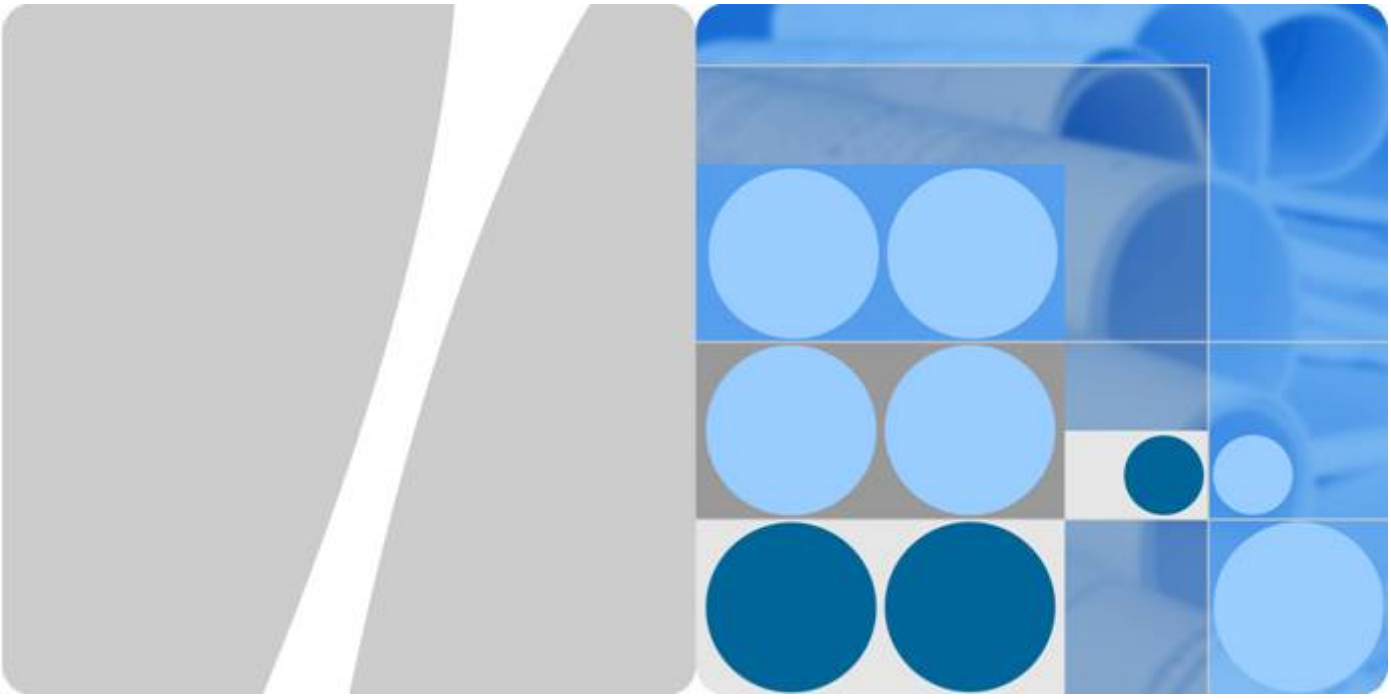


集中认证+本地转发

技术白皮书

文档版本　01

发布日期　2012-10-31

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://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 4008229999

前 言

修订记录

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

文档版本 01 (2012-10-31)

第一次正式发布。

目 录

1 介绍

定义

集中认证、本地转发是指 STA 认证报文通过隧道转发到 AC，STA 业务报文不通过隧道，经网关直接转发，实现在 AC 上对无线用户的集中接入控制功能，同时节约 AP 上行的广域网或 Internet 的出口带宽。

目的

大容量 AC 集中部署的场景，AC 全部位于网络核心层，通过 Internet 与各分支互联。集中认证、本地转发主要实现在三层组网中能采用 802.1X 认证或 Portal 认证，具体可以针对性的解决以下场景存在的问题：

1. 对于 AC 和 AP 之间是三层网络，直接转发的场景，802.1X 或 Portal 等接入控制点无法部署在 AC 上。AC 无法实现对无线用户的集中接入控制功能，导致无线空口控制和用户的接入控制分离。
2. 对于 AC 和 AP 之间是三层网络，隧道转发的场景，802.1X 或 Portal 等接入控制点可以部署在 AC 上。但是所有数据都走隧道，即使本地互访也会受 AP-AC 间链路带宽限制。
3. 对于 AC 和 AP 之间是三层网络，直接转发的场景，802.1X 或 Portal 等接入控制点部署在 Switch 上。成本和管理维护花费高，不容易部署和管理。

受益

集中认证、本地转发可以实现在三层组网中能采用 802.1X 认证或 Portal 认证，并在 AC 上对无线用户的集中接入控制功能，利于部署和管理，降低了成本和管理维护费用，节约 AP 上行的广域网或 Internet 的出口带宽。

2 原理描述

关于本章

对于 802.1X 和 Portal 认证用户，存在三种转发-认证方式：

- 本地转发-本地认证
- 集中转发-集中认证
- 本地转发-集中认证

本地转发-本地认证方式

这种模式下，认证控制点在 AP 上行的交换机设备上。只有 AC 与 AP 之间的控制报文走 CAPWAP 隧道，STA 认证协议报文（如 802.1X、Portal 认证）和认证后的 STA 业务数据报文不走 CAPWAP 隧道，经 AP 直接转发。

缺点：

- 802.1X 认证时的 EAP 报文和 Portal 认证时的 HTTP 报文都为二层认证报文，这就要求 STA 与认证控制点之间必须是二层网络，认证控制点往往部署在 AP 上行的交换机上，控制点不集中导致设备成本高，管理维护复杂；
- 802.1X 等认证控制点没有集中部署在 AC 上。AC 无法实现对接入用户的集中控制；
- 业务数据报文和认证协议报文存在安全隐患。

优点：

- 本地互访直接在 AP 上进行转发，无需经过 AC，节省 AP 上行带宽；
- 业务数据报文和认证协议报文都无须 CAPWAP 隧道封装，节省 AP 上行带宽。

集中转发-集中认证方式

这种模式下，认证控制点在 AC 设备上。AC 与 AP 之间的控制报文、STA 认证协议报文（如 802.1X、Portal 认证）、认证后的 STA 业务数据报文全部走 CAPWAP 隧道。

缺点：

802.1X 和 Portal 等接入控制点可以部署在 AC 上，但是所有数据都走 CAPWAP 隧道，即使本地互访也会受 AP-AC 链路带宽限制。

优点：

- 安全性高；
- AC 能够实现对无线用户的集中接入控制。

本地转发-集中认证方式

这种模式下，认证控制点在 AC 设备上，可通过配置，让 STA 认证报文（如 802.1X、Portal 认证）进入 CAPWAP 隧道，从而上送到 AC 设备，完成认证过程。而认证后的 STA 业务数据报文不通过隧道，经 AP 直接转发。

缺点：

相对于集中转发方式，业务数据报文安全性欠佳。

优点：

- 实现在 AC 上对无线用户的集中接入控制功能，主要包括用户的隔离、限速、ACL；
- 授权通过 CAPWAP 隧道下发到 AP 设备，提升网络安全性；
- 本地互访直接在 AP 上进行转发，无需经过 AC，节省 AP 上行带宽。

通过以上比较，如果需要在三层组网中实现 802.1X 和 Portal 认证，同时对链路带宽要求较高，可以选择本地转发-集中认证方式。

2.1 认证方式

2.2 数据转发方式

2.3 集中认证、本地转发

2.1 认证方式

2.1.1 802.1X 认证

802.1X 认证，又称 EAPOE（Extensible Authentication Protocol Over Ethernet）认证，主要目的是为了解决局域网用户的接入认证问题。

IEEE 802.1X 标准（以下简称 802.1X）的主要内容是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1X 协议仅关注接入端口的状态。当合法用户（根据帐号和密码）接入时，该端口打开；当非法用户接入或没有用户接入时，该端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题，是各种认证技术中最简化的实现方案。

802.1X 不仅支持基于端口的认证模式，还支持基于 MAC 的认证模式。

- 基于端口模式：当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源。但是当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 模式：当采用基于 MAC 地址方式时，该端口下的所有接入用户均需要单独认证。

802.1X 支持两种认证方式：

- EAP 终结认证：由网络接入设备终结用户的 EAP 报文，解析出用户名和密码，并对密码进行加密，再发送到 RADIUS 服务器进行认证。
- EAP 透传认证：也叫 EAP 中继认证，由网络接入设备直接把 802.1x 用户的认证信息以及 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证。

EAP 本身不是一个认证机制，而是一个通用架构。用来传输实际的认证协议。EAP 的好处就是当一个新的认证协议发展出来的时候，基础的 EAP 机制不需要随着改变。目前有超过 20 种不同的 EAP 协议。

802.1X 认证时的 EAP 报文为二层认证报文，在 AP 与 AC 间为三层组网且 AP 配置为直接转发模式的场景下，报文不能通过三层转发，会造成认证失败。使能协议报文隧道转发功能后，AP 将用户的 EAP 报文进行隧道封装，通过隧道转发给 AC 处理，在 AP、AC 之间实现认证报文的交互。

2.1.2 Portal 认证

Web 认证也称 Portal 认证，其基本原理是：用户首次打开浏览器，输入任何网址，都被强制重定向到 Portal 服务器的认证页面，只有在认证通过后，用户才能访问网络资源。未认证用户只能访问特定的站点服务器。Portal 认证通过 Web 页面输入用户名和密码，使用 Portal 协议完成认证过程。

Portal 协议主要用于 Portal 服务器和其他设备之间的信息交互。Portal 协议基于客户端/服务器结构，采用 UDP 作为传输协议。在 Portal 认证中，Portal 认证服务器和 AC 之间的通信使用 Portal 协议，AC 为客户端。Portal 认证服务器从认证页面中将用户输入的用户名和密码提取后，通过 Portal 协议传送给 AC。

Portal 认证实现机制，可分为直接认证方式和三层认证方式两种。

直接认证方式

用户 PC 与设备直连（或之间只有二层设备存在），设备能够学习到认证客户端的 MAC 地址，则设备可以利用 IP 和 MAC 地址来识别用户，此时配置 Portal 认证为直接认证方式。

直接认证流程简单，安全性高，实现起来也不会太复杂。但由于限制了用户 PC 只能与接入设备直连（或加二层设备），降低了组网的灵活性。

三层认证方式

当设备部署在汇聚层或核心层时，在认证客户端和设备之间存在三层转发设备，此时设备不一定能获取到认证客户端的 MAC 地址，所以以 IP 地址唯一标识用户，此时需要 Portal 认证配置为三层认证方式。

三层认证组网灵活，容易实现远程控制，但由于只有 IP 可以用来标识一个用户，所以安全性不高。

Portal 认证时的 HTTP 报文为二层认证报文，在 AP 与 AC 间为三层组网且 AP 配置为直接转发模式的场景下，报文不能通过三层转发，造成认证失败。使能协议报文隧道转发功能后，AP 将用户的 HTTP 认证报文进行隧道封装，通过隧道转发给 AC 处理，在 AP、AC 之间实现认证报文的交互。

2.2 数据转发方式

WLAN 网络中的数据包括控制消息和数据消息，其转发方式包括直接转发（又称为“本地转发”）和 CAPWAP 隧道转发（又称为“集中转发”）。

CAPWAP 隧道转发

2005 年，IETF 成立了 CAPWAP（Controlling and Provisioning of Wireless Access Point，无线接入点控制与供应）工作组以标准化 AP 和 AC 间的隧道协议，定义了 AP 发现 AC 等基本协议功能，即 CAPWAP 协议。

CAPWAP 消息包括“控制消息”和“数据消息”，二者基于不同的 UDP 端口发送，分别对应“控制隧道”和“数据隧道”。

CAPWAP 隧道有心跳检测机制和 DTLS 加密功能，为 CAPWAP 隧道提供安全保障。CAPWAP 协议规定控制隧道的 DTLS 为必选，数据隧道为可选。

CAPWAP 隧道转发又称为集中转发，即 AP 与 AC 间的报文经过 CAPWAP 隧道封装后再转发到上层网络，从而提高报文的转发安全性。

本地转发

直接转发又称为数据本地转发，即 AP 与 AC 间的报文没有经过 CAPWAP 隧道封装，直接转发到上层网络，从而提高报文的转发效率。

直接转发指 AP 不会对数据报文进行任何处理，发送原始报文。

应用说明

AP 与 AC 间的控制报文必须采用 CAPWAP 隧道进行转发，而数据报文除了可以采用 CAPWAP 隧道转发之外，还可以采用直接转发方式。

数据报文采用 CAPWAP 隧道转发的配置方法：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name ChinaNet
[Quidway-wlan-service-set-ChinaNet] forward-mode tunnel
```

数据报文采用直接转发的配置方法：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name ChinaNet
[Quidway-wlan-service-set-ChinaNet] forward-mode direct-forward
```

数据报文采用 CAPWAP 隧道转发方式，具有以下优势：

- AP 与 AC 之间的网络设备上无需进行 WLAN 业务 VLAN 的配置，组网简单、容错率高。
- CAPWAP 封装后的报文，进行了 DTLS 加密，业务报文更加安全。
- WLAN 业务报文通过 CAPWAP 隧道上送到 AC，由 AC 来集中转发，已经成为当今 WLAN 网络的主流转发方式。相比直接转发，所有 WLAN 的业务报文，必须经过 AC 才能转发出去，可以通过 AC，专门针对无线报文进行限速、监控、分析、过滤。

数据报文采用直接转发方式，具有以下优势：

- 可以根据现场网络环境灵活组网。
- WLAN 业务报文不会上送到 AC，AC 所受压力小。

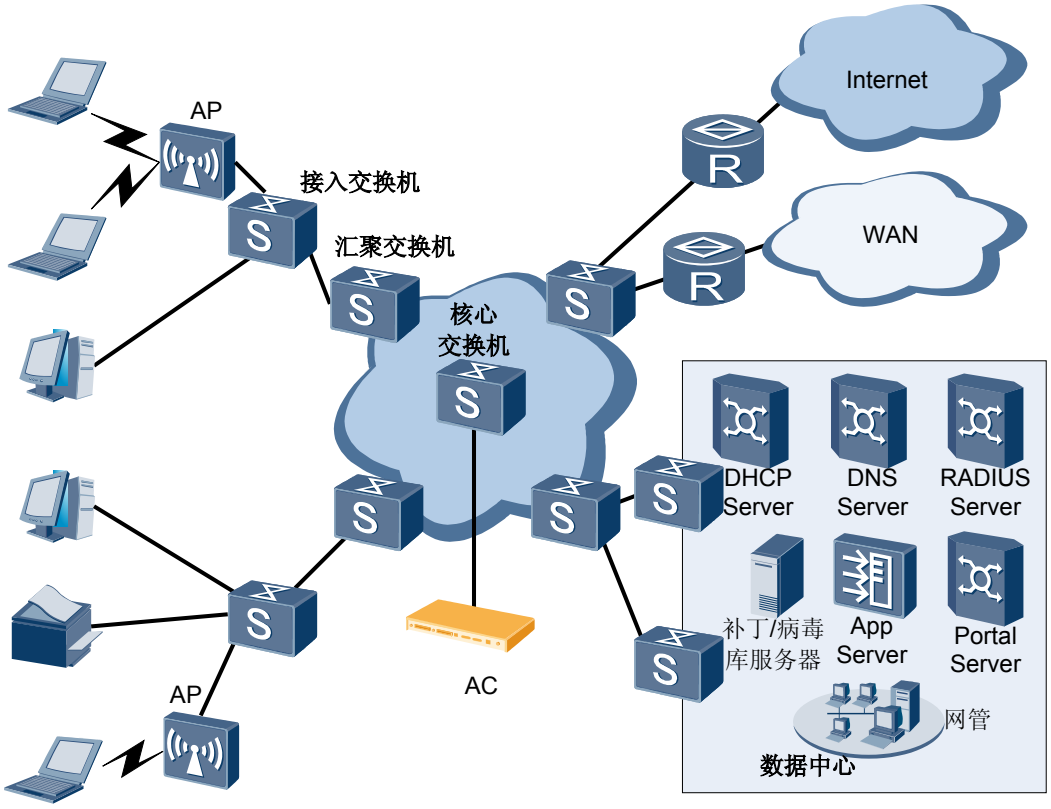
当 AC 为旁挂式组网（即 AC 的业务接入端口和上行端口为同一个以太网端口）时，如果数据是直接转发，则数据流不经过 AC；如果数据是隧道转发模式，则数据流经过 AC。

2.3 集中认证、本地转发

实际应用

大中型园区网的集成 AC 组网方案如图 2-1 所示。（以旁挂方式为例）

图 2-1 大中型园区网集中式 AC 方案



大中型园区网中，AP 数量众多，一般 AP 和 AC 之间属于三层组网。若采用 CAPWAP 隧道转发方式，所有的数据信息和控制信息都会由 CAPWAP 隧道到达 AC，由于 CAPWAP 隧道带宽限制，会直接影响到用户的网络信息传输速率。所以一般可以采用本地转发方式，只有控制信息才会到达 AC。

本地转发场景下，由于 AP 和 AC 之间是三层组网，802.1X 认证时的 EAP 报文和 Portal 认证的 HTTP 报文为二层认证报文，报文不能通过三层转发，802.1X 或 Portal 等接入控制点无法部署在 AC 上。AC 无法实现对无线用户的集中接入控制功能，导致无线空口控制和用户的接入控制分离。如果 802.1X 或 Portal 等接入控制点部署在 Switch 上。成本和管理维护花费高，不容易部署和管理。

采用集中认证、本地转发，用户使用 802.1X 认证或 Portal 认证方式时发送的认证报文都经过 CAPWAP 封装，发送给 AC，实现由 AC 统一认证的功能，解决了以上的难题。

使能 802.1X 认证报文的隧道转发功能方法：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name huawei
[Quidway-wlan-service-set-huawei] tunnel-forward protocol dot1x
```

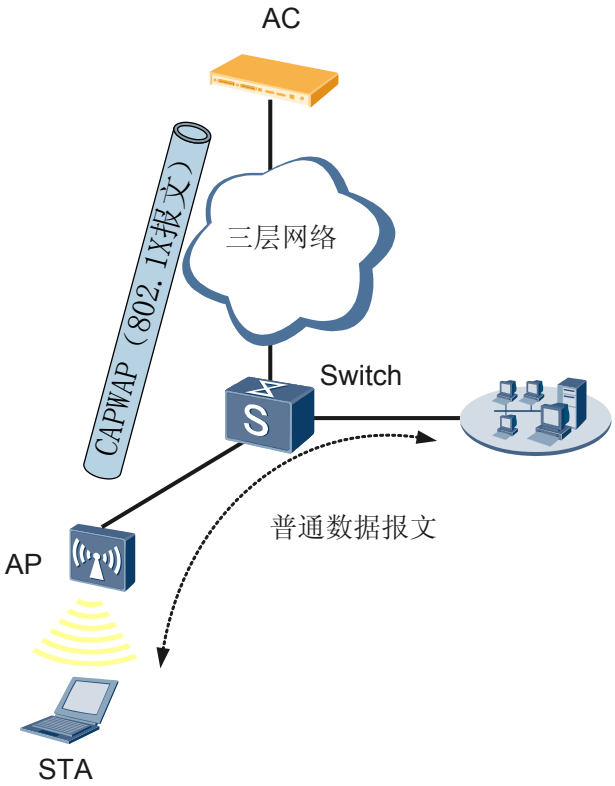
使能 Portal 认证报文的隧道转发功能方法：

```
<Quidway> system-view
[Quidway] wlan
[Quidway-wlan-view] service-set name huawei
[Quidway-wlan-service-set-huawei] tunnel-forward protocol http
```

基本流程

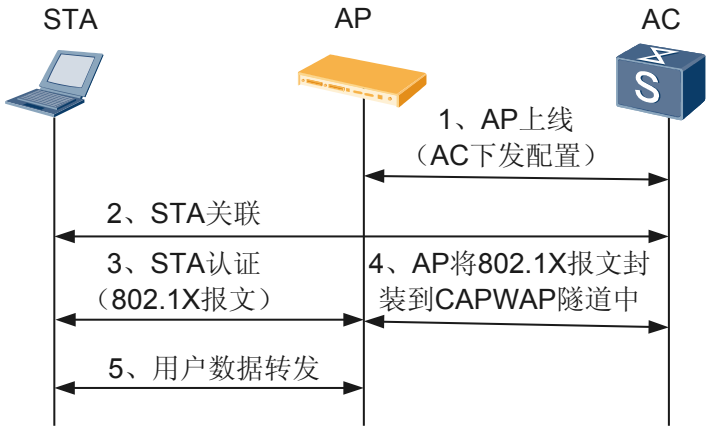
集中认证、本地转发的组网图如图 2-2 所示，所有 STA 的认证点均在 AC，STA 通过 802.1X 认证方式接入到网络，STA 访问网络的数据通过 AP 直接处理，不需要经 AC 转发。

图 2-2 集中认证、本地转发组网图



集中认证，本地转发的基本流程如图 2-3 所示：

图 2-3 集中认证、本地转发的基本流程



集中认证，本地转发的基本流程：

1. AP 通过广播或者单播方式发现 AC 上线，AC 下发配置的数据转发模式、以及 Dot1x 报文的转发方式给 AP。
2. STA 关联到 AC。
3. STA 进行 802.1X 认证，发送 Dot1x 报文到 AP。
4. AP 收到用户的 Dot1x 报文，AP 会将 Dot1x 报文封装到 CAPWAP 隧道中转发给 AC。AC 解封装隧道后进行认证或者转发处理。AC 给用户的 Dot1x 回应也需要封装隧道。
5. 用户认证成功后，进行数据转发。AP 根据配置的数据转发模式进行转发。本地转发时候，AP 不需要对用户数据封装 CAPWAP 隧道。

3 应用

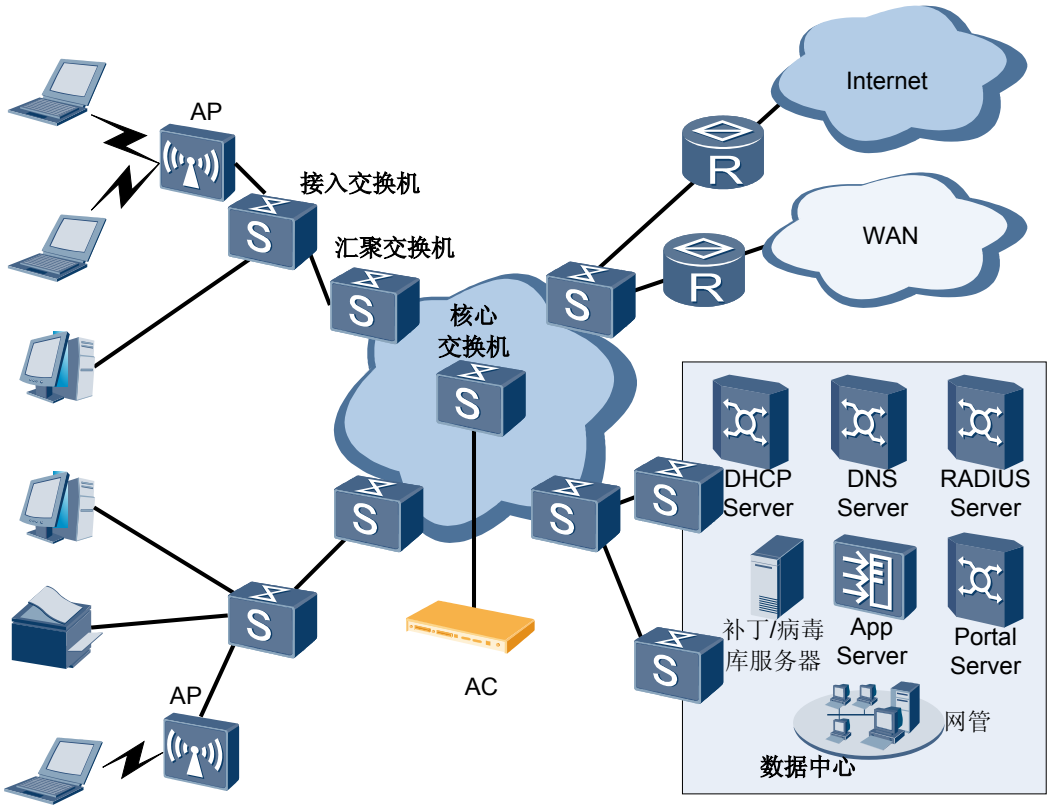
关于本章

3.1 集中认证、本地转发应用实例

实际应用

某大中型园区网的集成 AC 组网方案如图 3-1 所示。AP 与 AC 间为三层网络。AP 通过接入交换机，汇聚交换机，连接到核心交换机，再与 Internet、WAN、各类服务器互连。AP 下接入大量的 STA，用户使用 802.1X 认证或 Portal 认证，不希望网络速度受到影响，另外为方便网络管理员管理，期望能够在 AC 上集中管理 AP。

图 3-1 大中型园区网集中式 AC 方案



配置分析

- 采用集中认证+直接转发方式，在用户众多的情况下，可以保证用户的网络速度，并且实现在 AC 上集中管理 AP 的功能，方便维护和管理。
- 在 AC 上使能 802.1X 认证报文或 HTTP 认证报文的隧道转发功能。
- 汇聚交换机上配置业务 IP 地址池，AC 无线侧配置管理 IP 地址池。分别为 STA 和 AP 分配 IP 地址。

采用如下思路进行配置：

1. 配置接入交换机，汇聚交换机，核心交换机和 AC，使 AP 和 AC 互通。
   - 接入交换机直接接 AP 的端口，需要打管理 VLAN tag。AP 上为零配置。

- 接入交换机到 AC 之间要配置业务 VLAN 互通和管理 VLAN 互通。
- 汇聚交换机或核心交换机作为 STA 的 DHCP 服务器。汇聚交换机或核心交换机上配置 STA 的网关地址，STA 的网关地址不能配置在 AC 无线侧。
- AC 作为 AP 的 DHCP 服务器。AP 采用 DHCP relay 的方式去 AC 无线侧申请 IP 地址，AP 的网关可放在交换机上。
- 配置 AC 有线侧和无线侧的互通。

2. 在 AC 无线侧配置 WLAN 相关业务。
   - 配置 AC 全局参数（运营商标识、ID、国家码）和 AC 的源接口。
   - 配置 AP 地址池。
   - 配置 AP 的认证方式并使 AP 上线，加 AP 加入指定域。
   - 配置 WLAN-ESS 虚接口。
   - 配置射频模板并绑定到射频中
   - 配置安全模板，流量模板，配置服务集，配置转发方式为直接转发。并使能 EAP 报文的隧道转发功能。
3. 业务下发 AP。
   - 配置 AP 对应的 VAP 并下发配置。