

华为认证WLAN系列教程

HCNA-WALN

华为认证无线局域网络工程师

实验指导书



版权声明

版权所有 © 华为技术有限公司 2012。 保留一切权利。

本书所有内容受版权法保护，华为拥有所有版权，但注明引用其他方的内容除外。未经华为技术有限公司事先书面许可，任何人、任何组织不得将本书的任何内容以任何方式进行复制、经销、翻印、存储于信息检索系统或使用于任何其他任何商业目的。

版权所有 侵权必究。

商标声明



和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

华为认证WLAN系列教程HCNA-WLAN

华为认证无局域网络工程师

实验指导书

第1.0版本

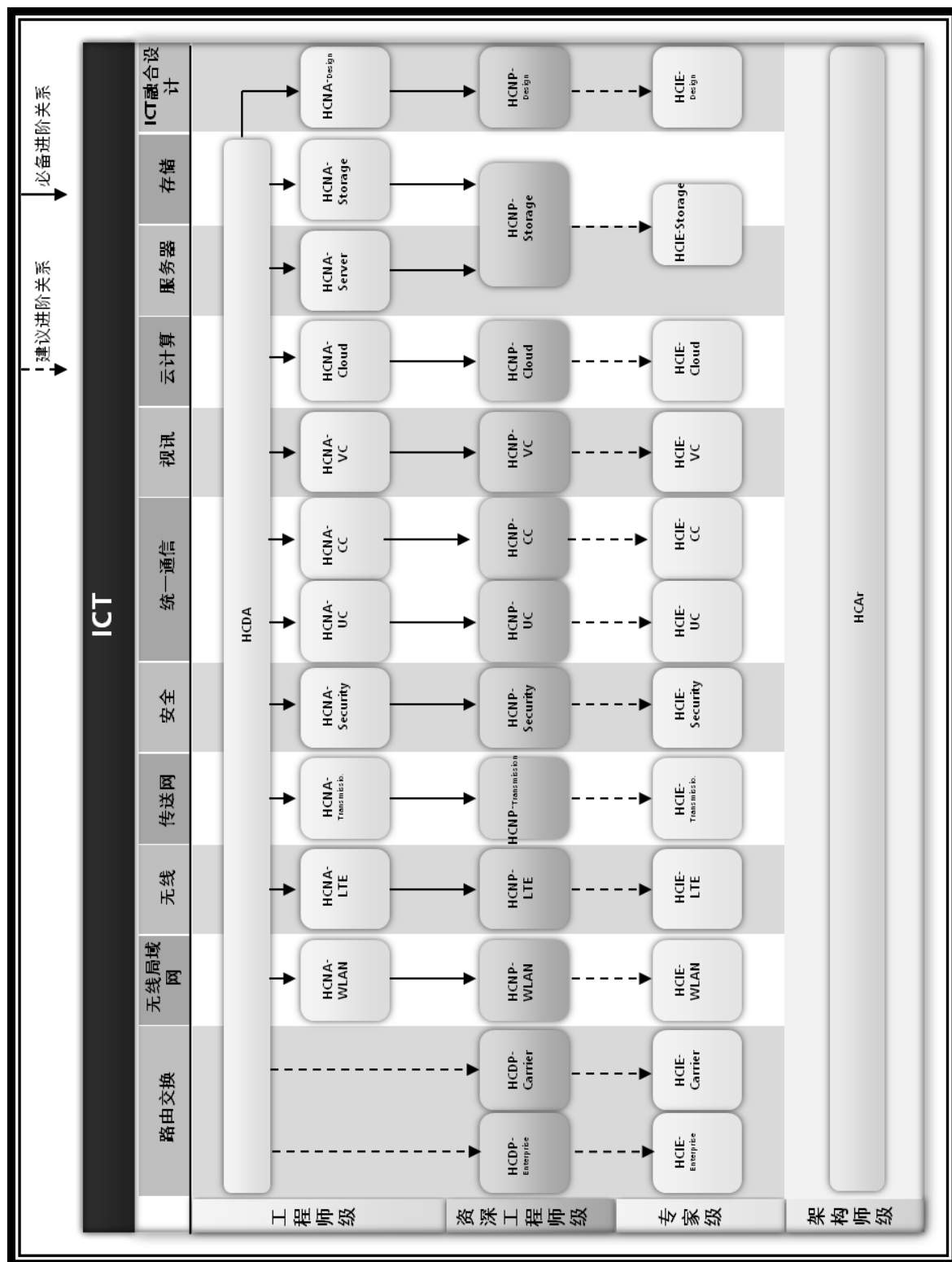
华为认证体系介绍

依托华为公司雄厚的技术实力和专业的培训体系，华为认证考虑到不同客户对WLAN技术不同层次的需求，致力于为客户提供实战性、专业化的技术认证。

根据WLAN技术的特点和客户不同层次的需求，华为认证为客户提供面向各个方向的四级认证体系。

HCNA-WLAN (Huawei Certified Network Associate-Wireless Local Area Network ，华为认证网络通信工程师WLAN方向) 主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为WLAN产品技术人士。HCNA-WLAN认证在内容上涵盖华为WLAN基础知识、CAPWAP协议及WLAN组网、华为WLAN产品特性及安全配置、WLAN高级技术及天线介绍以及WLAN网规网优和故障排除等内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在WLAN网络世界的潮头浪尖！



前言

简介

本书为HCNA-WLAN认证培训教程,适用于准备参加HCNA-WLAN考试的学员或者希望了解WLAN基础知识、CAPWAP协议及WLAN组网、华为WLAN产品特性及安全配置、WLAN高级技术及天线介绍以及WLAN网规网优和故障排除等相关WLAN技术的读者。

内容描述

本实验指导书共包含7个实验,从设备基本操作配置开始、逐一介绍了WLAN组网中的二层组网、安全、三层组网、eSight网管软件的配置与实现。

实验一为HCNA-WLAN实验环境准备,其中包括检查设备是否齐全、实际设备组网连线、AC配置清空,通过实验一的操作,帮助读者熟悉HCNA-WLAN设备及物理拓扑搭建。

实验二为AC初始化配置实验,通过基本的操作与配置,帮助读者熟悉无线控制器AC6605,理解AC6605的基本功能。

实验三为AP认证及WLAN配置流程,通过基本的组网配置,帮助读者掌握基本的WLAN组网能力。

实验四介绍了无线网络中安全的配置,重点讲解的是802.1X认证方式的安全,通过本章的实验,是读者掌握WLAN安全配置的方法,熟悉WLAN安全。

实验五介绍采用AC6605进行三层组网的配置与操作,通过三层组网配置,帮助读者全面掌握WLAN组网方式方法。

实验六为eSight WLAN网管实验,通过eSight实验,帮助读者掌握如何添加WLAN设备到eSight中,并且通过向导配置下发WLAN业务。

实验七为备份配置文件,清空AC配置实验,通过此实验,帮助读者掌握通过FTP备份设备配置文件的方法。

读者知识背景

本课程为华为认证基础课程，要求读者具有基本的无线局域网络知识背景，同时熟悉华为交换设备，了解基本数通知识。

本书常用图标



无线控制器
(AC)



无线接入点
(AP)



交换机



eSight 服务器



Radius 服务器



无线用户
(STA)

实验环境说明

组网介绍

本实验环境面向准备HCNA-WLAN考试的无线网络工程师。每套实验环境包括无线控制器2~9台，无线接入点2~9台，核心交换机1台， RADIUS/eSight服务器1台。每套实验环境适用于4~16名学员同时上机操作。

设备介绍

为了满足HCNA-WLAN实验需要，建议每套实验环境采用以下配置：

设备名称、型号与版本的对应关系如下：

设备名称	设备型号	软件版本
核心交换机	S3700-28TP-PWR-EI	Version 5.70 (S3700 V100R005C01SPC100)
无线控制器	AC6605-26-PWR	Version 5.70 (AC6605 V200R001C00SPC100)
无线接入点	AP6010DN-AGN	V200R001C00SPC100 (B028)

目录

前言	5
简介	5
内容描述	5
读者知识背景	6
本书常用图标	7
实验环境说明	8
组网介绍	8
设备介绍	8
实验一：实验环境准备	(*
实验目的	13
检查设备是否齐全	13
实验拓扑搭建说明：直连组网	14
实验拓扑搭建说明：旁挂组网	15
1.1 Console 线连接说明	16
1.2 清空 AC 配置	19
实验二：AC初始化配置实验	20
实验目的	20
实验规划	20
实验步骤	21
2.1 理解有线侧和无线侧	21
2.2 配置有线侧基础信息	22
2.3 配置无线侧基础信息	23
2.4 配置和测试有线侧管理接口 telnet 服务（密码认证）	25

2.5 配置和测试无线侧管理接口 telnet 服务（AAA 认证）	26
2.6 保存配置.....	27
2.7 关键配置汇总.....	27
实验三 AP认证及WLAN配置流程.....	30
实验目的	30
实验规划	30
实验步骤	31
3.1 配置流程说明.....	31
3.2 配置交换机.....	31
3.3 配置 AC 基本功能.....	31
3.4 配置 AP 认证及与 AC 互通	32
3.5 配置射频模板并应用到 AP 的天线接口上.....	34
3.6 配置 Wlan-ess 接口.....	35
3.7 配置安全模板、流量模板和 WLAN 服务集	35
3.8 绑定服务集到 AP 并提交配置执行	36
3.9 在 AC 上检查相关配置的命令	37
3.10 关键配置汇总.....	41
实验四 安全配置实验	43
实验目的	43
实验规划	43
实验步骤	44
4.1 配置 WEP 认证.....	44
4.2 配置 WPA PSK 认证.....	46
4.3 配置 WPA EAP 认证.....	49
4.4 配置 EAP 客户端.....	54

4.5 安全配置注意事项.....	57
4.6 关键配置汇总.....	58
实验五 “旁挂+三层组网”实验	62
实验目标	62
实验规划	62
实验步骤	63
5.1 变更 AP 的接线.....	63
5.2 更新 vlan 及 trunk.....	63
5.3 AP 上线配置.....	64
5.4 修改服务集的转发模式为隧道模式	65
5.5 关键配置.....	66
实验六 eSight WLAN网管实验（选做实验）	72
实验目标	72
实验规划	72
实验步骤	72
6.1 配置 AC 的 SNMP 团体参数	72
6.2 配置 eSight 发现 AC.....	73
6.3 使用向导配置 WLAN 服务集	74
6.4 使用 eSight 检查配置	79
6.5 关键配置.....	81
实验七 备份配置文件，清空AC配置	82
实验目标	82
实验规划	82
实验步骤	82
7.1 保存配置文件到 flash	82

7.2 在 AC 的 LSW 侧和 AC 侧分别配置 FTP 服务器	83
7.3 使用 FTP 备份配置到电脑上	83
7.4 清空 AC 配置.....	85
7.5 关键配置.....	86
附件：核心交换机基础配置（供搭建实验环境参考）	87

实验一：实验环境准备

实验目的

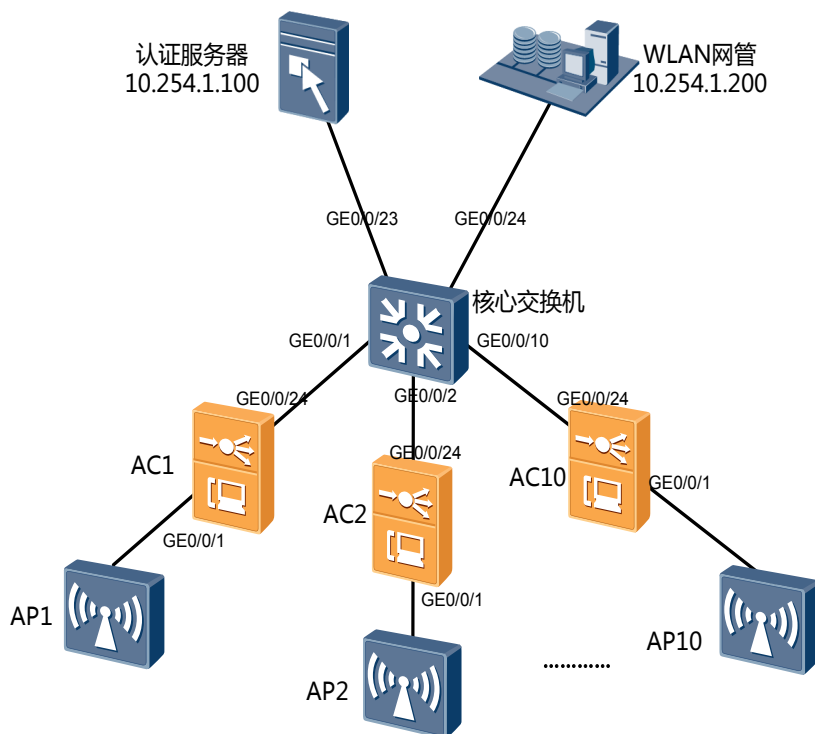
- 检查实验设备是否齐全
- 掌握WLAN实验网络基本组建方法
- 掌握清空AC配置的方法

检查设备是否齐全

实验开始之前请每组学员检查自己的实验设备是否齐全，实验清单如下：

设备名称	数量	备注
Radius认证服务器	所有组共1台	所有实验组共用
华为3700PoE交换机 或华为5700PoE交换机	所有组共1台	所有实验组共用，可支持10组，已做好预配置。
AC6605无线控制器	每组1台	要有PoE电源模块
AP6010DN	每组1颗	
笔记本或台式机	每组1台	台式机要有无线网卡
双绞线	每组4条	至少要2米长
console线	每组1条	笔记本的要用USB转COM线

实验拓扑搭建说明：直连组网



直连组网拓扑搭建说明：

本实验手册采用直连组网拓扑形式

直连组网适合中小型WLAN网络的部署，HCNA-WLAN所有基础实验全部采用直连组网拓扑。

第1组AC1的第24接口连接交换机的第1接口，AC的第1接口连接AP1。

第2组AC2的第24接口连接交换机的第2接口，AC的第1接口连接AP2。

第3组AC3的第24接口连接交换机的第3接口，AC的第1接口连接AP3

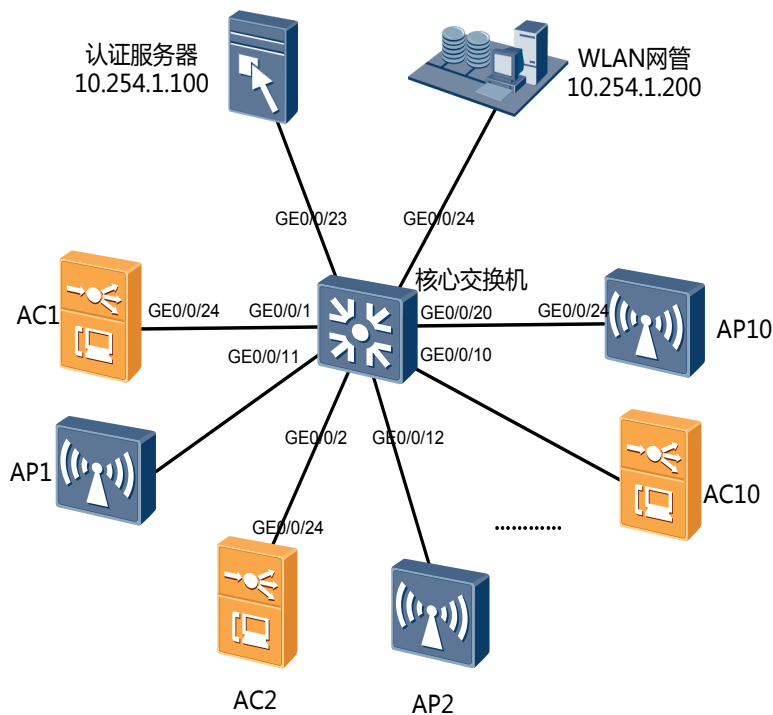
.....依此类推.....

第10组AC10的第24接口连接交换机的第10接口，AC的第1接口连接AP10。

核心交换机的配置已经配好，学员无需配置（配置指南见手册附件）。

认证服务器及WLAN网管平台已经配好，学员无需配置。

实验拓扑搭建说明：旁挂组网



旁挂组网拓扑搭建说明：

旁挂组网适合大型WLAN网络的部署，第五个实验为“三层组网+旁挂组网”实验。

第1组AC1的第24接口连接交换机的第1接口，AP1接交换机第11接口。

第2组AC2的第24接口连接交换机的第2接口，AP2接交换机第12接口。

第3组AC3的第24接口连接交换机的第3接口，AP3接交换机第13接口。

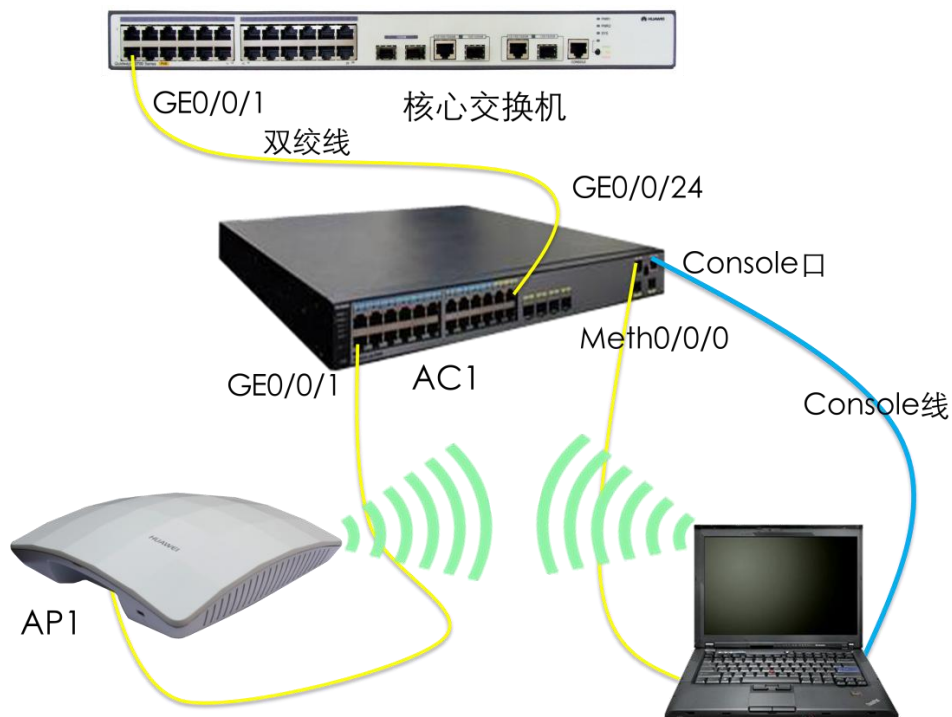
.....依此类推.....

第10组AC10的第24接口连接交换机的第10接口，AP10接交换机第20接口。

核心交换机的配置已经配好，学员无需配置（配置指南见手册附件）。

认证服务器及WLAN网管平台已经配好，学员无需配置。

1.1 Console 线连接说明



如图连接设备（不同的组接交换机的接口不同），并且给设备加电。

笔记本使用console线连接控制器，要使用USB转COM线并且安装正确的驱动程序，如果台式机则可以直接使用COM接口连接。

通过Windows 系统自带超级终端连接AC6605

用Console线缆将PC电脑连接至AC6605的Console接口。在计算机上打开终端仿真程序（如Windows 的超级终端），如下图建立一个新的连接。这里的名称和图标无特殊意义，可以随自己喜好定义和选择。

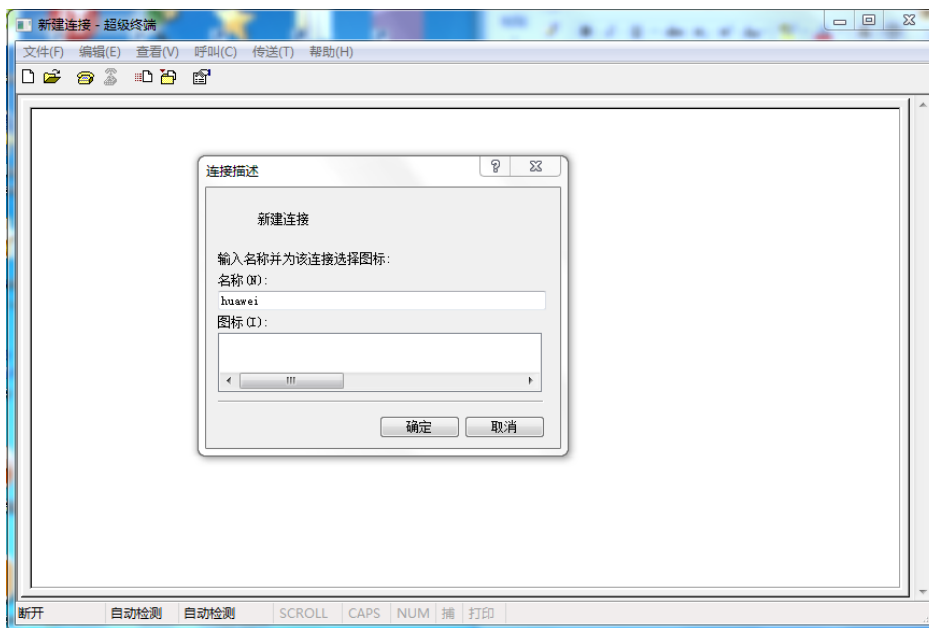


图1.1建立新的连接

选择配置的方式，确定所使用的COM口。



图1.2 连接接口选择

在拥有多个COM口的计算机上，请注意选择正确的COM接口，一般情况下计算机的串口为COM1。

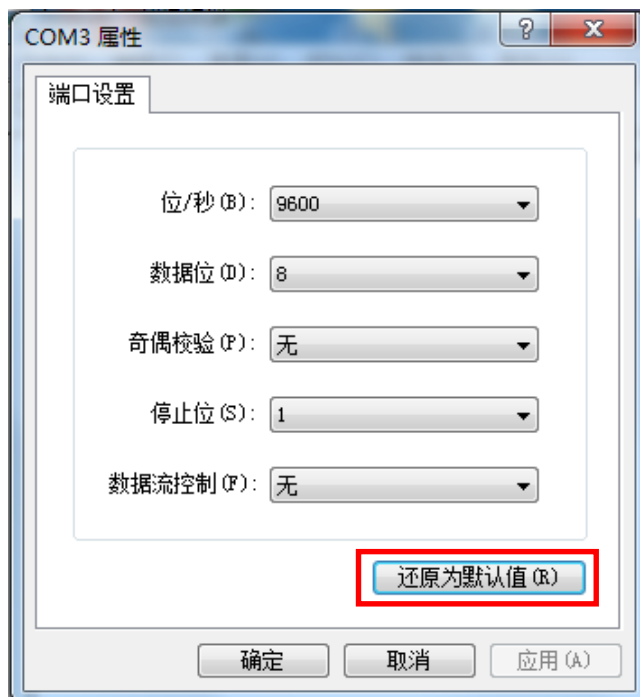


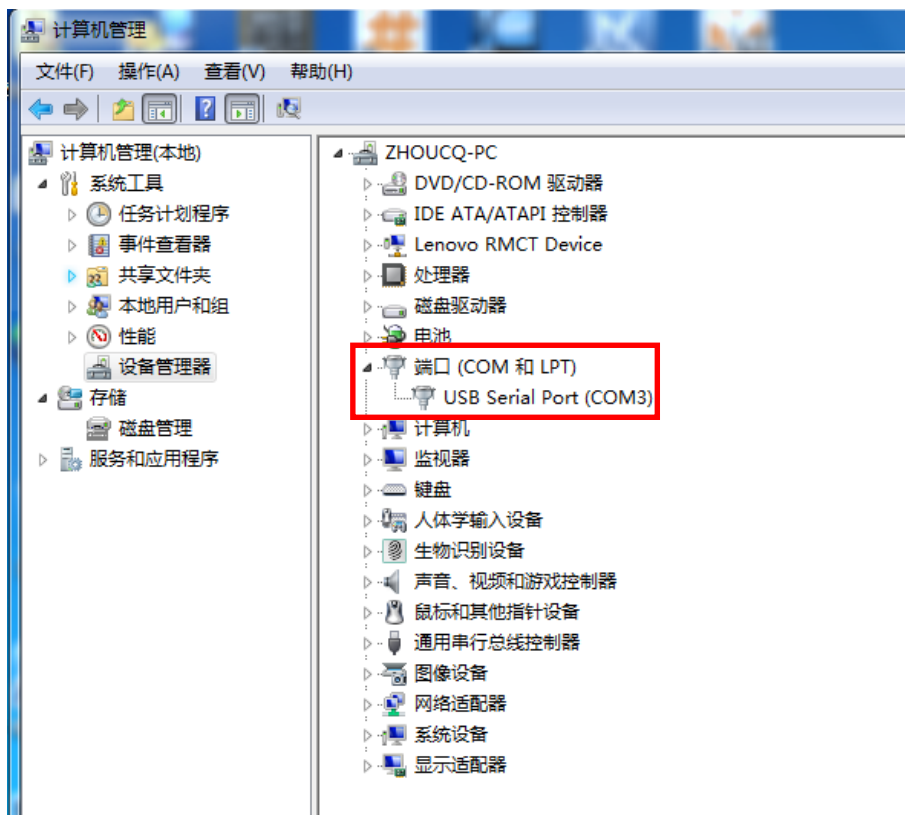
图1.3接口通信参数设置

在COM的属性界面中，点击“还原为默认值”，即可快速得到正确的参数信息的配置。然后点击“确定”进行连接。

打开电源，开启AC6605。如果以上参数设置正确，终端窗口会有启动过程文字出现，直到启动完毕，提示用户按Enter键。用户视图的命令行提示符，如<Quidway>会出现，至此用户进入了用户视图配置环境。

如果无法找到所使用的COM口，可以打开设备管理器，在设备管理器中找到相应的COM口。

步骤为 右击“我的电脑” → “管理” → “设备管理器” → “端口”，如下图所示：



1.2 清空 AC 配置

实验时，为避免残余配置对实验的影响，要求学生在实验完成后，关闭设备之前清空设备保存的配置信息；同时，实验开始时，确认设备从空配置启动，否则执行配置清空，并重启设备。

清空控制器的配置需要在有线侧和无线侧分别操作：

```
<LSW6605>reset saved-configuration
```

```
The configuration will be erased to reconfigure. Continue? [Y/N]:Y
```

Ctrl+Y 切换到无线侧继续清空无线侧的配置

```
<AC>reset saved-configuration
```

```
The configuration will be erased to reconfigure. Continue? [Y/N]:Y
```

重启控制器的命令是：

```
<LSW>reboot
```

```
<LSW>Otherwise, unsaved configuration will be lost. Continue?[Y/N]:Y
```

```
<LSW>Warning: All the configuration will be saved to the configuration file for  
the next startup:, Continue?[Y/N]:N
```

```
<LSW>System will reboot! Continue?[Y/N]:Y
```

实验二：AC初始化配置实验

实验目的

- 理解AC有线侧无线侧的区别
- 掌握配置AC有线侧VLAN的方法
- 掌握配置AC无线侧VLAN及路由的方法
- 掌握配置AC的telnet管理服务及认证方式
- 掌握保存AC配置的方法

实验规划

配置设备名称要分别在LSW侧和AC侧分别配置，每个学员知道自己的组号以后，按照如下规划配置设备名称及vlan及trunk，本实验以第1组配置为例。

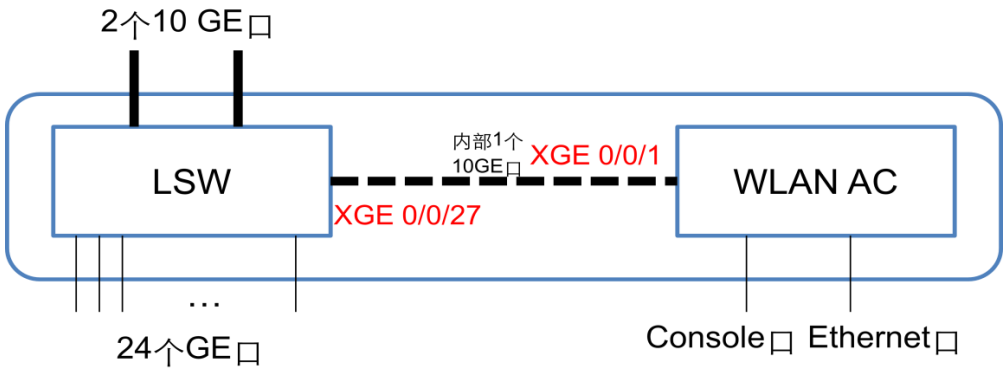
学员属于第X组	LSW配置	AC侧配置
设备名称	LSWX	ACX
AP管理VLAN	VLAN : X0	VLAN : X0 IP : 10.1.X0.100
业务VLAN (员工)	VLAN : X1	VLAN : X1 IP : 10.1.X1.100
业务VLAN (语音)	VLAN : X2	VLAN : X2 IP : 10.1.X2.100
业务VLAN (访客)	VLAN : X3	VLAN : X3 IP : 192.168.X.1
设备管理地址	MEth0/0/1 IP : 192.168.100.100	Ethernet0/0/0 IP : 192.168.100.200

内部10G接口配置	Trunk 放行相应VLAN: X0 to X3	Trunk放行相应VLAN: X0 to X3
组网方式：直连组网 + 二层组网		
本实验中，PC用于测试AC的Telnet，配置地址为192.168.100.10		

实验步骤

2.1 理解有线侧和无线侧

AC6605控制器的硬件分为有线侧（LSW）和无线侧（AC）两部分，其中有线侧相当于一个支持POE的三层交换机，有线侧和无线侧通过一条10G内部线缆相联，如图所示：



有线侧可以配置VLAN、三层交换和路由协议等。

无线侧可以配置VLAN、静态路由和WLAN业务。

第一次登陆会默认登陆到AC的有线侧，通过**display device**可以查看当前你所处的位置，通过组合键**ctrl + y** 或命令 **console switch**可以实现有线侧和无线侧的切换。

```
<Quidway>display device
AC6605-26-PWR's Device status:
Slot  Sub Type      Online   Power    Register   Status   Role
-----
0      -   AC6605-26   Present PowerOn   Registered Normal   Master
      4   POWER      Present PowerOn   Registered Normal   NA
```

Display device 命令如果看到设备子类型有AC6605-26字段，说明当前位于有线侧（LSW）。

```
<Quidway>console switch
Info: Switch console to AC.
<Quidway>display device
AC6605-AC's Device status:
Slot  Sub Type      Online   Power    Register    Alarm    Primary
-----
0      -   AC6605   Present  PowerOn   Registered   Normal   Master
<Quidway>console switch
Info: Switch console to LSW.
```

Display device 命令如果看到设备子类型有AC6605字段，说明当前位于无线侧（AC）。

2.2 配置有线侧基础信息

确认当前位于有线侧

```
<Quidway>dis device
AC6605-26-PWR's Device status:
Slot  Sub Type      Online   Power    Register    Status    Role
-----
0      -   AC6605-26   Present  PowerOn   Registered   Normal   Master
      4   POWER      Present  PowerOn   Registered   Normal   NA
```

创建管理vlan10、业务vlan 11 12 13

```
<Quidway>system-view
[Quidway]sysname LSW1
[LSW1]vlan batch 10 to 13
```

配置g0/0/1接口用来连接AP1

```
[LSW1]interface g0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk pvid vlan 10
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 to 13
[LSW1-GigabitEthernet0/0/1]quit
```

配置g0/0/24接口用来连接核心交换机

```
[LSW1]interface g0/0/24
```

```
[LSW1-GigabitEthernet0/0/24]port link-type trunk
[LSW1-GigabitEthernet0/0/24]port trunk allow-pass vlan 10 to 12
[LSW1-GigabitEthernet0/0/24]quit
```

配置内部的10G接口为trunk链路，放行管理vlan及业务vlan

```
[LSW1]inter XGigabitEthernet 0/0/27
[LSW1-XGigabitEthernet0/0/27] port link-type trunk
[LSW1-XGigabitEthernet0/0/27]port trunk allow-pass vlan 10 to 13
[LSW1-XGigabitEthernet0/0/27]quit
```

2.3 配置无线侧基础信息

确认当前位于有线侧

```
[LSW1]console switch
Info: Switch console to AC.
<Quidway>system
[Quidway]sysname AC1
```

创建管理vlan10、业务vlan 11 12 13并配置三层接口IP地址

```
[AC1]vlan batch 10 to 13
[AC1]interface vlan 10
[AC1-Vlanif10]ip address 10.1.10.100 24
[AC1-Vlanif10]quit
[AC1]interface vlan 11
[AC1-Vlanif11]ip address 10.1.11.100 24
[AC1-Vlanif11]quit
[AC1]interface vlan 12
[AC1-Vlanif12]ip address 10.1.12.100 24
[AC1-Vlanif12]quit
```

开启DHCP服务，并配置无线访客VLAN的DHCP地址池（注意如果在无线侧配置为业务VLAN网关的话，无线服务集配置必须采用隧道转发方式。直接转发时，业务VLAN的网关可以配置在有线侧或外部交换机上）

```
[AC1]dhcp enable
[AC1]interface Vlanif 13
[AC1-Vlanif13]ip address 192.168.1.1 24
[AC1-Vlanif13]dhcp select interface
```

配置内部的10G接口为trunk链路，放行管理vlan及业务vlan

```
[AC1]inter XGigabitEthernet 0/0/1
[AC1-XGigabitEthernet0/0/27]port link-type trunk
[AC1-XGigabitEthernet0/0/27]port trunk allow-pass vlan 10 to 13
[AC1-XGigabitEthernet0/0/27]quit
```

检查配置的接口是否已经变为UP状态

```
[AC1]display ip interface brief
.....
Interface                IP Address/Mask      Physical  Protocol
Ethernet0/0/0             unassigned           down      down
NULL0                    unassigned           up        up(s)
Vlanif10                  10.1.10.100/24       up        up
Vlanif11                  10.1.11.100/24       up        up
Vlanif12                  10.1.12.100/24       up        up
Vlanif13                  192.168.1.1/24       up        up
```

检查和三层交换机的路由是否可达，注意此时去100.100.100.100（交换机上的模拟公网的接口）不可达。

```
[AC1]ping -a 192.168.1.1 10.1.10.1
PING 10.1.10.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.10.1: bytes=56 Sequence=1 ttl=255 time=11 ms
  Reply from 10.1.10.1: bytes=56 Sequence=2 ttl=255 time=11 ms
  Reply from 10.1.10.1: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 10.1.10.1: bytes=56 Sequence=4 ttl=255 time=11 ms
  Reply from 10.1.10.1: bytes=56 Sequence=5 ttl=255 time=20 ms

--- 10.1.10.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/12/20 ms

[AC1]ping -a 192.168.1.1 100.100.100.100
PING 100.100.100.100: 56 data bytes, press CTRL_C to break
  Request time out
  Request time out
```



```
Request time out
Request time out
Request time out
```

配置静态默认路由指向交换机

```
[AC1]ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
```

此时再ping 100.100.100.100 已经可达

```
[AC1]ping -a 192.168.1.1 100.100.100.100
PING 100.100.100.100: 56 data bytes, press CTRL_C to break
  Reply from 100.100.100.100: bytes=56 Sequence=1 ttl=255 time=7 ms
  Reply from 100.100.100.100: bytes=56 Sequence=2 ttl=255 time=10 ms
  Reply from 100.100.100.100: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 100.100.100.100: bytes=56 Sequence=4 ttl=255 time=10 ms
  Reply from 100.100.100.100: bytes=56 Sequence=5 ttl=255 time=10 ms
--- 100.100.100.100 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 配置和测试有线侧管理接口 telnet 服务（密码认证）

开启和配置有线侧telnet服务，密码是huawei,默认是密码认证。

```
[LSW1]telnet server enable
Info: TELNET server has been enabled.
[LSW1]user-interface vty 0 4
[LSW1-ui-vty0-4]set authentication password cipher huawei
[LSW1-ui-vty0-4]user privilege level 15
[LSW1-ui-vty0-4]quit
```

有线侧和无线侧公用一个物理管理接口，接口名称不一样，在有线侧接口名称为Meth 0/0/1,配置其管理Ip为192.168.100.100 255.255.255.0。

```
[LSW1]interface MEth 0/0/1
[LSW1-METh0/0/1]ip address 192.168.100.100 24
```

连接电脑的以太网口和AC6605的ETH接口（console接口的左边），在电脑上配置IP地址为192.168.100.10 255.255.255.0并测试互通性及telnet。

```
C:\Users\WLAN>telnet 192.168.100.100
Login authentication
```

```
Password:huawei
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
<LSW1>sys
Enter system view, return user view with Ctrl+Z.
```

2.5 配置和测试无线侧管理接口 telnet 服务（AAA 认证）

开启并配置telnet服务，添加AAA的账号huawei用于telnet认证。

```
[AC1]telnet server enable
Info: TELNET server has been enabled.
[AC1]aaa
[AC1-aaa]local-user huawei password simple huawei
[AC1-aaa]local-user huawei service-type telnet
[AC1-aaa]local-user huawei privilege level 15
[AC1-aaa]quit
[AC1]user-interface vty 0 4
[AC1-ui-vty0-4]authentication-mode aaa
[AC1-ui-vty0-4]quit
```

配置管理接口Ethernet 0/0/0的IP地址用来管理控制器。

```
[AC1]interface Ethernet 0/0/0
[AC1-Ethernet0/0/0]ip address 192.168.100.200 24
[AC1-Ethernet0/0/0]quit
```

连接电脑的以太网口和AC6605的ETH接口（console接口的左边），在电脑上配置IP地址为192.168.100.10 255.255.255.0并测试互通性及telnet。

```
C:\Users\WLAN>ping 192.168.100.200
```

```
正在 Ping 192.168.100.200 具有 32 字节的数据:
来自 192.168.100.200 的回复: 字节=32 时间=23ms TTL=255
来自 192.168.100.200 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.100.200 的回复: 字节=32 时间=7ms TTL=255
来自 192.168.100.200 的回复: 字节=32 时间=4ms TTL=255
```

192.168.100.200 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间 (以毫秒为单位):

最短 = 1ms, 最长 = 23ms, 平均 = 8ms

```
C:\Users\WLAN>telnet 192.168.100.200
Login authentication
Username:huawei
Password:huawei
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
<AC1>sys
Enter system view, return user view with Ctrl+Z.
[AC1]display access-user
-----
UserID Username                IP address                MAC
-----
132   huawei                    192.168.100.10           -
-----
Total 1,1 printed
```

2.6 保存配置

有线侧配置保存。

```
<LSW1>save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]Y
Info: Please input the file name(*.cfg,*.zip) [vrpcfg.zip]:
Nov 15 2012 14:30:59+05:13 LSW1 %%01CFM/4/SAVE(1) [2]:The user chose Y when decid
ing whether to save the configuration to the device.
flash:/vrpcfg.zip exists, overwrite?[Y/N]:Y
Now saving the current configuration to the slot 0 .
Info: Save the configuration successfully.
```

无线侧配置保存。

```
<AC1>save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]Y
Info: Please input the file name(*.cfg,*.zip) [vrpcfg.zip]:
Now saving the current configuration to the slot 0 .
Info: Save the configuration successfully.
```

关键配置汇总

有线侧配置（以第1组为例）。

```
sysname LSW1
#
vlan batch 10 to 13
#
interface Vlanif1
#
interface MEth0/0/1
ip address 192.168.100.100 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
interface GigabitEthernet0/0/24
port link-type trunk
port trunk allow-pass vlan 10 to 12
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
user-interface con 0
user-interface vty 0 4
user privilege level 15
set authentication password cipher N`C55QK<`= /Q=^Q`MAF4<1!!
```

无线侧配置（以第1组为例）。

```
sysname AC1
#
vlan batch 10 to 13
#
dhcp enable
#
aaa
local-user admin password simple admin
local-user admin service-type http
local-user huawei password simple huawei
local-user huawei privilege level 15
local-user huawei service-type telnet
#
```

```
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 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Ethernet0/0/0
 ip address 192.168.100.200 255.255.255.0
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13
#
interface NULL0
#
 ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
```

实验三 AP认证及WLAN配置流程

实验目的

- 掌握认证AP上线的配置方法
- 理解各种无线配置模板
- 掌握WLAN配置的基本流程
- 掌握开放认证无线服务集的配置思路

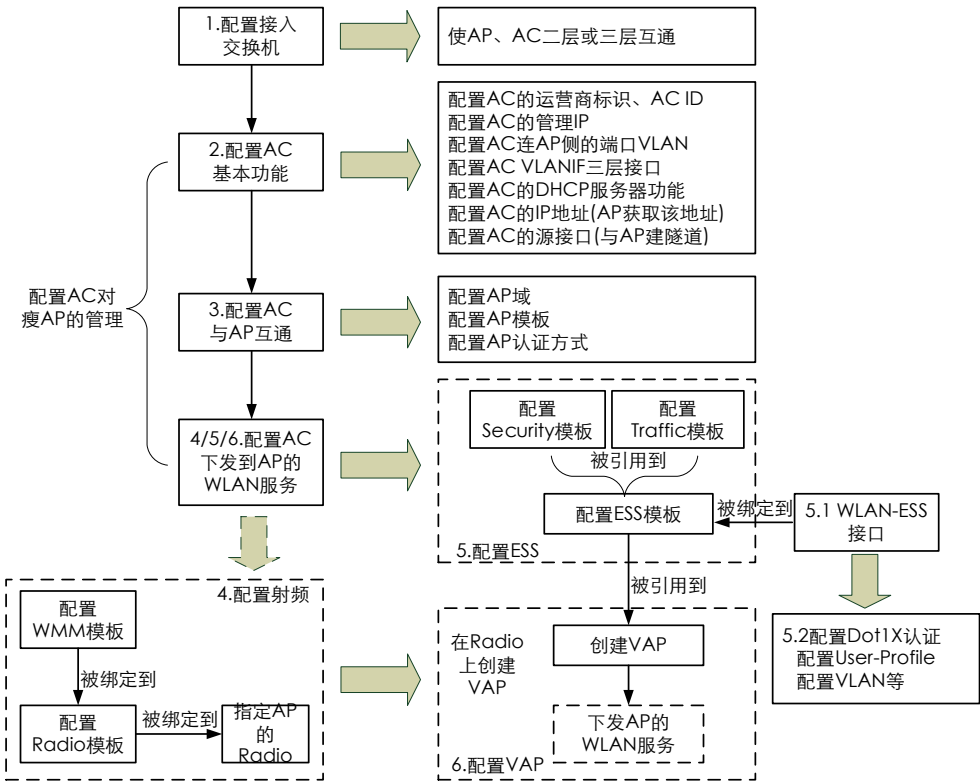
实验规划

X是学员所在组的编号，配置时对应替换，如第1组WMM模板为wmm-prof-1	
组网方式	直连组网 + 二层组网
AC基本属性	国家代码：CN
	运营商ID：other
	WLAN源：vlan X0
AP认证配置	AP认证方式：mac-auth
	AP MAC地址：在AP背后，填入这里
WMM模板配置	WMM模板：wmm-prof-X
射频模板配置	2.4G模板：radio2-prof-X
	5G模板：radio5-prof-X
服务集配置	SSID：huawei-guestX
	服务VLAN:vlan13
	转发模式：隧道转发
	流量模板：traffic-prof-X
	安全模板：security-prof-X
	Wlan-ess接口 0

	用户隔离：关闭
--	---------

实验步骤

3.1 配置流程说明



3.2 配置交换机

承接实验二的配置，交换机的配置已经完成。

3.3 配置 AC 基本功能

配置WLAN AC全局参数

```
[AC1]wlan ac-global country-code CN
[AC1]wlan ac-global ac id 0 carrier id other
```

默认国别是中国CN，运营商代码有四个，企业网应配置成other。

cmcc 中国移动

ctc 中国电信

cuc 中国联通

other 普通企业网（默认）

3.4 配置 AP 认证及与 AC 互通

配置AP的DHCP地址池及AP认证方式，控制器的地址发现采用option 43的方式。

```
[AC1]ip pool vlan10
[AC1-ip-pool-vlan10]network 10.1.10.0 mask 255.255.255.0
[AC1-ip-pool-vlan10]excluded-ip-address 10.1.10.100
[AC1-ip-pool-vlan10]gateway-list 10.1.10.1
[AC1-ip-pool-vlan10]dns-list 10.254.1.100
[AC1-ip-pool-vlan10]option 43 sub-option 3 ascii 10.1.10.100

[AC1]interface vlan 10
[AC1-Vlanif10]dhcp select global
[AC1-Vlanif10]quit
```

此时AP会得到地址10.1.X0.254，可以使用ping命令测试控制器和AP的互通性。

```
[AC1]ping 10.1.10.254
PING 10.1.10.254: 56 data bytes, press CTRL_C to break
Reply from 10.1.10.254: bytes=56 Sequence=1 ttl=64 time=2 ms
Reply from 10.1.10.254: bytes=56 Sequence=2 ttl=64 time=11 ms
Reply from 10.1.10.254: bytes=56 Sequence=3 ttl=64 time=11 ms
Reply from 10.1.10.254: bytes=56 Sequence=4 ttl=64 time=11 ms
Reply from 10.1.10.254: bytes=56 Sequence=5 ttl=64 time=11 ms
```

但是由于还没有配置AP认证列表，所以display ap all还看不到AP上线。

```
[AC1-wlan-view]display ap all
All AP information(Normal-0,UnNormal-0):
```

```
-----
AP      AP      AP      Profile  Region  AP
ID      Type      MAC      ID      ID      State
-----
Total number: 0
```


配置WLAN源接口及AP认证。

```
[AC1]wlan
[AC1-wlan-view]wlan ac source interface Vlanif 10
[AC1-wlan-view]ap-auth-mode ?
  mac-auth  MAC authenticated mode, default authenticated mode
  no-auth   No authenticated mode
  sn-auth   SN authenticated mode
```

AP认证支持三种，默认是MAC认证，需要手工添加AP列表到控制上，如认证方式被修改过，现在要重新改回MAC认证的命令是：

```
[AC1-wlan-view]ap-auth-mode mac-auth
```

手工添加认证的AP，首先要知道AP的类型和MAC，目前V2R1版的控制器的AP类型有13种，代码如下：

```
[AC1-wlan-view]display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN
17	AP6010SN-GN
19	AP6010DN-AGN
21	AP6310SN-GN
23	AP6510DN-AGN
25	AP6610DN-AGN

Total number: 13

本实验中我们用的AP是6010DN，类型代码是19，第1组的AP的MAC地址是**cccc-8110-2260**，所以我要添加AP到控制器的命令是：

```
[AC1-wlan-view]ap id 0 type-id 19 mac cccc-8110-2260
```

添加后AP后，AP的状态会经历从**fault**到**config**到**normal**的变化，最终会变为normal状态，如果等几分钟后没有变成该状态，你应该检查前面VLAN和DHCP及AP认证的配置是否有错。

```
[AC1-wlan-ap-0]dis ap all
All AP information (Normal-1, UnNormal-0):
```

AP ID	AP Type	AP MAC	Profile ID	Region ID	AP State
0	AP6010DN-AGN	cccc-8110-2260	0	0	normal

3.5 配置射频模板并应用到 AP 的天线接口上

配置WMM模板，采用默认配置。

```
[AC1-wlan-ap-0]quit
[AC1-wlan-view]wmm-profile name wmm-prof-1
[AC1-wlan-wmm-prof-wmm-prof-1]quit
```

配置2.4G射频模板，绑定WMM模板，并修改radio类型为80211bgn。

```
[AC1-wlan-view]radio-profile name radio2-prof-1
[AC1-wlan-radio-prof-radio2-prof-1]wmm-profile name wmm-prof-1
[AC1-wlan-radio-prof-radio2-prof-1]radio-type 80211bgn
Warning: Modify the Radio type may cause some parameters of Radio resume default value, are you sure to continue?[Y/N]:Y
[AC1-wlan-radio-prof-radio2-prof-1]quit
```

配置5G射频模板，绑定WMM模板，并修改radio类型为80211an。

```
[AC1-wlan-view]radio-profile name radio5-prof-1
[AC1-wlan-radio-prof-radio5-prof-1]wmm-profile name wmm-prof-1
[AC1-wlan-radio-prof-radio5-prof-1]radio-type 80211an
Warning: Modify the Radio type may cause some parameters of Radio resume default value, are you sure to continue?[Y/N]:Y
[AC1-wlan-radio-prof-radio5-prof-1]quit
```

配置完后可以使用display radio-profile all查看射频模板的ID ,配置时可以调用。

```
[AC1-wlan-view]display radio-profile all
```

```
-----  
ID      Name  
-----
```

```
0       radio2-prof-1
```

```
1       radio5-prof-1  
-----
```

```
Total: 2
```

绑定相应的射频模板到AP的天线上。

```
[AC1-wlan-view]ap 0 radio 0
```

```
[AC1-wlan-radio-0/0]radio-profile id 0
```

```
[AC1-wlan-view]ap 0 radio 1
```

```
[AC1-wlan-radio-0/1]radio-profile id 1
```

3.6 配置 Wlan-ess 接口

注意wlan-ess接口不成配置成trunk接口。

```
[AC1]interface Wlan-Ess 0
```

```
[AC1-Wlan-Ess0]dhcp enable
```

```
[AC1-Wlan-Ess0]port link-type hybrid
```

```
[AC1-Wlan-Ess0]port hybrid pvid vlan 13
```

```
[AC1-Wlan-Ess0]port hybrid untagged vlan 13
```

3.7 配置安全模板、流量模板和 WLAN 服务集

```
[AC1-wlan-view]traffic-profile id 0 name traffic-prof-1
```

```
[AC1-wlan-traffic-prof-traffic-prof-1]quit
```

```
[AC1-wlan-view]security-profile id 0 name security-prof-1
```

```
[AC1-wlan-sec-prof-security-prof-1]quit
```

```
[AC1-wlan-view]service-set name Huawei-guest1
```

```
[AC1-wlan-service-set-huawei-wlan1]ssid Huawei-guest1
```

```
[AC1-wlan-service-set-huawei-wlan1]service-vlan 13
```

```
[AC1-wlan-service-set-Huawei-guest1]wlan-ess 0
```

```
[AC1-wlan-service-set-Huawei-guest1]security-profile id 0
```

```
[AC1-wlan-service-set-Huawei-guest1]traffic-profile id 0
```

```
[AC1-wlan-service-set-Huawei-guest1]forward-mode tunnel
```

```
[AC1-wlan-service-set-Huawei-guest1]undo user-isolate
```

```
[AC1-wlan-service-set-Huawei-guest1]quit
```

3.8 绑定服务集到 AP 并提交配置执行

```
[AC1-wlan-view]ap 0 radio 0
[AC1-wlan-radio-0/0]service-set id 0
[AC1-wlan-radio-0/0]ap 0 radio 1
[AC1-wlan-radio-0/1]service-set id 0
[AC1-wlan-radio-0/1]quit

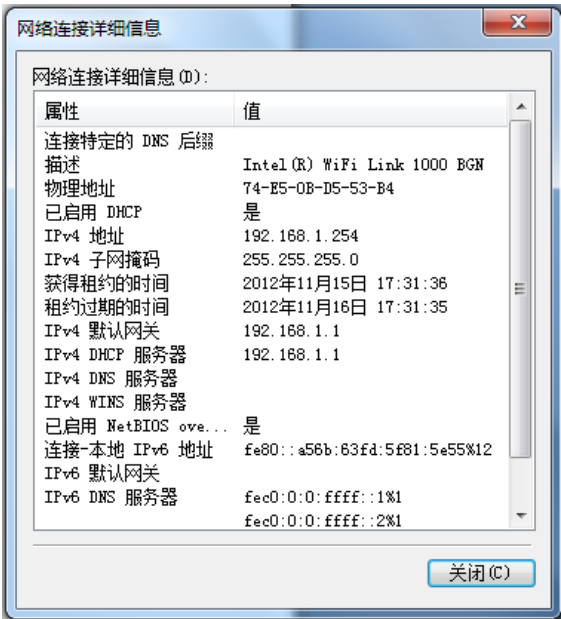
[AC1-wlan-view]commit ap 0
Warning: Committing configuration may cause service interruption,continue?[Y/N]
Y
```

配置提交后，AP会释放服务集为huawei-guestX的无线信号，认证方式为开放认证，使用无线终端接入后会获取192.168.X.0/24网段的地址，并且可以ping通控制器和交换机。

使用无线笔记本连接到Huawei-guest1。



IP地址是规划的X3VLAN的地址，如图所示。



```
C:\Users\WLAN>ping 100.100.100.100
```

```
正在 Ping 100.100.100.100 具有 32 字节的数据:
来自 100.100.100.100 的回复: 字节=32 时间=41ms TTL=255
来自 100.100.100.100 的回复: 字节=32 时间=9ms TTL=255
来自 100.100.100.100 的回复: 字节=32 时间=3ms TTL=255
来自 100.100.100.100 的回复: 字节=32 时间=12ms TTL=255
```

```
100.100.100.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间 (以毫秒为单位):
        最短 = 3ms, 最长 = 41ms, 平均 = 16ms
```

3.9 在 AC 上检查相关配置的命令

查看服务集。

```
<AC1>dis service-set all
```

```
-----
```

ID	Name	SSID
0	Huawei-guest1	Huawei-guest1

```
-----
```

Total: 1

<AC1>dis service-set id 0

```

-----
Service-set ID          : 0
Service-Set name        : Huawei-guest1
SSID                    : Huawei-guest1
Hide SSID                : disable
User isolate            : disable
Type                    : service
Maximum number of user  : 32
Association timeout(min) : 5
Traffic profile name    : traffic-prof-1
Security profile name   : security-prof-1
User profile name       : -
Wlan-ess interface      : Wlan-ess0
Igmp mode               : off
Forward mode            : tunnel
Service-vlan            : 13
Stack-vlan              : -
DHCP snooping           : disable
IPSG switch             : disable
DHCP trust port         : disable
DAI switch              : disable
ARP attack threshold(pps): 15
Protocol flag           : -
Offline-management switch: disable
-----

```

查看AP运行信息。

<AC1>dis ap all

All AP information(Normal-1,UnNormal-0):

```

-----
AP      AP      AP      Profile Region AP
ID      Type      MAC      ID      ID      State
-----
0       AP6010DN-AGN      cccc-8110-2260 0       0       normal
-----

```

<AC1>dis ap-run-info id 0

AP 0 run information:

```
Software version: V200R001C00SPC100
Hardware version: Ver.C
BIOS version: 028
Domain: CN
Cpu type: AR9344
Cpu frequency: 480 MHZ
Memory type: H5PS5162GFR-S6C&1
AP System software description: AP6010DN-AGN:V200R001C00SPC100
AP System hardware description: AP6010DN-AGN:Ver.C
AP manufacture: Huawei Technologies Co., Ltd.
AP software name: Huawei Access Point Software
AP software vendor: Huawei Technologies Co., Ltd.
AP online time: 9228 S
AP bom code: 000
Ip address: 10.1.10.254
Ip mask: 255.255.255.0
Gateway ip: 10.1.10.1
DNS server: 10.254.1.100
Memory size: 128 MB
Flash size: 32 MB
Run time: 10158 S
Up ethernet port speed: 1000 Mbps
Up ethernet port speed mode: auto
Up ethernet port duplex: full
Up ethernet port duplex mode: auto
```

查看终端信息。

```
<AC1>display access-user
```

UserID	Username	IP address	MAC
1171	74e50bd553b4	192.168.1.254	74e5-0bd5-53b4
1172	f83dff5a4f2	192.168.1.248	f83d-ffb5-a4f2

Total 2,2 printed

```
<AC1>display station assoc-info ap 0
```

STA MAC	AP-ID	RADIO-ID	SS-ID	SSID
f83d-ffb5-a4f2	0	0	0	Huawei-guest1
74e5-0bd5-53b4	0	0	0	Huawei-guest1

Total stations: 2

查看指定无线终端的详细信息。

```
[AC1]dis station status sta 5c0a-5b36-4a71
```

```
-----  
Station mac-address           : 5c0a-5b36-4a71  
Station ip-address            : 0.0.0.0  
Associated SSID                : Huawei-guest1  
Station online time(ddd:hh:mm:ss) : 000:00:01:15  
The upstream SNR(dB)          : 85.0  
The upstream aggregate receive power(dBm) : -48.0  
Station connect rate(Mbps)     : 43  
Station connect channel        : 153  
Station inactivity time(ddd:hh:mm:ss) : 000:00:00:00  
Station current state  
  Authorized for data transfer : YES  
  Qos enabled                   : YES  
  ERP enabled                   : No  
  HT rates enabled              : YES  
  Power save mode enabled       : No  
  Auth reference held           : No  
  uAPSD enabled                 : No  
  uAPSD triggerable             : No  
  uAPSD SP in progress          : No  
  This is an ATH node           : No  
  WDS workaround req            : No  
  WDS link                      : No  
Station's HT capability         : WQ  
Station ERP element(dBm)       : 0  
Station capabilities            : E  
Station's RSSI(dB)             : 47  
Station's radio mode            : 11n  
Station's AP ID                 : 0  
Station's Radio ID              : 1  
Station's Authentication Method : OPEN  
Station's Cipher Type           : NO CIPHER  
Station's User Name              : 5c0a5b364a71  
Station's Vlan ID                : 13  
Station's Channel Band-width    : 20MHz  
-----
```


关键配置汇总

```
#
 sysname AC1
#
 vlan batch 10 to 13
#
 wlan ac-global carrier id other ac id 0
#
 dhcp enable
#
 ip pool vlan10
 gateway-list 10.1.10.1
 network 10.1.10.0 mask 255.255.255.0
 excluded-ip-address 10.1.10.100
 dns-list 10.254.1.100
 option 43 sub-option 3 ascii 10.1.10.100
#
 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
#
 interface Vlanif12
 ip address 10.1.12.100 255.255.255.0
#
 interface Vlanif13
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
 interface Ethernet0/0/0
 ip address 192.168.100.200 255.255.255.0
#
 interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 to 13
#
 interface Wlan-Ess0
 port hybrid pvid vlan 13
 port hybrid untagged vlan 13
 dhcp enable
```

```
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
wlan
wlan ac source interface vlanif10
ap id 0 type-id 19 mac cccc-8110-2260 sn 210235448310C9000012
wmm-profile name wmm-prof-1 id 0
traffic-profile name traffic-prof-1 id 0
security-profile name security-prof-1 id 0
service-set name Huawei-guest1 id 0
forward-mode tunnel
wlan-ess 0
ssid Huawei-guest1
undo user-isolate
traffic-profile id 0
security-profile id 0
service-vlan 13
radio-profile name radio2-prof-1 id 0
radio-type 80211bgn
wmm-profile id 0
radio-profile name radio5-prof-1 id 1
radio-type 80211an
wmm-profile id 0
ap 0 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 0 radio 1
radio-profile id 1
service-set id 0 wlan 1
#
```

实验四 安全配置实验

实验目的

- 掌握WLAN认证模板的配置方式
- 掌握配置WEP认证的方法
- 掌握配置WPA/WPA2 PSK认证的方法
- 掌握配置WPA/WPA2 EAP认证的方法
- 掌握批量下发VAP的方法

实验规划

X是学员所在组的编号，配置时对应替换		
组网方式	直连组网 + 二层组网	
安全模板	Security-prof-wepX	ID:1 WEP密码：guest
	Security-prof-wpapskX	ID:2 WPA PSK密码：huaweipsk
	Security-prof-wpaepX	ID:3 用户名：huawei 密码：huawei
服务集	Huawei-guestX	安全模板：Security-prof-wepX
	Huawei-voiceX	SSID：Huawei-voiceX
		服务VLAN:vlan12
		转发模式：直接转发
		流量模板：traffic-prof-X
		安全模板：Security-prof-wpapskX
		Wlan-ess接口 1
		用户隔离：关闭
	Huawei-employeeX	SSID：Huawei-employeeX
		服务VLAN:vlan11

		转发模式：直接转发
		流量模板：traffic-prof-X
		安全模板：Security-prof-wpaepX
		Wlan-ess接口 2
		用户隔离：关闭

实验步骤

4.1 配置 WEP 认证

华为AC配置安全策略目前支持四类，，每一个服务集可以调用一种安全模板，如下所示：

安全策略	策略说明
wapi	中国WLAN安全标准，支持PSK认证或证书认证
wep	可以配置开放认证或share key认证，不安全
wpa	支持PSK认证或EAP认证
wpa2	支持PSK认证或EAP认证

```
[AC1-wlan-view]security-profile id 5 name test
[AC1-wlan-sec-prof-test]security-policy ?
wapi WLAN authentication and privacy infrastructure
wep Wired equivalent privacy
wpa Wi-Fi protected access
wpa2 Wi-Fi protected access version 2
```

服务集Huawei-guestX在上一个实验中采用open认证，现在要在原先配置的基础上修改其认证方式为WEP share-key认证，加密采用WEP 40位密码加密，密码是guest。

创建安全模板Security-prof-wep1，配置WEP加密密钥为guest。WEP支持40位密码和104位密码：

40位密码要配置5个ASCII字符或10个16进制数。

104位密码要配置13个ASCII字符或26个16进制数。

```
[AC1]wlan
[AC1-wlan-view]security-profile id 1 name Security-prof-wep1
[AC1-wlan-sec-prof-Security-prof-wep1]security-policy wep
[AC1-wlan-sec-prof-Security-prof-wep1]wep authentication-method share-key
[AC1-wlan-sec-prof-Security-prof-wep1]wep key wep-40 pass-phrase 0 guest
[AC1-wlan-sec-prof-Security-prof-wep1]quit
```

修改Huawei-guest1的安全模板，并重新提交到AP上执行。

```
[AC1-wlan-view]dis security-profile all
```

```
-----
ID          Name
0           security-prof-1
1           Security-prof-wep1
-----
```

```
[AC1-wlan-view]dis service-set all
```

```
-----
ID      Name                SSID
0       Huawei-guest1      Huawei-guest1
-----
```

```
Total: 1
```

```
[AC1-wlan-view]service-set id 0
[AC1-wlan-service-set-Huawei-guest1]security-profile id 1
[AC1-wlan-service-set-Huawei-guest1]quit
```

```
[AC1-wlan-view]commit ap 0
```

```
Warning: Committing configuration may cause service interruption,continue?[Y/N]
Y
```

验证WEP配置，查看安全模板的配置及绑定的服务集。

```
[AC1]display security-profile id 1
```

```
-----
Profile name          : Security-prof-wep1
Profile ID            : 1
Authentication        : Share key
Encryption            : WEP-40
-----
```

```
Service-set ID        SSID
0                     Huawei-guest1
-----
```

Bridge-profile ID	Bridge Name

使用display access-user ssid “SSID的名字” 可以查看指定SSID下面关联的用户汇总信息：

```
[AC1]display access-user ssid Huawei-guest1
```

UserID	Username	IP address	MAC

1188	5c0a5b364a71	192.168.1.252	5c0a-5b36-4a71

Total 1,1 printed			

使用display station status sta “终端MAC地址” 可以查看终端的关联详细信息，如关联的SSID名称、关联的时间、SNR信噪比、认证方式、vlan等。这里可看到终端5c0a-5b36-4a71是WEP-40位密码加密的。

```
[AC1]display station status sta 5c0a-5b36-4a71
```

Station mac-address	: 5c0a-5b36-4a71
Station ip-address	: 0.0.0.0
Associated SSID	: Huawei-guest1
Station online time(ddd:hh:mm:ss)	: 000:00:07:51
The upstream SNR(dB)	: 85.0
The upstream aggregate receive power(dBm)	: -34.0
Station connect rate(Mbps)	: 23
Station connect channel	: 1
Station inactivity time(ddd:hh:mm:ss)	: 000:00:02:15
.....	
Station's Authentication Method	: SHARE-KEY
Station's Cipher Type	: WEP-40
Station's User Name	: 5c0a5b364a71
Station's Vlan ID	: 13
Station's Channel Band-width	: 20MHz

4.2 配置 WPA PSK 认证

服务集Huawei-voiceX配置为WPA1-PSK认证。华为AC支持的WPA配置选项如下：

WPA分类	加密方式	认证方式
WPA1个人版	ccmp 或 tkip	psk(密码8-64个字符)
WPA1企业版	ccmp 或 tkip	dot1x peap 或 dot1x tls
WPA2个人版	ccmp 或 tkip	psk(密码8-64个字符)
WPA2企业版	ccmp 或 tkip	dot1x peap 或 dot1x tls

配置安全模板Security-prof-wpa-psk1，定义加密方式为TKIP，PSK密码是 huaweipsk。

```
[AC1-wlan-view]security-profile id 2 name Security-prof-wpa-psk1
[AC1-wlan-sec-prof-Security-prof-wpa-psk1]security-policy wpa
[AC1-wlan-sec-prof-Security-prof-wpa-psk1]wpa authentication-method psk
pass-phrase huaweipsk encryption-method tkip
[AC1-wlan-sec-prof-Security-prof-wpa-psk1]quit
[AC1-wlan-view]quit
```

配置服务集Huawei-voiceX调用的wlan-ess接口。

```
[AC1]interface Wlan-Ess 1
[AC1-Wlan-Ess1]dhcp enable
[AC1-Wlan-Ess1]port link-type hybrid
[AC1-Wlan-Ess1]port hybrid pvid vlan 12
[AC1-Wlan-Ess1]port hybrid untagged vlan 12
[AC1-Wlan-Ess1]quit
```

创建服务集Huawei-voiceX，并配置相关参数及绑定模板。

```
[AC1]wlan
[AC1-wlan-view]service-set id 1 name Huawei-voice1
[AC1-wlan-service-set-Huawei-voice1]ssid Huawei-voice1
[AC1-wlan-service-set-Huawei-voice1]service-vlan 12
[AC1-wlan-service-set-Huawei-voice1]wlan-ess 1
[AC1-wlan-service-set-Huawei-voice1]security-profile id 2
[AC1-wlan-service-set-Huawei-voice1]traffic-profile id 0
[AC1-wlan-service-set-Huawei-voice1]forward-mode direct-forward
[AC1-wlan-service-set-Huawei-voice1]undo user-isolate
[AC1-wlan-service-set-Huawei-voice1]quit
```

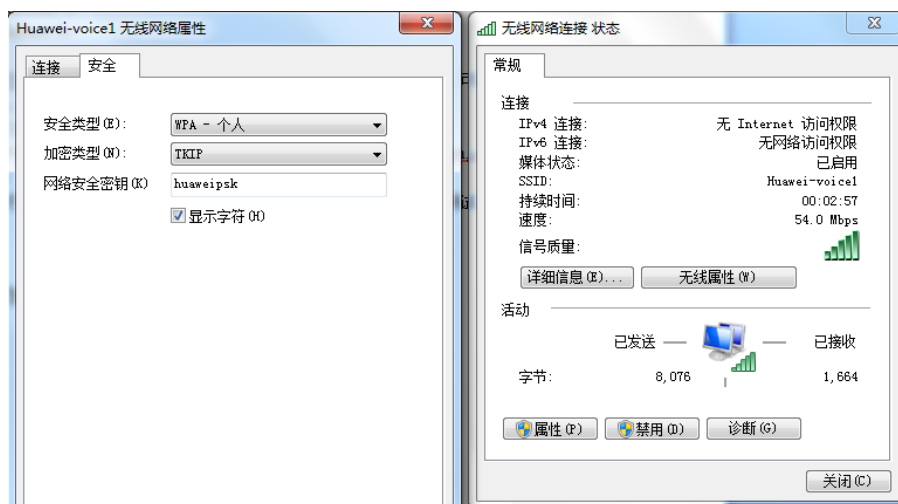
通过批处理命令批量配置VAP 如果有大量AP需要配置VAP的话 ,可以通过batch来执行 ,提高效率。

```
[AC1-wlan-view]batch ap 0 to 0 radio 0 to 1 service-set 1
Info: Command is being executed, please wait.
Success: 2
Failure: 0
```

通过命令commit all可以一次性提交全部AP的配置参数去执行 ,可以提高配置的效率。

```
[AC1-wlan-view]commit all
Warning: Committing configuration may cause service interruption,continue?[Y/N]
Y
```

此时WPA-PSK的配置已经完成 ,可以在无线PC上进行连接和测试互通性。



```
C:\Users\WLAN>ipconfig
```

无线局域网适配器 无线网络连接:

连接特定的 DNS 后缀:

本地链接 IPv6 地址.: fe80::a56b:63fd:5f81:5e55%12

IPv4 地址: 10.1.12.253

子网掩码: 255.255.255.0

默认网关.: 10.1.12.1


```
C:\Users\WLAN> ping 100.100.100.100
```

正在 Ping 100.100.100.100 具有 32 字节的数据:

来自 100.100.100.100 的回复: 字节=32 时间=20ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=4ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=7ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=13ms TTL=255

100.100.100.100 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 4ms, 最长 = 20ms, 平均 = 11ms

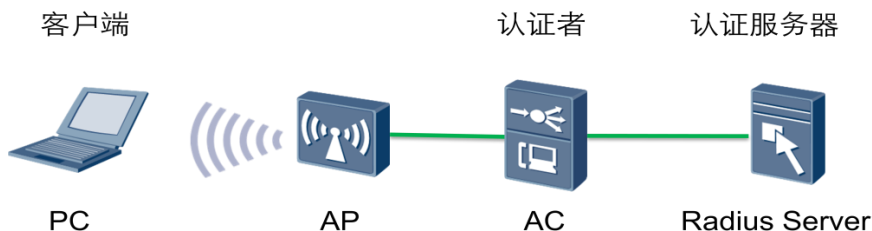
在AC上查看指定客户端的详细信息，可以看到客户端的认证类型。

```
<AC1>display station status sta 74e5-0bd5-53b4
```

```
-----
Station mac-address           : 74e5-0bd5-53b4
Station ip-address            : 0.0.0.0
Associated SSID                : Huawei-voice1
Station online time(ddd:hh:mm:ss) : 000:00:01:04
The upstream SNR(dB)          : 85.0
The upstream aggregate receive power(dBm) : -44.0
Station connect rate(Mbps)     : 37
Station connect channel        : 1
Station inactivity time(ddd:hh:mm:ss) : 000:00:00:00
Station current state
    Authorized for data transfer : YES
    .....
Station's Authentication Method : WPA1-PSK
Station's Cipher Type           : TKIP
Station's User Name             : 74e50bd553b4
Station's Vlan ID               : 12
Station's Channel Band-width    : 20MHz
```

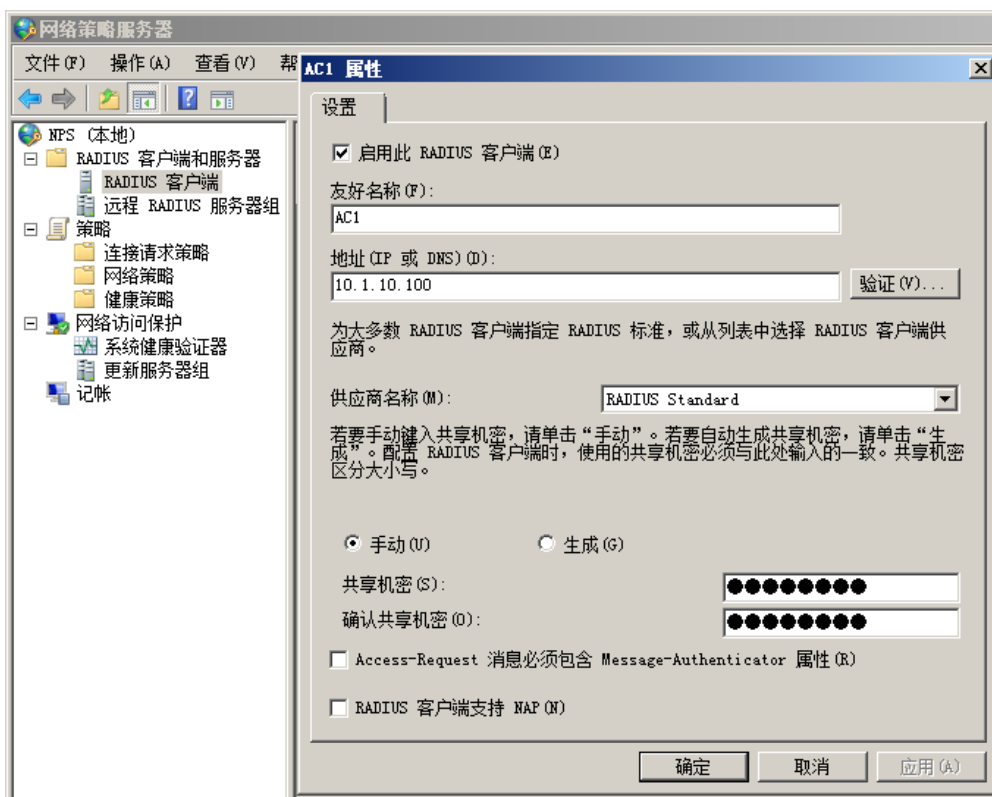
4.3 配置 WPA EAP 认证

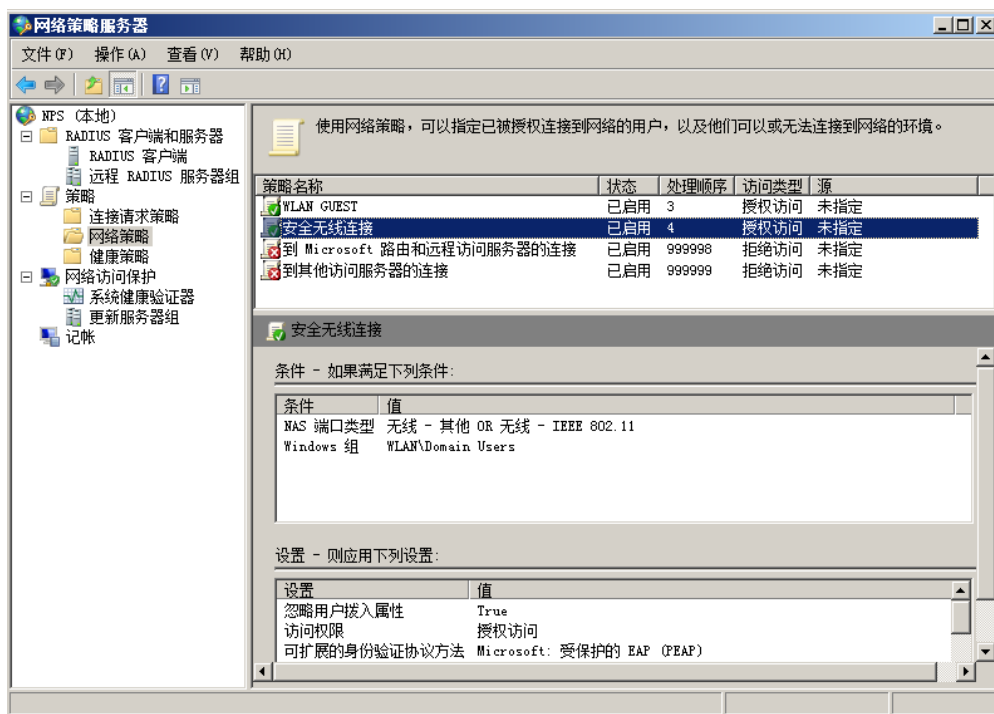
WLAN的EAP认证架构需要三个组件来实现：客户端、认证者、认证服务器。



实验中我们用到的认证服务器为10.254.1.100，radius的密码是：huawei，认证服务器已经配置好客户端和创建测试账号，用户：huawei 密码：huawei。

认证服务器已经配置好，学员无需配置。





在AC上配置radius认证服务器。

```
[AC1] radius-server template radius_huawei
[AC1-radius-radius_huawei] radius-server authentication 10.254.1.100 1812
[AC1-radius-radius_huawei] radius-server shared-key simple huawei
[AC1-radius-radius_huawei] quit
```

配置AAA方案。

```
[AC1] aaa
[AC1-aaa] authentication-scheme radius_huawei
[AC1-aaa-authen-radius_huawei] authentication-mode radius
[AC1-aaa-authen-radius_huawei] quit

[AC1-aaa] domain default
[AC1-aaa-domain-default] authentication-scheme radius_huawei
[AC1-aaa-domain-default] radius-server radius_huawei
```

配置安全模板Security-prof-wpaep1，定义加密方式为ccmp，认证方式为dot1x peap。

```
[AC1-wlan-view]security-profile id 3 name Security-prof-wpaep1
[AC1-wlan-sec-prof-Security-prof-wpaep1]security-policy wpa2
[AC1-wlan-sec-prof-Security-prof-wpaep1]wpa2 authentication-method dot1x peap
encryption-method ccmp
[AC1-wlan-sec-prof-Security-prof-wpaep1]quit
```

创建wlan-ess 接口，并且在接口上开启dot1x认证。

```
[AC1]interface Wlan-Ess 2
[AC1-Wlan-Ess2]port link-type hybrid
[AC1-Wlan-Ess2]port hybrid pvid vlan 11
[AC1-Wlan-Ess2]port hybrid untagged vlan 11
[AC1-Wlan-Ess2]dot1x-authentication enable
[AC1-Wlan-Ess2]dot1x authentication-method eap
[AC1-Wlan-Ess2]quit
```

创建服务集Huawei-employeeX，并配置相关参数及绑定模板。

```
[AC1-wlan-view]service-set id 2 name Huawei-employee1
[AC1-wlan-service-set-Huawei-employee1]ssid Huawei-employee1
[AC1-wlan-service-set-Huawei-employee1]service-vlan 11
[AC1-wlan-service-set-Huawei-employee1]wlan-ess 2
[AC1-wlan-service-set-Huawei-employee1]security-profile id 3
[AC1-wlan-service-set-Huawei-employee1]traffic-profile id 0
[AC1-wlan-service-set-Huawei-employee1]forward-mode direct-forward
[AC1-wlan-service-set-Huawei-employee1]tunnel-forward protocol dot1x
[AC1-wlan-service-set-Huawei-employee1]undo user-isolate
[AC1-wlan-service-set-Huawei-employee1]quit
```

通过批处理命令批量配置VAP 如果有大量AP需要配置VAP的话 ,可以通过batch来执行，提高效率。

```
[AC1-wlan-view]batch ap 0 to 0 radio 0 to 1 service-set 2
Info: Command is being executed, please wait.
Success: 2
Failure: 0
```

通过命令commit all可以一次性提交全部AP的配置参数去执行 ,可以提高配置的效率。

```
[AC1-wlan-view]commit all
Warning: Committing configuration may cause service interruption,continue?[Y/N]
y
```

此时WPA EAP的配置已经完成，可以通过如下命令验证配置参数。

```
[AC1]display current-configuration interface Wlan-Ess 2
```

```
#
```

```
interface Wlan-Ess2
```

```
port hybrid pvid vlan 11
```

```
port hybrid untagged vlan 11
```

```
dot1x-authentication enable
```

```
dot1x authentication-method eap
```

```
#
```

```
[AC1]dis security-profile id 3
```

```
-----
Profile name           : Security-prof-wpaeap1
Profile ID             : 3
Authentication         : WPA2 802.1x + PEAP
Encryption             : CCMP
-----
```

```
-----
Service-set ID        SSID
2                     Huawei-employee1
-----
```

```
-----
Bridge-profile ID      Bridge Name
-----
```

```
[AC1]dis service-set all
```

```
-----
ID    Name                SSID
0     Huawei-guest1       Huawei-guest1
1     Huawei-voice1       Huawei-voice1
2     Huawei-employee1    Huawei-employee1
-----
```

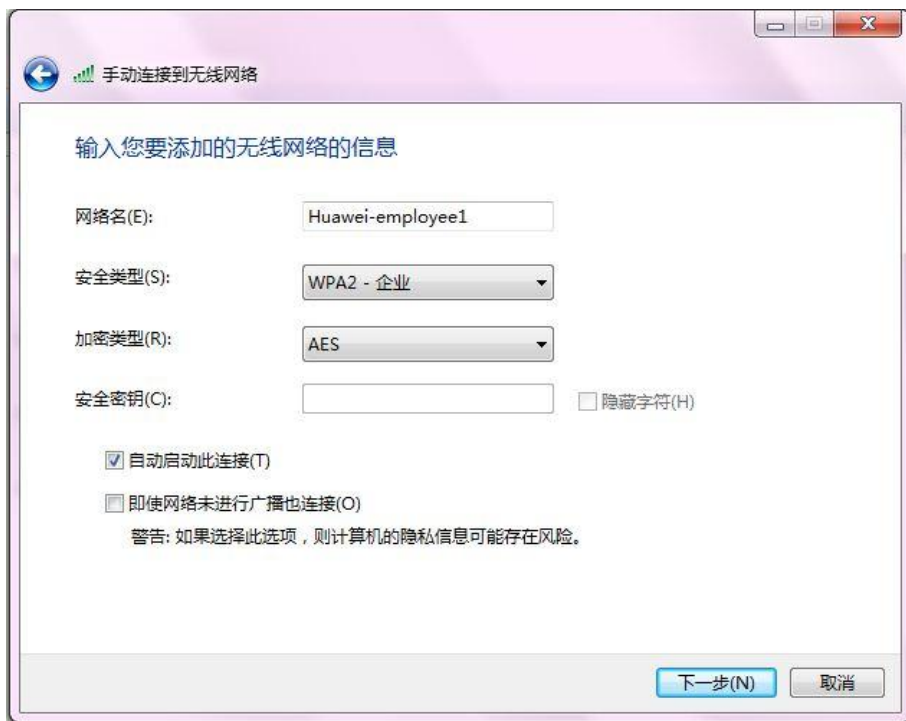
```
[AC1]display access-user
```

```
-----
UserID Username        IP address      MAC
-----
1593  huawei            10.1.11.254    5c0a-5b36-4a71
-----
```

```
Total 1,1 printed
```

4.4 配置 EAP 客户端

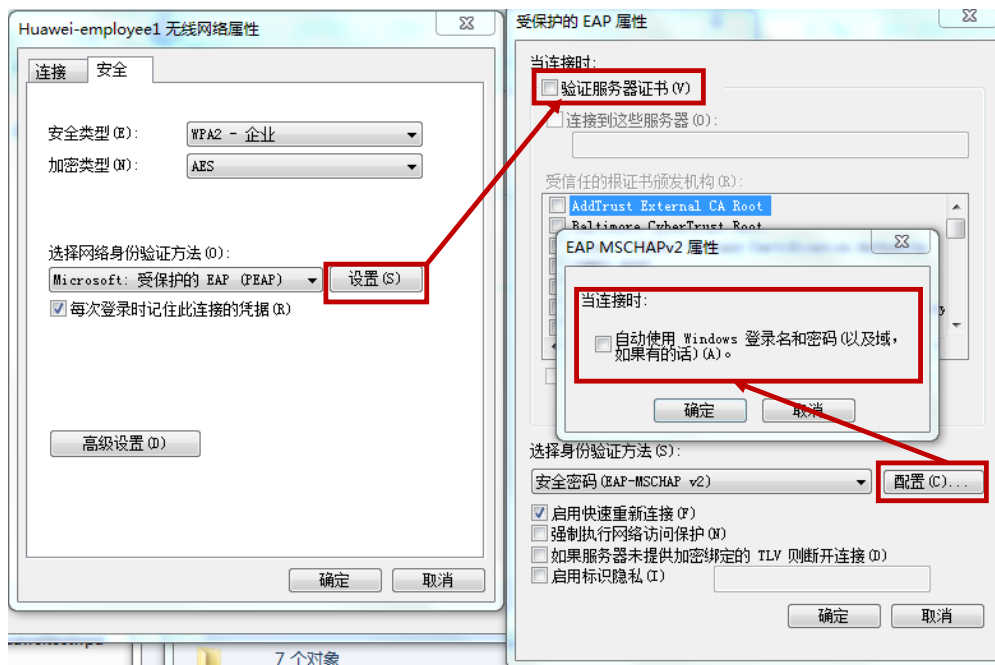
手工添加无线网络配置，不用下载CA证书，在window7终端的右下角网卡图标上单击“打开网络和共享中心”，单击“管理无线网络”，单击“添加”，点击“手工创建网络配置文件”，按如下参数配置网络配置文件，后点下一步：



完成以后点击“更改连接文件”。



更改配置如下：



此时会弹出认证信息，单击并输入用户名:huawei 密码:huawei。



可以看到用户认证成功，并且会得到相应的IP地址。



此时在无线终端上可以看到用户得到VLAN11的IP ,并且可以ping通核心交换机。

```
C:\Users\WLAN>ipconfig
```

无线局域网适配器 无线网络连接:

连接特定的 DNS 后缀:

本地链接 IPv6 地址.: fe80::a56b:63fd:5f81:5e55%12

IPv4 地址: 10.1.11.253

子网掩码: 255.255.255.0

默认网关.: 10.1.11.1

```
C:\Users\WLAN>ping 100.100.100.100
```

正在 Ping 100.100.100.100 具有 32 字节的数据:

来自 100.100.100.100 的回复: 字节=32 时间=64ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=7ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=7ms TTL=255

来自 100.100.100.100 的回复: 字节=32 时间=9ms TTL=255

100.100.100.100 的 Ping 统计信息:

数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间 (以毫秒为单位)：
最短 = 7ms，最长 = 64ms，平均 = 21ms

安全配置注意事项

安全策略配置注意事项：

如果在安全策略中采用了802.1x方式时，必须在WLAN-ESS接口视图下执行命令 `dot1x-authentication enable`和`dot1x authentication-method { chap | pap | eap }`配置WLAN-ESS接口下的认证方式为802.1x并配置WLAN用户的802.1x认证方法。

如果在安全策略中采用了MAC认证方式时，必须在WLAN-ESS接口视图下执行命令`mac-authentication enable`配置WLAN-ESS接口下的认证方式为MAC认证方式。

如果在安全策略中采用了Portal认证方式时，必须在WLAN-ESS接口视图下执行命令`web-authentication enable`配置WLAN-ESS接口下的认证方式为Portal认证方式。

802.1x+数据直接转发的组网情况下，需要在AC与AP之间配置二层协议透明传输，配置方法如下：

框式交换机设备：只需要在接口视图下执行命令`bpdu bridge enable`。

盒式交换机设备：全局视图下执行命令`l2protocol-tunnel user-defined-protocol protocol-name protocol-mac protocol-mac group-mac group-mac`；并且接口视图下执行命令`l2protocol-tunnel user-defined-protocol protocol-name enable`和命令`bpdu enable`。

802.1x+数据直接转发+三层组网情况下，由于802.1x认证时的EAP报文为二层认证报文，在AP与AC间为三层组网且AP配置为直接转发模式的场景下，报文不能通过三层转发。需要执行命令`tunnel-forward protocol dot1x`使能协议报文隧道转发功能，AP将用户的EAP报文进行隧道封装，通过隧道转发给AC处理，在AP、AC之间实现认证报文的交互。

直接转发和隧道转发配置注意事项：

如果转发模式为隧道转发，并且由AC给用户分配地址池，必须在WLAN-ESS接口视图下执行命令dhcp enable使能WLAN-ESS接口的DHCP功能。

如果转发模式为隧道转发，需要在WLAN-ESS接口视图下执行命令port hybrid pvid vlan vlan-id配置PVID。

如果转发模式为隧道转发，接入交换机上直接与AP相连的接口不能加入业务VLAN，防止产生MAC漂移。

如果转发模式为直接转发，接入交换机上直接与AP相连的接口需要加入业务VLAN。

关键配置汇总

```
sysname AC1
#
vlan batch 10 to 13
#
undo http server enable
#
wlan ac-global carrier id other ac id 0
#
dba-profile default0 type3 assure 40000 max 80000
#
dhcp enable
#
diffserv domain default
#
radius-server template radius_huawei
radius-server authentication 10.254.1.100 1812
radius-server accounting 10.254.1.100 1813
#
ip pool vlan10
gateway-list 10.1.10.1
network 10.1.10.0 mask 255.255.255.0
excluded-ip-address 10.1.10.100
dns-list 10.254.1.100
option 43 sub-option 3 ascii 10.1.10.100
#
aaa
authentication-scheme default
authentication-scheme radius_huawei
authentication-mode radius
```

```
authorization-scheme default
accounting-scheme default
domain default
authentication-scheme radius_huawei
radius-server radius_huawei
domain default_admin
local-user admin password simple admin
local-user admin service-type http
local-user huawei password simple huawei
local-user huawei privilege level 15
local-user huawei service-type telnet
#
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
#
interface Vlanif12
ip address 10.1.12.100 255.255.255.0
#
interface Vlanif13
ip address 192.168.1.1 255.255.255.0
dhcp select interface
#
interface Ethernet0/0/0
ip address 192.168.100.200 255.255.255.0
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 10 to 13
#
interface Wlan-Ess0
port hybrid pvid vlan 13
port hybrid untagged vlan 13
dhcp enable
#
interface Wlan-Ess1
port hybrid pvid vlan 12
port hybrid untagged vlan 12
dhcp enable
#
```

```
interface Wlan-Ess2
port hybrid pvid vlan 11
port hybrid untagged vlan 11
dot1x-authentication enable
dot1x authentication-method eap
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.1.10.1
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF00003DD6
snmp-agent sys-info version v3
snmp-agent trap enable basetrp
#
user-interface con 0
user-interface vty 0 4
authentication-mode aaa
user-interface vty 16 20
#
wlan
wlan ac source interface vlanif10
ap id 0 type-id 19 mac cccc-8110-2260 sn 210235448310C9000012
wmm-profile name wmm-prof-1 id 0
traffic-profile name traffic-prof-1 id 0
security-profile name security-prof-1 id 0
security-profile name Security-prof-wep1 id 1
wep authentication-method share-key
wep key wep-40 pass-phrase 0 guest
security-profile name Security-prof-wpa-psk1 id 2
security-policy wpa
wpa authentication-method psk pass-phrase huaweipsk encryption-method tkip
security-profile name Security-prof-wpa-eap1 id 3
security-policy wpa2
wpa authentication-method dot1x peap encryption-method ccmp
security-profile name test id 5
service-set name huawei-guest1 id 0
forward-mode tunnel
wlan-ess 0
ssid huawei-guest1
undo user-isolate
traffic-profile id 0
security-profile id 1
```

```
service-vlan 13
service-set name Huawei-voice1 id 1
wlan-ess 1
ssid Huawei-voice1
undo user-isolate
traffic-profile id 0
security-profile id 2
service-vlan 12
service-set name Huawei-employee1 id 2
wlan-ess 2
ssid Huawei-employee1
undo user-isolate
traffic-profile id 0
security-profile id 3
service-vlan 11
tunnel-forward protocol dot1x
radio-profile name radio2-prof-1 id 0
radio-type 80211bgn
wmm-profile id 0
radio-profile name radio5-prof-1 id 1
radio-type 80211an
wmm-profile id 0
ap 0 radio 0
radio-profile id 0
service-set id 0 wlan 1
service-set id 1 wlan 2
service-set id 2 wlan 3
ap 0 radio 1
radio-profile id 1
service-set id 0 wlan 1
service-set id 1 wlan 2
```

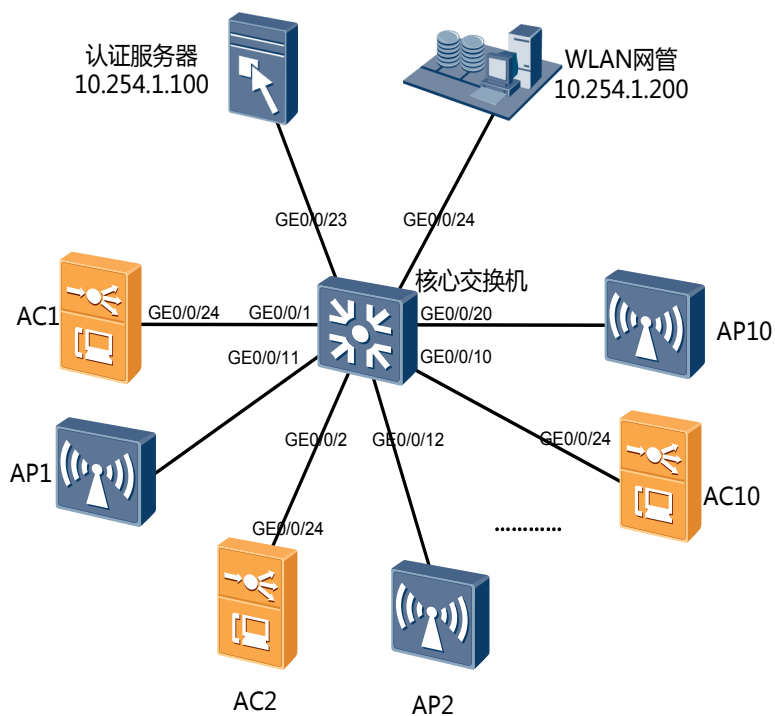
#

实验五 “旁挂+三层组网”实验

实验目标

- 掌握旁挂组网实验台的搭建方法
- 掌握三层组网的配置原理
- 掌握配置隧道转发的配置
- 验证三层组网的配置

实验规划



X是学员所在组的编号，配置时对应替换	
组网方式	旁挂组网+三层组网+隧道转发
AP变动	移动APX到核心交换机的G0/0/1X接口
AC变动	添加vlan 80X及trunk IP:10.1.201.1/24
	修改wlan source 为vlan 80X
	修改AP的vlan X0 DHCP池的option 43的配置

实验步骤

5.1 变更 AP 的接线

连接APX到核心交换机的第1X接口上，交换机接口的配置已经预先完成，如下：

```
<CoreSW3700>dis current-configuration interface Ethernet 0/0/11
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 10
 stp edged-port enable
#
```

5.2 更新 vlan 及 trunk

登录到AC有线侧LSW。

```
[LSW1]vlan 801
[LSW1-vlan801]quit
[LSW1]interface g0/0/24
[LSW1-GigabitEthernet0/0/24]port trunk allow-pass vlan 801
[LSW1-GigabitEthernet0/0/24]quit
[LSW1]interface XGigabitEthernet 0/0/27
[LSW1-XGigabitEthernet0/0/27]port trunk allow-pass vlan 801
[LSW1-XGigabitEthernet0/0/27]quit

[LSW1]console switch
Info: Switch console to AC.

[AC1]vlan 801
[AC1-vlan801]quit
[AC1]interface XGigabitEthernet 0/0/1
```

```
[AC1-XGigabitEthernet0/0/1]port trunk allow-pass vlan 801
[AC1-XGigabitEthernet0/0/1]quit

[AC1]interface Vlanif 801
[AC1-Vlanif801]ip address 10.1.201.100 24
[AC1-Vlanif801]quit
```

更新AP的默认路由的配置。

```
[AC1]undo ip route-static 0.0.0.0 0.0.0.0
[AC1]ip route-static 0.0.0.0 0.0.0.0 10.1.201.1
```

此时ACX可以ping通vlan80X的网关地址10.1.20X.1。

```
[AC1]ping 10.1.201.1
PING 10.1.201.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.201.1: bytes=56 Sequence=1 ttl=255 time=14 ms
  Reply from 10.1.201.1: bytes=56 Sequence=2 ttl=255 time=10 ms
  Reply from 10.1.201.1: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 10.1.201.1: bytes=56 Sequence=4 ttl=255 time=10 ms
  Reply from 10.1.201.1: bytes=56 Sequence=5 ttl=255 time=10 ms

--- 10.1.201.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/10/14 ms
```

5.3 AP 上线配置

修改DHCP配置和WLAN源的配置使AP可以发现控制器

```
[AC1]ip pool vlan10
[AC1-ip-pool-vlan10]dis this
#
ip pool vlan10
 gateway-list 10.1.10.1
 network 10.1.10.0 mask 255.255.255.0
 excluded-ip-address 10.1.10.100
 dns-list 10.254.1.100
 option 43 sub-option 3 ascii 10.1.10.100
#
return
```



```
[AC1-ip-pool-vlan10]undo option 43
[AC1-ip-pool-vlan10]option 43 sub-option 3 ascii 10.1.201.100
[AC1-ip-pool-vlan10]quit

[AC1]wlan
[AC1-wlan-view]wlan ac source interface Vlanif 801
Warning: Modify the source interface may cause service interruption, are you
s
ure to continue?[Y/N]:Y
```

5.4 修改服务集的转发模式为隧道模式

```
[AC1]wlan
[AC1-wlan-view]service-set id 1
[AC1-wlan-service-set-Huawei-voice1]forward-mode tunnel
[AC1-wlan-service-set-Huawei-voice1]quit
[AC1-wlan-view]service-set id 2
[AC1-wlan-service-set-Huawei-employee1]forward-mode tunnel
[AC1-wlan-service-set-Huawei-employee1]quit
[AC1-wlan-view]commit all
Warning: Committing configuration may cause service interruption,continue?[Y/N]
]Y
```

此时配置已经完成，等几分钟以后可以看到AP通过三层网络上线到控制器上，原先配置的服务集依然可用。

```
[AC1]dis ap all
All AP information(Normal-1,UnNormal-0):
```

AP ID	AP Type	AP MAC	Profile ID	Region ID	AP State
0	AP6010DN-AGN	cccc-8110-2260	0	0	normal

```
Total number: 1

[AC1]display station assoc-info ap 0
```

STA MAC	AP-ID	RADIO-ID	SS-ID	SSID
74e5-0bd5-53b4	0	0	2	Huawei-employee1
5c0a-5b36-4a71	0	0	0	huawei-guest1

```
[AC1]display service-set id 2
```

```
-----  
Service-set ID           : 2  
Service-Set name         : Huawei-employee1  
SSID                     : Huawei-employee1  
Hide SSID                 : disable  
User isolate              : disable  
Type                      : service  
Maximum number of user   : 32  
Association timeout(min) : 5  
Traffic profile name     : traffic-prof-1  
Security profile name    : Security-prof-wpaep1  
User profile name        : -  
Wlan-ess interface       : Wlan-ess2  
Igmp mode                 : off  
Forward mode             : tunnel  
Service-vlan              : 11  
Stack-vlan                : -  
DHCP snooping            : disable  
IPSG switch              : disable  
DHCP trust port          : disable  
DAI switch                : disable  
ARP attack threshold(pps): 15  
Protocol flag             : dot1x  
Offline-management switch: disable  
-----
```

关键配置

有线侧配置。

```
sysname LSW1  
#  
FTP server enable  
#  
vlan batch 10 to 13 801  
#  
undo http server enable  
#  
interface Vlanif1  
#  
interface MEth0/0/1
```

```
ip address 192.168.100.100 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 10
port trunk allow-pass vlan 10 to 13
#
.....
interface GigabitEthernet0/0/24
port link-type trunk
port trunk allow-pass vlan 10 to 12 801
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 10 to 13 801
#
```

无线侧配置。

```
sysname AC1
#
FTP server enable
#
vlan batch 10 to 13 801
#
undo http server enable
#
wlan ac-global carrier id other ac id 0
#
dba-profile default0 type3 assure 40000 max 80000
#
dhcp enable
#
diffserv domain default
#
radius-server template radius_huawei
radius-server authentication 10.254.1.100 1812
radius-server accounting 10.254.1.100 1813
#
ip pool vlan10
gateway-list 10.1.10.1
network 10.1.10.0 mask 255.255.255.0
excluded-ip-address 10.1.10.100
dns-list 10.254.1.100
```

```
option 43 sub-option 3 ascii 10.1.201.100
#
aaa
authentication-scheme default
authentication-scheme radius_huawei
authentication-mode radius
authorization-scheme default
accounting-scheme default
domain default
authentication-scheme radius_huawei
radius-server radius_huawei
domain default_admin
local-user ftp password simple ftp
local-user ftp ftp-directory flash:/
local-user ftp service-type ftp
local-user admin password simple admin
local-user admin service-type http
local-user huawei password simple huawei
local-user huawei privilege level 15
local-user huawei service-type telnet
#
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
#
interface Vlanif12
ip address 10.1.12.100 255.255.255.0
#
interface Vlanif13
ip address 192.168.1.1 255.255.255.0
dhcp select interface
#
interface Vlanif801
ip address 10.1.201.100 255.255.255.0
#
interface Ethernet0/0/0
ip address 192.168.100.200 255.255.255.0
#
interface XGigabitEthernet0/0/1
port link-type trunk
```

```
port trunk allow-pass vlan 10 to 13 801
#
interface Wlan-Ess0
port hybrid pvid vlan 13
port hybrid untagged vlan 13
dhcp enable
#
interface Wlan-Ess1
port hybrid pvid vlan 12
port hybrid untagged vlan 12
dhcp enable
#
interface Wlan-Ess2
port hybrid pvid vlan 11
port hybrid untagged vlan 11
dot1x-authentication enable
dot1x authentication-method eap
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 10.1.201.1
#
snmp-agent
snmp-agent local-engineid 000007DB7FFFFFFF00003DD6
snmp-agent sys-info version v3
snmp-agent trap enable basetrp
#
user-interface con 0
user-interface vty 0 4
authentication-mode aaa
user-interface vty 16 20
#
wlan
wlan ac source interface vlanif801
ap id 0 type-id 19 mac cccc-8110-2260 sn 210235448310C9000012
wmm-profile name wmm-prof-1 id 0
traffic-profile name traffic-prof-1 id 0
security-profile name security-prof-1 id 0
security-profile name Security-prof-wep1 id 1
wep authentication-method share-key
wep key wep-40 pass-phrase 0 guest
security-profile name Security-prof-wpa-psk1 id 2
security-policy wpa
```

```
wpa authentication-method psk pass-phrase huaweipsk encryption-method tkip
security-profile name Security-prof-wpaep1 id 3
security-policy wpa2
wpa authentication-method dot1x peap encryption-method ccmp
security-profile name test id 5
service-set name huawei-guest1 id 0
forward-mode tunnel
wlan-ess 0
ssid huawei-guest1
undo user-isolate
traffic-profile id 0
security-profile id 1
service-vlan 13
service-set name Huawei-voice1 id 1
forward-mode tunnel
wlan-ess 1
ssid Huawei-voice1
undo user-isolate
traffic-profile id 0
security-profile id 2
service-vlan 12
service-set name Huawei-employee1 id 2
forward-mode tunnel
wlan-ess 2
ssid Huawei-employee1
undo user-isolate
traffic-profile id 0
security-profile id 3
service-vlan 11
tunnel-forward protocol dot1x
radio-profile name radio2-prof-1 id 0
radio-type 80211bgn
wmm-profile id 0
radio-profile name radio5-prof-1 id 1
radio-type 80211an
wmm-profile id 0
ap 0 radio 0
radio-profile id 0
service-set id 0 wlan 1
service-set id 1 wlan 2
service-set id 2 wlan 3
ap 0 radio 1
radio-profile id 1
```

```
service-set id 0 wlan 1
service-set id 1 wlan 2
#
```

实验六 eSight WLAN网管实验（选做实验）

实验目标

- 掌握AC上SNMP协议的配置方法
- 掌握Esight发现AC的操作方法
- 掌握Esight先导式配置WLAN业务的方法
- 掌握Esight查看WLAN运行状况的方法

实验规划

eSight服务器IP	10.254.1.200
eSight服务器密码	用户名：huawei 密码：Abcd@1234（或咨询实验老师得知）
SNMP只读团体	huaweiro
SNMP读写团体	huaweirw
向导配置服务集	huawei-eSightX，PSK认证密码huaweipsk

实验步骤

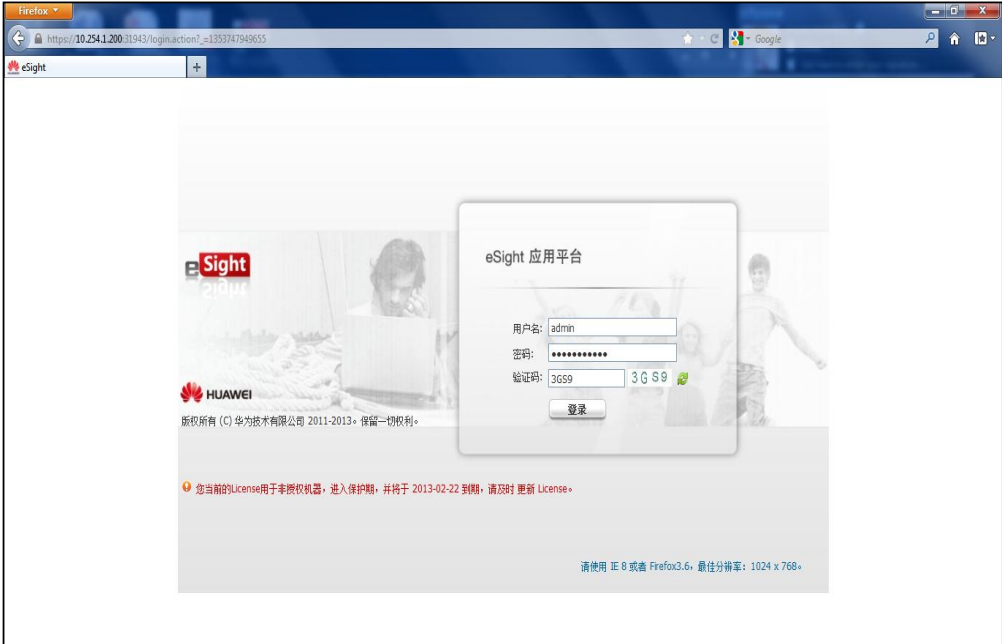
6.1 配置 AC 的 SNMP 团体参数

```
[AC1]snmp-agent community read huaweiro  
[AC1]snmp-agent community write huaweirw  
[AC1]snmp-agent sys-info version v2c
```


6.2 配置 eSight 发现 AC

使用PC接入配置的无线网络后，输入<http://10.254.1.200:8080>访问eSight服务器,用户名是admin,密码是Abcd@1234（注意：第一次安装好eSight的默认用户名是admin,密码是changeme123）。

用户浏览器推荐采用火狐内核浏览器，不推荐采用IE系列浏览器。



登录成功后，选择下拉菜单“资源”，并单击“添加设备”，按如下参数填写：

IP地址	10.1.X0.100
名称	ACX
SNMP版本	V2C
读团体字	huaweiro
写团体字	huaweirw

物理资源 > 设备资源 > 增加设备

基本信息

IP地址: 10.1.10.100 子网: /

名称: AC1

SNMP协议

选择协议模板

SNMP版本: V2c

读团体字: huaweiro 写团体字: huawerw

端口: 161 超时时间(秒): 3

Telnet协议(可选)

协议类型: Telnet 认证模式: 不认证

端口: 23 登录用户:

密码: 超时时间(秒): 60

确定 取消 应用

参数填好后，点“确定”，如果显示添加成功，说明已经已经配置正确。



物理资源 > 设备资源

子网: IP地址: 名称: 类型: 搜索

+ 增加设备 自动发现 设备导入 设置协议 同步 移动 更多

	名称	IP地址	类型	软件版本	厂商	时区	备注	操作
<input type="checkbox"/>	AC1	10.1.10.100	AC6605-AC	VRP5.70 V200R001C0...	Huawei	UTC+08:00 北京, 重庆, 香港特别行政区, 乌鲁木齐		

6.3 使用向导配置 WLAN 服务集

选择下拉菜单“网络应用”点击“WLAN管理”，如下图选择“业务管理-配置向导”：

1) 选择AC

选中ACX（X是你的组编号），点“下一步”。



2) 配置AC基本属性

这里已经在以前的实验里配置好，所以可以不用修改，直接点“下一步”。



3) 选择AP

点添加后，选择要添加配置的在线AP，点确定。



点“下一步”

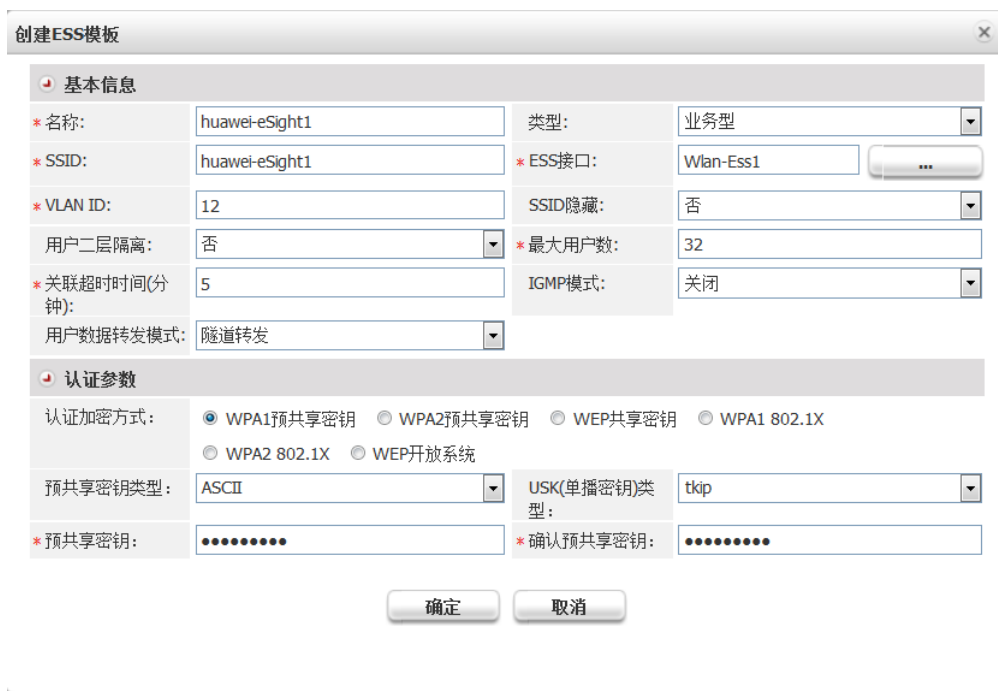


4) 配置模板

按如下参数填写。



点“增加”，创建一个ESS服务集，配置如下(wpa密码是huaweipsk):



选中所有配置的ESS 模板，点“确定”。

+ 创建

<input checked="" type="checkbox"/>	名称	类型	SSID	ESS接口	VLAN ID	用户数据转发模式
<input checked="" type="checkbox"/>	Huawei-employee1	业务型	Huawei-employee1	Wlan-Ess2	11	隧道转发
<input checked="" type="checkbox"/>	Huawei-voice1	业务型	Huawei-voice1	Wlan-Ess1	12	隧道转发
<input checked="" type="checkbox"/>	Huawei-guest	业务型	Huawei-guest	Wlan-Ess0	13	隧道转发
<input checked="" type="checkbox"/>	huawei-eSight1	业务型	huawei-eSight1	Wlan-Ess1	12	隧道转发

确定
取消

如下配置完成所有参数后，点“下一步”。

eSight

[系统](#) | [资源](#) | [故障](#) | [性能](#) | [操作维护](#) | [网络应用](#) | [报表](#)

admin ●

WLAN管理

WLAN管理 > 业务管理 > 配置向导

帮助

配置向导

AC

Fit AP

STA

SSID

Rogue AP

区域和位置

WLAN拓扑

WLAN业务拓扑

WLAN位置拓扑

AP模板: ap-profile-0

+ 创建

射频配置 1

✕ 删除

射频ID:

0

射频模板:

radio2-prof-1

...

工作状态:

打开

信道频宽:

20MHz

管理信道值:

1

发送功率等级:

1

可用天线数:

全部

ESS模板:

Huawei-voice1; huawei-guest1; huawei-esht1; Huawei-employee1;

+ 增加
 ✕ 清空

上一步
下一步
取消

5) 部署到AP

点击“部署”。

第 78 页

华为技术有限公司 版权所有，未经许可不得扩散

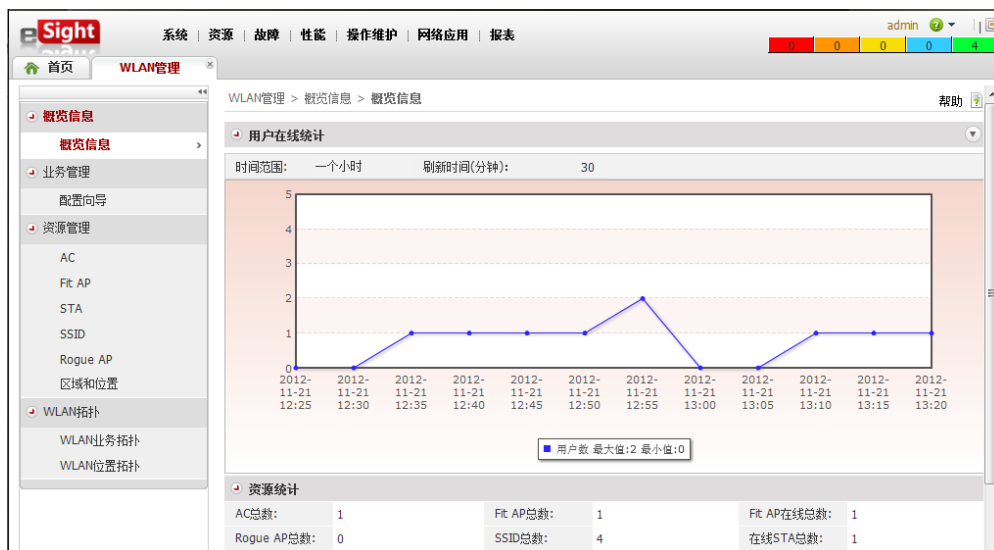


如果“部署状态”显示“完成”“部署结果”显示“成功”，此时可以单击下面的“完成”按钮完成向导化的WLAN配置。



6.4 使用 eSight 检查配置

点击“概览信息”可以看到在线用户信息，用户数量是随时间变化的折线图。

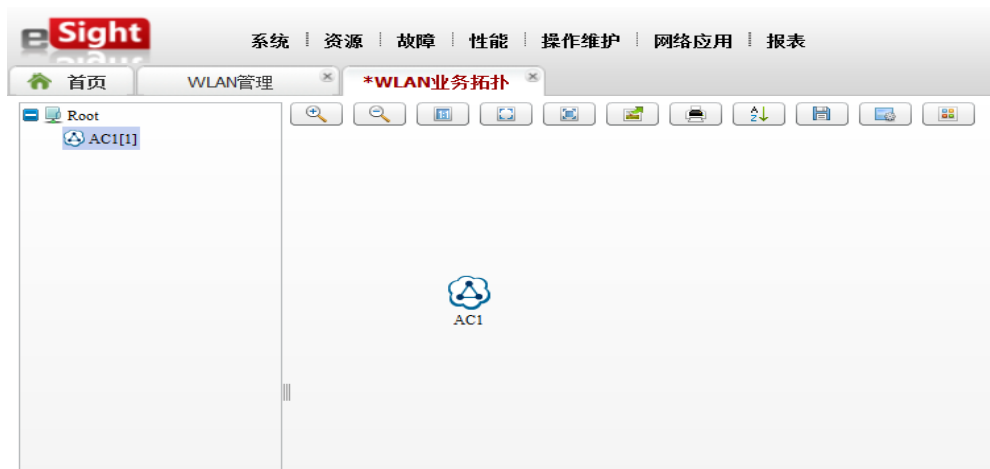


点击“资源管理”下的“SSID”，可以看到已经配置的服务集及VAP

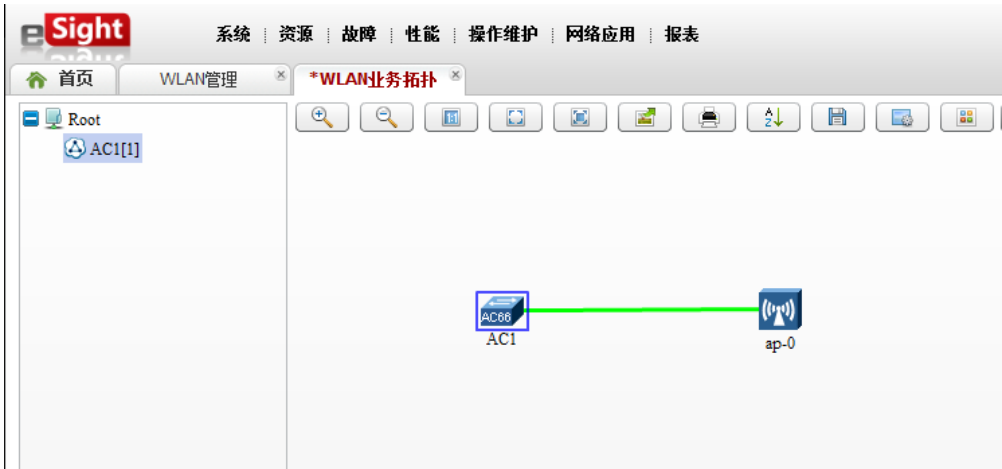
WLAN管理 > 资源管理 > SSID

SSID	接入AC名称	ESS模板名称	FIT AP数量	VAP数量	STA数量
Huawei-employee1	AC1	Huawei-employee1	1	1	0
huawei-eSight1	AC1	huawei-eSight1	1	1	1
Huawei-guest	AC1	Huawei-guest	1	1	0
Huawei-voice1	AC1	Huawei-voice1	1	1	1

点击“WLAN拓扑”下的“WLAN业务拓扑”，进入WLAN业务拓扑视图。

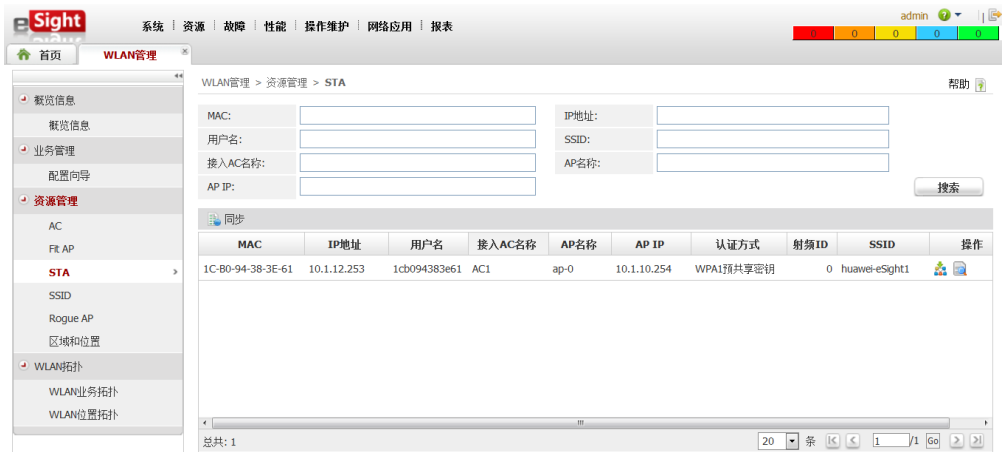



双击  AC1，可以看到AC 和AP的逻辑连接图。



点击“资源管理”下的“STA”可以看到关联到AC上的用户信息。

这里可以看到刚才通过向导配置的SSID上已经有无线用户关联上来，IP地址是vlan12的10.1.12.253，其关联的AP是10.1.10.254，认证方式是“WPA1预共享密钥”。



MAC	IP地址	用户名	接入AC名称	AP名称	AP IP	认证方式	射频ID	SSID	操作
1C-B0-94-38-3E-61	10.1.12.253	1cb094383e61	AC1	ap-0	10.1.10.254	WPA1预共享密钥	0	huawei-eSight1	

6.5 关键配置

```
snmp-agent
snmp-agent community read huaweiro
snmp-agent community write huaweirw
snmp-agent sys-info version v2c v3
```

实验七 备份配置文件，清空AC配置

实验目标

- 掌握保存AC配置文件的方法
- 掌握在AC配置FTP服务器的方法
- 掌握使用FTP备份设备配置的方法
- 掌握清空AC配置和重启AC的方法

实验规划

	LSW侧	AC侧
管理接口IP	192.168.100.100	192.168.100.200
备份配置文件名	lswvrpcfg.zip	acvrpcfg.zip
FTP账号	用户名:ftp 密码 : ftp	
FTP目录	Flash:/	

实验步骤

7.1 保存配置文件到 flash

控制器的LSW侧和AC侧的配置文件是分别存放的，因而要想妥善保存配置，应当在LSW侧和AC侧分别操作，可以使用命令save直接保存，也可以使用save 文件名的方式特别保存配置。这里采用特别保存的方式保存配置文件到闪存里。

```
<LSW1>save lswvrpcfg.zip
The current configuration will be written to the device.
Are you sure to continue?[Y/N]Y
Info: Save the configuration successfully.
```

```
<LSW1>console switch
Info: Switch console to AC.

<AC1>save acvrpcfg.zip
Are you sure to save the configuration to flash:/acvrpcfg.zip?[Y/N]:Y
Info: Save the configuration successfully.
```

保存后可以通过dir命令来验证保存的配置是否存在。

```
<AC1>dir
Directory of flash:/

   Idx  Attr      Size(Byte)  Date       Time       FileName
   ---  ---
    0  -rw-           784  Nov 16 2012 16:22:31  private-data.txt
    1  drw-           -   Oct 09 2012 17:54:33  syslogfile
    2  -rw-        1,369  Nov 16 2012 17:45:01  vrpcfg.zip
    3  -rw-    9,409,488  Oct 09 2012 18:11:01  ap6x10xn_v200r001c00spc100.bin
    4  -rw-        1,373  Nov 16 2012 18:01:16  acvrpcfg.zip

98,448 KB total (88,448 KB free)
```

7.2 在 AC 的 LSW 侧和 AC 侧分别配置 FTP 服务器

```
[LSW1]ftp server enable
[LSW1]aaa
[LSW1-aaa]local-user ftp password simple ftp ftp-directory flash:/
[LSW1-aaa]local-user ftp service-type ftp
```

```
<LSW1>console switch
Info: Switch console to AC.
```

```
[AC1]ftp server enable
[AC1]aaa
[AC1-aaa]local-user ftp password simple ftp ftp-directory flash:/
[AC1-aaa]local-user ftp service-type ftp
```

7.3 使用 FTP 备份配置到电脑上

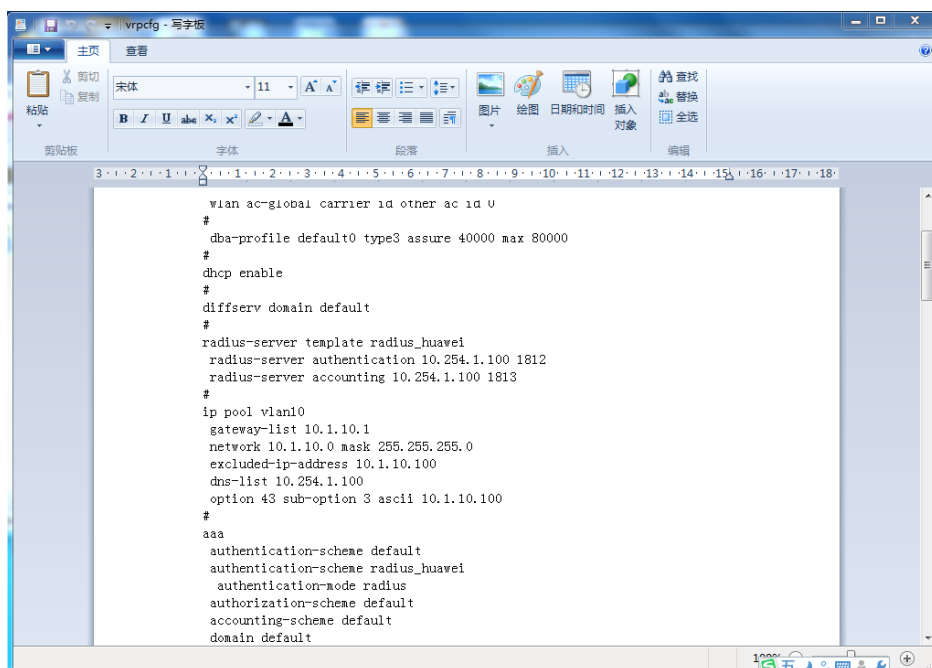
电脑使用双绞线连接到控制器的管理接口上

```
C:\Users\WLAN>d:
```

```
D:\>ftp 192.168.100.100
连接到 192.168.100.100。
220 FTP service ready.
用户(192.168.100.100:(none)):ftp
331 Password required for ftp.
密码:ftp
230 User logged in.
ftp> dir
200 Port command okay.
150 Opening ASCII mode data connection for *.
-rwxrwxrwx  1 noone  nogroup   9893 Sep 11 14:33 AC6605V200R001SPH001.pat
-rwxrwxrwx  1 noone  nogroup  41238675 Jan 01  2000 AC6605V200R001C00.cc
-rwxrwxrwx  1 noone  nogroup   1104 Nov 15 10:41 private-data.txt
-rwxrwxrwx  1 noone  nogroup    36 Sep 11 14:38 $_patchstate_reboot
drwxrwxrwx  1 noone  nogroup    0 Sep 11 14:38 syslogfile
drwxrwxrwx  1 noone  nogroup    0 Sep 11 14:39 resetinfo
-rwxrwxrwx  1 noone  nogroup  41223836 Oct 09 17:42 ac6605v200r001c00spc100.c
c
-rwxrwxrwx  1 noone  nogroup    680 Nov 16 17:54 vrpcfg.zip
-rwxrwxrwx  1 noone  nogroup    686 Nov 16 18:01 lswvrpcfg.zip
226 Transfer complete.
ftp: 收到 660 字节, 用时 0.00秒 660.00千字节/秒。
ftp> get lswvrpcfg.zip
200 Port command okay.
150 Opening ASCII mode data connection for lswvrpcfg.zip.
226 Transfer complete.
ftp: 收到 686 字节, 用时 0.00秒 686000.00千字节/秒。
```

```
D:\>ftp 192.168.100.200
连接到 192.168.100.200。
220 FTP service ready.
用户(192.168.100.200:(none)):ftp
331 Password required for ftp.
密码:ftp
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: 收到 1373 字节, 用时 0.00秒 1373000.00千字节/秒。
ftp>
```

打开电脑D盘根目录，可以看到备份的配置文件，ZIP文件可以使用解压缩解压后查看。



7.4 清空 AC 配置

实验后，为避免残余配置对后续实验的影响，要求学生在实验完成后，关闭设备之前清空设备保存的配置信息；同时，实验开始时，确认设备从空配置启动，否则执行配置清空，并重启设备。

清空控制器的配置需要在有线侧和无线侧分别操作：

```

<LSW6605>reset saved-configuration
The configuration will be erased to reconfigure. Continue? [Y/N]:Y
Ctrl+Y 切换到无线侧继续清空无线侧的配置
<AC>reset saved-configuration
The configuration will be erased to reconfigure. Continue? [Y/N]:Y
  
```

重启控制器的命令是：

```

<LSW>reboot
<LSW>reboot
<LSW>Otherwise, unsaved configuration will be lost. Continue?[Y/N]:Y
<LSW>Warning: All the configuration will be saved to the configuration file for
the next startup:, Continue?[Y/N]:N
  
```

```
<LSW>System will reboot! Continue?[Y/N]:Y
```

关键配置

```
FTP server enable
```

```
aaa
```

```
local-user ftp password simple ftp  
local-user ftp ftp-directory flash:/  
local-user ftp service-type ftp
```

附件：核心交换机基础配置（供搭建实验环境参考）

```
<CoreSW3700>dis current-configuration
#
!Software Version V100R005C01SPC100
sysname CoreSW3700
#
vlan batch 10 to 12 20 to 22 30 to 32 40 to 42 50 to 52 60 to 62 70 to 72 80 to
82 90 to 92 100 to 102
vlan batch 800 to 810 900
#
dhcp enable
#
undo http server enable
#
drop illegal-mac alarm
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password simple admin
local-user admin service-type http
#
interface Vlanif10
ip address 10.1.10.1 255.255.255.0
#
interface Vlanif11
ip address 10.1.11.1 255.255.255.0
dhcp select interface
#
interface Vlanif12
ip address 10.1.12.1 255.255.255.0
dhcp select interface
#
interface Vlanif20
ip address 10.1.20.1 255.255.255.0
#
interface Vlanif21
```

```
ip address 10.1.21.1 255.255.255.0
dhcp select interface
#
interface Vlanif22
ip address 10.1.22.1 255.255.255.0
dhcp select interface
#
interface Vlanif30
ip address 10.1.30.1 255.255.255.0
#
interface Vlanif31
ip address 10.1.31.1 255.255.255.0
dhcp select interface
#
interface Vlanif32
ip address 10.1.32.1 255.255.255.0
dhcp select interface
#
interface Vlanif40
ip address 10.1.40.1 255.255.255.0
#
interface Vlanif41
ip address 10.1.41.1 255.255.255.0
dhcp select interface
#
interface Vlanif42
ip address 10.1.42.1 255.255.255.0
dhcp select interface
#
interface Vlanif50
ip address 10.1.50.1 255.255.255.0
#
interface Vlanif51
ip address 10.1.51.1 255.255.255.0
dhcp select interface
#
interface Vlanif52
ip address 10.1.52.1 255.255.255.0
dhcp select interface
#
interface Vlanif60
ip address 10.1.60.1 255.255.255.0
#
```



```
interface Vlanif61
 ip address 10.1.61.1 255.255.255.0
 dhcp select interface
#
interface Vlanif62
 ip address 10.1.62.1 255.255.255.0
 dhcp select interface
#
interface Vlanif70
 ip address 10.1.70.1 255.255.255.0
#
interface Vlanif71
 ip address 10.1.71.1 255.255.255.0
 dhcp select interface
#
interface Vlanif72
 ip address 10.1.72.1 255.255.255.0
 dhcp select interface
#
interface Vlanif80
 ip address 10.1.80.1 255.255.255.0
#
interface Vlanif81
 ip address 10.1.81.1 255.255.255.0
 dhcp select interface
#
interface Vlanif82
 ip address 10.1.82.1 255.255.255.0
 dhcp select interface
#
interface Vlanif90
 ip address 10.1.90.1 255.255.255.0
#
interface Vlanif91
 ip address 10.1.91.1 255.255.255.0
 dhcp select interface
#
interface Vlanif92
 ip address 10.1.92.1 255.255.255.0
 dhcp select interface
#
interface Vlanif100
 ip address 10.1.100.1 255.255.255.0
```

```
#
interface Vlanif101
 ip address 10.1.101.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 10.1.102.1 255.255.255.0
 dhcp select interface
#
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 Vlanif807
 ip address 10.1.207.1 255.255.255.0
#
interface Vlanif808
 ip address 10.1.208.1 255.255.255.0
#
interface Vlanif809
 ip address 10.1.209.1 255.255.255.0
#
interface Vlanif810
 ip address 10.1.210.1 255.255.255.0
#
interface Vlanif900
 ip address 10.254.1.1 255.255.255.0
#
interface Ethernet0/0/1
```

```
port link-type trunk
port trunk allow-pass vlan 10 to 12 801
#
interface Ethernet0/0/2
port link-type trunk
port trunk allow-pass vlan 10 20 to 22 801 to 802
#
interface Ethernet0/0/3
port link-type trunk
port trunk allow-pass vlan 30 to 32 803
#
interface Ethernet0/0/4
port link-type trunk
port trunk allow-pass vlan 30 40 to 42 803 to 804
#
interface Ethernet0/0/5
port link-type trunk
port trunk allow-pass vlan 50 to 52 805
#
interface Ethernet0/0/6
port link-type trunk
port trunk allow-pass vlan 50 60 to 62 805 to 806
#
interface Ethernet0/0/7
port link-type trunk
port trunk allow-pass vlan 70 to 72 807
#
interface Ethernet0/0/8
port link-type trunk
port trunk allow-pass vlan 70 80 to 82 807 to 808
#
interface Ethernet0/0/9
port link-type trunk
port trunk allow-pass vlan 90 to 92 809
#
interface Ethernet0/0/10
port link-type trunk
port trunk allow-pass vlan 90 100 to 102 809 to 810
#
interface Ethernet0/0/11
port link-type access
port default vlan 10
stp edged-port enable
```

```
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 20
 stp edged-port enable
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 30
 stp edged-port enable
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 40
 stp edged-port enable
#
interface Ethernet0/0/15
 port link-type access
 port default vlan 50
 stp edged-port enable
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 60
 stp edged-port enable
#
interface Ethernet0/0/17
 port link-type access
 port default vlan 70
 stp edged-port enable
#
interface Ethernet0/0/18
 port link-type access
 port default vlan 80
 stp edged-port enable
#
interface Ethernet0/0/19
 port link-type access
 port default vlan 90
 stp edged-port enable
#
interface Ethernet0/0/20
 port link-type access
```

```
port default vlan 100
stp edged-port enable
#
interface Ethernet0/0/21
port link-type access
port default vlan 900
stp edged-port enable
#
interface Ethernet0/0/22
port link-type access
port default vlan 900
stp edged-port enable
#
interface Ethernet0/0/23
port link-type access
port default vlan 900
stp edged-port enable
#
interface Ethernet0/0/24
port link-type access
port default vlan 900
stp edged-port enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface NULL0
#
interface LoopBack100
ip address 100.100.100.100 255.255.255.255
#
interface LoopBack200
ip address 200.200.200.200 255.255.255.255
#
ip route-static 172.16.1.0 255.255.255.0 10.1.201.100
ip route-static 172.16.2.0 255.255.255.0 10.1.202.100
ip route-static 172.16.3.0 255.255.255.0 10.1.203.100
ip route-static 172.16.4.0 255.255.255.0 10.1.204.100
```

```
ip route-static 172.16.5.0 255.255.255.0 10.1.205.100
ip route-static 172.16.6.0 255.255.255.0 10.1.206.100
ip route-static 172.16.7.0 255.255.255.0 10.1.207.100
ip route-static 172.16.8.0 255.255.255.0 10.1.208.100
ip route-static 172.16.9.0 255.255.255.0 10.1.209.100
ip route-static 172.16.10.0 255.255.255.0 10.1.210.100
ip route-static 192.168.1.0 255.255.255.0 10.1.10.100
ip route-static 192.168.2.0 255.255.255.0 10.1.20.100
ip route-static 192.168.3.0 255.255.255.0 10.1.30.100
ip route-static 192.168.4.0 255.255.255.0 10.1.40.100
ip route-static 192.168.5.0 255.255.255.0 10.1.50.100
ip route-static 192.168.6.0 255.255.255.0 10.1.60.100
ip route-static 192.168.7.0 255.255.255.0 10.1.70.100
ip route-static 192.168.8.0 255.255.255.0 10.1.80.100
ip route-static 192.168.9.0 255.255.255.0 10.1.90.100
ip route-static 192.168.10.0 255.255.255.0 10.1.100.100
#
snmp-agent
snmp-agent local-engineid 000007DB7F00000100004E58
snmp-agent sys-info version v3
#
user-interface con 0
idle-timeout 0 0
user-interface vty 0 4
user privilege level 15
set authentication password simple huawei
#
return
```