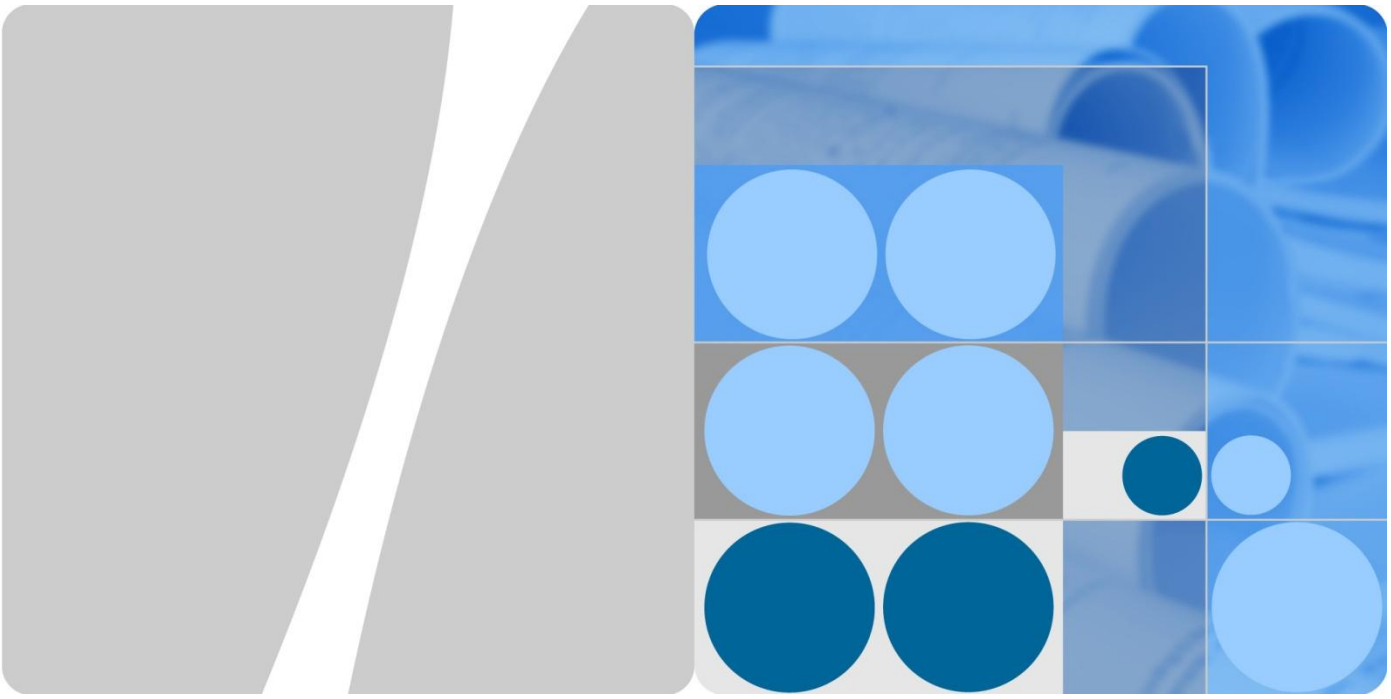


ONE NET Campus 园区 WLAN 方案 V100R001C02

技术建议书

文档版本 02

发布日期 2012-08-30

华为技术有限公司

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、复制本文档内容的部分或全部，并不得以任何形式传播。

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暗示的声明或保证。

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://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 400-822-9999

目 录

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

1 WLAN 方案概述

1.1 方案背景

1.1.1 技术背景

WLAN（Wireless Local Area Network）是指利用高频射频信号（例如 2.4GHz 或 5GHz）作为传输信道的无线局域网。

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 标准的有时也被称为 Wi-Fi 标准。而 802.11n 标准兼容 802.11a/b/g，带宽优势明显，已经成为当前的主流技术。随着 802.11ac 技术的出现，必将引领无线业务进入千兆时代，为用户带来千兆级别的接入速度。

表1-1 802.11 标准简介

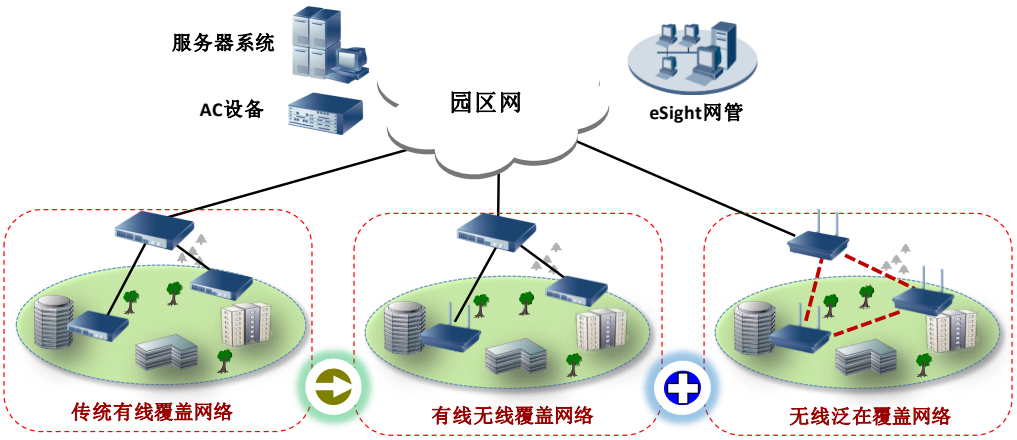
标准名称	发布时间	工作频率	理论速率	实际速率	备注
802.11b	1999	2.4GHz	11Mbps	6Mbps	早期标准
802.11a	1999	5.0GHz	54Mbps	22Mbps	应用很少
802.11g	2003	2.4GHz	54Mbps	22Mbps	早期标准
802.11n	2009	2.4/5.0GHz	150Mbps	75Mbps	结合 MIMO 技术，理论速率 600Mbps
802.11ac	2012	5.0GHz	1Gbps	400～500Mbps	802.11n 下一代标准
802.11ad	发展中	60GHz	7Gbps	发展中	面向家庭高清娱乐设备

版权所有 © 华为技术有限公司

1.1.2 企业无线园区网的发展及设计需求

随着技术的发展和大量移动终端的出现，企业园区也从最初的有线覆盖网络形式历经有线无线覆盖网络到现在的无线泛在覆盖网络形式。

图1-1 企业园区网的无线化发展示意图



由于无线网络覆盖场所的多样性、用户上网行为的复杂性、企业对于网络安全和网络质量的需求，需要在进行 WLAN 网络规划考时考虑以下方面：WLAN 网络的通信质量、网络安全、可靠性、统一管理以及部分行业对无线用户接入认证、授权、计费的需求。

1.2 WLAN 基本概念

1.2.1 网络架构模型

WLAN 网络在部署过程中，根据不同的需求有多种实现形式，根据网络架构分为：

- 自治式架构（即 FAT AP 或胖 AP 架构）
- 集中式架构（即 FIT AP 或瘦 AP 架构）

自治式架构和集中式架构两种网络结构比较如表 1-2 所示。

表1-2 自治式架构和集中式架构比较表

项目	自治式架构	集中式架构
适用场景	微型企业、个人	新生方式，增强管理，适用于大、中、小型企业
安全性	传统加密、认证方式，普通安全性	在传统认证方式的基础上增加基于用户位置的安全策略，高安全性

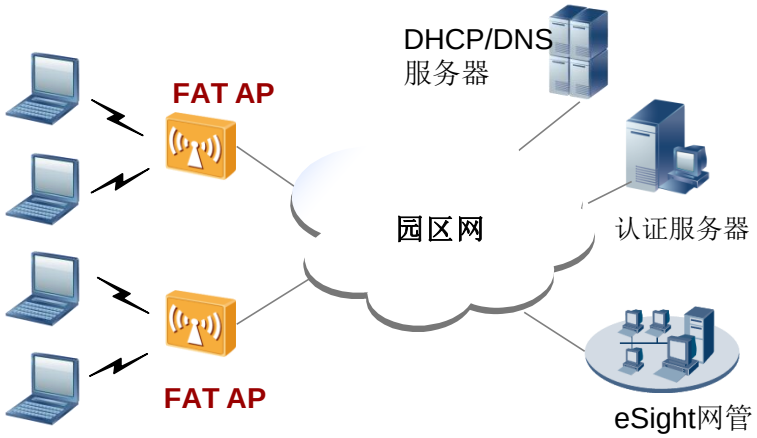
版权所有 © 华为技术有限公司

项目	自治式架构	集中式架构
网络管理	各 AP 都要加载配置文件	AC 上统一配置，AP 本身零配置，维护简单
用户管理	类似有线，根据 AP 接入的有线端口区分权限	虚拟专用组方式，根据用户名区分权限，使用灵活
WLAN 组网规模	L2 漫游，适合小规模组网	L2、L3 漫游，拓扑无关性，适合大规模组网
增值业务能力	实现简单数据接入	可扩展丰富业务

自治式架构

该架构下 AP 实现所有无线接入功能，不需要 AC 设备形态，如图 1-2 所示。

图1-2 WLAN 自治式架构图



WLAN 早期广泛采用自治式架构，随着企业大量部署 AP 后，对这些 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。

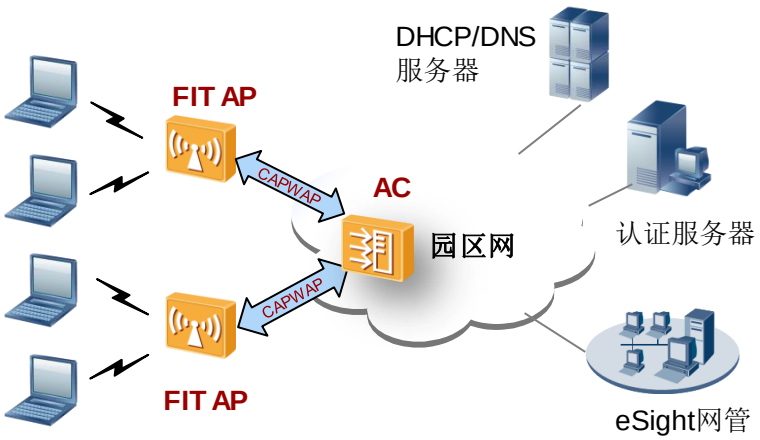
集中式架构

该架构通过无线控制器（AC）集中管理、控制多个 AP，如图 1-3 所示。所有无线接入功能由 AP 和 AC 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（Intrusion Detection Systems）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。

版权所有 © 华为技术有限公司

图1-3 WLAN 集中式架构图



AP 和 AC 间采用 CAPWAP 隧道协议进行通讯，AC 与 AP 间可以是直连或者穿越 Layer 2、Layer 3 网络。

CAPWAP 协议是基于 UDP 的应用层协议，协议传递的信息分为两类：控制信息和数据信息。

- 控制信息负责 AC 与 AP 之间的交互操作，包括 AP 自动发现 AC、AC 对 AP 进行安全认证、AP 从 AC 获取软件版本、AP 从 AC 获取配置等。
- 数据信息是封装后转发的无线数据。

两类信息分别使用不同的 UDP 端口号。CAPWAP 信息在 AP 与 AC 间交互时可以使用 DTLS 加密机制，保证通信的安全性。

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、集中认证和实施安全策略。此种方案为目前企业网通用方案。

在集中式网络架构下，又有如下划分：

- 根据 AC 部署方式，分为集中式和分布式
- 根据 AC 部署位置，分为旁挂和直路
- 根据 AC 硬件体现形式，分为集成 AC 和独立 AC
- 根据业务转发形式，分为本地转发和集中转发

1.2.2 集中式 AC 与分布式 AC

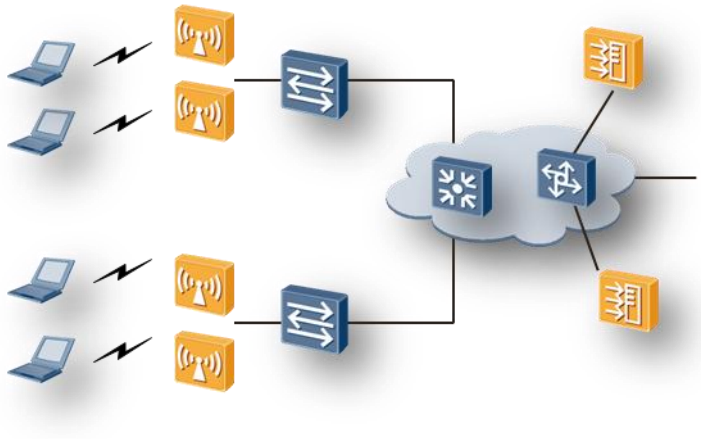
根据 AC 的部署方式，网络可分为集中式 AC 部署和分布式 AC 部署。

集中式 AC 部署

集中式 AC 部署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）。

华为专有和保密信息
版权所有 © 华为技术有限公司

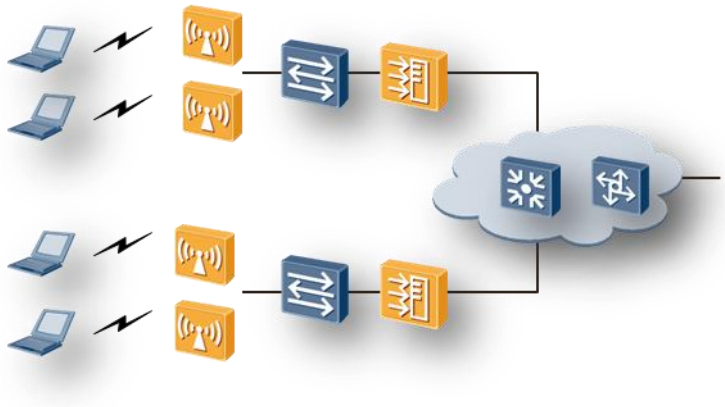
图1-4 集中式 AC 部署示意图



分布式 AC 部署

分布式 AC 部署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。

图1-5 分布式 AC 部署示意图



AC 的两种部署方式的优劣势对比如表 1-3 所示。

华为专有和保密信息
版权所有 © 华为技术有限公司

表1-3 集中式 AC 与分布式 AC 优缺点对比表

AC 部署方式	优点	缺点
集中式	• 节省投资 • 容量管理更简单有效，成本效益高 • 无线业务终结点少，便于管理 • 漫游部署简单、高效 • 无线网络运维管理更简单，可集中管理且配置灵活	AC 与 AP 之间的网络结构复杂，网络规划部署相对复杂
分布式	AC 与 AP 之间网络结构简单，网络部署相对简单	• 投资成本高 • 需要部署 AC 间漫游（除非各 AC 所在的区域间不考虑漫游） • 运维成本高

1.2.3 AC 旁挂与 AC 直路

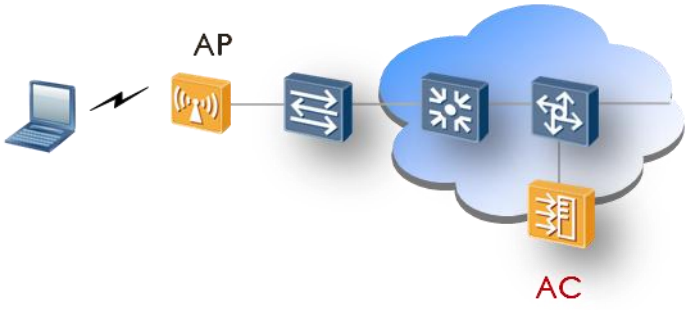
根据 AC 在网络上所处位置，可分为 AC 旁挂和 AC 直路。

旁挂

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。

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，目前主要用于网络改造、或者新建大、中型园区网络场景。

图1-6 AC 旁挂示意图



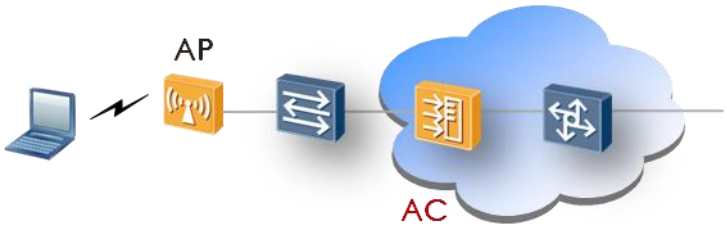
直路

直路方式是指将 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。

版权所有 © 华为技术有限公司

直路方式主要用于新建中、小型园区网络或原有网络汇聚/核心设备为华为设备的场景。

图1-7 AC 直路示意图



1.2.4 集成 AC 与独立 AC

根据 AC 硬件体现形式，可分为集成 AC 与独立 AC。

集成 AC

集成 AC 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，来实现对交换机下所有 AP 的管理。

独立 AC

独立 AC 方案是指采用单独的 AC 硬件设备，通过直路或者旁挂方式实现对于所有 AP 的管理。

集成 AC 和独立 AC 优缺点比较如表 1-4 所示。

表1-4 集成 AC 和独立 AC 优缺点比较表

AC 硬件形式	优点	缺点
集成 AC	部署简便，价格较低。	接入用户数少。
独立 AC	可以实现大容量、高性能的 WLAN 网络部署。	价格较高，成本高。

1.2.5 本地转发与集中转发

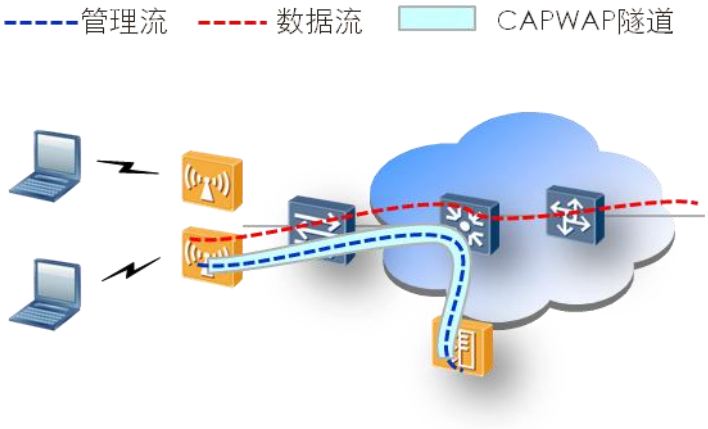
转发模式决定了 AP 针对用户数据采用不同的转发处理方式。

本地转发

又称直接转发，是指 AP 上对用户数据由本地转发到网络上层，不经过 AC 处理，AC 只对 AP 进行管理。而 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止。

版权所有 © 华为技术有限公司

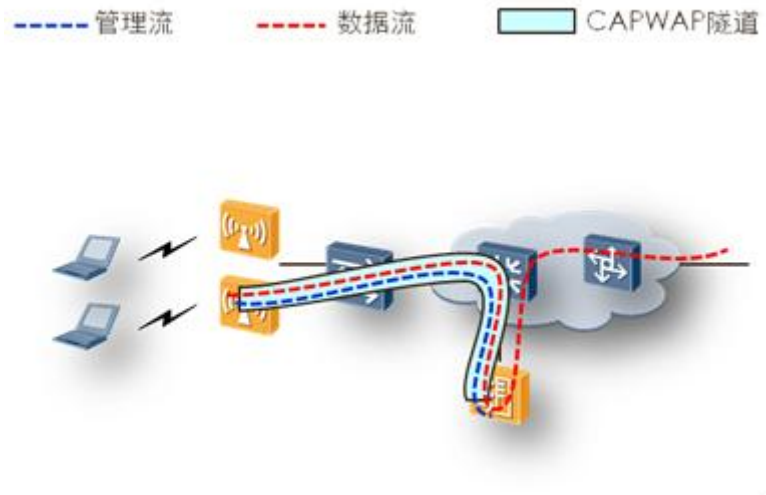
图1-8 本地转发示意图



集中转发

也称隧道转发。业务数据报文由 AP 统一封装后到达 AC 实现转发，AC 不但对 AP 进行管理，还作为 AP 流量的转发中枢。即 AP 管理流与数据流都封装在 CAPWAP 隧道中到达 AC。

图1-9 隧道转发示意图



本地转发与集中转发优缺点对比如表 1-5 所示。

版权所有 © 华为技术有限公司

表1-5 本地转发与集中转发优缺点对比表

转发方式	优点	缺点
本地转发	设备部署简单，数据流量不经过 AC，AC 负担小。	-
集中转发	数据流量和管理流量全部经过 AC，可以按用户需求规划安全监管策略。	AC 设备数据压力较大，对 AC 设备本身处理能力要求较高。

版权所有 © 华为技术有限公司

2 WLAN 基础网络规划

2.1 IP 地址规划

AC 的 IP 地址

AC 用于管理 AP，IP 地址一般通过静态手工配置。

AP 的 IP 地址

AP 的 IP 地址分配如果采用静态分配，由于 AP 数量较多，手动配置 IP 地址工作量大且容易出错，建议采用 DHCP 动态给 AP 分配 IP 地址。

DHCP 动态分配 AP 的 IP 地址时，可以有以下几种方式：

- 指定地址池分配
  - 根据 DHCP Option 60 表明 AP 身份而分配指定地址池的 IP：

    AP 的 DHCP Discover 报文携带 Option 60，例如内容为“Huawei AP”，表示请求分配 IP 地址的设备是华为 AP，而不是 WLAN 用户。DHCP Server 可以通过匹配或部分匹配 Option 60 字符串，来为 AP 从指定地址池中分配地址。

    如果网络中部署多个 DHCP Server 且只有部分支持 Option 60，交换机等设备充当 DHCP Relay 时需要支持识别 DHCP option 60 并将 DHCP 报文转发到相应的 DHCP Server 上。
  - 根据 VLAN 分配指定地址池的 IP：

    AP 相连交换机端口以 Trunk 方式加入 VLAN，允许通过的 VLAN 对应的地址池为 AP 分配 IP 地址。
  - 根据 AP 的 MAC 地址指定分配：

    在 DHCP Server 上配置 AP 的 MAC 以及对应的 IP 地址。
- 统一分配

  AP 的 IP 地址分配同 WLAN 用户一样，由 DHCP Server 统一分配，不再区别。

DHCP 动态分配 AP 的 IP 地址各种方式优劣势对比如表 2-1 所示。

版权所有 © 华为技术有限公司

表2-1 DHCP 动态分配 AP 的 IP 地址各种方式优劣势表

IP 地址分配方式		优势	劣势	适用场景
指定地址池分配	DHCP Option 60	AP 设备与无线用户的 IP 地址分离	需要交换机配套支持	对设备 IP 地址管理与用户 IP 地址管理要求隔离的
	根据 VLAN	AP 设备与无线用户的 IP 地址分离	网络配置工作量较大，不利于 AP 即插即用	对设备 IP 地址管理与用户 IP 地址管理要求隔离的
	根据 MAC	AP 设备与无线用户的 IP 地址分离	配置工作量较大，IP 地址管理难度加大	对少量 AP 设备管理有特殊要求的
统一分配		网络配置简单	-	对 AP IP 管理没有要求

无线终端/用户的 IP 地址

移动用户通过 DHCP 动态分配 IP 地址，不建议静态配置；对于基本不移动的无线终端（比如：无线打印机）可以静态配置。

2.2 SSID 规划

企业园区无线网络一般按照业务类型划分不同的 SSID（Service Set Identification）。

SSID 映射以太网中的 VLAN

通常，以太网中管理 VLAN 和业务 VLAN 分离。业务 VLAN 主要用于区分不同的业务类型或用户群体。

在 WLAN 网络中 SSID 也同样可以承担相应的工作。因此，在业务 VLAN 的规划中必须综合考虑 VLAN 与 SSID 的映射关系。业务 VLAN 应根据实际业务需要与 SSID 匹配映射关系，映射关系有 1:1、1:N、N:1、N:N 四种，AC 设备终结 VLAN 部署。

VAP 构建

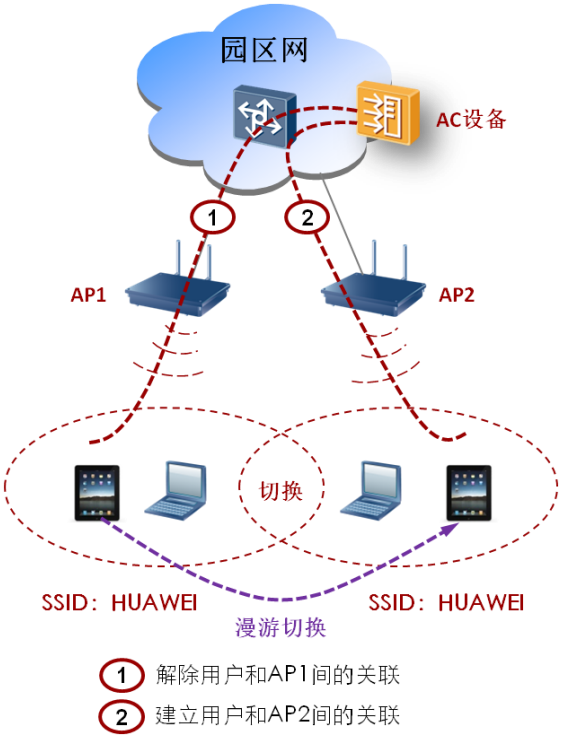
AP 可以配置多个 SSID，华为单频 AP 可支持 16 个 SSID，双频 AP 可支持 32 个 SSID。通过配置多个 SSID，可以将一个 AP 划分为多个 VAP（Virtual Access Point），每一个 SSID 对应一个 VAP，AC 针对 VAP 进行策略下发，VAP 根据策略进行终端与业务管理。

版权所有 © 华为技术有限公司

2.3 漫游规划

漫游是指用户在部署了 WLAN 网络的场所移动时，用户终端可以从一个 AP 的覆盖范围移动到另一个 AP 的覆盖范围，用户无需重新登录和认证。

图2-1 用户漫游切换示意图



如上图所示，假设终端与 AP1 已经建立关联信息，随着用户位置的移动，终端切换到 AP2，具体切换流程如下：

1. 客户端在各种信道中发送 802.11 请求帧。AP2 在信道 6（AP2 使用的信道）中收到请求后，通过在信道 6 中发送应答来进行响应。客户端收到应答后，对其进行评估，确定同哪个 AP 关联最合适。
2. 如图中的标号 1 所示，客户端通过信道 1（AP1 使用的信道）向 AP1 发送 802.11 解除关联信息，解除用户与 AP1 间的关联。
3. 如图中的标号 2 所示，客户端通过信道 6（AP2 使用的信道）向 AP2 发送关联请求，AP2 使用关联响应做出应答，建立用户与 AP2 间的关联。

WLAN 网络漫游中需注意以下两点：

- 漫游切换需要保证 SSID 相同，即两台 AP 切换区域需要配置相同的 SSID。
- 漫游切换 AP 必须是同一个 AC 管理。

版权所有 © 华为技术有限公司

2.4 AP 发现并选择 AC 方式规划

FIT AP 架构下的 WLAN 网络中，FIT AP 为零配置，当 FIT AP 部署到网络的时候，AP 需要去找到相应的 AC，并从 AC 上下载其配置。

AP 发现 AC 的机制有如下几种。

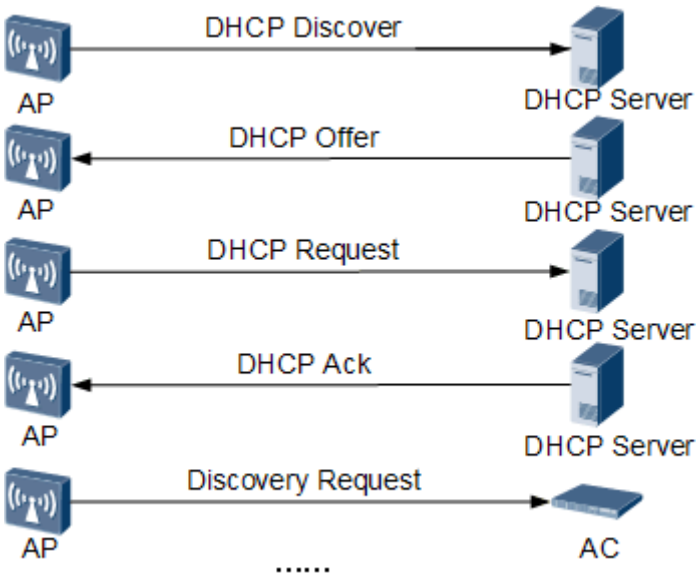
二层广播发现 AC

当 AC 和 AP 同在一个二层的网络中时，可以通过二层广播方式直接发现 AC。

通过 DHCP Option 43 发现 AC

Option 43 是 DHCP 协议的一个属性，携带 AC 的 IP 地址。当 DHCP Server 配置了 Option 43 后，它给 AP 分配 IP 时，在 DHCP Offer 报文中同时会将此属性告知 AP。

图2-2 通过 DHCP Option 43 发现 AC 的报文交互图

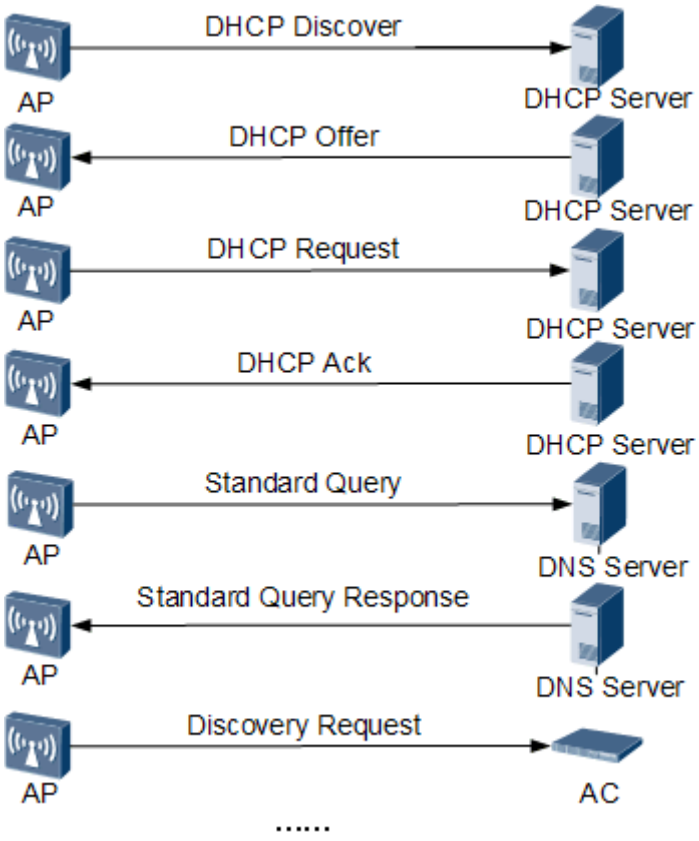


通过 DNS 发现 AC

当网络中部署了 DNS Server 时，还可以通过 DNS 方式让 AP 来发现 AC。需要在 DHCP Server 上配置 DNS Server IP 地址以及 AC 的域名。当 AP 通过 DHCP Server 获取 IP 地址时，DHCP Server 会在 DHCP Offer 报文中将 DNS 服务器 IP 地址（Option 6）和 AC 域名（Option 15）告知 AP，在 AP 获取到 IP 地址后，则通过 DNS Server 解析到 AC 的 IP，从而实现对 AC 的发现和关联。

版权所有 © 华为技术有限公司

图2-3 通过 DNS 发现 AC 的报文交互图



AP 上预配置 AC 列表

AP 可以预配置 AC 的 IP 地址列表。当预配置好 AC 列表时，AP 将不再启动正常的 L2 或 L3 的发现过程，故 AC 列表里的地址不可达时，AP 将永远连接不上 AC。

上述几种方式优劣势对比如下表所示。

表2-2 AP 发现并选择 AC 方式优劣势对比表

方式	部署要求	优势	劣势	适用网络
DHCP Option 43	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
DNS	部署 DNS Server；DHCP Server 支持 Option 15 属性			
二层广播发现	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

版权所有 © 华为技术有限公司

方式	部署要求	优势	劣势	适用网络
AP 上预配置静态 AC 列表	AP 预配置	对已有网络没有额外要求	需要对 AP 逐一进行配置，工作量大；若 AC 的 IP 地址发生变化，则需要重新修改 AP 的配置	小型 WLAN 网络

若无线网络部署了多个无线控制器，AP 通过上述某种方式发现了多个 AC 时，AP 根据 AC 负载动态选择接入到负载轻的 AC。

2.5 射频管理规划

与 IP 地址规划一样，WLAN 信道是 WLAN 网络设计中的重要一环，大型无线园区网网络必须对 WLAN 信道进行统一规划。

WLAN 信道规划的好坏，影响到无线网络的带宽、无线网络的性能、无线网络的扩展以及无线网络的抗干扰能力，也必将影响到无线网络的用户体验。

射频信道划分

WLAN 系统主要应用两个频段：2.4GHz 和 5.0GHz。

- 2.4GHz 频段信道划分：
  - 2.4G 频段具体频率范围为 2.4GHz～2.4835GHz 的连续频谱，信道编号 1～14。
  - HT20 信道划分：信道带宽为 20MHz，一般选取 1、6、11 三个不重叠信道，频率规划可用频点只有 3 个。
  - HT40 信道划分：信道带宽为 40MHz，受频率限制，只支持一个不重叠信道。
- 5.0GHz 频段信道划分：
  - 5.0G 频段分配的频谱并不连续，主要有两段：5.15GHz～5.35GHz、5.725GHz～5.85GHz。
  - HT20 信道划分：不重叠信道在 5.15GHz～5.35GHz 频段有 8 个，分别为 36、40、44、48、52、56、60、64；在 5.725GHz～5.85GHz 频段有 4 个，分别为 149、153、157、161。
  - HT40 信道划分：在该模式下，这两段频谱的可用信道分别为 4 个和 2 个。

AP 支持手动和自动两种方式设置工作信道。设置为自动方式后，一旦检测到信道冲突 AP 具有信道自动调整功能。建议 AP 采用自动设置工作信道方式，避免手动设置后一旦信道冲突将导致无法切换信道的问题。

版权所有 © 华为技术有限公司

射频信道覆盖

WLAN 信道规划需遵循两个原则：蜂窝覆盖、信道间隔。根据覆盖密度、干扰情况、选择 2.4G/5G 单频或双频覆盖。AP 交替使用 2.4G 的 1、6、11 信道及 5.0G 的 36、40、44 信道，避免信号相互干扰；一般情况单独使用 2.4G 或 5.0G 的频段，对于会议室等高密度用户接入的场所，可以启用双频进行覆盖，以便提供更好的接入能力。

图2-4 单频信道规划示意图

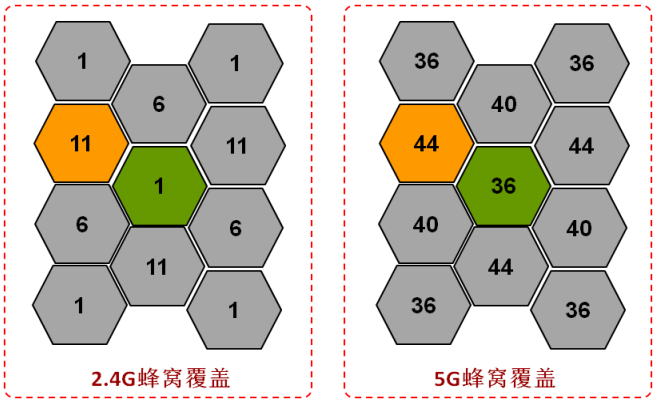
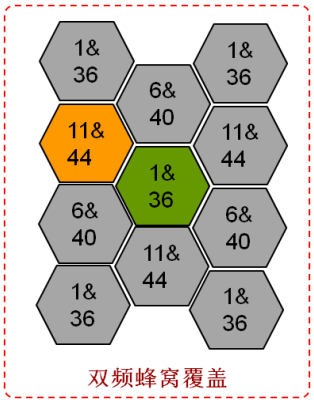


图2-5 双频信道规划示意图



2.6 无线网络安全规划

无线设备安全

- AP 防盗

  安装 AP 时安装防盗锁即可。

- AP 零配置

  传统的 FAT AP 组网模式要求在 AP 上配置大量的业务参数，同时需要在 AP 本地保存这些业务配置信息，一旦设备丢失，AP 的业务配置信息就可能被泄漏，形成网

版权所有 © 华为技术有限公司

络的安全漏洞。FIT AP 在设备上不保存业务配置，而是每次启动的时候从无线控制器动态加载业务配置，这样可以有效避免设备丢失造成配置泄漏。

当前 FIT AP 均能做到零配置。

无线 IDS/IPS

- IDS——非法 AP 检测

  非法 AP 主要指未经网络许可而非法部署的 AP 设备或者是对网络发起无线攻击的 AP 设备。

  对于非法部署的 AP 设备，可以通过控制 AP 接入（基于 MAC 地址、基于设备名称 SN 等）来防止非法 AP 接入网络。

  对于对网络发起无线攻击的 AP 设备，网络中合法部署的 AP 监听设备负责把监听到有攻击行为的无线设备上报给无线控制器，继而上报给网管。

  部署建议：

  - 对于非法部署的 AP 设备，由网络设备 AC 检测，启动相应功能即可。
  - 这里主要给出对发起无线攻击的 AP 的监听部署方案以及对比情况，如表 2-3 所示。可以根据实际网络要求进行取舍。

表2-3 对发起无线攻击的 AP 的监听部署方案优劣势对比表

部署方式	优点	劣势
部署专职监听 AP	实时监听网络，及时检测出非法 AP	网络部署成本高
业务 AP 兼职监听 AP	网络部署成本相对小	不能实时监听网络，无法及时检测到非法 AP

- IPS----黑白名单

  用户白名单功能：无线控制器支持静态配置白名单功能，该功能一旦启用，只有白名单上的无线用户才被认为是合法用户，其他非法用户的报文全部在 AC 上被丢弃，从而减少非法报文对无线网络的冲击。

  用户黑名单功能：无线控制器通过配置方式或者实时检测侦听的方式来确定设备是否被加入黑名单，被加入到黑名单中的设备发过来的报文全部在 AC 上丢弃，从而减少攻击报文对无线网络的冲击。

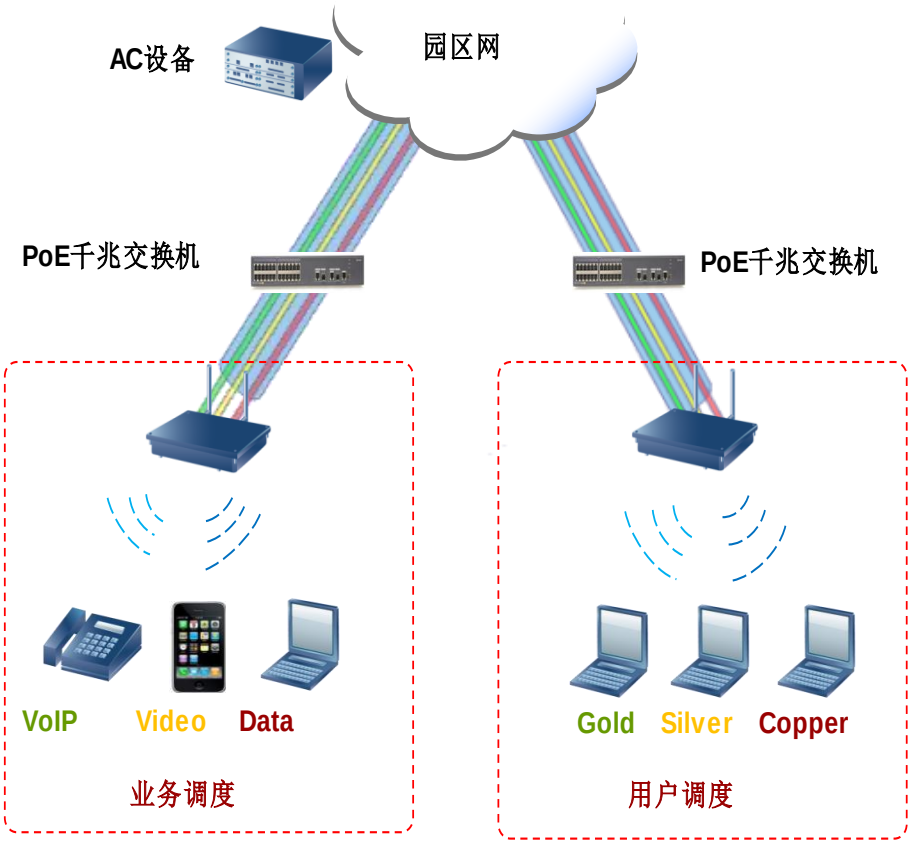
  部署建议：大中型园区网不建议部署，通过认证进行用户的合法检测即可。

2.7 QoS 规划

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

版权所有 © 华为技术有限公司

图2-6 WLAN QoS 规划



如图 2-6 所示，在企业园区中，常采用无线空口做 WMM 调度，有线侧进行优先级映射，园区网做 DiffServ 调度的方式，最大程度优化网络发生拥塞时的核心业务和 VIP 用户服务质量。在这里仅介绍 WMM 协议技术、优先级映射和流量管理技术。

流量管理

- 基于用户的流量管理

  防止 P2P 业务占用带宽导致其他用户无法正常使用无线网络，比如校园网。
- 基于 SSID 的流量管理

  防止某些 SSID 用户流量过大影响其他 SSID 用户的正常业务，比如访客 SSID 的流量控制。

无线空口做 WMM 调度

Wi-Fi 多媒体标准 WMM（Wi-Fi Multimedia）是一种无线 QoS 协议，无线空口上，WMM 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，从而保证语音、视频等应用在无线网络中有更好的质量。

版权所有 © 华为技术有限公司

WMM 按照优先级从高到低的顺序分为 AC（Access Category）-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个优先级队列，越高优先级队列中的报文，抢占信道的能力越高。

表2-4 WMM 队列优先级

WMM 队列	用户优先级（UP）
Voice	6 或 7
Video	4 或 5
Best Effort	2 或 3
Background	0 或 1

优先级的映射

优先级映射包括：无线优先级到有线优先级的映射、无线优先级到 CAPWAP 隧道优先级的映射。

- 上行无线到有线报文优先级映射

  AP 接收到无线客户端发送的 802.11（无线）数据报文后，将其转换为 802.3（以太网）报文，然后向网络侧继续转发。对于本地转发，完成用户优先级 UP 到 802.1P 优先级映射；对于集中转发，实现隧道优先级 Tunnel-802.1P 到 802.1P 优先级、Tunnle-TOS 到 TOS 的映射。

- 下行有线报文到无线报文优先级映射

  AP 接收到 802.3 以太报文后，将其转换为 802.11 报文，并在空口上依据报文中的 UP 优先级选择不同的 WMM 队列发送给用户终端。对于本地转发，需要完成 802.1P 到 UP 优先级映射；对于集中转发，在 AC 上可实现 TOS 优先级到 Tunnel-TOS 映射，802.1P 优先级到 Tunnle-802.1P 优先级映射。

2.8 可靠性规划

WLAN 网络可靠性主要是网络的负载分担，分为 AP 负载分担和 AC 的负载分担。

- AP 负载分担

  无线客户端一般会根据 AP 信号强度（RSSI）选择 AP，这很容易导致大量的客户端仅仅因为某个 AP 信号较强而连接到同一个 AP 上。由于这些客户端共享无线媒介，导致每个客户端的网络吞吐将大量减少。AP 负载分担可动态地确定在当前时刻和当前位置下哪些 AP 可以彼此分担负载，通过控制无线客户端接入的 AP，来实现这些 AP 间的负载分担。

  评估负载的方式有两种：

  – 按照用户在线会话数

版权所有 © 华为技术有限公司

- 按照用户流量

  当前 AP 负载分担策略是通过控制 STA 的接入实现负载均衡。当 AP 的负载情况超过阈值后，该 AP 就会拒绝新的终端的接入，此时终端将寻找负载较轻的 AP 进行连接，从而实现负载的均衡。

- AC 负载分担

  AC 负载分担即 AP 根据 AC 负载动态选择接入到负载轻的 AC 上去。

  AC 在响应报文（Discovery Response）中携带该 AC 负载信息（比如 AC 允许接入的最大 AP 数、当前接入的 AP 数、允许接入的最大 STA 数、当前接入的 STA 数），AP 通过比较各 AC 的负载情况选择一个负载轻的 AC 接入。

  通过 CAPWAP 隧道的心跳机制，AP 可及时发现控制器 Down，同时根据该方法重新选择一个负载轻的 AC 接入。

版权所有 © 华为技术有限公司

3 WLAN 接入认证计费方案

3.1 无线安全协议标准

如表 3-1 所示，WLAN 无线安全协议标准主要有：OPEN-SYSTEM（Open system authentication）、WEP（Wired Equivalent Privacy）、WPA/WPA2（Wi-Fi Protected Access）、WAPI（WLAN Authentication and Privacy Infrastructure）。

表3-1 WLAN 无线安全协议标准介绍

标准	简介	适用场景
OPEN-SYSTEM	开放系统认证是802.11的缺省设置，不进行认证。	一般用于有众多用户的运营网络
WEP	有线等效加密，即对于数据的加密和解密都使用同样的密钥和算法，主要用来保护WLAN空口信号的信息安全。	应用于小规模/低安全需求的WLAN网络（SOHO/家庭热点等）。
WPA/WPA2	• 基于 802.1x 架构进行身份认证 • 基于 PSK(Pre-Shared Key)、EAP（Extensible Authentication Protocol）等协议进行身份认证 • 基于 TKIP（Temporal Key Integrity Protocol）实现数据加密 • 基于 4 次握手实现用户会话密钥的动态协商 • WPA2 增加了预认证和 CCMP（Counter CBC-MAC Protocol）加密，同时兼容 WPA	广泛应用于各种大、中型WLAN网络和公共场合，为目前主推加密方案。

版权所有 © 华为技术有限公司

标准	简介	适用场景
WAPI	WAPI系统包含WAI鉴别及密钥管理和WPI（WLAN privacy infrastructure）数据传输保护： • 基于证书机制和自行设计的WAI(WLAN Authentication Infrastructure)认证协议完成身份鉴别和密钥管理，而没有重用802.1x，RADIUS等现有安全标准。 • 基于自行设计的WPI协议实现数据的加密保护。	中国标准，一般作为准入门槛测试。

华为 AC 均支持开放系统认证、WEP 加密、共享密钥认证、WPA/WPA2 认证和加密、WAPI 认证加密等无线接入安全特性。

3.2 WLAN 终端认证技术

IEEE 802.11 标准要求 WLAN 终端在准备连接到网络时，必须进行“身份验证”。

WLAN 终端身份认证主要有两种方式：开放系统认证（Open-system Authentication）和共享密钥认证（Shared-Key Authentication）。

- 开放系统认证是 IEEE 802.11 标准要求必备的一种方法，是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。在这种方式下，接入点并未验证工作站的真实身份，工作站以 MAC 地址作为身份证明，这种验证方式可以让所有符合 802.11 标准的终端都可以接入到 WLAN 网络中来。开放系统身份验证比较适合有众多用户的电信运营 WLAN 网络。
- 共享密钥式认证必需使用加密方式，要求每个 WLAN 终端都配置和 AP 完全一致的密钥（key）。由于配置工作量较大，一般适用于企业网、校园网及家庭网络等。

二者对比如下：

表3-2 WLAN 终端认证方式对比

认证方式	优点	缺点	适用场景
开放式系统认证	部署简单，终端接入速度快，有效带宽高。	安全性差，无法检验客户端是否合法，任何知道无线局域网 SSID 的用户都可以访问网络。	电信运营网络
共享密钥式认证	安全性较高，采用加密方式对密钥进行保护，空口密钥数据不再明文传输。	配置复杂，可扩展性不佳；每台终端和AP上都需要静态配置一个很长的密钥字符串。 有效带宽较低，加密降低了传输效率。	企业网、校园网及家庭网络等。

版权所有 © 华为技术有限公司

3.3 无线用户身份认证技术

相对于简单的 STA 身份验证过滤机制，链路层用户身份验证的安全性大大提高。通过提供有限的访问权限来验证用户身份，只有确定用户身份后才给予完整的网络访问权限，可有效判别用户的合法性。链路层身份验证是透明的，能配合任何网络层协议使用。

常用的 WLAN 的链路层身份验证主要有 MAC 认证、802.1x、Portal（DHCP+Web）、PPPoE 等几种认证方式。

对于企业园区，无线哑终端一般通过 MAC 认证接入，办公区域通过 802.1x 或 Portal 认证接入，访客区域一般通过 Portal 认证接入。

多种认证技术保证 STA 安全接入，合法用户访问合规资源，从源头上消除安全威胁。

MAC 认证

MAC 认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何的客户端。由于无线终端的网卡都具备唯一的 MAC 地址，因此可以通过检查无线终端数据包的源 MAC 地址来识别无线终端的合法性。MAC 地址过滤控制方式要求预先在 AP 中写入合法的 MAC 地址列表，只有当终端的 MAC 地址和合法 MAC 地址表中的地址匹配，AP 才允许终端与之通信。

在企业园区中 MAC 认证主要用于 IP 电话、打印机等哑终端设备的接入。

802.1x 认证

802.1x 是针对以太网而提出的基于端口进行网络访问控制的安全性标准草案。基于端口的网络访问控制利用物理层特性对连接到 LAN 端口的设备进行身份认证。如果认证失败，则禁止该设备访问 LAN 资源。

尽管 802.1x 标准最初是为有线以太网设计制定的，但它也适用于符合 802.11 标准的无线局域网，且被视为是 WLAN 的一种增强性网络安全解决方案。802.1x 体系结构包括三个主要的组件：

- 请求方（Supplicant）：提出认证申请的用户接入设备，在无线网络中，通常指待接入网络的无线客户机 STA。
- 认证方（Authenticator）：允许客户机进行网络访问的实体，在无线网络中，通常指访问接入点 AP 或控制器 AC 设备。
- 认证服务器（Authentication Sever）：为认证方提供认证服务的实体。认证服务器对请求方进行验证，然后告知认证方该请求者是否为授权用户。认证服务器可以是某个单独的服务器实体，也可以不是，后一种情况通常是将认证功能集成在认证方 Authenticator 中。

802.1x 技术是一种增强型的网络安全解决方案。在采用 802.1x 的无线局域网中，无线用户端安装 802.1x 客户端软件作为请求方，无线设备 AP/AC 内嵌 802.1x 认证代理作为认证方，同时它还作为 RADIUS 认证服务器的客户端，负责用户与 RADIUS 服务器之间认证信息的转发。

802.1x 体系本身不是一个完整的认证机制，而是一个通用架构。用来传输实际的认证协议。802.1x 体系的好处就是当一个新的认证协议发展出来的时候，基础的 802.1x 体系机

版权所有 © 华为技术有限公司

制不需要随之改变。802.1x 体系使用 EAP 认证协议，目前有超过 20 种不同的 EAP 协议。802.1x 认证常用的包括以下几种 EAP 认证模式：

- EAP-MD5
- EAP-TLS(Transport Layer Security)
- EAP-TTLS(Tunnelled Transport Layer Security)
- EAP-PEAP(Protected EAP)
- EAP-LEAP(Lightweight EAP)
- EAP-SIM

PPPoE 认证

PPPoE 是 PPP 协议应用到以太网进行的再一次封装，进行广播链路上点对点通讯的协商，包括服务器的发现和会话标识 Session ID 的确认。主要包括三个部分：

- 用户和接入设备在 LCP 阶段协商链路层参数。
- 将用户名和密码发送给接入设备进行 CHAP/PAP 认证，接入设备可以进行本地认证，也可以将用户名和密码发送给 AAA 服务器进行认证。
- 根据认证结果，判断是否进入到 NCP（IPCP）协商阶段，NCP 协商阶段接入设备给用户计算机分配网络层参数（例如 IP 地址等）。

PPP 的三个协商阶段通过后，用户就可以发送和接收数据报文。

PPPoE 也是一种认证模式，PPPoE 在 WLAN 使用时，和 WLAN 本身采用的认证加密没有关系。即不管采用 WEP、WPA 或者 WAPI，都可以选择 PPPoE 作为用户业务的认证协议。

Portal 认证

Portal 认证也称 Web 认证或 DHCP+Web 认证。客户端使用标准 Web 浏览器（例如 IE），填入用户名、密码信息，页面提交后，由 Web 服务器和设备配合完成用户的认证。

接入设备将来自客户的 HTTP 请求重定向到 Portal 服务器，在 Portal 页面上输入用户名、密码进行认证。用户在 Web 认证之前，必须先通过 DHCP、静态配置等获得 IP 地址。用户如果被配置成强制 Web 认证，则用户只需要输入自己喜欢的网页即可，系统自动下载认证网页。主要认证过程为：

1. 动态用户通过 DHCP 协议获取地址；
2. 用户访问 Web 认证服务器的认证页面，并在其中输入用户名、密码，Web 认证服务器将用户的信息通过内部协议，通知接入设备；
3. 接入服务器到相应的 AAA 服务器对该用户进行认证，将认证结果通知 Web 认证服务器；
4. Web 认证服务器通过 HTTP 页面将认证结果通知用户，如果认证成功用户即可正常访问网络资源。

Portal 认证通常需要多个服务器支持，如 DHCP 服务器、AAA 服务器等。

版权所有 © 华为技术有限公司

无线接入认证和安全协议对应关系

表3-3 无线接入认证和安全协议对应关系表

认证方法	安全协议	安全性	封装开销	地址分配	客户端软件	应用场景
MAC 认证	Open System	低	小	认证后分配	不需要	PDA、IP 电话等哑终端设备接入。
	WEP/WPA/WPA2+PSK	低	小	认证后分配	不需要	场景同上，需要维护 PSK 密码。
Portal 认证	Open System	中	小	认证前分配	不需要	中小型园区网络。
	WEP/WPA/WPA2+PSK	中	小	认证前分配	不需要	场景同上，需要维护 PSK 密码。
802.1x 认证	WEP/WPA/WPA2	高	小	认证后分配	需要	大中型园区网络。
PPPoE 认证	Open System	低	大	认证后分配	需要	运营商市场
	WEP/WPA/WPA2+PSK	低	大	认证后分配	需要	场景同上，需要维护 PSK 密码。

当前 WAPI 在企业网和运营商中应用很少，一般作为准入门槛测试，园区网中，从安全性和易部署性等多方面考虑，推荐 802.1x＋WPA2 的机制。

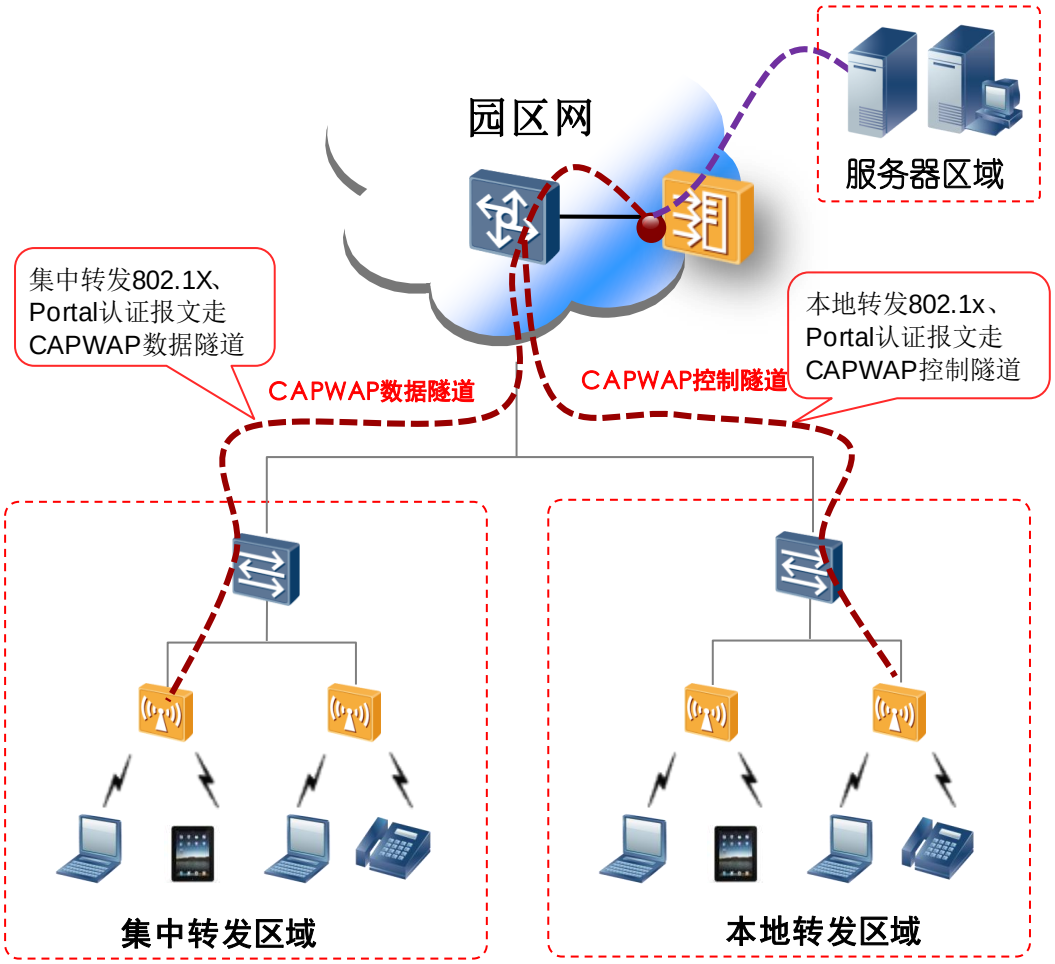
无线用户 AC 集中认证方案

无线用户在 AC 上集中认证，可以保证无线用户集中管理，通过 AC 控制隧道将授权信息下发到 AP 设备，精细化控制用户访问权限，并在用户漫游、安全控制等方面由 AC 做到灵活控制。

无线用户集中认证，需要保证相关认证协议能够上送 AC 处理。集中转发场景下，EAP、Portal 报文作为数据报文通过 CAPWAP 数据隧道上送 AC；在本地转发场景下，可通过配置让 EAP、Portal、PPPoE 报文进入 CAPWAP 控制隧道，从而上送到 AC 设备完成认证过程。

版权所有 © 华为技术有限公司

图3-1 无线用户 AC 集中认证示意图



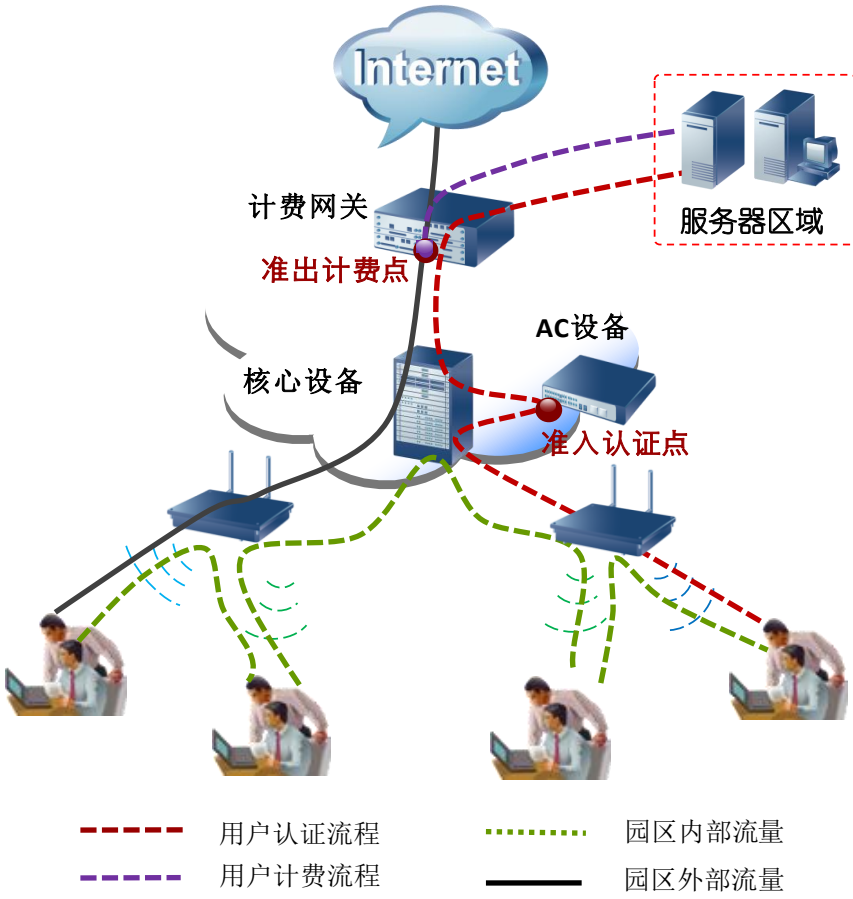
AC 集中认证组网如图 3-1 所示，认证方式包括 MAC、802.1x、Portal、PPPoE 等方式。园区网中，从安全性、易部署等角度考虑，一般推荐 802.1x+WPA2 接入认证。

3.4 认证、安全、计费功能与部署

由于无线网络安全威胁日益严重，因此对于企业园区的无线接入用户存在认证、授权、安全检查等需求；对于某些行业，例如校园网、广电网、酒店等行业，除了认证授权以外还要求实现计费功能。

华为专有和保密信息
版权所有 © 华为技术有限公司

图3-2 用户认证、安全、计费集成方案组网图



如上图所示，无线用户在 AC 集中认证和授权，实现准入控制。园区出口部署计费服务器，实现园区出口流量统一计费。无线数据转发模型采用本地转发，数据流量不经过 AC，提升网络性能。

采用此方式，实现无线园区用户集中认证，数据流量本地转发，安全管理和网络性能做到完美结合；并且实现了各功能组件可按需选择，提供认证、认证＋安全、认证＋计费、认证＋安全＋计费等多套方案。

3.4.1 认证、安全、计费系统功能组件

认证、安全、计费集成方案主要由服务器、客户端、计费网关三部分组成，其中服务器系统可分为认证、安全、计费、Portal 等四个组件，各组件功能如下表：

表3-4 认证、安全、计费系统各组件功能

序号	组件名称	功能描述	备注
1	用户认证组件	支持 MAC、802.1x、Portal、PPPoE 等接入认证和相关统计报表。	必选

版权所有 © 华为技术有限公司

序号	组件名称	功能描述	备注
2	安全管理组件	通过和客户端联动，支持终端补丁、防病毒等安全检查和修复功能。	可选
3	用户计费组件	支持基于时间和流量的计费，包括包月、包年、包半年、包学期、动态包天、动态包月、动态包年、包时长、包流量等主流计费方式。	可选
4	Portal 组件	弹出用户定制的认证页面，提供方便的用户自助服务平台，实现用户 Portal 接入认证。	可选
5	客户端软件	通过和服务器联动，完成接入认证、安全检查、用户计费等功能。	可选
6	计费网关	部署在园区网出口，实现出外网报文计费功能，包括基于时间和基于流量计费两种方式。	可选

表中，除了用户认证是必选组件外，其他组件可基于现网需求选择。例如，如果用户部署认证＋安全方案，并采用 Portal 认证，则可选取 1、2、4、5 组件。

注意

不同厂商对于功能组件的划分存在差异，另外用户需求也具有多样性，不能简单的和报价组件进行对应。

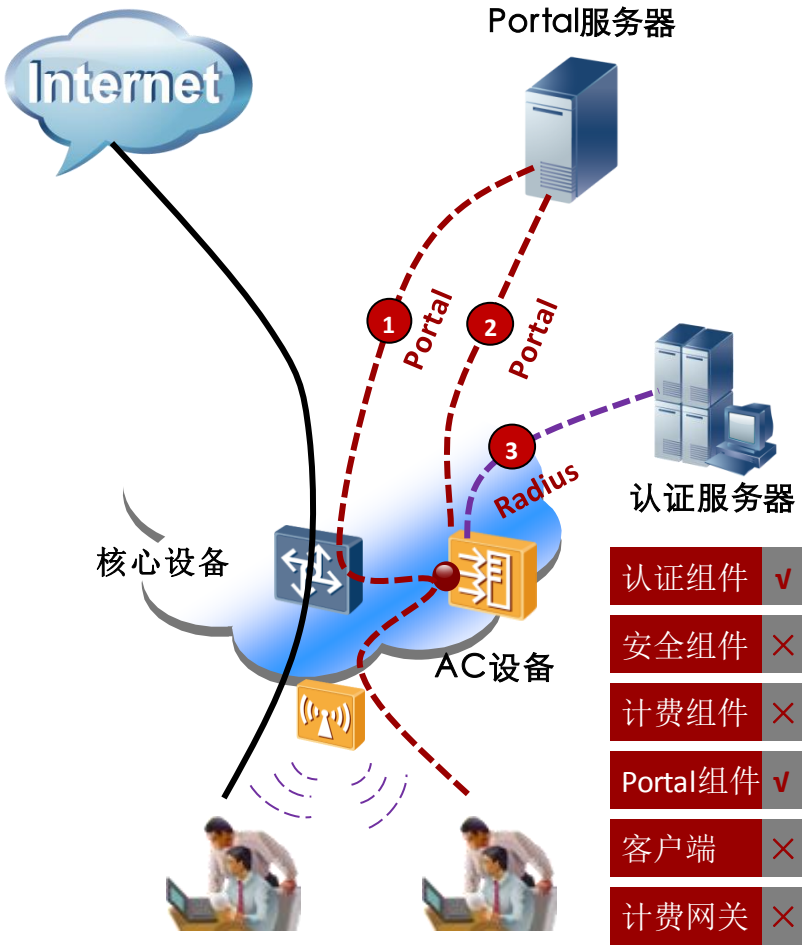
3.4.2 认证、安全、计费集成方案

集成方案之一：认证方案

认证方案适合中、小型企业用户，需要控制用户接入园区网络，同时由于企业员工较少，没有终端健康检查等安全需求。

版权所有 © 华为技术有限公司

图3-3 认证方案组网图



如上图，用户可选择 802.1x 认证或者 Portal 认证部署，本方案以 Portal 认证为例，服务器组件采用华为 TSM 系统，认证服务器和 Portal 服务器可部署在同一台服务器上。

功能实现流程：

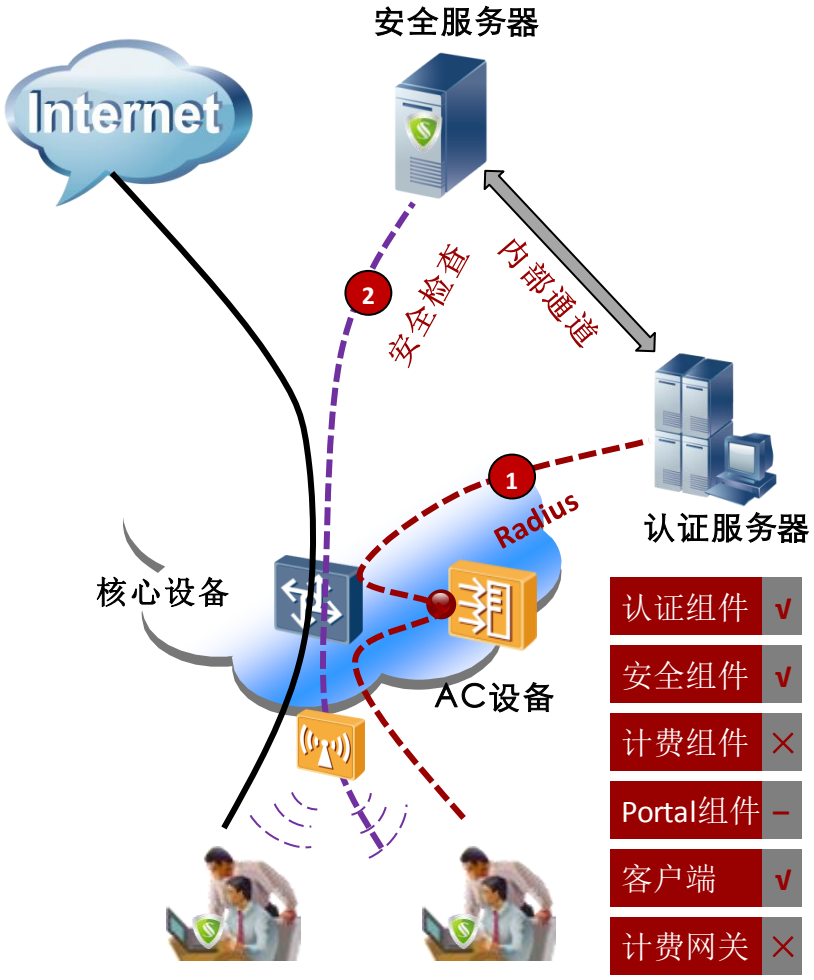
1. 无线用户通过 Web 页面认证，认证报文到 AC 后，通过 Portal 协议向 Portal 服务器发起认证。
2. Portal 服务器把用户信息回传给 AC 设备。
3. AC 设备和认证服务器通过 RADIUS 协议完成用户准入认证。

集成方案之二：认证＋安全方案

认证+安全方案适合政府、企业等对于安全要求较高的行业客户。通过准入控制＋安全检查，提升内网安全。并且服务器组件支持定制化选择，若用户只作准入认证，则可不选择安全组件。

版权所有 © 华为技术有限公司

图3-4 认证＋安全方案组网图



如上图，认证组件、安全组件、客户端为必选组件。其中服务器组件采用华为 TSM 系统，认证服务器和安全服务器之间为内部通道，一般部署在同一台服务器上。

功能实现流程：

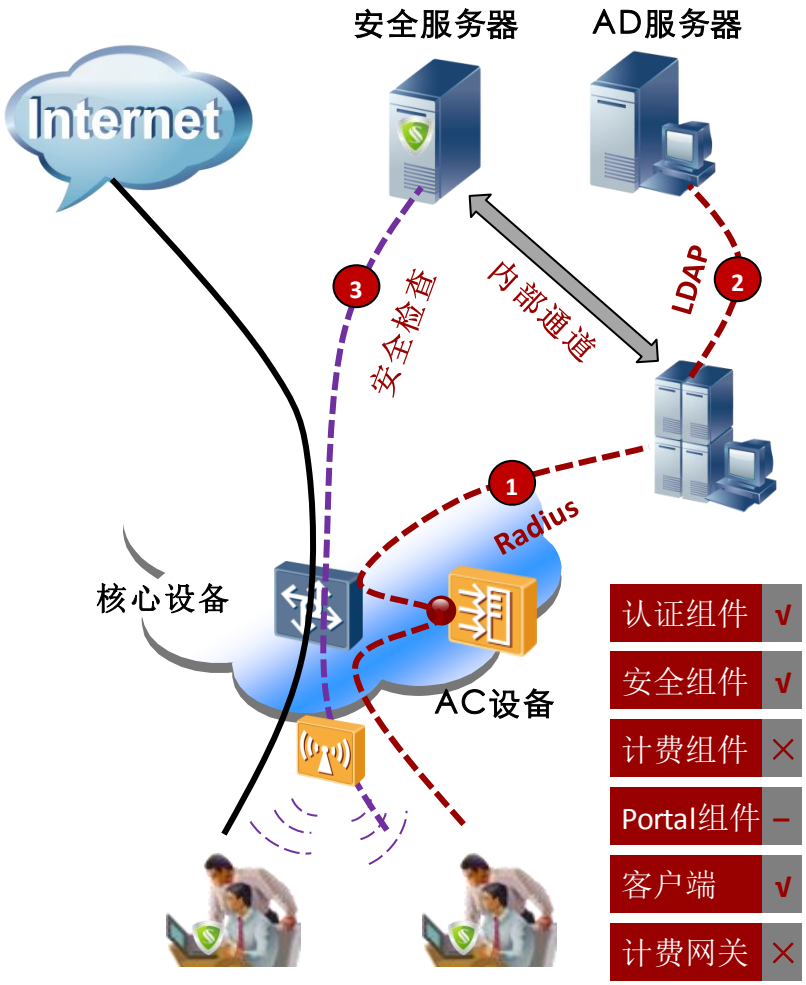
1. 无线用户认证报文到 AC 后，通过 RADIUS 协议（Portal 认证先到 Portal 服务器交互）到认证服务器完成认证过程。
2. 安全服务器和客户端配合，完成终端病毒库、补丁等健康检查功能，并可和软件服务器联动，进行终端修复操作。

集成方案之三：认证＋安全＋AD

认证＋安全＋AD 方案适合已经使用 LDAP 服务器管理用户，同时对于内网安全要求较高的企业。通过部署准入控制＋安全检查，提升内网安全；并和现有 AD 对接，保护用户投资。

版权所有 © 华为技术有限公司

图3-5 认证＋安全+AD 方案组网图



如上图，要实现认证+安全+AD 功能，认证组件、安全组件、客户端为必选组件；服务器组件采用华为 TSM 系统，认证服务器和安全服务器之间为内部通道，一般部署在同一台服务器上；LDAP 服务器为微软 AD 域服务器。

功能实现流程：

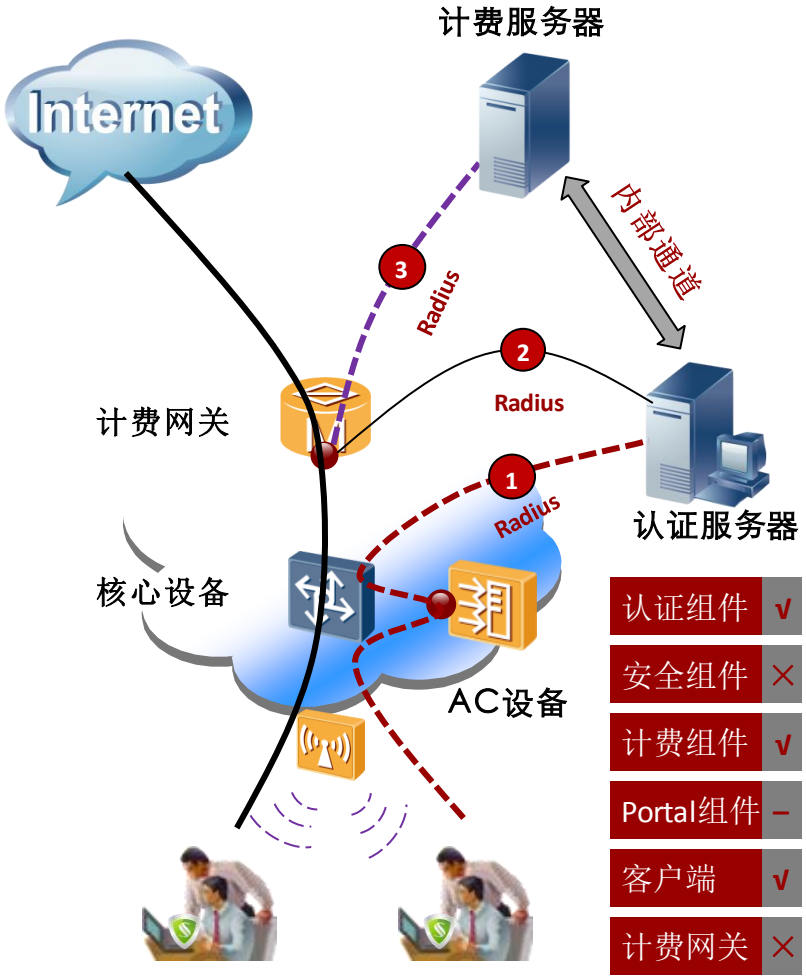
1. 无线用户认证报文到 AC 后，通过 RADIUS 协议向认证服务器发起准入认证。
2. 认证服务器和 AD 服务器通过 LDAP 协议获取用户信息，完成认证过程。
3. 安全服务器和客户端配合，完成终端病毒库、补丁等健康检查，并可和软件服务器联动，进行终端修复操作。

集成方案之四：认证＋计费

认证＋计费方案适合教育、酒店等有计费要求的行业网，同时对于内网安全要求一般的客户。通过准入准出一次认证，提升用户体验。并且计费网关可按需选择，节省用户投资。

版权所有 © 华为技术有限公司

图3-6 认证＋计费方案组网图



如上图，要实现认证+计费功能，认证组件、计费组件、Portal 组件、客户端、计费网关为必选组件。其中服务器组件采用合作方产品；认证服务器和计费服务器之间为内部通道，一般部署在同一台服务器上；计费网关一般选择合作方产品，大型行业网可使用 ME60 设备。

功能实现流程：

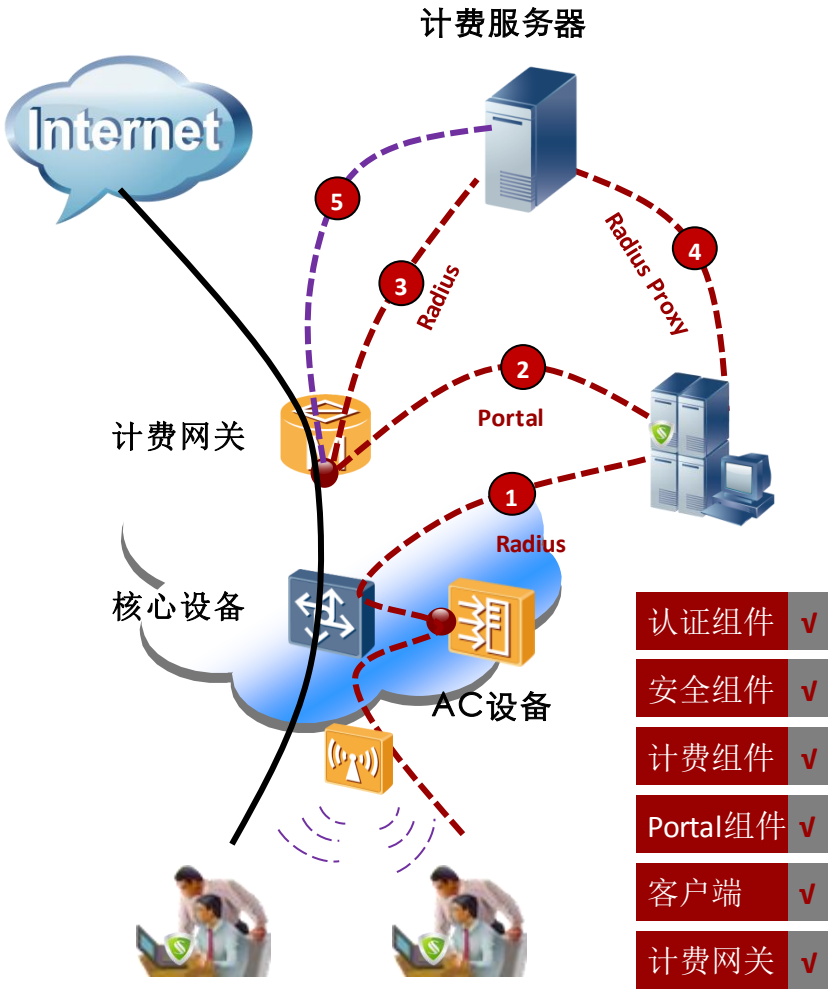
1. 无线用户认证报文到 AC 后，通过 RADIUS 协议到认证服务器完成内网准入认证。
2. 认证服务器通过 RADIUS 协议，主动通知计费网关进行准出认证，打开外网权限。
3. 用户访问外网，则计费网关开始计费，并向计费服务器通告计费信息。

集成方案之五：认证＋安全＋计费

认证＋安全＋计费部署方案适合有计费要求并且客户对于内网安全也有较高要求的行业，例如教育、能源等行业网。通过准入准出一次认证，提升用户体验；用户数据集中管理，方便系统维护。

版权所有 © 华为技术有限公司

图3-7 认证＋安全+计费方案组网图



如上图，要实现认证+安全+计费功能，认证组件、安全组件、计费组件、Portal 组件、客户端、计费网关均为必选组件。服务器组件主要采用华为 TSM 系统，计费服务器和计费网关采用第三方产品，大型园区可使用 ME60。

功能实现流程：

1. 无线用户认证报文到 AC 后，通过 RADIUS 协议到认证服务器完成内网准入认证。
2. 认证服务器的 Portal 组件主动向计费网关发起 Portal 认证，完成外网准出认证。
3. 计费网关继而通过 RADIUS 协议向计费服务器请求用户信息。
4. 计费服务器作为 RADIUS Proxy，从认证服务器获取用户信息，完成准出认证，同时同步用户信息到本地。
5. 用户访问外网，则计费网关开始计费，并向计费服务器通告计费信息。

版权所有 © 华为技术有限公司

集成方案小结

综上所述，WLAN 认证、授权、计费功能可以根据企业园区实际需求有选择性部署。按照常用使用场景可分为认证、认证＋安全、认证＋安全+AD、认证＋计费、认证＋安全+计费这五种方案。部署方案以及相应场景如下表：

表3-5 功能组件部署及对应场景列表

编号	方案名称	服务器组件				客户端	计费网关	应用场景
		认证	安全	Portal	计费			
1	认证	TSM	-	TSM	-	-	-	中小型企业，对于终端安全没有要求
2	认证+安全	TSM	TSM	TSM	-	TSM	-	政务、大中型企业等对内网安全较严格的场景
3	认证+安全+AD	TSM	TSM	TSM	-	TSM	合作方或 ME60	LDAP 服务器管理用户，同时内网安全要求较严格
4	认证+计费	合作方					合作方或 ME60	校园、广电、酒店等需要计费的行业市场。
5	认证+安全+计费	TSM	TSM	TSM	合作方	TSM	合作方或 ME60	教育、能源等需要计费的行业市场，同时内网安全要求较严格。

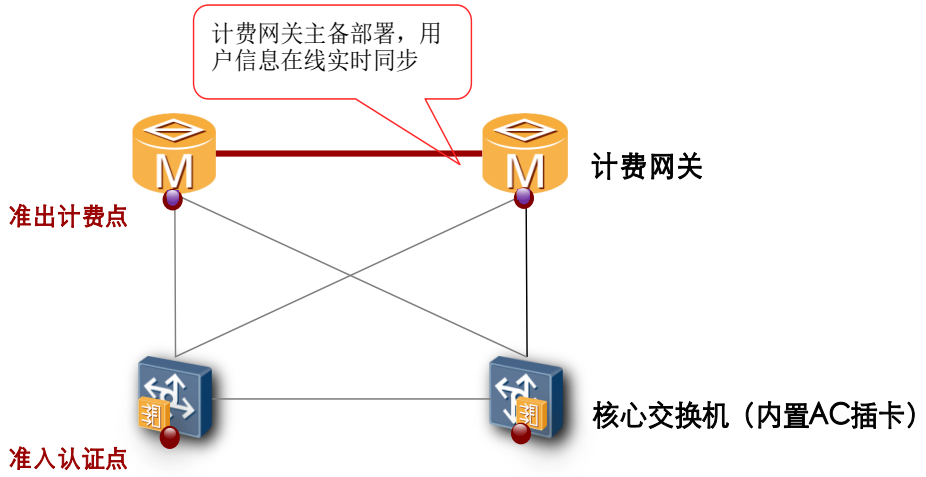
3.4.3 园区出口计费网关部署

如图 3-8 所示，园区网中计费网关一般作为准出设备，在用户报文出园区时进行计费。

计费网关部署在园区出口，具有单机和主备两种方式，为了提升园区网络可靠性，推荐采用主备方式。采用主备方式，网关可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到另一台设备，保证两台计费网关信息一致。

版权所有 © 华为技术有限公司

图3-8 计费网关主备方式部署及数据同步示意图



为保证数据准确性，通过以下步骤实现计费网关和服务器数据同步：

1. 用户通过准入认证获得内网访问权限，服务器记录用户名、密码、状态等在线信息。
2. 服务器通过同步机制把用户信息同步到计费网关，同步开放用户访问外网权限。
3. 用户访问外网，则在计费点直接开始计费，无需再做二次认证。

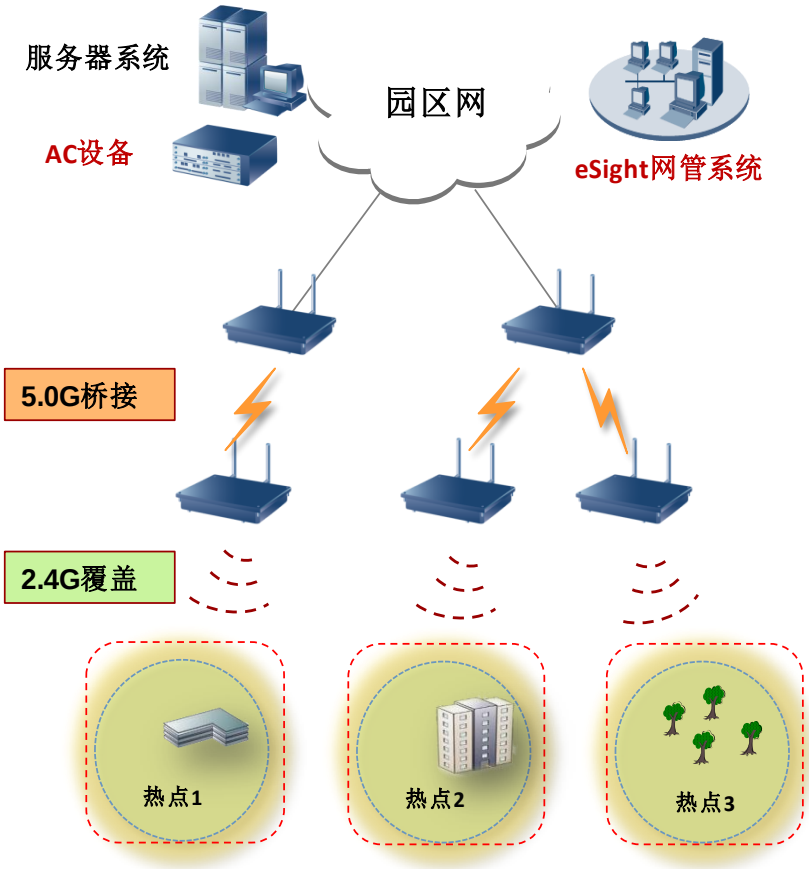
版权所有 © 华为技术有限公司

4 WDS 网桥无线数据回传典型方案

WDS（Wireless Distribution System）通过无线链路连接两个或者多个独立的有线局域网或者无线局域网，组建一个互通的网络，实现数据访问。

WDS 技术适用于在大型仓库、港口码头、山川河流等不适合部署线缆的恶劣环境以及乡村、郊区或者野外等人员稀疏环境，通过无线链路连接两个或者多个独立的有线局域网或者无线局域网，并为他们之间提供数据交换功能。WDS 技术方便了网络部署、安装，实现了灵活组网。

图4-1 WLAN 无线回传示意图



版权所有 © 华为技术有限公司

如图 4-1 所示，在不适合部署线缆的恶劣环境下，无线网桥通过 P2P/P2MP 桥接功能，实现热点区域覆盖和数据回传；其中桥接使用 5.0G 频段，无线覆盖使用 2.4G 频段。

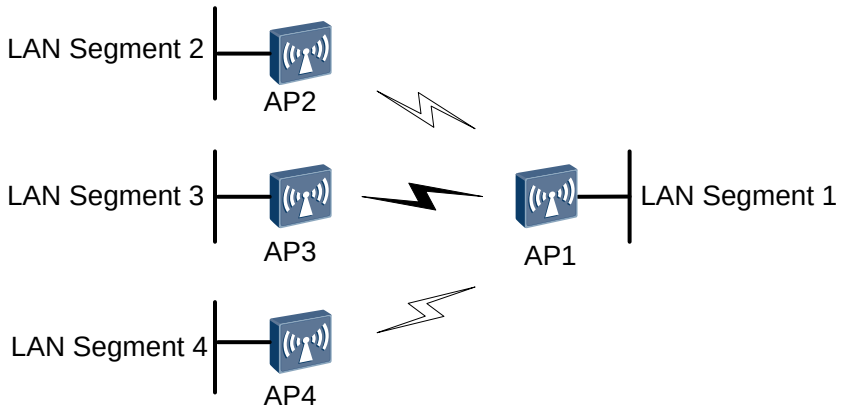
4.1 WDS 组网模式

在实际组网中，WDS 网桥组网模式可以分为点对点模式和点对多点模式。

图4-2 点对点组网模式示意图

如图 4-2 所示，WDS 通过两台设备实现了两个网络无线桥接，最终实现两个网络的互通。实际应用中，每一台设备可以通过配置对端设备的 MAC 地址，确定需要建立的桥接链路。

图4-3 点对多点组网模式示意图



如图 4-3 所示，在点到多点的组网环境中，一台设备作为中心设备，其他所有的设备都只和中心设备建立无线桥接，实现多个网络的互联。但是多个分支网络的互通都要通过中心桥接设备进行数据转发。

在点对多点组网场景下，AP 网桥链路之间、以及有线链路可能出现网络环路。为防止网络风暴、保证正确的二层转发，需要启用 STP 功能打开环路检测。STP 功能对 AP 有线接口、和开启了 WDS 的网桥接口有效。网桥端口的每个无线虚链路作为一个独立逻辑端口参与 STP 协议交互和控制。

版权所有 © 华为技术有限公司

4.2 WDS 组网性能指标

由于无线技术较容易受到应用环境、传输距离、天线增益、频宽等因素影响，因此在进行无线回传规划时需要关注现场环境带来的影响，传输性能如下表所示：

表4-1 无线网桥（WDS）P2P 传输性能指标

工作频段	环境	天线增益	典型距离下 802.11n HT20/HT40 吞吐量（Mbps）					
			500m	1km	2km	5km	10km	频宽
2.4G 覆盖/维护	市区	11dBi	80	80	45	15	/	HT20
		14dBi	80	80	80	36	15	HT20
		17 dBi	80	80	80	60	36	HT20
	郊区/农村	11dBi	80	80	70	32	12	HT20
		14dBi	80	80	80	55	32	HT20
		17 dBi	80	80	80	80	55	HT20
5.8G 无线回传	市区	11dBi	55/90	30/45	6/?	/	/	HT20/HT40
		15dBi	80/160	60/95	30/45	/	/	HT20/HT40
		18dBi	80/160	80/160	50/80	12/15	/	HT20/HT40
		21dBi	80/160	80/160	80/135	32/50	10/?	HT20/HT40
	郊区/农村	11dBi	80/160	80/135	45/65	8/?	/	HT20/HT40
		15dBi	80/160	80/160	48/70	10/?	/	HT20/HT40
		18dBi	80/160	80/160	80/120	30/45	8/?	HT20/HT40
		21dBi	80/160	80/160	80/160	50/80	27/40	HT20/HT40

2.4G 一般用于用户接入覆盖及设备维护，不建议回传使用，无线回传推荐 5.8G 频段，传输距离控制在 5KM 内。

表4-2 无线网桥（WDS）P2MP 传输性能指标

P2MP	影响因素		吞吐量影响因子	
	隐藏终端	多用户竞争	P	MP
1	无	无	1	1
2	0.6	0.95	0.57	0.285
3	0.6	0.9	0.54	0.18
4	0.6	0.9	0.54	0.135
5	0.6	0.8	0.48	0.096

版权所有 © 华为技术有限公司

P2MP	影响因素		吞吐量影响因子	
	隐藏终端	多用户竞争	P	MP
6	0.6	0.8	0.48	0.08

使用点对多点（P2MP）网桥时受隐藏终端和多用户竞争等因素影响，吞吐量将急剧下降；因此点对多点（P2MP）网桥吞吐量性能评估需在点对点（P2P）网桥数据基础上考虑吞吐量系数。

网络规划中，P2MP 网桥推荐不超过 4 个，无线回传距离控制在 5km 内。

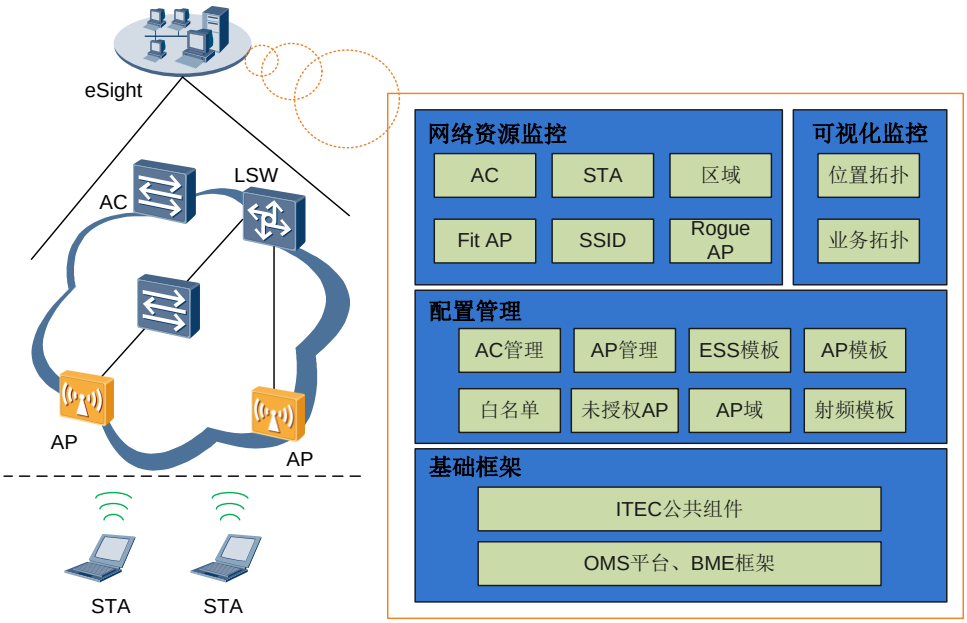
版权所有 © 华为技术有限公司

5 WLAN 网络管理方案

5.1 网管方案概述

华为公司 eSight 管理平台根据企业网网络管理特点，采用 B/S 架构，瘦客户端，远程登录。eSight 平台的 WLAN 功能模块组件化解耦，按需拆卸，便于在企业网不同场景下灵活组合，并能够提供二次开发和定制能力。

图5-1 eSight WLAN 网络管理



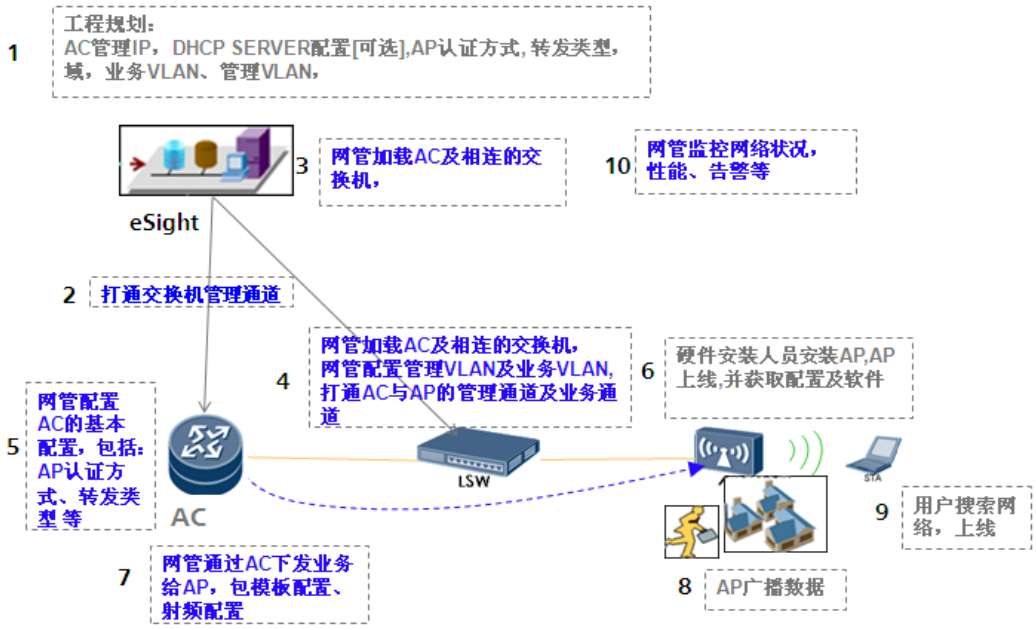
5.2 eSight WLAN 网络管理流程

WLAN 网络管理帮助用户快速完成无线网络部署，提供网络设备、非法 AP 等物理资源监控功能，实现故障的快速感知、定位及解决，同时通过无线相关报表及多形式分类资源统计，为用户日常运维及网络调整提供了依据，极大提升网络管理效率。

版权所有 © 华为技术有限公司

Sight WLAN 网络管理流程如图 5-2 所示。

图5-2 eSight WLAN 网络管理流程



网络部署

网络安装完毕后，用户通过简洁向导式部署页面，首先指定 AC 参数配置，其次创建网元级配置模板，通过规化表单批量导入 FIT AP 列表，最终批量完成 FIT AP 部署，快速完成 WLAN 网络的部署。

网络监控

用户可以通过网管物理拓扑，查看监控 AC 设备及链路状态；可以通过 WLAN 业务拓扑直观查看 STA、FIT AP、AC 接入关系；可以通过位置拓扑查看当前热点位置及射频信号覆盖范围并在视图上标识当前非法 AP 位置。

用户通过性能管理、告警管理及 WLAN 物理资源管理监控网络运行状况，并通过报表系统周期性给出 WLAN 相关报表，帮助用户实现轻松运维。

网络故障恢复

当网络中的 AP 出现异常或在 WLAN 网络的调试过程中，用户可以通过网管远程批量恢复 AP 的出厂设置；在 WLAN 网络中 AP 升级完成后或在 WLAN 网络的调试过程中，用户可以通过网管远程批量重启 AP；当网络中的 AP 出现硬件故障需要替换时，用户可以通过网管快速完成 AP 替换，AC 复制故障 AP 上原有的配置至替换新替换的 AP，快速保证 AP 替换后业务不变。

用户可以可通过 AP PING 上行设备 IP（包括网关或服务器 IP），根据测试结果，判断 AP 上行业务线路的通断情况；或通过 AP 下行 PING 用户 IP 地址，从而确认用户报障

版权所有 © 华为技术有限公司

原因是用户关联问题还是上行业务不通。AP Ping 受 AP 状态正常约束，所以提供 AC 的诊断，AC 下行 Ping，可诊断 AC 至 AP 链路通断。

5.3 企业 WLAN 网络管理规划

大中型园区无线网络管理

对于大中型园区 WLAN 网络，推荐使用专门的网管平台（例如 eSight）实现对 WLAN 网络的管理。它不仅可以实现对于 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，节省维护成本。

小型、微型园区无线网络管理

小型园区网络中可能不会部署专门的网管，此时可以通过 AC 上的本地管理对无线网络进行管理维护，包括相关配置、告警、软件版本管理等。

建议通过 Telnet 方式登录到 AC，实现普通或安全登录的要求。

基于用户的帐号管理可以确保只有相关资格的人才能登录网络进行网络运维管理，保护网络的安全与可靠性。

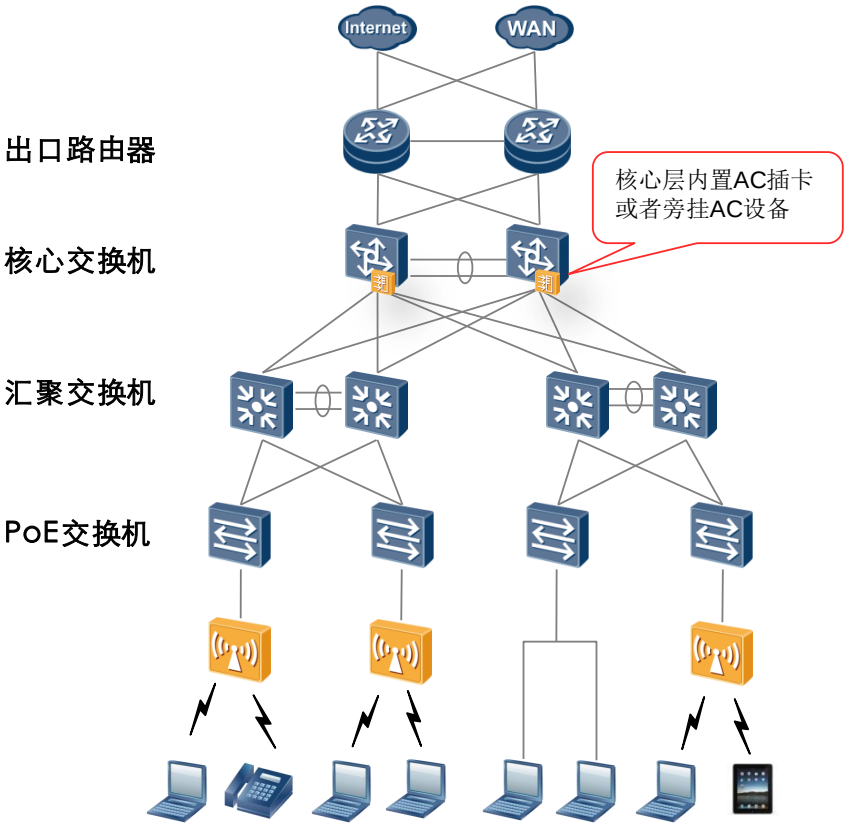
版权所有 © 华为技术有限公司

6 WLAN 网络组网推荐方案

6.1 大中型园区网 WLAN 组网推荐方案

大中型园区网定位为大中型企业总部、大型分部机构、高校、机场等。大型园区 WLAN 部署的 AP 数量较多，适用于有内部需求和访客上网需求的场所，也适用于网络改造，增加园区无线覆盖的场景。

图6-1 大中型园区网络拓扑示意图



华为专有和保密信息
版权所有 © 华为技术有限公司

大型园区 WLAN 方案一般在园区网的核心层部署 AC 设备，并采用主备方式保证高可靠性，由 AC 统一管理 AP 设备和无线用户。AC 设备推荐在核心交换机（如 S97/77 等）上直接配置插卡式 AC，方便管理；另外，也可采用旁挂独立 AC 设备（如 AC6605）。

大中型园区中 WLAN 网络部署规划主要有如下配置推荐：

表6-1 大中型园区中 WLAN 网络部署规划推荐配置

网络配置点	分类	推荐	备注
网络架构	FAT AP	-	-
	FIT AP	√	-
AC 部署方式	集中式	√	-
	分布式	-	-
AC 部署位置	旁挂	√	-
	直路	-	-
AC 硬件形式	集成 AC	√	-
	独立 AC	-	-
AP 类型	AP6010SN（室内型，支持 802.11a/b/g/n）	√	均可，根据实际需要
	AP6010DN（室内型，支持 802.11a/b/g/n）	√	
	AP6510DN（室外型，支持 802.11a/b/g/n）	√	
AC IP 地址规划	静态分配	√	-
	动态获取	-	-
AP IP 地址规划	静态分配	-	-
	动态获取	√	-
用户 IP 地址规划	静态分配	-	-
	动态获取	√	-
VLAN 和 SSID 映射关系	1:1	-	根据布网实际需要
	1:N	-	
	N:1	-	
	N:N	-	
DHCP Server 位置	独立 DHCP Server	√	-
	AC 上	-	-
AP 发现 AC 形式	Option 43	√	均可，根据实际需要
	Option 15	√	

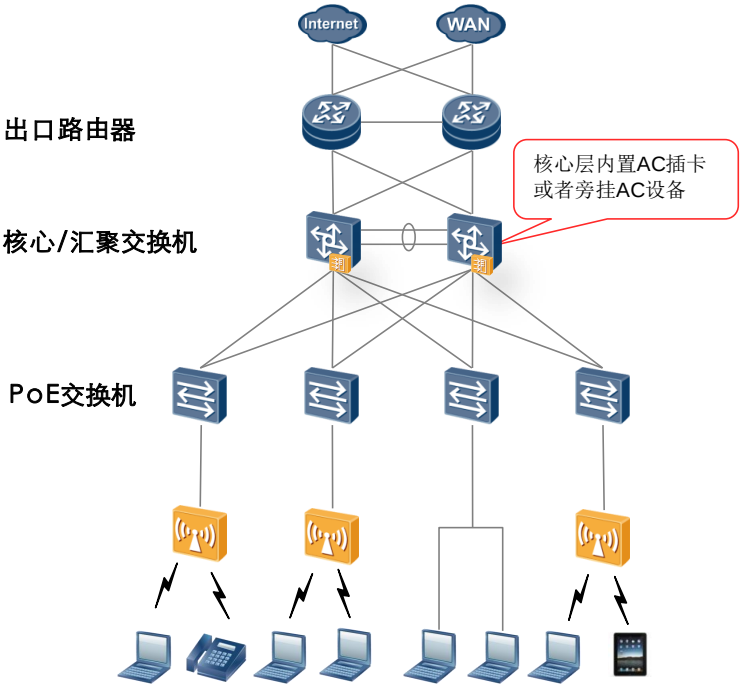
版权所有 © 华为技术有限公司

网络配置点	分类	推荐	备注
业务转发模式	独立转发	√	-
	隧道转发	-	-
认证方式	PSK 认证	-	-
	802.1x 认证	√	-
	Portal 认证	√	-
网管	eSight	√	-
认证授权计费	华赛 TSM 服务器	√	根据实际需要
	深澜服务器（国内计费）	√	
	计费网关（ME60 或 Srun3000）	√	
	第三方计费系统	√	

6.2 小型园区网 WLAN 部署方案

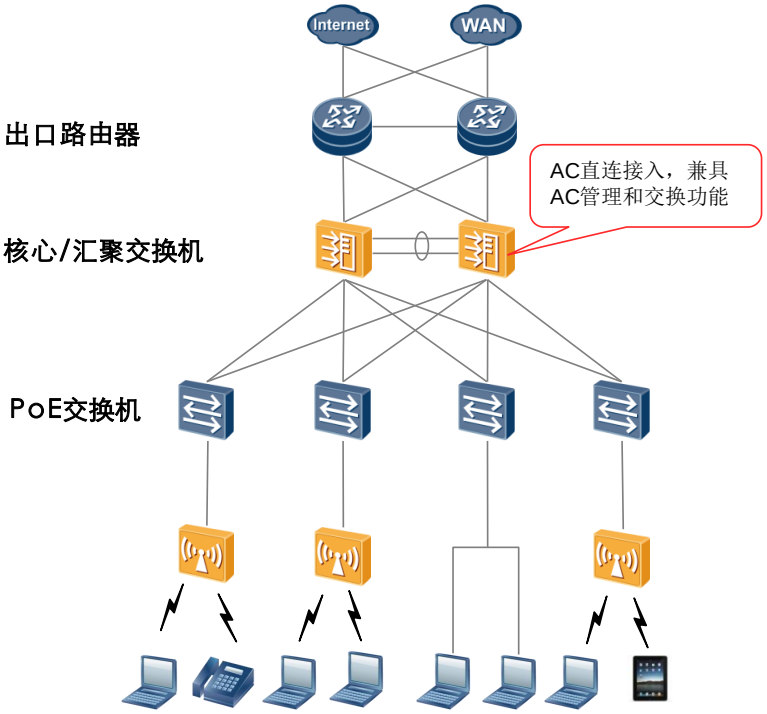
小型园区网定位为中小型企业无线园区网，网终端规模在 100～200 之间，也包括只在分支机构部署 WLAN 的场景。

图6-2 小型园区网（万兆）网络拓扑示意图



华为专有和保密信息
版权所有 © 华为技术有限公司

图6-3 小型园区网（普通）网络拓扑示意图



小型网络一般为核心/汇聚层合一的扁平化网络，可能由于成本因素较少考虑网络可靠性和网管系统。

对于小型万兆园区网，核心层采用框式交换机 S7700，内置 AC 插卡；对于普通小型园区网，可采用独立 AC 设备部署，如 AC6605 等。

对客户而言，本方案设计采用扁平化网络，具有架构简单的特点，并可以按需裁减备用设备、网管系统和服务器等设备达到节省投资的目的。

小型园区中 WLAN 网络部署规划主要配置推荐如下表所示：

表6-2 小型园区中 WLAN 网络部署规划推荐配置

网络配置点	分类	推荐	备注
网络架构	FAT AP	-	-
	FIT AP	√	-
AC 部署方式	集中式	√	-
	分布式	-	-
AC 部署位置	旁挂	√	均可，根据实际需要
	直路	√	
AC 硬件形式	集成 AC	√	小型万兆园区网络

版权所有 © 华为技术有限公司

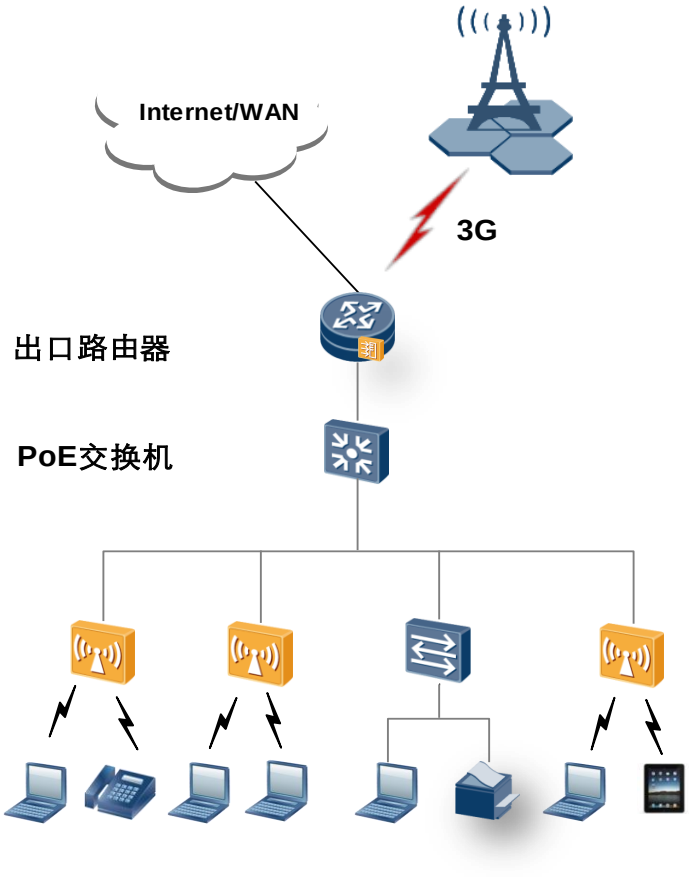
网络配置点	分类	推荐	备注
	独立 AC	√	可以采用集成AC；小型普通园区网络采用独立 AC。
AP 类型	AP6010SN（室内型，支持 802.11a/b/g/n）	√	均可，根据实际需要
	AP6010DN（室内型，支持 802.11a/b/g/n）	√	
	AP6510DN（室外型，支持 802.11a/b/g/n）	√	
AC IP 地址规划	静态分配	√	-
	动态获取	-	-
AP IP 地址规划	静态分配	-	-
	动态获取	√	-
用户 IP 地址规划	静态分配	-	-
	动态获取	√	-
VLAN 和 SSID 映射关系	1:1	-	根据布网实际需要
	1:N	-	
	N:1	-	
	N:N	-	
DHCP Server 位置	独立 DHCP Server	√	-
	AC 上	-	-
AP 发现 AC 形式	Option 43	√	均可，根据实际需要
	Option 15	√	
业务转发模式	独立转发	√	-
	隧道转发	-	-
认证方式	PSK 认证	√	-
	802.1x 认证	-	-
	Portal 认证	-	-
网管	eSight	-	可以不用专门的网管设备。
	单独维护	√	-

华为专有和保密信息
版权所有 © 华为技术有限公司

6.3 SOHO 型园区网络 WLAN 部署方案

本方案适用于 SOHO 型网络，SOHO 型（微小型）园区网终端规模在 100 以下，例如微型企业或者办事处等场景。

图6-4 SOHO 型园区网络拓扑示意图



SOHO 型园区一般采用出口、核心、汇聚融合的网络架构。使用 AR 集成 AC，如 AR1200 等接入路由器。

微型园区网络部署推荐如下表所示：

表6-3 SOHO 型园区中 WLAN 网络部署规划推荐配置

网络配置点	分类	推荐	备注
网络架构	FAT AP	-	-
	FIT AP	√	-
AC 部署方式	集中式	√	-
	分布式	-	-

华为专有和保密信息
版权所有 © 华为技术有限公司

网络配置点	分类	推荐	备注
AC 部署位置	旁挂	-	-
	直路	√	-
AC 硬件形式	集成 AC	√	AR G3 系列路由器集成 AC
	独立 AC	-	-
AP 类型	AP6010SN（室内型，支持 802.11a/b/g/n）	√	均可，根据实际需要
	AP6010DN（室内型，支持 802.11a/b/g/n）	√	
	AP6510DN（室外型，支持 802.11a/b/g/n）	√	
AC IP 地址规划	静态分配	√	-
	动态获取	-	-
AP IP 地址规划	静态分配	-	-
	动态获取	√	-
用户 IP 地址规划	静态分配	-	-
	动态获取	√	-
VLAN 和 SSID 映射关系	1:1	-	根据布网实际需要
	1:N	-	
	N:1	-	
	N:N	-	
DHCP Server 位置	独立 DHCP Server	√	-
	AC 上	-	-
AP 发现 AC 形式	Option 43	√	均可，根据实际需要
	Option 15	√	
业务转发模式	独立转发	√	-
	隧道转发	-	-
认证方式	PSK 认证	√	-
	802.1x 认证	-	-
	Portal 认证	-	-

版权所有 © 华为技术有限公司

7 WLAN 主要产品介绍

WLAN 系列产品主要包括 AC6605 盒式 AC 和 S9700/7700 ACU 插卡式 AC，以及 AP6010SN/DN，AP6310SN，AP6510DN，AP6610DN 等多款 AP。

7.1 AP6010SN 美观标准室内型单频 AP

图7-1 AP6010SN 产品实物图

产品规格

表7-1 AP6010SN 产品规格

项目	规格
IEEE 标准	802.11b/g/n 标准，支持 2.4GHz 频率
尺寸	180×180×50mm
重量	0.7kg
功耗	6.5W
供电	标准 802.3af
发射功率	100mW
天线	内置 2.4GHz 全向天线，增益 4dBi

版权所有 © 华为技术有限公司

主要性能

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11b/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

7.2 AP6010DN 美观标准室内型双频 AP

图7-2 AP6010DN 产品实物图

产品规格

表7-2 AP6010DN 产品规格

项目	规格
IEEE 标准	802.11a/b/g/n 标准，支持 2.4GHz 和 5GHz 频率
尺寸	180×180×50mm
重量	0.7kg
功耗	10.2W
供电	标准 802.3af
发射功率	100mW
天线	内置 2.4GHz 全向天线，增益 4dBi 内置 5GHz 全向天线，增益 5dBi

主要性能

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)

版权所有 © 华为技术有限公司

- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

7.3 AP6310SN 经济型室分单频 AP

图7-3 AP6310SN 产品实物图

产品规格

表7-3 AP6310SN 产品规格

项目	规格
IEEE 标准	802.11b/g/n 标准，支持 2.4GHz 频率
尺寸	240×200×40 mm
重量	1.5kg
功耗	6.5W
供电	标准 802.3af
发射功率	500mW

主要性能

- 20- 和 40-MHz 信道
- PHY 数据速率高达 150Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

版权所有 © 华为技术有限公司

7.4 AP6510DN 标准室外双频 AP

图7-4 AP6510DN 产品实物图

产品规格

表7-4 AP6510DN 产品规格

项目	规格
IEEE 标准	802.11a/b/g/n 标准，支持 2.4GHz 和 5GHz 频率
尺寸	265×265×83mm
重量	3.0kg
功耗	24W
供电	标准 802.3af
发射功率	2.4GHz-500mW 5GHz-125mW

主要性能

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

版权所有 © 华为技术有限公司

7.5 AP6610DN 全规格室外双频 AP

图7-5 AP6610DN 产品实物图

产品规格

表7-5 AP6610DN 产品规格

项目	规格
IEEE 标准	802.11a/b/g/n 标准，支持 2.4GHz 和 5GHz 频率
尺寸	265×265×83mm
重量	3.5kg
功耗	28W
供电	非标准 802.3at
发射功率	2.4GHz-500mW 5GHz-125mW
接口	支持 SFP 接口，支持交流本地供电

主要性能

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

版权所有 © 华为技术有限公司

7.6 AC6605

图7-6 AC6605 产品实物图

AC6605 产品有如下特点：

- 高性能
  - 支持快速漫游（缓存 PMK）
  - 高达 512 APs 管理能力
- 高可靠
  - AC 设备间 1+1 双链路备份
  - 上行链路 LACP、MSTP 50ms 保护
  - 双电源接口，备份保护
  - 风扇、电源热插拔，高温告警保护
- 强大的组网和业务能力
  - 丰富接口：2 个 10GE 光接口，4 个 GE Combo 接口，24 个 GE 电口。
  - 业务强大：精细化 QoS、丰富 L2/L3 功能、标准 MIB 接口。
- 保护投资
  - 无缝适应 WLAN 11b/g 和 11n
  - 华为标准软件平台，和宽带城域设备无缝融合

7.7 S9700/S7700 ACU 插卡

图7-7 S9700/S7700 ACU 插卡实物图

S9700/S7700 ACU 插卡支持如下功能：

- AP 管理与用户接入
  - 大容量：每块 ACU 插卡支持管理 1024 个 AP，最大可支持管理 11K 个 AP
  - 支持按模板批量配置 AP

版权所有 © 华为技术有限公司

- 灵活多样的用户认证模式：MAC、Portal 和 802.1x、Portal 免认证
- 支持全局调优、局部调优和射频捕盲

- 安全及权限控制
  - 丰富灵活的用户权限控制，支持用户分组、隔离、ACL 等。
  - 支持多种安全协议标准：WEP、WPA/WPA2(PSK/1X)、WAPI
  - 支持密钥管理，支持 AP 黑名单
  - 防 STA IP 地址仿冒、ARP 攻击（DAI）、DHCP 服务器仿冒
- 无线网络
  - 支持 CAPWAP 隧道协议、线速转发
  - 支持 WMM、优先级映射、CAR、流级别定义，支持负载分担和 AC 备份
  - 灵活的组网模式（本地转发/集中转发、二三层组网）、WDS 网络部署

版权所有 © 华为技术有限公司