

The privilege of HCNA/HCNP/HCIE:

With any Huawei Career Certification, you have the privilege on <http://learning.huawei.com/en> to enjoy:

- 1、e-Learning Courses: Logon <http://learning.huawei.com/en> and enter [Huawei Training/e-Learning](#)
 - If you have the HCNA/HCNP certificate: You can access Huawei Career Certification and Basic Technology e-Learning courses.
 - If you have the HCIE certificate: You can access all the e-Learning courses which marked for HCIE Certification Users.
 - Methods to get the HCIE e-Learning *privilege*: Please associate HCIE certificate information with your Huawei account, and email the account to Learning@huawei.com to apply for HCIE e-Learning privilege.
- 2、Training Material Download
 - Content: Huawei product training material and Huawei career certification training material.
 - Method: Logon <http://learning.huawei.com/en> and enter [Huawei Training/Classroom Training](#), then you can download training material in the specific training introduction page.
- 3、Priority to participate in [Huawei Online Open Class \(LVC\)](#)
 - The Huawei career certification training and product training covering all ICT technical domains like R&S, UC&C, Security, Storage and so on, which are conducted by Huawei professional instructors.
- 4、Learning Tools:
 - [eNSP](#): Simulate single Router&Switch device and large network.
 - [WLAN Planner](#): Network planning tools for WLAN AP products.
- In addition, Huawei has built up [Huawei Technical Forum](#) which allows candidates to discuss technical issues with Huawei experts, share exam experiences with others or be acquainted with Huawei Products.
- Statement:

This material is for personal use only, and can not be used by any individual or organization for any commercial purposes.

Huawei WLAN Certification Training

HCNA-WALN Experiment Guide for WLAN Engineers(WEB)

ISSUE:2.0



HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://e.huawei.com>



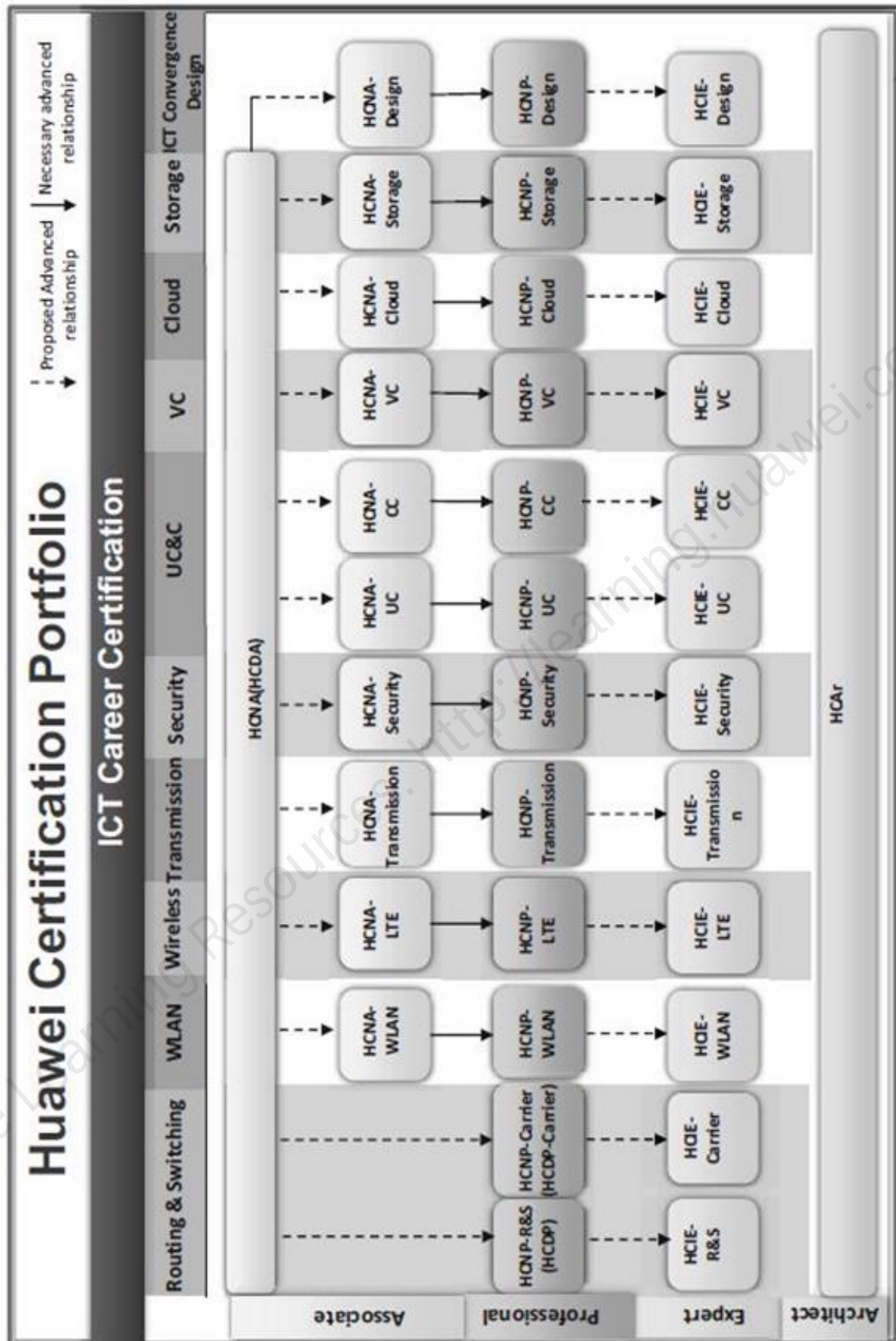
Huawei Certificate System

Relying on the strong technical strength and professional training system, Huawei provides a practical and professional four-level certificate system to meet various customer requirements on different WLAN technologies.

Huawei Certified Network Associate-Wireless Local Area Network (HCNA-WLAN) is designed for Huawei local offices, online engineers in representative offices, and readers who want to understand Huawei WLAN products and technology. HCNA-WLAN covers WLAN basics, Control and Provisioning of Wireless Access Points (CAPWAP) protocol, WLAN networking, Huawei WLAN product features, security configuration, WLAN advanced technology, antennas, WLAN network planning and optimization, and WLAN fault troubleshooting.

The HCNA-WLAN certificate system introduces you to the industry and market, helps you in innovation, and enables you to stand atop the WLAN frontiers.

More Learning Resources: <http://learning.huawei.com/en>



About This Document

Overview

This document is applicable to the candidates who are preparing for the HCNA-WLAN exam and the readers who want to understand the WLAN basics, the CAPWAP protocol, WLAN networking, Huawei WLAN product features, security configuration, WLAN advanced technology, antennas, WLAN network planning and optimization, and WLAN fault troubleshooting.

Description

This experiment guide introduces the following six experiments, covering basic configurations, and configurations and implementation of Layer 2 networking, security, Layer 3 networking, and the network management software eSight.

- Experiment 1: AC configuration initialization
This experiment involves basis operations and configurations on an AC, helping you know the AC6005 and its basic functions.
- Experiment 2: AP authentication and WLAN configuration process
This experiment lets you know basic WLAN network capabilities through basic WLAN configurations.
- Experiment 3: WLAN security configuration
This experiment mainly introduces 802.1x authentication, helping you know WLAN security and the configuration process.
- Experiment 4: WLAN configuration on eSight
This experiment involves how to add WLAN devices to the eSight and deliver WLAN services using the configuration wizard.
- Experiment 5: Bypass Layer 3 networking
This experiment uses the AC6005 and Layer 3 networking. The Layer 3 network configuration helps you comprehensively know WLAN networking modes.
- Experiment 6: Configuration file backup and AC configuration clearance
This experiment describes how to back up configuration files through File Transfer Protocol (FTP).

Background Knowledge Required

- The intended audience should know basic WLAN knowledge, Huawei switching devices, and basic datacom knowledge.

Common Icons



AC



AP



Switch



eSight



Radius Server



STA

Experiment Environment Overview

Networking Introduction

This experiment environment is prepared for WLAN engineers who are preparing for the HCNA-WLAN exam.

Each suite of experiment environment includes 2-6 ACs, 2-12 APs, 1 core switch, and 1 Remote Authentication Dial In User Service (RADIUS) or eSight server. Each suite of experiment environment is applicable to 4 to 12 candidates.

Device Introduction

The following table lists devices recommended for HCNA-WLAN experiments and the mappings between the device name, model, and software version.

Device name	Model	Software Version
Core Switch	S3700-28TP-PWR-EI or S5700-28C-PWR-EI	Version 5.70 (S3700 V100R005C01SPC100) Version 5.130 (S5700 V200R003C00SPC300)
AC	AC6005-8-PWR	AC6005 V200R007C10SPC100
AP	AP4030DN	AP4030DN V200R007C10SPC100
NMS	eSight Network	eSight Network V300R006C00SPC505

Experiment Environment Preparation

Checking Whether All Devices Are Available

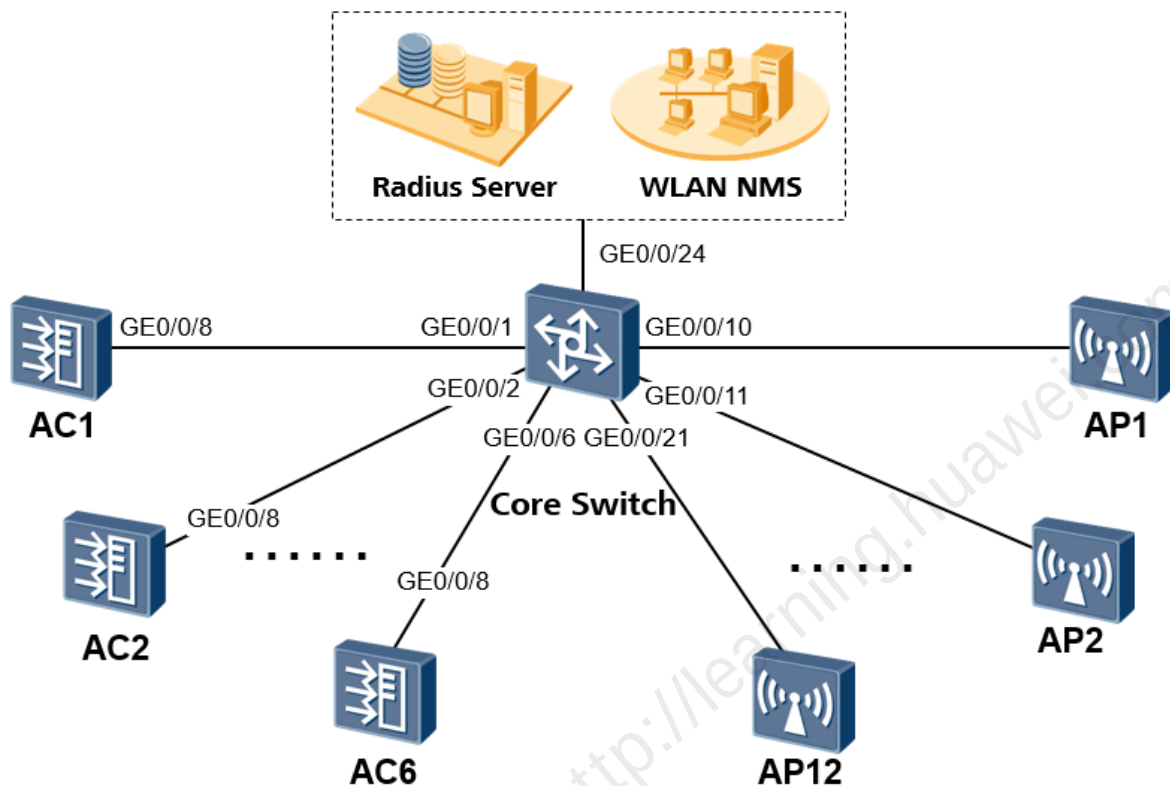
Before starting the experiment, check whether all required devices are ready. The following table lists the required devices.

Device	Quantity	Remarks
eSight	1	Shared by all groups
Radius Server	1	Shared by all groups
Huawei 3700PoE/ Huawei 5700PoE Switch	1	Shared by all groups
AC6005	One for each group	
AP4030DN	Two for each group	
Laptop or desktop computer	One for each group	A desktop computer requires a network adapter
Twisted pair	Four for each group	The twisted pair must be at least 2 meters long
Console cable	One for each group	

Each group must check whether the following devices are ready:

- One AC6005
- Two AP4030DN
- One laptop or desktop computer
- Four twisted pairs
- One console cable

Experiment topology



Key points of bypass topology establishment:

This course uses a layer 3 bypass topology. Devices are connected as follows:

For group 1, port 8 of AC1 is connected to port 1 of the switch. AP1 is connected to port 10 of the switch. AP2 is connected to port 11 of the switch.

For group 2, port 8 of AC2 is connected to port 2 of the switch. AP3 is connected to port 12 of the switch. AP4 is connected to port 13 of the switch.

For group 3, port 8 of AC3 is connected to port 3 of the switch. AP5 is connected to port 14 of the switch. AP6 is connected to port 15 of the switch.

The same rule applies to all other groups.

For group 6, port 8 of AC6 is connected to port 6 of the switch. AP11 is connected to port 20 of the switch. AP12 is connected to port 21 of the switch.

AC Configuration Removal

Trainees must remove previously saved configurations after the experiment is complete and before devices are turned off, to avoid any impact of the configurations on the next experiment. In addition, trainees must confirm that the device is not configured before an experiment starts. If it is not, remove the configurations and then restart the device.

You need a password to log in to the router. The login password is Admin@123 in this experiment.

```
Login authentication
```

```
Password:Admin@123
```

```
<AC6005>reset saved-configuration
```

```
This will delete the configuration in the flash memory.
```

```
The device configurations will be erased to reconfigure.
```

```
Are you sure? (y/n)[n]:y
```

```
Clear the configuration in the device successfully.
```

To restart the controller, run the following command:

```
<AC6005>reboot
```

```
Info: The system is comparing the configuration, please wait.
```

```
Warning: All the configuration will be saved to the next startup configuration.
```

```
Continue ? [y/n]:n
```

```
System will reboot! Continue ? [y/n]:y
```

```
Info: system is rebooting ,please wait...
```



Contents

About This Document.....	3
Overview	3
Description	3
Background Knowledge Required	4
Common Icons	4
Experiment Environment Preparation.....	6
1 Experiment 1:AC configuration initialization.....	12
1.1 About This Course.....	12
1.1.1 Objectives	12
1.1.2 Topology	12
1.1.3 Plan	13
1.2 Experiment Task	14
1.2.1 Configuration Procedure.....	14
1.3 Verification	25
1.3.1 Telnet AC	25
1.4 Reference Configuration	25
1.4.1 S5700 Configuration	25
1.4.2 AC Configuration.....	27
2 Experiment 2: AP Authentication and WLAN Configuration Roadmap	32
2.1 About This Course.....	32
2.1.1 Objectives	32
2.1.2 Topology	32
2.1.3 Plan	33
2.2 Experiment Task	35
2.2.1 Configuration Procedure.....	35
2.3 Verification	55
2.3.1 Checking the VAP List.....	55
2.3.2 Terminal Connection Test.....	55
2.4 Reference Configuration	56
2.4.1 S5700 Configuration	56
2.4.2 AC Configuration.....	58
3 Experiment 3: WLAN Security Configuration.....	64
3.1 About This Course.....	64
3.1.1 Objectives	64
3.1.2 Topology	64



3.1.3 Plan	65
3.2 Experiment Task	66
3.2.1 Configuration Procedure	66
3.3 Verification	83
3.3.1 Connect an STA to the WLAN	83
3.4 Reference Configuration	84
3.4.1 S5700 Configuration	84
3.4.2 AC Configuration	86
4 Experiment 4: eSight WLAN Management	92
4.1 About This Course	92
4.1.1 Objectives	92
4.1.2 Topology	92
4.1.3 Plan	93
4.2 Experiment Task	94
4.2.1 Configuration Procedure	94
4.3 Verification	113
4.3.1 Connect an STA to the WLAN	113
4.4 Reference Configuration	114
4.4.1 S5700 Configuration	114
4.4.2 AC Configuration	117
5 Experiment 5: Layer 3 Networking Experiment	123
5.1 About This Course	123
5.1.1 Objectives	123
5.1.2 Topology	123
5.1.3 Plan	124
5.2 Experiment Task	125
5.2.1 Configuration Procedure	125
5.3 Verification	130
5.3.1 Verify the L3 Network Status	130
5.4 Reference Configuration	131
5.4.1 S5700 Configuration	131
5.4.2 AC Configuration	133
6 Experiment 6: Backup the Configuration and Reset the Device	139
6.1 About This Course	139
6.1.1 Objectives	139
6.1.2 Plan	139
6.2 Experiment Task	140
6.2.1 Configuration Procedure	140
6.3 Verification	144
6.3.1 Checking the Device Configuration	144



6.4 Reference Configuration	147
6.4.1 Key Configuration.....	147
7 Appendix	148
7.1 Configuration of Core Switch.....	148

More Learning Resources: <http://learning.huawei.com/en>

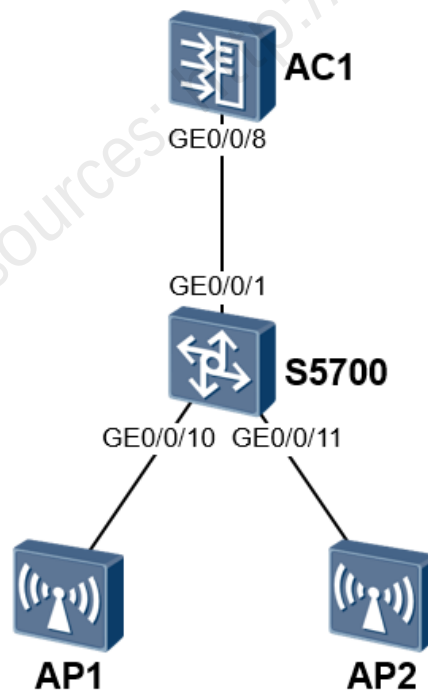
1 Experiment 1: AC configuration initialization

1.1 About This Course

1.1.1 Objectives

- Configure the initialization password
- Configure VLAN and routing in the AC
- Configure telnet service of the AC
- Save the configuration in the AC

1.1.2 Topology



1.1.3 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

The following table describes device connections.

Group No	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	- AP1-G0/0/10 - AP2-G0/0/11
2	AC2—G0/0/2	- AP3-G0/0/12 - AP4-G0/0/13
3	AC3—G0/0/3	- AP5-G0/0/14 - AP6-G0/0/15
4	AC4—G0/0/4	- AP7-G0/0/15 - AP8-G0/0/16
5	AC5—G0/0/5	- AP9-G0/0/17 - AP10-G0/0/18
6	AC6—G0/0/6	- AP11-G0/0/19 - AP12-G0/0/20

The following table describes an AC parameter configuration template.

Trainee GroupX	AC Configuration	
Console Password	Admin@123	
Device	ACX	
AP Management VLAN	VLAN: X0	IP: 10.1.X0.100
Service VLAN (Employee)	VLAN: X1	IP: 10.1.X1.100
Service VLAN (Voice)	VLAN: X2	IP: 10.1.X2.100
Service VLAN (Guest)	VLAN: X3	IP: 10.1.X3.100
AC Port Connecting to the Switch	GE0/0/8 VLANs X0 through X3 can pass the trunk interface	

Topology: layer2 and layer 3 bypass topology

1.2 Experiment Task

1.2.1 Configuration Procedure

Step1 Logging In to the Web Platform

Before logging in to the web platform, ensure that:

- The IP address of the device's access port has been configured.
- The device and your PC are properly connected.
- The device is running properly, and the HTTP and HTTPS services are correctly configured.
- The web browser software has been installed on your PC.

The IP address 169.254.1.1 and subnet mask 255.255.0.0 have been configured on MEth0/0/1 of the AC6605 before the delivery.

The IP address 169.254.1.1 and subnet mask 255.255.0.0 have been configured on MEth0/0/1 of the ACU2 before the delivery.

The IP address 169.254.1.1 and subnet mask 255.255.0.0 have been configured on VLANIF 1 of the AC6005 before the delivery, and interfaces GE0/0/1 to GE0/0/8 have been added to VLAN 1 by default.

Before the device is delivered, the HTTP and HTTPS services have been configured on the device. The default port number is 80 for HTTP and 443 for HTTPS. The default user name and password are respectively admin and admin@huawei.com.



Procedure

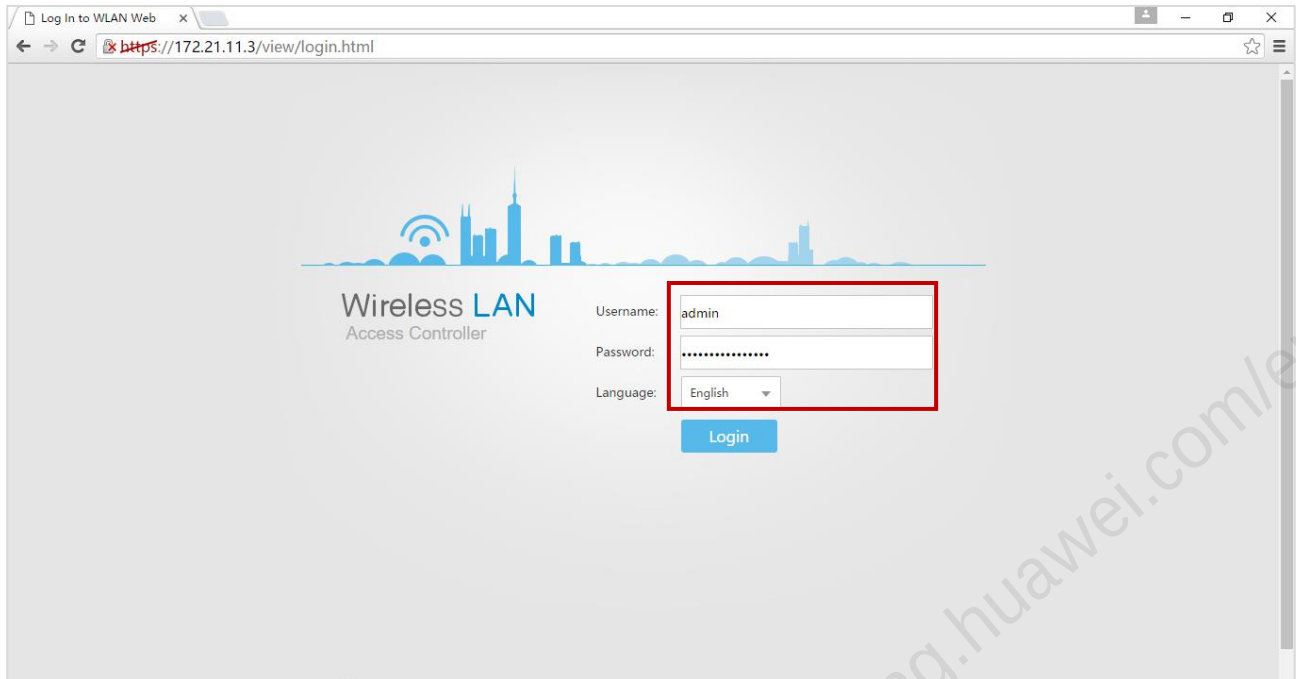
Open a browser such as Internet Explorer 7.0, enter http://IP address or https://IP address in the address box, for example, http://169.254.1.1 or https://169.254.1.1, and press Enter. (For the IP address, see IP addresses of access interfaces configured in Configuring an IP Address for Web Platform Login.) The web platform login page is displayed.

Select a language. The system supports English and Chinese. By default, the system uses the same language as the browser.

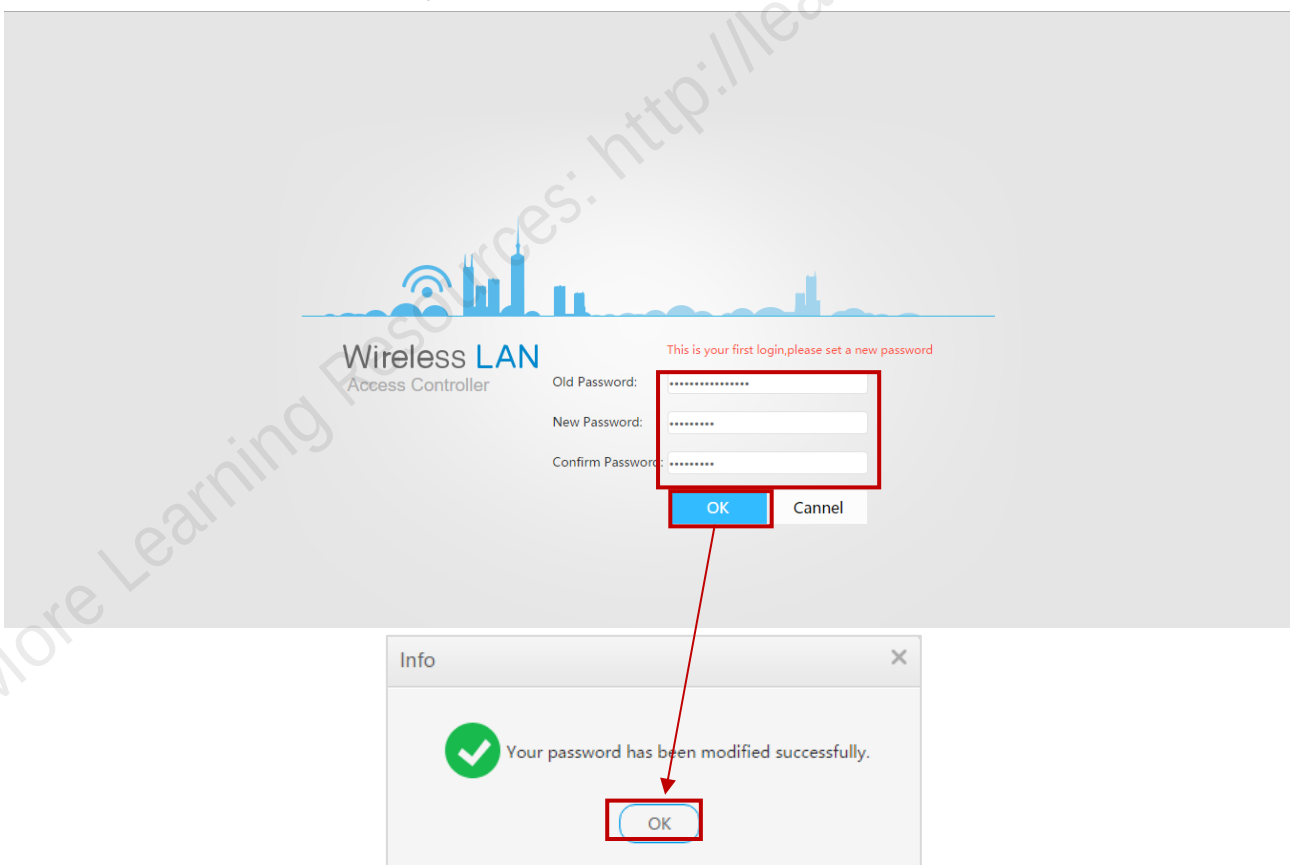
Enter a user name and password. The default user name and password are admin and admin@huawei.com.

Click Login.

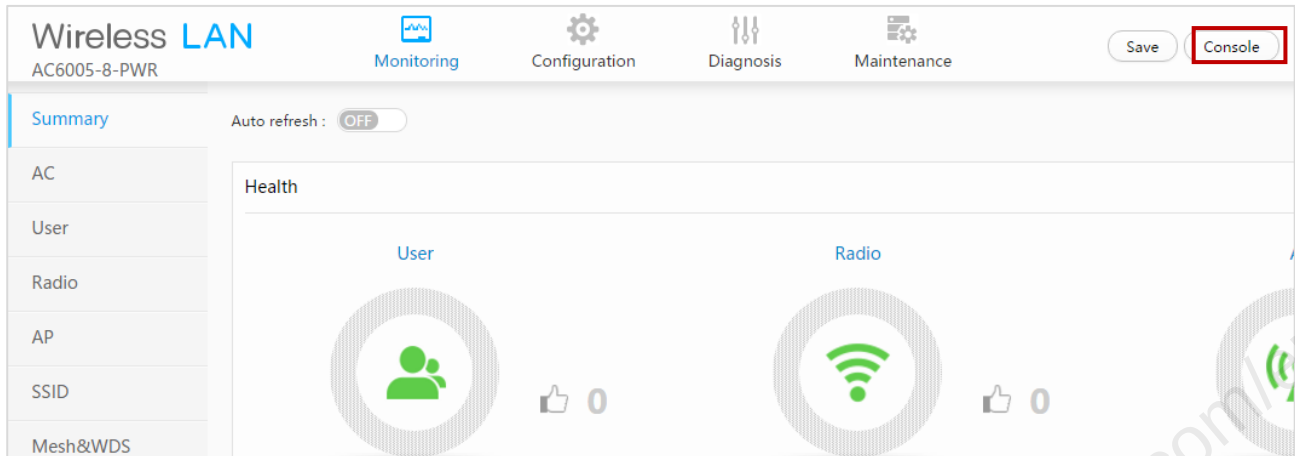
This experiment takes the first set of 172.21.11.3 as an example.



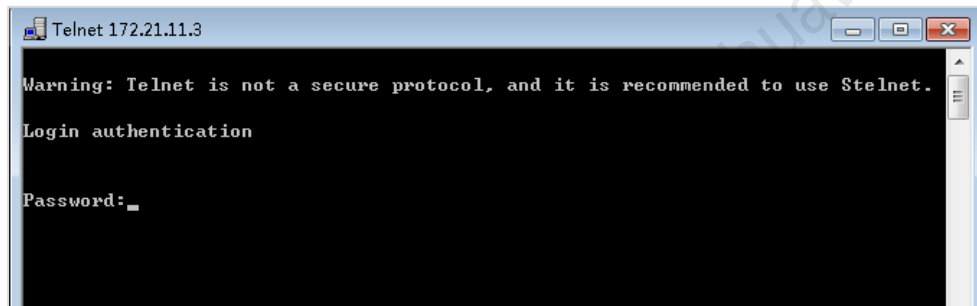
Change the password upon the first login. Changing the password to **Admin@123** is used as an example in this document.



After logging in to the web-based AC, click **Console** at the upper-right corner. The command-line interface (CLI) is displayed.



You can enter command lines to manage and maintain the device. The login password is **Admin@123**. (The Firefox browser is recommended.)



Step2 Configuring a Switch

Configure the access switch S5700. Add GE0/0/10 and GE0/0/11 to VLANX0 (management VLAN) and set the port VLAN ID (PVID) to VLANX0. Add GE0/0/8 to VLANs X0 through X3(Connect to AC).

```
<Huawei>system-view
[Huawei]sysname S5700
[S5700]vlan batch 10 to 13
[S5700]interface GigabitEthernet0/0/10
[S5700-GigabitEthernet0/0/10]port link-type trunk
[S5700-GigabitEthernet0/0/10]port trunk pvid vlan 10
[S5700-GigabitEthernet0/0/10]port trunk allow-pass vlan 10 to 13
[S5700-GigabitEthernet0/0/10]quit
[S5700]interface GigabitEthernet0/0/11
[S5700-GigabitEthernet0/0/11]port link-type trunk
[S5700-GigabitEthernet0/0/11]port trunk pvid vlan 10
[S5700-GigabitEthernet0/0/11]port trunk allow-pass vlan 10 to 13
[S5700-GigabitEthernet0/0/11]quit
[S5700]interface GigabitEthernet 0/0/1
[S5700-GigabitEthernet0/0/1]port link-type trunk
[S5700-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 to 13
[S5700-GigabitEthernet0/0/1]quit
```

Create a LoopbackX interface, and set its IP address to 10X.10X.10X.10X to simulate a public network interface. Create VLANIF interfaces to function as gateways of service VLANs.

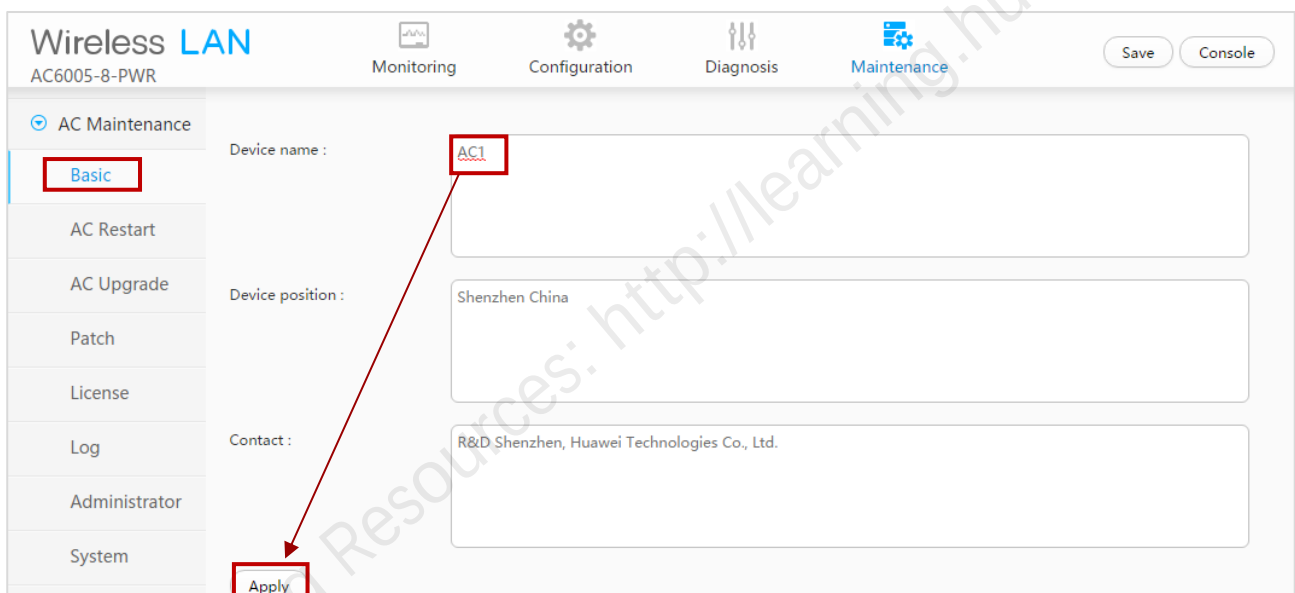
```
[S5700]interface LoopBack 1
```

```
[S5700- LoopBack1]ip address 101.101.101.101 32
[S5700- LoopBack1]quit
[S5700]interface Vlanif 10
[S5700-Vlanif10]ip address 10.1.10.1 24
[S5700-Vlanif10]quit
[S5700]interface Vlanif 11
[S5700-Vlanif11]ip address 10.1.11.1 24
[S5700-Vlanif11]quit
[S5700]interface Vlanif 12
[S5700-Vlanif12]ip address 10.1.12.1 24
[S5700-Vlanif12]quit
[S5700]interface Vlanif 13
[S5700-Vlanif13]ip address 10.1.13.1 24
[S5700-Vlanif13]quit
```

Step3 Configuring Basic AC Parameters

Naming an AC

Choose Maintenance > AC Maintenance > Basic. Set Device name to AC1. Click Apply.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

AC Maintenance

Basic

AC Restart

AC Upgrade

Patch

License

Log

Administrator

System

Device name : AC1

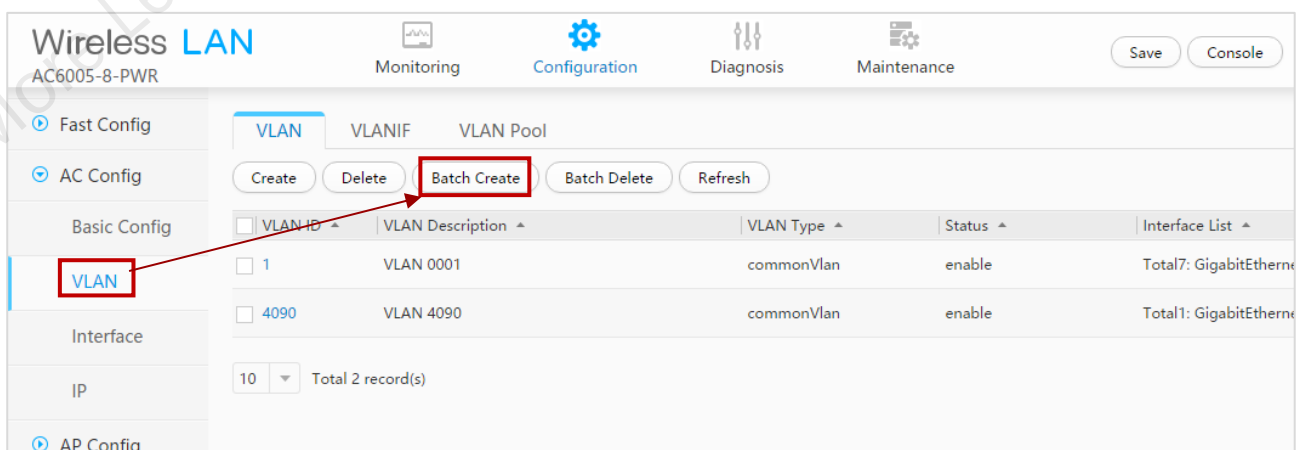
Device position : Shenzhen China

Contact : R&D Shenzhen, Huawei Technologies Co., Ltd.

Apply

Configuring VLANs

Choose Configuration > AC Config > VLAN, The VLAN configuration page is displayed, Click Batch Create.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config

AC Config

Basic Config

VLAN

Interface

IP

AP Config

VLAN

VLANIF

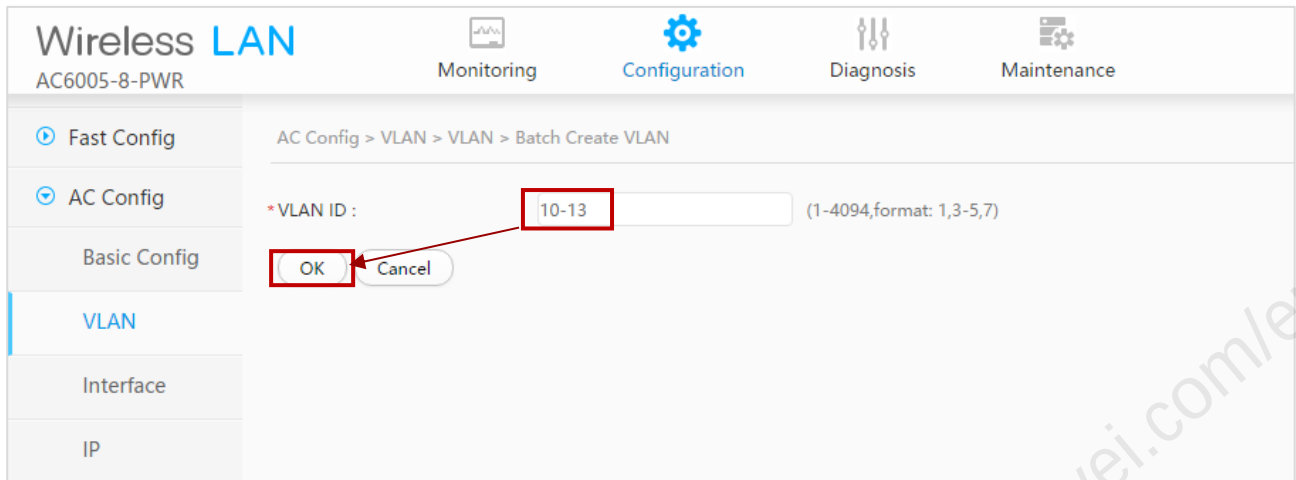
VLAN Pool

Create Delete Batch Create Batch Delete Refresh

VLAN ID	VLAN Description	VLAN Type	Status	Interface List
1	VLAN 0001	commonVlan	enable	Total7: GigabitEthernet
4090	VLAN 4090	commonVlan	enable	Total1: GigabitEthernet

10 Total 2 record(s)

Create VLANX0~VLANX3.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

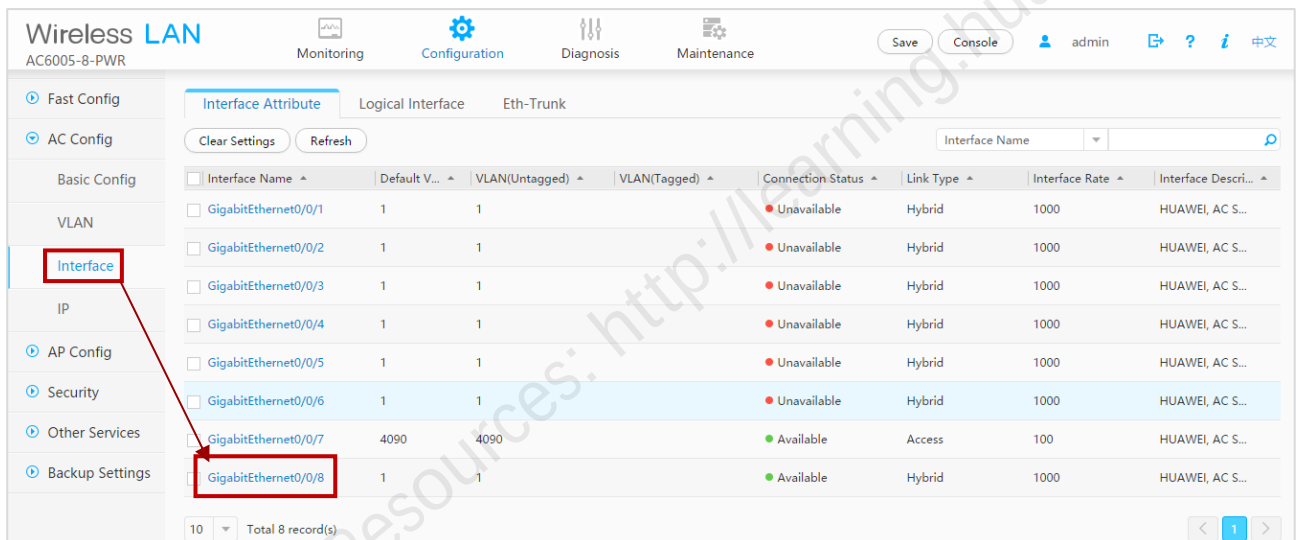
Fast Config AC Config Basic Config VLAN Interface IP

AC Config > VLAN > VLAN > Batch Create VLAN

*VLAN ID : 10-13 (1-4094,format: 1,3-5,7)

OK Cancel

Configure IP address of the GE0/0/8 interface to connect S5700.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

Fast Config AC Config Basic Config VLAN Interface IP AP Config Security Other Services Backup Settings

Interface Attribute Logical Interface Eth-Trunk

Clear Settings Refresh

Interface Name

Interface Name	Default V...	VLAN(Untagged)	VLAN(Tagged)	Connection Status	Link Type	Interface Rate	Interface Descri...
GigabitEthernet0/0/1	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/2	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/3	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/4	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/5	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/6	1	1		Unavailable	Hybrid	1000	HUAWEI, AC S...
GigabitEthernet0/0/7	4090	4090		Available	Access	100	HUAWEI, AC S...
GigabitEthernet0/0/8	1	1		Available	Hybrid	1000	HUAWEI, AC S...

10 Total 8 record(s)

AC Config

Basic Config

VLAN

Interface

IP

AP Config

Security

Other Services

Backup Settings

Interface name: GigabitEthernet0/0/8

Default VLAN: 1

Interface status: ON

Description: HUAWEI, AC Series, GigabitEthernet

Link type: Trunk

PHB mapping: OFF

Added VLAN ID: 10-13

Tagged

VLAN ID	Operation
1	
10-13	

Untagged

VLAN ID	Operation
No data.	

Configure attack defense

Attack Defense Profile:

OK Cancel

Check the interface configuration.

Wireless LAN

AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin

Interface Name

Interface Name	Default VLAN	VLAN(Untagged)	VLAN(Tagged)	Connection Status	Link Type	Interface Rate	Interface Description
GigabitEthernet0/0/1	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/2	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/3	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/4	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/5	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/6	1	1		Unavailable	Hybrid	1000	HUAWEI, AC Series...
GigabitEthernet0/0/7	4090	4090		Available	Access	100	HUAWEI, AC Series...
GigabitEthernet0/0/8	1		1,10-13	Available	Trunk	1000	HUAWEI, AC Series...

Configure IP addresses of the layer 3 interfaces corresponding to the VLANs.
Choose Configuration > AC Config > VLAN > VLANIF. The VLANIF page is displayed.
Click Create. Set parameters on the Create VLANIF page.

Wireless LAN

AC6005-8-PWR

Monitoring

Configuration

Diagnosis

Maintenance

Save

Console

admin

中文

Fast Config

AC Config

Basic Config

VLAN

Interface

IP

AP Config

Global IPv6: OFF

VLAN

VLANIF

VLAN Pool

Create

Delete

Refresh

Interface Name

Interface Name	Connection Status	IPv4 Address/mask	IPv6 Address/prefix	MTU (bytes)	Description
Vlanif1	Available	169.254.1.1/255.255...		1500	HUAWEI, AC Series, Vlanif1 Interface
Vlanif4090	Available	172.21.11.3/255.255...		1500	HUAWEI, AC Series, Vlanif4090 Interface

10

Total record(s)

Wireless LAN

AC6005-8-PWR

Monitoring

Configuration

Diagnosis

Maintenance

Save

Console

admin

Fast Config

AC Config

Basic Config

VLAN

Interface

IP

AP Config

Security

AC Config > VLAN > VLANIF > Create VLANIF

*VLAN ID: 10

Interface status: ON

MTU (bytes): 1500

Description:

IP address format: ☒ IPv4 ☐ IPv6

IPv4 Address

Primary IP address/mask: 10 . 1 . 10 . 100 / 255 . 255 . 255 . 0

Secondary IP address/mask:

OK

Cancel

Wireless LAN

AC6005-8-PWR

Monitoring

Configuration

Diagnosis

Maintenance

Save

Console

admin

Fast Config

AC Config

Basic Config

VLAN

Interface

IP

AP Config

Security

AC Config > VLAN > VLANIF > Create VLANIF

*VLAN ID: 11

Interface status: ON

MTU (bytes): 1500

Description:

IP address format: ☒ IPv4 ☐ IPv6

IPv4 Address

Primary IP address/mask: 10 . 1 . 11 . 100 / 255 . 255 . 255 . 0

Secondary IP address/mask:

OK

Cancel

Wireless LAN AC6005-8-PWR Monitoring Configuration Diagnosis Maintenance Save Console admin

AC Config > VLAN > VLANIF > Create VLANIF

*VLAN ID: 12 Interface status: ON

Basic Config MTU (bytes): 1500 Description:

VLAN IP address format: ☒ IPv4 ☐ IPv6

IPv4 Address Primary IP address/mask: 10.1.12.100 / 255.255.255.0

Secondary IP address/mask: . . . /

OK Cancel

Wireless LAN AC6005-8-PWR Monitoring Configuration Diagnosis Maintenance Save Console admin

AC Config > VLAN > VLANIF > Create VLANIF

*VLAN ID: 13 Interface status: ON

Basic Config MTU (bytes): 1500 Description:

VLAN IP address format: ☒ IPv4 ☐ IPv6

IPv4 Address Primary IP address/mask: 10.1.13.100 / 255.255.255.0

Secondary IP address/mask: . . . /

OK Cancel

Check the VLANIF interface

Wireless LAN AC6005-8-PWR Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

Global IPv6: OFF

VLAN VLANIF VLAN Pool

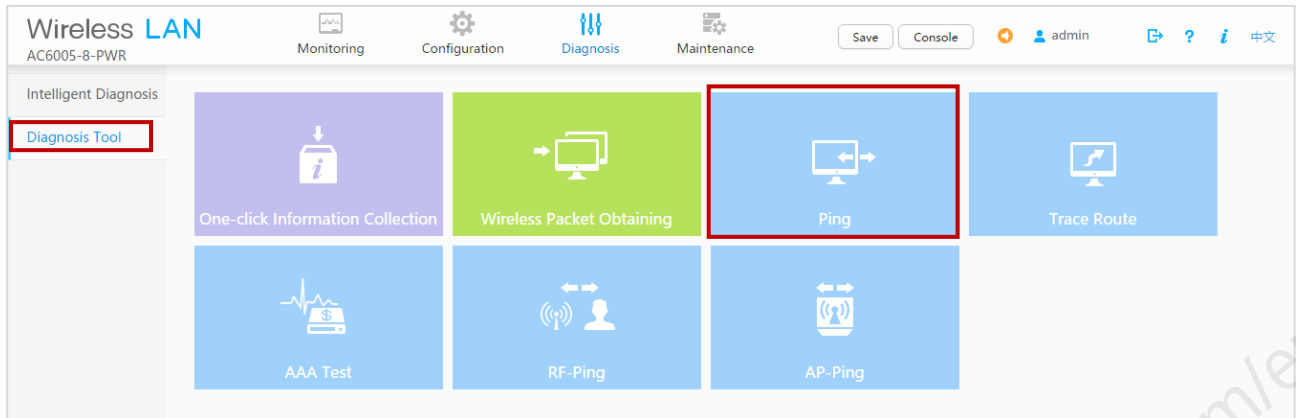
Create Delete Refresh Interface Nam

Interface Name	Connection Status	IPv4 Address/mask	IPv6 Address/prefix	MTU (bytes)	Description
Vlanif1	Available	169.254.1.1/255.255...		1500	HUAWEI, AC Series, Vlanif1 Interface
Vlanif10	Available	10.1.10.100/255.255...		1500	HUAWEI, AC Series, Vlanif10 Interface
Vlanif11	Available	10.1.11.100/255.255...		1500	HUAWEI, AC Series, Vlanif11 Interface
Vlanif12	Available	10.1.12.100/255.255...		1500	HUAWEI, AC Series, Vlanif12 Interface
Vlanif13	Available	10.1.13.100/255.255...		1500	HUAWEI, AC Series, Vlanif13 Interface
Vlanif4090	Available	172.21.11.3/255.255...		1500	HUAWEI, AC Series, Vlanif4090 Interface

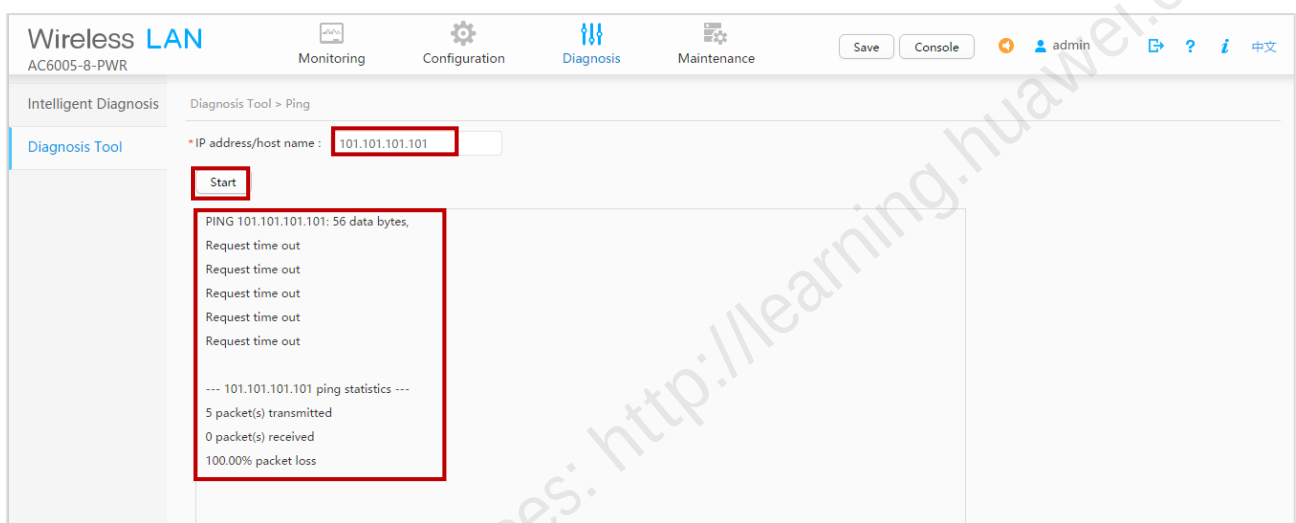
10 Total 6 record(s)

Check whether the route between the AC and the layer 3 switch is reachable. The following command output indicates that 10X.10X.10X (the simulated public network interface on the switch) cannot be pinged.

Choose Diagnosis > Diagnosis Tools > Ping.



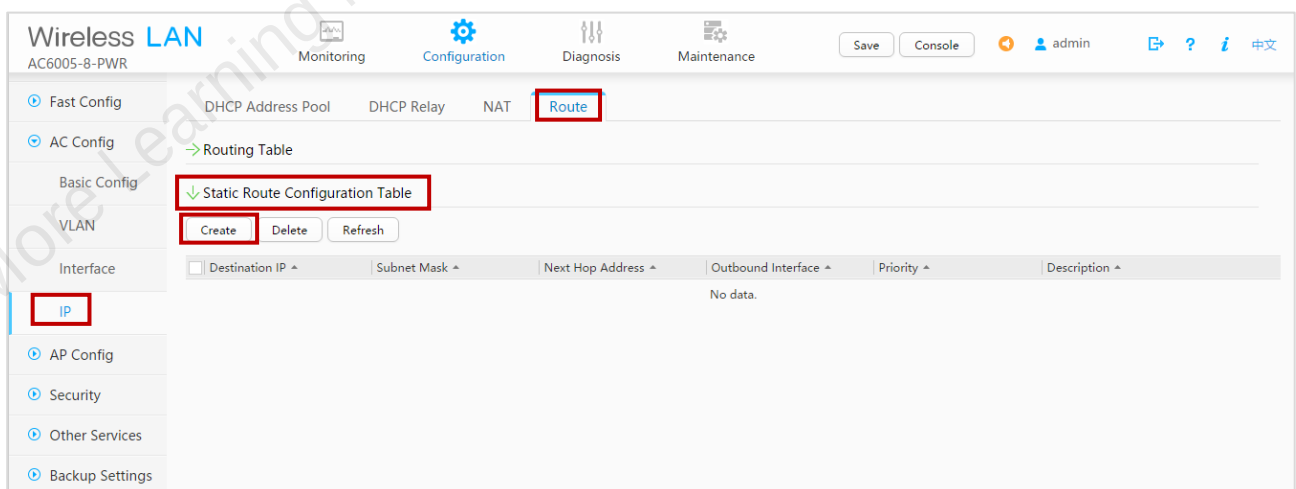
Enter the destination IP address, click start.



Configure a static route for the switch.

Choose Configuration > AC Config > IP > Route > Static Route Configuration Table. The static route management page is displayed.

Click Create, configure static route information on the new page, and click OK.



Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

Fast Config AC Config Basic Config VLAN Interface IP

AC Config > IP > Route > Create Static Route

* Destination IP : 0 . 0 . 0 . 0 * Subnet mask : 0 . 0 . 0 . 0

Next hop address : 10 . 1 . 10 . 1 Outbound interface : ...

Priority : Description :

OK Cancel

IP address 10X.10X.10X.10X can be pinged.

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

Intelligent Diagnosis Diagnosis Tool > Ping

* IP address/host name : 101.101.101.101

Start

PING 101.101.101.101: 56 data bytes,
Reply from 101.101.101.101: bytes=56 Sequence=1 ttl=255 time=9 ms
Reply from 101.101.101.101: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 101.101.101.101: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 101.101.101.101: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 101.101.101.101: bytes=56 Sequence=5 ttl=254 time=1 ms

--- 101.101.101.101 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/9 ms

Step4 Configuring and Testing the Telnet/SSH Service (AAA Authentication)

Enable and configure telnet service in the AC, add account huawei for AAA authentication.

Choose Maintenance > AC Maintenance > System > Service Management. Enable Telnet.

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

AC Maintenance File Management Service Management System Time

Basic AC Restart AC Upgrade Patch License Signature DB Log Alarm & Event Administrator System Electronic Label SNMP

You can add the trusted host through this page. Only the trusted host can access the specified service such as HTTP and HTTPS.

FTP : OFF

Telnet : ON

STelnet : ON

SFTP : OFF

Web server timeout interval (min) : 10

Apply

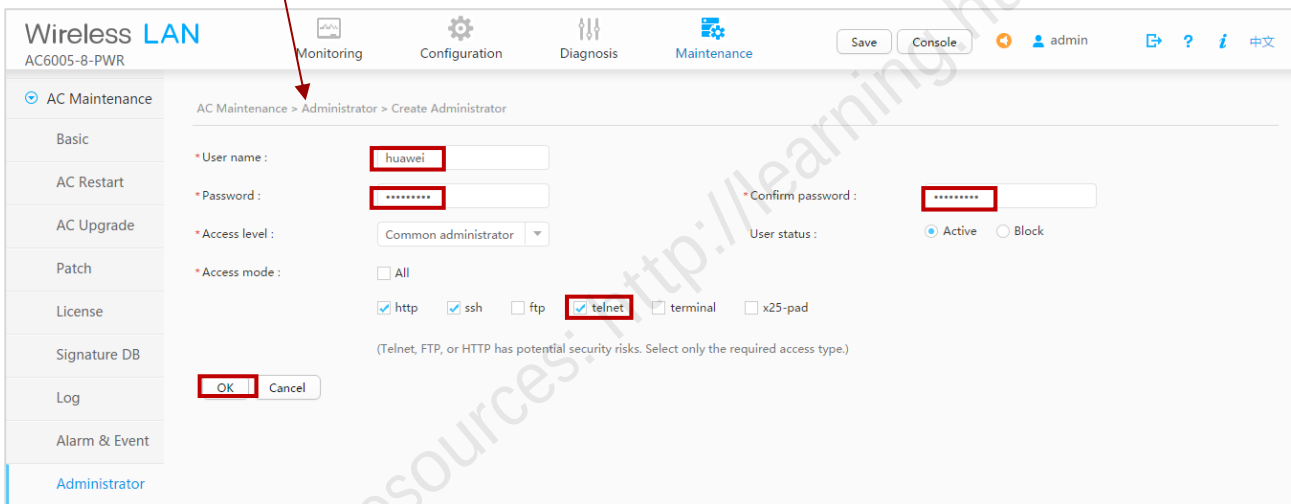
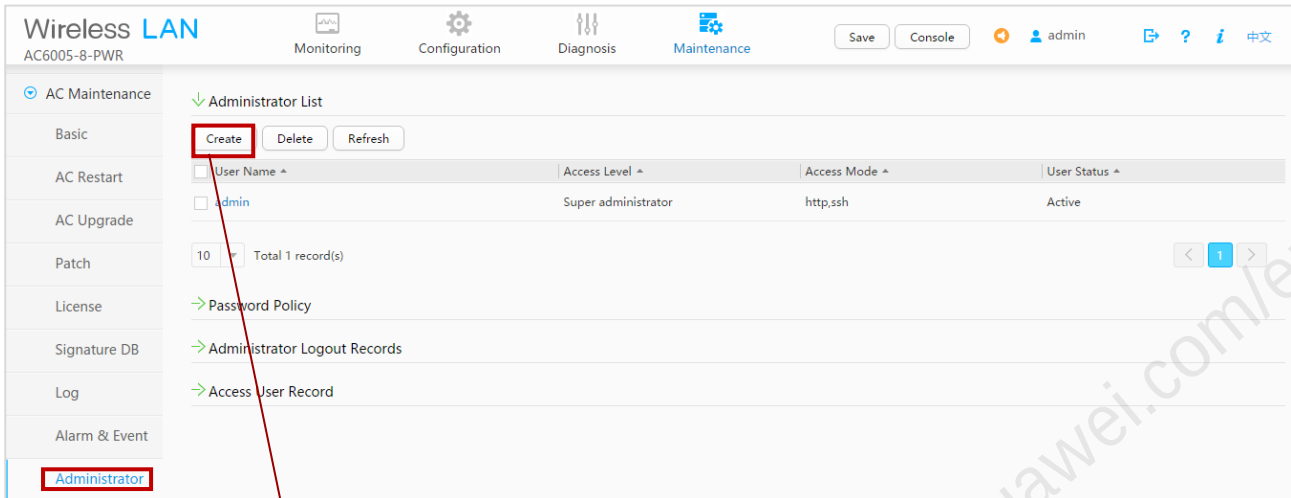
Trusted Host

Create Delete Refresh

IP Address Service Type Description

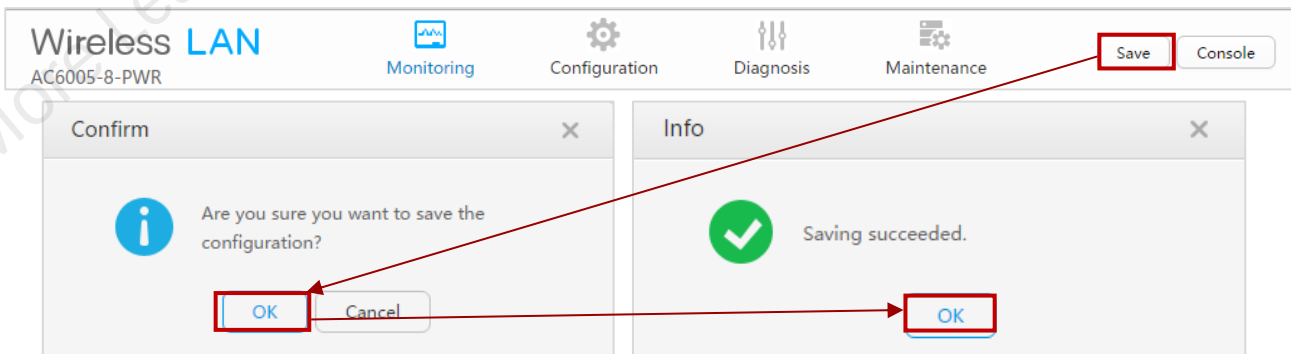
No data.

Choose **Maintenance > AC Maintenance > Administrator**. The **Administrator** page is displayed.
Create an administrator account: username huawei, password Admin@123.



Step5 Save the Configuration

Any change through web-based configuration, you need to click "save" to save the configuration to the device. If you don't save it, the configuration will lost after rebooted.
Save the configuration through the upper right of the page.



1.3 Verification

1.3.1 Telnet AC

After Configure telnet, test the telnet service on S5700.

```
<S5700>telnet 10.1.10.100
```

```
Trying 10.1.10.100 ...
```

```
Press CTRL+K to abort
```

```
Connected to 10.1.10.100 ...
```

```
Warning: Telnet is not a secure protocol, and it is recommended to use  
Stelnet.
```

```
Login authentication
```

```
Username:huawei
```

```
Password:
```

```
-----  
-----
```

```
User last login information:
```

```
-----  
-----
```

```
Access Type: Telnet
```

```
IP-Address : 10.1.10.1
```

```
Time : 2016-11-18 19:54:01+08:00
```

```
-----  
-----
```

```
<AC1>
```

```
Login AC successfully.
```

1.4 Reference Configuration

1.4.1 S5700 Configuration

```
#  
sysname S5700  
#  
vlan batch 10 to 13  
#  
lldp enable  
#  
undo http server enable  
undo http secure-server enable  
#  
undo nap slave enable
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@@@5d~9:M^ipCfL\iB)EQd>3Uwe%@@@
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
 ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
 ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
 ip address 10.1.13.1 255.255.255.0
#
interface MEth0/0/1
 ip address 172.21.11.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 10
```

```
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
interface LoopBack1
 ip address 101.101.101.101 255.255.255.255
#
user-interface con 0
 authentication-mode password
 set authentication password
 cipher %@@@;|J%=/[d[O@L[qD[Xhh~,3[~S{Zs:\Ot8H6*x_MAW=N$3[B,%@@@
user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password
 cipher %@@@`KL`QN[h79h[6AS2ggdT<+Hjaz5lH\hpS4]~^/-CFvtO+Hm<%@@@
 protocol inbound all
user-interface vty 16 20
#
return
```

1.4.2 AC Configuration

```
<AC1>display current-configuration
#
 sysname AC1
#
 http secure-server ssl-policy default_policy
```

```
http server enable
#
undo portal url-encode enable
#
ssl renegotiation-rate 1
#
vlan batch 10 to 13 4090
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name macportal_authen_profile
#
lldp enable
#
diffserv domain default
#
radius-server template default
#
pki realm default
    rsa local-key-pair default
    enrollment self-signed
#
ssl policy default_policy type server
pki-realm default
version tls1.0 tls1.1
ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
    encryption-algorithm aes-256
    dh group2
    authentication-algorithm sha2-256
    authentication-method pre-share
    integrity-algorithm hmac-sha2-256
    prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
aaa
    authentication-scheme default
    authentication-scheme radius
        authentication-mode radius
    authorization-scheme default
    accounting-scheme default
    domain default
        authentication-scheme default
    domain default_admin
        authentication-scheme default
    local-user admin password irreversible-cipher $1a$VNcE$6oR"2$aASkVyC1-
    ~~qx^~!e+:.S|>BJto>%VV[WvDxK./G$
    local-user admin privilege level 15
    local-user admin service-type ssh http
```

```
local-user huawei password irreversible-cipher
$1a$6@(!=HT_IP$A=lvP*~iu+0<..Y&4`Y6+j4$Xkcf=#aMU=5[4wEP$
local-user huawei privilege level 1
local-user huawei service-type telnet ssh http
#
interface Vlanif1
ip address 169.254.1.1 255.255.0.0
#
interface Vlanif10
ip address 10.1.10.100 255.255.255.0
#
interface Vlanif11
ip address 10.1.11.100 255.255.255.0
#
interface Vlanif12
ip address 10.1.12.100 255.255.255.0
#
interface Vlanif13
ip address 10.1.13.100 255.255.255.0
#
interface Vlanif4090
ip address 172.21.11.3 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
port link-type access
port default vlan 4090
stp disable
#
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
snmp-agent local-engineid 800007DB03845B12566919
snmp-agent community
read %^%#En_g+AWfX>adWz&5.!G~E^)^4&/r]vCSCEB~w~u%Zje-
$@`GH0BN7e"$A8PF(_n~lC9qvT)O*{4!I+:yR%^%#
snmp-agent community write %^%#atYiX7&TjG<o\Y/.2Y-
V/8bVI&sGJOTB4$0Y@{"2$306$`dp;=7cULM)*$.3Q!lXY<}!y7jZ,7BS"NNY%^%#
snmp-agent sys-info version v2c
snmp-agent
#
```

```
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh server secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh client secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh client key-exchange dh_group14_sha1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
user-interface con 0
authentication-mode password
set authentication password
cipher %^%#1<n6!"VC7VQQj=/vGNXG}:Eu&6zT3'C<qU9G'>N8A~"fK_+WA~0De+C]/yW"%^
%#
user-interface vty 0 4
authentication-mode aaa
user privilege level 3
protocol inbound telnet
user-interface vty 16 20
protocol inbound all
#
wlan
traffic-profile name default
security-profile name default
security-profile name default-wds
security wpa2 psk pass-phrase %^%#CB&>,Q$BB>x\Fn"|^%qToSj.2]:%J"+-
qK%aTJ_0%^%# aes
security-profile name default-mesh
security wpa2 psk pass-phrase %^%#]7|J" `LHnEQ=-,
GJS[q&>M">Qsqw;9mb8$0`_=6I%^%# aes
ssid-profile name default
vap-profile name default
mesh-handover-profile name default
mesh-profile name default
wds-profile name default
regulatory-domain-profile name default
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
provision-ap
#
dot1x-access-profile name dot1x_access_profile
#
```



```
mac-access-profile name mac_access_profile
#
undo ntp-service enable
#
return
```

More Learning Resources: <http://learning.huawei.com/en>

2

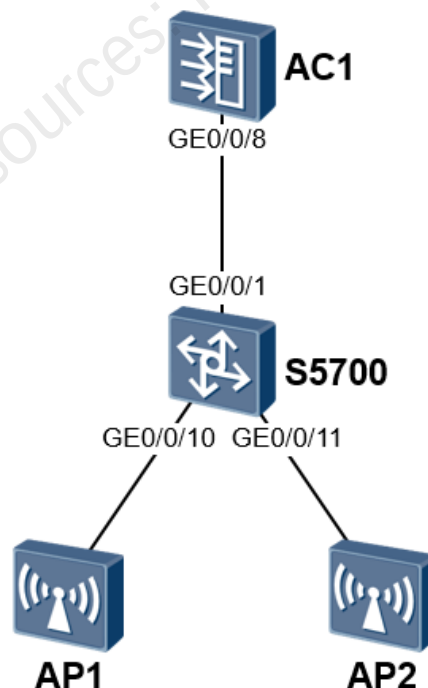
Experiment 2: AP Authentication and WLAN Configuration Roadmap

2.1 About This Course

2.1.1 Objectives

- Configure AP authentication
- Understand WLAN configuration profile
- Understand WLAN configuration roadmap
- Configure open system authentication

2.1.2 Topology



2.1.3 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

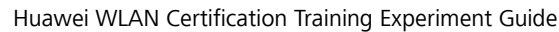
The following table describes device connections.

Group No.	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	- AP1-G0/0/10 - AP2-G0/0/11
2	AC2—G0/0/2	- AP3-G0/0/12 - AP4-G0/0/13
3	AC3—G0/0/3	- AP5-G0/0/14 - AP6-G0/0/15
4	AC4—G0/0/4	- AP7-G0/0/15 - AP8-G0/0/16
5	AC5—G0/0/5	- AP9-G0/0/17 - AP10-G0/0/18
6	AC6—G0/0/6	- AP11-G0/0/19 - AP12-G0/0/20

The following table describes an AC parameter configuration template.

AC Information	Country code: CN
	WLAN source: VLAN X0
AP Authentication	AP authentication mode: mac-auth
	AP MAC address
AP Group	Name: ap-groupX VAP ID 1: VAP profile: guestX regulatory domain profile: domainX VAP ID 2: VAP profile: voiceX regulatory domain profile: domainX VAP ID 3: VAP profile: employeeX regulatory domain profile: domainX
SSID Profile	Name: employeeX SSID Profile: employeeX
	Name: voiceX SSID Profile: voiceX

	Name: guestX SSID Profile: guestX
VAP Profile	Name: employeeX Forwarding mode: direct forwarding Service VLAN: 11 Referenced profile: SSID profile employeeX Name: voiceX Forwarding mode: direct forwarding Service VLAN: 12 Referenced profile: SSID profile voiceX Name: guestX Forwarding mode: tunnel forwarding Service VLAN: 13 Referenced profile: SSID profile guestX
Topology: layer2 and layer 3 bypass topology	



2.2.1 Configuration Procedure

```
graph TD
    Root[Configure AC management on fit APs] --> S1[1. Configure the access switch.]
    Root --> S2[2. Create an AP group.]
    Root --> S3[3. Configure the AP going online.]
    Root --> S4_5[4/5. Configure WLAN service parameters.]
    
    S1 --> T1[Enable layer 2 or layer 3 interconnection between the AP and AC.]
    S2 --> T2[Create an AP group.]
    S3 --> T3[Configure the DHCP server function of the AC. Create a regulatory domain profile. Configure the country code of the AC. Configure the authentication mode for the AP. Configure the AC source port (for establishing a tunnel with the AP).]
    S4_5 --> D1
    
    subgraph D1 [ ]
        direction TB
        S4_5_1[Configure the security profile.]
        S4_5_2[Configure the SSID profile.]
        S4_5_1 -- "Being referred to" --> S4_5_3[Configure the VAP profile.]
    end
    
    D1 --> T4[4. Configure the VAP profile.]
    
    T4 --> D2
    
    subgraph D2 [ ]
        direction TB
        S4_5_4[Bind the regulatory domain profile and VAP profile to the AP group.]
    end
    
    D2 --> T5[5. Bind the profile to the AP group.]
```

Configure AC management on fit APs.

1. Configure the access switch.
 - Enable layer 2 or layer 3 interconnection between the AP and AC.
2. Create an AP group.
 - Create an AP group.
3. Configure the AP going online.
 - Configure the DHCP server function of the AC. Create a regulatory domain profile. Configure the country code of the AC. Configure the authentication mode for the AP. Configure the AC source port (for establishing a tunnel with the AP).
- 4/5. Configure WLAN service parameters.
 - Configure the security profile. Configure the SSID profile. (Being referred to)
 - Configure the VAP profile. (4. Configure the VAP profile.)
 - Bind the regulatory domain profile and VAP profile to the AP group. (5. Bind the profile to the AP group.)

Continue the configuration from experiment 1, the configuration of the switch has been ready.

Continue the configuration from experiment 1, the configuration of the switch has been ready.

Choose Configuration > AP Config > AP Group > AP Group, The AP Group page is displayed. Click Create. Create ap-groupX.

The top screenshot shows the 'Wireless LAN' management interface for device AC6005-8-PWR. The 'AP Group' tab is selected, and the 'Create' button is highlighted with a red box. A red arrow points from this button to the bottom screenshot. The bottom screenshot shows the 'Create AP Group' dialog box. The 'AP group name' field is highlighted with a red box and contains the text 'ap-group1'. The 'OK' button is also highlighted with a red box.

Step5 Configuring AP Online Parameters

Enable DHCP server.

Click Configuration > AC Config > IP > DHCP Address Pool. set DHCP status to ON to enable the DHCP function, and click Create to create a DHCP address pool.

The screenshot shows the 'Wireless LAN' management interface for device AC6005-8-PWR. The 'DHCP Address Pool' tab is selected. The 'DHCP status' is set to 'ON' (highlighted with a red box). The 'Create' button is highlighted with a red box. The 'IP' tab is highlighted with a red box.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ?

Fast Config AC Config Basic Config VLAN Interface IP

AC Config > IP > DHCP Address Pool > Create DHCP Address Pool

*Address pool type : ☒ Global address pool ☐ Interface address pool

*Address pool name : ap

*Subnet address : 10 . 1 . 10 . 0 Subnet mask : 24(255.255.255.0)

Vendor-defined : sub-option

3 ascii 10.1.10.100

Advanced

Click Advanced, configure the gateway, the address pool interface.

Advanced

Lease : 1 Day 0 Hour 0 Minute

(The default value is 1 day; the maximum value is 999 days, 23 hours, and 59 minutes; the value 0 indicates t

Primary DNS server : Secondary DNS server :

Primary WINS server : Secondary WINS server :

DNS domain name :

Gateway IP : 10 . 1 . 10 . 1 (Maximum of 8 IP addresses)

Address pool interface : Vlanif10

Address Pool Interface

Vlanif10

Statically bound IP/MAC : /

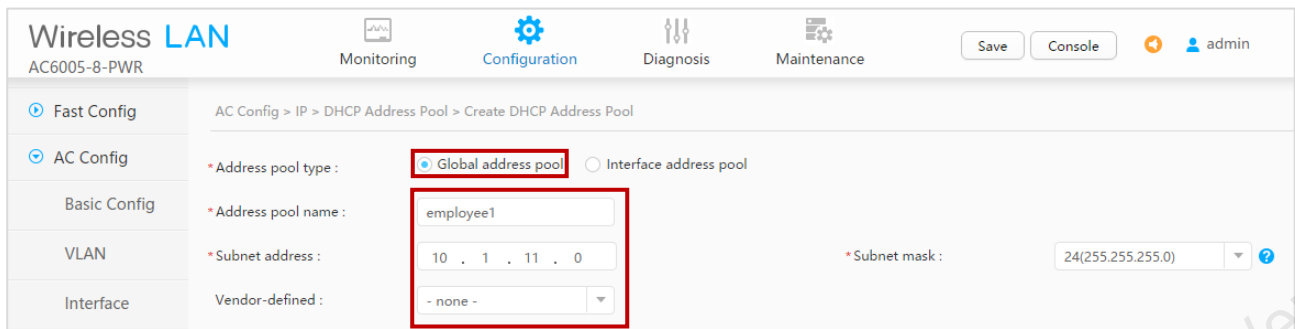
Statically Bound IP/MAC

No data.

NetBIOS type : Not specified

OK Cancel

Configure the subnet address for address pool employeeX.



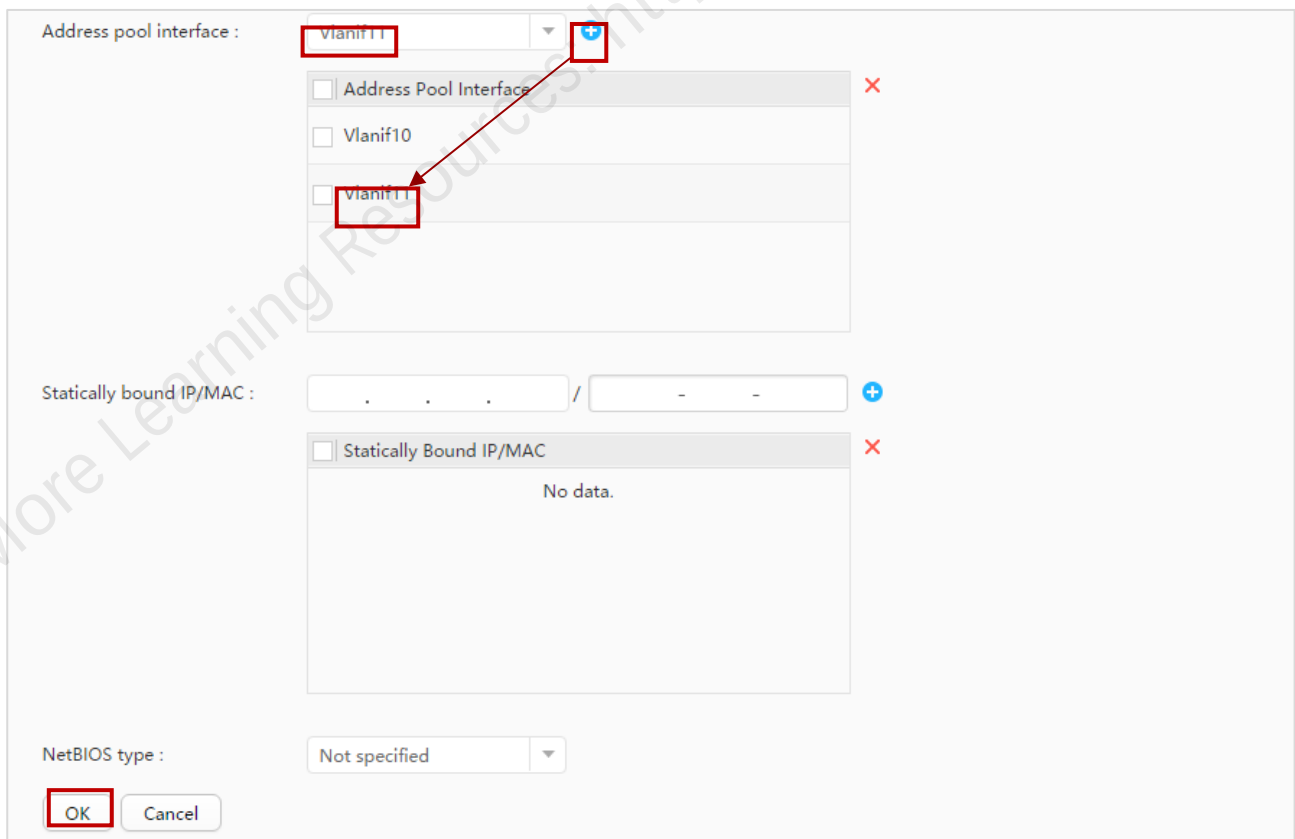
The screenshot shows the 'Wireless LAN' configuration page for 'AC6005-8-PWR'. The 'AC Config' tab is selected, and the 'DHCP Address Pool' configuration is shown. The 'Global address pool' radio button is selected. The 'Address pool name' is 'employee1'. The 'Subnet address' is '10.1.11.0' and the 'Subnet mask' is '24(255.255.255.0)'. The 'Vendor-defined' dropdown is set to '- none -'.

Configure the gateway IP address for address pool employeeX.



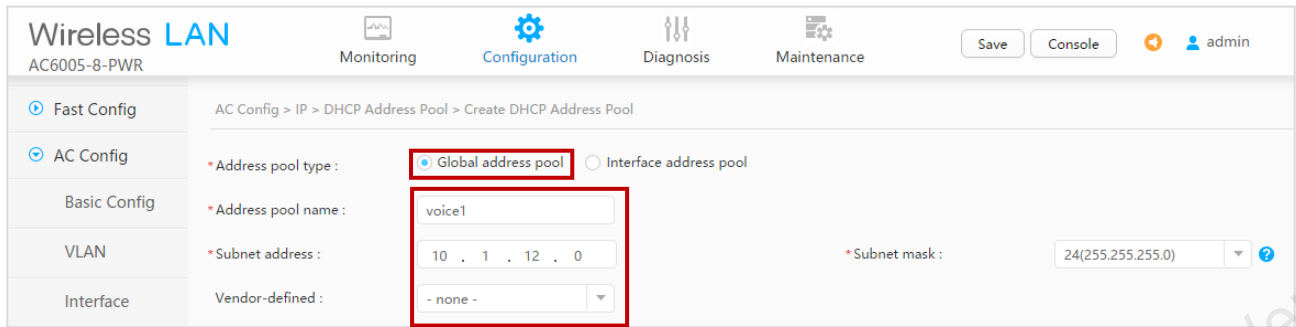
The screenshot shows the 'Gateway IP' configuration section. The 'Gateway IP' field is set to '10.1.11.1'. A red box highlights the '10.1.11.1' field and the '+' button next to it. Below the field, there is a table with a checkbox and the IP address '10.1.11.1'.

Configure the interface for address pool employeeX.



The screenshot shows the 'Address pool interface' configuration section. The 'Address pool interface' dropdown is set to 'Vlanif11'. A red box highlights the 'Vlanif11' dropdown and the '+' button next to it. Below the dropdown, there is a table with a checkbox and the interface name 'Vlanif11'. The 'Statically bound IP/MAC' section is empty, showing 'No data.' The 'NetBIOS type' dropdown is set to 'Not specified'. The 'OK' button is highlighted with a red box.

Configure the subnet address for address pool voiceX.



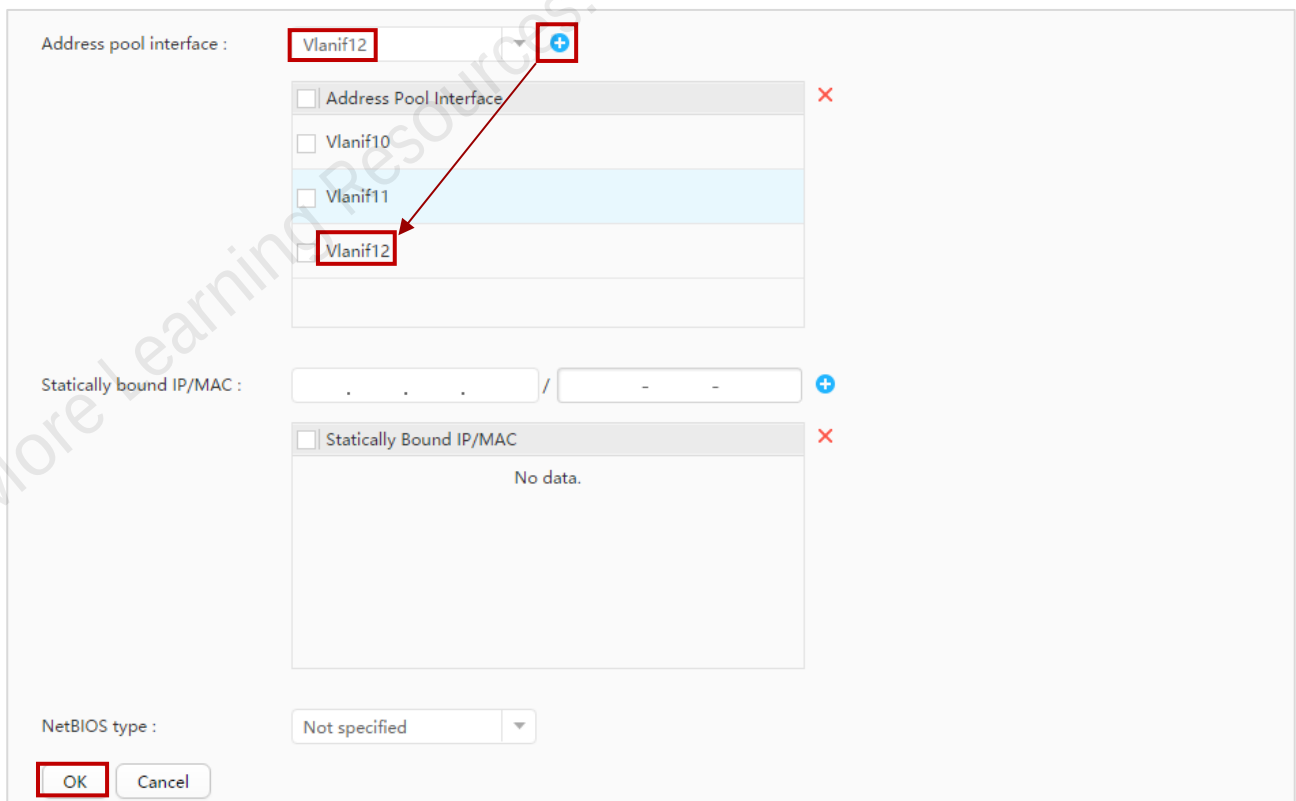
The screenshot shows the 'Wireless LAN' configuration page for 'AC6005-8-PWR'. The 'AC Config' tab is selected, and the 'DHCP Address Pool' configuration is shown. The 'Global address pool' radio button is selected. The 'Address pool name' is 'voice1'. The 'Subnet address' is '10.1.12.0' and the 'Subnet mask' is '24(255.255.255.0)'. The 'Vendor-defined' dropdown is set to '- none -'.

Configure the gateway IP address for address pool voiceX.



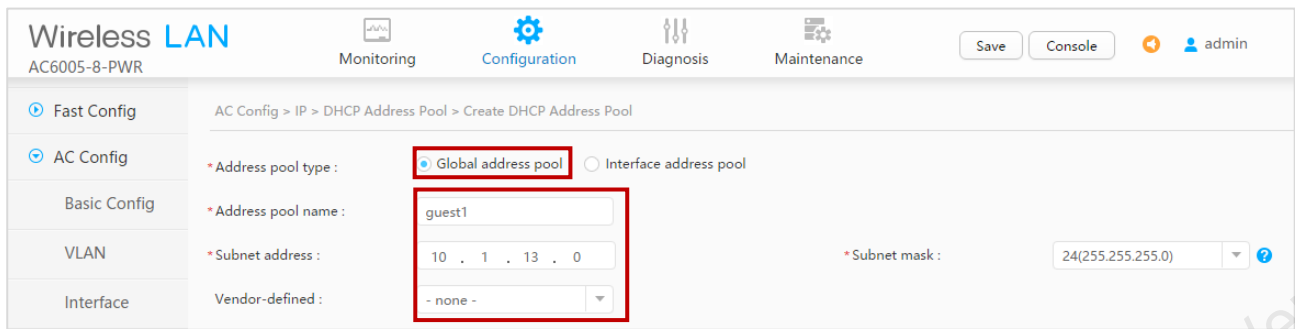
The screenshot shows the 'Gateway IP' configuration for the 'voice1' address pool. The 'Gateway IP' field is set to '10.1.12.1'. A list of 'Gateway IP' addresses is shown below, with '10.1.12.1' selected. The 'Maximum of 8 IP addresses' limit is indicated.

Configure the interface for address pool voiceX.



The screenshot shows the 'Address pool interface' configuration for the 'voice1' address pool. The 'Address pool interface' dropdown is set to 'Vlanif12'. A list of 'Address Pool Interface' options is shown below, with 'Vlanif12' selected. The 'Statically bound IP/MAC' field is empty. The 'NetBIOS type' is set to 'Not specified'. The 'OK' button is highlighted.

Configure the subnet address for address pool guestX.



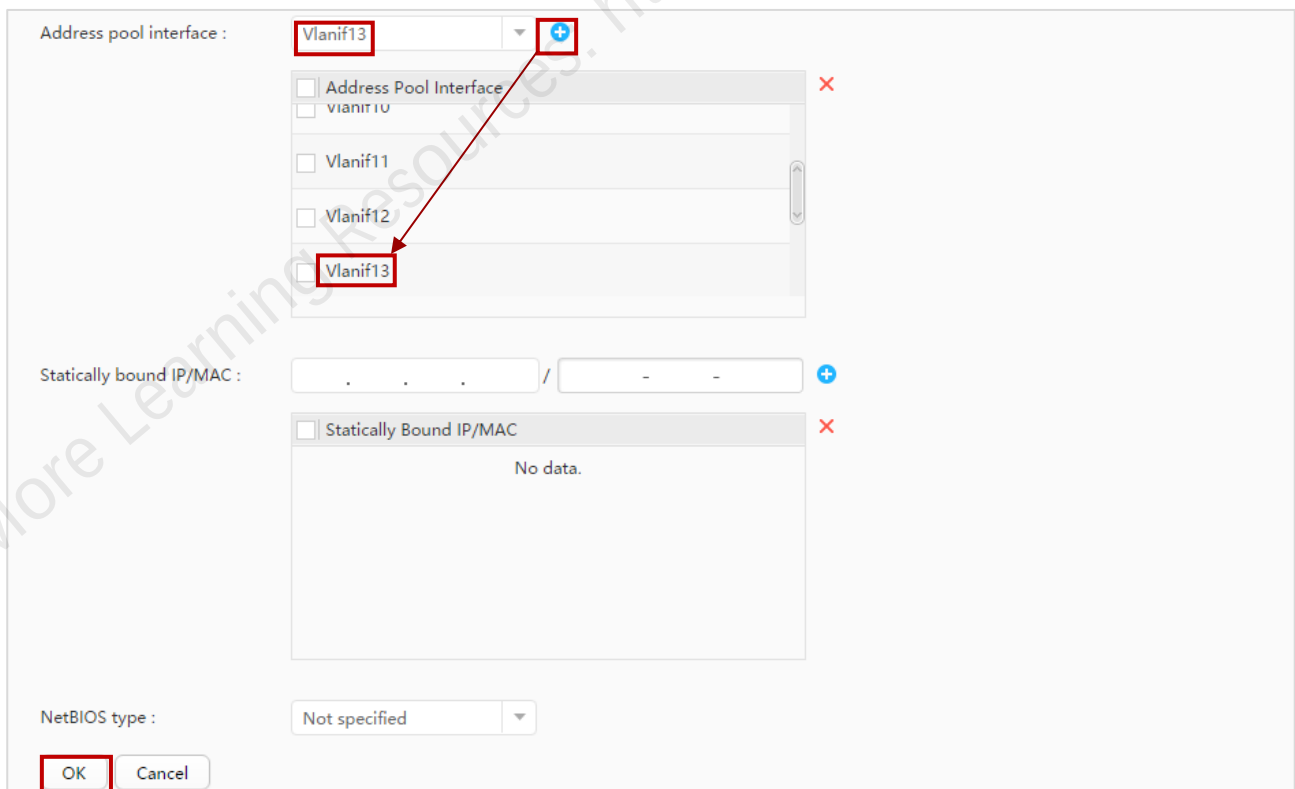
The screenshot shows the 'Wireless LAN' configuration page for 'AC6005-8-PWR'. The 'AC Config' tab is selected, and the 'Fast Config' section is expanded. The 'AC Config' sub-tab is active, showing the 'Create DHCP Address Pool' configuration. The 'Address pool type' is set to 'Global address pool'. The 'Address pool name' is 'guest1'. The 'Subnet address' is '10.1.13.0' and the 'Subnet mask' is '24(255.255.255.0)'. The 'Vendor-defined' dropdown is set to '- none -'.

Configure the gateway IP address for address pool guestX.



The screenshot shows the 'Gateway IP' configuration section. The 'Gateway IP' field is set to '10.1.13.1'. A red box highlights the '10.1.13.1' field and a '+' button next to it. Below the field, there is a list of 'Gateway IP' addresses, with '10.1.13.1' selected. A red arrow points from the '+' button to the '10.1.13.1' entry in the list.

Configure the interface for address pool guestX.



The screenshot shows the 'Address pool interface' configuration section. The 'Address pool interface' dropdown is set to 'Vlanif13'. A red box highlights the 'Vlanif13' dropdown and a '+' button next to it. Below the dropdown, there is a list of 'Address Pool Interface' options, with 'Vlanif13' selected. A red arrow points from the '+' button to the 'Vlanif13' entry in the list. The 'Statically bound IP/MAC' section is empty, showing 'No data.' The 'NetBIOS type' is set to 'Not specified'. The 'OK' button is highlighted with a red box.

Check the IP address pool.

DHCP Address Pool

DHCP Relay

NAT

Route

DHCP status : ON

Address Pool List

Create

Delete

Display Address Pool

Refresh

☐	Address Pool Name ^	Subnet Address ^	Subnet Mask ^	Gateway IP ^
☐	ap	10.1.10.0	255.255.255.0	<10.1.10.1>
☐	employee1	10.1.11.0	255.255.255.0	<10.1.11.1>
☐	voice1	10.1.12.0	255.255.255.0	<10.1.12.1>
☐	guest1	10.1.13.0	255.255.255.0	<10.1.13.1>

Create a regulatory domain profile.

Click Configuration > AP Config > Profile > Radio Management > Regulatory Domain Profile. Click Create on the right pane.

Wireless LAN

AC6005-8-PWR

Monitoring

Configuration

Diagnosis

Maintenance

Save

Console

Fast Config

AC Config

AP Config

AP Group

AP Config

Profile

Security

Other Services

Backup Settings

Profile Management

Wireless Service

Radio Management

Regulatory Domain Profile

RRM Profile

Air Scan Profile

2G Radio Profile

5G Radio Profile

AP

Mesh

WDS

WIDS

WLAN Location

Bluetooth Location

IoT

Regulatory Domain Profile List

Create

Delete

Clear

Display Reference

Regulatory Domain Profile Name

default

10

Total 1 record(s)

Create Regulatory Domain Profile

* Profile name :

domain1

Copy parameters from other profiles :

- none -

OK

Cancel

Regulatory Domain Profile : domain1 Display Reference

Country code : CHINA

[→ 2.4 GHz DCA Channel Set](#)

[→ 5 GHz DCA Channel Set](#)

Apply

Configure the AC source address and AP authentication mode.

AP authentication has three modes. By default, MAC authentication is used. Manually add APs based on MAC addresses.

Click Configuration > AC Config > Basic Config > AC Configuration, select VLANIF for AC source address, click ..., and set the AC source address to VLANIF801. Click Apply.

Wireless LAN
AC6005-8-PWR

Monitoring
Configuration
Diagnosis
Maintenance

Fast Config
AC Config
Basic Config
VLAN
Interface
IP
AP Config
Security

AC Configuration
Radio Calibration

AC source address : VLANIF LoopBack IP address

Vlanif10 ... ×

AP data buffer : OFF

AP authentication mode : MAC address authentic Add AP

IPv6 services for STAs : OFF

Advanced ⌵

Apply

Import the AP offline to the AC and add two APs to AP group ap-groupX. Name the two APs AP1 and AP2.

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

Fast Config AC Config AP Config

AP Group AP Info AP Whitelist AP Blacklist

AP List

Click the AP ID to access the AP Customized Settings page.

Deploy Create Replace Delete Add to Blacklist Refresh

AP ID AP MAC AP Name Gro... IP Address Type Version Serial Number STA... Login Period Status

No data.

Non-authorized AP List

Add to MAC Whitelist Add to SN Whitelist Add to Blacklist Refresh

Time

Time	Type	MAC Address	Serial Number	IP Address
2017-04-10 11:50:02	AP4030DN	4cfa-caae-b0c0	21500826412SG8914026	10.1.10.253
2017-04-10 11:49:59	AP4030DN	4cfa-cabf-d560	21500826412SG8919938	10.1.10.254

10 Total 2 record(s)

Add AP1

AP Config > AP Config > AP Info > Create AP

* Creation mode : ☒ Manually add ☐ Batch import

* Keyword : ☒ AP MAC ☐ AP SN

* AP MAC : 4cfa - cabf - d560 AP ID : 0 AP type : AP4030DN

OK Cancel

Add AP2

AP Config > AP Config > AP Info > Create AP

* Creation mode : ☒ Manually add ☐ Batch import

* Keyword : ☒ AP MAC ☐ AP SN

* AP MAC : 4cfa - caae - b0c0 AP ID : 1 AP type : AP4030DN

OK Cancel

After we add the AP to the MAC address authentication list, the status of the AP will change from fault to config and final to the normal status, we need to wait for several minutes, if the status could not change to normal status, pls re-check your configuration.

AP Info AP Whitelist AP Blacklist										
↓ AP List										
Click the AP ID to access the AP Customized Settings page.										
Deploy Create Replace Delete Add to Blacklist Refresh										
AP ID										
AP ID	AP MAC	AP Name	Gro...	IP Address	Type	Version	Serial Number	STA...	Login Period	Status
0	4cfa-cabf-d560	ap2	defa...	10.1.10.254	AP4030DN	V200R007C10S...	21500826412S...	0	1H:56M:35S	normal
1	4cfa-caae-b0c0	ap1	defa...	10.1.10.253	AP4030DN	V200R007C10S...	21500826412S...	0	1H:42M:55S	normal

Group online APs. Select two APs, and click Deploy.

Wireless LAN AC6005-8-PWR										
Monitoring Configuration Diagnosis Maintenance										
Fast Config AC Config AP Config AP Group AP Config Profile										
AP Info AP Whitelist AP Blacklist										
↓ AP List										
Click the AP ID to access the AP Customized Settings page.										
Deploy Create Replace Delete Add to Blacklist Refresh										
AP ID	AP MAC	AP Name	Gro...	IP Address	Type					
☒ 0	4cfa-cabf-d560	ap2	defa...	10.1.10.254	AP4030DN					
☒ 1	4cfa-caae-b0c0	ap1	defa...	10.1.10.253	AP4030DN					

Add the two APs to AP group ap-groupX.

AP Config > AP Config > AP Info > Deploy AP

AP group :

ap-group1

AP mode :

- none -

Selected AP List

AP ID ▲	AP M...	AP Name	AP Gr... ▲	IP Obtaining Mode	IP Address	IP Address Mask	Gateway
0	4cfa-ca...	ap1	default	- none -	10.1.10.254	255.255.255.0	10.1.10.1
1	4cfa-ca...	ap2	default	- none -	10.1.10.253	255.255.255.0	10.1.10.1

10

Total 2 record(s)

OK

Cancel

View AP information.

AP信息

AP白名单

AP黑名单

↓AP列表

ⓘ

点击AP ID 即可进入AP的个性化配置页面。

部署

新建

替换

删除

加入黑名单

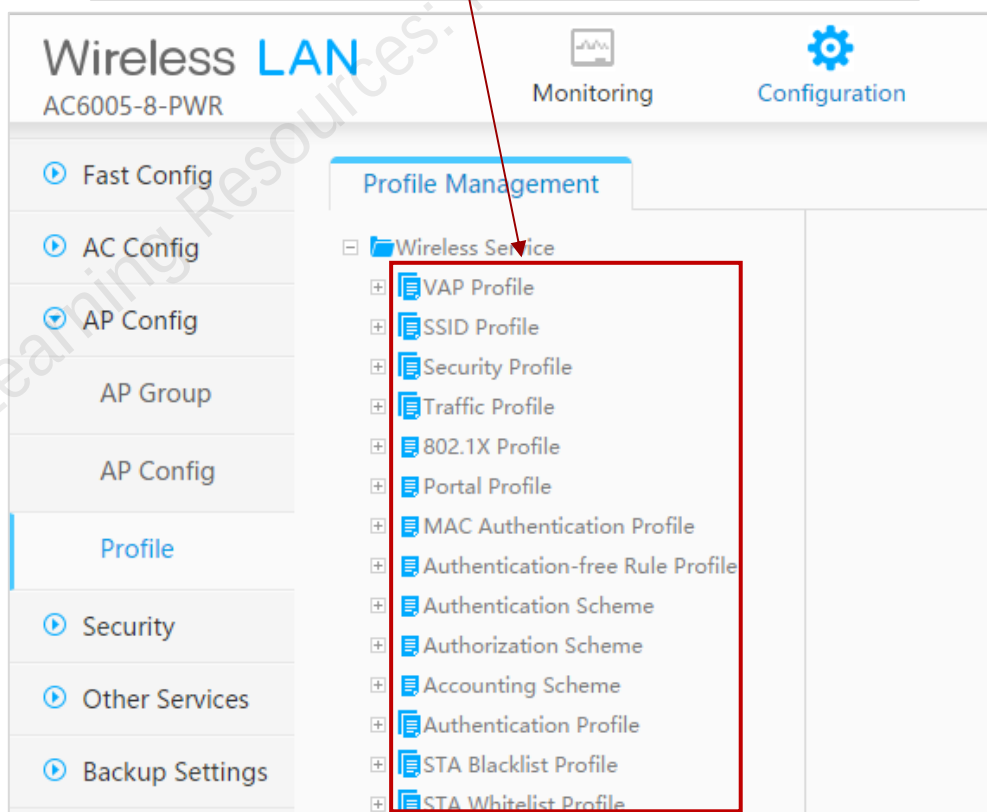
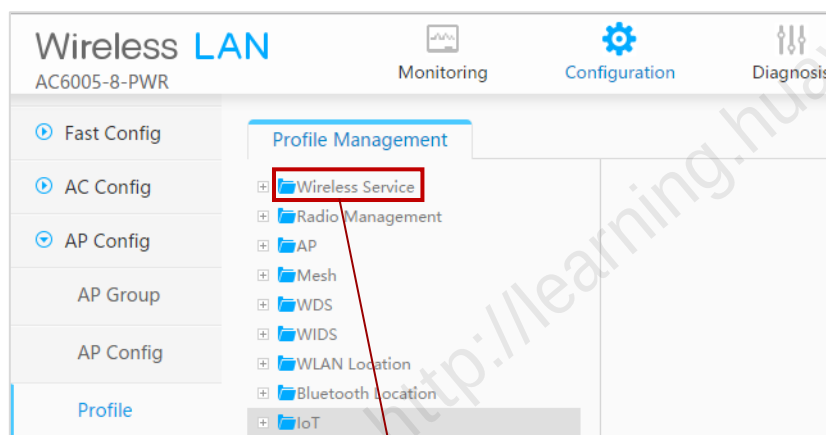
刷新

AP ID

☐ AP ID ^	AP MAC地址	AP名称 ^	组名... ^	IP地址	类型 ^	版本	序列号	终端数 ^	上线时长 ^	状态 ^
☐ 0	4cfa-cabe-eb60	ap1	ap-g...	10.1.10.254	AP4030DN	V200R007C10S...	21500826412S...	0	4M:43S	● normal
☐ 1	4cfa-cabf-d0c0	ap2	ap-g...	10.1.10.253	AP4030DN	V200R007C10S...	21500826412S...	0	4M:36S	● normal

Step6 Configuring WLAN Service Parameters

Choose Configuration > AP Config > Profile > Wireless Service, The wireless service configuration page is displayed.



Create an SSID profile.

Create the name is "employee", "voiceX" and "guestX" SSID profile, And the SSID name is "employee", "voiceX" and "guestX".

Profile Management

- Wireless Service
 - VAP Profile
 - SSID Profile**
 - Security Profile
 - Traffic Profile
 - 802.1X Profile
 - Portal Profile

SSID Profile List

Create
Delete
Clear
Display Reference

☐ SSID Profile Name

☐ default

Create SSID Profile

* Profile name :
Copy parameters from other profiles :
- none -

OK
Cancel

SSID Profile :
Display Reference

* SSID :
Association timeout (min) :

Maximum number of STAs :
Hide SSID after the maximum number of STAs is reached :
☒ ON

Disable non-HT terminal access :
☐ OFF

→ 802.11r

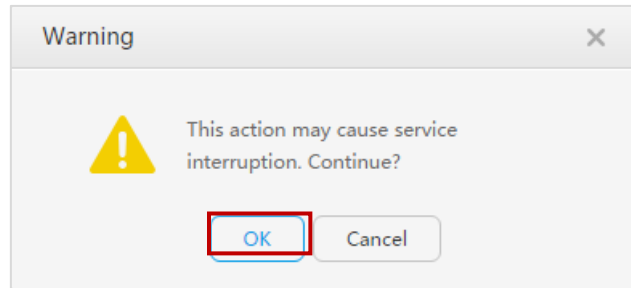
→ EDCA Parameters

→ Inbound CAR Parameters

→ Outbound CAR Parameters

→ Admin Frame Expense Optimization

→ Others



Create SSID Profile

* Profile name : Copy parameters from other profiles :

SSID Profile :

* SSID : Association timeout (min) :

Maximum number of STAs : Hide SSID after the maximum number of STAs is reached : ☒

Disable non-HT terminal access : ☐

→ 802.11r

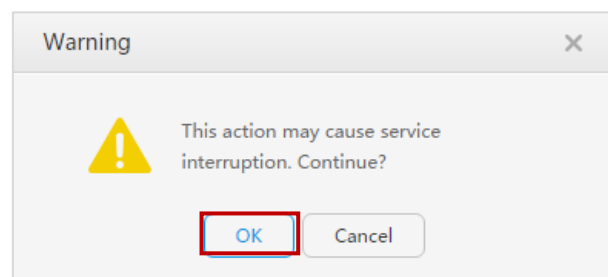
→ EDCA Parameters

→ Inbound CAR Parameters

→ Outbound CAR Parameters

→ Admin Frame Expense Optimization

→ Others



Create SSID Profile

* Profile name : Copy parameters from other profiles :

SSID Profile :

* SSID : Association timeout (min) :

Maximum number of STAs : Hide SSID after the maximum number of STAs is reached : ☒

Disable non-HT terminal access : ☐

→ 802.11r

→ EDCA Parameters

→ Inbound CAR Parameters

→ Outbound CAR Parameters

→ Admin Frame Expense Optimization

→ Others

Warning

 This action may cause service interruption. Continue?

Create "employee", "voiceX" and "guestX" VAP profile, configure "employee", "voice" forwarding mode to direct. "guestX" forwarding mode to tunnel, configure service VLAN.

Profile Management

- Wireless Service
 - VAP Profile**
 - default
 - SSID Profile
 - Security Profile
 - Traffic Profile
 - 802.1X Profile
 - Portal Profile
 - MAC Authentication Profile

VAP Profile List

☐ VAP Profile Name

☐ default

10 Total 1 record(s)

Create VAP Profile

* Profile name : Copy parameters from other profiles :

VAP Profile :

Status :	☒ ON	VAP type :	Service VAP
Service VLAN :	☒ Single VLAN ☐ VLAN Pool	Service VLAN ID :	11
Forwarding mode :	Direct	mDNS packets over tunnel :	☐ OFF
Band steering :	☒ ON	Roaming domain ID :	1
Home agent :	☐ AC ☒ AP	IP binding check :	☐ OFF
Layer 3 roaming :	☒ ON		
ARP probe :	☐ OFF		
IP learning :	☒ ON		
Strict IP learning :	☐ IPv4 ☐ IPv6		
DHCP trusted port :	☐ OFF	ND trusted port :	☐ OFF
Appending Option 82 :	☐ OFF		
Effective after logout :	☐ OFF		
Disable VAP periodically :	☐ OFF		
Broadcast flood attack detection :	☒ ON		
Broadcast attack threshold(pps) :	10	Adding attackers to the blacklist :	☐ OFF

Create VAP Profile

* Profile name : Copy parameters from other profiles :

VAP Profile :
voice1
Display Reference

Status :
ON

Service VLAN :
Single VLAN
VLAN Pool

Forwarding mode :
Direct

Band steering :
ON

Home agent :
AC
AP

Layer 3 roaming :
ON

ARP probe :
OFF

IP learning :
ON

Strict IP learning :
IPv4
IPv6

DHCP trusted port :
OFF

Appending Option 82 :
OFF

Effective after logout :
OFF

Disable VAP periodically :
OFF

Broadcast flood attack detection :
ON

Broadcast attack threshold(pps) :
10

Apply

VAP type :
Service VAP

Service VLAN ID :
12

mDNS packets over tunnel :
OFF

Roaming domain ID :
1

IP binding check :
OFF

ND trusted port :
OFF

Adding attackers to the blacklist :
OFF

Create VAP Profile

* Profile name :
guest1

Copy parameters from other profiles :
- none -

OK
Cancel

VAP Profile :

Status : ☒ ON

VAP type :

Service VLAN : ☒ Single VLAN ☐ VLAN Pool

Service VLAN ID :

Forwarding mode :

Band steering : ☒ ON

Home agent : ☐ AC ☒ AP

Roaming domain ID :

Layer 3 roaming : ☒ ON

ARP probe :

IP learning : ☒ ON

IP binding check :

Strict IP learning : ☐ IPv4 ☐ IPv6

ND trusted port :

DHCP trusted port :

Appending Option 82 :

Effective after logout :

Disable VAP periodically :

Broadcast flood attack detection : ☒ ON

Broadcast attack threshold(pps) :

Adding attackers to the blacklist :

Use the default forwarding mode (direct forwarding). Changing the forwarding mode will trigger risk notifications.

Confirm


Modifying forward mode may cause service interruption. Continue?

Bind the SSID profile to VAP profile.

Profile Management

Wireless Service

VAP Profile

guest1

voice1

default

employee1

SSID Profile [default]

Security Profile [default]

Traffic Profile [default]

Authentication Profile

STA Blacklist And Whitelist...

SAC Profile

UCC Profile

Hotspot2.0 Profile

Attack Defense Profile

SSID Profile

Security Profile

Traffic Profile

802.1X Profile

Portal Profile

* SSID Profile :

employee1

Display Reference

* SSID :

employee1

Association timeout (min) :

5

Maximum number of STAs :

64

Hide SSID after the maximum number of STAs is reached :

ON

Disable non-HT terminal access :

OFF

→ 802.11r

→ EDCA Parameters

→ Inbound CAR Parameters

→ Outbound CAR Parameters

→ Admin Frame Expense Optimization

→ Others

Apply

Profile Management

Wireless Service

VAP Profile

guest1

voice1

SSID Profile [default]

Security Profile [default]

Traffic Profile [default]

Authentication Profile

STA Blacklist And Whitelist...

SAC Profile

UCC Profile

Hotspot2.0 Profile

Attack Defense Profile

default

employee1

SSID Profile

Security Profile

Traffic Profile

802.1X Profile

Portal Profile

* SSID Profile :

voice1

Display Reference

* SSID :

voice1

Association timeout (min) :

5

Maximum number of STAs :

64

Hide SSID after the maximum number of STAs is reached :

ON

Disable non-HT terminal access :

OFF

→ 802.11r

→ EDCA Parameters

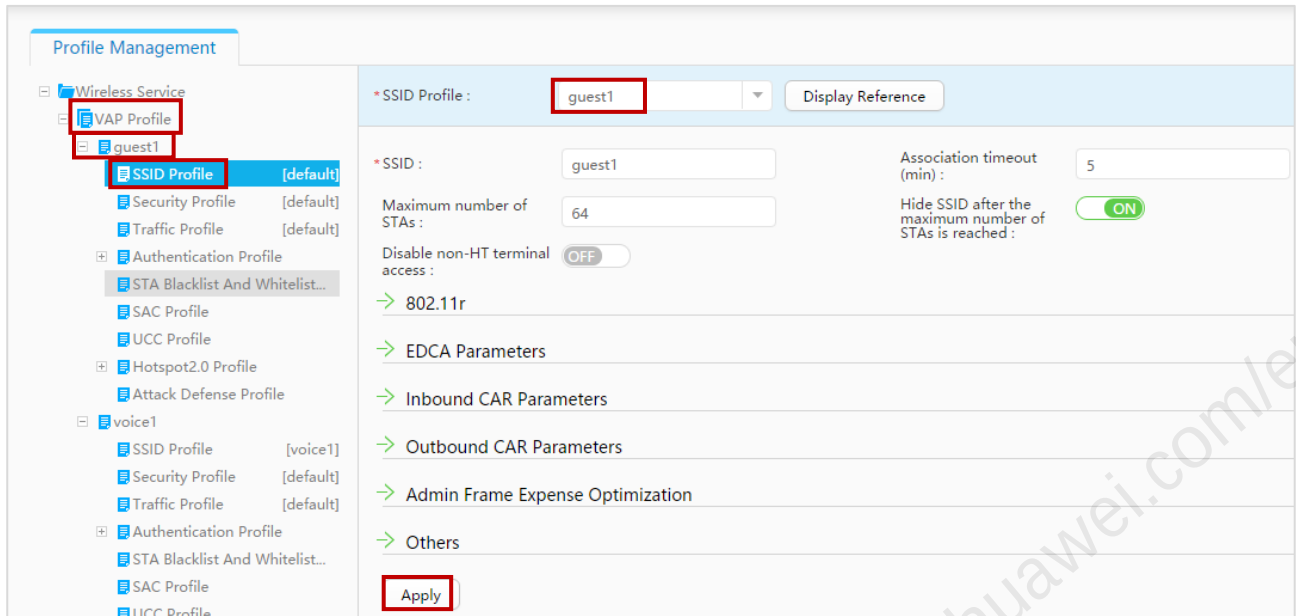
→ Inbound CAR Parameters

→ Outbound CAR Parameters

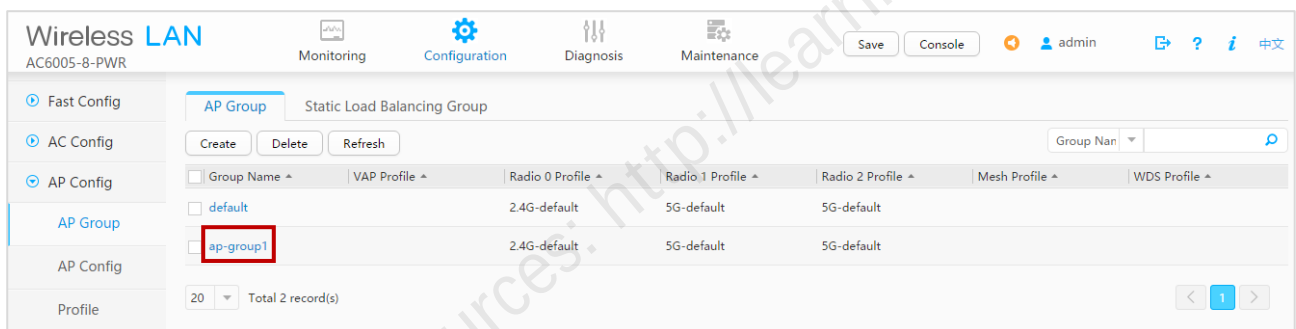
→ Admin Frame Expense Optimization

→ Others

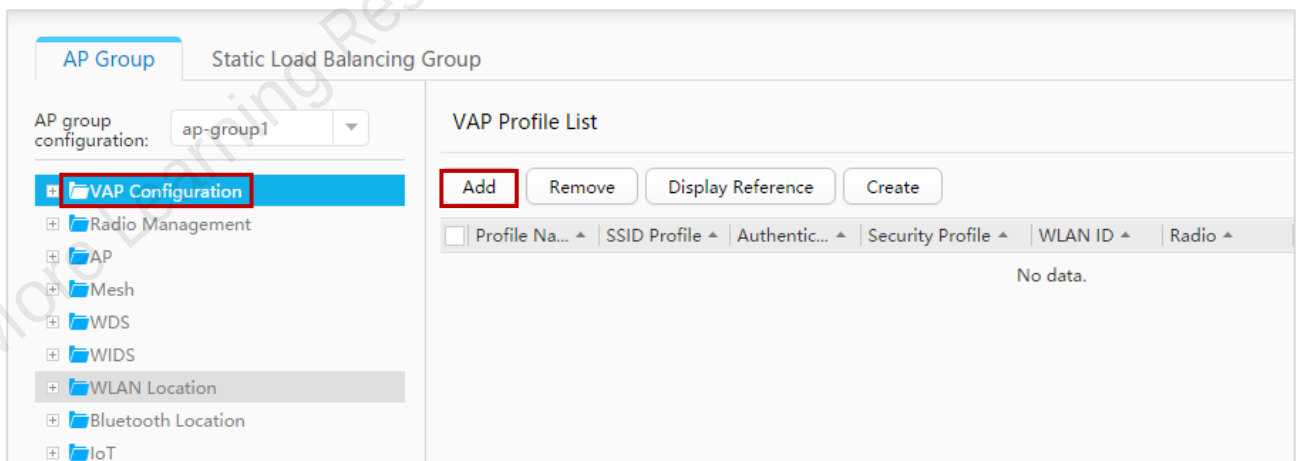
Apply



Bind regulatory domain profile and VAP profile to the AP group.
Choose configuration > AP configuration > AP group configuration , click ap-groupX.



Add VAP profile. Set WLAN ID and Radio.



Add VAP Profile

* VAP profile name : * WLAN ID :

* Radio :

Add VAP Profile

* VAP profile name : * WLAN ID :

* Radio :

Add VAP Profile

* VAP profile name : * WLAN ID :

* Radio :

Bind regulatory domain profile domainX to the AP group.

AP Group Static Load Balancing Group

AP group configuration:

* Regulatory Domain Profile :

Country code :

→ 2.4 GHz DCA Channel Set

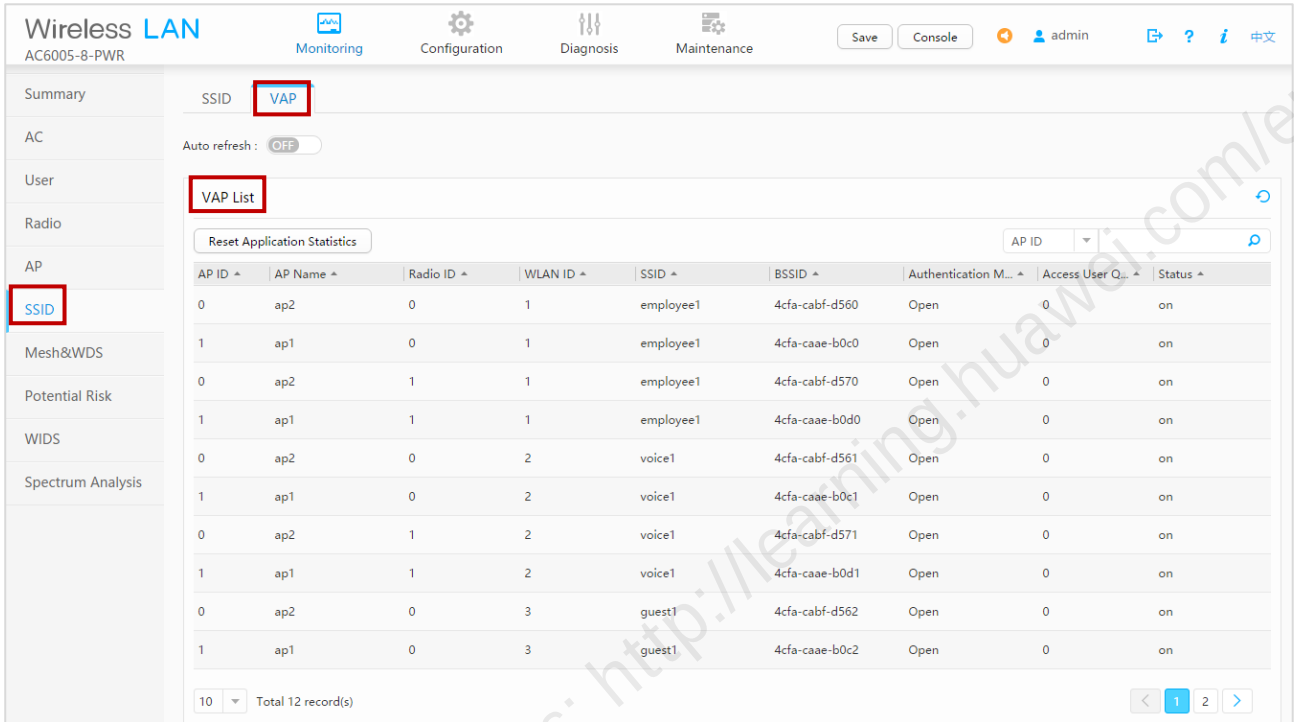
→ 5 GHz DCA Channel Set

Left sidebar menu items: VAP Configuration, Radio Management, Regulatory Domain..., Radio 0, Radio 1, Radio 2, AP, Mesh, WDS, WIDS, WLAN Location, Bluetooth Location, IoT

2.3 Verification

2.3.1 Checking the VAP List

Choose Monitoring > SSID > VAP > VAP List.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

Summary SSID **VAP**

AC Auto refresh: OFF

User **VAP List**

Radio

AP

SSID

Mesh&WDS

Potential Risk

WIDS

Spectrum Analysis

Reset Application Statistics

AP ID AP Name Radio ID WLAN ID SSID BSSID Authentication M... Access User Q... Status

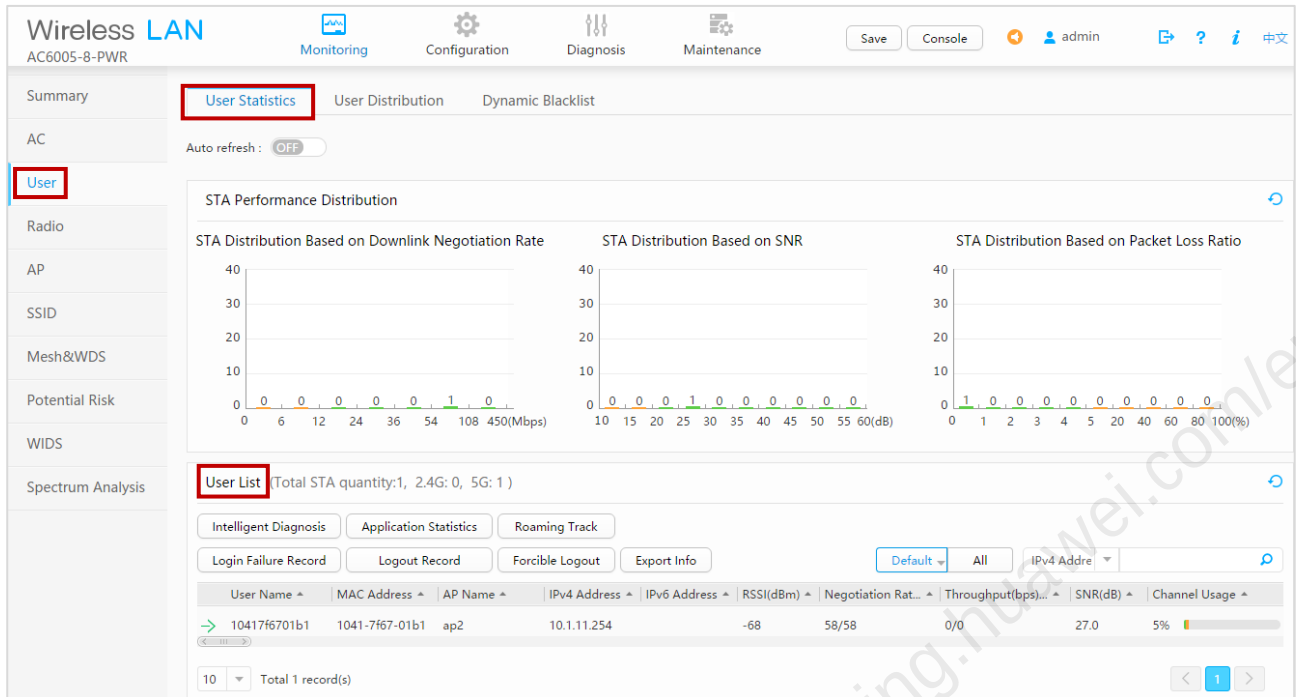
0	ap2	0	1	employee1	4cfa-cabf-d560	Open	0	on
1	ap1	0	1	employee1	4cfa-caae-b0c0	Open	0	on
0	ap2	1	1	employee1	4cfa-cabf-d570	Open	0	on
1	ap1	1	1	employee1	4cfa-caae-b0d0	Open	0	on
0	ap2	0	2	voice1	4cfa-cabf-d561	Open	0	on
1	ap1	0	2	voice1	4cfa-caae-b0c1	Open	0	on
0	ap2	1	2	voice1	4cfa-cabf-d571	Open	0	on
1	ap1	1	2	voice1	4cfa-caae-b0d1	Open	0	on
0	ap2	0	3	guest1	4cfa-cabf-d562	Open	0	on
1	ap1	0	3	guest1	4cfa-caae-b0c2	Open	0	on

10 Total 12 record(s)

2.3.2 Terminal Connection Test

Connect STAs to the WLANs with SSIDs employeeX, voiceX and guestX. Run the display station all commands on the AC.

Choose Monitoring > user > 用户统计, view user list.



On the wireless terminal, ping the IP address of the simulated public network interface on the switch.

```
C:\Users\zWX>ping 101.101.101.101
PING 101.101.101.101: 56 data bytes, press CTRL_C to break
    Reply from 101.101.101.101: bytes=56 Sequence=1 ttl=255 time=7 ms
    Reply from 101.101.101.101: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 101.101.101.101 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 7/9/10 ms
```

2.4 Reference Configuration

2.4.1 S5700 Configuration

```
#
sysname S5700
#
vlan batch 10 to 13
#
lldp enable
#
```

```
undo http server enable
undo http secure-server enable
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@%5d~9:M^ipCfL\iB)EQd>3Uwe%@@
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
 ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
 ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
 ip address 10.1.13.1 255.255.255.0
#
interface MEth0/0/1
 ip address 172.21.11.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 to 13
```

```
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
interface LoopBack1
 ip address 101.101.101.101 255.255.255.255
#
user-interface con 0
 authentication-mode password
 set authentication password
 cipher %@@@;|J%=/[d[O@L[qD[Xhh~,3[~S(Zs:\Ot8H6*x_MAW=N$3[B,%@@@
 user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password
 cipher %@@@`KL`QN[h79h[6AS2ggdT<+Hjaz5lH\hpS4]~^/-CFvtO+Hm<%@@@
 protocol inbound all
 user-interface vty 16 20
#
return
```

2.4.2 AC Configuration

```
#
```

```
sysname AC1
#
http secure-server ssl-policy default_policy
http server enable
#
undo portal url-encode enable
#
ssl renegotiation-rate 1
#
vlan batch 10 to 13 4090
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name macportal_authen_profile
#
lldp enable
#
dhcp enable
#
diffserv domain default
#
radius-server template default
#
pki realm default
  rsa local-key-pair default
  enrollment self-signed
#
ssl policy default_policy type server
pki-realm default
version tls1.0 tls1.1
ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
  encryption-algorithm aes-256
  dh group2
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
ip pool ap
  gateway-list 10.1.10.1
  network 10.1.10.0 mask 255.255.255.0
  option 43 sub-option 3 ascii 10.1.10.100
#
ip pool employee1
  gateway-list 10.1.11.1
  network 10.1.11.0 mask 255.255.255.0
#
```

```
ip pool voicel
 gateway-list 10.1.12.1
 network 10.1.12.0 mask 255.255.255.0
#
ip pool guestl
 gateway-list 10.1.13.1
 network 10.1.13.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authentication-scheme radius
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 domain default
  authentication-scheme default
 domain default_admin
  authentication-scheme default
 local-user admin password irreversible-cipher $1a$VNcE$6oR"2$aASkVyC1-
~qx^~!e+:.S|>BJto>%VV[WvDxK./G$
 local-user admin privilege level 15
 local-user admin service-type ssh http
 local-user huawei password irreversible-cipher
$1a$6@(!=HT_IP$A=lvP*~iu+0<..Y&4`Y6+j4$Xkcf=#aMU=5[4wEP$
 local-user huawei privilege level 1
 local-user huawei service-type telnet ssh http
#
interface Vlanif1
 ip address 169.254.1.1 255.255.0.0
#
interface Vlanif10
 ip address 10.1.10.100 255.255.255.0
 dhcp select global
#
interface Vlanif11
 ip address 10.1.11.100 255.255.255.0
 dhcp select global
#
interface Vlanif12
 ip address 10.1.12.100 255.255.255.0
 dhcp select global
#
interface Vlanif13
 ip address 10.1.13.100 255.255.255.0
 dhcp select global
#
interface Vlanif4090
 ip address 172.21.11.3 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
```

```
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
port link-type access
port default vlan 4090
stp disable
#
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
info-center timestamp log format-date
#
snmp-agent local-engineid 800007DB03845B12566919
snmp-agent community
read %^%#En_g+AWfX>adWz&5.!G~E^ 4&/r]vCScEB~w~u%Zje-
$@`GH0BN7e"$A8PF(_n~lC9qvT)O*{4!I+:yR%^%#
snmp-agent community write %^%#atYiX7&TjG<o\Y/.2Y-
V/8bVI&sGJOTB4$0Y@{"2$306$`dp;=7cULM)*$.3Q!lXY<}!y7jZ,7BS"NNY%^%#
snmp-agent sys-info version v2c
snmp-agent
#
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh server secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh client secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh client key-exchange dh_group14_sha1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
capwap source interface vlanif10
#
user-interface con 0
authentication-mode password
set authentication password
cipher %^%#1<n6!"VC7VQQj=/vGNXG}:Eu&6zT3'C<qU9G'>N8A~"fK_+WA~0De+C]/yW"
%^%#
user-interface vty 0 4
authentication-mode aaa
user privilege level 3
protocol inbound telnet
user-interface vty 16 20
protocol inbound all
#
```

```
wlan
traffic-profile name default
security-profile name default
security-profile name default-wds
security wpa2 psk pass-phrase %^%#CB&>,Q$BB>x\Fn|^%qToSj.2]:%J"+-
qK%aTJ_0%^%# aes
security-profile name default-mesh
security wpa2 psk pass-phrase %^%#]7|J"LhNEQ=-
GJS[q&>M">Qsqw;9mb8$0`_=6I%^%# aes
ssid-profile name guest1
ssid guest1
ssid-profile name voice1
ssid voice1
ssid-profile name default
ssid-profile name employee1
ssid employee1
vap-profile name guest1
forward-mode tunnel
service-vlan vlan-id 13
vap-profile name voice1
service-vlan vlan-id 12
ssid-profile voice1
vap-profile name default
vap-profile name employee1
service-vlan vlan-id 11
ssid-profile employee1
mesh-handover-profile name default
mesh-profile name default
wds-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
vap-profile guest1 wlan 3
radio 1
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
vap-profile guest1 wlan 3
radio 2
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
```



```
vap-profile guest1 wlan 3
ap-id 0 type-id 43 ap-mac 4cfa-cabe-eb60 ap-sn 21500826412SG8918066
ap-group ap-group1
ap-id 1 type-id 43 ap-mac 4cfa-cabf-d0c0 ap-sn 21500826412SG8919901
ap-group ap-group1
provision-ap
#
dot1x-access-profile name dot1x_access_profile
#
mac-access-profile name mac_access_profile
#
undo ntp-service enable
#
return
```

3

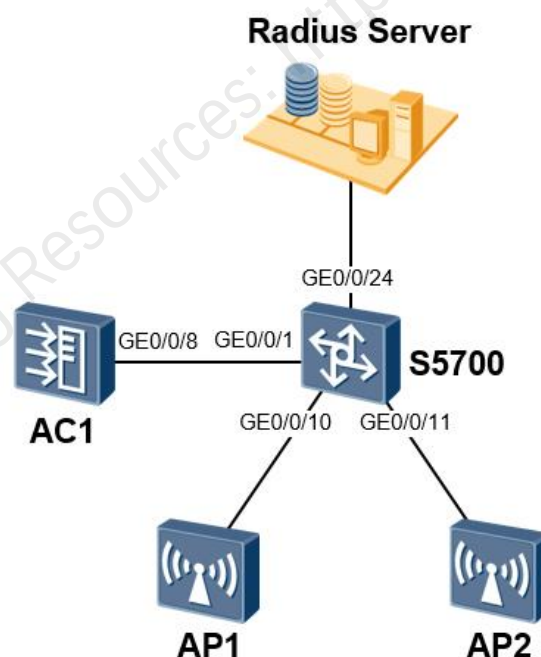
Experiment 3: WLAN Security Configuration

3.1 About This Course

3.1.1 Objectives

- Configure WLAN security profile
- Configure WEP authentication
- Configure WPA/WPA2 PSK authentication
- Configure WPA/WPA2 EAP authentication

3.1.2 Topology



3.1.3 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

The following table describes device connections.

Group No.	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	- AP1-G0/0/10 - AP2-G0/0/11
2	AC2—G0/0/2	- AP3-G0/0/12 - AP4-G0/0/13
3	AC3—G0/0/3	- AP5-G0/0/14 - AP6-G0/0/15
4	AC4—G0/0/4	- AP7-G0/0/15 - AP8-G0/0/16
5	AC5—G0/0/5	- AP9-G0/0/17 - AP10-G0/0/18
6	AC6—G0/0/6	- AP11-G0/0/19 - AP12-G0/0/20

The following table describes an AC parameter configuration template.

AP Group	Name: ap-groupX VAP ID 1: VAP profile: guestX regulatory domain profile: domainX VAP ID 2: VAP profile: voiceX regulatory domain profile: domain VAP ID 3: VAP profile: employeeX regulatory domain profile: domainX
RADIUS Server Profile	Name: huawei Key: huawei
Dot1x Profile	Name: employeeX
Authentication Scheme	Name: employeeX Apply: Radius Server Profile: huawei dot1x Profile: employeeX
SSID Profile	Name: employeeX SSID name: employeeX

	Name: voiceX SSID name: voiceX
	Name: guestX SSID name: guestX
Security Profile	Name: employeeX SSID name: employeeX
	Name: voiceX SSID name: voiceX
	Name: guestX SSID name: guestX
VAP Profile	Name: employeeX Forwarding mode: direct forwarding Service VLAN: 11 Referenced profile: SSID profile employeeX Security Profile employeeX
	Name: voiceX Forwarding mode: direct forwarding Service VLAN: 12 Referenced profile: SSID profile voiceX Security Profile voiceX
	Name: guestX Forwarding mode: tunnel forwarding Service VLAN: 13 Referenced profile: SSID profile guestX Security Profile guestX
Topology: layer2 and layer 3 bypass topology	

3.2 Experiment Task

3.2.1 Configuration Procedure

Step1 Configuring Portal Authentication

Huawei AC supports six access security policies, every VAP Profile can apply each of policies.

Security Policy	Policy Explain
open	Open system Authentication
wapi	WLAN Authentication and Privacy Infrastructure (WAPI)
wep	Wired equivalent privacy
wpa	Wi-Fi protected access
wpa2	Wi-Fi protected access version 2

wpa-wpa2	Wi-Fi protected access version 1&2
----------	------------------------------------

Security Profile : default Display Reference

Security policy : ☒ Open ☐ WEP ☐ WPA ☐ WPA2 ☐ WPA-WPA2 ☐ WAPI

Apply

Configure SSID guestX authentication to Portal authentication. and authentication mode to local authentication.

Choose configuration > Security > AAA > Built-In Portal Server, enter "Built-In Portal Server" page.

Portal server IP: IP address of the Portal server. Users are then redirected to the Portal server if they enter URLs that are not located in the free IP subnet.

SSL policy: SSL policy applied to HTTPS services provided by the Portal server.

Port: Port that provides the authentication service on the Portal server.

Authentication mode: Authentication mode including PAP and CHAP. You are advised to use the CHAP with high security.

Web page file: File in .zip format. The file contains web pages that users access during authentication.

Maximum number of users: Maximum number of users that can access the Portal server.

Wireless LAN
AC6005-8-PWR
Monitoring
Configuration
Diagnosis
Maintenance
Save
Console
admin
?
i
中文

Fast Config
AC Config
AP Config
Security
AAA

Authentication Profile
Service Scheme
External Portal Server
Built-In Portal Server
RADIUS
HWTACACS
Local User
Advanced

Server IP : 10 . 1 . 10 . 100
Port number : 2000
Page file package : - none -
SSL policy : default_policy
Authentication mode : chap
Maximum number of STAs : 1024

Apply

User Group
Customized Page

Create security profile guestX.

Choose configuration > AP Config > Profile > Wireless Service, the security profile list is displayed.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

Fast Config AC Config AP Config AP Group AP Config Profile Security Other Services

Profile Management

Wireless Service

VAP Profile

SSID Profile

Security Profile

default

default-wds

default-mesh

Traffic Profile

802.1X Profile

Portal Profile

MAC Authentication Profile

Authentication-free Rule Profile

Authentication Scheme

Security Profile List

Create Delete Clear Display Reference

Security Profile Name

default

default-wds

default-mesh

10 Total 3 record(s)

Create Security Profile

* Profile name : guest1

Copy parameters from other profiles : - none -

OK Cancel

Security Profile : guest1 Display Reference

Security policy : Open WEP WPA WPA2 WPA-WPA2 WAPI

Apply

Create Portal Profile guestX.

Profile Management

Wireless Service

VAP Profile

SSID Profile

Security Profile

Traffic Profile

802.1X Profile

Portal Profile

portal_access_profile

MAC Authentication Profile

Authentication-free Rule Profile

Authentication Scheme

Portal Profile List

Create Delete Display Reference

Portal Profile Name

portal_access_profile

10 Total 1 record(s)

Create Portal Profile

* Profile name : guest1

OK Cancel

Portal Profile :

Portal authentication : ☒ Built-in portal server ☐ External portal server

Built-in portal server anonymous login : ☐ OFF ☒ ON

Portal escape : ☐ OFF

Portal-server-up action re-authen : ☐ OFF

Create authentication profile guestX, and bind portal profile to the authentication profile.

Choose configuration > Security > AAA", enter authentication profile list.

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Config AP Config Security AAA User Group ACL SSL PKI

Authentication Profile Service Scheme External Portal Server Built-In Portal Server RADIUS HWTACACS Local User Advanced

Authentication Profile List

Create Delete Refresh

Profile Name 802.1X Profile Portal Profile MAC Authen... Authentication-free Rule Profile RADIUS Ser... HWTACACS...

mac_authen... dot1x_authen... portal_authen... default_authen... macportal_authen...

10 Total 5 record(s)

Create Authentication Profile

* Profile name :

Bind portal profile guestX to the authentication profile guestX.

Authentication Profile Service Scheme External Portal Server Built-In Portal Server RADIUS HWTACACS Local User Advanced

Authentication Profile List

mac_authen_profile dot1x_authen_profile portal_authen_profile default_authen_profile macportal_authen_profile guest1 802.1X Profile Portal Profile MAC Authentication Profile Authentication-free Rule Profile RADIUS Server Profile HWTACACS Server Profile Authentication Scheme Authorization Scheme Accounting Scheme Service Scheme

Portal Profile :

Select

Portal Profile List

Name

guest1

portal_access_profile

10 Total 2 record(s)

OK Cancel

Portal Profile : guest1

Display Reference

Create

Portal authentication : ☒ Built-in portal server ☐ External portal server

Built-in portal server anonymous login : OFF

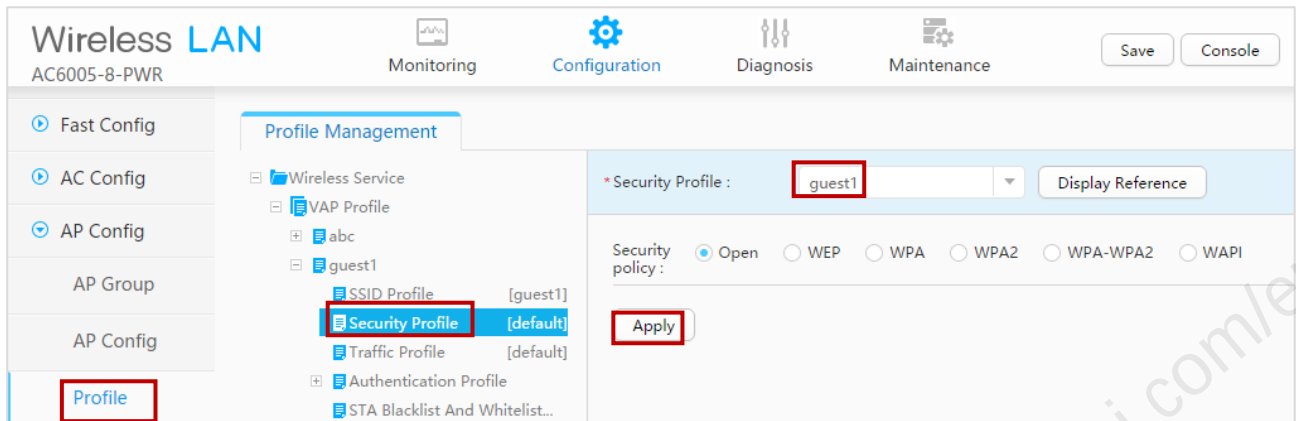
Portal escape : OFF

Portal-server-up action re-authen : OFF

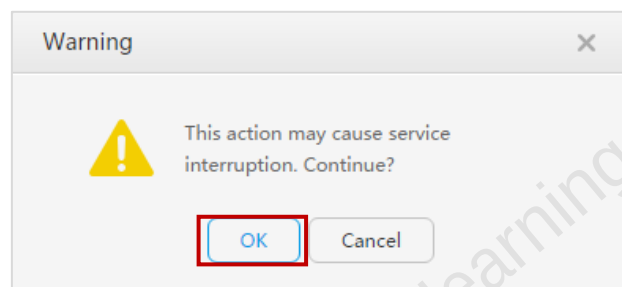
Built-in portal server : ON

Apply

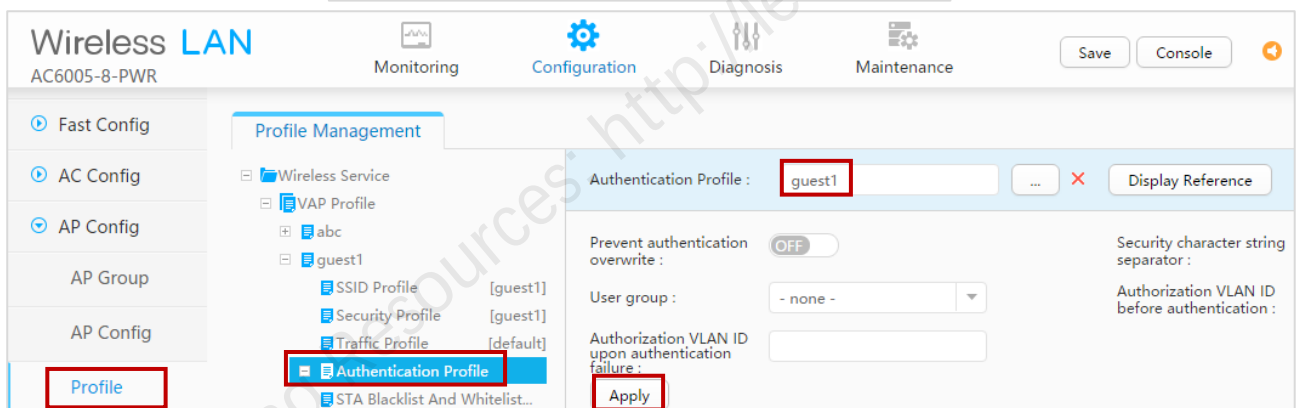
Enter VAP profile page, bind authentication profile guestX and security profile guestX to VAP profile guestX.



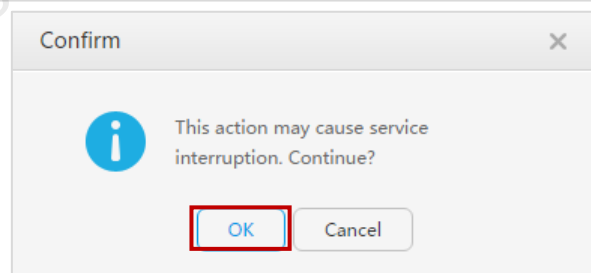
The screenshot shows the 'Wireless LAN' configuration page for 'AC6005-8-PWR'. The 'Profile Management' tab is active. In the left sidebar, 'Profile' is selected. The main area shows the 'VAP Profile' configuration for 'guest1'. The 'Security Profile' is set to 'guest1'. The 'Security policy' is set to 'Open'. The 'Apply' button is highlighted.



A warning dialog box with a yellow triangle icon. The text reads: 'Warning. This action may cause service interruption. Continue?'. There are 'OK' and 'Cancel' buttons.



The screenshot shows the 'Wireless LAN' configuration page for 'AC6005-8-PWR'. The 'Profile Management' tab is active. In the left sidebar, 'Profile' is selected. The main area shows the 'VAP Profile' configuration for 'guest1'. The 'Authentication Profile' is set to 'guest1'. The 'Prevent authentication overwrite' is set to 'OFF'. The 'Apply' button is highlighted.



A confirm dialog box with a blue circle icon. The text reads: 'Confirm. This action may cause service interruption. Continue?'. There are 'OK' and 'Cancel' buttons.

Create Portal account.

Choose configuration > Security > AAA > Local User, enter local user page.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

Fast Config AC Config AP Config Security AAA User Group

Authentication Profile Service Scheme External Portal Server Built-In Portal Server RADIUS HWTACACS Local User Advanced

Local User List

Create Delete Set a User Group Refresh

User Name Access Mode User Group User Status

No data.

User Password Policy

Security > AAA > Local user > Create User

* Creation mode : ☒ Manually add ☐ Batch import

* User name : guest01

* Password : *****

* Confirm password : *****

User status : ☒ Active ☐ Block

* Access mode : ☐ All ☒ web ☐ 802.1X ☐ ppp

OK Cancel

Wireless users can open the browser, and enter a website. The link will automatically go to Portal authentication page. After you input the right username and password, click "login". (NOTE: this experiment don't have DNS, we need to input the ip address, for example, 114.114.114.114).

Online Service...

https://10.1.10.100.2000/index.html

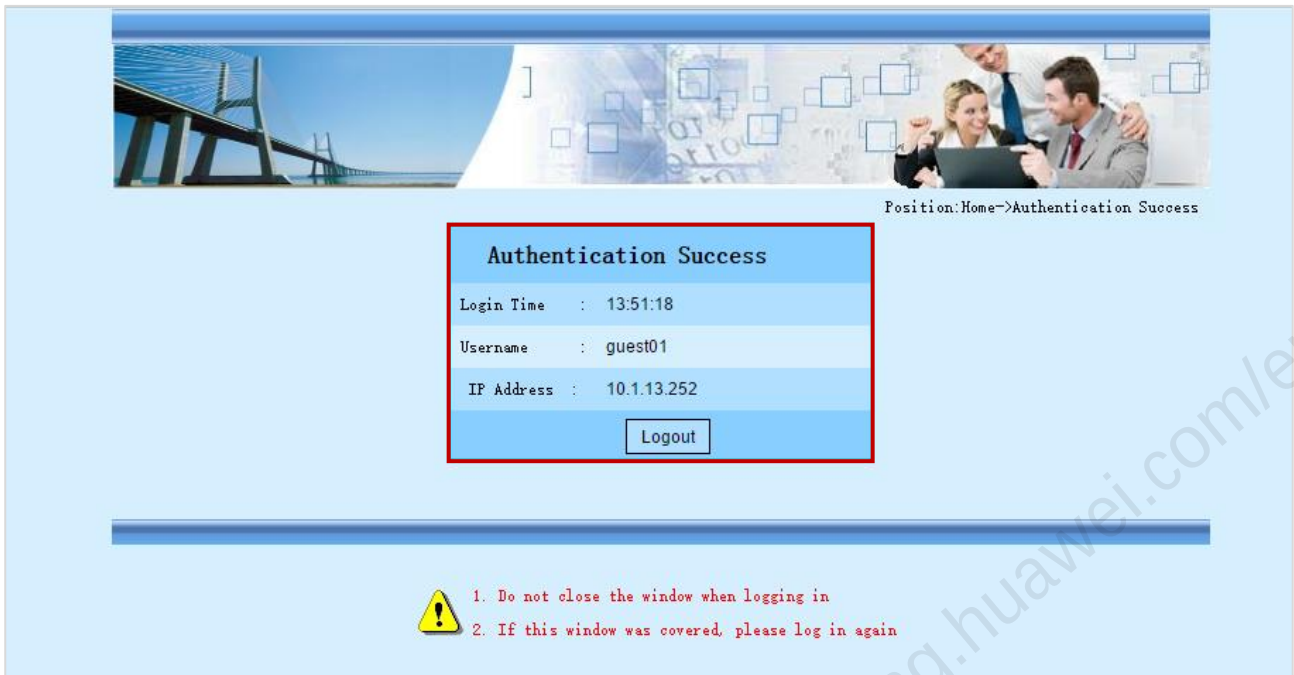
REGISTERED USER

User name: guest01

Password: *****

Login

Position: Home
Login



Then the configuration of Portal authentication has been finished, we can test the connection.

```
C:\Users\zWX>ping 101.101.101.101
PING 101.101.101.101: 56 data bytes, press CTRL_C to break
    Reply from 101.101.101.101: bytes=56 Sequence=1 ttl=255 time=7 ms
    Reply from 101.101.101.101: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 101.101.101.101 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 7/9/10 ms
```

Step2 Configuring WPA PSK Authentication

Configure the authentication type for SSID voiceX to WPA1-PSK. Huawei AC supports below WPA configuration option::

WPA Type	Encryption Method	Authentication Method
WPA/WPA2/WPA1-2 Personal	CCMP or TKIP	PSK(password 8-64 characters)
WPA/WPA2/WPA1-2 Enterprise	CCMP or TKIP	Dot1x

Configure security profile security-profile name voice1, encryption mode TKIP, password of PSK is voicevoice.

Choose Configuration > AP Config > Profile > Wireless Service > Security profile, the security profile page is displayed, in security profile list, click create, set the parameters.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Config AP Config AP Group AP Config Profile

Profile Management

Wireless Service VAP Profile SSID Profile Security Profile guest1 default default-wds default-mesh Traffic Profile

Security Profile List

Create Delete Clear Display Reference

Security Profile Name

guest1

default

Create Security Profile

* Profile name : voice1 Copy parameters from other profiles : - none -

OK Cancel

Security Profile : voice1 Display Reference

Security policy : Open WEP WPA WPA2 WPA-WPA2 WAPI

Authentication policy : PSK Dot1x

Encryption mode : AES TKIP AES-TKIP

Password type : HEX PASS-PHRASE

* Password : * Confirm password :

PTK update interval : OFF

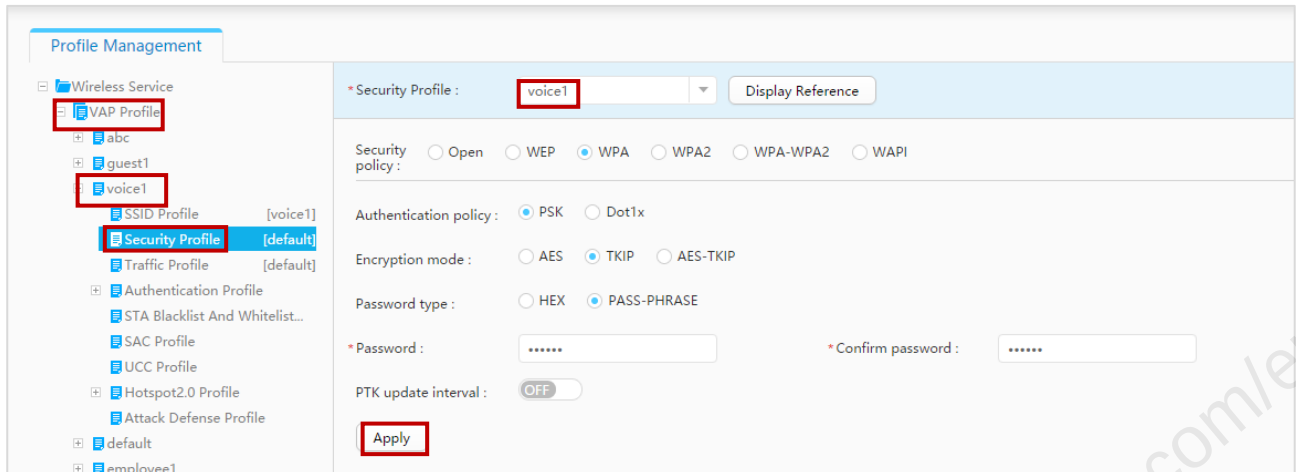
Apply

Warning

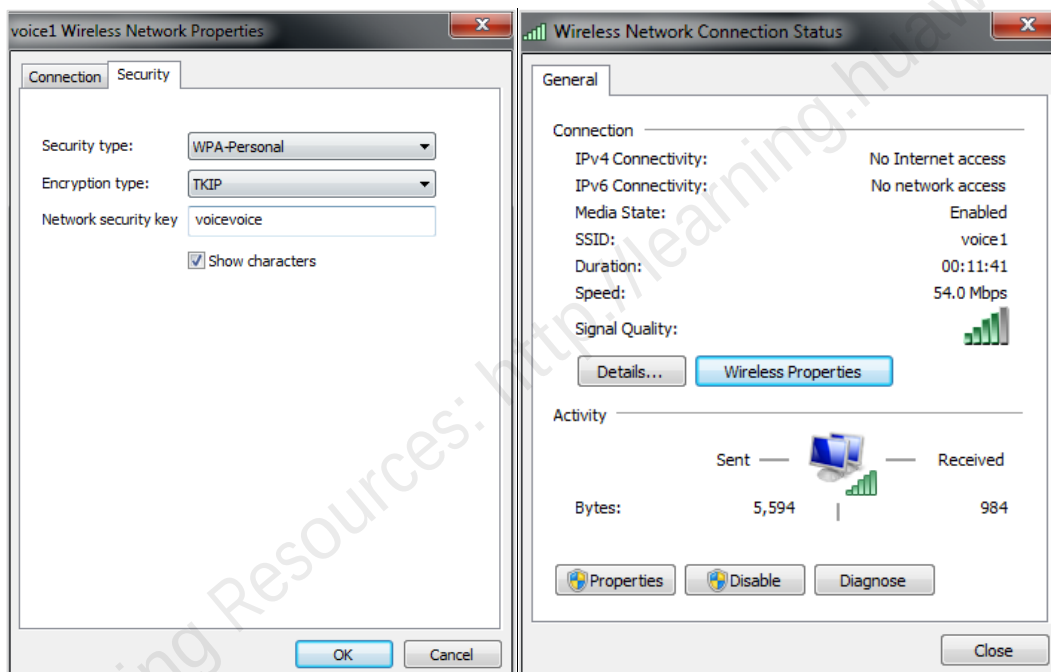
The current password is too simple. For the sake of security, you are advised to set a password containing at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special characters. Continue?

OK Cancel

Bind the security profile voiceX to VAP profile voiceX.



Then the Configuration of WPA-PSK has been finished, we can test the connection.



```
C:\Users\zwx>ping 101.101.101.101
```

```
PING 101.101.101.101: 56 data bytes, press CTRL_C to break
```

```
Reply from 101.101.101.101: bytes=56 Sequence=1 ttl=255 time=7 ms
```

```
Reply from 101.101.101.101: bytes=56 Sequence=2 ttl=255 time=10 ms
```

```
Reply from 101.101.101.101: bytes=56 Sequence=3 ttl=255 time=10 ms
```

```
Reply from 101.101.101.101: bytes=56 Sequence=4 ttl=255 time=10 ms
```

```
Reply from 101.101.101.101: bytes=56 Sequence=5 ttl=255 time=10 ms
```

```
--- 101.101.101.101 ping statistics ---
```

```
5 packet(s) transmitted
```

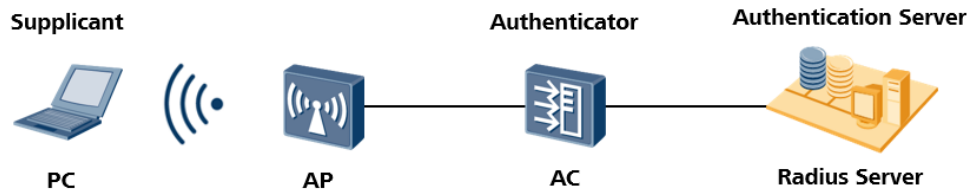
```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 7/9/10 ms
```

Step3 Configuring WPA EAP Authentication

The authentication architecture of EAP consists of three parts: clients, authenticator and authentication server.



The authentication server of this experiment had set an IP address 10.254.1.100, password: huawei, the authentication server was ready and test account: huawei, password: Huawei@123.

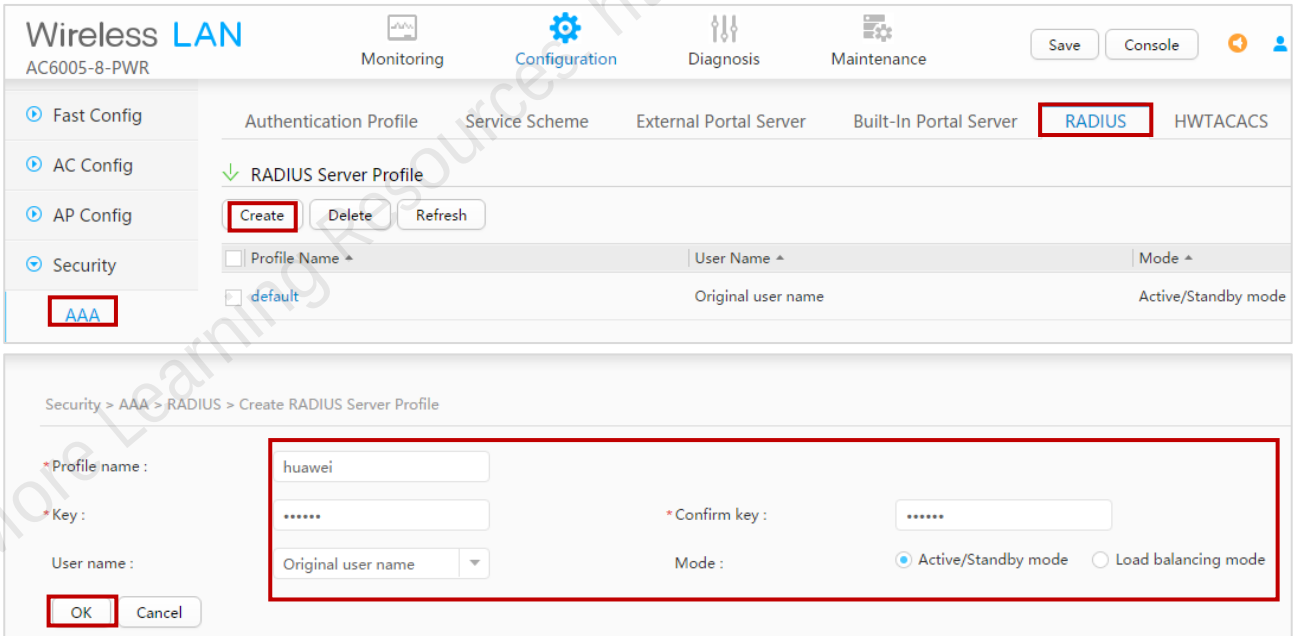
Configure radius service gateway in the S5700.

```
[S5700] vlan batch 200
[S5700] interface GigabitEthernet0/0/24
[S5700-GigabitEthernet0/0/24] port link-type access
[S5700-GigabitEthernet0/0/24] port default vlan 200
[S5700-GigabitEthernet0/0/24] quit
[S5700] interface Vlanif200
[S5700-Vlanif200] ip address 10.254.1.1 24
[S5700-Vlanif200] quit
```

Configure radius service and accounting scheme in the AC.

Configuring Radius profile.

Choose Configuration > Security > AAA > RADIUS, the RADIUS page is displayed.



The screenshot shows the Huawei Wireless LAN configuration interface. The top navigation bar includes Monitoring, Configuration, Diagnosis, and Maintenance. The left sidebar shows Fast Config, AC Config, AP Config, Security, and AAA. The main content area displays the RADIUS configuration page, which includes a table for RADIUS Server Profiles. The table has columns for Profile Name, User Name, and Mode. The 'default' profile is listed with the user name 'Original user name' and mode 'Active/Standby mode'. Below the table, there is a 'Create RADIUS Server Profile' form. The form includes fields for Profile name (huawei), Key (*****), Confirm key (*****), User name (Original user name), and Mode (Active/Standby mode). The 'OK' button is highlighted.

Create Radius Server

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Config AP Config Security

Authentication Profile Service Scheme External Portal Server Built-In Portal Server **RADIUS** HWTAC

→ RADIUS Server Profile

↓ Authentication/Accounting Server

Create Delete Refresh

AAA

Profile Name Server Type IP Address/Port Number Weight

No data.

Security > AAA > RADIUS > Create Authentication/Accounting Server

*Profile name : huawei

Server type : ☒ Authentication server ☐ Accounting server

Server Settings

*IP address : 10 . 254 . 1 . 100

Source address of outgoing packets : ☐ LoopBack ☒ IP address

Port number : 1812

Weight : 80

10 . 1 . 10 . 100

OK Cancel

Configure AAA.

Choose Configuration > AP Config > Profile > Wireless Service, enter AuthenticationScheme list.(by default, have a radius profile, you can not create).

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Config AP Config Security Other Services Backup Settings

Profile Management

Wireless Service

VAP Profile SSID Profile Security Profile Traffic Profile 802.1X Profile Portal Profile MAC Authentication Profile Authentication-free Rule Profile

Authentication Scheme

radius default

Authorization Scheme Accounting Scheme Authentication Profile

Authentication Scheme List

Create Delete Display Reference

Authentication Scheme Name

radius

default

10 Total 2 record(s)

Create Authentication Scheme

* Profile name :

Configure authentication mode for radius authentication.

Authentication Scheme :

First authentication : Second authentication :

Third authentication : Fourth authentication :

Configure access profile dot1x-access-profile name employeeX, authentication mode is eap.

Profile Management

- ☒ Wireless Service
 - VAP Profile
 - SSID Profile
 - Security Profile
 - Traffic Profile
 - ☒ 802.1X Profile
 - dot1x_access_profile
 - Portal Profile
 - MAC Authentication Profile

802.1X Profile List

802.1X Profile Name
dot1x_access_profile

10 Total 1 record(s)

Create 802.1X Profile

* Profile name :

802.1X Profile :

User authentication mode :

Reauthentication :

Maximum authentication request count :

Authentication timeout interval (s) :

EAP packet code number : EAP packet data type :

Configure security profile security-profile name employeeX, encryption mode is ccmp (aes).

Profile Management

- Wireless Service
 - VAP Profile
 - SSID Profile
 - Security Profile
 - Traffic Profile
 - 802.1X Profile
 - Portal Profile
 - MAC Authentication Profile
 - Authentication-free Rule Profile

Security Profile List

Create
Delete
Clear
Display Reference

Security Profile Name
guest1
voice1

Create Security Profile

* Profile name : employee1
Copy parameters from other profiles : - none -

OK
Cancel

Security Profile : employee1
Display Reference

Security policy :
☐ Open
☐ WEP
☐ WPA
☒ WPA2
☐ WPA-WPA2
☐ WAPI

Authentication policy :
☐ PSK
☒ Dot1x

Encryption mode :
☒ AES
☐ TKIP
☐ AES-TKIP

Management frame protection :
☐ OFF
☐ ON

PTK update interval :
☐ OFF
☐ ON

Apply

Configure authentication profile authentication-profile name employee.

Bind the access profile, authentication scheme, accounting scheme and radius server to authentication profile.

Choose Configuration > Security > AAA > Authentication Profile, enter authentication profile page, click create, create a employee authentication profile.

Wireless LAN

AC6005-8-PWR

- Fast Config
- AC Config
- AP Config
- Security
- AAA

Authentication Profile

- Authentication Profile List
- guest1
- mac_authen_profile
- dot1x_authen_profile
- portal_authen_profile
- default_authen_profile
- macportal_authen_profile

Authentication Profile List

Create
Delete
Refresh

Profile Name	802.1X Profile	Portal Profile	MAC Aut
guest1		guest1	
mac_authen...			

Create Authentication Profile

* Profile name :

Authentication Profile :

Prevent authentication overwrite : ☐

User group :

Authorization VLAN ID upon authentication failure :

Security character string separator :

Authorization VLAN ID before authentication :

Bind the dot1x access profile and radius server profile to authentication profile.

Authentication Profile Service Scheme External Portal Server Built-In Portal Server

Authentication Profile List

- guest1
- mac_authen_profile
- dot1x_authen_profile
- portal_authen_profile
- default_authen_profile
- macportal_authen_profile
- employee1**
- 802.1X Profile**
- Portal Profile
- MAC Authentication Profile
- Authentication-free Rule Profile
- RADIUS Server Profile

802.1X Profile :

User authentication mode :

Reauthentication : ☐

Maximum authentication request count :

Authentication timeout interval (s) :

EAP packet code number :

Authentication Profile | Service Scheme | External Portal Server | Built-In Portal Server | RADIUS

Authentication Profile List

- guest1
- mac_authen_profile
- dot1x_authen_profile
- portal_authen_profile
- default_authen_profile
- macportal_authen_profile
- employee1**
 - 802.1X Profile [employ...]
 - Portal Profile
 - MAC Authentication Profile
 - Authentication-free Rule Profile
 - RADIUS Server Profile**
 - HWTACACS Server Profile

RADIUS Server Profile : **huawei** Display Reference

Apply

Authentication Profile | Service Scheme | External Portal Server | Built-In Portal Server | RADIUS | HWTACACS | Local User | Advanced

Authentication Profile List

- guest1
- mac_authen_profile
- dot1x_authen_profile
- portal_authen_profile
- default_authen_profile
- macportal_authen_profile
- employee1**
 - 802.1X Profile [employ...]
 - Portal Profile
 - MAC Authentication Profile
 - Authentication-free Rule Profile
 - RADIUS Server Pr... [huawei]
 - HWTACACS Server Profile
 - Authentication Scheme**
 - Authorization Scheme

Authentication Scheme : **radius** Display Reference Create

First authentication : RADIUS authentication Second authentication : Not configured

Third authentication : Not configured Fourth authentication : Not configured

Apply

Bind security profile and authentication profile to VAP profile.

Profile Management

Wireless Service

- VAP Profile**
 - abc
 - guest1
 - voice1
 - default
 - employee1**
 - SSID Profile [employ...]
 - Security Profile [default]
 - Traffic Profile [default]
 - Authentication Profile
 - STA Blacklist And Whitelist...

VAP Profile : **employee1** Display Reference

Status : ☒ ON VAP type

Service VLAN : ☒ Single VLAN ☐ VLAN Pool Service

Forwarding mode : Direct mDNS p tunnel :

Band steering : ☒ ON

Home agent : ☐ AC ☒ AP Roaming

Level 2 roaming : ☒ ON

Profile Management

- Wireless Service
 - VAP Profile
 - abc
 - guest1
 - voice1
 - default
 - employee1
 - SSID Profile [employ...]
 - Security Profile [default]**
 - Traffic Profile [default]
 - Authentication Profile
 - STA Blacklist And Whitelist...
 - SAC Profile
 - UCC Profile

* Security Profile : **employee1** Display Reference

Security policy : ☐ Open ☐ WEP ☐ WPA ☒ WPA2 ☐ WPA-WPA2 ☐ WAPI

Authentication policy : ☐ PSK ☒ Dot1x

Encryption mode : ☒ AES ☐ TKIP ☐ AES-TKIP

Management frame protection : ☐ OFF

PTK update interval : ☐ OFF

Apply

Warning

 This action may cause service interruption. Continue?

OK Cancel

Profile Management

- Wireless Service
 - VAP Profile
 - abc
 - guest1
 - voice1
 - default
 - employee1
 - SSID Profile [employ...]
 - Security Profile [employ...]
 - Traffic Profile [default]
 - Authentication Profile**

Authentication Profile : **employee1** ... × Display Reference

Prevent authentication overwrite : ☐ OFF

User group : - none -

Authorization VLAN ID upon authentication failure :

Apply

Security character string separator :

Authorization VLAN ID before authentication :

Confirm

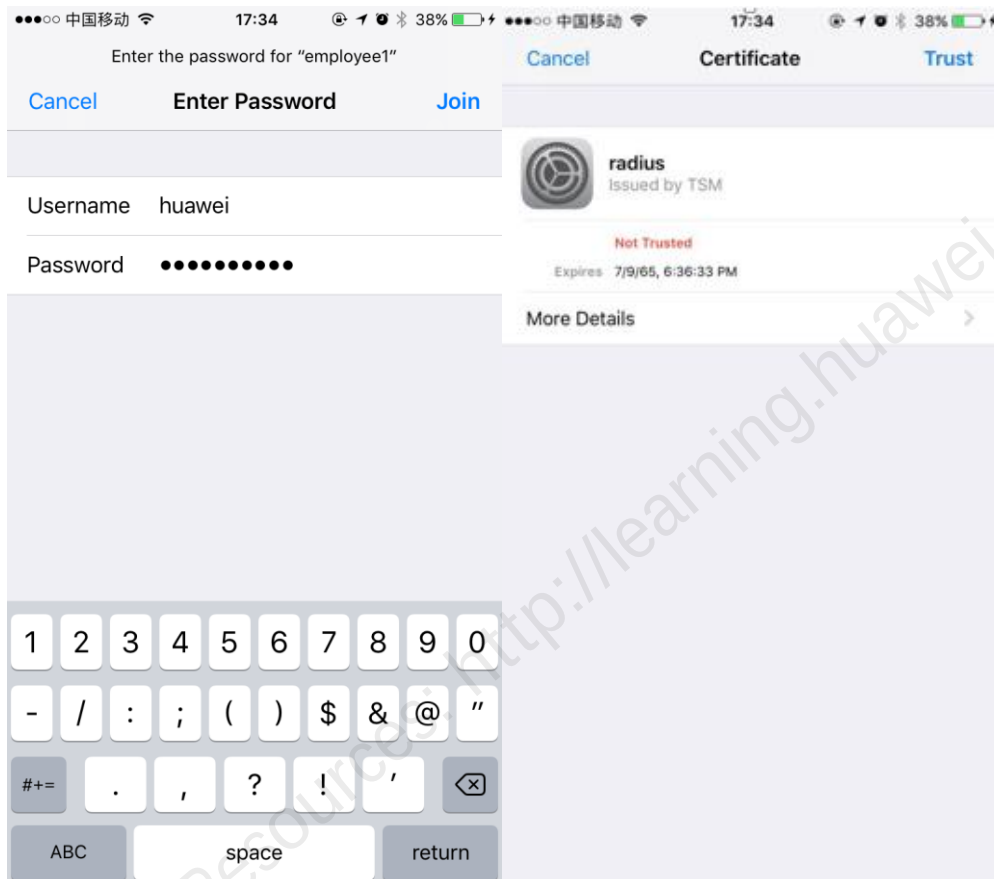
 This action may cause service interruption. Continue?

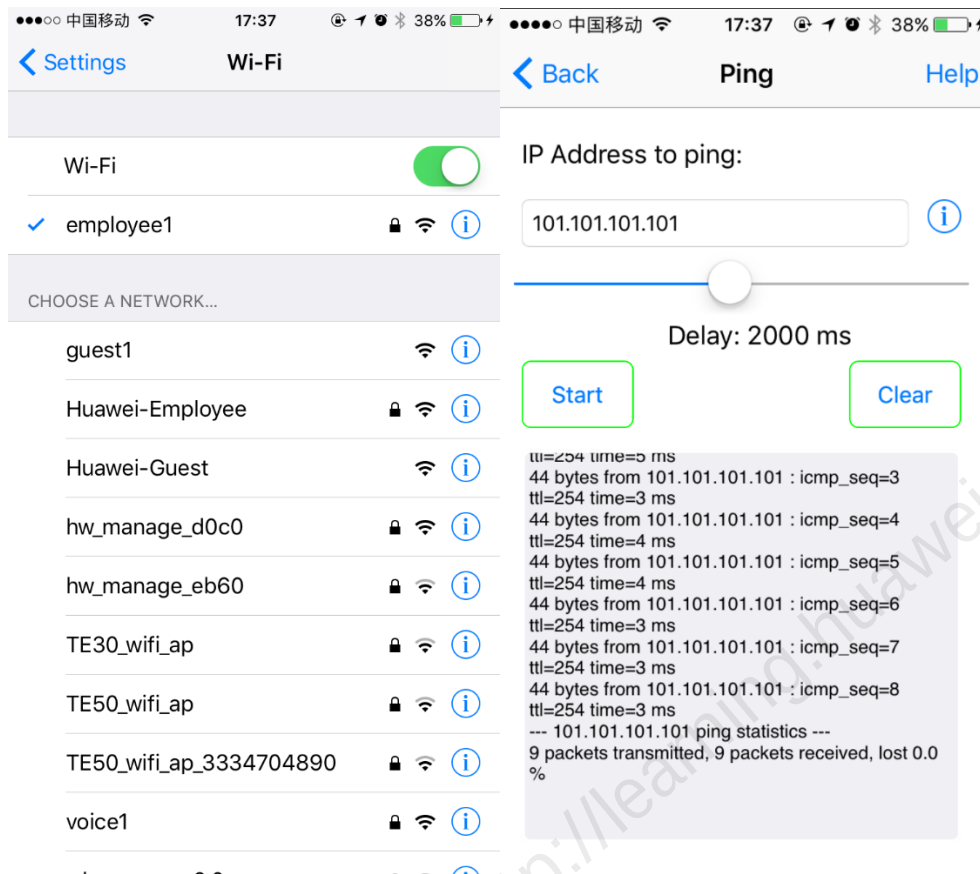
OK Cancel

3.3 Verification

3.3.1 Connect an STA to the WLAN

Connect iphone to the WLANs with SSIDs employeeX.





3.4 Reference Configuration

3.4.1 S5700 Configuration

```
#
sysname S5700
#
vlan batch 10 to 13 200
#
lldp enable
#
undo http server enable
undo http secure-server enable
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@@@5d~9:M^ipCfL\iB)EQd>3Uwe%@@@
```

```
local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
ip address 10.1.13.1 255.255.255.0
#
interface Vlanif200
ip address 10.254.1.1 255.255.255.0
#
interface MEth0/0/1
ip address 172.21.11.1 255.255.0.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/11
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
```

```
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
 port link-type trunk
 port default vlan 200
#
interface NULL0
#
interface LoopBack1
 ip address 101.101.101.101 255.255.255.255
#
user-interface con 0
 authentication-mode password
 set authentication password
 cipher %@@@;|J%=/[d[O@L[qD[Xhh~,3[~S(Zs:\Ot8H6*x_MAW=N$3[B,%@@@
user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password
 cipher %@@@`KL`QN[h79h[6AS2ggdT<+Hjaz5lH\hpS4]~^/-CFvtO+Hm<%@@@
 protocol inbound all
user-interface vty 16 20
#
return
```

3.4.2 AC Configuration

```
#
 sysname AC1
#
 http secure-server ssl-policy default_policy
 http server enable
#
 portal local-server ip 10.1.10.100
 portal local-server https ssl-policy default_policy port 2000
```

```
#
undo portal url-encode enable
#
ssl renegotiation-rate 1
#
vlan batch 10 to 13 4090
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
portal-access-profile guest1
authentication-profile name macportal_authen_profile
authentication-profile name guest1
portal-access-profile guest1
authentication-profile name employee1
dot1x-access-profile employee1
authentication-scheme radius
radius-server huawei
#
lldp enable
#
dhcp enable
#
diffserv domain default
#
radius-server template default
radius-server template huawei
radius-server authentication 10.254.1.100 1812 source ip-address
10.1.10.100 weight 80
undo radius-server user-name domain-included
#
pki realm default
rsa local-key-pair default
enrollment self-signed
#
ssl policy default_policy type server
pki-realm default
version tls1.0 tls1.1
ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
encryption-algorithm aes-256
dh group2
authentication-algorithm sha2-256
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
portal local-server enable
#
portal-access-profile name guest1
```

```
portal local-server enable
#
ip pool ap
 gateway-list 10.1.10.1
 network 10.1.10.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 10.1.10.100
#
ip pool employee1
 gateway-list 10.1.11.1
 network 10.1.11.0 mask 255.255.255.0
 dns-list 114.114.114.114
#
ip pool voice1
 gateway-list 10.1.12.1
 network 10.1.12.0 mask 255.255.255.0
#
ip pool guest1
 gateway-list 10.1.13.1
 network 10.1.13.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authentication-scheme radius
 authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 domain default
 authentication-scheme default
 domain default_admin
 authentication-scheme default
 local-user admin password irreversible-cipher $1a$VNcE$6oR"2$aASkVyC1-
 ~~qx^~!e+:.S|>BJto>%VV[WvDxK./G$
 local-user admin privilege level 15
 local-user admin service-type ssh http
 local-user huawei password irreversible-cipher
 $1a$6@(!=HT_IP$A=lvP*~iu+0<..Y&4`Y6+j4$Xkcf=#aMU=5[4wEP$
 local-user huawei privilege level 1
 local-user huawei service-type telnet ssh http
 local-user guest01 password cipher %^%#h)q(D@"^~3lbX|<1Hk1L#bj]RY3-
 pAYq#XEVAp>~%~%#
 local-user guest01 privilege level 0
 local-user guest01 service-type web
#
interface Vlanif1
 ip address 169.254.1.1 255.255.0.0
#
interface Vlanif10
 ip address 10.1.10.100 255.255.255.0
 dhcp select global
#
interface Vlanif11
 ip address 10.1.11.100 255.255.255.0
 dhcp select global
#
interface Vlanif12
```

```

ip address 10.1.12.100 255.255.255.0
dhcp select global
#
interface Vlanif13
ip address 10.1.13.100 255.255.255.0
dhcp select global
#
interface Vlanif4090
ip address 172.21.11.3 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
port link-type access
port default vlan 4090
stp disable
#
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
info-center timestamp log format-date
#
snmp-agent local-engineid 800007DB03845B12566919
snmp-agent community
read %^%#En_g+AWfX>adWz&5.!G~E^)^4&/r]vCScEB~w~u%Zje-
$@`GH0BN7e"$A8PF(_n~lC9qvT)O*{4!I+:yR%^%#
snmp-agent community write %^%#atYiX7&TjG<o\Y/.2Y-
V/8bVI&sGJOTB4$0Y@{"2$306$`dp;=7cULM)*$.3Q!lXY<}!y7jZ,7BS"NNY%^%#
snmp-agent sys-info version v2c
snmp-agent
#
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh server secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh client secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh client key-exchange dh_group14_sha1
#

```

```
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
capwap source interface vlanif10
#
user-interface con 0
 authentication-mode password
 set authentication password
 cipher %^%#1<n6!"VC7VQQj=/vGNXG}:Eu&6zT3'C<qU9G'>N8A~"fK_+WA~0De+C]/yW"
 %^%#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound telnet
user-interface vty 16 20
 protocol inbound all
#
wlan
 traffic-profile name default
 security-profile name guest1
 security-profile name voice1
 security wpa psk pass-
 phrase %^%#0)RfPJm>L58cY+4*K);#E~]V)7`\406bJM4syy*%^%# tkip
 security-profile name default
 security-profile name employee1
 security wpa2 dot1x aes
 security-profile name default-wds
 security wpa2 psk pass-phrase %^%#CB&>,Q$BB>x\Fn"|^%qToSj.2]:%J"+-
 qK%aTJ_0%^%# aes
 security-profile name default-mesh
 security wpa2 psk pass-phrase %^%#]7|J"LHnEQ=-,
 GJS[q&>M">Qsqw;9mb8$0`=6I%^%# aes
 ssid-profile name guest1
 ssid guest1
 ssid-profile name voice1
 ssid voice1
 ssid-profile name default
 ssid-profile name employee1
 ssid employee1
 vap-profile name guest1
 forward-mode tunnel
 service-vlan vlan-id 13
 ssid-profile guest1
 security-profile guest1
 authentication-profile portal_authen_profile
 vap-profile name voice1
 service-vlan vlan-id 12
 ssid-profile voice1
 security-profile voice1
 vap-profile name default
 vap-profile name employee1
 service-vlan vlan-id 11
 ssid-profile employee1
 security-profile employee1
 authentication-profile employee1
 mesh-handover-profile name default
 mesh-profile name default
```

```
wds-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
    regulatory-domain-profile domain1
radio 0
    vap-profile employee1 wlan 1
    vap-profile voice1 wlan 2
    vap-profile guest1 wlan 3
radio 1
    vap-profile employee1 wlan 1
    vap-profile voice1 wlan 2
    vap-profile guest1 wlan 3
radio 2
    vap-profile employee1 wlan 1
    vap-profile voice1 wlan 2
    vap-profile guest1 wlan 3
ap-id 0 type-id 43 ap-mac 4cfa-cabe-eb60 ap-sn 21500826412SG8918066
    ap-group ap-group1
ap-id 1 type-id 43 ap-mac 4cfa-cabf-d0c0 ap-sn 21500826412SG8919901
    ap-group ap-group1
provision-ap
#
dot1x-access-profile name dot1x_access_profile
dot1x-access-profile name employee1
#
mac-access-profile name mac_access_profile
#
undo ntp-service enable
#
return
```

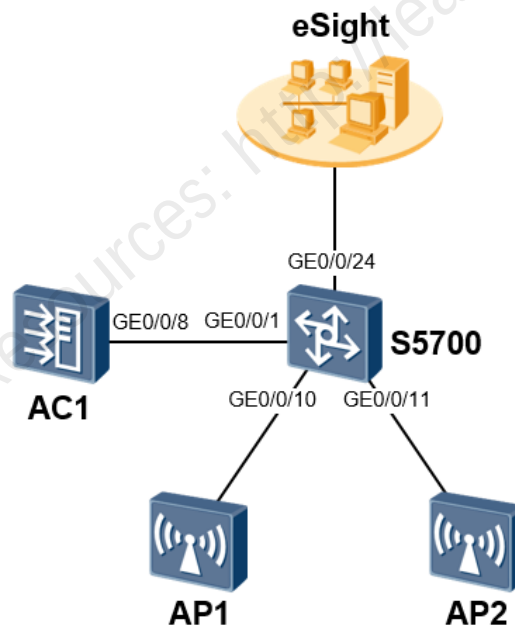
4 Experiment 4: eSight WLAN Management

4.1 About This Course

4.1.1 Objectives

- Configure SNMP in AC
- Understand the method of eSight discover AC
- Configure WLAN with eSight wizard

4.1.2 Topology



4.1.3 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

The following table describes device connections.

Group No.	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	- AP1-G0/0/10 - AP2-G0/0/11
2	AC2—G0/0/2	- AP3-G0/0/12 - AP4-G0/0/13
3	AC3—G0/0/3	- AP5-G0/0/14 - AP6-G0/0/15
4	AC4—G0/0/4	- AP7-G0/0/15 - AP8-G0/0/16
5	AC5—G0/0/5	- AP9-G0/0/17 - AP10-G0/0/18
6	AC6—G0/0/6	- AP11-G0/0/19 - AP12-G0/0/20

eSight Server IP	172.21.11.20
eSight Server password	Name: admin Password: Huawei@123
SNMP read only community	publicRO
SNMP read and write community	privateRW

4.2 Experiment Task

4.2.1 Configuration Procedure

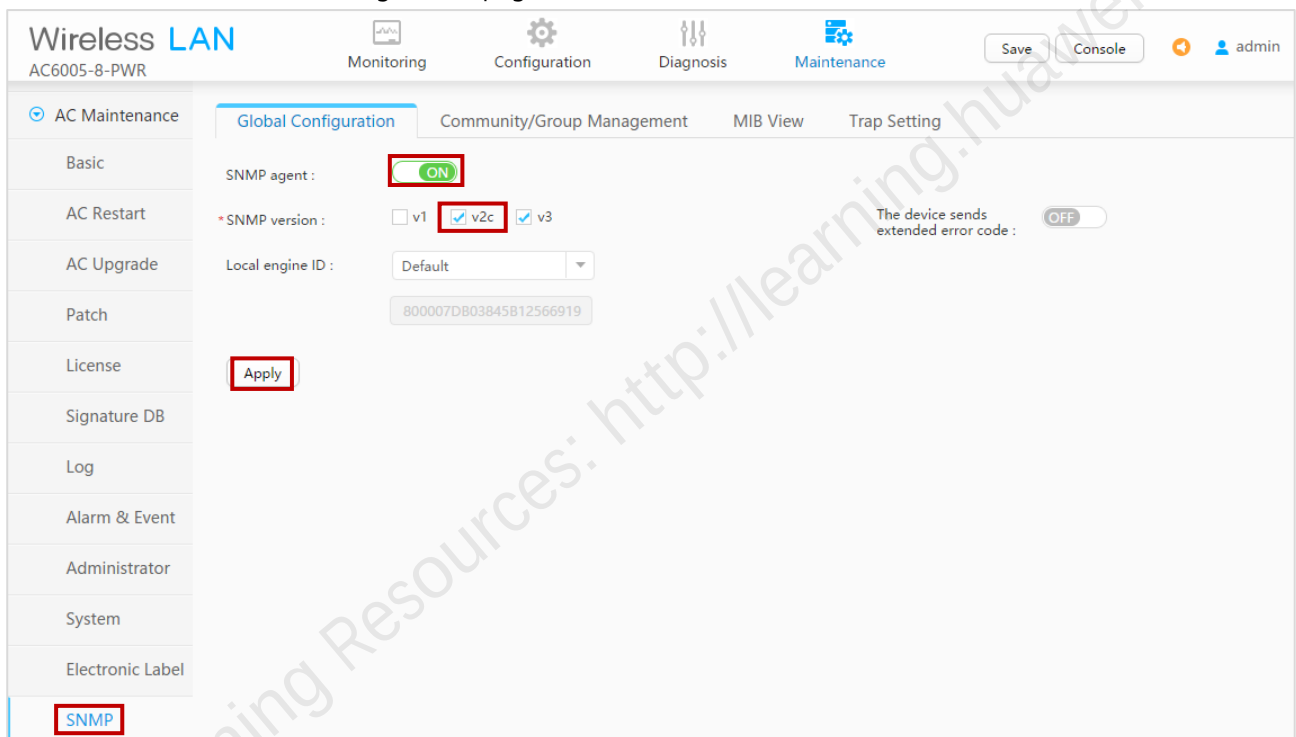
Step1 Configuring a Switch

Continue the configuration from experiment 1, the configuration of the switch has been ready.

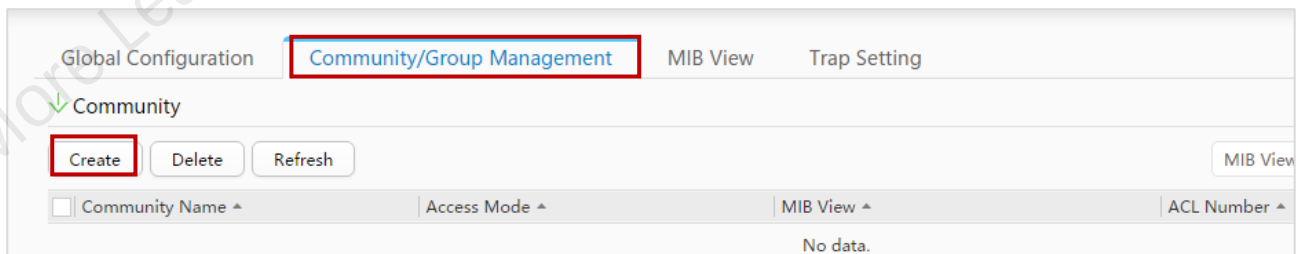
Step2 Configuring SNMP Parameters

Configure AC SNMP Community and static route.

Choose "Maintenance > AC Maintenance > SNMP > Global Configuration", enter the Global Configuration page.



Enter Community/Group Management, click create and set parameters for snmp.



AC Maintenance > SNMP > Community/Group Management > Create Community

* Community name : * Access mode :

MIB view : ACL number :

AC Maintenance > SNMP > Community/Group Management > Create Community

* Community name : * Access mode :

MIB view : ACL number :

Choose "Configuration > AC Config > IP > Route > Static Route Configuration Table", enter Static Route Configuration Table page.

In Static Route Configuration Table, click create, configure the static route.

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

Fast Config DHCP Address Pool DHCP Relay NAT **Route**

AC Config → Routing Table

Basic Config **Static Route Configuration Table**

VLAN

Interface ☐ Destination IP Subnet Mask Next Hop Address Outbound Interface Priority Description

IP

AP Config Security Other Services Backup Settings

Wireless LAN AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance Save Console admin ? i 中文

Fast Config AC Config > IP > Route > Create Static Route

AC Config * Destination IP : * Subnet mask :

Basic Config Next hop address : Outbound interface : ... ×

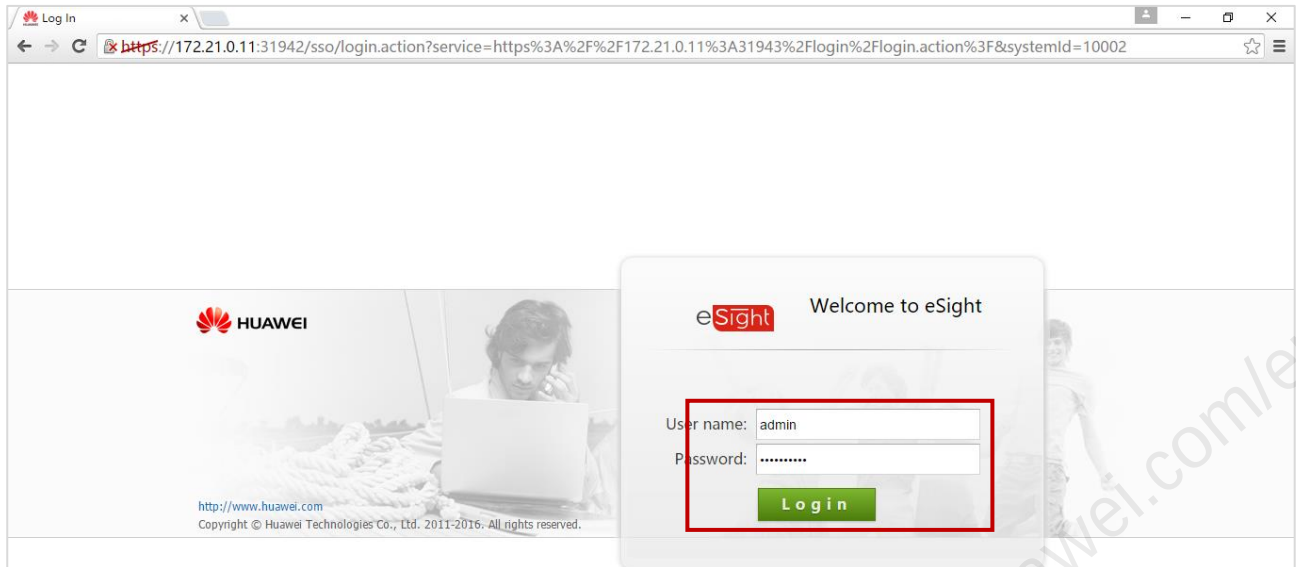
VLAN Priority : Description :

Interface

IP

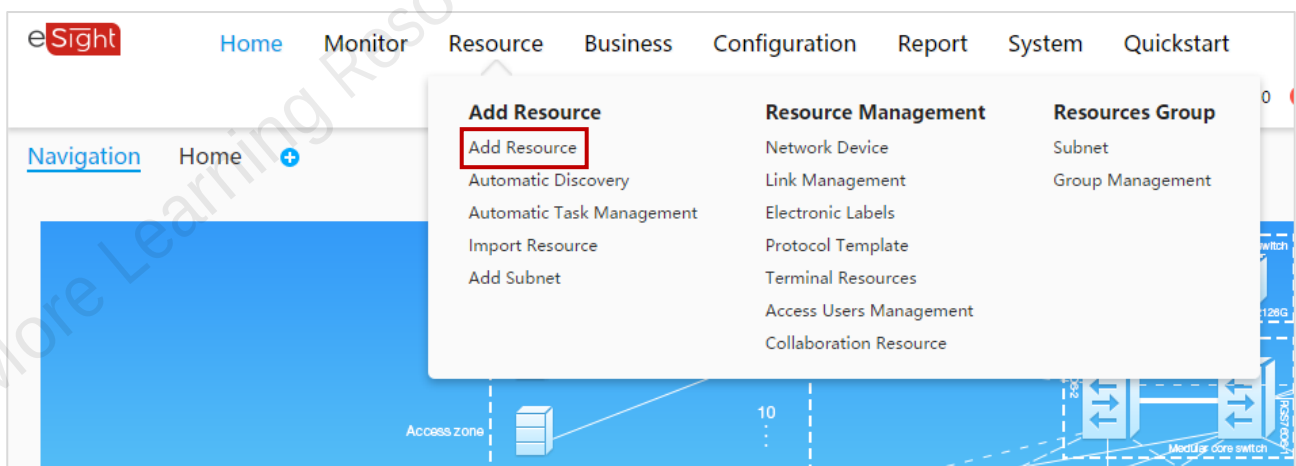
Step3 Configuring eSight Discover AC

After the PC connect to the WLAN, enter URL <http://172.21.11.20:8080> to access eSight Server, user name: admin, password: Huawei@123 (The initialized user name and password are: admin/Changeme123, you need change the initial password when you first login eSight). Should use google chrome or firefox browser.



After login in to eSight, select the pull-down menu “Resource”, and click “Add Device”,reference below parameters.

IP Address	172.21.11.X+2
Name	ACX
SNMP Version	V2C
Read Only Community	publicRO
Write Community	privateRW
Telnet Authentication mode	Password
Password	Admin@123



Basic Information

* IP address: 172.21.11.3 DNS Mapping Subnet: / ...
Name: AC1

SNMP

☐ Match template ☐ Select template ☒ Edit SNMP parameters

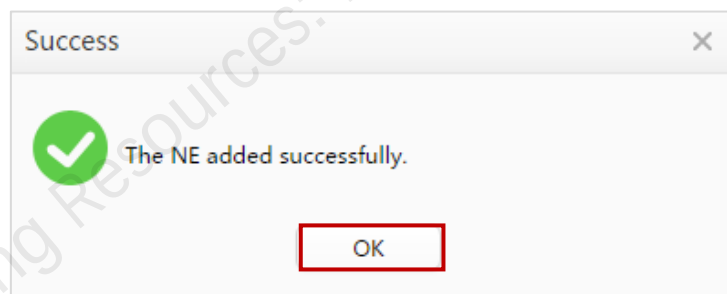
Set parameters in the template based on the SNMP information on the device. The security level of SNMP V3 is higher than the security levels of SNMP V1 and SNMPv2c. Authentication protocol are HMAC_SHA and HMAC_MD5. The security level of HMAC_SHA is higher than the security level of HMAC_MD5 but still cannot meet requirement AES_128 to enhance the security. Authentication password and encryption password are suggested not to be consistent.

SNMP version: V2c
* Read community: Write community:
* Port: 161 Timeout interval (s): 3

Telnet(optional)

☐ Match template ☐ Select template ☒ Edit Telnet parameters
Protocol: Telnet Authentication: Password
User name: * Port: 23
* Password: * Timeout interval (s): 20
☐ Privilege Model
OK Cancel Apply

Click "OK" when you finished, if displayed "Success" then means the configuring is succeeded.



eSight

Home Monitor Resource Business Configuration Report System Quickstart

0 0 0 0 0 0 0 0 admin

Network Device

+ Add Device Automatic Import Device Set Protocol More

All

Status	Name	IP Address	Type	Manufacturer	Remarks	Operation
●	AC1	172.21.11.3	AC6005-8-PWR	Huawei		

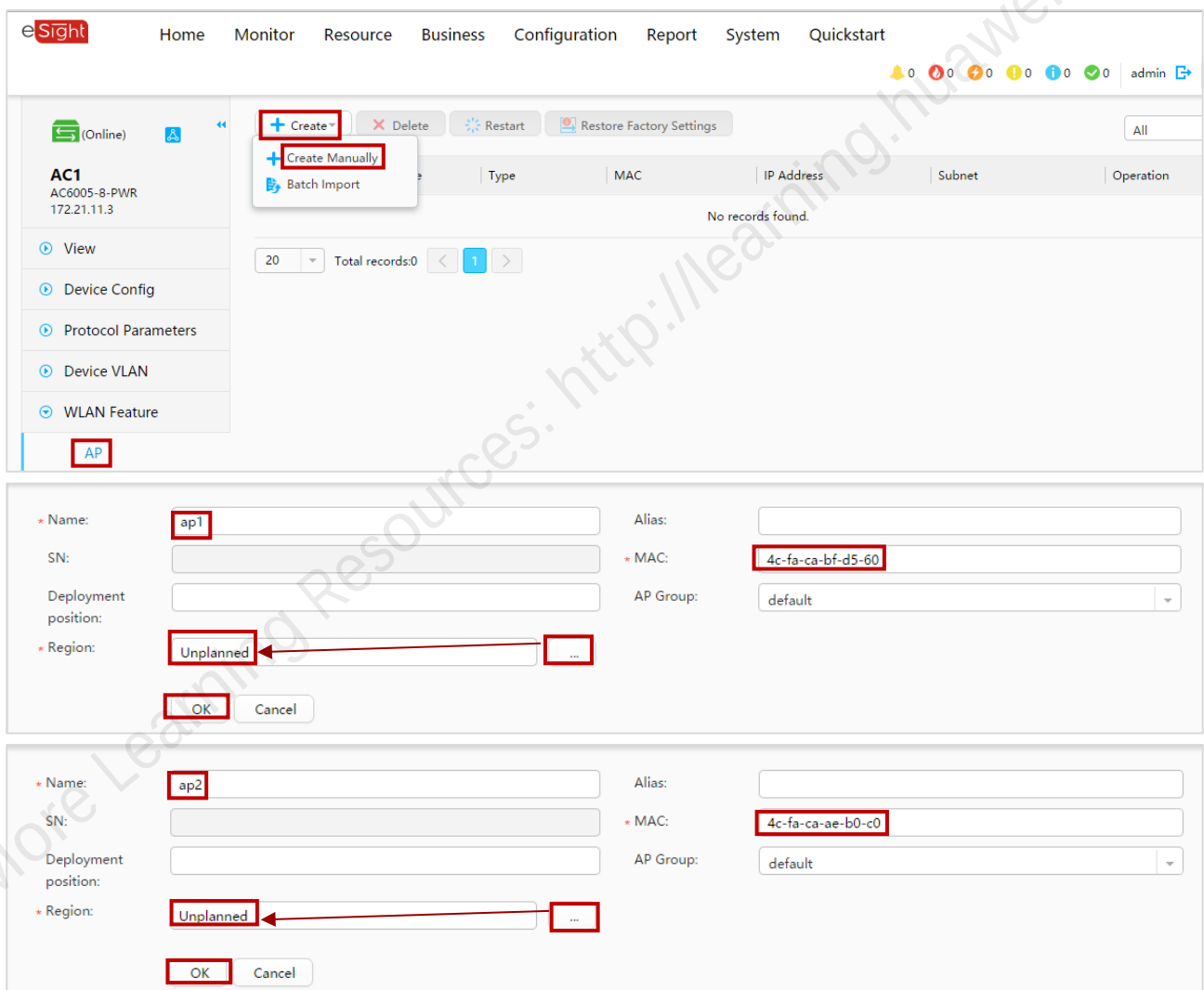
50 Total records:1

Step4 Configuring Basic AC Parameters

Select the pull-down menu "Resource", and click "Network Device".



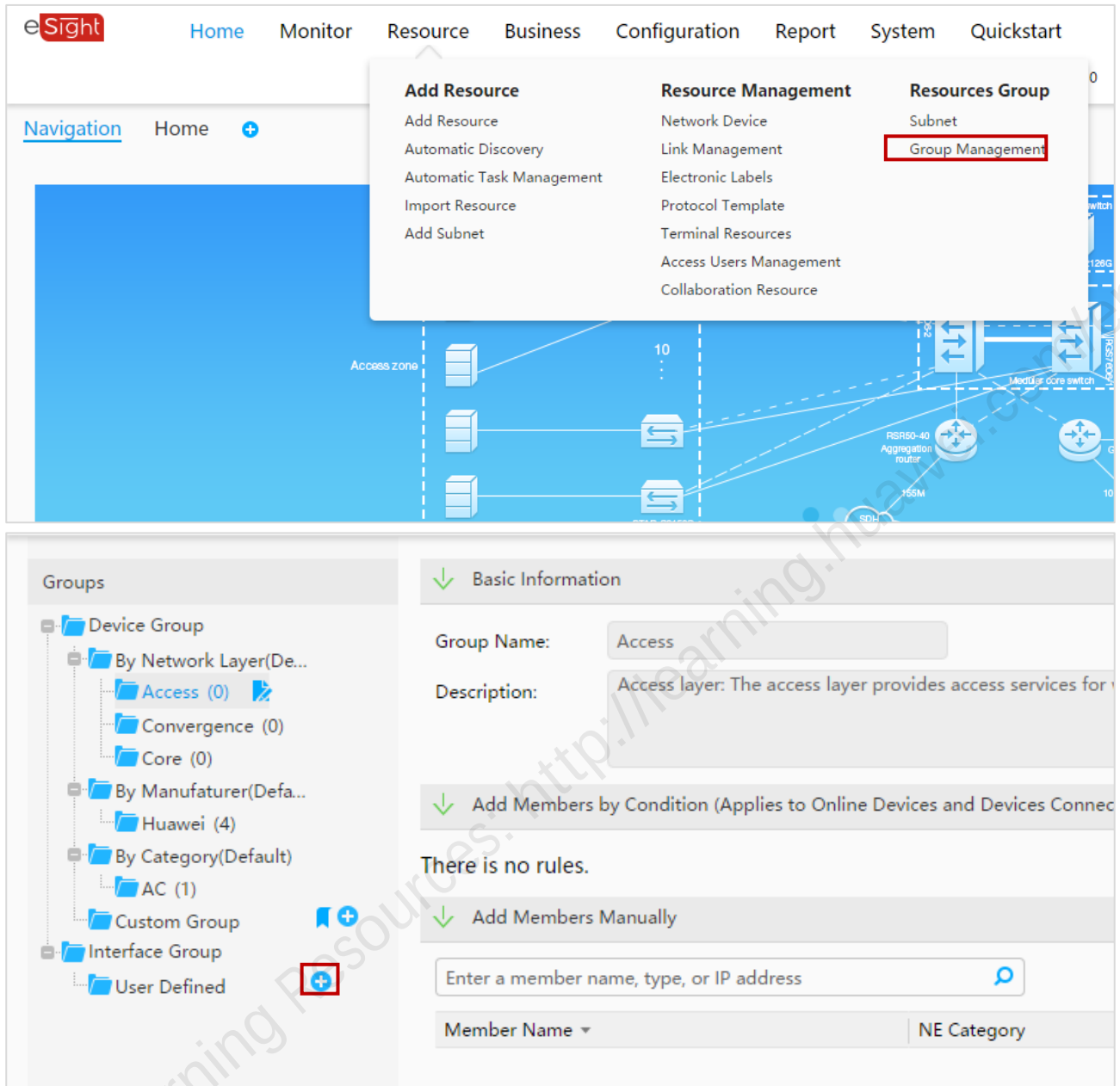
Click "WLAN Feature > AP", enter the Create Manually interface and add aps.



Configure interface Group huaweiX.

Select the pull-down menu "Resource > Resources Group > Group Management"

Click "Interface group > User Defined >  ", and the name for this experiment is "huawei1".



The screenshot displays the eSight network management interface. The top navigation bar includes links for Home, Monitor, Resource, Business, Configuration, Report, System, and Quickstart. The 'Resource' menu is open, showing options like Add Resource, Automatic Discovery, Automatic Task Management, Import Resource, Add Subnet, Resource Management (Network Device, Link Management, Electronic Labels, Protocol Template, Terminal Resources, Access Users Management, Collaboration Resource), and Resources Group (Subnet, Group Management). The 'Group Management' option is highlighted with a red box.

Below the navigation bar, the 'Groups' section on the left shows a tree structure of network groups. The 'User Defined' group is highlighted with a red box. The main panel displays the configuration for the 'Access' group, including a description: 'Access layer: The access layer provides access services for...'. The 'Add Members by Condition' section shows 'There is no rules.' and the 'Add Members Manually' section has a search bar for member names or IP addresses.

Base Info

* Group name:

huawei1

The name is available.

Description:

Group Conditions

satisfy all conditions

satisfy any condition

Dynamic condition:

Device Name

equals

+

Preview All

Group Members

+ Add Members Manually

✕ Delete

Device name, interface name or alias

Member Type	Interface Name	Device Name	Interface Aliasname	Interface Type
No records found.				

10

Total records:0

<

1

>

OK

Cancel

Link Interfaces

10G Interface

AR Cellular

All Interfaces

to select interfaces

All

Interface Name ^	Device Name ^	IP Address ^	Interface Aliasname ^	Interface IP ^	Interface Type
☐ GigabitEthernet0/0/3	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/3..		Ethernet
☐ GigabitEthernet0/0/4	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/4..		Ethernet
☐ GigabitEthernet0/0/5	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/5..		Ethernet
☐ GigabitEthernet0/0/6	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/6..		Ethernet
☐ GigabitEthernet0/0/7	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/7..		Ethernet
☒ GigabitEthernet0/0/8	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/8..		Ethernet

10

Total records:12

<

1

2

>

selected interfaces

Interface Name ^	Device Name ^	IP Address ^	Interface Aliasname ^	Interface IP ^	Interface Type
GigabitEthernet0/0/8	AC1	172.21.11.3	HUAWEI, AC Series, GigabitEthernet0/0/8 Inte...		Ethernet

10

Total records:1

<

1

>

OK

Cancel

华为专有和保密信息
版权所有 © 华为技术有限公司

100

<https://t.me/learningnets>

Base Info

Group name: ✓ The name is available.

Description:

Group Conditions

☒ satisfy all conditions ☐ satisfy any condition

Dynamic condition: equals + Preview All

Group Members

+ Add Members Manually ✗ Delete 🔍

☐	Member Type	Interface Name ^	Device Name ^	Interface Aliasname ^	Interface Type
☐	Add Manually	GigabitEthernet0/0/8	AC1	HUAWEI, AC Series, GigabitEth...	Ethernet

10 Total records:1 < 1 >

OK Cancel

Configure VLANIF and DHCP Server

Select the pull-down menu "Business> WLAN Management> Configuration and Deployment"

eSight Home Monitor Resource Business Configuration Report System Quickstart

Groups

- Device Group
 - By Network Layer(De...
 - Access (0)
 - Convergence (0)
 - Core (0)
 - By Manufacturer(Defa...
 - Huawei (4)
 - By Category(Default)
 - AC (1)
 - Custom Group
 - Interface Group

Network

- BGP/MPLS VPN Management
- MPLS Tunnel Management
- VLAN Management
- Voice Management
- iPCA Management
- SLA Management
- QoS Management
- AR Cellular Interface Management

Network Traffic Analysis

- Traffic Monitor
- Traffic Report
- Traffic Config

WLAN Management

- Configuration and Deployment
- Region Monitor
- Fault Diagnose

Collaboration

- IPPhone Management
- Unified Communications
- Intelligent Video Surveillance
- Telepresence Conference

Dynamic condition: equals + Preview All

Add devices on base configuration.

WLAN Configu...

Base Configuration

VLANIF & Addres...

Channel Configur...

Global AC Configur...

Device of Configuration

+ Add ✗ Delete

☐	Name	IP Address	Operator
No records found.			

Total records:0 < 1 /1 >

By subnet

Available Resource (Total records: 1)

Please input name or IP Addr

Name	IP
☒ AC1	172.21.11.3

All

Clear

Selected Resource (Total records: 1)

Name	IP
AC1	172.21.11.3

OK

Cancel

VLANIF And Address Pool Configure(AC1)

+ Create VLANIF

Delete

Create VLANIF

Batch Create VLANIF

VLANIF	The Address Pool Allocate	Relay IP Address	Operate
169.254.1.1	/ 255.255.0.0	Close	
4090 172.21.11.3	/ 255.255.0.0	Close	

10

Total records:2

< 1 >

Apply

Create VLANIF(AC1)

* VLAN ID:

10

* IP Address/Mask:

10.1.10.100

/

255.255.255.0

Address Pool:

☒ Open ☐ Close

The Address Pool Allocate:

Interface Allocate

Confirm

Cancel

Information

Add VLAN interface may lead to network barrier or device offline, continue?

Yes No

Create VLANIF(AC1)

* VLAN ID: 11

* IP Address/Mask: 10.1.11.100 / 255.255.255.0

Address Pool: ☒ Open ☐ Close

The Address Pool Allocate: Interface Allocate

Confirm Cancel

Information

Add VLAN interface may lead to network barrier or device offline, continue?

Yes No

VLANIF And Address Pool Configure(AC1)

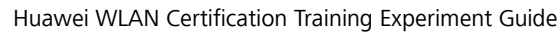
+ Create VLANIF Delete

	VLAN ID	VLANIF	The Address Pool Allocate	Relay IP Address	Operate
☐	1	169.254.1.1 / 255.255.0.0	Close		☐ ☐
☒	10	10.1.10.100 / 255.255.255.0	Interface Alloc...		☐ ☐
☒	11	10.1.11.100 / 255.255.255.0	Interface Alloc...		☐ ☐
☐	4090	172.21.11.3 / 255.255.0.0	Close		☐ ☐

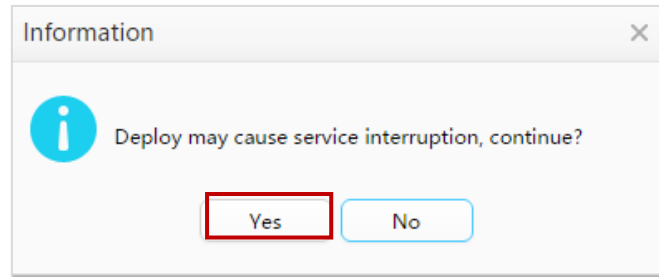
10 Total records:4 < 1 >

Apply

Configure Channel. Click "Base configuration > Channel Configuration ", set the allow pass VLANs and PVID for interface group".



The screenshot shows the 'Select Resource' dialog box. On the left, there is a sidebar with 'Interface Group' selected. The main area is divided into two sections: 'Available Resource (Total records: 1)' and 'Selected Resource (Total records: 1)'. In the 'Available Resource' section, a table has one row with 'Name' 'huawei1' and 'Description' empty. A red box highlights the 'huawei1' name, and a red arrow points from it to the 'Selected Resource' section. In the 'Selected Resource' section, a table also has one row with 'Name' 'huawei1' and 'Description' empty. A red box highlights the 'huawei1' name. At the bottom, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red box. A watermark 'More Learning Resources: http://learning.huawei.com/en' is visible across the image.



Deploy

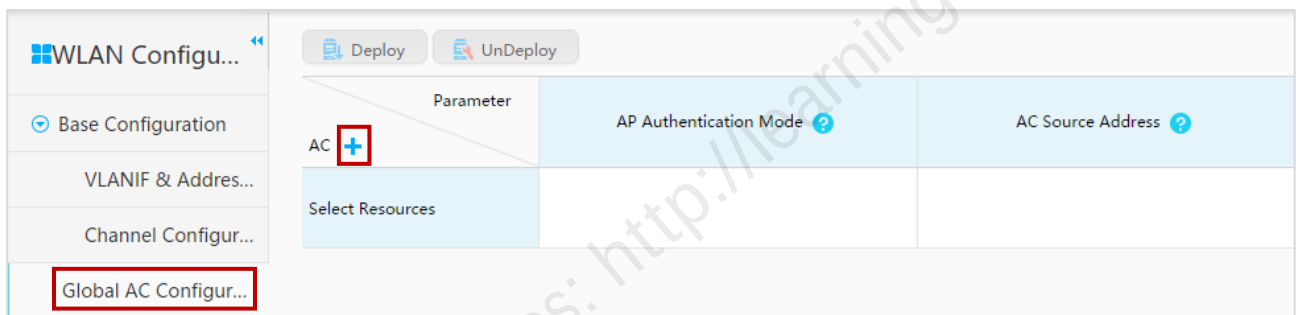
UnDeploy

Parameter	Allow Pass Vlan ?	Default Vlan(PVID) ?	Operation
Interface Group +			
huawei1	10 11 Deploy succeeded.	none Deploy succeeded.	

Step5 Configuring AP Online

Configure AP Authentication mode and AC Source Address.

Click "Global AC Configuration > AC > ", select Resource AC1".



Select Resource

Available Resource (Total records: 1)

Name	Description
☒ AC1	Huawei AC6005-8-PWR Huawei Versatile Routing Plat...

Selected Resource (Total records: 1)

Name	Description
AC1	Huawei AC6005-8-PWR Huawei Versatile Rou... ✗

OK Cancel

WLAN Configu...

Base Configuration

VLANIF & Addres...

Channel Configur...

Global AC Configur...

Deploy UnDeploy

AC +

Parameter	AP Authentication Mode ?	AC Source Address ?
AC1	MAC-mode	Vlanif10
	Undeployed	Undeployed

Information

Deploy may cause service interruption, continue?

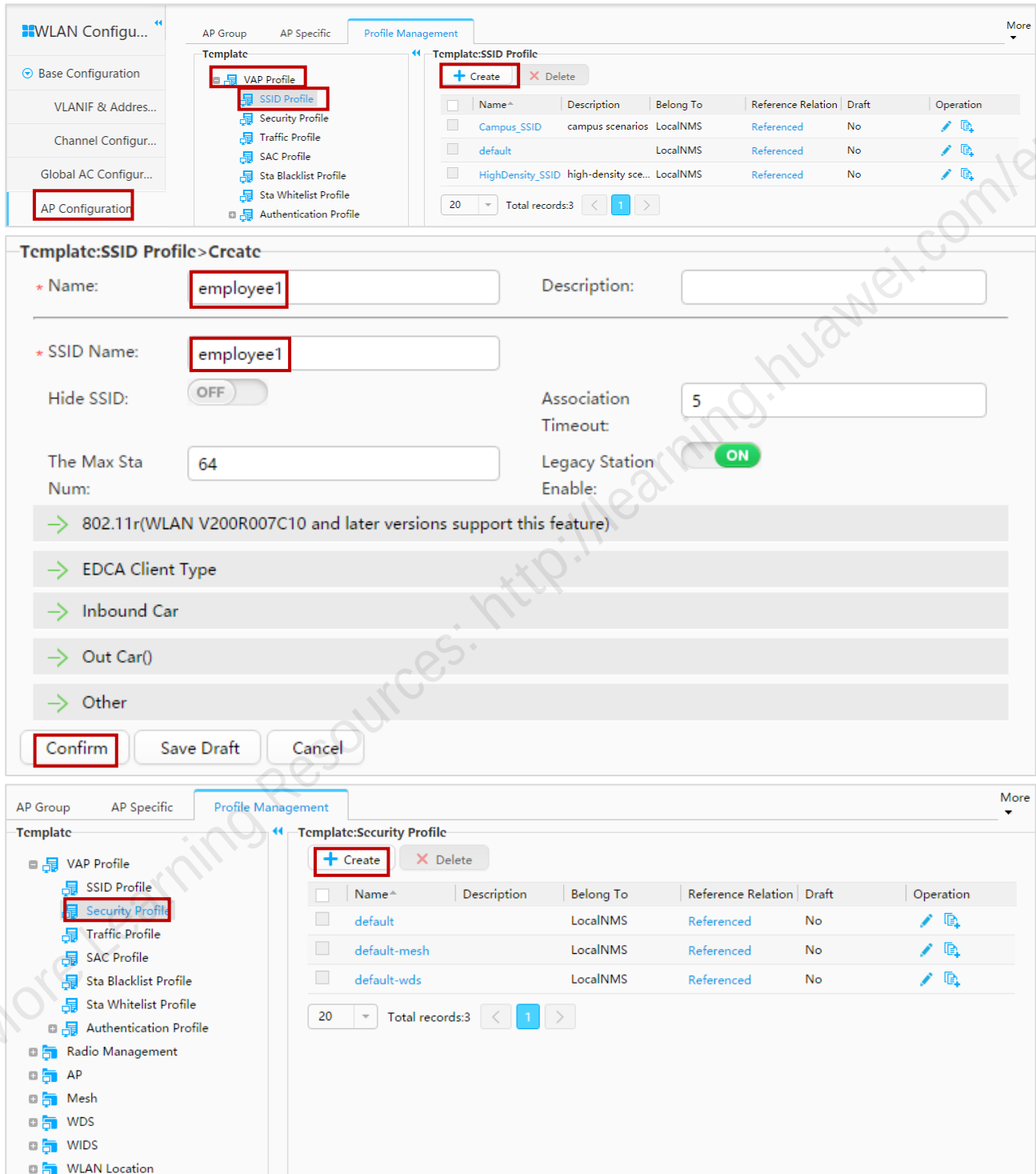
Yes No

Deploy UnDeploy

Parameter	AP Authentication Mode ?	AC Source Address ?	AP Collect time ?	Operation
AC1	✓ MAC-mode	✓ Vlanif10	✓ 5	✗
	Deploy succeeded.	Deploy succeeded.	Deploy succeeded.	

Step6 Configure WLAN Service Parameters

Create Profiles employeeX, Click "AP Configuration > Profile Management > VAP Profile > SSID Profile ", select Create". Configure the security policy for employeeX to WPA2, with the password employee.



The screenshot shows the Huawei WLAN Configuration interface. The left sidebar has a tree view with 'AP Configuration' selected. The main area is divided into two tabs: 'Template' and 'Template:SSID Profile'. In the 'Template' tab, 'VAP Profile' is selected, and 'SSID Profile' is highlighted. In the 'Template:SSID Profile' tab, the 'Create' button is highlighted. Below this, the 'Create' form is shown with the following fields:

- Name: employee1
- SSID Name: employee1
- Hide SSID: OFF
- The Max Sta Num: 64
- Description: (empty)
- Association Timeout: 5
- Legacy Station Enable: ON

Below the form, there are several expandable sections: '802.11r(WLAN V200R007C10 and later versions support this feature)', 'EDCA Client Type', 'Inbound Car', 'Out Car()', and 'Other'. At the bottom, there are 'Confirm', 'Save Draft', and 'Cancel' buttons.

The second part of the screenshot shows the 'Template:Security Profile' tab. The 'Create' button is highlighted. Below this, a table lists the security profiles:

Name	Description	Belong To	Reference Relation	Draft	Operation
default		LocalNMS	Referenced	No	Edit Delete
default-mesh		LocalNMS	Referenced	No	Edit Delete
default-wds		LocalNMS	Referenced	No	Edit Delete

The table has a 'Total records:3' indicator and a '1' button for pagination.

Template:Security Profile>Create

* Name: Description:

Security Policy: ☐ OPEN ☐ WEP ☒ WPA ☐ WPA2 ☐ WPA-WPA2 ☐ WAPI

Authentication Mode: ☒ PSK ☐ DOT1X

Cipher Mode: ☒ AES ☐ TKIP ☐ AES-TKIP

Password Type: ☒ PASS-PHRASE ☐ HEX

* Password: * Confirming Password:

PTK Update: ☒ ON PTK Update Interval(s):

Create VAP profiles employeeX. Set the data forwarding mode for employeeX to tunnel forwarding. Configure the service VLAN and bind the profile to the security profile and SSID profile.

AP Group AP Specific **Profile Management** More

Template

- VAP Profile
- SSID Profile
- Security Profile
- Traffic Profile
- SAC Profile
- Sta Blacklist Profile
- Sta Whitelist Profile
- Authentication Profile
- Radio Management
- AP
- Mesh
- WDS
- WIDS
- WLAN Location
- Bluetooth Location

Template:VAP Profile

Name	Description	Belong To	Reference Relation	Draft	Operation
Campus_VAP	campus scenarios	LocalNMS	Not referenced	No	Edit Delete
default		LocalNMS	Not referenced	No	Edit Delete
HighDensity_VAP	high-density sce...	LocalNMS	Not referenced	No	Edit Delete

20 Total records:3 < 1 >

Template:VAP Profile>Create

* Name: Description:

* Service Mode: ☒ ON

* VAP Type: ☒ Service ☐ AP-Management

* Service VLAN Type: ☒ VLAN ☐ VLAN POOL

* Service VLAN ID:

* Forward Mode: ☐ Direct-forward ☒ Tunnel

MDNS Tunnel Forward: ☐ OFF

Sta Access Mode: ☒ Disable ☐ Blacklist ☐ Whitelist

Band Steer Enable: ☒ ON

Home Agent: ☐ AC ☒ AP

VLAN Mobility Group ID:

Layer 3 roam: ☒ ON

ARP Anti-attack Check: ☐ OFF

IP Binding Check: ☐ OFF

User-bind Enable: ☐ OFF

DHCP Trust Port: ☐ OFF

ND Trust Port: ☐ OFF

Auto-off Service Enable: ☐ OFF

* Security Profile:

* SSID Profile:

* Traffic Profile:

Authentication Profile:

SAC Profile:

→ IP learning

↓ DHCP option insert

DHCP option insert enable: ☐ OFF

Configure AP groups ap-groupX to use the VAP profile.

WLAN Configu...

Base Configuration

VLANIF & Addres...

Channel Configur...

Global AC Configur...

AP Configuration

AP Group AP Specific Profile Management

AP Group Name	Group Members	AC Deployment	VAP Profile	Radio 2.4G Profile
default	0	--	--	default

10 Total records:1 < 1 >

AP Group AP Specific Profile Management More

* AP Group Name:

Copy Parameters From Other:

Profile: [+ Select Resources](#)

AC Deployment:

Modify AP's group maybe cause AP reset.
APs deleted will regroup in default group, using the configuration in default group.

Group Members:

[+ Add](#) [X Delete](#)

Status	Name	MAC	IP Address	SN	Type	AC Name
☐ Offline	ap2	4C-FA-CA-AE-B0-C0				AC1
☐ Offline	ap1	4C-FA-CA-BF-D5-60				AC1

20 Total records:2 [1](#)

OK [Create And Config](#) Cancel

AP Group AP Specific Profile Management

AP Group:

[VAP Profile](#)

- [Radio Management](#)
- [AP](#)
- [Mesh](#)
- [WDS](#)
- [WIDS](#)
- [WLAN Location](#)

VAP Profile List Configuration List

[+ Add](#) [X Remove](#)

Name	WLAN ID	Radio
No records found.		

10 Total records:0 [1](#)

VAP Profile List Configuration List

* VAP Profile: * WLAN ID:

* Radio: ?

[Confirm](#) [Cancel](#)

Deploy

Warning: Modify configuration may cause service interruption, The configuration will deploy to following device, continue?

☐ Deployment based on latest device configuration (Device configuration is synchronized before deployment, and command will be executed)

☐ Full deployment

AC Deployment	Deploy progress	Details
AC1		

[Deploy](#) [Cancel](#)

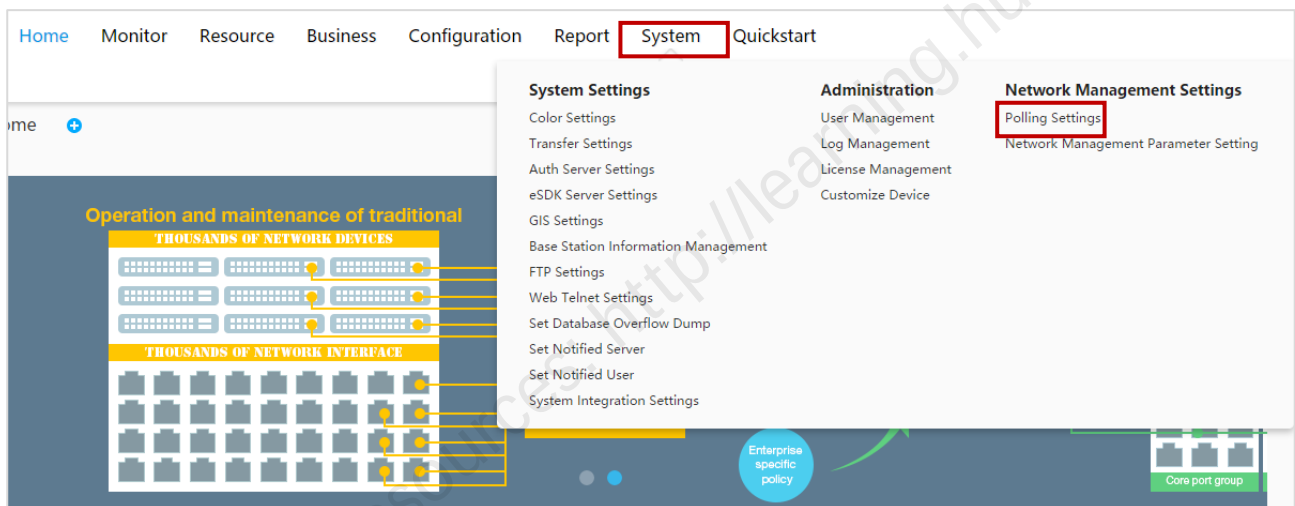
After finish above, ap still not online. Configure the function of ssh for AC, and test the SFTP for eSight. Username: admin, password: Changeme123.

```
[AC6005]ssh client first-time enable
[AC6005]sftp 172.21.0.11 31922
Please input the username:admin
Trying 172.21.0.11 ...
Press CTRL+K to abort
The server is not authenticated. Continue to access it? (y/n) [n]:y
Save the server's public key? (y/n) [n]:y
The server's public key will be saved with the name 172.21.0.11. Please wait...
```

Enter password:

sftp-client>

Click "System > Network Management Settings > Polling Settings". Configure Polling interval, make the AP online.



Network Manag...

Polling Settings

Network Management...

Resource Inventory Polling

☐ IP Address Polling interval (minute): 60

☒ Scheduled synchronization time: 02 : 20

Interface Status Polling

☒ Link interface Polling interval (minute): 5

☐ All interface Polling interval (minute): 60

☐ Base Station Polling interval (minute): 60

☐ AR Cellular Polling interval (minute): 15

WLAN Info Polling

☒ AP Info Polling interval(minute): 15

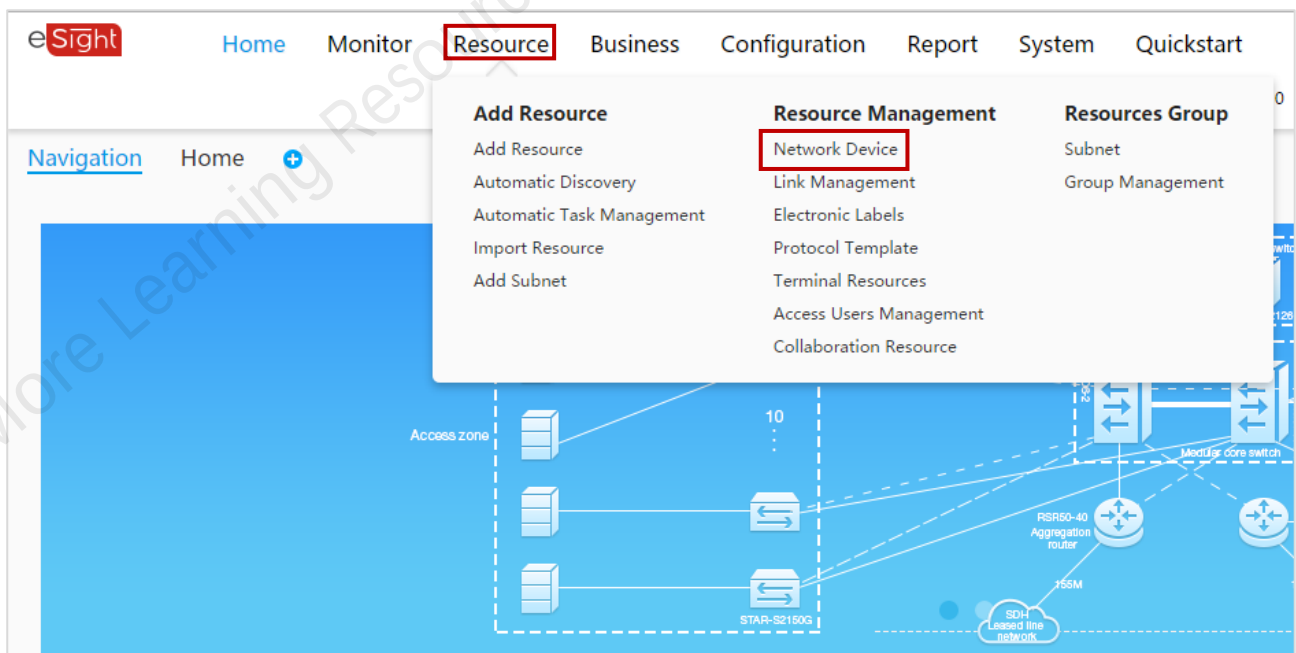
☒ Wlan Stock Info Polling interval(minute): 30

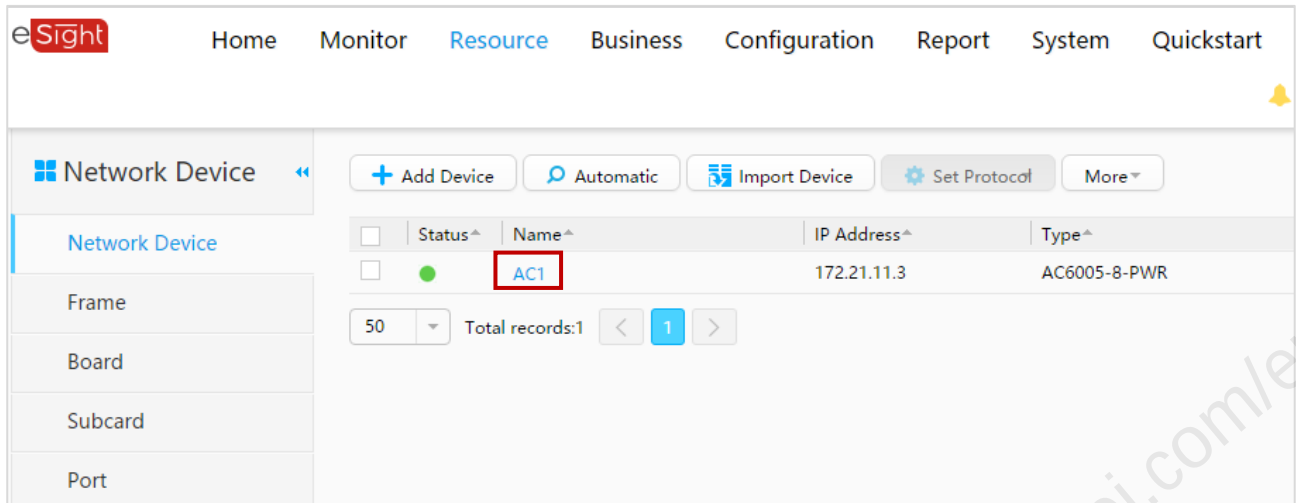
User Info Polling

☒ User Info Polling interval(minute): 15

Apply

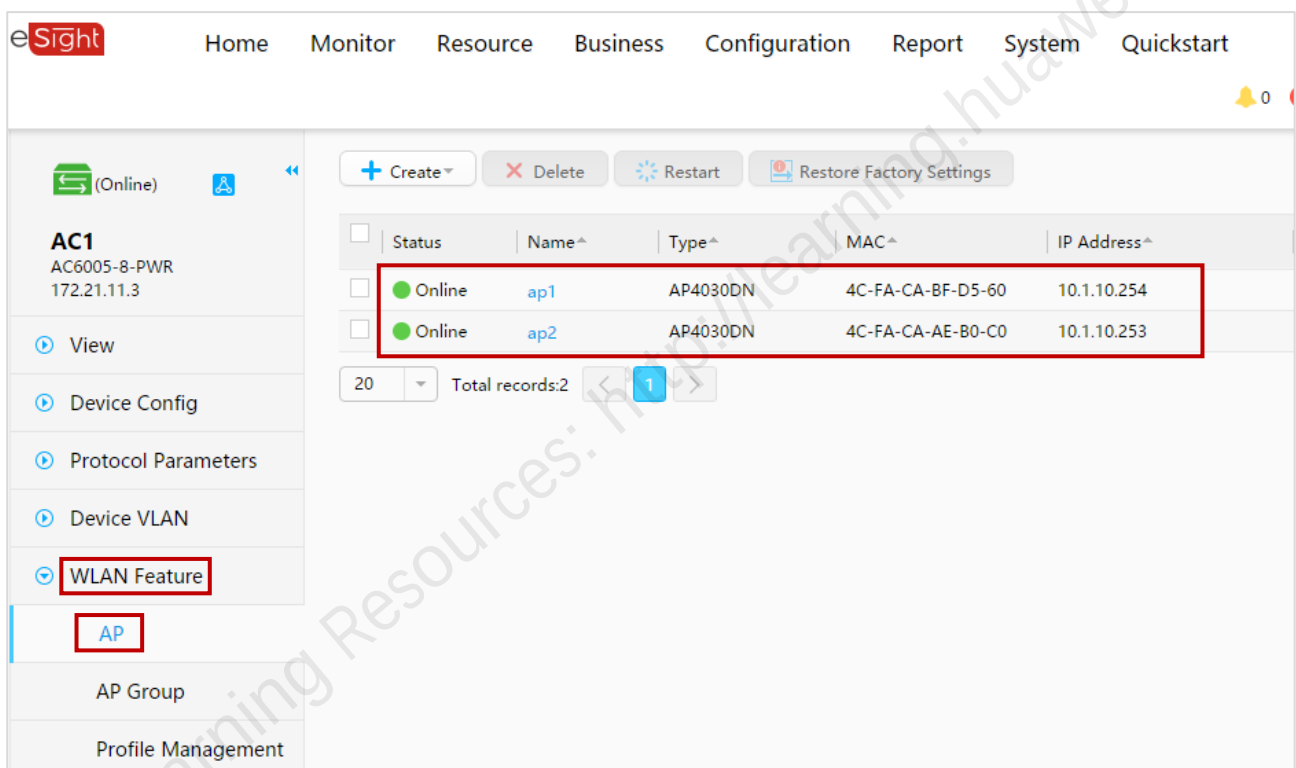
Check the AP Status and two Aps are online.





The screenshot shows the eSight Network Device Management interface. The left sidebar has a 'Network Device' section with a list of devices. The main area displays a table of network devices. The first device, 'AC1', is highlighted with a red box. The table has columns for Status, Name, IP Address, and Type.

Status	Name	IP Address	Type
Online	AC1	172.21.11.3	AC6005-8-PWR



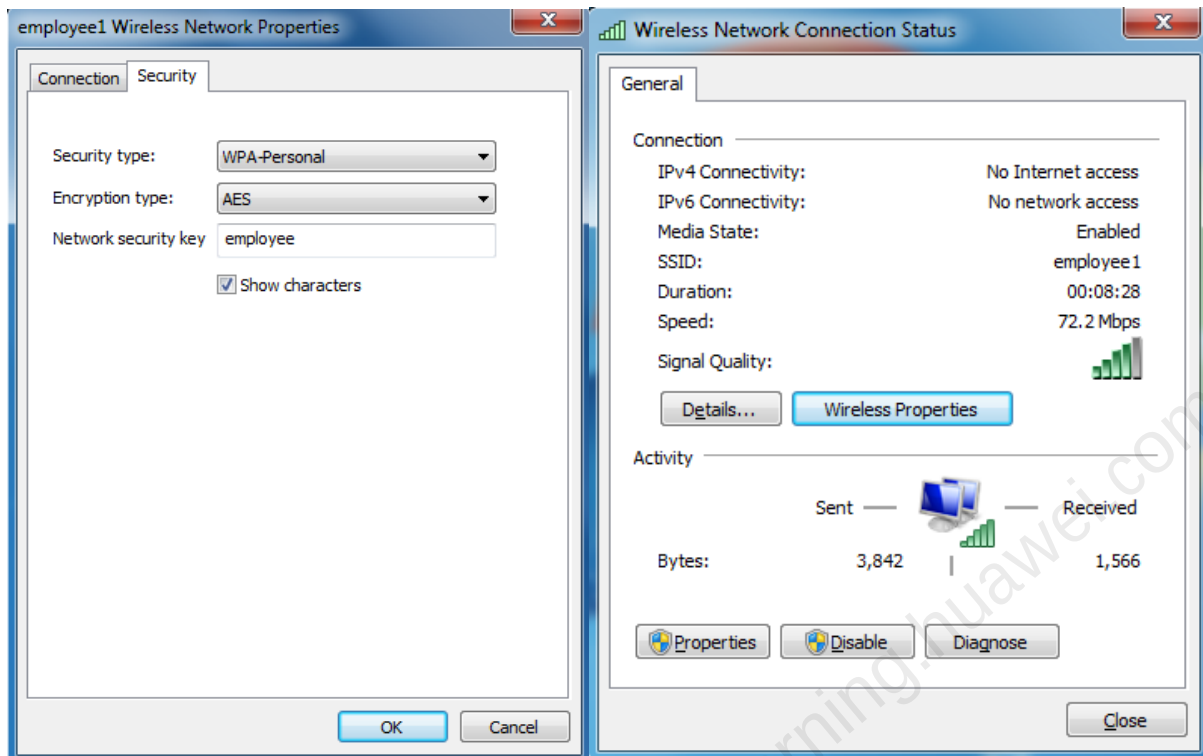
The screenshot shows the eSight WLAN Feature Configuration interface. The left sidebar has a 'WLAN Feature' section with a list of features. The main area displays a table of WLAN features. The first two rows, 'ap1' and 'ap2', are highlighted with a red box. The table has columns for Status, Name, Type, MAC, and IP Address.

Status	Name	Type	MAC	IP Address
Online	ap1	AP4030DN	4C-FA-CA-BF-D5-60	10.1.10.254
Online	ap2	AP4030DN	4C-FA-CA-AE-B0-C0	10.1.10.253

4.3 Verification

4.3.1 Connect an STA to the WLAN

Connect STAs to the WLANs with SSIDs employeeX.



```
C:\Users\zWX>ping 101.101.101.101
PING 101.101.101.101: 56 data bytes, press CTRL_C to break
    Reply from 101.101.101.101: bytes=56 Sequence=1 ttl=255 time=7 ms
    Reply from 101.101.101.101: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 101.101.101.101: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 101.101.101.101 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 7/9/10 ms
```

4.4 Reference Configuration

4.4.1 S5700 Configuration

```
#
sysname S5700
#
vlan batch 10 to 13 200
#
lldp enable
#
undo http server enable
```

```
undo http secure-server enable
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@@5d~9:M^ipCfL\iB)EQd>3Uwe%@@@
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
 ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
 ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
 ip address 10.1.13.1 255.255.255.0
#
interface Vlanif200
 ip address 10.254.1.1 255.255.255.0
#
interface MEth0/0/1
 ip address 172.21.11.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
 port link-type trunk
```

```
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/11
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
port link-type trunk
port default vlan 200
#
interface NULL0
#
interface LoopBack1
ip address 101.101.101.101 255.255.255.255
#
user-interface con 0
authentication-mode password
set authentication password
cipher %@@%;|J%=/[d[O@L[qD[Xhh~,3[~S(Zs:\Ot8H6*x_MAW=N$3[B,%@@@
user-interface vty 0 4
authentication-mode password
user privilege level 3
set authentication password
cipher %@@@`KL`QN[h79h[6AS2ggdT<+Hjaz5lH\hpS4]~^/-CFvtO+Hm<%@@@
protocol inbound all
user-interface vty 16 20
#
return
```

4.4.2 AC Configuration

```
#
 sysname AC1
#
 http secure-server ssl-policy default_policy
 http server enable
#
 portal local-server ip 10.1.10.100
 portal local-server https ssl-policy default_policy port 2000
#
 undo portal url-encode enable
#
 ssl renegotiation-rate 1
#
 vlan batch 10 to 13 4090
#
 authentication-profile name default_authen_profile
 authentication-profile name dot1x_authen_profile
 authentication-profile name mac_authen_profile
 authentication-profile name portal_authen_profile
 portal-access-profile guest1
 authentication-profile name macportal_authen_profile
 authentication-profile name guest1
 portal-access-profile guest1
 authentication-profile name employee1
 dot1x-access-profile employee1
 authentication-scheme radius
 radius-server huawei
#
 lldp enable
#
 dhcp enable
#
 diffserv domain default
#
 radius-server template default
 radius-server template huawei
 radius-server authentication 10.254.1.100 1812 source ip-address
 10.1.10.100 weight 80
 undo radius-server user-name domain-included
#
 pki realm default
 rsa local-key-pair default
 enrollment self-signed
#
 ssl policy default_policy type server
```

```
pki-realm default
version tls1.0 tls1.1
ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
encryption-algorithm aes-256
dh group2
authentication-algorithm sha2-256
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
portal local-server enable
#
portal-access-profile name guest1
portal local-server enable
#
ip pool ap
gateway-list 10.1.10.1
network 10.1.10.0 mask 255.255.255.0
option 43 sub-option 3 ascii 10.1.10.100
#
ip pool employee1
gateway-list 10.1.11.1
network 10.1.11.0 mask 255.255.255.0
dns-list 114.114.114.114
#
ip pool voicel
gateway-list 10.1.12.1
network 10.1.12.0 mask 255.255.255.0
#
ip pool guest1
gateway-list 10.1.13.1
network 10.1.13.0 mask 255.255.255.0
#
aaa
authentication-scheme default
authentication-scheme radius
authentication-mode radius
authorization-scheme default
accounting-scheme default
domain default
authentication-scheme default
domain default_admin
authentication-scheme default
```

```
local-user admin password irreversible-cipher $1a$VNcE$6oR"2$aSkVyC1-
~qx^~!e+:.S|>BJto>%VV[WvDxK./G$
local-user admin privilege level 15
local-user admin service-type ssh http
local-user huawei password irreversible-cipher
$1a$6@(!=HT_IP$A=lvP*~iu+0<..Y&4`Y6+j4$Xkcf=#aMU=5[4wEP$
local-user huawei privilege level 1
local-user huawei service-type telnet ssh http
local-user guest01 password cipher %^%#h)q(D@"^~3lbX|<1Hk1L#bj]RY3-
pAYq#XEVAp>~%^%#
local-user guest01 privilege level 0
local-user guest01 service-type web
#
interface Vlanif1
ip address 169.254.1.1 255.255.0.0
#
interface Vlanif10
ip address 10.1.10.100 255.255.255.0
dhcp select global
#
interface Vlanif11
ip address 10.1.11.100 255.255.255.0
dhcp select global
#
interface Vlanif12
ip address 10.1.12.100 255.255.255.0
dhcp select global
#
interface Vlanif13
ip address 10.1.13.100 255.255.255.0
dhcp select global
#
interface Vlanif4090
ip address 172.21.11.3 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
```

```
port link-type access
port default vlan 4090
stp disable
#
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
info-center timestamp log format-date
#
snmp-agent local-engineid 800007DB03845B12566919
snmp-agent community
read %^%#En_g+AWfX>adWz&5.!G~E^)4&/r]vCScEB~w~u%Zje-
$@`GH0BN7e"$A8PF(_n~lC9qvT)O*{4!I+:yR%^%#
snmp-agent community write %^%#atYiX7&TjG<o\Y/.2Y-
V/8bVI&sGJOTB4$0Y@{"2$306$`dp;=7cULM)*$.3Q!lXY<}!y7jZ,7BS"NNY%^%#
snmp-agent sys-info version v2c
snmp-agent
#
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh server secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh client secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh client key-exchange dh_group14_sha1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
capwap source interface vlanif10
#
user-interface con 0
authentication-mode password
set authentication password
cipher %^%#1<n6!"VC7VQQj=/vGNXG}:Eu&6zT3'C<qU9G'>N8A~"fK_+WA~0De+C]/yW"%^
%#
user-interface vty 0 4
authentication-mode aaa
user privilege level 3
protocol inbound telnet
user-interface vty 16 20
protocol inbound all
#
```

```
wlan
traffic-profile name default
security-profile name guest1
security-profile name voice1
security wpa psk pass-
phrase ^%#0)RfPJm>L58cY+4*K);#E~]V)7`\406bJM4syy*%^%# tkip
security-profile name default
security-profile name employee1
security wpa2 dot1x aes
security-profile name default-wds
security wpa2 psk pass-phrase ^%#CB&>,Q$BB>x\Fn"|^%qToSj.2]:%J"+-
qK%aTJ_0%^%# aes
security-profile name default-mesh
security wpa2 psk pass-phrase ^%#]7|J"LHnEQ=-
GJS[q&>M">Qsqw;9mb8$0`_=6I%^%# aes
ssid-profile name guest1
ssid guest1
ssid-profile name voice1
ssid voice1
ssid-profile name default
ssid-profile name employee1
ssid employee1
vap-profile name guest1
forward-mode tunnel
service-vlan vlan-id 13
ssid-profile guest1
security-profile guest1
authentication-profile portal_authen_profile
vap-profile name voice1
service-vlan vlan-id 12
ssid-profile voice1
security-profile voice1
vap-profile name default
vap-profile name employee1
service-vlan vlan-id 11
ssid-profile employee1
security-profile employee1
authentication-profile employee1
mesh-handover-profile name default
mesh-profile name default
wds-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
```

```
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
vap-profile guest1 wlan 3
radio 1
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
vap-profile guest1 wlan 3
radio 2
vap-profile employee1 wlan 1
vap-profile voice1 wlan 2
vap-profile guest1 wlan 3
ap-id 0 type-id 43 ap-mac 4cfa-cabe-eb60 ap-sn 21500826412SG8918066
ap-group ap-group1
ap-id 1 type-id 43 ap-mac 4cfa-cabf-d0c0 ap-sn 21500826412SG8919901
ap-group ap-group1
provision-ap
#
dot1x-access-profile name dot1x_access_profile
dot1x-access-profile name employee1
#
mac-access-profile name mac_access_profile
#
undo ntp-service enable
#
return
```

5

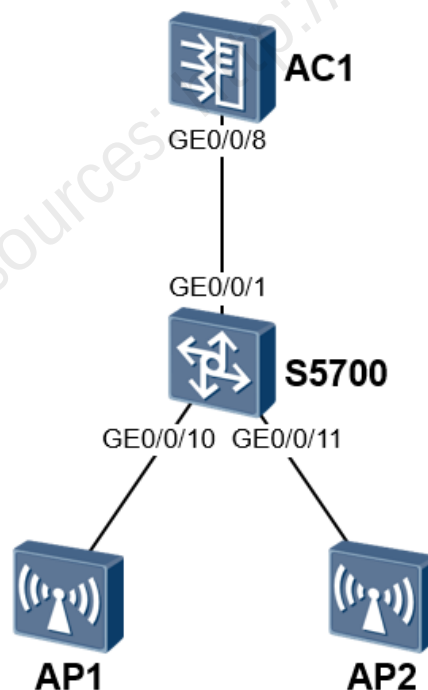
Experiment 5: Layer 3 Networking Experiment

5.1 About This Course

5.1.1 Objectives

- Understand the L3 networking structure
- Configure L3 networking device
- Configure tunnel forwarding
- Verify the configuration

5.1.2 Topology



5.1.3 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

The following table describes device connections.

Group No.	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	- AP1-G0/0/10 - AP2-G0/0/11
2	AC2—G0/0/2	- AP3-G0/0/12 - AP4-G0/0/13
3	AC3—G0/0/3	- AP5-G0/0/14 - AP6-G0/0/15
4	AC4—G0/0/4	- AP7-G0/0/15 - AP8-G0/0/16
5	AC5—G0/0/5	- AP9-G0/0/17 - AP10-G0/0/18
6	AC6—G0/0/6	- AP11-G0/0/19 - AP12-G0/0/20

The following table describes an AC parameter configuration template.

Trainee Group X	AC Configuration	
Console Port Login Password	Admin@123	
Device	ACX	
AP Management VLAN	VLAN: X0	IP: 10.1.X0.100
Service VLAN (Employee)	VLAN: X1	IP: 10.1.X1.100
Service VLAN (Voice)	VLAN: X2	IP: 10.1.X2.100
Service VLAN (Guest)	VLAN: X3	IP: 10.1.X3.100
AC Source interface (L3 Networking)	VLANif 80X	IP: 10.1.20X.100

Topology: layer2 and layer 3 bypass topology

5.2 Experiment Task

5.2.1 Configuration Procedure

Step1 Configuring a Switch

Configure the VLAN and Trunk on switch S5700, set the VLANIF80X ip address.

```
[S5700]vlan batch 801
[S5700]int GigabitEthernet 0/0/1
[S5700-GigabitEthernet0/0/1]port trunk allow-pass vlan 801
[S5700-GigabitEthernet0/0/1]quit

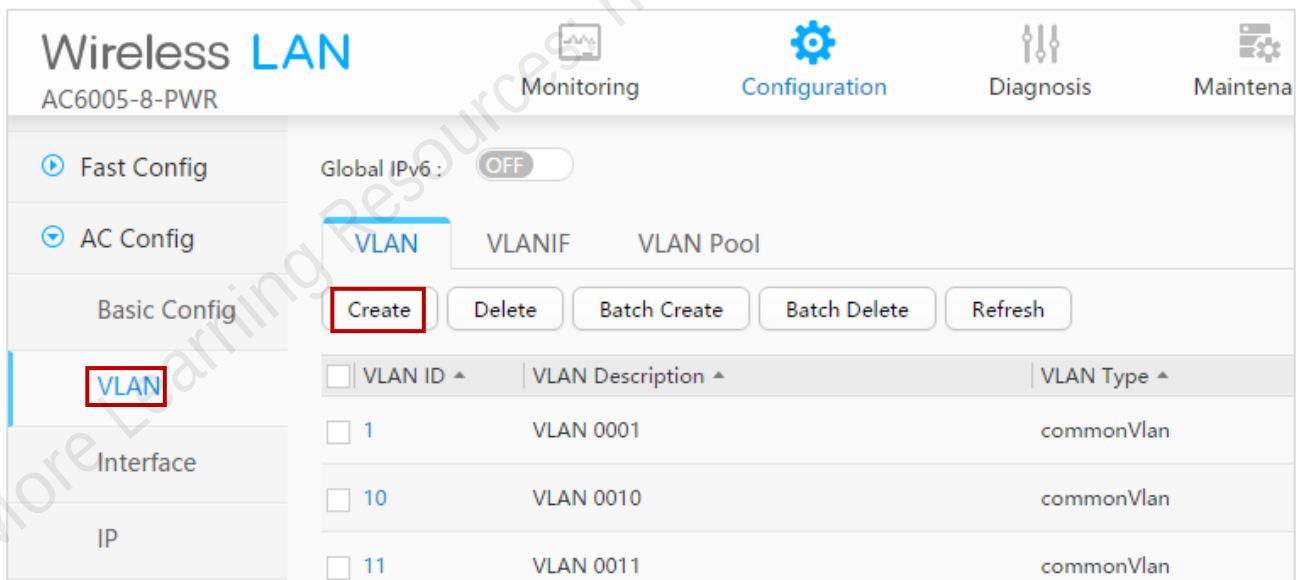
[S5700]int Vlanif 801
[S5700-Vlanif801]ip address 10.1.201.1 24
[S5700-Vlanif801]quit
```

Step2 Configuring Basic AC Parameters

Update the VLAN and Trunk Configuration, and set the VLANIF80X ip address.

Choose "Configuration > AC Config > VLAN", enter the VLAN page.

Click create, add VLAN80x.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Config Basic Config VLAN Interface IP

Global IPv6: OFF

VLAN VLANIF VLAN Pool

Create Delete Batch Create Batch Delete Refresh

VLAN ID	VLAN Description	VLAN Type
1	VLAN 0001	commonVlan
10	VLAN 0010	commonVlan
11	VLAN 0011	commonVlan

AC Config > VLAN > VLAN > Create VLAN

*VLAN ID : Description :

Select Interface

Available Interface List

☐ Interface Name
☐ GigabitEthernet0/0/1
☐ GigabitEthernet0/0/2
☐ GigabitEthernet0/0/3
☐ GigabitEthernet0/0/4
☐ GigabitEthernet0/0/5
☐ GigabitEthernet0/0/6
☐ GigabitEthernet0/0/7

Added Interface List

☐ Interface Name	Mode
☐ GigabitEthernet0/0/8	tagged

>

<

☒ Create VLANIF

Description :

IP address format : ☒ IPv4 ☐ IPv6

IPv4 address/mask :

Step3 Configuring AP Online

Modify DHCP configuration and WLAN configuration, make AP can discover AC.

Choose "Configuration > AC Config > IP > DHCP Address pool", enter DHCP Address pool page.

Click AP address pool, modify optionparameter.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config DHCP Address Pool DHCP Relay NAT Route

AC Config

DHCP status: **ON**

Basic Config

VLAN

Interface

IP

Address Pool List

Create Delete Display Address Pool Refresh

Address Pool Name	Subnet Address	Subnet Mask	Gateway IP	Lease
ap	10.1.10.0	255.255.255.0	<10.1.10.1>	1 Day 0 Hour 0 Minute
employee1	10.1.11.0	255.255.255.0	<10.1.11.1>	1 Day 0 Hour 0 Minute

AC Config > IP > DHCP Address Pool > Modify DHCP Address Pool

* Address pool type: ☒ Global address pool ☐ Interface address pool

* Address pool name: ap

* Subnet address: 10 . 1 . 10 . 0

* Subnet mask: 24(255.255.255.0)

Vendor-defined: sub-option

3 ascii 10.1.201.100

Advanced

OK Cancel

Modify AC source address.

Choose "Configuration > ACConfig > Basic Config > AC Configuration", enter AC configuration page.

Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Fast Config AC Configuration Radio Calibration

AC Config

Basic Config

VLAN

Interface

IP

AP Config

Security

AC source address: ☒ VLANIF ☐ LoopBack ☐ IP address

Vlanif801

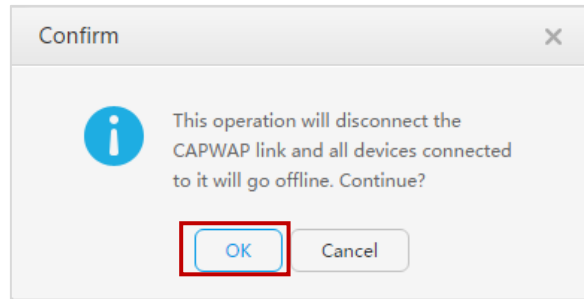
AP data buffer: OFF

AP authentication mode: MAC address authentication

IPv6 services for STAs: OFF

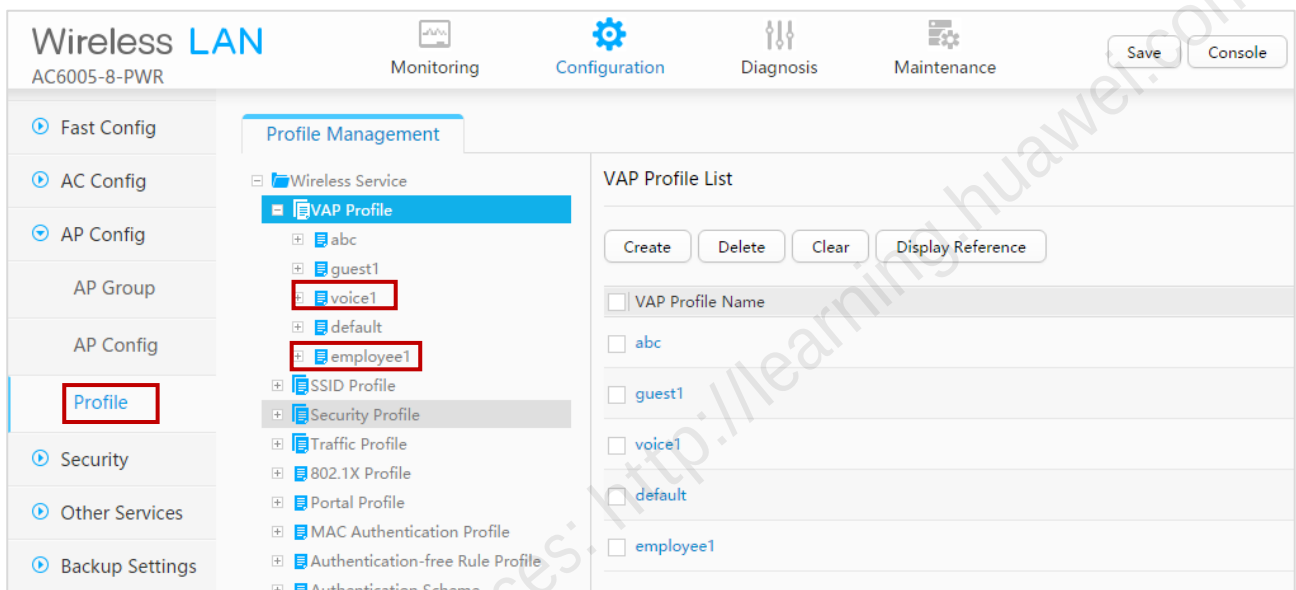
Advanced

Apply



Choose "Configuration > AP Config > Profile > Wireless Service", enter Wireless Service page.

Click VAPprofile, modify employee and voiceX forwarding mode to tunnel.



VAP Profile : voice1 Display Reference

Status : ☒ ON VAP type : Service VAP

Service VLAN : ☒ Single VLAN ☐ VLAN Pool Service VLAN ID : 12

Forwarding mode : Tunnel

Band steering : ☒ ON

Home agent : ☐ AC ☒ AP Roaming domain ID : 1

Layer 3 roaming : ☒ ON

ARP probe : ☐ OFF IP binding check : ☐ OFF

IP learning : ☒ ON

Strict IP learning : ☐ IPv4 ☐ IPv6

DHCP trusted port : ☐ OFF ND trusted port : ☐ OFF

Appending Option 82 : ☐ OFF

Effective after logout : ☐ OFF

Disable VAP periodically : ☐ OFF

Broadcast flood attack detection : ☒ ON

Broadcast attack threshold(pps) : 10 Adding attackers to the blacklist : ☐ OFF

Apply

Confirm

 Modifying forward mode may cause service interruption. Continue?

OK Cancel

VAP Profile : employee1 Display Reference

Status : ON VAP type : Service VAP

Service VLAN : ☒ Single VLAN ☐ VLAN Pool Service VLAN ID : 11

Forwarding mode : Tunnel

Band steering : ON

Home agent : ☐ AC ☒ AP Roaming domain ID : 1

Layer 3 roaming : ON

ARP probe : OFF IP binding check : OFF

IP learning : ON

Strict IP learning : ☐ IPv4 ☐ IPv6

DHCP trusted port : OFF ND trusted port : OFF

Appending Option 82 : OFF

Effective after logout : OFF

Disable VAP periodically : OFF

Broadcast flood attack detection : ON

Broadcast attack threshold(pps) : 10 Adding attackers to the blacklist : OFF

Apply

Confirm

i Modifying forward mode may cause service interruption. Continue?

OK Cancel

5.3 Verification

5.3.1 Verify the L3 Network Status

Then the Configuration of L3 Network has been finished, all Aps are online.

```
[AC1]display ap all
```



Info: This operation may take a few seconds. Please wait for a moment.done.

Total AP information:

nor : normal [2]

ID	MAC	Name	Group	IP	Type	State	STA	Uptime
0	4cfa-cabe-eb60	ap1	ap-group1	10.1.10.253	AP4030DN	nor	0	6S
1	4cfa-cabf-d0c0	ap2	ap-group1	10.1.10.254	AP4030DN	nor	1	26S

Total: 2

Check the station information.

[AC1]display station all

Rf/WLAN: Radio ID/WLAN ID

Rx/Tx: link receive rate/link transmit rate(Mbps)

STA MAC address	SSID	AP ID	Ap name	Rf/WLAN	Band	Type	Rx/Tx	RSSI	VLAN	IP
1041-7f67-01b1	voice1	0	ap1	0/2	2.4G	11g	35/46	-64	12	

Total: 1 2.4G: 1 5G: 0

5.4 Reference Configuration

5.4.1 S5700 Configuration

```
#
sysname S5700
#
vlan batch 10 to 13 200 801
#
lldp enable
#
undo http server enable
undo http secure-server enable
#
undo nap slave enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@@5d~9:M^ipCfL\iB)EQd>3Uwe%@@@
```

```
local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
ip address 10.1.13.1 255.255.255.0
#
interface Vlanif200
ip address 10.254.1.1 255.255.255.0
#
interface Vlanif801
ip address 10.1.201.1 255.255.255.0
#
interface MEth0/0/1
ip address 172.21.11.1 255.255.0.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 10 to 13 801
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/11
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
```

```
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
port link-type trunk
port default vlan 200
#
interface NULL0
#
interface LoopBack1
ip address 101.101.101.101 255.255.255.255
#
user-interface con 0
authentication-mode password
set authentication password
cipher %@@@;|J%=/[d[O@L[qD[Xhh~,3[~S{Zs:\Ot8H6*x_MAW=N$3[B,%@@@
user-interface vty 0 4
authentication-mode password
user privilege level 3
set authentication password
cipher %@@@`KL`QN[h79h[6AS2ggdT<+Hjaz5lH\hpS4]~^/-CFvtO+Hm<%@@@
protocol inbound all
user-interface vty 16 20
#
return
```

5.4.2 AC Configuration

```
#
sysname AC1
#
http secure-server ssl-policy default_policy
http server enable
```

```
#
portal local-server ip 10.1.10.100
portal local-server https ssl-policy default_policy port 2000
#
undo portal url-encode enable
#
ssl renegotiation-rate 1
#
vlan batch 10 to 13 801 4090
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
portal-access-profile guest1
authentication-profile name macportal_authen_profile
authentication-profile name guest1
portal-access-profile guest1
authentication-profile name employee1
dot1x-access-profile employee1
authentication-scheme radius
radius-server huawei
#
lldp enable
#
dhcp enable
#
diffserv domain default
#
radius-server template default
radius-server template huawei
radius-server authentication 10.254.1.100 1812 source ip-address
10.1.10.100 weight 80
undo radius-server user-name domain-included
#
pki realm default
rsa local-key-pair default
enrollment self-signed
#
ssl policy default_policy type server
pki-realm default
version tls1.0 tls1.1
ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
encryption-algorithm aes-256
dh group2
authentication-algorithm sha2-256
authentication-method pre-share
integrity-algorithm hmac-sha2-256
prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
```

```
portal local-server enable
#
portal-access-profile name guest1
portal local-server enable
#
ip pool ap
gateway-list 10.1.10.1
network 10.1.10.0 mask 255.255.255.0
option 43 sub-option 3 ascii 10.1.201.100
#
ip pool employee1
gateway-list 10.1.11.1
network 10.1.11.0 mask 255.255.255.0
dns-list 114.114.114.114
#
ip pool voice1
gateway-list 10.1.12.1
network 10.1.12.0 mask 255.255.255.0
#
ip pool guest1
gateway-list 10.1.13.1
network 10.1.13.0 mask 255.255.255.0
#
aaa
authentication-scheme default
authentication-scheme radius
authentication-mode radius
authorization-scheme default
accounting-scheme default
domain default
authentication-scheme default
domain default_admin
authentication-scheme default
local-user admin password irreversible-cipher $1a$VNcE$6oR"2$aASkVyC1-
~~qx^~!e+:.S|>BJto>%VV[WvDxK./G$
local-user admin privilege level 15
local-user admin service-type ssh http
local-user huawei password irreversible-cipher
$1a$6@(!=HT_IP$A=lvP*~iu+0<..Y&4`Y6+j4$Xkcf=#aMU=5[4wEP$
local-user huawei privilege level 1
local-user huawei service-type telnet ssh http
local-user guest01 password cipher %^%#h)q(D@""^~3lbX|<1Hk1L#bj]RY3-
pAYq#XEVAp>~%^^#
local-user guest01 privilege level 0
local-user guest01 service-type web
#
interface Vlanif1
ip address 169.254.1.1 255.255.0.0
#
interface Vlanif10
ip address 10.1.10.100 255.255.255.0
dhcp select global
#
interface Vlanif11
ip address 10.1.11.100 255.255.255.0
```

```
dhcp select global
#
interface Vlanif12
ip address 10.1.12.100 255.255.255.0
dhcp select global
#
interface Vlanif13
ip address 10.1.13.100 255.255.255.0
dhcp select global
#
interface Vlanif801
ip address 10.1.201.100 255.255.255.0
#
interface Vlanif4090
ip address 172.21.11.3 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
port link-type access
port default vlan 4090
stp disable
#
interface GigabitEthernet0/0/8
port link-type trunk
port trunk allow-pass vlan 10 to 13 801
#
interface NULL0
#
info-center timestamp log format-date
#
snmp-agent local-engineid 800007DB03845B12566919
snmp-agent community
read ^%#En_g+AWfX>adWz&5.!G~E^ )4&/r]vCSCEB~w~u%Zje-
$@`GH0BN7e"$A8PF(_n~lC9qvT)O*{4!I+:yR%^%#
snmp-agent community write ^%#atYiX7&TjG<o\Y/.2Y-
V/8bVI&sGJOTB4$0Y@{"2$306$`dp;=7cULM)*$.3Q!lXY<}!y7jZ,7BS"NNY%^%#
snmp-agent sys-info version v2c
snmp-agent
#
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh server secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh server key-exchange dh_group14_sha1
```

```
ssh client secure-algorithms cipher aes256_ctr aes128_ctr aes256_cbc
aes128 3des
ssh client secure-algorithms hmac sha2_256 sha2_256_96 sha1 sha1_96 md5
md5_96
ssh client key-exchange dh_group14_sha1
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
capwap source interface vlanif801
#
user-interface con 0
 authentication-mode password
 set authentication password
 cipher %^#1<n6!"VC7VQQj=/vGNXG}:Eu&6zT3'C<qU9G'>N8A~"fK_+WA~0DeC]/yW"
 %^#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound telnet
user-interface vty 16 20
 protocol inbound all
#
wlan
 traffic-profile name default
 security-profile name guest1
 security-profile name voice1
 security wpa psk pass-
 phrase %^#0)RfPJm>L58cY+4*K);#E~]V)7`\406bJM4syy*%^# tkip
 security-profile name default
 security-profile name employee1
 security wpa2 dot1x aes
 security-profile name default-wds
 security wpa2 psk pass-phrase %^#CB&>,Q$BB>x\Fn"|^%qToSj.2]:%J"+-
 qK%aTJ_0%^# aes
 security-profile name default-mesh
 security wpa2 psk pass-phrase %^#]7|J"LHnEQ=-,
 GJS[q&>M">Qsqw;9mb8$0`_=6I%^# aes
 ssid-profile name guest1
 ssid guest1
 ssid-profile name voice1
 ssid voice1
 ssid-profile name default
 ssid-profile name employee1
 ssid employee1
 vap-profile name guest1
 forward-mode tunnel
 service-vlan vlan-id 13
 ssid-profile guest1
 security-profile guest1
 authentication-profile portal_authen_profile
 vap-profile name voice1
 forward-mode tunnel
 service-vlan vlan-id 12
 ssid-profile voice1
 security-profile voice1
 vap-profile name default
```

```
vap-profile name employee1
forward-mode tunnel
service-vlan vlan-id 11
ssid-profile employee1
security-profile employee1
authentication-profile employee1
mesh-handover-profile name default
mesh-profile name default
wds-profile name default
regulatory-domain-profile name default
regulatory-domain-profile name domain1
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile employee1 wlan 1
vap-profile voicel wlan 2
vap-profile guest1 wlan 3
radio 1
vap-profile employee1 wlan 1
vap-profile voicel wlan 2
vap-profile guest1 wlan 3
radio 2
vap-profile employee1 wlan 1
vap-profile voicel wlan 2
vap-profile guest1 wlan 3
ap-id 0 type-id 43 ap-mac 4cfa-cabe-eb60 ap-sn 21500826412SG8918066
ap-group ap-group1
ap-id 1 type-id 43 ap-mac 4cfa-cabf-d0c0 ap-sn 21500826412SG8919901
ap-group ap-group1
provision-ap
#
dot1x-access-profile name dot1x_access_profile
dot1x-access-profile name employee1
#
mac-access-profile name mac_access_profile
#
undo ntp-service enable
#
return
```

6

Experiment 6: Backup the Configuration and Reset the Device

6.1 About This Course

6.1.1 Objectives

- Save the configuration of AC
- Configure FTP service in AC
- Backup the configuration of AC
- Reset the configuration of AC

6.1.2 Plan

You must configure devices according to the plan to avoid errors. This experiment uses group 1 as an example to illustrate rules for configuring the device name, VLAN, and Trunk.

The following table describes device connections.

Group No.	AC-Switch Port	AP-Switch Port
1	AC1—G0/0/1	• AP1-G0/0/10 • AP2-G0/0/11
2	AC2—G0/0/2	• AP3-G0/0/12 • AP4-G0/0/13
3	AC3—G0/0/3	• AP5-G0/0/14 • AP6-G0/0/15
4	AC4—G0/0/4	• AP7-G0/0/15 • AP8-G0/0/16
5	AC5—G0/0/5	• AP9-G0/0/17 • AP10-G0/0/18

6	AC6—G0/0/6	• AP11-G0/0/19 • AP12-G0/0/20
---	------------	--

Item	Parameter
Management IP	172.21.11.X+2
Backup Configuration File name	acvrpcfg.zip
FTP account	Name: ftp Password: Huawei@123
FTP Directory	Flash:/

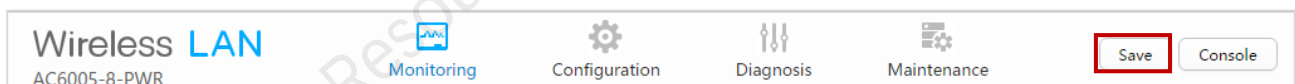
6.2 Experiment Task

6.2.1 Configuration Procedure

Step1 Save the Configuration

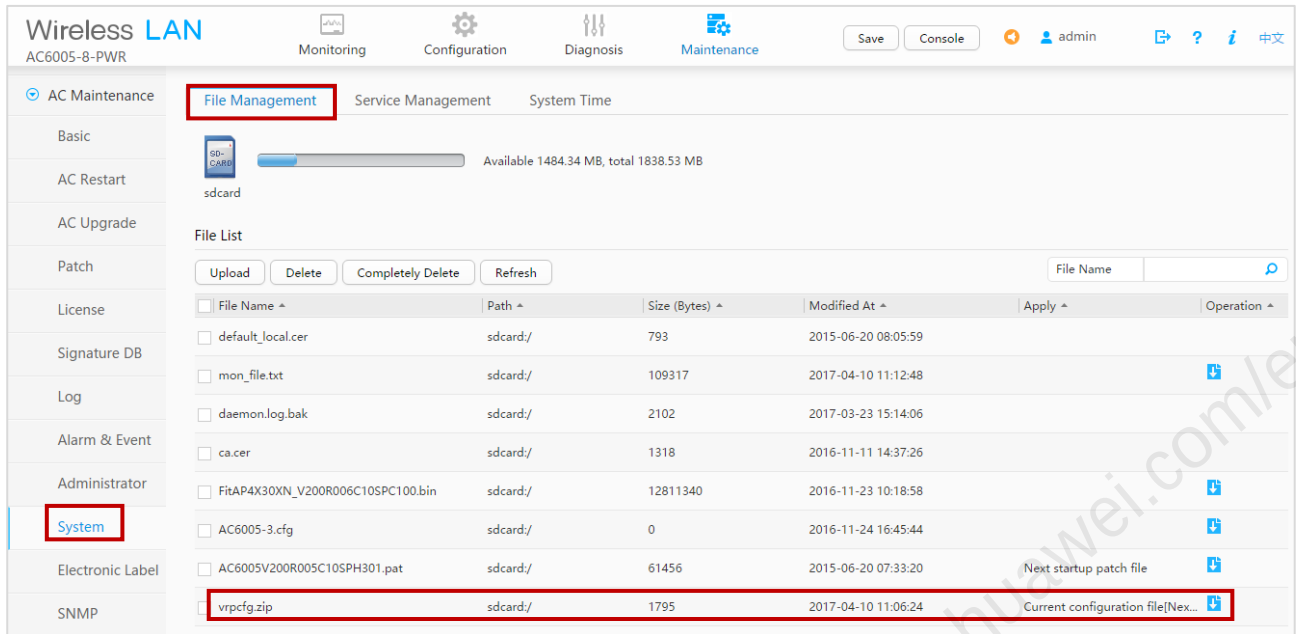
Any change through web-based configuration, you need to click “save” to save the configuration to the device. If you don’t save it , the configuration will lost after rebooted.

Save the configuration through the upper right of the page.



After saving, you can view information about the files and directories on the storage device.

Choose “Maintenance > System Configuration > File Management”. Enter the file management page.



Wireless LAN
AC6005-8-PWR

Monitoring Configuration Diagnosis Maintenance

Save Console admin ? i 中文

AC Maintenance **File Management** Service Management System Time

Basic
AC Restart
AC Upgrade
Patch
License
Signature DB
Log
Alarm & Event
Administrator
System
Electronic Label
SNMP

sdcard
Available 1484.34 MB, total 1838.53 MB

File List

Upload Delete Completely Delete Refresh

File Name Path Size (Bytes) Modified At Apply Operation

File Name	Path	Size (Bytes)	Modified At	Apply	Operation
☐ default_local.cer	sdcard:/	793	2015-06-20 08:05:59		
☐ mon_file.txt	sdcard:/	109317	2017-04-10 11:12:48		
☐ daemon.log.bak	sdcard:/	2102	2017-03-23 15:14:06		
☐ ca.cer	sdcard:/	1318	2016-11-11 14:37:26		
☐ FitAP4X30XN_V200R006C10SPC100.bin	sdcard:/	12811340	2016-11-23 10:18:58		
☐ AC6005-3.cfg	sdcard:/	0	2016-11-24 16:45:44		
☐ AC6005V200R005C10SPH301.pat	sdcard:/	61456	2015-06-20 07:33:20	Next startup patch file	
☐ vrpcfg.zip	sdcard:/	1795	2017-04-10 11:06:24	Current configuration file[Nex...]	

In the Storage Medium area, check the remaining size and total size of storage devices.

Manage files in the File Management area.

To search all files in a storage medium or all the storage media, click Search.

To move a file to the recycle bin, select the file and click Delete and Move to Recycle Bin. You can restore the deleted file in the Recycle Bin area.

To permanently delete a file, select the file and click Delete File Permanently.

To upload a file to the storage device, click Upload file.

To refresh the file list, click Refresh. To download a file to the local PC, select the file and click .

Step2 Configuring FTP Service on AC

Create a FTP user, Choose "Maintenance > Administrator > Administrator List", enter the administrator list page. Username:ftp, password:Huawei@123, level:15.

Wireless LAN

AC6005-8-PWR

Monitoring

Configuration

Diagnosis

Maintenance

Save

Console

AC Maintenance

Basic

AC Restart

AC Upgrade

Patch

License

Signature DB

Log

Alarm & Event

Administrator List

Create

Delete

Refresh

User Name ^	Access Level ^	Access Mode ^
admin	Super administrator	http,ssh
huawei	Common administrator	http,ssh,telnet

10 Total 2 record(s)

→ Password Policy

→ Administrator Logout Records

→ Access User Record

Administrator

AC Maintenance > Administrator > Create Administrator

* User name :

ftp

* Password :

.....

* Confirm password :

.....

* Access level :

Super administrator

User status :

Active

Block

* Access mode :

All

http

ssh

ftp

telnet

terminal

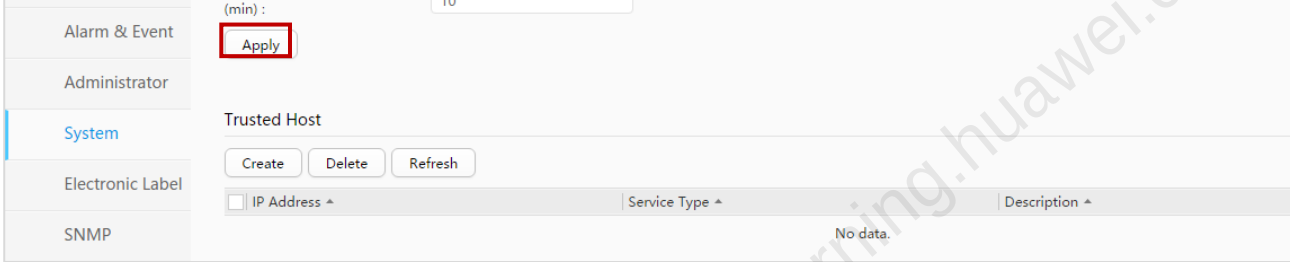
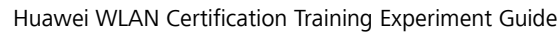
x25-pad

(Telnet, FTP, or HTTP has potential security risks. Select only the required access type.)

OK

Cancel

Enable FTP service in the global view, Choose "Maintenance> AC Maintenance > System > Service Management", enter Service managementpage.



The screenshot shows the 'System' configuration page in eSight. The 'Apply' button is highlighted with a red box. The 'Trusted Host' section contains a table with the following structure:

IP Address ^	Service Type ^	Description ^
No data.		

Buttons for 'Create', 'Delete', and 'Refresh' are visible above the table.

Step3 Backup the Configuration to PC

```

D:\>ftp 172.21.11.3

connect 172.21.11.3.

220 FTP service ready.

User(172.21.11.3:(none)): ftp

331 Password required for ftp.

password:ftp001

230 User logged in.

ftp> get acvrpcfg.zip

200 Port command okay.

150 Opening ASCII mode data connection for acvrpcfg.zip.

226 Transfer complete.

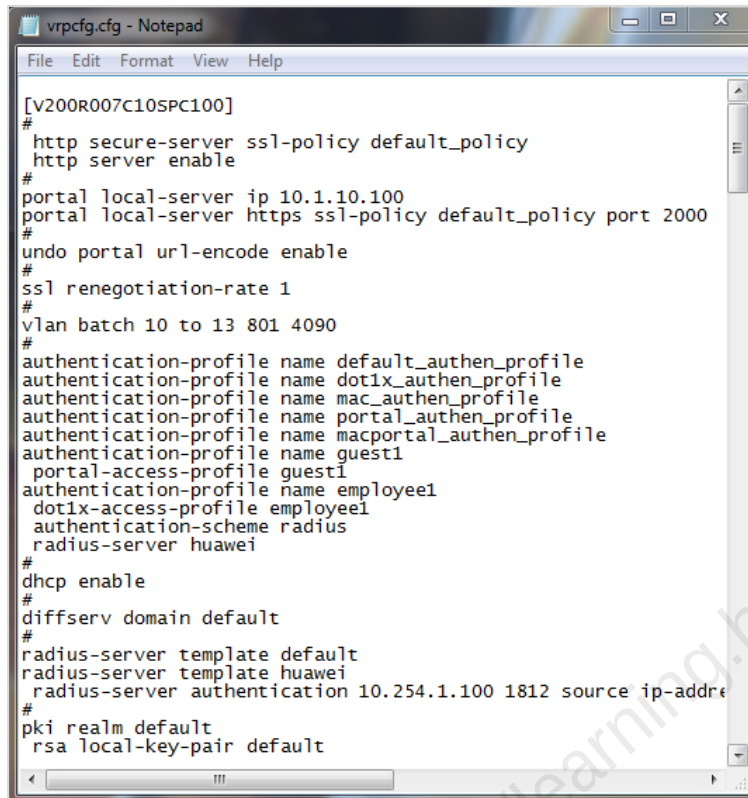
ftp: 1373 bytes received in 0.00Seconds 1373000.00Kbytes/sec.

ftp>
  
```

Step3 Backup the Configuration to PC

```
D:\>ftp 172.21.11.3
connect 172.21.11.3.
220 FTP service ready.
User(172.21.11.3:(none)): ftp
331 Password required for ftp.
password:ftp001
230 User logged in.
ftp> get acvrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for acvrpcfg.zip.
226 Transfer complete.
ftp: 1373 bytes received in 0.00Seconds 1373000.00Kbytes/sec.
ftp>
```

Then the configuration file is backuped in the PC, find the file in D:/ and then can opent it by notepad or wordpad.



```
vrpcfg.cfg - Notepad
File Edit Format View Help

[V200R007C10SPC100]
#
http secure-server ssl-policy default_policy
http server enable
#
portal local-server ip 10.1.10.100
portal local-server https ssl-policy default_policy port 2000
#
undo portal url-encode enable
#
ssl renegotiation-rate 1
#
vlan batch 10 to 13 801 4090
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name macportal_authen_profile
authentication-profile name guest1
portal-access-profile name guest1
authentication-profile name employee1
dot1x-access-profile employee1
authentication-scheme radius
radius-server huawei
#
dhcp enable
#
diffserv domain default
#
radius-server template default
radius-server template huawei
radius-server authentication 10.254.1.100 1812 source ip-address
#
pki realm default
rsa local-key-pair default
```

Step4 Reset the Configuration

After your practice finished, We need to reset the configuration of the devices before the practice, so as to avoid the impacting to the practice, please following below procedures to reset the configuration and reboot the device.

<AC1>reset saved-configuration

This will delete the configuration in the flash memory.

The device configurations will be erased to reconfigure.

Are you sure? (y/n)[n]:y

#

<AC1>reboot

Info: The system is comparing the configuration, please wait.....

Warning: All the configuration will be saved to the next startup configuration. Continue ?

[y/n]:n

System will reboot! Continue ? [y/n]:y

6.3 Verification

6.3.1 Checking the Device Configuration

It required set a new password When you login the device after reboot.

Please configure the login password:

Info: A plain text password is a string of 8 to 16 case-sensitive characters and must be a combination of at least two of the following:

uppercase letters A to Z, lowercase letters a to z, digits, and special characters. A cipher text password contains 68 characters.

Enter password:

Confirm password:

Only the default configuration exist.

```
<AC6005>display current-configuration
#
http secure-server ssl-policy default_policy
http server enable
#
ssl renegotiation-rate 1
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name macportal_authen_profile
#
diffserv domain default
#
radius-server template default
#
pki realm default
  rsa local-key-pair default
  enrollment self-signed
#
ssl policy default_policy type server
  pki-realm default
  version tls1.0 tls1.1 tls1.2
  ciphersuite rsa_aes_128_cbc_sha
#
ike proposal default
  encryption-algorithm aes-256
  dh group2
  authentication-algorithm sha2-256
  authentication-method pre-share
  integrity-algorithm hmac-sha2-256
  prf hmac-sha2-256
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
aaa
  authentication-scheme default
  authentication-scheme radius
    authentication-mode radius
  authorization-scheme default
  accounting-scheme default
  domain default
    authentication-scheme default
  domain default_admin
    authentication-scheme default
```

```

local-user admin password irreversible-
cipher %^%#M`4JPQpOV5o%dg<#chz:0uQcV}F#{FY6"T-
UeF>YO[10C!OPI-!:hyJLvcXC%^%#
local-user admin privilege level 15
local-user admin service-type ssh http
#
interface Vlanif1
ip address 169.254.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface NULL0
#
undo snmp-agent
#
stelnet server enable
undo telnet server enable
undo telnet ipv6 server enable
ssh server secure-algorithms cipher aes256_ctr aes128_ctr
ssh server secure-algorithms hmac sha2_256
ssh server key-exchange dh_group14_sha1
ssh client secure-algorithms cipher aes256_ctr aes128_ctr
ssh client secure-algorithms hmac sha2_256
ssh client key-exchange dh_group14_sha1
#
user-interface con 0
authentication-mode password
set authentication password
cipher %^%#h'O5Y|4b&.=,loK4{<@Qo0h6R~Q>oT[2{<X+y^:.,Sg*tSthkTO("UiYv~tN<
%^%#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
user-interface vty 16 20
protocol inbound all
#
wlan
traffic-profile name default
security-profile name default
security-profile name default-wds
security wpa2 psk pass-
phrase %^%#qNfI(V#y8:b/W|/(mY81#Z\D8~!8Y*#IO1RwV);+%^%# aes

```

```
security-profile name default-mesh
 security wpa2 psk pass-phrase %^%#o[7"I"t]\4xd-
e7_BV:3&kdR~nCGO!El4DSuB>~E%^%# aes
ssid-profile name default
vap-profile name default
mesh-handover-profile name default
mesh-profile name default
wds-profile name default
regulatory-domain-profile name default
air-scan-profile name default
rrm-profile name default
radio-2g-profile name default
radio-5g-profile name default
wids-spoof-profile name default
wids-profile name default
ap-system-profile name default
port-link-profile name default
wired-port-profile name default
serial-profile name preset-enjoyor-toeap
ap-group name default
provision-ap
#
dot1x-access-profile name dot1x_access_profile
#
mac-access-profile name mac_access_profile
#
 undo ntp-service enable
#
return
```

6.4 Reference Configuration

6.4.1 Key Configuration

```
[AC1]ftp server enable
[AC1]aaa
[AC1-aaa]local-user ftp password irreversible-cipher Huawei@123 ftp-
directory sdcard:/
[AC1-aaa]local-user ftp service-type ftp
[AC1-aaa]local-user ftp privilege level 15
Warning: This operation may affect online users, are you sure to change
the user privilege level ?[Y/N]y
```

7 Appendix

7.1 Configuration of Core Switch

```
#
sysname S5700
#
vlan batch 10 to 13 20 to 23 30 to 33 40 to 43 50 to 53 60 to 63 200
801 to 806
#
undo http server enable
undo http secure-server enable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@@5d~9:M^ipCfL\iB)EQd>3Uwe%@@@
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif10
 ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
 ip address 10.1.11.1 255.255.255.0
#
interface Vlanif12
 ip address 10.1.12.1 255.255.255.0
#
interface Vlanif13
 ip address 10.1.13.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.20.1 255.255.255.0
#
interface Vlanif21
 ip address 10.1.21.1 255.255.255.0
#
interface Vlanif22
 ip address 10.1.22.1 255.255.255.0
#
interface Vlanif23
```

```
ip address 10.1.23.1 255.255.255.0
#
interface Vlanif30
ip address 10.1.30.1 255.255.255.0
#
interface Vlanif31
ip address 10.1.31.1 255.255.255.0
#
interface Vlanif32
ip address 10.1.32.1 255.255.255.0
#
interface Vlanif33
ip address 10.1.33.1 255.255.255.0
#
interface Vlanif40
ip address 10.1.40.1 255.255.255.0
#
interface Vlanif41
ip address 10.1.41.1 255.255.255.0
#
interface Vlanif42
ip address 10.1.42.1 255.255.255.0
#
interface Vlanif43
ip address 10.1.43.1 255.255.255.0
#
interface Vlanif50
ip address 10.1.50.1 255.255.255.0
#
interface Vlanif51
ip address 10.1.51.1 255.255.255.0
#
interface Vlanif52
ip address 10.1.52.1 255.255.255.0
#
interface Vlanif53
ip address 10.1.53.1 255.255.255.0
#
interface Vlanif60
ip address 10.1.60.1 255.255.255.0
#
interface Vlanif61
ip address 10.1.61.1 255.255.255.0
#
interface Vlanif62
ip address 10.1.62.1 255.255.255.0
#
interface Vlanif63
ip address 10.1.63.1 255.255.255.0
#
interface Vlanif200
ip address 10.254.1.1 255.255.255.0
#
interface Vlanif801
ip address 10.1.201.1 255.255.255.0
```

```
#
interface Vlanif802
 ip address 10.1.202.1 255.255.255.0
#
interface Vlanif803
 ip address 10.1.203.1 255.255.255.0
#
interface Vlanif804
 ip address 10.1.204.1 255.255.255.0
#
interface Vlanif805
 ip address 10.1.205.1 255.255.255.0
#
interface Vlanif806
 ip address 10.1.206.1 255.255.255.0
#
interface MEth0/0/1
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13 801
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20 to 23 802
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 30 to 33 803
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 40 to 43 804
#
interface GigabitEthernet0/0/5
 port link-type trunk
 port trunk allow-pass vlan 50 to 53 805
#
interface GigabitEthernet0/0/6
 port link-type trunk
 port trunk allow-pass vlan 60 to 63 806
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk pvid vlan 10
 port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/11
 port link-type trunk
```

```
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 20
port trunk allow-pass vlan 20 to 23
#
interface GigabitEthernet0/0/13
port link-type trunk
port trunk pvid vlan 20
port trunk allow-pass vlan 20 to 23
#
interface GigabitEthernet0/0/14
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 33
#
interface GigabitEthernet0/0/15
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 33
#
interface GigabitEthernet0/0/16
port link-type trunk
port trunk pvid vlan 40
port trunk allow-pass vlan 40 to 43
#
interface GigabitEthernet0/0/17
port link-type trunk
port trunk pvid vlan 40
port trunk allow-pass vlan 40 to 43
#
interface GigabitEthernet0/0/18
port link-type trunk
port trunk pvid vlan 50
port trunk allow-pass vlan 50 to 53
#
interface GigabitEthernet0/0/19
port link-type trunk
port trunk pvid vlan 50
port trunk allow-pass vlan 50 to 53
#
interface GigabitEthernet0/0/20
port link-type trunk
port trunk pvid vlan 60
port trunk allow-pass vlan 60 to 63
#
interface GigabitEthernet0/0/21
port link-type trunk
port trunk pvid vlan 60
port trunk allow-pass vlan 60 to 63
#
interface GigabitEthernet0/0/22
#
```

```
interface GigabitEthernet0/0/23
  port link-type access
  port default vlan 200
#
interface GigabitEthernet0/0/24
  port link-type access
  port default vlan 200
#
interface NULL0
#
interface LoopBack1
  ip address 101.101.101.101 255.255.255.255
#
interface LoopBack2
  ip address 102.102.102.102 255.255.255.255
#
interface LoopBack3
  ip address 103.103.103.103 255.255.255.255
#
interface LoopBack4
  ip address 104.104.104.104 255.255.255.255
#
interface LoopBack5
  ip address 105.105.105.105 255.255.255.255
#
interface LoopBack6
  ip address 106.106.106.106 255.255.255.255
#
user-interface con 0
  authentication-mode password
  set authentication password
  cipher %@@@;($MM!"!U<_DW.Z.H!4L,$49.>!z*#!\EX>M5e+/7j&#$4<,%@@@
user-interface vty 0 4
user-interface vty 16 20
#
return
```

The privilege of HCNA/HCNP/HCIE:

With any Huawei Career Certification, you have the privilege on <http://learning.huawei.com/en> to enjoy:

- 1、e-Learning Courses: Logon <http://learning.huawei.com/en> and enter [Huawei Training/e-Learning](#)
 - If you have the HCNA/HCNP certificate: You can access Huawei Career Certification and Basic Technology e-Learning courses.
 - If you have the HCIE certificate: You can access all the e-Learning courses which marked for HCIE Certification Users.
 - Methods to get the HCIE e-Learning *privilege*: Please associate HCIE certificate information with your Huawei account, and email the account to Learning@huawei.com to apply for HCIE e-Learning privilege.
- 2、Training Material Download
 - Content: Huawei product training material and Huawei career certification training material.
 - Method: Logon <http://learning.huawei.com/en> and enter [Huawei Training/Classroom Training](#), then you can download training material in the specific training introduction page.
- 3、Priority to participate in [Huawei Online Open Class \(LVC\)](#)
 - The Huawei career certification training and product training covering all ICT technical domains like R&S, UC&C, Security, Storage and so on, which are conducted by Huawei professional instructors.
- 4、Learning Tools:
 - [eNSP](#): Simulate single Router&Switch device and large network.
 - [WLAN Planner](#): Network planning tools for WLAN AP products.
- In addition, Huawei has built up [Huawei Technical Forum](#) which allows candidates to discuss technical issues with Huawei experts, share exam experiences with others or be acquainted with Huawei Products.
- Statement:

This material is for personal use only, and can not be used by any individual or organization for any commercial purposes.