LevelOne

User Manual

WAP-6101

300Mbps Wireless Ceiling Gigabit PoE Access Point

TABLE OF CONTENTS

Copyright

Trademarks

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.

Chapter 1 Introduction

Congratulations on your purchase of this outstanding product: APC772AM-P01 Business Access Point are designed for small- and medium-sized businesses to extend the existing wired networks and has the ability to operate in different modes and can be used in a wide variety of wireless applications like AP, Point-to-Point. Universal

Repeater Mode not only has an easier setup method, but also provides better performance and compatibility to creates a virtually larger wireless network infrastructure by linking up other access points.

Support Multiple-SSID capability to use one Physical AP to simultaneously emulate 8 APs with different ESSIDs by separate their packets via VLAN technology.

1.1 Contents List

Items	Description	Contents	Quantity
1	**WAP-6101**		1pce
2	**Power Adapter**		1pce
3	**RJ45 Cable**		1pce
4	**CD**		1pce

Hardware Installation

1.2.1 WARNING

Attention

- Do not use the product in high humidity or high temperatures.
- Do not use the same power source for the Product as other equipment. Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the device.
- Do not open or repair the case yourself. If the Product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the Product on a stable surface and avoid using this product and all accessories outdoors.

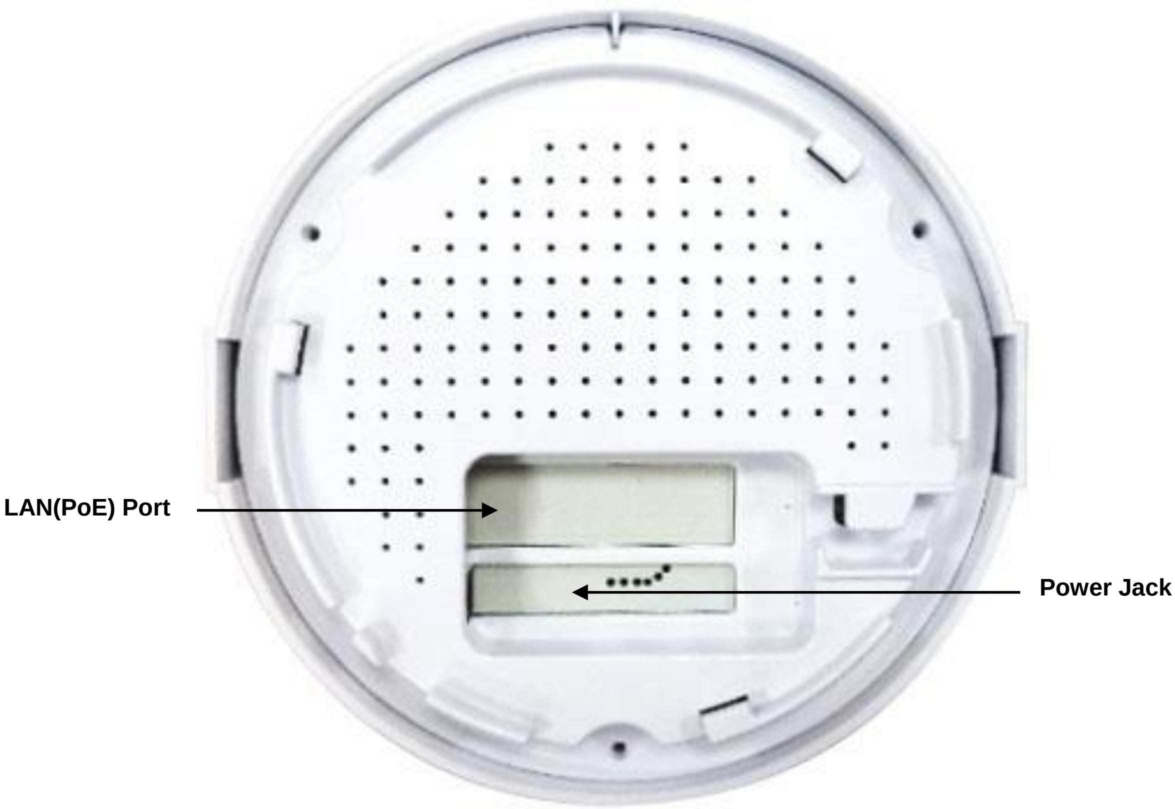
1.2.2 SYSTEM REQUIREMENTS

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11b, g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher (with Java 1.3.1 or higher) Windows® Users: Make sure you have the

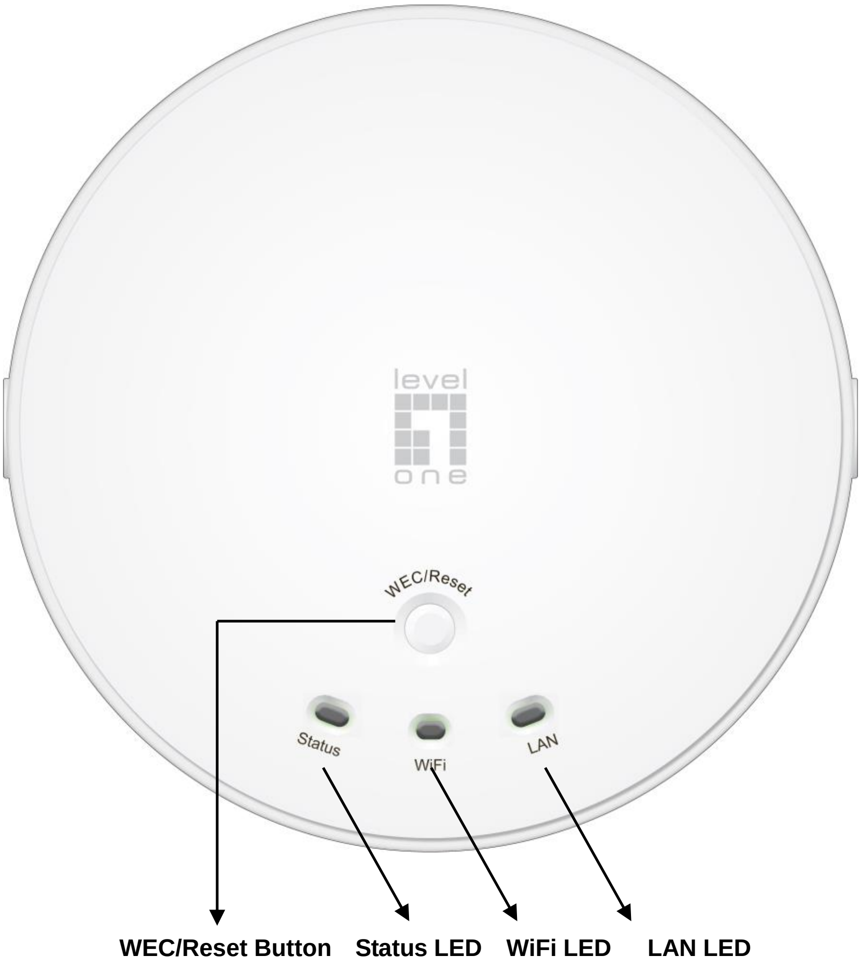
	latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	**Computer with the following:** • Windows® 7, Vista®, or XP with Service Pack 2 • An installed Ethernet adapter • CD-ROM drive

1.2.3 Hardware Configuration

Rear View:



1.2.4 LED Indicators



LED	Description
Status	Change Master Mode / Slave Mode When System is ready: (without click button.) Status LED in Solid : In Master Mode Status LED in Flash: In Slave Mode 1.Press Reset/WEC button 3 sec to trigger WEC or Reset_WEC function; Status LED flash very fast during this period 2.Press Reset/WEC button 5~10 sec till WiFi Dark then release Button to change Mode . Status LED flashes per 0.5 during this period. 3.Press Reset/WEC button 10 ~ 15sec WEC config status release. Status LED flashes per 1 sec during this period 4.Press Reset/WEC button 15 sec to reset to default. Status LED will be blink during this period then device reboot.
	Light Off: The device is power-off
WiFi	Green in flash: data packet transferred. Green in very flash per second during 2min:WPS PBC status When press Reset /WEC Button about 5~10 sec,then WiFi LED will be dark about 20 sec then blink. Dark: Wireless Radio is disable LED in Slow flash: Wireless Connection doesn't establish. LED in Solid : Wireless Connection established successfully.
LAN	LED in flash: data packet transferred

1.2.5 Button Indicators

Button	Description
Rese/WEC (Wireless Easy Connection)	Button for Reset and WEC Functions 1.Press Reset/WEC button 3 sec to trigger WEC or Reset_WEC function; **Status LED flash very fast during this period** 2.Press Reset/WEC button 5~10 sec till WiFi Dark then release Button to change Mode .**Status LED flashes per 0.5 during this period.** 3.Press Reset/WEC button 10 ~ 15sec WEC config status release. **Status LED flashes per 1 sec during this period** 4.Press Reset/WEC button 15 sec to reset to default. **Status LED will be blink during this period then device reboot.**

Chapter 2 Getting Started

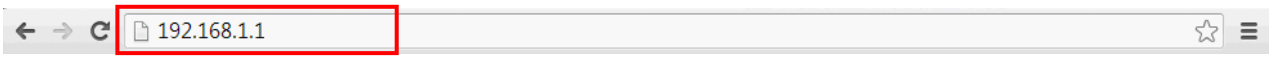
Please use windows EZ setup utility or Web UI wizard to enter the setup process.

2.1 Easy Setup by Configuring Web UI

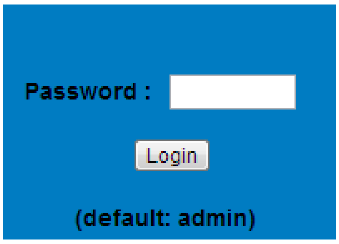
You can also browse web UI to configure the device. Firstly you need to launch the Setup Wizard browser first and then the Setup Wizard will guide you step-by-step to finish the basic setup process.

Browse to Activate the Setup Wizard

Type in the IP Address (**http://192.168.1.1**)

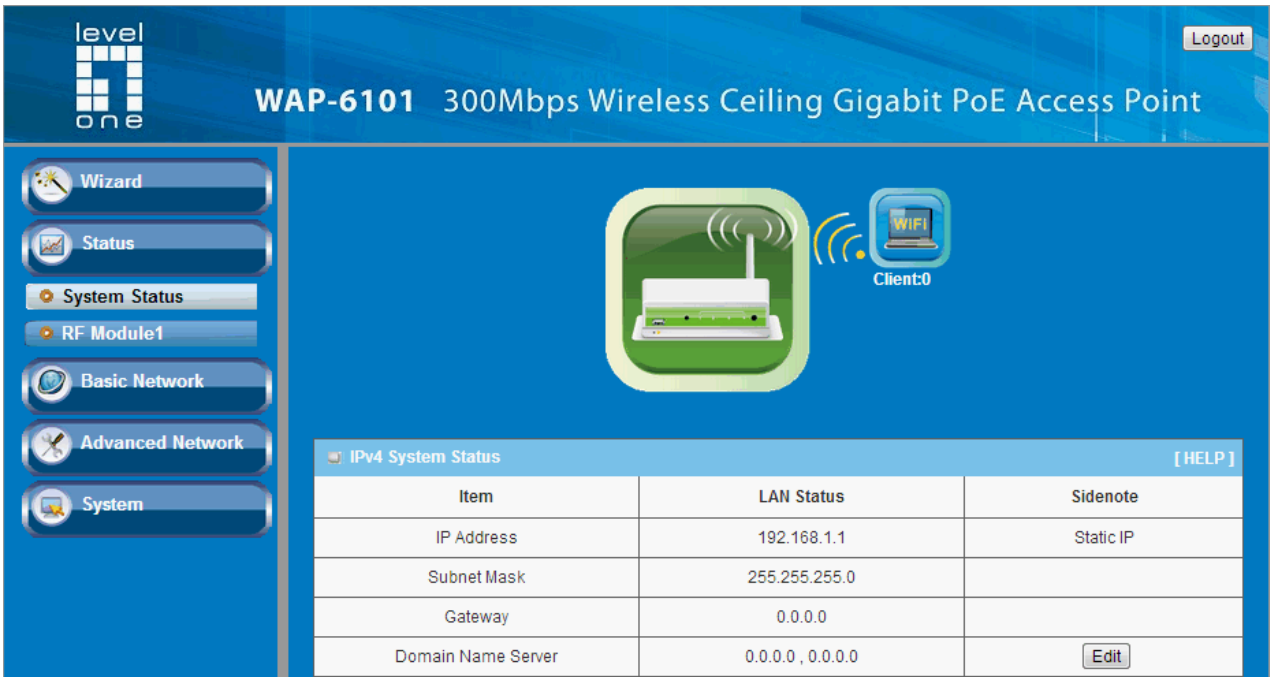


Type the default password **'admin'** in the System Password and then click **'login'** button.



Select **"Wizard"** for basic settings in a simple way.

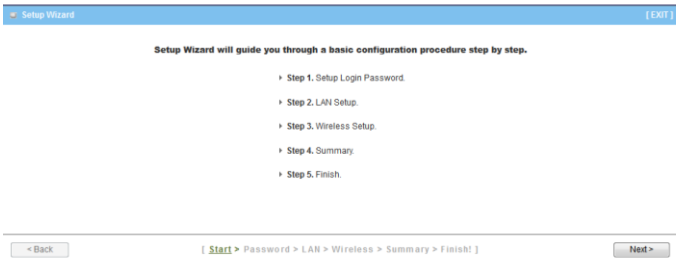
Or, you can go to **Basic Network / Advanced Network / Applications / System** to setup the configuration by your own selection.



IPv4 System Status [HELP]

Item	LAN Status	Sidenote
IP Address	192.168.1.1	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	Edit

Press **"Next"** to start the Setup Wizard.



Setup Wizard [EXIT]

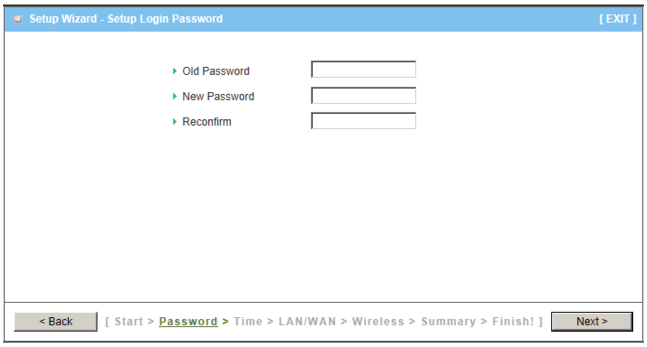
Setup Wizard will guide you through a basic configuration procedure step by step.

- **Step 1.** Setup Login Password.
- **Step 2.** LAN Setup.
- **Step 3.** Wireless Setup.
- **Step 4.** Summary.
- **Step 5.** Finish.

Configure with the Setup Wizard

Step 1

You can change the password of administrator here.



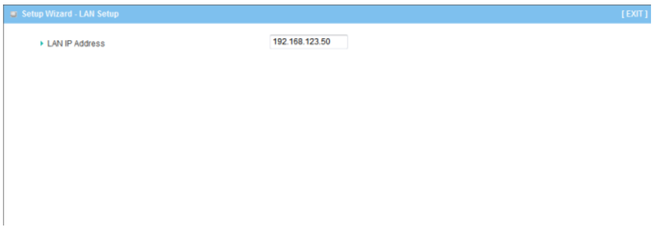
Setup Wizard - Setup Login Password [EXIT]

Old Password
New Password
Reconfirm

< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

Step 2

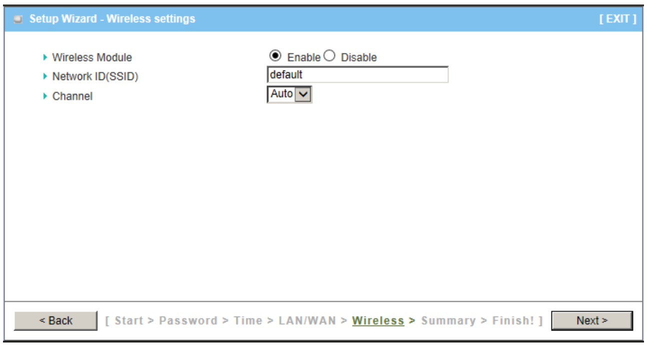
Entry LAN IP Address.



LAN IP Address: 192.168.123.50

Step 3-1

Wireless setting.



Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

Wireless Module: ● Enable ○ Disable

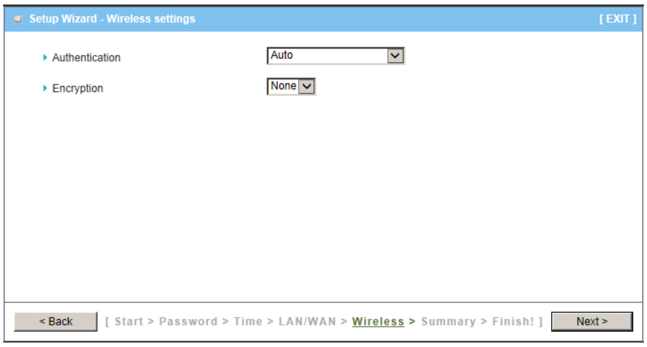
Network ID(SSID): default

Channel: Auto

Step 3-2

Wireless authentication and

encryption.



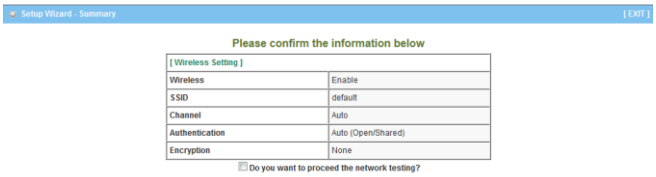
Setup Wizard - Wireless settings
[EXIT]
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

Authentication: Auto

Encryption: None

Step 4

Check the information again.



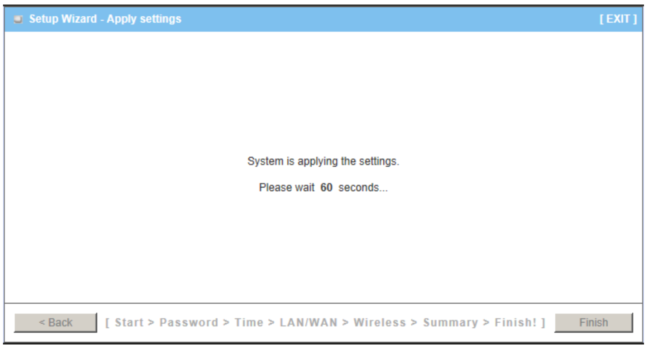
Please confirm the information below

[Wireless Setting]	
Wireless	Enable
SSID	default
Channel	Auto
Authentication	Auto (Open/Shared)
Encryption	None

□ Do you want to proceed the network testing?

Step 5

System is applying the setting.



Setup Wizard - Apply settings

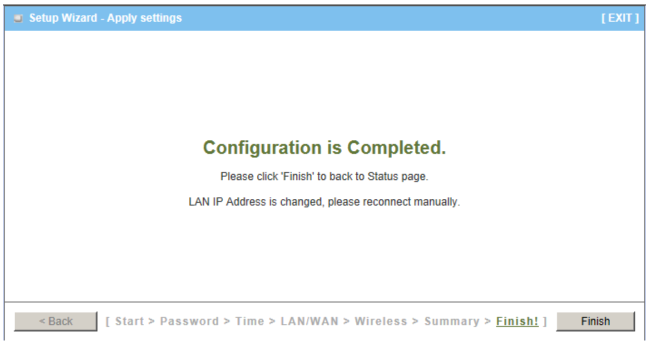
System is applying the settings.

Please wait **60** seconds...

[EXIT]
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Finish

Step 6

Click finish to complete it.



Setup Wizard - Apply settings

Configuration is Completed.

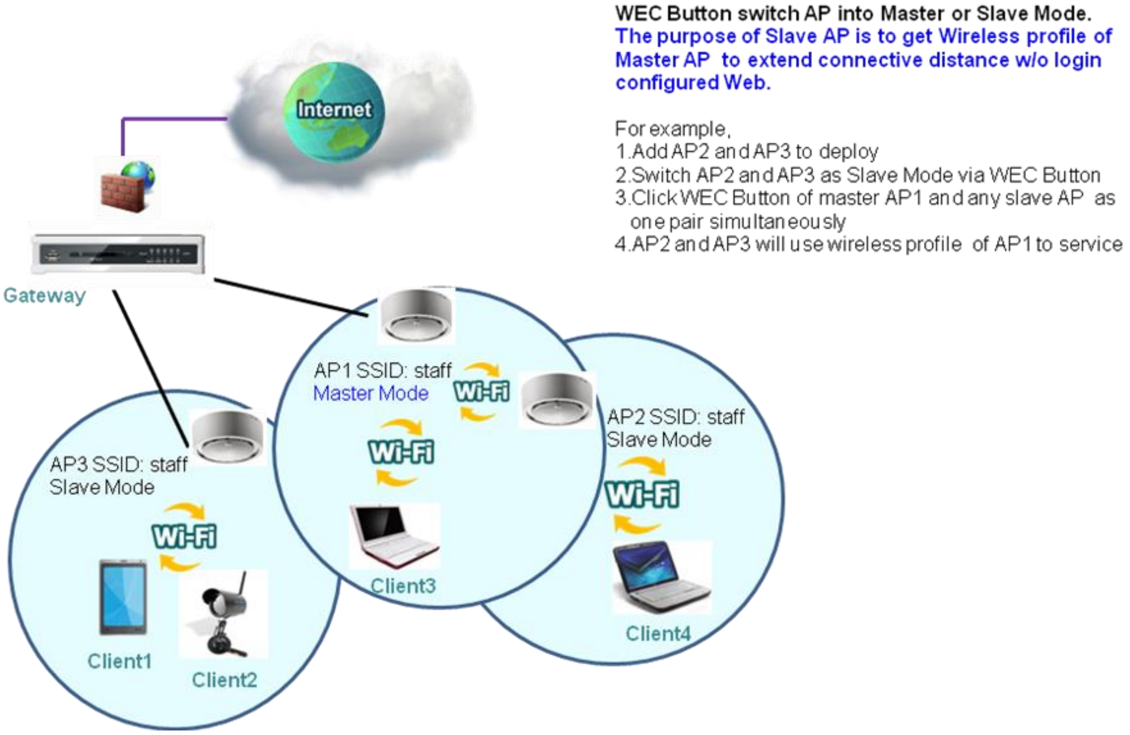
Please click 'Finish' to back to Status page.

LAN IP Address is changed, please reconnect manually.

[EXIT]
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Finish

2.2 Use WEC Button to Setup Wireless Profiles

WEC Button is Wireless Easy Connection. There are 2 purposes for this Button.
One is to switch AP into Master or Slave Mode.
However, Main purpose of Slave AP is to get Wireless profile of Master AP to extend connective distance w/o login configured Web.



WEC Button switch AP into Master or Slave Mode.
The purpose of Slave AP is to get Wireless profile of Master AP to extend connective distance w/o login configured Web.

For example,
1.Add AP2 and AP3 to deploy
2.Switch AP2 and AP3 as Slave Mode via WEC Button
3.Click WEC Button of master AP1 and any slave AP as one pair simultaneously
4.AP2 and AP3 will use wireless profile of AP1 to service

Access Point is in Master Mode

Generally speaking, the settings of Master AP can work in your Network environment.
When System is ready: (without click button.) Status LED in Solid : In Master Mode
※**Device Network IP Address depend as current Settings.**

Access Point is in Slave Mode

New deployed or reset-to-default Access points have to configure Wireless setting so that can work current network environment.
When System is ready: (without click button.) Status LED in Flash: In Slave Mode
※**Device Network IP Address is DHCP Client in Slave Mode.**

Please check if DHCP Server exists in your Network Environment.
If Not, please change to Master Mode after getting Wireless Profiles, it will be Default IP “Static IP”.(Due to New deployed or reset-to-default Access point**.**)

Configure Slave AP via WEC Button

Step 1
Check WiFi LED of Access Point which acts as Master Mode.
(Press Reset/WEC button 5~10 sec then release Button to change Mode .When System is ready Status LED in Solid : It is in Master Mode)
Step 2
Check WiFi LED of Access Point which acts as Slave Mode.
(Press Reset/WEC button 5~10 sec then release Button to change Mode .When System is ready Status LED in Flash : It is in Slave Mode)

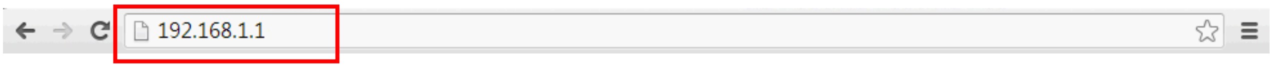
Step 3
Click WEC Button (about 1second) of master AP and any slave AP as one pair simultaneously

Step 4
WiFi LED of Master and Slave AP will flash and Negotiate WiFi Profile Configuration. This Process will finish within 20~30 sec.
Then Check WiFi LED:
LED in Slow flash: Wireless Connection doesn't establish.
LED in Solid : Wireless Connection established successfully.

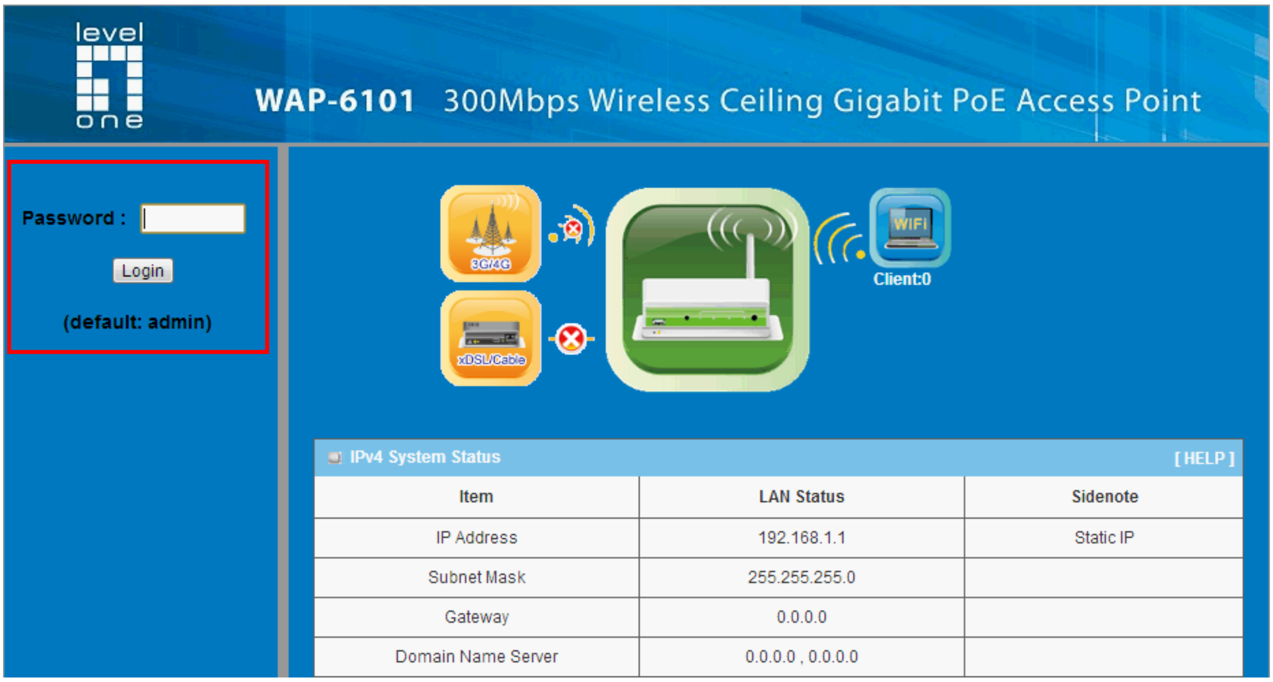
※If Negotiation failed or Master or Slave AP don’t existed, WiFi LED will Flash 2 min. Please try again.
※WEC Application bases on WiFi WPS Technology and only supports to use “AES” encryption to negotiate, currently. Please notify before configuring AP in Master Mode.

Chapter 3 Making Configurations

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: **192.168.1.1.** In the configuration section you may want to check the connection status of this device, to do Basic or Advanced Network setup or to check the system status. These task buttons can be easily found in the cover page of the UI (User Interface).



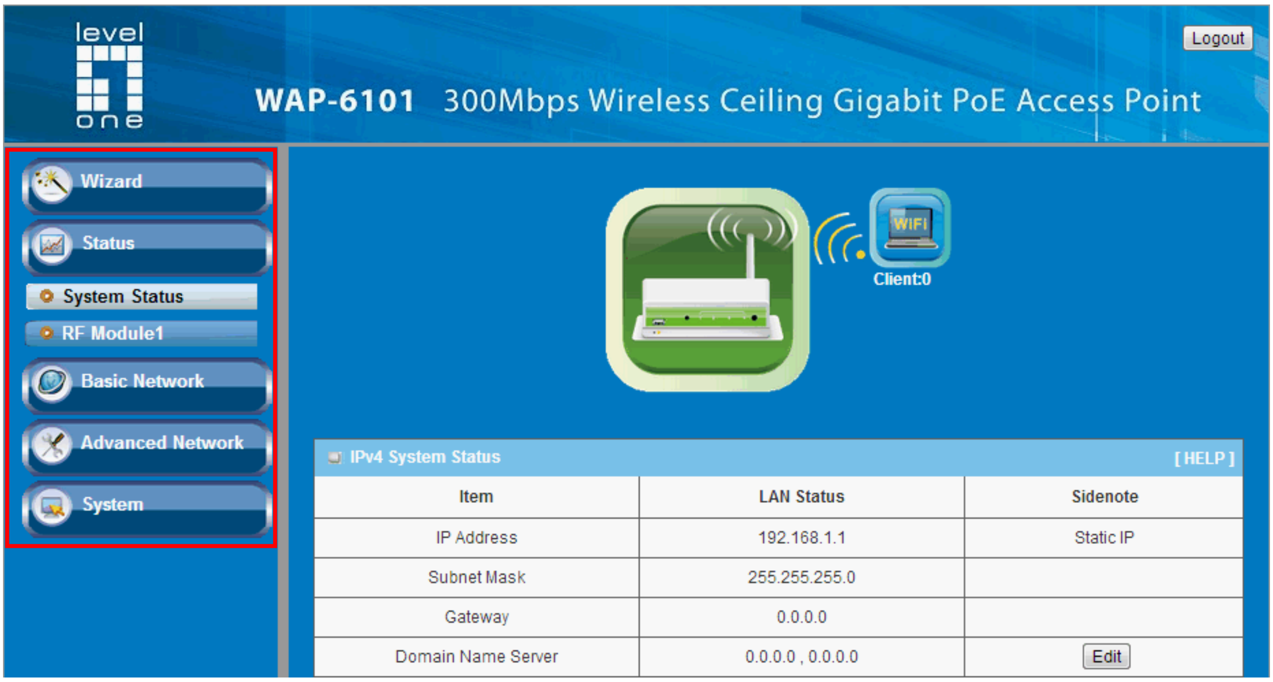
Enter the default username and password **"admin"** in the System Password and then click **'login'** button.



IPv4 System Status [HELP]

Item	LAN Status	Sidenote
IP Address	192.168.1.1	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	

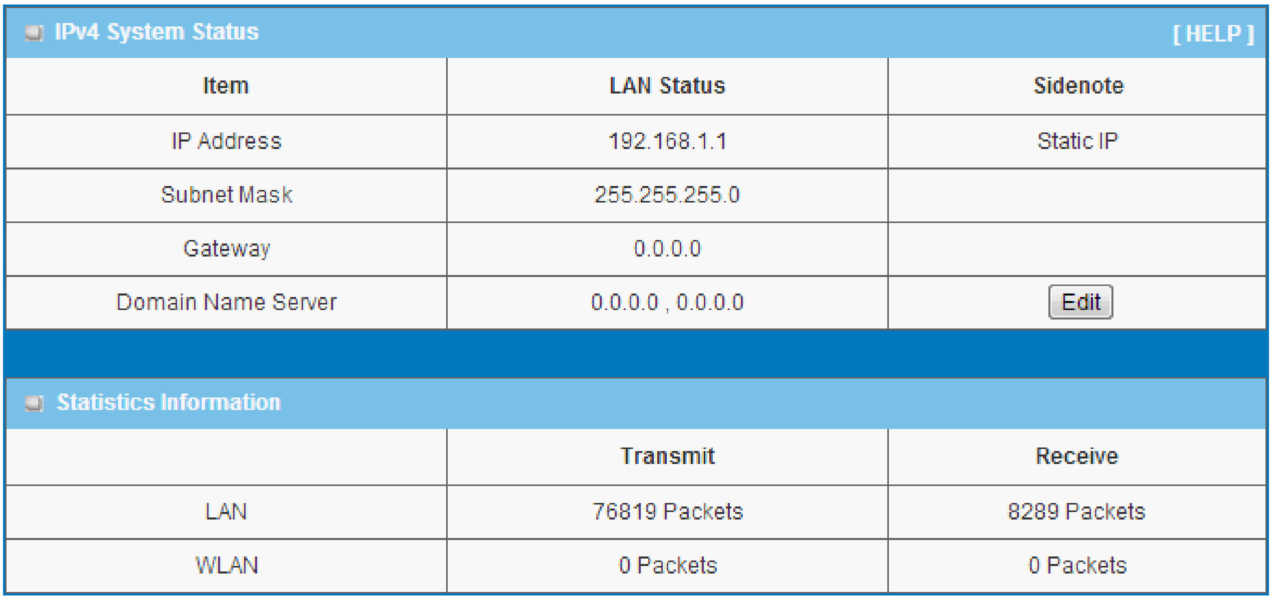
Afterwards, you can go **Wizard, Basic Network, Advanced Network, Application or System** respectively on left hand side of web page.



IPv4 System Status [HELP]

Item	LAN Status	Sidenote
IP Address	192.168.1.1	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	Edit

Note: *You can see the Connection Status screen below after you logged in.*



IPv4 System Status [HELP]

Item	LAN Status	Sidenote
IP Address	192.168.1.1	Static IP
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	Edit

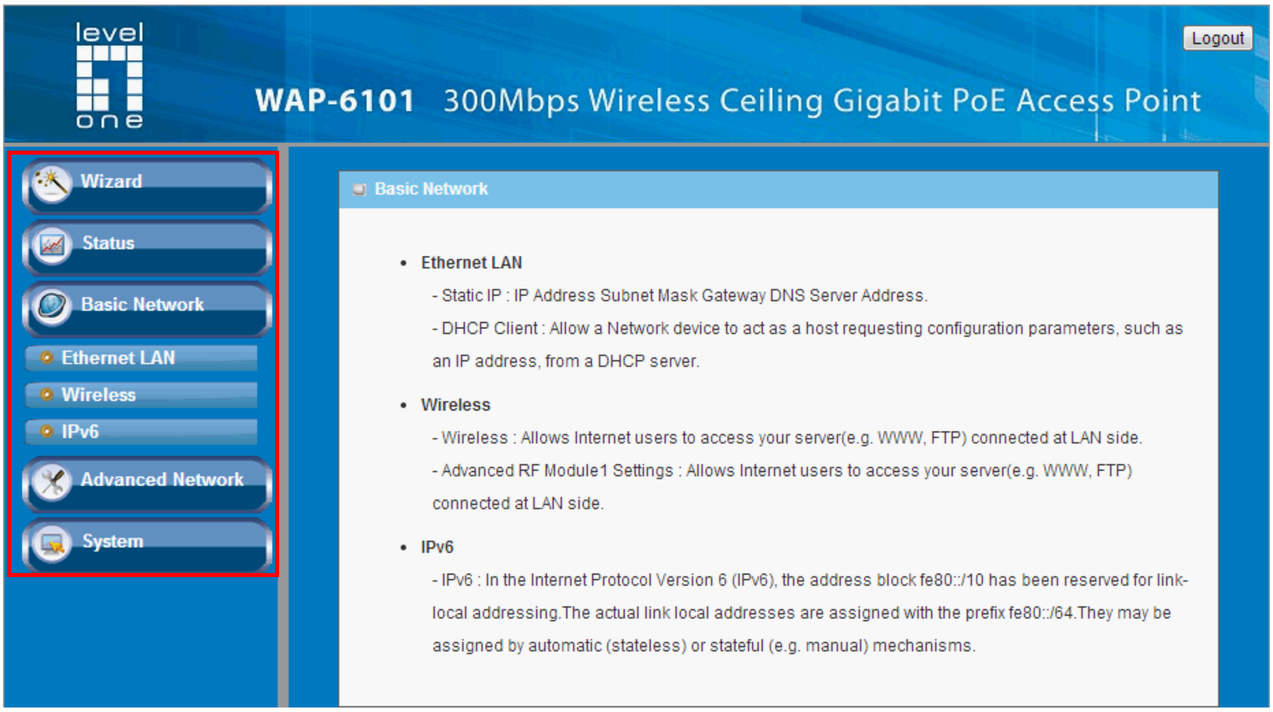
Statistics Information

	Transmit	Receive
LAN	76819 Packets	8289 Packets
WLAN	0 Packets	0 Packets

Note : *You can see all the status of this device in the ‘Status’ main menu section.*

3.1 Basic Network

You can enter Basic Network for **Ethernet LAN and Wireless** settings as the icon here shown



Basic Network

- Ethernet LAN
  - Static IP : IP Address Subnet Mask Gateway DNS Server Address.
  - DHCP Client : Allow a Network device to act as a host requesting configuration parameters, such as an IP address, from a DHCP server.
- Wireless
  - Wireless : Allows Internet users to access your server(e.g. WWW, FTP) connected at LAN side.
  - Advanced RF Module1 Settings : Allows Internet users to access your server(e.g. WWW, FTP) connected at LAN side.
- IPv6
  - IPv6 : In the Internet Protocol Version 6 (IPv6), the address block fe80::/10 has been reserved for link-local addressing.The actual link local addresses are assigned with the prefix fe80::/64.They may be assigned by automatic (stateless) or stateful (e.g. manual) mechanisms.

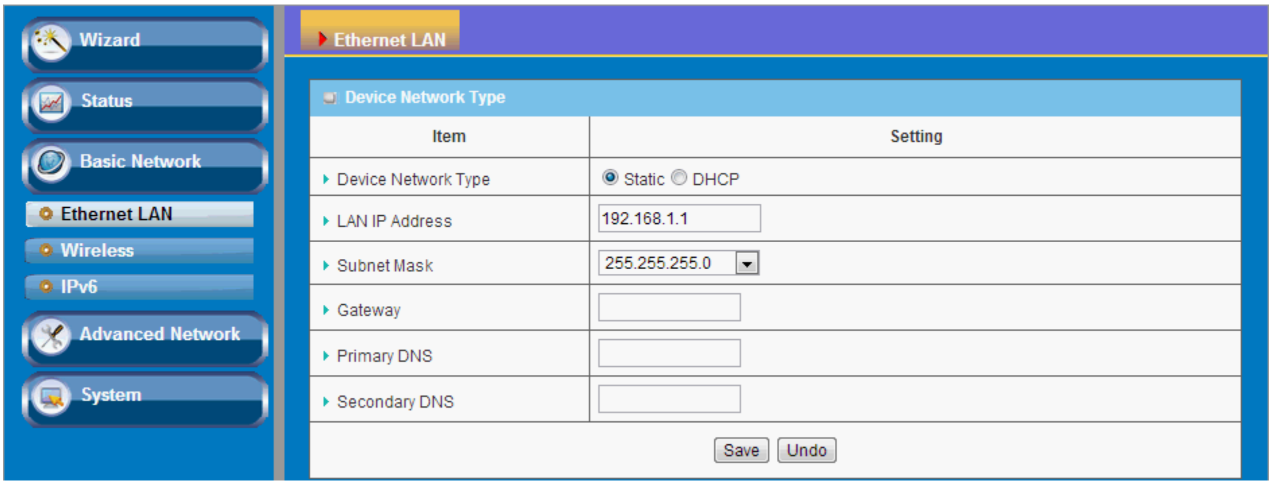
3.1.1 Ethernet LAN

This device supports two types as Follows:

Static IP: Allow a device to act as a Static host. If you need Static host and please entry IP Address.

DHCP: Allow a device to act as a host requesting configuration parameters, such as an IP address from a DHCP server.

Note: Please check if there is DHCP server in your Network, first.



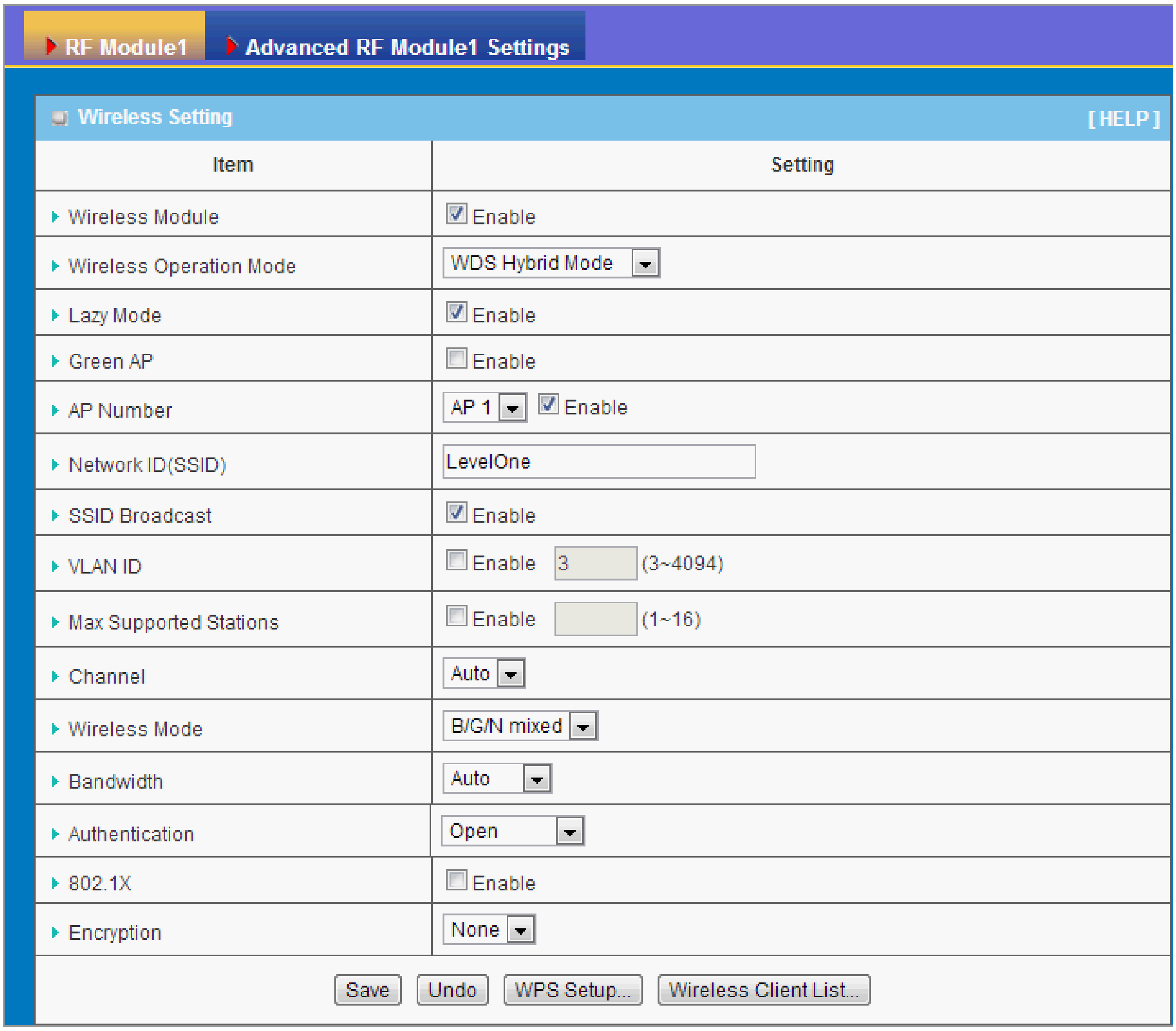
Device Network Type

Item	Setting
Device Network Type	● Static ○ DHCP
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	
Primary DNS	
Secondary DNS	

3.1.2 Wireless

Wireless settings allow you to set the WLAN (WiFi) configuration items. When the wireless configuration is done your WiFi LAN is ready to support your local WiFi devices such as your laptop PC, wireless printer and some portable wireless devices.

RF Module1 is 2.4GHz Wireless Module.



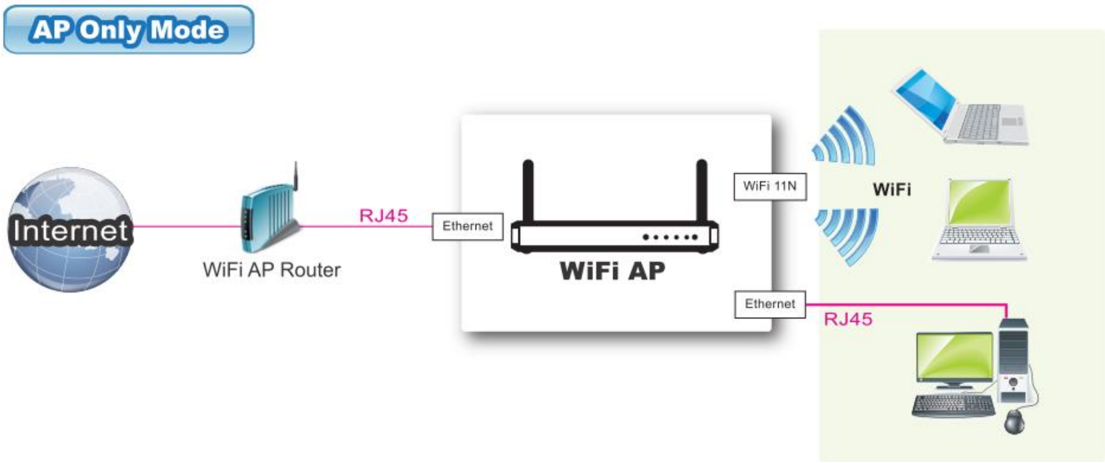
Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	WDS Hybrid Mode
Lazy Mode	☑ Enable
Green AP	□ Enable
AP Number	AP 1 ☑ Enable
Network ID(SSID)	LevelOne
SSID Broadcast	☑ Enable
VLAN ID	□ Enable 3 (3~4094)
Max Supported Stations	□ Enable (1~16)
Channel	Auto
Wireless Mode	B/G/N mixed
Bandwidth	Auto
Authentication	Open
802.1X	□ Enable
Encryption	None

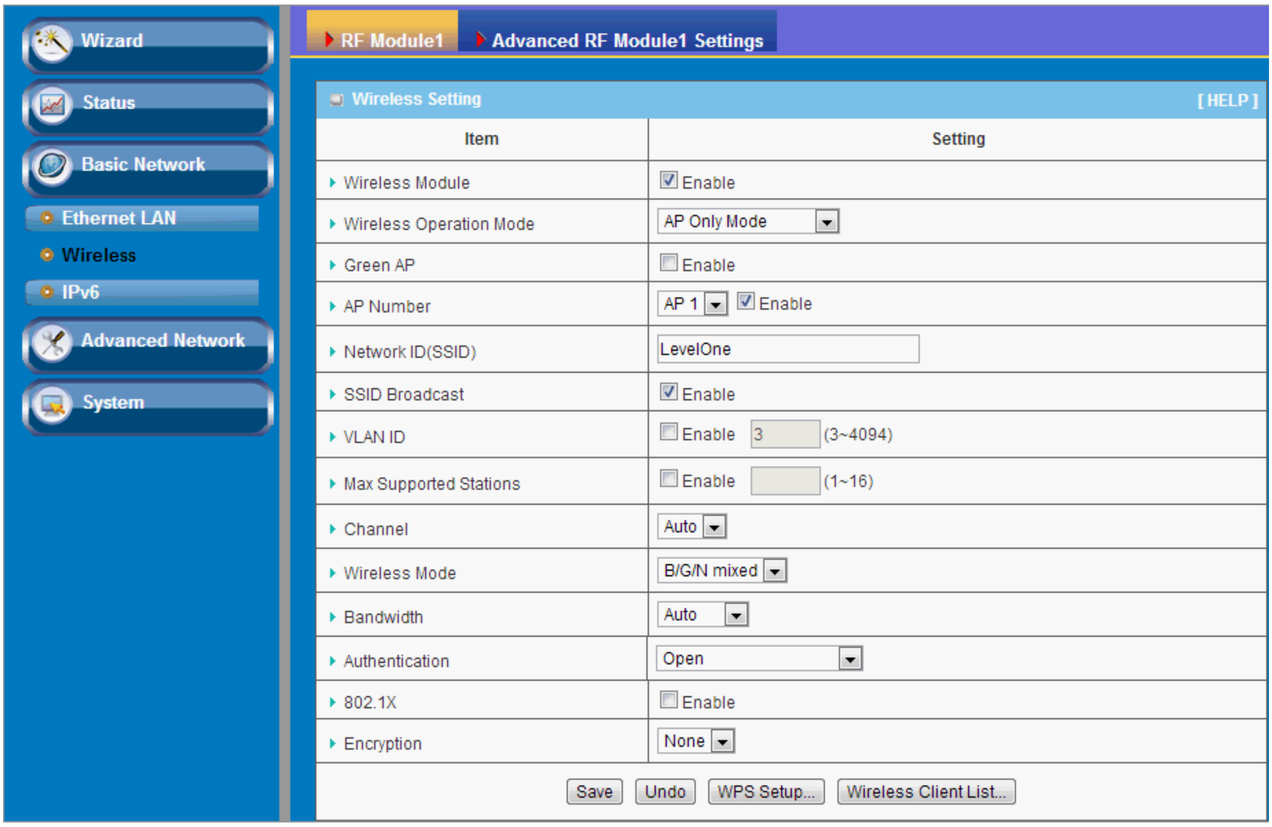
3.1.3.1 Wireless Setup

There are several wireless operation modes provided by this device. They are: “**AP Only Mode**”, “**WDS Hybrid Mode**”, “**WDS Only Mode**”, and “**Universal Repeater Mode**”. You can choose the expected mode from the list.

3.1.3.1.1 AP Only Mode

When acting as an access point, this device connects all the wireless stations to a wired network and the WAN Port is disabled consequently.





Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	AP Only Mode
Green AP	□ Enable
AP Number	AP 1 ☑ Enable
Network ID(SSID)	LevelOne
SSID Broadcast	☑ Enable
VLAN ID	□ Enable 3 (3~4094)
Max Supported Stations	□ Enable (1~16)
Channel	Auto
Wireless Mode	B/G/N mixed
Bandwidth	Auto
Authentication	Open
802.1X	□ Enable
Encryption	None

1. **Wireless Module:** Enable the wireless function.
2. **Wireless Operation Mode:** Choose “**AP Only Mode**” from the list.
3. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
4. **AP Number:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.

5. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
6. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
7. **VLAN ID:** Supports mapping of SSIDs to VLANs to separate workgroups across wireless and wired domains.
8. **Max Supported Stations:** Support Max Stations to associated related SSID.
9. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
10. **Wireless Mode:** RF1 Module can choose “N only”, “G/N mixed” or “B/G/N mixed” and the factory default setting is “B/G/N mixed”. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open (include 802.1x), Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

    - **Open**

      Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP configuration.

    - **Shared**

      Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP. Three types of shared key authentication are available today for home or small office WLAN environments.

    - **Auto**

      The AP will Select the Open or Shared by the client’s request automatically.

    - **WPA-PSK**

      Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

    - **WPA**

      Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this device. This key value must be consistent with the key value in the RADIUS server.

- **WPA2-PSK**

  Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA2**

  Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this device. This key value must be consistent with the key value in the RADIUS server.

- **WPA-PSK/WPA2-PSK**

  Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA/WPA2**

  Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this device. This key value must be consistent with the key value in the RADIUS server.

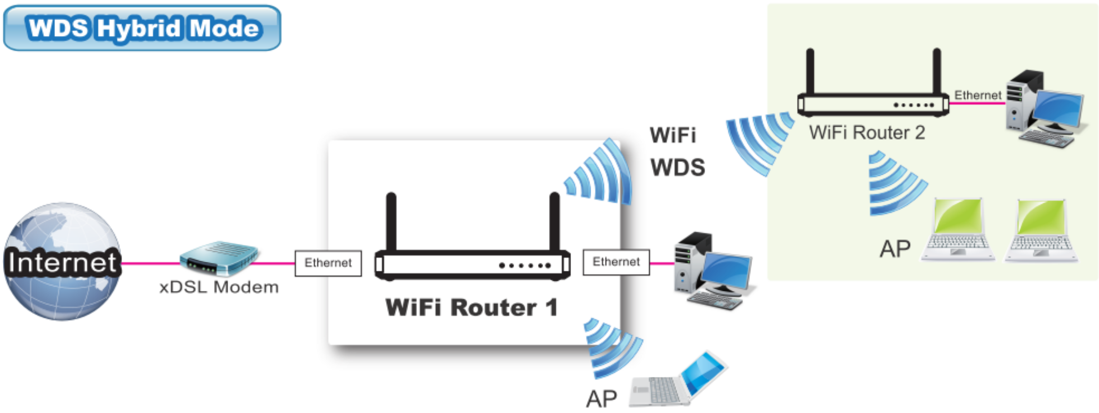
- **820.1x**

  When you select “Open” Authentication, GUI will display 802.1x. Please RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then select wep64 or wep128.

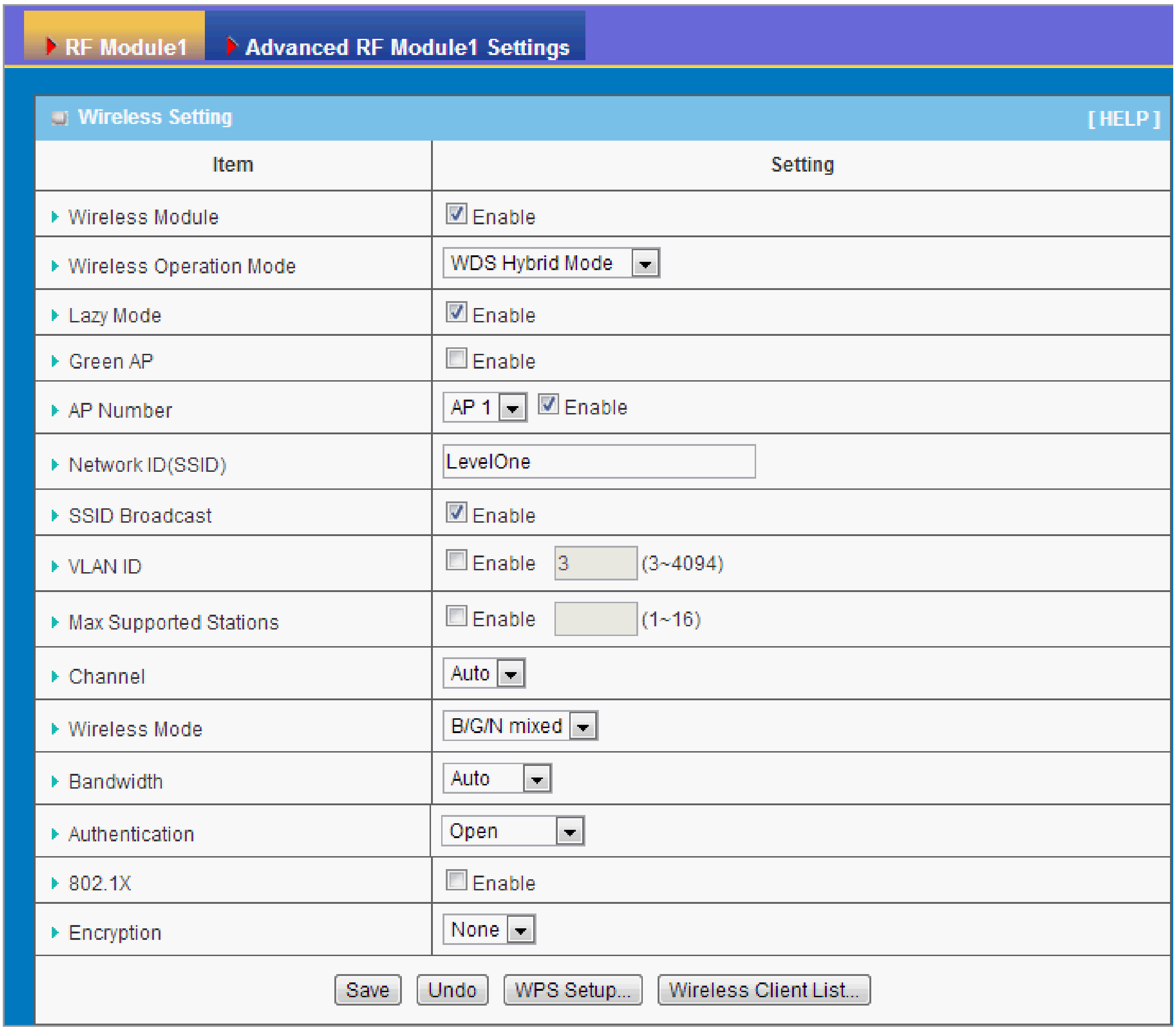
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.2 WDS Hybrid Mode

While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection



.



Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	WDS Hybrid Mode ▾
Lazy Mode	☑ Enable
Green AP	□ Enable
AP Number	AP 1 ▾ ☑ Enable
Network ID(SSID)	LevelOne
SSID Broadcast	☑ Enable
VLAN ID	□ Enable 3 (3~4094)
Max Supported Stations	□ Enable (1~16)
Channel	Auto ▾
Wireless Mode	B/G/N mixed ▾
Bandwidth	Auto ▾
Authentication	Open ▾
802.1X	□ Enable
Encryption	None ▾

1. **Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don’t have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers’ MAC address filled.
2. **Green AP:** Enable the Green AP function to reduce the power consumption

when there is no wireless traffics.

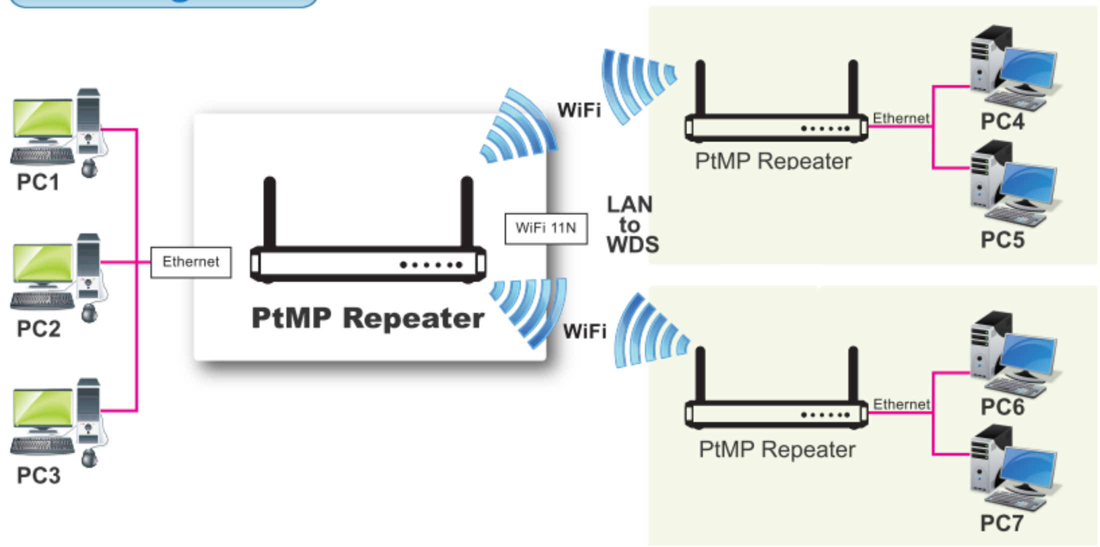
3. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
4. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
5. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
6. **VLAN ID:** Supports mapping of SSIDs to VLANs to separate workgroups across wireless and wired domains.
7. **Max Supported Stations:** Support Max Stations to associated related SSID.
8. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
9. **Wireless Mode:** RF1 Module can choose “N only”, “G/N mixed” or “B/G/N mixed” and the factory default setting is “B/G/N mixed”.
10. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK,WPA /WPA2, or 802.1x.
11. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

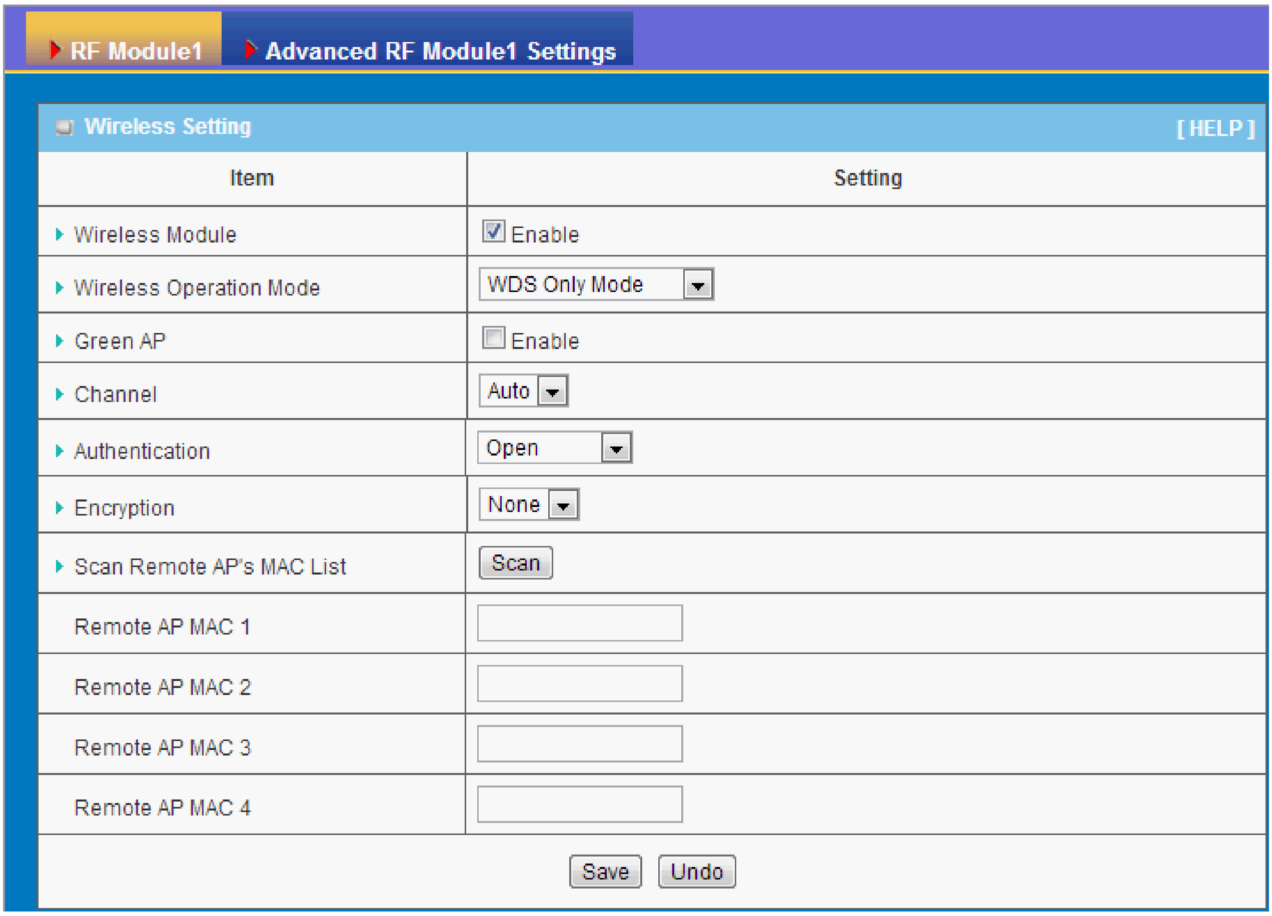
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.3 WDS Only Mode

WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools …etc.

WDS Only Mode





Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	WDS Only Mode
Green AP	□ Enable
Channel	Auto
Authentication	Open
Encryption	None
Scan Remote AP's MAC List	Scan
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	

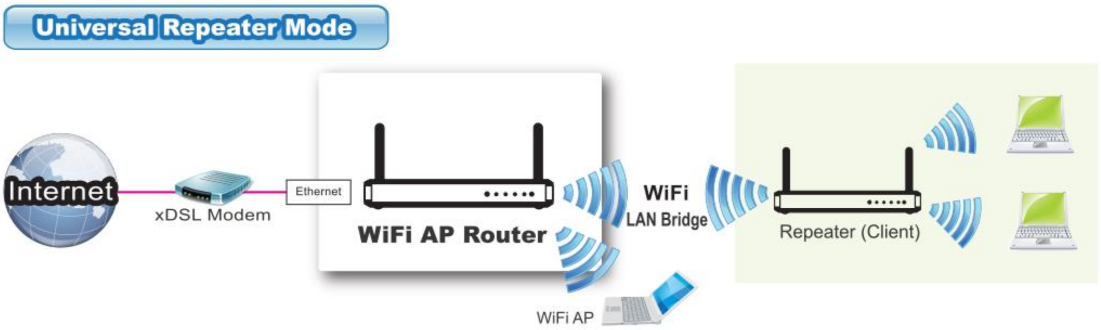
1. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
2. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
3. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

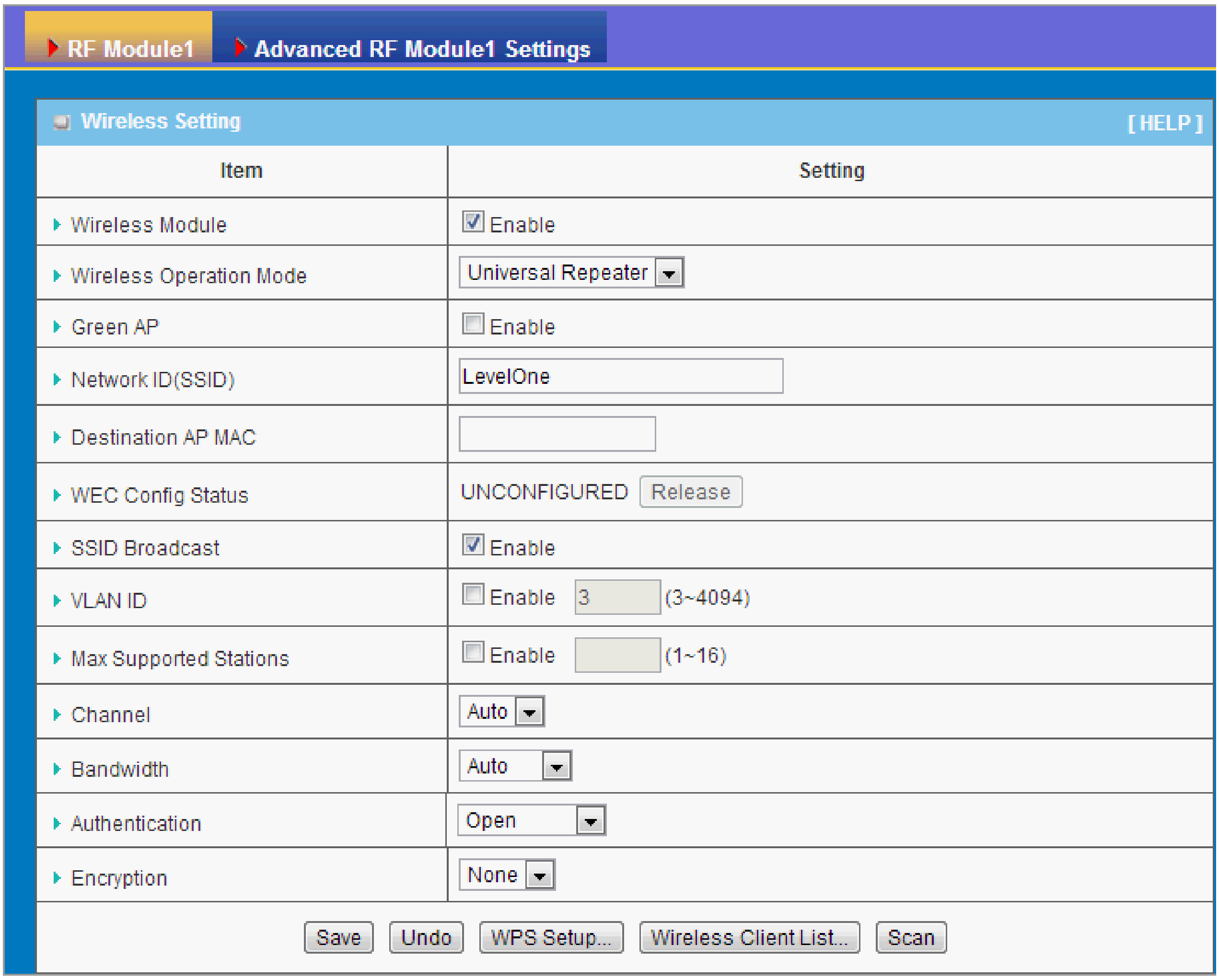
4. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.4 Universal Repeater Mode

Universal Repeater is a technology used to extend wireless coverage. It provides the function to act as Adapter (Client) and AP at the same time and can use this function to connect to a Root AP and use AP (SSID name must be the same as that of Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.





Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	Universal Repeater
Green AP	□ Enable
Network ID(SSID)	LevelOne
Destination AP MAC	
WEC Config Status	UNCONFIGURED Release
SSID Broadcast	☑ Enable
VLAN ID	□ Enable 3 (3~4094)
Max Supported Stations	□ Enable (1~16)
Channel	Auto
Bandwidth	Auto
Authentication	Open
Encryption	None

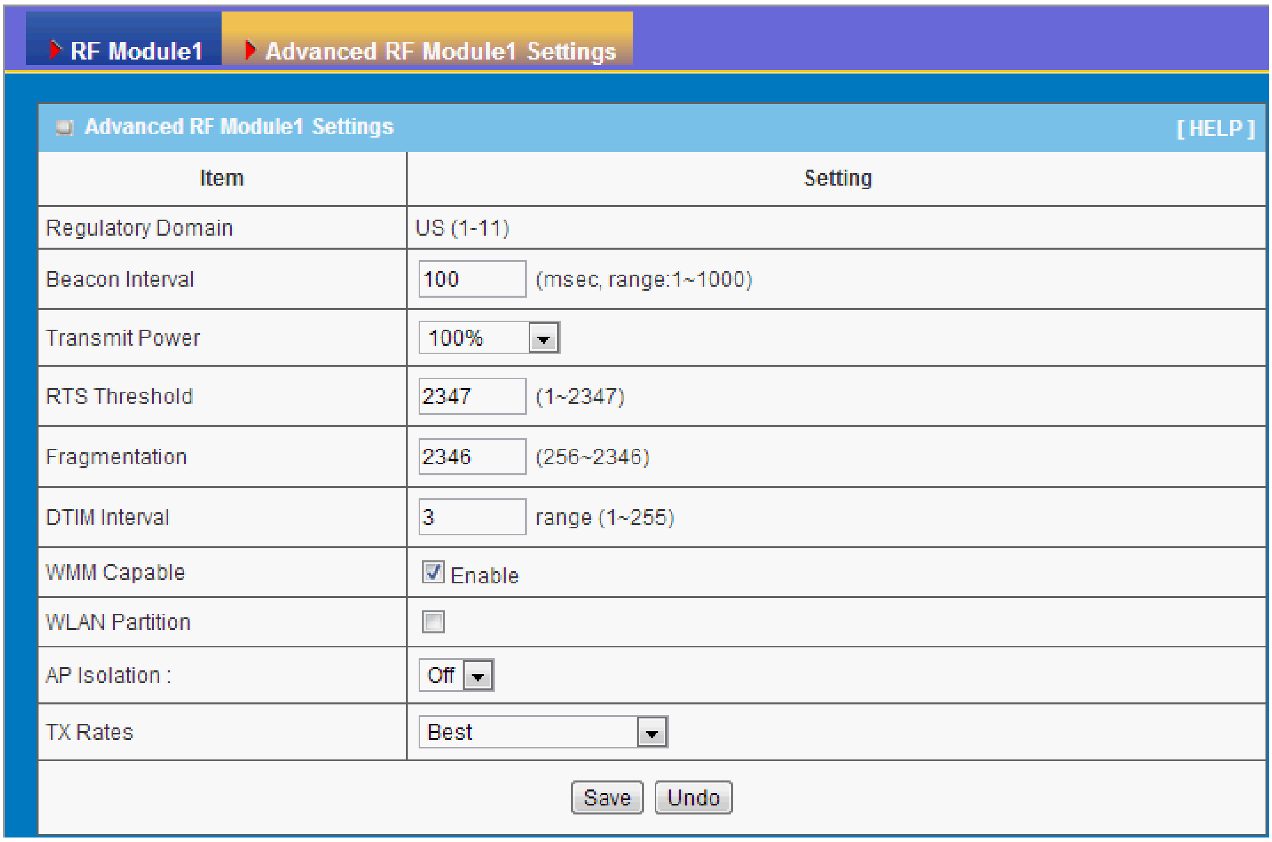
1. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
2. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
3. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
4. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
5. **VLAN ID:** Supports mapping of SSIDs to VLANs to separate workgroups across wireless and wired domains.
6. **Max Supported Stations:** Support Max Stations to associated related SSID.
7. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.2 Advanced Wireless Setup

This device provides advanced wireless setup for professional user to optimize the wireless performance under the specific installation environment.

3.1.3.2.1 Advanced RF Module1 Settings



Advanced RF Module1 Settings

Item	Setting
Regulatory Domain	US (1-11)
Beacon Interval	100 (msec, range:1~1000)
Transmit Power	100%
RTS Threshold	2347 (1~2347)
Fragmentation	2346 (256~2346)
DTIM Interval	3 range (1~255)
WMM Capable	☑ Enable
WLAN Partition	□
AP Isolation :	Off
TX Rates	Best

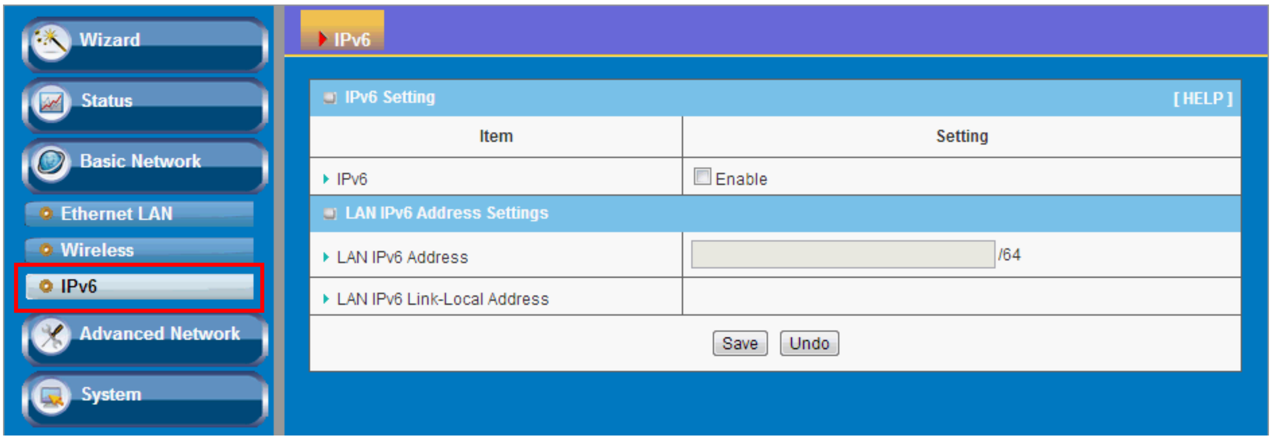
1. **Beacon interval**: Beacons are packets sent by a Access Point to synchronize wireless devices.
2. **Transmit Power**: Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.
3. **RTS Threshold:** If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.
4. **Fragmentation**: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF

coverage.

5. **DTIM interval**: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.
6. **WMM Capable:** WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
7. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
8. **TX Rate:** Can Fix TX Rate to transmit date.

3.1.3 IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6** (**Internet Protocol version 6**) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers.



IPv6 Setting [HELP]

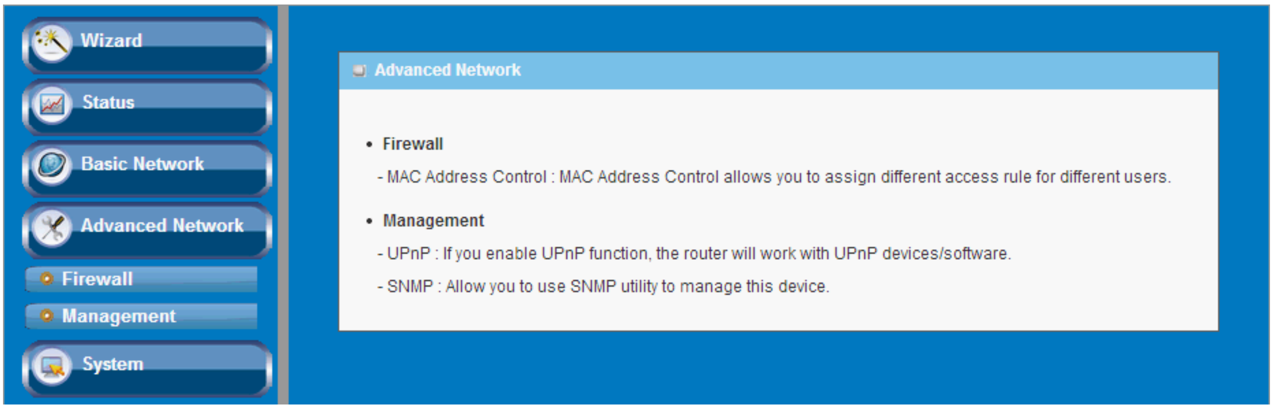
Item	Setting
IPv6	□ Enable
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	

1. **LAN IPv6 address settings:** Please enter "LAN IPv6 address" and ignore the "LAN IPv6 Link-Local address".

   "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

3.2 Advanced Network

This device also supports many advanced network features, such as Firewall, and Management. You can finish those configurations in this section.



Advanced Network

- **Firewall**

  - MAC Address Control : MAC Address Control allows you to assign different access rule for different users.

- **Management**

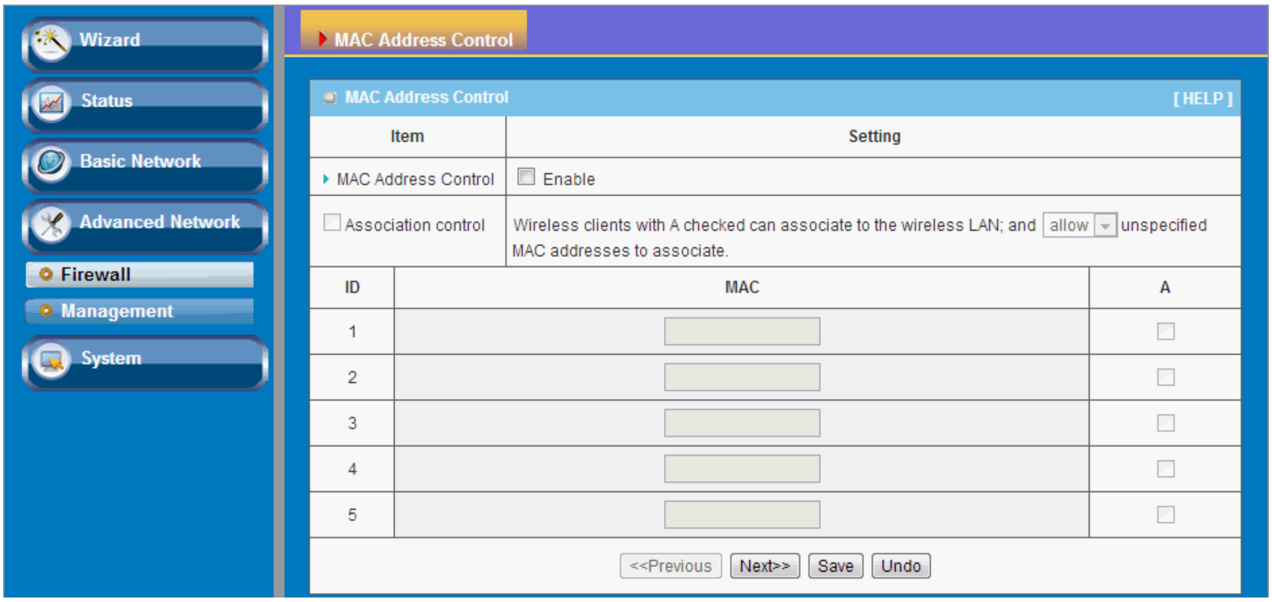
  - UPnP : If you enable UPnP function, the router will work with UPnP devices/software.
  - SNMP : Allow you to use SNMP utility to manage this device.

3.2.1 Firewall

The firewall includes MAC Address Control.

3.2.1.1 MAC Address Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.



MAC Address Control

Item	Setting
MAC Address Control	□ Enable
□ Association control	Wireless clients with A checked can associate to the wireless LAN; and allow ▾ unspecified MAC addresses to associate.

ID	MAC	A
1		□
2		□
3		□
4		□
5		□

1. **MAC Address Control**: Check "Enable" to enable the "MAC Address Control". All of the settings in this page will take effect only when "Enable" is checked.

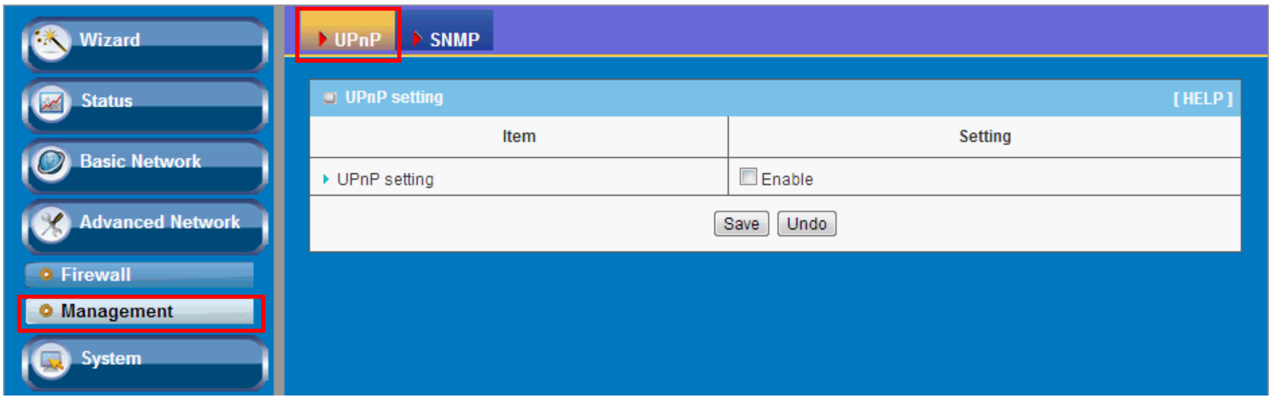
2. **Association control**: Check "Association control" to enable the control of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.2 Management

3.2.2.1 UPNP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some Network device. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming



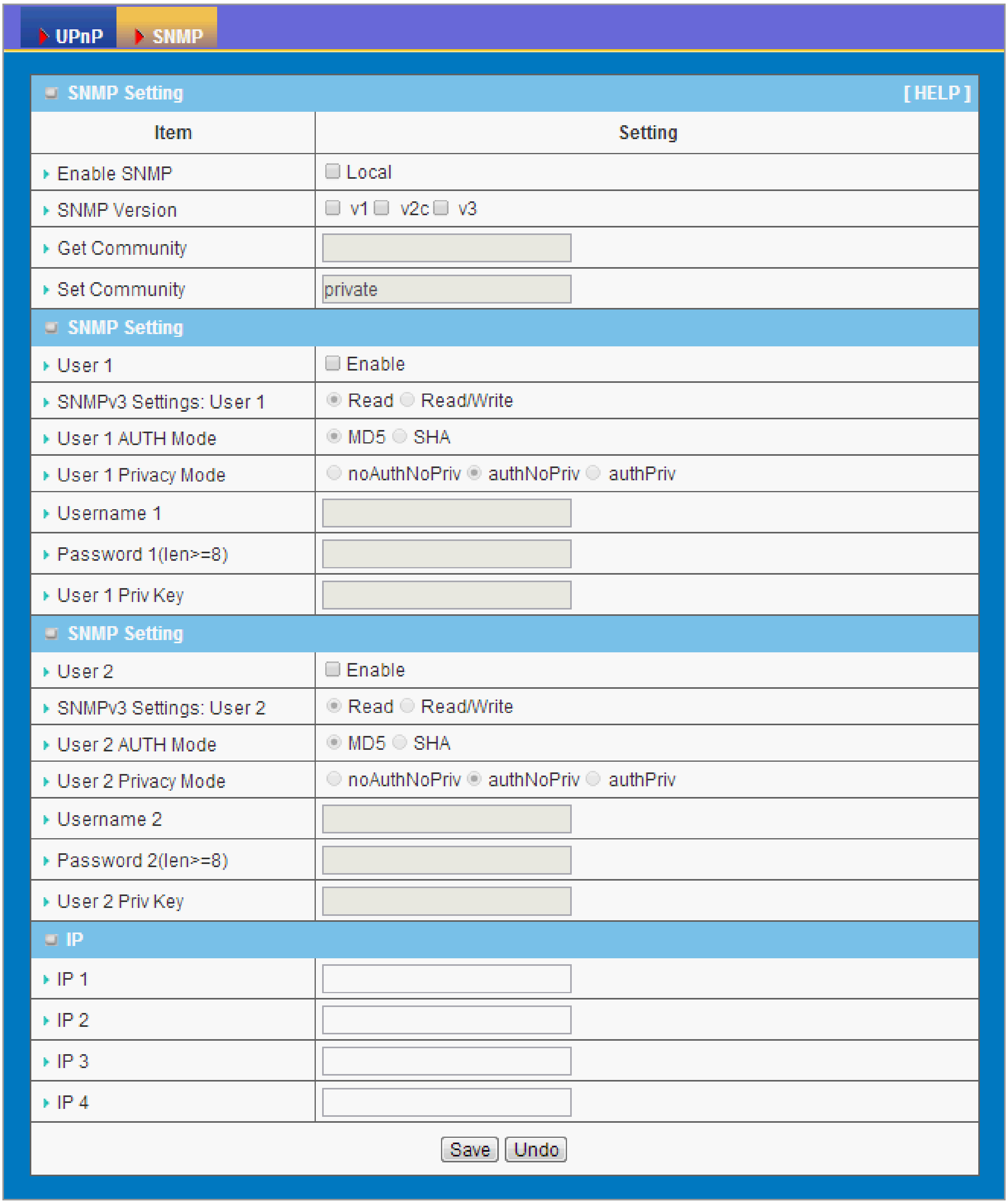
UPnP setting [HELP]

Item	Setting
UPnP setting	□ Enable

This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

3.2.2.2 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.



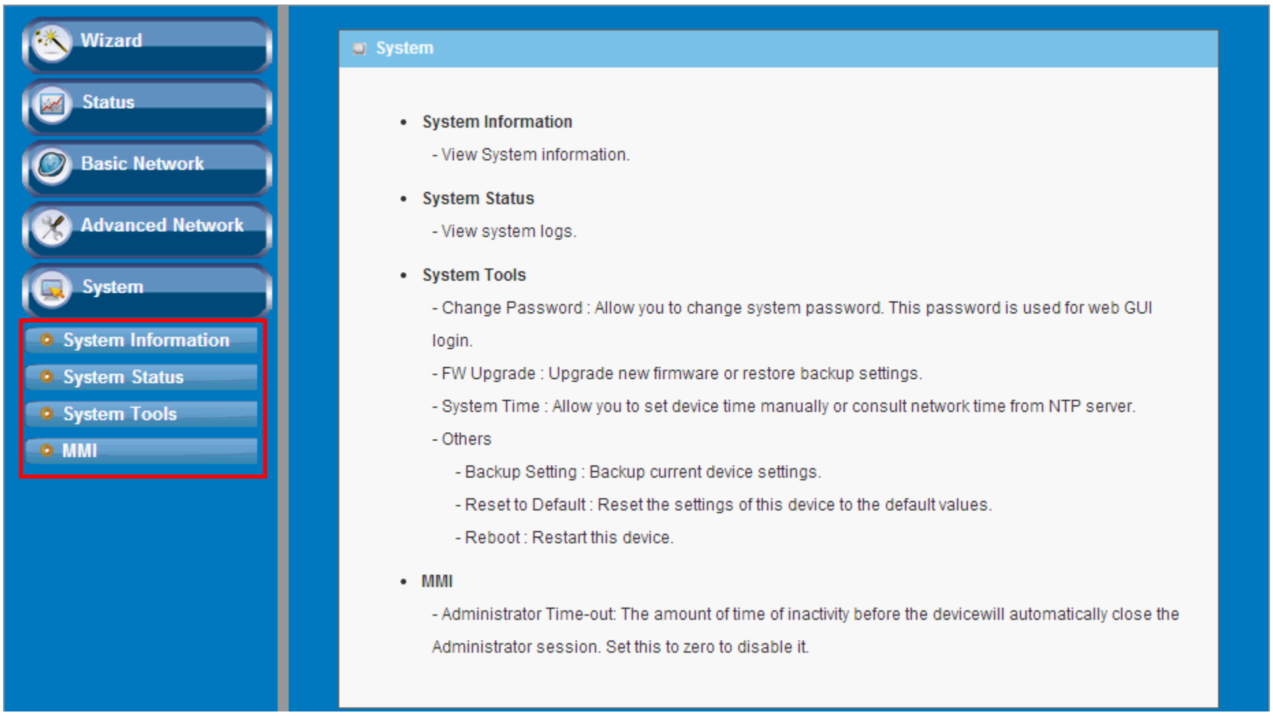
Item	Setting
Enable SNMP	□ Local
SNMP Version	□ v1 □ v2c □ v3
Get Community	
Set Community	private
SNMP Setting	
User 1	□ Enable
SNMPv3 Settings: User 1	● Read ○ Read/Write
User 1 AUTH Mode	● MD5 ○ SHA
User 1 Privacy Mode	○ noAuthNoPriv ● authNoPriv ○ authPriv
Username 1	
Password 1(len>=8)	
User 1 Priv Key	
SNMP Setting	
User 2	□ Enable
SNMPv3 Settings: User 2	● Read ○ Read/Write
User 2 AUTH Mode	● MD5 ○ SHA
User 2 Privacy Mode	○ noAuthNoPriv ● authNoPriv ○ authPriv
Username 2	
Password 2(len>=8)	
User 2 Priv Key	
IP	
IP 1	
IP 2	
IP 3	
IP 4	

1. **Enable SNMP**: Enable this Function.
2. **SNMP Version:** Supports SNMP V1, V2c, and V3.
3. **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
4. **Set Community:** The community of SetRequest that this device will accept.

5. **SNMPv3 Settings: User 1/2**: This device supports up to two SNMP management accounts. You can specify the account permission as “Read” or “Read/Write” respectively.
6. **User 1/2 AUTH Mode**: Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
7. **User 1/2 Privacy Mode:** You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
8. **Username 1/2:** Use this field to identify the user name for the specified level of access.
9. **Password 1/2:** Use this field to set the password for the specified level of access.
10. **User 1/2 Priv Key:** Use this field to define the encryption key for the specified level of access.
11. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

3.3 System

In this section you can see system information, system logs, use system tools for system update and do service scheduling and system administration setting.

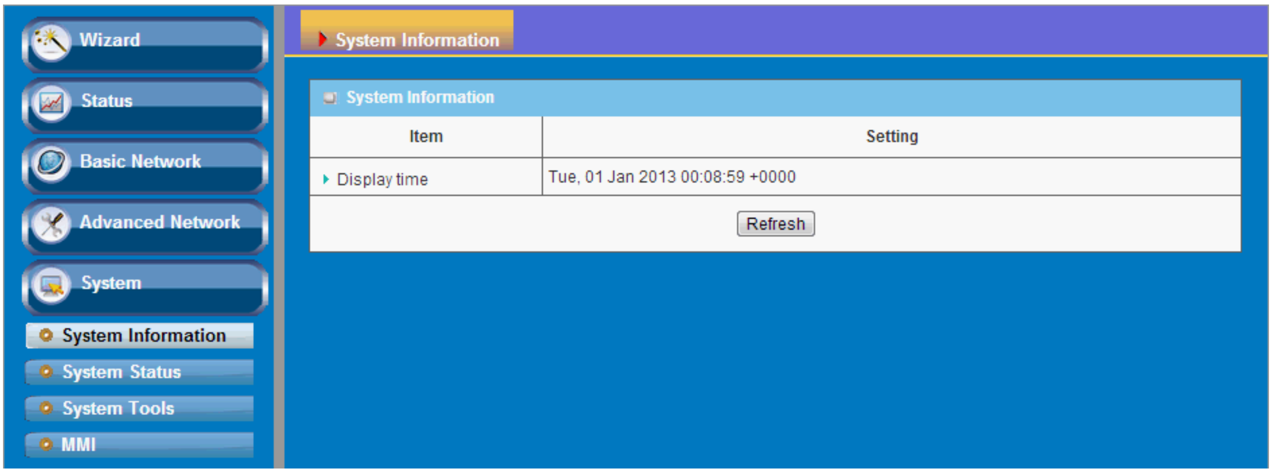


System

- System Information
  - View System information.
- System Status
  - View system logs.
- System Tools
  - Change Password : Allow you to change system password. This password is used for web GUI login.
  - FW Upgrade : Upgrade new firmware or restore backup settings.
  - System Time : Allow you to set device time manually or consult network time from NTP server.
  - Others
    - Backup Setting : Backup current device settings.
    - Reset to Default : Reset the settings of this device to the default values.
    - Reboot : Restart this device.
- MMI
  - Administrator Time-out: The amount of time of inactivity before the devicewill automatically close the Administrator session. Set this to zero to disable it.

3.3.1 System Information

You can view the System Information in this page.



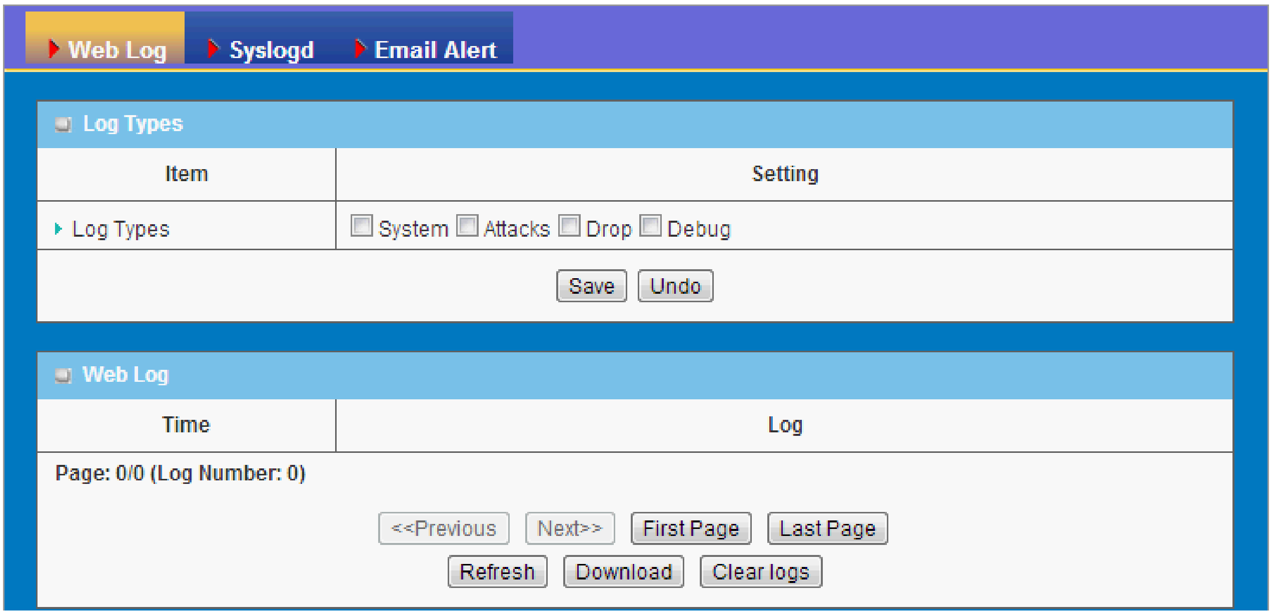
System Information

Item	Setting
Display time	Tue, 01 Jan 2013 00:08:59 +0000

Refresh

3.3.2 System Status

3.3.2.1 Web Log



Log Types

Item	Setting
Log Types	□ System □ Attacks □ Drop □ Debug

Save Undo

Web Log

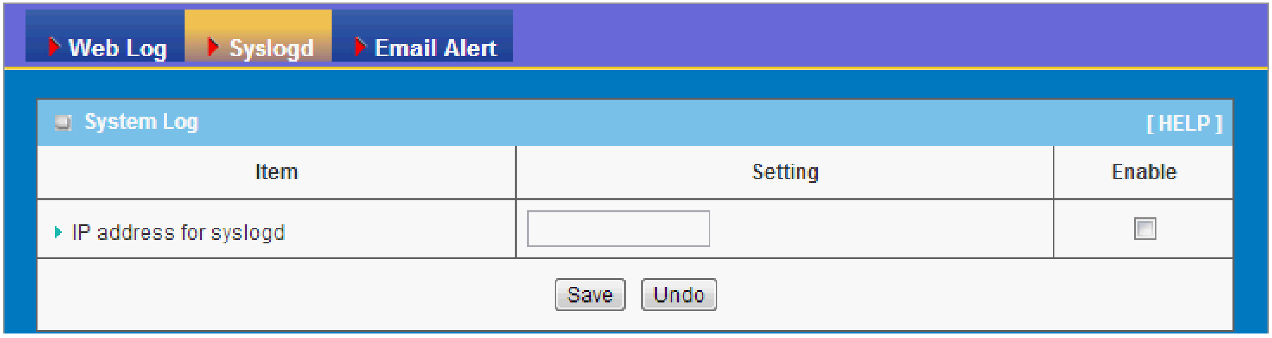
Time	Log

Page: 0/0 (Log Number: 0)

<<Previous Next>> First Page Last Page
Refresh Download Clear logs

1. **Log Types**: You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.
2. **Web Log**: You can browse, refresh, download, and clear the log messages.

3.3.2.2 Syslog



System Log

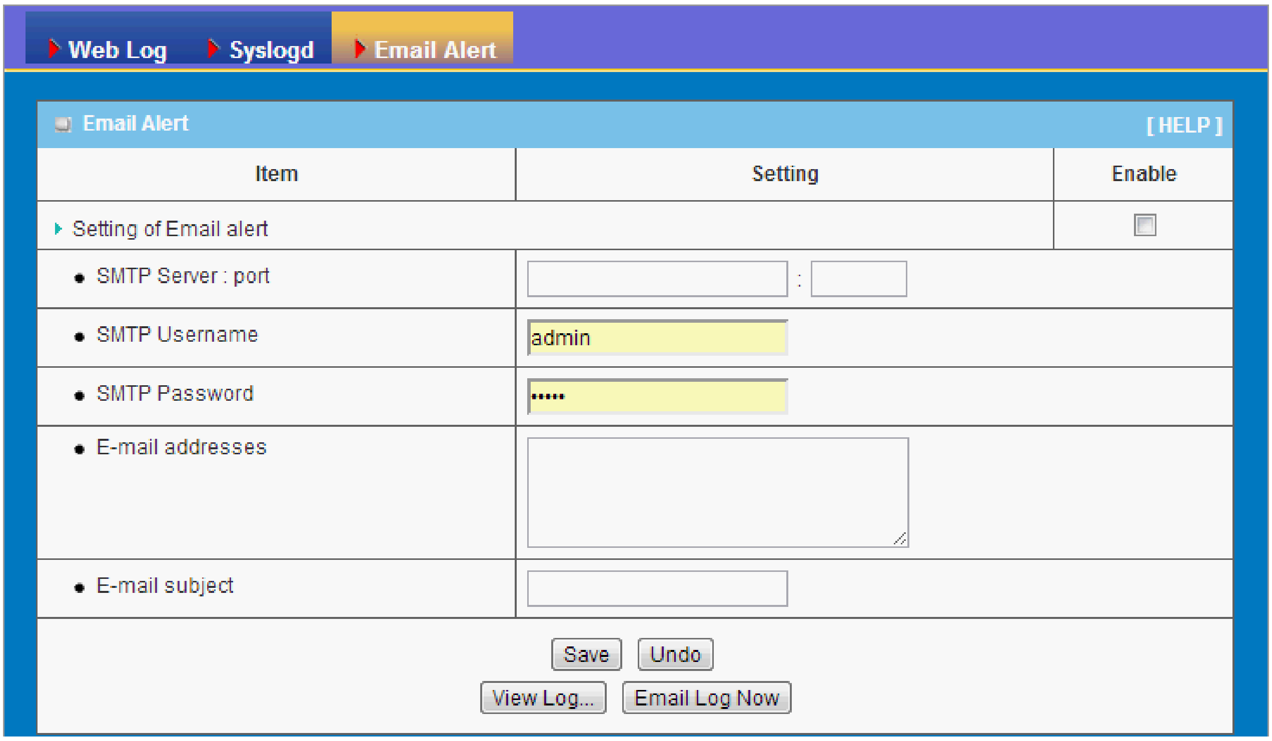
Item	Setting	Enable
IP address for syslogd		□

This device can also export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslogs

The items you have to setup include:

1. **IP Address for syslogd**: Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.

3.3.2.3 Email Alert



Email Alert

Item	Setting	Enable
Setting of Email alert		□
• SMTP Server : port	:	
• SMTP Username	admin	
• SMTP Password	•••••	
• E-mail addresses		
• E-mail subject		

This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

1. **Setting of Email alert**: Check if you want to enable Email alert (send syslog via email).
2. **SMTP Server: Port**: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25. For example, "mail.your_url.com" or "192.168.1.100:26".

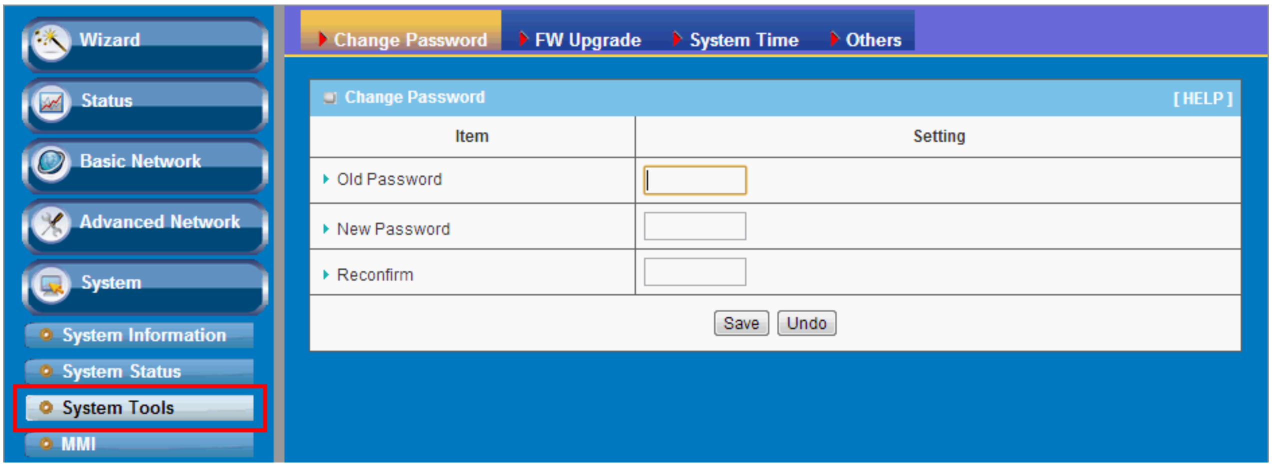
3. **SMTP Username:** Enter the Username offered by your ISP.
4. **SMTP Password:** Enter the password offered by your ISP.
5. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
6. **E-mail Subject**: The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.3 System Tools

3.3.3.1 Change Password

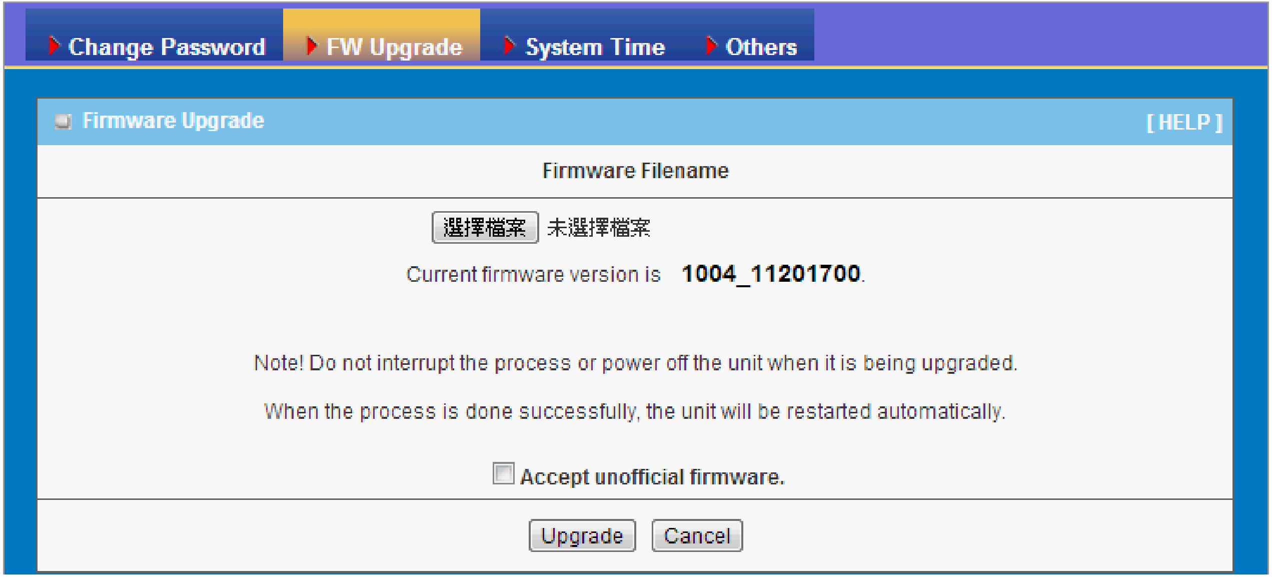
You can change the System Password here. We **strongly** recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



Item	Setting
Old Password	
New Password	
Reconfirm	

3.3.3.2 FW Upgrade

If new firmware is available, you can upgrade device firmware through the WEB GUI here.



Current firmware version is **1004_11201700**.

Note! Do not interrupt the process or power off the unit when it is being upgraded.

When the process is done successfully, the unit will be restarted automatically.

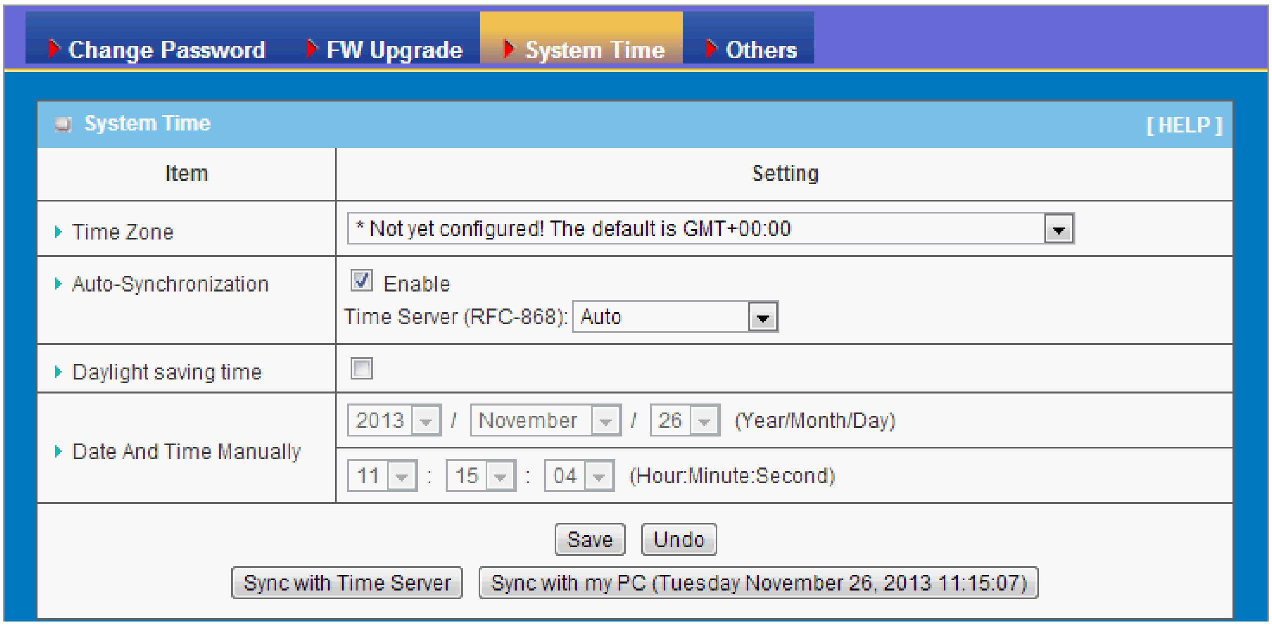
□ Accept unofficial firmware.

Press “browse” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

3.3.3.3 System Time

If new firmware is available, you can upgrade device firmware through the WEB GUI here.



System Time

Item	Setting
Time Zone	* Not yet configured! The default is GMT+00:00
Auto-Synchronization	☑ Enable Time Server (RFC-868): Auto
Daylight saving time	□
Date And Time Manually	2013 / November / 26 (Year/Month/Day) 11 : 15 : 04 (Hour:Minute:Second)

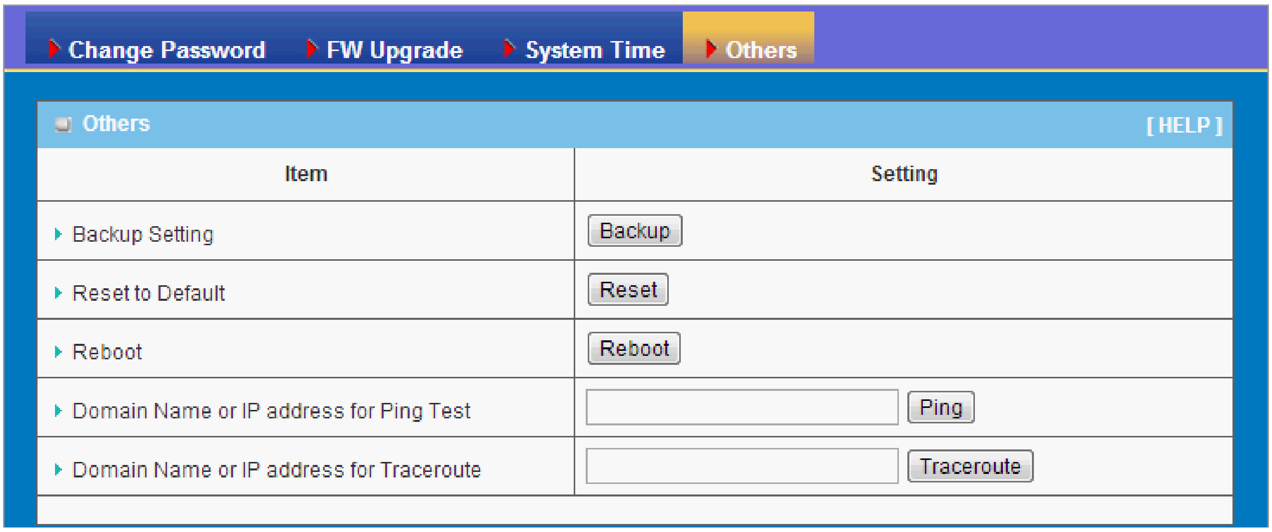
Sync with my PC (Tuesday November 26, 2013 11:15:07)

1. **Time Zone**: Select a time zone where this device locates.
2. **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol.
4. **Sync with my PC**: Click on the button if you want to set Date and Time using the PC’s Date and Time.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.3.4 Others

In this section you can do system backup, reset to default, system reboot settings and ping test.

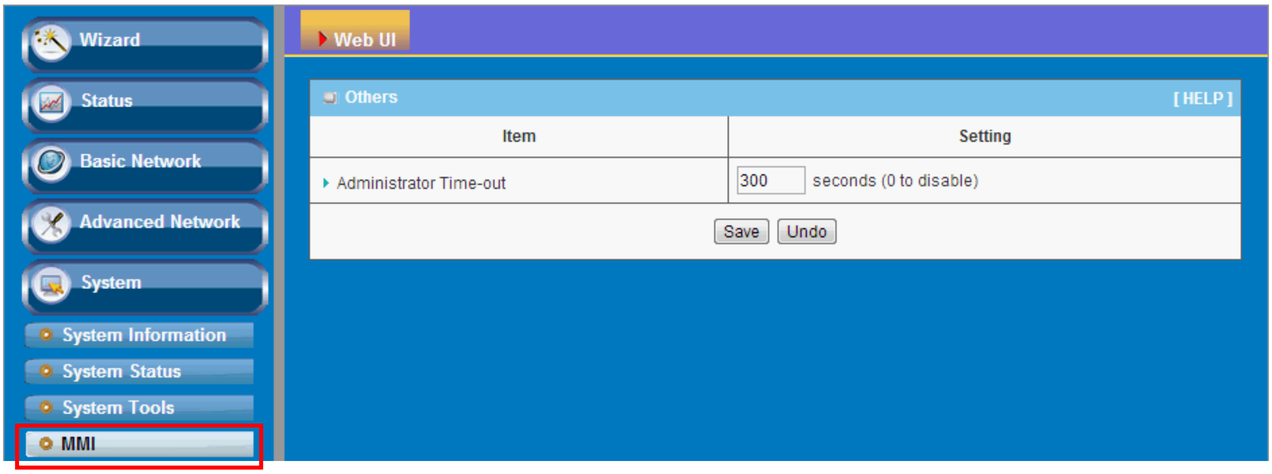


Item	Setting
Backup Setting	Backup
Reset to Default	Reset
Reboot	Reboot
Domain Name or IP address for Ping Test	Ping
Domain Name or IP address for Traceroute	Traceroute

1. **Backup Setting**: You can backup your settings by clicking the “**Backup”** button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.
2. **Reset to Default**: You can also reset this device to factory default settings by clicking the “**Reset**“ button.
3. **Reboot**: You can also reboot this device by clicking the “**Reboot**“ button.
4. **MAC Address for Wake-on-LAN**: Wake-on-LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can enter the MAC address of the computer, in your LAN network, to be remotely turned on.
5. **Domain Name or IP address for Ping Test**: This allows you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.
6. **Domain Name or IP address for Traceroute**: Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point

3.3.4 MMI

3.3.4.1 Web UI



Item	Setting
Administrator Time-out	300 seconds (0 to disable)

You can set UI administration time-out duration give remote administration host port in this page. When the host port is given please remember to check the enable box and save your settings.

CHAPTOR 4 Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the WiFi Concurrent N300 Business AP. You can refer to the following if you are having problems.

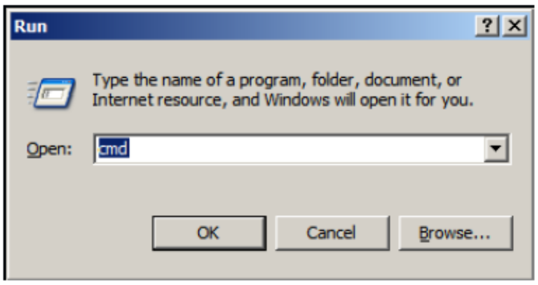
1 Why can’t I configure the device even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Access Point is responding.

Note: *It is recommended that you*

Go to **Start > Run**.

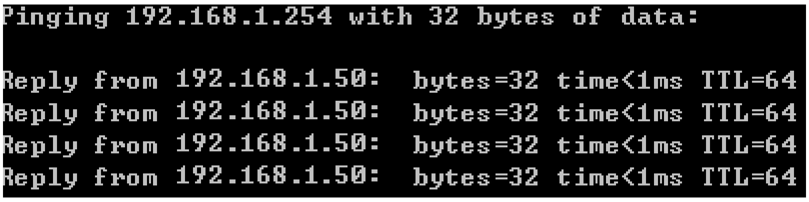
1. Type **cmd**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

2. Press **OK.**
3. Type **ipconfig** to get the IP of default gateway.
4. Type “**ping 192.168.1.50”.** Assure that you ping the correct IP Address assigned to the WiFi Concurrent N300 Business AP. It will show four replies if you ping correctly.



```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.50:  bytes=32 time<1ms TTL=64
Reply from 192.168.1.50:  bytes=32 time<1ms TTL=64
Reply from 192.168.1.50:  bytes=32 time<1ms TTL=64
Reply from 192.168.1.50:  bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on "My Computer" > Properties**.
2. **Select** the **Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on "**Network Adapters"**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click "**OK"**.

2 What can I do if my Ethernet connection does not work properly?

A. Make sure the RJ45 cable connects with the device.

B. Ensure that the setting on your Network Interface Card adapter is "Enabled".

C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.

D. If the connection still doesn't work properly, then you can reset it to default.

3 Something wrong with the wireless connection?

A. Can't setup a wireless connection?

I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.

II. Move the WiFi Concurrent N300 Business AP and the wireless client into the same room, and then test the wireless connection.

III. Disable all security settings such as **WEP**, and **MAC Address Control**.

IV. Turn off the WiFi Concurrent N300 Business AP and the client, then restart it and then turn on the client again.

V. Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.

VI. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.

VII. If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

B. What can I do if my wireless client can not access the Internet?

I. Out of range: Put the device closer to your client.

II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.

III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.

  i. **Right-click** on the **Local Area Connection icon** in the taskbar.

  ii. Select **View Available Wireless Networks in Wireless Configure**. Ensure you have selected the correct available network.

  iii. Reset the WiFi Concurrent N300 Business AP to default setting

C. Why does my wireless connection keep dropping?

I. Antenna Orientation.

  i. Try different antenna orientations for the WiFi Concurrent N300 Business AP.

  ii. Try to keep the antenna at least 6 inches away from the wall or other objects.

II. Try changing the channel on the WiFi Concurrent N300 Business AP, and your Access Point and Wireless adapter to a different channel to avoid interference.

III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4 What to do if I forgot my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the WiFi Concurrent N300 Business AP to default setting

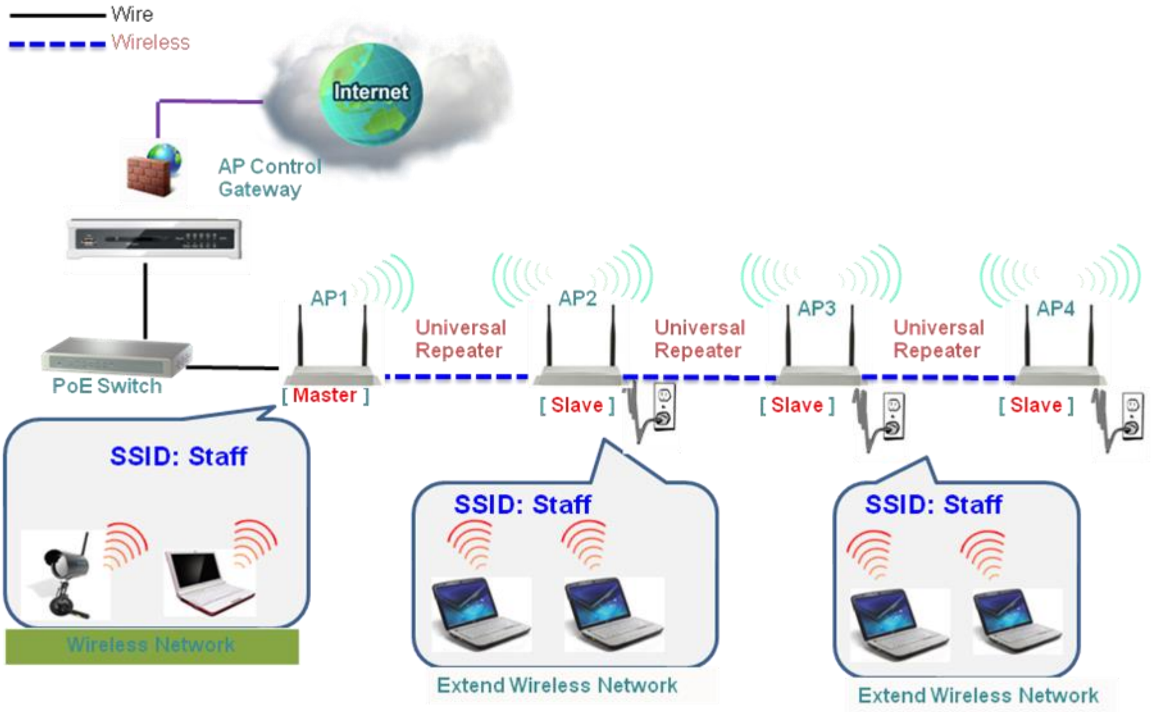
5 How to reset to default?

1. Ensure the WiFi Concurrent N300 Business AP is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the WiFi Concurrent N300 Business AP reboots, it has back to the factory **default** settings.

CHAPTOR 5 Application Description

5.1 Wireless Operation Mode

Application 1: Network Wireless Extend



Due to Limited environment, End-user uses Universal Repeater to extend Network access . For example:

1.Add AP2 ,AP3,AP4 to deploy

2.Switch AP2 ,AP3 and AP4 as Slave Mode via WEC Button

3.Click WEC Button of master AP1 and slave AP2 as one pair simultaneously

4.Click WEC Button to sync "Slave AP2 ,slave AP3"
and ""Slave AP3 ,slave AP4" "as one pair.

5.Setup "Extend Wireless" in sequence as follows: AP1→AP2→AP3→AP4

※If AP3 is removed, just Click WEC Button to sync "Slave AP2 ,slave AP4" as one pair.

Appendix A. Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux Kernel	GPLv2	Linux-2.6.21
busybox	GPLv2	busybox_1.3.2
bridge-utils	GPLv2	bridge-utils 1.1
udhcp server	GPLv2	udhcp-0.9.9

udhcp client		
fdisk	GPLv2	util-linux 2.12q
mke2fs, e2fsck	GPLv2	e2fsprogs v1.40.2
samba	GNUv2	samba 3.0.20
wireless tools	GPLv2	wireless tools
vsfptd	GPLv2	vsftpd-2.0.3
Transmission	MIT	Transmission-1.74
mt-daapd	GNUv2	mt-daapd-0.2.4
dnrd	GNUv2	DNRD-2.17
libcurl	cURL-7.19.6	
OpenSSL	BSD	openssl-1.00b3
ntfs-3g	GNUv2	ntfs-3g-2009.4.4
Zebra	GNUv2	zebra-0.95a
snmpd	CMU	snmp-4.1.2
pptp	GNUv2	pptp-1.7.1
pppoe	GPLv2	pppoe-3.8
pppd	BSD	ppp-2.4
l2tpd	GPLv2	l2tp-0.4
iptables	GNUv2	iptables-1.4.2
tc	GNUv2	iproute2-2.6.11
wget	GNU	wget-1.7.1

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If

you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS