MAIPU

MyPower WNC6600 Series Wireless Controller

Operation Guide V7.8.0.36

迈普通信技术股份有限公司
www.maipu.com

Copyright

Copyright ©2023, 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 Maipu Communication Technology 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. In no event shall Maipu be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this manual or the related content on the website, even if advised of the possibility of such damage.

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.

Manual Introduction

This document mainly introduces how to quickly use the WEB configuration function of the WNC6600 series wireless controller, including the configuration wizard and the introduction of specific functions. This document cooperates with "MyPower WNC6600 Series Wireless Controller Configuration Manual" and "MyPower WNC6600 Series Wireless Controller Command Manual" to help readers master the use of specific commands.

product version

The product version corresponding to this manual is shown below.

Product Name	Product Model
MyPower WNC6600 Series Wireless Controller	WNC6600-100-AC (V1)
	WNC6600-200 - AC (V1)
	WNC6600-500-AC (V1)
	WNC6600-1000-AC (V1)
	WNC6600-2000-AC (V1)

Readers

This manual is mainly applicable to the following persons:

- On-site technical support and maintenance personnel
- Administrators responsible for network configuration and maintenance

Conventions

Conventions of screen output format:

Format	Description
Screen print	Represents the output information of the screen
Keywords of Screen print	The red part represents the key information in the screen output

Symbol conventions:

Format	Description
Note	An alert that contains additional or supplementary information.

copyright ©Maipu, all rights reserved

Format	Description
Caution	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
Warning	An alert that calls attention to important information that if not understood or followed can result in personal injury or device damage.

Command conventions:

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
Italic	Italic text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

The icons used in the manual and the meanings:

Icon	Description
	Represents a generic switch

copyright ©Maipu, all rights reserved

Icon	Description
	Represents a generic router

Product supporting manual

The accompanying manuals for this product are as follows:

Manual Name	Overview
"MyPower WNC6600 Series Wireless Controller Installation Manual"	Introduces the hardware specifications and installation methods of the device in detail, and guides you to install the device.
"MyPower WNC6600 Series Wireless Controller Configuration Manual"	Introduces the configuration method and configuration steps of the device software functions in detail, and provides typical cases for reference.
"MyPower WNC6600 Series Wireless Controller Command Manual"	Introduces the commands of WNC6600 series devices in detail, which is equivalent to a command dictionary, which is convenient for consulting the functions of each command.

Data Acquisition Method

Obtain the latest product manuals from Maipu's website (www.maipu.com).

Technical Support

If you encounter difficult-to-determined or difficult-to-solve problems in the process of equipment operation and maintenance, and you still cannot solve them through the guidance of the manual, please contact Maipu Technology Service Center directly, and we will provide you with technical support services.

copyright ©Maipu, all rights reserved

Contents

copyright ©Maipu, all rights reserved

copyright ©Maipu, all rights reserved

copyright ©Maipu, all rights reserved

copyright ©Maipu, all rights reserved

1 Log into Device

The login methods include WEB page, console port login, Telnet login, and SSH login. Currently, the most commonly used login method is the WEB page. This method is easy to use, has strong visualization and operability, and can manage and configure the AC quickly and conveniently.

Console port login:

Use a serial cable to connect the console ports of the PC and the AC, select the Serial protocol and the corresponding COM port, and change the baud rate to 9600 to log into the AC.

Telnet login:

Use a network cable to connect the control PC (configure the static address of192.168.1.0/24 on the PC side) to the DC0 port of the AC (the default address is192.168.1.100), and the Telnet address is192.168.1.100.

SSH login:

Use a network cable to connect the control PC (configure the static address of192.168.1.0/24 on the PC side) to the DC0 port of the AC (the default address is192.168.1.100), and the SSH address is192.168.1.100.

WEB page login:

Use a network cable to connect the control PC to the DC0 port of the AC (configure a static address of192.168.1.0/24 on the PC side), open a WEB browser on the PC side, and enter:192.168.1.100 in the address bar to access the WEB login of the AC page, as shown in Figure1.1.

copyright ©Maipu, all rights reserved

Figure 1.1 Web login page

In the opened login interface, enter the default user name and password (user name: admin, password: admin), and the system will prompt that the password needs to be changed, after successfully changing the password, log in again and enter the WEB page of AC, as shown in Figure1.2.

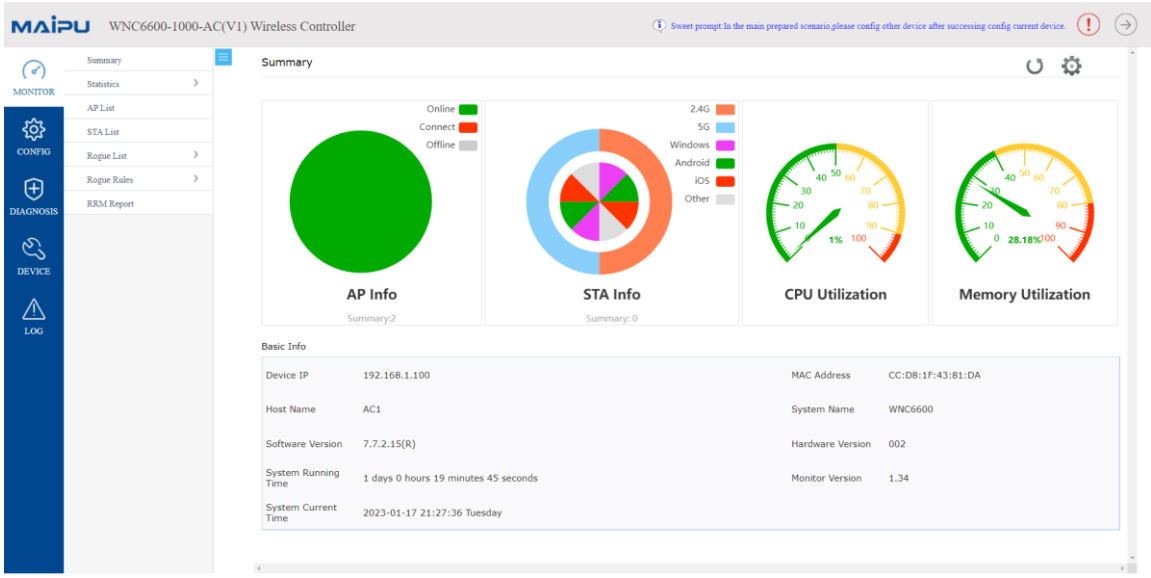


Figure 1.2 WEB page

After entering the page, you can modify the management address of the AC according to the networking requirements, as shown in Figure1.3.

copyright ©Maipu, all rights reserved

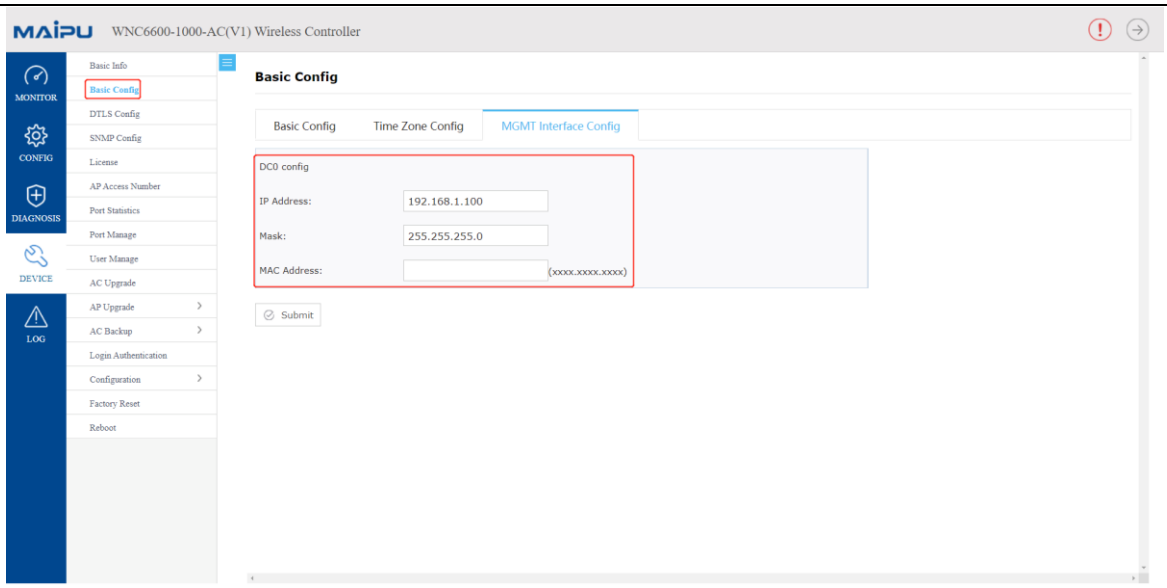


Figure 1.3 AC management address

You can also modify the country code of the AC according to the country and region. CN/HK/Russia/Belarus/Indonesia/Malaysia/Turkey/Thailand are currently supported, as shown in Figure1.4.

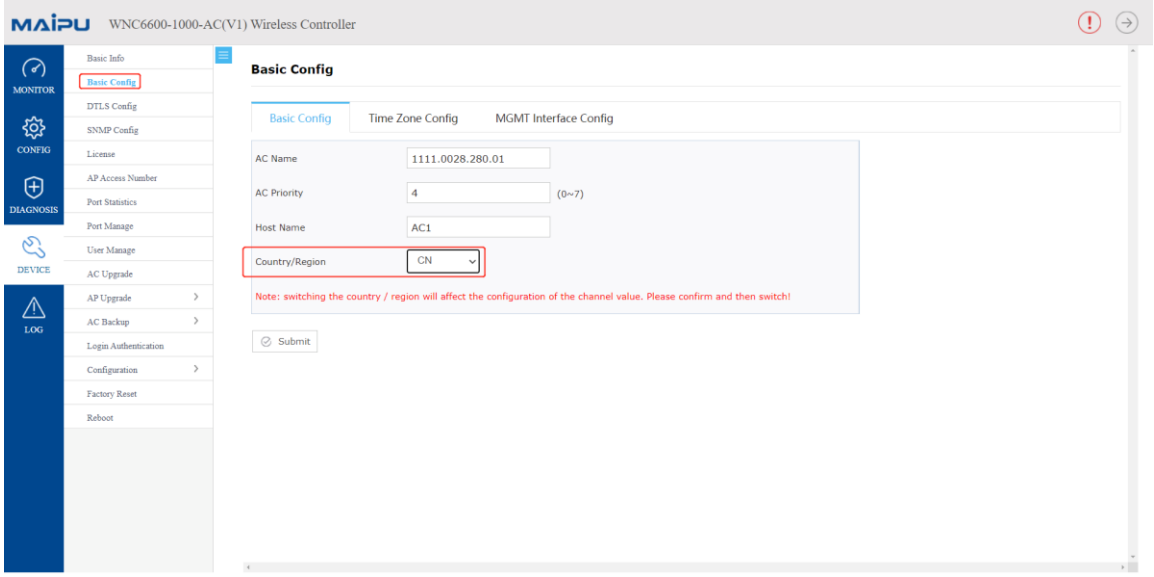


Figure 1.4 Configure the AC country code

The priority in the basic settings is the default priority, and the AC will carry this field in the packet for the AP to select the AC. If the AP joins the backup group, it carries the priority in the backup group, as shown in Figure1.5.

copyright ©Maipu, all rights reserved

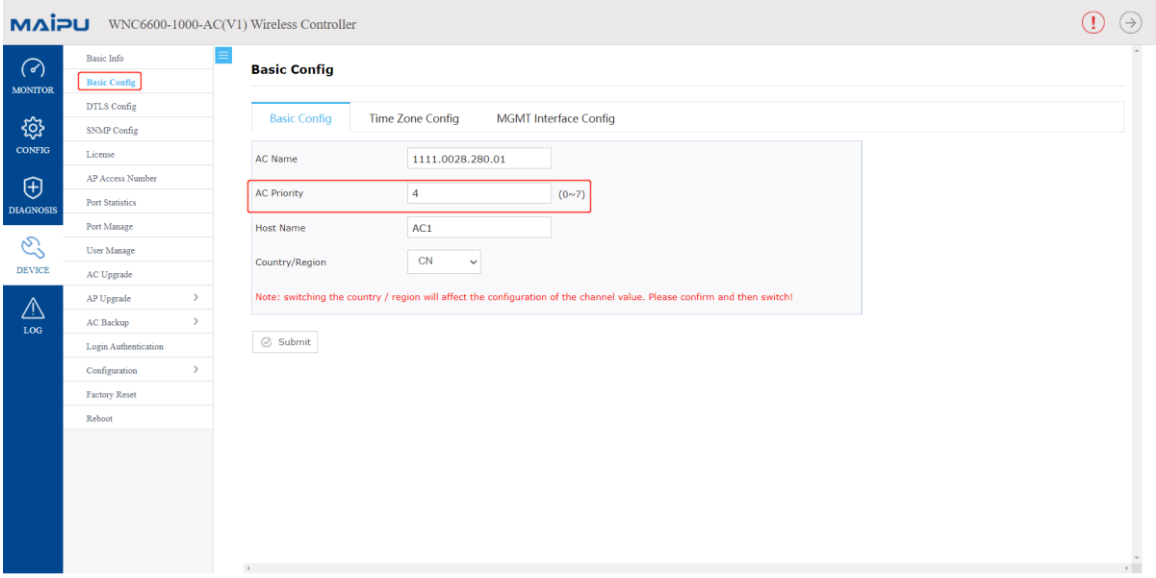


Figure 1.5 Configure AC priority

Note

- The current browser version is recommended to use IE8 and above.

copyright ©Maipu, all rights reserved

2 Quick Configuration Guide

2.1 Local Forwarding-wpa2-personal Authentication Configuration Guide

2.1.1 Networking Requirements

The AC connects to the L2 LAN through the bypass mode, the AP supplies power through the POE switch, the AP and the wireless terminal obtain IP addresses through DHCP, and the AP provides a wireless network with the name "abc" and enabled with wpa2-personal authentication.

2.1.2 Network Topology

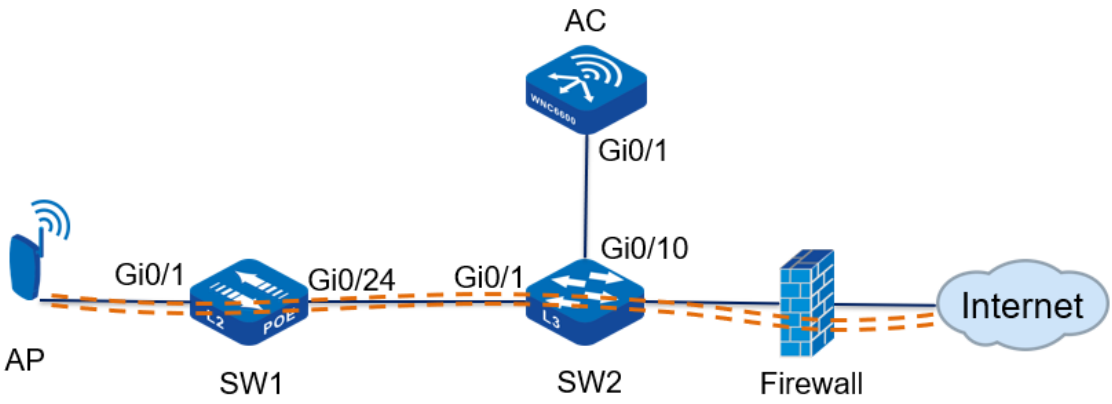


Figure2.1 wpa2-personal authentication in local forwarding mode

Topology introduction:

Wi-Fi security	wpa2-personal authentication, encryption type is AES
WLAN wireless service set	Wireless service set name: wlan1 SSID: abc Data forwarding mode: local forwarding
AP management VLAN	vlan10
AP service VLAN	vlan100
AP management IP address pool	192.168.10.10—192.168.10.100
AP management gateway	192.168.10.254 (on the core switch)
User IP address pool	192.168.100.10—192.168.100.100

copyright ©Maipu, all rights reserved

User gateway	192.168.100.254 (on the core switch)
DHCP server	The core switch acts as a DHCP server for APs and users

Table2.1 Topology introduction

2.1.3 Configuration Ideas

1. Configure intermediate network devices, including POE power supply switches and L3 core switches;
2. Configure DHCP server to provide IP address for AP;
3. Statically configure the IP address of the AC on the AP;
4. Create a wireless service set on the AC, and the authentication method is wpa2-personal;
5. Create an AP template on the AC, bind the wireless service set and apply it to the AP;
6. The wireless terminal accesses the wireless network, and the entries on the AC are normal;

2.1.4 Configuration Steps

1. POE switch (SW1) configuration

#Create vlan10 and vlan100 on SW1, and configure the link type of gigabitethernet0/1 connected to the AP as Trunk, allowing vlan10 and vlan100 to pass through, and the PVID is10.

```
SW1#cont
SW1(config)#vlan10,100
Please wait.....
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/1
SW1(config-if-gigabitethernet0/1)# switchport mode trunk
SW1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan10
SW1(config-if-gigabitethernet0/1)# exit
```

#Configure the link type of gigabitethernet0/24 connected to SW2 as Trunk, allowing vlan10 and vlan100 to pass through.

```
SW1#cont
SW1(config)#vlan10,100
Please wait.....
Done.
SW1(config)#
```

copyright ©Maipu, all rights reserved

```
SW1(config)#interface gigabitethernet 0/24
SW1(config-if-gigabitethernet0/24)# switchport mode trunk
SW1(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/24)# exit
```

2. Core switch (SW2) configuration

#Create vlan10, vlan100 and their corresponding vlan interface on SW2, and configure IP address for this interface, which will be used as the gateway between AP and wireless terminal.

```
SW2#cont
SW1(config)#vlan10,100
Please wait.....
Done.
SW2(config)#
SW2(config)#interface vlan10
SW2(config-if-vlan10)# ip address192.168.10.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan10)# exit
SW2(config)#
SW2(config)#interface vlan100
SW2(config-if-vlan100)# ip address192.168.100.25424
SW2(config-if-vlan100)# ip dhcp server
SW2(config-if-vlan100)#
```

#Configure the DHCP address pool ap-pool on SW2, dynamically allocate IP addresses for APs, and configure the gateway as192.168.10.254; configure the DHCP address pool sta-pool, dynamically allocate IP addresses for wireless terminals, and configure the gateway as192.168.100.254.

```
SW2#cont
SW2(config)#ip dhcp pool ap-pool
SW2(dhcp- config)# range192.168.10.10192.168.10.100255.255.255.0
SW2(dhcp- config)# default-router192.168.10.254
SW2(dhcp- config)# exit
SW2(config)#ip dhcp pool sta-pool
SW2(dhcp- config)# range192.168.100.10192.168.100.100255.255.255.0
SW2(dhcp- config)# default-router192.168.100.254
SW2(dhcp- config)# dns-server 8.8.8.8
SW2(dhcp- config)# exit
```

copyright ©Maipu, all rights reserved

#On SW2, configure the link type of gigabitethernet0/1 connected to SW1 as Trunk, allowing vlan10 and vlan100 to pass through; configure the link type of gigabitethernet0/10 connected to AC as access, and vlan as10.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/1
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW2(config-if-gigabitethernet0/24)# exit
SW2(config)#interface gigabitethernet 0/10
SW2(config-if-gigabitethernet0/24)# switchport mode access
SW2(config-if-gigabitethernet0/24)# switchport access vlan10
SW2(config-if-gigabitethernet0/24)# exit
```

#Configure the interface connected to the PC. On SW2, configure the link type of gigabitethernet0/20 as access and vlan as10. Connect the PC to port20 of the core switch SW2, and the PC can obtain the IP address.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/20
SW2(config-if-gigabitethernet0/20)# switchport mode access
SW2(config-if-gigabitethernet0/20)# switchport access vlan10
SW2(config-if-gigabitethernet0/20)# exit
```

3. AP configuration

#Connect the AP to the gigabitethernet0/1 port of the POE switch, AP supplies power normally, and check the IP address obtained by the AP on the core switch SW2.

```
SW2 #show ip dhcp pool ap-pool binding
Current DHCP binding information

Hardware-Address IP-Address Lease Status
0001.7a20.1840                1 92.1 68.10.101Day 05:58:44 ACKED

SW2 #
```

#Enter http://192.168.10.10 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

copyright ©Maipu, all rights reserved

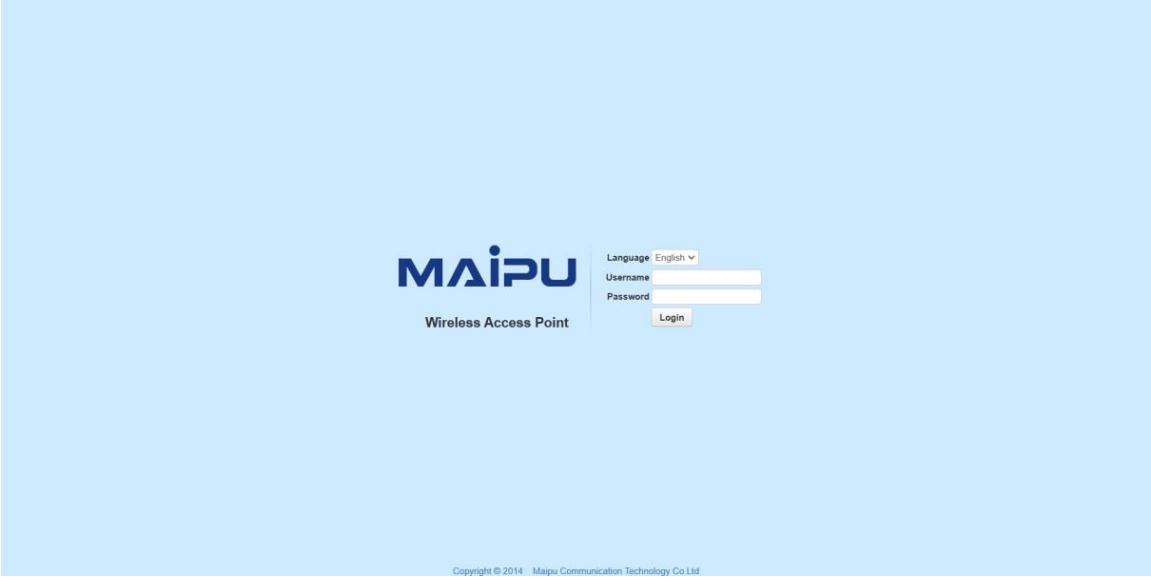


Figure 2.2 AP login page

#After entering the web management page of the AP, you will first enter the quick wizard configuration page. From step1 to step 3, you can directly use the default configuration. In step 4, configure the discovery method as static discovery, and configure the IPV4 address of the AC as192.168.10.1. If in the V6 environment, you can also configure the IPV6 address of the AC, and finally click the <Finish> button to complete the configuration, after the configuration is successful, it will jump to the system monitoring page.

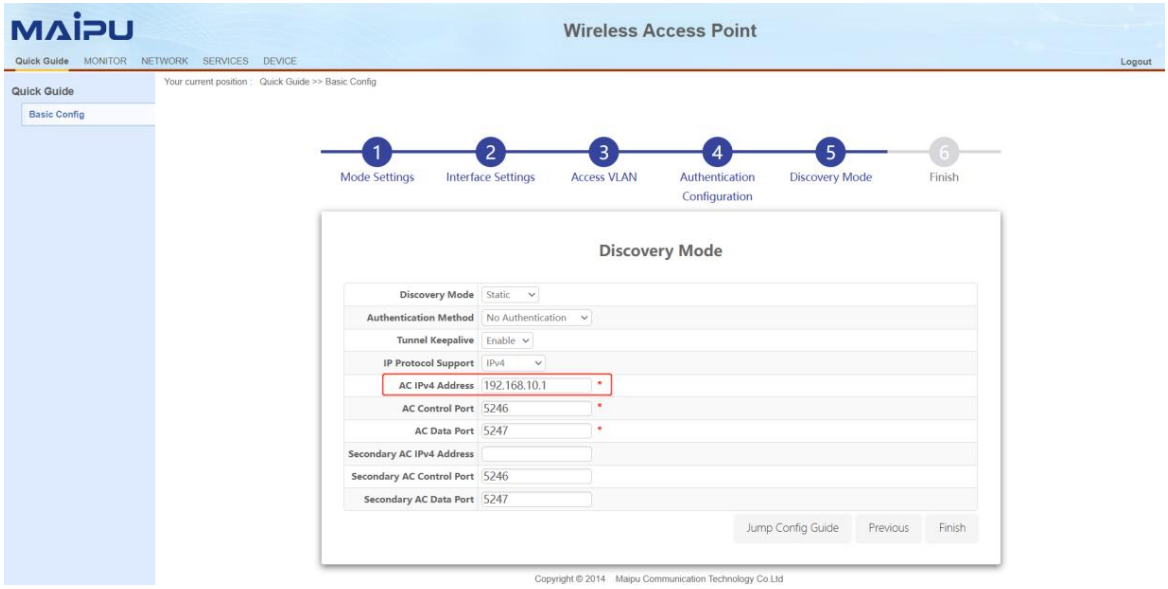


Figure 2.3 AP Configuration Wizard

4. AC configuration

#Create vlan10 and vlan100 on the AC, and create the corresponding vlan10 interface, which is used to establish a CAPWAP tunnel with the AP; configure the link type of gigabitethernet0/1 connected to SW2 to access, and vlan to10.

AC # con t

AC(config)#vlan10,100

copyright ©Maipu, all rights reserved

Please wait.....

Done.

AC(config)#

AC(config)#interface vlan10

AC(config-if-vlan10)# ip address192.168.10.124

AC(config-if-vlan10)# exit

AC(config)#interface gigabitethernet 0/1

AC(config-if-gigabitethernet0/1)# switchport mode access

AC(config-if-gigabitethernet0/1)# switchport access vlan10

After completing the above configuration, wait for about two minutes, the AP can successfully connect to the AC, and you can check the status of the AP on the AC. Enter http://192.168.10.1 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

Figure 2.4 AC login page

#Click MONITOR > AP list, and you can see that the AP is online, as shown in the figure below.

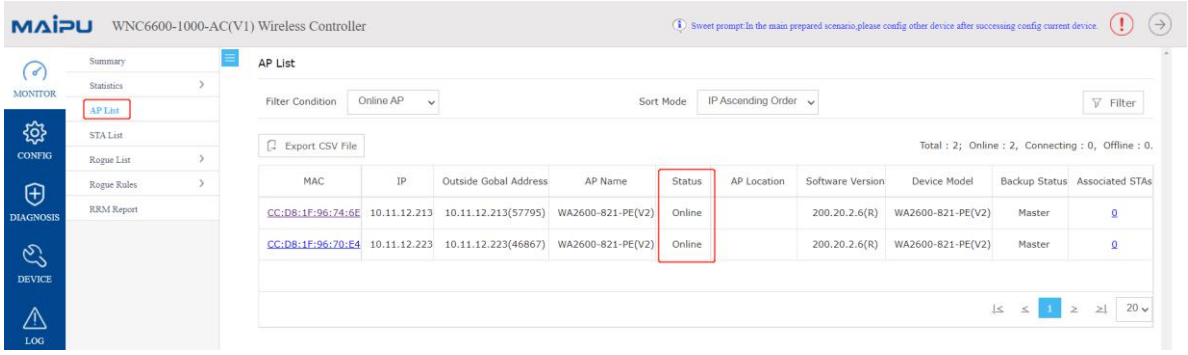


Figure 2.5 AP list

copyright ©Maipu, all rights reserved

#Create a wireless service set. Click CONFIG > WLAN > Wireless Service, and create a wireless service set, as shown in the figure below, the wireless name is wlan1, select “Enable” for sevice status, select "distributed forwarding" for forwarding mode, configure SSID as abc, configure user VLAN as100, select w pa2- personal for the authentication type, set the password to12345678, and use the default values for other configurations. Click the <OK> button to complete the configuration of the wireless service set.

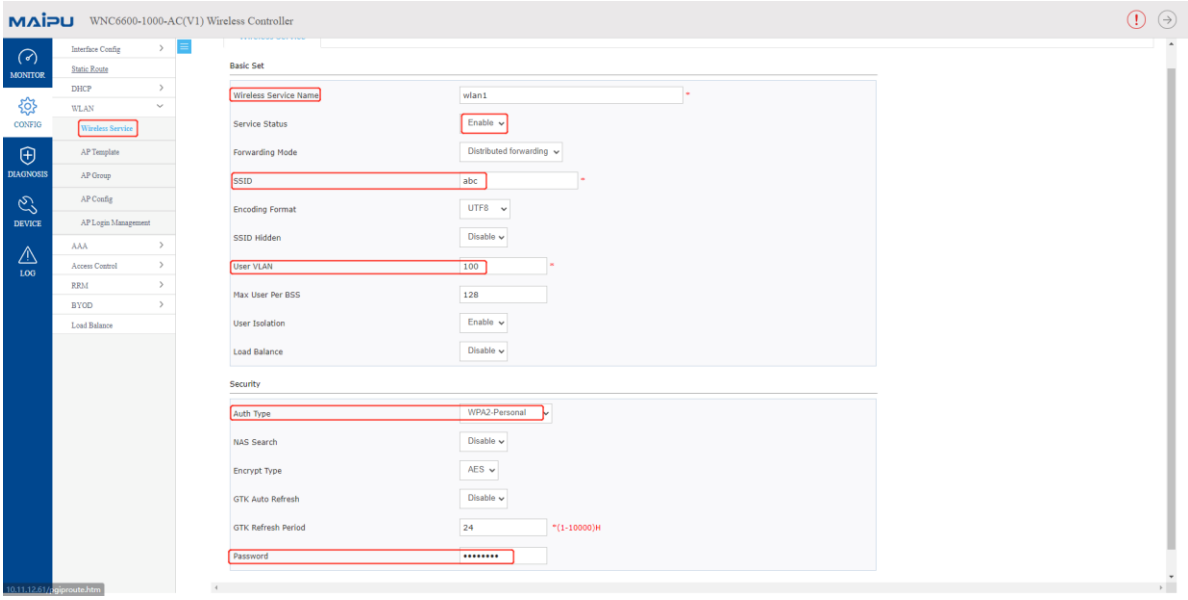


Figure 2.6 Wireless service configuration

#Bind the wireless service set to the AP profile. Click CONFIG > WLAN > AP Template to create an AP profile. By default, the name of the AP profile is Default_FitAP_Profile, which can be changed, after the creation is completed, the name cannot be changed, as shown in Figure2.7, create a new profile and name it profile1.

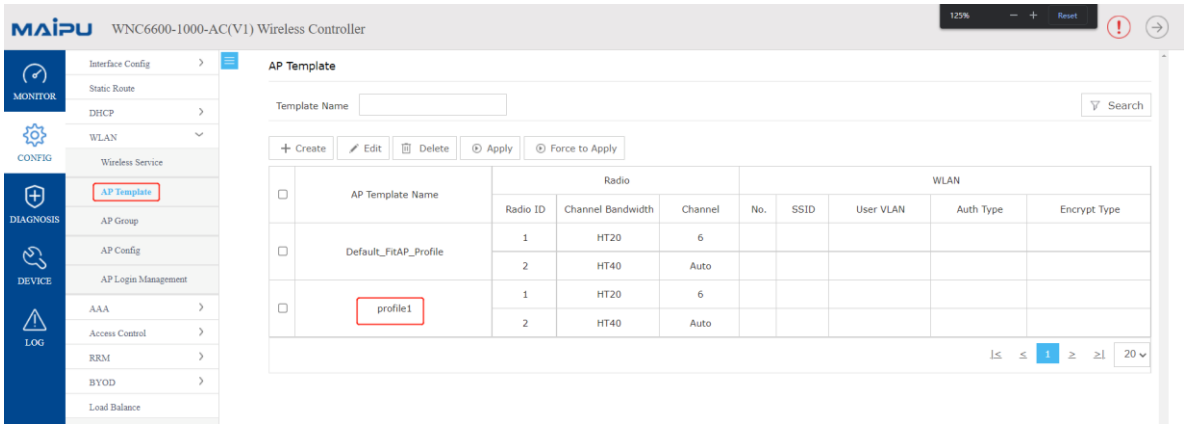


Figure 2.7 AP template

#Select the created AP template profile1, click the Edit button, Click BSS > Wireless Service Name, select wlan1 created above, select ALL for Radio ID, and use default values for other configurations, click <OK> button to complete AP template configuration.

copyright ©Maipu, all rights reserved

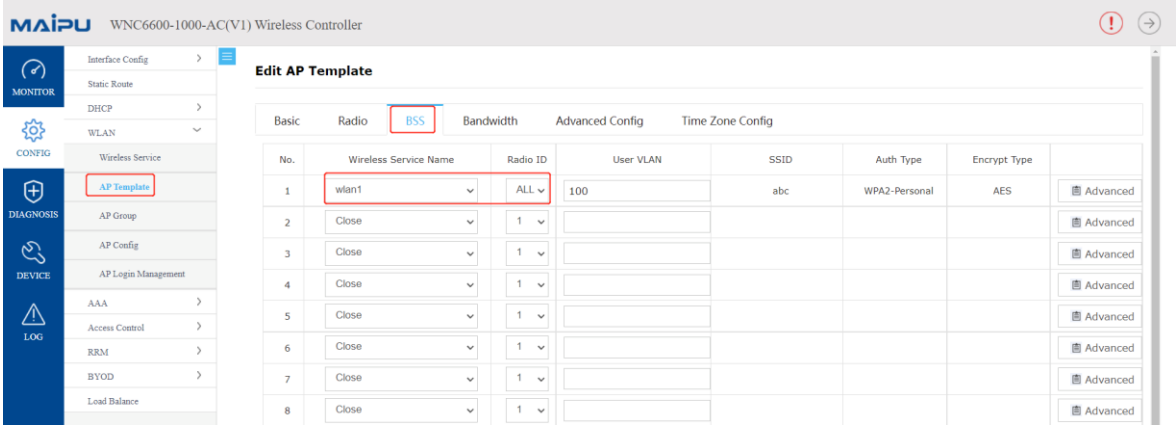


Figure 2.8 AP profile BSS configuration

#Apply the AP template. Click CONFIG > WLAN> AP Config, select the connected AP, select profile1 in the AP template, and then, click Apply in the template application.

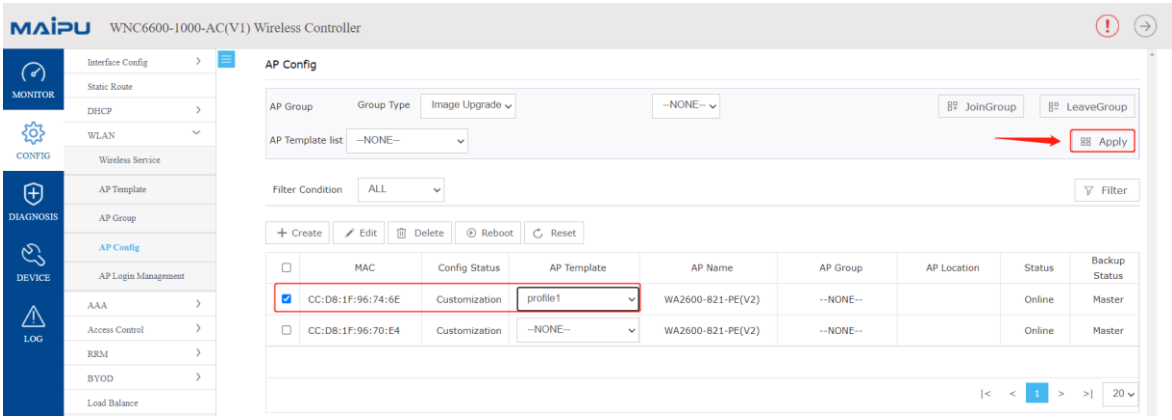


Figure 2.9 AP template application

2.1.5 Result Verification

#Wireless terminal access, after applying the AP template, after two minutes, turn on the wifi of the wireless terminal, and you can search for the wireless signal abc, after connecting to abc, click MONITOR >STA List on the AC web page, and you can see the information of the wireless terminal.

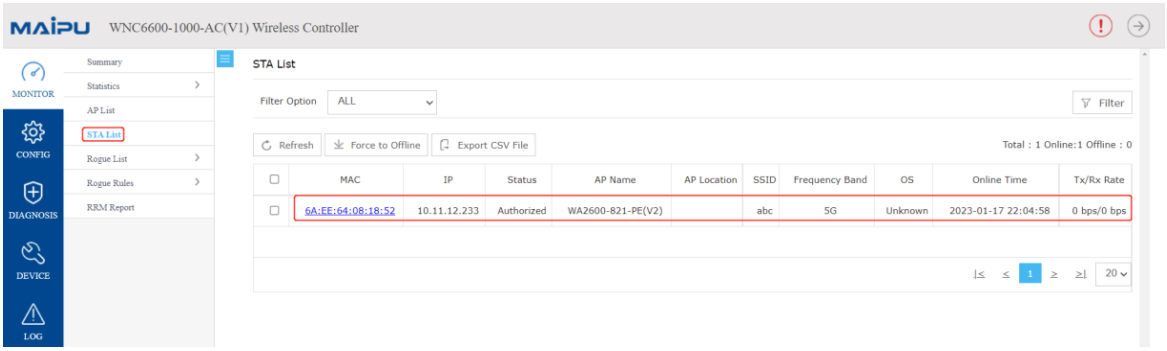


Figure2.10 Terminal list

copyright ©Maipu, all rights reserved

Note

- In addition to the BSS configuration, the AP template also needs to configure the working signal and channel bandwidth of the AP according to the actual network environment. The working channels of the2.4 G radio frequency generally choose1, 6, and11, and the channel bandwidth chooses HT20.
- The above example is based on a dual-band AP. Therefore, when configuring the BSS in the AP template, select all as the radio ID. For an AP that only supports2.4G radios, select1 as the radio ID.

2.2 Local Forwarding-portal Authentication Configuration Guide

2.2.1 Networking Requirements

The AC is connected to the L2 LAN through the bypass mode, the AP is powered by the POE switch, the AP and the wireless terminal obtain IP addresses through DHCP, and the AP provides a wireless network named "abc" and enabled with portal authentication.

2.2.2 Network Topology

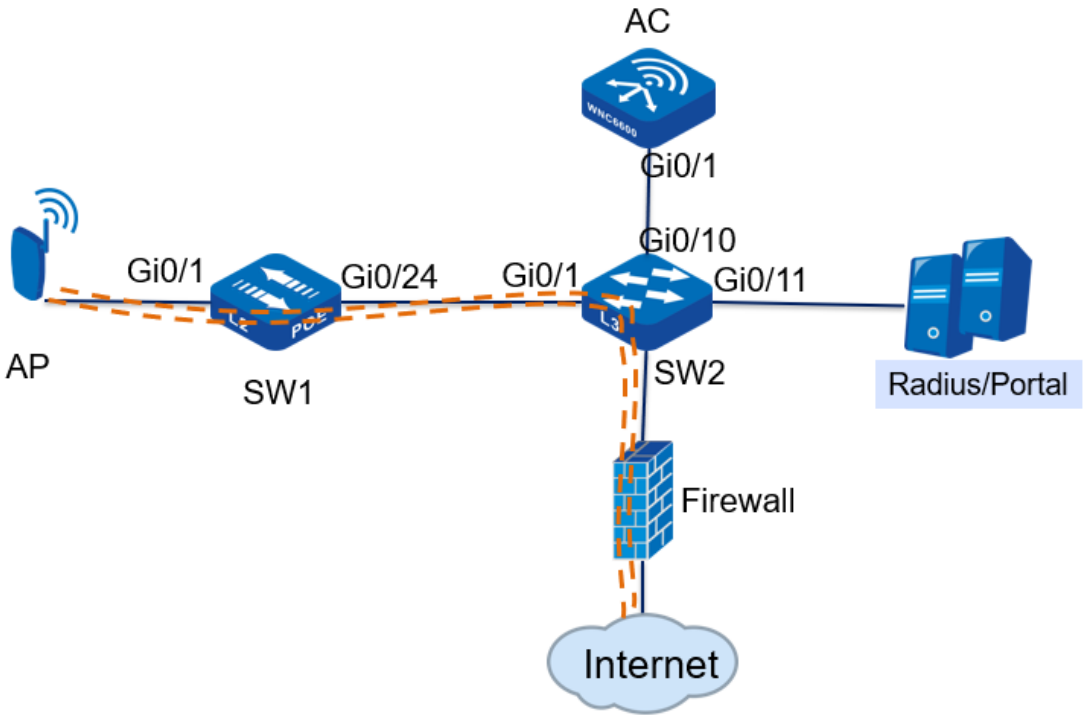


Figure2.11 Portal authentication in local forwarding mode

Topology introduction:

copyright ©Maipu, all rights reserved

Wi-Fi Security	portal authentication, no encryption
WLAN wireless service set	Wireless service set name: wlan1 SSID: abc Data forwarding mode: local forwarding
AP management VLAN	vlan10
AP service VLAN	vlan100
AP management IP address pool	192.168.10.10—192.168.10.100
AP management gateway	192.168.10.254 (on the core switch)
User IP address pool	192.168.100.10—192.168.100.100
User gateway	192.168.100.254 (on the core switch)
DHCP server	The core switch acts as a DHCP server for APs and users
AAS server IP address	192.168.10.253

Table 2.2 Topology introduction

2.2.3 Configuration Ideas

1. Configure intermediate network device interfaces, including POE power supply switches and Layer 3 core switches;
2. Configure DHCP server to provide IP address for AP;
3. Statically configure the IP address of the AC on the AP;
4. Create a portal redirection group on the AC and configure the portal server IP address;
5. Configure an authentication server on the AC and bind the authentication domain;
6. Create a wireless service set on the AC, bind the portal redirection combination authentication domain;
7. Create an AP template on the AC, bind the wireless service set and apply it to the AP;
8. Create an authentication account and password on the portal server;
9. The wireless terminal accesses the wireless network and can perform portal authentication;

2.2.4 configuration steps

1. POE switch (SW1) configuration

#Create vlan10 and vlan100 on SW1, and configure the link type of gigabitethernet0/1 connected to the AP as Trunk, allowing vlan10 and vlan100 to pass through, and the PVID is10.

```
SW1#cont
SW1(config)#vlan10,100
```

copyright ©Maipu, all rights reserved

```
Please wait......
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/1
SW1(config-if-gigabitethernet0/1)# switchport mode trunk
SW1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan10
SW1(config-if-gigabitethernet0/1)# exit
```

#Configure the link type of gigabitethernet0/24 connected to SW2 as Trunk, allowing vlan10 and vlan100 to pass through.

```
SW1#cont
SW1(config)#
SW1(config)#interface gigabitethernet 0/24
SW1(config-if-gigabitethernet0/24)# switchport mode trunk
SW1(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/24)# exit
```

2. Core switch (SW2) configuration

#Create vlan10, vlan100 and their corresponding vlan interface on SW2, and configure IP address for this interface, which will be used as the gateway between AP and wireless terminal.

```
SW2#cont
SW2 (config)#vlan10,100
Please wait......
Done.
SW2(config)#
SW2(config)#interface vlan10
SW2(config-if-vlan10)# ip address192.168.10.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan10)# exit
SW2(config)#
SW2(config)#interface vlan100
SW2(config-if-vlan100)# ip address192.168.100.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan100)#
```

#Configure the DHCP address pool ap-pool on SW2, dynamically allocate IP addresses for APs, and configure the gateway as192.168.10.254; configure the DHCP address pool sta-pool, dynamically allocate IP addresses for wireless terminals, and configure the gateway as192.168.100.254.

copyright ©Maipu, all rights reserved

```
SW2#cont
SW2(config)#ip dhcp pool ap-pool
SW2(dhcp- config)# range192.168.10.10192.168.10.100255.255.255.0
SW2(dhcp- config)# default-router192.168.10.254
SW2(dhcp- config)# exit
SW2(config)#ip dhcp pool sta-pool
SW2(dhcp- config)# range192.168.100.10192.168.100.100255.255.255.0
SW2(dhcp- config)# default-router192.168.100.254
SW2(dhcp- config)# dns-server 8.8.8.8
SW2(dhcp- config)# exit
```

#On SW2, configure the link type of gigabitethernet0/1 connected to SW1 as Trunk, allowing vlan10 and vlan100 to pass through; configure the link type of gigabitethernet0/10 connected to AC as access, and vlan as10.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/1
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW2(config-if-gigabitethernet0/24)# exit
SW2(config)#interface gigabitethernet 0/10
SW2(config-if-gigabitethernet0/24)# switchport mode access
SW2(config-if-gigabitethernet0/24)# switchport access vlan10
SW2(config-if-gigabitethernet0/24)# exit
```

#Configure the interface connected to PC. On SW2, configure the link type of gigabitethernet0/20 as access and vlan as10. Connect the PC to port20 of the core switch SW2, and the PC can obtain the IP address.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/20
SW2(config-if-gigabitethernet0/20)# switchport mode access
SW2(config-if-gigabitethernet0/20)# switchport access vlan10
SW2(config-if-gigabitethernet0/20)# exit
```

3. AP configuration

#Connect the AP to the gigabitethernet0/1 port of the POE switch, the AP is powered normally, and check the IP address obtained by the AP on the core switch SW2.

```
SW2 #show ip dhcp pool ap-pool binding
Current DHCP binding information
```

copyright ©Maipu, all rights reserved

Hardware-Address IP-Address Lease Status

0001.7a20.18401 92.1 68.10.101Day 05:58:44 ACKED

SW2 #

#Enter http://192.168.10.10 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

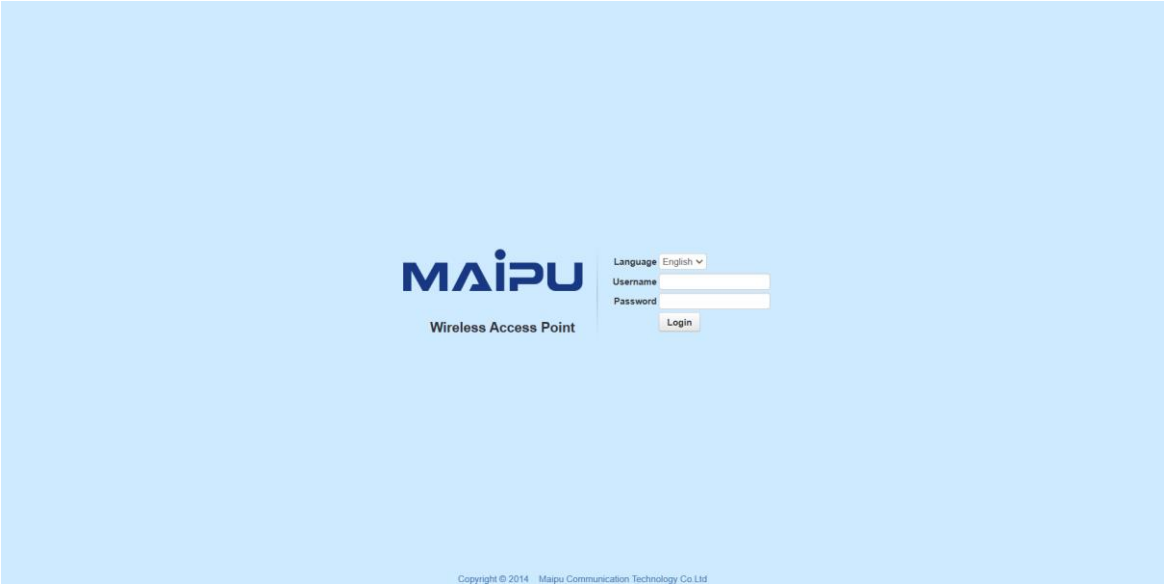
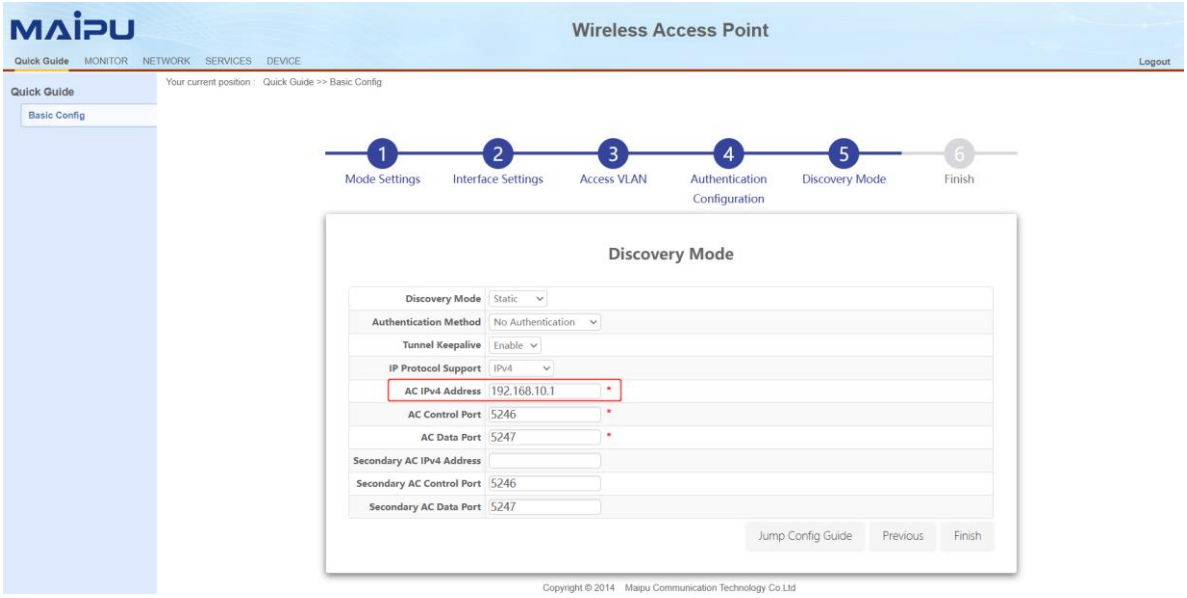


Figure 2.12 AP login page

#After entering the web management page of the AP, you will first enter the quick wizard configuration page. From step1 to step 3, you can directly use the default configuration. In step 4, configure the discovery method as static discovery, and configure the IPv4 address of the AC as192.168.10.1. If it is in the V6 environment, you can also configure the IPV6 address of the AC, and finally click the <Finish> button to complete the configuration, after the configuration is successful, it will jump to the system monitoring page.



copyright ©Maipu, all rights reserved

Figure 2.13 AP Configuration Wizard

4. AC configuration

#Create vlan10 and vlan100 on the AC, and create the corresponding vlan10 interface, which is used to establish a CAPWAP tunnel with the AP; configure the link type of gigabitethernet0/1 connected to SW2 to access, and vlan to10.

```
AC # con t
AC(config)#vlan10,100
Please wait.....
Done.
AC(config)#
AC(config)#interface vlan10
AC(config-if-vlan10)# ip address192.168.10.124
AC(config-if-vlan10)# exit
AC(config)#interface gigabitethernet 0/1
AC(config-if-gigabitethernet0/1)# switchport mode access
AC(config-if-gigabitethernet0/1)# switchport access vlan10
```

#After completing the above configuration, wait for about two minutes, the AP can successfully connect to the AC, and you can view the status of the AP on the AC. Enter http://192.168.10.1 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

Figure 2.14 AC login page

#Click MONITOR > AP list, and you can see that the AP is online, as shown in Figure2.15 below.

copyright ©Maipu, all rights reserved

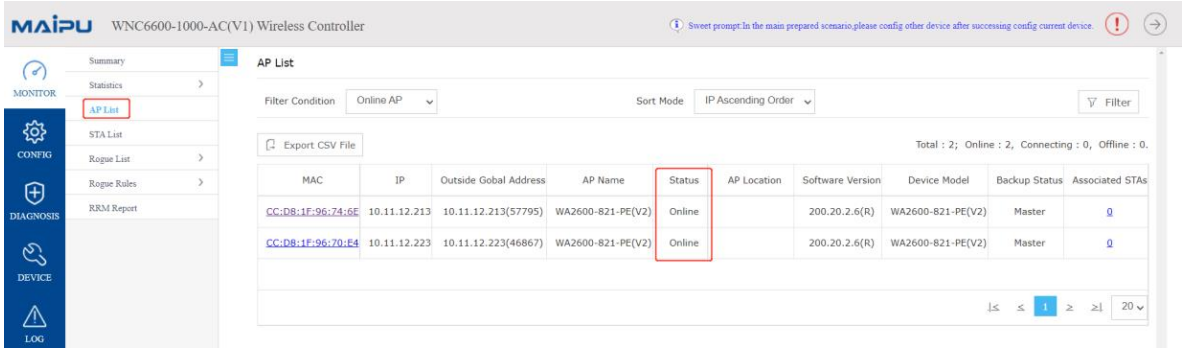


Figure 2.15 AP list

#Add NAS IP. Click CONFIG > AAA > NAS, select the IP address100.0.52.10, and click the <Add> button to set it as the NAS IP.

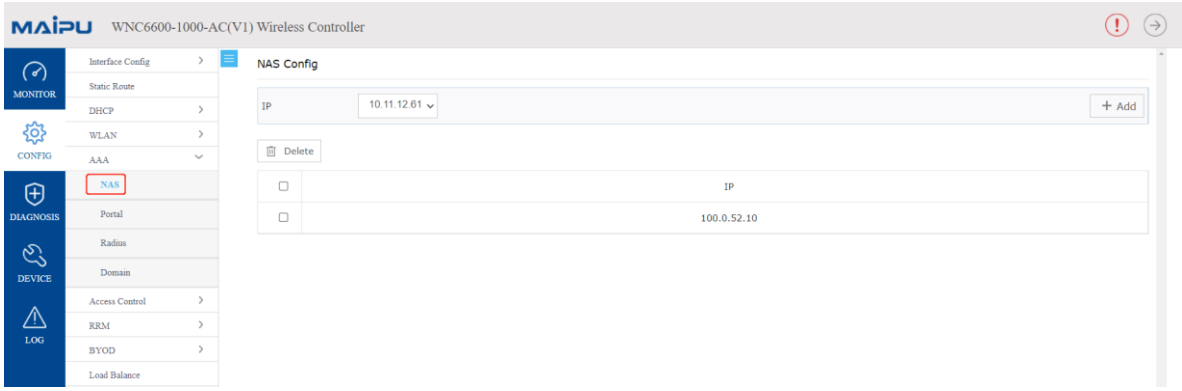


Figure 2.16 NAS configuration

#Create a portal redirection group. Click CONFIG > AAA > Portal > Basic Configuration, click <Create> to create a new portal redirection group, the Portal name is the name of the redirection group, here it is configured as portal, the Portal address is configured as192.168.10.253, and the URL is set to http://192.168.10.253:80/portal/Login.do according to the format in the help prompt, and enable registration and keepalive. In Portal client configuration, select100.0.52.10, click <Add>, after the above configuration, the portal redirection group is complete.

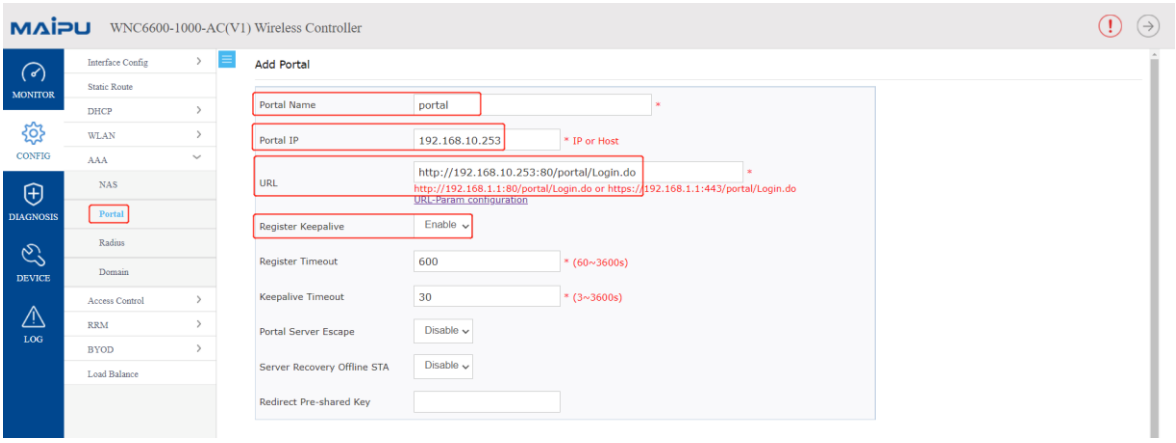


Figure 2.17 Portal configuration

copyright ©Maipu, all rights reserved

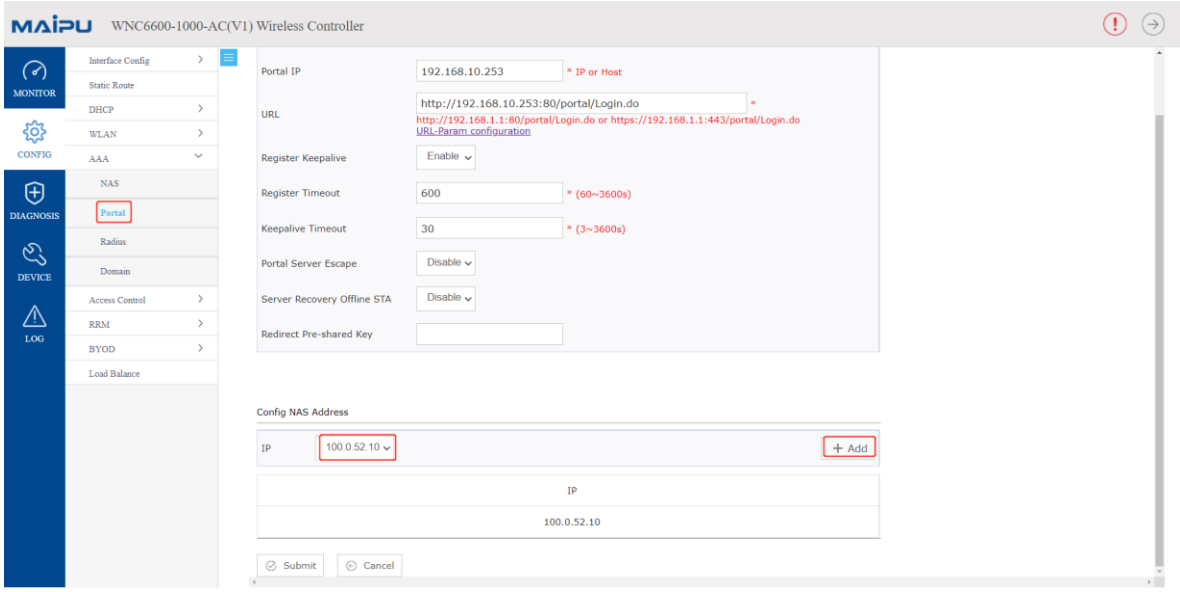


Figure 2.18 Portal client configuration

#Configure authentication server. Click CONFIG > Radius > Authentication Server List, click <Create>, create a new authentication server, configure the server address as192.168.10.253, configure the RADIUS client, set the IP address as100.0.52.10, configure the pre-shared key as admin, and click <Add>, after performing the above configuration, click the OK button below to complete the configuration of the authentication server.

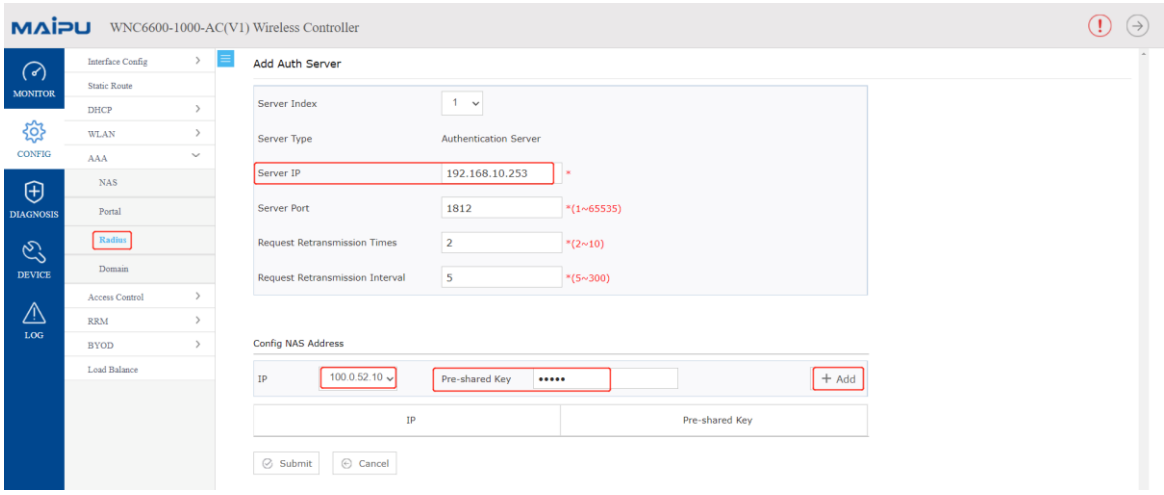


Figure 2.19 Authentication server configuration

#Domain configuration. Click CONFIG > AAA > Domain, click <Create> to create a new authentication domain, the domain name is the name of the authentication domain, here it is configured as yu, the authentication status is configured to enable, the authentication server selects192.168.10.253, and click <Add>, after performing the above configuration, click the OK button below to complete the configuration of the authentication domain.

copyright ©Maipu, all rights reserved

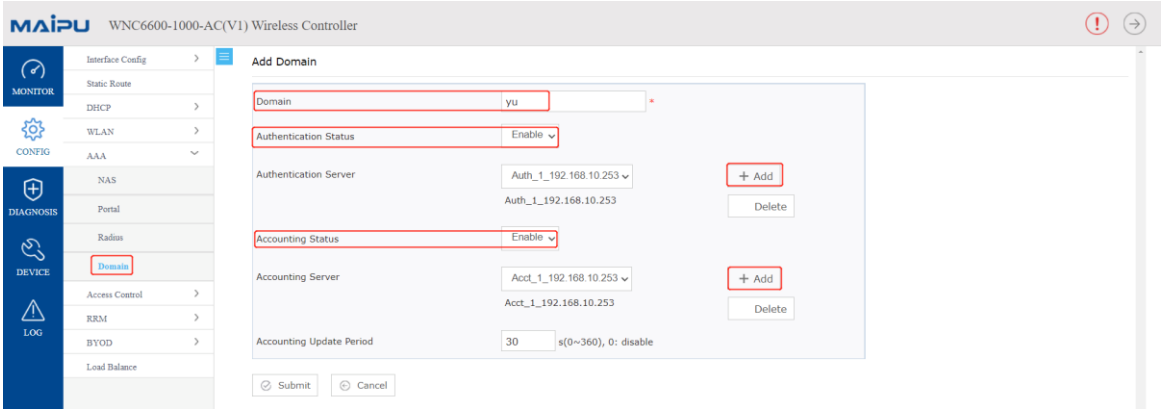


Figure 2.20 Domain configuration

#Create a wireless service set. Click CONFIG > WLAN > Wireless Service, create a wireless service set, as shown in the figure below, the wireless name is wlan1, select "Enable" for the wireless status, select "distributed forwarding" for forwarding mode, configure SSID to abc, configure user VLAN to100, select open for authentication mode, enable Portal authentication, select portal for Portal server name, select yu for Radius authentication domain, enable NAS information query, configure NAS information query AC-IP parameter as NAS IP address, and use default values for other configurations. Click the <OK> button to complete the wireless service set configuration.

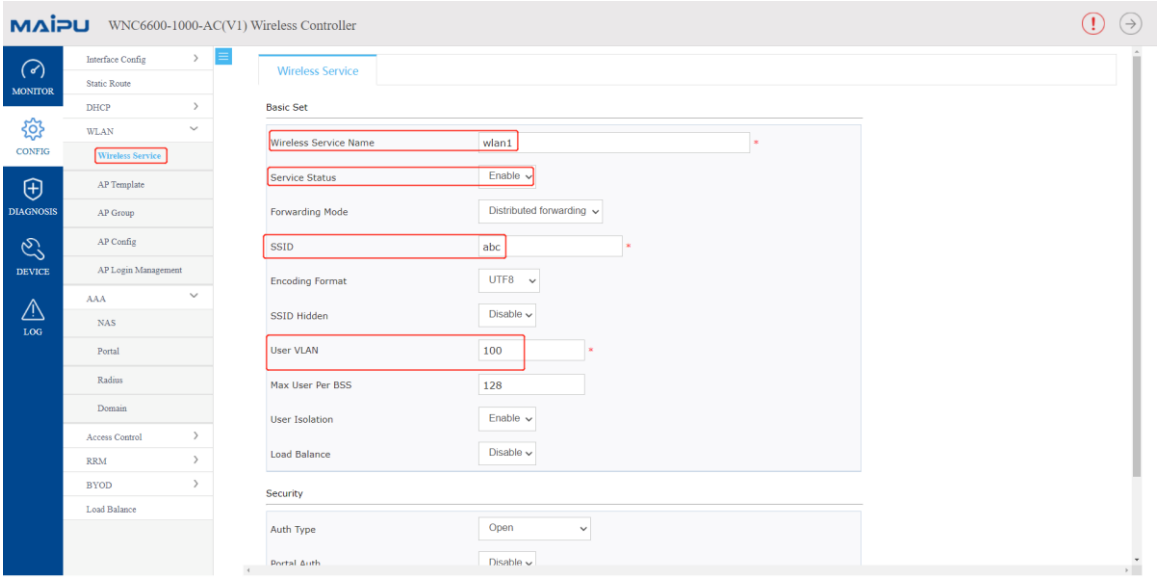


Figure 2.21 Wireless service configuration

copyright ©Maipu, all rights reserved

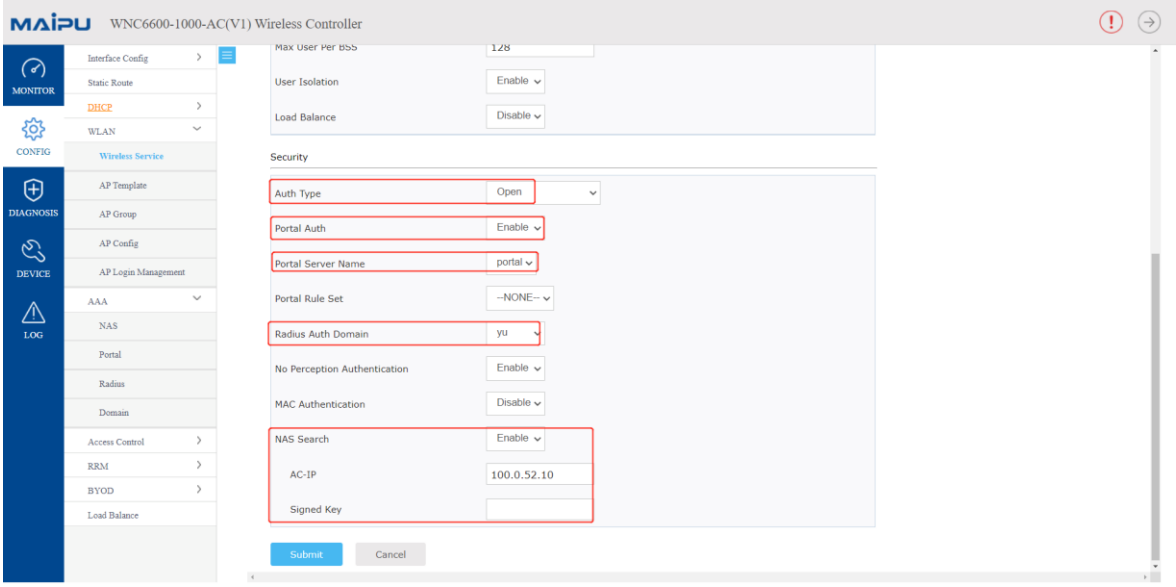


Figure2.22 Wireless service configuration

#Bind the wireless service set to the AP template. Click CONFIG > WLAN > AP Template, create an AP profile. By default, the name of the AP profile is Default_FitAP_Profile, which can be changed, after the creation is completed, the name cannot be changed. Create an AP profile and name it profile1, as shown in the figure below.

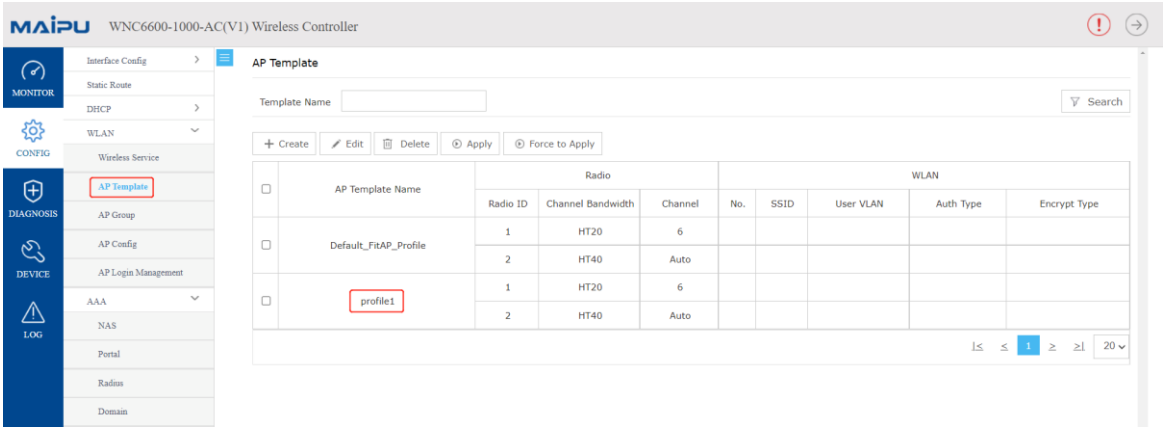


Figure 2.23 AP template

#Select the created AP template profile1, click the Edit button, click BSS > Wireless Service Name, select wlan1 created above, select ALL for Radio ID, and use default values for other configurations, click <OK> button to complete AP template configuration.

copyright ©Maipu, all rights reserved

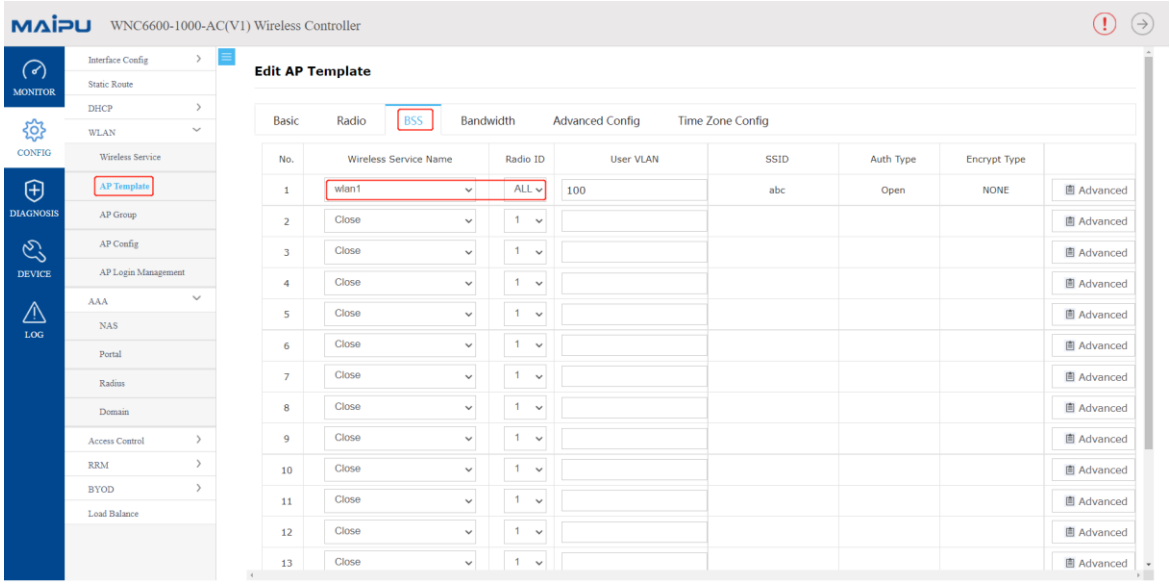


Figure 2.24 AP template BSS configuration

#AP template application. Click CONFIG > WLAN > AP Config, select the connected AP, select profile1 in the AP module, and then click Apply in the template application.

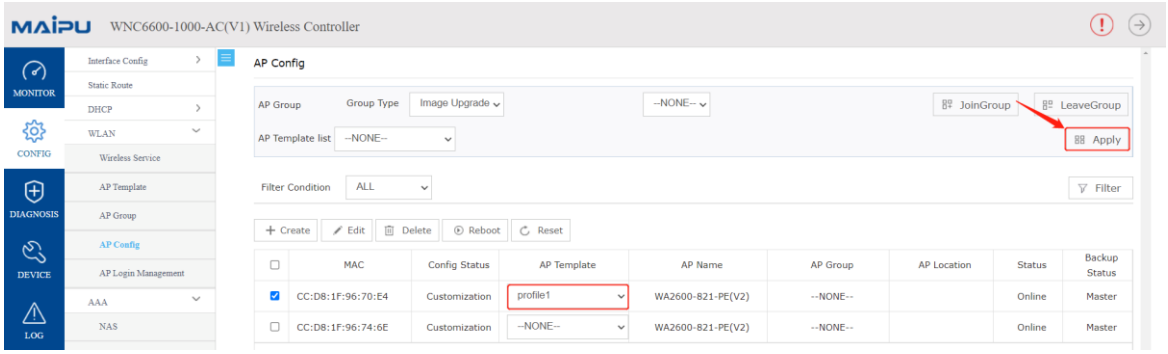


Figure 2.25 AP configuration

#Create an authentication account. Create an authentication account on the authentication server. The specific steps are omitted. For details, see 4.4 Add an Authentication User on Radius.

2.2.5 Result Verification

#Wireless terminal access, after applying the AP template, after two minutes, turn on the wifi of the wireless terminal, you can search for the wireless signal abc, and access it successfully.

1. If the uplink network and the DNS server 8.8.8.8 are interoperable (that is, the uplink network can already be connected to the external network), open the browser of the wireless terminal, access any website, and you will be redirected to the portal authentication page, after entering the account number and password created on the radius server, the authentication can be successful.

copyright ©Maipu, all rights reserved

2. If the uplink network is not connected to the DNS server 8.8.8.8, you can open the browser of the wireless terminal and manually enter http://2.3.4.5. If it is a V6 environment, manually enter http://[1::1], and you will be redirected to the portal authentication page, after entering the created account and password, the authentication is successful.

On the AC web page, click MONITOR > STA List, and you can see the information of wireless terminals.

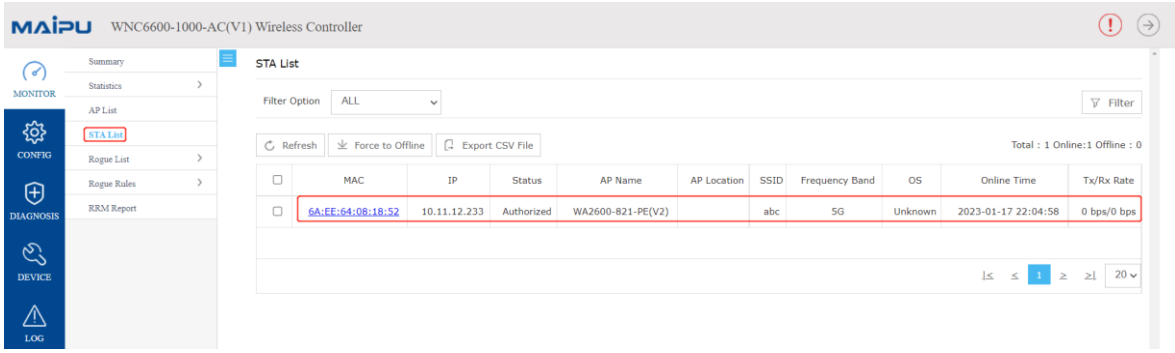


Figure 2.26 Terminal list

Note

- In addition to the BSS configuration, the AP template also needs to configure the working signal and channel bandwidth of the AP according to the actual network environment. The working channel of the2.4G radio frequency generally chooses1, 6, and11, and the channel bandwidth chooses HT20.
- The above example uses a dual-band AP as an example. Therefore, when configuring the BSS in the AP template, select all as the radio ID. For an AP that only supports2.4G radios, select1 as the radio ID.
- If the content platform is enabled on the authentication server, NAS information query needs to be enabled in the wireless service set configuration, and the AC IP parameter of NAS information query is configured as the NAS IP address.
- When performing portal redirection on a wireless terminal, it should be noted that the accessed website must use the http protocol.

copyright ©Maipu, all rights reserved

2.3 Centralized Forwarding-wpa2-enterprise Authentication Configuration Guide

2.3.1 Networking Requirements

The AC is connected to the L2 LAN through the bypass mode, the AP is powered by the POE switch, the AP and the wireless terminal obtain IP addresses through DHCP, and the AP provides a wireless network named "abc" and enabled with wpa2-enterprise authentication.

2.3.2 Network Topology

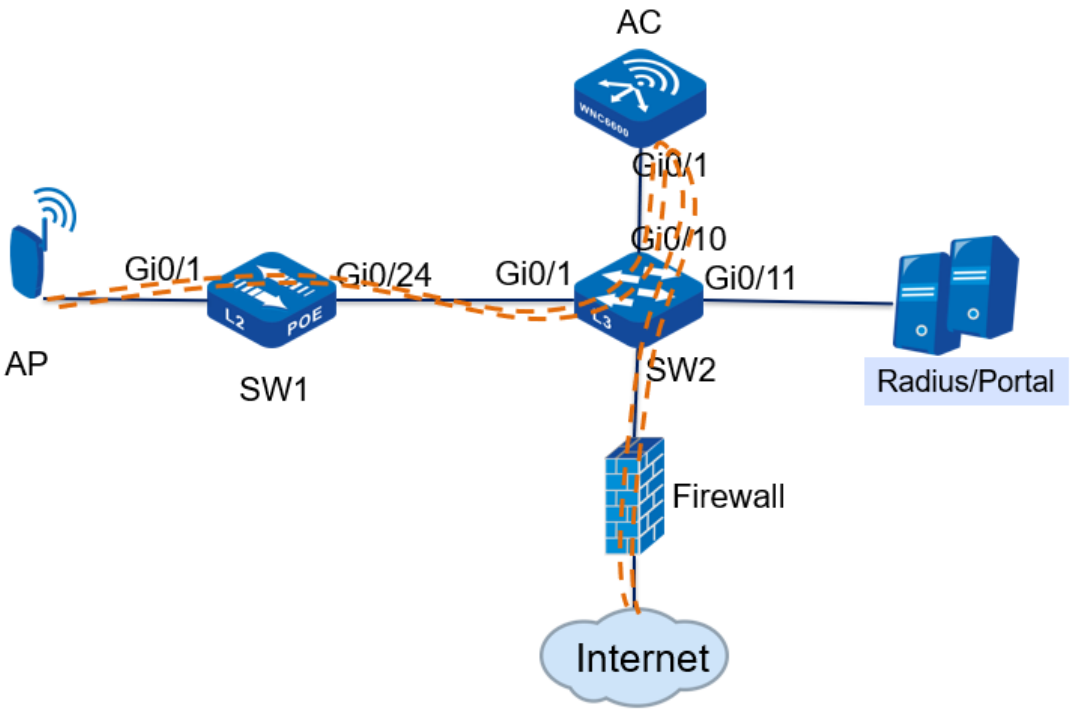


Figure 2.27 wpa2-enterprise authentication in centralized forwarding mode

Topology introduction:

Wi-Fi security	The authentication method is wpa2-enterprise, and the encryption type is AES
WLAN wireless service set	Wireless service set name: wlan1 SSID: abc Data forwarding mode: centralized forwarding
AP management VLAN	vlan10
AP service VLAN	vlan200
AP management IP address pool	192.168.10.10—192.168.10.100

copyright ©Maipu, all rights reserved

AP management gateway	192.168.10.254 (on the core switch)
User IP address pool	192.168.200.10—192.168.200.100
User gateway	192.168.200.254 (on the core switch)
DHCP server	The core switch acts as a DHCP server for APs and users
AAS server IP address	192.168.10.253

2.3.3 Configuration Ideas

1. Configure intermediate network device interfaces, including POE power supply switches and L3 core switches;
2. Configure DHCP server to provide IP address for AP;
3. Statically configure the IP address of the AC on the AP;
4. Configure an authentication server on the AC and bind the authentication domain;
5. Create a wireless service set on the AC, enable wpa2-enterprise authentication, and bind the authentication domain;
6. Create an AP template on the AC, bind the wireless service set and apply it to the AP;
7. Create an authenticated account and password on the AAS server;
8. The wireless terminal can successfully access the wireless network;

2.3.4 Configuration Steps

1. POE switch (SW1) configuration

#Create vlan10 and vlan200 on SW1, and configure the link type of gigabitethernet0/1 connected to the AP as Trunk, allowing vlan10 and vlan200 to pass through, and the PVID is10.

```
SW1#cont
SW1(config)#vlan10,200
Please wait.....
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/1
SW1(config-if-gigabitethernet0/1)# switchport mode trunk
SW1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,200
SW1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan10
SW1(config-if-gigabitethernet0/1)# exit
```

#Configure the link type of gigabitethernet0/24 connected to SW2 as Trunk, allowing vlan10 and vlan200 to pass through.

copyright ©Maipu, all rights reserved

```
SW1#cont
SW1(config)#interface gigabitethernet 0/24
SW1(config-if-gigabitethernet0/24)# switchport mode trunk
SW1(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW1(config-if-gigabitethernet0/24)# exit
```

2. Core switch (SW2) configuration

#Create vlan10, vlan200 and their corresponding vlan interface on SW2, and configure IP address for this interface, which will be used as the gateway between AP and wireless terminal.

```
SW2#cont
SW2(config)#vlan10,200
Please wait.....
Done.
SW2(config)#
SW2(config)#interface vlan10
SW2(config-if-vlan10)# ip address192.168.10.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan10)# exit
SW2(config)#
SW2(config)#interface vlan200
SW2(config-if-vlan200)# ip address192.168.200.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan200)#
```

#Configure the DHCP address pool ap-pool on SW2, dynamically allocate IP addresses for APs, and configure the gateway as192.168.10.254; configure the DHCP address pool sta-pool, dynamically allocate IP addresses for wireless terminals, and configure the gateway as192.168.100.254.

```
SW2#cont
SW2(config)#ip dhcp pool ap-pool
SW2(dhcp- config)# range192.168.10.10192.168.10.100255.255.255.0
SW2(dhcp- config)# default-router192.168.10.254
SW2(dhcp- config)# exit
SW2(config)#ip dhcp pool sta-pool
SW2(dhcp- config)# range192.168.200.10192.168.200.100255.255.255.0
SW2(dhcp- config)# default-router192.168.200.254
SW2(dhcp- config)# dns-server 8.8.8.8
SW2(dhcp- config)# exit
```

copyright ©Maipu, all rights reserved

#On SW2, configure the link type of gigabitethernet0/1 connected to SW1 as Trunk, allowing vlan10 and vlan200 to pass through; configure the link type of gigabitethernet0/10 connected to AC as Trunk, allowing vlan10 and vlan200 to pass through.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/1
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW2(config-if-gigabitethernet0/24)# exit
SW2(config)#interface gigabitethernet 0/10
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW2(config-if-gigabitethernet0/24)# exit
```

#Configure the interface connected to PC. On SW2, configure the link type of gigabitethernet0/20 as access and vlan as10. Connect the PC to port20 of the core switch SW2, and the PC can obtain the IP address.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/20
SW2(config-if-gigabitethernet0/20)# switchport mode access
SW2(config-if-gigabitethernet0/20)# switchport access vlan10
SW2(config-if-gigabitethernet0/20)# exit
```

3. AP configuration

#Connect the AP to the gigabitethernet0/1 port of the POE switch, the AP is powered normally, and check the IP address obtained by the AP on the core switch SW2.

```
SW2 #show ip dhcp pool ap-pool binding
Current DHCP binding information

Hardware-Address IP-Address Lease Status
0001.7a20.18401 92.1 68.10.101Day 05:58:44 ACKED

SW2 #
```

#Enter http://192.168.10.10 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

copyright ©Maipu, all rights reserved

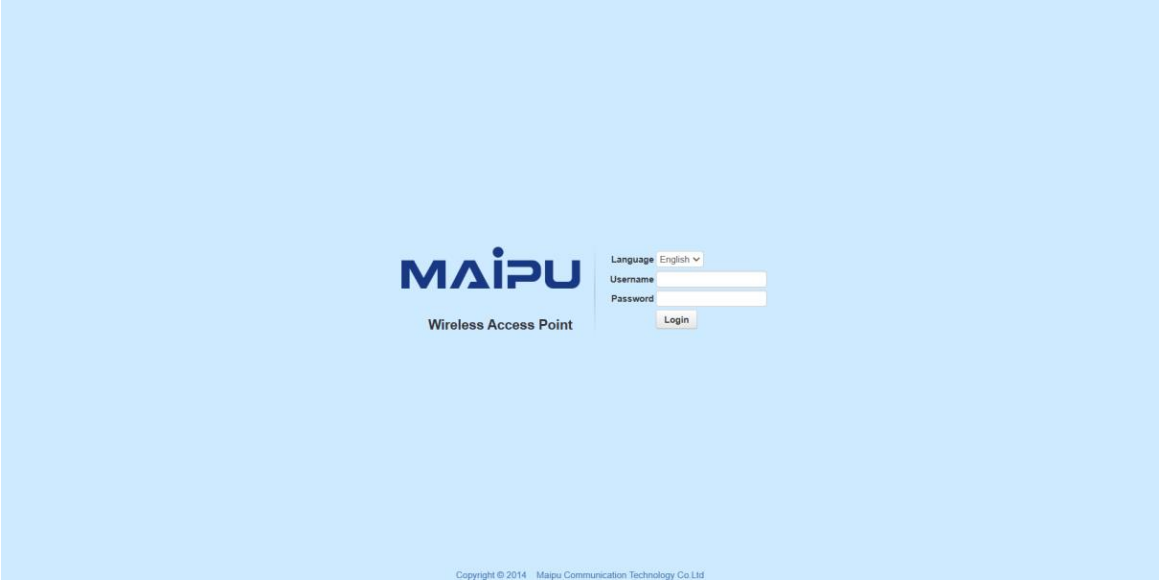


Figure 2.28 AP login page

#After entering the web management page of the AP, you will first enter the quick wizard configuration page. From step1 to step 3, you can directly use the default configuration. In step 4, configure the discovery method as static discovery, and configure the IPV4 address of the AC as192.168.10.1 Finally click the <Finish> button to complete the configuration, after the configuration is successful, it will jump to the system monitoring page.

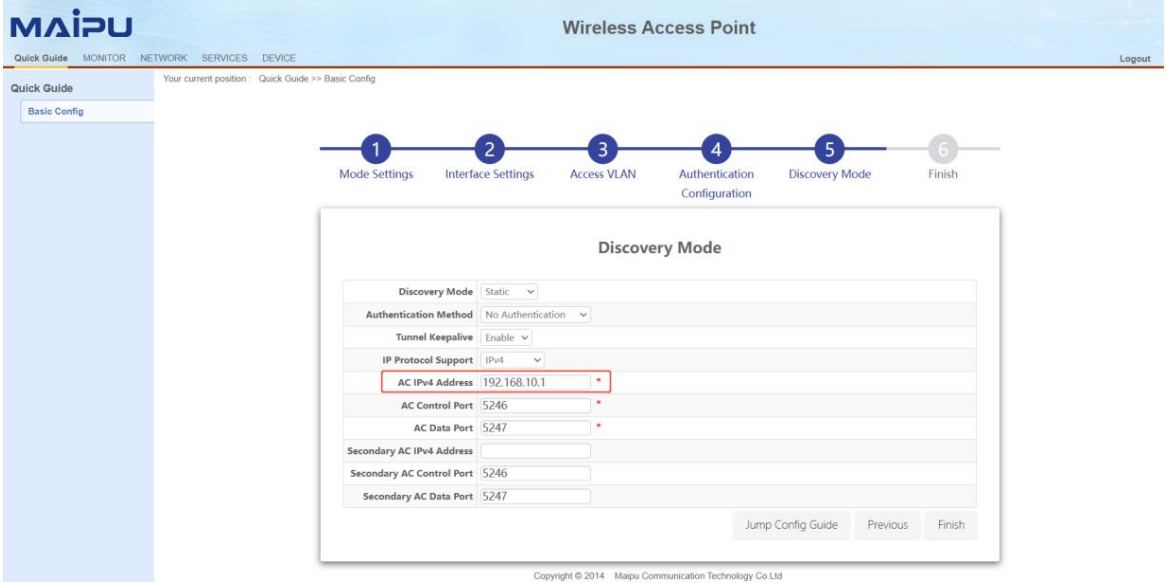


Figure 2.29 AP Configuration Wizard

4. AC configuration

#Create vlan10 and vlan200 on the AC, and create the corresponding vlan10 interface, which is used to establish a CAPWAP tunnel with the AP; configure the link type of gigabitethernet0/1 connected to SW2 as Trunk, allowing vlan10 and vlan200 to pass through.

AC # con t

AC(config)#vlan10,200

Please wait.....

copyright ©Maipu, all rights reserved

Done.

AC(config)#

AC(config)#interface vlan10

AC(config-if-vlan10)# ip address192.168.10.124

AC(config-if-vlan10)# exit

AC(config)#interface gigabitethernet 0/1

AC(config-if-gigabitethernet0/1)# switchport mode trunk

AC(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,200

#Configure VLAN200 on the AC to support centralized forwarding.

AC # con t

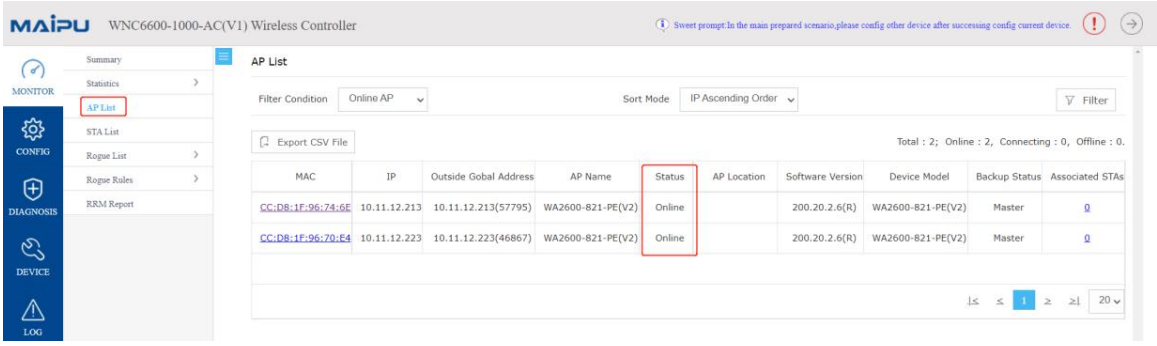
AC(config)#wireless vlan-list200

AC(config)# exit

#After completing the above configuration, wait for about two minutes, the AP can successfully connect to the AC, and you can view the status of the AP on the AC. Enter http://192.168.10.1 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in

Figure 2.30 AC login page

#Click MONITOR > AP List, and you can see that the AP is online, as shown in the figure below



copyright ©Maipu, all rights reserved

Figure 2.31 AP list

#Add NAS IP. Click CONFIG > AAA > NAS, select the IP address100.0.52.10, and click the <Add> button to set it as the NAS IP.

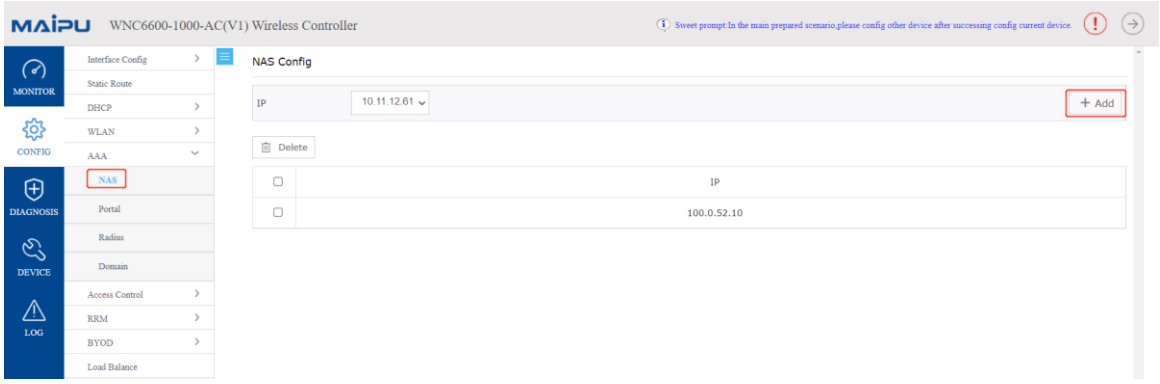


Figure 2.32 NAS configuration

#Configure authentication server. Click CONFIG > AAA > Radius > Authentication Server List, click <Create> to create a new authentication server, configure the server address as192.168.10.253, configure the RADIUS client, IP address as100.0.52.10, configure the pre-shared key as admin, and click <Add>, after performing the above configuration, click the OK button below to complete the configuration of the authentication server.

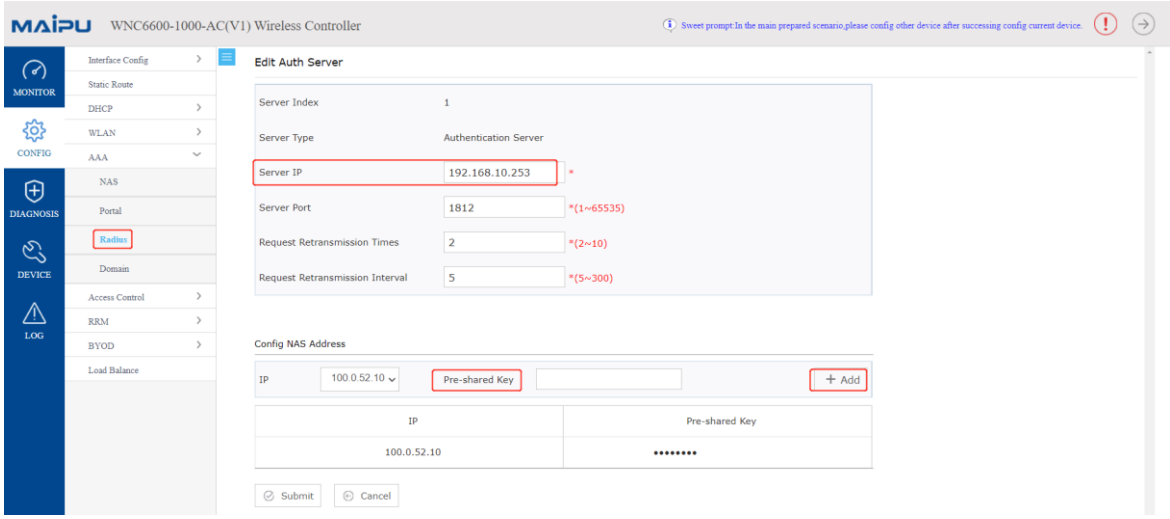


Figure 2.33 Authentication server configuration

#Domain configuration. Click CONFIG > AAA > Domain, click <Create> to create a new authentication domain, the domain name is the name of the authentication domain, here it is configured as yu, enable authentication service, the authentication server selects192.168.10.253, and click <Add>, after performing the above configuration, click the OK button below, and the configuration of the authentication domain is completed.

copyright ©Maipu, all rights reserved

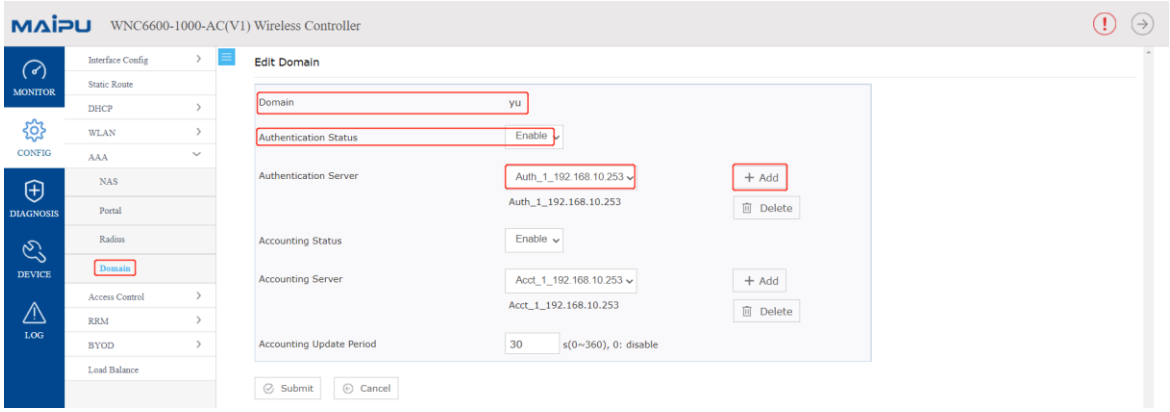


Figure 2.34 Domain Configuration

#Create a wireless service set. Click CONFIG > WLAN > Wireless Service to create a wireless service set, as shown in the figure below, the wireless name is wlan1, select "Enable" for service status, select "centralized forwarding" for forwarding mode, configure SSID as abc, configure user VLAN as100, select wpa2-enterprise for authentication mode, select yu for Radius authentication domain, and use the default values for other configurations. Click the <OK> button to complete the wireless service set configuration.

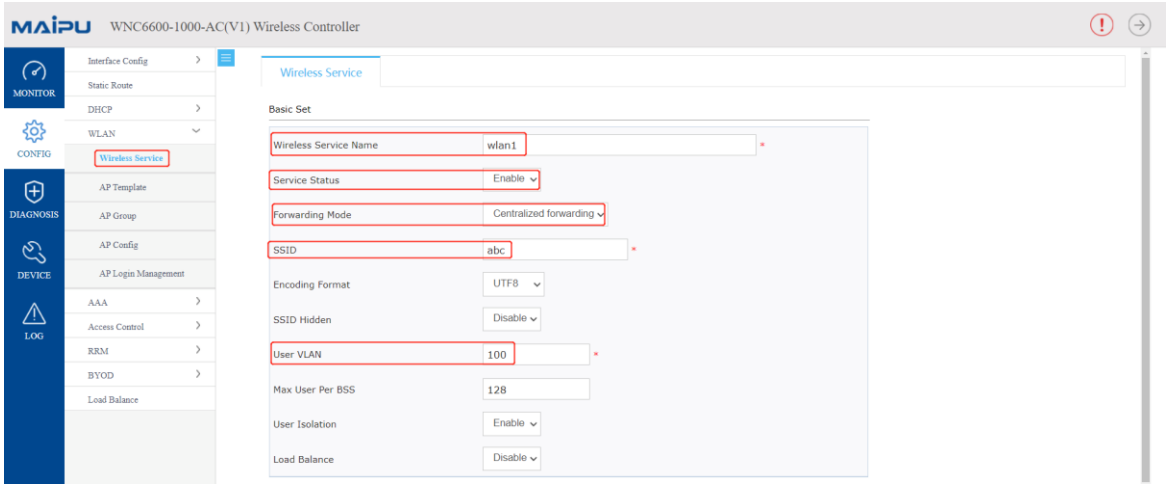


Figure 2.35 Wireless service configuration

copyright ©Maipu, all rights reserved

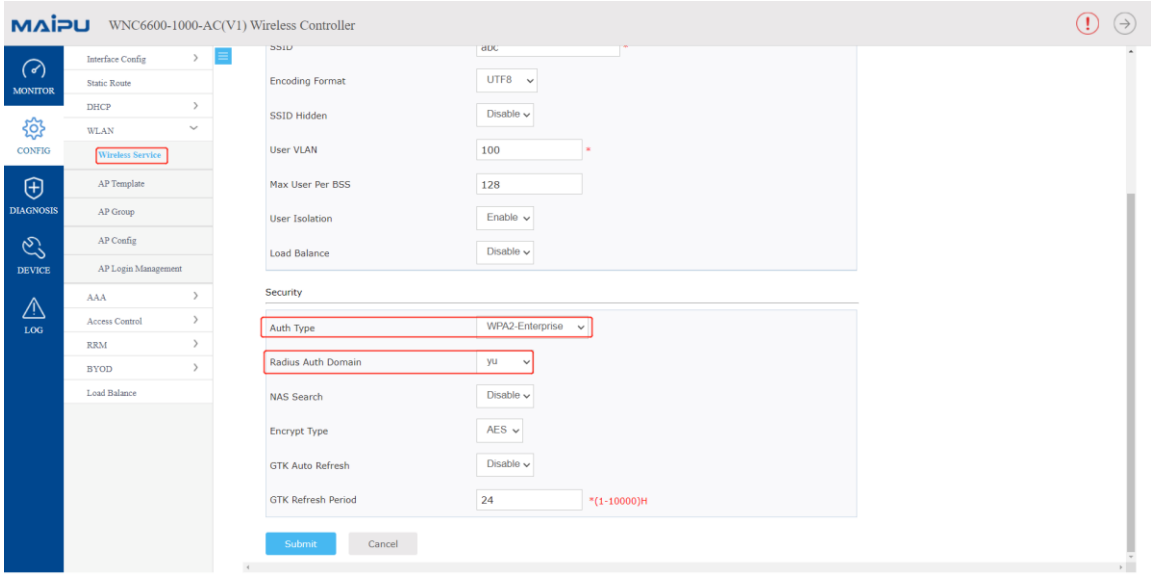


Figure 2.36 Wireless service configuration

#Bind the wireless service set to the AP template. Click CONFIG > WLAN > > AP template to create an AP profile, as shown in the figure below. By default, the name of the AP profile is Default_FitAP_Profile, which can be changed, and the name cannot be changed after creation.

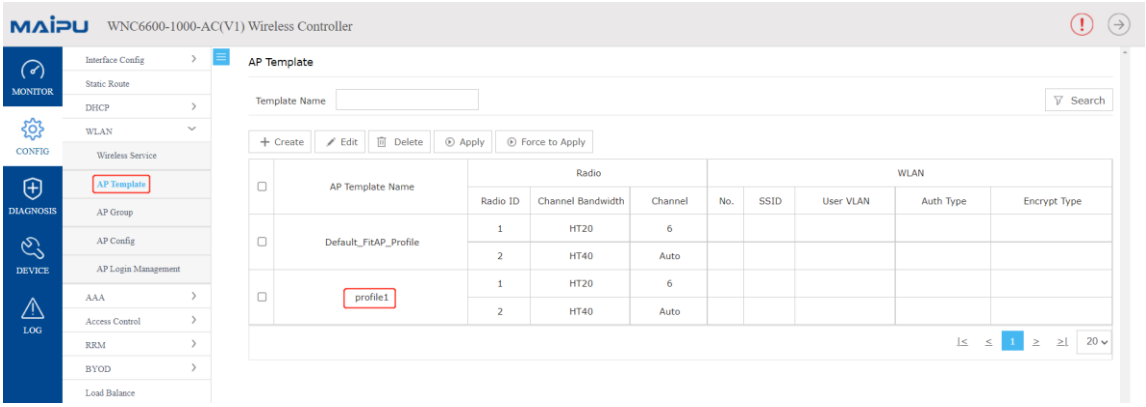
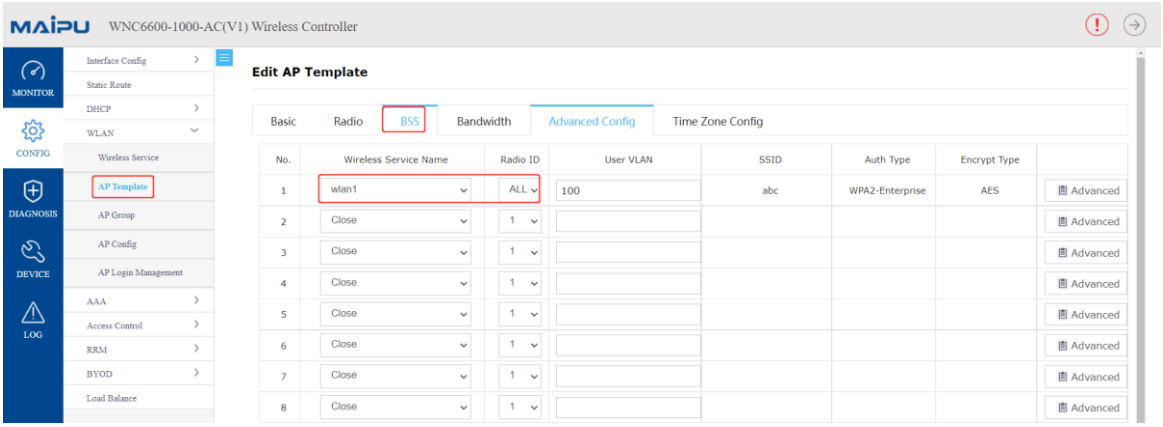


Figure 2.37 AP template

#Select the created AP template profile1, click the Edit button, click BSS > Wireless Service Name, select wlan1 created above, select ALL for Radio ID, and use default values for other configurations, click <OK> button to complete AP template configuration.



copyright ©Maipu, all rights reserved

Figure 2.38 AP template BSS configuration

#AP template application. Click CONFIG > WLAN > AP Config, select the connected AP, select profile1 in the AP module, and then click Apply in the template application.

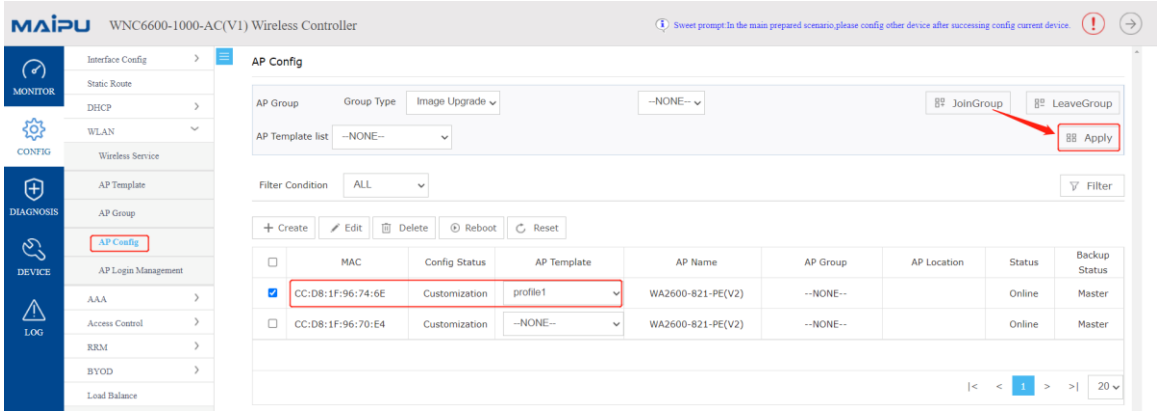


Figure 2.39 AP configuration

#Create an authentication account. Create an authentication account on the authentication server. The specific steps are omitted. For details, see 4.4 Add an Authentication User on Radius.

2.3.5 Result Verification

#Wireless terminal access, after applying the AP template, after two minutes, turn on the wifi of the wireless terminal, and you will be able to search for the wireless signal abc, and you can successfully access it after entering the user name and password. On the AC web page, click MONITOR > STA List, and you can see the information of wireless terminals.

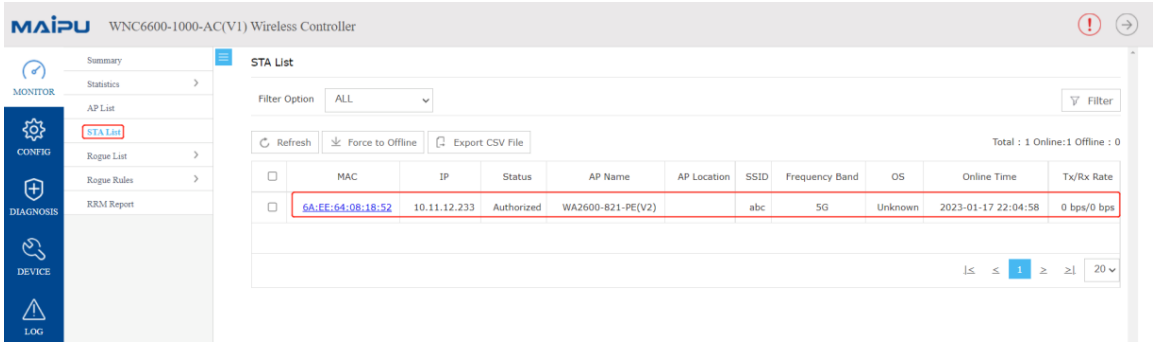


Figure 2.40 Terminal list

Note

- In addition to the BSS configuration, the AP template also needs to configure the working signal and channel bandwidth of the AP according to the actual network environment. The working channel of the2.4G radio frequency generally chooses1, 6, and11, and the channel bandwidth chooses HT20.

copyright ©Maipu, all rights reserved

- The above example uses a dual-band AP as an example. Therefore, when configuring the BSS in the AP template, select all as the radio ID. For an AP that only supports2.4G radios, select1 as the radio ID.

copyright ©Maipu, all rights reserved

3 AP and User Online Configuration

Taking local forwarding in a L3 network as an example, the common network diagram is shown in Figure 3.1.

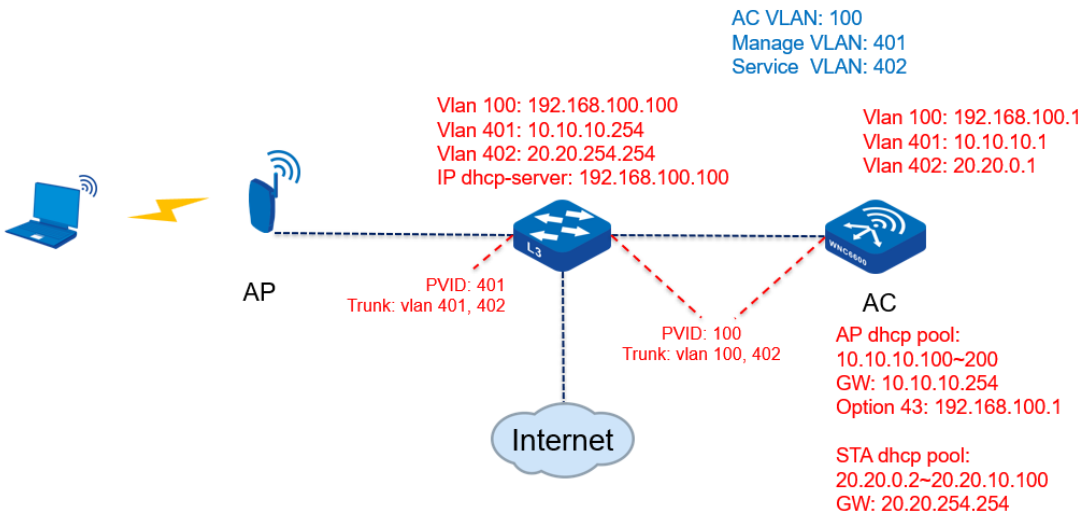


Figure 3.1 Network environment

3.1 VLAN and Interface Configuration

Configure the Vlan and the address of the Vlan interface to be used in the port configuration menu according to the network diagram, and configure the physical port corresponding to the AC, as shown in Figure 3.2.

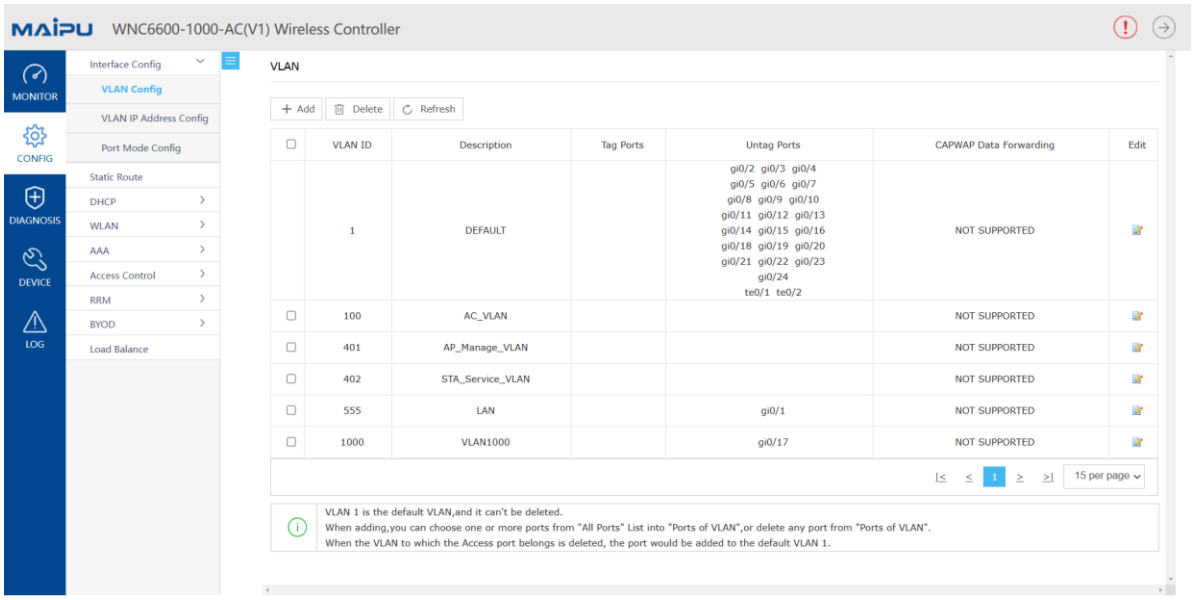


Figure 3.2 Configure vlan and interface address

copyright ©Maipu, all rights reserved

Note

- It should be noted here that if the AC is used as the user's DHCP server, the user VLAN must be configured as "support wireless service forwarding", as shown in 3.3.

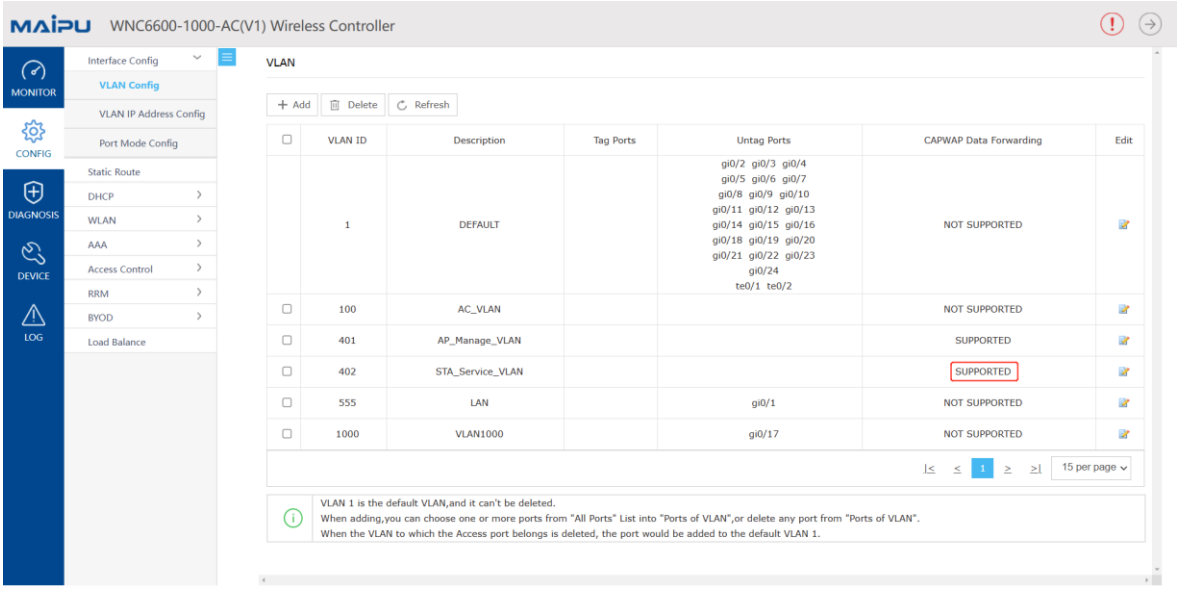


Figure 3.3 Support wireless service forwarding

In vlan address configuration, create a vlan and configure it, as shown in Figure 3.4 and 3.5.

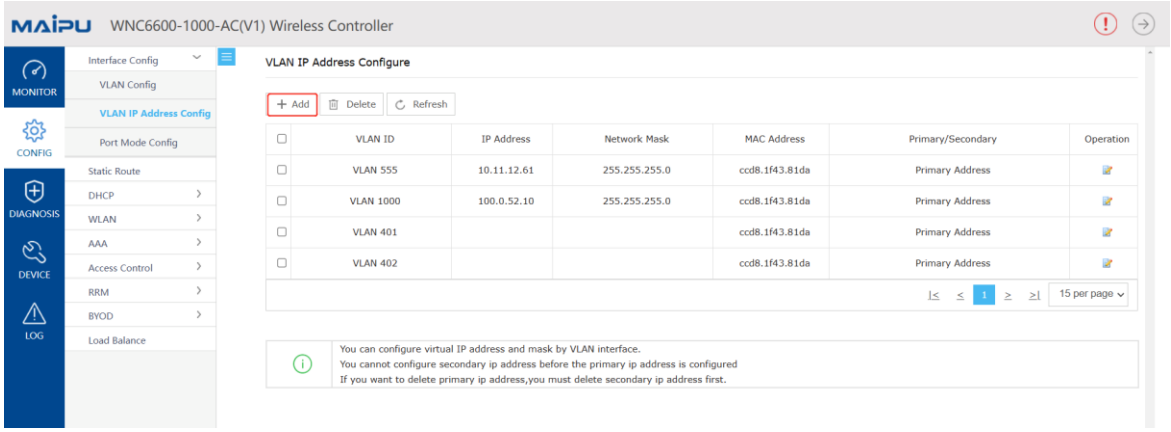
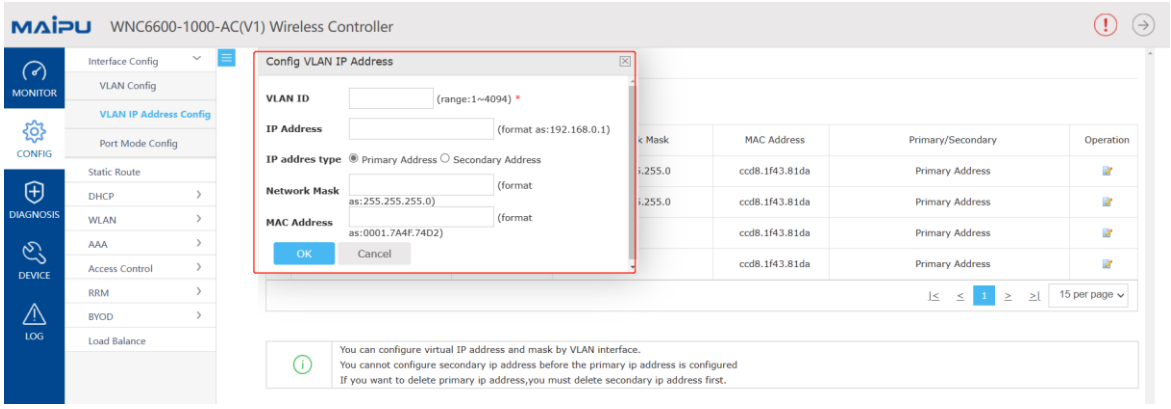


Figure 3.4 Create vlan



copyright ©Maipu, all rights reserved

Figure 3.5 Configure vlan

3.2 Route Configuration

If you need to add a route during the networking process, you can directly add it in the "Route" submenu, as shown in Figure 3.6.

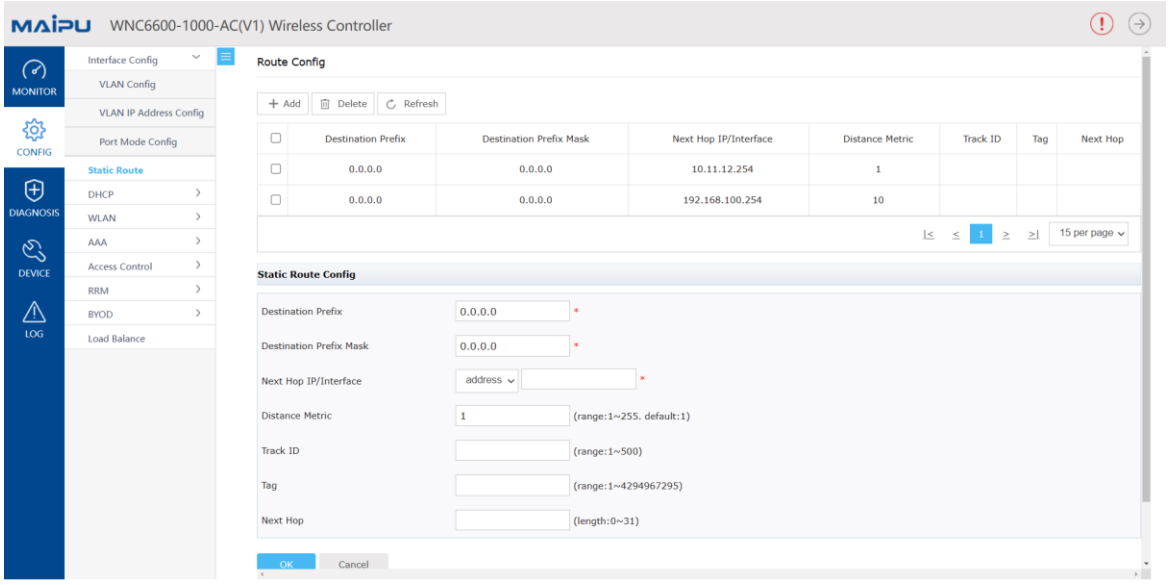


Figure 3.6 Add route

3.3 DHCP Configuration

Note

- AC can be used as a DHCP server (if you want to configure the unlimited enduance function of the AP, please do not use the AC as a DHCP server). Currently, the address pool supports three types: range, host, and network, which can be selected according to the networking requirements.

3.3.1 Configure AP Address Pool

Configure the AP address pool, as shown in Figure 3.7.

copyright ©Maipu, all rights reserved

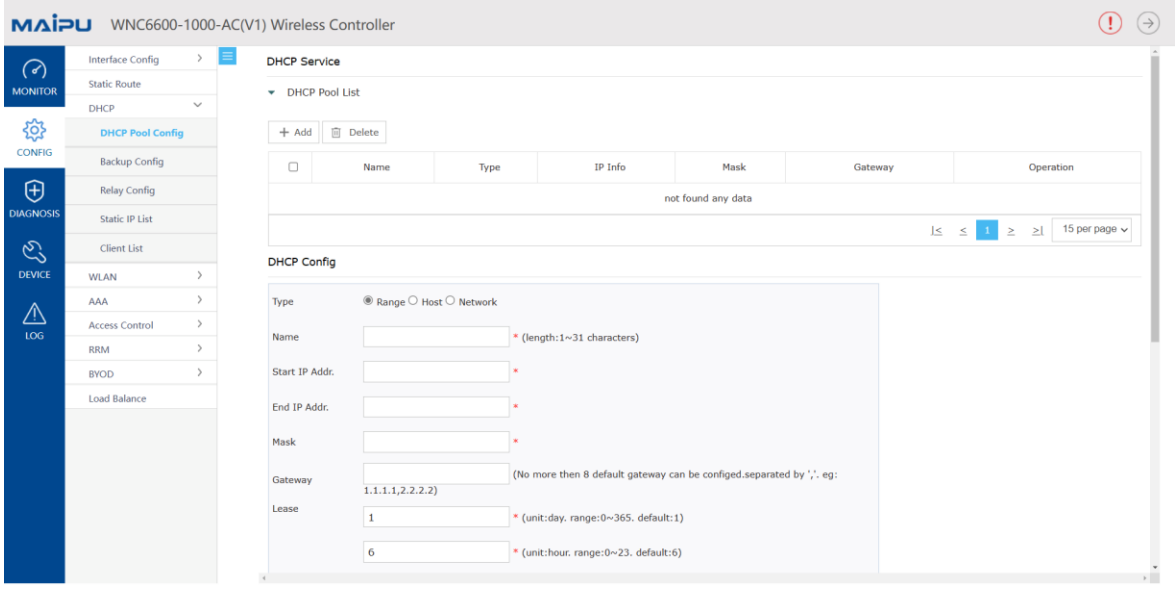


Figure 3.7 Configure AP address pool

Note

- If the AP goes online across the L3 network, you need to configure the Option 43 address (IP address of the AC), as shown in Figure 3.8.

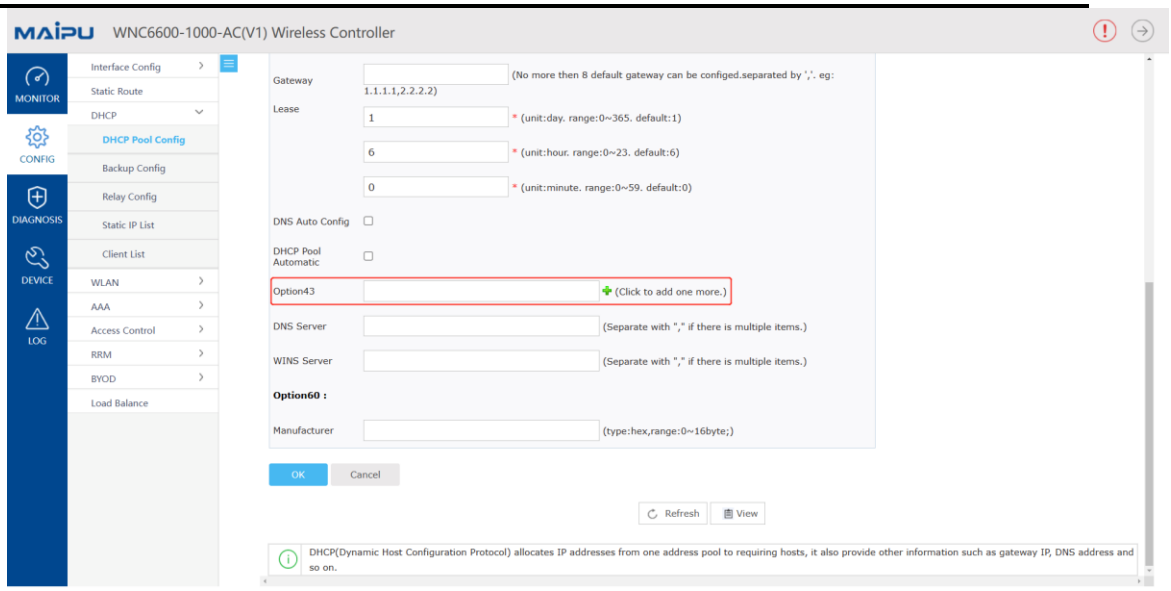


Figure 3.8 Configure option43 address

3.3.2 Configure STA Address Pool

The configuration of the STA address pool is the same as that of the AP address pool.

copyright ©Maipu, all rights reserved

3.4 Check Online Status of AP

Check the AP status on the WEB interface, as shown in Figure 3.9.

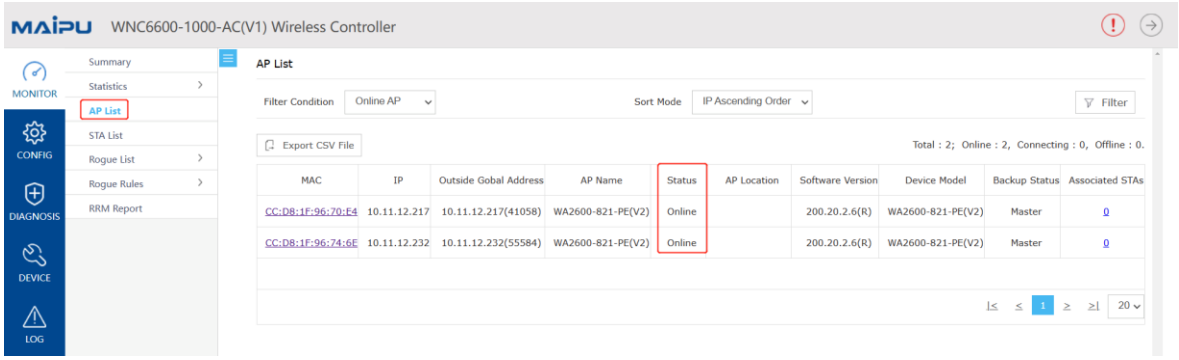
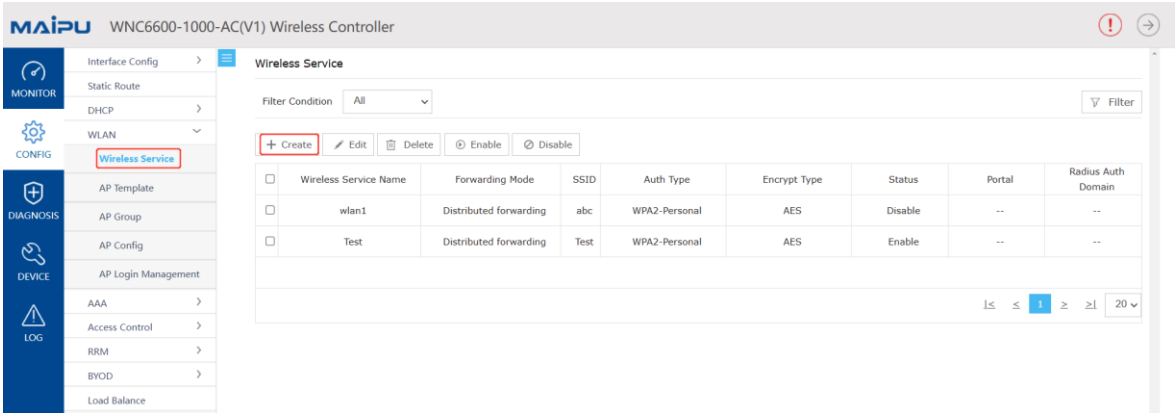


Figure 3.9 Check AP online status

Click the MAC address in the list to view more detailed AP information.

3.5 Wireless Service Set Configuration

Click "WLAN " in the "CONFIG" menu, select "Wireless Service " in the submenu to see the existing wireless services, and click "Create" at the top of the page to create a new wireless service, as shown in Figure 3.10.



copyright ©Maipu, all rights reserved

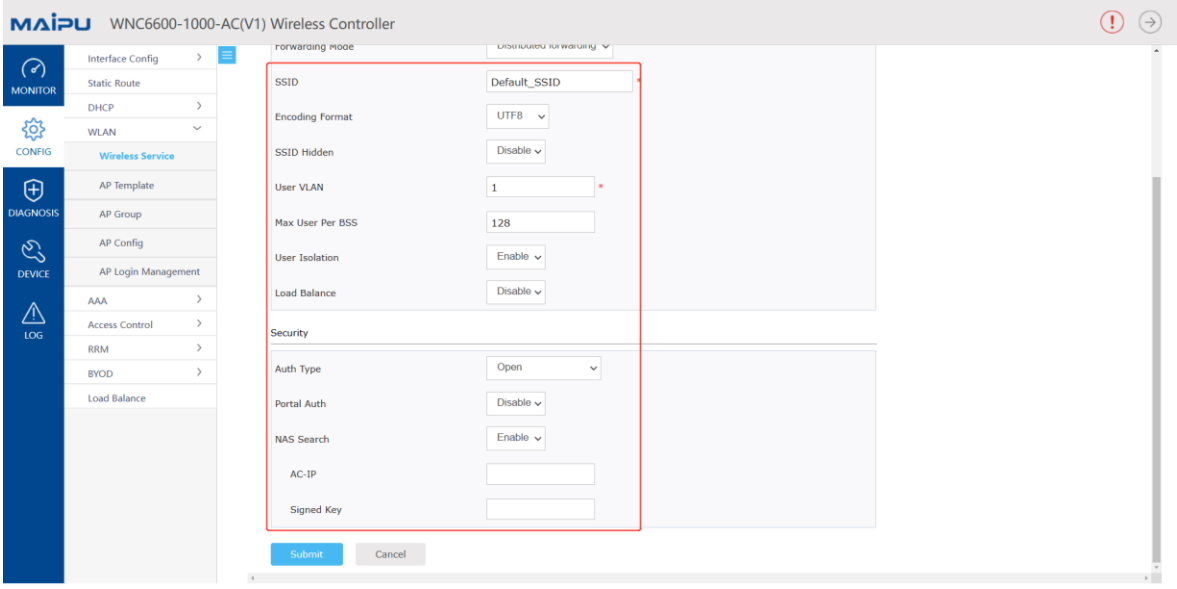


Figure 3.10 Create a wireless service set

Some functions of this page are introduced:

1. "Service Status": If this function is enabled, the wireless service will be enabled after it is created.
2. " SSID hidden": If this function is enabled, the user will not be able to search for the SSID, and can only connect through manual creation.
3. "User VLAN": User service VLAN.
4. " User Isolation": If this function is enabled, users under the same SSID cannot access each other (only users under the same SSID and the same AP can be isolated in the local forwarding network). If the customer has no special needs, please enable this function.
5. " Load balance ": If this function is enabled, when the wireless service is bound to multiple APs at the same time, according to the load of each AP, the user will be preferentially associated with the AP with a relatively small load.
6. " NAS Search": Please enable this function when connecting to content platforms or when you need to use X-MASTER APP.
7. "AC-IP": This address is the IP address on the AC communicating with the AP (the original ac source ip under wireless).
8. " Signed key": used by nasgetinfo, two parameters of time stamp and md5 signature are added in the return value of NAS information query. The md5 calculation parameters are: existing push parameters + time stamp + pre-shared key generation, and the pre-shared key used for NAS query uses the signature password in the NAS information query of the wireless service set.

copyright ©Maipu, all rights reserved

3.6 AP Template Configuration and Distribution

If no AP profile is created, the default profile "Default_FitAP_Profile" carried by the system can be used. On this page, you can directly choose to edit the existing default template or create a new template. Create a template named profile1 as shown in Figure 3.12.

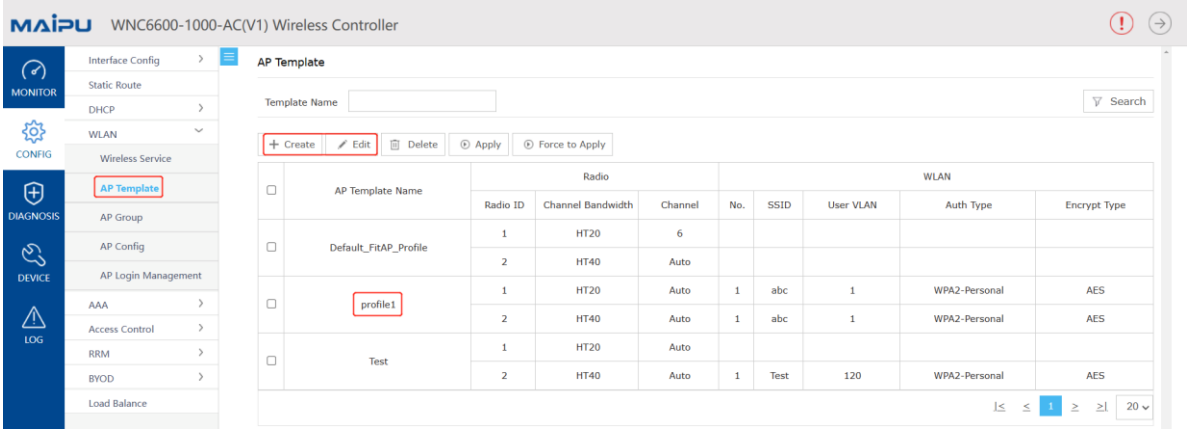


Figure 3.12 Create an AP template

3.6.1 Create an AP Template

1. Basic configuration

Figure 3.13 shows the basic configuration of an AP template.

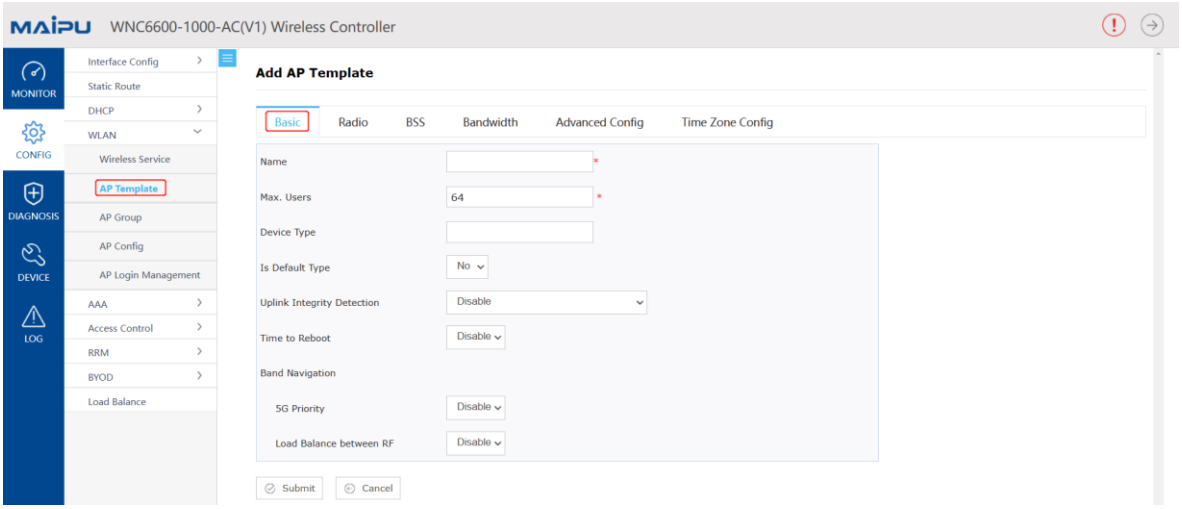


Figure 3.13 Basic configuration of AP template

Some functions of this page are introduced:

A. "Max. Users": This function indicates that the number of wireless terminals that can be accessed by the AP using this template can be limited.

B. "Uplink Integrity Detection": When the AP detects that the AC link is disconnected, handle it according to the configured link detection policy. The current uplink detection methods

copyright ©Maipu, all rights reserved

include: AP uplink physical link detection, AC/AP CAPWAP link detection; when a link abnormality is detected, the processing actions include: turn off RF and restart the AP.

C. "Band Navigation ": This function consists of two sub-functions, one is the navigation function (ie, 5G priority), and the other is the balancing function (ie, load balancing between RF).

D. "5G Priority": If this function is enabled, the AP will guide dual-band wireless terminals to connect to the 5G SSID first.

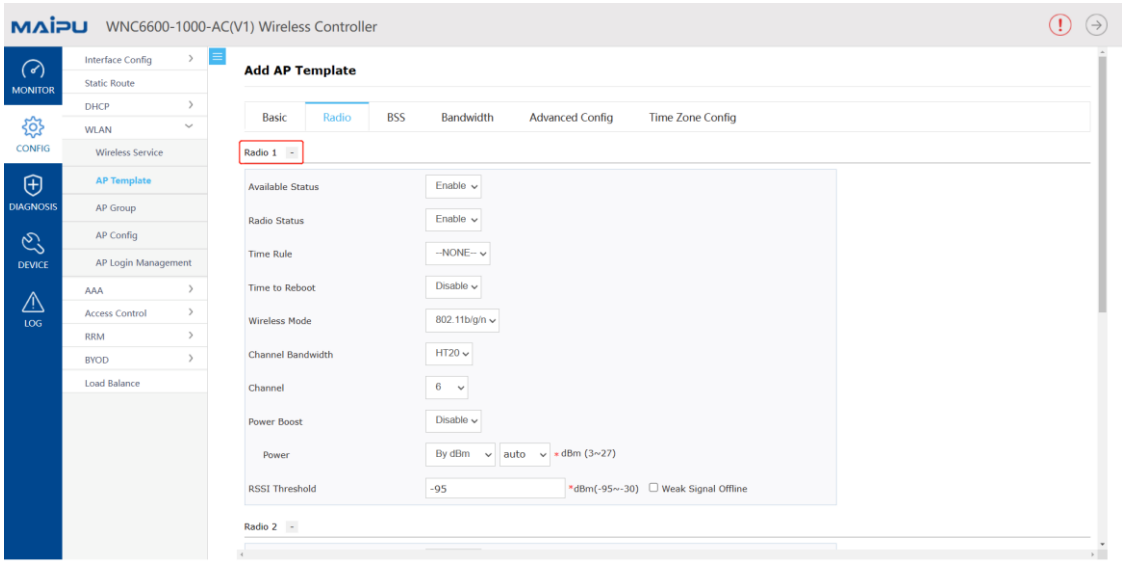
E. "Load balancing between RF": If this function is enabled, the AP will balance the number of STAs associated with2.4G and 5G radios.

Note

- It should be noted on this page that if you want to use the new AP template as the default template (that is, the template will be automatically loaded when the zero-configuration AP goes online), you must fill in the AP device type (the AP device type can be queried in the AP information). For example, If the device type is configured as "WA2600-830-PTE(V2)", all zero-configuration APs of the WA2600-830-PTE(V2) model will automatically load this template when they go online

2. RF configuration

By default, Radio1 is 2.4GHz and Radio2 is 5.2GHz, as shown in Figure 3.14.



copyright ©Maipu, all rights reserved

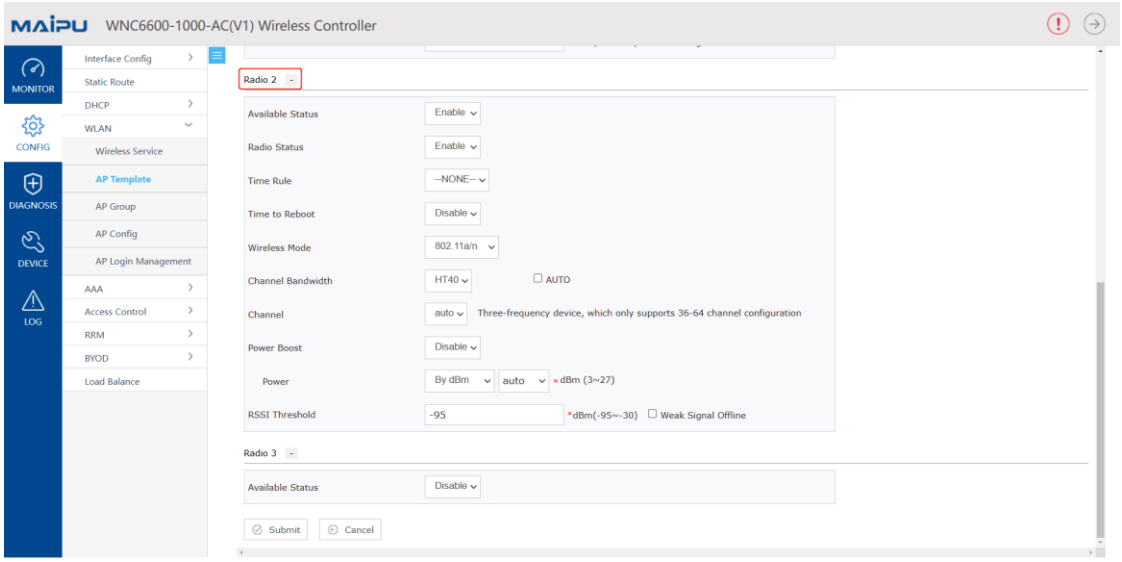


Figure 3.14 RF configuration

Some functions of the RF configuration page are introduced:

A. "Channel": When deploying APs in a large area, please try to ensure the use of1, 6, and11 channels for2.4G.

B. "RSSI Threshold": Users whose signal strength is lower than this threshold cannot access (please modify this value carefully).

The time policy can be bound in the RF timing policy, where the time policy is configured in the "Time Rules" in the "Access Control", as shown in Figure 3.15

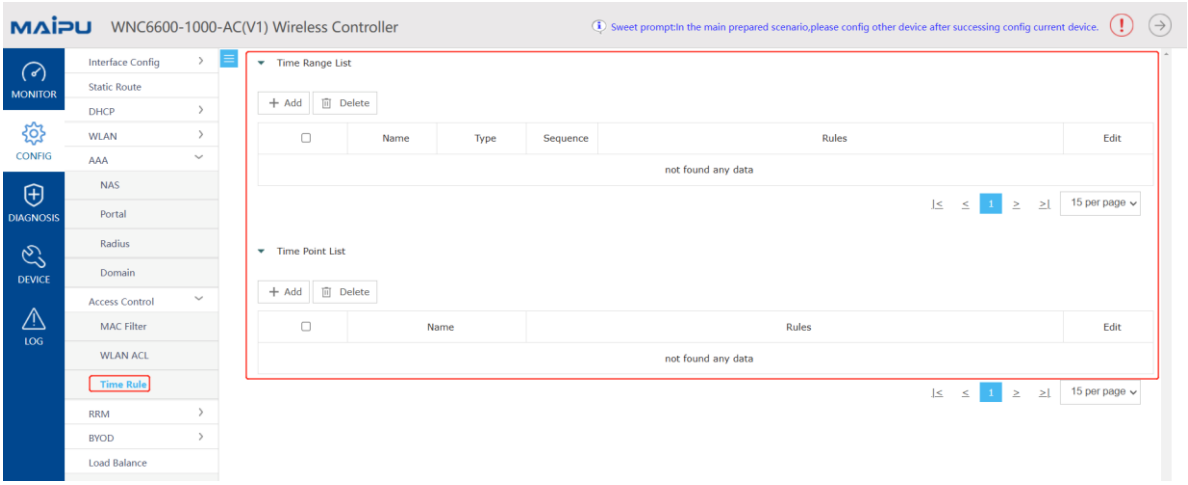


Figure 3.15 Timing policy

Note

- The forced rate in a/b/g mode must be configured with a value, and the forced rate in n/11ac mode is not configured by default;
- The supported rate of the a/b/g mode cannot be configured repeatedly with the

copyright ©Maipu, all rights reserved

mandatory rate;

- The supported rate of the n mode **mcs num** must be greater than or equal to mandatory rate **mcs num**;
- The supported rate of11ac mode **nss num** must be greater than or equal to the mandatory rate **nss num**. If the nss is the same, the supported rate **mcs num** must be greater than or equal to the mandatory rate **mcs num**;
- When the a/b/g multicast rate is auto, the AP selects the largest value in the mandatory rate set, and the multicast rate range must be selected in the mandatory rate set;
- The n/11ac multicast rate is disabled by default. If selected, its range must be within the range of the mandatory rate set;
- Management frame rate and Beacon frame rate must be selected within the mandatory rate set.
- If there is no special requirement, it is recommended to use the default value for the configuration of the wireless rate set.

3.BSS configuration

Bind the SSID in the AP template. Dual-band devices have Radio1 (2.4GHz) and Radio2 (5.2GHz) frequency bands. Tri-band devices have Radio1 (2.4GHz) and Radio2 (5.2GHz) frequency bands, and Radio3 (5.8GHz) frequency bands. Select the corresponding working frequency band according to actual needs. If all frequency bands are required, please select "ALL" in the Radio ID, as shown in Figure 3.16.

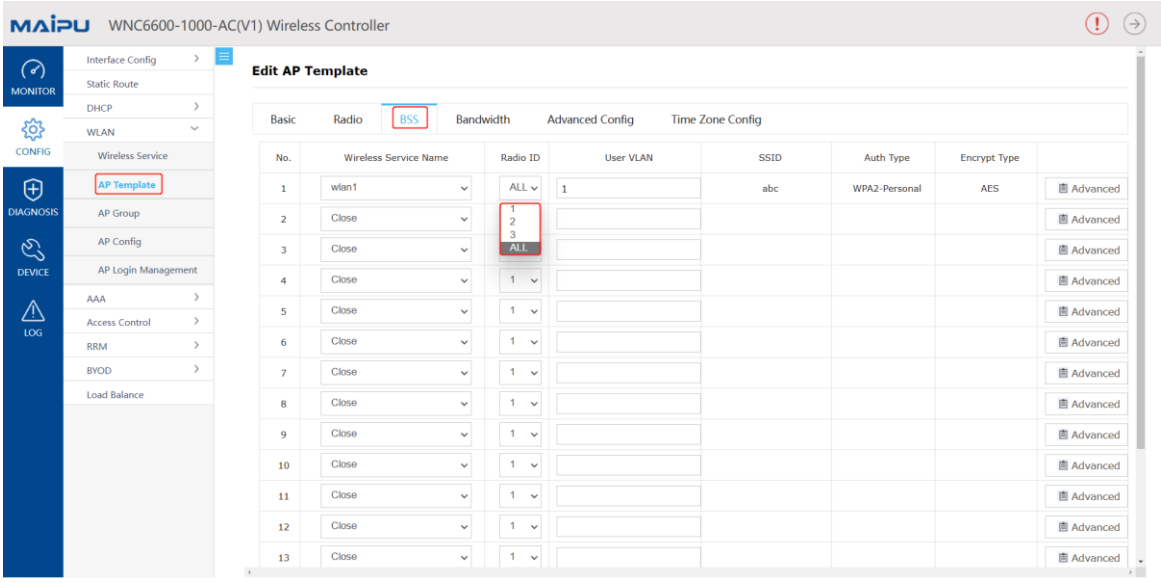


Figure 3.16 BSS configuration

copyright ©Maipu, all rights reserved

BSS can also perform customized configuration of "timing policy", "wireless access control", and "enable SAVI" functions. Click the " Advanced" button behind the row of the bound wireless service level to enter the custom configuration page, as shown in Figure 3.17 and 3.18.

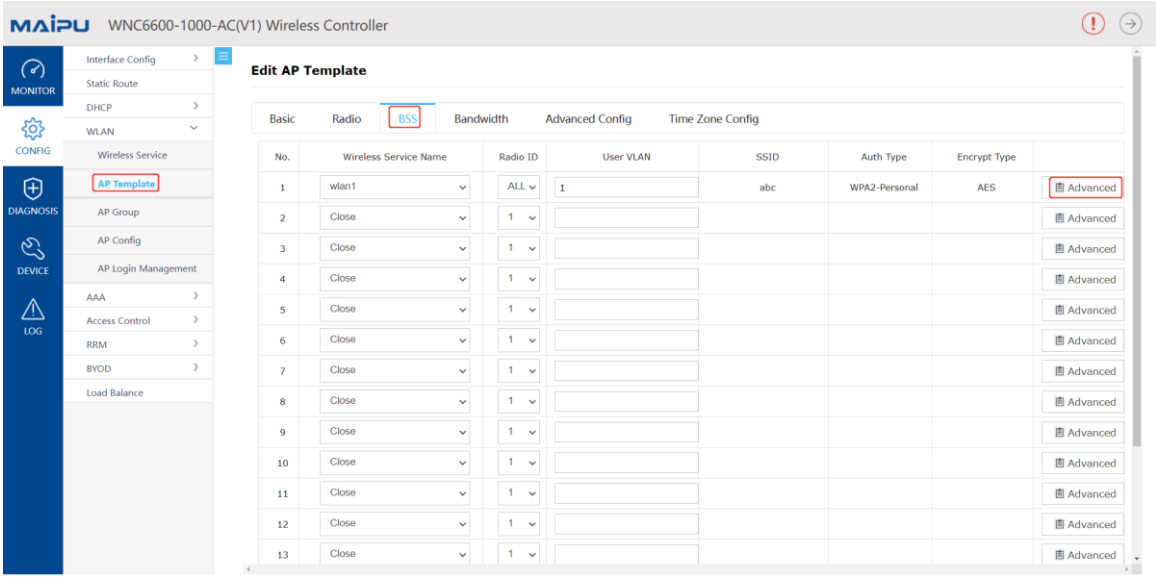


Figure 3.17 Edit BSS

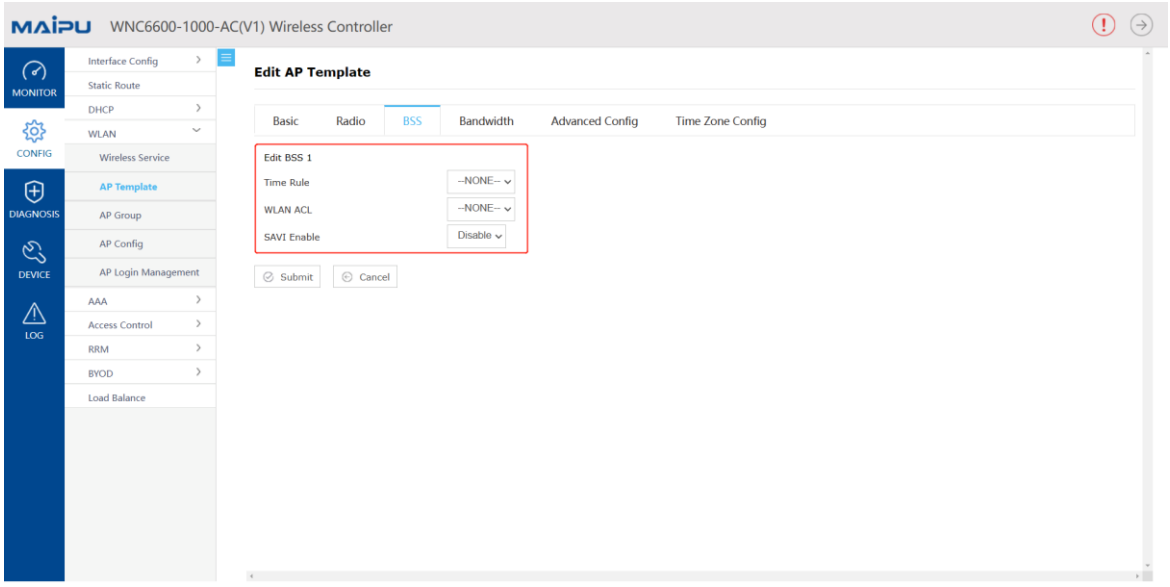


Figure 3.18 Customized configuration of BSS

Some functions and precautions:

A. "SAVI Enable": When this function is enabled, users will not be able to configure static IP privately.

B. "WLAN ACL": Only AP ACL can be bound here, please create before binding. Click CONFIG > Access Control > WLAN ACL, fill in the policy set name and select the policy set type,and click Add button to complete this configuration, as shown in Figure 3.19.

copyright ©Maipu, all rights reserved

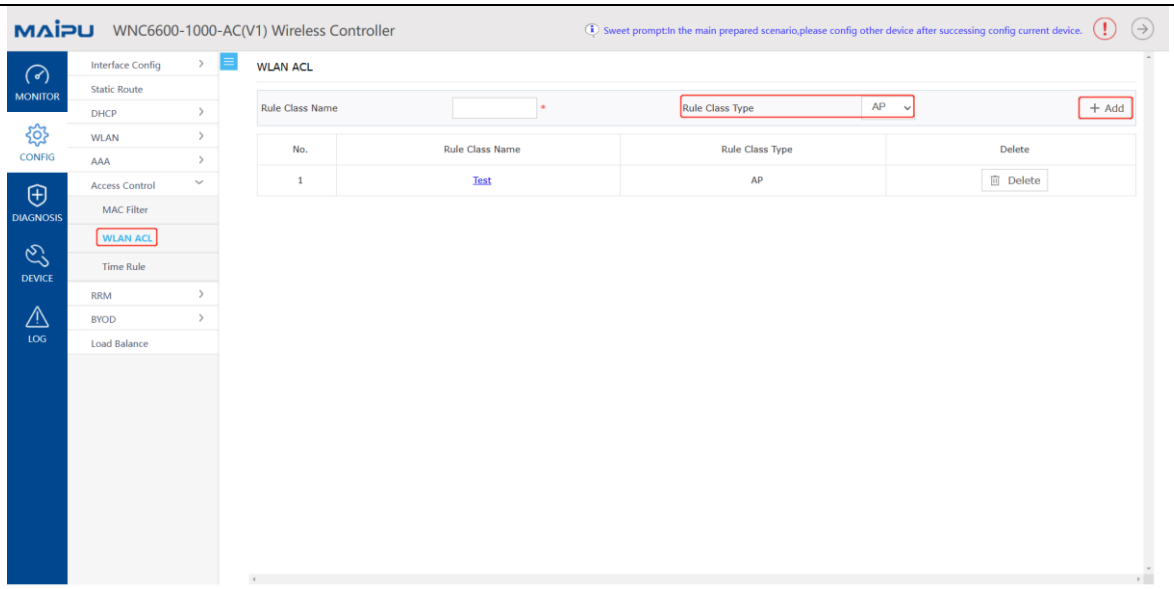


Figure 3.19 Create AP ACL

Click the created policy set name to edit the policy set, as shown in Figure 3.20.

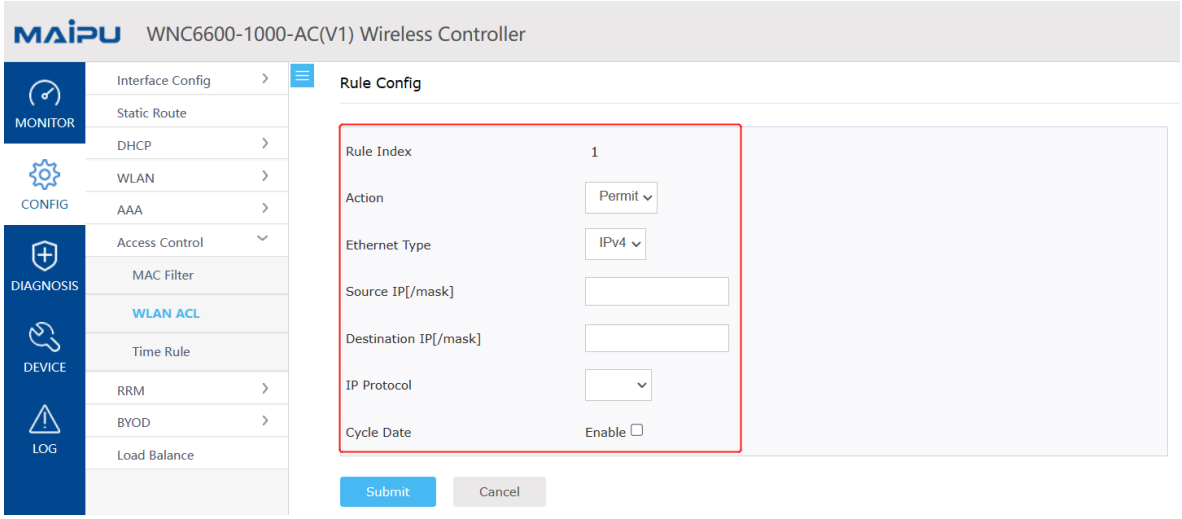
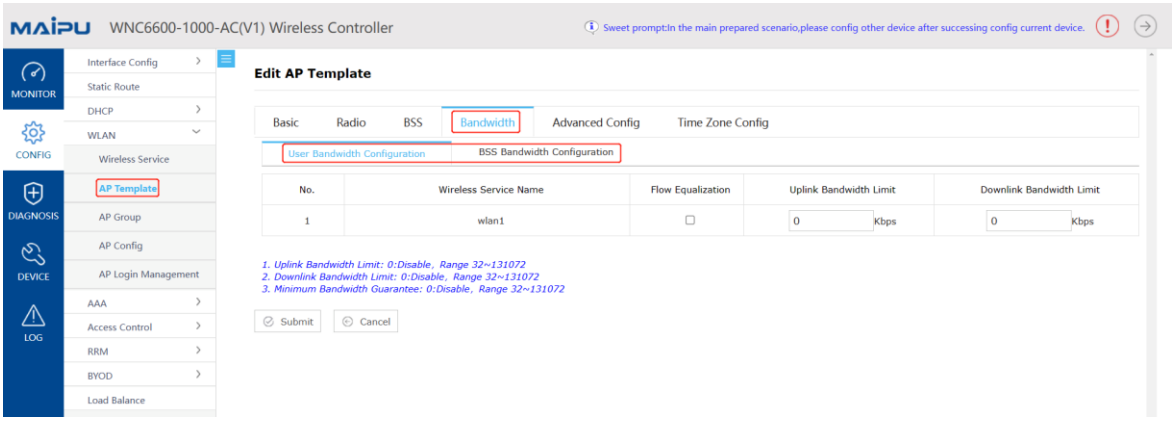


Figure 3.20 Configure Policy Set

4. Bandwidth configuration

Bandwidth configuration supports bandwidth configuration for users and BSS and intelligent equalization of user bandwidth, as shown in Figure 3.21.



copyright ©Maipu, all rights reserved

Figure 3.21 Bandwidth configuration

A. "User bandwidth configuration": Specifies the bandwidth limit of a single user under the wireless service, and equally share the bandwidth of multiple access users;

B. "BSS Bandwidth Configuration": Specifies the total bandwidth of the wireless service.

Note

- The sum of user bandwidth and BSS bandwidth limits cannot exceed the total AP bandwidth limit

5, advanced configuration

The advanced configuration in the AP template is shown in Figure 3.22.

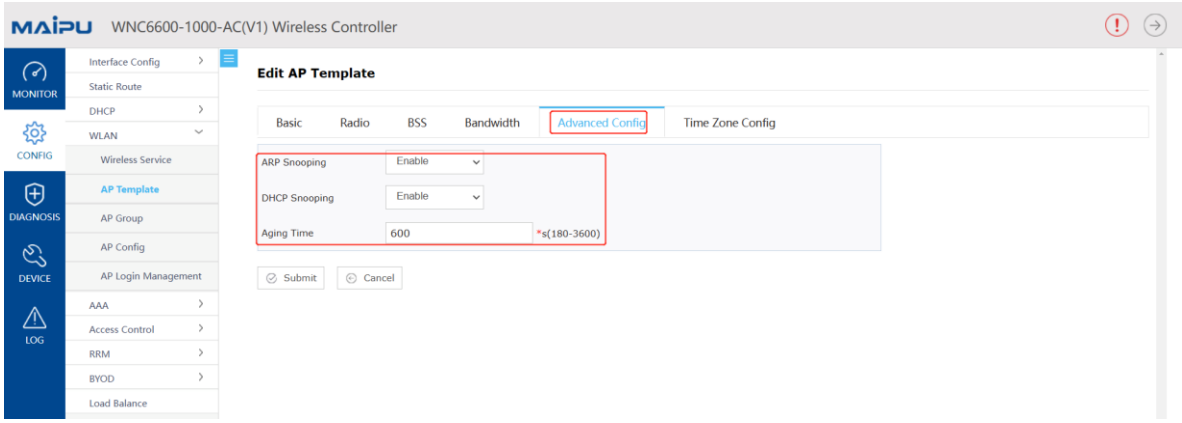


Figure 3.22 Advanced configuration

A. "ARP broadcast to unicast": If this function is enabled, all ARP broadcast packets from AP to STA will be converted to unicast.

B. "DHCP broadcast to unicast": If this function is enabled, all DHCP broadcast packets from AP to STA will be converted to unicast.

C. "Aging Time": The aging time of broadcast-to-unicast data entries on the AP.

6. Time zone setting

Figure 3.23 shows the time zone settings in the AP template.

copyright ©Maipu, all rights reserved

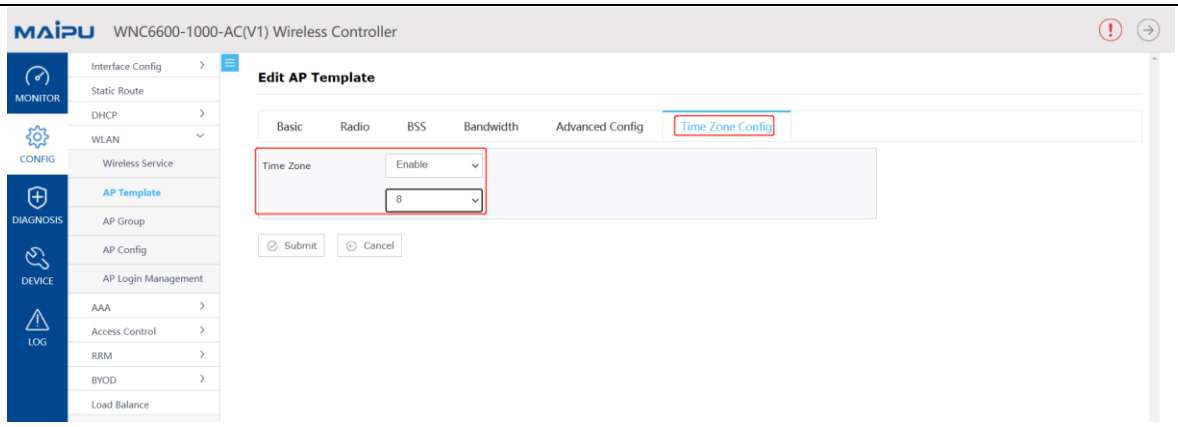


Figure 3.23 Advanced configuration

A. "Time Zone ": If this function is turned on, it can be set according to the time zone corresponding to the current country.

3.6.2 AP Template Delivery

Click CONFIG > WLAN > AP Config, check the AP that needs to deliver configuration (single selection or multiple selection), select the template in the AP template list menu, and click the Apply button on the right to complete the delivery of the template configuration, as shown in Figure 3.24.

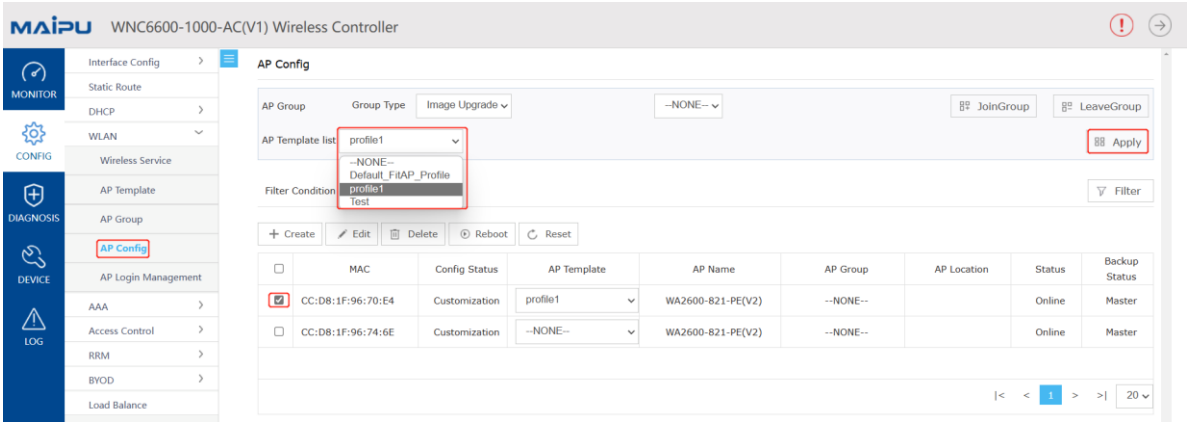


Figure 3.24 AP template delivery

3.6.3 Customize AP Configuration

In addition to delivering a unified template to APs, customized configurations can also be performed for a single AP.

Perform the customized configuration for the AP directly in the "AP Config" submenu, select the AP to be customized, and click "Edit", as shown in Figure 3.25 and 3.26.

copyright ©Maipu, all rights reserved

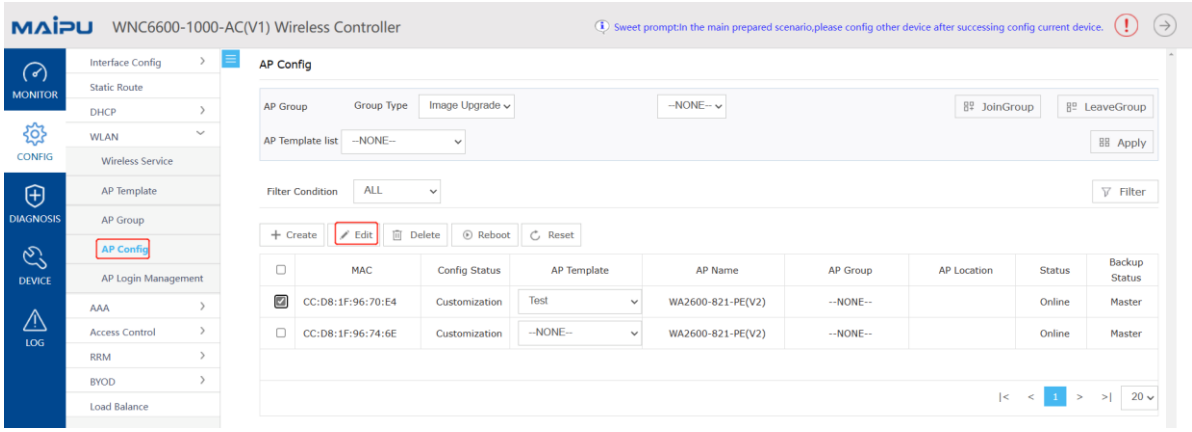


Figure 3.25 Select AP

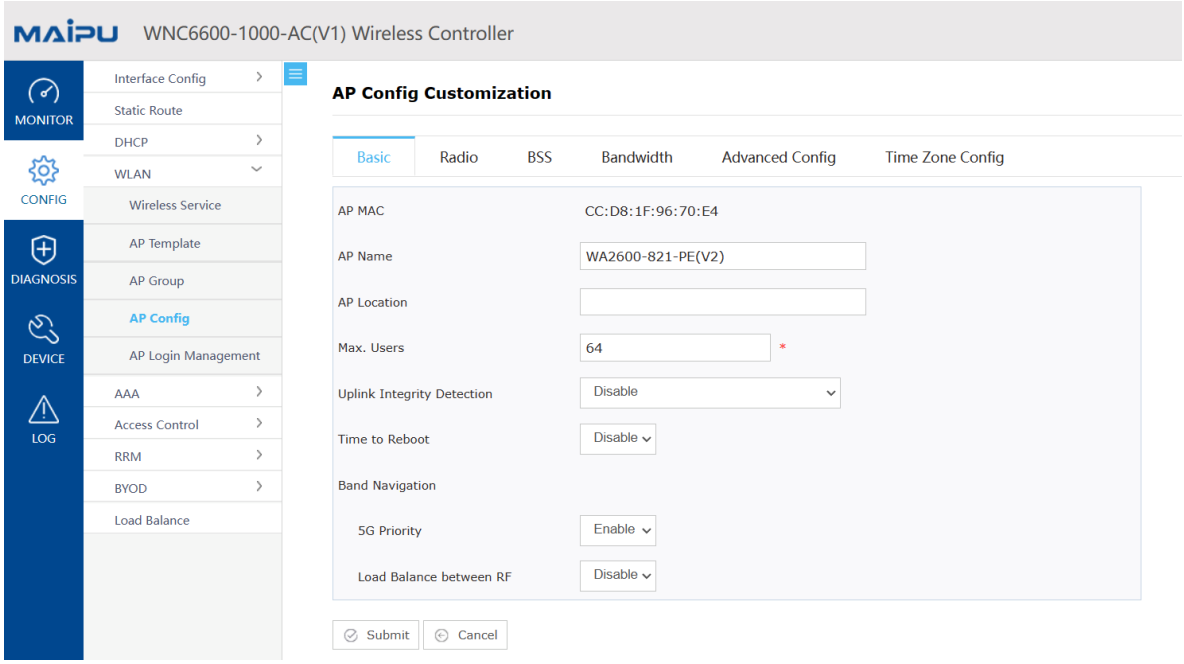


Figure 3.26 Customize AP configuration

3.6.4 DTLS Encryption Configuration

DTLS encryption supports two encryption methods, PSK and certificate, which can be selected during configuration. When enabling PSK encryption, you need to set a pre-shared key; when enabling certificate encryption, you need to import certificates to the device in advance, including AC certificates, CA certificates, and KEY certificates, as shown in Figure 3.27 and Figure 3.28.

copyright ©Maipu, all rights reserved

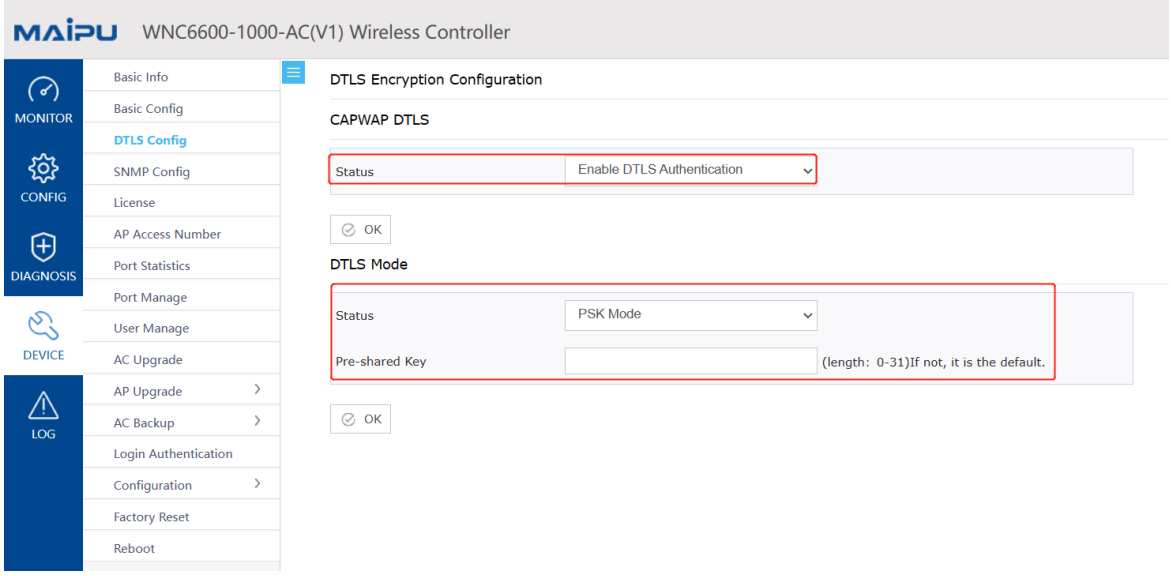


Figure 3.27 PSK encryption settings of DTLS

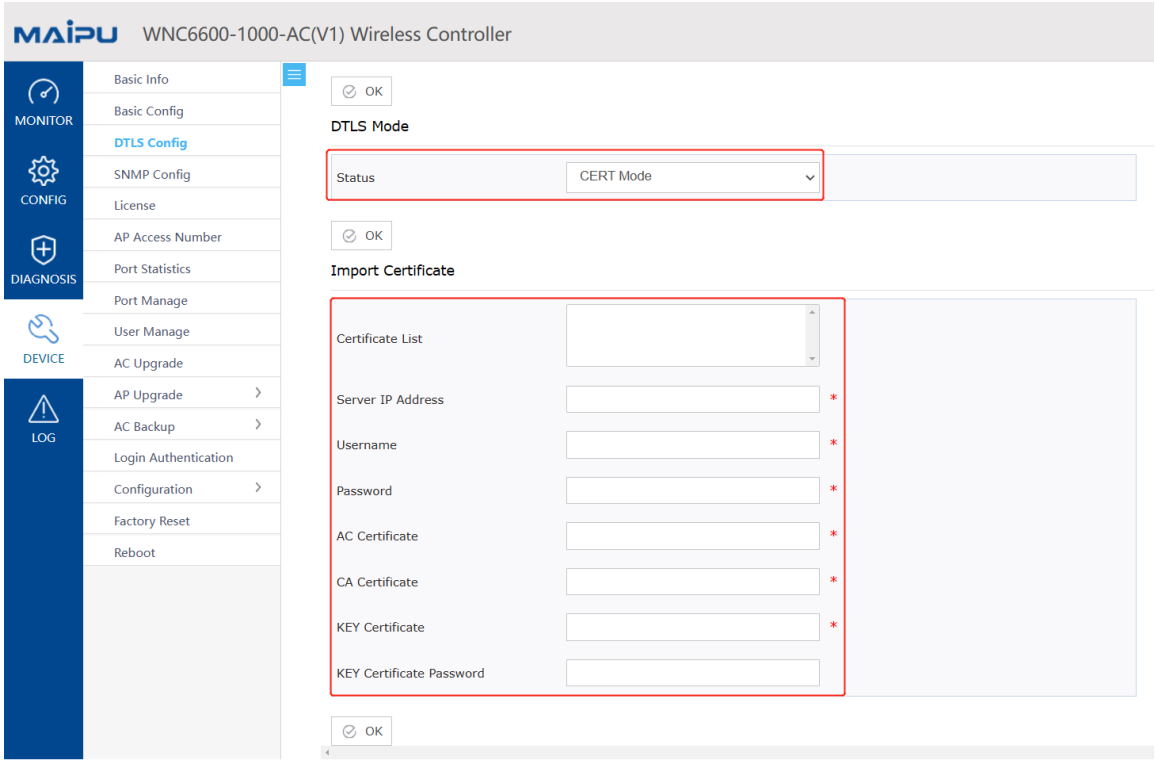


Figure 3.28 DTLS certificate mode encryption settings

copyright ©Maipu, all rights reserved

4 Authentication Function Configuration

4.1 NAS Configuration

Configure the address for communication between the AC and the authentication server. Multiple addresses can be configured, as shown in Figure 4.1.

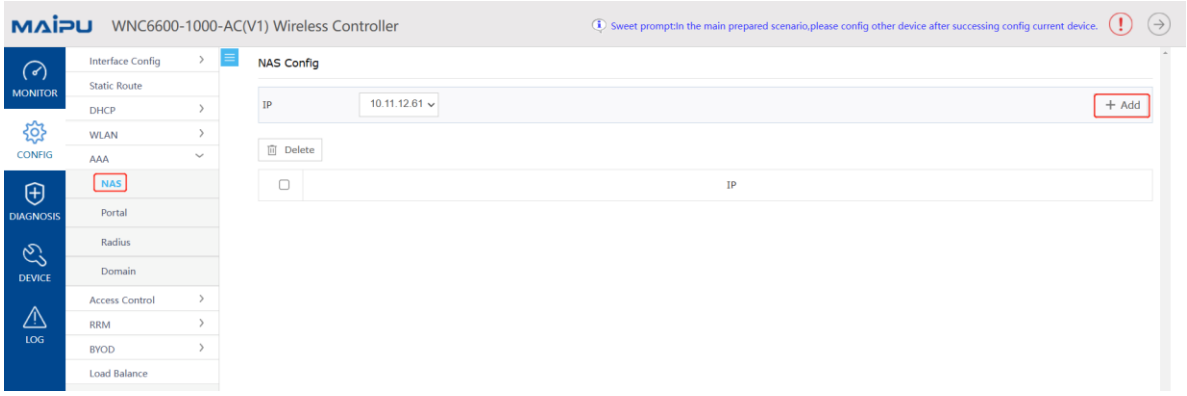


Figure 4.1 NAS configuration

4.2 Connect to Portal Server

Log in to the portal server management page: http://XXXX/portal/NMLogin.jsp

The AC device can be automatically registered to the portal-radius server, or can be manually registered. The following describes the manual registration method. Click "Device Management", select Add, and fill in the relevant configuration in the pop-up box.

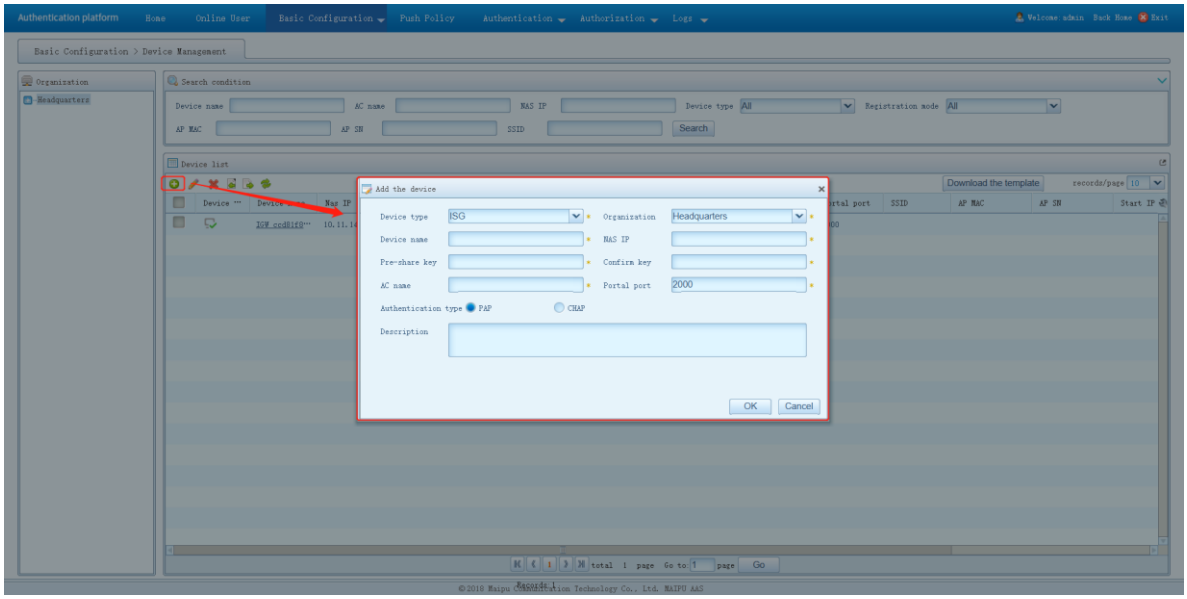


Figure 4.2 Portal server adding devices

copyright ©Maipu, all rights reserved

After adding, select the added device and click "View Status" to check whether the AC status is normal.

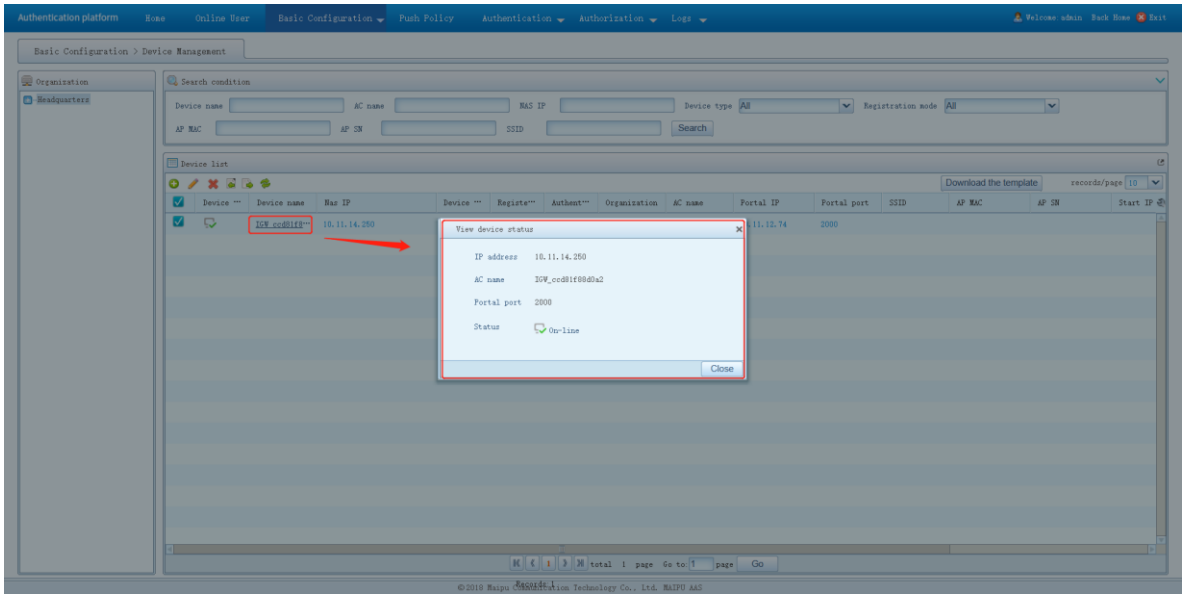


Figure 4.3 Check AC status

Note that the device key is the same as the shared key configured in radius on the AC.

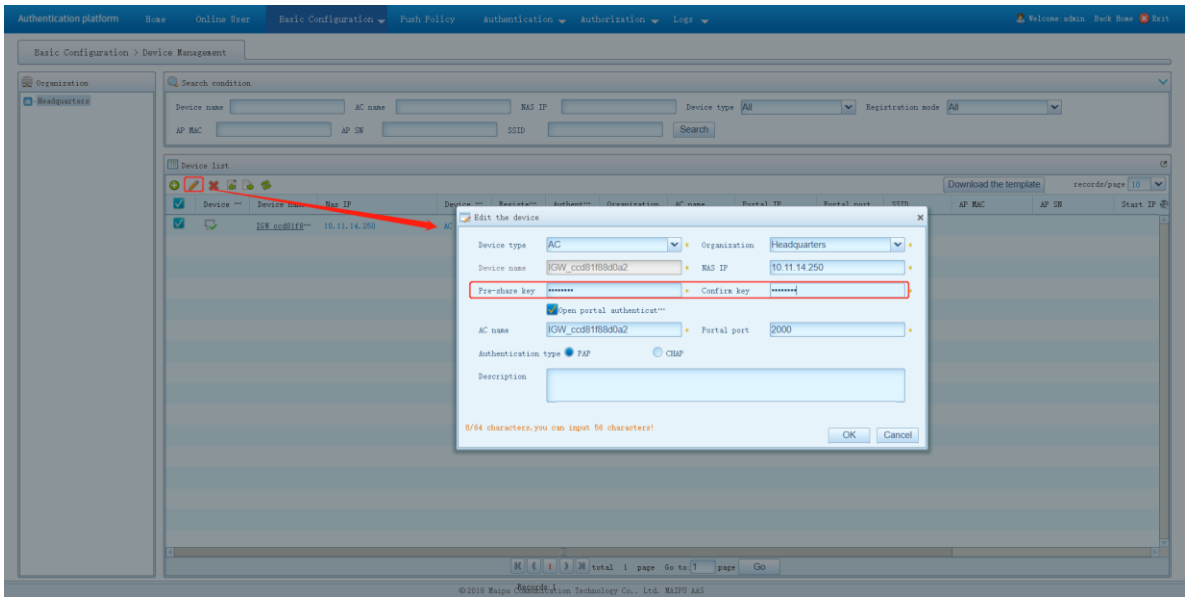


Figure 4.4 Shared key

4.3 Add AC Device on radius

Since the portal server and radius server are integrated together, the steps of adding AC devices have been completed in 5.2.

copyright ©Maipu, all rights reserved

4.4 Add Authenticated Users on radius

Click "User Management", select Add, and fill in the relevant configuration in the pop-up box.

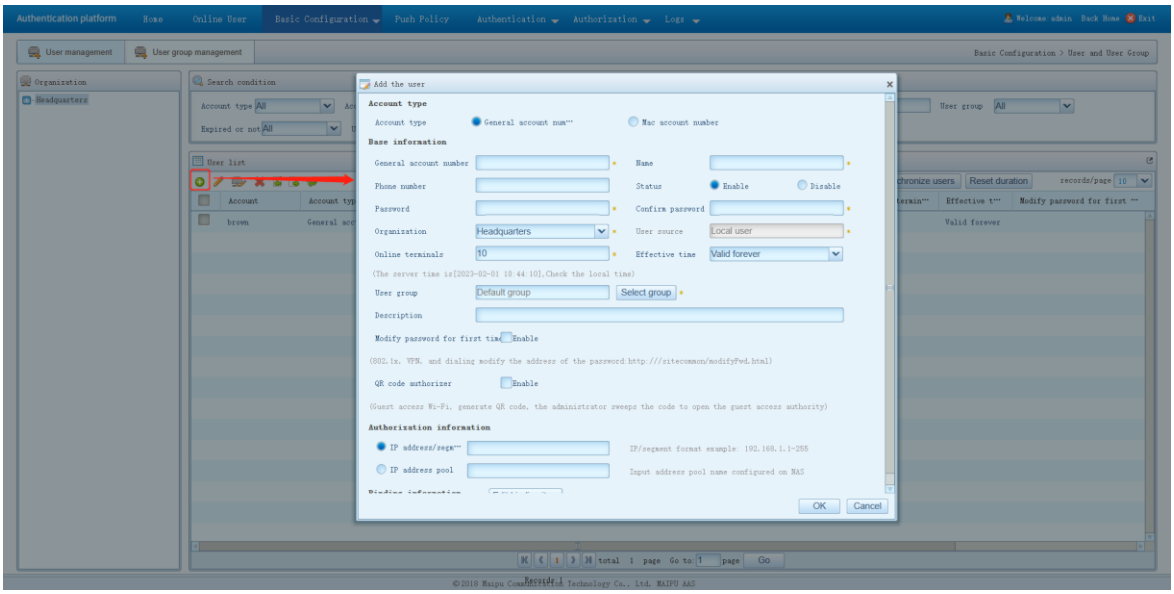


Figure 4.5 Add users on the radius server

Note

- The above content is the configuration for docking with Maipu portal server

4.5 802.1X Authentication Configuration

4.5.1 Add Device

Follow the steps in 4.3 and 4.4 to add AC to the authentication server

4.5.2 Configure radius on AC

1. Authentication server configuration

copyright ©Maipu, all rights reserved

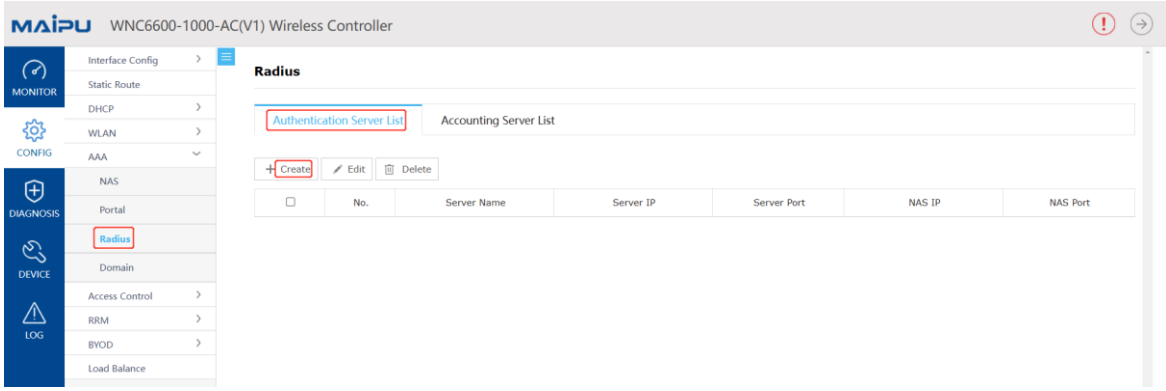


Figure 4.6 Create an authentication server

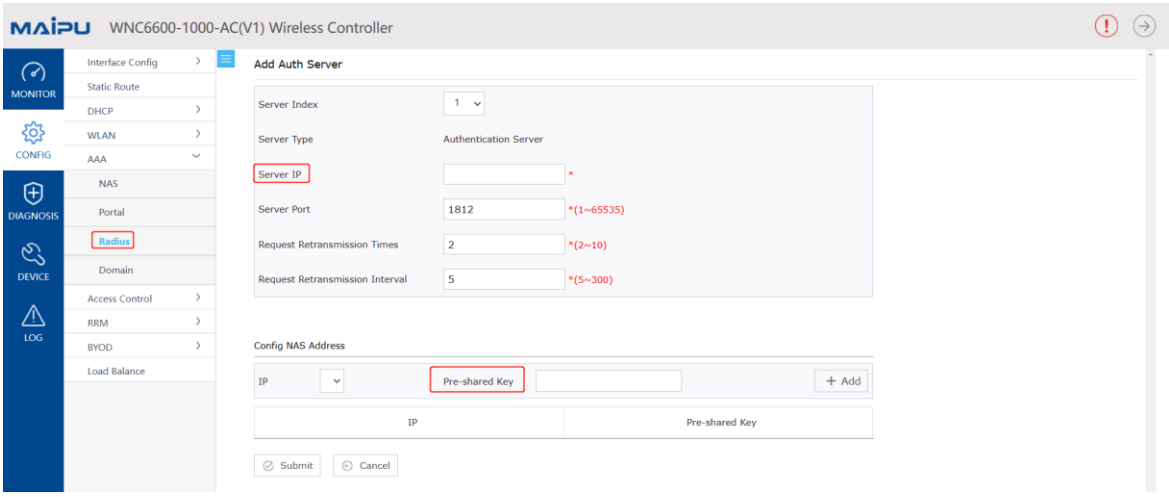


Figure 4.7 Authentication server configuration

2. Accounting server configuration

The accounting server is not a mandatory item and can be configured according to actual needs. The configuration method is the same as that of the authentication server. Please note that the port is distinguished from the authentication server.

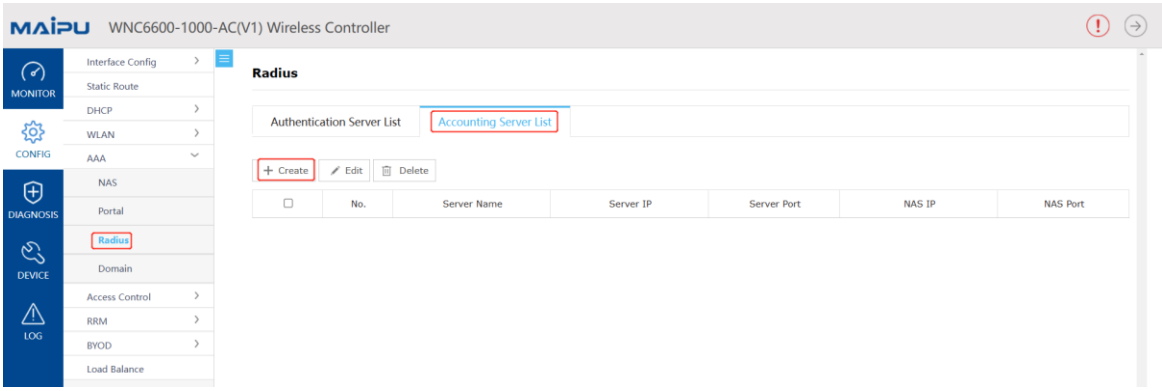


Figure 4.8 Create an accounting server

3. Authentication domain configuration

Bind the previously configured authentication server and accounting server to the domain.

copyright ©Maipu, all rights reserved

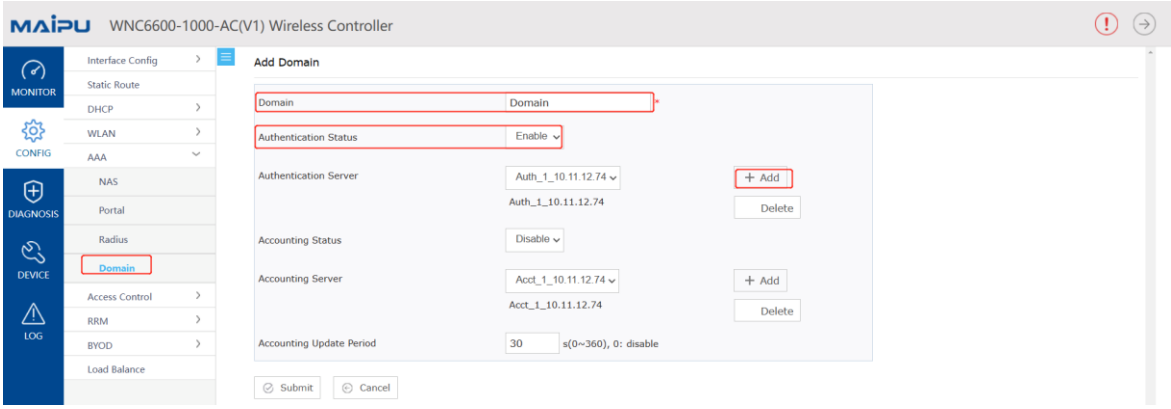


Figure 4.9 Configure authentication domain

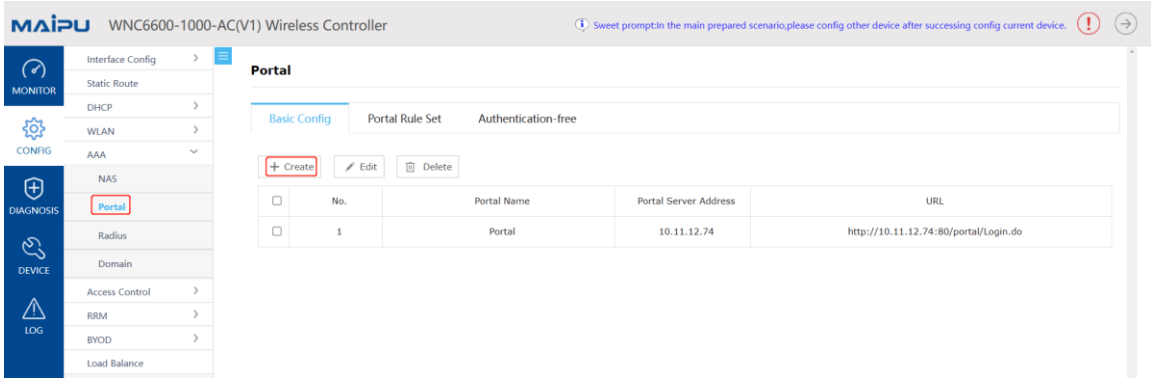
4.6 External Portal Authentication Configuration

4.6.1 Configure AC Device Name

Figure 4.10 Configure AC name

4.6.2 Portal Redirection Group Configuration and Application

1. Create a Portal redirection group



copyright ©Maipu, all rights reserved

Figure 4.11 Create a portal redirection group

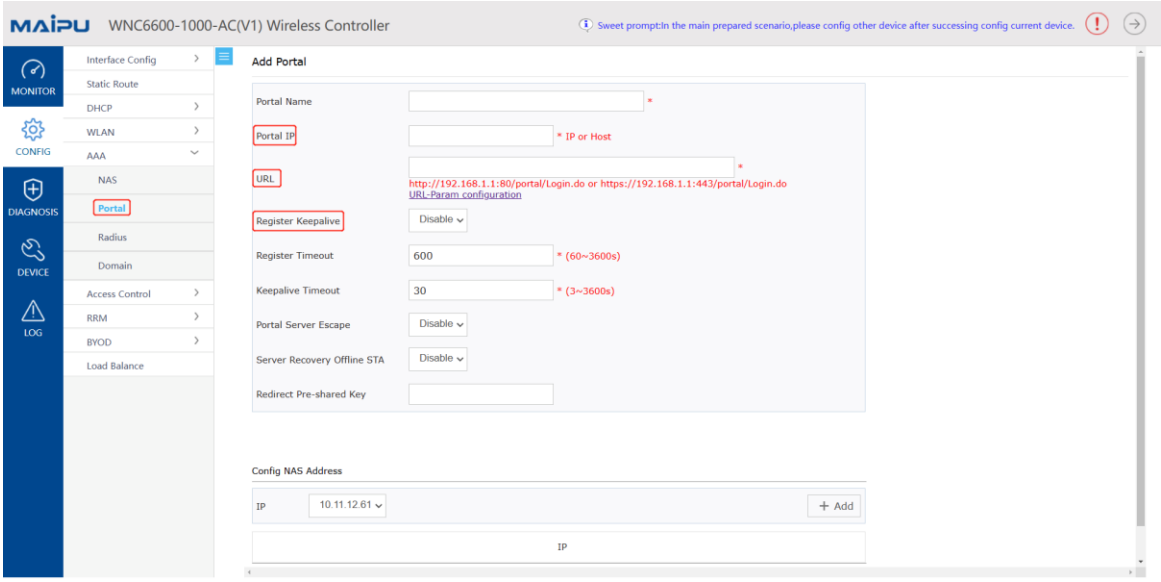


Figure 4.12 portal redirection group configuration

2. Click the URL parameter customization in the figure to customize the packet information in the URL, as shown in Figure 4.13

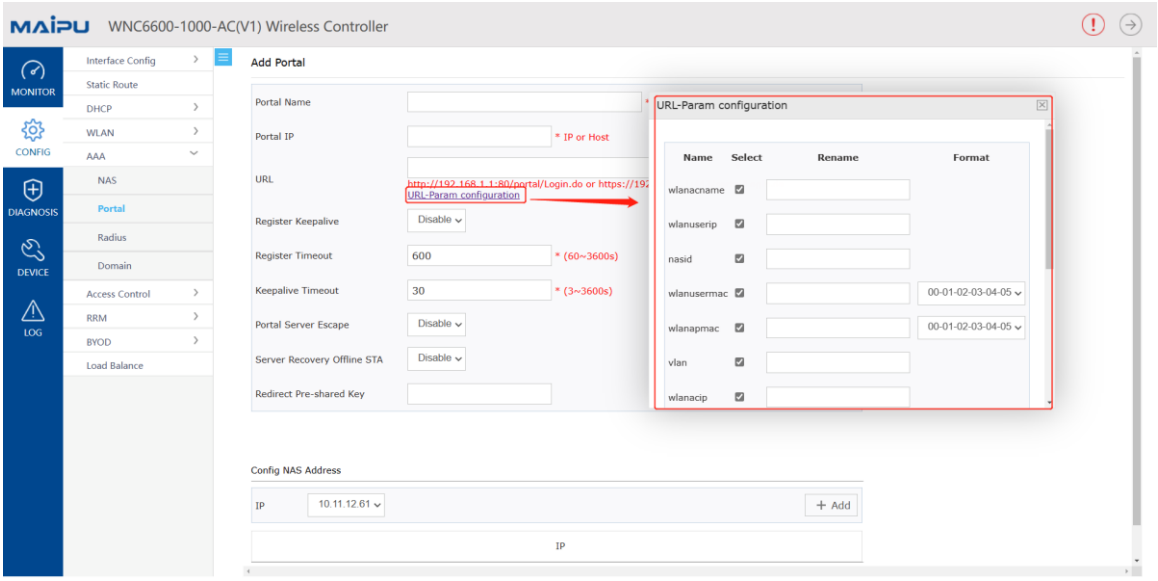


Figure 4.13 Custom configuration of URL parameters

Introduction to some functions:

A. **"URL"**: Portal redirection URL. The format is: http://xxxx:80/portal/Login.do or https://xxxx:443/portal/Login.do (the format of the built-in portal is: http://xxxx/portal_login.html).

B. **"Registration Keepalive"**: If the way of registering AC to Portal is dynamic registration, open this option (you don't need to manually add devices on the portal server during dynamic registration).

C. **"Portal Server Escape"**: After enabling the portal server escape, when the keepalive between the AC detection and the portal server times out, it will enter the escape mode, and the wireless

copyright ©Maipu, all rights reserved

terminal will access the SSID authenticated by the portal, and directly release its network authority without portal certified. When this function is used, **Registration Keepalive** must be enabled.

D. **"Server Recovery Offline STA"**: The users accessed during the portal escape can continue to access the network after the escape recovery. If this function is enabled, after the portal escape resumes, AC will kick the user who is accessed during the escape offline and let it go through portal authentication again.

E. **"Redirect Pre-shared Key"**: In order to solve the problem of the forgery vulnerability of the return value of the nasgetinfo interface, when the device performs portal redirection, two new parameters, timestamp and md5 signature, are added to the URL address of 302 to STA. The md5 calculation parameters are: the existing push parameters + timestamp + pre-shared key generation, and the pre-shared key uses the shared key configured in the portal configuration when the portal is redirected.

F. **"Portal client configuration"**: Select the NAS IP that can communicate with the portal server. Please configure this option carefully. Once the configuration is wrong, you need to delete the entire redirection group and add it again. This item cannot be modified separately.

G. **"URL Parameter Customization"**: Provides a more flexible and convenient url parameter selection method, which can be configured according to actual scenarios. The parameters include acname, userip, nasid, usermac, etc.

3. Configure the SSID of portal type

Create an SSID whose authentication method is open, and enable portal authentication.

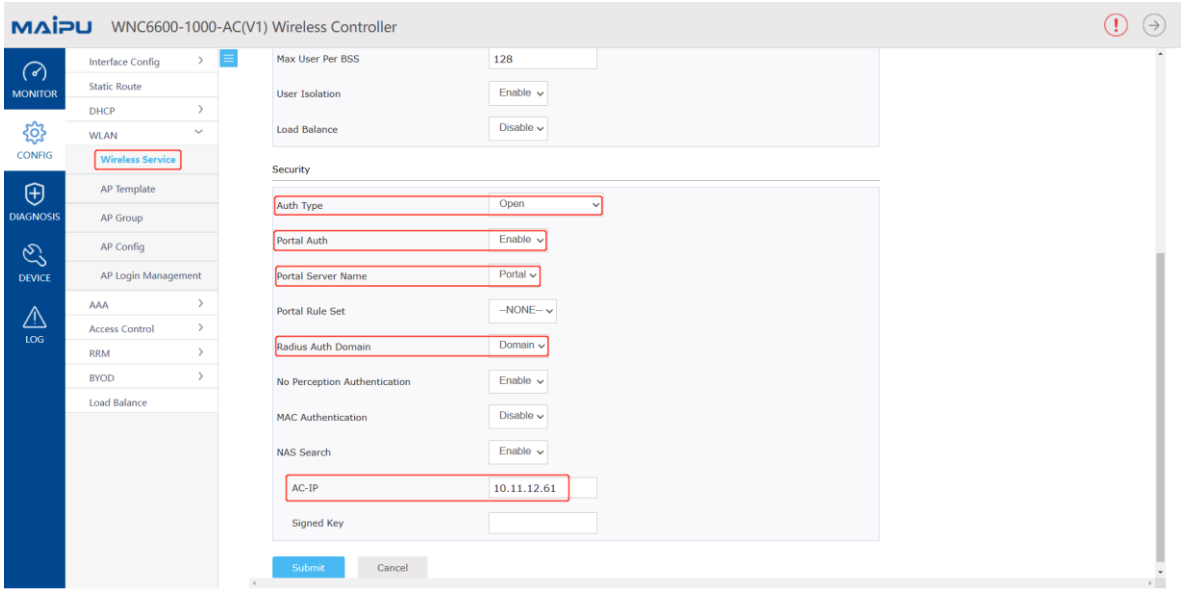


Figure 4.14 Create a wireless service set for portal authentication

Description of some functions:

copyright ©Maipu, all rights reserved

A. "Portal Server Name": Select the portal authentication server to be used (that is, the one created in 4.6.2.1).

B. "No Perception Authentication": After enabling this function, when the STA accesses the portal authentication wireless service set, the AC will carry the STA's MAC address to the portal server for a fast and non-perception query, and based on the query result, the STA will be allowed or rejected from the network.

C. "MAC Authentication": When portal authentication is enabled, you can choose to enable MAC address authentication, and the AC uses the user's MAC address as the user name and password to authenticate to the radius server.

D. "Radius Auth Domain": select the radius authentication domain to be used (that is, created in 4.5.2.3). If this item is not selected, the default domain will be used by default.

E. "NAS Search": If the content platform is enabled on the authentication server, NAS information query needs to be enabled in the wireless service set configuration, and the AC-IP parameter of NAS information query is configured as the NAS IP address. The signature password is used by nasgetinfo, and two new parameters, timestamp and md5 signature, are added to the return value of NAS information query. The md5 calculation parameters are: existing push parameters + time stamp + pre-shared key generation, and the pre-shared key used for NAS query uses the signature password in the NAS information query of the wireless service set.

copyright ©Maipu, all rights reserved

5 WPA3 Authentication Configuration

The full name of WPA3 is Wi-Fi Protected Access 3. It is a new Wi-Fi encryption protocol released by the Wi-Fi Alliance at the International Consumer Electronics Show (CES) in Las Vegas, USA on January 8,2018. It is a Subsequent version of the Wi-Fi authentication standard WPA2 technology

5.1. Centralized Forwarding-wpa3-enterprise Authentication Configuration Guide

5.1.1 Networking Requirements

The AC is connected to the L2 LAN through the bypass mode, the AP is powered by the POE switch, the AP and the wireless terminal obtain IP addresses through DHCP, and the AP provides a wireless network named "abc" and enabled with wpa3-enterprise authentication.

5.1.2 Network Topology

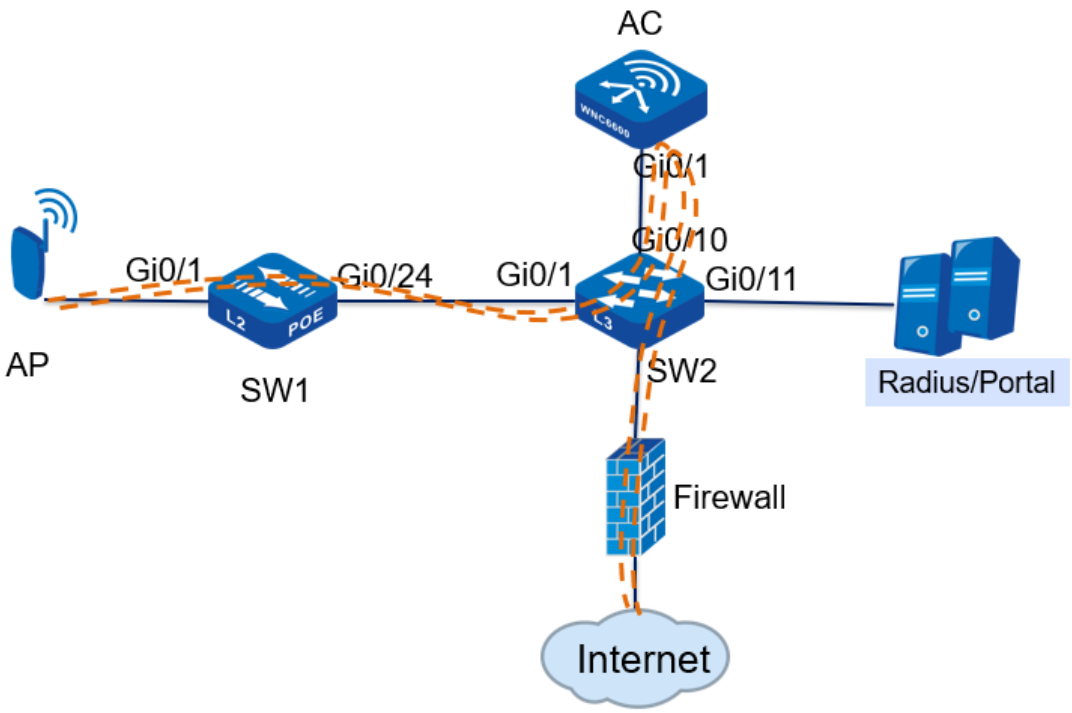


Figure 5.1 wpa3-enterprise authentication in centralized forwarding mode

Topology introduction:

Wi-Fi Security	The authentication method is wpa3-enterprise, and the encryption type is AES
WLAN wireless service set	Wireless service set name: wlan1

copyright ©Maipu, all rights reserved

	SSID: abc Data forwarding mode: centralized forwarding
AP management VLAN	vlan10
AP service VLAN	vlan200
AP management IP address pool	192.168.10.10—192.168.10.100
AP management gateway	192.168.10.254 (on the core switch)
User IP address pool	192.168.200.10—192.168.200.100
User gateway	192.168.200.254 (on the core switch)
DHCP server	The core switch acts as a DHCP server for APs and users
AAS server IP address	192.168.10.253

Table 5.1 Topology introduction

5.1.3 Configuration Ideas

1. Configure intermediate network device interfaces, including POE power supply switches and L3 core switches;
2. Configure DHCP server to provide IP address for AP;
3. Statically configure the IP address of the AC on the AP;
4. Configure an authentication server on the AC and bind the authentication domain;
5. Create a wireless service set on the AC, enable wpa3-enterprise authentication, and bind the authentication domain;
6. Create an AP template on the AC, bind the wireless service set and apply it to the AP;
7. Create an authentication account and password on the AAS server;
8. The wireless terminal can successfully access the wireless network;

5.1.4 Configuration Steps

1. POE switch (SW1) configuration

#Create vlan10 and vlan200 on SW1, and configure the link type of gigabitethernet0/1 connected to the AP as Trunk, allowing vlan10 and vlan200 to pass through, and the PVID is10.

```
SW1#cont
SW1(config)#vlan10,200
Please wait.....
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/1
SW1(config-if-gigabitethernet0/1)# switchport mode trunk
SW1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,200
```

copyright ©Maipu, all rights reserved

```
SW1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan10
SW1(config-if-gigabitethernet0/1)# exit
```

#Configure the link type of gigabitethernet0/24 connected to SW2 as Trunk, allowing vlan10 and vlan200 to pass through.

```
SW1#cont
SW1(config)#interface gigabitethernet 0/24
SW1(config-if-gigabitethernet0/24)# switchport mode trunk
SW1(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW1(config-if-gigabitethernet0/24)# exit
```

2. Core switch (SW2) configuration

#Create vlan10, vlan200 and their corresponding vlan interface on SW2, and configure IP address for this interface, which will be used as the gateway between AP and wireless terminal.

```
SW2#cont
SW2(config)#vlan10,200
Please wait......
Done.
SW2(config)#
SW2(config)#interface vlan10
SW2(config-if-vlan10)# ip address192.168.10.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan10)# exit
SW2(config)#
SW2(config)#interface vlan200
SW2(config-if-vlan200)# ip address192.168.200.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan200)#
```

#Configure the DHCP address pool ap-pool on SW2, dynamically allocate IP addresses for APs, and configure the gateway as192.168.10.254; configure the DHCP address pool sta-pool, dynamically allocate IP addresses for wireless terminals, and configure the gateway as192.168.100.254.

```
SW2#cont
SW2(config)#ip dhcp pool ap-pool
SW2(dhcp- config)# range192.168.10.10192.168.10.100255.255.255.0
SW2(dhcp- config)# default-router192.168.10.254
SW2(dhcp- config)# exit
SW2(config)#ip dhcp pool sta-pool
SW2(dhcp- config)# range192.168.200.10192.168.200.100255.255.255.0
```

copyright ©Maipu, all rights reserved

```
SW2(dhcp- config)# default-router192.168.200.254
SW2(dhcp- config)# dns-server 8.8.8.8
SW2(dhcp- config)# exit
```

#On SW2, configure the link type of gigabitethernet0/1 connected to SW1 as Trunk, allowing vlan10 and vlan200 to pass through; configure the link type of gigabitethernet0/10 connected to AC as Trunk, allowing vlan10 and vlan200 to pass through.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/1
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW2(config-if-gigabitethernet0/24)# exit
SW2(config)#interface gigabitethernet 0/10
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,200
SW2(config-if-gigabitethernet0/24)# exit
```

#Configure the interface connected to PC. On SW2, configure the link type of gigabitethernet0/20 as access and vlan as10. Connect the PC to port20 of the core switch SW2, and the PC can obtain the IP address.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/20
SW2(config-if-gigabitethernet0/20)# switchport mode access
SW2(config-if-gigabitethernet0/20)# switchport access vlan10
SW2(config-if-gigabitethernet0/20)# exit
```

3. AP configuration

#Connect the AP to the gigabitethernet0/1 port of the POE switch, the AP is powered normally, and check the IP address obtained by the AP on the core switch SW2.

```
SW2 #show ip dhcp pool ap-pool binding
Current DHCP binding information

Hardware-Address IP-Address Lease Status
0001.7a20.18401 92.1 68.10.101Day 05:58:44 ACKED
SW2 #
```

#Enter http://192.168.10.10 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

copyright ©Maipu, all rights reserved

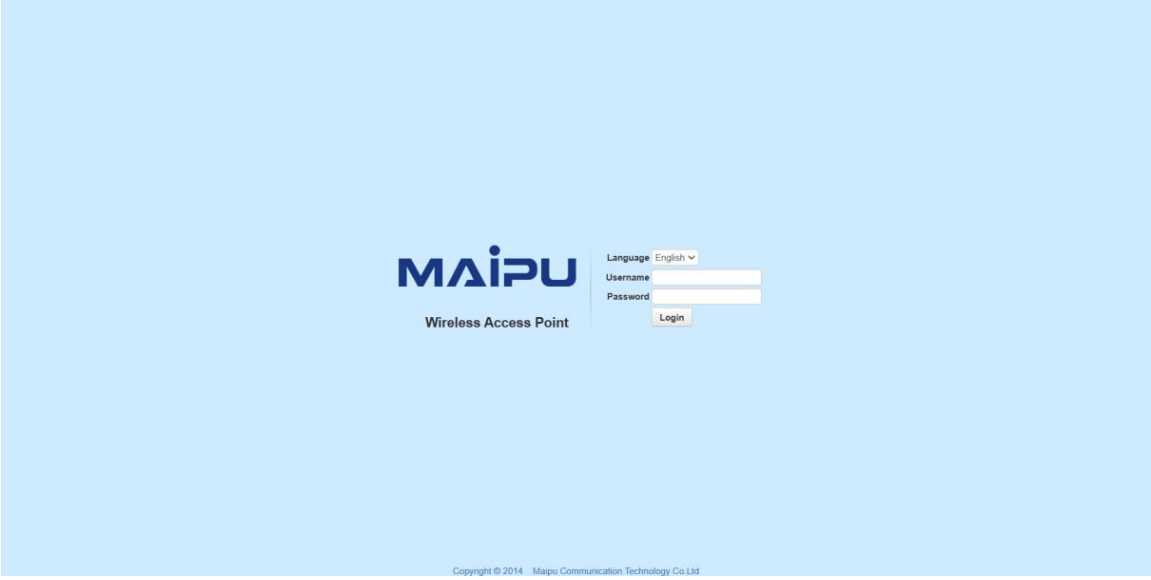


Figure 5.2 AP login page

#After entering the web management page of the AP, you will first enter the quick wizard configuration page. From step1 to step 3, you can directly use the default configuration. In step 4, configure the discovery method as static discovery, and configure the IPV4 address of the AC as192.168.10.1 Finally click the <Finish> button to complete the configuration, after the configuration is successful, it will jump to the system monitoring page.

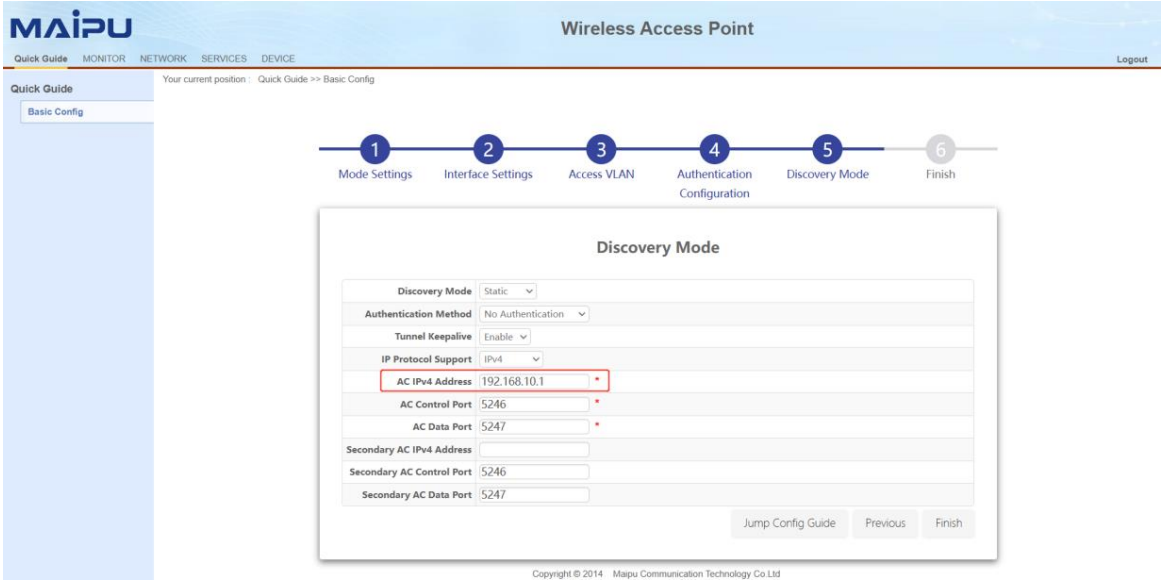


Figure 5.3 AP Configuration Wizard

4. AC configuration

#Create vlan10 and vlan200 on the AC, and create the corresponding vlan10 interface, which is used to establish a CAPWAP tunnel with the AP; configure the link type of gigabitethernet0/1 connected to SW2 as Trunk, allowing vlan10 and vlan200 to pass through.

AC # con t

AC(config)#vlan10,200

Please wait.....

copyright ©Maipu, all rights reserved

Done.

AC(config)#

AC(config)#interface vlan10

AC(config-if-vlan10)# ip address192.168.10.124

AC(config-if-vlan10)# exit

AC(config)#interface gigabitethernet 0/1

AC(config-if-gigabitethernet0/1)# switchport mode trunk

AC(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,200

#Configure VLAN200 on the AC to support centralized forwarding.

AC # con t

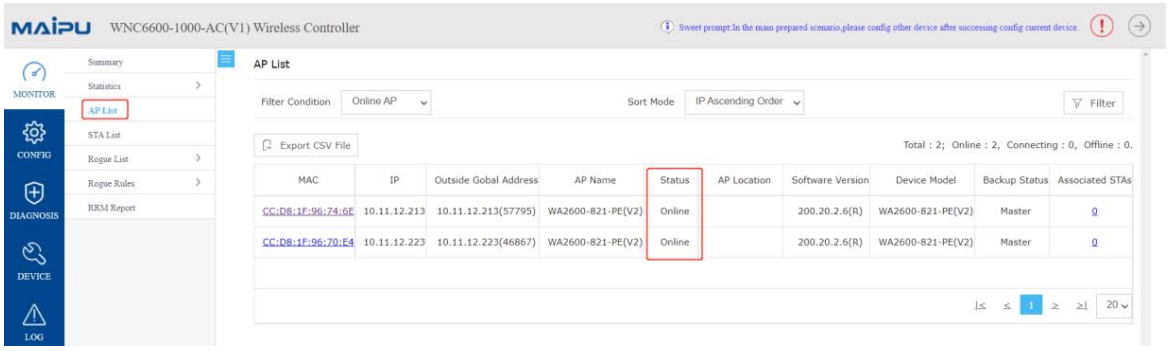
AC(config)#wireless vlan-list200

AC(config)# exit

#After completing the above configuration, wait for about two minutes, the AP can successfully connect to the AC, and you can view the status of the AP on the AC. Enter http://192.168.10.1 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in

Figure 5.4 AC login page

#Click MONITOR > AP List, and you can see that the AP is online, as shown in the figure below



copyright ©Maipu, all rights reserved

Figure 5.5 AP list

#Add NAS IP. Click CONFIG > AAA > NAS, select the IP address100.0.52.10, and click the <Add> button to set it as the NAS IP.

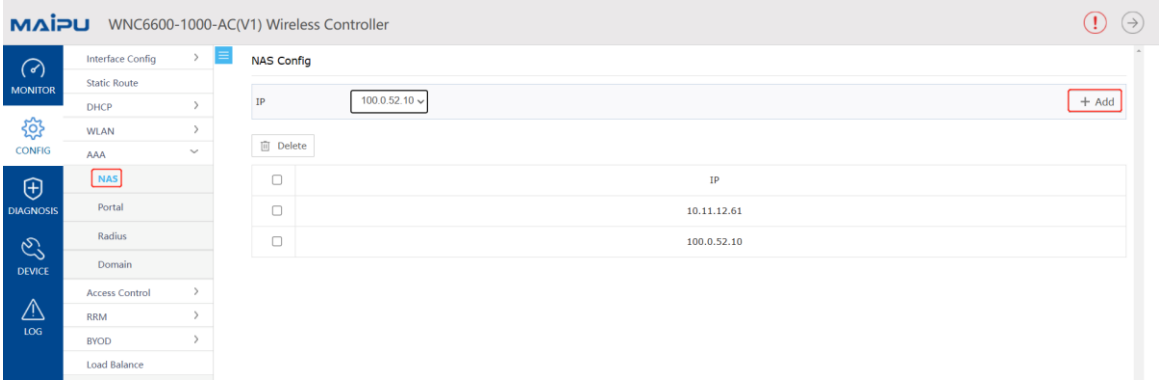


Figure 5.6 NAS configuration

#Configure authentication server. Click CONFIG > AAA > Radius > Auth Server List, click <Create> to create a new authentication server, configure the server address as 192.168.10.253, configure the RADIUS client, IP address as100.0.52.10, configure the pre-shared key as admin, and click <Add>, after performing the above configuration, click the OK button below to complete the configuration of the authentication server.

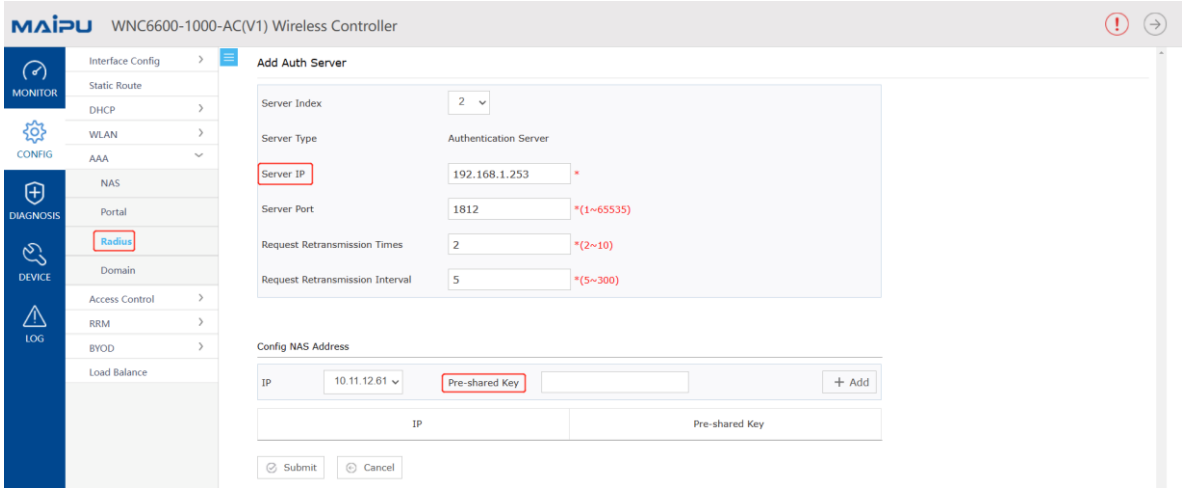


Figure 5.7 Authentication server configuration

#Domain configuration. Click CONFIG > AAA > Domain, click <Create> to create a new authentication domain, the domain name is the name of the authentication domain, here it is configured as yu, configure authentication status to enable, the authentication server selects 192.168.10.253, and click <Add>, after performing the above configuration, click the OK button below, and the configuration of the authentication domain is completed.

copyright ©Maipu, all rights reserved

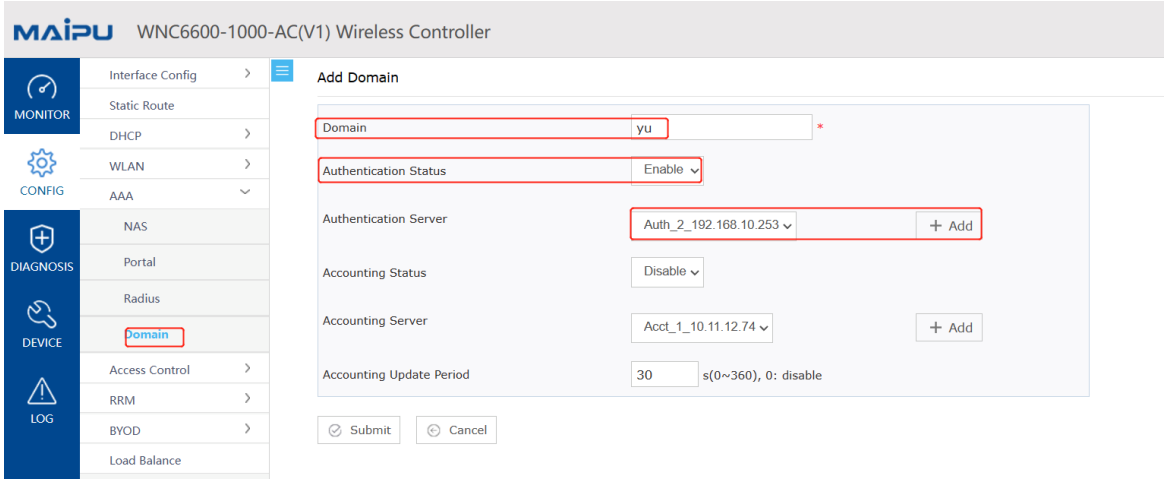


Figure 5.8 Domain configuration

#Create a wireless service set. Click CONFIG > WLAN > Wireless Service, create a wireless service set, as shown in the figure below, the wireless name is wlan1, select "Enable" for service status, select "Centralized forwarding" for forwarding mode, configure SSID as abc, configure user VLAN as100, select wpa3-enterprise for the authentication method, select yu for the Radius authentication domain, and use the default values for other configurations. Click the <OK> button to complete the configuration of the wireless service set.

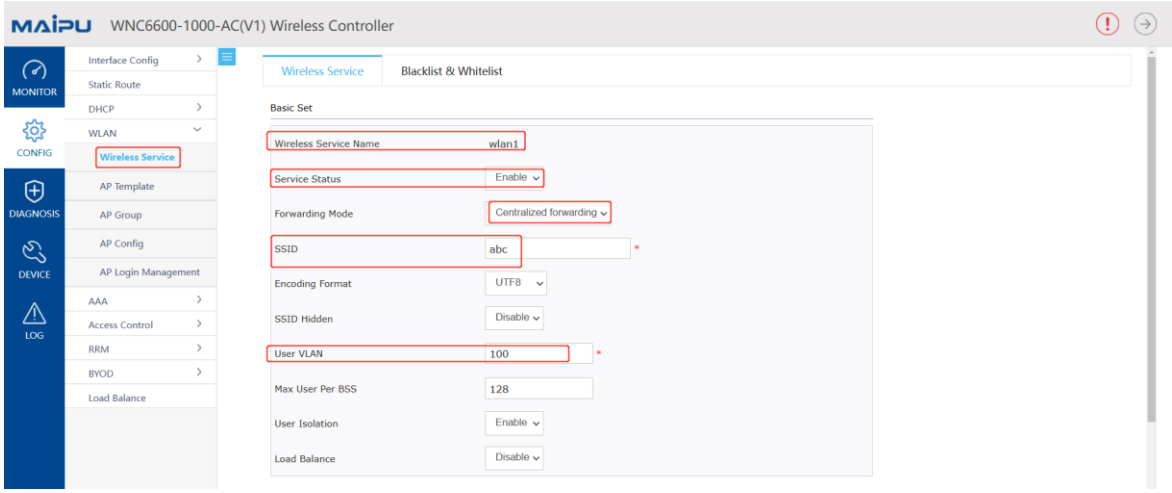


Figure 5.9 Wireless service configuration

copyright ©Maipu, all rights reserved

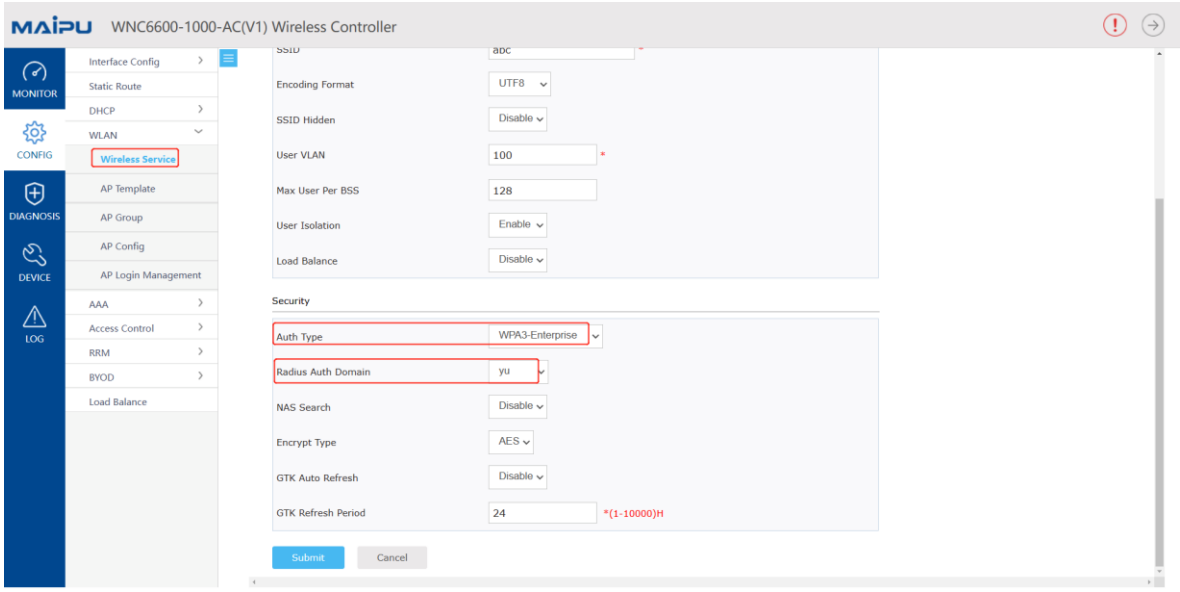


Figure 5.10 Wireless service configuration

#Bind the wireless service set to the AP profile. Click CONFIG > WLAN > AP template, create an AP template, as shown in the figure below. By default, the name of the AP template is Default_FitAP_Profile, which can be changed, and the name cannot be changed after creation.

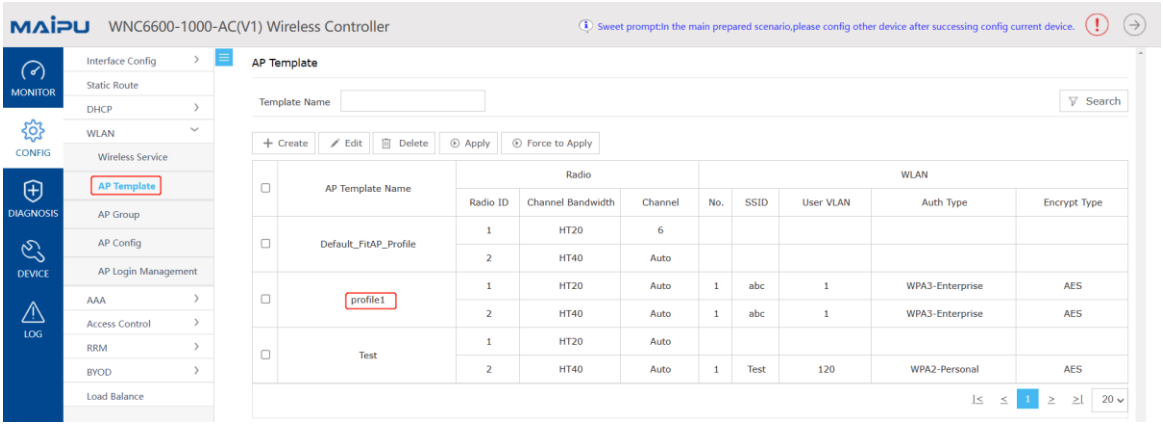


Figure 5.11 AP template

#Select the created AP template profile1, click the Edit button, click BSS > Wireless Service Name, select wlan1 created above, select ALL for Radio ID, use default values for other configurations, and click <OK> button to complete AP template configuration.

copyright ©Maipu, all rights reserved

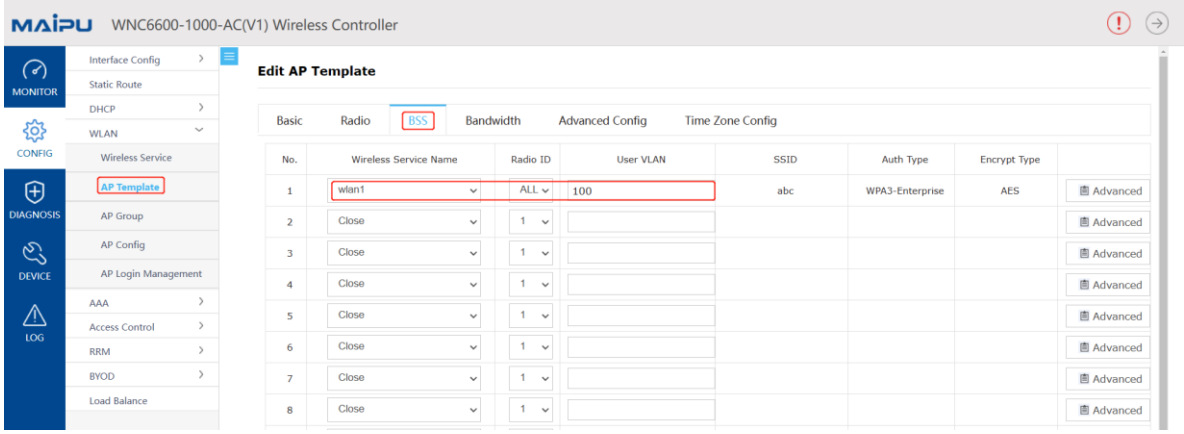


Figure 5.12 AP profile BSS configuration

#AP template application. Click CONFIG > WLAN > AP Config, select the connected AP, select profile1 in the AP module, and then click Apply in the template application.

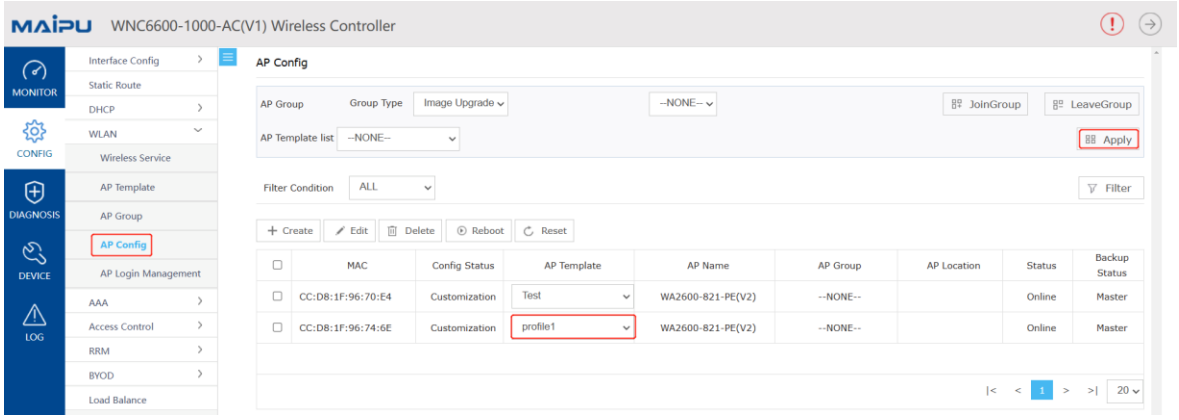
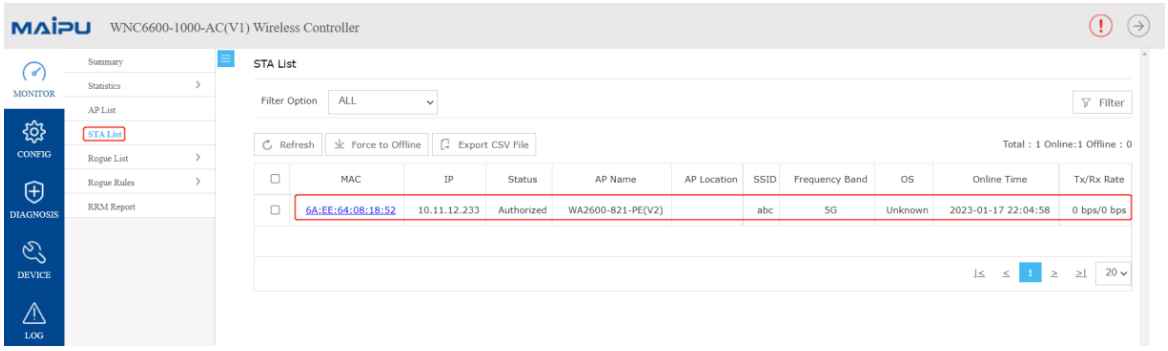


Figure 5.13 AP configuration

#Create an authentication account. Create an authentication account on the authentication server. The specific steps are omitted. For details, see 4.4 Add an Authentication User on Radius.

5.1.5 Result Verification

#Wireless terminal access, after applying the AP template, after two minutes, turn on the wifi of the wireless terminal, and you will be able to search for the wireless signal abc, and you can successfully access it after entering the user name and password. On the AC web page, click MONITOR > STA List, and you can see the information of wireless terminals.



copyright ©Maipu, all rights reserved

Figure 5.14 Terminal list

Note

- In addition to the BSS configuration, the AP template also needs to configure the working signal and channel bandwidth of the AP according to the actual network environment. The working channel of the 2.4G radio frequency generally chooses1, 6, and11, and the channel bandwidth chooses HT20.
- The above example is based on 8 series APs (WA2600-821-PE(V2), WA2600-821-PE(V3), WA2600-815-PE(V2), WA2600-815-PE(V3)) as an example, so when configuring the BSS in the AP template, select all as the radio ID, and select 1 as the radio ID for APs that only support 2.4 G radio frequency.

5. 2 Local Forwarding-wpa 3-personal Authentication Configuration Guide

5.2.1 Networking Requirements

The AC is connected to the L2 LAN through the bypass mode, the AP is powered by the POE switch, the AP and the wireless terminal obtain IP addresses through DHCP, and the AP provides a wireless network named "abc" and enabled with wpa 3-personal authentication.

5.2.2 Network Topology

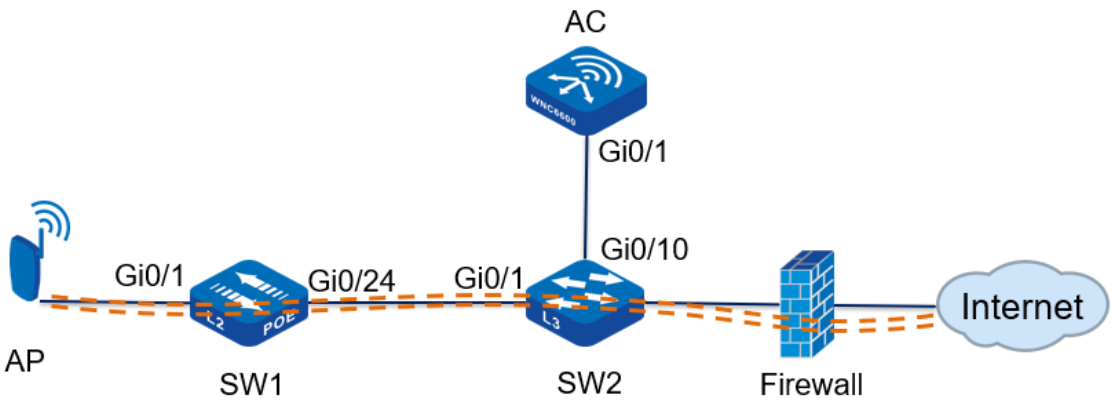


Figure 5.15 wpa3-personal authentication in local forwarding mode

Topology introduction:

copyright ©Maipu, all rights reserved

Wi-Fi Security	wpa3-personal authentication, encryption type is AES
WLAN wireless service set	Wireless service set name: wlan1 SSID: abc Data forwarding mode: local forwarding
AP management VLAN	vlan10
AP service VLAN	vlan100
AP management IP address pool	192.168.10.10—192.168.10.100
AP management gateway	192.168.10.254 (on the core switch)
User IP address pool	192.168.100.10—192.168.100.100
User gateway	192.168.100.254 (on the core switch)
DHCP server	The core switch acts as a DHCP server for APs and users

Table 5.2 Topology introduction

5.2.3 Configuration Ideas

1. Configure intermediate network devices, including POE power supply switches and L3 core switches;
2. Configure DHCP server to provide IP address for AP;
3. Statically configure the IP address of the AC on the AP;
4. Create a wireless service set on the AC, and the authentication method is wpa3-personal;
5. Create an AP template on the AC, bind the wireless service set and apply it to the AP;
6. The wireless terminal accesses the wireless network, and the entries on the AC are normal;

5.2.4 Configuration Steps

1. POE switch (SW1) configuration

#Create vlan10 and vlan100 on SW1, and configure the link type of gigabitethernet0/1 connected to the AP as Trunk, allowing vlan10 and vlan100 to pass through, and the PVID is10.

```
SW1#cont
SW1(config)#vlan10,100
Please wait.....
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/1
```

copyright ©Maipu, all rights reserved

```
SW1(config-if-gigabitethernet0/1)# switchport mode trunk
SW1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/1)# switchport trunk pvid vlan10
SW1(config-if-gigabitethernet0/1)# exit
```

#Configure the link type of gigabitethernet0/24 connected to SW2 as Trunk, allowing vlan10 and vlan100 to pass through.

```
SW1#cont
SW1(config)#vlan10,100
Please wait......
Done.
SW1(config)#
SW1(config)#interface gigabitethernet 0/24
SW1(config-if-gigabitethernet0/24)# switchport mode trunk
SW1(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW1(config-if-gigabitethernet0/24)# exit
```

2. Core switch (SW2) configuration

#Create vlan10, vlan100 and their corresponding vlan interface on SW2, and configure IP address for this interface, which will be used as the gateway between AP and wireless terminal.

```
SW2#cont
SW1(config)#vlan10,100
Please wait......
Done.
SW2(config)#
SW2(config)#interface vlan10
SW2(config-if-vlan10)# ip address192.168.10.25424
SW2(config-if-vlan10)# ip dhcp server
SW2(config-if-vlan10)# exit
SW2(config)#
SW2(config)#interface vlan100
SW2(config-if-vlan100)# ip address192.168.100.25424
SW2(config-if-vlan100)# ip dhcp server
SW2(config-if-vlan100)#
```

#Configure the DHCP address pool ap-pool on SW2, dynamically allocate IP addresses for APs, and configure the gateway as192.168.10.254; configure the DHCP address pool sta-pool, dynamically allocate IP addresses for wireless terminals, and configure the gateway as192.168.100.254.

```
SW2#cont
```

copyright ©Maipu, all rights reserved

```
SW2(config)#ip dhcp pool ap-pool
SW2(dhcp- config)# range192.168.10.10192.168.10.100255.255.255.0
SW2(dhcp- config)# default-router192.168.10.254
SW2(dhcp- config)# exit
SW2(config)#ip dhcp pool sta-pool
SW2(dhcp- config)# range192.168.100.10192.168.100.100255.255.255.0
SW2(dhcp- config)# default-router192.168.100.254
SW2(dhcp- config)# dns-server 8.8.8.8
SW2(dhcp- config)# exit
```

#On SW2, configure the link type of gigabitethernet0/1 connected to SW1 as Trunk, allowing vlan10 and vlan100 to pass through; configure the link type of gigabitethernet0/10 connected to AC as access, and vlan as10.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/1
SW2(config-if-gigabitethernet0/24)# switchport mode trunk
SW2(config-if-gigabitethernet0/24)# switchport trunk allowed vlan add10,100
SW2(config-if-gigabitethernet0/24)# exit
SW2(config)#interface gigabitethernet 0/10
SW2(config-if-gigabitethernet0/24)# switchport mode access
SW2(config-if-gigabitethernet0/24)# switchport access vlan10
SW2(config-if-gigabitethernet0/24)# exit
```

#Configure the interface connected to PC. On SW2, configure the link type of gigabitethernet0/20 as access and vlan as 10. Connect the PC to port 20 of the core switch SW2, and the PC can obtain the IP address.

```
SW2#cont
SW2(config)#interface gigabitethernet 0/20
SW2(config-if-gigabitethernet0/20)# switchport mode access
SW2(config-if-gigabitethernet0/20)# switchport access vlan10
SW2(config-if-gigabitethernet0/20)# exit
```

3. AP configuration

#Connect the AP to the gigabitethernet0/1 port of the POE switch, the AP is powered normally, and check the IP address obtained by the AP on the core switch SW2.

```
SW2 #show ip dhcp pool ap-pool binding
Current DHCP binding information

Hardware-Address IP-Address Lease Status
```

copyright ©Maipu, all rights reserved

0001.7a20.1840 1 92.1 68.10.101Day 05:58:44 ACKED

SW2 #

#Enter http://192.168.10.10 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

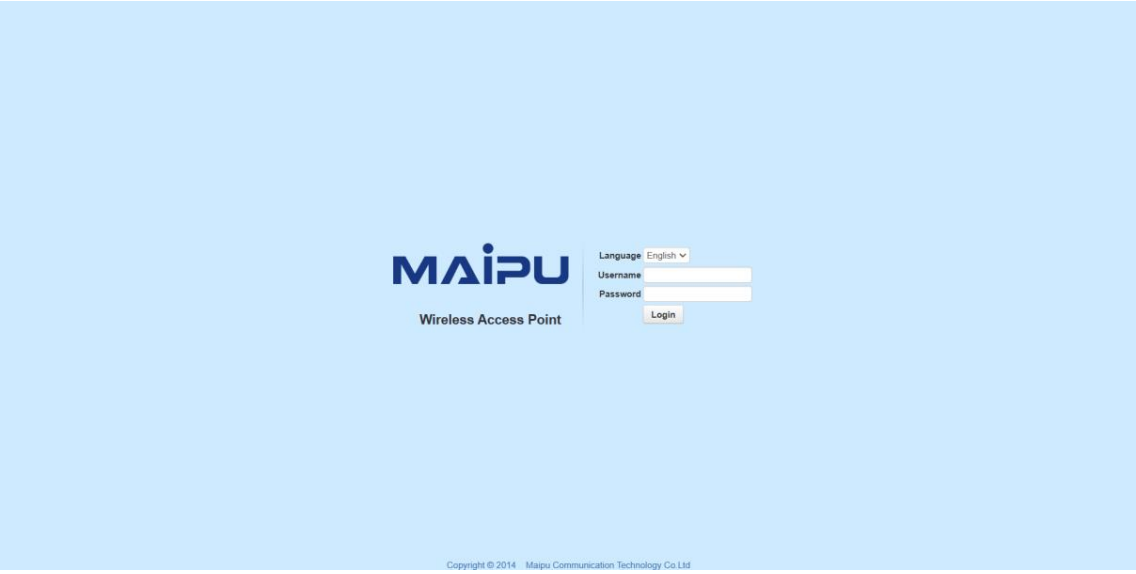


Figure 5.16 AP login page

#After entering the web management page of the AP, you will first enter the quick wizard configuration page. From step1 to step 3, you can directly use the default configuration. In step 4, configure the discovery method as static discovery, and configure the IPV4 address of the AC as192.168.10.1. If in the V6 environment, you can also configure the IPV6 address of the AC, and finally click the <Finish> button to complete the configuration, after the configuration is successful, it will jump to the system monitoring page.

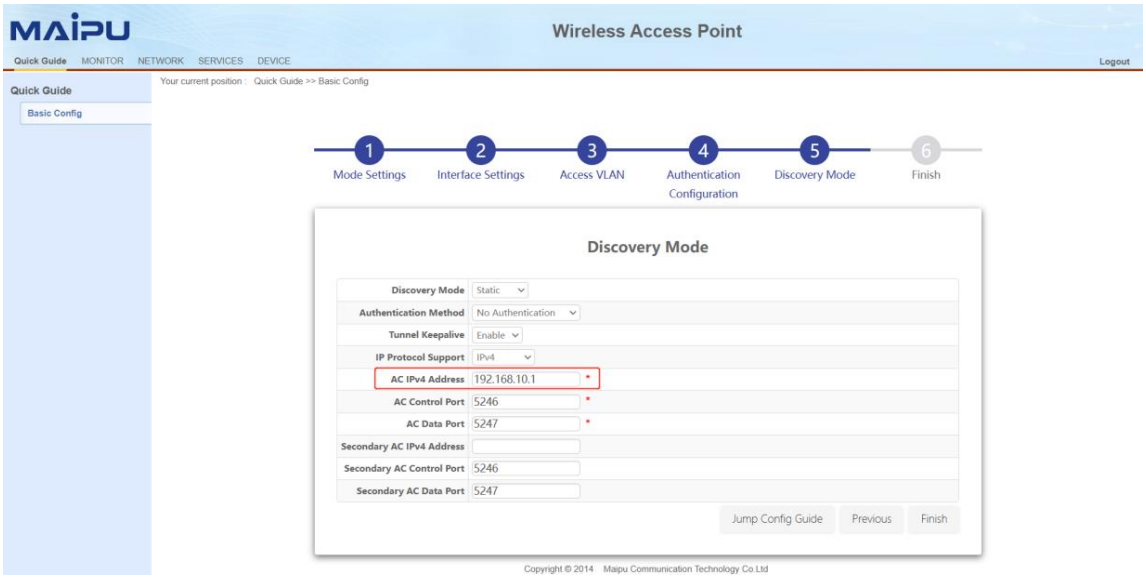


Figure 5.17 AP Configuration Wizard

4. AC configuration

copyright ©Maipu, all rights reserved

#Create vlan10 and vlan100 on the AC, and create the corresponding vlan10 interface, which is used to establish a CAPWAP tunnel with the AP; configure the link type of gigabitethernet0/1 connected to SW2 to access, and vlan to10.

```
AC # con t
AC(config)#vlan10,100
Please wait.....
Done.
AC(config)#
AC(config)#interface vlan10
AC(config-if-vlan10)# ip address192.168.10.124
AC(config-if-vlan10)# exit
AC(config)#interface gigabitethernet 0/1
AC(config-if-gigabitethernet0/1)# switchport mode access
AC(config-if-gigabitethernet0/1)# switchport access vlan10
```

#After completing the above configuration, wait for about two minutes, the AP can successfully connect to the AC, and you can check the status of the AP on the AC. Enter http://192.168.10.1 in the IE browser of the PC to jump to the login page, as shown in the figure below. Enter the user name and password, and click the <Login> button to log in.

Figure 5.18 AC login page

#Click MONITOR > AP List, and you can see that the AP is online, as shown in the figure below.

copyright ©Maipu, all rights reserved

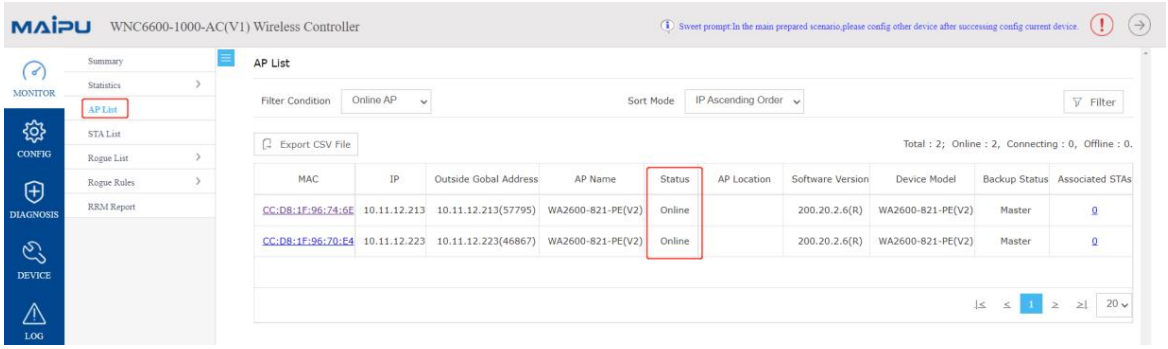
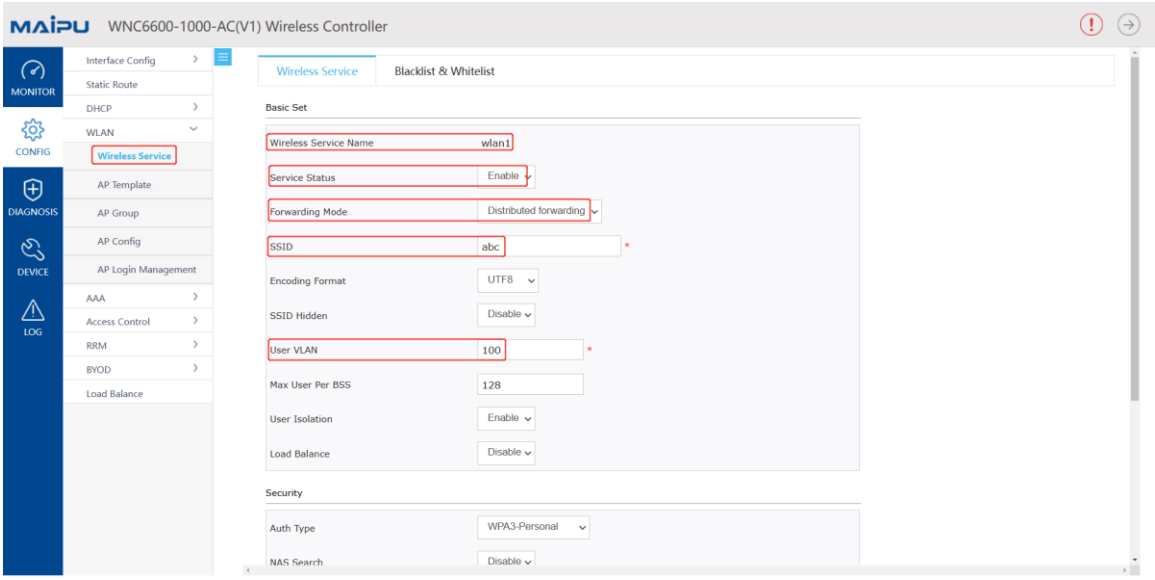


Figure 5.19 AP list

#Create a wireless service set. Click CONFIG > WLAN > Wireless Service, create a wireless service set, as shown in the figure below, the wireless name is wlan1, select “Enable” for service status, select "distributed forwarding" for forwarding mode, configure SSID as abc, configure user VLAN to100, select wpa3-personal as the authentication method, set the mode to compatible mode (compatible mode means that when the terminal does not support wpa3-personal authentication, it can be backward compatible with wpa2-personal authentication access), password key phrase is12345678, other configuration adopts the default value, and click the <OK> button to complete the configuration of the wireless service set.



copyright ©Maipu, all rights reserved

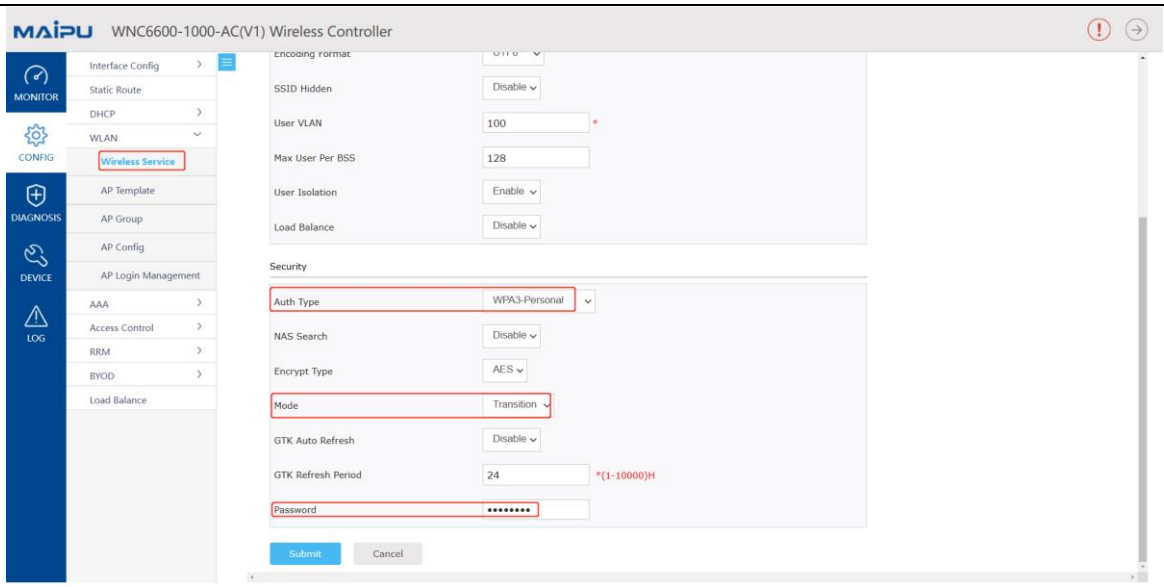


Figure 5.20 Wireless service configuration

#Bind the wireless service set to the AP template. Click CONFIG > WLAN > AP Template to create an AP template. By default, the name of the AP template is Default_FitAP_Profile, which can be changed, and the name cannot be changed after creation, as shown in Figure2.7, create a new profile and name it profile1.

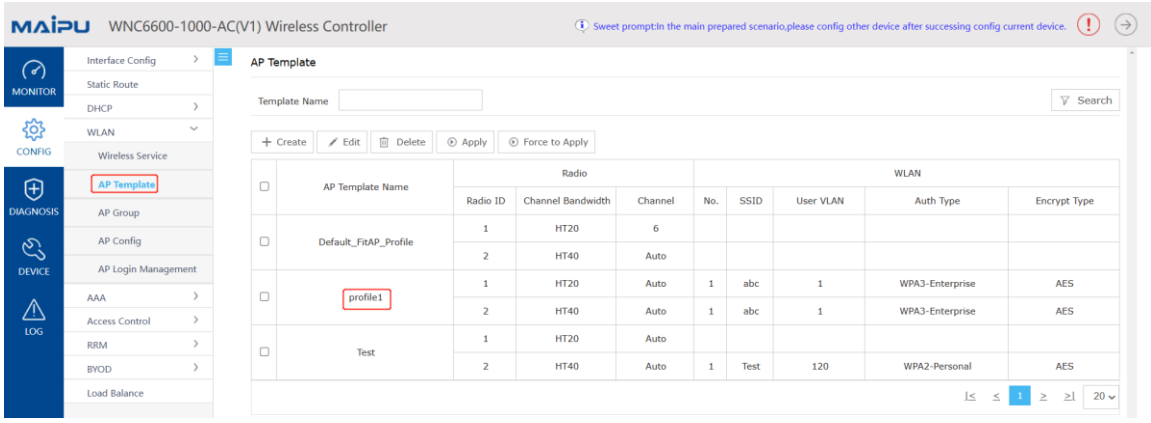


Figure 5.21 AP template

#Select the created AP template profile1, click the Edit button, click BSS > Wireless Service Name, select wlan1 created above, select ALL for Radio ID, and use default values for other configurations, and click <OK> button to complete AP template configuration.

copyright ©Maipu, all rights reserved

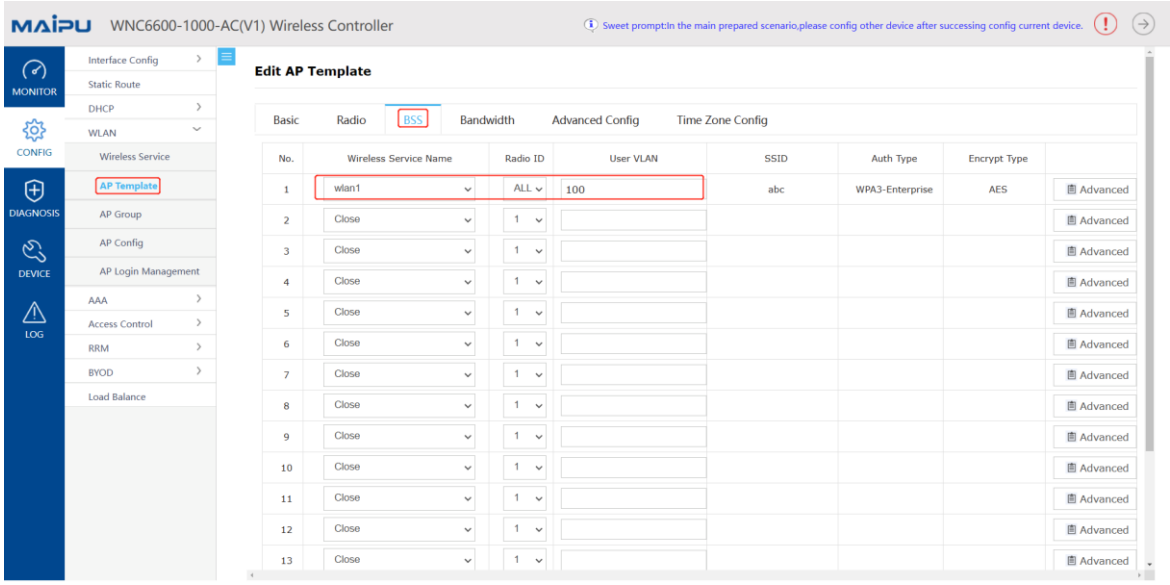


Figure 5.22 AP profile BSS configuration

#AP template application. Click CONFIG > WLAN > AP Config, select the connected AP, select profile1 in the AP template, and then click Apply in the template application.

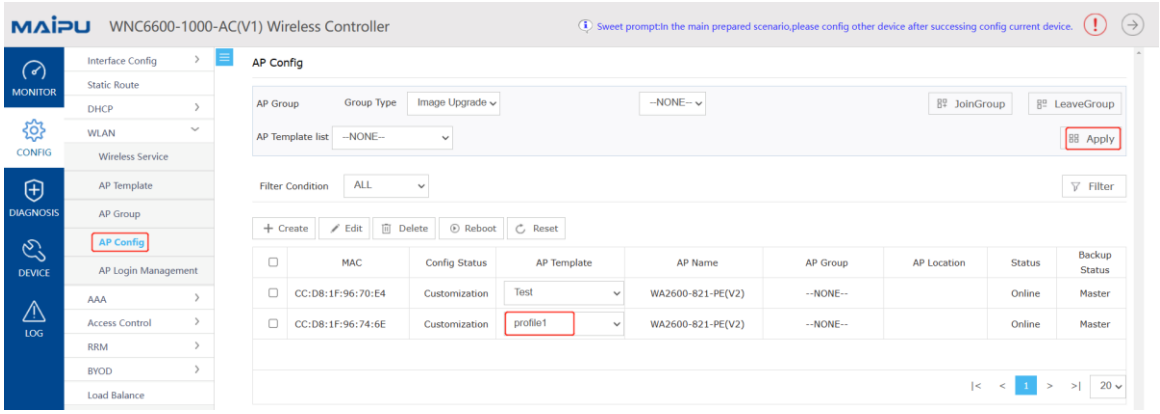


Figure 5.23 AP template application

5.2.5 Result Verification

#Wireless terminal access, after applying the AP template, after two minutes, turn on the wifi of the wireless terminal, and you can search for the wireless signal abc, after connecting to abc, on the AC web page, click MONITOR > STA List, and you can see the information of the wireless terminal.

copyright ©Maipu, all rights reserved

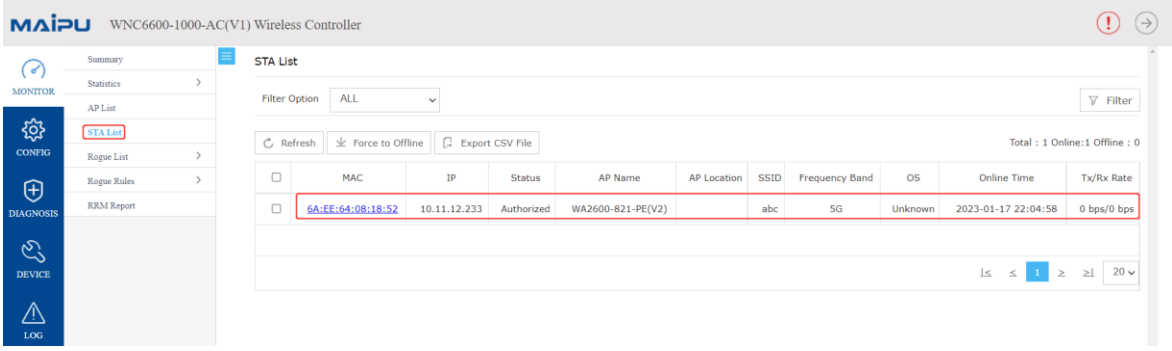


Figure 5.24 Terminal list

Note

- In addition to the BSS configuration, the AP template also needs to configure the working signal and channel bandwidth of the AP according to the actual network environment. The working channels of the2.4 G radio frequency generally choose1, 6, and11, and the channel bandwidth chooses HT20.
- The above example is based on 8 series APs (WA2600-821-PE(V2), WA2600-821-PE(V3), WA2600-815-PE(V2), WA2600-815-PE(V3)) as an example, so when configuring the BSS in the AP template, select all as the radio ID, and select1 as the radio ID for APs that only support 2.4G radio.
- The WPA3-personal authentication mode can be set to compatible mode and mandatory mode. Compatible mode means that when the terminal does not support wpa3-personal authentication, it can be backward compatible with wpa2-personal authentication access, and mandatory mode means that only the terminal that supports wpa3-personal authentication can be connected.

copyright ©Maipu, all rights reserved

6 Portal Server Escape

When the communication between the AC and the portal server is abnormal and normal portal authentication cannot be performed, to ensure that the original authenticated users can continue to surf the Internet normally and new users can access the network, the AC needs to support the portal server escape function.

The Portal server escape function is applicable to scenarios where user experience is prioritized over security authentication, because this function is only developed to meet the special needs of a small number of customers.

The escape function of the Portal server is implemented based on the keep-alive mechanism between Maipu AC and Maipu Portal server, so the registration and keep-alive functions need to be enabled in the portal redirection group. In addition, the default keep-alive packet sending cycle of the AC is 30s every time, which can be configured to 3s-3600s according to the needs, as shown in Figure 5.1.

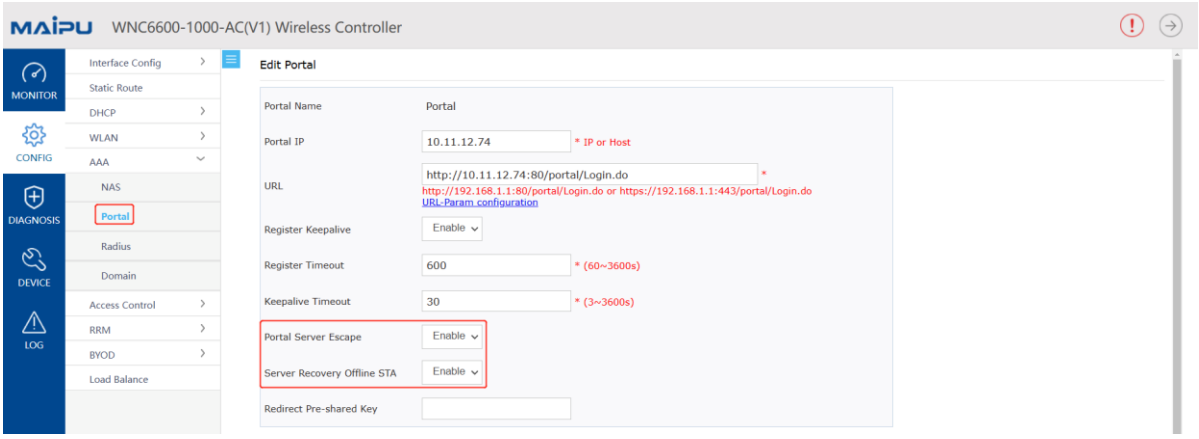


Figure 5.1 portal server registration and keepalive

copyright ©Maipu, all rights reserved

7 Portal Rule Group

7.1 Introduction to Portal Rule Group

Different actions and different types of rules can be configured under the Portal rule group, including permit, redirect, and CNA rules.

A. Configure the permit rule so that the terminal can access the network resources in the permit rule no matter whether it passes the portal authentication or not.

B. Configure the redirect rule so that no matter whether the terminal passes the portal authentication or not, it will redirect to the portal authentication page when accessing the network resources in the redirect rule.

C. Configure the CNA rules so that after the STA of the IOS system accesses the wireless network, the portal authentication page will pop up automatically, and the device displays the WiFi icon. Without portal authentication, the wireless network will not be disconnected.

7.2 Configure permit Rule Group

Select the portal rule group in the portal configuration and click Create to add a new portal rule group, as shown in Figure 6.1.

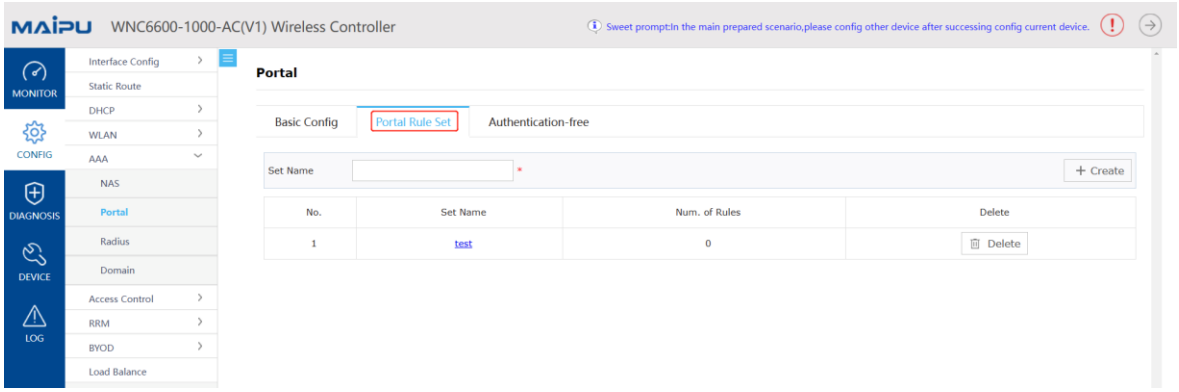


Figure 6.1 Create a portal rule group

Click Create, and the action is the permit rule. The supported configuration types are HOST, IP, NET, and URL. Select a type, enter the address, click OK, and a permit rule is successfully created, as shown in Figure 6.2.

copyright ©Maipu, all rights reserved

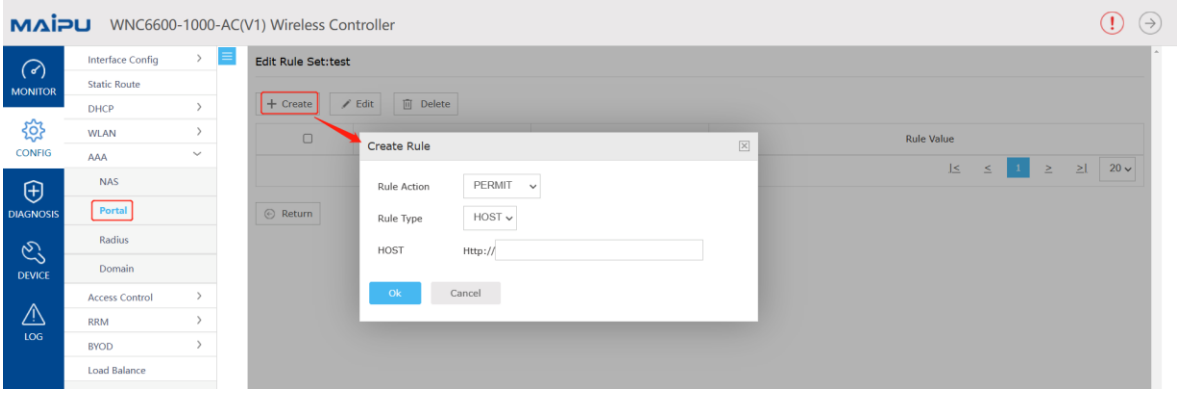


Figure 6.2 Configure the permit rule group

7.3 Configure redirect Rule Group

The configuration type supported by the action redirect rule is IP, as shown in Figure 6.3.

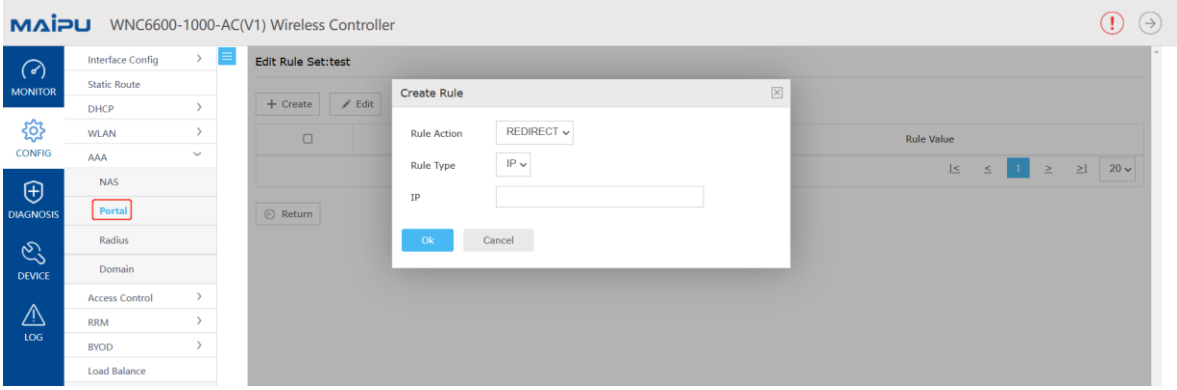


Figure 6.3 Configure redirect rule group

7.4 Configure CNA Rule Group

The configuration type supported by the action CNA rule is URL, as shown in Figure 6.4.

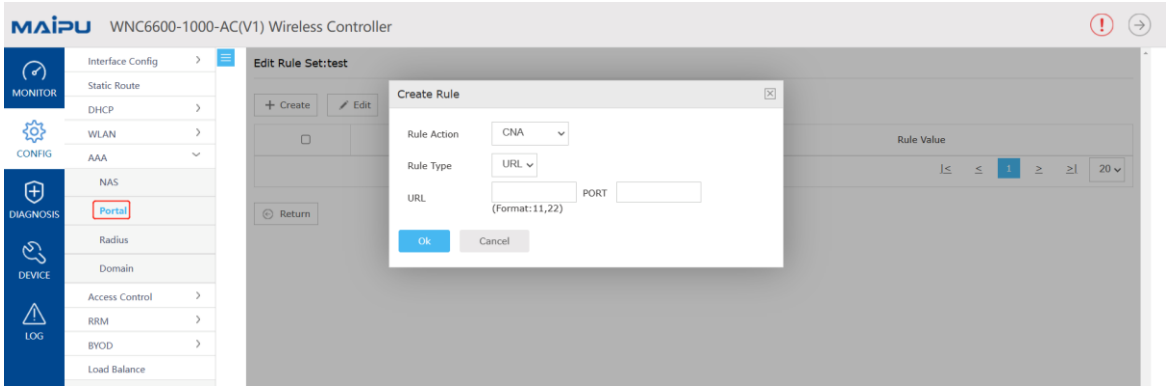


Figure 6.4 Configure CAN rule group

Currently configure CNA rules, and add the following addresses:

copyright ©Maipu, all rights reserved

captive.apple.com

www.airport.us

www.ibook.info

www.thinkdifferent.us

www.appleiphonecell.com

www.itools.info

7.5 Apply portal Rule Group

Before applying the portal rule group, you need to configure the portal authentication first, then create a new service set, select portal authentication, add the above configured portal rule group, and then it can be successfully applied, as shown in Figure 6.5.

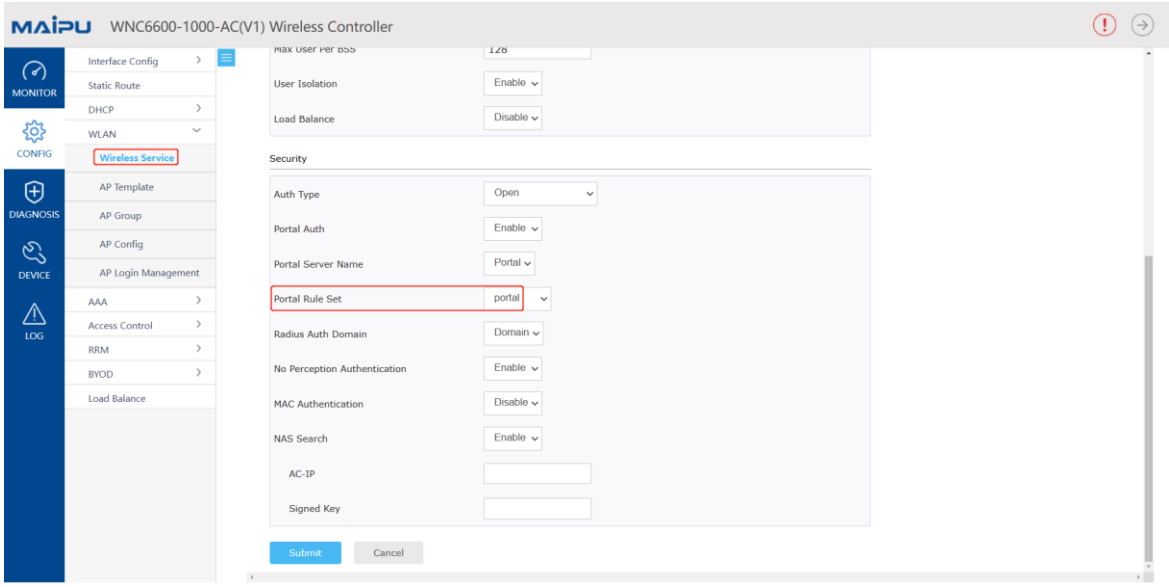


Figure 6.5 Apply portal rule group

copyright ©Maipu, all rights reserved

8 Channel and Power Auto Adjustment

8.1 Configure AP Scanning Group

For channel adjustment and power adjustment, you need to create an AP scan group first, as shown in Figure 7.1 and 7.2.

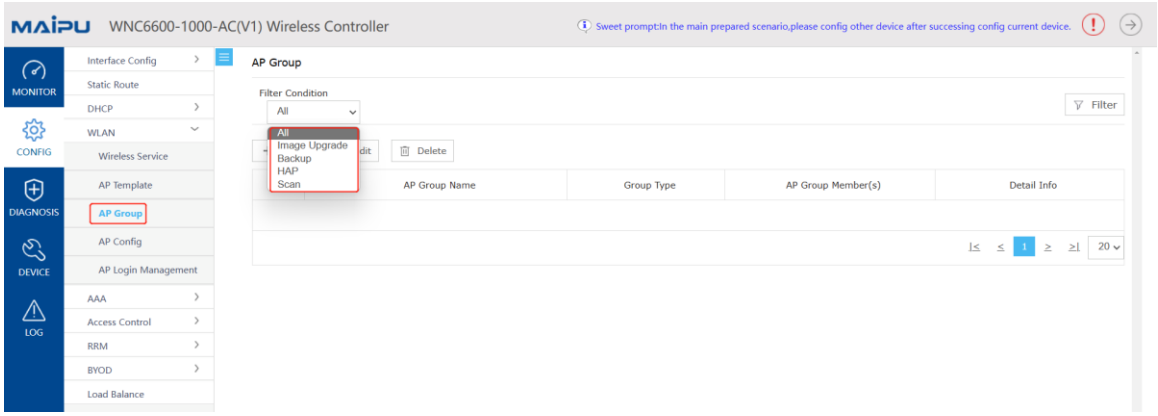


Figure 7.1 Create an AP scanning group

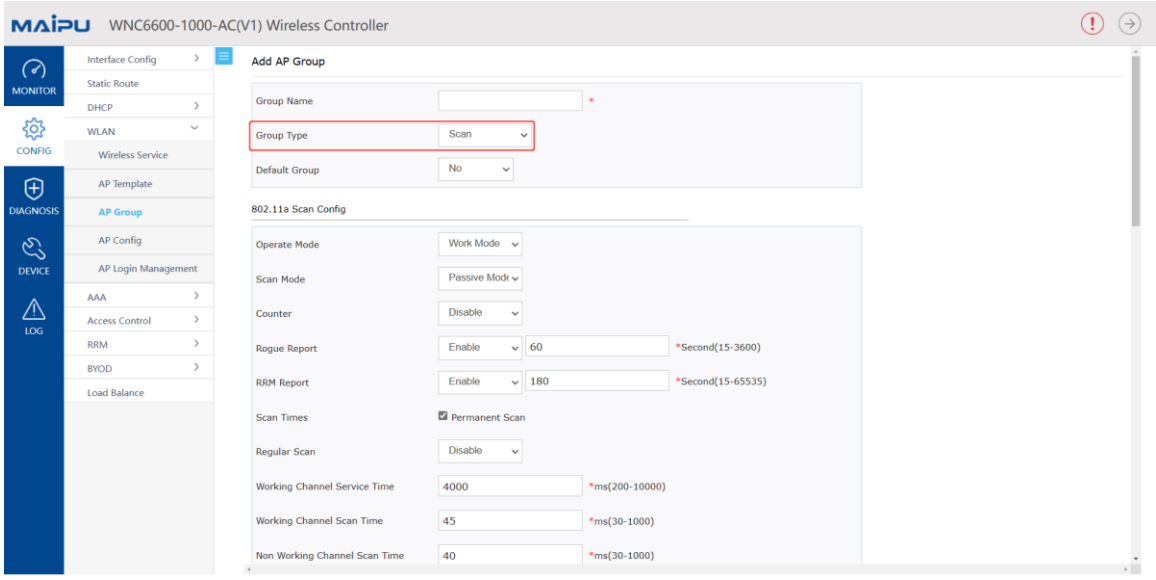


Figure 7.2 Configure AP scanning group

Introduction to some functions:

A. "Scan mode": In passive mode, only Beacon frames are passively accepted, and in active mode, STA will actively send probe request to detect the surrounding wireless environment;

B. "Rogue Counter": If you need to counter phishing AP, please turn on this option;

C. "Channel Set": select the channel to be scanned;

copyright ©Maipu, all rights reserved

D. "Neighborhood OUI": The default configuration is OUI "00017A" and "ccd81F" of Maipu equipment;

E. "Regular scan": provide scanning services within a specified time period;

F. "Default group": When the AP group is configured as the default group, all APs that have not joined the group will automatically join the group, and new online APs will also automatically join the default group (all types of AP groups can be configured as the default group).

After performing the scanning configuration of 2.4G and 5G respectively, click "OK" to complete the creation of the scanning group.

8.2 Add AP to Scan Group

Enter the "AP Configuration" page, and add the corresponding AP to the scanning group, as shown in Figure 8.3.

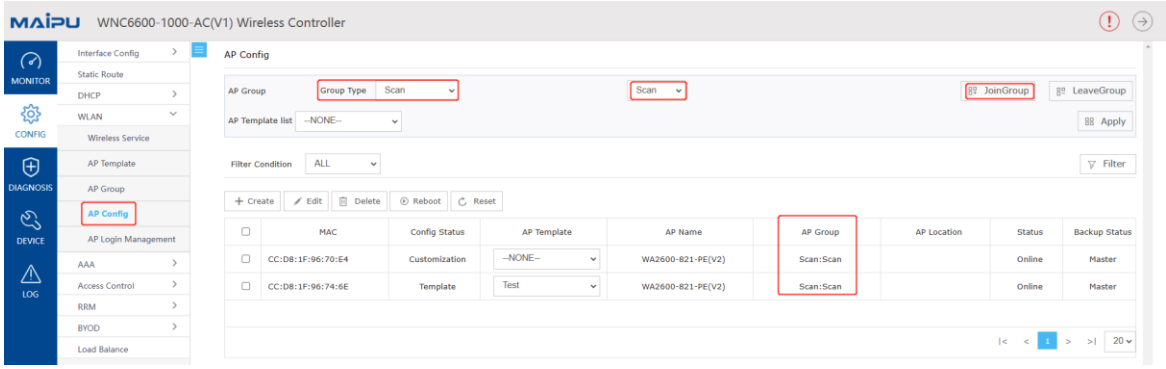


Figure 7.3 Adding APs to the scanning group

8.3 Auto Power Adjustment

Click "CONFIG" -> "RRM" -> "TPC" to configure related parameters of power adjustment, as shown in Figure 7.4.

copyright ©Maipu, all rights reserved

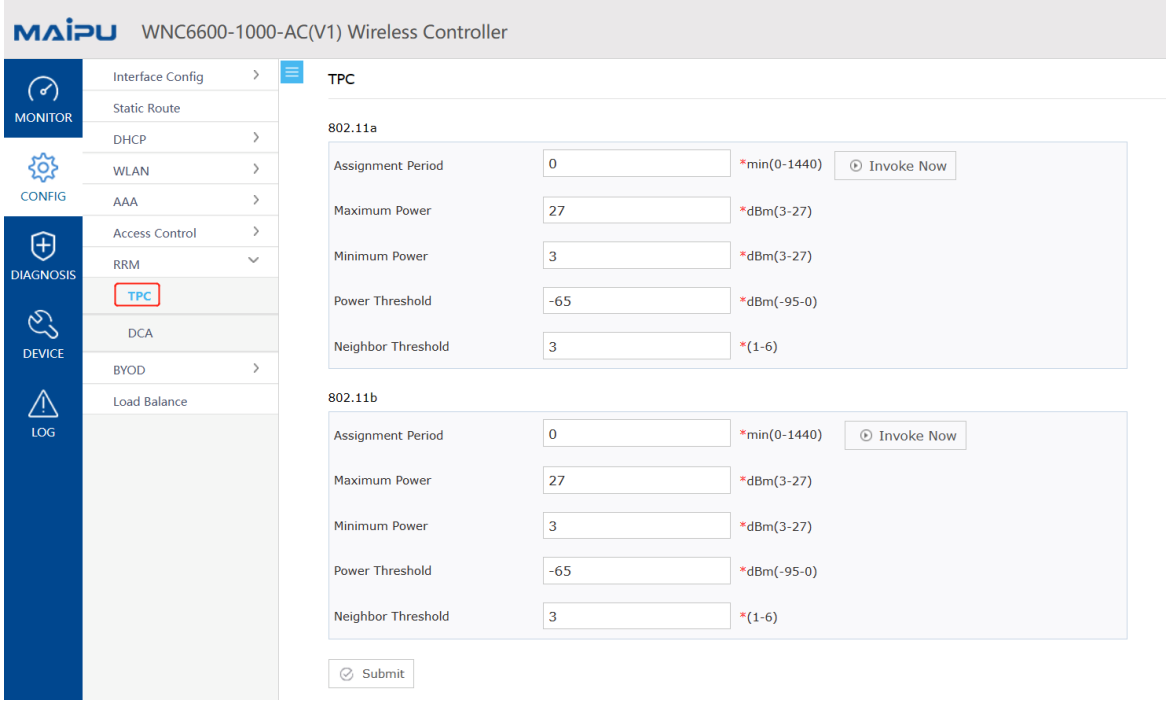


Figure 7.4 Configuring automatic power adjustment

8.4 Auto Channel Adjustment

Channel auto adjustment configuration is shown in Figure 7.5.

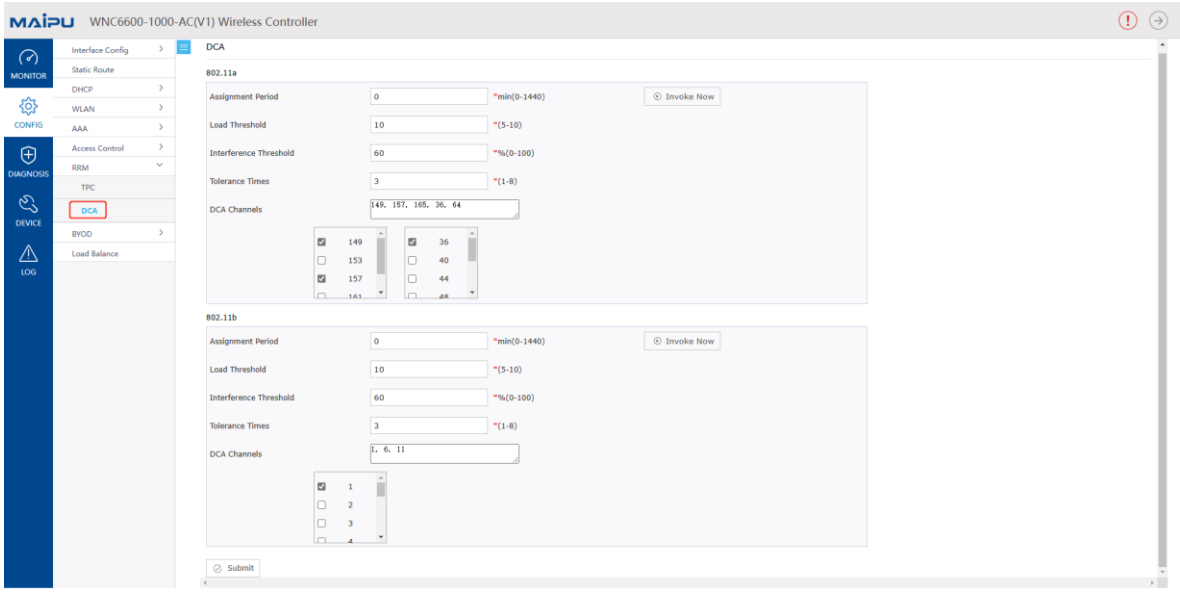


Figure 7.5 Configure auto channel adjustment

Note

- Since the AP cannot work and scan at the same time, and the user connection will be disconnected when the channel is switched, the above two functions are recommended

copyright ©Maipu, all rights reserved

to be used only in the initial stage of site survey or network deployment.

- The channel set selected here refers to the adjustable channel set, and only the selected channels will be adjusted during the automatic adjustment process.

copyright ©Maipu, all rights reserved

9 Illegal (Phishing) AP Detection and Countermeasures

When an AP not managed by the current AC broadcasts the same SSID as the AP managed by the current AC, the AP is regarded as an illegal AP and generally called a Rogue AP. Rogue device detection can monitor abnormal devices in the entire WLAN network, and countermeasures can be taken after Rogue devices are detected.

9.1 Create an AP Scanning Group

Please refer to the configuration of 7.1 to enable Rogue countermeasures in the scanning group.

9.2 Add AP to Scan Group

Please refer to the configuration of 7.2.

9.3 Configure Rogues Rules

9.3.1 Configure Friendly Rules

The friendly rules include a list of friendly BSSIDs, a list of friendly OUIs and SSIDs, and a list of friendly STAs. Configure the devices in friendly rules not to be countered under any circumstances, as shown in Figure 8.1.

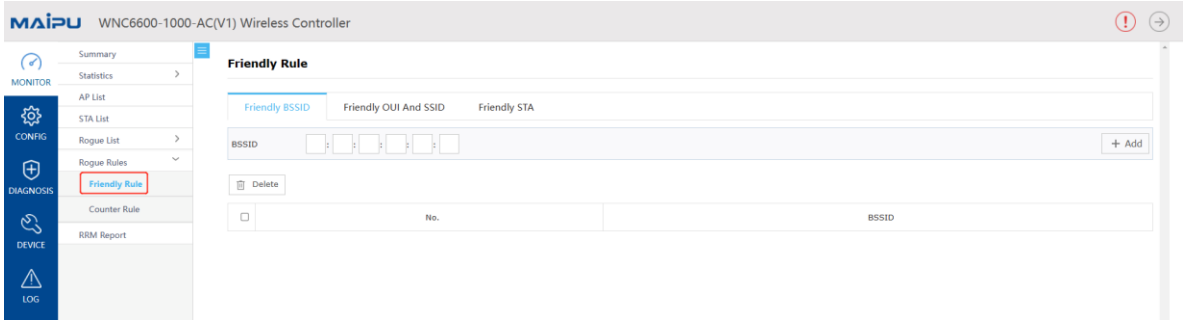


Figure 8.1 Configure friendly rules

Note

- The friendly OUI list and the friendly SSID list need to be used together, and take the

copyright ©Maipu, all rights reserved

intersection of the two.

9.3.2 Configure Counter Rules

1. Configure counter type

Counter types include unclassified devices, phishing devices, suspected phishing devices, static counter devices, and jamming devices. These five types of devices can be countered, as shown in Figure 8.2.

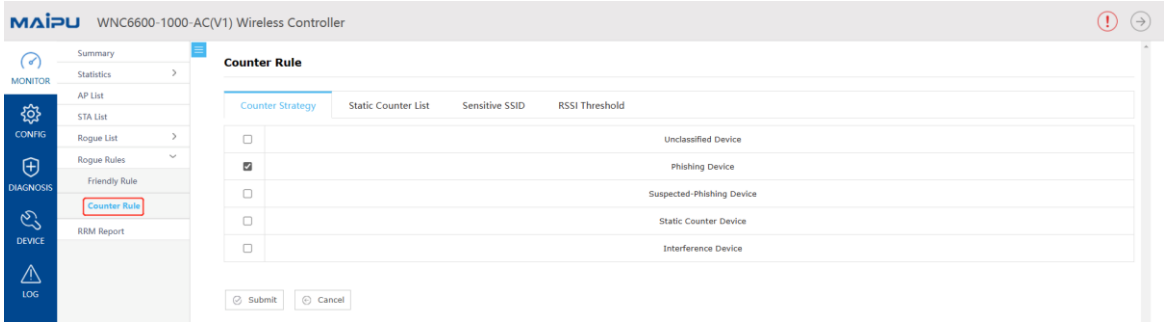


Figure 8.2 Configure counter type

2. Configure static counter list

Configure the BSSID to be countered in the static counter list, and then counter it according to its counter type, as shown in Figure 8.3.

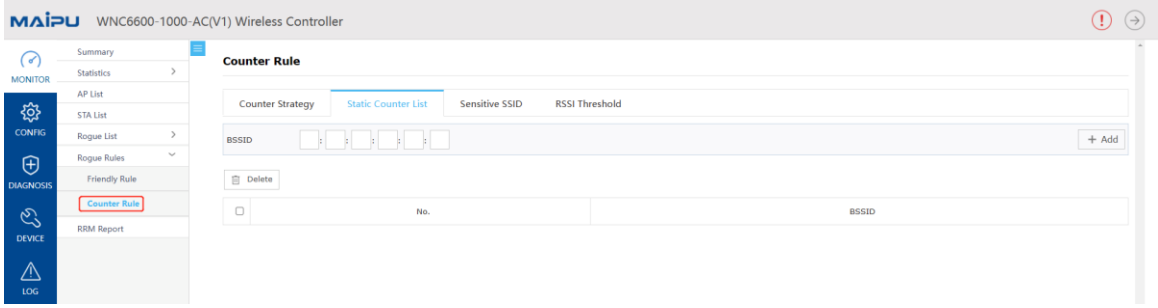


Figure 8.3 Configure static counter list

3. Configure sensitive SSID list

After the sensitive SSID list is configured, as long as an SSID matches the corresponding characters in the sensitive SSID list, it will be countered, and its SSID name will also appear in the countered list, as shown in Figure 8.4 and 8.5.

copyright ©Maipu, all rights reserved

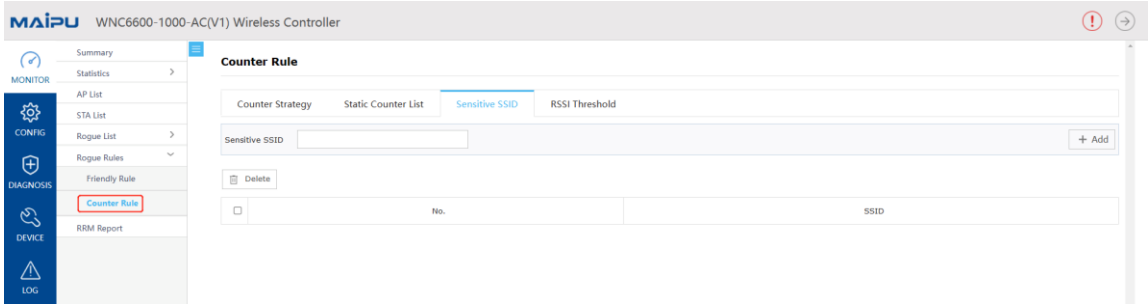


Figure 8.4 Configure sensitive SSID list

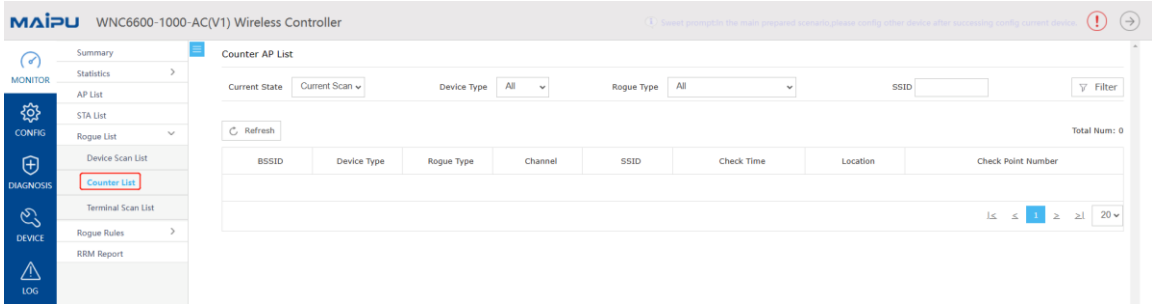


Figure 8.5 View AP counter list

4. Configure the RSSI threshold

After the RSSI threshold is configured, when the power of other wireless access devices in the environment is greater than the configured RSSI threshold, it will be added to the counter list and countered, as shown in Figure 8.6.

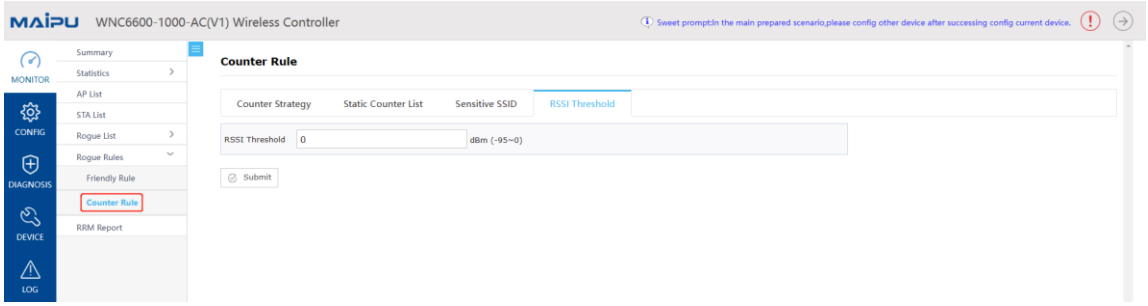


Figure 8.6 Configure RSSI Threshold

9.3.3 List of Rogues

This module can view the device scan list, counter list and terminal scan list.

In the device scanning list, you can view the BSSIDs in the surrounding environment, and can easily add them to the friendly BSSID list or static counter list, as shown in Figure 8.7. Device type filtering provides three types: AP, ADHOC, and bridge; Rogue type filtering provides six types: unclassified device, phishing device, suspected phishing device, friendly device, static counter device, and interference device.

copyright ©Maipu, all rights reserved

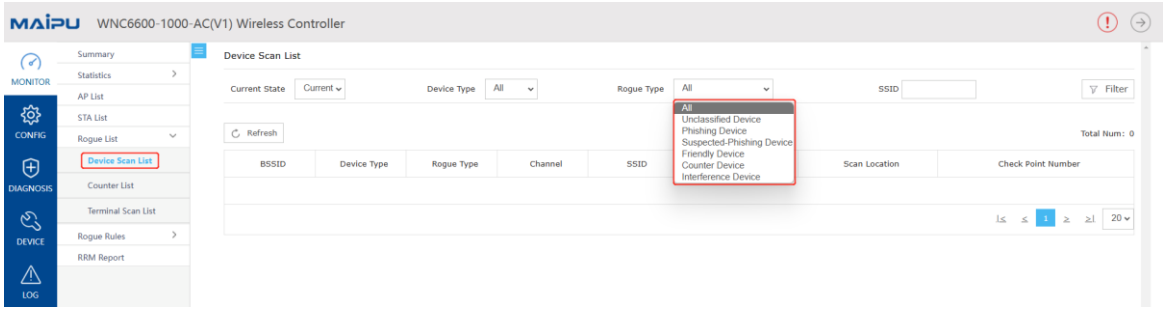


Figure 8.7 Device scan list

In the counter list, you can view all countered devices, providing information including device type, Rogue type, channel, SSID, etc., as shown in Figure 8.8.

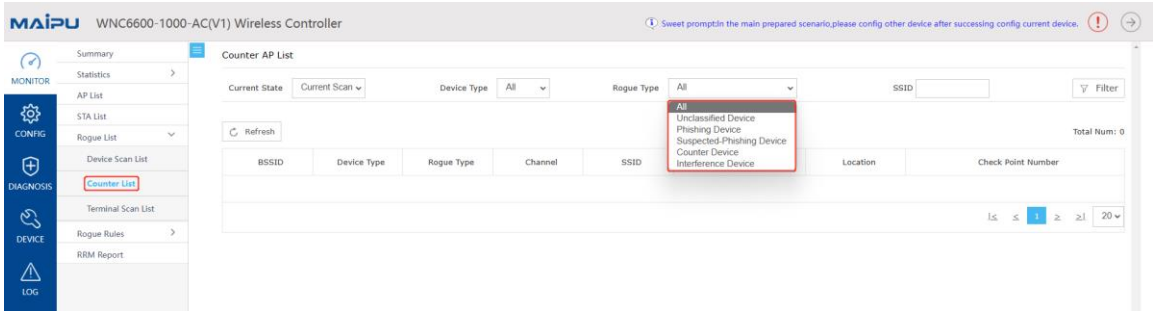


Figure 8.8 Counter list

In the terminal scanning list, you can view the terminals existing in the surrounding environment, and provide information including terminal MAC address, Rogue type, BSSID, etc., as shown in Figure 8.9.

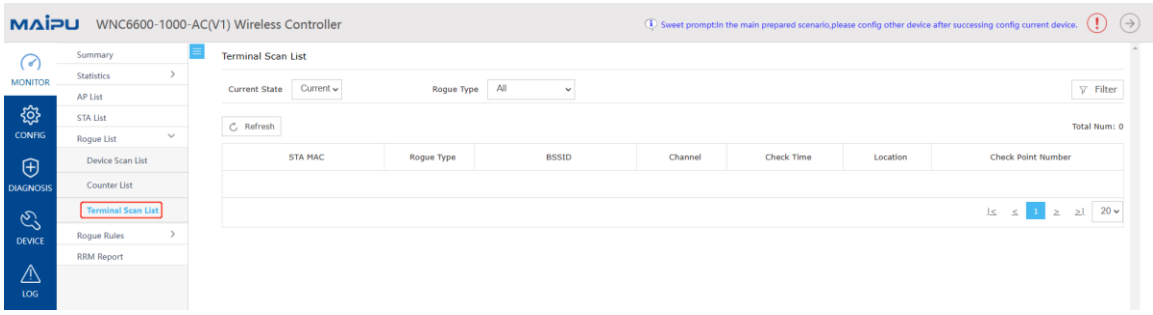


Figure 8.9 Terminal scan list

9.4 RRM Reporting

Please refer to the configuration in 7.1 to enable RRM reporting in the scanning group, and then add the corresponding APs to the scanning group. You can view the reported information in the RRM report, as shown in Figure 8.10.

copyright ©Maipu, all rights reserved

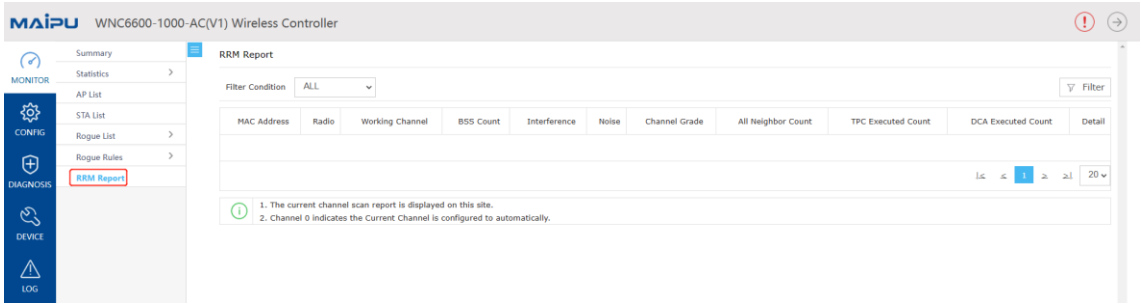


Figure 8.10 RRM reporting

copyright ©Maipu, all rights reserved

10 ACL Function Configuration

ACL can be called an access control list, also known as an access list, ACL controls the packets on the interface of the network device by defining a series of rules: allow to pass or discard, ACL is composed of a series of entries; these entries are called access control list entries ACE, according to different applications associated with wireless ACLs, they can be divided into two types:

1. Wireless AP ACL: Applied to the WLAN interface to filter and control the WLAN data.
2. Wireless BYOD ACL: used in conjunction with the BYOD STA control list to filter and control the corresponding STAs.

10.1 AP ACLs

10.1.1 Create Policy Set

Configure AP ACL in wireless access control, as shown in Figure 9.1.

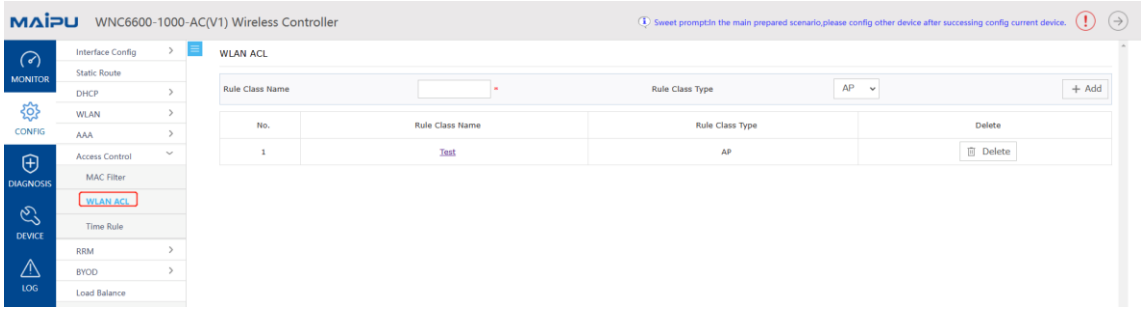


Figure 9.1 Create an AP ACL policy set

Create ACL rules in the created policy set. "Allow, Disable" in the default policy on this page means that the default policy will be matched when all the configured ACL rules are not matched, as shown in Figure 9.2.

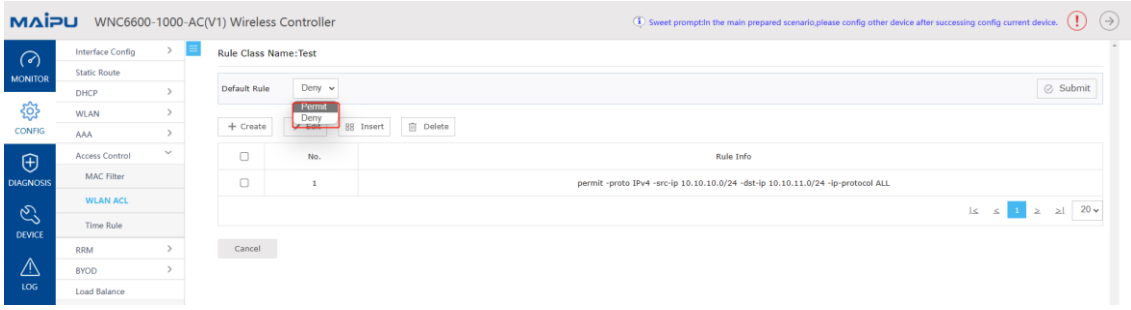


Figure 9.2 Create ACL rules

copyright ©Maipu, all rights reserved

Multiple policies can be created in each policy set, as shown in Figure 9.3.

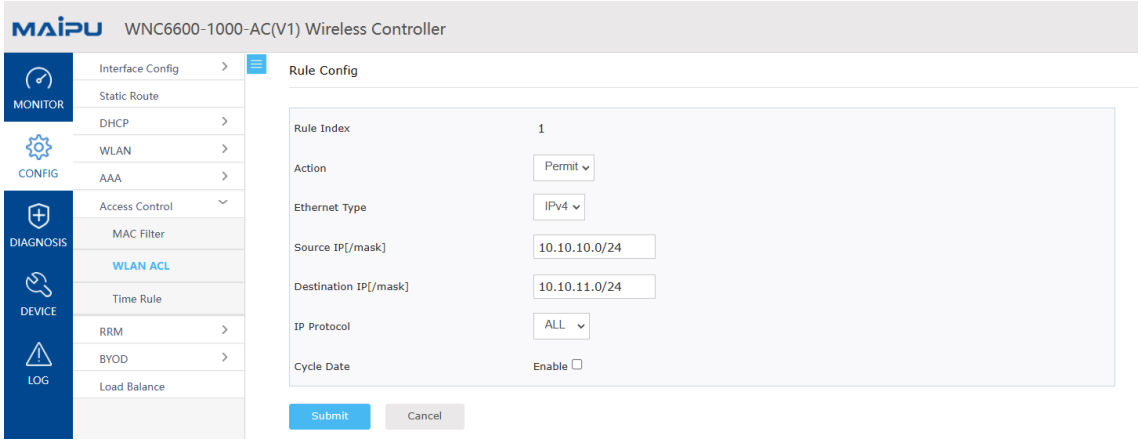


Figure 9.3 Create AP ACL rules

10.1.2 Application of Policy Sets

In the AP template or AP configuration, enter the BSS configuration, select "Advanced", and reference the above policy set in the "WLAN ACL", as shown in Figure 9.4.

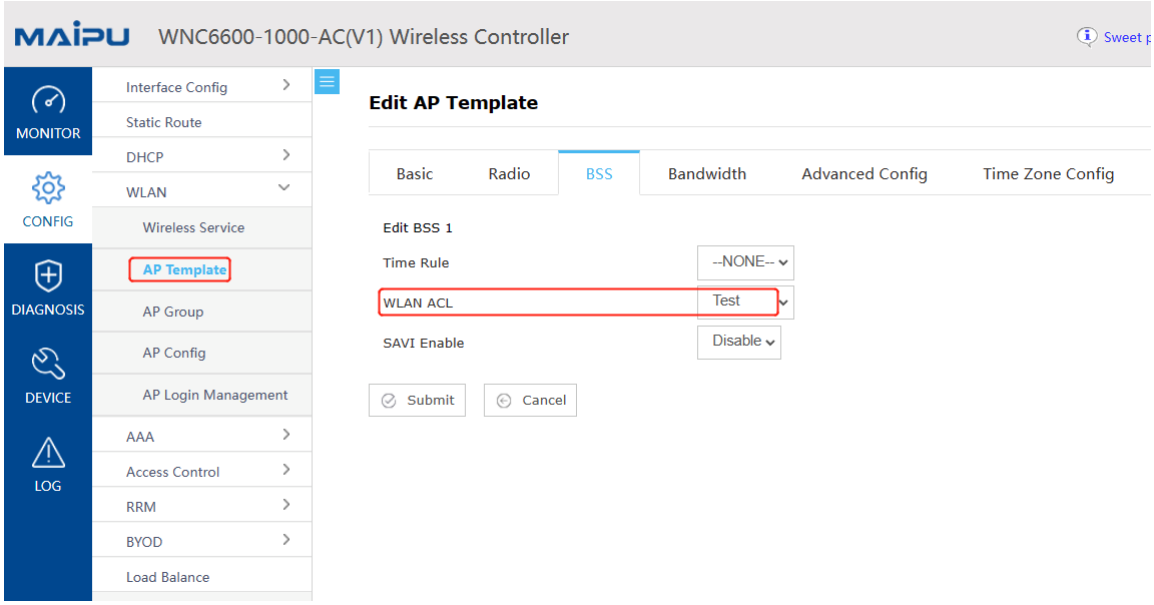


Figure 9.4 Apply AP ACL policy set

10.2 BYOD ACLs

10.2.1 Overview of BYOD ACLs

The BYOD (Bring Your Own Device) feature implements device identification (operating system identification) for dynamically online terminals and delivers NAC policies. The active function of WLAN

copyright ©Maipu, all rights reserved

ACL is to control the flow of wireless packets. The combination of Byod and Wlan ACL features, that is, on the basis of WLAN ACL, adding filtering rules to identify wireless packets according to device roles, making the control of smart terminals richer and more flexible.

10.2.2 Create Policy Set

To configure BYOD ACL in WLAN ACL, first create a BYOD ACL, as shown in Figure 9.5.

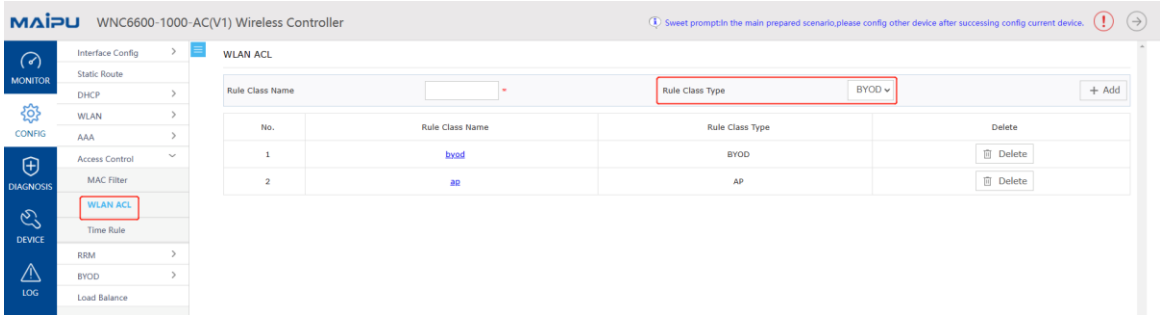


Figure 9.5 Create BYOD ACL policy set

The policy configuration is shown in Figure 9.6.

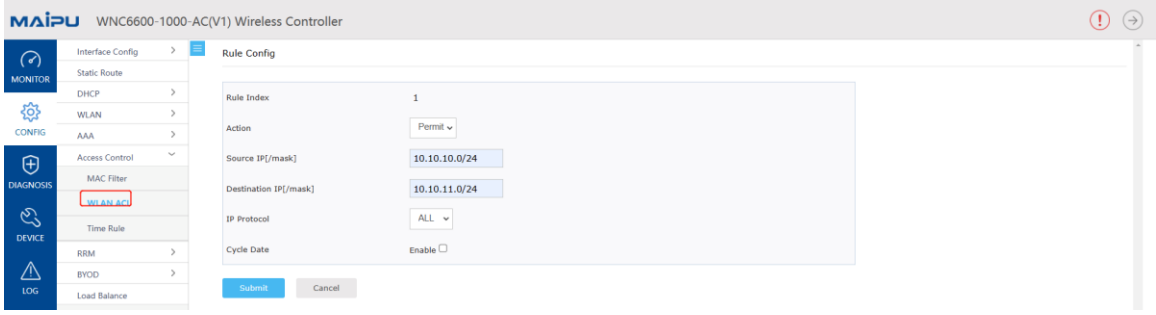


Figure 9.6 Configure BYOD ACL rules

10.2.3 Application of Policy Sets

Enter BYOD to reference the above policy set.

1. Apply policy set based on the operating system

Apply policy set in BYOD ACL in BYOD, as shown in Figure 9.7.

copyright ©Maipu, all rights reserved

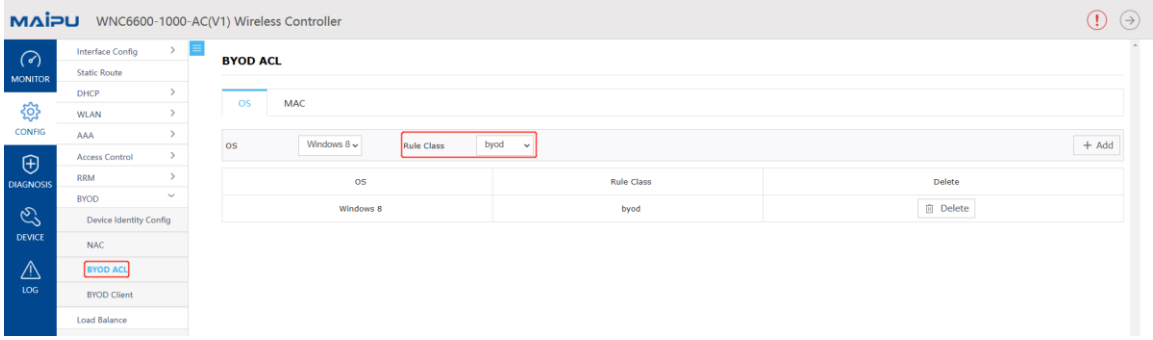


Figure 9.7 Apply policy set based on operating system

2. Apply policy set based on MAC address

Apply policy sets based on MAC addresses, as shown in Figure 9.8.

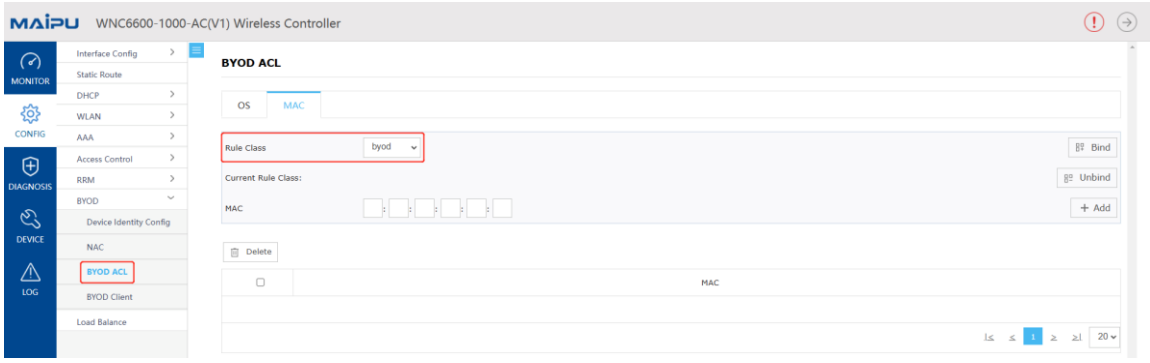


Figure 9.8 Apply policy set based on MAC address

copyright ©Maipu, all rights reserved

11 AP Unlimited Endurance (HAP Escape Technology)

11.1 Introduction to AP Unlimited Endurance

In the centralized management wireless network architecture of Fit AP+AC, if the AC goes down or the network between AC and AP is abnormal, the wireless network cannot continue to be used. Therefore, Maipu launched the "AP unlimited endurance" function to solve this problem. When this kind of problem occurs, old users will not get offline, and new users can continue to access. At the same time, if the AP restarts abnormally in this case, it can still meet the needs of new users to continue accessing.

11.2 Networking Requirements

The AP unlimited endurance technology can only be used in local forwarding networking, and requires that the DHCP server cannot be built on the AC.

11.3 Create a HAP AP Group

Create a HAP group in the AP group, as shown in Figure10.1.

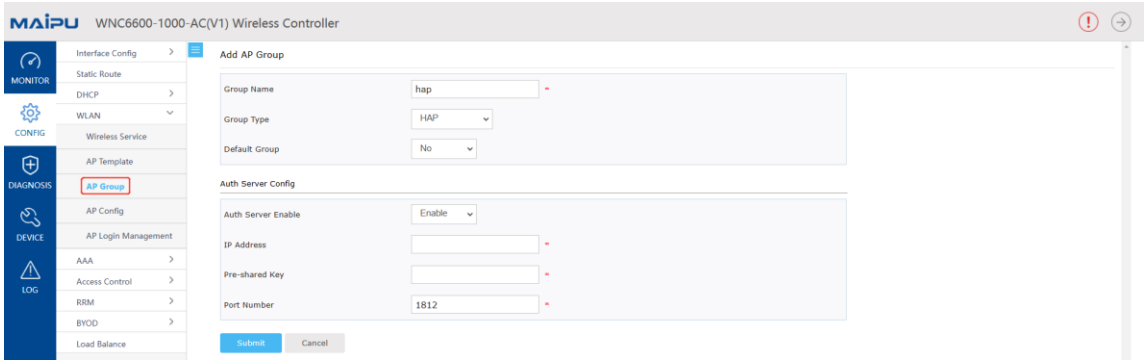


Figure10.1 Create a HAP group

Authentication server configuration: It is the same as the authentication configuration of AC.

copyright ©Maipu, all rights reserved

12 Timing Policy Configuration

12.1 Introduction to Timing Policy

The timing policy refers to the policy control of AP, Radio, BSS, etc. according to the time domain or time point information. The following policies are mainly supported:

A. Restart the AP, Radio, etc. at a specific time.

B. Enable or disable Radio and BSS services within a specific period of time.

12.2 Configure AP to Restart Regularly

In the time rule of access control, select a time point and click Create to create a time point table, as shown in Figure11.1 and11.2.

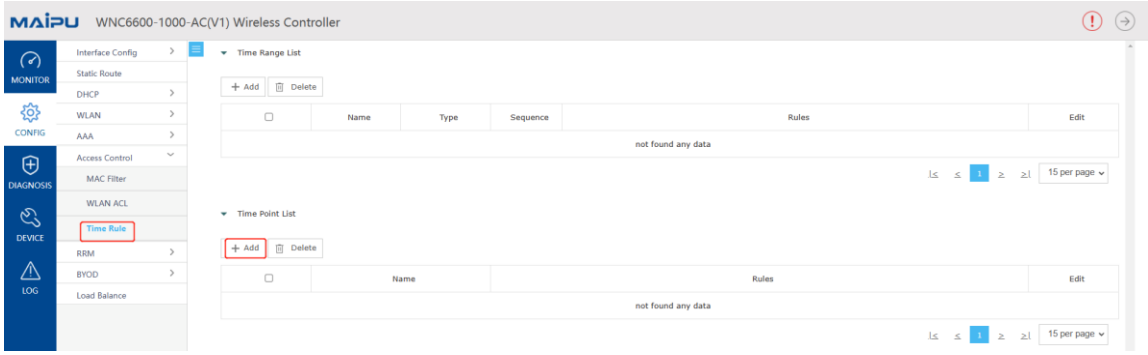


Figure11.1 Create time point table

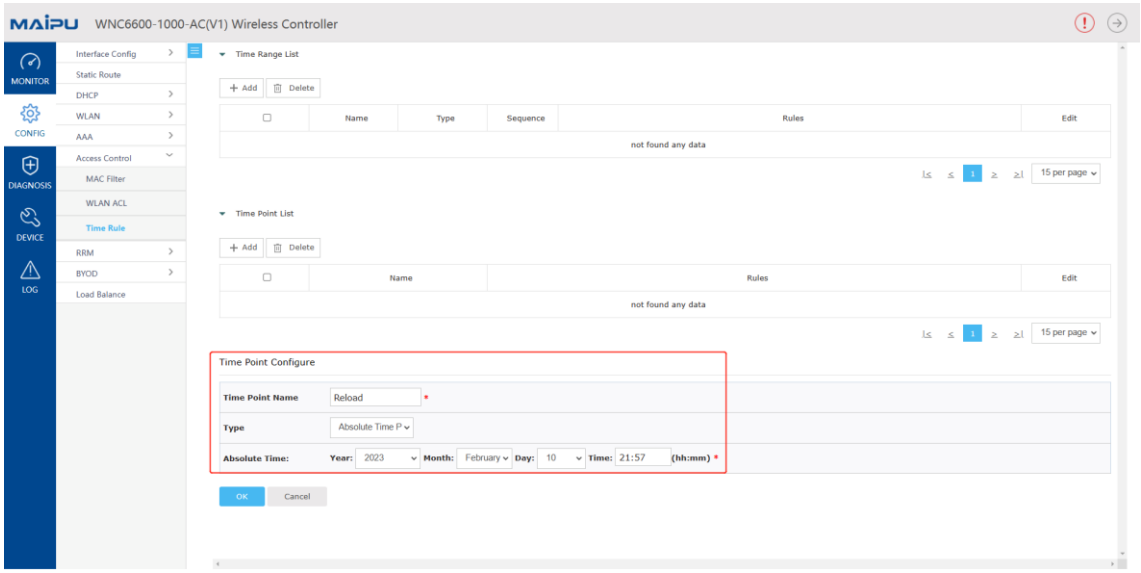
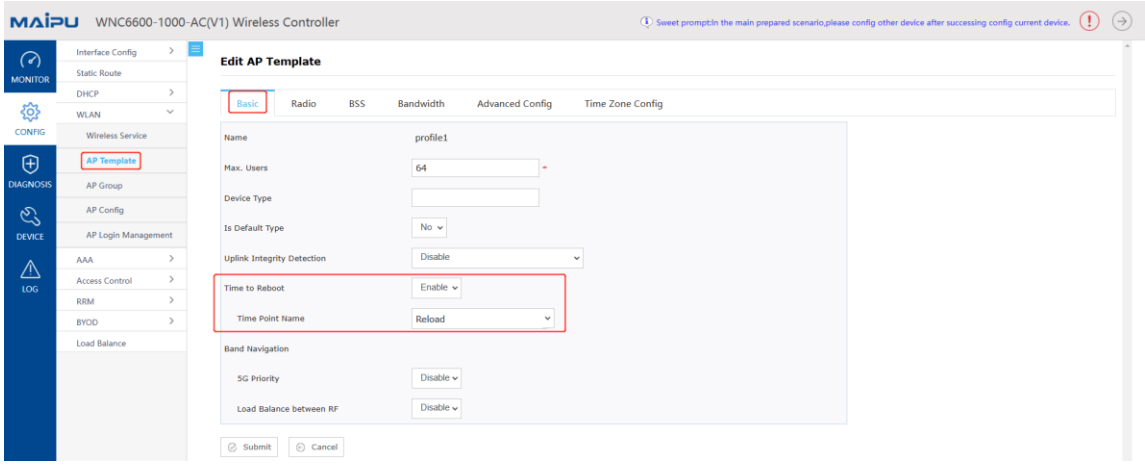


Figure11.2 Configuration time point table

copyright ©Maipu, all rights reserved

In the AP template or AP configuration, the time point policy established above can be applied in the basic configuration of the AP, as shown in Figure11.3.



the s

Figure11.3 AP timing restart

12.3 Configure a Scheduled Radio Restart

Establish a time point policy. The method is the same as that of creating the time point table in 11.2. In the AP ttemplate or AP configuration, the time point policy established above can be applied in the radio configuration, as shown in Figure11.4.

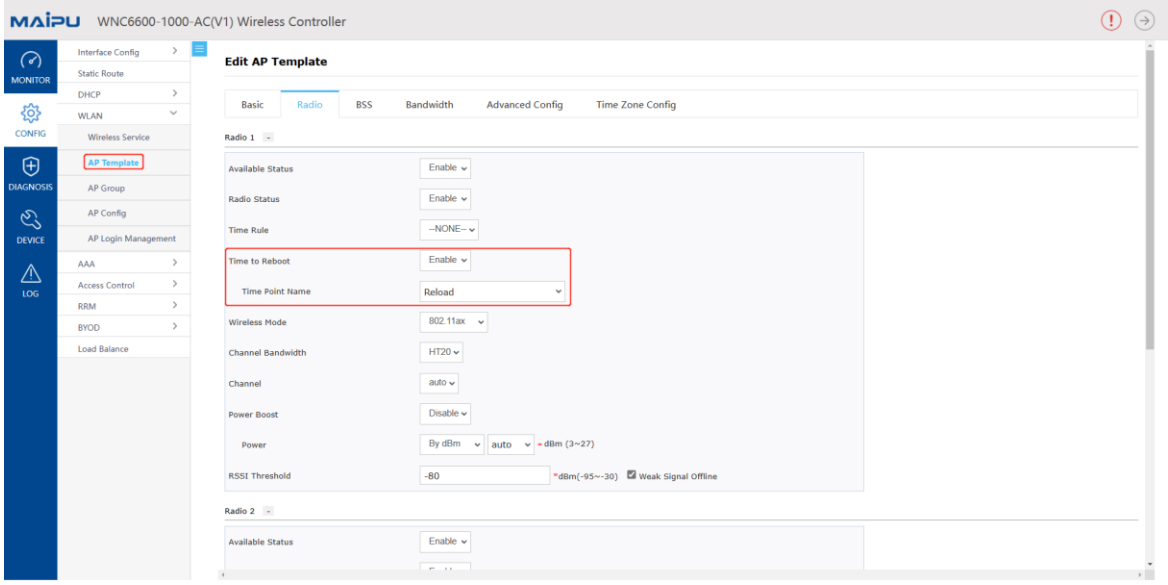


Figure11.4 RF timing restart

copyright ©Maipu, all rights reserved

12.4 Configure Radio Frequency to Enable in Time Range

In the time rule of access control, select the time domain and click Create to create the time domain table, as shown in Figure11.5 and11.6.

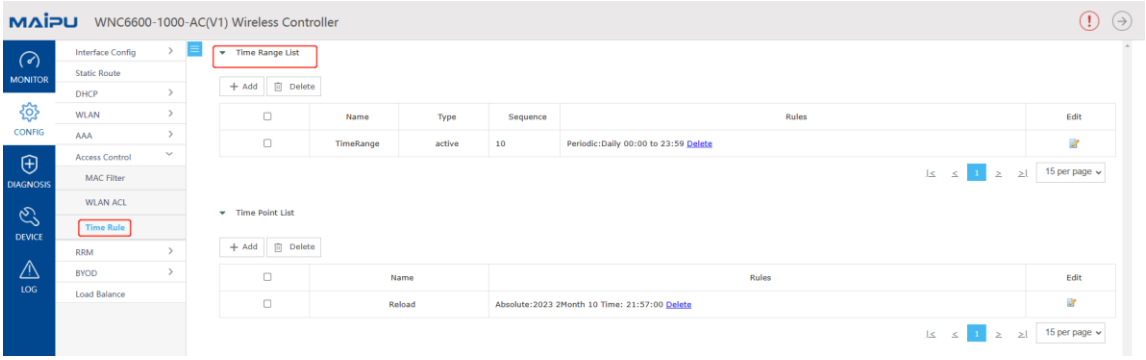


Figure11.5 Create a time domain table

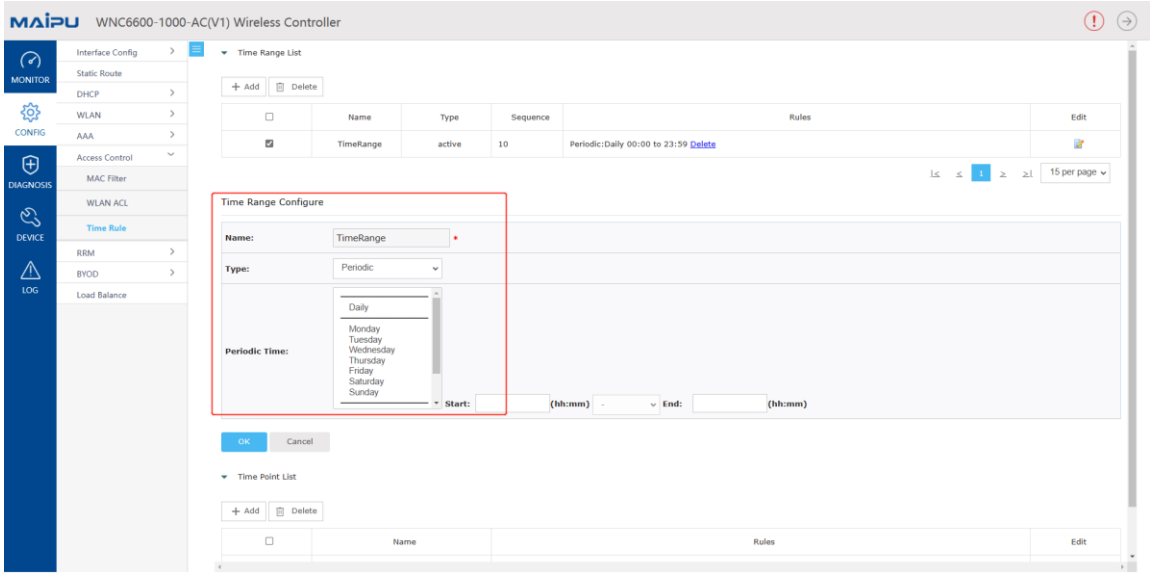


Figure11.6 Configure time domain table

In the AP template or AP configuration, the time domain policy established above can be applied in the radio configuration, as shown in Figure11.7.

copyright ©Maipu, all rights reserved

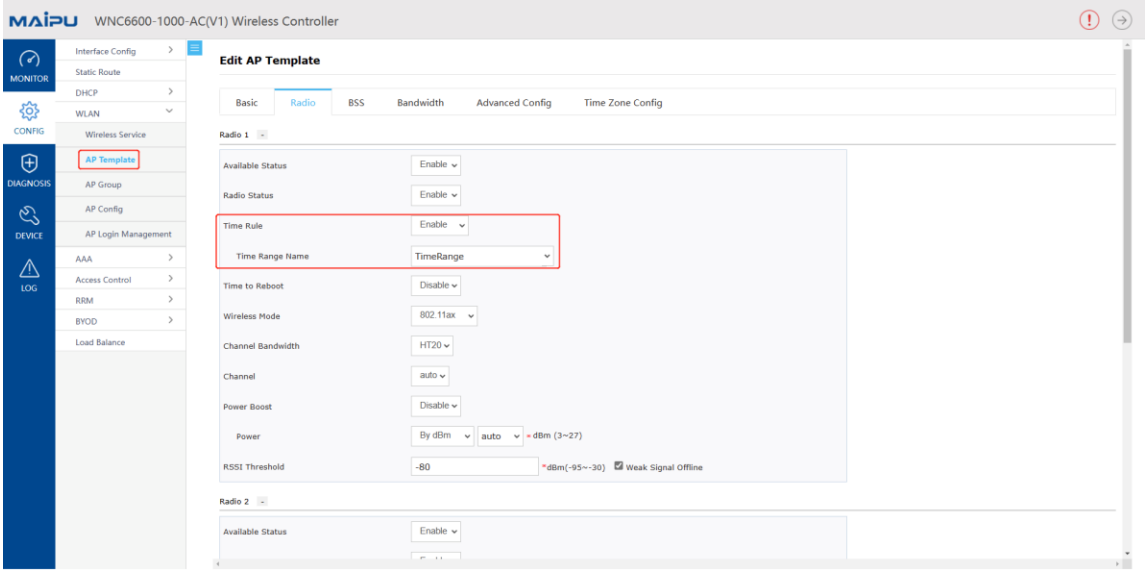


Figure 11.7 Enable radio in time range

12.5 Enable within Configured BSS Time Range

Establish time domain policies. The method is the same as that of creating the time domain in 11.4. In the AP template or AP configuration, the time domain policy established above can be applied in the BSS configuration, as shown in Figure11.8.

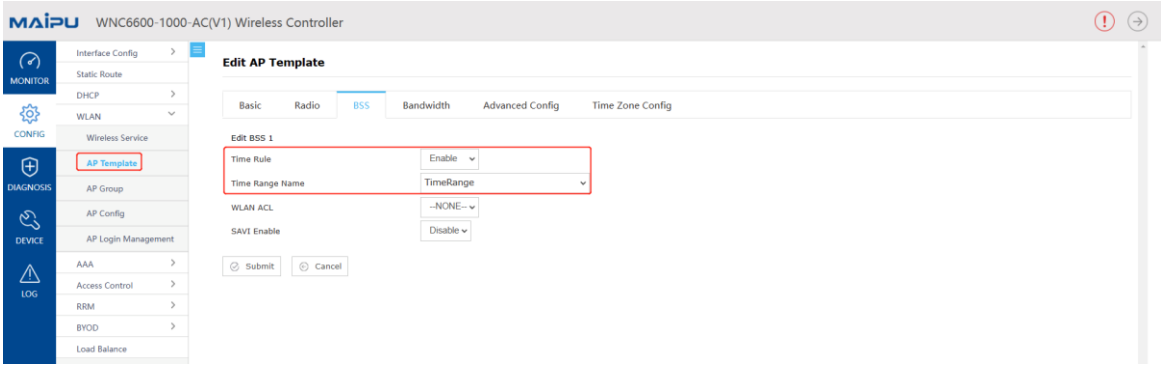


Figure11.8 Used in BSS time period

copyright ©Maipu, all rights reserved

13 Dual-Machine Hot Standby

Refer to the configuration manual for the configuration of the dual-machine configuration.

13.1 Configure Standby Link

Before configuring the AP standby group, you need to establish a standby channel at both ends, click "Create" to add a standby link, and enter the standby communication address/heartbeat address at both ends, as shown in Figure12.1.

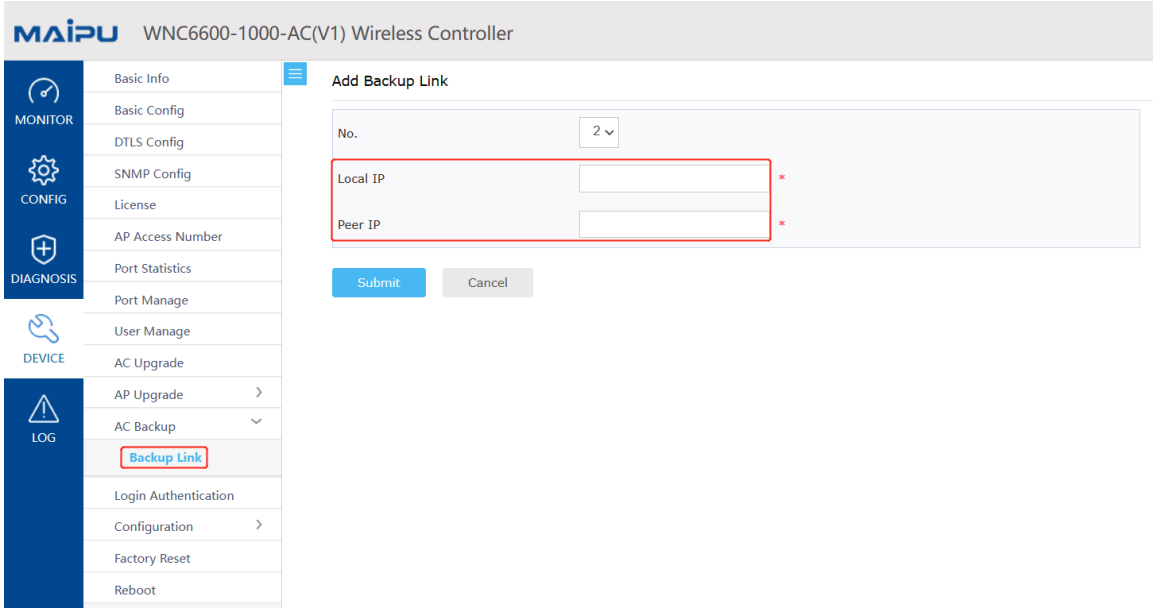


Figure12.1 Create a standby link

Note

- Both ACs need to be configured, and the standby link addresses of the two ACs cross each other.

13.2 Configure an AP Standby Group

Please refer to the configuration in 7.1, as shown in Figure12.2.

copyright ©Maipu, all rights reserved

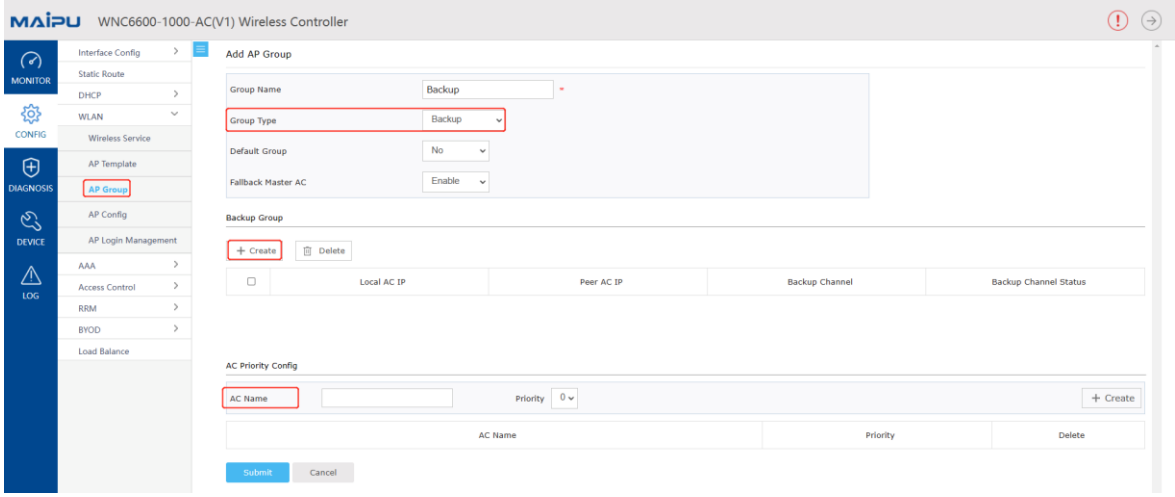


Figure12.2 Configure the AP standby group

AC name: The name is the same as the device name in 4.6.1.

Note

- Both ACs need to be configured, and the addresses of the two ACs cross each other.

13.3 Add APs to Standby Group

Please refer to the configuration in 7.2.

13.4 DHCP Configuration (Ignore This Step if DHCP Is Not on AC)

13.4.1 Hot Standby Configuration

For the ID of the local end and the ID of the peer end, please note that the positions of the two ACs are exchanged during configuration, as shown in Figure12.3.

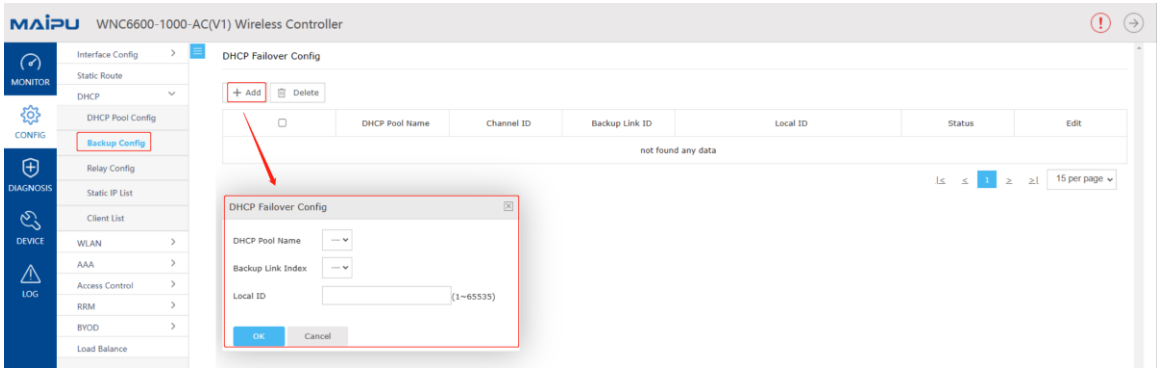


Figure12.3 Hot standby configuration

copyright ©Maipu, all rights reserved

13.4.2 Address Pool Configuration

The configuration of the address pool is similar to that of the stand-alone, but note that when configuring the AP address pool, you need to configure two option 43.

13.4.3 Note on Configuration

Please note that all configurations related to wireless must be the same when setting up the dual-machine hot standby environment. Otherwise, it may affect the normal operation of dual-machine.

copyright ©Maipu, all rights reserved

14 Troubleshooting

14.1 RF Detection

When there are Bluetooth devices or microwave ovens around the AP, the released Bluetooth signals and microwaves also belong to the2.4G frequency band, which will cause some interference to wireless signals. After the RF detection is enabled on the AC, the AP will scan the working channel or all channels, and report to the AC after detecting the Bluetooth signal or microwave signal. The user can enhance the signal of the AP or perform other customized configurations on the AC, such as RF detection duration configuration.

In "DIAGNOSIS" -> "Radio Frequency Detection", you can configure the duration of RF detection, ranging from10 to 3600 seconds.

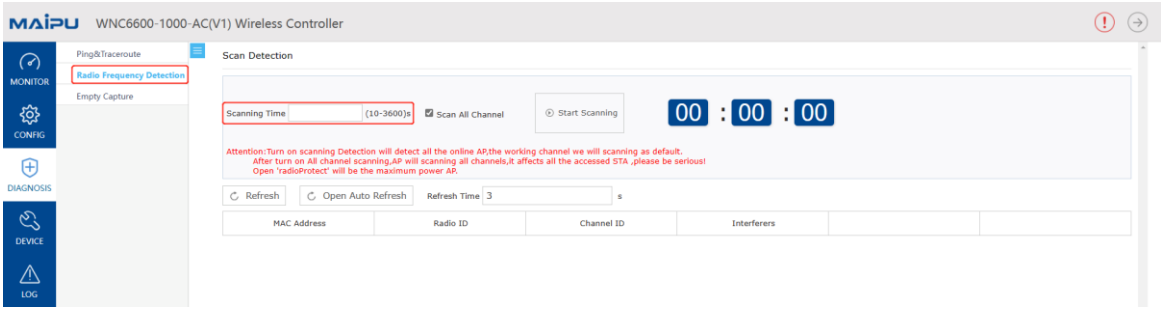


Figure13.1 RF detection duration configuration

By default, if Scan All Channels is not checked, scan the current working channel.

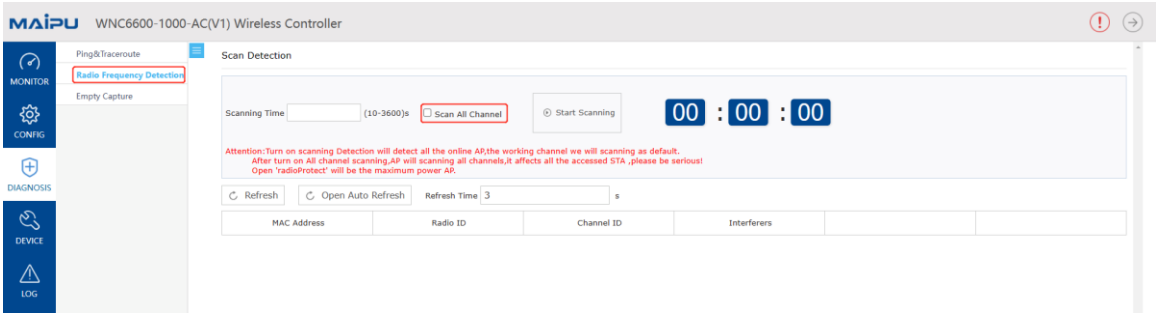


Figure13.2 RF detection channel

14.2 Empty Capture

14.2.1 Server Configuration

Set the information for uploading captured packet data, including the upload method, server address, user name and password, and choose to upload the compressed packet by default.

copyright ©Maipu, all rights reserved

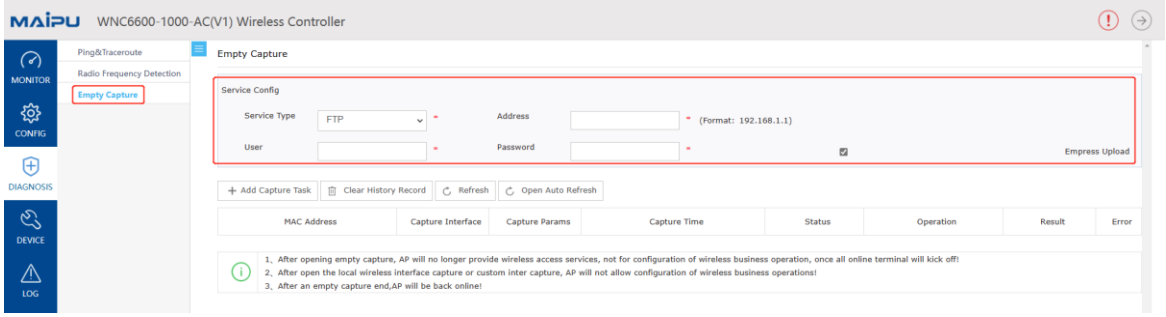
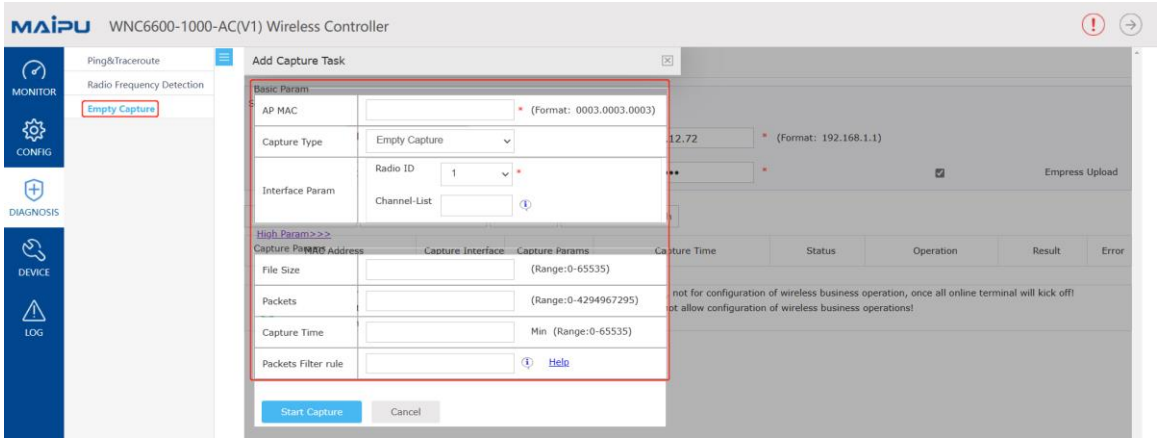


Figure 13.3 Capture server configuration

14.2.2 Create a Packet Capture Task

Click Add Capture Task, and the parameters that need to be configured include: AP MAC, capture type, interface parameters, among which the capture type can be divided into: empty capture, complete 2.4G or 5G full channel or partial channel information capture; local wireless interface capture, completing the information capture of the ath port of the AP; custom interface capture, completing the specified interface information capture, specifically including eth port, ath port, br port, etc. In addition, in the advanced parameter setting, you can set the file size, packets, capture time, and other parameters.



copyright ©Maipu, all rights reserved

15 BYOD

15.1 BYOD device identification configuration

Click "BYOD" -> "Device Identity Config", and you can enable the identification of the BYOD terminal operating system. After enabling it, the terminal access can identify the terminal's operating system. At the same time, the user can customize the operating system to identify the operating system that does not exist in the DHCP feature database.

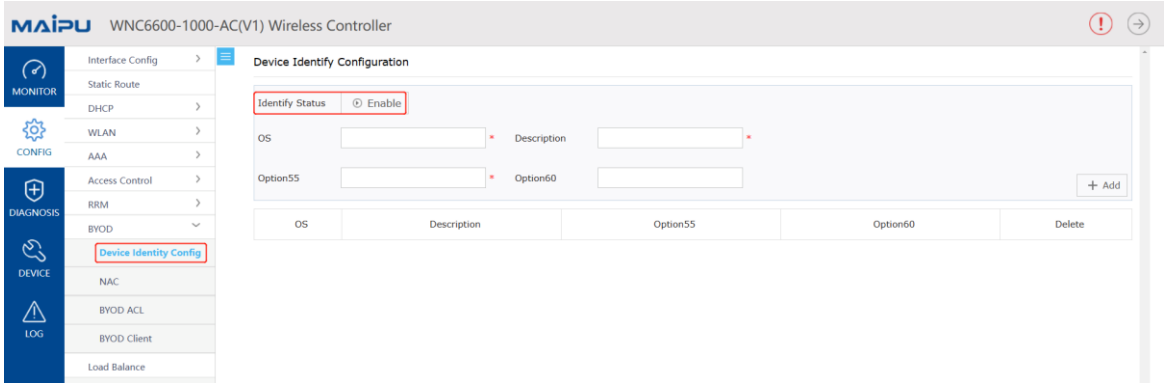


Figure14.1 Device Identity Configuration

15.2 NAC Policy

Click "BYOD" > "NAC", including two policies, VID binding and access deny.

15.2.1 VID Binding

After an operating system is configured to bind a VLAN, when a terminal of the operating system is accessed, the packet sent by the terminal will be changed to the corresponding VLAN.

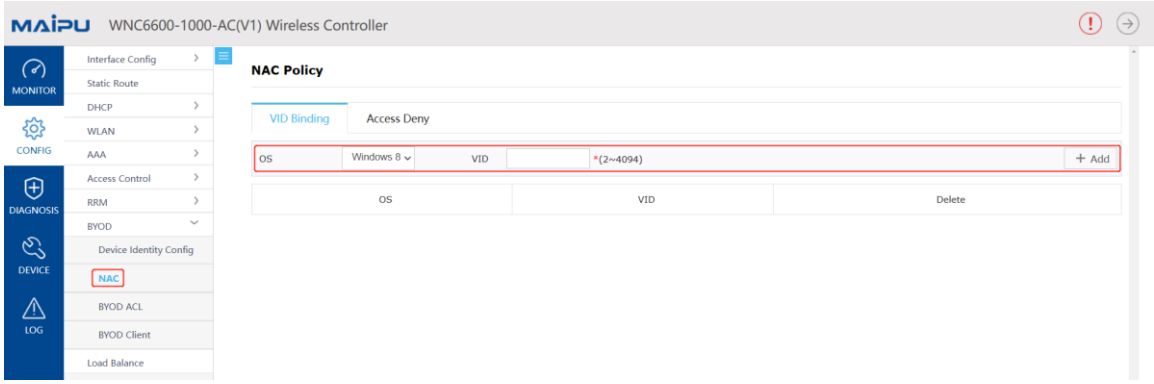


Figure14.2 VID Binding

copyright ©Maipu, all rights reserved

15.2.2 Deny Access

If the terminals of a certain operating system are configured to deny access, the wireless terminals of this system cannot be accessed.

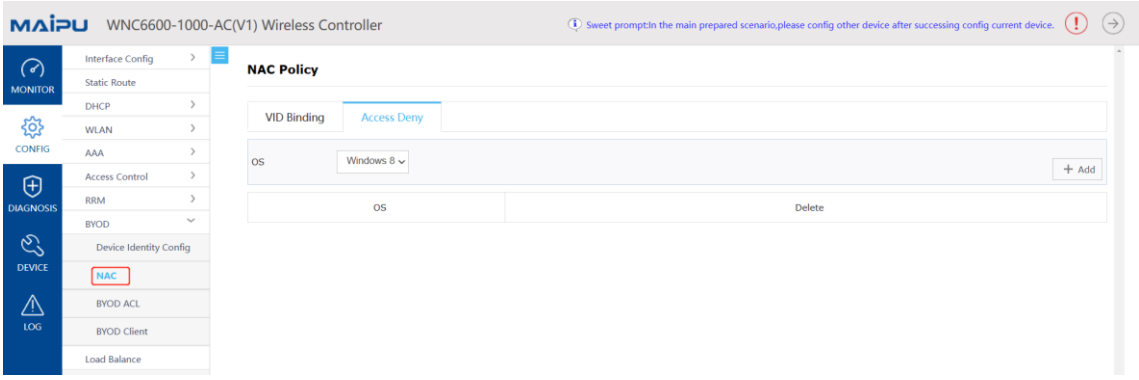


Figure14.3 Deny access

15.3 BYOD ACLs

See chapter 9.2 for details

15.4 BYOD Client

After enabling BYOD device identification, you can view the identified client types here.

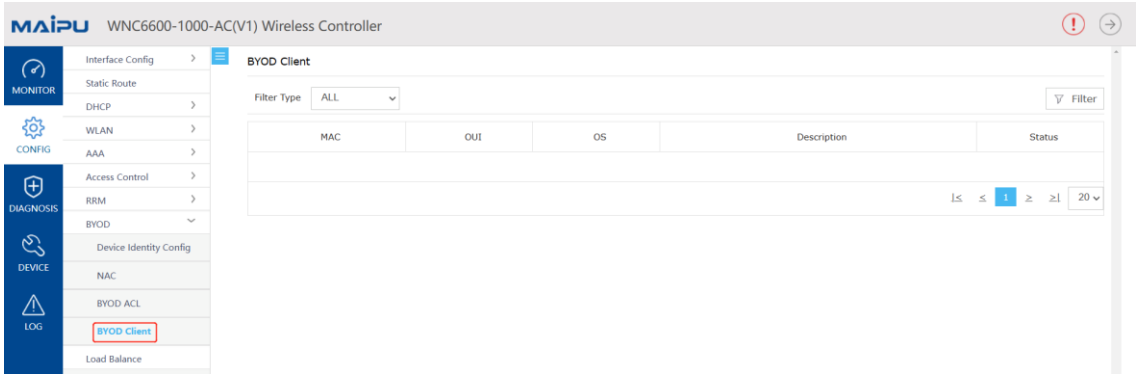


Figure14.4 BYOD client

copyright ©Maipu, all rights reserved

16 Load Balancing

16.1 Load Balancing

Load balancing, that is, balancing the load of clients in the WLAN network, fully guaranteeing the performance and bandwidth of each client.

Load balancing is mainly suitable for the occasions where a large number of APs are densely deployed, and the channels between APs may overlap; enabling the load balancing function helps to adjust the load of each AP, making the overall system performance better and user experience better.

When the STA client accesses the AP, the AC is responsible for performing load balancing. The AP periodically sends information about the connected wireless clients to the AC, and the AC uses the information for load balancing. The AC checks whether the AP that the client wants to connect to reaches the set load. If not, then the currently requested connection will be accepted; otherwise, based on the load balancing configuration, it will be decided whether the current connection is accepted or rejected.

Load balancing is to balance the load of each AP connected to the same AC, and load balancing will not be performed between APs connected to different ACs.

AC supports load balancing in two modes:

- User-Based Load Balancing

User-based load balancing mainly considers the number of STA users currently associated with the wireless system and the AP to decide whether to accept a new STA association request.

- Traffic-based load balancing.

Traffic-based load balancing. When a new STA is associated, the system determines whether the current AP enables the load balancing function based on the traffic on the AP.

16.2 Load Balancing Configuration

Click "CONFIG" -> "Load Balance", configure the parameters related to load balance.

copyright ©Maipu, all rights reserved

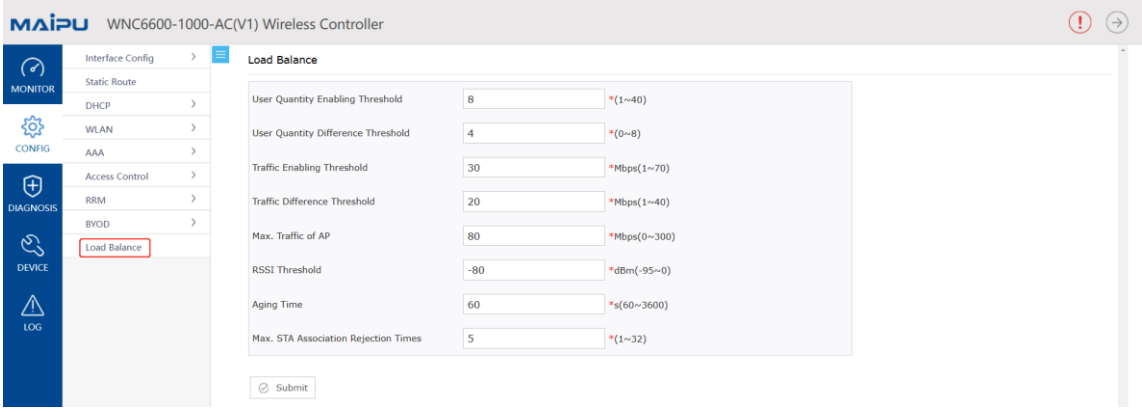


Figure15.1 Load balancing configuration

A. "**User Quantity Enabling Threshold** ": When the AP load associated with the terminal is greater than this value, the AC will make a load balancing decision;

B. " **User Quantity Difference Threshold**": It needs to be used in the load balancing formula, and the default value can be used;

C. "**Traffic Enabling Threshold**": when the AP traffic associated with the terminal is greater than this value, the AC will make a load balancing decision;

D. "**Max. Traffic of AP**": It needs to be used by the load balancing formula, and the default value can be used;

E. "**RSSI Threshold**": When the AP reports the terminal to the AC, it needs to make a judgment. If the RSSI is lower than the threshold, it will not report;

F. "**Aging time**": The aging time of terminal entries on the AP and AC, to prevent the terminal from being far away from the coverage of the AP;

G. "**Max. STA Association Rejection Times**": When the AP associated with the terminal does not meet the load balancing judgment result, the AC sends **delete sta**, and the AP sends disassociation to the terminal. If the terminal still continues to associate with this AP when the maximum number of rejections is exceeded, the STA is normally accessed;

16.3 Load Balancing Switch

Click "CONFIG" -> "WLAN " -> "Wireless Service " to create a wireless service set, enable load balancing, and you can choose load balancing based on the number of users or based on traffic.

copyright ©Maipu, all rights reserved

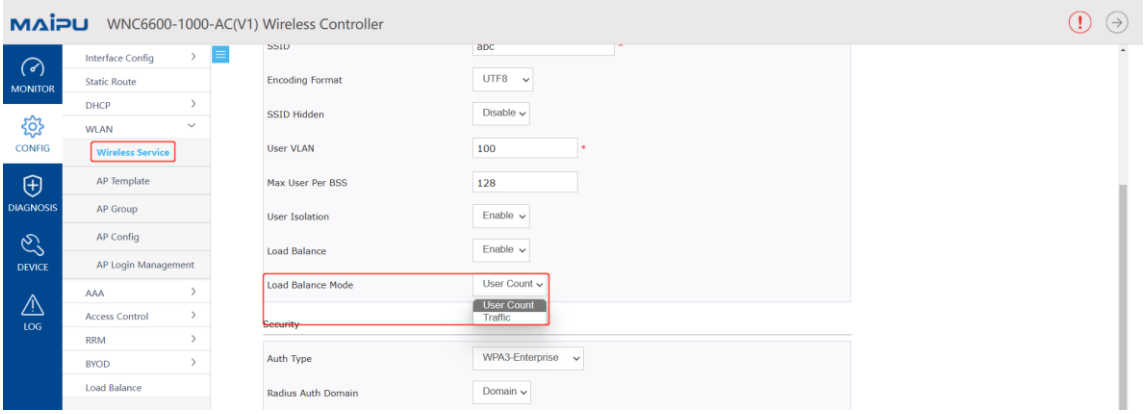


Figure15.2 Create a wireless service set with load balancing enabled

copyright ©Maipu, all rights reserved

17 AC Configuration Synchronization

When configuring the wireless environment, many of the same commands need to be configured between the active and standby ACs. When the commands that need to be synchronized are misconfigured, the network environment will be abnormal. When the environment is complex, there are many configuration commands, and there are clear requirements for the configuration order, multiple configurations may cause errors and cause abnormalities in the environment. So the wireless configuration in this environment can be handled by configuration synchronization.

17.1 Add AC Link Channel

Before performing configuration synchronization, you need to establish a synchronization channel at both ends, click Add AC Channel, and enter the communication addresses of both ends.

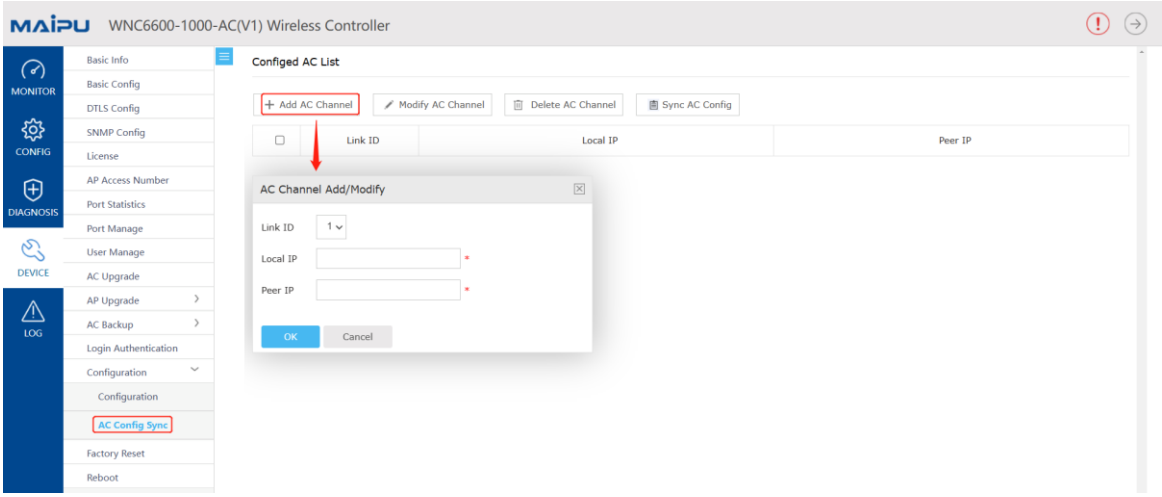


Figure16.1 Create an AC link channel

17.2 Synchronize AC Configuration

Select the link that needs to be synchronized, click Sync AC Config, and two options will appear: one is to replace the configuration, and all the wireless configurations of the local AC will be synchronized and overwritten to the peer device without saving; the other is to save the configuration, and the local wireless configuration is incrementally synchronized to the corresponding device and saved. After selecting the synchronization method, the configuration can be synchronized. At the same time, click View Config Info., and you can view the wireless configuration information of the local AC.

copyright ©Maipu, all rights reserved

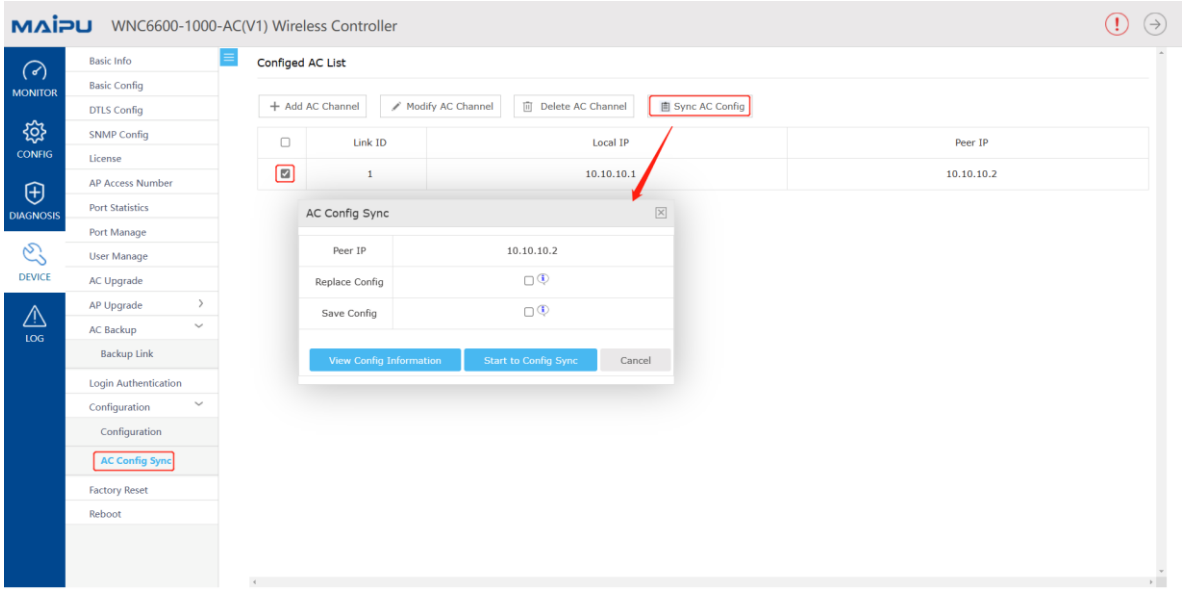


Figure16.2 AC Configuration Synchronization

copyright ©Maipu, all rights reserved

18 Device Upgrade

18.1 Upgrade AC Mirror File

AC provides users with three mirror upgrade methods:1. Upgrade through the network under **Monitor**; 2. Upgrade under the CLI command line of the AC; 3. Upgrade through the WEB page of the AC. This operation guide mainly introduces the upgrade of the WEB page. For other upgrade methods, refer to the "Device Upgrade Guide" for details.

18.1.1 Upgrade via HTTP

1. In AC Upgrade of DEVICE, select HTTP.
2. Then select the image file to be upgraded locally and upgrade it, as shown in Figure17.1.

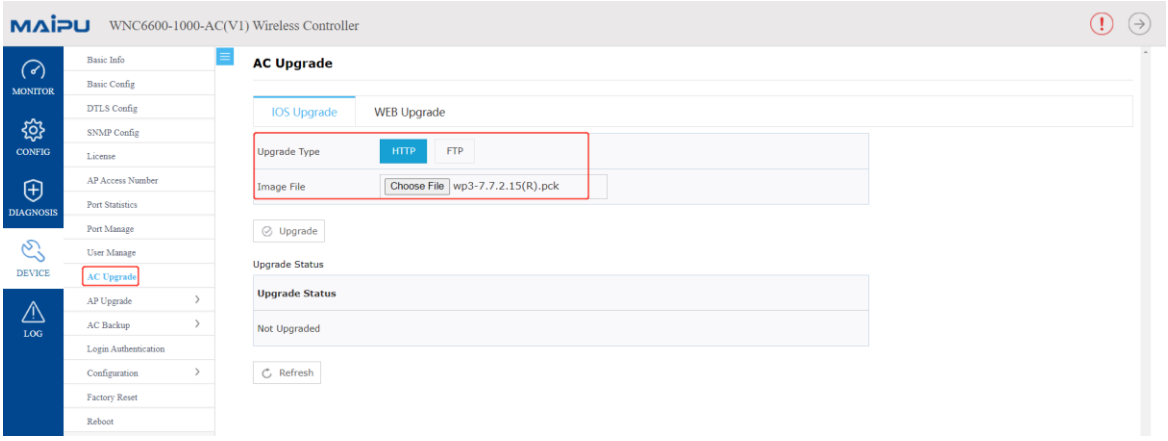


Figure17.1 HTTP upgrade

18.1.2 Upgrade via FTP

1. Configure the FTP server locally first, and save the AP image file to the FTP directory.
2. Then in the "AC Upgrade" of "DEVICE", select FTP and configure the corresponding options so that the AC can successfully obtain and upgrade the AC version image file through FTP, as shown in Figure17.2.

copyright ©Maipu, all rights reserved

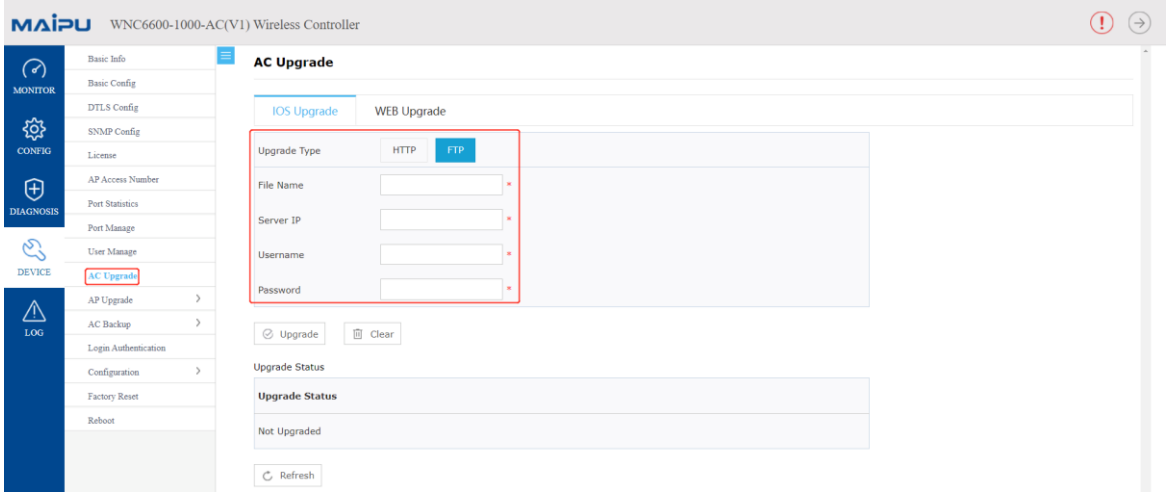


Figure17.2 FTP upgrade

18.2 Upgrade AP Software

Like the AC upgrade, this operation guide mainly introduces the WEB page upgrade of the AP, which is applicable to the upgrade of regular models except some special models. For other upgrade methods, see the "Device Upgrade Guide" for details.

18.2.1 FTP Upgrade

1. Configure an FTP server on the PC and save the AP image file to the FTP directory.
2. Configure FTP on the AC so that the AC can successfully obtain the AP version image file through FTP, as shown in Figure17.3.

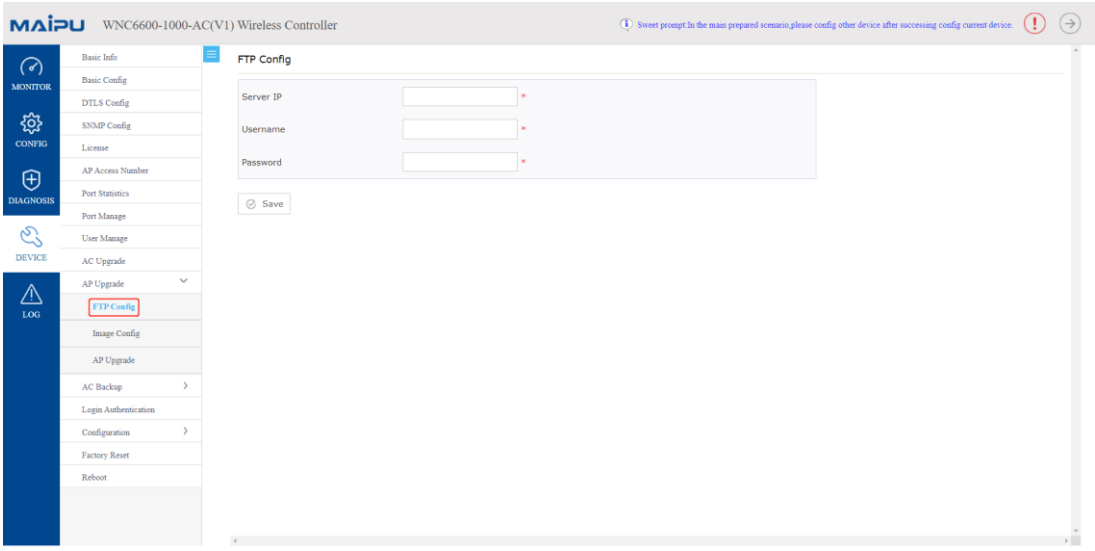


Figure17.3 FTP server configuration

copyright ©Maipu, all rights reserved

3. Click "Image Config", and click the "FTP" button on the pop-up page to obtain the AP image file, as shown in Figure17.4.

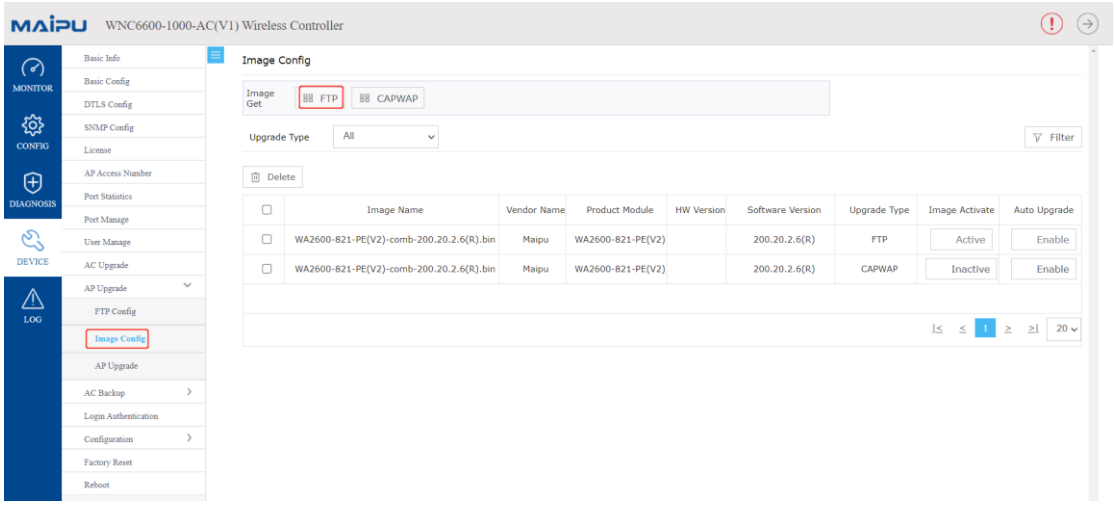


Figure17.4 Get AP image file

4. Perform upgrade operations in the "AP Upgrade" directory. Select the AP to be upgraded and the corresponding AP version, as shown in Figure17.5.

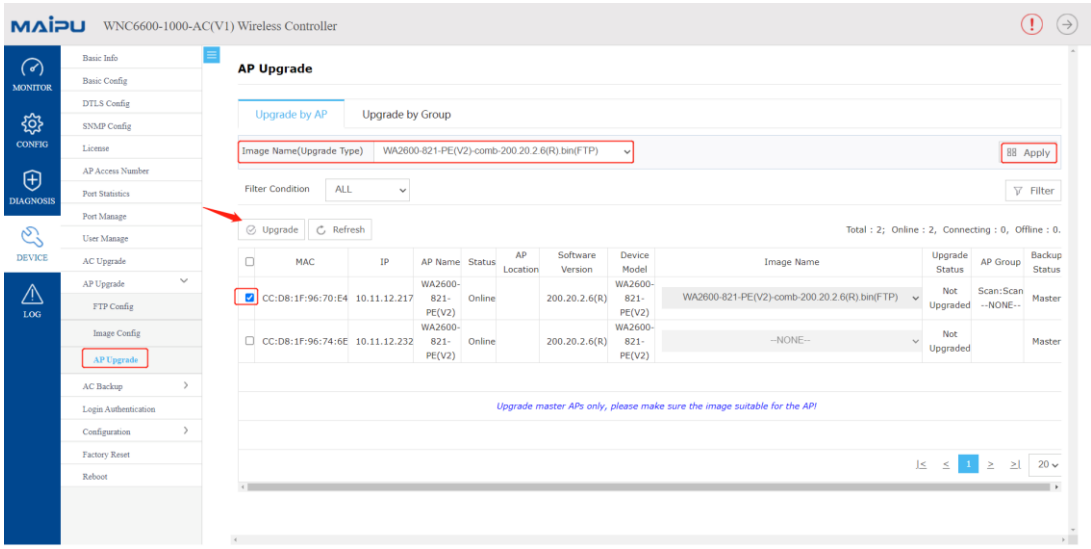


Figure17.5 AP upgrade

5. If the upgrade of multiple APs of the same type is involved in the present network, AP groups can be used for batch upgrade.
6. Create a new AP upgrade group and select the corresponding image file, as shown in Figure17.6 and17.7.

copyright ©Maipu, all rights reserved

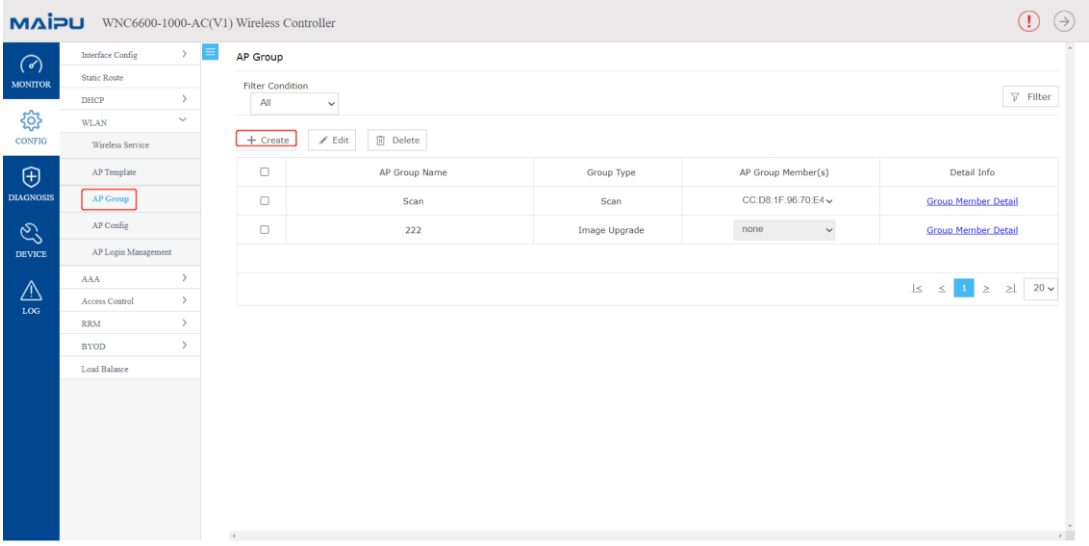


Figure17.6 Create an AP upgrade group

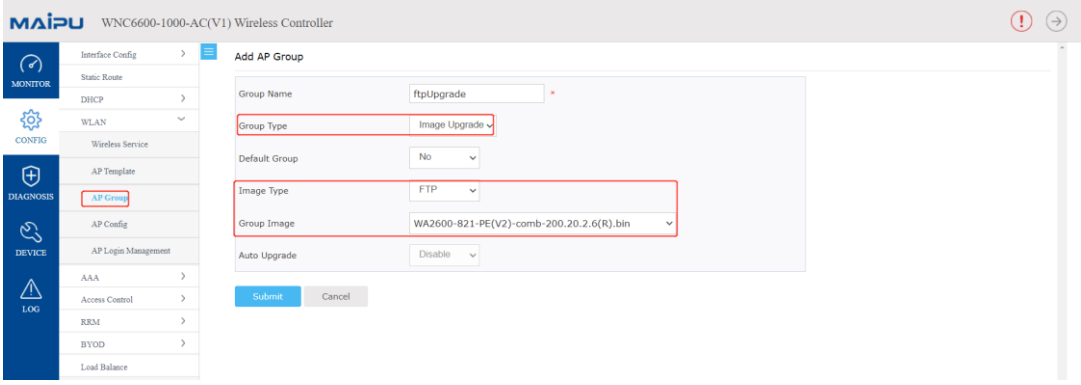


Figure17.7 Configure AP upgrade group

7. Add the APs to be upgraded to the upgrade group, as shown in Figure17.8.

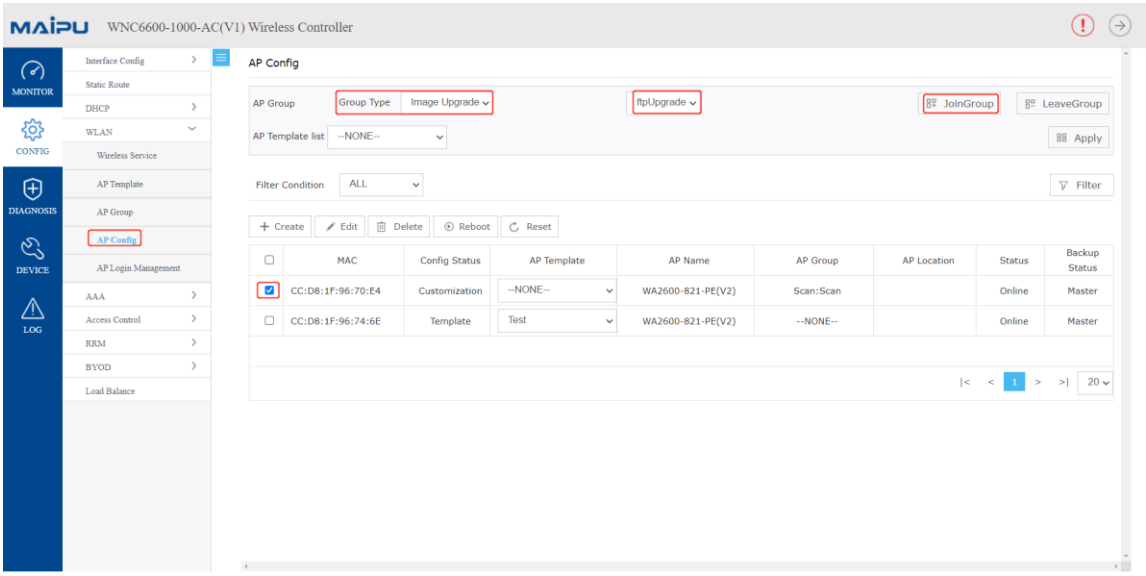


Figure17.8 Add APs to upgrade group

8. After successfully adding, you can perform the upgrade operation, as shown in Figure17.9.

copyright ©Maipu, all rights reserved

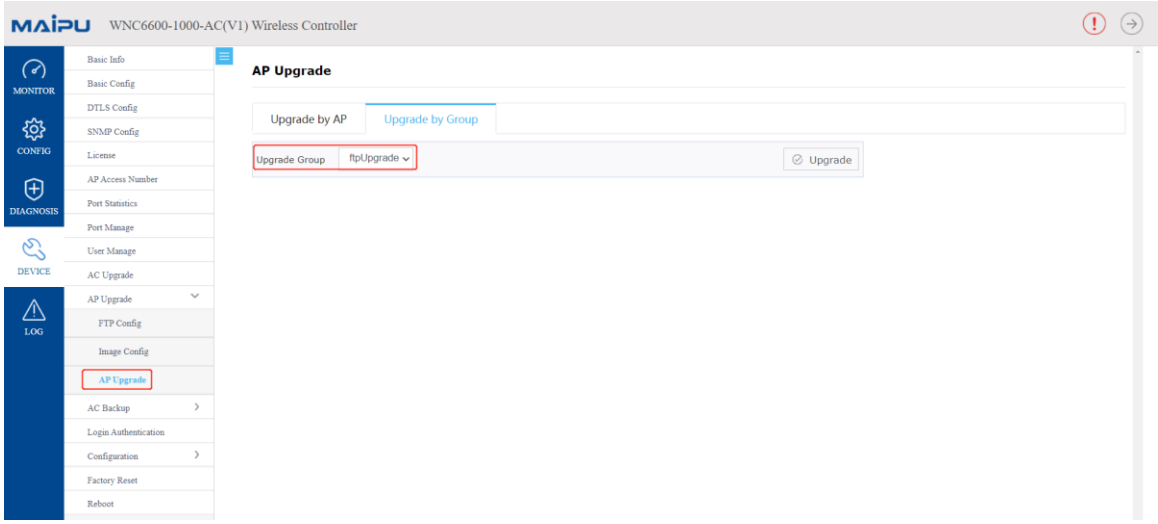


Figure17.9 AP group upgrade

9. You can also perform upgrade operations on the command line

wnc #configure terminal

wnc(config)#wireless ap upgrade192.168.1.10 WA2600-830-PTE(V2)-comb-300.4.1.1(R).bin comb ftp aa group groupname **(The AP needs to be added to the AP upgrade group before upgrading, the group name is recommended to use English)**

18.2.2 Upgrade via CAPWAP

1. Click CAPWAP and select the corresponding AP image file locally. It may take a while to obtain the image, please wait patiently, as shown in Figure17.10.

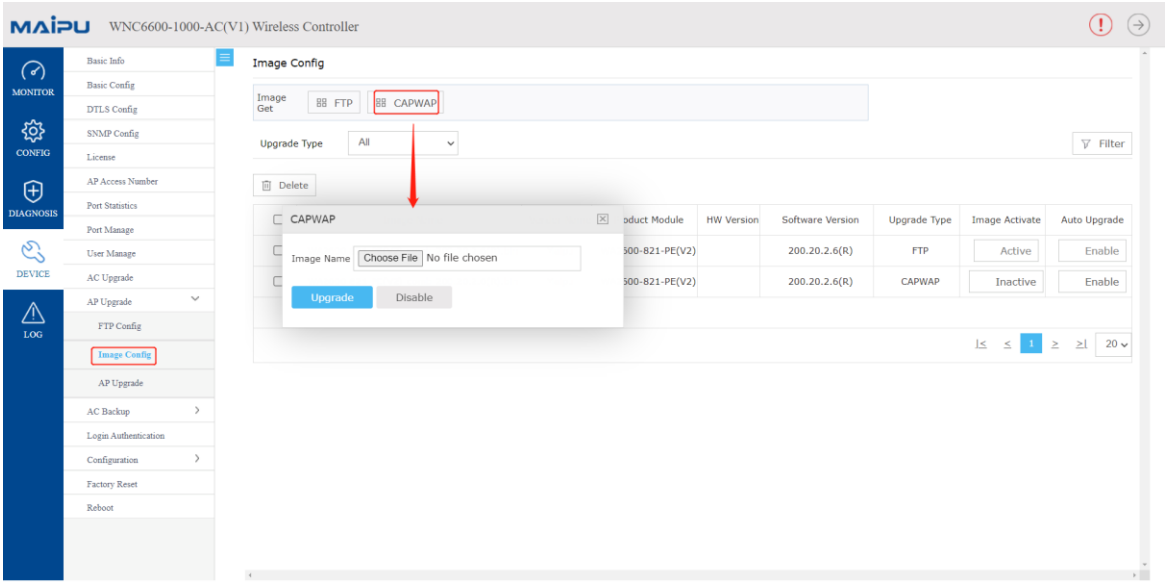


Figure17.10 Get AP image file

2. After obtaining the image successfully, you need to manually activate the image, as shown in Figure17.11.

copyright ©Maipu, all rights reserved

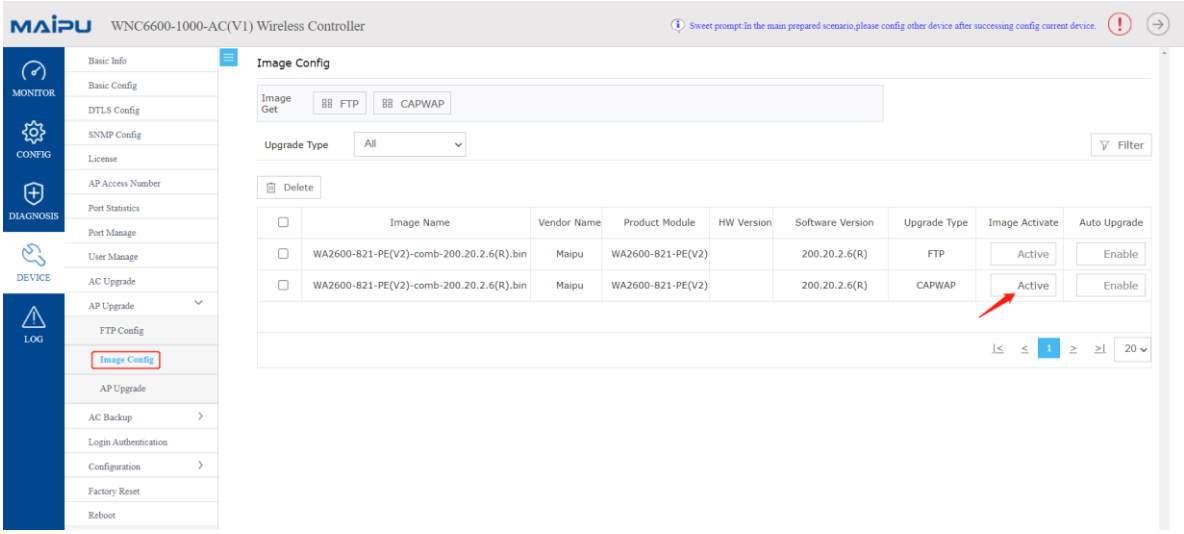


Figure17.11 Activate AP image file

3. Perform the upgrade operation in the AP upgrade submenu. The method is the same as step D in 17.2.1.

18.2.3 Online Auto Upgrade

When a new AP goes online, if the manufacturer and model are compatible with the image that has been activated and enabled with the auto upgrade, and the version is different, the AP will be automatically upgraded.

A. Obtain the image according to the ABC steps in 17.2.1.

B. Activate the image, and enable the auto upgrade, as shown in Figure17.12.

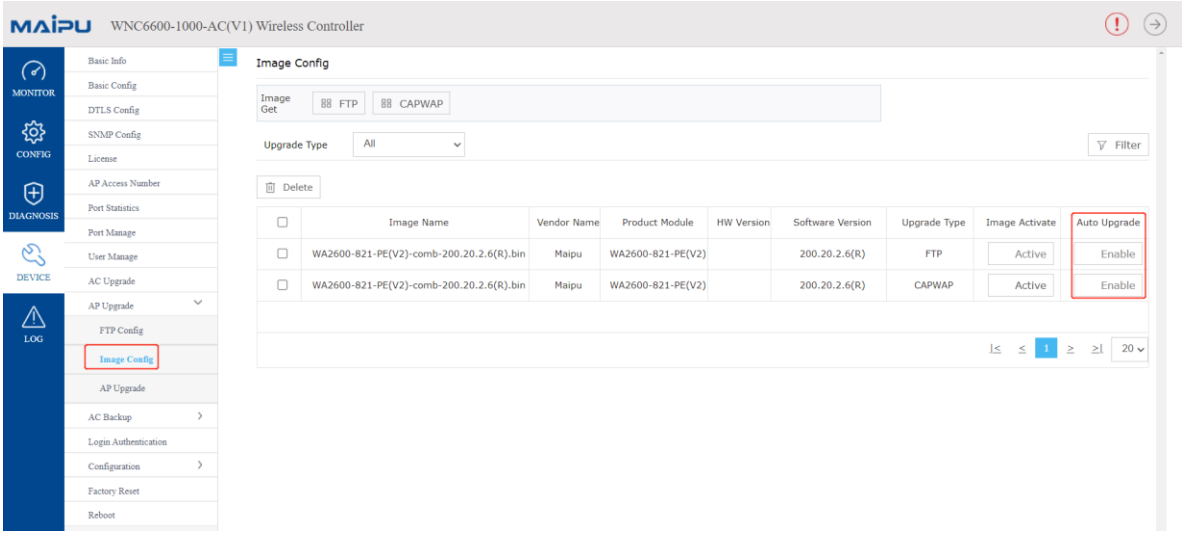


Figure17.12 AP auto upgrade

copyright ©Maipu, all rights reserved

19 License Configuration

19.1 Apply for License

To apply for a license file, please contact Technical Services directly.

19.2 Introduction to License

The number of APs that can be managed by the device can be increased by obtaining license. If you have obtained a license, you need to complete the activation of the license to make the authorization take effect on the device. The license file is bound to the device. When applying for the license file, you need to provide the SN (Serial Number) of the device.

In addition, without adding additional license files, the AC can also connect to a certain number of APs, which are:

Product Model	Default Access Quantity	Max. Accesses Allowed
WNC6600-100	32	128
WNC6600-500	64	512
WNC6600-1000	128	1024

19.3 Query Method of SN No.

First check the product serial number, as shown in Figure18.1.

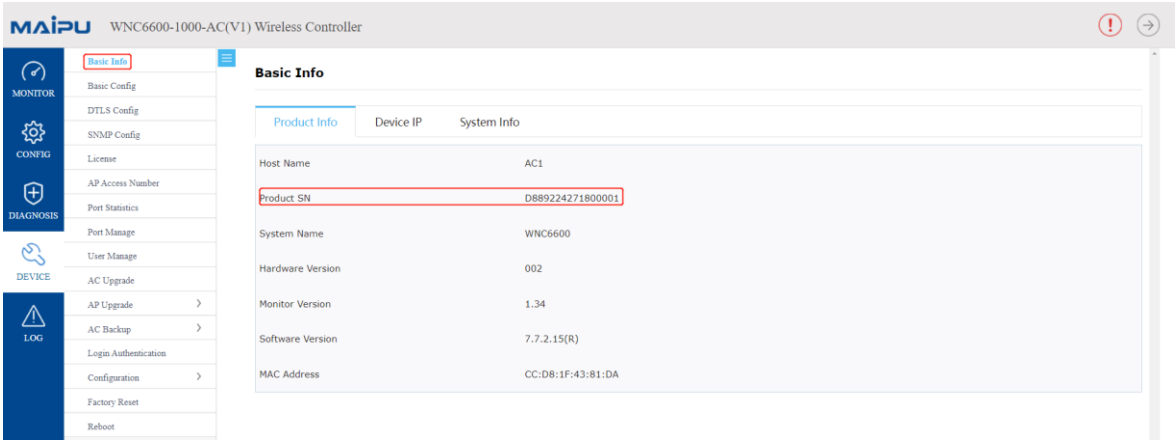


Figure18.1 Product serial number

copyright ©Maipu, all rights reserved

19.4 License Query

Query the license status on the AC through the web page, as shown in Figure18.2.

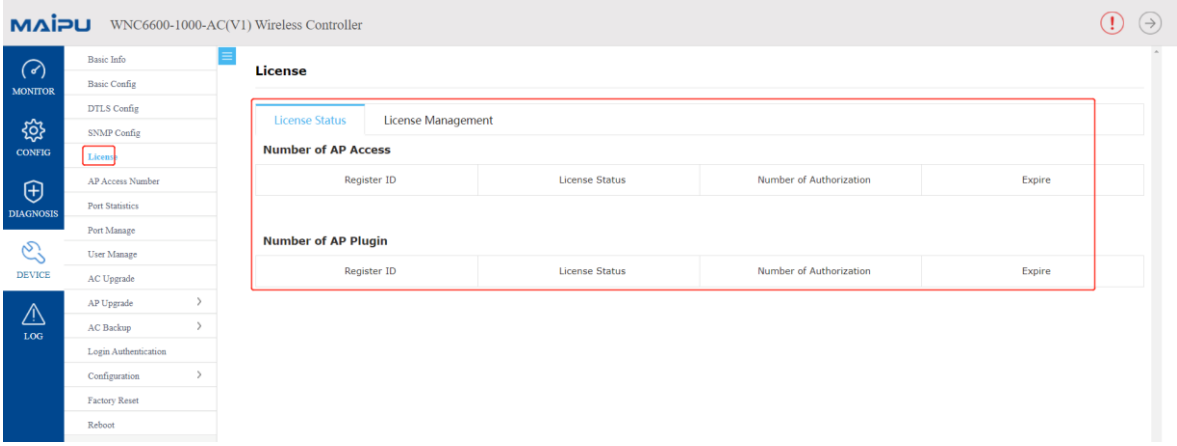


Figure18.2 License configuration

You can also query the license status on the CLI. For detailed commands, see the configuration manual.

19.5 Import and Export License

19.5.1 Import License

There are three ways to import a license: HTTP, FTP, and manual, as shown in Figure18.3.

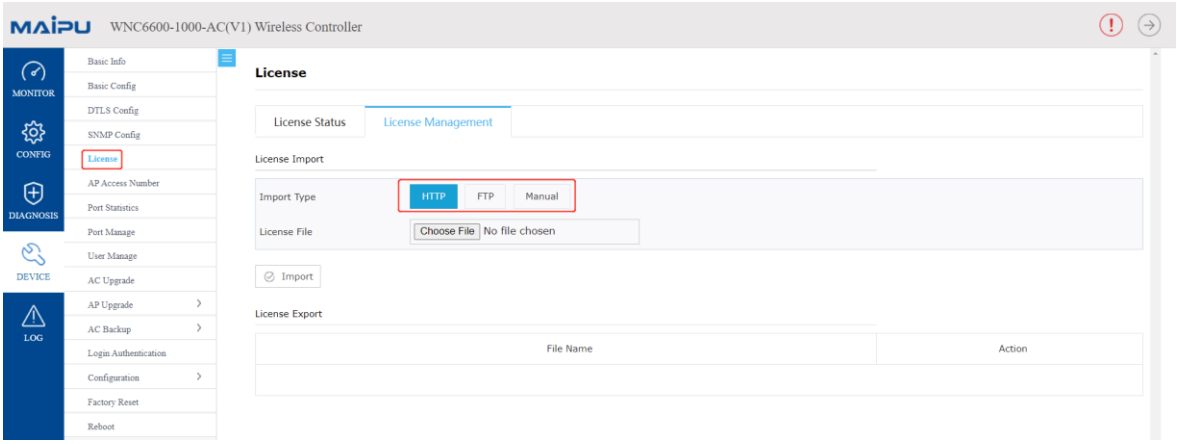


Figure18.3 License import method

Among them, the HTTP and FTP methods are used to directly import the license file to add the license. while "manual" needs to open the license file with Notepad first, and copy the content in the file to the blank box of "License Content".

Attachment: Manually import the License

copyright ©Maipu, all rights reserved

A. Use Notepad to open the lic file and copy all the content in the file and paste it into the "License Content" box on the WEB page, as shown in Figure18.4 and18.5.

Figure18.4 License content

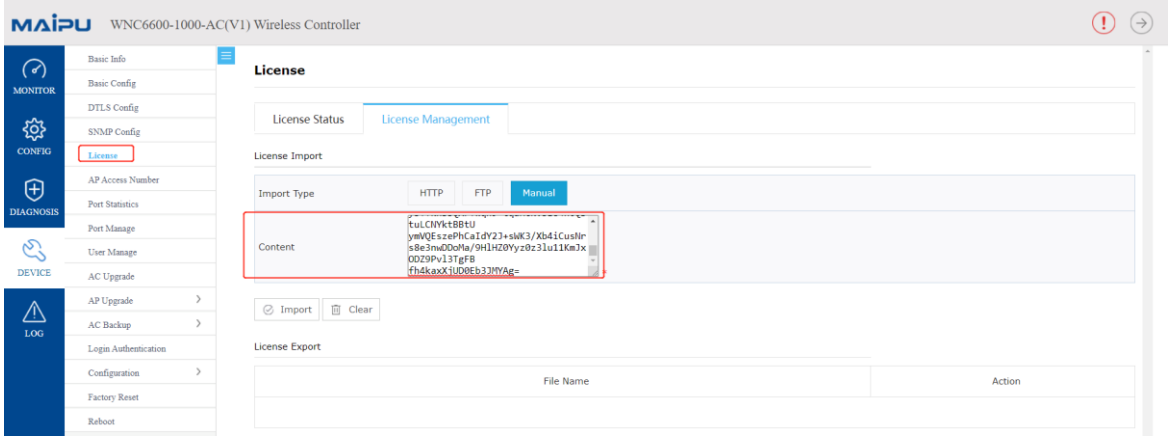


Figure18.5 Import License

19.5.2 Export License

Export the license configuration, as shown in Figure18.6.

copyright ©Maipu, all rights reserved

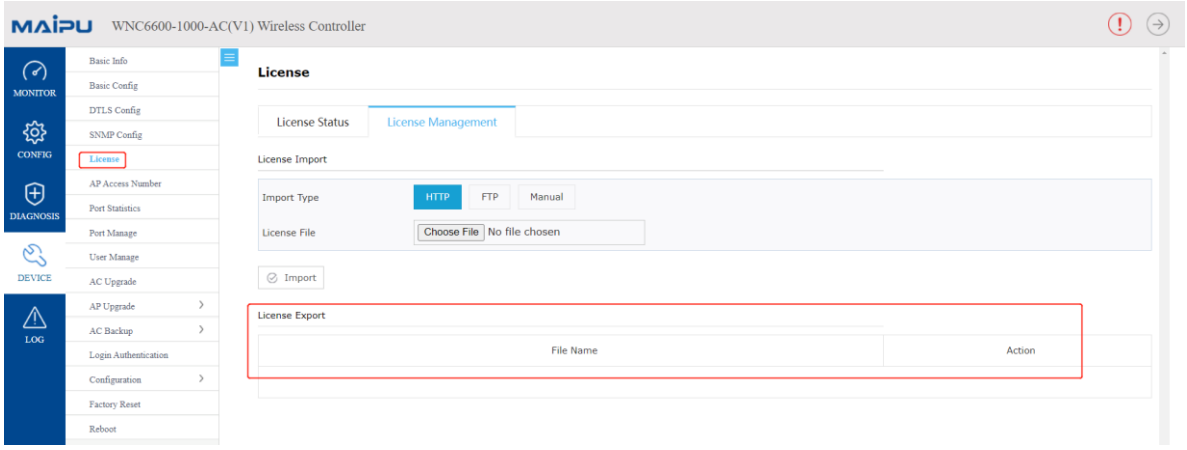


Figure18.6 Export License

copyright ©Maipu, all rights reserved

20 Black and White List

In the WLAN network environment, certain rules can be set to filter wireless terminals through the black and white list function, so as to realize the access control of wireless terminals. The effective scope of the black and white list can be divided into the global scope and the scope of the wireless service set. For the global black and white list, all STAs connected to the AC will be filtered. For the black and white list under the service set, only the STAs connected to the wireless service set will be filtered. to filter. If the blacklist and whitelist function is enabled in a service set, the association of STAs depends entirely on the blacklist and whitelist in the service set, and the impact of the global blacklist and whitelist on STA online is no longer considered.

20.1 Configure Blacklist and Whitelist Rule Groups

20.1.1 Create Rule Group

By default, there is no rule group configuration, and you can create the corresponding rule group, as shown in Figure20.1:

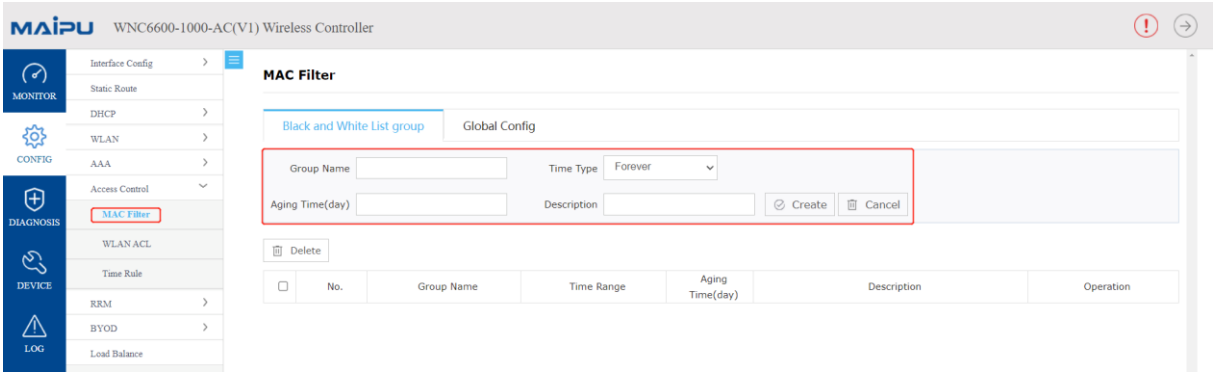


Figure 20.1 Create a blacklist and whitelist rule group

A. Group name: the name of the black and white list rule group, which is required here, such as input: black

B. Time Type: The time when the blacklist and whitelist groups take effect, there are two options, the default is permanent; the other option is the time period name (configure the time domain name and effective time period on the "Time Rules" page), only when the selected time period status is active, the macs in the blacklist and whitelist groups are valid.

C. Aging time: the unit is day, the range is 1-365, the default is no aging. The aging function takes effect only when the rule group is used as a whitelist; after this function is configured, the MAC configuration

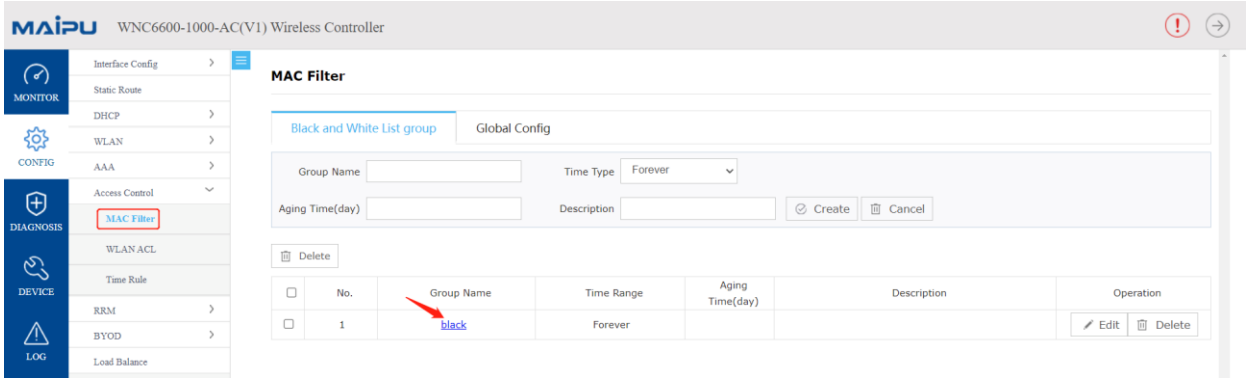
copyright ©Maipu, all rights reserved

in the rule group that has not been online for a long time (reaching the aging time) will be automatically deleted.

D. Description: The user can customize the configuration, and the maximum supported character length is 63. Note that Chinese is counted as two characters.

20.1.2 Add Terminal mac Configuration in Rule Group

After the creation operation is completed, click the link of the rule group "black" as shown in the figure 20.2, enter the sub-page, and add the terminal mac configuration;



Fifure 20.2 Rule groups

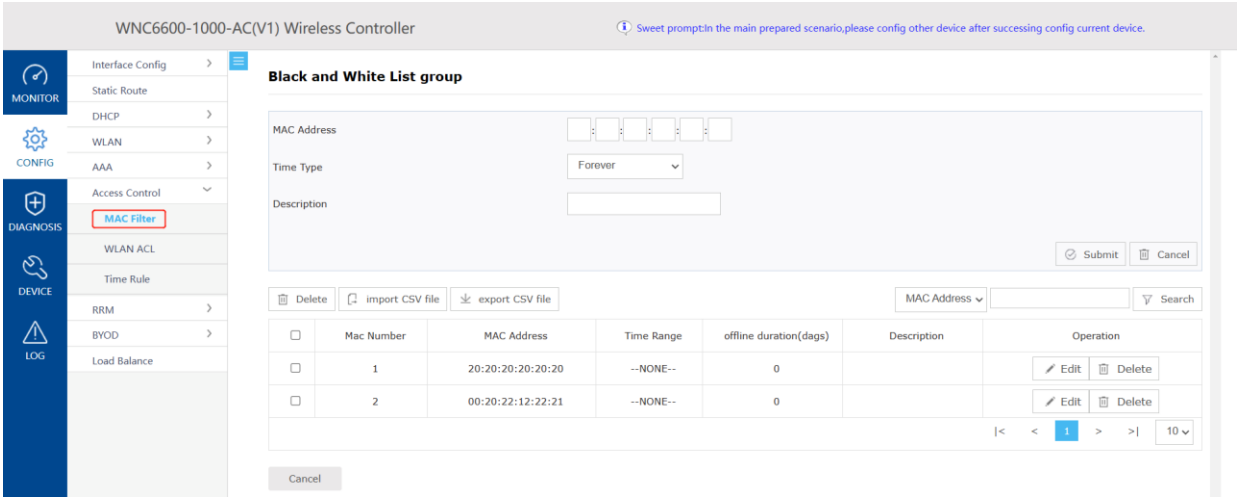


Figure 20.3 Add mac configuration in the rule group

There are two ways to add MAC addresses: Add one by one or click the "Import CSV file" button to import in batches

A. MAC Address: fill in the correct MAC address

B. Time Type: The time when the MAC address takes effect, there are two options, the default is permanent; the other option is the time period name (configure the time domain name and effective

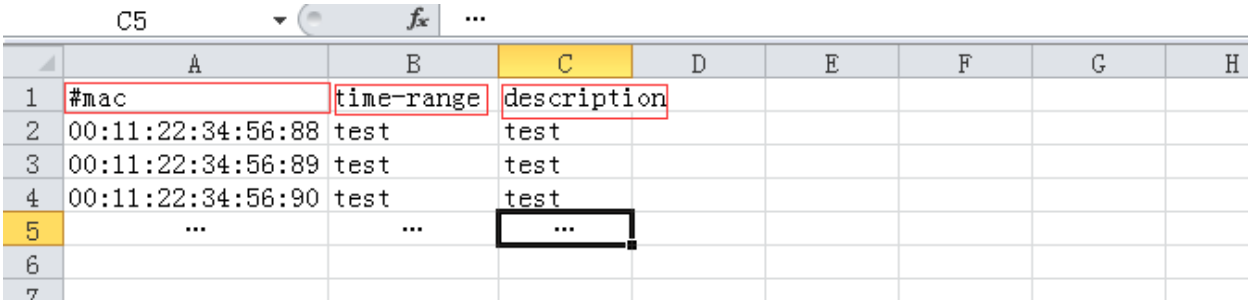
copyright ©Maipu, all rights reserved

time period on the "Time Rules" page). Only when the selected time period status is active, the MAC will take effect.

C. Description: Customize the MAC address information, the maximum length is 63, support Chinese and special characters (spaces are not supported).

D. Export CSV file: Zero-configuration export can check the format requirements filled in; it can also export all MAC address information in the rule group, which is convenient for statistics or backup.

E. Import CSV file: Add multiple pieces of MAC information in the exported CSV file, and then import it, which can realize the quick configuration of a large number of MACs. Pay attention to the MAC format: XX:XX:XX:XX:XX:XX, "time-range" and " description" is a separate column and can be empty, as shown in Figure 20.4:



	A	B	C	D	E	F	G	H
1	#mac	time-range	description					
2	00:11:22:34:56:88	test	test					
3	00:11:22:34:56:89	test	test					
4	00:11:22:34:56:90	test	test					
5	...	...	...					
6								

20. 4 Imported CSV file format

The content in the red box is the format guide

mac: fill in the correct MAC address according to the format;

time-range: Null value means permanent effect, if there is data, it will take effect according to the corresponding time domain, and the maximum supported character length is 31;

description: it can be empty, supports Chinese, English and special characters (spaces are not supported), and supports a maximum character length of 63;

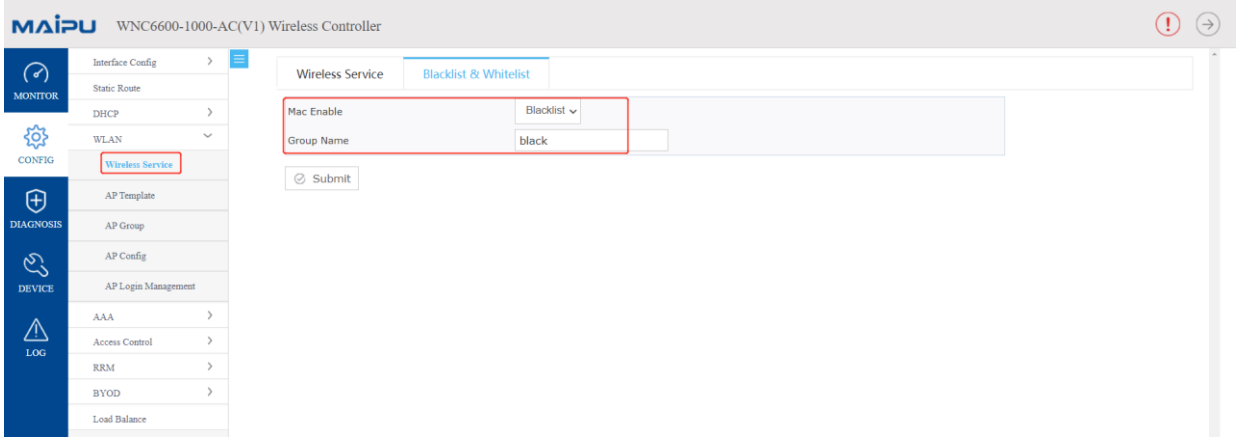
F. Search function: The filter rules are divided into two types: MAC address and description, and fuzzy search is performed after inputting conditions;

G. Offline duration: record the duration of the terminal being offline continuously, in days, and it will be cleared to 0 when the terminal is online.

20.2 Enable Whitelist Function under Service Set

Edit the service set, enter the page shown in Figure19.3, select the rule group black to enable the whitelist, terminals outside the black rule group cannot access the service set, and STAs in the black rule group can access the service set;

copyright ©Maipu, all rights reserved



20Enable the blacklist function under the service set

20.3 Enable Global Blacklist Function

As shown in Figure 19.4, select the rule group black to enable the global blacklist function. The STAs in the black rule group cannot access the signals released by all APs on the AC, and the STAs outside the black rule group can access the signals released by the APs on the AC;

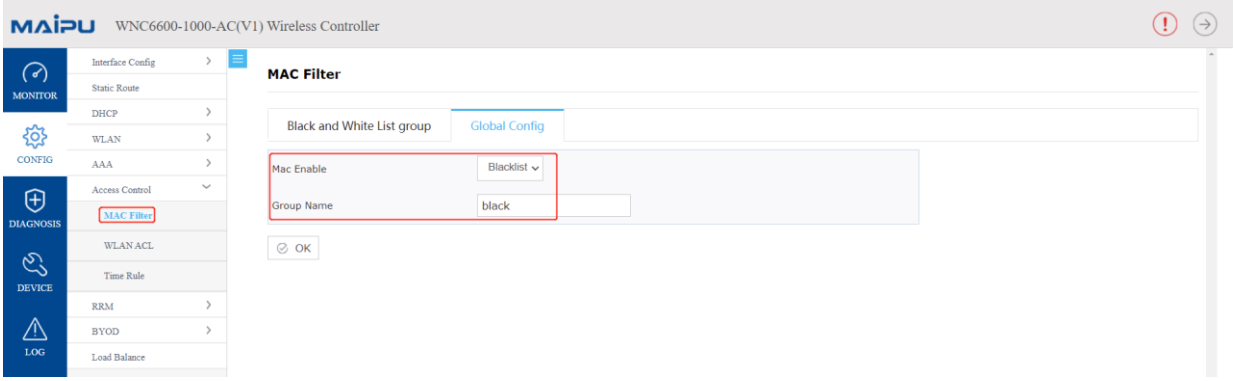


Figure 20.6 Enable the global blacklist function

Note

- If both the blacklist and whitelist function under the service set and the global blacklist and whitelist function are enabled at the same time, only the blacklist and whitelist function under the service set will take effect.

copyright ©Maipu, all rights reserved

21 Attachment: Product Introduction

MyPower WNC6600 series wired and wireless integrated controller is a wireless controller product independently developed by Maipu., which provides powerful WLAN access control functions for medium and large wireless LANs.

21.1 Product Forms

To meet the needs of different customers, WNC6600 provides three product forms, as shown in Table20-1.

Table 20-1Product form table

Product Model	Supported Interfaces and Descriptions
WNC6600-100-AC	24 10/100Base-T electrical interfaces, two COMBO ports (10/100/1000Base-T+100BASE-FX/1000Base-X), one DC0 port (10/100/100Base-T), one CONSOLE port (RJ45), one USB port, one Micro SD port (built-in), solidified single power supply, and can manage up to128 APs. Each of the first eight 10/100Base-T electrical ports supports 15.4W/30W POE power supply, and the whole machine supports a maximum of 8*15.4W or 4*30W POE power supply.
WNC6600-500-AC	12 10/100/1000Base-T electrical interfaces, 12 COMBO ports (10/100/1000Base-T+100BASE-FX/1000Base-X), two 10G optical interfaces (SFP+/1000BASE-X), one DC0 port (10/100/100Base-T), one CONSOLE port (RJ45/Micro USB), one USB port, one SD port, modular dual power supply, and can manage up to 512 APs.
WNC6600-1000-AC	12 10/100/1000Base-T electrical interfaces, 12 COMBO ports (10/100/1000Base-T+100BASE-FX/1000Base-X), two 10G optical interfaces (SFP+/1000BASE-X), one DC0 port (10/100/100Base-T), one CONSOLE port (RJ45/Micro USB), one USB port, one SD port, modular dual power supply, and can manage up to1024 APs.
WNC6600-2000-AC	12 Gigabit electrical ports+12 Gigabit COMBO ports, two 10G SFP+, 1+1 power supply, one CONSOLE port (RJ45/Micro USB), one USB port,1 SD port, and can manage up to2048 ports AP.

copyright ©Maipu, all rights reserved

21.2 Product Appearance and Dimension

WNC6600 adopts a centralized hardware platform, and all product forms of the whole series adopt a 1U standard desktop architecture, and the depth of the chassis varies with the product form.

Table 20-2Product Dimensions

Product Model	Dimension
WNC6600-100-AC	442mm * 380mm * 44.2mm (width x depth x height)
WNC6600-500-AC	440mm*420mm*44.2mm (width x depth x height)
WNC6600-1000-AC	
WNC6600-2000-AC	

21.2.1 Appearance of WNC6600-100-AC

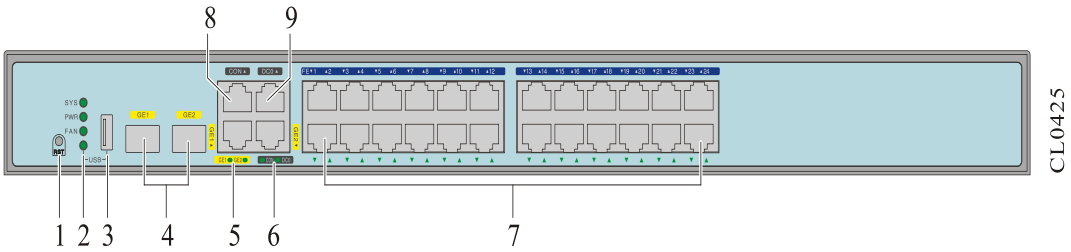


Figure 20-1The front panel of WNC6600-100-AC

1. Reset button (press and hold for 3 seconds to restart the device and clear user configuration at the same time)	2. Device Status Indicator SYS: system status PWR: power state FAN: fan status USB: USB interface status
3. USB port	4. Combo port (10/100/1000Base-T+100BASE-FX/1000Base-X)
5. Combo port status indicator	6. Port status indicator CON: Console port status indicator DC0: DC0 port status indicator
7. 10/100BASE-T electrical interface	8. Console port
9. DC0 port (10/100/1000Base-T)	

copyright ©Maipu, all rights reserved

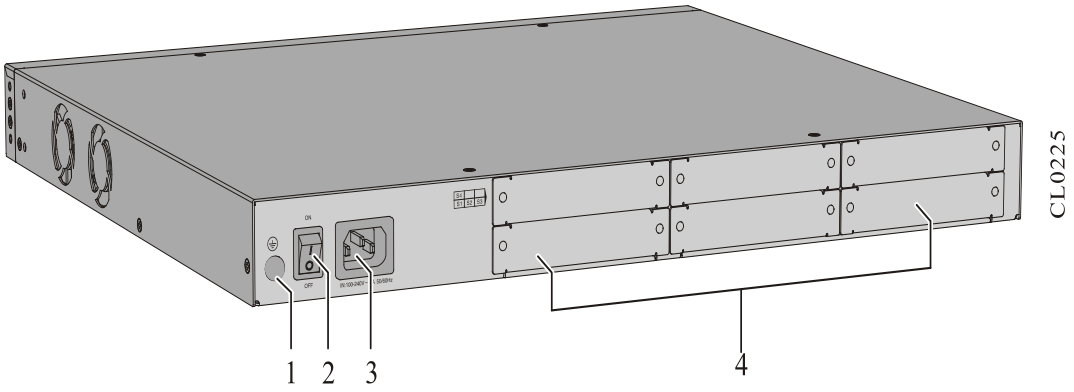


Figure 20-2The rear panel of WNC6600-100-AC

1. Ground terminal	2. Power switch
3. AC power outlet	4. Empty baffle

21.2.2 Appearance of WNC6600-500-AC

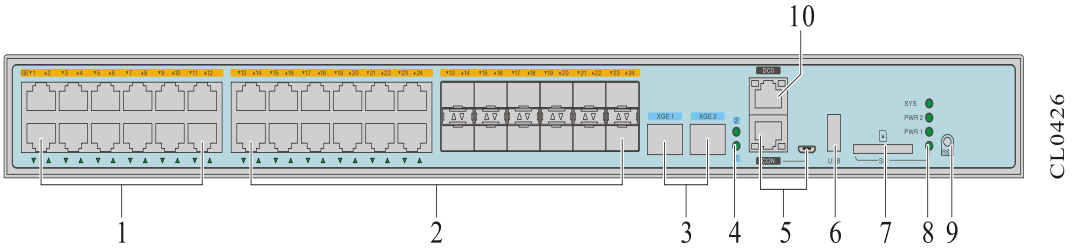


Figure 20-3 The front panel -3WNC6600-500-AC

1. 10/100/1000Base-T electrical interface	2. Combo port (10/100/1000Base-T+100BASE-FX/1000Base-X)
3. 10G SFP+ optical interface (SFP+/1000Base-X)	4. 10G optical interface status indicator
5. Console port (Micro USB/RS232)	6. USB port
7. SD card	8. Device Status Indicator SYS: system status PWR2: Power2 status PWR1: power supply1 status SD: SD card status indicator
9. Reset button (press and hold for 3 seconds to restart the device	10. DC0 port (10/100/1000Base-T)

copyright ©Maipu, all rights reserved

and clear user configuration at the same time)	

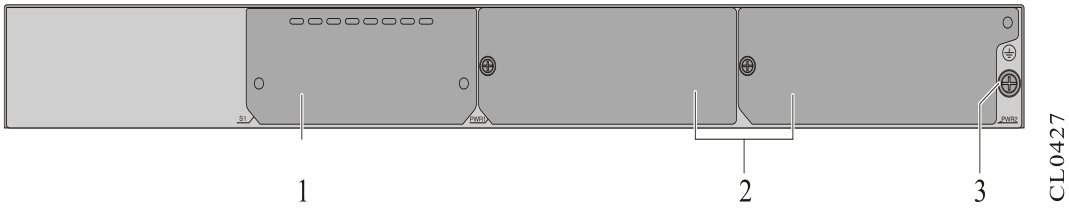


Figure 20-4The rear panel of WNC6600-500-AC

1. Empty baffle	2. Modular power supply (PWR1, PWR2)
3. Ground terminal	

21.2.3 Appearance of WNC6600-1000-AC/WNC6600-2000-AC

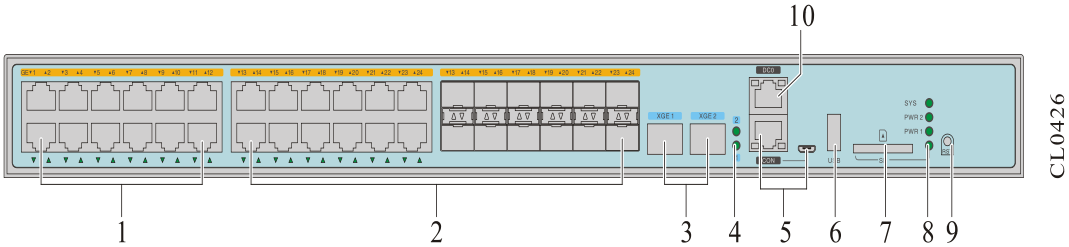


Figure 20-5 The front panel of WNC6600-1000-AC/WNC6600-2000- AC

1. 10/100/1000Base-T electrical interface	2. Combo mouth (10/100/1000Base-T+100BASE-FX/1000Base-X)
3. 10G SFP+ optical interface (SFP+/1000Base-X)	4. 10G optical interface status indicator
5. Console port (Micro USB/RS232)	6. USB port
7. SD card	8. Device Status Indicator SYS: system status PWR2: Power2 status PWR1: Power1 status SD: SD card status indicator
9. Reset button (press and hold for 3 seconds to restart the device and clear user configuration at the same time)	10. DC0 port (10/100/1000Base-T)

copyright ©Maipu, all rights reserved

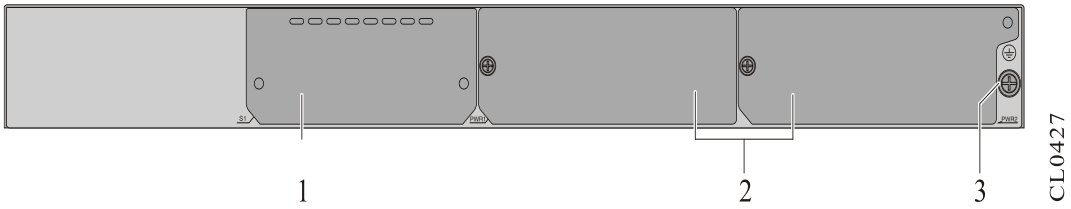


Figure 20-6 The rear panel of WNC6600-1000-AC/WNC6600-2000- AC

1. Empty baffle	2. Modular power supply (PWR1, PWR2)
3. Ground terminal	

21.3 Introduction to Optional Power Modules

WNC6600-500-AC, WNC6600-1000-AC/WNC6600-2000-AC provide two modular power supply slots, which support parallel operation of two power supplies for system power backup. Table 20-3 lists the modular power supply models and function descriptions supported by these two devices.

Table 20-3 Modular power supplies supported by WNC6600-500/1000/2000-AC

Model	Name	Remark
AD250-1S005E (V1)	250W AC power supply	100V~240V (3.5A) AC input,12V (21A) DC output, that is, the output power is 250W.
DD500-5D005E (V1)	500W DC power supply	-40V ~ -57V (15A) DC input,12V (10A) DC output, -53V (7A) DC output. The -53V power supply is a reserved PoE power supply, which is not used by this product.

21.3.1 AD250-1S005E (V1) Power Module

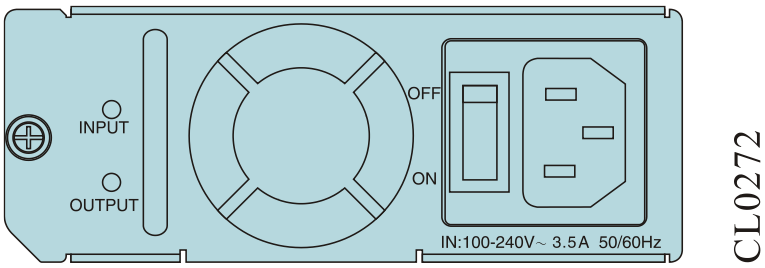


Figure 20-5AD250-1S005E (V1) power module panel diagram

copyright ©Maipu, all rights reserved

21.3.2 DD500-5 D 005E (V1) Power Module

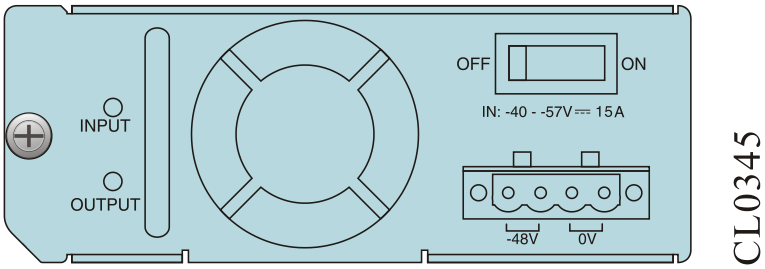


Figure 20-8 The panel of DD500-5D005E (V1) power module

Note

- Only WNC6600-500-AC, WNC6600-1000-AC, and WNC6600-2000-AC use modular power supplies, and WNC6600-100-AC uses built-in curing power supplies.
- WNC6600-500-AC, WNC6600-1000-AC, and WNC6600-2000-AC support 1+1 redundant backup and current sharing of dual power supplies of the same model, but do not support mixed insertion of AC and DC power modules.

21.4 Device Duct

The left and right sides of the wireless controller are the air inlet and outlet of the device, as shown in Figure 20.9. Enough space must be left on the left and right sides of the device (the space on the left and right sides should not be less than 60mm respectively) to ensure good ventilation.

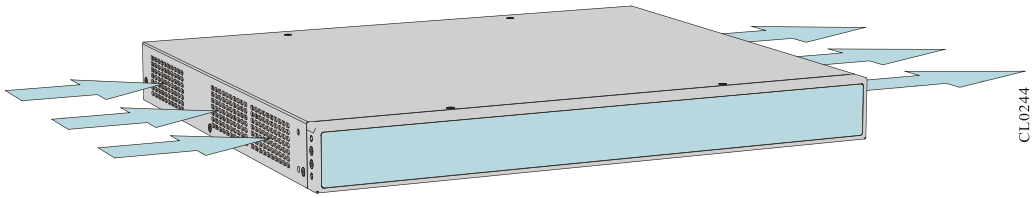


Figure 20-9 The air duct for the device

21.5 Physical Parameters

Table 20-3Physical parameters

Item	Description	
	WNC6600-100-AC	440mm x 380mm x 44.2mm

copyright ©Maipu, all rights reserved

Item	Description	
Dimensions (WxDxH)	WNC6600-500-AC	440mm x 420mm x 44.2mm
	WNC6600-1000-AC	
	WNC6600-2000-AC	
The maximum power consumption of the whole machine (full configuration)	WNC6600-100-AC	Static power: 39.2W Dissipated power (with POE): 58W POE power:123.2W
	WNC6600-500-AC	85W
	WNC6600-1000-AC	85W
	WNC6600-2000-AC	85W
Total Weight	WNC6600-100-AC	4.74Kg
	WNC6600-500-AC	7.32Kg (with two AD250-1S005E power supplies) 7.46Kg (with two DD500-5D005E power supplies)
	WNC6600-1000-AC NC6600-2000-AC	7.32Kg (with two AD250-1S005E power supplies) 7.46Kg (with two DD500-5D005E power supplies)
Modular power supply weight	AD250-1S005E	1.06Kg
	DD500-5D005E	1.14Kg
Rated input voltage of power supply	AC:100–240V 50/60Hz DC: -40 – -57V	
Short-term working temperature	-5℃–55℃	
Long-term working temperature	0℃~45℃	
Long-term working humidity	10%~90%	

Note

copyright ©Maipu, all rights reserved

- Short-term working conditions refer to working continuously for no more than 48 hours and accumulatively no more than15 days per year.

copyright ©Maipu, all rights reserved