN interface is 192.168.1.1. If this IP address is changed and you need to ping the IP address of the extender, enter the current IP address.

Step 7 If the PC pings through the default IP address of the extender and the following page appears, the connection between the PC and the AP is normal.



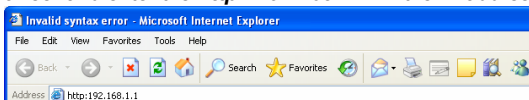
```
C:\WINDOWS\system32\ping.exe

Pinging 192.168.1.1 with 32 bytes of data:

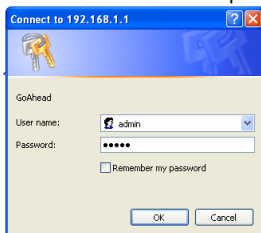
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

3.2 Log In to the Web Page

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



In the **login** window, enter the user name and the password.



Note:

The default user name and password are **admin** and **admin** respectively.

Click **OK** and you can log in to the Web page of the GP-L200N.

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** contain **LAN** and **DHCP clients**.

4.1.1 LAN

Choose **Internet Settings** > **LAN** to display the **Local Area Network (LAN) Settings** page.

Local Area Network (LAN) Settings

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

LAN Setup	
IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
LAN 2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
LAN2 IP Address	<input type="text"/>
LAN2 Subnet Mask	<input type="text"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS Server	<input type="text" value="192.168.1.5"/>
Secondary DNS Server	<input type="text" value="168.95.1.1"/>
MAC Address	<input type="text" value="00:1F:A4:90:39:C8"/>
DHCP Type	Server <input type="button" value="v"/>
Start IP Address	<input type="text" value="192.168.1.3"/>
End IP Address	<input type="text" value="192.168.1.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Primary DNS Server	<input type="text" value="10.10.10.251"/>
Secondary DNS Server	<input type="text" value="168.95.1.1"/>
Default Gateway	<input type="text" value="192.168.1.1"/>
Lease Time	<input type="text" value="86400"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
Statically Assigned	MAC: <input type="text"/> IP: <input type="text"/>
802.1d Spanning Tree	Disable <input type="button" value="v"/>
IGMP Proxy	Disable <input type="button" value="v"/>
UPNP	Disable <input type="button" value="v"/>
Router Advertisement	Disable <input type="button" value="v"/>
PPPoE Relay	Disable <input type="button" value="v"/>
DNS Proxy	Enable <input type="button" value="v"/>

In this page, you can configure LAN interface properties, DHCP server properties, and other parameters related to LAN.

The following table describes parameters in this page:

Field	Description
IP Address	The IP address of the 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 Disable .
LAN 2 IP Address	The second IP address of the LAN interface. This IP address should not collide with the IP address of the internal network.
LAN 2 Subnet Mask	The subnet mask of the second IP address of the LAN interface.
MAC Address	Display the current MAC address that LAN interface uses.
DHCP Type	<p>Enable or disable DHCP service. The default setting is Server, which indicates that DHCP service is enabled.</p> <p>After enabling DHCP service, you can configure the following parameters of the DHCP server:</p> <ul style="list-style-type: none">● Start IP Address: The start IP address of the DHCP address pool.● End IP Address: The end IP address of the DHCP address pool.● Subnet Mask: The subnet mask that DHCP server assigns.● Primary DNS Server: The primary DNS server that DHCP server assigns.● Secondary DNS Server: The secondary DNS server that DHCP server assigns.● Default Gateway: The gateway that DHCP server assigns.● Lease Time: The lease time of the IP address.● Statically Assigned: For binding MAC address and IP

Field	Description
	address.
802.1d Spanning Tree	It can provide redundant link and prevent network from generating loop. You may select Enable or Disable .
LLTD	After enabling LLTD (Link Layer Topology Discovery), Windows Vista automatically discovers link topology of other devices, 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.

After setting, click **Apply** to save the settings.

4.1.2 DHCP Clients

Choose **Internet Settings > DHCP Clients** to display the **DHCP Client List** page.

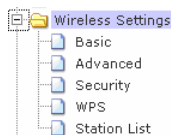
You could monitor DHCP clients here.

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

In this page, you can view the client information assigned by the DHCP server, including the MAC address, IP address, and the lease time of the IP address.

4.2 Wireless Settings

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



The sub-menus contain **Basic**, **Advanced**, **Security**, **WPS**, and **Station List**.

4.2.1 Basic

Choose **Wireless Settings** > **Basic** to display the **Basic Wireless Settings** page.

Basic Wireless Settings

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

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	GP-L200N
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:1F:A4:90:39:C8
Frequency (Channel)	2437MHz (Channel 6) ▾
Wireless Distribution System(WDS)	
WDS Mode	Disable ▾
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel Band/Width	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto ▾
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10) ▾
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Other	
HT TxStream	1 ▾
HT RxStream	1 ▾

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

Wireless Network

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	GP-L200N
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:1F:A4:90:39:C8
Frequency (Channel)	2437MHz (Channel 6) ▾

The following table describes parameters in the **Wireless Network** pane:

Field	Description
Radio On/Off	Enable or disable the wireless LAN interface.
Network Mode	<p>You can select a proper network mode in the drop-down list:</p> <ul style="list-style-type: none"> ● 11b/g mixed mode ● 11b only ● 11g only ● 11a only ● 11a/n mixed ● 11b/g/n mixed mode (default)
Network Name	The maximum length of the SSID is 32 characters. The

Field	Description
(SSID)	legal characters include letters, numerals, underline, and the combination of these characters.
Multiple SSID1~6	Wireless security setting can apply for each SSID independently.
Broadcast Network Name (SSID)	Whether to broadcast SSID. After this function is enabled, the AP broadcasts its SSID.
AP Isolation	Enable or disable isolation among AP clients. After this function is enabled, the client terminals that connect to the same AP cannot communicate with each other.
MBSSID AP Isolation	Enable or disable isolation among different SSIDs. After this function is enabled, the client terminals with different SSIDs cannot communicate with each other.
BSSID	The MAC address of the wireless interface.
Frequency (Channel)	You can select a proper channel from the drop-down list. The default is Channel 6 .

Wireless Distribution System (WDS)

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

(1) Lazy Mode

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

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

The following table describes parameters in the **Lazy Mode**:

Field	Description
-------	-------------

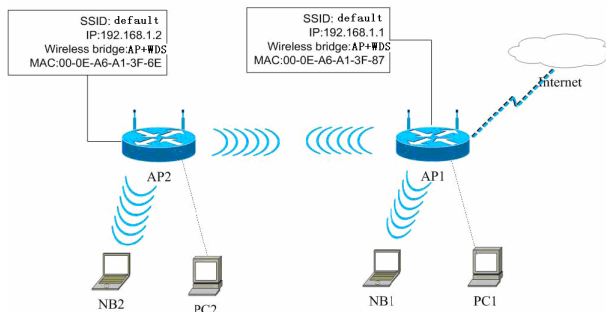
Field	Description
WDS Mode	Select Lazy Mode from the drop-down list.
Phy Mode	You can select CCK , OFDM , HTMIX , or GREENFIELD .
Encryp Type	You can select NONE , WEP , TKIP , or AES . If you select WEP , TKIP , or AES , you need to set the encryption key.
Encryp Key	Enter the encryption key.

Step 1 In the **Basic Wireless Settings** page, set the **WDS Mode** to **Lazy Mode**, set the same **Phy Mode** and **Encryp Type** as the peer AP, and enter the MAC address of the peer AP. Then, click **Apply** to save the settings.

Step 2 Choose **Wireless Settings > Security**. In the **Wireless Security/Encryption Settings** page that is displayed, set the **Security Mode** of the GP-L200N to accord with the peer AP.

(2) Bridge Mode

In the bridge mode, you can use the GP-L200N 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 GP-L200N.



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

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▾
Phy Mode	CCK ▾
EncrypType	WEP ▾
Encryp Key	<input type="text"/>
AP MAC Address	<input type="text" value="00:0C:43:28:60:E8"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>

The following table describes parameters in the **Lazy Mode**:

Field	Description
WDS Mode	Select the Bridge Mode .
Phy Mode	You can select CCK , OFDM , HTMIX , or GREENFIELD .
Encryp Type	You can select NONE , WEP , TKIP , or AES . If you select WEP , TKIP , or AES , you need to set the encryption key.
Encryp Key	Enter the encryption key.
AP MAC Address	The MAC address of another AP that connects to the GP-L200N by using WDS.

Step 2 In the **Basic Wireless Settings** page, set the same physical mode and encryption type as the peer AP, enter the MAC address of the peer AP, and then click **Apply** to save the settings. The GP-L200N then works in the **Bridge** mode.

Step 3 Choose **Wireless Settings > Security**. In the **Wireless Security/Encryption Settings** page that is displayed, set the **Security Mode** of the GP-L200N to accord with the peer AP.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	GP-L200N
"GP-L200N"	
Security Mode	<div> <div>Disable</div> <div> <div>Disable</div> <div>OPEN</div> <div>SHARED</div> <div>WEP/AUTO</div> <div>WPA</div> <div>WPA-PSK</div> <div>WPA2</div> <div>WPA2-PSK</div> <div>WPA2PSK</div> <div>WPA1WPA2</div> <div>802.1X</div> </div> </div>
Access Policy	
Policy	
Add a station Mac:	
<div>Apply</div>	

(3) Repeater Mode

In the **Repeater** mode, you can use the GP-L200N to connect to the primary router, for extending the wireless coverage.



Step 1 Choose **Wireless Settings > Basic** to display the **Basic Wireless Settings** page.

Wireless Network	
Radio On/Off	<input type="button" value="RADIO OFF"/>
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	GP-L200N
Multiple SSID1	
Multiple SSID2	
Multiple SSID3	
Multiple SSID4	
Multiple SSID5	
Multiple SSID6	
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:1F:A4:90:39:C8
Frequency (Channel)	2437MHz (Channel 6) ▾

Step 2 Set the **Frequency (Channel)** according to the peer AP (an AP that wants to connect to the GP-L200N by using WDS).


Step 3 In the **Basic Wireless Settings** page, set the WDS mode to **Repeater Mode**, set the same physical mode and encryption type as the peer AP, enter the MAC address of the peer AP, and then click **Apply** to save the settings. The GP-L200N then works in the **Repeater Mode**.

Wireless Distribution System(WDS)	
WDS Mode	Repeater Mode ▾
Phy Mode	CCK ▾
EncryptType	NONE ▾
AP MAC Address	
AP MAC Address	
AP MAC Address	
AP MAC Address	

Step 4 Choose **Wireless Settings > Security** to display the **Wireless Security/Encryption Settings** page.

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Auto
MCS	Auto
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The following table describes parameters in the **HT Physical Mode** pane:

Field	Description
Operation Mode	You can select Mixed Mode or Green Field . The default is Mixed Mode .
Channel BandWidth	You can select 20 or 20/40 . The default is 20/40 .
Guard Interval	You can select Long or Auto . The default is Auto .
MCS	The value should be in the range of 0 to 32. The default is Auto .
Reverse Direction Grant (RDG)	You can select Disable or Enable . The default is Enable .
Extension Channel	<p>When the channel bandwidth is set to 20/40 MHz, the extension channel provides a channel that is adjacent to the primary channel but is not overlapped. The wireless network acquires diploid bandwidth by this extension channel, that is, 20MHz bandwidth.</p> <p> 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 the primary bandwidth and the other is the</p>

Field	Description
	secondary. When the data is being transmitted, the channel can act as either 40MHz bandwidth or 20 MHz bandwidth independently. In this way, the data rate is doubled.
Aggregation MSDU (A-MSDU)	<p>Enable or disable A-MSDU.</p> <p>MSDU is the aggregation of multiple MSDUs by using certain method and the multiple MSDUs forms a greater load. The MSDU can be regarded as the Ethernet message. Usually, when an AP or a wireless client receives MSDUs from a protocol stack, the MSDUs are marked with the Ethernet message header (also called A-MSDU Subframes). Before being sent out, the A-MSDU Subframes need to be transformed into the message format of 802.11 one by one.</p> <p>A-MSDU aggregates multiple A-MSDU Subframes and encapsulates them into 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.</p>
Auto Block ACK	<p>Enable or disable Auto Block ACK.</p> <p>In order to ensure security of the data transmission, 802.11n protocol requires that if a client receives a unicast frame, the client should immediately send back an ACK frame. After the receiver of A-MPDU receives A-MPDU, the receiver needs to process every MPDU. In that case, the receiver sends out ACK frames to every MPDU. Block Acknowledgement is used to reduce the number of the ACK frames by using an ACK frame.</p>
Decline BA Request	Enable or disable Decline BA Request.

Other

Other	
HT TxStream	1 ▼
HT RxStream	1 ▼

The following table describes parameters of HT TxStream and HT RxStream:

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

4.2.2 Advanced

Choose **Wireless Settings** > **Advanced** to display the **Advanced Wireless Settings** page.

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.

Advanced Wireless	
BG Protection Mode	Auto <input type="button" value="v"/>
Basic Data Rates	Default(1-2-5.5-11 Mbps) <input type="button" value="v"/>
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	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable(only in A band)
Country Code	None <input type="button" value="v"/>

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

In this page, you can configure advanced wireless parameters, such as the beacon interval, data beacon rate, and the Tx power.



Note:

The advanced wireless setting is only for advanced user. For common users, do not change any setting in this page.

Advanced Wireless

The following table describes the primary parameters in the **Advanced Wireless** pane:

Field	Description
BG Protection Mode	You can select On , Off , or Auto . The default is Auto .
Basic Data Rates	You can select 1-2 Mbps , 1-2-5.5-11 Mbps , or 1-2-5.5-6-11-12-24 Mbps . The default is 1-2-5.5-11 Mbps .
Beacon Interval	By default, the data is sent to a station through the wireless beacon signal every 100 ms. The value range is 20~999.
Data Beacon Rate (DTIM)	The default DTIM is 1ms. The range is 1~255.
Fragment Threshold	The default fragment threshold is 2346. The range is 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 is Disable . 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 enables the system to transmit more data during a period of time.
Pkt_Aggregate	Pkt_Aggregate can aggregate multiple data packets together for improving transmission efficiency.

Field	Description
IEEE802.11H Support	By default, it is Disable .
Country Code	Select a proper country code from the drop-down list.

Wi-Fi Multimedia

The following table describes the primary parameters in the **Wi-Fi Multimedia** pane:

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 WMM Configuration 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 Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video Priority	Prioritize video traffic above other data traffic One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	5, 4
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities Traffic less sensitive to latency, but affected by	0, 3

Access Category	Description	802.1d Tags
	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

In the **Wi-Fi Multimedia** pane, click **WMM Configuration** and the following page appears:

WMM Parameters of Access Point						
	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	3	15	63	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7	15	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3	7	47	<input type="checkbox"/>	<input type="checkbox"/>

WMM Parameters of Station					
	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	<input type="checkbox"/>
AC_BK	7	15	1023	0	<input type="checkbox"/>
AC_VI	2	7	15	94	<input type="checkbox"/>
AC_VO	2	3	7	47	<input type="checkbox"/>

In this page, you can configure the WMM parameters of the access point and the station. The following table describes the parameters:

Field	Description
Aifsn	Aifsn (Arbitrary Inter-Frame Space Number). It affects the delay time of WMM access category. If you use voice or video service, set smaller values for AC_VI and AC_VO. If it is E-mail or Web service, set greater values for AC_BE and AC_BK.
CWMin	Cwmin (Mini. Contention Window) also affects 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 greater.
CWMax	It indicates the Maximum Contention Window.
Txop	Txop (Opportunity to Transmit) can optimize the WMM access. Compared with the WMM access that needs a higher priority, such as AC_VI and AC_VO, this value should be greater.
ACM	ACM (Admission Control Mandatory) only takes effect on AC_VI and AC_VO. The value of 0 indicates that the AP is in the charge of the

Field	Description
	access commands. The value 1 indicates that the client is in the charge of the access commands.
Ackpolicy	When WMM packets are being transmitting, AP receives an echo request. The value of 0 indicates that the AP does not send back an echo request, which brings positive effect for WMM. The value 1 indicates that the AP generates a response to the request.

**Note:**

The GP-L200N provides standard WMM settings. If you want to modify the parameters, please refer to the WMM settings of your WMM products.

(3) DLS (Direct Link Setup)

The GP-L200N 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 GP-L200N. In this way, the two WMM devices can transmit message directly.

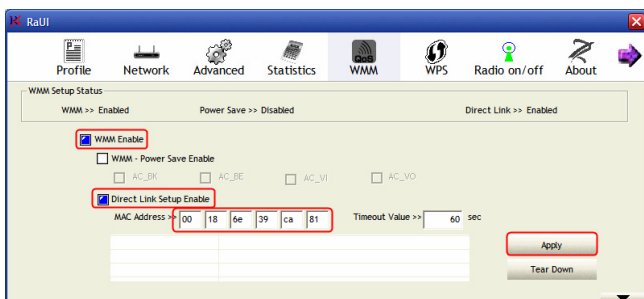
If you want to configure WMM DLS, do as follows:

Step 1 Prepare two wireless network cards (A and B) and one GP-L200N.

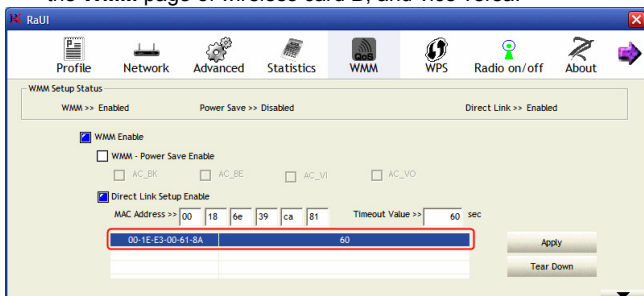
Step 2 Enable the DLS function on the **Advanced Wireless Settings** page.

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WMM Parameters	WMM Configuration

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



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



Multicast-to-Unicast Converter



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

4.2.3 Security

Choose **Wireless Settings** > **Security** to display the **Wireless Security/Encryption Settings** page.

Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	GP-L200N ▼
"GP-L200N"	
Security Mode	Disable ▼
Access Policy	
Policy	Disable ▼
Add a station Mac:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

In this page, you can set wireless security mode and the encryption key, to prevent unauthorized access or monitoring.

Select SSID

Select SSID	
SSID choice	GP-L200N ▼

SSID choice: select an SSID that you want to configure.

Security Mode

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

(1) **OPEN**

"GP-L200N"			
Security Mode		OPEN	
Wire Equivalence Protection (WEP)			
Default Key		Key 1	
WEP Keys	WEP Key 1 :		Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

The following table describes parameters of the **OPEN** mode:

Field	Description
Security Mode	Select OPEN .
Default Key	Select a key as the default key.
WEP Keys (WEP Key 1-4)	Set 64-bit or 128-bit key. The key format is Hex or ASCII .

(2) SHARED

"GP-L200N"			
Security Mode		SHARED	
Encrypt Type		WEP	
Wire Equivalence Protection (WEP)			
Default Key		Key 1	
WEP Keys	WEP Key 1 :		Hex
	WEP Key 2 :		Hex
	WEP Key 3 :		Hex
	WEP Key 4 :		Hex

The following table describes parameters of the **SHARED** mode:

Field	Description
Security Mode	Select SHARED .

Field	Description
Encrypt Type	You can select WEP or None .
Default Key	Select a key as the default key.
WEP Keys (WEP Key1-4)	Set 64-bit or 128-bit key. The key format is Hex or ASCII .

(3) **WEPAUTO**

"GP-L200N"			
Security Mode		WEPAUTO ▼	
Wire Equivalence Protection (WEP)			
Default Key		Key 1 ▼	
WEP Keys	WEP Key 1 :	<input type="text"/>	Hex ▼
	WEP Key 2 :	<input type="text"/>	Hex ▼
	WEP Key 3 :	<input type="text"/>	Hex ▼
	WEP Key 4 :	<input type="text"/>	Hex ▼

Parameter descriptions of the **WEPAUTO** mode are similar to those of the **OPEN** mode.

(4) **WPA**

"GP-L200N"	
Security Mode	WPA
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The following table describes parameters of the **WPA** mode:

Field	Description
Security Mode	Select WPA .
WPA Algorithms	You can select TKIP or AES .
Key Renewal Interval	Set the key renewal interval, in unit of seconds.
IP Address	The IP address of the Radius server.
Port	The default port number is 1812. You can change it according to the server setting.
Shared Secret	The shared key that is required for authentication at the Radius server.
Session Timeout	The value of 0 indicates no session time limit.
Idle Timeout	Set the idle timeout.

(5) **WPA-PSK**

"GP-L200N"	
Security Mode	WPA-PSK

WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

The following table describes parameters of the **WPA-PSK** mode:

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

(6) **WPA2**

"GP-L200N"	
Security Mode	WPA2

WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
PMK Cache Period	10 minute
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The following table describes parameters of the **WPA2** mode:

Field	Description
Security Mode	Select WPA2 .
WPA Algorithms	You can select TKIP , AES , or TKIPAES .
Key Renewal Interval	Set the key renewal interval.
PMK Cache Period	Set the PMK (Pairwise Master Key) cache 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.
IP Address	The IP address of the Radius server.
Port	The default port number is 1812. You can change it according to the server setting.
Shared Secret	The shared key that is required for authentication at the Radius server.
Session Timeout	The value of 0 indicates no session time limit.
Idle Timeout	Set the idle timeout.

(7) **WPA2-PSK**

"GP-L200N"	
Security Mode	WPA2-PSK
WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

The following table describes parameters of the **WPA2-PSK** mode:

Field	Description
Security Mode	Select WPA2-PSK .
WPA Algorithms	You can select TKIP , AES , or TKIPAES .
Pass Phrase	Set 8-bit or 64-bit key.

Field	Description
Key Renewal Interval	Set the key renewal interval.

(8) **WPAPSKWPA2PSK**

"GP-L200N"	
Security Mode	WPAPSKWPA2PSK ▼
WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

Parameter descriptions of the WPAPSKWPA2PSK mode are similar to those of **WPA2-PSK**.

(9) **WPA1WPA2**

"GP-L200N"	
Security Mode	WPA1WPA2 ▼
WPA	
WPA Algorithms	<input checked="" type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> TKIPAES
Key Renewal Interval	3600 seconds
Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

The following table describes parameters of the **WPA1WPA2** mode:

Field	Description
Security Mode	Select WPA1WPA2 .

Field	Description
WPA Algorithms	You can select TKIP , AES , or TKIPAES .
Key Renewal Interval	Set the key renewal interval.
IP Address	The IP address of the Radius server.
Port	The default port number is 1812. You can change it according to the server setting.
Shared Secret	The shared key that is required for authentication at the Radius server.
Session Timeout	The value of 0 indicates no session time limit.
Idle Timeout	Set the idle timeout.

(10) **802.1X**

GP-L200N

Security Mode

802.1X

802.1x WEP

WEP

☐ Disable
☐ Enable

Radius Server

IP Address

Port

1812

Shared Secret

Session Timeout

0

Idle Timeout

The following table describes parameters of the **802.1X** modes:

Field	Description
Security Mode	Select 802.1X .
IP Address	The IP address of the Radius server.
Port	The default port number is 1812. You can change it according to the server setting.
Shared Secret	The shared key that is required for authentication at the Radius server.
Session Timeout	The value of 0 indicates no session time limit.

Field	Description
Idle Timeout	Set the idle timeout.

Access Policy

The following table describes parameters of parameters in the **Access Policy** pane:

Field	Description
Policy	<ul style="list-style-type: none"> ● Disable: Stop access control to the wireless devices in the MAC list. ● Allow: Allow access control to the wireless devices in the MAC list. ● Reject: Reject access control to the wireless devices in the MAC list.
Add a station Mac	Enter the MAC address of wireless device that you want to allow or reject.

After setting, click **Apply** to save the settings.

4.2.4 WPS

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

Wi-Fi Protected Setup

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

WPS Config	
WPS:	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/>	

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	GP-L200N
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	94519761
<input type="button" value="Reset OOB"/>	

WPS Progress	
WPS mode	<input type="radio"/> PIN <input checked="" type="radio"/> PBC
<input type="button" value="Apply"/>	

WPS Status	
WSC: Idle	

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

WPS Config

WPS Config	
WPS:	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/>	

WPS: Enable or disable WPS.

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

WPS Summary

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	GP-L200N
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	94519761
<input type="button" value="Reset OOB"/>	

The **WPS Summary** pane displays the preset WPS information, such as WPS current status, WPS authentication mode, and WPS encryption type.

Click **Reset OOB** 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. In **Enrollee** and **Registrar** modes, PIN code negotiation should be applied.

(1) Enrollee Mode

- Step 1 Select the **Enrollee** mode on the wireless client and the software of wireless client generates a random PIN code, for example, 12345678.
- Step 2 In the **Wi-Fi Protected Setup** page, enter the PIN code of wireless client, for example, 12345678.
- Step 3 Click **Apply** on the **Wi-Fi Protected Setup** page to submit the settings.

WPS Progress	
WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN	<input type="text" value="12345678"/>
<input type="button" value="Apply"/>	

(2) **Registrar Mode**

Step 1 View the AP PIN on the **Wi-Fi Protected Setup** page, for example, 94519761.

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	GP-L200N
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	94519761
<input type="button" value="Reset OOB"/>	

Step 2 Select **Registrar** mode on the wireless client and enter the PIN code of the GP-L200N. See the following figure:

The screenshot shows a software interface with a top navigation bar containing icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main area is titled 'WPS AP List' and shows details for a device with ID 'default', MAC '00-E0-4C-81-86-D1', and SSID 'EzReg@W277000'. Below this is the 'WPS Profile List' section, which includes checkboxes for 'PIN', 'PBC', 'WPS Associate IE', 'WPS Probe IE', and 'Auto'. The 'WPS status' is shown as 'disconnected'. On the right side, there is a 'WPS' configuration panel with a 'Pin Code' field containing '94519761', a 'Config Mode' dropdown menu set to 'Registrar', and buttons for 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.

(3) **PBC Mode**

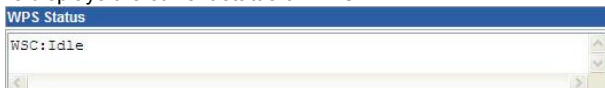
Step 1 In the **Wi-Fi Protected Setup** page, select the **PBC** mode and click **Apply**. You can also press the **WPS** button on the rear panel.

WPS Progress	
WPS mode	<input type="radio"/> PIN <input checked="" type="radio"/> PBC
<input type="button" value="Apply"/>	

- Step 2 Enable the PBC function on the wireless client. In that case, connection is automatically established between the GP-L200N and the wireless client.

WPS Status

This pane displays the current status of WPS.



4.2.5 Station List

Choose **Wireless Settings** > **Station List** to display the **Station List** page.

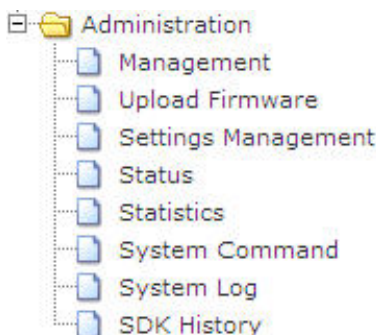
You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00:1E:4C:39:E4:46	1	1	0	1	20M	0	0
00:1B:77:03:7D:FB	2	1	0	5	20M	0	0

In this page, you can view the wireless networks that connect to the GP-L200N. If a new wireless network connects to the GP-L200N, refresh this page and the connection information of the new wireless network is also displayed.

4.3 Administration

The following figure shows the navigation menu of the **Administration**:



The sub-menus of the **Administration** contain **Management**, **Upload Firmware**, **Settings Management**, **Status**, **Statistics**, **System Command**, **System Log** and **SDK History**.

4.3.1 Management

Choose **Administration > Management** to display the **System Management** page.

System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Administrator Settings	
Account	<input type="text" value="admin"/>
Password	<input type="password" value="••••"/>
<div>Apply Cancel</div>	

The following table describes the parameters in this page:

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 restores to the factory default settings. The default account and the password are **admin** and **admin** respectively.

4.3.2 Upload Firmware

Choose **Administration > Upload Firmware** to display the **Upload Firmware** page.

Upgrade Firmware

Upgrade the Ralink SoC firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

The screenshot shows two web forms. The top form is titled 'Update Firmware' and has a 'Location:' label, a text input field, a 'Browse...' button, and an 'Apply' button. The bottom form is titled 'Update Bootloader' and has the same layout with 'Location:', a text input field, a 'Browse...' button, and an 'Apply' button.

To upload the firmware of the GP-L200N, click **Browse...** to select the correct firmware and click **Apply**. The system begins to upgrade firmware.

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

The procedure for upgrading the Bootloader is similar to the procedure for upgrading the firmware.

**Note:**

After the firmware is upgraded, the AP restores to the factory defaults. To avoid data 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

Choose **Administration > Settings Management** to display the **Settings Management** page.

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.

The screenshot displays the 'Settings Management' interface with three distinct sections:

- Export Settings:** Contains a text field labeled 'Export Button' and an 'Export' button.
- Import Settings:** Contains a text field labeled 'Settings file location', a 'Browse...' button, and 'Import' and 'Cancel' buttons.
- Load Factory Defaults:** Contains a text field labeled 'Load Default Button' and a 'Load Default' button.

The following table describes parameters in this page:

Field	Description
Export Settings	Click Export to export the settings to your local PC.
Import Settings	Click Browse... to select the configuration file on your PC and click Import to import the settings to AP.
Load Factory Defaults	Click Load Default and the system restores to the factory default settings.

4.3.4 Status

Choose **Administration > Status** to display the **Access Point Status** page.

Access Point Status

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

System Info	
SDK Version	3.4.1.0 (Nov 19 2010)
System Up Time	1 hour, 31 mins, 4 secs
System Platform	RT3050 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	192.168.1.1
Primary Domain Name Server	192.168.1.5
Secondary Domain Name Server	168.95.1.1
MAC Address	00:1F:A4:90:39:C8
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:1F:A4:90:39:C8

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

4.3.5 Statistic

Choose the **Administration > Statistics** to display the **Statistic** page.

Statistic

Take a look at the Ralink SoC statistics

Memory	
Memory total:	13832 kB
Memory left:	2972 kB
LAN	
LAN Rx packets:	3315
LAN Rx bytes:	421071
LAN Tx packets:	5412
LAN Tx bytes:	2090858
All interfaces	
Name	eth2
Rx Packet	3349
Rx Byte	470781
Tx Packet	5411
Tx Byte	2098505
Name	lo
Rx Packet	89
Rx Byte	13674
Tx Packet	89
Tx Byte	13674
Name	ra0
Rx Packet	149367
Rx Byte	36951471
Tx Packet	8039
Tx Byte	403680
Name	wds0
Rx Packet	0
Rx Byte	0
Tx Packet	-1
Tx Byte	-1
Name	wds1
Rx Packet	0
Rx Byte	0
Tx Packet	-1
Tx Byte	-1
Name	wds2
Rx Packet	0
Rx Byte	0
Tx Packet	-1
Tx Byte	-1

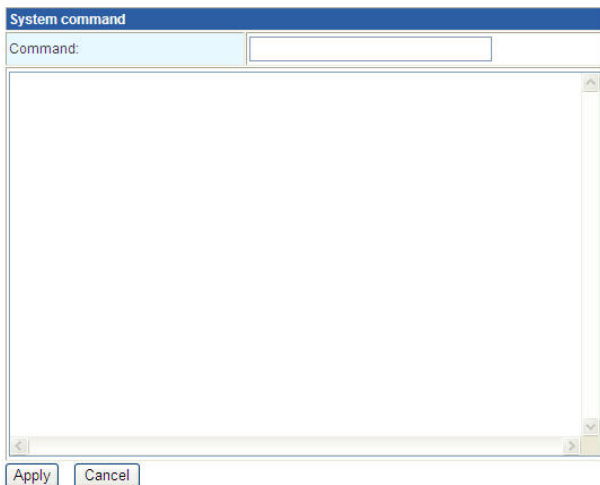
This page displays the memory status, the numbers of transmitted and received data packets of the WLAN, LAN, and WAN.

4.3.6 System Command

Choose **Administration > System Command** to display the **System Command** page.

System Command

Run a system command as root:



The screenshot shows a web browser window titled "System command". Inside the window, there is a label "Command:" followed by a text input field. Below the input field is a large, empty rectangular area, likely a command prompt or output display. At the bottom of the window, there are two buttons: "Apply" and "Cancel".

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

4.3.7 System Log

Choose **Administration > System Log** to display the **System Log** page.

System Log

Syslog:

Refresh

Clear

```

System Log
Jan 1 00:00:13 (none) user.info kernel: serial8250: ttyS1 at I/O 0xb0000c00 (ir
Jan 1 00:00:13 (none) user.info kernel: loop: loaded (max 8 devices)
Jan 1 00:00:13 (none) user.warn kernel: rdm_major = 254
Jan 1 00:00:13 (none) user.warn kernel: GDMA1_MAC_ADDRH -- : 0x00000000
Jan 1 00:00:13 (none) user.warn kernel: GDMA1_MAC_ADDRH -- : 0x00000000
Jan 1 00:00:13 (none) user.warn kernel: Ralink APSoC Ethernet Driver Initializat
Jan 1 00:00:13 (none) user.warn kernel: GDMA1_MAC_ADDRH -- : 0x0000001f
Jan 1 00:00:13 (none) user.warn kernel: GDMA1_MAC_ADDRH -- : 0xa49039c8
Jan 1 00:00:13 (none) user.alert kernel: PROC INIT OK!
Jan 1 00:00:13 (none) user.info kernel: PPP generic driver version 2.4.2
Jan 1 00:00:13 (none) user.info kernel: PPP BSD Compression module registered
Jan 1 00:00:13 (none) user.info kernel: NET: Registered protocol family 24
Jan 1 00:00:13 (none) user.info kernel: block2mtd: version $Revision: 1.1.1.1 $
Jan 1 00:00:13 (none) user.warn kernel: nf_conntrack version 0.5.0 (128
Jan 1 00:00:13 (none) user.info kernel: buckets, 1024 max)
Jan 1 00:00:13 (none) user.warn kernel: ip_tables: (C) 2000-2006 Netfilter Core
Jan 1 00:00:13 (none) user.info kernel: TCP cubic registered
Jan 1 00:00:13 (none) user.info kernel: NET: Registered protocol family 1
Jan 1 00:00:13 (none) user.info kernel: NET: Registered protocol family 10
Jan 1 00:00:13 (none) user.info kernel: NET: Registered protocol family 17
Jan 1 00:00:13 (none) user.info kernel: 802.1Q VLAN Support v1.8 Ben Greear <gr
Jan 1 00:00:13 (none) user.info kernel: All bugs added by David S. Miller <dave
Jan 1 00:00:13 (none) user.warn kernel: VFS: Mounted root (squashfs filesystem)
Jan 1 00:00:13 (none) user.info kernel: Freeing unused kernel memory: 108k free
Jan 1 00:00:13 (none) user.warn kernel: Algorithmics/MIPS FPU Emulator v1.5
Jan 1 00:00:13 (none) user.err kernel: devpts: called with bogus options
Jan 1 00:00:13 (none) user.warn kernel:
Jan 1 00:00:13 (none) user.warn kernel: phy_tx_ring = 0x00ed6000, tx_ring = 0xa
Jan 1 00:00:13 (none) user.warn kernel:
Jan 1 00:00:13 (none) user.warn kernel: phy_rx_ring = 0x00ed7000, rx_ring = 0xa
Jan 1 00:00:13 (none) user.warn kernel: RT305X_ESW: Link Status Changed
Jan 1 00:00:13 (none) user.warn kernel: CDMA_CSG_CFG = 81000007
Jan 1 00:00:13 (none) user.warn kernel: GDMA1_FWD_CFG = 710000
Jan 1 00:00:13 (none) user.warn kernel: RT305X_ESW: Link Status Changed
Jan 1 00:00:13 (none) user.warn kernel: RT305X_ESW: Link Status Changed
Jan 1 00:00:13 (none) user.warn kernel: rt2860v2_ap: module license 'unspecific
Jan 1 00:00:13 (none) user.warn kernel: 0x1300 = 00064380
Jan 1 00:00:13 (none) user.warn kernel: eth2.2: Setting MAC address to 00 1f a
Jan 1 00:00:13 (none) user.warn kernel: VLAN (eth2.2): Underlying device (eth2
Jan 1 00:00:13 (none) user.debug kernel: eth2.1: add 33:33:00:00:00:01 mcst ad
Jan 1 00:00:13 (none) user.debug kernel: eth2.1: add 01:00:5e:00:00:01 mcst ad
Jan 1 00:00:13 (none) user.debug kernel: eth2.1: add 33:33:ff:90:39:c8 mcst ad
Jan 1 00:00:13 (none) user.debug kernel: eth2.2: add 33:33:00:00:00:01 mcst ad
Jan 1 00:00:13 (none) user.debug kernel: eth2.2: add 01:00:5e:00:00:01 mcst ad
Jan 1 00:00:13 (none) user.debug kernel: eth2.2: add 33:33:ff:90:39:c8 mcst ad
Jan 1 00:00:13 (none) user.info kernel: device ra0 entered promiscuous mode
Jan 1 00:00:13 (none) user.info kernel: device eth2 entered promiscuous mode
Jan 1 00:00:13 (none) user.info kernel: br0: port 2(eth2) entering learning sta
Jan 1 00:00:13 (none) user.info kernel: br0: port 1(ra0) entering learning stat
Jan 1 00:00:13 (none) user.info kernel: br0: port 2(eth2) entering disabled sta

```

In this page, you can set the log server and view the system log.

After enabling the remote log server and entering the IP address of the server, click **Apply**, and then the log information is sent to the remote log server.

4.3.8 SDK History

Choose **Administration > SDK History** to display the **SDK History** page.

Ralink AP SDK - History

Version 3.4.1.0

New Feature:

- [WebUI/NVRAM] add RT3092AP DLS GUI
- [WebUI] R/V T GUI

App update:

- [Reset] adjust Default settings
- [Script] support GPL with driver insert/remove module

Fixed bug:

- [GPIO] Fix bug for GPIO=24~51
- [GPIO] add RALINK_GPIO_HAS_5124 for gpio24~gpio51
- [WebUI] STA site_survey error
- [WebUI] AP/STA display/Setting bugs
- [WebUI] WPA/WPA_Supplicant Certificate upload
- [BusyBox] Syslogd - avoid the read-only filesystem
- [Raether] MTU bug
- [Raether] Reorder the sequence of ei_close
- [Script] greenap.sh supports for MBSSID
- [Compile] sdk will compile goahead before matrix, so we should modify goahead's Makefile to compile matrix first
- [VPN] Multiple PPTP VPN pass through sessions are able to connect successfully for RT2880
- [NVRAM] rt3052 + i2s enabled => load default button's gpio=43

Version 3.4.0.0

New Chip Support:

- [SDK] RT3883 support
- [SDK] RT3652 support
- [SDK] RT3350 support

New Feature:

- [Linux] Ralink Flow Classifier
- [Linux] Linux-based Watchdog driver (/dev/watchdog)
- [WebUI] WPS supplicant support
- [SDK] More 3G data card support
- [App] video Flow Classification Command
- [App] Firewall - Portscan, Syn flood prevention, Snort Support
- [App] ITune Server support
- [App] User space watchdog daemon
- [App] cURL
- [App] Expat-C library for parsing XML
- [App] mpsstat
- [App] user space daemon supported 802.11f protocol
- [App] net-snmp 5.5
- [Web] Add WPS GUI for 2nd wireless interface
- [Web] Add WAPI GUI for 1st wireless interface
- [Web] Add WPA Supplicant GUI
- [Web] Add Wizard
- [Lib] Perl Compatible Regular Expressions
- [Lib] zlib-1.2.3
- [Lib] libcap-1.0
- [Lib] libncurses-5.7

Peripheral Components:

- [I2S] audio codec WM8750 support for I2S TX/RX
- [PCM] Multi-SPI for PCM SLIC supported

Fixed bug:

- [PCM] assign next unmask channel every DMA done.
- [I2S] Change audio codec sampling rate to the nearest frequency settings.
- [WebUI] 3G PIN, APN, Password, Username, and Dial number support
- [WebUI] 3G auto-connect mode support
- [USB] OTG USB driver bug fix
- [NVRAM] fix commit length threshold
- [NVRAM] fix memory leak bug
- [App] IGMP Proxy issues fixed. (see History in user/igmp/scrip3052.c)

In this page, you can view the new features, updates, and fixed bugs in the current version of the device.

5 Install the PowerLine Utility

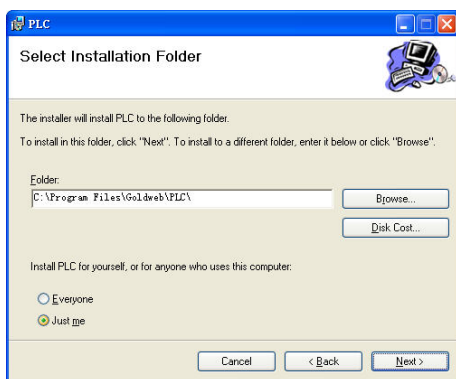
Before installing the PowerLine Utility, you need to verify that there is no other Powerline Utility installed on your computer. If another utility is already installed, please uninstall it and restart your computer.

Insert the Utility CD-ROM into the CD-ROM drive, select the **PowerLine Utility Installation** folder and runs the setup.exe. Follow the steps to install the Utility Program. No password or CD-Key is needed.

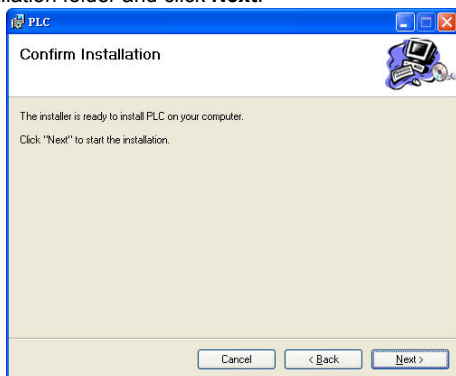
The installation utility similar to the following figure appears.



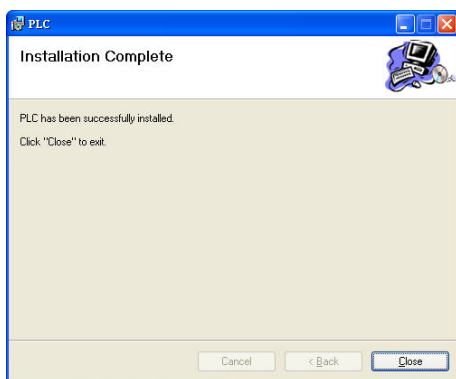
Click **Next** to continue.



Select the installation folder and click **Next**.



Confirm the installation and click **Next**. Wait until the following figure appears:



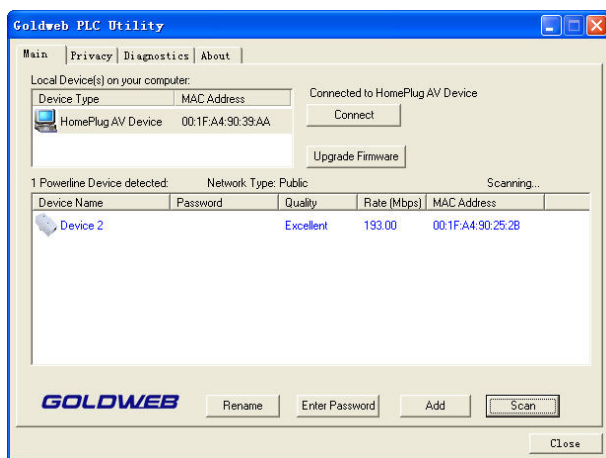
Click **Close** to complete installation.

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 the local HomePlug device connected to the network interface card (NIC) of the computer. You can click **Connect** on the right. Once connected to the local device, the utility automatically scans the powerline periodically for any other HomePlug devices. If no local HomePlug device is discovered, the status area above the **Connect** button displays a message '**NO HOMEPLUG ADAPTERS DETECTED**'.



The lower panel displays all the remote HomePlug devices discovered in the current logical network. The total number of remote devices connected on the same network is displayed on top of the Remote device panel. The **Network Type** (Public or Private) is also displayed according to the network status of the local

device. The scan status option is displayed in the upper right corner of the Remote device panel, indicating whether the Autoscanner functionality is turned on. The following information is displayed for all devices that appear in the lower panel.

Device Name

This column shows the default device name, which can be user re-defined. You can change the name by either clicking **Rename** in the lower area of the window or clicking the name and editing in the table.

Password

This column is blank by default and you can click **Enter Password** to set a password.

To set the **Password** of the device (required when creating a private network), click the name of a device in the lower panel to select the device and click **Enter Password**. In the window that is displayed, enter the password and click **OK**. The **Password** field accepts is not case-sensitive and can contain dashes.

A dialog box appears, asking whether the password is entered correctly. If a device is not found, you are notified along with the suggestions to resolve common problems. This process may take a few seconds.



MAC Address

This column shows the MAC address of the remote device.

Add

This button is used to add a remote device to the existing network by entering the device password of the device. Click **Add** and in the window that is displayed, enter a device name and the password. See the following figure:



A dialog box appears, asking whether the password is entered correctly and whether the device is found in the powerline network. If a device is not found, you are notified along with the suggestions to resolve common problems.

**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 is displayed.

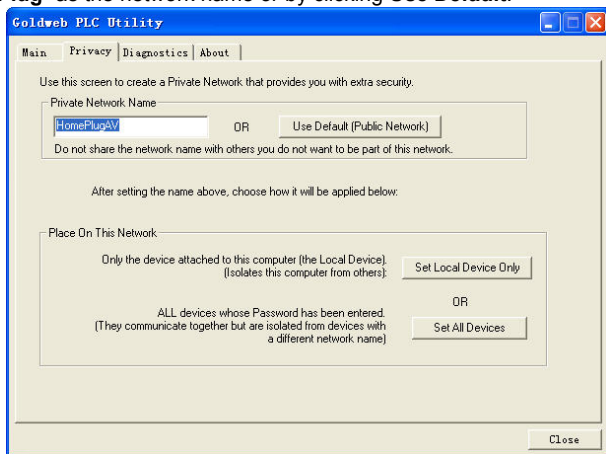
Scan

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 displayed information.

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 **Use Default**.

**Note:**

If the network name is changed to anything other than HomePlug, the **Network Type** in the main tab is displayed 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 shown in the **Main** tab prior to this are no longer present in the new network, effectively making the local devices not to communicate to the devices that are in the old logical

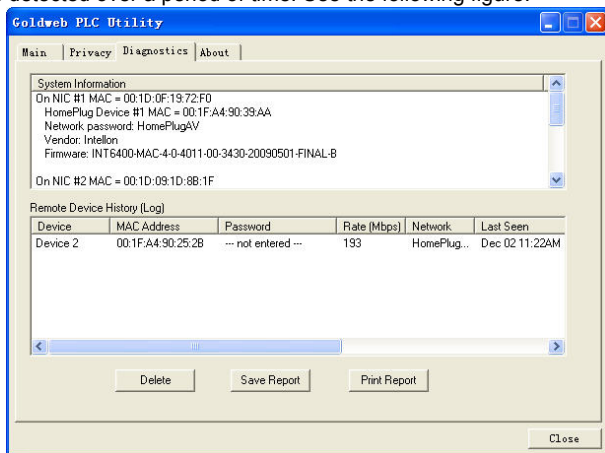
network. Devices previously set up with the same logical network (same network name) appear in the device list after this option is selected.

Set All Devices

This button is used to change the logical network of all devices that appear in the **Main** tab whose Device Password is entered for the same logical network. A window appears, indicating successful operation. For devices whose device passwords are not entered, this operation fails and a failure message is displayed.

6.3 Diagnostics Tab

The **Diagnostics** tab shows the system information and a history of all remote devices detected over a period of time. See the following figure:



The upper panel shows the technical data of the software and hardware in the host computer that is used to communicate over HomePlug on the Powerline network. It contains the following:

- Operating System Platform/Version
- Host Network Name
- User Name
- MAC Address of all NICs 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

The lower panel contains a history of all remote devices detected in the computer over a certain period of time. All devices that are in the powerline network are listed along with a few other parameters. For a device that is active in the current logical network, transfer rate is displayed in the **Rate** column; for a device in another network, or a device that no longer exists, “?” is displayed in the **Rate** column. The following remote device information is available in the **Diagnostics** tab:

- 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 can be saved to a text file for later use, or printed for reference for a technical support call. You can click **Delete** to delete devices that are not part of the network anymore. A dialog box appears, asking whether to delete a device whose password is entered.

6.4 About Tab

The **About** tab shows the software version and provides an html link to a website, such as www.goldwebcn.com. Clicking the web address field opens a web browser and takes you directly to the web site.



Preferences

The lower part of the panel displays options for setting the auto-scan feature.

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.

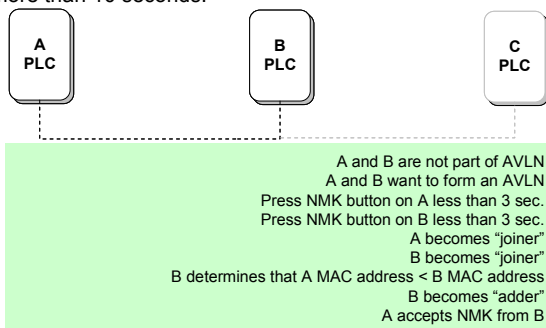
Operation progress and outcome can be monitored by observing the behavior of the Power LED.

7.1 Forming a HomePlug AV logical network

When two devices with different NMK values are connected to the same powerline and want them to form a logical network, do as follows:

- (1) Press the NMK button on the first device A for less than 3 seconds.
- (2) 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.

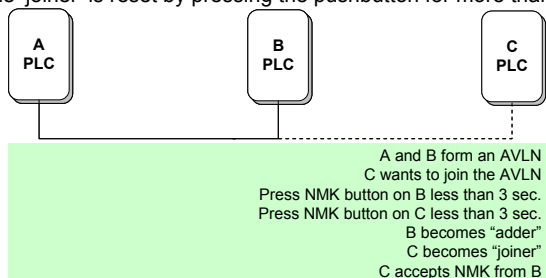


7.2 Joining a Network

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.
- (2) 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.



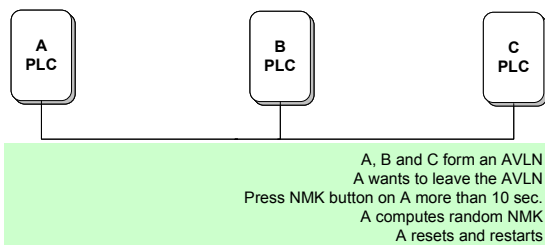
7.3 Leaving a Network

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.

- (1) 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.



8 About PowerLine QoS

The GP-L200N 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.

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

VLAN Tag User Priority	Default CAP Priority	TOS Bit User Priority	Default CAP 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

9 Parameters and Specifications

PLC Module SPEC	
Chipset	Intellon INT6400/INT1400
Serial Flash	16 Mbps
SDRAM:	128 Mbps
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	200 Mbps
Data Rate - TCP/UDP	65 Mbps TCP, 90 Mbps UDP
Modulation Band	2-30 MHz
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 Range	2.4GHz to 2.484GHz
Wireless Signal Rates With Automatic Fallback	11b: 11/5.5/2/1 Mbps 11g: 54/48/36/24/18/12/9/6 Mbps 11n: 150Mbps in 20MHz mode

Transmit Output Power	11n: 13-20 dBm 11g: 14-21 dBm 11b: 16-22 dBm
Receiver Sensitivity	11n: 150Mbps/-69 dBm 11g: 54Mbps/-75 dBm 11b: 11Mbps/-88 dBm
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
System SPEC	
System Support	Windows 98SE, 2000, ME, XP 32/64 bit and Vista 32/64bit
LEDs	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	<ul style="list-style-type: none"> ● 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, 50/60 Hz
EMC and Safety	
Regulatory Compliance	FCC Part 15 Class B, CE
Safety Regulations	UL
Green Standard	RoHS
Physical Characteristics	
Physical Dimension	L×W×H: 170mm×147mm×36.5mm
Weight	291g

Shenzhen Landing Electronics Co.,Ltd

Address: 3F Block A,BaiyingBuilding,No.1019 Nanhai Road,
Nanshan District,Shenzhen,Guangdong, China

Post Code:518067

E-Mail: sales@goldwebcn.com

Website: <http://www.goldwebcn.com>