



# **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 me 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	WNC6600-100-AC (V1)
Controller	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
ØNote	An alert that contains additional or supplementary information.

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:

lcon	Description
	Represents a generic switch

lcon	Description
$\mathbf{x}$	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.

## Contents

1 Lo	og into Device	ə10	
2 Q	Quick Configuration Guide14		
2.1	Local For	warding-wpa2-personal Authentication Configuration Guide	
	2.1.1	Networking Requirements	
	2.1.2	Network Topology	
	2.1.3	Configuration Ideas	
	2.1.4	Configuration Steps15	
	2.1.5	Result Verification	
2.2	Local For	warding-portal Authentication Configuration Guide	
	2.2.1	Networking Requirements	
	2.2.2	Network Topology	
	2.2.3	Configuration Ideas	
	2.2.4	configuration steps	
	2.2.5	Result Verification	
2.3	Centralize	ed Forwarding-wpa2-enterprise Authentication Configuration Guide	
	2.3.1	Networking Requirements	
	2.3.2	Network Topology	
	2.3.3	Configuration Ideas	
	2.3.4	Configuration Steps	
	2.3.5	Result Verification	
3 AP an	nd User Online	e Configuration	
3.1	VLAN and	d Interface Configuration	
3.2	Route Co	nfiguration	
3.3	DHCP Co	onfiguration	
	3.3.1	Configure AP Address Pool	
	3.3.2	Configure STA Address Pool	
3.4	Check Or	line Status of AP	
3.5	Wireless	Service Set Configuration	
3.6	AP Templ	late Configuration and Distribution	
	3.6.1	Create an AP Template	
	3.6.2	AP Template Delivery	
	3.6.3	Customize AP Configuration	
	3.6.4	DTLS Encryption Configuration	
4 Authe	ntication Fun	ction Configuration	

4.1	NAS Configuration
4.2	Connect to Portal Server
4.3	Add AC Device on radius
4.4	Add Authenticated Users on radius
4.5	802.1X Authentication Configuration
	4.5.1 Add Device
	4.5.2 Configure radius on AC
4.6	External Portal Authentication Configuration65
	4.6.1 Configure AC Device Name
	4.6.2 Portal Redirection Group Configuration and Application
5 WPA3	Authentication Configuration
5.1.	Centralized Forwarding-wpa3-enterprise Authentication Configuration Guide
	5.1.1 Networking Requirements
	5.1.2 Network Topology
	5.1.3 Configuration Ideas
	5.1.4 Configuration Steps
	5.1.5 Result Verification
5. 2 I	Local Forwarding-wpa 3-personal Authentication Configuration Guide
	5.2.1 Networking Requirements
	5.2.2 Network Topology
	5.2.3 Configuration Ideas
	5.2.4 Configuration Steps
	5.2.5 Result Verification
6 Portal S	Server Escape
7 Portal I	Rule Group
7.1	Introduction to Portal Rule Group90
7.2	Configure permit Rule Group
7.3	Configure redirect Rule Group
7.4	Configure CNA Rule Group
7.5	Apply portal Rule Group
8 Channe	el and Power Auto Adjustment
8.1	Configure AP Scanning Group
8.2	Add AP to Scan Group
8.3	Auto Power Adjustment
8.4	Auto Channel Adjustment
••••	

	9.1 Crea	ate an AP Scanning Group		
	9.2 Add	AP to Scan Group		
	9.3 Con	figure Rogues Rules		
	9.3.1	Configure Friendly Rules97		
	9.3.2	Configure Counter Rules		
	9.3.3	List of Rogues		
	9.4 RRI	<b>/</b> Reporting		
10	ACL Functio	n Configuration		
	10.1 AP A	CLs		
	10.1.1	Create Policy Set		
	10.1.2	Application of Policy Sets		
	10.2	BYOD ACLs		
	10.2.1	Overview of BYOD ACLs		
	10.2.2	Create Policy Set		
	10.2.3	Application of Policy Sets		
11	AP Unlimite	d Endurance (HAP Escape Technology)		
	11.1	Introduction to AP Unlimited Endurance		
	11.2	Networking Requirements		
	11.3	Create a HAP AP Group		
12	Timing Polic	y Configuration		
	12.1	Introduction to Timing Policy		
	12.2	Configure AP to Restart Regularly		
	12.3	Configure a Scheduled Radio Restart		
	12.4	Configure Radio Frequency to Enable in Time Range		
	12.5	Enable within Configured BSS Time Range		
13	Dual-Machir	e Hot Standby		
	13.1	Configure Standby Link		
	13.2	Configure an AP Standby Group		
	13.3	Add APs to Standby Group		
	13.4	DHCP Configuration (Ignore This Step if DHCP Is Not on AC)		
	13.4.1	Hot Standby Configuration		
	13.4.2 Address Pool Configuration			
13.4.3 Note on Configuration				
14	Troubleshoo	nting		
	14.1	RF Detection		
	14.2	Empty Capture		

14.2.	1 Server Configuration
14.2.2	2 Create a Packet Capture Task115
15 BYOD	
15.1	BYOD device identification configuration
15.2	NAC Policy
15.2.	1 VID Binding
15.2.2	2 Deny Access
15.3	BYOD ACLs
15.4	BYOD Client
16 Load Balan	<b>cing</b> 118
16.1	Load Balancing
16.2	Load Balancing Configuration
16.3	Load Balancing Switch
17 AC Configu	ration Synchronization
17.1	Add AC Link Channel
17.2	Synchronize AC Configuration
18 Device Upg	rade
18.1	Upgrade AC Mirror File
18.1.	1 Upgrade via HTTP123
18.1.2	2 Upgrade via FTP
18.2	Upgrade AP Software
18.2.	1 FTP Upgrade
18.2.2	2 Upgrade via CAPWAP
18.2.3	3 Online Auto Upgrade
19 License Co	nfiguration
19.1	Apply for License
19.2	Introduction to License
19.3	Query Method of SN No
19.4	License Query
19.5	Import and Export License
19.5.	1 Import License
19.5.2	2 Export License
20 Black and White List	
20.1	Configure Blacklist and Whitelist Rule Groups
20.1.	1 Create Rule Group
20.1.2	2 Add Terminal mac Configuration in Rule Group

	20.2	Enable Whitelist Function under Service Set
	20.3	Enable Global Blacklist Function
21	Attachment:	Product Introduction
	21.1	Product Forms
	21.2	Product Appearance and Dimension
	21.2.1	Appearance of WNC6600-100-AC
	21.2.2	Appearance of WNC6600-500-AC
	21.2.3	Appearance of WNC6600-1000-AC/WNC6600-2000-AC
	21.3	Introduction to Optional Power Modules
	21.3.1	AD250-1S005E (V1) Power Module
	21.3.2	DD500-5 D 005E (V1) Power Module142
	21.4	Device Duct
	21.5	Physical Parameters

# **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.

	USER LOGIN Username Account Password Password Login
Copyright © 2015 Maipu Commu	nication, All Rights Reserved
Recommend the use of browser over IE8.0,Op	timum screen resolution:1024768 pixels.

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 Figure 1.2.



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 Figure 1.3.

мліг	WNC6600-100	00-AC(V1) Wireless Controller	(!) ⇒
MONITOR	Basic Info Basic Config	Basic Config	×
ŝ	DTLS Config SNMP Config	Basic Config Time Zone Config MGMT Interface Config	
CONFIG	License AP Access Number	DC0 config	
DIAGNOSIS	Port Statistics Port Manage	IP Address: 192.168.1.100 Mask: 255.255.0	
DEVICE	User Manage AC Upgrade	MAC Address: (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
	AP Upgrade AC Backup	>     Submit	
	Login Authentication	3	
	Factory Reset Reboot		

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.

млія	WNC6600-1000	)-AC(VI	) Wireless Controller	r				(!) ⇒
MONITOR	Basic Info Basic Config		Basic Config					
ŝ	DTLS Config SNMP Config		Basic Config	Time Z	one Config MGMT In	erface Config		
CONFIG	License		AC Name		1111.0028.280.01			
	AP Access Number Port Statistics		AC Priority		4	(0~7)		
DIAGNOSIS	Port Manage		Host Name		AC1			
63	User Manage		Country/Region		CN V			
DEVICE	AC Upgrade							
	AP Upgrade	>	Note: switching the co	ountry / reg	gion will affect the configuration	of the channel value. Please confirm and then switch!		
LOG	AC Backup	>	Q. Submit					
	Login Authentication		6 Submic					
	Configuration	>						
	Factory Reset							
	Reboot							
			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 Figure 1.5.

мліг	WNC6600-1000-AC	C(V1) Wireless Controller	(!) ⇒
( MONITOR	Basic Info Basic Config	Basic Config	
ŝ	DTLS Config SNMP Config	Basic Config Time Zone Config MGMT Interface Config	
CONFIG	License	AC Name 1111.0028.280.01	
DIAGNOSIS	AP Access Number Port Statistics	AC Priority 4 (0~7)	
3	Port Manage	Host Name AC1	
DEVICE	AC Upgrade	Country/Region CN 🗸	
$\wedge$	AP Upgrade >	Note: switching the country / region will affect the configuration of the channel value. Please confirm and then switch!	
LOG	AC Backup >	🖉 Submit	
	Configuration >		
	Factory Reset		
	Reboot		





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

# **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 forwardi						
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

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)#

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

#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.



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.

uick Guide MONITOR NETWORK SERVICES E	DEVICE				
Your current position : Q	tuick Guide >> Basic Config				
Basic Config					
		0 0	0		
		2 3	4		
	Mode Settings Interfa	ce settings Access VLAN	Authentication	Discovery Mode	mish
			contiguration		
		Disco	very Mode		
	Discovery Mode	Static 🗸			
	Authentication Method	No Authentication			
	Tunnel Keepalive	Enable 👻			
	IP Protocol Support	IPv4 v			
	AC IPv4 Address	192.168.10.1			
	AC Control Port	5246			
	AC Data Port	5247			
	Secondary AC IPv4 Address				
	Secondary AC Control Port	5246			
		(mage)			
	Secondary AC Data Port	5247			

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

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 <u>http://192.168.10.1</u> 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.

	USER LOGIN	
	Username	
MAIDU	A Account	
	Password	
	Login	
Copyright © 2015 Maipu Commun Recommend the use of browser over IE8.0,Opti	cation, All Rights Reserved mum screen resolution:1024768 pixels.	

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.

0	Summary		AP List									
donitor _	Statistics	>	Filter Condition	Dnline AP 🗸		Sort	Mode	IP Ascending Order	~			
<b>کې</b>	STA List		C Export CSV File							Total : 2; Onlin	e : 2, Connectir	ıg : 0, Offline : 0
Ĥ	Rogue List Rogue Rules	>	MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated STAs
AGNOSIS	RRM Report		CC:D8:1F:96:74:6E	10.11.12.213	10.11.12.213(57795)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	Q
2 Device			CC:D8:1F:96:70:E4	10.11.12.223	10.11.12.223(46867)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٥



#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.

млі	ipu WNC6600-1000-2	C(V1) Wireless Controller	() 🔿
$\bigcirc$	Interface Config >		
(°) MONITOR	Static Route	Basic Set	
	DHCP >	Wireless Service Name wlan1	
<b>5</b>	WLAN ~		
CONFIG	Wireless Service	Service Status Enable 🗸	
Ð	AP Template	Forwarding Mode Distributed forwarding 🐱	
DIAGNOSI	IS AP Group	SSID abc -	
Ľ	AP Config	Encoding Format UTF8 🗸	
DEVICE	AP Login Management		
Λ	AAA >	SSID Hidden Disable 🗸	
	Access Control >	User VLAN 100 *	
	RRM >	Max User Per BSS 128	
	BYOD		
	Load Balance	User Isolation Enable 🗸	
		Lead Balance Disable ~	
		Security	
		Auth Type WPA2-Personal	
		NAS Search Disable 🗸	
		Encrypt Type AES 🗸	
		GTK Auto Refresh Disable 🗸	
		GTK Refresh Period 24 *(1-10000)H	
		Password ······	

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.

$\sim$	Interface Config	$\rightarrow$	= ,	AP Ten	nplate								
ONITOR	Static Route												
	DHCP	>		Templ	ate Name								
ŝ	WLAN	$\sim$		+ 0	ronto d'Edit III Doloto G	Analy D (	Fores to Apply						
NFIG	Wireless Service			τu	reate / Euit in Delete 0	Apply Of	Force to apply						
า	AP Template				AP Template Name		Radio			WLAN			
	ARGroup					Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type
10.010	Arthoup					1	HT20	6					
3	AP Config				Default_FitAP_Profile	2	HT40	Auto					
ICE	AP Login Managem	ent											
、	ААА	>			profile1	1	HIZO	6					
7	Access Control	>				2	HT40	Auto					
G												< <	1 > > 2

#### 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.

$\bigcirc$	Interface Config	> =	Edit AD	Template							
ONITOR	Static Route		Eult AF	rempiace							
	DHCP	>	Dasis	Dadia DCC	Band		Advanced Config Tim	. Zono Config			
<u>نې</u>	WLAN	~	Dasic	Radio DSS	Danu	width	Advanced Conlig Time	e zone conlig			
ONFIG	Wireless Service		No.	Wireless Service Nan	ne	Radio ID	User VLAN	SSID	Auth Type	Encrypt Type	
<del>〕</del>	AP Template		1	wlan1	~	ALL 🗸	100	abc	WPA2-Personal	AES	Advance
SNOSIS	AP Group		2	Close	~	1 🗸					Advance
2	AP Config		3	Close	~	1 🗸					Advance
VICE	AP Login Manageme	ent	4	Close	~	1					■ Advance
~	AAA	>		01							
<u>!\</u>	Access Control	>	5	Close	~	1 ¥					Advance
0G	RRM	>	6	Close	~	1 🗸					Advance
	BYOD	>	7	Close		1					the second

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.

мліғ	WNC6600-10	000-AC(V1)	Wireles	S Controller							(!) ⇒
$\bigcirc$	Interface Config	>	AP Co	nfig							1
MONITOR	Static Route						hene				
	DHCP	>	AP Gr	oup Group Type	Image Upgrade v		NONE ¥		HT JoinGro	oup 🗄 Le	aveGroup
<b>5</b> 35	WLAN	~	AP Ter	nplate listNONE	~				-		88 Apply
CONFIG	Wireless Service									L	
Ð	AP Template		Filter	Condition ALL	~						⊽ Filter
DIAGNOSIS	AP Group	+ Create / Edit III Delete (), Reboot (), Reset									
E.	AP Config										Backup
DEVICE	AP Login Management			MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Status
	ААА	>		CC:D8:1F:96:74:6E	Customization	profile1	WA2600-821-PE(V2)	NONE		Online	Master
	Access Control	>		CC:D8:1F:96:70:E4	Customization	NONE	✓ WA2600-821-PE(V2)	NONE		Online	Master
	RRM	>									
	BYOD	>									
	Load Balance								<	< 1 >	>  20 ~

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.

мліг	WNC660	0-1000-AC(V	1) Wireles	s Controller									(!) ⇒
	Summary	=	STA List	:									^
MONITOR	Statistics	>	<b>E</b> 1										
	AP List		Filter O	NLL V									∀ Filter
र्छेः	STA List		C, Ref	resh 😾 Force to Off	line 🔒 Export	CSV File						Total : 1 On	line:1 Offline: 0
CONFIG	Rogue List	>	0		e. e.t.								
Ĥ	Rogue Rules	>		MAC	IP	Status	AP Name	AP Location	SSID	Frequency Band	OS	Online Time	Tx/Rx Rate
DIAGNOSIS	RRM Report			6A:EE:64:08:18:52	10.11.12.233	Authorized	WA2600-821-PE(V2)		abc	5G	Unknown	2023-01-17 22:04:58	0 bps/0 bps
DEVICE Log												<u>i</u> <u>&gt;</u> <u>&gt;</u>	≥l 20 v

Figure2.10 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 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:

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

- 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

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

SW2#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 (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.

#### 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

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.

lick Guide	Your current position : Quick Guide >	> Basic Config							
Basic Config									
			2	-3		5	_	-6	
		Mode Settings Interfa	ace Settings	Access VLAN	Authentication	Discovery M	lode	Finish	
					Configuration				
				Discove	ery Mode				
		Discovery Mode	Static 🗸						
		Authentication Method	No Authentication						
		Tunnel Keepalive	Enable 🛩						
		IP Protocol Support	IPv4 V						
		AC IPv4 Address	192.168.10.1	•					
		AC Control Port	5246						
		AC Data Port	5247						
		Secondary AC IPv4 Address							
		Secondary AC Control Port	5246						
		Secondary AC Data Port	5247						

## 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 <u>http://192.168.10.1</u> 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.

	USER LOGIN
	Username
	A Account
MVIDO	Password
	Password
	Login
Copyright © 2015 Maipu Commu Recommend the use of browser over IE8.0,0p	unication, All Rights Reserved Dtimum screen resolution:1024768 pixels.



#Click MONITOR > AP list, and you can see that the AP is online, as shown in Figure 2.15 below.

2	Summary		AP List									
TOR _	Statistics	>										
	AP List		Filter Condition	Jhiine AP		Sort	Mode	IP Ascending Order	~			V Filter
}	STA List		C Export CSV File							Total : 2: Onlin	e : 2. Connectin	a : 0. Offline :
TG.	Rogue List	>						-				Aller Manager
1	Rogue Rules	>	MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated ST
OSIS	RRM Report		CC:D8:1F:96:74:6E	10.11.12.213	10.11.12.213(57795)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٩
			CC:D8:1F:96:70:E4	10.11.12.223	10.11.12.223(46867)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	Q
S CF												

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.

мліг	WNC6600	-1000-AC	(V1) Wireless	Controller	(!) ⇒
	Interface Config	>	NAS Conf	fig	<b>^</b>
MONITOR	Static Route				
	DHCP	>	IP	10.11.12.61 🗸	+ Add
<b>{</b>	WLAN	>			
CONFIG	AAA	~	🗊 Delet	te	
Ŧ	NAS			IP	
DIAGNOSIS	Portal			100.0.52.10	
e,	Radius				
DEVICE	Domain				
^	Access Control	>			
	RRM	>			
LOG	BYOD	>			
	Load Balance				



#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.

МЛІ	WNC6600	-1000-AC(	V1) Wireless Controller			
$\bigcirc$	Interface Config	>	Add Portal			ĺ.
MONITOR	Static Route					
	DHCP	>	Portal Name	portal	*	
<b>{</b>	WLAN	>	Portal IP	192.168.10.253 * IP or H	Host	
CONFIG	AAA	~				
Ĥ	NAS		URL	http://192.168.10.253:80/portal/Login.do o	ogin.do * r https://192.168.1.1:443/portal/Login.do	
DIAGNOSIS	Portal			ORC-Param configuration		
	Bading		Register Keepalive	Enable 🗸		
25	Rautus		Register Timeout	600 * (60~3	3600\$)	
DEVICE	Domain					
^	Access Control	>	Keepalive Timeout	30 * (3~36	500s)	
	RRM	>	Portal Server Escape	Disable 🗸		
LOG	BYOD	>				
	Load Balance		Server Recovery Offline STA	Disable v		
			Redirect Pre-shared Key			

Figure 2.17 Portal configuration

vi5	U WNC6600	-1000-AC(V	1) Wireless Controller		
	Interface Config	> 📃	Portal IP	192.168.10.253 * IP or Host	
or	Static Route				
	DHCP	>	URL	http://192.168.10.253:80/portal/Login.do  * http://192.168.1.1:80/portal/Login.do or https://192.168.1.1:443/portal/Login.do	
	WLAN	>		URL-Param configuration	
G	AAA	~	Register Keepalive	Enable 🗸	
	NAS		Register Timeout	600 8 (50-3500-)	
2120	Portal		Register Timeout	- (00~3600s)	
.515	Padins		Keepalive Timeout	30 * (3~3600s)	
	Kadius		Portal Server Escane	Disable v	
Е	Domain		Fortal Server Escape		
	Access Control	>	Server Recovery Offline STA	Disable 🗸	
5	RRM	>	Redirect Pre-shared Key		
	BYOD	>	·····,		
	Load Balance				
			Config NAS Address		
			IP 100.0.52.10 v	+ Add	
				IP	
				100.0.52.10	
			Submit Cancel		

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.

млір	WNC6600	)-1000-AC	(V1) Wireless Controller	(!) ⊖
$\bigcirc$	Interface Config	>	Add Auth Server	
MONITOR	Static Route			
	DHCP	>	Server Index 1 v	
<b>ç</b> ş	WLAN	>	Server Type Authentication Server	
CONFIG	AAA	~		
Ĥ	NAS		Server IP 192.168.10.253	
DIAGNOSIS	Portal		Server Port 1812 *(1~65535)	
N	Radius		Request Retransmission Times 2 *(2~10)	
DEVICE	Domain		Request Retransmission Interval 5 *(5~300)	
~	Access Control	>		
	RRM	>		
LOG	BYOD	>	Config NAS Address	
	Load Balance		10 100 0.52 10 v Pre-shared Key •••••	
			IP Pre-shared Key	
			⊘ Submit ⊙ Cancel	

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.

млія	WNC6600	-1000-AC	C(V1) Wireless Controller		(!) ⇒
	Interface Config	>	Add Domain		1
MONITOR	Static Route				
historia	DHCP	>	Domain	уи *	
<b>{</b>	WLAN	>	Authentication Status	Enable 🗸	
CONFIG	ААА	~			
Ĥ	NAS		Authentication Server	Auth_1_192.168.10.253 ~ + Add	
DIAGNOSIS	Portal			Auth_1_192.168.10.253 Delete	
N.	Radius		Accounting Status	Enable 🗸	
DEVICE	Domain		Accounting Server	Acct 1 192 168 10 253	
•	Access Control	>	2	Aret 1 102 168 10 253	
	RRM	>		Delete	
LOG	BYOD	>	Accounting Update Period	30 s(0~360), 0: disable	
	Load Balance				
			⊘ Submit 💿 Cancel		

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.

млі	WNC6600-10	000-4	C(V1) Wireless Controller		(!)  ()
( )	Interface Config Static Route	>	Wireless Service		
MONITOR	DHCP	>	Basic Set		
<b>{</b>	WLAN	$\sim$	Wireless Service Nam		
CONFIG	Wireless Service		Wireless bervice Nam	VIOITA -	
( <del>†</del> )	AP Template		Service Status	Enable 🗸	
DIAGNOSIS	AP Group		Forwarding Mode	Distributed forwarding $\checkmark$	
E,	AP Config		SSID	abc -	
DEVICE	AP Login Management	t	Encoding Format	UTF8 🗸	
$\wedge$	ААА	×	2010 15 11	Dirable	
LOG	NAS		SSID Hidden		
	Portal		User VLAN	100 *	
	Radius		Max User Per BSS	128	
	Domain		User Isolation	Enable 🗸	
	Access Control	>		Director	
	RRM	>	Load Balance	Disable V	
	BYOD	>	Security		
	Load Balance		Auth Type	Open v	
			rout tipe		
			Portal Auth	Disable 🗸	

Figure 2.21 Wireless service configuration

			-	Max User Per B55	128	
$\bigcirc$	Interface Config	>				
IONITOR	Static Route			User Isolation	Enable 🗸	
	DHCP	>		Load Balance	Disable 🗸	
 	WLAN	$\sim$		Load Datance		
CONFIG	Wireless Service			Security		
(fi)	AP Template			Auth Type	Open	
AGNOSIS	AP Group					
5	AP Config			Portal Auth	Enable V	
S.	AP Login Manageme	ent		Portal Server Name	portal 🗸	
JEVICE .	444	~		Portal Rule Set	NONE V	
$\triangle$						
LOG	NAS			Radius Auth Domain	yu 🗸	
	Portal			No Perception Authentication	Enable v	
	Radius			No Perception Authentication		
	Domain			MAC Authentication	Disable 🗸	
	Access Control	>		NAS Search	Enable 🗸	
	RRM	>		AC-IP	100.0.52.10	
	BYOD	>				
	Load Balance			Signed Key		

Figure 2.22 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.

мдія	WNC6600-10	000-AC(V1	) Wire	eless Controller								(!) ⊖		
$\bigcirc$	Interface Config	> 📃	AP T	emplate										
MONITOR	Static Route													
	DHCP	>	Terr	nplate Name										
ŝ	WLAN	~	+	Create & Edit III Delete D A	ooly DE	orce to Apply								
CONFIG	Wireless Service		-	Create F Luit B Delete OA	pply O I	огсе со мррну								
Ĥ	AP Template			AP Template Name		Radio				WLAN				
DIAGNOSIS	ABGraue			in template name	Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type		
5110110010	Ar Gioup				1	HT20	6							
25	AP Config			Default_FitAP_Profile	2	HT40	Auto							
DEVICE	AP Login Management	t.				LIT20								
~	AAA	~		profile1	-	HIZO	0							
	NAS				2	HT40	Auto							
100	Portal										1< <	1 ≥ ≥  20 ∨		
	Radius													
	Domain													



#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.

$\bigcirc$	Interface Config	>										
( ° )	Static Route		Edit AP	emplate								
	DHCP	>										
ŝ	WLAN	$\sim$	Basic	Radio	BSS Bandy	width		Advanced Config Time A	cone Config			
ONFIG	Wireless Service		No.	Wireless	Service Name	Ra	idio ID	User VLAN	SSID	Auth Type	Encrypt Type	
ŧ	AP Template		1	wlan1	~		ALL 🗸	100	abc	Open	NONE	Advanced
SNOSIS	AP Group		2	Close	~		1 ~					Advanced
2	AP Config		3	Close	~		1 ~					Advance
VICE	AP Login Manageme	nt	4	Close	~		1 ~					Advance
î\	AAA	~	5	Close	~		1 🗸					Advance
G	NAS			Close			1					th Advance
	Portal		0	0.000	-							E Advance
	Radius		7	Close	~		1 v					Advance
	Domain		8	Close	~		1 ~					Advance
	Access Control	>	9	Close	~		1 ~					Advance
	RRM	>	10	Close	~		1 ~					Advance
	BYOD	>	11	Close	~		1 ~					Advance
	Load Balance		12	Close	~		1 🗸					Advance

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.

мліг	WNC6600-	1000-AC	(V1) Wire	eless Controller							(!) ⇒
$\bigcirc$	Interface Config	>	AP C	Config							^
MONITOR	Static Route										
	DHCP	>	AP C	Group Group Type	Image Upgrade 🗸		NONE 🗸		BP JoinGro	pup 🔛	LeaveGroup
<b>{</b>	WLAN	~	AP T	emplate listNONE	~						88 Apply
CONFIG	Wireless Service										
Ŧ	AP Template		Filte	er Condition ALL	~						⊽ Filter
DIAGNOSIS	AP Group		+	Create & Edit III	Delete	C. Deset					
N	AP Config		-	create y cuit m	O REDUCT	O Reset					
DEVICE	AP Login Manageme	ent	C	] MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Status
~	ААА	~	2	CC:D8:1F:96:70:E4	Customization	profile1 ~	WA2600-821-PE(V2)	NONE		Online	Master
LOG	NAS		C	CC:D8:1F:96:74:6E	Customization	-NONE V	WA2600-821-PE(V2)	NONE		Online	Master



#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.

 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.  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 <u>http://[1::1]</u>, 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.

мліғ	MAIPU WNC6600-1000-AC(V1) Wireless Controller												
0	Summary		STA Lis	t									^
MONITOR	Statistics	>											
	AP List		Filter C	Option ALL	~								∀ Filter
CONFIG	STA List	、 、	🖒 Re	fresh	line 🗍 Expor	t CSV File						Total : 1 Onl	ine:1 Offline : 0
Ĥ	Rogue Rules	>		MAC	IP	Status	AP Name	AP Location	SSID	Frequency Band	OS	Online Time	Tx/Rx Rate
DIAGNOSIS	RRM Report			6A:EE:64:08:18:52	10.11.12.233	Authorized	WA2600-821-PE(V2)		abc	5G	Unknown	2023-01-17 22:04:58	0 bps/0 bps
DEVICE												ح 1 ک	≥! 20 ~
LOG LOG													
					Fi	aure 2	.26 Termina	al 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.

## 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

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

## Topology introduction:

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

- 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.

#### 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
#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.



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.

NVIDU	Wireless Access Point	
uick Guide MONITOR NETWORK SERVICES DEV	ACE	
Your current position : Quick	k Guide >> Basic Config	
Basic Config		
		6
	Mode Settings Interface Settings Access VLAN Authentication Discovery Mode Fi	nish
	Configuration	
	Discovery Mode	
	Discovery Mode Static 🛩	
	Authentication Method No Authentication	
	Tunnel Keepalive Enable 🗸	
	IP Protocol Support	
	AC IPv4 Address 192.168.10.1	
	AC Control Port 5246	
	AC Data Port 5247	
	AC Data Port 5247   Secondary AC IPv4 Address	
	AC Data Port 5247   Secondary AC IPv4 Address Secondary AC Control Port 5246	
	AC Data Pert 5247 * Secondary AC IPv4 Address Secondary AC Data Pert 5246 Secondary AC Data Pert 5247	
	AC Data Port 5247  Secondary AC Div4 Address Secondary AC Control Port 5246 Secondary AC Data Port 5247 Ivmn Crotho Guide Pravious	Einich

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.....

#### 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 <u>http://192.168.10.1</u> 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

	USER LOGIN Username R Account
	Password Password Password
	Login
Copyright © 2015 Maipu Commun Recommend the use of browser over IE8.0,Opt	nication, All Rights Reserved limum screen resolution:1024768 pixels.

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

2	Summary		AP List									
ITOR _	Statistics	>	Filter Condition	Dolino AP		Fort	Mode	IP Ascending Orde				V7 Pilker
3	AP List					3010	Houe	IT Pacending Order	Ŷ			v Fliter
2	STA List		C Export CSV File							Total : 2: Onlin	e : 2. Connectir	ia:0. Offline:0
IG	Rogue List	>	La capore corrine					-				
ć.	Rogue Rules	>	MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated STA
SIS	RRM Report		CC:D8:1F:96:74:6E	10.11.12.213	10.11.12.213(57795)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٩
			CC:D8:1F:96:70:E4	10.11.12.223	10.11.12.223(46867)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	۵

#### 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.

млір	WNC6600-	-1000-A0	C(V1)	Wireless Contr	roller 🕕 Sweet prompt in the main propared scenario please couling other device after successing couling current device. (]	) )
	Interface Config	>	=	NAS Config		^
MONITOR	Static Route					
	DHCP	>		IP	10.11.12.61 ¥	vdd
<u></u>	WLAN	>				
CONFIG	AAA	~		Delete		
Ð	NAS				Ib	
DIAGNOSIS	Portal				100.0.52.10	
e.	Radius					
DEVICE	Domain					
A	Access Control	>				
	RRM	>				
LOG	BYOD	>				
	Load Balance					

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.

мліг	WNC6600	-1000-AC	(V1) Wireless Controller		() Sweet prompt In the main prepared scenario, please	config other device after successing config current device.	(!)	$\ni$
$\bigcirc$	Interface Config	>	Edit Auth Server					^
MONITOR	Static Route DHCP	>	Server Index 1					
ŝ	WLAN	>	Server Type Aut	hentication Server				
CONFIG	ААА	~	Server IP 19	2.168.10.253				
Ð	NAS		Sequer Port	212	(50)			
DIAGNOSIS	Portal		Derver Port					
Ś	Domain		Request Retransmission Times 2	*(2~)	(0)			
DEVICE	Access Control	>	Request Retransmission Interval 5	*(5~:	800)			
	RRM	>						
	BYOD	>	Config NAS Address					
	Load Balance		IP 100.0.52.10 v Pre-	-shared Key	+ Add			
			IÞ		Pre-shared Key			
			100.0.52.10		•••••			
			⊘ Submit 💿 Cancel					

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.

$\bigcirc$	Interface Config	>	Edit Domain			
ONITOR	Static Route					
	DHCP	>	Domain	уч		
<u>ي</u>	WLAN	>	Authentication Status	Enable		
ONFIG	AAA	~				
Â	NAS		Authentication Server	Auth_1_192.168.10.253 ~	+ Add	
	Portal			Auth_1_192.168.10.253	🔟 Delete	
NS.	Radius		Accounting Status	Enable 🗸		
EVICE	Domain		Accounting Server	Acct_1_192.168.10.253 ~	+ Add	
A	Access Control	>		Acct 1 192.168.10.253		
	RRM	>			11 Delete	
LOG			Association Hadeta Declark	20 s(0-360) 0; disphis		

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.

млія	WNC6600	-1000-AC(V1	1) Wireless Controller		(!) →
$\bigcirc$	Interface Config	>	Martine Cambra		1
MONITOR	Static Route		wireless Service		
	DHCP	>	Basic Set		
र्द्रे	WLAN	$\sim$	Wireless Canvise Name	whent	
CONFIG	Wireless Service		wireless Service Name	wiani	
ŧ	AP Template		Service Status	Enable 🗸	
DIAGNOSIS	AP Group		Forwarding Mode	Centralized forwarding ~	
25	AP Config		SSID	abc	
DEVICE	AP Login Manager	nent	Encoding Format	UTF8 🗸	
~	AAA	>			
	Access Control	>	SSID Hidden	Disable 🗸	
	RRM	>	User VLAN	100 *	
	BYOD	>			
	Load Balance		Max User Per BSS	128	
			User Isolation	Enable 🗸	
			Load Balance	Disable 🗸	

Figure 2.35 Wireless service configuration

млір	WNC6600-1	000-AC	C(V1) Wireless Controller		(!)  ()
$\bigcirc$	Interface Config	$\rightarrow$	5510	*	1
( °) MONITOR	Static Route		Encoding Format	UTF8 🗸	
	DHCP	>	SSID Hidden	Disable 🗸	
<u></u>	WLAN	$\sim$			
CONFIG	Wireless Service		User VLAN	100 *	
Ŧ	AP Template		Max User Per BSS	128	
DIAGNOSIS	AP Group		User Isolation	Enable 🗸	
ES -	AP Config		Load Balance	Disable 🗸	
DEVICE	AP Login Managemer	at			
$\wedge$	AAA	>	Security		
	Access Control	>	Auth Type	WPA2-Enterprise 🗸	
	RRM	>			
	BYOD	>	Radius Auth Domain	yu 🗸	
	Load Balance		NAS Search	Disable ~	
			Encrypt Type	AES 🗸	
			GTK Auto Refresh	Disable 🗸	
			GTK Refresh Period	24 *(1-10000)H	
			Submit Cancel		

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.

мліг	WNC6600-1	1000-AC(	(V1) V	Wirel	ess Controller									(!)
$\bigcirc$	Interface Config	>	A	AP Tei	mplate									
MONITOR	Static Route													
	DHCP	>		Temp	olate Name									V Search
- ()	WLAN	~		+ 0	reate 🖌 Edit	iii Delete 🕞 A	only D Fr	orce to Apply						
CONFIG	Wireless Service							eres co replicit						
Ĥ	AP Template				AP Templat	e Name		Radio					WLAN	
DIAGNOSIS	AP Group			_			Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type
	AD Config			_	Default Fit	D D	1	HT20	6					
63	Arconig			0	Derault_Fitz	w_prome	2	HT40	Auto					
DEVICE	AP Login Manageme	nt					1	HT20	6					
$\wedge$	AAA	>			profil	e1	2	HT40	Auto					
	Access Control	>					2	1140	AUTO					
	RRM	>											<u> &lt;</u>	1 ≥ ≥  20∨
	BYOD	>												
	Load Balance													

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.

млі	WNC6600-10	00-AC(V	1) Wireless Co	ontroller							(!) ⊝
$\bigcirc$	Interface Config	> =									
( ° ) MONITOR	Static Route		Edit AP 1	emplate							
	DHCP	>	Desis	Dedia DCC	Pered		Advanted Config	7			
<u></u>	WLAN	~	Dasic	Radio BSS	Band	wiath	Advanced Conlig	me zone Config			
CONFIG	Wireless Service		No.	Wireless Service Na	me	Radio ID	User VLAN	SSID	Auth Type	Encrypt Type	
ŧ	AP Template		1	wlan1	~	ALL 🗸	100	abc	WPA2-Enterprise	AES	Advanced
DIAGNOSIS	AP Group		2	Close	~	1 🗸					Advanced
ES -	AP Config		3	Close	~	1 v					Advanced
DEVICE	AP Login Management		4	Close	~	1 v					自 Advanced
^	ААА	>									
<u>_!</u> _	Access Control	>	5	Close	~	1 ~					Advanced
LOG	RRM	>	6	Close	~	1 ~					Advanced
	BYOD	>	7	Close	~	1 v					Advanced
	Load Balance		8	Close	~	1 🗸					Advanced

#### 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.

млір	WNC6600-10	00-AC(V1	) Wirele	ss Controller			() Sweet prompt: In t	he main prepared scenario,please confi	ig other device after successing	g config current de	vice. $(!) \rightarrow$
$\bigcirc$	Interface Config	> 🔳	AP Con	fig							^
MONITOR	Static Route										
	DHCP	>	AP Gro	up Group Type	Image Upgrade 🗸		NONE 🗸		BP JoinGro	pup 8º	LeaveGroup
<u></u>	WLAN	~	AP Tem	plate listNONE	~						88 Apply
CONFIG	Wireless Service										
Ŧ	AP Template		Filter C	Condition ALL	~						⊽ Filter
DIAGNOSIS	AP Group		-h ce	anta di Estis di	Delete O Deheet	đ. Davat					
N	AP Config		- CI	eate / Luit III C	Velete (c) Rebuut	C Reset					
DEVICE	AP Login Management			MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Status
~	ААА	>		CC:D8:1F:96:74:6E	Customization	profile1	✓ WA2600-821-PE(V2	)NONE		Online	Master
	Access Control	>		CC:D8:1F:96:70:E4	Customization	-NONE	<ul> <li>WA2600-821-PE(V2</li> </ul>	)NONE		Online	Master
200	RRM	>									
	BYOD	>									
	Load Balance								<	< 1 >	>  20 ~

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. • 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.

# **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.

мді≓	WNC6600	-1000	-AC(V1) Wirel	ess Controlle	er				(!) ⇒
$\bigcirc$	Interface Config	~	VLAN						î.
MONITOR	VLAN Config		+ 40	d 🗊 Delete	C. Defrech				
562	VLAN IP Address	Config	1 00	Delete	O Relicial				
CONFIG	Port Mode Config	I		VLAN ID	Description	Tag Ports	Untag Ports	CAPWAP Data Forwarding	Edit
	Static Route						gi0/2 gi0/3 gi0/4 gi0/5 gi0/6 gi0/7		
$\oplus$	DHCP	>					gi0/8 gi0/9 gi0/10		
DIAGNOSIS	WLAN	>		1	DEFAULT		gi0/11 gi0/12 gi0/13 gi0/14 gi0/15 gi0/16	NOT SUPPORTED	2
E.	AAA	>					gi0/18 gi0/19 gi0/20 gi0/21 gi0/22 gi0/23		
DEVICE	Access Control	>					gi0/24		
•	RRM	>		100	AC VIAN		teo/1 teo/2	NOT SUPPOPTED	
	BYOD	>	0	100	AC_1041			NOT SOTTORIES	
LOG	Load Balance			401	AP_Manage_VLAN			NOT SUPPORTED	×
				402	STA_Service_VLAN			NOT SUPPORTED	<b>87</b>
				555	LAN		gi0/1	NOT SUPPORTED	
				1000	VLAN1000		gi0/17	NOT SUPPORTED	8
								<u> ≤</u> ≤ <u>1</u> ≥ ≥  15	per page 🗸
			()	VLAN 1 is the When adding, When the VLA	default VLAN,and it can't be deleted. you can choose one or more ports from N to which the Access port belongs is	n "All Ports" List into deleted, the port wou	"Ports of VLAN",or delete any port from "Port Ild be added to the default VLAN 1.	s of VLAN".	
			4						+

Figure 3.2 Configure vlan and interface address

# 🖉 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.

	Interface Config	~ 🔳	VLAN						
	VLAN Config								
0.0	VLAN IP Address	Config	+ Ad	ld 🔟 Delete	🖒 Refresh				
25	Port Mode Config			VLAN ID	Description	Tag Ports	Untag Ports	CAPWAP Data Forwarding	Edi
FIG	Static Route						gi0/2 gi0/3 gi0/4		
)	DHCP	>					gi0/8 gi0/9 gi0/10		
IOSIS	WLAN	>		1	DEFAULT		gi0/11 gi0/12 gi0/13 gi0/14 gi0/15 gi0/16	NOT SUPPORTED	
Y.	AAA	>					gi0/18 gi0/19 gi0/20		
S CE	Access Control	>					gi0/21 gi0/22 gi0/23 gi0/24		
	RRM	>	-				te0/1 te0/2		
7	BYOD	>	U	100	AC_VLAN			NOT SUPPORTED	
5	Load Balance			401	AP_Manage_VLAN			SUPPORTED	
				402	STA_Service_VLAN			SUPPORTED	
				555	LAN		gi0/1	NOT SUPPORTED	
				1000	VLAN1000		gi0/17	NOT SUPPORTED	2
								<u> &lt; 1</u> <u>&gt; &gt; </u> 15	per page 🗸
			i	VLAN 1 is the When adding,	default VLAN, and it can't be deleted. you can choose one or more ports fro	om "All Ports" List into "P	Ports of VLAN", or delete any port from "Ports	of VLAN".	

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.

мліг	WNC6600-1	1000-AC(V	1) Wireless	Controller					(!) ⇒
MONITOR	Interface Config VLAN Config	~ 🔳		ddress Configure					
CONFIG	VLAN IP Address C	Config		VLAN ID	IP Address	Network Mask	MAC Address	Primary/Secondary	Operation
	Static Route	>		VLAN 555 VLAN 1000	10.11.12.61	255.255.255.0	ccd8.1f43.81da	Primary Address Primary Address	22 22
L.	WLAN AAA	>		VLAN 401 VLAN 402			ccd8.1f43.81da	Primary Address Primary Address	*
	RRM BYOD	>						l≤ ≤ 1 ≥ ≥l 15	per page 🗸
LOG	Load Balance		()	You can configure virtu You cannot configure se If you want to delete pe	al IP address and mask acondary ip address bef rimary ip address,you m	by VLAN interface. ore the primary ip address is confi ust delete secondary ip address fi	gured rst.		

#### Figure 3.4 Create vlan

млір	WNC6600	-1000-AC(\	/1) Wireless Controller					(!) ⇒
$\bigcirc$	Interface Config	~	Config VLAN IP Address	1	×			î
MONITOR	VLAN Config		VLAN ID (1	range:1~4094) *				
<u></u>	Port Mode Config	Config	IP Address	(format as:192.168.0.1)	k Mask	MAC Address	Primary/Secondary	Operation
CONFIG	Static Route		IP addres type  Primary Address	O Secondary Address	i.255.0	ccd8.1f43.81da	Primary Address	
	DHCP	>	Network Mask as:255.255.255.0)	(format	\$.255.0	ccd8.1f43.81da	Primary Address	2
DIAGNOSIS	WLAN	>	MAC Address as:0001.7A4F.74D2)	(format		ccd8.1f43.81da	Primary Address	2
DEVICE	Access Control	>	OK Cancel			ccd8.1f43.81da	Primary Address	2
	RRM	>					l≤ ≤ 1 ≥ ≥l	15 per page 🗸
	BYOD	>						
103	Load Balance		(i) You can configure virtu You cannot configure s If you want to delete p	aal IP address and mask by VLAN interf econdary ip address before the primar rimary ip address,you must delete sec	ace. y ip address is cor ondary ip address	nfigured first.		

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.

3	Interface Config 👻 🗏 Route Config								
ONITOR	VLAN Config								
~~~	VLAN IP Address Co	onfig	+ Add	🗊 Delete 💍 Refresh	1				
	Port Mode Config			Destination Prefix	Destination Prefix Mask	Next Hop IP/Interface	Distance Metric	Track ID	Tag Next Hop
~	Static Route			0.0.0.0	0.0.0.0	10.11.12.254	1		
÷	DHCP	>		0.0.0.0	0.0.0.0	192.168.100.254	10		
GNOSIS	WLAN	>							15 per page v
<u>г</u>	AAA	>					21		To per page +
EVICE	Access Control	>	Static Route	Config					
A	RRM	>							
<u>'!\</u>	BYOD	>	Destination P	Prefix	*				
.OG	Load Balance		Destination P	Prefix Mask	•				
			Next Hop IP/	(Interface	address 🗸	*			
			Distance Met	tric	1 (range:1~2	255. default:1)			
			Track ID		(range:1~5	500)			
			Tag		(range:1~4	1294967295)			
			Next Hop		(length:0~:	31)			

Figure 3.6 Add route

## 3.3 DHCP Configuration



 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.

мдір	WNC6600-1	1000-AC(\	/1) Wireless Cor	ntroller							(!	
MONITOR	Interface Config Static Route	> =	DHCP Service	st								
CONFIG	DHCP DHCP Pool Config	Ŭ.	+ Add 🗎 I	Delete								
ŧ	Backup Config Relay Config			Name	Туре	IP Info	Mask t found any data	Gatew	ау		Operation	
DIAGNOSIS	Static IP List Client List								<u> </u> <	≤ 1 ≥	≥l 15 per page	9 ¥
DEVICE	WLAN	>	DHCP Config		ost <sup>O</sup> Network							
rog	Access Control	>	Name		•	(length:1~31 characters)						
	BYOD Load Balance	>	Start IP Addr.		•							
			Mask		•							
			Gateway	1.1.1.1,2.2.2.2	2)	No more then 8 default gateway c	in be configed.separate	ed by ','. eg:				
			Lease	1	•	(unit:day, range:0~365, default:	.)					
				D		<ul> <li>(unit:nour, range:0~23, default:t</li> </ul>	)					•



# 🖉 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.

мдіғ	WNC6600-	1000	-AC(V1) Wireless Con	troller			(!) →
MONITOR	Interface Config Static Route	>	Gateway	(No	o more then 8 d	efault gateway can be configed.separated by $^{\ast}_{r}^{\ast}_{r}$ eg:	
<u>ين</u>	DHCP DHCP Pool Config	Ň	Lease	1 • (0	unit:day. range: unit:hour. range	0~365. default:1) ::0~23. default:6)	
	Backup Config Relay Config			0 * (t	unit:minute. rar	1ge:0~59. default:0)	
DIAGNOSIS	Static IP List		DNS Auto Config				
Ľ	Client List		DHCP Pool Automatic				
DEVICE	WLAN	>	Option43			+ (Click to add one more.)	
	AAA Access Control	>	DNS Server			(Separate with "," if there is multiple items.)	
	RRM	>	WINS Server			(Separate with ", " if there is multiple items.)	
	Load Balance	,	Option60 :				
			Manufacturer			(type:hex,range:0~16byte;)	
			ок с	ancel			
						🖒 Refresh 📋 View	
			DHCP(Dyn so on.	amic Host Configuration Protocol) allo	ocates IP addre	sses from one address pool to requiring hosts, it also provi	e other information such as gateway IP, DNS address and

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.

## 3.4 Check Online Status of AP

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

мліғ	WNC660	0-1000-	AC(V1	) Wireless Cont	troller								(!)	$( \rightarrow )$
0	Summary		= ,	AP List										^
MONITOR	Statistics	>												
	AP List			Filter Condition	Online AP 🗸		Sort	Mode	P Ascending Order	~				
- tộj	STA List			C Export CSV File							Total : 2: Onlin	e : 2. Connectin	a: 0. Offline :	0.
CONFIG	Rogue List	>		La Export Cov The							10101 - 2, 01111	e . z, connectin	g. o, online .	0.
Ĥ	Rogue Rules	>		MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated ST	'As
DIAGNOSIS	RRM Report			CC:D8:1F:96:70:E4	10.11.12.217	10.11.12.217(41058)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	۵	
N				CC:D8:1F:96:74:6E	10.11.12.232	10.11.12.232(55584)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٥	
DEVICE														
$\wedge$												≤ ≤ 1	≥ ≥  20	~
LOG														

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.

млір	WNC6600-	-1000-A	C(V1) Wir	eless Controller							(!) ⊖
Q	Interface Config	>	Wireles	s Service							A
MONITOR	Static Route										
	DHCP	>	Filter (	Condition All	~						∀ Filter
<b>{</b> \city	WLAN	~	+ 0	eate 🖌 Edit 🔟 Del	ete (i) Enable (2) Disa	ble					
CONFIG	Wireless Service	]	T G	eate y cuit in Dei	ete S chable S bisa	Die					
( <del>+</del> )	AP Template			Wireless Service Name	Forwarding Mode	SSID	Auth Type	Encrypt Type	Status	Portal	Domain
DIAGNOSIS	AP Group			wlan1	Distributed forwarding	abc	WPA2-Personal	AES	Disable		
N	AP Config			Test	Distributed forwarding	Test	WPA2-Personal	AES	Enable		
DEVICE	AP Login Manager	ment									
^	AAA	>								<u>i</u> < <u>1</u>	≥ ≥  20 ∨
	Access Control	>									
100	RRM	>									
	BYOD	>									
	Load Balance										

мліғ	WNC6600-100	0-AC(V1	) Wireless Controller		(!) ⇒
$\bigcirc$	Interface Config >	=	Forwarding Mode		*
( ° ) MONITOR	Static Route		SSID	Default_SSID	
-0.	DHCP		Encoding Format	UTF8 V	
<b>5</b>	wlan ~				
CONFIG	Wireless Service		SSID Hidden	Disable 🗸	
Ð	AP Template		User VLAN	1	I
DIAGNOSIS	AP Group		Max User Per BSS	128	
Ľ	AP Config		User Isolation	Enable 🗸	
DEVICE	AP Login Management			Pirable.	
	AAA >		Load Balance	Disable V	
	Access Control >		Security		
	RRM >				
	BYOD		Auth Type	Open 🗸	
	Load Balance		Portal Auth	Disable ~	
			NAS Search	Enable 🗸	
			AC-IP		
			Signed Key		
			Submit Cancel	,	

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.

# 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.

$\bigcirc$	Interface Config	> =	AP Ten	nplate									
	Static Route												
	DHCP	>	Templ	ate Name									
 	WLAN	~	+ 0	cente d'Edit 🛱 Delete	C Apply C	Force to Apply							
ONFIG	Wireless Service		T U	reate 🗡 coit 🔟 Delete 🕑 Apply 🕑 Force to Apply									
ГШ	AP Template			AP Template Name		Radio					WLAN		
	AB Crown			in template frame	Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type	
5140515	AP Gloup				1	HT20	6						
$\tilde{z}$	AP Config			Default_FitAP_Profile	2	HT40	Auto						
EVICE	AP Login Manage	ement				11720					W042 Deeeeel	455	
^	AAA	>		profile1	1	HI20	Auto	1	abc	1	WPA2-Personal	AES	
<u>I</u>	Access Control	>			2	HT40	Auto	1	abc	1	WPA2-Personal	AES	
OG	RRM	>		Test	1	HT20	Auto						
	BYOD	>		rest	2	HT40	Auto	1	Test	120	WPA2-Personal	AES	

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.

мдіғ	WNC6600-10	000-AC(	V1) Wireless Controller		(!) ⇒
MONITOR	Interface Config Static Route	> =	Add AP Template		A
දරූ	WLAN	~	Basic Radio BSS	Bandwidth Advanced Config Time Zone Config	
(+)	Wireless Service		Name Max. Users	64 *	
DIAGNOSIS	AP Group		Device Type		
DEVICE	AP Login Managemer	nt	Is Default Type		
$\wedge$	AAA	>	Uplink Integrity Detection	Disable ~	
LOG	Access Control RRM	>	Time to Reboot	Disable v	
	BYOD	>	Band Navigation		
	Load Balance		5G Priority	Disable ~	
			Load Balance between RF	Disable v	
			🖉 Submit 💿 Cancel		

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

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.

млі	WNC6600-	1000-AC(	(V1) Wireless Controller		(!) ⇒
(d) MONITOR	Interface Config Static Route	> =	Add AP Template		ĺ
CONFIG	WLAN Wireless Service	~	Basic Radio BSS	Bandwidth Advanced Config Time Zone Config	
	AP Template AP Group		Available Status Radio Status	Enable v Enable v	
DEVICE	AP Config AP Login Managem	ent	Time Rule	-NONE- v	
LOG	AAA Access Control RRM	>	Wireless Mode	802.11bigh ~	
	BYOD Load Balance	>	Channel Bandwidth Channel	HT20 v	
			Power Boost Power	Disable v By dBm v auto v + dBm (3~27)	
			RSSI Threshold Radio 2 -	-95 *dBm(-95~-30) Uwak Signal Offline	

мліг	WNC6600-1	000-AC(	V1) Wireless Controller		(!) ⇒
MONITOR	Interface Config Static Route	> =	Radio 2 -	· · ·	
ŝ	DHCP	> ~	Available Status	Enable v	
	Wireless Service		Radio Status Time Rule	Enable v -NONE- v	
DIAGNOSIS	AP Group		Time to Reboot	Disable •	
DEVICE	AP Config AP Login Manageme	ent	Wireless Mode	802.11a/n v	
	AAA Access Control	>	Channel Bandwidth	HT40 v AUTO auto v Three-frequency device, which only supports 36-64 channel configuration	- 1
LOG	RRM BYOD	>	Power Boost	Disable ~	
	Load Balance		Power	By dBm v auto v + dBm (3~27)	- 1
			RSSI Threshold	-95 *dBm(-95*-30) UWeak Signal Offline	
			Radio 3 -	Disable v	
			Submit Cancel		ļ

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

мліғ	WNC6600	-1000-A	C(V1) Wireless Con	troller		Q	Sweet prompt:In the main prepared scenario,please	e config other device after	successing confi	g current devic	e. !	$( \rightarrow )$
$\bigcirc$	Interface Config	>	▼ Time Range List									<b>`</b>
MONITOR	Static Route											
	DHCP	>	+ Add 🔟 Dele	te								
<b>t</b> \$}	WLAN	>		Name	Туре	Sequence	Ru	les			Edit	
CONFIG	AAA	~					not found any data					-
( <del>+</del> )	NAS									45.4		-
DIAGNOSIS	Portal							<u>&gt;</u> [	<u>≤</u> 1 <u>≥</u>	<u>&gt;[</u> 15 p	er page 🗸	
NS:	Radius		<ul> <li>Time Point List</li> </ul>									
DEVICE	Domain											
^	Access Control	$\sim$	+ Add 🔟 Dele	ete								
	MAC Filter			N	ame		Rules				Edit	
100	WLAN ACL						not found any data					
	Time Rule							<	< 1 >	>  15 p	er page 🗸	
	RRM	>										
	BYOD	>										
	Load Balance											



# 🖉 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

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.

	Interface Config Static Route	>	Edit AP T	emplate							
~	DHCP	>	Basic	Radio	Band	width Adv	anced Config Time 2	one Config			
SNFIG	WLAN Wireless Service	~	No.	Wireless Service N	lame	Radio ID	User VLAN	SSID	Auth Type	Encrypt Type	
( <del>+</del> )	AP Template		1	wlan1	~	ALL ¥ 1		abc	WPA2-Personal	AES	Advance
GNOSIS	AP Group		2	Close	~	1 2					Advance
2	AP Config		3	Close	~	3 ALL					Advance
EVICE	AP Login Manageme	int	4	Close	~	1 🗸					Advance
$\wedge$	AAA	>	5	Close	~	1 🗸					Advance
.OG	RRM	>	6	Close	~	1 🗸					自 Advance
	BYOD	>	7	Close	~	1 ~					Advance
	Load Balance		8	Close	~	1 v					Advance
			9	Close	~	1 🗸					🖹 Advano
			10	Close	~	1 🗸					Advance
			11	Close	~	1 🗸					Advance 1
			12	Close	~	1 ×					自 Advano

Figure 3.16 BSS configuration

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.

$\bigcirc$	Interface Config	> ≡	Edit AP 1	emplate							
NITOR	Static Route		Luit Ar	emplace							
~~	DHCP	>	Basic	Radio BSS	Band	width A	dvanced Config Time Z	one Config			
<b>{</b> 0}	WLAN	~									
UNFIG	Wireless Service		No.	Wireless Service	Name	Radio ID	User VLAN	SSID	Auth Type	Encrypt Type	
$\oplus$	AP Template		1	wlan1	~	ALL 🗸	1	abc	WPA2-Personal	AES	Advance
AGNOSIS	AP Group		2	Close	~	1 v					Advance
2	AP Config		3	Close	~	1 ~					Advance
EVICE	AP Login Managem	nent	4	Close	~	1 ~					Advance
$\wedge$	AAA	>	5	Close	~	1 ~					Advance
	Access Control	>	5								E Advance
	RRM	>	6	Close	~	1 🗸					Advance
	BYOD	>	7	Close	~	1 🗸					Advance
	Load Balance		8	Close	~	1 v					Advance
			9	Close	~	1 🗸					🖻 Advance
			10	Close	~	1 🗸					Advance
			11	Close	~	1 🗸					自 Advanc
			12	Close	~	1 ~					自 Advanc
			13	Close	~	1 -					

Figure 3.17 Edit BSS

мліг	WNC6600	-1000	-AC(V1) Wireless	Controll	er					(!) ⇒
$\bigcirc$	Interface Config	>	Edit AP Te	mplate						
MONITOR	Static Route									
-0-	DHCP	>	Basic	Radio	RSS	Bandwidth	Advanced Config	Time Zone Config		
<u></u>	WLAN	~	busic	Tudio	0000	bundwiddi	Advanced coming	Time Lone comig		
CONFIG	Wireless Service		Edit BSS 1							
Ŧ	AP Template		Time Rule			NONE 🗸				
DIAGNOSIS	AP Group		WLAN ACL			NONE 🗸				
E.	AP Config		SAVI Enable			Disable 🗸				
DEVICE	AP Login Manage	ment	Submit	🕙 Can	cel					
$\wedge$	AAA	>								
105	Access Control	>								
	RRM	>								
	BYOD	>								
	Load Balance									
										v

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.

млір	WNC6600	-1000-	AC(V1) Wireless Controlle	r 🤅	Sweet prompt:In the main prepared scenario,please config othe	r device after successing config current device. $( ) \mathrel{\bigcirc}$
$\bigcirc$	Interface Config	>	WLAN ACL			
MONITOR	Static Route					
	DHCP	>	Rule Class Name	*	Rule Class Type Al	P V + Add
<b>5</b>	WLAN	>	No	Rule Class Name	Rule Class Type	Delete
CONFIG	AAA	>	10.	Rate Class Harrie	Rule Class Type	Denece
Ĥ	Access Control	~	1	Test	AP	ii Delete
DIAGNOSIS	MAC Filter					
s)	WLAN ACL					
DEVICE	Time Rule					
	RRM	>				
A	BYOD	>				
LOG	Load Balance					

Figure 3.19 Create AP ACL

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

млір	U WNC6600	)-1000-AC	(V1) Wireless Controller		
$\bigcirc$	Interface Config	> =	Rule Config		
MONITOR	Static Route				
	DHCP	>	Rule Index	1	
<u></u>	WLAN	>			
CONFIG	AAA	>	Action	Permit 🗸	
Ĥ	Access Control	$\sim$	Ethernet Type	IPv4 ✓	
DIAGNOSIS	MAC Filter		Source IP[/mask]		
2	WLAN ACL				
DEVICE	Time Rule		Destination IP[/mask]		
	RRM	>	IP Protocol	~	
$\overline{\mathbb{A}}$	BYOD	>	Cycle Date	Enable 🗆	
LOG	Load Balance				
			Submit Cancel		

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.

мліг	WNC6600	-1000-A	C(V1) Wireless Co	ontroller		(i) Sweet p	rompt:In the main prepa	ed scenario,please con	ig other device after	successing config current de	evice. 🚺	$(\rightarrow)$
MONITOR	Interface Config Static Route	>	Edit AP Temp	blate								_
CONFIG	DHCP WLAN Wireless Service	~	Basic F	tadio BSS	Bandwidth BSS Bandwidth	Advanced Config n Configuration	Time Zone Co	onfig				
Ŧ	AP Template		No.		Wireless Service Name		Flow Equalization	Uplink Bandy	vidth Limit	Downlink Bandwid	lth Limit	
DIAGNOSIS	AP Group		1		wlan1			0	Kbps	0	Kbps	
E	AP Config											
DEVICE	AP Login Manage	ment	1. Uplink Bandwid 2. Downlink Band	dth Limit: 0:Disable, Iwidth Limit: 0:Disable	Range 32~131072 e, Range 32~131072	072						
	AAA	>	3. Minimum Band	width Guarantee: 0:0	nsable, kange 32~131	072						
<u>_!\</u>	Access Control	>	🖉 Submit	Cancel								
200	RRM	>										
	BYOD	>										
	Load Balance											

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.



• 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.

мліғ	WNC6600	-1000-A	C(V1) Wireless Contro	oller			(!) ⇒
$( \mathbf{P} )$	Interface Config	> =	Edit AP Template	,			î
MONITOR	DHCP	>	Basic Radio	BSS Bandwidth	Advanced Config	Time Zone Config	
CONFIG	WLAN Wireless Service	Ý	ARP Snooping	Enable v			
Ð	AP Template		DHCP Snooping	Enable 🗸			
N	AP Group AP Config		Aging Time	600	*s(180-3600)		
DEVICE	AP Login Manage	ment	⊘ Submit 🔄 Ca	ancel			
	AAA Access Control	>					
106	RRM	>					
	Load Balance						

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.

мліг	WNC6600	-1000	AC(V1) Wireless Co	ntroller					(!) ⇒
$\bigcirc$	Interface Config	>	Edit AD Tomp	ate					1
MONITOR	Static Route		Eult AP Temp	ate					
	DHCP	>	Pasis D	ulia DCC	Danshuidth	Advansed Config	Time Zene Cenfig		
<u></u>	WLAN	$\sim$	Dasic Ra	IUIO DSS	Danuwidun	Advanced Conlig	Time zone conlig		
CONFIG	Wireless Service		Time Zone	Enable	~				
Ŧ	AP Template			8	~				
DIAGNOSIS	AP Group		-						
E.	AP Config		🕑 Submit	Cancel					
DEVICE	AP Login Manager	ment							
	ААА	>							
	Access Control	>							
100	RRM	>							
	BYOD	>							
	Load Balance								

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.

мліғ	WNC6600-	-1000-AC	(V1) Wi	reless Controller							(!) ⇒
$( \circ )$	Interface Config	> =	AP Cor	nfig							^
MONITOR	DHCP	>	AP Gro	up Group Type	Image Upgrade 🗸		-NONE- 🗸		87 JoinGr	oup 8≞ L	.eaveGroup
<b>{</b> \$}	WLAN	$\sim$	AP Ten	nplate list profile1	~						88 Apply
CONFIG	Wireless Service			-NONE-	Profile						
Ŧ	AP Template		Filter	Condition profile1							⊽ Filter
DIAGNOSIS	AP Group		1.0			d David					
N	AP Config		τu	eate / Edit III L	Velete V Reboot	C Reset					Rockup
DEVICE	AP Login Manager	ment		MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Status
	AAA	>		CC:D8:1F:96:70:E4	Customization	profile1 ~	WA2600-821-PE(V2)	NONE		Online	Master
	Access Control	>		CC:D8:1F:96:74:6E	Customization	NONE V	WA2600-821-PE(V2)	NONE		Online	Master
	RRM	>									
	BYOD	>							<	< 1 >	>  20 ¥
	Load Balance										



### 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.

	Interface Config > =	AP Cor	nfig							
ONITOR	Static Route									
	DHCP >	AP Gro	up Group Type	Image Upgrade 🗸		NONE 🗸		8º JoinGro	pup 🗄	LeaveGroup
ŝ	wlan ~	AP Ten	plate listNONE	~						88 Apply
NFIG	Wireless Service									
Ŧ	AP Template	Filter	Condition ALL	~						⊽ Filter
SNOSIS	AP Group									
2	AP Config	+ 0	eate Edit 🔟 D	elete 🕑 Reboot	C Reset					
		_	MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Backup
	AP Login Management	U								Status
ふ /ice	AP Login Management		CC:D8:1F:96:70:E4	Customization	Test 🗸	WA2600-821-PE(V2)	NONE		Online	Master
	AP Login Management AAA  Access Control		CC:D8:1F:96:70:E4 CC:D8:1F:96:74:6E	Customization Customization	Test	WA2600-821-PE(V2) WA2600-821-PE(V2)	NONE		Online	Master

Figure 3.25 Select AP

2	Interface Config	>	AD Confin Contoniantion						
ITOR	Static Route		AP Coming Customization						
	DHCP	>	Paric Dadio PSS	Pandwidth	Advanced Config	Time Zone Config			
25	WLAN	~	Dasic Radio D33	Danuwiutii	Advanced Conlig	Time Zone Coning			
IFIG	Wireless Service		AP MAC	CC:D8:1F:96:70:E4	Ļ				
F)	AP Template		AP Name	WA2600-821-PE(V2	2)				
NOSIS	AP Group				.)				
້	AP Config		AP Location						
∽ VICE	AP Login Manage	ment	Max. Users	64	*				
$\wedge$	AAA	>	Uplink Integrity Detection	Disable	~				
! <u>\</u> DG	Access Control	>	Time to Deboot	Disable					
	RRM	>	Time to Rebool	Disable +					
	BYOD	>	Band Navigation						
	Load Balance		5G Priority	Enable 🗸					
			Load Balance between RF	Disable 🗸					

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.

Basic Info			DTLS Encryption Configu	uration	
OR	Basic Config		CAPWAP DTLS		
	DTLS Config				
è	SNMP Config		Status	Enable DTLS Authentication	~
G	License				
3	AP Access Number		⊘ ок		
	Port Statistics		DTLS Mode		
	Port Manage			DOV/M 1	
5	User Manage		Status	PSK Mode	~
CE	AC Upgrade		Pre-shared Key		(length: 0-31)If not, it is the default.
	AP Upgrade	>			
2	AC Backup	>	⊘ ок		
	Login Authenticatio	n			
	Configuration	>			
	Factory Reset				
	Reboot				



MAIF	WNC6600	-1000-AC	C(V1) Wireless Controller			
$\bigcirc$	Basic Info	Ξ	Ø OK			
MONITOR	Basic Config		DTI S Mode			
	DTLS Config					
<b>5</b>	SNMP Config		Status	CERT Mode	~	
CONFIG	License					
Ĥ	AP Access Number		⊘ ок			
DIAGNOSIS	Port Statistics		Import Certificate			
	Port Manage				*	
63	User Manage		Certificate List			
DEVICE	AC Upgrade				*	
$\wedge$	AP Upgrade	>	Server IP Address		*	
LOG	AC Backup	>	Username		*	
	Login Authentication	n				
	Configuration	>	Password		*	
	Factory Reset		AC Certificate		*	
	Reboot					
			CA Certificate		*	
			KEY Certificate		*	
			KEY Certificate Password			
			⊘ OK			

Figure 3.28 DTLS certificate mode encryption settings

# **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.

мліғ	WNC6600	)-1000-A	C(V1) Wireless Controller	${ar 0}$ Sweet promptiln the main prepared scenario.please config other device after successing config current device. $({ar 1})$ $ ightarrow$
Q	Interface Config	>	NAS Config	
MONITOR	Static Route			
	DHCP	>	IP 10.11.12.61 v	+ Add
<u></u>	WLAN	>		
CONFIG	AAA	~	iii Delete	
( <del>†</del> )	NAS		0	Ib
DIAGNOSIS	Portal			
R	Radius			
DEVICE	Domain			
^	Access Control	>		
<u> </u>	RRM	>		
LOG	BYOD	>		
	Load Balance			

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

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

Organization	C Sarch condition							
- Headquarters	begiesend connection Device mase AC mase BAS IP Device type All  Begistration mode All AB BAC BAC BAC SSID Bearch							
	Device list							
	Download the template record/page 10							
	💆 Device name Has IP Device name Has IP Device name Has IP Device " Register" Authent" Organization 4C make Portal IP Portal port SSID 4F MAC 4F SN Start							
	IP address 10.11.14.200 AC mans 2079_collif(Nolls)2 Portal port 2000 Status Quellane Close							

Figure 4.3 Check AC status

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

Basic Configuration >	Device Hanagement	
@ Organization	Q Search condition	 
-Headquarters	bevice mase         AC mase         NAS IP         bevice type         AU         v         Reporteration mode         AU           AP NAC         AP SS         SSID         Search         Search         SSID         Search	×
	Device list	C
		vnload the template records/page 10 V
	Device " Device Boxe ligs IP Device " Review" Archaet Device Archaet Partal TP Partal part STD A     Device TP Review Revie	P MAC AP SN Start IP €
	Device type AC • Organization Headquarters •	
	Device name IGW_ccd81188d0a2 • NAS IP 10.11.14.250 •	
	Fre-share key . Confirm key	
	Comportal authenticat***	
	Authentication tree = 7.07 CH2	
	Description	
	8/64 characters, you can input 56 characters! OK Cancel	
		Ŧ
	K ( 1 ) M total 1 page Go to T page Go	
	Records 1	

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.

## 4.4 Add Authenticated Users on radius

🖳 User management 📃 User gr	p management		Basic Configuration > User and User Grou
Cremination	Sauch condition		
Perputation       Image: I	Account type     A	Res account mober      Res     Statur     Statur	x User group All   Center uners Reset duration record/page 30   Center Effective tr Relify pareved for first   Valid ferever
	K ( 1 )	M total 1 page Go to: 1 page GO	

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



• 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

мліг	WNC6600	)-1000-AC	(V1) Wireless Controller					(!) ⇒
$\bigcirc$	Interface Config	> =						•
( °) MONITOR	Static Route		Radius					
	DHCP	>	Authentication Server List	Accounting Server List				
<b>5</b>	WLAN	>	Autientication Server List	Accounting server List				
CONFIG	AAA	~	+ Create / Edit III De	lete				
( <del>+</del> )	NAS							
DIAGNOSIS	Portal		No.	Server Name	Server IP	Server Port	NAS IP	NAS Port
N	Radius							
DEVICE	Domain							
	Access Control	>						
$\triangle$	RRM	>						
LOG	BYOD	>						
	Load Balance							
мдір	WNC6600	)-1000-AC(	V1) Wireless Controller					() ⇒
( ( ه	Static Route							
MONITOR	DHCP	>	Server Index	1 v				
<b>{</b>	WLAN	>	Server Type	Authentication Server				
CONFIG	AAA	~			<b>—</b>			
Ĥ	NAS		Server IP					
DIAGNOSIS	Portal		Server Port	1812	*(1~65535)			
N	Radius		Request Retransmission Times	2	*(2~10)			
DEVICE	Domain		Request Retransmission Interval	5	*(5~300)			
	Access Control	>	Request Reconstruction interval	5	(3-300)			
	RRM	>						
LOG	BYOD	>	Config NAS Address					
	Load Balance		IP ¥	Pre-shared Key		+ Ac	ld	
			It	p	Pre-s	hared Key		

Figure 4.7 Authentication server configuration

### 2. Accounting server configuration

⊘ Submit ⊙ Cancel

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.

млія	WNC6600	)-1000-	AC(V1) Wireless Controlle	r				(!) ⇒				
$\bigcirc$	Interface Config	>	Badiue									
MONITOR	Static Route		Radius									
	DHCP	>	Authentication Conver	int Accounting Converting	1							
<u></u>	WLAN	>	Authentication Server	Accounting server Lis								
CONFIG	AAA	~										
Ĥ	NAS		+ Create / Edit	j Delete								
DIAGNOSIS	Portal		No.	Server Name	Server IP	Server Port	NAS IP	NAS Port				
e.	Radius											
DEVICE	Domain											
•	Access Control	>										
	RRM	>										
LOG	BYOD	>										
	Load Balance											



#### 3. Authentication domain configuration

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

Static Route   DHCP   DHCP   VILAN   CONFIG   AAA   NAS   Portal   Radius   Control   Access Control   RRM     RRM     Densin	$\bigcirc$	Interface Config	$\rightarrow$	Add Domain			
DHCP   WLAN   AAA   NAS   Portal   Radius   Accounting Status   Demain   Accounting Status   Detete   Accounting Status   Detete	MONITOR	Static Route					
WLAN     >       CONFIG     AAA       OCNFIG     AAA       MAS     Authentication Status       AAA     Authentication Status       ABA     Authentication Status       Portal     Authentication Status       Radius     Accounting Status       Denotein       Access Control     >       RRM     >		DHCP	>	Domain	Domain		
CONFIG     AAA     ~       NAS     Auth_n_10.11.12.74 ~     + Add       Auth_n_10.11.12.74 ~     Auth_n_10.11.12.74 ~       Radius     Accounting Status     Disable ~       CNUCE     Demain       Access Control ~     Accounting Sterver       RBM     Accounting Sterver	\$ \$	WLAN	>	Authentication Status	Enable 🗸		
NAS         Authentication Server         Auth_1_10.11.12.74 v         + Add           Acrossi         Portal         Auth_1_10.11.12.74 v         Delete           Radius         Accounting Status         Disable v         Counting Status         Counting Status           Accounting Server         Acct_1_10.11.2.74 v         + Add           Reside         Accounting Status         Disable v           Access Control         >         Acct_1_10.11.12.74 v         + Add           RRM         >         Access Control         >	CONFIG	AAA	~				
Accounting Status         Accounting Status         Accounting Status         Delete           CPUCE         Demain         Accounting Status         Disable v           Accounting Status         Accounting Status         Accounting Status         Accounting Status           Accounting Status         Accounting Status         Accounting Status         Accounting Status         Accounting Status           Accounting Status         Accounting Status         Accounting Status         Accounting Status         Accounting Status         Accounting Status           Accounting Status         Accounting Status         Accounting Status         Accounting Status         Accounting Status         Accounting Status	Ĥ	NAS		Authentication Server	Auth_1_10.11.12.74 🗸	+ Add	
Radius         Accounting Status         Disable v           Densin         Accounting Status         Accut 1_0 11.12.74 v         + Add           Access Control >         Accut 1_0 11.12.74 v         Delete		Portal			Auth_1_10.11.12.74	Delete	
Demain         Accounting Server         Acct_1_0.11.12.74 v         + Add           Access Control >         >         Acct_1_0.11.12.74 v         + Add	s)	Radius		Accounting Status	Disable 🗸		
Access Control > Acct_10.11.12.74 Delete	DEVICE	Domain		Accounting Server	Acct 1 10.11.12.74 ×	+ Add	
A RRM > Delete	•	Access Control	>		Act 1 10.11.12.74		
	<u>/!\</u>	RRM	>			Delete	
LOG BYOD > Accounting Update Period 30 s(0~360), 0: disable	LOG	BYOD	>	Accounting Update Period	30 s(0~360), 0: disable		
Load Balance		Load Balance					

Figure 4.9 Configure authentication domain

# 4.6 External Portal Authentication Configuration

### 4.6.1 Configure AC Device Name

мліғ	WNC6600-1	1000-AC(	V1) Wireless Controller		O Sweet prompt: In the main prepared scenario, please config oth	er device after successing config current device.	(!)	$( \rightarrow )$
(d) MONITOR	Basic Info Basic Config		Basic Config					^
ŝ	DTLS Config SNMP Config		Basic Config Time Z	one Config MGMT Int	erface Config			
CONFIG	License		AC Name	1111.0028.280.01				
÷	AP Access Number		AC Priority	4	(0~7)			
DIAGNOSIS	Port Manage		Host Name	AC1				
Ľ	User Manage		Country (Decise	CN				
DEVICE	AC Upgrade		Country/Region	CIN				
$\wedge$	AP Upgrade	>	Note: switching the country / reg	gion will affect the configuration	of the channel value. Please confirm and then switch!			
	AC Backup	>						
	Login Authentication		🕑 Submit					
	Configuration	>						
	Factory Reset							
	Reboot							

Figure 4.10 Configure AC name

### 4.6.2 Portal Redirection Group Configuration and Application

#### 1. Create a Portal redirection group

мліг	WNC6600	0-1000-	AC(V1) Wireless Controlle	er 🕕 Swe	et prompt:In the main prepared	scenario,please config other device after successing config current device.	(!)	$( \rightarrow )$
	Interface Config	$\rightarrow$	Bortal					^
MONITOR	Static Route		r or cur					
	DHCP	>	Pasis Config De	utal Dula Cat Authentication from				
<u></u>	WLAN	>	basic coning PC	Authentication-free				
CONFIG	AAA	$\sim$						
Â	NAS		+ Create	ii Delete				
DIAGNOSIS	Portal		□ No.	Portal Name	Portal Server Address	URL		
NS:	Radius			Portal	10.11.12.74	http://10.11.12.74:80/portal/Login.do		
DEVICE	Domain							
•	Access Control	>						
	RRM	>						
LÕG	BYOD	>						
	Load Balance							

млір	WNC6600	)-1000-,	AC(V1) Wireless Controller		① Sweet prompt:In the main prepared scenario,please of the second scenario.please of the seco	config other device after successing config current device. $(!)$ $( \Rightarrow$
$\bigcirc$	Interface Config	>	Add Portal			i i
MONITOR	Static Route					
	DHCP	>	Portal Name		*	
ऱ्र	WLAN	>	Portal IP		* IP or Host	
CONFIG	AAA	~				
( <del>+</del> )	NAS		URL	http://192.168.1.1:80/portal/	.ogin.do or https://192.168.1.1:443/portal/Login.do	
DIAGNOSIS	Portal		Pagistas Kaspalius	Disable v		
~	Radius		Register Reepairve			
DEVICE	Domain		Register Timeout	600	* (60~3600s)	
	Access Control	>	Keepalive Timeout	30	* (3~3600s)	
	RRM	>	Portal Server Escape	Disable 🗸		
LOG	BYOD	>				
	Load Balance		Server Recovery Offline STA	Disable 🗸		
			Redirect Pre-shared Key			
			Config NAS Address			
			IP 10.11.12.61 V		+	- Add
					Ib	
			•			· · · · · · · · · · · · · · · · · · ·

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

2	Interface Config	>	Add Portal						
NITOR	Static Route	>	Portal Name			URL-Param co	onfiguratio	n	×
ô}	WLAN	>	Portal ID		5 ID or Hort		-		
NFIG	AAA	~	Portal IP		TP of Host	Name	Select	Rename	Format
FI	NAS		URL	http://192.168.1.1:80/porta	al/Login.do or https://192	wlanacname	2		
NOSIS	Portal		Pegister Keepaliye	Disable v			-		
2	Radius		negista neepoire			wianuserip			
EVICE	Domain		Register Timeout	600	* (60~3600s)	nasid			
^	Access Control	>	Keepalive Timeout	30	* (3~3600s)	wlanusermac			00-01-02-03-04-05 🗸
<u>!\</u>	RRM	>	Portal Server Escape	Disable 🗸		wlanapmac			00-01-02-03-04-05 🗸
0.0	BYOD	>	Conver Deseuser Office CTA	Disable					
	Load Balance		Server Recovery Offline STA	Disable V		vlan			
			Redirect Pre-shared Key			wlanacip			

Figure 4.13 Custom configuration of URL parameters

Introduction to some functions:

- A. **"URL"**: Portal redirection URL. The format is: <u>http://xxxx:80/portal/Login.do</u> or <u>https://xxxx:443/portal/Login.do</u> (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

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:

- 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.

# **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			

	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

- 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

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

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.


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.

wick Guide MONITOR N				THICK SO A	occool onit				
AICK GUIDE MONITOR N	Your current position : Quick Guide >:	> Basic Config							
ick Guide									
Basic Config									
			2					-6	
		Mode Settings Interfa	Co Settings	Access VI AN	Authentication	Discovery	lode	Finich	
		mode Settings Interna	ce settings	Access VLAIV	Configuration	Discovery W	ioue	1 111311	
					conigatori				
				Discove	ery Mode				
		C 20 11							
		Discovery Mode	Static 🗸						
		Authentication Method	No Authentication	1					
		Tunnel Keepalive	Enable 🛩						
		IP Protocol Support	IPv4 V						
		AC IPv4 Address	192.168.10.1	•					
		AC Control Port	5246						
		AC Data Port	5247	•					
		Secondary AC IPv4 Address							
		Secondary AC Control Port	5246						
		Secondary AC Data Port	5247						
					li ve	op Config Guido	Provident	Einich	
					Jur	ip coming Guide	rievious	F1111311	

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.....

#### 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 <u>http://192.168.10.1</u> 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

	USER LOGIN
	A   Account
ΜΔΙΡυ	Password
	Password
	Login
Copyright © 2015 Maipu Commun Recommend the use of browser over IE8.0,Opti	iication, All Rights Reserved imum screen resolution:1024768 pixels.

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

	Summary		AP List									
OR	Statistics	>	Filter Condition	Dnline AP 🗸 🗸		Sort	Mode	IP Ascending Order	v			⊽ Filter
G	STA List Rome List	>	C Export CSV File							Total : 2; Onlin	e : 2, Connectin	ig:0, Offline
6	Rogue Rules	>	MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated S
515	RRM Report		CC:D8:1F:96:74:6E	10.11.12.213	10.11.12.213(57795)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٩
Е			CC:D8:1F:96:70:E4	10.11.12.223	10.11.12.223(46867)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	۵

#### 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.

мліғ	WNC6600	-1000-/	AC(V1) Wireless	Controller (!) $ ightarrow $
$\bigcirc$	Interface Config	>	NAS Config	· · · · · · · · · · · · · · · · · · ·
MONITOR	Static Route			
	DHCP	>	IP	100.0.52.10 v + Add
<u></u>	WLAN	>		
CONFIG	AAA	~	🗎 Delete	
( <del>+</del> )	NAS			IP
DIAGNOSIS	Portal			10.11.12.61
N	Radius			100.0.52.10
DEVICE	Domain			
•	Access Control	>		
	RRM	>		
LÓG	BYOD	>		
	Load Balance			

#### 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.

млі	U WNC6600	0-1000	AC(V1) Wireless	Controller					(!) ⇒
	Interface Config	>	Add Auth Ser	rver					î
MONITOR	Static Route DHCP	>	Server Index		2 🗸				
ξ <sup>Ω</sup>	WLAN	>	Server Type		Authentication Server				
	NAS	Ť	Server IP		192.168.1.253	•			
DIAGNOSIS	Portal		Server Port		1812	*(1~65535)			
Ľ	Radius		Request Retra	nsmission Times	2	*(2~10)			
DEVICE	Domain		Request Retra	nsmission Interval	5	*(5~300)			
À	Access Control RRM	>							
LOG	BYOD	>	Config NAS Add	dress					
	Load Balance		IP	10.11.12.61 🗸	Pre-shared Key			+ Add	
				IP		Pre-	-shared Key		
			⊘ Submit	<ul> <li>Cancel</li> </ul>					

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.

2	Interface Config	>	Add Domain	
TOR	Static Route			
ION	DHCP	>	Domain	yu *
	WLAN	>	Authentication Status	Enable 🗸
NFIG	AAA	~	<b></b>	
Ŧ	NAS		Authentication Server	Auth_2_192.168.10.253 v + Add
SNOSIS	Portal		Accounting Status	Disable 🗸
S	Radius			
	Domain		Accounting Server	Acct_1_10.11.12.74 ~ + Add
^	Access Control	>	Accounting Update Period	30 s(0~360), 0: disable
$\mathbb{N}$	RRM	>		
G	BYOD	>	😔 Submit 🕞 Cancel	
	Load Balance			

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.

1) Wireless Controller	(!) ⇒
Wireless Service         Blacklist & Whitelist           Basic Set         Basic Set	
Wireless Service Name wlan1	
Service Status     Enable v       Forwarding Mode     Centralized forwarding v	
SSID abc *	
SSID Hidden Disable ~	
User VLAN 100 * Max User Per BSS 128	_
User Isolation Enable ~ Load Balance Disable ~	
SSID     abc       Encoding Format     UTF8 ~       SSID Hidden     Disable ~       User VLAN     100 ~       Max User Per BSS     128 ~       User Isolation     Enable ~       Load Balance     Disable ~	

Figure 5.9 Wireless service configuration

млір	WNC6600-1	000-AC(V1	) Wireless Controller		(!)
$\bigcirc$	Interface Config	> =	SSID	apc	
	Static Route		Encoding Format	UTF8 🗸	
	DHCP	>	SSID Hidden	Disable v	
<b>ç</b> ş	WLAN	~	5515 110001		
ONFIG	Wireless Service		User VLAN	100 *	
Ŧ	AP Template		Max User Per BSS	128	
AGNOSIS	AP Group		User Isolation	Enable 🗸	
ES -	AP Config		Load Balance	Disable 🗸	
DEVICE	AP Login Manageme	ent			
$\wedge$	AAA	>	Security		
	Access Control	>	Auth Type	WPA3-Enterprise 🗸	
	RRM	>			
	BYOD	>	Radius Auth Domain	yu 🗸	
	Load Balance		NAS Search	Disable ~	
			Encrypt Type	AES V	
			GTK Auto Refresh	Disable 🗸	
			GTK Refresh Period	24 *(1-10000)H	
			Submit Cancel		

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.

мліғ	WNC6600	-1000	-AC(V	'1) W	vireless Controller		(i) Sweet	prompt:In the m	ain prep	ared scena	rio,please config othe	er device after successing config c	urrent device. 🚺 🧧
Q	Interface Config	>		AP T	emplate								
MONITOR	Static Route												
	DHCP	>		Tem	nplate Name								
<u></u>	WLAN	$\sim$		+	Create 🖌 Edit 🗊 Delete 🤇	Apply 6	Ence to Apply						
CONFIG	Wireless Service			-		s rubbelt	, roree correpty						
Ĥ	AP Template		AP Template Name		Radio								
DIAGNOSIS	AP Group					Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type
-	10.0-5-			_		1	HT20	6					
2	AP Config			0	Default_FitAP_Profile	2	HT40	Auto					
DEVICE	AP Login Manage	ement				1	HT20	Auto	1	abc	1	WPA3-Enterprise	AES
	AAA	>			profile1	2	11740						150
<u>_!</u>	Access Control	>				2	H140	Auto	1	abc	1	WPA3-Enterprise	AES
200	RRM	>			Test	1	HT20	Auto					
	BYOD	>				2	HT40	Auto	1	Test	120	WPA2-Personal	AES
	Load Balance											<u> ≤</u> ≤	1 ≥ ≥  20 ∨

#### 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.

2	Interface Config	> =	Edit AD	Tomplata									
NITOR	Static Route												
	DHCP	>	Bacic	Padio RSC Bar	dwidth	Advanced Config Time	Zone Config						
<u></u>	WLAN	~	Dasic		luwidur	Advanced coning Time :	Zone comig						
ONFIG	Wireless Service		No.	Wireless Service Name	Radio ID	User VLAN	SSID	Auth Type	Encrypt Type				
Ð	AP Template		1	wlan1 ~	ALL 🗸	100	abc	WPA3-Enterprise	AES	自 Advance			
NOSIS	AP Group		2	Close ~	1 🗸					Advano			
2	AP Config		3	Close ~	1 ~					■ Advance			
VICE	AP Login Managem	ent	4	Close 🗸	1 v					■ Advance			
~	AAA	>		01									
<u>!\</u>	Access Control	>	5	Close V	1 ¥					Advance			
	RRM	>	6	Close 🗸	1 🗸					Advano			
	BYOD	>	-	Close	1					in advance			

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.

мліғ	WNC6600-1000	0-AC(V	1) Wireles	s Controller							(!) ⇒		
$\bigcirc$	Interface Config >		AP Config								•		
MONITOR	Static Route												
	DHCP		AP Group	Group Type	Image Upgrade 🗸		NONE V		87 JoinGr	oup 🗄 l	eaveGroup		
<u></u>	wlan ~		AP Template	listNONE	~						88 Apply		
CONFIG	Wireless Service												
Ð	AP Template		Filter Condit	tion ALL	~						⊽ Filter		
DIAGNOSIS	AP Group		+ Create	+ Greate 🖌 Edit 📋 Delete 💿 Reboot 🗘 Reset									
2	AP Config												
DEVICE	AP Login Management		0	MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Status		
~	ааа >		CC:1	D8:1F:96:70:E4	Customization	Test	✓ WA2600-821-PE(V2)	NONE		Online	Master		
	Access Control		CC:1	D8:1F:96:74:6E	Customization	profile1	WA2600-821-PE(V2)	NONE		Online	Master		
	RRM >												
	BYOD												
	Load Balance								<	< 1 >	>  20 v		

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.

мліғ	WNC660	0-1000-AC(V	1) Wireles	s Controller									(!) ⊝
	Summary	=	STA List	t									
MONITOR	Statistics	>											
	AP List		Filter O	ALL	~								∀ Filter
<b>ş</b>	STA List		C. Pol	irash	fline C Export	CSV Eile						Total : 1 Onl	ine:1.0ffline:0
CONFIG	Rogue List	>	C Rei		Le cxpor	Cov The						10411 - 1 011	ne.r onne . o
Ĥ	Rogue Rules	>		MAC	IP	Status	AP Name	AP Location	SSID	Frequency Band	OS	Online Time	Tx/Rx Rate
DIAGNOSIS	RRM Report			6A:EE:64:08:18:52	10.11.12.233	Authorized	WA2600-821-PE(V2)		abc	5G	Unknown	2023-01-17 22:04:58	0 bps/0 bps
CS DEVICE												. ≤ ≤ 1 ≥	≥! 20 ∨

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:

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 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

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

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.





#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.

Ocack Guide         MONTOR         NETWORK         SERVICE         DEVICE           Auide         Vor current position:         Cack Guide >> Basic Config 1	Wireless Access Point	
Ver current position : Ouck Guide >> Basic Config		
Basic Config Mode Settings Interface Settings Access VLAN Authentication Configuration Discovery Mode Discovery Mode Disco		
1       2       3       4       5       6         Mode Settings       Interface Settings       Access VLAN       Authentication       Discovery Mode       Finish         Discovery Mode         Discovery Mode         Varianciation       V       V       V         Varianciation       No Authentication       V       V         Varianciation       V       V       V       V         Varianciation       V       V       V       V         Varianciation       Varianciation       V       V       V         Varianciation       Varianciation       V       V       V         Varianciation       Varianciation       V       V       V       V         Varianciation       Varianciation       Varianciation       V       V       V         Varianciation       <		
Discovery Mode     Static     Output       Authentication     Discovery Mode     Finish		
Mode Settings Interface Settings Access VLAN Authentication Discovery Mode Finish Configuration Discovery Mode Static V Authentication Method No Authentication V Tunnel Keepalive Enable V IP Protocol Support IP4 V AC Data Port 5246 * AC Data Port 5247 *		
Configuration         Discovery Mode         Discovery Mode         Discovery Mode       Static       Image: Configuration         Authentication Method       No Authentication       Image: Configuration         Tunnel Kespalive       Enable       Image: Configuration         Act Data Port       5247       *	iettings Interface Settings Access VLAN Authentication Discovery Mode Finish	
Discovery Mode Discovery Mode Static v Authentication Method No Authentication v In Protocol Support Protocol Support AC Ervk Address 192.168.10.1 * AC Control Port 5246 * AC Data Port 5247 *	Configuration	
Discovery Mode Discovery Mode Static  C Authentication Method No Authentication Tunnel Keepalive Endel  C IP Protocol Support D 20168.10.1 C AC Diva Address D22.168.10.1 C AC Diva Address D22.168.10.1 C C C C C C C C C C C C C C C C C C C		
Discovery Mode Static  Authentication Method No Authentication  Tunnal Keepalive Enable  IP Protocol Support IP-4  AC 10v4 Address 102.168.10.1  AC Control Port 5246  AC Data Port 5247  *	Discovery Mode	
Discovery Mode       Static         Authentication Method       No Authentication         Tunnal Keepalive       Enable         IP Protocol Support       IP44         AC 10rV4 Address       192.168.10.1         AC Control Port       5246         AC Data Port       5247		
Authentication Method       No Authentication         Tunnal Kespalive       Enable         IP Protocol Support       IPM         AC 19V4 Address       192.168.10.1         AC Control Port       5246         AC Data Port       5247	Discovery Mode Static V	
Tunnel Keepalive     Enable        IP Protocol Support     IP-4       AC IPV4 Address     192,168,10,1       AC Control Port     5246       AC Data Port     5247	rthentication Method No Authentication	
IP Protocol Support IP-4 v AC IP-4 Address 192.168.10.1 * AC Control Port 5246 * AC Data Port 5247 *	Tunnel Keepalive Enable 🗸	
AC IPv4 Address 192.168.10.1 * AC Control Port 5246 * AC Data Port 5247 *	IP Protocol Support	
AC Control Port 5246 * AC Data Port 5247 *	AC IPv4 Address 192.168.10.1	
AC Data Port 5247 *	AC Control Port 5246	
	AC Data Port 5247	
Secondary AC IPv4 Address	dary AC IPv4 Address	
Secondary AC Control Port 5246	dary AC Control Port 5246	
Secondary AC Data Port 5247	condary AC Data Port 5247	
lumo Config Guide Brouleur Einich		

Figure 5.17 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 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.

	USER LOGIN
	Account
ΜΔΙΡΟ	Password
	Password
	Login
Copyright © 2015 Maipu Com Recommend the use of browser over IE8.0,	munication, All Rights Reserved Optimum screen resolution:1024768 pixels.

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.

2	Summary		AP List									
TTOR	Statistics AP List	>	Filter Condition	Online AP 🗸 🗸		Sort	Mode	IP Ascending Order	~			⊽ Filter
} 1G	STA List		C Export CSV File							Total : 2; Online	e : 2, Connectin	ig:0,Offline:
	Rogue Rules	>	MAC	IP	Outside Gobal Address	AP Name	Status	AP Location	Software Version	Device Model	Backup Status	Associated ST
OSIS	RRM Report		CC:D8:1F:96:74:6E	10.11.12.213	10.11.12.213(57795)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	٩
5			CC:D8:1F:96:70:E4	10.11.12.223	10.11.12.223(46867)	WA2600-821-PE(V2)	Online		200.20.2.6(R)	WA2600-821-PE(V2)	Master	۵
-∕> VICE												

#### 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.

мліғ	WNC6600-	-1000	-AC(V1) Wireless Contro	roller (	] ∋
(	Interface Config	>	Wireless Service	e Blacklist & Whitelist	1
MONITOR	DHCP	>	Basic Set		
<b>CONFIG</b>	WLAN	Ň	Wireless Service Nan	ame wlan1	- 1
( <del>+</del> )	AP Template	J	Service Status	Enable	- 1
DIAGNOSIS	AP Group		Forwarding Mode	Distributed forwarding	- 1
es.	AP Config		SSID	abc	- 1
DEVICE	AP Login Manager	ment	Encoding Format	UTF8 🗸	
A	AAA Access Control	>	SSID Hidden	Disable v	- 1
LOG	RRM	>	User VLAN	100	- 1
	BYOD Load Balance	>	Max User Per BSS	128	- 1
			User Isolation	Enable V	
			Load Balance	Disable v	
			Security		
			Auth Type	WPA3-Personal 🗸	
			NAS Search	Disable 🗸	

$\bigcirc$	Interface Config	> 📃	Encoding rormat	0110 •	
	Static Route		SSID Hidden	Disable v	
-0	DHCP	>	User VLAN	100 *	
{Q}	WLAN	~			
ONFIG	Wireless Service		Max User Per BSS	128	
Ð	AP Template		User Isolation	Enable 🗸	
GNOSIS	AP Group		Load Balance	Disable ~	
S	AP Config				
	AP Login Manag	ement	Security		
~	AAA	>	Auth Type	WPA3-Personal	
	Access Control	>	NAS Search	Disable v	
100	RRM	>			
	BYOD	>	Encrypt Type	AES 🗸	
	Load Balance		Mode	Transition 🗸	
			GTK Auto Refresh	Disable 🗸	
			GTK Refresh Period	24 *(1-10000)H	
			6		

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.

мліғ	WNC6600	)-1000-AC	C(V1) V	Wireless Controller		( Sweet	prompt:In the m	ain prep	ared scena	rio,please config othe	r device after successing config	current device. 🚺 🔿	
$\bigcirc$	Interface Config	> =	AP 1	Template									
MONITOR	Static Route												
	DHCP	>	Ter	mplate Name		∀ Se							
ŝ	WLAN	~	+	Create di Edit III Delete (	annly (	Force to Apply							
CONFIG	Wireless Service		-			o roice to apply							
Ĥ	AP Template		0	AP Template Name		Radio					WLAN		
	AP Group				Radio ID	Channel Bandwidth	Channel	No.	SSID	User VLAN	Auth Type	Encrypt Type	
-	10 5.00p				1	HT20	6						
25	AP Config		U	Default_FitAP_Profile	2	HT40	Auto						
DEVICE	AP Login Manage	ement			1	HT20	Auto	1	abc	1	WPA3-Enterprise	AES	
Δ	AAA	>		profile1	2	1/740	A				WDA2 Februaries	450	
<u>_!</u> _	Access Control	>			2	H140	Auto	1	abc	1	WPA3-Enterprise	AES	
200	RRM	>	0	Test	1	HT20	Auto						
	BYOD	>			2	HT40	Auto	1	Test	120	WPA2-Personal	AES	
	Load Balance										<u>l&lt;</u> <	1 ≥ ≥l 20 ∨	



#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.

3	Interface Config	>	Edit AP T	emplate								
NITOR	Static Route			empiace								
A	DHCP	>	Basic	Radio	BSS Bandy	width		Advanced Config Time	e Zone Config			
25	WLAN	~						, ,	3			
NFIG	Wireless Service		No.	Wirele	ss Service Name	Rad	dio ID	User VLAN	SSID	Auth Type	Encrypt Type	
Ð	AP Template		1	wlan1	~	A	LL V	100	abc	WPA3-Enterprise	AES	自 Advance
iosis	AP Group		2	Close	~	1	~					Advance
3	AP Config		3	Close	~	1	~					Advance
CE	AP Login Managem	ent	4	Close	~	1	~					Advance
2	AAA	>	5	Close	¥	1	~					Advance
5	RRM	>	6	Close	~	1	~					自 Advance
	BYOD	>	7	Close	~	1	~					Advance
	Load Balance		8	Close	~	1	~					Advance
			9	Close	~	1	~					Advance
			10	Close	~	1	~					Advance
			11	Close	~	1	~					Advance
			15	Close								-

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.

мліғ	WNC6600-	1000-A	C(V1) W	/ireless Controller		¢	Sweet p	prompt:In the main prepared so	enario,please config other d	levice after successing co	nfig current dev	ice. $(!) \rightarrow$
$( \circ )$	Interface Config	>	AP Co	onfig								<u>^</u>
MONITOR	DHCP	>	AP G	roup Group Type	Image Upgrade 🗸	•		-NONE- V		₿₽ JoinGr	pup 8º l	eaveGroup
<u></u>	WLAN	$\sim$	AP Te	emplate listNONE	~							88 Apply
CONFIG	Wireless Service											
Ŧ	AP Template		Filte	r Condition ALL	~							⊽ Filter
DIAGNOSIS	AP Group			Course of Edite (17) ID		đ. Dt						
N	AP Config		Ŧ	Create FEat II L	elete 🕑 Rebool	C Reset						Bashus
DEVICE	AP Login Managem	nent		MAC	Config Status	AP Template		AP Name	AP Group	AP Location	Status	Status
~	ААА	>		CC:D8:1F:96:70:E4	Customization	Test	~	WA2600-821-PE(V2)	NONE		Online	Master
<u>_!\</u>	Access Control	>		CC:D8:1F:96:74:6E	Customization	profile1	~	WA2600-821-PE(V2)	NONE		Online	Master
	RRM	>										
	BYOD	>										21 20
	Load Balance									<	× <b>1</b> >	20 ~

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.

$\bigcirc$	Summary		STA Lis	:									
( ) MONITOR	Statistics	>	Filter (	ation ALL									77. 010
~	AP List		Filter C	Plion ALL	~								V Filter
र्\$	STA List		C Re	resh 🔟 Force to Off	line 🔂 Export	t CSV File						Total : 1 On	line:1 Offline : 0
CONFIG	Rogue List	>											
Ŧ	Rogue Rules	>		MAC	IP	Status	AP Name	AP Location	SSID	Frequency Band	OS	Online Time	Tx/Rx Rate
IAGNOSIS	RRM Report			6A:EE:64:08:18:52	10.11.12.233	Authorized	WA2600-821-PE(V2)		abc	5G	Unknown	2023-01-17 22:04:58	0 bps/0 bps
S Device												. ≤ ≤ <u>1</u> ≥	≥! 20 ∨

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 wpa2personal authentication access, and mandatory mode means that only the terminal that supports wpa3-personal authentication can be connected.

## **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.

мліғ	WNC6600	-1000-AC(	V1) Wireless Controller			(!) ⇒
$\bigcirc$	Interface Config	>	Edit Portal			Â
MONITOR	Static Route					
	DHCP	>	Portal Name	Portal		
<b>{</b> Q}	WLAN	>	Portal IP	10.11.12.74	* IP or Host	
CONFIG	AAA	$\sim$		http://doi.ul.10.74.00/cm		
ŵ	NAS		URL	http://10.11.12.74:80/poi http://192.168.1.1:80/portal/	rtal/Login.do Login.do or https://192.168.1.1:443/portal/Login.do	
	Portal			URL-Param configuration		
DIAGNOSIS			Register Keepalive	Enable 🗸		
3	Radius		De sister Times et	600	* (20. 2000.)	
DEVICE	Domain		Register Timeout	600	* (60~3600s)	
•	Access Control	>	Keepalive Timeout	30	* (3~3600s)	
<u> </u>	RRM	>	Portal Server Escape	Enable V		
LOG	BYOD	>	ronon ourren abeupe			
	Load Balance		Server Recovery Offline STA	Enable 🗸		
			Redirect Pre-shared Key			

Figure 5.1 portal server registration and keepalive

## **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.

млір	WNC6600	-1000-AC	(V1) Wireless Con	troller	() Sweet prompt:In the main prepared scenario,please co	nfig other device after successing config current device. $( )  imes )$
$\bigcirc$	Interface Config	> =	Portal			1
MONITOR	Static Route		- or car			
	DHCP	>	Basic Config	Portal Rule Set Authentication	n-free	
<b>{</b> \city	WLAN	>	basic comig	Portal Nule Set	in nee	
CONFIG	AAA	~	Set Name			+ Croata
Ĥ	NAS		Set Hame			T Cleate
DIAGNOSIS	Portal		No.	Set Name	Num. of Rules	Delete
e.	Radius		1	test	0	i Delete
DEVICE	Domain					
^	Access Control	>				
	RRM	>				
LOG	BYOD	>				
	Load Balance					

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.

$\bigcirc$	Interface Config	>	E	dit Rule Set:test				
MONITOR	Static Route							
	DHCP	>	l	+ Create	Edit 🔟 Delete			
<b>{</b> \city	WLAN	>			Create Rule	X	Rule Value	
CONFIG	AAA	~			Cleate Rule		Ic c 1 >	>1 20 -
Ĥ	NAS				Rule Action PERMIT V		in in the second se	
DIAGNOSIS	Portal			Return	Rule Type HOST 🗸			
3	Radius				HOST Http://			
DEVICE	Domain							
^	Access Control	>			Ok Cancel			
<u> </u>	RRM	>				_		
LOG	BYOD	>						
	Load Balance		- 11					



## 7.3 Configure redirect Rule Group

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

млі	WNC6600	-1000-AC	(V1) Wireless Controlle	r	(!) ⊖
MONITOR	Interface Config Static Route	> =	Edit Rule Set:test	Create Rule	
CONFIG	DHCP WLAN AAA	> > ~	- Create / Edit	Rule Action REDIRECT V	Rule Value
	NAS Portal		© Return	Rule Type IP V	
DEVICE	Radius Domain			Ok Cancel	
	Access Control	>			
LOG	BYOD Load Balance	>			

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.

мліғ	WNC6600	-1000-	-AC(V1) Wireless Contr	ller	(!) →
6	Interface Config	>	Edit Rule Set:test		
MONITOR	Static Route			Create Rule	
	DHCP	>	+ Create / Ed		
<b>{</b>	WLAN	>		Rule Action CNA 🗸	Rule Value
CONFIG	AAA	~		Rule Type URL V	
( <del>+</del> )	NAS			PORT	
DIAGNOSIS	Portal		💿 Return	(Format:11,22)	
N	Radius			Ok Cancel	
DEVICE	Domain				
^	Access Control	>			
	RRM	>			
LOG	BYOD	>			
	Load Balance				

Figure 6.4 Configure CAN rule group

Currently configure CNA rules, and add the following addresses:

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

## 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.

млір	WNC6600-	-1000-AC	(V1) Wireless Controller		Sweet prompt: In the main pre	pared scenario,please config other device after s	uccessing config current device.	(!) ⇒
0	Interface Config	>	AP Group					^
MONITOR	Static Route		Filter Condition					
	DHCP	>	All 🗸				V	Filter
<b>5</b>	WLAN	~	All					
CONFIG	Wireless Service		- Image Upgrade dit II	Delete				
Ŧ	AP Template		HAP Scan AP	Group Name	Group Type	AP Group Member(s)	Detail Info	
DIAGNOSIS	AP Group							
e.	AP Config						l≤ ≤ 1 ≥ ≥l	20 🗸
DEVICE	AP Login Manager	ment						
	AAA	>						
	Access Control	>						
	RRM	>						
	BYOD	>						
	Load Balance							



мліғ	WNC6600-	1000-AC(	V1) Wireless Controller		(!) ⇒
$\bigcirc$	Interface Config	> 🔳	Add AP Group		Î
MONITOR	Static Route	>	Group Name	•	
<u>ين</u>	WLAN	~	Group Type	Scan 🗸	
CONFIG	Wireless Service		Default Group	No v	
$\oplus$	AP Template				
DIAGNOSIS	AP Group		802.11a Scan Config		
E.	AP Config		Operate Mode	Work Mode 🗸	
DEVICE	AP Login Managem	ent	Scan Mode	Passive Modt -	
$\wedge$	AAA	>	Country 1	Dirable	
	Access Control	>	Counter	Disable	
	RRM	>	Rogue Report	Enable v 60 *Second(15-3600)	
	BYOD	>	DDM Deport	Enable + 180 * Second/15.65535)	
	Load Balance		кки керот	rumo A YAA Second YAASSA	
			Scan Times	Permanent Scan	
			Regular Scan	Disable v	
			Working Channel Service Time	4000 *ms(200-10000)	
			Working Channel Scan Time	45 *ms(30-1000)	
			Non Working Channel Scan Time	40 *ms(30-1000)	

Figure 7.2 Configure AP scanning group

Introduction to some functions:

- 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;

- 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.

мліг	WNC6600-1	000-A0	C(V1) Wire	eless Controller							(!) ⇒
0	Interface Config	> 😑	AP Cont	fig							^ ·
MONITOR	Static Route										
	DHCP	>	AP Grou	Group Type	Scan 🗸		Scan 🗸		89 34	binGroup	f≘ LeaveGroup
<b>5</b>	WLAN	~	AP Tem	plate listNONE	~						88 Apply
CONFIG	Wireless Service										
ŧ	AP Template		Filter C	ondition ALL ~							⊽ Filter
DIAGNOSIS	AP Group		+ cm	nto 🖌 Edit 🗐 Doloto	(i) Robert d <sup>a</sup> Br	unat					
N.	AP Config		+ cre	sate y cont	C Rebool	iser.					
DEVICE	AP Login Managemen	nt	0	MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Backup Status
~	AAA	>		CC:D8:1F:96:70:E4	Customization	NONE v	WA2600-821-PE(V2)	Scan:Scan		Online	Master
	Access Control	>		CC:D8:1F:96:74:6E	Template	Test 🗸	WA2600-821-PE(V2)	Scan:Scan		Online	Master
	RRM	>									
	BYOD	>									1 00
	Load Balance									< < 1	> >1 20 •

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.

2	Interface Config	> =	TPC			
NITOR	Static Route					
	DHCP	>	802.11a			
ર્ટ્	WLAN	>	Assignment Period	0	*min(0-1440) 💿 Invoke Now	
NFIG	AAA	>	Maximum Power	27	*dBm(3-27)	
5	Access Control	>				
	RRM	~	Minimum Power	3	*dBm(3-27)	
	ТРС		Power Threshold	-65	*dBm(-95-0)	
ડે	DCA		Neisbhas Threeheld	2	*(4.5)	
/ICE	BYOD	>	Neighbor Threshold	3	(1-0)	
$\mathbf{N}$	Load Balance		802.11b			
G			Assignment Period	0	*min(0-1440) ③ Invoke Now	
			Maximum Power	27	*dBm(3-27)	
			Minimum Power	3	*dBm(3-27)	
			Power Threshold	-65	*dBm(-95-0)	
			Neighbor Threshold	3	*(1-6)	

Figure 7.4 Configuring automatic power adjustment

## 8.4 Auto Channel Adjustment

мліғ	WNC6600	-1000-A0	(V1) Wireless Controller		() ⊖
0	Interface Config	> =	DCA		•
MONITOR	Static Route		802.11a		_
	DHCP	>	Assignment Period 0	*min(0-1440) ① Invoke Now	
<u>{</u>	WLAN	>			
CONFIG	AAA	>	Load Threshold 10	•(5-10)	
( <del>+</del> )	Access Control	>	Interference Threshold 60		
DIAGNOSIS	RRM	~	There is a second se		
~	TPC		iorerance nines 3	(64)	
<u>es</u>	DCA		DCA Channels	<b>b</b> , 157, 168, 36, 64	
DEVICE	BYOD	>	<b>F</b> 140		
$\wedge$	Load Balance		153		
LOG			157		
			- IAI -	· ·	
			802.11b		
			Assignment Period 0	*min(0-1440) ③ Invoke Now	
			Load Threshold 10	•(5-10)	
			Interference Threshold 60	***/0.100)	
				al (a-root)	
			Tolerance Times 3	*(1-8)	
			DCA Channels	6. 11	
			O Cubait		
			(		

Channel auto adjustment configuration is shown in Figure 7.5.





• 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

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.

# 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.

мліг	WNC6600-	1000-AC	(V1) Wireless Controller		(!) →
MONITOR	Summary Statistics	>	Friendly Rule		
CONFIG	AP List STA List Rogue List	>	Friendly BSSID Friendly OUI And SSID Friendly STA		+ Add
	Rogue Rules Friendly Rule	~			
DEVICE	Counter Rule RRM Report		□ No.	BSSID	
			Figure 8.1 Cont	figure friendly rules	



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

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.

млір	WNC6600	0-1000-	AC(V1) Wireless C	ontroller				(!) ⇒
0	Summary		Counter Bul					1
MONITOR	Statistics	>	Counter Rul	e				
-0-	AP List		Counter Stra	teau Static Counter List	Sensitive SSID	RSSI Threshold		
- <u>{õ</u> }	STA List			State counter est	Sensitive SSID	NOST THE SHOLE		
CONFIG	Rogue List	>					Unclassified Device	
Ĥ	Rogue Rules	~					Phishing Device	
DIAGNOSIS	Friendly Rule		0				Europeted Bhishing Device	
~	Counter Rule		0				Suspected Phisning Device	
63	RRM Report						Static Counter Device	
DEVICE							Interference Device	
$\wedge$								
LOG			⊘ Submit	ⓒ Cancel				



#### 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.

мліғ	WNC6600-1000-	AC(V1) Wireless Controller	(!) →
$\bigcirc$	Summary	Counter Rule	
MONITOR .	Statistics >		
-0-	AP List	Counter Strategy Static Counter List Sensitive SSID RSSI Threshold	
<u>{ô</u> }	STA List		
CONFIG	Rogue List >		+ Add
Ĥ	Rogue Rules 🛛 👻		
DIAGNOSIS	Friendly Rule	Delete	
N	Counter Rule	O No. BSSID	
DEVICE	RRM Report		

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.

ΔİΡ	U WNC6600	-1000-A	(V1) Wireless Controller	(!) (-
2	Summary		Counter Bula	
	Statistics	>		
	AP List		Country Charles Country Line Country Line Country Color	
25	STA List		Counter strategy static Counter List Sensitive SSID RSSI Threshold	
IFIG	Rogue List	>	Sensitive SSID	+ Add
a –	Rogue Rules	$\sim$		
, DSIS	Friendly Rule		Delete	
	Counter Rule		No. SSID	
e l	RRM Report			

Figure 8.4 Configure sensitive SSID list

мліг	WNC6600-1000	-AC(V1) Wireless	Controller			Sweet promption the main prepared scenario please config other device after successing config current device. $$				
0	Summary	Counter AP Lis	st							<b>^</b>
MONITOR	Statistics >									
	AP List	Current State	Current Scan 🗸	Device Type	All 🗸	Rogue Type	All 🗸	SSIC		
433	STA List									
CONFIG	Rogue List 🗸 🗸	💍 Refresh								Total Num: 0
( <del>†</del> )	Device Scan List	BSSID	Device Type	Rogue Type	Channel	SSID	Check Time	Location	Check Point Number	
DIAGNOSIS	Counter List									
2	Terminal Scan List								< 1 ک کا	≥l 20 ¥
DEVICE	Rogue Rules >									
	RRM Report									
$\triangle$										
LOG										

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.

мліғ	WNC6600	0-1000-AC	(V1) Wireless Controller	$\oplus$ Sweet promptin the main prepared scenario.please config other device after successing config current device. (D) $ ightarrow$
$\bigcirc$	Summary	=	Counter Rule	
MONITOR -	Statistics	>		
	AP List		Counter Strategy Static Counter List Considius SSID	bold
- <b>Ç</b> Ş	STA List		Counter strategy static counter list sensitive ssib	
CONFIG	Rogue List	>	RSSI Threshold 0 dBm (-95~0)	
Ĥ	Rogue Rules	~		
DIAGNOSIS	Friendly Rule		⊘ Submit	
~	Counter Rule			
DEVICE	RRM Report			
<u>^</u>				
200				



#### 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.

	Summary	=	Device Scan List							
DR	Statistics	>								
	AP List		Current State C	urrent 🗸	Device Type All	*	Rogue Type	All	SSID	∀ Filter
	STA List							All Unclassified Device		
s	Rogue List	$\sim$	🖒 Refresh					Phishing Device Suspected-Phishing Device		Total Num: 0
	Device Scan List	]	BSSID	Device Type	Rogue Type	Channel	SSID	Friendly Device Counter Device	Scan Location	Check Point Number
as	Counter List							Interference Device		
	Terminal Scan List									
	Rogue Rules	>								
	RRM Report									

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.

2	Summary		Counter AP List								
ITOR	Statistics	>									
	AP List		Current State	Current Scan 🗸	Device Type	All V	Rogue Type	All	SSID		∀ Filter
}	STA List							All Unclassified Device			
FIG	Rogue List	~	🖒 Refresh					Phishing Device Suspected-Phishing Device			Total Num:
9	Device Scan List		BSSID	Device Type	Rogue Type	Channel	SSID	Counter Device Interference Device	Location	Check Point Number	
OSIS	Counter List										
ş	Terminal Scan List									Is s 1 2	21 20
S ICE	Rogue Rules	>									
	RRM Report										

#### 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.

мліғ	WNC6600-1000	0-AC(\	(1) Wireless Contro	oller			() Sweet prompt:In	the main prepared scenario,ple	ase config other device	after successing config current device.	. Э
0	Summary	=	Terminal Scan List								^
MONITOR	Statistics >					41					-
	AP List		Current State	ent 🗸	Rogue Type	All Y				Ŷ	Filter
5	STA List		C. Rofrash							Tota	Num: 0
CONFIG	Rogue List 🗸 🗸		C Kertean							1018	Hum. U
Ĥ	Device Scan List		STA MAG	-	Rogue Type	BSSID	Channel	Check Time	Location	Check Point Number	
DIAGNOSIS	Counter List										
N	Terminal Scan List									اح ح 1 ک کا	20 🛩
DEVICE	Rogue Rules >										
	RRM Report										
$\wedge$											
LOG											



### 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.

2	Summary	=	RRM Report										
VITOR	Statistics	>											
	AP List		Filter Condition	ALL	~								
22	STA List		MAC Address	Radio	Working Channel	BSS Count	Interference	Noise	Channel Grade	All Neighbor Count	TPC Executed Count	DCA Executed Count	Detail
FIG	Rogue List	>											
5	Rogue Rules	>											
iosis	RRM Report											د 1 ء عا	≥l 20 v
ડે			i 1. The curr 2. Channel	ent channe 0 indicates	I scan report is displaye s the Current Channel is	d on this site. configured to auti	omatically.						

Figure 8.10 RRM reporting

## **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.

мдір	U WNC6600	-1000-	AC(V1) Wireless Control	ller	() Sweet promptin the main prepared scenario,please	config other device after successing config current device.	)
$\bigcirc$	Interface Config	>	WLAN ACL				^
MONITOR	Static Route		Rule Class Name	-	Rule Class Type A	+ Add	
~	DHCP	'				1.112	
<u>{</u> \$}	WLAN	>	No	Bule Class Name	Bula Class Tuna	Delate	
CONFIG	AAA	>	NO.	Rule class hame	Role Class Type	Derece	
Ĥ	Access Control	~	1	Tast	AP	1 Delete	
DIAGNOSIS	MAC Filter						
-	WLAN ACL						
DEVICE	Time Rule						
	RRM	>					
$\wedge$	BYOD	>					
LOG	Load Balance						



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.

млія	WNC6600	-1000	)-AC(\	V1) Wireless	Controller	${ar O}$ Sweet promptin the main prepared scenario.please config other device after successing config current device.	(!) ⇒
0	Interface Config	>	=	Rule Class Na	ame:Test		^
MONITOR	Static Route						
	DHCP	>		Default Rule	Deny 🗸	୍ର ହ	ubmit
<b>4</b> 03-	WLAN	>			Permit Deny		
CONFIG	AAA	>		+ Create	Edit 88	Insert 📋 Delete	
Ĥ	Access Control	×			No.	Rule Info	
DIAGNOSIS	MAC Filter			0	1	permit -proto IPv4 -src-ip 10.10.10.0/24 -dst-ip 10.10.11.0/24 -ip-protocol ALL	
~	WLAN ACL					اد د <mark>1</mark> ه ما	20 -
DEVICE	Time Rule						
	RRM	>		Cancel			
$\wedge$	BYOD	>					
LOG	Load Balance						



	Interface Config	> =	Rule Config	
DR	Static Route			
	DHCP	>	Rule Index	1
	WLAN	>		
IG	AAA	>	Action	Permit 🗸
	Access Control	~	Ethernet Type	IPv4 🗸
SIS	MAC Filter		Source IP[/mask]	10 10 10 0/24
	WLAN ACL		Source II (Finalsky	10.10.10.0/24
	Time Rule		Destination IP[/mask]	10.10.11.0/24
	RRM	>	IP Protocol	ALL 🗸
	RVOD	>		

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.

мліғ	WNC6600	0-1000-/	AC(V1) Wirele	ss Controlle	er			i Sweet p
	Interface Config	>	Edit AD	Template				
MONITOR	Static Route		Eult Ar	remplate				
	DHCP	>	Basic	Radio	BSS	Bandwidth	Advanced Config	Time Zone Config
<u>{</u>	WLAN	~	Dusie	Rudio	555	bundwiddi	Advanced comig	Time Zone comig
CONFIG	Wireless Service		Edit BSS :					
Ŧ	AP Template		Time Rule			NONE V	•	
DIAGNOSIS	AP Group		WLAN ACI	-		Test	,	
E.	AP Config		SAVI Enal	ole		Disable 🗸		
DEVICE	AP Login Manag	ement	⊘ Submi	t 🕞 Cano	el			
$\wedge$	AAA	>						
	Access Control	>						
200	RRM	>						
	BYOD	>						
	Load Balance							

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

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.

млір	WNC6600	-1000	-AC(\	(1) Wireless Con	ntroller	0 Sweet prompt: In the main prepared scenario, please	config other device after successing config current device. $( I ) ~~ \bigcirc$
$\bigcirc$	Interface Config	>	=	WLAN ACL			1
MONITOR	Static Route			Build Bloom Manage		Bulk along Burg	
-0-	DHCP	>		Rule Class Name		Rule class type	+ A00
<u>{</u> 0}	WLAN	>		No	Bule Class Name	Bula Class Time	Delate
CONFIG	AAA	>		NO.	Rule Class Name	Kule class type	Delete
Ĥ	Access Control	~		1	byod	BYOD	1) Delete
DIAGNOSIS	MAC Filter			2	ap	AP	间 Delete
Ľ	WLAN ACL Time Rule						
DEVICE	RRM	>					
$\wedge$	BYOD	>					
LOG	Load Balance						



The policy configuration is shown in Figure 9.6.

мліғ	WNC6600	0-1000-	AC(V1) Wireless Controller		(!) ↔
$( \mathbf{r} )$	Interface Config	>	Rule Config		
MONITOR	Static Route				
	DHCP	>	Rule Index	1	
<b>5</b>	WLAN	>			
CONFIG	лла	>	Action	Permit 🗸	
Ĥ	Access Control	~	Source IP[/mask]	10.10.10.0/24	
DIAGNOSIS	MAC Filter		Destination ID[/mask]	10 10 11 0/24	
~	WI AN ACI		Destination (P[/mask]	10.10.11.0/24	
DEVICE	Time Rule		IP Protocol	ALL ~	
	RRM	>	Cycle Date	Enable 🗆	
$\triangle$	BYOD	>			
LOG	Load Balance		Submit Cancel		

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.

$\bigcirc$	Interface Config	>								
	Static Route			BYOD ACL						
- Allow	DHCP	>								
ŝ	WLAN	>		US MAC						
DNFIG	AAA	>		on Windows 8 a	diag hand as			+ Add		
Ĥ	Access Control	>		CS MILLONS CV	Vendora 0 v					
SNOSIS	RRM	>		05	Rule Class		Delete			
~	BYOD	~		Windows 8	byod		Delete			
-3	Device Identity C	Onfig			0,00					
VICE	NAC									
$\wedge$	BYOD ACL									
OG	BYOD Client									
	Load Balance									

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.

млія	WNC6600-10	00-AC(	(V1) Wireless Controller			(!) →
	Interface Config 3		BYOD ACL			
錼	DHCP 2		OS MAC			
	AAA A		Rule Class	byod 🗸		8º Bind
	RRM 2		Current Rule Class:			8º Unbind
DEVICE	Device Identity Config		MAC			+ Add
	NAC BYOD ACL BYOD Client		Delete		мас	
	Load Balance					اح ح 1 ک کا 20 س

Figure 9.8 Apply policy set based on MAC address

# 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 Figure 10.1.

мліғ	WNC6600	-1000-	AC(V1) Wireless Controller			(!) ⋺			
0	Interface Config >		Add AP Group			1			
MONITOR	Static Route								
	DHCP	>	Group Name	hap	•				
 	WLAN	~	Group Type	HAP 🗸					
CONFIG	Wireless Service			Ale .					
Ĥ	AP Template		Default Group	NO					
DIAGNOSIS	AP Group		Auth Server Config	ith Server Config					
es.	AP Config		Auth Server Enable	Enable 🗸					
DEVICE	AP Login Manager	ment	IP Address		•				
~	AAA	>							
<u>_!</u> _	Access Control	>	Pre-shared Key		•				
200	RRM	>	Port Number	1812	•				
	BYOD	>							
	Load Balance		Submit Cancel						

Figure10.1 Create a HAP group

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

## **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.

мліг	WNC6600	-1000	AC(V1) Wireless Con	troller					(!) ⊙
MONITOR	Interface Config Static Route DHCP	>	▼ Time Range List + Add ① Del-	ete					Î
र्द्र	WLAN	>		Name	Туре	Sequence	Rules		Edit
CONFIG	AAA	>					not found any data		
Ĥ	Access Control	~						_	
DIAGNOSIS	MAC Filter							<u>لد د 1 ک کا</u>	15 per page ✓
N)	WLAN ACL		Time Point List						
DEVICE	Time Rule								
	RRM	>	+ Add 🗊 Del	ete					
$\triangle$	BYOD	>	0	N	ame		Rules		Edit
LOG	Load Balance						not found any data		
							not round any data		
								ند د ۱ ک کا	15 per page ∨

Figure11.1 Create time point table

мліғ	WNC6600-	1000-	AC(V1) Wireless Contro	ller							(!) ⊝
0	Interface Config	>	▼ Time Range List								•
MONITOR	Static Route										
	DHCP	>	+ Add 🗉 Delete								
۲ <u>۵</u>	WLAN	>		Name	Туре	Sequence			Rules		Edit
CONFIG	AAA	>					not	found any data			
( <del>+</del> )	Access Control	×									46
DIAGNOSIS	MAC Filter									<u> &lt; &lt; 1</u> >	≥[ 15 per page ♥
DEVICE	WLAN ACL		Time Doint List								
	Time Rule		- Third Point List								
	RRM	>	+ Add 🔟 Delete								
$\triangle$	BYOD	>		N	ame				Rules		Edit
LOG	Load Balance										
	not found any data										
										<u>د ۱</u> ک	≥l 15 per page ∨
			Time Point Configure								
			Time Point Name	Reload	•						
			Туре	Absolute Time	Pv						
			Absolute Time:	Year: 2023	✓ Month: Febr	uary v Day: 10	✓ Time: 21:57	(hh:mm) •			
			OK Cancel								



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.

мліг	WNC6600-1000-	AC(V1) Wireless Controller	${ar O}$ Sweet promptin the main prepared scenario.please config other device after successing config current device. $(ar )$	$( \Rightarrow $
(a) MONITOR	Interface Config >	Edit AP Template		
63	DHCP >	Basic Radio BSS	Bandwidth Advanced Config Time Zone Config	
CONFIG	Wireless Service	Name	profile1	
Ð	AP Template	Max. Users	64 -	
DIAGNOSIS	AP Group AP Config	Device Type		
DEVICE	AP Login Management	Is Default Type	No v	
$\wedge$	AAA >	Uplink Integrity Detection	Disable	
LOG	RRM >	Time to Reboot	Enable v	
	BYOD >	Time Point Name	Reload	
	Load Balance	Band Navigation		
		5G Priority	Disable ~	
		Load Balance between RF	Disable v	
		⊘ Submit 🔄 Cancel		the

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 Figure 11.4.

млі₽	WNC6600-	1000-AC	(V1) Wireless Controller		(!) 🤄	)
() MONITOR	Interface Config Static Route	> 🔳	Edit AP Template			Î
CONFIG	WLAN	~	Basic Radio BSS E	landwidth Advanced Config Time Zone Config		l
ŧ	AP Template		Radio 1 -	Enable v		l
DIAGNOSIS	AP Group AP Config		Radio Status	Enable v		l
DEVICE	AP Login Managen	>	Time Rule	-NONE-v		l
rog	Access Control RRM	>	Time Point Name	Reload		l
	BYOD Load Balance	>	Wireless Mode Channel Bandwidth	802.11ax v HT20 v		l.
			Channel	auto v		
			Power Boost	Disable v Burdhim v auto v adlan (3x22)		
			RSSI Threshold	-80 *48m(-45~-20) ☑ Weak Signal Offine		
			Radio 2 -			
			Available Status	Enable v		÷

Figure11.4 RF timing restart
# 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 Figure 11.5 and 11.6.

мліг	WNC6600	-1000	-AC(V1	) Wireless Cont	roller					(!) ⇒		
$\bigcirc$	Interface Config Static Route	>	<b>C</b>	<ul> <li>Time Range List</li> </ul>	]					^		
MONITOR	DHCP	>		+ Add 📋 Delet	te							
<b>{</b> \$}	WLAN	>			Name	Туре	Sequence	Rules		Edit		
CONFIG	AAA	>			TimeRange	active	10	Periodic:Daily 00:00 to 23:59 Delete				
( <del>+</del> )	Access Control	~							_			
DIAGNOSIS	MAC Filter							<u> </u> <u>&gt;</u>	i 1 ≥ ≥l	15 per page ↓		
~	WLAN ACL			Time Point List								
CS.	Time Rule			<ul> <li>Time Point List</li> </ul>								
DEVICE	RRM	>		+ Add 📋 Delete								
$\land$	BYOD	>			N	ame		Rules		Edit		
LOG	Load Balance				Pr	hoad	Abcolute:2022	Month 10 Time: 21-57-00 Delete				
				U		sives	A0301010-2020	Contract Time: 21.37.00 Dente				
								ء ءا	اح ح 1 ء	15 per page ↓		



мліг	WNC6600-1	1000-AC	C(V1) Wireless Contro	oller						(!) ⇒
MONITOR	Interface Config Static Route	> 🔳	<ul> <li>Time Range List</li> <li>+ Add Delete</li> </ul>							ĺ
ŝ	WLAN	>		Name	Туре	Sequence		Rules		Edit
CONFIG	AAA	>	2	TimeRange	active	10	Periodic:Daily 00:00 to 23:59 Delete			2
	Access Control MAC Filter	~							اح ح 1 ک کا	15 per page ↓
N)	WLAN ACL		Time Range Configure	2		7				
DEVICE	Time Rule		Name:	TimeRange	•					
	RRM	>	Type:	Periodic	~					
LOG	Load Balance		Periodic Time:	Daily Monday Tuesday Wednesday Thursday Friday Saturday	-i					
			OK Cancel     ✓ Time Point List     · + Add      Delete	Sunday	• Start:	(h	kmm) v Ind:	(hh:mm) Rules		Edit

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 Figure 11.7.

мліг	WNC6600-	1000-AC	V1) Wireless Controller		(!) ⊖
MONITOR	Interface Config Static Route	>	Edit AP Template		
CONFIG	WLAN Wireless Service	~	Basic Radio BSS Ba	ndwidth Advanced Config Time Zone Config	-1
	AP Template		Available Status	Enable v	
S.	AP Config	nent	Radio Status Time Rule	Enable v Enable v	- 1
	AAA Access Control	>	Time Range Name	TimeRange v	- 1
LOG	RRM BYOD	>	Time to Reboot	Deable v 802.11ex v	
	Load Balance		Channel Bandwidth	HT20 v	- 1
			Channel Power Boost	anto v Disable v	
			Power RSSI Threshold	By dBm         v         auto         v         ed8m (3-27)           s0         *d8m(-4530)         2 Weak Slond Office	
			Radio 2 -		
			Available Status	Enable •	

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 Figure 11.8.

мліг	WNC6600	-1000-A	C(V1) Wireless Controller		(!) ⊖
$\bigcirc$	Interface Config	>	Edit AP Template		1
MONITOR	Static Route				
	DHCP	>	Real Reals Rec. Re	- dubble Advantation for	The Test Carls
<b>{</b>	WLAN	~	Basic Radio BSS Ba	ndwidth Advanced Config	Time Zone Conng
CONFIG	Wireless Service		Edit BSS 1		
( <del>+</del> )	AP Template		Time Rule	Enable 👻	
DIAGNOSIS	AP Group		Time Range Name	TimeRange	
e.	AP Config		WLAN ACL	NONE ¥	
DEVICE	AP Login Manage	ment	SAVI Enable	Disable ~	
Λ	AAA	>	Submit 🕞 Cancel		
2:3	Access Control	>			
1003	RRM	>			
	BYOD	>			
	Load Balance				

Figure11.8 Used in BSS time period

# **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 Figure 12.1.

$\bigcirc$	Basic Info	Add Backup Link
MONITOR	Basic Config	
. 0.	DTLS Config	No. 2 V
ŝ	SNMP Config	Local IP *
CONFIG	License	
Ĥ	AP Access Number	Peer IP *
	Port Statistics	
	Port Manage	Submit Cancel
E.	User Manage	
DEVICE	AC Upgrade	
	AP Upgrade	
	AC Backup	
200	Backup Link	
	Login Authentication	
	Configuration >	
	Factory Reset	
	Reboot	
		Figure12.1 Create a standby link

 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 Figure 12.2.

млір	U WNC6600	-1000-	AC(V1) Wireless Controller					(!) →						
$\bigcirc$	Interface Config	>	Add AP Group					1						
MONITOR	Static Route													
-	DHCP	>	Group Name	Backup	-									
<u>{</u> \$}	WLAN	~	Group Type	Backup										
CONFIG	Wireless Service		Default Group	No	_									
Ŧ	AP Template													
DIAGNOSIS	AP Group		Fallback Master AC	Enable 🗸										
e.	AP Config		Backup Group											
DEVICE	AP Login Manage	ment	+ Create											
	ААА	>												
LOG	Access Control	>	Local AC IP		Peer AC IP	Backup Channel	Bac	.up Channel Status						
	RRM	>												
	BYOD	>												
	Load Balance		AC Priority Config											
			AC Name		Priority 0 v			+ Create						
				AC N	lame	Pi	iority	Delete						
			Submit Cancel	Submit Cancel										

Figure12.2 Configure the AP standby group

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



 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 Figure 12.3.

мліг	WNC6600-1	1000-AC(	1) Wireless Controller			(!) ⇒
6	Interface Config	> 🔳	DHCP Failover Config			1
MONITOR	Static Route					
	DHCP	~	+ Add 📋 Delete			
ŝ	DHCP Pool Config		DHCP Pool Name Channel ID Backup Link ID	Local ID	Status	Edit
CONFIG	Backup Config		not four	id any data		
Ð	Relay Config					>1 15 per page v
DIAGNOSIS	Static IP List		DHCD Evileurs Confin			
Ľ	Client List					
DEVICE	WLAN	>	DHCP Pool Name			
Λ	ААА	>	Backup Link Index			
106	Access Control	>				
	RRM	>	(1~63335)			
	BYOD	>	OK Cancel			
	Load Balance					



### **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 dualmachine hot standby environment. Otherwise, it may affect the normal operation of dual-machine.

# **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.



Figure 13.1 RF detection duration configuration

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

млія	WNC6600-1000-AC(	V1) Wireless Controller				(!) ()
MONITOR	Ping&Traceroute	Scan Detection				
CONFIG	control controls	Scanning Time (: Attention:Turn on scanning Detectio	0-3600)s Scan All Channel	<ul> <li>Start Scanning</li> <li>start Scanning as defaution</li> </ul>	00:00:00	
		After turn on All channel scan       Open 'radioProtect' will be the       C Refresh     C Open Auto	ning,AP will scanning all channels,it a e maximum power AP. Refresh Refresh Time 3	ffects all the accessed STA ,please be	serious!	
DEVICE		MAC Address	Radio ID	Channel ID	Interferers	

Figure 13.2 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.

Ping&Traceroute	Empty Capture							
Radio Frequency Detection	Service Config							
	Service Type FTP	~ -	Address	• (Format: 192.1)	68.1.1)			
	User		Password	-			Empre	iss Uploa
NOSIS	+ Add Capture Task 📋 Clear H	istory Record 💍 Refresh	💍 Open Auto Refresh					
2	MAC Address	Capture Interface	Capture Params	Capture Time	Status	Operation	Result	Erro
VICE								

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.



# 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.

млі	WNC6600	)-1000-AC	(V1) Wireless Cont	troller				(!)	$( \rightarrow )$
0	Interface Config	> =	Device Identify Cor	nfiguration					^
MONITOR	Static Route								
	DHCP	>	Identify Status	Enable					
<u></u>	WLAN	>	os		Description				
CONFIG	AAA	>							
Ĥ	Access Control	>	Option55	•	Option60			+ Add	
	RRM	>							
	BYOD	~	OS	Description		Option55	Option60	Delete	
Ľ	Device Identity	Config							
DEVICE	NAC								
$\wedge$	BYOD ACL								
LOG	BYOD Client								
	Load Balance								

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.

$\bigcirc$	Interface Config	>	NAC Boliev					
	Static Route		NAC FOICY					
	DHCP	>	MD Rinding	Access De	P0.4			
< <u>ç</u>	WLAN	>	VID binding	Access De	ny			
CONFIG	AAA	>	os	Windows 8 🗸	VID	*(2~4094)		+ Add
Ĥ	Access Control	>						
	RRM	>		OS		VID	Delete	
	BYOD	$\sim$						
25	Device Identity G	onfig						
DEVICE	NAC							
A	BYOD ACL							
LOG	BYOD Client							
	Load Balance							

Figure14.2 VID Binding

### 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.

мліг	WNC6600	-1000-AC(	(V1) Wireless Controller	$\oplus$ Sweet promptin the main prepared scenario,please config other device after successing config current device. 🕕 (	Ð
	Interface Config	> 🔳	NAC Policy		^
MONITOR	Static Route		had rolley		
	DHCP	>	VID Binding Access Domy		
<b>{</b>	WLAN	>	VID bilding Access Delly		
CONFIG	AAA	>	QS Windows 8 v		
Ĥ	Access Control	>		+ Add	
DIAGNOSIS	RRM	>	OS	Delete	
	BYOD	~			
2	Device Identity Co	onfig			
DEVICE	NAC				
$\wedge$	BYOD ACL				
LOG	BYOD Client				
	Load Balance				

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.

мліа	WNC6600	)-1000-AC(	V1) Wireless Controller					(!) ⇒
	Interface Config	> 🔳	BYOD Client					^ ^
MONITOR	Static Route							
	DHCP	>	Filter Type ALL V					⊽ Filter
<u></u>	WLAN	>	MAC	OUI	OS	Description		Status
CONFIG	AAA	>						
Ē	Access Control	>						
	RRM	>					1< <	1 ≥ ≥! 20 ∨
	BYOD	~						
Ľ	Device Identity Co	onfig						
DEVICE	NAC							
$\wedge$	BYOD ACL							
LOG	BYOD Client							
	Load Balance							

Figure14.4 BYOD client

# **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.

мліг	WNC6600	-1000-AC	(V1) Wireless Controller			(!) ⇒
Q	Interface Config	> =	Load Balance			<u>^</u>
MONITOR	Static Route					
	DHCP	>	User Quantity Enabling Threshold	8	*(1~40)	
<b>\$</b>	WLAN	>	User Quantity Difference Threshold	4	*(0~8)	
CONFIG	AAA	>				
Ĥ	Access Control	>	Traffic Enabling Threshold	30	*Mbps(1~70)	
	RRM	>	Traffic Difference Threshold	20	*Mbps(1~40)	
	BYOD	>				
25	Load Balance		Max. Traffic of AP	80	*Mbps(0~300)	
DEVICE			RSSI Threshold	-80	*dBm(-95~0)	
$\wedge$			Aging Time	60	*s(60~3600)	
LOG			Max. STA Association Rejection Times	5	*(1~32)	
			⊘ Submit			

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.

мліғ	WNC6600	-1000-AC(	(V1) Wireless Controller		(!) ⊖
$\bigcirc$	Interface Config	> =	5510	abc	•
MONITOR	Static Route		Encoding Format	UIF8 V	
~~	DHCP	>	SSID Hidden	Disable 🗸	
<u>{</u> \$}}	WLAN	Ň			
CONFIG	Wireless Service		User VLAN	100 *	
Ð	AP Template		Max User Per BSS	128	
DIAGNOSIS	AP Group		User Isolation	Enable 🗸	
ES .	AP Config		Load Balance	Enable V	
DEVICE	AP Login Manager	ment			
	ААА	>	Load Balance Mode	User Count	
<u></u>	Access Control	>	Security	Traffic	
200	RRM	>			
	BYOD	>	Auth Type	WPA3-Enterprise V	
	Load Balance		Radius Auth Domain	Domain 🗸	

Figure 15.2 Create a wireless service set with load balancing enabled

# **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.

мліг	WNC6600-1000-	AC(V1) Wireless Controller	(!) ⇒
$\bigcirc$	Basic Info	Configed AC List	÷
MONITOR	Basic Config		
~	DTLS Config	+ Add AC Channel / Modify AC Channel Delete AC Channel Sync AC Config	
₹ <u>ŏ</u> }	SNMP Config	Link ID Local IP Peer IP	
CONFIG	License		
Ĥ	AP Access Number	AC Channel Add/Modify	
DIAGNOSIS	Port Statistics		
	Port Manage	Link ID 1 V	
Ľ	User Manage	Local IP *	
DEVICE	AC Upgrade		
	AP Upgrade	Peer IP *	
	AC Backup		
	Login Authentication	UK Cancel	
	Configuration 🗸		
	Configuration		
	AC Config Sync		
	Factory Reset		
	Reboot		

#### 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.

Basic Info	Confige	d AC List			
Basic Config					
DTLS Config	+ Add	d AC Channel 📝 M	odify AC Channel 🗊 Delete AC	Channel 📋 Sync AC Config	
SNMP Config		Link ID		Local IP	Peer TP
License					
AP Access Number		1	1	10.10.10.1	10.10.10.2
Port Statistics		AC Config Sync		×	
Port Manage					
User Manage		Peer IP	10.10.10.2		
AC Upgrade		Replace Config			
AP Upgrade >		Save Config			
AC Backup 🗸					
Backup Link		View Config Inform	nation Start to Config Sync	Cancel	
Login Authentication					
Configuration ~					
Configuration					
AC Config Sync					
Factory Reset					
Reboot					
hebbon					

Figure16.2 AC Configuration Synchronization

# **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 Figure 17.1.

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 Figure 17.2.

млір	WNC6600-1000-	AC(V1) Wireless Controller	(!) ⇒
$\bigcirc$	Basic Info	AC Upgrade	
MONITOR	Basic Config		
	DTLS Config	IOS Upgrade WEB Upgrade	
- <b>Ç</b> Ş	SNMP Config		
CONFIG	License	Upgrade Type HTTP FTP	
Ĥ	AP Access Number	File Name	
DIAGNOSIS	Port Statistics		
	Port Manage	Server IP *	
Ľ	User Manage	Username *	
DEVICE	AC Upgrade		
	AP Upgrade	Password	
	AC Backup	Q Unorade III Clear	
	Login Authentication		
	Configuration >	Upgrade Status	
	Factory Reset	Upgrade Status	
	Reboot	Not Linemand	
		ing opginuuu	
		C Refresh	

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 Figure 17.3.

млір	U WNC6600-10	00-AC(V1) Wireless Controller	${f O}$ Sweet prompt. In the main prepared scenario, please config other device after successing config current device. (	$\rightarrow$
0	Basic Info	FTP Config		1
MONITOR	Basic Config			
	DTLS Config	Server IP		
£ģ3	SNMP Config	Username *		
CONFIG	License			
Â	AP Access Number	Password *		
DIAGNOSIS	Port Statistics			
DETUTION	Port Manage	Save		
$\mathcal{Z}$	User Manage			
DEVICE	AC Upgrade			
~	AP Upgrade	v		
	FTP Config			
	Image Config			
	AP Upgrade			
	AC Backup	>		
	Login Authentication			
	Configuration	>		
	Factory Reset			
	Reboot			
		¢		×



3. Click "Image Config", and click the "FTP" button on the pop-up page to obtain the AP image file, as shown in Figure 17.4.

млір	U WNC6600-	1000-AC(	V1) Wireless	Controller							(!) ⇒
$\bigcirc$	Basic Info	E	Image C	onfig							^
MONITOR	Basic Config										
	DTLS Config		Get	88 FTP 88 CAPWAP							
< <u>ç</u> ş	SNMP Config		Upgrade	Type All Y							
CONFIG	License		opgrooe				p main				
Ĥ	AP Access Number		ii Dele	te							
DIAGNOSIS	Port Statistics			Terrar Mana	Verder News	Des duras Mardada	HIM Marries	Coltana Maria	Usereda Tres	Terrare Anti-ate	A star University
	Port Manage		U	image Name	vendor name	Product Module	nw version	Software version	opgrade type	Image Activate	Auto Opgrade
63	User Manage			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	FTP	Active	Enable
DEVICE	AC Upgrade			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	CAPWAP	Inactive	Enable
$\wedge$	AP Upgrade	~									
	FTP Config										1 .
	Image Config									<u>j&lt;</u> <u>1</u>	$\geq \geq 1  20 \checkmark$
	AP Upgrade										
	AC Backup	>									
	Login Authentication										
	Configuration	>									
	Factory Reset										
	Reboot										

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 Figure 17.5.

млір	WNC6600-1	1000-AC(	V1) Wireless	Controller									(	<u>)</u> 🤄
$\bigcirc$	Basic Info		AP Upg	rade										
MONITOR	Basic Config													
	DTLS Config		11	de hu AD	Unavada b									
-{ĝ}	SNMP Config		Opgra	ade by AP	Upgrade b	y Group								
CONFIG	License		Image Na	ame(Upgrade T	(pe) WA260	0-821-PE(V	2)-comb-2	200.20.2	.6(R).bin(FTP)	~			88	Apply
Ĥ	AP Access Number			_										
DIAGNOSIS	Port Statistics		Filter Co	ndition AL	L v								$\nabla$	Filter
	Pert Manage													
S	User Manage		⊘ Upgr	rade 💍 Ref	resh						Total : 2; Onlin	ne : 2, Conne	cting : 0, O	fline : 0.
DEVICE	AC Upgrade			MAC	IP	AP Name	Status	AP	Software	Device	Image Name	Upgrade	AP Group	Backup
~	AP Upgrade	~				WA2600-				WA2600-		Not	Econ: Econ	
	FTP Config		CC:E	08:1F:96:70:E4	10.11.12.217	7 821- PE(V2)	Online		200.20.2.6(R)	821- PE(V2)	WA2600-821-PE(V2)-comb-200.20.2.6(R).bin(FTP)	Upgraded	NONE	Master
	Image Config		0.000	08.15.06.74.65	10 11 12 222	WA2600-	Online		200 20 2 6(0)	WA2600-	-NONE	Not		Master
	AP Upgrade		0 00.0	78.11.90.74.0L	10.11.12.232	PE(V2)	Online		200.20.2.0(K)	PE(V2)	TOTAL .	Upgraded		Master
	AC Backup	>												
	Login Authentication						U	ograde i	naster APs only,	please mak	te sure the image suitable for the API			
	Configuration	>												
	Factory Reset													-
	Reboot											15 5	~ 21	20 🗸
			4											•
			1											

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.
- Create a new AP upgrade group and select the corresponding image file, as shown in Figure17.6 and 17.7.

млір	WNC6600-	1000-AC(V	1) Wireless Co	ontroller			(!) ⇒
$\bigcirc$	Interface Config	> 📃	AP Group				1
MONITOR	Static Route		Filter Condit	tion			
	DHCP	>	All	~			⊽ Filter
<b>{</b>	WLAN	~					
CONFIG	Wireless Service		+ Create	🖌 Edit 📋 Delete			
Ŧ	AP Template			AP Group Name	Group Type	AP Group Member(s)	Detail Info
DIAGNOSIS	AP Group			Scan	Scan	CC:D8:1F:96:70:E4 ~	Group Member Detail
ez,	AP Config			222	Image Upgrade	none 🗸	Group Member Detail
DEVICE	AP Login Manageme	tin .					
$\wedge$	AAA	>					≤ ≤ 1 ≥ ≥  20 ¥
LOG	Access Control	>					
	RRM	>					
	BYOD	>					
	Load Balance						
			•				

#### Figure17.6 Create an AP upgrade group

млі	WNC6600-	1000-4	AC(V1) Wireless Controller		(!) ⇒
$\bigcirc$	Interface Config	>	Add AP Group		^
MONITOR	Static Route				
	DHCP	>	Group Name	ftpUpgrade *	
<b>5</b>	WLAN	$\sim$	Group Type	Image Upgrade 🗸	
CONFIG	Wireless Service		Defects Genera	No	
Ĥ	AP Template		Default Group		
DIAGNOSIS	AP Group		Image Type	FTP v	
N	AP Config		Group Image	WA2600-821-PE(V2)-comb-200.20.2.6(R).bin v	
DEVICE	AP Login Managem	ent	Auto Upgrade	Disable v	
Δ	AAA	>			
<u>_!</u> _ 1.06	Access Control	>	Submit Cancel		
	RRM	>			
	BYOD	>			
	Load Balance				

#### Figure 17.7 Configure AP upgrade group

7. Add the APs to be upgraded to the upgrade group, as shown in Figure 17.8.

млія	WNC6600-10	00-AC(V1	) Wirele	ess Controller							(!) ⇒
$( \mathbf{P} )$	Interface Config Static Route	>	AP Cor	nfig							^
MONITOR	DHCP WLAN	> ~	AP Gro	oup Group Type	Image Upgrade 🗸	]	ftpUpgrade 🗸		BP JoinGr	oup	LeaveGroup
CONFIG	Wireless Service		Filter								
DIAGNOSIS	AP Group		+ Ci	reate 🖌 Edit 🛅 D	elete 🕑 Reboot	🖒 Reset					· · · · · ·
DEVICE	AP Login Management			MAC	Config Status	AP Template	AP Name	AP Group	AP Location	Status	Backup Status
	AAA Access Control	>		CC:D8:1F:96:70:E4	Customization	NONE V Test V	WA2600-821-PE(V2) WA2600-821-PE(V2)	Scan:Scan		Online	Master
	RRM BYOD	>							Le		20.0
	Load Balance										, .



8. After successfully adding, you can perform the upgrade operation, as shown in Figure 17.9.

мліг	WNC6600-1	000-AC(	V1) Wireless Controller	(!) ⇒
$\bigcirc$	Basic Info	=	AD Harmonda	<u>^</u>
( ) MONITOR	Basic Config		AP Upgrade	
	DTLS Config		Unergedie hur 400 Unergedie hur Cerum	
र्द्र	SNMP Config		Opgrade by AP Opgrade by Group	
CONFIG	License		Upgrade Group flpUpgrade 🗸	
Ĥ	AP Access Number			
DIAGNOSIS	Port Statistics			
	Port Manage			
E.	User Manage			
DEVICE	AC Upgrade			
	AP Upgrade	~		
	FTP Config			
	Image Config			
	AP Upgrade			
	AC Backup	>		
	Login Authentication			
	Configuration	>		
	Factory Reset			
	Reboot			

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.

млір	WNC6600-10	000-AC(V1) Wireless Controller			(!) ⇒
0	Basic Info	Image Config			*
MONITOR	Basic Config				
	DTLS Config	Get BB FTP BB CAPWAP			
< <u>ç</u> ş	SNMP Config	Upprade Type All			
CONFIG	License				P 1.000
Ĥ	AP Access Number	Delete			
DIAGNOSIS	Port Statistics		Marsian Descade Ture	Impos Astivato	Auto Unorodo
	Port Manage	CAPWAP	opgrade type	Image Activate	Auto Opgrade
63	User Manage	Image Name Choose File No file chosen 500-821-PE(V2) 200.20.	.2.6(R) FTP	Active	Enable
DEVICE	AC Upgrade	500-821-PE(V2) 200.20.	.2.6(R) CAPWAP	Inactive	Enable
$\wedge$	AP Upgrade	V Upgrade Disable			
LOG	FTP Config			14 A .	a al 20
	Image Config			12 2 1	≥ ≥[ 20 ♥
	AP Upgrade				
	AC Backup	>			
	Login Authentication				
	Configuration	>			
	Factory Reset				
	Reboot				
		4			×

Figure17.10 Get AP image file

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

мліғ	WNC6600-	1000-AC(V1	) Wireless	Controller		(i) Swee	t prompt:In the m	ain prepared scenario,please o	onfig other device after	successing config curren	device. 🚺	
$\bigcirc$	Basic Info		Image C	onfig								
IONITOR	Basic Config											
	DTLS Config		Image Get BB FTP BB CAPWAP									
٢ <u></u>	SNMP Config		Ungrade								⊽ Filtor	
CONFIG	License		opjinde i jpe					y Pilo				
Ĥ	AP Access Number		🗊 Dele	rte								
AGNOSIS	Port Statistics											
	Port Manage		U	Image Name	Vendor Name	Product Module	HW Version	Software Version	Upgrade Type	Image Activate	Auto Upgrade	
2	User Manage			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	FTP	Active	Enable	
DEVICE	AC Upgrade			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	CAPWAP	Active	Enable	
Λ	AP Upgrade	~										
LOG	FTP Config									_		
	Image Config									$ \leq \leq 1$	≥ ≥l 20	
	AP Upgrade											
	AC Backup	>										
	Login Authentication											
	Configuration	>										
	Factory Reset											
	Reboot											

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 Figure 17.12.

млір	WNC6600-1	1000-AC(	V1) Wireless	Controller							(!) ⇒	
	Basic Info		Image C	mage Config								
MONITOR	Basic Config		Image									
	DTLS Config		Get	Get 88 FTP 88 CAPWAP								
<b>{</b> \circ}	SNMP Config License		Upgrade Type All							∀ Filter		
CONFIG			- 19 · · · · · · ·									
( <del>+</del> )	AP Access Number		1 Dele	te								
DIAGNOSIS	Port Statistics			Tenne Neme	Vender Neme	Denduct Medula	WW Versien	Celturase Version	Unarrado Tuno	Image Activate	Auto Unorado	
	Port Manage		0	inage warne	venuor marrie	Product Module	nw version	Sortware version	opgrade type	Image Activate	Auto opgrade	
23	User Manage			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	FTP	Active	Enable	
DEVICE	AC Upgrade			WA2600-821-PE(V2)-comb-200.20.2.6(R).bin	Maipu	WA2600-821-PE(V2)		200.20.2.6(R)	CAPWAP	Active	Enable	
$\wedge$	AP Upgrade	~										
	FTP Config											
	Image Config									$\leq \leq 1$	≥ ≥[ 20 ∨	
	AP Upgrade											
	AC Backup	>										
	Login Authentication											
	Configuration	>										
	Factory Reset											
	Reboot											



# **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 Figure 18.1.

мліг	WNC6600-10	000-AC(V1	) Wireless Controller		(!) ⇒
MONITOR	Basic Info Basic Config		Basic Info		i
<u></u>	DTLS Config SNMP Config		Product Info Device IP Syste	em Info	
CONFIG	License		Host Name	AC1	
DIAGNOSIS	Port Statistics		Product SN	D889224271800001	
ez i	Port Manage User Manage		System Name	WNC6600	
DEVICE	AC Upgrade	>	Hardware Version	1 34	
	AC Backup	>	Software Version	7.7.2.15(R)	
	Login Authentication Configuration	>	MAC Address	CC:D8:1F:43:81:DA	
	Factory Reset				
	Reboot				



### **19.4 License Query**

Query the license status on the AC through the web page, as shown in Figure 18.2.

млі	WNC6600-1	000-AC(V	1) Wireless Controller			(!) →					
$( \circ )$	Basic Info		License			1					
MONITOR	DTLS Config		License Status	License Status License Management							
CONFIG	SNMP Config		Number of AP Access								
Ŧ	AP Access Number		Register ID	License Status	Number of Authorization	Expire					
DIAGNOSIS	Port Statistics Port Manage		there is a fit to plan in								
DEVICE	User Manage		Register ID	License Status	Number of Authorization	Expire					
$\wedge$	AP Upgrade	>									
LOG	AC Backup Login Authentication	>									
	Configuration	>									
	Factory Reset Reboot										

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 Figure 18.3.

мліг	WNC6600-1	1000-AC(	V1) Wireless Controller		(!) ⇒
MONITOR	Basic Info Basic Config		License		1
<b>t</b> ĝ;	DTLS Config SNMP Config		License Status	License Management	
CONFIG	License		License Import		
( <del>†</del> )	AP Access Number		Import Type	HTTP FTP Manual	
DIAGNOSIS	Port Statistics				
~	Port Manage		License File	Choose File No file chosen	
23	User Manage				
DEVICE	AC Upgrade		🕑 Import		
Λ	AP Upgrade	>	License Export		
	AC Backup	>			
2003	Login Authentication			File Name	Action
	Configuration	>			
	Factory Reset				
	Reboot				

#### 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

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 Figure 18.4 and 18.5.

A CONTRACT AND A CONTRACT		_
Version:2 Module Name:LICENSE_AP_NUM Register ID:1420706266336 Register Code: Machine Code:1234567890 Register Number:1024 Register Date:2015-01-08 End Date:-1		*
AgZy5uUuxsG4xQX7cSawkedu6oZ7XAX/4VUyxhYLmF9mwy7D2hg9yBPqmdXef93t97405aZUzrvQ qqOWJHcDUxbIImmbBD+dZF/203nOB16knCtsLvxw73/hn2dSYDadt/HMcEhdfR017BVADSdmjdwA K9DGkvZ1/2fOmaubAYs=		
4	Þ	-



мліғ	WNC6600-100	00-AC(V1	) Wireless Controller		! ⇒
	Basic Info	=	License		· · · · · · · · · · · · · · · · · · ·
MONITOR	Basic Config		License		
	DTLS Config		Liconco Status Liconc	iconce Management	
- <del>(</del> ĝ}	SNMP Config		License status		
CONFIG	License		License Import		
Ĥ	AP Access Number				
DIAGNOSIS	Port Statistics		Import lype	HIIP FIP Manual	
	Port Manage			tuLCNYktBBtU vmV0EszePhCaIdY23+sWK3/Xb4iCusNr	
E.	User Manage		Content	s8e3nwDDoMa/9HlHZ0Yyz0z3lu11KmJx ODZ9Pvl3TgF8	
DEVICE	AC Upgrade			fh4kaxXjUD0Eb3JMYAg=	
	AP Upgrade	>	🖓 Imnort 🕅 Clear		
	AC Backup	>	C infin		
	Login Authentication		License Export		
	Configuration	>		File Name	Action
	Factory Reset				
	Reboot				

Figure18.5 Import License

### 19.5.2 Export License

Export the license configuration, as shown in Figure 18.6.

млія	WNC6600-1	1000-AC(V	1) Wireless Controller		(!) ⇒
MONITOR	Basic Info Basic Config		License		Î
ŝ	DTLS Config SNMP Config		License Status	License Management	
CONFIG	License		License Import		
	AP Access Number Port Statistics		Import Type	HTTP FTP Manual	
	Port Manage		License File	Choose File No file chosen	
63	User Manage				
DEVICE	AC Upgrade		⊘ Import		
$\wedge$	AP Upgrade	>	License Export		
	AC Backup	>			
	Login Authentication			File Name Action	
	Configuration	>	L		
	Factory Reset				
	Reboot				

Figure18.6 Export License

# **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. 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:

мліғ	WNC6600-	1000-AC(	V1) Wireless Controller					(!) ⇒
Q	Interface Config	>	MAC Filter					^
MONITOR	Static Route		HACTING					
	DHCP	>	Plack and Milita List group	Clobal Config				
<u></u>	WLAN	>	Black and white List group	Global Conlig				
CONFIG	AAA	>	Group Name	Time Type	e Forever 🗸			
Ĥ	Access Control	~						
DIAGNOSIS	MAC Filter		Aging Time(day)	Description	1	⊘ Create 🔟 Cancel		
~	WLAN ACL		i Delete					
DEVICE	Time Rule		No. Gro	up Name Time	Range Agins	g Descript	on Operatio	0
	RRM	>			Time(da	ay)		
$\wedge$	BYOD	>						
LOG	Load Balance							

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

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;

млір	WNC6600-	1000-AC	(V1) Wirel	ess Controll	er				(!) ⇒		
$\bigcirc$	Interface Config	>	MAG	1AC Filter							
MONITOR	Static Route		MAC								
	DHCP	>	DI	and Milete	clebel Cen	6					
£ģ3	WLAN	>	Dia		Global Con	ng					
CONFIG	AAA	>	G	iroup Name		Time Type Forever	~				
Ĥ	Access Control	$\sim$									
DIAGNOSIS	MAC Filter		Aging	Time(day)	Description 🖉 Create 🛅 Cancel						
~	WLAN ACL		Ū D	elete							
DEVICE	Time Rule			No.	Group Name	Time Range	Aging	Description	Operation		
	RRM	>	-			-	Time(day)				
$\triangle$	BYOD	>	U	1	black	rorever			Zedit 🔟 Delete		
LOG	Load Balance										

#### Fifure 20.2 Rule groups

	WNC6600-1000-AC(V1) Wireless Controller					Sweet prompt	$\oplus$ Sweet promptin the main prepared scenario,please config other device after successing config current device.				
0	Interface Config	> 🔳	Black ar	nd White List o	Iroup					*	
MONITOR	Static Route		Diacital		hodb						
	DHCP	>									
<b>5</b>	WLAN	>	MAC Addre	255							
CONFIG	ААА	>	Time Type			Forever 🗸					
Ĥ	Access Control	~	Description								
DIAGNOSIS MAC Filter											
~	WLAN ACL		⊘ Submit 📋 Cancel								
Ľ.	Time Rule										
DEVICE	RRM	>	1 Delete	e 📮 import CSV	file 坐 export CSV file			MAC Address 💊	~	√ Search	
À	BYOD	>		Mac Number	MAC Address	Time Range	offline duration(dags)	Description	Operation	n	
LOG	Load Balance			1	20:20:20:20:20:20	NONE	0		🖌 Edit 📋	Delete	
				2	00:20:22:12:22:21	NONE	0		🖌 Edit 📋	Delete	
									< < 1 >	>  10 🗸	
			Cancel								

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

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:

	C5 🔻 🔄	$f_x$						
	A	В	С	D	E	F	G	H
1	#mac	time-range	descripti	on				
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								
7								

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;

млі	WNC6600-	1000-AC(	(V1) Wireless Controller		(!) ↔
6	Interface Config	>	Wireless Service Blacklist &	Whitelist	*
MONITOR	Static Route				
	DHCP	>	Mac Enable	Blacklist 🗸	
<b>{</b>	WLAN	$\sim$	Group Name	black	
CONFIG	Wireless Service		2 Submit		
Ŧ	AP Template		Oubline		
DIAGNOSIS	AP Group				
S.	AP Config				
DEVICE	AP Login Managem	ent			
^	AAA	>			
	Access Control	>			
Log	RRM	>			
	BYOD	>			
	Load Balance				

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;

мдір	WNC6600-	1000-AC(V	1) Wireless Controller		(!) ⇒
( )	Interface Config Static Route	> =	MAC Filter		1
MONITOR	DHCP	>	Black and White List group	Global Config	
CONFIG	AAA	>	Mac Enable	Blacklist 🗸	
	Access Control MAC Filter	~	Group Name	black	
Ľ	WLAN ACL Time Rule		⊘ ок		
DEVICE	RRM	>			
rog	BYOD Load Balance	>			

Figure 20.6 Enable the global blacklist function



 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.

# **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.

# 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)	<ul> <li>2. Device Status Indicator</li> <li>SYS: system status</li> <li>PWR: power state</li> <li>FAN: fan status</li> <li>USB: USB interface status</li> </ul>
3.	USB port	4. Combo port (10/100/1000Base-T+100BASE- FX/1000Base-X)
5.	Combo port status indicator	<ol> <li>Port status indicator</li> <li>CON: Console port status indicator</li> <li>DC0: DC0 port status indicator</li> </ol>
7.	10/100BASE-T electrical interface	8. Console port
9.	DC0 port (10/100/1000Base-T)	



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	<ol> <li>Bevice Status Indicator</li> <li>SYS: system status</li> <li>PWR2: Power2 status</li> <li>PWR1: power supply1 status</li> <li>SD: SD card status indicator</li> </ol>
9.	Reset button (press and hold for 3 seconds to restart the device	10. DC0 port (10/100/1000Base-T)



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	<ul> <li>8. Device Status Indicator</li> <li>SYS: system status</li> <li>PWR2: Power2 status</li> <li>PWR1: Power1 status</li> <li>SD: SD card status indicator</li> </ul>
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)



# 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

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



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



- 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

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

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



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