High speed access point/CPE 300 Mbps

AP/CPE OUTDOOR WIRELESS

Model: GO300N

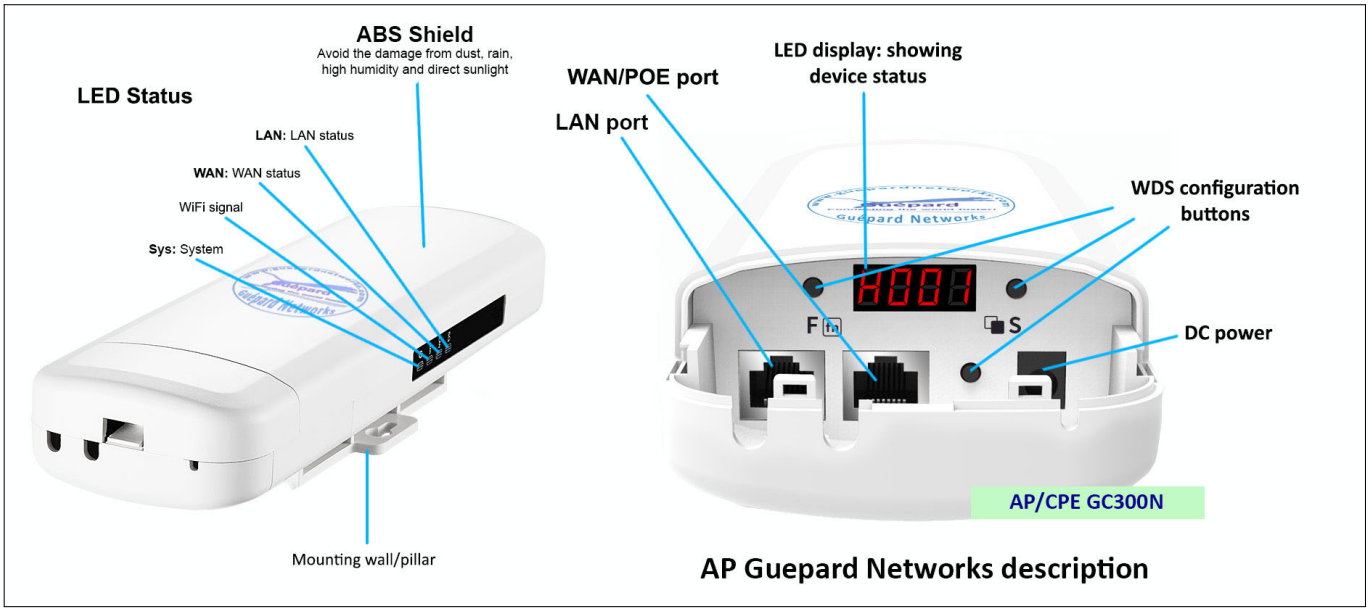
ADVANCED TECHNOLOGY

GO300N was integrated Qualcomm's chipsets. This is an 11N 300Mbps High Power Outdoor CPE/AP/Router/WISP, wireless distance can be 500 - 1.000 meters *(as pair CPEs)*. This Outdoor CPE with the 802.11n Wi-Fi standard combined 300Mbps Wi-Fi speed over 2.4GHz (300Mbps) and equipped fast ethernet WAN port, fast ethernet data rate can be taking care 20-40 end users at the same time. Matching access demand to enjoy seamless HD movies, streaming, online gaming, wireless security and other bandwidth-intensive tasks.

GO300N with user-friendly Web management interface and multi-operation mode like: AP, WDS, Repeater, Gateway, multi-function for many appications.

1st Hardware and Operation mode Instruction

1) Hardware interface



P1. GO300N physical interface

LED display: parameter indicator: *(first character indicate **H**: Host - master or **C**: Client – slave or **P**: Power of transmit frequency; second number indicate: last 3 number of IP address or strength of transmit frequency from 1-10).*

DC Power: DC power connector

LED Lights: LED Indicator of System/WiFi signal/WAN port/LAN port.

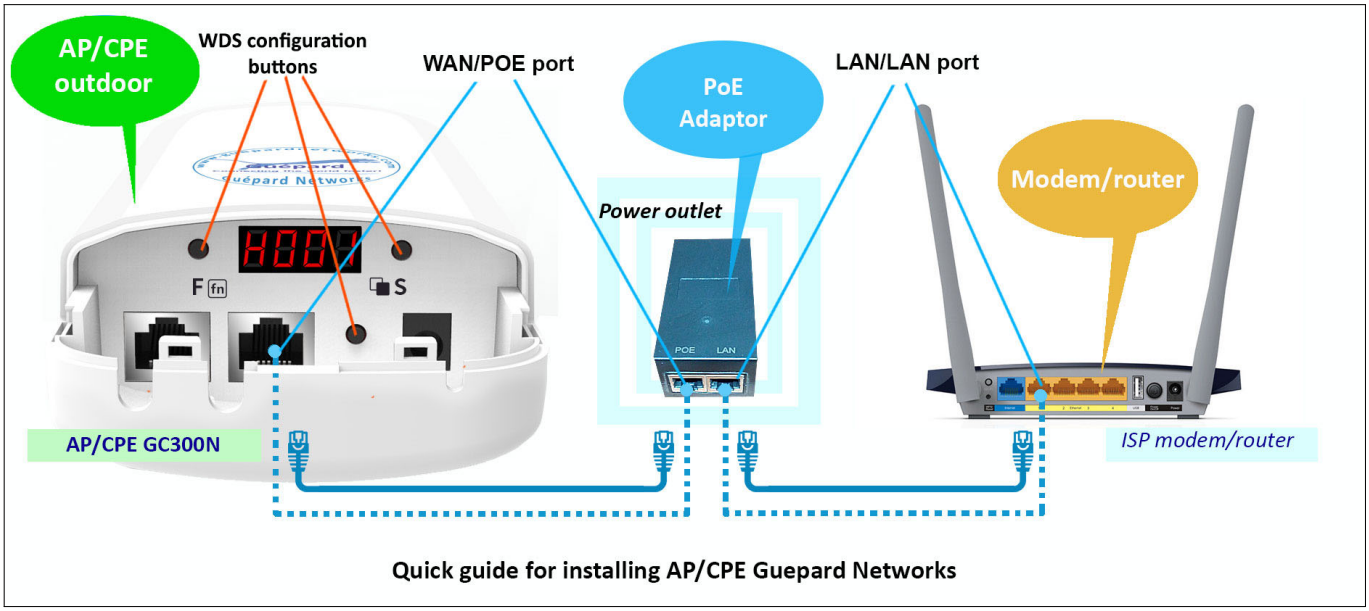
WAN/POE Port: Fast ethernet WAN/POE Port this port using connect with ADSL modem or Internet mainly or over POE adapter *(if do not use DC Power connector)*.

LAN: Fast ethernet LAN Port for more cable end users.

WDS configuration Button (F, S, reset): making paired CPEs.

2) How to supply data and power to GO300N?

The connection diagram showed as P1, internet cable connect to PoE adapter's LAN Port, GO300N's WAN/POE port connect to POE adapter's POE Port, then end users will access into GO300N through cable (GO300N's LAN port) or wireless (2.4GHz).



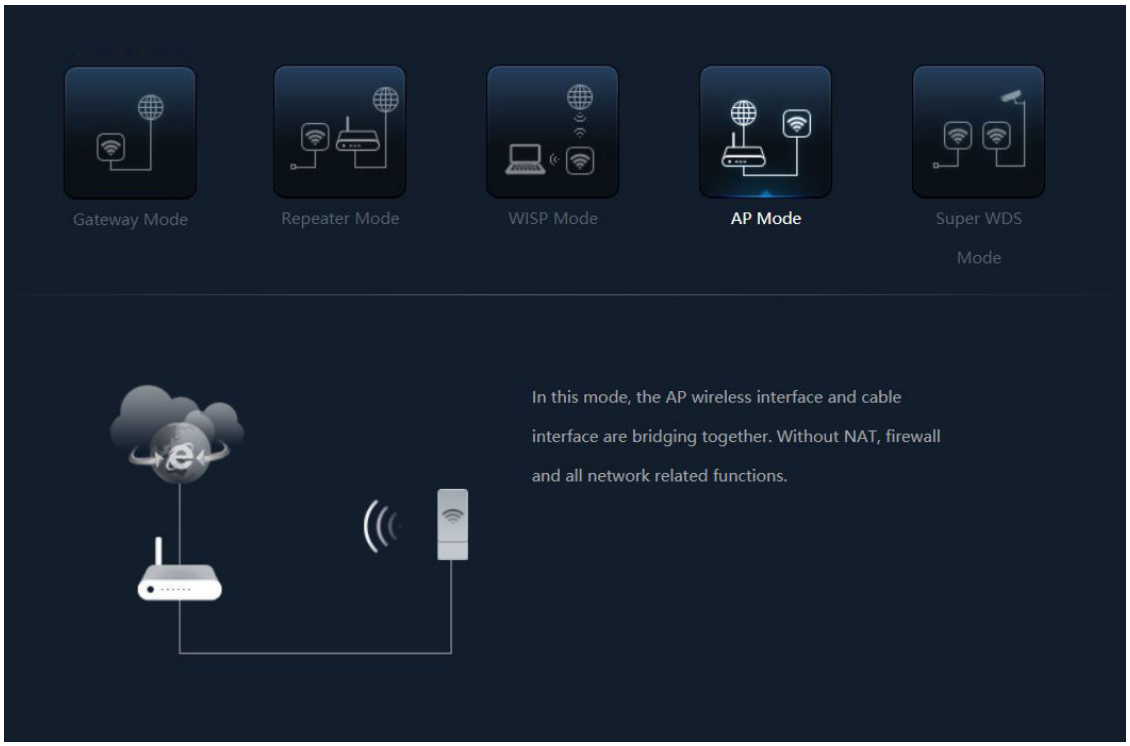
P2. GO300N use PoE adapter: 24V passive PoE (attached in GO300N complete set)

Please note: *if the Wireless AP support 24V passive PoE then the PoE adapter should be 24V Passive PoE. If the wireless AP support 48V IEEE 802.3af/at standard PoE then the PoE adapter should be 48V PoE standard.*

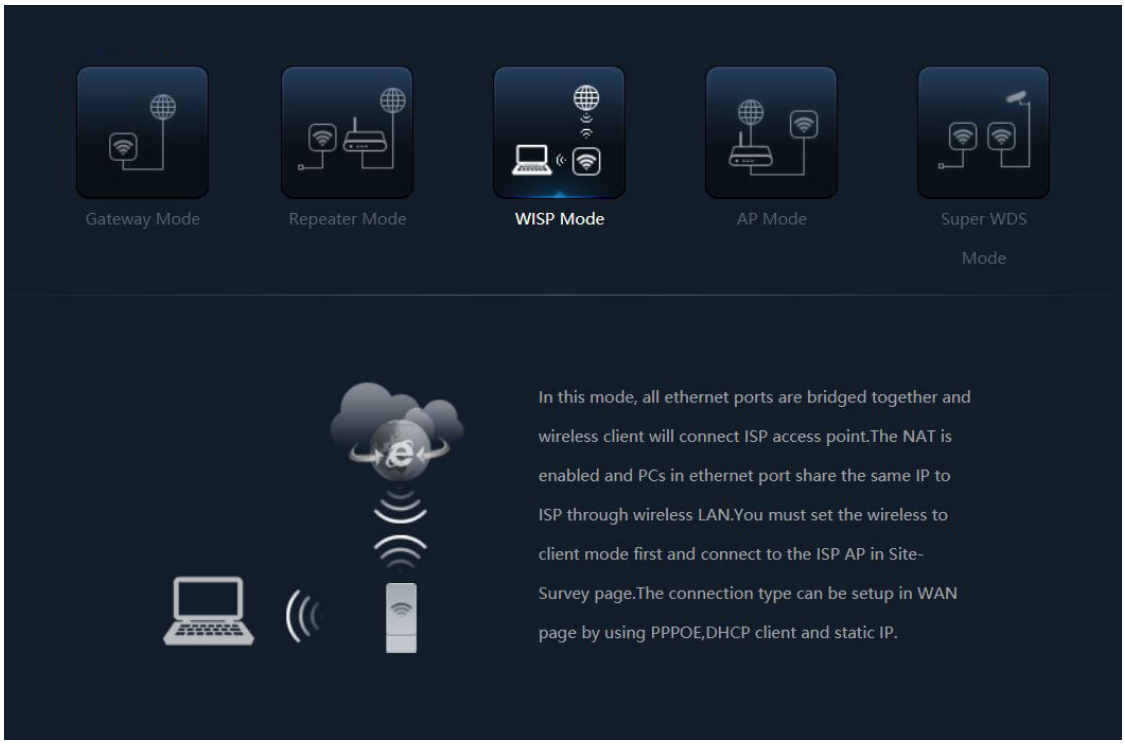
All operation modes

Operation as diagram as below:

P3. Gateway mode diagram



P4. AP mode diagram



P5. WISP mode diagram

P6. Repeater mode diagram

P7. Super WDS mode diagram

There are five operation modes on this wireless AP/CPE.

How to connect GO300N Wireless AP

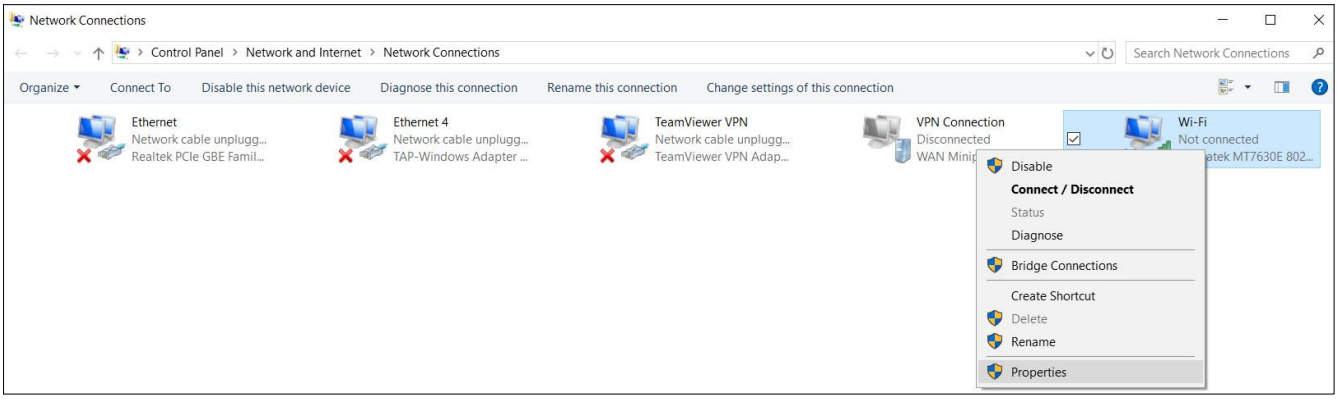
Users can connect the PC/Laptop/Smartphone/Tablet… into this wireless AP by Wireless SSID and LAN cable: The default SSID is **Wireless 2.4G** for 2.4GHz, SSID's password is **66666666** *(number six eight times)*.

2st GUI Login (Graphic User Interface)

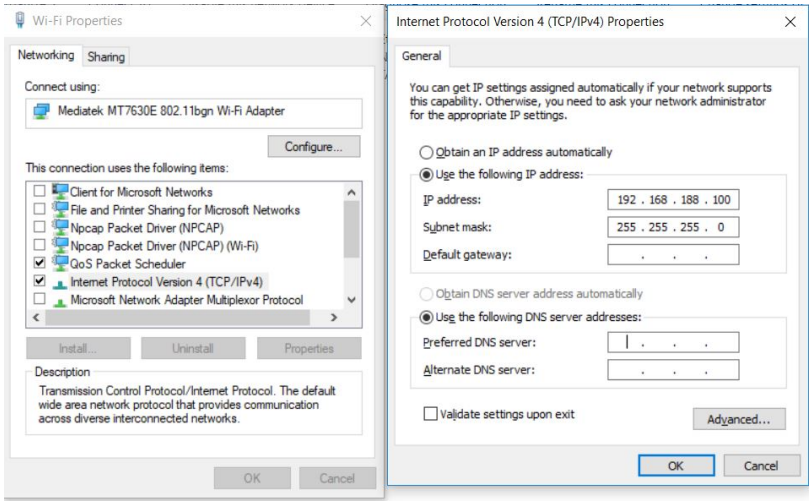
1） Choose the proper power supply mode and operation mode

2） Assign an IP address for local PC/Workstation

Following steps will show how to assign an IP address (static IP) for PC after connect wireless AP and PC by wired cable or wireless: configure local IP address as **192.168.188.X** *(X can be selected from 2-252)* the same network segment as ceiling AP, subnet mask 255.255.255.0, As P3 and P4 shows.



*P8. Check **Control Panel>Network and Internet>Network Connections>Wi-Fi>Properties** (Win 10)*



P9. Assign IP address for PC/Workstation (Such as: 192.168.188.100)

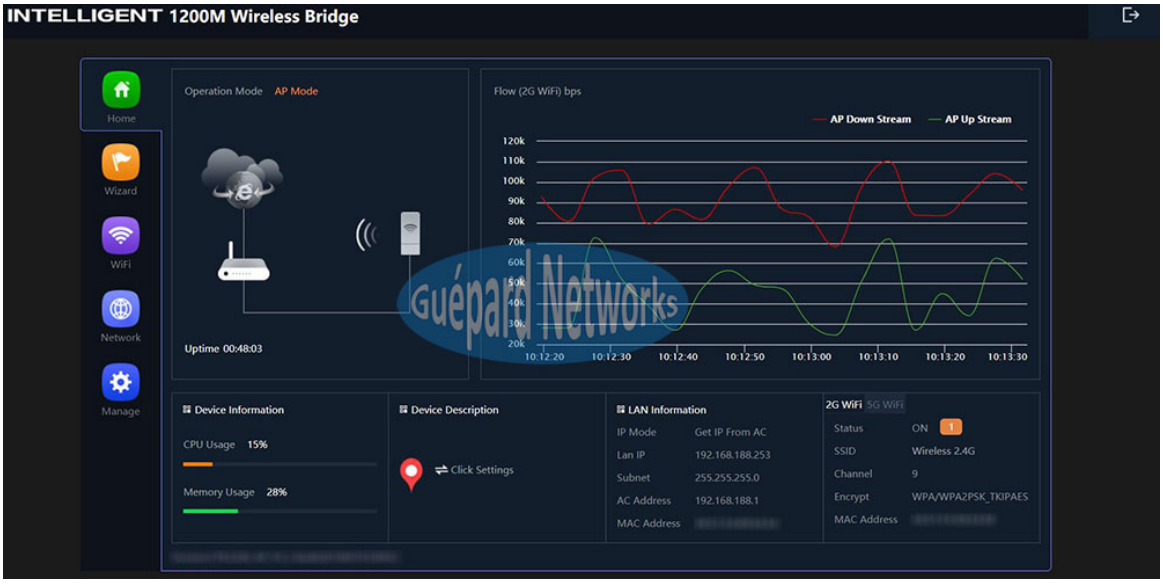
3) Open browser Microsoft Edge, Chrome, Firefox… and input device's default IP **192.168.188.253** *(this is IP default of Wireless AP)* on the address bar, then press Enter, a login page will pop up, input **admin** in Login Device cell, then press Enter or Login button on Admin interface.

Note: GO300N GUI (support 2.4GHz band) same as GUI GO1200ac excepted GO300N did not support dual band 2.4GHz/5.8GHz. So we use Illustrated GO1200ac picture for GO300N.

P10. Login interface (GO300N GUI same as Illustrated GO1200ac picture).

3rd Settings GUI (Graphic User Interface)

1) Home *(Device status)*: After success login, then P6 Device Status will be showed:



P11. Infographic of Device Status (GO300N GUI same as Illustrated GO1200ac picture).

Note: GO300N GUI (support 2.4GHz band) same as GUI GO1200ac excepted GO300N did not support dual band 2.4GHz/5.8GHz

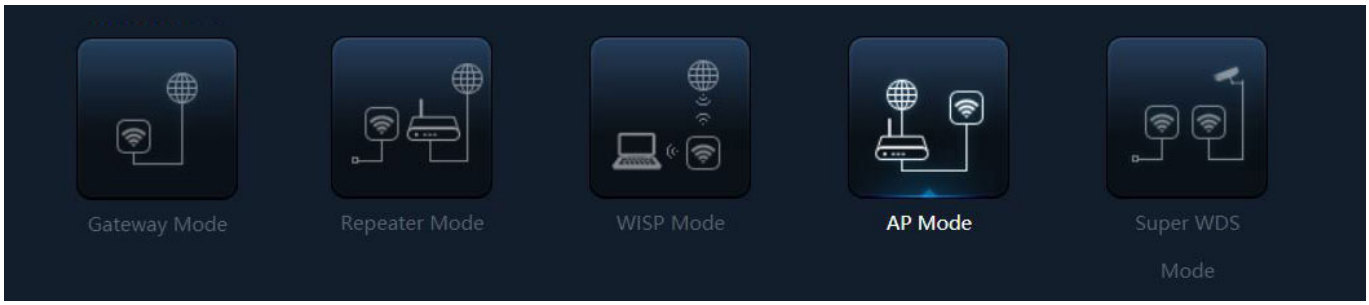
Home *(Detail of indices):*

- Operation Mode: Current mode of device *(As P6 picture above is **AP mode**)*
- *Uptime: device period time running until current (As P6 picture above is **48 minutes and 03 seconds**).*
- Flow (2G WiFi) bps: Flow chart of 2.4GHz describe flow of AP upstream and downstream in real time.
- Device Information: ratio of CPU, Memory usage.
- Device Description: description space for this device *(Ex: administrator can input device name, location… which hint for maintenance).*
- LAN Information: showing LAN parameter such as: IP Mode, LAN IP, Subnet, AC/Gateway Address, MAC Address.
- 2G WiFi/5G WiFi: tab showing 2G WiFi/5G WiFi parameter such as: Status (online users), SSID, Channel, Encrypt, MAC Address.

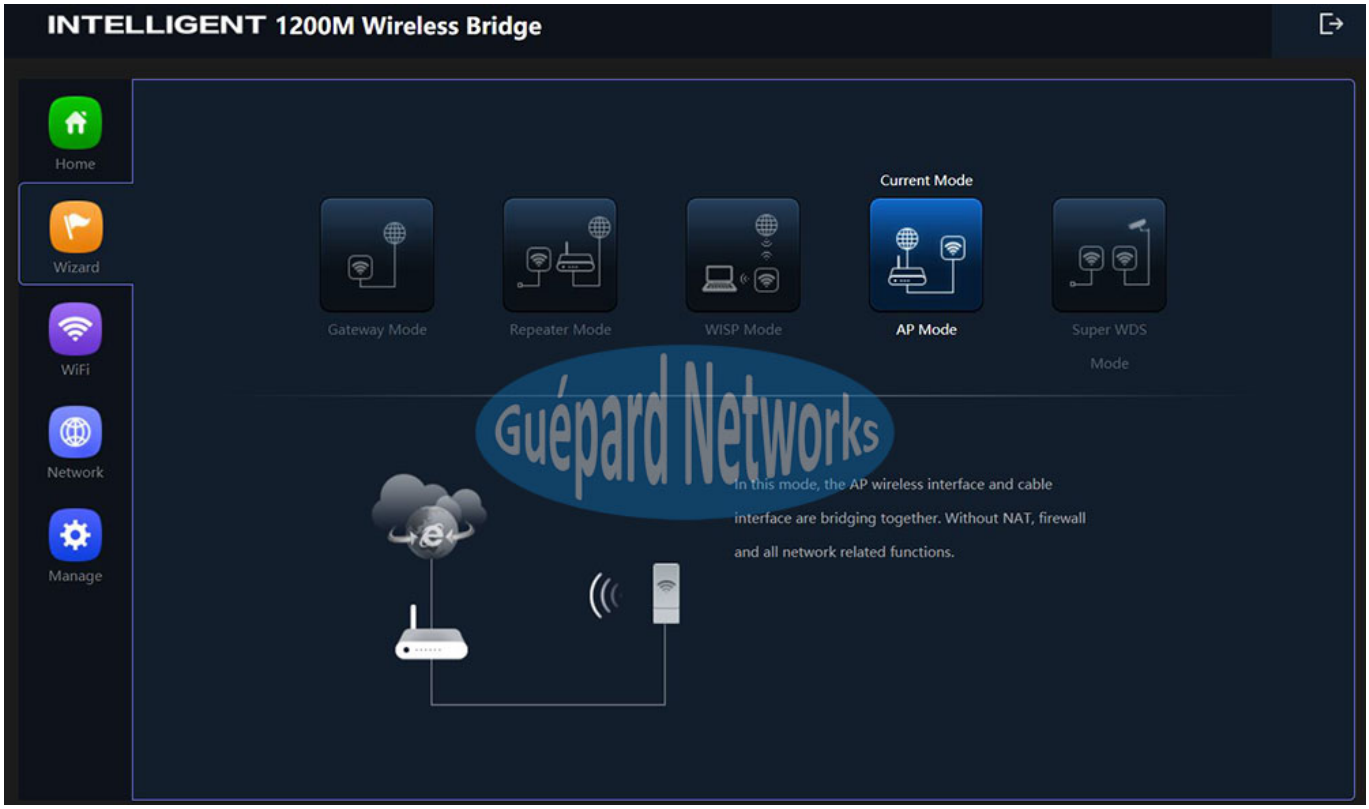
2) Wizard: Shortcut for switching wireless AP's operation modes.

Click ***Wizard*** in Status page will have pop-up following page to configure the operation mode:

There are five operation mode of ceiling wireless AP and there are explanation for each operation mode for better use, see P7 below:



P12. Switching function between wireless AP/CPE's operation modes.



P13. Device is running in AP mode (GO300N GUI same as Illustrated GO1200ac picture).

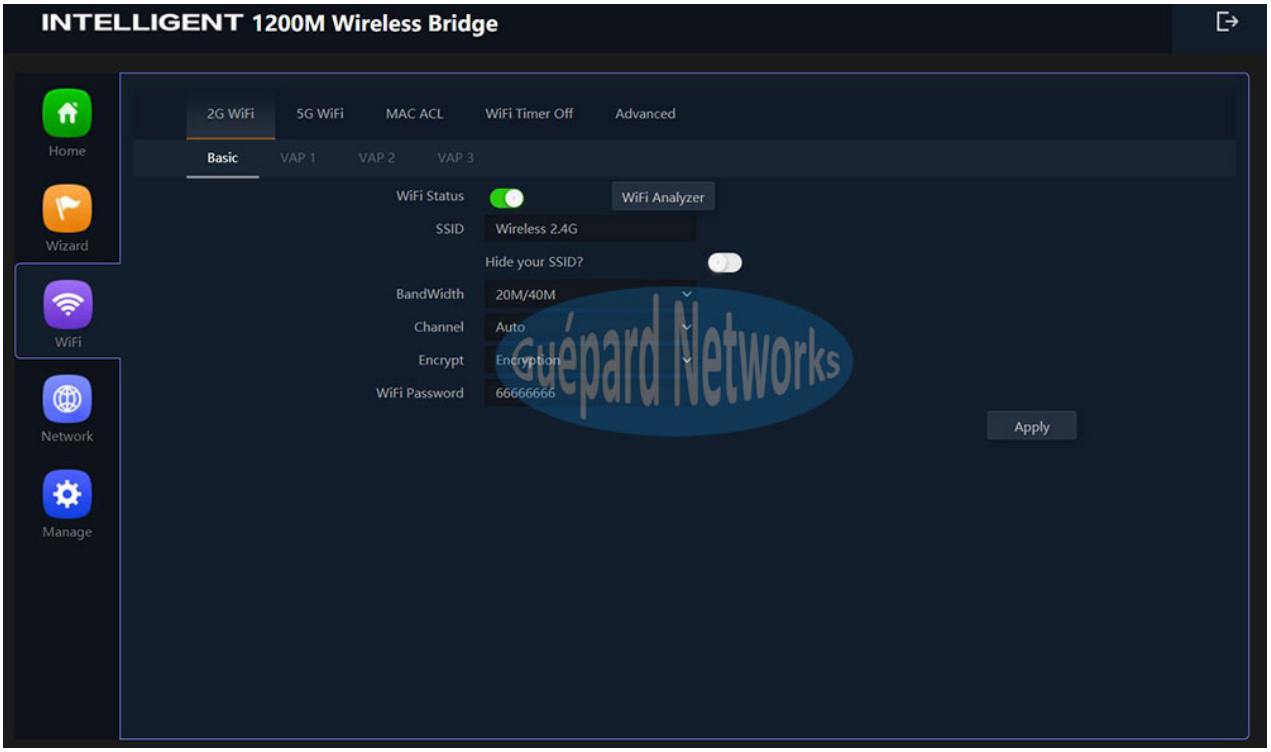
There are five operation mode of ceiling wireless AP and there are explanation for each operation mode for better use.

- ***Gateway Mode:*** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enable and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.
- ***Repeater Mode:*** In this mode, the user can access wireless AP, device can be connected to other wireless network using the wireless. All interfaces are bridged together. Without NAT, firewall and all network related functions.
- ***WISP Mode:*** In this mode, all Ethernet ports are bridged together and wireless clients will connect ISP access point. The NAT is enabled and PCs in Ethernet port share the same IP to ISP through wireless LAN. You must set wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client and static IP.
- ***AP Mode:*** In this mode, the AP wireless interface and cable interface bridging together. Without NAT, firewall and all network related functions.
- ***Super WDS Mode:*** In this mode, the wireless interface can be connected with other wireless AP through WDS *(The Wireless Distribution System)*, and the wireless interface and cable interface. Without NAT, firewall and all network related functions.

3) WiFi:

In **WiFi**, user can check and configure all indices: 2G WiFi, 5G WiFi, MAC ACL, WiFi Timer Off, Advanced.

■ **2G WiFi:** This section allow configure 04 SSIDs in 2.4GHz frequency, such as: Basic, VAP1, VAP2, VAP3.



P14. WiFi configuration for 2.4GHz frequency (GO300N GUI same as Illustrated GO1200ac picture).

… WiFi Status: Switching button is green meaning this SSID is On status. ***WiFi Analyzer*** button is utility for checking all APs and their broadcast channel in current region, which will help us choosing good channel to broadcasting.

… SSID: naming SSID for device in 2.4GHz frequency.

… Hide your SSID?: hiding device's SSID after setting up and connecting.

… BandWidth: choosing broadcasting bandwidth which will give full device bandwidth or half bandwidth with longer distance.

… Channel: choosing device's broadcasting channel which will have not interference with other AP's channel.

… Encrypt: choosing Encryption *(with Password)* or Open *(without Password)*

… WiFi Password: inputting password *(if choosing Encryption)*

… WiFi Status: Switching button is green meaning this SSID is On status. ***WiFi Analyzer*** button is utility for checking all APs and their broadcast channel in current region, which will help us choosing good channel to broadcasting.

… SSID: naming SSID for device in 5.8GHz frequency.

… Hide your SSID?: hiding device's SSID after setting up and connecting.

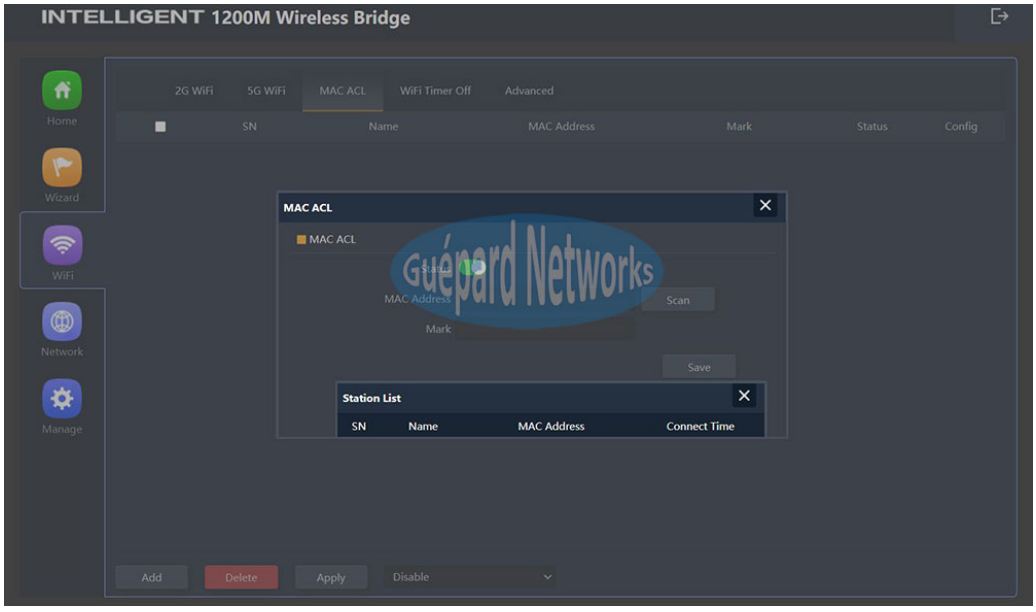
… BandWidth: choosing broadcasting bandwidth which will give full device bandwidth or half bandwidth with longer distance.

… Channel: choosing device's broadcasting channel which will have not interference with other AP's channel.

… Encrypt: choosing Encryption *(with Password)* or Open *(without Password)*

… WiFi Password: inputting password *(if choosing Encryption)*

■ **MAC ACL:** This section manage users with MAC/ACL in Access Control List. Users in this list is under device management, Disable *(Disable this function)* or allowing *(Allows the device to pass in the rule)* or denied *(Prohibited rules within the device through)* clients/users access device.



P16. ACL configuration.

… Status: click ***Add*** button for adding new user. Switching button is green meaning this function is On status.

… MAC Address: MAC address of user/client. ***Scan*** button is utility for checking all users and their MACs.

… Mark: marking users for hint.

… Click ***Apply*** button for applying new user or ***Delete*** for deleting user.

■ **WiFi Timer Off:** This function will set Off period of device.

P17. WiFi Timer Off.

… WiFi Timer Off: Switching button is green meaning this function is running.

- Time Frame: choosing time frame.
- Click ***Apply*** button for finish.

■ **Advanced**

P18. WiFi Advanced configuration.

… Country Region: Set channels for 2.4GHz match country policy *(Reference: https://en.wikipedia.org/wiki/List_of_WLAN_channels)*
… 2G Mode: choosing 802.11 protocol standards for 2.4GHz frequency, such as: 802.11 b/g/n.
… Multicast Fast: On/Off this function *(definition reference: https://en.wikipedia.org/wiki/Multicast).*
… Maximum for per AP: allow max users connect per AP.
… WLAN Partition: This feature effectively segregates the wireless band of your choice from the rest of the Network. With Ethernet-to-WLAN Access disabled.
… Short GI (switch On/Off): Guard Interval is intended to avoid signal loss from multi-path effect.
… Coverage Threshold: This function allow GO300N's antennas improving more sensitive to client devices. Which help GO300N can keep tight connection with clients and improving broadcasting distance.
… Packet Threshold: This value is used to set the maximum size of packet a client can send. Smaller packets improve reliability, but they will decrease performance. Unless you're facing problems with an unreliable network, reducing the fragmentation threshold is not recommended. Make sure it is set to the default settings (recommend 2346).
… RTS Threshold: RTS stands for 'Request to send' and is send by the client to the access point – it essentially asks for permission to send the next data packet. The lower the threshold, the more stable your Wi-Fi network, since it essentially asks more often when sending packages. However, if you don't have problems with your Wi-Fi you should make sure that the RTS Threshold is set to the maximum allowed.
… TX Power: This function allow to increase transmitting power which will device transmitting longer distance and passing more barrier (wall, floor, tree canopy…)
… DFS: Dynamic Frequency Selection (DFS) is a WiFi function that enables WLANs to use 5 GHz frequencies that are generally reserved for radars. If you are planning to use DFS channels, you first have to verify that both

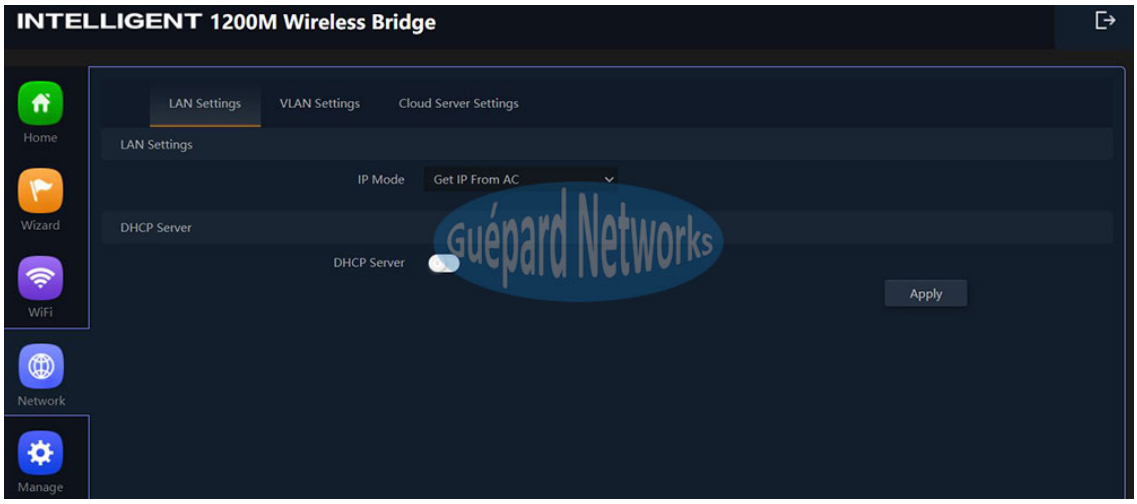
your WiFi access points and wireless clients support this functionality.

… 2G Distance: choosing suitable distance scenario for pair CPEs in 2.4GHz frequency.

4) Network:

Setting up Network on device.

➢ **AP Mode:** When AP run in AP Mode



P19. WiFi configuration in AP mode.

■ **LAN Settings** *(AP Mode)*

… IP Mode: choosing method to get IP from LAN *(Such as: Static IP/Get IP from AC/Gateway).*

… Click ***Apply*** button for finish.

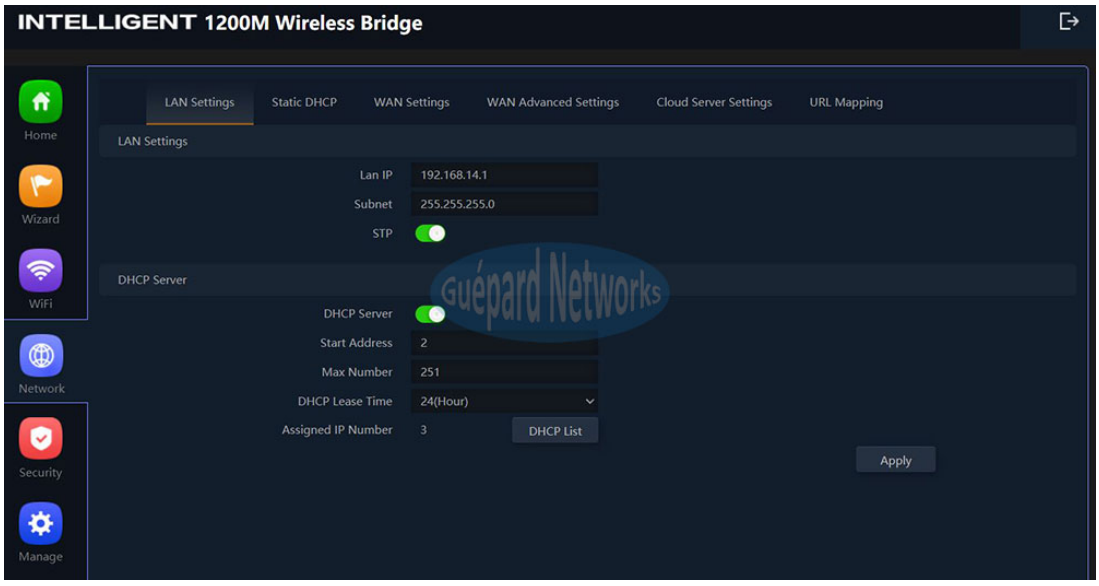
■ **VLAN Settings:** configuring VLAN per SSID. For using this function, checking ***On*** in drag list at the bottom GUI.

P20. VLAN Settings in AP mode.

… 2G WiFi: input VLAN per SSID in 2.4GHz frequency *(Such as: AP/VAP1/VAP2/VAP3).*

… Click ***Apply*** button for finish.

➢ **Gateway Mode:** When AP run in Gateway Mode



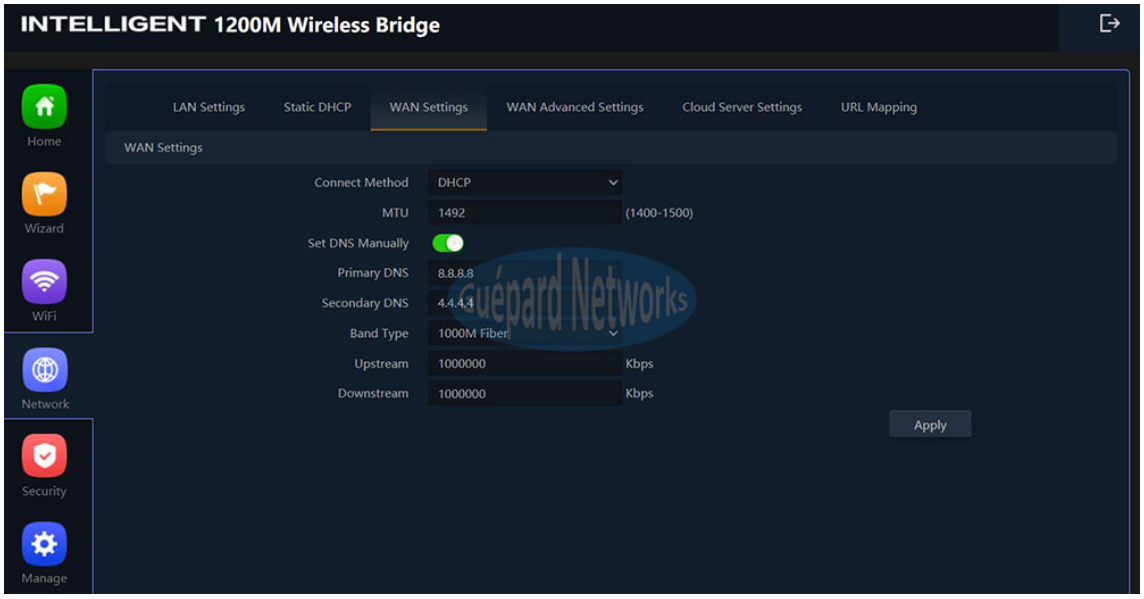
P21. WiFi configuration in Gateway mode.

■ ***LAN Settings*** *(GatewayMode)*

- … LAN IP: inputting range LAN IP of device *(static IP host)*.
- … Subnet: inputting LAN Subnet.
- … STP *(Spanning Tree Protocol)*: switching button to green to activate this function.
- … DHCP Servers *(Dynamic Host Configuration Protocol)*: switching button to green to activate this function.
- … Start Address: inputting start IP address *(avoid IP address had setup in LAN IP above).*
- … Max Number: inputting quantity of IP addresses except LAN IP of device*(limited quantity: 254 IP addresses)*
- … DHCP Lease Time: choosing time period to release all IP addresses.
- … Assigned IP Number: Numbers of IP addresses have been assigned. Clicking ***DHCP List*** button to view assigned IPs.

■ **Static DHCP:** setting up LAN clients/users with static IP by using this function.

■ **WAN Settings:** this function is configure WAN port which connect ISP's modem, router, fiber converter or business's switch, router.



P22. WAN Settings configuration in Gateway mode.

- … Connect Method: choosing which connecting method use for device *(Static, PPPoE, DHCP).*
- … MTU: the maximum transmission unit the size of the largest protocol data unit (PDU) that can be communicated in a single network layer transaction *(we can set: 1400-1500).*
- … Set DNS Manually: setting default DNS for device. We can use DNS information of ISP or another public DNS, such as Google: 8.8.8.8/8.8.4.4
- … Primary DNS: configuring first DNS information.
- … Secondary DNS: configuring second DNS information *(if Primary DNS is busy or timeout)*.
- … Band Type: choosing real bandwidth which connect to WAN port.
- … Upstream: inputting allowed upstream bandwidth.

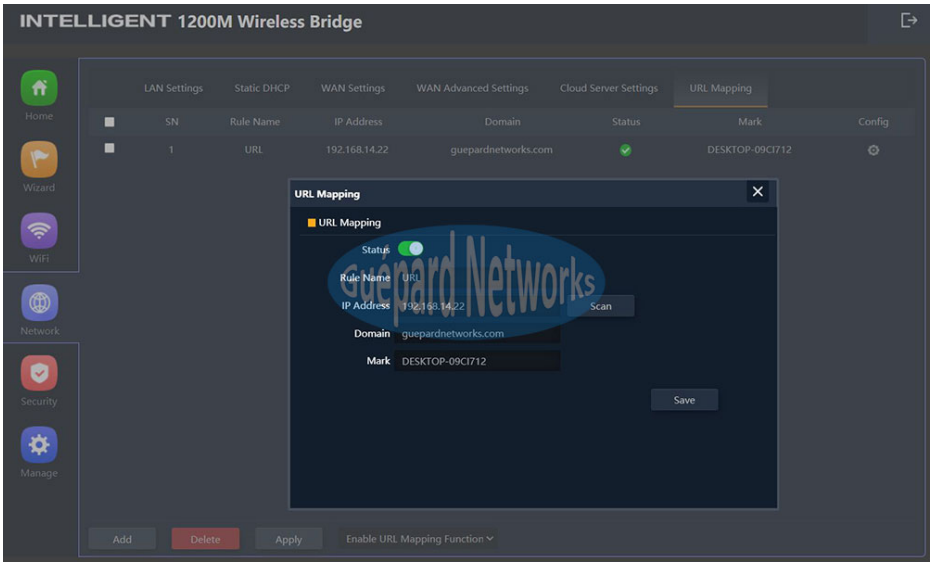
… Downstream: inputting allowed downstream bandwidth.

- **WAN Advanced Settings:**

P23. WAN Advanced Settings

… Enable web server access on WAN port *(8080)*: Switching button to green to activate this function.
… MAC Clone: cloning client/user MAC. Switching button to green to activate this function.
… Enable Ping Access on WAN: Allowing clients/users outside LAN can ping this device over WAN port connection. Switching button to green to activate this function.
… Enable IPsec pass through on VPN connection: Switching button to green to activate this function.
… Enable PPTP pass through on VPN connection: Switching button to green to activate this function.
… Enable L2TP pass through on VPN connection: Switching button to green to activate this function.

- **URL Mapping:**

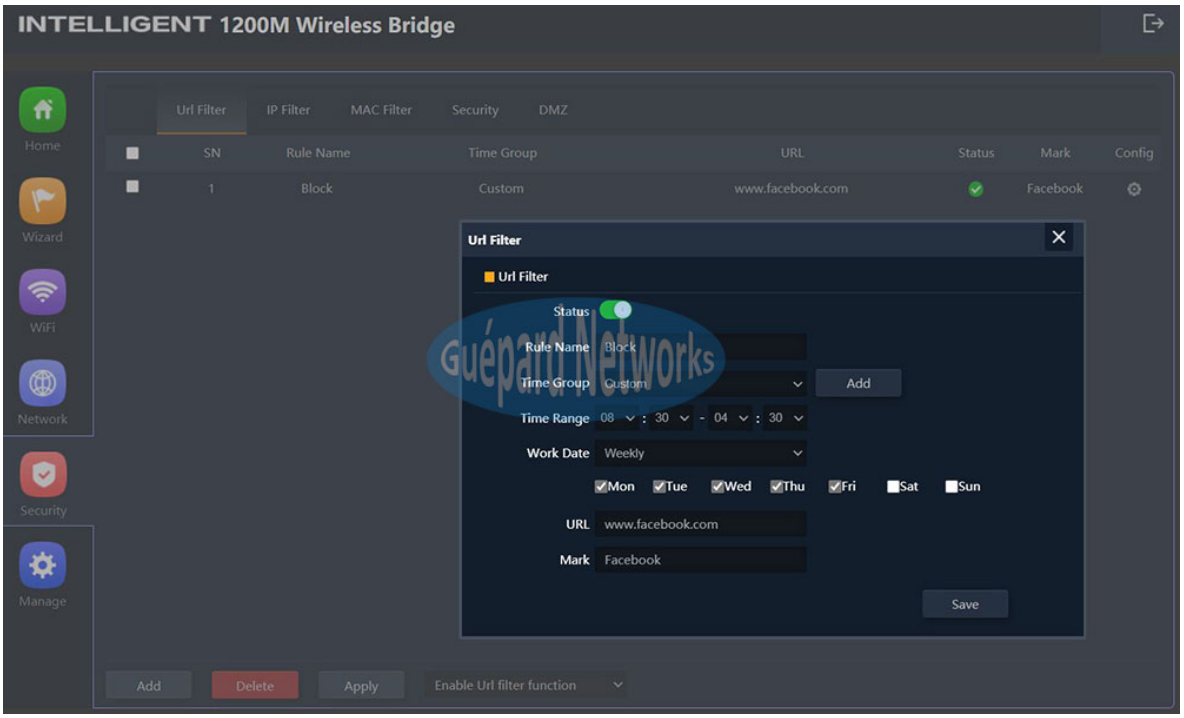


P24. Configuring URL Mapping

5) Security: running in Gateway/WISP Mode

➢ **Gateway Mode:** When AP run in Gateway Mode

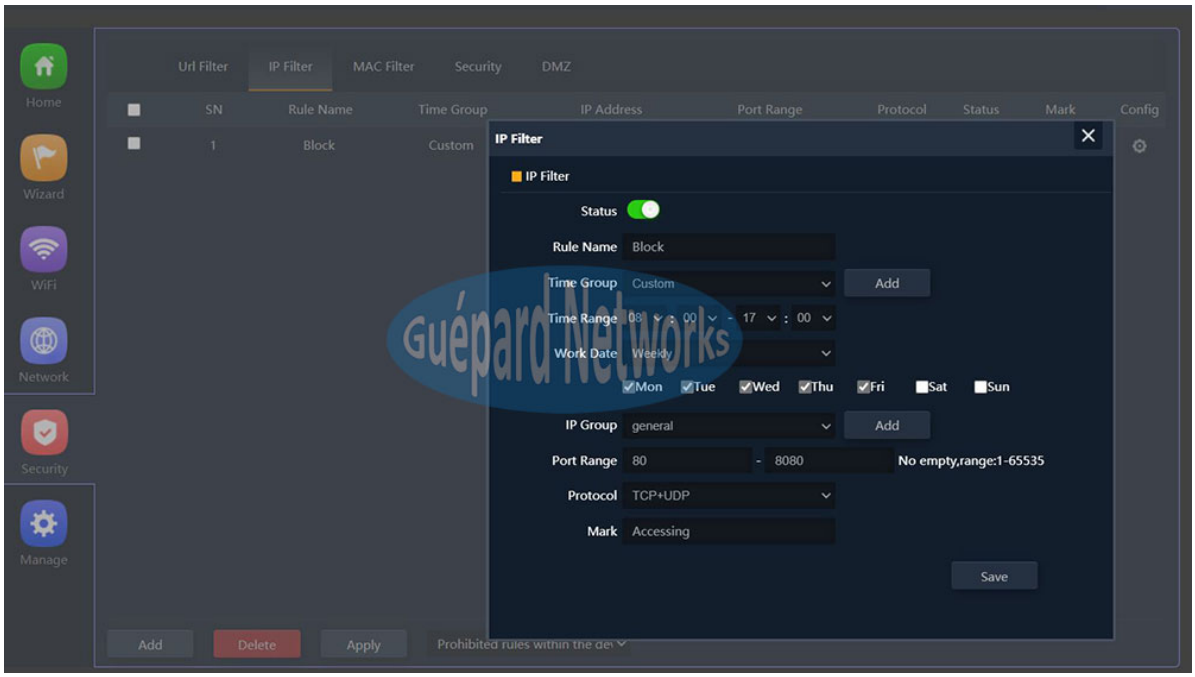
■ **URL Filter:** this function issues rules permit or prohibit staffs/users access prohibited websites with schedule time or permanent.



P25. Configuring URL Filter

… Click ***Add*** button in the bottom for creating new rule.
… Switching button ***Status*** to green to activate this rule.
… Rule Name: naming the rule.
… Time Group: choosing created previous time group or Any or Custom for applying this rule.
… Time Range: scheduling time in hours.
… Work Date: scheduling time in daily or week.
… URL: website address for applying this rule.
… Mark: marking hint.
… Click ***Save*** button for saving new rule.
… Apply all rules by choosing *Enable URL Filter Function* in bottom drag list, click ***Apply*** button for finish.
… Remove rule by choosing rule and click ***Delete*** button in the bottom.

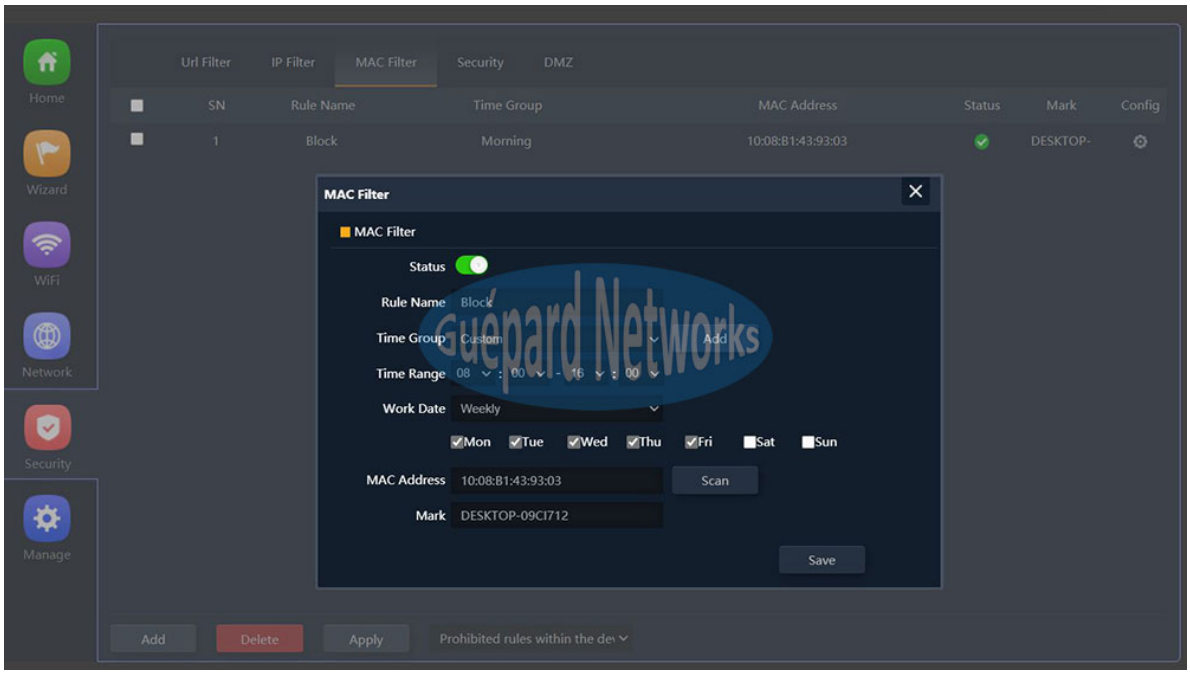
■ **IP Filter:** This function issues rules permit or prohibit staffs/users in IP Range/IP Group access prohibited service ports & Protocol with schedule time or permanent.



P26. Configuring IP Filter

… Click ***Add*** button in the bottom for creating new rule.
… Switching button ***Status*** to green to activate this rule.
… Rule Name: naming the rule.
… Time Group: choosing created previous time group or Any or Custom for applying this rule.
… Time Range: scheduling time in hours.
… Work Date: scheduling time in daily or week.
… IP Group: choosing created previous IP group *(IP range)* or Custom for applying this rule.
… Port Range: rule approve in port range *(1-65535).*
… Mark: marking hint.
… Click ***Save*** button for saving new rule.
… Apply all rules by choosing *Prohibited rules within the device through (or Allow the device to pass in the rule)* in bottom drag list, click ***Apply*** button for finish.
… Remove rule by choosing rule and click ***Delete*** button in the bottom.

■ **MAC Filter:** This function issues rules permit or prohibit staffs/users with MACs access through device in schedule time or permanent.

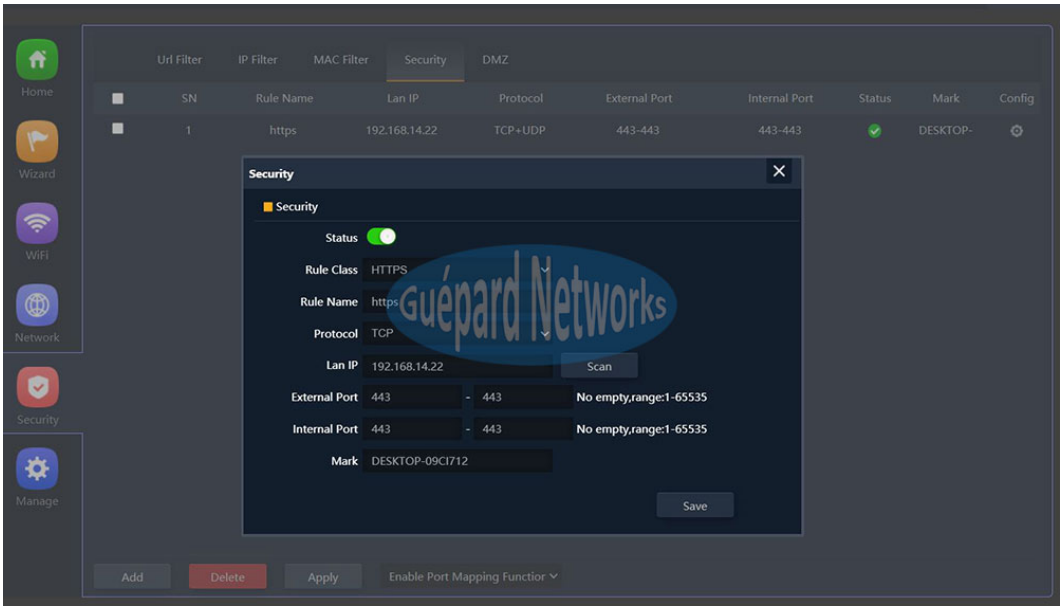


P27. Configuring MAC Filter

… Click ***Add*** button in the bottom for creating new rule.
… Switching button ***Status*** to green to activate this rule.
… Rule Name: naming the rule.
… Time Group: choosing created previous time group or Any or Custom for applying this rule.
… Time Range: scheduling time in hours.
… Work Date: scheduling time in daily or week.
… Mark: marking hint.
… Click ***Save*** button for saving new rule.
… Apply all rules by choosing *Prohibited rules within the device through (or Allow the device to pass in the rule)* in bottom drag list, click ***Apply*** button for finish.
… Remove rule by choosing rule and click ***Delete*** button in the bottom

■ **Security:** Mapping port function.

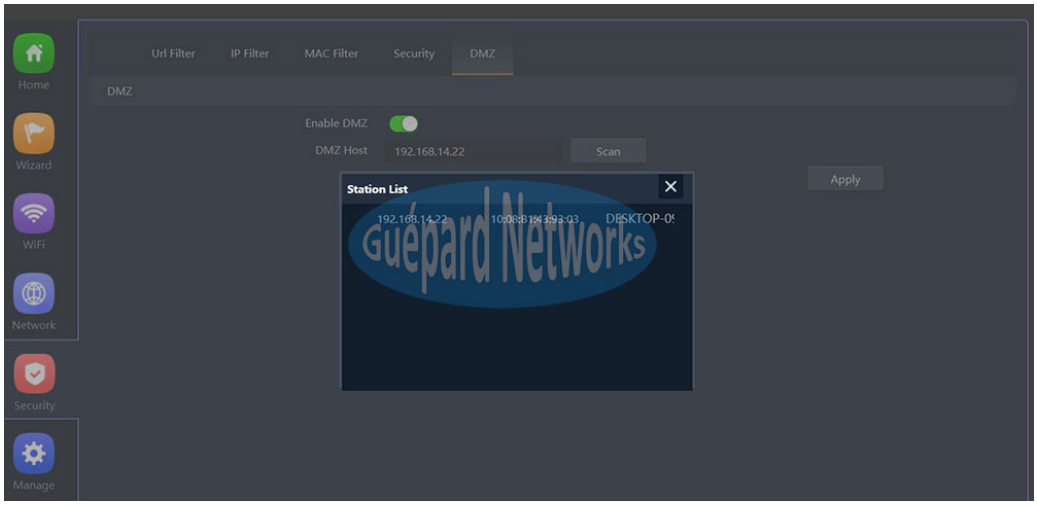
… Click ***Add*** button in the bottom for creating new rule.
… Switching button ***Status*** to green to activate this rule.
… Rule Class: choosing the available rules, such as: User defined, HTTP, HTTPS, FTP, POP3, SMTP, DNS, Telnet, IPSEC, Remote Desktop.
… Rule Name: Naming rule.
… Protocol: Choosing the available protocols, such as: TCP, UDP or Both.
… LAN IP: inputting client/user IP LAN or ***Scan*** button for selecting.



P28. Configuring Security.

… External port: inputting port range to connect WAN *(1-65535).*
… Internal port: inputting port range to connect from LAN *(1-65535).*
… Mark: marking hint.
… Click ***Save*** button for saving new rule.
… Apply rule by selecting new rule and *Enable Port Mapping Function* in bottom drag list, click ***Apply*** button for finish.
… Remove rule by choosing rule and click ***Delete*** button in the bottom

■ **DMZ:** The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.



P29. Configuring DMZ.

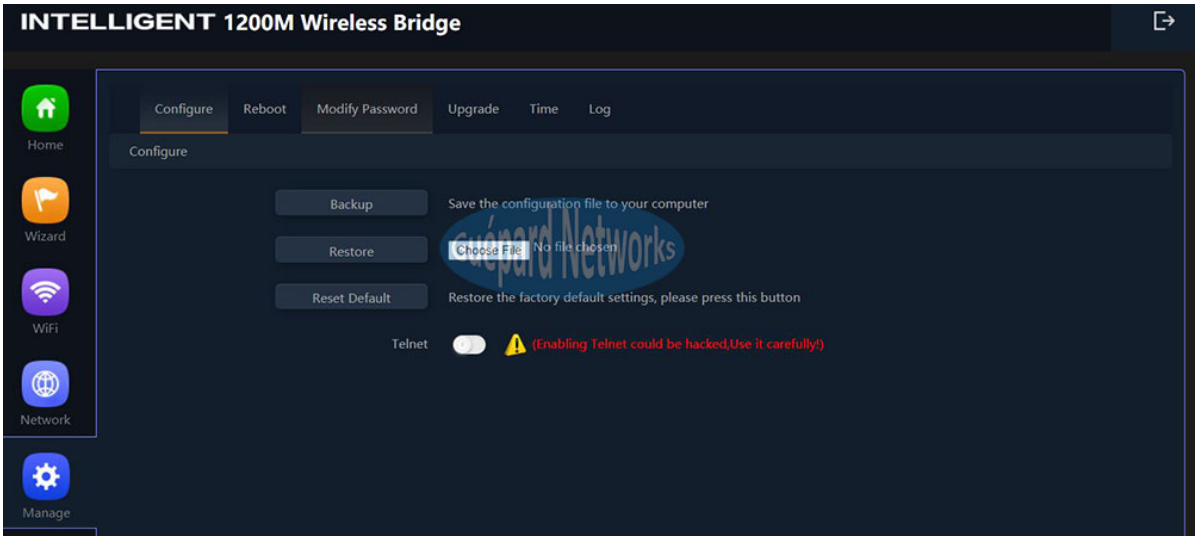
… Switching button ***Enable DMZ*** to green to activate this function.
… DMZ Host: inputting Host's IP address which need move to this zone (DMZ). Or choosing Host's IP address by ***Scan*** button.
… Click ***Apply*** button for finish.

6) Manage: running in AP/Gateway/WISP Mode

This section manage basis configurations of device included:

➢ **AP Mode:** When AP run in AP Mode

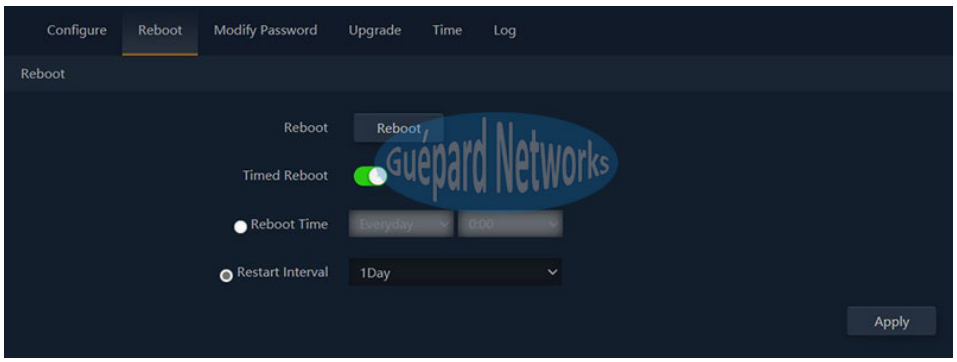
■ **Configure**



P30. Configuring Management (AP mode).

… Backup: Save the configuration file on device to your computer.
… Restore: Restore the configuration file on your computer (by click ***Choose file*** button and browsing file) to device.
- Reset Default: reset device to factory default.

■ **Reboot**



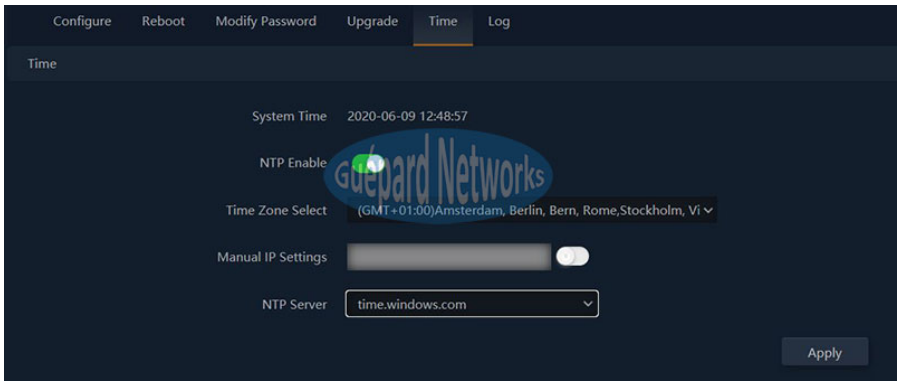
P31. Configuring Reboot.

… Reboot: reboot device immediately.
… Timed reboot: switching button to green to activate this function.
… Reboot time: choosing the date and time in week to restart device.
… Restart interval: interval to restart device in period 1 day - 10 days.
… Click ***Apply*** button for finish.

- **Modify Password**

… Old Password: inputting Old Password.
… New Password: inputting New Password which want to change.
… Confirm Password: confirming New Password.
… Click ***Apply*** button for finish.

- **Upgrade:** upgrading new firmware for device.
- **Time:** updating time for device.



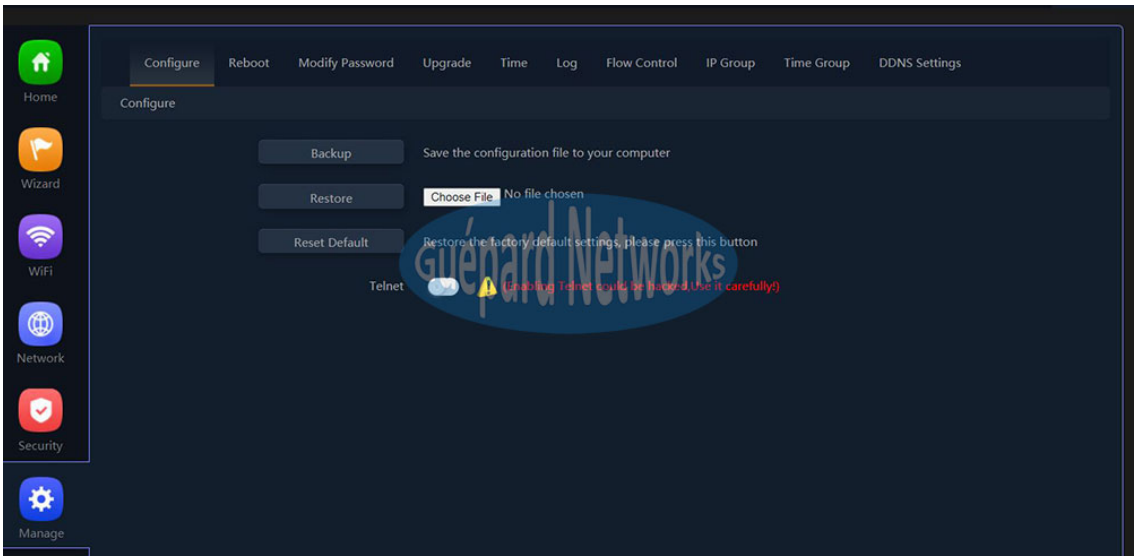
P31. Configuring System Time.

… System Time: current time of device.
… NTP Enable: switching button to green to activate NTP function.
… Time Zone Select: choosing local time zone.
… Manual IP Settings: switching button to green to activate this function.
… NTP Server: choosing available public NTP servers.
… Click ***Apply*** button for finish.

- **Log:** managing device's log.

➢ **Gateway Mode:** When AP run in Gateway/WISP Mode

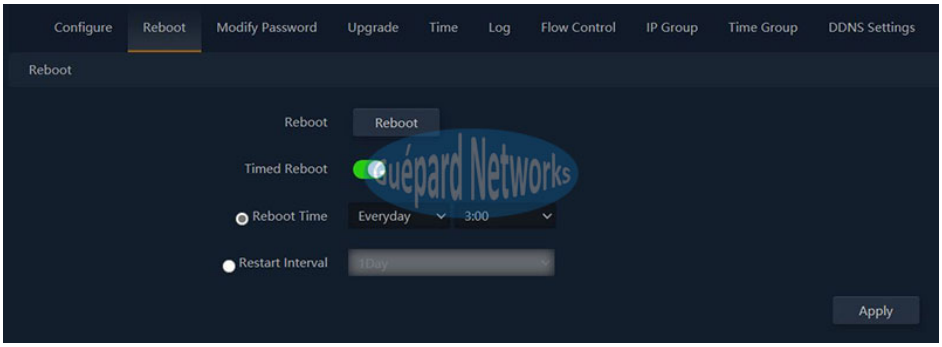
- **Configure**



P32. Configuring management (Gateway/WISP mode).

… Backup: Save the configuration file on device to your computer.
… Restore: Restore the configuration file on your computer (by click ***Choose file*** button and browsing file) to device.
- Reset Default: reset device to factory default.

■ Reboot



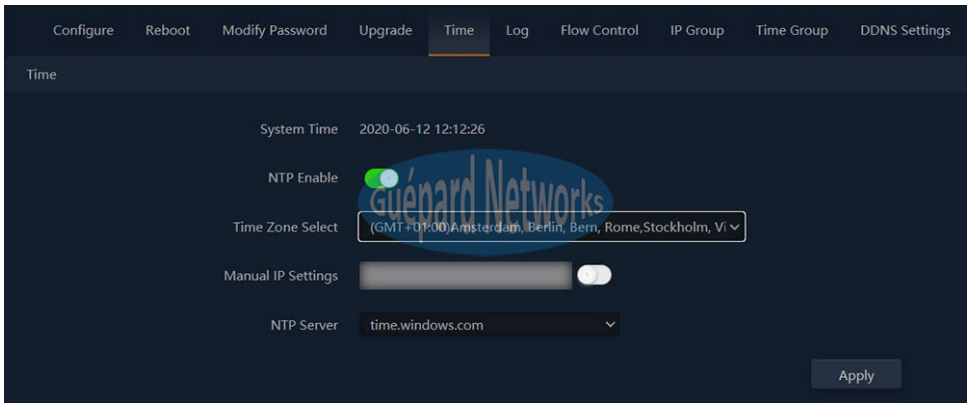
P33. Configuring Reboot (Gateway/WISP mode).

… Reboot: reboot device immediately.
… Timed reboot: switching button to green to activate this function.
… Reboot time: choosing the date and time in week to restart device.
… Restart interval: interval to restart device in period 1 day - 10 days.
… Click ***Apply*** button for finish.

■ Modify Password

… Old Password: inputting Old Password.
… New Password: inputting New Password which want to change.
… Confirm Password: confirming New Password.
… Click ***Apply*** button for finish.

- **Upgrade:** upgrading new firmware for device.
- **Time:** updating time for device.



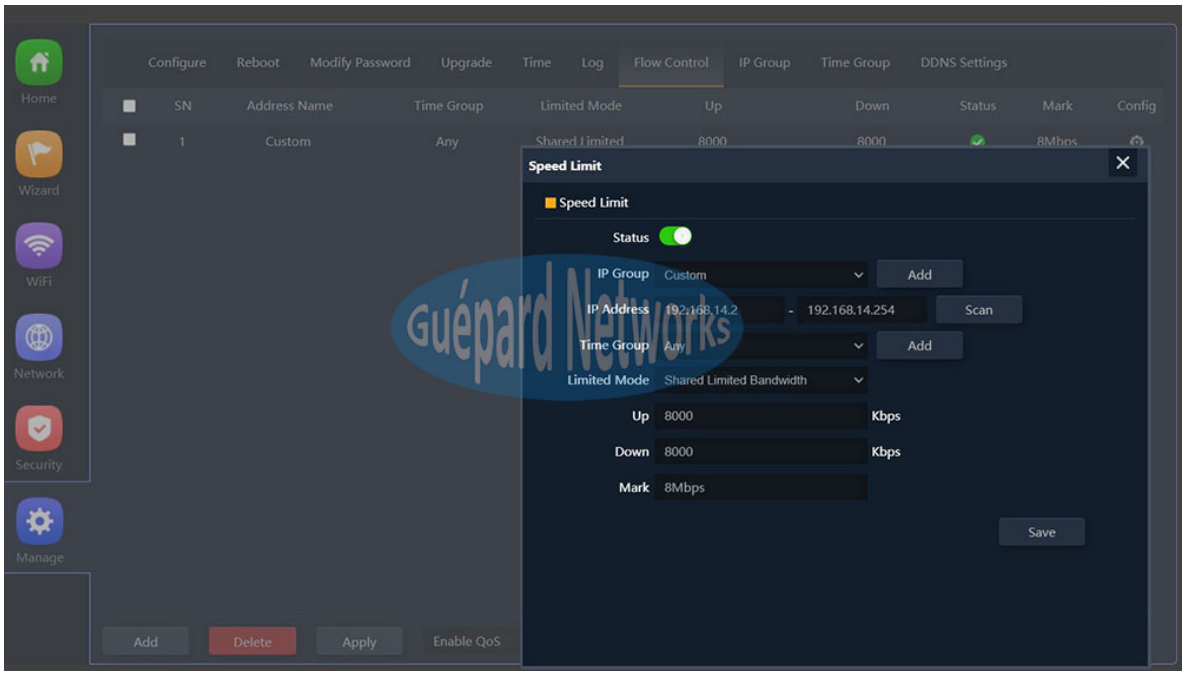
P34. Configuring System Time (Gateway/WISP mode).

… System Time: current time of device.
… NTP Enable: switching button to green to activate NTP function.
… Time Zone Select: choosing local time zone.
… Manual IP Settings: switching button to green to activate this function and inputting NTP's IP address.
… NTP Server: choosing available public NTP servers.
… Click ***Apply*** button for finish.

- **Log:** managing device's log.

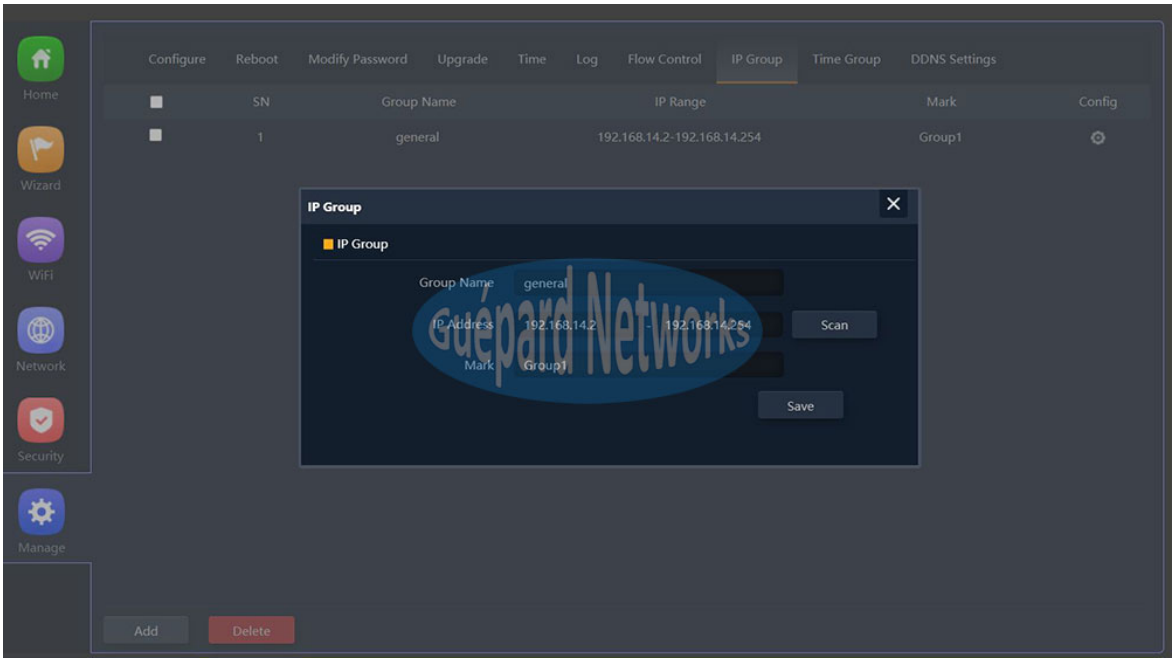
- **Flow Control:** this function (QoS) control all bandwidth flows to users which can assure system quality of service.

… Click ***Add*** button in the bottom for creating new QoS rule.
… Switching button ***Status*** to green to activate this rule.
… IP Group: choosing created previous IP group *(IP range)* or Custom for applying this rule.
… IP Address: inputting IP range or choosing IP address from running list by clicking ***Scan*** button.
… Time Group: scheduling time in daily or week.
… Limited Mode: choosing QoS mode, such as: *Exclusive limited bandwidth (the allowed bandwidth per client/user in IP range)* or *Shared Limited Bandwidth (shared total bandwidth for all clients/users in IP range).*
… Up: fixed upstream in rate Kbps.
… Down: fixed downstream in rate Kbps.
… Mark: marking hint.
… Click ***Save*** button for saving new QoS rule.
… Apply all rules by choosing *Enable QoS (or Disable)* in bottom drag list, click ***Apply*** button for finish.
… Remove rule by choosing rule and click ***Delete*** button in the bottom.



P35. Configuring QoS-Flow Control (Gateway/WISP mode).

- **IP Group:** creating Groups with IP range. Every Group can use rule which controlled by administrator.

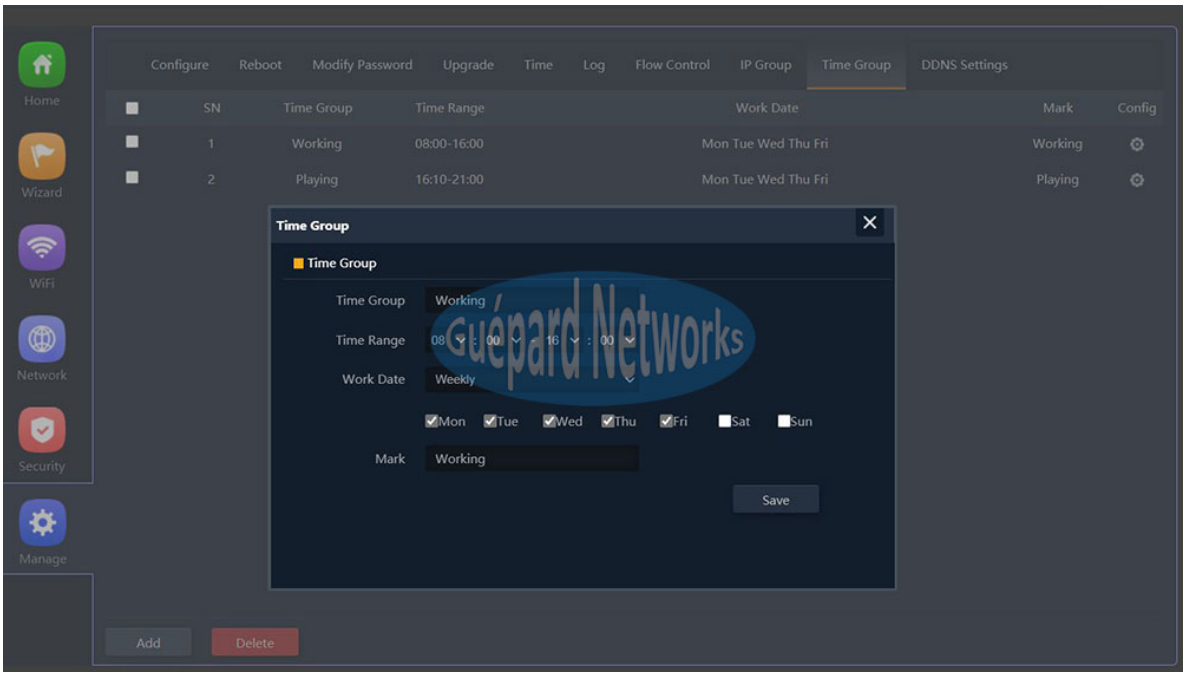


P35. Creating IP Group (Gateway/WISP mode).

… Click ***Add*** button in the bottom for creating new Group.
… Group Name: Naming Group.
… IP Address: inputting IP range or choosing IP address from running list by clicking ***Scan*** button.
… Mark: marking hint.
… Click ***Save*** button for saving new Group.
… Remove Group by choosing Group and click ***Delete*** button in the bottom.

- **Time Group:** creating Groups with time schedule. Every Group can use rule which controlled by administrator.

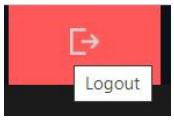
… Click ***Add*** button in the bottom for creating new time group.
… Time Group: Naming new time group.
… Time Range: scheduling time in hours.
… Work Date: scheduling time in daily or week.
… Mark: marking hint.
… Click ***Save*** button for creating new time group.
… Remove time group by choosing time group and click ***Delete*** button in the bottom.



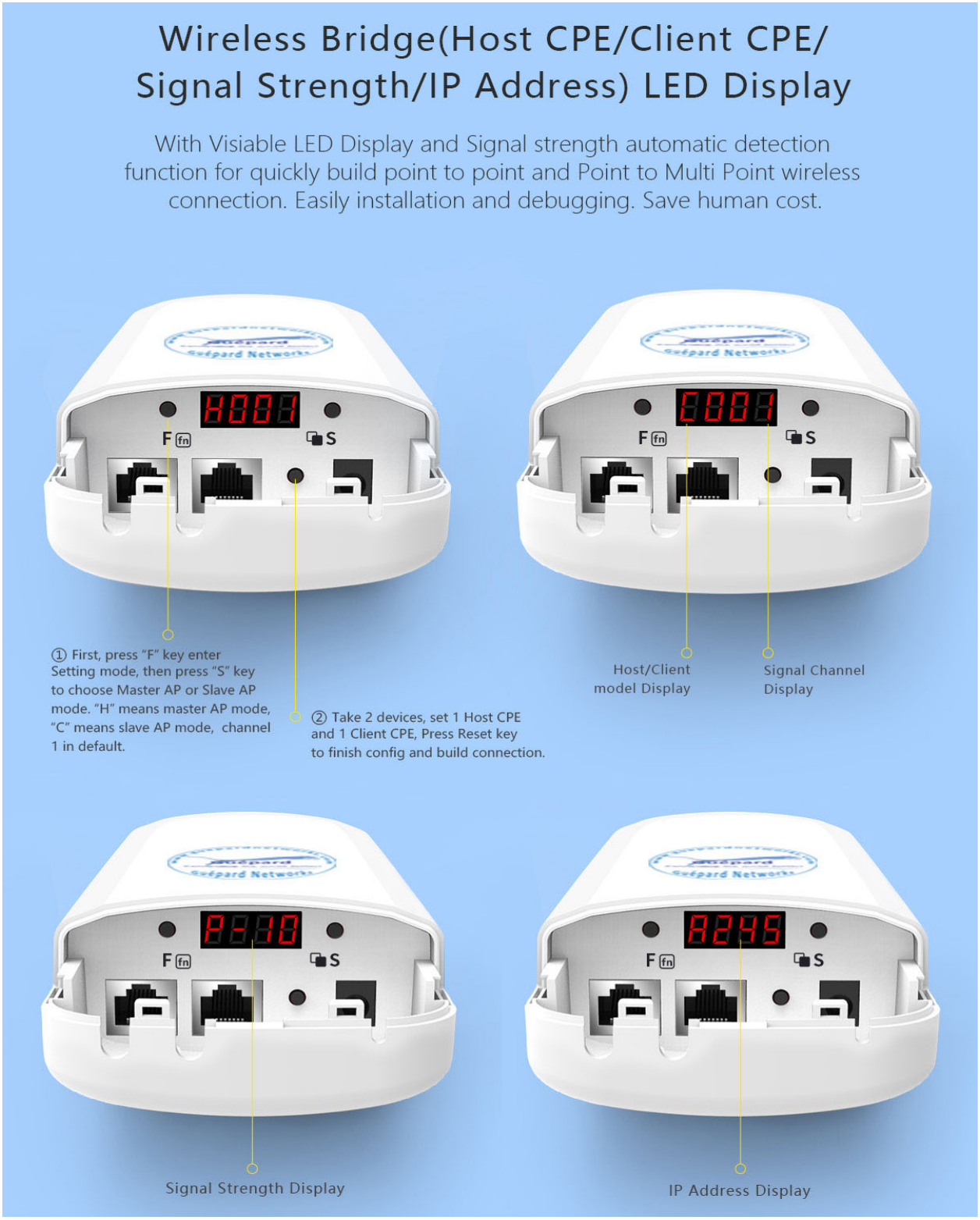
P36. Creating Time Group (Gateway/WISP mode).

7) Exit: Exit GUI (Graphic User Interface).

Exiting device's GUI by clicking button on the right top as below:



4th WDS configuration buttons:



5th Trouble Shooting:

No.	Symptoms of AP device	Solution
1	***AP's Indicator off***	Please make sure the PoE module connection is connected right PoE Port. And PoE adapter connect right power outlet.
2	***I forget user name and password in GUI login***	Press and hold the "Reset" button more than 15 seconds to restore factory default
3	***I cannot login the AP through WEB management***	1. Please make sure PC and AP's IP Address are in same network segment, then check if can Ping AP's IP address: PC start--input "and" in Run, then ping 192.168.188.253 2. Login again after Restore this ceiling AP to factory default. 3. Make sure there isn't any equipment to take IP address of 192.168.188.253 in the same network 4. Check LAN cable to avoid any problem, recommend do not use unshielded twisted pair Ethernet cable.
4	***I forget the AP's SSID and passwords***	1. Login to AP's GUI page by internet cable, then reset password in WiFi setting. 2. Restore to factory default
5	***I can't access to AP's IP address***	1. Check AP's DHCP and make it enabled in Gateway mode. 2. Check the internet connection between AP and the root router/switch in AP and Repeater mode. 3. Or AP run in AP mode. PC should change IP matching AP's IP subnet.
6	***I can't access into Internet even finished the settings of wireless AP***	1. If dynamic IP user, login wireless AP's WEB page, check Internet settings--WAN Setting--Dynamic IP, fill in right information. 2. If ADSL user, login wireless AP's WEB page, check Internet settings--WAN setting--PPPOE, then input the right user name and password 3. Please set PC's IP address as obtain IP address automatically
7	***How to change IP address in local network***	Click **Advanced** settings-**Network**-**LAN** settings-**IP** address setting-**Apply**
8	***How to Reset Wireless AP***	Press and hold the "Reset" button more than 15 seconds after power on. The Wireless AP will be restored back factory default after the Wireless AP restart.