大数据、云计算、人工智能、信息安全人才培养丛书
“互联网+”新形态一体化教材

无线网络技术

WUXIAN WANGLUO JISHU

主编◎马　翔　高大伟　周　华

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

大数据、云计算、人工智能、信息安全人才培养丛书
“互联网+”新形态一体化教材

无线网络技术

WUXIAN WANGLUO JISHU

主　编◎马　翔　高大伟　周　华
副主编◎朴锦春　金　勋　徐立清

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书通过丰富的实例，系统、深入地阐述了无线网络技术的基本概念、基本原理和基本分析方法。全书共 10 个项目，包括 802.1X 典型配置、AC 热备典型配置、AP 典型配置、IPv6 配置及相关认证、AC 典型配置、典型配置举例、本地 Portal server 典型配置、无线网链路配置、无线典型配置、无线网络传输控制。本书所有知识点都结合具体实例讲解，便于读者理解和掌握，可作为高等院校通信类、电子信息类、计算机类等相关专业的教材，也可作为相关专业技术人员和管理人员的参考用书。

图书在版编目（CIP）数据

无线网络技术 / 马翔，高大伟，周华主编 . — 上海：
上海交通大学出版社，2021.8（2023.2 重印）

ISBN 978-7-313-25056-8

Ⅰ. ①无… Ⅱ. ①马… ②高… ③周… Ⅲ. ①无线网
Ⅳ. ① TN92

中国版本图书馆 CIP 数据核字（2021）第 124575 号

无线网络技术
WUXIAN WANGLUO JISHU

主　　编：马翔　高大伟　周华
出版发行：上海交通大学出版社
邮政编码：200030
印　　制：北京荣玉印刷有限公司
开　　本：889 mm × 1194 mm　1/16
字　　数：306 千字
版　　次：2021 年 8 月第 1 版
书　　号：ISBN 978-7-313-25056-8
定　　价：54.00 元

地　　址：上海市番禺路 951 号
电　　话：64071208
经　　销：全国新华书店
印　　张：13.5
印　　次：2023 年 2 月第 2 次印刷

前言

信息化时代初期，有线网络无处不在，人们通过各种有线技术进行“互联网”体验。随着人们对信息的需求不断增加，这些有线技术也变得更加先进，功能更加强大。但是，随着时间的推移，人们开始渴望更多的功能、更便捷的通信，而笔记本计算机的普及和无线网络技术的出现，使这一需求得到较好的满足。

伴随着“宽带大众化”的口号，无线互联网的时代已经到来。但是，高效的无线网络互联仍然面临着一些关键性的技术难题。更高的容量、更多的功能以及更少的使用限制，是人们对于无线技术的需求，但这些需求却很难同时得到满足。另外，业界面临的频谱资源短缺的问题日益突出，这就要求无线通信能更高效地利用稀缺的频谱资源。这些问题对于网络技术的发展是很大的挑战。为了满足不断增长的用户需求，市场上已经出现了多种相互竞争的无线技术。

本书以具体的无线网配置为主线讲解最新的无线网络技术知识。全书共 10 个项目，包括 802.1X 典型配置、AC 热备典型配置、AP 典型配置、IPv6 配置及相关认证、AC 典型配置、典型配置举例、本地 Portal server 典型配置、无线网链路配置、无线典型配置、无线网络传输控制。通过 10 个项目的具体配置实训，使读者掌握无线网技术的应用及相关的知识。

本书在编写上具有如下特点：

（1）采用任务驱动、案例引导的撰写方式，从工作过程出发，从项目出发，以实际应用为主线，突破以知识点的层次递进作为理论体系的传统模式，将职业工作过程系统化，按照工作过程来组织和讲解知识，培养学生的职业技能和职业素养。

（2）根据读者的学习特点，在编写过程中将内容划分为多个任务，每一个任务通过任务描述、知识准备、任务实施、知识拓展、技能拓展等模块进行具体的配置训练和知识讲解，以“做”为中心，“教”和“学”都围绕着“做”展开，在学中做，在做中学，从而提高学生的自我学习能力。

（3）紧跟行业技能发展，着重于当前主流技术讲解，与行业联系密切，达到学以致用的目的。

此外，本书作者还为广大一线教师提供了服务于本书的教学资源库，有需要者可致电 13810412048 或发邮件至 2393867076@qq.com。

本书可作为高校计算机相关专业教学用书，也可作为相关技术人员技术培训或工作参考用书。由于编写时间仓促，加之网络技术发展迅猛，书中存在的不足和疏漏之处，敬请广大读者批评指正，以便再版时修订完善，在此表示衷心的感谢。

目录

项目 1　802.1X 典型配置

在 IEEE 802 LAN 中，未经授权的用户可以没有任何阻碍地通过连接到局域网的设备进入网络。随着局域网技术的广泛应用，特别是运营网络的出现，对网络的安全认证的需求已经提上了日程。在以太网技术便捷的基础上，提供用户对网络或设备访问合法性认证，已经成为业界关注的焦点。IEEE 802.1X 协议正是在这样的背景下提出的。

IEEE 802.1X 是一个基于端口的网络存取控制（port-based network access control）标准，为 LAN 提供点对点式的安全接入。这是 IEEE 标准委员会针对以太网的安全缺陷而专门制定的标准，能够在利用 IEEE 802 LAN 优势的基础上，提供一种对连接到局域网设备的用户进行认证的手段。

本项目的任务结构如下：

任务 1.1　802.1X Auth-Fail/Guest VLAN 典型配置

任务描述

如图 1-1 所示，AC 与 AP 使用 VLAN 100 关联，Client 和 AP 被划分在不同的 VLAN 中，且 Client 和 AP 都是通过 DHCP server 获取 IP 地址的。要求：

（1）采用 EAP 中继方式对客户端进行本地 802.1X 认证。

（2）本地 EAP 认证方法采用 peap-mschapv2。

（3）当 Client 认证通过正常上线后，可以接入 VLAN 300 进行网络办公。

（4）配置 Guest VLAN 400，当 Client 不进行认证时，只能进入 VLAN 400 访问特定的网络资源。

（5）配置 Auth-Fail VLAN 500，当 Client 认证失败时，只能访问 VLAN 500 中的资源。

笔记

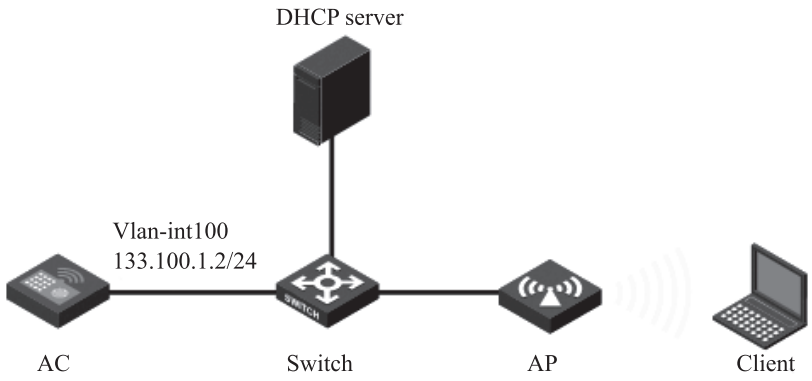


图 1-1　802.1X Auth-Fail/Guest VLAN 典型配置

知识准备

1. Guest VLAN

在有些网络如校园网或企业网中，用户在通过 802.1X 认证之前属于“缺省”的 VLAN（Guest VLAN），用户访问该 VLAN 内的资源不需要认证，只能访问有限的网络资源，但不能访问其他网络资源 。这个 VLAN 就是 Guest VLAN。没有通过认证的客户端计算机处于 Guest VLAN 中，它们只能访问 Guest VLAN 服务器的资源，用户从处于 Guest VLAN 的服务器上可以获取 802.1X 客户端软件、升级客户端，或执行其他一些应用升级程序（如防病毒软件、操作系统补丁程序等）。这是因为如果没有专用的认证客户端或者客户端版本过低等，就会导致在一定的时间内端口上无客户端能认证成功，接入设备就会把该端口加入 Guest VLAN。认证成功后，端口离开 Guest VLAN，用户就可以访问特定的网络资源。

2. 802.11ac

从核心技术来看，802.11ac 是在 802.11n 标准之上建立起来的，包括将使用 802.11n 的 5 GHz 频段。

不过在通道的设置上，802.11ac 将沿用 802.11n 的 MIMO（多进多出）技术，为它的传输速率达到 Gbit/s 量级打下基础，第一个阶段的目标达到的传输速率为 1 Gbit/s，目的是达到有线电缆的传输速率。

802.11ac 每个通道的工作频宽将由 802.11n 的 40 MHz，提升到 80 MHz 甚至 160 MHz，再加上约 10% 的实际频率调制效率提升，最终理论传输速度将由 802.11n 最高的 600 Mbit/s 跃升至 1 Gbit/s。当然，实际传输率可能在 300~400 Mbit/s，接近目前 802.11n 实际传输率（75~150 Mbit/s）的 3 倍，足以在一条信道上同时传输多路压缩视频流。

此外，802.11ac 还将兼容 802.11 全系列所有标准和规范，包括即将发布的 802.11s 无线网状架构以及 802.11u 等。在安全性方面，它将完全遵循 802.11i 安全标准的所有内容，使无线连接能够达到企业级用户的需求。根据 802.11ac 的实现目标，未来 802.11ac 将帮助企业或家庭实现无缝漫游，并且支持无线产品相应的安全、管理以及诊断等应用。

3. Switch

Switch 是交换机，前身是网桥。交换机使用硬件来完成以前网桥使用软件来完成的过滤、学习和转发任务。Switch 速度比 HUB 快，这是由于 HUB 不知道目标地址在何处，所以发送数据到所有的端口。而 Switch 中有一张转发表，如果知道目标地址在何处，就把数据发送到指定地点；如果不知道目标地址就把数据发送到所有端口。经过这样过滤可以降低整个网络的数据传输量，提高效率。

笔记

任务实施

1.1.1 配置思路

由于本地 EAP 认证方法采用 peap-mschapv2，因此需要配置用于 EAP 认证的 SSL 服务器端策略。

1.1.2 配置注意事项

（1）Auth-Fail VLAN 和 Guest VLAN 都只支持 clear 类型的无线服务模板。

（2）配置 AP 的序列号时，确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

在无特殊组网要求的情况下，无线环境中通常使用端口安全特性。

1.1.3 配置步骤

1. 配置 AC

（1）配置 AC 接口。

```
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 133.100.1.2 16
[AC-Vlan-interface100] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN
[AC] vlan 200
[AC-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN
[AC] vlan 300
```

笔记

```
[AC-vlan300] quit
# 创建 VLAN 400 作为 Guest VLAN
[AC] vlan 400
[AC-vlan400] quit
# 创建 VLAN 500 作为 Auth-Fail VLAN
[AC] vlan 500
[AC-vlan500] quit
# 配置 AC 的 GigabitEthernet1/0/1 接口的属性为 Trunk，并允许 VLAN 100、VLAN 200、VLAN 300、VLAN 400 和 VLAN 500 通过
[AC] interface gigabitethernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300 400 500
[AC-GigabitEthernet1/0/1] quit
# 创建 WLAN-ESS1 接口，并配置接口的属性为 Hybrid
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200、VLAN 300、VLAN 400 和 VLAN 500 不带 Tag 通过
[AC-WLAN-ESS1] port hybrid pvid vlan 200
[AC-WLAN-ESS1] undo port hybrid vlan 1
[AC-WLAN-ESS1] port hybrid vlan 200 300 400 500 untagged
# 在 Hybrid 端口上使能 MAC-VLAN 功能
[AC-WLAN-ESS1] mac-vlan enable
# 在 WLAN-ESS 接口上配置端口安全模式为 802.1X 认证
[AC-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 配置认证失败的用户可以访问 VLAN 500
[AC-WLAN-ESS1] dot1x auth-fail vlan 500
# 配置未认证的用户可以访问 VLAN 400
[AC-WLAN-ESS1] dot1x guest-vlan 400
[AC-WLAN-ESS1] quit
```

（2）配置无线服务。

```
# 创建 clear 类型的服务模板 1
[AC] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service
[AC-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1
```

```
[AC-wlan-st-1] bind wlan-ess 1
# 启用无线服务
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

（3）配置射频接口并绑定服务模板。

```
# 创建 AP 的管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号
[AC] wlan ap officeap model WA2620E-AGN
[AC-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 AP 的 radio 2 视图
[AC-wlan-ap-officeap] radio 2
# 将在 AC 上配置的 clear 类型的服务模板 1 与射频 2 进行绑定
[AC-wlan-ap-officeap-radio-2] service-template 1
# 使能 AP 的 radio 2
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
```

（4）全局配置 802.1X 本地认证及用户名。

```
# 全局下使能端口安全
[AC] port-security enable
# 配置 802.1X 认证模式为 EAP
[AC] dot1x authentication-method eap
# 创建 SSL 服务器端策略 test
[AC] ssl server-policy test
[AC-ssl-server-policy-test] quit
# 配置 EAP Profile 为 test
[AC] eap-profile test
# 绑定 SSL 服务器端策略 test
[AC-eap-prof-test] ssl-server-policy test
# 配置认证方式为 peap-mschapv2
[AC-eap-prof-test] method peap-mschapv2
[AC-eap-prof-test] quit
# 配置 local-server
[AC] local-server authentication eap-profile test
# 配置 local-user 用户名为 user，密码为 123456
[AC] local-user user
```

笔记

笔记

```
[AC-luser-user] password simple 123456
[AC-luser-user] service-type lan-access
[AC-luser-user] quit
```

2. 配置 Switch

```
# 创建 VLAN 100、VLAN 300、VLAN 400 和 VLAN 500，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN，VLAN 400 作为 Guest VLAN，VLAN 500 作为 Auth-Fail VLAN
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
[Switch] vlan 500
[Switch-vlan500] quit
# 配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的属性为 Access，并允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# 使能 PoE 功能
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/3 接口的属性为 Access，并允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
[Switch-GigabitEthernet1/0/3] quit
```

1.1.4 验证配置

笔记

（1）在 AC 上通过 display wlan client 命令可以看到，当 Client 直接关联 SSID 而不进行认证时，Client 进入 VLAN 400。

```
[AC] display wlan client
 Total Number of Clients             : 1
Client Information
 SSID: service
-------------------------------------------------------------------------------------------------
MAC Address    User Name          APID/RID IP Address              VLAN
-------------------------------------------------------------------------------------------------
0021-632f-f7bb  NULL              1   /2   0.0.0.0                 400
-------------------------------------------------------------------------------------------------
```

（2）当 Client 使用正确的用户名和密码通过 iNode 认证上线时，Client 进入 VLAN 300。在“iNode 智能客户端”选择“新建”选项，如图 1-2 所示。

图 1-2　iNode 智能客户端

在弹出的“新建连接向导”中单击“下一步（N）”按钮，如图 1-3 所示。

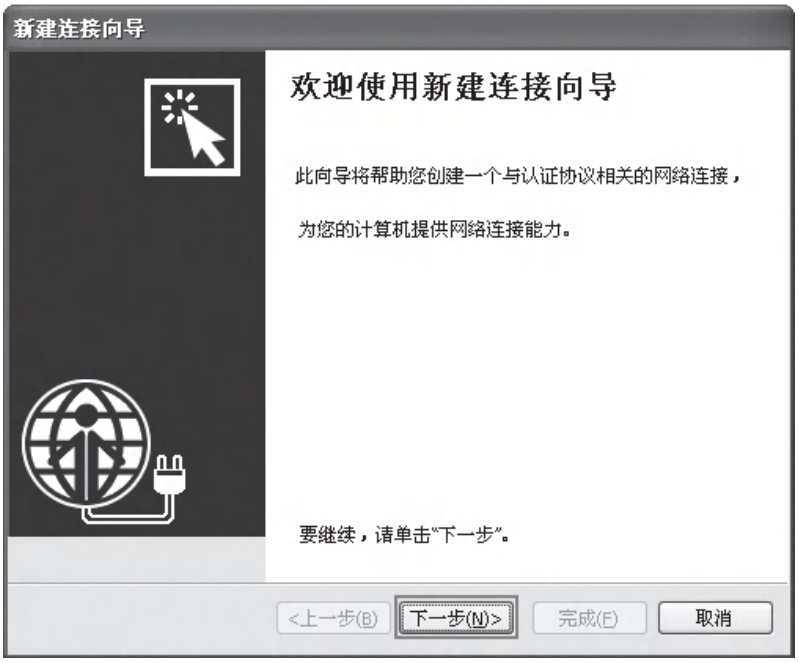


图 1-3　新建连接向导

笔记

选择“802.1X 协议（X）”，单击“下一步（N）”按钮，如图 1-4 所示。

图 1-4　选择认证协议

选择“普通连接（C）”，单击“下一步（N）”按钮，如图 1-5 所示。

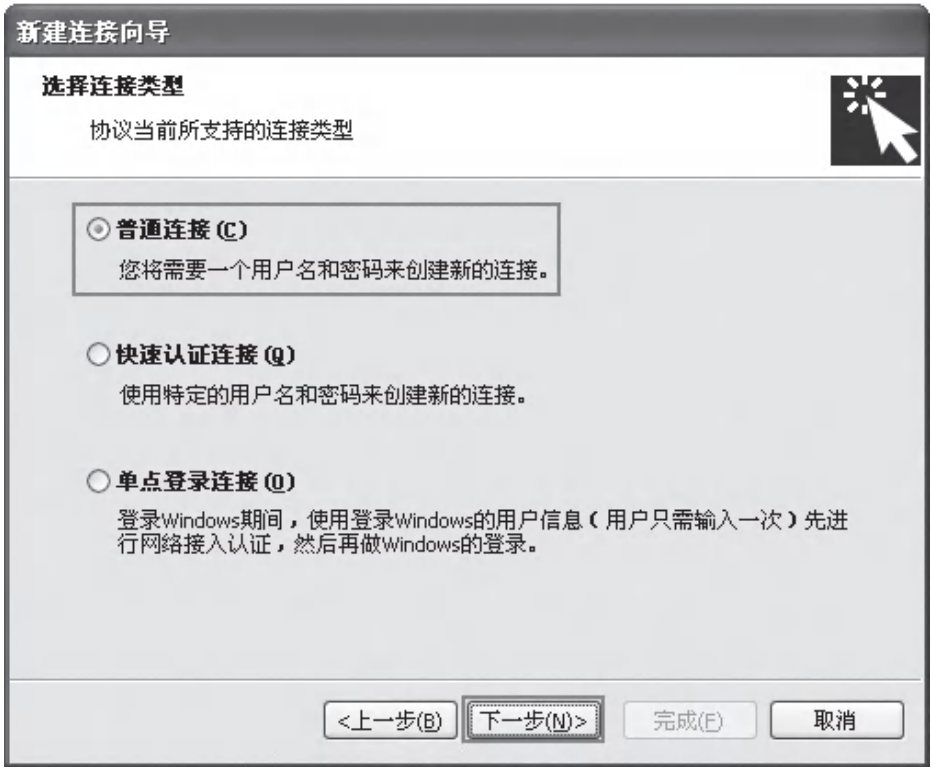


图 1-5　选择连接类型

选择“启用高级认证（E）”和“证书认证（I）”，单击“证书设置（S）...”按钮，如图 1-6 所示。

笔记

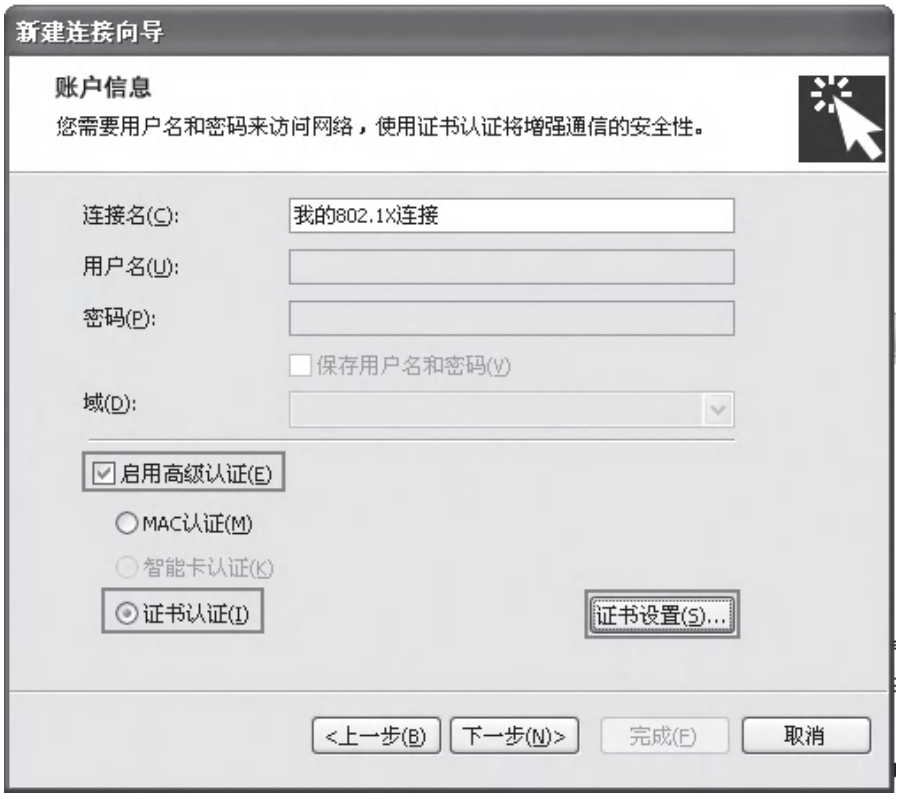


图 1-6　账户信息

在弹出的“证书认证高级设置”窗口中，选择认证类型为“PEAP（A）”，输入错误的用户名和密码，单击“确定”按钮，如图 1-7 所示。

图 1-7　证书认证高级设置

笔记

使用 display wlan client 命令查看设备所处 VLAN 为认证通过的 VLAN 300。

```
[AC] display wlan client
 Total Number of Clients             : 1
Client Information
 SSID: service
-------------------------------------------------------------------------------------------------
MAC Address    User Name          APID/RID IP Address              VLAN
-------------------------------------------------------------------------------------------------
0023-8933-21ff    user            1   /2    0.0.0.0                300
-------------------------------------------------------------------------------------------------
```

（3）当 Client 使用错误的用户名和密码通过 iNode 认证上线时，Client 上线后进入 VLAN 500。

在 AC 上使用 display wlan client 命令查看设备所处 VLAN 为 Auth-Fail 的 VLAN 500。

```
[AC] display wlan client
 Total Number of Clients             : 1
Client Information
 SSID: service
-------------------------------------------------------------------------------------------------
MAC Address    User Name          APID/RID IP Address              VLAN
-------------------------------------------------------------------------------------------------
2477-0374-2cc0  user              1   /2    0.0.0.0                500
-------------------------------------------------------------------------------------------------
```

在 AC 上 ping 接入的 Client，确认 Client 加入 Auth-Fail 的 VLAN 并且通信正常（Client 的 IP 地址通过 DHCP 获得，可在 Client 上进行查看）。

```
[AC] ping 133.20.0.1
  PING 133.20.0.1: 56  data bytes, press CTRL_C to break
  Reply from 133.20.0.1: bytes=56 Sequence=0 ttl=128 time=2 ms
  Reply from 133.20.0.1: bytes=56 Sequence=1 ttl=128 time=2 ms
  Reply from 133.20.0.1: bytes=56 Sequence=2 ttl=128 time=1 ms
  Reply from 133.20.0.1: bytes=56 Sequence=3 ttl=128 time=2 ms
  Reply from 133.20.0.1: bytes=56 Sequence=4 ttl=128 time=1 ms

  --- 133.20.0.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

笔记

从下面的显示信息中可以看到，MAC 地址为 0023-8933-21ff 的 Client 认证成功并进入 VLAN 300，MAC 地址为 2477-0374-2cc0 的 Client 认证失败并进入 VLAN 500（Auth-fail VLAN），MAC 地址为 0021-632f-f7bb 的 Client 不认证则进入 VLAN 400（Guest VLAN）。

```
[AC] display wlan client
Total Number of Clients             : 3
Client Information
SSID: service
-------------------------------------------------------------------------------------------------
MAC Address    User Name     APID/RID IP Address                VLAN
-------------------------------------------------------------------------------------------------
0021-632f-f7bb  NULL              1   /2   0.0.0.0               400
0023-8933-21ff  user              1   /2   0.0.0.0               300
2477-0374-2cc0 user               1   /2   0.0.0.0               500
-------------------------------------------------------------------------------------------------
```

任务 1.2　802.1X 热备典型配置

任务描述

如图 1-8 所示，AC 1 和 AC 2 均支持双机热备，现要求 AC 1 和 AC 2 在运行双机热备情况下支持 802.1X 客户端的信息备份，在主备 AC 切换的过程中，客户端不会重新上下线，可以继续正常通信。要求如下：

（1）采用加密类型的服务模板，加密套件采用 AES-CCMP。

（2）在 AC 1 正常工作的情况下，Client 通过 AC 1 进行 802.1X 认证接入；在 AC 1 发生故障的情况下，Client 通过 AC 2 接入。

（3）802.1X 的认证方式采用 EAP 中继方式。

（4）采用 RADIUS 服务器作为认证服务器，RADIUS 服务器上注册的接入设备 NAS-IP 是 133.1.1.3/16。

（5）防止用户通过恶意假冒其他域账号从本端口接入网络。

（6）配置 VRRP 来提高链路的可靠性，保证业务流量在切换过程中不会中断。

（7）将 VLAN 10 作为备份 VLAN，用于双机热备。

笔记

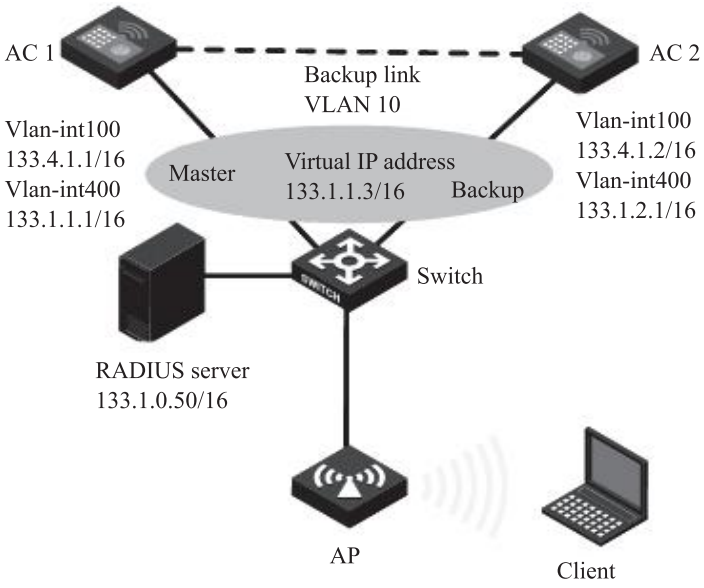


图 1-8　802.1X 热备典型配置

任务实施

1.2.1 配置思路

（1）为实现 802.1X 认证，需要在 AC 上配置端口安全。

（2）为实现 802.1X 认证状态的备份，需要配置双机热备功能。

（3）在无线环境中，为了保证 AC 在切换过程中，无线服务不中断，同时使客户端的信息在 AC 间同步，需要配置双 AC 备份及 IACTP 隧道。

（4）在双 AC 备份配置中，为了让 AP 优先连接到 AC 1，需要为 AC 1 配置较高的优先级。

（5）在 VRRP 配置中，为了让 AC 1 成为 Master，需要为 AC 1 配置较高的优先级。

（6）由于部分 802.1X 客户端不支持与设备进行握手报文的交互，因此需要关闭设备的在线用户握手功能，避免该类型的在线用户因没有回应握手报文而被强制下线。

（7）对于无线局域网来说，802.1X 认证可以由客户端主动发起，或由无线模块发现用户后自动触发，不需要通过端口定期发送 802.1X 组播报文的方式来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭 802.1X 组播触发功能。

（8）为了防止用户通过恶意假冒其他域账号从本端口接入网络，需要配置端口的强制认证域。

1.2.2 配置注意事项

（1）主备 AC 热备相关配置必须保持一致。

（2）配置 AP 的序列号时，应确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

笔记

1.2.3 配置步骤

1. 配置 AC 1

（1）配置 AC 1 接口。

```
# 创建 VLAN 10 作为双机热备的 VLAN
<AC1> system-view
[AC1] vlan 10
[AC1-vlan10] quit
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 133.4.1.1 16
[AC1-Vlan-interface100] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN
[AC1] vlan 200
[AC1-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN
[AC1] vlan 300
[AC1-vlan300] quit
# 创建 VLAN 400 作为 RADIUS server 所在 VLAN，并配置其 IP 地址
[AC1] vlan 400
[AC1-vlan400] quit
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] ip address 133.1.1.1 16
[AC1-Vlan-interface400] quit
# 配置 AC 1 与 Switch 相连的 GigabitEthernet 1/0/1 接口的属性为 Trunk，并允许 VLAN 10、VLAN 200、VLAN 300、VLAN 400 通过
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 10 200 300 400
[AC1-GigabitEthernet1/0/1] quit
```

笔记

（2）配置无线接口。

```
# 创建 WLAN-ESS1 接口
[AC1] interface wlan-ess 1
# 配置 WLAN-ESS1 接口类型为 Hybrid
[AC1-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过
[AC1-WLAN-ESS1] port hybrid pvid vlan 200
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 200 untagged
# 使能 MAC-VLAN 功能
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
```

（3）配置无线服务。

```
# 创建 crypto 类型的服务模板 1
[AC1] wlan service-template 1 crypto
# 将 WLAN-ESS1 接口绑定到服务模板 1
[AC1-wlan-st-1] bind wlan-ess 1
# 设置当前服务模板的 SSID 为 service
[AC1-wlan-st-1] ssid service
# 配置加密套件为 CCMP
[AC1-wlan-st-1] cipher-suite ccmp
# 配置安全信息元素为 RSN
[AC1-wlan-st-1] security-ie rsn
# 启用无线服务
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

（4）配置射频接口并绑定服务模板。

```
# 创建 AP 的管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号
[AC1] wlan ap officeap model WA2620E-AGN
[AC1-wlan-ap-officeap] serial-id 21023529G007C000020
# 指定该 AP 在 AC 1 上优先级为 7
[AC1-wlan-ap-officeap] priority level 7
# 进入 AP 的 radio 2 视图
```

```
[AC1-wlan-ap-officeap] radio 2
# 将服务模板 1 绑定到 radio 2 口并使能 radio 2
[AC1-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
[AC1-wlan-ap-officeap-radio-2] radio enable
[AC1-wlan-ap-officeap-radio-2] return
```

笔记

（5）配置 802.1X。

```
# 全局下使能端口安全
[AC1] port-security enable
# 选择 802.1X 认证方式为 EAP 中继方式
[AC1] dot1x authentication-method eap
# 进入 WLAN-ESS1 接口视图
[AC1] interface wlan-ess 1
# 配置 WLAN-ESS1 接口的端口安全模式为 userlogin-secure-ext
[AC1-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 使能 WLAN-ESS1 上端口安全的双机热备功能
[AC1-WLAN-ESS1] port-security synchronization enable
# 使能 11key 类型的密钥协商功能
[AC1-WLAN-ESS1] port-security tx-key-type 11key
# 指定 802.1X 用户使用的强制认证域 office，以防止用户通过恶意假冒其他域账号从本端口接入网络
[AC1-WLAN-ESS1] dot1x mandatory-domain office
# 关闭 802.1X 的组播触发功能，以节省无线网络的通信带宽
[AC1-WLAN-ESS1] undo dot1x multicast-trigger
# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线
[AC1-WLAN-ESS1] undo dot1x handshake
[AC1-WLAN-ESS1] quit
```

（6）配置 RADIUS 认证策略和认证域。

```
# 创建名称为 office 的 RADIUS 方案并进入该方案视图
[AC1] radius scheme office
# 配置 RADIUS 方案的主认证服务器及其通信密钥
[AC1-radius-office] primary authentication 133.1.0.50
[AC1-radius-office] key authentication key
# 配置 AC 1 发送 RADIUS 报文使用的 nas-ip 地址为 133.1.1.3
[AC1-radius-office] nas-ip 133.1.1.3
[AC1-radius-office] quit
```

笔记

```
# 创建 ISP 域 office，并进入其视图
[AC1] domain office
# 为 lan-access 用户配置计费为 none，不计费
[AC1-isp-office] accounting lan-access none
# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office
[AC1-isp-office] authentication lan-access radius-scheme office
# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office
[AC1-isp-office] authorization lan-access radius-scheme office
[AC1-isp-office] quit
```

（7）配置 VRRP。

```
# 在 VLAN 400 中配置 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 133.1.1.3
[AC1] interface vlan-interface 400
[AC1-Vlan-interface400] vrrp vrid 1 virtual-ip 133.1.1.3
# 配置 AC 1 在备份组 1 中的优先级为 200
[AC1-Vlan-interface400] vrrp vrid 1 priority 200
[AC1-Vlan-interface400] quit
```

（8）配置双机热备。

```
# 配置备份 VLAN 编号为 VLAN 10
[AC1] dhbk vlan 10
# 使能双机热备功能，且支持对称路径
[AC1] dhbk enable backup-type symmetric-path
# 配置双机热备模式下的设备 ID 为 1
[AC1] nas device-id 1
```

（9）配置双 AC 备份。

```
# 配置备份 AC（AC 2）的 IP 地址为 133.4.1.2
[AC1] wlan backup-ac ip 133.4.1.2
# 开启 AC 间热备份功能
[AC1] hot-backup enable
# 配置热备 AC 间连接心跳周期为 2000 毫秒（缺省情况下）
[AC1] hot-backup hellointerval 2000
# 配置热备 AC 间数据端口的 VLAN ID 为 100
[AC1] hot-backup vlan 100
# 配置客户端信息备份功能
[AC1] wlan backup-client enable
```

（10）配置 IACTP 隧道。

笔记

```
# 配置漫游隧道，漫游组名称为 roam
[AC1] wlan mobility-group roam
# 配置 IACTP 隧道的源地址为 133.4.1.1，成员地址为 133.4.1.2
[AC1-wlan-mg-roam] source ip 133.4.1.1
[AC1-wlan-mg-roam] member ip 133.4.1.2
# 开启 IACTP 隧道
[AC1-wlan-mg-roam] mobility-group enable
[AC1-wlan-mg-roam] quit
```

2. 配置 AC 2

（1）配置 AC 2 接口。

```
# 创建 VLAN 10 作为双机热备的 VLAN
<AC2> system-view
[AC2] vlan 10
[AC2-vlan10] quit
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 133.4.1.2 16
[AC2-Vlan-interface100] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN
[AC2] vlan 200
[AC2-vlan200] quit
# 创建 VLAN 300 作为 Client 接入的业务 VLAN
[AC2] vlan 300
[AC2-vlan300] quit
# 创建 VLAN 400 作为 RADIUS server 所在 VLAN，并配置其 IP 地址
[AC2] vlan 400
[AC2-vlan400] quit
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] ip address 133.1.1.2 16
[AC2-Vlan-interface400] quit
```

笔记

```
# 配置 AC2 与 Switch 相连的 GigabitEthernet 1/0/1 接口的属性为 Trunk，并允许 VLAN 10、VLAN 200、VLAN 300、VLAN 400 通过
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 10 200 300 400
[AC2-GigabitEthernet1/0/1] quit
```

（2）配置无线接口。

```
# 创建 WLAN-ESS1 接口
[AC2] interface wlan-ess 1
# 配置 WLAN-ESS1 接口的属性为 Hybrid
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 200，禁止 VLAN 1 通过并允许 VLAN 200 不带 Tag 通过
[AC2-WLAN-ESS1] port hybrid pvid vlan 200
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 200 untagged
# 开启 MAC-VLAN 功能
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
```

（3）配置无线服务。

```
# 创建 crypto 类型的服务模板 1
[AC2] wlan service-template 1 crypto
# 将 WLAN-ESS1 接口绑定到服务模板 1
[AC2-wlan-st-1] bind wlan-ess 1
# 设置当前服务模板的 SSID 为 service
[AC2-wlan-st-1] ssid service
# 配置加密套件为 AES-CCMP
[AC2-wlan-st-1] cipher-suite ccmp
# 配置安全信息元素为 RSN
[AC2-wlan-st-1] security-ie rsn
# 使能无线服务
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
```

（4）配置射频接口并绑定服务模板。

笔记

```
# 创建 AP 的管理模板，其名称为 officeap，型号名称选择 WA2620E-AGN，并配置其序列号
[AC2] wlan ap officeap model WA2620E-AGN
[AC2-wlan-ap-officeap] serial-id 21023529G007C000020
# 进入 AP 的 radio 2 视图
[AC2-wlan-ap-officeap] radio 2
# 将在 AC 2 上配置的服务模板 1 与射频 2 进行关联，Client 通过服务模板 1 接入 VLAN 300
[AC2-wlan-ap-officeap-radio-2] service-template 1 vlan-id 300
# 使能 AP 的 radio 2
[AC2-wlan-ap-officeap-radio-2] radio enable
[AC2-wlan-ap-officeap-radio-2] return
```

（5）配置 802.1X。

```
# 全局下使能端口安全
[AC2] port-security enable
# 选择 802.1X 认证方式为 EAP
[AC2] dot1x authentication-method eap
# 配置 WLAN-ESS1 接口的端口安全模式为 userlogin-secure-ext
[AC2-WLAN-ESS1] port-security port-mode userlogin-secure-ext
# 使能 WLAN-ESS1 上端口安全的双机热备功能
[AC2-WLAN-ESS1] port-security synchronization enable
# 使能 11key 类型的密钥协商功能
[AC2-WLAN-ESS1] port-security tx-key-type 11key
# 指定 802.1X 用户使用的强制认证域 office，以防止用户通过恶意假冒其他域账号从本端口接入网络
[AC2-WLAN-ESS1] dot1x mandatory-domain office
# 关闭 802.1X 的组播触发功能，以节省无线网络的通信带宽
[AC2-WLAN-ESS1] undo dot1x multicast-trigger
# 关闭在线用户握手功能，以避免不支持在线握手功能的客户端被强制下线
[AC2-WLAN-ESS1] undo dot1x handshake
[AC2-WLAN-ESS1] quit
```

笔记

（6）配置 RADIUS 认证策略和认证域。

```
# 创建名称为 office 的 RADIUS 方案并进入该方案视图
[AC2] radius scheme office
# 配置 RADIUS 方案的主认证服务器及其通信密钥
[AC2-radius-office] primary authentication 133.1.0.50
[AC2-radius-office] key authentication key
# 配置 AC 2 发送 RADIUS 报文使用的 nas-ip 地址为 133.1.1.3
[AC2-radius-office] nas-ip 133.1.1.3
[AC2-radius-office] quit
# 创建 ISP 域 office，并进入其视图
[AC2] domain office
# 为 lan-access 用户配置计费为 none，不计费
[AC2-isp-office] accounting lan-access none
# 为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office
[AC2-isp-office] authentication lan-access radius-scheme office
# 为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office
[AC2-isp-office] authorization lan-access radius-scheme office
[AC2-isp-office] quit
```

（7）配置 VRRP。

```
# 在 VLAN 400 中配置 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 133.1.1.3
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] vrrp vrid 1 virtual-ip 133.1.1.3
[AC2-Vlan-interface400] quit
```

（8）配置双机热备。

```
# 配置备份 VLAN 为 VLAN 10
[AC2] dhbk vlan 10
# 使能双机热备功能，且支持对称路径
[AC2] dhbk enable backup-type symmetric-path
# 配置双机热备模式下的设备 ID 为 2
[AC2] nas device-id 2
```

（9）配置双 AC 备份。

笔记

```
# 配置备份 AC（AC 1）的 IP 地址为 133.4.1.1
[AC2] wlan backup-ac ip 133.4.1.1
# 开启 AC 间热备份功能
[AC2] hot-backup enable
# 配置热备 AC 间连接心跳周期为 2000 毫秒（缺省情况下）
[AC2] hot-backup hellointerval 2000
# 配置热备 AC 间数据端口的 VLAN 编号为 VLAN 100
[AC2] hot-backup vlan 100
# 配置客户端信息备份功能
[AC2] wlan backup-client enable
```

（10）配置 IACTP 隧道。

```
# 配置漫游隧道，漫游组名称为 roam
[AC2] wlan mobility-group roam
# 配置 IACTP 隧道的源地址为 133.4.1.2，成员地址为 133.4.1.1
[AC2-wlan-mg-roam] source ip 133.4.1.2
[AC2-wlan-mg-roam] member ip 133.4.1.1
# 开启 IACTP 隧道
[AC2-wlan-mg-roam] mobility-group enable
[AC2-wlan-mg-roam] quit
```

3. 配置 Switch

```
# 创建 VLAN 100、VLAN 300 和 VLAN 400，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 300 为无线用户接入的 VLAN，VLAN 400 作为 RADIUS server 所在 VLAN
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] vlan 400
[Switch-vlan400] quit
# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/1
```

笔记

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/2 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 RADIUS server 相连的 GigabitEthernet1/0/3 接口的属性为 Access，并允许 VLAN 400 通过
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 400
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/4 接口的属性为 Access，并允许 VLAN 100 通过
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
# 使能 PoE 功能
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

4. 配置 RADIUS 服务器

下面以 iMC 为例 [使用 iMC 版本为：iMC PLAT 7.0（E0202）、iMC UAM 7.0（E0202）]，说明 RADIUS 服务器的基本配置。

（1）增加接入设备。登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的“接入策略管理”→“接入设备管理”→“接入设备配置”菜单项，单击“增加”按钮，进入“增加接入设备”页面，单击“手工增加”按钮，进入“手工增加接入设备”页面，如图 1-9 所示。设置与 AC 交互报文时使用的认证、计费共享密钥为“key”；设置认证和计费的端口号分别为“1812”和“1813”；选择业务类型为“ LAN 接入业务”；选择接入设备类型为“H3C（General）”；选择或手工增加接入设备，添加 IP 地址为“133.1.1.3”的接入设备；其他参数采用缺省值，并单击“确定”按钮完成操作。

图 1-9　增加接入设备

（2）配置接入策略。选择“用户”页签，单击导航树中的“接入策略管理”→“接入策略管理”菜单项，单击“增加”按钮，创建一条接入策略，如图 1-10 所示。接入策略名输入“802.1x”；证书认证选择“EAP 证书认证”；证书认证类型选择“EAP-PEAP 认证”；认证证书子类型选择“MS-CHAPV2 认证”；其他参数采用缺省值，并单击“确定”按钮完成操作。

图 1-10　配置接入策略

（3）增加接入服务配置。选择“用户”页签，单击导航树中的“接入策略管理”→“接入服务管理”菜单项，单击“增加”按钮，创建一条接入服务，如图 1-11 所示。接入服务名输入“802.1x”；缺省接入策略选择之前创建的策略“802.1x”；其他参数采用缺省值，并单击“确定”按钮完成操作。

图 1-11　增加接入服务配置

（4）增加用户配置。选择“用户”页签，单击导航树中的“接入用户管理”→“接入用户”菜单项，单击“增加”按钮，增加一个接入用户，如图 1-12 所示。单击“增加用户”。用户姓名输入“key”；证件号码输入“000”；其他参数采用缺省值，并单击“确定”按钮完成操作。

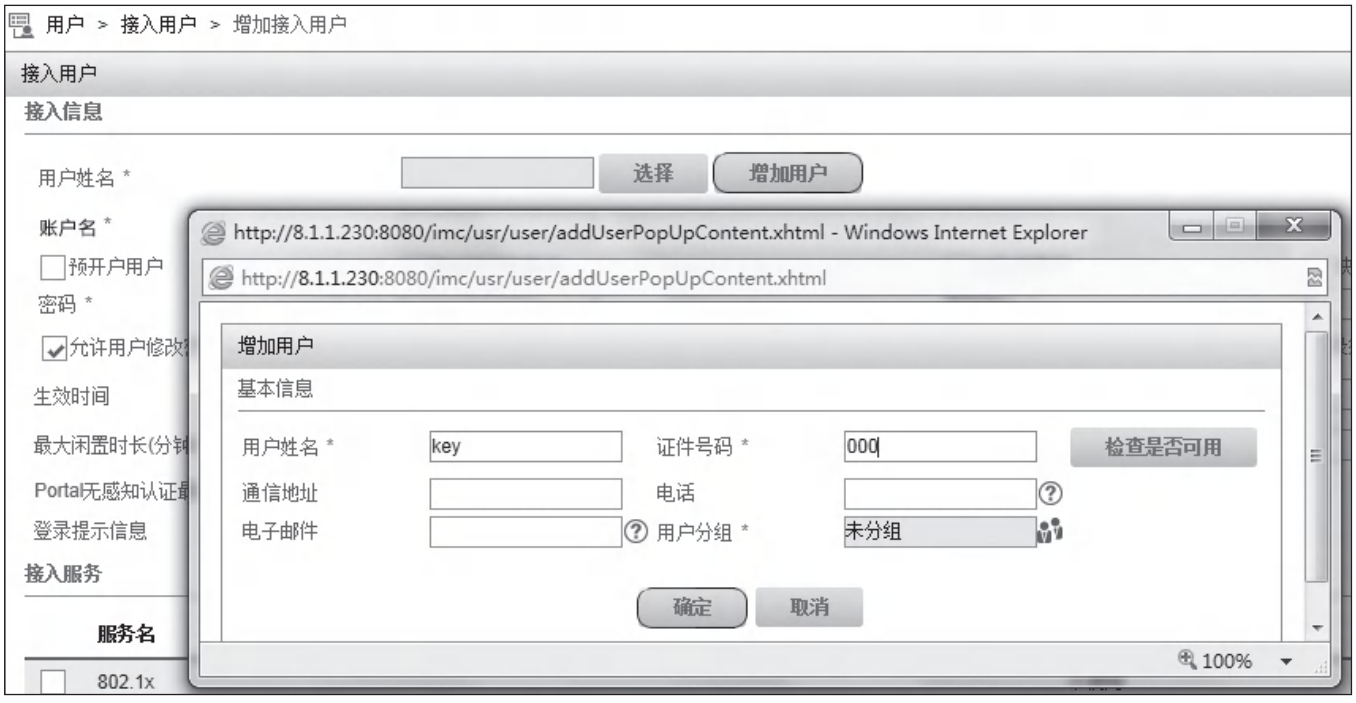


图 1-12　增加用户配置

（5）增加接入用户配置。选择“用户”页签，单击导航树中的“接入用户管理”→

“接入用户”菜单项，单击“增加”按钮，增加一个接入用户，如图 1-13 所示。单击“选择”按钮，在页面中选择上面创建的用户“key”；账号名输入“key”；密码与密码确认均输入“123456”；选择服务名“802.1x”；其他参数采用缺省值，并单击“确定”按钮完成操作。

笔记

图 1-13　增加接入用户配置

1.2.4 验证配置

Client 进行 802.1X 认证上线，输入用户名“key”和密码“123456”后，认证成功。

在 AC 1 上使用 display wlan client 命令查看 Client 的上线 VLAN 信息，可以看到 Client 使用 VLAN 300 上线。

```
[AC1] display wlan client
 Total Number of Clients             : 1
Client Information
 SSID: service
-------------------------------------------------------------------------------
MAC Address    User Name          APID/RID IP Address          VLAN
-------------------------------------------------------------------------------
0022-3f90-938e key                1   /2   0.0.0.0             300
-------------------------------------------------------------------------------
```

使用 display connection 命令查看连接信息，可以看到只有一个客户端与 AC 1 建立了连接。

笔记

```
[AC1] display  connection

Index=5   ,Username=key@office
MAC=00-22-3F-90-93-8E
IP=N/A
IPv6=N/A
 Total 1 connection(s) matched.
```

在 AC 2 上使用 display wlan client 命令查看 Client 的上线 VLAN 信息，同样可以看到 Client 使用 VLAN 300 上线。此处 AP 为 Backup 状态，实际是 AC 1 备份过来的 Client。

```
[AC2] display wlan client
 Total Number of Clients             : 1
Client Information
 SSID: service
--------------------------------------------------------------------------------------------------------
MAC Address    User Name          APID/RID IP Address                    VLAN
--------------------------------------------------------------------------------------------------------
0022-3f90-938e key                1   /2     0.0.0.0                     300
--------------------------------------------------------------------------------------------------------
```

使用 display connection 命令查看连接信息，可以看到只有一个客户端与 AC 2 建立了连接。

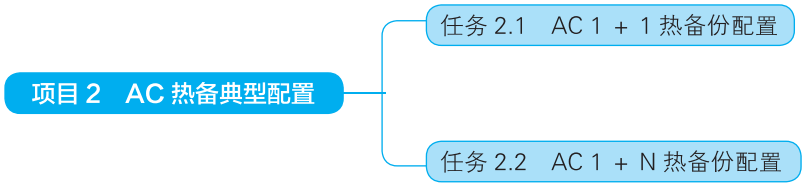
```
[AC2] display  connection

Index=4   ,Username=key@office
MAC=00-22-3F-90-93-8E
IP=N/A
IPv6=N/A
 Total 1 connection(s) matched.
```

将 AC 1 断开，可以发现 Client 未下线，仍然可以正常通信。

项目 2 AC 热备典型配置

接入控制器（access controller）是一种网络设备，负责管理某个区域内无线网络中的 AP（无线接入点），对不同 AP 进行下发配置、修改配置、射频智能管理、用户接入控制等。该设备由无线网络发展而来，由于最初的无线网络是自主单体的管理方式，对于需要大面积无线覆盖的区域，往往需要多个 AP 协同工作，单独配置 AP 的方式已经成为制约工作的瓶颈，因此衍生出无线控制器。目前的无线控制器已经有了长足的发展，集成了三层交换机以及认证系统等众多功能，成为运营商以及企业部署无线局域网的必备设备。

本项目的任务结构如下：



任务 2.1　AC 1 ＋ 1 热备份配置

任务描述

如图 2-1 所示，为了避免单台 AC 故障导致无线客户端无法接入网络，在网络中部署了两台 AC，实现 1+1 热备份。AC 1 作为主用 AC 负责提供无线服务，AC 2 作为备用 AC 为 AC1 提供备份，AC 1 与 AC 2 通过一台二层交换机相连。要求如下：

（1）AP 和 Client 通过 DHCP server 获取 IP 地址。

（2）当 AC 1 发生故障时，能够立即切换到 AC 2 继续为 Client 提供无线服务；在 AC 1 故障恢复后，能够切换回 AC 1 为 Client 提供无线服务。

笔记

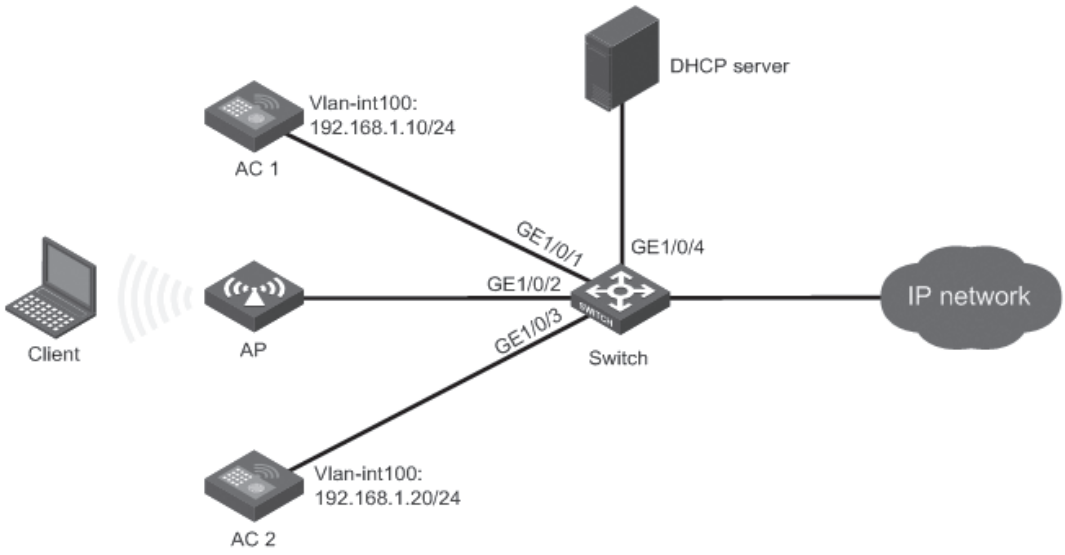


图 2-1　AC 1 + 1 热备份配置

任务实施

2.1.1 配置思路

为了在主 AC 故障恢复后，AP 可以重新切换到主 AC 上，需要保证 AC 1 的优先级高于 AC 2。

2.1.2 配置注意事项

（1）配置 AP 的序列号时，应确保该序列号与 AP 唯一对应，AP 的序列号可以通过 AP 设备背面的标签获取。

（2）主、备 AC 上对于需要提供服务的同一 AP，其 AP 模板视图下的配置必须保持一致（除 AC 的 IP 地址和优先级配置之外），否则当 AC 的主、备状态切换之后，无法保证 AP 设备工作正常。

2.1.3 配置步骤

1. 配置 AC 1

（1）配置 AC 1 接口。

```
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道
<AC1> system-view
[AC1] vlan 100
```

[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 192.168.1.10 255.255.255.0
[AC1-Vlan-interface100] quit
创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 192.168.2.10 255.255.255.0
[AC1-Vlan-interface200] quit
在 AC 1 上配置热备份功能，同时配置 VLAN 200 作为 AC 间用于热备份的本端数据端口的 VLAN
[AC1] hot-backup enable domain 1
[AC1] hot-backup vlan 200
在 AC 1 上配置 AC 2 的 IP 地址 192.168.1.20 为备份 AC 和 AP 建立隧道的接口的 IP 地址
[AC1] wlan backup-ac ip 192.168.1.20
创建 WLAN-ESS 1 接口
[AC1] interface wlan-ess 1
配置 WLAN-ESS 1 接口类型为 Hybrid
[AC1-WLAN-ESS1] port link-type hybrid
配置当前 Hybrid 端口的 PVID 为 VLAN 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 Tag 通过
[AC1-WLAN-ESS1] port hybrid pvid vlan 100
[AC1-WLAN-ESS1] undo port hybrid vlan 1
[AC1-WLAN-ESS1] port hybrid vlan 100 untagged
使能 MAC VLAN 功能
[AC1-WLAN-ESS1] mac-vlan enable
[AC1-WLAN-ESS1] quit
配置 AC 的 GigabitEthernet 1/0/1 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 和 VLAN 200 通过
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] quit

笔记

笔记

（2）配置无线服务。

```
# 创建 clear 类型的服务模板 1
[AC1] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service
[AC1-wlan-st-1] ssid service
# 将 WLAN-ESS 1 接口绑定到服务模板 1
[AC1-wlan-st-1] bind wlan-ess 1
# 启用无线服务
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
# 在 AC 1 的 AP 模板视图下配置 AP 名称为 officeap1，型号名称选择 WA2620E-AGN
[AC1] wlan ap officeap1 model WA2620E-AGN
# 设置主 AC 上 AP 的接入优先级为 6，序列号为 21023529G007C000020
[AC1-wlan-ap-officeap1] priority level 6
[AC1-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 AP 的 radio1 射频视图，配置服务模板 1 与射频 1 进行关联，使能 AP 的 radio1 射频
[AC1-wlan-ap-officeap1] radio 1
[AC1-wlan-ap-officeap1-radio-1] service-template 1
[AC1-wlan-ap-officeap1-radio-1] radio enable
[AC1-wlan-ap-officeap1-radio-1] quit
[AC1-wlan-ap-officeap1] quit
```

2. 配置 AC 2

（1）配置 AC 2 接口。

```
# 创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 LWAPP 隧道
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 192.168.1.20 255.255.255.0
[AC2-Vlan-interface100] quit
# 创建 VLAN 200 作为 ESS 接口的缺省 VLAN，同时作为 Client 接入的业务 VLAN，并为该接口配置 IP 地址
[AC2] vlan 200
```

```
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 192.168.2.20 255.255.255.0
[AC2-Vlan-interface200] quit
# 在 AC 2 上配置热备份功能，同时配置 VLAN 200 作为 AC 间用于热备份的本端数据端口的 VLAN
[AC2] hot-backup enable domain 1
[AC2] hot-backup vlan 200
# 在 AC 2 上配置 AC 1 的 IP 地址 192.168.1.10 为主 AC 和 AP 建立隧道的接口的 IP 地址
[AC2] wlan backup-ac ip 192.168.1.10
# 创建 WLAN-ESS 1 接口
[AC2] interface wlan-ess 1
# 配置 WLAN-ESS 1 接口类型为 Hybrid
[AC2-WLAN-ESS1] port link-type hybrid
# 配置当前 Hybrid 端口的 PVID 为 VLAN 100，禁止 VLAN 1 通过并允许 VLAN 100 不带 Tag 通过
[AC2-WLAN-ESS1] port hybrid pvid vlan 100
[AC2-WLAN-ESS1] undo port hybrid vlan 1
[AC2-WLAN-ESS1] port hybrid vlan 100 untagged
# 使能 MAC VLAN 功能
[AC2-WLAN-ESS1] mac-vlan enable
[AC2-WLAN-ESS1] quit
# 配置 AC 的 GigabitEthernet 1/0/1 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 和 VLAN 200 通过
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC2-GigabitEthernet1/0/1] quit
```

（2）配置无线服务。

```
# 创建 clear 类型的服务模板 1
[AC2] wlan service-template 1 clear
# 设置当前服务模板的 SSID 为 service
[AC2-wlan-st-1] ssid service
# 将 WLAN-ESS1 接口绑定到服务模板 1
[AC2-wlan-st-1] bind wlan-ess 1
```

笔记

笔记

```
# 启用无线服务
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
# 在 AC 2 的 AP 模板视图下配置 AP 名称为 officeap1，型号名称选择 WA2620E-AGN
[AC2] wlan ap officeap1 model WA2620E-AGN
# 设置 AP 的序列号为 21023529G007C000020，以及 AP 的接入优先级取系统缺省值 4
[AC2-wlan-ap-officeap1] serial-id 21023529G007C000020
# 进入 AP 的 radio1 射频视图，配置服务模板与射频 1 进行关联，使能 AP 的 radio 1 射频
[AC2-wlan-ap-officeap1] radio 1
[AC2-wlan-ap-officeap1-radio-1] service-template 1
[AC2-wlan-ap-officeap1-radio-1] radio enable
[AC2-wlan-ap-officeap1-radio-1] quit
[AC2-wlan-ap-officeap1] quit
```

3. 配置 Switch

```
# 创建 VLAN 100 和 VLAN 200，其中 VLAN 100 用于转发 AC 和 AP 间 LWAPP 隧道内的流量，VLAN 200 为无线用户接入的 VLAN
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] vlan 200
[Switch-vlan200] quit
# 配置 Switch 与 AC 1 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 WLAN 100，允许 VLAN 100 和 VLAN 200 通过
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
# 配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口的属性为 Access，当前 Access 端口允许 VLAN 100 通过，并使能 PoE 功能
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 Switch 与 AC 2 相连的 GigabitEthernet1/0/3 接口的属性为 Trunk，当前 Trunk 端口的 PVID 为 VLAN 100，允许 VLAN 100 和 VLAN 200 通过
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/3] quit
# 配置 Switch 与 DHCP server 相连的 GigabitEthernet1/0/4 接口的属性为 Access，并允许 VLAN 100 通过
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
[Switch-GigabitEthernet1/0/4] quit
```

笔记

2.1.4 验证配置

（1）查看 AC 热备份状态、AP 运行状态和客户端运行状态。

在 AC 1 上使用 display hot-backup state 命令查看备份状态，可以看到 Link State 为 Connect，Peer Board MAC 为对端备份 AC 的 MAC 地址，Peer Board State 为 Normal。

```
[AC1] display hot-backup state
**************************************************************
Vlan ID                 : 20
Domain ID               : 1
Link State              : Connect
Peer Board MAC          : 000f-e27e-0bc7
Peer Board State        : Normal
Hello Interval          : 30
```

在 AC 2 上使用 display hot-backup state 命令查看备份状态，可以看到 Link State 为 Connect，Peer Board MAC 为对端主 AC 的 MAC 地址，Peer Board State 为 Normal。

```
[AC2] display hot-backup state
**************************************************************
Vlan ID                 : 20
Domain ID               : 1
```

笔记

```
Link State                : Connect
Peer Board MAC            : 000f-e212-ff01
Peer Board State          : Normal
Hello Interval            : 30
```

在 AC 1 上使用 display wlan ap name officeap1 命令查看 AP 的注册状态，结果为 Run/M。

```
[AC1] display wlan ap name officeap1
 AP Profile
-------------------------------------------------------------------------------------------------------
 AP Name       APID   State      Model             Serial-ID
-------------------------------------------------------------------------------------------------------
 officeap1     1      Run/M      WA2620E-AGN       21023529G007C000020
-------------------------------------------------------------------------------------------------------
```

在 AC 2 上使用 display wlan ap name officeap1 命令查看 AP 的注册状态，结果为 Run/B。

```
[AC2] display wlan ap name officeap1
AP Profile
-------------------------------------------------------------------------------------------------------
 AP Name   APID   State    Model                Serial-ID
-------------------------------------------------------------------------------------------------------
 officeap1 1      Run/B    WA2620E-AGN          21023529G007C000020
```

在 AC 1 上使用 display wlan client 命令查看上线的无线客户端状态，结果为 Running。

```
[AC1] display wlan client
 Total Number of Clients         : 1
 Total Number of Clients Connected : 1
Client Information
-------------------------------------------------------------------------------------------------------
 MAC Address       BSSID           AID   State          PS Mode      QoS Mode
-------------------------------------------------------------------------------------------------------
 001b-110b-7274    000f-e28b-fd40  1     Running        Active       None
-------------------------------------------------------------------------------------------------------
```

在 AC 2 上使用 display wlan client 命令查看上线的无线客户端状态，结果为 Running/B。

```
[AC2] display wlan client
 Total Number of Clients         : 1
```

笔记

```
Total Number of Clients Connected : 1
Client Information
-------------------------------------------------------------------------------------------------------
MAC Address      BSSID          AID    State        PS Mode      QoS Mode
-------------------------------------------------------------------------------------------------------
001b-110b-7274   000f-e28b-fd40 1      Running/B    Active       None
-------------------------------------------------------------------------------------------------------
```

（2）当主 AC 发生故障和故障恢复时，查看 AP 状态与客户端状态的变化。

当 AC 1 发生故障时，本地 AP 连接的状态由 Run/B 切换为 Run/M，上线的无线客户端状态由 Running/B 变为 Running。

```
[AC2] display wlan ap name officeap1
AP Profile
-------------------------------------------------------------------------------------------------------
AP Name          APID   State    Model              Serial-ID
-------------------------------------------------------------------------------------------------------
officeap1        1      Run/M    WA2620E-AGN        21023529G007C000020
-------------------------------------------------------------------------------------------------------
[AC2] display wlan client
 Total Number of Clients         : 1
 Total Number of Clients Connected : 1
 Client Information
-------------------------------------------------------------------------------------------------------
 MAC Address      BSSID          AID    State        PS Mode      QoS Mode
-------------------------------------------------------------------------------------------------------
 001b-110b-7274   000f-e28b-fd40 1      Running      Active       None
-------------------------------------------------------------------------------------------------------
```

在 AC 1 上使用 display wlan ap name officeap1 命令查看 AP 的连接状态，可以看到由 Run/M 切换为 Run/B；使用 display wlan client 命令查看上线的无线客户端状态，结果为 Running/B。

```
[AC1] display wlan ap name officeap1
 AP Profile
-------------------------------------------------------------------------------------------------------
 AP Name          APID   State    Model              Serial-ID
-------------------------------------------------------------------------------------------------------
 officeap1        1      Run/B    WA2620E-AGN        21023529G007C000020
-------------------------------------------------------------------------------------------------------
[AC1] display wlan client
```

笔记

```
Total Number of Clients        : 1
Total Number of Clients Connected : 1
Client Information
-------------------------------------------------------------------------------------------------
MAC Address      BSSID          AID    State        PS Mode    QoS Mode
-------------------------------------------------------------------------------------------------
001b-110b-7274   000f-e28b-fd40 1      Running/B    Active     None
-------------------------------------------------------------------------------------------------
```

在 AC 1 故障排除后，在 AC 1 上使用 display wlan ap name officeap1 命令查看 AP 的连接状态，可以看到由 Run/B 切换为 Run/M；使用 display wlan client 命令查看上线的无线客户端状态，结果为 Running。

```
[AC1] display wlan ap name officeap1
AP Profile
-------------------------------------------------------------------------------------------------
AP Name     APID   State        Model                Serial-ID
-------------------------------------------------------------------------------------------------
officeap1   1      Run/M        WA2620E-AGN          21023529G007C000020
-------------------------------------------------------------------------------------------------
[AC1] display wlan client
Total Number of Clients        : 1
Total Number of Clients Connected : 1
Client Information
-------------------------------------------------------------------------------------------------
MAC Address      BSSID          AID    State        PS Mode    QoS Mode
-------------------------------------------------------------------------------------------------
001b-110b-7274   000f-e28b-fd40 1      Running      Active     None
-------------------------------------------------------------------------------------------------
```

在 AC 2 上使用 display wlan ap name officeap1 命令查看 AP 的连接状态，结果为 Run/B；使用 display wlan client 命令查看上线的无线客户端状态，结果为 Running/B。

```
[AC2] display wlan ap name officeap1
AP Profile
-------------------------------------------------------------------------------------------------
AP Name     APID     State      Model              Serial-ID
-------------------------------------------------------------------------------------------------
```

```
officeap1       1          Run/B      WA2620E-AGN      21023529G007C000020
-------------------------------------------------------------------------------
[AC2] display wlan client
 Total Number of Clients         : 1
 Total Number of Clients Connected : 1
 Client Information
-------------------------------------------------------------------------------
 MAC Address     BSSID          AID   State        PS Mode     QoS Mode
-------------------------------------------------------------------------------
 001b-110b-7274  000f-e28b-fd40  1     Running/B    Active      None
-------------------------------------------------------------------------------
```

笔记

任务 2.2　AC 1 + N 热备份配置

任务描述

如图 2-2 所示，无线网络中有两台无线控制器 AC 1 和 AC 2，分别为 AP 1 和 AP 2 提供无线服务。现要求在网络中增加一台 AC，作为两台主 AC 的备份 AC。要求如下：

（1）在检测到主 AC 故障后的 30 秒内，AP 会主动切换连接到备份 AC 上。

（2）在主 AC 故障排除后，AP 会尝试与主 AC 重新协商并建立隧道，如果建立成功，则 AP 会切断和备份 AC 的连接，自动切换到主 AC 上。

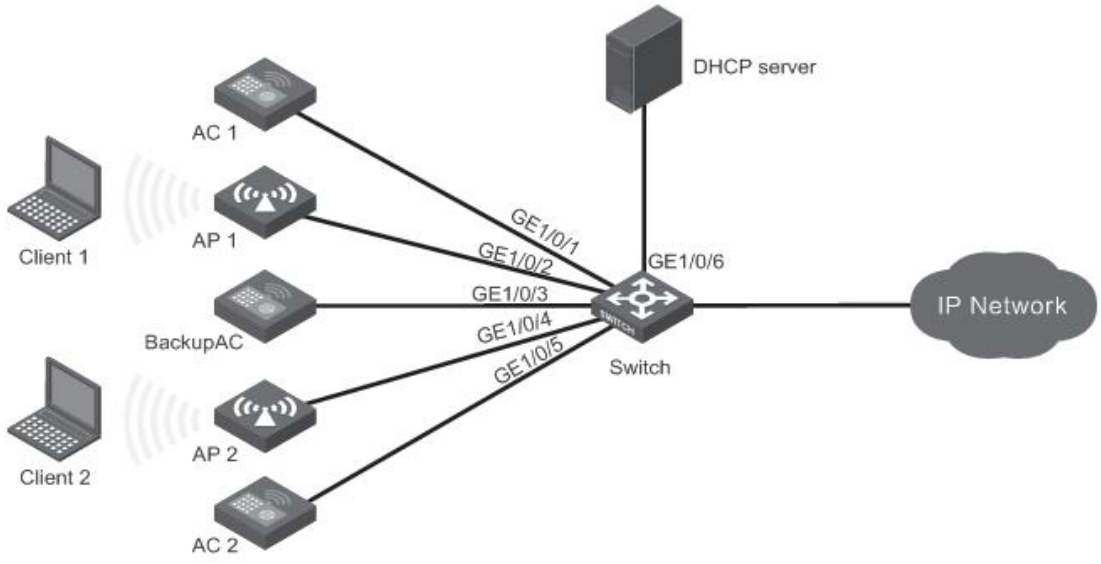


图 2-2　AC 1+N 热备份配置