Wireless AP User Manual

(Applicable to Maipu AP Series)

V2.0

Chengdu Maipu International Infotech Co., Ltd

No. 16, Jiuxing Avenue

Hi-tech Park

Chengdu, Sichuan Province

People's Republic of China - 610041

Tel: (86) 28-85148850, 85148041

Fax: (86) 28-85148948, 85148139

URL: http: // www.maipu.com

Email: overseas@maipu.com

Copyright

Copyright ©2013, Maipu Communication Technology Co., Ltd. All Rights Reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Maipu Communication Technology Co., Ltd.

MAIPU and 迈普 are trademarks of Chengdu Maipu International Infotech Co., Ltd

All other trademarks that may be mentioned in this manual are the property of their respective owners.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Preface

Thank you for using Maipu high-performance wireless access point (AP). The AP is the next-generation wireless access point of high performance based on 802.11ac and can provide the wireless access rate multiple times of the traditional 802.11a/b/g/n. In addition, the AP can cover more extensive area.

The AP supports both the FAT and FIT work mode and can switch flexibly between these two modes as required by the network planning. The AP needs to cooperate with the wireless network controller when acting as a fit AP and can be deployed independently when acting as a fat AP. By supporting the Fat and Fit work-modes, the AP can be smoothly upgraded to the large-scale network from the small-size WLAN network. This can greatly protect the user investment.

In addition, the AP provides the Web UI with brief and simple options, which enables the user to complete the setting quickly and enables the user to use the AP more convenient and efficient.

Chapter 1: product overview, briefly describes the main AP feature and product specifications.
Chapter 2: detailed configuration guide, instructs you to configure the AP parameters and advanced features.
Appendix is added for restoring the factory default of AP, in which way AP can be restored when Web configuration is not available.

*since firmware upgrade is necessary for APs, this user manual may not be based on the newest firmware and some pages may be slightly different.

Contents

Copyright 2
Preface 3
1 Product Introduction 6
1.1 Overview 6
1.2 Main Features 6
2 Detailed Configuration Guide 8
2.1 PC Configuration 8
2.2 System Login 11
2.3 System Status 13
2.3.1 Device Information 13
2.3.2 WLAN Status 13
2.3.3 Activity Client 14
2.3.4 Peak Clients 14
2.3.5 Network Flow 15
2.3.6 System Load 15
2.3.5 Network Detection 16
2.4 Wireless Configuration 18
2.4.1 2.4G Wireless SSID 18
2.4.2 Wireless Configuration 21
2.4.3 WMM 22
2.4.4 Advanced Settings 22
2.4.5 5G Wireless Configuration 23
2.5 Network 25
2.5.1 IP Address 25
2.5.2 DNS Setting 26
2.5.3 DHCP Service 26
2.5.4 DHCP Patch 28
2.5.5 LLDP 28
2.6 Security 29
2.6.1 ARP Protection 29
2.6.2 DHCP Bind 29
2.6.3 MAC Filter 30
2.6.4 Broadcast Control 31
2.6.5 Smart QoS 31
2.6.6 RADIUS 32

2.6.7 Portal 33
2.7 Setting 34
2.7.1 Management 34
2.7.2 Web Management 35
2.7.3 Administrator 35
2.7.4 Profiles 36
2.7.5 Firmware Upgrade 37
2.7.6 System Time 38
2.7.7 OUI Update 39
2.8 System Log 39
2.8.1 Event Log 40
2.8.2 Network Log 40
2.8.3 Security Log 41
2.8.4 Alarm Log 41
Appendix 42
Hardware Restoration Configuration 42

1 Product Introduction

1.1 Overview

The Maipu Wireless AP is the next-generation wireless access point of high performance based on 802.11ac (for some models) and can provide the wireless access rate multiple times of the traditional 802.11a/b/g. In addition, the AP can cover more extensive area.

The AP supports both the Fat and Fit work mode and can switch flexibly between these two modes as required by the network planning. The AP needs to cooperate with the wireless network controller when acting as a fit AP and can be deployed independently when acting as a fat AP. By supporting the Fat and Fit work-modes, the AP can be smoothly upgraded to the large-scale network from the small-size WLAN network. This can greatly protect the user investment.

1.2 Main Features

Easy to deploy

The AP can automatically detect the AC and delivers the configuration via the AC. The wireless network can be enabled for the AP zero configuration. The AP can integrate with the existing AP, firewall, authentication server, and other network architecture seamlessly without changing the existing network architecture.

Centralized management

The AP can act as a fit AP and cooperate with the AC. The AC uniformly controls all the fit APs in the network and the status of all the devices can be viewed. Comparing with the traditional fat AP, the AC and the fit AP application mode greatly facilitate the administrator to manage the entire network.

AP centralized upgrade

The AP can achieve the centralized management by the wireless network controller in the network and uniformly upgrade the AP to the latest version. The AP can apply new firmware automatically without manual interference, which reduces the workload of network maintenance. The feature is especially important in the large-scale network.

User isolation policy

The AP supports the isolation between the wireless users. When this function enabled, two wireless clients cannot communicate directly. The wireless client can intelligently visit the upstream wired network.

Multiple forms and convenient installation

This series APs have multiple form design and can be applicable to different installation scenarios. There is no need to smash the wall to lay out cables and furnish the wall for the second time. The AP provides the wireless coverage based on the wired network and can be installed conveniently and quickly. Cooperating with the wireless network controller, the wireless AP can achieve plug-and-play and AP zero configuration, and all the AP management, control, and configuration are completed by the AC. The network management personnel does not need to manage and maintain the mass of APs one by one, and all actions, such as the configuration, firmware upgrade, and security policy update can be delivered uniformly by the AC.

2 Detailed Configuration Guide

2.1 PC Configuration

To facilitate the user management, the AP integrates the web management function. Through this function, we can realize various management functions in a simple mode to facilitate using. When the user configures the hardware, the user can use the PC to configure the AP.

Through the PC connected to the AP, the user can easily perform the web management after the following configuration.

The default IP address of the AP is 192.168.170.1 and this parameter can be set as required. The following takes the default value as an example. The PC is set by the following steps:

1) Connect the PC to the Ethernet port of the AP.
2) Set the IP address of the PC.
3) Select **Network** > **Network** > **Local Connection**.
4) Right-click **Local Connection** and click **Properties** on the displayed menu.
5) Select **Internet Protocol Version 4 (TCP/IPv4)**, as shown in Figure 2-1.

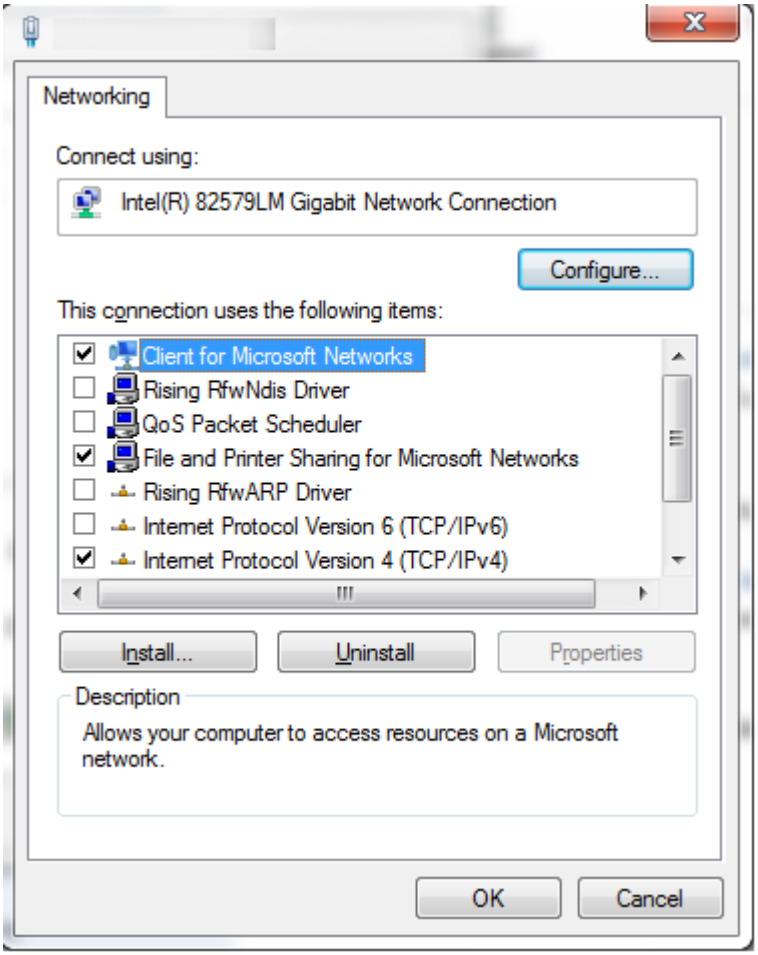


Figure 2-1 Select Internet TCP/IP protocol on the attribute window

Click **Properties** to set the IP address of the PC.

On the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, choose **Use the following IP address** and input 192.168.170.xxx in **IP address**, 255.255.255.0 in **Subnet mask**, and input 192.168.170.1 (default IP address of the AP) in **Default gateway**.

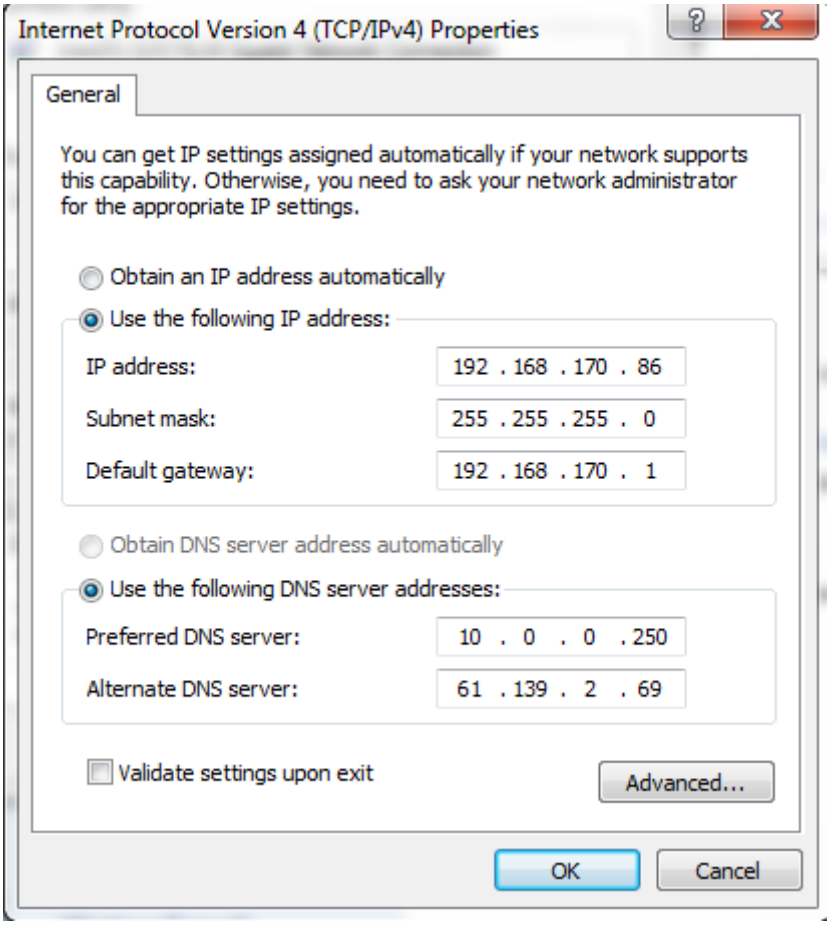


Figure 2-2 Input IP address on the TCP/IPv4 attribute interface

1) Click **OK** to complete the configuration.
2) Test whether the PC is connected to the AP.
3) Choose **Start** > **Run**. Input **cmd** > and click **OK**.
4) Execute the ping command in command prompt to test whether the connection succeeds.
5) Ping 192.168.170.1.

The result is displayed, as shown in Figure 2-3.

```
Pinging 192.168.170.1 with 32 byte of data:
Replyfrom  192.168.170.1:bytes=32  time<10ms
TTL=64
Replyfrom  192.168.170.1:bytes=32  time<10ms
TTL=64
```

Figure 2-3 Connection success between the PC and AP

If the information in Figure 2-3 is displayed, it indicates that the connection succeeds.

The result may also be displayed, as shown in Figure 2-4.

```
Pinging 192.168.170.1 with 32 byte of data:

Requesttimed out.
Requesttimed out.
Requesttimed out.

Ping statistics for 192.168.170.1:
Packets:Sent=4,Received=4,Lost=0(100% loss).
```

Figure 2-4 Connection failure between the PC and AP

If the information in Figure 2-4 is displayed, it indicates that the PC is not correctly connected to the AP.

In this case, you should check:

1) Check whether the indicator is on.
2) Check whether the TCP/IP is correctly filled.

2.2 System Login

The AP provides the local and remote web management. Input http://192.168.170.1 in the address bar of the Internet browser to log in to the AP configuration interface. (If https is enabled, then use https://192.168.170.1 to login. By default, https is disabled.) The login interface is displayed, as shown in Figure 2-5.

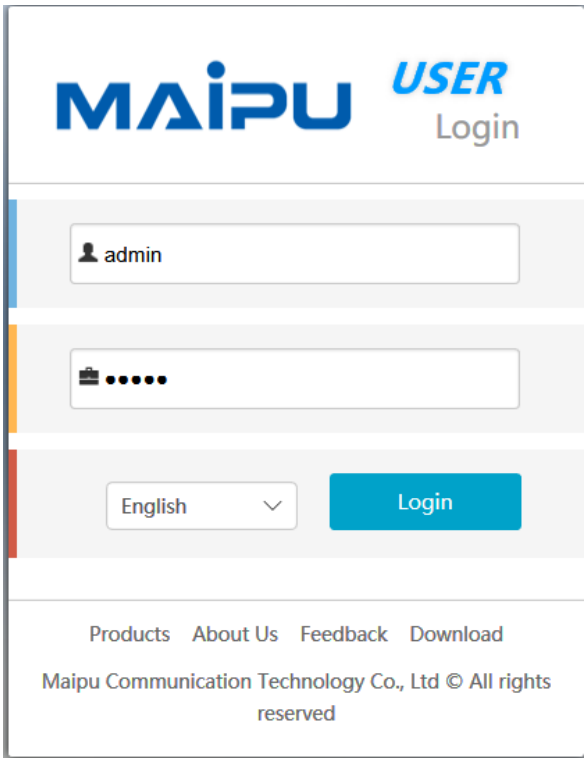


Figure 2-5 The AP configuration interface

Both the default user name and password of the AP are ***admin*** and the default IP address is 192.168.170.1.

After correctly logging in to the system, the homepage is displayed, as shown in Figure 2-6. The homepage may vary slightly for different models.

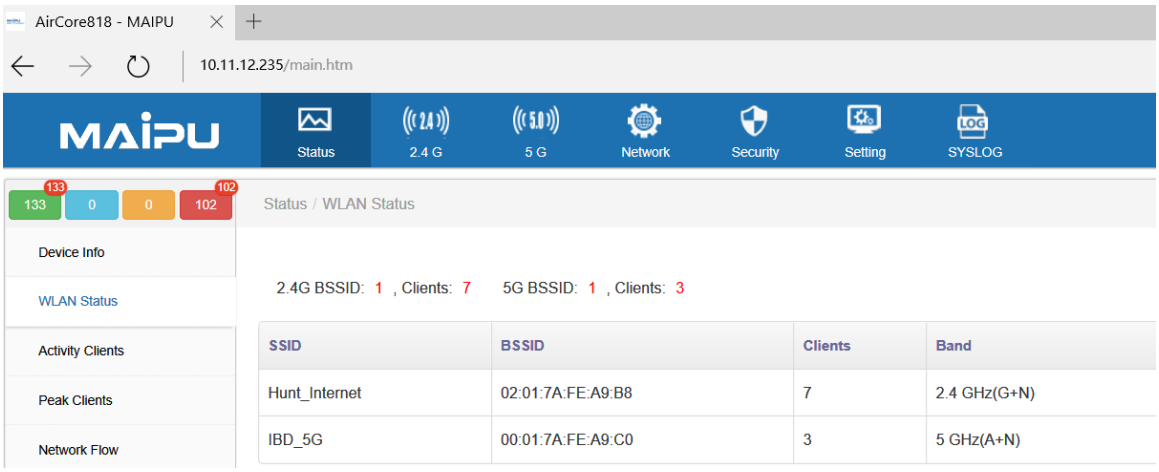


Figure 2-6 The homepage displayed after logging in to the system

The homepage displays the system wireless status of the device, including the SSIDs configured on this AP and number of connected terminals for each SSID.

2.3 System Status

2.3.1 Device Information

On the **Device Info** interface, the device information of the AP, including **Hostname**, **Device Model**, **Serial Number**, **Firmware Version**, **MAC Address**, and **Uptime**, is displayed as shown in Figure 2-7.

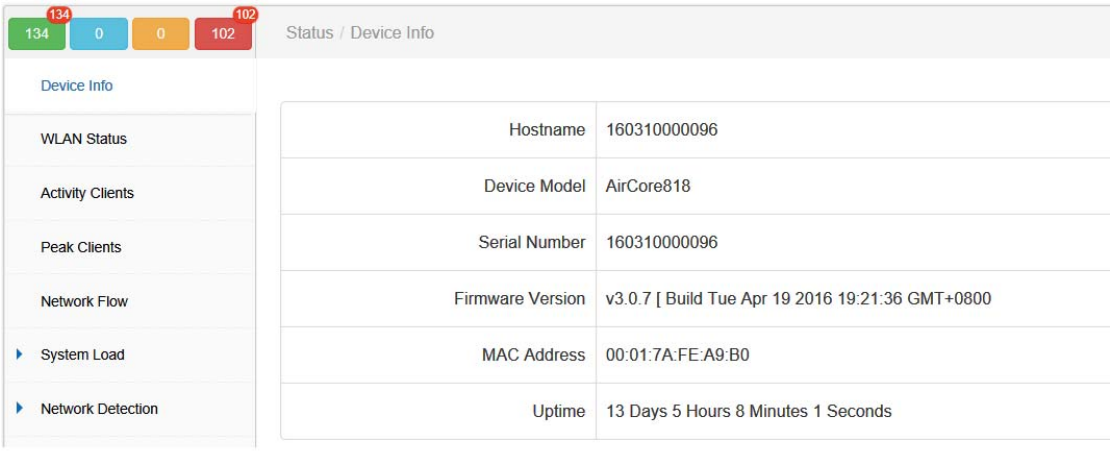
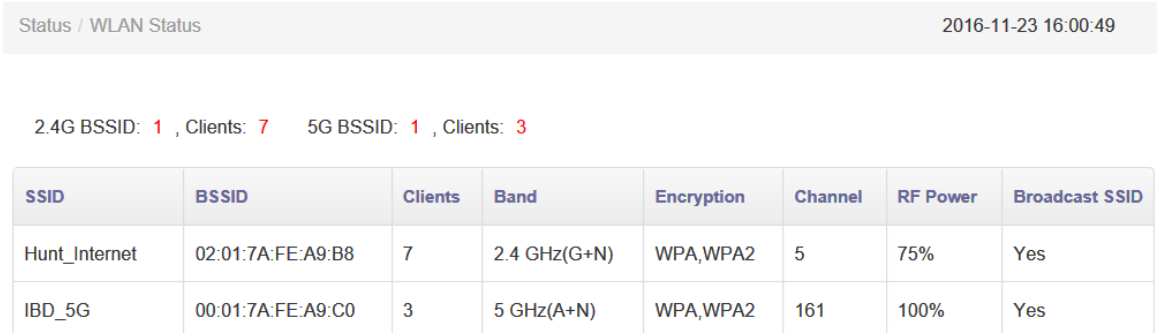


Figure 2-7 The device information interface

2.3.2 WLAN Status

On the **WLAN Status** interface, the status information of the AP wireless connection, including **SSID, BSSID, Clients, Band, Encryption, Channel, RF Power** and **Broadcast SSID**, is displayed as shown in Figure 2-8.



SSID	BSSID	Clients	Band	Encryption	Channel	RF Power	Broadcast SSID
Hunt_Internet	02:01:7A:FE:A9:B8	7	2.4 GHz(G+N)	WPA,WPA2	5	75%	Yes
IBD_5G	00:01:7A:FE:A9:C0	3	5 GHz(A+N)	WPA,WPA2	161	100%	Yes

Figure 2-8 The WLAN status interface

2.3.3 Activity Client

On the **Activity Clients** interface, the information of the host that is successfully connected to the AP can be viewed. On the top line there is a sum of 2.4G and 5G total terminals. As shown in Figure 2-9.

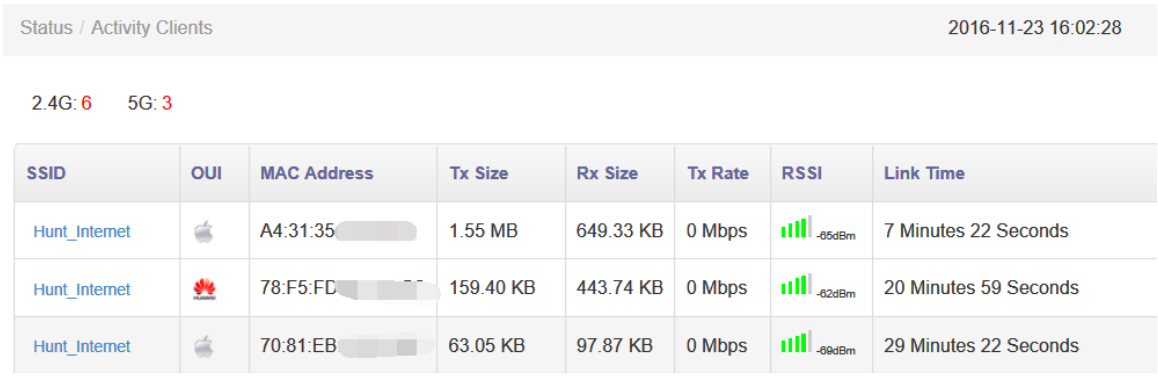


Figure 2-9 The WLAN client information

(1) **SSID**: Service Set ID that terminals connecting to.

(2) **OUI**: the manufacturer's icon recognized by AP will show here.

(3) **MAC Address**: specifies the MAC address of the host that is successfully connected to the AP.

(4) **Tx Size**: specifies the data traffic that sent by the host.

(5) **Rx Size**: specifies the data traffic received by the host.

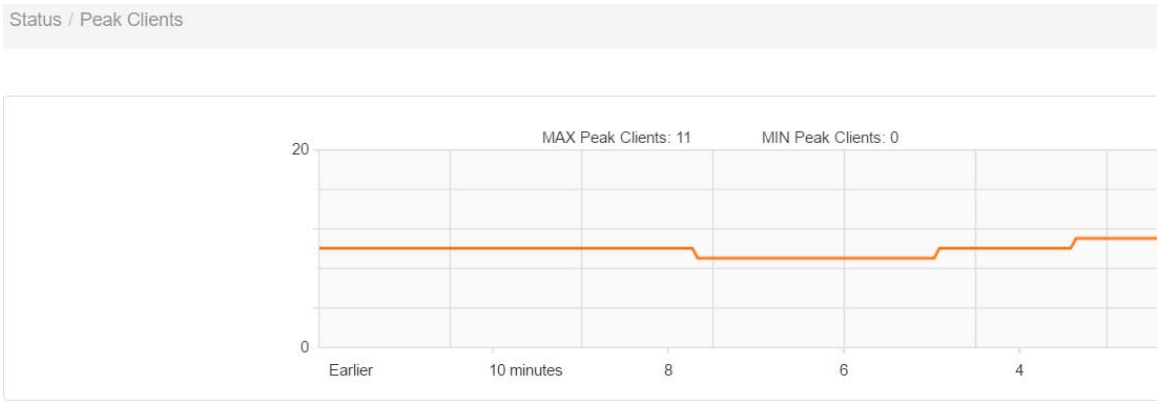
(6) **Tx Rate**: specifies the current rate of sending data package by the host.

(7) **RSSI**: specifies the signal strength between the host and the AP.

(8) **Link Time**: specifies the time that the host is connected to the AP.

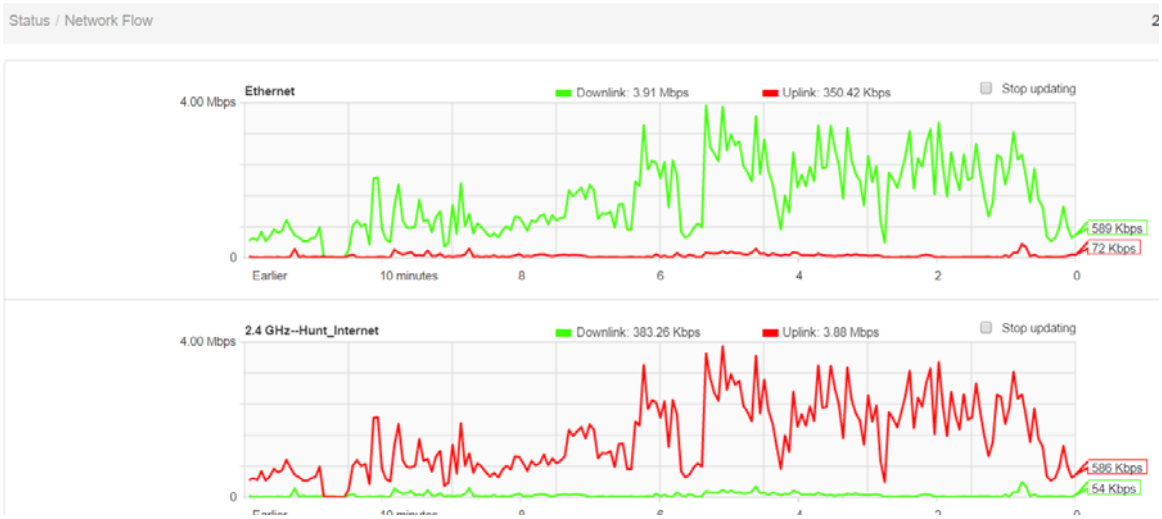
2.3.4 Peak Clients

On Peak Clients page, the number of terminals connected to this AP can be viewed based on different time lines. Shown as below:



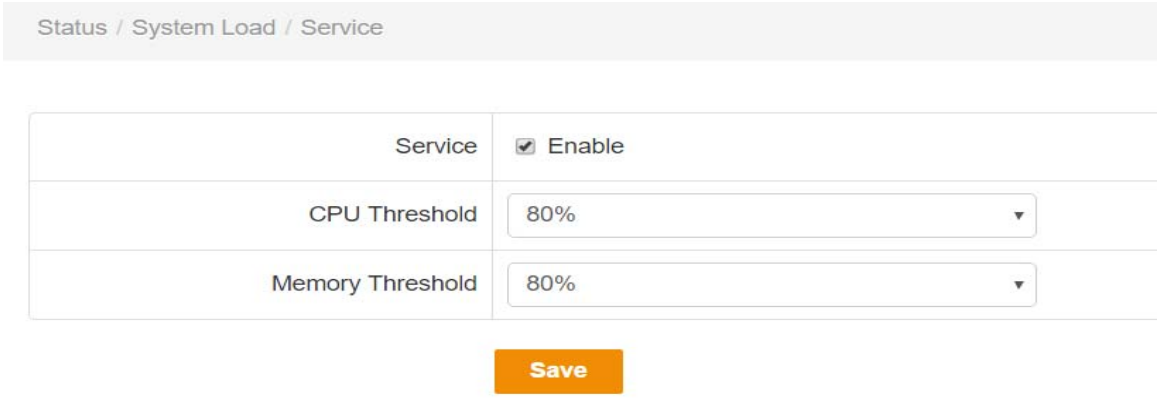
2.3.5 Network Flow

Network Flow shows all the interfaces (includes wired and wireless ones) traffic flow, based on different timeline. It shows both downlink and uplink and is updating in real-time.



2.3.6 System Load

On the **System Load** interface, you can set the CPU and Memory threshold. When the value is higher than the value set, there will be log generated. Also, by go to System Load subpage, you can view the current AP memory and CPU load, as shown in Figure 2-10.



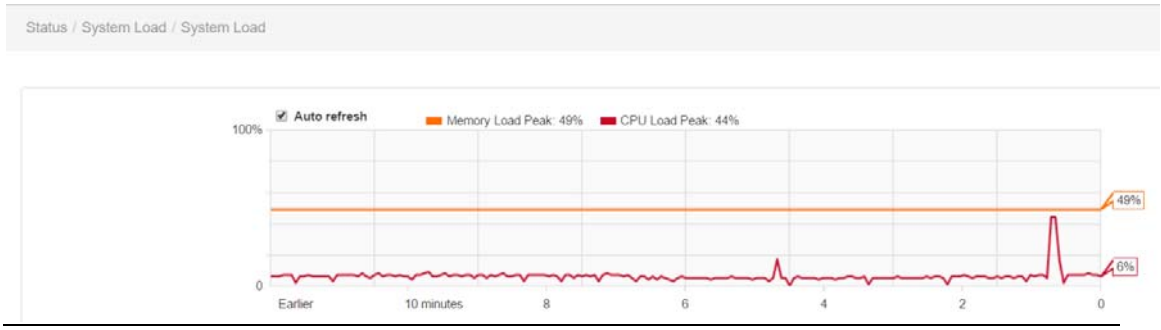


Figure 2-10 The system load interface

(1) **Service**: specifies whether to enable the system load alarm mechanism.

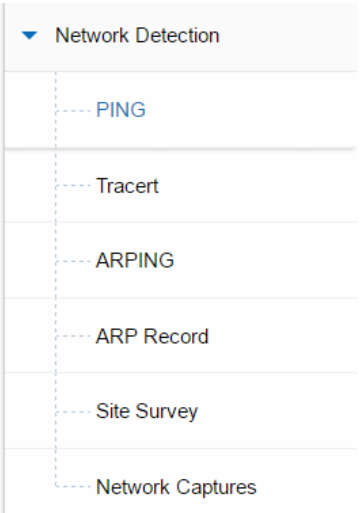
CPU Threshold: specifies the CPU alarm threshold.

Memory Threshold: specifies the memory alarm threshold.

(2) **Auto refresh**: specifies whether to automatically refresh the current system load status.

2.3.5 Network Detection

On the detection interface, you can detect the network connection status by ping, tracert, ARPING, ARP record, Site Survey, Network Captures etc. (Ping test is used as an example here.）, as shown in Figure 2-11.



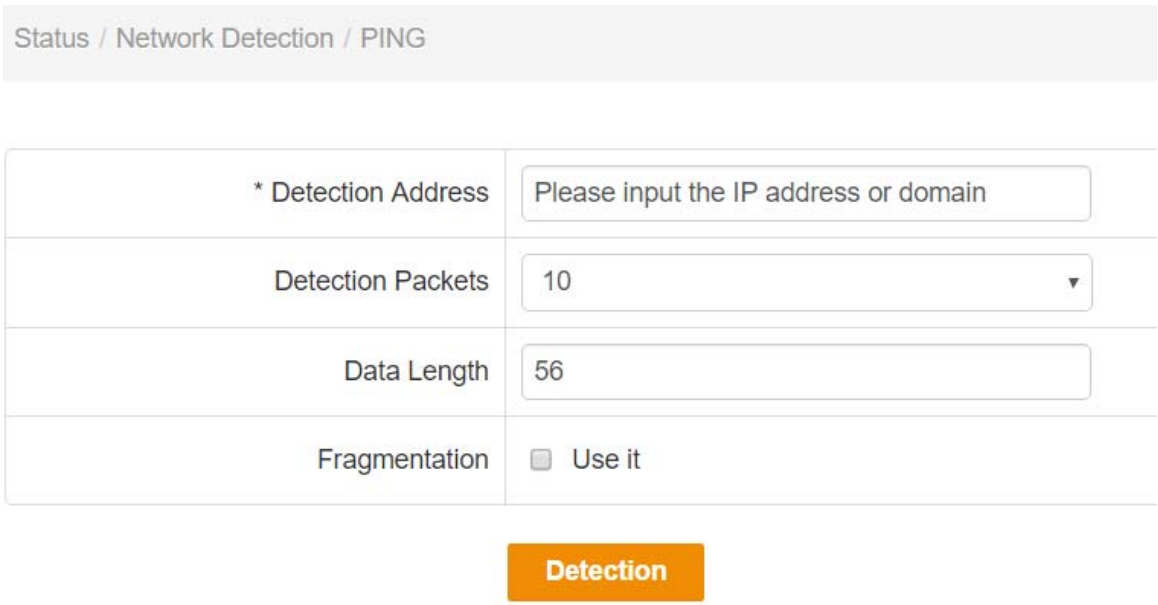


Figure 2-11 The ping detection interface

(1) **Detection Address**: specifies the target host for the system sending the ICMP packet.

(2) **Detection Packets**: specifies the number of ICMP packets sent by the system. The number must an integer from 1 to 10.

(3) **Detection**: notifies the system to begin to send the ICMP packet.

```
PING 10.11.12.254 (10.11.12.254): 56 data bytes
64 bytes from 10.11.12.254: seq=0 ttl=255 time=0.374 ms
64 bytes from 10.11.12.254: seq=1 ttl=255 time=0.301 ms
64 bytes from 10.11.12.254: seq=2 ttl=255 time=0.327 ms
64 bytes from 10.11.12.254: seq=3 ttl=255 time=0.310 ms
64 bytes from 10.11.12.254: seq=4 ttl=255 time=0.311 ms

--- 10.11.12.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.301/0.324/0.374 ms
```

Figure 2-12 The results of network detection.

2.4 Wireless Configuration

2.4.1 2.4G Wireless SSID

On the **2.4G Page,** you can configure basic SSID, detailed wireless network config, WMW, and advanced settings.

Choose **WEB Management** > **2.4 GHz** > **SSID** to enter the **Basic Settings** interface, as shown in Figure 2-13.

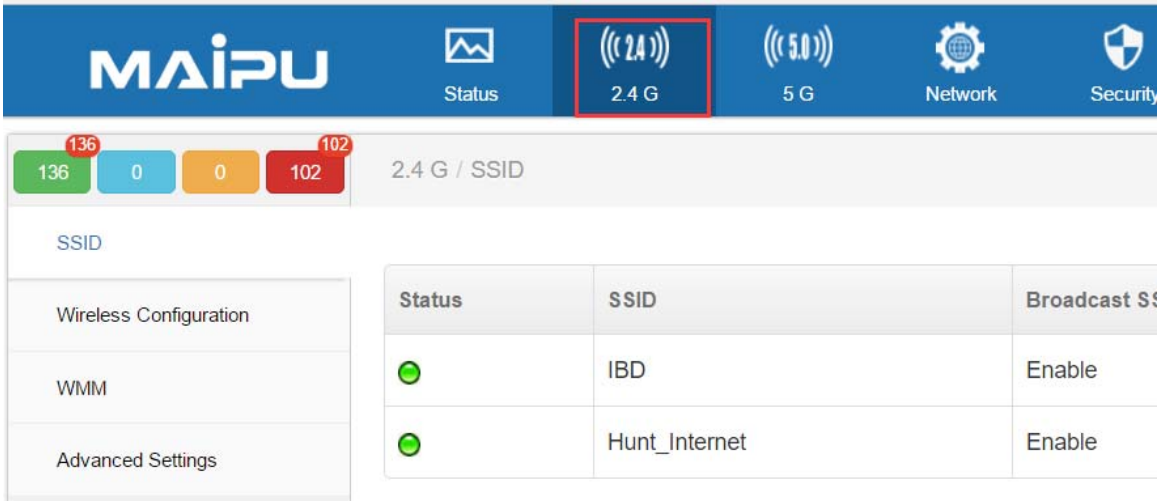
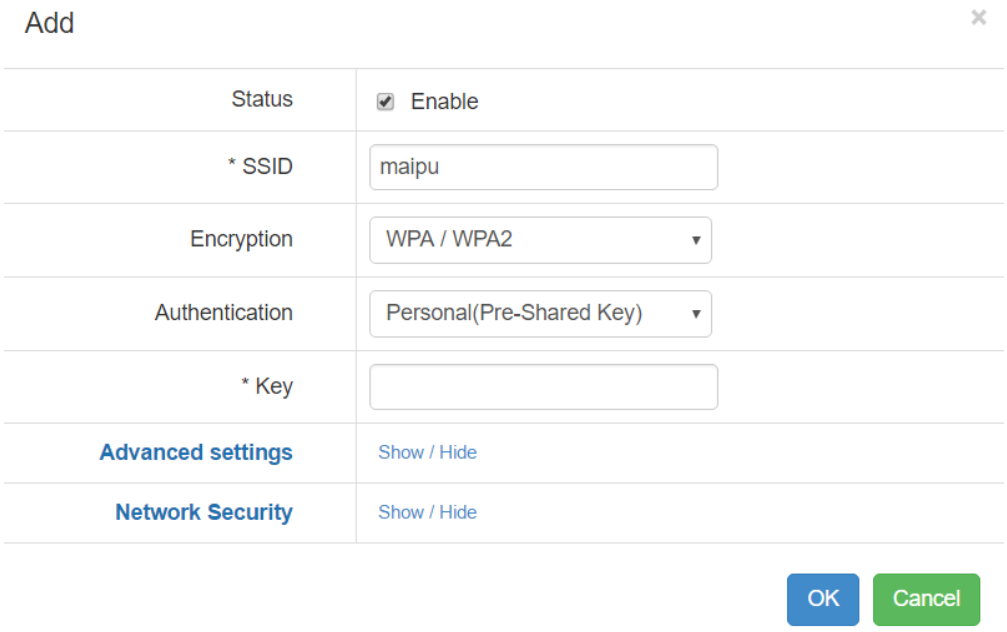


Figure 2-13 The wireless parameter interface

Click **Add** button to add the details of SSID and related security.



(1) **Status**: specifies whether to enable or disable this wireless SSID.

(2) **SSID**: short for Service Set Identifier, can divide a WLAN into several subnetworks requiring different authentications. Each subnetwork needs independent authentication and only users passing the authentication can enter the corresponding subnetwork. This can prevent the unauthorized users entering this network. That is to say, SSID is the name of your network.

(3) **Encryption**: specifies whether to encrypt the set SSID. The AP provides the WEP, WPA, WPA2, and WPA/WPA2 four encryption modes.

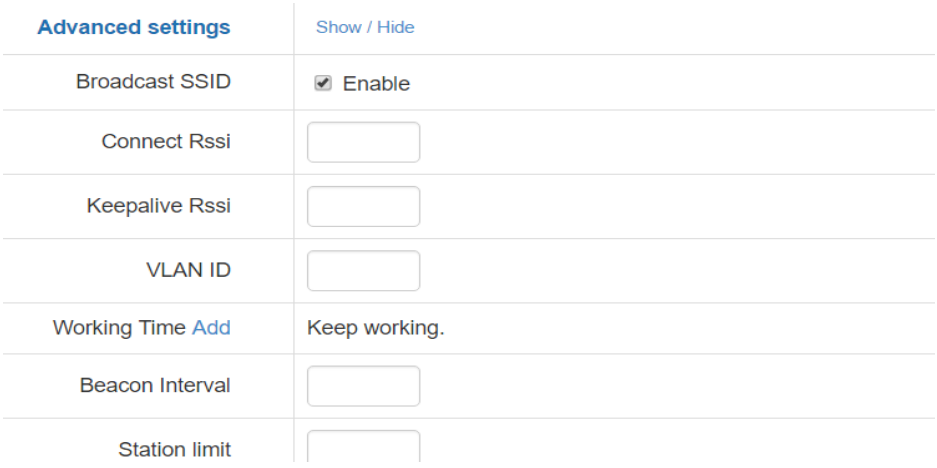
WEP: short for Wired Equivalent Privacy, encrypts the data transmitted in wireless mode between two devices to prevent the unauthorized user to bug or invade the wireless network.

WPA: short for Wi-Fi Protected Access, has the WPA and WPA2 standards and protects the Wi-Fi security. It is generated based on several serious weaknesses found in the last generation of system WEP by the researcher.

(4) **Authentication**: specifies the authentication type. Two types are available, Personal (Pre-shared Key) and Enterprise (Radius). When Personal is chosen, enter a key with 8~63 characters. When Enterprise is chosen, a Radius server will be needed.

(5) **Key**: based on the different encryption type, input the password here.

If Extending **Advanced Settings**, there will be more options available:



(1) Broadcast SSID: specifies whether to allow the wireless network to be searched by others through the SSID name. When this function is disabled,

the wireless network is still available, but it will not be searched in others' available network list and the wireless network efficiency will be affected to a certain extent.

(2) Connect RSSI: set the RSSI value which can allow terminals to connect. When the RSSI value on terminal device is lower than this value, the terminal will not be allowed to connect to this AP.

(3) Keepalive RSSI: RSSI threshold that AP still allows terminals to be online.

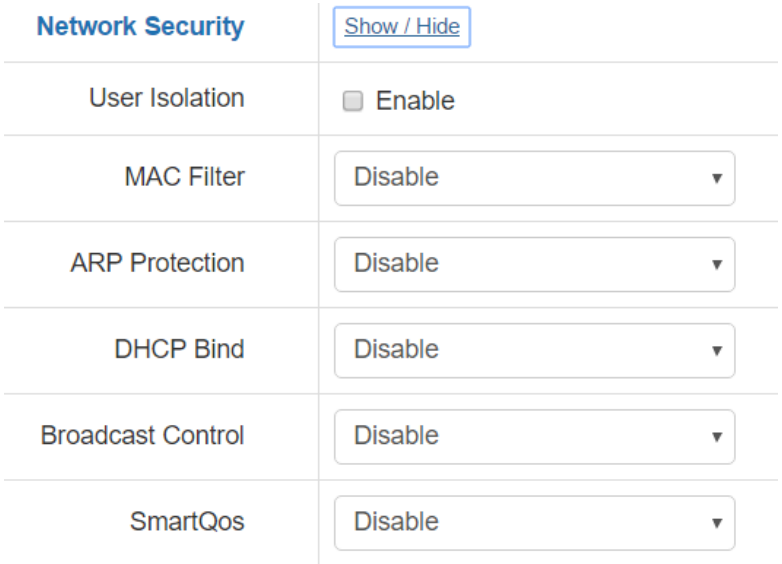
(4) VLAN ID: specifies the VLAN ID to be allocated to the AP.

(5) Working Time: by default, AP is always working. By setting up the work time, users can make a schedule that can automatically get AP start and stop working.

(6) Beacon Interval: set the interval time that AP will send the Beacon frame.

(7) Station limit: set the number of terminals this SSID can allow to be connected.

If extending **Network Security** option, more advanced security settings can be done. Shown as below:



(1) User Isolation: if enabled, the wireless terminals connected to this AP can't directly communicate each other. However, terminal's uplink to Internet won't be affected.

(2) MAC Filter: choose the mac-filter list configured in **Security** Page. To enable this feature, you should configure all details of MAC lists in **security** page first.

(3) ARP Protection: choose the ARP Protection list configured in **Security** Page. To enable this feature, you should configure all details of ARP protection lists in **security** page first.

(4) DHCP Bind: choose the DHCP binding list configured in **Security** Page. To enable this feature, you should configure all details of DHCP bind list in **security** page first.

(5) Broad Control: choose the broadcast control list configured in **Security** Page. To enable this feature, you should configure all details of related list in **security** page first.

(6) Smart Qos: choose the SmartQos rule configured in **Security** Page. To enable this feature, you should configure all details of related list in **security** page first.

2.4.2 Wireless Configuration

On the **2.4G** page, you can configure the wireless radio information of the AP. Choose **WEB Management** > **2.4GHz** > **Wireless Configuration**, as shown in Figure 2-14.

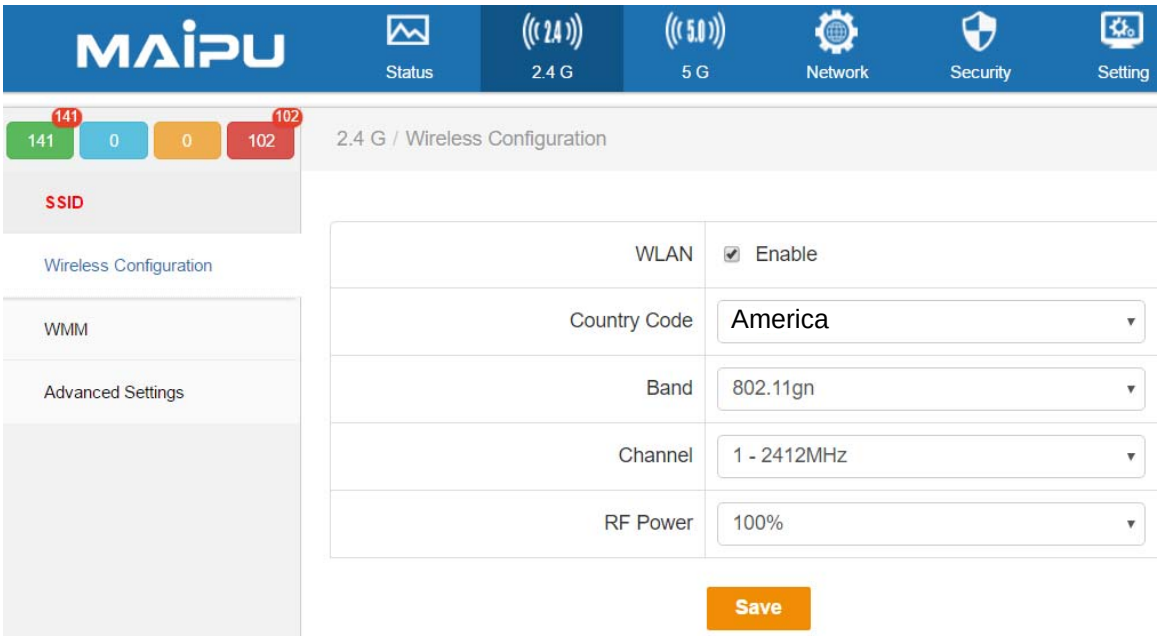


Figure 2-14 The Wireless configuration

(1) WLAN: turn on or turn off 2.4G Radio. If not enable, all 2.4G radio will be turned off.

(2) Band: specifies the network protocol mode that the AP works at. Currently, the AP supports the combination of the 802.11b, 802.11g,

802.11gn, protocols. (For 5GHz Radio, it will support 802.11a, 802.11n, and some models support 802.11ac).

(3) Channel: indicates wireless channel. It is the data signal transmission channel considering the wireless signal as transmission media. When multiple devices exist in the area covered by the AP signal, set different channels to avoid interference. The AP has a total of 1 to 11 channels. (based on different region, 12, 13, 14 channel may be optional.)

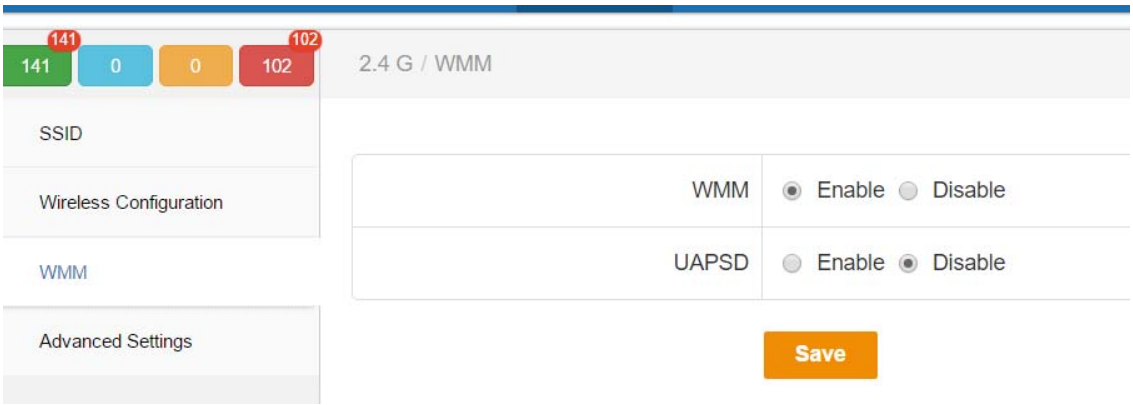
（4）RF Power: adjusts the output power of the AP. RF Power can be decreased to lower the interference chance if the other APs around have too strong signal.

2.4.3 WMM

WMM is known as Wireless Multi-Media, it provides the higher priority for those time-sensitive services such as Video and voice. You can enable or disable this WMM function in this page.

Another option is **U-APSD**; it is one type of the Power Saving. By default it is enabled.

Shown as below:



2.4.4 Advanced Settings

Under **Advanced Settings**, some professional settings are provided. As below:

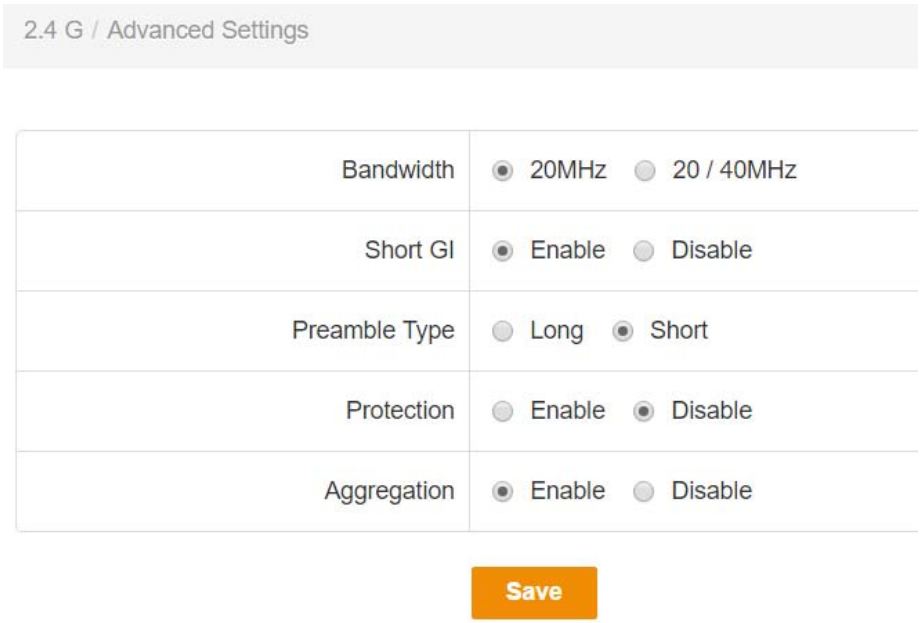


Figure 2-17 The advanced setting interface

(1) **Bandwidth**: can be set to **20MHz** or **40MHz**. **40MHz** here indicates the coexistence of 20MHz and 40MHz.

(2) **Short GI**: can be set to **Enable** or **Disable**. GI indicates the transmission interval of the data block. A short GI results in faster transmission rate and also high probability of error, especially in the multipath effect environment.

(3) **Preamble Type**: can be set to **Long** or **Short**. The 802.11 frame contains three parts: preamble, header, and payload. When the preamble is short, the transmission rate is high, but the compatibility may be poor.

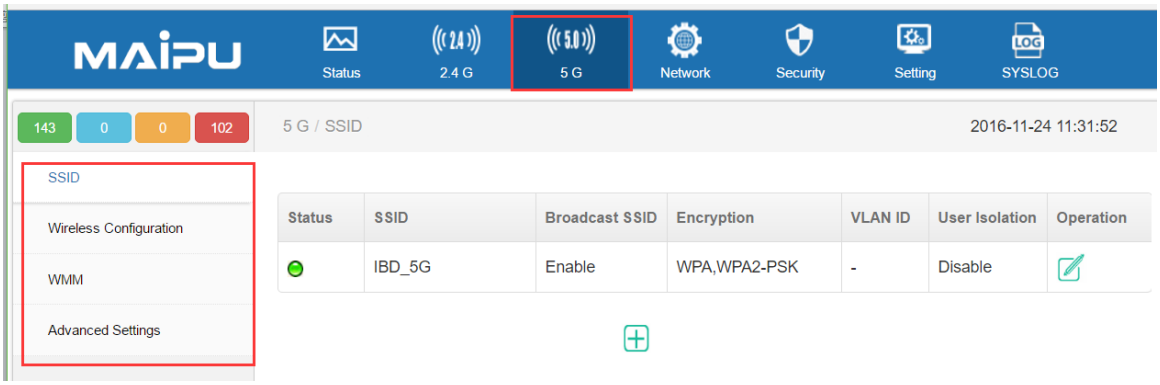
(4) **Protection**: can be set to **Enable** or **Disable**. Protection, b/g Protection, indicates the protection mode of 802.11b. Because the work modes of b, g, and n are different, the entire network efficiency will be greatly reduced if the 802.11b protection is enabled.

(5) **Aggregation**: can be set to **Enable** or **Disable**. Combining multiple data frames as one frame can obviously improve the network efficiency.

2.4.5 5G Wireless Configuration

5G wireless configuration has exact the same options as 2.4G wireless

configuration. The only difference is about wireless frequency and the related protocol.



For 5G detailed settings, kindly refer to the 2.4G part from chapter 2.4.1 to 2.4.4.

2.5 Network

2.5.1 IP Address

On the **IP Address** interface, you can configure the IP address, subnet mask, and gateway of the AP. Through these functions, you can specify the AP to register on a certain AC. If the AP and AC do not exist in the same LAN, the gateway and IP address of the AP need to be filled. If the AP and AC exist in the same LAN, the information can be omitted.

Choose Network > **IP Address** to enter the **IP Address** interface, as shown in Figure 2-21.

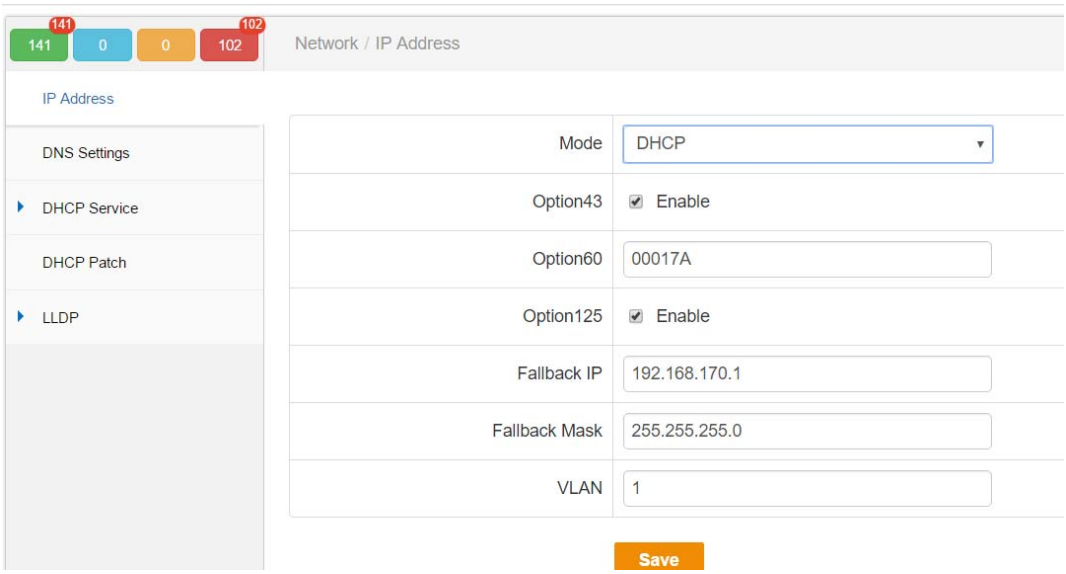


Figure 2-21 The IP address interface

(1) **Mode**: configure the AP's Management IP as DHCP or Static. If by DHCP, then AP will try to get IP address from the DHCP Server in the network. By Static, user has to configure all the IP related info, including IP address, Netmask, Gateway etc.

(2) **Option 43**: enable or disable. Option 43 is for AP to get the WLC's address. If enable this option, AP can directly get AC's IP address by the DHCP offer which has this option 43 info.

(3) **Option 60**: it is the vendor ID used in DHCP request process. When enabled, AP will send DHCP request with this ID and only if the DHCP

Server has such ID permitted and matched, Server will assign IP address to AP.

(4) **Option 125**: it is also included in DHCP process. AP will check this Option 125 info when received Offer from Server. Only when it matches the option 125 info of this AP, AP will accept this DHCP Offer.

(5) **Fallback IP**: secondary address of this AP. It won't change and always reachable when is visited by this IP. It's a backup IP for visiting once the main IP is not found.

(6) **Fallback Mask**: the network mask of the Fallback IP.

(7) **VLAN**: specifies the vlan number of the Management IP. By default it is VLAN 1.

2.5.2 DNS Setting

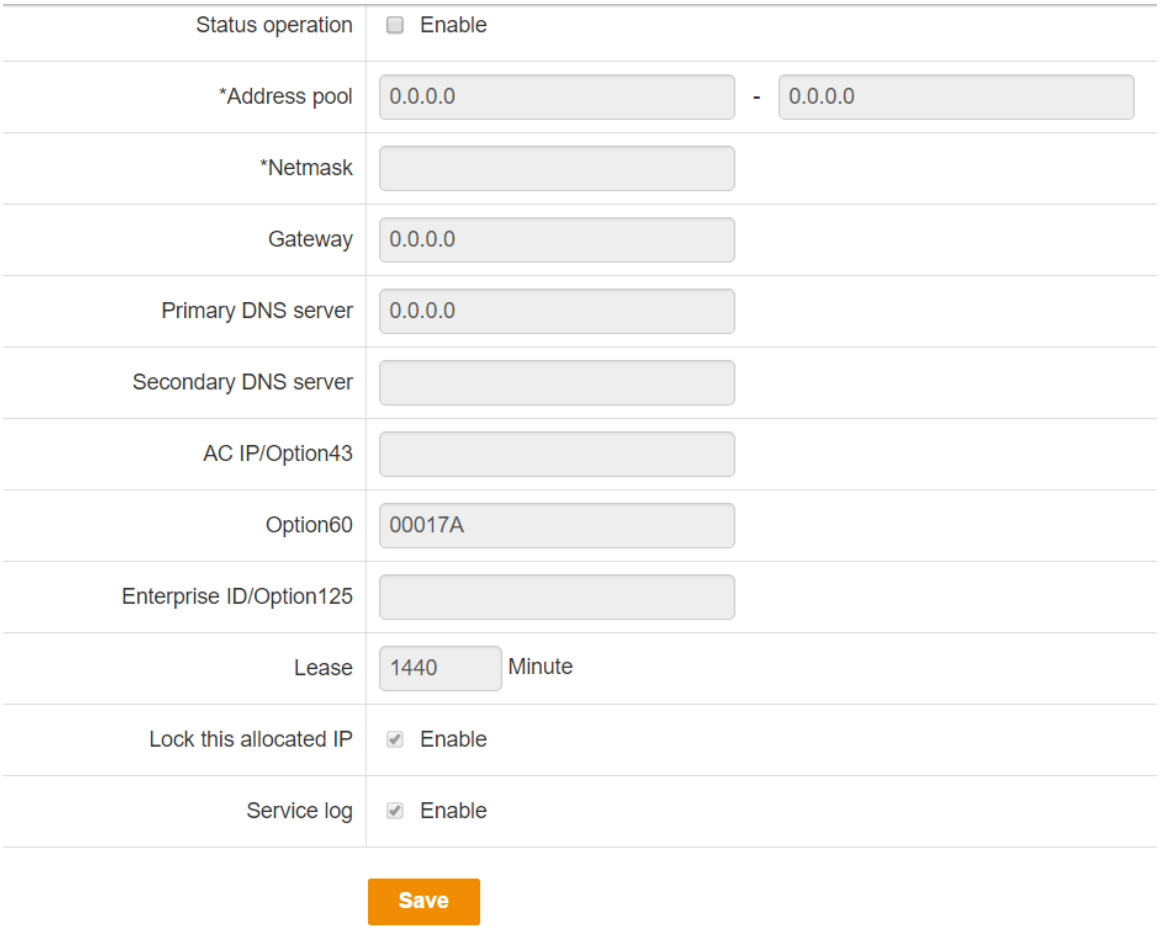
This function allows the user to modify the DNS configuration information of the AP and is usually used for the tracert detection function of the AP.

Figure 2-23 The DNS setting interface

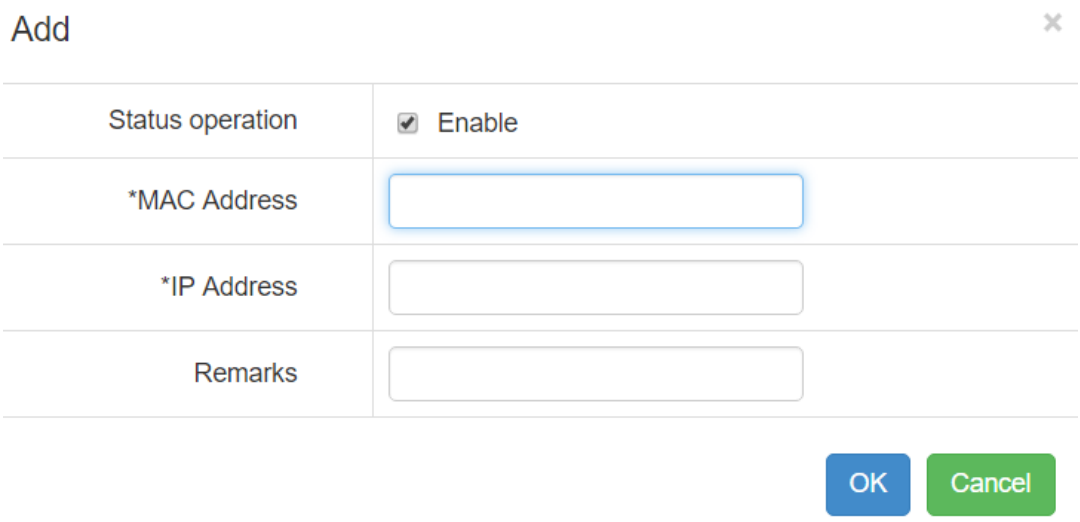
2.5.3 DHCP Service

Maipu AP itself can also work as a DHCP Server and assign IP address to the devices in this network. You can be configured by **DHCP Service.**

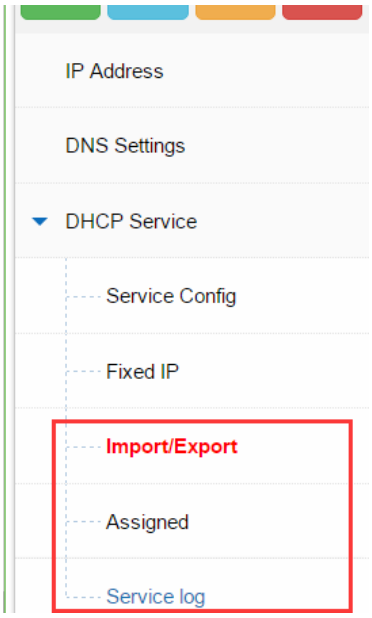
Go to **DHCP Service->Service Config,** and you can configure the DHCP Server parameters such as IP pool range, Gateway, DNS, option 43, option 60 and option 125 etc. referred as below:



Besides, users can assign a specific IP to a specific network device by binding its MAC address to the fixed iP. This can be done by the **Fixed IP** option.



Uses can also import/export the existing DHCP pool. There is also information about DHCP assignment available by going to **Assigned** Page and **Service Log**.



2.5.4 DHCP Patch

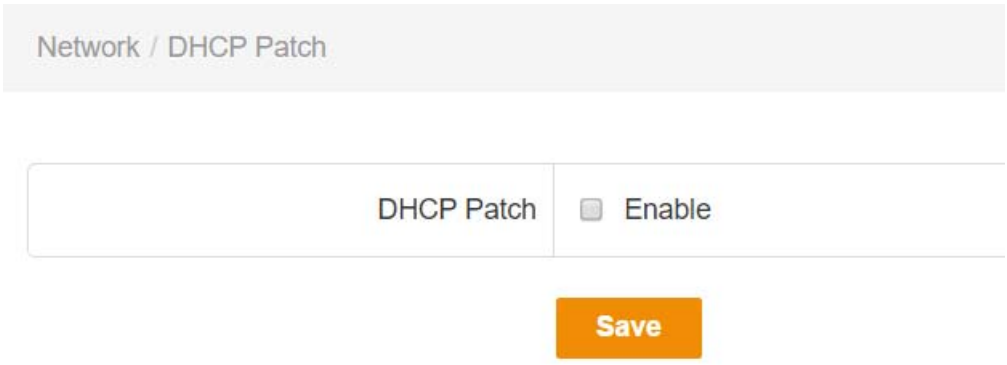


Figure 2-24 The DHCP patch interface

For some operating systems, such as Win7 and Mac OS X, the WLAN clients only receive the unicast DHCP packets, and do not receive the broadcast DHCP packets. Therefore, the DHCP patch function is added to the AP to solve the problem that some systems cannot obtain the IP address.
By default, it is disabled. If there is no problem of DHCP, please keep it disabled.

2.5.5 LLDP

The Link Layer Discovery Protocol or LLDP is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network.
On this LLDP Page, you could change the parameters including **Status**, **Tx**

Interval, **Time to Live** and **Fast Change**. You can also see the LLDP devices in the network by going to **the LLDP Neighbor State** Page.

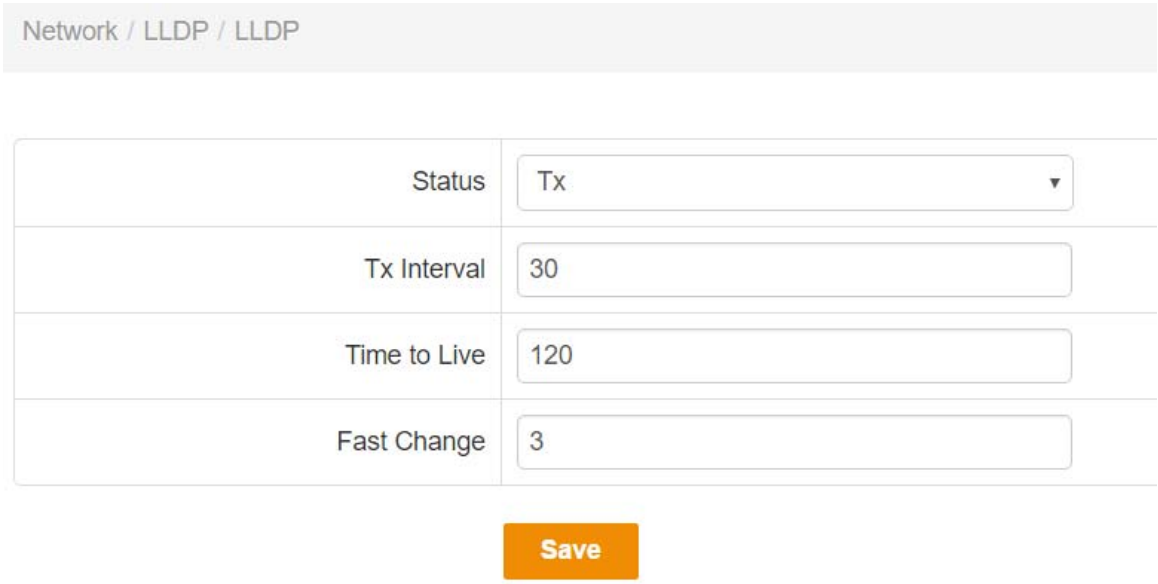


Figure 2-26 LLDP

2.6 Security

2.6.1 ARP Protection

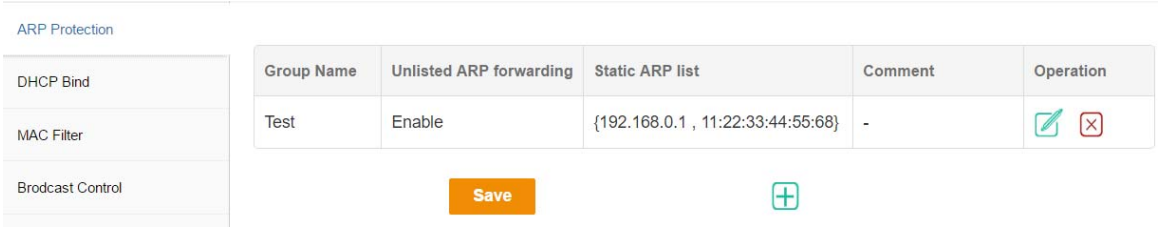


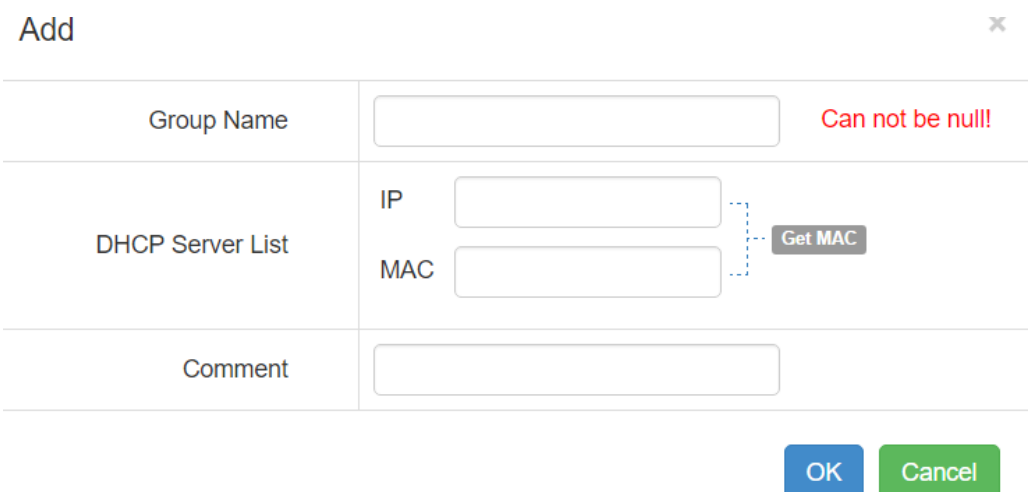
Figure 2-27 The ARP protection

Add one group with the static IPs and related MACs address. Then all of those ARP lists will be blocked. If enabled the “unlimited ARP forwarding”, those not included in the list won’t be affected.
After the configuration, the ARP Protection group should be chosen in Wireless SSID configuration, under **SSID->Network Security->ARP Protection.**

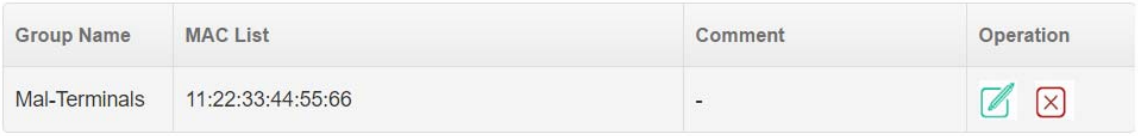
2.6.2 DHCP Bind

Sometimes there may be harmful DHCP Server in the network. By DHCP Bind, you can specify the DHCP Server with the IP and MAC address. Only the DHCP

Offer from this DHCP Server will be allowed to pass.
After the configuration, the group should be chosen in Wireless SSID configuration, under **SSID->Network Security->DHCP Bind.**



2.6.3 MAC Filter

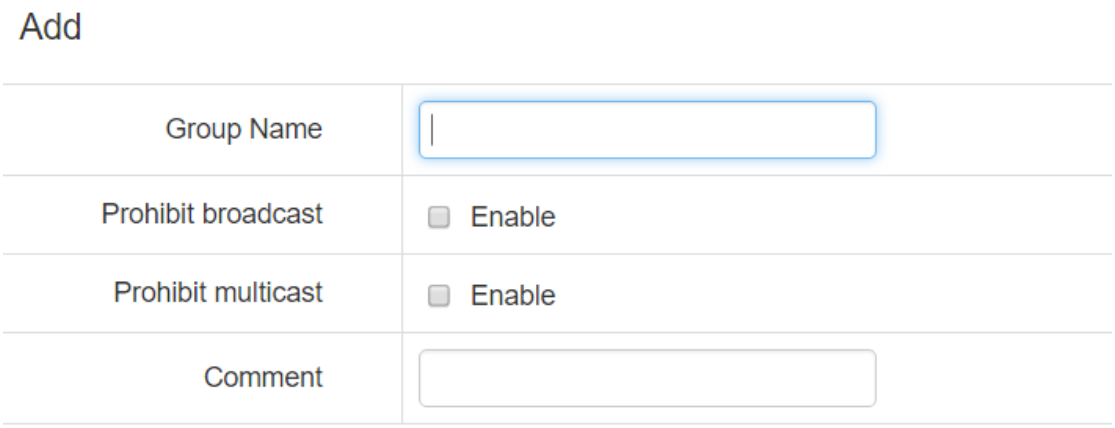


Users can configure the MAC group list here.

After the configuration, the group should be chosen in Wireless SSID configuration, under **SSID->Network Security->MAC Filter.** Whitelist or Blacklist can be chosen. Then choose the MAC list configured here.

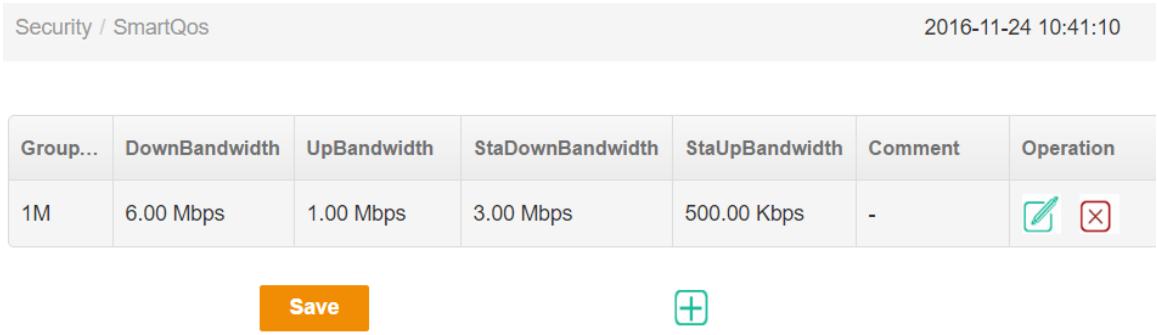
When choose **Whitelist**, only the listed MAC address will be allowed to connect to the AP.
When choose **Blacklist**, the listed MAC address will NOT be allowed to connect.

2.6.4 Broadcast Control

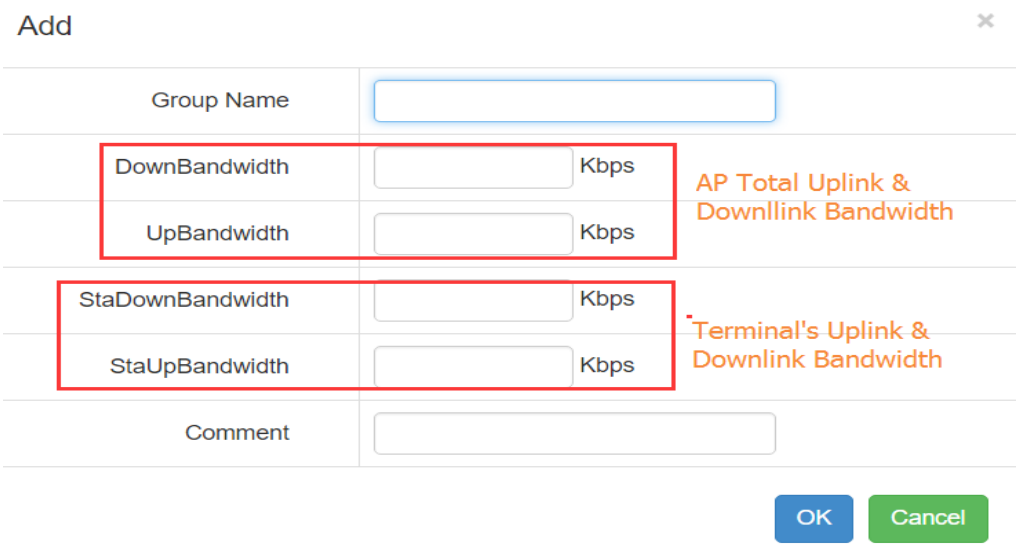


Broadcast control can be used to **Prohibit Broadcast** & **multicast** in the wireless network.
After the configuration, the group should be chosen in Wireless SSID configuration, under **SSID->Network Security->Broadcast Control.**

2.6.5 Smart QoS



Smart QoS can be used to limit the uplink and downlink speed as per AP or per user. Shown as below:

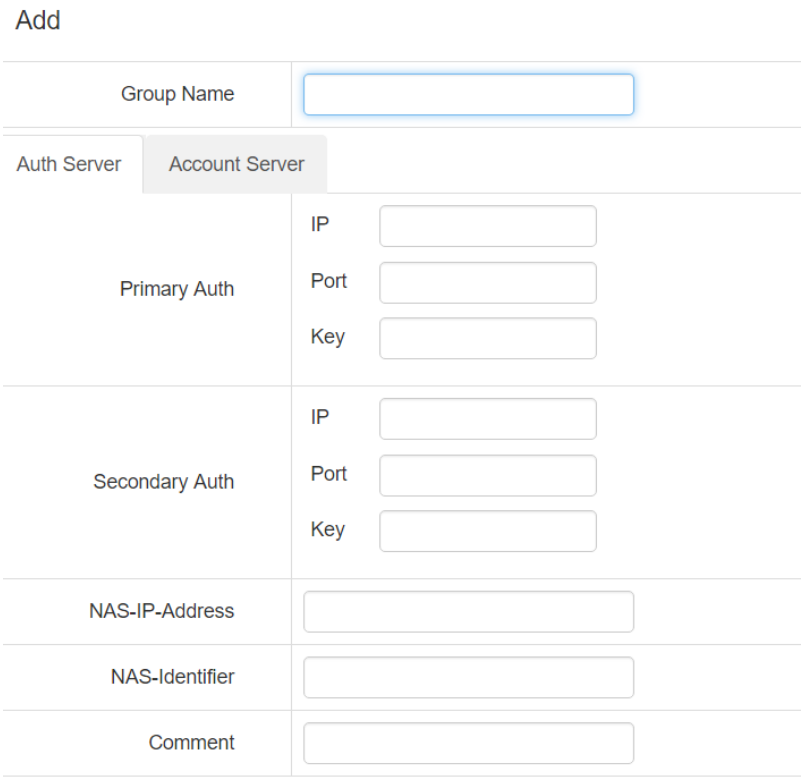


After the configuration, the group should be chosen in Wireless SSID configuration, under **SSID->Network Security->SmartQoS.**

2.6.6 RADIUS

If user is using WAP/WAP2-Enterprise Security Type, a third-Party Radius Server is needed in the network.

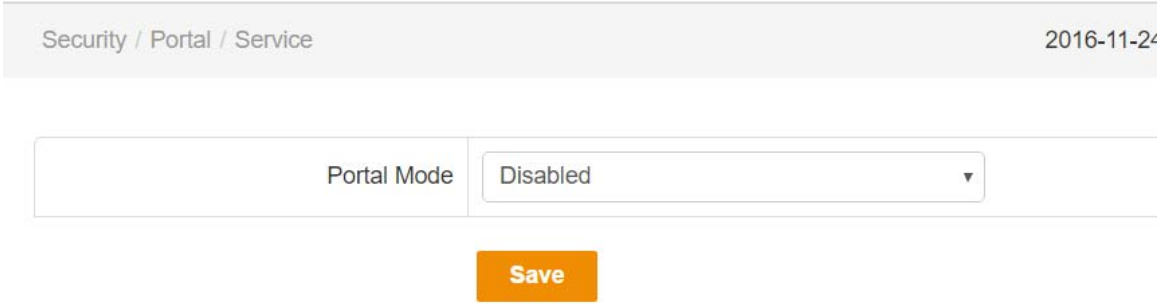
AP itself can also work with the third Party Radius Server by configuring the related info here. For the Radius parameters, please make sure it has the correct info configured here, or it can't communicate with Radius Server Properly.



After the configuration, when SSID is configured as WPA/WPA2-Enterprise, then the Radius Server can be chosen.

2.6.7 Portal

Portal page is to configure the Portal related parameters here.



2.7 Setting

2.7.1 Management

Choose **Setting->Management** to enter the **Management** page, as shown in Figure 2-28.

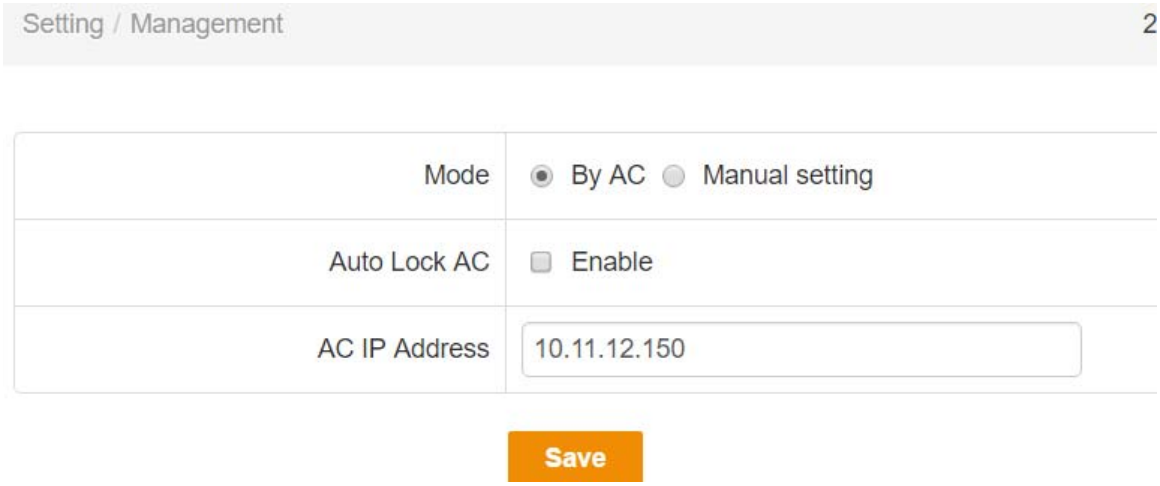


Figure 2-28 The management

(1) **By AC**: Mode for the AP is set to **By AC** by default. When the AP starts, the AP will automatically search the wireless AC in the LAN, register on the AC automatically (or by DHCP option 43 to find the AC's address), and download default template configuration from the AC, and the configuration takes effect immediately. For details, refer to the AP template description in the AC manual.

(2) **Auto Lock AC**: when this is enabled, AP will only be controlled by one AC, even if there is other AC available in the network.

(3) **AC IP address**: If DHCP option 43 is not enabled, and AP is managed by AC, then user has to input the AC's IP address here. If DHCP option 43 is enabled in DHCP Server, then AP can automatically get the AC's IP address.

2.7.2 Web Management

On the **Web management** interface, you can change the Hostname, **Web Timeout.** Maipu AP also supports https(by default disabled), user can enable here and the https port would be 443 by default.

User can also change the http or https port. As shown in Figure 2-29.

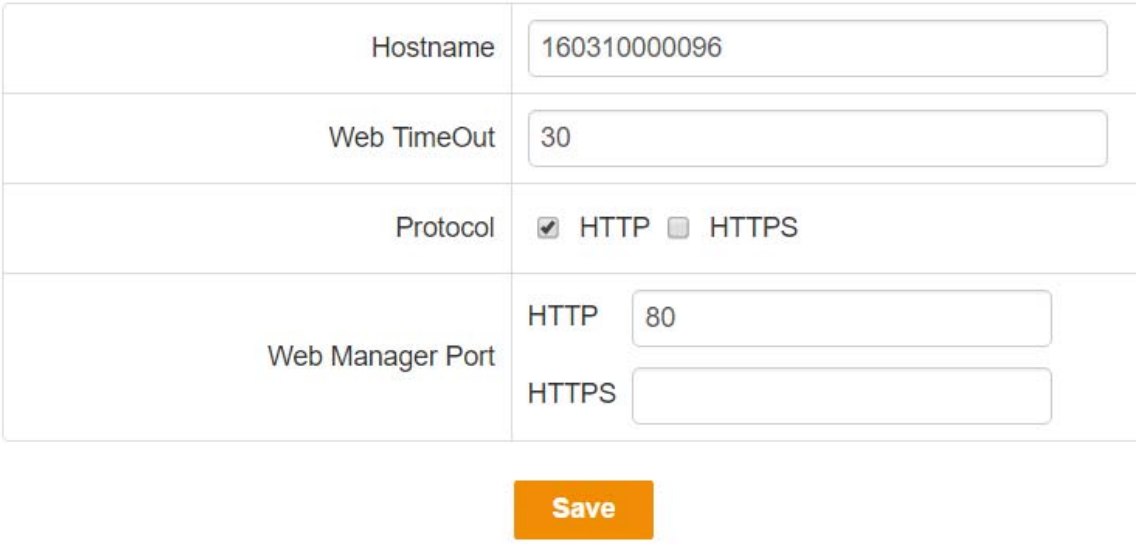
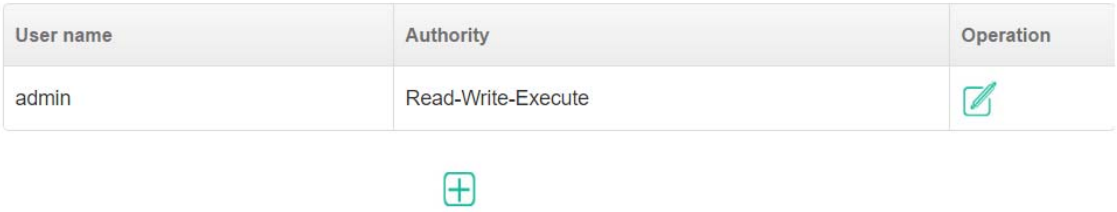


Figure 2-29 The web Management interface

2.7.3 Administrator

On the **Administrator** interface, you can set the local user name, password, and administrative authority of the user for logging in to the web management page.



Server Auth can also be supported in case Radius auth is required for logging in the web UI.

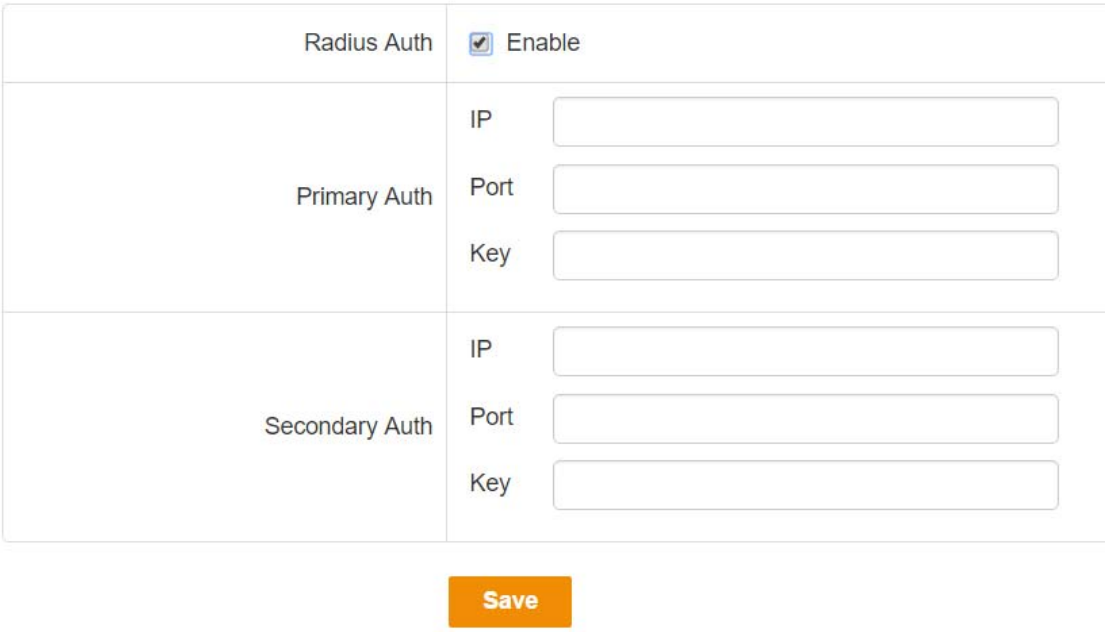


Figure 2-30 the administrator setting interface

2.7.4 Profiles

On the **Profile** interface**,** you can choose **Restore factory**, **Restore backup**, and **Save current**.

Choose **Settings** > **Profiles** to enter the **Restore factory**, **Restore backup**, and **Save current** interfaces, as shown in Figure 2-31.

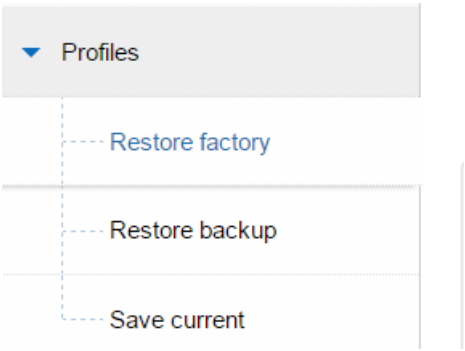


Figure 2-31 The configuration file interface

2.7.5 Firmware Upgrade

Firmware upgrade is a necessary function for the network product. The software must be optimized and upgraded continuously to satisfy the changeable network environment and meet different requirements. Whether the software upgrade can be promoted to meet the changeable requirements is more and more concerned by users.

Choose **Settings** > **Firmware Update** to enter the **Firmware Update** interface, as shown in Figure 2-32.

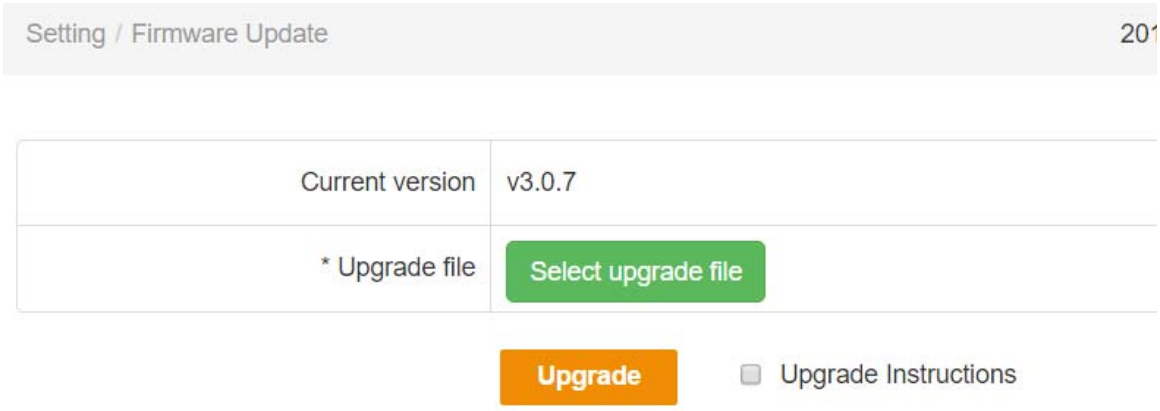


Figure 2-32 The firmware upgrade interface

Current version: displays the software version number used by the current system.

Upgrade file: specifies the software package for upgrading the system, which is provided by the manufacturer.

Notes:

1) There is risk for firmware upgrading. Do not pause during the upgrading. The whole upgrading process will take about two minutes. A message will be prompted when the upgrade succeeds, therefore please wait patiently during the upgrading.
2) After the upgrade succeeds, reboot the AP manually to take the new version into effect. If the upgrade error message is prompted, do not reboot the AP and just repeat the upgrade operations until the upgrade succeeds. If the upgrade error occurs and the AP is powered off or the AP is powered off during upgrading, the system will fail to be started. In this case, contact the technical personnel for support.

2.7.6 System Time

On the **System time** interface, set the AP system time, as shown in Figure 2-33.

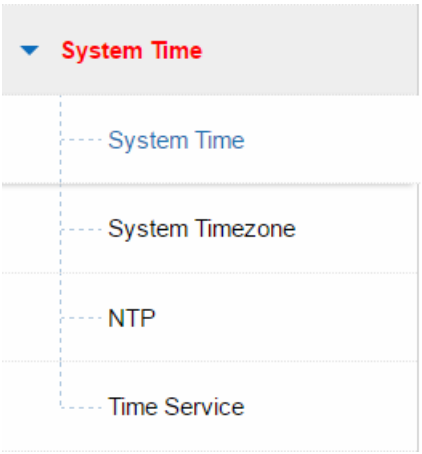
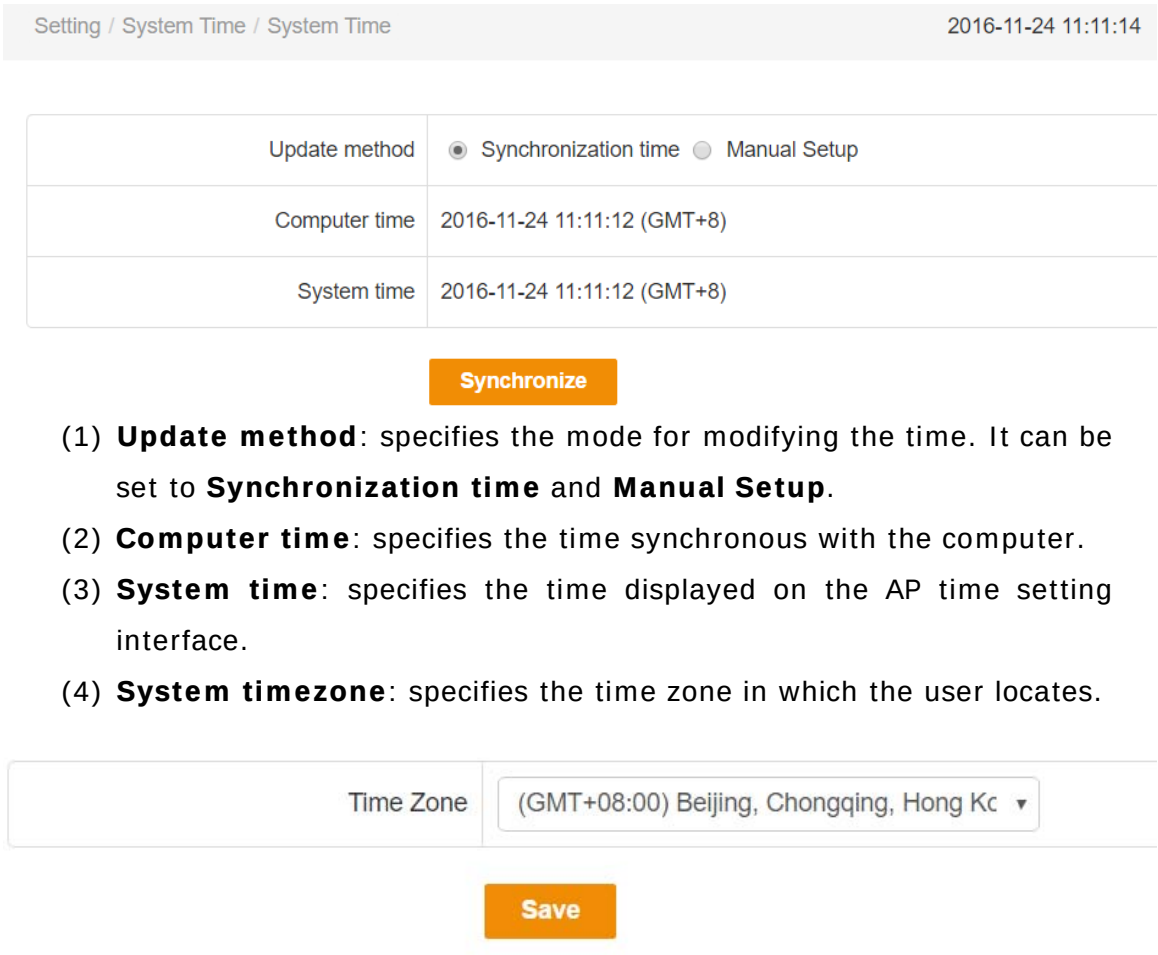


Figure 2-33 The system time interface



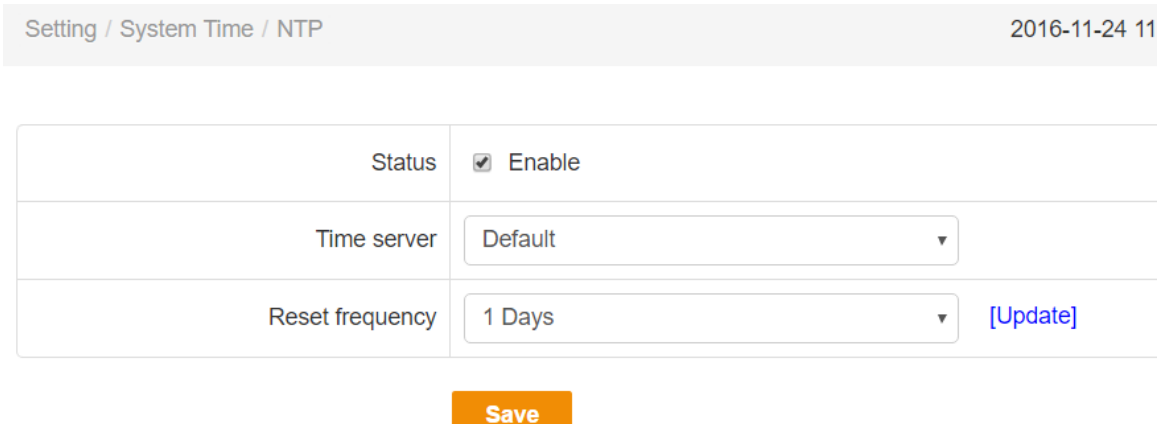
(1) **Update method**: specifies the mode for modifying the time. It can be set to **Synchronization time** and **Manual Setup**.

(2) **Computer time**: specifies the time synchronous with the computer.

(3) **System time**: specifies the time displayed on the AP time setting interface.

(4) **System timezone**: specifies the time zone in which the user locates.

(5) **Network time**: the AP will be automatically synchronized the time with the time server in a regular period.



(6) **Time service**: the user can choose whether to enable the time synchronization function.

2.7.7 OUI Update

You can update the OUI info by enabling OUI update on this page. The update frequency could also be configured here.

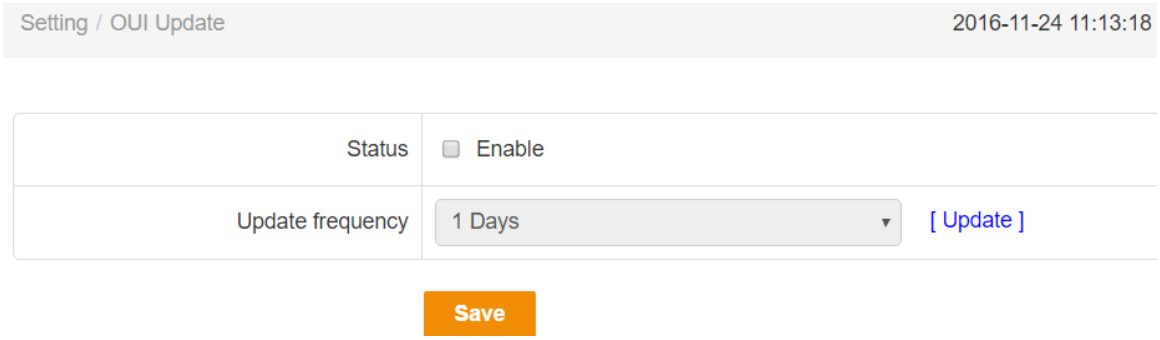


Figure 2-34 OUI Update

2.8 System Log

The AP running status is recorded and saved as a log to help us locate the fault, troubleshoot, and manage network security, and help us to analyze whether the AP is normal and whether the network is healthy.

2.8.1 Event Log

Choose **WEB Management** > **System Log** > **Event Log** to enter the **Event Log** interface, as shown in Figure 2-36.

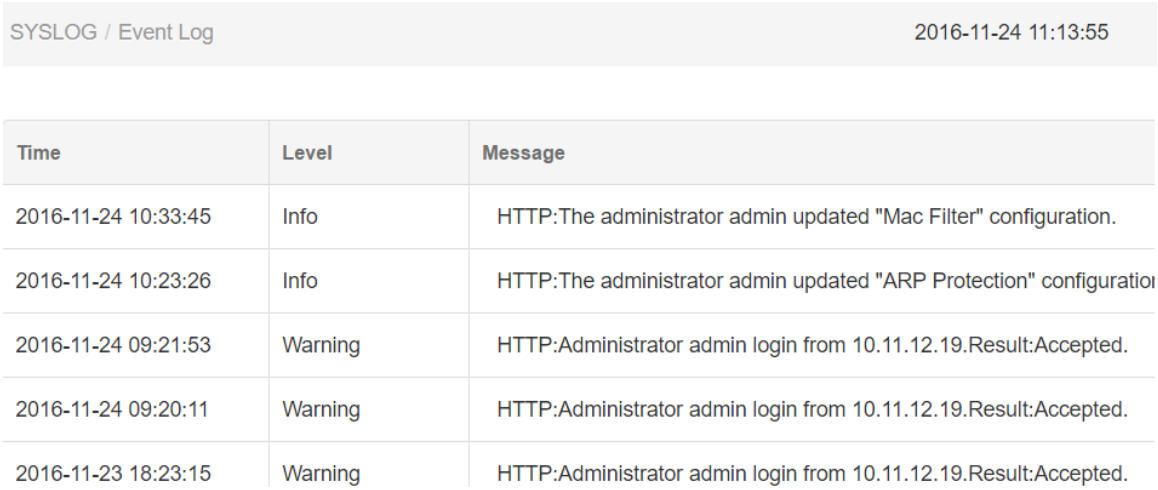


Figure 2-36 The event log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

(4) **Refresh**: click **Refresh** to refresh the latest log information.

(5) **Clear**: click **Clear** to clear the log information.

(6) **Export**: click **Export** to export the log to a text.

2.8.2 Network Log

Choose **SYSLog** > **Network Log** to enter the **Network Log** interface, as shown in Figure 2-39.

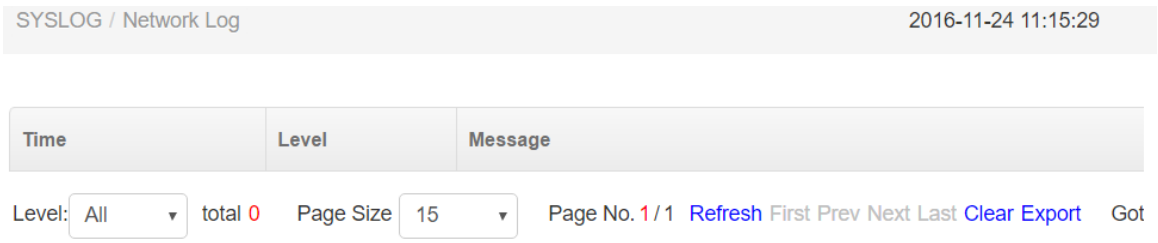


Figure 2-39 The network log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

2.8.3 Security Log

The security log contains the log tracing events, such as logging in to the system, change the visit authority, and start and shut down the system, as shown in Figure 2-38.

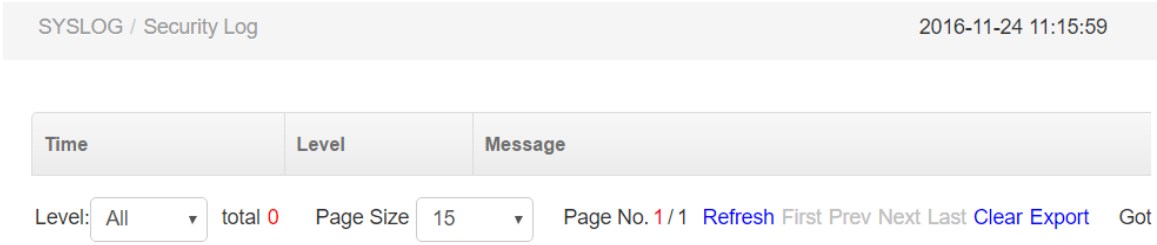


Figure 2-38 The security log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: can be classified into **Info** and **Warning**. **Info** records the running events and **Warning** reminds you notice based on the running event recorded.

(3) **Message**: records the running event.

2.8.4 Alarm Log

Choose **SysLog** > **Alarm Log** to enter the **Alarm Log** interface, as shown in Figure 2-37.

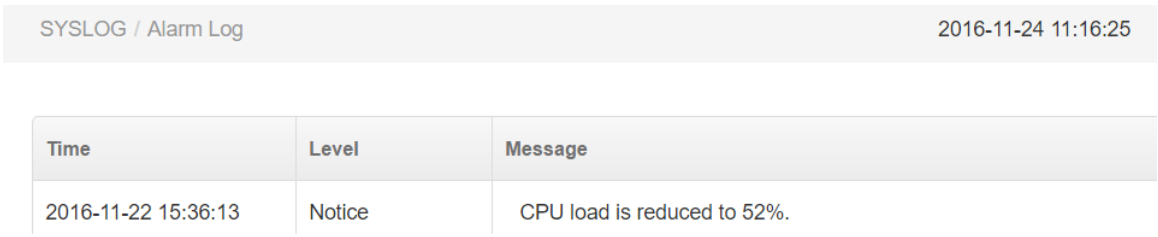


Figure 2-37 The alarm log interface

(1) **Time**: specifies the instant time when the system changes.

(2) **Level**: contains **Warning**. **Warning** reminds you notice.

(3) **Message**: records the running event.

Appendix

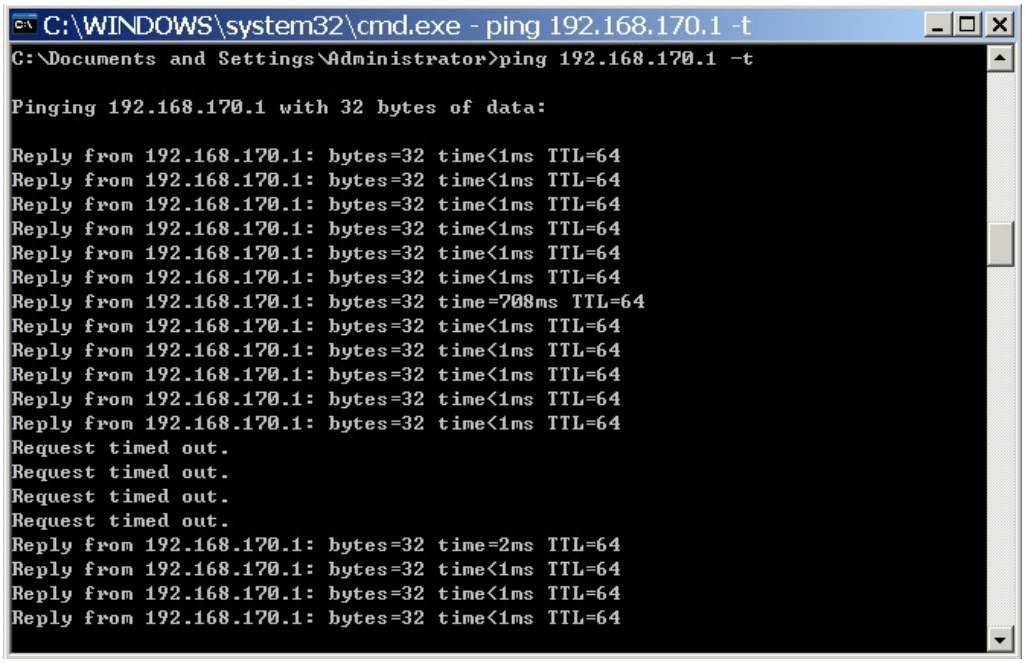
Hardware Restoration Configuration

If the AP password loss or other fault occurs, you can press the **Reset** button on the front panel to clear the configuration and restore the AP to the default setting.

Operation Steps:

Step 1: Power on the AP and start the AP to the normal work status. (The AP can be pinged through via the PC.)

Step 2: Use a sharp object to press the **Reset** button on the front panel and release the **Reset** button until the ping value is changed to a larger value, as shown in the following figure.



Step 3: Enable the AP to reboot automatically. The system restores the default configuration when the AP is rebooted normally.

Notes:

(1) This function will take effect when the AP is started normally. (The AP can be pinged through via the PC.)

(2) Press the **Reset** button and do not release in the midway.

(3) Contact the technical personnel for support if the system does not work normally.

FCC Caution:

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.