



WS6603 无线接入控制器

V100R003C05

配置指南

文档版本 04

发布日期 2012-07-10

版权所有 © 华为技术有限公司 2012。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本档内容会不定期进行更新。除非另有约定，本档仅作为使用指导，本档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <http://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前言

读者对象

本文档介绍 WS6603 设备的配置过程。

本文档（本指南）主要适用于以下工程师：

- 安装调测工程师
- 系统维护工程师
- 数据配置工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
 警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
 窍门	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从两个或多个选项中选取一个。
[x y ...]	表示从两个或多个选项中选取一个或者不选。
{ x y ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x y ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ~ n 次。
#	由“#”开始的行表示为注释行。

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 04（2012-07-10）

第四次正式发布。

相对于版本 03 (2011-09-30)的变化如下：

- 修改配置 WLAN 业务示例
- 修改配置 WLAN 接入安全策略

文档版本 03（2011-09-30）

第三次正式发布。

文档版本 02（2011-08-15）

第二次正式发布。

文档版本 01（2011-06-30）

第一次正式发布。

目录

前言.....	ii
1 调测.....	1
1.1 登录设备并检查软件版本.....	2
1.1.1 通过串口登录系统.....	2
1.1.2 检查软件版本.....	5
1.2 设备维护方式配置.....	6
1.2.1 本地维护设备.....	6
1.2.2 远程维护设备.....	6
1.3 基本配置.....	28
1.3.1 修改系统名称.....	28
1.3.2 配置系统时间.....	28
1.3.3 配置系统操作用户.....	30
1.3.4 配置端口.....	34
1.4 配置 License.....	36
1.5 保存与备份数据.....	37
1.5.1 配置文件传输方式.....	37
1.5.2 手动保存与备份数据.....	44
1.5.3 自动保存和备份数据.....	48
2 基础配置.....	53
2.1 配置网络时间.....	54
2.1.1 （可选）配置 NTP 身份验证功能.....	55
2.1.2 配置 NTP 广播模式.....	56
2.1.3 配置 NTP 组播模式.....	58
2.1.4 配置 NTP 客户端或服务器模式.....	60
2.2 配置系统安全.....	62
2.2.1 配置防火墙.....	62
2.2.2 配置防对系统的恶意攻击.....	64
2.2.3 配置防非法用户登录.....	65
2.3 配置 ACL.....	67
2.3.1 配置基本 ACL.....	68
2.3.2 配置高级 ACL.....	69
2.3.3 配置链路层 ACL.....	70

2.3.4 配置用户自定义 ACL.....	71
2.4 配置 QoS.....	74
2.4.1 配置流量管理.....	74
2.4.2 配置队列调度.....	76
2.4.3 配置基于 ACL 规则的流量管理.....	79
3 配置 WLAN 业务.....	84
3.1 配置运营商 ID 和 AC ID.....	87
3.2 配置 AC 三层接口.....	87
3.3 配置 DHCP server.....	88
3.4 配置 AP 的版本升级.....	89
3.5 配置数据的转发模式.....	90
3.6 添加 AP 并上线.....	90
3.7 配置 WLAN 射频.....	92
3.7.1 配置 Radio 模板.....	92
3.7.2 在射频上绑定 Radio 模板.....	94
3.7.3 配置基于 AP 域的射频调优.....	94
3.7.4 （可选）配置 AP 射频资源管理.....	95
3.7.5 （可选）配置 AP 负载均衡组.....	95
3.8 配置 ESS 和 VAP.....	96
3.8.1 配置 ESS.....	96
3.8.2 配置 VAP 并绑定 ESS.....	97
3.9 配置 WLAN 的 QoS 策略.....	98
3.9.1 配置射频的 QoS 策略.....	98
3.9.2 配置 VAP 的 QoS 策略.....	99
3.10 配置 WLAN 接入安全策略.....	101
3.11 配置 802.11n.....	103
3.12 查看 AP 信息.....	104
4 WLAN 业务配置示例.....	106
4.1 WLAN 组网概述.....	107
4.2 WLAN 业务配置流程.....	108
4.3 配置 WLAN 业务示例.....	109
4.3.1 配置业务示例-直连式二层组网，数据隧道转发.....	109
4.3.2 配置业务示例-旁挂式二层组网，数据本地转发.....	117
4.3.3 配置业务示例-直连式三层组网，数据本地转发.....	126
4.3.4 配置业务示例-旁挂式三层组网，数据隧道转发.....	134
4.3.5 配置业务示例-双链路热备保护，直连式二层组网.....	143
4.3.6 配置业务示例-双链路热备保护，旁挂式三层组网.....	157
4.3.7 配置 WLAN 业务示例-AC QoS 策略.....	172
4.3.8 配置业务示例-接入安全策略.....	178
4.3.9 配置业务示例-配置 AP 负载均衡组.....	184
5 协议配置.....	190

5.1 配置路由.....	191
5.1.1 配置路由策略示例.....	191
5.1.2 配置静态路由示例.....	193
5.1.3 配置 RIP 路由协议示例.....	195
5.1.4 配置 OSPF 路由协议示例.....	198
5.1.5 配置 IS-IS 路由协议示例.....	201
5.1.6 配置 BGP 路由协议示例.....	203
5.2 配置 DHCP.....	207
5.2.1 配置 DHCP 标准模式.....	208
5.2.2 配置 DHCP Server 模式.....	209
5.2.3 配置 DHCP Option43 模式.....	210
5.2.4 配置 DHCP Option60 模式.....	212
5.2.5 配置 DHCP Option15 模式.....	214
5.2.6 配置 DHCP MAC 地址段模式.....	215
5.3 配置 AAA.....	217
5.3.1 配置远程 AAA（RADIUS 协议）.....	218
5.3.2 配置采用 RADIUS 认证和计费示例.....	221
5.4 配置 MSTP.....	223
5.5 配置 Ethernet CFM OAM.....	226
6 配置组播业务.....	230
6.1 组播缺省配置信息.....	231
6.1.1 配置组播全局参数.....	231
6.1.2 配置组播 VLAN 和组播节目.....	233
7 运维管理.....	236
7.1 配置告警.....	237
7.2 更换 AP.....	238

1 调测

关于本章

本章从硬件、软件、对接，以及维护管理的角度，对设备提供的基本功能进行调测与验证，确保设备稳定、可靠地投入网上运行。

1.1 登录设备并检查软件版本

介绍通过串口方式登录设备，并检查软件版本是否正确的方法。

1.2 设备维护方式配置

用户可使用维护终端登录 AC 设备，进行本地维护或远程维护，请根据实际情况选择。

1.3 基本配置

介绍调测阶段的一些基本配置，包括修改系统名称、配置系统时间和配置系统操作用户等。

1.4 配置 License

License 平台为 AC 设备提供注册机制。在系统初使化时，AC 各业务模块需要注册受控资源项或受控功能项。

1.5 保存与备份数据

AC 设备支持保存与备份数据，以满足系统升级的需要，并且保证系统在发生升级失败或者严重问题时的恢复能力。

1.1 登录设备并检查软件版本

介绍通过串口方式登录设备，并检查软件版本是否正确的方法。

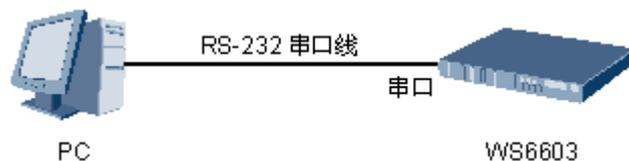
1.1.1 通过串口登录系统

通过本任务实现操作控制台通过串口与 AC 设备相连并登录到 AC 设备，实现对设备的本地维护管理。

组网图

本地串口方式配置组网如图 1-1 所示。

图 1-1 本地串口方式配置组网图



操作步骤

步骤 1 连接串口线。

将计算机串口通过标准的 RS-232 串口线与 AC 设备的 WAC 单板上的维护串口 CON 相连接，如图 1-1 所示。

步骤 2 打开超级终端。

1. 新建连接。

在计算机上选择“开始 > 程序 > 附件 > 通讯 > 超级终端”，打开“连接描述”对话框，输入连接名称，如图 1-2 所示，单击“确定”。

图 1-2 新建连接



2. 设置串口。

选择计算机上与 AC 设备实际连接的标准字符终端或 PC 终端串口号，假设为“COM1”，如图 1-3 所示。单击“确定”按钮。

图 1-3 选择连接使用串口

**步骤 3** 设置终端通信参数。

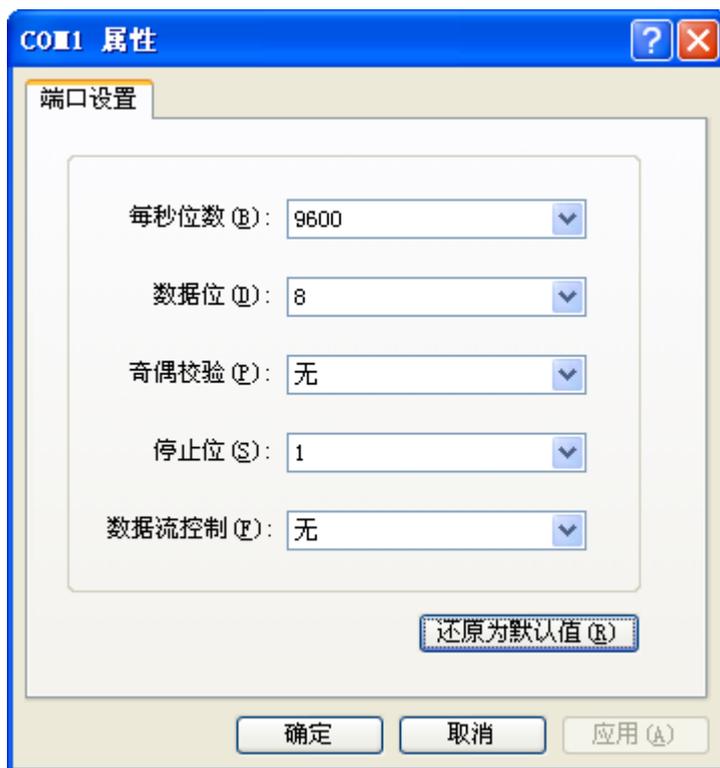
在出现的“COM1 属性”对话框中设置参数，如图 1-4 所示。这里设置为：

- 波特率为 9600bit/s
- 数据位为 8
- 奇偶校验为无
- 停止位为 1
- 数据流控制为无

说明

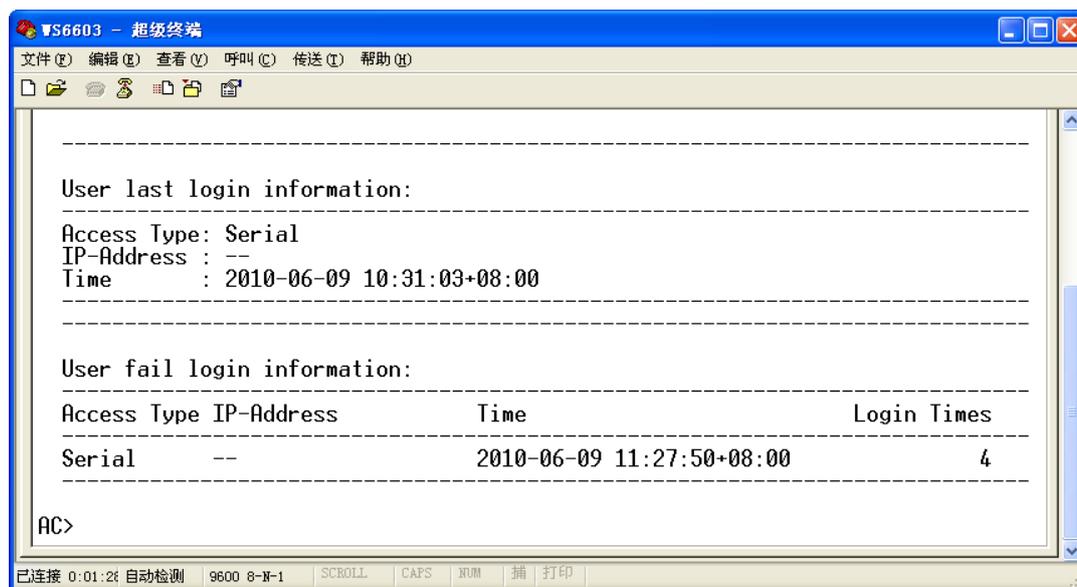
- 超级终端波特率的设置必须与 AC 设备的串口波特率参数一致。系统默认串口波特率为 9600bit/s。
- 如果登录后超级终端界面输入字符出现乱码，一般是由于终端的波特率设置与 AC 设备的波特率设置不一致导致，可尝试使用其他波特率登录系统。系统支持的波特率包括 9600bit/s、19200bit/s、38400bit/s、57600bit/s、115200bit/s。

图 1-4 超级终端参数设置图



单击“确认”按钮后出现超级终端界面，如图 1-5 所示。

图 1-5 超级终端界面图



---结束

操作结果

在超级终端界面中敲击回车键，出现输入用户名的提示符。根据提示输入用户名和密码进行用户注册（系统缺省的超级用户名为：**root**，密码为：**admin**），直到出现命令行提示符（如 **WAC>**）。

若登录不成功，请点击操作界面上的“断开”图标后再点击“呼叫”图标，若还无法登录，请回到第 1 步检查参数设置或物理连接是否正确，确认设置正确后再重新登录。

1.1.2 检查软件版本

检查当前运行的软件版本是否符合现场开局的要求。

操作步骤

步骤 1 使用 **display language** 命令检查当前运行的主机软件版本是否符合现场开局的要求。

步骤 2 使用 **display version** 命令检查当前运行的单板软件版本是否符合现场开局的要求。

步骤 3 使用 **filesystem cmd dir /all** 命令检查当前系统 Flash 中的版本文件是否正确。

----结束

操作结果

- 主机软件版本、单板软件版本符合现场开局的要求。
- 如果不符合要求，请及时联系华为技术有限公司客户服务中心，必要时进行主机软件的升级。

任务示例

举例：查询设备当前运行的主机软件版本和单板软件版本信息。

```
huawei>display language
Local:
  Description: CHINESE SIMPLIFIED (DEFAULT LANGUAGE)
  Version:     WS6603V100R003C05
  Encoding:    GBK

General:
  Description: ENGLISH (DEFAULT LANGUAGE)
  Version:     WS6603V100R003C05
  Encoding:    ANSI
huawei>display version
{ <cr>|backplane<K>|frameid/slotid<S><Length 1-15> } :
Command:
    display version

VERSION : WS6603V100R003C05
PATCH  : SPC100
PRODUCT WS6603
Uptime is 5 day(s), 1 hour(s), 16 minute(s), 44 second(s)
huawei>enable
huawei#filesystem cmd dir /all
Directory of flash:/

 0  -rw-   227824  Nov 13 2010 02:29:01  data_bak.dat
 1  -rw-   15162118  Nov 11 2010 02:11:49  program.efs
 2  -rw-   15162118  Nov 13 2010 02:26:15  program_bak.efs
 3  -rw-   227824  Nov 11 2010 02:15:01  data.dat
 4  -rw-      774  Nov 11 2010 02:06:40  ver_match.efs
 5  -rw-   52490  Nov 11 2010 02:14:51  cp1d1.efs
```

```
6 -rw-      4 Apr 08 2010 13:13:53 lic_switch.efs
7 -rw-    1584 Oct 25 2010 00:30:40 lic.efs
8 -rw-     396 Apr 08 2010 16:25:54 rsa_host_key.efs
9 -rw-     540 Jul 18 2010 15:58:27 rsa_server_key.efs
10 -rw-   4512 Nov 11 2010 02:45:44 patch_load.efs
11 -rw-     11 Jul 01 2010 19:27:50 test.txt
12 -rw-   1192 Nov 16 2010 02:24:44 alm_static.efs
13 -rw-     494 Nov 09 2010 00:24:02 cfm.efs
14 -rw- 6365506 Nov 02 2010 21:53:13 wa6x3xn_v100r003c01b013.bin
15 -rw-     394 Aug 05 2010 22:42:43 owner.efs
16 -rw-   32667 Oct 19 2010 02:15:56 iposlogbufffile.dat
17 -rw-   19147 Apr 21 2010 23:11:44 iposlogfile1.dat
18 -rw- 6379423 Nov 05 2010 04:16:11 wa6x1_v100r003c01b013_k.bin
19 -rw- 16511555 Oct 10 2010 05:27:51 ws6x3xn_v100r003c01b012_k.bin
20 -rw- 6365506 Oct 12 2010 00:21:47 wa6x3xn_v100r003c01b015.bin
21 -rw-   16600 Jul 30 2010 14:33:43 wlan_log.txt
22 -rw- 6160412 Aug 06 2010 11:49:23 wa6x1_v100r001c01spc300b075.bin
23 -rw- 6379423 Nov 04 2010 19:31:39 wa6x1_v100r003c01b021_k.bin
24 -rw- 6184860 Nov 07 2010 06:29:36 wa6x1_v100r003c01b021.bin
```

116392960 bytes total (31116288 bytes free)

1.2 设备维护方式配置

用户可使用维护终端登录 AC 设备，进行本地维护或远程维护，请根据实际情况选择。

1.2.1 本地维护设备

介绍通过本地串口方式登录 AC 设备的操作方法，登录成功后可以对 AC 设备进行相应的配置和管理。

背景信息

通过本地串口方式登录 AC 设备的操作方法前面章节已经详细介绍，具体步骤请参见 [1.1.1 通过串口登录系统](#)。

1.2.2 远程维护设备

介绍远程维护设备的几种方式，用户可以根据实际情况进行选择。

Telnet 方式登录（带内管理）

通过本操作实现通过上行端口（带内管理接口）以 Telnet 方式登录到 AC 设备，对其进行维护和管理。

前提条件

已通过本地串口方式登录 AC 设备，具体操作请参见“[1.1.1 通过串口登录系统](#)”。

说明

以下操作中在 AC 设备上的配置需要通过本地串口配置完成。

组网

Telnet 方式通过局域网和广域网进行带内管理配置组网如 [图 1-6](#) 和 [图 1-7](#) 所示。

图 1-6 Telnet 方式通过局域网进行带内管理配置组网图

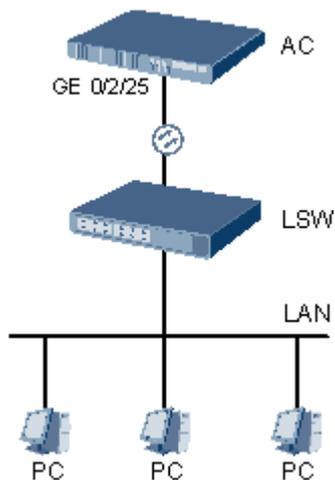
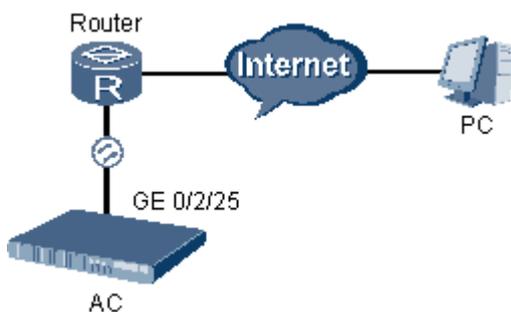


图 1-7 Telnet 方式通过广域网进行带内管理配置组网图



数据规划

使用 Telnet 方式（带内管理）登录 AC 设备的数据规划如表 1-1 所示。

表 1-1 Telnet 方式（带内管理）登录 AC 设备的数据规划

配置项	数据
AC 上行端口	<ul style="list-style-type: none"> ● VLAN ID: 30 ● 端口号: 0/2/25 ● IP 地址: 10.50.1.10/24
维护终端	IP 地址: 10.10.1.10/24
路由器接 AC 侧的接口（Telnet 方式通过广域网进行带内管理时选择此项）	IP 地址: 10.50.1.1/24

操作步骤

步骤 1 搭建组网环境。

- 如果选择通过局域网带内管理方式 Telnet 到 AC 设备，搭建如图 1-6 所示的组网环境。
- 如果选择通过广域网带内管理方式 Telnet 到 AC 设备，搭建如图 1-7 所示的组网环境。

步骤 2 设置 VLAN 三层接口 IP 地址。

1. 使用 **vlan** 命令创建管理 VLAN。

```
huawei(config)#vlan 30
```

2. 使用 **port vlan** 命令增加 VLAN 上行端口。

```
huawei(config)#port vlan 30 0/2 25
```

3. 在 VLANIF 模式下，使用 **ip address** 命令设置 VLAN 三层接口的 IP 地址。

```
huawei(config)#interface vlanif 30  
huawei(config-if-vlanif30)#ip address 10.50.1.10 24
```

说明

如果上行以太网端口的报文不含 VLAN tag（即 untag），则需要使用 **native-vlan** 命令配置上行接口的缺省 VLAN 与上行接口的 VLAN 相同。

步骤 3 添加带内管理路由。

- 如果搭建图 1-6 所示的局域网本地管理环境，不需要添加路由。
- 如果搭建图 1-7 所示的广域网远程管理环境，使用 **ip route-static** 命令配置 AC 设备管理接口到维护终端的路由。

```
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

步骤 4 运行 Telnet 程序。

在维护终端上选择“开始 > 运行...”，在“运行”窗口中的“打开”地址栏处输入“telnet 10.50.1.10”如：图 1-8 所示（以 Windows 操作系统为例），单击“确定”，弹出远程登录的对话框。

图 1-8 运行 Telnet 程序界面



步骤 5 登录系统。

在弹出的远程登录对话框中输入用户名和密码。系统缺省的用户名为：**root**，密码为：**admin**。成功登录系统后会给出提示信息，如下所示。

```
>>User name:root  
>>User password:admin //维护终端上不显示
```

Huawei Integrated Access Software.

Copyright (C) Huawei Technologies Co., Ltd. 2002-2009. All rights reserved.

---结束

操作结果

用户登录系统后，可以对 AC 设备进行维护管理。

Telnet 方式登录（带外管理）

通过本操作实现通过本地维护网口 ETH（带外管理接口）以 Telnet 方式登录到 AC，对其进行维护和管理。

前提条件

已通过本地串口方式登录 AC，具体操作请参见“[1.1.1 通过串口登录系统](#)”。

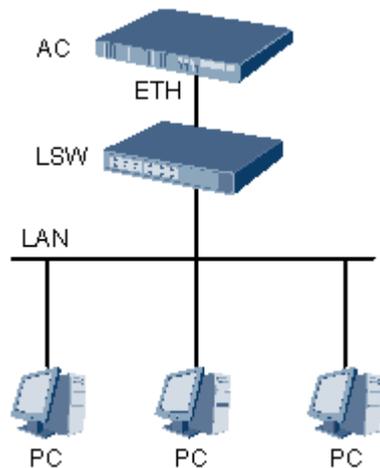
 说明

以下操作中在 AC 上的配置需要通过本地串口配置完成。

组网

Telnet 方式通过局域网和广域网进行带外管理配置组网如[图 1-9](#)和[图 1-10](#)所示。

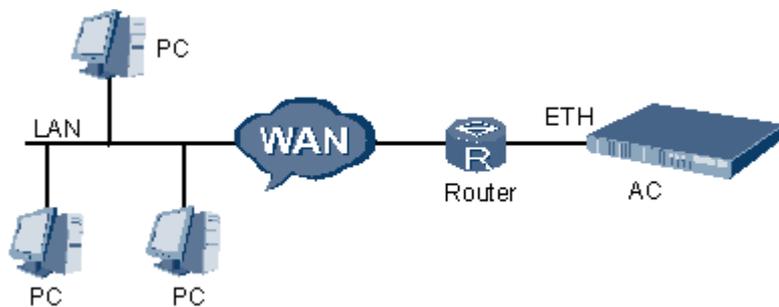
图 1-9 Telnet 方式通过局域网进行带外管理配置组网图



 说明

AC 通过直通网线（Straight Through Cable）与局域网相连，且 AC 维护网口的 IP 地址与维护终端的 IP 地址在同一网段；也可以将维护终端的网口与 AC 主控板的维护网口直接连接，对设备进行带外管理，但此时要使用交叉网线（Crossover Cable）。

图 1-10 Telnet 方式通过广域网进行带外管理配置组网图



数据规划

Telnet 方式通过局域网和广域网进行带外管理数据规划如表 1-2 和表 1-3 所示。

表 1-2 Telnet 方式通过局域网进行带外管理的数据规划

配置项	数据
维护网口	IP 地址：10.50.1.10/24 说明 维护网口（主控板上的 ETH 口）默认的 IP 地址为 10.11.104.2，子网掩码为 255.255.255.0。
维护终端	IP 地址：10.50.1.20/24（需要与维护网口的 IP 地址在同一网段）

表 1-3 Telnet 方式通过广域网进行带外管理的数据规划

配置项	数据
维护网口	IP 地址：10.50.1.10/24 说明 维护网口（主控板上的 ETH 口）默认的 IP 地址为 10.11.104.2，子网掩码为 255.255.255.0。
维护终端	IP 地址：10.10.1.10/24
路由器接 AC 设备侧的接口	IP 地址：10.50.1.1/24

操作步骤

步骤 1 搭建组网环境。

- 如果选择通过局域网带外管理方式 Telnet 到 AC 设备，搭建如图 1-9 所示的组网环境。
- 如果选择通过广域网带外管理方式 Telnet 到 AC 设备，搭建如图 1-10 所示的组网环境。

步骤 2 设置维护网口 IP 地址。

在 MEth 模式下，使用 **ip address** 命令设置维护网口 IP 地址。

```
huawei(config)#interface meth 0  
huawei(config-if-meth0)#ip address 10.50.1.10 24
```

步骤 3 添加带外管理路由。

- 如果搭建图 1-9 所示的局域网本地管理环境，不需要添加路由。
- 如果搭建图 1-10 所示的广域网远程管理环境，使用 **ip route-static** 命令配置 AC 设备管理接口到维护终端的路由。

```
huawei(config-if-meth0)#quit  
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

步骤 4 运行 Telnet 程序。

在维护终端上选择“开始 > 运行...”，在“运行”窗口中的“打开”地址栏处输入“telnet 10.50.1.10”如：图 1-11 所示（以 Windows 操作系统为例），单击“确定”，弹出远程登录的对话框。

图 1-11 运行 Telnet 程序界面



步骤 5 登录系统。

在弹出的远程登录对话框中输入用户名和密码。系统缺省的用户名为：**root**，密码为：**admin**。成功登录系统后会给出提示信息，如下所示。

```
>>User name:root  
>>User password:admin //维护终端上不显示
```

```
Huawei Integrated Access Software.  
Copyright(C) Huawei Technologies Co., Ltd. 2002-2009. All rights reserved.
```

----结束

操作结果

用户登录系统后，可以对 AC 进行维护管理。

SSH 方式登录（带内管理）

通过本操作实现通过上行端口（带内管理接口）以 SSH 方式登录到 AC 设备，对 AC 设备进行维护和管理。SSH（Secure Shell）通过提供认证、加密和鉴权来保证网络通信的安全性，当用户通过一个不能保证安全的网络环境远程登录到 AC 设备时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护 AC 设备不受诸如 IP 地址欺诈、明文密码截取攻击等影响。

前提条件

- 已通过本地串口方式登录 AC 设备，具体操作请参见“[1.1.1 通过串口登录系统](#)”。
 说明
以下操作中在 AC 设备上的配置需要通过本地串口配置完成。
- 已经准备好调测以 SSH 方式登录 AC 设备时使用的工具：客户端软件密码生成工具 Puttygen.exe、客户端软件密码转换工具 sshkey.exe 和运行 SSH 客户端工具 putty.exe。

组网

SSH 方式通过局域网和广域网进行带内管理配置组网如[图 1-12](#)和[图 1-13](#)所示。

图 1-12 SSH 方式通过局域网进行带内管理配置组网图

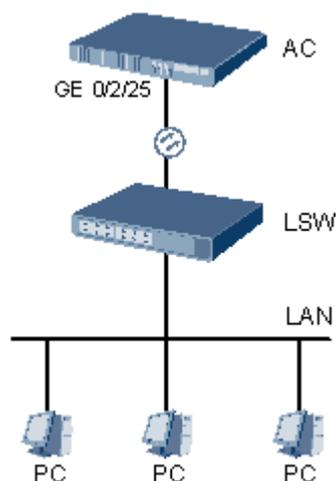
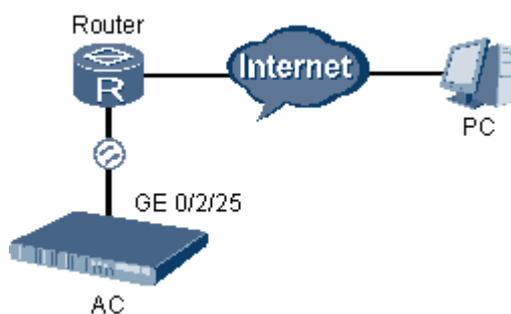


图 1-13 SSH 方式通过广域网进行带内管理配置组网图



数据规划

使用 SSH 方式登录 AC 设备的数据规划如[表 1-4](#)所示。

表 1-4 SSH 方式登录 AC 设备的数据规划

配置项	数据
AC 设备上行端口	<ul style="list-style-type: none">● VLAN ID: 30● 端口号: 0/2/25● IP 地址: 10.50.1.10/24● 用户认证方式: RSA 公钥认证● RSA 公钥名: key
新用户	<ul style="list-style-type: none">● 用户名/密码: huawei/test01● 权限: 操作员级● 可重复登录数: 4
维护终端	IP 地址: 10.10.1.10/24
路由器接 AC 侧的接口 (SSH 方式通过广域网进行带内管理时选择此项)	IP 地址: 10.50.1.1/24

操作步骤

步骤 1 搭建组网环境。

- 如果选择通过局域网带内管理方式以 SSH 登录到 AC 设备, 搭建如图 1-12 所示的组网环境。
- 如果选择通过广域网带内管理方式以 SSH 登录到 AC 设备, 搭建如图 1-13 所示的组网环境。

步骤 2 设置 VLAN 三层接口 IP 地址。

1. 使用 **vlan** 命令创建管理 VLAN。
huawei(config)#**vlan 30**
2. 使用 **port vlan** 命令增加 VLAN 上行端口。
huawei(config)#**port vlan 30 0/2 25**
3. 在 VLANIF 模式下, 使用 **ip address** 命令设置 VLAN 三层接口的 IP 地址。
huawei(config)#**interface vlanif 30**
huawei(config-if-vlanif30)#**ip address 10.50.1.10 24**

说明

如果上行以太网端口的报文不含 VLAN tag (即 untag), 则需要使用 **native-vlan** 命令配置上行接口的缺省 VLAN 与上行接口的 VLAN 相同。

步骤 3 添加带内管理路由。

- 如果搭建图 1-12 所示的局域网本地管理环境, 不需要添加路由。
- 如果搭建图 1-13 所示的广域网远程管理环境, 使用 **ip route-static** 命令配置 AC 设备管理接口到维护终端的路由。
huawei(config)#**ip route-static 10.10.1.0 24 10.50.1.1**

步骤 4 创建一个用户。

使用 **terminal user name** 命令增加一个用户。

```
huawei(config)#terminal user name  
User Name(length<6, 15>):huawei  
User Password(length<6, 15>):test01//维护终端上不显示
```

```
Confirm Password(length<6, 15>):test01//维护终端上不显示
User profile name(<=15 chars)[root]:
User's Level:
  1. Common User  2. Operator:2
Permitted Reenter Number(0--4):4
User's Appended Info(<=30 chars):
Adding user succeeds
Repeat this operation? (y/n)[n]:n
```

步骤 5 创建 SSH 本地密钥对。

使用 **rsa local-key-pair create** 命令创建 SSH 本地密钥对。



注意

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，完成创建 SSH 本地密钥对的操作。

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..+++++++
.....+++++++
.....+++++++
.....+++++++
```

步骤 6 设置 SSH 用户认证方式。

使用 **ssh user huawei authentication-type rsa** 命令选择 SSH 用户认证方式。

SSH 用户认证方式分为以下四种，这里以 **rsa** 为例进行介绍。

- **password**: 使用普通的口令。
- **rsa**: 使用 RSA 公钥。
- **all**: 使用 **password** 或 **rsa** 认证，即用户通过 **password** 或者 **rsa** 认证两者之一都可以登录到设备上。
- **password-publickey**: 使用 **password** 和 **publickey** 方式认证，即用户必须通过 **password** 和 **rsa** 两种认证后才可以登录到设备上。

```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

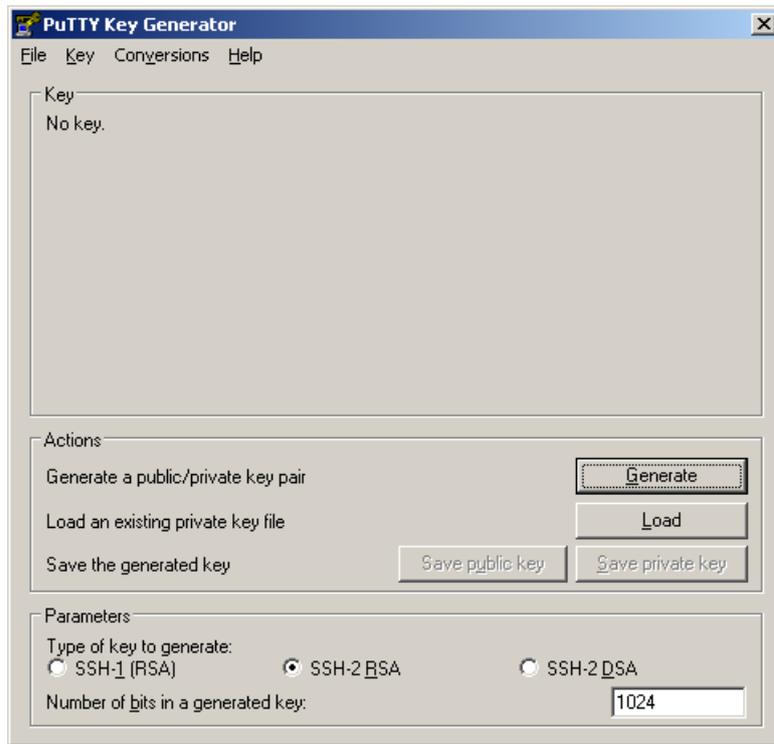
Command:
ssh user huawei authentication-type rsa
%Authentication type setted, and will be in effect next time.
```

步骤 7 生成 RSA 公钥。

1. 打开密码生成工具。

打开客户端软件密码生成工具 **Puttygen.exe**，如图 1-14 所示。

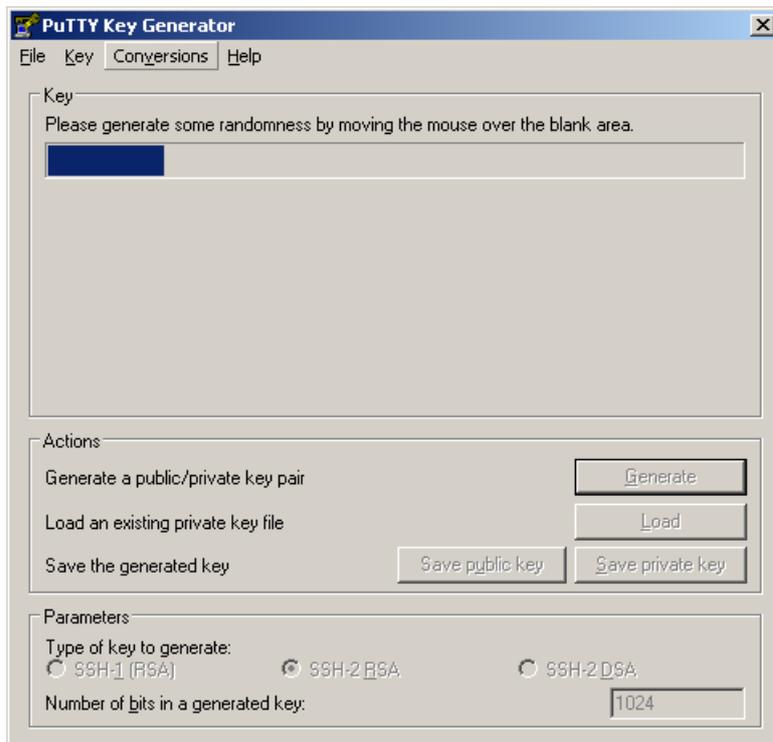
图 1-14 密码生成工具界面图



2. 生成客户端密钥。

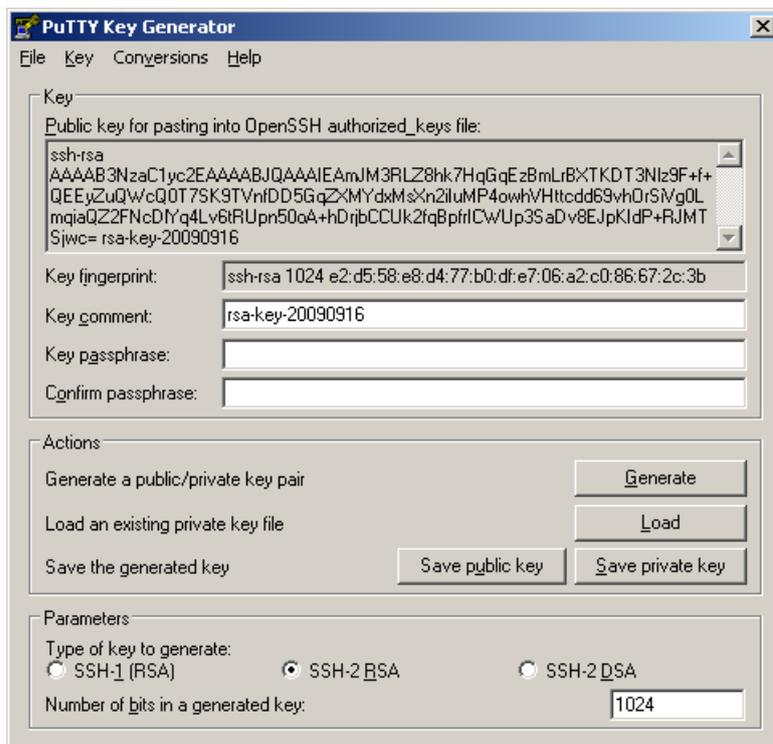
在“Parameters”区域中选择密钥类型为“SSH-2 RSA”后，单击“Generate”，根据页面提示移动鼠标进行密钥生成，如图 1-15 所示。

图 1-15 密码生成工具界面图



完成密钥生成后，单击“Save public key”和“Save private key”，保存 public key 和 private key。如图 1-16 所示。

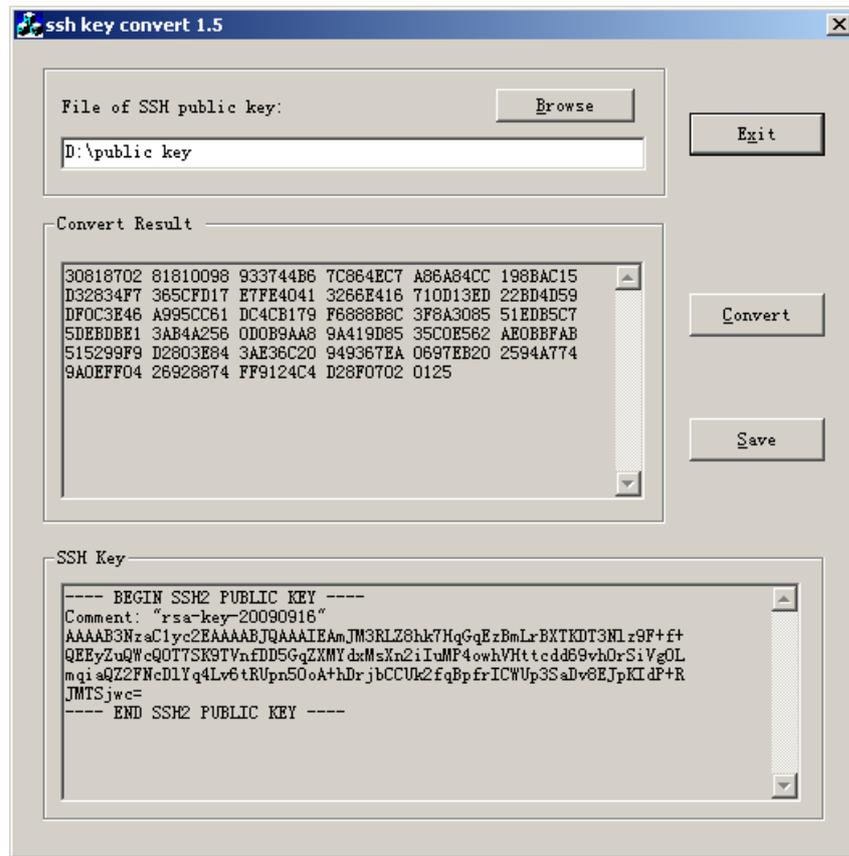
图 1-16 保存 public key 和 private key



3. 生成 RSA 公钥。

打开客户端软件密码转换工具 sshkey.exe，单击“Browse”，选择上面保存的 public key 文件。然后单击“Convert”，将客户端公钥转换成 RSA 公钥，如图 1-17 所示。

图 1-17 客户端公钥转换成 RSA 公钥工具界面图



步骤 8 生成 SSH 用户公钥。

创建 RSA 公钥 key，在 config-rsa-key-code 命令行模式下将 RSA 公钥拷贝进服务器端。

```

huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.

huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".

huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15

huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59

huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7

huawei(config-rsa-key-code)#SDEBDBE1 3AB4A256 OD0B9AA8 9A419D85 35COE562 AE0BBFAB

huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774

huawei(config-rsa-key-code)#9A0EFF04 26928874 FF9124C4 D28F0702 0125
    
```

```
huawei(config-rsa-key-code)#public-key-code end
```

```
huawei(config-rsa-public-key)#peer-public-key end
```

步骤 9 将公钥授给 SSH 用户。

使用 `ssh user assign rsa-key` 将公钥 key 授给用户 huawei。

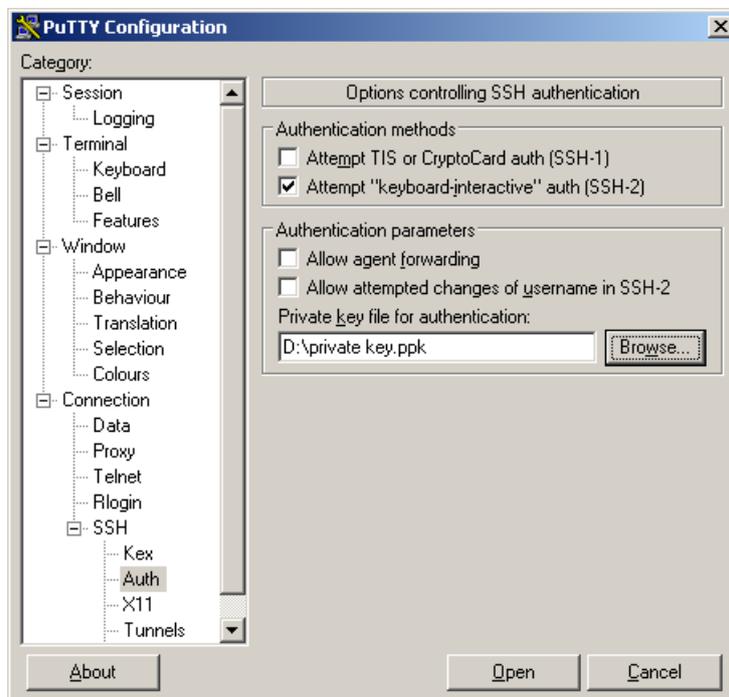
```
huawei(config)#ssh user huawei assign rsa-key key
```

步骤 10 登录系统。

1. 打开客户端工具。

运行 SSH 客户端工具 `putty.exe`，在导航树中选择“SSH > Auth”，指定 RSA 私钥文件，如图 1-18 所示。单击“Browse”，弹出文件选择窗口。选择私钥文件，并确定。

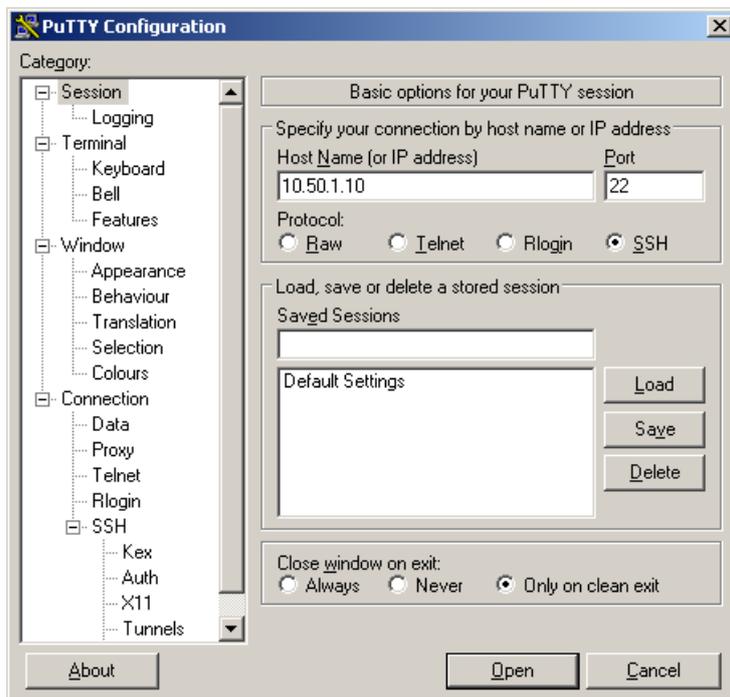
图 1-18 SSH 客户端工具界面图



2. 登录系统。

在目录树中选择“Session”，在“Host Name (or IP address)”文本框中输入 AC 设备的 IP 地址如图 1-19 所示，然后单击“Open”登录系统。

图 1-19 SSH 客户端登录界面图



因为设置的用户认证方式为 RSA，此时系统会给出提示信息，如图 1-20 所示。输入相应的用户名即可登录系统（这里的用户名为 **huawei**）。

图 1-20 SSH 客户端登录界面图



---结束

操作结果

用户登录系统后，可以对 AC 设备进行维护管理。

SSH 方式登录（带外管理）

通过本操作实现通过本地维护网口 ETH（带外管理接口）以 SSH 方式登录到 AC，对 AC 进行维护和管理。SSH（Secure Shell）通过提供认证、加密和鉴权来保证网络通信的安全性，当用户通过一个不能保证安全的网络环境远程登录到 AC 时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护 AC 不受诸如 IP 地址欺诈、明文密码截取攻击等影响。

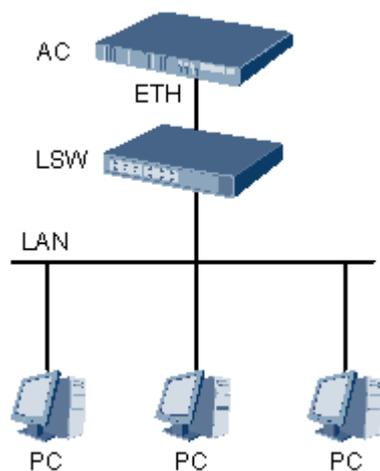
前提条件

- 已通过本地串口方式登录 AC，具体操作请参见“[1.1.1 通过串口登录系统](#)”。
-  说明
- 以下操作中在 AC 上的配置需要通过本地串口配置完成。
- 已经准备好调测以 SSH 方式登录 AC 时使用的工具：客户端软件密码生成工具 Puttygen.exe、客户端软件密码转换工具 sshkey.exe 和 SSH 客户端工具 putty.exe。

组网

SSH 方式通过局域网和广域网进行带外管理配置组网如[图 1-21](#)和[图 1-22](#)所示。

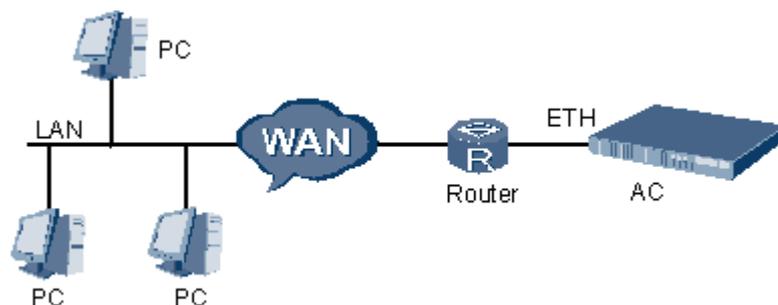
图 1-21 SSH 方式通过局域网进行带外管理配置组网图



 说明

AC 通过直通网线（Straight Through Cable）与局域网相连，且 AC 维护网口的 IP 地址与维护终端的 IP 地址在同一网段；也可以将维护终端的网口与 AC 主控板的维护网口直接连接，对设备进行带外管理，但此时要使用交叉网线（Crossover Cable）。

图 1-22 SSH 方式通过广域网进行带外管理配置组网图



数据规划

使用 SSH 方式登录 AC 的数据规划如表 1-5 所示。

表 1-5 SSH 方式登录 AC 的数据规划

配置项	数据
AC 网口	<ul style="list-style-type: none">● IP 地址：10.50.1.10/24● 用户认证方式：RSA 公钥认证● RSA 公钥名：key
新用户	<ul style="list-style-type: none">● 用户名/密码：huawei/test01● 权限：操作员级● 可重复登录数：4
维护终端	IP 地址：10.10.1.10/24
路由器接 AC 接口（SSH 方式通过广域网进行带外管理时选择此项）	IP 地址：10.50.1.1/24

操作步骤

步骤 1 搭建组网环境。

- 如果选择通过局域网带外管理方式以 SSH 方式登录到 AC 设备，搭建如图 1-21 所示的组网环境。
- 如果选择通过广域网带外管理方式以 SSH 方式登录到 AC 设备，搭建如图 1-22 所示的组网环境。

步骤 2 设置维护网口 IP 地址。

在 MEth 模式下，使用 **ip address** 命令设置维护网口 IP 地址。

```
huawei(config)#interface meth 0
huawei(config-if-meth0)#ip address 10.50.1.10 24
```

步骤 3 添加带外管理路由。

- 如果搭建图 1-21 所示的局域网本地管理环境，不需要添加路由。
- 如果搭建图 1-22 所示的广域网远程管理环境，使用 **ip route-static** 命令配置 AC 设备管理接口到维护终端的路由。

```
huawei(config-if-meth0)#quit
huawei(config)#ip route-static 10.10.1.0 24 10.50.1.1
```

步骤 4 创建一个用户。

使用 **terminal user name** 命令增加一个用户。

```
huawei(config)#terminal user name
User Name(length<6,15>):huawei
User Password(length<6,15>):test01//维护终端上不显示
Confirm Password(length<6,15>):test01//维护终端上不显示
User profile name(<=15 chars)[root]:
User's Level:
  1. Common User  2. Operator:2
Permitted Reenter Number(0-4):4
User's Appended Info(<=30 chars):
```

```
Adding user succeeds
Repeat this operation? (y/n)[n]:n
```

步骤 5 创建 SSH 本地密钥对。

使用 **rsa local-key-pair create** 命令创建 SSH 本地密钥对。



注意

成功完成 SSH 登录的首要操作是：配置并产生本地 RSA 密钥对。请您在进行其它 SSH 配置之前，完成创建 SSH 本地密钥对的操作。

```
huawei(config)#rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 512]:
Generating keys...
..+++++++
.....+++++++
.....+++++++
.....+++++++
```

步骤 6 设置 SSH 用户认证方式。

使用 **ssh user huawei authentication-type rsa** 命令选择 SSH 用户认证方式。

SSH 用户认证方式分为以下四种，这里以 **rsa** 为例进行介绍。

- **password**: 使用普通的口令。
- **rsa**: 使用 RSA 公钥。
- **all**: 使用 **password** 或 **rsa** 认证，即用户通过 **password** 或者 **rsa** 认证两者之一都可以登录到设备上。
- **password-publickey**: 使用 **password** 和 **publickey** 方式认证，即用户必须通过 **password** 和 **rsa** 两种认证后才可以登录到设备上。

```
huawei(config)#ssh user huawei authentication-type
{ all<K>|password-publickey<K>|password<K>|rsa<K> }:rsa

Command:
ssh user huawei authentication-type rsa
%Authentication type setted, and will be in effect next time.
```

步骤 7 生成 RSA 公钥。

1. 打开密码生成工具。

打开客户端软件密码生成工具 **Puttygen.exe**，如 [图 1-23](#) 所示。

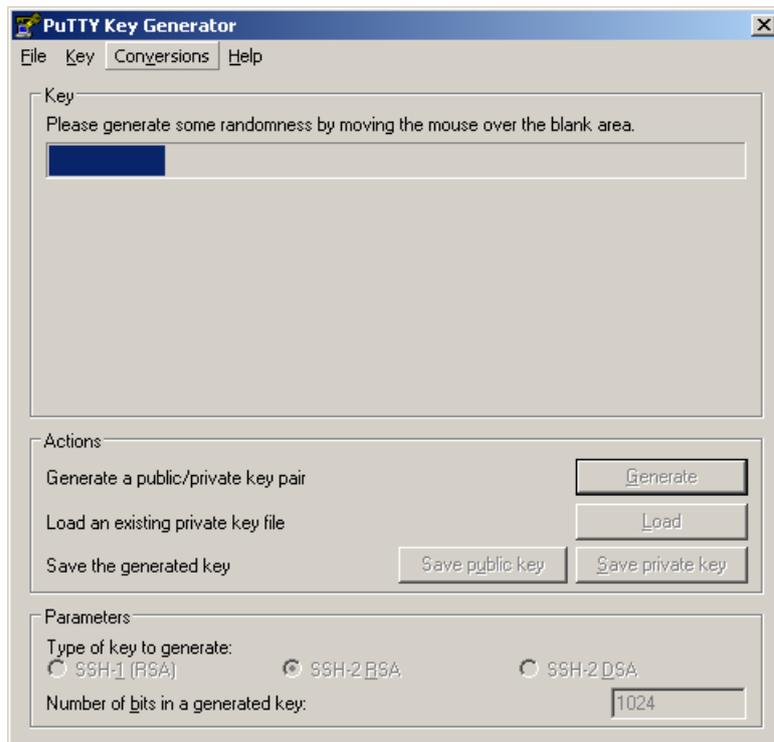
图 1-23 密码生成工具界面图



2. 生成客户端密钥。

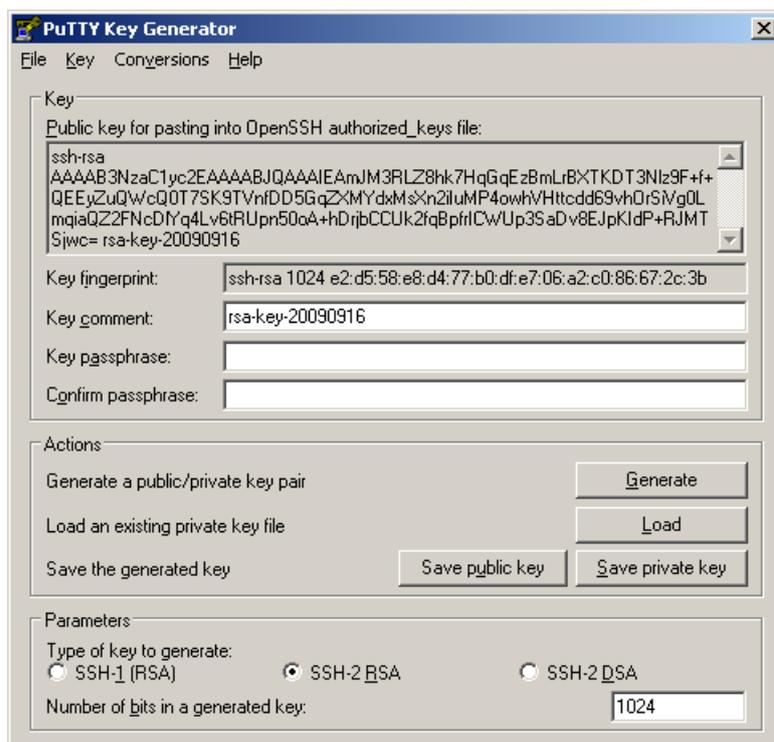
在“Parameters”区域中选择密钥类型为“SSH-2 RSA”后，单击“Generate”，根据页面提示移动鼠标进行密钥生成，如图 1-24 所示。

图 1-24 密码生成工具界面图



完成密钥生成后，单击“Save public key”和“Save private key”，保存 public key 和 private key。如图 1-25 所示。

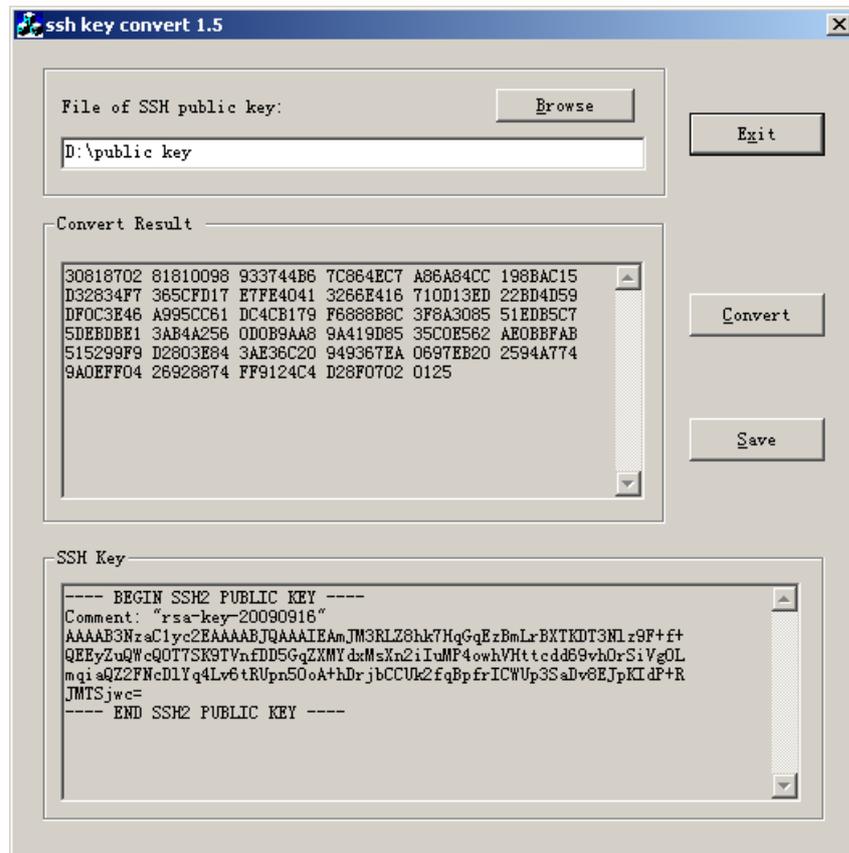
图 1-25 保存 public key 和 private key



3. 生成 RSA 公钥。

打开客户端软件密码转换工具 sshkey.exe，单击“Browse”，选择上面保存的 public key 文件。然后单击“Convert”，将客户端公钥转换成 RSA 公钥，如图 1-26 所示。

图 1-26 客户端公钥转换成 RSA 公钥工具界面图



步骤 8 生成 SSH 用户公钥。

创建 RSA 公钥 key，在 config-rsa-key-code 命令行模式下将 RSA 公钥拷贝进服务器端。

```
huawei(config)#rsa peer-public-key key
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.

huawei(config-rsa-public-key)#public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".

huawei(config-rsa-key-code)#30818702 81810098 933744B6 7C864EC7 A86A84CC 198BAC15

huawei(config-rsa-key-code)#D32834F7 365CFD17 E7FE4041 3266E416 710D13ED 22BD4D59

huawei(config-rsa-key-code)#DF0C3E46 A995CC61 DC4CB179 F6888B8C 3F8A3085 51EDB5C7

huawei(config-rsa-key-code)#5DEBDBE1 3AB4A256 OD0B9AA8 9A419D85 35COE562 AE0BBFAB

huawei(config-rsa-key-code)#515299F9 D2803E84 3AE36C20 949367EA 0697EB20 2594A774

huawei(config-rsa-key-code)#9A0EFF04 26928874 FF9124C4 D28F0702 0125
```

```
huawei(config-rsa-key-code)#public-key-code end
```

```
huawei(config-rsa-public-key)#peer-public-key end
```

步骤 9 将公钥授给 SSH 用户。

使用 `ssh user assign rsa-key` 将公钥 key 授给用户 huawei。

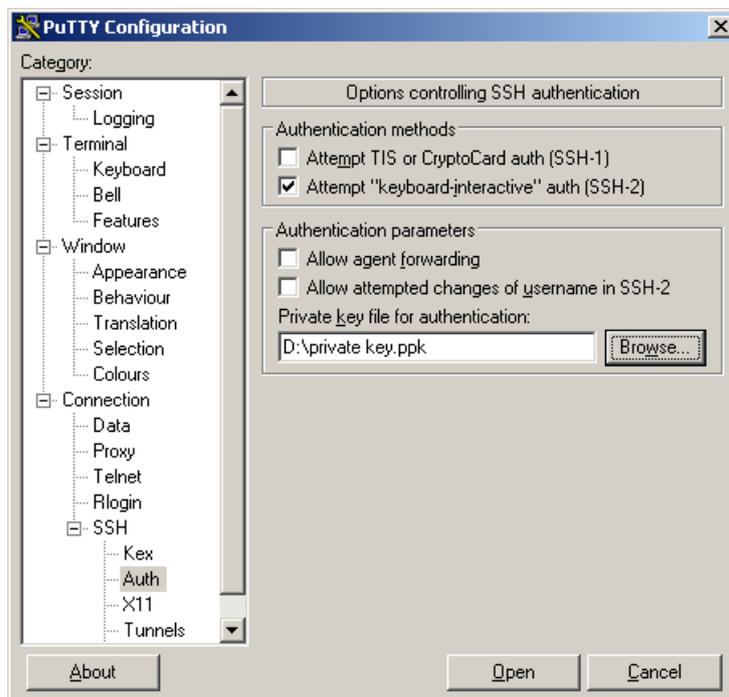
```
huawei(config)#ssh user huawei assign rsa-key key
```

步骤 10 登录系统。

1. 打开客户端工具。

运行 SSH 客户端工具 `putty.exe`，在导航树中选择“SSH > Auth”，指定 RSA 私钥文件，如图 1-27 所示。单击“Browse”，弹出文件选择窗口。选择私钥文件，并确定。

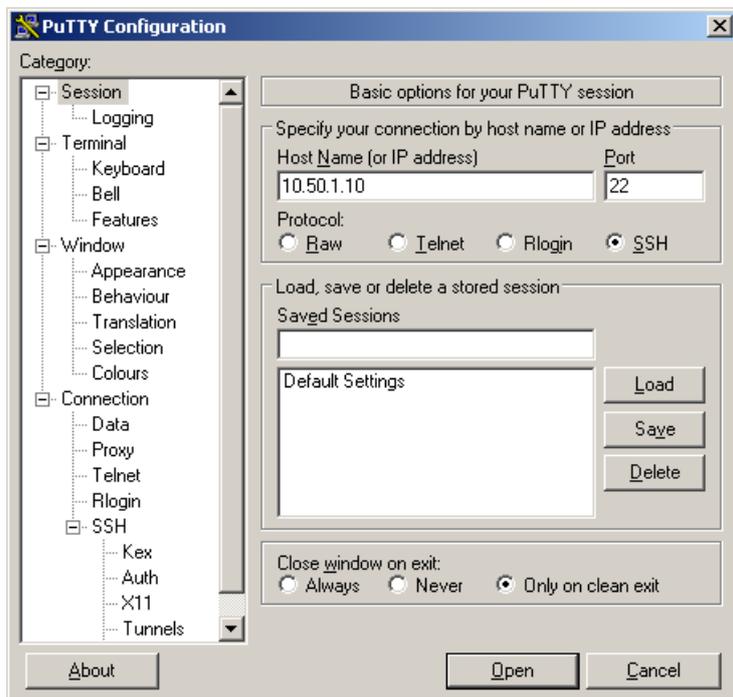
图 1-27 SSH 客户端工具界面图



2. 登录系统。

在目录树中选择“Session”，在“Host Name (or IP address)”文本框中输入 AC 设备的 IP 地址如图 1-28 所示，然后单击“Open”登录系统。

图 1-28 SSH 客户端登录界面图



因为设置的用户认证方式为 RSA，此时系统会给出提示信息，如图 1-29 所示。输入相应的用户名即可登录系统（这里的用户名为 **huawei**）。

图 1-29 SSH 客户端登录界面图



---结束

操作结果

用户登录系统后，可以对 AC 进行维护管理。

1.3 基本配置

介绍调测阶段的一些基本配置，包括修改系统名称、配置系统时间和配置系统操作用户等。

1.3.1 修改系统名称

通过修改系统名称为具有实际意义的值，来区分不同的 AC 设备，方便对 AC 设备进行管理。

背景信息

- 缺省情况下设备名称为 WAC。
- 系统名称设置后立即生效。
- 修改设备名称将影响命令行接口的提示符。

操作步骤

步骤 1 在特权模式下，使用 **sysname** 命令设置系统名称。

---结束

操作结果

修改系统名称执行成功后，命令行接口的提示符变为设置的系统名称。

任务示例

举例：命名中国深圳局第一台 AC 设备的名称为 SZ_WS6603_1。
WAC(config)#**sysname** SZ_WS6603_1
SZ_WS6603_1(config)#

1.3.2 配置系统时间

配置 AC 设备的系统时间、时区、时间戳、NTP（Network Time Protocol，网络时间协议）和夏令时的起止时间。

操作步骤

步骤 1 配置系统时间。

使用 **display time** 命令查看当前系统时间。如果系统时间与当地标准时间一致，则不需要修改。如果不一致，使用 **time** 命令修改系统时间。

步骤 2 配置系统时区。

使用 **display timezone** 命令查看当前系统时区。如果系统时区与当地标准一致，则不需要修改。如果不一致，使用 **timezone** 命令修改系统时区。

 说明

- 系统时区包括东时区和西时区。“GMT+”表示东时区，即本地时间快于格林威治时间；“GMT-”表示西时区，即本地时间慢于格林威治时间。
- 缺省情况下，系统时区为 GMT+8:00。

步骤 3 配置时间戳。

使用 **display time time-stamp** 命令查看网管和网元之间的时间戳（SNMP 接口的显示时间格式）。如果时间戳与实际规划一致，则不需要修改。如果不一致，使用 **time time-stamp** 命令修改时间戳。

 说明

网管和网元之间的 SNMP 接口时间格式有两类格式：UTC 时间和网元本地时间。缺省情况下，网管和网元之间的接口时间格式为网元本地时间格式。

步骤 4 配置 NTP，使网络内所有设备的时钟保持一致。

- （可选）使用 **ntp-service refclock-master** 命令配置 NTP 主时钟。
- 使用 **ntp-service unicast-server** 命令配置 NTP 单播服务器模式，并指定作为本地时间服务器的远程服务器 IP 地址和本地收发 NTP 消息的接口。

 说明

- NTP 协议支持客户端/服务器模式、对等体模式、广播模式和组播模式四种工作模式，此处以客户端/服务器模式为例。如果需要配置其他模式，请参见[配置网络时间](#)。
- 客户端和服务端上必须有能够相互通信的三层接口和接口 IP 地址。
- 在客户端/服务器模式下，只需在客户端配置，服务器端除了配置 NTP 主时钟外，不需要进行其他配置。
- 在客户端/服务器模式下，只能是客户端同步到服务器，服务器不会同步到客户端。
- 同步设备的时钟层数必须小于被同步设备的时钟层数，否则，不能进行时钟同步。
- 对于运行 NTP 的设备，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。当设备工作在客户端模式时，不需要设置系统时间，设备自动向远程服务器同步。

步骤 5 配置夏令时的起止时间。

使用 **display time dst** 命令查看当前系统夏令时的起止时间。如果系统夏令时的起止时间与实际一致，则不需要修改。如果不一致，使用 **time dst** 命令修改夏令时的起止时间。

----结束

操作结果

系统时间、时区、时间戳、NTP 配置、夏令时的起止时间与实际一致。

任务示例

举例：设置网管与网元之间的时间戳为 UTC 时间。

```
huawei#display time time-stamp
Current time-stamp is: local time //修改前的时间戳为网元本地时间

huawei#time time-stamp
{ local<K>|utc<K> }:utc

Command:
time time-stamp utc

huawei#display time time-stamp
Current time-stamp is: UTC (Coordinated Universal Time) //修改后的时间戳为UTC时间
```

举例：AC 设备 A 当前时区为 GMT+7:00，采用网络时钟调整时间，通过 VLAN 接口 2 向 NTP 服务器 AC 设备 B（IP 地址：10.20.20.20/24，所处层数：4）发送同步时钟请求报文。设置夏令时信息，其中开始时间是 5 月 1 日的 00:00:00，结束时间是 9 月 30 日的 00:00:00，调整时间为 1:00。即如果本地时间为 5:00，则调整后为 6:00。

```
huawei(config)#timezone GMT+ 7:00
huawei(config)#ntp-service refclock-master 4
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 1:00
```

举例：AC 设备 A 当前时区为 GMT- 4:00，采用本地时间，当前时间为 2010-01-01 12:10:10。设置夏令时信息，其中开始时间是 5 月 1 日的 00:00:00，结束时间是 9 月 30 日的 00:00:00，调整时间为 2:00。即如果本地时间为 5:00，则调整后为 7:00。

```
huawei(config)#timezone GMT- 4:00
huawei(config)#time 2010-01-01 12:10:10
huawei(config)#time dst start 5-1 00:00:00 end 9-30 00:00:00 adjust 2:00
```

1.3.3 配置系统操作用户

当对 AC 设备进行访问和配置管理时，需要增加不同属性的系统操作用户。本节介绍如何增加系统操作用户和修改系统操作用户的属性。

增加系统操作用户

当对 AC 设备进行访问和配置时，需要增加不同属性的系统操作用户，便于管理。

前提条件

具有管理员及管理员级别以上的操作权限。

背景信息

- 超级用户和管理员级的操作用户拥有增加比自身级别低的用户权限，即：
 - 超级用户可以增加管理员级、操作员级和普通用户级的操作用户。
 - 管理员级用户只能增加操作员级和普通用户级的操作用户。
- 操作用户名不能和已有的操作用户名重复，且不能为 **all** 和 **online**。
- 可以连续增加多个操作用户，整个系统最多可以增加 127 个操作用户，包括 root 用户总共 128 个用户。
- 系统最多可支持 10 个终端用户同时在线。

增加系统操作用户时，需要配置操作用户属性，包括用户的帐号、口令、用户模板、权限、可重复登录次数和操作用户附加信息。具体如表 1-6 所示。

表 1-6 操作用户属性

操作用户属性	操作用户属性说明
帐号	又称操作用户名，由 6 ~ 15 个可打印的字符组成，在整个系统中是唯一的，不能重复。帐号中不能有空格出现，并且不区分字母大小写。
口令	又称密码，由 6 ~ 15 个字符组成。口令中至少包含 1 个数字和 1 个字母，并且区分字母大小写。

操作用户属性	操作用户属性说明
用户模板	用户模板名由 1 ~ 15 可打印的字符组成，一个用户模板中包括用户名的有效期、用户密码的有效期、开始登录时间、结束登录时间。
权限	<p>根据分配的操作权限不同，AC 设备将操作用户权限分四个级别：普通用户级、操作员级、管理员级和超级用户级。各级用户只能增加比自身级别低的用户。操作用户操作管理权限如下所示：</p> <ul style="list-style-type: none"> ● 普通用户级：执行基本的系统操作以及简单的查询操作。 ● 操作员级：可对设备、业务进行配置。 ● 管理员级和超级用户级： <ul style="list-style-type: none"> - 两者共同点在于： <ul style="list-style-type: none"> - 可执行所有配置操作。 - 负责对设备、用户帐号以及操作管理权限进行维护管理。 - 两者不同点在于： <ul style="list-style-type: none"> - 超级用户仅有一个，是系统最高级别的用户；而管理员级用户可以有多个。 - 超级用户可以增加管理员级用户；而管理员级用户不可以增加超级用户。
可重复登录数	一个操作用户是否可以从多个终端同时登录，由该操作用户的可重复登录次数决定，范围是 0 ~ 4，一般设置为 1。
操作用户附加信息	操作用户附加信息是操作用户的一种补充性信息，由一串字符组成，可以为空，最多为 30 个字符，可以是操作用户的联系电话、地址等。

操作步骤

步骤 1 使用 **terminal user name** 命令增加与实际规划一致的系统操作用户。

步骤 2 使用 **display terminal user** 命令查询操作用户信息。

----结束

操作结果

查询到的操作用户信息与实际规划一致。

任务示例

举例：在管理员用户权限下增加一个系统操作用户：账号为 huawei，口令为 test01，用户模板为默认模板 root，权限为普通用户级，可重复登录次数为 3 次，操作用户附加信息为 user。

```
huawei(config)#terminal user name
User Name(length<6, 15>):huawei
User Password(length<6, 15>):test01//维护终端上不显示
Confirm Password(length<6, 15>):test01//维护终端上不显示
User profile name(<=15 chars)[root]:
User's Level:
```

```

1. Common User 2. Operator:1
Permitted Reenter Number(0--4):3
User's Appended Info(<=30 chars):user
Adding user succeeds
Repeat this operation? (y/n)[n]:n
    
```

```
huawei(config)#display terminal user name huawei
```

Name	Level	Status	Reenter Num	Profile	Append Info
huawei	User	Offline	3	root	user

修改系统操作用户属性

当系统操作用户属性不符合当前规划时，需要修改相关属性，包括口令、用户模板、权限、可重复登录数，以及操作用户附加信息等。

前提条件

用户具有相关的操作权限，请参见“背景信息”处的描述。

背景信息

修改系统操作用户属性的修改项及约束条件如表 1-7 所示。

表 1-7 修改操作用户属性

操作用户属性修改项	约束条件
口令	<ul style="list-style-type: none"> ● 超级用户和管理员级的操作用户可以修改自身以及比自身级别低的操作用户的口令，修改比自身级别低的操作用户的口令时不需要输入原有口令。 ● 普通用户级和操作员级的操作用户，只可以修改自己的口令，且修改时需要输入原口令。
用户模板	<ul style="list-style-type: none"> ● 只有超级用户和管理员级的操作用户可以修改自身以及比自身级别低的操作用户绑定的模板。 ● 操作用户的用户名和密码应该满足将要绑定的用户模板的规格，否则绑定不成功。
权限	只有超级用户和管理员级的操作用户可以修改比自身级别低的操作用户的权限，并且他们只能将这些操作用户权限修改为比自身级别更低的权限。
可重复登录数	<ul style="list-style-type: none"> ● 只有超级用户和管理员级的操作用户可以修改比自身级别低的操作用户的可重复登录次数。 ● 超级用户的可重复登录次数不能被修改。
操作用户附加信息	<ul style="list-style-type: none"> ● 超级用户和管理员级的操作用户可以修改自身以及比自身级别低的操作用户的附加信息。 ● 普通用户级和操作员级的操作用户只能修改自身的附加信息。

操作步骤

步骤 1 修改系统操作用户属性。



说明

在执行修改操作前，可以使用 **display terminal user** 命令查询需要修改的操作用户的属性。

- 使用 **terminal user password** 命令修改操作用户口令。
用户口令长度限制在 6 ~ 15 个字符之间，并且口令中至少包含 1 个数字和 1 个英文字母，并且区分字母大小写。
- 使用 **terminal user user-profile** 命令修改操作用户模板。
- 使用 **terminal user level** 命令修改操作用户权限。
- 使用 **terminal user reenter** 命令修改操作用户可重复登录数。
- 使用 **terminal user apdinfo** 命令修改操作用户的附加信息。
当系统出现故障时，可以通过查询用户附加信息与用户取得联系。建议修改用户附加信息为用户的联系方式或者地址等具有实际意义的值。

步骤 2 检查系统操作用户信息。

使用 **display terminal user** 命令查询系统操作用户信息。

---结束

操作结果

查询到的系统操作用户信息与修改的系统操作用户属性一致，使用该操作用户原来的帐号和新的口令可以登录到 AC 设备。

任务示例

举例：修改账号为 huawei 的系统操作用户属性，修改口令为 test02，用户模板为 operator，权限为操作员级，可重复登录次数为 4 次，操作用户附加信息为 operator。

```
huawei(config)#terminal user password
User Name(<=15 chars):huawei
New Password(length<6, 15>):test02//控制台上不显示
Confirm Password(length<6, 15>):test02//控制台上不显示
Information takes effect
Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user user-profile
User Name(<=15 chars):huawei
Permitted user-profile[root]:operator
Confirm user-profile:operator
Configuration will take effect when the user logs on next time.
Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user level
User Name(<=15 chars):huawei
1. Common User 2. Operator:
User's Level:2
Confirm Level:2
Information will take effect when this user logs on next time
Repeat this operation? (y/n)[n]:n

huawei(config)#terminal user reenter
User Name(<=15 chars):huawei
Permitted Reenter Number(0--4):4
Confirm Reenter Number(0--4):4
Information will take effect when this user logs on next time
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#terminal user apdinfo
User Name(<=15 chars):huawei
User's Appended Info(<=30 chars):operator
Information takes effect
Repeat this operation? (y/n)[n]:n
```

```
huawei(config)#display terminal user name huawei
```

Name	Level	Status	Reenter Num	Profile	Append Info
huawei	Operator	Offline	4	operator	operator

1.3.4 配置端口

介绍增加端口描述信息和配置端口属性的方法。

增加端口描述信息

通过本任务设置端口的描述信息。

背景信息

为 AC 设备的物理端口增加描述信息后，可以方便用户在系统维护时进行信息查询。

操作步骤

步骤 1 在全局模式下，使用 **port desc** 增加端口的描述信息。
端口的描述信息为字符串，用于标识机框中单板的端口。

步骤 2 使用 **display port desc** 查看端口描述信息。

---结束

任务示例

举例：规划用户端口描述信息格式为“小区编号-楼编号-楼层编号/机框号-槽位号-端口号”，“小区编号-楼编号-楼层编号”为 AP 设备放置的物理位置，机框号-槽位号-端口号为本设备与 AP 设备连接的物理端口。该规划可以体现 AP 设备位置及 AP 与 AC 设备连接的关系，方便在维护时查询。现在 AC 设备 0/2/0 的端口接入的 AP 放置于 A 小区 01 号楼、楼层为 1，要求为该端口按照规划增加描述信息。

```
huawei(config)#port desc 0/2/0 description A-01-01/0-2-0
huawei(config)#display port desc 0/2/0
```

F/ S/ P	IMA Group	Port Description
0/ 2/ 0	-	A-01-01/0-2-0

配置端口属性

通过本任务对指定的端口进行属性配置，使系统与 AP、交换机或上层设备通讯正常。

背景信息

AC 设备需要与 AP、交换机或上层设备使用端口对接，因此需要注意端口属性的一致性。

缺省配置

AC 设备端口属性的系统缺省值如表 1-8 所示。

表 1-8 端口属性缺省值

参数项	缺省值（光口）	缺省值（电口）
端口自协商模式	自协商	自协商
端口速率	<ul style="list-style-type: none"> ● GE 光口为 1000Mbit/s。 ● 10 GE 光口为 10000Mbit/s。 	不能进行配置 说明 去使能端口自协商模式后，可以对端口速率进行配置。
双工模式	全双工	不能进行配置 说明 去使能端口自协商模式后，可以对端口双工模式进行配置。
网线适应方式	不支持	支持
流量控制	关闭	关闭

操作步骤

- 配置端口物理属性。
 1. （可选）设置以太网端口自协商模式。
 使用命令 **auto-neg** 对以太网端口自协商模式进行设置。可以对自协商模式进行使能或者去使能：
 - 当使能自协商模式后，端口自动和对接端口协商以太网端口的端口速率和工作模式。
 - 当去使能自协商模式后，端口的速率和工作模式处于强制模式（使用默认或命令行设置的速率和工作模式）。
 2. （可选）设置以太网端口速率。
 使用命令 **speed** 设置以太网端口速率，当端口速率配置成功后，可以使端口以设定的速率工作。进行配置时的注意事项：
 - 配置原则是互连的两个设备对应端口的端口速率应一致，以避免无法通讯的问题。
 - 需要去使能自协商模式。
 3. （可选）配置以太网端口双工模式。
 使用命令 **duplex** 配置以太网端口双工模式。端口双工状态可以为半双工、全双工、自协商三种模式，进行配置时的注意事项：
 - 配置原则是互连的两个设备对应端口双工状态应一致，以避免无法通讯的问题。

- 需要去使能自协商模式。
- 4. (可选) 配置以太网端口的网线适应方式。
使用命令 **mdi** 配置以太网端口的网线适应方式，使之与实际使用的网线匹配。
网线适应方式有以下三种：
 - **normal**: 指定以太网端口的网线适应方式为使用直通网线。这时与该以太网端口实际连接的网线类型必须为直通网线。
 - **across**: 指定以太网端口的网线适应方式为使用交叉网线。这时与该以太网端口实际连接的网线类型必须为交叉网线。
 - **auto**: 指定以太网端口的网线适应方式为自适应方式。这时与该以太网端口实际连接的网线类型既可以使用直通网线也可以使用交叉网线。
- 配置端口的流量控制。
使用 **flow-control** 命令用于开启端口的流量控制。当端口的流量比较大，需要对其进行控制时，使用此命令，以避免造成网络拥塞，丢失数据包。流量控制需要本端和对端设备均支持，配置时需要注意：
 - 如果对端设备支持流量控制，本端一般设置为开启流量控制开关。
 - 如果对端设备不支持流量控制，本端一般设置为关闭流量控制。系统缺省值为关闭流量控制。
- 配置以太网端口镜像。
使用命令 **mirror port** 配置以太网端口镜像，当系统出现问题时，需要将系统中某个端口的流量复制到其它的端口输出，用于流量观测、网络故障诊断、数据分析。

---结束

任务示例

举例：以太网端口 0/2/0 为电口，设置其属性为：端口速率 1000Mbit/s，全双工模式，支持流量控制，不支持自协商模式。

```
huawei(config)#interface scu 0/2
huawei(config-if-scu-0/2)#auto-neg 0 disable
huawei(config-if-scu-0/2)#speed 0 1000
huawei(config-if-scu-0/2)#duplex 0 full
huawei(config-if-scu-0/2)#flow-control 0
```

1.4 配置 License

License 平台为 AC 设备提供注册机制。在系统初使化时，AC 各业务模块需要注册受控资源项或受控功能项。

前提条件

已经获取 License 文件。获取 License 文件的详细操作方法请参见随软件一起发布的《商用 License 发放流程》指导书。

 说明

在获取 License 文件时，需要提供设备的 ESN。可以使用 **display license** 命令查看设备的 ESN 信息。

背景信息



注意

- WS6603 默认开启 License 功能。
- 如果设备没有加载 License 文件，或者 License 文件错误，系统会进入试用期（试用期默认为 30 天）。
- 设备在试用期内可以支持上线最大 AP 数（1024 个）。试用期结束后，如果设备仍然没有加载正确的 License 文件，系统将保留最先注册的 5 个 AP 上线，强制其他所有 AP 下线。
- 设备正确加载了 License 文件后，允许最大 AP 上线数量按照 License 实际授权数控制。

操作步骤

步骤 1 使用 **load license** 命令加载设备的 License 文件。

License 文件加载成功后，无需进行任何操作，设备会根据加载的 License 文件判断允许的 AP 上线数目。

步骤 2 使用 **display license** 命令查看加载的 License 文件信息。

---结束

任务示例

举例：通过 TFTP 方式加载设备的 License 文件。SN 为 LIC2010032900A800，ESN 为 B5EA73AB92469D177B0EE92C4F56FDF78B357BFC。

```
WAC(config)#display license
License function is disabled

Active main board license protocol version:1.2
Active main board LIB version:1.2.038
Active main board license serial No.:...//此时还没有License文件
Active main board ESN:B5EA73AB92469D177B0EE92C4F56FDF78B357BFC...//ESN信息
huawei(config)#load license tftp 10.11.104.2 license
huawei(config)#display license
License function is enabled

Active main board license protocol version:1.2
Active main board LIB version:1.2.038
Active main board license serial No.:LIC2010032900A800...//已经加载License文件
Active main board ESN:B5EA73AB92469D177B0EE92C4F56FDF78B357BFC
```

1.5 保存与备份数据

AC 设备支持保存与备份数据，以满足系统升级的需要，并且保证系统在发生升级失败或者严重问题时的恢复能力。

1.5.1 配置文件传输方式

介绍 FTP、SFTP、TFTP 和 Xmodem 传输方式的配置方法。

配置 FTP 文件传输方式

当需要通过 AC 设备的带内或带外网口传输文件（上传文件或下载文件）时，可根据本操作指导配置 FTP 传输方式，使 FTP 服务器与 AC 设备之间可以正常通信，实现 FTP 方式的文件传输。

前提条件

- FTP 服务器的以太网端口与 AC 设备的带内或带外网口已经通过网线直接相连。
 - 与带内网口（上行口）连接使用交叉网线。
 - 与带外网口（维护网口）连接使用直连网线。
- 操作控制台（维护终端）已经使用 Telnet 方式登录到 AC 设备，并进入全局配置模式。

工具、仪表和材料

- 交叉网线
- 直连网线

对系统的影响

无

注意事项

当 FTP 服务器与 AC 设备直接相连时，需要使用交叉网线。其他情况下使用直通网线连接。

操作步骤

步骤 1 在 FTP 服务器上配置 FTP 服务器以太网端口 IP 地址。

根据不同组网下 IP 地址的规划情况配置 FTP 服务器以太网端口 IP 地址，确保 FTP 服务器以太网端口与 AC 设备的带内或带外网口能相互 Ping 通即可。

例如：如果 FTP 服务器以太网端口与 AC 设备直接相连，则 FTP 服务器以太网端口 IP 地址与 AC 设备的带内或带外网口 IP 地址需要在同一网段。

步骤 2 在 FTP 服务器上运行 FTP 应用程序并设置相关参数。

运行 FTP 应用程序，设置文件的存放路径和 FTP 用户名、密码。

步骤 3（该步骤用于配置手动文件传输时使用的 FTP 用户属性）使用 **ftp set** 命令配置 FTP 用户名和密码。

```
huawei(config)#ftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//命令行上看不到输入
```

 说明

系统缺省的 FTP 用户名为 anonymous，密码为 anonymous@huawei.com。

步骤 4（可选，需要使用自动备份数据库文件功能时，执行此步骤）使用 **file-server auto-backup data** 命令配置 FTP 用户名、密码和端口号。

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 ftp path test user
User Name(<=40 chars):huawei
User Password(<=40 chars):huawei//命令行上看不到输入
```

----结束

参考信息

- 任何运行 FTP 软件的计算机都可以作为 FTP 服务器。
- 使用 FTP 协议进行文件传输时，需要验证用户名和密码。除了在 FTP 服务器上设置用户名和密码外，在 FTP 客户端（如 AC 设备）中也需要设置 FTP 用户名和密码，并且要保证与 FTP 服务器侧配置一致。

配置 SFTP 文件传输方式

当需要通过 AC 设备的带内或带外网口传输文件（上传文件或下载文件）时，可根据本操作指导配置 SFTP 传输方式，使 SFTP 服务器与 AC 设备之间可以正常通信，实现 SFTP 方式的文件传输。

前提条件

- SFTP 服务器的以太网端口与 AC 设备的带内或带外网口已经通过网线直接相连。
 - 与带内网口（上行口）连接使用交叉网线。
 - 与带外网口（维护网口）连接使用直连网线。
- 操作控制台（维护终端）已经使用 Telnet 方式登录到 AC 设备，并进入全局配置模式。

工具、仪表和材料

- 交叉网线
- 直连网线

对系统的影响

无

注意事项

当 SFTP 服务器与 AC 设备直接相连时，需要使用交叉网线。其他情况下使用直通网线连接。

操作步骤

步骤 1 在 SFTP 服务器上配置 SFTP 服务器以太网端口 IP 地址。

根据不同组网下 IP 地址的规划情况配置 SFTP 服务器以太网端口 IP 地址，确保 SFTP 服务器以太网端口与 AC 设备的带内或带外网口能相互 Ping 通即可。

例如：如果 SFTP 服务器以太网端口与 AC 设备直接相连，则 SFTP 服务器以太网端口 IP 地址与 AC 设备的带内或带外网口 IP 地址需要在同一网段。

步骤 2 在 SFTP 服务器上运行 SFTP 应用程序并设置相关参数。

运行 SFTP 应用程序，设置文件存放路径、SFTP 用户名、密码、端口号。缺省端口号为 22。

步骤 3（该步骤用于配置手动文件传输时使用的 SFTP 用户属性）使用 **ssh sftp set** 命令配置 SFTP 用户名、密码和端口号。

```
huawei(config)#ssh sftp set
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//命令行上看不到输入
  Listening Port(0--65535):22
```

步骤 4（可选，需要使用自动备份数据库文件功能时，执行此步骤）使用 **file-server auto-backup data** 命令配置 SFTP 用户名、密码和端口号。

```
huawei(config)#file-server auto-backup data primary 10.10.20.1 sftp path test port 22 user
  User Name(<=40 chars):huawei
  User Password(<=40 chars):huawei//命令行上看不到输入
```

 说明

AC 系统没有缺省的 SFTP 用户名、密码和端口号。

---结束

参考信息

- 任何运行 SFTP 软件的计算机都可以作为 SFTP 服务器。
- 使用 SFTP 协议进行文件传输时，需要验证用户名和密码。除了在 SFTP 服务器上设置用户名、密码和端口号外，在 SFTP 客户端（如 AC 设备）中也需要设置 SFTP 用户名、密码和端口号，并且要保证与 SFTP 服务器侧配置一致。

配置 TFTP 文件传输方式

当需要通过 AC 设备的带内或带外网口传输文件（上传文件或下载文件）时，可根据本操作指导配置 TFTP 传输方式，使 TFTP 服务器与 AC 设备之间可以正常通信，实现 TFTP 方式的文件传输。

前提条件

- TFTP 服务器的以太网端口与 AC 设备的带内或带外网口已经通过网线直接相连。
 - 与带内网口（上行口）连接使用交叉网线。
 - 与带外网口（维护网口）连接使用直连网线。
- 操作控制台（维护终端）已经使用 Telnet 方式登录到 AC 设备，并进入全局配置模式。

工具、仪表和材料

- 交叉网线
- 直连网线

对系统的影响

无

注意事项

当 TFTP 服务器与 AC 设备直接相连时，需要使用交叉网线。其他情况下使用直通网线连接。

操作步骤

步骤 1 在 TFTP 服务器上配置 TFTP 服务器以太网端口 IP 地址。

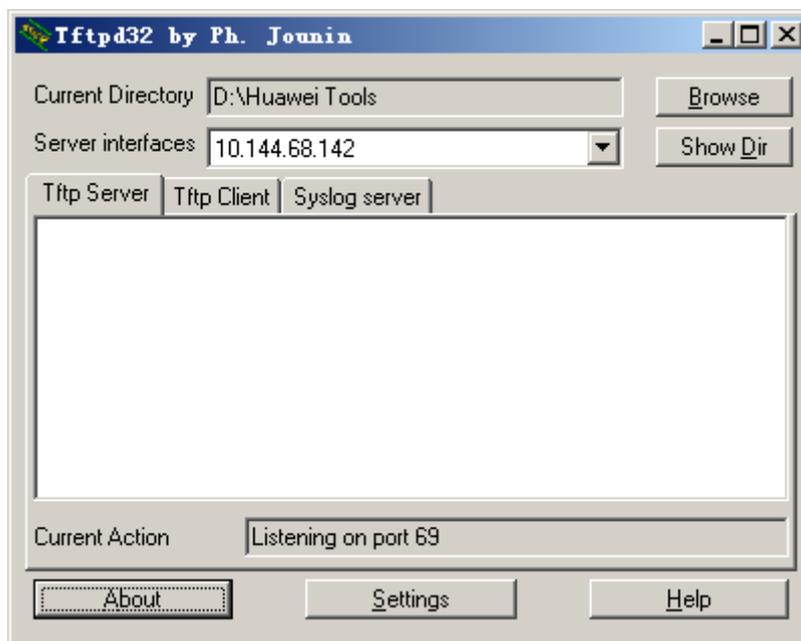
根据不同组网下 IP 地址的规划情况配置 TFTP 服务器以太网端口 IP 地址，确保 TFTP 服务器以太网端口与 AC 设备的带内或带外网口能相互 Ping 通即可。

例如：如果 TFTP 服务器以太网端口与 AC 设备直接相连，则 TFTP 服务器以太网端口 IP 地址与 AC 设备的带内或带外网口 IP 地址需要在同一网段。

步骤 2 在 TFTP 服务器上运行 TFTP 应用程序并设置相关参数。

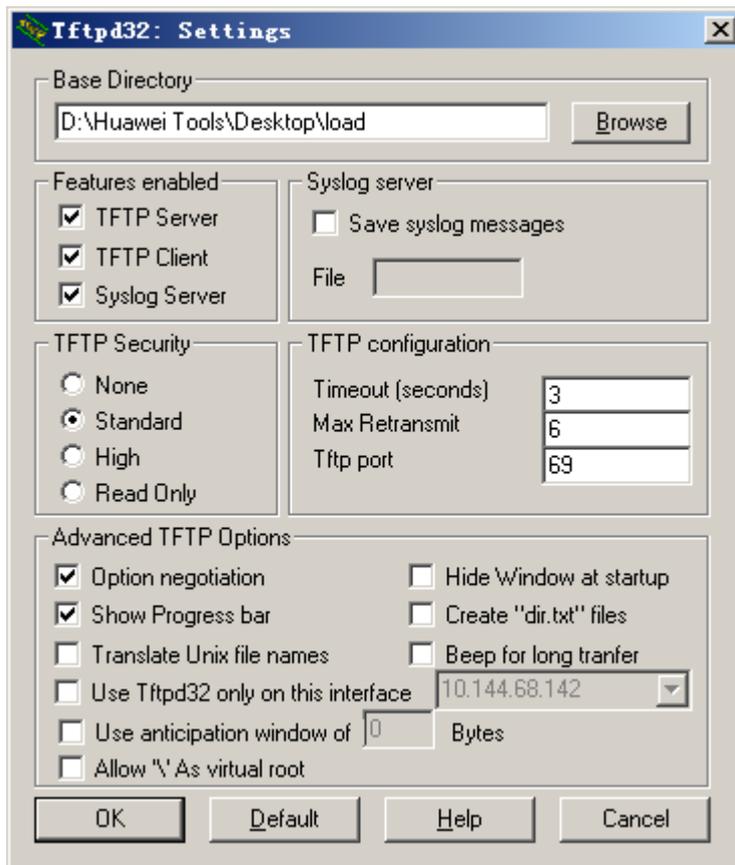
1. 在 TFTP 服务器上运行 TFTP 应用程序后，出现如**图 1-30** 所示的界面。在其中的“Server interfaces”下拉列表中选择步骤 1 中设置好的 IP 地址。

图 1-30 TFTP 主界面图



2. 在**图 1-30** 所示的界面中，单击“Settings”。
3. 在弹出的对话框中单击“Browse”，选择文件存放路径，如**图 1-31** 所示。

图 1-31 TFTP 参数配置界面图



---结束

参考信息

- 任何运行 TFTP 软件的计算机都可以作为 TFTP 服务器。
- “Server interfaces” 下拉列表中的 IP 地址为 TFTP 服务器的 IP 地址，TFTP 软件会自动识别 IP 地址。如果 TFTP 服务器有多个 IP 地址，需要选择正确的 IP 地址。
- 在采用 TFTP 方式传输文件时，如果不成功，请检查：
 - 选择的 TFTP 服务器 IP 地址是否正确。
 - 从 TFTP 服务器是否可以 Ping 通 AC 设备带内或带外网口 IP 地址。
 - TFTP 服务器上是否运行了 TFTP 应用程序。
 - TFTP 应用程序中的目录设置是否正确。
 - 是否已经使用命令启动 TFTP 传输功能。
 - 输入的文件名是否正确。

配置 Xmodem 文件传输方式

当需要通过 AC 设备的维护串口传输文件（上传文件或下载文件）时，可根据本操作指导配置 Xmodem 传输方式，使操作控制台与 AC 设备之间可以正常通信，实现 Xmodem 方式的文件传输。

前提条件

操作控制台（维护终端）已经通过串口登录到 AC 设备，并进入全局配置模式。

工具、仪表和材料

RS232 串口线（操作控制台通过串口登录到 AC 设备时使用）

对系统的影响

无

注意事项



注意

由于是通过串口进行文件传输，因此 Xmodem 方式的传输速度有限。在条件允许的情况下，请尽可能使用 FTP 等其他传输方式。

- AC 设备的串口波特率必须与操作控制台的串口波特率保持一致。
- 只有主用主控板才能使用 Xmodem 传输方式。
- 使用 Telnet 方式登录系统的用户禁止使用 Xmodem 方式传输文件。

操作步骤

步骤 1 在 AC 设备上查询串口波特率。

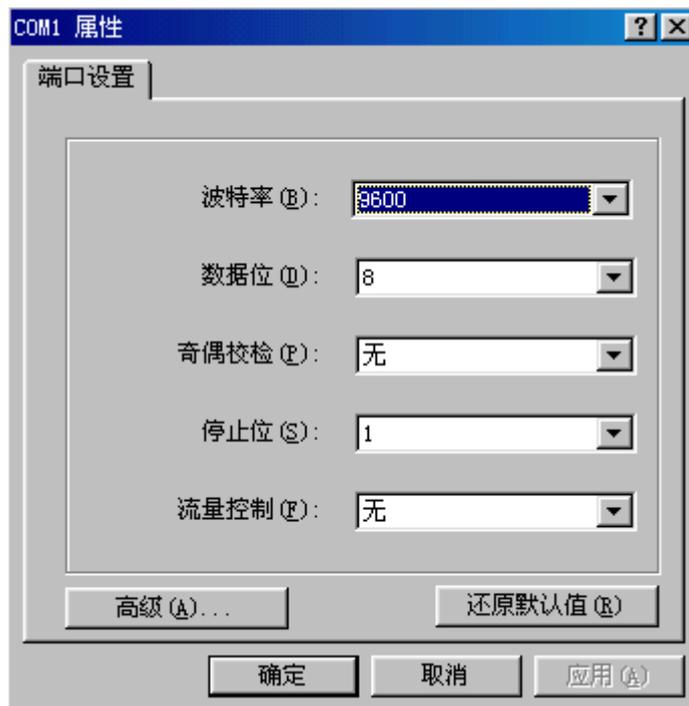
```
huawei(config)#display baudrate
Current active serial baudrate: 9600 bps
```

步骤 2（可选，当需要重新配置串口波特率时执行此步骤）使用 **baudrate** 命令配置 AC 设备的串口波特率。设置较高波特率可以提高传输速度。

举例：操作控制台的串口波特率为 9600bit/s，AC 设备当前串口波特率为 4800bit/s，则需要 AC 设备上执行如下命令：

```
huawei(config)#baudrate 9600
```

步骤 3 在操作控制台上打开“超级终端”工具，配置串口波特率与 AC 设备一致。



---结束

1.5.2 手动保存与备份数据

将数据以手动的方式保存到 Flash memory 或者服务器中，防止由于意外重启导致数据丢失。

手动保存数据

配置以手动方式保存系统数据文件。

背景信息

数据库文件和配置文件都是保存配置数据的文件，其中数据库文件以二进制格式保存配置，配置文件以命令行格式保存配置。数据的保存包括数据库文件和配置文件的保存，手动保存各操作所对应的命令及功能如表 1-9 所示。

表 1-9 手动保存数据操作列表

保存操作	命令	功能
手动保存数据库文件	save data	仅保存数据库文件，不保存配置文件
手动保存配置文件	save configuration	仅保存配置文件，不保存数据库文件
手动保存数据库文件和配置文件	save	同时保存数据库文件和配置文件

操作步骤

步骤 1 请根据实际需要，选择表 1-9 中的一种保存方式对系统数据进行手动保存操作。

----结束

操作结果

系统提示数据库文件、配置文件保存完成。

任务示例

任意选择以下一种方式，保存数据库文件或配置文件。

- 保存当前系统的数据库文件。

```
huawei(config)#save data
The data is being saved, please wait a moment...

huawei(config)#
1 [2010-07-12 14:32:00+08:00]:The percentage of saved data on 6 slot's main
control board is: 21%

huawei(config)#
1 [2010-07-12 14:32:03+08:00]:The percentage of saved data on 6 slot's main
control board is: 27%

huawei(config)#
1 [2010-07-12 14:32:06+08:00]:The percentage of saved data on 6 slot's main
control board is: 66%

huawei(config)#
1 [2010-07-12 14:32:09+08:00]:The percentage of saved data on 6 slot's main
control board is: 72%

huawei(config)#
1 [2010-07-12 14:32:12+08:00]:The percentage of saved data on 6 slot's main
control board is: 96%

huawei(config)#
1 [2010-07-12 14:32:15+08:00]:The percentage of saved data on 6 slot's main
control board is: 98%

huawei(config)#
1 [2010-07-12 14:32:18+08:00]:The percentage of saved data on 6 slot's main
control board is: 98%

huawei(config)#
1 [2010-07-12 14:32:19+08:00]:The data of 6 slot's main control board is saved
completely
```

- 保存当前系统的配置文件。

```
huawei#save configuration

huawei#
It will take several minutes to save configuration file, please wait...

huawei#
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

- 同时保存当前系统的数据库文件和配置文件。

```
WS6803(config)#save
{ <cr>|configuration<K>|data<K> }:
```

```
Command:
    save

huawei(config)#
    It will take several minutes to save configuration file, please wait...

huawei(config)#
    Configuration file had been saved successfully
    Note: The configuration file will take effect after being activated

huawei(config)#
    The data is being saved, please wait a moment...

huawei(config)#
    1 [2010-07-12 14:35:05+08:00]:The percentage of saved data on 6 slot's main
control board is: 21%

huawei(config)#
    1 [2010-07-12 14:35:08+08:00]:The percentage of saved data on 6 slot's main
control board is: 27%

huawei(config)#
    1 [2010-07-12 14:35:11+08:00]:The percentage of saved data on 6 slot's main
control board is: 66%

huawei(config)#
    1 [2010-07-12 14:35:14+08:00]:The percentage of saved data on 6 slot's main
control board is: 72%

huawei(config)#
    1 [2010-07-12 14:35:17+08:00]:The percentage of saved data on 6 slot's main
control board is: 78%

huawei(config)#
    1 [2010-07-12 14:35:20+08:00]:The percentage of saved data on 6 slot's main
control board is: 96%

huawei(config)#
    1 [2010-07-12 14:35:23+08:00]:The percentage of saved data on 6 slot's main
control board is: 98%

huawei(config)#

huawei(config)#
    1 [2010-07-12 14:35:25+08:00]:The data of 6 slot's main control board is saved
completely
```

手动备份数据

配置以手动方式备份系统数据。

前提条件

已经完成对数据的保存，具体操作请参见[手动保存数据](#)。

背景信息

数据的备份包括数据库文件和配置文件的备份，手动备份各操作所对应的命令及功能如[表 1-10](#) 所示。

表 1-10 手动备份数据操作列表

备份操作	命令	功能
手动备份数据库文件	back data	<ul style="list-style-type: none"> ● 将数据库文件手动备份到备份服务器。 ● 备份文件所存放的服务器 IP 必须与 FTP/SFTP/TFTP 工具中设置的服务器 IP 一致，文件名需指定。
手动备份配置文件	backup configuration	<ul style="list-style-type: none"> ● 将配置文件手动备份到备份服务器。 ● 备份文件所存放的服务器 IP 必须与 FTP/SFTP/TFTP 工具中设置的服务器 IP 一致，文件名需指定。

操作步骤

步骤 1 请根据实际需要，选择表 1-10 中的一种备份方式对系统数据进行手动备份操作。

----结束

操作结果

备份完成后，在 FTP 工具中设置的文件存放路径下可以看到备份出来的对应文件。

任务示例

1. 在备份服务器上配置并启动 FTP 工具，具体请参见[配置 FTP 文件传输方式](#)。
2. 任意选择以下一种方式，将数据库文件或配置文件备份到服务器。
 - 使用 FTP 方式手动将系统的数据库文件备份到备份服务器，并指定该服务器的 IP 地址为 10.10.10.1、数据库文件名为 data0.dat。

```

huawei(config)#backup data ftp 10.10.10.1 data0.dat
Please save database file before backup, or the database file that is backed
up may be not the lastest one. Are you sure to continue? (y/n)[n]: y
Load(backup,duplicate,...) begins, please wait and notice the rate of progress
Any operation such as reboot or switchover will cause failure and
unpredictable result
                    
```
 - 使用 FTP 方式手动将系统的配置文件备份到备份服务器，并指定该服务器的 IP 地址为 10.10.10.1、配置文件名为 config0.txt。

```

huawei(config)#backup configuration ftp 10.10.10.1 config0.txt
Please save configuration file before backup, or the configuration file
backedup may be not the lastest. Are you sure to continue? (y/n)[n]: y
Load(backup,duplicate,...) begins, please wait and notice the rate of progress
Any operation such as reboot or switchover will cause failure and
unpredictable result
                    
```

1.5.3 自动保存和备份数据

将数据以自动的方式保存到 Flash memory 或服务器中，防止由于意外重启导致数据丢失。

自动保存数据

当自动保存开关打开时，系统将根据用户设置的某个时间点或时间间隔，周期性检查系统中是否修改了数据信息，如果修改了配置则保存，否则不保存。

背景信息

数据的保存包括数据库文件和配置文件的保存，自动保存各操作所对应的命令及功能如表 1-11 所示。

表 1-11 自动保存数据操作列表

保存操作	命令	功能
设置自动保存的文件类型	autosave type { all configuration data }	<ul style="list-style-type: none">● data: 仅保存数据库文件。● configuration: 仅保存配置文件。● all: 既保存数据库文件又保存配置文件。
定点自动保存数据库文件	autosave time	<ul style="list-style-type: none">● 根据用户设置的某个固定时间点自动保存数据。● 缺省情况下，系统在每天的 00:00:00 自动保存一次。
周期性自动保存数据库文件	autosave interval	<ul style="list-style-type: none">● 根据用户设置的时间间隔自动保存数据。● 缺省情况下，系统每隔 30 分钟自动保存一次。

说明

- 缺省情况下，系统中的周期自动保存开关为关闭状态，即系统不自动保存数据，此时需要用户手动保存数据。
- 当周期自动保存开关打开时，用户仍然可以手动保存数据，具体操作请参见[手动保存数据](#)。



注意

过于频繁的保存对系统有影响，因此建议设置自动保存间隔时间（周期）大于 60 分钟，最好大于或等于一天。

操作步骤

步骤 1 请根据实际需要，选择表 1-11 中的一种保存方式对系统数据进行自动保存操作。

---结束

操作结果

使用 **display autosave configuration** 命令查询得到已经正确配置的定点自动保存时间或周期自动保存时间。

任务示例

1. 配置系统自动保存的数据类型，包括数据库文件和配置文件。

```
Huawei(config)#autosave type  
{ all<K>|configuration<K>|data<K> }:all
```

```
Command:  
autosave type all
```

2. 配置系统中的数据文件每天定点保存或周期保存。

- 设置系统中数据文件在每天 02:00:00 自动保存，并打开系统配置数据的定点自动保存开关。

```
huawei(config)#autosave time 02:00:00  
System autosave time switch: off  
Autosave time: 02:00:00  
Autosave type: data and configuration file
```

```
huawei(config)#autosave time on  
System autosave time switch: on  
Autosave time: 02:00:00  
Autosave type: data and configuration file
```

- 设置系统中数据文件的自动保存时间间隔为 1440 分钟，并打开周期自动保存开关。系统将会每隔 1440 分钟检查配置是否有变更，如果有变更就进行自动保存，反之不保存。



注意

“autosave interval” 开关和 “autosave time” 开关互斥，即两个开关不能同时打开。如果需要在两种配置中切换，需先关闭已经打开的那个开关。

```
huawei(config)#autosave interval 1440  
System autosave interval switch: off  
Autosave interval: 1440 minutes  
Autosave type: data and configuration file
```

```
huawei(config)#autosave interval on  
System autosave interval switch: on  
Autosave interval: 1440 minutes  
Autosave type: data and configuration file
```

```
System autosave modified configuration switch: on  
Autosave interval: 30 minutes  
Autosave type: data and configuration file
```

配置自动备份服务器

配置用于自动备份数据的服务器。

背景信息

- 可以配置主用和备用两个备份服务器确保数据备份的可靠性，也可以仅配置一个主用服务器。
- 当主用服务器失效时，数据将自动备份到备用服务器。

操作步骤

步骤 1 任意选择以下一种方式，数据库文件、配置文件或日志文件所需备份到的服务器的 IP。

- 配置“数据库文件”自动备份到主用服务器（IP 为 10.10.10.1）和备用服务器（IP 为 10.10.10.2），数据传输方式为 ftp。

```
huawei(config)#file-server auto-backup data primary 10.10.10.1 ftp user
  User Name(<=40 chars):123
  User Password(<=40 chars):123 //输入不可见
huawei(config)#file-server auto-backup data secondary 10.10.10.2 ftp user
  User Name(<=40 chars):123
  User Password(<=40 chars):123 //输入不可见
```

- 配置“配置文件”自动备份到主用服务器（IP 为 10.10.10.1）。

```
huawei(config)#file-server auto-backup configuration primary 10.10.10.1 ftp user
  User Name(<=40 chars):123
  User Password(<=40 chars):123 //输入不可见
```

- 配置“日志文件”自动备份到主用服务器（IP 为 10.10.10.1）。

```
huawei(config)#file-server auto-backup log primary 10.10.10.1 ftp user
  User Name(<=40 chars):123
  User Password(<=40 chars):123 //输入不可见
```

---结束

后续处理

- 使用 **display file-server auto-backup data** 命令可以查询到已经正确配置备份服务的 IP 地址。

```
huawei(config)#display file-server auto-backup data
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path      :
-----
```

```
Server type: Secondary
Trans mode : FTP
IP address : 10.10.10.2
User name  : 123
Path      :
```

```
-----
Current Server: Primary server
```

- 使用 **display file-server auto-backup configuration** 命令可以查询到已经正确配置备份服务的 IP 地址。

```
huawei(config)#display file-server auto-backup configuration
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path      :
```

```
-----
Current Server: Primary server
```

- 使用 **display file-server auto-backup log** 命令可以查询到已经正确配置备份服务的 IP 地址。

```
huawei(config)#display file-server auto-backup log
```

```
-----
Server type: Primary
Trans mode : FTP
IP address : 10.10.10.1
User name  : 123
Path       :
-----
```

```
Current Server: Primary server
```

自动备份数据

配置以自动方式备份系统配置数据或者数据库文件。

前提条件

- 已经完成对数据的自动保存配置，具体请参见[自动保存数据](#)。
- 已经完成对备份服务器的配置，具体请参见[配置自动备份服务器](#)。

背景信息

数据的备份包括数据库文件和配置文件的备份，自动备份各操作所对应的命令及功能如表 1-12 所示。

表 1-12 自动备份数据操作列表

备份操作	命令	功能
自动备份数据库文件	auto-backup manual data	将数据库文件立即自动备份到备份服务器。
	<ul style="list-style-type: none"> ● auto-backup period data interval ● auto-backup period data enable 	<ul style="list-style-type: none"> ● 将数据库文件周期性自动备份到备份服务器。 ● 先设置数据库文件自动备份的周期和起始时间，再使能数据库文件自动备份功能。
自动备份配置文件	auto-backup manual configuration	将配置文件立即自动备份到备份服务器。
	<ul style="list-style-type: none"> ● auto-backup period configuration interval ● auto-backup period configuration enable 	<ul style="list-style-type: none"> ● 将配置文件周期性自动备份到备份服务器。 ● 将先设置配置文件自动备份的周期和起始时间，再使能配置文件自动备份功能。
自动备份日志文件	<ul style="list-style-type: none"> ● auto-backup period log interval ● auto-backup period log enable 	先设置日志文件自动备份的周期和起始时间，再使能日志文件自动备份功能。

操作步骤

步骤 1 请根据实际需要，选择表 1-12 中的一种备份方式对系统数据进行自动备份操作。

---结束

操作结果

备份完成后，在 FTP 工具中设置的文件存放路径下可以看到备份出来的对应文件，文件名由系统分配。

任务示例

1. 在备份服务器上配置并启动 FTP 工具，具体请参见配置 FTP 文件传输方式。
2. 任意选择以下一种或几种方式，将数据库文件、配置文件或日志文件备份到服务器。
 - 将系统中的当前数据库文件立即备份至备份服务器。
huawei(config)#auto-backup manual data
 - 手动系统中的当前配置文件立即备份至备份服务器。
huawei(config)#auto-backup manual configuration
 - 配置数据库文件的自动备份周期为 1 天，备份开始时间为 02:30，并使能数据库文件自动备份到备份服务器的功能。
huawei(config)#auto-backup period data interval 1 time 02:30
huawei(config)#auto-backup period data enable
 - 配置文件的自动备份周期为 1 天，备份开始时间为 03:30，并使能配置文件自动备份到备份服务器的功能。
huawei(config)#auto-backup period configuration interval 1 time 03:00
huawei(config)#auto-backup period configuration enable
 - 配置日志文件的自动备份周期为 1 天，备份开始时间为 06:00，并使能配置文件自动备份到备份服务器的功能。
huawei(config)#auto-backup period log interval 1 time 06:00
huawei(config)#auto-backup period log enable



注意

步骤 1 中，备份服务器即 FTP 服务器，即“配置自动备份服务器”中所配置的服务器 IP 地址与“配置数据传输方式”中所配置的服务器 IP 地址必须相同。

2 基础配置

关于本章

基础配置主要包括一些常用配置和公共配置，以及业务配置中的预配置。基础配置之间没有明显的逻辑关系，可以根据实际需要进行配置。

2.1 配置网络时间

配置 NTP 协议，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用（如网络管理系统、网络计费系统）。

2.2 配置系统安全

配置设备系统的网络安全和保护措施，以防止系统受到恶意攻击等威胁。

2.3 配置 ACL

介绍了 AC 设备中 ACL 分类、ACL 规则及其相关配置。

2.4 配置 QoS

介绍了 AC 设备中 QoS（Quality of Service）的相关配置操作。

2.1 配置网络时间

配置 NTP 协议，使网络内所有设备的时钟基本保持一致，从而使设备能够提供基于统一时间的多种应用（如网络管理系统、网络计费系统）。

背景信息

NTP 协议简介：

- NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。它定义了协议实现过程中所使用的结构、算法、实体和协议。
- NTP 是从时间协议（TIME PROTOCOL）和 ICMP 时间戳报文（ICMP TIMESTAMP MESSAGE）演变而来，主要是从准确性和强壮性方面进行了特殊的设计。
- NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。
- 对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

NTP 协议主要应用于需要网络中所有主机或路由器时钟保持一致的场合，比如：

- 在网络管理中，对从不同路由器采集来的日志信息、调试信息进行分析时，需要以时间作为参照依据。
- 计费系统要求所有设备的时钟一致。
- 完成某些功能，如定时重启网络中的所有路由器，要求所有路由器的时钟保持一致。
- 多个系统协同处理同一个比较复杂的事件时，为保证正确的执行顺序，多个系统必须参考同一时钟。
- 在备份服务器和客户机之间进行增量备份时，要求备份服务器和所有客户机之间的时钟同步。

对于网络中的各设备来说，如果依靠管理员手工输入命令来修改系统时钟是不可能的，这不但工作量巨大，而且也不能保证时钟的精确性。但通过配置 NTP，可以很快将网络中设备的时钟同步，同时也能保证很高的精度。

NTP 协议支持四种工作模式：服务器/客户端模式、对等体模式、广播模式和组播模式。AC 设备支持 NTP 协议的全部四种工作模式。

缺省配置

网络时钟的缺省配置如表 2-1 所示。

表 2-1 网络时钟的缺省配置表

参数项	缺省值
身份验证功能	去使能
NTP 验证密钥	无
允许建立的最大 NTP 同步连接数	100

参数项	缺省值
时钟层数	16

2.1.1 （可选）配置 NTP 身份验证功能

配置 NTP 的身份验证功能，以提高网络的安全性，防止未授权的用户对时钟进行修改。

前提条件

在配置 NTP 验证功能之前，需完成 AC 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用验证功能。配置 NTP 验证功能可以分为配置客户端的 NTP 验证和配置服务器端的 NTP 验证两个部分。

注意事项

- 如果客户端没有使能 NTP 验证功能，不论服务器端是否使能 NTP 验证，客户端均可以与服务器端同步。
- 如果使能了 NTP 验证功能，应同时配置可信的密钥。
- 服务器端的配置和客户端的配置应保持一致。
- 在客户端已配置 NTP 验证的情况下，服务器端只要配置了与客户端相同的验证密钥，客户端就能通过验证。此时服务器端不需要使能 NTP 验证功能，也不必声明该密钥是可信的。
- 客户端只会同步到提供可信密钥的服务器，如果服务器提供的密钥不是可信的密钥，那么客户端不会与其同步。
- 配置 NTP 的身份验证功能流程是“开始—使能 NTP 验证功能—配置 NTP 验证密钥—声明可信的密钥—结束”。

操作步骤

步骤 1 使用 `ntp-service authentication enable` 命令使能 NTP-service 身份验证功能。

步骤 2 使用 `ntp-service authentication-keyid` 命令设置 NTP 验证密钥。

步骤 3 使用 `ntp-service reliable authentication-keyid` 命令指定密钥是可信的。

----结束

任务示例

举例：启动 NTP 的身份验证功能，配置验证密钥为 aNiceKey、密钥编号为 42，最后将 42 号密钥配置为可信密钥。

```
huawei(config)#ntp-service authentication enable
huawei(config)#ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
huawei(config)#ntp-service reliable authentication-keyid 42
```

2.1.2 配置 NTP 广播模式

配置 AC 设备采用 NTP 广播模式进行时钟的同步。配置完成后服务器端周期性从指定端口广播时钟同步报文，客户端侦听来自服务器的广播消息包，根据收到的广播消息包对本地时钟进行同步。

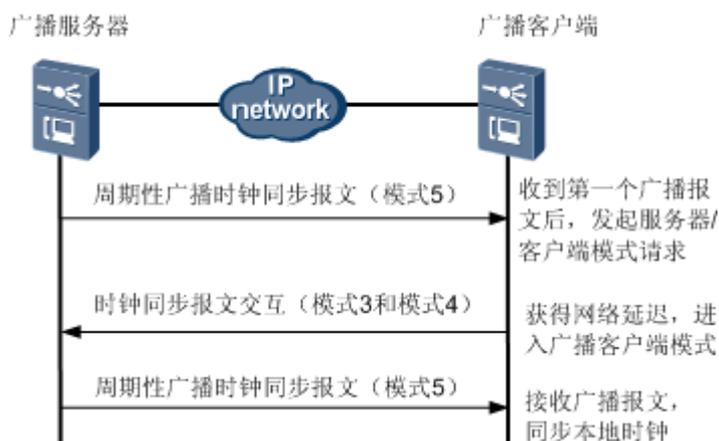
前提条件

在配置 NTP 广播模式之前，需完成 AC 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在广播模式中，服务器端周期性地向广播地址 255.255.255.255 发送时钟同步报文，报文中的 Mode 字段设置为 5（广播模式）。客户端侦听来自服务器的广播报文。当客户端接收到第一个广播报文后，客户端与服务器交互 Mode 字段为 3（客户模式）和 4（服务器模式）的 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入广播客户端模式，继续侦听广播报文的到来，根据到来的广播报文对系统时钟进行同步。如图 2-1 所示。

图 2-1 NTP 广播模式



注意事项

1. 广播模式下，需要同时配置 NTP 服务器端和客户端。
2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

- 配置广播服务器主机。
 1. 使用 **ntp-service refclock-master** 命令设置本地时钟作为 NTP 主时钟，并指定 NTP 主时钟所处的层数。
 2. （可选）配置 NTP 身份验证功能。

建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

- a. 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。
 - b. 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。
 - c. 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。
3. 增加 VLAN 的三层虚接口。
 - a. 使用 **vlan** 命令创建 VLAN。
 - b. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
 - c. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
 - d. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。
 4. 使用 **ntp-service broadcast-server** 命令设置主机的 NTP 广播服务器模式，并指定向广播客户端发送消息时使用的密钥 ID。
- 配置广播客户端主机。
 1. （可选）配置 NTP 身份验证功能。

建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

 - a. 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。
 - b. 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。
 - c. 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。
 2. 增加 VLAN 的三层虚接口。
 - a. 使用 **vlan** 命令创建 VLAN。
 - b. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
 - c. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
 - d. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。
 3. 使用 **ntp-service broadcast-client** 命令设置主机为 NTP 广播客户端。

---结束

任务示例

举例：配置 AC_S 设备以本地时钟作为 NTP 主时钟，时钟层次为 2，采用 NTP 广播模式，通过 VLAN 2 的三层接口 IP 地址 10.10.10.10/24 周期性的以广播方式发送时钟同步报文；AC_C 作为 NTP 客户端，通过 VLAN 2 的三层接口 IP 地址 10.10.10.20/24 侦听来自服务器的广播消息包，并与广播服务器端的时钟进行同步。

1. AC_S 侧配置：

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
```

```
huawei(config-if-vlanif2)#ntp-service broadcast-server  
huawei(config-if-vlanif2)#quit
```

2. AC_C 侧配置:

```
huawei(config)#vlan 2  
huawei(config)#port vlan 2 0/2 24  
huawei(config)#interface vlanif 2  
huawei(config-if-vlanif2)#ip address 10.10.10.20 24  
huawei(config-if-vlanif2)#ntp-service broadcast-client  
huawei(config-if-vlanif2)#quit
```

2.1.3 配置 NTP 组播模式

配置 AC 采用 NTP 组播模式进行时钟的同步。配置完成后服务器端从指定端口周期性组播时钟同步报文，客户端侦听来自服务器的组播消息包，根据收到的组播消息包对本地时钟进行同步。

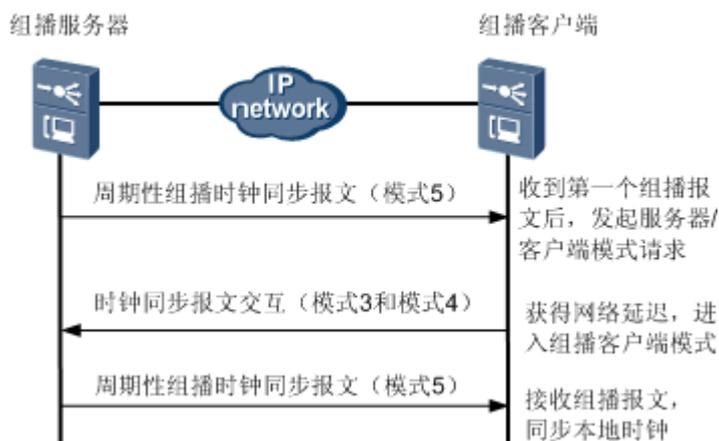
前提条件

在配置 NTP 组播模式之前，需完成 AC 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在组播模式中，服务器端周期性地向用户配置的组播地址（若用户没有配置组播地址，则使用默认的 NTP 组播地址 224.0.1.1）发送时钟同步报文，报文中的 Mode 字段设置为 5（组播模式）。客户端侦听来自服务器的组播报文。当客户端接收到第一个组播报文后，客户端与服务器交互 NTP 报文，以获得客户端与服务器间的网络延迟。之后，客户端就进入组播客户模式，继续侦听组播报文的到来，根据到来的组播报文对系统时钟进行同步。如图 2-2 所示。

图 2-2 NTP 组播模式



注意事项

1. 组播模式下，需要同时配置 NTP 服务器端和客户端。
2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

- 配置组播服务器主机。
 1. 使用 **ntp-service refclock-master** 命令设置本地时钟作为 NTP 主时钟，并指定 NTP 主时钟所处的层次数。
 2. （可选）配置 NTP 身份验证功能。

建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

 - a. 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。
 - b. 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。
 - c. 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。
 3. 增加 VLAN 的三层虚接口。
 - a. 使用 **vlan** 命令创建 VLAN。
 - b. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
 - c. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
 - d. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。
 4. 使用 **ntp-service multicast-server** 命令设置主机的 NTP 组播服务器模式，并指定向组播客户端发送消息时使用的密钥 ID。
- 配置组播客户端主机。
 1. （可选）配置 NTP 身份验证功能。

建议在一些对安全性要求较高的网络中，运行 NTP 协议时启用验证功能。服务器端的配置和客户端的配置应保持一致。

 - a. 使用 **ntp-service authentication enable** 命令使能 NTP-service 身份验证功能。
 - b. 使用 **ntp-service authentication-keyid** 命令设置 NTP 验证密钥。
 - c. 使用 **ntp-service reliable authentication-keyid** 命令指定密钥是可信的。
 2. 增加 VLAN 的三层虚接口。
 - a. 使用 **vlan** 命令创建 VLAN。
 - b. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
 - c. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
 - d. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。
 3. 使用 **ntp-service multicast-client** 命令设置主机为 NTP 组播客户端。

---结束

任务示例

举例：配置 AC_S 设备以本地时钟作为 NTP 主时钟，时钟层次为 2，采用 NTP 组播模式，通过 VLAN 2 的三层接口 IP 地址 10.10.10.10/24 周期性的以组播方式发送时钟同步

报文：AC_C 作为 NTP 客户端，通过 VLAN 2 的三层接口 IP 地址 10.10.10.20/24 侦听来自服务器的组播消息包，并与组播服务器端的时钟进行同步。

1. AC_S 侧配置：

```
huawei(config)#ntp-service refclock-master 2
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#ntp-service multicast-server
huawei(config-if-vlanif2)#quit
```

2. AC_C 侧配置：

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.20 24
huawei(config-if-vlanif2)#ntp-service multicast-client
huawei(config-if-vlanif2)#quit
```

2.1.4 配置 NTP 客户端或服务器模式

配置 AC 作为 NTP 客户端向网络中的 NTP 服务器进行时间同步。

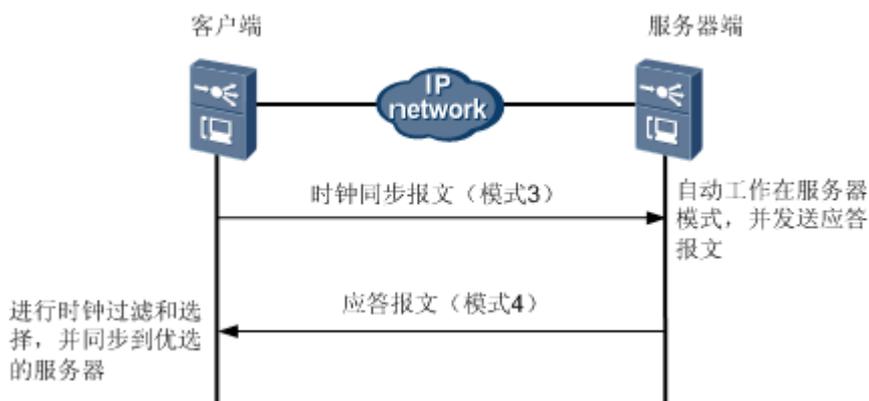
前提条件

在配置 NTP 客户端或服务器模式之前，需完成 AC 设备的网络接口和路由协议的配置，使服务器端和客户端的网络层可达。

背景信息

在客户端/服务器模式中，客户端向服务器发送时钟同步报文，报文中的 Mode 字段设置为 3（客户模式）。服务器端收到报文后会自动工作在服务器模式，并发送应答报文，报文中的 Mode 字段设置为 4（服务器模式）。客户端收到应答报文后，进行时钟过滤和选择，并同步到优选的服务器。如图 2-3 所示。

图 2-3 NTP 客户端/服务器模式



注意事项

1. 当设备采用客户端/服务器模式时，只需在客户端进行配置，服务器端不需进行配置。

2. 同步设备的时钟层数必须小于或等于被同步设备的时钟层数，否则，不能进行时钟同步。

操作步骤

步骤 1 配置 VLAN 的三层虚接口。

1. 使用 **vlan** 命令创建 VLAN。
2. 使用 **port vlan** 命令将上行口加入到 VLAN 中，使带 VLAN 的用户报文通过上行端口上行。
3. 使用 **interface vlanif** 命令从全局配置模式创建 VLAN 接口并进入 VLANIF 模式，以便配置虚拟的三层接口。
4. 使用 **ip address** 命令配置 VLAN 接口 IP 地址和子网掩码，让 VLAN 中的 IP 报文能够参与三层转发。

步骤 2 使用 **ntp-service unicast-server** 命令配置 NTP 单播服务器模式，并指定作为本地时间服务器的远程服务器 IP 地址和本地收发 NTP 消息时的接口。

说明

- 此命令中的 *ip-address* 是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。
- 通过 *source-interface* 参数指定 NTP 报文的源接口后，NTP 报文的源 IP 地址将被设置为指定接口的主 IP 地址。
- 服务器端只有当其时钟被同步后，才能作为时间服务器去同步其他设备。
- 当服务器端的时钟层数大于或等于客户端的时钟层数时，客户端将不会向其同步。
- 可以通过多次执行 **ntp-service unicast-server** 命令配置多个服务器，客户端依据时钟优选来选择最优的时钟源。

步骤 3（可选）配置 ACL 规则。

过滤通过三层接口的报文，只允许来自时钟服务器的 IP 报文访问该三层接口，禁止其它非授权访问。建议在对系统安全性比较高的场合使用 ACL 规则。

1. 使用 **acl adv-acl-numbe** 命令创建告警访问控制列表。
2. 使用 **rule** 命令根据数据包的源地址信息/目的地址信息/IP 承载的协议类型/协议的特性制定流规则，允许或禁止符合条件的数据包通过。
3. 使用 **packet-filter** 命令为指定端口配置 ACL 过滤规则，并使之生效。

----结束

任务示例

举例：配置一台 AC 设备作为 NTP 服务器（IP 地址：10.20.20.20/24），另一台 AC 设备（VLAN 2 的三层接口 IP 地址 10.10.10.10/24，网关：10.10.10.1）作为客户端，客户端通过 VLAN 接口向服务器发送同步时钟请求报文，服务器端响应请求报文进行时钟同步；同时配置 ACL 规则，只允许来自时钟服务器的 IP 报文访问该三层接口。

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.10.10.10 24
huawei(config-if-vlanif2)#quit
huawei(config)#ntp-service unicast-server 10.20.20.20 source-interface vlanif 2
huawei(config)#acl 3010
huawei(config-acl-adv-3010)#rule deny ip source any destination 10.10.10.10 0.0.0.0
huawei(config-acl-adv-3010)#rule permit ip source 10.20.20.20 0.0.0.0 destination 10.10.10.10 0.0.0.0
huawei(config-acl-adv-3010)#quit
huawei(config)#packet-filter inbound ip-group 3010 port 0/2/24
```

2.2 配置系统安全

配置设备系统的网络安全和保护措施，以防止系统受到恶意攻击等威胁。

背景信息

系统安全特性的配置是为了防止来自于网络侧或用户侧的非法报文对设备的攻击，从而保证设备在网络上稳定运行。包括：

- ACL/包过滤防火墙
- 黑名单
- 防 DoS 攻击
- 防 ICMP/IP 攻击
- 源路由过滤
- 源 MAC 地址过滤
- 用户侧环网检测
- 允许/拒绝访问地址段

系统安全相关的缺省配置如表 2-2 所示。

表 2-2 系统安全缺省配置

参数项	缺省值
防火墙黑名单	去使能
防 DoS 攻击	去使能
防 ICMP 攻击	去使能
防 IP 攻击	去使能
源路由过滤	去使能
用户侧环网检测	去使能

2.2.1 配置防火墙

配置系统防火墙可以对访问设备管理接口的报文进行控制，防止未授权的操作用户通过带内或带外方式入侵系统。

背景信息

防火墙包括：

- 黑名单：使用黑名单功能可以将特定 IP 地址发送来的报文屏蔽，其最主要的一个应用特色是可以动态地进行表项的添加或删除。当防火墙根据报文的行为特征察觉到特定 IP 地址的攻击企图之后，即可主动添加黑名单表项，从而将该 IP 地址发送过来的报文过滤掉。

- **ACL 包过滤防火墙：**通过配置 ACL 实施数据包的过滤。当用户需要限制某个端口只可以通过某类型的报文，一般使用 ACL 报文过滤功能来实现。

例如：用户需要一个端口只允许源 IP 为 1.1.1.1 报文在入方向通过，其他报文不能通过。则需要做如下配置：

1. 配置一条 ACL 规则 rule1，允许源 IP 为 1.1.1.1 的报文通过。
2. 配置一条 ACL 规则 rule2，禁止所有报文通过。
3. 使用 **firewall packet-filter** 在 **inbound** 方向，先绑定 rule2，再绑定 rule1。

 说明

在 AC 中，激活 ACL 有两种方式，两种激活方式对于同一 ACL 中的子规则的执行优先级不同：

- 使用 **firewall packet-filter** 命令对 ACL 进行激活，主要用于网管。对于同一 ACL 中的子规则的执行优先级由软件完成，同一 ACL 中的子规则的执行优先级是先配置的优先级高。
- 使用 **packet-filter** 命令对 ACL 进行激活。对于同一 ACL 中的子规则的执行优先级由硬件完成，同一 ACL 中子规则的执行优先级是后配置的优先级高。



注意

为保障设备安全，必须配置防火墙，对访问设备管理接口的报文进行控制。

操作步骤

- 配置防火墙黑名单。

有两种方式：使用 ACL 规则配置防火墙黑名单功能和通过增加不信任报文的源 IP 地址配置防火墙黑名单功能。这两种方式可以二选一，也可以共同作用。

当两种方式共同作用时，防火墙黑名单功能的优先级比 ACL 规则的优先级要高。即系统首先检查防火墙黑名单，再匹配 ACL 规则。

 说明

防火墙黑名单功能只对来自用户侧的报文有效。

- 使用高级 ACL 规则配置防火墙黑名单功能。
 1. 使用 **acl** 命令创建 ACL。使能防火墙黑名单功能同时应用的 ACL 只能是高级 ACL，所以 ACL 的范围为 3000 ~ 3999。
 2. 使用 **rule(adv acl)**命令创建高级 ACL 规则。
 3. 使用 **quit** 命令回退到全局配置模式。
 4. 使用 **firewall blacklist enable acl-number acl-number** 命令使能防火墙黑名单功能。
- 通过增加不信任报文的源 IP 地址配置防火墙黑名单功能。
 1. 使用 **firewall blacklist item** 命令在黑名单中增加不信任报文的源 IP 地址。
 2. 使用 **firewall blacklist enable** 命令使能防火墙黑名单功能。
- 配置防火墙（基于 ACL 进行报文过滤）。
 1. 使用 **acl** 命令创建 ACL。配置防火墙包过滤的 ACL 只能是基本和高级 ACL，所以，ACL 的范围为 2000 ~ 3999。

2. 对于不同的 ACL 需要使用不同的 **rule** 命令创建规则。
 - 基本 ACL 规则：使用 **rule(basic acl)**命令。
 - 高级 ACL 规则：使用 **rule(adv acl)**命令。
3. 使用 **quit** 命令回退到全局配置模式。
4. 使用 **firewall enable** 命令使能防火墙功能。默认去使能。
如果需要基于 ACL 对接口进行报文过滤，需要使能这个功能。
5. 如果是配置 METH 接口的防火墙过滤规则，则使用 **interface meth** 命令进入 MEth 模式；如果是配置 VLANIF 接口的防火墙过滤规则，则使用 **interface vlanif** 命令进入 VLANIF 模式。
6. 使用 **firewall packet-filter** 命令在接口上应用防火墙包过滤规则。

---结束

任务示例

举例：将 IP 地址 192.168.10.18 加入到防火墙黑名单，老化时间为 100 分钟。

```
huawei(config)#firewall blacklist item 192.168.10.18 timeout 100
huawei(config)#firewall blacklist enable
```

举例：将 10.10.10.0 网段的 IP 地址加入防火墙黑名单，绑定 ACL 3000。

```
huawei(config)#acl 3000
huawei(config-acl-adv-3000)#rule deny ip source 10.10.10.0 0.0.0.255 destination
10.10.10.20 0
huawei(config-acl-adv-3000)#quit
huawei(config)#firewall blacklist enable acl-number 3000
```

举例：防止 172.16.25.0 网段的用户访问 IP 地址为 172.16.25.28 的 AC 设备的维护网口。

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)#rule 5 deny icmp source 172.16.25.0 0.0.0.255 destination
172.16.25.28 0
huawei(config-acl-adv-3001)#quit
huawei(config)#firewall enable
huawei(config)#interface meth 0
huawei(config-if-meth0)#firewall packet-filter 3001 inbound
ACL applied successfully
```

2.2.2 配置防对系统的恶意攻击

通过使能防 DoS、ICMP/IP 攻击，以及增加源路由和 MAC 地址过滤等配置，防止恶意用户对系统的攻击，提高系统的安全性。

背景信息

防止恶意用户对系统的攻击有以下几种措施，根据实际需求进行配置。

- 防 DoS 攻击：对用户发送的控制报文进行限制性接收的防御攻击。
- 防 ICMP 攻击：系统丢弃从用户侧发给设备本身的 ICMP 报文，防止用户侧 Ping 设备的三层接口地址。
- 防 IP 攻击：系统丢弃从用户侧发给设备本身的 IP 报文。
- 源路由过滤：把用户发送的 IP 报文中含有路由选项字段的报文过滤掉。

操作步骤

- 配置防御 DoS 攻击。

使用 **security anti-dos enable** 命令使能全局防御 DoS 攻击功能。

使能全局防 DoS 攻击后，系统收到攻击报文，会把用户端口加入黑名单。去使能 DoS 攻击后，系统将删除黑名单。

应用场景：两台 AP（AP1 和 AP2）通过 AC 接入网络，如果其中非法 AP（AP1）发送大量协议控制报文，冲击系统 CPU，则会导致设备 CPU 占有率过高，而不能正常处理同设备下其它 AP（如 AP2）的业务。要实现防 DoS 攻击，把攻击端口屏蔽或抑制其协议报文的发送，使设备免受攻击。

- 配置源路由过滤。

使用 **security source-route enable** 命令使能源路由过滤功能。主要用于过滤上报到三层的带有路由信息的报文。

应用场景：路由通常是动态的，应用程序并不对选路进行控制。通过源路由发送者可以通过在 IP 报文中加入路由信息，从而进行选路，这时，报文将按照发送者的意图，走网络中的一条特定的路由。为了防止以上情况出现，需要配置源路由过滤，AC 将对 IP 报文进行合法性检查，将匹配的源路由选项的报文丢弃。

---结束

任务示例

举例：使能系统全局防御 DoS 攻击功能。

```
huawei(config)#security anti-dos enable
```

2.2.3 配置防非法用户登录

只有配置的允许访问设备的地址段才能访问设备，配置的拒绝访问设备的地址段不能访问设备，以防止非法 IP 地址段的用户登录系统，维护系统的安全。

背景信息

每种防火墙允许添加 10 条地址段信息。

增加一个地址段时，不允许首地址和已有的首地址重复。

删除一个地址段时，只需要输入此地址段的首地址。

操作步骤

- 配置防非法用户 Telnet 登录设备。

1. 使用 **sysman ip-access telnet** 命令配置允许通过 Telnet 协议访问设备的 IP 地址段。



注意

为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。

2. 使用 **sysman ip-refuse telnet** 命令配置拒绝 Telnet 访问设备的 IP 地址段。



说明

允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。

3. 使用 **sysman firewall telnet enable** 命令使能 Telnet 协议的防火墙功能。系统缺省防火墙处于去使能状态。
- 配置防非法用户通过 SSH 方式登录设备。
 1. 使用 **sysman ip-access ssh** 命令配置允许通过 SSH 方式访问设备的 IP 地址段。



注意

为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。

2. 使用 **sysman ip-refuse ssh** 命令配置拒绝通过 SSH 方式访问设备的 IP 地址段。



说明

允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。

3. 使用 **sysman firewall ssh enable** 命令使能 SSH 协议的防火墙功能。系统缺省防火墙处于去使能状态。
- 配置防非法用户通过 SNMP 方式（网管）登录设备。
 1. 使用 **sysman ip-access snmp** 命令配置允许通过 SNMP 方式访问设备的 IP 地址段。



注意

为了保障设备安全，必须遵循最小授权原则，配置允许访问的地址段，且仅在其中增加必要的管理网段 IP 地址，其余 IP 地址不允许访问设备管理接口。

2. 使用 **sysman ip-refuse snmp** 命令配置拒绝通过 SNMP 方式访问设备的 IP 地址段。



说明

允许访问的地址段和拒绝访问的地址段最好不重复，只有在允许访问地址段且不在拒绝访问地址段的 IP 地址才能访问设备。

3. 使用 **sysman firewall snmp enable** 命令使能 SNMP 协议的防火墙功能。系统缺省防火墙处于去使能状态。

---结束

任务示例

举例：使能系统的 Telnet 协议防火墙，只允许 134.140.5.1 ~ 134.140.5.254 地址段的用户 Telnet 登录设备。

```
huawei(config)#sysman ip-access telnet 134.140.5.1 134.140.5.254
huawei(config)#sysman firewall telnet enable
```

举例：使能系统的 SSH 协议防火墙，只允许 133.7.22.1 ~ 133.7.22.254 地址段的用户通过 SSH 方式登录设备。

```
huawei(config)#sysman ip-access ssh 133.7.22.1 133.7.22.254
huawei(config)#sysman firewall ssh enable
```

举例：使能系统的 SNMP 协议防火墙，拒绝 10.10.20.1 ~ 10.10.20.254 地址段的用户通过网管登录设备。

```
huawei(config)#sysman ip-refuse snmp 10.10.20.1 10.10.20.254
huawei(config)#sysman firewall snmp enable
```

2.3 配置 ACL

介绍了 AC 设备中 ACL 分类、ACL 规则及其相关配置。

背景信息

ACL（Access Control List），即访问控制列表，通过配置的一系列匹配规则对特定的数据包进行过滤，从而识别需要过滤的对象。在识别出特定的对象之后，根据预先设定的策略允许或禁止相应的数据包通过。ACL 过滤报文流过程是在为进行 QoS 或用户安全的配置做准备。

ACL 分类如表 2-3 所示。

表 2-3 ACL 分类列表

类别	取值范围	特点
基本 ACL	2000 ~ 2999	只能根据三层源 IP 制定规则，对数据包进行相应的分析处理。
高级 ACL	3000 ~ 3999	可以根据数据包的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、针对协议的特性（例如 TCP 的源端口、目的端口、ICMP 消息的类型）等内容制定规则。 利用高级 ACL 制定比基本 ACL 更准确、更丰富、更灵活的规则。
链路层 ACL	4000 ~ 4999	可以根据源 MAC 地址、VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定规则，对数据进行相应处理。
用户自定义 ACL	5000 ~ 5999	可以根据二层数据帧的前 80 个字节中的任意 32 字节进行匹配，对数据报文作出相应的处理。

当一条报文流到达，与两条以上的流规则相匹配，系统匹配顺序如下：

- 同一条 ACL 内的子规则，如果同时激活，默认先配置的规则较后配置的规则具有更高的执行优先级。
- 同一条 ACL 内的子规则，如果是逐条单独激活，则后激活的规则较先激活的规则具有更高的执行优先级。
- 不同的 ACL 间下发的子规则，后激活的子规则较先激活的子规则具有更高的执行优先级。

注意事项

由于 ACL 在使用上灵活多变，所以在配置上给出以下建议：

- 建议在任何一条 ACL 的子规则里，首先定义一条普遍适用的规则，例如 `permit any` 或者 `deny any`，使任何报文都有一条流规则与之匹配，就能确认没有特别标识的报文默认是转发还是过滤。
- 激活后的 ACL 规则会占用到硬件资源，与协议模块（例如 DHCP，IPoA 等）功能共享硬件资源，同时这部分硬件资源较为有限，因此不可避免存在资源不足的情况。为了避免因为 ACL 占用相关硬件资源，而造成其他业务功能启动失败的情况，建议用户在配置数据时先启动协议模块，然后再激活 ACL。出现启动某个协议模块失败的情况，处理思路如下：
 1. 首先考虑是否是因为 ACL 占用资源过多而导致启动失败。
 2. 如果确认是 ACL 问题，可以去激活或者删除一部分不重要，或者暂时不使用的 ACL 配置后，再来进行协议模块的配置和启用。

2.3.1 配置基本 ACL

配置基本 ACL 适用于当设备需要根据源 IP 地址对数据包进行流分类的场景。

背景信息

基本 ACL 的编号取值范围为：2000 ~ 2999。

基本 ACL 只能根据三层源 IP 制定规则，对数据包进行相应的分析处理。

操作步骤

步骤 1（可选）设置时间段。

使用 `time-range` 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建基本 ACL。

使用 `acl` 创建基本 ACL 并且进入该 ACL 模式。ACL 序号的取值只能在 2000 到 2999 之间。

步骤 3 配置基本 ACL 子规则。

在 `acl-basic` 模式下，使用 `rule` 命令创建基本 ACL 子规则，主要参数：

- `rule-id`：ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- `permit`：允许符合条件的数据包通过的关键字。
- `deny`：丢弃符合条件的数据包的关键字。
- `time-range`：该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 **packet-filter** 命令激活 ACL。
- 使用 **firewall packet-filter** 命令激活 ACL，详细配置过程请参考[配置防火墙](#)。
- 执行 QoS 操作，请参考[配置基于 ACL 的流量管理](#)。

----结束

任务示例

举例：每周五的 00:00 到 12:00，AC 的 0/2/0 端口只能接收来自 2.2.2.2 的数据包，其他数据包将被丢弃。

```
huawei(config)#time-range time1 00:00 to 12:00 fri
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule permit source 2.2.2.2 0.0.0.0 time-range time1
huawei(config-acl-basic-2000)#rule deny time-range time1
huawei(config-acl-basic-2000)#quit
huawei(config)#packet-filter inbound ip-group 2000 port 0/2/0
huawei(config)#save
```

2.3.2 配置高级 ACL

当设备需要根据数据包的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性（例如 TCP 的源端口、目的端口、ICMP 消息的类型）对数据包进行流分类时用本任务。

背景信息

高级 ACL 的编号取值范围为：3000 ~ 3999。

高级 ACL 支持根据以下信息对报文进行流分类：

- 协议类型
- 源 IP 地址
- 目的 IP 地址
- 源端口号（UDP 或者 TCP 报文的源端口）
- 目的端口号（UDP 或者 TCP 报文的目的端口）
- ICMP 报文的类型
- precedence 值：数据包的优先级字段
- ToS（Type of Service）值：数据包的服务类型字段
- DSCP（Diff-Serv Code Point）值：数据包的差分服务编码点

操作步骤

步骤 1（可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建高级 ACL。

使用 **acl** 创建高级 ACL 并且进入 **acl-adv** 模式，ACL 序号的取值只能在 3000 到 3999 之间。

步骤 3 配置高级 ACL 规则。

在 `acl-adv` 模式下，使用 `rule` 创建 ACL 规则，主要参数：

- **rule-id**: ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**: 允许符合条件的数据包通过的关键字。
- **deny**: 丢弃符合条件的数据包的关键字。
- **time-range**: 该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 `packet-filter` 命令激活 ACL。
- 使用 `firewall packet-filter` 命令激活 ACL，详细配置过程请参考[配置防火墙](#)。
- 执行 QoS 操作，请参考[配置基于 ACL 的流量管理](#)。

---结束

任务示例

举例一：AC 设备上设置一个 VLAN，该 VLAN 具有三层 IP 地址（10.10.10.101）。现在不允许从用户侧发起对设备上 VLAN 接口的 ICMP 操作（如 ping 操作）和 telnet 操作。

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)rule 1 deny icmp destination 10.10.10.101 0
huawei(config-acl-adv-3001)rule 2 deny tcp destination 10.10.10.101 0 destination-port eq telnet
huawei(config-acl-adv-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/0
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/0
huawei(config)#save
```

举例二：AC 设备上设置一个 VLAN，该 VLAN 具有三层 IP 地址（10.10.10.101），AC 的 20 号端口连接了一个 AP，AP 地址为 10.10.10.20，AP 下连接的用户 IP 网段为 192.168.1.0/24。

通过限定可以访问 AC 系统的 IP 网段范围，提高系统的安全性。如下举例中，限定仅 AP 和指定网段终端可访问 AC 系统。

```
huawei(config)#acl 3001
huawei(config-acl-adv-3001)rule 1 deny ip destination 10.10.10.101 0
huawei(config-acl-adv-3001)rule 2 permit ip source 10.10.10.20 0 destination 10.10.10.101 0
huawei(config-acl-adv-3001)rule 3 permit ip source 192.168.1.0 0.0.0.255 destination 10.10.10.101 0
huawei(config-acl-adv-3001)quit
huawei(config)#packet-filter inbound ip-group 3001 rule 1 port 0/2/20
huawei(config)#packet-filter inbound ip-group 3001 rule 2 port 0/2/20
huawei(config)#packet-filter inbound ip-group 3001 rule 3 port 0/2/20
```

2.3.3 配置链路层 ACL

当设备需要根据源 MAC 地址、VLAN ID、二层协议类型、目的 MAC 地址等链路层信息进行流分类时使用。

背景信息

链路层 ACL 的编号取值范围为：4000 ~ 4999。

链路层 ACL 支持根据以下链路层的信息进行分类：

- 以太网承载的协议类型
- 802.1p 优先级
- VLAN ID 信息
- 源 MAC 地址
- 目的 MAC 地址

操作步骤

步骤 1（可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建链路层 ACL。

使用 **acl** 创建链路层 ACL 并且进入 **acl-link** 模式。ACL 序号的取值只能在 4000 到 4999 之间。

步骤 3 配置链路层 ACL 规则。

在 **acl-link** 模式下，使用 **rule** 命令创建链路层 ACL 规则，主要参数：

- **rule-id**: ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**: 允许符合条件的数据包通过的关键字。
- **deny**: 丢弃符合条件的数据包的关键字。
- **time-range**: 该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

- 使用 **packet-filter** 命令激活 ACL。
- 执行 QoS 操作，请参考[配置基于 ACL 的流量管理](#)。

----结束

任务示例

举例：创建一条允许源 MAC 地址为 2222-2222-2222、目的 MAC 地址为 00e0-fc11-4141、VLAN ID 为 12、COS 值为 1、类型为 0x8863（pppoe-control 消息）的数据包通过的规则。

```
huawei(config)#acl 4001
huawei(config-acl-link-4001)rule 1 permit type 0x8863 cos 1 source 12
2222-2222-2222 0000-0000-0000 destination 00e0-fc11-4141 0000-0000-0000
huawei(config-acl-basic-4001)quit
huawei(config)#save
```

2.3.4 配置用户自定义 ACL

当设备需要根据二层数据帧的前 80 个字节中的任意 32 字节制定流分类规则时使用。

前提条件

配置用户自定义 ACL 需要用户对二层数据帧的构成有深入的了解，在配置前根据二层数据帧的格式做好规划。

背景信息

用户自定义 ACL 的编号取值范围为：5000 ~ 5999。

用户自定义 ACL 访问控制列表可以根据数据帧的前 80 个字节中的任意 32 字节制定 ACL 规则。

图 2-4 数据帧的前 64 个字节示意图

```

AA AA AA AA AA AA BB BB BB BB BB BB CC CC CC CC
DD DD EE FF GG GG HH HH II II JJ KK LL LL MM MM
MM MM NN NN NN NN OO OO PP PP QQ QQ QQ QQ RR RR
RR RR SS TT UU UU VV VV VV VV VV VV VV VV VV VV
    
```

各个字母的含义及偏移量取值如表 2-4 所示。

表 2-4 字母与其含义对照列表

字母	含义	偏移量	字母	含义	偏移量
A	目的 MAC 地址	0	L	IP 校验和	28
B	源 MAC 地址	6	M	源 IP 地址	30
C	VLAN tag 字段	12	N	目的 IP 地址	34
D	协议类型	16	O	TCP 源端口	38
E	IP 版本号	18	P	TCP 目的端口	40
F	TOS 字段	19	Q	序列号	42
G	IP 包的长度	20	R	确认字段	46
H	ID 号	22	S	IP 头长度和保留比特位	50
I	Flags 字段	24	T	保留比特位和 flags 比特位	51
J	TTL 字段	26	U	Window Size 字段	52
K	协议号（6 代表 TCP，17 代表 UDP）	27	V	其他	54

说明

各个字段的偏移量是它们在 ETH II + VLAN tag 数据帧中的偏移量。在用户自定义 ACL 中，用户可以使用规则掩码和偏移量两个参数共同从数据帧中提取前 80 个字节中的任意字节，然后用用户定义的规则比较，从而过滤出匹配的数据帧，作相应的处理。

操作步骤

步骤 1（可选）设置时间段。

使用 **time-range** 创建生效时间段，可以在创建 ACL 规则时引用。

步骤 2 创建用户自定义 ACL。

使用 **acl** 创建用户自定义 ACL 并且进入 **acl-user** 模式。ACL 序号的取值只能在 5000 到 5999 之间。

步骤 3 配置用户自定义 ACL 规则。

在 **acl-user** 模式下，使用 **rule** 创建 ACL 规则，主要参数：

- **rule-id**: ACL 规则 ID，当需要创建指定 ID 号的 ACL 规则时使用此参数。
- **permit**: 允许符合条件的数据包通过的关键字。
- **deny**: 丢弃符合条件的数据包的关键字。
- **rule-string**: 用户自定义的规则字符串，为十六进制数，且字符个数必须是偶数。
- **rule-mask**: 用户自定义的规则掩码，为正掩码，用于和数据包作“与”操作，提取数据包的信息。
- **offset**: 偏移量，以数据包的头部为基准，指定从第几个字节开始进行“与”操作。与规则掩码共同作用，从报文提取出任意一段字符串。
- **time-range**: 该 ACL 规则生效时间段的关键字。

步骤 4 激活 ACL。

ACL 配置完成后，只是生成了 ACL 控制列表，并不能实际生效，还需要配合其他命令激活 ACL 才能够生效。比较常见的如：

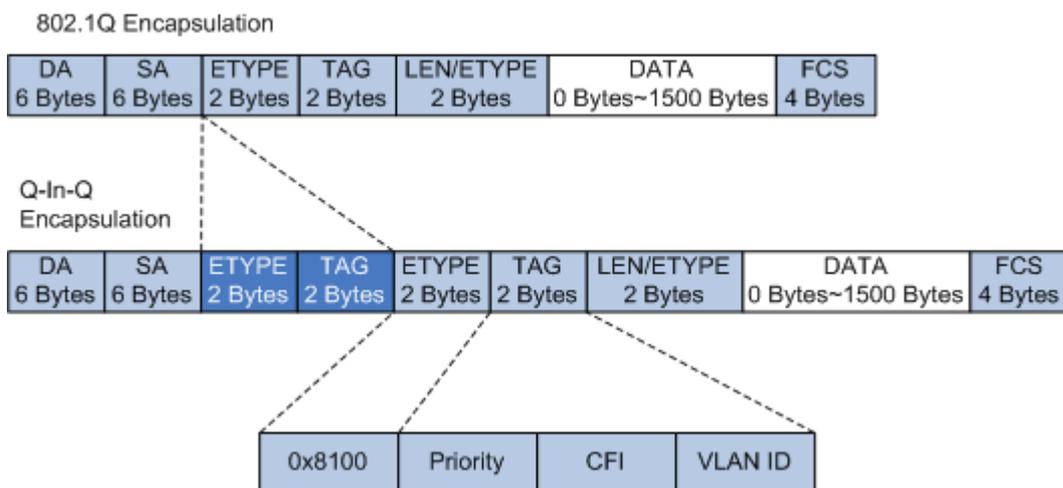
- 使用 **packet-filter** 命令激活 ACL。
- 执行 QoS 操作，请参考[配置基于 ACL 的流量管理](#)。

----结束

任务示例

举例：从 0/2/0 端口送到 AC 的报文为携带两层 VLAN tag 的 QinQ 报文，现在要求将外层 VLAN(其内层 VLAN ID 为 10)的 cos 优先级修改为 5。

图 2-5 QinQ 报文格式



```
huawei(config)#acl 5001
huawei(config-acl-user-5001)#rule 1 permit 8100 ffff 16
```



说明

QinQ 报文的类型值，不同的厂家有不同的设置，华为公司采用默认的 0x8100。如图 2-5 所示，该类型值的偏移量应该是 16 个字节。

```
huawei(config-acl-user-5001)#rule 10 permit 0a ff 19
```



说明

19 是指以数据包的头部为基准，偏移 19 个字节进行“与”操作。0a 是指 QinQ 报文中内层 TAG 字段的取值。在本例中，内层 TAG 字段中第 2 个字节是 VLAN ID 的一部分，正好是内层 VLAN ID 的值（VLAN 10）。

```
huawei(config-acl-user-5001)#quit
```

```
huawei(config)#traffic-priority inbound user-group 5001 cos 5 port 0/2/0
```

2.4 配置 QoS

介绍了 AC 设备中 QoS（Quality of Service）的相关配置操作。

背景信息

QoS 是通过系统的配置，实现为不同的业务提供不同的服务质量。对于 QoS 来说，没有统一的业务模型，所以需要事先做好全网业务的 QoS 规划，然后制定配置方案。

在 AC 系统中，QoS 实现的关键点主要是以下内容：

- 流量管理
通过流量管理的配置，可以实现对用户业务或者针对端口的流量限速。
- 队列调度
对于已经执行流量管理的业务报文来说，通过队列调度的配置，可以将业务报文置于不同的优先级队列中，实现系统内的 QoS 保证。

除以上关键点之外，AC 还支持 HQoS（Hierarchical Quality of Service，层次化 QoS）、基于 ACL 的流量管理。

- HQoS
支持对 HQoS 用户、HQoS 用户组两层的流量管理。
- 基于 ACL 的流量管理
对于用户有灵活需求来实现业务流的 QoS 保障的场景，可以通过 ACL 实现灵活的流分类（请参考“[配置 ACL](#)”），然后再对流进行 QoS 动作。

2.4.1 配置流量管理

介绍在 AC 上配置流量管理的方法。

概述

AC 支持对进入系统或者送出系统的业务流量进行流量管理。支持基于端口+VLAN 实施流量管理。

此外，AC 可以针对以太网端口进行限速、可以针对进入系统的广播报文及未知报文（多播、单播）进行流量抑制。

配置以太网端口限速

通过本任务对指定的以太网端口进行上行流量限制。

前提条件

- 以太网端口限速仅对以太网端口生效。
- 超过指定速率的流量将被丢弃。

操作步骤

步骤 1 在全局配置模式下，使用 **line-rate** 命令配置对指定的以太网端口进行上行流量限制。
主要配置参数如下：

- **target-rate**：限制端口的速率，单位为 Kbps。
- **port**：取值为机框号/槽位号/端口号。

步骤 2 使用 **display qos-info line-rate port** 命令查询以太网端口流量限制配置值。

----结束

任务示例

举例：设置以太网端口 0/2/0 限速为 6400kbit/s。

```
huawei(config)#line-rate 6400 port 0/2/0
huawei(config)#display qos-info line-rate port 0/2/0

line-rate:
port 0/2/0:
    Line rate: 6400 Kbps
```

配置流量抑制

配置流量抑制的目的在于抑制系统收到的广播、未知组播、未知单播报文，以保证系统用户的正常业务开展。

背景信息

配置流量抑制即可以针对单板进行，也可以针对单板的端口进行。

操作步骤

步骤 1 使用 **interface scu** 进入 SCU 模式。

步骤 2 查询流量抑制的阈值信息。

使用 **display traffic-suppress all** 查询流量抑制的阈值信息。

步骤 3 使用命令 **traffic-suppress** 针对 SCU 单板的端口配置流量抑制。

主要参数：

- **broadcast**：设置为广播流量抑制。
- **multicast**：设置为未知多播流量抑制。
- **unicast**：设置为未知单播流量抑制。
- **value**：抑制流量等级的索引。此索引值为步骤 2 中查询到的值。

----结束

任务示例

举例：配置 SCU 单板 0 端口，对广播报文按照抑制流量等级 8 进行流量控制。

```
huawei(config)#interface scu 0/2
huawei(config-if-scu-0/2)#display traffic-suppress all
```

Command:
display traffic-suppress all
Traffic suppression ID definition:

NO.	Min bandwidth(kbps)	Max bandwidth(kbps)	Package number(pps)
1	6	145	12
2	12	291	24
3	24	582	48
4	48	1153	95
5	97	2319	191
6	195	4639	382
7	390	9265	763
8	781	18531	1526
9	1562	37063	3052
10	3125	74126	6104
11	6249	148241	12207
12	12499	296483	24414
13	0	0	0

PortID	Broadcast_index	Multicast_index	Unicast_index
0	7	7	OFF
1	7	7	OFF
2	7	7	OFF
3	7	7	OFF

```
huawei(config-if-scu-0/2)#traffic-suppress all broadcast value 8
huawei(config-if-scu-0/2)#display traffic-suppress 0
```

Traffic suppression ID definition:

NO.	Min bandwidth(kbps)	Max bandwidth(kbps)	Package number(pps)
1	6	145	12
2	12	291	24
3	24	582	48
4	48	1153	95
5	97	2319	191
6	195	4639	382
7	390	9265	763
8	781	18531	1526
9	1562	37063	3052
10	3125	74126	6104
11	6249	148241	12207
12	12499	296483	24414
13	0	0	0

```
Current traffic suppression index of broadcast      : 8
Current traffic suppression index of multicast     : 7
Current traffic suppression index of unknown unicast : 7
```

2.4.2 配置队列调度

队列是在物理端口内进行报文调度的单位。配置队列调度可以在出现网络拥塞时保证关键业务的报文得到及时处理。

背景信息

对于 AC 系统来讲，其上下行方向上都有可能发生拥塞，需要配置保证关键业务报文的处理，AC 支持 PQ、WRR 两种调度方式。

配置队列调度模式

通过本任务配置队列调度方式，确保在发生阻塞时高优先级队列中的报文得到及时处理。

背景信息

AC 支持三种队列调度模式：严格优先级调度 PQ（Strict-Priority Queue）、加权轮循调度 WRR（Weighted Round Robin）和 PQ+WRR 调度。

- 严格优先级调度 PQ
严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。
缺省情况下系统采用严格优先级调度 PQ 方式。
- 加权轮循调度 WRR
系统支持 8 个优先级队列的加权轮循调度，每个队列有一个加权值（由高到低依次为 w7、w6、w5、w4、w3、w2、w1、w0）。加权值表示获取资源的比重。加权轮循队列调度是在队列之间轮流调度，保证每个队列都得到一定的服务时间。
队列权重与实际队列的对应关系如表 2-5 所示。

表 2-5 队列权重与实际队列的对应关系表

队列号	配置权重	实际队列权重（支持 8 个队列的端口）	实际队列权重（支持 4 个队列的端口）
7	W7	W7	-
6	W6	W6	-
5	W5	W5	-
4	W4	W4	-
3	W3	W3	W7+W6
2	W2	W2	W5+W4
1	W1	W1	W3+W2
0	W0	W0	W1+W0

Wn：表示队列 n 的权重。各队列权重之和必须等于 0 或者 100（队列权重为 255 的除外）。

- PQ+WRR 混合调度
 - 系统支持部分队列进行 PQ 调度，部分队列进行 WRR 调度。当指定 WRR 值为 0 时表示该队列进行 PQ 调度。

- 进行 PQ 调度的队列应是高优先级的队列。
- 参与轮询调度的各队列权重之和必须等于 100。

操作步骤

步骤 1 使用 `queue-scheduler` 命令配置队列调度方式。

步骤 2 使用 `display queue-scheduler` 命令查询队列调度方式配置信息。

---结束

任务示例

举例：设置队列调度方式为加权轮循调度，8 个队列的权重分别为 10、10、20、20、10、10、10、10。

```
huawei(config)#queue-scheduler wrr 10 10 20 20 10 10 10 10
huawei(config)#display queue-scheduler
Queue scheduler mode : WRR
-----
Queue  Scheduler Mode  WRR Weight
-----
0      WRR                    10
1      WRR                    10
2      WRR                    20
3      WRR                    20
4      WRR                    10
5      WRR                    10
6      WRR                    10
7      WRR                    10
-----
```

举例：设置队列调度模式为 PQ+WRR 调度，6 个 WRR 调度的队列的权值分别为 20、20、10、30、10、10。

```
huawei(config)#queue-scheduler wrr 20 20 10 30 10 10 0 0
huawei(config)#display queue-scheduler
Queue scheduler mode : WRR
-----
Queue  Scheduler Mode  WRR Weight
-----
0      WRR                    20
1      WRR                    20
2      WRR                    10
3      WRR                    30
4      WRR                    10
5      WRR                    10
6      PQ                    --
7      PQ                    --
-----
```

配置队列与 802.1p 优先级的映射关系

配置队列与 802.1p 优先级的映射关系，使系统能根据配置的映射关系将不同优先级的报文分配到指定的队列中。此配置增强了向队列分配报文的灵活性。

背景信息

- 此配置为系统级配置，对所有业务板有效。
- 缺省情况下，队列与 802.1p 优先级的映射关系如表 2-6 所示。

表 2-6 队列与 802.1p 优先级的映射关系表

队列号	实际队列号（支持 8 个队列的端口）	实际队列号（支持 4 个队列的端口）	802.1p 优先级
7	7	3	7
6	6	3	6
5	5	2	5
4	4	2	4
3	3	1	3
2	2	1	2
1	1	0	1
0	0	0	0

操作步骤

步骤 1 使用 `cos-queue-map` 命令配置 802.1p 优先级与队列的映射关系。

步骤 2 使用 `display cos-queue-map` 命令查询 802.1p 优先级与队列映射关系。

----结束

任务示例

举例：配置 802.1p 优先级 0 映射到队列 0，802.1p 优先级 1 映射到队列 2，其它优先级全部映射到队列 6。

```
huawei(config)#cos-queue-map cos0 0 cos1 2 cos2 6 cos3 6 cos4 6 cos5 6 cos6 6 cos7 6
huawei(config)#display cos-queue-map
```

CoS and queue map:

```
-----
CoS          Queue ID
-----
0            0
1            2
2            6
3            6
4            6
5            6
6            6
7            6
-----
```

2.4.3 配置基于 ACL 规则的流量管理

通过配置 ACL 可以根据用户的需求灵活地实现流分类，当这种基于 ACL 的流分类动作完成后，可以针对这些业务流进行 QoS 动作。

配置对匹配 ACL 规则的流量进行限制

通过本任务对通过指定端口匹配 ACL 规则的流量进行限制，并对超过限制的流量进行相应处理。如打上 DSCP 标记或直接丢弃。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要限制流量的端口正常工作。

背景信息

- 仅对访问控制列表中动作为 permit 的规则有效。
- 所限制的速率必须是 64 的整数倍。

操作步骤

- 步骤 1** 使用 **traffic-limit** 命令对通过指定端口匹配 ACL 规则的流量进行限制。
使用该命令可以设定当端口接收流量超过限制值时所采取的动作，有两种选择：
- **drop**: 丢弃。
 - **remark-dscp value**: 当需要对超过限制的流量设置 DSCP 优先级时，输入此参数。
- 步骤 2** 使用 **display qos-info traffic-limit port** 命令查询指定端口的流量控制信息。
- 结束

任务示例

举例：对端口 0/2/0 接收到的匹配 ACL 2001 的流规则的报文流进行限速（限速为 512Kbit/s）。当流量超过设定流量时，将超过部分的报文打上 DSCP 优先级（af1）。

```
huawei(config)#traffic-limit inbound ip-group 2001 512 exceed remark-dscp af1 port
0/2/0 //af1代表着dscp的一种类型: Assured Forwarding 1服务(10)
huawei(config)#display qos-info traffic-limit port 0/2/0
traffic-limit:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5    running
    Target rate: 512 Kbps
    Exceed action: remark-dscp af1
```

配置对匹配 ACL 规则的流量标记优先级

通过本任务对通过指定端口匹配 ACL 规则的流量标记优先级，使该流量能得到与指定优先级相匹配的服务。可标记的优先级类型有 ToS、DSCP、802.1p。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要标记优先级的端口正常工作。

背景信息

- 仅对访问列表中动作为 permit 的规则有效。
- ToS 优先级和 DSCP 优先级互斥，不能同时配置。

操作步骤

步骤 1 使用 **traffic-priority** 命令对通过指定端口匹配 ACL 规则的流量标记优先级。

步骤 2 使用 **display qos-info traffic-priority port** 查询设置的优先级。

----结束

任务示例

举例：将端口 0/2/0 接收到的匹配 ACL 规则 2001 的流量标记优先级。其中 DSCP 优先级为 10（af1），本地优先级为 0。

```
huawei(config)#traffic-priority inbound ip-group 2001 dscp af1 local-precedence 0
port 0/2/0
huawei(config)#display qos-info traffic-priority port 0/2/0
traffic-priority:
port 0/2/0:
Inbound:
  Matches: Acl 2001 rule 5 running
  Priority action: dscp af1 local-precedence 0
```

配置对匹配 ACL 规则的流量进行统计

通过本任务对匹配 ACL 规则的流量进行统计，以便对该流量进行分析、监控。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要流量统计的端口正常工作。

背景信息

仅对访问列表中动作为 permit 的规则有效。

操作步骤

步骤 1 使用 **traffic-statistic** 命令对通过指定端口匹配 ACL 规则的流量进行统计。

步骤 2 使用 **display qos-info traffic-statistic port** 查询通过指定端口匹配 ACL 规则的流量统计信息。

----结束

任务示例

举例：对端口 0/2/0 接收到的匹配 ACL 2001 规则的流量进行统计。

```
huawei(config)#traffic-statistic inbound ip-group 2001 port 0/2/0
huawei(config)#display qos-info traffic-statistic port 0/2/0
traffic-statistic:
port 0/2/0:
Inbound:
  Matches: Acl 2001 rule 5 running
  0 packet
```

配置对匹配 ACL 规则的流量进行镜像

通过本任务将通过某端口且匹配 ACL 规则的流量镜像到指定端口上。镜像操作不会影响镜像源端口上流量的接收与发送。用户可以对通过镜像目的端口的流量进行分析，实现对镜像源端口上流量的监控。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要流镜像的端口正常工作。

背景信息

- 访问列表中动作必须配置为 permit。
- 镜像目的端口不能是聚合端口。
- 系统只支持一个镜像目的端口，并且镜像目的端口只能是上行端口。

操作步骤

步骤 1 使用 **traffic-mirror** 命令对通过指定端口匹配 ACL 规则的流量进行镜像操作。

步骤 2 使用 **display qos-info traffic-mirror port** 命令查询指定端口匹配 ACL 规则的流镜像信息。

---结束

任务示例

举例：将端口 0/2/0 下接收到的匹配 ACL 规则 2001 的流量镜像到端口 0/2/1。

```
huawei(config)#traffic-mirror inbound ip-group 2001 port 0/2/0 to port 0/2/1
huawei(config)#display qos-info traffic-mirror port 0/2/0
traffic-mirror:
port 0/2/0:
  Inbound:
    Matches: Acl 2001 rule 5      running
    Mirror to: port 0/2/1
```

配置对匹配 ACL 规则的流量进行重定向

通过本任务将通过某端口且匹配 ACL 规则的流量重定向到指定端口转发。重定向操作成功后，源端口不再转发匹配 ACL 规则的流量，而是改由重新指定的端口转发。

前提条件

相关 ACL 及其子规则已经完成配置，并且需要重定向的端口正常工作。

背景信息

- 仅对访问列表中动作为 permit 的规则有效。
- 目前系统只支持将业务端口上匹配 ACL 规则的流量重定向到上行端口；将上行端口上匹配 ACL 规则的流量重定向到相同类型单板的端口。

操作步骤

- 步骤 1** 使用 **traffic-redirect** 命令对通过指定端口匹配 ACL 规则的流量进行重定向操作。
- 步骤 2** 使用 **display qos-info traffic-redirect port** 命令查询指定端口上匹配 ACL 规则的流量的重定向信息。

----结束

任务示例

举例：将端口 0/2/0 接收到的匹配 ACL 2001 规则的流量重定向到端口 0/2/16 进行转发。

```
huawei(config)#traffic-redirect inbound ip-group 2001 port 0/2/0 to port 0/2/1
huawei(config)#display qos-info traffic-redirect port 0/2/0
traffic-redirect:
port 0/2/0:
Inbound:
  Matches: Acl 2001 rule 5      running
  Redirected to: port 0/2/1
```

3 配置 WLAN 业务

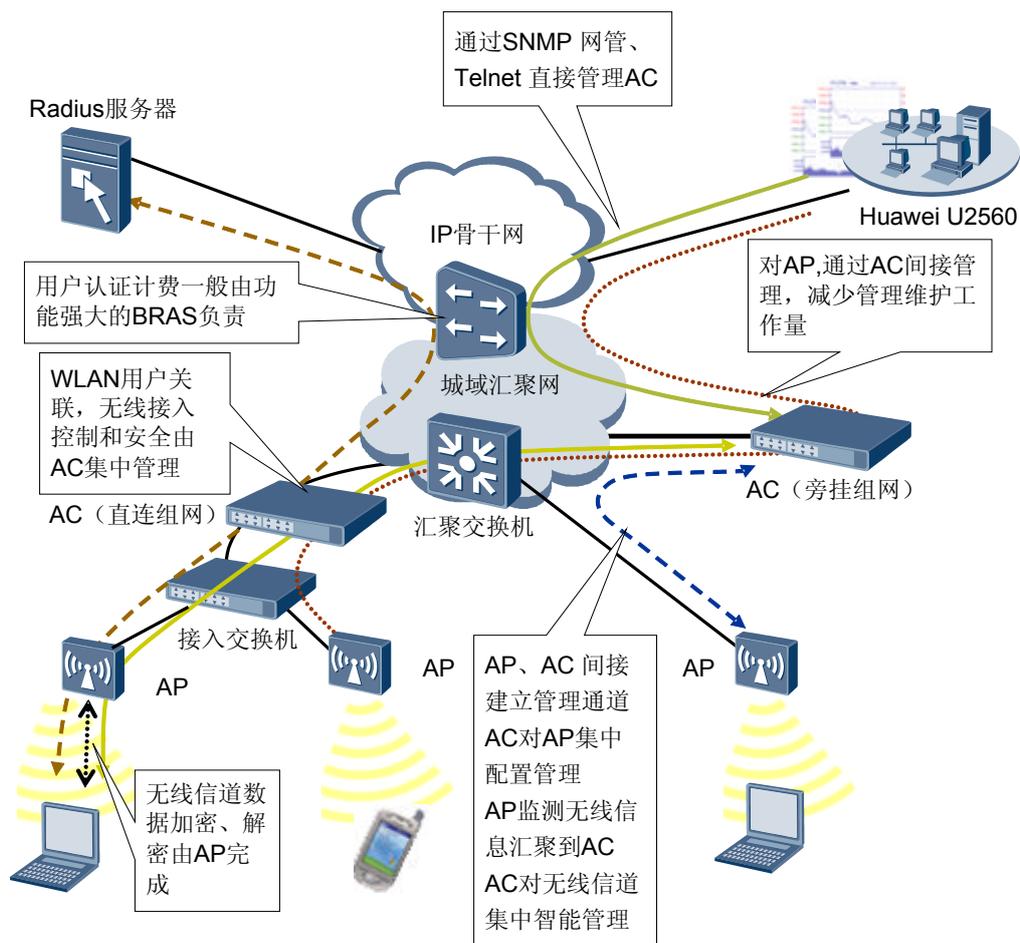
关于本章

介绍 AC+瘦 AP 组网模式下的 WLAN 业务配置过程。该章节中的所有操作均在 AC 系统上进行。

WLAN(Wireless Local Area Network)无线局域网是计算机网络与无线通信技术相结合的产物。它以无线多址信道作为传输媒介，利用电磁波完成数据交互，实现传统有线局域网的功能。

WLAN（AC+瘦 AP）组网模式如[图 3-1](#) 所示。

图 3-1 AC+瘦 AP 组网模式



无线终端通过 WLAN 接入技术连通互联网的数据流主要传输在两段不同传输媒介，即无线终端与 AP 之间的无线链路以及 AP 与 AC 之间的有线链路：

- AP 与 AC 之间的有线链路建立过程可以分为 AP 发现 AC、AP 与 AC 建立 CAPWAP 隧道、AP 加入 AC、AP 版本更新过程、AP 配置更新过程、数据检查过程以及运行状态确定七个步骤。
 1. AP 启动后，通过三种方式发现 AC：分别是单播、组播和广播方式。一般情况下单播方式的 AC 发现可以采用三种方法：DHCP 发现、DNS 发现和静态配置。
 - DHCP 方式：AP 通过 DHCP 报文从 AC 的 IP 地址池中分到 IP 地址。AC 在分配给 AP 的地址时，采用 OPTION 138/OPTION 43/OPTION 189 携带 AC 的 IP 地址。
 - DNS 方式：AP 通过 DNS 的域名解析获得 AC 的 IP 地址。
 - 静态配置：在 AP 上静态配置 AC 的 IP 地址。
 2. AP 根据此 IP 地址通过与 AC 协商，AP 接收到响应消息后开始与 AC 建立 CAPWAP 隧道，该隧道是采用 DTLS 加密传输 UDP 数据报文。
 3. CAPWAP 隧道建立后，AP 与 AC 之间通过发送加入请求消息和加入响应消息进行协商。在协商过程中，AC 会判决是否允许该 AP 加入。

4. AP 根据协商参数判断当前版本是否是最新版本，如果不是最新版本，则 AP 将在 CAPWAP 隧道上开始更新软件版本。AP 在软件版本更新完成后重新启动，重复进行 AC 发现、建立 CAPWAP 隧道、加入过程。
 5. 版本更新完成后，AP 向 AC 发送配置状态请求消息，向 AC 通告当前本地配置（天线、射频配置、速率、信道、功率），AC 会立即响应配置状态响应消息，可以立即更新 AP 请求的配置。
 6. 配置更新完成后，AP 会将配置更新的结果通过改变状态请求消息反馈给 AC，AC 根据这个消息获得 AP 上更新结果，并反馈改变状态响应消息。
 7. 在以上步骤完成后，AP 进入“normal”状态，开始正常工作。
- 无线终端与 AP 之间的无线链路建立过程可以分为终端扫描 AP、终端在 AP 上认证和终端与 AP 进行关联三个步骤。
 1. 无线局域网中多个 AP 定期发送 BEACON 帧，无线终端在每个信道上检测多个设备定期发送的 BEACON 帧后，选择一台 AP 作为 WLAN 接入设备。
 2. 无线终端在通过 AP 的 802.11 链路认证后，发送关联请求给 AP。AP 会将关联请求帧转发给 AC，由 AC 决定是否允许此无线终端加入，并发送站点配置请求消息给 AP。
 3. 无线终端开始拨号进行 802.1x 认证，与 AP 建立关联关系。

3.1 配置运营商 ID 和 AC ID

为了便于区分运营商和 AC，分别给运营商和 AC 配置一个 ID 编号。

3.2 配置 AC 三层接口

配置 AC 三层接口即配置 AC 管理 AP 的 VLAN 接口，使 AP 能够与 AC 建立连接。

3.3 配置 DHCP server

如果由 AC 给 AP 分配地址，则需要在 AC 上配置 DHCP Server。

3.4 配置 AP 的版本升级

AP 在正常运行之前或 AC 版本变更后，AP 和 AC 协商决定与当前 AC 版本对应的 AP 运行版本，如果版本不匹配，AP 开始升级。

3.5 配置数据的转发模式

3.6 添加 AP 并上线

添加 AP 有三种方式：离线添加 AP、自动添加 AP，以及手工确认未认证列表中的 AP。

3.7 配置 WLAN 射频

AP 设备上线后，需要给 AP 设备配置射频模板。

3.8 配置 ESS 和 VAP

AP 正常上线，可以对 VAP 进行参数配置，完成 WLAN 业务配置。

3.9 配置 WLAN 的 QoS 策略

对 AP 和 STA 进行 QoS 参数配置，针对不同的接入用户提供差异化的 QoS 策略。

3.10 配置 WLAN 接入安全策略

WLAN 接入安全策略确保 STA 接入 WLAN 网络及数据收发安全性。

3.11 配置 802.11n

配置 802.11n 为 WLAN 接入用户提供更高的“接入速率配置”。

3.12 查看 AP 信息

介绍如何查看 AP 的状态、认证模式、性能统计等详细信息。

3.1 配置运营商 ID 和 AC ID

为了便于区分运营商和 AC，分别给运营商和 AC 配置一个 ID 编号。

操作步骤

步骤 1 使用 **wlan ac-global** 命令，为指定 AC 配置编号，并配置 AC 设备的运营商标识。

 说明

目前运营商标识为：cmcc/中国移动、ctc/中国电信、cuc/中国联通、other/其他运营商。

----结束

任务示例

举例：配置 AC 设备的运营商标识为 ctc，编号为 1。

```
huawei(config)#wlan ac-global ac id 1 carrier id ctc
```

3.2 配置 AC 三层接口

配置 AC 三层接口即配置 AC 管理 AP 的 VLAN 接口，使 AP 能够与 AC 建立连接。

背景信息

如果存在多个管理 AP 的 VLAN，则需要配置多个 VLAN 接口。

操作步骤

步骤 1 使用 **interface vlanif** 命令创建 VLANIF 接口。

步骤 2 使用 **ip address** 命令配置 VLANIF 接口的 IP 地址。

步骤 3 配置 VLANIF 为 AP 在 AC 上的源。

- 如果只有 1 个管理 AP 的 VLAN，使用 **wlan ac source interface vlanif** 命令将该 VLANIF 配置为 AP 在 AC 上的源。
- 如果存在多个管理 AP 的 VLAN，则建议创建 Loopback 接口，确保在部分 VLANIF 故障的情况下，其他 VLANIF 下的 AP 还可以继续工作。

1. 使用 **interface loopback** 命令创建 Loopback 接口。
2. 使用 **ip address** 命令配置 Loopback 接口的 IP 地址。
3. 使用 **wlan ac source interface loopback** 命令将该 Loopback 接口配置为 AP 在 AC 上的源。



注意

设置为 Loopback 接口的地址，必须使用 32 位掩码，作为 AC 的源 IP 地址，用于 AP 和 AC 之间建立隧道使用。



说明

VLANIF 与 Loopback 接口绑定成功后，发往此 Loopback 接口的报文通过绑定的 VLANIF 接口送往设备。

---结束

3.3 配置 DHCP server

如果由 AC 给 AP 分配地址，则需要在 AC 上配置 DHCP Server。

前提条件

在管理 AP 的 VLANIF 下配置 DHCP Server。

操作步骤

步骤 1 使用 **ip pool** 命令创建一个 IP 地址池。

步骤 2 使用 **gateway** 命令配置 IP 地址池的网关地址，需要与管理 AP 的 VLANIF 接口地址对应。



说明

IP 地址池的网关地址与 VLANIF 接口 IP 地址对应，用来定义 AP 上线后从那个地址池获取 IP 地址。

步骤 3 使用 **section** 命令配置 IP 地址池中的地址段。

步骤 4 使用 **option** 命令配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP Option43 方式给 AP 通告 AC 的 IP 地址。



注意

- 当 AP 需要获取 AC 的 IP 地址时，如果在二层组网情况下，此字段是可选的，如果在三层组网情况下，此字段是必选的。
- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。
- 如果涉及多个 IP 地址，则格式必须为“HuaweiAC-x.x.x.x,x.x.x.x”，即 IP 地址之间用逗号隔开。

---结束

任务示例

举例：创建一个 IP 地址池，IP 地址池的网关地址为 172.1.1.1/24，地址段从 172.1.1.2 到 172.1.1.124，Option 43 字段名称为 HuaweiAC-172.1.1.1。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.124
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-172.1.1.1
```

3.4 配置 AP 的版本升级

AP 在正常运行之前或 AC 版本变更后，AP 和 AC 协商决定与当前 AC 版本对应的 AP 运行版本，如果版本不匹配，AP 开始升级。

背景信息

AP 设备升级的两种场景：

- 自动升级：AP 之前未上线工作，在新注册时发现自身版本比 AC 设备或者 FTP 服务器上的 AP 版本低，则启动升级。
- 在线升级：AP 当前在工作过程中，发现自身版本比 AC 设备或者 FTP 服务器上的 AP 版本低，则启动升级。

AP 设备支持两种版本升级模式：

- **ac-mode**：AP 升级时从 AC 上下载升级版本。
- **ftp-mode**：AC 设备通过 **ap-update ftp-server** 命令下发 FTP 配置信息后，由 AP 到 FTP 服务器下载升级版本。

配置时需要注意以下事项：

- 预先设置升级模式控制 AP 版本升级方式，**ac-mode**、**ftp-mode** 二选一。
- **ac-mode** 方式 AC 上可以一次配置大量同类 AP 加载版本，但最大只支持 8 个 AP 同时加载，其他 AP 照此相继进行版本加载；**ftp-mode** 方式对同时加载 AP 的数量没有限制。

 说明

目前仅支持同时对一种类型的 AP 进行加载。

操作步骤

- 配置 **ac-mode** 升级模式。
 1. 在全局模式下，使用 **load file** 命令将 AP 的升级文件加载到 AC 设备中。
 2. 在 WLAN-AC 模式下，使用 **ap-update mode** 命令设置 AP 升级模式的为“**ac-mode**”。
 3. 在 WLAN-AC 模式下，使用 **ap-update update-filename** 设置与 AP 类型对应的升级文件名。
 4. 如果是在线升级，还需要执行如下操作：
 - a. 使用 **ap-update multi-load** 命令按 AP 类型批量升级。
 - b. 升级完成后使用 **ap-update multi-reset ap-type** 命令批量复位升级完成的 AP。
- 配置 **ftp-mode** 升级模式。
 1. 使用 **ap-update ftp-server** 命令，设置或修改 FTP 服务端 IP、客户端用户名、密码。

 说明
将 AP 升级所需的升级文件保存在 FTP 服务目录下。
 2. 在 WLAN-AC 模式下，使用 **ap-update mode** 命令设置 AP 升级模式的为“**ftp-mode**”。

3. 在 WLAN-AC 模式下，使用 **ap-update update-filename** 设置与 AP 类型对应的升级文件名。
4. 如果是在线升级，还需要执行如下操作：
 - a. 使用 **ap-update multi-load** 命令按 AP 类型批量升级。
 - b. 升级完成后使用 **ap-update multi-reset ap-type** 命令批量复位升级完成的 AP。

---结束

任务示例

举例：在 AC 上配置 AP 升级模式为“ac-mode”，对应类型为 WA601（ap-type 为 0）的 AP 的对应版本文件为 ap_firmware.bin，进行在线升级。

```
huawei(config)#load file tftp 10.11.104.1 ap_firmware.bin
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-update mode ac-mode
huawei(config-wlan-ac-view)#ap-update update-filename ap_firmware.bin ap-type 0
huawei(config-wlan-ac-view)#ap-update multi-load ap-type 0
huawei(config-wlan-ac-view)#ap-update multi-reset ap-type 0
```

3.5 配置数据的转发模式

操作步骤

步骤 1 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 2 配置数据的转发模式。

- 执行命令 **forward-mode type { ess | ap }**，配置基于 ESS 或基于 AP 的数据转发模式。
 - 执行命令 **forward-mode ess essid mode { direct-forward | tunnel }** 配置 ESS 的数据转发模式，可以配置为直接转发或隧道转发。
 - 执行命令 **forward-mode ap by-region region mode { direct-forward | tunnel }** 配置 AP 域的数据转发模式，可以配置为直接转发或隧道转发。
 - 执行命令 **forward-mode ap apid-list mode { direct-forward | tunnel }**，配置 AP 的数据转发模式，可以配置为直接转发或隧道转发。

步骤 3 执行命令 **display forward-mode**，查询数据转发模式的配置类型和基于不同配置类型的数据转发模式。

---结束

3.6 添加 AP 并上线

添加 AP 有三种方式：离线添加 AP、自动添加 AP，以及手工确认未认证列表中的 AP。

前提条件

- AC 设备的基本功能已经配置完成。
- AP 和 AC 之间网络连接正常。

背景信息

- AP 上线的一般流程如下：
 - 如果某 AP 已经离线添加，则该 AP 可以直接上线。
 - 如果没有离线添加 AP，但 AP 的认证模式为“no-auth”（即“不认证”），或者 AP 在已设置的“白名单”中，则该 AP 可以自动添加并上线。
 - 如果此 AP 设备不存在于黑名单中，也不存在于白名单或 AP 列表中，且当前 AP 的认证模式不为 no-auth 模式，那么此 AP 设备会被阻止上线，但其信息会被记录到未认证 AP 列表之中。该 AP 通过确认未认证 AP 列表中的 AP 设备方式添加。
- AP 类型：
 - AP 的类型必须唯一，且必须与实际使用的 AP 类型一致，否则会导致 AP 无法正常上线。
 - AP 上线时，将判断此 AP 的类型是否与 AC 上所配置的 AP 类型表中的匹配，如果不匹配，则 AP 上线失败。
- AP 域：
 - 1 个 AP 只能且必须加入 1 个 AP 域才能正常上线。
 - 系统缺省存在 1 个 AP 域，当 AP 上线自动确认时，将自动加入缺省域。用户可以指定任何一个已存在的 AP 域为缺省域。
- AP 模板：1 个 AP 只能且必须绑定 1 个 AP 模板才能正常上线。

操作步骤

步骤 1 在 AC 上配置将上线的 AP 类型。

1. 使用 **wlan ac** 命令，进入 WLAN-AC 模式。
2. 使用 **display ap-type** 命令查看 AC 上支持的 AP 类型。
3. 如果将上线的 AP 类型不在查询结果中，使用 **ap-type** 命令新增 AP 类型。

 说明

缺省情况下，系统预置了 12 种缺省支持的 AP 设备类型，包括：WA601、WA631、WA651、WA602、WA632、WA652、WA603SN、WA603DN、WA633SN、WA603DE、WA653DE、WA653SN。

步骤 2 添加 AP。

- 离线添加 AP：
 1. 使用 **ap-auth-mode** 命令配置 AP 上线时根据“MAC”或“SN”认证。
 2. 使用 **ap** 命令离线增加 AP，AP ID 根据用户预定义的 ID 进行设置，根据 AP 的认证模式输入 MAC 或 SN。
 3. 将 AP 上线，AP 将直接进入“normal”状态。
- 自动添加 AP：
 1. 使用 **ap-auth-mode** 命令配置 AP 上线时“不认证”；或者使用 **ap-whitelist** 命令，增加合法 AP 的 MAC 或者 SN 到白名单里。
 2. 将 AP 上线，AP 将直接进入“normal”状态。

 说明

如果需要设置 AP 不上线，使用 **ap-blacklist** 命令将 AP 添加到黑名单中。

- 确认未认证列表中的 AP：

1. 使用 **ap-confirm** 命令确认未认证列表中的 AP，确认成功后，AP 将进入“normal”状态。

步骤 3 (可选) 使用 **ap-region** 命令增加 AP 域，便于 AP 的集中管理，如果不新建，则使用系统缺省域。使用 **region-id** 命令将添加的 AP 加入指定域。

步骤 4 (可选) 使用 **ap-profile** 命令创建 AP 模板并配置模板参数 (MTU、日志服务器地址、备份模式)。使用 **profile-id** 命令将添加的 AP 引用指定的 AP 模板。

步骤 5 查看 AP 是否添加成功。

使用 **display ap** 命令查添加的 AP 状态。

```
huawei(config-wlan-ac-view)#display ap all
```

```
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
0	WA631	0	0	fault
1	WA601	1	101	normal
2	WA601	0	102	normal
3	WA632	0	0	fault

```
Total number: 4
```

----结束

3.7 配置 WLAN 射频

AP 设备上线后，需要给 AP 设备配置射频模板。

背景信息

1 个 AP 开工后系统默认为其创建 Radio，最多可以创建 4 个 Radio，无需手工创建。目前 radio-id 为 0 的射频为 2.4G 频段，radio-id 为 1 的射频为 5G 频段。

3.7.1 配置 Radio 模板

Radio 模板需要绑定 WMM 模板并按照配置向导配置射频参数。

操作步骤

步骤 1 使用 **wlan ac** 命令，进入 WLAN-AC 模式。

步骤 2 使用 **radio-profile** 命令创建 Radio 模板。

 说明

Radio 模板创建成功后，模板内的参数均自动配置为默认值。

步骤 3 使用 **display radio-profile** 命令查看 Radio 模板配置的各项属性。

#创建 Radio 模板“radio-profile-1”，所有配置均为默认值。

```
huawei(config-wlan-ac-view)#radio-profile name radio-profile-1 id 1
```

```
huawei(config-wlan-radio-prof-radio-profile-1)#display radio-profile name radio-profile-1
```

```
-----  
Profile ID           :1  
Profile name         :radio-profile-1  
Radio type           :802.11b/g  
Rate mode            :auto  
Rate (Mbps)          :54  
Channel mode         :auto
```

```

Power mode                               :auto
Calibrate interval (min)                  :720
PER threshold (%)                          :30
Conflict rate threshold (%)               :60
RTS/CTS threshold (Byte)                  :2347
Fragmentation threshold (Byte)            :2346
Short retry number limit                   :7
Long retry number limit                    :4
Support short preamble                     :support
DTIM interval (Beacon interval numbers) :3
Beacon interval (time unit)                :1000
WMM profile ID                             :-
WMM profile name                           :-
Interference detect switch                 :disable
Calibrate switch                           :enable
Common frequency disturb threshold (%)     :50
Adjacent frequency disturb threshold (%)   :50
Station disturb threshold                  :32
802.11n guard interval mode                :normal
802.11n A-MPDU length limit               :3
    
```

步骤 4 (可选) 使用 **radio-type** 命令配置指定 Radio 模板中的射频类型参数。

 说明

- “radio-type” 的缺省值为 “80211bg”。
- 如果绑定了该模板的某个射频不支持新修改的射频类型，修改会失败。
- 新修改的射频类型和速率参数冲突时，修改会失败。比如新修改射频类型为 802.11b，但模板中的速率为指定速率模式且指定值为 54Mbps，此时修改失败。

步骤 5 (可选) 使用 **rate auto max-rate rate-value** 命令配置指定 Radio 模板中的速率模式参数。

 说明

rate auto max-rate rate-value 命令设置 Radio 模板中的速率模式参数为自动模式并配置最大速率。此模式下绑定本模板的射频可以在最大值及其以下的速率取值中自动选择速率。

步骤 6 (可选) 使用 **power-mode** 命令配置指定 Radio 模板中功率模式参数。

 说明

“power-mode” 的缺省配置为 “auto”，既射频能够根据射频环境自动选择一个合适的值或进行调整，无需用户指定。

步骤 7 (可选) 使用 **channel-mode** 命令配置指定 Radio 模板中的信道模式参数。

 说明

“channel-mode” 的缺省配置为 “auto”，既射频能够根据射频环境自动选择一个合适的信道或进行调整，无需用户指定信道。推荐用户使用此模式。

步骤 8 使用 **bind wmm-profile** 命为指定 Radio 模板绑定 WMM 模板。

#配置 Radio 模板 “radio-profile-1” 绑定 WMM 模板 “wmm-profile-1”。

```

huawei(config-wlan-radio-prof-radio-profile-1)#bind wmm-profile name wmm-profile-1
huawei(config-wlan-radio-prof-radio-profile-1)#display radio-profile name radio-profile-1
    
```

```

Profile ID                               :1
Profile name                             :radio-profile-1
.....
WMM profile ID                           :1
WMM profile name                          :wmm-profile-1
.....
    
```

 说明

只有绑定了 WMM 模板的 Radio 模板才可以被射频绑定。

---结束

3.7.2 在射频上绑定 Radio 模板

为指定射频绑定 Radio 模板，绑定成功后，Radio 模板参数会应用到该射频中。

背景信息

Radio 模板参数内容包括：射频类型、射频速率、射频信道模式、射频功率模式、调优检测周期、丢包/错包率门限、冲突率门限、分段门限、RTS/CTS 门限、短/长帧重传次数门限、是否支持短前导码、DTIM 周期、beacon 帧周期、WMM 参数等。

操作步骤

步骤 1 使用 `wlan ac` 命令，进入 WLAN-AC 模式。

步骤 2 使用 `radio` 命令进入射频视图。

步骤 3 使用 `bind radio-profile` 命令为指定射频绑定 Radio 模板。

步骤 4 使用 `display binding radio-profile` 命令查询指定 Radio 模板的绑定关系。

#查看 Radio 模板“huawei”的绑定状态。

```
huawei(config-wlan-ac-view)#display binding radio-profile name radio-profile-1
```

```
-----  
AP  RADIO  
-----
```

```
1    0  
-----
```

```
Total: 1
```

---结束

任务示例

#为 AP1 的 Radio 0 绑定 Radio 模板“radio-profile-1。”

```
huawei(config)#wlan ac
```

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
```

```
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-profile-1
```

3.7.3 配置基于 AP 域的射频调优

对指定域进行全局调优配置，避免出现大面积的射频信号劣化。

背景信息

调优策略的目的是为了使 Radio 下用户之间发射功率不干扰。

操作步骤

步骤 1 使用 `wlan ac` 命令，进入 WLAN-AC 模式。

步骤 2 配置射频调优。

- 使用 `calibrate startup` 命令启动指定域的全局调优。

- 使用 `calibrate auto-startup` 定时启动调优。



说明

在调优过程中，如果希望探测到非法邻居，请在步骤 2 中配置命令时，选择“listen-uncontrol-neighbor”参数。

---结束

任务示例

#设置每天凌晨 2 点定时启动域 3 的全局调优，并在调优的同时监听该域周围所有的非法邻居。

```
huawei(config)#wlan ac
```

```
huawei(config-wlan-ac-view)#calibrate auto-startup region 3 time 2:0:0 listen-uncontrol-neighbor
```

3.7.4（可选）配置 AP 射频资源管理

AP 的射频资源管理包括调整信道、传输功率和检测&纠正覆盖黑洞。

背景信息

自动调优无需用户指定，AP 能够根据射频环境自动选择合适的信道或值分别对信道和功率进行调整。自动调优和用户指定是互斥的，只能指定一种模式，两者无优先级关系。

操作步骤

- 步骤 1** 在射频模板模式下，使用 **channel-mode auto** 命令配置指定射频模板中的信道模式参数为自动模式，这样 AP 能够根据射频环境自动选择一个合适的信道或进行调整，无需用户指定信道。系统缺省情况下为自动模式，无需配置即可实现信道的自动选择和调整。



说明

在 WLAN 网络运行期间，AC 会周期性触发 AP 测量网络环境，以判断是否调整 AP 信道以及如何调整 AP 信道。

- 步骤 2** 在射频模板模式下，使用 **power-mode auto** 命令配置指定射频模板中的功率模式参数为自动模式，这样 AP 能够根据射频环境自动选择一个合适的值或进行调整，无需用户指定。



说明

在 WLAN 网络运行期间，AC 会周期性触发 AP 采集邻居信息，判断是否需要调整 AP 的传输功率，以完整覆盖 WLAN 区域。

- 步骤 3** 当 WLAN 网络中的 AP 设备丢失，或者障碍物的阻挡会造成覆盖黑洞，AC 会周期性检测网络中是否有覆盖黑洞的存在并进行纠正。

---结束

3.7.5（可选）配置 AP 负载均衡组

AC 根据配置策略控制 AP 接入的无线用户，以保证 WLAN 实现负载均衡，优化网络性能。

背景信息

在集中式控制系统中，无线终端关联 AP 设备都是需要经过 AC 许可。在实际应用中，无线终端会扫描到多台 AP 设备，并且向多台设备发送关联请求帧，无论采用 Split MAC、Local MAC 或者 Remote MAC，AP 设备收到无线终端的关联请求帧后都会将此帧转发给 AC，由 AC 根据自身策略决定无线终端可以关联到哪台 AP。

操作步骤

步骤 1 使用 **wlan ac** 命令，进入 WLAN-AC 模式。

步骤 2 使用 **load-balance group** 命令创建一个负载均衡组并进入该组的配置视图。

1. 使用 **member** 命令用来向指定负载均衡组内添加射频。添加后当有 STA 关联这个射频时，会先比较该射频和组内其他已正常工作射频的负载均衡情况来决定是否让 STA 关联这个射频。
2. （可选）使用 **traffic gap** 命令用来配置指定负载均衡组的负载均衡模式为流量模式。
3. （可选）使用 **session gap** 命令用来配置指定负载均衡组的负载均衡模式为会话模式。
4. 使用 **associate-threshold** 命令用来配置指定负载均衡组的最大关联次数。

 说明

新建的组中所有参数都取默认值，直到用户修改。

----结束

3.8 配置 ESS 和 VAP

AP 正常上线，可以对 VAP 进行参数配置，完成 WLAN 业务配置。

3.8.1 配置 ESS

ESS 是一个业务参数集合，是 VAP 的属性集合。当它被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上。

前提条件

Security 模板和 Traffic 模板已经配置完成。

操作步骤

步骤 1 使用 **wlan ac** 命令，进入 WLAN-AC 模式。

步骤 2 使用 **ess** 命令创建 ESS。

#创建一个名字为“huawei”的 ESS，设置其 SSID 为“huawei-1”，IGMP 模式为“snooping”，配置 Traffic 模板为“huawei”，Security 模板为“huawei”，其他参数为默认值。

```
huawei(config-wlan-ac-view)#ess name huawei ssid huawei-1 traffic-profile huawei  
security-profile huawei igmp-mode snooping
```

步骤 3 使用 **vlan-mapping** 命令配置 VLAN 映射模式及配置 VLAN。

 说明

- 当需要对绑定同样 ESS 创建的 VAP 上行业务配置相同 VLAN 时，配置 ESS 的业务 VLAN 模式为 **ess-mode**。
- 当需要根据 AP 区分业务时，配置 ESS 的业务 VLAN 模式为 **ap-mode**。
- 当需要根据 AP 域区分业务时，配置 ESS 的业务 VLAN 模式为 **region-mode**。

步骤 4 使用 **display ess** 命令查看 ESS 配置的各项属性。

#查看 ESS 为“huawei”的各项配置属性。

```
huawei(config-wlan-ac-view)#display ess name huawei
```

```
ESS ID: 17
ESS name: huawei
SSID: huawei-1
Hide SSID: disable
User isolate: enable
Type: service
Maximum number of user: 32
User association time out: 5 minutes
Traffic profile name: huawei
Security profile name: huawei
IGMP mode: snooping
-----
```

步骤 5 使用 **display vlan-mapping ess** 命令查看 ESS 配置的 VLAN。

```
huawei(config-wlan-ac-view)#display vlan-mapping ess name huawei
```

```
-----
ESS ID          : 17
ESS Name        : huawei
VLAN Mapping Mode : Region Mode
Region ID to VLAN ID Mapping List:
-----
```

```
Region ID      VLAN ID
101            101
-----
```

```
Total: 1
Remark: Other Regions in this ESS use default VLAN ID 1
```

----结束

任务示例

#创建一个名字为“huawei”的 ESS，设置其 SSID 为“huawei-1”，IGMP 模式为“snooping”，配置 Traffic 模板为“huawei”，Security 模板为“huawei”，VLAN 映射模式为 AP 域映射，Ap-region 101 映射 VLAN 101。其他参数为默认值。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ess name huawei ssid huawei-1 traffic-profile huawei
security-profile huawei igmp-mode snooping
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei type tag region 101 vlan 101
```

3.8.2 配置 VAP 并绑定 ESS

VAP 下发到 AP 设备后，与 VAP 绑定的 ESS 参数作为 VAP 的参数一起下发到 AP 设备，AP 设备将根据 VAP 的参数提供给用户不同的业务。

背景信息

VAP 是 AP 设备上的业务功能实体。用户可以在 AP 设备上的每个射频上创建不同的 VAP，通过为 AP 设备的指定射频绑定 ESS，就可以创建 vap。使用 **commit** 命令提交配置，VAP 下发到 AP 设备。

前提条件

- 指定射频上已经绑定了 Radio 模版，具体请参见 [3.7.2 在射频上绑定 Radio 模版](#)。
- ESS 参数已经创建，具体请参见 [3.8.1 配置 ESS](#)。

操作步骤

步骤 1 使用 **wlan ac** 命令，进入 WLAN-AC 模式。

步骤 2 创建 VAP。

- 创建单个 VAP，绑定 ESS。
 1. 使用 **vap ap** 命令，为指定 AP 的指定射频绑定 ESS 参数。
 2. 使用 **commit** 命令提交指定 AP 的配置。
- 批量创建 VAP，绑定 ESS。

说明

预配置可以理解为离线配置、批量配置，需要将所有的模板创建完成。后续创建 VAP 的时候直接将模板批量进行绑定，模板的配置过程和实时在线配置一样，因为离线没有 AP 实体，暂不创建 VAP。上述针对 AP 类型的离线配置完成后，待 AP 上线后，根据其 AP 类型、radioID、radio 模板、ess 模板和 AP 域批量下发 VAP 参数。

使用 **service-batch ap-type** 命令为指定类型的 AP 设备的指定射频绑定射频模板和 ESS。

---结束

任务示例

```
#配置 AP1 对应的 VAP，ESS 名称为“huawei”。
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei
huawei(config-wlan-ac-view)#commit ap 1
#配置指定类型 WA601 的 AP 设备的射频 0 绑定射频模板 1 和 ESS 2。
huawei(config-wlan-ac-view)#service-batch ap-type name wa601 radio 0 radio-profile
id 1 ess id 2
```

3.9 配置 WLAN 的 QoS 策略

对 AP 和 STA 进行 QoS 参数配置，针对不同的接入用户提供差异化的 QoS 策略。

3.9.1 配置射频的 QoS 策略

配置 QoS 策略是创建 WMM 模板，然后将 WMM 模板绑定到射频模板。

背景信息

Wi-Fi 多媒体标准 WMM (Wi-Fi Multimedia) 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。

操作步骤

- 步骤 1** 使用 **wlan ac** 命令，进入 WLAN-AC 模式。
- 步骤 2** 使用 **wmm-profile { id profile-id | name profile-name }*** 命令创建 WMM 模板。
 -  说明
 - WMM 模板创建成功后，模板内的参数均自动配置为默认值。
- 步骤 3** 使用 **wmm enable** 命令用来使能 WMM 功能，使能 WMM 功能后，相关配置的 WMM 参数才会生效，否则 AP 设备使用自己默认的 WMM 参数。
- 步骤 4** 使用 **wmm mandatory enable** 命令用来打开控制许可开关。此时不允许未使能 WMM 功能的终端连接使能了 WMM 功能的 AP。
- 步骤 5** 使用 **display wmm-profile { all | id profile-id | name profile-name }** 命令查看 WMM 模板配置的各项属性。

#创建 WMM 模板 “wmm-profile-1”，所有配置均为默认值。

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-profile-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#display wmm-profile name wmm-profile-1
Profile ID      : 1
Profile name    : wmm-profile-1
WMM switch     : enable
Mandatory switch: disable
Client EDCA parameters:
-----
          ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO    3        2        2       47
AC_VI    4        3        2       94
AC_BE   10        4        3        0
AC_BK   10        4        7        0
-----
AP EDCA parameters:
-----
          ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO    3        2        1       47       normal
AC_VI    4        3        1       94       normal
AC_BE    6        4        3        0       normal
AC_BK   10        4        7        0       normal
-----

```

说明

终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同报文获得不同级别的服务，我们将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样。

四个优先级队列的名称和优先级顺序默认为：AC_VO(语音) > AC_VI(视频) > AC_BE(尽力而为) > AC_BK(背景)。

四个优先级队列的优先级顺序并不是绝对的，可以通过参数修改来调整优先级顺序，这些参数称为 EDCA 参数(Enhanced Distributed Channel Access)。包括 AIFSN (arbitration inter Frame spacing number 仲裁帧间隙数)、ECWmin (exponentn form of CWmin 最小竞争窗口指数形式)、ECWmax(exponent form of CWmax 最大竞争窗口指数形式)、TXOPLimit (transmission opportunity limit 传输机会限制)以及 ack-policy (ACK 策略)。

- AIFSN: WMM 针对不同 AC 队列可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。
- ECWwin 和 ECWmax: 这两个数值决定了平均退避时间值，数值越大，用户的平均退避时间越长。
- TXOPLimit: 用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用的信道时长越大，如果是 0，则每次占用信道后，只能发送一个报文。
- ack-policy: 有 normal ack(应答)和 no ack(不应答)两种策略，默认为 noraml ack。

占用信道发送报文的原理：终端在占用信道发送报文前，先监听信道，当信道空闲时间大于或等于空闲等待时间时，在竞争窗口范围内随即选择退避时间进行退避，最先结束退避的终端竞争到信道，开始发送报文。

步骤 6 (可选) 使用 **wmm edca client { ac-vo | ac-vi | ac-be | ac-bk } { aifsn aifsn-value | ecw ecwmin ecwmin-value ecwmax ecwmax-value | txoplimit txoplimit-value }** *命令配置终端上四个 WMM 队列的 EDCA 参数。

步骤 7 (可选) 使用 **wmm edca ap { ac-vo | ac-vi | ac-be | ac-bk } { aifsn aifsn-value | ecw ecwmin ecwmin-value ecwmax ecwmax-value | txoplimit txoplimit-value | ack-policy { normal | noack } }** *命令配置 AP 上四个 WMM 队列的 EDCA 参数和 ACK 策略。

----结束

3.9.2 配置 VAP 的 QoS 策略

配置 QoS 策略是创建 Traffic 模板就是配置 VAP 的 QoS 策略。

操作步骤

步骤 1 使用 **wlan ac** 命令，进入 WLAN-AC 模式。

步骤 2 使用 **traffic-profile { name profile-name | id profile-id }** *命令创建 Traffic 模板。

 说明

Traffic 模板创建成功后，模板内的参数均自动配置为默认值。

步骤 3 (可选) 使用 **8021p { designate value | up-mapping value0 value1 value2 value3 value4 value5 value6 value7 }** 命令配置 AP 的上行 802.3 报文的 802.1p 优先级值。

步骤 4 (可选) 使用 **8021p-map-up value0 value1 value2 value3 value4 value5 value6 value7** 命令配置下行时 802.1p 优先级值到用户优先级值的映射关系。

步骤 5 使用 **display traffic-profile { all | id profile-id | name profile-name }** 命令查看 Traffic 模板配置的各项属性。

#查看 Traffic 模板“huawei”的各项属性。

```

huawei(config-wlan-ac-view)#traffic-profile name huawei id 1
huawei(config-wlan-traffic-prof-huawei)#display traffic-profile name huawei
Profile ID           : 1
Profile name        : huawei
Client Limit Rate(up) : -
VAP Limit Rate(up)  : -
Client Limit Rate(down) : -
VAP Limit Rate(down) : -
802.1p Mapping Mode : mapping
-----
User-priority  802.1p
0               0
1               1
2               2
3               3
4               4
5               5
6               6
7               7
-----
802.1p to User-priority Mapping List:
-----
802.1p  User-priority
0       0
1       1
2       2
3       3
4       4
5       5
6       6
7       7
-----
Tunnel priority(up) Mapping Mode:tos(inner) to tos(outer)
-----
TOS(inner)      TOS(outer)
0               0
1               1
2               2
3               3
4               4
5               5
6               6
7               7
-----
Tunnel priority(down) Mapping Mode:tos(inner) to tos(outer)
-----
TOS(inner)      TOS(outer)
0               0
1               1

```

2	2
3	3
4	4
5	5
6	6
7	7

 说明

STA 发出的 802.11 报文要通过 AP 进入以太网时，需要转换成 802.3 报文，这期间可以不进行优先级映射，也可以按照不同的 VAP 设置不同的优先级，或者按照 UP 域的优先级映射关系获取到 8021p 优先级。

802.3 报文通过 AP 转发给 STA 时，被转换成 802.11 报文，其中的 UP 域可以根据 DSCP、CoS 映射而来，或者由流分类设置。

步骤 6 (可选) 使用 `tunnel-priority { up | down } designate { tos | 8021p } priority-value` 命令配置上、下行隧道优先级值。

步骤 7 (可选) 使用 `rate-limit { client | vap } { up | down } ratelimit-value` 命令配置上、下行速率。

----结束

3.10 配置 WLAN 接入安全策略

WLAN 接入安全策略确保 STA 接入 WLAN 网络及数据收发的安全性。

背景信息

WLAN 业务的接入安全策略的作用在于两方面：

- 一方面控制 STA 能否接入 WLAN 网络。一般有开放式认证 (open-system) 和共享密钥式 (shared-key) 认证。
- 另一方面采用加密技术，确保 STA 收发数据的安全性。一般有静态 WEP、802.1X 动态 WEP、临时密钥完整性协议(TKIP)、CBC-MAC 计数模式协议 (CCMP) 和网络层加密协议。

WLAN 的接入安全策略通过配置接入安全模板来实现，通过被 ESS 引用而生效。

操作步骤

步骤 1 使用 `wlan ac` 命令，进入 WLAN-AC 模式。

步骤 2 使用 `security-profile { id profile-id | name profile-name } *` 命令，配置用户的接入安全模板。

模板创建后，系统会给模板中各认证策略配置缺省值，如表 3-1 所示。

表 3-1 认证策略配置缺省值列表

认证策略	认证方式	加密方式
WEP	开放系统认证	空密钥
WPA1	802.1x+PEAP	TKIP
WPA2	802.1x+PEAP	CCMP

认证策略	认证方式	加密方式
WAPI	WAI	WPI

步骤 3 各种配置具体如下所示：

- 开放系统认证：
 1. 使用 **security-profile { id profile-id | name profile-name }** *命令进入指定的接入安全模板。
 2. 使用 **authentication policy wep** 命令配置接入安全模板采用 WEP 认证。
 3. 使用 **policy wep open-system** 命令配置指定模板的接入安全策略为开放系统认证。

- 共享密钥认证：
 1. 使用 **security-profile { id profile-id | name profile-name }** *命令进入指定的接入安全模板。
 2. 使用 **authentication policy wep** 命令配置接入安全模板采用 WEP 认证。
 3. 使用 **policy wep share-key** 命令配置指定模板的接入安全策略为共享密钥认证。
 4. 使用 **wep key { wep-40 | wep-104 } { pass-phrase | hex } key-id key-value** 命令配置 WEP 的密钥。



配置密钥时，如果选择 WEP-40 方式，则输入 10 个十六进制或者 5 个 ASCII 字符；如果选择 WEP-104 方式，则输入 26 个十六进制或者 13 个 ASCII 字符。

5. 使用 **wep default-key key-id** 命令配置缺省的密钥索引。

- WPA1/WPA2 认证：



采用 WPA1/WPA2+PSK/802.1x 认证模式时，需要使能设备的 802.1x 特性和 802.1x 全局 MAC 地址控制开关。WPA1/WPA2+PSK 认证模式下使能 802.1x 功能是因为 PSK 密钥交互承载在 EAPOL 报文之上。

1. 使用 **dot1x enable** 命令使能设备的 802.1x 特性。
2. 使用 **dot1x mac-control** 命令使能 802.1x 全局 MAC 地址控制开关。
3. 使用 **wlan ac** 命令，进入 WLAN-AC 模式。
4. 使用 **security-profile { id profile-id | name profile-name }** *命令进入指定的接入安全模板。
5. 使用 **authentication policy { wpa1 | wpa2 }** 命令配置接入安全模板采用 WPA1/WPA2 认证。
6. 配置 WPA1/WPA2 的认证方式和加密方式：
 - 如果采用预共享密钥的接入认证方式和密钥，则使用 **policy { wpa1-psk | wpa2-psk } { tkip | ccmp } { pass-phrase | hex } <key>**命令配置。
 - 如果采用 802.1x 的接入认证方式和密钥，则使用 **policy { wpa1 | wpa2 } { tkip | ccmp } 802dot1x { peap | sim }**命令配置。

- WAPI 认证：

1. 使用 **security-profile { id profile-id | name profile-name }** *命令进入指定的接入安全模板。
2. 使用 **authentication policy wapi** 命令配置接入安全模板采用 WAPI 认证。

3. 配置 WAPI 的认证方式和加密方式:

- 采用共享密钥认证方式:
 - a. 使用 **wapi wai psk { pass-phrase | hex } key** 命令进行配置。
- 采用证书认证方式:

 说明

使用证书认证前, 需要先将 AC、AP 的证书下载到设备上。

- a. 使用 **wapi wai certificate** 配置 WAPI 的认证采用证书认证。
- b. 使用 **wapi certification { ac | asu | issuer } import file-name file_name** 命令来导入 AC 的证书文件、AC 的私钥文件以及 ASU 的证书文件。建立证书文件和模板之间的绑定关系。
- c. (可选) 使用 **wapi private-key import file-name file_name** 命令导入 AC 的私钥文件。如果 AC 的证书不包含私钥文件, 需要执行此命令。
- d. 使用 **wapi asu-server ip ip-addr** 命令设置 ASU 服务器的 IP 地址。WAPI 证书方式下, AC 会将证书发送到该 IP 地址所在的 ASU 服务器。

步骤 4 使用 **display security-profile { all | { id profile-id | name profile-name } [detail] }** 命令查看所配置的接入安全模板。

---结束

任务示例

#配置接入安全模板“security-5”, 使用 WAPI 认证, 采用证书认证方式; 配置 ASU 服务器的 IP 地址为 10.10.10.1, AC 认证证书为 huawei-ac.cer, ASU 认证证书为 huawei-asu.cer, AC 证书的私钥文件为 ac-key.key, Issuer 认证证书为 huawei-issuer.cer。

```
huawei(config-wlan-ac-view)#security-profile name security-5
huawei(config-wlan-security-prof-security-5)#authentication policy wapi
huawei(config-wlan-security-prof-security-5)#wapi wai certificate
huawei(config-wlan-security-prof-security-5)#wapi asu-server ip 10.10.10.1
huawei(config-wlan-security-prof-security-5)#wapi certificate ac import file-name huawei-ac.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate issuer import file-name huawei-issuer.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate asu import file-name huawei-asu.cer
huawei(config-wlan-security-prof-security-5)#wapi private-key import file-name ac-key.key...//-----对于证书和私钥合一的证书文件, 此配置可以省略
huawei(config-wlan-security-prof-security-5)#quit
```

3.11 配置 802.11n

配置 802.11n 为 WLAN 接入用户提供更高的“接入速率配置”。

背景信息

802.11n 作为 802.11 协议族的一个新协议, 支持 2.4GHz 和 5GHz 两个频段, 提高通讯速率的手段主要在于增加带宽和提高信道利用率两个方面。

- 增加带宽: 802.11n 通过将两个 20MHz 的带宽绑定在一起组成一个 40MHz 通讯带宽, 在实际工作时可以作为两个 20MHz 的带宽使用(一个为主带宽, 一个为次带宽, 收发数据时既可以 40MHz 的带宽工作, 也可以单个 20MHz 带宽工作), 这样可将速率提高一倍, 提高无线网络的吞吐量
- 提高信道利用率:

1. 802.11n 标准中采用 A-MPDU 聚合帧格式，即将多个 MPDU 聚合为一个 A-MPDU，只保留一个 PHY 头，删除其余 MPDU 的 PHY 头，减少了传输每个 MPDU 的 PHY 头的附加信息，同时也减少了 ACK 帧的数目，从而降低了协议的负荷，有效的提高网络吞吐量
2. 802.11n 支持在物理层的优化，提供短间隔功能。原 11a/g 的 GI 时长 800ns，而短间隔 Short GI 时长为 400ns，在使用 Short GI 的情况下，可提高 10% 的速率。

操作步骤

- 步骤 1** 使用 `wlan ac` 命令，进入 WLAN-AC 模式。
- 步骤 2** 使用 `radio-profile { id profile-id | name profile-name } *` 命令创建 Radio 模板。
- 步骤 3** 使用 `radio-type { 80211an | 80211bgn | 80211gn | 80211n }` 命令配置射频模板中的射频类型。
- 步骤 4** 使用 `80211n guard-interval-mode { short | normal }` 命令配置 GI 模式。
- 步骤 5** 使用 `80211n a-mpdu max-length-exponent exponent-value` 命令配置 MPDU 汇聚的帧长度大小值。
- 步骤 6** 使用 `quit` 命令退出 Radio 模板视图。
- 步骤 7** 使用 `radio ap-id ap-id radio-id radio-id` 命令进入射频的配置视图。
- 步骤 8** 使用 `channel { 20MHz | 40MHz-minus | 40MHz-plus }` `channel` 命令设置 AP 设备的信道和信道频宽。
- 步骤 9** 使用 `80211n mcs mcs-value` 命令配置射频类型为 11n 的射频的 MCS 值。
- 步骤 10** 使用 `radio enable` 命令使能指定射频。

---结束

3.12 查看 AP 信息

介绍如何查看 AP 的状态、认证模式、性能统计等详细信息。

背景信息

在日常维护工作中，可以在任意视图下选择执行以下命令，了解 AP 的运行状况。

操作步骤

- 使用 `display ap` 命令查看 AP 的索引、MAC 地址、SN 和工作状态等。
- 使用 `display ap-auth-mode` 命令查看 AP 的认证模式。
- 使用 `display ap-performance-statistic` 命令查看 AP 的性能统计信息。
- 使用 `display ap-profile` 命令查看 AP 的配置模板信息。
- 使用 `display ap-region` 命令查看 AP 域的信息。
- 使用 `display ap-run-info` 命令查看 AP 的运行信息。

- 使用 **display ap-type** 命令查看 AP 的设备类型信息。

----结束

4 WLAN 业务配置示例

关于本章

以示例方式介绍了不同 WLAN 组网场景中 QoS，接入安全，业务管理等配置。

[4.1 WLAN 组网概述](#)

WLAN 业务组网可以分为直连式组网和旁挂式网络组网两种典型组网方式。

[4.2 WLAN 业务配置流程](#)

介绍 WLAN 业务基本配置流程。

[4.3 配置 WLAN 业务示例](#)

介绍 AC+瘦 AP 组网环境下的典型业务配置示例。

4.1 WLAN 组网概述

WLAN 业务组网可以分为直连式组网和旁挂式网络组网两种典型组网方式。

背景信息

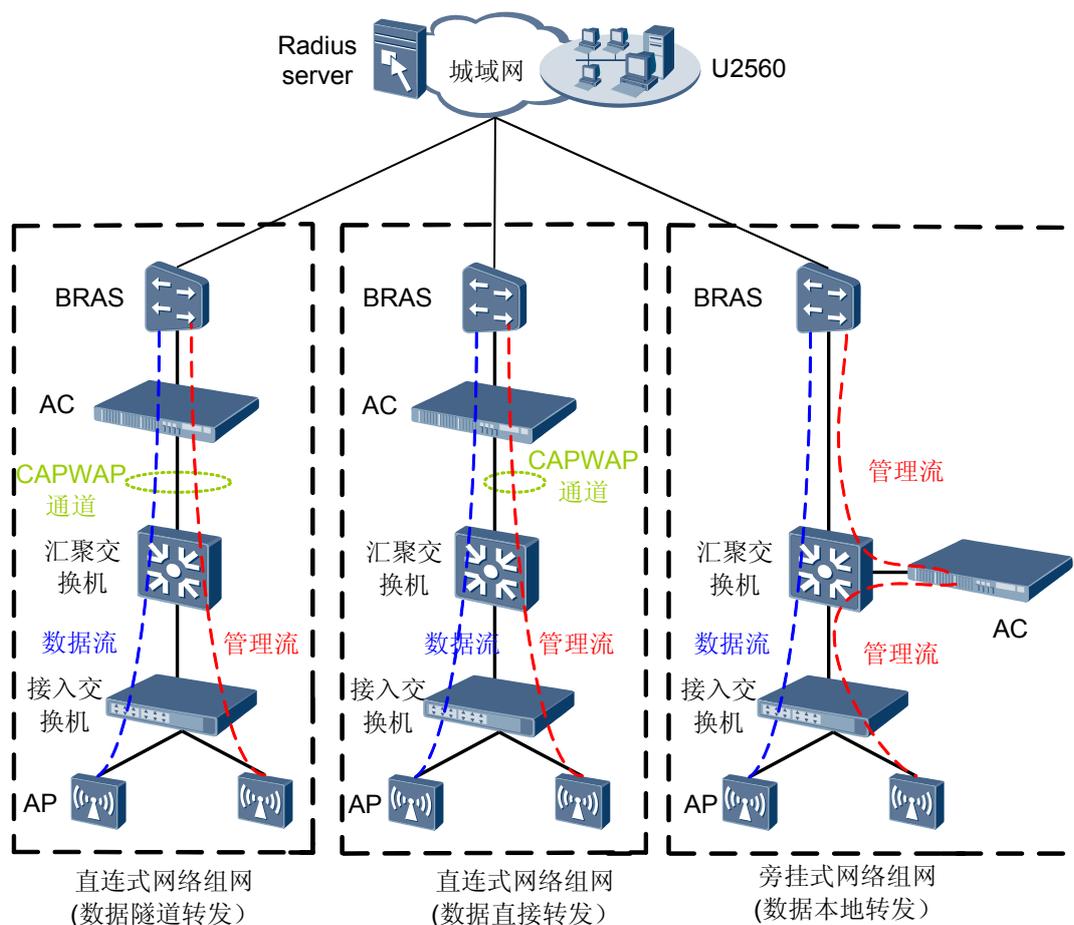
- 直连式组网是指 AC 挂在 BRAS 下面，AP 的数据业务和管理报文都由 AC 集中转发和处理，AP 和 AC 建立 CAPWAP 隧道。
在这种组网模式下，AC 具有很强的转发能力，能胜任汇聚层功能。适用于大规模集中部署的 WLAN 网络，并可以简化网络架构。
- 旁挂式组网是指 AC 旁挂在 BRAS 旁边，不承载数据业务转发功能，只对 AP 进行管理，AP 数据通过本地转发。
此种组网方式下，BRAS 管辖范围内的部署的 AP 都由 BRAS 旁挂的 AC 管理，AC 部署相对集中，适合于 AP 部署比较分散的全城热点部署的情况。

组网图

WLAN 业务典型组网图如[图 4-1](#)所示。

- 直连式网络组网（数据隧道转发）：AP 的管理流和业务流均封装在 CAPWAP 协议的隧道中，用不同的 VLAN 区分业务流。由 AC 进行转发。
- 直连式网络组网（数据直接转发）：AP 的管理流封装在 CAPWAP 协议的隧道中，而 AP 的数据业务流不加 CAPWAP 封装，直接由 AP 发送到 AC，再由 AC 透传至上层设备中。
- 旁挂式网络组网（数据本地转发）：AP 管理流必须通过 AC 处理，AP 的数据流不经过 AC，直接本地转发。同时 AC 的管理流通过 BRAS 处理。

图 4-1 WLAN 业务典型接入组网图



4.2 WLAN 业务配置流程

介绍 WLAN 业务基本配置流程。

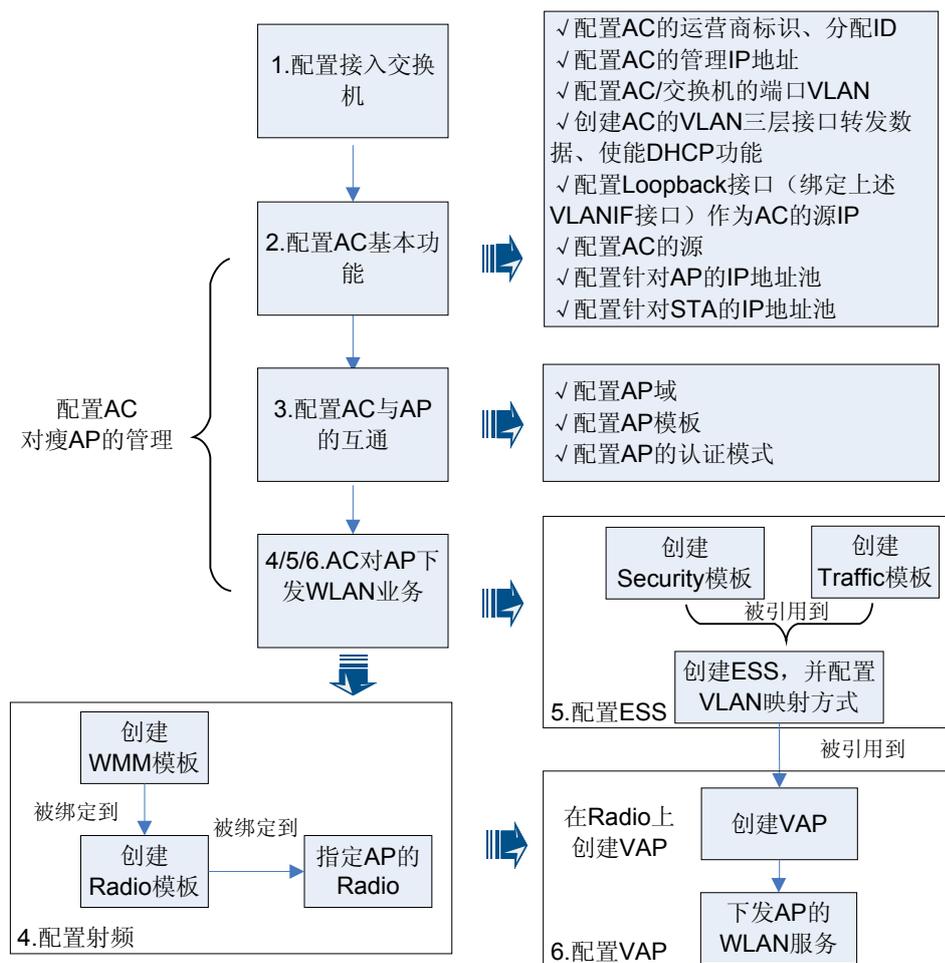
配置流程

WLAN 业务的配置流程如图 4-2 所示，可以分为 6 个部分：

1. 配置 AP 的上层交换机
2. AC 基础配置
3. 配置 AC 与 AP 的互通
4. 配置 AP 的射频
5. 配置 AP 的 ESS
6. 配置 VAP，下发 WLAN 服务

具体的配置过程请参见“业务示例”。

图 4-2 WLAN 业务的配置流程



4.3 配置 WLAN 业务示例

介绍 AC+瘦 AP 组网环境下的典型业务配置示例。

4.3.1 配置业务示例-直连式二层组网，数据隧道转发

直连式组网适用于大规模集中部署的 WLAN 网络，并可以简化网络架构。

业务需求

WLAN 网络中，AC 位置较低，AP 大规模集中部署。

AC 与 AP 在同一个局域网内，且 AC 与 AP 在同一网段内。

AP 的数据流和管理流都采用隧道转发模式，由 AC 集中转发和处理。该模式对 AC 性能要求比较高，且配置相对简单（只需配置 AC 到 STA 的业务网关即可）。

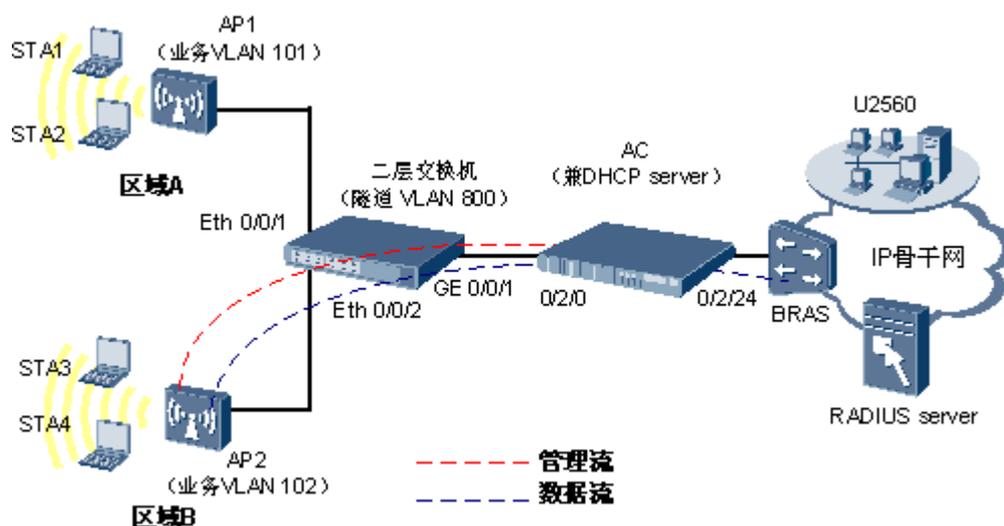
组网说明

网络供应商为某两个临近小区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 和 AP 之间采用“直连式”二层组网，组网如图 4-3 所示，由 AC 下发业务 VLAN，管理 VLAN 和业务 VLAN 都封装在 CAPWAP 隧道中。由二层交换机给 AP 管理报文打管理 VLAN tag。到达 AC 后，AP 的管理流终止，AC 解开 CAPWAP 头，再根据内层业务 VLAN 将业务流转发到上层设备中。

AC 同时作为 DHCP server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

图 4-3 直连式组网网络（二层组网，数据隧道转发）



前提条件

- AP、AC、二层交换机正常上电。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。

数据规划

表 4-1 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 800（由二层交换机打 VLAN tag）
AP Region	AP1：101

配置项	数据
	AP2: 102
ESS	<ul style="list-style-type: none"> ● 名称: huawei-1 ● SSID: huawei-F4 ● 映射模式: AP 域映射 ● 映射 VLAN: 101 ● 数据转发模式: 隧道转发
	<ul style="list-style-type: none"> ● 名称: huawei-2 ● SSID: huawei-F5 ● 映射模式: AP 域映射 ● 映射 VLAN: 102 ● 数据转发模式: 隧道转发
上网业务 VLAN	STA1/STA2: VLAN 101 (由 AC 下发)
	STA3/STA4: VLAN 102 (由 AC 下发)
二层交换机上 VLAN	接入 AP 端口配置为 Trunk 类型, 缺省 VLAN 为 800, 接入 AC 的端口配置为 Trunk 类型, 允许 VLAN 800 通过。AP 的管理 VLAN 和业务 VLAN 都封装在 CAPWAP 隧道中。
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址(Meth 0 接口)	10.11.104.2/24
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24
STA1,STA2 地址池	192.168.3.2 ~ 192.168.3.254/24
STA3,STA4 地址池	192.168.4.2 ~ 192.168.4.254/24
AP 管理网关	192.168.1.1/24
DHCP 服务器	AC 作为 DHCP 服务器, 给 AP 分配 IP 地址。

操作步骤

步骤 1 配置二层交换机, 使 AP 与 AC 二层互通。

1. 配置二层交换机连接 AP 的以太网端口 (Eth 0/0/1 和 Eth 0/0/2) 类型为 Trunk 类型, 缺省 VLAN 为 800。



说明

此处配置以华为 S3300 系列交换机为例, 其他类型交换机请参考对应《命令手册》。

**注意**

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置交换机连接 AC 的 GE 端口 1（GE 0/0/1）类型为 Trunk 类型，允许 VLAN 800 通过。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

步骤 2 AC 基础配置。

1. 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。

#配置 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

2. 配置 AC 连接二层交换机端口 VLAN。

#创建 VLAN 101、102 和 800。

```
huawei(config)#vlan 101
huawei(config)#vlan 102
huawei(config)#vlan 800
```

#将 VLAN 800 加入业务端口 0/2/0。

```
huawei(config)#port vlan 800 0/2 0
```

3. 配置 AC 的上行端口。

#端口 0/2/24 为上行端口，将 VLAN 101 和 VLAN 102 加入上行端口。

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

4. 在 AC 上创建 VLANIF。

#VLANIF 800 的 IP 地址为 192.168.1.1，作为数据转发的三层接口。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

使能 VLANIF 800 的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 分配 IP 地址。

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

使能 VLANIF 101, VLANIF 102 的 DHCP 功能，使 AC 兼作 DHCP server，为 STA 分配 IP 地址。

```
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.3.1 255.255.255.0
huawei(config-if-vlanif101)#dhcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.4.1 255.255.255.0
huawei(config-if-vlanif102)#dhcps enable
huawei(config-if-vlanif102)#quit
```

5. 设置 AC 的源。

#配置 VLANIF 800 作为 AC 的源。

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

6. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ap-server 对应 VLAN 800。

 说明

IP 地址池的网关地址必须与管理 VLAN 的三层接口 VLANIF 的 IP 地址相同，用于定义 AP 上线后获取 IP 的地址池。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

#(可选)配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei(config-ip-pool-ap-server)#quit
```

 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

7. 在 AC 上配置 STA 的 IP 地址池。

```
huawei(config)#ip pool stal-server
It's successful to create an IP address pool
huawei(config-ip-pool-stal-server)#gateway 192.168.3.1 255.255.255.0
huawei(config-ip-pool-stal-server)#section 0 192.168.3.2 192.168.3.254
huawei(config-ip-pool-stal-server)#quit
huawei(config)#ip pool sta2-server
It's successful to create an IP address pool
```

```
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei(config-ip-pool-sta2-server)#quit
```

步骤 3 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（type-id 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

3. 配置 AP 域。

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

4. 配置 API 加入 AP 域 101，AP2 加入 AP 域 102。

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:
ap id 1

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
    ap id 2

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

步骤 4 配置 AP 对应的射频。

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

步骤 5 配置 AP 对应的 ESS。

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile
traffic-1 security-profile security-1
```

说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
```

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0
```

步骤 6 配置数据转发模式。

```
#配置数据转发模式为根据 ESS 转发。
huawei(config-wlan-ac-view)#forward-mode type ess
#配置名为“huawei-1”和“huawei-2”的 ESS 采用隧道转发模式。
huawei(config-wlan-ac-view)#forward-mode ess 0 mode tunnel
huawei(config-wlan-ac-view)#forward-mode ess 1 mode tunnel
```

步骤 7 配置 AP 对应的 VAP，下发 WLAN 服务。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

---结束

操作结果

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-F4 和 huawei-F5 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

配置文件

AC 上的配置文件

```
#
[vlan-config]
<vlan-config>
vlan 800
vlan 101 to 102
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0
#
[vlanif]
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
<vlanif800>
interface vlanif 800
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
```

```
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id etc ac id 1
wlan ac
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode tunnel
forward-mode ess 1 mode tunnel
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
#
<ip-pool-sta1-server>
ip pool sta1-server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

4.3.2 配置业务示例-旁挂式二层组网，数据本地转发

旁挂式组网适用于 AC 部署相对集中，AP 部署比较分散的全城热点部署的 WLAN 网络。

业务需求

WLAN 网络中，AC 位置较低，AP 部署比较分散。

AC 与 AP 在同一个局域网内，且 AC 与 AP 在同一网段内。

AP 的数据流和管理流都采用直接转发模式，该模式对 AC 性能要求比较低。

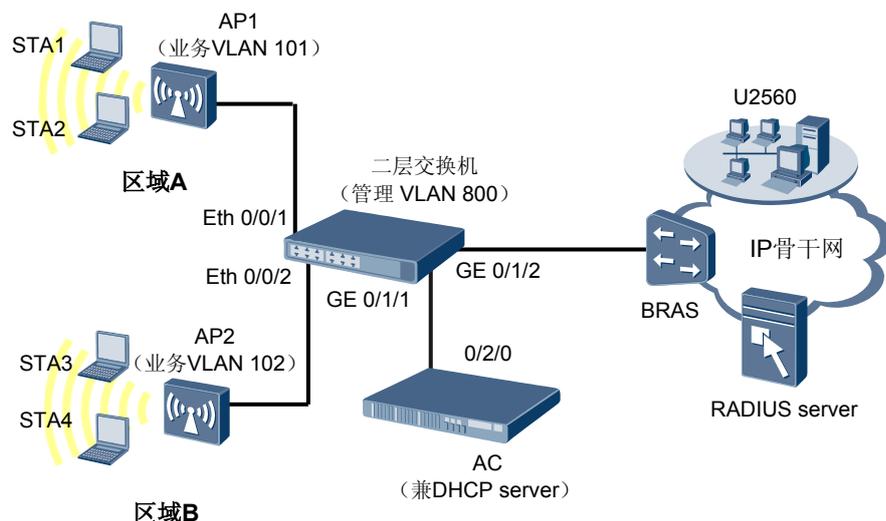
组网说明

网络供应商为某两个临近小区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 和 AP 之间采用“旁挂式”二层组网，组网如图 4-4 所示，由 AC 下发业务 VLAN，二层交换机透传所有的业务 VLAN，并给 AP 管理报文打管理 VLAN tag。AC 同时作为 DHCP server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

AP1 和 AP2 的业务数据都是由本地直接转发，AC 只对 AP 进行管理。

图 4-4 旁挂式组网网络（二层组网，数据本地转发）



前提条件

- AP、AC、二层交换机正常上电。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接用户的认证和计费的要求，已完成相应的配置。

数据规划

表 4-2 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式

配置项	数据
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 800（由二层交换机打 VLAN tag）
AP Region	AP1： 101
	AP2： 102
ESS	<ul style="list-style-type: none"> ● 名称： huawei-1 ● SSID： huawei-F4 ● 映射模式： AP 域映射 ● 映射 VLAN： 101 ● 数据转发模式： 直接转发
	<ul style="list-style-type: none"> ● 名称： huawei-2 ● SSID： huawei-F5 ● 映射模式： AP 域映射 ● 映射 VLAN： 102 ● 数据转发模式： 直接转发
上网业务 VLAN	STA1/STA2： VLAN 101（由 AC 下发）
	STA3/STA4： VLAN 102（由 AC 下发）
二层交换机上 VLAN	<ul style="list-style-type: none"> ● 接 AP1 端口（Eth 0/0/1）： Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 101 和 800 通过 ● 接 AP2 端口（Eth 0/0/2）： Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 102 和 800 通过 ● 接 AC 端口（GE 0/0/1）： Trunk 类型，允许 VLAN 800 通过 ● 接 BARS 端口（GE 0/0/2）： Trunk 类型，允许 VLAN 101/102 通过
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址(Meth 0 接口)	10.11.104.2/24
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24
AP 管理网关	192.168.1.1/24
STA1,STA2 地址池	192.168.3.2 ~ 192.168.3.254/24
STA3,STA4 地址池	192.168.4.2 ~ 192.168.4.254/24
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址。

操作步骤

步骤 1 配置二层交换机，使 AP 与 AC 二层互通。

1. 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800，分别允许 VLAN 101/800 和 VLAN 102/800 通过。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考对应《命令手册》。



注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan 101
[huawei-vlan101]quit
[huawei]vlan 102
[huawei-vlan102]quit
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置交换机连接 AC 的 GE 端口（GE 0/0/1）类型为 Trunk 类型，允许 VLAN 800 通过。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

3. 配置交换机连接 BRAS 的 GE 端口（GE 0/0/2）类型为 Trunk 类型，允许 VLAN 101、VLAN 102 通过。

```
[huawei]interface GigabitEthernet 0/0/2
[huawei-GigabitEthernet0/0/2]port link-type trunk
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 101
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 102
[huawei-GigabitEthernet0/0/2]quit
```

步骤 2 AC 基础配置。

1. 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。

#配置 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

2. 配置 AC 连接二层交换机端口 VLAN。

#创建 VLAN 101,102,800。

```
huawei(config)#vlan 800
```

```
huawei(config)#vlan 101 to 102
```

#将 VLAN 800 加入业务端口 0/2/0。

```
huawei(config)#port vlan 800 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
```

3. 在 AC 上创建 VLANIF。

#VLANIF 800 的 IP 地址为 192.168.1.1，作为数据转发的三层接口。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

使能 VLANIF 800 的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 分配 IP 地址。

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

使能 VLANIF 101,VLANIF 102 的 DHCP 功能，使 AC 兼作 DHCP server，为 STA 分配 IP 地址。

```
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.3.1 255.255.255.0
```

```
huawei(config-if-vlanif101)#dhcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.4.1 255.255.255.0
```

```
huawei(config-if-vlanif102)#dhcps enable
huawei(config-if-vlanif102)#quit
```

4. 设置 AC 的源。

#配置 VLANIF 800 作为 AC 的源。

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

5. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ap-server 对应 VLAN 800。

说明

IP 地址池的网关地址必须与管理 VLAN 的三层接口 VLANIF 的 IP 地址相同，用于定义 AP 上线后获取 IP 的地址池。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

#（可选）配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei(config-ip-pool-ap-server)#quit
```

 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

6. 在 AC 上配置 STA 的 IP 地址池。

```
huawei(config)#ip pool stal-server
It's successful to create an IP address pool
huawei(config-ip-pool-stal-server)#gateway 192.168.3.1 255.255.255.0
huawei(config-ip-pool-stal-server)#section 0 192.168.3.2 192.168.3.254
huawei(config-ip-pool-stal-server)#quit
huawei(config)#ip pool sta2-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei(config-ip-pool-sta2-server)#quit
```

步骤 3 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（type-id 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

3. 配置 AP 域。

```
#AP 域 ID 分别为 101 和 102。
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

4. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
    ap id 1
```

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
    ap id 2
```

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

步骤 4 配置 AP 对应的射频。

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

步骤 5 配置 AP 对应的 ESS。

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1
```

```
#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，  
Security 模板“security-1”  
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile  
traffic-1 security-profile security-1
```

 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101  
Success: 1  
Failure: 0  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102  
Success: 1  
Failure: 0
```

步骤 6 配置数据转发模式。

#配置数据转发模式为根据 ESS 转发。

```
huawei(config-wlan-ac-view)#forward-mode type ess
```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用直接转发模式。

```
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward  
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

步骤 7 配置 AP 对应的 VAP，下发 WLAN 服务。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

 说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1  
huawei(config-wlan-ac-view)#commit ap 2  
huawei(config-wlan-ac-view)#quit
```

----结束

操作结果

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-F4 和 huawei-F5 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

配置文件

AC 上的配置文件

```
#  
[vlan-config]  
<vlan-config>  
vlan 800  
vlan 101 to 102
```

```

port vlan 101 to 102 0/2 0
port vlan 800 0/2 0
#
[vlanif]
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
<vlanif800>
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id etc ac id 1
wlan ac
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode direct-forward
forward-mode ess 1 mode direct-forward
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
#
<ip-pool-sta1-server>

```

```
ip pool stal-server
 gateway 192.168.3.1 255.255.255.0
 section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-server
 gateway 192.168.4.1 255.255.255.0
 section 0 192.168.4.2 192.168.4.254
#
return
```

4.3.3 配置业务示例-直连式三层组网，数据本地转发

直连式组网适用于大规模集中部署的 WLAN 网络，并可以简化网络架构。

业务需求

WLAN 网络中，AC 位置较高，AP 大规模集中部署。

AP 的数据流采用直接转发模式，该模式对 AC 性能要求相对较低，且配置相对复杂一些（需配置 AP 到 AC 及 STA 的业务网关）。

组网说明

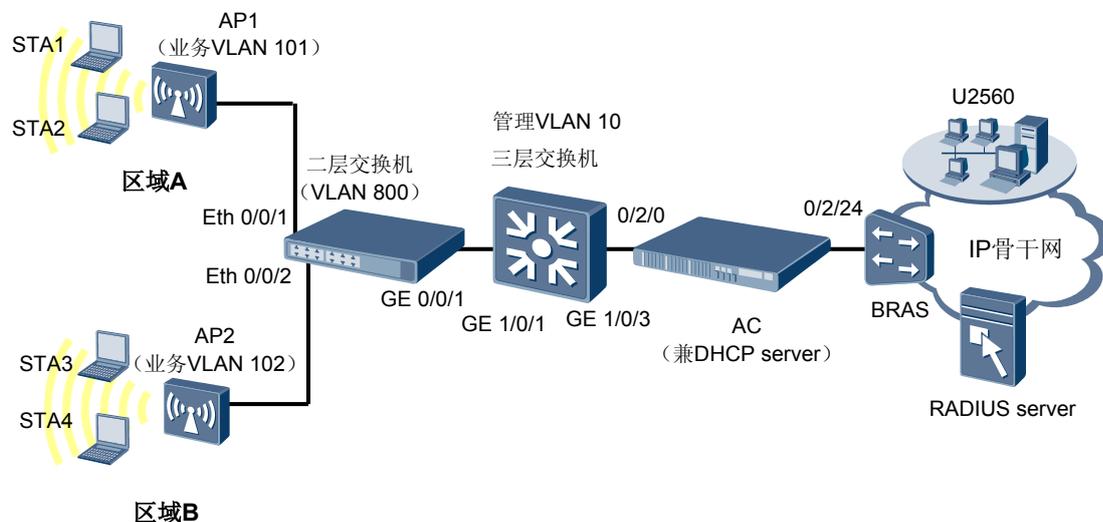
网络供应商为某两个相隔较远的区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。区域内的用户按流量计费。

AC 采用“直连式”三层组网，组网如图 4-5 所示，由 AC 下发业务 VLAN，二层交换机透传所有的业务 VLAN，并给 AP 管理报文打管理 VLAN tag。

AC 同时作为 DHCP Server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

AP1 和 AP2 的业务数据都是由本地直接转发，AC 只对 AP 进行管理。即 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止；AP 业务流不加 CAPWAP 封装，而直接由 AP 发送到三层交换机，再由三层交换机透传至上层设备中。

图 4-5 直连式组网网络（三层组网，数据本地转发）



前提条件

- AP、AC、二层和三层交换机正常工作，交换机上 VLAN 已经创建。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。

数据规划

表 4-3 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 10
AP Region	AP1：101
	AP2：102
ESS	<ul style="list-style-type: none"> ● 名称：huawei-1 ● SSID：huawei-F4 ● 映射模式：AP 域映射 ● 映射 VLAN：101 ● 数据转发模式：直接转发
	<ul style="list-style-type: none"> ● 名称：huawei-2 ● SSID：huawei-F5 ● 映射模式：AP 域映射 ● 映射 VLAN：102 ● 数据转发模式：直接转发
上网业务 VLAN	STA1/STA2：VLAN 101（由 AC 下发）
	STA3/STA4：VLAN 102（由 AC 下发）
二层交换机上 VLAN	<ul style="list-style-type: none"> ● 接 AP1 端口（Eth 0/0/1）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 101/800 通过 ● 接 AP2 端口（Eth 0/0/2）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 102/800 通过 ● 接三层交换机端口（GE 0/0/1）：Trunk 类型，允许 VLAN 101/102/800 通过
三层交换机上 VLAN	<ul style="list-style-type: none"> ● 接二层交换机端口（GE 1/0/1）：Trunk 类型，允许 VLAN 101/102/800 通过 ● 接 AC 端口（GE 1/0/3）：Hybrid 类型，允许 VLAN 101/102/800 通过

配置项	数据
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址	192.168.1.1/32
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24
AP 管理网关	192.168.1.1/24（三层交换机上）
STA1,STA2 地址池	192.168.3.2 ~ 192.168.3.254/24
STA3,STA4 地址池	192.168.4.2 ~ 192.168.4.254/24
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址

操作步骤

步骤 1 配置交换机，使 AP 与 AC 互通。

- 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800，允许 VLAN 101/800 和 VLAN 102/800 通过。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考对应《命令手册》。



注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan batch 101 102 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

- 配置二层交换机连接三层交换机的 GE 端口（GE 0/0/1）透传所有管理 VLAN 与业务 VLAN。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

- 配置三层交换机连接二层交换机的 GE 端口(GE 1/0/1)透传所有管理 VLAN 与业务 VLAN。



说明

此处配置以华为 S9300 系列交换机为例，其他类型交换机请参考对应《命令手册》。

- ```
[huawei]vlan batch 101 102 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet1/0/1]quit
```
- 配置三层交换机连接 AC 的 GE 端口(GE 1/0/3)透传管理 VLAN。

```
[huawei]vlan 10
[huawei-vlan10]quit
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type hybrid
[huawei-GigabitEthernet1/0/3]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/3]quit
```
  - 配置三层交换机的 DHCP Relay 功能。

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]quit
```
  - 创建 VLAN10, 并配置 VLANIF 10 的 IP 地址为 192.168.2.1, 作为连接 AC 的三层接口。

```
[huawei]interface Vlanif 10
[huawei-Vlanif10]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif10]quit
```

## 步骤 2 AC 基础配置。

- 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。  
#配置 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。  
huawei(config)#wlan ac-global carrier id ctc ac id 1
- 配置 AC 连接二层交换机端口 VLAN。  
#创建 VLAN 101、102、10。  
huawei(config)#vlan 101  
huawei(config)#vlan 102  
huawei(config)#vlan 10  
#将 VLAN 10,VLAN 101,VLAN 102 加入业务端口 0/2/0。  
huawei(config)#port vlan 10 0/2 0  
huawei(config)#port vlan 101 to 102 0/2 0
- 在 AC 上创建 VLANIF。  
#VLANIF 10 的 IP 地址为 192.168.2.2, 作为连接三层交换机的三层接口。  
huawei(config)#vlan 10  
huawei(config)#interface vlanif 10  
huawei(config-if-vlanif10)#ip address 192.168.2.2 255.255.255.0  
{ <cr>|description<K>|sub<K> }:  
  
Command:  
ip address 192.168.2.2 255.255.255.0  
huawei(config)#quit  
使能 VLANIF 101,VLANIF 102 的 DHCP 功能, 使 AC 兼作 DHCP server, 为 STA 分配 IP 地址。  
huawei(config)#interface vlanif 101  
huawei(config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0  
{ <cr>|description<K>|sub<K> }:  
  
Command:  
ip address 192.168.3.1 255.255.255.0  
huawei(config)#quit  
huawei(config)#interface vlanif 102  
huawei(config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0  
{ <cr>|description<K>|sub<K> }:

```
Command:
ip address 192.168.4.1 255.255.255.0
huawei(config)#quit
```

使能 VLANIF 接口的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 和 STA 分配 IP 地址。

```
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#dhcps enable
huawei(config-if-vlanif10)#quit
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#dhcps enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#dhcps enable
huawei(config-if-vlanif102)#quit
```

#### 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 和 STA 从 AC 上获取 IP 地址。

#### 4. 设置 AC 的源。

#配置 vlanif 10 作为 AC 的源。

#### 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

#### 5. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ap-server 对应 vlanif 10。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

#配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.2.2
huawei(config-ip-pool-ap-server)#quit
```

#### 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

#### 6. 在 AC 上配置 STA 的 IP 地址池。

```
huawei(config)#ip pool stal-server
It's successful to create an IP address pool
huawei(config-ip-pool-stal-server)#gateway 192.168.3.1 255.255.255.0
huawei(config-ip-pool-stal-server)#section 0 192.168.3.2 192.168.3.254
huawei(config-ip-pool-stal-server)#quit
huawei(config)#ip pool sta2-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei(config-ip-pool-sta2-server)#quit
```

#### 7. 配置 AC 到 192.168.1.0 网段的路由。

```
huawei(config)#ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

### 步骤 3 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
huawei(config-wlan-ac-view)#quit
```

2. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

| ID | Type    |
|----|---------|
| 0  | WA601   |
| 1  | WA631   |
| 2  | WA651   |
| 3  | WA602   |
| 4  | WA632   |
| 5  | WA652   |
| 6  | WA603SN |
| 7  | WA603DN |
| 8  | WA633SN |
| 11 | WA603DE |
| 12 | WA653DE |
| 14 | WA653SN |

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（type-id 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

| AP ID | AP Type | Profile ID | Region ID | AP State |
|-------|---------|------------|-----------|----------|
| 1     | WA601   | 0          | 0         | normal   |
| 2     | WA601   | 0          | 0         | normal   |

Total number: 2

3. 配置 AP 域。

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

4. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 1

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:  
ap id 2

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

#### 步骤 4 配置 AP 对应的射频。

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)#radio-profile name radio-1 id 1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

#### 说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

#### 步骤 5 配置 AP 对应的 ESS。

1. 创建 Security 模板。

#Security 模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#Traffic 模板名为“traffic-1”，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1 id 1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile tra
ffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile tra
ffic-1 security-profile security-1
```

#### 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0
```

**步骤 6** 配置数据转发模式。

```
#配置数据转发模式为根据 ESS 转发。
huawei(config-wlan-ac-view)#forward-mode type ess
#配置名为“huawei-1”和“huawei-2”的 ESS 采用数据直接转发模式。
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

**步骤 7** 配置 AP 对应的 VAP，下发 WLAN 服务。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1 wlan 1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2 wlan 1
```

 说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----结束

## 操作结果

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-F4 和 huawei-F5 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

## 配置文件

AC 上的配置文件

```
#
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
```

```
wlan ac-global carrier id etc ac id 1
wlan ac
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode direct-forward
forward-mode ess 1 mode direct-forward
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2
#
<ip-pool-stal-server>
ip pool stal-server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip-pool-sta2-server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

### 4.3.4 配置业务示例-旁挂式三层组网，数据隧道转发

旁挂式组网适用于 AC 部署相对集中，AP 部署比较分散的全城热点部署的 WLAN 网络。

## 业务需求

WLAN 网络中，AC 位置较高，AP 部署比较分散。

AP 的数据流采用隧道转发模式，由 AC 集中转发和处理。该模式对 AC 性能要求比较高，且配置相对简单（只需配置 AC 到 STA 的业务网关即可）。

## 组网说明

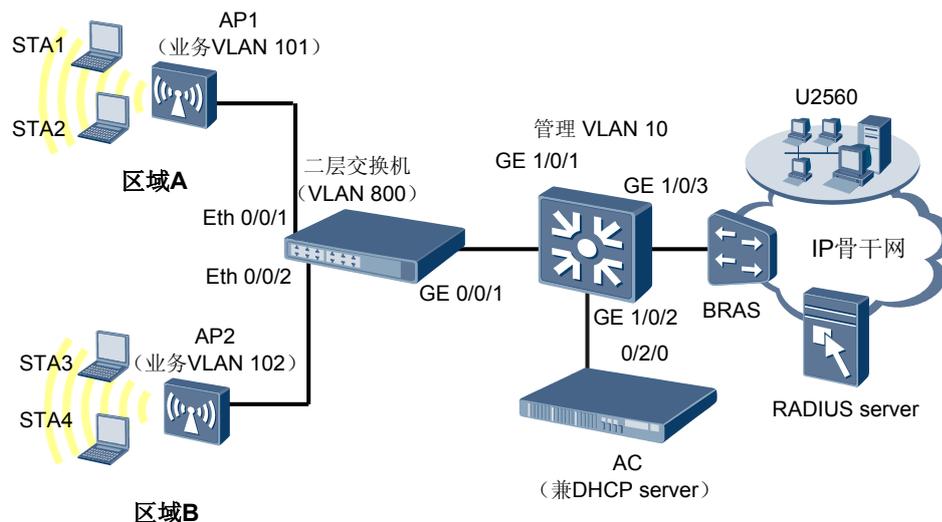
网络供应商为某两个相隔较远的区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。区域内的用户按流量计费。

AC 采用“旁挂式”三层组网，组网如图 4-6 所示，由 AC 下发业务 VLAN，二层交换机透传所有的业务 VLAN，并给 AP 管理报文打管理 VLAN tag。

AC 同时作为 DHCP Server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

AP1 和 AP2 上业务数据采用隧道转发模式。

图 4-6 旁挂式组网网络（三层组网，数据隧道转发）



## 前提条件

- AP、AC、二层和三层交换机正常工作，交换机上 VLAN 已经创建。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。

## 数据规划

表 4-4 数据规划表

配置项	数据
WLAN 服务	AP 认证类型: WEP 认证策略, Open-system 认证模式
	认证报文的加密类型: 不加密
AP 管理 VLAN	VLAN 10
AP Region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> <li>● 名称: huawei-1</li> <li>● SSID: huawei-F4</li> <li>● 映射模式: AP 域映射</li> <li>● 映射 VLAN: 101</li> <li>● 数据转发模式: 隧道转发</li> </ul>
	<ul style="list-style-type: none"> <li>● 名称: huawei-2</li> <li>● SSID: huawei-F5</li> <li>● 映射模式: AP 域映射</li> <li>● 映射 VLAN: 102</li> <li>● 数据转发模式: 隧道转发</li> </ul>
上网业务 VLAN	STA1/STA2: VLAN 101 (由 AC 下发)
	STA3/STA4: VLAN 102 (由 AC 下发)
二层交换机上 VLAN	<ul style="list-style-type: none"> <li>● 接 AP1 端口 (Eth 0/0/1): Trunk 类型, 缺省 VLAN ID 为 800, 允许 VLAN 800 通过</li> <li>● 接 AP2 端口 (Eth 0/0/2): Trunk 类型, 缺省 VLAN ID 为 800, 允许 VLAN 800 通过</li> <li>● 接三层交换机端口 (GE 0/0/1): Trunk 类型, 允许 VLAN 800 通过</li> </ul>
三层交换机上 VLAN	<ul style="list-style-type: none"> <li>● 接二层交换机端口 (GE 1/0/1): Trunk 类型, 允许 VLAN 103/800/801 通过</li> <li>● 接 AC 端口 (GE 1/0/2): Hybrid 类型, 允许 VLAN 103/800/801 通过</li> <li>● 接 BRAS 端口 (GE 1/0/3): Trunk 类型, 允许 VLAN 101/102 通过</li> </ul>
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址	192.168.1.1/32
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24

配置项	数据
AP 管理网关	192.168.1.1/24（三层交换机上）
STA1,STA2 地址池	192.168.3.2 ~ 192.168.3.254/24
STA3,STA4 地址池	192.168.4.2 ~ 192.168.4.254/24
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址

## 操作步骤

### 步骤 1 配置交换机，使 AP 与 AC 互通。

1. 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800，允许 VLAN 800 通过。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考对应《命令手册》。



### 注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan batch 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 0
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置二层交换机连接三层交换机的 GE 端口（GE 0/0/1）透传所有管理 VLAN。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

3. 配置三层交换机连接二层交换机的 GE 端口(GE 1/0/1)透传所有管理 VLAN 与业务 VLAN。



说明

此处配置以华为 S9300 系列交换机为例，其他类型交换机请参考对应《命令手册》。

```
[huawei]vlan batch 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet1/0/1]quit
```

4. 配置三层交换机连接 AC 的 GE 端口(GE 1/0/2)透传管理 VLAN。

```
[huawei]vlan 10
[huawei-vlan10]quit
```

- ```
[huawei]interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2]port link-type hybrid
[huawei-GigabitEthernet1/0/2]port hybrid tagged vlan 10
[huawei-GigabitEthernet1/0/2]quit
```
- 配置三层交换机连接 BRAS 的 GE 端口(GE 1/0/3)透传业务 VLAN。

```
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type trunk
[huawei-GigabitEthernet1/0/3]port trunk allow-pass vlan 101 102
[huawei-GigabitEthernet1/0/3]quit
```
 - 配置三层交换机的 DHCP Relay 功能。

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]quit
```
 - 创建 VLAN10, 配置 VLANIF 10 的 IP 地址为 192.168.2.1, 作为连接 AC 的三层接口。

```
[huawei]interface Vlanif 10
[huawei-Vlanif1]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif1]quit
```

步骤 2 AC 基础配置。

- 配置全局 AC 参数 (运营商标识、全局 ID) 方便识别和管理。
#配置 AC 运营商标识为 CTC (CTC-中国电信, CMCC-中国移动, CUC-中国联通, other-其他运营商), 全局 AC ID 为 1。

```
huawei (config)#wlan ac-global carrier id ctc ac id 1
```
- 配置 AC 连接二层交换机端口 VLAN。
#创建 VLAN 101、102、10。

```
huawei (config)#vlan 101
huawei (config)#vlan 102
huawei (config)#vlan 10
```


#将 VLAN 10,VLAN 101,VLAN 102 加入业务端口 0/2/0。

```
huawei (config)#port vlan 10 0/2 0
huawei (config)#port vlan 101 to 102 0/2 0
```
- 在 AC 上创建 VLANIF。
#VLANIF 10 的 IP 地址为 192.168.2.2, 作为连接三层交换机的三层接口。

```
huawei (config)#vlan 10
uawei (config)#interface vlanif 10
huawei (config-if-vlanif1)#ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```


Command:

```
ip address 192.168.2.2 255.255.255.0
huawei (config)#quit
```


使能 VLANIF 101,VLANIF 102 的 DHCP 功能, 使 AC 兼作 DHCP server, 为 STA 分配 IP 地址。

```
huawei (config)#interface vlanif 101
huawei (config-if-vlanif101)#ip address 192.168.3.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```


Command:

```
ip address 192.168.3.1 255.255.255.0
huawei (config)#quit
huawei (config)#interface vlanif 102
huawei (config-if-vlanif102)#ip address 192.168.4.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```


Command:

```
ip address 192.168.4.1 255.255.255.0
huawei (config)#quit
```

使能 VLANIF 接口的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 和 STA 分配 IP 地址。

```
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#dhcp enable
huawei(config-if-vlanif10)#quit
huawei(config)#interface vlanif 101
huawei(config-if-vlanif101)#dhcp enable
huawei(config-if-vlanif101)#quit
huawei(config)#interface vlanif 102
huawei(config-if-vlanif102)#dhcp enable
huawei(config-if-vlanif102)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 和 STA 从 AC 上获取 IP 地址。

4. 设置 AC 的源。

#配置 vlanif 10 接口作为 AC 的源。

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

5. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ap-server 对应 vlanif 10。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

#配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.2.2
huawei(config-ip-pool-ap-server)#quit
```

 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

6. 在 AC 上配置 STA 的 IP 地址池。

```
huawei(config)#ip pool sta1-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta1-server)#gateway 192.168.3.1 255.255.255.0
huawei(config-ip-pool-sta1-server)#section 0 192.168.3.2 192.168.3.254
huawei(config-ip-pool-sta1-server)#quit
huawei(config)#ip pool sta2-server
It's successful to create an IP address pool
huawei(config-ip-pool-sta2-server)#gateway 192.168.4.1 255.255.255.0
huawei(config-ip-pool-sta2-server)#section 0 192.168.4.2 192.168.4.254
huawei(config-ip-pool-sta2-server)#quit
```

7. 配置 AC 到 192.168.1.0 网段的路由。

```
huawei(config)#ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

步骤 3 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
huawei(config-wlan-ac-view)#quit
```

2. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

| ID | Type |
|----|---------|
| 0 | WA601 |
| 1 | WA631 |
| 2 | WA651 |
| 3 | WA602 |
| 4 | WA632 |
| 5 | WA652 |
| 6 | WA603SN |
| 7 | WA603DN |
| 8 | WA633SN |
| 11 | WA603DE |
| 12 | WA653DE |
| 14 | WA653SN |

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（type-id 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

| AP ID | AP Type | Profile ID | Region ID | AP State |
|-------|---------|------------|-----------|----------|
| 1 | WA601 | 0 | 0 | normal |
| 2 | WA601 | 0 | 0 | normal |

Total number: 2

3. 配置 AP 域。

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

4. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:
ap id 1

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

Command:
ap id 2

```
huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit
```

步骤 4 配置 AP 对应的射频。

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#wmm-profile name wmm-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit
```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)#radio-profile name radio-1 id 1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

 说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

步骤 5 配置 AP 对应的 ESS。

1. 创建 Security 模板。

#Security 模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#Traffic 模板名为“traffic-1”，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1 id 1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile tra
ffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile tra
ffic-1 security-profile security-1
```

 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0
```

步骤 6 配置数据转发模式。

#配置数据转发模式为根据 ESS 转发。

```
huawei(config-wlan-ac-view)#forward-mode type ess
#配置名为“huawei-1”和“huawei-2”的 ESS 采用数据隧道转发模式。
huawei(config-wlan-ac-view)#forward-mode ess 0 mode tunnel
huawei(config-wlan-ac-view)#forward-mode ess 1 mode tunnel
```

步骤 7 配置 AP 对应的 VAP，下发 WLAN 服务。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1 wlan 1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2 wlan 1
```

说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----结束

操作结果

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-F4 和 huawei-F5 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

配置文件

AC 上的配置文件

```
#
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 13
port vlan 101 to 102 0/2 13
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
<vlanif101>
interface vlanif101
ip address 192.168.3.1 255.255.255.0
dhcp enable
#
<vlanif102>
interface vlanif102
ip address 192.168.4.1 255.255.255.0
dhcp enable
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
```

```
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 0 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 1 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
forward-mode ess 0 mode tunnel
forward-mode ess 1 mode tunnel
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2
#
<ip-pool-stal-server>
ip pool stal-server
gateway 192.168.3.1 255.255.255.0
section 0 192.168.3.2 192.168.3.254
#
<ip-pool-sta2-server>
ip pool sta2-server
gateway 192.168.4.1 255.255.255.0
section 0 192.168.4.2 192.168.4.254
#
return
```

4.3.5 配置业务示例-双链路热备保护，直连式二层组网

WLAN 网络中一个 AC 往往控制上千台 AP，上万个用户（STA），通过配置主备 AC 与 AP 间的双链路，确保 WLAN 网络的业务稳定运行。

业务需求

主备 AC 跨设备间保护。

主备 AC 同时与 AP 通信。

当系统检测到 AP 与主用 AC 之间的链路发生故障时，启动主备倒换，业务不中断。

AC 配置主备优先级，主用 AC 优先级高于备用 AC 优先级，当主用 AC 恢复正常，业务从备用 AC 切换到优先级较高的主用 AC。

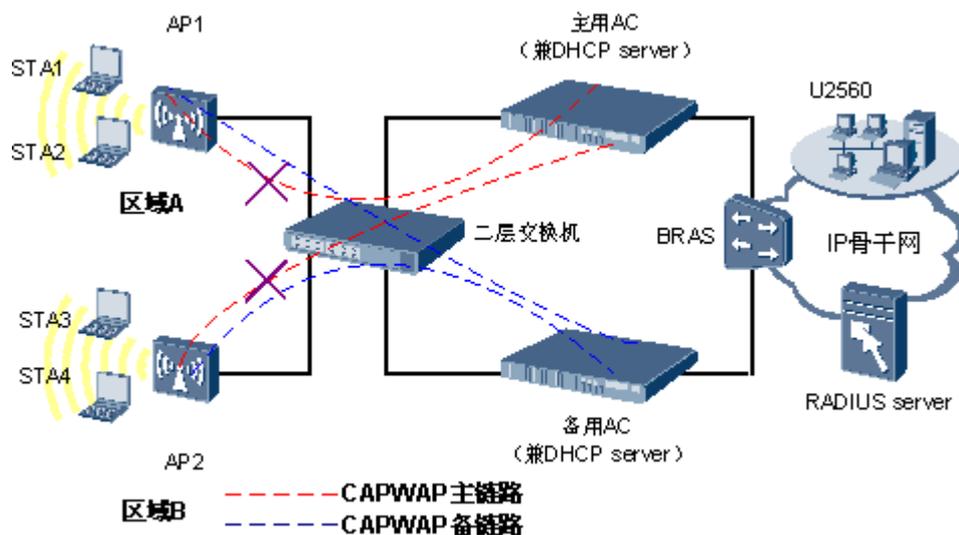
组网说明

网络供应商为某两个临近小区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 和 AP 之间采用“直连式”二层组网，组网如图 4-7 所示，主备 AC 上的业务配置相同，同时与 AP 通信。

STA 的 IP 地址由二层交换机分配；AP 的 IP 地址由 AC 分配，自动分配地址。

图 4-7 双链路热备保护（二层组网）



配置原则

- 确保 AP 能够同时跟主备 AC 通信。具体来讲，要求 AP 和主备 AC 属于同一个 VLAN，同时要求 AP 和主备 AC 的 IP 地址在同一个网段。
- AP 的 IP 地址分配：主备 AC 都开启 DHCP server 功能，配置 IP 地址池（包括配置网关地址，Option43 和 Option60，以及 section），给 AP 自动分配 IP 地址。需注意把主备 AC 的 IP 地址池错开，以避免分配的 IP 地址冲突。
- 指定 AC 的源接口：只能使用与 AP 地址同网段的 VLANIF 作为 AC 的源接口。
- WLAN 数据配置：
 - 在主备 AC 上分别打开双链路开关，并配置相应的主备优先级。
 - 在主备 AC 上配置其他 WLAN 相关数据，并确保二者的配置完全一致。



注意

- 不允许运营商 ID 配置为“other”。如果运营商 ID 配置为“other”，将导致双链路热备倒换后，STA 使用 WPA 或 WAPI 方式重新认证失败。
- 不支持通过 AC 给 STA 分配 IP 地址，或者 AC 作为 STA 的网关。

前提条件

- AP、AC、二层交换机正常上电。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。
- 已使用维护终端成功登录系统 AC 系统。

数据规划

表 4-5 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 800（由二层交换机打 VLAN tag）
AP Region	AP1：101
	AP2：102
ESS	<ul style="list-style-type: none"> ● 名称：huawei-1 ● SSID：huawei-F4 ● 映射模式：AP 域映射 ● 映射 VLAN：101 ● 数据转发模式：直接转发
	<ul style="list-style-type: none"> ● 名称：huawei-2 ● SSID：huawei-F5 ● 映射模式：AP 域映射 ● 映射 VLAN：102 ● 数据转发模式：直接转发
上网业务 VLAN	STA1/STA2：VLAN 101（由 AC 下发）
	STA3/STA4：VLAN 102（由 AC 下发）

配置项	数据
二层交换机上 VLAN	<ul style="list-style-type: none"> ● 接 AP1 端口（Eth 0/0/1）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 800，VLAN 101 通过 ● 接 AP2 端口（Eth 0/0/2）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 800，VLAN 102 通过 ● 接主 AC 端口（GE 0/0/1）：Trunk 类型，允许 VLAN 800，VLAN 101，VLAN 102 通过 ● 接备 AC 端口（GE 0/0/2）：Trunk 类型，允许 VLAN 800，VLAN 101，VLAN 102 通过
AC Carrier ID/AC ID	CTC/1
AP 管理 IP 地址池	192.168.1.3 ~ 192.168.1.254/24
AP 管理网关	192.168.1.1/24
STA1, STA2 IP 地址池	192.168.5.2 ~ 192.168.5.254
STA3, STA4 IP 地址池	192.168.6.2 ~ 192.168.6.254
主备 AC IP 地址	主用 AC: 192.168.1.1/24 备用 AC: 192.168.1.2/24
主备 AC 优先级	主用 AC: 1 备用 AC: 2
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址。二层接入交换机做 DHCP 服务器给 STA 分配 IP 地址。

操作步骤

- 配置二层交换机，使 AP 与 AC 二层互通。
 1. 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参加对应《命令手册》。



注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan batch 101 102 800
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
```

```
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置二层交换机连接 AC 的以太网端口（GE0/0/1 和 GE0/0/2）类型为 Trunk 类型，允许 VLAN 101，VLAN 102，VLAN 800 通过。

- 连接主用 AC

```
[huawei]interface gigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

- 连接备用 AC

```
[huawei]interface gigabitEthernet 0/0/2
[huawei-GigabitEthernet0/0/2]port link-type trunk
[huawei-GigabitEthernet0/0/2]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/2]quit
```

配置 STA 的 IP 地址池

```
[huawei] interface Vlanif 101
[huawei-Vlanif101] ip address 192.168.5.1 255.255.255.0
[huawei-Vlanif101] dhcp select interface
[huawei-Vlanif101] quit
[huawei] interface Vlanif 102
[huawei-Vlanif102] ip address 192.168.6.1 255.255.255.0
[huawei-Vlanif102] dhcp select interface
[huawei-Vlanif102] quit
```

● AC 基础配置。

1. 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。

- 主用 AC

配置主用 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

- 备用 AC

配置备用 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

 说明

必须保证主 AC 和备 AC 上配置的 AC ID 和运营商 ID 一致，避免业务配置中 BSSID 不一致导致主备切换后，业务切换失败。

2. 配置 AC 连接二层交换机端口 VLAN。

- 主用 AC

主 AC 上创建 vlan 101，vlan 102，vlan 800，并加入业务端口 0/2/0，并配置端口隔离。

```
huawei(config)#vlan 101 to 102
huawei(config)#vlan 800
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#port vlan 800 0/2 0
huawei(config)#isolate port 0/2/0
```

- 备用 AC

备 AC 上创建 vlan 101, vlan 102, vlan 800, 并加入业务端口 0/2/0, 并配置端口隔离。

```
huawei(config)#vlan 101 to 102
huawei(config)#vlan 800
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#port vlan 800 0/2 0
huawei(config)#isolate port 0/2/0
```

3. 配置 AC 的上行端口。

- 主用 AC

#端口 0/2/24 为上行端口, 将 VLAN 101 和 VLAN 102 加入上行端口。

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

- 备用 AC

#端口 0/2/24 为上行端口, 将 VLAN 101 和 VLAN 102 加入上行端口。

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

4. 在 AC 上创建 VLANIF。

- 主用 AC

#VLANIF 800 的 IP 地址为 192.168.1.1。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

使能 VLANIF 800 的 DHCP 功能, 使 AC 兼作 DHCP server, 为 AP 分配 IP 地址。

```
huawei(config-if-vlanif800)#dhcp enable
huawei(config-if-vlanif800)#quit
```

- 备用 AC

#VLANIF 800 的 IP 地址为 192.168.1.2。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.2 255.255.255.0
```

使能 VLANIF 800 的 DHCP 功能, 使 AC 兼作 DHCP server, 为 AP 分配 IP 地址。

```
huawei(config-if-vlanif800)#dhcp enable
huawei(config-if-vlanif800)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接, 可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

5. 设置 AC 的源。

- 主用 AC

#配置 VLANIF 800 作为 AC 的源。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

- 备用 AC

#配置 VLANIF 800 作为 AC 的源。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

6. 在 AC 上配置 AP 的 IP 地址池。

- 主用 AC

#IP 地址池 ap-server 对应 VLAN 800。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.3 192.168.1.128
```

- 备用 AC

#IP 地址池 ap-standby 对应 VLAN 800。

```
huawei(config)#ip pool ap-standby
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.2 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.129 192.168.1.254
```

● 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为 “sn-auth”。

- 主用 AC

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

- 备用 AC

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. 离线添加 AP。

- 主用 AC

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2 (type-id 为 0)。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

- 备用 AC

 说明

此时还未建立双链路，AP 在主用 AC 上线后，就不能在备用 AC 正常上线。
请先切断主链路，让 AP 在备用 AC 上线，进行以下操作。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2 (type-id 为 0)。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

3. 配置 AP 域。

- 主用 AC

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

- 备用 AC

#AP 域 ID 分别为 101 和 102。

```

huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit

```

4. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

- 主用 AC

```

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> } :

```

```

Command:
ap id 1

```

```

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> } :

```

```

Command:
ap id 2

```

```

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

```

- 备用 AC

```

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> } :

```

```

Command:
ap id 1

```

```

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> } :

```

```

Command:
ap id 2

```

```

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

```

● 配置 AP 对应的射频。

- 主用 AC

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```

huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit

```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```

huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit

```

- 备用 AC

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit
```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit
```

 说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

- 配置 AP 对应的 ESS。

- 主用 AC

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile
traffic-1 security-profile security-1
```

 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0
```

- 备用 AC

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```

huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit

```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```

huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit

```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```

huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1

```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```

huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile
traffic-1 security-profile security-1

```

说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```

huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0

```

- 配置数据转发模式。

- 主用 AC

#配置数据转发模式为根据 ESS 转发。

```

huawei(config-wlan-ac-view)#forward-mode type ess

```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用直接转发模式。

```

huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward

```

```

huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward

```

- 备用 AC

#配置数据转发模式为根据 ESS 转发。

```

huawei(config-wlan-ac-view)#forward-mode type ess

```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用直接转发模式。

```

huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward

```

```

huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward

```

- 配置 AP 对应的 VAP，下发 WLAN 服务。

- 主用 AC

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```

huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2

```

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

- 备用 AC

📖 说明

此时还未建立双链路，AP 在主用 AC 上线后，就不能在备用 AC 正常上线。

请先切断主链路，让 AP 在备用 AC 上线，进行以下操作。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

📖 说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

📖 说明

配置下发完成后，主链路和备链路都要保持连接状态。

● 开启 AC 的双链路热备保护开关

- 主用 AC

开启主用 AC 的双链路热备保护开关，配置备份 AC 的 IP 地址为 192.168.1.2/24，主用 AC 的主备优先级为 1。

📖 说明

通过配置 AC 的优先级来决定主备 AC，优先级高的 AC 作为主 AC，优先级低的 AC 作为备 AC。数字越小，优先级越高。优先级相同情况下 AC 负载轻的为主 AC；负载相同情况下比较 IP 地址，IP 地址小的 AC 为主 AC。

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.1.2 priority 1
```

- 备用 AC

开启备用 AC 的双链路热备保护开关，配置备份 AC 的 IP 地址为 192.168.1.1/24，备用 AC 的主备优先级为 2。

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.1.1 priority 2
```

----结束

操作结果

当系统检测到 AP 与主用 AC 之间的链路发生故障时，启动主备倒换，业务不中断；当主用 AC 恢复正常时，业务切换到主用 AC。

配置文件

主 AC 上的配置文件：

```
#
[vlan-config]
<vlan-config>
```

```

vlan 101 to 102
vlan 800
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0
#
[vlanif]
<vlanif800>
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.1.2 priority 1
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.3 192.168.1.128
#
return
备 AC 上的配置文件:
#
[vlan-config]
<vlan-config>
vlan 101 to 102
vlan 800
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
port vlan 800 0/2 0

```

```

#
[vlanif]
<vlanif800>
interface vlanif 800
ip address 192.168.1.2 255.255.255.0
dhcp enable
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.1.1 priority 2
wlan ac source interface vlanif 800
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-ap-standby>
ip pool ap-standby
gateway 192.168.1.2 255.255.255.0
section 0 192.168.1.129 192.168.1.254
#
return
二层交换机上的配置文件：
#
vlan batch 101 102 800
#
interface Vlanif101
ip address 192.168.5.1 255.255.255.0
dhcp select interface
#
interface Vlanif102
ip address 192.168.6.1 255.255.255.0
dhcp select interface
#
interface Ethernet0/0/1
port link-type trunk

```

```
port trunk pvid vlan 800
port trunk allow-pass vlan 101 800
port-isolate enable group 1
#
interface Ethernet0/0/2
port link-type trunk
port trunk pvid vlan 800
port trunk allow-pass vlan 102 800
port-isolate enable group 1
#
interface GigabitEthernet0/0/1
port hybrid tagged vlan 101 to 102 800
#
interface GigabitEthernet0/0/2
port hybrid tagged vlan 101 to 102 800
#
return
```

4.3.6 配置业务示例-双链路热备保护，旁挂式三层组网

WLAN 网络中一个 AC 往往控制上千台 AP，上万个用户（STA），通过配置主备 AC 与 AP 间的双链路，确保 WLAN 网络的业务稳定运行。

业务需求

主备 AC 跨设备间保护。

主备 AC 同时与 AP 通信。

当系统检测到 AP 与主用 AC 之间的链路发生故障时，启动主备倒换，业务不中断。

AC 配置主备优先级，主用 AC 优先级高于备用 AC 优先级，当主用 AC 恢复正常，业务从备用 AC 切换到优先级较高的主用 AC。

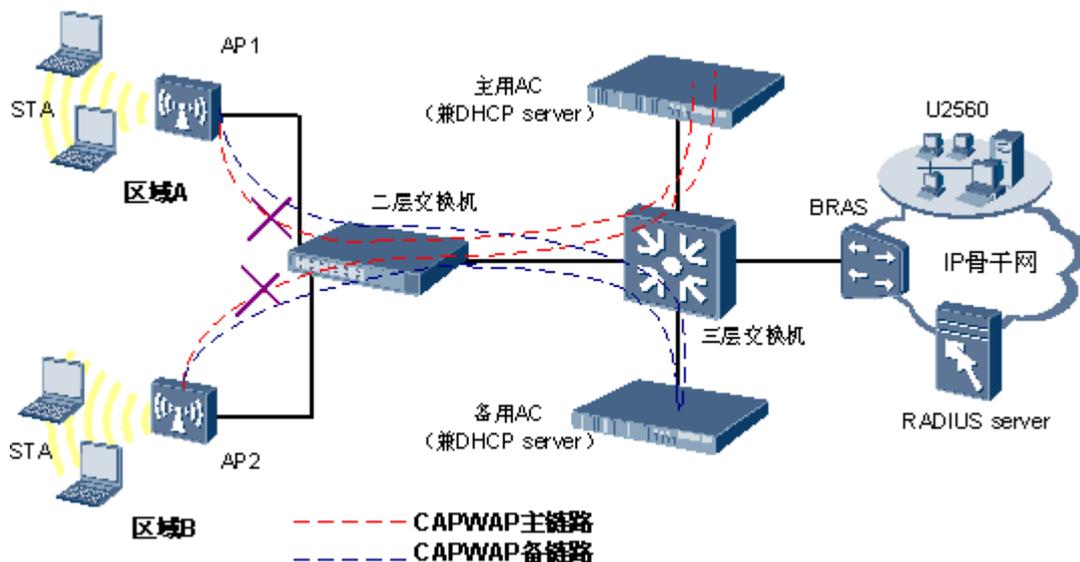
组网说明

网络供应商为某两个相隔较远的区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。区域内的用户按流量计费。

AC 采用“旁挂式”三层组网，组网如[图 4-8](#)所示，主备 AC 上的业务配置相同，同时与 AP 通信。

STA 的 IP 地址由三层交换机分配；AP 的 IP 地址由 AC 分配，自动分配地址。

图 4-8 双链路热备保护（三层组网）



配置原则

- 确保 AP 能够同时跟主备 AC 通信。
- AP 的 IP 地址分配：
主备 AC 都开启 DHCP server 功能，配置 IP 地址池（包括配置网关地址，Option43 和 Option60，以及 section），给 AP 自动分配 IP 地址。需注意把主备 AC 的 IP 地址池错开，以避免分配的 IP 地址冲突。
- 指定 AC 的源接口：只能使用与 AP 地址同网段的 VLANIF 接口或者 Loopback 接口作为 AC 的源接口。
- WLAN 数据配置：
 - 在主备 AC 上分别打开双链路开关，并配置相应的主备优先级。
 - 在主备 AC 上配置其他 WLAN 相关数据，并确保二者的配置完全一致。



注意

- 不允许运营商 ID 配置为“other”。如果运营商 ID 配置为“other”，将导致双链路热备倒换后，STA 使用 WPA 或 WAPI 方式重新认证失败。
- 不支持通过 AC 给 STA 分配 IP 地址，或者 AC 作为 STA 的网关。

前提条件

- AP、AC、二层和三层交换机正常工作，交换机上 VLAN 已经创建。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。
- 已使用维护终端成功登录系统 AC 系统。

数据规划

表 4-6 数据规划表

配置项	数据
WLAN 服务	AP 认证类型: WEP 认证策略, Open-system 认证模式
	认证报文的加密类型: 不加密
AP 管理 VLAN	VLAN 10
AP Region	AP1: 101
	AP2: 102
ESS	<ul style="list-style-type: none"> ● 名称: huawei-1 ● SSID: huawei-F4 ● 映射模式: AP 域映射 ● 映射 VLAN: 101 ● 数据转发模式: 直接转发
	<ul style="list-style-type: none"> ● 名称: huawei-2 ● SSID: huawei-F5 ● 映射模式: AP 域映射 ● 映射 VLAN: 102 ● 数据转发模式: 直接转发
上网业务 VLAN	STA1/STA2: VLAN 101 (由 AC 下发)
	STA3/STA4: VLAN 102 (由 AC 下发)
二层交换机上 VLAN	<ul style="list-style-type: none"> ● 接 AP1 端口 (Eth 0/0/1): Trunk 类型, 缺省 VLAN ID 为 800, 允许 VLAN 101/800 通过 ● 接 AP2 端口 (Eth 0/0/2): Trunk 类型, 缺省 VLAN ID 为 800, 允许 VLAN 102/800 通过 ● 接三层交换机端口 (GE 0/0/1): Trunk 类型, 允许 VLAN 101/102/800 通过
三层交换机上 VLAN	<ul style="list-style-type: none"> ● 接二层交换机端口 (GE 1/0/1): Trunk 类型, 允许 VLAN 101/102/800 通过 ● 接主 AC 端口 (GE 1/0/2): Hybrid 类型, 允许 VLAN 101/102/10 通过 ● 接备 AC 端口 (GE 1/0/4): Hybrid 类型, 允许 VLAN 101/102/10 通过 ● 接 BRAS 端口 (GE 1/0/3): Trunk 类型, 允许 VLAN 101/102 通过
AC Carrier ID/AC ID	CTC/1
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24

配置项	数据
AP 管理网关	192.168.1.1/24（三层交换机上）
STA1 的 IP 地址池	192.168.5.2 ~ 192.168.5.254/24
STA3 的 IP 地址池	192.168.6.2 ~ 192.168.6.254/24
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址，三层接入交换机做 DHCP 服务器给 STA 分配 IP 地址。
主备 AC IP 地址	主用 AC: 192.168.2.2/24 备用 AC: 192.168.2.3/24
主备 AC 优先级	主用 AC: 1 备用 AC: 2
AP 动态 IP 地址	192.168.1.2 ~ 192.168.1.254/24

操作步骤

- 配置交换机，使 AP 与 AC 互通。
 1. 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Hybrid 类型，缺省 VLAN 分别为 800，允许 VLAN 800 通过。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考对应《命令手册》。



注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type trunk
[huawei-Ethernet0/0/1]port trunk pvid vlan 800
[huawei-Ethernet0/0/1]port trunk allow-pass vlan 101 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type trunk
[huawei-Ethernet0/0/2]port trunk pvid vlan 800
[huawei-Ethernet0/0/2]port trunk allow-pass vlan 102 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置二层交换机连接三层交换机的 GE 端口（GE 0/0/1）透传所有管理 VLAN 与业务 VLAN。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet0/0/1]quit
```

- 配置三层交换机连接二层交换机的 GE 端口(GE 1/0/1)透传所有管理 VLAN 与业务 VLAN。

 说明

此处配置以华为 S9300 系列交换机为例，其他类型交换机请参考对应《命令手册》。

```
[huawei]vlan batch 10 101 102 800
[huawei]interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1]port link-type trunk
[huawei-GigabitEthernet1/0/1]port trunk allow-pass vlan 101 102 800
[huawei-GigabitEthernet1/0/1]quit
```

- 配置三层交换机连接主用 AC 的 GE 端口(GE 1/0/2)透传管理 VLAN。

```
[huawei-vlan10]quit
[huawei]interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2]port link-type hybrid
[huawei-GigabitEthernet1/0/2]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/2]quit
```

- 配置三层交换机连接备用 AC 的 GE 端口(GE 1/0/4)透传管理 VLAN。

```
[huawei-vlan11]quit
[huawei]interface GigabitEthernet 1/0/4
[huawei-GigabitEthernet1/0/4]port link-type hybrid
[huawei-GigabitEthernet1/0/4]port hybrid tagged vlan 10 101 102
[huawei-GigabitEthernet1/0/4]quit
```

- 配置三层交换机连接 BRAS 的 GE 端口(GE 1/0/3)透传业务 VLAN。

```
[huawei]interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3]port link-type trunk
[huawei-GigabitEthernet1/0/3]port trunk allow-pass vlan 101 102
[huawei-GigabitEthernet1/0/3]quit
```

- 配置三层交换机的 DHCP Relay 功能。

```
[huawei]dhcp enable
[huawei]interface Vlanif 800
[huawei-Vlanif103]ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif103]dhcp select relay
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.2
[huawei-Vlanif103]dhcp relay server-ip 192.168.2.3
[huawei-Vlanif103]quit
```

- VLANIF 10 的 IP 地址为 192.168.2.1，作为连接主用 AC 和备用 AC 的三层接口。

```
[huawei]interface Vlanif 10
[huawei-Vlanif10]ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif10]quit
```

配置 STA 的 IP 地址池。

```
[huawei]interface Vlanif 101
[huawei-Vlanif101]ip address 192.168.5.1 255.255.255.0
[huawei-Vlanif101]dhcp select interface
[huawei-Vlanif101]quit
[huawei]interface Vlanif 102
[huawei-Vlanif102]ip address 192.168.6.1 255.255.255.0
[huawei-Vlanif102]dhcp select interface
[huawei-Vlanif102]quit
```

● AC 基础配置。

- 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。
 - 主用 AC

配置主用 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

- 备用 AC

配置备用 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

 说明

必须保证主 AC 和备 AC 上配置的 AC ID 和运营商 ID 一致，避免业务配置中 BSSID 不一致导致主备切换后，业务切换失败。

2. 配置 AC 连接三层交换机端口 VLAN。

- 主用 AC

主 AC 上创建 vlan10, vlan 101 和 vlan 102, 并加入业务端口 0/2/0, 并配置端口隔离。

```
huawei(config)#vlan 10
huawei(config)#vlan 101 to 102
huawei(config)#port vlan 10 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#isolate port 0/2/0
```

- 备用 AC

备 AC 上创建 vlan10, vlan 101 和 vlan 102, 并加入业务端口 0/2/0, 并配置端口隔离。

```
huawei(config)#vlan 10
huawei(config)#vlan 101 to 102
huawei(config)#port vlan 10 0/2 0
huawei(config)#port vlan 101 to 102 0/2 0
huawei(config)#isolate port 0/2/0
```

3. 在 AC 上创建 VLAN 及 VLANIF。

- 主用 AC

VLANIF 10 的 IP 地址为 192.168.2.2, 作为连接三层交换机的三层接口。

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
Command:
ip address 192.168.2.2 255.255.255.0
```

使能 VLANIF 接口的 DHCP 功能, 使 AC 兼作 DHCP server, 为 AP 分配 IP 地址。

```
huawei(config-if-vlanif10)#dhcps enable
huawei(config-if-vlanif10)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接, 可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

- 备用 AC

VLANIF 19 的 IP 地址为 192.168.2.3, 作为连接三层交换机的三层接口。

```
huawei(config)#vlan 10
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 192.168.2.3 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 192.168.2.3 255.255.255.0
```

使能 VLANIF 接口的 DHCP 功能, 使 AC 兼作 DHCP server, 为 AP 分配 IP 地址。

```
huawei(config-if-vlanif11)#dhcp enable
huawei(config-if-vlanif11)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

4. 设置 AC 的源。

- 主用 AC

配置 VLANIF 接口作为主用 AC 的源。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

- 备用 AC

配置 VLANIF 接口作为备用 AC 的源。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 10
huawei(config-wlan-ac-view)#quit
```

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

5. 在 AC 上配置 AP 的 IP 地址池。

- 主用 AC

IP 地址池 ap-server 对应 vlanif 10。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.128
huawei(config-ip-pool-ap-server)#quit
```

#配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.2.2,192.168.2.3
huawei(config-ip-pool-ap-server)#quit
```

- 备用 AC

IP 地址池 ap-standby 对应 vlanif 10。

```
huawei(config)#ip pool standby
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.129 192.168.1.254
huawei(config-ip-pool-ap-server)#quit
```

#配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.2.3,192.168.2.2
huawei(config-ip-pool-ap-server)#quit
```

 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

1. 配置 AC 到 192.168.1.0 网段的路由。

- 主用 AC

```
huawei(config)#ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

- 备用 AC

```
huawei(config)#ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

● 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为 “sn-auth”。

- 主用 AC

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

- 备用 AC

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. 离线添加 AP。

- 主用 AC

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2 (type-id 为 0)。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入 “normal” 状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

- 备用 AC

 说明

此时还未建立双链路，AP 在主用 AC 上线后，就不能在备用 AC 正常上线。请先切断主链路，让 AP 在备用 AC 上线，进行以下操作。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2 (type-id 为 0)。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

3. 配置 AP 域。

- 主用 AC

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

- 备用 AC

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)#ap-region id 101
huawei(config-wlan-ap-region-101)#quit
huawei(config-wlan-ac-view)#ap-region id 102
huawei(config-wlan-ap-region-102)#quit
```

4. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

- 主用 AC

```
huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
ap id 1
```

```
huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
```

```
Command:
```

```

ap id 2

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

- 备用 AC

huawei(config-wlan-ac-view)#ap id 1
{ <cr>|ap-type<K>|type-id<K> } :

Command:
ap id 1

huawei(config-wlan-ap-1)#region-id 101
huawei(config-wlan-ap-1)#quit
huawei(config-wlan-ac-view)#ap id 2
{ <cr>|ap-type<K>|type-id<K> } :

Command:
ap id 2

huawei(config-wlan-ap-2)#region-id 102
huawei(config-wlan-ap-2)#quit

```

- 配置 AP 对应的射频。

- 主用 AC

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```

huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit

```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```

huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit

```

- 备用 AC

1. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```

huawei(config-wlan-ac-view)#wmm-profile name wmm-1
huawei(config-wlan-wmm-prof-wmm-profile-1)#quit

```

2. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```

huawei(config-wlan-ac-view)#radio-profile name radio-1
huawei(config-wlan-radio-prof-radio-1)#bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)#quit

```

3. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```

huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)#quit

```

 说明

可以为一个 AP 指定不同的射频模板，也可以为多个 AP 指定同一个射频模板。

- 配置 AP 对应的 ESS。

- 主用 AC

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile
traffic-1 security-profile security-1
```

 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102
Success: 1
Failure: 0
```

- 备用 AC

1. 创建 Security 模板。

#创建名为“security-1”的 Security 模板，认证模式为 WEP 认证，使用开放认证，不加密。

```
huawei(config-wlan-ac-view)#security-profile name security-1
huawei(config-wlan-security-prof-security-1)#authentication policy wep
huawei(config-wlan-security-prof-security-1)#policy wep open-system
huawei(config-wlan-security-prof-security-1)#quit
```

2. 创建 Traffic 模板（即 QoS 模板）。

#创建名为“traffic-1”的 Traffic 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)#traffic-profile name traffic-1
huawei(config-wlan-traffic-prof-traffic-1)#quit
```

3. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-F4 traffic-profile
traffic-1 security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-F5 traffic-profile  
traffic-1 security-profile security-1
```

 说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

4. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101，配置 Ap-Region 102 映射 VLAN 102。

```
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode region  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag region 101 vlan 101  
Success: 1  
Failure: 0  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode region  
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag region 102 vlan 102  
Success: 1  
Failure: 0
```

● 配置数据转发模式。

- 主用 AC

#配置数据转发模式为根据 ESS 转发。

```
huawei(config-wlan-ac-view)#forward-mode type ess
```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用直接转发模式。

```
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward  
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

- 备用 AC

#配置数据转发模式为根据 ESS 转发。

```
huawei(config-wlan-ac-view)#forward-mode type ess
```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用直接转发模式。

```
huawei(config-wlan-ac-view)#forward-mode ess 0 mode direct-forward  
huawei(config-wlan-ac-view)#forward-mode ess 1 mode direct-forward
```

● 配置 AP 对应的 VAP，下发 WLAN 服务。

- 主用 AC

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1  
huawei(config-wlan-ac-view)#commit ap 2  
huawei(config-wlan-ac-view)#quit
```

- 备用 AC

 说明

此时还未建立双链路，AP 在主用 AC 上线后，就不能在备用 AC 正常上线。

请先切断主链路，让 AP 在备用 AC 上线，进行以下操作。

1. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1  
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-2
```

 说明

● VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。

● VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

2. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)#commit ap 1
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

说明

配置下发完成后，主链路和备链路都要保持连接状态。

● 开启 AC 的双链路热备保护开关。

- 主用 AC

开启主用 AC 的双链路热备保护开关，配置备份 AC 的 IP 地址为 192.168.2.3/24，主用 AC 的主备优先级为 1。

说明

通过配置 AC 的优先级来决定主备 AC，优先级高的 AC 作为主 AC，优先级低的 AC 作为备 AC。数字越小，优先级越高。优先级相同情况下 AC 负载轻的为主 AC；负载相同情况下比较 IP 地址，IP 地址小的 AC 为主 AC。

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.2.3 priority 1
```

- 备用 AC

开启备用 AC 的双链路热备保护开关，配置备份 AC 的 IP 地址为 192.168.2.2/24，备用 AC 的主备优先级为 2。

```
[huawei]wlan ac
huawei(config-wlan-ac-view)#wlan ac protect enable protect-ac 192.168.2.2 priority 2
```

----结束

操作结果

当系统检测到 AP 与主用 AC 之间的链路发生故障时，启动主备倒换，业务不中断；当主用 AC 恢复正常时，业务切换到主用 AC。

配置文件

主 AC 上的配置文件：

```
#
[board-bind]
<board-bind>
isolate port 0/2/0
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.2 255.255.255.0
dhcp enable
#
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
```

```
wlan ac
wlan ac protect enable protect-ac 192.168.2.3 priority 1
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-ap-server>
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.3 192.168.1.128
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.2,192.168.2.3
#
return
备 AC 上的配置文件:
#
[board-bind]
<board-bind>
isolate port 0/2/0
[vlan-config]
<vlan-config>
vlan 10
vlan 101 to 102
port vlan 10 0/2 0
port vlan 101 to 102 0/2 0
port vlan 101 to 102 0/2 24
#
[vlanif]
<vlanif10>
interface vlanif 10
ip address 192.168.2.3 255.255.255.0
dhcp enable
#
[post-system]
<post-system>
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
```

```

#
[wlan-ac-view]
<wlan-ac-view>
wlan ac-global carrier id ctc ac id 1
wlan ac
wlan ac protect enable protect-ac 192.168.2.2 priority 2
wlan ac source interface vlanif 10
ap-region id 101
quit
ap-region id 102
quit
ap-auth-mode sn-auth
ap id 1 type-id 0 mac 5489-9849-8194 sn SN000001
region-id 101
quit
ap id 2 type-id 0 mac 5489-984c-1114 sn SN000002
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
traffic-profile name traffic-1 id 1
quit
security-profile name security-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile id 1
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 1
quit
ess name huawei-1 id 0 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 id 1 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess id 0 mode region
vlan-mapping ess id 0 type tag region 101 vlan 101
vlan-mapping ess id 1 mode region
vlan-mapping ess id 1 type tag region 102 vlan 102
vap ap 1 radio 0 ess id 0 wlan 1
vap ap 2 radio 0 ess id 1 wlan 1
#
[ip-pool]
<ip-pool-standby>
ip pool standby
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.129 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.2.3,192.168.2.2
#
return

```

二层交换机上的配置文件：

```

#
vlan batch 101 102 800
#
interface Ethernet0/0/1
port link-type trunk
port trunk pvid vlan 800
port trunk allow-pass vlan 101 800
port-isolate enable group 1
#
interface Ethernet0/0/2
port link-type trunk
port trunk pvid vlan 800
port trunk allow-pass vlan 102 800
port-isolate enable group 1
#
interface GigabitEthernet0/0/1
port link-type trunk

```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 101 102 800
#
return
三层交换机上的配置文件：
#
vlan batch 10 101 102 800
#
interface Vlanif10
ip address 192.168.2.1 255.255.255.0
#
interface Vlanif101
ip address 192.168.5.1 255.255.255.0
dhcp select interface
#
interface Vlanif102
ip address 192.168.6.1 255.255.255.0
dhcp select interface
#
interface Vlanif800
ip address 192.168.1.1 255.255.255.0
dhcp select relay
dhcp relay server-ip 192.168.2.2
dhcp relay server-ip 192.168.2.3
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 101 102 800
#
interface GigabitEthernet0/0/2
port hybrid tagged vlan 10 101 to 102
#
interface GigabitEthernet0/0/3
port link-type trunk
port trunk allow-pass vlan 101 102
#
interface
GigabitEthernet0/0/4
port hybrid tagged vlan 10 101 to 102
#
return
```

4.3.7 配置 WLAN 业务示例-AC QoS 策略

某一区域部署了多个 AP，针对接入用户的不同，每个 AP 配置不同 QoS 策略，为用户提供差异化的 WLAN 服务质量。

组网需求

如图 4-9 所示，STA1、STA2 通过 AP1 连接到 internet 网络，STA3、STA4 和 STA5 通过 AP2 连接到 internet 网络。其中 STA5 为 VIP 客户。

AP1 下用户优先满足语音需求，AP2 下用户优先满足视频需求。当网络带宽不足时，优先满足 VIP 客户的使用需求。

图 4-9 配置 QoS 策略的业务组网图

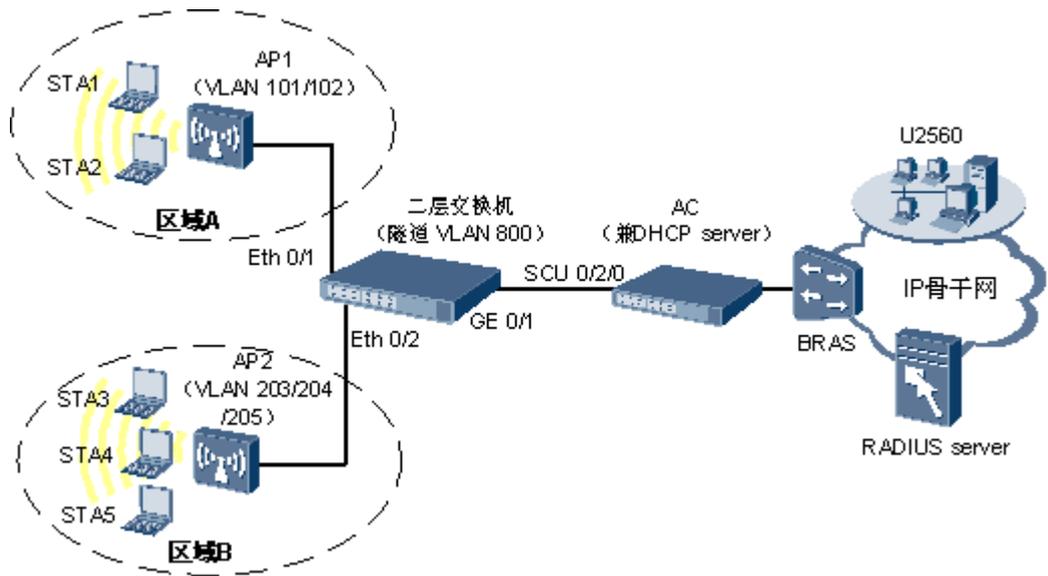


表 4-7 数据规划表

配置项	数据
WLAN 服务	SSID: huawei-1 Traffic 模板: huawei VLAN:101 VLAN Priority: 4
	SSID: huawei-2 Traffic 模板: huawei VLAN:102 VLAN Priority: 5
	SSID: huawei-3 Traffic 模板: huawei VLAN:203 VLAN Priority: 4
	SSID: huawei-4 Traffic 模板: huawei-vip VLAN:204 VLAN Priority: 6

配置项	数据
	SSID: huawei-5 Traffic 模板: huawei-vip VLAN:205 VLAN Priority: 5
AP 射频模板	AP1 射频模板:huawei; WMM 模板: huawei
	AP2 射频模板:huawei-vi; WMM 模板: huawei-vi
AP 管理 VLAN	VLAN 800 (由二层接入交换机分配)
AP Region	AP1: 101
	AP2: 102
AP 业务 VLAN	AP1: VLAN 101、VLAN 102
	AP2: VLAN 203、VLAN 204、VLAN 205
接入交换机上 VLAN	VLAN 800/101/102/203/204/205
AC Carrier ID/AC ID	CTC/1

数据准备

- AC 和 AP 之间的 CAPWAP 隧道已经建立。
- AC 能和 AP 可以进行正常通信。
- AP 具有 WMM 功能。
- 隧道转发模式下，交换机端口 1 和端口 2 不能加入业务 vlan；直接转发模式下，交换机端口 1 和端口 2 需要加入业务 vlan，即允许所有 vlan 通过。

操作步骤

步骤 1 配置 AC 与 AP 互通。

1. 创建 VLAN。

```
#创建 VLAN 101、102、203、204、205 和 800。
huawei(config)#vlan 101 to 102
huawei(config)#vlan 203 to 205
huawei(config)#vlan 800
```

#设置 VLAN 101 和 VLAN 203 对应优先级为 4，VLAN 102 和 VLAN 205 对应优先级为 5，VLAN 204 对应优先级为 6。

```
huawei(config)#vlan priority 101 4
huawei(config)#vlan priority 102 5
huawei(config)#vlan priority 203 4
huawei(config)#vlan priority 204 6
huawei(config)#vlan priority 205 5
```

2. 配置 AC 上连接 AP 的端口。

```
#配置端口 1 加入 VLAN 101、VLAN 102、VLAN 203、VLAN 204 和 VLAN 205。
huawei(config)#port vlan 101 0/2 0
huawei(config)#port vlan 102 0/2 0
huawei(config)#port vlan 203 0/2 0
huawei(config)#port vlan 204 0/2 0
huawei(config)#port vlan 205 0/2 0
huawei(config)#port vlan 800 0/2 0
```

步骤 2 配置 AP 对应的各类模板。

1. 创建 WMM 模板。

#创建 WMM 模板“huawei”，采用默认配置，其中优先级队列顺序为默认值：
AC_VO(语音)>AC_VI(视频)。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wmm-profile name huawei id 1
huawei(config-wlan-wmm-prof-huawei)#quit
```

#创建 WMM 模板“huawei-vi”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wmm-profile name huawei-vi id 2
```

#修改 WMM 模板“huawei-vi”中的队列优先级参数，使优先级队列顺序为：AC_VI
(视频)>AC_VO(语音)。

```
huawei(config-wlan-wmm-prof-huawei-vi)#wmm edca ap ac-vi ecw ecwmin 1 ecwmax
 1 aifsn 1 txoplimit 36 ack-policy normal
huawei(config-wlan-wmm-prof-huawei-vi)#wmm edca client ac-vi ecw ecwmin 1 ecwmax 3
  aifsn 1 txoplimit 36
huawei(config-wlan-wmm-prof-huawei-vi)#quit
```

2. 创建 Radio 模板。

#创建名为“huawei”的 Radio 模板，绑定 WMM 模板“huawei”。

```
huawei(config-wlan-ac-view)#radio-profile name huawei id 1
huawei(config-wlan-radio-prof-huawei)#bind wmm-profile name huawei
huawei(config-wlan-radio-prof-huawei)#quit
```

#创建名为“huawei-vi”的 Radio 模板，绑定 WMM 模板“huawei-vi”。

```
huawei(config-wlan-ac-view)#radio-profile name huawei-vi id 2
huawei(config-wlan-radio-prof-huawei-vi)#bind wmm-profile name huawei-vi
huawei(config-wlan-radio-prof-huawei-vi)#quit
```

3. 创建 Security 模板。

#创建名为“huawei”的 Security 模板。

```
huawei(config-wlan-ac-view)#security-profile name huawei id 6
huawei(config-wlan-security-prof-huawei)#quit
```

4. 创建 Traffic 模板。

#创建名为“huawei”的 Traffic 模板，设置 VAP 下行限速为 1024K，STA 客户端
下行限速为 512K。

```
huawei(config-wlan-ac-view)#traffic-profile name huawei id 1
huawei(config-wlan-traffic-prof-huawei)#rate-limit client down 512
huawei(config-wlan-traffic-prof-huawei)#rate-limit vap down 1024
huawei(config-wlan-traffic-prof-huawei)#quit
```

#创建名为“huawei-vip”的 Traffic 模板。设置 VAP 下行限速为 2048K，STA 客户
端下行限速为 1024K。设置其映射模式为指定，上、下行隧道优先级值均为 6。

```
huawei(config-wlan-ac-view)#traffic-profile name huawei-vip id 2
huawei(config-wlan-traffic-prof-huawei-vip)#rate-limit client down 1024
huawei(config-wlan-traffic-prof-huawei-vip)#rate-limit vap down 2048
huawei(config-wlan-traffic-prof-huawei-vip)#8021p designate 6
huawei(config-wlan-traffic-prof-huawei-vip)#8021p-map-up 6 6 6 6 6 6 6
huawei(config-wlan-traffic-prof-huawei-vip)#quit
```

步骤 3 配置 AP 的射频。

```
#配置 AP1 的射频，绑定 Radio 模板“huawei”。
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name huawei
huawei(config-wlan-radio-1/0)#quit

#配置 AP2 的射频，绑定 Radio 模板“huawei-vi”。
huawei(config-wlan-ac-view)#radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)#bind radio-profile name huawei-vi
huawei(config-wlan-radio-2/0)#quit
```

步骤 4 配置 ESS 与 SSID。

- #创建名为“huawei-1”的 ESS，SSID 为“huawei-1”，绑定 Traffic 模板“huawei”，Security 模板“huawei”。

```
huawei(config-wlan-ac-view)#ess name huawei-1 ssid huawei-1 traffic-profile huawei
security-profile huawei

#配置 ESS 的 VLAN 映射关系为根据 ESS 映射，映射 VLAN 101。
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-1 type tag vlan 101
Success: 1
Failure: 0
```
- #创建名为“huawei-2”的 ESS，SSID 为“huawei-2”，绑定 Traffic 模板“huawei”，Security 模板“huawei”。

```
huawei(config-wlan-ac-view)#ess name huawei-2 ssid huawei-2 traffic-profile huawei
security-profile huawei

#配置 ESS 的 VLAN 映射关系为根据 ESS 映射，映射为 VLAN 102。
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-2 type tag vlan 102
Success: 1
Failure: 0
```
- #创建名为“huawei-3”的 ESS，SSID 为“huawei-3”，绑定 Traffic 模板“huawei”，Security 模板“huawei”。

```
huawei(config-wlan-ac-view)#ess name huawei-3 ssid huawei-3 traffic-profile huawei
security-profile huawei-vi

#配置 ESS 的 VLAN 映射关系为根据 ESS 映射，映射为 VLAN 203。
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-3 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-3 type tag vlan 203
Success: 1
Failure: 0
```
- #创建名为“huawei-4”的 ESS，SSID 为“huawei-4”，绑定 Traffic 模板“huawei”，Security 模板“huawei”。

```
huawei(config-wlan-ac-view)#ess name huawei-4 ssid huawei-4 traffic-profile huawei
security-profile huawei

#配置 ESS 的 VLAN 映射关系为根据 ESS 映射，映射为 VLAN 204。
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-4 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-4 type tag vlan 204
Success: 1
Failure: 0
```
- #创建名为“huawei-5”的 ESS，SSID 为“huawei-5”，绑定 Traffic 模板“huawei-vip”，Security 模板“huawei”。

```
huawei(config-wlan-ac-view)#ess name huawei-5 ssid huawei-5 traffic-profile huawei
-vip security-profile huawei

#配置 ESS 的 VLAN 映射关系为根据 ESS 映射，映射为 VLAN 205。
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-5 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name huawei-5 type tag vlan 205
Success: 1
Failure: 0
```

步骤 5 下发 WLAN 服务到 AP 上。

- 下发 WLAN 服务到 AP1 的射频 0 上。

```
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-1 wlan 2
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name huawei-2 wlan 3
huawei(config-wlan-ac-view)#commit ap 1
```

- 下发 WLAN 服务到 AP2 的射频 0 上。

```
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-3 wlan 4
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-4 wlan 5
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name huawei-5 wlan 6
huawei(config-wlan-ac-view)#commit ap 2
```

----结束

操作结果

AP1 和 AP2 下用户可以搜索到 5 个 WLAN 网络，其网络标识分别为 huawei-1、huawei-2、huawei-3、huawei-4、huawei-5。STA1 - STA5 分别选择 huawei-1 到 huawei-5 的 WLAN 网络。

- STA1、STA2、STA3 和 STA4 用户速率最大为 512K。STA5 用户速率最大为 1024K。
- AP1 下用户 STA1 和 STA2 的语音通信优先被满足。AP2 下用户 STA3、STA4 和 STA5 的视频通信优先被满足。
- 当网络带宽不足时，按照规划配置，会陆续出现以下结果：
 - 因为 STA1 和 STA3 的通信优先级为 4，低于其他 STA 用户，会最先出现语音中断，下载速度缓慢等现象。
 - 当带宽继续减少时，STA2 的视频通信开始出现故障，随后语音也会出现中断现象。
 - 带宽继续减少，此时虽然 STA5 的通信优先级为 5，低于 STA4 的优先级 6，但是因为其 QoS 策略为指定映射为 6，这样 STA4 和 STA5 的实际优先级一致，会同时出现语音中断现象，随后可能发生视频通信故障。

配置文件

AC 上的配置文件（QoS 策略部分）

```
#
system-view
vlan 101 to 102
vlan 203 to 205
vlan 800
vlan priority 101 4
vlan priority 102 5
vlan priority 203 4
vlan priority 204 6
vlan priority 205 5
port vlan 101 0/2 0
port vlan 102 0/2 0
port vlan 203 0/2 0
port vlan 204 0/2 0
port vlan 205 0/2 0
port vlan 800 0/2 0
wlan ac
wmm-profile name huawei id 1
quit
wmm-profile name huawei-vi id 2
wmm edca ap ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
wmm edca client ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
quit
traffic-profile name huawei id 1
rate-limit client down 512
rate-limit vap down 1024
```

```
quit
traffic-profile name huawei-vip id 2
rate-limit client down 1024
rate-limit vap down 2048
8021p-map-up 6 6 6 6 6 6 6
8021p designate 6
quit
radio-profile name huawei id 1
bind wmm-profile id 1
quit
radio-profile name huawei-vi id 2
bind wmm-profile id 2
quit
security-profile huawei id 6
quit
radio ap-id 1 radio-id 0
bind radio-profile id 1
quit
radio ap-id 2 radio-id 0
bind radio-profile id 0
quit
ess name huawei-1 id 2 ssid huawei-1 traffic-profile huawei security-profile huawei
ess name huawei-2 id 3 ssid huawei-2 traffic-profile huawei security-profile huawei
ess name huawei-3 id 4 ssid huawei-3 traffic-profile huawei security-profile huawei
ess name huawei-4 id 5 ssid huawei-4 traffic-profile huawei-vip security-profile huawei
ess name huawei-5 id 6 ssid huawei-5 traffic-profile huawei-vip security-profile huawei
vlan-mapping ess id 2 type tag vlan 101
vlan-mapping ess id 3 type tag vlan 102
vlan-mapping ess id 4 type tag vlan 203
vlan-mapping ess id 5 type tag vlan 204
vlan-mapping ess id 6 type tag vlan 205
vap ap 1 radio 0 ess id 2 wlan 2
vap ap 1 radio 0 ess id 3 wlan 3
vap ap 2 radio 0 ess id 4 wlan 4
vap ap 2 radio 0 ess id 5 wlan 5
vap ap 2 radio 0 ess id 6 wlan 6
```

4.3.8 配置业务示例-接入安全策略

某一区域部署了多个 AP，针对接入用户的不同，每个 AP 配置不同接入安全策略，为用户提供差异化的接入安全控制。

组网需求

如图 4-10 所示，AP1 和 AP2 为接入用户提供 WLAN 服务，用户可以搜索到 5 个无线网络，其中：

- SSID 为 huawei-1 的无线网络采用开放式系统认证。
- SSID 为 huawei-2 的无线网络的 WLAN 服务采用共享密钥认证+WEP-104 加密。
- SSID 为 huawei-3 的无线网络采用 WPA1 认证+TKIP 加密。
- SSID 为 huawei-4 的无线网络采用 WPA2 认证+CCMP 加密。
- SSID 为 huawei-5 的无线网络采用 WAPI 证书认证。

图 4-10 配置接入安全策略的业务组网图

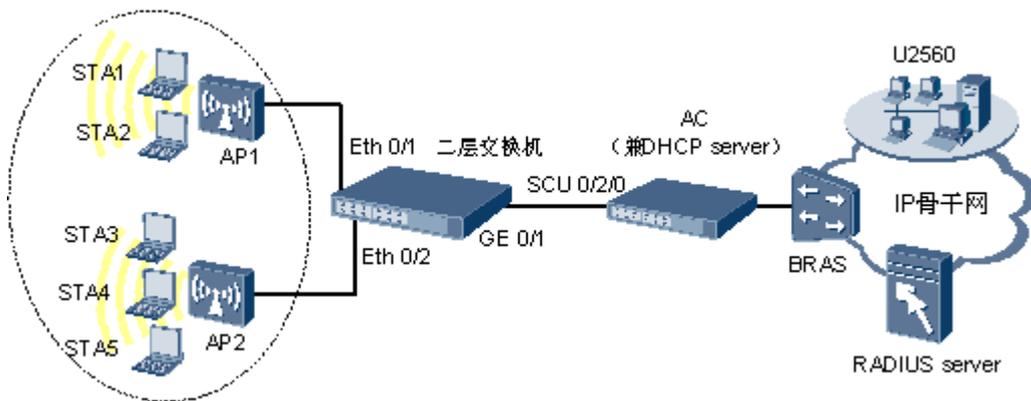


表 4-8 数据规划表

配置项	数据
接入安全策略	<ul style="list-style-type: none"> ● 安全模板: security-1 ● SSID: huawei-1 ● 认证模式: 开放式系统认证
	<ul style="list-style-type: none"> ● 安全模板: security-2 ● SSID: huawei-2 ● 认证模式: 共享密钥认证 ● 加密方式: WEP-104 加密 ● 密钥: 十进制, ABCDEFGHIJKL1、ABCDEFGHIJKL2、ABCDEFGHIJKL3、ABCDEFGHIJKL4
	<ul style="list-style-type: none"> ● 安全模板: security-3 ● SSID: huawei-3 ● 认证模式: WPA1 认证 (802.1x+PEAP) ● 加密方式: TKIP
	<ul style="list-style-type: none"> ● 安全模板: security-4 ● SSID: huawei-4 ● 认证模式: WPA2 认证 (802.1x+SIM) ● 加密方式: CCMP
	<ul style="list-style-type: none"> ● 安全模板: security-5 ● SSID: huawei-5 ● 认证模式: WAPI 认证 (证书认证)
ASU 服务器 IP 地址	10.10.10.1/24

前提条件

- AC 和 AP 之间的 CAPWAP 隧道已经建立。
- AC 能和 AP 可以进行正常通信，AP1 和 AP2 处于正常工作状态。
- AC 证书和 ASU 证书文件已经保存到设备的 Flash，文件名为 huawei-ac.cer 和 huawei-asu.cer。AC 的私钥文件为 ac-key.key。
- Radius 服务器已配置用户名、密码，创建 AAA 用户等信息。
- 无线终端上完成无线网络的配置。

说明

操作步骤中的前三步与配置业务示例-直连式二层组网，数据隧道转发的配置示例相同，不再赘述，具体请参见 [4.3.1 配置业务示例-直连式二层组网，数据隧道转发](#)。

配置安全模板 security-3 的安全策略时，需配置 WPA 使用 dot1x 认证方式和相应的加密方式。

配置安全模板 security-4 的安全策略时，需配置 WPA2 使用 dot1x 认证方式和相应的加密方式。

操作步骤

步骤 1 配置交换机和 AC，使 AP 和 AC 互通。（略）

步骤 2 配置 AC 的基本功能。（略）

步骤 3 配置 AP 并上线。（略）

步骤 4 配置 AP 对应的射频。

#创建名为“wmm”的 WMM 模板，参数采用默认配置。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wmm-profile name wmm id 1
huawei(config-wlan-wmm-prof-wmm)#quit
```

#创建名为“radio”的射频模板，绑定 WMM 模板“wmm”。

```
huawei(config-wlan-ac-view)#radio-profile name radio
huawei(config-wlan-radio-prof-radio)#bind wmm-profile name wmm
huawei(config-wlan-radio-prof-radio)#quit
```

#将 AP1 和 AP2 对应的射频绑定射频模板“radio”。

```
huawei(config-wlan-ac-view)#radio ap-id 0 radio-id 0
huawei(config-wlan-radio-0/0)#bind radio-profile name radio
huawei(config-wlan-radio-0/0)#quit
huawei(config-wlan-ac-view)#radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)#bind radio-profile name radio
huawei(config-wlan-radio-1/0)#quit
```

步骤 5 配置 RADIUS Server 与 AAA 方案，并配置域名信息。

```
huawei(config)#radius-server template peap.radius.com
huawei(config-radius-peap.radius.com)#radius-server authentication 10.137.146.163 1812
huawei(config-radius-peap.radius.com)#radius-server accounting 10.137.146.163 1813
huawei(config-radius-peap.radius.com)#radius-server shared-key huawei
huawei(config-radius-peap.radius.com)#quit
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme radius
huawei(config-aaa-authen-radius)#authentication-mode radius
huawei(config-aaa-authen-radius)#quit
huawei(config-aaa)#accounting-scheme radius
huawei(config-aaa-accounting-radius)#accounting-mode radius
```

```
huawei(config-aaa-accounting-radius)#quit
huawei(config-aaa)#domain peap.radius.com
huawei(config-aaa-domain-peap.radius.com)#authentication-scheme radius
huawei(config-aaa-domain-peap.radius.com)#accounting-scheme radius
huawei(config-aaa-domain-peap.radius.com)#radius-server peap.radius.com
huawei(config-aaa-domain-peap.radius.com)#quit
```

步骤 6 采用 WPA1/WPA2 认证模式时，需要使能设备的 802.1x 特性和 802.1x 全局 MAC 地址控制开关。

```
huawei(config)#dot1x enable
huawei(config)#dot1x mac-control
```

步骤 7 创建接入安全模板 security-1、security-2、security-3、security-4、security-5。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)#quit
huawei(config-wlan-ac-view)#security-profile name security-2 id 2
huawei(config-wlan-security-prof-security-2)#quit
huawei(config-wlan-ac-view)#security-profile name security-3 id 3
huawei(config-wlan-security-prof-security-3)#quit
huawei(config-wlan-ac-view)#security-profile name security-4 id 4
huawei(config-wlan-security-prof-security-4)#quit
huawei(config-wlan-ac-view)#security-profile name security-5 id 5
huawei(config-wlan-security-prof-security-5)#quit
```

步骤 8 配置接入安全模板。

- 配置接入安全模板 security-1 的安全策略。

#配置模板的 WEP 认证采用开放式系统认证。

```
huawei(config-wlan-ac-view)#security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)#policy wep open-system
```

- 配置接入安全模板 security-2 的安全策略。

#配置模板的 WEP 认证采用共享式认证。

```
huawei(config-wlan-ac-view)#security-profile name security-2 id 2
huawei(config-wlan-security-prof-security-2)#policy wep share-key
```

#配置模板的 WEP 认证采用 WEP-104 加密，密钥使用十进制输入，密钥分别为 ABCDEFGHIJKL1、ABCDEFGHijkl2、ABCDEFGHijkl3、ABCDEFGHijkl4。

```
huawei(config-wlan-security-prof-security-2)#wep key wep-104 pass-phrase 0 ABCDE
FGHIJKL1
huawei(config-wlan-security-prof-security-2)#wep key wep-104 pass-phrase 1 ABCDE
FGHIJKL2
huawei(config-wlan-security-prof-security-2)#wep key wep-104 pass-phrase 2 ABCDE
FGHIJKL3
huawei(config-wlan-security-prof-security-2)#wep key wep-104 pass-phrase 3 ABCDE
FGHIJKL4
```

 说明

WEP 数据加密方式需要指定一个加密密钥。

#配置模板采用 WEP 认证。

```
huawei(config-wlan-security-prof-security-2)#authentication policy wep
huawei(config-wlan-security-prof-security-2)#quit
```

- 配置接入安全模板 security-3 的安全策略。

#配置模板的 WPA1 认证采用 802.1x+PEAP 方式，采用 TKIP 加密。

```
huawei(config-wlan-ac-view)#security-profile name security-3 id 3
huawei(config-wlan-security-prof-security-3)#policy wpa1 tkip 802dot1x peap
```

#配置模板采用 WPA1 认证。

```
huawei(config-wlan-security-prof-security-3)#authentication policy wpa1
huawei(config-wlan-security-prof-security-3)#quit
```

- 配置接入安全模板 security-4 的安全策略。

#配置模板的 WPA2 认证采用 802.1x+SIM 方式，采用 CCMP 加密。

```
huawei(config-wlan-ac-view)#security-profile name security-4 id 4
huawei(config-wlan-security-prof-security-4)#policy wpa2 ccmp 802dot1x sim
```

#配置模板采用 WPA2 认证。

```
huawei(config-wlan-security-prof-security-4)#authentication policy wpa2
huawei(config-wlan-security-prof-security-4)#quit
```

- 配置接入安全模板 security-5 的安全策略。

#配置模板的 WPAI 认证采用证书认证方式。

```
huawei(config-wlan-ac-view)#security-profile name security-5 id 5
huawei(config-wlan-security-prof-security-5)#wapi wai certificate
```

#配置 ASU 服务器的 IP 地址为 10.10.10.1, AC 认证证书为 huawei-ac.cer, ASU 认证证书为 huawei-asu.cer, AC 证书的私钥文件为 ac-key.key, Issuer 认证证书为 huawei-issuer.cer。

 说明

- 系统支持对同一个接入安全模板同时绑定 CA 证书、AC 证书和 ASU 证书, 且每种证书只能绑定一个, 重复同一种模板时系统会提示该证书已绑定。
- ASU 的证书和 Issuer 的证书, 必须加载一个。

```
huawei(config-wlan-security-prof-security-5)#wapi asu-server ip 10.10.10.1
huawei(config-wlan-security-prof-security-5)#wapi certificate ac import file-name huawei-ac.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate issuer import file-name huawei-issuer.cer
huawei(config-wlan-security-prof-security-5)#wapi certificate asu import file-name huawei-asu.cer
huawei(config-wlan-security-prof-security-5)#wapi private-key import file-name ac-key.key
...//-----对于证书和私钥合一的证书文件, 此配置可以省略
```

#配置模板采用 WAPI 认证。

```
huawei(config-wlan-security-prof-security-5)#authentication policy wapi
huawei(config-wlan-security-prof-security-5)#quit
```

步骤 9 配置 ESS, 创建 VAP。

- 创建名为 ESS-1 的 ESS, SSID 为 huawei-1, 绑定 Traffic 模板 ctc, Security 模板 security-1。下发 WLAN 服务到 AP1 的射频 0 上, WLAN ID 为 1。

```
huawei(config-wlan-ac-view)#traffic-profile name ctc
huawei(config-wlan-traffic-prof-ctc)#quit
huawei(config-wlan-ac-view)#ess name ess-1 ssid huawei-1 traffic-profile ctc security-profile security-1
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-1 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-1 type tag vlan 101
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name ess-1
huawei(config-wlan-ac-view)#commit ap 1
```

- 创建名为 ESS-2 的 ESS, SSID 为 huawei-2, 绑定 Traffic 模板 ctc, Security 模板 security-2。下发 WLAN 服务到 AP1 的射频 0 上, WLAN ID 为 1。

```
huawei(config-wlan-ac-view)#ess name ess-2 ssid huawei-2 traffic-profile ctc security-profile security-2
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-2 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-2 type tag vlan 101
huawei(config-wlan-ac-view)#vap ap 1 radio 0 ess name ess-2
huawei(config-wlan-ac-view)#commit ap 1
```

- 创建名为 ESS-3 的 ESS, SSID 为 huawei-3, 绑定 Traffic 模板 ctc, Security 模板 security-3。下发 WLAN 服务到 AP2 的射频 0 上, WLAN ID 为 1。

```
huawei(config-wlan-ac-view)#ess name ess-3 ssid huawei-3 traffic-profile ctc security-profile security-3
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-3 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-3 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-3
huawei(config-wlan-ac-view)#commit ap 2
```

- 创建名为 ESS-4 的 ESS, SSID 为 huawei-4, 绑定 Traffic 模板 ctc, Security 模板 security-4。下发 WLAN 服务到 AP2 的射频 0 上, WLAN ID 为 1。

```
huawei(config-wlan-ac-view)#ess name ess-4 ssid huawei-4 traffic-profile ctc security-profile security-4
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-4 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-4 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-4
huawei(config-wlan-ac-view)#commit ap 2
```

- 创建名为 ESS-5 的 ESS，SSID 为 huawei-5，绑定 Traffic 模板 ctc，Security 模板 security-5。下发 WLAN 服务到 AP2 的射频 0 上，WLAN ID 为 1。

```
huawei(config-wlan-ac-view)#ess name ess-5 ssid huawei-5 traffic-profile ctc security-profile security-5
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-5 mode ess
huawei(config-wlan-ac-view)#vlan-mapping ess name ess-5 type tag vlan 102
huawei(config-wlan-ac-view)#vap ap 2 radio 0 ess name ess-5
huawei(config-wlan-ac-view)#commit ap 2
huawei(config-wlan-ac-view)#quit
```

----结束

操作结果

AP1 和 AP2 下的接入用户可以搜索到 5 个无线网络,其网络标识分别为 huawei-1、huawei-2、huawei-3、huawei-4、huawei-5。

- 选择 SSID 为 huawei-1 的网络时，用户无需验证即可以正常使用 WLAN 服务。
- 选择 SSID 为 huawei-2 的网络时，用户需要有共享密钥才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-3 和 huawei-4 的网络时，用户需要通过 802.1x 认证才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-5 的网络时，用户需要有匹配的证书才可以使用 WLAN 服务。

配置文件

AC 上的配置文件（安全模板+VAP 部分）

```
#
[vlan-config]
<vlan-config>
vlan 101 to 102
#
[config]
<config>
dot1x enable
dot1x mac-control
#
[radius]
<radius>
radius-server template "peap.radius.com"
radius-server authentication 10.137.146.163 1812
radius-server accounting 10.137.146.163 1813
#
[aaa]
<aaa>
aaa
authentication-scheme "radius"
authentication-mode radius
#
accounting-scheme "radius"
accounting-mode radius
#
domain "peap.radius.com"
authentication-scheme "radius"
accounting-scheme "radius"
radius-server "peap.radius.com"
#
[wlan-ac-view]
```

```
wlan ac
wmm-profile name wmm id 1
quit
traffic-profile name ctc id 2
quit
security-profile name security-1 id 1
quit
security-profile name security-2 id 2
policy wep share-key
wep key wep-104 pass-phrase 0 ABCDEFGHIJKL1
wep key wep-104 pass-phrase 1 ABCDEFGHIJKL2
wep key wep-104 pass-phrase 2 ABCDEFGHIJKL3
wep key wep-104 pass-phrase 3 ABCDEFGHIJKL4
quit
security-profile name security-3 id 3
authentication policy wpa1
policy wpa1 tkip 802dot1x peap
quit
security-profile name security-4 id 4
authentication policy wpa2
policy wpa2 ccmp 802dot1x sim
quit
security-profile name security-5 id 5
authentication policy wapi
wapi asu-server ip 10.10.10.1
quit
radio-profile name radio id 2
bind wmm-profile id 1
quit
radio ap-id 0 radio-id 0
bind radio-profile id 2
quit
radio ap-id 1 radio-id 0
bind radio-profile id 2
quit
ess name ess-1 id 1 ssid huawei-1 traffic-profile ctc security-profile
security-1
ess name ess-2 id 2 ssid huawei-2 traffic-profile ctc security-profile
security-2
ess name ess-3 id 3 ssid huawei-3 traffic-profile ctc security-profile
security-3
ess name ess-4 id 4 ssid huawei-4 traffic-profile ctc security-profile
security-4
ess name ess-5 id 5 ssid huawei-5 traffic-profile ctc security-profile
security-5
vlan-mapping ess id 1 type tag vlan 101
vlan-mapping ess id 2 type tag vlan 101
vlan-mapping ess id 3 type tag vlan 102
vlan-mapping ess id 4 type tag vlan 102
vlan-mapping ess id 5 type tag vlan 102
#
return
```

4.3.9 配置业务示例-配置 AP 负载均衡组

AC 根据配置策略控制 AP 接入的无线用户，以保证 WLAN 实现负载均衡，优化网络性能。

组网说明

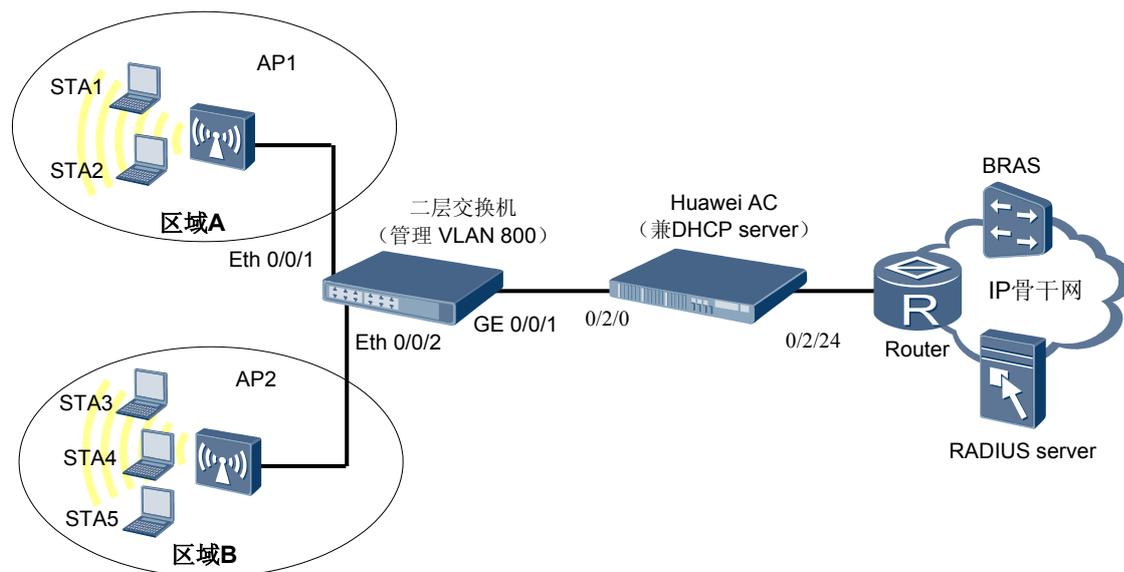
在集中式控制系统中，无线终端关联 AP 设备都是需要经过 AC 许可。在实际应用中，无线终端会扫描到多台 AP 设备，并且向多台设备发送关联请求帧，无论采用 Split MAC、Local MAC 或者 Remote MAC，AP 设备收到无线终端的关联请求帧后都会将此帧转发给 AC，由 AC 根据自身策略决定无线终端可以关联到哪台 AP。

网络供应商为某两个临近小区域（区域 A，区域 B）提供 WLAN 上网服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。配置 AP 负载均衡后，AC 根据配置策略控制 AP 接入的无线用户，以保证 WLAN 实现负载均衡，优化网络性能。

AC 和 AP 之间采用“直连式”二层组网，组网如图 4-11 所示，

AC 同时作为 DHCP server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

图 4-11 直连式组网网络（二层组网，数据隧道转发）



前提条件

- AP、AC、二层交换机正常上电。
- 路由器，BRAS，AAA/WEB 服务器等设备相关功能调试完成。
- BRAS 上根据对接入用户的认证和计费的要求，已完成相应的配置。

数据规划

表 4-9 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 800（由二层交换机打 VLAN tag）
AP Region	AP1：101
	AP2：102

配置项	数据
二层交换机上 VLAN	接入 AP 端口配置为 Access 类型，缺省 VLAN 为 800，接入 AC 的端口配置为 Trunk 类型，允许 VLAN 800 通过。AP 的管理 VLAN 和业务 VLAN 都封装在 CAPWAP 隧道中。
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址(Meth 0 接口)	10.11.104.2/24
AP 管理 IP 地址池	192.168.1.2 ~ 192.168.1.254/24
AP 管理网关	192.168.1.1/24
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址。

操作步骤

步骤 1 配置二层交换机，使 AP 与 AC 二层互通。

1. 配置二层交换机连接 AP 的以太网端口（Eth 0/0/1 和 Eth 0/0/2）类型为 Access 类型，缺省 VLAN 为 800。



说明

此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考对应《命令手册》。



注意

需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei]vlan 800
[huawei-vlan800]quit
[huawei]interface Ethernet 0/0/1
[huawei-Ethernet0/0/1]port link-type access
[huawei-Ethernet0/0/1]port default vlan 800
[huawei-Ethernet0/0/1]port-isolate enable
[huawei-Ethernet0/0/1]quit
[huawei]interface Ethernet 0/0/2
[huawei-Ethernet0/0/2]port link-type access
[huawei-Ethernet0/0/2]port default vlan 800
[huawei-Ethernet0/0/2]port-isolate enable
[huawei-Ethernet0/0/2]quit
```

2. 配置交换机连接 AC 的 GE 端口 1（GE 0/0/1）类型为 Trunk 类型，允许 VLAN 800 通过。

```
[huawei]interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1]port link-type trunk
[huawei-GigabitEthernet0/0/1]port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1]quit
```

步骤 2 AC 基础配置。

1. 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。

#配置 AC 运营商标识为 CTC（CTC-中国电信，CMCC-中国移动，CUC-中国联通，other-其他运营商），全局 AC ID 为 1。

```
huawei(config)#wlan ac-global carrier id ctc ac id 1
```

2. 配置 AC 连接二层交换机端口 VLAN。

#创建 VLAN 101、102 和 800。

```
huawei(config)#vlan 101
huawei(config)#vlan 102
huawei(config)#vlan 800
```

#将 VLAN 800 加入业务端口 0/2/0。

```
huawei(config)#port vlan 800 0/2 0
```

3. 配置 AC 的上行端口。

#端口 0/2/24 为上行端口，将 VLAN 101 和 VLAN 102 加入上行端口。

```
huawei(config)#port vlan 101 0/2 24
huawei(config)#port vlan 102 0/2 24
```

4. 在 AC 上创建 VLANIF。

#VLANIF 800 的 IP 地址为 192.168.1.1，作为数据转发的三层接口。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 192.168.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 192.168.1.1 255.255.255.0
```

使能 VLANIF 800 的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 分配 IP 地址。

```
huawei(config-if-vlanif800)#dhcps enable
huawei(config-if-vlanif800)#quit
```

 说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

5. 设置 AC 的源。

#配置 VLANIF 800 作为 AC 的源。

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

6. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ctc-ap-server 对应 VLAN 800。

 说明

IP 地址池的网关地址必须与 VLANIF 的 IP 地址相同，用于定义 AP 上线后获取 IP 的地址池。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 192.168.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 192.168.1.2 192.168.1.254
#（可选）配置 DHCP 服务的 Option 60 和 Option 43 功能，通过 DHCP option 43 通告 AC 的 IP 地址。
huawei(config-ip-pool-ap-server)#option 60 string Huawei AP
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-192.168.1.1
huawei(config-ip-pool-ap-server)#quit
```

 说明

- 配置 option 60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option 43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

步骤 3 配置 AC 与 AP 的互通。

1. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#ap-auth-mode sn-auth
```

2. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)#display ap-type all
All AP types information:
```

ID	Type
0	WA601
1	WA631
2	WA651
3	WA602
4	WA632
5	WA652
6	WA603SN
7	WA603DN
8	WA633SN
11	WA603DE
12	WA653DE
14	WA653SN

Total number: 12

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（type-id 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)#ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)#ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)#display ap all
All AP information:
```

AP ID	AP Type	Profile ID	Region ID	AP State
1	WA601	0	0	normal
2	WA601	0	0	normal

Total number: 2

步骤 4 配置 AP 负载均衡组。

创建一个负载均衡组并进入该组的配置视图。

```
huawei(config-wlan-ac-view)#load-balance-group id 0 name Balanced_Group0
huawei(config-wlan-load-group-Balanced_Group0)
```

1. 向指定负载均衡组内添加射频。

```
huawei(config-wlan-load-group-Balanced_Group0)#member ap-id 1 radio-id 0
huawei(config-wlan-load-group-Balanced_Group0)#member ap-id 2 radio-id 0
```

2. 配置指定负载均衡组的负载均衡模式为流量模式。

```
huawei(config-wlan-load-group-Balanced_Group0)#traffic gap 40
```

 说明

如果配置指定负载均衡组的负载均衡模式为会话模式，只需要将 traffic gap 40 改为 session gap gap-threshold，gap-threshold 取值范围 1-100。

3. 配置指定负载均衡组的最大关联次数。

```
huawei(config-wlan-load-group-Balanced_Group0)#associate-threshold 8
```

----结束

配置文件

AC 上的配置文件

```
#
wlan ac-global carrier id ctc ac id 1
vlan 101
vlan 102
vlan 800
port vlan 800 0/2 0
port vlan 101 0/2 24
port vlan 102 0/2 24
interface vlanif 800
ip address 192.168.1.1 255.255.255.0
dhcp enable
quit
wlan ac
wlan ac source interface vlanif 800
quit
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
option 60 string Huawei AP
option 43 string HuaweiAC-192.168.1.1
quit
wlan ac
ap-auth-mode sn-auth
quit
ap id 1 type-id 0 sn SN000001
ap id 2 type-id 0 sn SN000002
quit
load-balance-group name Balanced_Group0 id 0
  associate-threshold 8
  session gap 8
  member ap-id 1 radio-id 0
  member ap-id 2 radio-id 0
quit
```

5 协议配置

关于本章

协议配置主要包括一些常用协议配置。协议配置之间没有明显的逻辑关系，可以根据实际需要进行配置。

5.1 配置路由

以示例的方式介绍 AC 设备所支持的路由策略及路由协议的配置过程。

5.2 配置 DHCP

AC 设备在网络中能够实现 DHCP Relay 功能。配置 DHCP Relay 适用于用户通过 DHCP 协议动态地从 DHCP 服务器获取 IP 地址的场景。

5.3 配置 AAA

介绍在 AC 设备上 AAA 配置的过程，包括 AC 作为本地 AAA 服务器和远程 AAA 服务器的配置过程。

5.4 配置 MSTP

AC 设备实现了 MSTP（Multiple Spanning Tree Protocol）协议的应用功能，同时也兼容 STP（Spanning Tree Protocol）协议和 RSTP（Rapid Spanning Tree Protocol）协议，能够支持 MSTP 环状组网，满足了组网多样性的需求。

5.5 配置 Ethernet CFM OAM

介绍 Ethernet CFM OAM 在 AC 上的配置。

5.1 配置路由

以示例的方式介绍 AC 设备所支持的路由策略及路由协议的配置过程。

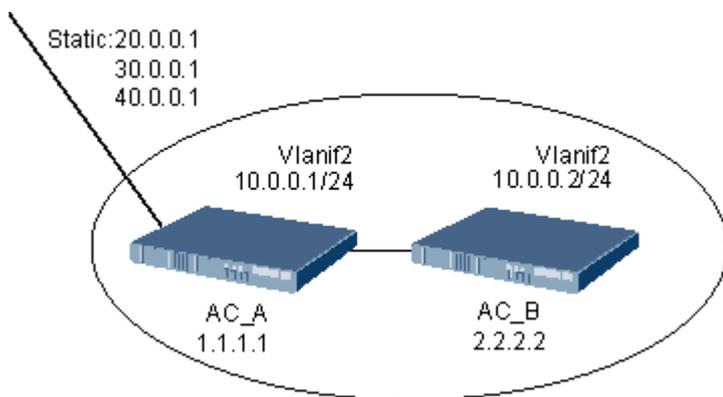
5.1.1 配置路由策略示例

通过本任务实现路由策略的配置。

业务需求

- AC_A 和 AC_B 均运行 OSPF 路由协议，且处于 Area 0 区间。
- AC_A 设备引入外部静态路由，在 AC_B 上配置路由过滤策略。

图 5-1 路由策略配置组网图



操作步骤

步骤 1 在 AC_A 上执行的配置

1. 配置 AC_A 的三层接口 IP 地址。

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.1 24
huawei(config-if-vlanif2)#quit
```
2. 启动 AC_A 的 OSPF 协议，指定该接口所属区域号。

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
3. 配置 AC_A 的 OSPF Router ID。

```
huawei(config)#router id 1.1.1.1
```
4. 配置三条静态路由。

```
huawei(config)#ip route-static 20.0.0.1 32 vlanif 2 10.0.0.2
huawei(config)#ip route-static 30.0.0.1 32 vlanif 2 10.0.0.2
huawei(config)#ip route-static 40.0.0.1 32 vlanif 2 10.0.0.2
```

5. 在 OSPF 中引入静态路由，提高 OSPF 获取路由的能力。

```
huawei(config)#ospf
huawei(config-ospf-1)#import-route static
huawei(config-ospf-1)#quit
```

6. 保存数据。

```
huawei(config)#save
```

步骤 2 在 AC_B 上执行的配置

1. 配置 AC_B 的三层接口 IP 地址。

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.0.0.2 24
huawei(config-if-vlanif2)#quit
```

2. 配置访问控制列表。

```
huawei(config)#acl 2000
huawei(config-acl-basic-2000)#rule deny source 30.0.0.0 255.255.255.0
huawei(config-acl-basic-2000)#rule permit source any
huawei(config-acl-basic-2000)#quit
```

3. 启动 AC_B 的 OSPF 协议，指定该接口所属区域号。

```
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.0.0.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. 配置 AC_B 的 OSPF Router ID。

```
huawei(config)#router id 2.2.2.2
```

5. 配置 OSPF 对接收的外部路由进行过滤。

```
huawei(config)#ospf
huawei(config-ospf-1)#filter-policy 2000 import
huawei(config-ospf-1)#quit
```

6. 保存数据。

```
huawei(config)#save
```

----结束

操作结果

1. AC_A 与 AC_B 能正常运行 OSPF 协议并且通信。
2. 通过在 AC_B 上配置路由过滤规则，使接收到的三条静态路由在 AC_B 上部分可见，部分被屏蔽掉——20.0.0.0 和 40.0.0.0 网段的路由是可见的，30.0.0.0 网段的路由则被屏蔽。

配置文件

在 AC_A 上:

```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 10.0.0.1 24
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
quit
router id 1.1.1.1
```

```
ip route-static 20.0.0.1 32 vlanif 2 10.0.0.2
ip route-static 30.0.0.1 32 vlanif 2 10.0.0.2
ip route-static 40.0.0.1 32 vlanif 2 10.0.0.2
ospf
import-route static
quit
save
```

在 AC_B 上:

```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 10.0.0.1 24
acl 2000
rule deny source 30.0.0.0 255.255.255.0
rule permit source any
quit
ospf
area 0
network 10.0.0.0 0.0.0.255
quit
quit
router id 2.2.2.2
ospf
filter-policy 2000 import
quit
save
```

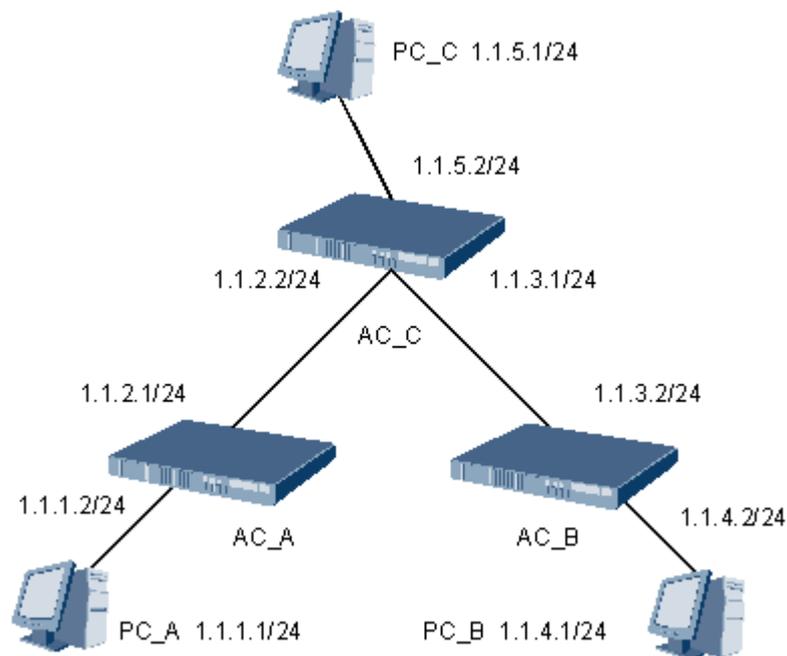
5.1.2 配置静态路由示例

通过手工添加静态路由实现 AC 设备间的互通。

业务需求

三台具有路由器功能的 AC_A、AC_B、AC_C 通过配置静态路由，使任意两台计算机之间能互通。

图 5-2 静态路由配置组网图



前提条件

已配置各 AC 上行口的 Native VLAN，确保通信正常。

操作步骤

步骤 1 配置三层接口 IP 地址。

三台设备的配置方法相同，这里仅以 AC_A 为例。

```
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 1.1.1.2 24
huawei(config-if-vlanif2)#ip address 1.1.2.1 24 sub
huawei(config-if-vlanif2)#quit
```

步骤 2 配置静态路由。

1. 配置 AC_A 的静态路由

```
huawei(config)#ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
huawei(config)#ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

2. 配置 AC_B 的静态路由

```
huawei(config)#ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
huawei(config)#ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

3. 配置 AC_C 的静态路由

```
huawei(config)#ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
huawei(config)#ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

步骤 3 配置用户主机网关。

1. 在 PC_A 上设置缺省网关为 1.1.1.2
2. 在 PC_B 上设置缺省网关为 1.1.4.2
3. 在 PC_C 上设置缺省网关为 1.1.5.2

步骤 4 保存数据。

```
huawei(config)#save
```

----结束

操作结果

所有用户主机或 AC 之间均能两两互相通信。

配置文件

以在 AC_A 上的配置为例。

```
vlan 2
port vlan 2 0/2 0
interface vlanif 2
ip address 1.1.1.2 24
ip address 1.1.2.1 24 sub
quit
ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
```

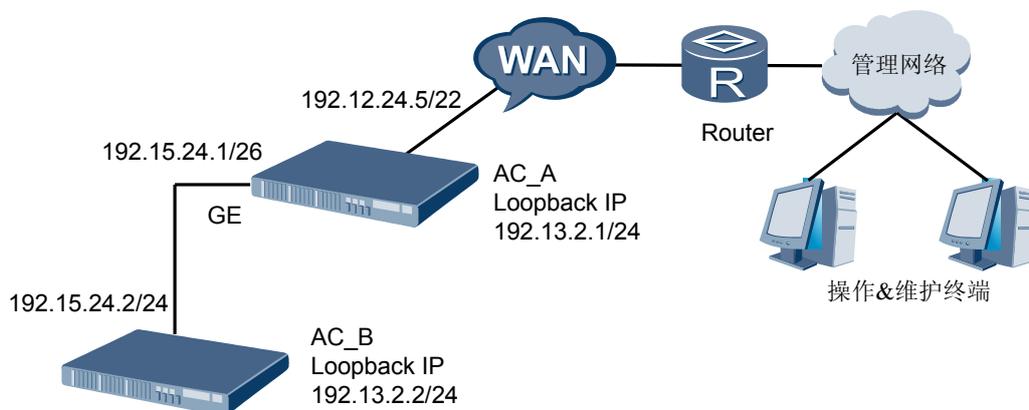
5.1.3 配置 RIP 路由协议示例

通过本任务使配置数据后的相关设备正常运行 RIP 协议。

业务需求

- AC_A 使用 0/2/16 端口与 AC_B 级联，使用 0/2/24 端口上行，通过 WAN 与管理中心网络相连。
- AC_A、AC_B 均使能 RIP 协议，使得管理用户可以通过 RIP 路由访问 AC_A、AC_B，实现对 AC_A、AC_B 的操作与维护。

图 5-3 RIP 路由协议配置组网图



数据规划

RIP 路由协议配置数据规划如表 5-1 所示。

表 5-1 RIP 路由协议配置数据规划表

配置项	数据
AC_A	上行端口：0/2/24 管理 VLAN：100 管理 VLAN 三层接口地址：192.13.24.5/22 Loopback 接口地址：192.13.2.1/24
	RIP 版本：V2 RIP 路由过滤策略：根据 IP 地址前缀列表 abc 进行路由过滤，只允许通过 VLAN 100 三层接口发布 IP 地址为 192.13.2.1、192.13.2.2 的路由信息。
	级联端口：0/2/16 级联管理 VLAN：10 级联管理 VLAN 三层接口地址：192.15.24.1/26

配置项	数据
AC_B	级联端口：0/2/16 管理 VLAN：10 管理 VLAN 三层接口地址：192.15.24.2/26 Loopback 接口地址：192.13.2.2/24
	RIP 版本：V2 RIP 路由过滤策略：根据 IP 地址前缀列表 abc 进行路由过滤，只允许通过 VLAN 10 三层接口发布 IP 地址为 192.13.2.2 的路由信息。

操作步骤

- 配置 AC_A
 1. 配置支持 RIP 协议的三层接口


```

                    huawei(config)#vlan 100
                    huawei(config)#port vlan 100 0/2 24
                    huawei(config)#interface vlanif 100
                    huawei(config-if-vlanif100)#ip address 192.13.24.5 22
                    huawei(config-if-vlanif100)#quit
                    huawei(config)#interface loopBack 0
                    huawei(config-if-loopback0)#ip address 192.13.2.1 24
                    huawei(config-if-loopback0)#quit
                    
```
 2. 启动 RIP 功能


```

                    huawei(config)#rip 1
                    huawei(config-rip-1)#network 192.13.24.0
                    huawei(config-rip-1)#network 192.13.2.0
                    huawei(config-rip-1)#version 2
                    huawei(config-rip-1)#quit
                    
```
 3. 配置路由过滤策略


```

                    huawei(config)#ip ip-prefix abc permit 192.13.2.1 32
                    huawei(config)#ip ip-prefix abc permit 192.13.2.2 32
                    huawei(config)#rip 1
                    huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 100
                    huawei(config-rip-1)#quit
                    
```
 4. 配置级联接口


```

                    huawei(config)#vlan 10
                    huawei(config)#port vlan 10 0/2 16
                    huawei(config)#interface vlanif 10
                    huawei(config-if-vlanif10)#ip address 192.15.24.1 26
                    huawei(config-if-vlanif10)#quit
                    
```
 5. 启动级联接口 RIP 功能


```

                    huawei(config)#rip 1
                    huawei(config-rip-1)#network 192.15.24.0
                    huawei(config-rip-1)#quit
                    
```
 6. 保存数据


```

                    huawei(config)#save
                    
```
- 配置 AC_B
 1. 配置支持 RIP 协议的三层接口


```

                    huawei(config)#vlan 10
                    huawei(config)#port vlan 10 0/2 16
                    huawei(config)#interface vlanif 10
                    
```

```
huawei(config-if-vlanif10)#ip address 192.15.24.2 26
huawei(config-if-vlanif10)#quit
huawei(config)#interface loopBack 0
huawei(config-if-loopback0)#ip address 192.13.2.2 24
huawei(config-if-loopback0)#quit
```

2. 启动 RIP 功能

```
huawei(config)#rip 1
huawei(config-rip-1)#network 192.15.24.0
huawei(config-rip-1)#network 192.13.2.0
huawei(config-rip-1)#version 2
huawei(config-rip-1)#quit
```

3. 配置路由过滤策略

```
huawei(config)#ip ip-prefix abc permit 192.13.2.2 32
huawei(config)#rip 1
huawei(config-rip-1)#filter-policy ip-prefix abc export vlanif 10
huawei(config-rip-1)#quit
```

4. 保存数据

```
huawei(config)#save
```

----结束

操作结果

管理中心的维护终端可以登录到 AC_A、AC_B 上，对设备进行操作与维护。

配置文件

在 AC_A 上:

```
vlan 100
port vlan 100 0/2 24
interface vlanif 100
ip address 192.13.24.5 22
quit
interface loopBack 0
ip address 192.13.2.1 24
quit
rip 1
network 192.13.24.0
network 192.13.2.0
version 2
quit
ip ip-prefix abc permit 192.13.2.1 32
ip ip-prefix abc permit 192.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 100
quit
vlan 10 smart
interface vlanif 10
ip address 192.15.24.1 26
quit
rip 1
network 192.15.24.0
quit
save
```

在 AC_B 上:

```
vlan 10
port vlan 10 0/2 16
interface vlanif 10
ip address 192.15.24.2 26
quit
interface loopBack 0
```

```

ip address 192.13.2.2 24
quit
rip 1
network 192.15.24.0
network 192.13.2.0
version 2
quit
ip ip-prefix abc permit 192.13.2.2 32
rip 1
filter-policy ip-prefix abc export vlanif 10
quit
save
    
```

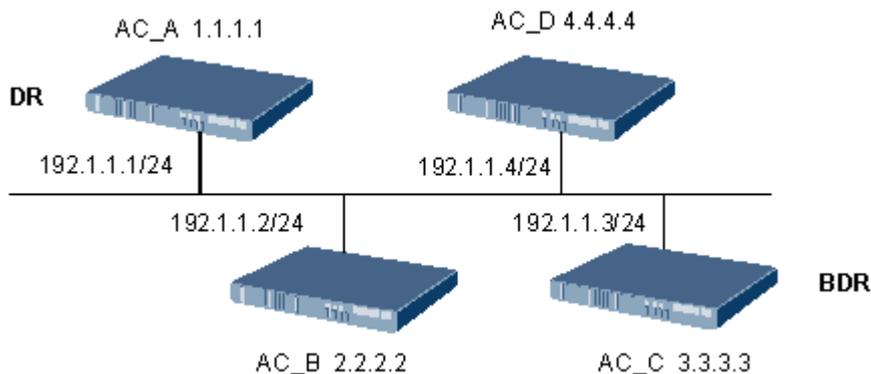
5.1.4 配置 OSPF 路由协议示例

通过本任务使配置数据后的相关设备正常运行 OSPF 协议。

业务需求

- 四台 AC 设备上均运行 OSPF 路由协议。
- AC_A 的 DR（Designated Router）优先级最高，AC_C 的 DR 优先级为次高，AC_A 做为 DR 实现对网络链路状态广播。

图 5-4 OSPF 路由协议配置组网图



数据规划

OSPF 路由协议配置数据规划如表 5-2 所示。

表 5-2 OSPF 路由协议配置数据规划表

配置项	数据	备注
AC_A	三层接口 IP 地址：192.1.1.1/24	-
	优先级：100	-
	VLAN ID：2	-
	Router ID：1.1.1.1	-
AC_B	三层接口 IP 地址：192.1.1.2/24	-

配置项	数据	备注
	优先级: 80	-
	VLAN ID: 2	-
	Router ID: 2.2.2.2	-
AC_C	三层接口 IP 地址: 192.1.1.3/24	-
	优先级: 90	-
	VLAN ID: 2	-
	Router ID: 3.3.3.3	-
AC_D	三层接口 IP 地址: 192.1.1.4/24	-
	优先级: 不配置	缺省值 1
	VLAN ID: 2	-
	Router ID: 4.4.4.4	-

前提条件

- 已配置各 AC 上行口的 Native VLAN，确保通信正常。
- AC 设备间的 OSPF 区域编号要一致。

操作步骤

步骤 1 在 AC_A 上执行的配置

- 配置 AC_A 的三层接口 IP 地址。

```

huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.1 24
huawei(config-if-vlanif2)#quit

```
- 配置 AC_A 的 OSPF Router ID。

```

huawei(config)#router id 1.1.1.1

```
- 启动 AC_A 的 OSPF 功能。

```

huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 1.1.1.1 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit

```
- 配置 AC_A 的 OSPF 优先级。

```

huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 100
huawei(config-if-vlanif2)#quit

```
- 保存数据。

```

huawei(config)#save

```

步骤 2 在 AC_B 上执行的配置

1. 配置 AC_B 的三层接口 IP 地址。
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.2 24
huawei(config-if-vlanif2)#quit
2. 配置 AC_B 的 OSPF Router ID。
huawei(config)#router id 2.2.2.2
3. 启动 AC_B 的 OSPF 功能。
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 2.2.2.2 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
4. 配置 AC_B 的 OSPF 优先级。
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 80
huawei(config-if-vlanif2)#quit
5. 保存数据。
huawei(config)#save

步骤 3 在 AC_C 上执行的配置

1. 配置 AC_C 的三层接口 IP 地址。
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.3 24
huawei(config-if-vlanif2)#quit
2. 配置 AC_C 的 OSPF Router ID。
huawei(config)#router id 3.3.3.3
3. 启动 AC_C 的 OSPF 功能。
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 3.3.3.3 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
4. 配置 AC_C 的 OSPF 优先级。
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ospf dr-priority 90
huawei(config-if-vlanif2)#quit
5. 保存数据。
huawei(config)#save

步骤 4 在 AC_D 上执行的配置

1. 配置 AC_D 的三层接口 IP 地址。
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 192.1.1.4 24
huawei(config-if-vlanif2)#quit
2. 配置 AC_D 的 OSPF Router ID。
huawei(config)#router id 4.4.4.4
3. 启动 AC_D 的 OSPF 功能。
huawei(config)#ospf
huawei(config-ospf-1)#area 0

```
huawei(config-ospf-1-area-0.0.0.0)#network 192.1.1.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#network 4.4.4.4 0.0.0.0
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```

4. 保存数据。

```
huawei(config)#save
```

---结束

操作结果

通过 **display ip routing-table** 命令能够查询学习到的路由表，主机之间能够实现互通。

配置文件

各 AC 的配置类似，这里以 AC_A 上的配置为例。

```
vlan 2
port vlan 2 0/2 24
interface vlanif 2
ip address 192.1.1.1 24
quit
router id 1.1.1.1
ospf
area 0
network 192.1.1.0 0.0.0.255
network 1.1.1.1 0.0.0.0
quit
quit
interface vlanif 2
ospf dr-priority 100
quit
save
```

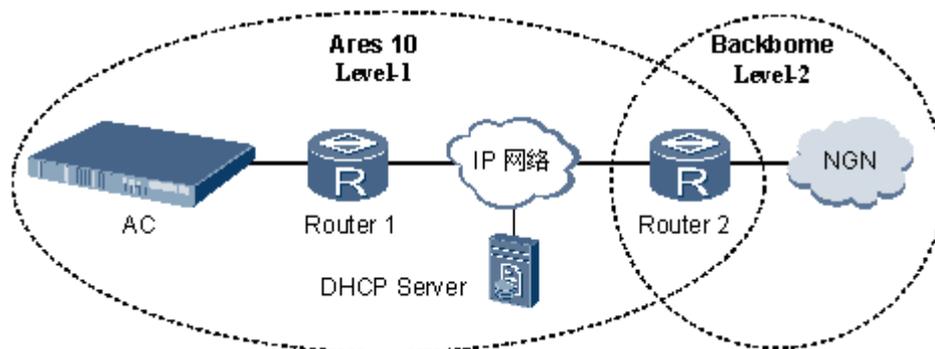
5.1.5 配置 IS-IS 路由协议示例

通过本任务使配置数据后的相关设备正常运行 IS-IS 协议。

业务需求

- AC 通过三层接口将其接入的业务转发到 NGN 网络中。
- AC 通过 IS-IS 协议学习到 NGN 网络的路由。与 Level-1-2 路由器相连的 Level-2 路由器的 Area ID，不同于 Level-1-2 路由器的 Area ID。

图 5-5 IS-IS 路由协议配置组网图



数据规划

IS-IS 路由协议配置数据规划如表 5-3 所示。

表 5-3 IS-IS 路由协议配置数据规划表

配置项	数据
AC	IS-IS 进程号： 1
	网络实体名称： 10.0000.0000.0001.00。其中： <ul style="list-style-type: none"> ● 区域 ID： 10 ● 系统 ID： 0000.0000.0001 ● Level 级别： Level-1 ● 主机名： AC
	IS-IS 接口： <ul style="list-style-type: none"> ● 端口号： 0/2/24 ● VLAN ID： 20 ● IP 地址： 192.15.24.5/16
Router1	IS-IS 进程号： 1
	网络实体名称： 10.0000.0000.0002.00。其中： <ul style="list-style-type: none"> ● 区域 ID： 10 ● 系统 ID： 0000.0000.0002 ● Level 级别： Level-1 ● 主机名： Router1
	IS-IS 接口： 1/0/0 IP 地址： 192.15.20.8/16
Router2	IS-IS 进程号： 1
	网络实体名称： 10.0000.0000.0005.00。其中： <ul style="list-style-type: none"> ● 区域 ID： 10 ● 系统 ID： 0000.0000.0005 ● Level 级别： Level-1-2 ● 主机名： Router2
	IS-IS 接口： 1/0/0 IP 地址： 192.15.18.5/16

操作步骤

- 在 AC 上配置 IS-IS 协议。
 1. 配置三层接口。
 huawei(config)#vlan 20
 huawei(config)#port vlan 20 0/2 24

```
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#ip address 192.15.24.5 16
huawei(config-if-vlanif20)#quit
```

2. 启动 IS-IS 进程。

```
huawei(config)#isis 1
huawei(config-isis-1)#
```

3. 配置网络实体名。

```
huawei(config-isis-1)#network-entity 10.0000.0000.0001.00
```

4. 配置路由器的 Level 级别。

```
huawei(config-isis-1)#is-level level-1
```

5. 配置本地主机名。

```
huawei(config-isis-1)#is-name AC
huawei(config-isis-1)#quit
```

6. 使能 IS-IS 接口。

```
huawei(config)#interface vlanif 20
huawei(config-if-vlanif20)#isis enable 1
```

- 在 Router1 上配置 IS-IS 协议。
与 AC 的配置相似，此处不再赘述。
- 在 Router2 上配置 IS-IS 协议。
与 AC 的配置相似，此处不再赘述。

----结束

操作结果

- 使用 **display isis lsdb** 命令可以查询到 IS-IS LSDB。
- 使用 **display isis route** 命令可以查询到 IS-IS 路由。Level-1 路由器的路由表中应该存在一条缺省路由，且下一跳为 Level-1-2 路由器；Level-2 路由器应该有去往所有 Level-1 和 Level-2 路由器的路由。

配置文件

```
vlan 20
port vlan 20 0/2 24
interface vlanif 20
ip address 192.15.24.5 16
quit
isis 1
network-entity 10.0000.0000.0001.00
is-level level-1
is-name AC
quit
interface vlanif 20
isis enable 1
```

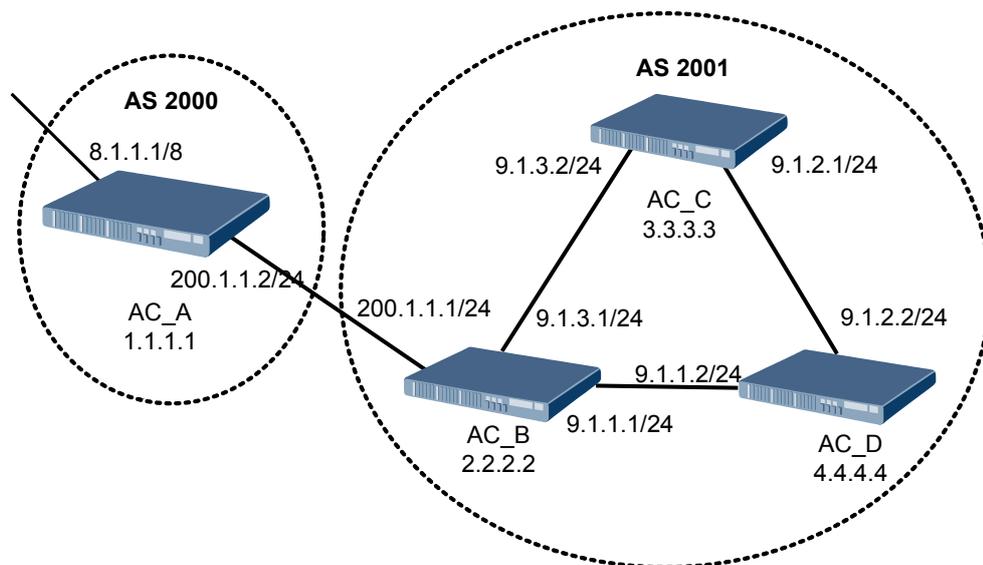
5.1.6 配置 BGP 路由协议示例

通过本任务使配置数据后的相关设备正常运行 BGP 协议。

业务需求

在 AC_A 和 AC_B 之间配置 EBGP 连接。在 AC_B、AC_C、AC_D 之间配置 IBGP 连接。

图 5-6 BGP 路由协议配置组网图



数据规划

BGP 路由协议配置数据规划如表 5-4 所示。

表 5-4 BGP 路由协议配置数据规划表

配置项	数据	备注
AC_A	VLAN 6 的接口 IP 地址： 200.1.1.2/24	用于与 AS2001 的 EBGP 连接。
	VLAN 2 的接口 IP 地址：8.1.1.1/8	-
	Router ID：1.1.1.1	-
	所属 AS 号：2000	-
AC_B	VLAN 6 的接口 IP 地址： 200.1.1.1/24	用于与 AS2000 的 EBGP 连接。
	VLAN 3 的接口 IP 地址： 9.1.3.1/24	用于与 AC_C 的 IBGP 连接。
	VLAN 4 的接口 IP 地址： 9.1.1.1/24	用于与 AC_D 的 IBGP 连接。
	Router ID：2.2.2.2	-
	所属 AS 号：2001	-
AC_C	VLAN 3 的接口 IP 地址： 9.1.3.2/24	用于与 AC_B 的 IBGP 连接。

配置项	数据	备注
	VLAN 5 的接口 IP 地址： 9.1.2.1/24	用于与 AC_D 的 IBGP 连接。
	Router ID: 3.3.3.3	-
	所属 AS 号: 2001	-
AC_D	VLAN 5 的接口 IP 地址： 9.1.2.2/24	用于与 AC_C 的 IBGP 连接。
	VLAN 4 的接口 IP 地址： 9.1.1.2/24	用于与 AC_B 的 IBGP 连接。
	Router ID: 4.4.4.4	-
	所属 AS 号: 2001	-

操作步骤

步骤 1 在 AC_A 上执行的配置

1. 配置 AC_A 的三层接口 IP 地址。

```

huawei(config)#vlan 6
huawei(config)#port vlan 6 0/2 16
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 200.1.1.2 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 2
huawei(config)#port vlan 2 0/2 24
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 8.1.1.1 8
huawei(config-if-vlanif2)#quit
    
```

2. 启动 AC_A 的 BGP 功能。

```

huawei(config)#bgp 2000
huawei(config-BGP)#router-id 1.1.1.1
huawei(config-BGP)#peer 200.1.1.1 as-number 2001
huawei(config-BGP)#network 8.0.0.0 8
huawei(config-BGP)#quit
    
```

3. 保存数据。

```

huawei(config)#save
    
```

步骤 2 在 AC_B 上执行的配置

1. 配置 AC_B 的三层接口 IP 地址。

```

huawei(config)#vlan 6
huawei(config)#port vlan 6 0/2 16
huawei(config)#interface vlanif 6
huawei(config-if-vlanif6)#ip address 200.1.1.1 24
huawei(config-if-vlanif6)#quit
huawei(config)#vlan 3
huawei(config)#port vlan 3 0/2 18
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.1 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 4
huawei(config)#port vlan 4 0/2 17
huawei(config)#interface vlanif 4
    
```

```
huawei(config-if-vlanif4)#ip address 9.1.1.1 24
huawei(config-if-vlanif4)#quit
```

2. 启动 AC_B 的 BGP 功能。

```
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 2.2.2.2
huawei(config-BGP)#peer 200.1.1.2 as-number 2000
huawei(config-BGP)#peer 9.1.3.2 as-number 2001
huawei(config-BGP)#peer 9.1.1.2 as-number 2001
huawei(config-BGP)#import-route direct
huawei(config-BGP)#quit
```

3. 保存数据。

```
huawei(config)#save
```

步骤 3 在 AC_C 上执行的配置

1. 配置 AC_C 的三层接口 IP 地址。

```
huawei(config)#vlan 3
huawei(config)#port vlan 3 0/2 18
huawei(config)#interface vlanif 3
huawei(config-if-vlanif3)#ip address 9.1.3.2 24
huawei(config-if-vlanif3)#quit
huawei(config)#vlan 5
huawei(config)#port vlan 5 0/2 19
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ip address 9.1.2.1 24
huawei(config-if-vlanif5)#quit
```

2. 启动 AC_C 的 BGP 功能。

```
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 3.3.3.3
huawei(config-BGP)#peer 9.1.3.1 as-number 2001
huawei(config-BGP)#peer 9.1.2.2 as-number 2001
huawei(config-BGP)#quit
```

3. 保存数据。

```
huawei(config)#save
```

步骤 4 在 AC_D 上执行的配置

1. 配置 AC_D 的三层接口 IP 地址。

```
huawei(config)#vlan 4
huawei(config)#port vlan 4 0/2 17
huawei(config)#interface vlanif 4
huawei(config-if-vlanif4)#ip address 9.1.1.2 24
huawei(config-if-vlanif4)#quit
huawei(config)#vlan 5 smart
huawei(config)#port vlan 5 0/2 19
huawei(config)#interface vlanif 5
huawei(config-if-vlanif5)#ip address 9.1.2.2 24
huawei(config-if-vlanif5)#quit
```

2. 启动 AC_D 的 BGP 功能。

```
huawei(config)#bgp 2001
huawei(config-BGP)#router-id 4.4.4.4
huawei(config-BGP)#peer 9.1.2.1 as-number 2001
huawei(config-BGP)#peer 9.1.1.1 as-number 2001
huawei(config-BGP)#quit
```

3. 保存数据。

```
huawei(config)#save
```

----结束

操作结果

- 通过 **display bgp routing-table** 命令可看到：
 - 在 AC_A 上与 AC_B 建立了 EBGP 连接。
 - 在 AC_B、AC_C、AC_D 建立了 IBGP 连接。
 - 在 AC_C 和 AC_D 上有目的网段为 8.0.0.0/8 的路由，其下一跳为 AC_A 的接口地址。
- 可在 AC_C 和 AC_D 上使用 **ping** 命令，结果为与 AC_A 的 IP 为 8.1.1.1/24 的三层接口互通。

配置文件

各 AC 的配置类似，这里以 AC_A 上的配置为例。

```
vlan 6
port vlan 6 0/2 16
interface vlanif 6
ip address 200.1.1.2 24
quit
vlan 2
port vlan 2 0/2 24
interface vlanif 2
ip address 8.1.1.1 8
quit
bgp 2000
router-id 1.1.1.1
peer 200.1.1.1 as-number 2001
network 8.0.0.0 8
quit
```

5.2 配置 DHCP

AC 设备在网络中能够实现 DHCP Relay 功能。配置 DHCP Relay 适用于用户通过 DHCP 协议动态地从 DHCP 服务器获取 IP 地址的场景。

背景信息

AC 设备可以工作在 DHCP Relay 的二层方式或者三层方式下，对用户和 DHCP 服务器之间交互的 DHCP 报文进行转发。系统默认工作在二层方式下，透传用户发起的 DHCP 报文，不需要进行配置。如果 AC 工作在三层方式下，要求 DHCP 服务器支持 DHCP Relay 的功能并且进行相关的配置。三层工作方式又划分为以下三种工作模式：

- DHCP 标准模式
AC 通过识别用户所属 VLAN（在设备上建立业务虚端口时所使用的 VLAN），为不同的 VLAN 绑定其对应的 DHCP 服务器组。
DHCP 标准模式的配置思路主要是：首先进行 DHCP Relay 工作模式的配置，然后配置 DHCP 服务器组，最后为 VLAN 绑定 DHCP 服务器组。
- DHCP Option60 模式
AC 可以通过用户终端发出的 DHCP 报文中的 Option60 字段来区分用户，为不同的 Option60 域绑定其对应的 DHCP 服务器组。
DHCP Option60 模式的配置思路主要是：首先进行 DHCP Relay 工作模式的配置，其次配置 DHCP 服务器组，然后创建 Option60 域，最后绑定 Option60 域与服务器。
- MAC 地址段模式

AC 可以通过用户终端所处的 MAC 地址段来区分用户，为不同的 MAC 地址段绑定其对应的 DHCP 服务器组。

MAC 地址段模式的配置思路主要是：首先进行 DHCP Relay 工作模式的配置，其次配置 DHCP 服务器组，然后定义 MAC 地址段，最后绑定 MAC 地址段与服务器。

5.2.1 配置 DHCP 标准模式

配置 DHCP 标准模式适用于为 VLAN（在设备上建立业务虚端口时所使用的 VLAN）不同的用户指定其对应的 DHCP 服务器组的场景。

前提条件

已经完成 VLAN 的配置。

操作步骤

步骤 1 配置 DHCP 转发模式。

配置 DHCP 转发模式有两种方式，可以二选一：

- 在全局配置模式下，使用 **dhcp mode layer-3 standard** 命令配置 DHCP Relay 的工作模式为三层标准模式（layer-3,standard）。如果选择了 **VLAN** 关键字，并且输入了 **VLAN ID**，则此配置仅针对该 VLAN 生效。



选择的 VLAN 需要配置了 VLANIF 且不能绑定模板。

- 在 VLAN 业务模板中配置：
 1. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
 2. 使用 **dhcp mode layer-3 standard** 命令进行配置。
 3. 使用 **commit** 命令使模板配置参数生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
 4. 使用 **quit** 命令退出 VLAN 业务模板模式。
 5. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 1.1 配置的 VLAN 业务模板。

步骤 2 配置 DHCP 服务器组。

1. 在全局配置模式下，使用 **dhcp-server** 命令创建 DHCP 服务器组。
 - **igroup-number**：DHCP Server 组的组号，用以标识一个服务器组。可以先使用 **display dhcp-server all-group** 查看已经配置的 DHCP 服务器组，确定一个系统没有使用的 DHCP 服务器组号。
 - **ip-addr**：DHCP 服务器组内的 DHCP 服务器的 IP 地址，最多可以输入 4 台服务器的 IP 地址。



注意

在此处配置的 DHCP 服务器 IP 地址需要与实际工作在网络侧的 DHCP 服务器 IP 地址保持一致。

2. （可选）使用 **dhcp server mode** 命令配置 DHCP 服务器的工作模式。

DHCP 服务器组中的 DHCP 服务器可以工作在负荷分担模式或者主备模式，系统缺省值为负荷分担模式。

步骤 3 绑定 VLAN 与 DHCP 服务器。

1. 在全局配置模式下，使用 **interface vlanif** 创建 VLAN 三层接口。
VLANID 必须与前提条件中已经创建的 VLANID 相同。
2. 在 VLANIF 模式下，使用 **ip address** 为 VLAN 三层接口配置 IP 地址。
配置完成后，VLAN 中的 IP 报文以此 IP 地址作为源 IP 地址进行三层转发。



注意

- 如果 AC 到 DHCP 服务器之间只有二层设备，则 VLAN 三层接口的 IP 地址应当与 DHCP 服务器的 IP 地址在同一网段。
- 如果 AC 的上级设备为三层设备，则 VLAN 接口的 IP 地址与 DHCP 服务器的 IP 地址可以不在同一网段，但是必须保证此 VLAN 接口与 DHCP 服务器之间存在路由。

3. 在 VLANIF 模式下，使用 **dhcp-server** 为该 VLAN 绑定 DHCP 服务器。
该命令需要输入 **group-number** 参数，此参数的取值为已经创建的 DHCP Server 组的组号。

----结束

任务示例

举例：为 VLAN 2（三层接口 IP 地址为 10.1.1.101）的用户绑定服务器组 1，服务器组 1 包含两台 DHCP 服务器，两台 DHCP 服务器工作于主备方式，DHCP 服务器响应最大时间为 20s，DHCP 服务器响应超时的最大次数为 10，主用服务器 IP 地址为 10.1.1.9，备用服务器 IP 地址为 10.1.1.10。

```
huawei(config)#dhcp mode layer-3 standard
huawei(config)#dhcp server mode backup 20 10
huawei(config)#dhcp-server 1 ip 10.1.1.9 10.1.1.10
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.1.101 24
huawei(config-if-vlanif2)#dhcp-server 1
huawei(config-if-vlanif2)#quit
```

5.2.2 配置 DHCP Server 模式

配置 DHCP Server 模式适用于为 AC 直接作为 DHCP 服务器为 AP 提供 DHCP 服务功能。

前提条件

已经完成 VLAN 的配置。

操作步骤

步骤 1 绑定 VLAN 与使能 DHCP 服务功能。

1. 在全局配置模式下，使用 **interface vlanif** 创建 VLAN 三层接口。

VLANID 必须与前提条件中已经创建的 VLANID 相同。

2. 在 VLANIF 模式下，使用 **ip address** 为 VLAN 三层接口配置 IP 地址。
配置完成后，VLAN 中的 IP 报文以此 IP 地址作为源 IP 地址进行三层转发。



- 如果 AC 到 DHCP 服务器之间只有二层设备，则 VLAN 三层接口的 IP 地址应当与 DHCP 服务器的 IP 地址在同一网段。
- 如果 AC 的上级设备为三层设备，则 VLAN 接口的 IP 地址与 DHCP 服务器的 IP 地址可以不在同一网段，但是必须保证此 VLAN 接口与 DHCP 服务器之间存在路由。

3. 在 VLANIF 模式下，使用 **dhcps enable** 使能该 VLANIF 接口的 DHCP 服务功能。

步骤 2 创建与 VLANIF 接口对应的 IP 地址池。

1. 在全局配置模式下，使用 **ip pool** 创建 IP 地址池。
2. 在 IP 地址池模式下，使用 **gateway** 设置 IP 地址池的网关地址，需要与 VLANIF 接口地址对应。

---结束

任务示例

举例：使能 VLANIF 2（三层接口 IP 地址为 10.1.1.101）的 DHCP 服务功能，创建 IP 地址池 ap-server 作为 VLANIF 接口对应的 IP 地址池。

```
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.1.101 255.255.255.0
huawei(config-if-vlanif2)#dhcps enable
huawei(config-if-vlanif2)#quit
huawei(config)#ip pool ap-server
huawei(config-ip-pool-ap-server)#gateway 10.1.1.101 255.255.255.0
huawei(config-ip-pool-ap-server)#quit
```

5.2.3 配置 DHCP Option43 模式

配置 DHCP Option43 模式主要应用在 WLAN 业务中 AP 设备从 DHCP 服务器获取地址后，通过 DHCP 服务器下发 Option43 属性发现 AC 设备并完成注册。

前提条件

- 已经完成 VLAN 的配置。
- Option43 属性已经定义。

背景信息

AC 设备开展 WLAN 业务时，如果 AP 从网络中的 DHCP 服务器获取 IP 地址，则需要 AC 设备上启动 DHCP Option43 功能，将 AC 设备的 IP 地址通过 Option43 方式通知 DHCP 服务器。这样 DHCP 服务器在给 AP 分配 IP 地址时，会将 AC 设备的 IP 地址通过相关报文通知给 AP，这样 AP 在获取 IP 地址后才能与 AC 设备建立连接。

操作步骤

步骤 1 在 AC 上创建 VLANIF。

#VLANIF 800 的 IP 地址为 172.1.1.1，作为数据转发的三层接口。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
ip address 172.1.1.1 255.255.255.0
```

步骤 2 设置 AC 的源。

#配置 VLANIF 800 作为 AC 的源。

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

步骤 3 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ctc-ap-server 对应 VLAN 800。

说明

IP 地址池的网关地址必须与 VLANIF 的 IP 地址相同，用于定义 AP 上线后获取 IP 的地址池。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
```

步骤 4 配置 DHCP 服务的 Option 功能，通过 DHCP option43 通告 AC 的 IP 地址。

#配置 AC 设备向网络通告其 IP 地址为 172.1.1.1。

```
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-172.1.1.1
huawei(config-ip-pool-ap-server)#quit
```



注意

- 当 AP 需要获取 AC 的 IP 地址时，如果在二层组网情况下，此字段是可选的，如果在三层组网情况下，此字段是必选的。
- 配置 Option 43 时，请注意 option 选项参数的格式必须为“HuaweiAC-x.x.x.x”，其中“x.x.x.x”为 IP 地址。
- 如果涉及多个 IP 地址，则格式必须为“HuaweiAC-x.x.x.x,x.x.x.x”，即 IP 地址之间用逗号隔开。

---结束

任务示例

#在 AC 设备上创建 VLANIF 800，配置 IP 地址为 172.1.1.1，设置 VLANIF 800 为 AC 设备的源地址，创建 IP 地址池 ap-server，配置 AC 设备向网络通告其 IP 地址为 172.1.1.1。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

```
Command:
```

```
ip address 172.1.1.1 255.255.255.0
huawei(config-if-vlanif800)#quit
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
huawei(config-ip-pool-ap-server)#option 43 string HuaweiAC-172.1.1.1
huawei(config-ip-pool-ap-server)#quit
```

5.2.4 配置 DHCP Option60 模式

配置 DHCP Option60 模式适用于为不同 Option60 域的用户指定其对应的 DHCP 服务器组的场景。

前提条件

- 已经完成 VLAN 的配置。
- 在配置前，需要确定用户终端的 Option60 域名。

背景信息

在 AC 设备开展多业务时，如视频组播、IP 电话这些业务由不同的业务提供商提供，他们可能使用不同的 DHCP Server 或同一 DHCP Server 下不同的 Relay IP 地址来为用户分配 IP 地址等信息，所以需要配置用户使用 DHCP Option60 模式从 DHCP Server 上申请 IP 地址。

DHCP Option60 模式是指按照 DHCP 报文的 Option60 选项中的字符串（称之为域名）来选择 DHCP 服务器组。此时，需要事先配置好 Option60 域名和域名绑定的 DHCP 服务器组。该模式的实质是按照报文的“域”信息来区分用户，可以区分相同 VLAN 中的不同业务类型。

操作步骤

步骤 1 配置 DHCP 转发模式。

配置 DHCP 转发模式有两种方式，可以二选一：

- 在全局配置模式下，使用 **dhcp mode layer-3 option60** 命令配置 DHCP Reley 的工作模式为三层 Option60 模式（layer-3,option60）。如果选择了 VLAN 关键字，并且输入了 VLANID，则此配置仅针对该 VLAN 生效。

说明

选择的 VLAN 需要配置了 VLANIF 且不能绑定模板。

- 在 VLAN 业务模板中配置：
 1. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
 2. 使用 **dhcp mode layer-3 option60** 命令进行配置。
 3. 使用 **commit** 命令使模板配置参数生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
 4. 使用 **quit** 命令退出 VLAN 业务模板模式。
 5. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 1.1 配置的 VLAN 业务模板。

步骤 2 配置 DHCP 服务器组。

1. 在全局配置模式下，使用 **dhcp-server** 命令创建 DHCP 服务器组。
 - **igroup-number**: DHCP Server 组的组号，用以标识一个服务器组。可以先使用 **display dhcp-server all-group** 查看已经配置的 DHCP 服务器组，确定一个系统没有使用的 DHCP 服务器组号。
 - **ip-addr**: DHCP 服务器组内的 DHCP 服务器的 IP 地址，最多可以输入 4 台服务器的 IP 地址。



注意

在此处配置的 DHCP 服务器 IP 地址需要与实际工作在网络侧的 DHCP 服务器 IP 地址保持一致。

2. (可选) 使用 **dhcp server mode** 命令配置 DHCP 服务器的工作模式。

DHCP 服务器组中的 DHCP 服务器可以工作在负荷分担模式或者主备模式，系统缺省值为负荷分担模式。

步骤 3 创建 DHCP Option60 域。

在全局配置模式下，使用 **dhcp domain** 命令创建 DHCP 域并进入 DHCP 域模式。Option60 域的域名需要根据相连接的终端设备类型来配置。

步骤 4 绑定 DHCP Option60 域与 DHCP 服务器组。

在 Option60 域模式下，使用 **dhcp-server** 命令给 DHCP 域绑定 DHCP Server 组。配置完成后，属于该 DHCP 域的客户端将对应到 DHCP Server 服务器组。

步骤 5 配置域相应的网关地址。

1. 在全局配置模式下，使用 **interface vlanif** 创建 VLAN 三层接口。
VLANID 必须与前提条件中已经创建的 VLANID 相同。
2. 在 VLANIF 模式下，使用 **ip address** 为 VLAN 三层接口配置 IP 地址。
配置完成后，VLAN 中的 IP 报文以此 IP 地址作为源 IP 地址进行三层转发。



注意

- 如果 AC 到 DHCP 服务器之间只有二层设备，则 VLAN 接口的 IP 地址应当与 DHCP 服务器的 IP 地址在同一网段。
- 如果 AC 的上级设备为三层设备，则 VLAN 接口的 IP 地址与 DHCP 服务器的 IP 地址可以不在同一网段，但是必须保证此 VLAN 接口与 DHCP 服务器之间存在路由。

3. 在 VLANIF 模式下，使用 **dhcp domain gateway** 命令配置 DHCP 域相应的 IP 网关地址。

这个网关地址必须是在 VLAN 接口下已经配置的接口 IP 地址。因为在同一个 VLAN 接口下，可以为不同的 Option60 域配置不同的网关，所以能实现按照报文的“域”信息来选择不同的 DHCP 服务器。

---结束

任务示例

举例：为 VLAN2（三层接口 IP 地址为 10.1.2.1/24）中的 Option60 域名为 msft 的用户绑定服务器组 2，服务器组 2 包含两台 DHCP 服务器，两台 DHCP 服务器工作于负荷分担模式，主用服务器 IP 地址为 10.10.10.10，备用服务器 IP 地址为 10.10.10.11。

```
huawei(config)#dhcp mode layer-3 Option60
huawei(config)#dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei(config)#dhcp domain msft
huawei(config-dhcp-domain-msft)#dhcp-server 2
huawei(config-dhcp-domain-msft)#quit
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.2.1 24
huawei(config-if-vlanif2)#dhcp domain msft gateway 10.1.2.1
```

5.2.5 配置 DHCP Option15 模式

配置 DHCP Option15 模式主要应用在 WLAN 业务中 AP 设备从 DHCP 服务器获取地址后，通过 DNS 服务器获取 AC 的 IP 地址。

前提条件

- 已经完成 VLAN 的配置。
- DNS 服务器上已按照规划配置了域名和 IP 地址的对应关系。
- Option15 属性已经定义。

背景信息

AC 设备开展 WLAN 业务时，如果 AP 设置从网络中的 DHCP 服务器获取 IP 地址，可以在 AC 设备上启动 DHCP Option15 功能，将 AC 设备的域名和对应解析域名的 DNS 服务器的 IP 地址发送给 DHCP 服务器。这样 AP 获得 DHCP 服务器分配的 IP 地址时，同时获得了 AC 设备的域名和对应 DNS 服务器的 IP 地址，AP 将域名发送给 DNS 服务器进行解析即可获得 AC 设备的 IP 地址。

操作步骤

步骤 1 在 AC 上创建 VLANIF。

#VLANIF 800 的 IP 地址为 172.1.1.1，作为数据转发的三层接口。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 172.1.1.1 255.255.255.0
```

步骤 2 设置 AC 的源。

#配置 VLANIF 800 作为 AC 的源。

 说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
```

步骤 3 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ctc-ap-server 对应 VLAN 800。



说明

IP 地址池的网关地址必须与 VLANIF 的 IP 地址相同，用于定义 AP 上线后获取 IP 的地址池。

```
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
```

- 步骤 4** 配置 DHCP 服务的 Option 15 功能，通过 DHCP option15 通告 AC 设备的域名和对应解析域名的 DNS 服务器的 IP 地址。

#配置 IP 地址池 ap-server 的 DNS 后缀为 huawei.com。

```
huawei(config-ip-pool-ap-server)#dns-suffix huawei.com
```

#在 IP 地址池 ap-server 上创建 DNS 主服务器，IP 地址为 172.10.1.1。

```
huawei(config-ip-pool-ap-server)#dns-server 172.10.1.1
huawei(config-ip-pool-ap-server)#quit
```

----结束

任务示例

#在 AC 设备上创建 VLANIF 800，配置 IP 地址为 172.1.1.1，设置 VLANIF 800 为 AC 设备的源地址，创建 IP 地址池 ap-server，配置 AC 设备域名为 huawei.com，对应解析域名的 DNS 服务器 IP 地址为 172.10.1.1。

```
huawei(config)#interface vlanif 800
huawei(config-if-vlanif800)#ip address 172.1.1.1 255.255.255.0
{ <cr>|description<K>|sub<K> }:
```

Command:

```
ip address 172.1.1.1 255.255.255.0
huawei(config-if-vlanif800)#quit
huawei(config)#wlan ac
huawei(config-wlan-ac-view)#wlan ac source interface vlanif 800
huawei(config-wlan-ac-view)#quit
huawei(config)#ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)#gateway 172.1.1.1 255.255.255.0
huawei(config-ip-pool-ap-server)#section 0 172.1.1.2 172.1.1.254
huawei(config-ip-pool-ap-server)#dns-suffix huawei.com
huawei(config-ip-pool-ap-server)#dns-server 172.10.1.1
{ <cr>|secondary<K>|third<K> }:
```

Command:

```
dns-server 172.10.1.1
huawei(config-ip-pool-ap-server)#quit
```

5.2.6 配置 DHCP MAC 地址段模式

配置 DHCP MAC 地址段模式适用于为不同 MAC 地址段的用户指定其对应的 DHCP 服务器组的场景。

前提条件

已经完成 VLAN 的配置。

背景信息

在组网时，网络中会同时存在多家厂商的设备，而每个厂商的设备都有一个固定的 MAC 地址段，此时则可以使用 MAC 地址段模式的 DHCP Relay 方式来从 DHCP Server 获取 IP 地址。

AC 支持基于 MAC 地址段选择 DHCP Server，配置完成后，此 MAC 地址段的客户端将会从对应的 DHCP Server 上获得 IP 地址。

操作步骤

步骤 1 配置 DHCP 转发模式。

配置 DHCP 转发模式有两种方式，可以二选一：

- 在全局配置模式下，使用 **dhcp mode layer - 3 mac-range** 命令配置 DHCP Reley 的工作模式为三层 MAC 地址段模式（layer - 3,mac-range）。如果选择了 **VLAN** 关键字，并且输入了 *VLANID*，则此配置仅针对该 VLAN 生效。



说明

选择的 VLAN 需要配置了 VLANIF 且不能绑定模板。

- 在 VLAN 业务模板中配置：
 1. 使用 **vlan service-profile** 命令创建 VLAN 业务模板并进入 VLAN 业务模板模式。
 2. 使用 **dhcp mode layer - 3 mac-range** 命令进行配置。
 3. 使用 **commit** 命令使模板配置参数生效。必须执行此操作 VLAN 业务模板相关配置才能生效。
 4. 使用 **quit** 命令退出 VLAN 业务模板模式。
 5. 使用 **vlan bind service-profile** 命令为 VLAN 绑定步骤 1.1 配置的 VLAN 业务模板。

步骤 2 配置 DHCP 服务器组。

1. 在全局配置模式下，使用 **dhcp-server** 命令创建 DHCP 服务器组。
 - *igroup-number*: DHCP Server 组的组号，用以标识一个服务器组。可以先使用 **display dhcp-server all-group** 查看已经配置的 DHCP 服务器组，确定一个系统没有使用的 DHCP 服务器组号。
 - *ip-addr*: DHCP 服务器组内的 DHCP 服务器的 IP 地址，最多可以输入 4 台服务器的 IP 地址。



注意

在此处配置的 DHCP 服务器 IP 地址需要与实际工作在网络侧的 DHCP 服务器 IP 地址保持一致。

2. （可选）使用 **dhcp server mode** 命令配置 DHCP 服务器的工作模式。

DHCP 服务器组中的 DHCP 服务器可以工作在负荷分担模式或者主备模式，系统缺省值为负荷分担模式。

步骤 3 定义 MAC 地址段。

1. 在全局配置模式下，使用 **dhcp mac-range** 命令创建 MAC 地址段并进入 MAC 地址段模式。

range-name 参数为 MAC 地址段的名称，地址段名称能起到注释作用，无其他特殊意义。
2. 在 MAC 地址段模式下，使用 **mac-range** 命令用于设置 MAC 地址范围。

步骤 4 绑定 MAC 地址段与 DHCP 服务器。

在 MAC 地址段模式下，使用 **dhcp-server** 命令为该 MAC 地址段绑定 DHCP Server 组。

步骤 5 配置 MAC 地址段相应的网关地址。

1. 在全局配置模式下，使用 **interface vlanif** 创建 VLAN 三层接口。
VLANID 必须与前提条件中已经创建的 VLANID 相同。
2. 在 VLANIF 模式下，使用 **ip address** 为 VLAN 三层接口配置 IP 地址。
配置完成后，VLAN 中的 IP 报文以此 IP 地址作为源 IP 地址进行三层转发。



注意

- 如果 AC 到 DHCP 服务器之间只有二层设备，则 vlan 接口的 IP 地址应当与 DHCP 服务器的 IP 地址在同一网段。
 - 如果 AC 的上级设备为三层设备，则 vlan 接口的 IP 地址与 DHCP 服务器的 IP 地址可以不在同一网段，但是必须保证此 VLAN 接口与 DHCP 服务器之间存在路由。
3. 在 VLANIF 模式下，使用 **dhcp mac-range gateway** 命令配置 DHCP 域相应的 IP 网关地址。
这个网关地址必须是在 VLAN 接口下已经配置的接口 IP 地址。因为在同一个 VLAN 接口下，可以为不同的 MAC 地址段配置不同的网关，所以能实现按照报文的 MAC 地址段信息来选择不同的 DHCP 服务器。

----结束

任务示例

举例：为 VLAN2（三层接口 IP 地址为 10.1.2.1/24）中的部分用户（MAC 地址段在 0000-0000-0001 到 0000-0000-0100 之间）绑定服务器组 2，服务器组包含两台 DHCP 服务器，两台 DHCP 服务器工作于负荷分担模式，主用服务器 IP 地址为 10.10.10.10，备用服务器 IP 地址为 10.10.10.11。

```
huawei(config)#dhcp mode layer-3 mac-range
huawei(config)#dhcp-server 2 ip 10.10.10.10 10.10.10.11
huawei(config)#dhcp mac-range huawei
huawei(config-mac-range-huawei)#mac-range 0000-0000-0001 to 0000-0000-0100
huawei(config-mac-range-huawei)#dhcp-server 2
huawei(config-mac-range-huawei)#quit
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip address 10.1.2.1 24
huawei(config-if-vlanif2)#dhcp mac-range huawei gateway 10.1.2.1
```

5.3 配置 AAA

介绍在 AC 设备上 AAA 配置的过程，包括 AC 作为本地 AAA 服务器和远程 AAA 服务器的配置过程。

背景信息

AAA 是指 Authentication, Authorization and Accounting，亦即认证、授权、计费。在用户访问网络资源的过程中，对通过认证的用户授予一定的权限，并记录用户使用网络的原始数据。

- Authentication(认证)：确认用户是否被允许访问网络资源。
- Authorization(授权)：确认用户可以访问哪些网络资源。

- Accounting(计费): 记录用户访问网络资源的原始数据。

应用环境

AAA 认证一般用于 PPPoA、PPPoE、802.1X、VLAN、WLAN、ISDN、Admin Telnet (通过域名关联用户名和密码) 等方式接入的用户。

AAA 功能应用组网图如图 5-7 所示。

图 5-7 AAA 功能应用组网图



上图说明在 AC 上启用 AAA 功能时，有两种应用方法：

- AC 作为本地 AAA 服务器使用，此时配置本地 AAA 功能。本地 AAA 不支持计费功能。
- AC 作为远程 AAA 服务器的客户端，通过 RADIUS 协议与 RADIUS server 连接，实现 AAA 功能。RADIUS 协议不支持授权功能。

5.3.1 配置远程 AAA (RADIUS 协议)

AC 使用 RADIUS 协议与 RADIUS 服务器对接，完成认证、计费功能。

背景信息

- RADIUS 的定义：
 - RADIUS (Remote Authentication Dial-In User Service) 是远程认证拨号用户服务的简称，它是一种分布式的、服务器-客户端结构的信息交互协议，常用来管理大量分散的拨号用户。
 - RADIUS 通过管理一个简单的用户数据库来对用户进行认证和计费。
 - 用户通过 NAS (Network Access Server) 把认证和计费请求传递给 RADIUS 服务器。
- RADIUS 的工作原理：
 - 当用户想要通过某个网络与 NAS 建立连接从而获得访问其它网络的权利时 (或取得使用某些网络资源的权利)，NAS 负责把用户的认证、计费信息传递给 RADIUS 服务器。RADIUS 协议规定了 NAS 与 RADIUS 服务器之间如何传递用户信息和计费信息。
 - RADIUS 服务器负责接收 NAS 发送的用户连接请求，对用户的名称和密码完成认证，并把用户所需的配置信息返回给 NAS。
- 配置规格：
 - AC 的 RADIUS 协议配置是以 RADIUS 服务器组为单位进行的。
 - 一个 RADIUS 服务器组在实际组网环境中：
 - 可以是一台独立的 RADIUS 服务器。
 - 可以是两台配置相同、但 IP 地址不同的主/备 RADIUS 服务器。
 - 每个 RADIUS 服务器模板的属性包括：

- 主服务器的 IP 地址。
- 备份服务器的 IP 地址。
- 共享密钥以及 RADIUS 服务器类型。
- RADIUS 协议配置只是定义了 AC 和 RADIUS Server 之间进行信息交互所必须的一些参数。为了使这些参数能够生效，必须在某个域引用该 RADIUS 服务器组。

操作步骤

- 配置认证方案。

说明

- 认证方案用来指定系统对该 ISP(Internet Service Provider)域下所有用户使用的认证方法。
- 系统最多可配置 16 个认证方案。缺省情况下，系统有一个“default”方案，不能删除，只能修改其认证方式。

1. 使用 **aaa** 命令进入 AAA 模式。
2. 使用 **authentication-scheme** 命令添加认证方案。
3. 使用 **authentication-mode radius** 命令配置认证方案的认证方式。
4. 使用 **quit** 命令退出域模式。

- 配置计费方案。

说明

- 计费方案用来指定系统对该 ISP(Internet Service Provider)域下所有用户使用的计费方法。
- 系统最多可配置 128 个计费方案。缺省情况下，系统有一个“default”方案，不能删除，只能修改其计费方式。

1. 在 AAA 模式下，使用 **accounting-scheme** 命令新增一个 AAA 计费方案。
2. 使用 **accounting-mode radius** 命令配置计费模式。
3. 使用 **accounting interim interval** 命令配置实时计费间隔时间。系统缺省值为 0min，即不进行实时计费。
4. 使用 **quit** 命令退出域模式。

- 配置 RADIUS 服务器模板。

1. 使用 **radius-server template** 命令创建 RADIUS 服务器模板并进入相应的配置模式。
2. 使用 **radius-server authentication** 命令配置 RADIUS 认证服务器的 IP 地址和 UDP 端口号。

说明

- 为了保证 AC 与 RADIUS 服务器能够正常交互，在设置 RADIUS 服务器的 IP 地址和 UDP 端口之前，必须确保 RADIUS 服务器与 AC 的路由连接正常。
 - 必须保证 AC 上的 RADIUS 服务端口配置与 RADIUS 服务器上的端口配置保持一致。
3. 使用 **radius-server accounting** 命令配置 RADIUS 计费服务器的 IP 地址和 UDP 端口号。
 4. (可选) 使用 **radius-server shared-key** 命令配置 RADIUS 服务器的共享密钥。

说明

- RADIUS 客户端（即 AC）与 RADIUS 服务器使用 MD5 算法来加密 RADIUS 报文，双方通过配置加密密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。
- 缺省情况下，RADIUS 服务器的共享密钥为“huawei”。

5. (可选) 使用 **radius-server timeout** 命令配置 RADIUS 服务器响应超时时长。系统缺省值为 5s。

如果在 RADIUS 请求报文传送出去, 在超过超时时长后 AC 还没有得到 RADIUS 服务器的响应, 则重传 RADIUS 请求报文, 以保证用户确实能够得到 RADIUS 服务。

6. (可选) 使用 **radius-server retransmit** 命令配置服务器请求报文的最大传送次数。系统缺省值为 3。

当 AC 向 RADIUS 服务器重传 RADIUS 请求报文的次数超过最大传送次数, AC 认为与当前 RADIUS 服务器的通信已经中断, 并将转而向其它 RADIUS 服务器发送请求报文。

7. (可选) 使用 **(undo)radius-server user-name domain-included** 命令配置发送给 RADIUS 服务器的用户名是否携带域名。缺省情况下, RADIUS 服务器的用户名携带域名。
 - 接入用户通常以 “userid@domain-name” 的格式命名, “@” 后面的部分为域名, AC 通过该域名来决定将用户归于哪个域。
 - 如果指定某个 RADIUS 服务器组不允许用户名中携带域名, 那么该 RADIUS 服务器组不能在两个乃至两个以上的域中同时配置使用。否则, 当接入用户名相同时, 会出现虽然实际用户不同 (在不同的域中) 但 RADIUS 服务器认为用户相同 (因为传送到它的用户名相同) 的错误。

8. 使用 **quit** 命令返回到全局配置模式。

- 创建域。

域是用户群, 一个域是由同属于一类用户构成的用户群。

一般说来, 在 “userid@domain-name” 形式 (例如 huawei20041028@huawei.net) 的用户名中, “@” 后的 “domain-name” 即为域名, “userid” 作为用于身份认证的用户名。

用于用户登陆的域名长度不大于 15 个字符, 其余不大于 20 个字符。

1. 使用 **aaa** 命令进入 AAA 模式。
2. 在 AAA 模式下, 使用 **domain** 命令创建域。

- 引用 RADIUS 服务器模板。

 说明

必须先创建 RADIUS 服务器模板, 才可以在域中引用它。

1. 在域模式下, 使用 **radius-server template** 命令引用 RADIUS 服务器模板。
2. 使用 **quit** 命令返回到 AAA 模式。

----结束

任务示例

举例: 域 isp 下的用户 user1 采用 RADIUS 协议与 RADIUS 服务器进行认证、计费。计费间隔为 10min, 认证密码为 a123456。RADIUS 服务器 129.7.66.66 作为主认证和计费服务器。129.7.66.67 作为备认证和计费服务器。其中, 认证端口号为 1812, 计费端口号为 1813。其它参数采用缺省值。

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
```

```
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
huawei(config)#radius-server template hwtest
huawei(config-radius-hwtest)#radius-server authentication 129.7.66.66 1812
huawei(config-radius-hwtest)#radius-server authentication 129.7.66.67 1812 secondary
huawei(config-radius-hwtest)#radius-server accounting 129.7.66.66 1813
huawei(config-radius-hwtest)#radius-server accounting 129.7.66.67 1813 secondary
huawei(config-radius-hwtest)#quit
huawei(config)#aaa
huawei(config-aaa)#domain isp
huawei(config-aaa-domain-isp)#authentication-scheme newscheme
huawei(config-aaa-domain-isp)#accounting-scheme newscheme
huawei(config-aaa-domain-isp)#radius-server hwtest
huawei(config-aaa-domain-isp)#quit
huawei(config-aaa)#quit
```

5.3.2 配置采用 RADIUS 认证和计费示例

AC 使用 RADIUS 协议与 RADIUS 服务器对接，完成认证和计费功能。

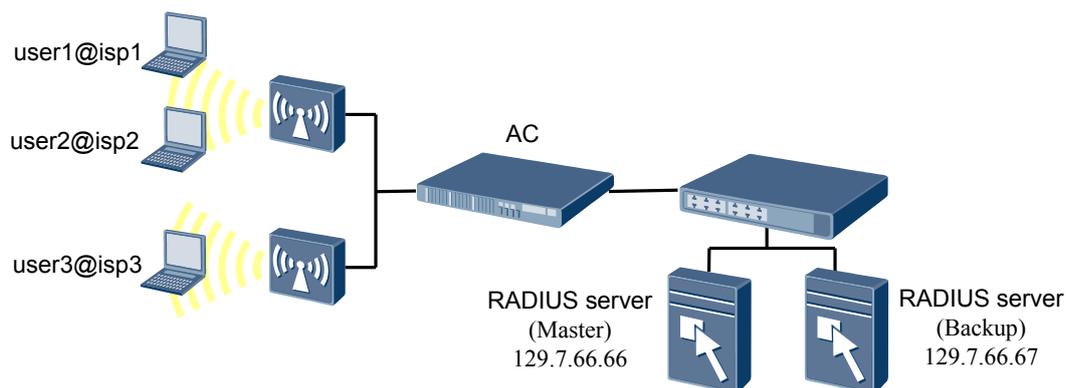
业务需求

- 使用 RADIUS 服务器对 isp1 域中用户名为 user1 的用户进行认证和计费。
- RADIUS 服务器 129.7.66.66 作为主认证和计费服务器。
- RADIUS 服务器 129.7.66.67 作为备认证和计费服务器。
- 认证端口号为 1812，计费端口号为 1813。
- 其它参数采用缺省值。

组网图

配置采用 RADIUS 认证和计费示例组网图如图 5-8 所示。

图 5-8 配置采用 RADIUS 认证和计费示例组网图



操作步骤

步骤 1 配置认证方案。

配置认证方案 newscheme，使用 RADIUS 协议对用户进行认证。

```
huawei(config)#aaa
huawei(config-aaa)#authentication-scheme newscheme
huawei(config-aaa-authen-newscheme)#authentication-mode radius
huawei(config-aaa-authen-newscheme)#quit
```

步骤 2 配置计费方案。

配置计费方案 newscheme，使用 RADIUS 协议对用户进行计费,计费间隔时间为 10min。

```
huawei(config-aaa)#accounting-scheme newscheme
huawei(config-aaa-accounting-newscheme)#accounting-mode radius
huawei(config-aaa-accounting-newscheme)#accounting interim interval 10
huawei(config-aaa-accounting-newscheme)#quit
huawei(config-aaa)#quit
```

步骤 3 配置 RADIUS 协议。

创建 RADIUS 服务器模板 radtest，设置 RADIUS 服务器 129.7.66.66 作为主认证和计费服务器，RADIUS 服务器 129.7.66.67 作为备认证和计费服务器。

```
huawei(config)#radius-server template radtest
Note: Create a new server template
huawei(config-radius-radtest)#radius-server authentication 129.7.66.66 1812
huawei(config-radius-radtest)#radius-server authentication 129.7.66.67 1812 secondary
huawei(config-radius-radtest)#radius-server accounting 129.7.66.66 1813
huawei(config-radius-radtest)#radius-server accounting 129.7.66.67 1813 secondary
huawei(config-radius-radtest)#quit
```

步骤 4 创建域。

创建域 ispl。

```
huawei(config)#aaa
huawei(config-aaa)#domain ispl
Info: Create a new domain
```

步骤 5 引用认证方案。

必须先创建认证方案，才可以在域中引用它。

```
huawei(config-aaa-domain-ispl)#authentication-scheme newscheme
```

步骤 6 引用计费方案。

必须先创建计费方案，才可以在域中引用它。

```
huawei(config-aaa-domain-ispl)#accounting-scheme newscheme
```

步骤 7 引用 RADIUS 服务器模板。

必须先创建 RADIUS 服务器模板，才可以在域中引用它。

```
huawei(config-aaa-domain-ispl)#radius-server radtest
huawei(config-aaa-domain-ispl)#quit
```

步骤 8 配置 AAA 用户。

创建 AAA 用户 user1，密码为 a123456。

```
huawei(config-aaa)#local-user shenzhen@ispl password a123456
```

----结束

操作结果

isp1 域中 user1 用户的用户名和密码必须完全正确才能通过认证，允许登录 AC 设备，并且开始对此用户计费。

配置文件

```
aaa
authentication-scheme newscheme
authentication-mode radius
quit
accounting-scheme
newscheme
accounting-mode
radius
accounting interim interval 10
quit
quit
radius-server template radtest
radius-server authentication 129.7.66.66
1812
radius-server authentication 129.7.66.67 1812 secondary
radius-server accounting 129.7.66.66 1813
radius-server accounting 129.7.66.67 1813 secondary
quit
aaa
domain ispl
authentication-scheme newscheme
radius-server
radtest
quit
quit
aaa
local-user shenzhen@ispl password a123456
```

5.4 配置 MSTP

AC 设备实现了 MSTP（Multiple Spanning Tree Protocol）协议的应用功能，同时也兼容 STP（Spanning Tree Protocol）协议和 RSTP（Rapid Spanning Tree Protocol）协议，能够支持 MSTP 环状组网，满足了组网多样性的需求。

应用环境

- MSTP 应用于冗余网络，弥补 STP 和 RSTP 的缺陷，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。
- MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，在数据转发过程中支持按 VLAN 进行负载均衡。

操作步骤

步骤 1 使能 MSTP 功能。

- 缺省情况下，设备上的 MSTP 功能处于去使能状态。
- 在 MSTP 功能使能后，设备会根据用户配置的协议模式来决定是在 STP 兼容模式下运行或者是在 MSTP 模式运行。

- MSTP 功能使能后，MSTP 根据收到的配置消息（即 BPDU 报文）动态维护相应 VLAN 的生成树状态；MSTP 功能去使能后，AC 将成为透明桥，不再维护生成树的状态。
- 1. 使用 **stp enable** 命令使能网桥的 MSTP 功能。
- 2. 使用 **stp mode mstp** 命令使能端口的 MSTP 功能。
- 3. 使用 **display stp** 命令查询网桥或端口的 MSTP 功能是否已经使能。

步骤 2 配置 MSTP 域名。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. （可选）使用 **region-name** 命令配置 MST 域的名称。
MST 域名具有缺省值，为设备的桥 MAC 地址。

步骤 3 配置 MSTP 实例。

配置 VLAN 映射表（即 VLAN 和生成树的对应关系表），把 VLAN 和生成树联系起来。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. 使用 **instance vlan** 命令映射指定 VLAN 到指定 MSTP 实例。
 - 缺省情况下，所有 VLAN 均映射到 CIST（Common And Internal Spanning Tree），即实例 0 上。
 - 一个 VLAN 不能映射到不同的实例上，即如果将一个已经设置映射的 VLAN 重新映射到一个不同的实例上时，则自动取消原来的映射关系。
 - 一个 MSTP 实例中最大允许配置 10 个 VLAN 段。



说明

VLAN 段是指从一个起始的 VLAN ID 开始到一个终止的 VLAN ID 的连续 VLAN ID 范围。

3. 使用 **check region-configuration** 命令查询 MST 域参数的当前配置信息。

步骤 4 手工激活 MST 域的配置。

1. 使用 **stp region-configuration** 命令进入 MST 域模式。
2. 使用 **active region-configuration** 命令手工激活 MST 域的配置。
3. 使用 **display stp region-configuration** 命令查询 MST 域已生效的参数配置信息。

步骤 5 配置设备在 MSTP 实例中的优先级。

1. 使用 **stp priority** 命令配置设备在指定生成树实例中的优先级。
2. 使用 **display stp** 命令查询当前设备上的 MSTP 的配置信息。

步骤 6 其它可选配置。

- 配置 MSTP 域参数。
 - 使用 **stp md5-key** 命令设定域配置 MD5 加密算法的 MD5-KEY 值。
 - 在 MST 域模式下，使用 **vlan-mapping module** 命令按模映射所有 VLAN 到指定的 MSTP 实例。
 - 在 MST 域模式下，使用 **revision-level** 命令配置设备的 MSTP 修订级别。
 - 使用 **reset stp region-configuration** 命令恢复 MST 域所有配置参数为缺省值。
- 指定设备为根桥或备份根桥。
 - 使用 **stp root** 命令指定当前设备作为指定生成树实例的根桥或备份根桥设备。
- 配置特定网桥的时间参数。

- 使用 **stp timer forward-delay** 命令配置特定网桥的 Forward Delay 时间。
- 使用 **stp timer hello** 命令设置特定网桥的 Hello Time 时间。
- 使用 **stp timer max-age** 命令设置特定网桥的 Max Age 时间。
- 使用 **stp time-factor** 命令设置特定网桥的超时时间因子。
- 配置特定端口参数。
 - 使用 **stp port transmit-limit** 命令设定当前端口在 Hello Time 时间内配置消息报文的发送数目。
 - 使用 **stp port edged-port enable** 命令将端口配置为边缘端口。
 - 使用 **stp port cost** 命令设置端口在指定生成树实例中的路径开销。
 - 使用 **stp port port-priority** 命令设置特定端口的优先级。
 - 使用 **stp port point-to-point** 命令设定与端口相连的链路是否是点到点链路。
- 配置设备保护功能。
 - 使用 **stp bpdu-protection enable** 命令使能设备的 BPDU 保护功能。
 - 使用 **stp port loop-protection enable** 命令启动端口的环路保护功能。
 - 使用 **stp port root-protection enable** 命令使能端口的 Root 保护功能。
- 配置 MST 域的最大跳数。
 - 使用 **stp max-hops** 命令配置 MST 域的最大跳数。
- 配置交换网络直径。
 - 使用 **stp bridge-diameter** 命令配置交换网络的直径。
- 配置路径开销计算标准。
 - 使用 **stp pathcost-standard** 命令配置路径开销计算标准。
- 清除 MSTP 协议统计信息。
 - 使用 **reset stp statistics** 命令清除设备的 MSTP 统计信息。

----结束

任务示例

配置 MSTP 参数，具体参数信息如下：

- 使能 MSTP 功能。
- 启动 0/2/16 端口的 MSTP 功能。
- 设置 MSTP 协议的运行模式为 MSTP 兼容模式。
- 配置 MST 域参数：
 - 配置 MD5 加密算法的 MD5-KEY 为 0x11ed224466。
 - 配置 MST 域名为 huawei-mstp-bridge。
 - 映射 VLAN2 ~ VLAN10、VLAN12 ~ VLAN16 到 MSTP 实例 3。
 - 按模 16 将所有的 VLAN 分别映射到相应的 MSTP 实例中。
 - 配置设备的 MSTP 修订级别为 100。
- 配置 MST 域的最大跳数为 10。
- 手工激活 MST 域的配置。
- 设备在指定生成树实例 2 中的优先级为 4096。

- 指定当前设备为 MSTP 实例 2 的根桥设备。
- 配置交换网络的直径为 6。
- 路径开销计算标准为 IEEE 802.1t 标准方法。
- 配置特定网桥的时间参数：
 - 特定网桥的 Forward Delay 时间为 2000 厘秒。
 - 特定网桥的 Hello Time 时间为 1000 厘秒。
 - 特定网桥的 Max Age 时间为 3000 厘秒。
 - 特定网桥的超时时间因子为 6。
- 配置特定端口参数：
 - 端口在每个 Hello Time 时间内最大发送数目为 16。
 - 端口 0/2/16 为边缘端口。
 - 端口在指定生成树实例中的路径开销为 1024。
 - 端口的优先级为 64。
 - 与 0/2/16 端口相连的链路为点对点链路。
- 使能设备的 BPDU 保护功能。

```
huawei(config)#stp enable
Change global stp state may active region configuration,it may take several
minutes,are you sure to change global stp state? [Y/N][N]y
huawei(config)#stp port 0/2/16 enable
huawei(config)#stp mode mstp
huawei(config)#stp md5-key 11ed224466
huawei(config)#stp region-configuration
huawei(stp-region-configuration)#region-name huawei-mstp-bridge
huawei(stp-region-configuration)#instance 3 vlan 2 to 10 12 to 16
huawei(stp-region-configuration)#vlan-mapping module 16
huawei(stp-region-configuration)#revision-level 100
huawei(stp-region-configuration)#active region-configuration
huawei(stp-region-configuration)#quit
huawei(config)#stp instance 2 priority 4096
huawei(config)#stp instance 2 root primary
huawei(config)#stp max-hops 10
huawei(config)#stp bridge-diameter 6
huawei(config)#stp pathcost-standard dot1t
huawei(config)#stp timer forward-delay 2000
huawei(config)#stp timer hello 1000
huawei(config)#stp timer max-age 3000
huawei(config)#stp time-factor 6
huawei(config)#stp port 0/2/16 transmit-limit 16
huawei(config)#stp port 0/2/16 edged-port enable
huawei(config)#stp port 0/2/16 instance 0 cost 1024
huawei(config)#stp port 0/2/16 instance 0 port-priority 64
huawei(config)#stp port 0/2/16 point-to-point force-true
huawei(config)#stp bpdu-protection enable
```

5.5 配置 Ethernet CFM OAM

介绍 Ethernet CFM OAM 在 AC 上的配置。

前提条件

Router 设备支持 Ethernet CFM OAM 功能。

业务需求

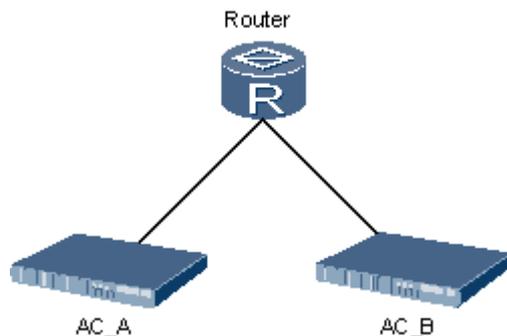
远端的两台设备周期性的发送检测报文，检测其连通性。

组网图

Ethernet CFM OAM 配置组网如[图 5-9](#)所示。

Ethernet 网络中，AC_A 和 AC_B 之间的链路采用 Ethernet CFM OAM 机制，以检测链路故障。在 AC_A 和 AC_B 上分别配置本端 MEP 和远端 MEP，AC_B 设备的本端 MEPID 与 AC_A 配置的远端 MEPID 一致，远端 MEPID 与 AC_A 的本端 MEPID 一致。

图 5-9 Ethernet CFM OAM 组网图



数据规划

Ethernet CFM OAM 配置数据规划，如[表 5-5](#)所示。

表 5-5 Ethernet CFM OAM 配置数据规划表

配置项	数据
AC_A	端口: 0/2/24 Smart VLAN: 100 MEP: 2/6/5 CC-interval: 10 minutes
AC_B	端口: 0/2/24 Smart VLAN: 200 MEP: 2/6/5 CC-interval: 10 minutes

操作步骤

步骤 1 创建 VLAN。

业务 VLAN ID 为 100，VLAN 类型为 Smart。

```
huawei(config)#vlan 100
```

步骤 2 加入上行端口。

将端口 0/2/24 加入到 VLAN 100 中。

```
huawei(config)#port vlan 100 0/2 24
```

步骤 3 (可选配置) 设置端口 Native VLAN。

配置上行以太网端口的报文是否携带 VLAN tag。上行端口是否设置 Native VLAN 取决于与之直接相连的上层设备是否支持携带 VLAN tag 的报文。AC 的设置与上层设备保持一致即可。报文为 Untagged 类型。

```
huawei(config)#interface scu 0/2
huawei(config-if-scu-0/2)#native-vlan 24 vlan 100
huawei(config-if-scu-0/2)#quit
```

步骤 4 配置 MD 维护域。

- 不能创建索引、级别相同的 MD。
- 不能创建名字类型和名字都相同的 MD。
- MD 与其对应 MA 的名字长度之和必须小于等于 44 个字符。

```
huawei(config)#cfm md 2 name-format string huawei level 3
```

步骤 5 配置 MA 维护集。

- 1 个 MD 下面最多能配置 4096 个 MA。系统最多可配置 4096 个 MA，即如果在一个 MD 下面配置了 4096 个 MA，则在其它的 MD 下面将不能再配置 MA。不能创建不存在 MD 下面的 MA。不能创建系统中已经存在的 MA。
- MA 与其对应 MD 的名字长度之和必须小于等于 44 个字符。
- 配置 MA 管理对象的 CC 报文发送周期为 10 分钟。系统缺省值为 1 分钟。

```
huawei(config)#cfm ma 2/6 name-format string cfmhuawei cc-interval 10m
```

步骤 6 配置 MEP 维护节点。

- MEP 是维护通信信道的端点，Ethernet CFM OAM 依靠信道两端的 MEP 来检测该信道的连通性。
- 缺省情况下：MEP 的管理功能为使能状态；发送 CFM 报文的优先级为 7；CC 报文发送功能为使能状态。

```
huawei(config)#cfm ma 2/6 vlan 100 mhf-creation default-mhf
huawei(config)#cfm ma 2/6 meplist 5
huawei(config)#cfm mep 2/6/5 direction down port 0/2/24 priority 7
```

步骤 7 配置使能远端 MEP 维护功能。

缺省情况下，远端 MEP 检测功能处于去使能状态。

```
huawei(config)#cfm remote-mep-detect enable
```

步骤 8 使能全局本端 CFM 全局功能。系统缺省值为 disable，即去使能全局本端 CFM 功能。

```
huawei(config)#cfm enable
```

步骤 9 使能全局远端 MEP 检测功能。系统缺省值为 disable，即去使能全局远端 MEP 检测功能。

```
huawei(config)#cfm remote-mep-detect enable
```

步骤 10 保存数据。

```
huawei(config)#save
```



说明

AC_A 的远端 MEP 需要在 AC_B 上配置，配置方法与 AC_A 的配置基本相同，此处不再赘述。

----结束

操作结果

配置完成后，在 AC_A 或 AC_B 上执行 **display cfm statistics mep** 命令可以查询报文统计信息，其中“CCM Sent Pkt Num”和“CCM Received Pkt Num”均不为零。

配置文件

```
vlan 100 smart
port vlan 100 0/2 24
interface scu 0/2
native-vlan 24 100
quit
cfm md 2 name-format string huawei level 3
cfm ma 2/6 name-format string cfmuawei cc-interval 10m
cfm mep 2/6/5 direction down port 0/2/24 priority 7
cfm remote-mep-detect enablecfm enable
cfm remote-mep-detect enable
save
```

6 配置组播业务

关于本章

介绍 AC 在单网元组网、级联组网、MSTP 组网方式下的组播业务配置过程。

AC 组播特性主要应用于直播电视（Live TV）和准视频点播（NVOD，Near-Video On Demand）组播视频业务。

在组播处理模式上，AC 支持“IGMP Proxy”和“IGMP Snooping”二层组播协议。两者都实现组播视频数据转发功能，但处理机理不同：

- **IGMP Snooping** 通过侦听用户与组播路由器之间通信的 IGMP 报文获取相关信息维护组播转发表项。
- **IGMP Proxy** 是靠拦截用户和组播路由器之间的 IGMP 报文并进行相关处理后，再将它转发给上层组播路由器。从组播用户的角度看，AC 是一台组播路由器，完成 IGMP 协议中路由器部分的功能；从组播路由器来看，AC 设备是一个组播用户。

在组播节目配置上，AC 支持节目库静态配置和动态生成两种方式。

- **静态节目库方式**：在用户观看视频节目前，先配置好节目列表。该方式可以通过权限模板实现组播受控，但根据视频业务的变更，需要经常维护节目列表和权限模板。支持节目主机功能、节目预加入功能以及组播带宽管理功能。
- **动态生成节目方式**：根据用户点播动态生成节目。这种方式无需配置和维护节目列表，但不支持节目管理、用户组播带宽管理、节目预览和预加入功能。

当 Triple Play 业务高优先级流量突然增加不会导致 IGMP 报文丢包，AC 设备会优先处理和发送 IGMP 报文。

6.1 组播缺省配置信息

提供了组播协议、版本、节目配置方式、带宽管理功能、预览功能和日志功能的系统缺省配置信息。

6.1 组播缺省配置信息

提供了组播协议、版本、节目配置方式、带宽管理功能、预览功能和日志功能的系统缺省配置信息。

AC 组播业务系统缺省配置如表 6-1 所示。

表 6-1 组播业务缺省配置信息

特性	缺省配置
组播协议	关闭
IGMP Version	V3
组播节目配置方式	静态配置方式
组播带宽管理	Enable
组播预览	Enable
组播日志开关	Enable

6.1.1 配置组播全局参数

基于设备全局配置二层组播协议（IGMP Proxy、IGMP Snooping）的通用参数，对所有组播 VLAN 有效。

背景信息

组播全局参数包括通用组查询、特定组查询、组播报文处理策略。

通用组查询说明：

- 目的：通用组查询是 AC 通过定期发送通用组查询报文，以确认是否有组播用户在没有发送 leave 报文情况下就离开了组播组。AC 根据查询结果定期更新组播转发表，及时释放已离开的组播用户带宽。
- 原理：AC 会定期向所有在线的 IGMP 用户发送通用组查询报文。若 AC 在一定的时间内（健壮系数*通用查询间隔+通用查询最大响应时间）没有收到某一 IGMP 用户的响应报文，则认为该用户已离开该组播组，并将其从组播组中删除。

特定组查询说明：

- 目的：特定组查询是在不具有快速离开属性的组播用户发送 leave 报文后，AC 发送特定组查询报文以确认该用户是否真的已离开组播组。
- 原理：当 IGMP 用户主动离开某组播组时，如切换频道，会主动向 AC 发送离开报文。若该用户不具有快速离开属性，AC 将向该组播组发送特定组查询报文。若在一定的时间内（健壮系数*特定查询间隔+特定查询最大响应时间）没有收到该用户的响应报文，才将该用户从组播组中删除。

组播全局参数的系统缺省值如表 6-2 所示。配置时，根据实际数据规划进行调整。

表 6-2 组播全局参数系统缺省配置

参数项	缺省值
通用组查询参数	通用组查询时间间隔：125s 通用组查询最大响应时间：10s 通用组查询健壮性系数（查询次数）：2
特定组查询参数	特定组查询时间间隔：1s 特定组查询最大响应时间：0.8s 特定组查询健壮性系数（查询次数）：2

操作步骤

步骤 1 在全局配置模式使用 **btv** 命令进入 BTV 模式。

步骤 2 配置通用组查询参数。

1. 使用 **igmp proxy router gen-query-interval** 命令设置通用组查询时间间隔。系统缺省值为 125s。
2. 使用 **igmp proxy router gen-response-time** 命令设置通用组查询最大响应时间。系统缺省值为 10s。
3. 使用 **igmp proxy router robustness** 命令设置通用组查询次数。系统缺省值为 2。

步骤 3 配置特定组查询参数。

1. 使用 **igmp proxy router sp-query-interval** 命令设置特定组查询时间间隔。系统缺省值 1s。
2. 使用 **igmp proxy router sp-response-time** 命令设置特定组查询最大响应时间。系统缺省值 0.8s。
3. **igmp proxy router sp-query-number** 使用命令设置特定组查询次数。系统缺省值为 2。

步骤 4 使用 **display igmp config global** 命令查询配置的参数是否正确。

----结束

任务示例

举例：配置组播通用查询参数：查询时间间隔为 150s，查询最大响应时间为 20s，查询次数为 3 次。

```
huawei(config)#btv
huawei(config-btv)#igmp proxy router gen-query-interval 150
huawei(config-btv)#igmp proxy router gen-response-time v3 20
huawei(config-btv)#igmp proxy router robustness 3
```

举例：配置组播特定组查询参数：查询时间间隔为 200s，查询最大响应时间为 100s，查询次数为 3 次。

```
huawei(config)#btv
huawei(config-btv)#igmp proxy router sp-query-interval 200
huawei(config-btv)#igmp proxy router sp-response-time v3 100
huawei(config-btv)#igmp proxy router sp-query-number 3
```

6.1.2 配置组播 VLAN 和组播节目

组播业务应用中使用 MVLAN (multicast-vlan) 来区分不同的组播内容提供商。一般为每个组播内容提供商分配一个 MVLAN，基于 VLAN 实现组播节目、组播协议、组播版本管理，以及实现组播域控制和用户权限控制。

背景信息

创建组播 VLAN，必须先创建普通 VLAN。组播 VLAN 可以与单播 VLAN 相同，组播和单播共用一个业务流通道；组播 VLAN 可以与单播 VLAN 不同，组播与单播业务流使用不同的业务流通道。

一个用户端口可以同时加入到多个组播 VLAN 中，具有如下约束：

- 同一个用户端口的所有组播 VLAN 中，最多只允许有一个组播 VLAN 的节目是动态生成的。
- 同一个用户端口的所有组播 VLAN 支持的 IGMP 版本应该是一致的。
- 同一个用户端口不允许属于多个 IGMP V3 Snooping 模式的组播 VLAN。

AC 设备在处理组播业务时，发出组播报文的源 IP 地址，有多种情况：

- 如果节目 VLAN 配置了三层接口的 IP 地址，则源地址为此 IP 地址，并且要保证此 IP 地址与 BRAS 和上层路由器在同一网段。
- 如果没有配置三层接口的 IP 地址，则源地址为组播节目源的“Hostip”。
- 如果“Hostip”也没有配置，则取默认地址：0.0.0.0。

基于组播 VLAN 配置二层组播协议、组播版本、组播节目、组播上行口，各属性系统缺省值如表 6-3 所示。

表 6-3 组播 VLAN 各属性系统缺省配置

参数项	缺省值
节目匹配方式	动态配置节目方式
组播上行口模式	default
二层组播协议	off (没有启动组播功能)
IGMP Version	V3
上行口转发 IGMP 报文优先级	6

操作步骤

步骤 1 创建组播 VLAN。

1. 使用 **vlan** 命令创建 VLAN。
2. 使用 **multicast-vlan** 命令将已创建的 VLAN 配置为组播 VLAN。

步骤 2 配置组播节目。

组播 VLAN 的节目采用动态生成方式，这种方式不需要节目列表，根据用户点播动态生成节目。但不支持节目和用户组播带宽管理、节目预览和预加入功能。

1. 使用 **igmp match group** 命令配置可动态生成节目组的节目地址范围。用户只允许点播在该组播节目地址范围内的节目。

步骤 3 配置组播上行口。

1. 使用 **igmp uplink-port** 命令指定组播上行口。对应组播 VLAN 的组播报文都从该上行口转发和接收。
2. 在 BTV 模式下使用 **igmp uplink-port-mode** 命令更改组播上行口模式。系统缺省为 default 模式，当采用 MSTP 组网时选用 mstp 模式。
 - default 模式：如果组播 VLAN 只包含一个上行口，上行的 IGMP 报文只从该端口发送；如果组播 VLAN 包含多个上行口，IGMP 报文向所有的上行口发送。
 - mstp 模式：用于 MSTP 组网。

步骤 4 选择组播协议。

使用 **igmp mode { proxy | snooping }** 命令选择二层组播协议。系统缺省关闭组播功能。

当采用 IGMP Snooping 时，可以开启 report 报文、leave 报文代理功能，当组播用户加入或离开组播节目时，AC 可实现组播代理功能。两个功能分开独立控制。

- 使用 **igmp report-proxy enable** 命令开启 snooping report 报文代理功能。当某节目的第一个用户加入时，经过鉴权后，AC 把用户报文发送到网络侧，从组播路由器引入相应的组播流；该节目的后续加入请求，AC 不再转发到网络侧。
- 使用 **igmp leave-proxy enable** 命令开启 snooping leave 报文代理功能。当节目的最后一个用户离线时，AC 把用户报文发送到网络侧，告知上层设备停止发送组播流；前面用户的离线请求，AC 不转发到网络侧。

步骤 5 配置 IGMP Version。

使用 **igmp version{ v2 | v3 }** 命令配置 IGMP Version。系统缺省是开启 IGMP V3，如果网络中上下层是 IGMP V2 设备，无法识别 IGMP V3 报文时，使用该命令进行切换。

IGMP V3 版本兼容 IGMP V2 版本报文处理。AC 开启 IGMP V3 时，如果上层组播路由器切换为 V2，AC 收到 V2 报文时，会自动切换为 IGMP V2。在设置的 V2 版本生存时间内没有再收到 V2 报文，系统又会恢复到 V3 版本。在 BTV 模式下使用 **igmp proxy router timeout** 命令设置 IGMP V2 版本生存时间。系统缺省值为 400s。

步骤 6 更改 IGMP 报文转发优先级。

使用 **igmp priority** 命令更改上行口转发 IGMP 报文优先级。系统缺省优先级为 6，一般不需要更改。

- IGMP proxy 模式下，向网络侧发送的 IGMP 报文的优先级采用组播 VLAN 下的本命令所设置的优先级。
- IGMP Sooping 模式下，向网络侧转发的 IGMP 报文采用用户所在的业务流的优先级。业务流优先级通过流量模板设置。

步骤 7 查询配置信息是否正确。

- 使用 **display igmp config vlan** 命令查询组播 VLAN 各属性配置信息。
- 使用 **display igmp program vlan** 命令查询组播 VLAN 节目信息。

----结束

任务示例

举例：创建 VLAN101，动态配置节目方式，组播 VLAN 上行端口 0/2/24，采用 IGMP Proxy 协议、IGMP V3 版本。

```
huawei(config)#vlan 101
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp uplink-port 0/2/24
huawei(config-mvlan101)#igmp mode proxy
  Are you sure to change IGMP mode?(y/n) [n]:y
huawei(config-mvlan101)#igmp version v3
```

7 运维管理

关于本章

介绍通过设置告警和保存数据对设备进行基本维护管理。

7.1 配置告警

告警管理主要完成告警记录、告警设置、告警统计等功能，通过告警管理可对设备进行维护，保证其正常高效运行。

7.2 更换 AP

当需要更换 AP 时，为避免重新配置数据，可以直接将需要更换的 AP 的 MAC 地址或 SN 修改为新 AP 的 MAC 地址或 SN，修改后新 AP 以原 AP 的 AP-ID 上线，原 AP 所配置的所有数据在新 AP 上生效，不用重新配置。

7.1 配置告警

告警管理主要完成告警记录、告警设置、告警统计等功能，通过告警管理可对设备进行维护，保证其正常高效运行。

背景信息

告警是系统检测到故障而产生的通知，告警产生之后，系统根据目前配置的终端的情况向各个终端进行广播，主要包括网管工作站（NMS，Network Management System）用户和命令行界面（CLI，Command Line Interface）用户。

告警包括故障告警和恢复告警。故障告警在某个时刻产生之后一直存在，直到该故障被修复，使得告警被清除为止。

用户可根据对告警的关注程度和实际需要，对告警进行自定义设置，包括自定义告警级别、告警在命令行的输出方式和告警信息的统计。

操作步骤

- 使用 **alarm active clear** 命令清除当前系统中的未恢复的告警。
 - 当活动告警长时间没有恢复时，您可以使用此命令清除该告警。
 - 清除告警前可以使用 **display alarm active** 命令查询当前有哪些活动告警。
- 使用 **alarm alarmlevel** 命令设置告警级别。
 - 告警级别分成四类：critical（严重）、major（重要）、minor（次要）、warning（警告）。
 - 参数“default”表示还原告警为缺省级别。
 - 告警级别可以通过 **display alarm list** 命令来查询。
 - 系统给每条告警都指定了缺省的也是推荐的告警级别，如无特殊需求一般采用该缺省值即可。
- 使用 **alarm jitter-proof** 命令设置告警防抖动功能的开关和防抖动周期。
 - 为了防止系统中的故障告警和其恢复告警频繁的出现，您可以通过使能告警防抖动功能来对系统的告警进行过滤。
 - 使能防抖动功能后，系统中的告警不会立即上报给网管，而是等待一个告警防抖动周期后才上报。
 - 如果在一个告警防抖动的周期中，该告警的状态恢复，则该告警将不会上报给网管。
 - 可以使用 **display alarm jitter-proof** 命令查询当前系统是否已经开启了告警防抖动功能和告警防抖动周期。
 - 系统默认关闭告警防抖动功能，可以根据设备运行情况来判断是否需要使能该功能。
- 使用 **alarm output/undo alarm output** 命令设置/屏蔽告警输出到命令行终端。
 - 设置告警是否输出对告警的产生没有影响，系统产生的告警仍然会被记录。用户可以使用 **display alarm history** 命令查询被屏蔽输出的告警。
 - 当某条告警的输出方式设置冲突时，以最后一次设置为准。
 - 恢复告警的输出方式与故障告警的输出方式一致。当设置了故障告警输出方式时，系统自动同步其恢复告警的输出方式。反之亦然。

- 使用 **alarm-event statistics period** 命令设置告警的统计周期。
 - 系统将根据设置的周期对告警和事件的出现次数进行统计，当需要保留统计结果时，使用 **alarm-event statistics save** 命令将统计结果保存在 Flash memory 中。
 - 使用对告警和事件的统计结果可以帮助定位系统当前存在的问题原因。
 - 可以使用 **display alarm statistics** 命令查询告警统计记录。
- 使用 **display alarm configuration** 命令按照告警标识查询告警配置信息。能查询到的告警配置信息包括告警标识、告警名称、告警类别、告警分类、告警级别、默认告警级别、参数个数、命令行输出标志、转换标志和告警详细解释。
- 使用 **display alarm statistics** 命令查询告警统计记录。
 - 当需要了解某个告警在某个时间段产生的频度，进而了解设备的工作状况，分析可能存在的故障时，使用此命令。
 - 目前系统支持查询当前分钟、当前 24 小时、前 15 分钟、前 24 小时的告警统计信息。

---结束

任务示例

举例：屏蔽所有级别为“警告”的告警输出到命令行终端，同时打开告警防抖动功能的开关，并设置告警防抖动周期为 15 秒；设置 ID 为 0x0a310021 的告警的级别修改为“严重”，并配置将当前系统中级别为“严重”的告警统计保存在 Flash memory 中，以便后续通过查看告警统计信息定位系统存在的问题。

```
huawei(config)#undo alarm output alarmlevel warning
huawei(config)#alarm jitter-proof on
huawei(config)#alarm jitter-proof 15
huawei(config)#alarm alarmlevel 0x0a310021 critical
huawei(config)#alarm-event statistics save
```

7.2 更换 AP

当需要更换 AP 时，为避免重新配置数据，可以直接将需要更换的 AP 的 MAC 地址或 SN 修改为新 AP 的 MAC 地址或 SN，修改后新 AP 以原 AP 的 AP-ID 上线，原 AP 所配置的所有数据在新 AP 上生效，不用重新配置。

背景信息

由于 AP 的配置和 MAC 地址或 SN 绑定，如果现网运行中的 AP 发生故障需要更换，就需要重新配置数据，不利于业务的快速恢复。为此 AC 设备开发了 AP 更换功能，更换后的新 AP 无需配置即可替代原 AP 开展业务。

- 新 AP 必须与需要更换的 AP 的类型一致。
- 新 AP 的 MAC 地址和 SN 不能和现网中存在的 MAC 地址和 SN 冲突。

操作步骤

- 步骤 1** 直接使用同类型的新 AP 更换故障 AP，使用 **ap modify** 命令将故障 AP 的 MAC 地址和 SN 更换成新 AP 的 MAC 地址和 SN。

---结束

操作结果

新 AP 正常开展被替换故障 AP 的各项业务。

任务示例

举例：将 AP ID 为 0 的 AP 更换成 MAC 地址为 0002-3333-3333，SN 为 SN000008 的新 AP。

```
huawei(config-wlan-ac-view)#ap modify 0 mac 0002-3333-3333 sn SN000008
```