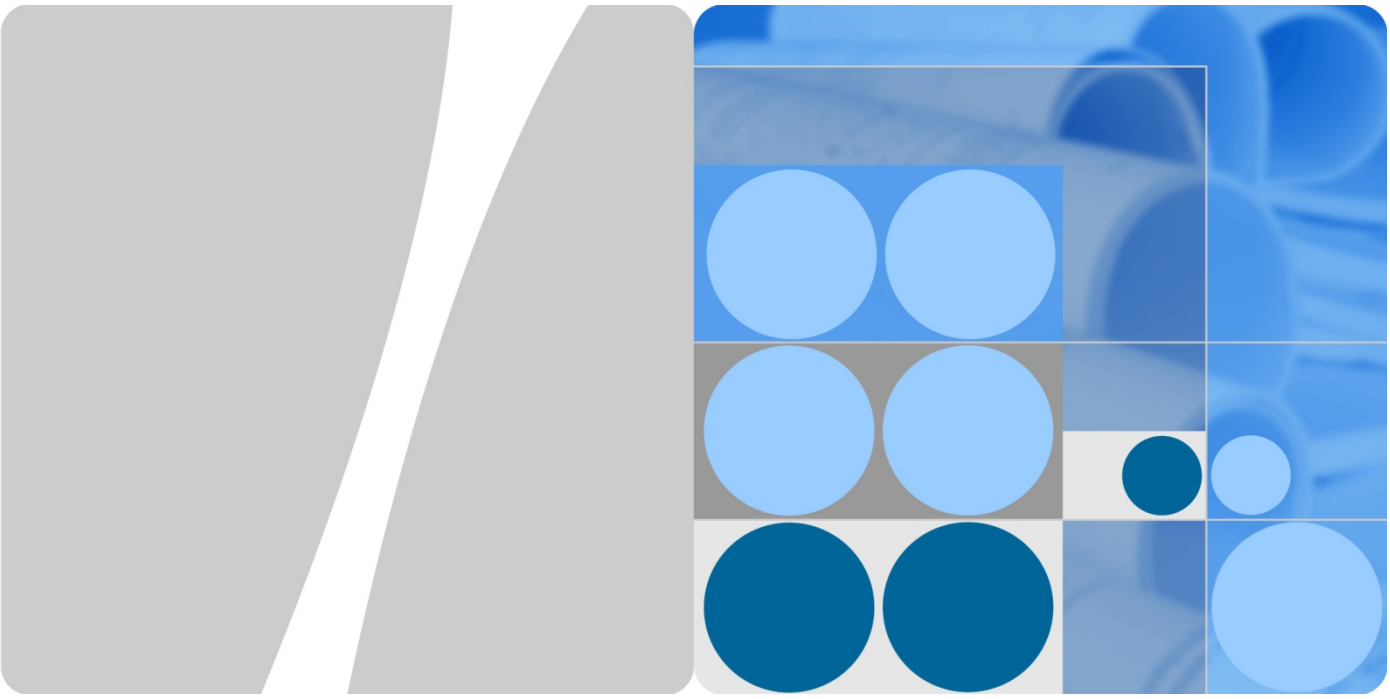


企业 WLAN 解决方案
V100R001C00
部署指南

文档版本 02

发布日期 2012-01-05

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

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，本文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，华为公司对本文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，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、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

目 录

1 企业 WLAN 方案概述

1.1 WLAN 简介

1.1.1 WLAN 基本概念

WLAN（Wireless Local Area Network）广义上是指是指以无线电波、激光、红外线等无线信道来代替有线局域网中的部分或全部传输媒介所构成的无线局域网。而狭义的WLAN 是指利用高频射频信号（例如 2.5GHz 或 5GHz）作为传输信道的无线局域网。

广义的 WLAN 实际上包含了多种技术标准，例如蓝牙、802.11 系列、HiperLAN2 等。随着技术的发展和演进，802.11 系列由于技术相对简单，通信可靠，具有灵活、移动、高吞吐量和快速安装等特点，成为 WLAN 的主流标准。在下文中的 WLAN 均指基于802.11 系列标准的技术。

802.11 是 IEEE 在 1997 年为 WLAN 定义的一个无线网络通信的工业标准。此后这一标准又不断得到补充和完善，形成 802.11 的标准系列。例如比较重要的 802.11、802.11a、802.11b、802.11e、802.11g、802.11i、802.11n 等。其中基于 802.11b 标准的有时也被成为 Wi-Fi 标准。

1.1.2 WLAN 的优劣势

WLAN 的优势

WLAN 的优势是显而易见的：

- 网络使用自由。凡是自由空间均可连接网络，不受限于线缆和端口位置。在办公大楼、机场候机厅、度假村、商务酒店等场所尤为适用。
- 网络建设更经济、通信更便利。终端与交换设备之间省去布线，有效降低布线成本。也适用于特殊地理环境下的网络建设，如隧道、港口码头、高速公路等。
- 工作更高效。不受限于时间和地点的接入网络，满足各行各业对于网络应用的需求。例如体育场馆、商业展馆、制造车间、物流运输等。

WLAN 的劣势

WLAN 带来快速便捷的网络接入方式，但也存在一定的劣势：

- 性能：无线局域网是依靠无线电波进行传输的。电波通过无线发射装置发射，而建筑物、车辆、树木和其它障碍物都可能阻碍电磁波的传输，所以会影响网络性能。
- 速率：无线信道的传输速率与有线信道（例如光纤）相比要低得多。目前 WLAN 一般传输速率都在百兆级别，最高也只有 600Mbit/s（802.11n）。
- 安全性：本质上无线电波不要求建立物理的连接通道，无线信号是发散的。从理论上讲，很容易监听到无线电波广播范围内的任何信号，造成通信信息泄漏。

1.1.3 WLAN 的基本架构

基于 802.11 系列标准的 WLAN 网络主要由 STA、AP、AC 等部件组成。

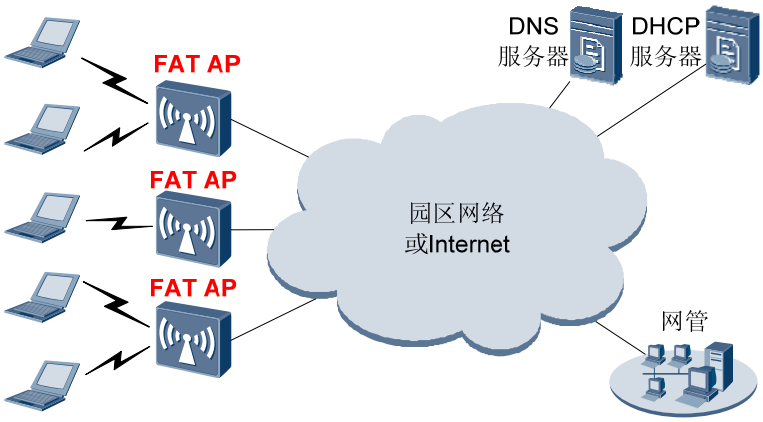
- STA（Station）：指各种接入终端，例如电脑、手机、PDA 等。
- AP（Access Point）：AP 是 WLAN 网络的主要设备，是实现无线技术的关键部件。AP 对上提供有线连接，对下提供无线接入，起到有线和无线网络的桥接作用。
- AC（Access Controller）：AC 主要完成对 AP 设备的管理。包括 AP 点管理、射频管理、用户认证、完全管理等。AC 通过 CAPWAP（Controlling and Provisioning of Wireless Access Point）协议完成管理功能。

WLAN 网络主要有自治式和集中式两种网络架构。

自治式架构

自治式架构又称为 FAT AP 架构。在该架构下，AP 实现所有无线接入功能（称为“胖 AP”），不需要 AC 设备形态。如图 1-1 所示。

图1-1 自治式架构

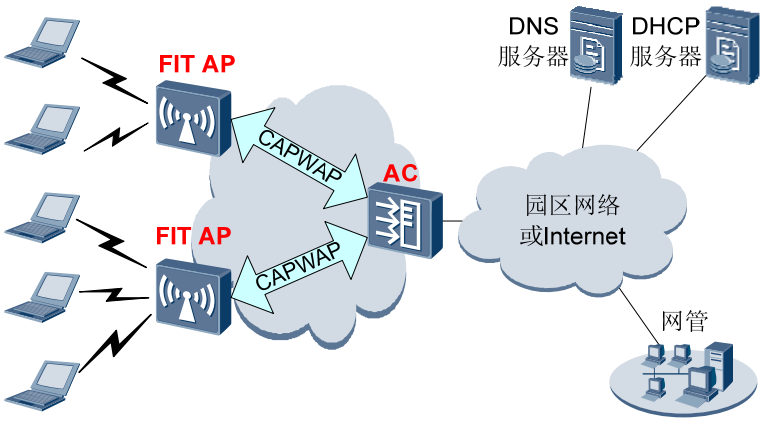


WLAN 早期广泛采用自治式架构，随着企业大量部署 AP 时，对 AP 进行配置、升级软件等管理工作将给用户带来很高的操作成本，管理成本提高，自治式架构应用逐步减少。

集中式架构

集中式架构又称为 FIT AP 架构。在该架构下，通过 AC 集中管理和控制多个 AP（称为瘦 AP），如图 1-2 所示。

图1-2 集中式架构



在集中式架构下，所有无线接入功能由 AP 和 AC 间共同完成：

- AC 完成网络具有重要意义的功能，例如移动管理、身份验证、VLAN 划分、射频资源管理、无线 IDS 和数据包转发等。
- AP 完成无线空口的控制，例如无线信号发射与探测响应、数据加密解密、数据传输确认、空口数据优先级管理等等。
- AP 和 AC 间采用 CAPWAP 协议进行通讯，AC 与 AP 间可以是直连或者穿越二层或三层网络。

集中式架构是企业网、运营商等 WLAN 方案的主要架构，便于集中管理、集中认证和集中安全管理。下文中的 WLAN 部署方案均基于集中式架构。

1.2 企业 WLAN 组网方案

对于企业的 WLAN 网络部署来说，可以按照企业和机构的规模大小、机构类型等因素来考虑采用不同的 WLAN 组网方案。

1.2.1 大中型园区网 WLAN 方案

大中型园区网定位为大中型企业总部、大型分支机构、高校、机场等场所。大型园区 WLAN 部署的 AP 数量较多，有内部需求可能也有访客上网需求。

从网络运维以及安全考虑，大中型园区网主要采用集中式架构（FIT AP 架构）来部署 WLAN。根据 AC 的部署方式，又可分为集中式 AC 方案和分布式 AC 方案。

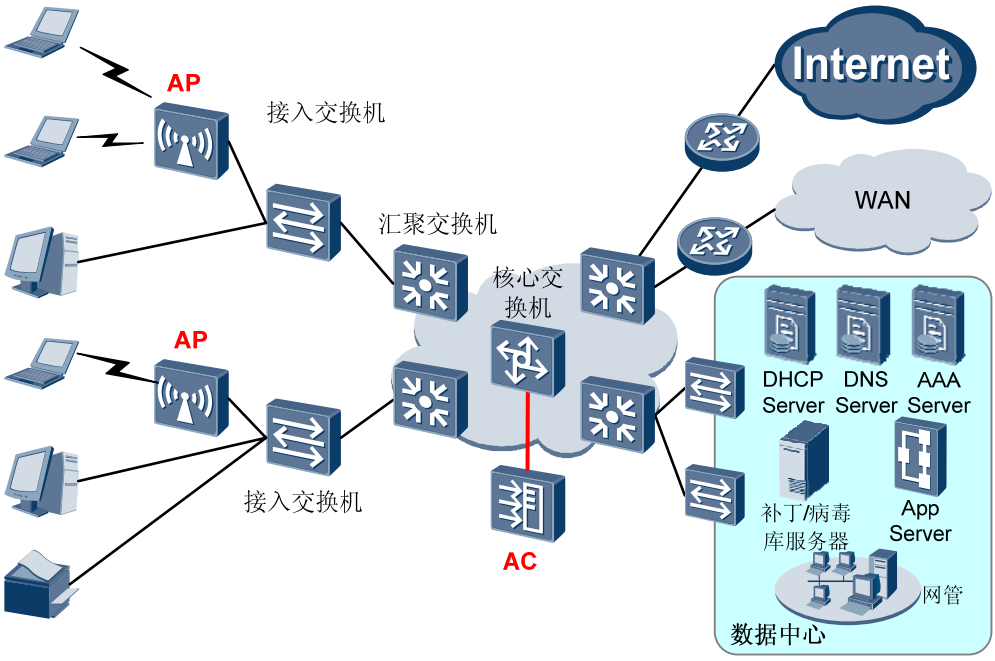
集中式 AC 方案

集中式 AC 方案，是指整个网络中集中部署 AC 设备（一般是独立的 AC 设备），来控制和管理整网的 AP 设备。AC 的部署可以采用直路（直接部署在 AP 和汇聚/核心交换机之间）或旁挂方式（旁挂在汇聚/核心交换机旁侧）。

- 直路方式主要用于新建网络或原有网络汇聚/核心设备为华为设备的场景。
- 旁挂方式主要用于原有网络汇聚/核心设备非华为设备的场景。

大中型园区网的集成 AC 组网方案如图 1-3 所示。（以旁挂方式为例）

图1-3 大中型园区网集中式 AC 方案

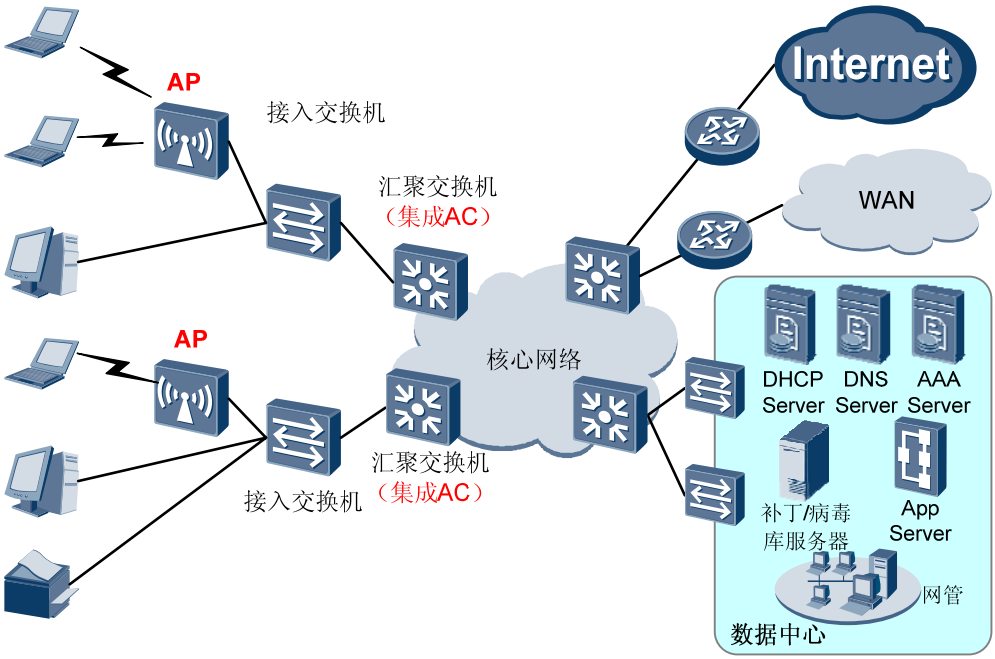


分布式 AC 方案

分布式 AC 方案，是指网络中分区域采用多个 AC 设备，分别对本区域的 AP 设备进行管理。分布式 AC 方案一般不采用独立的 AC 设备，而是采用在汇聚交换机上集成 AC 功能，来实现对本交换机下挂的所有 AP 进行管理。

大中型园区网的集成 AC 组网方案如图 1-4 所示。

图1-4 大中型园区网集成 AC 方案



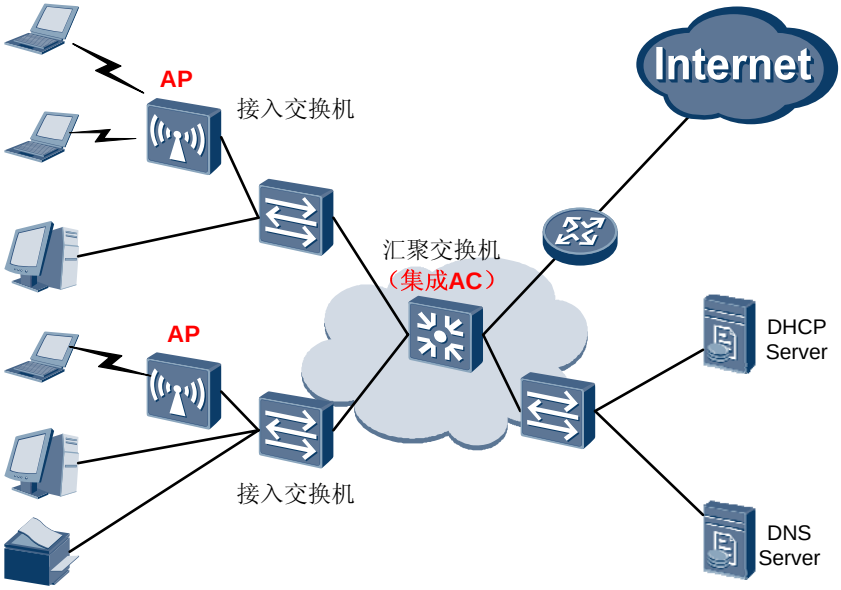
1.2.2 小型园区网 WLAN 方案

小型园区网定位为中小型企业包括独立的小型园区网，也包括只在分支机构部署 WLAN 的场景。小型园区网 WLAN 部署规模小于大型园区但高于 SOHO。

相对于大型 WLAN 网络而言，小型园区网 WLAN 可能较少考虑网络可靠性，可能因为成本因素而不需要专门的网管设备以及认证服务器。

小型园区网由于规模较小，一般采用集中式 AC 方案。可采用独立 AC 设备或者交换机集成 AC 的部署方式。如图 1-5 所示。（以交换机集成 AC 为例）

图1-5 小型园区网 WLAN 方案

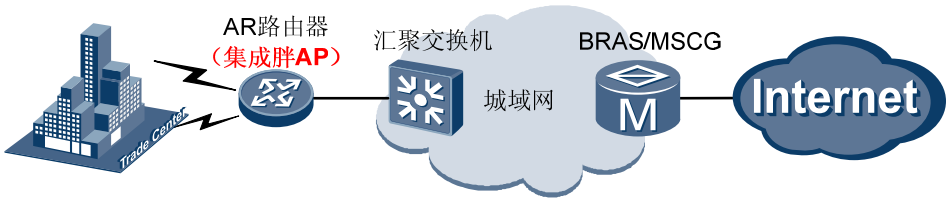


1.2.3 SOHO WLAN 方案

SOHO WLAN 方案主要适用于用户规模较小的独立的小型场点，如小型企业、商店、咖啡吧、SOHO 办公等，或者独立部署 WLAN 业务的企业分支机构。SOHO WLAN 网络中一般不会单独部署认证服务器以及网管设备。

SOHO 的 WLAN 方案一般可采用自治式架构（胖 AP 架构），不需要 AC 设备。此时可采用华为公司的 AR 路由器作为胖 AP（也可采用第三方的胖 AP 产品）来进行组网。如图 1-6 所示。

图1-6 SOHO WLAN 方案



注意

使用 AR 路由器作为胖 AP 实现 SOHO WLAN 的部署指导，请直接参考 AR 路由器产品的产品文档。

1.2.4 分支 WLAN 方案

分支 WLAN 方案定位为总部与分支均部署了 WLAN 且总部需要管理分支 WLAN 的场景（完全不需要总部管理的场景，可根据分支的大小归入前面三种场景）。

企业分支根据可能 AC 部署方式分为大小型，与分支的规模大小没有严格的对应关系。企业分支的 WLAN 方案如图 1-7 和图 1-8 所示。

图1-7 大型分支 WLAN 方案

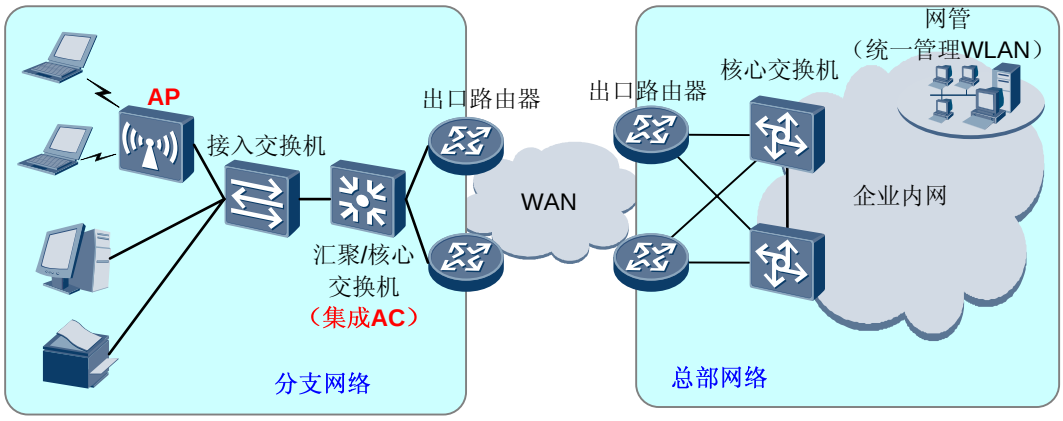
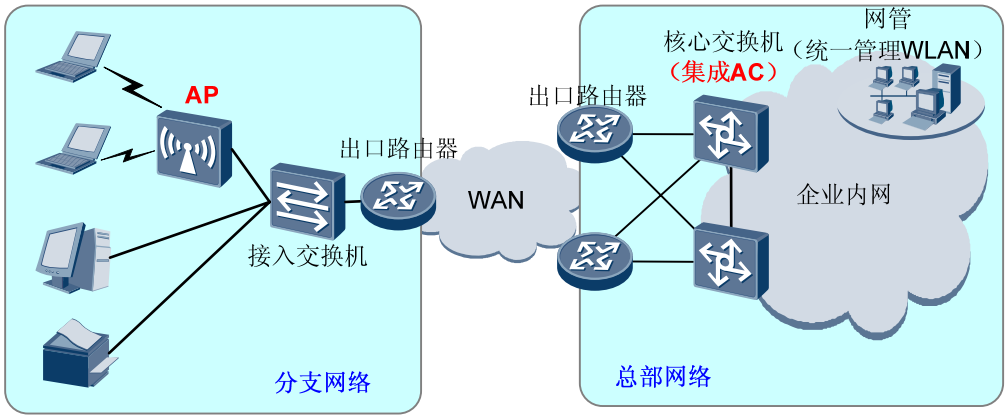


图1-8 小型分支 WLAN 方案



注意

在后续的部署指导中，以完整的大中型园区网 WLAN 方案为基础，按照 AC 的设备形态（独立 AC 和集成 AC）为维度进行描述。部署的相关指导对于各种不同类型的企业网络均可参考使用。例如对于小型园区网来说，可能不需要 TSM 服务器和网管服务器的部署等，则可以略去这部分配置。

2 独立 AC 方案部署

2.1 概述

2.1.1 方案简介

在 WLAN 部署中，最关键的部件包括 AP 和 AC。独立 AC 方案是指采用单独的 AC 硬件设备（例如 WS6603 产品），通过直路或者旁挂方式实现对于所有 AP 的管理。

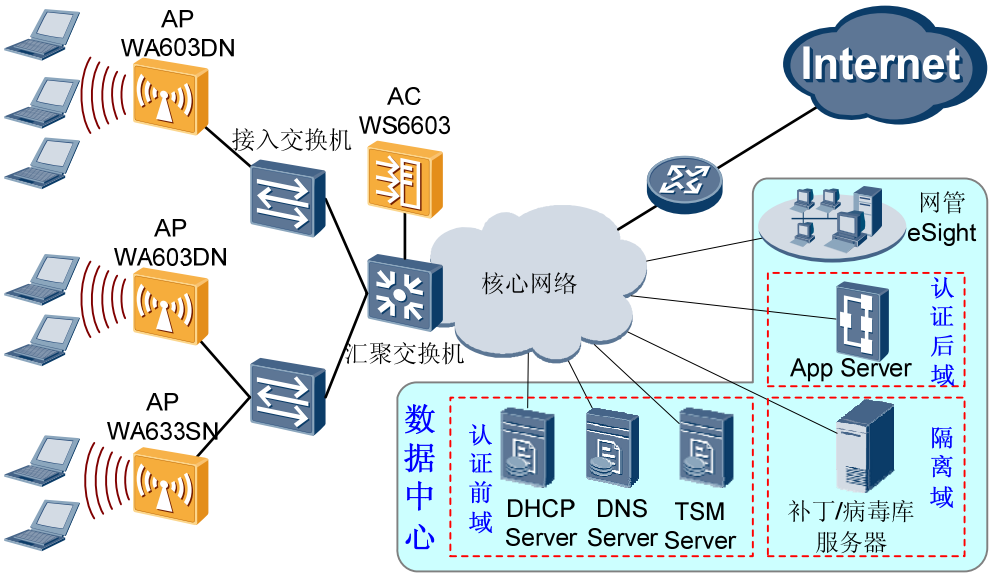
- 直路方式是指在将 AC 部署在 AP 与用户网关设备（汇聚或核心交换机）之间，实现对下辖所有 AP 的管理。
- 旁挂方式是指将 AC 部署在用户网关设备（汇聚或核心交换机）一侧，实现对用户网关设备下所有 AP 的管理。

独立 AC 方案一般应用在集中式 AC 的 WLAN 部署方案中。独立 AC 的性能优异，可以实现大容量高性能的 WLAN 网络部署。但是独立 AC 相比交换机集成的 AC 价格昂贵一些。企业可以根据自身的实际情况进行选择。

2.1.2 典型组网

企业 WLAN 独立 AC 方案的典型组网如图 2-1 所示。

图2-1 独立 AC 方案典型组网图



在独立 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP（例如 WA603DN）来负责无线终端的接入。使用独立的 AC 设备（WS6603）并旁挂在用户业务网关（汇聚或者核心交换机）一侧，负责完成对 AP 设备的管理。

在用户的安全和管理方面，使用 TSM 来实现对用户的接入认证，并实现对于用户的网络权限的策略控制。例如未认证时或认证失败时只能访问认证前域；认证通过但是终端不安全只能访问隔离域；认证通过并且终端安全可以访问认证后域。

在网络管理方面，使用企业专业网管系统 eSight 来实现对于企业网络的管理。

2.1.3 配套产品和版本

表2-1 独立 AC 方案配套产品和版本

部件	产品	版本
AP	WA603SN WA603DN WA633SN WA653SN WA653DN WA653EN	V100R003C01
AC	WS6603	V100R003C05
接入交换机	非特定，推荐 S2700/S3700 系列	非特定
汇聚交换机	非特定，推荐 S5700/S9300 系列	非特定
NAC 服务器	TSM	V100R002C06

部件	产品	版本
网管服务器	eSight	V200R001C00
DHCP 服务器	非特定，可以是外置服务器，或者交换机内置的 DHCP 服务器，也可以使用 AC 内置的 DHCP 服务器	非特定
DNS 服务器	非特定	非特定

2.1.4 部署思路

前置任务

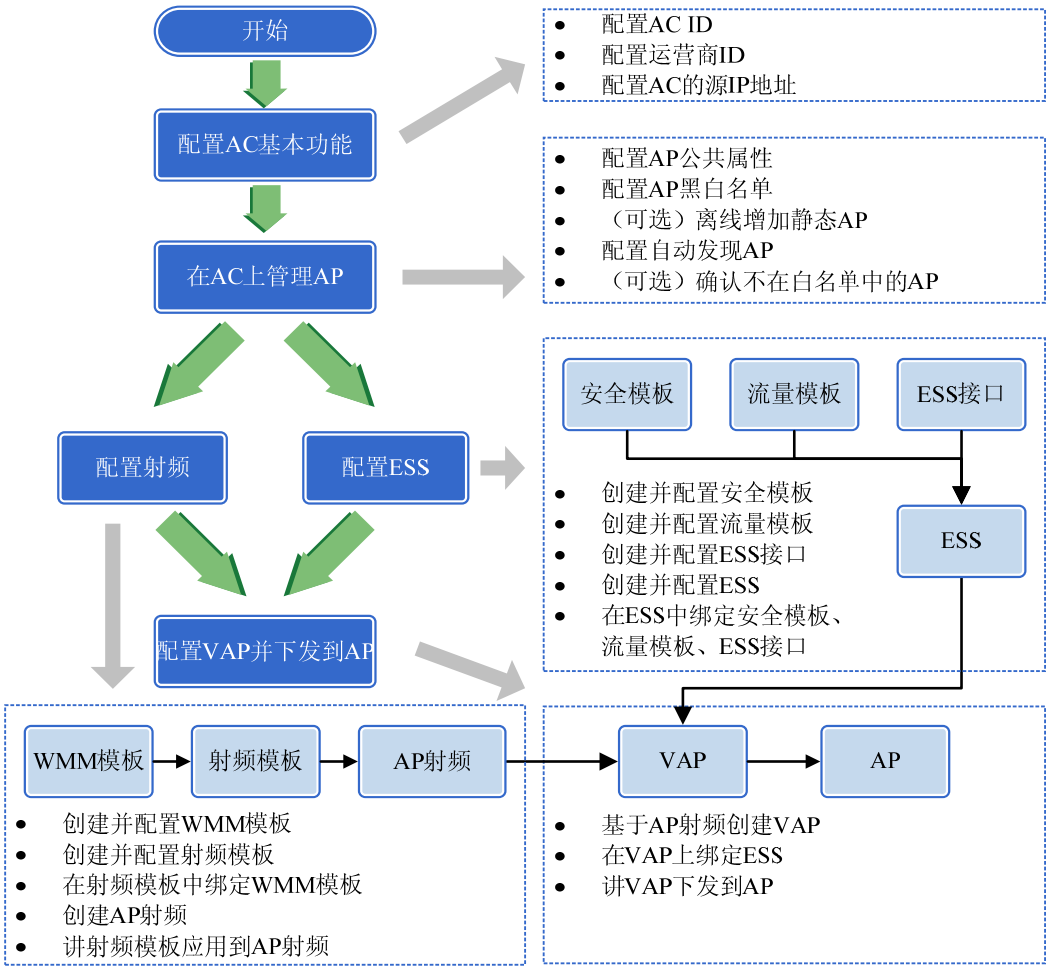
- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- TSM 服务器的操作系统和 TSM 软件已经安装完毕。
- eSight 网管服务器的操作系统和 eSight 软件安装完毕。
- 完成 VLAN/SSID、IP 地址等数据的规划。

配置思路

配置思路	配置注意事项
在各网元部件上配置接口、VLAN、IP 地址和路由，实现网络的基础互通。	NA
配置 AP 发现 AC 的方式，包括以下两种： • AP 通过 DHCP 服务器返回的报文中的 Option 43 字段来得知 AC 的 IP 地址。 • AP 通过 DHCP 服务器返回的报文中的 Option 15 字段得知 AC 的 DNS 域名，然后向 DNS 服务器发送 DNS 解析请求来得知 AC 的 IP 地址。	• 第一种方式要求 DHCP 服务器上配置 Option 43 选项，内容为 AC 的 IP 地址。 • 第二种方式要求 DHCP 服务器上配置 Option 15 选项，内容为 AC 的 DNS 域名。同时配置 DNS 服务器，增加 AC 域名对应的 IP 地址。
配置 AC 对 AP 的管理，配置步骤如下： • 配置 AC 基本功能。 • 在 AC 上管理 AP。 • 配置 WLAN 射频。 • 配置 ESS（Extended Service-Set）。 • 配置 VAP（Virtual AP）并下发到 AP。	详细的 AC 配置流程顺序、步骤详解和相互关系可以参见图 2-2。

配置思路	配置注意事项
（可选）在业务网关上配置 NAC 功能，实现对 WLAN 接入用户的认证和授权。	主要包括： • 配置 AAA 功能，设置用户的归属域、认证/授权的模式以及相应的 AAA 服务器等。 • 在接入交换机上配置 802.1x 认证或者在汇聚交换机上配置 Portal 认证。
（可选）配置 TSM 服务器。主要配置包括： • 配置认证服务器（Portal 认证服务器或者 802.1x 认证服务器），用于对终端进行安全认证。 • 配置隔离域和认证后域的信息。 • 配置策略模板，并将策略下发到用户。 • 配置用户账号（包括普通账号、MAC 账号、AD 账号及 LDAP 账号等），为账号配置接入隔离域及后域，实现对用户的网络权限控制。	• DHCP 服务器、DNS 服务器、TSM 服务器属于认证前域。 • 用于安全修复的补丁服务器或者病毒库服务器则划分到隔离域。 • 其他的应用服务器属于认证后域。 • 如果是普通账号，则需要在 TSM 服务器上配置用户名和密码。 • 如果是 AD 域账号，则需要另外部署域控制服务器，并配置用户名和密码。然后将账号同步至 TSM 服务器。
配置移动终端，安装用于网络接入的客户端软件（例如 802.1x 拨号软件）。	• 对于 Portal 认证来说，一般不需要对终端进行特殊配置。（但某些系统可能也有 Portal 认证客户端）。 • 而对于 802.1x 认证来说，需要在客户端上安装并配置 802.1x 认证客户端。 • 如果使用 TSM 作为 NAC 的认证服务器，那么客户端需使用 TSM Agent（它自带 Portal 认证或 802.1x 认证客户端）。
（可选）使用 eSight 进行 WLAN 网络管理。	通过 eSight 软件，可以查看： • WLAN 的概览信息 • 所有 AC 状态和基本信息 • 指定 AC 的详细信息 • AC 的告警信息 • AC 的性能指标 详细配置请参见“4 WLAN 网络管理”。

图2-2 独立 AC 方案的 AC 配置流程图



2.2 配置网络互通

配置网络互通主要是在网络设备上配置接口、VLAN、IP 地址、路由等，以及在服务器上配置 IP 地址等，实现终端、网络设备、服务器之间的网络层互相连通。

详细的配置过程略，请参考相应产品的产品文档。

2.3 配置 AP 发现 AC

2.3.1 概述

当 FIT AP 上线后，需要知道本 AP 所归属 AC 的 IP 地址，才能从 AC 获得相应的参数配置。AP 发现 AC 通常有三种方式：

- 广播方式

在这种方式下，AP 通过广播的方式向网络中所有的 AC 发起 CAPWAP 隧道连接，当有 AC 响应该 AP 后，CAPWAP 隧道建立。这种方式下，AP 发现 AC 是自主行为，在 AC 上无需进行任何配置。

- 通过 DHCP Option43 发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option43 选项，将 AC 的 IP 地址告知 AP。

- 通过 DHCP Option15 和 DNS 解析发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option15 选项，将 AC 的 DNS 域名告知 AP。

  AP 再向 DNS 服务器发起 AC 域名的解析请求，DNS 服务器返回响应报文，告知 AC 的 IP 地址。

上述几种方式的对比如表 2-2 所示。

表2-2 AP 发现 AC 的不同方式对比

方式	部署要求	优势	劣势	适用网络
广播方式	无	对已有网络没有额外要求	仅能用于AP/AC二层组网中	小型 WLAN 网络，AP/AC 二层组网
Option43 方式	DHCP Server 启动 Option 43 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网
Option15+ DNS 方式	部署 DNS Server； DHCP Server 支持 Option 15 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网

2.3.2 配置 AP 通过 DHCP Option43 发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option43 选项。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者 AC 内置的 DHCP 服务器。

本节以 AC（WS6603）内置的 DHCP 服务器来举例说明配置过程，其他情况请参考相应产品的产品文档。

配置步骤

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口。

步骤 4 执行命令 **ip address** *ip-address mask*，设置 VLANIF 的 IP 地址作为数据转发的三层接口。

步骤 5 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 6 执行命令 **wlan ac source interface vlanif** *vlan-id*，设置 AC 的源 IP 地址。

步骤 7 执行命令 **ip pool** *pool-name*，创建 IP 地址池。

步骤 8 执行命令 **gateway** *ip-address mask*，配置 IP 地址池的网关。

步骤 9 执行命令 **section** *section-id start-ip-address end-ip-address*，配置 IP 地址池中的地址段。

步骤 10 执行命令 **option 43 string** *text*，配置 DHCP 服务的 Option 功能，通过 DHCP option43 通告 AC 的 IP 地址。

注意

- 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

2.3.3 配置 AP 通过 DHCP Option15 和 DNS 解析发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option15 选项。同时需要指定 DNS 服务器，用于对 AC 的域名进行解析。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者 AC 内置的 DHCP 服务器。

本节以 AC（WS6603）内置的 DHCP 服务器来举例说明配置过程，其他情况请参考相应产品的产品文档。

有关 DNS 服务器的部署和配置请参考相应产品的产品文档。

配置步骤

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口。

步骤 4 执行命令 **ip address** *ip-address mask*，设置 VLANIF 的 IP 地址作为数据转发的三层接口。

步骤 5 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 6 执行命令 **wlan ac source interface vlanif** *vlan-id*，设置 AC 的源 IP 地址。

步骤 7 执行命令 **ip pool** *pool-name*，创建 IP 地址池。

步骤 8 执行命令 **gateway** *ip-address mask*，配置 IP 地址池的网关。

步骤 9 执行命令 **section** *section-id start-ip-address end-ip-address*，配置 IP 地址池中的地址段。

步骤 10 执行命令 **dns-suffix** *suffix-content*，配置 IP 地址池的 DNS 后缀。

步骤 11 执行命令 **dns-server** *ip-address* [**secondary** | **third**]，配置 IP 地址池的 DNS 服务器地址。

----结束

2.4 配置 AC

2.4.1 配置 AC 基本功能

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac-global** { **carrier id** { **cmcc** | **ctc** | **cuc** | **other** } | **ac id** *ac-id* } *，配置 AC ID，同时可以配置 AC 的运营商标识。

步骤 4 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 5 执行命令 **wlan ac source interface** { **loopback** *loopback-num* | **vlanif** *vlanif-num* }，配置 loopback 接口或 VLANIF 接口地址为 AC 源的 IP 地址。

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

----结束

2.4.2 在 AC 上管理 AP

配置 AP 公共属性

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。

步骤 5 执行命令 **max-sta-num** *max-sta-num*，配置某 AP 类型允许接入 AC 的 AP 个数。

步骤 6 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式。

步骤 7 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置 AP 升级对应的升级文件。

- 当升级模式为 ac-mode 时，需要将 AP 升级文件上载到 AC 中。
- 当升级模式为 ftp-mode 时，执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftp-username* | **ftp-password** *ftp-password*] *，配置 FTP 服务器 IP、客户端用户名、密码。

----结束

配置 AP 黑白名单

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **ap-whitelist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加合法 AP 的 MAC 或者 SN 到白名单里，可以批量增加。

步骤 5 执行命令 **ap-blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加非法 AP 的 MAC 或者 SN 到黑名单里，可以批量增加。

----结束

（可选）离线配置 AP

通常情况下，当配置了 AP 的公共属性和 AP 黑白名单后，AP 上线时，AC 是自动发现 AP 的。但是也可以通过手工的方式，离线增加一个 AP。

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行 **ap-auth-mode** *auth-mode* 命令，修改 AP 的认证模式，MAC 认证或 SN 认证。

步骤 5 执行命令 **ap id** *ap-id* [{ **type-id** *type-id* | **ap-type** *ap-type* } { **mac** *ap-mac* | **sn***ap-sn* } *]，离线增加一个 AP。

步骤 6 （可选）执行命令 **region-id** *region-id*，将增加的 AP 加入指定域。

步骤 7 （可选）执行命令 **profile-id** *profile-id*，将增加的 AP 绑定指定 AP 模板。

步骤 8 （可选）执行命令 **cpu warn-threshold** *threshold-num* 命令设置 AP 的 CPU 告警阈值。

步骤 9 （可选）执行命令 **mem warn-threshold** *threshold-num* 命令设置 AP 的内存告警阈值。

----结束

配置自动发现 AP

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。

步骤 5 执行命令 **ap-auth-mode** *auth-mode*，配置 AP 的认证方式（MAC、SN 或不检测）。

----结束

（可选）确认不在白名单中的 AP

如果 AP 未在白名单中配置，那么 AP 上线后，会处于未授权状态，此时，需要在 AC 上手工对 AP 进行确认，确认之后，AP 进入授权状态。

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **ap-confirm** { **all** | { **mac** *ap-mac* | **sn** *ap-sn* } [**id** *ap-id*] }，对 AP 进行确认。

AP 确认成功后，其 MAC 或 SN 将自动加入白名单，此 AP 自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，AP 正常工作。

----结束

2.4.3 配置 WLAN 射频

配置 WMM 模板

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }*，配置 WMM 模板。

步骤 5 执行命令 **wmm enable**，使能 WMM 功能。

步骤 6 执行命令 **wmm mandatory enable**，打开 WMM 控制许可开关。

步骤 7 （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* }*，配置终端上四个 WMM 队列的 EDCA 参数。

步骤 8 （可选）执行命令 **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** } }*，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

配置射频模板并绑定 WMM 模板

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。

步骤 5 （可选）执行命令 **radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。

步骤 6 （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。

步骤 7 （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。

步骤 8 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }，为射频模板绑定 WMM 模板。只有绑定了 WMM 模板的射频模板才可以被射频绑定。

----结束

将射频模板应用到指定射频

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。

步骤 5 执行命令 **bind radio-profile** { **id** *profile-id* | **name** *profile-name* }，为射频绑定射频模板。

----结束

（可选）配置 AP 射频资源管理

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。

步骤 5 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

步骤 6 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

步骤 7 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。

步骤 8 手工启动全局调优：

1. 执行命令 **quit**，返回 WLAN 视图。
2. 执行命令 **calibrate startup region** *region-id* [**listen-uncontrol-neighbor**]，启动指定域的全局调优。
3. 执行命令 **calibrate auto-startup region** *region-id* **time** *time* [**listen-uncontrol -neighbor**]，定时启动调优。

----结束

（可选）配置 AP 负载均衡

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **load-balance-group** { **name** *group-name* | **id** *group-id* }*，配置负载均衡组。

步骤 5 执行命令 **member ap-id** *ap-id* **radio-id** *radio-id*，向负载均衡组内添加射频。

步骤 6 配置负载均衡组的负载均衡模式：

- 执行命令 **traffic gap** *gap-threshold*，配置负载均衡组的负载均衡模式为流量模式。
- 执行命令 **session gap***gap-threshold*，配置负载均衡组的负载均衡模式为会话模式。缺省情况下，负载均衡组的负载均衡模式为会话模式。

步骤 7 执行命令 **associate-threshold** *associate-threshold*，配置负载均衡组的最大关联次数。

----结束

2.4.4 配置 ESS

配置安全模板

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* }*，配置安全模板。

步骤 5 配置安全策略，选择下述认证方式中的一种：

- WEP 开放系统认证
  - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
  - 执行命令 **wep authentication-methodopen-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
- WEP 共享密钥认证
  - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
  - 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。

- 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。
- 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

- WPA/WPA2 认证
  - 执行命令 **security-policy wpa**，配置安全策略为 WPA 方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 802.1x 认证方式和相应的加密方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
- WAPI 认证
  - 执行命令 **security-policyapi**，配置安全策略为 WAPI 方式。
  - 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。
  - 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file-name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
  - 执行命令 **wapi import private-key file-name** *file-name*，导入 AC 的私钥文件。
  - 执行命令 **wapi asuip** *ip-address*，配置 ASU 服务器的 IP 地址。

----结束

配置流量模板

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }*，配置流量模板。

步骤 5 （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。

步骤 6 （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，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 7 （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。

步骤 8 （可选）执行命令 **tunnel-priority up designate** { **tos** | **8021p** } *priority-value*，指定上行隧道优先级值。或者执行命令 **tunnel-priority up map** { **tos-tos** | **tos-8021p** | **8021p-tos** | **8021p-8021p** } *value0 value1 value2 value3 value4 value5 value6 value7*，配置上行隧道优先级的映射关系。

----结束

配置 ESS 并绑定安全模板和流量模板

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **ess name** *ess-name* [**id** *ess-id*] **ssid** *ssid* **traffic-profile** *traffic-profile-name* **security-profile** *security-profile-name* [**ssid-hide** { **enable** | **disable** } | **user-isolate** { **enable** | **disable** } | **type** { **service** | **ap-management** | **ac-management** } | **max-user-number** *user-number* | **association-timeout** *time* | **igmp-mode** { **proxy** | **snooping** | **off** }] *，配置 ESS 并绑定安全模板和流量模板。

----结束

2.4.5 配置 VAP 并下发到 AP

配置 VAP 并绑定 ESS

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **vap ap** *ap-id* **radio** *radio-id* **ess** { **id** *ess-id* | **name** *ess-name* } [**wlan** *wlan-id*]创建单个 VAP 或执行命令 **vap batch ap** { *ap-id* [**to** ap-id] } &<1-10> **radio** { *radio-id* [**to** *radio-id*] } &<1-10> **ess** { *ess-id* [**to** *ess-id*] } &<1-10>创建多个 VAP。

说明

也可以执行 **service-batch ap-type** { i**d** *ap-type-id* | **name** *ap-type-value* } **radio** *radio-id* **radio-profile** { **id** *profile-id* | **name** *radio-profile-name* } **ess id** { *ess-id* [**to** *ess-id*] } &<1-10>命令批量配置 VAP。

----结束

将 VAP 下发到 AP

步骤 1 执行命令 **enable**，进入特权模式。

步骤 2 执行命令 **config**，进入全局配置模式。

步骤 3 执行命令 **wlan ac**，进入 WLAN-AC 模式。

步骤 4 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

----结束

2.5 配置 NAC

2.5.1 概述

NAC 简介

如何在企业中构建安全的网络，在办公便捷、网络资源合理共享的同时发现并隔离不合法和不安全的终端主机，确保只有被授权的和通过安全检查的终端主机才能访问网络资源，从而保护重要的网络资源，是高层管理人员和 IT 部门较为关注的问题。

按照通用的企业网络架构，对于用户的认证和授权是通过部署 NAC 系统来完成。NAC 系统一般由如下部件组成：

- 终端代理

  终端代理是安装在用户终端系统上的专用客户端软件，与准入服务器联动进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。

- 网络准入设备

  网络准入设备是终端访问网络的网络控制点，是企业安全策略的实施者，负责按照准入服务器制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。

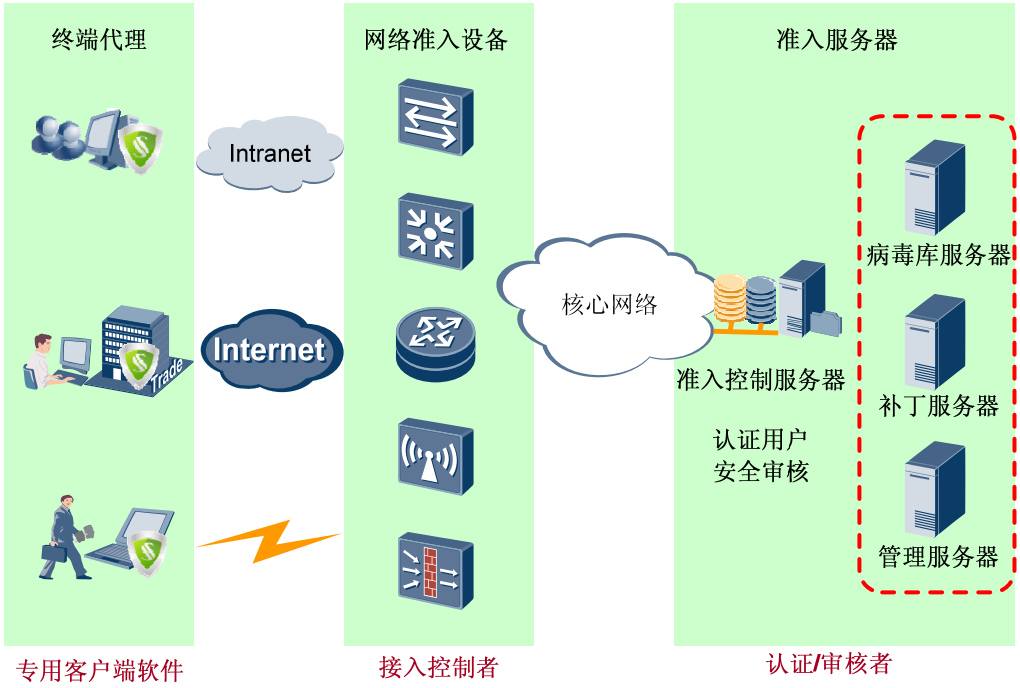
  网络准入设备通常又可称为用户业务网关，并不是一个物理实体，而是一个角色概念，通常由网络中的汇聚交换机（或者接入交换机）来担任。

- 准入服务器

  准入服务器是后台的安全管理和控制服务器。它可以进行用户管理，增加、删除、修改用户权限及用户部门配置，及安全策略的定制和管理等。还需要进行用户认证和安全审核，实施安全策略，并且与网络准入设备联动，下发用户权限。另外，准入服务器也包括病毒库服务器和补丁服务器等用于终端安全修复的服务器。

  准入服务器经常也被称为 AAA 服务器，它与用户业务网关之间可采用 RADIUS 等协议进行通信，共同完成对于用户的认证、计费和授权等功能。

图2-3 NAC 系统组成示意图



终端代理的详细描述和部署指导，请参考“2.7.2 配置认证客户端”。准入服务器的详细描述和部署指导，请参考“2.6 配置 TSM 服务器”。本节主要描述网络准入设备上的 NAC 功能部署。

业务网关上的 NAC 配置

在业务网关上（例如 S9300 交换机），NAC 的部署主要包括如下几方面：

- 配置 AAA 功能，设置用户的归属域、认证/授权的模式以及相应的 AAA 服务器等。
- 在用户接入的接口下配置 802.1x 或者 Portal 认证。

下面以 S9300 作为业务网关为例，列出了最基本的常用 NAC 配置步骤。更详细完整的配置步骤和内容请参见所使用产品的产品文档。

2.5.2 配置 AAA 功能

配置认证方案

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authentication-scheme** *authentication-scheme-name*，创建认证方案，并进入认证方案视图。

步骤 4 执行命令 **authentication-mode** { **hwtacacs** | **radius** | **local** }* [**none**]，配置认证模式。

----结束

配置授权方案

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **authorization-scheme** *authorization-scheme-name*，创建授权方案，并进入授权方案视图。

步骤 4 执行命令 **authorization-mode** [**hwtacacs**] { **if-authenticated** | **local** | **none** }，配置授权模式。

----结束

配置计费方案

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **accounting-scheme** *accounting-scheme-name*，创建计费方案，并进入计费方案视图。

步骤 4 执行命令 **accounting-mode** { **hwtacacs** | **radius** | **none** }，配置计费模式。

----结束

配置 RADIUS 服务器模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **radius-server template** *template-name*，创建 RADIUS 服务器模板，并进入 RADIUS 服务器模板视图。

步骤 3 执行命令 **radius-server authentication** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 认证服务器。

步骤 4 执行命令 **radius-server accounting** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 计费服务器。

步骤 5 执行命令 **quit**，返回系统视图。

步骤 6 执行命令 **radius-server authorization** *ip-address* { **server-group** *group-name* | **shared-key** { **cipher** | **simple** } *key-string* } * [**ack-reserved-interval** *interval*]，配置 RADIUS 授权服务器。

----结束

配置域

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域，并进入域视图。

步骤 4 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域使用的认证方案。

步骤 5 （可选）执行命令 **authorization-scheme** *authorization-scheme-name*，配置域使用的授权方案。

如果使用 RADIUS 认证，则省略本步骤。

步骤 6 执行命令 **accounting-scheme** *accounting-scheme-name*，配置域使用的计费方案。

步骤 7 执行命令 **radius-server** t*emplate-name*，配置域使用的 RADIUS 服务器模板。

----结束

2.5.3 配置 Portal 认证

配置 Web 认证服务器

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **web-auth-server** *server-name*，配置 Web 认证服务器，并进入 Web 认证服务器视图。

步骤 3 执行命令 **server-ip** *ip-address*，配置 Web 认证服务器的 IP 地址。

步骤 4 执行命令 **url** *url-string*，配置 Web 认证服务器对应的 URL。

步骤 5 执行命令 **port** *port-number* [**all**] ，配置 Web 认证服务器接收 S9300 发送的通知报文的端口号。

----结束

接口下绑定 Web 认证服务器

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 i**nterface** *interface-type interface-number*，进入接口视图。

说明

只能是 VLANIF 接口，目前 S9300 只能通过 VLANIF 接口完成对接入用户的 Web 认证。

步骤 3 执行命令 **web-auth-server** *server-name*，在 VLANIF 接口下绑定 Web 认证服务器。

----结束

（可选）配置 Portal 认证的 Free Rule

当某些特殊用户在未通过认证的情况下需要访问特定资源，可以配置 Free Rule。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **portal free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address mask* { *mask-length* | *ip-mask* } | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address mask* { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* }* } }*，配置免认证规则。

----结束

2.5.4 配置 802.1x 认证

使能 802.1x 认证

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x enable**，使能全局 802.1x 认证功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 4 执行命令 **dot1x enable**，在接口下使能 802.1x 认证功能。

----结束

配置 802.1x 用户的认证方法

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x authentication-method** { **chap** | **eap** | **pap** }，配置 802.1x 用户的认证方法。

----结束

（可选）使能 MAC 旁路认证功能

MAC 旁路认证，指当终端进行 802.1x 认证失败后，把它的 MAC 地址作为用户名和密码上送 RADIUS 服务器进行认证。对于某些特殊终端，例如打印机等，无法使用和安装 802.1x 终端软件，可以通过基于 MAC 的旁路认证方式进行认证。

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **dot1x mac-bypass**，在接口下使能 MAC 旁路认证功能。

----结束

2.6 配置 TSM 服务器

2.6.1 概述

TSM 简介

为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为公司推出 TSM 产品，该产品为企业提供整合的内部网络安全解决方案，实现从终端到业务系统的控制和管理功能。

TSM 基于 TSM 代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

TSM 系统基于 Client/Server 模式，由 TSM Server 和 TSM Agent 两部分组成。其中 TSM Agent 是 TSM 的一个组件，作为 TSM 的客户端软件，安装在终端主机。（详见“2.7.2 配置认证客户端”）

TSM Server 是 TSM 系统的后台服务器部分，它可以作为企业 NAC 系统的准入服务器来进行部署，可提供接入认证、权限控制、终端管理、攻击防御、资产管理等功能，并具有高可靠性、执行灵活、融合开放等特点。

TSM in WLAN

对于企业的 WLAN 网络来说，在网络中部署 TSM 服务器，主要实现以下两大功能：

- 对本地用户进行管理，增加、删除、修改用户权限及用户部门配置，以及安全策略的定制和管理等。或者对外部认证源服务器的用户账号进行同步。
- 与网络准入设备联动，基于用户账号（本地账号或者同步的外部账号）完成用户认证和安全审核，实施安全策略，下发用户权限。

下面的 TSM 服务器部署也主要围绕着两大方面来进行介绍。包括如下内容：

- 配置普通账号
- 同步 AD 域账号
- 配置 Portal 认证控制
- 配置 802.1x 认证控制

注意

TSM 不支持同时启用 802.1x 交换机接入控制方式和 Portal 网关接入控制方式。

2.6.2 配置普通账号

在 TSM 中，用户管理涉及三个依次隶属的概念：部门、终端用户、账号。一个部门可以包含多个终端用户，一个终端用户可包含多个账号。

账号可以分为本地账号和外部认证源账号（例如 AD 域账号）两种。

- 本地账号是指用户名和密码等信息都配置在 TSM 服务器上的普通账号。
- 外部认证源账号是指企业中另外部署了其他认证服务器，为了确保终端用户使用现有的账号而不是新建账号进行认证，TSM 服务器上只同步外部认证源账号信息（不包括密码），用户直接使用外部认证源账号进行网络登录。

配置部门信息

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。

步骤 3 在右侧操作区域选择“部门”页签。

步骤 4 在部门导航树选择待创建部门的上级部门。

步骤 5 在“部门”页签下方单击“增加”，出现“增加部门”对话框。如图 2-4 所示。

图2-4 增加部门

步骤 6 输入部门的参数后，单击“确定”，出现“增加成功”的对话框。

步骤 7 单击“确定”，完成部门信息的创建。

----结束

配置终端用户信息

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。

步骤 3 在右侧操作区域选择“用户”页签。

步骤 4 在部门导航树选择需要创建终端用户的目标部门。

步骤 5 在“用户”页签下方单击“增加”，出现“增加用户”对话框。

图2-5 增加用户

步骤 6 输入终端用户的参数后，单击“确定”，出现“增加成功”的对话框。

步骤 7 单击“确定”，完成终端用户信息的创建。

----结束

配置本地账号信息

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。

步骤 3 在右侧操作区域选择“用户”页签。

步骤 4 在“部门用户管理”界面左侧的部门导航树选择需要创建普通账号的目标部门。

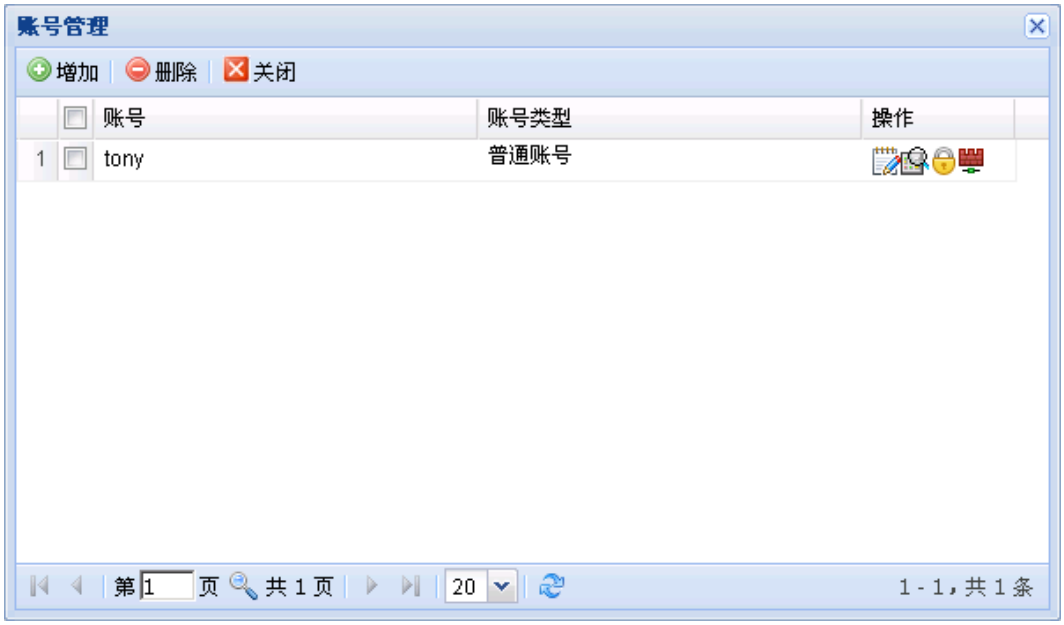
“部门用户管理”界面右侧显示该部门下的所有终端用户，如图 2-6 所示。

图2-6 查看指定部门的所有终端用户

		用户名	所属部门	用户ID	职务	办公电话	描述	操作
1		张三	TSM财务部	00000001	会计	0755-368...	负责公司的各类...	
2		李四	TSM财务部	00000002	会计	0755-368...	负责公司的各类...	
3		王五	TSM财务部	00000003	会计	0755-368...	负责公司的各类...	

步骤 5 在需要创建普通账号的终端用户右侧单击。显示终端用户的账户列表。如图 2-7 所示。

图2-7 查看终端用户的账户列表



步骤 6 单击“增加”，出现“增加账号”对话框，如图 2-8 所示。

图2-8 增加账号

步骤 7 输入普通账号的参数后，单击“确定”，出现“增加成功”的对话框。

步骤 8 单击“确定”，完成普通账号信息的创建。

----结束

2.6.3 配置按 OU 方式同步 AD 域账号信息

注意

关于 AD 域控制服务器的设置，以及用户账号信息的创建的步骤，请参考相关产品的帮助或文档，或者参考 TSM Server 软件的联机帮助文档。

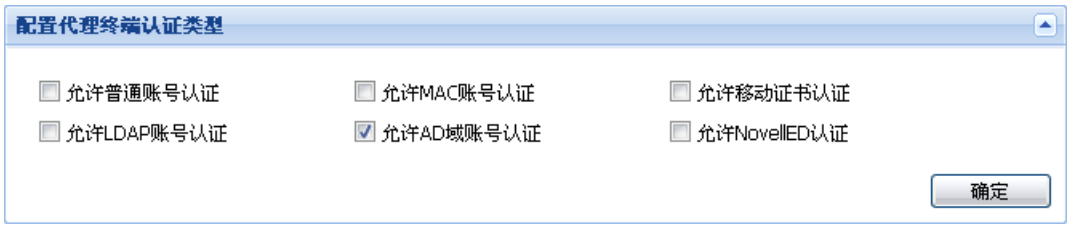
本节只描述如何将 AD 域服务器上的 AD 账号信息同步到 TSM 服务器的过程和步骤。

启用 Microsoft AD 域认证方式

步骤 1 在 TSM 管理器的导航栏单击“系统配置”。

步骤 2 在左侧菜单栏选择“终端配置 > 全局参数”。出现“配置代理终端认证类型”对话框。如图 2-9 所示。

图2-9 配置代理终端认证类型



步骤 3 选中“允许 AD 域账号认证”。

步骤 4 单击“确定”，出现“修改成功”的对话框。

步骤 5 单击“确定”，完成配置。

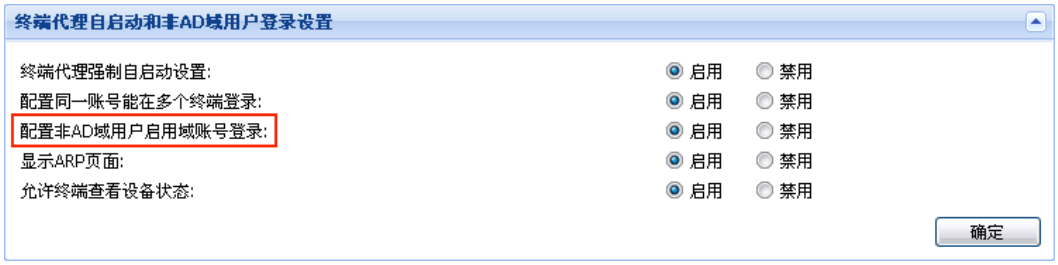
----结束

（可选）配置非 Microsoft AD 域用户启用域账号登录

步骤 1 在 TSM 管理器的导航栏单击“系统配置”。

步骤 2 在左侧菜单栏选择“终端配置 > 全局参数”。出现“终端代理自启动和非 AD 域用户登录”对话框。如图 2-10 所示。

图2-10 终端代理自启动和非 AD 域用户登录



步骤 3 根据实际情况选择是否允许未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证。

- 要允许未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证，选中“配置非 AD 域用户启用域账号登录”右侧的“启用”。
- 要禁止未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证，选中“配置非 AD 域用户启用域账号登录”右侧的“禁用”。

步骤 4 单击“确定”，出现“修改成功”的对话框。

步骤 5 单击“确定”，完成配置。

----结束

配置 Microsoft AD 域控制器的连接参数

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 > AD 服务器”。

步骤 3 单击“增加”，出现“增加 AD”对话框，如图 2-11 所示。

图2-11 增加 AD 服务器

详细参数解释如表 2-3 所示。

表2-3 设置同步 Microsoft AD 域账号时 Microsoft AD 域控制器连接的参数说明

参数	类型	说明
同步类型	必填项	设置是否从 Microsoft AD 域控制器同步节点与账号。 按 OU 同步 Microsoft AD 域账号时，选择“按 OU 同步”。
认证源	必填项	设置 Microsoft AD 域控制器的名称，方便管理员区分 TSM 与哪一台 Microsoft AD 域控制器联动。 该名称不能与已配置的认证源名称重复，最大长度为 100byte。
类型	无	显示外部认证源的类型。
主服务器地址	必填项	输入 Microsoft AD 域控制器的 IP 地址。
备用服务器地址	选填项	如果 Microsoft AD 域控制器采用主备方式部署，请输入 Microsoft AD 备份域控制器的 IP 地址。

参数	类型	说明
端口	必填项	输入 Microsoft AD 域控制器提供目录服务的端口号。 在安装 Microsoft AD 域控制器时，如果不配置 SSL，Microsoft AD 域控制器默认使用 389 作为服务端口。如果配置了 SSL，Microsoft AD 域控制器默认使用 636 作为服务端口。 除非在安装规划时改变了服务端口，否则请保持默认值。
服务器域名	必填项	输入 Microsoft AD 域控制器的域名。
基准 DN	必填项	输入根节点的 DN。
同步账号	必填项	输入在 Microsoft AD 域控制器中创建的同步账号。
同步密码	必填项	输入“同步账号”对应的密码。
认证账号	选填项	输入在 Microsoft AD 域控制器中创建的认证账号。
认证密码	选填项	输入“认证账号”对应的密码。
AD 故障时，允许 AD 认证直接通过(Kerberos 除外)	选填项	设置当 Microsoft AD 域控制器出现故障时，是否取消向 Microsoft AD 域控制器验证终端用户身份的过程。该参数仅适用于非 Kerberos 认证流程。 选中该项，当 Microsoft AD 域账号认证不采用 Kerberos 认证流程时，只要终端用户使用的 Microsoft AD 域账号已经同步到 TSM 管理器，则终端用户能够认证通过。
启用 SSL	选填项	设置是否启用 SSL。启用 SSL 后，TSM 与 Microsoft AD 域控制器联动时，将采用 SSL 协议加密，能够提高联动过程的安全性。 在 TSM 配置启用 SSL 的前提条件是：已经在 Microsoft AD 域控制器完成了 SSL 的相关配置。有关在 Microsoft AD 域控制器配置 SSL 的操作请参见 Microsoft AD 域控制器的相关文档。

步骤 4 输入 Microsoft AD 域控制器的连接参数后，单击“确定”，出现“增加成功”的对话框。

步骤 5 单击“确定”，完成 Microsoft AD 域控制器的连接参数的配置。

----结束

配置部门信息

请参见“2.6.2 配置普通账号”中的“配置部门信息”。

设置 Microsoft AD 域账号支持的接入方式

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。如图 2-12 所示。

图2-12 查看外部认证源列表

步骤 3 单击认证源右侧的。出现“外部认证源配置”对话框。如图 2-13 所示。

图2-13 配置外部认证源

步骤 4 在“登录类型”中选中需要支持的接入受控网络的方式。

步骤 5 单击“确定”，出现“设置成功”的对话框。

步骤 6 单击“确定”，完成配置。

----结束

（可选）自定义 TSM 管理器与 Microsoft AD 域控制器字段的关联关系

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。

步骤 3 单击认证源右侧的。出现“外部认证源配置”对话框。如图 2-14 所示。

图2-14 配置外部认证源

步骤 4 选择“部门”页签。输入部门参数。

步骤 5 选择“用户”页签。输入终端用户参数。如图 2-15 所示。

图2-15 配置外部认证源的终端用户信息

步骤 6 选择“其它”页签。输入其它参数。如图 2-16 所示。

图2-16 配置外部认证源的其它信息

步骤 7 单击“确定”，出现“设置成功”的对话框。

步骤 8 单击“确定”，完成配置。

----结束

关联源 DN 与目标部门

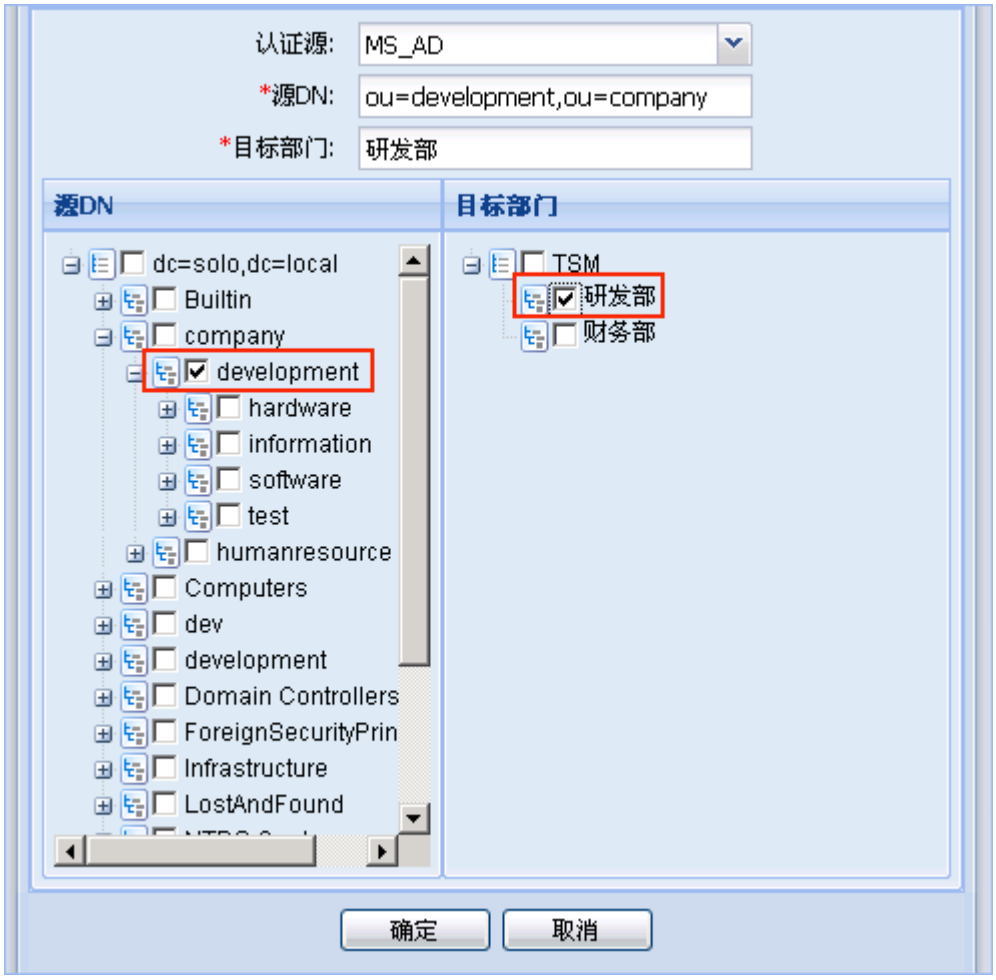
指定源节点与目标部门的关联关系，以便源节点的子节点及其账号能够同步复制到 TSM 管理器的目标部门。

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 > 同步范围”。

步骤 3 单击“增加 OU 同步”。出现设置源 DN 和目标部门的关联对话框，如图 2-17 所示。

图2-17 设置源 DN 和目标部门的关联



步骤 4 设置源 DN 与目标部门的关联参数，单击“确定”，出现“增加成功”对话框。

步骤 5 单击“确定”，完成源 DN 和目标部门的关联。

----结束

配置同步任务的执行周期

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。

图2-18 查看外部认证源列表

步骤 3 单击认证源右侧的。出现“自动同步设置”对话框。如图 2-19 所示。

图2-19 自动同步设置

步骤 4 设置自动同步参数，单击“确定”，出现“设置成功”的对话框。

步骤 5 单击“确定”，完成配置。

----结束

立即同步子节点和账号

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“外部数据源 >AD 服务器”，出现外部认证源列表。

图2-20 查看外部认证源列表

步骤 3 单击认证源右侧的。出现“同步任务开始执行”对话框。

步骤 4 单击“确定”，等待同步任务完成。

----结束

2.6.4 配置 Portal 认证控制

配置 Portal 网关

步骤 1 在 TSM 管理器顶部单击“接入控制”。

步骤 2 在左侧的菜单栏中选择“接入控制配置 >PORTAL 网关”。

步骤 3 选择“PORTAL 网关”页签。

步骤 4 单击“增加”。出现 Portal 网关配置对话框，如图 2-21 所示。

图2-21 Portal 网关配置

步骤 5 输入 Portal 网关的连接参数。

步骤 6 单击“增加”，出现“增加 IP 地址段”对话框。

图2-22 增加 IP 地址段

步骤 7 输入起始 IP 地址和结束 IP 地址。

步骤 8 单击“确定”，关闭“增加 IP 地址段”对话框。完成 IP 地址段的配置，将终端主机所在网段加入 IP 地址列表，表示对这些 IP 地址段启用 Portal 认证网关。

步骤 9 单击“确定”，出现“增加成功”对话框。

步骤 10 单击“确定”，完成配置。

----结束

配置隔离域

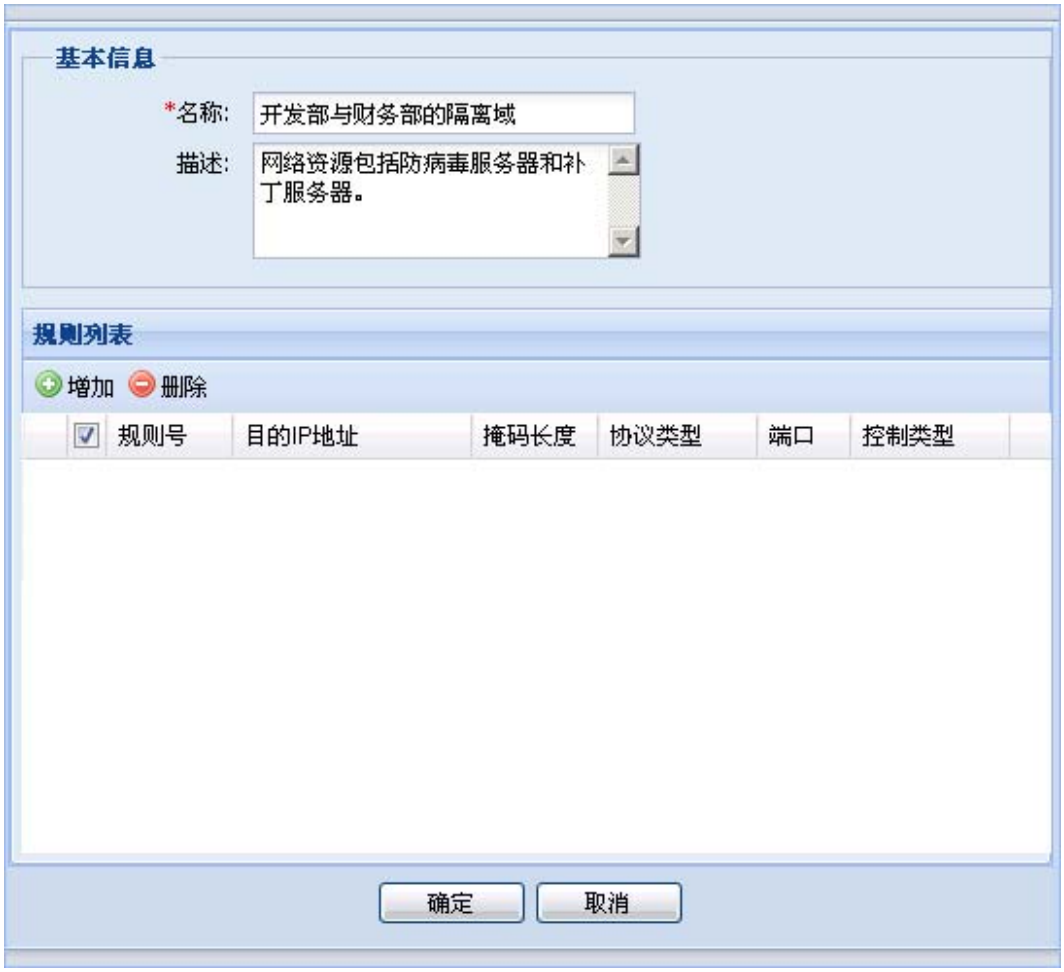
步骤 1 在 TSM 管理器顶部单击“接入控制”。

步骤 2 在左侧的菜单栏中选择“接入控制配置 > PORTAL 网关”。

步骤 3 选择“隔离域”页签。

步骤 4 单击“增加”，出现隔离域配置对话框。

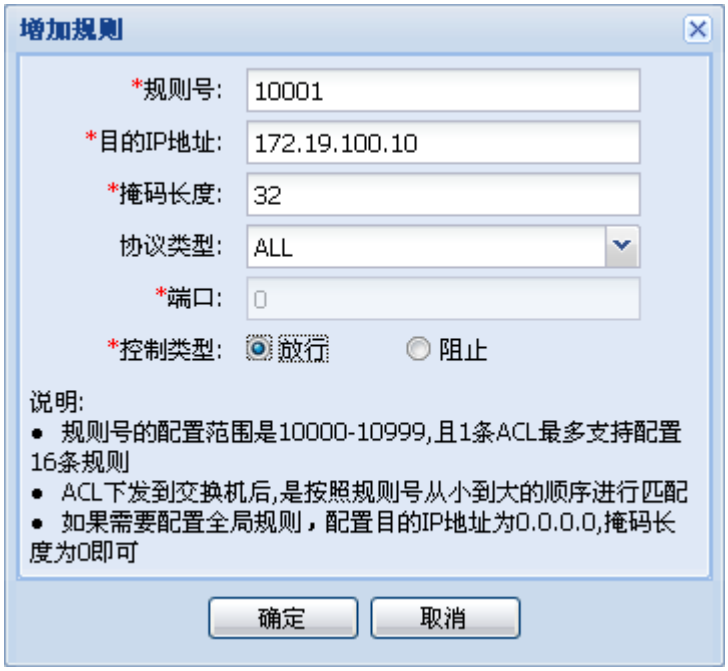
图2-23 隔离域配置



步骤 5 输入隔离域的相关参数。

步骤 6 单击“增加”。出现“增加规则”对话框。

图2-24 增加规则



步骤 7 输入规则的相关参数。单击“确定”，完成规则的配置并返回隔离域配置对话框。

步骤 8 单击“确定”，出现“增加成功”对话框。

步骤 9 单击“确定”，完成隔离域的配置。

----结束

配置认证后域

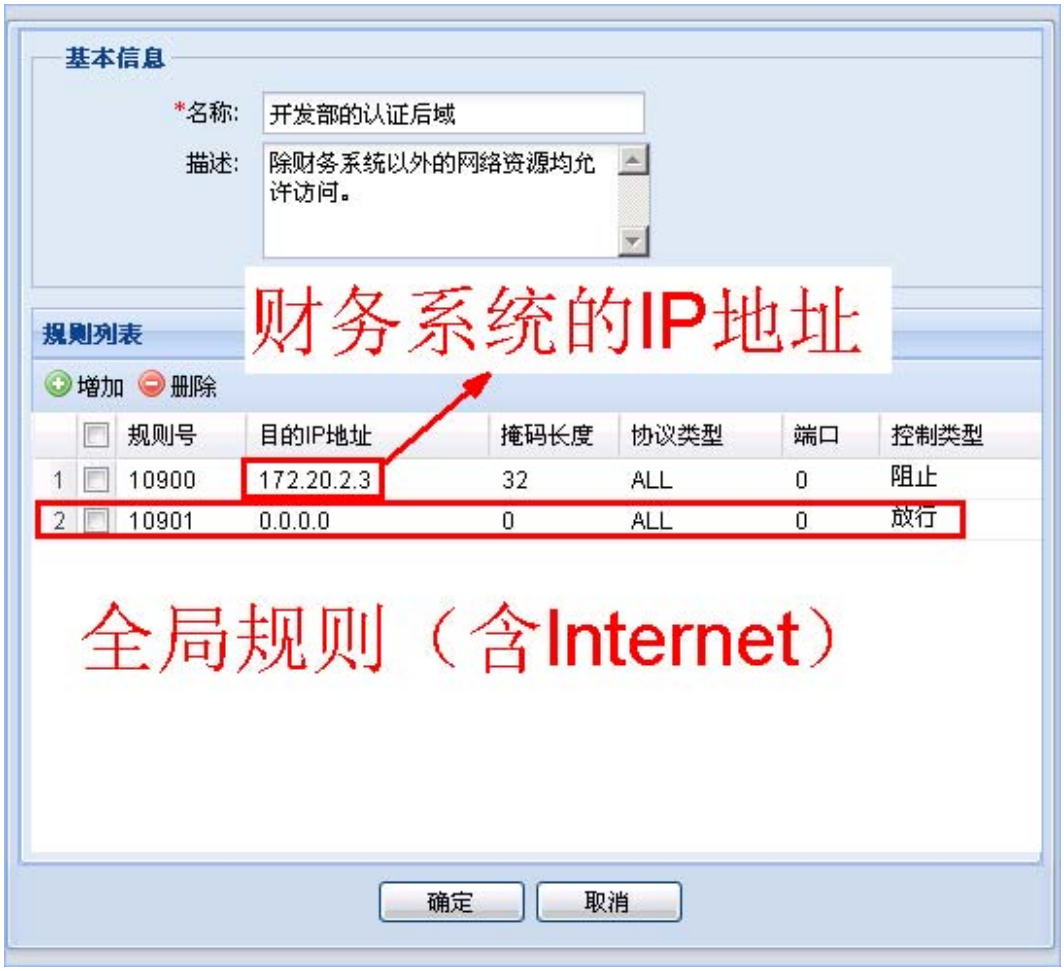
步骤 1 在 TSM 管理器顶部单击“接入控制”。

步骤 2 在左侧的菜单栏中选择“接入控制配置 > PORTAL 网关”。

步骤 3 选择“后域”页签。

步骤 4 单击“增加”，出现认证后域配置对话框。

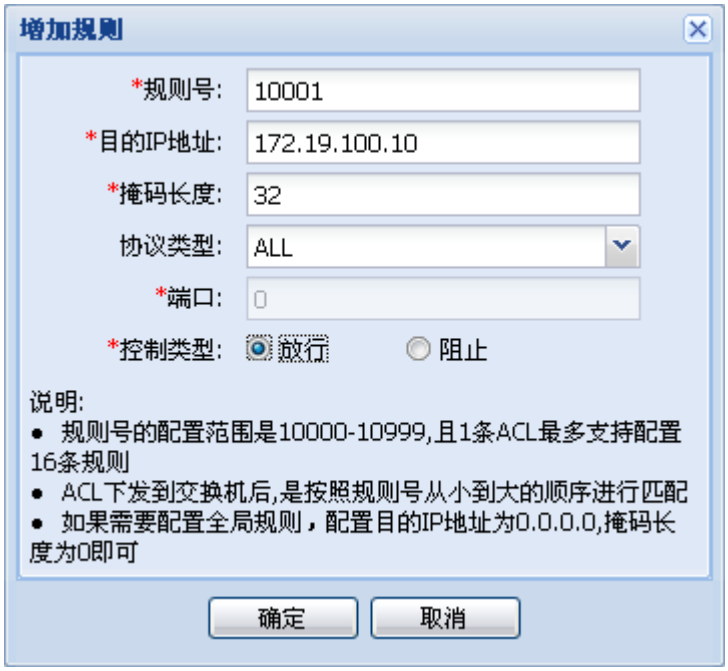
图2-25 认证后域配置



步骤 5 输入认证后域的相关参数。

步骤 6 单击“增加”。出现“增加规则”对话框。

图2-26 增加规则



步骤 7 输入规则的相关参数。单击“确定”，完成规则的配置并返回认证后域配置对话框。

步骤 8 单击“确定”，出现“增加成功”对话框。

步骤 9 单击“确定”，完成认证后域的配置。

----结束

将隔离域和认证后域应用到部门

步骤 1 在 TSM 管理器的导航栏单击“部门管理”。

步骤 2 在左侧菜单栏选择“部门用户 > 部门用户管理”。

步骤 3 选择“部门”页签。

步骤 4 在部门导航树中选中待应用隔离域和认证后域的部门，然后在工具栏单击“部门接入控制管理”。

步骤 5 选择“自定义设置”。

步骤 6 选择“PORTAL 网关”页签。

步骤 7 设置开发部的隔离域和认证后域。

图2-27 设置部门的隔离域和认证后域

步骤 8 单击“确定”，出现“设置成功”对话框。

步骤 9 单击“确定”，完成隔离域和认证后域到部门的应用。

----结束

2.6.5 配置 802.1x 认证控制

注意

本节所描述的配置步骤和过程是基于 802.1x 标准协议(交换机组中的交换机类型选择除“华为 NAC 系列”之外的类型)，该种方式下，无法基于部门和角色对用户权限进行控制。

如果选择的是华为 NAC 系列，则还可以配置隔离域、认证后域，并应用到部门或者具体账号。相关详细配置请参考 TSM Server 的帮助文档。

配置交换机组

步骤 1 在 TSM 管理器的导航栏单击“接入控制”。

步骤 2 在左侧菜单栏选择“接入控制配置 > 802.1x 交换机”。

步骤 3 选择“交换机组”页签。

步骤 4 单击“增加”，输入交换机组的相关参数。

图2-28 输入交换机组的相关参数

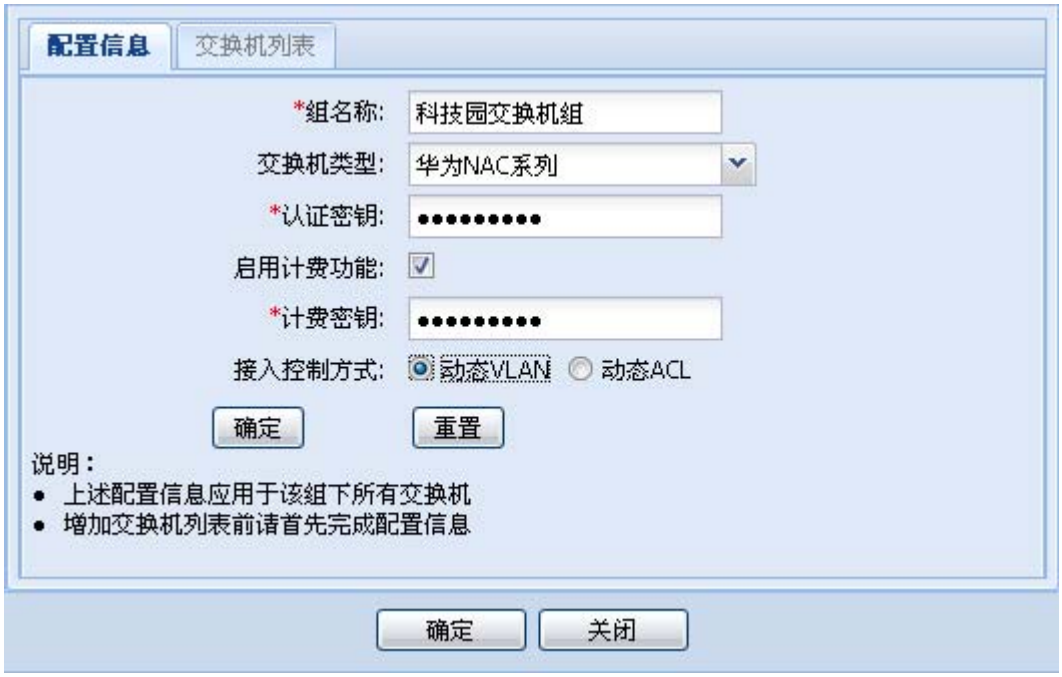


表2-4 增加交换机组的参数说明

参数	说明
组名称	输入交换机组的唯一名称。
交换机类型	选择该交换机组中交换机的厂家类型，未在下拉列表中单独列出的交换机类型，请选择其他类型。
认证密钥	交换机上配置的与 TSM 控制器通信的认证加密密钥。
启用计费功能	少数交换机需要启用计费功能，才能使认证通过的终端主机长时间保持端口开放，服务器上配置启用该功能用于配合交换机完成计费。
计费密钥	如果配置启用计费功能，此处填写交换机上配置的计费加密密钥。

参数	说明
接入控制方式	当“交换机类型”设置为“华为 NAC 系列”时，设置是通过“动态 VLAN”还是“动态 ACL”来实现接入控制。在使用标准 802.1x 协议的交换机实施接入控制时不能选择接入控制方式。

步骤 5 单击“确定”，出现“保存配置信息成功”对话框。

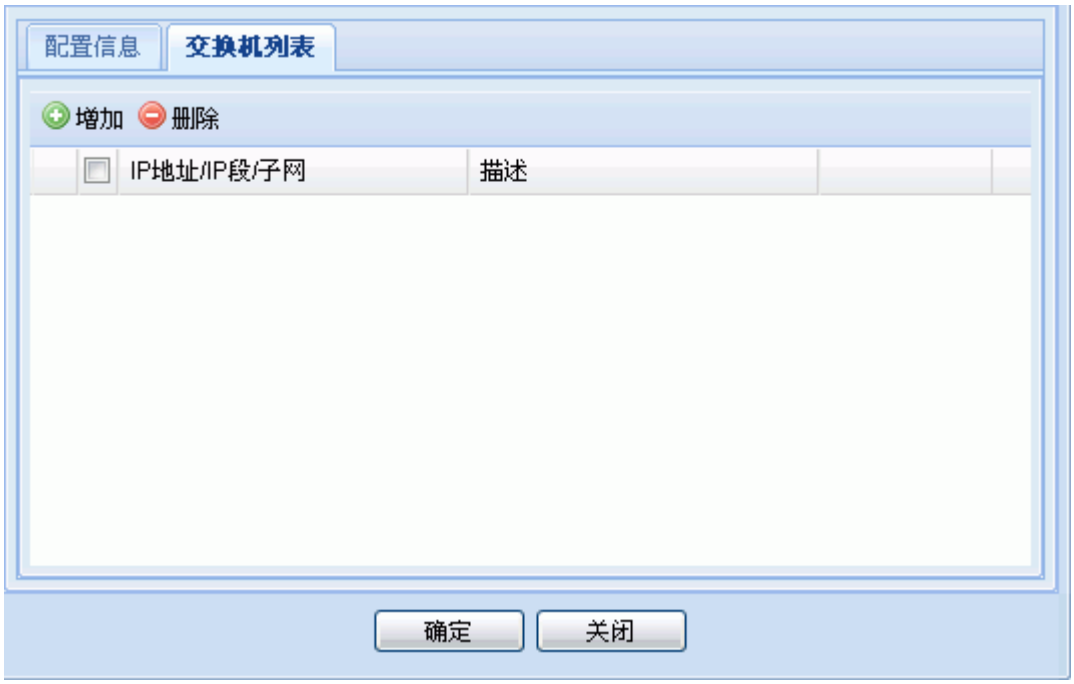
步骤 6 单击“确定”，完成交换机组的配置。

----结束

配置交换机列表

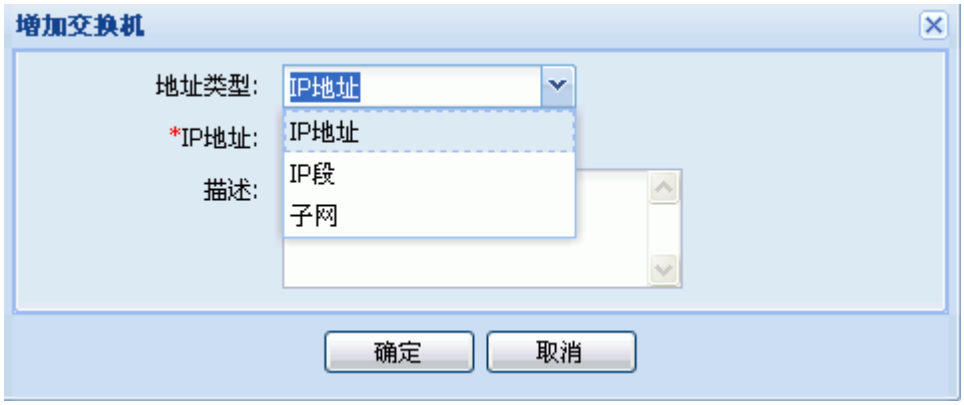
配置交换机组成功后，会自动跳转到交换机列表界面。

图2-29 交换机列表



步骤 2 单击“增加”，出现“增加交换机”对话框。

图2-30 增加交换机



步骤 3 输入交换机的参数。

表2-5 增加交换机的参数说明

参数	说明
地址类型	• IP 地址：通过增加 IP 地址增加一台交换机。 • IP 段：指定一个地址段，该 IP 地址段中的所有地址均是交换机的 IP 地址。 • 子网：通过地址 + 掩码的方式指定一个子网，该子网中所有的 IP 地址均为交换机的 IP 地址。 交换机可能配置了多个 IP 地址，NAS-IP 是交换机专门供 RADIUS 通信用的地址，添加的交换机 IP 地址必须是交换机的 NAS-IP，否则会产生“radius no response”错误。 如果交换机没有提供配置 NAS-IP 的命令，则应在交换机路由表中查找到达 TSM 控制器的出接口，出接口对应的 IP 地址作为添加交换机时输入的 IP 地址。
描述	输入交换机的描述信息，方便管理员维护该交换机列表。

步骤 4 单击“确定”，出现“增加交换机成功”对话框。

步骤 5 单击“确定”，完成交换机的配置。

----结束

2.7 配置终端

对于 WLAN 接入的终端（STA），需要具备支持 802.11 系列标准的无线网络硬件模块（例如无线网卡），才能实现和 AP 的无线对接。

在 STA 上，首先要对无线网络进行配置，例如设置 WLAN 网络的 SSID、密码和加密方式等，这样 STA 才能正常接入 AP。

其次，如果在企业网络中，部署了 NAC 系统，用户接入时需要进行认证，则还可能需要在 STA 上配置认证的客户端（例如 802.1x 认证），用户才能正常接入企业网络。

2.7.1 配置无线网络

配置无线网络可以使用自动发现的方式进行，也可以采用手工添加的方式进行。对于自动发现的方式，只要在 STA 发现 WLAN 网络后，按照相应的提示进行连接（有可能需要输入连接的密码）即可。

说明

推荐 STA 使用自动发现的方式来连接到 WLAN 网络。对于手工配置无线网络的方式，请参考 STA 所对应的文档进行配置。

2.7.2 配置认证客户端

概述

在企业网络中，用户的接入认证方式一般有 Portal 认证和 802.1x 认证两种。

- 对于 Portal 认证，一般不需要特殊的客户端，只需要使用 Web 浏览器访问 Portal 服务器，在认证页面上输入用户名和密码，提交之后即可进行认证。
- 对于 802.1x 认证，需要安装 802.1x 拨号的客户端软件，在软件界面上输入用户名和密码，然后进行 802.1x 拨号，向服务器发起认证。

对于 802.1x 认证的客户端，请参考您所使用的客户端软件的使用说明书或者帮助文档来进行配置。

本节以华为提供的 TSM Agent 软件来介绍认证客户端的配置。

TSM Agent

TSM 是华为技术有限公司自主研发的一种基于主机保护和集中安全管理的防护软件。是针对企业等组织的局域网内部网络安全开发的终端安全管理系统。

TSM 系统基于 Client/Server 模式，由 TSM Server 和 TSM Agent 两部分组成。TSM Agent 是 TSM 的一个组件，作为 TSM 的客户端软件，安装在终端主机。

TSM Agent 并不仅仅是一个认证客户端软件，而是一个终端安全综合管理软件，它提供了强大的终端安全管理功能，包括：

- 提供身份认证功能。
- 检查终端主机的安全隐患，并协助终端用户消除安全隐患来提高终端主机的安全性。
- 实时管理终端用户的行为，引导终端用户遵循组织机构制定的安全策略。
- 监控终端主机的运行状态。
- 协助终端用户安装 Microsoft Windows 操作系统补丁及其他软件。
- 在终端主机出现问题时接受管理员的远程协助。

- 注册资产，设置资产的所在地和责任人。
- 诊断终端用户无法连接服务器的故障原因。
- 接收管理员发布的公告。

TSM Agent 的认证功能

对于 TSM Agent 来说，支持 Portal 认证、802.1x 认证、MAC 认证等多种认证方式，并且其认证方式是集成融合的，一个客户端即可实现多种认证方式。用户不需要再使用 Web 浏览器或者单独的 802.1x 客户端软件。

TSM Agent 配置步骤

注意

很多情况下，TSM Agent 的安装程序已经根据企业的部署需求，由网络管理员或华为技术支持工程师完成定制，此时终端用户只需要完成软件的安装后，即可进行认证并接入网络，无需进行额外的配置。

步骤 1 在终端上安装 TSM Agent 软件，具体过程略。

安装完成后，Windows 桌面的系统托盘中会出现 TSM Agent 的图标。表示终端用户未进行认证。

步骤 2 双击图标，打开 TSM Agent 认证界面，如图 2-31 所示。

图2-31 TSM Agent 认证界面

步骤 3 在账号和密码框中分别输入用户名和密码。然后根据需要选择是否“保存密码”和“自动认证”。

说明

用户名和密码必须已在 TSM 服务器上注册，详细过程请参见“2.6.2 配置普通账号”或者“2.6.3 配置按 OU 方式同步 AD 域账号信息”。

步骤 4 如果是首次使用 TSM Agent，则单击“高级设置”按钮，展开高级设置选项，如图 2-32 所示。

1. 在“服务器”中输入 TSM 认证服务器的 IP 地址。
2. 如果要使用 802.1x 认证，则选中“启用 802.1x 协议”复选框，并且根据需要选择是否启用安全认证（推荐启用）以及 802.1x 的接入协议（推荐使用标准协议即可）。如果使用 Portal 认证，则不选中“启用 802.1x 协议”复选框。
3. 单击“保存”按钮，保存所有的高级设置。

图2-32 TSM Agent 认证高级选项

步骤 5 单击“认证”按钮，客户端发起认证，如图 2-33 所示。

图2-33 TSM Agent 发起认证

如果认证通过，则系统托盘中的图标变成，表示终端用户成功通过身份认证和安全认证。用户可以正常访问网络。

说明

如果系统托盘中的图标为，表示终端用户已经通过安全认证，但是终端主机存在违规信息。如果系统托盘中的图标为，表示终端用户未通过安全认证，终端主机的网络访问受限。

----结束

注意

上述配置过程是以普通账号来进行举例的。在企业网络中，用户也可以通过 AD 域账号进行认证。如图 2-34 所示。

如果用户使用 AD 域账号登录，则需要注意以下几点：

- 需要另外部署域控制服务器，在域服务器上配置用户名和密码。有关于控制服务器的配置请按照相关产品的文档指导进行。
- TSM 服务器上只需要同步配置 AD 域用户账号。请参考“2.6.3 配置按 OU 方式同步 AD 域账号信息”。
- 用户终端需要加入域，详细配置请参考终端操作系统（例如 Windows）的帮助文档。

图2-34 使用 AD 域账号进行认证

2.8 配置举例

组网需求

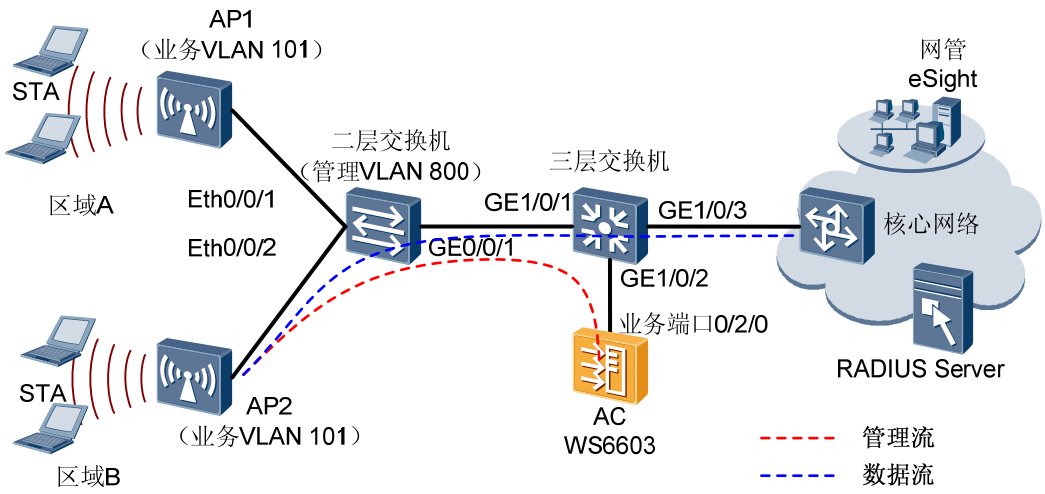
企业网络中为某两个相隔较远的区域（区域 A、区域 B）提供 WLAN 接入服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 使用 WS6603，采用“旁挂式”组网，如图 2-35 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2-35 独立 AC 旁挂组网图



说明

本举例中未包含 NAC 部分的配置。

数据准备

表2-6 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 800（由二层交换机打 VLAN tag）
AP Region	AP1：101
	AP2：102
ESS	• 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
	• 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）

配置项	数据
	STA3/STA4：VLAN 102（由 AC 下发）
二层交换机上 VLAN	• 接 AP1 端口（Eth0/0/1）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 101/800 通过 • 接 AP2 端口（Eth0/0/2）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 102/800 通过 • 接三层交换机端口（GE0/0/1)：Trunk 类型，允许 VLAN 101/102/800 通过
三层交换机上 VLAN	• 接二层交换机端口（GE1/1/1）：Trunk 类型，允许 VLAN 101/102/800 通过 • 接 AC 端口（GE1/1/2）：Trunk 类型，允许 VLAN800 通过 • 接上行网络端口（GE1/1/3）：Trunk 类型，允许 VLAN 101/102 通过
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址(Loopback 接口)	3.3.3.3/32
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）
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（Eth0/0/1 和 Eth0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800，分别允许 VLAN101/800 和 VLAN102/800 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相应的产品文档。

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 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 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. 配置二层交换机连接三层交换机的 GE 端口（GE0/0/1）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
[huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[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(GE0/1/1)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相应的产品文档。

```
[huawei] interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1] port link-type trunk
[huawei-GigabitEthernet1/0/1] port trunk allow-pass vlan 101
[huawei-GigabitEthernet1/0/1] port trunk allow-pass vlan 102
[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(GE0/1/2)透传管理 VLAN。

```
[huawei] interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2] port link-type trunk
[huawei-GigabitEthernet1/0/2] port trunk allow-pass vlan 800
[huawei-GigabitEthernet1/0/2] quit
```

5. 配置三层交换机连接上行网络的 GE 端口(GE0/1/3)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
[huawei-GigabitEthernet1/0/3] port trunk allow-pass vlan 102
[huawei-GigabitEthernet1/0/3] quit
```

6. 配置三层交换机的 DHCP Relay 功能。

```
[huawei] dhcp enable
[huawei] interface vlanif 800
[huawei-Vlanif800] ip address 192.168.1.1 255.255.255.0
```

```
[huawei-Vlanif800] dhcp select relay
[huawei-Vlanif800] dhcp relay server-ip 192.168.2.2
[huawei-Vlanif800] quit
```

7. VLANIF1 的 IP 地址为 192.168.2.1，作为连接 AC 的三层接口。

```
[huawei] interface vlanif 1
[huawei-Vlanif1] ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif1] quit
```

8. 配置三层交换机中继 DHCP 服务到 AC 上，AC 作为 DHCP 服务器。

```
[huawei] dhcp server group AC-srv1
[huawei-dhcp-server-group-AC-srv1] dhcp-server 0 3.3.3.3
[huawei-dhcp-server-group-AC-srv1] quit
```

9. 配置三层交换机到 AC 的路由。

说明

IP 地址 3.3.3.3 为 AC 的 Loopback 接口 IP 地址。

```
[huawei] ip route 3.3.3.3 255.255.255.255 192.168.2.2
```

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，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. 在 AC 上创建 VLANIF。

#VLANIF 1 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)# interface vlanif 1
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
```

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-vlanif1)# dhcps enable
huawei(config-if-vlanif1)# 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. 配置 Loopback 接口，作为 AC 的源 IP，用于 AP 和 AC 之间建立隧道通信。

说明

设置 Loopback 接口地址，必须使用 32 位掩码。

```
huawei(config)# interface loopback 0
huawei(config-if-loopback0)# ip address 3.3.3.3 255.255.255.255
huawei(config-if-loopback0)# quit
```

5. 设置 AC 的源 IP 地址。

#配置 Loopback 接口作为 AC 的源 IP 地址。

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 loopback 0
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 loopback0。

```
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 Option60 和 Option43 功能，通过 DHCP option43 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-3.3.3.3
huawei(config-ip-pool-ap-server)# quit
```

说明

- 配置 option60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option43 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. 配置 AC 到 192.168.1.0 网段的路由。

```
huawei(config)# ip route 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
15 SRG1201GW
------------------------------------------------------------------------------
Total number: 13
```

#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（typeid 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 AP Profile Region AP
ID Type ID ID 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，也可以为多个 AP 指定同一个射频。

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 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。

```
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 vlan101
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 vlan102
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

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
interface vlanif 1
ip address 192.168.2.2 255.255.255.0
dhcps enable
quit
nterface loopback 0
```

```
ip address 3.3.3.3 255.255.255.255
quit
wlan ac
wlan ac source interface loopback 0
quit
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
quit
option 60 string Huawei AP
option 43 string HuaweiAC-3.3.3.3
quit
ip route 192.168.1.0 255.255.255.0 192.168.2.1
wlan ac
ap-auth-mode sn-auth
quit
ap id 1 type-id 0 sn SN000001
ap id 2 type-id 0 sn SN000002
ap-region id 101
quit
ap-region id 102
quit
ap id 1
region-id 101
quit
ap id 2
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile name wmm-1
quit
radio ap-id 1 radio-id 0
bind radio-profile name radio-1
quit
radio ap-id 2 radio-id 0
bind radio-profile name radio-1
quit
security-profile name security-1 id 1
authentication policy wep
policy wep open-system
quit
traffic-profile name traffic-1 id 1
quit
ess name huawei-1 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess name huawei-1 mode region
vlan-mapping ess name huawei-1 type tag region 101 vlan 101
vlan-mapping ess name huawei-2 mode region
vlan-mapping ess name huawei-2 type tag region 102 vlan 102
forward-mode type ess
forward-mode ess 0 mode direct-forward
forward-mode ess 1 mode direct-forward
vap ap 1 radio 0 ess name huawei-1 wlan 1
```

```
vap ap 2 radio 0 ess name huawei-2 wlan 1
commit ap 1
commit ap 2
quit
```

3 集成 AC 方案部署

3.1 概述

3.1.1 方案简介

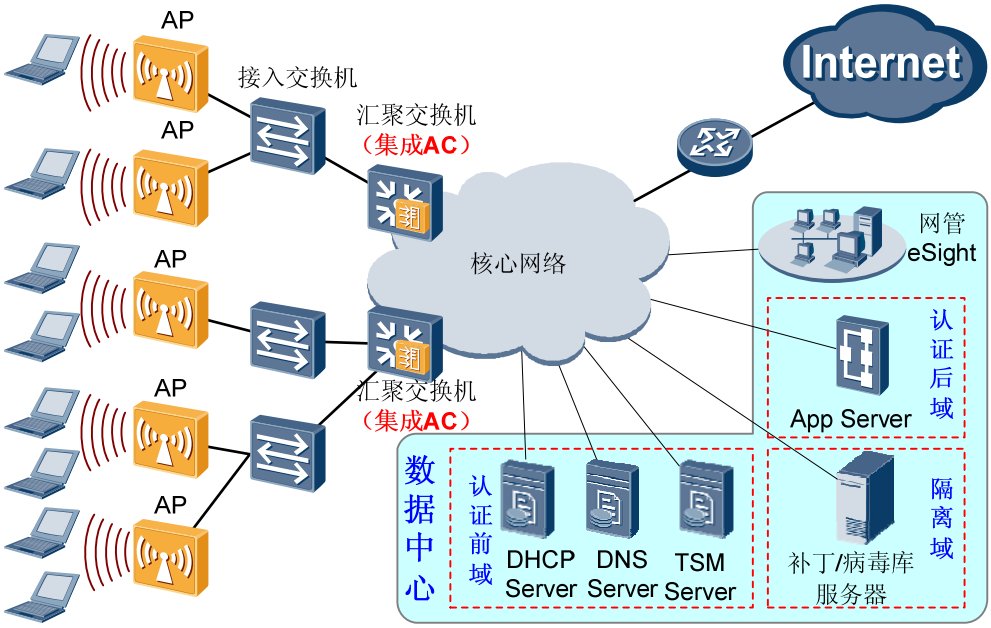
在 WLAN 部署中，最关键的部件包括 AP 和 AC。集成 AC 方案是指不采用单独的 AC 硬件设备，而是采用在交换机中集成的 AC 硬件插卡（例如 S9300 的 SPU 板），来实现对交换机下所有 AP 的管理。

集成 AC 方案可应用在集中式 AC 部署方案中，也可应用在分布式 AC 部署方案中。集成 AC 方案部署较为简便，价格相对低廉一些，但是性能方面与独立的 AC 设备相比略差。企业可以根据自身的实际情况进行选择。

3.1.2 典型组网

企业 WLAN 集成 AC 方案的典型组网如图 3-1 所示。

图3-1 集成 AC 方案典型组网图



在集成 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP（例如 WA603DN）来负责无线终端的接入。使用 S9300 集成的 SPU 板卡作为 AC，负责完成对 AP 设备的管理。

在用户的安全和管理方面，使用 TSM 来实现对用户的接入认证，并实现对于用户的网络权限的策略控制。例如未认证时或认证失败时只能访问认证前域；认证通过但是终端不安全只能访问隔离域；认证通过并且终端安全可以访问认证后域。

在网络管理方面，使用企业专业网管系统 eSight 来实现对于企业网络的管理。

3.1.3 配套产品和版本

表3-1 集成 AC 方案配套产品和版本

部件	产品	版本
AP	WA603SN WA603DN WA633SN WA653SN WA653DN WA653EN	V100R003C01
接入交换机	非特定，推荐 S2700/S3700 系列	非特定
汇聚交换机	S9300	V100R006C00
AC	S9300 SPU 插卡	V100R006C00
NAC 服务器	TSM	V100R002C06
网管服务器	eSight	V200R001C00
DHCP 服务器	非特定，可以是外置服务器，或者交换机内置的 DHCP 服务器，也可以使用 AC 内置的 DHCP 服务器	非特定
DNS 服务器	非特定	非特定

3.1.4 部署思路

前置任务

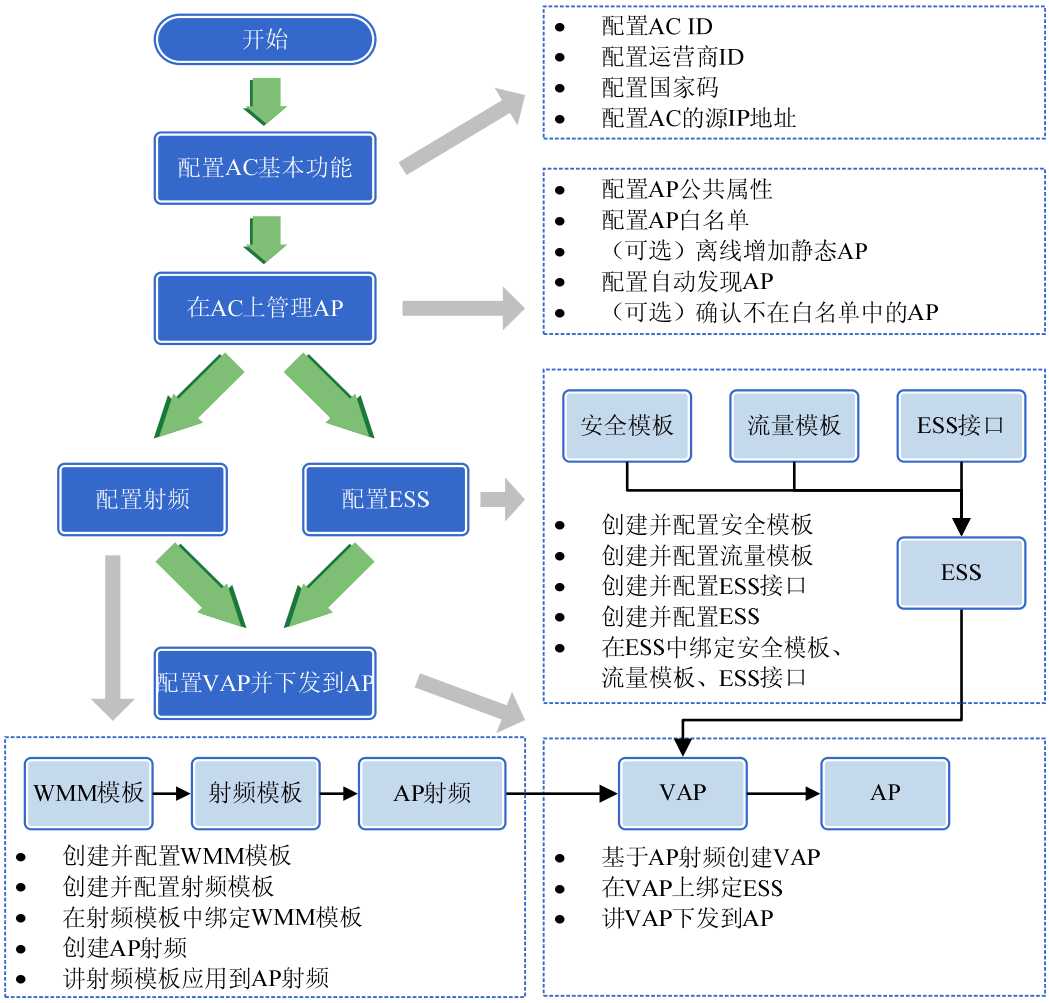
- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- TSM 服务器的操作系统和 TSM 软件已经安装完毕。
- eSight 网管服务器的操作系统和 eSight 软件安装完毕。
- 完成 VLAN/SSID、IP 地址等数据的规划。

配置思路

配置思路	配置注意事项
在各网元部件上配置接口、VLAN 和 IP 地址，实现网络的基础互通。	NA
配置 AP 发现 AC 的方式，包括以下两种： • AP 通过 DHCP 服务器返回的报文中的 Option 60 字段来得知 AC 的 IP 地址。 • AP 通过 DHCP 服务器返回的报文中的 Option 15 字段得知 AC 的 DNS 域名，然后向 DNS 服务器发送 DNS 解析请求来得知 AC 的 IP 地址。	• 第一种方式要求 DHCP 服务器上配置 Option 60 选项，内容为 AC 的 IP 地址。 • 第二种方式要求 DHCP 服务器上配置 Option 15 选项，内容为 AC 的 DNS 域名。同时配置 DNS 服务器，增加 AC 域名对应的 IP 地址。
配置 AC 对 AP 的管理，配置步骤如下： • 配置 AC 基本功能。 • 在 AC 上管理 AP。 • 配置 WLAN 射频。 • 配置 ESS。 • 配置 VAP 并下发到 AP。	详细的 AC 配置流程顺序、步骤详解和相互关系可以参见图 3-2。
（可选）在业务网关上配置 NAC 功能，实现对 WLAN 接入用户的认证和授权。	主要包括： • 配置 AAA 功能，设置用户的归属域、认证/授权的模式以及相应的 AAA 服务器等。 • 在用户接入的接口下配置 802.1x 或者 Portal 认证。
（可选）配置 TSM 服务器。主要配置包括： • 配置认证服务器（Portal 认证服务器或者 802.1x 认证服务器），用于对终端进行安全认证。 • 配置隔离域和认证后域的信息。 • 配置策略模板，并将策略下发到用户。 • 配置用户账号（包括普通账号、MAC 账号、AD 账号及 LDAP 账号等），为账号配置接入隔离域及后域，实现对用户的网络权限控制。	• DHCP 服务器、DNS 服务器、TSM 服务器属于认证前域。 • 用于安全修复的补丁服务器或者病毒库服务器则划分到隔离域。 • 其他的应用服务器属于认证后域。 • 如果是普通账号，则需要在 TSM 服务器上配置用户名和密码。 • 如果是 AD 域账号，则需要另外部署域控制服务器，并配置用户名和密码。然后将账号同步至 TSM 服务器。

配置思路	配置注意事项
配置移动终端，安装用于网络接入的客户端软件（例如 802.1x 拨号软件）。	• 对于 Portal 认证来说，一般不需要对终端进行特殊配置。（但某些系统可能也有 Portal 认证客户端）。 • 而对于 802.1x 认证来说，需要在客户端上安装并配置 802.1x 认证客户端。 • 如果使用 TSM 作为 NAC 的认证服务器，那么客户端需使用 TSM Agent（它自带 Portal 认证或 802.1x 认证客户端）。
（可选）使用 eSight 进行 WLAN 网络管理。	通过 eSight 软件，可以查看： • WLAN 的概览信息 • 所有 AC 状态和基本信息 • 指定 AC 的详细信息 • AC 的告警信息 • AC 的性能指标 详细配置请参见“4 WLAN 网络管理”。

图3-2 集成 AC 方案的 AC 配置流程图



3.2 配置网络互通

请参见“2.2 配置网络互通”。

3.3 配置 AP 发现 AC

3.3.1 概述

当 FIT AP 上线后，需要知道本 AP 所归属 AC 的 IP 地址，才能从 AC 获得相应的参数配置。AP 发现 AC 通常有三种方式：

- 广播方式

在这种方式下，AP 通过广播的方式向网络中所有的 AC 发起 CAPWAP 隧道连接，当有 AC 响应该 AP 后，CAPWAP 隧道建立。这种方式下，AP 发现 AC 是自主行为，在 AC 上无需进行任何配置。

- 通过 DHCP Option43 发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option43 选项，将 AC 的 IP 地址告知 AP。

- 通过 DHCP Option15 和 DNS 解析发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option15 选项，将 AC 的 DNS 域名告知 AP。

  AP 再向 DNS 服务器发起 AC 域名的解析请求，DNS 服务器返回响应报文，告知 AC 的 IP 地址。

3.3.2 配置 AP 通过 DHCP Option43 发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option43 选项。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者 AC 内置的 DHCP 服务器。

本节以 S9300 交换机内置的 DHCP 服务器（VLANIF 接口地址池）来举例说明配置过程，其他情况请参考相应产品的产品文档。

配置步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 功能。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

步骤 5 执行命令 **dhcp select interface**，配置设备采用接口地址池的 DHCP 服务器模式。

步骤 6 执行命令 **dhcp server option 43 sub-option 3 ascii** *X.X.X.X*，配置 DHCP Option43 选项。

----结束

3.3.3 配置 AP 通过 DHCP Option15 和 DNS 解析发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option15 选项。同时需要指定 DNS 服务器，用于对 AC 的域名进行解析。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者集成 AC（SPU 板）内置的 DHCP 服务器。

本节以 S9300 交换机内置的 DHCP 服务器（VLANIF 接口地址池）来举例说明配置过程，其他情况请参考相应产品的产品文档。

有关 DNS 服务器的部署和配置请参考相应产品的产品文档。

配置步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dhcp enable**，使能 DHCP 功能。

步骤 3 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。

步骤 4 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置 VLANIF 接口的 IP 地址。

步骤 5 执行命令 **dhcp select interface**，配置设备采用接口地址池的 DHCP 服务器模式。

步骤 6 执行命令 **dhcp server domain-name** *domain-name*，配置地址池的 DNS 域名。

说明

这里配置的域名即为 AC 的域名，在 DNS 服务器上需要配置该域名对应的 IP 地址为 AC 的 IP 地址。

步骤 7 执行命令 **dhcp server dns-list** *ip-address* &<1-8>，为 DHCP 客户端指定 DNS 服务器的 IP 地址。

----结束

3.4 配置 AC

3.4.1 配置 AC 基本功能

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan ac-global ac id** *ac-id* [**carrier id** { **cmcc** | **ctc** | **cuc** |**other** }]，配置 AC ID，同时可以配置 AC 的运营商标识。

在实际应用中，为了便于管理，用户需要为每个 AC 配置 AC ID 和运营商标识。

缺省情况下，AC ID 为 0，运营商标识为 **other**。

步骤 3 执行命令 **wlan ac-global country-code** *country-code*，配置 AC 的国家码标识。

步骤 4 执行命令 **wlan**，进入 WLAN 视图。

步骤 5 执行命令 **wlan ac source interface** { **LoopBack** *loopback-num* | **Vlanif** *vlan-id* }，配置 AC 的源地址。

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

----结束

3.4.2 在 AC 上管理 AP

配置 AP 公共属性

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap-license** *ap-license number*，配置允许接入 AC 的 AP 个数。

步骤 4 执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。

步骤 5 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式。

步骤 6 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置 AP 升级对应的升级文件。

- 当升级模式为 ac-mode 时，需要将 AP 升级文件上载到 AC 中。
- 当升级模式为 ftp-mode 时，执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftp-username* | **ftp-password** *ftp-password*] *，配置 FTP 服务器 IP、客户端用户名、密码。

----结束

配置 AP 白名单

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap-whitelist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加合法 AP 的 MAC 或者 SN 到白名单里，可以批量增加。

----结束

（可选）离线配置 AP

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap id** *ap-id* [{ **type-id** *type-id* | **ap-type** *ap-type* } { **mac** *ap-mac* | **sn***ap-sn* } *]，离线增加一个 AP。

步骤 4 （可选）执行命令 **region-id** *region-id*，将增加的 AP 加入指定域。

步骤 5 （可选）执行命令 **profile-id** *profile-id*，将增加的 AP 绑定指定 AP 模板。

步骤 6 （可选）执行命令 **ap-threshold** { **cpu-usage** | **memory-usage** } *threshold-value*，配置 AP 的 CPU 和内存的告警阈值。

步骤 7 （可选）执行命令 **ap-threshold temperature** *high-value* [*low-value*]，配置 AP 的温度告警阈值。

----结束

配置自动发现 AP

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。

步骤 4 执行命令 **ap-auth-mode** *auth-mode*，配置 AP 的认证方式（MAC、SN 或不检测）。

----结束

（可选）确认不在白名单中的 AP

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap-confirm** { **all** | { **mac** *ap-mac* | **sn** *ap-sn* } [**id** *ap-id*] }，对 AP 进行确认。

AP 确认成功后，其 MAC 或 SN 将自动加入白名单，此 AP 自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，AP 正常工作。

----结束

3.4.3 配置 WLAN 射频

配置 WMM 模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }*，配置 WMM 模板。

步骤 4 执行命令 **wmm enable**，使能 WMM 功能。

步骤 5 （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* }*，配置终端上四个 WMM 队列的 EDCA 参数。

步骤 6 （可选）执行命令 **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** } }*，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

配置射频模板并绑定 WMM 模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。

步骤 4 （可选）执行命令 **radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。

步骤 5 （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。

步骤 6 （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。

步骤 7 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }，为射频模板绑定 WMM 模板。只有绑定了 WMM 模板的射频模板才可以被射频绑定。

----结束

将射频模板应用到指定射频

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。

步骤 4 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }，为指定射频绑定射频模板。

----结束

（可选）配置 AP 射频资源管理

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。

步骤 4 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

步骤 5 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

步骤 6 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。

步骤 7 手工启动全局调优：

1. 执行命令 **quit**，返回 WLAN 视图。
2. 执行命令 **calibrate startup region** *region-id* [**listen-uncontrol-neighbor**]，启动指定域的全局调优。
3. 执行命令 **calibrate auto-startup region** *region-id* **time** *time* [**listen-uncontrol -neighbor**]，定时启动调优。

----结束

（可选）配置 AP 负载均衡

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **load-balance-group** { **name** *group-name* | **id** *group-id* }*，配置负载均衡组。

步骤 4 执行命令 **member ap-id** *ap-id* **radio-id** *radio-id*，向负载均衡组内添加射频。

步骤 5 配置负载均衡组的负载均衡模式：

- 执行命令 **traffic gap** *gap-threshold*，配置负载均衡组的负载均衡模式为流量模式。
- 执行命令 **session gap***gap-threshold*，配置负载均衡组的负载均衡模式为会话模式。缺省情况下，负载均衡组的负载均衡模式为会话模式。

步骤 6 执行命令 **associate-threshold** *associate-threshold*，配置负载均衡组的最大关联次数。

----结束

3.4.4 配置 ESS

配置 WLAN-ESS 接口

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface wlan-ess** *wlan-ess-number*，创建 WLAN-ESS 接口。

步骤 3 配置 WLAN-ESS 接口下接入用户的认证方式：

- 执行命令 **dot1x-authentication enable**，配置认证方式为 802.1x 认证。
- 执行命令 **mac-authentication enable**，配置认证方式为 MAC 认证。
- 执行命令 **web-authentication enable**，配置认证方式为 Portal 认证（Web 认证）。

步骤 4 如果采用 802.1x 认证，执行如下步骤：

1. 执行命令 **dot1x authentication-method** { **chap** | **pap** | **eap** }，配置 802.1x 认证方法。
2. （可选）执行命令 **dot1x guest-vlan** *vlan-id*，配置端口所在的 guest-vlan。
3. （可选）执行命令 **dot1x restrict-vlan** *vlan-id*，配置端口所在的 restrict-vlan。
4. （可选）执行命令 **dot1x authentication domain** *domain-name*，在接口上绑定域。

步骤 5（可选）执行命令 **port-isolate enable**，用于使能 AC 设备上的端口隔离功能。

----结束

配置安全模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* }*，配置安全模板。

步骤 4 配置安全策略：

- WEP 开放系统认证

- 执行命令**令 security-policy wep**，配置安全策略为 WEP 方式。
- 执行命令 **wep authentication-methodopen-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。

- WEP 共享密钥认证
  - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
  - 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
  - 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。
  - 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。
- WPA/WPA2 认证
  - 执行命令 **security-policy wpa**，配置安全策略为 WPA 方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 802.1x 认证方式和相应的加密方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
- WAPI 认证
  - 执行命令 **security-policyapi**，配置安全策略为 WAPI 方式。
  - 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。
  - 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file-name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
  - 执行命令 **wapi import private-key file-name** *file-name*，导入 AC 的私钥文件。
  - 执行命令 **wapi asuip** *ip-address*，配置 ASU 服务器的 IP 地址。

----结束

配置流量模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }*，配置流量模板。

步骤 4 （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。

步骤 5 （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，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 6 （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。

步骤 7 （可选）执行命令 **tunnel-priority up designate** { **tos** | **8021p** } *priority-value*，指定上行隧道优先级值。或者执行命令 **tunnel-priority up map** { **tos-tos** | **tos-8021p** | **8021p-tos** |

8021p-8021p } *value0 value1 value2 value3 value4 value5 value6 value7*，配置上行隧道优先级的映射关系。

----结束

配置 ESS 并绑定 WLAN-ESS 接口、安全模板和流量模板

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* }*，创建 ESS。

步骤 4 执行命令 **forward-mode** { **direct-forward** | **tunnel** }，配置 ESS 的数据转发模式。

步骤 5 （可选）执行命令 **type** { **ac-management** | **ap-management** | **service** }，配置 ESS 类型。

步骤 6 （可选）执行命令 **ssid** *ssid*，配置 ESS 的 SSID。

步骤 7 （可选）执行命令 **service-vlan**，配置 ESS 的 VLAN ID。

步骤 8 执行命令 **wlan-ess** *wlan-ess-number*，在 ESS 中绑定 WLAN-ESS 接口。

步骤 9 执行命令 **security-profile** { **name** *profile-name* | **id** *profile-id* }，在 ESS 中绑定安全模板。

步骤 10 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }，在 ESS 中绑定流量模板。

----结束

3.4.5 配置 VAP 并下发到 AP

配置 VAP 并绑定 ESS

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。

步骤 4 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } [**wlan** *wlan-id*]，在射频上绑定 ESS。

说明

也可以在 WLAN 视图下使用 **batch ap** { *ap-id* [**to** *ap-id*] } &<1-10> **radio** { *radio-id* [**to** *radio-id*] } &<1-10> **service-set** { *service-set-id* [**to** *service-set-id*] } &<1-10>命令批量配置 VAP。

----结束

将 VAP 下发到 AP

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

----结束

3.5 配置 NAC

请参见“2.5 配置 NAC”。

3.6 配置 TSM 服务器

请参见“2.6 配置 TSM 服务器”。

3.7 配置终端

请参见“2.7 配置终端”。

3.8 配置举例

组网需求

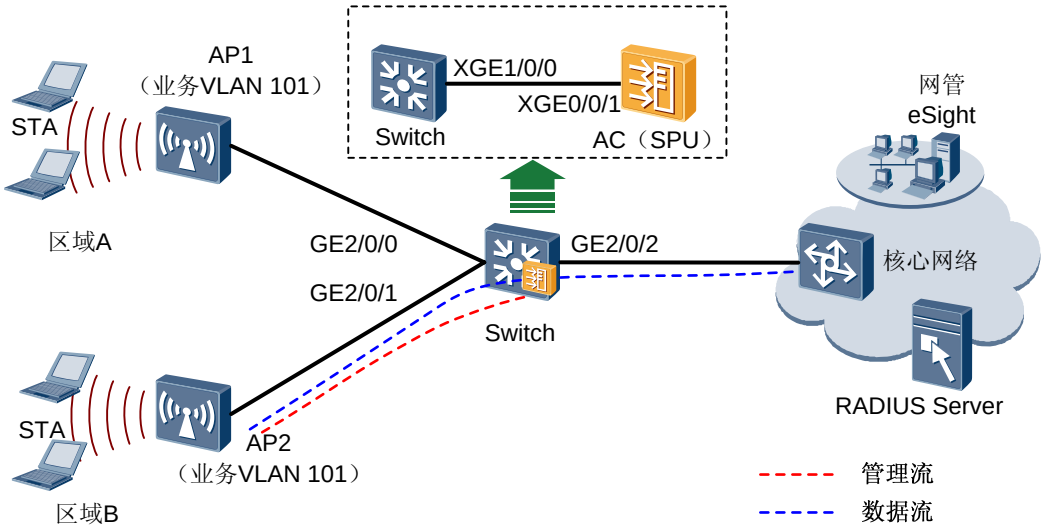
企业网络中为某两个相隔较远的区域（区域 A、区域 B）提供 WLAN 接入服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 使用 S9300 集成的 SPU 板，插在 S9300 的 1 槽位，如图 3-3 所示，由 AC 分配下发业务 VLAN，S9300 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3-3 集成 AC 组网图



说明

本举例中未包含 NAC 部分的配置。

数据准备

表3-2 数据规划表

配置项	数据
WLAN 服务	WEP，Open-system 认证模式，不加密
AP 管理 VLAN	VLAN 100（Switch 分配）
AP Region	AP1：101
	AP2：102
ESS	• 名称：huawei-1 • SSID：huawei-1 • WLAN 虚接口：WLAN-ESS 0 • 数据转发模式：隧道转发
	• 名称：huawei-2 • SSID：huawei-2 • WLAN 虚接口：WLAN-ESS 1 • 数据转发模式：隧道转发
WLAN 用户 VLAN	AP1：VLAN 101 AP2：VLAN 102
交换机 VLAN	VLAN 100/101/102

配置项	数据
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址	Vlanif 接口：192.168.0.1/24
AP 管理 IP 地址池	192.168.0.2～192.168.0.254/24
AP 网关	192.168.1.1/24（AC）
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址

配置思路

步骤 1 配置 Switch 和 AC，实现 AP 和 AC 互通。

步骤 2 配置 AC 的基本功能，包括配置 AC 运营商标识和 ID、AC 与 AP 之间通信的源接口，实现 AC 作为 DHCP Server 功能。

步骤 3 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。

步骤 4 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

其中配置 VAP，需要：

1. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
2. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。
3. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
4. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。

----结束

操作步骤

步骤 1 配置 Switch 和 AC，使 AP 和 AC 互通。

#配置 Switch 连接 AP 的以太网端口（GE2/0/0 和 GE2/0/1）类型为 trunk 类型，PVID 为 100。

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] interface GigabitEthernet 2/0/0
[Quidway-GigabitEthernet2/0/0] port link-type trunk
[Quidway-GigabitEthernet2/0/0] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/0] port trunk allow-pass vlan 100 101
[Quidway-GigabitEthernet2/0/0] quit
[Quidway] interface GigabitEthernet 2/0/1
[Quidway-GigabitEthernet2/0/1] port link-type trunk
[Quidway-GigabitEthernet2/0/1] port trunk pvid vlan 100
```

```
[Quidway-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 102
[Quidway-GigabitEthernet2/0/1] quit
```

#配置 Switch 上连接 AC 的 XGE 接口透传所有业务和管理 VLAN。

```
[Quidway] interface XGigabitEthernet 1/0/0
[Quidway-XGigabitEthernet1/0/0] port link-type trunk
[Quidway-XGigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 102
```

#配置 AC 上连接 Switch 的 XGE 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC
[AC] vlan batch 100 to 102
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[AC-XGigabitEthernet0/0/1] quit
```

步骤 2 配置 AC 的基本功能。

#配置 AC 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC] wlan ac-global ac id 1 carrier id  ctc
[AC] wlan ac-global country-code cn
```

#创建 VLANIF 接口，配置其 IP 地址作为数据转发的三层接口，使能 DHCP 服务功能。

Vlanif 100 为 AP 分配 IP 地址，Vlanif 101 为区域 A 的 STA 分配 IP 地址，Vlanif 102 为区域 B 的 STA 分配 IP 地址。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

说明

AP 需要获取一个 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 AC 为 DHCP 服务器，AP 从 AC 上获取 IP 地址。

#配置 AC 的源接口，用于 AP 和 AC 之间建立隧道通信。

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
[AC-wlan-view] quit
```

说明

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

步骤 3 配置 AP 并上线。

#配置 AP 的认证方式为“no-auth”。

```
[AC-wlan-view] ap-auth-mode no-auth
```

说明

如果 AP 认证模式为“no-auth”，上线 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。

#配置 AP 域 ID 分别为 101 和 102。

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```

#配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

步骤 4 配置 WLAN-ESS 虚接口。

```
[AC] interface wlan-ess 0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] quit
```

步骤 5 配置 AP 对应的射频。

#创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm-1 id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

#创建名为“radio-1”的射频模板，绑定 WMM 模板“wmm-1”。

```
[AC-wlan-view] radio-profile name radio-1
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[AC-wlan-radio-prof-radio-1] quit
```

#将 AP1 和 AP2 对应的射频绑定射频模板“radio-1”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] radio-profile name radio-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name radio-1
[AC-wlan-radio-1/0] quit
```

步骤 6 配置 AP 对应的服务集。

#创建安全模板。

安全模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
[AC-wlan-view] security-profile name security-1 id 1
[AC-wlan-sec-prof-security-1] wep authentication-method open-system
[AC-wlan-sec-prof-security-1] security-policy wep
[AC-wlan-sec-prof-security-1] quit
```

#配置 QoS 策略，创建流量模板。

流量模板名为“traffic-1”，参数采用缺省配置。

```
[AC-wlan-view] traffic-profile name traffic-1
[AC-wlan-traffic-prof-traffic-1] quit
```

#分别创建与 AP1 及 AP2 对应的服务集，并绑定流量模板及安全模板、WLAN-ESS 接口。

```
[AC-wlan-view] service-set name huawei-1
[AC-wlan-service-set-huawei-1] ssid huawei-1
[AC-wlan-service-set-huawei-1] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-1] wlan-ess 0
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] forward-mode tunnel
[AC-wlan-service-set-huawei-1] quit
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-2] wlan-ess 1
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] forward-mode tunnel
[AC-wlan-service-set-huawei-2] quit
```

配置 AP 对应的 VAP，下发 WLAN 服务。

#将 AP1 和 AP2 对应的射频绑定服务集“Huawei-1”和“Huawei-2”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] service-set name huawei-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
```

#下发 AP 的 WLAN 服务。

```
[AC-wlan-view] commit ap 0
[AC-wlan-view] commit ap 1
```

步骤 7 验证配置结果。

AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-1 和 huawei-2 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

----结束

配置文件

- AC 上的配置文件

```
#
 sysname AC
#
 vlan batch 100 to 102
#
 dhcp enable
#
 wlan ac-global carrier id ctc ac id 1
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
#
interface WLAN-ESS0
 port hybrid untagged vlan 101
#
interface WLAN-ESS1
 port hybrid untagged vlan 102
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 to 102
#
wlan
 wlan ac source interface Vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 0
 ap id 1
 wmm-profile name wmm-1 id 1
 traffic-profile name traffic-1 id 1
 security-profile name security-1 id 2
 service-set name huawei-1 id 3
  wlan-ess 0
  ssid huawei-1
  traffic-profile id 1
  service-vlan 101
  forward-mode tunnel
 service-set name huawei-2 id 4
  wlan-ess 1
  ssid huawei-2
  traffic-profile id 2
```

```
  service-vlan 102
  forward-mode tunnel
 radio-profile name radio-1 id 1
  wmm-profile id 1
 ap 0 radio 0
  radio-profile name radio-1
  service-set name huawei-1 wlan 1
 ap 1 radio 0
  radio-profile name radio-1
  service-set name huawei-2 wlan 2
#
return
```

- Switch 的配置文件

```
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 102
#
interface GigabitEthernet1/0/0
 port link-type trunk
 port trunk allow-pass vlan 100 to 102
#
```

4 WLAN 网络管理

4.1 概述

4.1.1 eSight 简介

eSight 应用平台是华为面向企业网管理推出的新一代面向企业园区和分支网络管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。eSight 应用平台支持对 IT&IP，以及第三方设备的统一管理，同时提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

在华为的企业 WLAN 部署方案中，推荐使用 eSight 应用平台实现对 WLAN 网络的管理。eSight 不仅可以实现对于 WLAN 业务的 AC、AP、STA 等节点和资源的监控，还可以实现对于 AC、AP 等节点和业务的配置。

4.1.2 典型组网

请参见“图 2-1 独立 AC 方案典型组网图”或者“图 3-1 集成 AC 方案典型组网图”。

4.1.3 配套产品和版本

表4-1 eSight 配套产品和版本

部件	产品	版本
网管服务器	eSight	V200R001C00
AP	WA603SN WA603DN WA633SN WA653SN WA653DN WA653EN	V100R003C01
AC	S9300 SPU 插卡	V100R006C00
	WS6603	V100R003C05

部件	产品	版本
接入交换机	非特定，推荐 S2700/S3700 系列	非特定
汇聚交换机	S9300	V100R006C00
NAC 服务器	TSM	V100R002C06
DHCP 服务器	非特定，可以是外置服务器，或者交换机内置的 DHCP 服务器，也可以使用 AC 内置的 DHCP 服务器	非特定
DNS 服务器	非特定	非特定

4.1.4 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- eSight 网管服务器的操作系统和 eSight 软件安装完毕。
- eSight 系统中已经添加了各设备网元。

配置思路

配置思路	配置注意事项
配置 WLAN 业务，主要步骤如下： • 创建并配置 AP • 配置 AP 域 • 配置 AP 模板、射频模板、ESS 模板 • 配置 AP 上线	• 配置 AP 域、AP 模板、射频模板、ESS 模板之间没有先后顺序关系。 • 配置的 AP 域、AP 模板、射频模板、ESS 模板将在配置 AP 上线中被引用或绑定。 • 配置 AP 上线包括：配置 AP 白名单、离线增加 AP、（自动发现 AP）、确认未授权的 AP。其中自动发现 AP 不需要配置。
监控 WLAN 业务。	通过 eSight 应用平台，可以： • 查看 WLAN 概要信息 • 查看 AC 信息 • 查看 AP 信息 • 查看 STA 信息 • 查看 SSID 信息 • 查看 Rogue AP 信息

4.2 配置 WLAN 业务

4.2.1 创建并配置 AC

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”。

步骤 3 在右侧的窗口中，单击“创建”，在“新建 AC”窗口中单击“选择”，在弹出窗口中选择 AC 设备，单击“确定”，新建 AC 设备。

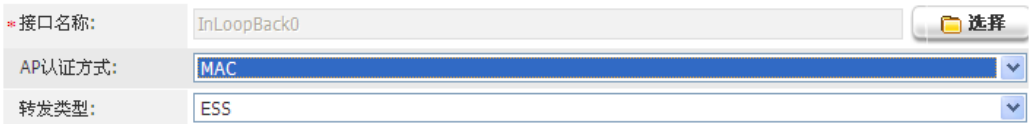
步骤 4 在“新建 AC”窗口中，单击“确定”，AC 创建成功。

步骤 5 单击设置 AC 的基本参数。

步骤 6 在“接口名称”后单击“选择”，选择相应接口，单击“确定”。

步骤 7 配置“AP 认证方式”和“转发类型”参数。如图 4-1 所示。

图4-1 配置 AC 基本参数



说明

当 AP 认证方式设置为“不认证”，AP 将自动上线。

当 AP 认证方式设置为“MAC”或“SN”时，用户需要手工导入 AP 设备、离线创建 AP、在白名单中增加 AP 的 MAC 或 SN、在未授权 AP 中对 AP 进行上线确认。

转发类型为 ESS 时，AP 以其绑定的 ESS 模板设置的用户数据转发模式转发用户数据。

转发类型为 AP 时，AP 以自己设置的用户数据转发模式转发用户数据。

----结束

4.2.2 配置 AP 域

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“WLAN 管理 > AP 域”。

步骤 4 单击“创建”，在弹出的窗口中设置 AP 域的相关参数。如图 4-2 所示。

图4-2 配置 AP 域

布放类型取值原则如下。

- 离散布放：域内 AP 的布放非常独立，AP 间信号无任何干扰，此时相当于一个 AP 就是一个域，如果为每个这样的 AP 都创建一个域，用户配置将非常繁琐，因此可以创建一个特殊的域来包含所有的这类 AP，这个域内的 AP 都不需要调优，每个射频都以最大发送功率工作即可。
- 普通布放：域内各 AP 之间分布比较稀疏，为满足基本的业务需求，每个射频的发送功率要求至少达到其最大发送功率的 50%。
- 密集布放：域内各 AP 之间分布比较密集，为满足基本的业务需求，每个射频的发送功率最小可以只达到其最大发送功率的 25%。

步骤 5 单击“确定”，新增 AP 域在列表中显示。

说明

可单击，修改 AP 域的相关参数。

可单击，将对应的 AP 域设置为默认 AP 域。

----结束

4.2.3 配置模板

通过配置 AP 模板、射频模板、和 ESS 模板并将这些模板与 AP 进行绑定，完成对 AP 的业务配置。

配置 AP 模板

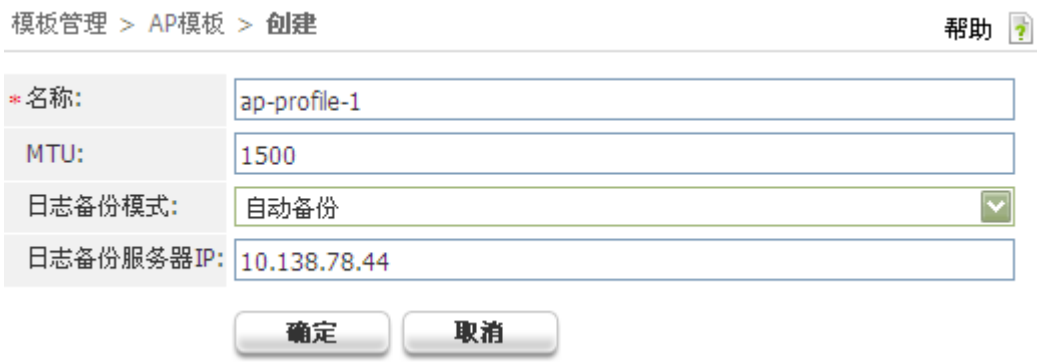
步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > AP 模板”。

步骤 4 单击“创建”，在弹出的窗口中设置 AP 模板的相关参数。如图 4-3 所示。

图4-3 配置 AP 模板



步骤 5 单击“确定”，新增 AP 模板在列表中显示。

说明

可单击，修改 AP 模板的相关参数。

----结束

配置射频模板

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > 射频模板”。

步骤 4 单击“创建”，在弹出的窗口中设置射频模板的相关参数。如图 4-4 所示。

图4-4 配置射频模板

步骤 5 单击“确定”，新增射频模板在列表中显示。

说明

可单击，修改射频模板的相关参数。

----结束

配置 ESS 模板

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“模板管理 > ESS 模板”。

步骤 4 单击“创建”，在弹出的窗口中设置 ESS 模板的相关参数。如图 4-5 所示。

图4-5 配置 ESS 模板

步骤 5 单击“确定”，新增 ESS 模板在列表中显示。

说明

可单击，修改 ESS 模板的相关参数。

----结束

4.2.4 配置 AP 上线

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“不认证”，或者 AP 的 MAC 或 SN 在已设置的“白名单”中，则该 AP 可以自动添加并上线。
- 如果 AP 设备不存在于白名单或 AP 列表中，且其认证模式非“不认证”情况下，则该 AP 设备存在于未认证 AP 列表之中。可通过确认未认证 AP 列表中的 AP 设备方式添加 AP 设备。

配置 AP 白名单

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“WLAN 管理 > AP 白名单”。

步骤 4 单击“创建”，在弹出的窗口中设置 AP 白名单的相关参数。如图 4-6 所示。

图4-6 配置 AP 白名单

步骤 5 单击“确定”，新增 AP 白名单在列表中显示。

----结束

离线增加 AP

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“WLAN 管理 > AP”。

步骤 4 单击“创建”，在弹出的窗口中设置 AP 的相关参数。如图 4-7 所示。

图4-7 离线增加 AP

步骤 5 单击“AP 域”的“选择”按钮，选择 AP 所属的域。

步骤 6 单击“AP 模板”的“选择”按钮，为 AP 绑定 AP 模板。

步骤 7 单击“射频模板”的“绑定”按钮，为 AP 绑定射频模板。

步骤 8 单击“ESS 模板”的“绑定”按钮，为 AP 绑定 ESS 模板。

步骤 9 单击“确定”，完成离线 AP 的创建。

----结束

确认未授权 AP

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。

步骤 3 在左侧的导航树中选择“WLAN 管理 > 未授权 AP”。

步骤 4 单击“同步”，同步所有 AP 的数据。

步骤 5 如果有未授权的 AP，单击“上线确认”。

图4-8 确认未授权 AP

----结束

4.3 监控 WLAN 业务

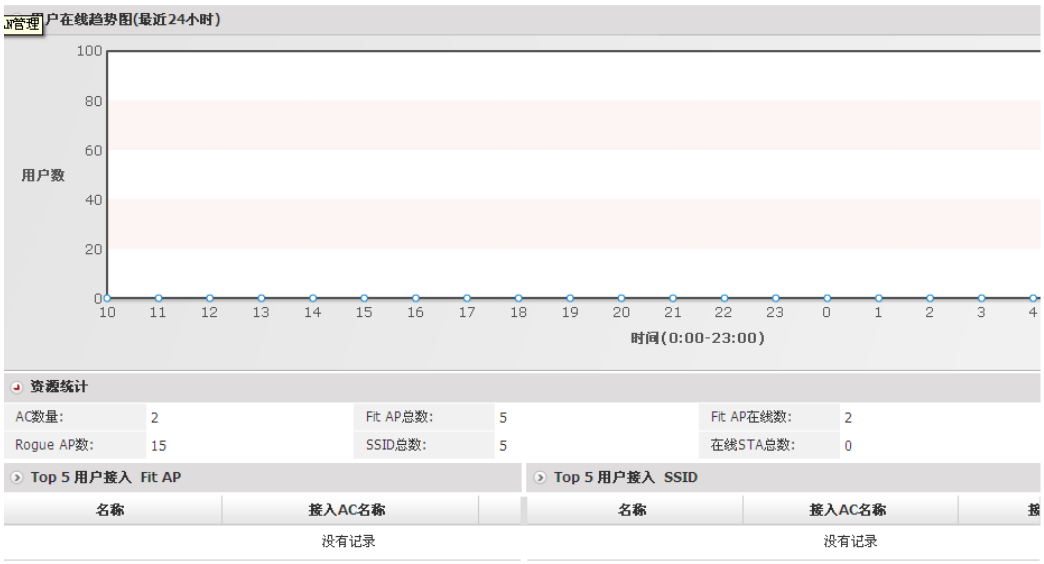
4.3.1 查看 WLAN 概要信息

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“概览信息 > 概览信息”，在右侧的窗口中可以看到 WLAN 的概要信息，如图 4-9 所示。包括：

- 用户在线趋势图（最近 24 小时）
- 资源统计（AC 数量、Fit AP 总数、Fit AP 在线数、Rogue AP 数、SSID 总数、在线 STA 总数）
- Top 5 用户接入 Fit AP
- Top 5 用户接入 SSID
- Top 5 告警设备

图4-9 查看 WLAN 概要信息



----结束

4.3.2 查看 AC 信息

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中可以看到所有 AC 概要信息，如图 4-10 所示。

图4-10 查看 AC 概要信息

步骤 3 单击某个 AC 的名称，可以查看指定 AC 的详细信息，如图 4-11 所示。

图4-11 查看 AC 详细信息

----结束

4.3.3 查看 AP 信息

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > Fit AP”，在右侧的窗口中可以看到所有 AP 概要信息，如图 4-12 所示。

图4-12 查看 AP 概要信息

步骤 3 单击某个 AP 的名称，可以查看指定 AP 的详细信息，如图 4-13 所示。

图4-13 查看 AP 详细信息

----结束

4.3.4 查看 STA 信息

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > STA”，在右侧的窗口中可以看到所有 STA 信息，如图 4-14 所示。

图4-14 查看 STA 信息

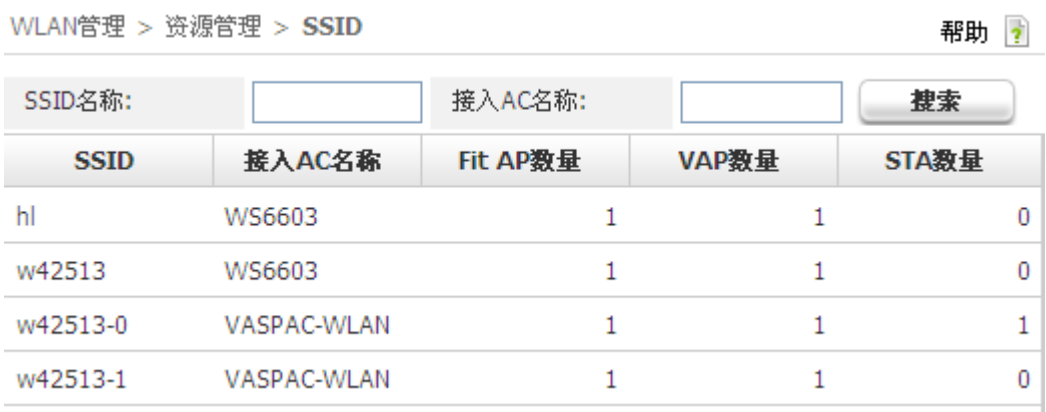
----结束

4.3.5 查看 SSID 信息

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 > SSID”，在右侧的窗口中可以看到所有 SSID 信息，如图 4-15 所示。

图4-15 查看 SSID 信息



----结束

4.3.6 查看 Rogue AP 信息

Rogue AP 即非法 AP，是未授权加入无线网络的接入点，或不具有正确安全配置的接入点。非法 AP 可以允许非授权的网络访问，造成无线终端在不知情的情况下错误地接入到非法 AP，从而造成网络资源的浪费。

步骤 1 在主菜单中选择“网络应用 > WLAN 管理”。

步骤 2 在左侧的导航树中选择“资源管理 ＞Rogue AP”，在右侧的窗口中可以看到所有 Rogue AP 信息，如图 4-16 所示。部分信息解释如下：

- BSSID：非法 AP 的 MAC 地址。
- 信道：接入点之间通过无线频道通信。当在同一区域中有多个接入点时，相邻接入点设置的信道输至少要间隔 5 个信道，以避免互相干扰。
- RSSI：（Received Signal Strength Indicator）接收信号强度指示。

图4-16 查看 Rogue AP 信息

ID	BSSID	信道	RSSI(dbm)	邻居AP名称	接入AC名称
0	28-6E-D4-31-95-00	6	-0.01	ap-1	VASPAC-WLAN
1	28-6E-D4-27-0D-E1	6	-0.01	ap-1	VASPAC-WLAN
2	28-6E-D4-27-0D-E2	6	-0.01	ap-1	VASPAC-WLAN
3	28-6E-D4-2B-23-60	6	-0.01	ap-1	VASPAC-WLAN
4	28-6E-D4-27-0D-60	6	-0.01	ap-1	VASPAC-WLAN
5	28-6E-D4-27-0D-E0	6	-0.01	ap-1	VASPAC-WLAN
6	02-04-18-03-00-80	6	-0.01	ap-1	VASPAC-WLAN
7	28-6E-D4-31-95-0F	6	-0.01	ap-1	VASPAC-WLAN
8	5C-4C-A9-00-67-E0	6	-0.01	ap-1	VASPAC-WLAN
9	5C-4C-A9-00-67-EF	6	-0.01	ap-1	VASPAC-WLAN
10	02-04-18-03-01-00	6	-0.01	ap-1	VASPAC-WLAN
11	28-6E-D4-31-93-F0	6	-0.01	ap-1	VASPAC-WLAN
12	28-6E-D4-31-93-FF	6	-0.01	ap-1	VASPAC-WLAN
13	28-6E-D4-2B-23-6F	6	-0.01	ap-1	VASPAC-WLAN
14	28-6E-D4-31-A2-41	11	-0.01	ap-1	VASPAC-WLAN

----结束