华为WLAN认证概述

HUAWEI

前言

- 根据WLAN从业者的学习和进阶需求，华为WLAN认证分为工程师级别、高级工程师级别和专家级别三个认证等级。
- HCIA课程聚焦WLAN基础技术，旨在让WLAN从业者对于WLAN概念、发展、历史、无线通信的工作原理以及WLAN简单部署有所了解。
- HCIP课程聚焦WLAN现网技术及网规网优，旨在提升WLAN工程师对于现网常用技术的理解，且能够熟练掌握WLAN网规网优技巧，从容应对现网项目。
- HCIE课程聚焦WLAN解决方案，旨在让WLAN资深工程师熟悉传统WLAN解决方案的同时，对于高级技术、新技术、新解决方案都能有新的认识，胜任WLAN网络架构师工作。

目标

- 学完本课程，您将能够：
  - 描述华为WLAN技术模块
  - 描述华为WLAN职业认证架构
  - 熟悉HCIE-WLAN课程架构
  - 熟悉HCIE-WLAN考点

目录

华为WLAN技术全景图

WLAN技术基础

WLAN技术基础

- 无线通信的基本概念
- 802.11标准介绍
- WLAN的关键技术
- Wi-Fi 6技术
- WLAN常见报文与工作原理
- WLAN安全基础
- WLAN天线基础
- WLAN基本配置
- WLAN网络部署介绍

WLAN常见技术应用及网规网优

WLAN可靠性技术

- WLAN可靠性技术
- WLAN配置同步技术
- WLAN N+1备份技术

WLAN漫游技术

- WLAN漫游技术
- WLAN快速漫游
- WLAN智能漫游

WLAN安全技术

- PSK/PPSK
- 802.1X认证
- Portal & MAC地址认证

WLAN常见场景

- 办公场景
- 酒店、宿舍等十多个场景

WLAN网络规划设计

- WLAN网络规划与设计方法
- WLAN网规工具及输出件

WLAN网络优化

- WLAN网络优化技术
- WLAN网络优化工具

WLAN解决方案

WLAN传统园区解决方案

- WLAN可靠性技术
- WLAN漫游技术
- WLAN安全技术
- WLAN网络管理

WLAN新解决方案

- SDN技术
- WLAN定位技术
- WLAN智能运维
- 云管解决方案
- WLAN与物联网技术
- WLAN IPv6组网

华为WLAN职业认证全景图

深入掌握WLAN技能，融合解决方案设计，助力WLAN专家养成。

运筹帷幄，构建WLAN解决方案

WLAN高级技术应用 ✚ WLAN项目部署 ✚ WLAN解决方案

高级岗位

WLAN专家工程师

专注技术应用与网络规划设计，深入讲解，注重实践。

两大领域，深耕实战技能

WLAN技术应用

- 可靠性技术原理与部署
- 漫游技术原理与部署
- 安全技术原理与部署
- 射频资源管理原理与技术

WLAN网规网优

- WLAN十大典型组网建网标准
- WLAN网络规划与设计方法
- WLAN网规工具及输出件
- WLAN网络优化技术

中级岗位

WLAN高级工程师

理论基础，新手入门，掌握WLAN运维基本知识。

五大模块，推开WLAN大门

无线通信技术概念与技术 | WLAN网络技术基础 | WLAN安全技术基础 | WLAN网络配置与部署 | WLAN项目部署介绍

初级岗位

即将从事相关领域的工作者或技术爱好者

HCIE-WLAN考试组成

笔试：H12-351

考点：全国VUE考点

试题数量：60

考试时长：90分钟

Lab：H12-352

考点：深圳/成都/北京/杭州

考试时长：8小时

HCIE-WLAN课程框架

HCIE-WLAN考试注意事项

笔试注意事项

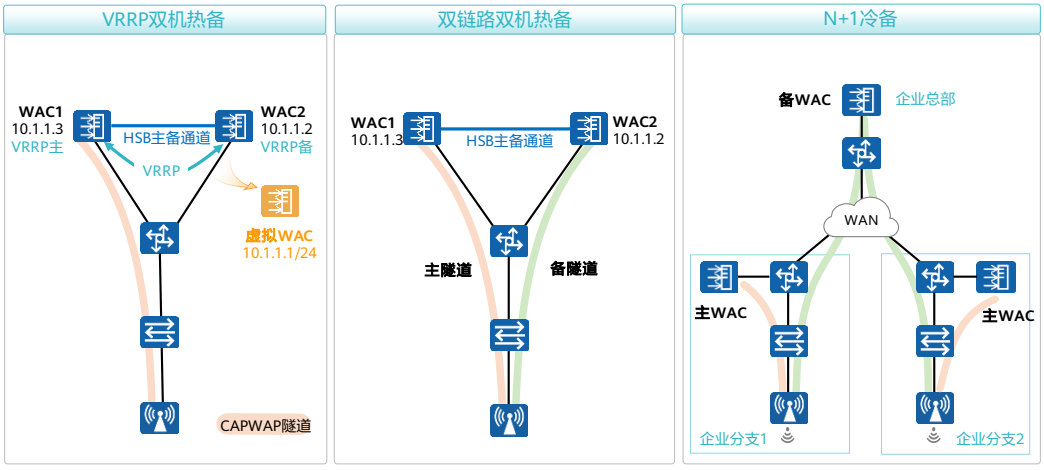
- 熟悉课程内容
- 结合产品文档复习
- 包含判断、单选、多选、拖拽以及填空题。

上机考试注意事项

- 上午考察WLAN网络规划。
- Lab配置过程中建议及时保存。

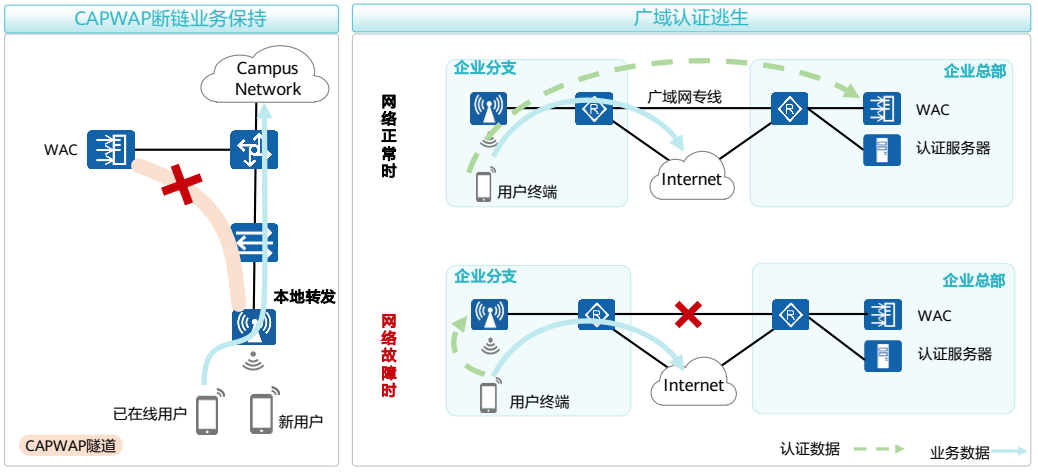
目录

WLAN组网可靠性



HUAWEI

WLAN业务可靠性



HUAWEI

- 广域认证逃生通常应用在总部分支网络中，由于总部分支中间跨广域网，在传统解决方案中，WLAN很多业务都是集中到AC处理，这就对总部分支之间的广域网提出了很高的要求，如高带宽、低时延、高稳定性。而实际场景中，很多总部分支之间并不是使用企业专线，而是租用运营商网络，中间网络质量无法保证，从而带来网络安全性差、用户业务体验差等问题。针对上述问题，华为WLAN提出了全新的解决方案，通过在分支建立分支AP组，将用户接入、接入认证等业务下移至AP处理，减少分支对总部的依赖，对于分支与总部断开连接的情况，也能保证分支用户能够继续使用WLAN网络。

目录

提升无线用户体验的WLAN技术

高密覆盖
100/AP ->400/AP

高密接入控制技术

双频DFA算法，多用户并发性能提升30%。

SmartRadio智能漫游负载均衡

主动优化80%弱覆盖用户。

VR/高清视频
100 Mbps/人，时延低至15 ms

智能调度技术

SmartRadio智能冲突优化，有序调度用户业务，时延低至15ms。

移动办公
200 m^2/AP

智能天线技术

高达232种波束组合，实时干扰检测，灵活调整覆盖方向，覆盖距离提升20%。

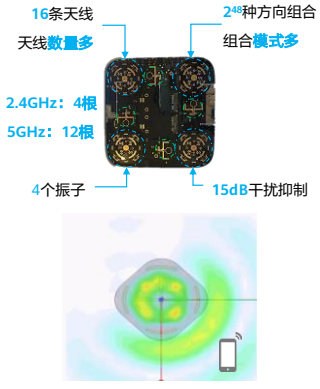
射频调优

- WLAN网络中，AP的工作状态会受到周围环境的影响。例如，当相邻AP的工作信道存在重叠频段时，某个AP的功率过大会对相邻AP造成信号干扰。通过射频调优功能，动态调整AP的信道、功率和频段等，可以使同一AC管理的各AP保证覆盖的同时又能尽量避免干扰，保证AP工作在最佳状态。

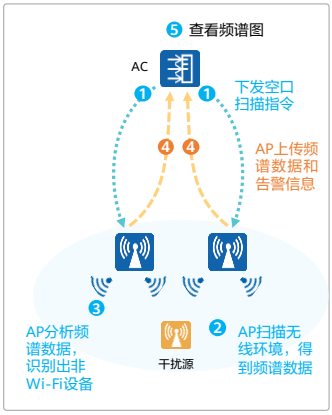
当网络规模过大时，手动进行射频资源调优时，工作量大，建议使用自动调优方式。

WLAN抗干扰技术

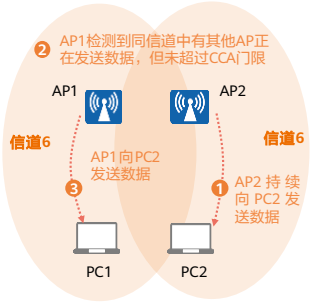
智能天线



频谱分析



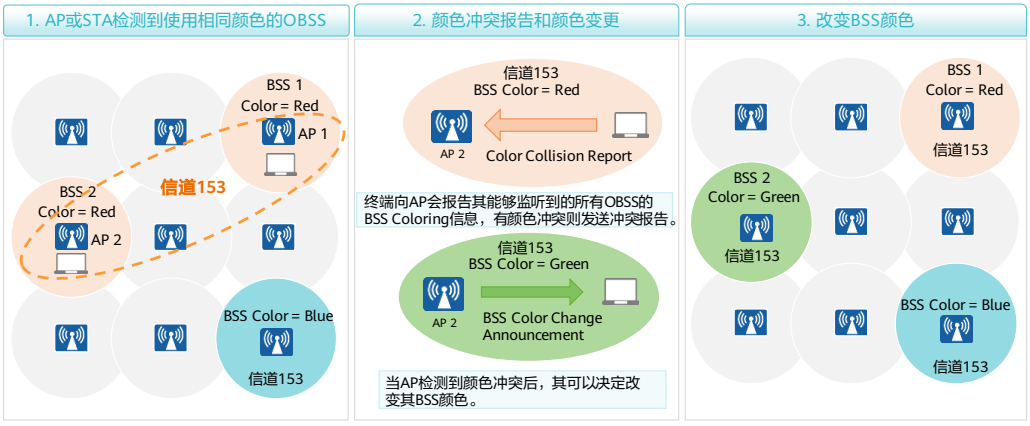
空闲信道评估CCA



HUAWEI

802.11ax BSS Coloring

- BSS Coloring是一种解决重叠基本服务集（OBSS）带来的负面影响，从而提升空间重用率的方法，减少因为重叠BSS导致的MAC层竞争开销，其目标是提升空间复用率，同时不会因为BSS间的干扰而导致节点间PHY层传输速率的降低。



HUAWEI

- 对于802.11ax的AP，其如果检测到使用相同颜色的OBSS，则它能够更改变其BSS颜色，减少同频干扰。若AP与AP间的BSS Coloring一样，那么这也是一种BSS Coloring的冲突，即颜色冲突。如上图所示，如果802.11ax AP听到来自其他AP或者该AP节点的不同BSS Coloring字段，那么是检测到一次颜色冲突。
- 另外，如果终端检测到颜色冲突，则该终端会向其关联的AP发送颜色冲突报告。终端向AP会报告其能够监听到的所有OBSS的BSS Coloring信息。
- AP会通过Beacon告知所有关联在本BSS内部的节点，BSS Coloring的改变。BSS Coloring的改变还可以通过探测响应和重新关联响应帧中进行通知。图中，AP告知节点BSS Coloring的颜色变化，其New BSS Color子字段则包含新BSS Coloring的数值。
- 当AP检测到颜色冲突后，其可以决定改变其BSS颜色。不过改变BSS Coloring的标准和选择新BSS Coloring信息的方法超出802.11ax草案修正案的范围。WLAN供应商目前可以自行制定，例如Aerohive信道选择协议（ACSP）。
- AP会通过Beacon告知所有关联在本BSS内部的节点，BSS Coloring的改变。BSS Coloring的改变还可以通过探测响应和重新关联响应帧中进行通知。如上图所示，AP告知节点BSS Coloring的颜色变化，其New BSS Color子字段则包含新BSS Coloring的数值。

TWT

- TWT（Target Wakeup Time，唤醒时间调度）是由802.11ah标准首次提出，初衷是针对IoT设备，尤其是低业务量的设备（例如智能电表等）设计的一套节能机制，使得IoT设备能够尽可能长时间地处于休眠状态，从而实现极低功耗的目的。

区别于过去的Wi-Fi标准，Wi-Fi 6具有支持TWT的新特性，其允许AP告知客户端何时休眠，并给客户端提供何时唤醒的调度表。每次客户端休眠的时间虽然很短，但多次这样的休眠会明显延长设备的续航时间。

HUAWEI

- 每一代新的Wi-Fi标准都可以延长客户端的续航时间，因为数据传输的距离更长、速度更快，因此客户端可以实现更低的功耗。然而区别于过去的Wi-Fi标准，Wi-Fi 6还支持一项称为“唤醒时间调度（TWT）”的新特性，其允许AP告知客户端何时休眠，并给客户端提供何时唤醒的调度表。每次客户端休眠的时间虽然很短，但多次这样的休眠会明显延长设备的续航时间。
- TWT（Target Wakeup Time）：按需唤醒终端Wi-Fi，终端功耗可降低30%。
- TWT是由802.11ah标准首次提出，初衷是针对IoT设备，尤其是低业务量的设备（例如智能电表等）设计的一套节能机制，使得IoT设备能够尽可能长时间地处于休眠状态，从而实现极低功耗的目的。建立TWT协议后，站点无须接收Beacon帧，而是按照一个更长的周期醒来。802.11ax标准对其进行改进，引入了一些针对站点行为的规则，在满足节能的前提下实现了对信道接入的管控。TWT分为单播TWT和广播TWT。

目录

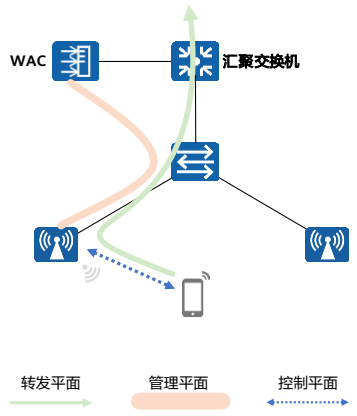
Wi-Fi真的不安全?

容易受到攻击　　数据容易泄露　　网络入口容易破解

如何应对?

不以方便为借口	最小的特权	纵深防御	攻防博弈论
方便与安全通常是对立的，公共场合的Wi-Fi一般只为方便忽略了安全。	不要给予用户太多不需要的特权。	认证，授权，加密，入侵防御，端点完整性。	没有任何一种设备或者协议是永保安全的，安全是动态的，只有不断更新才是保证安全的唯一法则。

WLAN网络架构及安全方案



管理平面安全	**1. 内容：** 关注管理用户的应用和业务数据的安全，即管理信息的安全。 **2. 威胁：** 擅自访问和滥用系统功能做非法操作等。 **3. 缓解措施：** AAA、HWTATACS用户管理、SSH、SNMPv3、HTTPS、DTLS等。
控制平面安全	**1. 内容：** 关注设备运行的各种协议的安全 **2. 威胁：** ARP/ICMP/TCP/UDP/泛洪引起的CPU超载等 **3. 缓解措施：** WPA/WPA2/WPA3、WIDS、WIPS、URL过滤、入侵检测、反病毒。
转发平面安全	**1. 内容：** 关注转发路径上数据安全，防止攻击在网络中扩散。 **2. 威胁：** DoS/DDoS攻击、ARP/IP欺骗引起不能正常工作等。 **3. 缓解措施：** 流量抑制、防MAC地址漂移、端口隔离、CAPWAP数据隧道加密、Navi AC、IPSec VPN。

HUAWEI

- 为了实现网络安全，华为参考了ITU-T X.805通用安全模型，根据网络中的不同数据流，将网络分为管理、控制、用户三个平面，每个平面根据网络层次分为设备、网络、应用三个层次，提出了分平面、分层的华为网络安全架构模型，用来指导各大解决方案进行网络安全威胁分析和制定安全策略、方案。
  - 管理平面：关注管理用户的应用和业务数据的安全，即管理信息的安全，包括操作、维护和管理信息。
  - 控制平面：WLAN设备需要运行各种各样的协议来达成业务，这些协议自身需要考虑安全性，避免被攻击或者仿冒。
  - 转发平面：信息流的转发主要通过IP报文的目的MAC地址、目的IP地址来查找路径转发，相关安全性主要针对转发路径上如何避免对WLAN设备自身的恶意攻击行为，以及预防某些攻击流量在IP网络中的扩散。
- 通过将管理平面、控制平面和转发平面进行隔离，WLAN设备能够保证任何一个平面在遭受攻击时，不会影响其他平面的正常运行。

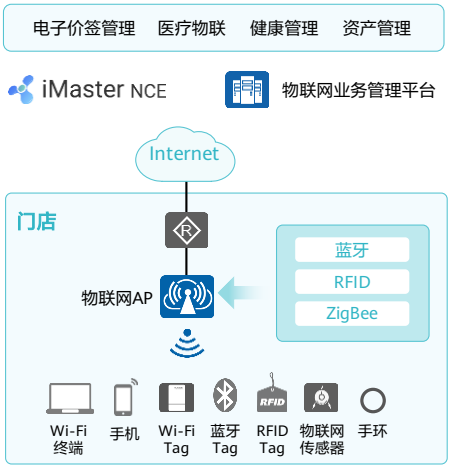
WLAN网络架构及安全方案

目录

物联网是新一轮的信息产业革命

PC互联网	移动互联网	物联网
		
最初的互联网主要针对固定终端，计算机终端设备能够接入网络共享资源。	进入21世纪，随着智能终端的发展，以智能应用为代表的移动互联网正迅猛发展，移动终端纷纷接入网络。	物联网被称为是世界信息产业革命的第三次浪潮。华为预测，到2025年将有1000亿个“物”会被连接到网络中，将极大影响人们的生活。

Wi-Fi & IoT融合，统一网络部署和运维管理



华为物联网AP

- Wi-Fi & IoT融合架构。
- AP与IoT基站合一，配套资源减半（接入/供电管理）。
- 支持云化管理，即插即用，业务配置简单。
- Wi-Fi与IoT配置联动，感知冲突时自动切换Wi-Fi信道。

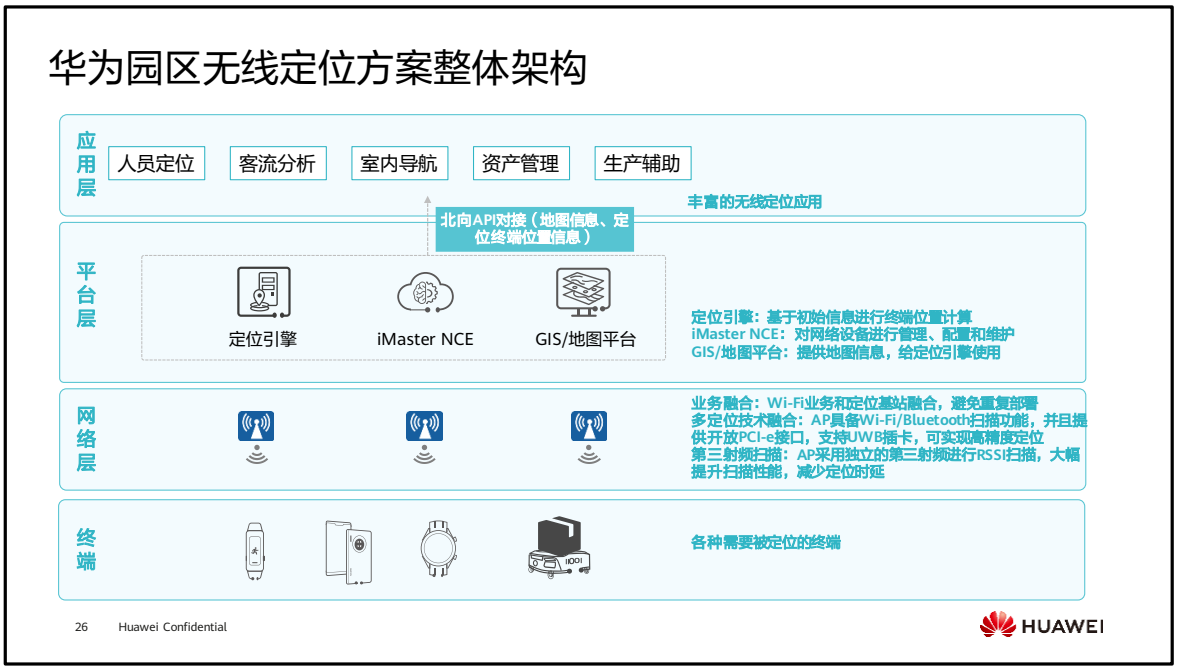
HUAWEI

- 统一入口，便于扩展降低维护成本：
  - 日常办公使用Wi-Fi接入服务。
  - 内置蓝牙模块，支持RFID，ZigBee拓展IoT物联业务。
  - Wi-Fi和IoT接入网络管理合一，简化运维。
- 统一管理，降低建网成本：
  - IoT业务与Wi-Fi业务共回传网络。
  - 只需管理和维护一个物理站点。
  - 提供USB口和标准Mini-PCI-E接口，方便物联网业务拓展。

定位服务的应用场景

人员定位	客流分析	室内导航	资产管理	生产辅助
				
• 外来访客管理 • 产线工人定位 • 特殊人员位置跟踪	• 商场热图 • 人物画像 • 消费习惯分析 • 精准营销	• 商场店铺导航 • 机场、车站路线规划 • 停车导航、反向寻车	• 资产定位 • 资产轨迹回溯 • 电子围栏 • 资产使用调度	• AGV、机械臂精准定位 • 仓储物流管理 • 车间危化区域防护 • 高危作业环境人员定位

科技在发展，时代在进步，对室内定位服务的诉求越来越多。



- 应用层：和位置信息相关的应用。基于位置信息，进行上层应用平台的开发，或者生产管理系统、行政管理系统等客户已有系统调用位置信息相关的API，进行应用开发和呈现。
- 平台层：平台层主要可以分为三大部分：
  - 定位引擎：对获取到的位置初始信息，如RSSI、时间等进行计算，得出被定位对象的位置坐标。
  - iMaster NCE：对网络设备进行管理、配置和维护。
  - GIS/地图平台：主要提供地图信息，给定位引擎使用。
- 网络层：AP提供Wi-Fi/Bluetooth的信号覆盖和管理（根据实际业务场景选择是否部署iBeacon，在手机导航场景下一般需要部署iBeacon）。
  - AP扫描Wi-Fi终端RSSI数据并将数据上报。
  - AP扫描蓝牙终端RSSI数据并将数据上报。
  - AP可作为标准iBeacon进行广播。
  - AP透传PCI-e插卡定位报文。
- 终端层：各种需要被定位的终端。

目录

WLAN运维挑战三“难”

问题主动识别“难”

- 往往要等到用户投诉才知道网络故障
- 无法识别潜在的影响用户感知的问题

用户体验衡量“难”

- 用户体验不好，但设备指标正常
- 缺少用户和网络关联分析

问题定位分析“难”

- 网络出现问题后，缺少方便的回溯手段
- 定位问题时，缺少故障发生时的关键数据

基于预测性和AI提升用户和业务体验

实时体验可视

1. **每区域：**通过7维评价体系，直观呈现整网或每个区域的网络状况及用户体验
2. **每用户：**实时呈现每个用户的全旅程网络体验（谁、何时、连接至哪个AP、体验、问题），故障可回溯
3. **每应用：**实时语音与实时视频应用体验感知，快速智能定界问题设备，分析质差根因

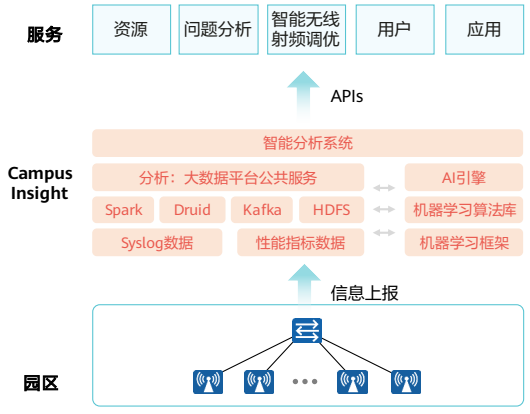
分钟级故障定界

1. **主动问题识别：**经过华为20万+终端持续训练的AI算法，主动识别85%的网络潜在问题
2. **分钟级故障定位：**基于故障推理引擎，分钟级问题定界并识别问题根因，给出有效的修复建议
3. **智能故障预测：**利用AI学习历史数据动态生成基线，通过和实时数据对比分析从而预测可能发生的故障

智能网络调优

1. **实时仿真反馈：**基于楼层设备的邻居和射频信息，实时评估无线网络信道冲突情况，并给出优化建议
2. **预测性调优：**基于历史数据的分析识别边缘AP、预测AP的负载趋势，进行无线网络的预测性调优并查看调优前后的增益对比，整网性能提升50%+（Tolly认证）。

CampusInsight：基于AI的园区网络分析器



业务服务：面向场景提供数据分析服务

- **问题识别：**连接/空口性能/漫游/设备四类问题的智能识别。
- **接入分析&性能体验：**连接问题以及性能体验问题分析。
- **用户&网络画像：**用户旅程回放，AP详情分析。
- **应用分析：**音视频质量感知。

数据分析：大数据平台和数据分析服务

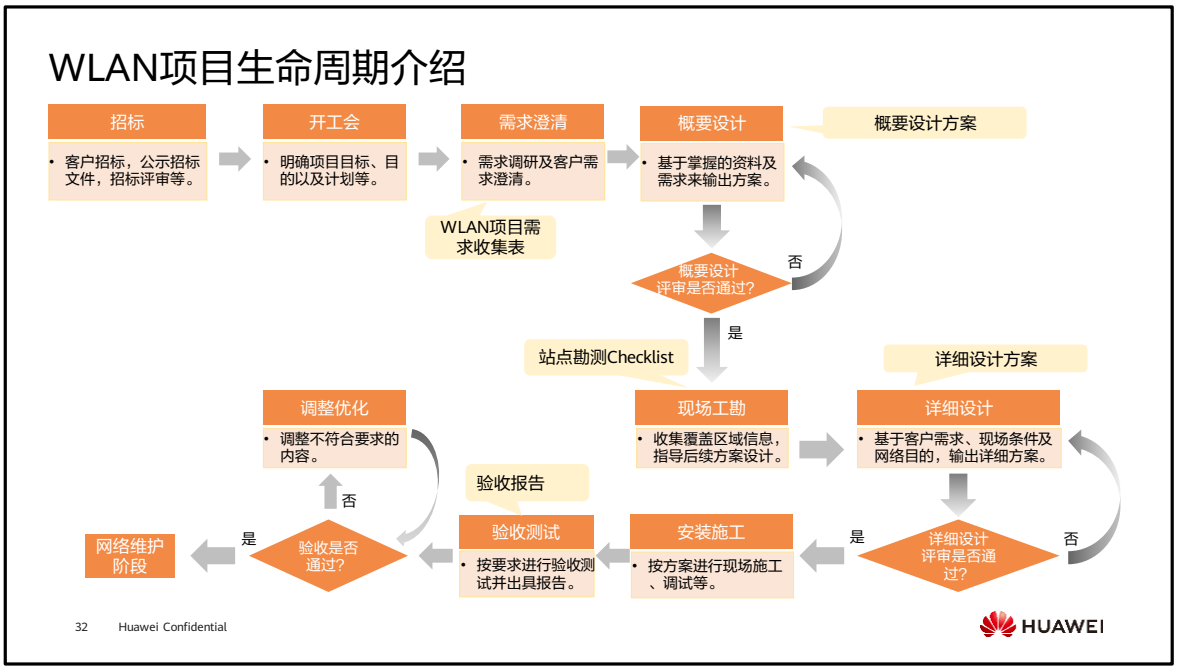
- **数据存储：**预处理实时流、分布式处理离线流、数据存储服务。
- **数据分析：**模式识别、AI引擎、数据汇聚&查询。

数据采集：秒级采集性能指标以及日志

- **数据采集：**用户、射频、AP、交换机、用户日志等多维度数据。

HUAWEI

目录



- 一般网络项目的服务流程分为需求澄清、概要设计、站点勘测、详细设计、安装调测、优化和验收。

思考题

1. 在高密场景下，如何保证无线用户的网络体验?
2. 以下哪些是WLAN网络保障业务的可靠性技术？（ ）
   A. VRRP
   B. HSB
   C. CAPWAP断链逃生
   D. 广域逃生

- 高密场景可以基于高密场景的建网标准来进行网络规划和网络优化，可以使用Wi-Fi 6的三射频AP（智能天线）来提升单AP终端接入量，另外可以采用射频资源管理、负载均衡以及QoS等技术来保障用户体验。
- CD

本章总结

- 本章主要介绍了华为WLAN的认证架构、技术重点以及重点阐述HCIE-WLAN的整体课程和知识架构。旨在让工程师们对于HCIE-WLAN的主要课程内容和技术重点有一定的了解。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN组网技术

HUAWEI

前言

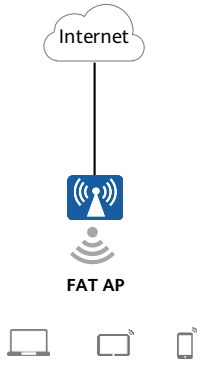
- 随着WLAN在企业网络中的应用越来越广泛，如何设计一个良好的WLAN组网架构、选择合适的WLAN组网方式、构建一个满足其业务要求的WLAN网络成为企业面临的重要问题。
- 本章主要介绍了WLAN组网技术，包括多类WLAN组网的架构、原理及应用场景。

目标

- 学完本课程后，您将能够：
  - 描述华为WLAN组网架构
  - 描述常见WLAN组网技术及其原理
  - 描述不同WLAN组网技术的应用场景
  - 完成不同WLAN组网技术的配置

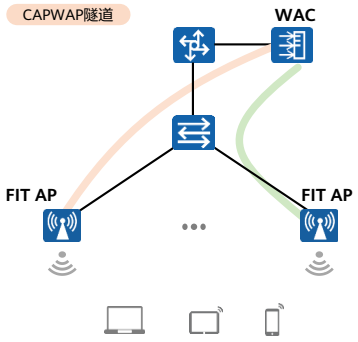
目录

FAT AP架构



1. FAT AP（胖AP）架构又称为自治式网络架构。
2. 部署单个FAT AP时，由于FAT AP具备较好的独立性，不需要另外部署集中控制设备，因此部署方便，成本低廉。
3. 主要应用于家庭WLAN以及微型门店WLAN等场景。
4. 在典型的企业WLAN场景中，无线信号覆盖面积更大，接入用户更多，需要部署的AP数量也更多，若采用FAT AP方案，每个FAT AP是独立工作的，缺少统一的控制设备，因此管理、维护较为复杂。

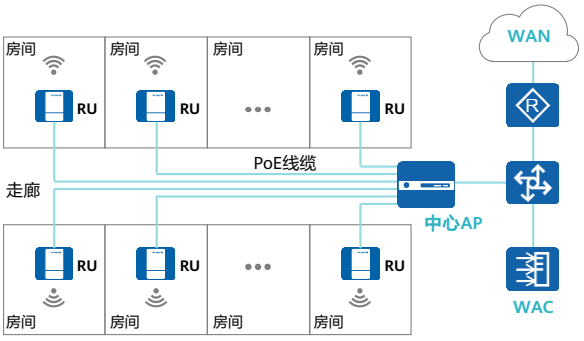
WAC+FIT AP架构



1. WAC负责WLAN的接入控制、数据转发、AP的配置管理、漫游管理、安全控制等。
2. FIT AP（瘦AP）负责802.11报文的加解密、实现802.11的物理层功能、接受WAC的管理及空口的统计等简单功能。
3. WAC和AP之间使用的通信协议是CAPWAP。
4. 相比于FAT AP架构，WAC+FIT AP架构的优点如下：
   - 多AP的场景下，配置与部署更容易。
   - 安全性更高。
   - 更新与扩展容易。
5. 主要应用于大中小型园区，及企业集中管理与部署WLAN的场景。

在WAC+FIT AP架构下，不同的组网方式、不同的数据转发方式及WAC的数量都会对WLAN组网有一定的影响。

敏捷分布式架构

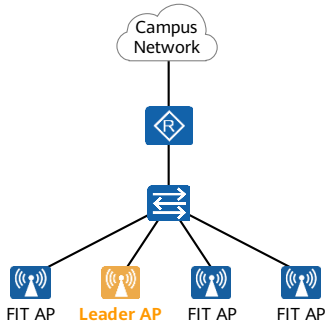


1. 敏捷分布式架构把传统的AP分解为中心AP和远端单元（Remote Unit，RU）两种独立的设备。
2. 中心AP可以部署在机房、弱电井和走廊等，远端单元可以通过线缆连接穿过墙体直接安装在房间内，让每个房间都可以独享优质的无线接入服务。
3. 主要应用于宿舍、酒店、和病房等密集场景。

HUAWEI

- 在宿舍、酒店和病房等房间密集的场景，如果采用WAC+FIT AP架构，每个房间布放一个AP，会造成大量报文上送到WAC，容易造成WAC出现性能瓶颈。为了解决WAC性能瓶颈问题，同时又解决每个独立房间的覆盖问题，可以将AP部署在走廊上，AP上的天线通过拉远的方式把信号引入各个房间，但是这种方案存在拉远距离的限制（距离拉得越远，信号衰减越大），同时多个房间共享一个AP，会出现信号质量差和性能不高的问题。
- 方案优势：
  - 管理简单：只需管理少量中心AP，近万个房间只需要200个AP的管理开销。
  - 灵活部署，覆盖无死角：中心AP和远端单元之间通过网线入室部署，无穿墙衰减与馈线损耗，信号覆盖效果更好。远端单元支持面板、挂墙和吸顶等多种安装方式。
  - 超远距离覆盖：相比传统AP的天线只能拉远15 m，中心AP和远端单元之间网线连接距离可达100 m，网络部署的范围扩大数倍，并且中心AP支持部署在走廊时，可提供超过100 m的超远距离覆盖。

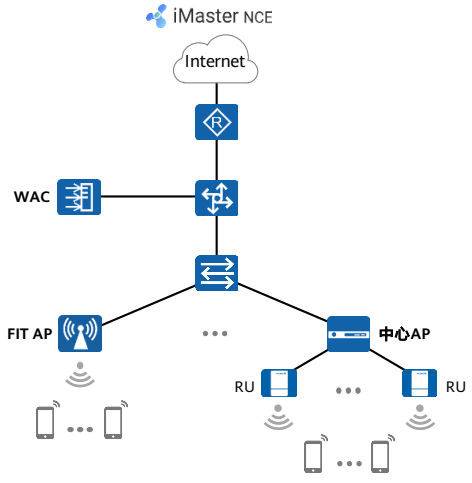
Leader AP架构



1. Leader AP组网中无需WAC。用户将其中1台AP设置为Leader AP模式，将其他AP以FIT AP模式接入网络，和Leader AP二层互通。
2. Leader AP会在二层网络中广播自己的角色，其它AP自动发现并连接Leader AP。
3. Leader AP的功能和WAC非常类似，提供基于CAPWAP隧道的统一接入管理和配置运维功能，提供集中的无线资源管理和漫游管理功能。
4. 用户只需登录Leader AP配置无线业务，所有AP都会提供相同的无线业务，终端可以在不同AP间漫游。
5. 主要应用于小微企业。

- 一些小微企业想要搭建自己的无线网络，由自己独立管理，且不采用云管理架构。在这种场景下，如果使用FAT AP架构，则不能统一管理和维护所有的AP，也无法为用户提供良好的漫游体验；如果选用WAC + FIT AP架构，则因为终端数量少，无线覆盖面积小，需要的AP数量不多，用户却要为WAC设备和License付出较高的成本。如果在组网中，某个AP能够承担管理其它AP的职责，提供统一运维和连续漫游的能力，就能够满足这类小微企业的需求。华为公司设计的Leader AP架构能满足这一需求。

WLAN云管理架构



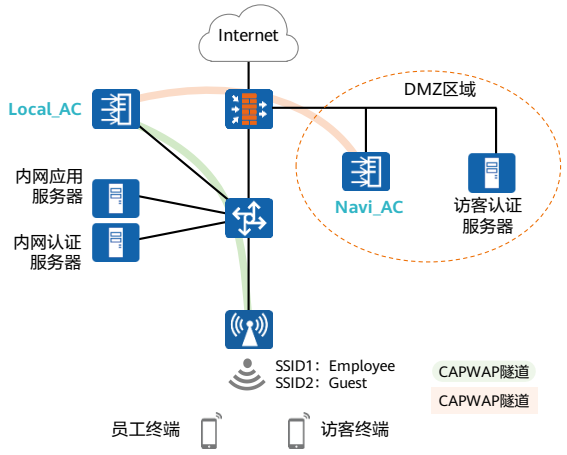
1. 在部署网络时，传统网络解决方案会存在部署成本高、后期运维困难等问题，尤其是对于分支站点数量多、站点地域分散的企业，这些问题尤为明显。
2. 若采用云管理架构，通过云管理平台，可实现在任意地点对设备进行集中的管理和维护，大大降低网络部署运维成本。
3. 当云AP布放完成后，无须网络管理员到安装现场对云AP进行软件调试，云AP上电后即可自动连接到指定的云管理平台加载指定的配置文件、软件包和补丁文件等系统文件，实现零配置上线。网络管理员可以随时随地通过云管理平台统一给AP下发配置，使业务批量配置更快捷。
4. 适用于中小型企业，例如连锁门店、中小型商超等。

HUAWEI

- 华为云管理平台：iMaster NCE-Campus作为“华为CloudCampus解决方案”的核心部件，提供对华为网络设备，如AP、AR、交换机和防火墙等设备的统一管理。通过iMaster NCE-Campus不仅可实现多租户的统一管理、网络设备的即插即用、网络业务批量部署等功能，而且由云管理平台提供的应用软件编程接口（Application Programming Interface，API）可实现与第三方平台对接，扩展更多的增值业务。
- 云管理架构相比传统的WAC+FIT AP架构，有如下优势。
  - 即插即用，自动开局，减少网络部署成本。
  - 统一运维。所有云管理网元统一在云管理平台上进行监控和管理。
  - 工具化。通常情况下，云解决方案会在云端提供各类工具，有效降低OPEX。例如，华为CloudCampus解决方案提供了端到端的云工具（如CloudCampus App）。

目录

Navi AC

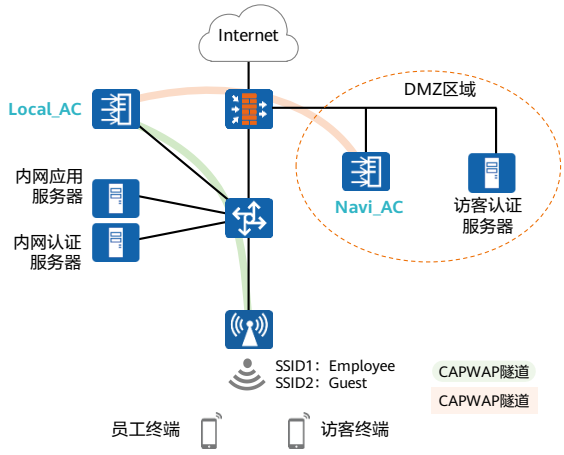


1. 大型企业在部署无线网络时，往往需同时为内部员工及访客提供接入服务，而访客数据可能会给网络带来潜在的安全威胁。
2. 企业可以将访客流量引导到DMZ中的Navi AC进行集中管理，从而实现员工和访客数据的隔离。

HUAWEI

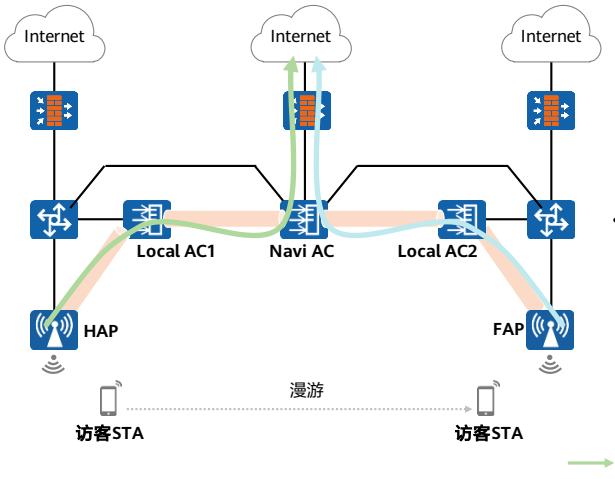
- Local AC：承担对AP的集中管理和协同功能，如STA上线、AP配置下发等。
- Navi AC：集中处理无线用户的安全、控制和管理等功能，如身份认证、授权和计费等。
- Local AC和Navi AC间的CAPWAP隧道：Local AC上的用户数据报文通过CAPWAP隧道集中到Navi AC上进行处理。
- DMZ：为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间，在该区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器等。通过这个DMZ区域，从而更加有效地保护了内部网络。

Navi AC典型应用场景



1. 员工在Local AC上完成准入认证，其流量在企业内网转发，员工可访问内网应用服务器。
2. 访客在Navi AC上完成准入认证，其流量从Local AC通过CAPWAP隧道转发到DMZ进行处理，访客只能访问DMZ中的服务器和Internet资源。

Navi AC方案下的跨AC漫游



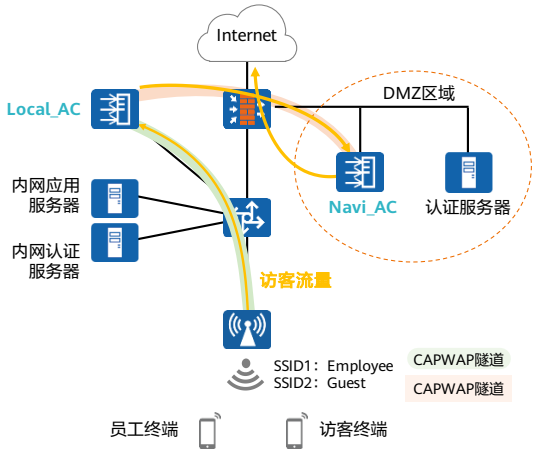
- 漫游前：
  - STA发送业务报文给HAP。
  - HAP接收到STA发送的业务报文并发送给Local AC1。
  - Local AC1通过CAPWAP隧道将业务报文转发给Navi AC。
  - Navi AC直接将业务报文发送至上层网络。
- 漫游后：
  - STA发送业务报文给FAP。
  - FAP接收到STA发送的业务报文并发送给Local AC2。
  - Local AC2通过CAPWAP隧道将业务报文转发至Navi AC。
  - Navi AC直接将业务报文发送至上层网络。

漫游前流量　漫游后流量　CAPWAP隧道

HUAWEI

- 在Navi AC方案中，仅支持在连接到同一个Navi AC的多个Local AC之间实现无线漫游。

Navi AC配置举例



业务需求

某企业为避免访客流量带来的网络安全风险，要求将访客流量引至DMZ进行集中管理。

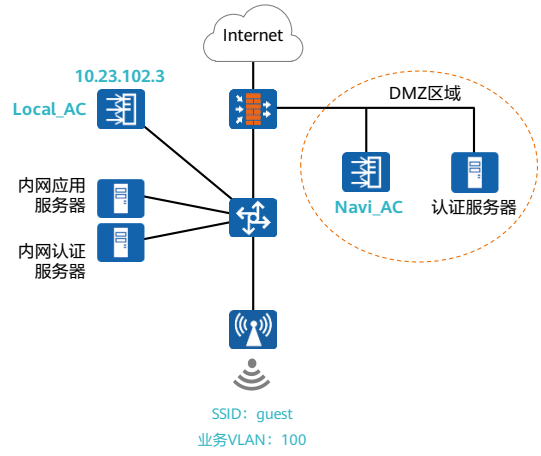
配置思路

1. 在Navi AC上创建并配置VAP模板、开启Navi AC功能、指定Local AC，并将VAP模板绑定到指定Local AC下。
2. 在Local AC上指定Navi AC、创建并配置VAP模板（配置与Navi AC保持一致），并在AP组下引用VAP模板。

HUAWEI

- 组网需求：
  - Local AC和Navi AC之间路由可达。
  - DHCP部署方式：Navi AC作为DHCP服务器为访客分配IP地址。
  - 访客业务数据转发方式：通过CAPWAP隧道转发至Navi AC。
- 配置思路：
  - 在Navi AC上创建并配置VAP模板、开启Navi AC功能、指定Local AC，并将VAP模板绑定到指定Local AC下。
  - 在Local AC上指定Navi AC、创建并配置VAP模板（配置与Navi AC保持一致），并在AP组下引用VAP模板。

Navi AC配置举例 - Navi AC配置



1.在Navi AC上创建并配置VAP模板、开启Navi AC功能、指定Local AC，并将VAP模板绑定到指定Local AC下。

#在Navi AC上创建并配置VAP模板。

```
[Navi_AC-wlan-view] ssid-profile name ssid1
[Navi_AC-ssid-prof-ssid1] ssid guest
[Navi_AC-ssid-prof-ssid1] quit
[Navi_AC-wlan-view] vap-profile name navi-ac
[Navi_AC-vap-prof-navi-ac] ssid-profile ssid1
[Navi_AC-vap-prof-navi-ac] service-VLAN VLAN-id 100
[Navi_AC-vap-prof-navi-ac] forward-mode tunnel
```

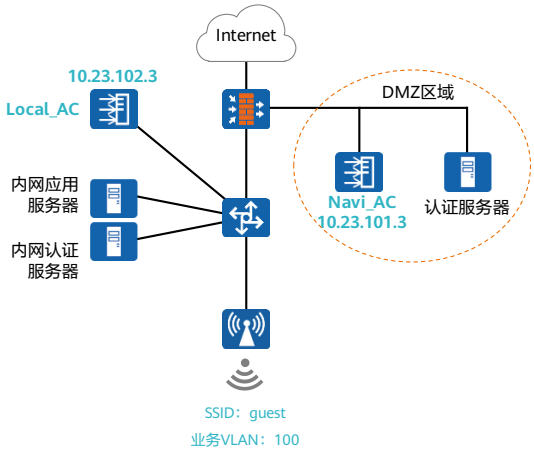
#开启Navi AC功能。

```
[Navi_AC-wlan-view] navi-ac enable
```

#指定Local AC，并将VAP模板绑定到指定Local AC下。

```
[Navi_AC-wlan-view] navi-ac
[Navi_AC-wlan-view-navi-ac] local-ac ac-id 1 ip-address 10.23.102.3
[Navi_AC-wlan-view-navi-local-ac-1] vap-profile navi-ac wlan 1
```

Navi AC配置举例 - Local AC配置



2.在Local AC上指定Navi AC、创建并配置VAP模板（配置与Navi AC保持一致），并在AP组下引用VAP模板。

#指定Navi AC。

```
[Local_AC] wlan
[Local_AC-wlan-view] navi-ac ac-id 1 ip-address 10.23.101.3
```

#在Local AC上创建并配置VAP模板。

```
[Local_AC-wlan-view] ssid-profile name ssid1
[Local_AC-ssid-prof-ssid1] ssid guest
[Local_AC-ssid-prof-ssid1] quit
[Local_AC-wlan-view] vap-profile name navi-ac
[Local_AC-vap-prof-navi-ac] ssid-profile ssid1
[Local_AC-vap-prof-navi-ac] service-VLAN VLAN-id 100
[Local_AC-vap-prof-navi-ac] forward-mode tunnel
[Local_AC-vap-prof-navi-ac] type service-navi navi-ac-id 1 navi-wlan-id 1
```

#在Local AC上绑定VAP模板。

```
[Local_AC-wlan-view] ap-group name group1
[Local_AC-wlan-ap-group-group1] vap-profile navi-acwlan 2 radio all
```

查看配置结果（1）

- 使用**display navi-ac run-status**命令用来查看Navi AC/Local AC的运行状态。

```
<WAC> display navi-ac run-status all
Current role: navi
--------------------------------------------------------------------------------
AC ID     AC IP            Mac              Role     Status   STA  Description
--------------------------------------------------------------------------------
1         192.168.160.253  ac4e-914a-2d26   local    normal   6    LocalAC1
--------------------------------------------------------------------------------
Total:1
```

- 使用**display navi-ac station**命令用来查看在Navi AC上的STA接入信息。

```
<WAC> display navi-ac station all
WLAN: WLAN ID
--------------------------------------------------------------------------------
STA MAC          AC ID  WLAN  VLAN  IPv4 address     SSID
--------------------------------------------------------------------------------
6cb0-ce40-df62   1      8     200   192.168.1.254    Guest
--------------------------------------------------------------------------------
Total: 1
```

查看配置结果 (2)

- 使用**display navi-ac vap**命令查看Navi VAP的相关信息。

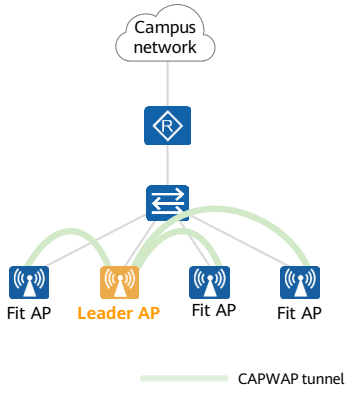
```
<WAC> display navi-ac vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AC ID     AC IP            AC MAC          WID  Status  Auth type     STA  SSID
--------------------------------------------------------------------------------
1         192.168.160.253  AC4E-914A-2D26  8    ON      Open+Portal   1    guest
--------------------------------------------------------------------------------
Total: 1
```

Navi AC常用维护命令

功能描述	命令行
查看Navi AC/Local AC的运行状态	**display navi-ac run-status** { **ac-id** *ac-id* | **all** }
查看在Navi AC上的STA接入信息	**display navi-ac station** { **ac-id** *ac-id* | **ssid** *ssid* | **sta-mac** *sta-mac-address* | **vlan** *vlan-id* | **all** }
查看Navi VAP的相关信息	**display navi-ac vap** { **ac-id** *ac-id* | **all** }
查看Navi AC/Local AC的上线失败/下线记录	**display navi-ac connect-record** { **ac-id** *ac-id* | **ac-mac** *ac-mac* | **all** }
查看Navi VAP创建失败记录	**display navi-ac vap create-fail-record** { **ac-id** *ac-id* | **all** }
清除Navi AC/Local AC的上线失败/下线记录	**reset navi-ac connect-record** { **ac-id** *ac-id* | **ac-mac** *ac-mac* | **all** }

目录

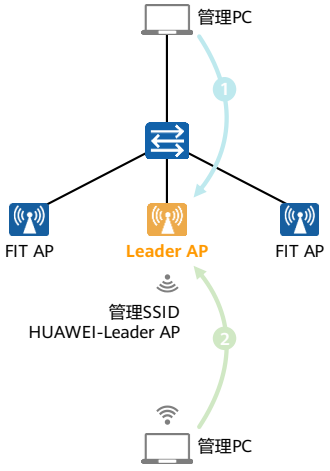
Leader AP方案说明



1. 用户将其中1台AP设置为Leader AP模式，将其他AP以FIT AP模式接入网络，和Leader AP二层互通。
2. Leader AP会在二层网络中广播自己的角色，其它AP自动发现并连接Leader AP。
3. Leader AP提供基于CAPWAP隧道的统一接入管理和配置运维功能，提供集中的无线资源管理和漫游管理功能。
4. 用户只需登录Leader AP配置无线业务，所有AP都会提供相同的无线业务，终端可以在不同AP间漫游。

管理Leader AP

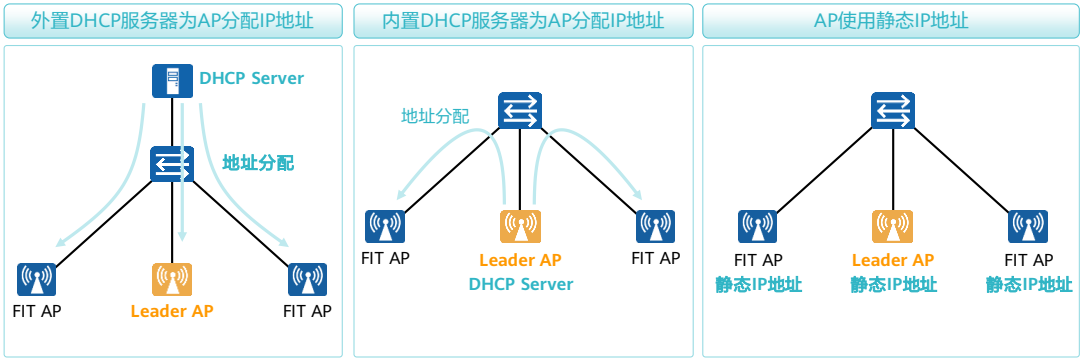
- 用户可通过如下方式对Leader AP进行管理：
  - 通过有线网络进行登录。
  - 通过管理SSID进行登录。



HUAWEI

- 考虑到运维的方便，支持用户通过空口登录Leader AP对其进行管理，用户可通过无线终端接入Leader AP的管理SSID，管理SSID有如下几个特点：
  - 默认为Open认证，无PSK。
  - 默认采用隧道转发模式，终端接入该SSID后，从Leader AP获取地址，且默认网关在Leader AP上，网关地址为192.168.1.1。
  - 所有AP都会通告该管理SSID，SSID的默认名称为HUAWEI-Leader AP。
  - 该管理SSID无法被删除，只能被隐藏；网络管理员只能修改网关IP地址，不能变更SSID名称。
  - 管理SSID只能用于AP管理，用户无法接入该SSID进行上网。

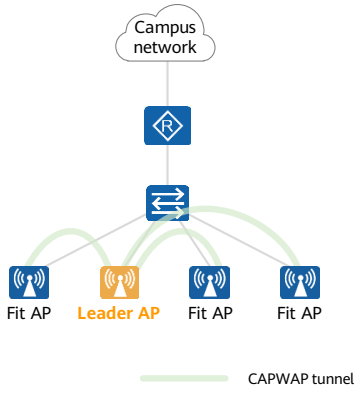
Leader AP组网场景下的AP地址分配



HUAWEI

- 缺省情况下，与Leader AP处于同一网络中的其他AP在Leader AP上线是不需要认证的。
- FIT AP接入到Leader AP的方式：
  - 支持由外置DHCP服务器为所有AP分配IP地址，用户需保证Leader AP与FIT AP在同一个VLAN下，FIT AP通过CAPWAP广播方式发现Leader AP。
  - 支持Leader AP作为FIT AP的DHCP服务器，在该场景中，建议Leader AP和FIT AP在一个VLAN内。
  - 支持FIT AP以静态设置IP地址方式接入，建议Leader AP和FIT AP在一个VLAN内。
- Leader AP的CAPWAP接口创建方式。
  - 考虑到配置的简易性，Leader AP 不支持手动配置CAPWAP接口，该接口由Leader AP自动创建。
- 支持FIT AP与Leader AP之间采用三层组网方式
  - 支持在FIT AP上配置静态AC-List（Leader AP的IP地址）。
  - 支持FIT AP通过DHCP option43获取Leader AP的地址。
- Leader AP支持配置DTLS控制面和转发面的加解密。
- 当FIT AP接入后，可开启MAC或SN认证以增加安全性。

Leader AP典型部署流程

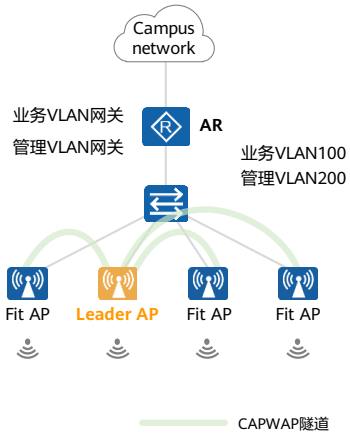


- 在AP中选择一台作为Leader AP。
- 将所有AP连线、上电。
- 在手机上安装CloudCampus APP，并使用APP对被选为Leader AP的设备进行扫码，此时APP会自动连接至被选为Leader AP的设备所释放的管理SSID，并提示用户通过APP将该设备切换至Leader AP。
- AP重启，然后切换至Leader AP模式。
- 用户的CloudCampus APP自动连接至Leader AP的管理SSID，用户通过APP的引导界面完成Leader AP的配置（DHCP服务配置、SSID配置等）。
- 其他FIT AP从Leader AP获取IP地址，并发现该Leader AP，然后与Leader AP建立CAPWAP隧道，并获得业务配置。

HUAWEI

- 在部署Leader AP前，网络管理员需手工选择一台AP作为Leader AP（AP出厂默认是FIT AP）。建议选举原则：9700D>8760>6760>5760。
- 纳管AP数量：
  - AirEngine 8700系列：桥接模式：48；网关模式：24。
  - AirEngine 5700系列/AirEngine 6700系列：桥接模式：24；网关模式：12。

Leader AP配置案例



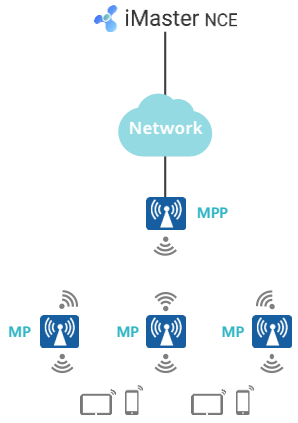

```
[LeaderAP] vlan batch 100 200
[LeaderAP] interface vlanif 200
[LeaderAP-Vlanif200] ip address 192.168.200.254 255.255.255.0
[LeaderAP-Vlanif200] management-interface
[LeaderAP] capwap interface source vlanif 200
[LeaderAP] wlan
[LeaderAP-WLAN] inner-gateway disable        // 采用直接转发方式
[LeaderAP-WLAN] ssid-profile name open       // 创建SSID模板
[LeaderAP-WLAN-SSID-prof-open] ssid Open     // SSID名称
[LeaderAP-WLAN] vap-profile name open        // 创建VAP模板
[LeaderAP-WLAN-vap-prof-open] service-vlan vlan-id 100 // 配置业务VLAN
[LeaderAP-WLAN-vap-prof-open] ssid-profile open        // 调用前面配置好的SSID模板
```


HUAWEI

- 当AP个数超过24个后，建议为无线终端配置外置网关，例如，在本例中的AR路由器。

目录

Mesh简介



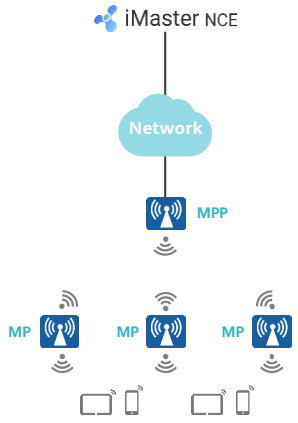
无线Mesh网络WMN（Wireless Mesh Network）是指利用无线链路将多个AP连接起来，并最终通过一个或两个Portal节点接入有线网络的一种星型动态自组织自配置的无线网络。

快速部署 | 健壮性 | 灵活组网 | 应用场景广 | 高性价比

HUAWEI

- 传统的WLAN网络中，STA与AP之间是以无线信道为传输介质，AP的上行链路则是有线网络。如果组建WLAN网络前没有有线网络基础，大量的时间和成本消耗在构建有线网络过程中，对于组建后的WLAN网络，如果需要对其中某些AP位置进行调整，则需要调整相应的有线网络，操作困难。综上所述，传统WLAN网络的建设周期长、成本高、灵活性差的弊端，使其在应急通信、无线城域网或有线网络薄弱地区等应用场合不适合部署。而Mesh网络只需要安装AP，建网速度非常快。
- 无线Mesh网络减少了节点之间的布线需求，但仍具有分布式网络所提供的冗余机制和重新路由功能。因此：
  - 添加新的设备时，只需要为设备接上电源，Mesh网络可以自动进行配置，并确定最佳的多跳传输路径。
  - 移动设备时，Mesh网络能够自动发现拓扑变化，并自动调整通信路由，以获取最有效的传输路径。

Mesh的基本概念



- **MP（Mesh Point）**：使用IEEE 802.11MAC和物理层协议进行无线通信，并且支持Mesh功能的节点。该节点支持自动拓扑、自动发现路由、数据报文转发等功能。MP节点可以同时提供Mesh服务和用户接入服务。
- **MPP（Mesh Portal Point）**：连接Mesh网络和其他类型网络的MP节点。这个节点具有Portal功能，可以实现Mesh内部节点和外部网络的通信。
- **邻居MP**：与某个Mesh节点处于直接通信范围内的MP或MPP，称为该Mesh节点的邻居MP。
- **候选MP**：MP准备与之建立Mesh链路的邻居MP。
- **对端MP**：已与MP建立起Mesh连接的邻居MP，称为该MP的对端MP。

Mesh邻居发现

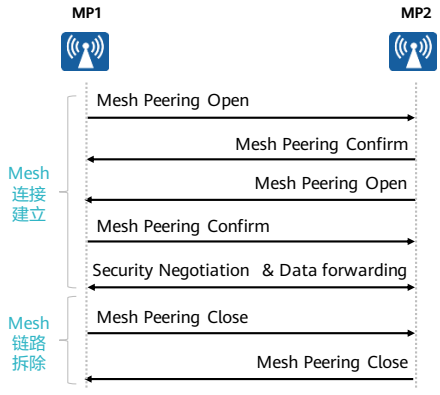
1. Mesh邻居发现

- 在建立Mesh网络之前，首先需要发现邻居MP设备。Mesh网络中，各节点通过被动扫描来获取邻居MP的信息。
- 被动扫描：MP在每个信道上侦听邻居MP定时发送的Mesh Beacon信标帧（信标帧中包括Mesh ID等信息），以获取邻居MP的相关信息。

2. 更新邻居关系表

- 每个MP都存在邻居关系表，该表将所有邻居节点的信息分为四类：普通AP邻居、其他Mesh网络节点、候选MP节点、对端MP节点。
- 对于被动扫描方式，如果MP发现自己接收到的Mesh Beacon信标帧中的Mesh ID与自己的Mesh ID一致，则在邻居关系表中将该邻居设备记录为候选MP节点。

Mesh连接管理

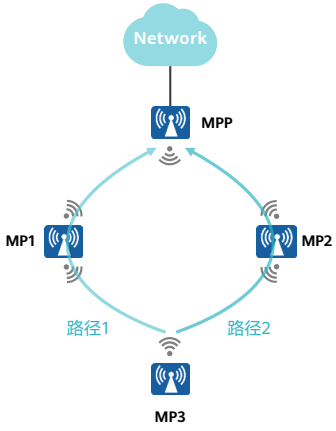


- **Mesh连接建立**
  - MP在选出候选MP节点后，可以与之发起Mesh连接建立过程。
  - 建立Mesh连接的双方通过两次Mesh Peering Open/Confirm的交互，完成Mesh连接的建立。
  - Mesh连接建立后，需要继续进行后续的密钥协商阶段，只有密钥协商成功之后Mesh节点才可以参与Mesh数据转发。
- **Mesh链路拆除**
  - Mesh连接双方中任意一方，均可以主动向对方发送Mesh Peering Close报文，以关闭双方间的Mesh连接。收到Mesh Peering Close消息的MP，需要向对方MP回应一个Mesh Peering Close消息。

HUAWEI

- Mesh连接管理包括Mesh连接建立和Mesh连接拆除两个过程，采用Mesh Peering Open/Confirm/Close三种Mesh连接管理Action帧交互实现。

Mesh路由技术背景



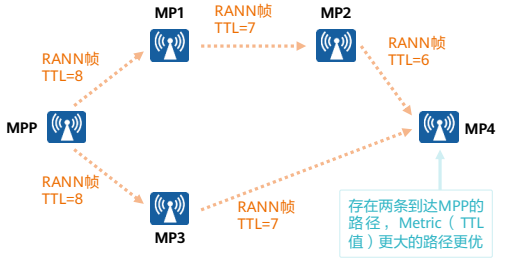
为什么需要Mesh路由

- 在Mesh网络中，任何一个源和目的地之间都会存在多条可用的、质量变化的Mesh链路。
- 因此，必须在Mesh网络内支持选路协议，802.11s标准中定义的HWMP路由协议应运而生。

HWMP定义的路由管理帧

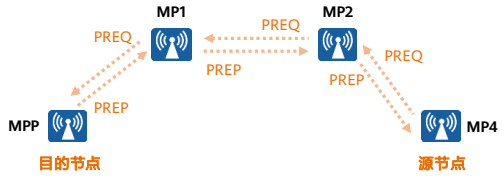
RANN网关通告帧：是通知其他节点MPP的存在

- MPP节点定时广播RANN帧。
- MP收到RANN消息后，将TTL减1，更新路径Metric信息，再将其广播出去。



PREQ（路由请求帧）与PREP（路由应答帧）

- 在按需路由模式中，源节点广播PREQ帧建立到目的节点的路由，MP节点收到PREQ帧后，回应PREP帧。



HUAWEI

- 在802.11s路由协议中，定义了下面几种路由管理帧：
  - RANN（Root Announcement Frame）：网关通告帧，目的是通知其他节点MPP的存在。
    - MPP节点定时广播RANN帧。
    - MP收到RANN消息后，将TTL减1，更新路径Metric信息，再将其广播出去，不做其他处理。读取RANN帧的内容后，判断RANN中的网关是否已经存在于自己的网关列表中，如果不存在，则在列表中新增该网关的条目；如果存在，则依据RANN中的信息，更新相应条目的信息。
  - PREQ（Path Request）与PREP（Path Reply）：路由请求帧和路由应答帧。在按需路由模式中，源节点广播PREQ消息建立到目的节点的路由，MP节点收到PREQ帧后，回应路由应答帧。

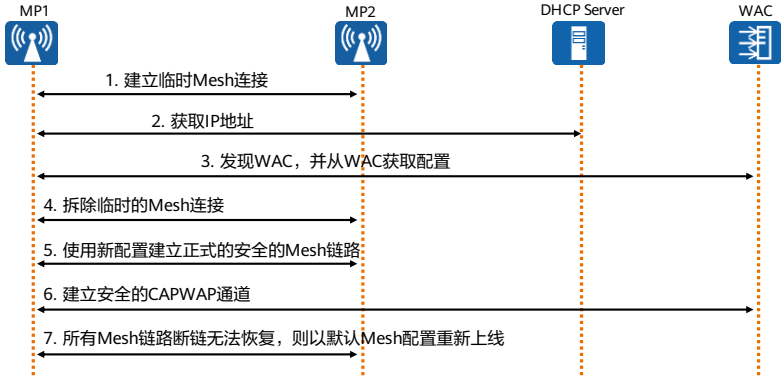
Mesh网络中的路由选择模式

先应路由模式	按需路由模式
• 根节点周期性地广播RANN消息。 • 当一个Mesh节点收到RANN消息并且需要创建或者更新到根节点的路由时，它会单播发送PREP消息到根，同时将RANN消息继续广播出去。 • 这样，MPP创建一条从根节点到源节点的反向路径，MP创建一条从根节点到源节点的转发路径。	• 源节点广播PREQ消息建立到目的节点的路由。 • 如果当前PREQ的序列号比前一个PREQ消息的序列号大或者序列号相同但度量值更优，在收到PREQ消息之后，中间节点创建或者更新到源节点的路由； • 如果没有到达目的路由，中间节点继续转发PREQ。

- Mesh网络中支持按需路由和先应路由两种路由选择模式：
  - 按需路由模式：源节点广播PREQ消息建立到目的节点的路由。如果当前PREQ的序列号比前一个PREQ消息的序列号大或者序列号相同但度量值更优，在收到PREQ消息之后，中间节点创建或者更新到源节点的路由；如果没有到达目的路由，中间节点继续转发PREQ。
  - 先应路由模式：根节点周期性地广播RANN消息。当一个Mesh节点收到RANN消息并且需要创建或者更新到根节点的路由时，它会单播发送PREP消息到根，同时将RANN消息继续广播出去。这样，MPP创建一条从根节点到源节点的反向路径，MP创建一条从根节点到源节点的转发路径。
- HWMP将先应路由模式和按需路由模式相结合，确保数据帧能够始终通过传输质量最好的Mesh链路传输。
- 华为MESH特性基于标准802.11s协议开发了私有MESH路由协议并进行优化，其特点是在无线链路搭建时，考虑减少通讯的转发次数，使能基于静态的到目的节点跳数较小的路径构造转发拓扑。

MP节点零配置上线

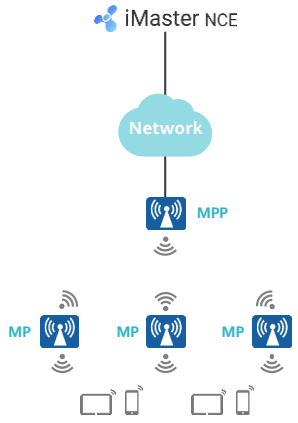
- 零配置（Zero Touch Configure）上线是指在采用WAC+FIT AP组建Mesh网络时，仅需要在AP上线前先在WAC上对AP进行少量的离线管理配置，而不需要本地直接登录到AP上进行任何配置就可以完成AP的上线过程。该功能为大量AP同时开局的场景提供了极大的便利。



HUAWEI

- MP1上电后，通过默认Mesh ID和默认预共享密钥等信息与已成功关联到WAC的邻居MP2进行Mesh Peering Open/Confirm交互，建立临时的非安全的Mesh连接，并建立到MPP节点的路由。
- MP1节点通过建立的Mesh连接与DHCP server交互获取到自己和WAC的IP地址。
- MP1节点通过建立的Mesh连接发现WAC并完成与WAC的关联，建立临时的CAPWAP隧道，并从WAC获取配置信息。
- MP1获取到新配置后，通过Mesh Peering Close消息主动断开临时的非安全的连接。
- MP1用新的mesh配置再次进行Mesh Peering Open/Confirm交互，然后完成密钥协商，协商出MP间通信的最终密钥，最后建立正式的安全的Mesh链路。
- MP1以更新后的配置重新与WAC建立安全的CAPWAP隧道。
- 当MP1长时间无法与MP2建立mesh链路，则恢复默认配置，重新从步骤1开始，直到MP1以更新后的配置重新与WAC建立安全的CAPWAP隧道。

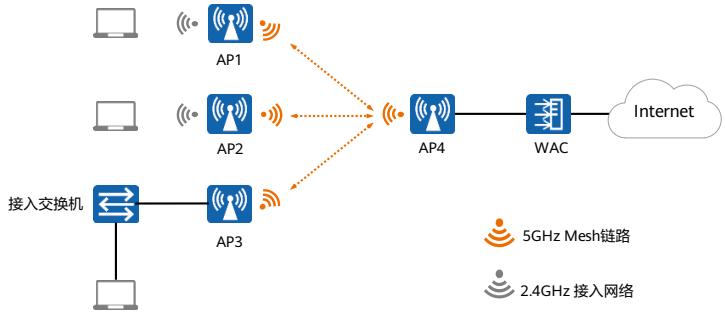
Mesh网络的设计要点



- **MPP布放：**
  - MPP需通过空口与MP对接，因此其布放位置需综合考虑接入有线网络的便利性，以及与各MP对接的视线条件。
- **规划设计：**
  - **回传信道选择：**为了达到较高的吞吐量和较好的用户体验，一般选择空口质量较好的5G信道作为回传信道。
  - **HT40和HT20选择：**在回传层中，推荐使用HT40模式，可提供更高的回传速率。而在MP-终端之间的网络中，由于目前较多的终端还不支持HT40模式，且HT40模式也很少应用在2.4G射频上，所以在接入层一般使用HT20模式。
  - **DFS影响：**回传信道避免使用DFS信道，才避免信道切换导致业务中断。

Mesh应用 - Mesh无线桥接

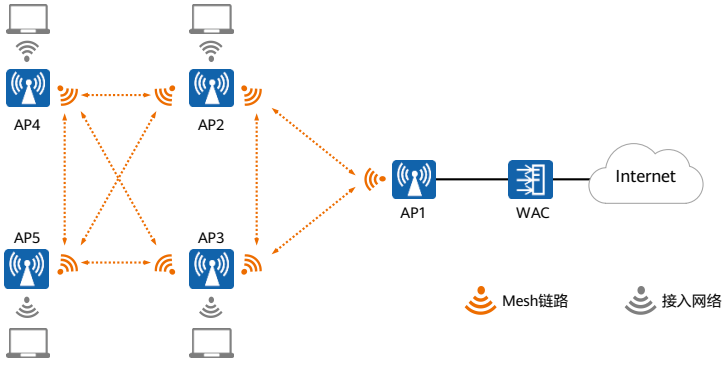
- 如图所示，AP1～AP3为有线用户和无线用户提供网络接入服务，由于地理位置或环境因素限制，AP1～AP3无法通过有线方式接入Internet。AP1～AP3通过与AP4建立Mesh网络，可实现无线用户的网络接入服务。



- 可用于小型广场的无线信号覆盖，距离有线网络存在一定距离的远端MP直接采用无线Mesh链路与MPP相连，从而使得整个网络提供更大范围的无线信号覆盖服务。

Mesh应用 - 单MPP节点的Mesh网络

- 如图所示，AP2～AP5为无线用户提供网络接入服务，AP1提供到Internet的有线连接。AP1～AP5通过网状互联形成安全的、自配置、自愈合的室外Mesh网络，便于对不利于有线布线的室外环境进行快速和经济的无线网络部署。

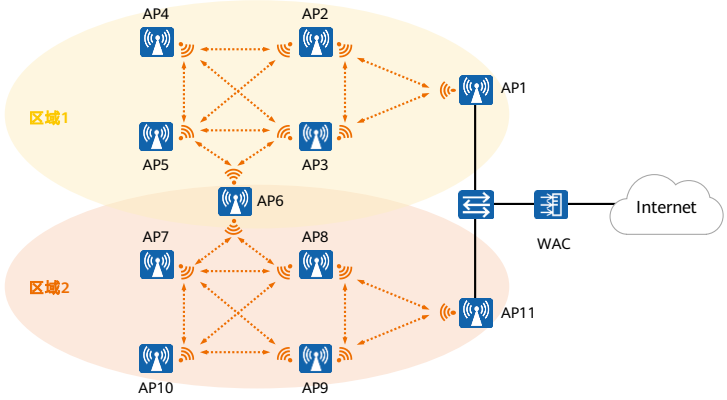


HUAWEI

- 网状拓扑Mesh组网可以检测到其他MP，并且形成Mesh链路。该网络拓扑存在空口冗余链路，使用时，可以结合Mesh路由选择性地阻塞冗余链路来消除环路，在Mesh链路故障时还可以启用备份链路，实现可靠性。

Mesh应用 - 多MPP节点Mesh网络

- AP1和AP11提供到Internet的有线连接，AP2～AP5为区域1内有线用户和无线用户提供接入服务，AP7～AP10为区域2内有线用户和无线用户提供接入服务，AP6位于区域1和区域2的重叠区域。



HUAWEI

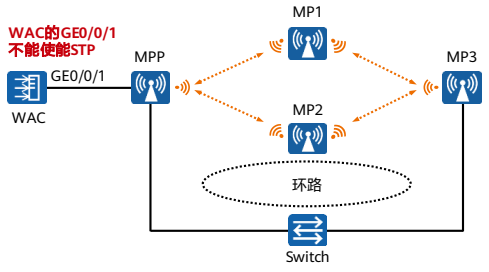
- 与MPP建立Mesh链路的MP和该MPP的无线信道相同。当覆盖不同区域时，可以配置多个MPP节点，通过将MPP配置在不同的工作信道，减少MP间相互竞争无线信道使用权，影响整体性能。同时，每个MP还能自主选择一个跳数最少的最优MPP节点作为连接有线网络的网关设备。

Mesh网络支持的STP场景

- 用户在部署Mesh网络时，应充分考虑链路的环路问题，尽量避免环路出现。Mesh网络仅支持单一环路破环，Mesh网络可以支持的STP场景，如下所示：

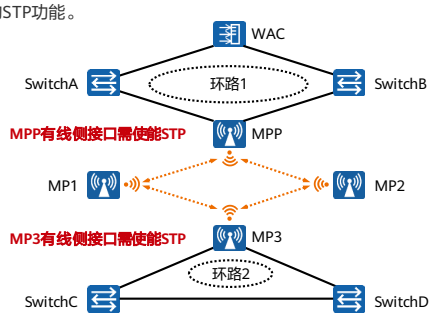
场景一

- 环路涉及的非AP网元使能STP功能，且和Mesh网络相连的其他不涉及环路的网元不使能STP功能。



场景二

- Mesh网络中接有双网口AP，AP有线侧接口出现单一环路且有线侧接口未绑定为Eth-Trunk接口，当需要STP报文不向无线侧透传时，需使能AP的STP功能。

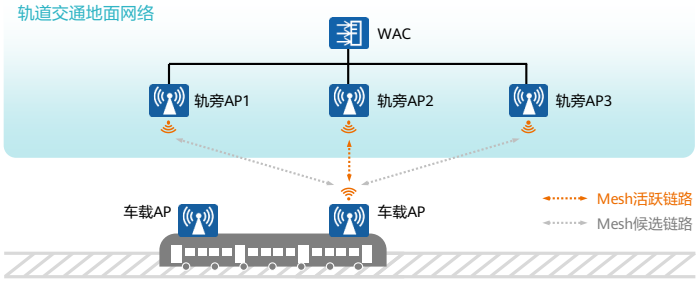


HUAWEI

- 在Mesh网络，Mesh链路对STP报文仅做透传。如果AP使能STP功能，AP不会将STP报文传至无线侧，只会对AP有线侧进行破环。
- 如场景一所示，Switch和Mesh链路构成了单个环路，此时需要在涉及环路的网元Switch上配置STP功能，而在不涉及环路的网元WAC上要保证连接MPP节点的GE0/0/1接口未使能STP功能，环路网络才能成功破环。
- 如场景二所示，WAC、SwitchA、SwitchB和MPP节点构成了单一环路（环路1），SwitchC、SwitchD和MP3节点也构成了单一环路（环路2），如果Mesh链路透传了STP报文，则环路1会将不相关的环路2的网元SwitchC和SwitchD计算在内，造成环路1的STP计算错误。此时需要使能MPP节点和MP3节点的STP功能，让两个环路的STP报文不向无线侧透传。在环路1内MPP节点会参与环路1的STP计算，并根据计算结果阻塞有线侧接口。在环路2内MP3节点会参与环路2的STP计算，并根据计算结果阻塞有线侧接口。
- Mesh网络内部允许冗余的Mesh链路存在，Mesh转发路径由Mesh路由决定，Mesh链路不会出现环路。

车地通信场景Mesh链路快速切换（1）

- 列车在行进的过程中，车载AP会与邻近的轨旁AP建立多条Mesh链路，并选择一条质量最好的Mesh链路作为活跃链路传输数据，其他Mesh链路为候选链路。
- 随着列车的行进，当前的活跃链路质量会变差或者候选链路中出现了质量更好的链路，此时，车载AP会在候选链路中选择一条最优链路作为新的活跃链路，进行链路的快速切换，以保证列车和地面网络间的高质量通信。



HUAWEI

- 在轨交系统中车地通信子系统是重要组成部分，它为高速移动的列车和地面网络之间提供了数据通道，承载了车载资讯等业务的数据传输。当前，车地通信主要依靠无线通信技术来实现，WLAN具有方便快捷、经济高效的优势，通过WLAN实现车地通信子系统可以为轨交企业提高经济效益。但由于AP覆盖范围有限，列车在高速运行状态下需要不停的切换接入的AP而引起漫游，WLAN漫游一般需要100ms甚至更长的切换时间，会造成车载资讯等业务的数据丢包或延迟，如车载多媒体出现卡顿或花屏等现象，无法满足车地通信子系统的要求。
- 车地通信快速切换可以实现车地通信链路的无缝切换，能为高速运行的列车提供可靠的、稳定的数据链路，为用户提供流畅的车载资讯业务。
- 使用车地通信快速切换实现车地通信具备如下优势：
  - 低通信成本：相对于3G、LTE等无线通信技术，基于WLAN Mesh技术的车地通信快速切换使用ISM（Industrial, Scientific, Medical）频段，用户无需申请许可证即可使用ISM频段射频。另外，车地通信快速切换不会产生额外的通信费用，而且可以很好的融合现有的轨交网络，方便轨交业务的拓展。
  - 高可靠性：车地通信快速切换基于WLAN Mesh技术，具备Mesh的冗余链路的特点，列车在行进过程中车载AP会和多个轨旁AP建立冗余Mesh链路，一旦活跃链路质量变差，车载AP会立刻从其他Mesh链路中挑选更好的链路作为活跃链路，有效保障了车地通信的链路质量。

    - 高质量数据传输：车地通信快速切换实现了Mesh链路的无缝切换，可以保证车载多媒体等业务的流畅播放。而且相对于其他无线技术，WLAN具备更大的带宽，可以为用户提供更多的数据业务。
- 车地通信快速切换的网络是基于Mesh单跳组网的二层网络，主要由WAC、轨旁AP和车载AP组成。
    - WAC：部署在轨道交通地面网络系统中，主要对轨旁AP进行管理和控制。
    - 轨旁AP：是FIT AP，作为MPP部署在轨道沿线，通过有线的方式和WAC二层互通。
    - 车载AP：是FAT AP，作为MP部署在车头和车尾，通过Mesh链路以无线的方式接入地面轨旁AP。
- 车地通信快速切换网络模型根据对车载AP不同的使用情况主要有以下三种：
    - 列车运行时，仅部署在车头的车载AP工作，车尾车载AP不工作。列车到达终点站后调换运行方向时，其工作的车载AP也会随之调换。
    - 列车运行时，仅部署在车尾的车载AP工作，车头车载AP不工作。列车到达终点站后调换运行方向时，其工作的车载AP也会随之调换。
    - 列车运行时，车头和车尾的车载AP均工作，以达到负载分担的效果，工作时两个车载AP使用不同的信道和轨旁AP通信。

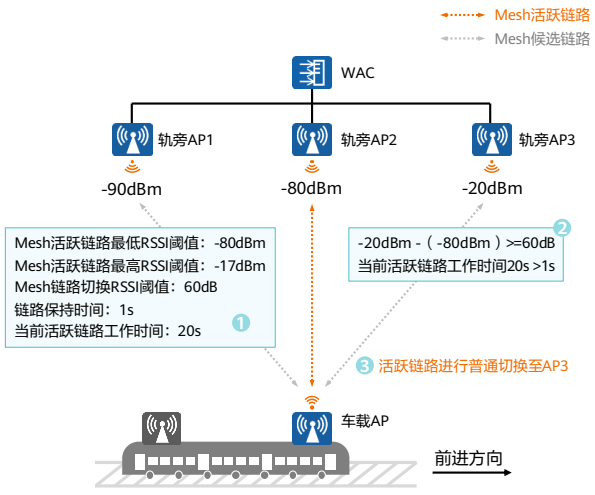
车地通信场景Mesh链路快速切换（2）

- 快速切换的实现过程主要分为：Mesh建链和拆链、链路快速切换和组播数据保障。
- 链路快速切换依靠车地通信快速切换算法实现，车地通信快速切换算法分为基础切换算法和基于位置信息的增强型切换算法。两种算法都需要根据链路条件进行普通切换或紧急切换。

- Mesh建链和拆链：
  - 在车地通信快速切换的应用中车载AP会和邻近的轨旁AP建立Mesh链路，只要轨旁AP的接收信号强度指示RSSI（Received Signal Strength Indicator）大于等于一定值（Mesh链路最低RSSI阈值–5dB），且建立的Mesh链接数没有达到最大值，车载AP就会和该轨旁AP建立Mesh链路，其建链过程和普通Mesh应用的建链过程相同。
  - 车载AP会和多个轨旁AP建立Mesh链路，并从中选取链路质量满足要求的Mesh链路作为数据传输的活跃链路，其他Mesh链路作为候选链路。随着列车的行进，车载AP会根据车地通信快速切换算法进行链路快速切换，选取质量更好的候选链路作为活跃链路，确保车地通信链路始终处于最佳状态。
  - 如果Mesh链路的信号强度小于一定值（Mesh链路最低RSSI阈值–5dB），且该Mesh链路为非活跃链路，则车载AP会进行拆链，断开该Mesh链路，以便和其他轨旁AP建立更好的Mesh链路。
- 基于位置信息的增强型切换算法：
  - 基于位置信息的增强型切换算法是在基础算法的基础上结合轨旁AP的位置信息，进行普通切换和紧急切换。
  - 在车地通信的应用场景中，由于暂时性的射频环境变化，离列车较远的轨旁AP信号在短暂的时间内可能会比离列车最近的轨旁AP信号好，如果此时活跃链路正好发生切换，活跃链路可能误切到较远的轨旁AP上。为了进一步提升车地通信链路的质量，减少活跃链路的切换次数，用户可以选择基于轨旁AP位置的增强型链路切换算法。该算法要求轨旁AP要以一定格式，在轨道沿线按递增或递减的顺序命名。

车地通信场景 - Mesh链路快速切换（普通切换）

- 列车在行进过程中，当链路同时满足以下三个条件时则进行普通切换：
  - 候选链路的RSSI - 当前活跃链路的RSSI >= Mesh链路切换RSSI阈值。
  - 候选链路为候选区域内链路。
  - 当前活跃链路的工作时间大于等于链路保持时间。

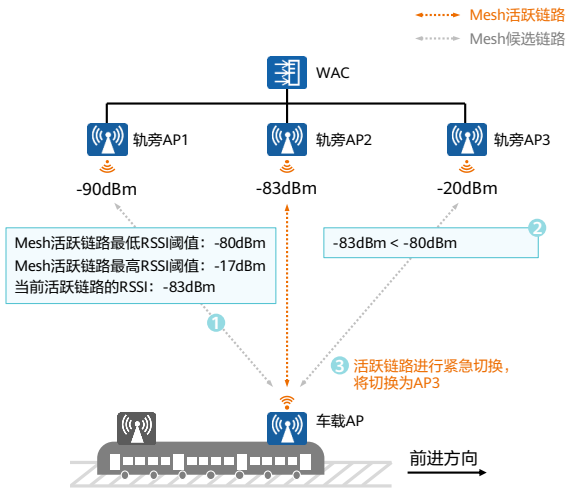


HUAWEI

- 关于“候选链路为候选区域内链路”：
  - “大于等于Mesh链路最低RSSI阈值且小于等于Mesh链路最高RSSI阈值”的区域被定义为“候选区域”。如果候选链路的RSSI值大于等于Mesh链路最低RSSI阈值且小于等于Mesh链路最高RSSI阈值，则认为该候选链路在候选区域内。反之，则候选链路在候选区域外。
- 当前活跃链路的工作时间大于等于链路保持时间：
  - 链路保持时间是为了防止活跃链路频繁切换影响链路质量而设置的，链路成为活跃链路的时长要大于等于链路保持时间，才允许当前活跃链路进行普通切换。否则，只允许链路进行紧急切换。
- 默认情况下mesh链路的保持时间为4000ms。

车地通信场景 - Mesh链路快速切换（紧急切换）

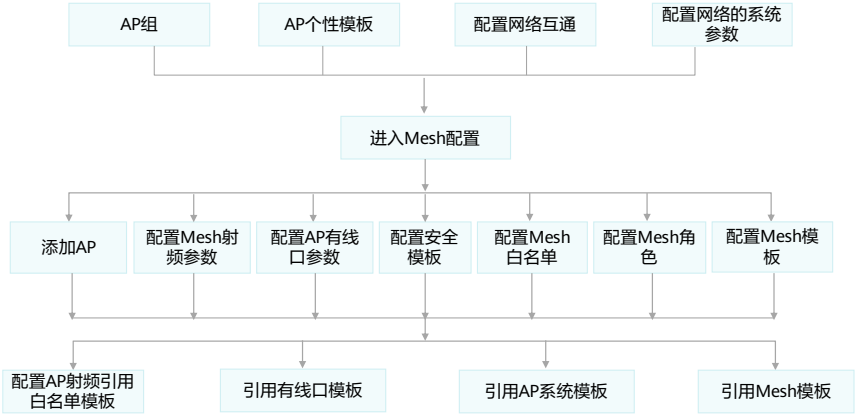
- 紧急切换发生在如下情形：
  - 候选链路的RSSI一直没有达到普通切换的条件，当活跃链路的RSSI值在候选区域外（小于Mesh链路最低RSSI阈值或大于Mesh链路最高RSSI阈值）时，进行紧急切换。
  - 当前活跃链路的RSSI在没有变差的情况下，其链路速率低于紧急切换最低速率阈值且低速率持续的时间达到了紧急切换最低速率持续时间，进行紧急切换。
  - 在进行紧急切换时，会在候选区域内选择RSSI最好的候选链路作为活跃链路。如果在候选区域内没有候选链路，且当前活跃链路没有断链，则不进行活跃链路的切换，保持当前活跃链路。



HUAWEI

- 轨旁AP故障等原因引起的活跃链路断链或者列车出站首次选取活跃链路时，由于当前没有活跃链路，所以也会进行紧急切换。切换时，首先在候选区域内选择质量最好的候选链路作为活跃链路。如果在候选区域内没有候选链路，则在其他区域内选择RSSI最好的候选链路作为活跃链路。
- 组播数据保障：
  - 在轨道交通中，车载播放器通过组播为乘客提供多媒体资讯服务，保障组播数据传输可以为乘客提供流畅的多媒体资讯服务。在车地通信的场景中，车载多媒体设备被加入一个组播组，由于活跃链路需要随着列车的前行不停的进行切换，仅轨旁AP和车载AP能感知到活跃链路的切换，其他地面设备（如轨旁AP接入的交换机等）无法感知链路切换，致使组播流无法正确转发。此时，车载AP和地面网络设备需使能IGMP Snooping功能，使车载AP和地面网络设备可以建立二层组播转发表。在切换新的链路后，车载AP发送Report报文给新的轨旁AP，新的轨旁AP通知地面网络设备也根据Report报文更新组播转发表。为了保证组播业务不中断，在新轨旁AP接收组播流之前，车载AP还是需要保证能从老的轨旁AP上接收组播流。当车载AP从新轨旁AP接收到组播流后，车载AP主动发送Leave报文给老的轨旁AP断开组播流，保证了组播数据流的“无缝切换”。

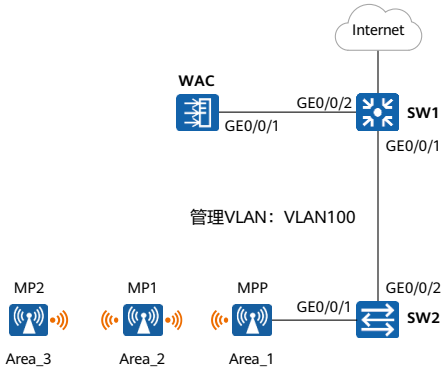
Mesh配置流程图



HUAWEI

- Mesh配置注意事项：
  - AP7060DN、WA375DD-CE、AP5510-W-GP、AD9431DN-24X（含配套RU）、AD9430DN-24（含配套RU）、AD9430DN-12（含配套RU）、AP7030DE、AP9330DN、AP2030DN、AP2050DN、AP2050DN-E、AP2050DN-S、AP2030DN-S、AP2051DN、AP2051DN-S、AP2051DN-L-S、AirEngine 5760-10、AP2051DN-E不支持Mesh功能。
  - 4.9G频段仅适用于室外无线回传的场景，只能用于WDS或Mesh无线回传链路，无法用于无线覆盖业务。4.9G频段不在DFS重选信道范围内。
  - 本章是只针对Mesh的配置过程，按照本章配置步骤配置完毕后，可以实现Mesh功能，即AP之间可以通过Mesh链路连接至AC。要实现用户的WLAN的业务应用，后续还需完成WLAN基本业务的配置任务，详细请参照WLAN基本业务配置。
  - WLAN Mesh功能与WLAN WDS功能互斥，即如果已配置了WLAN WDS功能，不能再进行WLAN Mesh配置。
  - 工作模式配置为monitor模式的射频，如果已部署WDS或Mesh业务，则射频实际生效模式为normal模式。
  - 在配置Mesh功能时，应尽量避免使用雷达信道。在Mesh建链时，使用雷达信道建立Mesh链路比使用非雷达信道慢几分钟至十几分钟。

Mesh普通业务配置案例需求

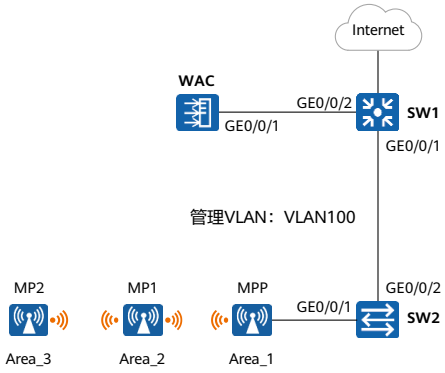


- 业务需求：
  - 在企业内部各区域通过建立Mesh无线回传链路，实现无线信号覆盖区域拓展，降低网络部署成本。
- 组网需求
  - WAC组网方式：旁挂在汇聚交换机上，与AP之间采用二层组网。
  - 无线回传方式：Mesh portal-node方式。
  - 回传射频：5G频段。

HUAWEI

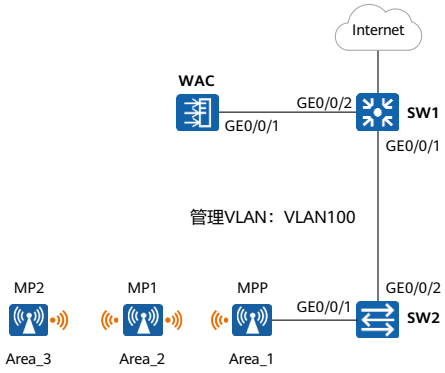
- 配置思路：
  - 配置网络互通，使区域A的AP（MPP节点）可以通过有线的方式在WAC上线。
  - 配置Mesh业务，使区域B和区域C的AP（MP节点）可以通过Mesh链路在WAC上线。

Mesh普通业务配置案例（1）



1.（略）配置周边设备SW1及SW2。
2.（略）配置WAC与其它网络设备互通。
3.（略）在WAC上使能DHCP功能，并通过接口地址池为AP分配IP地址。

Mesh普通业务配置案例（2）



4. 创建AP组，并配置国家码。

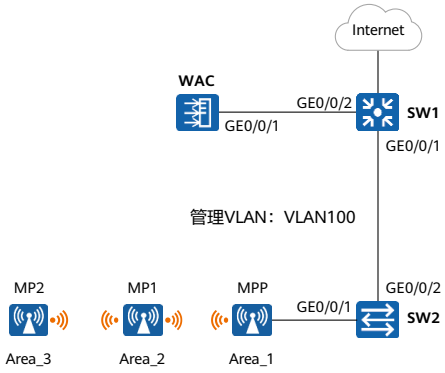
#创建MPP的AP组和MP的AP组，用于将相同配置的AP都加入同一AP组中。

```
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] quit
[WAC-wlan-view] ap-group name mesh-mp
```

#创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[WAC-wlan-view] regulatory-domain-profile name domain1
[WAC-wlan-regulate-domain-domain1] country-code CN
[WAC-wlan-regulate-domain-domain1] quit
#
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] regulatory-domain-profile domain1
[WAC-wlan-ap-group-mesh-mpp] quit
#
[WAC-wlan-view] ap-group name mesh-mp
[WAC-wlan-ap-group-mesh-mp] regulatory-domain-profile domain1
```

Mesh普通业务配置案例（3）



5. 配置WAC的源接口，并将AP手动加入AP组。

#配置WAC的源接口。

```
[WAC] capwap source interface vlanif 100
```

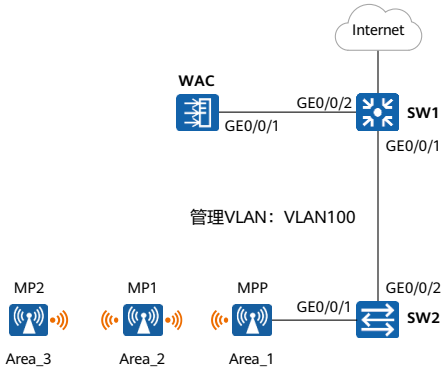
#将area_1加入到AP组“mesh-mpp”中，将area_2、area_3加入到AP组“mesh-mp”中。

```
[WAC] wlan
[WAC-wlan-view] ap auth-mode mac-auth
[WAC-wlan-view] ap-id 1 ap-mac 60de-4476-e360
[WAC-wlan-ap-1] ap-name area_1
[WAC-wlan-ap-1] ap-group mesh-mpp
#
[WAC-wlan-view] ap-id 2 ap-mac dcd2-fc04-b500
[WAC-wlan-ap-2] ap-name area_2
[WAC-wlan-ap-2] ap-group mesh-mp
```

#将area_3加入到AP组“mesh-mp”的配置与area_2相似，不再赘述。

- 举例中使用的AP为AP8130DN，具有射频0和射频1两个射频。

Mesh普通业务配置案例（4）



6. 配置Mesh的射频参数。

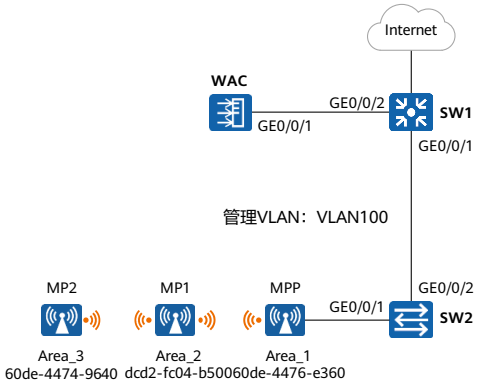
#配置Mesh节点使用的主要射频参数。

```
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] radio 1
[WAC-wlan-group-radio-mesh-mpp/1] channel 40mhz-plus 157
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-group-radio-mesh-mpp/1] coverage distance 4
[WAC-wlan-group-radio-mesh-mpp/1] quit
[WAC-wlan-ap-group-mesh-mpp] quit
#
[WAC-wlan-view] ap-group name mesh-mp
[WAC-wlan-ap-group-mesh-mp] radio 1
[WAC-wlan-group-radio-mesh-mp/1] channel 40mhz-plus 157
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-group-radio-mesh-mp/1] coverage distance 4
```


HUAWEI

- 本例中使用的是AP8130DN的射频1，“coverage distance”参数为射频覆盖距离，缺省情况下是3，单位是100m。本例中使用参数为4，用户可以根据实际情况配置该参数。

Mesh普通业务配置案例（5）



7. 配置Mesh的业务参数。

#配置Mesh链路使用的安全模板“mesh-sec”，“mesh-sec”支持WPA2+PSK+AES的安全策略。

```
[WAC-wlan-view] security-profile name mesh-sec
[WAC-wlan-sec-prof-mesh-sec] security wpa2 psk pass-phrase a1234567 aes
```

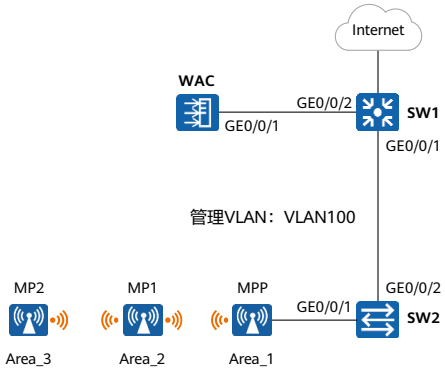
#配置Mesh白名单。

```
[WAC-wlan-view] mesh-whitelist-profile name mesh-list
[WAC-wlan-mesh-whitelist-mesh-list] peer-ap mac 60de-4476-e360
[WAC-wlan-mesh-whitelist-mesh-list] peer-ap mac dcd2-fc04-b500
[WAC-wlan-mesh-whitelist-mesh-list] peer-ap mac 60de-4474-9640
```

#配置Mesh角色。配置area_1的Mesh角色为“Mesh-portal”，缺省情况下Mesh角色为“Mesh-node”，所以area_2、area_3可以使用默认配置。Mesh角色是通过AP系统模板配置的。

```
[WAC-wlan-view] ap-system-profile name mesh-sys
[WAC-wlan-ap-system-prof-mesh-sys] mesh-role Mesh-portal
```

Mesh普通业务配置案例（6）



8. 配置Mesh模板和白名单。

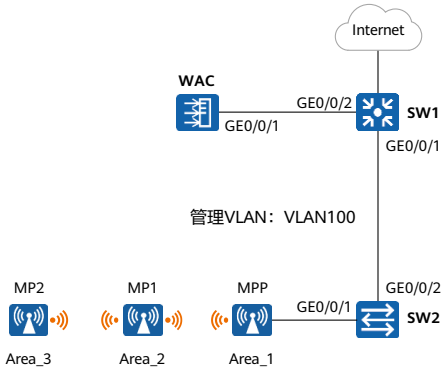
#配置Mesh模板。配置Mesh网络的ID为“mesh-net”，Mesh链路老化时间为30秒，并引用安全模板和Mesh白名单。

```
[WAC-wlan-view] mesh-profile name mesh-net
[WAC-wlan-mesh-prof-mesh-net] mesh-id mesh-net
[WAC-wlan-mesh-prof-mesh-net] link-aging-time 30
[WAC-wlan-mesh-prof-mesh-net] security-profile mesh-sec
```

#配置AP射频引用Mesh白名单模板。

```
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] radio 1
[WAC-wlan-group-radio-mesh-mpp/1] mesh-whitelist-profile mesh-list
[WAC-wlan-group-radio-mesh-mpp/1] quit
[WAC-wlan-ap-group-mesh-mpp] quit
[WAC-wlan-view] ap-group name mesh-mp
[WAC-wlan-ap-group-mesh-mp] radio 1
[WAC-wlan-group-radio-mesh-mp/1] mesh-whitelist-profile mesh-list
```

Mesh普通业务配置案例（7）



9. 在AP组引用相关模板，使Mesh业务生效。

#配置AP组“mesh-mpp”引用AP系统模板“mesh-sys”，使MPP角色在area_1上生效。

```
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] ap-system-profile mesh-sys
```

#配置AP组“mesh-mpp”和“mesh-mp”分别引用Mesh模板“mesh-net”，使Mesh业务生效。

```
[WAC-wlan-view] ap-group name mesh-mpp
[WAC-wlan-ap-group-mesh-mpp] mesh-profile mesh-net radio 1
[WAC-wlan-ap-group-mesh-mpp] quit
[WAC-wlan-view] ap-group name mesh-mp
[WAC-wlan-ap-group-mesh-mp] mesh-profile mesh-net radio 1
```

Mesh普通业务配置案例（8）

10. 验证Mesh业务配置结果。

```
<WAC> display ap all
Total AP information:
nor : normal          [3]
Extra information: P : insufficient power supply
--------------------------------------------------------------------------------------------------------------------------------
ID   MAC                 Name        Group       IP              Type          State  STA  Uptime     ExtraInfo
--------------------------------------------------------------------------------------------------------------------------------
1    60de-4476-e360      area_1      mesh-mpp    10.23.100.254   AP8130DN      nor    0    13M:45S    -
2    dcd2-fc04-b500      area_2      mesh-mp     10.23.100.251   AP8130DN      nor    0    5M:22S     -
3    60de-4474-9640      area_3      mesh-mp     10.23.100.253   AP8130DN      nor    0    4M:14S     -
--------------------------------------------------------------------------------------------------------------------------------
Total: 3
```

完成配置后，执行命令display ap all，查看Mesh各节点是否成功上线，当“State”字段显示为“nor”，则表示AP已成功上线。

Mesh普通业务配置案例（9）

11. 验证Mesh业务配置结果。

```
<WAC> display wlan mesh link all
Rf   : radio ID                 Dis  : coverage distance(100m)
Ch   : channel                  Per  : drop percent(%)
TSNR : total SNR(dB)            P-   : peer
Mesh : Mesh mode                Re   : retry ratio(%)
RSSI : RSSI(dBm)                MaxR : max RSSI(dBm)
--------------------------------------------------------------------------------------------------------------------------------
APName     P-APName   P-APMAC          Rf Dis  Ch   Mesh  P-Status  RSSI  MaxR  Per  Re  TSNR  SNR(Ch0~3:dB)  Tx(Mbps)  Rx(Mbps)
--------------------------------------------------------------------------------------------------------------------------------
area_1     area_2     dcd2-fc04-b500   1  4    157  portal normal    -30   -27   0    12  67    62/65/-/-      192       192
area_1     area_3     60de-4474-9640   1  4    157  portal normal    -26   -24   0    12  71    67/68/-/-      192       192
area_3     area_2     dcd2-fc04-b500   1  4    157  node   normal    -19   -3    0    5   77    66/76/-/-      192       192
area_3     area_1     60de-4476-e360   1  4    157  node   normal    -32   -4    0    26  64    55/63/-/-      192       192
area_2     area_1     60de-4476-e360   1  4    157  node   normal    -32   -4    0    12  64    62/61/-/-      192       192
area_2     area_3     60de-4474-9640   1  4    157  node   normal    -14   -12   0    4   82    71/82/-/-      192       192
--------------------------------------------------------------------------------------------------------------------------------
Total: 6
```


- Mesh业务生效后，执行命令**display wlan mesh link all**，查看Mesh链路相关信息。

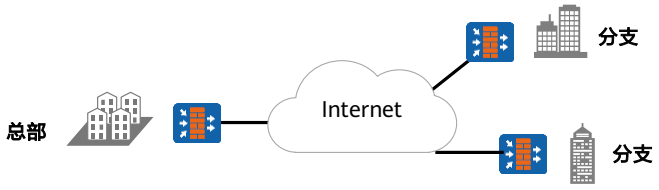
查看Mesh链路信息

功能描述	命令行
查看Mesh型VAP的相关信息	**display mesh vap** { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**mesh-id** *mesh-id*]
查看所有的或指定网络标识的Mesh型VAP的信息	**display mesh vap** { **all** | **mesh-id** *mesh-id* }，可以查看所有的或指定网络标识的Mesh型VAP的信息
查看Mesh链路的相关信息	**display wlan mesh link** { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **mesh-profile** *profile-name* }

目录

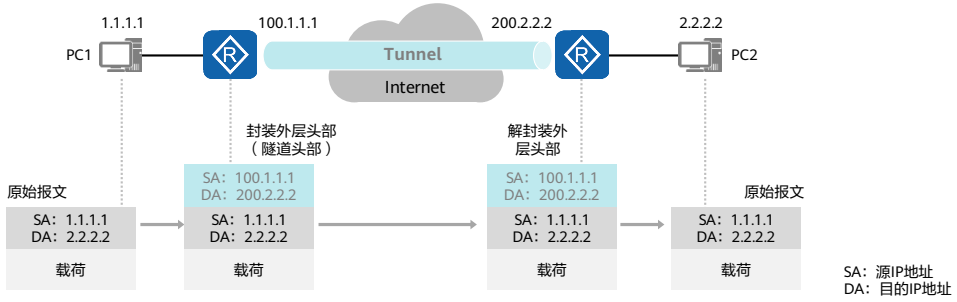
VPN产生的背景及基本概念

- A公司在各地都有分支，分支与总部、分支与分支之间的网络需要安全、可靠地互访，如果租用专线将分支及总部连接起来固然满足需求，但成本太高。直接用Internet来传输数据又存在安全问题。
- 基于IP的VPN（Virtual Private Network，虚拟专用网）是通过相关技术在共享的IP网络基础设施上模拟出来的专用网络设施。VPN有两个显著的特点：专用型、虚拟性。



隧道技术原理

- 隧道（Tunnel）类似于一座桥，可以在底层网络（比如Internet）之上构建转发通道，用户可以自行构建隧道网络，不需要底层网络的管理者（比如运营商）介入。
- 实现隧道的技术有很多，常见的隧道技术有：MPLS，GRE，L2TP，IPSec，VXLAN等，虽然有各种各样的隧道技术，但其基本实现思路是一致的。



HUAWEI

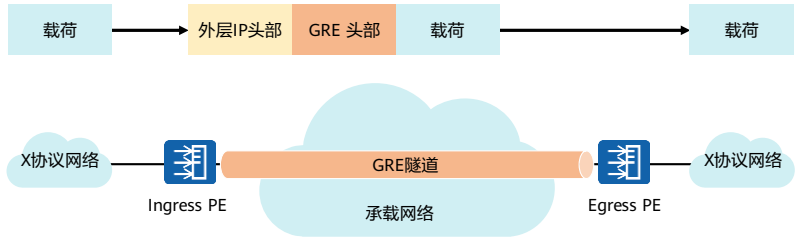
GRE简介

- 通用路由封装协议GRE（Generic Routing Encapsulation）可以对某些网络层协议（如IPX、IPv6、AppleTalk等）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如IPv4）中传输。
- GRE提供了将一种协议的报文封装在另一种协议报文中的机制，是一种三层隧道封装技术，使报文可以通过GRE隧道透明的传输，解决异种网络的传输问题。

- GRE实现机制简单，对隧道两端的设备负担小。
- GRE隧道可以通过IPv4网络连通多种网络协议的本地网络，有效利用了原有的网络架构，降低成本。
- GRE隧道扩展了跳数受限网络协议的工作范围，支持企业灵活设计网络拓扑。

基本原理

- 报文在GRE隧道中传输包括封装和解封装两个过程。如图所示，如果X协议报文从Ingress PE向Egress PE传输，则封装在Ingress PE上完成，而解封装在Egress PE上进行。封装后的数据报文在网络中传输的路径，称为GRE隧道。



HUAWEI

- 封装：
  - Ingress PE从连接X协议的接口接收到X协议报文后，首先交由X协议处理。
  - X协议根据报文头中的目的地址在路由表或转发表中查找出接口，确定如何转发此报文。如果发现出接口是GRE Tunnel接口，则对报文进行GRE封装，即添加GRE头。
  - 承载网络的传输协议为IP，因此给报文加上外层IP头。IP头的源地址就是隧道源地址，目的地址就是隧道目的地址。
  - 根据该IP头的目的地址（即隧道目的地址），在承载网络的路由表中查找相应的出接口并发送报文。之后，封装后的报文将在该网络中传输。
- 解封装：
  - 解封装过程和封装过程相反。
    - Egress PE从GRE Tunnel接口收到该报文，分析IP头发现报文的目的地址为本设备，则Egress PE去掉IP头后交给GRE协议处理。
    - GRE协议剥掉GRE报头，获取X协议，再交由X协议对此数据报文进行后续的转发处理。

GRE的Keepalive检测

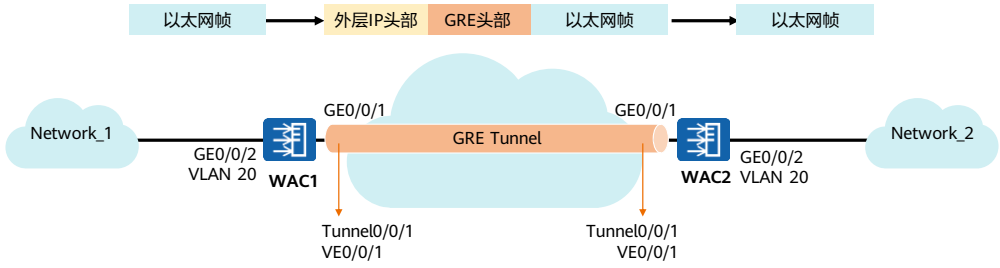
- 由于GRE协议并不具备检测链路状态的功能，如果对端接口不可达，隧道并不能及时关闭该Tunnel连接，这样会造成源端会不断的向对端转发数据，而对端却因隧道不通接收不到报文，由此就会形成数据空洞。
- GRE的Keepalive检测功能可以检测隧道状态，即检测隧道对端是否可达。如果对端不可达，隧道连接就会及时关闭，避免因对端不可达而造成的数据丢失，有效防止数据空洞，保证数据传输的可靠性。

HUAWEI

- Keepalive检测功能的实现过程如下：
  - 当GRE隧道的源端使能Keepalive检测功能后，就创建一个定时器，周期地发送Keepalive探测报文，同时通过计数器进行不可达计数。每发送一个探测报文，不可达计数加1。
  - 对端每收到一个探测报文，就给源端发送一个回应报文。
  - 如果源端的计数器值未达到预先设置的值就收到回应报文，就表明对端可达。如果源端的计数器值到达预先设置的值——重试次数（Retry Times）时，还没收到回送报文，就认为对端不可达。此时，源端将关闭隧道连接。但是源端口仍会继续发送Keepalive报文，若对端Up，则源端口也会Up，建立隧道链接。
- 注意：
  - 对于设备实现的GRE Keepalive检测功能，只要在隧道一端配置Keepalive，该端就具备Keepalive功能，而不要求隧道对端也具备该功能。隧道对端收到报文，如果是Keepalive探测报文，无论是否配置Keepalive，都会给源端发送一个回应报文。

Ethernet over GRE

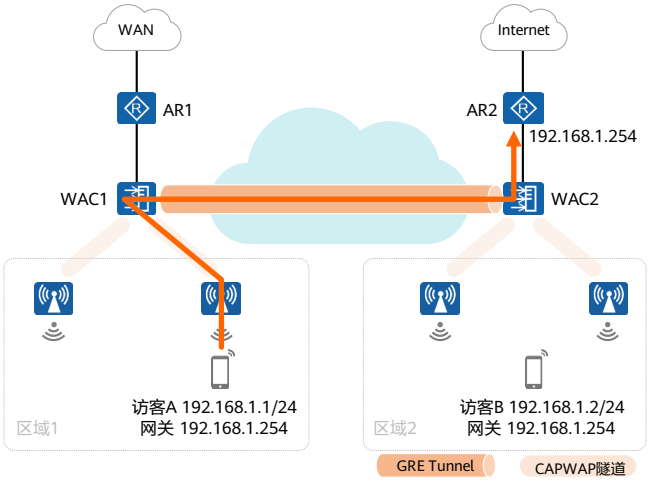
- 如图所示，Network_1和Network_2网络都是以太网络，两个网络之间通过IP/MPLS骨干网相连，如果用户希望两个网络之间能够二层互通，可以部署Ethernet over GRE功能（也称EoGRE），实现以太报文通过GRE隧道进行透传。



HUAWEI

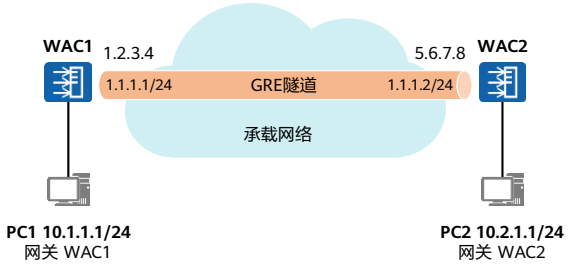
- Ethernet over GRE是将以太网协议的报文通过GRE封装后，在另一个网络层协议（如IPv4）的网络中传输，具体工作原理如下：
  - WAC1的用户侧物理以太网接口GE0/0/2收到Network_1的以太报文，以太报文中携带了VLAN Tag信息。
  - WAC1从GE0/0/2收到的以太报文后，在设备内基于MAC和VLAN进行二层转发，找到出接口VE0/0/1。
  - 以太报文在WAC1的VE0/0/1上进行出接口处理后，将转发到VE0/0/1绑定的Tunnel0/0/1接口，经过GRE封装（协议代码为0x6558）后，进行后续的GRE转发处理，报文经过GRE隧道转发至WAC2。
  - WAC2的Tunnel0/0/1接口上对收到的报文进行GRE解封装，检查到协议代码为0x6558后，将以太报文转发给Tunnel0/0/1接口绑定的VE0/0/1接口。
  - GRE解封装后的以太网报文进入WAC2的VE0/0/1以后，在设备内基于MAC和VLAN进行二层转发，找到出接口GE0/0/2。
  - WAC2将以太报文从出接口GE0/0/2发往Network_2。

通过Ethernet over GRE实现WAC之间的二层互通



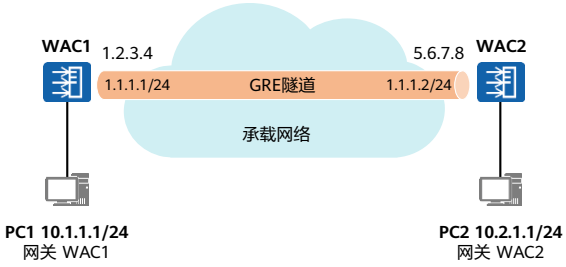
- 某企业供访客接入的区域分为两个区域，两个区域之间通过IP/MPLS骨干网相连。
- 两个区域的访客终端的网关统一为AR2，且由AR2为访客终端分配IP地址。即要求区域1的访客终端与AR2之间二层可达。
- 网络管理员可以在WAC1和WAC2上部署Ethernet over GRE功能，将WAC1上所有访客的流量通过Ethernet over GRE隧道转发至WAC2。

配置GRE通过静态路由实现IPv4协议互通示例（1）



- 组网需求：
  - 实现PC1和PC2通过承载网络互通，承载网络对PC1及PC2所在网段并无感知。
  - 需要在WAC1和WAC2之间建立“直连链路”，部署GRE隧道，通过静态路由指定到达对端的报文通过Tunnel接口转发，PC1和PC2就可以互相通信了。

配置GRE通过静态路由实现IPv4协议互通示例（2）



1.（略）配置各物理接口的IP地址。

2.（略）完成承载网络的路由配置，使得WAC1的1.2.3.4地址可与WAC2的5.6.7.8地址之间路由可达。

3. 在WAC1上配置GRE隧道接口。

```
[WAC1] interface tunnel 1
[WAC1-Tunnel1] tunnel-protocol gre
[WAC1-Tunnel1] ip address 1.1.1.1 255.255.255.0
[WAC1-Tunnel1] source 1.2.3.4
[WAC1-Tunnel1] destination 5.6.7.8
```

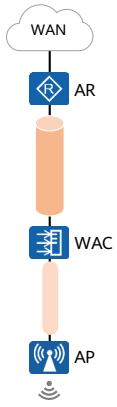
4. 在WAC2上配置GRE隧道接口。

```
[WAC2] interface tunnel 1
[WAC2-Tunnel1] tunnel-protocol gre
[WAC2-Tunnel1] ip address 2.2.2.2 255.255.255.0
[WAC2-Tunnel1] source 5.6.7.8
[WAC2-Tunnel1] destination 1.2.3.4
```

5. 在WAC1及WAC2上配置静态路由。

```
[WAC1] ip route-static 10.2.1.0 255.255.255.0 tunnel 1
[WAC2] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

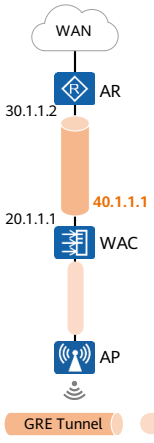
配置Ethernet over GRE实现WAC与无线网关二层互通示例（1）



- 组网需求：
  - 在某无线城市项目中，AP负责用户流量的接入，WAC负责AP的接入和用户的认证，AR作为用户网关负责IP地址分配及Internet接入等功能。
  - 由于该局点的需要接入的AP数量非常多，因此为避免AR上大量的GRE隧道频繁建立及删除导致资源消耗严重等问题，采用WAC和AR之间通过Ethernet over GRE实现二层互通的方案。
- 在WAC侧部署Ethernet over GRE隧道的配置思路如下：
  - 所有设备之间运行IGP路由协议实现公网互通。
  - 在WAC上创建Tunnel接口，部署GRE隧道。
  - 在WAC上创建VE接口，并接入相应的VLAN。
  - 在WAC上将VE接口与GRE隧道绑定，实现Ethernet报文通过GRE隧道转发。

- 本举例仅给出WAC侧的Ethernet over GRE相关配置，涉及WLAN的相关配置及AR上的Ethernet over GRE相关配置请参考相应的配置文档。

配置Ethernet over GRE实现WAC与无线网关二层互通示例（2）



1.（略）配置WAC各物理接口的IP地址。

2. 在WAC上配置Tunnel接口，部署GRE隧道。这里假设GRE隧道的源接口地址为20.1.1.1，目的接口地址为30.1.1.2。

```
[WAC] interface tunnel 1
[WAC-Tunnel1] tunnel-protocol gre
[WAC-Tunnel1] ip address 40.1.1.1 255.255.255.0
[WAC-Tunnel1] source 20.1.1.1
[WAC-Tunnel1] destination 30.1.1.2
```

3. 创建VE接口并加入VLAN，注意VE接口和用户侧报文的入接口加入相同的VLAN。

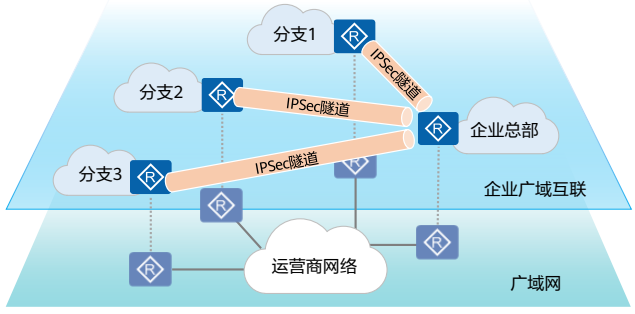
```
[WAC] interface Virtual-Ethernet0/0/1
[WAC-Virtual-Ethernet0/0/1] portswitch
[WAC-Virtual-Ethernet0/0/1] port link-type trunk
[WAC-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[WAC-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 30
```

4. VE接口与GRE隧道绑定，实现Ethernet报文通过GRE隧道转发。

```
[WAC] interface tunnel 1
[WAC-Tunnel1] map interface virtual-ethernet 0/0/1
```

IPSec VPN的产生背景

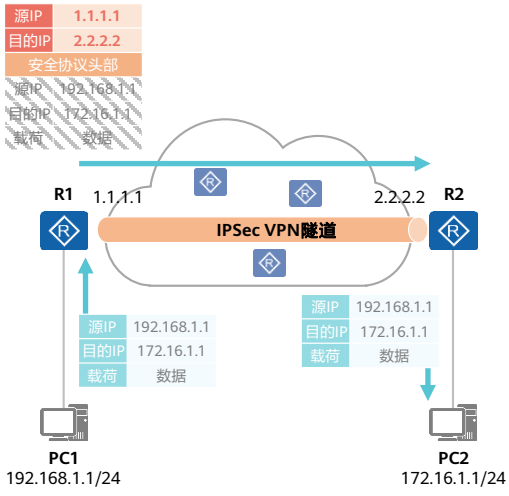
- 企业分支之间经常有互联的需求，企业互联的方式很多，可以使用广域网专线或者Internet线路。
- 部分企业从成本和需求出发会选择使用Internet进行互联，但是存在安全风险，需要保障数据在传输时不会被窃取或者被篡改。
- IPSec通过将数据报文进行加密传输，达到保障企业安全互联的目的。



HUAWEI

- IPSec VPN指的是通过IPSec技术保护的VPN隧道。

IPSec简介



- 网络中部署IPSec （Internet Protocol Security）后，可对传输的数据进行保护处理，降低信息泄露的风险。
- IPSec是IETF制定的一组开放的网络安全协议。
- IPSec通过加密与验证等方式，从以下几个方面保障了用户业务数据在Internet中的安全传输：
  - 数据来源验证（身份验证）
  - 数据加密
  - 数据完整性校验
  - 抗重放攻击

HUAWEI

- IPSec通过加密与验证等方式，从以下几个方面保障了用户业务数据在Internet中的安全传输：数据来源验证：接收方验证发送方身份是否合法。
- 数据加密：发送方对数据进行加密，以密文的形式在Internet上传送，接收方对接收的加密数据进行解密后处理或直接转发。
- 数据完整性：接收方对接收的数据进行验证，以判定报文是否被篡改。
- 抗重放：接收方拒绝旧的或重复的数据包，防止恶意用户通过重复发送捕获到的数据包所进行的攻击。

IPSec协议框架

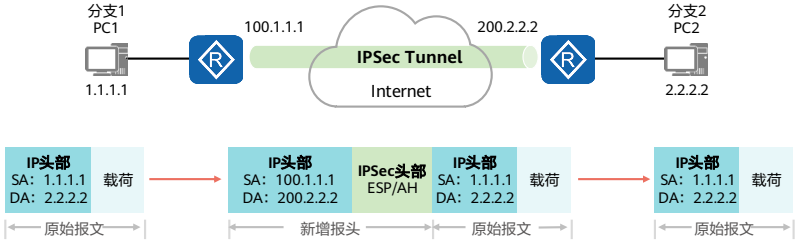
- IPSec并不是一个单独的协议，而是一种公开标准的技术解决方案。

HUAWEI

- IPSec通过验证头AH（Authentication Header）和封装安全载荷ESP（Encapsulating Security Payload）两个安全协议实现IP报文的安全保护：
  - AH是报文头验证协议，主要提供数据源验证、数据完整性验证和防报文重放功能，不提供加密功能。
  - ESP是封装安全载荷协议，主要提供加密、数据源验证、数据完整性验证和防报文重放功能。
- AH和ESP协议提供的安全功能依赖于协议采用的验证、加密算法：
  - AH和ESP都能够提供数据源验证和数据完整性验证，使用的验证算法为MD5（Message Digest 5）、SHA1（Secure Hash Algorithm 1）、SHA2-256、SHA2-384和SHA2-512，以及SM3（Senior Middle 3）算法。
  - ESP还能够对IP报文内容进行加密，使用的加密算法为对称加密算法，包括DES（Data Encryption Standard）、3DES（Triple Data Encryption Standard）、AES（Advanced Encryption Standard）、SM1、SM4。
- IPSec加密和验证算法所使用的密钥可以手工配置，也可以通过因特网密钥交换IKE（Internet Key Exchange）协议动态协商。IKE协议建立在Internet安全联盟和密钥管理协议ISAKMP（Internet Security Association and Key Management Protocol）框架之上，采用DH（Diffie-Hellman）算法在不安全的网络上安全地分发密钥、验证身份，以保证数据传输的安全性。IKE协议可提升密钥的安全性，并降低IPSec管理复杂度。

IPSec封装模式 - 隧道模式

- 封装模式是指将AH（authentication header）或ESP（Encapsulating Security Payload）相关的字段插入到原始IP报文中，以实现对报文的认证和加密，封装模式有传输模式和隧道模式两种。



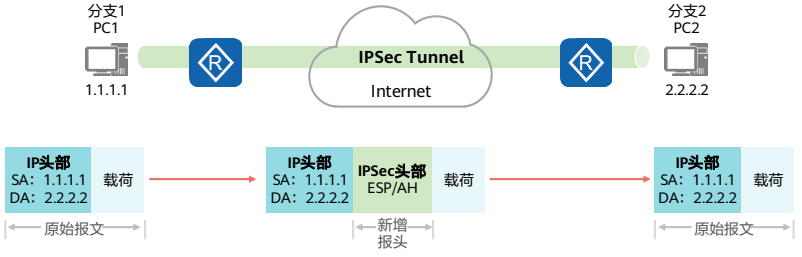
在隧道模式下，AH头或ESP头被插到原始IP头之前，另外生成一个新的报文头放到AH头或ESP头之前，保护IP头和负载。隧道模式主要应用于两台VPN网关之间或一台主机与一台VPN网关之间的通信。

HUAWEI

- 隧道模式下，AH协议的完整性验证范围为包括新增IP头在内的整个IP报文。ESP协议验证报文的完整性检查部分包括ESP头、原IP头、传输层协议头、数据和ESP报尾，但不包括新IP头，因此ESP协议无法保证新IP头的安全。ESP的加密部分包括原IP头、传输层协议头、数据和ESP报尾。
- 注：在本例中，ESP的尾部数据或认证数据未在图中体现。

IPSec封装模式 - 传输模式

- 封装模式是指将AH或ESP相关的字段插入到原始IP报文中，以实现对报文的认证和加密，封装模式有传输模式和隧道模式两种。



在传输模式中，AH头或ESP头被插入到IP头与传输层协议头之间，保护TCP/UDP/ICMP负载。传输模式不改变报文头，故隧道的源和目的地址必须与IP报文头中的源和目的地址一致，所以只适合两台主机或一台主机和一台VPN网关之间通信。

HUAWEI

- 传输模式下，AH协议的完整性验证范围为整个IP报文。ESP协议验证报文的完整性检查部分包括ESP头、传输层协议头、数据和ESP报尾，但不包括IP头，因此ESP协议无法保证IP头的安全。ESP的加密部分包括传输层协议头、数据和ESP报尾。
- 注：在本例中，ESP的尾部数据或认证数据未在图中体现。

IPSec安全协议

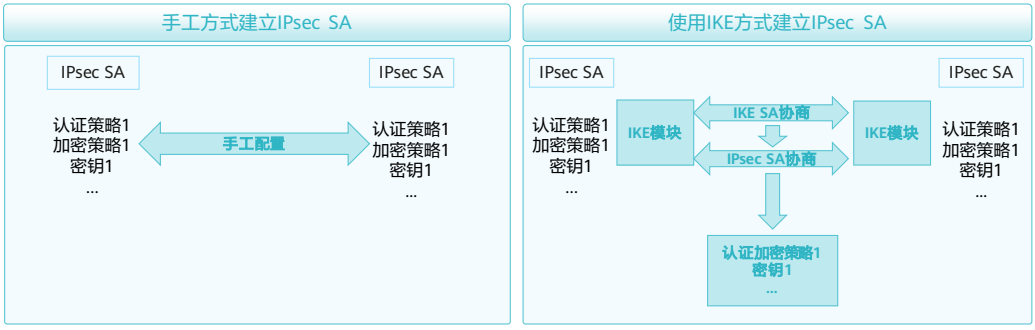
- IPsec使用认证头AH和封装安全载荷ESP两种安全协议来传输和封装数据，提供认证或加密等安全服务。

AH	AH认证包头协议。 提供数据源认证、数据完整性校验、防重放攻击等功能； 不支持数据加密。
ESP	ESP封装安全荷载协议。 提供数据源认证、数据完整性校验、防重放攻击、数据加密等功能。

  - AH和ESP协议提供的安全功能依赖于协议采用的验证、加密算法:
  - AH和ESP都能够提供数据源验证和数据完整性验证，使用的验证算法为MD5（Message Digest 5）、SHA1（Secure Hash Algorithm 1）、SHA2-256、SHA2-384和SHA2-512，以及SM3（Senior Middle 3）算法。
  - ESP还能够对IP报文内容进行加密，使用的加密算法为对称加密算法，包括DES（Data Encryption Standard）、3DES（Triple Data Encryption Standard）、AES（Advanced Encryption Standard）、SM1、SM4。

安全联盟介绍

- IPsec SA（Security Association，安全联盟）可以帮助IPsec对特定要素进行约定，比如：加密算法使用DES，认证算法使用MD5，封装方式使用Tunnel等。
- 建立IPsec SA一般有两种方式：手工方式和IKE方式，分别适用于小型网络和中大型网络。



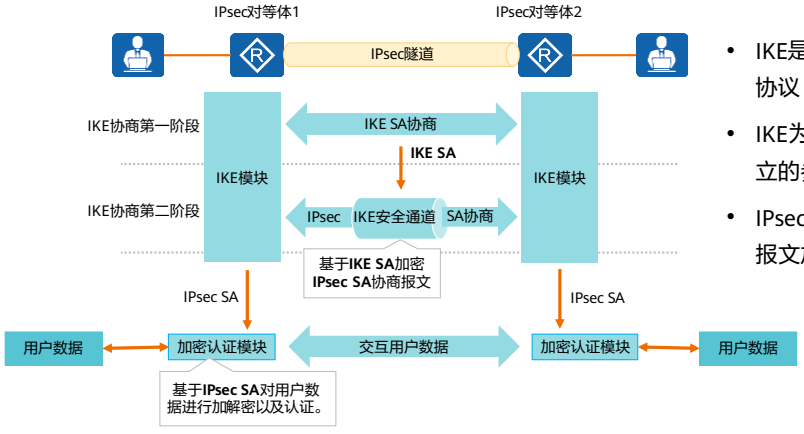
HUAWEI

- SA是单向的逻辑连接，因此两个IPsec对等体之间的双向通信，最少需要建立两个SA来分别对两个方向的数据流进行安全保护。
- 有两种方式建立IPsec安全联盟：手工方式和IKE自动协商方式。二者的主要区别为：
  - 密钥生成方式不同：手工方式下，建立SA所需的全部参数，包括加密、验证密钥，都需要用户手工配置，也只能手工刷新，在中大型网络中，这种方式的密钥管理成本很高；IKE方式下，建立SA需要的加密、验证密钥是通过DH算法生成的，可以动态刷新，因而密钥管理成本低，且安全性较高。
  - 生存周期不同：手工方式建立的SA，一经建立永久存在；IKE方式建立的SA，其生存周期由双方配置的生存周期参数控制。
- 因此，手工方式适用于对等体设备数量较少时，或是在小型网络中。对于中大型网络，推荐使用IKE自动协商建立SA。

IKE介绍

- 因特网密钥交换IKE（Internet Key Exchange）协议建立在Internet安全联盟和密钥管理协议ISAKMP(Internet Security Association and Key Management Protocol)定义的框架上，是基于UDP（User Datagram Protocol）的应用层协议。
- 它为IPsec提供了自动协商密钥、建立IPsec安全联盟的服务，能够简化IPsec的使用和管理，大大简化IPsec的配置和维护工作。
- IKE的主要作用：
  - 降低IPsec手工配置的复杂度
  - 安全联盟定时更新
  - 密钥定时更新
  - 允许在端与端之间动态认证

IKE与IPsec的关系



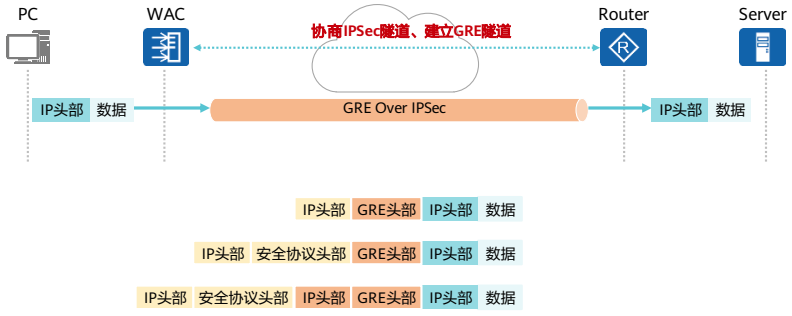
- IKE是基于UDP之上的一个应用层协议，是IPsec的信令协议。
- IKE为IPsec协商建立SA，并把建立的参数及生成的密钥交给IPsec。
- IPsec使用IKE建立的IPsec SA对IP报文加密或验证处理。

HUAWEI

- IKE是UDP之上的一个应用层协议，是IPsec的信令协议。
- IKE与IPsec的关系如上图所示，对等体之间建立一个IKE SA完成身份验证和密钥信息交换后，在IKE SA的保护下，根据配置的AH/ESP安全协议等参数协商出一对IPsec SA。此后，对等体间的数据将在IPsec隧道中加密传输。

IPSec增强原理 - GRE over IPSec

- GRE over IPSec可利用GRE和IPSec的优势，通过GRE将组播、广播和非IP报文封装成普通的IP报文，通过IPSec为封装后的IP报文提供安全地通信，进而可以提供在总部和分支之间安全地传送广播、组播的业务，例如视频会议或动态路由协议消息等。

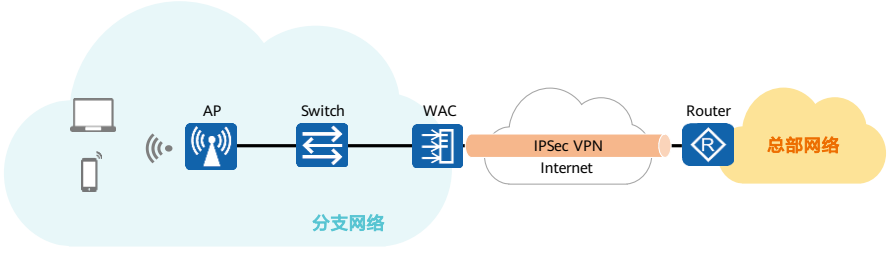


HUAWEI

- 当网关之间采用GRE over IPSec连接时，先进行GRE封装，再进行IPSec封装。GRE over IPSec使用的封装模式为可以是隧道模式也可以是传输模式。因为隧道模式跟传输模式相比增加了IPSec头，导致报文长度更长，更容易导致分片，所以推荐采用传输模式GRE over IPSec。
- IPSec封装过程中增加的IP头即源地址为IPSec网关应用IPSec安全策略的接口地址，目的地址即IPSec对等体中应用IPSec安全策略的接口地址。
- IPSec需要保护的数据流为从GRE起点到GRE终点的数据流。GRE封装过程中增加的IP头即源地址为GRE隧道的源端地址，目的地址为GRE隧道的目的端地址。

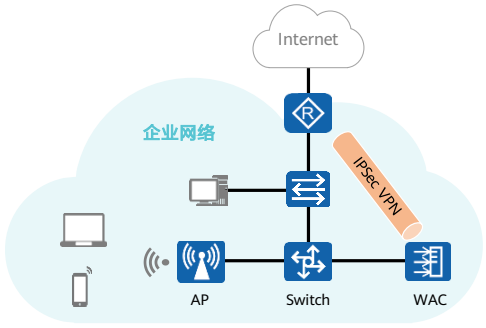
IPSec应用场景：WAC作为分支网关与总部网关建立IPSec隧道

- WAC作为企业分支网关，用户通过无线接入网络。分支和总部之间的数据流通过IPSec隧道进行安全保护传送，虽然是在公网上传输，但都得到加密和认证保护。



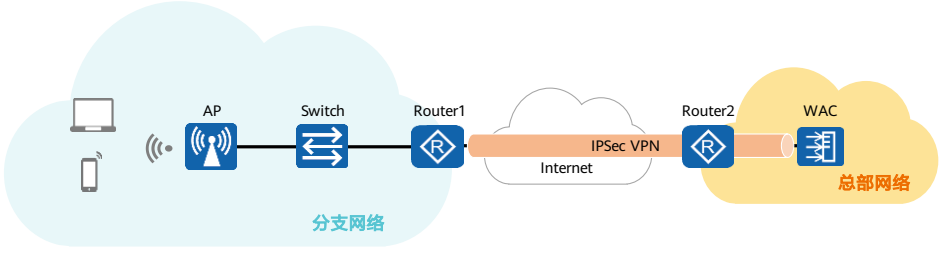
IPSec应用场景：WAC与企业内部网关建立IPSec隧道

- WAC在企业内部，企业有独立的出口网关（Router）。用户通过无线接入网络，WAC和Router之间的数据流通过IPSec隧道进行安全保护传送，虽在企业内部传输，但都得到加密和认证保护，以防被获取。



IPSec应用场景：分支AP通过IPSec隧道与总部WAC互联

- WAC在企业总部内部，有独立的出口网关（Router2）。企业分支未部署WAC，分支网关与总部WAC建立IPSec隧道，分支AP通过IPSec隧道与总部WAC互联，以防数据被获取。

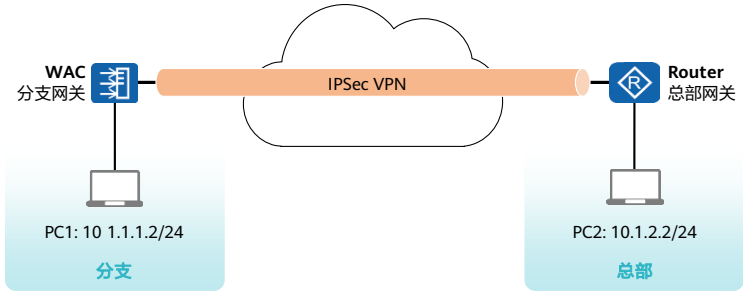


IPSec隧道建立方式

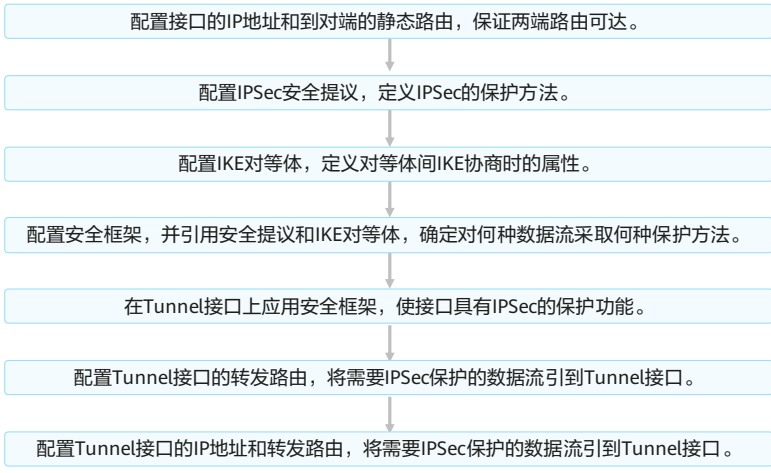
方式	描述
采用ACL方式建立IPSec隧道	由ACL来指定要保护的数据流范围，通过配置安全策略并将安全策略绑定在实际的接口上来完成IPSec的配置。采用ACL方式建立IPSec隧道包括手工方式和IKE动态协商方式。 有以下两种方式建立SA： • 手工方式：SA所需的全部信息都必须手工配置。 • IKE动态协商方式：由IKE协议完成密钥的自动协商，实现动态协商来创建和维护SA。 当对等体设备数量较少时，或是在小型网络中，手工配置SA是可行的。对于中大型网络中，推荐使用IKE协商建立SA。
采用虚拟隧道接口方式建立IPSec隧道	采用虚拟隧道接口建立IPSec隧道是基于路由方式。这种方式下，由路由来选择需要保护的数据流。通过配置安全框架并在虚拟隧道接口上应用安全框架来完成IPSec的配置。所有路由到IPSec虚拟隧道接口的报文都将进行IPSec保护。

配置虚拟隧道接口建立GRE over IPSec示例

- WAC为公司分支网关，Router为公司总部网关，分支与总部通过公网建立通信。
- 公司希望对分支与总部之间相互访问的流量进行安全保护。分支与总部通过公网建立通信，可以在分支网关与总部网关之间建立一个IPSec隧道来实施安全保护。
- 由于分支较为庞大，有大量需要IPSec保护的数据流，可基于虚拟隧道接口方式建立GRE over IPSec，对Tunnel接口下的流量进行保护，不需使用ACL定义待保护的流量特征。



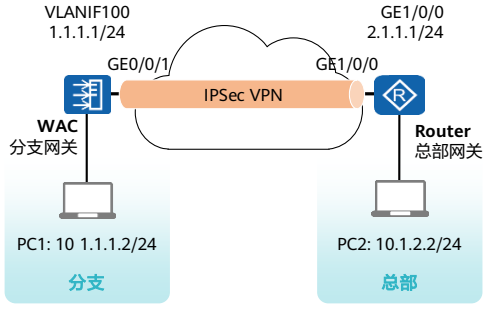
GRE over IPSec 配置流程



HUAWEI

- 本例仅关注IPSec配置。

配置虚拟隧道接口建立GRE over IPSec示例（1）



1.（略）分别在WAC和Router上配置接口的IP地址和到对端的静态路由。

2. 分别在WAC和Router上创建IPSec安全提议。

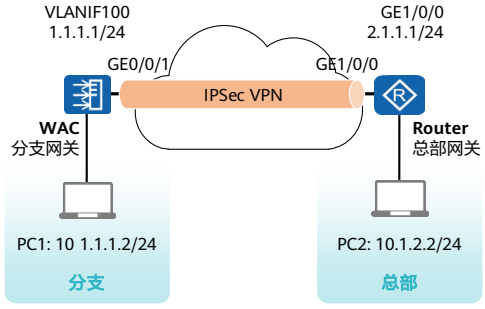
#在WAC上配置IPSec安全提议。

```
[WAC] ipsec proposal tran1
[WAC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[WAC-ipsec-proposal-tran1] esp encryption-algorithm aes-128
```

#在Router上配置IPSec安全提议。

```
[Router] ipsec proposal tran1
[Router-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[Router-ipsec-proposal-tran1] esp encryption-algorithm aes-128
```

配置虚拟隧道接口建立GRE over IPSec示例（2）



3. 分别在WAC和Router上配置IKE对等体。

#在WAC上配置IKE安全提议。

```
[WAC] ike proposal 5
[WAC-ike-proposal-5] authentication-algorithm sha2-256
[WAC-ike-proposal-5] encryption-algorithm aes-128
[WAC-ike-proposal-5] dh group14
```

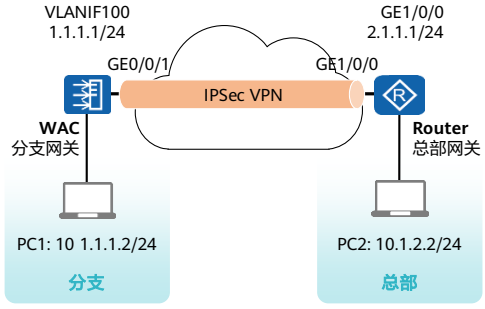
#在AC上配置IKE对等体。

```
[WAC] ike peer spub
[WAC-ike-peer-spub] undo version 2
[WAC-ike-peer-spub] ike-proposal 5
[WAC-ike-peer-spub] pre-shared-key cipher huawei@1234
```

#在Router上配置IKE安全提议。

```
[Router] ike proposal 5
[Router-ike-proposal-5] authentication-algorithm sha2-256
[Router-ike-proposal-5] encryption-algorithm aes-128
[Router-ike-proposal-5] dh group14
```

配置虚拟隧道接口建立GRE over IPSec示例（3）



#在Router上配置IKE对等体。

```
[Router] ike peer spua
[Router-ike-peer-spua] undo version 2
[Router-ike-peer-spua] ike-proposal 5
[Router-ike-peer-spua] pre-shared-key cipher huawei@1234
```

4.分别在WAC和Router上创建安全框架。

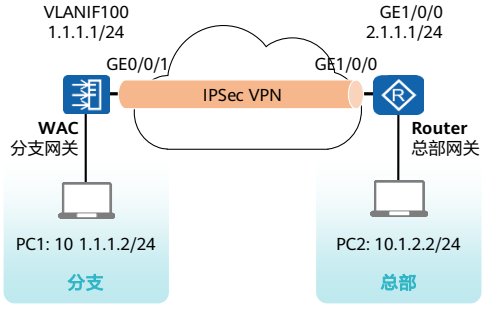
#在WAC上配置安全框架。

```
[WAC] ipsec profile profile1
[WAC-ipsec-profile-profile1] proposal tran1
[WAC-ipsec-profile-profile1] ike-peer spub
```

#在Router上配置安全框架。

```
[Router] ipsec profile profile1
[Router-ipsec-profile-profile1] proposal tran1
[Router-ipsec-profile-profile1] ike-peer spua
```

配置虚拟隧道接口建立GRE over IPSec示例（4）



5. 分别在WAC和Router的接口上应用各自的安全框架。

#在WAC的接口上引用安全框架。

```
[WAC] interface tunnel 0/0/0
[WAC-Tunnel0/0/0] ip address 192.168.1.1 255.255.255.0
[WAC-Tunnel0/0/0] tunnel-protocol ipsec
[WAC-Tunnel0/0/0] source 1.1.1.1
[WAC-Tunnel0/0/0] destination 2.1.1.1
[WAC-Tunnel0/0/0] ipsec profile profile1
```

#在Router的接口上引用安全框架。

```
[Router] interface tunnel 0/0/0
[Router-Tunnel0/0/0] ip address 192.168.1.2 255.255.255.0
[Router-Tunnel0/0/0] tunnel-protocol ipsec
[Router-Tunnel0/0/0] source 2.1.1.1
[Router-Tunnel0/0/0] destination 1.1.1.1
[Router-Tunnel0/0/0] ipsec profile profile1
```

6. 配置Tunnel接口的转发路由，将需要IPSec保护的数据流引到Tunnel接口。

```
[WAC] ip route-static 10.1.2.0 255.255.255.0 tunnel 0/0/0
```

#在Router上配置不再赘述。

配置虚拟隧道接口建立GRE over IPSec示例（5）

- 配置成功后，分别在WAC和Router上执行display ike sa会显示所配置的信息，以WAC为例。

```
[WAC] display ike sa
IKE SA information :
  Conn-ID        Peer            VPN     Flag(s)   Phase     RemoteType        RemoteID
 ------------------------------------------------------------------------------------------------------------
    16           2.1.1.1:500             RD|ST     v1:2      IP                2.1.1.1
    14           2.1.1.1:500             RD|ST     v1:1      IP                2.1.1.1

  Number of IKE SA : 2
 ------------------------------------------------------------------------------------------------------------
 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

思考题

1. Navi AC方案中，Navi AC的功能是什么?
2. Mesh网络的AP角色有哪些?
3. Mesh的组网方式主要有哪几种?

- Navi AC：集中处理无线用户的安全、控制和管理等功能，如身份认证、授权和计费等。
- Mesh网络AP角色定义：
  - MP（Mesh Point）：使用IEEE 802.11MAC和物理层协议进行无线通信，并且支持Mesh功能的节点。该节点支持自动拓扑、自动发现路由、数据报文转发等功能。MP节点可以同时提供Mesh服务和用户接入服务。
  - MPP（Mesh Portal Point）：连接Mesh网络和其他类型网络的MP节点。这个节点具有Portal功能，可以实现Mesh内部节点和外部网络的通信。
  - 邻居MP：与某个Mesh节点处于直接通信范围内的MP或MPP，称为该Mesh节点的邻居MP。
  - 候选MP：MP准备与之建立Mesh链路的邻居MP。
  - 对端MP：已与MP建立起Mesh连接的邻居MP，称为该MP的对端MP。
- 链状组网，星状组网，网状组网。

本章总结

- Navi AC、Leader AP、Mesh、GRE和IPsec VPN是WLAN网络中常见的技术或网络架构。资深WLAN工程师需要清楚掌握这些技术的工作原理和部署方法，才能够应对复杂的网络。

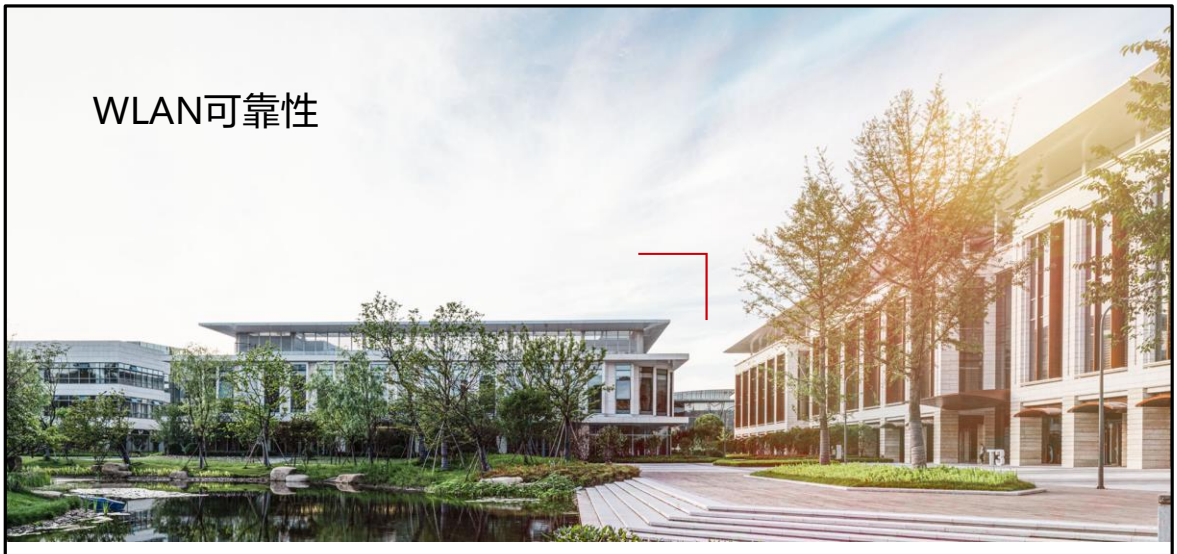
Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN可靠性



HUAWEI

前言

- 随着网络的快速普及和应用的日益深入，各种企业业务实现了数字化。网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为关注的焦点。
- 在实际网络中，难以避免各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。本章将重点介绍华为WLAN可靠性方案，包括双机热备份、双链路冷备份、N+1冷备份以及CAPWAP断链逃生策略。

目标

- 学完本课程后，您将能够：
  - 描述常见WLAN可靠性方案，包括双机热备份、双链路冷备份、N+1冷备份以及CAPWAP断链逃生
  - 实现常见WLAN可靠性方案的基本配置

目录

WLAN可靠性概述

- WLAN可靠性技术的种类繁多，我们根据其解决网络故障的侧重不同，可分为：
  - 故障检测技术：侧重于网络的故障检测和诊断。例如BFD是一种通用的故障检测技术，可用于各层面的故障检测；以太网OAM用于链路层的故障检测。
  - 保护倒换技术：侧重于网络的故障恢复，主要通过对硬件、链路、路由信息和业务信息等进行冗余备份以及故障时的快速切换，从而保证网络业务的连续性。
  - 逃生技术：侧重于网络故障后WLAN业务保障，通过部署逃生策略，可实现故障后原有业务不中断，原有用户不被迫下线。

- 本章将重点介绍保护倒换技术以及逃生技术。

常用保护倒换技术及比较

对比项	VRRP热备份	双链路热备份	双链路冷备份	N+1备份
切换速度	切换速度快，对业务影响小。	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，主备切换过后STA不需要掉线重连。	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，STA需要重新上线，业务会出现短暂中断。	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，AP、STA均需要重新上线，业务会出现短暂中断，中断时间比双链路冷备份中断时间长。
异地部署	不支持	支持	支持	支持
约束条件	主备WAC的型号和软件版本需完全一致。		主备WAC产品形态可以不同，WAC的软件版本必须一致。	
	一台备WAC只支持为一台主WAC提供备份。			一台备WAC支持为多台主WAC提供备份，能降低购买设备的成本。
适用范围	可靠性要求高 无需异地部署主WAC	可靠性要求高 要求异地部署主备WAC	可靠性要求较低	可靠性要求较低 成本控制要求较高

CAPWAP断链逃生概述

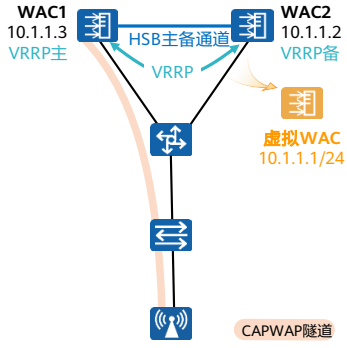
- 在WAC+FIT AP网络架构中，AP和WAC之间通过CAPWAP隧道作为控制报文的转发通道。当CAPWAP链路故障时，AP上原有用户被迫下线，新用户也无法再接入。
- 通过部署CAPWAP断链逃生解决方案，可以保证CAPWAP链路故障后，原有用户不被迫下线，新用户仍可以接入，从而提升企业网络的可靠性。

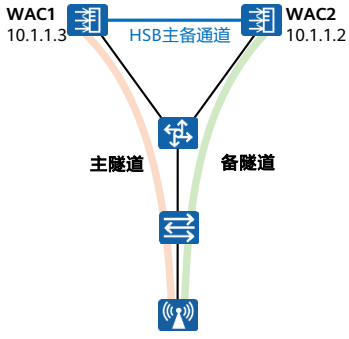
- 特别是在总部分支场景中，分支本地常常不部署WAC，分支的AP设备通过广域网络，连接到企业总部的WAC设备进行统一管理，但是广域网络的质量难以保证，这种情况下，WAC与AP连接中断的风险大大提升，一旦CAPWAP链路中断，将严重影响整体网络质量。

目录

双机热备份简介

- 双机热备是指两台互为备份的WAC，当其中一个WAC设备、AP与WAC间物理链路或WAC上层链路发生故障时，用户不需要重新进行关联认证，其业务被自动切换到另一台WAC上。
- 根据采用的关键基础技术的不同，WAC双机热备可以分为**VRRP双机热备、双链路双机热备**两种。



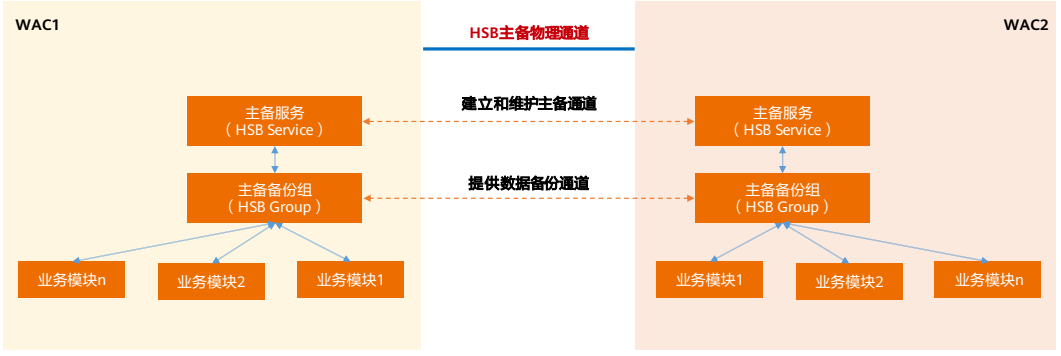


HUAWEI

- 支持双机热备的前提是两台WAC产品形态、组网、以及配置上保证一致（WAC管理口IP等必须不同的配置除外）。
- 说明：
  - 双链路：AP与主备WAC间分别建立CAPWAP链路。
  - VRRP：虚拟路由冗余协议。
- 基于双链路双机热备，AP分别与主备WAC建立CAPWAP链路，通过针对AP或AP组设置主备WAC的优选顺序，实现不同AP支持不同主备WAC场景，达到主备WAC上流量负载分担的目的。
- 基于VRRP双机热备，两台WAC对外呈现为一台虚拟WAC，所以不支持负载分担。另外，基于VRRP双机热备通过VRRP报文协商两台WAC的主备，VRRP报文只能在二层网络中传输，无法跨三层网络传输，所以基于VRRP双机热备不支持WAC间三层组网热备。
- 双机热备份场景，主WAC上的WIDS表项信息不支持备份到备WAC上，主备切换后，WIDS表项信息会丢失。
- 双链路热备份场景下不支持WAC间漫游。
- 双链路热备份场景下不支持备份Portal认证信息。如果配置了Portal认证，主备WAC倒换后，Portal认证的无线用户需要重新输入用户名和密码。

主备公共机制HSB

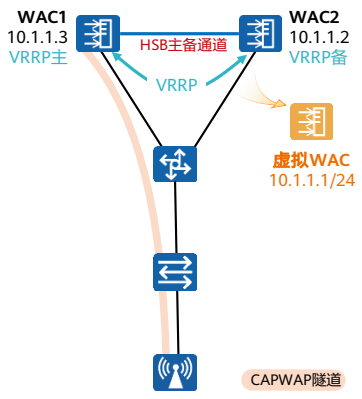
- 主备公共机制HSB（Hot-Standby Backup）提供两种公共服务：
  - 主备服务（HSB service）：建立和维护主备通道，为各个主备业务模块提供通道通断事件和报文发送接收接口。
  - 主备备份组（HSB group）：HSB备份组内部绑定HSB service，为各个主备业务模块提供数据备份通道。



HUAWEI

- 主备服务模块：负责备份通道的建立和维护（Hello处理）、通道connect或者disconnect时通知相关联的业务模块。
- 主备备份组模块：
  - 与一个VRRP实例绑定，借用VRRP机制协商出主备实例。
  - 负责业务的主备协商，批量备份、实时备份、状态信息同步，通知相关业务模块进行业务信息备份。
- 业务模块：响应业务备份组模块的各种主备事件，进行批量备份、实时备份、状态同步处理。
- WAC目前只支持主备服务和主备备份组单实例，即整机只支持配置一个备份服务和一个备份组。
- 由于主备WAC之间需频繁交互HSB心跳报文，且心跳报文作为关键报文直接影响主备WAC之间的工作与协商结果，为保证HSB系统正常运行，也为了防止备份数据丢失，建议为HSB通道规划单独的物理链路。

VRRP双机热备

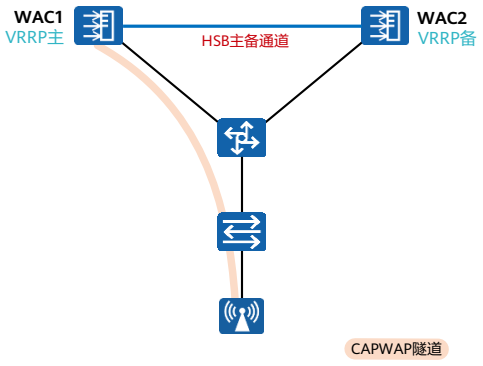


- 两台WAC组成一个VRRP组，主、备WAC对AP始终显示为同一个虚拟IP地址，主WAC通过HSB主备通道同步业务信息到备WAC上。
- 两台WAC通过VRRP协议产生一台虚拟WAC，缺省情况下，主WAC承担虚拟WAC的具体工作，当主WAC故障时，备WAC接替其工作。所有AP与虚拟WAC建立CAPWAP隧道。
- AP只看到一个WAC的存在，WAC间的主备切换由VRRP决定。
- 这种方式一般将主备WAC部署在同一地理位置，和其他备份方式比较，其业务切换速度更快。
- 支持更多保护特性：上行链路监控支持BFD+VRRP。下行链路支持MSTP破解环路。

HUAWEI

- HSB业务实时备份：
  - 用户数据备份。
  - CAPWAP隧道信息备份。
  - AP表项备份。
  - DHCP地址信息备份。
- HSB主备通道，可通过两台WAC之间的直连物理链路承载，也可通过交换机承载，例如复用VRRP报文交互所处的物理通道。

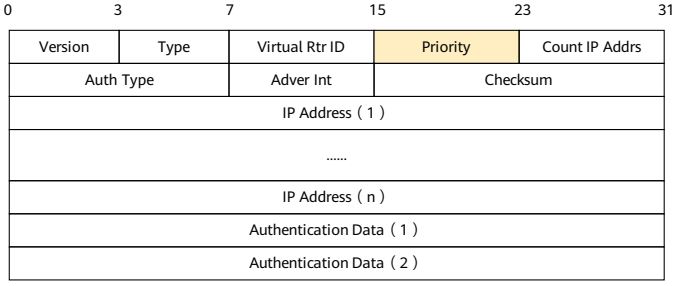
VRRP双机热备工作流程概述



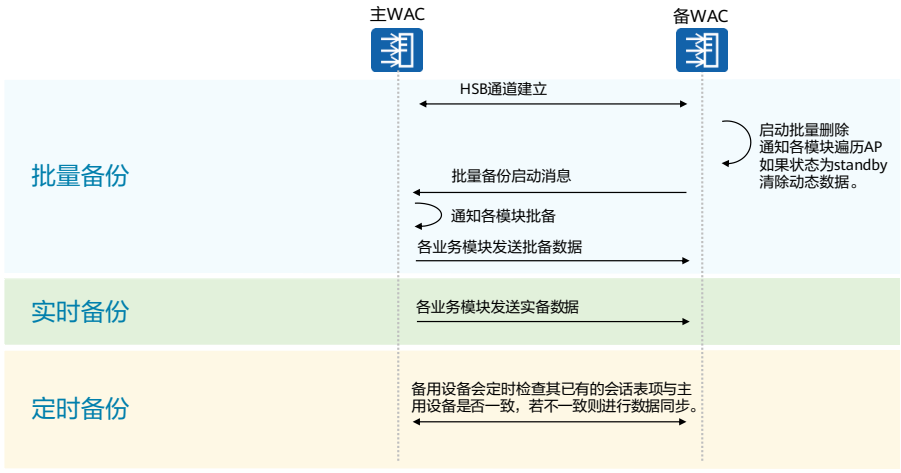
1. 主备协商：两台WAC通过HSB备份服务通道分别发送携带优先级信息VRRP报文（VRRP报文Priority字段），根据VRRP协议报文中优先级协商主备。
2. 数据备份：基于VRRP双机热备备份信息包括用户表项、CAPWAP链路信息以及AP表项等信息， 备份的方式有实时备份，批量备份，定时备份。
3. 主备倒换：当其中一个WAC设备、AP与WAC间物理链路或WAC上层链路发生故障时，将触发主备设备切换角色。
4. 主备回切：发生主备倒换后，当原主WAC恢复链路后，在抢占方式下，会触发主备设备回切。

VRRP主备协商

- 两台WAC通过HSB备份服务通道交换携带优先级信息的VRRP报文，协商主备。
- 主WAC通过免费ARP报文，向其他设备通告虚拟MAC。
- 主WAC周期性的发送VRRP心跳报文，实时报告工作状态。



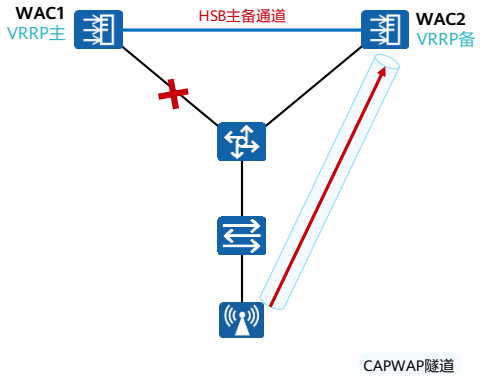
VRRP双机热备数据同步流程



HUAWEI

- 当主用设备出现故障，流量切换到备份设备时，要求主用设备和备份设备的会话表项完全一致，否则有可能导致会话中断，因此，在主备之间需要进行数据同步。
- 基于VRRP双机热备备份信息包括用户表项、CAPWAP链路信息以及AP表项等信息，备份的方式有实时备份，批量备份，定时备份。
  - 批量备份：主用设备会将已有的会话表项一次性同步到新加入的备份设备上，使主备WAC信息对齐，这个过程称为批量备份。批量备份会在WAC主备确立时进行触发。
  - 实时备份：如果在运行过程中产生新的会话表项，业务模块会判断是否存在主备环境，并且当前身份是否为主，如果是，调用HSB主备服务向对端业务模块发送备份信息，这个过程称为实时备份。
  - 定时同步：为了进一步保证主备设备上表项的完全一致，备用设备会每隔30分钟检查其已有的会话表项与主用设备是否一致，若不一致则将主用设备上的会话表项同步到备用设备，这个过程称为定时同步。

VRRP双机热备主备切换 - 下行链路断开切换

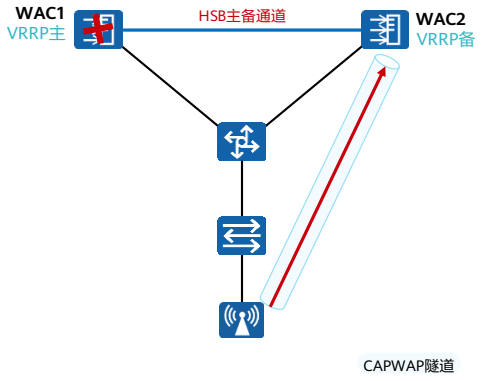


- 当主WAC下行链路断开后，HSB备份组感知到Vlanif接口状态为down，通知HSB通道通知对端HSB备份组进入独立运行状态。
- 备WAC的HSB备份组收到事件后，通知业务模块对AP状态进行变更，AP状态变为”normal”。
- 备WAC的VRRP机制会感知到VRRP心跳超时，状态变更为“master”，同时HSB感知到此变化。VRRP等待Master_Down_Timer超时后，对外发送虚拟WAC IP地址的免费ARP报文，备WAC接管理AP。

HUAWEI

- Master_Down_Timer：备WAC将持续接收来自当前主WAC的VRRP报文，每当报文到达时，备WAC上的Master_Down_Timer会被重置。如果一定时间内没有收到来自主WAC的VRRP报文并导致Master_Down_Timer超时，那么备WAC将认为主WAC已经失效。
- HSB备份组的状态：
  - Active：激活状态。
  - Inactive：未激活状态。
  - Independent：独立运行状态。
  - Switching：主备切换状态。
- VRRP协议中定义了三种状态机：初始状态（Initialize）、活动状态（Master）、备份状态（Backup）。其中，只有处于Master状态的设备才可以转发那些发送到虚拟IP地址的报文。

VRRP双机热备主备切换 - 主WAC故障切换

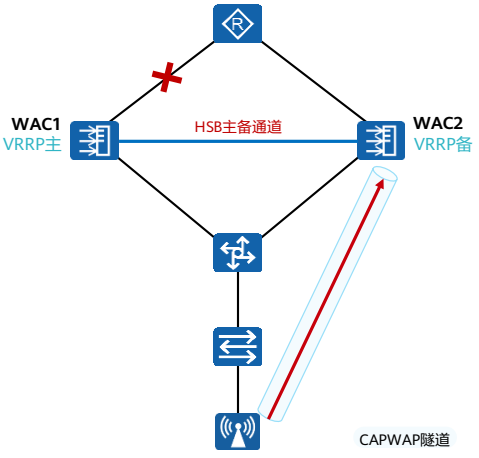


- 主WAC故障，HSB通道中断，HSB模块并不能通知主WAC发生异常，需等待备HSB进入独立运行状态，并感知到VRRP状态异常后，通知AP进行状态切换，完成主备切换。

HUAWEI

- 如果HSB默认的心跳报文发送间隔为3秒，重传次数为5次，主备切换只能等待备WAC VRRP超时（默认配置时间 3 秒），备WAC的VRRP状态发生改变，HSB查询到VRRP状态改变，会判断自身的HSB备份组状态，因为HSB通道心跳是15秒，没有超时，HSB备份组查询自己的状态为 backup，并不会去通知业务模块更改AP状态，只有在HSB通道心跳超时后，HSB备份组状态变为独立运行，这时才会通知业务模块更改AP状态为normal，完成主备切换。
- 如果配置HSB默认的心跳报文发送间隔为2秒，重传次数为1次， VRRP 的心跳报文发送间隔为3秒，重传次数为1次，在整机断电重启的情况下，HSB备份组状态变化能够先于VRRP的状态发生变化，这样在VRRP超时后，HSB备份组能够及时通知业务模块更改AP状态切换，完成主备切换。

VRRP双机热备主备切换 - 上行链路断开切换

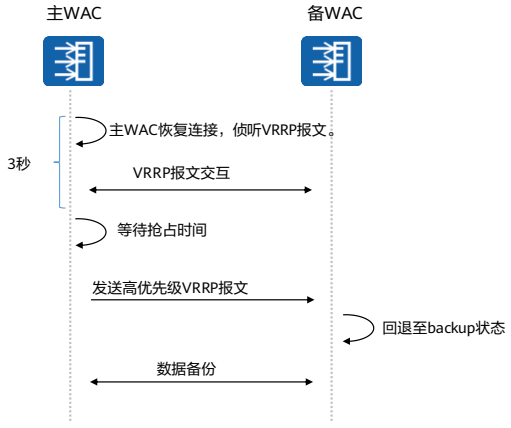


- 通过配置VRRP联动功能实现对上行链路或接口监视，当主WAC上行链路断开后，VRRP备份组会降低主WAC优先级，触发VRRP主备切换。
- 备份组中Master和Backup设备必须都工作在抢占方式下。

HUAWEI

- 当Master设备上行接口故障时，由于VRRP无法感知非备份组内接口的状态变化，可能会导致业务中断。通过联动接口状态，配置VRRP监视上行接口，当被监视的接口故障时，降低Master设备优先级，触发VRRP主备切换，以实现链路切换，减小接口故障对业务转发的影响。
- 被监视的接口故障恢复时，原Master设备在备份组中的优先级将恢复原来的值，重新抢占成为Master，继续承担流量转发的业务。
- 配置VRRP与接口状态联动时，备份组中Master和Backup设备必须都工作在抢占方式下。建议Backup设备配置为立即抢占，Master设备配置为延时抢占。

VRRP双机热备主备回切

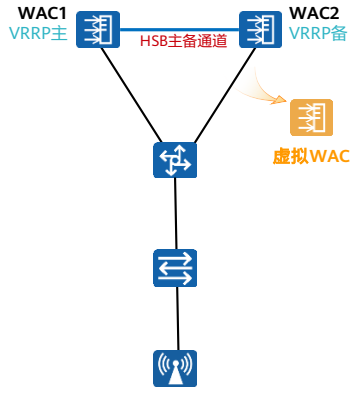


- VRRP双机热备场景下，发生主备倒换后，当原主WAC恢复链路后，在抢占方式下，主备WAC等待回切延时后，会触发主备回切。

HUAWEI

- 原主WAC恢复连接后，VRRP的状态由“Initialize”变成“backup”，开始监听VRRP报文。
- 监听3秒，确认备WAC收到VRRP报文后，开始回切延时计时。
- 计时结束，原主WAC重新开始发送高优先级的VRRP报文，通知原备WAC回切倒换。
- 原备WAC收到优先级更高的VRRP报文，退回到“backup”状态。
- 主WAC故障恢复后，在抢占方式下，将重新选举成为Master；在非抢占方式下，将保持在Backup状态。

配置基于VRRP的双机热备份 - 配置思路



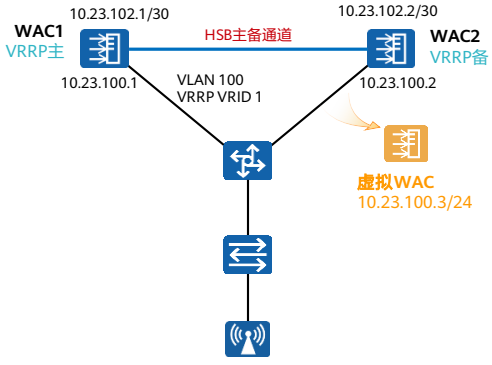
配置思路

- 配置VRRP备份组
- 配置HSB主备服务
- 配置HSB备份组
- 配置业务功能绑定
- 使能HSB备份组
- 检查配置结果

HUAWEI

- 在配置VRRP热备份功能之前，需完成任务：配置接口的网络层属性，使网络层路由可达。
- 配置VRRP热备份功能时，两台WAC组成一个虚拟WAC，WAC下挂接的所有AP与虚拟WAC进行通信，因此通过命令capwap source配置WAC的源IP地址时，应该配置为HSB备份组绑定的VRRP备份组的虚拟IP地址。

配置基于VRRP的双机热备份 - 配置VRRP备份组



在WAC1上创建管理VRRP备份组，配置AC1在该备份组中的优先级为120，并配置抢占时间为1800秒。

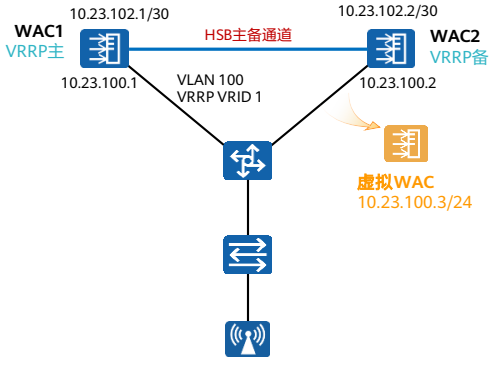
```
[WAC1] interface vlanif 100
[WAC1-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.3
[WAC1-Vlanif100] vrrp vrid 1 priority 120
[WAC1-Vlanif100] vrrp vrid 1 preempt-mode timer delay 1800
[WAC1-Vlanif100] admin-vrrp vrid 1
[WAC1-Vlanif100] quit
```

在WAC2上创建管理VRRP备份组， 优先级以及抢占保持默认配置。

```
[WAC2] interface vlanif 100
[WAC2-Vlanif100] vrrp vrid 1 virtual-ip 10.23.100.3
[WAC2-Vlanif100] admin-vrrp vrid 1
[WAC2-Vlanif100] quit
```


- 本例只进行管理VRRP的配置举例。

配置基于VRRP的双机热备份 - 配置HSB主备服务



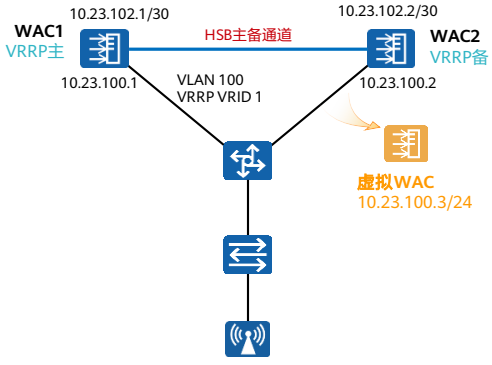
在WAC1上创建HSB主备服务0，并配置其主备通道IP地址和端口号，配置HSB主备服务报文的重传次数和发送间隔。

```
[WAC1] hsb-service 0
[WAC1-hsb-service-0] service-ip-port local-ip 10.23.102.1 peer-ip
10.23.102.2 local-data-port 10241 peer-data-port 10241
[WAC1-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
```

在WAC2上创建HSB主备服务0，并配置其主备通道IP地址和端口号，配置HSB主备服务报文的重传次数和发送间隔。

```
[WAC2] hsb-service 0
[WAC2-hsb-service-0] service-ip-port local-ip 10.23.102.2 peer-ip
10.23.102.1 local-data-port 10241 peer-data-port 10241
[WAC2-hsb-service-0] service-keep-alive detect retransmit 3 interval 6
```

配置基于VRRP的双机热备份 - 配置HSB备份组



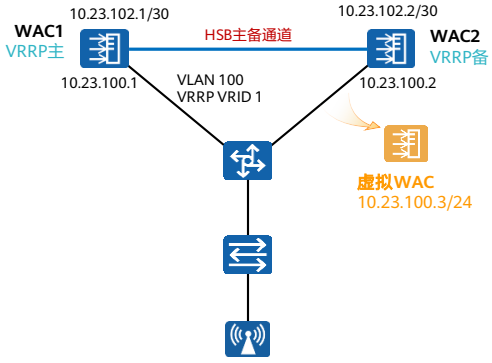
在WAC1上创建HSB备份组0，并配置其绑定HSB主备服务0和管理VRRP备份组。

```
[WAC1] hsb-group 0
[WAC1-hsb-group-0] bind-service 0
[WAC1-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[WAC1-hsb-group-0] quit
```

在WAC2上创建HSB备份组0，并配置其绑定HSB主备服务0和管理VRRP备份组。

```
[WAC2] hsb-group 0
[WAC2-hsb-group-0] bind-service 0
[WAC2-hsb-group-0] track vrrp vrid 1 interface vlanif 100
[WAC2-hsb-group-0] quit
```

配置基于VRRP的双机热备份 - 绑定业务使能备份组



在WAC1上绑定NAC业务、WLAN业务以及DHCP业务，使能HSB。

```
[WAC1] hsb-service-type access-user hsb-group 0
[WAC1] hsb-service-type ap hsb-group 0
[WAC1] hsb-service-type dhcp hsb-group 0
[WAC1] hsb-group 0
[WAC1-hsb-group-0] hsb enable
```

在WAC1上绑定NAC业务、WLAN业务以及DHCP业务，使能HSB。

```
[WAC2] hsb-service-type access-user hsb-group 0
[WAC2] hsb-service-type ap hsb-group 0
[WAC2] hsb-service-type dhcp hsb-group 0
[WAC2] hsb-group 0
[WAC2-hsb-group-0] hsb enable
```

配置基于VRRP的双机热备份 - 检查配置结果

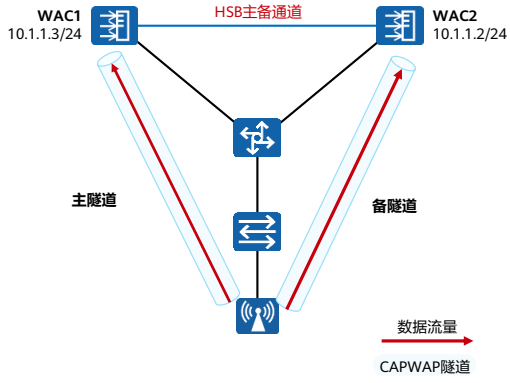
执行命令**display hsb-group** *group-index*，查看HSB备份组的信息。

```
[WAC1]display hsb-group 0
Hot Standby Group Information:
-------------------------------------------------------------
  HSB-group ID                  : 0
  Vrrp Group ID                 : 1
  Vrrp Interface                : Vlanif100
  Service Index                 : 0
  Group Vrrp Status             : Master
  Group Status                  : Active
  Group Backup Process          : Realtime
  Peer Group Device Name        : AC6005
  Peer Group Software Version   : V200R007C10SPC300B220
  Group Backup Modules          : -
-------------------------------------------------------------
```

执行命令**display hsb-service** *service-index*，命令查看HSB主备服务的信息。

```
[WAC1]display hsb-service 0
Hot Standby Service Information:
-------------------------------------------------------------
  Local IP Address              : 10.23.102.1
  Peer IP Address               : 10.23.102.2
  Source Port                   : 10241
  Destination Port              : 10241
  Keep Alive Times              : 3
  Keep Alive Interval           : 6
  Service State                 : Connected
  Service Batch Modules         :
-------------------------------------------------------------
```

双链路双机热备简介

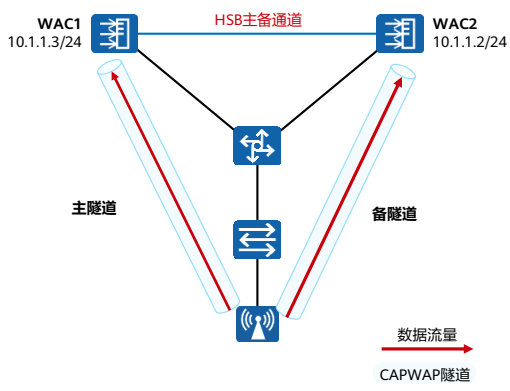


- AP同时与主备WAC之间分别建立CAPWAP隧道，WAC间的业务信息通过HSB主备通道同步。
- 当AP和主WAC间链路断开，AP会通知备WAC切换成主WAC。
- 通过WAC优先级确立主备WAC。WAC优先级相同的情况下，根据WAC负载（AP和STA个数）确立主备WAC。

HUAWEI

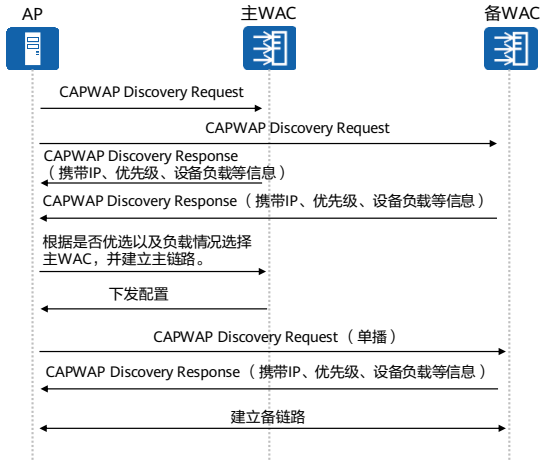
- 该方案除了支持主备备份之外，还支持负载分担模式。负载分担模式下可以指定一部分AP的主WAC为WAC1，与其建立CAPWAP主链路，一部分AP的主WAC为WAC2，与其建立CAPWAP主链路。
- 双链路双机热备的主备WAC不受地理位置限制，部署灵活，可进行负载分担，有效利用资源，但业务切换速度较慢。

双链路双机热备工作流程概述



1. 建立主备链路：优选出主WAC并建立主链路，主WAC下发配置完成后，建立备链路。
2. 数据备份：主备WAC通过HSB通道备份用户的接入认证信息，从而支持更多的STA加密认证方式在主备切换或者回切时业务不中断。
3. 主备倒换：当主WAC故障或者下行链路断开时，将触发主备设备切换角色，激活备链路，原有用户流量直接切换至新的主WAC。
4. 主备回切：使能全局回切开关，发生主备倒换后，当原主WAC 恢复链路后，会触发主备设备回切。

双链路双机热备主备协商



- 建立主链路：
  - 在Discovery阶段优选出主WAC。
  - 其他过程跟正常情况下的CAPWAP隧道建立过程一致。
- 建立备链路：
  - 为了避免业务配置重复下发导致错误，在AP和主WAC建立主隧道并且配置下发完成后，才开始启动备CAPWAP链路的建立。

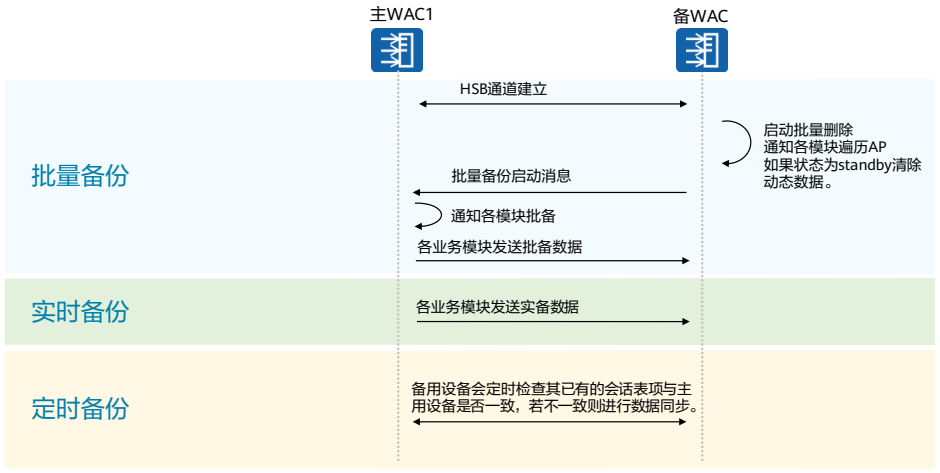
HUAWEI

- AP定期向主备WAC发送CAPWAP Discovery Request 报文，如果主备WAC都正常，都会回应CAPWAP Discovery Response 报文，并在该报文中携带优选WAC的IP地址、备选WAC的IP地址、双链路特性开关、各自的优先级、各自的负载情况以及各自的IP地址。
- AP收集到主备WAC回应的 CAPWAP Discovery Response 报文后，根据优选WAC的IP地址、备选WAC的IP地址、WAC的优先级、设备的负载情况以及WAC IP 地址来选择主WAC并开始与其建立 CAPWAP 主链路。优选顺序如下：
  - AP查看优选WAC，如果只有一个优选WAC，则此WAC作为主WAC。如果存在多个优选WAC，则选择负载最轻的WAC作为主WAC，如果负载相同选择IP地址最小的作为主WAC。
  - 负载的比较方式：比较WAC设备的负载情况，即AP个数和STA个数，负载轻的为主WAC。优先选择当前可接入AP数大的WAC为主WAC，如果当前可接入AP数相同，则选择当前可接入STA数大的WAC为主WAC。
    - 当前可接入AP数=可接入的最大AP数-当前已接入的AP数。
    - 当前可接入STA数=可接入的最大STA数-当前已接入的STA数。

- 如果没有优选WAC，查看备选WAC，如果只有一个备选WAC，则此WAC作为主WAC，如果存在多个备选WAC，则选择负载最轻的WAC作为主WAC，如果负载相同选择IP地址最小的作为主WAC；
- 如果备选WAC不存在，比较WAC的优先级，优先级值小的为主WAC；优先级相同情况下，则选择负载最轻的WAC作为主WAC；负载相同情况下，比较IP地址，IP地址小的为主WAC。

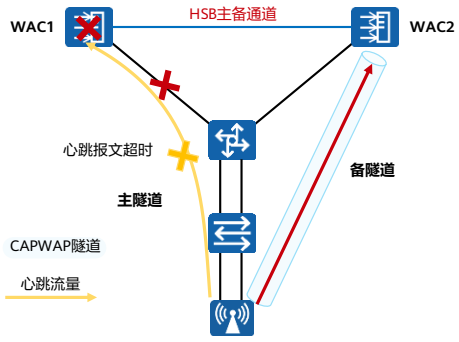
- 备链路建立：
  - AP向备WAC发送单播CAPWAP Discovery Request报文。备WAC接收到CAPWAP Discovery Request 报文后，回应CAPWAP Discovery Response报文，在该报文中携带优选WAC的IP地址、备选WAC的IP地址、双链路特性开关、负载情况及其优先级。AP收到备WAC回应的CAPWAP Discovery Response报文后，获取到双链路特性开关为打开，并保存其优先级。
  - AP发送的Join Request中，会携带一个自定义消息类型，告诉备WAC配置已经下发过了，不需要再下发。WAC收到Join Request，获取到该自定义消息时，在配置下发阶段，会跳过配置下发流程，避免对AP重复下发配置。
  - 备链路建立完成后，AP重新根据两个链路的优先级决策出主备WAC。

双链路双机主备数据同步



- 双链路双机热备场景下，业务直接绑定HSB备份服务，这样HSB对业务仅提供备份数据收发的功能，用户的主备状态由双链路机制进行维护。
- 双链路双机热备通过HSB通道备份用户的接入认证信息，从而支持更多的STA加密认证方式在主备切换或者回切时业务不中断。HSB备份也分为实时备份，批量备份，定时备份。

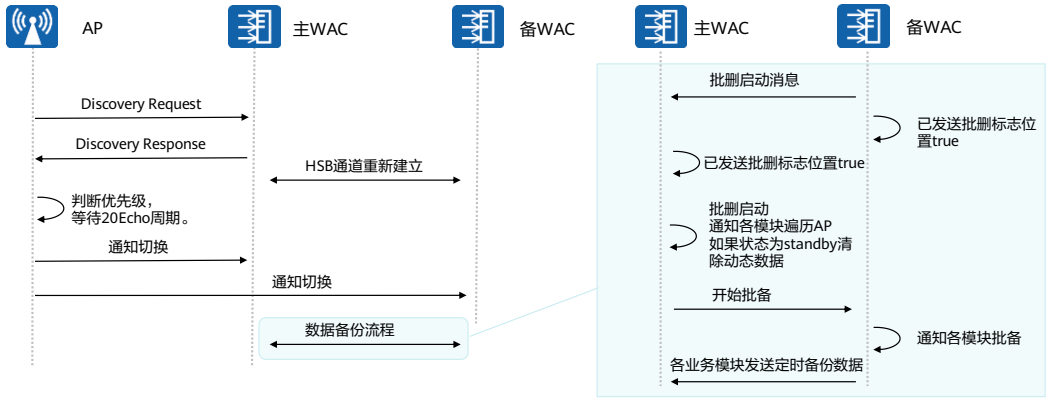
双链路双机热备主备倒换



- 双链路热备主备切换由AP进行判断操作，当主WAC故障或者下行链路断开，主备WAC会进行主备切换。
- 建立双链路后，AP会定期向主备WAC发送Echo报文进行CAPWAP心跳检测，检查CAPWAP链路状态。
- WAC1和交换机的链路中断或者WAC1故障，AP等待和WAC1的一定次数的心跳报文超时，判断CAPWAP主链路故障，
- AP在发送给WAC2的Echo Request报文中携带主信息，WAC2从备份状态切换为工作状态，激活备链路，接管AP，使业务不中断。

双链路双机热备主备回切

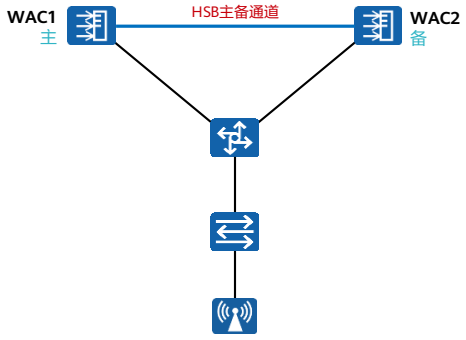
- 优先级回切模式下，AP会定期发送Discovery Request报文检测原来的主链路的状态，当链路恢复后，AP检测到该链路的优先级比当前使用的主链路的优先级更高，触发回切。



HUAWEI

- 为避免网络震荡导致频繁倒换，缺省情况下等待20个Echo周期时间后，通知WAC进行主备回切，同时AP把STA的数据业务向新升级为主的WAC上发送。
- 对于双链路备份链路切换有两种模式：
  - 优先级切换：AP根据优先级优先切换到主链路。
  - 网络稳定性模式：在满足主备链路切换的条件下，AP优先切换到网络稳定性更高的链路，此时决定切换的因素与主备链路角色无关，只与链路的网络稳定性相关。
- 优先级切换为缺省以及常用切换模式，本章中重点介绍优先级切换模式。
- 对于网络稳定性模式，主备链路网络稳定性由Echo报文丢包率衡量，如果符合以下所有条件，表示满足主备链路切换的条件，否则不满足：
  - AP每周期统计当前使用链路指定次数的Echo报文，计算其丢包率大于丢包率起始门限。
  - 当前使用链路丢包率高于另一条链路丢包率，且差值大于丢包率差值门限。

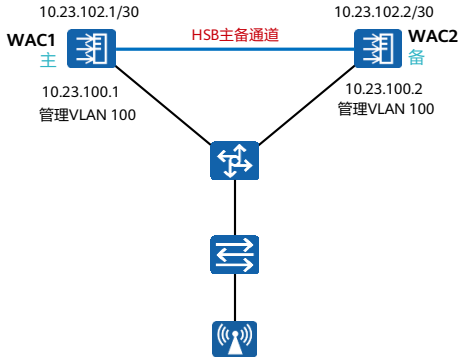
配置基于双链路的双机热备份



配置思路

- 配置双链路备份功能
- 配置主备链路切换模式（可选）
- 配置双机热备功能
- 检查配置

配置基于双链路的双机热备份 - 配置双链路备份功能



在WAC1上，配置优选WAC的IP地址为WAC1的源地址，备选WAC的IP地址为WAC2的源地址。（主备设备配置相似，仅展示WAC1的配置）

```
[WAC1-wlan-view] ap-system-profile name wlan-net
[WAC1-wlan-ap-system-prof-wlan-net] primary-access ip-address 10.23.100.1
[WAC1-wlan-ap-system-prof-wlan-net] backup-access ip-address 10.23.100.2
[WAC1-wlan-view] ap-group name ap-group1
[WAC1-wlan-ap-group-ap-group1] ap-system-profile wlan-net
[WAC1-wlan-ap-group-ap-group1] quit
[WAC1-wlan-view] undo ac protect restore disable
[WAC1-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]: y
```

在主用WAC1上重启AP，下发双链路备份配置信息至AP。

```
[WAC1-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]:y
[WAC1-wlan-view] quit
```


HUAWEI

- 缺省情况下，双链路备份功能未开启，执行命令ac protect enable会提示重启所有AP。AP重启后，双链路备份功能开始生效。
- 若双链路备份功能已开启，此处再执行命令ac protect enable不会重启AP，需要在主WAC上继续执行命令ap-reset重启AP，AP重启后，双链路备份功能开始生效。
- 如果在配置双链路备份时需要使用WDS或Mesh，建议配置CAPWAP心跳检测的间隔时间为25秒，心跳检测报文次数至少为6次。否则由于双链路备份时缺省的心跳报文间隔时间为25秒，心跳检测报文次数为3次，会导致WDS或Mesh链路不稳定，无法保证用户正常接入。
- 配置CAPWAP心跳检测间隔时间和次数低于默认值会影响CAPWAP链路可靠性，请谨慎修改，建议使用默认值。

配置基于双链路的双机热备份 - 配置链路切换模式（可选）

- 链路切换模式分两种：
  - 优先级模式（缺省）：AP优先切换到主链路。
  - 网络稳定性模式：AP优先使用高稳定性网络的链路。此处网络稳定性由Echo报文丢包率衡量。

如需将优先级模式修改为网络稳定性模式，可执行以下命令：

```
[WAC1-wlan-view] ap-system-profile name wlan-net
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch mode network-stabilization
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch packet-loss echo-probe-time 30
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch packet-loss start-threshold 30
```

配置一个统计周期内探测Echo报文的次数。

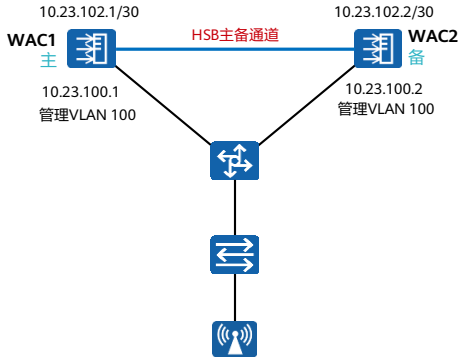
```
[WAC1-wlan-view] ac protect link-switch packet-loss echo-probe-time 20
```

配置主备链路切换的丢包率起始门限和丢包率差值门限。

```
[WAC1-wlan-view] ac protect link-switch packet-loss gap-threshold 15
[WAC1-wlan-view] ac protect link-switch packet-loss start-threshold 20
```


- 执行命令ac protect link-switch packet-loss echo-probe-time echo-probe-time，配置一个统计周期内探测Echo报文的次数。
  - 缺省情况下，一个统计周期内探测Echo报文的次数为20次。
- 执行命令ac protect link-switch packet-loss { gap-threshold gap-threshold | start-threshold start-threshold }，配置主备链路切换的丢包率起始门限和丢包率差值门限。
  - 缺省情况下，主备链路切换的丢包率起始门限为20%，丢包率差值门限为15%。

配置基于双链路的双机热备份 - 配置双机热备份功能



在WAC1上创建HSB主备服务0，并配置其主备通道IP地址和端口号。

```
[WAC1] hsb-service 0
[WAC1-hsb-service-0] service-ip-port local-ip 10.23.102.1 peer-ip
10.23.102.2local-data-port 10241 peer-data-port 10241
[WAC1-hsb-service-0] quit
```

配置将WLAN业务与NAC业务绑定WAC1的HSB主备服务。

```
[WAC1] hsb-service-type ap hsb-service 0
[WAC1] hsb-service-type access-user hsb-service 0
```

在WAC2上完成同样操作。

```
[WAC2] hsb-service 0
[WAC2-hsb-service-0] service-ip-port local-ip 10.23.102.1 peer-ip
10.23.102.2local-data-port 10241 peer-data-port 10241
[WAC2-hsb-service-0] quit
[WAC2] hsb-service-type ap hsb-service 0
[WAC2] hsb-service-type access-user hsb-service 0
```

配置基于双链路的双机热备份 - 检查配置结果

在WAC1和WAC2上执行命令**display ac protect**，可以查看到双链路备份的配置信息。

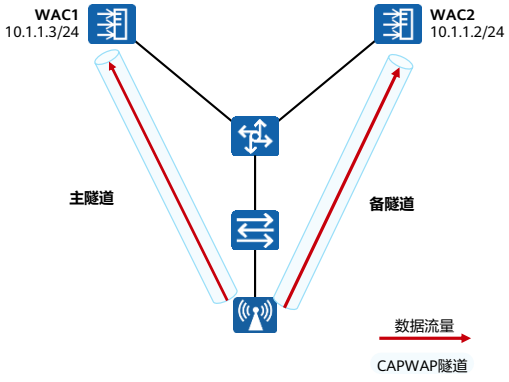
```
[WAC1] display ac protect
------------------------------------------------------------------
Protect state          : enable
Protect AC IPv4        : 10.23.100.3
Protect AC IPv6        : -
Priority               : 0
Protect restore        : enable
...
------------------------------------------------------------------
[WAC2] display ac protect
------------------------------------------------------------------
Protect state          : enable
Protect AC IPv4        : 10.23.100.2
Protect AC IPv6        : -
Priority               : 1
Protect restore        : enable
...
------------------------------------------------------------------
```

在WAC1和WAC2上执行display hsb-service 0命令，查看主备服务的建立情况，可以看到Service State字段的显示为Connected，说明主备服务通道已经成功建立。

```
[WAC1] display hsb-service 0
Hot Standby Service Information:
------------------------------------------------------------------
  Local IP Address          : 10.23.102.1
  Peer IP Address           : 10.23.102.2
  Source Port               : 10241
  Destination Port          : 10241
  Keep Alive Times          : 5
  Keep Alive Interval       : 3
  Service State             : Connected
  Service Batch Modules     : AP
  Shared-key                : -
------------------------------------------------------------------
```

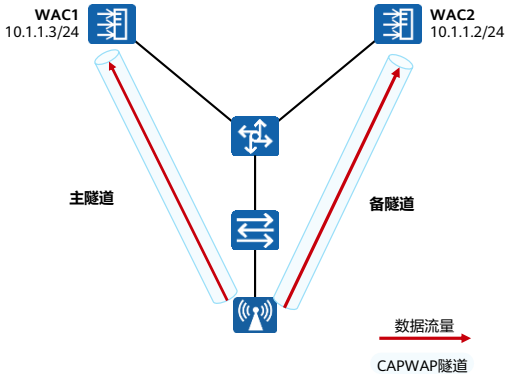
目录

双链路冷备份简介



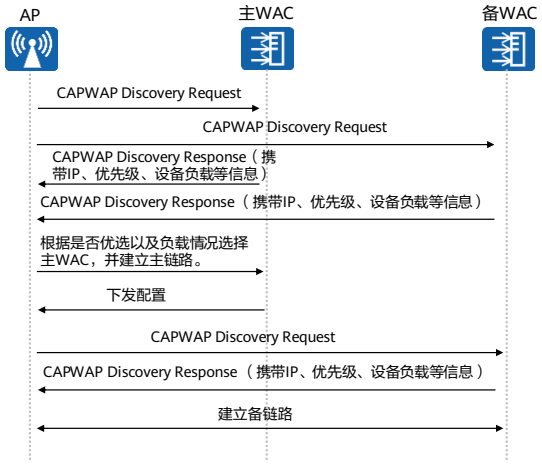
- 双链路冷备份是指在WAC+FIT AP的网络架构中，使用两台WAC来管理相同AP，AP同时和两台WAC建立CAPWAP链路，其中一台WAC作为主WAC，为AP提供业务服务，另一台WAC作为备WAC，不提供业务服务。
- 为保证主备WAC能够提供相同的业务服务，需要在主备WAC上配置相同的业务。

双链路冷备份工作流程概述



1. 建立主备链路：优选出主WAC并建立主链路，主WAC下发配置完成后，建立备链路。
2. 主备倒换：当主WAC故障或者下行链路断开时，将触发主备设备切换角色，激活备链路，AP上原有用户下线并重新上线。
3. 主备回切：使能全局回切开关，发生主备倒换后，当原主WAC 恢复链路后，触发主备设备回切。

双链路冷备份主备CAPWAP链接建立过程

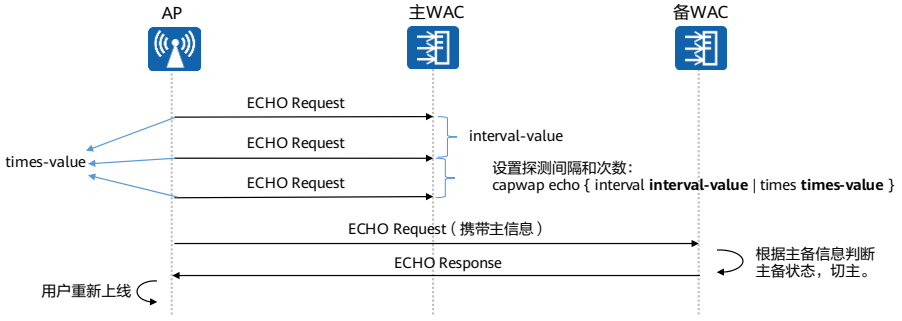


- 建立主链路
  - 在Discovery阶段要优选出主WAC。
  - 其他过程跟正常情况下的CAPWAP隧道建立过程一致。
- 建立备链路
  - 为了避免业务配置重复下发导致错误，在AP和WAC建立主隧道并且配置下发完成后，才开始启动备CAPWAP链路的建立。

- 主备链路建立过程与双链路双机热备一致。

双链路冷备份主备倒换

- AP建立双链路后，会定期向主备WAC进行ECHO探测，并在ECHO报文中携带链路的主备信息。
- 当AP检测到主链路中断后，则AP在发送给备WAC的Echo Request报文中携带主信息，备WAC收到Echo Request报文后判断该链路已经变为主状态，将自己从备WAC切换为主WAC，AP上原有用户下线并重新上线。

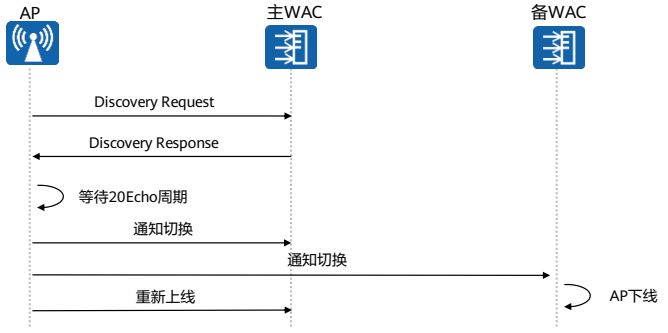


HUAWEI

- 主备倒换由AP进行判断操作。当主WAC故障或者下行链路断开时，主备WAC会进行主备倒换，主WAC由工作状态倒换为备份状态，备WAC由备份状态倒换为工作状态。流程如下：
  - AP和主备WAC建立双链路后，会定期向主备WAC发送Echo报文进行CAPWAP心跳检测，检查CAPWAP链路状态。
  - 当链路故障时，WAC无法回应AP的Echo报文。在连续经过一定次数的CAPWAP心跳检测间隔时间内，主WAC没有回应AP，AP判断CAPWAP主链路故障。
  - AP在发送给备WAC的Echo Request报文中携带主信息，备WAC收到Echo Request报文中的主信息后，将自己切换为工作状态，CAPWAP备链路也切换为工作状态，同时AP把STA的数据业务向新的主WAC上发送。
- 如果在配置双链路备份时需要使用WDS或Mesh，建议配置CAPWAP心跳检测的间隔时间为25秒，心跳检测报文次数至少为6次。否则由于双链路备份时缺省的心跳报文间隔时间为25秒，心跳检测报文次数为3次，会导致WDS或Mesh链路不稳定，无法保证用户正常接入。

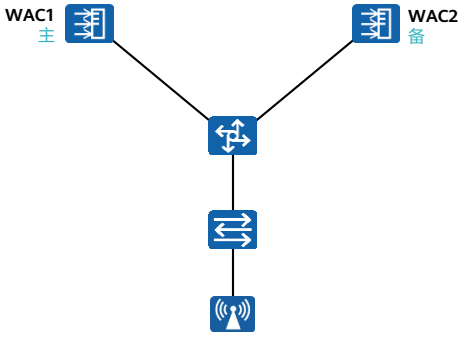
双链路冷备份主备回切

- AP会定期发送Discovery Request报文检测原来的主链路的状态，当链路恢复后，AP检测到该链路的优先级比当前使用的主链路的优先级更高，触发回切。
- 为避免网络震荡导致频繁倒换，缺省情况下等待20个Echo周期时间后，通知WAC进行主备回切，同时AP把STA的数据业务向新升级为主的WAC上发送。



- 双链路冷备份链路切换同样支持网络稳定模式，切换方式与双链路热备份中描述一致。

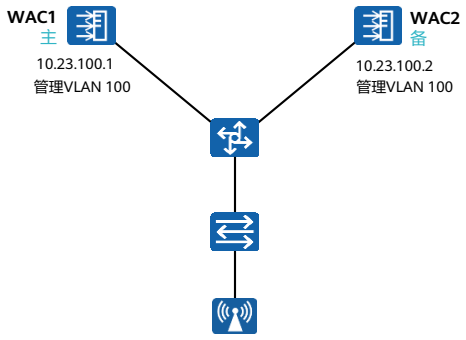
配置基于双链路的冷备



配置思路

- 配置双链路备份组
- 配置链路切换模式（可选）
- 检查配置

配置基于双链路的冷备 - 配置双链路备份功能



在WAC1上，配置备份WAC2的IP地址，WAC1的优先级，用于双链路备份。全局使能双链路备份和回切功能，重启所有AP使双链路备份功能生效。

```
[WAC1-wlan-view] ac protect protect-ac ip-address 10.23.100.3
[WAC1-wlan-view] ac protect priority 0
[WAC1-wlan-view] undo ac protect restore disable
[WAC1-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]: y
```

在WAC2上，配置主用WAC1的IP地址，WAC2的优先级，用于双链路备份。

```
[WAC2-wlan-view] ac protect protect-ac ip-address 10.23.100.2
[WAC2-wlan-view] ac protect priority 1
[WAC2-wlan-view] undo ac protect restore disable
[WAC2-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]: y
```


HUAWEI

- 如果在配置双链路备份时需要使用WDS或Mesh，建议配置CAPWAP心跳检测的间隔时间为25秒，心跳检测报文次数至少为6次。否则由于双链路备份时缺省的心跳报文间隔时间为25秒，心跳检测报文次数为3次，会导致WDS或Mesh链路不稳定，无法保证用户正常接入。
- 配置CAPWAP心跳检测间隔时间和次数低于默认值会影响CAPWAP链路可靠性，请谨慎修改，建议使用默认值。
- 缺省情况下，双链路备份功能未使能，执行命令ac protect enable会提示重启所有AP。AP重启后，双链路备份功能开始生效。
- 若双链路备份功能已使能，此处再执行命令ac protect enable不会重启AP，需要在主WAC上继续执行命令ap-reset重启AP，AP重启后，双链路备份功能开始生效。

配置基于双链路的冷备 - 配置链路切换模式（可选）

- 链路切换模式分两种：
  - 优先级模式（缺省）：AP优先切换到主链路。
  - 网络稳定性模式：AP优先使用高稳定性网络的链路。此处网络稳定性由Echo报文丢包率衡量。

如需将优先级模式修改为网络稳定性模式，可执行以下命令：

```
[WAC1-wlan-view] ap-system-profile name wlan-net
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch mode network-stabilization
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch packet-loss echo-probe-time 30
[WAC1-wlan-ap-system-prof-wlan-net] ac protect link-switch packet-loss start-threshold 30
```

配置一个统计周期内探测Echo报文的次数。

```
[WAC1-wlan-view] ac protect link-switch packet-loss echo-probe-time 20
```

配置主备链路切换的丢包率起始门限和丢包率差值门限。

```
[WAC1-wlan-view] ac protect link-switch packet-loss gap-threshold 15
[WAC1-wlan-view] ac protect link-switch packet-loss start-threshold 20
```


- 执行命令ac protect link-switch packet-loss echo-probe-time echo-probe-time，配置一个统计周期内探测Echo报文的次数。
  - 缺省情况下，一个统计周期内探测Echo报文的次数为20次。
- 执行命令ac protect link-switch packet-loss { gap-threshold gap-threshold | start-threshold start-threshold }，配置主备链路切换的丢包率起始门限和丢包率差值门限。
  - 缺省情况下，主备链路切换的丢包率起始门限为20%，丢包率差值门限为15%。

配置基于双链路的冷备 - 检查配置结果

执行命令display ac protect，查看双链路备份开关状态、WAC的回切功能开关状态、WLAN视图下WAC的优先级和备WAC的IP地址。

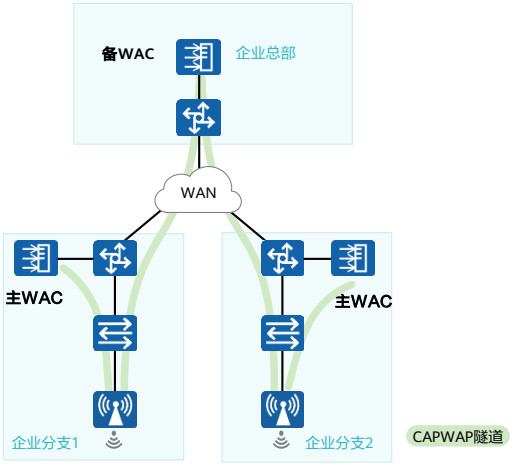
```
[WAC1]display ac protect
------------------------------------------------------------------
Protect state             : enable
Protect AC                : 10.23.100.2
Priority                            : 0
Protect restore           : enable
Coldbackup kickoff station          : disable
------------------------------------------------------------------
[WAC2]display ac protect
------------------------------------------------------------------
Protect state             : enable
Protect AC                : 10.23.100.1
Priority                            : 1
Protect restore           : enable
Coldbackup kickoff station          : disable
------------------------------------------------------------------
```

在WAC1和WAC2上执行display ap-system-profile命令，查看两台WAC上双链路信息。

```
[WAC1] display ap-system-profile name ap-system1
------------------------------------------------------------------
AC priority                         : 0
Protect AC IP address               : 10.23.100.2
Primary AC                          :
Backup AC                           :
...
------------------------------------------------------------------
[WAC2] display ap-system-profile name ap-system1
------------------------------------------------------------------
AC priority                         : 1
Protect AC IP address               : 10.23.100.1
Primary AC                          :
Backup AC                           :
...
------------------------------------------------------------------
```

目录

N+1冷备份简介

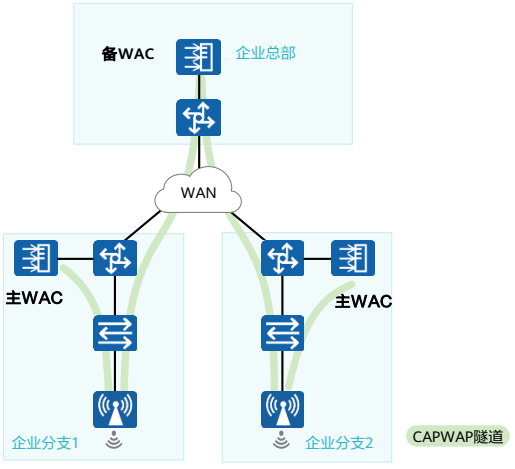


- 使用一台WAC作为备WAC，为多台主WAC提供备份服务。
- 本例中，企业总部的WAC可作为分支1与分支2的本地WAC的备份WAC。
- 网络正常情况下，AP只与各自所属的主WAC建立CAPWAP隧道。
- 当主WAC故障或主WAC与AP间CAPWAP链路故障时，备WAC替代主WAC来管理AP，备WAC与AP间建立CAPWAP链路，为AP提供业务服务。
- 支持主备倒换，支持主备回切。

HUAWEI

- 当AP与主用WAC之间的CAPWAP隧道中断时，将触发AP与备用WAC建立CAPWAP隧道，此时AP会重新与该WAC建链、重启并获取配置，在该过程中，业务将会受影响。

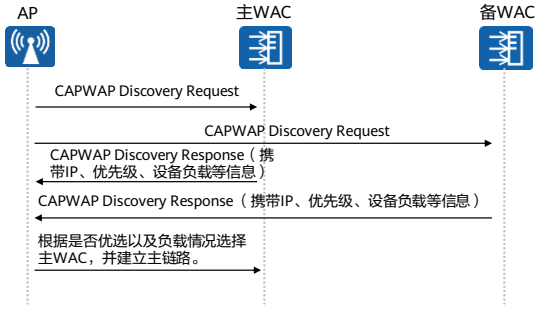
N+1冷备份工作流程概述



1. 建立主链路：优选出主WAC，AP与所属主WAC建立CAPWAP隧道。
2. 主备倒换：当主WAC故障或主WAC与AP间CAPWAP链路故障时，备WAC与AP间建立CAPWAP链路，AP原有用户重新上线。
3. 主备回切：使能全局回切开关，发生主备倒换后，当原主WAC 恢复链路后，会触发主备设备回切。

N+1冷备份主备选择

- 建立主链路
  - 在Discovery阶段要优选出主WAC。
  - 其他过程跟正常情况下的CAPWAP隧道建立过程一致。



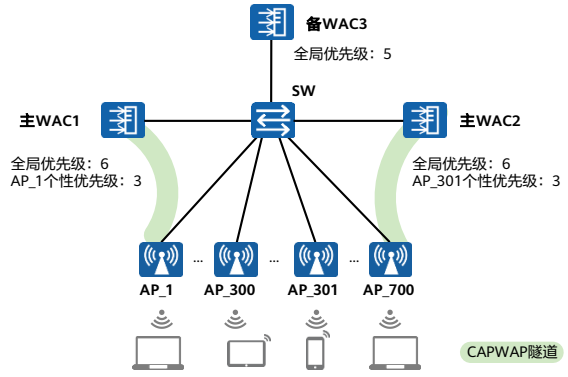
HUAWEI

- 在Discovery阶段，AP发送DiscoveryRequest报文，WAC在收到AP的报文后会回应Discovery Response报文，并在Discovery Response报文中携带优选WAC的IP地址、备选WAC的IP地址、N+1备份开关、WAC优先级、负载情况以及WAC的IP地址。AP根据收到的多个WAC回应的信息，来选择主WAC并开始与其建立CAPWAP链路。
- 在规划N+1备份组网时，需要保证通过比较WAC的优先级就能选择出主WAC，以确保所有 AP 都能够在预先规划的主WAC中上线。否则 AP 上线时会根据WAC的负载或IP地址情况选择主WAC，无法确保AP在预先规划的主WAC中上线。或者保证通过指定的优选WAC和备选WAC就能选择出主WAC。
- 主WAC优选顺序如下：
  - AP查看优选WAC，如果只有一个优选WAC，则此WAC作为主WAC。如果存在多个优选WAC，则选择负载最轻的WAC作为主WAC，如果负载相同选择IP地址最小的作为主WAC。
  - 负载的比较方式：比较WAC设备的负载情况，即AP个数和STA个数，负载轻的为主WAC。优先选择当前可接入AP数大的WAC为主WAC，如果当前可接入AP数相同，则选择当前可接入STA数大的WAC为主WAC。
    - 当前可接入AP数=可接入的最大AP数-当前已接入的AP数。
    - 当前可接入STA数=可接入的最大STA数-当前已接入的STA数。

- 如果没有优选WAC，查看备选WAC，如果只有一个备选WAC，则此WAC作为主WAC，如果存在多个备选WAC，则选择负载最轻的WAC作为主WAC，如果负载相同选择IP地址最小的作为主WAC；
- 如果没有备选WAC，比较WAC的优先级，优先级最高的作为主WAC。优先级取值越小，优先级越高。
- 优先级相同情况下，则选择负载最轻的WAC作为主WAC。
- 负载相同情况下，继续比较IP地址，IP地址小的为主WAC。

主备优先级

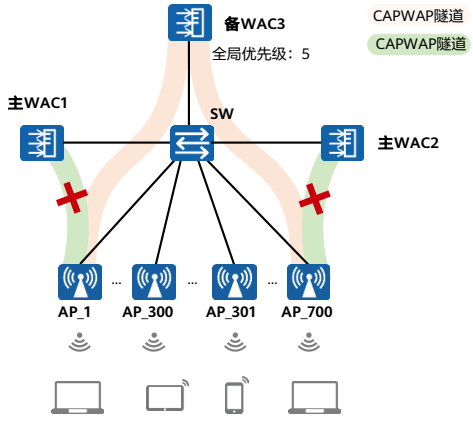
- WAC上存在两种优先级：
  - 全局优先级：针对所有AP配置的WAC优先级。
  - 个性优先级：针对指定的单个AP或指定AP组中的AP配置的WAC优先级。



HUAWEI

- 当WAC收到AP发送的Discovery Request报文时，如果WAC没有为该AP配置个性优先级，则在回应的Discovery Response报文中携带全局优先级；如果WAC已为该AP配置了个性优先级，则在回应的Discovery Response报文中携带个性优先级。正确配置主WAC和备WAC的不同优先级，可以控制AP能够在指定的主WAC或备WAC上线。
- 如图所示：
  - 在Discovery阶段，AP_1通过向WAC发送Discovery Request报文，请求WAC的回应。
  - 当WAC1接收到AP_1的Discovery Request报文时，由于WAC1仅指定了AP_1的个性优先级，则返回给AP_1的优先级为3。
  - WAC2和WAC3没有为AP_1配置个性优先级，所以WAC2回应全局优先级6，WAC3回应全局优先级5。
  - AP_1根据所有WAC回应的信息，进行优先级比较，比较出WAC1的优先级最高，选择WAC1作为主WAC，发送关联请求接入。
  - 如果WAC1或WAC1和AP_1间的CAPWAP链路发生故障，在主WAC上没有指定备WAC的前提条件下，AP_1会重新发送Discovery Request报文，获取WAC的优先级。此时WAC2回应全局优先级6，WAC3回应全局优先级5，比较出WAC3优先级最高，所以选择WAC3作为备WAC发送关联请求接入。

N+1冷备份主备倒换

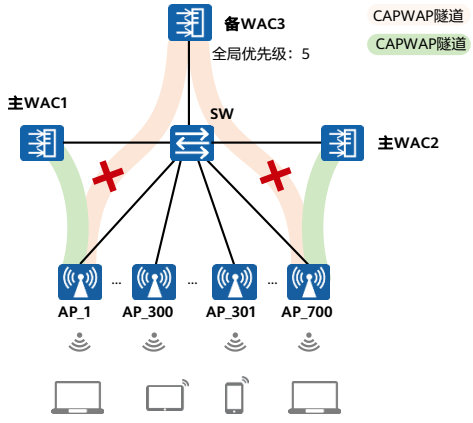


- 正常情况下，AP只和主WAC建立CAPWAP链路，并定期向主WAC发送心跳报文进行心跳检测，不和备WAC建立CAPWAP链路。
- 当AP检测到心跳报文超时后，认为AP和主WAC间的链路中断，会与备WAC建立CAPWAP链路。
- 建立CAPWAP链路后备WAC会重新下发配置给AP，为保证备WAC下发给AP的WLAN业务配置和主WAC下发的相同，必须要求所有主WAC上的WLAN相关业务配置，都要在备WAC上同样配置。
- 为保证 AP 能够在主备倒换后正常工作，设计时需充分考虑备WAC设备规格。

HUAWEI

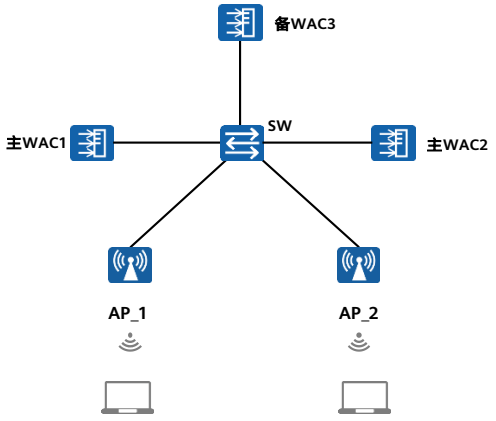
- 建立链路存在两种情况：
  - 如果主WAC上配置了备WAC的IP地址，则AP直接和备WAC建立CAPWAP链路；
  - 如果主WAC上未配置备WAC的IP地址，则AP需要通过发送广播Discovery Request报文发现WAC，重新进行主备选择、选出备WAC，再和备WAC建立CAPWAP链路。
- 为保证 AP 能够在主备倒换后正常工作，需要同时满足下面两个要求：
  - 备WAC中能够上线的AP数不小于任意一个主WAC中实际上线 AP 数。
  - 所有主WAC中上线的AP数总和不能超过备WAC中可配置AP规格数目。
- N+1备份中，N取值取决于备WAC上可配置AP规格数目和N个主WAC实际管理的AP数目，即要求N个主WAC实际管理的AP数目总和，不大于备WAC上可配置AP规格数目。

N+1冷备份主备回切



- AP和备WAC建立CAPWAP链路后，从备WAC获取对应主WAC的IP地址，然后定期发送Primary Discovery Request报文对主WAC进行探测。
- 主WAC恢复后，会回应AP的探测报文，并携带优先级。
- AP通过WAC回应的报文判断主WAC恢复，再根据优先级比对以及回切开关配置，判断是否回切。

配置N+1冷备份



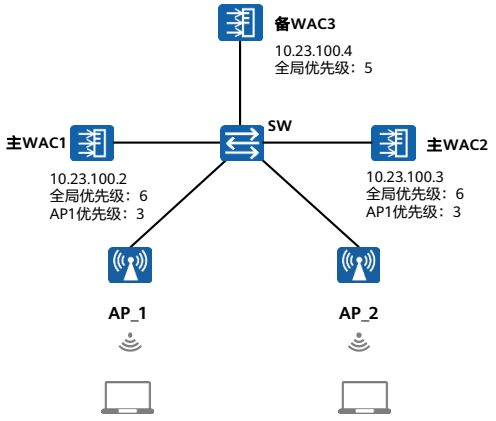
配置思路

- 配置主备WAC全局优先级
- 配置主备回切功能
- 配置心跳检测（可选）
- 配置主备切换模式（可选）
- 使能N+1备份功能

HUAWEI

- 对于心跳检测和主备切换模式和其他备份方法一致，案例中都采用了缺省配置，这里不再举例阐述。

配置N+1冷备份 - 配置WAC全局优先级



在WAC1上，配置备WAC3的IP地址、全局优先级，用于N+1备份。

```
[WAC_1-wlan-view] ac protect priority 6
[WAC_1-wlan-view] ac protect protect-ac ip-address 10.23.100.4
```

在WAC2上，配置备WAC3的IP地址、全局优先级，用于N+1备份。

```
[WAC_2-wlan-view] ac protect priority 6
[WAC_2-wlan-view] ac protect protect-ac ip-address 10.23.100.4
```

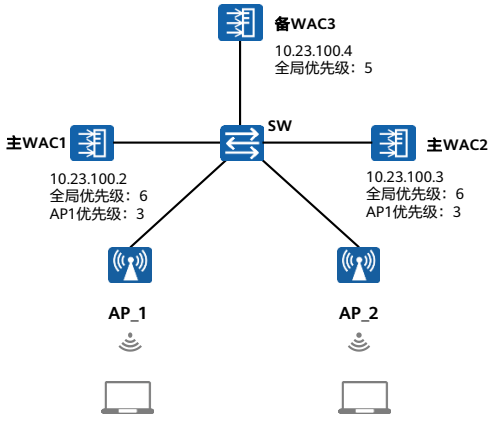
在WAC3上，配置WAC1、WAC2的IP地址、全局优先级，用于N+1备份。

```
[WAC_3-wlan-view] ac protect priority 5
[WAC_3-wlan-view] ac protect protect-ac ip-address 10.23.100.2
[WAC_3-wlan-view] ac protect protect-ac ip-address 10.23.100.3
```


HUAWEI

- 通过配置WAC的优先级来决定主备WAC，优先级高的WAC作为主WAC，优先级低的WAC作为备WAC。
- 数字越小，优先级越高。
- 优先级相同情况下可接入AP数大的WAC为主WAC。
- 可接入AP数量相同情况下可接入用户数大的WAC为主WAC。
- 以上都相同的情况下IP地址小的WAC为主WAC。

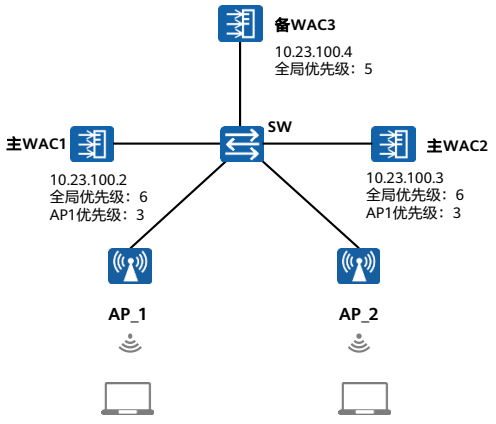
配置N+1冷备份 - 配置主备回切功能



在WAC3上使能主备回切功能，主WAC上无需使能。

[WAC3-wlan-view] **undo ac protect restore disable**

配置N+1冷备份 - 使能N+1备份功能



在WAC_1上，使能N+1备份功能，重启所有AP使N+1备份功能生效。

```
[WAC_1-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[WAC_1-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]:y
```

在WAC_2上，使能N+1备份功能，重启所有AP使N+1备份功能生效。

```
[WAC_2-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[WAC_2-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]:y
```

在WAC_3上，使能N+1备份功能，重启所有AP使N+1备份功能生效。

```
[WAC_3-wlan-view] undo ac protect restore disable
Info: Protect restore has already enabled.
[WAC_3-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[WAC_3-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]:y
```


HUAWEI

- 缺省情况下，N+1备份功能开启，执行命令undo ac protect enable会提示Info。需要在主WAC上继续执行命令ap-reset all重启所有AP，AP重启后，N+1备份功能开始生效。

配置N+1冷备份 - 检查配置结果

在主WAC1和WAC2上上执行命令**display ac protect**和**display ap-system-profile**，查看WAC上N+1备份信息。

```
[WAC_1-wlan-view] display ac protect
------------------------------------------------------------------
Protect state          : disable
Protect AC IPv4        : 10.23.100.4
Protect AC IPv6        : -
Priority               : 6
Protect restore        : enable
...
------------------------------------------------------------------
[WAC_1-wlan-view] display ap-system-profile name ap-system
------------------------------------------------------------------
AC priority                    : 3
Protect AC IP address          : -
Primary AC                     : -
Backup AC                      : -
...
------------------------------------------------------------------
```

在备WAC_3上执行命令**display ac protect**和**display ap-system-profile**，查看WAC上N+1备份信息。

```
[WAC_3-wlan-view] display ac protect
------------------------------------------------------------------
Protect state          : disable
Protect AC IPv4        : -
Protect AC IPv6        : -
Priority               : 5
Protect restore        : enable
------------------------------------------------------------------
[WAC_3-wlan-view] display ap-system-profile name ap-system
------------------------------------------------------------------
AC priority                    :-
Protect AC IP address          : 10.23.100.2
Primary AC                     :-
Backup AC                      :-
------------------------------------------------------------------
[WAC_3-wlan-view] display ap-system-profile name ap-system1
------------------------------------------------------------------
AC priority                    :-
Protect AC IP address          : 10.23.100.3
Primary AC                     :-
Backup AC                      :-
------------------------------------------------------------------
```

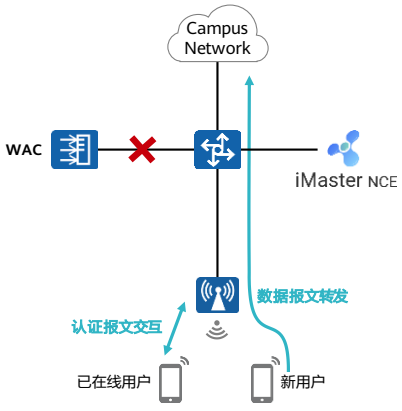
目录

CAPWAP断链逃生简介

- CAPWAP断链逃生是指WLAN网络直接转发场景中，当CAPWAP链路故障时，通过部署的逃生策略，实现原有WLAN业务不中断，原有用户不被迫下线。
- CAPWAP逃生策略包括：
  - CAPWAP断链后VAP业务保持
  - CAPWAP断链后启用备份VAP
  - 广域认证逃生

- CAPWAP断链后VAP业务保持。
  - CAPWAP断链后，AP能够继续提供数据业务，老用户的业务不中断，部分新用户仍可以安全性不高的认证方式接入。
- 广域认证逃生。
  - 总部分支场景中，CAPWAP断链后，AP能够继续提供数据业务，老用户的业务不中断，新用户仍可使用断链前的认证方式在AP本地认证接入。
- CAPWAP断链后启用备份VAP。
  - CAPWAP断链后，关闭原有VAP，自动开启备份VAP。所有用户从原有VAP下线，用户手动关联备份VAP，使得用户可以通过备份VAP生成的逃生SSID临时接入。

本地转发CAPWAP断链业务保持



功能说明

1. 用户数据通过本地转发模式转发。AP与WAC之间的CAPWAP链路中断后，已在线用户的业务不会中断，用户的数据可正常转发。
2. 使能CAPWAP断链允许新用户接入功能后，当WAC与AP之间断链时，新用户接入过程中的认证、关联以及后期的密钥协商阶段将在AP与STA之间完成。
3. 新用户能否接入上线取决于其绑定的认证方式。

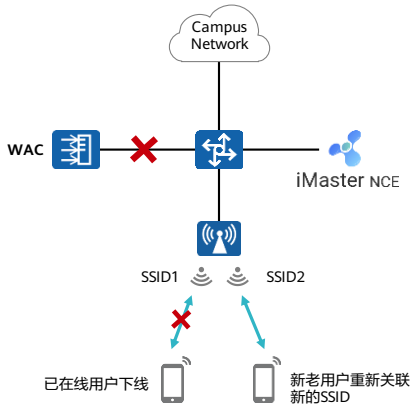
应用场景

对于没有部署备份WAC的小型无线网络，该特性可保证当AP与WAC断开连接时，用户数据转发不中断，提升业务可靠性。

HUAWEI

- 在当前方案中，WAC与AP之间的组网形态必须为本地转发，不能使用隧道转发模式。
- 未使能CAPWAP断链允许新用户接入功能时，STA完成接入过程中的关联以及后期的密钥协商阶段都是发生在WAC与STA之间；使能CAPWAP断链允许新用户接入功能后，STA完成接入过程中的认证、关联以及后期的密钥协商阶段都是发生在AP与STA之间。
- 新用户接入时：
  - OPEN、WEP、WPA/WPA2-PSK，新用户认证方式不变。
  - MAC认证、Portal认证、MAC优先的Portal认证，新用户使用免认证接入。
  - 其他认证方式，新用户无法接入。

CAPWAP断链启用备份VAP



功能说明

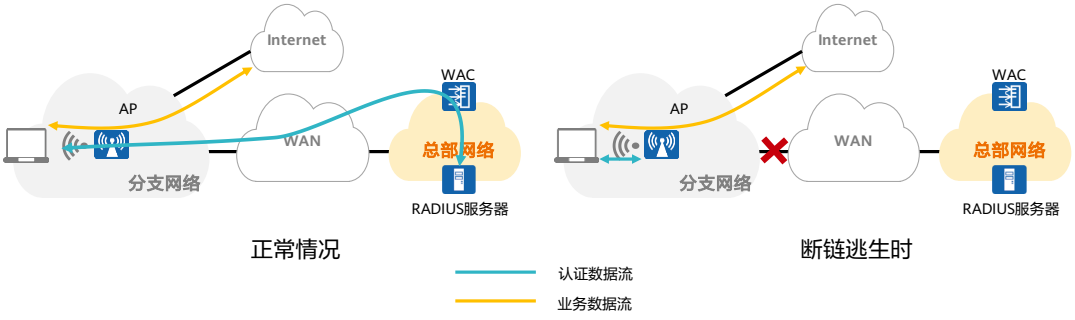
1. 老用户全部下线，所有用户以备份VAP的认证方式接入。
2. 备份VAP支持OPEN、WEP、WPA+PSK、WPA2+PSK、以及WPA-WPA2+PSK的认证方式。
3. 故障恢复后， AP 再自动关闭逃生SSID，恢复原有SSID 。
4. 数据业务转发方式只能是直接转发。

应用场景

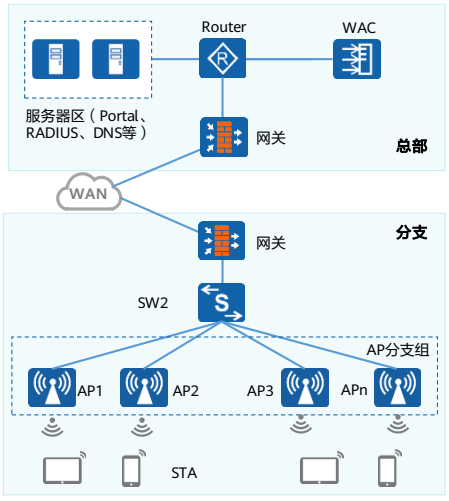
对于没有部署备份WAC的小型无线网络，该特性相对CAPWAP断链业务保持的逃生策略，安全性较高。

广域认证逃生简介

- 在园区总部分支场景中，总部与分支之间跨越广域网，WAC部署在园区总部，AP部署在园区分支。当分支AP与总部WAC断开时，可以部署园区广域认证逃生方案，使园区AP与总部WAC断开后，新用户仍然能接入到网络中。



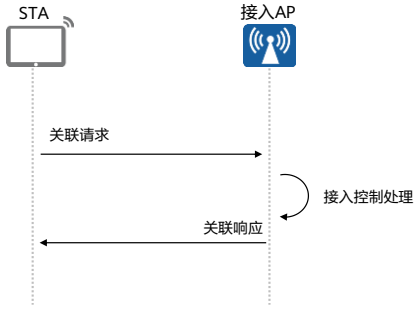
广域认证逃生网络架构



- 在分支建立分支AP组，将用户接入、接入认证等业务下移至AP处理，减少分支对总部的依赖，对于分支与总部断开连接的情况，也能保证分支用户能够继续使用WLAN网络。
  - WAC：用于集中监控和管理AP。
  - 分支AP组：用于统一管理分支AP组内的成员AP。
  - AP1～APn：分支AP组内的成员AP（加入分支AP组的AP简称分支AP）。

STA在离线分支AP上线过程

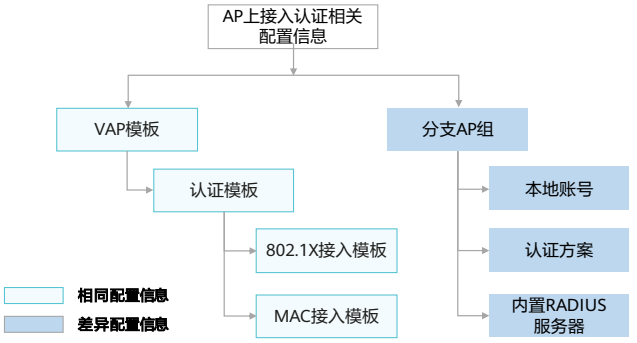
- 在广域认证逃生场景下，WAC与AP断链时，STA接入采用分布式AP控制方案。此方案使得关键业务下移到AP侧，降低网络中丢包和延时概率，有效提升用户的业务体验。
- STA在离线分支AP上线时，前两个阶段与普通上线过程相同，主要区别在于关联阶段：



- STA向接入AP发送关联请求，请求帧中会携带STA自身的各种参数以及根据服务配置选择的各种参数（主要包括支持的速率、支持的信道、支持的QoS的能力以及选择的接入认证和加密算法）。
- 接入AP收到关联请求后对STA进行接入控制。
- 接入AP向STA发送关联响应。

广域认证逃生实现过程：WAC配置下发到AP

- 在广域网络中断，WAC与AP断链时，AP要具有本地认证功能，对新接入的用户进行认证，所以WAC需要将接入认证相关配置下发到AP。
- 配置下发的内容可以分为两部分:
  - AP与WAC上相同信息的配置下发。
  - AP与WAC上差异信息的配置下发。



HUAWEI

- 配置下发的内容可以分为两部分：
  - AP与WAC上相同信息的配置下发：为减少管理员重复配置的工作量，AP与WAC上相同的信息复用VAP模板视图下的配置。下发的配置包括VAP模板绑定的认证模板，认证模板绑定的802.1X接入模板和MAC接入模板等。
  - AP与WAC上差异信息的配置下发：差异信息主要包括用户在进行本地认证时需要的本地账号和认证方案相关配置，对于802.1X接入用户，还需要配置内置RADIUS服务器用于处理EAP认证报文。AP与WAC上差异的信息配置在分支AP组视图下，相同分支AP组内的AP下发的信息相同。
- 说明：
  - WAC上的配置仅会下发到分支AP上。

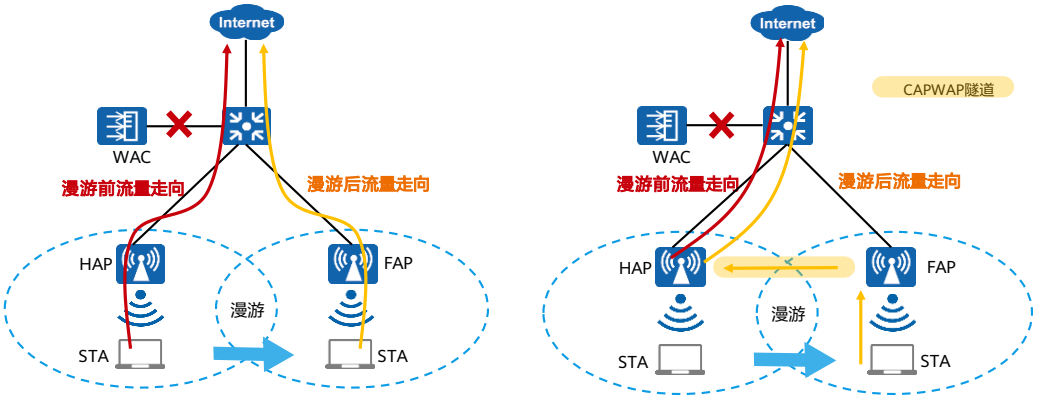
广域认证逃生实现过程：AP内置RADIUS服务器功能

- AP内置的RADIUS服务器功能能够处理EAP认证报文，实现在不部署外部认证服务器的情况下，完成无线终端的802.1X认证。
- AP内置RADIUS服务器功能支持的EAP认证协议包括：
  - EAP-TLS
  - EAP-PEAP
  - EAP-TTLS

- 当用户使用802.1X认证时，由于手机等无线终端不支持EAP终结方式，所以设备的802.1X认证方式必须配置为EAP中继方式。当设备配置为EAP中继认证方式时，设备不会处理EAP认证报文，EAP认证报文需要发送到认证服务器进行处理。

离线分支AP间漫游

- 在广域认证逃生场景下，AP离线时，STA在离线分支AP间的漫游可以分为二层漫游和三层漫游。



- 二层漫游后STA仍然在原来的子网中，FAP对二层漫游用户的报文转发同普通新上线用户没有区别，直接在FAP本地的网络转发。
- 三层漫游时，用户漫游前后不在同一个子网中，为了支持用户漫游后仍能正常访问漫游前的网络，需要将用户流量通过隧道转发到原来的子网进行中转。

CAPWAP链路恢复（1）

- CAPWAP断链业务保持：
  - 当认证方式为非open时，所有用户会被强制下线，用户需要重新上线。
  - 当认证方式为open时，对用户的处理方式有所不同：
    - CAPWAP断链期间AP未重启：对于断链前就在线的用户，不会被强制下线；对于断链期间新上线的用户，会被强制下线。
    - CAPWAP断链期间AP重启：所有用户都相当于断链期间新上线的用户，会被强制下线。

CAPWAP链路恢复（2）

- 广域认证逃生：
  - 所有用户表项将被同步到WAC，在WAC上进行重认证，在重认证通过之前，所有用户将保持断链时的网络权限。如果重认证成功，WAC下发新的网络权限覆盖断链时的网络权限，用户无需重新上线即可正常使用网络；如果重认证失败，用户会被强制下线，需要重新上线。
- CAPWAP断链启用备份VAP：
  - AP自动关闭备份VAP，恢复原有VAP，所有用户从备份VAP下线，需要重新在已恢复的原VAP上线。

逃生策略对比

逃生策略	使用的组网和认证方式	逃生后用户的认证方式	优点	缺点
CAPWAP断链业务保持	适用组网：所有直接转发组网。 适用认证方式：所有认证方式。	老用户业务保持，新用户接入时， OPEN、WEP、WPA/WPA2-PSK，新用户认证方式不变。 MAC认证、Portal认证、MAC优先的Portal认证，新用户使用免认证接入。 其他认证方式，新用户无法接入。	部署简单	安全性不够高，部分认证，新用户无法接入。
广域认证逃生	适用组网：总部分支场景直接转发组网 适用认证方式： WPA/WPA2-PPSK认证。 MAC认证。 802.1X认证。 MAC和802.1X混合认证。	老用户业务保持，新用户认证方式不变。	CAPWAP断链后，新用户仍可以在本地AP上认证，安全性较高。	部署复杂，很多认证方式不支持该逃生策略。
CAPWAP断链启用备份VAP	适用组网：所有直接转发组网。 适用认证方式：所有认证方式。	老用户全部下线，所有用户以备份VAP的认证方式接入。 备份VAP支持OPEN、WEP、WPA+PSK、WPA2+PSK、WPA-WPA2+PSK的认证方式。	相对广域认证逃生策略，部署较简单。 相对CAPWAP断链业务保持的逃生策略，安全性较高。	用户强制下线需重新关联逃生SSID。

配置CAPWAP断链业务保持以及VAP备份

全局CAPWAP断链业务保持在AP系统模板中配置。

```
[WAC-wlan-view] ap-system-profile name ap-system
[WAC-wlan-ap-system-prof-ap-system] keep-service enable allow new-access
[WAC-wlan-ap-system-prof-ap-system] quit
```

VAP下的CAPWAP断链业务保持在VAP模板中配置，优先级高于AP系统模板。

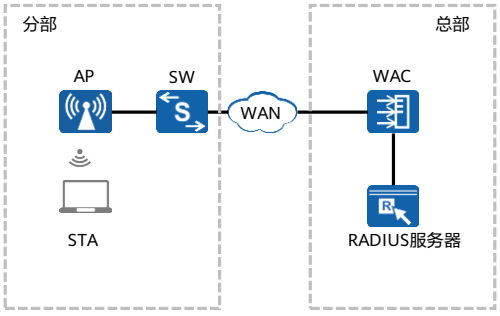
```
[WAC-wlan-view] vap-profile name vap1
[WAC-wlan-vap-prof-vap1] keep-service enable allow new-access
```

CAPWAP断链后，关闭原有VAP，自动开启备份VAP，假设原有VAP模板名为normalvap，备份VAP模板名为backupvap。

```
[WAC-wlan-view]vap-profile name backupvap
[WAC-wlan-vap-prof-backupvap]copy-from normalvap
[WAC-wlan-vap-prof-backupvap]type service-backup ap-offline
```


- keep-service enable：使能CAPWAP断链业务保持功能。
- keep-service enable allow new-access：CAPWAP断链允许新用户接入功能。
- 如果用户希望离线AP允许Portal认证或MAC认证的新用户上线，则必须配置no-auth参数：keep-service enable allow new-access no-auth。
- 在WDS网络中执行该命令，命令功能不生效。
- 设备检测和设备反制功能与离线AP允许新用户上线功能互斥，使能断链允许新用户接入功能后，如果同时执行命令wids device detect enable和wids contain enable开启设备检测和设备反制功能，AP掉线后继续提供数据服务，但AWC将该AP判断为非法设备或干扰设备并加入反制列表，反制机制会阻止新用户接入，因此AP离线后新用户接入功能将不生效。
- 对于AP掉线备份业务型VAP：
  - 配置的AP掉线备份VAP数达到AP上的VAP最大规格时，如果开启了离线管理VAP功能，AP离线时，离线管理VAP不生效。
  - AP掉线备份业务型VAP不能与VAP模板下的断链业务保持功能、DHCP报文的隧道转发功能或mDNS报文的隧道转发功能同时配置。

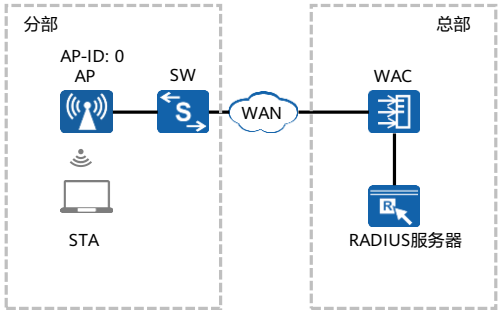
配置广域逃生举例



配置思路

- 创建配置分支AP组
- 配置分支AP组认证方式为本地认证方式
- 配置分支AP组内的本地用户和用户接入类型
- 配置内置RADIUS服务器
- 检查配置结果

配置广域逃生 - 创建配置分支AP组



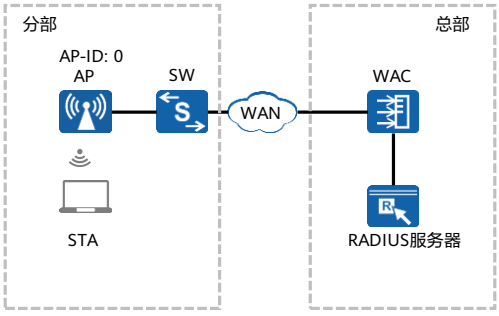
创建名为g1的分支AP组，并将AP 0添加到分支AP组中。

[WAC-wlan-view] **branch-group name** *g1*
[WAC-wlan-branch-group-g1] *ap 0*
Warning: This operation may cause AP reset. Continue? [Y/N]:y

HUAWEI

- 一个分支AP组最多支持50个AP加入。
- AP加入分支AP组后会重启，请谨慎操作。

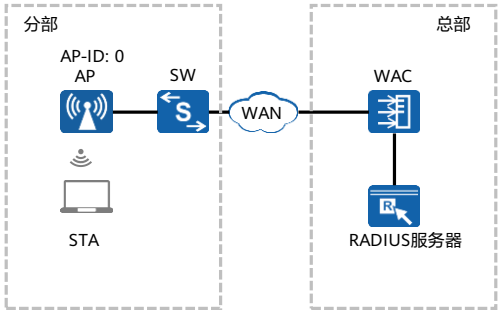
配置广域逃生 - 配置分支AP组认证方式



配置分支AP组g1的认证方式为本地认证。

[WAC] **aaa**
[WAC-aaa] **authentication-scheme** *branch*
[WAC-aaa-authen-branch] **authentication-mode** *local*
[WAC-aaa-authen-branch] **quit**
[WAC-aaa] **quit**
[WAC] **wlan**
[WAC-wlan-view] **branch-group name** *g1*
[WAC-wlan-branch-group-g1] **authentication-scheme** *branch*

配置广域逃生 - 配置分支AP组内的本地用户



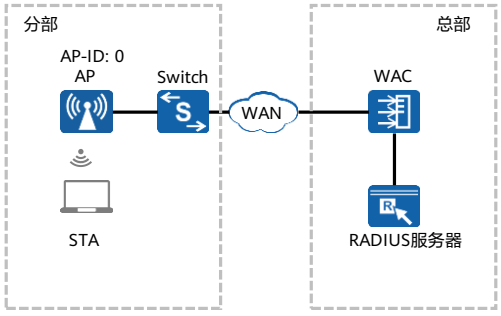
802.1X认证：

[WAC-wlan-branch-group-g1] **local-user** *test1* **password cipher** *Huawei@123*
[WAC-wlan-branch-group-g1] **local-user** *test1* **service-type** 8021x

MAC认证：

[WAC-wlan-branch-group-g1] **local-user** *e005c5fab829* **password cipher** *Huawei@123*
[WAC-wlan-branch-group-g1] **local-user** *e005c5fab829* **service-type** *8021x*

配置广域逃生 - 配置内置RADIUS服务器



配置内置RADIUS服务器。

```
[WAC-wlan-branch-group-g1] local-eap-server
authentication eap-method eap-peap eap-ttls eap-tls
[WAC-wlan-branch-group-g1] local-eap-server
authentication certificate ca format pem filename
caserver.pem
[WAC-wlan-branch-group-g1] local-eap-server
authentication certificate local format pem filename
serverlocal.pem
[WAC-wlan-branch-group-g1] local-eap-server
authentication private-key format pem filename server.pem
password Huawei@123
[WAC-wlan-branch-group-g1] load-authentication-file
```


HUAWEI

- 举例中配置的CA证书、本地证书和私钥文件仅为示例，实际配置中请根据实际情况，配置符合实际要求的CA证书、本地证书和私钥文件。

配置广域逃生 - 检查配置结果

在WAC与AP断链情况下，登录AP，可以看到本地用户已上线。

```
<AP> display access-user
--------------------------------------------------------------------------------
UserID   Username          IP address      MAC             Status
--------------------------------------------------------------------------------
6        test1             10.23.11.163    e005-c5fa-b829  Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

其他常用查询命令：

- 命令display branch-group，查看分支AP组的配置信息。
- 命令display ap branch-group，查看分支AP组中AP的信息。
- 命令display ap authentication-file status，查看当前AP证书加载的信息。

思考题

1. 华为常用的倒换保护技术中，不支持异地部署的是哪种?
2. CAPWAP断链逃生，仅在哪种转发方式支持?

HUAWEI

- VRRP双机热备
- 直接转发

本章总结

- 本章介绍了WLAN网络可靠性常用保护倒换方案包括双机热备份、双链路冷备份、N+1备份以及CAPWAP断链逃生策略包括CAPWAP断链业务保持、广域认证逃生、CAPWAP断链启用备份VAP的基本原理以及典型配置。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN漫游

HUAWEI

前言

- WLAN网络的最大优势就是无线终端不受物理介质的影响，可以在WLAN信号覆盖范围内四处移动并且能够保持业务不中断。
- WLAN漫游可保证用户IP地址不变，漫游后仍能访问初次上线时关联的网络，且业务不中断。
- 本课程介绍了WLAN漫游的基本概念、漫游技术详解、漫游体验优化手段、典型漫游场景及漫游故障排除等。

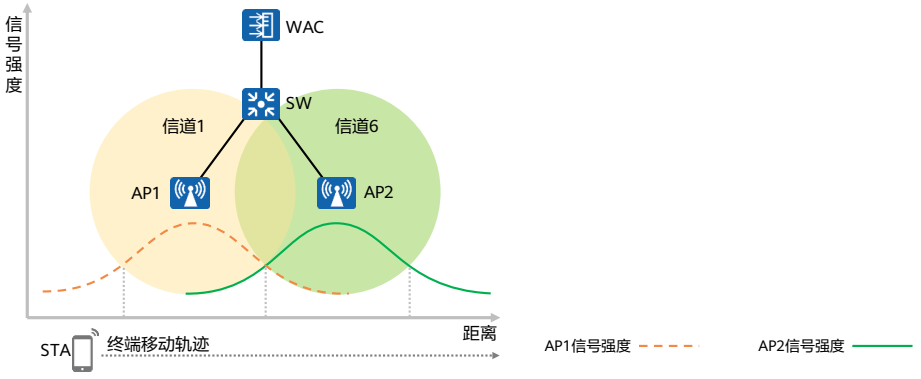
目标

- 学完本课程后，您将能够：
  - 描述WLAN漫游的技术原理
  - 描述常见的WLAN漫游优化技术
  - 描述华为WLAN典型漫游场景
  - 排除WLAN漫游故障

目录

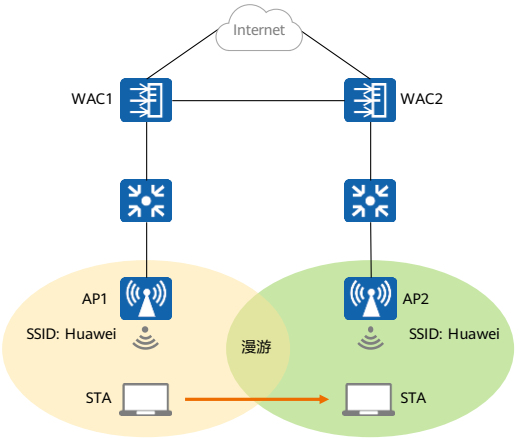
什么是WLAN漫游

- STA在不同AP的信号覆盖范围之间移动，保持用户业务不中断的技术成为WLAN漫游。
- 如图所示，STA从AP1的信号覆盖范围移动到AP2的信号覆盖范围时，保持业务不中断。

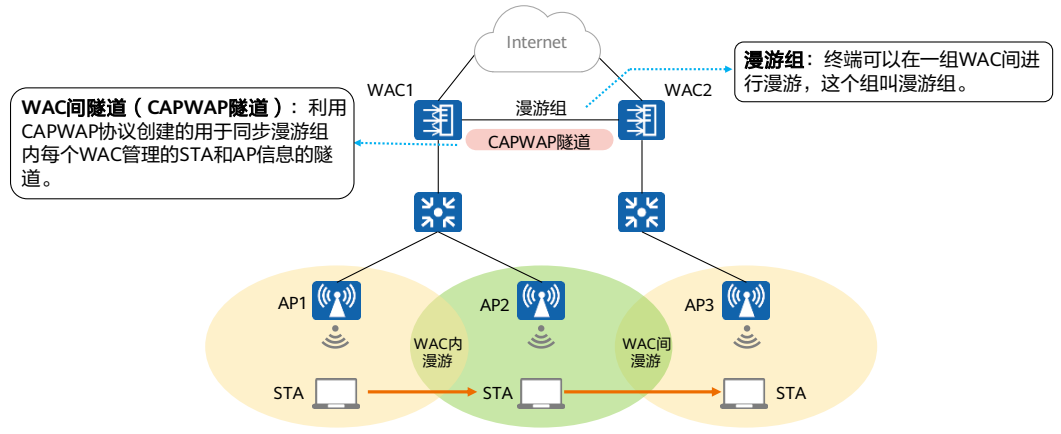


WLAN漫游解决的问题

- 实现WLAN漫游的一组AP必须使用相同的SSID和安全模板（安全模板名称可以不同，但是安全模板的配置必须相同），此外，认证方式和认证参数也要相同。
- WLAN漫游主要解决以下问题：
  - 避免漫游过程中的认证时间过长导致丢包甚至业务中断。
  - 确保用户授权信息不变。
  - 确保用户IP地址不变。



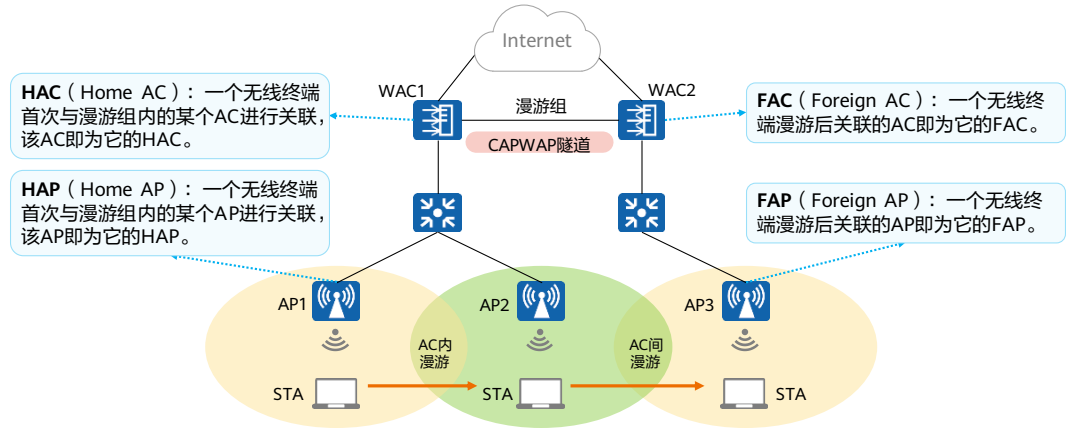
WLAN漫游的网络架构



HUAWEI

- 在本例中，AP1及AP2均由WAC1管理，AP3由WAC2管理。

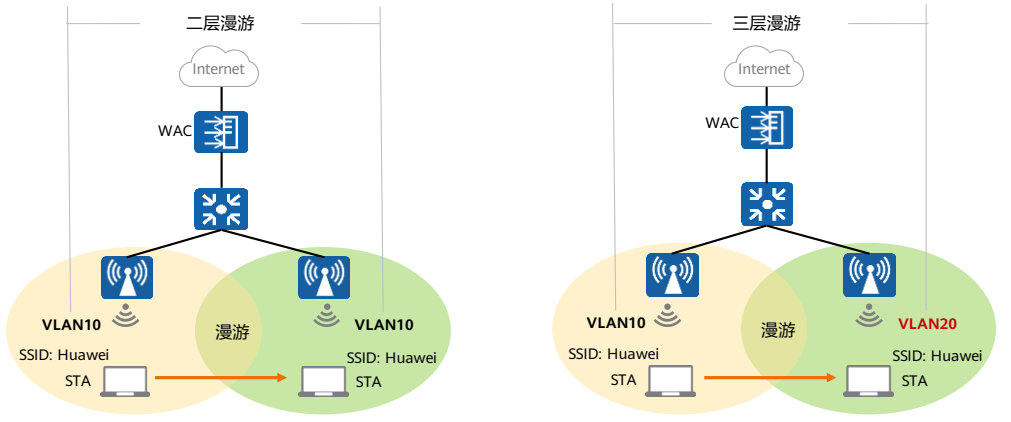
WLAN漫游的相关术语



HUAWEI

- 相关概念：
  - HAC（Home AC）：一个无线终端首次与漫游组内的某个WAC进行关联，该WAC即为它的HAC。
  - HAP（Home AP）：一个无线终端首次与漫游组内的某个AP进行关联，该AP即为它的HAP。
  - FAC（Foreign AC）：一个无线终端漫游后关联的WAC即为它的FAC。
  - FAP（Foreign AP）：一个无线终端漫游后关联的AP即为它的FAP。
- WAC内漫游：如果漫游过程中关联的是同一个WAC，这次漫游就是WAC内漫游。
- WAC间漫游：如果漫游过程中关联的不是同一个WAC，这次漫游就是WAC间漫游。

WLAN漫游类型

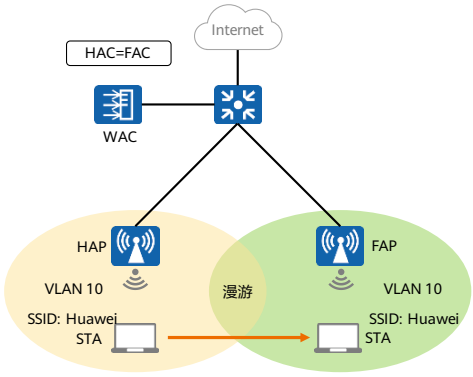


HUAWEI

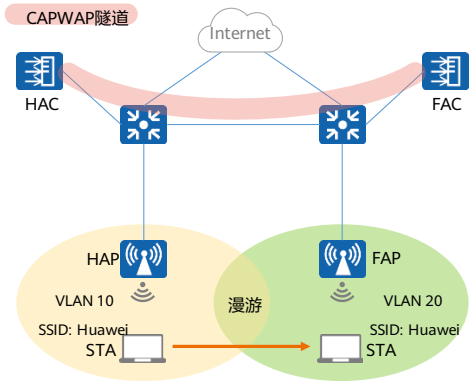
- 二层漫游：终端在AP之间移动时，终端漫游前后，AP的业务VLAN不变，对应的用户网关不变。
- 三层漫游：漫游前后SSID的业务VLAN不同，AP所提供的业务网络为不同的3层网络，对应不同的用户网关；此时，为保持漫游用户IP地址不变的特性，需要将用户流量迂回到初始接入网段的AP，实现跨VLAN漫游。
- 网络中有时会出现以下情况：两个子网的VLAN ID相同，此时为了避免系统仅仅依据VLAN ID将用户在两个子网间的漫游误判为二层漫游，需要通过漫游域来确定设备是否在同一个子网内，只有当VLAN相同且漫游域也相同的时候才是二层漫游，否则是三层漫游。

WAC内漫游

- WAC内漫游：如果漫游过程中，终端关联的是同一个WAC，此次漫游就是WAC内漫游；
- WAC内漫游可看作是WAC间漫游的一种特殊情况，即HAC和FAC重合。



WAC间漫游



- 漫游组：在WLAN网络中，可以对不同的WAC进行分组，STA可以在同一个组的WAC间进行漫游，这个组为漫游组。
- WAC间隧道：为了支持WAC间漫游，漫游组内的所有WAC需要同步每个WAC管理的STA和AP设备的信息，因此在WAC间建立一条隧道作为数据同步和报文转发的通道。WAC间隧道也是利用CAPWAP协议创建的。

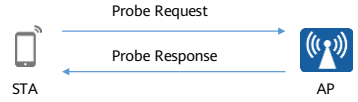
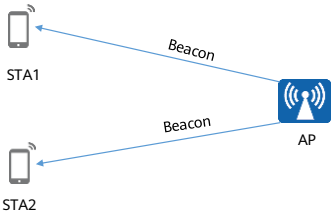
- STA在WAC间进行漫游，通过选定一个WAC作为漫游组服务器，在该WAC上维护漫游组的成员表，并下发到漫游组内的各WAC，使漫游组内的各WAC间相互识别并建立WAC间隧道。
  - 漫游组服务器既可以是漫游组外的WAC，也可以是漫游组内选择的一个WAC。
  - 一个WAC可以同时作为多个漫游组的漫游组服务器，但是自身只能加入一个漫游组。
  - 漫游组服务器管理其他WAC的同时不能被其他的漫游组服务器管理。也就是说如果一个WAC是作为漫游组服务器角色负责向其他WAC同步漫游配置的，则它无法再作为被管理者接受其他WAC向其同步漫游配置（即配置了漫游组就不能再配置漫游组服务器）。
  - 漫游组服务器作为一个集中配置点，不需要有特别强的数据转发能力，只需要能够和各个WAC互通即可。

目录

终端主动漫游流程

- 终端基于AP的信号强度进行判断，达到预设阈值后触发漫游，一般包括如下三个动作：
  - 扫描：用于发现终端当前所在位置下可见的小区（通过BSSID标识），并测量用于选网判断的网络信息。
  - 选网：基于扫描到的小区信息，选择一个小区作为漫游目标。
  - 漫游：基于终端和网络能力，选择与网络侧匹配的漫游方式。

终端主动漫游：扫描

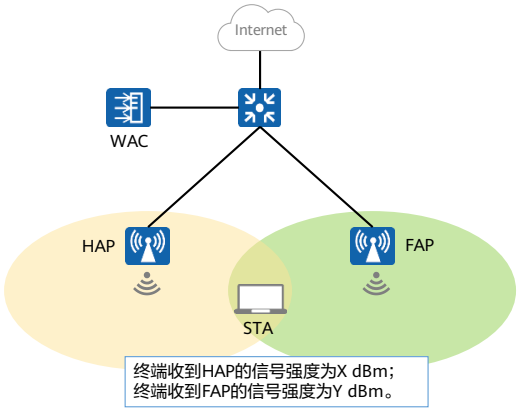
终端主动扫描	终端被动扫描
	
STA依次在每个信道发出Probe Request帧，寻找与STA有相同SSID的AP，只有能够提供指定SSID无线服务的AP接收到该Probe Request后才回复Probe Response。	STA在每个信道上侦听AP定期发送的Beacon信标帧（信标帧中包含SSID、支持速率等信息），以获取AP的相关信息。

HUAWEI

- STA可以通过主动扫描和被动扫描获取到周围的无线网络信息。
- 主动扫描：STA工作过程中，会定期地搜索周围的无线网络，也就是主动扫描周围的无线网络。终端发送主动扫描帧（Probe Request），AP在监听到扫描帧后会进行回复（Probe Response），终端收到Probe Response后感知小区存在。
- 被动扫描：终端监听到AP发送的beacon帧后感知到小区存在，具有概率性。
- 漫游前，终端将轮询扫描所有信道。

终端主动漫游：选网

- 终端执行完扫描后会基于扫描结果产生小区列表，按照一定的规则在列表中搜索可漫游的小区，当所有小区都不满足规则时不进行小区切换。对于选网规则，不同终端设备厂商存在较大差异。



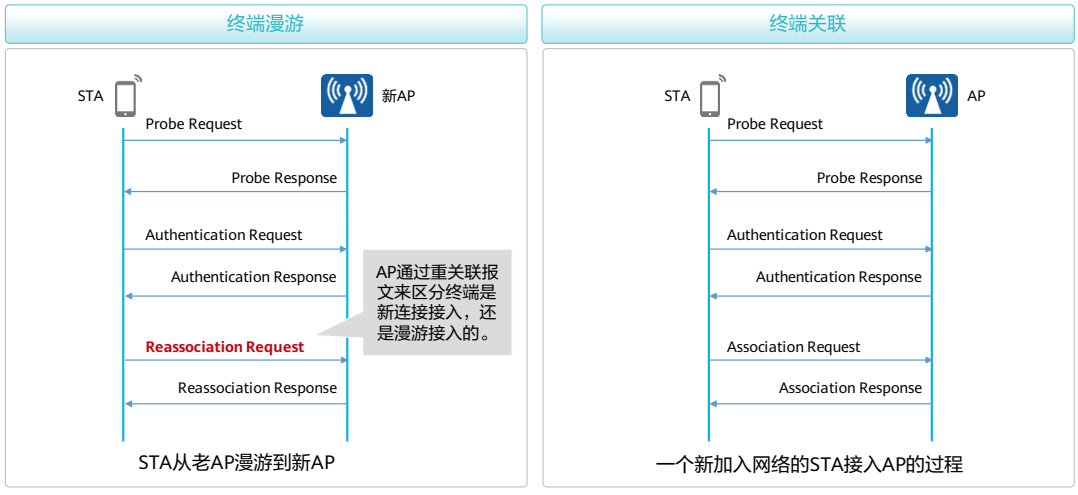
终端主动漫游选网规则

- A：漫游切换信号强度阈值；
- B：漫游切换信号强度差阈值；
- 当满足(X<A) & ((Y-X)>B)时，则满足漫游切换规则，触发终端主动漫游。

HUAWEI

- 以华为手机为例，触发漫游的阈值:
  - 高密：5G：-70 dBm　2.4G：-72 dBm
  - 低密：5G：-74 dBm　2.4G：-78 dBm
- 漫游时优选5G网络，并要求目标小区有至少4dB的增益。

终端主动漫游：漫游



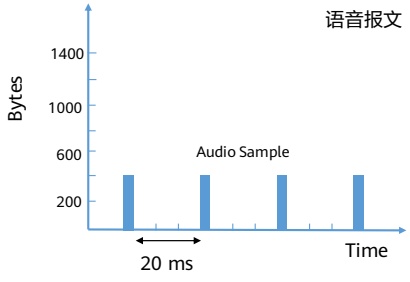
HUAWEI

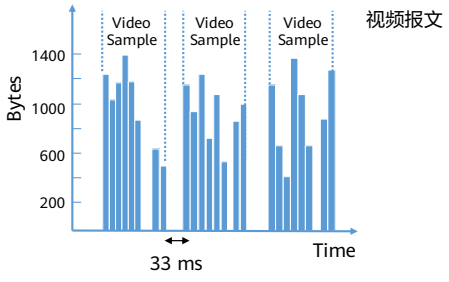
- 一个新加入网络的STA（非漫游终端）接入AP的过程与一个漫游到新AP的终端的接入过程存在一定差异，其中关键差异在于重关联帧。
- AP只有接收到重关联报文才会认为终端是从另外一个AP上漫游过来的，从而设备进行漫游流程的处理。

目录

漫游对业务的影响

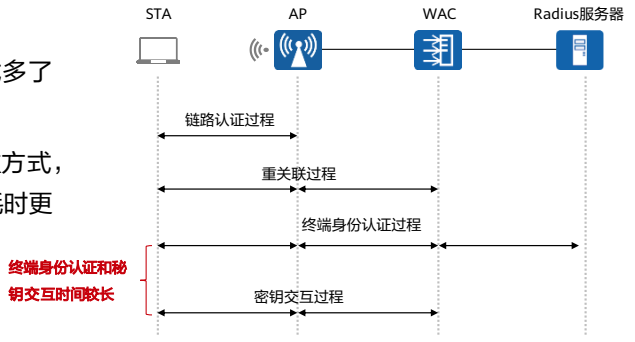
- 视频及语音类业务对时延及丢包是非常敏感的。以语音为例，一般情况下，业务恢复时间不应超过50 ms，漫游时连续丢包数量不应超过3个（业务恢复时间小于60 ms）。
  - 语音报文，一般是按照固定间隔持续发送，例如左图所示的报文间隔为20 ms。
  - 视频报文，每一帧视频画面需要多个报文进行承载，不同帧产生的报文数量及报文长度并不一致，如右图所示的帧间隔为33 ms。





漫游过程耗时

- 漫游切换时间是影响无线用户漫游过程中业务体验的核心指标；
- 802.1x认证漫游过程相比Open方式多了身份认证和秘钥协商过程；
- 802.1x认证漫游过程相比WEP和PSK方式，身份认证过程时间较长，漫游过程耗时更长。

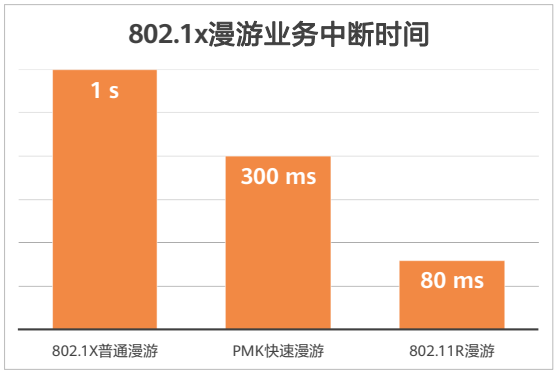


HUAWEI

- 由于Open认证、WEP认证和PSK认证的流程很短，因此漫游的时间也很短，基本能够满足业务不中断的需求。
- 相比之下，802.1x认证的过程较长、交互的报文较多，因此漫游时间大于200ms，对于实时性要求较高的业务，如语音业务等影响较大。

漫游优化概述

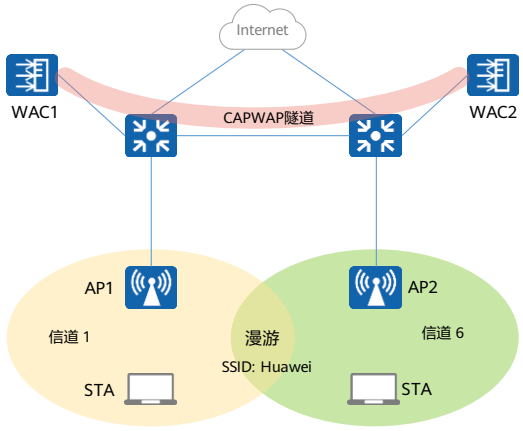
- 终端在切换过程中，业务会中断一段时间，中断时间与使用的漫游方式相关。



WLAN漫游优化方式

- PMK快速漫游
- 802.11r漫游
- 智能漫游（粘性终端）

PMK（Pairwise Master Key）快速漫游

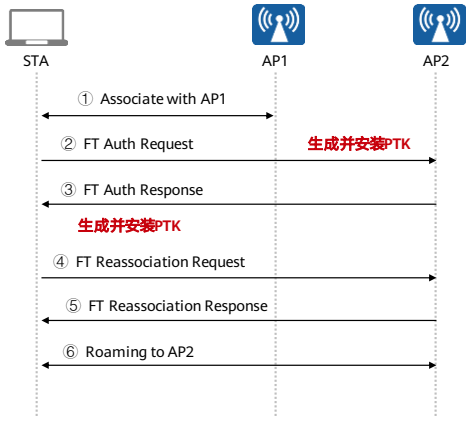


- STA首次通过AP1接入网络时，当STA在WAC1认证成功并生成PMK后，STA和WAC1分别保存PMK信息，每个PMK信息对应一个PMK-ID，PMK-ID是由PMK、SSID、STA的MAC地址和BSSID计算出来的，WAC1通过CAPWAP隧道将PMK信息同步给WAC2。
- 当STA在漫游过程中向AP2发起重关联请求时，重关联请求帧中包含了PMK-ID信息。
- AP2收到请求后及时向WAC2通报用户切换消息。
- WAC2根据STA携带的PMK-ID信息查找PMK缓存表中STA对应的PMK，如果能查找到，就认为STA已经进行过802.1X认证，直接跳过认证过程，利用缓存的PMK开始进行密钥协商。

HUAWEI

- 当用户使用WPA2-802.1X安全策略，或使用WPA-WPA2-802.1X安全策略且802.1X客户端上选择认证方式为WPA2，同时STA支持快速漫游技术时，用户在漫游过程中不需要重新完成802.1X认证过程，只需要完成密钥协商过程即可。这样，通过PMK快速漫游，可以缩短802.1X用户的漫游延时，提升用户上网体验。

WAC内802.11r快速漫游

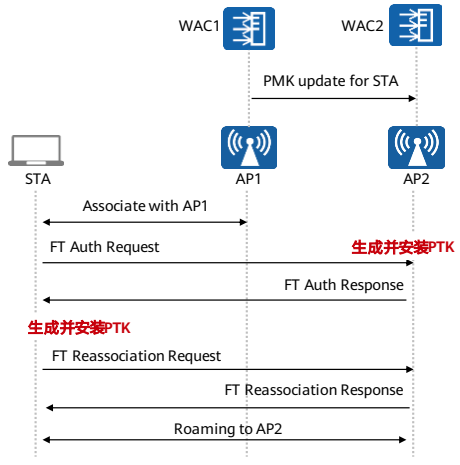


- STA首次通过AP1接入网络时，STA在WAC认证成功并生成PMK。
- WAC根据PMK生成PMK-R0（由SSID、MDID、WAC的MAC地址和STA的MAC地址计算得来）和每个AP对应的PMK-R1（由PMK-R0、AP的MAC地址和STA的MAC地址计算得来），并将PMK-R1下发给AP1。
- STA和WAC通过密钥协商的四次握手和二次握手分别生成并安装PTK和GTK。
- STA在漫游过程中向AP2发起FT认证请求，并将PMK-R1下发给AP2。
- AP2收到请求后，根据其中包含的信息和PMK-R1生成并安装PTK，同时启动重关联定时器，向STA发送802.11 FT认证应答。
- STA收到应答后，根据其中包含的信息生成并安装PTK。STA向AP2发起重关联请求。
- AP2收到重关联请求后，关闭重关联定时器，并向STA发送重关联应答。
- STA收到应答后，完成漫游。

HUAWEI

- 802.11r协议定义了在同一MD (Mobility Domain) 中，通过FT（Fast BSS Transition）功能省略了用户漫游过程中的802.1X认证和密钥协商，减少信息交互次数，从而实现漫游过程中业务数据流低延时，用户不会感知业务中断，提高用户上网体验。
- PTK (Pairwise Transient Key) 成对临时秘钥； PTK 是从 PMK 衍生得出的，用来加密客户端的单播数据帧。
- GTK (Group Transient Key) 组临时密钥是从 GMK 衍生得出的，并且用于加密某个特定 SSID/无线接入点的组播 /广播帧。

WAC间802.11r快速漫游



- STA首次通过AP1接入网络时，STA与WAC1认证成功并生成PMK；
- WAC1根据PMK生成PMK-R0（由SSID、MDID、WAC的MAC地址和STA的MAC地址计算得来）和AP1对应的PMK-R1（由PMK-R0、AP的MAC地址和STA的MAC地址计算得来），并将PMK-R1下发给AP1。
- STA和AC通过密钥协商的四次握手和二次握手分别生成并安装PTK和GTK。
- WAC1通过WAC间隧道将PMK信息同步给WAC2。
- WAC2根据PMK生成PMK-R0和AP2对应的PMK-R1，并将PMK-R1下发给AP2。
- STA在漫游过程中向AP2发起FT认证请求，并将PMK-R1下发给AP2；
- AP2收到请求后，根据其中包含的信息和PMK-R1生成并安装PTK，同时启动重关联定时器，向STA发送802.11 FT认证应答；
- STA收到应答后，根据其中包含的信息生成并安装PTK。STA向AP2发起重关联请求；
- AP2收到重关联请求后，关闭重关联定时器，并向STA发送重关联应答；
- STA收到应答后，完成漫游。

HUAWEI

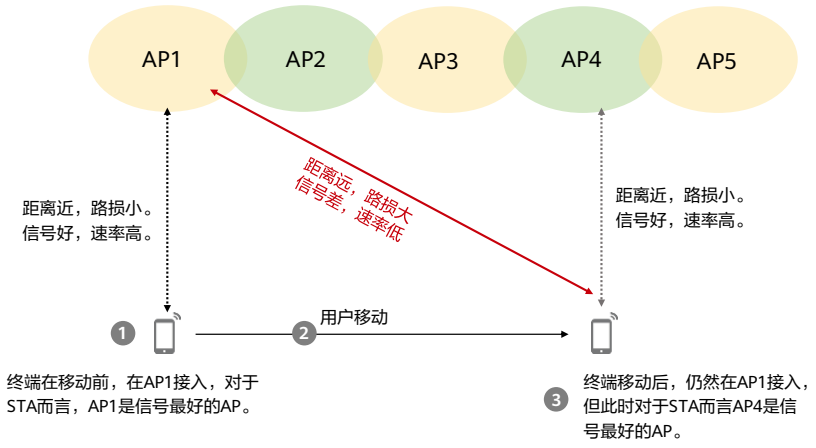
- MDID指的是漫游域ID。
- PTK (Pairwise Transient Key) 成对临时秘钥； PTK 是从 PMK 衍生得出的，用来加密客户端的单播数据帧。
- GTK (Group Transient Key) 组临时密钥是从 GMK 衍生得出的，并且用于加密某个特定 SSID/无线接入点的组播 /广播帧。

WLAN漫游类型比较

漫游类型	是否需要STA支持	适用安全策略	描述
普通漫游	不涉及	所有安全策略	适用所有场景，配置简单，漫游过程中业务可能有短暂中断。
PMK快速漫游	是	WPA2+802.1X/WPA-WPA2+802.1X（802.1X客户端上选择认证方式为WPA2）	漫游时省略了802.1X认证过程，只需要密钥协商，延时较低。
802.11r漫游	是	开放式系统认证/WPA2+PSK+AES/WPA2+PPSK+AES/WPA2+802.1X+AES	漫游时省略了认证和密钥协商过程，延时低。

- PMK快速漫游，适用场景较少（只有漫游回已经完成认证的AP才能生效）。

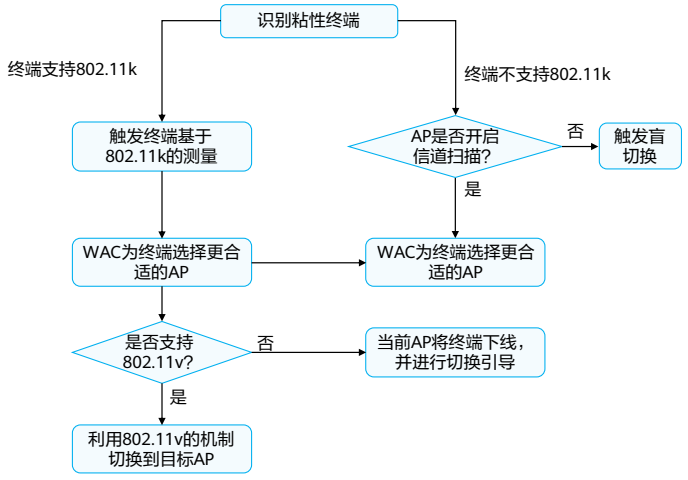
移动场景下的粘性终端



HUAWEI

- 现网应用中，有一类终端漫游的主动性较差，主要表现为：始终“坚持”关联在其最初关联的AP上，即使随着终端的移动，其已经与当前关联的AP距离很远，此时信号很弱、无线传输速率很低，但是这类终端依旧不能漫游到其他信号更好的AP。我们将这类终端称为“粘性终端”。
- 粘性终端带来的危害：
  - 终端自身业务体验差：终端始终关联在信号差的AP上，导致无线信道速率下降严重。
  - 影响无线信道整体性能：终端信号差、速率低，导致经常传输丢包或者重传，长时间占用无线信道，影响其他信号好的终端不能得到足够的时间占用无线信道。

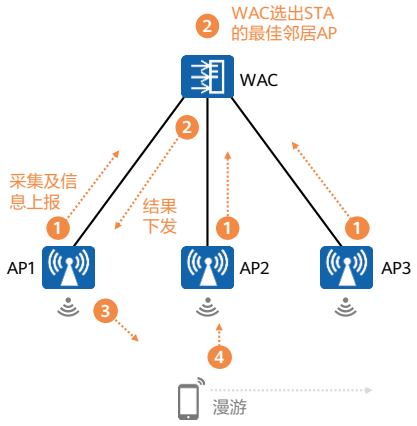
华为智能漫游的主要原理



HUAWEI

- 为了解决粘性终端的问题，华为提出了智能漫游方案。
- 从漫游流程来说，任何一次的漫游都要经过漫游测量、漫游判决和漫游执行这三个过程。
  - 网络侧通过收集终端信息以判断终端是否粘性，并获知终端能力。
  - 根据判决机制和收集的信息决定粘性终端是否要进行漫游、漫游到哪个AP。
  - 在漫游执行中，WAC帮助粘性终端选择更合适的AP进行接入。

智能漫游的流程

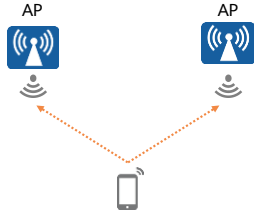


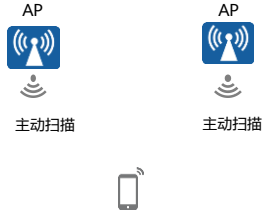
1. AP采集周边的终端信息，发现邻居AP，将信息周期性上报给WAC。
2. WAC在终端邻居表中选出STA的最佳邻居AP，例如AP2，并将其作为STA的漫游目标下发给AP1。
3. AP1通过802.11v的BSS transition机制或者强制用户下线的方式，促使STA漫游到目标AP2上。
4. STA漫游到目标AP2上。

- STA关联到AP1时，AP1实时采集STA的信噪比和接入速率，并判断STA是否为粘性终端。如果AP1认为STA为粘性终端，则将此信息上报WAC。

智能漫游 - 邻居AP信息收集

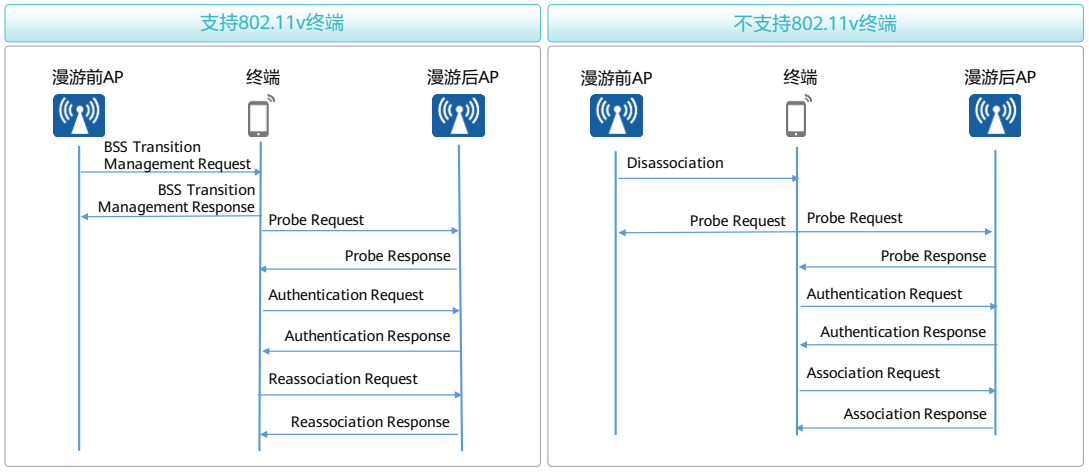
支持802.11k的终端	不支持802.11k的终端
• 在当前关联的AP检测到终端为粘性时，主动触发终端进行基于802.11k机制的邻居信息收集。	• **不支持802.11k的终端，需要AP通过主动扫描发现终端的邻居AP。**





粘性终端需要网络帮助其选择更合适的AP，这就需要网络侧收集终端周边的AP的信息。这个信息需要通过测量来收集，802.11k本身就提供了这种测量和信息收集的机制，对于支持802.11k的终端可以直接利用这个测量机制。对于不支持802.11k的终端则需要AP通过主动扫描发现终端的邻居AP。

智能漫游 - 引导终端漫游切换流程



HUAWEI

- 对于支持802.11v的终端，网络侧为终端指定最合适的漫游后AP。具体流程为：通过BSS Transition Management Request消息把目的AP的信息（例如AP工作的信道等）发送给终端，终端通过BSS Transition Management Response响应AP发出的802.11v切换请求消息，终端与目标AP之间进行认证信息交互后，通过重关联消息接入新的AP。
- 对于不支持802.11v的终端或者虚假支持802.11v的终端（在其发送的报文中宣称支持802.11v，但实际能力并不支持802.11v的终端），WAC通知当前AP将该粘性用户下线，并向当前关联的AP下发终端黑名单。AP对黑名单中的终端处理如下：暂停响应终端发送的Probe Request 10次；拒绝终端关联1次。

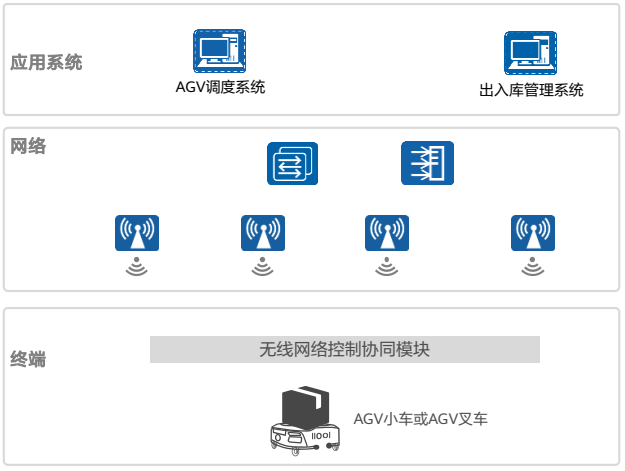
智能漫游关键配置

- 配置智能漫游。

```
[WAC-wlan-view] rrm-profile name wlan-rrm
[WAC-wlan-rrm-prof-wlan-rrm] undo smart-roam disable                    //使能智能漫游功能
[WAC-wlan-rrm-prof-wlan-rrm] smart-roam roam-threshold check-snr  //指定用户漫游触发方式为基于终端信噪比
[WAC-wlan-rrm-prof-wlan-rrm] smart-roam roam-threshold snr 15           //设置触发门限值
```

目录

智能仓储场景下的漫游及存在的问题



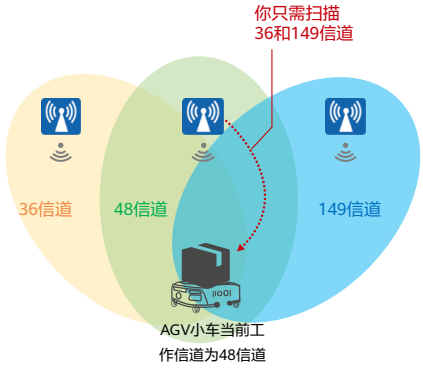
- 漫游主动性差：依靠网络侧踢下线的方式触发漫游，导致性能不稳定；
- 漫游时延偏大：终端漫游过程中，网络中断时间往往超过1~2 s，导致业务受影响；
- 漫游异常掉线：终端异常掉线，并出现降速和停顿现象，需要人工介入。

HUAWEI

- 伴随自动化浪潮，全球物流行业IT投资额持续快速增长。其中仓储物流是物流产业中最重要的环节之一，行业需求快速发展的同时，自动机器人控制、调度对WLAN的通信实时性、可靠性、并发能力提出了前所未有的要求。
- 802.11v、802.11r等提高漫游速度的协议并非强制，相当比例的终端并不支持，这一问题导致终端在与前一BSS连接断开后且漫游前需进行全信道扫描，这对于连续的、延迟敏感的网络业务来说是灾难性的。
- 在智能仓储场景中，为了实现货物自动拣选和自动分拣，需要通过WLAN网络实现AGV (Automated Guided Vehicle) 终端位置、状态信息上报和运行控制指令的下发。针对这一场景，开启自动导航漫游优化功能，使WLAN网络将运行控制信息实时、可靠、正确地传递给目标设备。

无损漫游关键技术：高效无损扫描（1）

- 问题1：
  - 漫游及时性取决于扫描效率；
  - 全信道扫描时长无法承受（100 ms*13，甚至100 ms*24）。
- 优化方案：
  - 基于网络拓扑自动识别算法，AP通知终端只扫描邻居信道，扫描结果更及时、可靠。

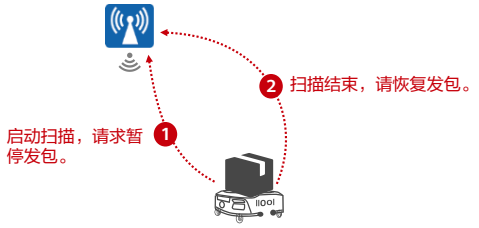


HUAWEI

- 针对智能仓储AGV终端漫游场景，华为从下面几点来实现无损漫游；
- 华为无损漫游技术从实际的网络拓扑来提高终端的扫描效率，根据网络拓扑选择合适的邻居信道，用以向终端传递所需扫描的信道集。扫描结果将更及时可靠，极大的提高终端扫描效率；
- 另外在终端切信道扫描前，终端会告知AP，AP则将报文缓存、延迟发出，这样可以保证在终端扫描过程中可以做到零丢包。

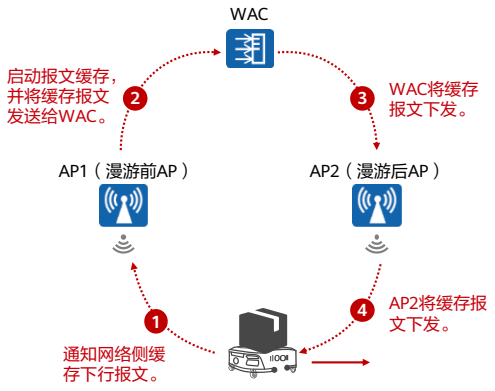
无损漫游关键技术：高效无损扫描（2）

- 问题2：
  - AGV终端切换信道扫描的过程中，AP继续下发报文会导致丢包；
- 优化方案：
  - 终端切信道扫描前，终端会告知AP，AP则将报文缓存、延迟发出，终端扫描结束后再通知AP恢复发包，这样可以保证在终端扫描过程中可以做到零丢包。



无损漫游关键技术：无损漫游切换

- 问题：
  - AGV终端漫游后，漫游前AP未发送报文会被丢弃。
- 优化方案：
  - AGV终端启动漫游前通知网络侧缓存下行报文。
  - 网络侧启动报文缓存。
  - AGV终端漫游结束，网络侧下发缓存报文。



无损漫游关键技术：抗干扰增强

- 问题：
  - 当前AGV应用流量不大，但是对可靠性要求非常高。环境恶化会导致可靠性降低，从而影响AGV终端业务。
- 优化方案：
  - QoS优化：上下行的AGV业务报文优先级均提高至VO等级。
  - AGV VAP的AMC算法在环境恶化时需要降低发送速率，以提高抗干扰能力。

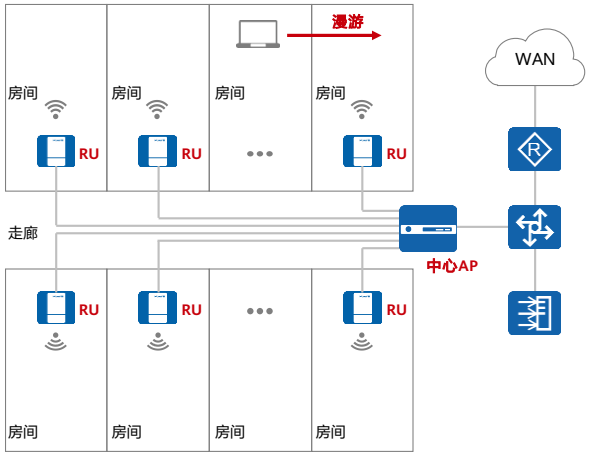
配置智能仓储场景下的漫游优化

- 使能自动导航漫游优化功能。

```
[WAC-wlan-view] vap-profile name profile-name
[WAC-wlan-vap-prof] autonavigation-roam-optimize  enable
```

- 配置注意事项：
  - 由于2.4G射频干扰较严重，建议在5G射频下使用自动导航漫游优化功能。
  - 自动导航漫游优化功能仅在转发模式为隧道转发时生效。

医疗场景 - 敏捷分布式SFN漫游



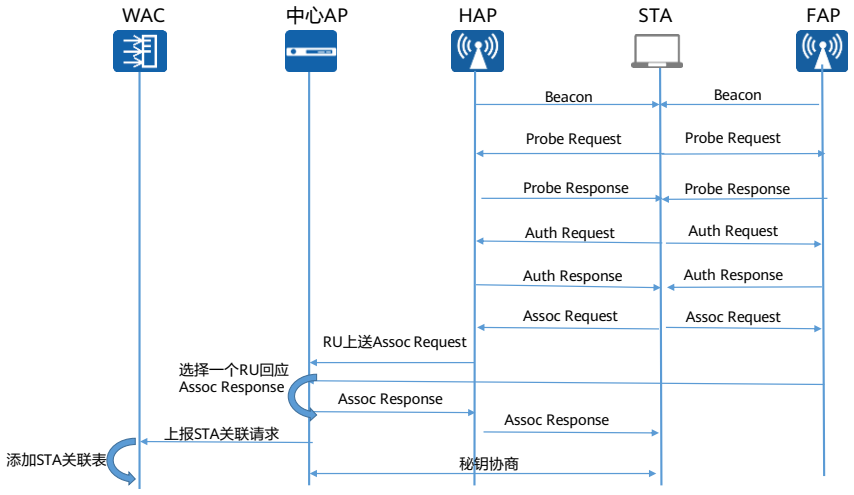
敏捷分布式SFN（Same Frequency Network）漫游功能。

敏捷分布式SFN漫游是指在敏捷分布式WLAN组网中，一个中心AP内的所有RU部署在相同工作信道上并使用公共BSSID和终端通信，终端在同一个SSID信号覆盖范围内自由移动时漫游无感知、业务不中断的漫游体验功能。

HUAWEI

- 在医疗场景中，由于医护人员的医疗手持终端不支持802.11k/802.11v/802.11r协议，因此在移动查房过程中通过手持医疗终端进行病房巡视、输液核对、生命体征录入等业务时终端漫游主动性较差，容易出现丢包或延时大的问题，导致需重新登录应用软件或重新扫码，上网业务被中断，严重影响医护人员的工作效率。
- 为了解决上述问题，华为推出了敏捷分布式SFN（Same Frequency Network）漫游功能。敏捷分布式SFN漫游是指在敏捷分布式WLAN组网中，一个中心AP内的所有RU部署在相同工作信道上并使用公共BSSID和终端通信，终端在同一个SSID信号覆盖范围内自由移动时漫游无感知、业务不中断的漫游体验功能。
- 相比传统的中心AP内漫游，敏捷分布式SFN漫游屏蔽了终端差异对漫游效果的影响，同时在漫游切换阶段省去了用户重关联、认证及密钥协商的过程，漫游切换平滑且速度快，并且大大降低了丢包概率。
- 典型应用场景可分为以下几种：医院仅部署内网供医护人员使用，仅一个射频的一个VAP上开启敏捷分布式SFN漫游。
- 医院同时部署内网和外网，内外网部署在不同的射频上，内网射频开启敏捷分布式SFN漫游，外网射频采用传统的中心AP内漫游。
- 医院同时部署内网和外网，内外网部署在同一个射频上，内网VAP开启敏捷分布式SFN漫游后，外网VAP自动开启敏捷分布式SFN漫游。

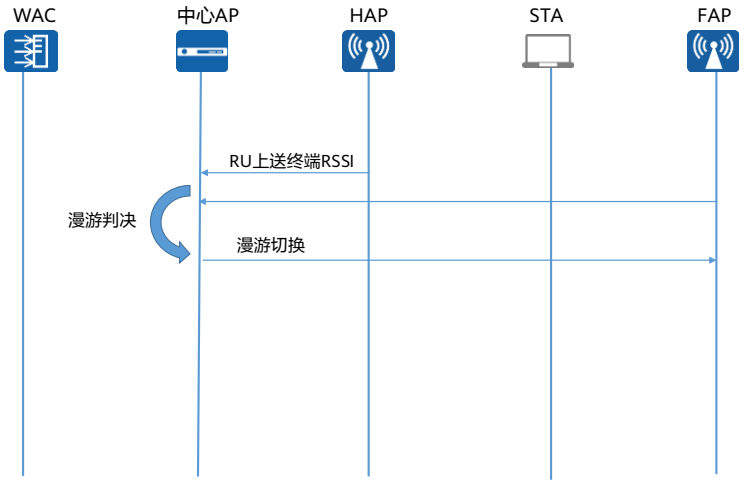
敏捷分布式SFN漫游实现机制 - 终端接入阶段



HUAWEI

- STA接入阶段：
  - 所有RU采用中心AP根据MAC地址自动生成的公共BSSID向STA广播发送Beacon帧。
  - STA发送Probe Request，所有RU收到Probe Request后均用公共BSSID回复Probe Response。
  - STA发送Auth Request，所有RU收到Auth Request后均用公共BSSID回复Auth Response。
  - STA发起Assoc Request，所有RU收到该Assoc Request后均上送至中心AP处理，并上报STA的SNR给中心AP。
  - 中心AP选定一个SNR最优的RU回复Assoc Response，同时在一定时间内再次收到其他RU上报的Assoc Request报文做丢弃处理。后续只有被选定的RU和STA通信。
  - 中心AP向WAC上报STA关联请求，WAC将STA信息添加到用户关联表。
  - 中心AP、RU和STA进行单播和组播密钥协商。

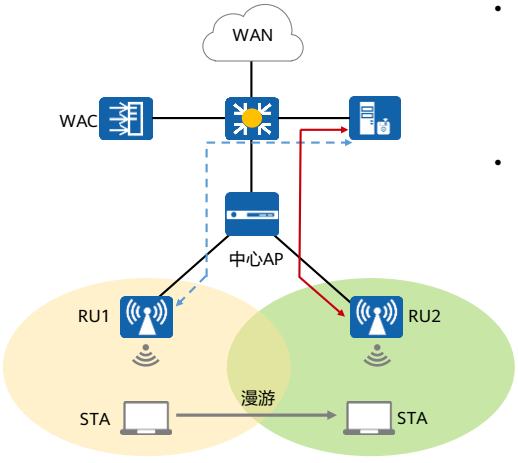
敏捷分布式SFN漫游实现机制 - 漫游切换阶段



HUAWEI

- 漫游切换阶段：
  - HAP（首次关联的RU）周期性上报终端RSSI给中心AP，FAP（漫游后关联的RU）周期性上报邻居RSSI给中心AP。
  - 中心AP通过漫游判断算法选择一个最优的RU作为漫游切换的FAP，然后同步终端信息给FAP。中心AP周期性依次判断以下三个切换条件是否满足，当符合任意一个切换条件时，即可以发生漫游切换，如果有多个RU同时满足以下三个条件，则选择信号强度最强的RU进行漫游切换。
    - 终端RSSI累积变化值达到指定阈值。
    - 周边RU信号强度优于当前RU信号强度的次数达到配置的值。
    - 周边RU相比当前RU的信号强度差值达到配置的差值。

敏捷分布式SFN内网数据报文处理流程



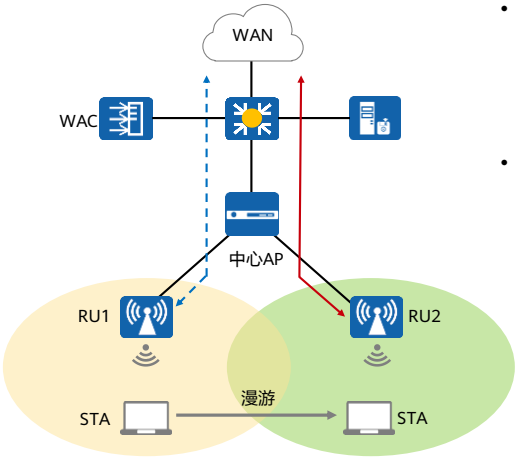
- 漫游前：
  - STA发送业务报文给RU1。
  - RU1接收到STA发送的业务报文并发送给中心AP。
  - 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络。
- 漫游后：
  - STA发送业务报文给RU2。
  - RU2接收到STA发送的业务报文并发送给中心AP。
  - 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络。

漫游前数据报文走向

漫游后数据报文走向

STA网关

敏捷分布式SFN外网数据报文处理流程



- 漫游前：
  - STA发送业务报文给RU1；
  - RU1接收到STA发送的业务报文并发送给中心AP；
  - 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络。
- 漫游后：
  - STA发送业务报文给RU2；
  - RU2接收到STA发送的业务报文并发送给中心AP；
  - 中心AP接收到STA发送的业务报文通过用户网关发送给上层网络。

漫游前数据报文走向

漫游后数据报文走向

STA网关

配置敏捷分布式SFN漫游

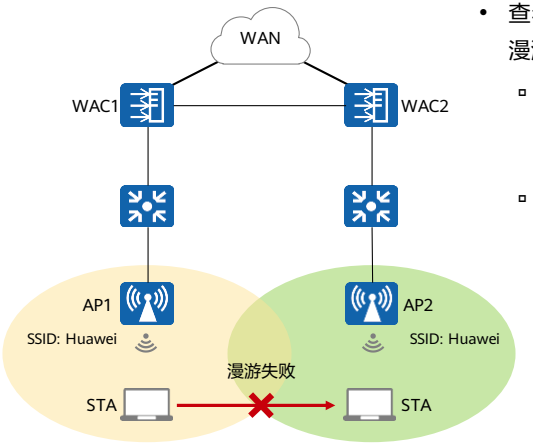
- 开启敏捷分布式SFN漫游功能。

```
[WAC-wlan-view] vap-profile name profile-name
[WAC-wlan-vap-prof] sfn-roam enable
```

- 配置注意事项：
  - 如果2.4G或5G射频同时开启敏捷分布式SFN漫游，则建议使用不同的SSID，否则可能导致STA切换射频，影响用户体验。自动导航漫游优化功能仅在转发模式为隧道转发时生效。
  - 一个射频上只能有一个VAP使能敏捷分布式SFN漫游功能。
  - 开启敏捷分布式SFN漫游功能的射频上不能再配置信道扫描、信道调优和智能漫游。
  - 敏捷分布式SFN漫游不支持AP个性化配置，只能基于AP组配置。

目录

STA漫游失败故障定位思路



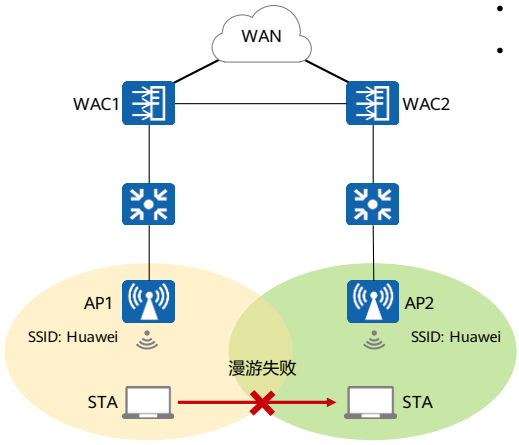
- 查看终端上线和下线失败原因，判断终端是接入失败还是漫游失败。
  - 在WAC上执行命令display station online-fail-record sta-mac查看终端上线失败原因；在WAC上执行命令display station offline-record sta-mac查看终端下线记录。
  - 如果用户上线失败原因中记录的时间点和用户漫游失败的时间点相同，请让STA直接在漫游后的AP上线，如果上线失败，请参照STA关联失败故障处理流程；如果用户下线原因中记录的时间点和用户漫游失败的时间点相同，则是漫游检查失败。

STA漫游失败故障定位

- 用户漫游失败的常见原因包括：
  - 安全模板配置不一致。
  - 用户发生三层漫游，但设备配置了禁止三层漫游。
  - 如果WAC间漫游，可能WAC间漫游配置不正确或者业务VLAN未创建。
  - 如果是漫游掉线，可能AP的信号覆盖不连续，或者功率配置不合理。
  - 空口存在来自友商的相同SSID的信号。
  - 智能漫游弱信号踢用户下线阈值不合理。
  - 是否漫游前后属于不同子网，却配置成了二层漫游（VLAN相同）。

- 如果用户下线原因中记录的时间点和用户漫游失败的时间点相同，则是漫游检查失败；漫游失败检查的常见原因包括以上几点。

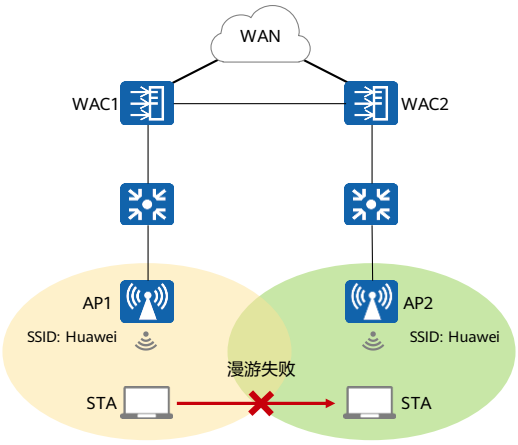
STA漫游失败故障定位 - 检查安全模板配置



- 检查漫游前后的AP上安全模板配置是否一致。
- 进入安全模板视图重新配置密钥，保证漫游前后AP的安全模板配置一致。

```
[WAC-wlan-view] security-profile name default
[WAC-wlan-sec-prof-default] security wpa2 psk pass-phrase huawei123 aes
```

STA漫游失败故障定位 - 检查三层漫游配置



检查是否配置了禁止三层漫游

1. 判断当前是二层漫游还是三层漫游。

```
[WAC] display vap-profile name default
--------------------------------------------------------------------------------
Service VLAN ID              : 101
Service VLAN Pool            : -
Permit VLAN ID               : -
Auto off service switch      : disable
Auto off starttime           : -
Auto off endtime             : -
STA access mode              : disable
STA blacklist profile        :
STA whitelist profile        :
Home agent                   : ap
VLAN mobility group          : 2
Layer3 roam                  : enable
--------------------------------------------------------------------------------
```

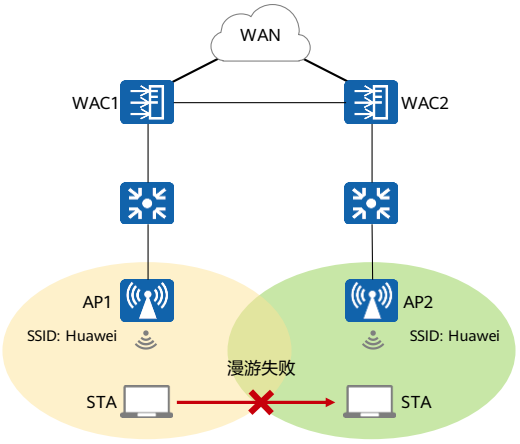
2. 对于三层漫游，检查VAP模板下是否开启了禁止三层漫游。

```
[WAC-wlan-view] vap-profile name default
[WAC-wlan-vap-prof-default] display this
#
 layer3-roam disable
```


HUAWEI

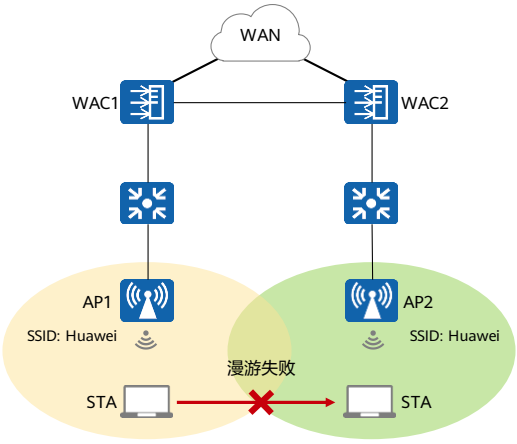
- 进入漫游前后AP所属的AP组下绑定的VAP模板，检查VAP模板下是否开启了禁止三层漫游。
- 如果用户是三层漫游，且配置了禁止三层漫游，则会导致漫游失败。
- 根据STA是否在同一个子网内漫游，可以将漫游分为二层漫游和三层漫游。
  - 如果两个子网的VLAN ID不同，那么这两个子网是处于不同的网段，STA在这两个子网间漫游是属于三层漫游。
  - 网络中有时候会出现以下情况：两个子网的VLAN ID相同，但是这两个子网又属于不同的子网。此时为了避免系统仅仅依据VLAN ID将用户在两个子网间的漫游误判为二层漫游，需要通过漫游域来确定设备是否在同一个子网内，只有当VLAN相同且漫游域也相同的时候才是二层漫游，否则是三层漫游。
  - 进入漫游前后AP所属的AP组下绑定的VAP模板，检查VAP模板下是否开启了禁止三层漫游。如果用户是三层漫游，且配置了禁止三层漫游，则会导致漫游失败。

STA漫游失败故障定位 - 检查漫游前后VLAN配置是否正确



- 检查漫游前后VLAN配置是否正确。
  - 漫游前后的业务VLAN需要正确创建，尤其对于WAC间漫游，参与漫游的所有WAC上都需要创建漫游前和漫游后的业务VLAN；
  - 如果是直接转发，漫游后AP到漫游前AP这条链路上所有的端口必须放通业务VLAN，且WAC上的业务VLAN必须创建，保证漫游后用户的数据报文转发正常。

STA漫游失败故障定位 - 检查漫游组状态是否正常



如果是WAC间漫游，则检查漫游组状态是否正常。

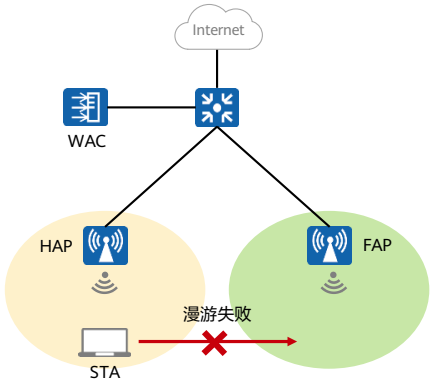
```
<WAC> display mobility-group name roam
--------------------------------------------------------------------------------
AC ID    State       IP address
--------------------------------------------------------------------------------
1        normal      192.168.10.3
2        fault       192.168.10.4
--------------------------------------------------------------------------------
```

如果漫游组成员状态是“fault”，查看当前漫游组的配置信息是否正确。

```
[WAC] mobility-group name mobility
[WAC-mc-mg-mobility] display this
#
  member ip-address 192.168.10.1
  member ip-address 192.168.10.2
```

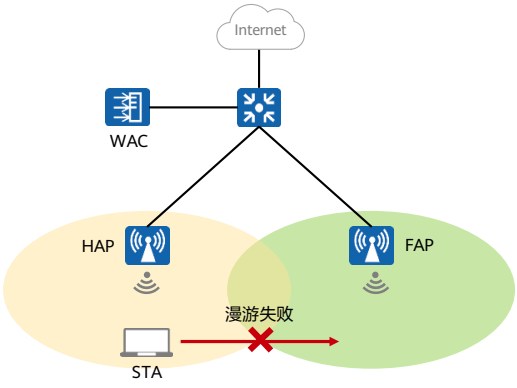
如果配置正确，执行命令ping检查WAC间网络是否互通。

检查信号覆盖是否连续



- 检查漫游前后两个AP的信号覆盖是否连续。
  - 漫游前后两个AP的距离如果太远，则用户在走动过程中可能会因为信号覆盖不连续而先离线再上线，导致漫游失败；
  - 使用CloudCampus APP等常用的工具来检查AP的信号覆盖情况；
  - 如果确认AP之间的信号不连续，可以通过增加AP发射功率或增加AP来满足信号连续覆盖。

STA漫游失败故障定位 - 检查功率配置是否合理



检查功率配置是否合理。

```
<WAC> display radio ap-id 25
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
-------------------------------------------------------------------------------
AP ID Name     RfID Band Type   Status CH/BW    CE/ME   STA  CU
-------------------------------------------------------------------------------
25    ap-yuan  0    2.4G bgn    on     8/20M    29/29   1    21%
25    ap-yuan  1    5G   an11ac on     165/20M  23/30   0    4%
-------------------------------------------------------------------------------
Total:2
```


HUAWEI

- 如果功率配置过小，容易造成信号覆盖盲点。此时，需要在射频视图下执行eirp命令增大发射功率。
- 如果功率配置过大（如满功率），容易导致终端关联远端AP而出现漫游不灵敏。此时，需要在射频视图下执行eirp命令适当降低发射功率或者配置智能漫游功能。

STA漫游失败故障定位 - 网络环境中是否存在同名的非法SSID

- 检查WLAN网络环境中是否存在同名的非法SSID。

```
<WAC> display ap neighbor ap-id 0
Radio: Radio ID of AP
......
Uncontrol AP:
```

Radio	BSSID	Channel	RSSI(dBm)	Last Update Time	SSID
0	d0d0-4b22-df00	1	-50	2019-08-24/15:32:18	
0	c4b8-b4f0-6980	1	-44	2019-08-24/15:31:06	
0	10c1-72dd-12e0	11	-41	2019-08-24/15:28:27	roam
0	9c50-ee45-6240	1	-54	2019-08-24/15:32:06	

Total: 4

- 查看Uncontrol AP中是否存在同名的非法SSID。如果存在则需要关闭此非法SSID信号。

STA漫游失败故障定位 - 检查问题是否解决

- 将终端在两个AP间移动，执行命令display station roam-track查看终端的漫游轨迹，如果漫游轨迹显示正常则问题解决，如果仍然漫游失败，请收集漫游时系统的日志和诊断日志并收集如下故障诊断信息，然后寻求技术支持。

命令	使用说明
[WAC] **trace enable** [WAC] **trace object mac-address**	查看STA上线或者漫游全流程跟踪信息。
[WAC] **display station online-fail-record** [WAC] **display station offline-record**	查看用户上线失败或下线原因。
[WAC-diagnose] **display wlan wsta block-sta-number all** [WAC-diagnose] **display wlan wsta online-statistics** [WAC-diagnose] **display wlan wsta online-fail-record by-mac** [WAC-diagnose] **display wlan wsta peak-statistics**	查看用户上线失败或下线原因码。
[WAC-diagnose] **display diagnostic-information**	获取系统的一键诊断信息，该信息包括版本、补丁版本、当前配置和已保存配置 、异常、部分日志等。

思考题

1. 无线终端漫游时，是否需要重新认证或者重新登录?
2. 是否所有终端都支持802.11r漫游?
3. 如何判断终端是不是三层漫游?

HUAWEI

- 参考答案：
  - 无线终端漫游时，并不需要重新认证或者重新登录。
  - 并不是所有的终端都支持11r漫游，很多传统终端都不支持11r漫游。
  - 如果两个子网的VLAN ID不同，那么这两个子网是处于不同的网段，STA在这两个子网间漫游是属于三层漫游。如果两个子网的VLAN ID相同但是漫游域不同，则也属于三层漫游。

本章总结

- 本章介绍了WLAN漫游的网络架构，漫游对业务的影响；通过11r漫游、智能漫游，敏捷分布式SFN漫游等漫游优化手段，使得漫游切换平滑且速度快，并且大大降低了丢包概率；从而实现漫游过程中业务数据流低延时，用户不会感知业务中断，提高用户上网体验。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN射频资源管理

HUAWEI

前言

- 射频资源管理能够自动检查周边无线环境、动态调整信道和发射功率等射频资源、智能均衡用户接入，从而调整无线信号覆盖范围，降低射频信号干扰，使无线网络能够快速适应无线环境变化。
- 通过配置射频资源管理，可以动态调整射频资源以适应无线信号环境的变化，确保用户接入无线网络的服务质量，保持最优的射频资源状态，提高用户上网体验。
- 本课程主要介绍WLAN射频调优、WLAN负载均衡、WLAN抗干扰、WLAN QoS、VIP用户体验保障。

目标

- 学完本课程后，您将能够：
  - 描述常见的WLAN射频调优技术
  - 描述常见的WLAN负载均衡技术
  - 描述常见的WLAN抗干扰技术
  - 描述WLAN QoS的工作原理
  - 描述VIP用户体验保障机制

目录

射频调优概述

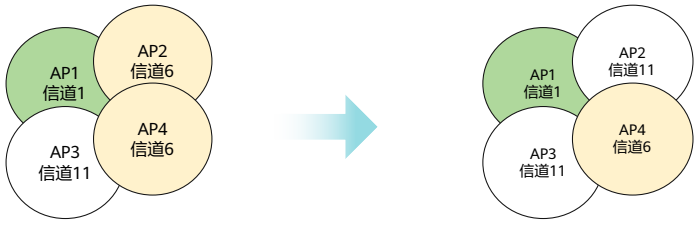
- WLAN网络中，AP的工作状态会受到周围环境的影响。例如，当相邻AP的工作信道存在重叠频段时，某个AP的功率过大会对相邻AP造成信号干扰。通过射频调优功能，动态调整AP的信道、功率和频段等，可以使同一WAC管理的各AP保证覆盖的同时又能尽量避免干扰，保证AP工作在最佳状态。

当网络规模过大时，手动进行射频资源调优时，工作量大，建议使用自动调优方式。

- 当网络中接入新的AP或AP退服，外部无线环境恶化都会触发无线调优。

动态调整信道

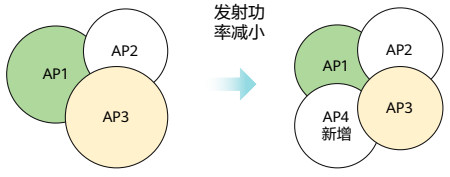
- 信道调整前，AP2和AP4都使用信道6，存在信号干扰；信道调整后，AP2切换到信道11，干扰消除，相邻AP工作在非重叠信道。
- 通过信道调整，可以保证每个AP能够分配到最优的信道，尽可能地减少和避免相邻或相同信道的干扰，保证网络的可靠传输。



信道调整前　　信道调整后

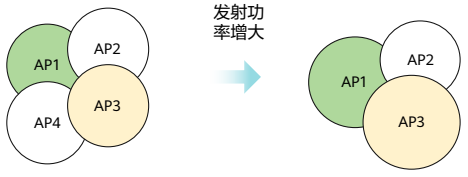
动态调整功率

功率减小



- 在增加邻居AP时，相应AP的功率会减小。
- 当增加AP4后，在保证满足覆盖需求的原则下，尽量减少干扰，通过功率调整功能，每个AP的发射功率将会减小。

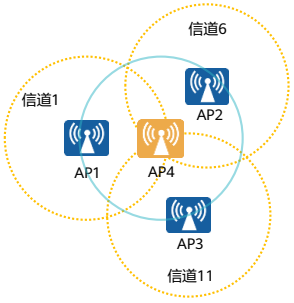
功率增大



- 在减少邻居AP时，相应AP的功率会增加。
- 当AP4离线后，由于当前WLAN无法满足覆盖需求，因此通过功率调整功能，相应AP的发射功率将会有所增加。

动态调整频段

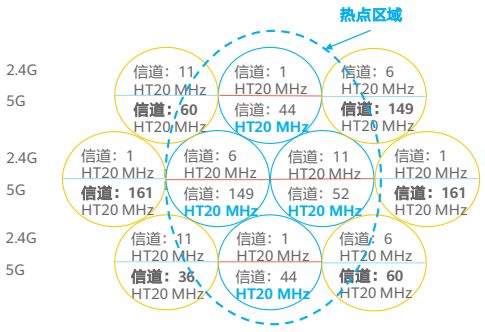
- 动态调整频段：能够自动识别2.4 GHz冗余射频，并自动切换或关闭冗余射频，降低了2.4 GHz同频干扰，增加了系统容量。如图所示，4个AP均工作在2.4 GHz频段。
- 无论AP4工作在哪个信道都会与邻居AP存在同信道或者邻信道干扰，且AP4所覆盖的区域完全可以由其他三个AP进行覆盖。AP4为该WLAN网络中的冗余AP。



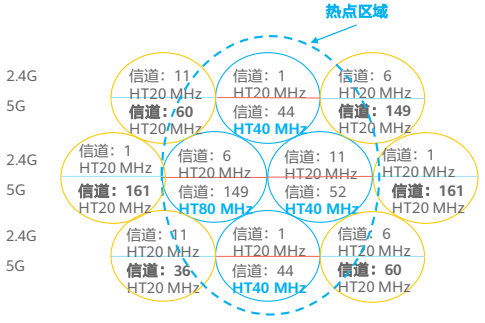
- 对于冗余射频，采用如下处理策略：
  - 切换为5 GHz：如果5 GHz可用信道比较多且该冗余射频支持切换到5 GHz，可以切换为5 GHz来增加5 GHz射频的最大容量。
  - 切换为monitor：如果5 GHz信道资源使用已经饱和，可以切换为monitor，专用于扫描类业务。
  - 关闭射频：关闭冗余射频不会产生覆盖问题，同时有利于降低同频干扰。

动态调整频宽

- 对于室内非高密部署场景（AP间距10 m~15 m）的5 GHz网络，自适应地切换信道与带宽、提升网络吞吐量，同时保障核心业务质量。



5 GHz配置为HT20 MHz模式，限制了用户带宽。



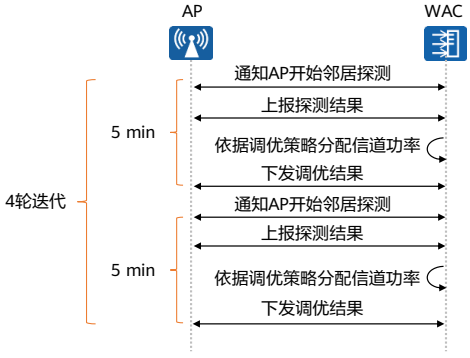
根据算法自动增加5 GHz频宽，提升用户带宽。

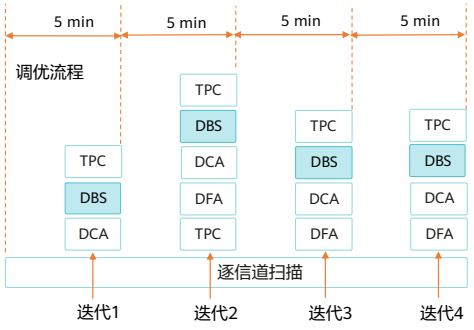
HUAWEI

- 对于室内高密场景下的5G网络，因为调整频宽不会导致额外的干扰，所以DBS (Dynamic Bandwidth Selection)算法会根据信道的分配将热点区域的频宽向上调整为40 MHz或80 MHz，提升网络吞吐量。
- 当其他AP的信道和增加频宽后的热点区域信道发生干扰后，根据DBS算法，优先保证网络无干扰，减少热点区域的频宽。

射频调优原理

- 射频调优的实现主要包括四个过程：采集、分析、决策、执行。
- 在这几个过程中涉及五个关键技术点：邻居关系、DCA (Dynamic Channel Allocation)算法、TPC (Transmit Power Control)、 DBS (Dynamic Bandwidth Selection)和DFA (Dynamic Frequency Assignment)算法。





HUAWEI

- 使能全局调优后，WAC通知各个AP开始周期性的进行邻居探测。
- AP进行周期性的邻居探测并将探测结果上报WAC。
- WAC等待所有AP都上报邻居信息后开始运行全局调优算法为AP分配信道、带宽和功率。
  - 全局调优算法主要包括动态信道调整算法DCA (Dynamic Channel Allocation)、动态带宽选择算法DBS (Dynamic Bandwidth Selection)、动态频段调整算法DFA (Dynamic Frequency Assignment)和发送功率控制算法TPC (Transmit Power Control)。
- WAC向AP下发调优结果。如果是第一次启动全局调优，WAC等待一段时间后根据新收集到的邻居信息再次启动全局调优，如此连续调优多次，可以使得调优结果尽快逼近最佳并稳定下来。
- 每轮调优持续时间5min，一次典型的自动调优需完成四轮共计20分钟。

邻居关系 - 邻居探测

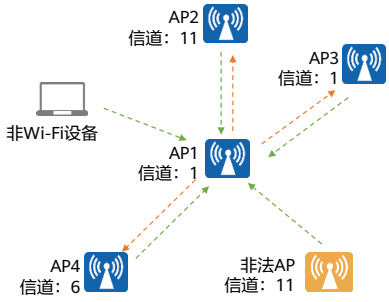
- 主动探测：主动发送邻居探测，目的是让周边邻居AP感知本AP的存在。
- 被动探测：被动接收邻居信息，目的是感知周边邻居AP的存在。

HUAWEI

- 邻居探测的目的是让周边AP感知本AP的存在或者本AP感知周边AP的存在。这种探测分为两种方式：主动探测与被动探测。
  - 主动探测：主动发送邻居探测，目的是让周边邻居AP感知本AP的存在。AP周期性（默认一分钟为周期T0）地在不同信道发送带有特定组播地址的probe request，并进行多次发送。为防止并发导致无法接收邻居消息，在发送周期结束时增 加一个随机数时间延时为接收预留时间。为防止大量AP组网的场景下，可能出现探测冲突的情况，在WAC上设计了一个补救机制，如果A收到B，而B没有收到A，会将A补到B的探测结果中。
  - 被动探测：被动接收邻居信息，目的是感知周边邻居AP的存在。被动探测主要用于收集合法AP实际的干扰，非法AP干扰探测，和非Wi-Fi设备干扰探测等。

邻居关系 - 邻居信息收集

- 邻居信息收集包含：邻居关系、邻居干扰、邻居负载。



主动探测

AP以最大发射功率在不同信道（比如1、6、11）轮询发送Probe Request请求，目的地址为特定组播地址01:25:9e:ee:ee:ee。

被动探测

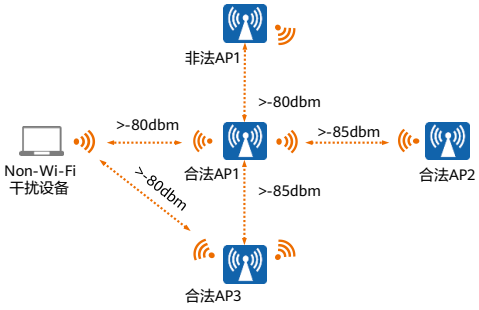
AP在不同信道上轮询收集消息，消息包括Beacon、Data、Probe Request、 Probe Response等，干扰强度的大小根据消息中带有的RSSI进行加权计算。

HUAWEI

- 邻居信息收集主要收集每个AP的邻居，负载以及干扰，这些作为算法的输入进行调优运算。
- 合法AP：
  - 邻居关系收集： 主动探测AP以最大发射功率在不同信道（比如，1、6、11）轮询发送Probe Request请求，被动探测AP在与主动探测AP相同的信道上收集Probe Request请求 信息，这种专门用于邻居探测请求的消息使用特别的组播地址： 01:25:9e:ee:ee:ee
  - 邻居干扰收集： 但实际上，合法邻居AP并不一定是一最大功率发射，也就是说AP间的干扰并不一定总是这么大，因此需要收集合法AP实际的干扰大小。实际干扰的收集是主动探测AP在不同信道上轮询收集消息，消息包括Beacon、Data、Probe Request、 Probe Response等，干扰强度的大小根据消息中带有的RSSI进行加权计算。
  - 邻居负载收集：对于合法邻居除了收集邻居关系，干扰大小之外，还需要收集每个合法AP的负载情况。这里的负载通过合法AP本身来收集，包括AP上行和下行的吞吐率。

邻居关系 - 邻居关系的上报与建立

- 根据AP上报的探测结果，WAC上可以描述出AP与周边设备的邻居关系，以及整个WAC下所有射频设备（含合法AP、非法AP以及非Wi-Fi干扰设备）的邻居关系。



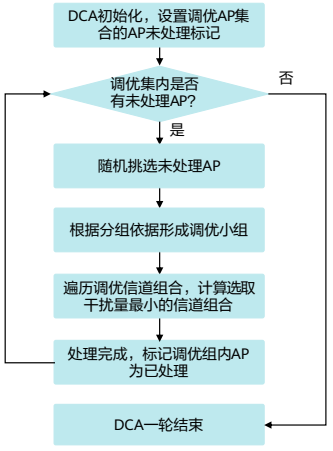
合法AP				
Radio	AP ID	AP name	Channel	Received RSSI(dbm)
0	2	AP2	11	-33
0	3	AP3	1	-45

非法AP				
Radio	BSSID	Channel	RSRP(dBm)	SSID
0	0020-1306-0680	1	-79	TEST

HUAWEI

- 为防止上报的数据过大，仅上报信号强度大于-85 dBm的合法邻居和信号强度大于-80 dBm的非法邻居。
- 对于邻居关系可以抽象成节点和边表示：
  - 节点：包括合法AP、还包括Non-Wi-Fi干扰设备、非法AP。
  - 边： 表示两个节点的邻居信息，除了节点之间的干扰强度，还包括负载等其他附属属性。同时，边是有方向性的，例如非Wi-Fi设备影响某个AP的干扰强度。

信道调优算法（DCA）- 全局信道调优



- DCA一次迭代过程如图所示
  - 在调优集内随机挑选未处理AP，根据分组依据形成调优小组。
  - 为待分配信道的AP调优组预选择新的信道组合，并比较该信道组合与原有信道组合，如果使用该信道后AP的干扰量更小，则使用该信道替换原有信道，否则为AP维持当前信道，并计算下一组信道组合下的干扰量，以此类推，选取干扰最小的信道组合。
  - 处理完成后标记该调优小组内AP为已处理，直至调优集内所有AP均被处理。
- 调优小组分组依据
  - Leader选举机制：随机选取。
  - 根据AP的邻居信息RSSI进行排序。
  - 分组大小（由信道决定）。

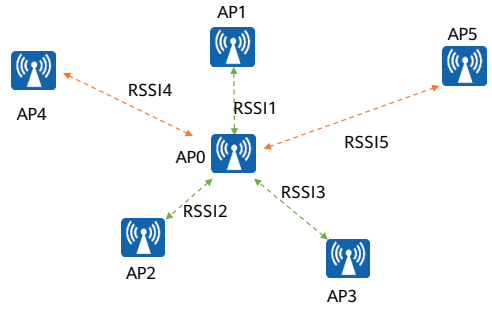
信道个数	1	2	3	4	5	>=6
直接邻居	0	2	3	3	2	0

信道调优算法（DCA）- 局部信道调优

- 局部信道调优的目标是在局部信号环境恶化时通过小范围内的信道和功率调整，使局部的信号环境达到最佳。
- 局部调优算法中基本的DCA和TPC算法与全局调优完全相同。
- 以下几个场景会触发局部调优：
  - AP上线、AP下线、非法AP干扰、无线环境恶化、非Wi-Fi设备干扰、手动触发局部调优。

功率调整算法（TPC）

- 随机选择AP进行功率调优，直到所有AP配置完成 。

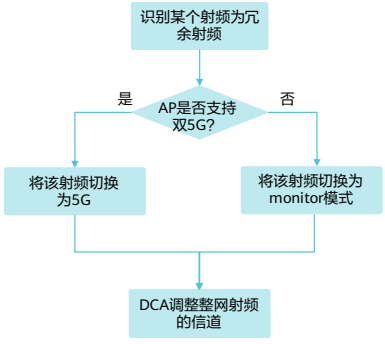


HUAWEI

- TPC (Transmit Power Control)算法，即发射功率控制算法，与DCA都属于自动调优的组成部分，但两个算法本身是独立的。TPC算法根据周围AP来确定本AP的覆盖边界，进而调整本AP的发射功率。TPC算法和DCA的信道分配结果无关，只取决于AP间距离。
- AP与AP1的距离近选择发射功率调整选择缓和策略，远则选择激进调整策略：
  - 缓和调整策略AP发送功率EIRP计算方法：
    - EIRP = TPC覆盖的阈值 + （ EIRP – RSSI1 ）+ min（ RSSI1 – RSSI2，RSSI2 – RSSI3 ）/2；
  - 激进调整策略AP发送功率EIRP计算方法：
    - EIRP = TPC覆盖的阈值 + max（ EIRP – RSSI1，0 ）+ min（ RSSI1 – RSSI2，5 ）+ min（ RSSI2 – RSSI3，5 ）。
- TPC覆盖的阈值：
  - 当开启射频调优时，对于AP的布放场景不同，AP布放距离不同或AP布放 高度不同，TPC的覆盖阈值不同，实际使用时需要根据AP的实际布放调整AP的TPC，以使TPC的结果能达到最优的覆盖效果。阈值越大，TPC调整的功率值会整体提高。
- 本案例中将该AP所有同频/异频的邻居AP的按RSSI从高到低排列，前三个邻居AP作为参考，此处标记为AP1，AP2，AP3。

- 以AP与最近的邻居AP1的距离远近（干扰大小）选择AP功率调整策略，根据AP1、AP2、AP3相邻两者之间差值及 TPC 覆盖的阈值计算该AP的调整功率。
- 与预设的TPC最大、最小功率值进行比较，限制调整功率范围，避免信号干扰或者无法满足射频覆盖。如果调整功率小于TPC最小功率，则设置TPC最小功率为调整功率；如果调整功率大于TPC最大功率，则设置TPC最大功率为调整功率；否则，调整功率不变。
- 与当地法规比较，如果调整功率大于法规规定最大功率，则以法规为准，反之调整功率不变。

频段调整算法（DFA）



DFA对于冗余射频的处理步骤

- 在此过程中，一旦漏洞检测机制检测到2.4G射频存在覆盖漏洞，切换后的5G射频会回切到2.4G射频。
- 如果WAC出现重启，AP上线时会携带WAC重启前的信道、功率、频段、射频开关等配置信息重新上线。如果AP长时间未上线，在上线后会重新进行冗余射频的判断和频段分配。
- 当关闭DFA功能时，冗余射频将恢复为原配置值。例如，被自动切换为5G或monitor状态的射频将恢复为2.4G。

- 冗余射频：即功率调整后，依然对周围AP造成干扰的射频。

频宽调整算法（DBS）

- DBS算法基本原理
  - 根据能够组成80 MHz/40 MHz信道的能力，对可用的5 GHz信道进行分组。
  - 按拓扑距离对AP进行分配顺序排序。
  - 根据干扰指数、带宽满足度、信道隔离度、信道复用指数等因素，分配主信道。
  - 各AP基于20 MHz信道，按分配顺序升级为40 MHz和80 MHz。
- 算法触发条件

被触发的算法	触发类型	触发条件描述	被触发的操作
DBS算法	事件触发	算法启动时间	AP干扰测量，可用信道分组，射频信道带宽分配
DBS算法	周期触发，周期P	周期触发P到达	AP干扰测量，可用信道分组，射频信道带宽分配

- 邻居探测的目的是让周边AP感知本AP的存在或者本AP感知周边AP的存在。这种探测分为两种方式：主动探测与被动探测。
  - 主动探测：主动发送邻居探测，目的是让周边邻居AP感知本AP的存在。AP周期性（默认一分钟为周期T0）地在不同信道发送带有特定组播地址的probe request， 并进行多次发送。为防止并发导致无法接收邻居消息，在发送周期结束时增 加一个随机数时间延时为接收预留时间。为防止大量AP组网的场景下，可能 出现探测冲突的情况，在WAC上设计了一个补救机制，如果A收到B，而B没有收到A，会将A补到B的探测结果中。
  - 被动探测：被动接收邻居信息，目的是感知周边邻居AP的存在。被动探测主要用于收集合法AP实际的干扰，非法AP干扰探测，和非Wi-Fi设备干扰探测等。

AI加持的智能无线射频调优

场景1：人工调优

约**20%**客户会选择手工规划信道等，但面临的挑战：

手工规划不是最优

无法实时感知

网络环境复杂，干扰变化大

实时仿真反馈

结合**环境变化实时反馈**，提供预测、仿真工具，驱动网络优化。

场景2：自动调优

约**80%**会采用设备自动调优，但面临的挑战：

均衡调优未考虑负载

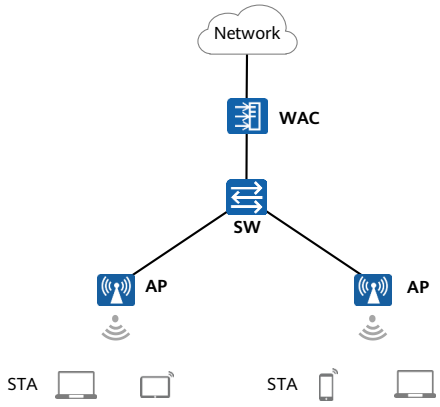
仅感知当前状态

无法感知历史负载与干扰

预测性调优

基于大数据+AI ，提供**业务权重**的权衡调优能力。

WLAN调优关键配置思路



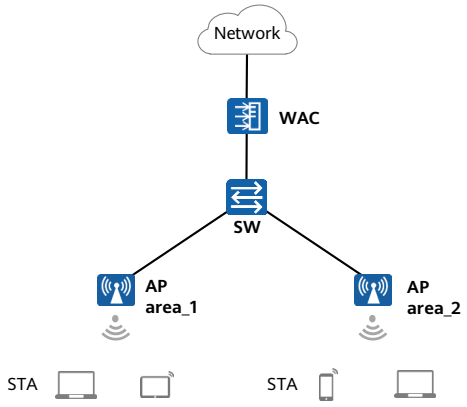
配置思路

- 使能信道自动选择功能和发送功率自动选择功能。
- 创建空口扫描模板，并配置扫描信道集合、扫描间隔时间和扫描持续时间。
- 创建并引用射频模板。
- 配置射频调优模式为手动调优，并手动触发射频调优。
- 检查配置结果。

HUAWEI

- 射频调优功能不适用于AP相互无法感知的场景，例如：AP使用定向天线、AP相隔较远或者AP间被阻隔等导致无法相互感知的情况。
- 射频调优功能不适用于高密场景、WDS/Mesh回传场景、轨交场景和室外定向天线的覆盖场景。
- 射频的工作模式为监控模式时，此射频不参与调优。

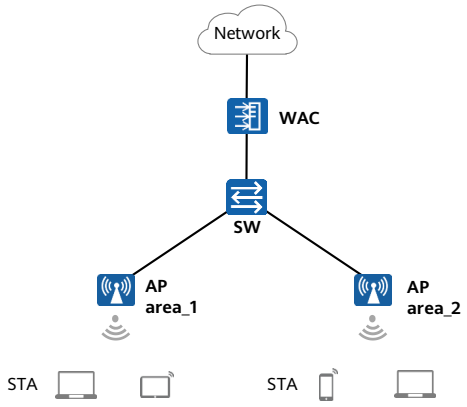
WLAN调优关键配置举例（1）



使能信道自动选择功能和发送功率自动选择功能。缺省情况下，信道自动选择功能和发送功率自动选择功能都已经使能。

```
[WAC] wlan
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] radio 0
[WAC-wlan-group-radio-ap-group1/0] calibrate auto-channel-select enable
[WAC-wlan-group-radio-ap-group1/0] calibrate auto-txpower-select enable
[WAC-wlan-group-radio-ap-group1/0] quit
[WAC-wlan-ap-group-ap-group1] radio 1
[WAC-wlan-group-radio-ap-group1/1] calibrate auto-channel-select enable
[WAC-wlan-group-radio-ap-group1/1] calibrate auto-txpower-select enable
```

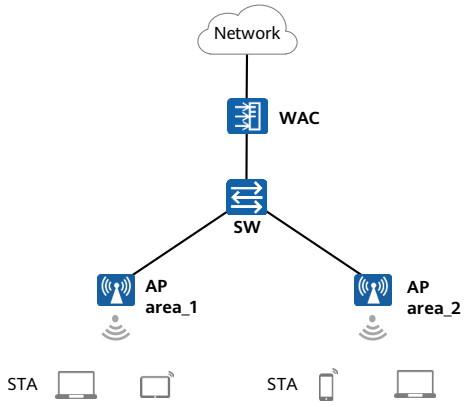
WLAN调优关键配置举例（2）



创建空口扫描模板“wlan-airscan”，并配置扫描信道集合、扫描间隔时间和扫描持续时间。缺省情况下，空口扫描信道集合为AP对应国家码支持的所有信道。

```
[WAC-wlan-view] air-scan-profile name wlan-airscan
[WAC-wlan-air-scan-prof-wlan-airscan] scan-channel-set country-channel
[WAC-wlan-air-scan-prof-wlan-airscan] scan-period 80
[WAC-wlan-air-scan-prof-wlan-airscan] scan-interval 80000
```

WLAN调优关键配置举例（3）



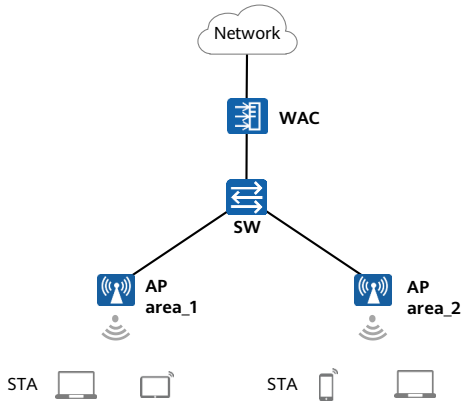
创建2G射频模板“wlan-radio2g”，并在该模板下引用空口扫描模板“wlan-airscan”。

```
[WAC-wlan-view] radio-2g-profile name wlan-radio2g
[WAC-wlan-radio-2g-prof-wlan-radio2g] air-scan-profile wlan-airscan
```

创建5G射频模板“wlan-radio5g”，并在该模板下引用空口扫描模板“wlan-airscan”。

```
[WAC-wlan-view] radio-5g-profile name wlan-radio5g
[WAC-wlan-radio-5g-prof-wlan-radio5g] air-scan-profile wlan-airscan
```

WLAN调优关键配置举例（4）



在名为“ap-group1”的AP组下引用5G射频模板“wlan-radio5g”和2G射频模板“wlan-radio2g”。

[WAC-wlan-view] **ap-group name** *ap-group1*
[WAC-wlan-ap-group-ap-group1] **radio-5g-profile** *wlan-radio5g* **radio** *1*
Warning: This action may cause service interruption. Continue?[Y/N]**y**
[WAC-wlan-ap-group-ap-group1] **radio-2g-profile** *wlan-radio2g* **radio** *0*
Warning: This action may cause service interruption. Continue?[Y/N]**y**

配置射频调优模式为手动调优，并手动触发射频调优。缺省情况下，射频调优的模式为自动模式。

[WAC-wlan-view] **calibrate enable manual**
[WAC-wlan-view] **calibrate manual startup** Warning: The operation may cause business interruption, continue?[y/n]:**y**

WLAN调优关键配置举例 - 检查配置结果

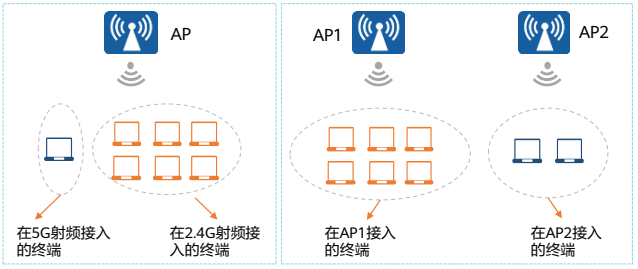
在AC上执行**display radio all**命令，查看射频调优效果。

```
[WAC-wlan-view] display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working Mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
--------------------------------------------------------------------------------------------------------------------
AP ID Name RfID      Band   Type   ST     CH/BW     CE/ME     STA   CU      WM
--------------------------------------------------------------------------------------------------------------------
1     area_2  0      2.4G   bgn    on     1/20M     28/28     1     10%     normal
1     area_2  1      5G     an     on     149/20M   29/29     0     15%     normal
0     area_1  0      2.4G   bgn    on     6/20M     28/28     1     15%     normal
0     area_1  1      5G     an     on     153/20M   29/29     0     49%     normal
--------------------------------------------------------------------------------------------------------------------
Total:4
```

目录

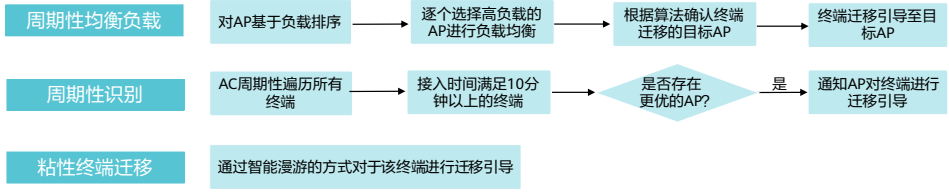
负载均衡概述

- 为了更好的满足人们的接入需求，更多、更密的AP被布放到体育场馆，餐厅等场所，但是有时候布放更多的AP并没有均匀分担接入的用户数；由于Wi-Fi空口采用的是基于竞争的多址接入方式，在同一个射频下接入的用户数越多，竞争开销越大，体现在空口吞吐率也会越低，用户体验也就越差。
- 针对负载不均衡的问题，设计了负载均衡特性。通过终端迁移、频谱导航和负载均衡将接入用户合理分配到不同的射频，减少空口竞争开销，提升空口吞吐率和用户体验。



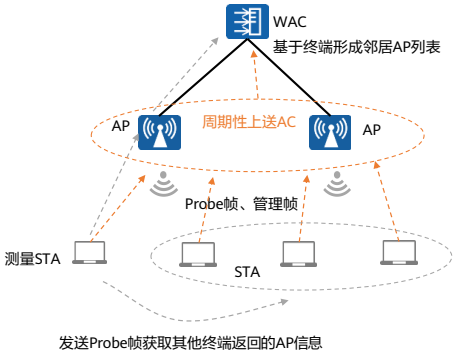
终端迁移引导技术

- 终端迁移功能综合了频谱导航、负载均衡和智能漫游等功能。
- 在终端关联前，AP确认终端是否具备双频能力，对支持双频的终端进行2.4 GHz频段的probe抑制，让终端优先接入5 GHz射频，参见频谱导航。
- 在终端关联后，通过目标AP选择算法，综合衡量终端的双频能力、AP的负载和信号质量，引导终端接入更优的AP。



终端邻居AP列表

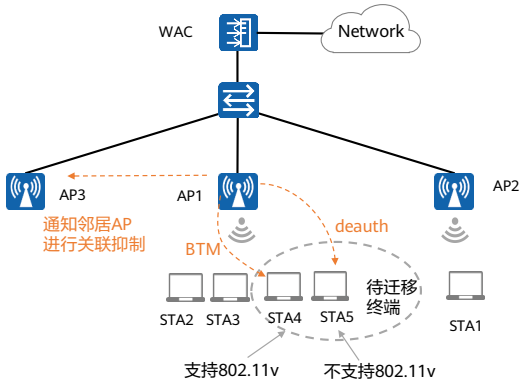
- 终端迁移功能中，在对终端迁移前需要确认终端迁移的目标AP，而目标AP是从终端的邻居AP中选择的。因此，WAC就需要收集、存储并维护终端的邻居AP信息列表。
- 终端的邻居AP信息的获取方式包括终端Probe收集和终端Beacon report测量。



- 终端Beacon report测量的类型分为三种模式：
  - Active：主动模式，测量终端向其他终端发送Probe帧后获取其他终端返回的AP信息。
  - Passive：被动模式，测量终端不向其他终端发送Probe帧，只获取其他终端的AP信息。
  - Beacon Table：Beacon表模式，直接获取其他终端上的AP信息。

终端迁移的方式

- 当终端满足了迁移的触发条件时，AP会对终端进行迁移引导。



- 对于支持802.11v协议的终端，AP优先采用BTM方式对终端进行迁移，如果终端不支持802.11v协议，则使用deauth方式进行迁移。
- AP在通过BTM或deauth消息通知终端迁移前，会通知邻居AP进行终端的关联抑制，抑制的方式包括probe抑制和auth抑制。
- 对于存在语音视频业务的终端，不做迁移处理。
- 终端新上线或发生漫游后，5分钟内不做迁移引导处理。

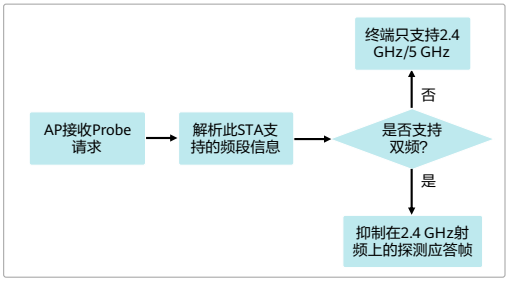
HUAWEI

- BTM方式：BSS Transition Management。

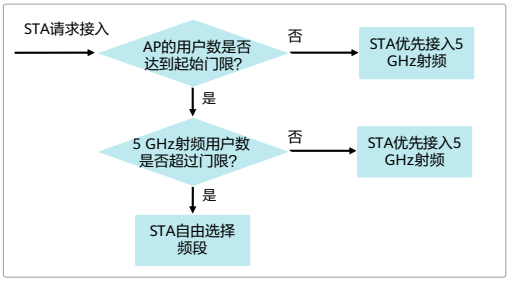
频谱导航概述

- 通过频谱导航功能，AP可以控制STA优先接入5 GHz，减少2.4 GHz频段上的负载和干扰，提升用户体验。
- 在同一个AP的不同频段(2.4 GHz & 5 GHz)的射频上实现负载均衡。

优先接入5 GHz频段



STA自由选择接入频段

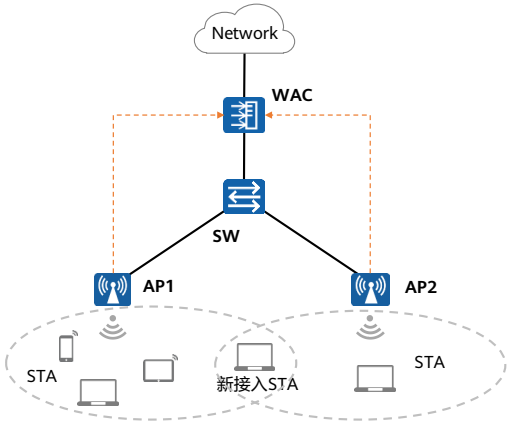


HUAWEI

- 优先接入5 GHz频段：
  - 在AP的接入用户数达到频谱导航5 GHz优先的起始门限前，优先接入5 GHz频段。
  - 当AP收到一个新STA (STA_1)发送的探测请求帧 (Probe Request)时，会从中解析此STA支持的频段信息。如果支持双频，则抑制在2.4 GHz射频上的探测应答帧 (Probe Response)，从而引导STA接入到5 GHz射频。
- STA自由选择接入频段：
  - 当AP的接入用户数达到频谱导航5 GHz优先的起始门限，并且AP的5 GHz射频接入用户数相对于总接入用户数占比超过占比门限，则由STA自由选择接入频段。

负载均衡概述

- 负载均衡适用于高密度无线网络环境中，用来有效保证STA的合理接入。
- 负载均衡的分类：
  - 静态负载均衡
  - 动态负载均衡（建议使用）

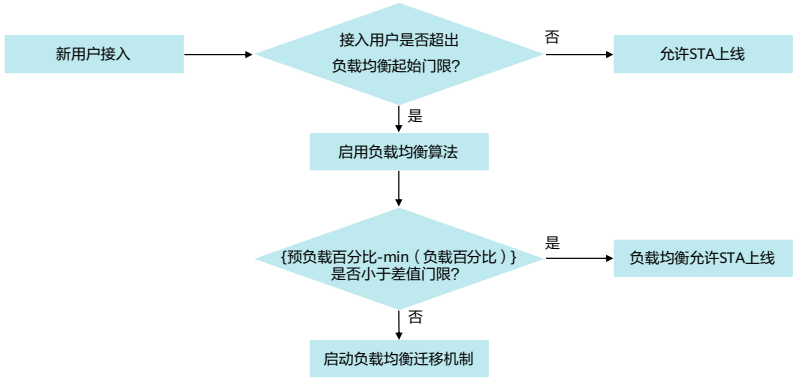


HUAWEI

- 使能负载均衡功能的AP必须连接到同一WAC上。
- 使能负载均衡功能的STA能够扫描到相互进行负载均衡的AP的SSID。

负载均衡算法

- 负载百分比：$\frac{\text{当前射频已关联的用户数}}{\text{射频支持的最大关联用户数}} \times 100\%$
- 预负载百分比：取STA预加入的AP射频的负载百分比。

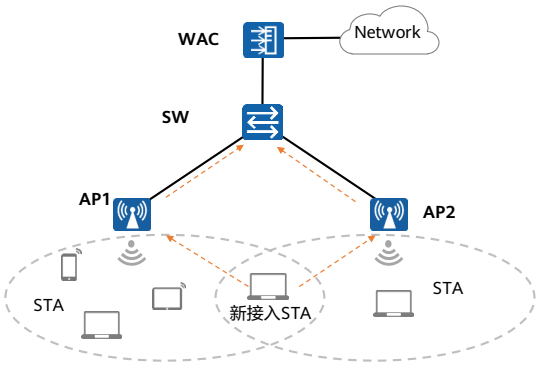


HUAWEI

- 负载均衡算法如下：通过公式（当前射频已关联的用户数/当前射频支持的最大关联用户数）×100%，计算出均衡组内所有成员（即所有AP射频）的负载百分比，得到最小值。然后取STA预加入的AP射频的负载百分比与最小值的差值，并将此差值跟设置的负载差值门限（通过命令行配置）比较，如果差值小于预设置的负载差值门限，则认为负载均衡；否则，认为负载不均衡，并启动负载均衡迁移机制。

静态负载均衡

- 静态负载均衡：将提供相同业务的一些AP通过手工配置加入到一个负载均衡组中。



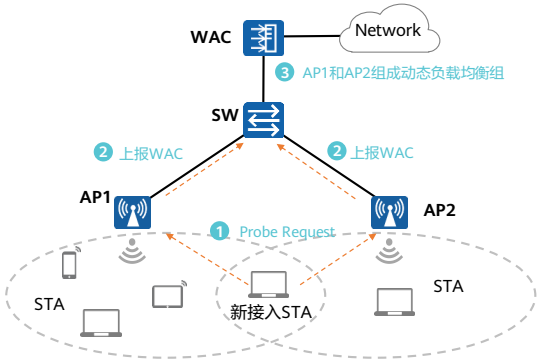
- AP周期性地向WAC发送与其关联的STA的信息，WAC根据这些信息周期性地执行负载均衡过程。
- AP的一个射频只能加入一个负载均衡组。
- 每个负载均衡组内成员有限，最多支持16个成员。

HUAWEI

- 按照是否需要手工创建负载均衡组，分为静态负载均衡和动态负载均衡
- 静态负载均衡：将提供相同业务的一些AP通过手工配置加入到一个负载均衡组中。AP周期性地向WAC发送与其关联的STA的信息，WAC根据这些信息周期性地执行负载均衡过程。
- 实现静态负载均衡，需要满足：
  - 图中的AP是以单频AP（即AP仅支持一个射频：2.4 GHz或5 GHz）为例。如果是多频AP，则AP上相同频段的射频之间实现负载均衡。
  - 每个负载均衡组内成员有限，最多支持16个成员。

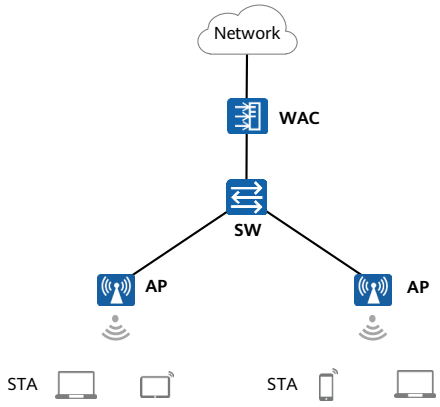
动态负载均衡

- 动态负载均衡：STA上线之前，发送广播的Probe Request报文，扫描周围的AP。AP收到STA探测信号后，上报WAC。WAC将所有上报该STA的AP动态组成一个组，然后根据负载均衡算法判断是否要引导该STA接入到负载相对较轻的AP。动态负载均衡解决了静态负载均衡的成员数目有限的缺点。



- 新加入的STA上线之前，发送广播的Probe Request报文，扫描周围的AP。
- AP收到STA探测信号后，上报WAC。
- WAC将上报该STA的AP动态组成一个组，根据负载均衡算法判断STA是否允许接入。
- 负载均衡的实现过程：
  - AP1射频下有4个在线STA，AP2射频下有1个在线STA，超过负载均衡起始门限5，AP1射频和AP2射频支持的最大关联用户数为10，配置的负载差值门限为5%。
  - 通过上面公式可以得出，AP1射频的负载百分比为40%（4/10×100%=40%），AP2射频的负载百分比为10%（1/10×100%=10%）。因此，负载百分比的最小值为10%。AP1的负载百分比与最小值的差值为30%（40%-10%=30%），大于负载门限值（5%），判断结果为两AP当前的负载不均衡，需要启动负载均衡机制，从AP1迁移部分STA到AP2。

WLAN动态负载均衡配置思路



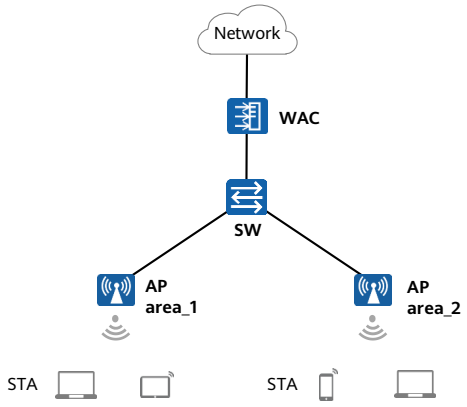
配置思路

- 创建RRM模板，在RRM模板使能动态负载均衡功能。
- 创建并引用射频模板。
- 检查配置结果。

HUAWEI

- 射频调优功能不适用于AP相互无法感知的场景，例如：AP使用定向天线、AP相隔较远或者AP间被阻隔等导致无法相互感知的情况。
- 射频调优功能不适用于高密场景、WDS/Mesh回传场景、轨交场景和室外定向天线的覆盖场景。
- 射频的工作模式为监控模式时，此射频不参与调优。

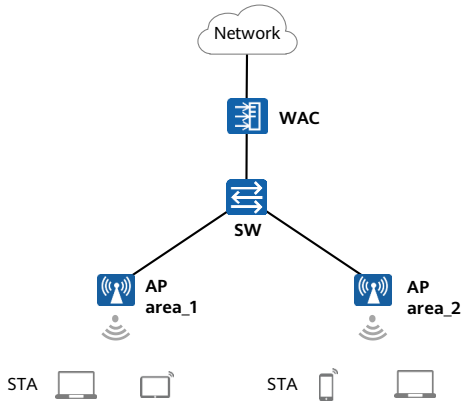
WLAN动态负载均衡配置举例（1）



创建RRM模板“wlan-net”，在RRM模板“wlan-net”使能动态负载均衡功能，并指定动态负载均衡的起始门限为15个，差值门限为25%。

```
[WAC] wlan
[WAC-wlan-view] rrm-profile name wlan-net
[WAC-wlan-rrm-prof-wlan-net] undo sta-load-balance dynamic disable
[WAC-wlan-rrm-prof-wlan-net] sta-load-balance dynamic sta-number start-threshold 15
[WAC-wlan-rrm-prof-wlan-net] sta-load-balance dynamic sta-number gap-threshold percentage 25
[WAC-wlan-rrm-prof-wlan-net] quit
```

WLAN动态负载均衡配置举例（2）



创建2G射频模板“wlan-radio2g”，并在该模板下引用RRM模板“wlan-net”。

```
[WAC-wlan-view] radio-2g-profile name wlan-radio2g
[WAC-wlan-radio-2g-prof-wlan-radio2g] rrm-profile wlan-net
[WAC-wlan-radio-2g-prof-wlan-radio2g] quit
```

创建5G射频模板“wlan-radio5g”，并在该模板下引用RRM模板“wlan-net”。

```
[WAC-wlan-view] radio-5g-profile name wlan-radio5g
[WAC-wlan-radio-5g-prof-wlan-radio5g] rrm-profile wlan-net
[WAC-wlan-radio-5g-prof-wlan-radio5g] quit
```

在名为“ap-group1”的AP组下引用射频模板。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] radio-5g-profile wlan-radio5g radio 1
[WAC-wlan-ap-group-ap-group1] radio-2g-profile wlan-radio2g radio 0
[WAC-wlan-ap-group-ap-group1] quit
```

WLAN动态负载均衡举例 - 检查配置结果

AC上执行命令**display rrm-profile name** *wlan-net*，可以查看到动态负载均衡的配置。

```
[WAC-wlan-view] display rrm-profile name wlan-net
------------------------------------------------------------------------------
...
Station load balance                                    : enable
Station load balance mode                               : sta-number
Station load balance sta-number start threshold         : 15
Station load balance sta-number gap threshold(percentage)  : 25
...
------------------------------------------------------------------------------
```

查看指定STA的动态负载均衡组信息。

```
[WAC-wlan-view] display station neighbor sta-mac e019-1dc7-1e08
-------------------------------------------------------------------------------------------------------------------------------------------
Device MAC       Device ID  Device Name       Radio ID  Probe info(RSSI/HH:MM:SS)        11k info[RCPI/RSNI/HH:MM:SS]
-------------------------------------------------------------------------------------------------------------------------------------------
 1047-80ab-c9a0  5          AP5               1         -48/16:28:24                     205/45/16:28:24
-------------------------------------------------------------------------------------------------------------------------------------------
Total neighbors: 1, total records: 1
```

目录

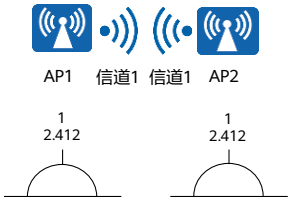
抗干扰技术概述

- 无线空口是个比较复杂的环境，WLAN空口的性能与许多因素相关：非WLAN无线设备干扰、WLAN无线设备间同频、邻频干扰等，这些干扰都会使WLAN系统性能降低。为了避免和消减无线干扰的影响，设计了以下特性：
  - 智能天线
  - 频谱分析
  - CCA
  - BSS Coloring

- 智能天线：
  - 智能天线的硬件部分由多个天线组成的天线阵列，根据天线选择算法选择其中部分天线阵子进行信号的发射和接收，不同天线的组合可以形成不同的信号辐射方向，从而为处于不同位置的STA选择最佳的天线，提高信号接收质量，提升系统的吞吐量。
- 频谱分析：
  - 通过频谱分析服务器对采集到的无线信号进行特征分析，识别出非Wi-Fi (Non-Wi-Fi)干扰设备，消除干扰对WLAN网络的影响。
- CCA：
  - CCA，即空闲信道评估，是指WLAN芯片在向空口发射信号前，先评估信道是否空闲。如果空闲，则发射信号；如果忙，则等待。
- BSS Color：
  - 当STA侦听到802.11ax信号时，可以通过表示BSS颜色的比特位 (BSS color bit)或者MAC地址识别来自OBSS（Overlapping Basic Service Set，重叠基本服务集）的信号，并根据相关信息进行空口冲突判断和干扰管理。

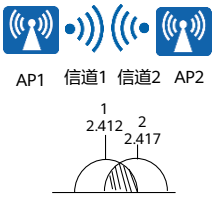
WLAN无线设备干扰

同频干扰



两个工作在相同频段上的AP之间的相互干扰。例如，对于规模较大的WLAN网络（例如高校），同一信道常常需要被不同AP使用。当这些AP之间存在着重复区域时，就存在同频干扰问题。

邻频干扰



两个中心频率不同的AP的发射频宽有重叠的部分，形成了邻频干扰。因此，邻频设备距离太近或信号太强时，会导致整体的噪声变高，影响网络性能。

非Wi-Fi设备干扰

- 2.4 GHz ISM (Industry Science Medicine)是全世界公开通用使用的无线频段，开发的产品具有全球通用性，各种无线产品均可使用此频段，微波炉、无绳电话、蓝牙设备等均会对WLAN网络产生频率干扰。
- 相比2.4 GHz频段，5 GHz频段干扰较少，目前使用此频段的设备主要为雷达、无线传感器、数字卫星、无线ATM网、软件无线电等。

蓝牙耳机

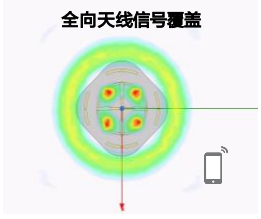
微波炉

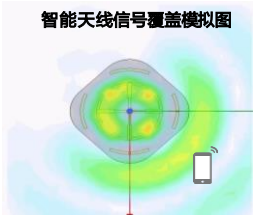
无绳电话

雷达

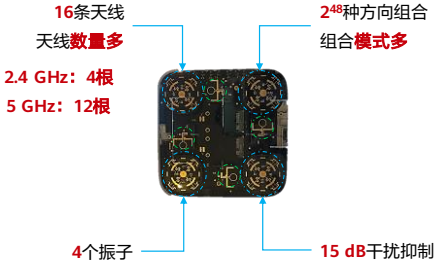
智能天线

- 智能天线是一个天线阵列，所谓天线阵列，就是一列取向相同，同极化，低增益的天线按一定的方式排列和激励，利用波的干涉原理产生强方向性的方向图，形成所希望的波束。
- 智能天线在水平面上具有多个定向辐射和1个全向辐射模式。





- 天线以全向模式接收终端发射的信号；
- 智能天线算法根据接收到的信号判断终端所在位置，并控制CPU发送控制信号选择最大辐射方向指向终端的定向辐射模式。

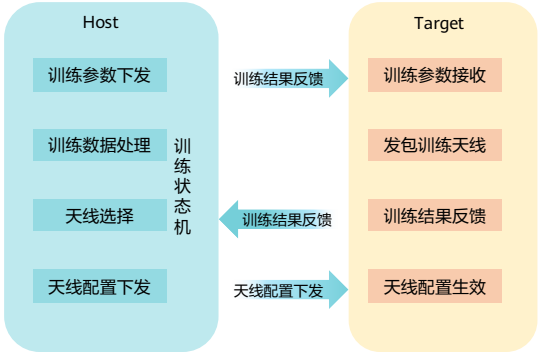


华为智能天线架构图

HUAWEI

智能天线阵列组合算法（1）

- 智能天线选择算法：针对不同的天线组合通过发送训练包，根据在不同天线组合下用户反馈的误包率(PER，Packet Error Rate)和接收信号强度(RSSI，Received Signal Strength Indicator)来为当前用户最合适的天线组合。



- Host侧维护了一个训练状态机，完成训练参数下发、训练数据处理、天线选择和天线配置下发等功能；
- Target侧负责训练参数接收、实际发包训练天线、训练结果反馈和天线配置生效等功能。

- Host侧维护了一个训练状态机，完成训练参数下发、训练数据处理、天线选择和天线配置下发等功能；Target侧负责训练参数接收、实际发包训练天线、训练结果反馈和天线配置生效等功能。
- 另外，针对多用户MU-MIMO场景，多个用户配对后，根据这几个用户在单用户模式下选择的天线模式，选择多用户时的天线模式：
  - 如果多个用户在单用户时天线模式相同，则多用户MIMO的天线模式不变。
  - 如果多个用户在单用户时天线模式不同，则多用户MIMO的天线模式采用全向天线模式。

智能天线阵列组合算法（2）

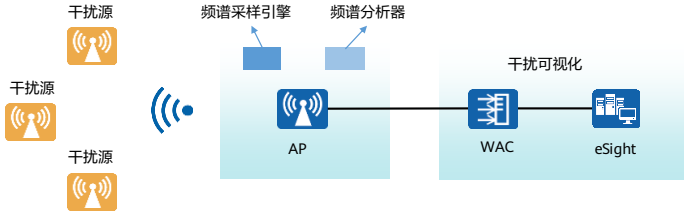
- 天线训练主要有两种方式触发，周期触发和性能突变触发：
  - 周期触发：以上次训练完成后运行的时间作为判断依据，该时间如果大于预设的时间周期，触发重新训练。对于周期性触发训练，触发周期是根据用户数进行动态调整。接入用户数越多，触发的周期越长，避免因为天线训练频繁占用系统性能，造成用户体验差。

接入用户数范围	<=5	>5 且 <=10	>10 且 <=20	>20
训练周期 (s)	30	100	180	300

  - 性能突变触发：系统稳定后，采集吞吐量并对一段时间内的吞吐量进行累加平均作为比较的基准值，利用基准值与当前节点的吞吐量差值与预先设置的门限进行比较，如果差值超过门限多次，表明当前节点性能波动较大，此时触发重新训练机制。

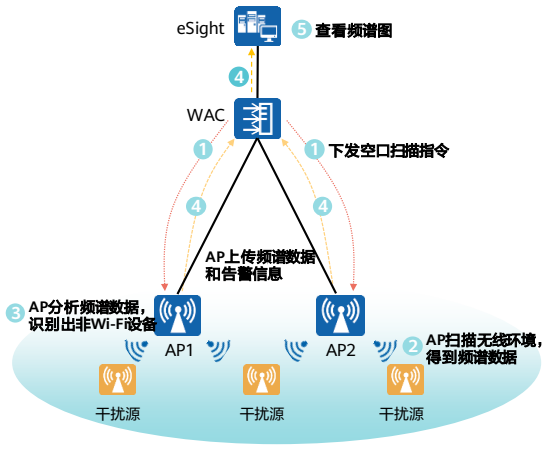
频谱分析概念

- 频谱分析的网络架构包括频谱采样引擎、频谱分析器、干扰可视化三个部分。
- 频谱采样引擎：用于收集无线网络的频谱信息，然后将频谱信息传输频谱分析器。
- 频谱分析器：用于分析频谱数据，识别出干扰源类型，输出干扰设备报告并将干扰设备报告发送给干扰可视化功能模块。
- 干扰可视化：用于图示呈现干扰源信息，如实时频谱图等。



频谱分析网络架构

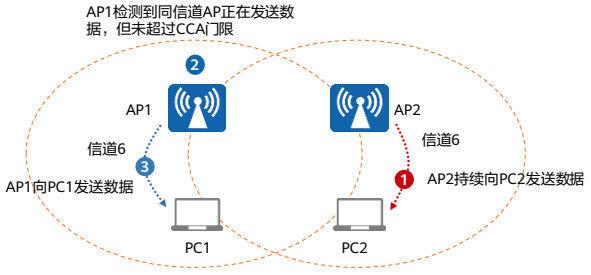
频谱分析工作原理



- WAC向AP下发空口扫描指令。
- AP周期性地扫描无线环境。AP扫描后可得到原始的频谱采样数据。每个频谱采样数据包含一组子载波，可用于干扰识别。
- AP作为频谱分析器，它的频谱分析模块根据算法对采样数据进行计算，通用的算法包括了脉冲提取、脉冲合并、脉冲分簇、提取时间签名、提取频率特征、计算周期、计算占空比等几个处理步骤。当AP计算出上述特征后，可使用一种或多种特征跟设备加载的干扰源特征库进行匹配，从而识别出非Wi-Fi设备。
- AP可以将数据直接上传频谱绘图服务器，也可以通过WAC中转将数据直接上传频谱绘图服务器。
- 在可视化界面查看频谱图。

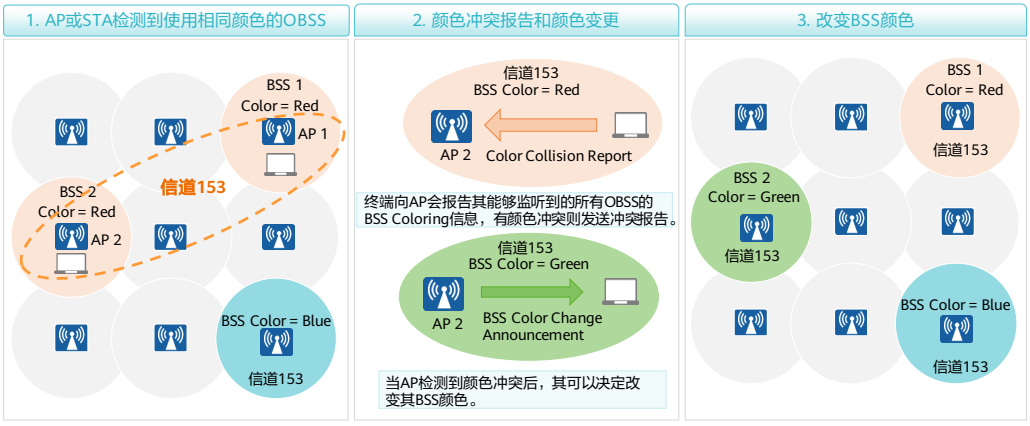
CCA

- CCA（Clear Channel Assessment，空闲信道评估）阈值是WLAN芯片评估信道是否空闲的标准，当信道中的噪声强度超过阈值时，则认为当前信道繁忙；反之，则认为当前信道空闲。
- 在部署WLAN网络时，配置合理的CCA阈值，能够降低信号干扰，提高信道复用程度。
  - 如果AP部署比较密集，希望缩小实际覆盖范围来忽略远端弱信号时，建议提高CCA阈值。
  - 如果AP部署比较稀疏，希望尽量扩大可以有效接收信号的范围时，建议降低CCA阈值。

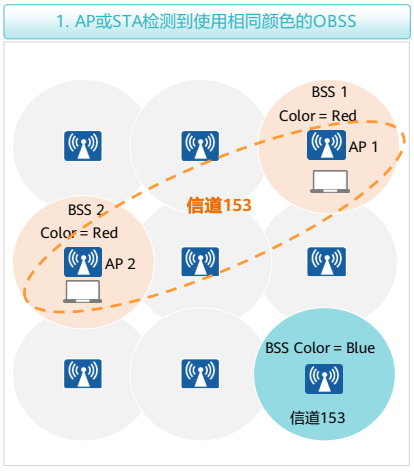


802.11ax BSS Coloring

- BSS Coloring是一种用于解决由于重叠基本服务集 (OBSS)提升空间重用率的方法，减少因为重叠BSS导致的MAC层竞争开销，其目标是提升空间复用率，同时不会因为BSS间的干扰而导致节点间PHY层传输速率的降低。

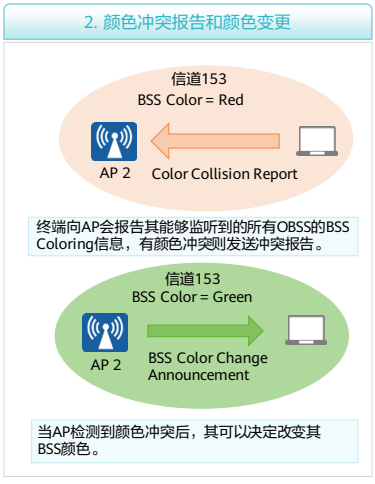


802.11ax BSS Coloring工作机制 (1)



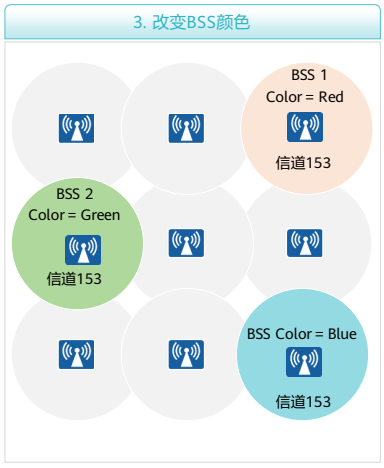
- 802.11ax设备通过向PHY头部添加字段（即BSS Coloring字段）来区分BSS，节点在竞争时，根据检测到物理层头部的BSS Coloring字段来分配MAC层的竞争行为。若BSS Coloring字段信息相同，那么代表在同一个BSS内 (intra-BSS)。若BSS Coloring字段信息不同，那么代表这里是重叠覆盖区域，在多个BSS间 (inter-BSS)。
- 通过着色机制，无线传输在其开始时就被标记，这会帮助周围其它设备决定是否允许无线介质被同时使用。
- BSS着色机制要达到的目标就是，使设备能够区分自己网络中的传输与邻近网络中的传输。自适应功率和灵敏度阈值允许动态调整发射功率和信号检测阈值以增加空间重用效率，在尽可能的情况下最大地去减少同频干扰。

802.11ax BSS Coloring工作机制 (2)



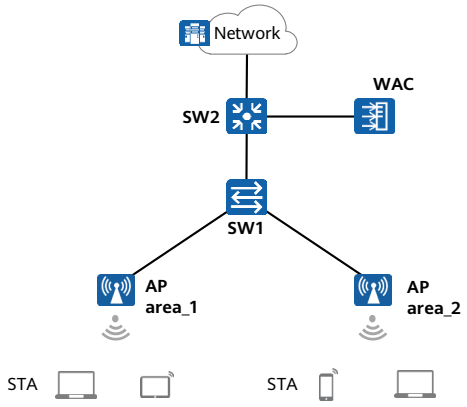
- 对于802.11ax的AP，其如果检测到使用相同颜色的OBSS，则它能够更改变其BSS颜色，减少同频干扰。若AP与AP间的BSS Coloring一样，那么这也是一种BSS Coloring的冲突，即颜色冲突。如图所示，如果802.11ax AP听到来自其他AP或者该AP节点的不同BSS Coloring字段，那么是检测到一次颜色冲突。
- 另外，如果终端检测到颜色冲突，则该终端会向其关联的AP发送颜色冲突报告。终端向AP会报告其能够监听到的所有OBSS的BSS Coloring信息。
- AP会通过Beacon告知所有关联在本BSS内部的节点，BSS Coloring的改变。BSS Coloring的改变还可以通过探测响应和重新关联响应帧中进行通知。如图所示，AP告知节点BSS Coloring的颜色变化，其New BSS Color子字段则包含新BSS Coloring的数值。

802.11ax BSS Coloring工作机制 (3)



- 当AP检测到颜色冲突后，其可以决定改变其BSS颜色。不过改变BSS Coloring的标准和选择新BSS Coloring信息的方法超出802.11ax草案修正案的范围。WLAN供应商目前可以自行制定，例如Aerohive信道选择协议（ACSP）。
- AP会通过Beacon告知所有关联在本BSS内部的节点，BSS Coloring的改变。BSS Coloring的改变还可以通过探测响应和重新关联响应帧中进行通知。如上图所示，AP告知节点BSS Coloring的颜色变化，其New BSS Color子字段则包含新BSS Coloring的数值。

频谱分析配置举例（1）



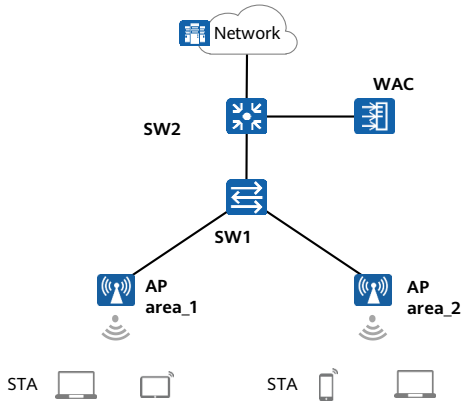
创建AP系统模板“wlan-spectrum”，并配置频谱服务器信息和频谱分析时非Wi-Fi设备的信息在AC上的老化时间。

```
[WAC] wlan
[WAC-wlan-view] ap-system-profile name wlan-spectrum
[WAC-wlan-ap-system-prof-wlan-spectrum] spectrum-analysis server ip-address 10.137.43.4 port 32181 via-ac ac-port 5001
[WAC-wlan-ap-system-prof-wlan-spectrum] spectrum-analysis non-wifi-device aging-time 5
[WAC-wlan-ap-system-prof-wlan-spectrum] quit
```

创建空口扫描模板“wlan-airscan”，并配置扫描间隔时间和扫描持续时间。

```
[WAC-wlan-view] air-scan-profile name wlan-airscan
[WAC-wlan-air-scan-prof-wlan-airscan] scan-period 100
[WAC-wlan-air-scan-prof-wlan-airscan] scan-interval 8000
[WAC-wlan-air-scan-prof-wlan-airscan] quit
```

频谱分析配置举例（2）



创建2G射频模板“wlan-radio2g”，并在该模板下引用空口扫描模板“wlan-airscan”。

```
[WAC-wlan-view] radio-2g-profile name wlan-radio2g
[WAC-wlan-radio-2g-prof-wlan-radio2g] air-scan-profile wlan-airscan
```

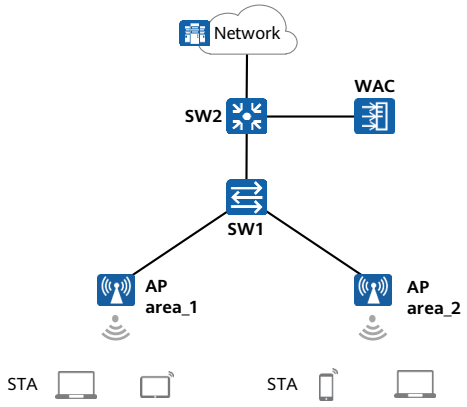
创建5G射频模板“wlan-radio5g”，并在该模板下引用空口扫描模板“wlan-airscan”。

```
[WAC-wlan-view] radio-5g-profile name wlan-radio5g
[WAC-wlan-radio-5g-prof-wlan-radio5g] air-scan-profile wlan-airscan
```

在名为“ap-group1”的AP组下引用5G射频模板“wlan-radio5g”和2G射频模板“wlan-radio2g”。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] radio-5g-profile wlan-radio5g radio 1
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-ap-group-ap-group1] radio-2g-profile wlan-radio2g radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
```

频谱分析配置举例（3）



开启AP射频上传频谱分析数据功能。服务器可使用上传的数据进行频谱分析和频谱绘图。**spectrum-report**命令重启后将会失效，需要用户重新配置。

[WAC-wlan-view] **spectrum-report ap-name** *area_1* **radio** *0*
[WAC-wlan-view] **spectrum-report ap-name** *area_1* **radio** *1*

频谱分析配置结果验证

在WAC上查看频谱分析功能的配置信息。

```
[WAC-wlan-view] display ap-system-profile name wlan-spectrum
------------------------------------------------------------------------------
AP report to                    : AC
Server IP                       : 10.137.43.4
Server port                     : 32181
AC port                         : 5001
Device aging-time(minute)       : 5
------------------------------------------------------------------------------
```

在WAC上查看上报频谱报文到频谱服务器的AP列表。

```
[WAC-wlan-view] display spectrum-analysis server-reporter
------------------------------------------------------------
ID          AP name                 Radio ID
------------------------------------------------------------
1           area_1                  0
1           area_1                  1
------------------------------------------------------------
Total: 2
```

在WAC上查看检测到的非Wi-Fi设备。

```
[WAC-wlan-view] display wlan non-wifi-device all
------------------------------------------------------------------
Detect AP name                      : area_1
Detect AP radio ID                  : 1
Detect AP channel                   : 36
Non-Wi-Fi device type               : 9
Non-Wi-Fi device name               : Unknown fix freq device
Non-Wi-Fi device frequency type     : Narrow bandwidth
Non-Wi-Fi device channel            : 149,150
Non-Wi-Fi device RSSI               : -62,-66
Non-Wi-Fi device detect time last   : 2017-07-02/08:16:56
Non-Wi-Fi device center frequency(MHz) : 5749
Non-Wi-Fi device bandwidth(KHz)     : 70
Non-Wi-Fi device duty(%)            : 100
Non-Wi-Fi device interfere level    : 3
------------------------------------------------------------------
Total: 1
```

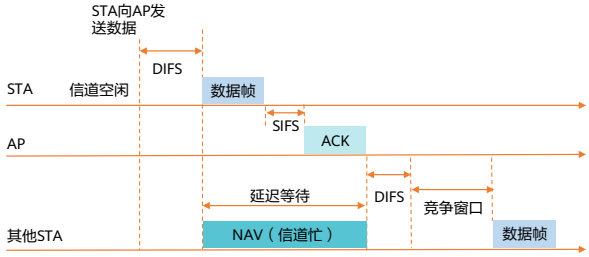
目录

WLAN QoS概述

- WLAN QoS (Quality of Service)，网络管理者根据各种业务的特点来对网络资源进行合理的规划和分配，从而为不同的应用提供不同质量的接入服务，以满足用户需求，同时提高网络资源的利用率。
- WLAN QoS是为了满足无线用户的不同网络流量需求而提供的一种差分服务的能力。在WLAN网络中使用QoS技术，可以实现：
  - 无线信道资源的高效利用：通过Wi-Fi多媒体标准WMM（Wi-Fi Multimedia，Wi-Fi多媒体），让高优先级的数据优先竞争无线信道。
  - 网络带宽的有效利用：通过优先级映射，让高优先级数据优先进行传输。
  - 网络拥塞的降低：通过流量监管，限制用户的发送速率，有效避免因为网络拥塞导致的数据丢包。
  - 无线信道的公平占用：通过Airtime调度，同一射频下的多个用户可以在时间上相对公平的占用无线信道。
  - 不同类型业务的差分服务：通过将报文信息与ACL规则进行匹配，或者通过应用识别，识别同类报文。为同类报文提供相同的QoS服务，实现对不同类型业务的差分服务。

WMM（1）

- 802.11 MAC层通过协调功能 (Coordination Function)来确定BSS中的STA之间如何发送或接收数据。802.11的MAC包括两个机制：
  - 分布式协调功能DCF (Distributed Coordination Function)：使用CSMA/CA机制，每个STA通过争用信道来获取数据帧的发送权。
  - 点协调功能PCF (Point Coordination Function)：使用集中控制的接入算法，用类似于探询的方法把数据帧的发送权轮流交给各STA，从而避免碰撞冲突。



CSMA/CA的工作原理

HUAWEI

- 802.11协议中必须有DCF机制，PCF是可选项。
- CSMA/CA机制，如图所示：
  - STA要向AP发送数据，先检测信道空闲状态。若检查到空闲，等待DIFS时间后发送数据帧，并等待确认。STA发送数据帧中携带了NAV信息，其他STA接收到此帧后更新自己的NAV信息，表明在这段时间内信道忙，如果有数据要发送，需要延迟等待。
  - AP正确接收数据帧，等待SIFS后向STA发送ACK帧。当ACK帧发送结束，信道开始空闲。等待DIFS时间后，需要发送数据的各STA开始利用退避算法争用信道。退避计数器最先减小到0的STA开始发送数据帧。
- 帧间间隔IFS (InterFrame Space)：802.11规定，所有STA完成数据帧发送后，必须等待IFS时间才能发送下一帧。帧间间隔的长短取决于该站要发送的帧的类型。高优先级帧需要等待时间较短，可以优先获得发送权。常用三种帧间隔如下：短帧间间隔SIFS (Short IFS)：分隔属于一次对话的各帧，优先级高。使用此类型的帧有：ACK帧、CTS帧等。

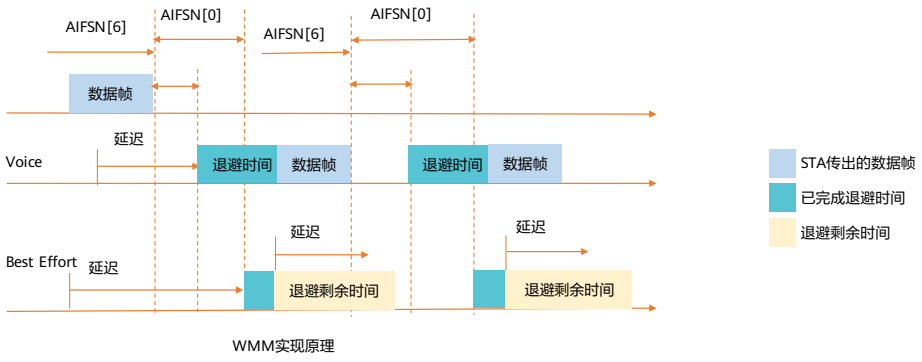
WMM (2)

- 每个WAC队列定义了一套增强的分布式信道访问EDCA (Enhanced Distributed Channel Access)参数，该参数决定了队列占用信道的能力大小，可以实现高优先级的WAC占用信道的机会大于低优先级的WAC。

参数名	参数含义	具体用法
AIFSN	仲裁帧间隙数 (Arbitration Inter Frame Spacing Number)	AIFSN数值越大，用户的空闲等待时间越长，优先级越低
ECWmin ECWmax	最小竞争窗口指数和最大竞争窗口指数形式 (Exponent form of CWmin, Exponent form of Cwmax)	这两个值共同决定了平均退避时间值，这两个数值越大，用户的平均退避时间越长，优先级越低
TXOPLimit	传输机会限制 (Transmission Opportunity Limit)	用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用信道的时间越长；如果是0，则每次占用信道后只能发送一个报文
ACK	协议规定ACK策略有两种：Normal ACK和No ACK	No ACK针对通信质量较好，干扰较小的情况；Normal ACK指在成功接收到报文后，发送ACK进行确认

WMM (3)

- Voice报文的AIFSN (AIFSN[6])和退避时间比Best Effort报文的小。当这两类报文同时要发送时，用户优先级高的Voice报文优先竞争到无线信道。



WMM实现原理

HUAWEI

- ECWmax=<退避时间>=ECWmin。
- 数据帧的时长由TXOPLimit决定。
- WMM协议定义了两种ACK策略：Normal ACK和No ACK。
  - Normal ACK策略：对于发送端发送的每个单播报文，接收端在成功接收到报文后，都需要发送ACK帧进行确认。
  - No ACK策略：在通信质量很好、干扰很小的情况下，为了提高传输效率，可以选择不应答ACK帧。
  - ACK策略仅对AP生效。
  - 在通信质量较差的情况下，不推荐使用No ACK策略，可能会造成丢包率增大。

无线用户优先级

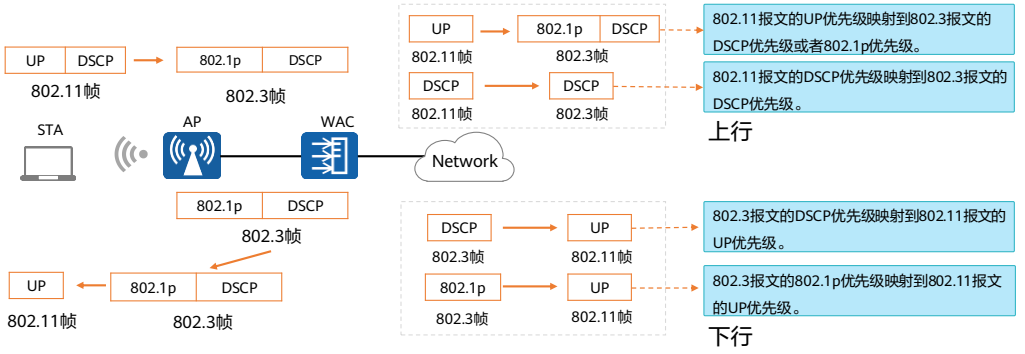
- WMM协议将报文分为4个无线接入类别WAC（Wireless Access Category），与802.11报文中用户优先级UP（User Preference)的对应关系如表所示，在AP上，根据数据报文的UP值确定数据属于哪一个WMM访问类别，然后根据WMM的优先级转发数据。

UP	WAC
7	AC_VO（Voice）
6	
5	AC_VI（Video）
4	
3	AC_BE（Best Effort）
0	
2	AC_BK（Background）
1	

- UP值：用户优先级，它代表802.11报文的优先级。存在于802.11的MAC头的QoS字段里面。UP值的范围是0－7共8个等级。在WMM协议中，规定了WMM和UP的映射关系。WMM一共有4个类别，每个类别映射到2个UP值。在AP上，根据数据报文的UP值确定数据属于哪一个WMM访问类别，然后根据WMM的优先级转发数据。
- 四个优先级队列，高优先级的WAC 占用信道的机会大于低优先级的WAC，从而使不同的WAC 能获得不同级别的服务。
- 通常我们视频会议中的语音以及视频对应的就是AC_VO和AC_VI，而我们网络上的QQ语音，QQ视频均为AC_BE。

优先级映射

- 不同的报文使用不同的报文优先级。例如，STA发出的802.11报文中携带UP优先级或DSCP优先级，有线网络中的VLAN报文使用802.1p优先级，IP报文使用DSCP优先级。当报文经过不同网络时，为了保持报文的优先级，需要在设备上配置优先级字段的映射关系。



HUAWEI

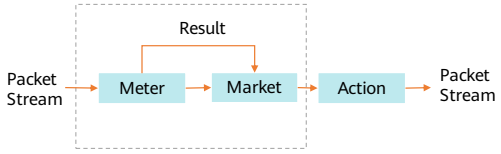
- 上行时，STA将802.3帧通过无线网卡发出变成802.11帧，AP接收到STA发送的802.11报文后，可将802.11报文进行优先级映射：
  - 802.11报文的UP优先级映射到802.3报文的DSCP优先级或者802.1p优先级。
  - 802.11报文的DSCP优先级映射到802.3报文的DSCP优先级。
- 下行时，WAC将网络侧收到的802.3报文，通过隧道或直接转发方式发送给AP。AP接收到802.3报文后，将802.3报文的DSCP优先级或者802.1p优先级映射为802.11报文的UP优先级，然后发给STA。

流量监管和流量整形概述

- 流量监管和流量整形通过监督进入网络的流量速率，用来限制流量及其资源的使用，保证更好地为用户提供服务。
- 流量监管：
  - 流量监管TP (Traffic Policing)就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。
- 流量整形：
  - 流量整形TS (Traffic Shaping)是一种主动调整流量输出速率的措施。当下游设备的入接口速率小于上游设备的出接口速率或发生突发流量时，下游设备入接口处可能出现流量拥塞的情况，此时用户可以通过在上游设备的接口出方向配置流量整形，将上游不规整的流量进行削峰填谷，输出一条比较平整的流量，从而解决下游设备的拥塞问题。
- 流量监管和流量整形的主要区别在于：
  - 利用流量监管进行报文控制时，直接丢弃不符合速率要求的报文。而流量整形则会将不符合速率要求的报文先行缓存，当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。
  - 流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

流量监管的组成

- Meter：通过令牌桶机制对网络流量进行度量，向Marker输出度量结果。
- Marker：根据Meter的度量结果对报文进行染色，报文会被染成green、yellow、red三种颜色。
- Action：根据Marker对报文的染色结果，对报文进行一些动作，动作包括：
  - pass：对测量结果为“符合”的报文继续转发。
  - remark + pass：修改报文内部优先级后再转发。
  - discard：对测量结果为“不符合”的报文进行丢弃。



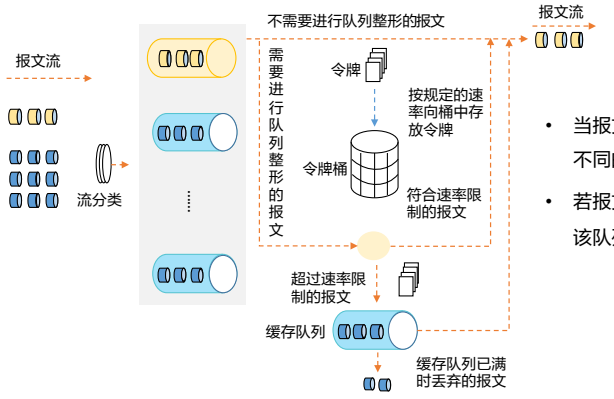
流量监管组件

HUAWEI

- 默认情况下，green报文、yellow报文进行转发，red报文丢弃。

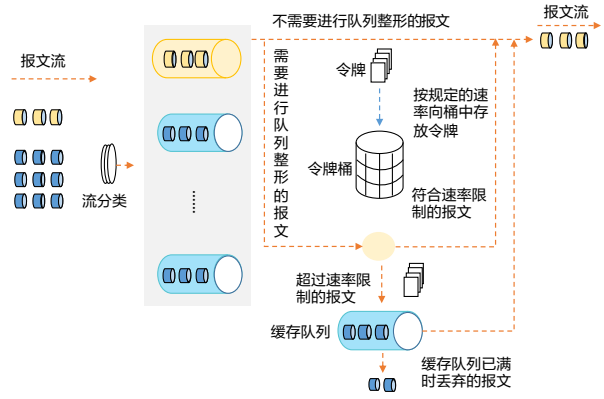
流量整形（1）

- 流量整形是一种应用于接口或队列的流量控制技术，可以对从接口上经过的所有报文或某类报文进行速率限制。以接口下采用单速单桶技术的基于流的队列整形为例介绍流量整形的处理流程。



- 当报文到来的时候，首先对报文进行分类，使报文进入不同的队列。
- 若报文进入的队列没有配置队列整形功能，则直接发送该队列的报文；否则，进入下一步处理。

流量整形 (2)



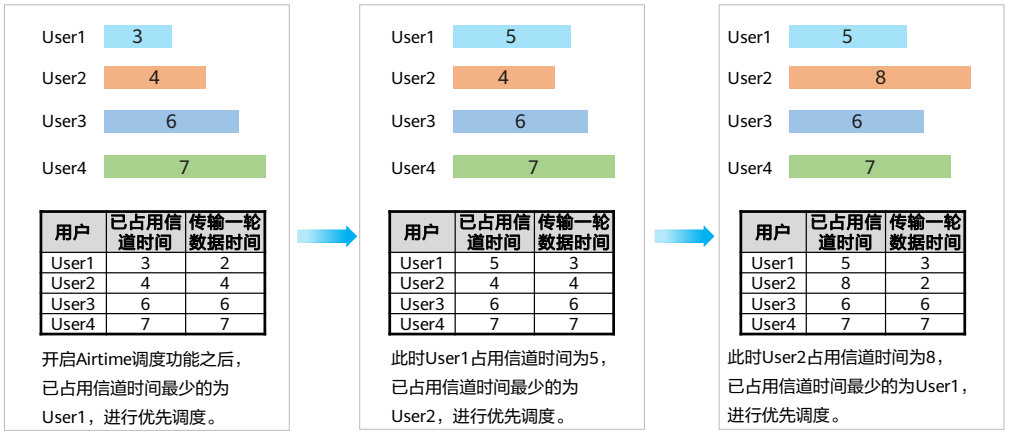
- 按用户设定的队列整形速率向令牌桶中放置令牌：
  - 如果令牌桶中有足够的令牌可以用来发送报文，则报文直接被发送，在报文被发送的同时，令牌做相应的减少。
  - 如果令牌桶中没有足够的令牌，则将报文放入缓存队列，如果报文放入缓存队列时，缓存队列已满，则丢弃报文。

- 缓存队列中有报文的时候，系统按一定的周期从缓存队列中取出报文进行发送，每次发送都会与令牌桶中的令牌数作比较，直到令牌桶中的令牌数减少到缓存队列中的报文不能再发送或缓存队列中的报文全部发送完毕为止。

Airtime调度定义

- Airtime调度是在同一射频下对每个用户的无线信道占用时间进行调度，确保每个用户相对公平的占用无线信道。
- 开启Airtime调度功能后，设备会对同一射频下多个用户占用无线信道的时间进行统计，以累加的方式记录每个用户占用无线信道的时间，根据占用无线信道时间由小到大进行排序。
- Airtime调度相对于传统的调度方式增加了以下功能：
  - 新用户传输数据时，从原来的直接放入用户队列末尾修改为根据占用无线信道时间插入指定的位置。
  - 用户传输完第一个队列数据后判断该用户是否还有数据需要传输，如果没有数据传输直接调用第二个用户，如果仍有数据需要传输则根据占用的无线信道时间插入到队列中并调用当前占用时间最短的用户。

Airtime调度功能举例



- 每次传输数据设备会优先调度占用信道时间最短的用户，确保每个用户相对公平的占用无线信道。
- 考虑到防止最先接入的用户后期一直无法占用无线信道传送数据，以保证先后接入的用户有相同的权重，设备会周期性的对所有用户的无线信道占用时间统计清零。
- 在设备和终端上开启WMM功能后，用户报文会分不同的类型（业务类型，分为VI/VO/BE/BK）进行调度。例如语音类报文只会跟语音类报文进行调度，视频类报文只会跟视频类报文进行调度。
- 如果多用户传输的是不同类型的报文，则Airtime调度不生效。例如两个用户进行报文传输，第一个用户传输的是语音类报文，另一个用户传输的是视频类报文，则两个用户之间不会进行Airtime调度。

智能应用识别（1）

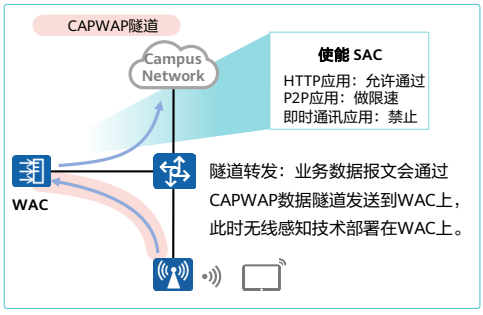
- 智能应用控制SAC（Smart Application Control)是一个智能的应用协议识别与分类引擎，利用业务感知技术，对报文中的第4～7层内容和一些动态协议（如HTTP、RTP）进行检测和识别，根据分类结果实施精细化QoS策略控制。
- 该功能的应用场景分为两种：
  - 针对应用协议配置QoS策略：希望能够规范WLAN网络中员工的上网行为，保证网络质量。
  - 针对语音视频业务进行优化：WLAN网络中存在语音视频需求，希望提升语音视频质量。例如对于使用VoIP的语音终端希望能够提升通话质量，保证电话会议不中断。

- 部分针对应用协议的QoS策略：
  - 对于一般的网络浏览行为予以放行，保证企业员工能够访问网络，正常办公。
  - 对于QQ_IM等IM类型应用程序进行阻断，限制企业员工从事与工作无关的事务，规范用户上网行为。
  - 对于BT、eDonkey_eMule等P2P报文则限制其带宽，保证网络质量。

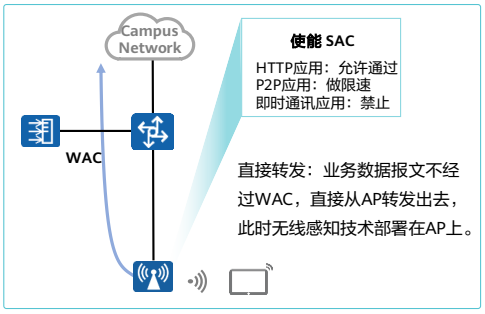
智能应用识别（2）

- 语音或视频业务优化只能部署在WAC上仅对隧道转发的业务场景生效。对于非语音和视频应用的其他应用协议配置QoS策略功能，根据数据转发方式的不同，将该功能部署在不同的设备上。

隧道转发方式下对应用协议配置QoS策略应用场景

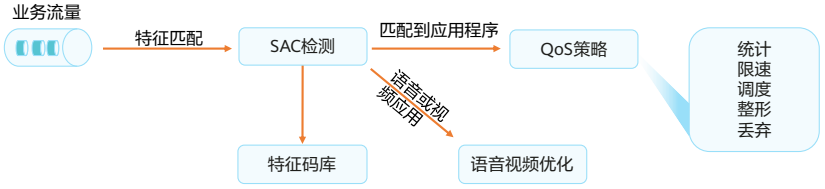


直接转发方式下对应用协议配置QoS策略应用场景



智能应用识别原理

- 特征识别技术是业务感知技术的最基本技术。不同的应用程序通常会采用不同的协议，而不同的应用协议具有各自的特征，这些特征可能是特定的端口、特定的字符串或者特定的比特序列，能标识该协议的特征称为特征码。
- 特征识别技术，即通过匹配数据报文中的特征码来确定应用。协议的特征不仅在单个报文中体现，某些协议报文的特征是分布在多个报文中的，需要对多个报文进行采集分析，才能够识别出协议类型。



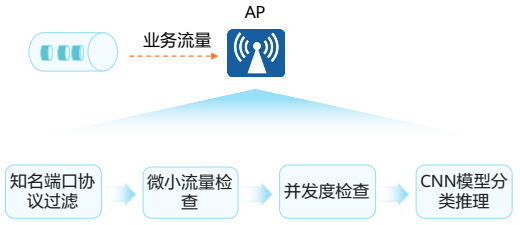
SAC工作机制

HUAWEI

- 系统对流经设备的业务流进行分析，将分析结果和加载到设备上的特征库进行对比，通过匹配数据报文中的特征码来识别出应用程序，根据识别结果实施精细化QoS策略控制或者对语音和视频应用进行优化从而提高语音和视频的通信质量。

动态流检测（1）

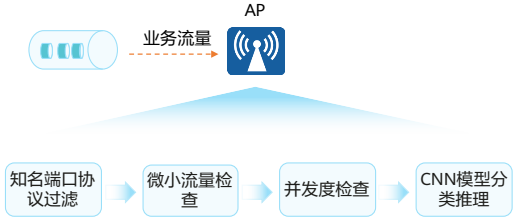
- 动态流检测DFI (Dynamic Flow Inspection)是一种利用流量行为对用户的TCP/UDP流量进行应用识别，根据识别结果进行应用保障的应用识别技术。
- DFI可识别的应用大类为VoIP、视频直播、视频会议、长视频点播、短视频点播、文件传输、游戏、远程桌面、Web类、在线协同办公、知名端口协议。



DFI应用识别过程

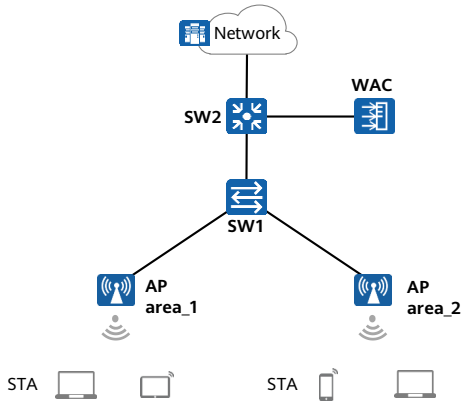
动态流检测（2）

- 设备首先将会对业务流量的端口信息进行匹配，如果匹配知名端口，则可根据端口信息来进行流量分类。
- 其次设备会对业务流量做微小流量检查，如果业务流量存在时间特别短则该流量属于微小流量，对其识别意义不大。
- 接下来是对业务流量进行并发度检查，主要目的是排除一些P2P的流量。
- 如果以上步骤还未识别出流量，则设备将会调用卷积神经网络CNN（Convolutional Neural Networks)模型分类推理模块，对业务流量的类型进行推理。



DFI应用识别过程

WLAN QoS配置举例 - WMM配置（1）



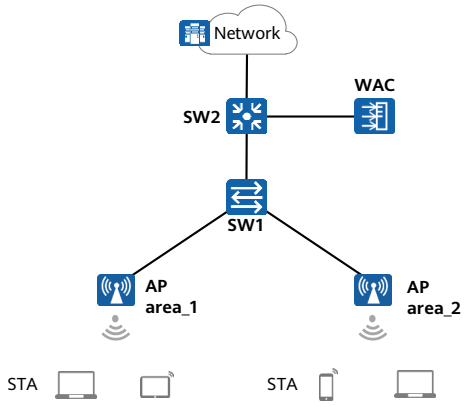
进入2 GHz和5 GHz射频模板，配置AP上的EDCA参数，使语音和视频业务优先使用网络带宽。

[WAC] **wlan**
[WAC-wlan-view] **radio-2g-profile name** *wlan-radio2g*
[WAC-wlan-radio-2g-prof-wlan-radio2g] **wmm edca-ap ac-vo aifsn** *2* **ecw ecwmin** *2* **ecwmax** *4* **txoplimit** *0* **ack-policy normal**
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-radio-2g-prof-wlan-radio2g] **wmm edca-ap ac-vi aifsn** *5* **ecw ecwmin** *3* **ecwmax** *5* **txoplimit** *0* **ack-policy normal**
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-radio-2g-prof-wlan-radio2g] **wmm edca-ap ac-be aifsn** *12* **ecw ecwmin** *6* **ecwmax** *10* **txoplimit** *0* **ack-policy normal**
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-radio-2g-prof-wlan-radio2g] **wmm edca-ap ac-bk aifsn** *12* **ecw ecwmin** *8* **ecwmax** *10* **txoplimit** *0* **ack-policy normal**
Warning: This action may cause service interruption. Continue?[Y/N]y

HUAWEI

- 5 GHz射频模板配置方式与2 GHz射频模板类似，此处不再赘述。

WLAN QoS配置举例 - WMM配置 (2)



进入名为“wlan-net”的SSID模板，配置STA上的EDCA参数，使语音和视频业务优先使用网络带宽。

```
[WAC-wlan-view] ssid-profile name wlan-net
[WAC-wlan-ssid-prof-wlan-net] wmm edca-client ac-vo aifsn 2 ecw ecwmin 2 ecwmax 4 txoplimit 0
[WAC-wlan-ssid-prof-wlan-net] wmm edca-client ac-vi aifsn 5 ecw ecwmin 3 ecwmax 5 txoplimit 0
[WAC-wlan-ssid-prof-wlan-net] wmm edca-client ac-be aifsn 12 ecw ecwmin 6 ecwmax 10 txoplimit 0
[WAC-wlan-ssid-prof-wlan-net] wmm edca-client ac-bk aifsn 12 ecw ecwmin 8 ecwmax 10 txoplimit 0
[WAC-wlan-ssid-prof-wlan-net] quit
```

WLAN QoS配置举例 - 配置优先级映射

创建名为“wlan-traffic”的流量模板，并配置优先级映射关系。

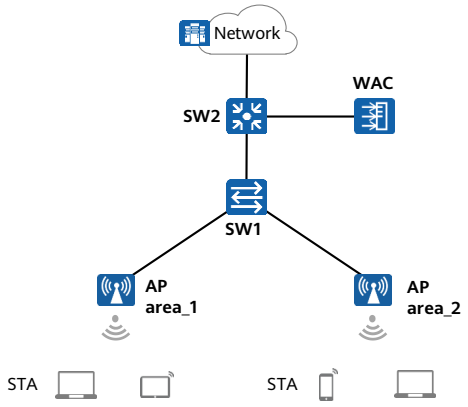
```
[WAC-wlan-view] traffic-profile name wlan-traffic
[WAC-wlan-traffic-prof-wlan-traffic] priority-map downstream trust dscp
[WAC-wlan-traffic-prof-wlan-traffic] priority-map downstream dscp 48 to 55 dot11e 4
[WAC-wlan-traffic-prof-wlan-traffic] priority-map downstream dscp 56 to 63 dot11e 5
[WAC-wlan-traffic-prof-wlan-traffic] priority-map downstream dscp 32 to 39 dot11e 6
[WAC-wlan-traffic-prof-wlan-traffic] priority-map downstream dscp 40 to 47 dot11e 7
[WAC-wlan-traffic-prof-wlan-traffic] priority-map tunnel-upstream trust dot11e
[WAC-wlan-traffic-prof-wlan-traffic] priority-map tunnel-upstream dot11e 6 dscp 32
[WAC-wlan-traffic-prof-wlan-traffic] priority-map tunnel-upstream dot11e 7 dscp 40
[WAC-wlan-traffic-prof-wlan-traffic] priority-map tunnel-upstream dot11e 4 dscp 48
[WAC-wlan-traffic-prof-wlan-traffic] priority-map tunnel-upstream dot11e 5 dscp 56
```

在VAP模板“wlan-net”中引用流量模板“wlan-traffic”。

```
[WAC-wlan-view] vap-profile name wlan-net
[WAC-wlan-vap-prof-wlan-net] traffic-profile wlan-traffic
Warning: This action may cause service interruption. Continue?[Y/N]y
```


- 结果验证：
  - 在WAC上执行命令display radio-2g-profile name wlan-radio2g，查看2G射频模板中AP上EDCA参数的配置信息。可以看到“AC_VI”和“AC_VO”报文的EDCA参数优先级高于“AC_BE”和“AC_BK”报文，因此，视频和语音业务会优先使用无线信道。查看5G射频模板的配置信息与之类似。
  - 在WAC上执行命令display ssid-profile name wlan-net，查看SSID模板中STA上EDCA参数的配置信息。可以看到“AC_VI”和“AC_VO”报文的EDCA参数优先级高于“AC_BE”和“AC_BK”报文，因此，视频和语音业务会优先使用无线信道。
  - 在WAC上执行命令display traffic-profile name wlan-traffic，查看流量模板中优先级映射的配置信息。可以看到“AC_VI”和“AC_VO”报文映射后的隧道DSCP优先级高于“AC_BE”和“AC_BK”报文对应的优先级，因此，视频和语音业务会优先传输。

WLAN QoS配置举例 - 配置流量监管



创建名为“wlan-traffic”的流量模板，并配置每个STA的上行速率限制为2 M，VAP下所有STA的总上行速率限制为30 M。

```
<WAC6606> system-view
[WAC6606] sysname WAC
[WAC] wlan
[WAC-wlan-view] traffic-profile name wlan-traffic
[WAC-wlan-traffic-prof-wlan-traffic] rate-limit client up 2048
[WAC-wlan-traffic-prof-wlan-traffic] rate-limit vap up 30720
```

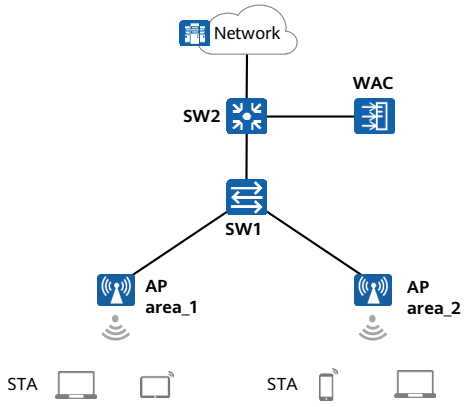
创建名为“wlan-net”的VAP模板，引用对应的流量模板。

```
[WAC-wlan-view] vap-profile name wlan-net
[WAC-wlan-vap-prof-wlan-net] traffic-profile wlan-traffic
Warning: This action may cause service interruption. Continue?[Y/N]y
```


HUAWEI

- 结果验证：在WAC上执行命令**display traffic-profile name wlan-traffic**，查看流量模板下速率限制的配置信息，可以看到单个STA的上行速率限制为2048 kbit/s (2 Mbps)，VAP下所有STA的总上行速率限制为30720 kbit/s (30 Mbps)。

WLAN QoS配置举例 - 配置Airtime调度



创建名为“wlan-rrm”的RRM模板，使能Airtime调度功能。

```
[WAC] wlan
[WAC-wlan-view] rrm-profile name wlan-rrm
[WAC-wlan-rrm-prof-wlan-rrm] airtime-fair-schedule enable
```

在2G射频模板“wlan-radio2g”下引用RRM模板“wlan-rrm”。

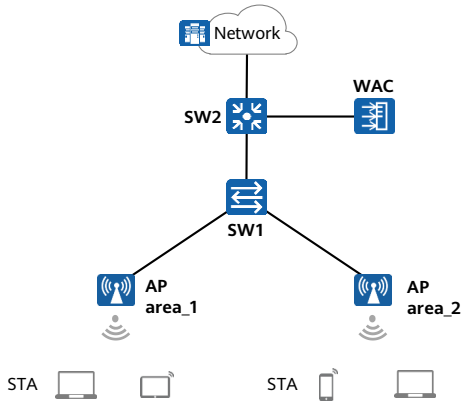
```
[WAC-wlan-view] radio-2g-profile name wlan-radio2g
[WAC-wlan-radio-2g-prof-wlan-radio2g] rrm-profile wlan-rrm
```

在5G射频模板“wlan-radio5g”下引用RRM模板“wlan-rrm”。

```
[WAC-wlan-view] radio-5g-profile name wlan-radio5g
[WAC-wlan-radio-5g-prof-wlan-radio5g] rrm-profile wlan-rrm
```


- 结果验证：在WAC上执行命令**display rrm-profile name wlan-rrm**，可以看到RRM模板中已经使能了Airtime调度功能，因此，用户能够相对公平的占用网络带宽时间。

WLAN QoS配置举例 - 基于ACL的报文过滤



创建ACL 3001，禁止源IP地址为10.23.101.10、目的IP地址为10.23.101.11的报文通过。

[WAC] **acl** *3001*
[WAC-acl-adv-3001] **rule deny ip source** *10.23.101.10 0* **destination** *10.23.101.11 0*

创建名为“wlan-traffic”的流量模板，并引用ACL。

[WAC] **wlan**
[WAC-wlan-view] **traffic-profile name** *wlan-traffic*
[WAC-wlan-traffic-prof-wlan-traffic] **traffic-filter inbound ipv4 acl** *3001*

创建名为“wlan-traffic”的流量模板，并引用ACL。

[WAC-wlan-view] **vap-profile name** *wlan-net*
[WAC-wlan-vap-prof-wlan-net] **traffic-profile** *wlan-traffic*
Warning: This action may cause service interruption. Continue?[Y/N]**y**
[WAC-wlan-vap-prof-wlan-net] **quit**

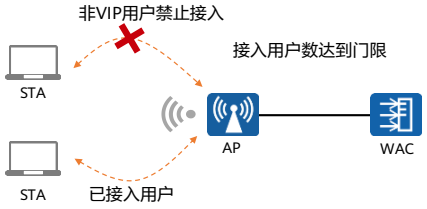
HUAWEI

- 结果验证：在WAC上执行命令**display traffic-profile name wlan-traffic**，可以看到流量模板下已经配置了基于ACL 3001的报文过滤，因此，源IP地址为10.23.101.10、目的IP地址为10.23.101.11的报文将不能通过。

目录

VIP用户优先接入

- 在一些用户密集的场景（如：展会、球场），如果对射频或者VAP的接入用户数不做限制，单个射频或者VAP上接入的用户会很多。这些终端工作在同一信道，由于业务并发叠加、空口竞争等因素的影响，会降低用户的业务体验。
- 通过配置VIP用户优先接入功能，可以实现当接入用户数达到门限时，VIP用户替换已接入的非VIP用户正常接入，优先保障VIP用户的接入体验。



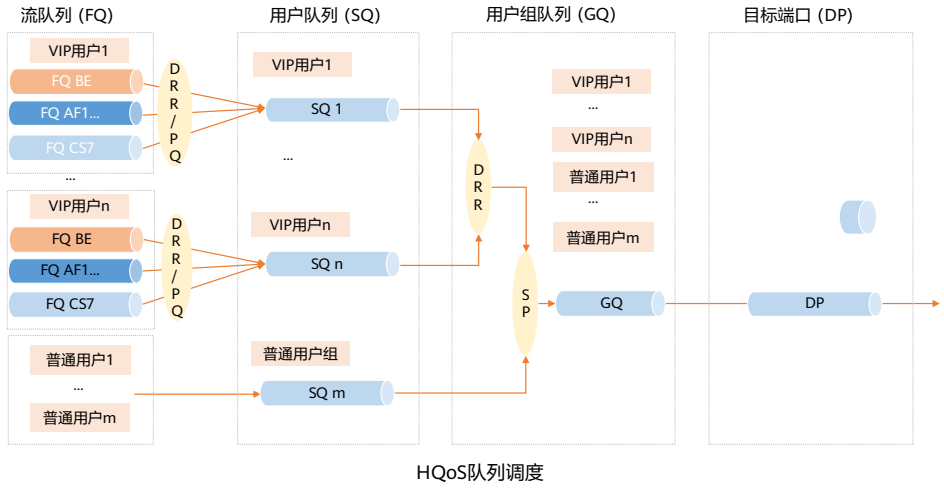
- 设备通过判断用户是否在VIP用户组内来识别是否是VIP用户。用户授权结构增加优先级字段，VIP用户绑定VIP用户组，下发授权后，VIP用户组内的用户继承该优先级。
- 当AP接入用户数达到门限值后，非VIP用户尝试连接AP，无法接入到网络。
- 当AP接入用户数达到门限值后，VIP用户尝试连接AP，AP强制一台已接入的非VIP用户下线，同时VIP用户连接上网络。

VIP用户优先调度

- VIP用户优先调度采用HQoS实现，HQoS即层次化QoS（Hierarchical Quality of Service），是一种通过多级队列调度机制，解决Diffserv模型下多用户多业务带宽保证的问题。HQoS采用多级调度的方式，可以精细区分单个端口下不同无线用户和业务的流量，提供差异化的带宽管理服务。
- WAC侧HQoS：
  - 在WAC上进行HQoS调度时，设备会另外划分队列缓存，用于缓存需要层次化调度的业务流队列，并对这些流队列先进行一轮多层次化调度。目前设备支持流队列FQ（Flow Queue）、用户队列SQ（Subscriber Queue)和用户组队列GQ（Group Queue)。
- AP侧HQoS：
  - HQoS除了在WAC上对无线流量进行多级调度外，在AP上也会进行多级调度。

- 传统的QoS采用一级调度，单个端口只能区分服务等级，无法区分无线用户。属于同一优先级的流量，使用同一个端口队列，不同无线用户的流量彼此之间竞争同一个队列资源，无法对端口上单个无线用户的单个业务流量进行区分服务。HQoS采用多级调度的方式，可以精细区分单个端口下不同无线用户和不同业务的流量，提供差异化的带宽管理服务。

WAC侧HQoS（1）



HQoS队列调度

HUAWEI

- 在WAC上进行HQoS调度时，设备会另外划分队列缓存，用于缓存需要层次化调度的业务流队列，并对这些流队列先进行一轮多层次化调度。目前设备支持流队列FQ (Flow Queue)、用户队列SQ (Subscriber Queue)和用户组队列GQ (Group Queue)。
- 识别VIP用户：
  - 设备通过判断用户是否在VIP用户组内来识别是否是VIP用户。用户授权结构增加优先级字段，VIP用户绑定VIP用户组，下发授权后，VIP用户组内的用户继承该优先级。
- 识别关键应用：
  - 设备通过自带的应用识别功能和应用特征库，就可以识别各种常见应用。用户也可以根据应用的特征自定义一个新的应用。例如将访问特定IP地址和端口的流量定义为自定义应用，就可以对此应用制定优先转发的策略，从而实现该应用的加速。

WAC侧HQoS（2）

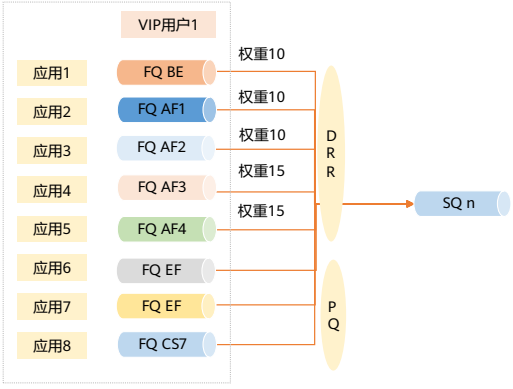
- FQ：FQ用于缓存一个VIP用户的各个服务等级中的一个优先级的数据流。每个VIP用户的数据流都可以根据报文的DSCP/802.1p优先级被划分成1～8个服务等级，即每个VIP用户可以使用8个FQ，分别对应8个服务等级（优先级从低到高分别为BE、AF1、AF2、AF3、AF4、EF、CS6、CS7）。对于关键应用，可以将其优先级适当调高，以保证其能够被优先调度。同时FQ队列也支持流量整形，从而限制每个用户的总带宽。

802.1p优先级	DSCP优先级	服务等级
7	56	CS7
6	48	CS6
5	40、46	EF
4	32、34、36、38	AF4
3	24、26、28、30	AF3
2	16、18、20、22	AF2
1	8、10、12、14	AF1
0	0~7、9、11、13、15、17、19、21、23、25、27、29、31、33、35、37、39、41~45、47、49~55、58~63	BE

DSCP/802.1p优先级到服务等级的映射关系

WAC侧HQoS（3）

- SQ：SQ主要用来区分不同的用户。每一个VIP用户上线时都被分配一个SQ；而所有的普通用户上线时，只会分配到同一个普通用户组SQ（即端口SQ，是WAC设备为每个设备端口预留的SQ）。

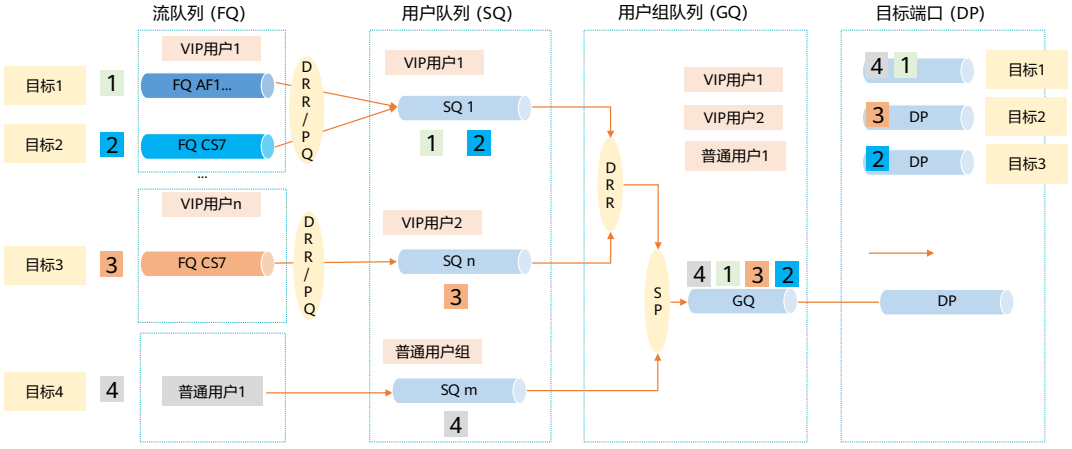


- 对于VIP用户，每个SQ都有8个固定的FQ组成（BE、AF1、AF2、AF3、AF4、EF、CS6、CS7）。在SQ对FQ进行调度时，队列CS7、CS6、EF采用PQ调度，队列AF4、AF3、AF2、AF1、BE采用DRR调度，其中队列AF4、AF3的权重为15，队列AF2、AF1、BE的权重为10。
- 用户可以借助PQ+DRR调度，将重要协议的报文和时延敏感应用的业务报文通过调高优先级放入PQ调度的各队列中，将其他应用按各自的优先级放入采用DRR调度的各队列中，按照权重值对各队列进行循环调度。这样既可以确保能优先调度时延敏感应用的业务报文，又可以避免低优先级队列的报文长期得不到带宽。

WAC侧HQoS（4）

- **用户组队列GQ：**
  - GQ就是多个用户定义为一个组，比如同一个接口下AP的所有用户就被归为一个GQ，因此又被称为端口GQ。一个GQ可以绑定多个SQ，但是一个SQ只能绑定到一个GQ内。在GQ对SQ进行调度时，VIP用户的SQ之间采用的是权重相同的DRR调度；VIP用户SQ与普通用户组SQ之间使用SP调度。
- **目标端口DP：**
  - 目标端口即设备的物理端口，数据最终通过目标端口转发出去。
- **DRR调度：**
  - DRR (Deficit Round Robin)调度中，Deficit表示队列的带宽赤字，初始值为0。每次调度前，系统按权重为各队列分配带宽，计算Deficit值，如果队列的Deficit值大于0，则参与此轮调度，发送一个报文，并根据所发送报文的长度计算调度后Deficit值，作为下一轮调度的依据；如果队列的Deficit值小于0，则不参与此轮调度，当前Deficit值作为下一轮调度的依据。
- **PQ调度：**
  - PQ调度，针对于关键业务类型应用设计，PQ调度算法维护一个优先级递减的队列系列并且只有当更高优先级的所有队列为空时才服务低优先级的队列。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

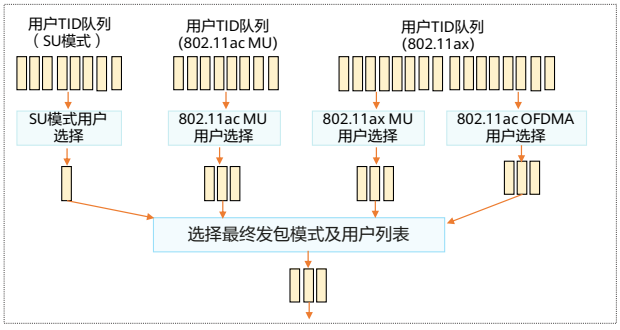
WAC侧HQoS - 举例



HUAWEI

AP侧HQoS（1）

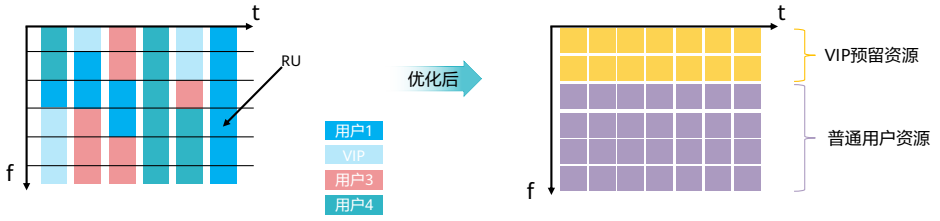
- 识别VIP用户：与WAC的识别过程略有区别，设备根据用户是否在VIP用户组内、最近发包速率和信号强度来识别VIP用户。增加信号强度作为识别VIP用户的条件是为了防止VIP用户速率过低导致拖慢整网速率。
- 识别关键应用：WMM协议定义了一套信道竞争EDCA参数，可以区分高优先级报文并保证高优先级报文优先占用信道资源。



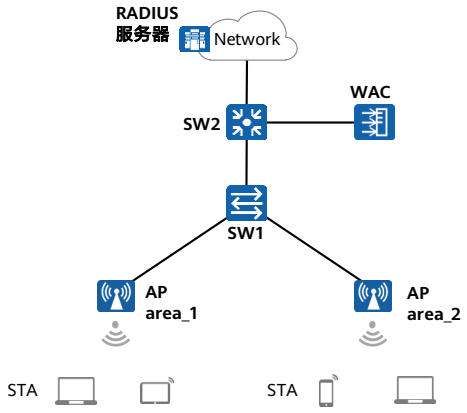
- 不同的发包模式（SU/802.11ac MU/802.11ax MU/802.11ax OFDMA等），计算出本模式下的所有TID计算权重。
- 每种发包模式将所计算的权重值按照从高至低的顺序进行排序，并选择其中最高的1个（SU模式）或多个（MU模式）用户作为该模式的调度用户列表。
- 将各发包模式生成的调度结果进行汇总，选择权重最高的用户所使用发包模式作为发包模式，生成最终的调度结果（参与发包的STA列表）。

AP侧HQoS（2）

- VIP用户带宽保障：
  - 通过对VIP用户和普通用户时域资源的精细化分配，主要是精确分配VIP用户和普通用户的空口发送机会，保证VIP用户发送优先级，从而使得VIP用户可以享受更优的空口带宽。
- VIP用户空口带宽预留：
  - VIP用户空口带宽预留算法基于802.11ax灵活的时域和频域资源分配实现，实时评估用户实际需要的时频资源，通过为VIP用户预留/分配满足其业务需要的时频资源，从而保证VIP用户的体验。



VIP用户优先接入举例 - 配置VIP用户优先级

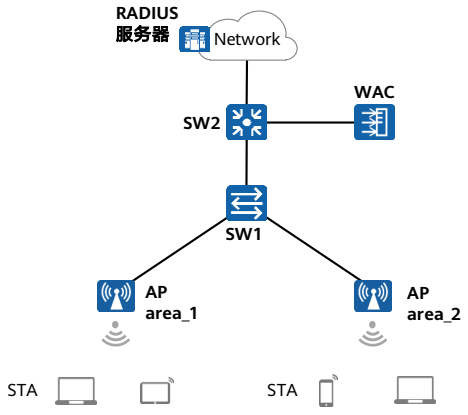


配置用户组的优先级为“1”，标记用户组为VIP用户组。

```
[WAC] user-group vip_group
[WAC-user-group-vip_group] priority 1
```


HUAWEI

VIP用户优先接入举例 - 基于用户数CAC的VIP用户优先接入



创建RRM模板，并在RRM模板下打开基于用户数的用户CAC功能，并配置接入用户数阈值为32，配置用户接入数达到基于用户数的CAC门限时，新用户基于优先级替换接入功能。

```
[AC-wlan-view] rrm-profile name wlan-rrm
[WAC-wlan-rrm-prof-wlan-rrm] uac client-number enable
[WAC-wlan-rrm-prof-wlan-rrm] uac client-number threshold access 32
[WAC-wlan-rrm-prof-wlan-rrm] uac reach-access-threshold priority-replace
```

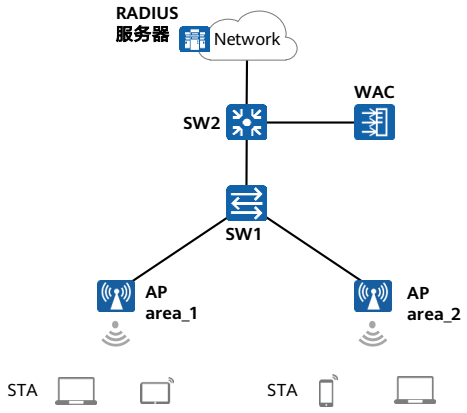
创建2G/5G射频模板，并在该模板下引用RRM模板“wlan-rrm”。

```
[WAC-wlan-view] radio-2g-profile name wlan-radio2g
[WAC-wlan-radio-2g-prof-wlan-radio2g] rrm-profile wlan-rrm
```

在名为“ap-group1”的AP组下引用射频模板。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] radio-5g-profile wlan-radio5g radio 1
Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-ap-group-ap-group1] radio-2g-profile wlan-radio2g radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
```

VIP用户优先接入举例 - 基于VAP的VIP用户优先接入



配置单个VAP下能够关联成功的最大用户数为40，配置用户接入数达到单个VAP下能够接入的最大用户数门限时，新用户基于优先级替换接入功能。

```
[WAC-wlan-view] ssid-profile name wlan-net
[WAC-wlan-ssid-prof-wlan-net] max-sta-number 40
[WAC-wlan-ssid-prof-wlan-net] reach-max-sta priority-replace
```


HUAWEI

- 配置完成后需在服务器上配置VIP用户及VIP用户组授权信息。
- 检查配置结果：
  - 执行命令display user-group vip_group，查看VIP用户组的配置信息，可以看到“vip_group”用户组的优先级为“1”。
  - 执行命令display rrm-profile name wlan-rrm，查看RRM模板的配置信息，可以看到用户接入数达到基于用户数的用户CAC门限时，新用户的接入策略为基于优先级替换接入。
  - 执行命令display ssid-profile name wlan-net，查看SSID模板配置信息，可以看到用户接入数达到单个VAP下能够接入的最大用户数门限时，新用户的接入策略为基于优先级替换接入。

思考题

1. 华为射频调优方案主要应用场景有哪些?
2. 华为WLAN QoS技术主要解决了什么问题?
3. 华为VIP用户体验保障功能主要应用场景是什么？技术实现是怎样的?

HUAWEI

- 开局部署、日常运维、新增AP、AP退服、非法AP干扰、非Wi-Fi设备干扰。
- 不同的应用需求对于网络的要求是不同的，原始的WLAN网络由于速率较低，更多的应用在普通的数据传输。随着WLAN技术的快速发展和广泛应用，WLAN技术逐渐地应用到媒体、金融、教育机构以及企业网络中，WLAN网络中的流量除了普通的数据，还包括延时性要求较高的多媒体数据，例如语音、视频等。通过WLAN QoS，网络管理者根据各种业务的特点来对网络资源进行合理的规划和分配，从而为不同的应用提供不同质量的接入服务，以满足用户需求，同时提高网络资源的利用率。
- 1）在一些用户密集的场景（如：展会、球场），如果对射频或者VAP的接入用户数不做限制，单个射频或者VAP上接入的用户会很多。这些终端工作在同一信道，由于业务并发叠加、空口竞争等因素的影响，会降低用户的业务体验。对于这些场景，通常会限制射频或者VAP的用户接入数，一旦达到最大接入用户数，则不再允许新用户接入，但是同时会导致VIP用户也无法正常接入，降低了VIP用户的用户体验。
- 2）VIP用户优先接入：在设备上配置VIP用户优先接入，当接入用户数达到VAP最大用户数或用户CAC门限时，如果再有新用户接入到网络，该用户先进行认证，认证成功后，在授权阶段判断该用户是否是VIP用户，如果是，则允许该用户接入并替换一个非VIP用户，强制该非VIP用户下线；如果不是，则强制该用户下线。VIP用户优先调度：通过HQoS即层次化QoS技术解决了VIP用户业务带宽保证的问题。

本章总结

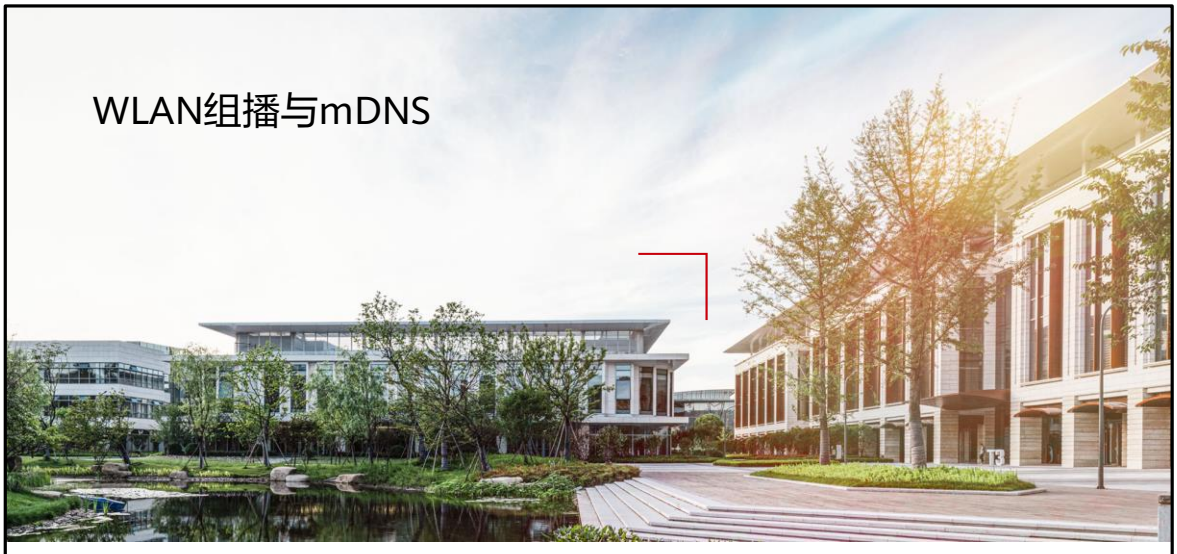
- 本章介绍了华为射频资源管理方案，通过自动检查周边无线环境、动态调整信道和发射功率等射频资源、智能均衡用户接入、提供差分服务、保障VIP用户体验，从而调整无线信号覆盖范围，降低射频信号干扰，使无线网络能够快速适应无线环境变化，提升用户体验。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

WLAN组播与mDNS



HUAWEI

前言

- IP组播技术有效地解决了单点发送、多点接收的问题，实现了IP网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。作为一种与单播和广播并列的通信方式，组播的意义不仅在于此。更重要的是，可以利用网络的组播功能方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等互联网的信息服务领域。
- 本课程系统地介绍了IP组播的基本概念，在此基础上介绍了在WLAN网络中部署组播业务的注意事项，以及涉及的相关技术，包括WLAN组播网络优化技术、mDNS、mDNS网关等。

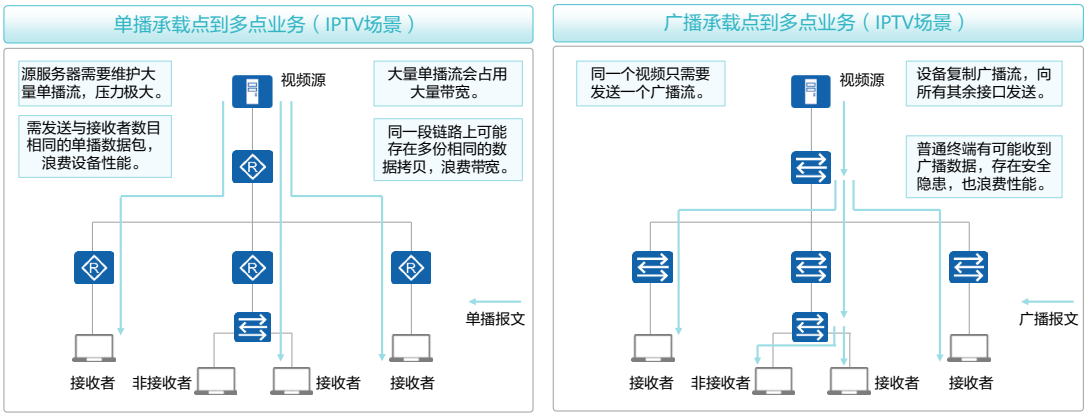
目标

- 学完本课程后，您将能够：
  - 描述IP组播的基本概念
  - 描述WLAN网络中部署组播时所涉及的相关技术及其原理
  - 描述mDNS的基本原理
  - 描述mDNS网关的基本概念及工作原理、部署mDNS网关或进行策略控制

目录

点到多点业务的困境

- 点到多点业务可以由单播，组播，广播进行承载，现网中也有各种各样的实现方式。但使用单播或者广播承载点到多点业务时会存在以下问题。

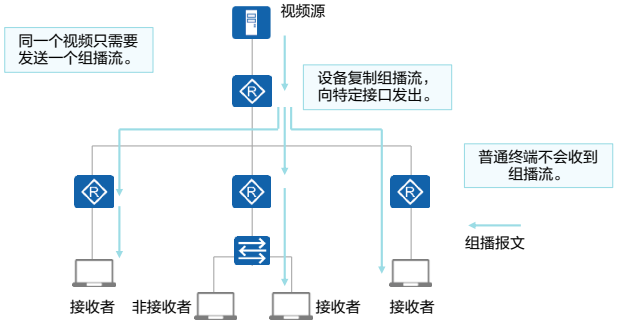


HUAWEI

- 单播（Unicast）是在一台源IP主机和一台目的IP主机之间进行。网络上绝大部分的数据都是以单播的形式传输的，例如电子邮件收发、网上银行都是采用单播实现的。
  - 在单播通信中每一个数据包都有确切的目的IP地址；对于同一份数据，如果存在多个接收者，Server需发送与接收者数目相同的单播数据包；当接收者增加到成百上千时，将极大加重Server创建相同数据和发送多份相同拷贝后所产生的消耗，网络中的设备性能及链路带宽都会面临一定程度的浪费；单播方式较适合用户稀少的网络，当用户量较大时很难保证网络传输质量。
- 广播（Broadcast）是在一台源IP主机和网络中所有其它的IP主机之间进行，属于一对所有的通讯方式，所有主机都可以接收到（不管是否需要）。
  - 广播数据包被限制在广播域中；一旦有设备发送广播数据，则广播域内所有设备都会收到这个数据包，并且不得不耗费资源去处理，大量的广播数据包将消耗网络的带宽及设备资源；广播方式只适合共享网段，且信息安全性和有偿服务得不到保障。

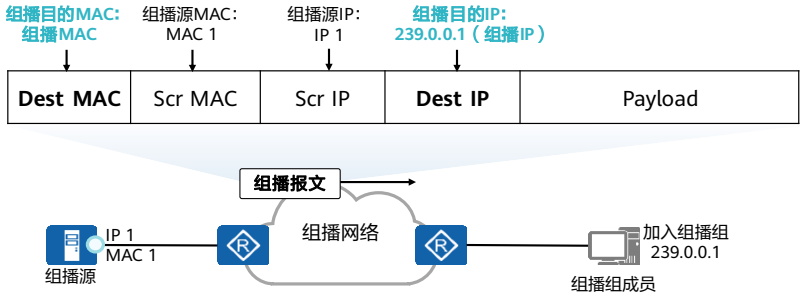
使用组播承载点到多点业务

- 组播方式下，单一的信息流沿组播分发树被同时发送给一组用户，相同的组播数据流在每一条链路上仅有一份。相比单播和广播，使用组播的好处如下：
  - 相比单播，用户的增加不会导致信息源负载的加重，不会导致网络资源消耗的显著增加。
  - 相比广播，不会造成网络资源的浪费，并能提高信息传输的安全性，而且组播可以实现跨网段的传输。



组播报文结构

- 组播数据报文的结构与单播报文类似，但组播数据报文的目的MAC地址与目的IP地址与单播报文有很大差异。
  - 组播目的IP地址：目的IP地址为组播IP地址，地址范围从224.0.0.0到239.255.255.255。
  - 组播目的MAC地址：目的MAC地址为组播MAC地址，组播MAC地址由组播IP地址映射而来。



组播IP地址

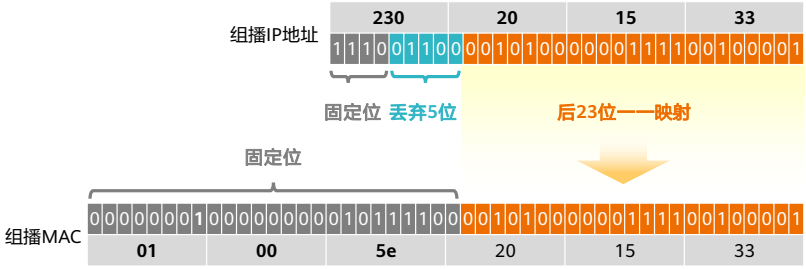
- 在IPv4地址空间中，D类地址（224.0.0.0/4）被用于组播。组播IP地址被用于标识组播组。
- 大多数情况下，同一个组播网络里不同的业务（比如，IPTV，语音会议）需要使用不同的组播IP地址。
- IANA对D类地址做了进一步的定义，几种主要的组播地址如下表所示：

范围	含义
224.0.0.0—224.0.0.255	为路由协议预留的永久组地址
224.0.1.0—231.255.255.255 233.0.0.0—238.255.255.255	Any-Source临时组播组地址
232.0.0.0—232.255.255.255	Source-Specific临时组播组地址
239.0.0.0—239.255.255.255	本地管理的Any-Source临时组播组地址

- IPv4组播地址：
  - IPv4地址空间分为五类，即A类、B类、C类、D类和E类。D类地址为IPv4组播地址，范围是从224.0.0.0到239.255.255.255，用于标识组播组，且仅能作为组播报文的目的地址使用，不能作为源地址使用。
  - IPv4组播报文的源地址字段为IPv4单播地址，可使用A、B或C类地址，不能是D类、E类地址。
  - 在网络层上，加入同一组播组的所有用户主机能够识别同一个IPv4组播组地址。一旦网络中某用户加入该组播组，则此用户就能接收以该组地址为目的地址的IP组播报文。

组播MAC地址

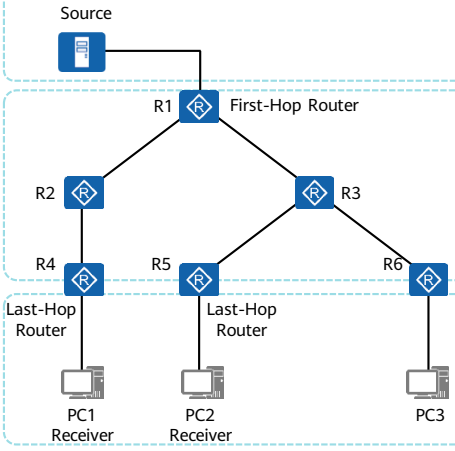
- 对于单播报文，其目的MAC地址是链路上目标节点的地址。但是对于组播报文，其目的地可能是多个接收者，因此，组播MAC地址被用于在数据链路层标识对应的组播组接收者（组成员）。
- IANA规定，IPv4组播MAC地址的高24位为0x01005e，第25位为0，低23位为IPv4组播地址的低23位，例如组播组地址239.20.15.33对应的组播MAC地址为01-00-5e-20-15-33。



HUAWEI

- IPv4组播地址的前4位是固定的1110，对应组播MAC地址的高25位，后28位中只有23位被映射到MAC地址，因此丢失了5位的地址信息，直接结果是有32个IPv4组播地址映射到同一MAC地址上。例如IP地址为224.0.1.1、224.128.1.1、225.0.1.1、239.128.1.1等组播组的组播MAC地址都为01-00-5e-00-01-01。网络管理员在分配地址时必须考虑这种情况。
- IETF认为同一个局域网中两个或多个组地址生成相同的MAC地址的几率非常低，不会造成太大的影响。
- 组播MAC地址标识了一组设备，这种MAC地址第1个字节的最低比特位为1，例如0100-5e-00ab。
- 一个组播MAC地址所标识的一组设备有着共同的特点，那就是它们都加入了相同的组播组，这些设备将会侦听目的MAC地址为该组播MAC地址的数据帧。只有单播MAC地址才能够被分配给一个以太网接口，组播或广播MAC地址是不能被分配给任何一个以太网接口的，换句话说，这两种类型的MAC地址不能作为数据帧的源MAC地址，而只能作为目的MAC地址。
- 对于组播MAC地址，相信大家并不会太陌生，例如STP协议的BPDU载荷便是被直接封装在以太网数据帧中的，并且数据帧的目的MAC地址为0180-c200-0000，这就是一个组播MAC地址，类似这样的例子还有很多，此处不再一一列举，这些组播MAC地址并不与组播IP地址存在关联。
- 除此之外，还有一类组播MAC地址是我们需要格外关注的，那就是与组播IP地址存在映射关系的组播MAC地址。本课程介绍的组播MAC地址对应该类型。

组播网络基本架构



源端网络：发送组播数据至组播网络。

无需任何信令协议

组播转发网络：形成无环的组播转发路径，该转发路径也被称为组播分发树(Multicast Distribution Tree)。

组播路由协议
例如PIM等等

成员端网络：感知组播组成员位置与加入的组播组。

组成员管理协议
IGMP

HUAWEI

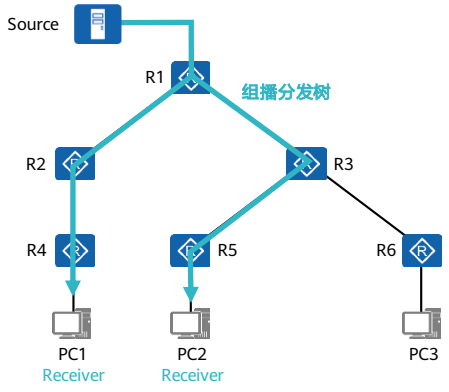
- 组播源（Source）：组播流量的发送者，例如多媒体服务器。组播源无需运行任何组播协议，只需简单地将组播数据发送出来即可。
- 组播接收者（Receiver）：也被称为组播组成员，是期望接收特定组播组流量的设备，例如运行多媒体直播客户端软件的PC。
- 组播组（Multicast Group）：用IP组播地址进行标识的一个集合。任何用户主机（或其他接收设备），加入一个组播组，就成为了该组成员，可以识别并接收发往该组播组的组播数据。
- 组播路由器（Multicast Router）：支持组播、运行组播协议的网络设备，实际上不仅仅路由器能够支持组播，交换机、防火墙等设备也能够支持组播（取决于设备型号），路由器仅是一个代表。
- 第一跳路由器（First-Hop Router）：组播转发路径上，与组播源相连且负责转发该组播源发出的组播数据的路由器。
- 最后一跳路由器（Last-Hop Router）：组播转发路径上，与组播组成员相连且负责向该组成员转发组播数据的路由器。
- IGMP（Internet Group Management Protocol，因特网组管理协议），是TCP/IP协议族中负责IP组播成员管理的协议，它用来在接收者和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

组播路由协议概述

- 组播路由协议：建立并维护组播路由表，以便实现组播数据转发。

组播路由协议的作用：

- 在接收组播报文时，判断该报文是否在正确的接口上到达，从而确保组播数据转发的无环化。
- 在网络中建立一棵组播分发树（组播流量转发的路径树）。
- 组播分发树体现在每一台组播路由器上便是组播转发表项。



HUAWEI

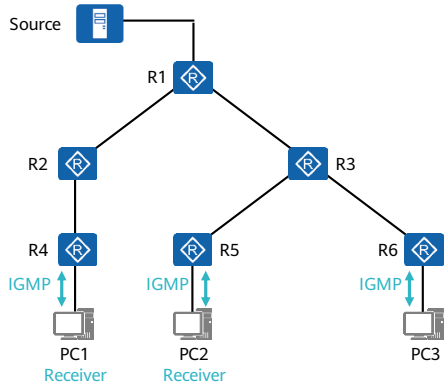
- 单播数据包的转发，就是一个一对一的模型，路由器将IP数据包送到它的目的地，单播路由器并不关心数据包的源地址。而组播数据是由组播源产生，发向一组接收者，组播路由器将数据包从源分发下去，一直到组播的接收者。那么组播路由器如何知道，该将组播数据向哪里去转发，哪些地方需要组播流量？组播流量要走什么路径？这就要用到组播路由协议了。
- 组播流量与单播流量不同，组播流量发往一组接收者，如果网络中有环路存在，那么情况比单播环路严重得多，因此所有的组播路由器必须知道组播的源，也必须把组播数据包从源（来的方向）向目标转发。
- 为了保证数据从上游转发到下游，每一个组播路由器都维护一个组播前传表（组播路由表）。
- 单播路由协议确定去往某个目的的最短（最优）路径，它不会关心数据的源；而组播路由协议必须去判断上游接口（离源更近的接口）。

IGMP概述

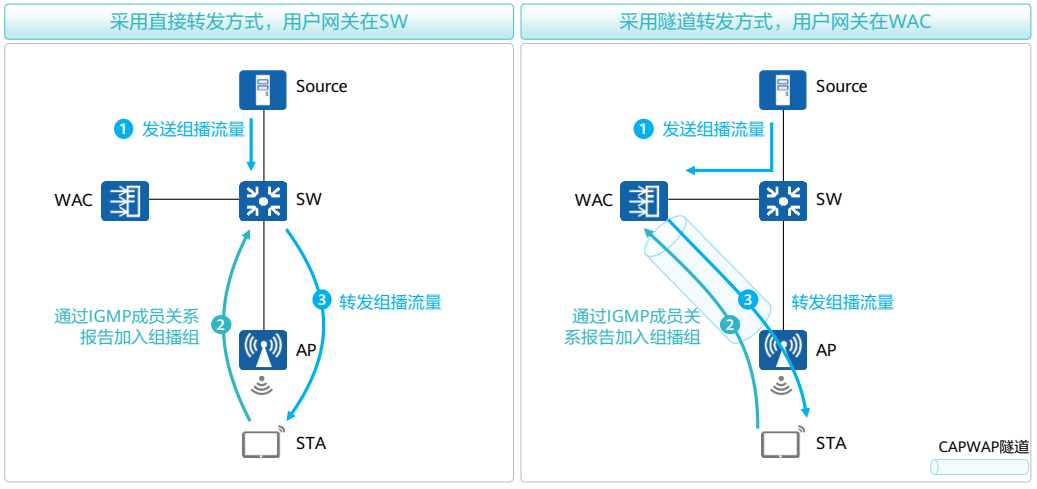
- IGMP是TCP/IP协议族中负责IPv4组播成员管理的协议，用来在接收者和与其直接相邻的组播路由器之间建立和维护组播组成员关系。
- 协议版本：IGMPv1、IGMPv2及IGMPv3。

IGMP的作用：

- IGMP用于主机（组播成员）和最后一跳路由器之间。
- 主机使用IGMP报文向路由器申请加入和退出组播组。默认时路由器是不会向接口下转发组播数据流的，除非该接口上存在组成员。
- 路由器通过IGMP查询网段上是否有组播组的成员。



WLAN网络中的组播部署场景



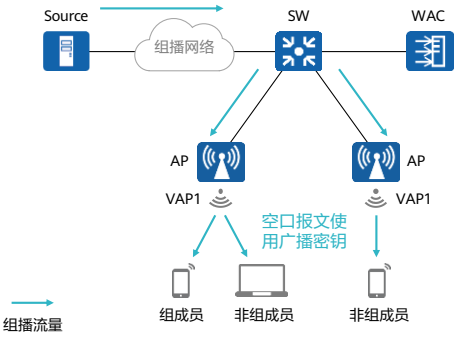
HUAWEI

- 采用直接转发方式，用户网关在SW。
  - SW需激活IP组播路由功能、并激活IGMP。
  - SW维护组播转发表、维护组成员关系，收到组播流量后，向组播组成员进行转发。
- 采用隧道转发方式，用户网关在WAC。
  - WAC需激活IP组播路由功能、并激活IGMP。
  - WAC维护组播转发表、维护组成员关系，收到组播流量后，向组播组成员进行转发。

目录

IGMP Snooping (1)

- IGMP Snooping (Internet Group Management Protocol Snooping)是一种二层组播技术，通过侦听三层组播设备和用户主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文在数据链路层的转发。



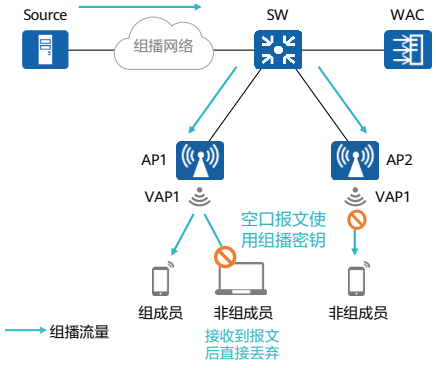
使能IGMP Snooping前

当组播数据从三层组播设备转发下来以后，处于接入边缘的二层组播设备AP负责将组播数据转发给用户主机，使用户收看所点播的节目；

当AP没有运行IGMP Snooping时，组播数据在二层被广播。

IGMP Snooping (2)

- 对于AP1而言，使能IGMP Snooping的AP1在收到上游发来的组播数据后，在空口使用组播密钥对数据进行转发，该AP下所关联的终端都会在空口收到组播数据，但是未加入该组播组的终端收到数据后，将其直接丢弃，避免了性能浪费。



使能IGMP Snooping后

使能IGMP Snooping功能后，AP会侦听主机和上游三层设备之间交互的IGMP报文，通过分析报文中携带的信息（报文类型、组播组地址、接收报文的接口等），建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发。

HUAWEI

- 在本例中，AP2所部署的VAP业务中，没有任何组播组的成员，因此在使能IGMP Snooping后，AP2从SW收到发往组播组的流量后，不会向空口进行转发。

IGMP Snooping关键配置

- 在流量模板下使能IGMP Snooping功能，并配置相关参数。该流量模板可被关联至VAP模板，并下发给AP执行。

```
[WAC] wlan
[WAC-wlan-view] traffic-profile name default
[WAC-wlan-view-traffic-prof-default] igmp-snooping enable
[WAC-wlan-view-traffic-prof-default] quit
#
[WAC-wlan-view] vap-profile name default
[WAC-wlan-vap-prof-default] traffic-profile default
```


- igmp-snooping enable命令用于开启二层组播业务，为了保证组播业务体验，建议在AP系统模板视图下关闭组播报文限速功能 (traffic-optimize broadcast-suppression other-multicast disable)。

组播转单播概述及应用场景

- 组播转单播功能：AP通过侦听用户上报的IGMP成员关系报告报文和离开报文来维护组播转单播表项。当AP向客户端发送组播报文时，根据组播转单播表项，将组播数据报文转换为单播数据报文，从而提高组播数据流传输效率。
- 组播转单播自适应功能：开启该功能后，当组播转单播出现空口性能瓶颈时，AP自动将终端数最少的组播组切换为组播模式，当空口性能改善持续一段时间后，AP自动将终端数最多的组播组切换为单播模式，从而在不需要人工干预的情况下，自动调整空口性能，提升整体无线用户体验。

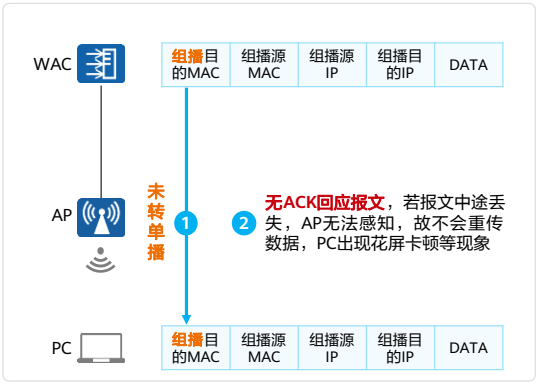
电子书包场景

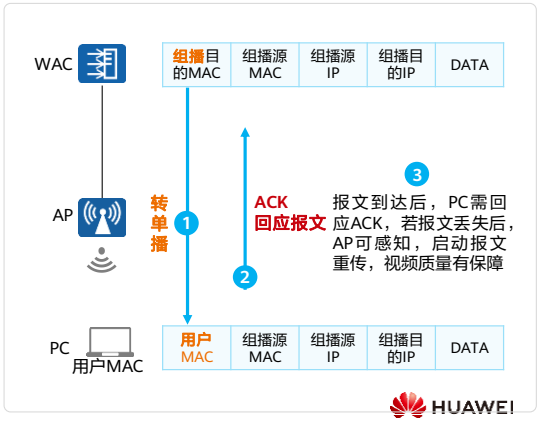
- 教室内部署一台AP提供WLAN接入功能，学生一人一平板电脑，平板电脑通过WLAN接入网络，接收网络中组播教学服务器的数据。
- 组播转单播功能及组播转单播自适应功能可用于该场景改善组播业务体验。

- 空口组播报文无ACK机制，易丢包，会造成无线用户点播组播视频时易花屏，为了满足某些对组播流传输有较高要求的应用，如高清视频点播，用户可以开启组播转单播功能。

组播转单播技术原理

- 在AP上侦听组播协议报文，建立组播转单播表项，表项中记录了用户MAC（单播MAC），组播数据报文查表转发，并将目的MAC由组播MAC替换为用户MAC，即将组播报文转换成单播报文发给用户，达到降低丢包率的目的。





组播转单播关键配置

- 在流量模板下使能组播转单播功能。

```
[WAC] wlan
[WAC-wlan-view] traffic-profile name default
[WAC-wlan-view-traffic-prof-default] traffic-optimize multicast-unicast enable
[WAC-wlan-view-traffic-prof-default] undo traffic-optimize multicast-unicast dynamic-adaptive disable
```

组播CAC

- 随着IPTV业务发展，组播业务急剧增加，在二层网络中部署IPTV业务时，有可能会存在下列问题：
  - 当网络上有大量用户使用组播业务时，会导致资源不足时，服务质量大幅下降。
  - 当网络带宽不足时，带宽无法承受所有的组播流量，用户画面质量会变差。
- 二层组播CAC限制就是针对上述问题制定的一种解决方法。
- CAC（Call Admission Control)称为接入管理控制。二层组播CAC是指通过一系列规则来进行组播用户接入控制，保证整体组播业务的可用性。

组播CAC原理

基于组播带宽的组播用户接入控制

- 当组播带宽不足时，限制新用户接入组播组。
- 如果用户同时配置了全局和VAP的基于组播带宽的组播用户接入控制：
  - 当用户数据报文直接转发时，组播带宽占用只在VAP体现，因此配置的全局基于组播带宽的组播用户接入控制不生效。
  - 当用户数据报文隧道转发时，配置的全局和VAP的基于组播带宽的组播用户接入控制都生效。全局或VAP的组播带宽不足均会限制新用户接入。

基于组播组点播数的组播用户接入控制

- 当组播组点播数达到最大值时，限制新用户接入组播组。
- 如果用户同时配置了全局和VAP的基于组播组点播数的组播用户接入控制：
  - 当用户数据报文直接转发时，配置的全局基于组播组点播数的组播用户接入控制不生效。
  - 当用户数据报文隧道转发时，配置的全局和VAP的基于组播组点播数的组播用户接入控制都生效。全局或VAP的组播组点播数达到最大值均会限制新用户接入。

- 用户可以配置基于组播带宽的组播用户接入控制或基于组播组点播数的组播用户接入控制，这两种方式无依赖关系，可以独立使用，也可以叠加使用。

组播CAC - 关键配置

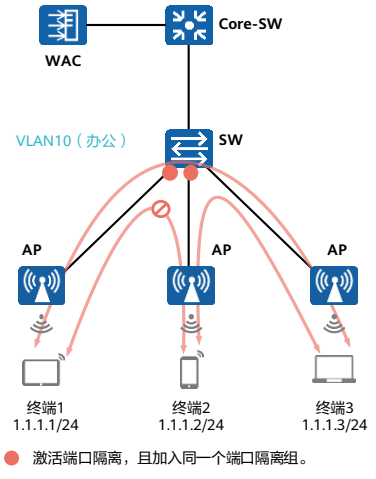
- 基于组播带宽的组播用户接入控制，配置VAP最大组播带宽。

```
[WAC] wlan
[WAC-wlan-view] traffic-profile name default
[WAC-wlan-view-traffic-prof-default] igmp-snooping max-bandwidth max-bandwidth
```

- 基于组播组点播数的组播用户接入控制，配置VAP最大组播组点播数。

```
[WAC] wlan
[WAC-wlan-view] traffic-profile name default
[WAC-wlan-view-traffic-prof-default] igmp-snooping max-user max-user
```

端口隔离



需求

- 实现同一个VLAN内不同用户之间的隔离，加强用户通信安全，避免无效的广播报文影响业务。
- 实现同一个VLAN内不同用户之间交互的数据能够通过上层设备集中转发。

方案

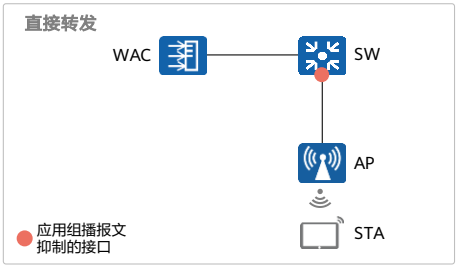
- 采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。
- 只需将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。
- 端口隔离分为二层隔离三层互通和二层三层都隔离两种模式：
  - 如果用户希望隔离同一VLAN内的广播报文，但是不同端口下的用户还可以进行三层通信，则可以将隔离模式设置为二层隔离三层互通。
  - 如果用户希望同一VLAN不同端口下用户彻底无法通信，则可以将隔离模式配置为二层三层均隔离。

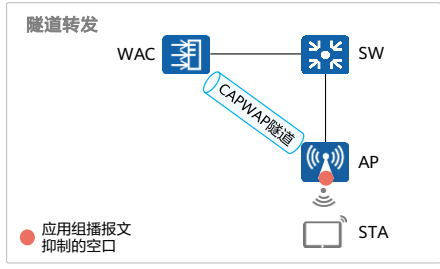
HUAWEI

- 端口隔离功能为用户提供了更安全、更灵活的组网方案。
- 端口隔离可搭配ARP代理功能使用。在某些场景中，我们可能希望同一个VLAN内的终端之间交互的数据通过上层设备集中转发，而不是直接通过接入层交换机交互，这样可以确保流量不会通过接入层交换机直接交互，而必须经由上层设备转发，便于在上层设备部署流量管控策略，我们将这种模式称为集中转发模式。对于集中转发模式，由于下行二层设备都配置了端口隔离，需要核心网关上配置对应的ARP代理，一般采用的是VLAN内ARP代理。

组播报文抑制

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵，终端上网速率慢。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在WAC的流量模板下配置组播报文抑制。





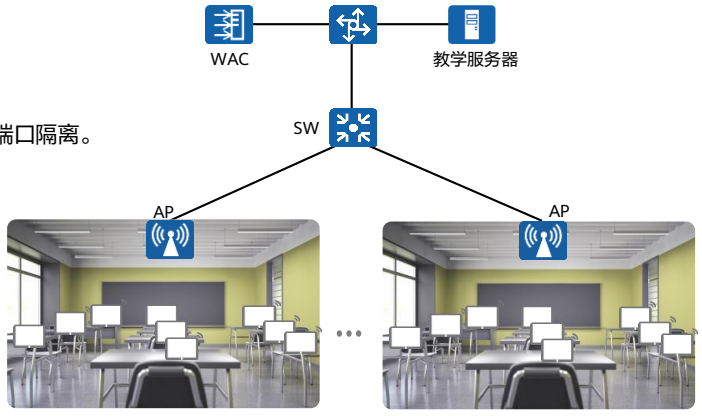
组播报文抑制功能配置示例

- 配置允许通过的最大组播报文的流量为100 pps，如果有组播业务，建议按照业务流量来进行流量限制。

```
[WAC] wlan
[WAC-wlan-view] traffic-profile name test
[WAC-wlan-traffic-prof-test] traffic-optimize multicast-suppression packets 100
```

WLAN组播网络优化应用在电子书包场景

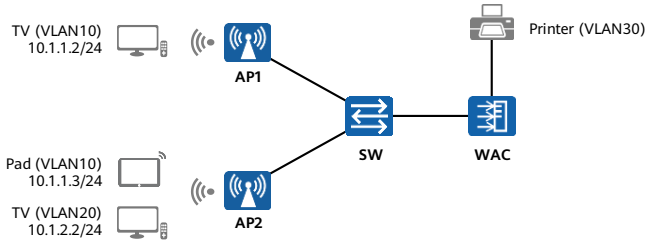
- WLAN组播网络优化手段：
  - 配置组播报文抑制功能。
  - 配置组播转单播功能。
  - 在与AP直连的设备接口上配置端口隔离。



目录

mDNS技术背景

- 传统的基于TCP/IP协议的通信模式下，如果设备之间需要通信，必须知道对端设备的IP地址。
- 由于IP地址不便记忆，为了提升可用性，网络管理员可以配置DNS服务以方便其他设备通过域名访问网络资源。当一个设备通过域名访问其他设备时，需要通过DNS服务器用来解析域名对应的IP地址，在某些低成本的网络中，部署DNS服务器的成本较高。为了减少网络设备的手工配置成本，苹果公司提出了零配置网络Zeroconf (Zero-configuration networking)。

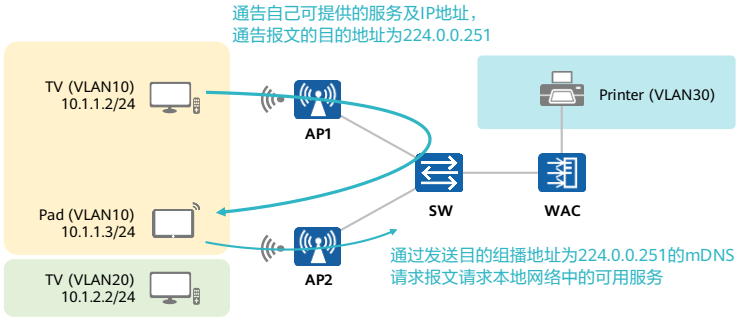


HUAWEI

- 零配置网络是指网络设备在不需要管理员参与配置的情况下，实现自动地址配置、域名解析和服务发现，广泛应用在家庭无线网络和企业办公网络中。

mDNS

- Bonjour技术是基于组播域名系统mDNS (Multicast Domain Name System)和基于DNS的服务发现协议DNS-SD (DNS-Based Service Discovery)的零配置网络技术的解决方案，是一种应用在二层广播域的技术，实现二层广播域内网络设备自动获取地址和发现服务。

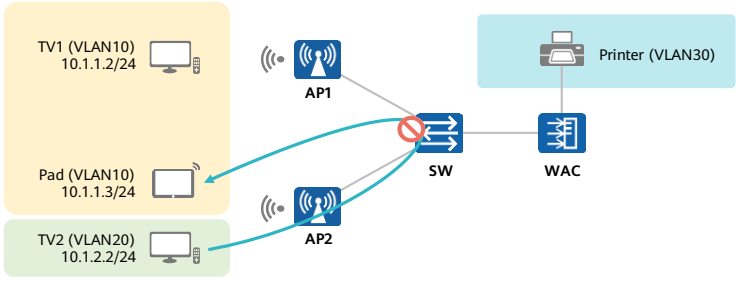


HUAWEI

- 使用Bonjour技术的服务提供设备（例如Apple TV）通过组播地址（IPv4地址为224.0.0.251）在网络中宣布自己可以提供的服务。用户终端设备（例如iPhone、iPad等客户端）通过发送目的组播地址为224.0.0.251的mDNS请求报文请求本地网络中的可用服务。通过这种方式，一方面实现了网络中的服务共享，另一方面方便客户端能够访问网络中的服务资源。
- 然而，mDNS协议进行信息交互时使用的目的组播地址（224.0.0.251）仅在二层广播域生效，即只能在同一VLAN内转发，不能实现跨VLAN或跨三层设备转发。

mDNS网关概述

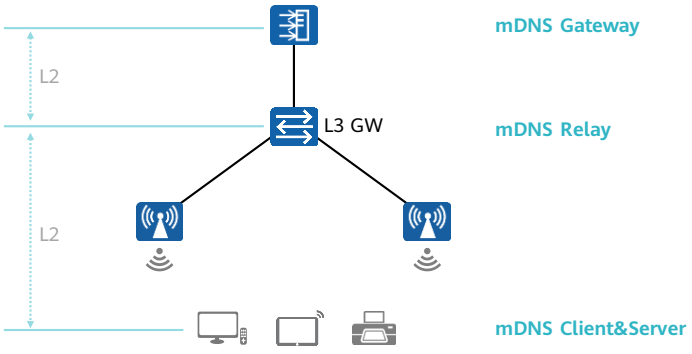
- Bonjour技术仅能实现同VLAN内的服务发现，为了实现跨VLAN的服务发现，华为公司提出了mDNS网关的解决方案。mDNS网关应用在苹果公司提出的Bonjour技术解决方案中，记录网络中所有可用的打印机和Airplay服务列表，并应答支持Bonjour技术的用户终端的服务请求，这样，支持Bonjour技术的用户终端可以实现跨VLAN和跨网段的服务发现。



HUAWEI

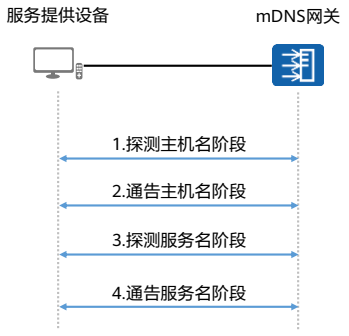
- 华为公司提出了mDNS网关的解决方案，通过在WAC上部署mDNS网关，可以实现跨VLAN的服务发现。WAC上部署mDNS网关后，WAC设备下挂的直连网段的服务提供设备（图中的TV1、TV2及Printer）以组播形式发送mDNS报文通告服务，WAC收到报文后记录服务信息。客户端（图中的Pad）发送mDNS请求报文发现服务时，WAC收到请求报文后通过查询服务列表回应网络中可用的服务，从而实现了跨VLAN的服务发现。
- 在mDNS网关的解决方案中，需要服务提供设备与WAC之间处于同一网段。如果WAC作为mDNS网关与提供服务的设备或终端跨网段连接，即Swich和WAC之间是三层网络，VLAN10和VLAN20的mDNS消息不能被SW转发到mDNS网关，因此mDNS网关上不能记录VLAN10和VLAN20内提供的服务。通过在SW上部署mDNS中继，可以解决这个问题，实现跨网段的服务发现。

mDNS网络中可能涉及的网元



HUAWEI

mDNS网关原理 - 服务提供设备通告服务

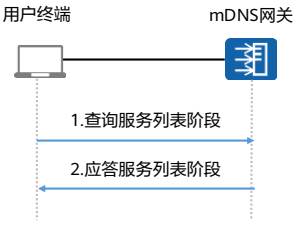


- 服务提供设备上电启动后，自动生成一个主机名，并发送目的组播地址为224.0.0.251的mDNS请求报文探测主机名是否与其他服务提供设备重复，以确保主机名在网络中唯一。
- 服务提供设备以组播方式发送mDNS报文通告其主机名和IP地址，mDNS网关收到请求报文后记录此主机名和IP地址信息。
- 服务提供设备发送目的组播地址为224.0.0.251的mDNS请求报文探测服务名是否与其他服务提供设备重复，以确保服务名在网络中唯一。
- 服务提供设备以组播方式发送mDNS报文通告其服务信息，mDNS网关收到请求报文后记录此服务信息，包括服务名、服务类型、TTL值、主机名和IP地址。

- 服务提供设备把所能提供的服务通告给mDNS网关，这样，mDNS网关就能记录网络中所有可用的服务信息。主机名用来标识服务提供设备。服务名用来标识设备所能提供的服务和记录服务类型。
- 服务提供设备上电启动后，自动生成一个主机名，并发送目的组播地址为224.0.0.251的mDNS请求报文探测主机名是否与其他服务提供设备重复，以确保主机名在网络中唯一。mDNS网关收到探测报文后查询本地记录的主机名列表，如果存在此主机名，表示网络中已经有其他服务提供设备使用此名字，则发送冲突报文给服务提供设备。服务提供设备收到冲突报文后生成一个新的主机名，重新进行探测。如果在探测时间内没有收到mDNS网关的冲突回应报文，表示主机名可用。如果在探测时间内持续冲突，则在下一探测时间继续发送请求报文。
- 服务提供设备以组播方式发送mDNS报文通告其主机名和IP地址，mDNS网关收到请求报文后记录此主机名和IP地址信息。
- 服务提供设备发送目的组播地址为224.0.0.251的mDNS请求报文探测服务名是否与其他服务提供设备重复，以确保服务名在网络中唯一。mDNS网关收到探测报文后查询本地记录的服务信息列表，如果存在此服务名，表示网络中已经有其他服务提供设备使用此服务名，则发送冲突报文。服务提供设备收到冲突报文后生成一个新的服务名，重新进行探测。如果在探测时间内没有收到mDNS网关的冲突回应报文，表示服务名可用。如果在探测时间内持续冲突，则在下一探测时间继续发送请求报文。
- 服务提供设备以组播方式发送mDNS报文通告其服务信息，mDNS网关收到请求报文后记录此服务信息，包括服务名、服务类型、TTL值、主机名和IP地址。
- mDNS服务提供设备在其网段内发送组播的服务相关mDNS报文，Relay设备通过ACL规则抓取收到的组播mDNS的报文，除了按照原来的组播处理规则在本地继续转发外，还要复制一份报文，并修改这些报文的源地址和目的地址，采用单播的方式发送给mDNS Gateway，由mDNS Gateway记录并登记相关服务信息。

mDNS网关原理 - 用户终端请求发现服务

- 终端以组播方式发送mDNS请求报文，查询网络中是否提供某种服务。
- mDNS网关接收到请求报文后，查找服务信息列表，把能够提供此服务的主机名和IP地址回应给终端。这样，终端可以选择相应的服务提供设备建立连接。

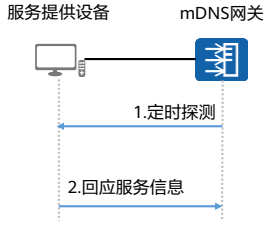


HUAWEI

- 在本阶段，当存在mDNS中继设备时，查询报文发到mDNS网关的过程与mDNS服务提供者发布mDNS服务的过程相似。
- mDNS网关收到终端的服务查询请求后，根据终端的请求，查找在线的服务列表和域名表，回应给mDNS中继设备。
- mDNS网关回应报文的是单播UDP报文：Src IP=Gateway IP、Dst IP=Relay IP、Dest Port=5353。
- mDNS中继收到mDNS网关的回应报文后，根据报文中的Transaction ID查表，找到历史上对应的请求报文的终端信息，修改发出的回应报文：目的地址Dest IP=224.0.0.251、Src IP=Relay IP，Transaction ID=0，TTL=255，组播发送到终端/服务提供者所在的VLAN。最后删除Client IP、Client VLAN和Transaction ID对照表。

mDNS网关原理 - 网关定时发现服务

- mDNS网关支持定时发现服务功能，每隔一个探测周期mDNS网关以组播方式发送服务信息查询消息，服务提供设备收到查询消息后会回应服务信息。
- mDNS网关收到回应报文后刷新服务信息列表。



这种方式保证了服务提供设备的服务信息及时通告给mDNS网关，也保证了mDNS网关维护的服务信息列表的及时性和完整性。

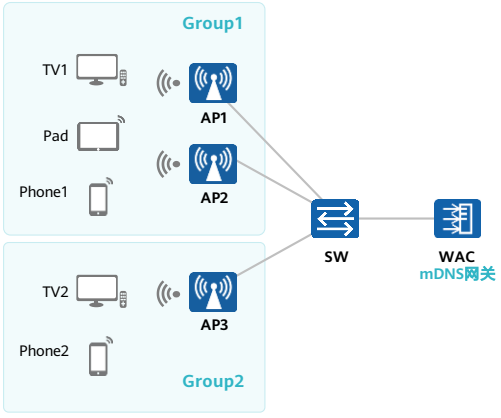
HUAWEI

- 如果一个VLAN内部署的都是mDNS服务提供者，并且它们都已经在网络连接之前启动了，那么便可能不会主动通知mDNS网关自己所提供的服务，所以需要mDNS中继/网关来定时探测、刷新服务列表和服务提供者的主机状态。

mDNS网关原理 - mDNS策略控制概述

- 配置mDNS网关后，客户端接入网络后，可以发现同一mDNS网关上的所有服务提供设备，无法做到设备和服务提供者的精确控制。例如，手机从某一AP接入网络，手机上不仅可以发现从该AP接入的Apple TV，也可以发现其他的Apple TV，即不容易区分选择，也不安全。
- 为了能够更精准的让客户端发现mDNS服务提供设备，可以通过mDNS策略控制功能，让客户端和mDNS服务提供设备按照预先设置的策略进行匹配。该策略基于AP的位置进行控制，因此客户端必须通过无线接入网络。当客户端移动到其他位置时，位置信息可以随之更改。位置信息类型包括AP Name、AP Group、AP Location、AP邻居。其中，AP Name、AP Group、AP Location在网络中部署AP时指定，AP邻居由AP自行发现。有以下两种控制策略。
  - 基于服务类型和AP位置的控制策略
  - 基于服务提供者和AP位置的控制策略

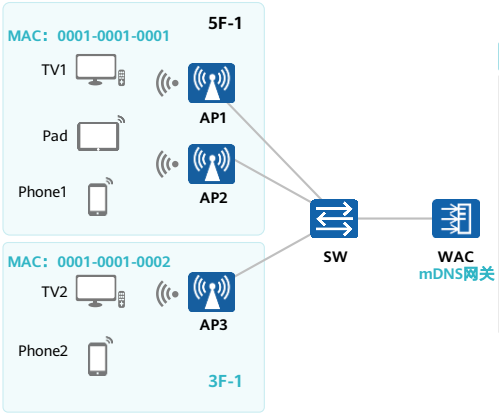
mDNS网关原理 - mDNS策略控制（1）



基于服务类型和AP位置的控制策略

- 对于加入到策略中的服务类型，其客户端和服务提供者接入的AP位置信息匹配策略时才会发现对应服务。
- 例如，终端及服务提供设备分别在不同的AP Group中接入。配置基于服务类型_airplay._tcp.local和位置信息为AP Group的控制策略，属于同一个AP Group的用户和服务提供者可以互相发现。则Phone1和Pad可以发现TV1，但不能发现处于不同AP Group的TV2。Phone2只能发现处于同一AP Group的TV2。

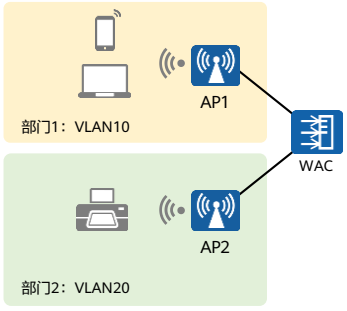
mDNS网关原理 - mDNS策略控制（2）



基于服务提供者和AP位置的控制策略

- mDNS网关基于服务提供者的MAC地址和AP位置信息配置策略。客户端和服务提供者的位置信息必须匹配控制策略才能发现服务。
- 例如，AP1和AP2位于的AP Location信息为5F-1，可以通过配置策略，让MAC地址为0001-0001-0001的TV1仅让位置信息为5F-1的客户端（Phone1和Pad）发现。从3F-1接入的用户Phone3无法发现TV1。

配置案例1：AP与WAC间二层组网的mDNS网关应用（1）



- 某网络存在2个部门，它们分别对应2个VLAN。
- 部门1中存在mDNS客户端，部门2中存在服务提供设备，为确保网络业务顺利开展，需在WAC上部署mDNS网关。

1. 在WAC上使能mDNS网关功能。

```
[WAC] mdns gateway enable
```

2. 在WAC上配置mDNS组。

```
[WAC] mdns group group1
[WAC-mdns-group-group1] user-vlan 10
[WAC-mdns-group-group1] service-vlan 20
```

3. 在WAC上配置定时发现服务功能。

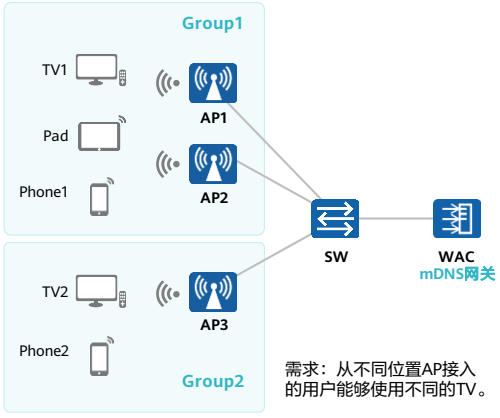
```
[WAC] vlan 10
[WAC-vlan10] mdns probe interval 100
[WAC] vlan 20
[WAC-vlan20] mdns probe interval 100
```

配置案例1：AP与WAC间二层组网的mDNS网关应用（2）

- 在WAC上执行命令**display mdns gateway**，查看mDNS网关的配置信息。

```
[WAC] display mdns gateway
mDNS Information:
------------------------------------------------------------------------------
 mDNS Gateway Status              : Enable
 mDNS Gateway Policy              : Enable
 mDNS Policy no-match action      : Permit
 mDNS Gateway Unicast             : Disable
 mDNS Source IP                   : -
------------------------------------------------------------------------------
 Gateway Probe Vlan               : vlan10  vlan20
------------------------------------------------------------------------------
```

配置案例2：mDNS策略控制



需求：从不同位置AP接入的用户能够使用不同的TV。

1. 在WAC上使能mDNS网关功能。

```
[WAC] mdns gateway enable
```

2. 在WAC上配置mDNS网关允许记录的常用服务类型。

```
[WAC] mdns permit service-type _airplay._tcp.local id 1
[WAC] mdns permit service-type _printer._tcp.local id 2
......
```

3. 在WAC上配置基于服务类型和AP位置的策略控制功能。

```
[WAC] mdns policy enable no-match permit
[WAC] mdns policy service-type
[WAC-mdns-policy-service-type] service-type _airplay._tcp.local
location-type ap-group location same
```

思考题

1. WLAN组播网络优化有哪些手段?

- IGMP Snooping、组播转单播、组播CAC、组播报文抑制等。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN安全与防御

HUAWEI

前言

- WLAN是以无线电波代替网线进行数据传播的，相比有线网络布放简单，但由于其传输媒介的特殊性，导致WLAN安全问题显得尤为突出。
- 本章首先简要介绍了WLAN网络安全威胁及安全方案，然后从管理平面、控制平面安全及转发平面安全入手，分别介绍WLAN的安全方案。

目标

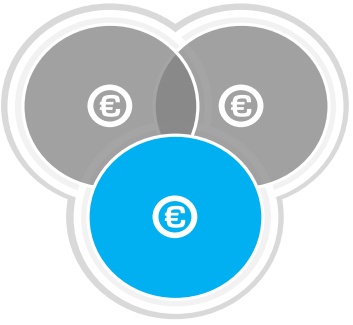
- 学完本课程后，您将能够：
  - 描述WLAN的常见安全威胁
  - 描述华为WLAN网络安全架构
  - 描述华为WLAN安全策略
  - 完成华为WLAN安全配置

目录

WLAN安全概述

防止信息被窃取

- 通过软件侦听无线信息
- 通信内容反向解密



防止未经授权的访问

- 非法用户接入
- 越权访问资源

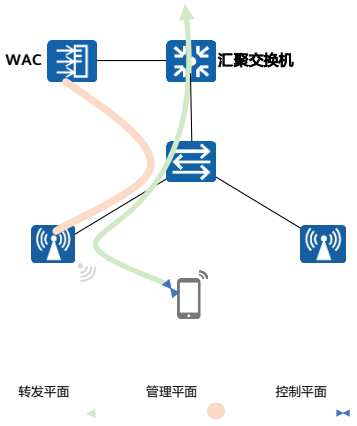
提供稳定高效的无线接入

- 非法AP等干扰导致信号不稳定
- DOS攻击导致WLAN不可用

WLAN常见安全威胁

- **扫描攻击**：非法用户利用工具扫描开放式SSID，得到免费的互联网使用权限，然后攻击网络。
- **WEP攻击**：非法用户捕获发送到目标系统的数据包，进行分析、破解密钥。
- **地址欺骗**：使用工具捕获数据包，非法用户就能得到一个有效MAC地址，进行MAC地址欺骗攻击。
- **Rogue设备入侵**：非法AP释放用户常用的SSID，用户错误地连接该SSID后，数据被侦听。
- **DDoS攻击**：攻击者短时间内发送大量同类型报文到网络中，导致WLAN设备无法处理合法用户数据。

WLAN网络架构及安全方案



管理平面安全	**1. 内容：** 关注管理用户的应用和业务数据的安全，即管理信息的安全。 **2. 威胁：** 擅自访问和滥用系统功能做非法操作等。 **3. 缓解措施：** AAA、HWTATACS用户管理、SSH、SNMPv3、HTTPS、DTLS等。
控制平面安全	**1. 内容：** 关注设备运行的各种协议的安全 **2. 威胁：** ARP/ICMP/TCP/UDP/泛洪引起的CPU超载等 **3. 缓解措施：** WPA/WPA2/WPA3、WIDS、WIPS、URL过滤、入侵检测、反病毒。
转发平面安全	**1. 内容：** 关注转发路径上数据安全，防止攻击在网络中扩散。 **2. 威胁：** DoS/DDoS攻击、ARP/IP欺骗引起不能正常工作等。 **3. 缓解措施：** 流量抑制、防MAC地址漂移、端口隔离、CAPWAP数据隧道加密、Navi AC、IPSec VPN。

HUAWEI

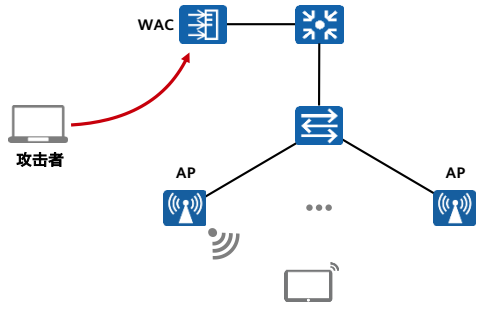
- 为了实现网络安全，华为参考了ITU-T X.805通用安全模型，根据网络中的不同数据流，将网络分为管理、控制、用户三个平面，每个平面根据网络层次分为设备、网络、应用三个层次，提出了分平面、分层的华为网络安全架构模型，用来指导各大解决方案进行网络安全威胁分析和制定安全策略、方案。
  - 管理平面：关注管理用户的应用和业务数据的安全，即管理信息的安全，包括操作、维护和管理信息。
  - 控制平面：WLAN设备需要运行各种各样的协议来达成业务，这些协议自身需要考虑安全性，避免被攻击或者仿冒。
  - 转发平面：信息流的转发主要通过IP报文的目的MAC地址、目的IP地址来查找路径转发，相关安全性主要针对转发路径上如何避免对WLAN设备自身的恶意攻击行为，以及预防某些攻击流量在IP网络中的扩散。
- 通过将管理平面、控制平面和转发平面进行隔离，WLAN设备能够保证任何一个平面在遭受攻击时，不会影响其他平面的正常运行。

目录

WLAN网络管理面安全防御能力

- 在设备的管理平面，为了保障设备的操作系统和管理应用能够正常运行，提供了如下的安全防御能力：
  - WLAN设备登录的安全
  - AAA用户管理的安全
  - SNMP管理设备的安全
  - 禁用不安全的管理协议从业务平面接入
  - 信息中心的安全
  - AP管理安全—CAPWAP控制隧道加密

WLAN设备登录的安全



Console口方式登录WLAN设备

- 谨慎配置Console口的登录密码

SSH方式登录WLAN设备

- 配置密码认证或者RSA认证
- 修改端口号为未知名端口号
- 通过ACL控制允许登录的客户端IP

Web网管方式登录WLAN设备

- 部署AAA认证
- 修改端口号为未知名端口号
- 通过ACL控制允许登录的客户端源IP
- ACL过滤规则
- 通过安全HTTP（即HTTPS）登录Web网管

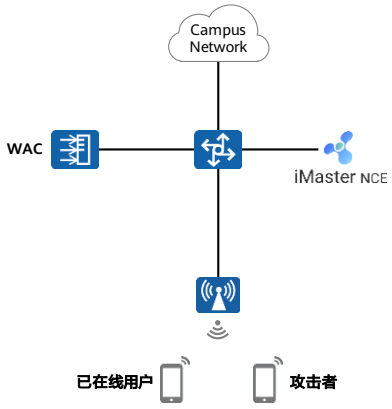
HUAWEI

- SSH方式登录WLAN设备。
  - 攻击行为：
    - 暴力破解密码：攻击者在侦听到SSH端口后，尝试进行连接，设备提示认证，则会进行暴力破解尝试通过认证，获取访问权限。
    - 拒绝服务式攻击：SSH Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。
  - 安全策略：
    - 密码认证和Public-Key认证：SSH Server支持密码认证和Public-Key认证，只有通过认证的用户才能登录WLAN设备，进入命令行界面。
    - 关闭服务：当开启SSH Server服务器时，设备将开启Socket服务，易被攻击者扫描。当不使用SSH Server时，可以关闭SSH Server。
    - 变更端口号：缺省情况下，SSH服务器的端口号为22。端口号22属于知名端口号，易被扫描和攻击。可以修改SSH Server的端口为私有端口，减小被扫描攻击的概率。
    - ACL：在用户界面视图（user-interface）可以配置各个VTY通道的ACL过滤规则，通过ACL控制允许登录的客户端IP。
- Web网管方式登录WLAN设备。
  - 攻击行为：
    - 拒绝服务式攻击：Web Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

- 慢连接攻击：在HTTP的报文头中声明较大的content-length，也就是报文内容的长度。在提交了报文头以后，将后面的报文体部分卡住不发送，这时服务器在接收了长度以后，就会等待客户端发送剩余的内容，攻击者保持连接并且以10秒～100秒/字节的速度去发送大量报文，就达到了消耗资源的效果。受到攻击后，会出现Web用户登录慢、用户掉线、频繁断连、无法登录等现象。

- 安全策略
  - AAA认证：Web Server支持AAA认证，只有通过认证的用户才能登录WLAN设备，进入控制页面。用户在进行登录时，要求输入用户名、密码和随机生成的验证码，减小了帐号被破解的概率。
  - 关闭服务：当开启Web Server服务器时，WLAN设备将开启Socket服务，易被攻击者扫描。当不使用Web Server时，可以关闭Web Server。
  - 变更端口号。
  - ACL：通过ACL控制允许登录的客户端源IP，其他用户不允许登录。
  - HTTP over SSL：提供安全的传输服务，防止传输的数据被窃听获取。

AAA用户管理的安全



攻击行为

黑客可以通过用户名、密码等关键信息进行遍历尝试来获取系统管理员的登录权限。

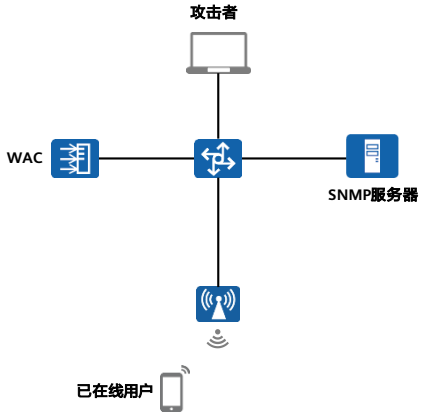
安全策略

针对常见的用户名、密码攻击和破解尝试，可配置用户可认证失败次数和可再次进行认证的时间间隔的参数来防止非法用户登录。

HUAWEI

- 使能本地帐号锁定功能，配置用户的重试时间间隔为6分钟、连续输入错误密码的限制次数为4次及帐号锁定时间为6分钟。
- [HUAWEI-aaa] local-aaa-user wrong-password retry-interval 6 retry-time 4 block-time 6 // 缺省情况下，本地帐号锁定功能处于使能状态，用户的重试时间间隔为5分钟、连续认证失败的限制次数为3次，帐号锁定时间为5分钟。
- 配置了这两个参数后，在用户登录失败N次后，会暂时将用户阻塞一段时间，降低试探成功的机率，增强WLAN设备的安全性。

SNMP管理设备的安全



攻击行为

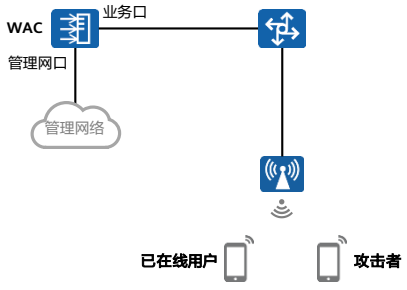
- 攻击者通过改变发送报文的源IP，获取到授权用户的权限，从而执行未经授权的管理操作。
- 拦截管理站和SNMP代理间的通信，获取到用户名、密码或者团体名等信息，获取非法授权。
- 拦截SNMP消息，进行重排序、延迟、重发，从而影响正常操作，直到攻击者获得非法的未授权访问权限。

安全策略

- SNMP有三个版本：SNMPv1、SNMPv2c、SNMPv3
- SNMPv1、SNMPv2c为不安全协议，支持ACL和VACM（基于视图的访问控制）。
- SNMPv3支持MD5/SHA认证、DES和AES加密算法。

- SNMP是用于管理网络设备的协议。SNMP有三个版本：SNMPv1、SNMPv2c、SNMPv3。
- SNMPv1、SNMPv2c为不安全协议，支持ACL和VACM（基于视图的访问控制）。通过给团体名关联ACL和MIB视图，将允许访问设备的网管和允许访问的节点限定在一定范围内，从而在一定程度上提供了系统安全的保护。
- 对于SNMPv3，增加了支持USM（基于用户的安全模型）的安全机制，当前支持MD5/SHA认证、DES和AES加密算法。通过对通信的数据进行认证和加密，解决消息被伪装、篡改、泄密等安全问题。
- MD5和DES是弱加密算法，从V200R019C00版本开始，仅当安装了弱加密算法插件时才支持MD5和DES参数。
- 出于安全考虑，建议配置认证加密的v3用户，并使用v3认证加密方式来管理WLAN设备。通过给用户关联ACL、MIB视图限制用户的访问权限。

禁用不安全的管理协议从业务平面接入



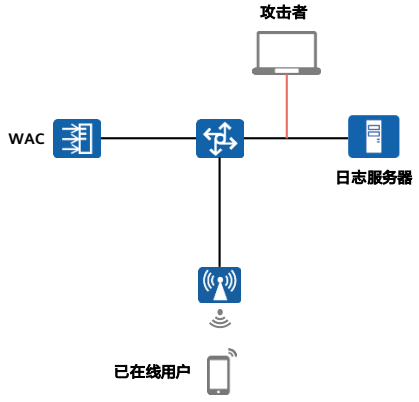
安全策略

WLAN设备业务口默认支持管理协议，同时WLAN设备支持专用的管理网口使用管理协议登录，如果客户网络有专门的管理面规划，仅通过专用管理网口对设备进行管理，可以禁止业务口使用管理协议对设备登录。

HUAWEI

- 对于有专用管理网口的WLAN设备，在防攻击策略视图下使用deny命令将上送CPU的Telnet\SSH\HTTP\SNMP\FTP\Ping（ICMP）等管理协议动作设置为丢弃，可以限制管理协议从业务平面接入。

信息中心的安全



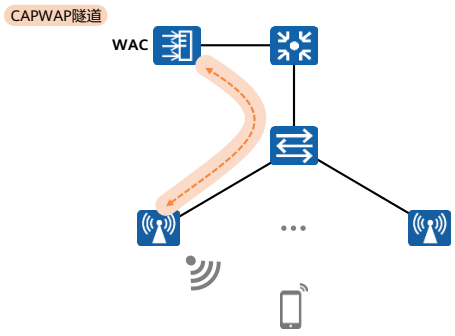
攻击行为

- 当用户需要监控的WLAN设备不在本地且需要查询该WLAN设备产生的信息时，可以在该WLAN设备上配置信息输出到日志服务器，以方便用户在日志主机侧接收设备产生的信息。黑客可以通过截获网络中日志传输报文获得用户信息等。

安全策略

- 执行命令**info-center loghost**可以配置信息输出到日志主机。
- 为了提高日志传输的安全性，需要选择参数**ssl-policy** *policy-name*配置基于TCP模式的SSL加密方式。

AP管理安全 - CAPWAP控制隧道加密



安全风险

使用非DTLS方式，会导致AP与AC间的使用明文传输，在经过非信任网络时会有安全风险。

安全策略

AP与AC建立CAPWAP隧道时，更好的保证管理报文的完整性和私密性，可以配置CAPWAP控制隧道DTLS加密功能。目前，设备仅支持通过预共享密钥的方式对管理报文进行加密。

HUAWEI

- 开启CAPWAP控制隧道DTLS加密功能，DTLS加密的预共享密钥配置为huawei@123。
  - <HUAWEI> system-view
  - [HUAWEI] capwap dtls psk huawei@123
  - [HUAWEI] capwap dtls control-link encrypt

WLAN网络管理平面安全防御常用配置（1）

- WLAN设备登录的安全：修改BootROM密码。

```
Press CTRL+B to enter BIOS menu: 1
Password:
 Info: You are advised to change the password to ensure security. BIOS Menu (Version: 072)
1. Boot with default mode
2. Enter serial submenu
3. Enter startup submenu
4. Enter ethernet submenu
5. Enter file system submenu
6. Modify BOOTROM password
7. Clear password for console user
8. Config HigMem to Flash Flag
9. Reboot (Press CTRL+E to enter Diag menu)
Enter your choice(1-9): 6
Confirm old password :
Please enter new password :
Please confirm new password :
The password is changed successfully.
```

WLAN网络管理平面安全防御常用配置（2）

WLAN设备登录的安全：SSH方式登录

```
[HUAWEI] stelnet server enable
[HUAWEI] ssh server port 55535
 [HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI] user-interface vty 14
[HUAWEI-ui-vty14] acl 2000 inbound
```

WLAN设备登录的安全：WEB方式登录

```
[HUAWEI] http server enable
[HUAWEI] http server port 55536
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule 5 permit source 10.10.10.1 0
[HUAWEI] http acl 2000
```


- 当需要限制某个地址或地址段的用户登录到WLAN设备时，使用inbound；当需要限制已经登录的用户登录到其它WLAN设备时，使用outbound。

WLAN网络管理平面安全防御常用配置（3）

AAA用户管理：配置用户可认证失败次数和可再次进行认证的时间间隔

```
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user wrong-password retry-interval 6 retry-time 4 block-time 6
```

缺省情况下，本地帐号锁定功能处于使能状态，用户的重试时间间隔为5分钟、连续认证失败的限制次数为3次，帐号锁定时间为5分钟。

向IPv4地址为192.168.2.2的日志主机发送信息。信息采用TCP模式进行传输，通过SSL策略进行加密，引用已创建好的SSL策略huawei123。

```
[HUAWEI] ssl policy huawei123 type client
[HUAWEI-ssl-policy-huawei123] quit
[HUAWEI] info-center loghost 192.168.2.2 transport tcp ssl-policy huawei123
```

开启CAPWAP控制隧道DTLS加密功能，DTLS加密的预共享密钥配置为huawei@123。

```
[HUAWEI] capwap dtls psk huawei@123
[HUAWEI] capwap dtls control-link encrypt
```

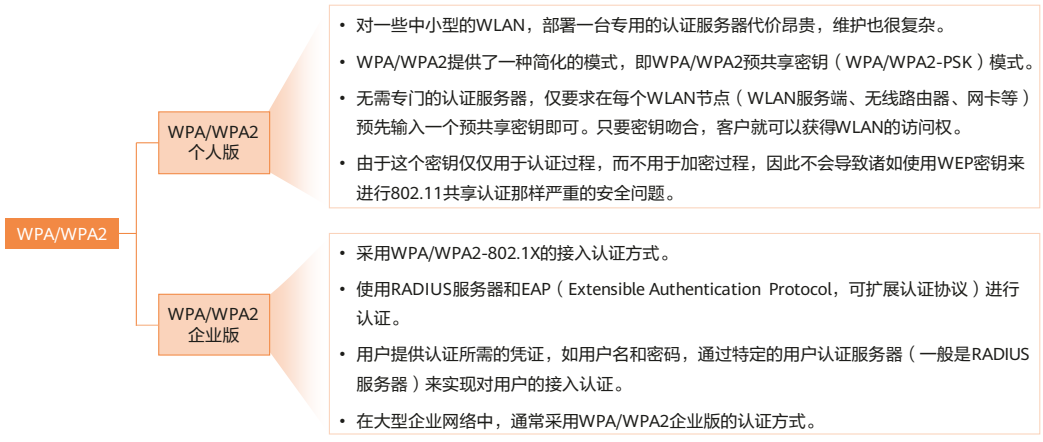
目录

WLAN控制平面安全

- 针对空口面临的各种安全威胁，华为WLAN网络提供了多种保护措施：
  - 无线用户接入安全
  - WIDS/WIPS
  - URL过滤
  - 入侵检测
  - 反病毒

- 针对控制面，攻击行为是多样化的，而针对性的保护措施也是非常多的，除了本页列举的保护措施外，还有本机防攻击、通过业务与管理隔离进行防攻击、设备攻击防范、防ARP欺骗攻击、防ARP泛洪攻击、防DHCP服务器欺骗、防DHCP泛洪攻击、路由协议安全、组播安全等等。本课程聚焦重点的控制平面安全技术。

无线用户接入安全：WPA/WPA2



HUAWEI

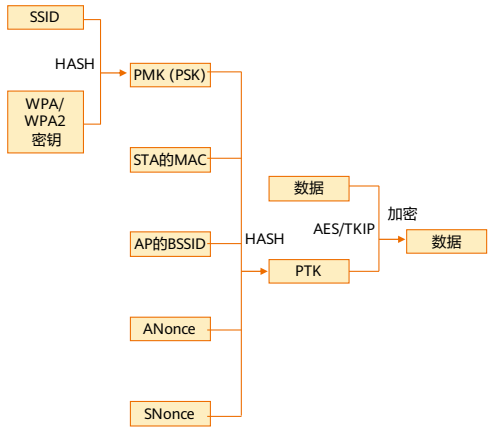
- 由于WEP共享密钥认证采用的是基于RC4对称流的加密算法，需要预先配置相同的静态密钥，无论从加密机制还是从加密算法本身，都很容易受到安全威胁。为了解决这个问题，在802.11i标准没有正式推出安全性更高的安全策略之前，Wi-Fi联盟推出了针对WEP改良的WPA。WPA的核心加密算法还是采用RC4，在WEP基础上提出了临时密钥完整性协议TKIP（Temporal Key Integrity Protocol）加密算法，采用了802.1X的身份验证框架，支持EAP-PEAP、EAP-TLS等认证方式。随后802.11i安全标准组织又推出WPA2，区别于WPA，WPA2采用安全性更高的区块密码锁链-信息真实性检查码协议CCMP（Counter Mode with CBC-MAC Protocol）加密算法。
- 为了实现更好的兼容性，在目前的实现中，WPA和WPA2都可以使用802.1X的接入认证、TKIP或CCMP的加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。
- 综上所述，WPA/WPA2安全策略涉及了链路认证阶段、接入认证阶段、密钥协商和数据加密阶段。
- WPA/WPA2有两种认证方式：WPA/WPA2-PSK认证、WPA/WPA2-802.1X认证。
    - WPA/WPA2-PSK认证：WPA和WPA2都可以使用PSK认证，支持TKIP或AES两种加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。WPA/WPA2-PSK认证主要用于个人、家庭与小型SOHO网络，对网络安全要求相对较低，不需要认证服务器。如果STA只支持WEP加密，则升级为PSK+TKIP无需升级硬件，而升级为PSK+AES可能需要升级硬件。

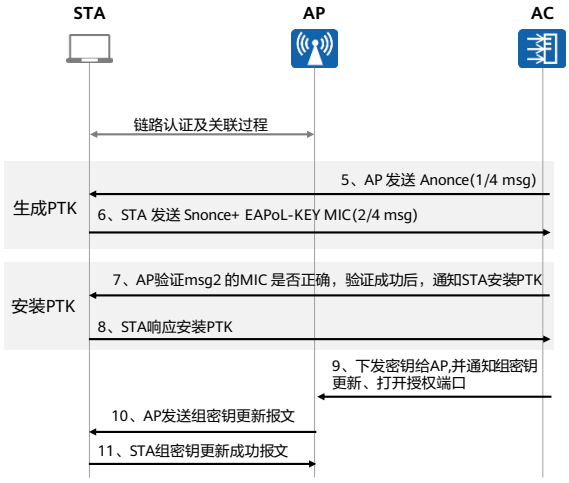
- WPA/WPA2-802.1X认证：WPA和WPA2都可以使用802.1X认证，支持TKIP或AES两种加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。WPA/WPA2-802.1X认证主要用于企业网络等安全要求较高的网络，需要独立的认证服务器。如果用户的设备只支持WEP加密，则升级为802.1X+TKIP无需升级硬件，而升级为802.1X+AES可能需要升级硬件。
- STA的种类多种多样，支持的认证和加密方式也有所差异，为了便于多种类型的终端接入，方便网络管理员的管理，可以使用混合方式配置WPA和WPA2。配置安全策略为WPA-WPA2，则支持WPA或WPA2的终端都可以接入设备进行认证；配置加密方式为TKIP-AES，则支持TKIP加密或AES加密的终端都可以对业务报文进行加密。

WPA/WPA2密钥概述

- 在802.11i里定义了两种密钥层次模型，一种是成对密钥层次结构，主要用来保护STA与AP之间往来的数据；一种是群组密钥层次结构，主要用来描述STA与AP之间的广播或组播数据。
- 密钥协商阶段是根据接入认证生成的成对主钥PMK (Pairwise Master Key)产生成对临时密钥PTK (Pairwise Transient Key)和群组临时密钥GTK (Group Temporal Key)。
  - PMK：用于生成PTK的材料，即配置的预共享密钥，不用于实际的数据加解密。
  - PTK：用于加密单播报文。
  - GTK：用于加密组播和广播无线报文。

WPA/WPA2密钥协商





HUAWEI

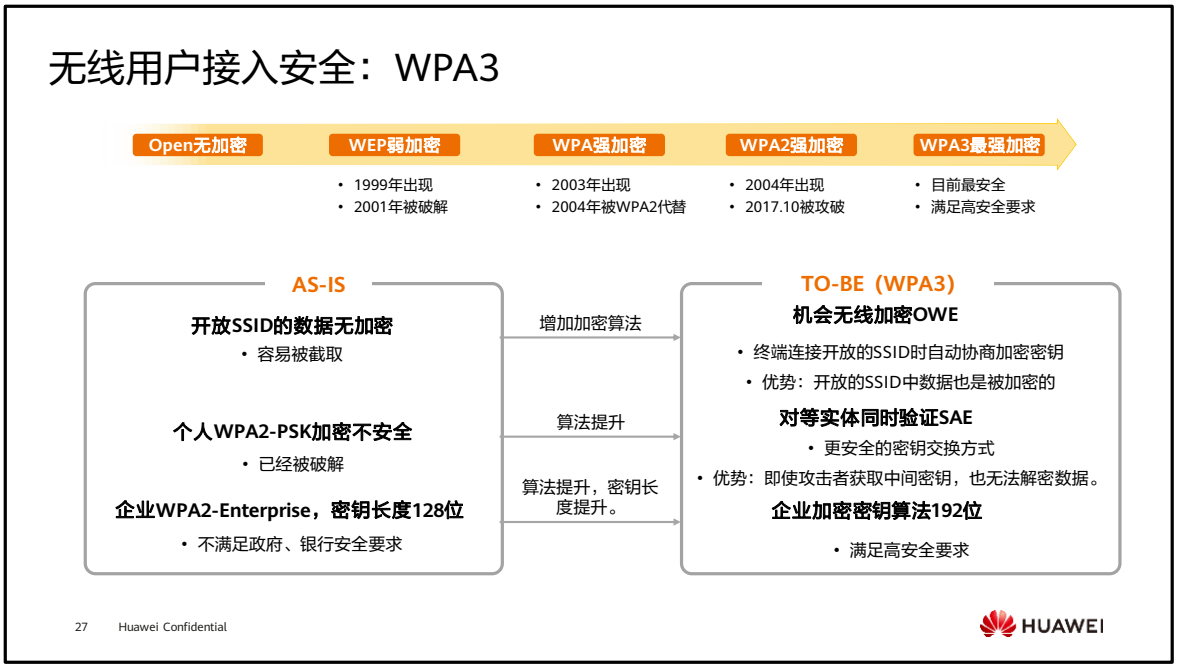
WLAN安全加密

- 在WLAN用户通过认证后并赋予访问权限后，网络必须保护用户所传送的数据不被窥视。主要的方法为对数据报文进行加密，保证只有特定的设备可以对接收到的报文成功解密。
- WLAN加密方式：
  - TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）
  - CCMP（Counter Mode with CBC-MAC Protocol，区块密码锁链-信息真实性检查码协议）
- WPA采用了TKIP加密算法，提供密钥重置机制，并增强了密钥的有效长度，很大程度上弥补了WEP的不足。
- WPA2采用CCMP加密机制，该加密机制使用的AES (Advanced Encryption Standard)加密算法是一种对称的块加密技术，比TKIP更难被破解。
- 目前，WPA和WPA2都可以使用TKIP或AES加密算法，以达到更好的兼容性，它们在安全性上几乎没有差别。

- 无线网络使用开放性介质，如果传输链路没有采取适当的加密保护，使用上的风险就会大幅增加。既然是开放性的网络介质，只要拥有适当的设备，任何人都可以偷窥未经保护的数据。
- 通信安全主要有三种目的。当数据通过网络，数据保护协议必须能够协助网管人员达成这些目的。
  - 机密性（confidentiality）是为了防范数据不受未经授权的第三者拦截。
  - 完整性（Integrity）则是确定数据没有遭到篡改。
  - 认证（authentication）是所有安全策略的基础，因为数据的可信度，部分取决于数据来源的可靠性。使用者必须确认数据的来源的正确性。是统必须利用认证来保护数据。授权（authorization）与访问控制两者均基于真实性之上。在允许访问任何数据之前，是统必须确认使用者的身份（真实性），以及是否允许该使用者访问数据。
- 对于认证，主要通过网络准入控制技术实现，WLAN安全加密技术的目的则主要是保证数据的机密性和完整性。

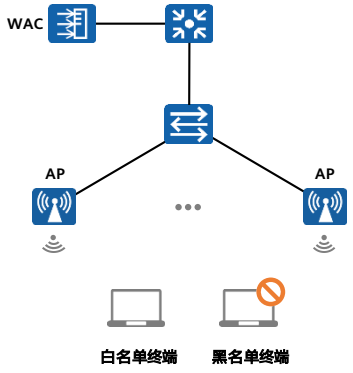
各种安全策略的使用场景和安全性对比

安全策略	链路认证	接入认证	加密算法	建议使用场景	说明
Open	开放系统认证	不涉及	不加密	安全性要求较低的网络	无线设备不需要认证，可以直接访问网络
WEP-open	开放系统认证	本身无接入认证，配套Portal认证或MAC认证	不加密或RC4	用户流动性大的机场、车站、商业中心、会议场馆等公共场所	单独使用时不安全，任何无线终端均可接入网络，建议同时配置Portal认证或MAC认证
WEP-share-key	共享密钥认证	不涉及	RC4	安全性要求较低的网络	WEP安全性低，不建议使用
WPA/WPA2-PSK	开放系统认证	PSK认证	TKIP或AES	家庭用户或中小型企业网络	安全性高于WEP-共享密钥认证，无需第三方服务器，成本低
WPA/WPA2-802.1X	开放系统认证	802.1X认证	TKIP或AES	安全要求高的大型企业网络	安全性高，但需要第三方服务器，成本高



- 相较于WPA/WPA2，WPA3主要在以下几个方面有所改进：
  - 新增支持WPA3-SAE，提供更安全的握手协议。理论上SAE握手协议能够提供前向保密，即使攻击者知道了网络中的密码，也不能解密获取到流量。而在WPA2网络中，在得到密码后就可以解密之前获取的流量。所以，WPA3的SAE握手协议在这方面做出了很大的改进。
  - 加强了算法强度，支持安全套件Suite B，也就是WPA3支持256位密钥的AES-GCM和384位曲线的椭圆曲线加密。
- 和WPA/WPA2类似，根据不同的使用场景和安全性要求，WPA3也可以分为企业版和个人版，即WPA3-802.1X和WPA3-SAE。
- WPA3个人版引入了SAE握手协议，和WPA/WPA2-PSK认证相比，可以有效地抵御离线字典攻击，增加暴力破解的难度，并且SAE握手协议能够提供前向保密，即使攻击者知道了网络中的密码，也不能解密获取到流量，大大提升了WPA3个人网络的安全。
- WPA3企业版仍然使用WPA2企业版的认证体系，采用可扩展认证协议EAP的方法进行身份验证，但是在算法强度上WPA3做了加强，将加密套件更换成了美国联邦安全局定义的CNSA（Commercial National Security Agency）套件，CNSA套件具有强大的加密算法，被用在对安全性要求极高的场合。
- WPA3企业版支持安全套件Suite B，该安全套件使用192 bit最小安全，支持GCMP-256（伽罗瓦/反模式协议，Galois Counter Mode Protocol）、GMAC-256（GCMP的伽罗瓦消息认证码，Galois Message Authentication Code）和SHA384。
- 由于WPA2仍在广泛使用，为了能兼容暂时不支持WPA3的终端能接入WPA3网络，Wi-Fi联盟规定了WPA3的过渡模式，即WPA3和WPA2在未来的一段时间里可以共存。该模式仅针对WPA3个人版，WPA3企业版不支持过渡模式。
- V200R019C00版本AC和AP支持WPA3认证，V200R019C10版本仅AC支持WPA3认证。

无线用户接入安全：STA黑白名单



安全策略

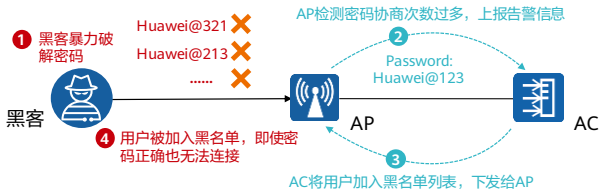
在WLAN网络环境中，可以通过黑白名单功能设定一定的规则过滤STA，实现对STA的接入控制。

- **白名单列表：**允许接入WLAN网络的STA的MAC地址列表。使能白名单功能后，只有匹配白名单列表的用户可以接入无线网络，其他用户都无法接入无线网络。
- **黑名单列表：**拒绝接入WLAN网络的STA的MAC地址列表。使能黑名单功能后，匹配黑名单列表的用户无法接入无线网络，其他用户都可以接入无线网络。

- 如果使能了STA白名单或黑名单，但其名单列表为空，则所有用户都可以接入无线网络。
- 在WLAN设备上可以配置多个STA黑白名单模板，引用到不同的VAP模板或者AP系统模板。对于一个VAP模板或者AP系统模板，同一时间仅能应用STA白名单生效或者STA黑名单生效。

无线用户接入安全：防暴力破解

密码暴力破解	密码防暴力破解
• 密码暴力破解是一种针对于密码的破译方法。 • 暴力破解的原理其实就是穷举法，也就是根据题目的条件确定答案的范围，并使用这些答案进行逐一验证，直到某个答案符合题目的条件。	• 用户认证时，AP检测一定时间内密钥协商失败次数是否超过阈值，如果超过，则认为该用户在暴力破解密码，AP上报告警信息给AC。 • 若同时使能动态黑名单功能则AP将该用户加入到黑名单列表，丢弃该用户的所有报文，直至动态黑名单老化。



HUAWEI

- 攻击行为：
  - 暴力破解法，又称为穷举法，是一种针对于密码的破译方法，即将密码进行逐个推算直到找出真正的密码为止。例如一个已知是四位并且全部由数字组成的密码，其可能共有10000种组合，因此最多尝试10000次就能找到正确的密码。理论上利用这种方法可以破解任何一种密码，问题只在于如何缩短破解时间。当WLAN网络采用的安全策略为WPA/WPA2-PSK，WAPI-PSK，WEP-Share-Key时，攻击者即可利用暴力破解法来破解出密码。
- 安全策略：
  - 为了提高密码的安全性，可以通过防暴力破解密钥功能，延长用户破解密码的时间。AP通过检测WPA/WPA2-PSK，WAPI-PSK，WEP-Share-Key认证时在一定的时间内的密钥协商失败次数是否超过配置的阈值，来确定是否存在攻击。如果超过，则认为该用户在通过暴力破解法破解密码，AP上报告警信息给AC，如果同时使能了动态黑名单功能，则AP将该用户加入到动态黑名单列表中，丢弃该用户的所有报文，直至动态黑名单老化。

无线用户接入安全：管理帧保护PMF

- Spoof攻击通过侦听获取STA和AP的相关信息，然后进行伪造欺骗合法设备。该攻击行为能够得手是因为WPA2仅对数据帧加密而未对管理帧加密。
- PMF（Protected Management Frame，管理帧保护）是WFA发布的基于802.11w标准的一项规范，目的是将WPA2中对数据帧的安全措施扩展至单播和多播管理帧，以提升网络的安全性。

- 攻击行为：
  - WLAN网络的管理帧不加密，可能引发安全问题。
- 安全策略：
  - 管理帧保护功能PMF（Protected Management Frame）是WFA发布的基于IEEE 802.11w标准的一项规范，目的是将WPA2中对数据帧的安全措施扩展至单播和多播管理action帧，以提升网络的可信度。
  - 部署PMF可以解决如下问题：
    - 黑客窃取AP和用户之间通信的管理帧信息。
    - 黑客仿冒AP向用户发送去关联和去认证请求，使用户下线。
    - 黑客仿冒用户向AP发送去关联请求，使用户下线。

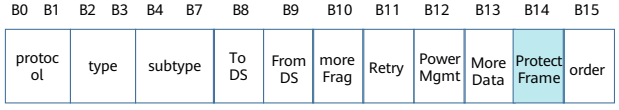
管理帧加密

单播管理帧加密

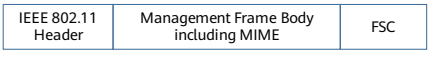
- 单播管理帧加密与单播数据帧类似，但仅支持CCMP算法，并直接复用与数据帧相同的加密密钥PTK；
- 密钥的生成、协商、下发、加解密处理、密钥管理与数据帧一致。
- 由于是对数据部分本身进行加密，单播空口管理帧进行加密时需要在MAC帧头的FC中“Protected Frame”bit来指示。

多播管理帧加密

- 多播管理帧加密机制与多播数据帧类似，仅对数据部分计算并增加完整性校验值（MIC），但是多播管理帧使用的是与GTK相独立的IGTK密钥；IGTK生成、协商、下发和管理处理机制同GTK（协议定义GTK刷新时需要同时刷新IGTK），IGTK通过4次握手或2次握手消息随着GTK一起下发。
- 多播管理帧在收发进行加解密时使用AES-128-CMAC算法进行MIC计算；IGTK的bits 0–127作为AES-128-CMAC key使用。
- 多播管理帧的数据部分不允许进行加密。
- 加密后的广播管理帧增加MIME字段用于完整性校验。



Frame Control field



BIP Encapsulation

HUAWEI

加密管理帧收发处理原则

- 对于不支持PMF的终端，AP收发不加密的robust管理帧，收到加密robust管理帧时丢弃；终端收到加密多播robust管理帧时忽略掉MIME即可。
- 对于支持PMF的终端，在PMF协商成功（获得密钥）之前，AP不允许收发robust管理帧，但未加密的去关联、去认证消息除外。
- 对于支持PMF的终端，在PMF协商成功（获得密钥）之后，AP收发加密robust管理帧，收到不加密robust管理帧时丢弃。
- 多播管理帧不能对数据部分本身进行加密，只能添加MIME进行完整性保护。

WIDS&WIPS功能概述

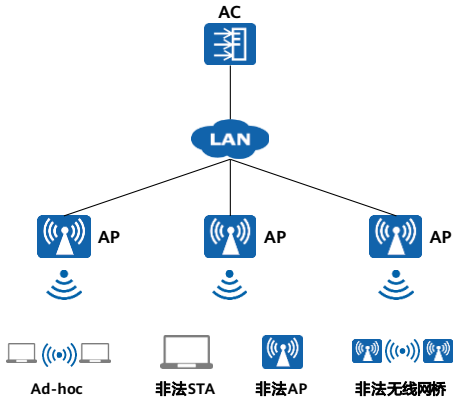
WIDS

WIDS（Wireless Intrusion Detection System，无线入侵检测系统）依照一定的安全策略，对网络、系统的运行状况进行监视，分析用户的活动，判断入侵事件的类型，检测非法的网络。

WIPS

WIPS（Wireless Intrusion Prevention System，无线入侵防预系统）通过对无线网络的实时监测，对于检测到的入侵事情，攻击行为进行主动防御和预警。

WIDS&WIPS：非法设备类型



- Ad-hoc：几台带有无线网卡的设备组成的临时无线网络，也称为Ad-hoc网络。
- 非法STA：连接在非法AP上的STA。
- 非法AP：不在WIDS白名单中，且SSID与本地SSID相同或满足仿冒SSID的匹配规则的AP。
- 非法无线网桥：不在WIDS白名单中，且SSID与本地SSID相同或满足仿冒SSID的匹配规则的无线网桥。

WIDS&WIPS：无线网络设备识别

管理帧识别

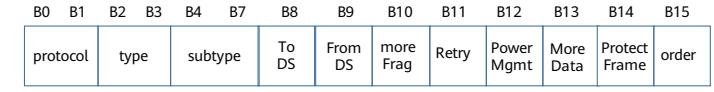
根据802.11 MAC帧Frame Body中网络类型来识别：

管理帧类型	网络类型	设备类型
Probe Request、Association Request和Reassociation Request	独立型网络	Ad-hoc设备
	基础型网络	STA
Beacon、Probe Response、Association Response和Reassociation Response	独立型网络	Ad-hoc设备
	基础型网络	AP

数据帧加密

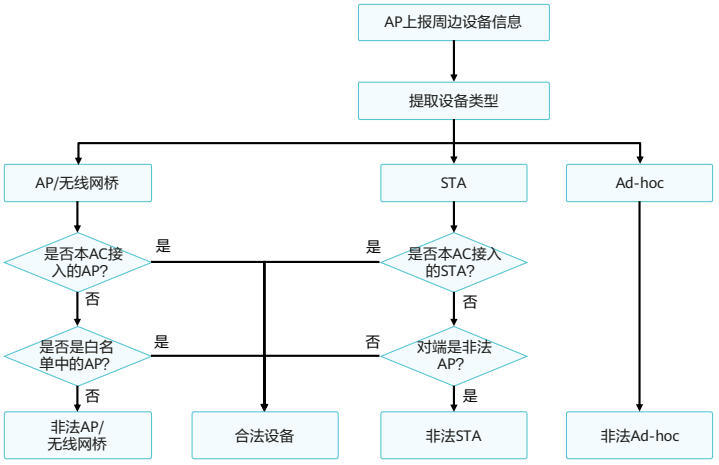
根据To DS & From DS域来识别：

To DS	From DS	设备类型
0	0	Ad-hoc设备
0	1	AP
1	0	STA
1	1	无线网桥



Frame Control field

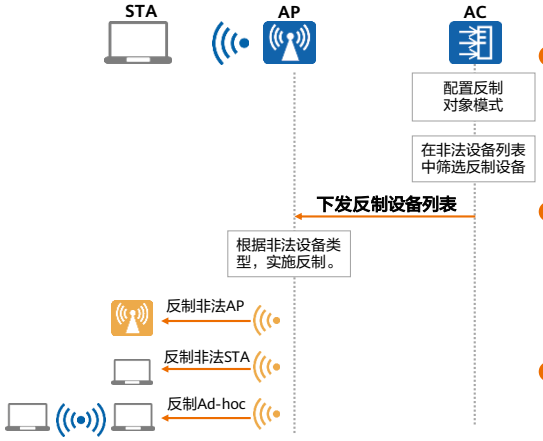
WIDS&WIPS：非法设备判断



HUAWEI

- 首先AC逐一提取AP上报的周边邻居信息表项，根据设备类型进行如下判断：
  - AP合法性识别：用户可通过MAC/SSID/OUI白名单协助进行AP归类；非AC管理的且不属于MAC/SSID/OUI白名单的AP为非法AP，否则属于合法AP。
  - 终端合法性识别：关联到非法AP的终端为非法终端，否则属于合法终端。
  - 网桥合法性识别：同AP合法性识别。
  - Ad-hoc：所有Ad-hoc都为非法设备。
- 注：AC将设备判决为非法AP后，会触发“非法AP告警”，以SNMP trap方式通知网络管理台，其他非法设备类型，不会触发“非法设备告警”。
- 设备安全类别分类：
  - 合法设备：非AC管理的且无安全风险的设备。
  - 非法设备：非AC管理的且可能存在安全风险的设备。
  - 干扰设备：只与管理网络中存在信道重叠的AP。

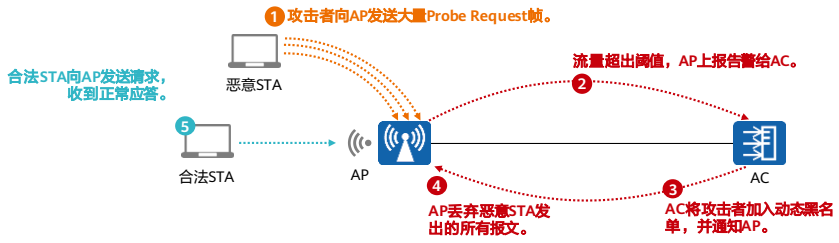
WIDS&WIPS：非法设备反制



1. AC配置反制设备列表模式，同时使能反制功能。
2. AC根据配置的反制模式，从监测AP每一次上报的无线设备列表中，选择对应非法设备列表下发到该监测AP。
3. 监测AP根据AC下发的反制设备列表进行反制处理。

WIDS&WIPS：泛洪攻击检测及防范

- AP持续监控每个STA的流量，当流量超出设置的阀值时，该STA被认为正在网络内泛洪流量，AP上报告警信息给AC。使能动态黑名单时攻击设备被加入动态黑名单，AP丢弃该攻击设备所有报文，以防对无线网络造成冲击。



HUAWEI

- 上报攻击设备信息包括：攻击设备的MAC地址、信道、攻击类型、RSSI等信息。命令：
  - attack detection enable flood
  - attack detection flood intvalue timesvalue 指定检测泛洪攻击的周期和检测周期内AP接收同类报文的个数
- AP支持以下报文进行泛洪攻击检测
  - 认证请求帧Authentication Request
  - 去认证帧Deauthentication
  - 关联请求帧Association Request
  - 去关联帧Disassociation
  - 探测帧Probe Request
  - Action帧
  - EAPOL Start
  - EAPOL-Logoff
  - PS-Poll
  - 802.11 Null数据帧

WIDS&WIPS：Spoof攻击检测及防范

欺骗报文类型

- 广播型去关联帧Disassociation
- 广播型去认证帧Deauthentication

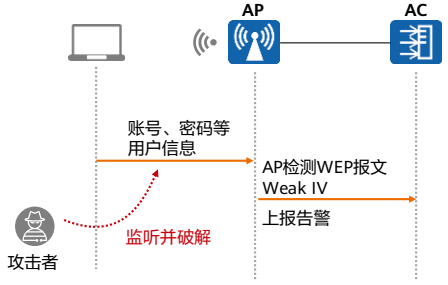
防范原理

当AP接收到上述两种报文，AP检测报文源地址是否为AP自身MAC地址，如果是，则表示WLAN网络受到解除认证报文或解除关联报文的欺骗攻击，AP上报告警信息给AC。

HUAWEI

- 命令：attack detection enable spoof。

WIDS&WIPS：Weak IV检测及防范



检测原理

通过识别每个WEP报文的IV来预防攻击，当含有弱向量的报文被检测到，AP向AC上报告警信息，提醒用户使用其他安全策略来避免STA使用弱向量加密。

HUAWEI

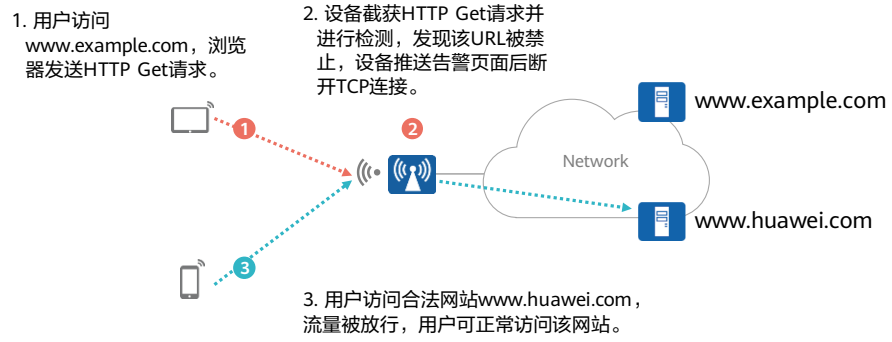
- WLAN使用WEP进行加密的时候，对于每一个报文都会产生一个24 bit的IV，当一个WEP报文被发送时，IV和共享密钥一起作为输入来生成密钥串，密钥串和明文加密，最终生成密文。Weak IV是指使用不安全的方法生成IV，例如频繁生成重复的IV甚至是始终生成相同的IV。由于在终端发送报文时IV作为报文头的一部分被明文发送，攻击者很容易暴力破解出共享密钥后访问网络资源。
- Weak IV检测通过识别每个WEP报文的IV来预防这种攻击，当一个包含有Weak IV的报文被检测到，AP向WAC上报告警信息，便于用户使用其他的安全策略来避免终端使用弱向量加密。

URL过滤

- 随着互联网应用的迅速发展，计算机网络在经济和生活的各个领域迅速普及，使得信息的获取、共享和传播更加方便，但同时也给企业带来了前所未有的威胁：
  - 员工在工作时间随意地访问与工作无关的网站，严重影响了工作效率。
  - 员工随意访问非法或恶意的网站，造成公司机密信息泄露，甚至会带来病毒、木马和蠕虫等威胁攻击。
  - 在内部网络拥堵时段，无法保证员工正常访问与工作相关的网站（如公司主页、搜索引擎等），影响工作效率。
- 当用户发起HTTP或HTTPS的URL请求时，通过URL过滤功能可以实现对用户的请求进行放行、告警或者阻断。使用URL过滤后：
  - 当用户访问合法的网站时，放行此请求。
  - 当用户访问非法的网站时，阻断此请求。

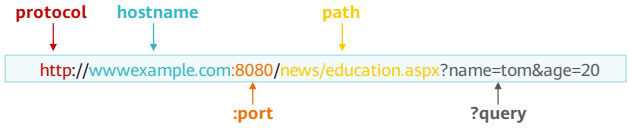
- 根据无线用户业务数据报文转发方式不同，URL需要部署在不同的网络设备中。
  - 隧道转发：AC和AP之间建立CAPWAP隧道集中转发用户数据报文，此时URL业务会部署在AC上。无线用户的业务数据报文在AP上进行CAPWAP封装，经过AP和AC之间的CAPWAP隧道发送到AC上，在AC上解掉CAPWAP封装后对原始的无线用户的业务数据报文进行URL过滤。
  - 直接转发：业务数据报文不需要经过AC转发，此时URL业务会部署在AP上。AP收到业务数据报文之后直接对原始用户数据报文进行URL过滤。

URL过滤原理


1. 用户访问
www.example.com，浏览
器发送HTTP Get请求。
2. 设备截获HTTP Get请求并
进行检测，发现该URL被禁
止，设备推送告警页面后断
开TCP连接。
www.example.com
Network
www.huawei.com
3. 用户访问合法网站www.huawei.com，
流量被放行，用户可正常访问该网站。

URL地址结构

- URL（Uniform Resource Locator，统一资源定位符）用来完整地描述Internet上的网页或者其他资源的地址。
- URL的一般格式为：protocol://hostname:port/path?query
  - protocol：使用的应用协议，最常用的是HTTP协议。
  - hostname：Web服务器的域名或者IP地址。
  - :port：可选，通信端口。各种应用协议都有默认的端口号，如HTTP协议的默认端口为80。当服务器采用默认端口时，URL过滤规则中不用配置端口号。当服务器采用非默认端口时，URL过滤规则中不能省略端口号。
  - path：由零个或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址。
  - ?query：可选，用于给动态网页传递参数。



URL匹配方式

- URL进行匹配时，不同的匹配方式存在如下优先级顺序，由高至低如下所示：
- 精确匹配 > 后缀匹配 > 前缀匹配 > 关键字匹配。

匹配方式	定义	条目	匹配结果
前缀匹配	匹配所有以指定字符串开头的URL	www.example*	匹配所有以www.example开头的URL，如： •www.example.com •www.example.com/solutions.do
后缀匹配	匹配所有以指定字符串结尾的URL	*aspx	匹配所有以aspx结尾的URL，如： •www.example.com/news/solutions.aspx •www.example.com/it/price.aspx •10.1.1.1/sports/abc.aspx
关键字匹配	匹配所有包含指定字符串的URL	*sport*	匹配所有包含sport的URL，如： •sports.example.com/news/solutions.aspx •sports.example.com/it/ •10.1.1.1/sports/
精确匹配	首先判断URL和指定字符串是否匹配，如果未匹配，则去除URL的最后一个目录，再和指定字符串进行匹配；如果还未匹配，则继续去除URL的最后一个目录，再和指定字符串进行匹配。以此类推，直到用域名去匹配指定的字符串为止	www.example.com	根据匹配规则，以下URL可以匹配： •www.example.com •www.example.com/news •www.example.com/news/en/ 以下URL不会匹配该条目： •www.example.com.cn/news •www.example.org/news/www.example.com

- 4种匹配针对整个URL，默认只对HTTP协议数据进行过滤。在开启HTTPS代理后或开启加密流量过滤功能后可以对HTTPS协议访问进行过滤。
- HTTP方式：直接提取HTTP协议报文中的URL，跟配置的URL黑白名单匹配。
- HTTPS方式：HTTPS是承载在SSL协议之上的，SSL协议将HTTP协议传输的内容整体进行了加密。只能识别SSL协议中的字段SNI、CN、SAN，提取出url跟配置的url黑白名单匹配。

URL过滤方式

- 配置了URL过滤功能以后，设备将对URL信息进行如下处理，将URL信息与白名单进行匹配：
  - 如果匹配白名单，则允许该请求通过。
  - 如果未匹配白名单，则进行下一步检测。
- 将URL信息与黑名单进行匹配：
  - 如果匹配黑名单，则阻断该请求。
  - 如果未匹配黑名单，则配置的URL过滤功能不起作用，报文按正常流程处理。

- 黑白名单：
  - 设备将HTTP上网请求的URL与黑白名单进行匹配，如果匹配白名单则允许该HTTP请求，如果匹配黑名单则阻止该HTTP请求。
  - 当上网请求的URL与白名单匹配时，不会再进行后续的处理。设置白名单有利于提高匹配效率。
- URL自定义分类：
  - URL自定义分类由用户自行配置和维护。URL自定义分类将具有相同特征的URL进行分类，用户可以根据业务配置策略，允许或拒绝各个分类URL的访问。相对于预定义URL分类，用户可以使用自定义分类对URL进行更为精细化的控制。

入侵防御实现机制

- 入侵防御是一种安全机制，通过分析网络流量，检测入侵（包括缓冲区溢出攻击、木马、蠕虫等），并通过一定的响应方式，实时地中止入侵行为，保护企业信息系统和网络架构免受侵害。入侵防御的基本实现机制如下：

重组应用数据	协议识别和协议解析	特征匹配	响应处理
WAC首先进行IP分片报文重组以及TCP流重组，确保了应用层数据的连续性，有效检测出逃避入侵防御检测的攻击行为。	WAC根据报文内容识别多种常见应用层协议。 识别出报文的协议后，AC根据具体协议分析方案进行更精细的分析，并深入提取报文特征。	AC将解析后的报文特征与签名进行匹配，如果命中了签名，则进行响应处理。	完成检测后，AC根据管理员配置的动作对匹配到签名的报文进行处理。

- 入侵防御是一种安全机制，通过分析网络流量，检测入侵（包括缓冲区溢出攻击、木马、蠕虫等），并通过一定的响应方式，实时地中止入侵行为，保护企业信息系统和网络架构免受侵害。入侵防御的主要优势有如下几点。
  - 实时阻断攻击：设备采用直路方式部署在网络中，能够在检测到入侵时，实时对入侵活动和攻击性网络流量进行拦截，将对网络的入侵降到最低。
  - 深层防护：新型的攻击都隐藏在TCP/IP协议的应用层里，入侵防御能检测报文应用层的内容，还可以对网络数据流重组进行协议分析和检测，并根据攻击类型、策略等确定应该被拦截的流量。
  - 全方位防护：入侵防御可以提供针对蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具、后门等攻击的防护措施，全方位防御各种攻击，保护网络安全。
  - 内外兼防：入侵防御不但可以防止来自于企业外部的攻击，还可以防止发自于企业内部的攻击。系统对经过的流量都可以进行检测，既可以对服务器进行防护，也可以对客户端进行防护。
  - 不断升级，精准防护：入侵防御特征库会持续的更新，以保持最高水平的安全性。您可以从升级中心定期升级设备的特征库，以保持入侵防御的持续有效性。

入侵防御：签名

- 入侵防御签名用来描述网络中攻击行为的特征，WAC通过将数据流和入侵防御签名进行比较来检测和防范攻击。

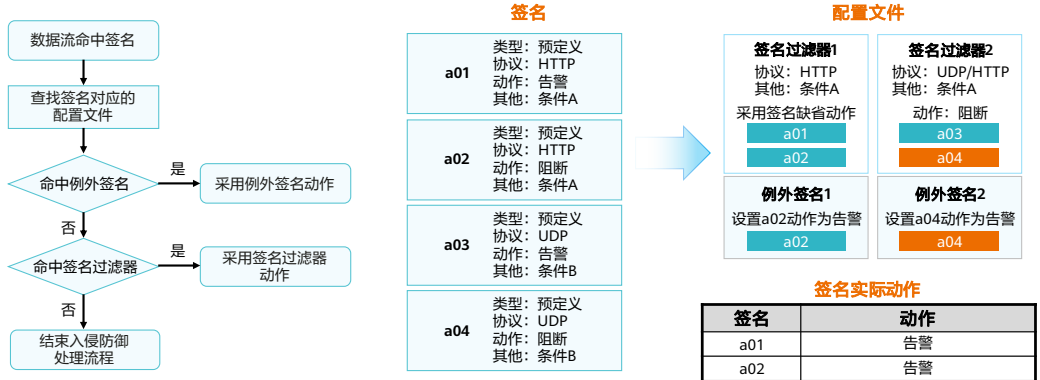
预定义签名	自定义签名
• 预定义签名是入侵防御特征库中包含的签名。预定义签名的内容是固定的，不能创建、修改或删除。 • 每个预定义签名都有缺省的动作，分为： ▫ 放行：指对命中签名的报文放行，不记录日志。 ▫ 告警：指对命中签名的报文放行，但记录日志。 ▫ 阻断：指丢弃命中签名的报文，阻断该报文所在的数据流，并记录日志。	• 自定义签名是指管理员通过自定义规则创建的签名。 • 新的攻击出现后，其对应的攻击签名通常都会晚一点才会出现。当用户自身对这些新的攻击比较了解时，可以自行创建自定义签名以便实时地防御这些攻击。 • 自定义签名创建后，系统会自动对自定义规则的合法性进行检查，避免低效签名浪费系统资源。 • 自定义签名的动作分为阻断和告警，可以在创建自定义签名时配置签名的响应动作。

- 建议只在非常了解攻击特征的情况下才配置自定义签名。因为自定义签名设置错误可能会导致配置无效，甚至导致报文误丢弃或业务中断等问题。
- 签名过滤器：
  - 由于设备升级特征库后会存在大量签名，而这些签名是没有进行分类的，且有些签名所包含的特征本网络中不存在，需过滤出去，故设置了签名过滤器进行管理。管理员分析本网络中常出现的威胁的特征，并将含有这些特征的签名通过签名过滤器提取出来，防御本网络中可能存在的威胁。
  - 签名过滤器是满足指定过滤条件的集合。签名过滤器的过滤条件包括：签名的类别、对象、协议、严重性、操作系统等。只有同时满足所有过滤条件的签名才能加入签名过滤器中。一个过滤条件中如果配置多个值，多个值之间是“或”的关系，只要匹配任意一个值，就认为匹配了这个条件。
  - 签名过滤器的动作分为阻断、告警和采用签名的缺省动作。签名过滤器的动作优先级高于签名缺省动作，当签名过滤器的动作不采用签名缺省动作时，以签名过滤器设置的动作为准。
  - 各签名过滤器之间存在优先关系（按照配置顺序，先配置的优先）。如果一个入侵防御模板中的两个签名过滤器包含同一个签名，当报文命中此签名后，设备将根据优先级高的签名过滤器的动作对报文进行处理。

- 例外签名：
  - 由于签名过滤器会批量过滤出签名，且通常为了方便管理设置为统一的动作。如果管理员需要将某些签名设置为与签名过滤器不同的动作时，可将这些签名引入到例外签名中，并单独配置动作。
  - 例外签名的动作分为告警和放行。
  - 例外签名的动作优先级高于签名过滤器。如果一个签名同时命中例外签名和签名过滤器，则以例外签名的动作为准。
  - 例如，签名过滤器中过滤出一批符合条件的签名，且动作统一设置为阻断。但是员工经常使用的某款自研软件却被拦截了。观察日志发现，用户经常使用的该款自研软件命中了签名过滤器中某个签名，被误阻断了。此时管理员可将此签名引入到例外签名中，并修改动作为放行。

入侵防御对数据流的处理

- 当数据流命中的攻击防御模板中包含入侵防御模板时，设备将数据流送到入侵防御模块，并依次匹配入侵防御模板引用的签名。



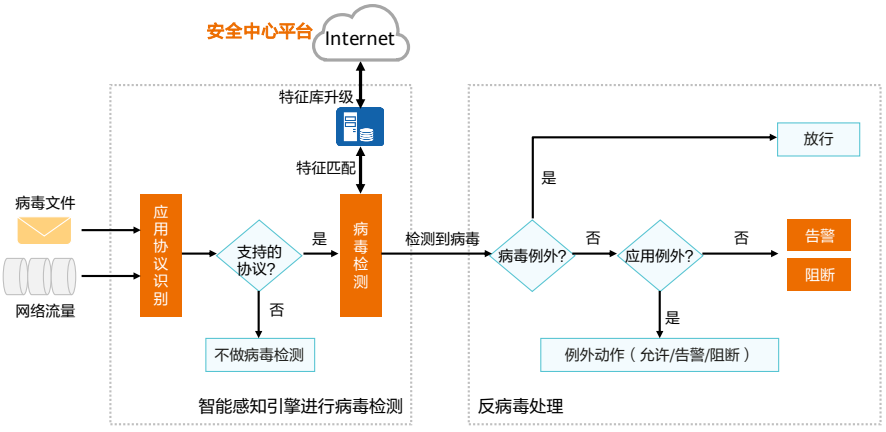
签名实际动作

签名	动作
a01	告警
a02	告警
a03	阻断
a04	告警

- 当数据流命中多个签名，对该数据流的处理方式如下：
  - 如果这些签名的实际动作都为告警时，最终动作为告警。
  - 如果这些签名中至少有一个签名的实际动作为阻断时，最终动作为阻断。
  - 当数据流命中了多个签名过滤器时，设备会按照优先级最高的签名过滤器的动作来处理。

反病毒

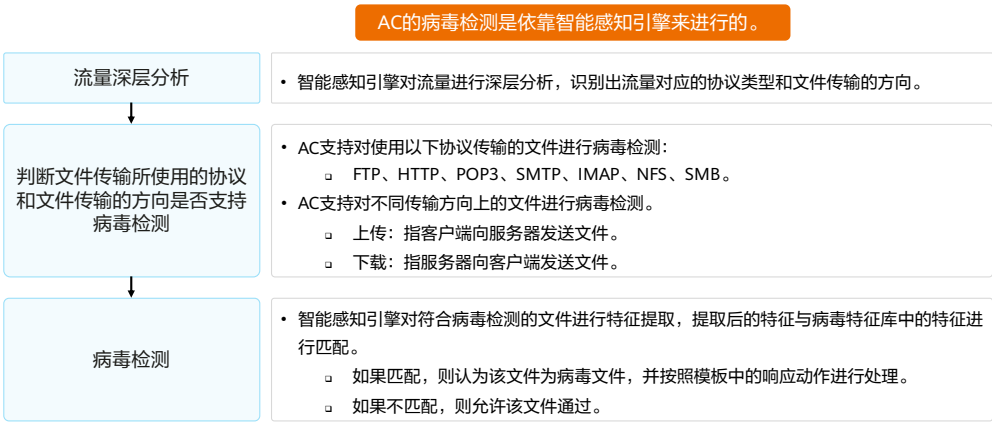
- WAC利用专业的智能感知引擎和不断更新的病毒特征库实现对病毒文件的检测和处理。



HUAWEI

- 病毒是一种恶意代码，可感染或附着在应用程序或文件中，一般通过邮件或文件共享等协议进行传播，威胁用户主机和网络的安全。有些病毒会耗尽主机资源、占用网络带宽，有些病毒会控制主机权限、窃取数据，有些病毒甚至会对主机硬件造成破坏。
- 反病毒是一种安全机制，它可以通过识别和处理病毒文件来保证网络安全，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生。

反病毒：智能感知引擎进行病毒检测



- 病毒特征库是由华为公司通过分析各种常见病毒特征而形成的。该特征库对各种常见的病毒特征进行了定义，同时为每种病毒特征都分配了一个唯一的病毒ID。当设备加载病毒特征库后，即可识别出特征库里已经定义过的病毒。同时，为了能够及时识别出最新的病毒，设备上的病毒特征库需要不断地从升级中心进行升级。

反病毒处理（1）

- 当AC检测出传输文件为病毒文件时，需要进行如下处理：

1. 判断该病毒文件是否命中病毒例外

- 当用户认为已检测到的某个病毒为误报时，可以将该对应的病毒ID添加到病毒例外。
- 如果检测结果命中了病毒例外，则该文件的响应动作为放行。

2. 判断该病毒文件是否命中应用例外

- 如果不是病毒例外，则判断该病毒文件是否命中应用例外。如果是应用例外，则按照应用例外的响应动作（放行、告警和阻断）进行处理。
- 在配置响应动作时：
  - 如果只配置协议的响应动作，则协议上承载的所有应用都继承协议的响应动作。
  - 如果协议和应用都配置了响应动作，则以应用的响应动作为准。

反病毒处理（2）

3. 按照模板中配置的协议和传输方向对应的响应动作进行处理

- 如果病毒文件既没命中病毒例外，也没命中应用例外，则按照模板中配置的协议和传输方向对应的响应动作进行处理。
- AC对不同协议在不同的文件传输方向上支持不同的响应动作。

协议	传输方向	响应动作	说明
HTTP	上传/下载	告警/阻断，默认为阻断	告警：允许病毒文件通过，同时生成病毒日志。 阻断：禁止病毒文件通过，同时生成病毒日志。
FTP	上传/下载	告警/阻断，默认为阻断	
NFS	上传/下载	告警	
SMB	上传/下载	告警/阻断，默认为阻断	
SMTP	上传	告警	
POP3	下载	告警	
IMAP	上传/下载	告警	

本机防攻击

- 在网络中，存在着大量针对CPU的恶意攻击报文以及需要正常上送CPU的各类报文。针对CPU的恶意攻击报文会导致CPU长时间繁忙的处理攻击报文，从而引发其他业务的断续甚至系统的中断；大量正常的报文也会导致CPU占用率过高，性能下降，从而影响正常的业务。
- 为了保护CPU，保证CPU对正常业务的处理和响应，设备提供了本机防攻击功能。本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。
- 本机防攻击包含：
  - CPU防攻击
  - 攻击溯源

- CPU防攻击：
  - CPU防攻击可以针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。
  - CPU防攻击的核心部分是CPCAR（Control Plane Committed Access Rate）功能。CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。
- 攻击溯源：
  - 攻击溯源可以针对DoS（Denial of Service）攻击进行防御。设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再根据攻击报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员，以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。

本机防攻击：CPU防攻击

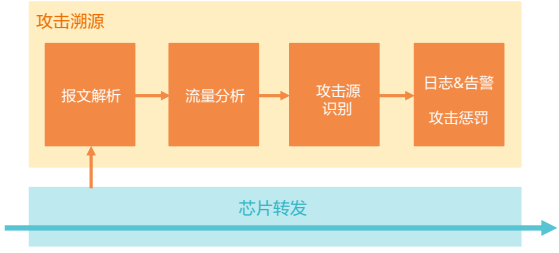
- CPU防攻击针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定的范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。

多级安全机制，实现对设备的分级保护	动态链路保护功能CPU限速
• 第一级：对上送CPU的报文按照协议类型进行速率限制。 • 第二级：对上送CPU的报文，按照协议优先级进行调度。 • 第三级：对上送CPU的报文统一限速，对超过统一限速值的报文随机丢弃。	当设备检测到SSH Session数据、Telnet Session数据、SSHv6 Session数据、Telnetv6 Session数据以及FTP Session数据建立时，会启动对此Session的动态链路保护功能，后续上送报文如匹配此Session特征信息，此类数据将会享受高速率上送的权利，由此保证了此Session相关业务的运行可靠性、稳定性。

- CPU防攻击针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定的范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。多级安全机制，保证设备的安全，实现了对设备的分级保护。
- 设备通过以下策略实现对设备的分级保护：
  - 第一级：对上送CPU的报文按照协议类型进行速率限制，保证每种协议上送CPU的报文不会过多。
  - 第二级：对上送CPU的报文，按照协议优先级进行调度，保证优先级高的协议先得到处理。
  - 第三级：对上送CPU的报文统一限速，对超过统一限速值的报文随机丢弃，保证整体上送CPU的报文不会过多，保护CPU安全。
- 动态链路保护功能的CPU报文限速，是指当设备检测到SSH Session数据、Telnet Session数据、SSHv6 Session数据、Telnetv6 Session数据以及FTP Session数据建立时，会启动对此Session的动态链路保护功能，后续上送报文如匹配此Session特征信息，此类数据将会享受高速率上送的权利，由此保证了此Session相关业务的运行可靠性、稳定性。

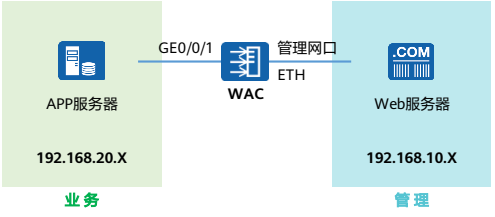
本机防攻击：攻击溯源

- 针对DoS攻击进行防御。设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再对这些攻击报文根据报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。
  - 攻击溯源包括报文解析、流量分析、攻击源识别和发送日志告警通知管理员以及实施惩罚四个过程。
  - 找出攻击源，然后管理员通过ACL或配置黑名单的方式限制攻击源，以保护设备CPU。



通过业务与管理隔离进行防攻击

- 例：192.168.10.X网段设备和WLAN设备独立管理网口ETH相连，并可以正常登录设备；192.168.20.X网段设备和WLAN设备的业务口GE0/0/1相连，并可以正常登录设备。如果不进行管理网口隔离，会出现192.168.20.X设备可以Ping通192.168.10.X设备现象，导致管理网口地址泄露，容易被攻击。



业务平面和管理平面隔离

- 为提高网络安全性，防止非法用户的攻击，可以通过配置管理口和业务口的接口策略和路由策略，实现管理口与业务口的隔离。
- 为了避免STA通过Telnet等方式访问设备，使业务面和管理面隔离，可以配置安全防护功能。

WLAN网络控制面安全防御常用配置 - WPA3配置

- 配置WPA3-SAE认证，配置用户口令为huawei@123。

```
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 sae pass-phrase huawei@123 aes
```

- 配置WPA3-802.1X认证方式。

```
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 dot1x gcmp256
```

- 配置WPA2和WPA3认证，配置用户口令为huawei@123。

```
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 psk-sae pass-phrase huawei@123 aes
```

WLAN网络控制面安全防御常用配置 - WIDS&WIPS配置（1）

- 配置AP组，并开启非法设备检测和反制功能。

```
# [AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] radio 0
[AC-wlan-group-radio-ap-group1/0] work-mode normal
[AC-wlan-group-radio-ap-group1/0] wids device detect enable
[AC-wlan-group-radio-ap-group1/0] wids contain enable
```

- 配置AP组，并开启非法设备检测和反制功能

```
[AC-wlan-ap-group-ap-group1] radio 1
[AC-wlan-group-radio-ap-group1/1] work-mode normal
[AC-wlan-group-radio-ap-group1/1] wids device detect enable
[AC-wlan-group-radio-ap-group1/1] wids contain enable
```

- 创建名为“wlan-wids”的WIDS模板，并配置反制模式为反制仿冒SSID的非法AP。

```
[AC-wlan-view] wids-profile name wlan-wids
[AC-wlan-wids-prof-wlan-wids] contain-mode spoof-ssid-ap
```

WLAN网络控制面安全防御常用配置 - WIDS&WIPS配置（2）

- 在AP组“ap-group1”中引用WIDS模板“wlan-wids”。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] wids-profile wlan-wids
[WAC-wlan-ap-group-ap-group1] quit
```

- 验证配置结果，通过命令**display wlan ids contain ap**可以查看到被反制的AP2。

```
[WAC-wlan-view] display wlan ids contain ap
 #Rf: Number of monitor radios that have contained the device
CH: Channel number
--------------------------------------------------------------------------------
MAC address   CH  Authentication  Last detected time              #Rf        SSID
--------------------------------------------------------------------------------
000b-6b8f-**** 11  wpa-wpa2       *****                           1           wlan-net
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

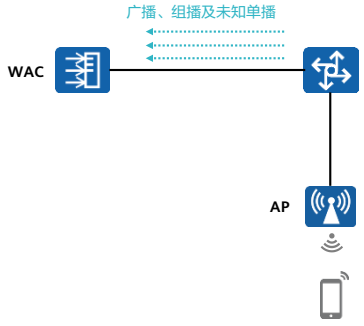
目录

WLAN转发平面安全

- 对于WLAN的转发平面安全，需关注转发路径上数据安全，防止攻击在网络中扩散。可采取如下措施：
  - 流量抑制
  - ACL
  - 防MAC地址漂移
  - 端口隔离
  - CAPWAP数据隧道加密
  - Navi AC
  - IPSec VPN

流量抑制

- 流量抑制是用于控制广播、组播以及未知单播报文，防止这三类报文引起广播风暴的安全技术。流量抑制主要通过配置阈值来限制流量。



流量抑制原理

- 当WLAN设备某个二层以太接口收到广播、组播或未知单播报文时，如果根据报文的目的MAC地址WLAN设备不能明确报文的出接口，WLAN设备会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低WLAN设备转发性能。
- 入方向上，设备支持分别对三类报文按包速率进行流量抑制。
- 设备监控三类报文速率并和配置的阈值相比较，当入口流量超过配置的阈值时，设备会丢弃超额的流量。

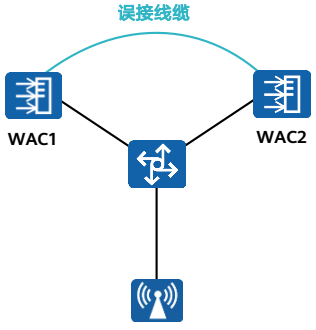
ACL

分类	适用的IP版本	功能介绍	说明
基本ACL	IPv4	可使用IPv4报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv4 ACL简称基本ACL，编号范围为2000～2999。
高级ACL	IPv4	既可使用IPv4报文的源IP地址，也可使用目的地址、IP优先级、ToS、DSCP、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP（User Datagram Protocol）源端口/目的端口号等来定义规则。	高级IPv4 ACL简称高级ACL，编号范围为3000～3999。
二层ACL	IPv4	可根据报文的以太网帧头信息来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、以太帧协议类型等。	编号范围为4000～4999。
用户ACL	IPv4	既可使用IPv4报文的源IP地址或源用户组，也可使用目的地址或目的用户组、目的域名、IP优先级、ToS、DSCP、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号等来定义规则。	编号范围为6000～6999。
基本ACL6	IPv6	可使用IPV6报文的源IP地址、分片标记和时间段信息来定义规则。	基本IPv6 ACL简称基本ACL6，编号范围为2000～2999。
高级ACL6	IPv6	可以使用IPv6报文的源地址、目的地址、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口、ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。	高级IPv6 ACL简称高级ACL6，编号范围为3000～3999。
用户ACL6	IPv6	可以使用IPv6报文的源地址、目的地址、目的域名、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口、ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。	用户IPv6 ACL简称用户ACL6或UCL6。编号范围为6000～6999。

- 通过ACL可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。
- 访问控制列表ACL是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL通过规则对数据包进行分类，这些规则应用到WLAN设备上，WLAN设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。例如可以用访问列表描述：拒绝任何用户终端使用Telnet登录本机，允许每个用户终端经由SMTP向本机发送电子邮件。
- 每个ACL中可以定义多个规则，根据规则的功能分为：基本ACL、基本ACL6、高级ACL、高级ACL6、二层ACL、用户ACL和用户ACL6。

MAC地址防漂移

- 网络中产生环路或非法用户进行网络攻击都会造成MAC地址发生漂移，导致MAC地址不稳定。



MAC地址防漂移的方式

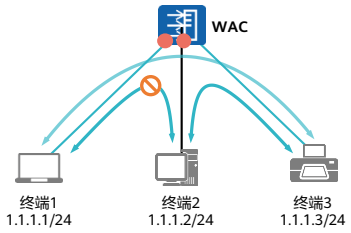
- 提高接口MAC地址学习优先级
- 不允许相同优先级接口MAC地址漂移

值得注意的是，MAC漂移的出现多数是由于网络中存在环路，或者出现了攻击行为，上述手段可以防止出现MAC地址漂移，但是“治标不治本”，治本的方法是解决环路问题，或排查攻击行为。

HUAWEI

- 网络中产生环路或非法用户进行网络攻击都会造成MAC地址发生漂移，导致MAC地址不稳定。可以通过两种方法来避免这种情况：
  - 提高接口MAC地址学习优先级接口配置不同的MAC地址学习优先级后，如果不同接口学到相同的MAC地址表项，那么高优先级接口学到的MAC地址表项可以覆盖低优先级接口学到的MAC地址表项，防止MAC地址发生漂移。
  - 不允许相同优先级接口MAC地址漂移网络中WLAN设备的上行接口连接服务器，下行接口连接用户。为防止非法用户伪造服务器MAC地址入侵WLAN设备，可以配置不允许相同优先级的接口发生MAC地址漂移。这样接口将不再学习相同的MAC地址，非法用户将无法使用网络设备MAC地址干扰WLAN设备与网络设备正常通信。

端口隔离



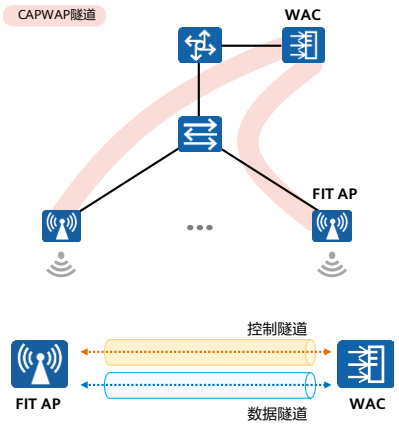
需求

- 实现同一个VLAN内不同用户之间的隔离，加强用户通信安全，避免无效的广播报文影响业务。
- 实现同一个VLAN内不同用户之间交互的数据能够通过上层设备集中转发。

方案

- 采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。
- 只需将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。
- 端口隔离分为二层隔离三层互通和二层三层都隔离两种模式：
  - 如果用户希望隔离同一VLAN内的广播报文，但是不同端口下的用户还可以进行三层通信，则可以将隔离模式设置为二层隔离三层互通。
  - 如果用户希望同一VLAN不同端口下用户彻底无法通信，则可以将隔离模式配置为二层三层均隔离。

CAPWAP数据隧道加密

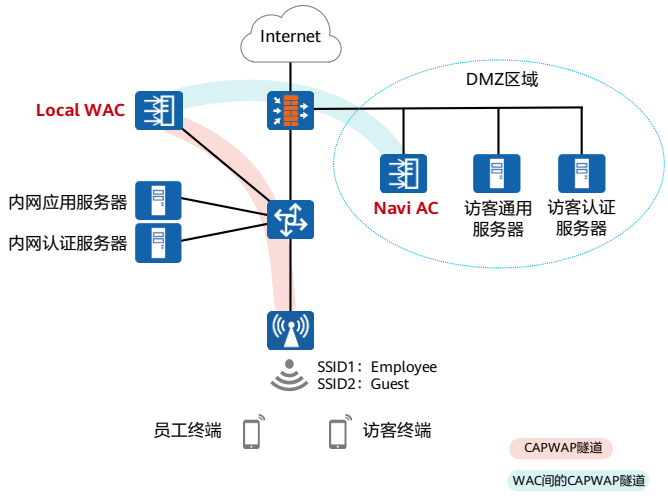


- 数据转发方式为隧道转发时，AP和AC之间的业务数据报文通过CAPWAP数据隧道传输。
- 为了进一步提升业务数据安全性，可以通过命令开启CAPWAP数据隧道DTLS加密功能，对CAPWAP数据隧道中的报文进行加密传输。

HUAWEI

- 数据转发方式为隧道转发时，AP和AC之间的业务数据报文通过CAPWAP数据隧道传输。为了进一步提升业务数据安全性，可以通过命令capwap dtls data-link encrypt enable开启CAPWAP数据隧道DTLS加密功能，对CAPWAP数据隧道中的报文进行加密传输。
- 系统视图和AP系统模板视图均可以配置CAPWAP数据隧道DTLS加密功能，两者的区别在于：前者是对AC上在线且支持该功能的AP生效，后者是对配置了AP系统模板下的AP生效。该功能从优先级的角度来看，AP系统模板视图下的优先级高于系统视图，当AP系统模板视图下也开启了CAPWAP数据隧道DTLS加密功能后，以AP系统模板视图下的配置为准。
- 在AP系统模板视图下开启CAPWAP数据隧道DTLS加密功能。
  - <HUAWEI> system-view
  - [HUAWEI] wlan
  - [HUAWEI-wlan-view] ap-system-profile name system1
  - [HUAWEI-wlan-ap-system-prof-system1] capwap dtls data-link encrypt enable #在系统视图下开启CAPWAP数据隧道DTLS加密功能。
  - <HUAWEI> system-view
  - [HUAWEI] capwap dtls data-link encrypt

Navi AC (1)

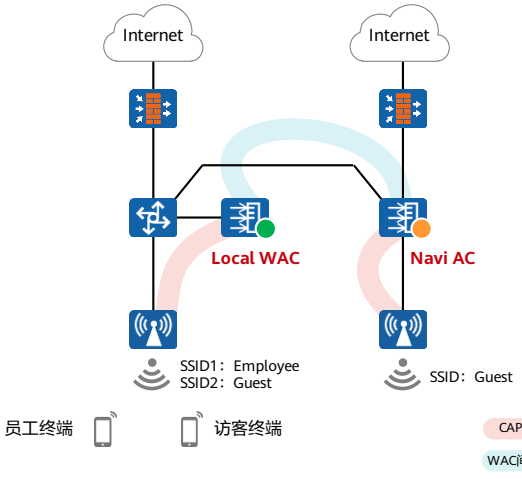


Navi AC方案说明

1. 大型企业在部署无线网络时，需同时为内部员工及访客提供接入服务，而访客数据可能会给网络带来潜在的安全威胁。
2. 企业可以将访客流量引导到DMZ区域中的Navi AC进行集中管理，从而实现内部员工接入和访客接入安全隔离。

1. **Local WAC**：承担对AP的集中管理和协同功能，如STA上线、AP配置下发等。
2. **Navi AC**：集中处理无线用户的安全、控制和管理等功能，如身份认证、授权和计费等。
3. **Local AC和Navi AC间的CAPWAP隧道**：Local AC上的用户数据报文通过CAPWAP隧道集中到Navi AC上进行转发。

Navi AC (2)



典型应用场景

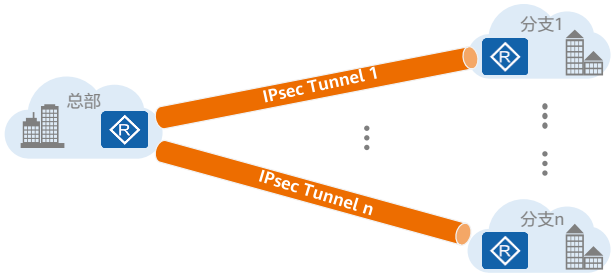
1. 企业员工和访客流量安全隔离，访客管控与内网解耦。
2. 业务出口和运营出口独立。
3. 员工统一在Local AC认证、授权，认证点在Local AC。
4. 访客流量统一经Local AC CAPWAP转发到Navi AC认证授权，认证点在Navi AC。
5. 员工流量经过Local AC出口到Internet。
6. 访客流量统一经Local AC CAPWAP转发到Navi AC出口到Internet。

HUAWEI

- 上行流量（AP-->Local AC-->Navi AC）：
  - AP接收到用户报文后，如果发现是上行业务数据，并且发现该VAP的转发方式是隧道转发，则直接将用户报文进行CAPWAP封装并发给Local AC。
  - Local AC接收到报文后，进行解封装，并识别出该用户报文归属的VAP。Local AC会对VAP进行判断，如果该VAP是Navi AC类型的VAP（下文简称Navi VAP），则Local AC将会对用户报文再次进行CAPWAP封装，并携带Navi VAP标记（即WLAN ID，该WLAN ID用于建立Navi AC和Local AC之间的CAPWAP隧道）、用户VLAN等信息，然后将报文发送给Navi AC。
  - Navi AC接收到报文后，进行解封装，并根据携带的Navi VAP标记，识别出该用户报文归属的VAP，并执行对应的VAP业务，如认证业务等。
- 下行流量（Navi AC-->Local AC-->AP）：
  - Navi AC接收到报文后，如果发现报文是无线下行业务数据，则先执行对应的下行业务，再将用户报文进行CAPWAP封装并发给Local AC。
  - Local AC接收到报文后，进行解封装。Local AC将下行报文再次进行CAPWAP封装后转发到AP。
  - AP接收到报文后，进行解封装。如果是单播报文，则通过转发表进行转发，如果是广播报文，则根据VLAN进行转发。

IPSec隧道

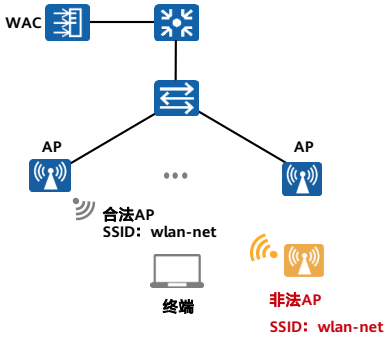
- IPSec通过在IPSec对等体间建立双向安全联盟形成一个安全互通的IPSec隧道，并通过定义IPSec保护的数据流将要保护的数据引入该IPSec隧道，然后对流经IPSec隧道的数据通过安全协议进行加密和验证，进而实现在Internet上安全传输指定的数据。
- IPSec安全联盟可以手工建立，也可以通过IKEv1或IKEv2协议自动协商建立。本文重点介绍如何定义IPSec保护的数据流、IKE自动协商建立安全联盟的过程。



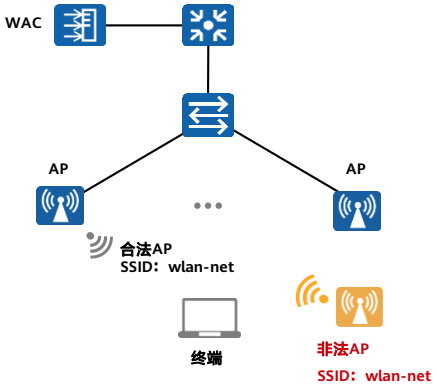
目录

案例：非法AP模糊匹配反制

- 案例描述：通常银行、机场等公共场所提供WLAN上网服务，用户搜索到SSID后即可接入网络。但是如果存在私设AP，并设置与合法SSID相同或相似的SSID，用户搜索SSID时，有可能误接入到私设AP，存在安全隐患。为了解决此问题，可以配置设备检测和反制。开启非法AP模糊匹配反制后，对非法AP进行反制，使用户从仿冒SSID下线。



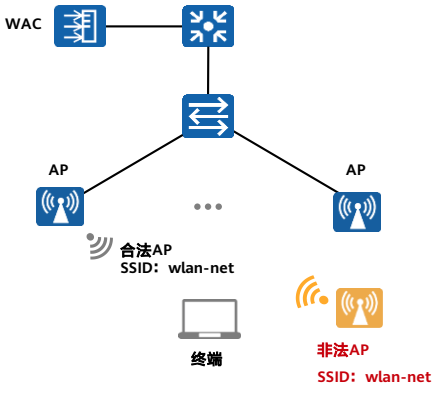
配置思路



配置思路

- 配置WLAN基本业务，使STA可正常接入WLAN网络。
- 配置SSID仿冒识别规则。
- 配置非法设备检测和反制功能，使AP能够检测无线设备信息并上报给AC，并对识别的非法设备进行反制，使STA断开和非法设备的连接。

配置模糊匹配规则



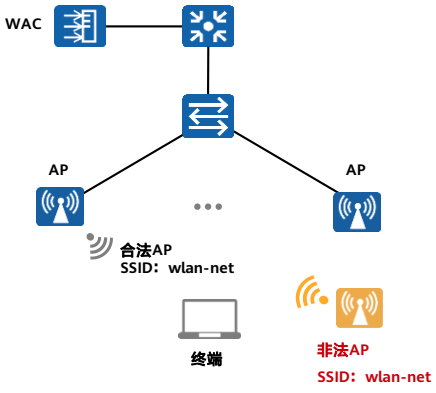
创建名为“default”的SSID仿冒识别规则模板，并配置仿冒SSID模糊匹配字符为wlan，使用正则表达式**^wlan$**。

```
[WAC-wlan-view] wids-spoof-profile name default
[WAC-default-spoof-prof-default] spoof-ssid fuzzy-match regex ^wlan$
[WAC-default-spoof-prof-default] quit
```


HUAWEI

- 合法SSID是wlan-net，可能存在仿冒SSID有wlan-nat或wlan，可使用正则表达式^wlan$配置模糊匹配规则。

开启检测及反制功能



开启设备检测以及设备反制功能

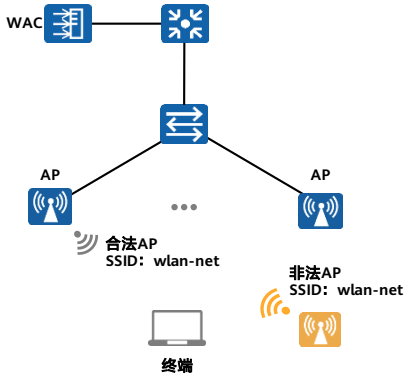
```
[AC-wlan-view] ap-group name default
[AC-wlan-ap-group-default] radio 0
[AC-wlan-group-radio-default/0] wids device detect enable
[AC-wlan-group-radio-default/0] wids contain enable

[AC-wlan-view] ap-group name default
[AC-wlan-ap-group-default] radio 1
[AC-wlan-group-radio-default/1] wids device detect enable
[AC-wlan-group-radio-default/1] wids contain enable

[AC-wlan-view] wids-profile name default
[AC-default-prof-default] contain-mode spoof-ssid-ap
[AC-default-prof-default] wids-spoof-profile default

[AC-wlan-ap-group-default] ap-group name default
[AC-wlan-ap-group-default] wids-profile default
```

配置案例：非法AP模糊匹配反制 - 结果验证



通过命令**display wlan ids contain ap**可以查看到被反制的AP。

```
[AC-wlan-view] display wlan ids contain ap
#Rf: Number of monitor radios that have contained the device
CH: Channel number
--------------------------------------------------------------------------------
 MAC address  CH  Authentication  Last detected time  #Rf  SSID
--------------------------------------------------------------------------------
000b-6b8f-fc6a 11  wpa-wpa2        2014-11-20/16:16:57 1   wlan-net
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

STA试图通过非法AP连接无线网络，但非法AP受到反制，STA的流量断开后，连入合法AP，流量正常。

思考题

1. WPA3加密密钥算法有多少位?

- 192

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

WLAN网络准入控制

HUAWEI

前言

- 网络准入控制（Network Admission Control，NAC）从对接入网络的终端安全控制入手，将终端安全状况和网络准入控制结合在一起，通过检查、隔离、加固和审计等手段，加强网络用户终端的主动防御能力，保证企业中每个终端的安全性，进而保护企业整网的安全性。
- 本文介绍了网络准入控制中用到的AAA机制及其相关技术，介绍了常用的准入认证方式包括802.1X认证、MAC认证、Portal认证以及混合认证的原理详解以及用户授权方式，介绍了华为NAC解决方案，并对NAC典型方案配置进行了举例。

目标

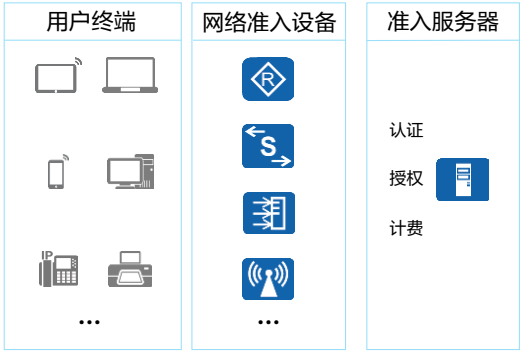
- 学完本课程后，您将能够：
  - 描述网络准入控制的基本概念
  - 描述AAA基本概念以及常用技术原理
  - 描述常见的认证方案及其工作原理
  - 描述华为NAC解决方案以及相关特性
  - 完成华为NAC典型配置

目录

- NAC（Network Admission Control）：网络接入控制。
- 解决方案中包含（第三方应用认证、终端类型识别、NAC逃生机制）。

网络准入控制（NAC)概述

- NAC（Network Admission Control)称为网络接入控制，通过对接入网络的客户端和用户的认证保证网络的安全，是一种“端到端”的安全技术。

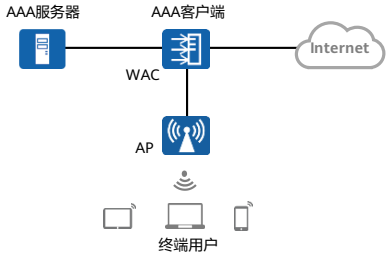


NAC系统架构

- **用户终端：**各种终端设备，例如PC、手机、打印机、摄像头等。
- **网络准入设备：**终端访问网络的认证控制点，准入设备对接入用户进行认证，是企业安全策略的实施者，按照网络制定的安全策略实施相应的准入控制（如允许接入网络或拒绝接入网络）。准入设备可以是交换机、路由器、无线接入控制器、无线接入点或者其他网络设备。
- **准入服务器（AAA)：**准入服务器的功能是实现对用户的认证、授权和计费。

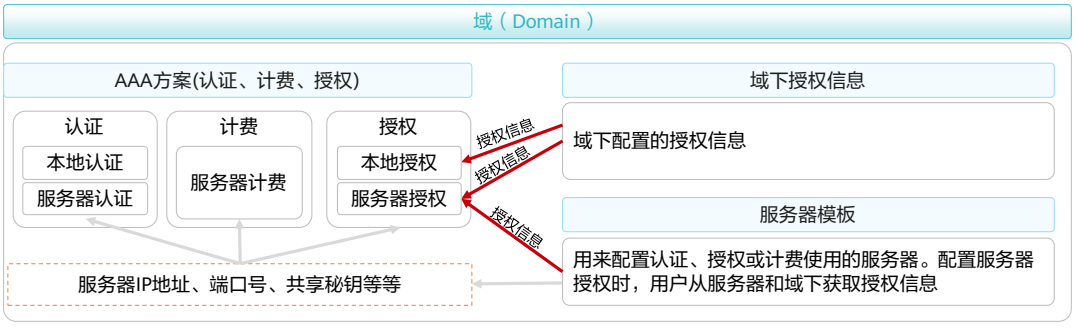
AAA简介

- AAA是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。
  - 认证：验证用户是否可以获得网络访问权。
  - 授权：授权用户可以使用哪些服务。
  - 计费：记录用户使用网络资源的情况。
- AAA采用客户端/服务器结构。
  - AAA客户端负责验证用户身份与管理用户接入。
  - AAA服务器负责集中管理用户信息。



AAA用户管理

- NAS（Network Access Server，网络接入服务器）设备对用户的管理是基于域的，每个用户都属于一个域，一个域是由属于同一个域的用户构成的群体。
- 域统一管理AAA方案、服务器模板和授权等配置信息。



- NAS设备一般包含WLAN设备（AC、AP）、交换机、防火墙等。
- NAC用户支持在认证模板下直接管理AAA方案、服务器模板和授权等AAA配置信息，可以不基于域来管理。
- 授权方法：
  - 授权方法为本地授权时，用户从域下获取授权信息。
  - 授权方法为服务器授权时，用户从服务器和域下获取授权信息。域下配置的授权信息比服务器下发的授权信息优先级低，如果两者的授权信息冲突，则服务器下发的授权优先生效；如果两者的授权信息不冲突，则两者的授权信息同时生效。这样处理可以通过域管理进行灵活授权，而不必受限于服务器提供的授权。

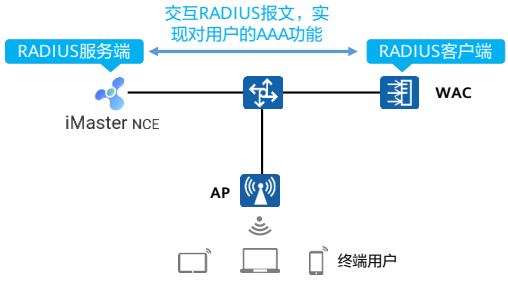
AAA常用技术方案

- 目前华为设备支持基于RADIUS、HWTACACS、HACA、LDAP或AD来实现AAA，在实际应用中， RADIUS最为常用。

技术方案	交互协议	认证	授权	计费
RADIUS	UDP	✓	✓	✓
HWTACACS	TCP	✓	✓	✓
HACA	HTTP2.0	✓	✓	✓
LDAP	TCP	✓	✓	✗
AD	TCP	✓	✓	✗
本地认证授权	/	✓	✓	✗

RADIUS概述

- AAA可以通过多种协议来实现，在实际应用中，最常使用RADIUS协议。
- RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。
- 该协议定义了基于UDP (User Datagram Protocol)的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为默认的认证、计费端口。
- RADIUS协议的主要特征如下：
  - 客户端/服务器模式
  - 安全的消息交互机制
  - 良好的扩展性



RADIUS架构描述

RADIUS客户端：一般位于NAS上

设备作为RADIUS协议的客户端，实现以下功能：

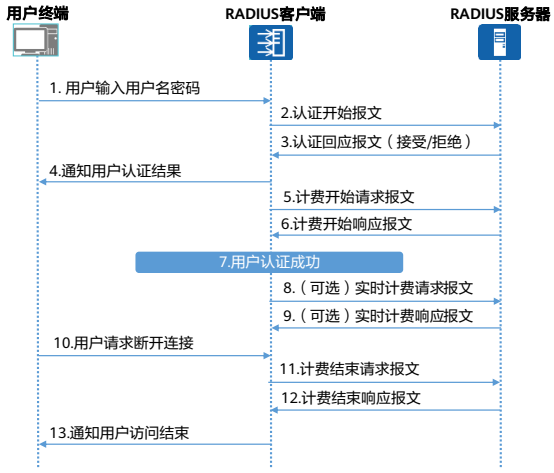
- 支持标准RADIUS协议及扩展属性，包括RFC2865、RFC2866。
- 支持厂商RADIUS扩展属性。
- RADIUS服务器状态探测功能。
- 计费结束请求报文的本地缓存重传功能。
- RADIUS服务器主备或负载分担功能。

RADIUS服务器：一般运行在中心计算机或工作站上，一般需要维护三个数据库

Users	Clients	Dictionary
用于存储用户信息（如用户名、密码以及使用的协议、IP地址等配置信息）。	用于存储RADIUS客户端的信息（如共享密钥、IP地址等）。	用于存储RADIUS协议中的属性和属性值含义的信息。

- RADIUS客户端可以遍布整个网络，负责传输用户信息到指定的RADIUS服务器，然后根据从服务器返回的信息进行相应处理（如接受/拒绝用户接入）。

RADIUS认证、授权、计费流程



RADIUS服务器状态探测

- 设备将RADIUS服务器的状态分为三种，三种状态的含义及出现的场景如下表所示：

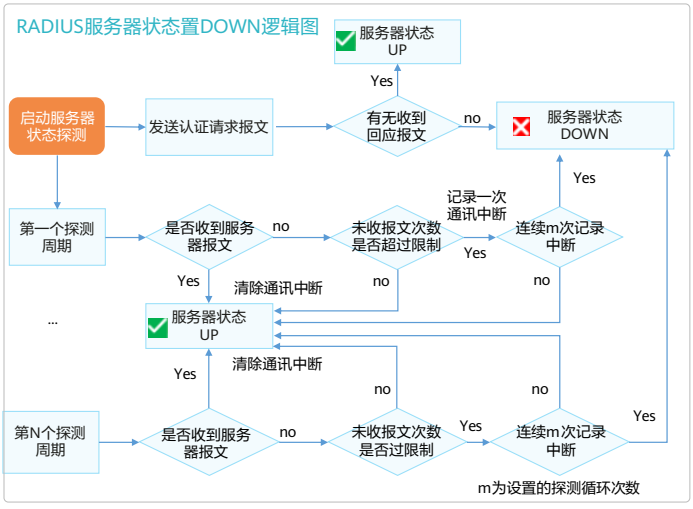
状态	RADIUS服务器是否可用	出现该状态场景
UP	RADIUS服务器可用。	RADIUS服务器的初始状态。 设备收到RADIUS服务器的报文。
DOWN	RADIUS服务器不可用。	满足将RADIUS服务器的状态标记为Down的条件。
Force-up（强制Up）	在没有可用的RADIUS服务器时，会选择Force-up状态的服务器。	dead-time定时器超时。

- 自动探测功能可以检测RADIUS服务器的可达性。按照RADIUS服务器状态的差异，自动探测可以分为以下三种情况：

状态	是否支持自动探测	何时发送自动探测报文
UP	通过命令行开启（radius-server detect-server up-server interval）	自动探测周期过后发送
DOWN	缺省支持	自动探测周期过后发送
Force-up（强制Up）	缺省支持	立即发送

- 设备在将RADIUS服务器的状态标记为Down后就会启动dead-time定时器，该定时器定义了Down状态可持续的时长。定时器超时后，设备将服务器的状态标记为Force-up。之后，如果有新用户需要通过RADIUS方式进行认证，在没有可用的RADIUS服务器的情况下，设备会尝试和Force-up状态的服务器重新建立连接。
- RADIUS服务器的可用性和可维护性是用户接入认证的基本条件，当设备与RADIUS服务器之间无法通信时，RADIUS服务器不能对用户进行认证和授权。为了解决该问题，设备支持在RADIUS服务器Down时的用户逃生功能，即RADIUS服务器Down后，用户无法获取服务器授权时，仍能够具有一定的网络访问权限。但是，RADIUS服务器Down时的用户逃生功能必须在设备将RADIUS服务器的状态标记为Down后才能启用。如果RADIUS服务器的状态没有标记为Down、设备又不能与RADIUS服务器正常通信，这会导致用户既获取不到服务器授权也不能进行逃生，进而造成用户没有任何网络访问权限。所以，设备必须及时感知到RADIUS服务器的状态，在RADIUS服务器状态为Down时，使用户能够获取逃生权限；在RADIUS服务器状态恢复Up后，用户退出逃生权限，进行重认证。
- 需要注意的是，对于用户账号存储在第三方服务器的场景，例如账号存储在AD\LDAP服务器，建议在本地RADIUS服务器上配置自动探测账号，以避免由于本地RADIUS服务器向第三方服务器查询账号导致服务器性能降低。

RADIUS服务器状态处理



服务器DOWN后的处理

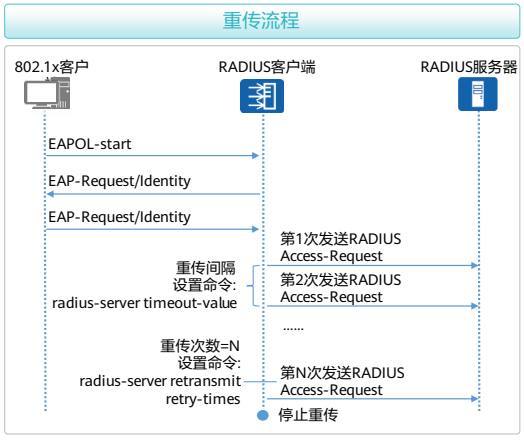
- 设备将RADIUS服务器的状态标记为Down之后，通过配置逃生功能，使用户能够进入逃生授权。
- 设备探测到RADIUS服务器状态恢复为Up后，通过配置重认证功能，使用户重认证获取RADIUS服务器授权。

HUAWEI

- 服务器DOWN的条件分为两种：
  - 在RADIUS服务器状态探测过程中，将RADIUS服务器标记为Down状态：系统启动后，RADIUS服务器状态探测定时器开始运行。从设备发送第一个RADIUS认证请求报文开始计算，如果设备一直没有收到RADIUS服务器的报文，并且在一个探测周期内满足条件：未收到RADIUS服务器报文的次数（n）大于或等于连续无响应的最大次数（dead-count），则记录一次通讯中断。在持续没有收到RADIUS服务器报文的情况下，探测周期循环几次，就在第几次记录通讯中断时将RADIUS服务器标记为Down。
  - 将长时间无响应的RADIUS服务器标记为Down状态：连续两个无响应的认证请求报文的时间间隔大于max-unresponsive-interval时，RADIUS服务器被标记为Down，此机制能够确保用户获取逃生授权。

RADIUS HWTACACS HACA LDAP AD 本地认证授权

RADIUS报文重传机制



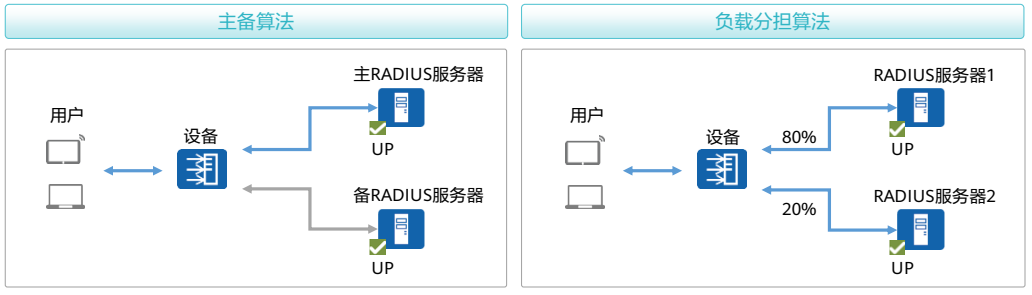
- 触发重传的条件
  - 用户认证过程中，设备发送认证请求报文到RADIUS服务器，当因网络故障、时延等原因导致设备无法收到服务器的回应报文时，会触发RADIUS报文重传，重传次数和重传间隔通过定时器进行控制。
- 停止重传的条件
  - 收到RADIUS服务器的回应报文，设备停止重传。
  - 达到最大重传次数后，设备停止重传。
  - 探测到RADIUS服务器的状态为Down，还没有达到最大重传次数，设备再进行一次重传。如果收到RADIUS服务器的回应报文，停止重传，并将RADIUS服务器的状态恢复为Up；如果未收到RADIUS服务器的回应报文，也停止重传，RADIUS服务器的状态为Down。

HUAWEI

- RADIUS报文重传是针对一个服务器而言的，如果RADIUS服务器模板中配置了多个服务器，整体重传时间取决于重传间隔、重传次数、RADIUS服务器的状态、服务器的个数以及选择服务器的算法。
- 满足以下任意一个条件，设备停止重传：收到RADIUS服务器的回应报文。收到RADIUS服务器的回应报文后，设备会停止重传，此时设备标记RADIUS服务器的状态为Up。
- 探测到RADIUS服务器的状态为Down。设备将RADIUS服务器的状态置为Down后：
  - 如果达到最大重传次数，则停止重传，RADIUS服务器的状态为Down。
  - 如果还没有达到最大重传次数，设备会再重传一次认证请求报文到RADIUS服务器。相当于给状态为Down的服务器一次机会。如果收到RADIUS服务器的回应报文，停止重传，并将RADIUS服务器的状态恢复为Up；如果未收到RADIUS服务器的回应报文，也停止重传，RADIUS服务器的状态为Down。
- 达到最大重传次数。达到最大重传次数后，设备会停止重传，此时：
  - 如果收到RADIUS服务器的回应报文，此时设备标记RADIUS服务器的状态为Up。
  - 如果已经探测到RADIUS服务器的状态为Down，设备将服务器的状态置为Down。
  - 如果没收到RADIUS服务器的回应报文也没有探测到服务器的状态为Down，此时，设备不会切换服务器的状态，服务器实际上没有响应。

RADIUS服务器选择机制

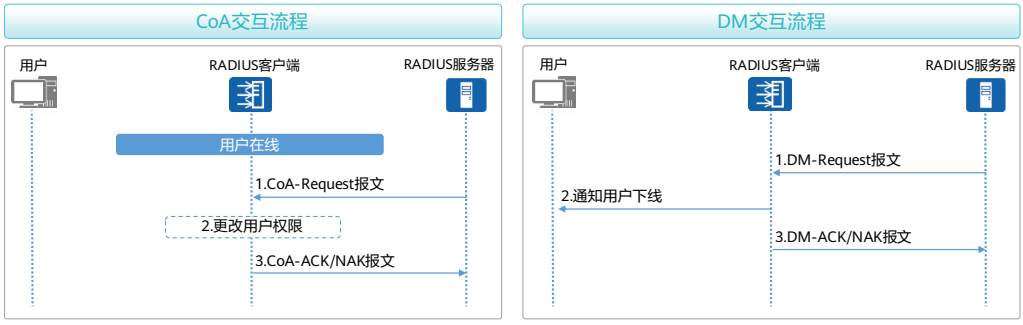
- 大型企业网络中通常会部署多台RADIUS服务器，这样做的目的一是为了在一台服务器故障的情况下，不会影响用户接入；二是为了在大量用户接入时，多个服务器之间能够负载均衡，单个服务器的资源不会被耗尽。
- 当RADIUS服务器模板中配置了多个服务器，设备在向服务器发送报文时，根据命令行的配置通过以下其中一种机制选择RADIUS服务器：



- 主备算法： 主备顺序根据配置RADIUS认证服务器或RADIUS计费服务器时的权重决定，权重值较大者为主，如果权重值相同，则先配置的服务器为主。在所有状态为Up的服务器中，优先向主服务器发送认证或计费报文，如果主服务器没有回应，则向备服务器发送。
- 负载分担算法：设备在向服务器发送认证或计费报文时，会根据配置RADIUS认证服务器或RADIUS计费服务器时的权重来分配报文发送的服务器。RADIUS服务器1的状态为Up、权重为80，RADIUS服务器2的状态为Up、权重为20。则设备向RADIUS服务器1发送报文的概率为80/(80+20)=80%，设备向RADIUS服务器2发送报文的概率为20/(80+20)=20%。
- 执行命令radius-server algorithm { loading-share | master-backup } [based-user] ，配置RADIUS服务器的运算法则。
  - 缺省情况下，RADIUS服务器采用主备运算法则。
  - 当RADIUS服务器模板下配置多台认证或者计费服务器时，设备根据配置的运算法则和权重参数weight，决定如何选择RADIUS服务器：若选择主备算法，则权重参数weight决定主备，weight值较大者为主，如果weight值相同，则先配置的服务器为主服务器。
  - 如选择负载均衡算法，则权重参数weight决定报文的分配。

RADIUS用户动态授权

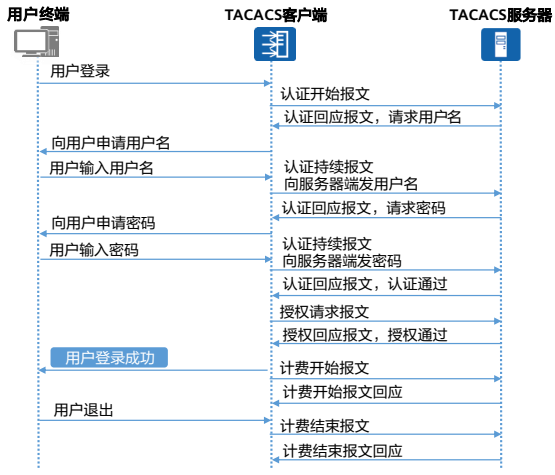
- 设备支持RADIUS CoA/DM功能，提供一种动态修改在线用户权限或者强制用户下线的机制。
- CoA (Change of Authorization)是指用户认证成功后，管理员可以通过RADIUS协议来修改在线用户的权限或对其进行重认证。
- DM (Disconnect Message)是指用户下线报文，即由RADIUS服务器主动发起的强制用户下线的报文。



HWTACACS协议介绍

简介

- HWTACACS（华为终端访问控制器控制系统协议）是在TACACS (RFC 1492)基础上进行了功能增强的安全协议。是一种集中式的、客户端/服务器结构的信息交互协议，使用TCP协议传输，TCP端口号为49。
- HWTACACS提供的认证、授权和计费服务相互独立，能够在不同的服务器上实现。
- HWTACACS协议主要用于采用点对点协议PPP (Point-to-Point Protocol)或虚拟私有拨号网络VPDN (Virtual Private Dial-up Network)方式接入Internet的接入用户以及对设备进行操作的管理用户的认证、授权和计费。



HUAWEI

- HWTACACS协议与其他厂商支持的TACACS+协议都实现了认证、授权、计费的功能。HWTACACS和TACACS+的认证流程与实现方式是一致的，HWTACACS协议能够完全兼容TACACS+协议。

HWTACACS与RADIUS对比

项目	HWTACACS	RADIUS
数据传输	通过TCP传输，网络传输更可靠。	通过UDP传输，网络传输效率更高。
加密方式	共享密钥，除了标准的HWTACACS报文头，对报文主体全部进行加密。	共享密钥，只是对认证报文中的密码字段进行加密。
认证和授权	认证与授权分离，使得认证、授权服务可以在不同的安全服务器上实现。	认证与授权结合不能分离。
命令行授权	支持对设备上的配置命令进行授权使用。	不支持对设备上的配置命令进行授权使用。
应用场景	因命令行授权功能强大，多用于设备认证。	适用范围较广，终端认证以及设备认证均适用。

- HWTACACS协议与RADIUS协议的相似点包括：结构上都采用客户端/服务器模式。
  - HWTACACS客户端：一般位于网络接入服务器NAS (Network Access Server)上，可以遍布整个网络，负责传输用户信息到指定的HWTACACS服务器，然后根据从服务器返回的信息进行相应处理。
  - HWTACACS服务器：一般运行在中心计算机或工作站上，维护相关的用户认证和网络服务访问信息，负责接收用户连接请求并认证用户，然后给客户端返回所有需要的信息。
- 都使用共享密钥对传输的用户信息进行加密。
- 都有较好的灵活性和可扩展性。
- 认证授权分离举例：例如，可以用一台HWTACACS服务器进行认证，另外一台HWTACACS服务器进行授权。
- 命令行授权：
  - 支持：即用户可使用的命令行受到命令级别和AAA授权的双重限制，某一级别的用户输入的每一条命令都需要通过HWTACACS服务器授权，如果授权通过，命令才可以被执行。
  - 不支持：用户登录设备后可以使用的命令行由用户级别决定，用户只能使用级别等于或低于用户级别的命令行。

RADIUS | HWTACACS | HACA | LDAP | AD | 本地认证授权

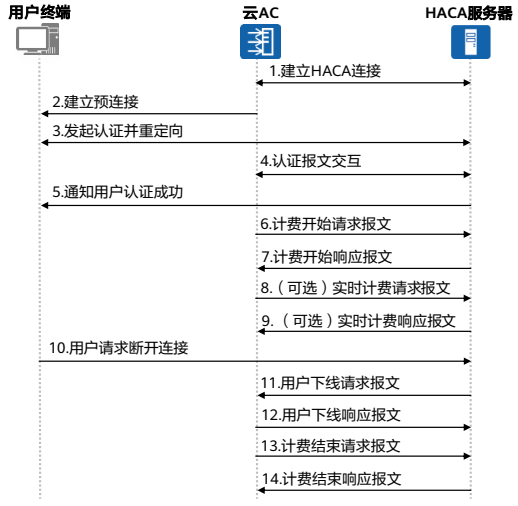
HACA协议介绍

简介

- CloudCampus云管理场景下用户准入认证采用Portal认证时，由于认证服务器部署在互联网中，设备到服务器之间可能需要穿越NAT，而普通的Portal认证采用Portal协议无法穿越NAT，因此采用华为敏捷云认证HACA (Huawei Agile Cloud Authentication)使设备与服务器之间建立连接，然后进行Portal认证。

应用场景

- HACA仅支持MAC优先的Portal认证场景，将iMaster NCE-Campus服务器作为HACA服务器部署在云端实现外置Portal服务器以及认证计费服务器。
- 当前仅支持iMaster NCE-Campus作为HACA服务器。



HUAWEI

- iMaster NCE-Campus是智简园区网络解决方案基于Web的集中式管理控制系统，支持网络业务管理、网络安全管理、用户准入管理、网络监控、网络质量分析、网络应用分析、告警和报表等特性，提供大数据分析的能力，同时提供开放的接口、支持与其他平台集成。企业用户可以通过iMaster NCE-Campus进行业务配置、日常运维等工作，实现规模设备的集中管理。
- 支持Portal认证或MAC优先的Portal认证。

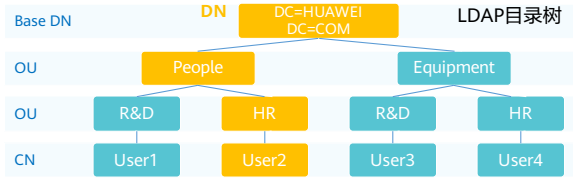
LDAP协议介绍

简介

- 轻量级目录存取协议LDAP (Lightweight Directory Access Protocol)是一种目录访问协议。
- LDAP协议是基于Client/Server结构提供目录信息的绑定和查询，所有的目录信息存储在LDAP服务器上。
- LDAP定义了多种操作来实现LDAP的各种功能，其中可以利用LDAP的绑定和查询操作来实现用户的认证和授权功能。

应用场景

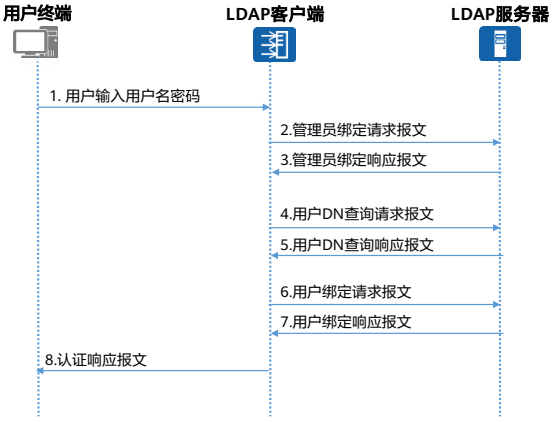
- 网络接入设备和LDAP服务器对接，利用LDAP的绑定和查询操作来实现用户的认证和授权功能。



- CN (Common Name)：通用名称。表示对象名称。
- DC (Domain Controller)：域控制器。表示对象所属的区域，一般一台LDAP服务器即为一个域控制器。
- DN (Distinguished Name)：区别名。对象的位置，从对象开始逐层描述到根区别名，例如User1的DN为"CN=User1，OU=R&D，OU=People，dc=HUAWEI，dc=COM"。
- Base DN：根区别名。
- OU (Organization Unit)：组织单元。表示对象所属的组织。

RADIUS HWTACACS HACA LDAP AD 本地认证授权

LDAP认证、授权流程



LDAP搜索/绑定：

绑定 (bind)是一个专有术语，用于描述LDAP客户端发起请求与LDAP服务器建立会话的过程。搜索绑定是以匿名方式或使用固定帐户连接到LDAP服务器，并搜索认证用户的专有名称，搜索成功则尝试再次使用用户的密码进行绑定。

用户DN查询：

LDAP服务器收到用户DN查询请求报文后，根据报文中的查询起点、查询范围、以及过滤条件，对用户DN进行查找。查询得到的用户DN可以是一个或多个。例如目录结构信息，查询起点为"dc=HUAWEI，dc=COM"，则返回的DN为"CN=User2，Departments=R&D，OU=People，dc=HUAWEI"和"CN=User2，Departments=R&D，OU=Equipment，dc=HUAWEI, dc=COM"。

HUAWEI

- 当用户需要访问LDAP服务器时，用户输入用户名和密码，向LDAP客户端发起认证请求。例如用户输入用户名为User2、密码为Huawei@123。
- LDAP客户端获取到用户的用户名和密码，以管理员DN和管理员密码为参数向LDAP服务器发送管理员绑定请求报文以获得查询权限。
- LDAP服务器收到管理员绑定请求报文后，验证管理员DN和管理员密码是否正确。如果管理员DN和管理员密码正确，则向LDAP客户端发送绑定成功的管理员绑定响应报文。
- LDAP客户端收到绑定响应报文后，以用户输入的用户名为参数构造过滤条件，向LDAP服务器发送用户DN查询请求报文。例如：构造过滤条件为CN=User2。
- LDAP服务器收到用户DN查询请求报文后，根据报文中的查询起点、查询范围、以及过滤条件，对用户DN进行查找。如果查询成功，则向LDAP客户端发送查询成功的响应报文。查询得到的用户DN可以是一个或多个。查询起点为"dc=huawei,dc=com"，则返回的DN为"CN=User2，Departments=R&D，OU=People，dc=huawei，dc=com"和“CN=User2，Departments=R&D，OU=Equipment，dc=huawei，dc=com"。
- LDAP客户端根据查询得到的用户DN和用户输入的密码为参数，向LDAP服务器发送用户绑定请求报文。
- LDAP服务器收到用户绑定请求报文后，检查用户输入的密码Huawei@123是否正确。
  - 如果用户输入的密码正确，则向LDAP客户端发送绑定成功的绑定响应报文。
  - 如果用户输入的密码不正确，则向LDAP客户端发送绑定失败的响应报文。LDAP客户端以查询到的下一个用户DN为参数，继续向LDAP服务器发送绑定请求，直至有一个DN绑定成功。如果所有用户DN都绑定失败，则LDAP客户端通知用户认证失败。

- 认证成功后，LDAP客户端通知用户认证成功，用户获得访问权限。

RADIUS HWTACACS HACA LDAP AD 本地认证授权

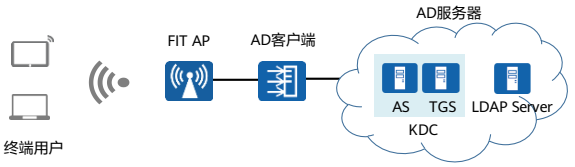
AD协议介绍

简介

- Kerberos是一种通过密钥系统实现在不安全的开放网络中安全传输数据的网络认证协议，它不要求网络上所有主机安全，并假定网络上传送的数据可以被任意地读取和修改。该协议基于TCP，对应的端口号为88。
- Kerberos协议可集成到LDAP认证过程中，利用Kerberos协议的对称密钥体制来提高密码传输的安全性，防止在LDAP认证过程中泄露用户的密码，这种集成了Kerberos协议的认证方式称为AD (Active Directory Users and Computers)认证。

应用场景

用于网络接入设备和AD服务器对接场景。



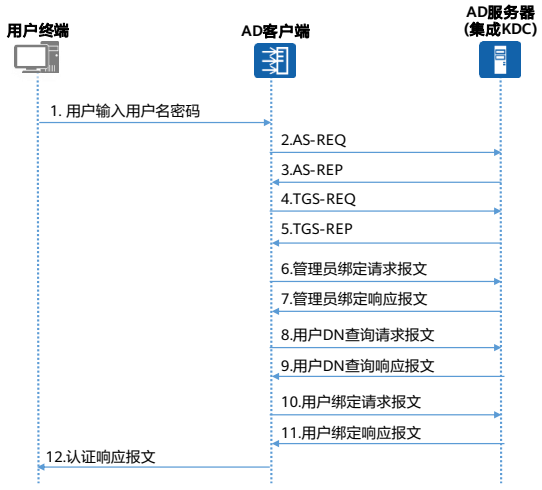
AD服务器组成

- LDAP Server：LDAP服务器，服务器上存储了所有的目录信息。
- KDC (Key Distribution Center)：密钥分配中心，也就是Kerberos服务器，存储了所有客户端的密码和账户信息。KDC由AS和TGS组成。
- AS (Authentication Server)：认证服务器，提供访问TGS的凭证Ticket。
- TGS (Ticket-Granting Server)：票据授予服务器，提供访问AD服务器的凭证Ticket。

HUAWEI

- AD客户端：集成了Kerberos和LDAP协议的接入设备。
- AD服务器：AD服务器是集成了Kerberos和LDAP认证的服务器，通常情况下，LDAP服务器和Kerberos服务器是合二为一的。

AD认证、授权流程



相比LADP的认证、授权流程，AD的认证、授权流程增加了2~5加解密流程。

2. 向Kerberos服务器发送AS-REQ请求报文，该报文以明文形式向Kerberos服务器发送用户名

3. AS服务器向客户端返回AS-REP报文，AS-REP报文中用AS和TGS服务器的共享密钥对Ticket进行加密，再用客户端的密码对加密后的Ticket和会话密钥Session key进行加密。

4. AD客户端用自己的密码解密AS-REP报文，获得Session key和加密后的Ticket。

5. Kerberos服务器用AS和TGS之间共享的密钥解密Ticket，提取Ticket中的Session key，利用Session key解密认证单Authenticator，获得认证单中的客户端名称和时间信息与Ticket中的信息一致的话，则验证通过，发送REP报文。

- 当用户需要访问AD服务器时，用户发起认证请求，向AD客户端发送用户名和密码。
- 当AD客户端首次访问AD服务器时，需要向集成在AD服务器中的Kerberos服务器验证自己的身份，向Kerberos服务器发送AS-REQ请求报文，该报文以明文形式向Kerberos服务器发送用户名。
- Kerberos服务器根据获取的用户名在数据库中查找此用户。如果查找成功，AS服务器会生成一个Kerberos服务器和客户端之间共享的会话密钥Session key。同时AS服务器会生成一个Ticket，AD客户端以后就可以凭这个Ticket向Kerberos服务器请求访问AD服务器的凭证，无需再验证自己的身份了。AS服务器向客户端返回AS-REP报文，AS-REP报文中用AS和TGS服务器的共享密钥对Ticket进行加密，再用客户端的密码对加密后的Ticket和会话密钥Session key进行加密。
- AD客户端用自己的密码解密AS-REP报文，获得Session key和加密后的Ticket。AD客户端向Kerberos服务器发送TGS-REQ报文请求获得访问AD服务器的Ticket，报文中包括一个认证单Authenticator、加密后的Ticket、客户端名称、AD服务器名称等。认证单Authenticator是利用Session key加密的客户端用户名、IP地址、时间信息、域名等信息。
- Kerberos服务器用AS和TGS之间共享的密钥解密Ticket，提取Ticket中的Session key，利用Session key解密认证单Authenticator，获得认证单中的客户端名称和时间信息与Ticket中的信息一致的话，则验证通过。Kerberos服务器会向客户端返回一个利用客户端密码加密的TGS-REP报文，报文包括客户端与AD服务器的会话密钥，以及利用AD服务器的密码加密后的Ticket。Ticket中包括会话密钥Session key、客户端名称、服务器名称、Ticket的有效期等。Kerberos客户端利用自身密码解密TGS-REP报文，获得客户端与AD服务器共享的Session key以及利用AD服务器密码加密后的可以访问AD服务器的Ticket。

- 第6步到第12步，与LDAP认证、授权流程的第2步到第8步基本一致，差异在于第10步用户绑定过程采用Session Key和凭证Ticket对用户密码进行加密和验证，提高了认证的安全性:第10步的用户绑定请求报文中，包含了AD客户端利用Session key对用户名和密码进行加密的认证单Authenticator，以及利用AD服务器密码加密后的访问AD服务器的凭证Ticket。
- AD服务器收到用户绑定请求报文，先用自己的服务器密码解开凭证Ticket，然后查看Ticket是否在有效期内，在有效期内，用Ticket中携带的会话密钥Session key解密认证单Authenticator，然后进行用户绑定请求报文的处理，检查用户输入的密码是否正确。

RADIUS HWTACACS HACA LDAP AD 本地认证授权

本地认证、授权

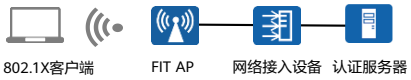
- 设备作为AAA服务器时被称为本地AAA服务器，本地AAA服务器支持对用户进行认证和授权，不支持计费。
- 以内置EAP认证为例，手机终端不支持PAP和CHAP协议时，手机终端无法支持配置为802.1X+本地认证方式。此时可以配置内置EAP认证。设备充当认证服务器和用户信息数据库，无线客户端在本地进行身份验证。
- 内置EAP认证功能支持EAP-PEAP、EAP-TLS、EAP-TTLS认证方式，这些认证方式需要使用证书。

HUAWEI

- 内置EAP认证实现802.1X认证：组网中未部署外置的认证服务器时，通过AC作为内置EAP服务器实现802.1X认证。
- 内置EAP认证和外置认证服务器组合场景：组网中有外置的认证服务器，当外置认证服务器可用时，通过外置服务器实现802.1X认证。当外置服务器故障时，已在线用户保持在线状态，新接入用户通过AC内置EAP服务器进行802.1X认证。
- 内置EAP认证不支持服务器探测功能。
- 内置EAP认证不支持计费功能。
- 内置EAP认证不支持服务器授权功能。

目录

802.1X认证概述



简介

- 802.1X认证是一种基于端口的网络接入控制协议，即在接入设备的端口这一级验证用户身份并控制其访问权限。
- 802.1X认证使用EAPoL（Extensible Authentication Protocol over LANs，局域网可扩展认证协议）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。

组网方式

- 802.1X客户端一般为用户终端设备，用户可以通过启动客户端软件发起802.1X认证。
- 网络接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

应用场景

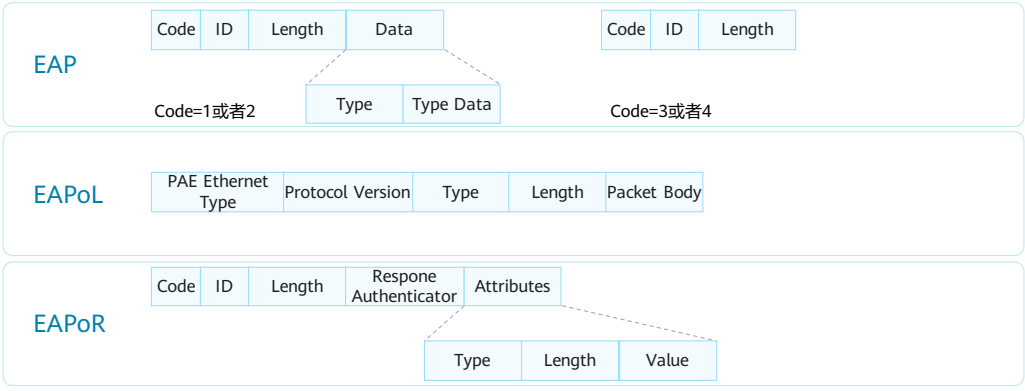
- 适用于对安全要求较高的办公用户认证场景。

HUAWEI

- 802.1X协议为二层协议，不需要到达三层，对接入设备的整体性能要求不高，可以有效降低建网成本。
- 认证报文和数据报文通过逻辑接口分离，提高安全性。

802.1X认证协议

- 802.1X认证系统使用可扩展认证协议EAP (Extensible Authentication Protocol)来实现客户端、设备端和认证服务器之间的信息交互。



HUAWEI

- EAPoL：802.1X协议定义的一种报文封装格式，主要用于在客户端和设备之间传送EAP协议报文，以允许EAP协议报文在LAN上传送。
- EAPoR：EAP报文被直接封装到RADIUS报文中（EAP over RADIUS，简称为EAPoR），以便穿越复杂的网络到达认证服务器。为支持EAP中继方式，RADIUS协议增加了两个属性：EAP-Message（EAP消息）和Message-Authenticator（消息认证码）。其中，EAP-Message属性用来封装EAP报文，Message-Authenticator属性用于对认证报文进行认证和校验，防止非法报文欺骗。

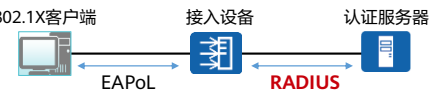
802.1X认证方式

- 根据接入设备对802.1X客户端发送的EAPoL报文处理机制的不同，可将认证方式分为EAP中继方式和EAP终结方式。

EAP中继方式

- 接入设备将802.1X客户端发来的EAP报文直接封装到RADIUS报文中，无需对EAP内的数据进行处理。
- 这种方式对认证服务器的要求较高。

EAP终结方式

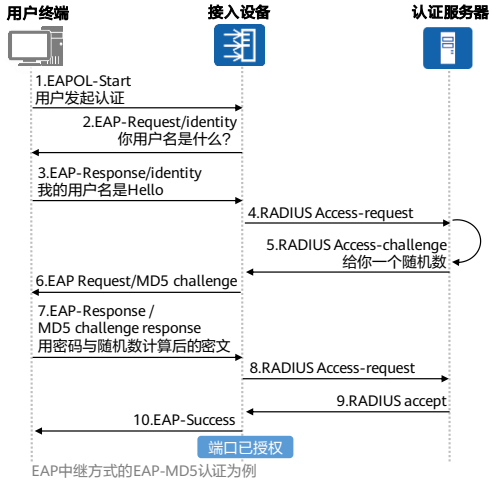


- 接入设备需要“提取”EAP报文中的信息并封装到RADIUS报文中发送给认证服务器。
- 这种方式对接入设备的要求较高。

HUAWEI

- EAP中继方式的优点是设备端处理更简单，支持更多的认证方法，缺点则是认证服务器必须支持EAP，且处理能力要足够强。对于常用的EAP-TLS、EAP-TTLS、EAP-PEAP三种认证方式，EAP-TLS需要在客户端和服务器上加载证书，安全性最高，EAP-TTLS、EAP-PEAP需要在服务器上加载证书，但不需要在客户端加载证书，部署相对灵活，安全性较EAP-TLS低。
- EAP终结方式的优点是现有的RADIUS服务器基本均支持PAP和CHAP认证，无需升级服务器，但设备端的工作比较繁重，因为在这种认证方式中，设备端不仅要从来自客户端的EAP报文中提取客户端认证信息，还要通过标准的RADIUS协议对这些信息进行封装，且不能支持除MD5-Challenge之外的其它EAP认证方法。PAP与CHAP的主要区别是CHAP密码通过密文方式传输，而PAP密码通过明文的方式传输。因而PAP方式认证的安全性较低，实际应用通常采用CHAP方式认证。

802.1X认证流程



EAP中继方式的EAP-MD5认证为例

认证触发方式

- **客户端主动触发方式：**用户主动开启客户端输入用户名和密码向接入设备发送EAP报文来触发认证。
- **接入设备主动触发方式：**接入设备在接收到用户终端发送的DHCP/ARP报文后，主动触发用户终端自动弹出客户端界面，用户输入用户名和密码即可启动认证。

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。

HUAWEI

- EAP终结方式与EAP中继方式的认证流程相比，不同之处在于用来对用户密码信息进行加密处理的MD5 Challenge由设备端生成，之后设备端会把用户名、MD5 Challenge和客户端加密后的密码信息一起送给RADIUS服务器，进行相关的认证处理。而在EAP中继方式中，用来对用户密码进行加密处理的挑战字由认证服务器生成，设备端只是负责将EAP报文封装在RADIUS报文中透传认证服务器，整个认证处理都由认证服务器来完成。

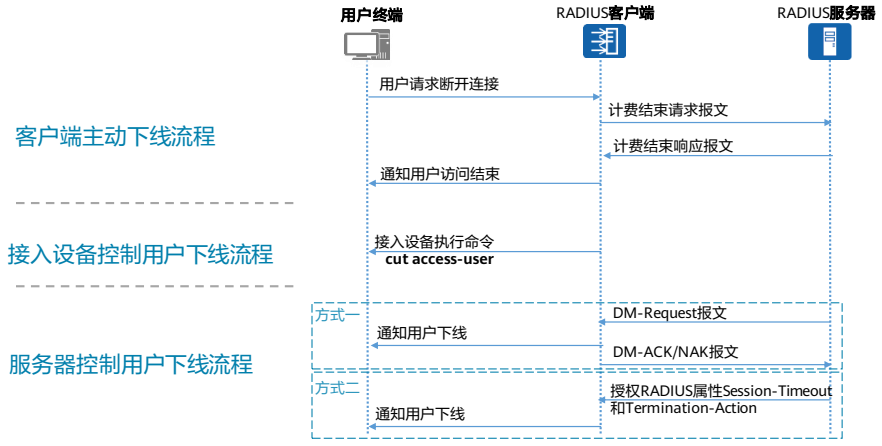
802.1X重认证

当前用户状态	配置点	配置方式	触发条件
认证成功状态	接入设备侧	802.1X认证成功用户进行周期性重认证	定期触发
		手动对指定MAC地址进行单次重认证	手动触发
	RADIUS服务器侧	对用户下发RADIUS标准属性	条件触发
认证异常状态（RADIUS服务器Down）	接入设备侧	当RADIUS服务器真正UP时对用户进行重认证	条件触发

- 认证成功状态：若管理员在认证服务器上修改了某一用户的访问权限、授权属性等参数，此时如果用户已经在线，则需要及时对该用户进行重认证以确保用户的合法性。配置对在线802.1X用户进行重认证功能后，设备会把保存的在线用户的认证参数（用户上线后，设备上会保存该用户的认证信息）发送到认证服务器进行重认证，若认证服务器上用户的认证信息没有变化，则用户正常在线；若用户的认证信息已更改，则用户将会被下线，此后用户需要重新进行认证。
- 用户在预连接阶段或认证失败阶段：设备会记录用户表项信息，并能够为用户分配受限的网络访问权限。为使用户能够及时认证成功，获取正常的网络访问权限，设备根据用户表项对没有认证成功的用户进行重认证。在用户表项老化时间到达之前，如果用户重认证没有成功，设备将删除对应的表项信息，并收回授予用户的网络访问权限；如果用户重认证成功，设备将用户加入到认证成功的用户表项，并授予认证成功后的网络访问权限。

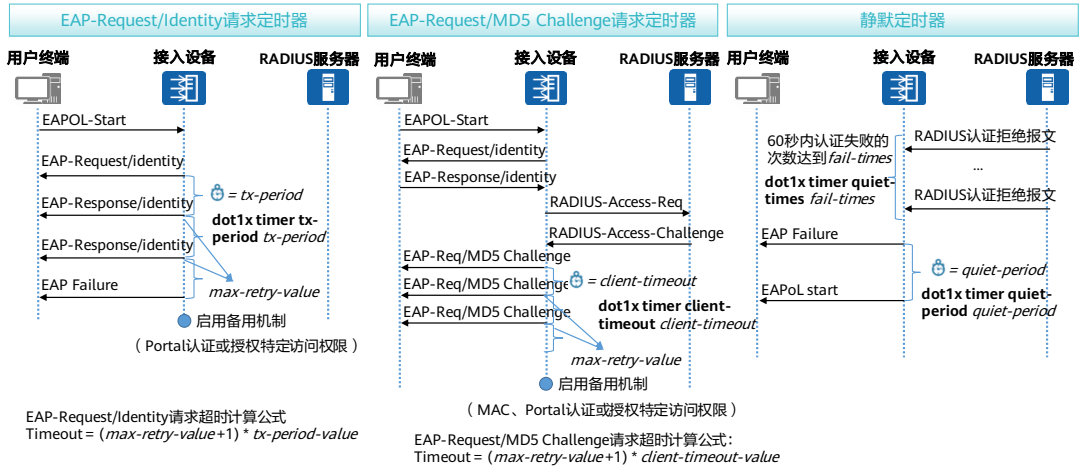
802.1X认证用户下线

- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。



- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。
- 接入设备控制用户下线
  - 在接入设备上执行命令cut access-user强制指定用户下线。当管理员发现非法用户在线，或在测试中想让某一用户下线后重新上线，可以通过在设备上执行命令强制该用户下线。
- 服务器控制用户下线有以下方式：
  - RADIUS服务器可通过DM报文（Disconnect Message）强制用户下线。DM(Disconnect Message)是指用户离线报文，即由RADIUS服务器端主动发起的强迫用户下线的报文。
  - RADIUS服务器通过授权RADIUS标准属性Session-Timeout和Termination-Action。其中，Session-Timeout为用户在线时长定时器，Termination-Action属性值为0表示将用户下线。当用户在线的时长达到定时器指定的数值时，设备会将用户下线。

802.1X定时器



HUAWEI

- EAP-Request/Identity请求定时器：在802.1X认证中，设备会向客户端发送EAP-Request/Identity报文请求用户名，请求报文的重传次数和时间间隔由命令行控制。
- EAP-Request/MD5 Challenge请求定时器：设备启动802.1X客户端认证超时定时器。若在该定时器设置的时长内，设备没有收到客户端的响应，则设备将重发该报文。若设备重传请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。这能够避免不断重复向用户发送认证请求报文而占用大量的设备资源。
- 802.1X认证静默定时器：使能静默功能后，若某一用户在60秒内认证失败的次数超过规定的值，则设备会将该用户静默一段时间，在静默时间内，设备会丢弃该用户的802.1X认证请求，从而避免用户在短时间内频繁认证失败。

目录

Portal认证概述

简介

- Portal认证也称为Web认证。
- 用户可以通过Web认证页面，输入用户帐号和密码信息，实现对终端用户身份的认证。
- 用户可通过两种方式实现认证页面访问：
  - 主动认证：用户通过浏览器主动访问Portal认证网站。
  - 重定向认证：用户输入的访问地址不是Portal认证网站地址，被接入设备强制访问Portal认证网站（通常称为重定向）。

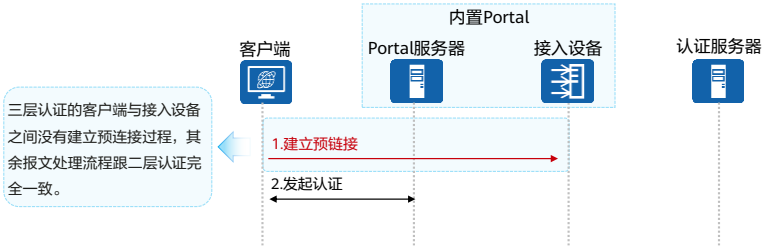
应用场景

Portal认证不需要安装专门的客户端软件，因此主要用于无客户端软件要求的接入场景或访客接入场景。

- 客户端：一般情况下，客户端是安装有运行HTTP/HTTPS协议的浏览器的主机，有时也会有安装相应的客户端软件（如浏览器）。
- 接入设备：交换机、路由器等接入设备的统称，主要有三方面的作用。
  - 在认证之前，将认证网段内用户的所有HTTP/HTTPS请求都重定向到Portal服务器。
  - 在认证过程中，与Portal服务器、认证服务器交互，完成对用户身份认证、授权与计费的功能。
  - 在认证通过后，允许用户访问被管理员授权的网络资源。
- Portal服务器：接收客户端认证请求的服务器系统，提供门户（Portal）服务和认证界面，与接入设备交互客户端的认证信息。
- 认证服务器：与接入设备进行交互，完成对用户的认证、授权与计费。
- Portal认证的优点：
  - 一般情况下，客户端不需要安装额外的软件，直接在网页上认证，简单方便。
  - 便于运营，可在网页上进行广告发布、企业宣传等业务拓展。
  - 技术成熟，被广泛应用于运营商、连锁快餐、酒店、学校等网络。
  - 部署位置灵活，可以在接入层或关键入口作访问控制。
  - 用户管理灵活，可基于用户名与VLAN/IP地址/MAC地址的组合对用户进行认证。

Portal认证方式

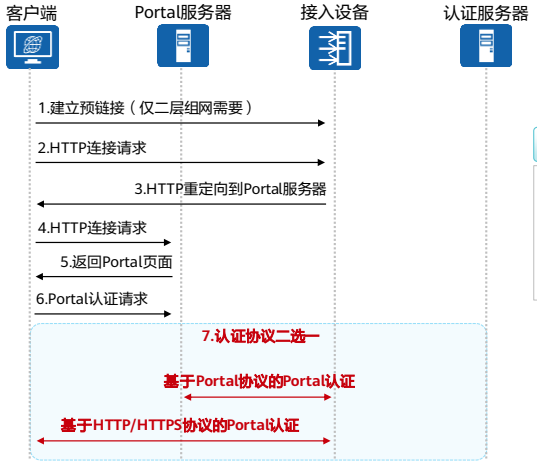
- 按照网络中实施Portal认证的网络层次来分，Portal认证方式分为两种：二层认证方式和三层认证方式。
  - 二层认证方式：客户端与接入设备直连（或之间只有二层设备存在），设备能够学习到用户的MAC地址并可以利用IP和MAC地址来识别用户，此时可配置Portal认证为二层认证方式。
  - 三层认证方式：当设备部署在汇聚层或核心层时，在认证客户端和设备之间存在三层转发设备，此时设备不一定能获取到认证客户端的MAC地址，所以将以IP地址唯一标识用户，此时需要将Portal认证配置为三层认证方式。
- Portal认证还支持内置Portal认证方式，将Portal认证服务器部署在接入设备内部进行认证。



HUAWEI

- Portal认证还支持内置Portal认证方式，Portal认证服务器部署在接入设备内部进行认证。

Portal认证接入协议



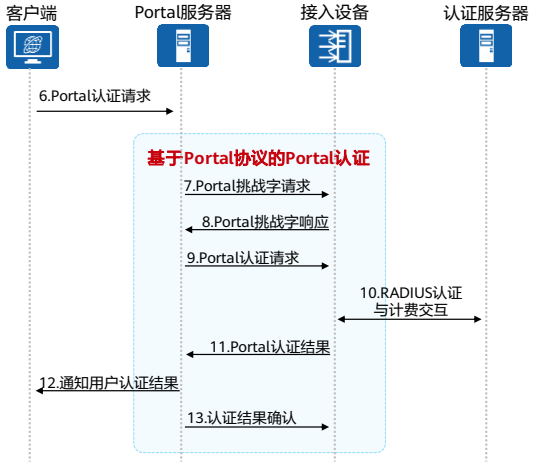
Portal认证协议

- Portal协议：描述了Portal服务器和接入设备之间的协议交互。
- HTTP/HTTPS协议：描述了客户端和接入设备之间的协议交互。

HUAWEI

- 需根据实际网络情况选择不同的Portal认证方式：
  - 采用二层认证方式时，接入设备可以学习到客户端的MAC地址，因此接入设备可以利用IP地址和MAC地址来识别用户。二层认证流程简单，安全性高，但由于限制了用户只能与接入设备处于同一网段，所以组网灵活性不高。
  - 采用三层认证方式时，接入设备不能获取到认证客户端的MAC地址，只能以IP地址作为用户的唯一标识。三层认证组网灵活，容易实现远程控制，但由于只能以IP地址作为用户的唯一标识，相比之下安全性更低。
- Portal认证认证流程如下：
  - 在认证之前客户端与接入设备之间建立起预连接，即客户端用户在认证成功之前在接入设备上已建立用户在线表项，并且只有部分网络访问权限。对于三层认证方式，客户端与接入设备之间没有建立预连接过程，其余报文处理流程跟二层认证完全一致。
  - 客户端发起HTTP连接请求。
  - 接入设备收到HTTP连接请求报文时，如果是访问Portal服务器或免认证网络资源的HTTP报文，则接入设备允许其通过；如果是访问其它地址的HTTP报文，则接入设备将其URL地址重定向到Portal认证页面。
  - 客户端根据获得的URL地址向Portal服务器发起HTTP连接请求。
  - Portal服务器向客户端返回Portal认证页面。
  - 用户在Portal认证页面输入用户名和密码后，客户端向Portal服务器发起Portal认证请求。
  - 按照不同认证协议规定的协议交互流程进行用户名和密码等参数的传递。

Portal认证流程 - 基于Portal协议



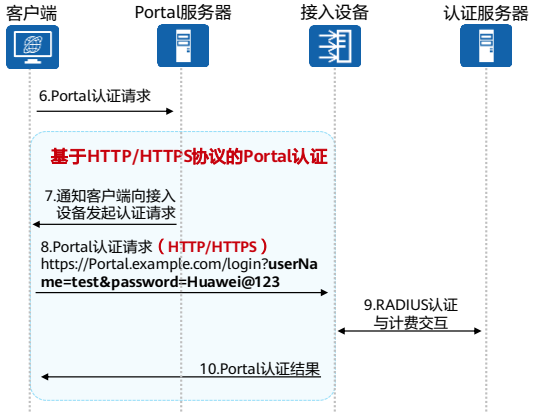
Portal认证协议

- 采用的是客户机/服务器结构，基于UDP。
- 支持CHAP和PAP两种认证方式。相比较PAP，CHAP有更高的安全性。
- 采用TLV格式携带用户名、密码、用户MAC等属性信息。
- 使用接入设备内置Portal服务器（即接入设备同时作为portal认证服务器）进行Portal认证时，仅支持Portal协议。
- 一般情况下，建议采用Portal协议作为认证协议来传递用户名和密码等参数。

HUAWEI

- 以CHAP认证方式为例，基于Portal协议的Portal认证流程如下：
  - Portal服务器收到Portal认证请求后，如果Portal服务器与接入设备之间采用CHAP认证，则Portal服务器向接入设备发起Portal挑战字请求报文；如果Portal服务器与接入设备之间采用PAP认证，则接入设备直接进行第9步。
  - 接入设备向Portal服务器回应Portal挑战字应答报文。
  - Portal服务器将用户输入的用户名和密码封装在Portal认证请求报文中，并发送给接入设备。
  - 接入设备与RADIUS服务器之间进行用户信息的认证，内容包括：
    - 接入设备根据获取到的用户名和密码，向RADIUS服务器发送RADIUS认证请求。
    - RADIUS服务器对用户名和密码进行认证。如果认证成功，则RADIUS服务器向接入设备发送认证接受报文；如果认证失败，则RADIUS服务器返回认证拒绝报文。由于RADIUS协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
    - 接入设备根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则接入设备向RADIUS服务器发送计费开始请求报文。
    - RADIUS服务器返回计费开始响应报文，并开始计费，将用户加入自身在线用户列表。
  - 接入设备向Portal服务器返回Portal认证结果，并将用户加入自身在线用户列表。
  - Portal服务器向客户端发送认证结果报文，通知客户端认证成功，并将用户加入自身在线用户列表。
  - Portal服务器向接入设备发送认证应答确认。

Portal认证流程 - 基于HTTP/HTTPS协议



HTTP/HTTPS认证协议

- 当Portal服务器不支持Portal协议时，可采用HTTP/HTTPS作为认证协议。
- 客户端直接将用户信息通过HTTP请求的方式传递给接入设备，目前支持POST和GET两种请求方法。
  - POST：请求的数据放置在HTTP请求包的包体中，不作为URL的一部分，不易被窃取，安全性较高。设备默认支持此请求方法。
  - GET：请求的数据会附加在URL之后，以“?”分割URL和数据。数据在URL中对所有人都是可见的，易被窃取，安全性较差。

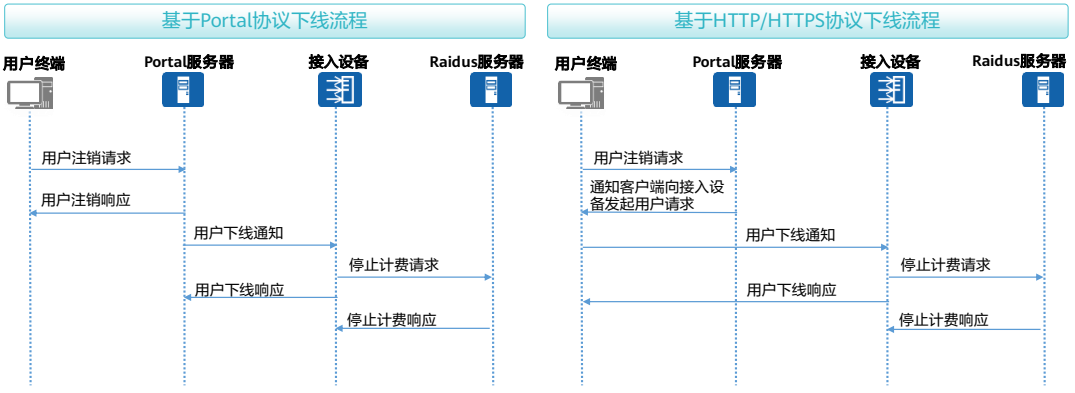
HUAWEI

- 超文本传输安全协议HTTPS (Hypertext Transfer Protocol Secure)，也常称为HTTP over TLS (Hyper Text Transfer Protocol over Transport Layer Security)或HTTP over SSL (Hyper Text Transfer Protocol over Secure Socket Layer)，是以安全为目标的HTTP通道，简单讲是HTTP的安全版。HTTPS通过HTTP进行通信，并使用SSL/TLS来加密数据。
- URL（Uniform Resource Locator，统一资源定位符），是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的URL，它包含的信息包括指出文件的位置以及浏览器应该怎么处理它。
- 当使用基于HTTP/HTTPS协议的Portal认证时，具体流程如下：
  - Portal服务器通知客户端向接入设备发起Portal认证请求。
  - 客户端向接入设备发起Portal认证请求 (HTTP POST/GET)。
  - 设备收到认证请求后，会根据参数名称解析请求报文来获取用户名和密码等参数，然后将获取的用户名和密码向RADIUS服务器进行认证，具体过程与基于Portal的认证流程相同。
  - 接入设备向客户端返回Portal认证结果，并将用户加入自身在线用户列表。
- 采用GET方式发送HTTP请求举例：https://Portal.example.com/login?userName=test&password=Huawei@123，可以看到用户名和密码在URL的后面以明文方式传递，可能会被网络上的其他用户捕获，

带来安全隐患。

Portal认证用户下线 - 客户端主动下线

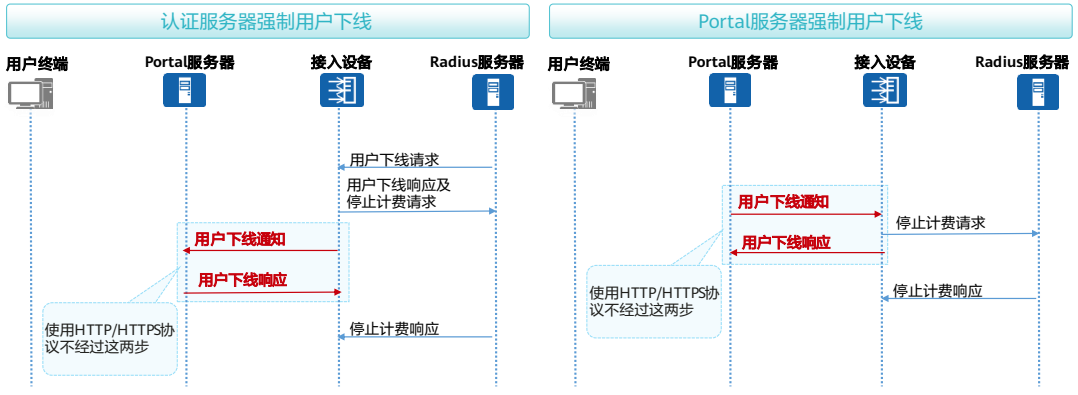
- 由用户发起的主动下线，例如用户点击注销按钮，客户端向Portal服务器发送用户注销请求，基于Portal和HTTP/HTTPS协议下线流程不同。



- 用户下线方式分为客户端主动下线，接入设备控制用户下线和服务器控制用户下线。

Portal认证用户下线 - 服务器强制用户下线

- 在Protal认证组网中，涉及两类服务器，认证服务器和Portal服务器，两类服务器均可强制用户下线，流程如下。

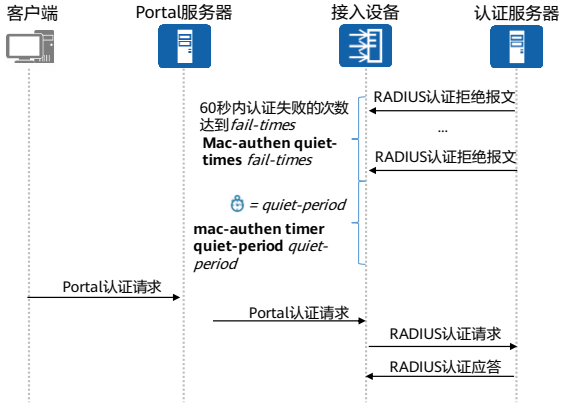


HUAWEI

- Portal认证还支持接入设备控制用户下线，用户通过接入设备侧直接下发命令通知用户下线。

Portal认证定时器 - 静默定时器

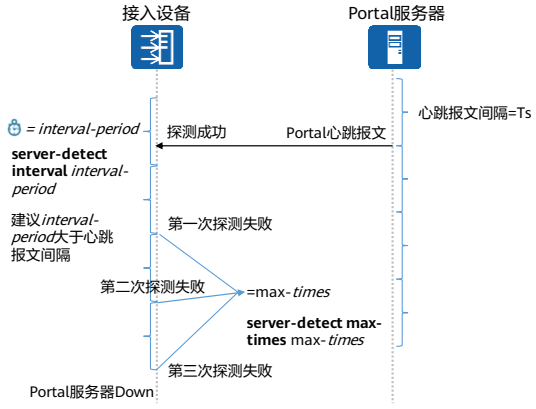
- 在进行Portal认证过程中，用户在60秒内认证失败的次数超过指定的次数时，接入设备会将该用户静默一段时间，在静默期间，接入设备会丢弃该用户的Portal认证请求。

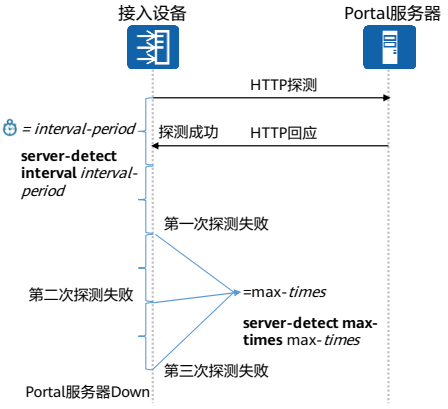


- 适用于使用Portal或HTTP/HTTPS协议的外置Portal服务器，或者使用Portal协议的内置Portal服务器场景。

Portal认证定时器 - 服务器探测定时器

- 服务器探测定时器用于规定Portal认证过程中服务器状态探测的周期。
- 设备对Portal服务器的探测方式有Portal方式和HTTP方式两种。



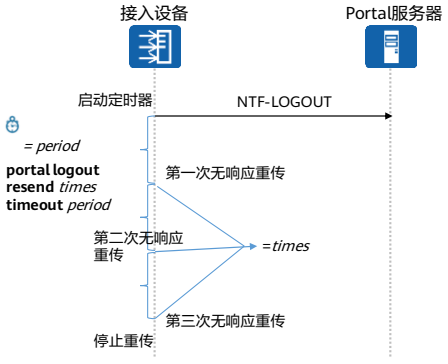


HUAWEI

- 适用于使用Portal协议或HTTP/HTTPS协议的外置Portal服务器场景。

Portal认证定时器 - 用户下线重传定时器

- 为使Portal服务器能够接收到用户下线报文，保证Portal服务器上的用户在线信息正确，接入设备提供用户下线报文重传功能，在用户下线重传周期period内，接入设备没有收到Portal服务器的用户下线应答报文，会重传用户下线报文，最多重传times次。

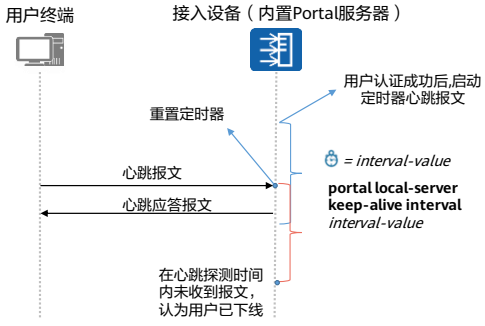


HUAWEI

- 适用于使用Portal协议的外置Portal服务器场景。

Portal认证定时器 - 内置Portal心跳探测定时器

- 用户认证通过后，推送给用户一个连接保持页面，表示该用户处于认证状态。这个连接保持页面中嵌入心跳程序，定期向接入设备发送心跳报文表示该用户在线。
- 如果在指定的心跳探测时间内接入设备没有收到用户发送的心跳报文或认证报文，则可以认为该用户异常离线，并指定该用户下线。



HUAWEI

- 内置Portal服务器的心跳探测模式分为强制探测模式和自动探测模式。
  - 强制探测模式：对于所有用户，如果在指定的时间内接入设备没有收到过用户的心跳报文，则指定用户下线。
  - 自动探测模式：设备会检测用户客户端网页浏览器是否支持心跳程序，如果支持，则采用强制探测模式对该用户进行探测；如果不支持，则不对该用户进行探测。建议采用该模式，避免浏览器不支持心跳程序导致用户下线。

目录

MAC认证概述

- 包含认证客户端、接入设备和认证服务器。
- 终端：尝试接入网络的终端设备。
- 接入设备：是终端访问网络的网络控制点，安全策略的实施者，负责按照客户网络制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。
- 认证服务器：用于确认尝试接入网络的终端身份是否合法，还可以指定身份合法的终端所能拥有的网络访问权限。

简介

- MAC地址认证（简称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。
- 以用户的MAC地址作为身份凭据到认证服务器进行认证。
- 缺省时，交换机收到DHCP/ARP/DHCPv6/ND报文后均能触发对用户进行MAC认证。支持通过配置，使交换机收到任意的数据帧后触发MAC认证。

应用场景

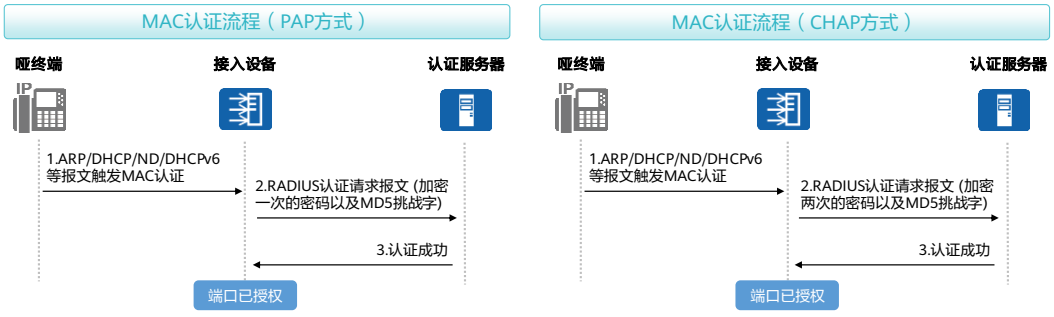
- **不需要**用户安装任何客户端软件。
- 适用于IP电话、打印机等**哑终端**接入的场景。

HUAWEI

- 哑终端：哑终端表示相对于其他终端而言功能较为有限、交互方式比较单一。其具体的含义根据不同的场合（语境）而变化。这里的哑终端泛指无法输入用户名和密码等认证信息的终端。
- 缺省情况下，MAC认证的用户名和密码均为不带分隔符“-”的MAC地址。如“0005e0112233”。

MAC认证流程

- 接入设备与RADIUS服务器之间通过RADIUS报文进行交互，对于MAC认证用户密码的处理，有PAP和CHAP两种方式：
  - PAP：Password Authentication Protocol，即密码认证协议，设备使用随机生成MD5挑战字对MAC认证用户的密码进行一次加密。
  - CHAP：Challenge Handshake Authentication Protocol，即质询握手认证协议，设备使用随机生成的MD5挑战字对MAC认证用户的密码进行两次加密。



HUAWEI

- MAC认证流程：
  - 接入设备首次检测到终端的MAC地址，进行MAC地址学习，触发MAC认证。
  - 接入设备生成相应的MD5挑战字对MAC认证的用户名和密码进行加密，设备支持PAP和CHAP两种处理方式。以PAP为例，准入设备将用户名、加密一次的密码以及MD5挑战字封装在RADIUS请求报文中发送给RADIUS服务器，请求RADIUS服务器对该终端进行MAC认证。CHAP方式的MAC认证与PAP方式的MAC认证相比，不同之处在于设备和RADIUS服务器使用MD5挑战字对MAC认证用户的密码进行了两次加密。
  - RADIUS服务器使用收到的MD5挑战字对本地数据库中对应MAC认证用户的密码进行一次加密，如果与设备发来的密码相同，则向设备发送认证接受报文，表示终端MAC认证成功，允许该终端访问网络。

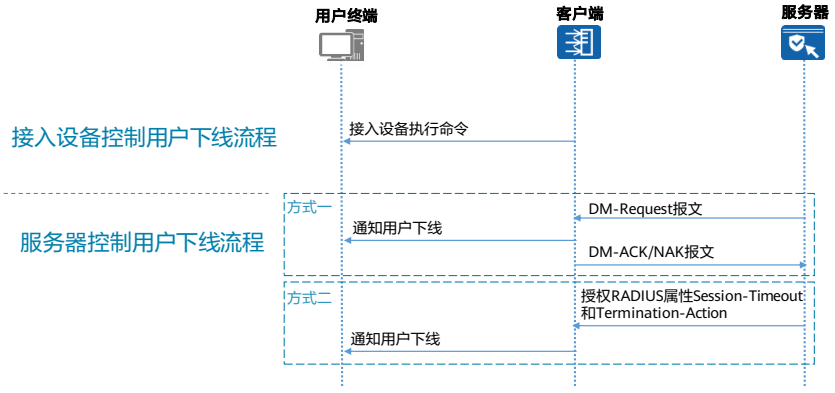
MAC重认证

当前用户状态	配置点	配置方式	触发条件
认证成功状态	接入设备侧	802.1X认证成功用户进行周期性重认证	定期触发
		手动对指定MAC地址进行单次重认证	手动触发
	RADIUS服务器侧	对用户下发RADIUS标准属性	条件触发
认证异常状态（RADIUS服务器Down）	接入设备侧	当RADIUS服务器真正UP时对用户进行重认证	条件触发

- 认证成功状态：若管理员在认证服务器上修改了某一用户的访问权限、授权属性等参数，此时如果用户已经在线，则需要及时对该用户进行重认证以确保用户的合法性。配置对在线用户进行重认证功能后，设备会把保存的在线用户的认证参数（用户上线后，设备上会保存该用户的认证信息）发送到认证服务器进行重认证，若认证服务器上用户的认证信息没有变化，则用户正常在线；若用户的认证信息已更改，则用户将会被下线，此后用户需要重新进行认证。
- 用户在预连接阶段或认证失败阶段：设备会记录用户表项信息，并能够为用户分配受限的网络访问权限。为使用户能够及时认证成功，获取正常的网络访问权限，设备根据用户表项对没有认证成功的用户进行重认证。在用户表项老化时间到达之前，如果用户重认证没有成功，设备将删除对应的表项信息，并收回授予用户的网络访问权限；如果用户重认证成功，设备将用户加入到认证成功的用户表项，并授予认证成功后的网络访问权限。

MAC认证用户下线

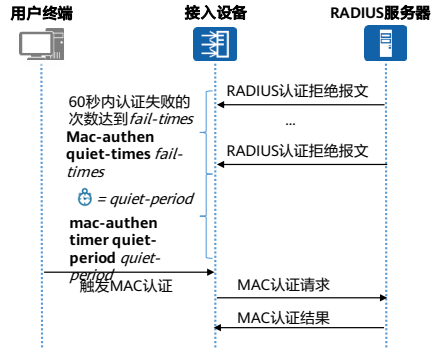
- MAC认证用户下线方式分为接入设备控制用户下线和服务器控制用户下线。



- 服务器控制用户下线有以下方式：
  - RADIUS服务器可通过DM报文 (Disconnect Message)强制用户下线。DM是指用户离线报文，即由RADIUS服务器端主动发起的强迫用户下线的报文。
  - RADIUS服务器通过授权RADIUS标准属性Session-Timeout和Termination-Action。其中，Session-Timeout为用户在线时长定时器，Termination-Action属性值为0表示将用户下线。当用户在线的时长达到定时器指定的数值时，设备会将用户下线。

MAC认证定时器 - 静默定时器

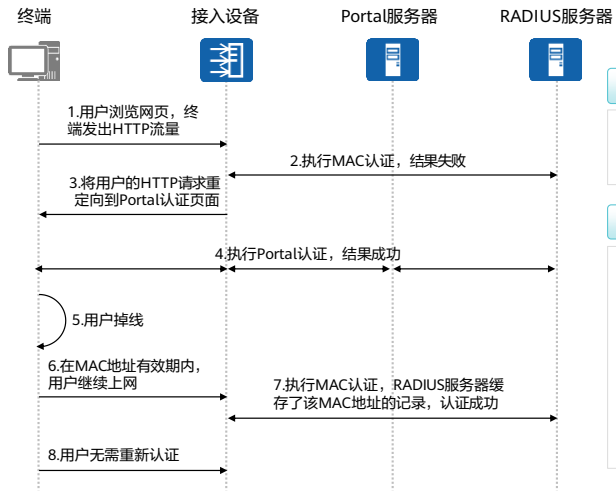
- 在MAC认证过程中，使能静默功能，若某一用户在60秒内认证失败的次数达到指定值，则设备会将该用户静默一段时间，静默期间，设备会丢弃该用户的MAC认证请求。



- 在MAC认证过程中，若用户在短时间内频繁认证失败，一方面会占用过多的系统资源，另一方面存在攻击者通过多次尝试输入用户名和密码的方式暴力破解用户名和密码的风险。
- 使能静默功能后，若某一用户在60秒内认证失败的次数达到指定值，则设备会将该用户静默一段时间，静默期间，设备会丢弃该用户的MAC认证请求。

目录

混合认证 - MAC优先的Portal认证



技术背景

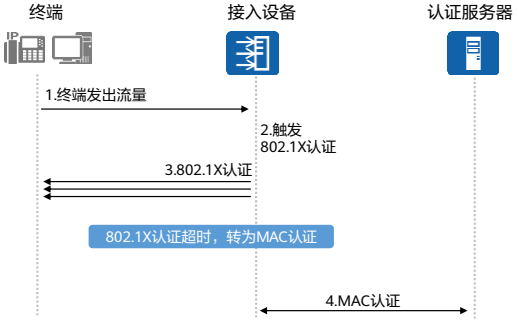
用户进行Portal认证成功后，如果断开网络，重新连接时需要再次输入用户名、密码，体验差。

MAC优先的Portal认证

- 用户进行Portal认证成功后，在一定时间内断开网络重新连接，能够直接通过MAC认证接入，无需输入用户名密码重新进行Portal认证。
- 该功能需要在设备配置MAC+Portal的混合认证，同时在认证服务器上开启MAC优先的Portal认证功能并配置MAC地址有效时间。

混合认证 - MAC旁路认证

- 802.1X认证、MAC认证和Portal认证各有各的特点，可采用混合认证的方式来满足不同的应用场景与认证需求。



- 当接入设备接口下同时存在PC和打印机/传真机等哑终端时，可以通过MAC旁路认证功能，使不具备802.1X认证能力的哑终端能够通过MAC认证方式接入网络。
- MAC旁路认证比单纯的MAC认证多一个802.1X认证环节，故时间要比MAC认证时间长。

目录

用户授权

- 以RADIUS服务器授权为例，常见的授权信息有：
  - VLAN：为了将受限的网络资源与未认证用户隔离，通常将受限的网络资源和未认证的用户划分到不同的VLAN。用户认证成功后，认证服务器将指定VLAN授权给用户。
  - ACL：用户认证成功后，认证服务器将指定ACL授权给用户，则设备会根据该ACL对用户报文进行控制。
  - UCL：用户控制列表UCL组（User Control List）是网络成员的集合。UCL组里面的成员，可以是PC、手机等网络终端设备。借助UCL组，管理员可以将具有相同网络访问策略的一类用户划分为同一个组，然后为其部署一组网络访问策略，满足该类别所有用户的网络访问需求。相对于为每个用户部署网络访问策略，基于UCL组的网络控制方案能够极大的减少管理员的工作量。

状态	802.1x	MAC认证	Portal认证	MAC优先的Portal
动态VLAN	√	√	×	×
动态ACL	√	√	√	√
UCL	√	√	√	√

- 由于RADIUS协议合并了认证和授权的过程，因此当采用RADIUS作为认证服务器时，认证接受报文中也包含了用户的授权信息。
- 授权VLAN：用户认证成功后，认证服务器将指定VLAN授权给用户。此时，设备会将用户所属的VLAN修改为授权的VLAN，授权的VLAN并不改变接口的配置。但是，授权的VLAN优先级高于用户配置的VLAN，即用户认证成功后生效的VLAN是授权的VLAN，用户配置的VLAN在用户下线后生效。
- RADIUS服务器授权ACL有两种方法：
  - 授权静态ACL：RADIUS服务器通过RADIUS标准属性Filter-Id将ACL ID授权给用户。为使授权的ACL生效，需要提前在设备上配置相应的ACL及规则。
  - 授权动态ACL：RADIUS服务器通过华为RADIUS扩展属性HW-Data-Filter将ACL ID及其ACL规则授权给用户。ACL ID及其ACL规则需要在RADIUS服务器上配置，设备上不需要配置。
- RADIUS服务器授权UCL组有两种方式：
  - 授权UCL组名称：RADIUS服务器通过RADIUS标准属性Filter-Id将UCL组名称授权给指定用户。
  - 授权UCL组ID：RADIUS服务器通过华为RADIUS扩展属性HW-UCL-Group将UCL组ID授权给指定用户。
  - 无论是哪一种授权UCL组方式，都必须提前在设备上配置相应的UCL组及UCL组的网络访问策略。
- RADIUS协议具有良好的可扩展性，协议RFC2865中定义的26号属性Vendor-Specific用于设备厂商对RADIUS进行扩展，以实现标准RADIUS没有定义的功能。华为公司的RADIUS扩展属性可参考具体产品文档。

免认证与认证事件授权

免认证（free-rule）

用户认证成功之前，为满足用户基本的网络访问需求，譬如下载802.1X客户端、更新病毒库等，需要用户免认证就能获取部分网络访问权限。

免认证规则模板（free-rule-template）

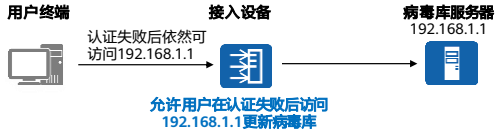
- 方式1：普通的免认证规则，由IP地址、MAC地址、源接口、VLAN等参数确定。
- 方式2：关联ACL。

认证事件授权

用户在认证过程中遇到不同事件时（如认证前、认证失败、认证服务器失效等），需要拥有一定的权限。

授权参数

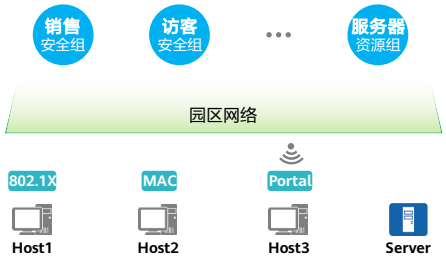
- VLAN：授予用户相应VLAN内的资源访问权限。
- 用户组（UCL）：根据用户组对具有相同特征的用户进行权限下发。
- 业务方案（service-scheme）：可在业务方案内绑定UCL、VLAN、QoS-profile等参数。



HUAWEI

- 使用ACL方式配置免认证规则时，使用的ACL编号范围：6000～6031。
- 根据认证事件授权的方式（一般是非认证成功状态的授权），又被成为逃生，对于不同的认证方式，有不同的逃生方案，有些逃生方案是共有的，有些逃生方案只有特定的认证方式才支持。详细内容请查阅相应产品文档中“NAC逃生”相关内容。

安全组



什么是安全组

1. 安全组是拥有相同网络访问策略的一组用户或资源。安全组仅与用户身份有关，与用户VLAN、IP等网络信息完全解耦。
2. 安全组既可以根据5W1H条件授权给用户，符合5W1H条件的用户授权到指定安全组（动态安全组），也可以通过静态绑定IP地址的方式定义安全组（静态安全组）。

什么是资源组

1. 对于静态的服务器资源，可以通过在安全组中绑定IP地址段的方式进行表达。但是对于IP地址集有重合的服务资源，无法通过安全组进行区分。
2. 资源组可以解决这个问题，资源组之间允许IP地址允许重复，资源组可以作为组间策略的目的地址。

HUAWEI

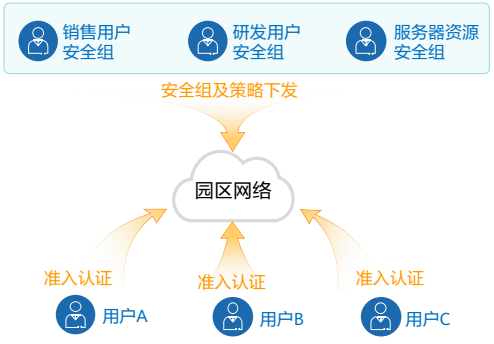
- 5W1H:
  - Who：接入用户的身份，例如公司的领导、普通员工、访客。
  - Where：接入用户的地点，例如园区内接入，或远程接入。
  - What：接入用户使用的终端类型，例如是手机接入，还是PC/便携机接入。
  - When：接入用户的时间，例如是白天接入，还是晚上接入。
  - Whose：设备归属，例如是公司终端的还是自带终端。
  - How：接入用户的方式，例如是有线接入，还是无线接入。

策略控制

- 安全组和资源组定义完成之后，管理员就可以基于组来定义全网的组间策略。
- 策略矩阵用于承载组间策略的配置。组间权限策略主要控制组到组之间的访问权限。

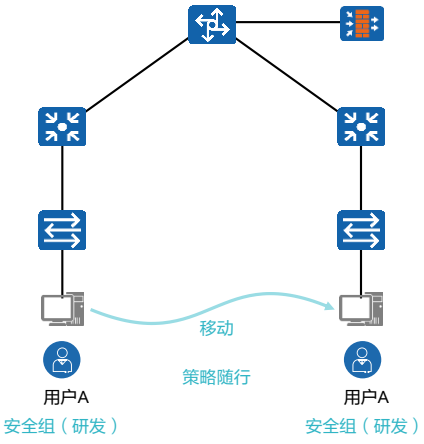
基于安全组的策略管理

- 基于安全组的策略管理，不管用户身处何地，使用哪个IP地址，都可以保证该用户获得相同的网络权限，对其执行对应的用户策略。



1. 定义基于安全组的权限控制策略，将策略下发到网络设备
2. 用户的流量进入网络后，网络设备根据流量对应的源、目的安全组执行策略
3. 用户执行准入认证后，获得授权的安全组

基于安全组的权限控制

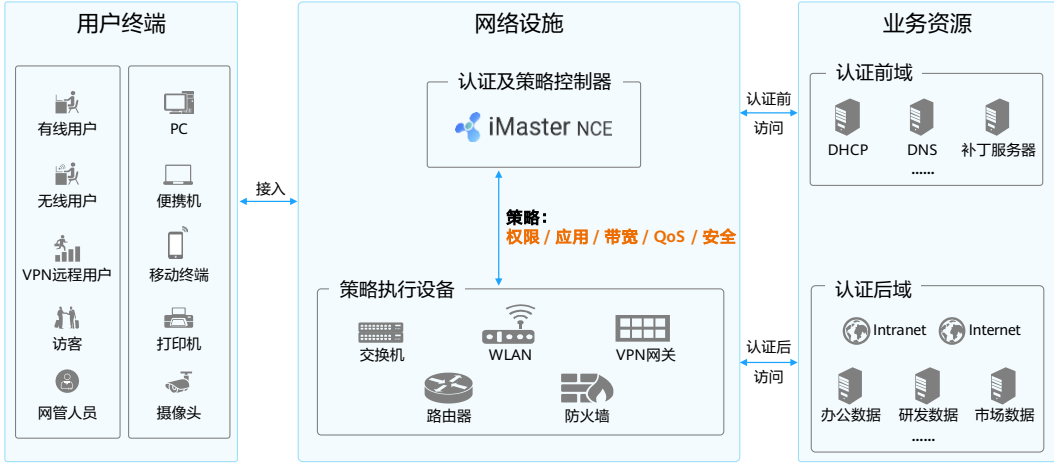


用户权限控制：策略随行

- **用户权限控制都基于安全组执行。**
- **用户互访权限控制：**
  - 同认证点的用户互访权限控制。
  - 跨认证点的用户互访权限控制。
- **资源访问权限控制：**
  - 内外网资源访问权限控制。

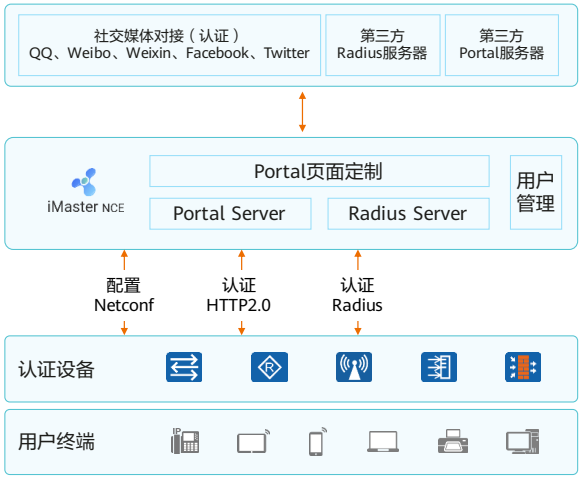
目录

华为NAC解决方案



HUAWEI

华为NAC架构图

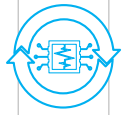


- 认证方式：
  - Portal认证：用户名密码、匿名、短信、QQ、新浪微博、微信、Facebook、Twitter、Passcode认证。
  - MAC认证。
  - 802.1x认证。
- 传输协议：
  - 认证数据采用HTTP2.0、Radius协议传输。
  - 配置数据采用Netconf协议传输。
- 开放认证：
  - 支持对接第三方Portal服务器。
  - 支持对接QQ、Weibo、Weixin、社交媒体。

华为NAC方案策略控制

条件：基于5W1H的策略

用户/用户组/角色	**用户身份 Who**
站点、区域、设备组、设备类型、设备、SSID、IP地址	**接入位置 Where**
按星期/时间	**接入时间 When**
PC/IOS/Android等	**终端类型 What**
公司/自带终端	**设备属性 Whose**
有线/无线 Portal、MAC、802.1x认证方式等	**接入方式 How**



智能策略引擎 iMaster NCE

结果：精细化的权限控制

权限	VLAN/ACL/安全组，VIP用户...
带宽	上行带宽/下行带宽，DSCP
QoS	高/中/低 流量时长管控（仅Portal）
应用	应用组/应用
安全	URL过滤

用户认证实施步骤

自动化网络部署完成

控制器自动化配置下发

设备纳管 → 配置认证规则 → 配置授权结果 → 配置授权规则 → 在线控制策略

多种用户认证源，满足统一用户管理需求

用户身份来源	说明	主要用于
本地自建账号	用户名/密码，MAC账号，访客自注册账号	企业员工，访客人员，运维人员
对接社交媒体	微信，QQ，新浪微博，Facebook，Twitter	访客人员
对接AD/LDAP	Microsoft AD，Novell Edirectory，IBM Tivoli，Sun One，JIT Galaxy，Open LDAP	企业员工，访客人员
对接第三方数据库	SQL Server数据库，Oracle数据库	企业员工，访客人员
对接第三方HTTP服务器	设置认证URL	企业员工，访客人员
对接第三方Radius服务器	RADIUS中继	企业员工
对接Token服务器	RSA SecurID、达芬奇密码动态身份认证系统等	企业员工
证书认证	对接证书服务器，支持X509证书	企业员工

终端识别与策略自动化概述

需求&挑战

某高校

50+类智能终端

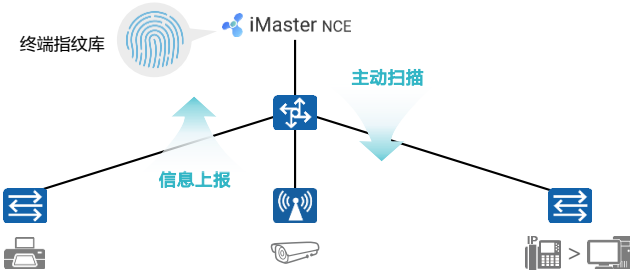
终端由二级学院采集
MAC采集难、易错

某企业

10+/天认证报障

仿冒很难定位

终端识别与策略自动化概述



基于终端类型的

自动认证

识别为打印机

- 自动(MAC)认证，免MAC录入。

基于终端类型的

自动授权

识别为摄像头

- 自动加入“视频监控”组。
- 设置为“VIP”用户。

基于终端类型的

仿冒检测

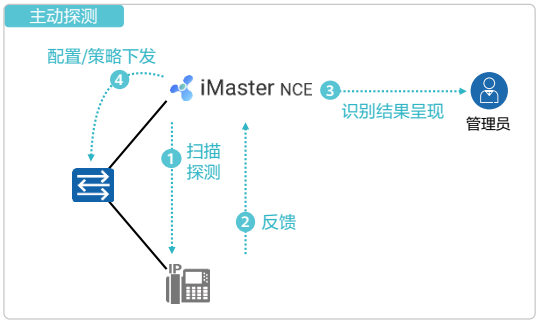
先识别为IP电话，后识别为PC。

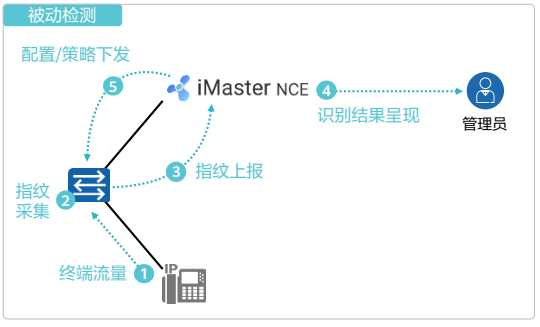
- 上报终端仿冒告警。

HUAWEI

终端识别：支持主动与被动检测方式

- 终端可视化：终端类型统计（厂商、OS）、终端与接入端口关系、接入策略查看（VLAN、QoS、认证方式）、报表导出。
- 终端策略自动化：
  - 支持终端自动准入，根据终端类型进行准入，实现哑终端自动MAC认证。
  - 支持基于终端组授权策略（VLAN、安全组、访问权限、QoS），支持IPv4、IPv6双栈终端。



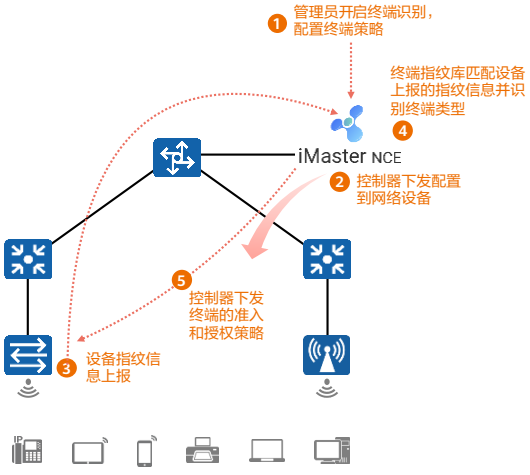


HUAWEI

终端识别：终端识别通过下列几种方法实现

类型	识别方法	识别方法说明	适用的场景
信息上报	MAC OUI	MAC地址前三字节用于表示厂商。	仅识别设备厂商。
	HTTP UserAgent	浏览器UserAgent信息中包含厂商、终端类型、操作系统、浏览器等信息。	手机、平板型号、PC、工作站、音视频智能终端。
	DHCP Option	终端DHCP报文的部分属性可用于终端分类，常用属性有55、60、12。	手机、平板型号、PC、工作站、IP摄像头、IP话机、打印机等。
	LLDP	链路层设备发现协议，包携带设备型号。	IP话机、IP摄像头、网络设备等。
	mDNS	mDNS报文含有终端型号信息和业务信息。	苹果终端、打印机、IP摄像头等。
主动扫描	SNMP Query	通过查询SNMP mib节点中的设备信息相关的节点获取识别信息。	网络设备、打印机等。
	NMAP	通过NMAP软件对终端进行OS、服务扫描，可探测终端型号和OS信息。	PC、工作站、如打印机、话机、IP摄像头等。

终端识别：基于终端类型的策略自动下发流程



1. 管理员在iMaster NCE界面，开启终端识别功能，并选择终端类型，指定终端类型的策略。
2. iMaster NCE将终端识别功能相关配置下发到网络设备。
3. 终端接入网络时，网络设备可以采集终端的指纹信息，上报给iMaster NCE。
4. iMaster NCE自动匹配终端指纹库，识别终端的类型。
5. iMaster NCE根据管理员定义的策略，对终端自动下发对应的准入和授权策略。

Portal页面模板

手机端页面

PC端页面

用户名密码模板　匿名认证模板　短信认证模板　Facebook模板　微信模板　Passcode模板

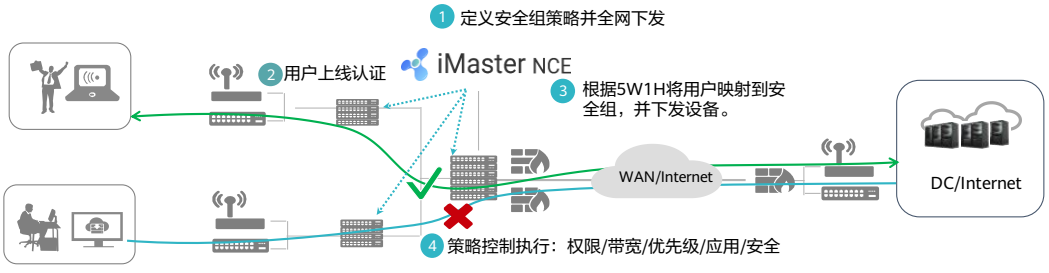
- 多套Portal模板（手机端和PC端），可根据场景自由选择。
- 内置多种语言：简体中文，英语，德语，西班牙语，可扩展支持其他语言。

Portal页面定制

- 完整的页面类型：
  - 认证页面、认证成功页面、用户须知页面、注册页面、注册成功页面、修改密码页面、用户名验证页面、重置密码页面。
- 丰富的控件：
  - 标题、图片、文本、背景、语言链接。
- 灵活的样式编辑：
  - 拖拽式操作：可拖动调整行顺序，拖动调整行高、列宽。
  - 区域样式设置，包括背景图片、背景色、边框大小颜色、边框圆角、内边距、外边距。

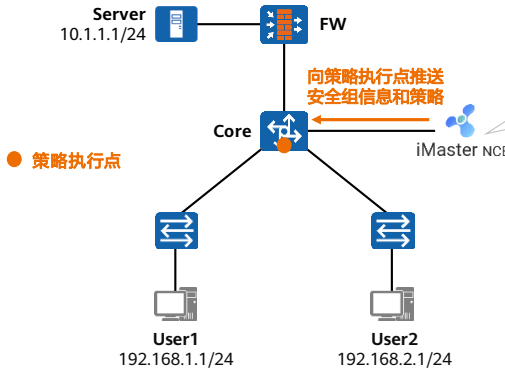
业务随行，实现用户随时随地接入权限一致

用户名	用户组	接入方式	接入地点	准入时间	权限	访问带宽	优先级
Mark	物理系	有线	宿舍	8:00-22:00	科研、互联网、资料共享	2 Mbps	中
Joy	经研院	有线	办公室	全天	科研、互联网、OA、管理、资料	4 Mbps	较高
Terry	外校	有线/无线	任意	8:00-18:00	公开资料共享	500 kbps	低
Jim	校长	有线/无线	行政楼	全天	所有	4 Mbps	最高



HUAWEI

业务随行工作原理详解（1）



创建安全组；将Server的IP地址静态绑定到Server安全组，另外配置授权规则及授权结果，将User1及User2分别授权到安全组Group1及Group2：

安全组信息：

组名	组ID	地址段
Group1	1	动态
Group2	2	动态
Server	3	10.1.1.1/32

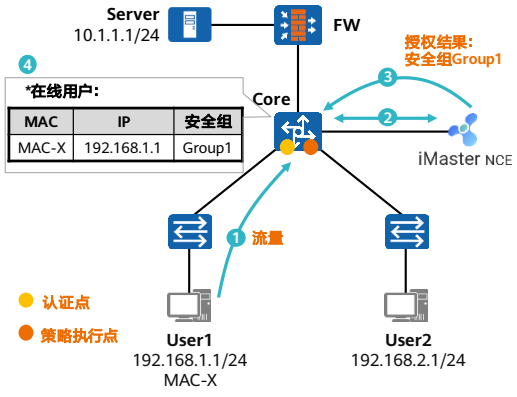
定义权限策略，也即组间通信策略：

源组 \ 目的组	Group1	Group2	Server
Group1	√	×	√
Group2	×	√	√
Server	√	√	√

HUAWEI

- 动态组：需要认证之后才可以接入网络的用户及终端。
- 静态组：使用固定的IP地址的终端。包括服务器，网络设备的接口，以及使用固定的IP地址免认证接入的特殊用户等所有可用IP地址描述的网络成员。

业务随行工作原理详解（2）



1. 用户接入（以User1为例），Core作为认证点，负责与iMaster NCE交互用户认证信息。Core与接入交换机建立策略联动。
2. iMaster NCE判断该用户的登录条件，将该用户与对应的授权策略中绑定的安全组（Group1）进行关联。
3. User1认证通过，iMaster NCE通知认证点该用户所属安全组。
4. iMaster NCE将终端的IP地址与组Group1关联，并记录到IP-安全组表中。同时，认证点设备Core也形成在线用户表项。

在Core的在线用户表中，包含用户的UserID（用户标识）和Username（用户名）等信息。

NAC逃生策略

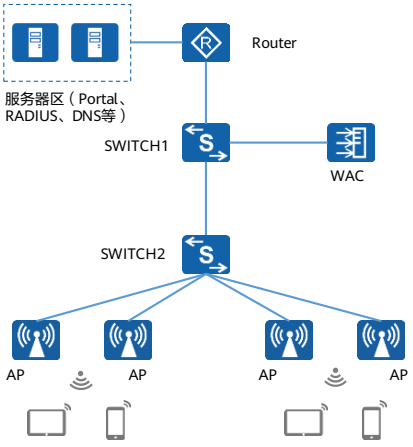
- 当认证服务器Down，或者认证失败用户及处于预连接状态的用户，可以授予用户一定的网络访问权限。这种非认证成功状态的授权，称为逃生。对于不同的认证方式，有不同的逃生方案。

认证方式	触发方式	逃生方式	配置方式
Portal	Portal服务器Down	新用户免认证接入。	执行命令authentication event portal-server-down action authorize
	认证服务器Down		执行命令authentication event authen-server-down action authorize
	认证失败		执行命令authentication event authen-fail action authorize
	预连接		执行命令authentication event pre-authen action authorize
MAC&802.1X	认证服务器Down	对于新接入用户。 802.1X认证： 1. 通过本地配置的账号/密码认证。 2. 采用PSK密钥完成认证。 MAC认证： 1. 通过本地配置的MAC地址进行认证。 2. 免认证接入。	执行命令authentication event authen-server-down action authorize
	认证失败		执行命令authentication event authen-fail action authorize
	预连接		执行命令authentication event pre-authen action authorize

- 仅HTTP报文触发的Portal认证用户支持该功能，HTTPS报文触发的Portal认证用户不支持。
- 不支持为在线Portal用户授权VLAN。
- 用户授权顺序如下，设备会按照所处状态并依照优先级顺序依次检查是否配置了相应的权限，如果已配置，则按照配置的进行授权，如果未配置，则对下一优先级进行检查。认证服务器Down时的授权顺序：认证服务器Down时的网络访问权限 ⇨ 用户在认证失败时的网络访问权限 ⇨ 用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- 用户在认证失败时的授权顺序：用户在认证失败时的网络访问权限 ⇨ 用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- 用户在预连接状态时的授权顺序：用户在预连接阶段的网络访问权限 ⇨ 按照是否开启预连接功能进行授权处理。
- Portal服务器Down时的授权顺序：Portal服务器Down时的网络访问权限 ⇨ 维持Portal服务器Down前的访问权限。

目录

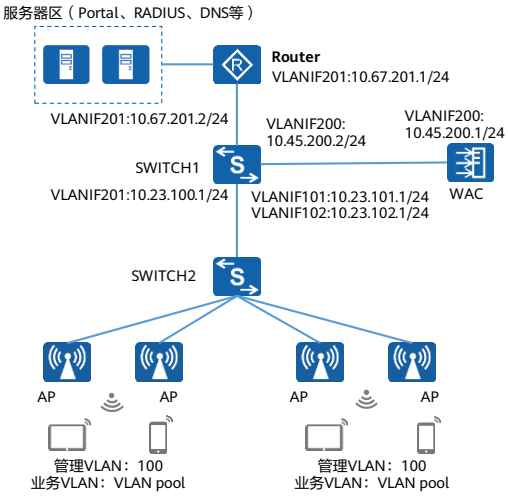
NAC配置举例 - 配置MAC优先的Portal认证



配置思路

- 配置WLAN业务参数，实现STA访问WLAN网络功能。
- 配置WLAN基本业务，实现AC与上下游网络互通和AP上线。
- 配置RADIUS认证参数。
- 配置Portal服务器模板。
- 配置Portal接入模板，管理Portal接入控制参数。
- 配置MAC接入模板，用于MAC优先的Portal认证。
- 配置免认证规则模板，实现AC放行访问DNS服务器的报文。
- 配置ACL，实现为认证通过后的用户能够访问客户问题处理系统。
- 配置认证模板，管理NAC认证的相关配置。

MAC优先的Portal认证 - RADIUS配置（1）



配置RADIUS服务器模板。

[WAC] **radius-server template radius_huawei**

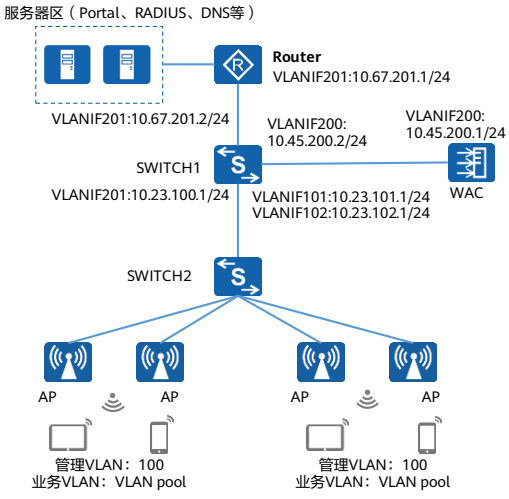
[WAC-radius-radius_huawei] **radius-server authentication** *172.16.1.1 1812*

[WAC-radius-radius_huawei] **radius-server accounting** *172.16.1.1 1813*

[WAC-radius-radius_huawei] **radius-server shared-key cipher** *Huawei@123*

[WAC-radius-radius_huawei] **quit**

MAC优先的Portal认证 - RADIUS配置（2）



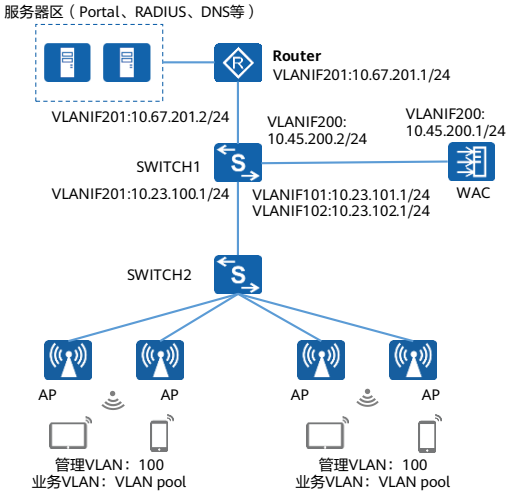
配置RADIUS方式的认证方式。

```
[WAC] aaa
[WAC-aaa] authentication-scheme radius_huawei
[WAC-aaa-authen-radius_huawei] authentication-mode radius
[WAC-aaa-authen-radius_huawei] quit
[WAC-aaa] quit
```

配置RADIUS方式的计费方案。

```
[WAC-aaa] accounting-scheme scheme1
[WAC-aaa-accounting-scheme1] accounting-mode radius
[WAC-aaa-accounting-scheme1] accounting realtime 15
[WAC-aaa-accounting-scheme1] quit
[WAC-aaa] quit
```

MAC优先的Portal认证 - Portal配置



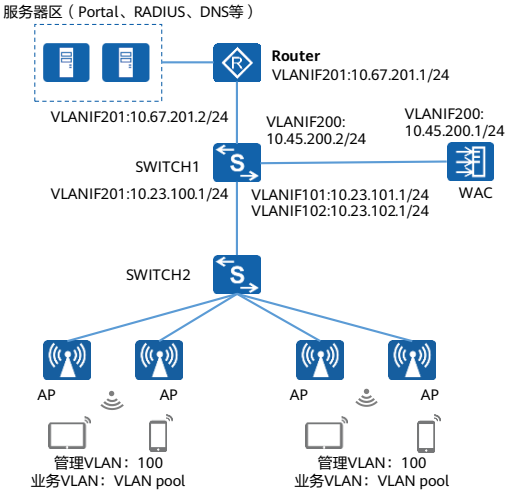
配置Portal服务器模板。

```
[WAC] web-auth-server abc
[WAC-web-auth-server-abc] server-ip 172.16.1.1
[WAC-web-auth-server-abc] shared-key cipher Admin@123
[WAC-web-auth-server-abc] port 50200
[WAC-web-auth-server-abc] url https://172.16.1.1:8445/portal
[WAC-web-auth-server-abc] server-detect
[WAC-web-auth-server-abc] quit
```


HUAWEI

- 配置Portal逃生功能，要求设备侧通过命令server-detect开启心跳探测功能；同时要求服务器侧支持并开启心跳探测功能。

MAC优先的Portal认证 - 接入模板配置（1）



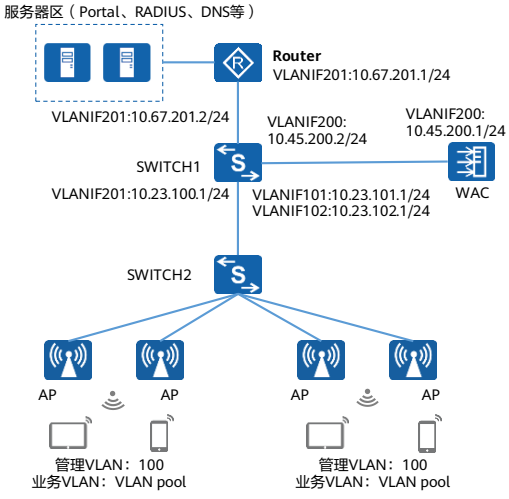
配置Portal接入模板“portal1”。

```
[WAC] portal-access-profile name portal1
[WAC-portal-access-profile-portal1] web-auth-server abc direct
[WAC-portal-access-profile-portal1] quit
```

配置MAC接入模板，用于MAC优先的Portal认证。

```
[WAC] mac-access-profile name mac1
[WAC-mac-access-profile-mac1] quit
```

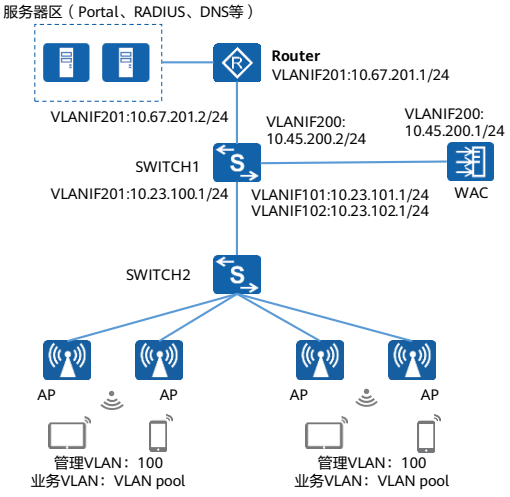
MAC优先的Portal认证 - 接入模板配置（2）



配置认证模板"p1"，并启用MAC优先的Portal认证。

```
[WAC] authentication-profile name p1
[WAC-authentication-profile-p1] portal-access-profile portal1
[WAC-authentication-profile-p1] mac-access-profile mac1
[WAC-authentication-profile-p1] free-rule-template default_free_rule
[WAC-authentication-profile-p1] authentication-scheme radius_huawei
[WAC-authentication-profile-p1] radius-server radius_huawei
[WAC-authentication-profile-p1] quit
```

MAC优先的Portal认证 - VAP引用接入模板



创建名为"guest"VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板。

```
[WAC-wlan-view] vap-profile name guest
[WAC-wlan-vap-prof-guest] forward-mode tunnel
 Warning: This action may cause service interruption. Continue?[Y/N]y
[WAC-wlan-vap-prof-guest] service-vlan vlan-pool sta-pool
[WAC-wlan-vap-prof-guest] security-profile wlan-security
[WAC-wlan-vap-prof-guest] ssid-profile guest
[WAC-wlan-vap-prof-guest] authentication-profile p1
[WAC-wlan-vap-prof-guest] quit
```

配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板的配置。

```
[WAC-wlan-view] ap-group name guest
[WAC-wlan-ap-group-guest] vap-profile guest wlan 1 radio all
[WAC-wlan-ap-group-guest] quit
```


HUAWEI

NAC常用维护命令

功能	配置命令
查看NAC接入用户信息	display access-user
查看漫游用户的漫游表信息	display access-user roam-table
查看802.1X认证的相关信息	display dot1x
查看MAC认证相关信息	display mac-authen
查看Portal认证相关信息	display portal
查看内置Portal服务器上Portal认证用户的连接状态	display portal local-server connect
查看Portal服务器状态信息	display server-detect state
查看Portal认证静默用户信息	display portal quiet-user { all | user-ip { ip-address | ipv6-address } | server-ip ip-address }
查看MAC认证静默用户信息	display mac-authen quiet-user { all | mac-address mac-address }
查看VAP内在线用户数	display access-user-num [interface wlan-dbss wlan-dbss-interface-id]

思考题

1. 授权方法为服务器授权时，用户从服务器和域都可以获取授权信息。如果同时配置了服务器和域的授权信息，且两者的授权信息冲突，则以下说法正确的是？（　）

   A. 服务器下发的授权生效

   B. 域下授权生效

   C. 两者的授权信息同时生效

   D. 报错，两者授权信息均无法生效

- A

本章总结

- 本课程系统介绍了NAC相关原理详解以及华为NAC解决方案。
- 通过本课程的学习，搭配基于实际环境的练习，学员将能独立完成华为NAC典型方案配置。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN与IoT融合

HUAWEI

前言

- 在Wi-Fi网络迅猛增长的同时，连接物与物的IoT也在快速地发展和应用。
- 物联网中使用的无线技术有很多，按照覆盖范围可以分为短距无线通信技术和广域无线通信技术。短距无线通信技术包括Wi-Fi、RFID、蓝牙、ZigBee等，广域无线通信技术包括SigFox、远程物联网 (Long Range, LoRa)和窄带物联网 (Narrow Band-Internet of Things, NB-IoT)等。
- 短距无线接入技术和Wi-Fi的覆盖范围是接近的，如果进行多网合一和融合部署，会大大降低整体的部署和运维成本。

目标

- 学完本课程后，您将能够：
  - 描述常见短距无线通信技术及其特点
  - 描述华为WLAN物联网AP及其主要功能
  - 描述华为智简园区物联网方案

目录

趋势：物联网是新一轮的信息产业革命

PC互联网 1994

最初的互联网主要针对固定终端，计算机等终端设备能够接入网络实现资源共享。

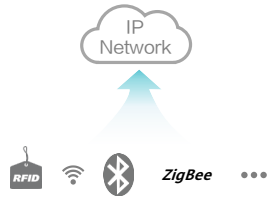
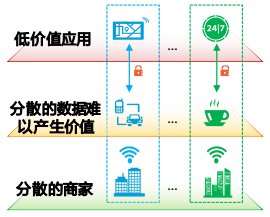
移动互联网 2009

进入21世纪，随着智能终端的发展，以智能应用为代表的移动互联网正迅猛发展，移动终端纷纷接入网络。

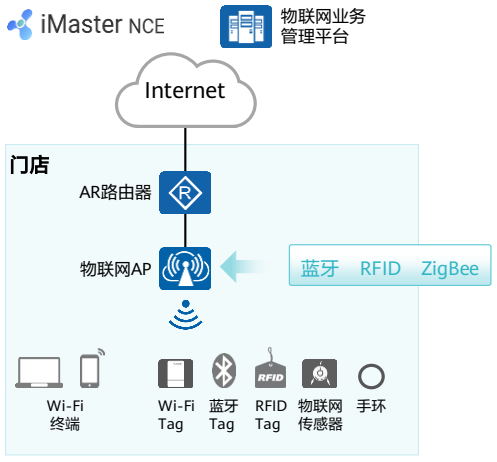
物联网 2025

物联网被称为是世界信息产业革命的第三次浪潮。预计到2025年将有1000亿个“物”会被连接到网络中，将极大影响人们的生活。

挑战：多技术、多终端重复组网

将多样化的无线传感器接入网络	降低物联网部署成本	促进物联网投资商业变现
		
物联网传感技术多种多样，均有各自适用的场景，如何将这些多样化的传感网平滑接入现有网络是推广物联网应用面临的一大挑战。	企业为了实现资产管理功能需要部署大量的资产标签和数据传输网络，部署规划和现场工勘、安装等耗费巨额人工成本；资产管理网络与办公网络分开部署形成的大量节点为后期的管理和运维带来巨大成本。	超市分店多，广告点击率低于，网络投资回报低，如何依托电子价签、室内定位等物联网应用为客户提供更多增值服务、实现商业变现是商家面临的挑战。

解决方案：多网合一，融合部署，大数据分析



多网合一

- 借助物联网融合AP实现办公网与物联网实现多网合一。
- 管理、运维实现一套网络，降低部署、管理成本。

融合部署

- 统一网规、统一工勘
- 一次部署多网共用
- 方便扩展

大数据分析

- 物联网用户数据分析，实现精准营销，助力商业价值实现。

目录

短距无线IoT技术概述

- 在Wi-Fi网络迅猛增长的同时，连接物与物的IoT也在快速地发展和应用。
- 物联网中使用的无线技术有很多，按照覆盖范围可以分为短距无线通信技术和广域无线通信技术。
- 短距无线通信技术主要包括：
  - Wi-Fi：被广泛应用的无线局域网通信技术。
  - RFID：可以通过射频信号自动识别目标对象，并对其信息进行存储和管理。主要用于门禁、考勤刷卡、智能货架、图书管理等场景。
  - 蓝牙：短距离通信技术，随着智能穿戴、智能家居、车联网等物联网产业的兴起，越来越受到开发者的重视。
  - ZigBee：一种短距离、自组织、低功耗、低速率的物联网无线接入技术。主要用于工业、农业和商业领域的监视、传感器、自动化和控制等产品
- 广域无线通信技术包括SigFox、远程物联网（Long Range，LoRa）和窄带物联网（Narrow Band-Internet of Things，NB-IoT）等。

短距无线通信技术：RFID（1）

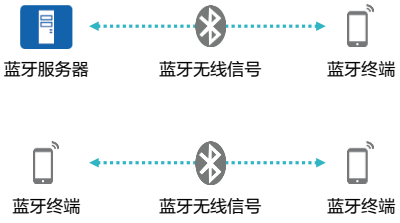
- RFID (Radio Frequency Identification)即射频识别技术，是一种非接触的自动识别技术，其基本原理是利用射频信号和空间耦合（电感或电磁耦合）或雷达反射的传输特性，实现对被识别物体的自动识别。通过射频信号识别目标对象，并对其信息进行标志、登记、存储和识别。
- RFID系统通常由电子标签、读写器和信息处理平台三部分组成：
  - 电子标签 (RFID Tag)：由芯片和标签天线或线圈组成，通过电感耦合或电磁反射原理与读写器进行通信；
  - 读写器：读取（在读写卡中还可以写入）标签信息的设备，也称为读卡器；
    - 天线：电子标签和读写器都有天线。电子标签的天线一般内置标签内。读写器的天线可以内置在读写器中，也可以通过射频线与读写器天线接口相连。
  - 信息处理平台：统一对信息进行存储和管理。

短距无线通信技术：RFID（2）

RFID分类	频率	通信距离	应用场景
低频射频卡	125 kHz~134.2 kHz	<10 cm	短距离、低成本的应用：门禁控制、校园卡、动物监管、货物跟踪。
中频射频卡	13.56 MHz	<1 m	门禁控制和需传送大量数据的应用系统，公交、手机支付。
高频射频卡	433 MHz、 865 MHz～868 MHz、 902 MHz～928 MHz、2.45 GHz、5.8 GHz	3 m~100 m	较长的读写距离和高读写速度的场合：供应链管理、后勤管理等。

短距无线通信：Bluetooth（1）

- 蓝牙（Bluetooth)是当今使用最广泛的短距无线物联网技术之一。1994年由爱立信公司初创，1998年爱立信联合诺基亚、英特尔、IBM、东芝成立了蓝牙技术联盟（Bluetooth Special Interest Group, SIG)。SIG发布了低功耗蓝牙（Bluetooth Low Energy, BLE)技术，旨在用于智能家庭、运动健身等市场，2016年又推出新一代蓝牙标准BLE 5.0，与之前相比，传输速度更快、覆盖距离更远、功耗更低。



RFID Bluetooth ZigBee Wi-Fi

短距无线通信：Bluetooth（2）

工作频段	2.4 GHz ISM频段，2.402 GHz-2.480 GHz
双工方式	全双工，TDD时分双工，可同时传输语言和数据
组网方式	支持点对点通信、点对多点通信
通信特点	采用调频通信，具有很好的抗干扰能力
功率	美国FCC要求<0 dbm(1 mw)，其他国家可扩展为100 mw
传输距离	绝大部分小于10 m，极限100 m
传输速率	1 Mb/s
典型应用	外围设备互联（蓝牙耳机、鼠标等）、 智能穿戴设备(手环、手表等)、物联网（家用电子设备）

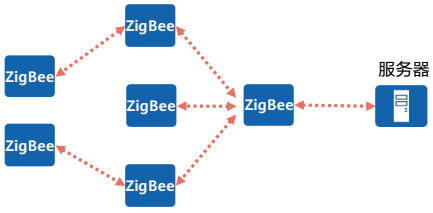
HUAWEI

- 蓝牙是一种短距离通信技术。随着智能穿戴、智能家居、车联网等物联网产业的兴起，蓝牙越来越受到开发者的重视，从而衍生出大量的蓝牙产品，从传统的具备蓝牙功能的手机、蓝牙耳机、蓝牙音箱、蓝牙鼠标、蓝牙键盘等，再到智能手环、智能手表、运动手环、车载设备、智能家居产品等。

RFID Bluetooth ZigBee Wi-Fi

短距无线通信：ZigBee

- ZigBee（又称紫蜂）是一种基于IEEE802.15.4的通信协议的短距离、低功耗的无线通信技术。
  - ZigBee标准由ZigBee联盟发布与维护，广泛应用于工业和智慧家庭领域。
  - ZigBee具有近距离、自组织、低功耗、低数据速率等特点。
  - ZigBee支持星型组网、MESH组网和混合组网（星型组网+MESH组网）三种不同的组网方式。
  - ZigBee的出现使得在一个开放式全球标准的基础上，让稳定的、低成本的、低功耗的、无线联网的监控和控制产品成为可能。

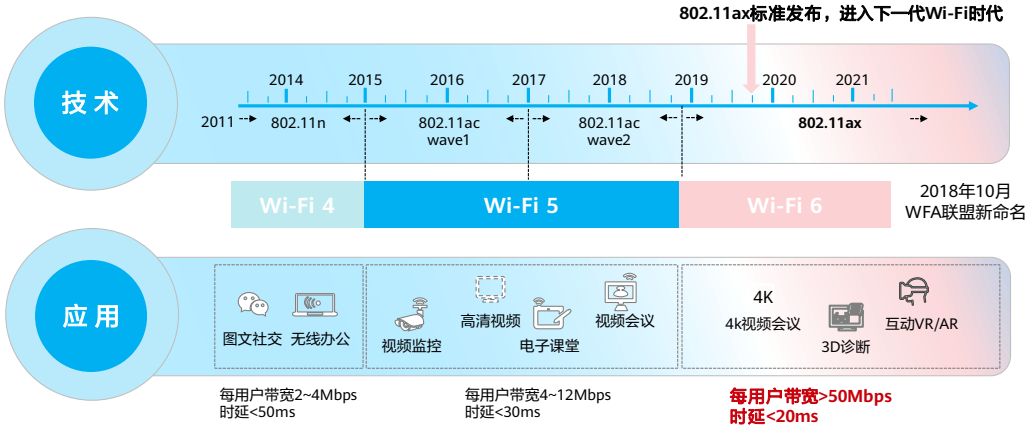


HUAWEI

- ZigBee是一项新型的无线通信技术，适用于传输范围短数据传输速率低的一系列电子元器件设备之间。ZigBee无线通信技术可于数以千计的微小传感器相互间，依托专门的无线电标准达成相互协调通信，因而该项技术常被称为Home RF Lite无线技术、FireFly无线技术。ZigBee无线通信技术还可应用于小范围的基于无线通信的控制及自动化等领域，可省去计算机设备、一系列数字设备相互间的有线电缆，更能够实现多种不同数字设备相互间的无线组网，使它们实现相互通信，或者接入因特网。
- ZigBee无线通信技术是基于蜜蜂相互间联系的方式而研发生成的一项应用于互联网通信的网络技术。相较于传统网络通信技术，ZigBee无线通信技术表现出更为高效、便捷的特征。

短距通信技术：Wi-Fi

- Wi-Fi 是一种基于IEEE802.11标准的无线联网技术，是当今最热门的无线局域网技术。



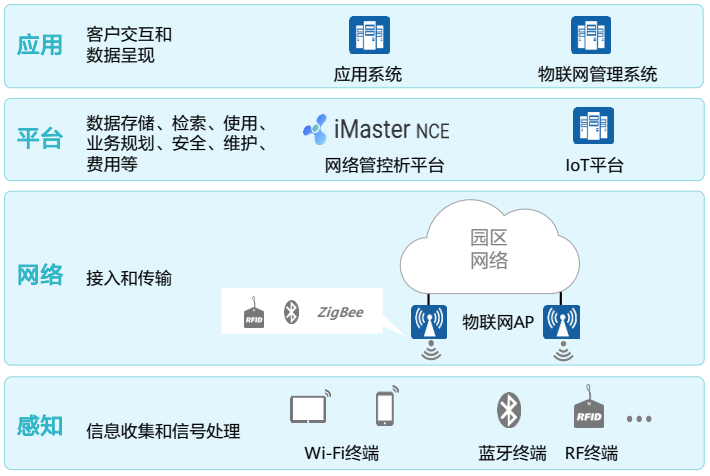
HUAWEI

短距无线通信技术简要对比

	RFID	Bluetooth	ZigBee	Wi-Fi	技术对比
技术标准	ISO/IEC18000标准, ISO11785（低频），ISO/IEC14443标准（13.56 MHz），ISO/IEC15693标准（13.56 MHz）、EPC标准DSRC标准	IEEE802.15.1	IEEE802.15.4	IEEE802.11	各有各的技术规范
工作频段	低频：125 kHz~134.2 kHz、 中频：13.56 MHz 高频：433 MHz 865 MHz～868 MHz 902 MHz～928 MHz 2.45 GHz/5.8 GHz	2.402 GHz-2.480 GHz	868 MHz / 915 MHz, 2.4 GHz	2.4~2.4835 GHz 5.150~5.850 GHz	Wi-Fi与RFID或ZigBee共存时，可以利用频段隔离来避免干扰；Wi-Fi与蓝牙共存时，蓝牙通过跳频规避干扰，即Wi-Fi可以与以上3种物联网无线接入技术共存。
典型距离	低频：<10 cm 中频：<1 m 高频：3 m~100 m	1-100 m	2.4GHz 频段: 10-100 m	50-100 m	覆盖距离接近，可实现共站址部署。
发射功率	中低频时，阅读器功率极小，高频时阅读器的发射功率为2 W,其对应的有源RFID标签小于100 mw。	1-100 mW	1-100 mW	终端：36 mW，AP：100~500 mW	RFID 、蓝牙或ZigBee所需功率极小，可由AP统一供电。
典型应用	门禁系统、智能卡、货物追踪等。	鼠标、无线耳机、手机、电脑等邻近节点数据交换。	家庭自动化、楼宇自动化、远程控制。	无线局域网，家庭，室内场所高速上网。	

目录

华为智简园区网络架构：统一承载无线及物联网业务



统一入口，便于扩展降低维护成本

- 日常办公使用Wi-Fi接入服务。
- AP内置蓝牙模块，支持RFID，ZigBee拓展IoT业务。
- AP提供USB口和标准Mini-PCI-E接口，方便物联网业务拓展。

统一管理，降低建网成本

- IoT与Wi-Fi共回传。
- 只需管理和维护一个物理站点。

HUAWEI

- 为了解决融合问题，华为推出物联网AP，在AP上进行IoT扩展，提供蓝牙、RFID 、Zigbee等IoT连接方式，实现Wi-Fi、蓝牙、RFID等不同无线技术方案的统一入口。
- 通过在物联网AP上集成蓝牙、RFID、Zigbee等插卡，实现其他各种物联网连接方式在AP上的共站址、共回传、统一入口和统一管理。这种无线技术共站址、共回传和共电源的方式可以明显降低成本、减少施工量和减少对周边环境的破坏，并且可以做到灵活扩展。

华为智简园区网络：物联网AP

HUAWEI

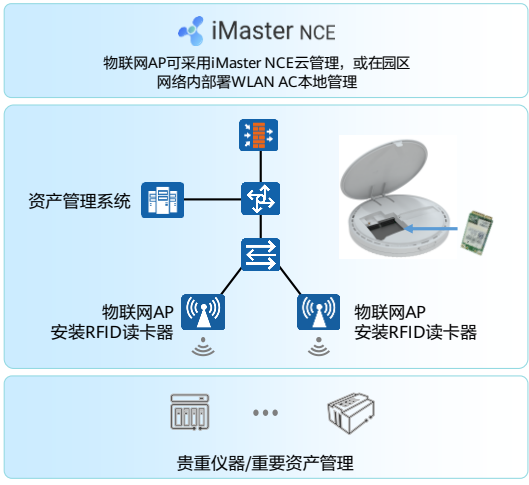
华为智简园区资产管理方案

- 资产管理指的是企业、政府、高校等机构的固定资产如贵重仪器、电子设备等的管理，包括资产的全生命周期管理活动。

当前资产管理面临的挑战：人工资产盘点效率低下；资产使用状态不可知；资产丢失无法回溯和及时追踪。

资产管理 智慧医疗 电子价签

华为智简园区资产管理方案：技术实现



资产在线盘点：

- 通过RFID读取资产的RFID标签状态，进而获取资产状态。
- RFID标签信息周期性上报，资产盘点周期短。

资产状态、使用率可视化：

- 可实现资产状态和位置实时获取；RFID上报资产使用状态，能够在系统上实时统计资产使用率；通过使用率分析后，能够在系统上发布闲置状态，提升资产利用率。
- 资产使用情况统计数据提供资产申购和审计的量化依据。

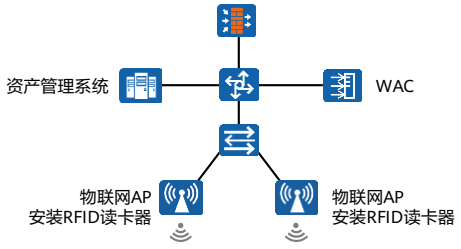
电子围栏防丢失：

- RFID网关的信号覆盖一定的范围，具有区域属性。设定固定ID的RFID信号覆盖区域为电子围栏区，通过识别RFID标签的所属区域，当RFID标签（资产）移除该区域时，系统可及时产生告警和提示，避免资产丢失。

HUAWEI

- RFID网关：AP通过PCI-e接口对接第三方RFID插卡，融合RFID网关功能，侦听环境中RFID标签的广播数据。RFID网关具备独立ID。
- RFID标签：资产安装RFID标签，RFID标签周期性广播RFID报文，其中携带RFID标签ID、标签在位状态、设备工作状态（电流标签）等信息。

华为智简园区资产管理方案：典型配置（1）



场景介绍

在企业中部署RFID资产管理方案，进行固定资产的管理。

配置思路

以WAC+AP组网为例，按照以下步骤进行相关配置；

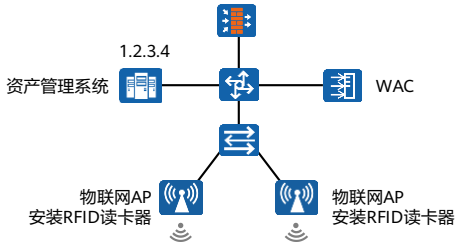
1. 配置IoT模板，指定资产资产管理系统的IP地址和端口号。
2. 配置AP组引用IoT模板，指定AP和资产管理系统通信的端口号和通信协议。

网规建议

RFID信号覆盖距离为25米，因此AP布放需要考虑RFID信号覆盖。

RFID标签尽量粘贴在资产表面/上方，避免信号被屏蔽。

华为智简园区资产管理方案：典型配置（2）



1.配置名为“IoT”的IoT模板，指定资产管理系统的IP地址和端口号。

```
[WAC-wlan-view] iot-profile name iot
[WAC-wlan-iot-prof-IOT] management-server  server-ip 1.2.3.4 server-port 8081
```

2.在AP组下引用iot模板，指定AP和资产管理系统通信的端口号和通信协议。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1] card 1
[WAC-wlan-group-card-ap-group1/1] iot-profile iot config-agent tcp port 50201
```

医疗物联网方案场景概述（1）

基础业务阶段（有线时代）	临床业务阶段（有线无线融合时代）	物联网业务阶段（物联网时代）
关注业务**功能**： • HIS • LIS • PACS • RIS	关注业务**流程**： • 移动护理系统 • 手术麻醉系统 • ICU监护系统 • 电子病历系统	关注业务**对象**： • 人（医护人员、患者、家属） • 物（设备、药品、耗材） • 流程（业务、管理）

- HIS：医院信息系统（Hospital Information System）
- LIS：实验室信息管理系统（Laboratory Information Management System）
- PACS：影像归档和通信系统（Picture Archiving and Communication Systems）
- RIS：放射科信息管理系统（Radiology Information System）

资产管理 智慧医疗 电子价签

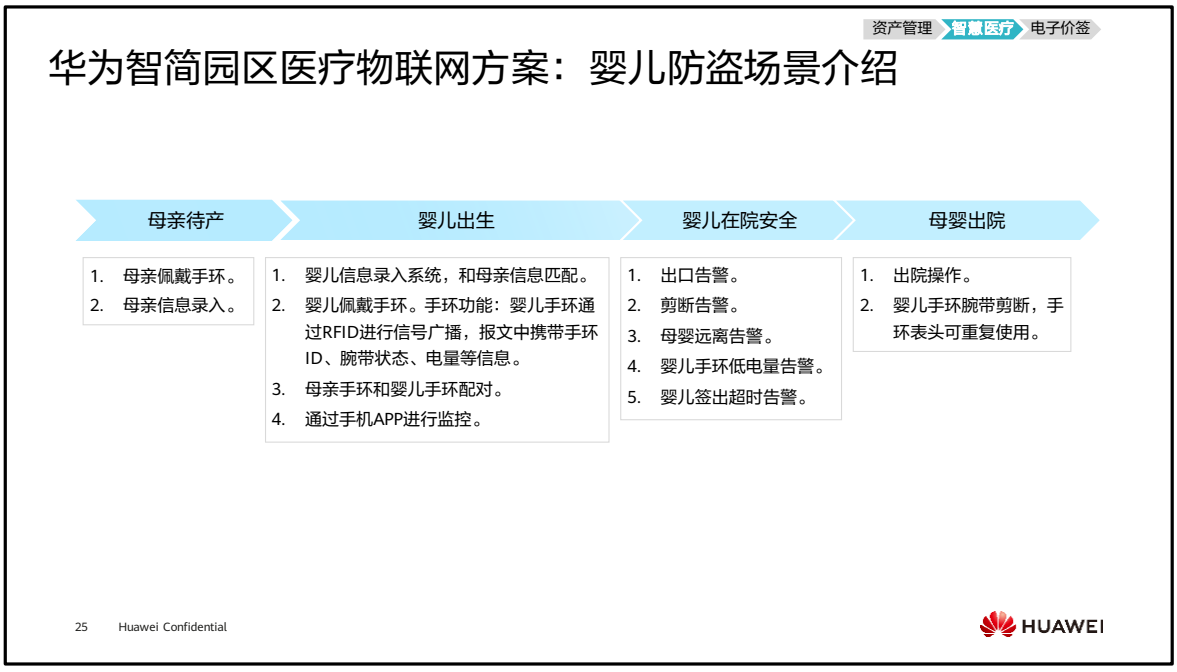
医疗物联网方案场景概述（2）

物联医院	移动临床	智慧就医	医疗网络融合
• 基于传感网络的物联网应用架构，实现人、物、流程的精细化管理。 • 输液监护、婴儿防盗、人资管理、生命体征监测等物联网应用。	• 通过 SmartRadio 无损漫游技术优化移动医疗体验，实现查房、医嘱执行的移动化、无纸化，提升医护人员工作效率。	• 提供院内导航和导诊服务等，以提升患者就诊效率。 • 实现智慧病房系统等，以改善患者就医体验。	• 无线、物联网、导航定位网络融合，降低建设成本和运维难度。 • 网络需要支持多厂家物联设备对接，满足长期演进需求。

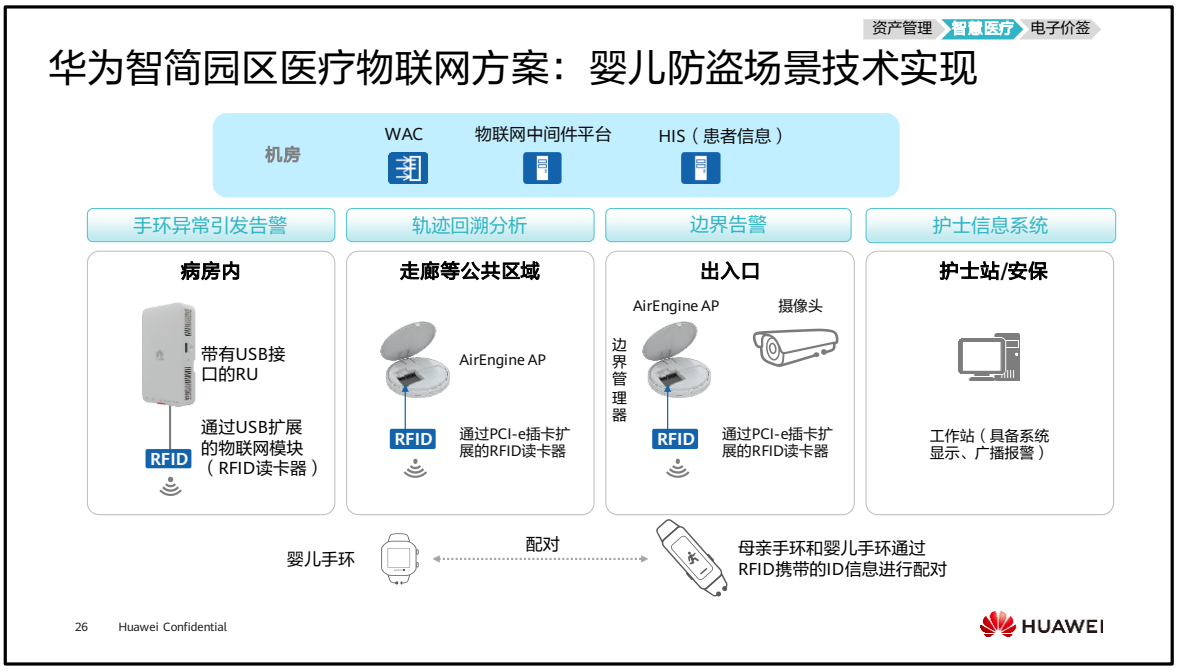



HUAWEI

- 在医院医疗场景中，医院希望能够利用技术手段实现输液管理和婴儿防盗，防止出现重大医疗事故或者安全事故，如婴儿丢失，提升医院管理能力，提升病人满意度。
- 另外医院需要对重要医疗资产进行资产管理，使用人工手动盘点排查管理资产的方式耗时长，成本高，并且很难定位流失的资产去向。医院同样希望通过技术手段实现资产定位和管理，降低管理成本和复杂度。
- 针对这种场景，华为公司提供智慧医疗-医疗物联网方案，通过将人、物加入物联网，实现婴儿防盗、输液管理和医疗资产管理。
- 使用智慧医疗-医疗物联网的方案有如下优点：
    - 利用技术手段防止出现重大医疗事故和重大安全事故，提升医院管理能力和病人满意度。
    - 利用技术手段定位和管理资产，能做到对资产位置的监控，避免资产流失，节省人力成本。
    - 医疗物联网网络复用WLAN网络，实现双网合一，降低医疗物联网网络的部署和维护成本，方便管理员统一管理网络。



- 出口告警：婴儿被抱出，到达出口，出口存在出口管理设备，婴儿手环RFID信号触发告警。系统接收到告警报文并解析出产生告警的出口位置，进行声光报警和门禁/摄像头联动等安全措施。
- 剪断报警（婴儿手环报文上报剪断信息）、信号丢失（没有信息上报系统做告警处理）。
- 母婴远离告警：母亲手环根据信号强度情况分析当前婴儿距离，当识别到距离超过阈值时候，产生告警。
- 婴儿手环低电量告警：婴儿手环广播RFID报文中携带的电量字段，系统接收到低电量时候产生低电量告警。
- 婴儿签出超时告警：由系统进行处理，设置签出时间，在签出时间到期后，婴儿没有返回病房，产生异常告警。

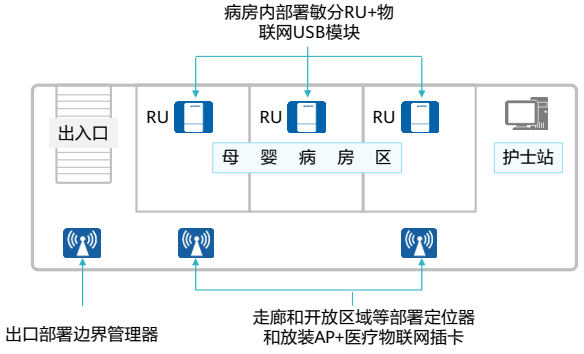


- 手环异常引发告警
  - 手环通过RFID上报心跳报文，服务器检测不到心跳，产生丢失告警。
  - USB扩展物联网模块通过射频定位，可确认当前手环位置，当婴儿被抱走超时，产生签出超时告警。
  - 手环被剪断，通过RFID上报变化，服务器识别剪断告警。
  - 母亲手环开启距离监控，通过接收到婴儿手环的RFID信号强度进行距离判断，距离超限时产生远离告警。
- 轨迹回溯分析
  - 通过在走廊等公共区域部署物联网插卡，实时获取婴儿手环的位置，可以在婴儿被抱出和出现异常的情况下进行轨迹回溯和分析
- 边界告警
  - 婴儿被抱到出口处，边界管理器和手环RFID交互，识别到手环位置异常，系统产生出口告警。
  - 系统在产生出口告警时候可以进行门禁系统联动、视频监控系统联动。
- 护士信息系统
  - 护士对入园/出院等信息录入。
  - 各类告警信息在护士站或者安保中心进行声音/系统告警/视频联动。

- 护士站确认和查看告警。

华为智简园区医疗物联网方案：婴儿防盗场景部署

- 病房内部署敏分AP (RU) + 物联网USB模块。走廊和开放区域部署AP + 物联网PCI-e插卡。各个出口部署边界管理器和声光报警器。护士站办公电脑安装婴儿防盗管理系统，具备声音报警功能。



华为智简园区智慧零售电子价签方案：方案简介

- 零售企业的核心诉求：降低价签的人工配置和运维成本，降低配置错误率。
- 当前传统电子价签方案的问题：投入大，运维难，维护成本高。

传统纸质价签

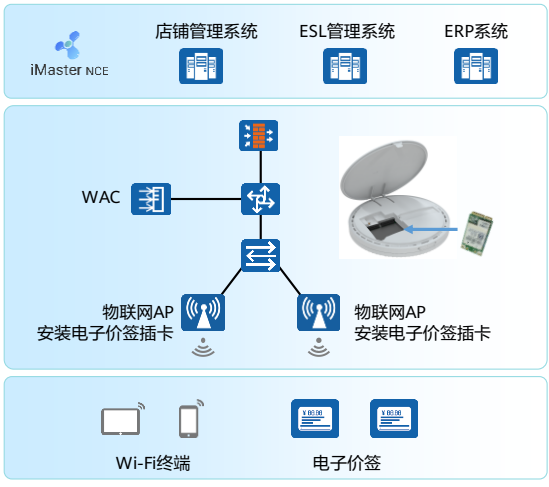
- 商品价格等信息变更慢，需人工维护，维护成本高。
- 错误率高，准确性完全依赖人工。

传统电子价签

- 虽然可省去高昂的纸质价签维护成本，但需建设专网，基建一次性投入大，专用网络维护费用高。

资产管理 智慧医疗 电子价签

华为智简园区智慧零售电子价签方案：电子价签技术实现



方案实现

1. 店铺管理系统调用ERP系统产品信息， 且与ESL管理系统对接对产品进行价格等信息的管理；
2. 华为物联网AP提供内置PCI插槽对接ESL插卡；
3. ESL管理系统获取到商品对应标价信息，通过AP内置的ESL插卡发送无线报文信息给ESL；
4. ESL接收到信息后以点阵的方式显示商品价格；
5. ESL使用射频为2.4GHz RFID。

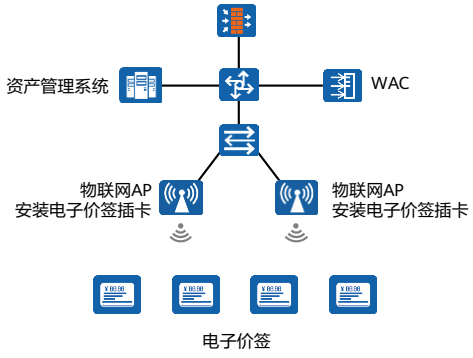
方案价值

两网合一，融合部署，统一规划，节省整体投资

HUAWEI

- ESL：extended signaling link
- 业务场景介绍：
  - 客户在企业总部、分部和门店统一部署电子价签、基站和ESL服务器。企业总部和分部的ESL服务器分别对接客户ERP系统。客户对自己ERP系统里的商品做价格调整，结果会同步到ESL服务器。ESL服务器根据ERP的调价结果和预置的调价计划（一般在商场打烊后）执行价格调整。同时，ESL服务器还可以基于价签显示商品的其他信息，比如有效期、优惠说明、产品详细参数等功能。
- ERP介绍
  - ERP系统是企业资源计划 (Enterprise Resource Planning)的简称，是指建立在信息技术基础上，集信息技术与先进管理思想于一身，以系统化的管理思想，为企业员工及决策层提供决策手段的管理平台。

华为智简园区智慧零售电子价签方案：典型配置指导（1）



场景介绍

在某大型超市中部署物联网AP+电子价签插卡方案，电子价签插卡和管理系统之间进行业务下发和上送。

配置思路

以WLAN+AP组网为例，首先完成网规和信道分配，按照以下步骤进行相关配置：

1、将卡类型配置为Ethernet连接方式（当前ESL场景的主流插卡均使用Ethernet方式接口）。

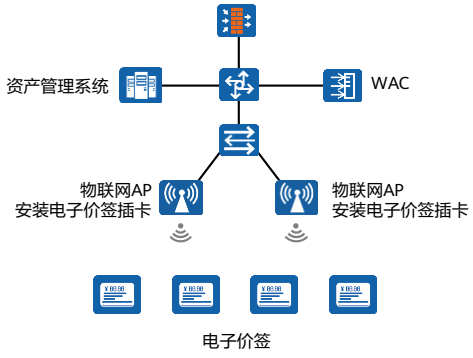
2、配置插卡使用的VLAN，不配置时，默认和AP使用相同vlan。

3、将wired-port-profile绑定给对应的card下。

网规建议

由于零售场景存在货架遮挡，对ESL业务可能存在影响，因此在网规中需要考虑货架遮挡，尽量减少货架对AP/ESL融合基站的遮挡。

华为智简园区智慧零售电子价签方案：典型配置指导（2）



1.将卡类型配置为Ethernet连接方式（当前ESL场景的主流插卡均使用Ethernet方式接口）

```
[WAC-wlan-view] ap-group name ESL
[WAC-wlan-ap-group-esl] card 1
[WAC-wlan-ap-group-card-esl/1] card connect-type Ethernet
```

2.配置插卡使用的VLAN，不配置时，默认和AP使用相同vlan

```
[WAC-wlan-view] wired-port-profile name ESL
[WAC-wlan -wired-port-esl] vlan pvid 805
[WAC-wlan -wired-port-esl] vlan untagged 805
```

3.将wired-port-profile绑定到card 1下

```
[WAC-wlan-view] ap-group name ESL
[WAC-wlan-ap-group-esl] card 1
[WAC-wlan-ap-group-card-esl/1] card connect-type ethernet
[WAC-wlan-ap-group-card-esl/1] wired-port-profile ESL
```

思考题

1. 常见的短距无线射频技术有哪些?
2. 不同短距无线射频技术的特点和使用场景分别是怎样的?

HUAWEI

- 常见的短距无线射频技术有哪些?
  - RFID、Bluetooth、ZigBee、Wi-Fi等。
- 不同短距无线射频技术的特点和使用场景分别是怎样的?
  - RFID利用射频信号和空间耦合（电感或电磁耦合）或雷达反射的传输特性实现物体识别，覆盖了低频到超高频不同频段范围，适用范围比较广，如门禁、资产管理等场景均可以使用。
  - Bluetooth技术是使用最广泛的全球短距离无线标准之一，遵循IEEE802.15.1协议标准，工作在2.4 GHz频段。目前在外围设备互联（蓝牙耳机、鼠标等）、智能穿戴设备（手环、手表等）、物联网（家用电子设备）均有使用。
  - Zigbee基于IEEE802.15.4的通信协议的短距离、低功耗的无线通信技术。ZigBee具有近距离、自组织、低功耗、低数据速率等特点。ZigBee支持星型组网、MESH组网和混合组网（星型组网+MESH组网）三种不同的组网方式。ZigBee广泛应用于工业和智慧家庭领域。
  - Wi-Fi基于IEEE802.11标准的无线联网技术，工作在2.4 GHz和5 GHz频段，主要使用在无线局域网，家庭，室内场所高速上网。

本章总结

- 本章首先介绍了物联网的基本概念及发展趋势，随后介绍了常见的短距无线通信技术，包括Wi-Fi、RFID、蓝牙、ZigBee，最后讲解了华为智简园区物联网方案，以及华为物联网AP。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN无线定位技术

HUAWEI

前言

- 无线定位技术是通过对无线电磁波特征参数的测量，采用一些算法确定终端所处位置的技术。
- 无线定位技术的应用，如GPS定位、北斗卫星定位在日常生活中较为常见，为大家所熟知。但是卫星定位主要在室外环境使用，在室内，由于建筑物对信号的屏蔽，卫星定位难以正常使用。
- 为了满足室内定位的需求，各种室内定位技术应运而生，如基于射频、传感器、机器视觉、地磁等的定位技术，目前很多技术如地磁还处在研究实验阶段。基于射频的无线定位技术已经得到较为广泛的应用，常见的射频技术有：Wi-Fi、蓝牙、和UWB（Ultra-Wideband，超带宽）等。

目标

- 学完本课程后，您将能够：
  - 描述常见无线射频定位技术的基本原理
  - 描述华为园区无线定位方案和应用场景

目录

无线定位技术的发展

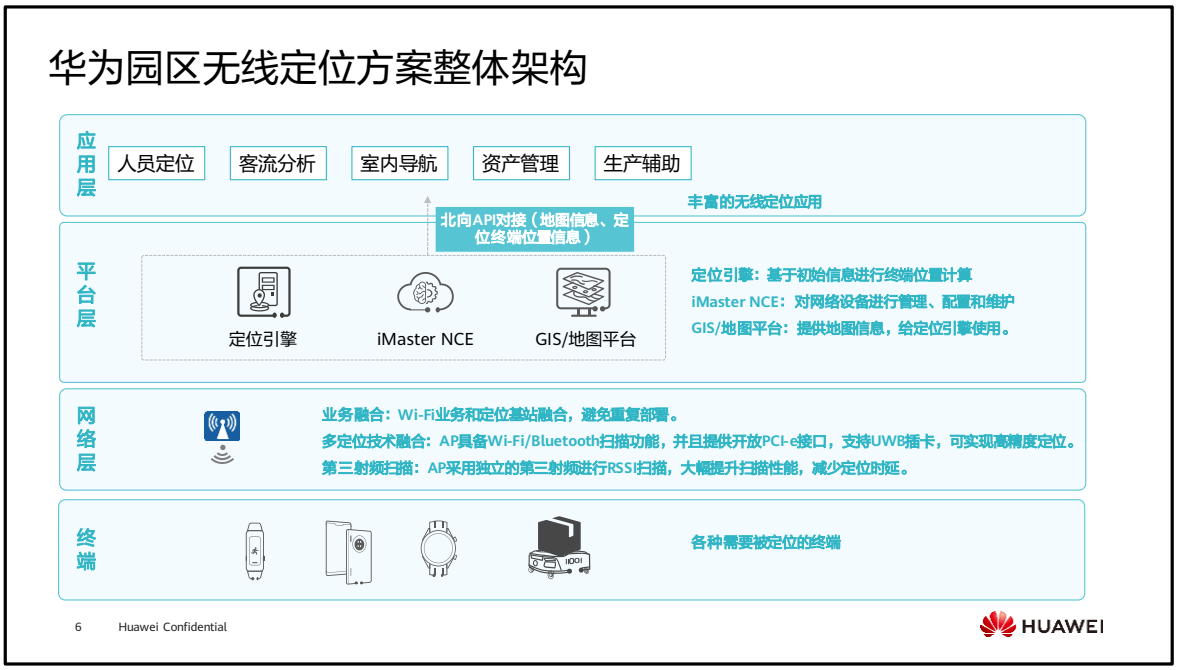
- 从GPS、短波等广域定位技术，再到如今的室内定位技术，定位技术发展迅速。
- 基于射频信号的室内定位技术包括Wi-Fi、蓝牙、Zigbee、蜂窝网络、RFID、UWB等。

分类	定位方式	定位精度	优缺点
室外定位	卫星定位：如GPS、GLONAS、GALILEO、北斗卫星导航系统等	10米	优点：室外定位精度较高 缺点：受环境、天气、位置等影响较大，耗电高。
	基站定位：如GSM蜂窝基站定位、CDMA基站定位	市区20-200米 郊区1000-2000米	优点：定位精度低 缺点：需要三个基站共同完成定位，条件严苛。
室内定位	无线射频：RFID、ZigBee、Wi-Fi Bluetooth、UWB等	0.1米-10米	优点：室内定位精度高 缺点：需要根据不同环境和定位要求选择对应的技术，部署成本和适用场景各不相同。

位置服务的行业场景应用

人员定位	客流分析	室内导航	资产管理	生产辅助
				
• 外来访客管理 • 产线工人定位 • 特殊人员位置跟踪	• 商场热图 • 人物画像 • 消费习惯分析 • 精准营销	• 商场店铺导航 • 机场、车站路线规划 • 停车导航、反向寻车	• 资产定位 • 资产轨迹回溯 • 电子围栏 • 资产使用调度	• AGV、机械臂精准定位 • 仓储物流管理 • 车间危化区域防护 • 高危作业环境人员定位

科技在发展，时代在进步，对室内定位服务的诉求越来越多。



- 应用层：和位置信息相关的应用。基于位置信息，进行上层应用平台的开发，或者生产管理系统、行政管理系统等客户已有系统调用位置信息相关的API，进行应用开发和呈现。
- 平台层：平台层主要可以分为三大部分：
  - 定位引擎：对获取到的位置初始信息，如RSSI、时间等进行计算，得出被定位对象的位置坐标。
  - iMaster NCE：对网络设备进行管理、配置和维护。
  - GIS/地图平台：主要提供地图信息，给定位引擎使用。
- 网络层：AP提供Wi-Fi/Bluetooth的信号覆盖和管理（根据实际业务场景选择是否部署iBeacon，在手机导航场景下一般需要部署iBeacon）
  - AP扫描Wi-Fi终端RSSI数据并将数据上报。
  - AP扫描蓝牙终端RSSI数据并将数据上报。
  - AP可作为标准iBeacon进行广播。
  - AP透传PCI-e插卡定位报文。
- 终端层：各种需要被定位的终端。

目录

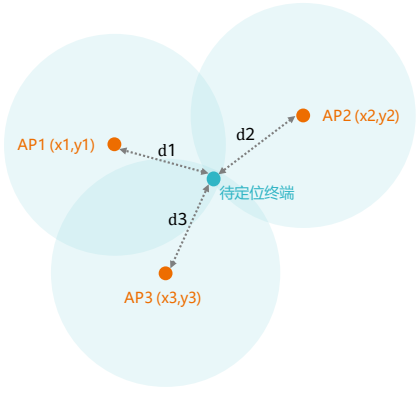
无线定位技术原理概述

- 无线定位是利用接收到的无线电信号的统计特征对源目标进行定位，所依赖的无线电信号的主要参数包括信号强度、到达角度以及传播时延等。

基于信号强度	基于信号传播时间	基于信号到达角度
• **前提条件：** ▫ 信号功率随传播距离衰减模型已知 • **常用方式：** ▫ RSSI传播模型法 ▫ RSSI指纹	• **前提条件：** ▫ 信号传播速度是已知的 ▫ 电磁波沿着最短路径进行传播 (LOS)，不考虑信号反射、折射、衍射等因素。 • **常用方式：** ▫ TOA ▫ TDOA ▫ TOF	• **前提条件：** ▫ 测量点具有方向性的天线 (Directional Antenna) 或天线阵列 (Antenna Array)，能够得到移动节点发送信号的方向，从而根据信号的到达方向来进行定位。 • **常用方式：** ▫ AOA ▫ PoA

- RSSI (Received Signal Strength Indication)传播模型法：利用信号强度测量得到距离的方法。
- RSSI指纹：利用场强作为指纹特征值。
- TOA (Time of Arrival)、TDOA (Time Difference of Arrival)：信号到达时间、到达时间差测量，需要基站之间进行时间同步。
- TOF (Time of Fight)：利用信号飞行时间进行距离测量。
- AOA (Angle of Arrive)：基于信号到达角度的定位算法是一种典型的基于测距的定位算法。
- PoA (Phase of Arrive)：使用接收的载波相位来确定两个设备之间的距离。

基于信号强度（传播模型法）



技术原理

- 通过无线信号中的RSSI与距离的函数关系，来确定待定位终端与AP之间的距离。
- 根据多个AP（至少3个，越多精度越高）接收计算的同一终端的距离值以及AP的点位来确定待定位终端的位置；

信号在自由空间传播遵循固定的衰减模型：

$$P_d = P_0 - 10n\log(\frac{d}{d_0})$$

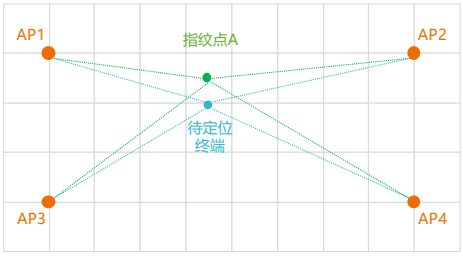
P_d为待定位点接收到的信号强度，P_0为距离辐射源d_0处的信号强度。

n 为信号衰减系数。

优点与缺点

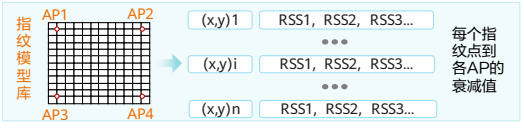
- **优点：**部署简单，成本低。
- **缺点**：定位精度较差，抗干扰能力较差。

基于信号强度（指纹法）



技术原理

1. 在地图上，每间隔若干距离取一个指纹点；
2. 获取每个指纹点到各AP的信号强度；
3. 将该指纹点到各AP信号强度作为该点的信号强度特征值；
4. 将收集到的终端的信号强度，与各指纹点的信号强度特征值做匹配，寻找相似度最高的指纹点。



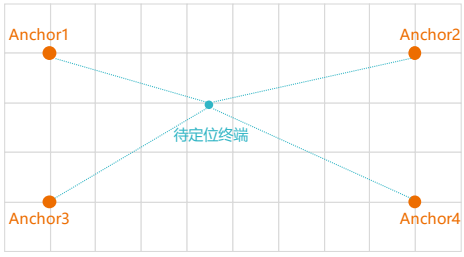
优点与缺点

- **优点：** 定位精度高。
- **缺点：** 对AP部署点位要求高；指纹点的信号强度需要按时采集，维护成本高。

HUAWEI

- RSSI指纹的获取可以通过两种方式获取：
  - 在环境中进行实际的采集，该指纹库维护方式较为复杂，环境中指纹信息发生变化对定位结果影响较大；
  - 通过AP部署位置和环境情况进行计算，形成虚拟的指纹库，该方式不需要大量的采集工作，但是环境对指纹的影响将导致指纹模型库不够准确，从而导致定位结果不准确。
- 采用RSSI指纹定位方法时，定位精度受信号波动、终端位置、信号多径传输等多个因素影响，误差较大。

基于信号传播时间



根据信号传输时长测算距离

技术原理

- TOA (Time of Arrival)：利用电波到达时间来确定距离目标的距离，再利用三点定位原理，计算得到目标位置。
- TDOA (Time Difference of Arrival)：通过不同Anchor（基站）收到信号到达的时间差来计算目标到与不同Anchor的距离差，再利用双曲线特性计算得到目标定位。

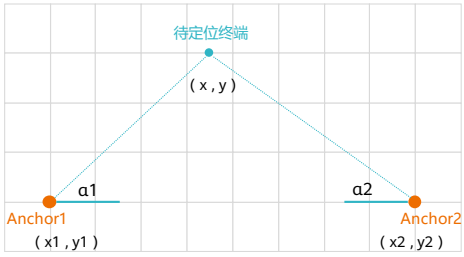
优点与缺点

- **优点：**定位精度高。
- **缺点：**需实现时间同步（一定精确量级的时间同步）；部署成本高。

HUAWEI

- Anchor：定位基站。
- TOA (Time of Arrival)：利用电波到达时间来确定距离目标的距离，再利用三点定位原理，计算得到目标位置。待定位终端发射信号到达3个以上的参考节点接收机(Anchor)，通过测量到达不同Anchor所用的时间，得到发射点与Anchor之间的距离，然后以Anchor为圆心，所测得的距离为半径绘制圆，3个圆的交点即为待定位终端所在的位置。但是TOA要求参考节点与被测点保持严格的时间同步，多数应用场合无法满足这一要求。
- TDOA (Time Difference of Arrival)：通过不同基站收到信号到达的时间差来计算目标到与不同基站的距离差，再利用双曲线特性计算得到目标定位。TDOA定位即双曲线定位，二维定位中需要使用4个定位Anchor。Anchor时间同步之后，待定位终端发送一个广播报文，Anchor收到之后，标记接收到此报文的时间戳，并将内容发送到计算服务器，计算服务器根据其他Anchor的定位报文的时间戳，计算出待定位终端的位置。通过测量待定位终端到每两个Anchor之间的距离差，距离差等于常量即可绘制出双曲线，而曲线交点即可确定标签坐标。
    - 双曲线：定义为与两个固定的点的距离差是常数的点的集合。双曲线焦点即为目标位置。

基于信号到达角度



技术原理

AOA定位原理： Anchor装有天线阵列时，天线阵列根据待定位终端发送的信号来确定入射角度。两个Anchor的入射角分别为α1，α2，以各Anchor为起点，入射角方向构造直线的交点，即为终端的位置。假设终端的置坐标为（x，y），Anchor的位置坐标为（xi，yi），是已知量，根据其几何意义，则它们之间满足：

(x-x1) tan α1=y-y1

(x-x2) tan α2=y-y2

可根据以上方程式解出带定位终端的位置（x，y）。

优点与缺点

- **优点：** 定位精度较高，算法通信开销低（最少仅需单个AP）。
- **缺点：** 多径效应会影响信号从一个完全不同的角度到达接收端，因此多径对AOA的影响很大；配备有AOA参数估计的节点硬件尺寸、功耗及成本相对较大，接收机天线的角度分辨率也受到硬件设备的极限限制。

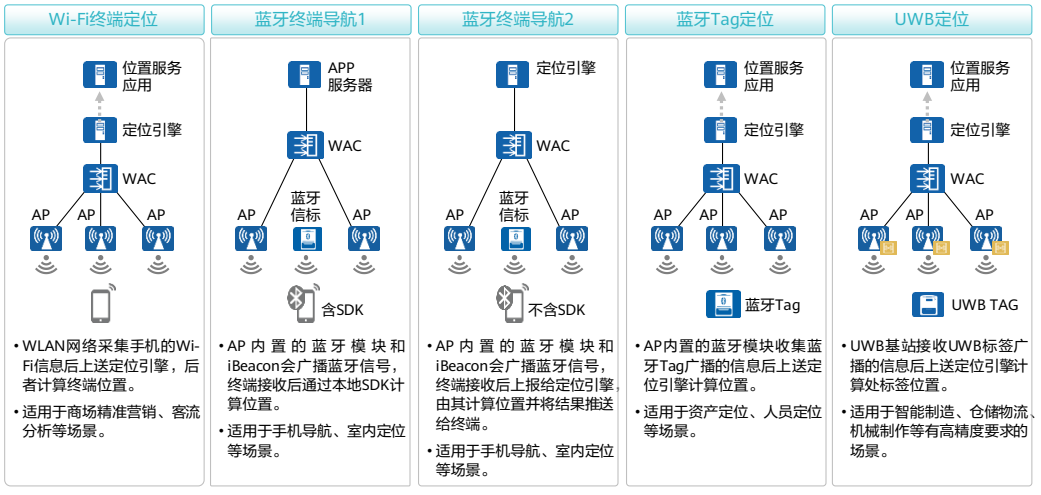
- AOA (Angle of Arrival)：基于信号到达角度的定位算法，通过硬件设备感知发射节点信号的到达方向，计算接收节点和锚节点之间的相对方位或角度，然后再利用三角测量法或其他方式计算出未知节点的位置。

室内无线定位技术

定位技术	RFID	Wi-Fi	Bluetooth	Zigbee	UWB
常用算法	TDOA	RSSI、AOA	RSSI、AOA	RSSI	TDOA、AOA
定位精度	米级	米级	米级	米级	亚米级别
传输范围	5米	300米	100米	300米	150米
穿透性	一般	一般	一般	一般	良好
抗干扰性	弱	一般	弱	一般	良好
应用	电子标签、仓库和工厂等货品定位等	商场、公园及写字楼等低精度定位需求场景	商场、公园及写字楼等低精度定位需求场景	大型工厂和车间等	安保、医疗、工业及物流等

目录

华为智简园区无线定位方案概述

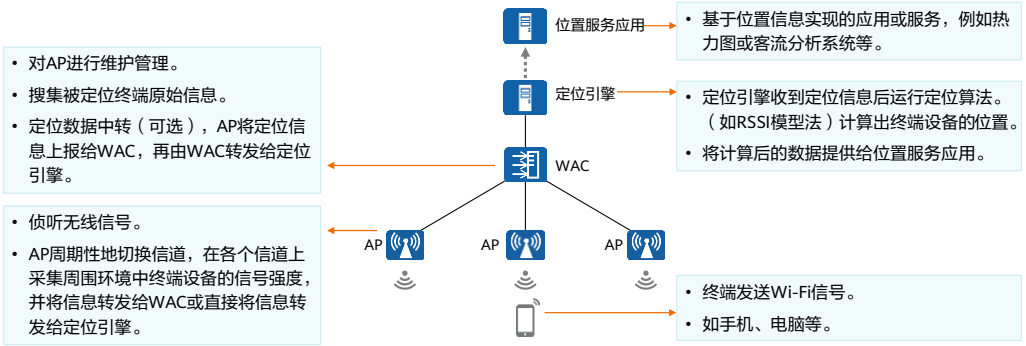


HUAWEI

- 对于以上无线定位方案，定位精度都会受到AP安装环境、部署密度、部署高度、安装角度、空间障碍物分布等多种因素影响，实际定位精度可能会与理论值存在或大或小的偏差，实际交付过程中需进行现场调试。

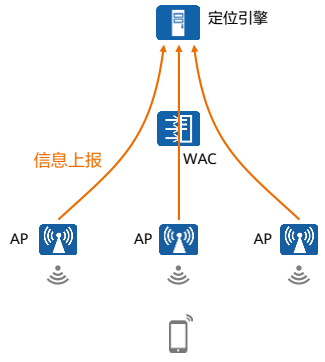
Wi-Fi终端定位技术概述

- Wi-Fi终端定位技术是在Wi-Fi信号覆盖范围内，对Wi-Fi终端（如手机、电脑）进行定位的技术。
- AP将收集到的周围环境中终端发射的Wi-Fi信号信息上报给定位引擎，定位引擎根据无线信号强度信息与AP的位置，计算出终端的位置信息，结合室内地图展现给用户。



- Wi-Fi定位还可以对非法AP（非统一部署的AP设备）和非Wi-Fi干扰源（例如微波炉等）进行定位。

Wi-Fi终端定位技术实现



Step 1：AP采集无线信号

- AP 周期性地切换信道，在各个信道上采集周围环境中终端的帧信息，并记录每个收到帧的 RSSI（信号强度）、时间戳、速率、信道等定位信息。

Step 2：WLAN设备上报数据信息给定位引擎

- 方式一集中转发：AP先将数据上报给WAC，由WAC再将数据上报给定位引擎。
- 方式二直接上报：AP直接将数据上报给定位引擎。

Step 3：定位引擎进行定位计算

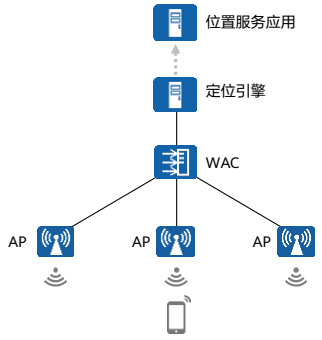
为了更精确地计算每个终端的位置，定位引擎需要至少收到3个AP上报的定位信息。

定位引擎收到定位信息后，根据用户事先导入的地图信息和标识的AP的位置，按照RSSI定位算法通过对报文中的RSSI、SNR（信噪比）等信息进行计算，计算出终端所在的位置并展现在室内地图或管理平台中。

HUAWEI

- WAC支持以UDP协议报文或者HTTP协议报文方式将位置信息上报给定位引擎。

Wi-Fi终端定位技术典型配置（1）



场景介绍：

- 在某商场部署基于Wi-FI定位的客流分析系统，整体组网架构如图所示。

配置思路：

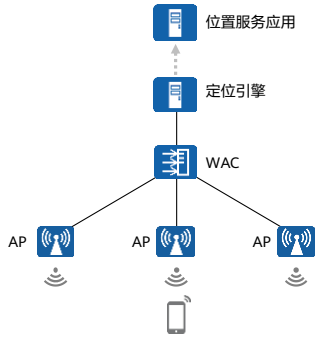
以WAC+AP组网为例，首先完成网规和信道分配，按照以下步骤进行相关配置：

1. 配置WLAN参数，使能Radio。
2. 配置空口扫描模板”wlan-air-scan”，配置空口扫描信道集合。
3. 扫描模板”wlan-air-scan”绑定到radio。
4. 配置定位模板”wlan-location”，配置定位参数。

网规建议：

- 三角定位，确保待定位终端到三个AP视距可达，推荐AP部署间距15米以内。
- 室外款型由于部署间距较大不支持该定位方案。

Wi-Fi终端定位技术典型配置（2）



1. 配置空口扫描模板"wlan-air-scan"，配置空口扫描信道集合。

```
[WAC-wlan-view] air-scan-profile name wlan-air-scan
[WAC-wlan-air-scan-prof-wlan-air-scan] scan-channel-set country-channel
[WAC-wlan-air-scan-prof-wlan-air-scan] scan-period 100
[WAC-wlan-air-scan-prof-wlan-air-scan] scan-interval 1000
```

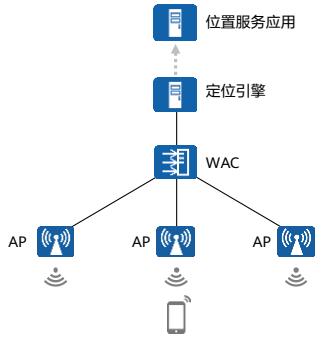
2. 扫描模板"wlan-air-scan"绑定到radio模板下。

```
[WAC-wlan-view] radio-2g-profile name wlan-radio-2g
[WAC-wlan-radio-2g-prof-wlan-radio-2g] air-scan-profile wlan-air-scan
```


HUAWEI

- 对时延要求高，且被测试终端关联到AP上的情况建议使用参数work-channel，仅扫描工作信道，避免扫描所有信道的时间开销。

Wi-Fi终端定位技术典型配置（3）

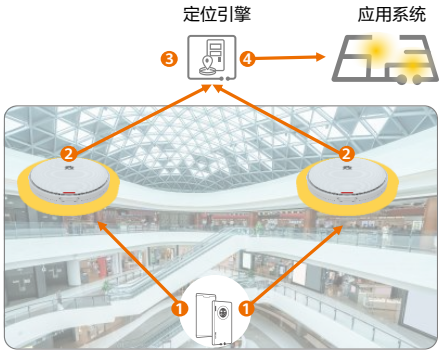


3. 配置定位模板"wlan-location"，配置定位参数。

[WAC-wlan-view] **location-profile name** *wlan-location*
[WAC-wlan-location-prof-wlan-location] **private mu-enable**
[WAC-wlan-location-prof-wlan-location] **private report-frequency** *500* // 根据实际场景，对时延要求较高场景，推荐使用最小值500ms。
[WAC-wlan-location-prof-wlan-location] **private mu protocol-version v5** // V5和V3可选，V5具备扩展参数，建议使用V5对接。
[WAC-wlan-location-prof-wlan-location] **private server ip-address** *192.168.1.2* **port** *32180* //定位引擎的IP地址和端口。

4. 注意需要使能扫描功能（如通过配置VAP，配置方法参照产品手册）。

Wi-Fi终端定位技术典型应用

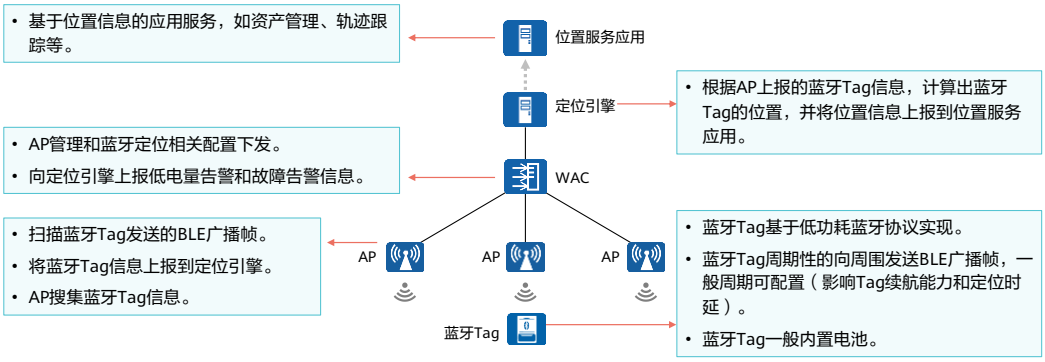


某商场需要进行顾客热力图分析，以在人员密集区域进行广告投放，提高广告投放效果。

1. 手机终端在正常使用时在2.4 GHz和5 GHz均会在不同信道发送大量的管理和业务帧，如Probe帧等，其中携带了终端特征信息。
2. AP处在正常工作模式下，在用户指定的扫描信道中逐个进行扫描，侦听上述帧，并提取终端和RSSI信息，按照指定的格式封装到IP报文中上报到定位引擎。
3. 定位引擎收到多个AP上报的终端信息，使用定位算法（如RSSI模型法）计算出手机终端的具体位置，并将位置数据上报到应用系统。
4. 应用系统将终端位置信息结合商场的地图进行呈现，展示顾客热力图。

蓝牙Tag定位技术概述

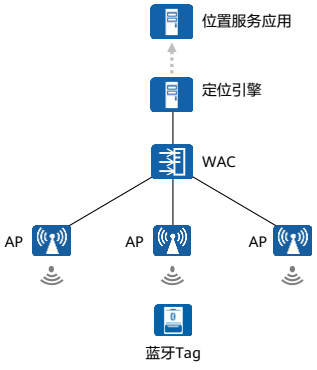
- 蓝牙Tag（泛指蓝牙低功耗设备）定位主要用来实现定位环境中部署蓝牙Tag后，AP内置蓝牙模块进行扫描后，AP将获取到的蓝牙Tag信息上传到定位引擎，定位引擎计算出位置信息，并将位置信息上报给位置服务应用。



HUAWEI

- 对于AP可以管理的低功耗蓝牙设备，需要适配华为AP南向接口。

蓝牙Tag定位技术实现



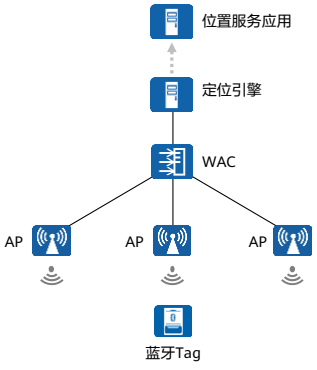
Step 1：完成WLAN网规，根据定位环境和定位诉求，进行AP位置规划，并形成AP位置信息。

Step 2：AP作为BLE侦听设备，侦听网络中蓝牙Tag发送的BLE广播帧。

Step 3：AP向定位引擎上报BLE设备信息。

Step 4：定位引擎计算蓝牙Tag位置，并将蓝牙Tag位置信息上报到位置服务应用上进行呈现。

蓝牙Tag定位技术典型配置（1）



场景介绍：

- 在某商场需要对扫地车进行定位，扫地车上安装蓝牙Tag，组网如图所示。

配置思路：

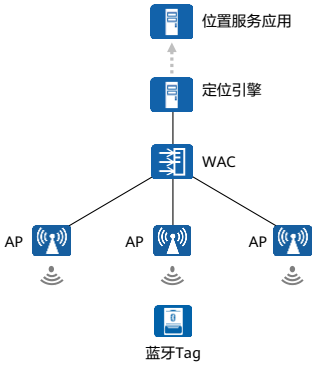
以WAC+AP组网为例，按照以下步骤进行相关配置：

1. 配置ble-profile，使能蓝牙扫描，配置蓝牙扫描方式、上报方式和定位引擎的地址和端口号。
2. 将ble-profile绑定到ap-group。

网规建议：

- 三角定位，确保待定位终端到三个AP视距可达，推荐AP部署间距15米以内。
- 室外款型由于部署间距较大不支持该定位方案。

蓝牙Tag定位技术典型配置（2）



1. 配置ble-profile，使能蓝牙扫描，配置蓝牙扫描方式、上报方式和定位引擎的地址和端口号。

[WAC-wlan-view] **ble-profile name** *wlan-ble*
[WAC-wlan-ble-prof-wlan-ble] **report enable** // 使能蓝牙Tag定位报文上报
[WAC-wlan-ble-prof-wlan-ble] **sniffer enable tag-mode** // 扫描方式一共三个，tag-mode，iBeacon-mode，transparent-mode，可以根据场景选择具体使用的mode。
[WAC-wlan-ble-prof-wlan-ble] **report-mode immediate** // 立即上报和周期性上报两种方式
[WAC-wlan-ble-prof-wlan-ble] **report-to-server ip-address** *192.168.2.13* **port** *65432* //*设置定位引擎接收定位报文的IP和PORT

2. 将ble-profile绑定到ap-group。

[WAC-wlan-view] **ap-group name** *ap-group1*
[WAC-wlan-ap-group-ap-group1] **ble-profile** *wlan-ble*

蓝牙Tag定位技术典型应用

某仓库中需要对叉车进行定位，避免出现叉车调度不合理现象

1. 蓝牙Tag安装在叉车顶部后，周期性（如1秒）广播低功耗蓝牙报文，蓝牙报文中携带Tag ID信息。
2. AP内置的蓝牙模块开启扫描功能后，可以接收环境中的BLE帧，合理的WLAN网规可以保证多个AP同时接收到一个BLE帧，AP将接收到的BLE帧封装成IP报文，上报到指定的定位引擎上。
3. 定位引擎接收到多个AP上报的BLE帧，使用定位算法如RSSI模型法，计算出蓝牙Tag的具体位置，并将位置数据上报到应用系统。
4. 应用系统将叉车的位置信息结合仓库的地图进行实时呈现，可以进行叉车位置实时跟踪。

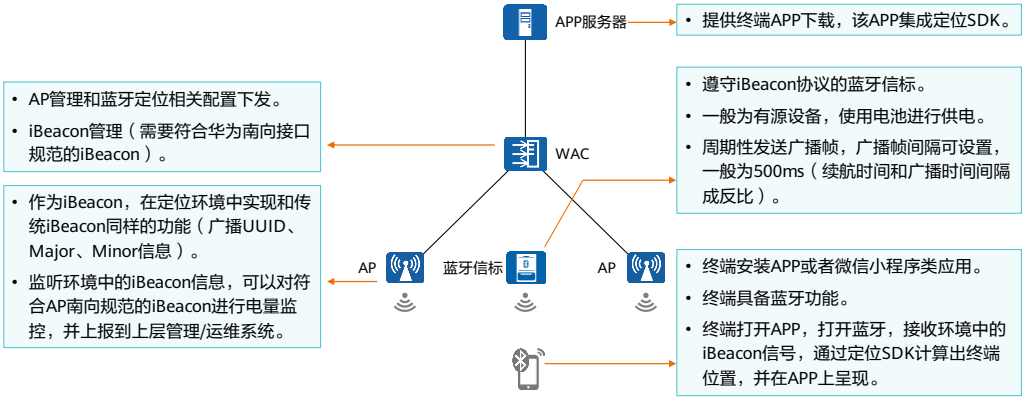
蓝牙终端导航方案概述

- 蓝牙终端导航技术主要是指在导航的诉求下，终端通过一定方式进行位置定位和路线设定，并在终端APP上进行呈现的方案。
- 该方案中位置定位方式主要有两种：
  - 方式一：终端具备定位SDK，可以通过终端APP进行位置计算及展示和应用呈现。
  - 方式二：终端不具备定位SDK，终端接收蓝牙信标(iBeacon)发送的信息，并将其上报到定位引擎，定位引擎计算出终端位置后将位置信息返回给终端APP进行呈现。

- SDK（Software Development Kit，软件开发工具包）是一系列程序接口，文档，开发工具的集合。

蓝牙终端导航方案技术实现（1）

- 蓝牙终端导航实现方式一：终端具备定位SDK，可以通过终端APP进行位置计算及展示和应用呈现。

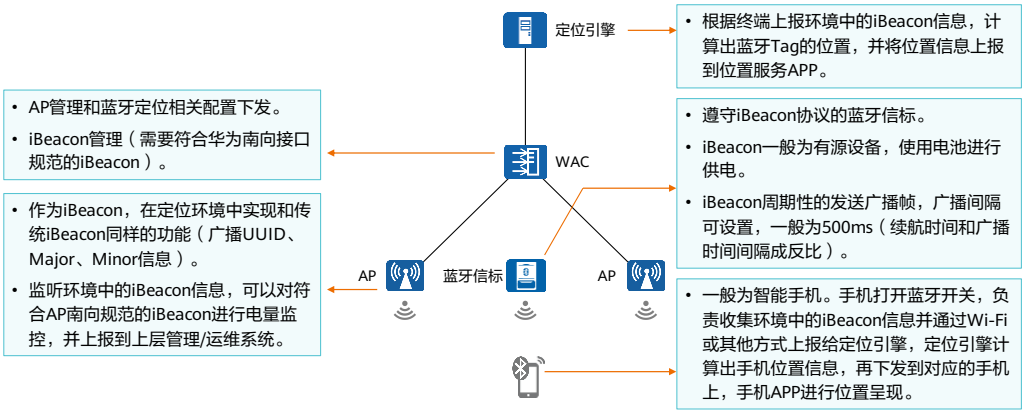


HUAWEI

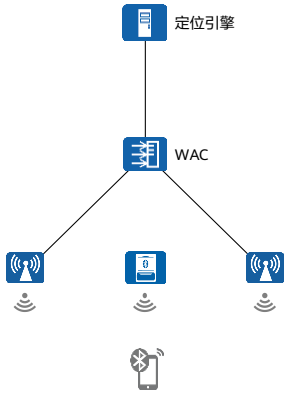
- 对于AP可以管理的低功耗蓝牙设备，需要适配华为AP南向接口。

蓝牙终端导航方案技术实现（2）

- 蓝牙终端导航实现方式二：终端不具备定位SDK，终端接收蓝牙信标（iBeacon)发送的信息，并将其上报到定位引擎，定位引擎计算出终端位置后将位置信息返回给终端APP进行呈现。



蓝牙终端导航方案典型配置（1）



场景介绍：

- 在某商场需要对扫地机进行定位，扫地车上安装蓝牙Tag，组网情况如左图。

配置思路：

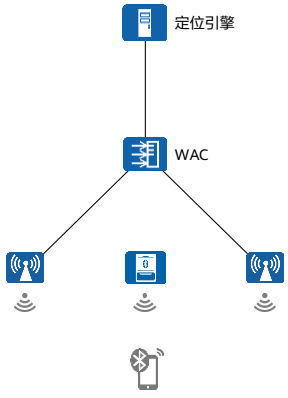
以WLAN+AP组网为例，按照以下步骤进行相关配置：

1. 配置ble-profile，使能蓝牙广播，配置蓝牙广播参数。
2. 将ble-profile绑定到ap-group。

网规建议：

- 三角定位，确保待定位终端到三个AP视距可达，推荐AP部署间距15米以内。
- 室外款型由于部署间距较大不支持该定位方案。

蓝牙终端导航方案典型配置（2）



1. 配置ble-profile，使能蓝牙扫描，配置蓝牙扫描方式、上报方式和定位引擎的地址和端口号。

```
[WAC-wlan-view] ble-profile name wlan-ble
[WAC-wlan-ble-prof-wlan-ble] broadcaster enable  //使能ibeacon广播
[WAC-wlan-ble-prof-wlan-ble] tx-power-12  //配置ibeacon发射功率，可选配置项。
[WAC-wlan-ble-prof-wlan-ble] broadcasting-interval 330 //配置ibeacon广播间隔，单位为ms。
[WAC-wlan-ble-prof-wlan-ble] broadcasting-content UUID UUID-hex
7D2D84574F7133A0065DC68A98F4CABC Major Major-hex 53FC Minor Minor-hex 271B //配置广播参数，如UUID Major Minor。
[WAC-wlan-ble-prof-wlan-ble] sniffer enable ibeacon-mode  //使能侦听ibeacon,可以在AP/AC上查看iBeacon信息。
[WAC-wlan-ble-prof-wlan-ble] report-mode immediate
[WAC-wlan-ble-prof-wlan-ble] report-to-server ip-address 192.168.2.13 port 65432 //将AP侦听到的ibeacon信息上报到指定的管理服务器上。
[WAC-wlan-ble-prof-wlan-ble] report enable
```

2. 将ble-profile绑定到ap-group。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] ble-profile wlan-ble
```

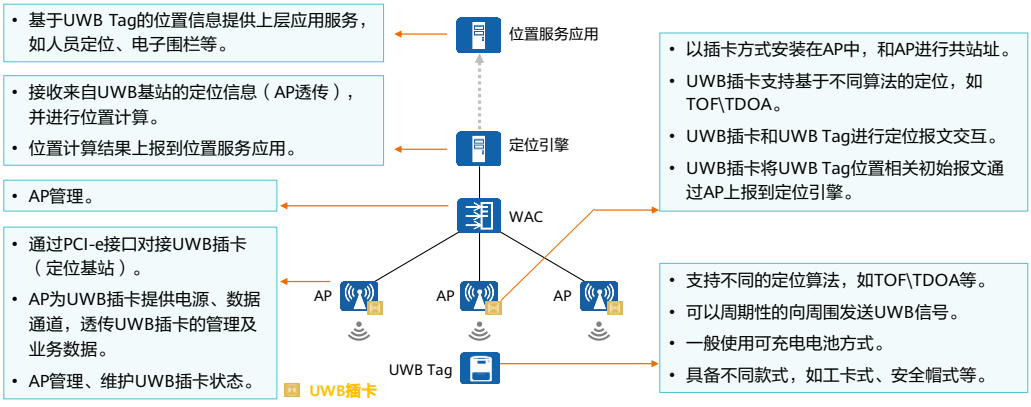
蓝牙终端导航（终端含SDK）典型应用

旅客到达某陌生机场，需要进行行李提取，旅客借助导航快速到达行李提取处，旅程体验大大优化

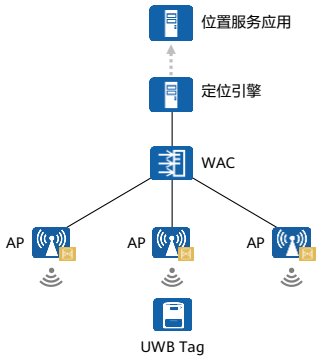
1. 旅客打开机场微信小程序或机场导航应用APP（应用中已经继承定位SDK ），应用提醒旅客打开蓝牙。
2. 旅客手机开始接收环境中的蓝牙信号，机场部署的独立iBeacon和AP iBeacon在持续进行蓝牙信号广播，旅客手机接收到后，基于蓝牙报文携带的UUID、Major、Minor信息，通过RSSI衰减模型或者指纹算法进行计算，得到当前自己的位置，并在手机应用上进行呈现；旅客在手机应用中输入“行李提取处”，得到规划路线，按照规划路线快速到达目的地。
3. AP在该场景中既可以作为iBeacon使用，也可以开启蓝牙扫描功能接收环境中部署的iBeacon广播报文，对于符合AP南向接口的iBeacon，AP可以获取到电量、状态信息。
4. AP可以将获取到的环境中独立iBeacon的状态数据上报给指定服务器，实现iBeacon的管理和维护。

UWB定位技术概述

- UWB定位技术是指利用UWB定位基站和UWB定位标签，通过一定的算法，如TDOA、TOF等解算出UWB标签的位置，可以实现较高精度的定位。



UWB定位技术实现



Step 1：WLAN网规，针对定位环境和定位需求，进行AP融合UWB基站点位规划、制图，并根据环境情况确定合适的定位算法。进行AP融合UWB插卡基站安装。

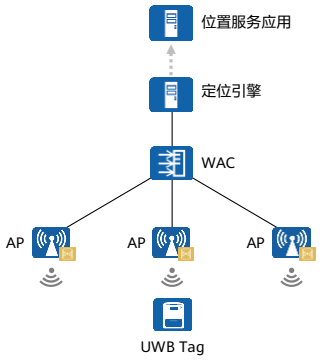
Step 2：WAC对AP（融合UWB插卡）进行配置，指定PCI-e接口方式，定位引擎IP地址和端口号等。

Step 3：UWB插卡根据用户指定的算法，进行UWB Tag信号接收和处理，并将定位数据通过PCI-e接口发给AP，AP将数据上报至定位引擎。

Step 4：定位引擎对AP上报的原始定位信息进行计算，计算出UWB Tag的位置，并将位置信息上报给位置服务应用。

Step 5：位置服务应用基于位置信息、以及UWB Tag和被定位对象（人或物体）之间的关系进行呈现，实现诸如人员定位、资产定位、轨迹跟踪等应用。

UWB定位技术典型配置（1）



场景介绍：

- 在某工厂中部署UWB定位方案，进行人员管理。

配置思路：

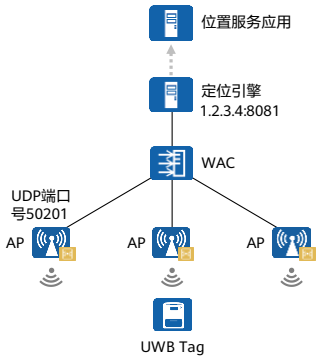
以WAC+AP组网为例，按照以下步骤进行相关配置：

1. 配置IoT模板，指定定位引擎的IP地址和端口号；
2. 配置AP组引用iot模板，指定AP和资产管理server通信的端口号和通信协议。

网规建议：

- AP间距15米以内，相互之间无遮挡，“田”字格式部署，被定位对象需要在UWB基站信号覆盖范围内，定位精度受现场环境影响较大，需进行现场工勘及网规。

UWB定位技术典型配置（2）



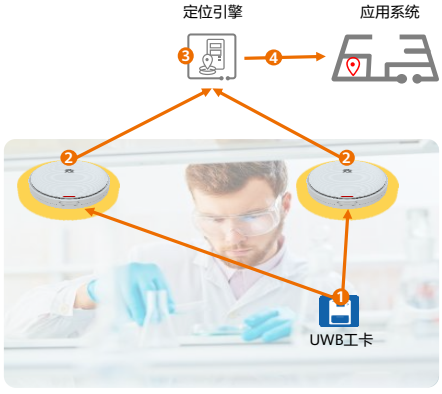
1. 配置名为“IoT”的IoT模板，指定定位引擎IP地址和端口号。

```
[WAC-wlan-view] iot-profile name iot
[WAC-wlan-iot-prof-IOT] management-server server-ip 1.2.3.4 server-port 8081
```

2. 配置AP组引用IoT模板，指定AP和定位引擎的端口号和通信协议。

```
[WAC-wlan-view] ap-group name ap-group1
[WAC-wlan-ap-group-ap-group1]] card 1    //此处需根据插卡的实际位置设置
[WAC-wlan-group-card-ap-group1/1] iot-profile iot config-agent udp port 50201
```

UWB定位技术典型应用



某化工厂需要对工作人员进行位置定位，对于进入危险区域的不具备操作权限的员工，进行提醒和告警，以减少安全事故的发生。（以TDOA算法方式为例）

1. 工作人员佩戴UWB工卡，UWB工卡广播的信息中携带工卡ID、广播报文序列号等信息，UWB基站（AP融合UWB插卡）将收到该信号。
2. UWB基站之间通过主从关系，进行时钟同步，即主基站周期性发包，从基站进行时钟同步，从而进行时间校准。不同基站接收到相同UWB工卡广播序列号的信息后，可以获取到信号到达时间差，将工卡ID、时间信息通过AP上报到定位引擎。
3. 定位引擎将AP上报的报文进行计算，计算出UWB工卡的坐标，并将坐标信息上报给应用系统。
4. 应用系统在地图上设置危险区域，当被定位的UWB工卡坐标进入该区域时，在系统上产生告警，通过UWB基站将告警发送给UWB工卡，UWB工卡进行声光报警。由于UWB工卡发包间隔较小（可设置到1秒内），告警信息可以及时有效的下发给佩戴工卡的工作人员。

华为园区无线定位方案汇总

定位方案	适用场景	部署要求	定位精度	优缺点
Wi-Fi终端定位	商场、超市等场景的客流分析、热力图、用户大数据分析	3+AP共同覆盖定位区域，AP间距15米，被定位点位到基站间视距可达	3-10米	优点：不需要额外部署设备，部署简单 缺点：定位误差大，终端行为难以控制
蓝牙Tag定位	企业、医疗、教育、机场等场景中固定资产管理	3+AP共同覆盖定位区域，AP间距15米，被定位点位到基站间视距可达	3-10米	优点：不需要额外部署设备，部署简单 缺点：终端一般使用电池，需要进行电量管理
蓝牙终端导航	商场顾客导航、机场旅客导航	补充独立iBeacon做定位辅助，AP和独立iBeacon之间建议8米间距	1-3米	优点：AP可以作为iBeacon，并对环境中的独立iBeacon进行管理 缺点：终端需具备惯性导航模块
UWB定位	制造、电厂、化工厂等人员实时定位、巡检等	呈田字形部署，AP间距推荐15米，视距可达，没有金属等障碍物遮挡	0.3米	优点：定位精度高 缺点：部署难，成本高

- 3+AP指的是至少3个AP。
- 惯性导航模块指手机里面陀螺仪、加速度仪等。

思考题

1. 无线定位原理按照测量特征，可以分为哪几类?
2. 无线定位射频技术有哪些?

HUAWEI

- 可以分为三类：基于信号强度，基于信号传播时间，基于信号到达角度
- Wi-Fi、蓝牙、RFID、UWB、Zigbee等

本章总结

- 为了满足室内定位的需求，各种室内定位技术应运而生，如基于射频、传感器、机器视觉、地磁等的定位技术，目前很多技术如地磁还处在研究实验阶段。基于射频的无线定位技术已经得到较为广泛的应用，常见的射频技术有：Wi-Fi、蓝牙、和UWB（Ultra-Wideband，超带宽）等。
- 本章介绍了Wi-Fi定位、蓝牙定位及UWB定位技术原理及其场景化应用。

学习推荐

- 华为智简园区室内无线定位解决方案
  - https://e.huawei.com/cn/material/bookshelf/bookshelfview/202003/11212222

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

构建IPv6 WLAN网络

HUAWEI

前言

- 全球可供分配的IPv4（Internet Protocol Version 4）地址已经枯竭，所有的运营商不能再申请到公网的IPv4地址池。已经申请到的IPv4公网地址大部分已使用，剩余的IPv4地址无法满足移动互联网、工业互联网、物联网业务场景的诉求。
- IPv6（Internet Protocol Version 6）也被称为IPng（IP Next Generation）。它是Internet工程任务组IETF（Internet Engineering Task Force）设计的一套规范，是IPv4的升级版本。
- 全球网络向IPv6演进，IPv4被IPv6取代是不可逆转的趋势，而园区网络在IPv6演进大潮中首当其中。
- 本课程主要讲述IPv6基本概述、基于IPv6的WLAN组网及应用、基于IPv6的WLAN网络准入控制、IPv6中的WLAN安全、以及WLAN网络的IPv6演进。

目标

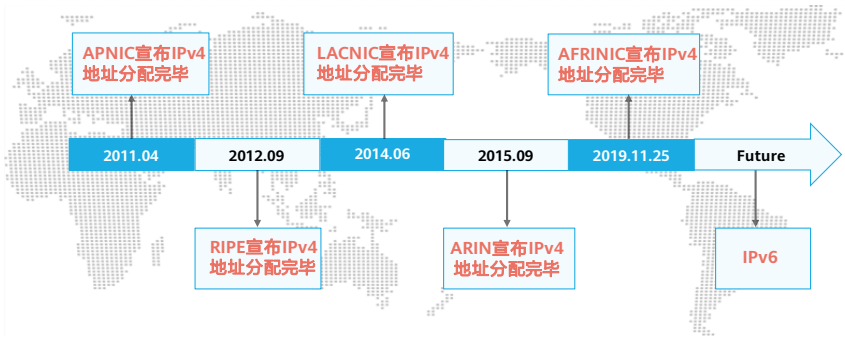
- 学完本课程后，您将能够：
  - 描述IPv6的基本概念
  - 描述基于IPv6的WLAN组网及常见应用
  - 描述基于IPv6的网络准入控制及其工作机制
  - 描述基于基于IPv6的WLAN网络安全技术
  - 归纳WLAN网络中的IPv6演进方案

目录

概述 地址 报文 路由 过滤

IPv4现状

- 2011年2月3日，IANA（Internet Assigned Numbers Authority，因特网地址分配组织）宣布将其最后的468万个IPv4地址平均分配到全球5个RIR（Regional Internet Registry，区域互联网注册管理机构），此后IANA再没有可分配的IPv4地址。



HUAWEI

- IANA，是负责全球互联网IP地址编号分配的机构。IANA将部分IPv4地址分配给大洲级的RIR，再由各RIR进行所辖区域内地址分配，五大RIR包括：
  - RIPE：Reseaux IP Europeans，欧洲IP地址注册中心，服务于欧洲、中东地区和中亚地区；
  - LACNIC：Latin American and Caribbean Internet Address Registry，拉丁美洲和加勒比海Internet地址注册中心，服务于中美、南美以及加勒比海地区；
  - ARIN：American Registry for Internet Numbers，美国Internet编号注册中心，服务于北美地区和部分加勒比海地区；
  - AFRINIC：Africa Network Information Centre，非洲网络信息中心，服务于非洲地区；
  - APNIC：Asia Pacific Network Information Centre，亚太互联网络信息中心，服务于亚洲和太平洋地区。
- 实践证明IPv4是一个非常成功的协议，它本身也经受住了Internet从少量计算机组网发展到目前上亿台计算机互联的考验。但该协议是几十年前基于当时的网络规模而设计的。在今天看来，IPv4的设计者们对于Internet的估计和预想显得很不充分。随着Internet的扩张和新应用的不断推出，IPv4越来越显示出它的局限性。
- Internet规模的快速扩张是当时完全没有预料到的，特别是近十年来，更是爆炸式增长，已经走进了千家万户，人们的日常生活已经离不开它，但正因为发展太快，IP地址空间耗尽的问题迫在眉睫。
- 20世纪90年代，IETF推出NAT（Network Address Translation，网络地址转换）与CIDR（Classless Inter Domain Routing，无类别域间路由）等技术来推迟IPv4地址耗尽发生的时间点。但是这些过渡方案只能减缓地址枯竭的速度，并不能从根本上解决问题。

概述 地址 报文 路由 过滤

IPv6的优势

“无限”地址空间	地址长度为128bit，海量的地址空间，满足物联网等新兴业务、有利于业务演进及扩展。
层次化的地址结构	相较于IPv4地址，IPv6地址的分配更加规范，利于路由聚合（缩减IPv6路由表规模）、路由快速查询。
即插即用	IPv6支持无状态地址自动配置（SLAAC），终端接入更简单。
简化的报文头部	简化报文头，提高效率；通过扩展包头支持新应用，利于路由器等网络设备的转发处理，降低投资成本。
安全特性	IPSec、真实源地址认证等保证端到端安全；避免NAT破坏端到端通信的完整性。
移动性	对移动网络实时通信有较大改进，整个移动网络性能有比较大的提升。
增强的QoS特性	额外定义了流标签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源。

HUAWEI

- 近乎无限的地址空间：与IPv4相比，这是最明显的好处。IPv6地址是由128 bit构成，单从数量级来说，IPv6所拥有的地址容量是IPv4的约8×10^{28}倍，号称可以为全世界的每一粒沙分配一个网络地址。这使得海量终端同时在线，统一编址管理，变为可能，为万物互连提供了强有力的支撑。
- 层次化的地址结构：正因为有了近乎无限的地址空间，IPv6在地址规划时就根据使用场景划分了各种地址段。同时严格要求单播IPv6地址段的连续性，便于IPv6路由聚合，缩小IPv6地址表规模。
- 即插即用：任何主机或者终端要获取网络资源，传输数据，都必须有明确的IP地址。传统的分配IP地址方式是手工或者DHCP自动获取，除了上述两个方式外，IPv6还支持SLAAC（Stateless Address Autoconfiguration，无状态地址自动配置）。
- 端到端网络的完整性：大面积使用NAT技术的IPv4网络，从根本上破坏了端到端连接的完整性。使用IPv6之后，将不再需要NAT网络设备，上网行为管理、网络监管等将变得简单，与此同时，应用程序也不需要开发复杂的NAT适配代码。
- 安全性得到增强：IPsec（Internet Protocol Security，因特网协议安全协议）最初是为IPv6设计的，所以基于IPv6的各种协议报文（路由协议、邻居发现等），都可以端到端地加密，当然该功能目前应用并不多。而IPv6的数据面报文安全性，跟IPv4+IPsec的能力，基本相同。
- 可扩展性强：IPv6的扩展属性报文头部，并不是主数据包的一部分，但是在必要的时候，这些扩展头部会插在IPv6基本头部和有效载荷之间，能够协助IPv6完成加密功能、移动功能、最优路径选路、QoS等，并可提高报文转发效率。
- 移动性改善：当一个用户从一个网段移动到另外一个网段，传统的网络会产生经典式“三角式路由”，IPv6网络中，这种移动设备的通信，可不再经过原“三角式路由”，而做直接路由转发，降低了流量转发的成本，提升了网络性能和可靠性。
- QoS可得到进一步增强：IPv6保留了IPv4所有的QoS属性，额外定义了20Byte的流标

签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源，目前该机制并没有得到充分的开发和应用。

IPv6地址表示

- IPv6地址的长度为128bit，一般用冒号分割为8段，每一段16bit，每一段内用十六进制表示，字母不区分大小写。

16bit		16bit		16bit		16bit		16bit		16bit		16bit		16bit
2001	:	0DB8	:	0000	:	0000	:	0008	:	0800	:	200C	:	417A

- IPv6地址可以分为如下两部分：
  - 前缀：n比特，相当于v4地址中的网络ID。
  - 接口标识：128-n比特，相当于v4地址中的主机ID。
  - 与IPv4地址类似，IPv6也用“IPv6地址/掩码长度”的方式来表示IPv6地址。
  - IPv6地址：2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64。

网络前缀	接口标识
2001:0db8:6101:0001:	**5ed9:98ff:feca:a298**

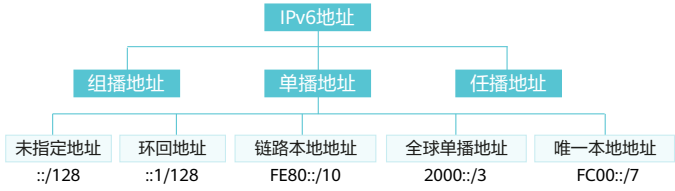
IPv6地址格式

- 首选格式
  - 冒号分割为8段，每一段16bit，每一段内用十六进制表示。
  - 用“IPv6地址/掩码长度”的方式来表示。
  - 例如：2001:0DB8:0000:0001:0000:0000:0000:45ff/64。
- 压缩格式
  - 每段前导0可以省略，但是如果该段为全0，则至少保留一个“0”字符；拖尾的0不能被省略。
  - 一个或多个连续的段为全0时，可用“::”表示，整个IPv6地址缩写中只允许有一个“::”。
  - 例如：2001:DB8:0:1::45ff/64。
- 内嵌IPv4地址的格式
  - 地址的前96bit为IPv6地址格式，后32bit为IPv4地址格式。
  - IPv6部分可采用首选或压缩格式，IPv4部分采用点分十进制格式。
  - 例如：0:0:0:0:0:0:166.168.1.2/64。

概述 地址 报文 路由 过滤

IPv6地址分类

- IPv6地址分为单播地址、任播地址（Anycast Address）、组播地址三种类型。和IPv4相比，取消了广播地址类型，以更丰富的组播地址代替，同时增加了任播地址类型。



- **单播地址（Unicast Address）：** 标识一个接口，目的为单播地址的报文会被送到被标识的接口。
- **组播地址（Multicast Address）：** 标识多个接口，目的为组播地址的报文会被送到被标识的所有接口。
- **任播地址（Anycast Address）：** 标识多个接口，目的为任播地址的报文会被送到最近的一个被标识接口，最近节点是由路由协议来定义的。

HUAWEI

- IPv6单播地址：IPv6单播地址标识了一个接口，由于每个接口属于一个节点，因此每个节点的任何接口上的单播地址都可以标识这个节点。发往单播地址的报文，由此地址标识的接口接收。IPv6定义了多种单播地址，目前常用的单播地址有：未指定地址、环回地址、全球单播地址、链路本地地址、唯一本地地址ULA（Unique Local Address）。
  - 未指定地址：IPv6中的未指定地址即0:0:0:0:0:0:0:0/128或者::/128。该地址可以表示某个接口或者节点还没有IP地址，可以作为某些报文的源IP地址（例如在NS报文的重复地址检测中会出现）。源IP地址是::的报文不会被路由设备转发。
  - 环回地址：IPv6中的环回地址即0:0:0:0:0:0:0:1/128或者::1/128。环回与IPv4中的127.0.0.1作用相同，主要用于设备给自己发送报文。该地址通常用来作为一个虚接口的地址（如Loopback接口）。实际发送的数据包中不能使用环回地址作为源IP地址或者目的IP地址。
  - 全球单播地址：全球单播地址是带有全球单播前缀的IPv6地址，其作用类似于IPv4中的公网地址。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。全球单播地址由全球路由前缀（Global routing prefix）、子网ID（Subnet ID）和接口标识（Interface ID）组成。
  - 链路本地地址：链路本地地址是IPv6中的应用范围受限制的地址类型，只能在连接到同一本地链路的节点之间使用。它使用了特定的本地链路前缀FE80::/10（最高10位值为1111111010），同时将接口标识添加在后面作为地址的低64比特。当一个节点启动IPv6协议栈时，启动时节点的每个接口会自动配置一个链路本地地址（其固定的前缀+EUI-64规则形成的接口标识）。这种机制使得两个连接到同一链路的IPv6节点不需要做任何配置就可以通信。所以链路本地地址广泛应用于邻居发现，无状态地址配置等应用。

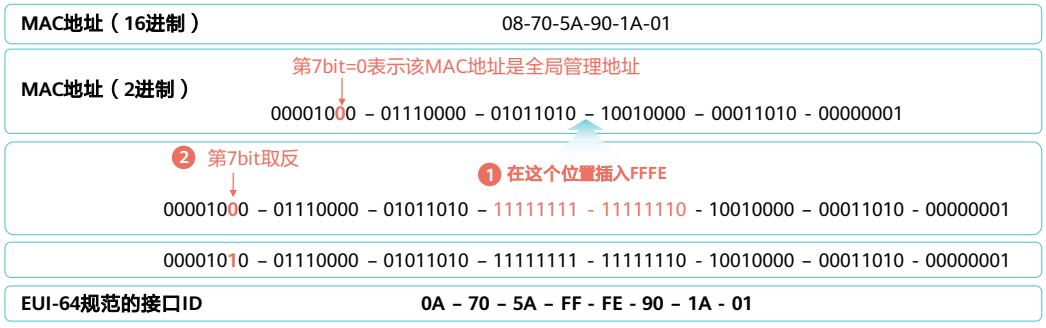
    - 唯一本地地址：唯一本地地址是另一种应用范围受限的地址，它仅能在一个站点内使用。由于本地站点地址的废除（RFC3879），唯一本地地址被用来代替本地站点地址。
      唯一本地地址的作用类似于IPv4中的私网地址，任何没有申请到提供商分配的全球单播地址的组织机构都可以使用唯一本地地址。唯一本地地址只能在本地网络内部被路由转发而不会在全球网络中被路由转发。

- IPv6组播地址：IPv6的组播与IPv4相同，用来标识一组接口，一般这些接口属于不同的节点。一个节点可能属于0到多个组播组。发往组播地址的报文被组播地址标识的所有接口接收。例如组播地址FF02::1表示链路本地范围的所有节点，组播地址FF02::2表示链路本地范围的所有路由器。
- IPv6任播地址：任播地址标识一组网络接口（通常属于不同的节点）。目标地址是任播地址的数据包将发送给其中路由意义上最近的一个网络接口。

概述 地址 报文 路由 过滤

IPv6地址接口标识

- 接口ID可通过三种方式生成：手工配置、系统自动生成，或基于IEEE EUI-64规范生成。
- 其中，基于IEEE EUI-64规范自动生成接口ID的方式最为常用，其将MAC地址转换为IPv6接口标识。



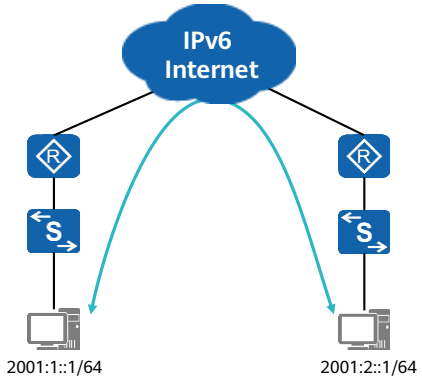
HUAWEI

- 目前有三种方式可以产生IPv6接口ID：
  - IEEE EUI-64规范
    - 接口ID的典型长度是64位，IEEE EUI-64规范给出了一个由48位MAC地址自动生成64位Interface ID的方法。
    - 具体的转换算法为：将上述的第7bit0转换为1，在MAC地址的中间（24bit处）插入两个字节：FFFE。
    - 这种由MAC地址产生IPv6地址接口ID的方法可以减少配置的工作量，只需要获取一个IPv6前缀就可以与接口ID形成IPv6地址。
    - 使用这种方式最大的缺点就是某些恶意者可以通过二层MAC推算出三层IPv6地址。
  - 设备随机生成
    - 设备采用随机生成的方法产生一个接口ID，目前Windows操作系统使用该方式。
  - 手动配置
    - 顾名思义，手动配置就是人为指定接口ID来实现。

常见单播地址 - GUA

- GUA（Global Unicast Address，全球单播地址），也被称为可聚合全球单播地址。该类地址全球唯一，用于需要有互联网访问需求的主机，相当于IPv4的公网地址。

- 全局路由前缀：由提供商指定给一个组织机构，一般至少为48bit。
- 子网ID：组织机构根据自身网络需求划分子网。
- 接口标识：用来标识一个设备的接口。



HUAWEI

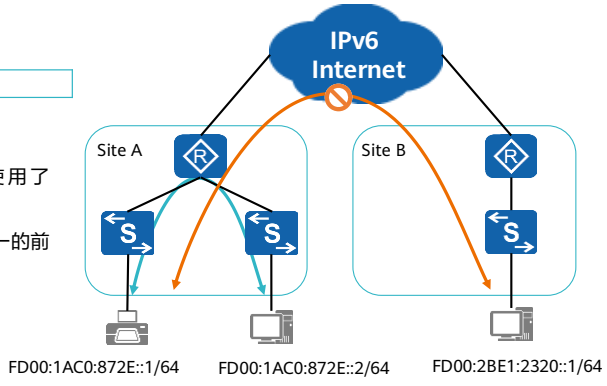
- 可以向运营商申请GUA或者直接向所在地区的IPv6地址管理机构申请。

常见单播地址 - ULA

- ULA（Unique Local Address，唯一本地地址）是IPv6私网地址，只能够在内网中使用。该地址空间在IPv6公网中不可被路由，因此不能直接访问公网。

8bit	40bit	16bit	64bit
1111 1101	Global ID	子网ID	接口标识
	随机产生		

- 唯一本地地址使用FC00::/7地址块，目前仅使用了FD00::/8地址段。FC00::/8预留为以后拓展用。
- ULA虽然只在有限范围内有效，但也具有全球唯一的前缀（虽然随机方式产生，但是冲突概率很低）。

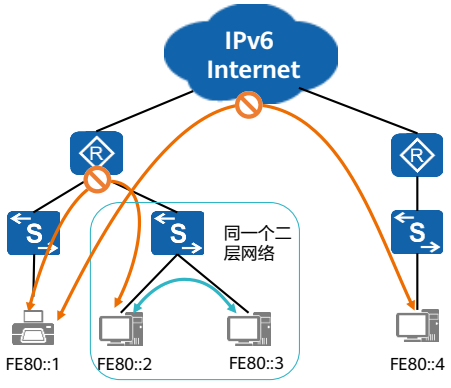


常见单播地址 - LLA

- LLA（Link-Local Address，链路本地地址）是IPv6中另一种应用范围受限制的地址类型。LLA的有效范围是本地链路，前缀为FE80::/10。

10bit	54bit	64bit
1111 1110 10	0	接口标识
	固定为0	

- LLA用于一条单一链路层面的通信，例如IPv6地址无状态自动配置、IPv6邻居发现等。
- 源或目的IPv6地址为链路本地地址的数据包将不会被转发到始发的链路之外，换句话说，链路本地地址的有效范围为本地链路。
- 每一个IPv6接口都必须具备一个链路本地地址。华为设备支持自动生成和手工指定两种配置方式。



IPv6地址和IPv4地址比较

	IPv4	IPv6
地址空间	2^{32}	2^{128}
表示方式	点分十进制	冒号隔开的十六进制
地址类型	单播、组播、广播	单播、组播、任播
其它	A、B、C等主类地址	IPv6中无此概念
	组播地址（224.0.0.0/4）	IPv6组播地址（FF00::/8）
	广播地址	IPv6中无此概念
	未指定的地址0.0.0.0/32	未指定的地址::/128
	环回地址127.0.0.0/8	环回地址是::1/128
	公网IP地址	全球单播地址
	私网IP地址（10.0.0.0/8，172.16.0.0/12以及192.168.0.0/16）	唯一本地地址（FD00::/8）
	APIPA地址（169.254.0.0/16）	链路本地地址（FE80::/10）

IPv6地址分配

- IPv6协议具有地址空间巨大的特点，但同时长达128比特的IPv6地址又要求高效合理的地址自动分配和管理策略。
- 目前IPv6地址的分配方法有以下几种：
  - 手动配置。手动配置IPv6地址/前缀及其他网络配置参数（DNS、NIS、SNTP服务器地址等参数）。
  - 无状态自动地址分配。由接口ID生成链路本地地址，再根据路由通告报文RA（Router Advertisement）包含的前缀信息自动配置本机地址。
  - 有状态自动地址分配，即DHCPv6方式。DHCPv6又分为如下两种：
    - DHCPv6有状态自动分配。DHCPv6服务器自动分配IPv6地址/PD前缀及其他网络配置参数（DNS、NIS、SNTP服务器地址等参数）。
    - DHCPv6无状态自动分配。主机IPv6地址仍然通过路由通告方式自动生成，DHCPv6服务器只分配除IPv6地址以外的配置参数，包括DNS、NIS、SNTP服务器等参数。

IPv6地址手动配置

- 使能设备转发IPv6单播报文的能力。

```
[WAC] ipv6
```

- 使能接口转发IPv6单播报文的能力。

```
[WAC] interface vlanif 200
[WAC-Vlanif200] ipv6 enable
```

- 自动配置接口的链路本地地址。

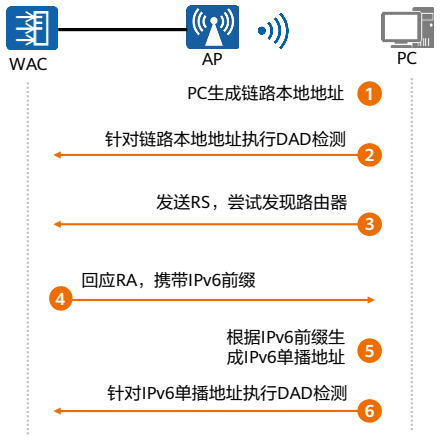
```
[WAC-Vlanif200] ipv6 address auto link-local
```

- 手工配置接口的全球单播地址。

```
[WAC-Vlanif200] ipv6 address 2001:DB8:13::1 64
```

概述 地址 报文 路由 过滤

IPv6无状态地址自动配置



1. PC根据本地接口ID自动生成IPv6链路本地地址。
2. PC对该IPv6链路本地地址进行DAD检测，如果该地址无冲突则将其启用。
3. PC以IPv6链路本地地址为源发送RS报文，尝试在链路上发现IPv6路由器。
4. WAC发送RA报文（携带可用于无状态地址自动配置的IPv6地址前缀。WAC在没有收到RS报文时也能够主动发出RA报文）。
5. PC解析WAC发送的RA报文，获得IPv6地址前缀，使用该前缀加上本地的接口ID生成IPv6单播地址。
6. PC对生成的IPv6单播地址进行DAD检测，如果没有检测到冲突，则启用该地址。

HUAWEI

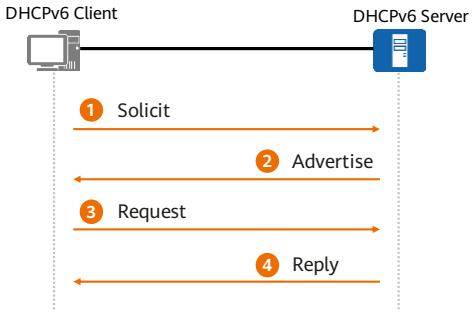
- 重复地址检测DAD（Duplicate Address Detect）是在接口使用某个IPv6单播地址之前进行的，主要是为了探测是否有其它的节点使用了该地址。尤其是在地址自动配置的时候，进行DAD检测是很必要的。一个IPv6单播地址在分配给一个接口之后且通过重复地址检测之前称为试验地址（Tentative Address）。此时该接口不能使用这个试验地址进行单播通信。
- 路由器通告RA（Router Advertisement）报文：每台路由器（含IPv6 WAC）为了让二层网络上的主机和设备知道自己的存在，都会定时发送组播的RA报文，RA报文中会带有网络前缀信息。
- 路由器请求RS（Router Solicitation）报文：很多情况下主机接入网络后希望尽快获取网络前缀进行通信，此时主机可以立刻发送RS报文，网络上的设备将回应RA报文。

动态主机配置协议DHCPv6

- DHCPv6的定义：
  - DHCPv6（Dynamic Host Configuration Protocol for IPv6，IPv6动态主机配置协议）是一种运行在客户端和服务器之间的协议，与IPv4中的DHCP一样，所有的协议报文都是基于UDP的。DHCPv6可为IPv6主机分配IPv6地址/前缀和其他网络配置参数。
- DHCPv6的优点：
  - 更好地控制IPv6地址的分配。DHCPv6方式不仅可以记录为IPv6主机分配的地址，还可以为特定的IPv6主机分配特定的地址，便于网络管理。
  - DHCPv6支持为网络设备分配IPv6前缀，便于全网络的自动配置和层次化管理。
  - 除了为IPv6主机分配IPv6地址/前缀外，还可以分配DNS服务器IPv6地址等网络配置参数。

DHCPv6有状态自动分配 - 四步交互

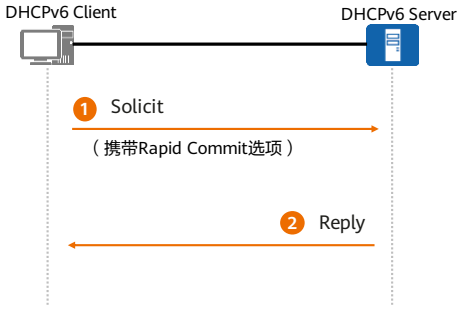
- 四步交互是指DHCPv6客户端与服务器交互四次来完成前缀/地址等参数获取的过程。



1. DHCPv6客户端发送Solicit消息，请求DHCPv6服务器为其分配IPv6地址/前缀和网络配置参数。
2. DHCPv6服务器回复Advertise消息，通知客户端可以为其分配的地址/前缀和网络配置参数。
3. 如果DHCPv6客户端接收到多个服务器回复的Advertise消息，则根据消息接收的先后顺序、服务器优先级等，选择其中一台服务器，并向该服务器发送Request消息，请求服务器确认为其分配地址/前缀和网络配置参数。
4. DHCPv6服务器回复Reply消息，确认将地址/前缀和网络配置参数分配给客户端使用。

DHCPv6有状态自动分配 - 两步交互

- DHCPv6客户端可以在发送的Solicit消息中携带Rapid Commit选项，表示客户端希望服务器能够快速为其分配地址/前缀和网络配置参数。



1. DHCPv6客户端发送Solicit报文，携带Rapid Commit选项。
2. DHCPv6服务器接收到Solicit报文后，如果其支持快速分配，则直接回复Reply报文，为客户端分配IPv6地址/前缀和其他网络配置参数；如果不支持快速分配，则将采用四步交互方式。

DHCPv6无状态自动分配

- DHCPv6服务器为已经具有IPv6地址/前缀的客户端分配除地址/前缀以外的其他网络配置参数，该过程称为DHCPv6无状态自动配置。

1. DHCPv6客户端以组播的方式向DHCPv6服务器发送Information-request报文，该报文中携带Option Request选项，指定客户端需要从服务器获取的配置参数。
2. 服务器收到该报文后，为客户端分配网络配置参数，并单播发送Reply报文将网络配置参数返回给客户端。客户端检查Reply报文中提供的信息，如果与Information-request报文中请求的配置参数相符，则按照Reply报文中提供的参数进行网络配置；否则，忽略该参数。

DHCPv6配置命令介绍（1）

- 为设备开启DHCP服务。

  [WAC] **dhcp enable**

- 创建IPv6地址池。

  [WAC] **dhcpv6 pool** *pool-name*

- 在IPv6地址池视图下配置网络前缀。

  [WAC-dhcpv6-pool-ap_pool] **address prefix** *ipv6-prefix/ipv6-prefix-length*

- 使能接口发布RA报文功能。
- 默认情况下，华为设备接口抑制ICMPv6 RA报文的发送。此时，本网络的主机将不会定期收到更新IPv6地址前缀的信息。若需要周期性的向主机发布RA报文中的IPv6地址前缀和有状态自动配置标志位的信息时，使用undo ipv6 nd ra halt命令使能系统发布RA报文的功能。

  [WAC-Vlanif200] **undo ipv6 nd ra halt**

- 配置在接口下使能DHCPv6服务器功能。

  [WAC-Vlanif200] **dhcpv6 server** *pool-name*

DHCPv6配置命令介绍（2）

- 配置RA报文中的有状态自动配置地址的标志位：
  - 如果设置了该标志位，则主机通过有状态自动配置获得IPv6地址。
  - 如果清除了该标志位，则主机通过无状态自动配置获得IPv6地址，即通过RA报文向主机发布IPv6地址前缀信息自动生成IPv6地址。

```
[WAC-Vlanif200] ipv6 nd autoconfig managed-address-flag
```

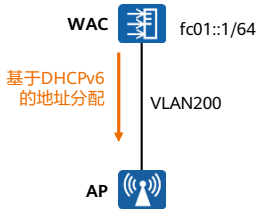
- 配置RA报文中的有状态自动配置其他信息的标志位：
  - 如果设置了该标志位，则主机可通过有状态自动配置获得除IPv6地址外的其他配置信息，包括路由器生存时间、邻居可达时间、邻居的重传时间、链路的MTU信息。
  - 如果清除了该标志位，则主机进行无状态自动配置。即路由设备通过RA报文向主机发布除IPv6地址外的其他配置信息，包括路由器生存时间、邻居可达时间、邻居的重传时间、链路的MTU信息。

```
[WAC-Vlanif200] ipv6 nd autoconfig other-flag
```

- 查看IPv6接口信息：

```
[WAC] display ipv6 interface [ interface-type interface-number | brief ]
```

DHCPv6配置举例



在WAC上完成接口IPv6地址配置及DHCPv6服务配置，使得AP能够通过DHCPv6获得IPv6地址。

在WAC上使能IPv6并配置IPv6地址。

```
[WAC] ipv6
[WAC] interface vlanif 200
[WAC-Vlanif200] ipv6 enable
[WAC-Vlanif200] ipv6 address auto link-local
[WAC-Vlanif200] ipv6 address fc01::1/64
```

在WAC上配置DHCPv6服务，并在接口使能该服务。

```
[WAC] dhcp enable
[WAC] dhcpv6 pool ap_pool
[WAC-dhcpv6-pool-ap_pool] address prefix fc01::/64

[WAC] interface vlanif 200
[WAC-Vlanif200] undo ipv6 nd ra halt
[WAC-Vlanif200] ipv6 nd autoconfig managed-address-flag
[WAC-Vlanif200] ipv6 nd autoconfig other-flag
[WAC-Vlanif200] dhcpv6 server ap_pool
```

AP通过DHCPv6方式获取IPv6地址，查看AP地址。

```
[AP] display ipv6 interface brief
......
Interface                  Physical        Protocol
Vlanif1                    up              up
[IPv6 Address] FC01::9
```

IPv6报文构成

- IPv6报文一般由三个部分组成：

IPv6基本报头	IPv6扩展报头	上层协议数据单元

  - 基本报头：提供报文转发的基本信息，路由器通过解析基本报头就能完成绝大多数的报文转发任务。
  - 扩展报头：提供一些扩展的报文转发信息，如分段、加密等，该部分不是必需的，也不是每个路由器都需要处理，仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展头。
  - 上层协议数据单元：一般由上层协议报头和它的有效载荷构成，该部分与IPv4的上层协议数据单元相似。

- IPv6基本报头（IPv6 Header）
  - 每一个IPv6数据报文都必须包含报头，其长度固定为40字节。
  - 基本报头提供报文转发的基本信息，会被转发路径上的所有路由器解析。
- 扩展报头（Extension Headers）
  - IPv6扩展报头是可能跟在基本IPv6报头后面的可选报头。IPv6数据包中可以包含一个或多个扩展报头，当然也可以没有扩展头，这些扩展报头可以具有不同的长度。IPv6报头和扩展报头代替了IPv4报头及其选项。新的扩展报头格式增强了IPv6的功能，使其具有极大的扩展性。与IPv4报头中的选项不同，IPv6扩展报头没有最大长度的限制，因此可以容纳IPv6通信所需要的所有扩展数据。扩展报头提供报文转发的扩展信息，并不会被路径上所有的路由器解析，一般只会被目的路由器解析处理。
- 上层协议数据单元（Upper Layer Protocol Data Unit）
  - 上层协议数据单元一般由上层协议报头和它的有效载荷构成，有效载荷可以是一个ICMPv6报文、一个TCP报文或一个UDP报文。

概述 地址 报文 路由 过滤

IPv6和IPv4报文比较

IPv4报头（20Byte ~ 60Byte）

Version	~~IHL~~	ToS	Total Length
~~Identification~~		~~Flags~~	~~Fragment Offset~~
TTL	Protocol	~~Header Checksum~~	
Source address			
Destination address			
~~Options~~			~~Padding~~

IPv6基本报头（40Byte）

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source address		
Destination address		

IPv6头部相较于IPv4的改进

- **取消三层校验：**协议栈中二层和四层的已提供校验，因此IPv6直接取消了IP的三层校验，节省路由器处理资源。
- **取消中间节点的分片功能：**中间路由器不再处理分片，只在产生数据的源节点处理，省却中间路由器为处理分片而耗费的大量CPU资源。
- **定义定长的IPv6报头：**有利于硬件的快速处理，提高路由器转发效率。
- **安全选项的支持：**IPv6提供了对IPSec的完美支持，如此上层协议可以省去许多安全选项。
- **增加流标签：**提高QoS效率。

保留的字段 ~~取消的字段~~ 名字/位置变化 新增字段

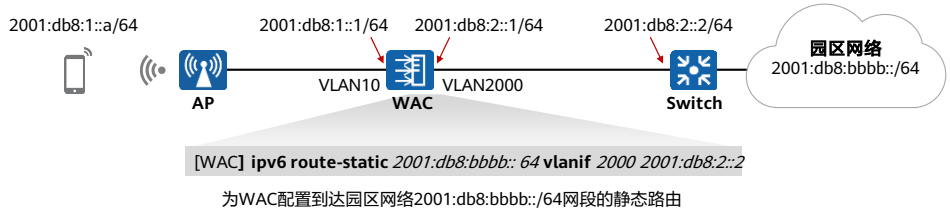
HUAWEI

- IPv6基本报头也称之为固定报头。固定报头包含8个字段，总长度为40Byte。这8个字段分别为：版本（Version）、流量类型（Traffic Class）、流标签（Flow Label）、净荷长度（Payload Length）、下一个报头（Next Header）、跳数限制（Hop Limit）、源IPv6地址、目的IPv6地址。
- 版本（Version）
  - 该字段规定了IP协议的版本，其值为6。长度为4bit。
- 流类别（Traffic Class）
  - 该字段功能和IPv4中的服务类型功能类似，表示IPv6数据报文的类或优先级。长度为8bit。
- 流标签（Flow Label）
  - 与IPv4相比，该字段是新增的。它用来标识这个数据报属于源节点和目标节点之间的一个特定数据报序列，它需要由中间IPv6路由器进行特殊处理。该字段长度为20bit。一般来说一个流可以通过源/目的IPv6地址和流标签来确定。
- 有效载荷长度（Payload Length）
  - 该字段表示IPv6数据报有效载荷的长度。有效载荷是指紧跟IPv6报头的数据报的其它部分（即扩展报头和上层协议数据单元）。该字段长度为16bit，能表示最大长度为65535Byte的有效载荷。如果有效载荷的长度超过这个值，该字段会置0，而有效载荷的长度用逐跳选项扩展报头中的超大有效载荷选项来表示。

- 下一个报头（Next Header）
  - 该字段定义紧跟在IPv6报头后面的第一个扩展报头（如果存在）的类型，或者上层协议数据单元中的协议类型。该字段长度为8bit。
- 跳数限制（Hop Limit）
  - 该字段类似于IPv4中的TTL（Time to Live）字段。它定义了IP数据报所能经过的最大跳数。每经过一个路由器，该数值减去1，当该字段的值为0时，数据报将被丢弃。该字段长度为8bit。
- 源地址（Source Address）
  - 表示发送方的地址，长度为128bit。
- 目的地址（Destination Address）
  - 表示接收方的地址，长度为128bit。

IPv6单播路由：静态路由

- 路由器根据路由转发数据包，路由可通过手动配置和使用动态路由算法计算产生，其中手动配置产生的路由就是静态路由。
- 静态路由比动态路由使用更少的带宽，并且不占用CPU资源来计算和分析路由更新。但是当网络发生故障或者拓扑发生变化后，静态路由不会自动更新，必须手动重新配置。静态路由有5个主要的参数：目的地址和掩码、出接口和下一跳、优先级。



为WAC配置到达园区网络2001:db8:bbbb::/64网段的静态路由

HUAWEI

- 在创建静态路由时，可以同时指定出接口和下一跳。
  - 对于不同的出接口类型，也可以只指定出接口或只指定下一跳。对于点到点接口，指定出接口。
  - 对于NBMA（Non Broadcast Multiple Access）接口，指定下一跳。
  - 对于广播类型接口，指定出接口。如果也指定下一跳，下一跳地址可以不是链路本地地址。
- 在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。
- 在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是IPv6静态缺省路由。缺省情况下，没有创建IPv6静态缺省路由。
- 配置静态路由时应注意以下几点：
  - 静态路由如果不配置优先级，默认优先级为60。
  - 如果将目的地址与掩码都配置为全0，则表示配置的是缺省路由。

IPv6单播路由协议简介

OSPFv3	IS-IS for IPv6	BGP4+
1. 基于链路运行，单链路支持多实例。 2. 取消LSA头部IP地址信息，实现与网络层协议解耦。 3. LSA内新定义泛洪范围字段，支持未知LSA的处理。 4. 新增LSA支持IPv6路由发布。	1. 不是新协议或新版本，仅是原有协议上做了简单扩展，IS-IS路由器和IS-IS路由器可以实现互通。 2. 新增1种NLPID（网络层协议标识）宣告自身支持IPv6。 3. 新增2种TLV，支持宣告IPv6网络可达性和接口IPv6地址信息。	1. 不是新协议或新版本，只需在MP-BGP（BGP多协议）架构上支持IPv6地址族，BGP4+路由器和BGP4路由器可以实现互通。 2. 新添2种NLRI（网络层可达信息），支持发布IPv6可达路由及下一跳信息，支持撤销不可达路由。

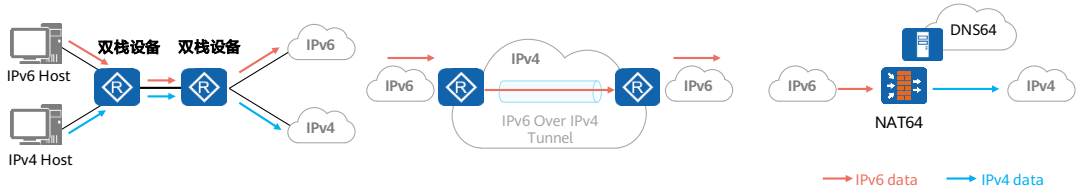
版本未变，简单扩展

IPv6过渡技术简介（1）

- 由于NAT技术的应用，缓解了IPv4地址不足产生的问题，但是部署IPv6是解决IPv4地址不足的最终方案。当前世界上不同地区对部署IPv6的需求强烈程度不一，且当前IPv4网络仍然占主流地位，因此短时间内IPv6和IPv4将会共存。
- IPv4网络演变为IPv6网络主要有以下三种技术：
  - 双栈技术：在一台设备上同时启用IPv4协议栈和IPv6协议栈的技术。
  - 隧道技术：将一种协议的数据封装在另一种协议中的技术。
  - 转换技术：将IPv6地址和IPv4地址进行转换的一种技术。
- 没有最好的过渡技术方案，没有任何一种技术方案能够解决所有问题，通常是多种技术组合成不同的过渡方案，满足不同的网络场景。

IPv6过渡技术简介（2）

IPv4/IPv6双栈	隧道技术	转换技术
• 设备支持IPv4/IPv6，IPv4及IPv6独立部署，在一段时间内并存。对现有IPv4业务影响较小。 • 演进方案相对简单、易理解。网络规划设计工作量相对更少。 • 现有软硬件（网络设备、终端、操作系统等）已经有很大一部分支持双栈。 • 对设备的硬件/软件有要求，设备需支持双栈。	• 将IPv4流量封装在IPv6隧道中，或者将IPv6流量封装在IPv4隧道中。 • 适用于在IPv4传输网络中实现IPv6孤岛之间的互通，或者在IPv6传输网络中实现IPv4孤岛之间的互通。 • 部署隧道技术的设备（一般是隧道端点）需支持双栈及相应的隧道技术。	• 将IPv4流量转换成IPv6，反之亦然。需在网络中部署网络层协议转换（NAT）设备、DNS设备。 • 适用于纯IPv4网络与纯IPv6网络之间的通信，反之亦然。 • 破坏了端到端连接的完整性。需针对特殊应用提供ALG功能。 • 网络管理/审计变得复杂。



目录

IPv6 WLAN网络总体概述

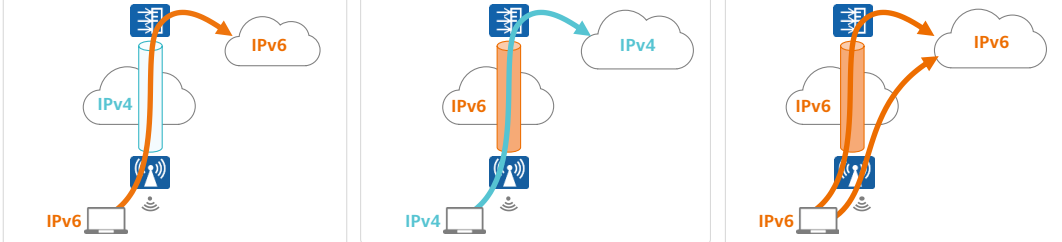
- 管理面（OSS-设备）
  - WLAN设备（WAC与AP）的WEB管理页面支持通过IPv6访问。
  - WLAN设备（WAC与AP）可通过Telnetv6及SSHv6等方式管理。
  - 支持OSS通过IPv6 SNMP管理WLAN设备（WAC与AP）。
- 控制面（WAC-AP）
  - 在典型场景中，WAC作为DHCPv6服务器为AP分配IPv6地址，AP可通过IPv6地址与WAC建立CAPWAP隧道。
- 业务面（STA业务报文）
  - 在IPv4的基础上，SSID支持IPv6终端接入，可通过部署DHCPv6实现终端地址自动配置。
  - 可针对IPv6用户部署802.1X、MAC或Portal认证提高安全性。
  - 网络出口处可部署NAT64/DNS64实现IPv6用户与IPv4网络间通信。

- OSS（Operations support systems，运营支撑系统）是网络业务开展和运营时所使用的支撑平台。在一个典型的网络中，OSS可以是网管平台，或者SDN控制器。

IPv6 WLAN组网分类

- 视基础网络（WAC与AP之间的网络）类型和无线终端的类型差异，可分解为四种组网场景：IPv6 over IPv4（典型组网）、IPv4 over IPv6、IPv6 over IPv6、IPv4 over IPv4（纯IPv4组网）。

IPv6 over IPv4	IPv4 over IPv6	IPv6 over IPv6
• 适用于基础网络是纯IPv4网络，而无线终端为IPv6终端的场景（典型组网）。 • 将IPv6流量封装在IPv4隧道中，仅适用于隧道转发。	• 适用于基础网络是纯IPv6网络，而无线终端为IPv4终端的场景。 • 将IPv4流量封装在IPv6隧道中，仅适用于隧道转发。	• 在IPv6基础网络中构建无线IPv6通信网络，即端到端IPv6场景。 • 适用于隧道转发和直接转发。

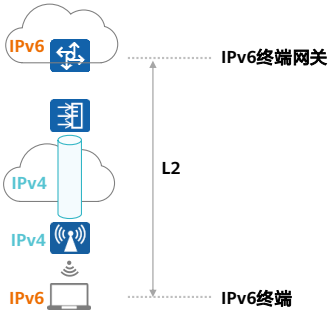


WAC的IPv6能力

- WAC全面支持IPv4/IPv6双栈，既可以作为无线IPv6用户的L3网关，也可以充当L2网桥。

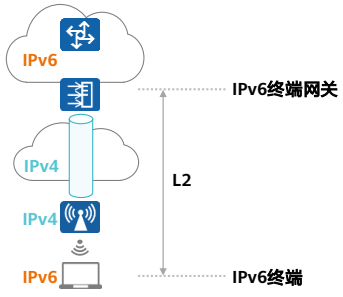
WAC作为L2网桥

WAC对于隧道中的STA报文仅做L2透传，无需支持IPv6路由功能，无需运行IPv6动态路由协议、DHCPv6等相关协议。



WAC作为IPv6终端的网关

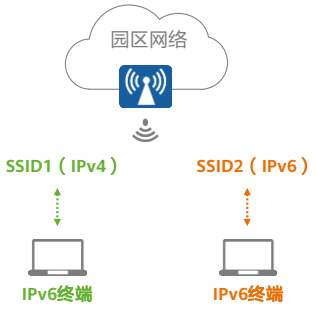
WAC作为终端的L3网关，是IPv6网络和IPv4网络的边界，此时WAC必须是IPv4/IPv6双栈设备。

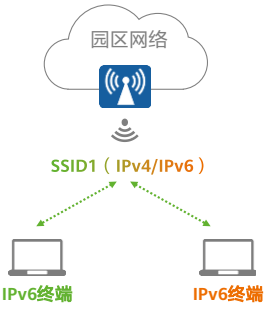


WLAN的IPv4/IPv6终端接入

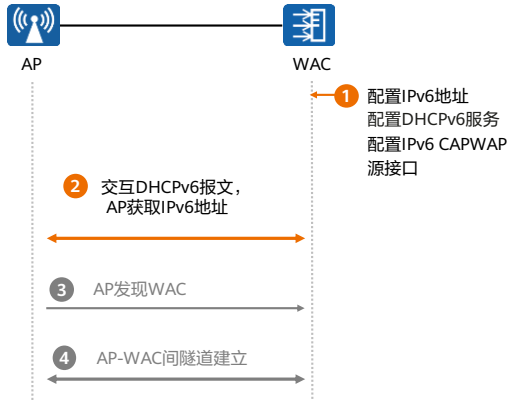
- 对于同时存在IPv4和IPv6终端的场景，有如下两种接入方案：

多SSID方案	双栈SSID方案
分别为IPv4及IPv6部署不同的SSID。	使用一个SSID同时满足IPv4及IPv6用户接入。



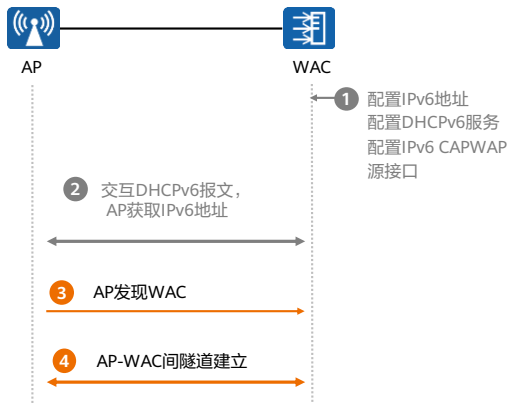


IPv6 AP上线（1）



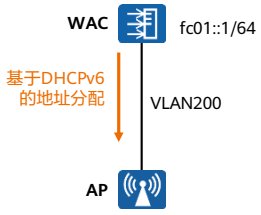
1. 在WAC上完成IPv6地址、DHCPv6服务及IPv6 CAPWAP源接口配置。
2. AP通过DHCPv6从WAC获取IPv6地址。除了DHCPv6方式，AP还可通过如下方式获取IPv6地址：
   - SLAAC方式：AP具有SLAAC功能，自动根据WAC（或其他设备）下发的IPv6前缀生成一个全局IPv6地址。
   - 静态地址方式：管理员通过Console口连接AP直接进行配置IPv6地址，或者在WAC上为AP配置静态IPv6地址，重启AP后生效。

IPv6 AP上线 (2)



3. AP发现WAC：
   - 静态方式：AP上预先配置了WAC的静态IPv6地址列表。
   - 动态方式：
     - DHCPv6方式：在DHCPv6服务器上配置响应报文中携带Option 52，且Option 52携带WAC的IP地址列表。
     - DNS方式：AP通过DHCPv6服务获取WAC的域名和DNS服务器的IPv6地址，即在DHCPv6服务器上配置响应报文中携带Option 24，且Option 24携带上述信息，AP将向DNS服务器查询WAC的域名对应的IP地址。
     - 组播方式：AP未获取到WAC地址列表，则发送目的地址为FF02::18C的组播IPv6报文——CAPWAP Discovery Request尝试发现WAC。
4. AP与WAC之间建立IPv6 CAPWAP隧道。

IPv6 AP上线配置案例



在WAC上完成接口IPv6地址配置、DHCPv6服务配置以及CAPWAP隧道源接口配置，使得AP能够通过DHCPv6获得IPv6地址，并与WAC建立隧道。

在WAC上使能IPv6并配置IPv6地址

```
[WAC] ipv6
[WAC] interface vlanif 200
[WAC-Vlanif200] ipv6 enable
[WAC-Vlanif200] ipv6 address auto link-local
[WAC-Vlanif200] ipv6 address fc01::1/64
```

在WAC上配置DHCPv6服务，并在接口使能该服务

```
[WAC] dhcp enable
[WAC] dhcpv6 pool ap_pool
[WAC-dhcpv6-pool-ap_pool] address prefix fc01::/64

[WAC] interface vlanif 200
[WAC-Vlanif200] undo ipv6 nd ra halt
[WAC-Vlanif200] ipv6 nd autoconfig managed-address-flag
[WAC-Vlanif200] ipv6 nd autoconfig other-flag
[WAC-Vlanif200] dhcpv6 server ap_pool
```

在WAC上配置IPv6 CAPWAP源接口

```
[WAC] capwap source ipv6-address fc01::1
或
[WAC] capwap source interface vlanif 200
```


- **ipv6 nd autoconfig managed-address-flag**命令用来设置RA报文中的有状态自动配置地址的标志位。如果设置了该标志位，则主机通过有状态自动配置获得IPv6地址。
- **ipv6 nd autoconfig other-flag**命令用来设置RA报文中的有状态自动配置其他信息的标志位。如果设置了该标志位，则主机可通过有状态自动配置获得除IPv6地址外的其他配置信息，包括路由器生存时间、邻居可达时间、邻居的重传时间、链路的MTU信息。
- 在本例中，WAC与AP处于相同的VLAN，AP通过发送组播CAPWAP Discovery Request报文发现WAC。

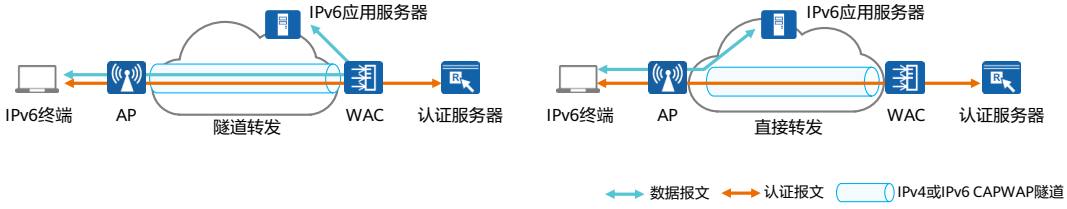
目录

IPv6用户接入认证

- 对于IPv6无线终端，支持802.1X认证、MAC认证及Portal认证。
- WAC支持IPv4/IPv6双栈，支持与IPv4或IPv6 RADIUS服务器对接。
- 根据认证类型、WLAN转发方式、CAPWAP隧道接口地址类型、服务器类型等的不同，部署场景有所不同。

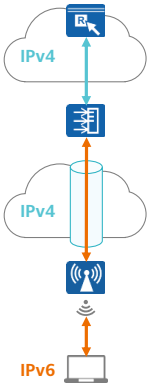
802.1X认证概述

- 802.1X是一种基于端口的网络接入控制协议（Port based network access control protocol）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级验证用户身份并控制其访问权限。
- 802.1X系统为典型的Client/Server结构，包括三个实体：客户端、接入设备和认证服务器。
- 在典型场景中，WAC作为接入设备与认证服务器（RADIUS服务器）对接，WAC可能会从RADIUS服务器获取针对IPv6终端相关的扩展选项，比如ACL授权、IPv6地址等，以便支持IPv6终端的认证、授权和计费功能。
- 在IPv6 WLAN组网中，数据转发方式将影响用户数据报文的转发行为，但无论采用何种数据转发方式，认证报文都采用隧道转发，AP将认证报文通过CAPWAP隧道送达WAC。



802.1X各场景中的认证报文交互（1）

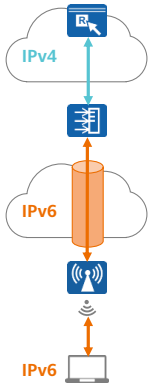
CAPWAP地址类型：IPv4；RADIUS服务器类型：IPv4



- WAC 、AP及RADIUS服务器工作在IPv4环境中。
- WAC与AP建立IPv4 CAPWAP隧道。
- 认证报文在AP与WAC之间交互，通过IPv4 CAPWAP隧道承载。
- WAC与认证服务器之间基于IPv4交互RADIUS协议报文。

IPv4报文 IPv6报文

CAPWAP地址类型：IPv6；RADIUS服务器类型：IPv4

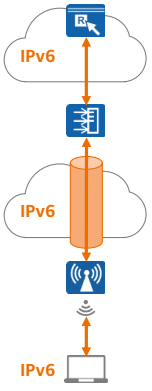


- RADIUS服务器为IPv4单栈服务器。
- WAC、AP建立IPv6 CAPWAP隧道。
- 认证报文在AP与WAC之间交互，通过IPv6 CAPWAP隧道承载。
- WAC与认证服务器之间基于IPv4交互RADIUS报文。

IPv4报文 IPv6报文

802.1X各场景中的认证报文交互（2）

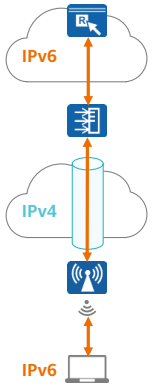
CAPWAP地址类型：IPv6；RADIUS服务器类型：IPv6



- 端到端的IPv6网络。
- WAC与AP建立IPv6 CAPWAP隧道。
- 认证报文在AP与WAC之间交互，通过IPv6 CAPWAP隧道承载。
- WAC与认证服务器之间基于IPv6交互RADIUS协议报文。

IPv4报文 IPv6报文

CAPWAP地址类型：IPv4；RADIUS服务器类型：IPv6

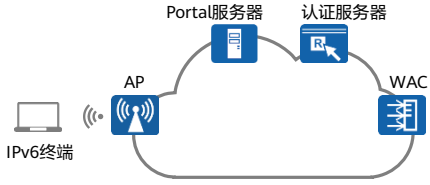


- RADIUS服务器为IPv6单栈服务器。
- WAC、AP建立IPv4 CAPWAP隧道。
- 认证报文在AP与WAC之间交互，通过IPv4 CAPWAP隧道承载。
- WAC与认证服务器之间基于IPv6交互RADIUS报文。

IPv4报文 IPv6报文

Portal认证

- Portal认证通常也称为Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源。
- Portal认证系统主要包括四个基本要素：客户端、接入设备、Portal服务器与认证服务器。
- 在典型场景中，WAC作为Portal认证的接入设备。当终端未通过认证时，其WEB访问请求将被重定向至IPv6 Portal服务器，后者推送Portal页面供终端进行认证。
- 管理员可通过配置使用户通过Portal认证前能够访问开放的资源，如DNS服务器、安全补丁服务器、Portal认证服务器等。



目录

ACL

- 访问控制列表ACL（Access Control List）是由一系列规则组成的集合，ACL通过这些规则对数据包进行分类，从而设备可以对不同类报文进行不同的处理。
- IPv6 ACL（ACL6）可实现IPv6流量的处理，其基本原理与IPv4 ACL相同。

分类	对应编号范围	应用场景
基本ACL6	编号范围为2000～2999	可以使用报文的源IP地址、分片标记和时间段信息来定义规则。
高级ACL6	编号范围为3000～3999	可以使用报文的源地址、目的地址、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口和ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。
用户ACL6	编号范围为6000～6999	可以使用报文的源地址、目的地址、目的域名、IP承载的协议类型、针对协议的特性（例如TCP的源端口、目的端口和ICMPv6协议的类型、ICMPv6 Code）等内容定义规则。

基本ACL6的配置

- （系统视图）使用编号（2000～2999）创建一个数字型的基本ACL6，并进入基本ACL6视图。

  acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

- （系统视图）使用名称创建一个命名型的基本ACL6，并进入基本ACL6视图。

  acl ipv6 name *acl6-name* { **basic** | *acl6-number* } [**match-order** { **auto** | **config** }]

- （ACL6视图）配置基本ACL6规则。

  rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }]

高级ACL6的配置

- （系统视图）使用编号（3000～3999）创建一个数字型的高级ACL6，并进入高级ACL6视图。

  acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

- （系统视图）使用名称创建一个命名型的高级ACL6，进入高级ACL6视图。

  acl ipv6 name *acl6-name* { **advance** | *acl6-number* } [**match-order** { **auto** | **config** }]

- （ACL6视图）配置高级ACL6规则。根据IP承载的协议类型不同，在设备上配置不同的高级ACL6规则。对于不同的协议类型，有不同的参数组合。当参数protocol为TCP时，高级ACL6的命令格式如下：

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }]

ACL6配置示例

- 在ACL6 2001中配置规则，允许源IPv6地址是fc00:1::1/128主机地址的报文通过。

```
[HUAWEI] acl ipv6 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:1::1 128
```

- 在ACL6 3001中配置规则，允许源IPv6地址是fc00:1::1主机地址且目的IPv6地址是fc00:2::/64网段的ICMPv6报文通过。

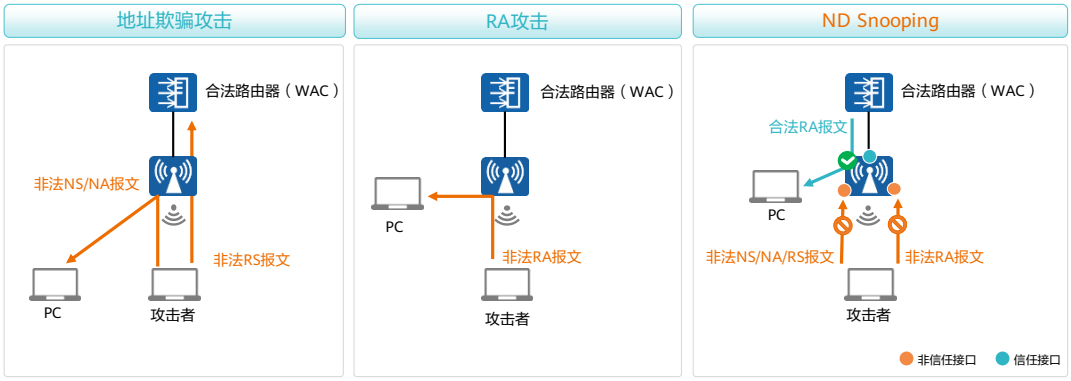
```
[HUAWEI] acl ipv6 3001
[HUAWEI-acl6-adv-3001] rule permit icmpv6 source fc00:1::1 128 destination fc00:2:: 64
```

- 在名称为no-web的高级ACL6中配置规则，禁止fc00:1::3和fc00:1::4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80）。

```
[HUAWEI] acl ipv6 name no-web
[HUAWEI-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::3 128
[HUAWEI-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::4 128
```

ND Snooping

- ND Snooping功能是通过侦听用户重复地址检测DAD过程的邻居请求报文NS建立ND Snooping动态绑定表，从而记录下报文的源IPv6地址、源MAC地址、所属VLAN、入端口等信息，以防止地址欺骗攻击、RA攻击。

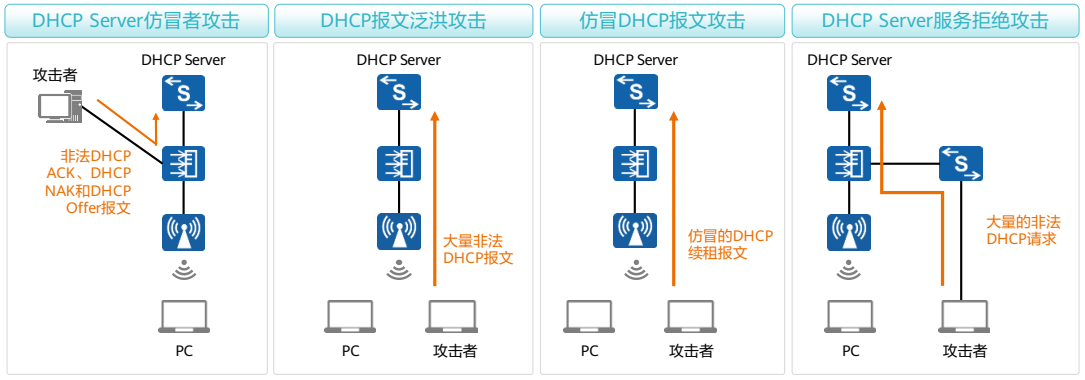


- ND协议是IPv6的一个关键协议，它功能强大，但是因为其没有任何安全机制，所以容易被攻击者利用。在网络中，常见的ND攻击有如下两种情况。
  - 地址欺骗攻击：攻击者仿冒其他用户的IP地址发送邻居请求报文NS（Neighbor Solicitation）/邻居通告报文NA（Neighbor Advertisement），会改写网关上或者其他用户的ND表项，导致被仿冒用户无法正常接收报文，从而无法正常通信。同时攻击者通过截获被仿冒用户的报文，可以非法获取用户的游戏、网银等帐号口令，会造成这些用户的重大利益损失。
  - RA攻击：攻击者仿冒网关向其他用户发送路由器通告报文RA（Router Advertisement），会改写其他用户的ND表项或导致其它用户记录错误的IPv6配置参数，造成这些用户无法正常通信。
  - 为了避免上述ND攻击带来的危害，设备提供了ND Snooping功能以对ND攻击进行防范。
- ND Snooping：
  - 在AP上部署ND Snooping，将其与合法路由器（WAC）相连的接口配置为信任接口，并在用户侧接口上使能ND协议报文合法性检查功能。
  - 对于从用户侧接口收到的NA/NS/RS报文，AP会根据生成的ND Snooping动态绑定表进行，对于非法报文将直接丢弃，从而可以避免伪造的NA/NS/RS报文带来的危害。
  - 对于从用户侧接口（默认为非信任接口）收到的RA报文进行丢弃，仅处理信任

接口收到的RA报文，从而可以避免伪造的RA报文带来的各种危害。

DHCP Snooping（1）

- DHCP Snooping是DHCP的一种安全特性，用于保证DHCP客户端从合法的DHCP服务器获取IP地址，并记录DHCP客户端IP地址与MAC地址等参数的对应关系，防止网络上针对DHCP的攻击。



HUAWEI

- DHCP Server仿冒者攻击：DHCP Server仿冒者回应给DHCP Client仿冒信息，如错误的网关地址、错误的DNS（Domain Name System）服务器、错误的IP等信息，DHCP Client将无法获取正确的IP地址和相关信息，导致合法客户无法正常访问网络或信息安全受到严重威胁。
- DHCP报文泛洪攻击：在DHCP网络环境中，若攻击者短时间内向设备发送大量的DHCP报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。
- 仿冒DHCP报文攻击：攻击者冒充合法用户不断向DHCP Server发送DHCP Request报文来续租IP地址，会导致这些到期的IP地址无法正常回收，以致一些合法用户不能获得IP地址；而若攻击者仿冒合法用户的DHCP Release报文发往DHCP Server，将会导致用户异常下线。
- DHCP Server服务拒绝攻击：存在大量攻击者恶意申请IP地址，会导致DHCP Server中IP地址快速耗尽而不能为其他合法用户提供IP地址分配服务。
- DHCP Snooping的信任功能，能够保证客户端从合法的服务器获取IP（Internet Protocol）地址。
  - 网络中如果存在私自架设的DHCP Server仿冒者，则可能导致DHCP客户端获取错误的IP地址和网络配置参数，无法正常通信。DHCP Snooping信任功能可以控制DHCP服务器应答报文的来源，以防止网络中可能存在的DHCP Server仿冒者为DHCP客户端分配IP地址及其他配置信息。
  - DHCP Snooping信任功能将接口分为信任接口和非信任接口：信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。
  - 非信任接口在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文。

DHCP Snooping（2）

- 防止DHCP Server仿冒者攻击：可配置设备接口的“信任/非信任”工作模式，将与合法DHCP服务器直接或间接连接的接口设置为信任接口，其他接口设置为非信任接口。此后，从非信任（Untrusted）接口上收到的DHCP回应报文将被直接丢弃，这样可以有效防止DHCP Server仿冒者的攻击。
- 防止DHCP报文泛洪攻击：使能设备对DHCP报文上送DHCP报文处理单元的速率进行检测的功能。此后，设备将会检测DHCP报文的上送速率，并仅允许在规定速率内的报文上送至DHCP报文处理单元，而超过规定速率的报文将会被丢弃。
- 防止仿冒DHCP报文攻击：配置DHCP Snooping绑定表、DHCP协议报文合法性检查功能。设备通过将DHCP Request续租报文和DHCP Release报文与绑定表进行匹配操作能够有效的判别报文是否合法（主要是检查报文中的VLAN、IP、MAC、接口信息是否匹配动态绑定表），若匹配成功则转发该报文，匹配不成功则丢弃。
- 防止DHCP Server服务拒绝攻击：配置设备或接口允许接入的最大DHCP用户数，当接入的用户数达到该值时，则不再允许任何用户通过此设备或接口成功申请到IP地址。

- 防止DHCP Server仿冒者攻击：可配置设备接口的“信任/非信任”工作模式，将与合法DHCP服务器直接或间接连接的接口设置为信任接口，其他接口设置为非信任接口。此后，从“非信任（Untrusted）”接口上收到的DHCP回应报文将被直接丢弃，这样可以有效防止DHCP Server仿冒者的攻击。
- 防止DHCP报文泛洪攻击：使能设备的DHCP Snooping功能时，可同时使能设备对DHCP报文上送DHCP报文处理单元的速率进行检测的功能。此后，设备将会检测DHCP报文的上送速率，并仅允许在规定速率内的报文上送至DHCP报文处理单元，而超过规定速率的报文将会被丢弃。
- 防止仿冒DHCP报文攻击：配置DHCP Snooping绑定表、DHCP协议报文合法性检查功能。设备通过将DHCP Request续租报文和DHCP Release报文与绑定表进行匹配操作能够有效的判别报文是否合法（主要是检查报文中的VLAN、IP、MAC、接口信息是否匹配动态绑定表），若匹配成功则转发该报文，匹配不成功则丢弃。
- 防止DHCP Server服务拒绝攻击：配置设备或接口允许接入的最大DHCP用户数，当接入的用户数达到该值时，则不再允许任何用户通过此设备或接口成功申请到IP地址。

目录

园区网络的IPv6演进：现网评估

端	管	云
• 评估终端设备类型 • 评估终端设备的操作系统及IPv6支持度 • 评估终端设备使用的应用的IPv6支持度 • 升级/替换终端，升级应用程序	• 评估网络设备类型、软硬件能力、License等 • 评估网络设备的IPv6支持度，包括IPv6路由协议、双栈、过渡技术、安全、可靠性、QoS、网络管理等 • 评估网络设备的IPv6（双栈）性能 • 替换/升级设备以支持IPv6且满足性能要求	• 梳理IDC承载业务的类型、流量模型 • 梳理IDC承载网络使用的技术/协议并评估IPv6支持度 • 评估业务系统的IPv6支持度 • 操作系统、数据库、应用系统、业务系统等需支持IPv6

评估设备控制面的能力

- 对IPv6相关路由和VPN等的支持情况
- IPv6和IPv4并存时的协议规格
- IPv6和IPv4并存时的可靠性及IPv6协议健壮性
- IPv6和IPv4并存时设备安全防护能力

评估设备转发面的能力

- IPv6和IPv4并存的转发性能规格
- IPv6和IPv4并存的转发表项规格
- IPv6和IPv4并存的QoS和ACL能力
- IPv6过渡技术的支持能力

支撑系统

- 评估网管系统、日志系统、AAA系统、DNS系统等的IPv6支持度

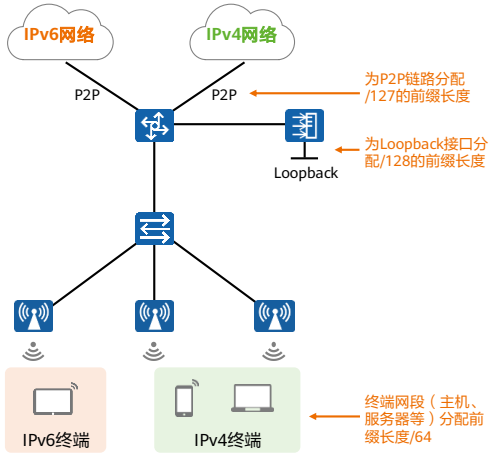
WLAN网络的IPv6演进（1）

整体目标

当前园区网络为IPv4网络，需向IPv6演进，实现IPv4及IPv6用户的接入，且IPv6无线终端能够访问IPv6网络资源。

地址规划

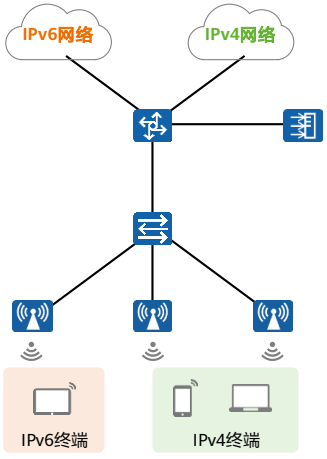
- 明确地址类型与地址规划。确保IPv6地址规划的连续性、可聚合性、可扩展性；
- 可在IPv6地址中规划适当的bit用于承载业务信息、VLAN信息或位置信息，利于路由规划、QoS部署；
- 建议为终端网段（用户主机、服务器等）分配/64的前缀长度；
- 建议为P2P链路分配/127的前缀长度；
- 建议为Loopback接口分配/128的前缀长度。



WLAN网络的IPv6演进（2）

地址分配

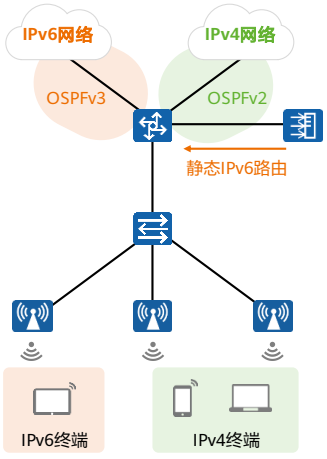
- 对于园区终端IPv6地址获取方式主要有DHCPv6、SLAAC或者手工配置三种方案。
- 针对大量用户的无线终端，建议优先采用DHCPv6方案分配地址。
- 部分不支持DHCPv6的终端可采用SLAAC方案。
- 网络中WAC的数量较少，WAC的地址采用手工配置方式。AP数量较多，可以配置DHCPv6或者SLAAC为AP分配地址。



WLAN网络的IPv6演进（3）

路由可达性

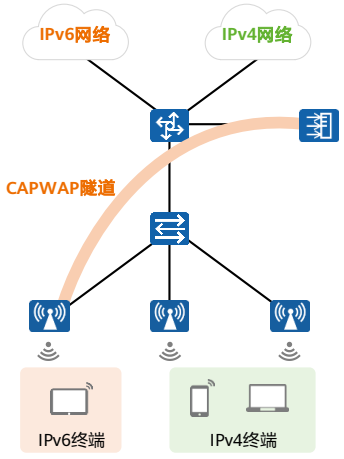
- 针对当前园区网络进行路由设计，三层设备需支持IPv4及IPv6双栈。
- 如果园区网络规模较小、组网简单，可采用IPv6静态路由；如果规模较大，考虑OSPF协议的广泛应用，建议采用OSPFv3实现园区网络内部互联互通。
- 现网中若已存在OSPFv2，则针对OSPFv3的区域规划可与OSPFv2保持一致。



WLAN网络的IPv6演进（4）

AP管理与WLAN业务规划

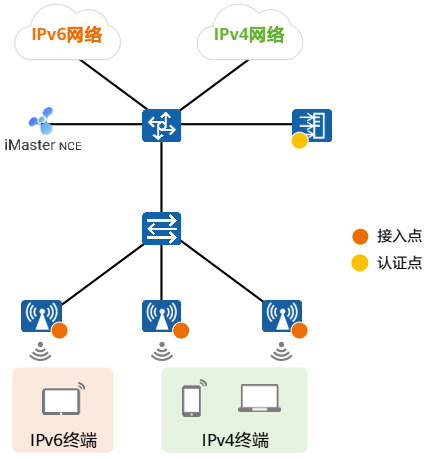
- WAC和AP之间的CAPWAP隧道支持IPv4和IPv6，但同一时间只能选择IPv4或者IPv6中的一种方式，即WAC只能通过IPv4或IPv6中的一种方式管理AP，默认为IPv4。
- AP支持以IPv4或者IPv6方式上线，即AP仅可获取一个地址。
- 为便于IPv4及IPv6终端管理，可设置多个SSID，分别接入IPv4、IPv6单栈用户。



WLAN网络的IPv6演进（5）

接入认证

- 对于园区网络改造场景，常为IPv4向IPv6演进，在相当长一段时间内会同时存在IPv4及IPv6终端。网络需具备相应接入及认证能力。
- 认证方案应提供双栈终端单次认证，避免双栈终端访问IPv4、IPv6业务需要重复执行两次单独认证。
- 园区网络应支持IPv6用户的802.1x、Portal、MAC认证多种方式，针对不同终端灵活采用对应的方案。对于认证点及接入点设计，IPv6方案可与IPv4方案保持一致。
- 无线IPv6用户的认证点为WAC。WAC作为认证点需支持IPv6 RADIUS，满足未来单栈演进诉求。



思考题

1. 简述IPv6相比于IPv4的优点。
2. 简述IPv6报文头相比于IPv4的不同之处。

HUAWEI

- 答案1：“无限”地址空间，层次化的地址结构，即插即用，简化的报文头部，安全特性，移动性，增强的QoS特性。
- 答案2：
  - 采用了基本报头+扩展报头的报文形式。
  - 取消了IP的校验：第二层和第四层的校验已经足够健壮了，因此IPv6直接取消了IP的三层校验，节省路由器处理资源。
  - 取消中间节点的分片功能：中间路由器不再处理分片，只在产生数据的源节点处理，省却中间路由器为处理分片而耗费的大量CPU资源。
  - 定义定长的IPv6报头：有利于硬件的快速处理，提高路由器转发效率。
  - 安全选项的支持：IPv6提供了对IPSec的完美支持，如此上层协议可以省去许多安全选项。
  - 增加流标签：提高QoS效率。

本章总结

- IPv6作为下一代互联网协议，具备了IPv4无法比拟的诸多优点，可以完美解决现阶段IPv4无法满足的业务发展的问题。
- IPv6不仅仅具有庞大的地址空间，除此以外，IPv6还简化了报文头，提升了路由器报文转发效率；IPv6地址易于划分与规划，便于路由聚合；IPv6可以实现即插即用，增强了QoS等等。
- 本课程主要讲述了IPv6的基本概念、基于IPv6的WLAN组网及应用、基于IPv6的WLAN网络准入控制、IPv6中的WLAN安全、以及WLAN网络的IPv6演进。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

CloudCampus解决方案

HUAWEI

前言

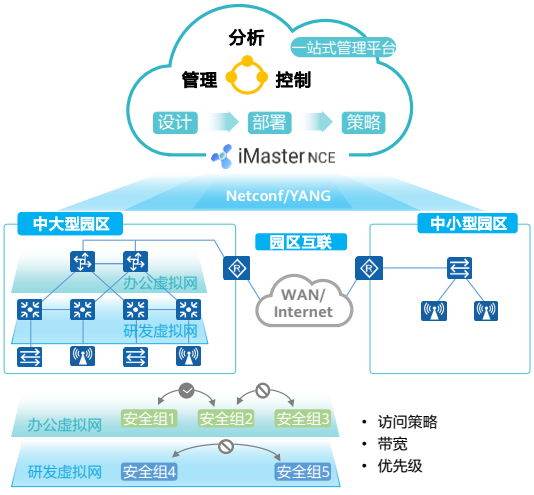
- 数字化变革时代，企业IT网络的可用性及灵活性直接决定着办公及生产效率，甚至关系到业务决策和执行的成败。
- 华为智简园区（CloudCampus）致力于为企业构建一张超宽、智慧、极简、安全、开放的基于业务意图的园区网络，时刻洞察并快速响应网络及业务需求，赋予企业捕捉转瞬即逝的商机能力。
- 本课程系统地介绍华为CloudCampus解决方案，讲解解决方案架构、关键组件及功能特性，并逐一从超宽联接、极简网络、一网多用、智能策略、智能运维等多个维度介绍智简园区解决方案的关键功能或特性。

目标

- 学习完本课程后，您将能够：
  - 描述CloudCampus解决方案
  - 描述CloudCampus解决方案的架构、关键组件及亮点功能
  - 描述CloudCampus解决方案定义的超宽、极简网络
  - 理解基于VXLAN的虚拟化园区及适用场景
  - 区分常见的园区网络准入认证方案
  - 描述CloudCampus的智能策略、智能运维

目录

园区网络一站式自动驾驶解决方案



网络开通”快”，部署效率提升

- **设备即插即用：**设备极简开局，场景导航，模板配置。
- **网络极简部署：**网络资源池化，一网多用，业务自动化发放。

业务发放”快”，用户体验提升

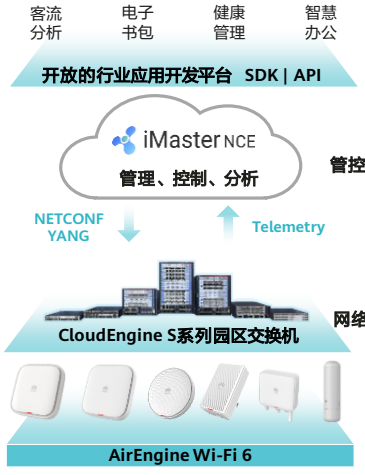
- **业务随行：**图形化策略配置，用户漫游权限不变，体验不变。
- **终端智能识别：**终端接入防仿冒，终端智能识别准确率高。
- **智能HQos：**基于应用调度和整形，带宽精细化管理。

智能运维“快”，整网性能提升

- **实时体验可视：**每时刻、每用户、每区域的网络体验可视。
- **精准故障分析：**主动识别85%的典型网络问题并给出建议。
- **智能网络调优：**基于历史数据的无线网络预测性调优。

HUAWEI

Wi-Fi 6时代的智简园区网络



各行各业都在进行数字化转型

政企办公	教育	零售	制造	无线城市
构建全无线化数字空间 企业向学习型组织转型	新一代数字化 无线互动课堂	提升购物体验， 提高线下转化率	有线无线物联的 工业互联网融合	通过无线化、物联化 提升城市运行效率

管控析一站式运维大脑，iMaster NCE-Campus

建网全自动，使能Wi-Fi 6的业务
规划自动化 · 建网自动化 · 策略自动化

运维全智能，保障Wi-Fi 6的体验
用户体验可视 · 故障定界 · 网络调优自愈

Wi-Fi 6 Ready的有线网络

接入全万兆，释放Wi-Fi 6的速度

- Multi-GE交换机 + 高密25GE盒式交换机 + 100G核心，构建Wi-Fi 6超宽通道
- 默认无线用户融合管理，高达10K AP，50K用户并发，满足Wi-Fi 6时代海量用户并发接入
- 万人无线园区，百G核心CloudEngine S12700E，吞吐57.6Tbps，管理5万无线用户，6倍性能

全无线，AirEngine Wi-Fi 6

极速
业界独家双频16天线
10.75Gbps，是业界的2倍

覆盖稳
智能天线
波随人动，覆盖远20%

应用稳
DynamicTurbo
应用加速，<10ms时延

HUAWEI

全场景：单园区到多分支互联全覆盖

	简单业务园区	多业务园区	多分支互联园区
网络特征	规模较小、业务简单； 站点数量多，模型相似。	规模较大、业务复杂、多业务共存	存在多个分支站点，站点间存在通过混合WAN链路互访需求。
典型场景	酒店、普教等多分支及小型企业园区	高校、政府、大企业园区等	大企业、金融网点等

全生命周期：一站式管理中心极简管理

全融合：一套控制器管理LAN侧、WAN侧

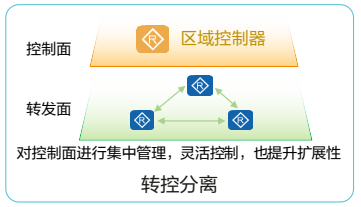
- CloudCampus解决方案融合了园区LAN、WAN业务的配置、管理模型，除了提供园区LAN侧业务的配置管理外，同时也支持对WAN侧互联业务的管理，实现LAN-WAN一体化的融合管理。

一套控制器，支持管理纯LAN和LAN-WAN融合

部署简单

图形化界面，灵活组网，设备即插即用

配置简化



对控制面进行集中管理，灵活控制，也提升扩展性

转控分离

网络业务数据可视化，对全网络的状态进行监控、分析

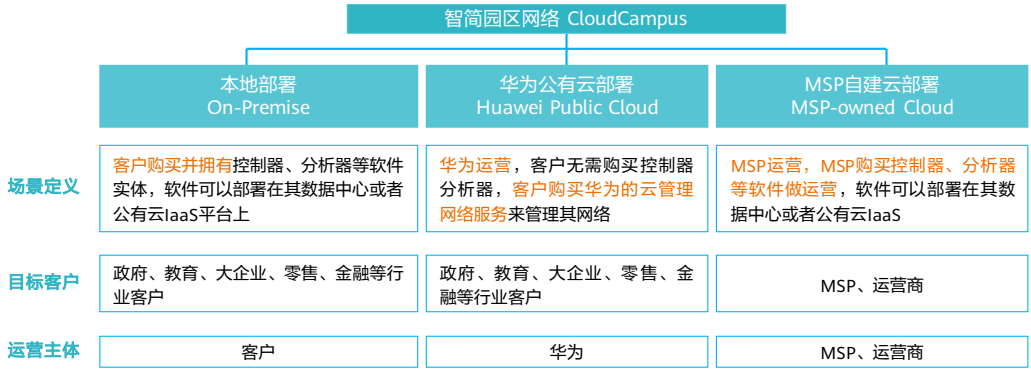
运维简单

运营商提供的业务可从WAN延伸到LAN及增值服务

价值延伸

HUAWEI

多模式：CloudCampus的三种部署模式



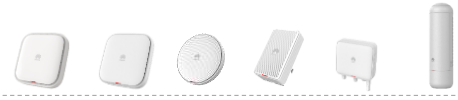
HUAWEI

- MSP : Management Service Provider , 管理服务提供商

解决方案组件1：智简园区网络硬件产品简介

CloudEngine S系列交换机

CloudEngine S系列园区交换机，可通过Multi-GE接入、 25GE/40GE汇聚、高密100GE核心构建智能超宽的有线网络。同时，通过智能HQoS、随板AC、加密流量威胁防御等先进网络技术，构建Wi-Fi 6时代的高品质承载网络。



AirEngine Wi-Fi 6 AP

AirEngine系列无线局域网产品，基于Wi-Fi 6（802.11ax）标准，并借鉴源自华为5G的关键技术，打造极速性能、稳定体验、智能组网的全无线园区网络。

HiSecEngine AI防火墙

华为HiSecEngine系列产品，结合分布式硬件平台，提供业界领先的安全防护性能和拓展能力；

NetEngine AR路由器

NetEngine系列AR路由器基于ARM架构多核处理器和无阻塞交换架构，融合 SD-WAN、路由、交换、VPN、安全等多种功能，满足企业业务多元化和云化趋势下对网络设备高性能的需求。

HUAWEI

- 网络作为企业数字化转型的最重要组成部分，如何承载并敏捷部署业务，如何保障企业上云体验，如何保障企业ICT安全是网络必须尽快解决的现实问题。未来网络一定是极简和AI，能主动感知业务变化，及时预知网络隐患，从而驱动企业ICT基础设施的变革，帮助企业重塑商业模式、提升客户体验并开创未来。
  为了帮助用户打造智能时代IP网络的强劲引擎，华为面向园区、数据中心、广域网络、WLAN及网络安全等主力场景，提出针对CloudEngine交换机、NetEngine路由器、AirEngine Wi-Fi 6 AC及AP、HiSecEngine安全网关四大品类的“四大Engine”品牌战略。

解决方案组件2：iMaster NCE-Campus

HUAWEI

- iMaster NCE-Campus是智简园区网络解决方案基于Web的集中式管理控制系统，支持网络业务管理、网络安全管理、用户准入管理、网络监控、网络质量分析、网络应用分析、告警和报表等特性，提供大数据分析的能力，同时提供开放的接口、支持与其他平台集成。企业用户可以通过iMaster NCE-Campus进行业务配置、日常运维等工作，实现规模设备的集中管理。

解决方案组件3：iMaster NCE-CampusInsight

AS-IS：以设备为中心的网络管理

以设备为中心，无法感知用户体验

“救火式”响应，无法识别潜在故障

依靠专业工程师**现场定位故障**

TO-BE：以用户体验为中心的AI智能运维

体验可视化：基于Telemetry秒级数据采集，每用户每应用每时刻体验可视

分钟级潜在故障识别和根因定位

基于动态基线、大数据关联等识别潜在故障

KPI关联分析和协议回放，精准定位问题根因

网络预测性调优：通过AI 智能分析AP的负载趋势，完成无线网络的预测性调优闭环

利用算法提升效率，通过场景化的持续学习和专家经验，智能运维将运维人员从复杂的告警和噪声解放出来，使运维更加自动化和智能化

HUAWEI

基于一站式管理中心提供全生命周期极简管理

蓝色背景部分为iMaster NCE提供的网络全生命周期管理服务

HUAWEI

规 建 维 优

Day 0：华为WLAN云网规

- 云网规缩减规划时间，基于内置经验库确保信号覆盖。

① 获取平面图

② 进入华为在线WLAN网规工具：WLAN Planner

1.环境设置

2.区域设置

3.设备布放

4.信号仿真

5.导出报告

③ 在华为WLAN云网规工具中，用户可以通过简单的5步来完成WLAN网络规划

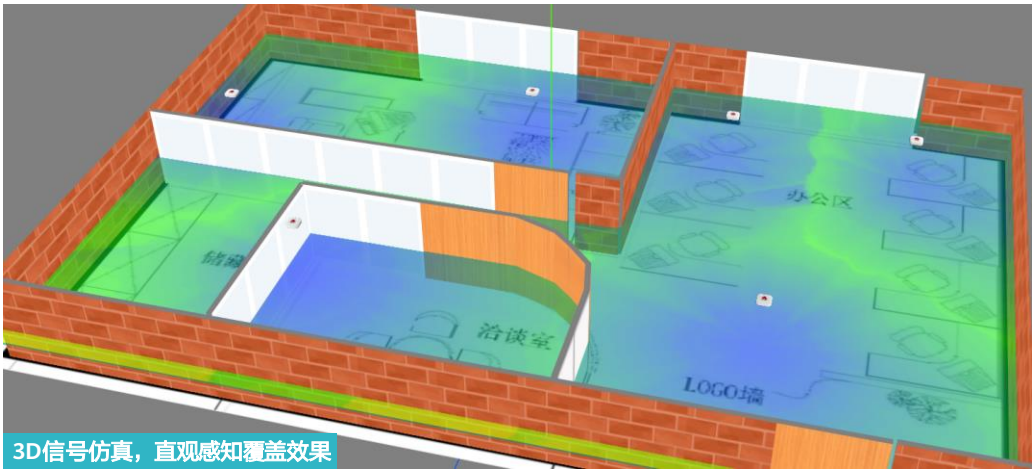
④ 使用网规报告指导现场施工

网规结果可导入iMaster NCE

HUAWEI

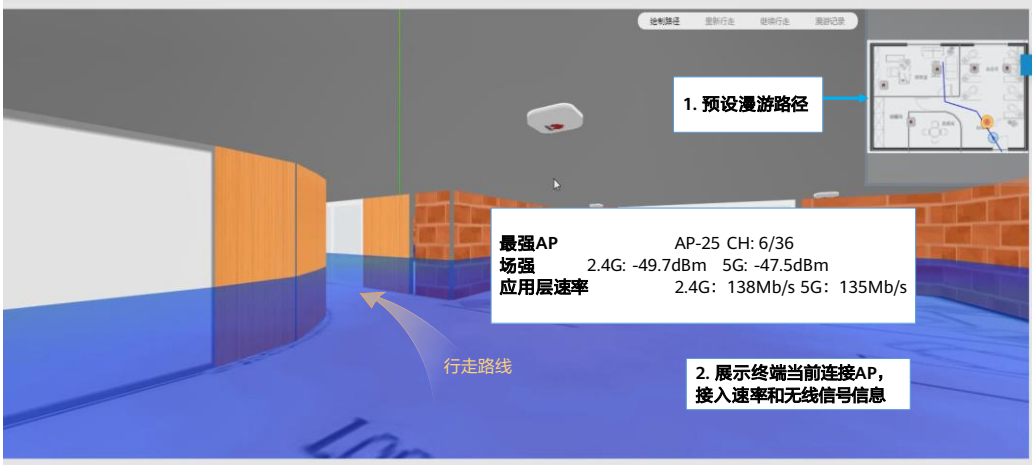
- Wlan Planner网址：https://serviceturbo-cloud-cn.huawei.com/serviceturbocloud/dist/#/toolappmarket

Day 0：3D网规，直观感知信号覆盖和漫游效果



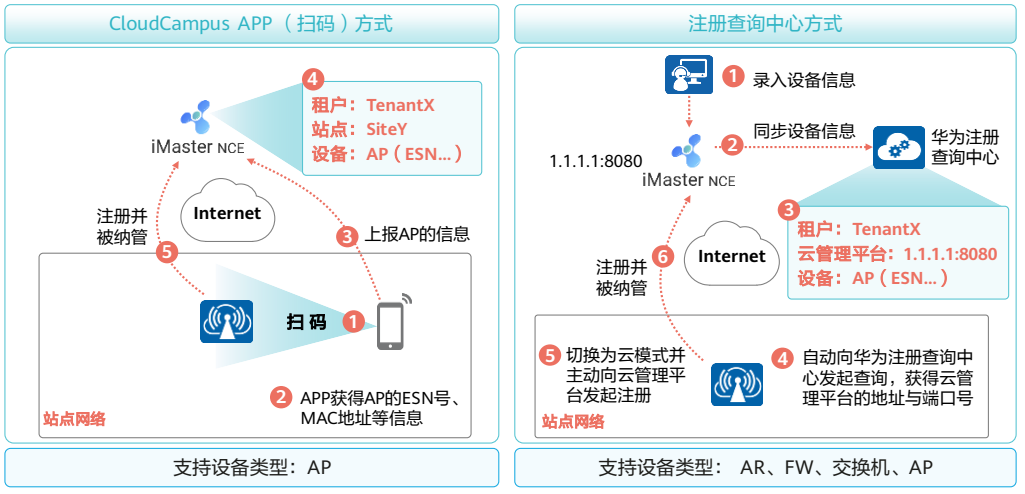
3D信号仿真，直观感知覆盖效果

Day 0：3D网规，漫游仿真，提前判断漫游效果



规 建 维 优

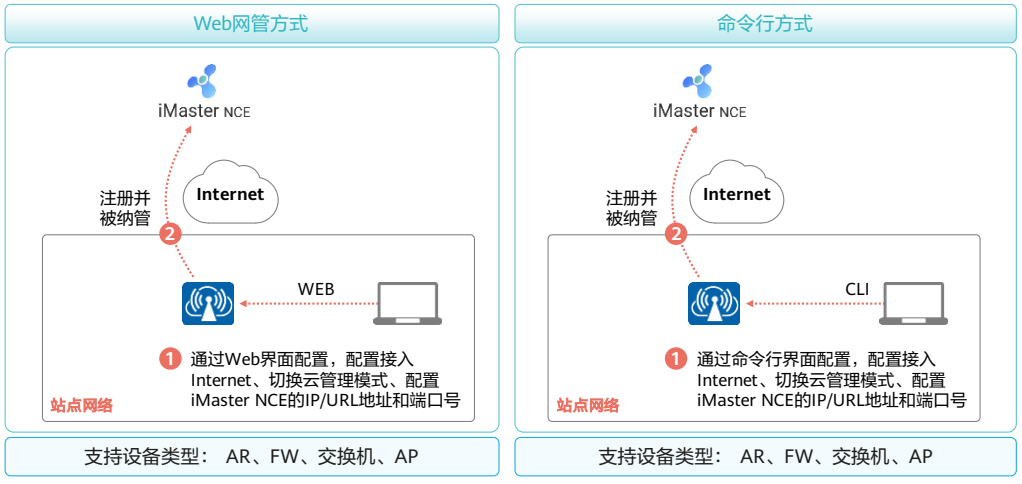
Day 1：设备即插即用（1）



HUAWEI

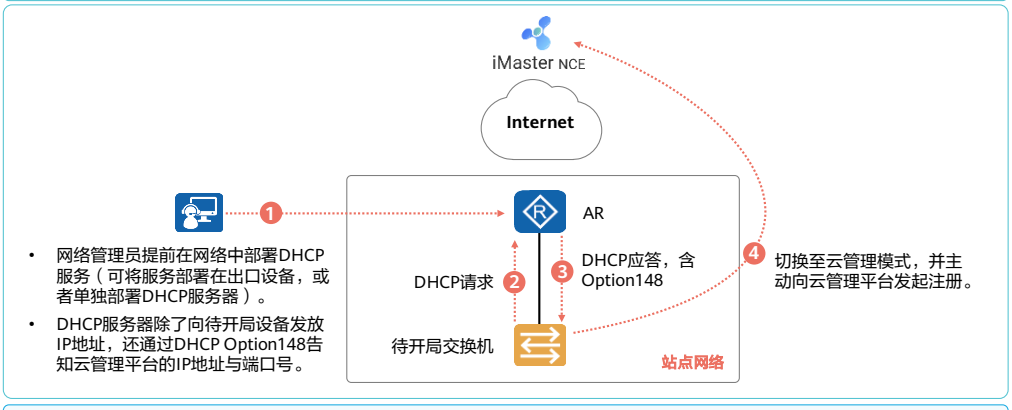
- 注册查询中心是华为在Internet上设立的公有云服务，可以理解为一个云上平台。主要用于实现用户网络设备的即插即用。对于网络设备的开局配置而言，最重要的是向iMaster NCE发起注册并被纳管。华为CloudCampus支持公有云部署模式、MSP自建云部署模式，因此在Internet上可能存在多个iMaster NCE的实例，那么网络设备开机接入网络后，如何知道该向哪一个iMaster NCE发起注册呢?
- 华为设立了注册查询中心，用户可以选择注册查询中心方式来实现CloudCampus华为公有云或MSP自建云场景下的网络设备即插即用。用户首先在iMaster NCE上录入待管理网络设备的信息，其中包括设备的SN号等。iMaster NCE将该信息同步给华为注册查询中心，注册查询中心会维护相关信息。当用户购买的华为云管理网络设备以出厂的方式接入网络并获取IP地址后，会主动向注册查询中心发起查询。设备在出厂时已经预置注册查询中心的域名，该域名全球统一，设备通过不同地区的DNS服务器发起解析请求并得到各地的注册查询中心地址。此后注册查询中心会将设备对应的iMaster NCE的IP地址等信息返回给设备，于是设备便能向该地址发起注册申请，完成纳管过程。

Day 1：设备即插即用（2）



Day 1：设备即插即用（3）

DHCP Option148方式

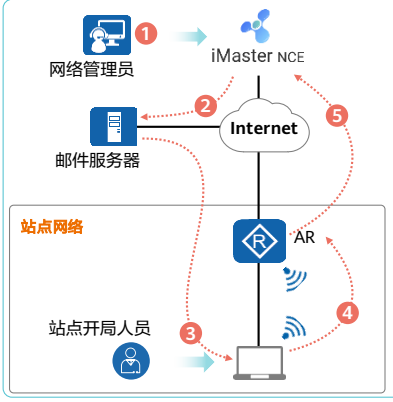


- 网络管理员提前在网络中部署DHCP服务（可将服务部署在出口设备，或者单独部署DHCP服务器）。
- DHCP服务器除了向待开局设备发放IP地址，还通过DHCP Option148告知云管理平台的IP地址与端口号。

支持设备类型： AR、交换机、AP

Day 1：设备即插即用（4）

Email开局



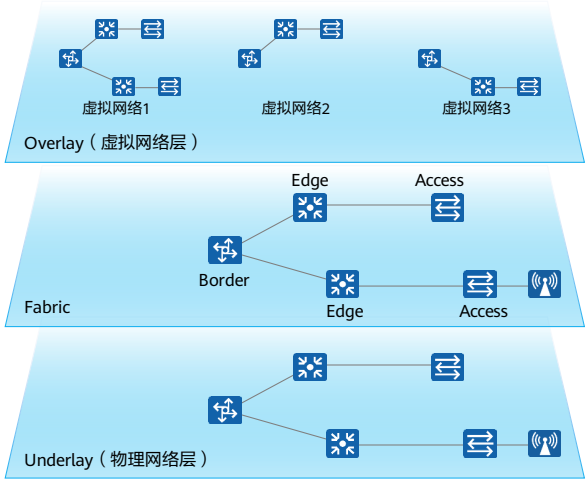
1. 网络管理员在控制器上进行ZTP配置并选择邮件开局方式。
2. 控制器将开局配置“打包”为一系列字符串，通过邮件发往管理员指定的邮箱。
3. 站点开局人员在站点的PC上登录邮箱，收取上述开局邮件。
4. 站点开局将站点的PC连接到CPE（可通过有线或无线方式），然后点击邮件正文中的超链接，此时PC会自动登录到CPE，并将超链接中的参数解析，得到CPE的开局配置，然后将配置写入CPE。
5. CPE接入WAN网络，自动向控制器发起注册申请。

注：此处CPE指的是图中的AR路由器

支持设备类型： AR

规 建 维 优

Day 1：中大型园区网络部署，VXLAN虚拟园区网络



- 可以根据业务需求创建多个虚拟网络，实现业务隔离
- 通过VXLAN实现L2及L3通信

- 通过虚拟化技术，构建基于任意物理拓扑的逻辑拓扑
- 在Fabric上创建业务网络，与物理网络解耦

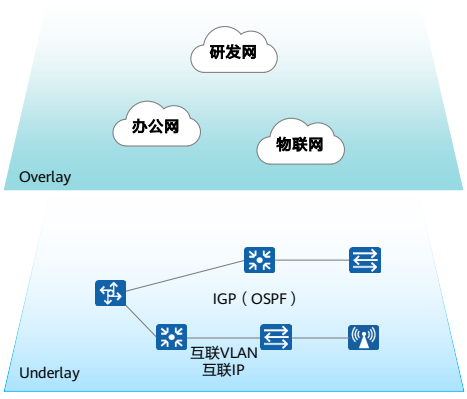
- 由物理设备建立的物理网络
- 为园区内所有业务提供互联互通能力
- 业务数据转发的基础承载网

HUAWEI

- VXLAN技术将物理网络作为Underlay网络，在其上构建出虚拟的二层或三层网络，即Overlay网络。Overlay网络利用Underlay网络提供的三层转发路径，实现报文在不同站点间传递。
- 在技术应用中，一般为不同的业务创建不同的Overlay网络。对于业务来说，Underlay网络是透明的，只能感知到Overlay网络。

规 建 维 优

Day 1：中大型园区网络部署，Underlay部署自动化



基于图形化界面和Netconf/YANG实现Underlay自动化

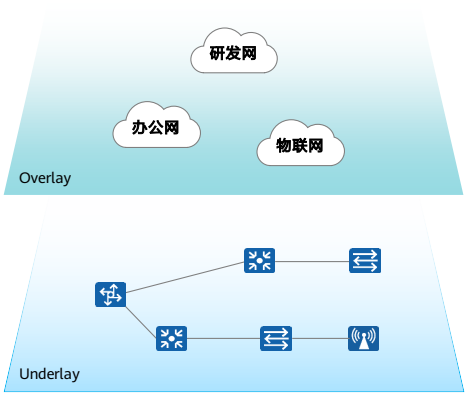
设备录入	• 通过Excel录入设备信息和拓扑信息
资源配置	• 网络资源池规划：IP、VLAN • 预配置，基于配置模板和特性模板
设备安装	• 设备安装和连线，并上电 • 手工将出口/核心设备注册到控制器
自动配置下发	• 汇聚/接入/AP自动上线，并进行拓扑校验 • 设备自动获取配置
自动路由编排	• 创建Fabric，使能路由自动编排，路由自动编排
设备故障	• APP扫码零配置替换

注：支持先配置后安装、或先安装后配置

HUAWEI

- 可以先配置后安装、或先安装后配置，区别是前者要求提前录入拓扑信息；后者可以自动发现拓扑。

Day 1：中大型园区网络部署，Overlay部署自动化



场景

高校、政府园区、商业楼宇等，需为多种业务或多个租户提供隔离的虚拟网络，实现一网多用，提升网络资源利用率。

需求

1. 将物理网络划分为多个虚拟网络，相互隔离
2. 虚拟网络部署自动化

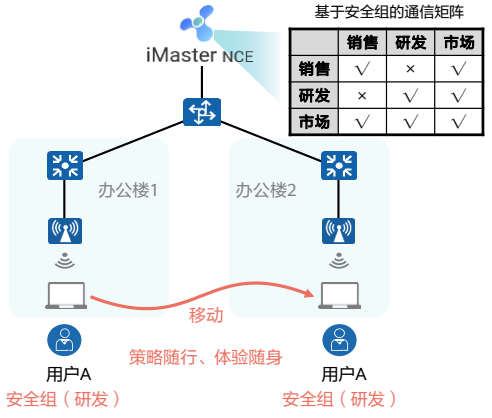
解决方案和价值

一网多用	• 基于VXLAN实现一网多用 • 通过BGP-EVPN实现隧道自动建立
自动化	• Netconf/YANG • 基于控制器的图形化界面操作
平滑演进	• 汇聚层+接入层（无需支持VXLAN）策略联动 • 控制器支持对VLAN网络的自动化部署

规 建 维 优

Day 2：基于SDN实现场景

- 基于SDN实现精细化的策略控制和自动化部署，业务随行。



	销售	研发	市场
销售	√	×	√
研发	×	√	√
市场	√	√	√

场景

企业、高教、政府等对网络策略进行精细化管理的场景

需求

1. 精细化策略控制，用户全网移动，策略和业务体验不变。
2. 灵活和极简的策略部署，降低OPEX。

解决方案和价值

- 基于安全组：
  - 基于用户和应用的策略/体验，包括权限、带宽和QoS
- SDN：
  - 基于SDN控制器，集中策略管控
  - 面向业务意图
- 自然语言：
  - 图形化界面
  - 基于自然语言的配置

HUAWEI

- OPEX（Operating Expense）指的是企业的管理支出，即运营成本。指企业运行付出的各种支出成本，包括维护费用、营销费用、人工成本以及折旧。

基于iMaster NCE的全网监控

健康度

- 站点健康度概览
- 站点间监控（Overlay拓扑及互联状况）
- 终端、应用、设备360
- .....

告警

- 当前告警、历史告警、屏蔽告警
- 告警通知方式设置（Email通知）
- .....

报表

- 统计分析（含终端行为分析）
- 敏捷报表
- .....

事件日志

- 终端认证事件
- 设备关键事件
- 设备上下线日志

基于iMaster NCE的简化运维

配置维护

- 设备配置结果查看
- 设备配置保存

诊断工具

- Ping、Trace、获取报文头、报文路径跟踪、诊断信息收集、应用质量检测、.....

设备维护

- 设备资产监控（机框、单板、子卡等）
- 设备升级
- 设备License激活
- 设备配置文件备份、恢复
- .....

iMaster NCE-CampusInsight特性

- iMaster NCE-CampusInsight，基于预测性和AI提升用户和业务体验。

实时体验可视

1. **每区域：**通过7维评价体系，直观呈现整网或每个区域的网络状况及用户体验
2. **每用户：**实时呈现每个用户的全旅程网络体验（谁、何时、连接至哪个AP、体验、问题），故障可回溯
3. **每应用：**实时语音与实时视频应用体验感知，快速智能定界问题设备，分析质差根因

分钟级故障定位

1. **主动问题识别：**经过华为20万+终端持续训练的AI算法，主动识别85%的网络潜在问题
2. **分钟级故障定位：**基于故障推理引擎，分钟级问题定界并识别问题根因，给出有效的修复建议
3. **智能故障预测：**利用AI学习历史数据动态生成基线，通过和实时数据对比分析从而预测可能发生的故障

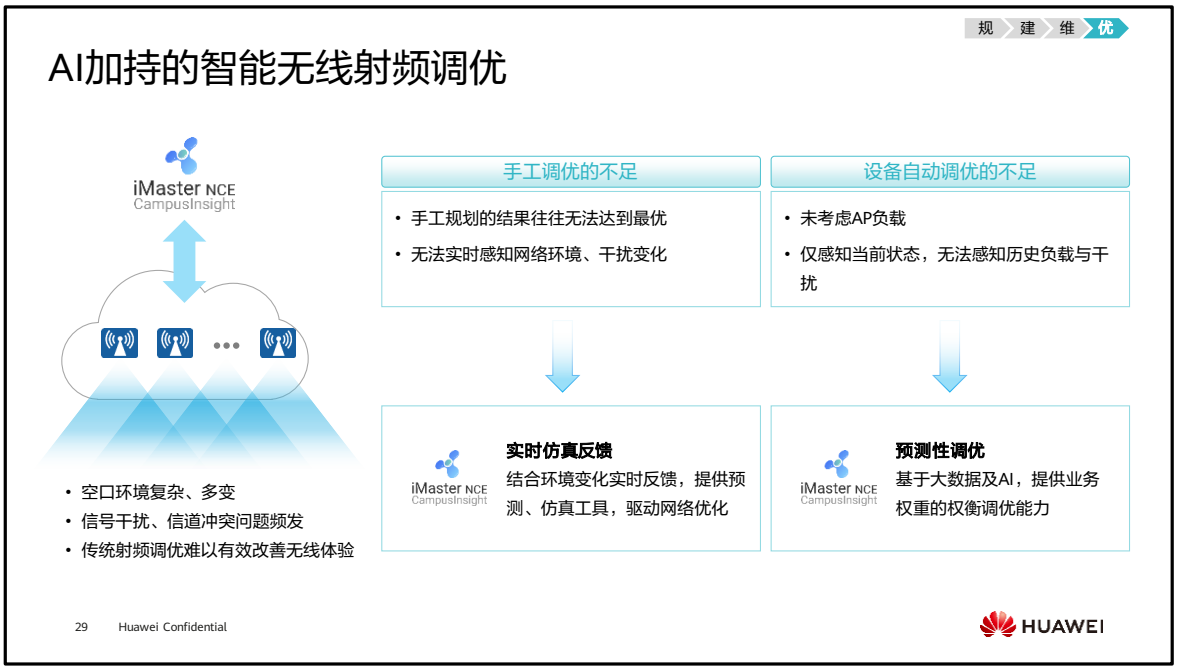
智能网络调优

1. **实时仿真反馈：**基于楼层设备的邻居和射频信息，实时评估无线网络信道冲突情况，并给出优化建议
2. **预测性调优：**基于历史数据的分析识别边缘AP、预测AP的负载趋势，进行无线网络的预测性调优并查看调优前后的增益对比，整网性能提升50%+（Tolly认证）。

CloudCampus APP实现规划、开局、运维端到端极简

全生命周期的移动APP

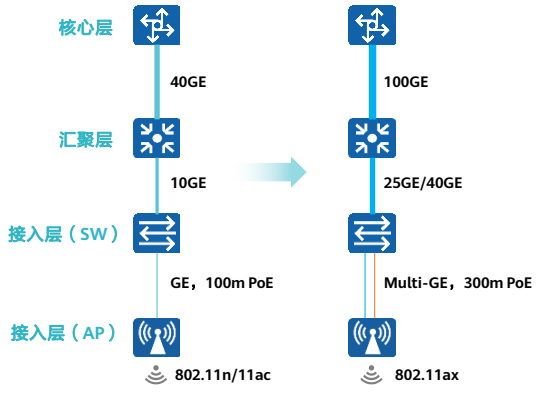
工勘	对接云网规平台，基于图纸可以进行照片、文字的记录
网规	对接云网规，随时随地查看网规结果、热图、AP属性等
开局	扫码开局
验收	一键测试、单业务测试、项目测试 基于云网规工程的点位验收
运维	移动运维，设备、应用监控 蓝牙/管理VAP接入AP、AP离线诊断



- 手工调优不足：
  - 部分客户采取人工调优，手工规划信道的方式，但由于规划过程投入巨大，一次规划需要持续多天多次调整，而最终的结果却可能越调越差（信道规划冲突，AP安装后距离过近相互干扰）。一旦遇到环境变化（新增AP部署，新加了一堵墙等），则原先的规划则需要重新调整，而且可能是牵一发而动全身，难度可想而知。
- 实时仿真反馈：
  - 针对网络干扰进行主动避让和调整，通过射频质量评估得分仿真效果，不需要管理员到现场反复调整配置和验证。能大幅提升运维效率，提升用户无线网体验。
- 设备自动调优的不足：
  - 传统的设备自动调优是以信号覆盖为中心，同时凌晨触发的调优缺少用户行为数据（凌晨时只有少量或没有用户接入），仅能基于当前的状态调优，无法感知真实AP的负载，对于白天的干扰也无法感知，所以效果难以保证，无法充分利用射频资源。
- 预测性调优：
  - 相比传统的基于“过去值”的调优方式，智能无线射频调优采集历史7天的用户接入数据，采用AI智能算法准确预测AP的负载趋势，基于“未来值”来指导射频调优，实现真正的网随人动。

目录

端到端带宽升级，满足数字化终端和业务增长需求



场景需求

- **场景：**企业办公、校园等场景带宽需求持续增加
- **需求：**
  - 能够利旧现有的综合布线，并提升端到端带宽。
  - AP布放密度提高，如何在满足AP上行带宽前提下增加PoE传输距离。

解决方案

- **Multi-GE → 25GE/40GE → 100GE：**满足未来网络演进需要
- **光电混合缆：**结合光纤远距离通信及电缆可供电的优势，将这两个优势整合到一根线缆上。
- **300米远距供电：**300米PoE++供电

光电混合交换机以及光电混合缆

AP网线接入方案

- 可配合POE交换机通过网线AP进行直接供电，简化布线，节省人工成本。
- 网线的传输距离有限，在100米左右，对部署有限制。
- 常用网线所能提供的数据传输速率有限。

AP光纤接入方案

- 无法进行POE供电，需要寻找独立电源进行供电。
- 可提供较远的传输距离。
- 可提供10Gbps以上的传输速率。

光电混合缆方案：结合网线接入以及光纤接入的优势，端口直接供电，带宽更高，传输距离更远

CloudEngine S12700E：性能超强的园区网络交换新核心

CloudEngine S12700E-4　CloudEngine S12700E-12　CloudEngine S12700E-8

主控板MPUE

GE电 X5E/X5S

交换网板SFUE

GE光 X6E/X6S

100G X6E/100G X6S

10GE X6E/X6S

海量吞吐　有线无线融合　全可编程 业务敏捷

场景	典型应用
中大型园区场景	作为核心交换机，融合WLAN AC功能，提升无线流量转发能力，融合有线和无线策略控制，减少配置和故障节点。
园区虚拟化场景	作为VXLAN虚拟园区的Border节点，结合控制器实现园区网络的一网多用，提升网络资源利用率。
园区大带宽互联场景	园区和数据中心100G互联、园区和广域100G互联及园区内100G互联，满足高速增长的业务需求。

全场景WLAN，室内室外多场景高密接入

室外人流密集覆盖：场馆（AP安装高度：>15米）

AP+定向天线覆盖

三射频+小角度天线内置定向覆盖

室内人流密集场景：小型峰会会场、礼堂（AP安装高度：3-15米）

传统全向覆盖

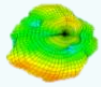
小角度天线内置，定向覆盖

流量突发场景：电子课堂、会议室（AP安装高度<3m，人均＞4Mbps）

双射频

三射频

室内多隔断场景：多隔断办公区（AP安装高度：<3米）



全向天线

智能天线

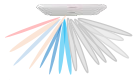
HUAWEI

AirEngine 8760-X1-PRO：加持华为5G技术的Wi-Fi 6 AP

AirEngine 8760-X1-PRO

16空间流+灵活射频模式切换

16条空间流



超高容量

10.75 Gbps

射频模式：4+8+独立扫描射频/4+12/4+8+4

2个10G上行接口

双PoE供电，提高AP可靠性

光口：10GE SFP+
电口：10GE x2
支持光电混合线缆

独立探针

可配合CampusInsight进行
基于大数据的射频调优

独立硬件+双频扫描
实时网络优化

微风道+液冷

微风道：组合式散热系统

液冷

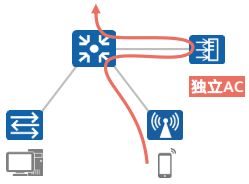
参数名称	规格	参数名称	规格
端口	2*10GE电口+1*10GE SFP+	天线	内置智能天线
蓝牙	蓝牙5.0	供电	直流：42.5V~57V；PoE++，双电源备份
AP速率	1.15Gbps+9.6Gbps	USB接口	1
内置IoT模组	ZigBee、RFID、资产管理、电子价签	安全性	硬件加密：IPSec、DTLS；WPA3

HUAWEI

目录

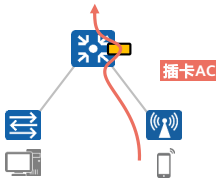
随板AC，实现有线及无线网络深度融合

独立AC



- 独立的业务转发
- 割裂的设备管理
- 分离的用户策略

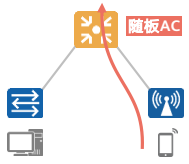
插卡AC



- AC作为交换机的插卡，安装在交换机上
- 仅是硬件层面的融合

有线及无线认证点分离、策略控制分散、流量转发分离、故障排除困难、管理困难

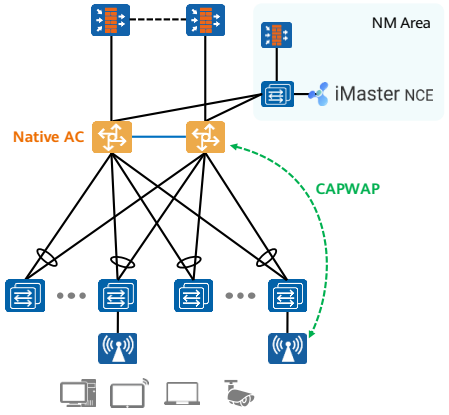
有线无线融合（随板AC，Native AC）



交换机融合WAC功能，无线流量转发无瓶颈，并且减少故障点，有线无线集中管理：

- 有线及无线业务统一管理、融合转发
- 有线及无线用户融合管理、网关融合
- 有线及无线认证点融合
- 有线及无线统一策略执行

融合转发、融合认证、融合策略执行



统一转发：有线和无线的转发流量统一在核心交换机上处理

统一认证：核心交换机为有线和无线统一认证点和三层网关

统一策略执行：核心交换机为有线和无线统一的策略执行点

Wi-Fi & IoT融合，统一网络部署和运维管理

场景与挑战

- 场景：零售、医疗、教育、企业等园区，基于物联网提供创新的数字化业务。
- Wi-Fi和IoT（蓝牙、RFID等）单独部署，众多无线网络，成本高，业务扩展不灵活；无线网络繁杂，存在射频干扰，影响业务体验。

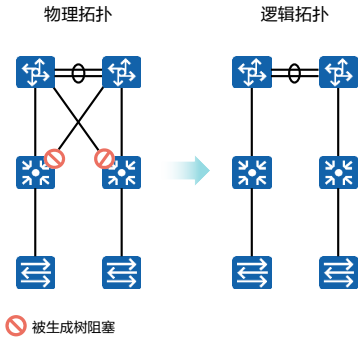
华为物联网AP

- Wi-Fi & IoT融合架构。
- AP与IoT基站合一，配套资源减半（接入/供电）。
- 支持云化管理，即插即用，业务配置简单。
- Wi-Fi与IoT配置联动，感知冲突时自动切换Wi-Fi信道。

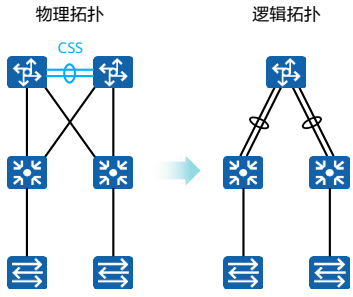
HUAWEI

CSS横向虚拟化，“二虚一”链路更宽，管理更简单

传统：路由冗余，链路1:1保护



华为：设备集群，链路1+1保护



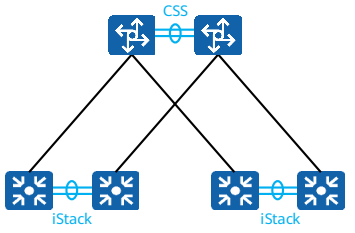
- 2台核心设备基于CSS虚拟为1台设备，网元管理数降低50%
- 汇聚设备基于Eth-Trunk实现上行链路聚合，带宽提升100%

HUAWEI

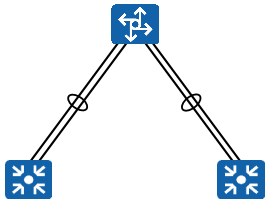
iStack横向虚拟化，“多虚一”简化设备配置和管理

- CSS/iStack + Eth-trunk 可将网络拓扑形成逻辑上的“树形”结构，简化网络拓扑，规避二层环路，提高网络可靠性。

物理拓扑



逻辑拓扑

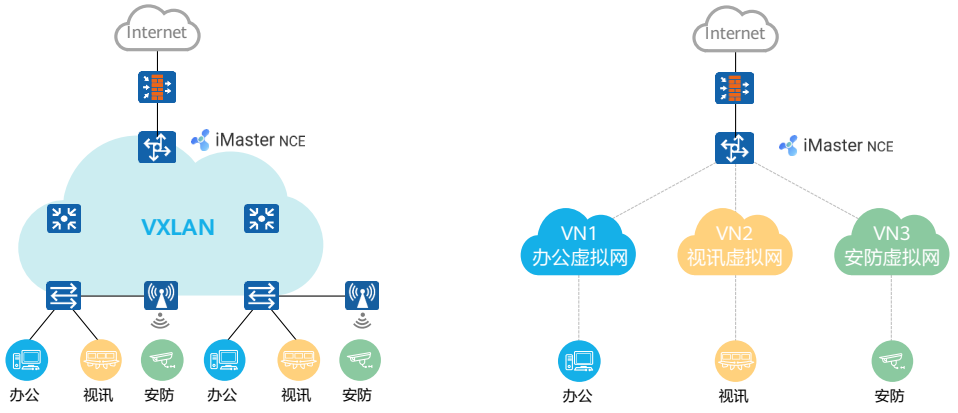


- 多台设备虚拟为一台设备，极大简化网络配置和设备管理
- 配合Eth-Trunk上行链路聚合，负载均衡，提升上行链路可靠性
- 支持业务口堆叠，无需专用堆叠口或堆叠卡，组网方便灵活。

目录

“一虚多”实现一网多用

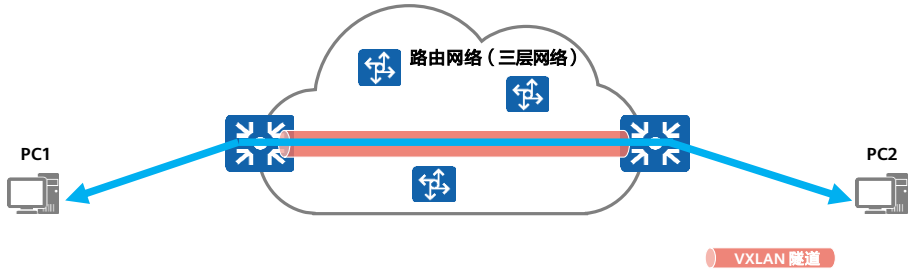
- 一张网承载多种业务，物理网络部署自动化，虚拟网络开通自动化，业务策略发放自动化。



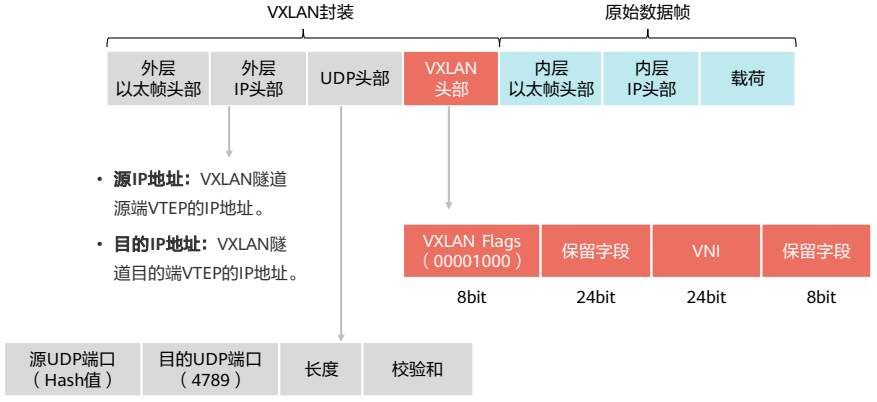
HUAWEI

VXLAN简介

- VXLAN在本质上属于一种VPN技术，能够在任意路由可达的网络上叠加二层虚拟网络，通过VXLAN网关实现VXLAN网络内部的互通，同时，也可以实现与传统的非VXLAN网络的互通。
- VXLAN通过采用MAC in UDP封装来延伸二层网络，将以太报文封装在IP报文之上，通过路由在网络中传输，无需关注虚拟机的MAC地址。且路由网络无网络结构限制，具备大规模扩展能力。

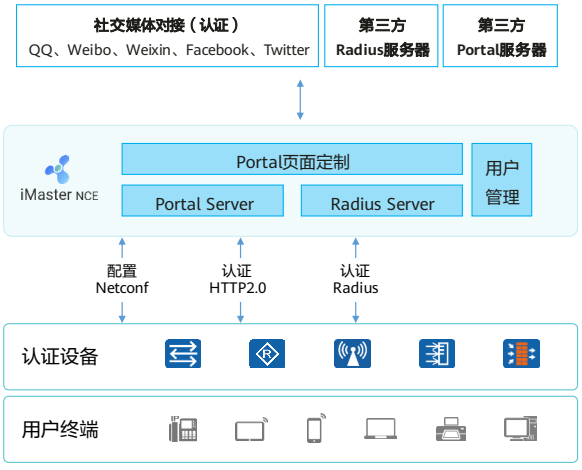


VXLAN的报文格式



目录

用户接入认证



认证方式：

- Portal认证：用户名密码、匿名、短信、QQ、新浪微博、微信、Facebook、Twitter、Passcode认证
- MAC认证
- 802.1x认证

传输协议：

- 认证数据采用HTTP2.0、Radius协议传输
- 配置数据采用Netconf协议传输

开放认证：

- 支持对接第三方Portal服务器
- 支持对接QQ、Weibo、Weixin、Facebook、Twitter社交媒体

智能策略引擎，实现精细化的策略控制

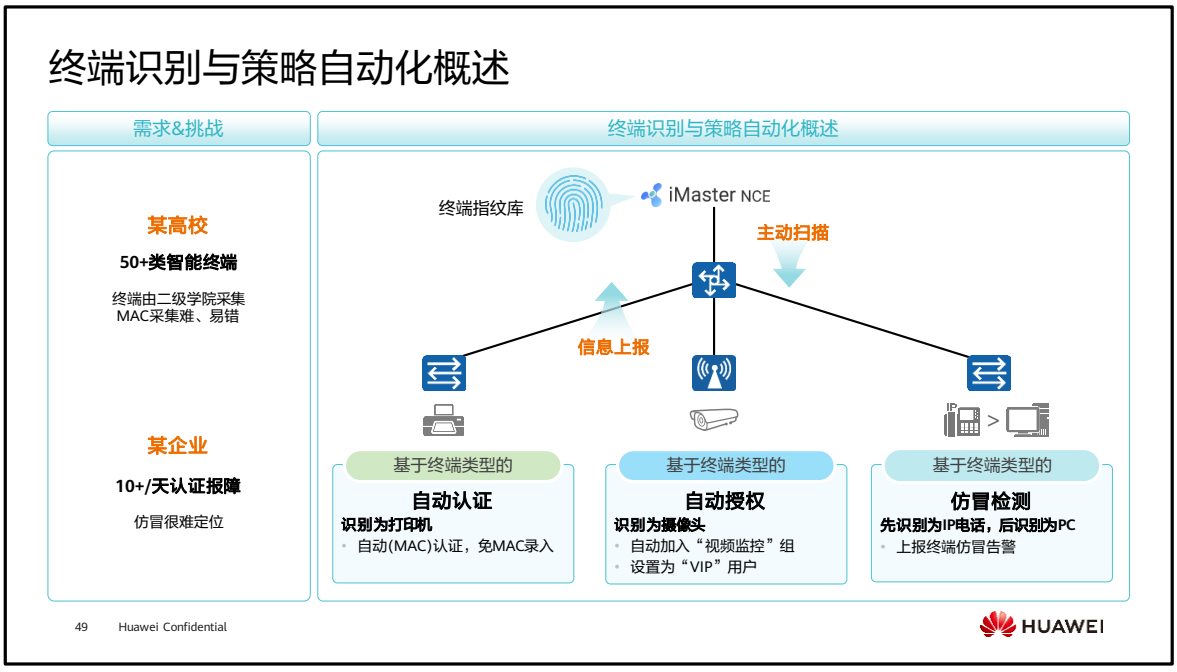
条件：基于5W1H的策略

用户/用户组/角色	用户身份 Who
站点、区域、设备组、设备类型、设备、SSID、IP地址	接入位置 Where
按星期/时间	接入时间 When
PC/IOS/Android等	终端类型 What
公司/自带终端	设备属性 Whose
有线/无线 Portal、MAC、802.1x认证方式等	接入方式 How

智能策略引擎

结果：精细化的权限控制

权限	VLAN/ACL/安全组，VIP用户...
带宽	上行带宽/下行带宽，DSCP
QoS	高/中/低 流量时长管控（仅Portal）
应用	应用组/应用
安全	URL过滤

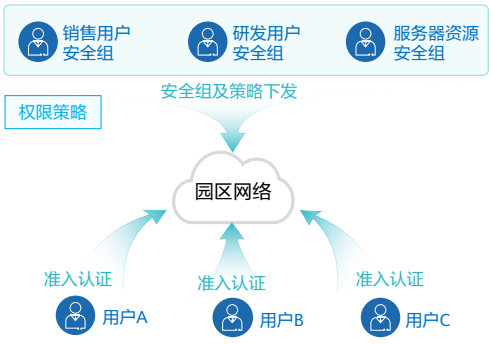


- 园区网络中，接入终端除了智能终端（PC、手机），还有哑终端IP话机、打印机、IP摄像头等哑终端。当前园区网络终端管理主要面临以下两个问题：
  - 当前网络管理系统只能查看接入终端的IP和MAC，并不知道终端具体是什么设备，无法对网络终端做更精细的管理。
  - 不同类型的终端，需部署的网络业务配置和策略也不同，管理员需要手动为每种类型的业务终端配置不同的业务配置和策略，业务部署复杂且操作繁琐。
- 为了解决如上两个场景问题，华为推出了终端识别与策略自动下发方案，可支持如下功能：
  - 通过iMaster NCE-Campus可查看全网终端类型、系统等分类，比如哑终端：打印机、IP摄像头、一卡通、门禁等，并基于终端的类型进行分类统计和流量呈现。
  - 针对园区IP话机、打印机、IP摄像头等哑终端设备，无需管理员手动为每种类型的业务终端配置不同的业务配置和策略。iMaster NCE-Campus能够自动的识别终端，并为终端设备下发对应的准入策略和业务配置。

目录

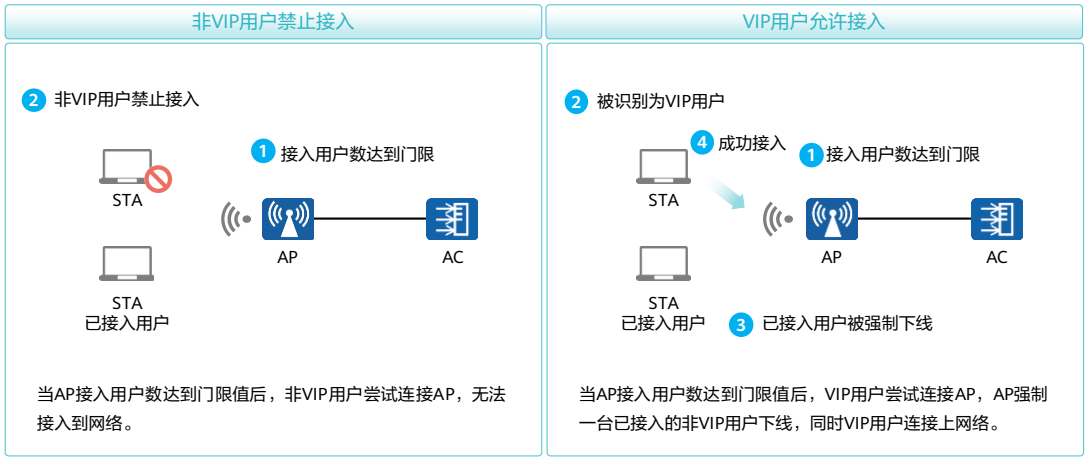
业务随行，基于安全组的策略管理

- 业务随行：不管用户身处何地，使用哪个IP地址，都可以保证该用户获得相同的网络权限，对其执行对应的用户策略。



1. 引入安全组，安全组即拥有相同网络访问策略的一组用户。
2. 定义基于安全组的权限控制策略、用户体验策略，将策略下发到网络设备。
4. 用户的流量进入网络后，网络设备根据流量所述的源、目的安全组执行策略。
3. 用户执行准入认证后，获得授权的安全组。

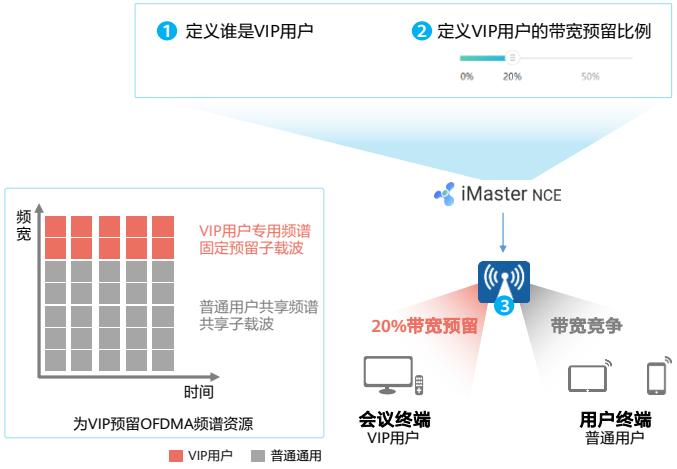
VIP用户优先接入



HUAWEI

- 在一些用户密集的场景（如：展会、球场），为了提升用户的业务体验，对射频和VAP的接入用户数做了限制，同时部署了VIP用户优先接入功能，保障用户接入数达到门限值时，VIP新用户仍然可以正常接入，提升了VIP用户的用户体验。
- 识别VIP用户：
  - 设备通过判断用户是否在VIP用户组内来识别是否是VIP用户。用户授权结构增加优先级字段，VIP用户绑定VIP用户组，下发授权后，VIP用户组内的用户继承该优先级。
- VIP用户接入优先：
  - 在设备上配置VIP用户优先接入，当接入用户数达到VAP最大用户数或用户CAC门限时，如果再有新用户接入到网络，该用户先进行认证，认证成功后，在授权阶段判断该用户是否是VIP用户，如果是，则允许该用户接入并替换一个非VIP用户，强制该非VIP用户下线；如果不是，则强制该用户下线。
  - Portal认证场景，对于预连接状态的用户无法判断其用户优先级，这些用户将被作为高优先级用户处理，VIP新用户接入替换时，不会替换这些用户。
- VIP用户业务优先：
  - 在用户授权过程中，当用户被标记为VIP用户后：VIP用户业务不会被限速；VIP用户业务优先调度；优先级重标记。

VIP带宽预留：保障VIP终端的带宽需求



场景

会议室内用户突增，用户的移动终端抢占WLAN空口资源，导致会议终端的无线体验下降

需求

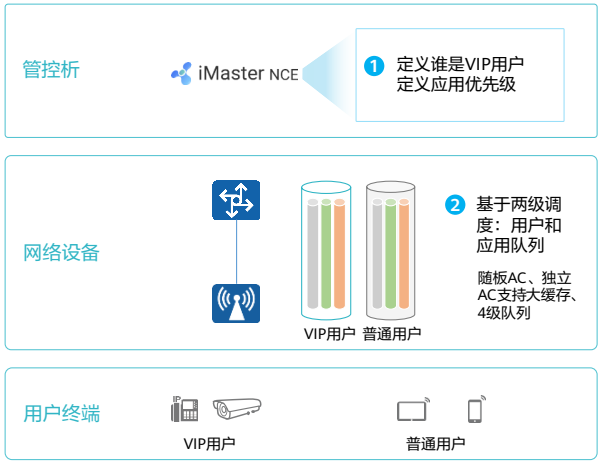
识别VIP用户，保障VIP终端的带宽需求

解决方案

- 为VIP预留OFDMA频谱资源
- 按需预留：
  - 当AP无VIP用户时，不会预留
  - 仅为VIP用户预留足够多的资源

HUAWEI

智能HQoS：用户和应用双因素的QoS策略



挑战

- 传统QoS基于端口带宽进行调度，流量管理可以基于服务等级进行业务区分，难基于用户进行区分。
- 传统QoS无法同时对多个用户的多个业务进行流量管理和调度。

解决方案

- HQoS（Hierarchical Quality of Service）既能区分用户流量又能根据用户业务的优先级进行调度。
- HQoS通过多级队列进一步细化区分业务流量，对多个用户、多种业务等传输对象进行统一管理和分层调度。

目录

智能运维全景图

故障预测 & 自治自愈	自治自愈	高干扰错时自动调优		
	故障预测	光模块故障预测		
故障识别 & 根因分析 *Big Data & ML*	群障分析	四大类Issue分析： 基于规则引擎的快速根因分析		网络拨测 面向接入业务
	个障分析	接入分析： 协议回放	体验分析： 质差用户分析	应用分析： 音视频应用质量感知
体验可视 *Telemetry*	体验可视	全网质量评估体系 WiFi信号热图	每用户旅程回放	有线无线一体化拓扑 WLAN调优可视可对比

CampusInsight： 云化部署 单机部署 集群部署

智能识别四类典型问题（1）

类型	名称	描述
连接类	认证失败（无线+有线）	认证类问题以认证控制点为统计维度，统计一段时间内认证失败/认证超时/认证慢人数与总认证人数的对比值，当此对比值超过学习阈值（此阈值基于历史认证数据学习产生）后，则命中认证控制点认证类问题
	认证超时（无线+有线）	
	认证慢（无线+有线）	
	关联失败（无线）	关联类问题以AP为统计维度，统计一段时间内关联失败/关联慢人数与总关联人数的对比值，当此对比值超过学习阈值后（此阈值基于历史关联数据学习产生），则命中AP关联类问题
	关联慢（无线）	
	DHCP失败（无线+有线）	DHCP类问题以认证控制点为统计维度，统计一段时间内DHCP失败/DHCP慢人数与总DHCP人数的对比值，当此对比值超过学习阈值（此阈值基于历史认证数据学习产生）后，则命中认证控制点DHCP类问题
	DHCP慢（无线+有线）	

智能识别四类典型问题（2）

类型	名称	描述
性能类	弱覆盖（无线）	统计每个AP下历史接入用户的信号强度，如果某个AP下大部分接入用户信号较弱，且持续时间较长，则认为此AP周边存在弱覆盖问题
	高干扰（无线）	统计一段时间内受到同频、邻频、非WIFI频段等各种信号干扰的射频超过学习阈值（基于每个射频历史干扰数据学习产生），并持续一段时间，则命中高干扰问题
	高信道利用率（无线）	统计一段时间内射频持续处于繁忙状态，包括正常WIFI数据传输对信道频段占用，以及信号干扰对信道频段占用，如果利用率的占用超过学习阈值（基于每个射频的历史信道利用率干扰数据学习产生），并持续一段时间，则命中高信道利用率问题
	空口拥塞（无线）	以射频为统计维度，如果射频上需要传输的数据过多产生积压，导致用户数据出现延迟或丢弃。如果射频上持续出现积压超过动态阈值，则命中空口拥塞问题
	非5G优先接入（无线）	以同时广播2.4G、5G两个频段的AP为统计维度，统计其下一段时间内接入的支持5G频段的终端，是否时常接入2.4G频段，导致用户时延较大。如果此AP下持续出现此场景，则命中非5G优先接入问题
	终端容量（无线）	以AP为统计维度，统计长时间内AP持续接入大量用户，且接入用户数超过学习阈值（基于AP历史接入的用户数学习产生），则命中终端容量

智能识别四类典型问题（3）

类型	名称	描述
漫游类	乒乓漫游（无线）	统计两个AP在短时间内，其下用户在AP间产生多次漫游记录，且漫游前后用户关键指标较差。如果漫游次数达到学习阈值，则判定两AP产生乒乓漫游问题
	漫游异常（无线）	按天统计每个AP的漫游异常事件（漫游失败、漫游耗时过长等），如果异常事件数达到学习阈值，判定此AP周边存在漫游异常
设备类	AP离线（无线）	设备类问题以设备为统计维度，统计设备级别指标异常，并持续时间达到学习阈值，则命中设备类问题
	设备离线（无线+有线）	
	PoE供电故障（有线）	
	转发表项超限（有线）	
	高CPU利用率（无线+有线）	
	高内存利用率（无线+有线）	
	CPU CAR丢包（有线）	

思考题

1. 华为网络准入控制方案支持基于5W1H的策略，其中Whose代表(　　)。

   A. 终端类型

   B. 接入方式

   C. 用户身份

   D. 设备归属

- D

本章总结

- 华为智简园区（CloudCampus）致力于为企业构建一张超宽、智慧、极简、安全、开放的基于业务意图的园区网络。
- 华为CloudCampus解决方案从超宽联接、极简网络、一网多用、智能策略、智能运维等多个维度提升了园区网络的部署效率，用户体验以及整网性能。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

CloudCampus大中型园区网络方案

设计基于VXLAN的虚拟化园区网络

HUAWEI

前言

- 华为CloudCampus智简园区网络解决方案基于智简网络意图驱动的理念，在云和SDN基础上，引入大数据分析和AI等技术，帮助企业构建一张智能、极简、融合、开放和安全的网络。
- 本课程主要针对大中型园区网络，即通常指具备2000终端以上的接入管理能力的网络。为了支持大量终端接入，接入层需要提供高密度有线端口和大量无线接入的AP设备，并且能够根据终端类型进行差异化接入控制。为了保证业务可持续性，同时要能支持虚拟网络、业务随行等高级能力。

目标

- 学完本课程后，您将能够：
  - 描述大中型园区网络的需求与挑战
  - 描述CloudCampus大中型园区网络层次与网络架构
  - 描述园区网络Underlay、Fabric及Overlay的概念及关系
  - 根据实际需求完成基于VXLAN的虚拟化园区网络的Underlay网络设计
  - 根据实际需求完成基于VXLAN的虚拟化园区网络的Fabric及Overlay网络设计
  - 根据实际需求完成基于VXLAN的虚拟化园区网络WLAN业务设计、准入认证设计及运维管理设计

目录

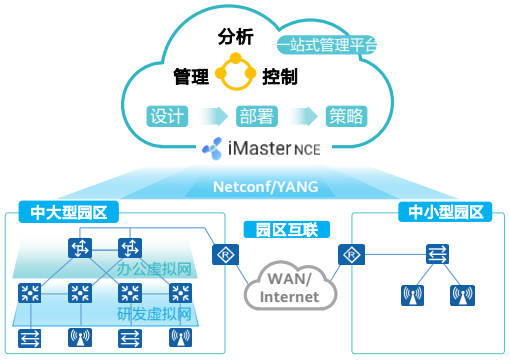
大中型园区网络的业务需求与挑战

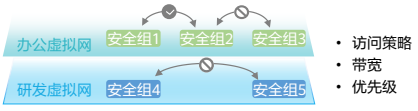
- 移动化、大数据、人工智能、物联网和云计算等新技术正加速各行业数字化转型与升级。数字化转型也对企业的可持续发展产生了巨大影响。企业园区网络作为企业数字化转型的基石，随着BYOD移动办公、云计算、SDN软件定义网络、物联网、人工智能以及大数据等概念的持续升温，新技术、新应用层出不穷，这些应用和业务进入企业园区，给传统园区网络带来了很多挑战。

融合承载	用户体验感知	网络自动化
需求： 接入终端及业务多样化，需要融合承载的园区网络。 **挑战：** • Wi-Fi及IoT等业务各自独立规划、部署、管理，网络总体建设成本高。 • 网络管理、运维工作量大。	**需求：** 网络运维需自动化、智能化，随时随地感知用户体验。 **挑战：** • 无法第一时间感知业务故障。 • 故障发生后更多是依赖专业人员的运维经验判定业务故障原因，故障无法快速定位。 • 网络无法实现自主优化。	**需求：** 应用和业务激增带来的部署、策略复杂性，网络需实现自动化。 **挑战：** • 重复工作量大，手工配置繁琐。 • 新业务上线需逐台设备进行配置，周期长，成本高。 • 网络策略部署与调整工作量大。

华为CloudCampus智简园区网络解决方案

- 华为CloudCampus解决方案基于智简网络（Intent-Driven Network，IDN）意图驱动的理念，在云和SDN基础上，引入大数据分析和AI等技术，帮助企业构建一张智能、极简、融合、开放和安全的网络。





- 访问策略
- 带宽
- 优先级

HUAWEI

- 有线、无线与物联网融合，满足接入终端及业务多样化。
  - 华为园区交换机（S系列交换机）通过融合无线接入控制器AC（Access Controller），实现有线无线深度融合，为用户提供有线和无线一致化的管理和体验。华为AP支持IoT模块，AP与IoT基站合一，实现Wi-Fi & IoT网络融合极简管理。通过融合用户认证和管理功能，及策略联动功能，为有线无线用户提供统一认证和接入策略控制，管理员可以获得一致的用户管理体验，简化有线无线网络的运维管理。
- 全场景WLAN，满足客户差异化的接入需求。
  - 针对普通室内、高密场馆、室外场景以及密集房间等多种场景，华为提供最新Wi-Fi 6 AP、高密AP和分布式Wi-Fi方案，实现高密度无死角的WLAN覆盖以及接入体验保障，部署便捷，节约投资成本。
  - Wi-Fi 6是第6代Wi-Fi，标准吸纳了大量5G关键技术，如OFDMA、MU-MIMO、1024 QAM等。Wi-Fi 6相比Wi-Fi 5实现网络带宽提升4倍，并发用户数提升4倍，网络时延从平均30ms降低至20ms，可以轻松应对有超大带宽、超高密接入、超低时延要求的应用场景，如4K超高清视频会议（超大带宽）、高密场馆（超高并发）、VR（超低时延）等应用场景。华为依托于对5G技术的深厚理解和掌握，也成为了Wi-Fi 6标准的主要贡献者，公司专家担任了5个Wi-Fi国际标准工作组主席职位。
- 光电混合交换机 & 300米PoE++，更高带宽，更灵活的网络部署。
  - 随着802.11ax标准及产品的问世，无线终端接入速率已超过1Gbps，千兆端口接入已无法满足。华为提供光电混合交换机，搭配光电混合缆为AP提供300米远距PoE++供电传输。

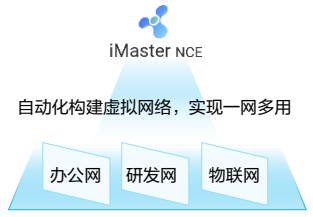
CloudCampus：极简的园区网络部署

物理网络自动化

通过iMaster NCE-Campus图形化界面完成：

1. 设备即插即用自动化开局
2. Underlay网络路由编排
3. 互通性配置
4. 实现自动化部署

虚拟网络自动化



通过iMaster NCE-Campus图形化界面完成：

1. 统一部署Fabric基于BGP-EVPN 的控制面，自动建立VXLAN 隧道。
2. 实现全自动化的虚拟化网络建设。
3. 业务集中式配置，实现业务自动发放。

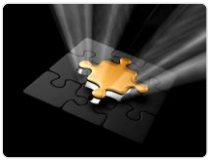
用户策略自动化

通过iMaster NCE-Campus图形化界面完成：

1. 基于图形化界面规划用户组及组间策略。
2. 策略自动下发。
3. 业务随行，不论用户在什么位置接入，都将获取统一的策略和一致的业务体验。

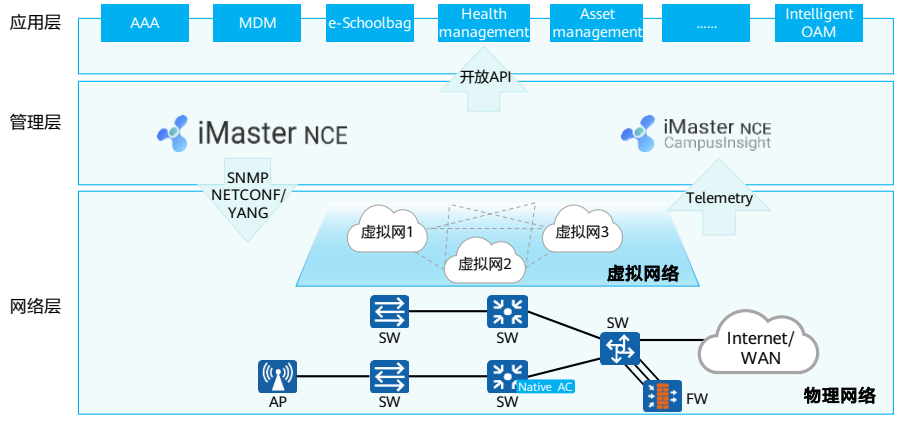
CloudCampus：智能的园区网络运维

- 华为CloudCampus解决方案引入iMaster NCE-CampusInsight（园区网络分析器），颠覆传统聚焦资源状态的监控方式，实现按照用户、应用、时间维度的数据可视，以及实现潜在故障识别和根因定位，提升用户体验。

每时刻、每用户全旅程体验可见	网络问题自动识别	网络问题智能定界，分析根因
		
1. iMaster NCE-CampusInsight采用业界标准的Telemetry技术，动态秒级抓取网络KPI数据，故障可回溯。 2. 通过多维度采集数据，实时呈现每个用户的网络画像，全旅程网络（谁、何时、连接至哪个AP、体验、问题）可视。	1. 通过大数据和AI技术，自动识别连接类、空口性能类、漫游类和设备类问题，提升潜在问题识别率到85%。 2. 利用机器学习历史数据动态生成基线，通过和实时数据对比分析，从而预测可能发生的故障。	1. 基于网络运维专家系统和多种AI算法，智能识别故障模式以及影响范围，协助管理员定界问题。 2. 基于大数据平台，分析问题可能发生的原因并给出修复建议。

CloudCampus网络架构（大中型园区场景）

- CloudCampus解决方案在大中型园区场景的网络架构如图所示，分为网络层、管理层和应用层。



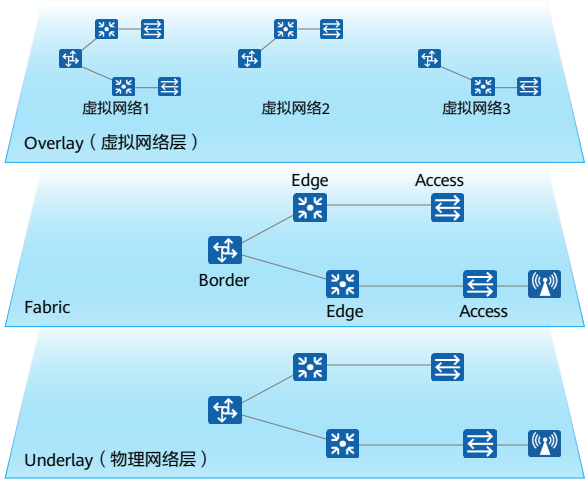
HUAWEI

- 网络层
  - 引入虚拟化技术，把网络层分为物理网络和虚拟网络。
    - 物理网络：又称为Underlay网络，为园区网络提供基础连接服务。为了适应多类型终端的接入需求，物理网络提供统一的三网融合接入能力，可以同时接入有线终端、无线终端和IoT（Internet of Things，物联网）终端。
    - 虚拟网络：又称为Overlay网络，通过虚拟化技术，在物理网络上构建出一张或者多张虚拟的Overlay网络，业务策略被部署在虚拟化网络上，与物理网络脱离，从而将业务的复杂度和网络的复杂度相互解耦。虚拟网络可以有多张，服务于不同的业务，或者服务于不同的客户群。
- 管理层
  - 管理层为网络提供配置管理，业务管理，维护和故障检测、安全威胁分析等管理能力。传统园区网络中，使用网管系统进行网络管理，网管系统虽然能够呈现网络状态，但是缺乏灵活性和自动化能力。如果业务需求发生变动，需要管理员对业务进行规划，然后手工重新修改相应网络设备（路由器、交换机、防火墙）上的配置。这种手工调整的方式效率低且容易出错。在快速变化的业务环境下，网络的灵活性非常关键，需要有自动化的工具来协助管理网络和业务。CloudCampus采用iMaster NCE-Campus实现网络和业务的自动发放。

    - iMaster NCE-Campus实现了对设备、应用的抽象，允许应用通过编排、调用抽象模型，快速实现应用的开发和自动部署。通过iMaster NCE-Campus，我们面对的不再是独立的若干个设备（例如：交换机、路由器、AP等）和设备上的离散的配置（例如访问控制策略、QoS策略、路由策略），而是对外呈现出完整的网络概念。

- 应用层
    - CloudCampus解决方案基于iMaster NCE-Campus提供了标准化接口，通过开放API接口将网络识别的用户身份、网络资源、业务质量、网络中的位置信息、网络拓扑等多种信息，对上层业务开放，通过这些标准化的开放接口，第三方可以根据自身业务需求量身定制业务创新应用，满足在教育、商业、企业、政府等多个领域的业务需求。

VXLAN虚拟园区网络层次及概念



- 可以根据业务需求创建多个虚拟网络，实现业务隔离。
- 通过VXLAN实现L2及L3通信。

- 通过虚拟化技术，构建基于任意物理拓扑的逻辑拓扑。
- 在Fabric上创建业务网络，与物理网络解耦。

- 由物理设备建立的物理网络。
- 为园区内所有业务提供互联互通能力。
- 业务数据转发的基础承载网。

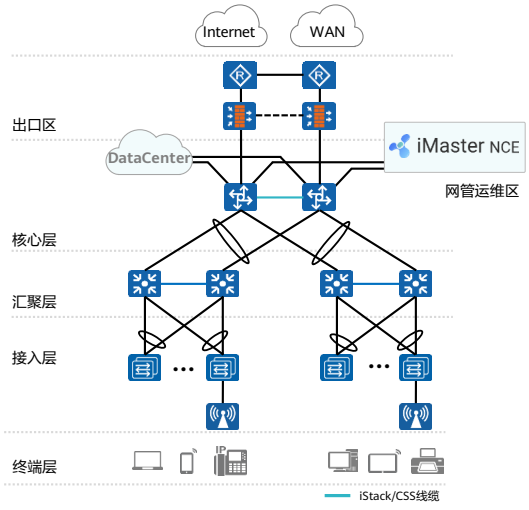
HUAWEI

- 物理网络层（Underlay）：是由实体网络设备（如交换机、AP、防火墙、路由器等）建立的物理拓扑组网，为园区所有业务提供互联互通的能力，是园区业务数据转发的基础承载网络。
- Fabric：是通过虚拟化技术（VXLAN）构建在物理Underlay拓扑之上的全互联逻辑拓扑。业务网络在Fabric上创建，从而实现业务网络与物理网络的解耦，当业务网络需要调整变化时，不需要改变物理网络的拓扑结构。
- 虚拟网络层（Overlay）：是在物理层基础上通过虚拟化技术抽象出来的，将物理层网络资源进行池化处理，让业务层可按需调度的网络资源池。VN（Virtual Network，虚拟网络）是在Fabric上基于业务需求创建多个虚拟网络，实现业务隔离。传统园区网络为了实现业务隔离，办公网和安防网是独立的两套物理网络，在虚拟化网络中，通过虚拟网络层实现物理网络的共享，通过创建两个VN即可实现在一套物理网上创建业务隔离的办公网和安防网。

目录

Underlay网络设计大纲

网络架构概述



- **出口区：**园区内部网络到外部网络的边界，用于实现内部用户接入到外部网络，外部用户（包括客户、合作伙伴、分支机构、远程用户等）接入到内部网络。网络安全及广域网接入方案是出口区设计的重点。
- **数据中心区：**部署服务器和应用系统的区域，为企业内部和外部用户提供数据和应用服务。
- **管理运维区：**部署网络管理服务器（例如网管系统、认证服务器等）的区域。
- **核心层：**园区网骨干，是园区数据交换的核心，联接园区网的各个组成部分，如数据中心区、管理运维区、出口区等。
- **汇聚层：**完成数据汇聚或交换的功能，也可以提供一些关键的网络基本功能，如路由、 QoS、安全等。
- **接入层：**为终端用户提供园区网接入功能，是终端接入网络的第一层。
- **终端层：**接入园区网络的各种终端设备位于该层。

HUAWEI

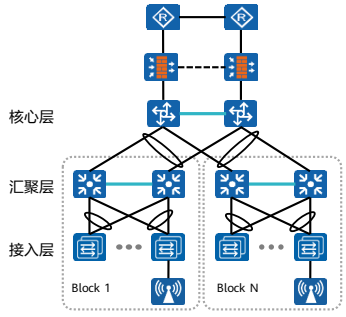
- 大中型园区网络通常采用核心层为“根”的树形网络架构，如图所示，拓扑稳定，易于扩展和维护。园区网络可划分为多个层次：接入层、汇聚层、核心层，以及多个分区：出口区、数据中心区、管理运维区等，各功能分区模块清晰，模块内部调整涉及范围小，易于进行问题定位。
- 终端层：
  - 终端层是指接入园区网络的各种终端设备，例如电脑、打印机、IP话机、手机、摄像头等。
- 接入层：
  - 接入层为用户提供各种接入方式，是终端接入网络的第一层。接入层通常由接入交换机组成，接入层交换机在网络中数量众多，安装位置分散，通常是简单的二层交换机。如果终端层存在无线终端设备，接入层需要无线接入点AP设备，AP设备通过接入交换机接入网络。
- 汇聚层：
  - 汇聚层是接入层与园区核心骨干网之间的网络分界线，主要用于转发用户间的“横向”流量，同时转发到核心层的“纵向”流量。汇聚层可作为部门或区域内部的交换核心，实现与区域或部门专用服务器区的连接。另外汇聚层还可以扩展接入终端的数量。

- 核心层：
    - 核心层是园区数据交换的核心，连接园区网的各个组成部分，如数据中心区、汇聚层、出口区等，核心层负责整个园区网络的高速互联。网络需要实现带宽的高利用率和网络故障的快速收敛，通常需要部署高性能的核心交换机，通常三个以上部门规模的园区网建议规划核心层。针对无线网络，核心层包括AC，无线终端通过AP接入网络后，AP通过CAPWAP（Control and Provisioning of Wireless Access Points，无线接入点控制协议）隧道和AC建立通信机制。
- 出口区
    - 园区出口是园区内部网络到外部网络的边界，内部用户通过出口区接入到外部网络，外部网络的用户通过出口区接入到内部网络。出口区一般需要部署出口路由器和防火墙。路由器解决内外网互通问题，防火墙提供边界安全防护能力。
- 数据中心区
    - 数据中心区是管理业务服务器（例如文件服务器、邮件服务器等）的区域，为企业内部和外部用户提供业务服务。
- 管理运维区
    - 管理运维区是管理网络服务器（例如网管系统、认证服务器等）的区域。标准的网管系统通过SNMP（Simple Network Management Protocol，简单网络管理协议）和网络设备交互，能够提供配置、管理和维护功能。
- 此外，园区中可能还会有DMZ（Demilitarized Zone，半信任区）区，DMZ区为外部访客（非企业员工）提供访问业务，通常将公用服务器部署在该区域，其安全性受到严格控制。

网络架构设计

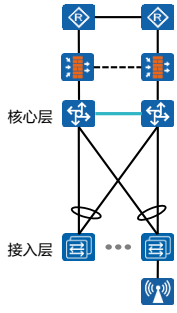
- 在实际应用中，可以根据网络规模或业务需要灵活选择三层、二层或一层架构。

三层架构



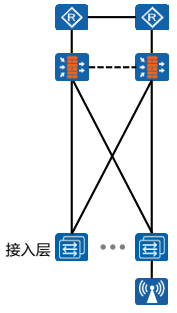
适用场景：用户规模较大，或涉及多栋楼的大型园区网络（例如高校园区网）的大型园区。

两层架构



适用场景：涉及一栋楼的中小型园区网络。

一层架构



适用场景：用户规模比较小的小型园区或分支机构。

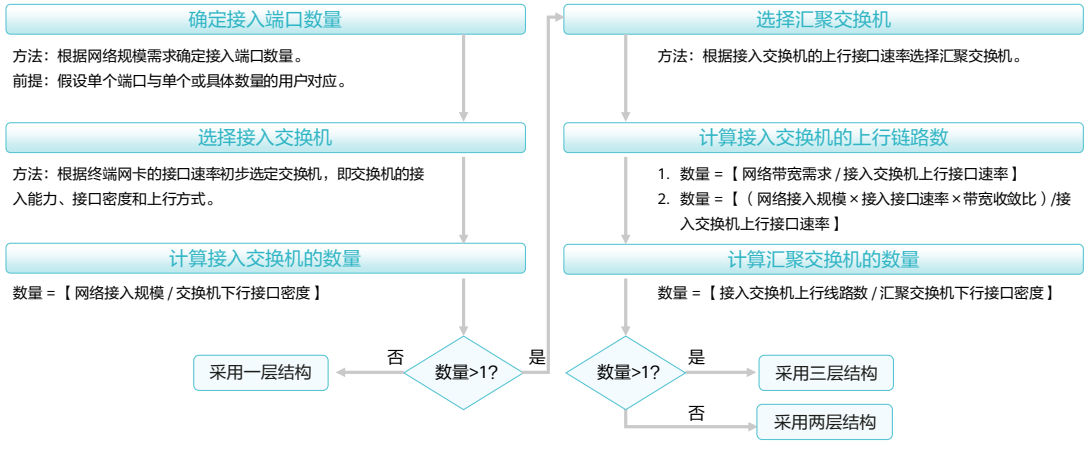
- 层次化设计
- 模块化设计
- 冗余设计
- 对称性设计

HUAWEI

- 层次化设计：
  - 每层可以看作为是园区网内一个具有特定角色和功能的、结构定义良好的模块，层次化的设计结构，易于扩展和维护，降低了设计的复杂度和难度。
- 模块化设计：
  - 每个模块对应一个部门、功能或业务区域，可根据网络规模灵活扩展，部门或区域内部调整涉及范围小，容易进行问题定位。
- 冗余设计：
  - 双节点冗余性设计可以保证设备级可靠，适当的冗余提高可靠性，但过度的冗余也不便于运行维护。如果无法实现双节点冗余设计，对框式的核心交换机或者出口路由器，可以考虑单板级的冗余，如双主控板，双交换网板。另外，关键链路可以采用Eth-Trunk链路实现链路级可靠性。
- 对称性设计：
  - 网络的对称性便于业务部署，拓扑直观，便于协议设计和分析。

分层模型设计

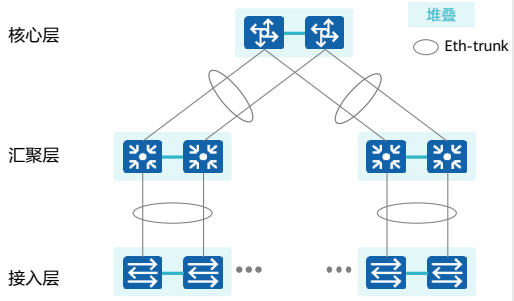
- 网络设计时，一般会根据网络规模采用自底向上的方法来确定采用基层架构。



- 根据网络规模确定接入交换机的端口数量，一般情况下，假设一个端口对应一个终端或一个网络接入点（如无线AP）。
- 根据终端网卡的接口速率初步确定交换机。
- 计算接入交换机数量，接入交换机数量=【接入端口数量÷接入交换机的下行端口密度】。如果数量大于1，继续选择汇聚交换机；否则就可以采用一层架构。
- 根据接入交换机的上行端口速率选择汇聚交换机。
- 计算接入交换机的上行线路数量，有如下两种计算方法：
  - 根据网络带宽计算：上行线路数量=【网络带宽÷接入交换机的上行端口速率】
  - 根据网络规模计算：上行线路数量=【接入端口数量x接入端口速率x带宽收敛比÷接入交换机的上行端口速率】
- 计算汇聚交换机数量，汇聚交换机数量=【接入交换机的上行线路数量÷汇聚交换机的下行端口密度】。如果数量大于1，采用三层架构；否则可以采用两层架构。
- 上面计算方法中的“【 】”表示计算结果取整数偏大值。

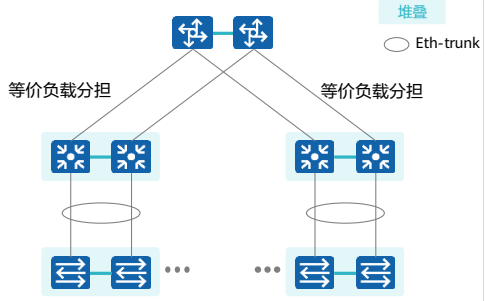
分层组网设计

堆叠核心组网



无环组网，不需要复杂的环网协议和可靠性协议设计，保证了网络设备级和链路级可靠性的同时，简化了网络拓扑，减少了部署和维护工作量。

双核心组网

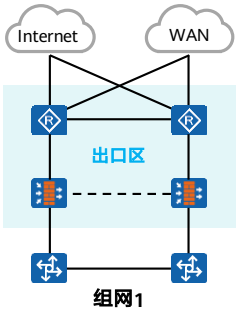


堆叠组网从业务角度看只有一个核心；双核心组网，从业务角度看有两个核心，汇聚层可以同时有两条到核心的等价路由，核心设备升级过程中可以保证业务不中断。

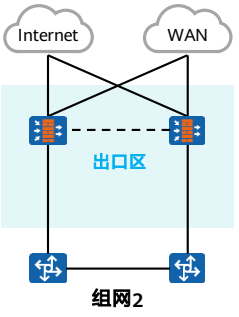
- 从简化运维角度，推荐采用堆叠核心组网，如果客户对业务中断很敏感，建议使用双核心组网。
- 大中型园区二层组网常用的组网类型是堆叠核心组网。

网络出口设计

- 园区出口区一般需要部署出口路由器和防火墙。路由器解决内外网互通的问题，防火墙提供边界安全防护能力。为了保证可靠性，路由器和防火墙通常采用设备冗余部署。大中型园区推荐出口部署设备冗余备份。
- 根据是否需要部署路由器，通常有两种组网模型：



组网1



组网2

组网模型选择

出口链路类型：

- Ethernet类型，选择组网2。
- EI、CE1、CPOS等非以太网的链路，选择组网1。

SD-WAN需求：

- 有SD-WAN需求，选择组网1，且配套AR路由器。
- 无SD-WAN需求，选择组网2。

协议对接需求：

- 如果出口设备与外部网络运行BGP，考虑到路由器的路由表规模和性能更强大，同时考虑到在出口设备上需要部署许多路由策略，建议选择组网1。

VLAN设计

- VLAN编号建议连续分配，以保证VLAN资源合理利用。
- 建议预留一定数量的VLAN以方便后续扩展。
- VLAN划分需要区分业务VLAN、 管理VLAN和互联VLAN。
- 最常用的划分方式是基于接口的方式进行划分，根据不同的设计原则，将接入交换机不同接口划分到不同的VLAN，从而实现不同业务类型用户的隔离需求。

HUAWEI

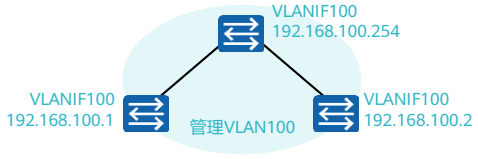
- 业务VLAN：
  - 通常可以按照逻辑区域、地理区域、人员结构和业务类型分层规划VLAN。
  - 如用户对语音的时延比较敏感，需要优先保证语音，建议针对语音业务规划Voice VLAN功能，华为交换机可以自动识别语音流，将语音流加入到Voice VLAN中传输，并进行有针对性的QoS保障，当网络发生拥塞时可以优先保证语音流的传输。
  - 如果不同的用户有相同的组播数据业务，建议规划组播VLAN，将用户VLAN和组播VLAN绑定，这样可以避免上游网关在多个用户VLAN复制组播数据流。
  - 业务VLAN不建议采用VLAN1。
- 管理VLAN：
  - 二层交换机建议规划管理VLAN，并将管理VLAN的VLANIF接口作为管理接口，网管设备通过该接口来管理交换机；建议所有二层交换机使用同一个管理VLAN。
  - 三层设备（网关及以上设备）建议使用业务口作为管理接口，不需要专门规划管理VLAN。
- 互联VLAN：
  - 互联VLAN一般用在两台三层交换机之间或三层交换机与路由器之间，创建VLANIF接口进行三层互联。

网络架构及拓扑设计 > 基础业务设计 > LAN自动化设计

IP地址设计

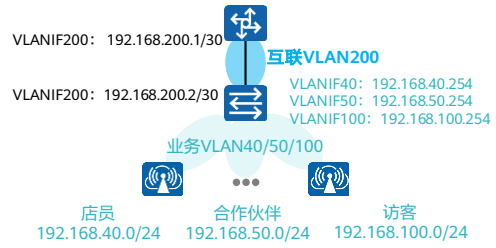
- 园区网的IP地址主要分为业务IP地址、管理IP地址和互联IP地址。

管理IP地址



二层设备使用VLANIF地址作为管理IP地址，建议网关以下的所有二层交换机使用同一IP网段。

业务IP及互联IP地址



业务IP地址是服务器、主机以及网关的IP地址。

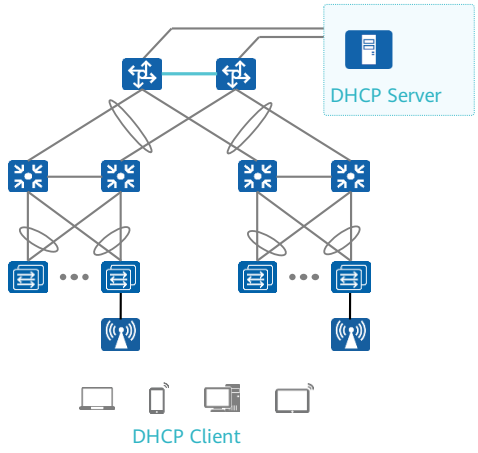
- 网关IP地址推荐统一使用相同的末位数字，如.254。
- 各业务IP地址范围要清晰区分，每一类业务终端IP地址连续、可聚合。
- 建议使用掩码为24位的IP地址段。

互联IP地址推荐使用30位掩码的IP地址，核心设备可使用主机地址较小的IP地址。

HUAWEI

- IP地址的规划建议遵循如下原则：
  - 唯一性：一个IP网络中不能有两个主机采用相同的IP地址。
  - 连续性：同一业务的节点地址要连续，便于路由规划和汇总。连续的地址便于路由聚合，可以减小路由表的大小，加快路由计算和收敛速度。
  - 扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时无需新增地址段及路由条目。
  - 易维护：设备地址段、各业务地址段清晰区分，易于后续基于地址段实施统计监控、安全防护等策略。IP地址的规划也可以与VLAN的规划对应起来。
- 三类IP地址设计中其他注意点：
  - 业务IP地址：考虑到广播域范围及规划的简易程度，建议为每个业务地址段预留掩码为24位的IP地址段，如果业务终端超出200个，再为其顺延一个掩码为24位的IP地址段。
  - 管理IP地址：三层设备建议规划三层接口用于管理和开局，接口地址作为管理IP地址用于和控制器互通或者本地登录。
  - 互联IP地址：互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。

DHCP服务设计



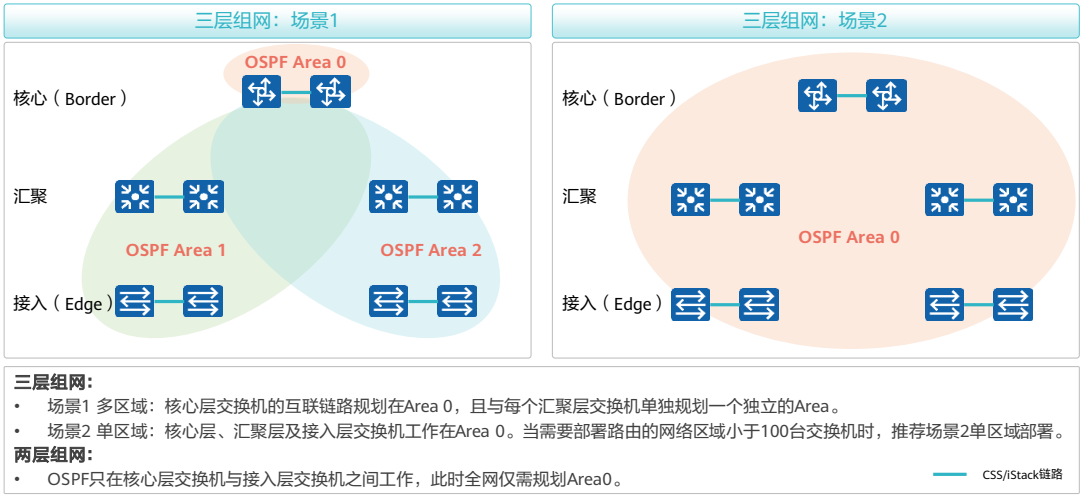
面向终端的DHCP服务

- 建议整个园区规划一个DHCP Server来简化运维。
- 建议在接入层设备配置DHCP Snooping，以避免非法攻击。
- 网络管理员可以根据网络需求为不同的主机选择不同的分配策略：
  - 动态分配机制：为主机分配一个有限期限（租期）IP地址。适用于主机需要临时接入或者IP地址不足的场景，例如企业办事处的出差员工便携机、咖啡厅的移动终端。
  - 静态分配机制：为指定主机分配固定的IP地址。适用于对IP地址有特殊要求的主机，例如DNS Server的地址。
- 地址池规划需要将静态配置的IP地址过滤掉。
- 根据客户端在线时间合理规划租期。
- 大中型园区DHCP服务器和园区主机通常不在同一个网段，建议网关开启DHCP中继功能。

HUAWEI

- 面向网络开局的DHCP服务推荐通过核心交换机提供，在网络开局章节中介绍。

路由设计



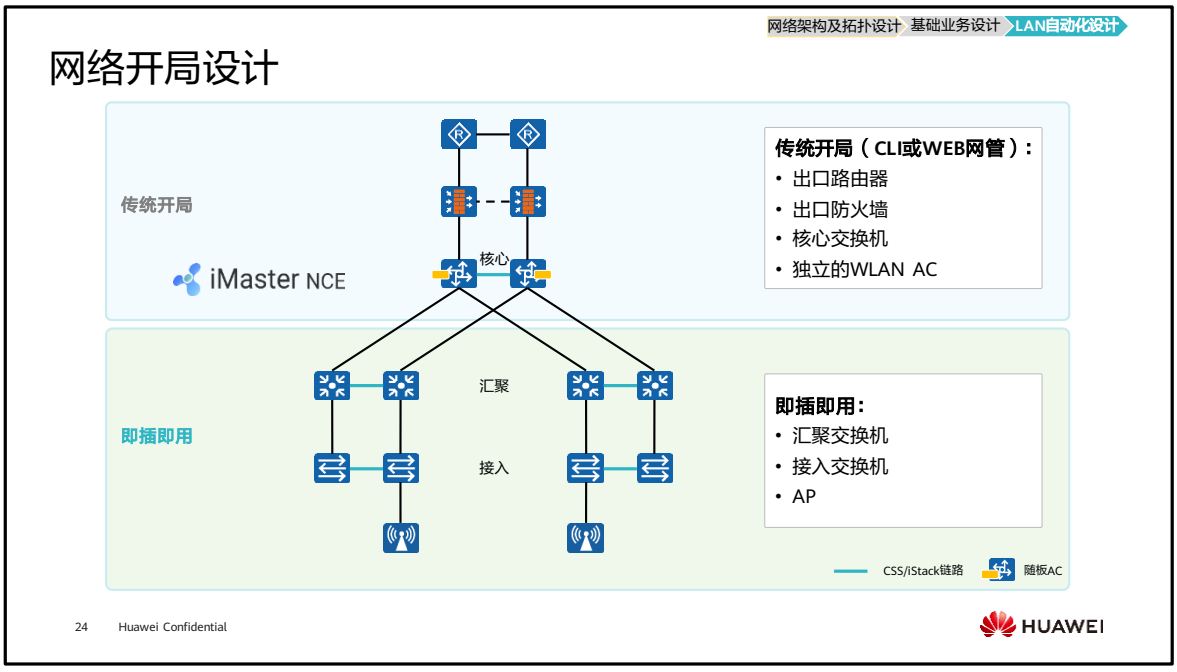
三层组网：
- 场景1 多区域：核心层交换机的互联链路规划在Area 0，且与每个汇聚层交换机单独规划一个独立的Area。
- 场景2 单区域：核心层、汇聚层及接入层交换机工作在Area 0。当需要部署路由的网络区域小于100台交换机时，推荐场景2单区域部署。

两层组网：
- OSPF只在核心层交换机与接入层交换机之间工作，此时全网仅需规划Area0。

CSS/iStack链路

HUAWEI

- 路由设计包括园区内部路由和园区出口路由设计。
  - 内部路由设计：主要满足园区内部设备、终端的互通需求并且与外部路由交互。根据网关位置，建议按照如下两种场景设计内部路由：
    - 网关在汇聚层：核心层、汇聚层都需要部署路由，考虑路由表能够根据网络拓扑变化而动态刷新，推荐规划IGP动态路由协议，如OSPF。
    - 网关在核心层：只需要在核心层配置路由，建议优先采用静态路由。
  - 出口路由设计：
    - 主要满足内部终端访问Internet、广域网的需求。
    - 大中型园区一般企业分支机构众多，出口需要支持多种链路用于Internet访问和企业内部互访，需要大量路由引入园区内部，因此建议规划动态路由协议，如OSPF。
- 园区动态路由协议建议规划OSPF，以下为OSPF设计注意点：
  - Router ID建议采用Loopback接口IP地址。
  - 区域（Area）划分遵循核心、汇聚、接入的分层原则，骨干区域建议包含出口路由器和核心交换机，非骨干区域的设计则是根据地理位置和设备性能而定。

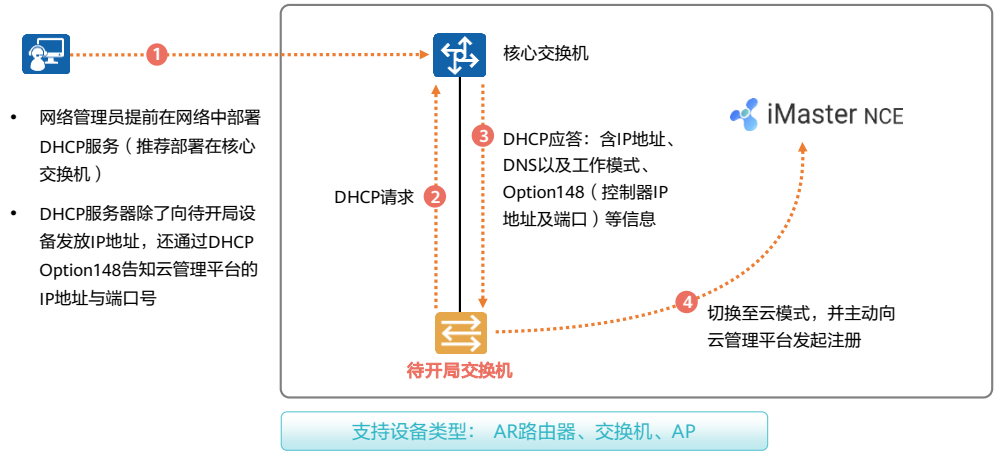


- 大中型园区出口和核心设备通常部署在核心机房，地理位置集中，业务复杂，开局通常需要网络工程师进站调测。因此核心层及核心以上的设备（包含核心层设备，旁挂独立AC设备和出口设备）推荐采用WEB网管开局方式或命令行开局方式。
- 核心以下的设备（包含汇聚层设备、接入层设备和AP）由于数量众多，业务配置相似，从简化部署考虑，推荐即插即用开局。
  - 推荐采用DHCP Option方式的即插即用开局。
  - DHCP Option方式的即插即用开局是指在园区的DHCP服务器上配置为设备提供的IP地址和Option参数（通过Option148配置iMaster NCE-Campus的IP地址，通过Option43配置AC的IP地址），这样，设备上线后自动向DHCP服务器获取管理IP及Option参数，并向iMaster NCE-Campus自动上线注册。核心以下的交换机通过DHCP Option148向iMaster NCE-Campus注册上线，AP通过DHCP Option43向AC注册上线。

网络开局方式推荐

区域	设备	开局推荐	备注
出口	路由器	本地命令行（CLI）或Web网管	-
	防火墙	本地命令行（CLI）或Web网管	-
核心层	核心交换机	本地命令行	-
	独立AC	Web网管	可选DHCP Option148
汇聚层	汇聚交换机	DHCP Option148	可选本地命令行
接入层	接入交换机	DHCP Option148	可选本地命令行
	AP	DHCP Option43	可选本地命令行

网络开局：基于DHCP的网络设备即插即用

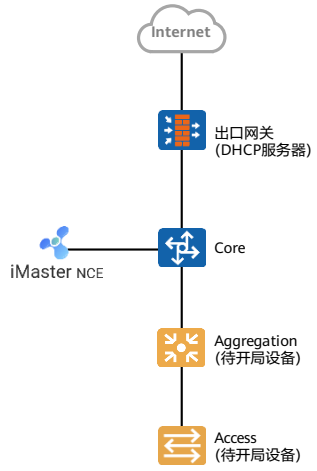


- 网络管理员提前在网络中部署DHCP服务（推荐部署在核心交换机）
- DHCP服务器除了向待开局设备发放IP地址，还通过DHCP Option148告知云管理平台的IP地址与端口号

HUAWEI

- 网络管理员率先部署DHCP服务器，并配置Option148参数，在参数中写入模式类型（云化模式）、控制器的域名或地址及端口号信息，网络设备通过DHCP获取这些信息后，即可自动注册到控制器。
  - 租户的站点核心交换机可作为DHCP服务器，管理员手工配置其DHCP Server功能，并配置Option148参数。有条件时，也可使用第三方DHCP服务器。
  - 站点内的网络设备启动后，通过DHCP获取IP地址等参数，并通过Option148获得运行模式、控制器的IP地址及端口号等参数，设备自动重启并切换为云模式，然后再次申请地址。已经处于云模式的设备获取地址后，自动向控制器发起注册申请。

网络开局流程：设备先上线，再完成规划



准备工作

- 管理员在出口网关部署DHCP服务器功能（或部署一台单独的DHCP服务器），配置Option 148。
- 管理员配置Core，使其被iMaster NCE纳管。

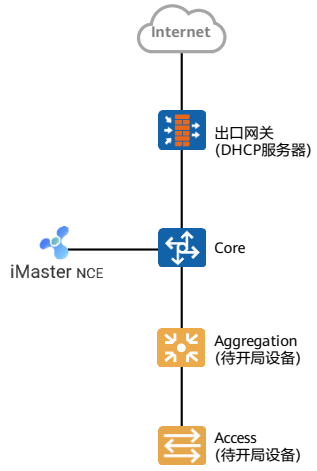
交换机的上线过程

1. Aggregation加电，主动发送LLDP报文与Core协商，获取PnP VLAN。
2. Aggregation使用PnP VLAN向DHCP服务器获取IP地址、Option 148参数。
3. Aggregation根据从DHCP服务器获取到的iMaster NCE信息，向其注册。
4. Access交换机加电后的工作过程类似（与步骤1-3类似）。
5. 管理员将交换机的信息（SN号、设备型号等）导入到iMaster NCE（可批量导入）。
6. 交换机通过LLDP发现网络拓扑，并各自将拓扑信息上报iMaster NCE（通过NETCONF），iMaster NCE可根据这些信息发现网络拓扑。
7. 管理员在iMaster NCE上对网络进行规划、配置发放。

HUAWEI

- 在华为CloudCampus解决方案中，通过DHCP服务器可以实现交换机的即插即用，无需在交换机上手动使能NETCONF功能和配置iMaster NCE-Campus地址。
  - 交换机空配置启动后，先使用VLAN 1主动向DHCP服务器发起请求。
  - 用户也可以采用自定义的VLAN作为设备发起DHCP申请的VLAN，该VLAN被称为PnP VLAN。
- 在本例中，我们假设网络中采用非VLAN1作为PnP VLAN。用户需要在Core上配置PnP VLAN，或者在Core被iMaster NCE纳管后，在iMaster NCE上配置PnP VLAN。
- 对于本方式：先部署设备上线、再确定网络拓扑。
  - 开局部署时，管理员通过推荐的开局注册上线的方法，部署设备上线。如果设备互联有聚合链路，开局安装上线时，由于链路聚合还未配置，冗余的链路会被STP阻断。设备上线注册到控制器后，管理员开始通过控制器检查拓扑，部署链路聚合和业务配置。
- 该开局流程适用于安装时间段要求分散的场景。
- 注意：
  - LLDP：Link Layer Discovery Protocol，链路层发现协议。
  - NETCONF：Network Configuration Protocol，网络配置协议。
  - PnP：Plug and Play，即插即用。

网络开局流程：先完成规划，设备再上线



准备工作

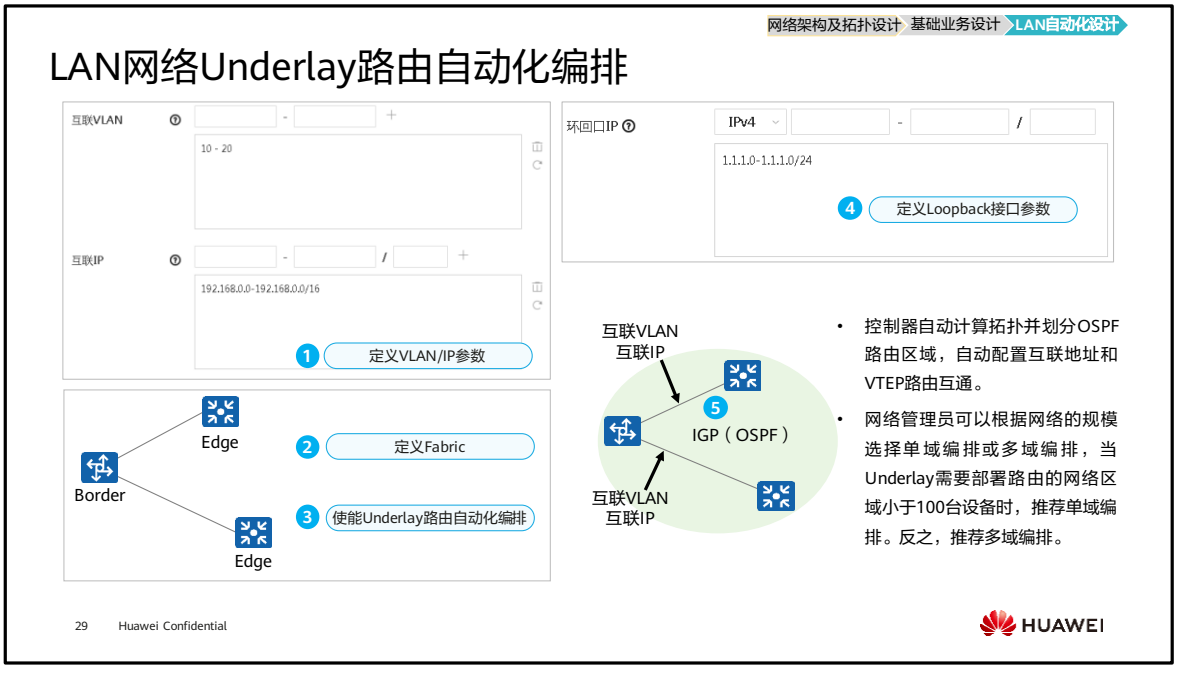
- 管理员在出口网关部署DHCP服务器功能（或部署一台单独的DHCP服务器），配置Option 148。
- 管理员配置Core，使其被iMaster NCE纳管。
- **管理员根据iMaster NCE提供的模板（Excel文档）进行网络拓扑规划，完成后将该模板导入iMaster NCE。**

交换机的上线过程

1. Aggregation、Access加电，分别完成PnP VLAN协商、DHCP报文交互过程，然后向iMaster NCE注册。
2. Aggregation、Access被iMaster NCE纳管，向其上报LLDP邻居信息，iMaster NCE根据设备上报的LLDP信息与此前管理员上传的网络拓扑规划文档进行比对，如果发现拓扑不一致则进行报错，**管理员可根据报错提示进行拓扑纠错**。
3. 管理员在iMaster NCE上对网络进行规划、配置发放。

HUAWEI

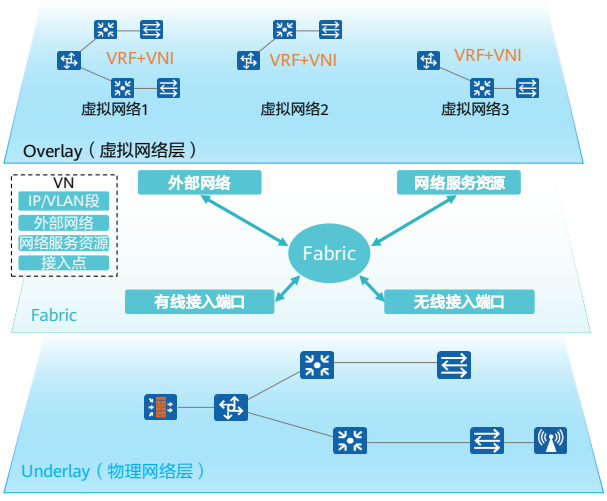
- 该开局流程适用于安装时间段要求集中的场景。优先推荐管理员采用先规划网络，再部署设备上线的方式开局部署。当管理员不具备预先规划网络的条件时，可采用先部署设备上线、再确定网络拓扑的开局部署方式。
- 先规划网络，再部署设备上线。
  - 开局部署时，管理员先在控制器上录入设备ESN信息，指定堆叠设备，指定聚合链路，完成网络拓扑的规划。
  - 管理员也可以通过模板批量导入上述规划信息，完成网络拓扑的规划。推荐采用模板批量导入，简化操作。
  - 然后再通过推荐的开局注册上线的方法，部署设备上线。
  - 设备上线注册到控制器，控制器会自动检查设备实际拓扑和规划拓扑是否一致。安装施工过程中如果连线错误，控制器会第一时间通知管理员。



- Underlay自动化需规划以下网络资源：
  - Fabric对应的网络范围，设备之间通过VLANIF三层互联：每一条互联链路分配1个VLAN。
  - 设备互联VLANIF接口IP地址：自动分配30位掩码长度的互联地址。
  - 设备Loopback地址：自动采用Loopback0的IP地址作为OSPF的Route ID地址和VTEP地址，自动分配32位掩码长度的Loopback0的IP地址。

目录

Fabric设计概述



Fabric设计

园区Fabric是对Underlay网络抽象后的资源池化网络，Fabric将Underlay网络资源池化，以便实现“一网多用”。

Fabric设计主要包含以下部分：

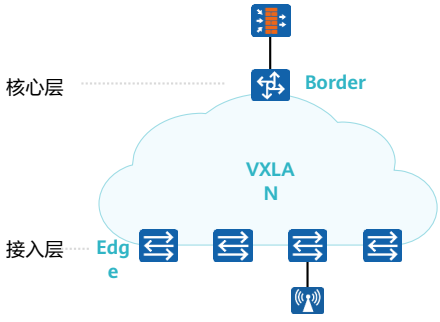
- Fabric组网及节点设计
- Fabric与外部网络互联设计
- Fabric网络服务资源规划
- Fabric的接入管理

HUAWEI

- Fabric网络服务资源规划：
  - 在Fabric网络的资源模型设计中，通过在Border节点创建网络服务资源，使得园区内部业务终端能够访问网络管理区的服务资源，比如DHCP服务器、准入服务器等。
  - 网络服务资源可以创建多个，也可以一个网络服务资源模型包含多个服务资源的访问地址。
  - 如果网络管理区需要访问的服务资源较少，建议这些服务资源都规划在一个网络服务资源模型中。这样，可以节省互联的VLAN和IP地址资源，简化网络管理区侧的路由配置。
- Fabric接入管理：
  - Fabric的接入管理主要是配置认证控制点，对接入点资源进行规划，供VN创建时选用。
  - 其中，有线接入点资源指的是终端接入的交换机端口，无线接入点资源指的是终端接入的SSID。

Fabric组网设计：二层架构

- Fabric网络有两层组网和三层组网，二三层组网架构的选择和网络架构设计类似。
- Fabric网络架构的选择依赖物理网络，若物理网络为二层架构时Fabric网络架构如图所示。
  - 核心层交换机做Border设备
  - 接入层交换机为Edge设备



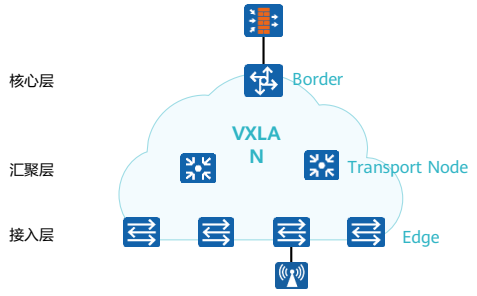
HUAWEI

- 二层架构的应用场景：
  - 应用于网络规模小、接入用户少的场景。
  - 应用于接入用户相对集中的场景，如：所有接入用户处于同一栋楼的同一楼层。

Fabric组网设计：三层架构

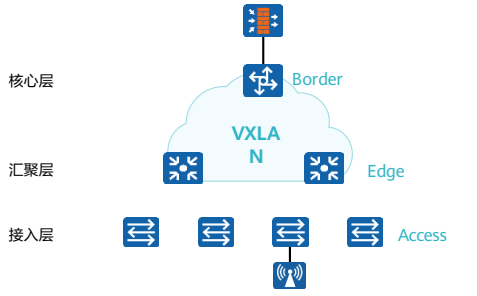
- 若物理网络架构为三层架构，Fabric网络架构有如下两种方案选择：

VXLAN到接入层



方案描述：核心设备作为Border，接入设备作为Edge，汇聚设备做Fabric网络的传输节点。
适用场景：适合新建场景，整网采用虚拟化网络，业务布放和网络管理更加简便。

VXLAN到汇聚层



方案描述：核心设备作为Border，汇聚设备作为Edge，接入设备仅作有线用户或AP的接入点，汇聚设备同接入设备之间做策略联动，实现在接入设备上控制用户的准入。
适用场景：适合改造场景，可以兼容低端的接入交换机。

HUAWEI

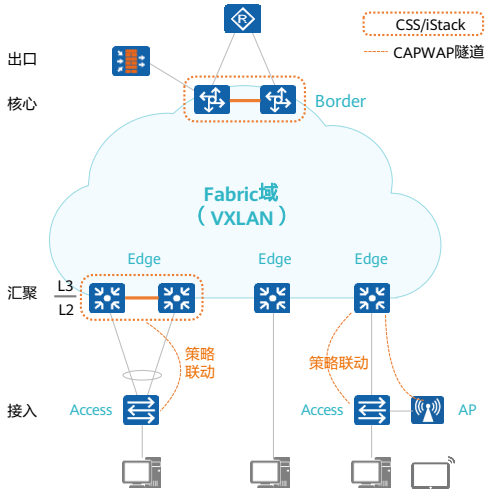
- 三层架构的应用场景：
  - 应用于网络规模大、接入用户多（接入交换机多）的场景。
  - 应用于接入用户相对分散的场景，如：所有接入用户处于不同的楼栋，因此每栋楼可以通过汇聚交换机进行流量集中，而楼栋之间通过核心机房的核心交换机进行流量集中。

Fabric组网场景汇总

- 针对二层或三层组网架构，可选Border或Edge作为网关。
  - 集中式网关：Border做网关可统一集中管理、简化运维。
  - 分布式网关：Edge做网关方便扩展网络规模。

组网	网关位置	Edge位置	终端规模	适用场景
集中式网关，VXLAN到接入	Border	接入交换机	<=50000	终端规模不超过50000，优先推荐
集中式网关，VXLAN到汇聚	Border	汇聚交换机	<=50000	终端规模不超过50000
分布式网关	Edge	汇聚交换机	<=100000	终端规模超过50000，优先推荐

Fabric节点设计

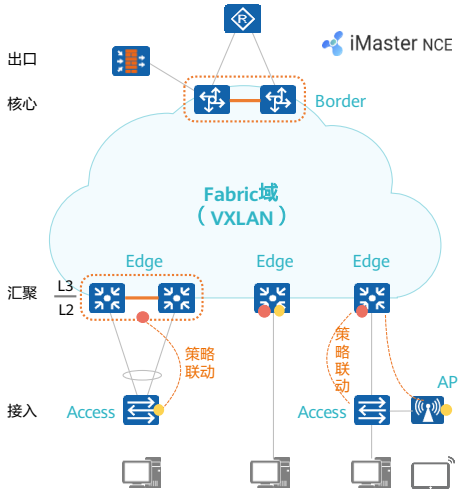


- **Border节点**（CSS/iStack或单台交换机，推荐CSS）
  - 推荐使用大容量交换机（如S12700或S12700E）。
  - 核心层和汇聚层互联的单板选择ENP单板，互联链路部署Eth-Trunk。
- **Edge节点**（CSS/iStack或单台交换机，推荐CSS/iStack）
  - 推荐使用大容量交换机（如S7700、S6700、S12700系列等）。
  - Eth-Trunk用于核心和汇聚交换机、汇聚和接入交换机之间的互联。
- **接入节点**
  - Access节点：每个节点可以是堆叠（≤5台）或单台交换机；支持多层接入交换机（最多2层接入交换机）。
  - 无线接入节点：瘦AP，由随板AC管理。

HUAWEI

- Border建议选择核心设备，Edge可以选择接入设备或汇聚设备，推荐接入设备作为Edge节点。
- VXLAN网络中建议配置BGP EVPN路由反射器，只需要Edge和Border之间建BGP对等体，Edge之间不需要建BGP对等体。如果不配置路由反射器，则所有Edge之间及Edge与Border之间都需要配置BGP对等体，不仅配置复杂，而且大量的BGP连接会消耗设备CPU性能。
- Border、Edge都可以作为路由反射器，但是Border作为核心设备处理能力最强，因此建议选择Border做路由反射器。
- 注：ENP，Ethernet Network Processor 以太网络处理器。

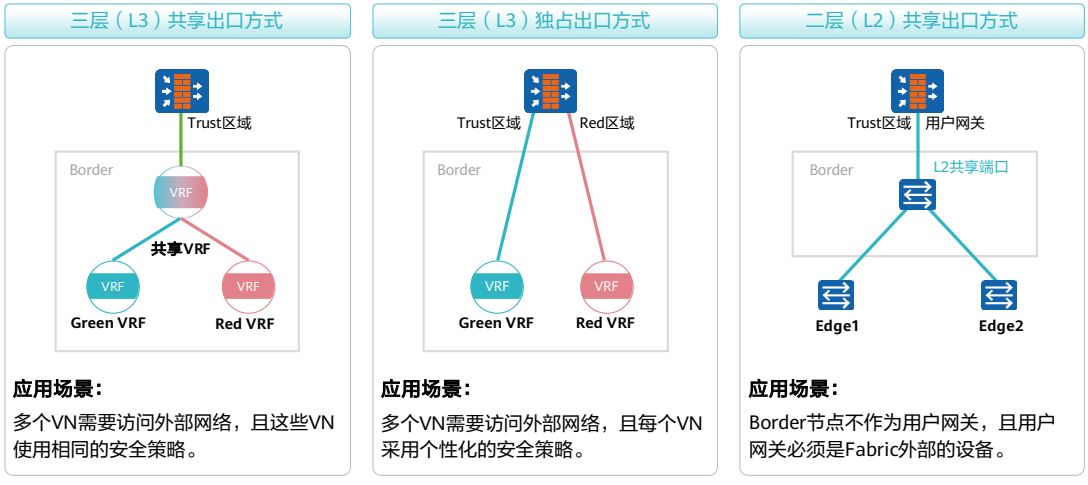
Fabric节点设计：策略联动



- 控制点和执行点使用CAPWAP隧道建立连接（策略联动所使用的管理隧道）。
- CAPWAP隧道主要完成用户关联、消息传递、用户授权策略下发、用户信息同步等功能。
- 配置策略联动后，执行点可以实时透传BPDU报文，实时上报用户下线和用户接入位置，并请求执行点来执行用户访问策略，从而控制用户对网络的访问。

HUAWEI

Fabric与外部网络互联设计

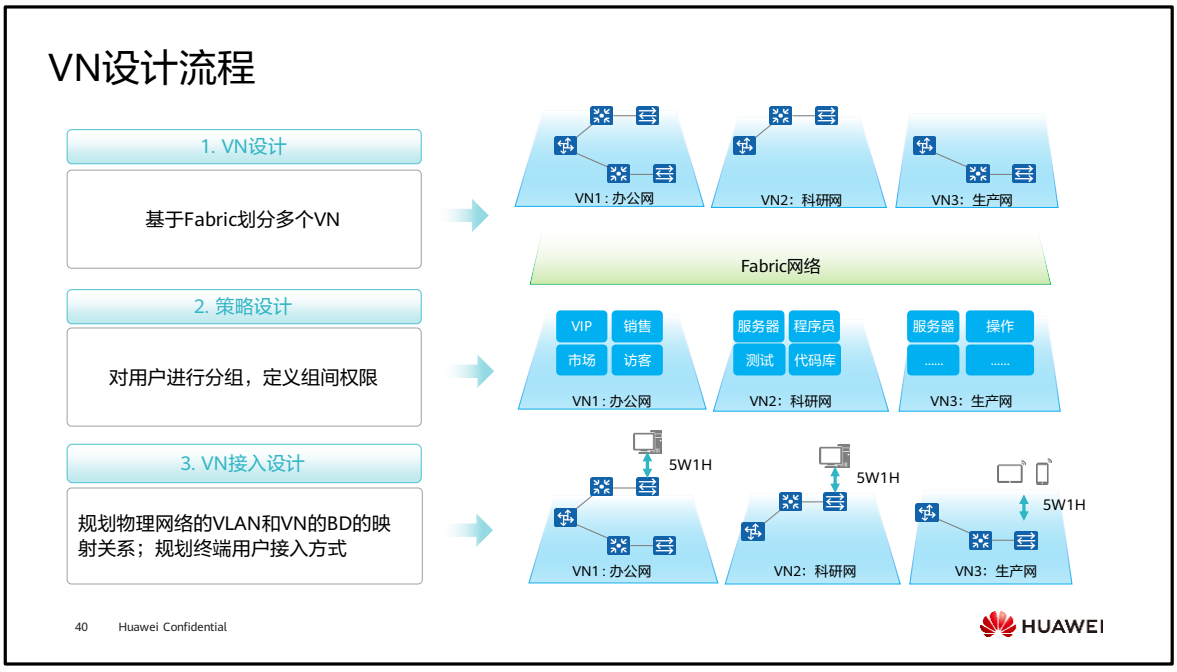


HUAWEI

- 园区网络中所有终端数据在园区内部访问都是通过VXLAN隧道转发，当园区内部需要与外部网络互访时须经过Border节点，如访问Internet、数据中心或其它分支，通过Border与外部网络互通。
- Fabric网络与出口的互联分为三种方式：三层共享出口方式、二层共享出口方式、三层独占出口方式。三层共享出口适用于防火墙无需对虚拟网络（VN）进行安全检测，所有VN流量划分在同一个安全区域；三层独占出口方式适用于防火墙需要对VN进行安全检测，VN流量划分成多个安全区域；二层共享出口方式适用于用户网关必须是Fabric外部的设备，Border和出口防火墙之间是二层互联。
  - 三层共享出口方式，园区共享同一个VPN-Instance（VRF）访问外部网络，Border和出口防火墙之间路由发布可以采用静态路由或动态BGP路由。
    - 静态路由设计关注点：Border上学习到全局内部路由，同时通过默认路由指向出口防火墙；Border上VPN-Instance通过配置静态默认路由指向与出口防火墙互联的Public接口；若有多个出口防火墙可以部署NQA或BFD静态路由联动进行出口路由切换。
    - BGP路由设计关注点：Border与防火墙建立BGP连接，把VPN-Instance中用户路由汇总后重发布进入BGP。

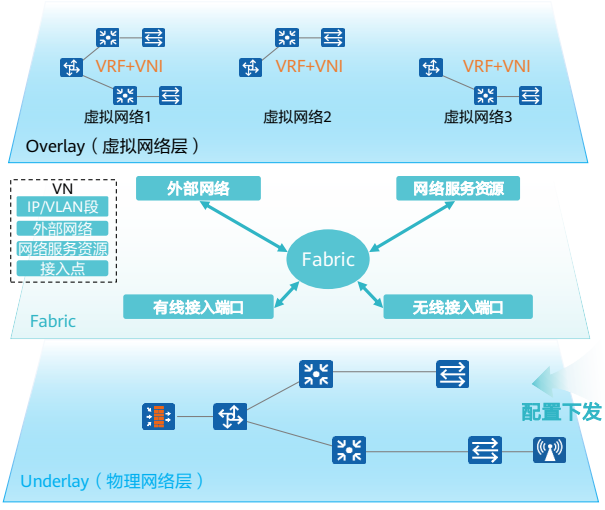
    - 三层独占出口方式，防火墙根据VPN-Instance数划分相同数量的安全区域，并通过物理接口或者子接口与Border背靠背连接。Border上VPN-Instance通过配置静态默认路由指向防火墙安全区域对应的接口或者子接口。
- 二层业务共享出口方式，Border通过二层连接出口设备，用户网关部署在出口设备来实现访问外部网络。
- 应用场景：
    - 通常园区网络与外部网络的出口路由较少，推荐三层共享出口方式，Border和出口防火墙之间路由发布采用静态路由方式。
    - 当出口防火墙需要对各VN进行基于安全区域的安全检测时，可采用三层独占出口的方式。
    - 二层共享出口方式只适用于用户网关必须在Fabric外部的场景，在高教场景中，如果网络中存在BRAS（Broadband Remote Access Server，宽带远程接入服务器）设备做用户的认证点，并且网络中需实施PPPoE拨号业务，那么可以使用该外部网络互联方案。

目录



- VN设计：
  - 虚拟网络通常根据园区的业务来划分，独立的业务作为一个VN，VN之间默认是隔离的。例如在校园网中，访客业务、教学业务、物联网业务、视频监控业务等可以划分成独立的VN。例如在企业园区中，办公网络业务、生产网络业务、科研网络业务等可划分成独立的VN。
- 策略设计：
  - 由于用户角色的差异而导致的部分隔离需求，建议不要通过VN来实现，因为VN间默认是隔离的，互通需要做额外的配置，用户角色差异的隔离建议用策略管控技术（如业务随行）来部署。
- VN接入设计：
  - Edge节点是业务数据从物理网络进入VN的边界点，根据用户所属的VLAN进入不同的VN。因此在设计网络时，需要先规划好物理网络的VLAN和VN的BD的映射关系，同时配置有线用户和无线用户的VLAN。
- 5W1H：
  - Who：接入用户的身份，例如公司的领导、普通员工、访客。
  - Where：接入用户的地点，例如园区内接入，或远程接入。
  - What：接入用户使用的终端类型，例如是手机接入，还是PC/便携机接入。
  - When：接入用户的时间，例如是白天接入，还是晚上接入。
  - Whose：设备归属，例如是公司终端的还是自带终端。
  - How：接入用户的方式，例如是有线接入，还是无线接入。

VN设计



1. 网络服务抽象

- 通过编排实现物理网络资源池化，将网络抽象为FaaS（Fabric as a Service），VN是FaaS的实例，包括：
- IP/VLAN
- 外部网络
- 网络资源：IP/VLAN段是VN提供给客户端使用网络资源的能力
- 接入点：终端通过接入点接入VN

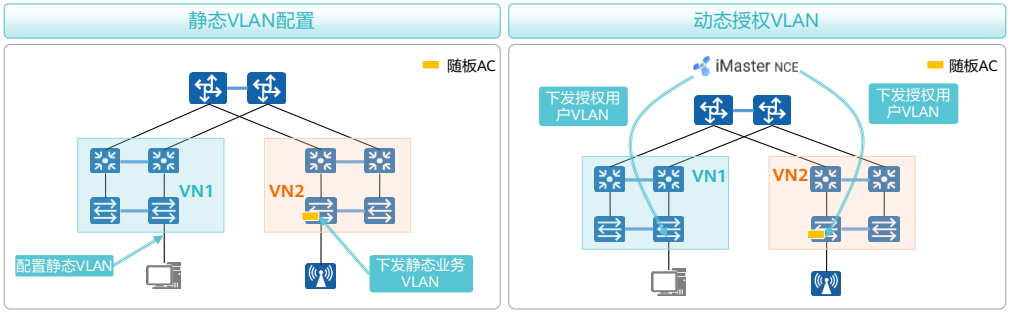
部署VN

2. 网络业务编排

- 下发VLAN与VNI的映射关系
- 下发vBDIF对应的IP地址段
- 下发VRF绑定到vBDIF

VN接入设计

- Edge节点是业务数据从物理网络进入VN的边界点，根据用户所属的VLAN进入不同的VN。因此在设计网络时，需要先规划好物理网络的VLAN和VN的BD的映射关系，同时配置有线用户和无线用户的VLAN。
- 有线用户流量根据VLAN直接接入虚拟网络；无线用户流量被转发到随板AC后，随板AC解封装CAPWAP报文后根据VLAN进入对应的BD转发。



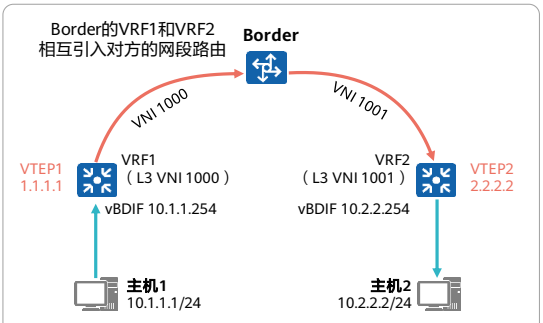
HUAWEI

- 动态授权VLAN：
  - 有线用户通过授权用户VLAN，下发到对应的接入端口，或者通过策略联动的方式下发到接入交换机的端口。
  - 无线用户的SSID下会配置业务VLAN，但该业务VLAN实际不生效，在用户认证后会下发认证授权的VLAN，实际以授权的VLAN生效。
- 静态VLAN配置：
  - 有线用户在接入交换机的端口配置静态VLAN。
  - 无线用户在SSID下配置静态的业务VLAN。
- 应用场景：
  - 静态VLAN方式适用于终端接入位置固定、不认证的场景，这种接入方式更安全，但是缺乏灵活性，当终端位置发生变化时，需要重新配置。
  - 动态授权VLAN的方式是结合用户认证流程下发VLAN信息的，适用于任意位置接入，且需要认证的场景，这种接入方式灵活性高，当终端位置变化时，不需要修改配置。动态接入的自动化程度更高，管理和使用更方便，建议采用动态接入方式。
- 无线用户的VN接入设计：
  - 如果采用分布式网关，Edge节点部署随板AC功能，无线用户流量经过CAPWAP隧道转发至随板AC，随板AC解封装CAPWAP报文后，再根据无线用户所属的VLAN进入对应的VXLAN网络。
  - 如果采用集中式网关，Border节点部署随板AC功能，建议规划无线用户流量直接通过CAPWAP隧道转发至随板AC，随板AC解封装CAPWAP报文后根据VLAN进入对应的BD进行转发，管理员需将有线终端和无线终端接入VLAN划分在不

重叠范围，有线终端VLAN在Edge绑定BD，无线终端VLAN在Border绑定BD。

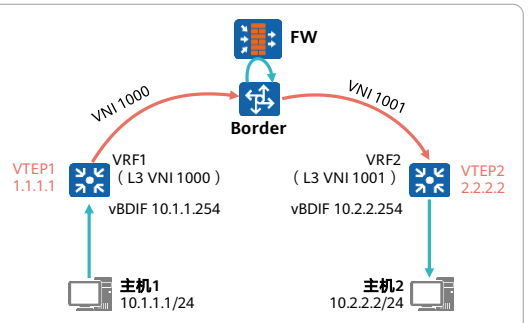
VN之间互访设计

不同的VN直接在Border上互通



- 不同VN之间互访的流量通过Border转发，Border需负责打通VN（VRF）之间互访的路由。
- 适用于两个VN属于相同的安全区域，安全控制需求比较低的场景。

不同的VN到外部网关上做互通



- 不同VN之间互访的流量通过Border引导到外部网关，由外部网关执行安全检查或发回，再由Border转发到目的地。
- 适用于两个VN属于不同的安全区域，安全控制需求高的场景。

HUAWEI

- VN之间的互访，可以通过Border或外部网关实现。
  - 通过Border互通：
    - 两个VN如果属于相同的安全区域，安全控制需求比较低，可以直接在Border上互通，另外可以结合业务随行策略进行权限控制。要实现不同VN的互通，需要在Border上互相引入对方可访问的网段路由。
  - 通过外部网关互通：
    - 两个VN如果属于不同的安全区域，安全控制需求高，建议在外部网关防火墙上做互通，同时在防火墙上配置安全区域策略进行权限控制。

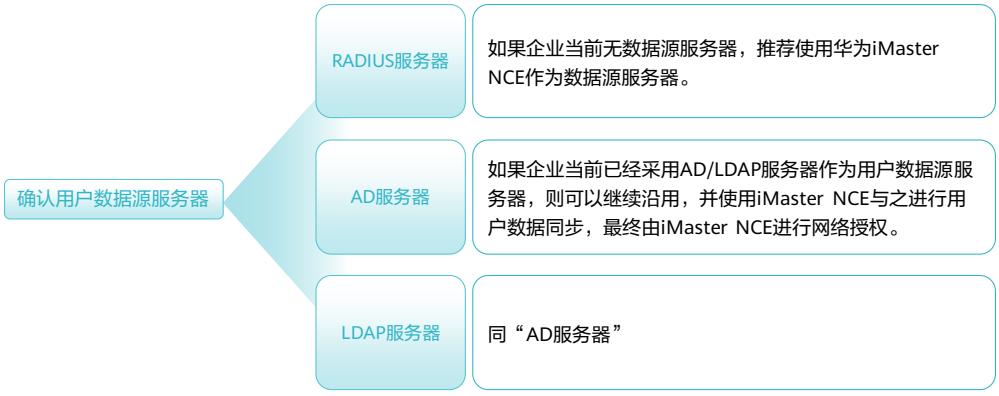
目录

HUAWEI

- 网络准入控制方案的设计目标就是在用户网络解决用户终端认证和策略管控两大问题，根据用户组织结构和账号信息，实现用户的分类认证和策略管控。

用户管理方案设计

- 用户管理方案设计主要是确认用户数据源服务器，企业常见的用户数据源服务器有RADIUS服务器、AD服务器和LDAP服务器。



用户认证技术选择

- 常用的认证技术包括802.1X，MAC和Portal认证，各种认证方式差异如表所示：

对比项	802.1X认证	MAC认证	Portal认证
客户端需求	有特殊要求	无特殊要求	无特殊要求
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高
适合场景	通常适用于对安全要求较高的办公用户的网络认证	打印机、传真机等哑终端接入认证的场景	通常适用于流动性较大，终端类型复杂的访客用户网络认证

- 在大中型园区网络中，企业员工建议使用802.1X认证、访客使用Portal认证、哑终端使用MAC认证。
- 如果客户希望在同一个接入点使用多种认证方式，可以考虑配置成混合认证模式，配置混合认证后，终端使用任意认证方式，只要校验成功，均可以接入网络，适合同一个端口给多种类型用户接入的场景。比如IP话机下挂PC终端的场景，可以配置MAC+802.1X混合认证，IP话机用MAC认证，PC终端用802.1X认证。

- 如果选择802.1X或MAC认证，属于二层认证技术，认证点必须与用户主机位于同一网段，建议接入层作为认证点和策略执行点。如果接入层支持802.1X报文透传，则建议部署策略联动，网关作为认证点和策略控制点，接入设备作为策略执行点，降低策略部署复杂度。
- 如果选择Portal认证，认证点位置与用户主机IP可达即可。建议部署二层Portal认证。

已认证用户与VN的关联

用户在iMaster NCE上创建虚拟网络

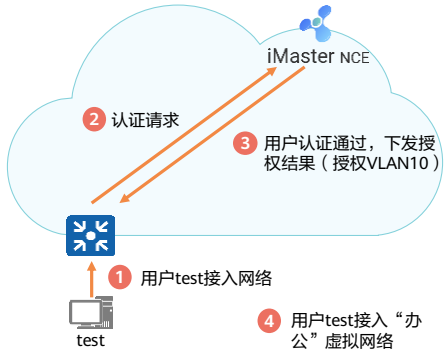
管理员创建VN，并指定VN的IP网段与VLAN：

“办公”虚拟网络
VLAN10：10.1.10.0/24
VLAN20：10.1.20.0/24

“研发”虚拟网络
VLAN30：10.1.30.0/24
VLAN40：10.1.40.0/24

管理员配置用户的认证规则、授权规则及授权结果，使得用户认证成功后，获得相应VLAN，例如配置用户test通过802.1X认证后获得授权VLAN10。

用户认证后获得VLAN授权，根据VLAN关联到虚拟网络



HUAWEI

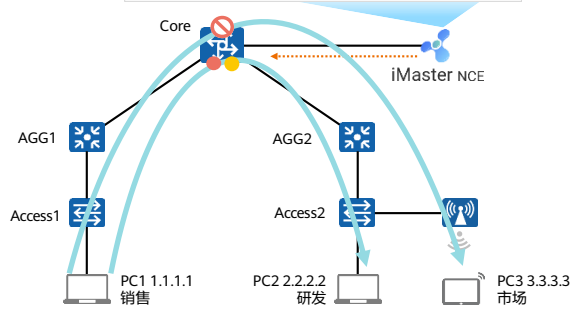
业务随行场景化方案（1）

安全组

组名	组ID
销售	1
研发	2
市场	3
…	…

基于安全组的通信矩阵

	销售	研发	市场	…
销售	√	×	√	…
研发	×	√	√	…
市场	√	√	√	…
…	…	…	…	…



场景描述：

- 集中的认证点+集中的策略执行点。
- 认证点与策略执行点合一。
- 网络不支持VXLAN组网。

场景特点：

- Core作为全网有线、无线用户的集中认证点。
- Core作为业务随行的策略执行点。
- Core拥有全网用户的认证信息，流量转发至该设备后，由其根据用户所定义的通信矩阵进行策略执行。
- 网络无需支持或部署VXLAN。

● 认证点　● 策略执行点　⋯◂ 安全组及通信矩阵下发

HUAWEI

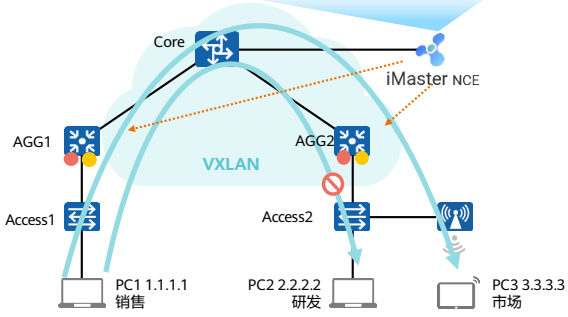
业务随行场景化方案（2）

安全组

组名	组ID
销售	1
研发	2
市场	3
…	…

基于安全组的通信矩阵

	销售	研发	市场	…
销售	√	×	√	…
研发	×	√	√	…
市场	√	√	√	…
…	…	…	…	…



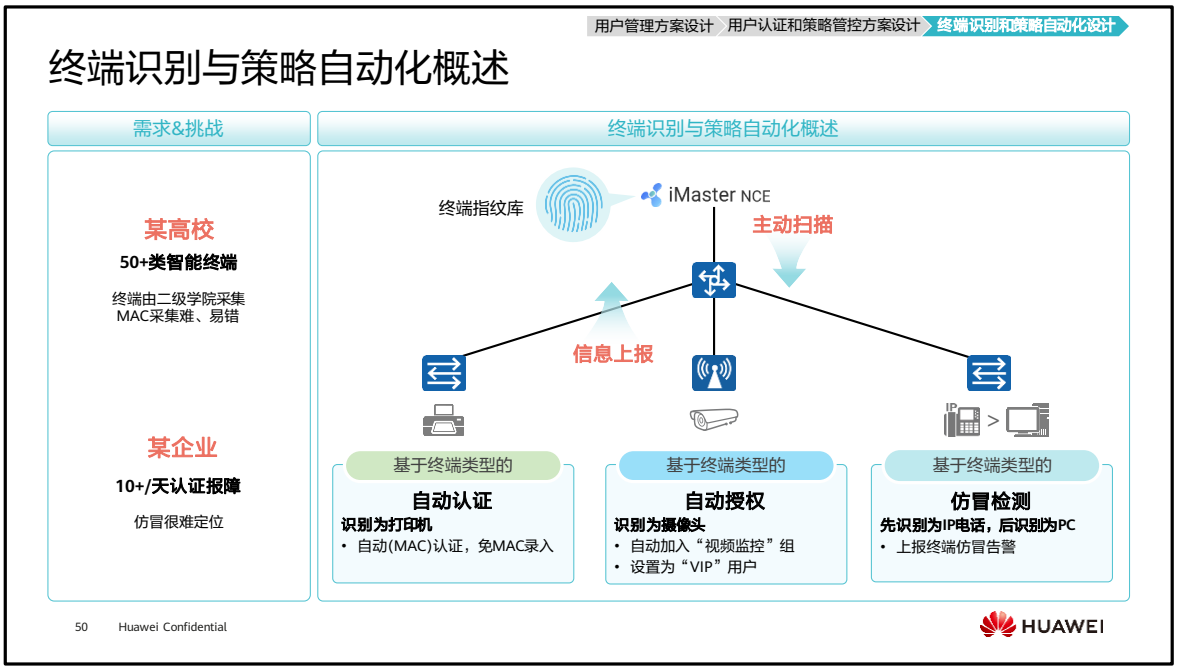
场景描述：

- 基于VXLAN的虚拟化园区，业务自动发放。
- 多个认证点+策略执行点。

场景特点：

- 全网存在多个认证点，例如认证点分散在汇聚交换机上。
- 汇聚交换机支持VXLAN，作为策略执行点。
- 同一台汇聚交换机下的流量互访在该交换机上执行策略。
- 不同汇聚交换机下的接入用户之间的互访流量，通过VXLAN进行封装，并在VXLAN封装中写入源安全组ID，在远端汇聚交换机上执行策略。

认证点　策略执行点　安全组及通信矩阵下发



- 大中型园区网络中，接入终端除了智能终端（PC、手机），还有IP话机、打印机、IP摄像头等哑终端。当前园区网络终端管理主要面临以下两个问题：
  - 当前网络管理系统只能查看接入终端的IP和MAC，并不知道终端具体是什么设备，无法对网络终端做更精细的管理。
  - 不同类型的终端，需部署的网络业务配置和策略也不同，管理员需要手动为每种类型的业务终端配置不同的业务配置和策略，业务部署复杂且操作繁琐。
- 为了解决如上两个场景问题，华为推出了终端识别与策略自动下发方案，可支持如下功能：
  - 通过iMaster NCE-Campus可查看全网终端类型、系统等分类，比如哑终端：打印机、IP摄像头、一卡通、门禁等，并基于终端的类型进行分类统计和流量呈现。
  - 针对园区IP话机、打印机、IP摄像头等哑终端设备，无需管理员手动为每种类型的业务终端配置不同的业务配置和策略。iMaster NCE-Campus能够自动的识别终端，并为终端设备下发对应的准入策略和业务配置。

终端识别

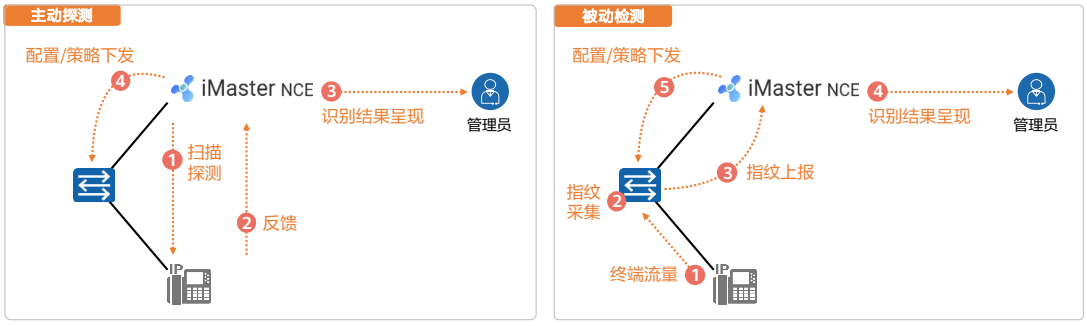
- 网络管理员部署终端识别与策略自动下发方案，需要完成终端识别方法设计、终端策略设计两部分。
- iMaster NCE-Campus的终端管理提供终端识别功能，可呈现终端的类型、操作系统、生产厂商。
- 终端识别通过下列几种方法实现：

类型	识别方法	识别方法说明	适用的场景
被动指纹识别（信息上报）	MAC OUI	MAC地址前三字节用于表示厂商，但很多情况下不准确。	仅识别设备厂商。
	HTTP UserAgent	浏览器UserAgent信息中包含厂商、终端类型、操作系统、浏览器等信息。	手机、平板型号、PC、工作站、音视频智能终端。
	DHCP Option	终端DHCP报文的部分属性可用于终端分类，常用属性有55、60、12。	手机、平板型号、PC、工作站、IP摄像头、IP话机、打印机等。
	LLDP	链路层设备发现协议，包携带设备型号。	IP话机、IP摄像头、网络设备等。
	mDNS	mDNS报文含有终端型号信息和业务信息。	苹果终端、打印机、IP摄像头等。
主动扫描识别	SNMP Query	通过查询SNMP mib节点中的设备信息相关的节点获取识别信息。	网络设备、打印机等。
	NMAP	通过NMAP软件对终端进行OS、服务扫描，可探测终端型号和OS信息。	PC、工作站、如打印机、话机、IP摄像头等。

- 终端接入网络时，网络设备可以采集终端的信息，上报给iMaster NCE-Campus或iMaster NCE-Campus主动扫描终端信息，iMaster NCE-Campus自动识别终端的类型、操作系统和厂商。

终端识别方法：主动与被动检测

- 终端可视化：终端类型统计（厂商、OS）、终端与接入端口关系、接入策略查看（VLAN、QoS、认证方式）、报表导出。
- 终端策略自动化：
  - 支持终端自动准入，根据终端类型进行准入，实现哑终端自动MAC认证。
  - 支持基于终端组授权策略（VLAN、安全组、访问权限、QoS），支持IPv4、IPv6双栈终端。



HUAWEI

- 被动指纹采集方法：通过网络设备采集终端报文的特征指纹，上报给iMaster NCE-Campus控制器做终端类型识别。
- 主动扫描方法：通过iMaster NCE-Campus控制器主动探测或扫描终端，根据终端设备的反馈信息做终端类型识别。

终端识别方法设计（1）

1. 网络分析

当园区网络管理员想通过iMaster NCE-Campus呈现终端的类型，基于终端类型做网络管理，需要完成如下工作：

1. 收集网络中的终端类型，比如PC，手机，打印机，IP摄像头，门禁等。
2. 是否部署Portal认证。
3. 终端是动态DHCP分配IP地址，还是静态分配IP地址。

2. 根据下表逐项遍历

利用搜集的信息，根据下表逐项遍历，选择需要开启的终端识别方法。（多选，符合的识别方法都需开启）

识别方法	可识别的终端类型	适用场景
MAC OUI	所有IP终端(仅识别设备厂商)	通用场景
HTTP UserAgent	手机、平板型号、PC、工作站、音视频智能终端	仅Portal认证的终端场景
DHCP Option	手机、平板型号、PC、工作站、IP摄像头、IP话机、打印机等	仅终端是动态IP分配的场景
LLDP	IP话机、IP摄像头、网络设备等	通用场景
mDNS	苹果终端、打印机、IP摄像头等	通用场景
SNMP Query	网络设备、打印机	本地部署场景
NMAP	PC、工作站、打印机、话机、IP摄像头等	本地部署场景

- 在本页中，“通用场景”指的是认证场景、非认证场景、动态IP场景、静态IP场景。
- 不认证场景下，接入设备需开启ARP SNOOPING功能，控制器才能显示有线终端的信息。

终端识别方法设计（2）

3. 终端识别功能开启方法

- 若管理员无法精确选出应采用的终端识别的方法，推荐开启5个识别方法：MAC OUI，HTTP UserAgent，DHCP Option，LLDP，mDNS。
- NMAP扫描方法识别周期长，推荐默认关闭，被动指纹识别方法无法满足终端识别的场景再开启NMAP识别方法。

识别方法	功能开启	除了开启终端识别功能还需同时开启的功能
MAC OUI	接入交换机和AP开启	-
HTTP UserAgent	Portal认证的设备	-
DHCP Option	接入交换机和AP开启	接入交换机需开启DHCP Snooping功能，AP默认已开启DHCP Snooping功能。
LLDP	接入交换机和AP开启	-
mDNS	接入交换机和AP开启	接入交换机和AP需开启mDNS Snooping功能。
SNMP Query	控制器开启	-
NMAP	控制器开启	-

终端策略设计

- 园区网络管理员可以通过iMaster NCE-Campus为终端设备自动下发对应策略，而无需手动为每种类型的业务终端配置不同的业务配置和策略。
- 终端策略支持基于终端类型或操作系统或生产厂商下发对应终端策略。

关于策略设计

- 基于终端类型的策略自动下发依赖准入认证来授权策略。
- 接入交换机和AP上需部署准入认证。
- 有哑终端的场景需要在接入交换机和AP上开启MAC认证。

网络开启终端识别功能

梳理网络中需要自动下发策略的终端类型，
并设计对应的授权策略，在iMaster NCE-Campus上配置。

条件	准入策略	授权策略
操作系统：Android	用户准入	授权ACL 1
操作系统：IOS	用户准入	授权ACL 2
终端类型：打印机	自动准入	授权VLAN10
终端类型：IP摄像头	自动准入	授权VLAN20
终端类型：IP话机	自动准入	授权VLAN30；DSCP 48
终端类型：门禁	自动准入	授权VLAN40
生产厂商：ABC	用户准入	授权ACL 100

- 对于哑终端（打印机、IP话机、IP摄像头等）推荐采用基于终端的类型自动下发准入和授权策略，实现哑终端设备的业务自动发放，即插即用。

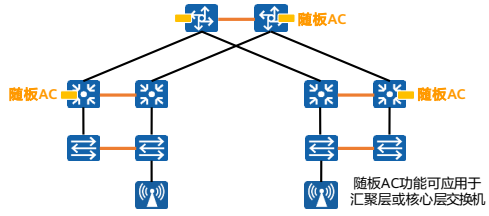
目录

WLAN业务方案

- CloudCampus网络自动化有两个无线业务方案：
  - 随板AC方案：适用于有线无线是同一维护团队的客户。
  - 独立AC方案：适用于有线无线不是同一维护团队的客户。

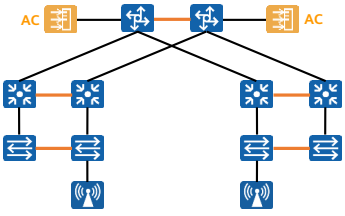
随板AC方案

1. 交换机内置AC功能。
2. 支持业务随行，有线无线用户统一在交换机上做策略。
3. 有线无线用户统一运维。



独立AC方案

1. 独立AC（旁挂到核心设备）。
2. 无线用户支持业务随行，但需IP-Group同步方案配合。
3. 有线无线用户不统一运维。



HUAWEI

- 大中型园区的WLAN网络通常采用AC+ FIT AP的组网架构。根据AC在园区网络中的部署位置，可分为AC旁挂式组网和AC直连式组网，采用随板AC时，只能采用直连式组网；采用独AC时，有直连式与旁挂式两种组网方式，推荐采用旁挂式组网。

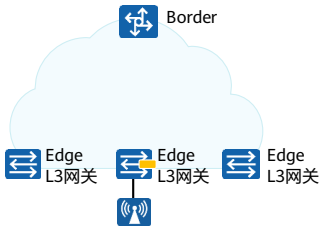
AC选型

- 华为WLAN网络中部署的AC包括随板AC（交换机内置AC功能，实现有线无线业务融合）与独立AC两种类型，基于AC的性能规格能力以及项目的实际诉求进行选择，选择因素包括如下几个方面：
  - 管理AP的数量。
  - 接入的并发终端数量。
  - 转发能力，特别是集中转发模式下。
  - 支持的用户并发上线速率，比如高教场景需要重点考虑此因素，教学区域在下课时可能存在大量并发上线的场景。
- 通常规格满足的情况下，首选随板AC，但是如果有线无线独立组网时或后续大量有扩容需求，推荐独立AC。除了需要考虑上面的规格要求外，还需考虑关键特性的满足情况，如需如下特性只能选择随板AC：
  - 需支持有线无线融合，提供统一认证与统一管理。
  - 需支持业务随行功能。

随板AC方案在VXLAN虚拟化园区中的部署（1）

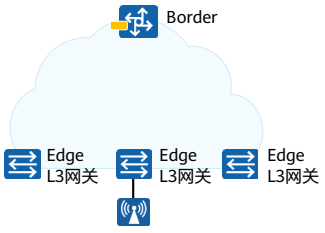
分布式网关场景

随板AC



- 场景1：Edge交换机具备随板AC功能，管理下联的AP。
- 当整网无线用户数量超过50K时，推荐Edge部署随板AC功能。在本场景中，AP推荐采用隧道转发模式。

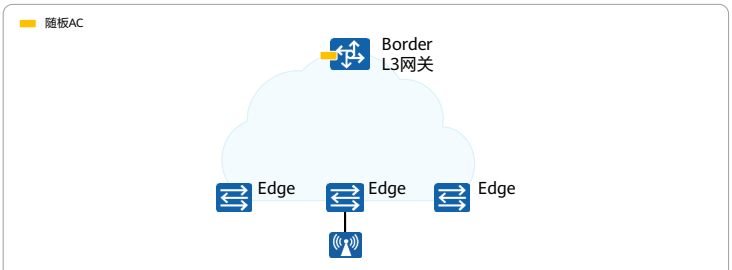
随板AC



- 场景2：Border交换机具备随板AC功能，管理全网AP。
- 当整网无线用户数量小于50K时，推荐Border部署随板AC功能。在本场景中，AP推荐采用隧道转发模式。

随板AC方案在VXLAN虚拟化园区中的部署（2）

集中式网关场景



- 场景：Border交换机具备随板AC功能，管理全网AP。
- 推荐Border部署随板AC功能，AP推荐采用隧道转发模式。

WLAN虚拟化部署方案设计

- 对于集中式网关和分布式网关组网，WLAN虚拟化部署方案设计参见如下表格：

组网	AC	无线终端网关	AP转发模式	无线流量虚拟化位置	终端规模	适用场景
集中式网关	Border随板AC	Border	隧道转发	Border	<=50000	无线终端集中转发，终端规模不超过50000，优先推荐
	Border随板AC	Border	本地转发	Edge	<=50000	无线终端本地转发，不推荐
	独立AC旁挂Border	Border	隧道转发	Border	<=50000	有线网络先改造，无线终端集中转发，优先推荐
	独立AC旁挂Border	Border	本地转发	Edge	<=50000	有线网络先改造，无线终端本地转发，不推荐
分布式网关	Edge	Edge	隧道转发	Edge	50000-100000	终端规模超过50000，无线终端集中转发，优先推荐

- 在虚拟化网络方案中，对于新建和有线无线同步改造场景，优先推荐随板AC，AP优先选择隧道转发模式。

办公区场景WLAN建网标准及设计


普通办公区


高端办公区

场景描述

1. 业务类型：
   网页浏览 、语音、电子白板、电子邮件、文件传输与即时通信为主。
2. 分布人数：
   4~5 ㎡/人。
3. 层高：
   3~4 m。

建网标准

1. 体验速率：50 Mbps，续航速率：10 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：45个终端。
   ② 并发率：40%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10^{-5}。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
普通办公区	低	高	高	室内内置全向天线AP	AP外漏安装	AP间距推荐18~20 m等间距部署2.4 GHz & HT20，5 GHz & HT40。
高端办公区	高	高	高	室内内置全向天线AP，支持MIMO 8*8及以上。	暗装在非金属吊顶内部或者增加美化罩	

会议室场景建网标准及设计

场景描述

1. 业务类型：
   网页浏览、Email、电子白板和即时通信等
2. 分布人数：
   ① 小型会议室典型20人/50㎡；
   ② 大型会议室60人/200㎡。
3. 层高：
   室内3~5 m。

建网标准

1. 体验速率：50 Mbps，续航速率：10 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：30个终端。
   ② 并发率：40%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10^{-5}。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
会议室	高	高	高	室内内置全向天线AP	暗装在非金属吊顶内部或者增加美化罩	AP布放远离门口并均匀分布在房间内2.4 GHz & HT20 5GHz & HT40。

HUAWEI

- 体验速率：网络轻负载下的感知速率。
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率，可以通俗理解为峰值速率。
- 续航速率：网络高负载下的保障速率。
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率，可以通俗理解为保障速率。
- 2.4G@HT20 5G@HT40指的是2.4G使用20M频宽，5G使用40M频宽。

展厅场景建网标准及设计

场景描述

1. 业务类型：

   网页浏览、高清视频与即时通信为主。

2. 分布人数：

   约8~10㎡/人。

3. 层高：

   室内5~8 m。

建网标准

1. 体验速率：50 Mbps，续航速率：16 Mbps。
2. 容量KPI：
   - ① 单AP接入用户数：30个终端。
   - ② 并发率：30%。
   - ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   - ① 漫游时延小于20ms，丢包率小于10-5。
   - ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
展厅	高	高	高	室内外置天线AP + 定向天线	外漏安装	AP间距推荐16 m等间距部署2.4 GHz & HT20，5 GHz & HT40。

体育场馆看台区场景建网标准及设计

场景描述

1. 业务类型：
   网页浏览、高清视频和即时通信等。
2. 分布人数：
   看台区域典型240用户/约120平米。
3. 位置分布：
   大中型体育场看台区会分为2~3层，呈阶梯状。

建网标准

1. 体验速率：16 Mbps，续航速率：4 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：40个终端。
   ② 并发率：30%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10^{-5}。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
看台区	低	高	高	室外外置天线AP + 定向天线	马道吊顶安装或看台后部边沿挂壁安装	AP沿看台等间距部署，覆盖区域长度小于20 m，5GHz天线间隔4 m，2.4 GHz间隔12 m；覆盖区域长度大于20 m，5G天线间隔4 m，2.4GHz间隔16 m；2.4 GHz & HT20，5 GHz & HT20。

HUAWEI

- 体验速率：网络轻负载下的感知速率。
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率，可以通俗理解为峰值速率。
- 续航速率：网络高负载下的保障速率。
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率，可以通俗理解为保障速率。
- 2.4G@HT20 5G@HT40指的是2.4G使用20M频宽，5G使用40M频宽。

教室场景建网标准及设计

场景描述

1. 业务类型：
   网页浏览、高清视频、电子白板、即时通信为主。
2. 分布人数：
   高峰时段2用户/平米。
3. 层高：
   室内3~5 m。

建网标准

1. 体验速率：32 Mbps，续航速率：5 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：50 终端。
   ② 并发率：40%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
普通教室	高	高	高	室内内置全向天线的AP	AP吸顶安装，安装在横梁或天花板下方。	100平及以下房间，总人数100以下，部署1台AP。
阶梯教室	高	高	高	室内内置全向天线的AP，支持MIMO 8*8及以上。	AP吸顶安装，安装在天花板下方。	W型部署，AP间距15米，按照每台AP覆盖100人部署。

HUAWEI

- 体验速率：网络轻负载下的感知速率。
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率。
- 续航速率：网络高负载下的保障速率。
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率。

图书馆场景建网标准及设计


图书馆自习区

场景描述

1. 业务类型：
   网页浏览、高清视频、电子白板、即时通信为主
   网页浏览 和即时通信为主。
2. 分布人数：
   高峰时段2平米/用户。
3. 层高：
   室内3~5 m。

建网标准

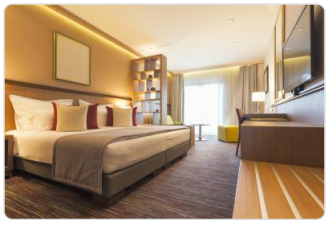
1. 体验速率：32 Mbps，续航速率：5 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：50 终端。
   ② 并发率：30%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。


图书馆书架区

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
书架区	高	高	高	室内内置全向天线的AP	AP吸顶安装，安装在横梁或天花板下方。	吸顶安装，AP间距15米左右，W型部署。
自习区	高	高	高	室内内置全向天线的AP，支持MIMO 8*8及以上。	AP吸顶安装，安装在天花板下方。	安装在天花板下方，AP间距20米，按照每台AP覆盖100人部署。

客房/宿舍场景建网标准及设计



场景描述

1. 业务类型：
   网页浏览、高清视频、游戏和即时通讯为主。
2. 分布人数：
   单房间1~2人。
3. 层高：
   室内3~4m。

建网标准

1. 体验速率：50 Mbps，续航速率：30 Mbps。
2. 容量KPI：
   ① 单RU接入用户数：4 终端。
   ② 并发率：100%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，且丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案	客房间墙体说明
客房一	低	高	中	敏分RU	面板或挂壁安装	一个AP覆盖一个房间 2.4GHz & HT20， 5GHz & HT20。	150 mm及以上厚度实墙，衰减：2.4 GHz为10dB，5GHz为15dB及以上。
客房二	低	高	中	敏分RU	推荐挂壁，靠近中间墙体安装	一个AP覆盖两个房间 2.4GHz & HT20， 5GHz & HT20。	150mm及以下厚度实墙或隔板，衰减：2.4GHz为10dB，5GHz为15dB及以下。

- 体验速率：网络轻负载下的感知速率
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率。
- 续航速率：网络高负载下的保障速率
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率。

商超场景建网标准及设计


超市

商铺

场景描述

1. 业务类型：
   网页浏览、高清视频和即时通信为主。
2. 分布人数：
   高峰时段1人/4 ㎡。
3. 层高：
   框式无顶，层高不定；
   普通区，层高3~5米。

建网标准

1. 体验速率：32 Mbps，续航速率：10 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：30个终端。
   ② 并发率：40%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，且丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。

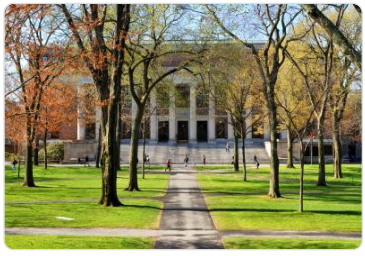
一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
店铺	中	低	中	室内内置全向天线AP	AP吸顶安装在天花板下方	大店铺以AP覆盖半径8-10米来部署；小店铺按照1个AP部署。2.4GHz & HT20，5GHz & HT40。

HUAWEI

- 体验速率：网络轻负载下的感知速率
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率，可以通俗理解为峰值速率。
- 续航速率：网络高负载下的保障速率
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率，可以通俗理解为保障速率。
- 2.4G@HT20 5G@HT40指的是2.4G使用20M频宽，5G使用40M频宽。

室外场景建网标准及设计



场景描述

1. 业务类型：
   网页浏览、游戏和即时通信为主。
2. 分布人数：
   约20~30平米/用户。
3. 层高：
   室外开放区域无层高。

建网标准

1. 体验速率：16 Mbps，续航速率：5 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：100个终端。
   ② 并发率：30%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -70 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，且丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
室外区域	低	低	高	室外内置定向天线AP/室外外置天线AP + 全向天线	AP外漏安装	AP沿外墙40 m等间距安装，安装高度4-6 m，覆盖距离最远180 m，或者AP抱灯杆安装，2.4GHz & HT20；5GHz & HT40。

AGV场景建网标准及设计


AGV仓库


AGV小车工作

场景描述

1. 业务类型：
   网页浏览、高清视频、语音通话、及时通信为主。
2. 业务特点：
   带宽低、漫游多、丢包敏感。

建网标准

1. 体验速率：32 Mbps，续航速率：5 Mbps。
2. 容量KPI：
   ① 单AP接入用户数：10~20个终端。
   ② 并发率：50%。
   ③ Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65 dBm。
4. 其他KPI：
   ① 漫游时延小于20 ms，丢包率小于10-5。
   ② 视频语音等关键业务时延小于10 ms。

一景一策

场景	美观性	容量	覆盖	推荐AP类型	安装方式	网规方案
AGV区域	低	低	高	室内外置天线AP + 全向天线	AP吸顶外漏安装	AP挂高小于等于6 m，间距约15~20 m等三角布放。

- 体验速率：网络轻负载下的感知速率。
  - 在网络轻载下（信道利用率小于20%），@95% 区域，用户测速（SpeedTest）能达到的目标速率，可以通俗理解为峰值速率。
- 续航速率：网络高负载下的保障速率。
  - 在多用户并发场景下，90%时间内，网络负载<80%，并发测速（SpeedTest）能够达到的目标速率，可以通俗理解为保障速率。

机场场景建网标准及设计

场景描述

1. 业务类型：
   - 网页浏览 、高清视频，语音通话、即时通信为主。
2. 分布人数：
   - 高峰时段，2平米/用户。
3. 层高：
   - 镂空区，层高不定；普通区，层高3~5米。

建网标准

1. 体验速率：50Mbps，续航速率：10Mbps。
2. 容量KPI：
   - 单AP接入用户数：60 终端。
   - 并发率：20%。
   - Speedtest测速：满足建网标准。
3. 覆盖KPI：95%的区域RSSI ≥ -65dBm。
4. 其他KPI：
   - 漫游时延小于20ms@丢包率10^{-5}。
   - 视频语音等关键业务时延小于10ms。

一景一策

场景	美观性	容量	覆盖	推荐AP选型	安装方式	网规方案
镂空区	高	高	高	室内外置天线AP + 定向天线	挂壁	安装在检录摄像头附近，AP正对乘客排队区，同向AP间距15米。
普通区	高	高	高	室内内置全向天线AP	吸顶	安装在顶部天花下方或者借助美化罩，AP正向下覆盖，W型部署，AP间距18米。

目录

智能运维方案部署设计

- 华为iMaster NCE-CampusInsight，颠覆传统聚焦资源状态的监控方式，将人工智能应用于运维领域，通过Telemetry技术采集网络设备的性能指标和日志数据，通过大数据、人工智能算法及更多高级分析技术，通过场景化的持续学习和专家经验，将运维人员从复杂的告警和噪声解放出来，使得用户网络体验可视化、运维变得自动化和智能化。
- 智能运维方案集成了iMaster NCE-CampusInsight、iMaster NCE-Campus和设备等组件，当前iMaster NCE-CampusInsight支持对华为云交换机、云AP设备的管理和智能分析。

网络带宽设计	部署位置设计
由于设备需定时上报数据到iMaster NCE-CampusInsight，园区网络需要预留带宽保障数据上报，平均每设备消耗3Kbps带宽。	iMaster NCE-CampusInsight和iMaster NCE-Campus可以部署在不同位置，只要两者网络互通就可以协同工作，但是为了避免中间网络不稳定性，建议两者部署在同一位置，如同一个数据中心。

智能运维设计注意事项

网络部署设计注意事项

- 网络部署时，需要保证网络设备和分析器之间路由可达，网络设备能将KPI性能数据和日志信息上送到iMaster NCE-CampusInsight。
- 网络部署时，需要保证设备时钟和分析器的时钟保持同步，建议部署NTP Server来同步网络的系统时钟。

智能无线射频调优功能设计注意事项

同一个区域内的AP，不支持同时部署智能无线射频调优功能和传统无线射频调优功能。

协议回放功能设计注意事项

DHCP相关接入类问题的识别和协议回放，需要AC设备作为DHCP服务器或在AC设备上开启DHCP Snooping功能。

音视频质量分析功能设计注意事项

音视频质量分析功能需要设备将相关日志信息上送到分析器，交换机和WLAN设备配置的日志上送周期要尽量保持一致，上送周期偏差最大不可超过20s。

思考题

1. 针对大型园区网络架构设计，一般选择(　　)组网。

   A. 一层架构

   B. 二层架构

   C. 三层架构

   D. 多层架构

- C

思考题

2. 针对终端规模超过50000的大型园区网络，推荐的Fabric组网场景是(　　)，其中网关位置在(　　)上，Edge位置在(　　)上。

A. 集中式网关

B. 分布式网关

C. Edge

D. Border

E. 接入交换机

F. 汇聚交换机

- BCF

本章总结

- 为了让园区网络满足数字化转型的需求，需要对园区网络进行系统的重构，华为CloudCampus解决方案基于智简网络意图驱动的理念，帮助企业构建一张智能、极简、融合、开放和安全的网络。
- 本课程主要针对大中型园区场景，从方案架构、技术方案对比、工程设计建议、运维等方面分别进行了阐述，帮助学员了解华为CloudCampus解决方案技术，并帮助设计出满足要求的最佳园区网络方案。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

CloudCampus中小型园区网络方案

HUAWEI

前言

- 随着技术和行业数字化的发展，尤其是连锁门店、分公司等中小场景业务正逐步通过云化管理的网络接入到企业内部来。
- 云化管理的网络已经成为中小型园区网络建设的趋势，通过采用云化方案，企业可以获得管理效率的提升，网络能够更加快速的支撑新的业务开拓。
- 本章聚焦中小型园区网络，重点介绍中小型园区网络的设计与规划方法，从方案架构、技术方案对比、工程设计建议、运维等方面分别进行了阐述。

目标

- 学完本课程后，您将能够：
  - 描述中小型园区网络的业务需求、发展趋势及挑战
  - 描述华为CloudCampus中小型园区网络方案架构
  - 描述典型的中小型园区网络组网方案
  - 根据用户需求，独立完成CloudCampus中小型园区网络方案设计，含组网设计、物理网络设计、站点开局设计、基础网络业务设计、WLAN设计、准入控制设计、QoS设计、安全设计及运维管理设计

目录

技术发展趋势

网络云化

- 业务的云化架构的演进让企业将精力放在业务上，不用过于关心IT架构的建设。
- 为了适应业务的云化，企业需要创造一个无所不在、智能可控、随需应变的网络。
- 网络需要变革成为一种服务而不是某种解决方案。

万物互联

- 物联网应用导致终端数量和种类出现了海量的增长，产生大量的数据。
- 多样化的传感网需平滑接入到现有网络。
- 接入到园区网络的终端类型变的非常复杂，网络变成了综合多种终端、介质的融合型的网络。

- 网络云化：
  - 云计算在过去十年已经彻底改变了企业的生产方式，大量业务经由云端进行部署和运营，企业因此可以迅速推出新的业务。云化架构的演进让企业将精力放在业务上，不用过于关心IT架构的建设。
  - 而网络作为“端-管-云”中最重要的管道，直接决定了用户的体验。为了适应业务的云化，企业需要创造一个无所不在、智能可控、随需应变的网络。传统的网络架构无法适应这种变化，网络需要变革成为一种服务而不是某种解决方案，这就是网络云化给企业带来的商业价值，也是网络云化发展的趋势。
  - 网络云化是网络服务化的实现手段，正如IaaS让企业不再重复建设基础设施那样，网络云化之后，企业不用关心建设网络需要什么样的架构，在哪里建设网络，功能如何实现，只需要关心企业实现商业价值的时候，网络需要提供什么样的功能，这使得企业彻底获得网络云化带来的好处，更加聚焦业务。
- 万物互联：
  - 物联网应用近年来逐渐成熟，应用也非常的广泛，例如大型仓库中物品的定位、园区资产管理、车库导航等。
  - 首先，物联网在园区网络中的应用，直接导致了接入到网络中的终端数量和种类出现了海量的增长，这必然会产生大量的数据需要传输和存储。
  - 其次，物联网的传感技术多种多样，例如：Bluetooth、ZigBee、RFID等都有各自的应用场景。如何将这些多样化的传感网平滑接入到现有网络中，也是园区网络需要解决的问题。
  - 最后，有了物联网以后，接入到园区网络的终端类型变的非常复杂，网络已经不是单纯的以太网，而是综合了多种终端、介质的融合型的网络。

中小型园区网络的业务需求与挑战

行业变化加速，园区网络业务需求发生了变化

随着网络云化，云计算、云安全、大数据、物联网等ICT新技术的高速发展，各行各业都正在发生翻天覆地的变化。

- 传统商超零售利用免费Wi-Fi吸引顾客，并通过无线定位客流分析数据实现精准营销。
- 在教育领域，电子课堂越来越普及，丰富的多媒体教学更能激发学生的兴趣。
- 中小企业等通过云管理网络互联、远程接入、移动办公、云化数据统一管理和分析，实现业务极简部署、快速开通。

传统的部署管理方案存在以下问题

1. 部署效率低，影响业务开通速度。

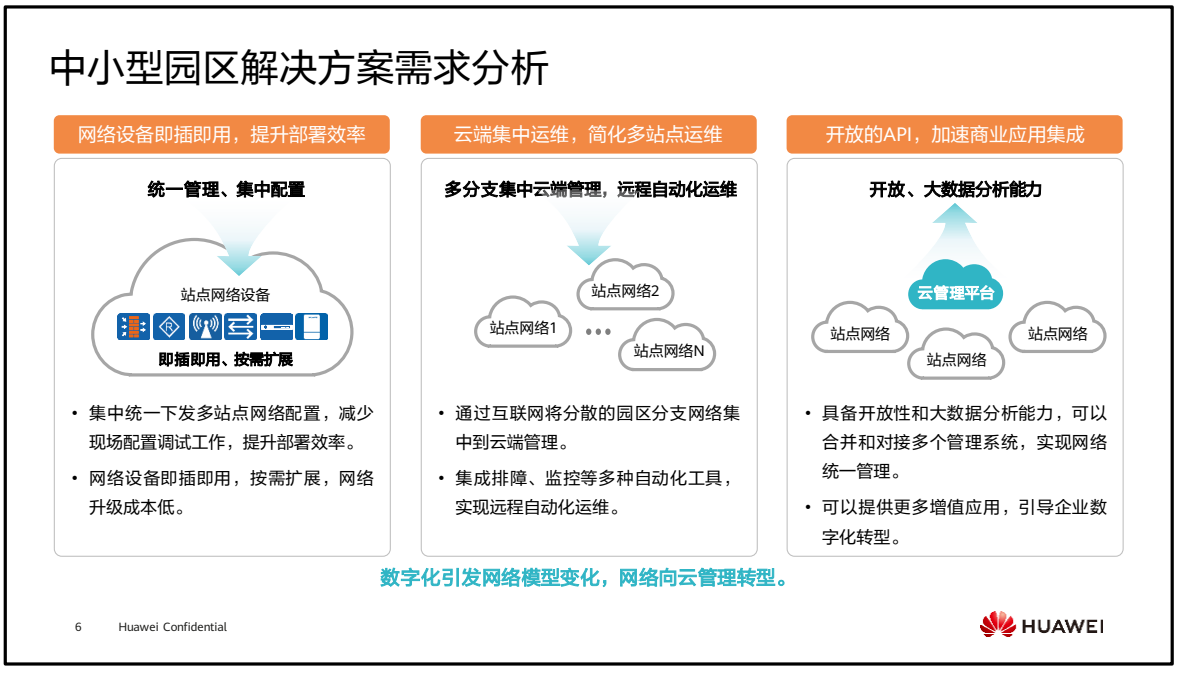
网络的工勘规划、部署、软调配置、优化等一系列工作，全部需要现场专业IT人员完成。

2. 网络管理复杂，OPEX占比居高不下。

本地化、专业化的运维模式导致运维效率低下，人力成本居高不下；网管，策略控制服务器、计费、数据分析平台等独立部署，专业管理维护成本高。

3. 网络开放性差。

传统网络的多管理系统提供的开放数据需要再次整合，同时由于接口的不兼容性，网络对接应用的速度赶不上应用开发速度。



- 华为智简园区网络解决方案将网络管理从本地迁移到云上，实现基于互联网的多分支网络自动化和集中化管理。使得网络管理具备多租户、超大规模、弹性扩展等云的特征，并且可以提供传统网络不能提供的数据收集和分析能力。同时对接入客户的整体流量进行限制，基于某种应用的流量限制、用户可访问URL的管控。
- 网络设备即插即用，提升部署效率。
  - iMaster NCE-Campus集中统一下发多站点网络配置，减少现场配置调试工作，实现部署效率提升。网络即插即用，按需扩展，网络升级成本低。
- 云端集中运维，简化多站点运维。
  - iMaster NCE-Campus可以通过互联网将分散的园区分支网络集中到云端管理，并且集成排障、监控等多种自动化工具，实现远程自动化运维。
- 开放的API，加速商业应用集成。
  - iMaster NCE-Campus的开放性和大数据分析能力，可以合并和对接多个管理系统，实现网络统一管理。也可以提供更多增值应用，引导企业数字化转型。

目录

华为智简园区解决方案部署场景

	本地部署场景 On-Premises Scenario	华为公有云部署场景 Huawei Public Cloud Scenario	MSP自建云部署场景 MSP-owned Cloud Scenario
场景定义	传统模式：客户购买并拥有控制器、分析器等，将其部署在数据中心或者公有云IAAS平台上，管理自己的网络，不对外提供网络管理服务。	华为公有云云管理模式：客户通过购买华为的公有云云管理服务，使用部署在华为公有云平台上的云管理SaaS服务来管理其网络。	MSP云管理模式：MSP购买控制器、分析器等云管理平台软件，部署在其数据中心或者公有云IAAS，对外提供网络管理服务。
运营主体	客户	华为	MSP、运营商
软件报价模式（硬件报价模式均一致）	点餐或者N1套包，均为永久License + SNS	租户订阅模式（激活码形式）	• MSP订阅模式（License文件形式） • 租户不需从华为订阅服务
推荐适用场景	大中型园区网络	中小型园区网络	中小型园区网络

HUAWEI

- 中小型园区网络规模相对比较小，对Capex和Opex比较敏感，因此，其网络管理模式推荐采用公有云云管理模式，通过华为或MSP对外提供的网络管理SaaS服务来管理其网络。
- 采用公有云云管理模式，既可以选择华为公有云云管理，也可以选择MSP自建云云管理模式，二者本质上没有差别，唯一的区别在于运营主体不同，云管理服务的提供者不同。为方便说明，后续若无特殊说明，仅以华为公有云云管理为例进行说明。

华为云管理解决方案价值

增值SaaS

行业化应用

iMaster NCE

iMaster NCE　iMaster NCE CampusInsight

多租户网络




超宽连接，网络和应用品质提升

- 全场景WLAN，大带宽、高并发，低时延。
- 平台和网络安全可靠，符合行业和相关国家法律法规标准。
- 开放API，提供行业化应用，加速数字化转型进程。

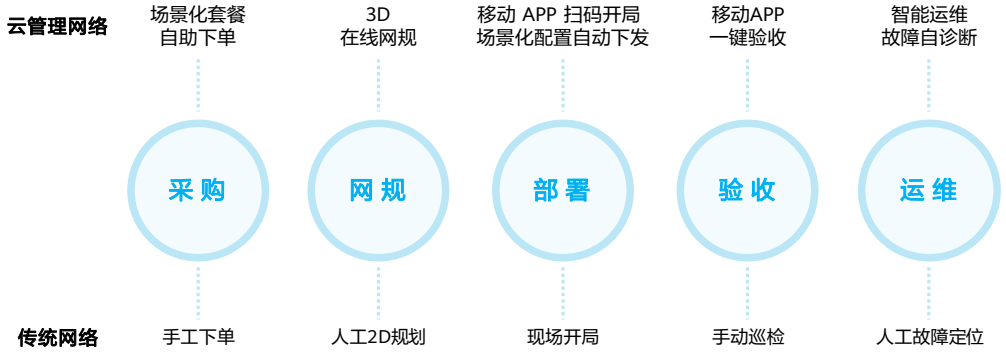
极简管理，OpEx降低

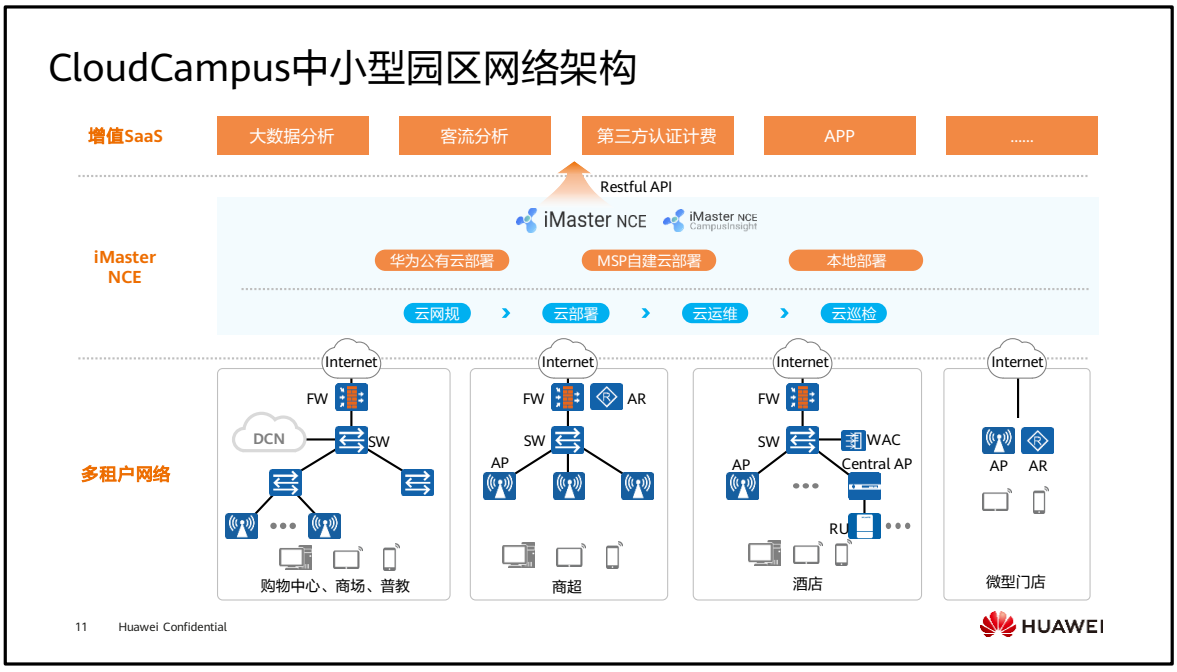
- 室内外在线网规平台，定制化网规模板，网规报告自动生成。
- 多元化的场景配置套餐：拓扑+设备款型及参数，一站式配齐。
- 基于GIS地图、逻辑拓扑、移动APP等丰富的手段运维。
- 多分支在线集中巡检，报告自动生成。

极智运维，基于AI的云化极智运维

- 网络智能运维，保障用户和应用接入体验，潜在故障主动预测。
- SD-WAN：智能保障关键业务的广域互联，带来分支的极致体验。

全生命周期极简管理

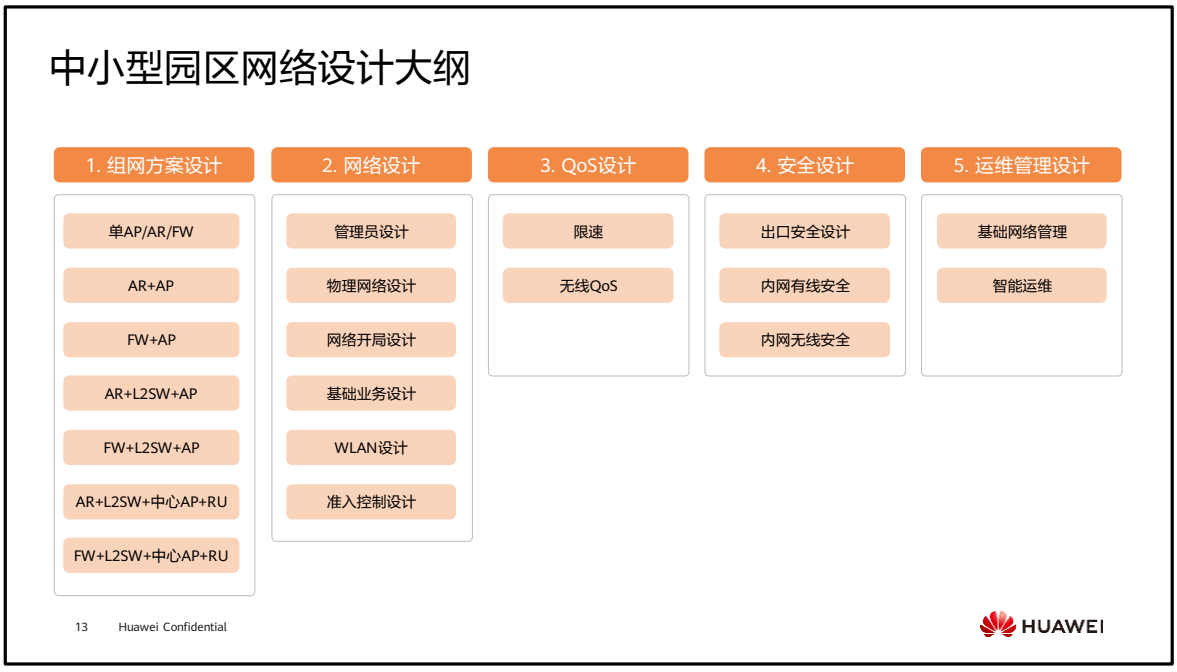




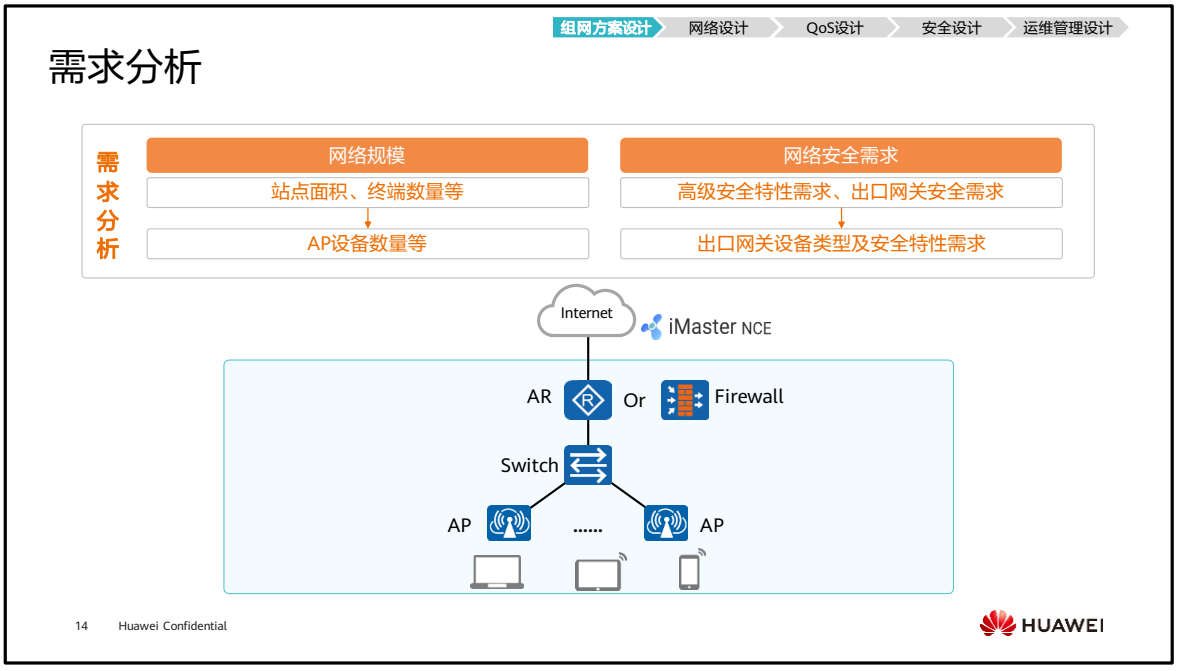
- 华为CloudCampus中小型园区网络解决方案，利用云计算的技术实现网络的自动化和集中化管理，提供传统网络不能提供的数据收集和分析能力，从而实现网络（LAN/WLAN）即服务。
- 华为CloudCampus中小型园区网络解决方案架构分为三层： 多租户网络、iMaster NCE和增值SaaS平台。
- 多租户网络：由包含AP、交换机、防火墙和AR等上百款型的网络设备组成，部署在客户侧，提供用户接入。
- 云管理平台：iMaster NCE-Campus也可以称为云管理平台、SDN控制器，是智简园区网络解决方案的核心部件，是基于云的网络管理运维和控制系统，除了可以对云化设备的基本管理配置、远程运维监控、用户的准入控制外，还可以基于大数据平台实现多样的增值业务。iMaster NCE-CampusInsight网络智能分析平台，是网络的智能分析引擎，为用户网络提供智能运维服务。iMaster NCE-CampusInsight将人工智能应用于运维领域：基于设备性能指标、终端日志等数据，通过大数据分析、人工智能算法及更多高级分析技术将网络中的用户体验数字化，辅助客户及时发现网络问题，改善用户体验。
- 增值SaaS平台：通过iMaster NCE-Campus开放接口与其它业务系统（如大数据等）对接，向租户提供客流分析、商业Portal推送、电子价签、资产管理以及医疗物联网等丰富的增值应用服务。
- 华为CloudCampus解决方案包括华为公有云部署、MSP自建云部署和本地部署三大场景，其中本地部署方案主要面向大中型园区网络，华为公有云部署方案和MSP自建云部署方案面向中小型园区网络，下文将详细介绍这两种部署场景与方案。对中小型企业市场客户提供基础云管理方案，该方案是一个全新的商业模式，对于MSP来说是从卖设备向卖服务进行了转变，对于租户来说实现了设备的云化管理，带来更为便捷

的使用体验。

目录



- CloudCampus中小型园区网络解决方案架构设计思路：
  - 首先构建一个统一承载、按需定义、弹性伸缩的云化园区通信网络，按照用户的需求和使用场景来决定多租户网络的组网方案，并且按照用户实际业务需求进行网络设计，包括物理网络设计、基础网络业务、WLAN业务、用户接入控制设计等。
  - 然后再通过一套集中的云化管理系统，对网络实现自动管理和智能分析，包括开局自动化和智能运维等特性。同时满足安全性、可靠性以及开放性的基础网络属性要求，需要考虑到网络安全性设计以及与其他增值平台的对接设计。



- 在组网方案设计之前，需要提前明确：
  - 客户网络的规模，包括网络部署的面积和网络中预期承载的终端数量。根据这些信息决定部署AP的数量。
  - 客户对网络安全的述求，是否需要一些高级的安全特性、网关出口设备是否需要双机热备等因素来决定出口设备的选型。

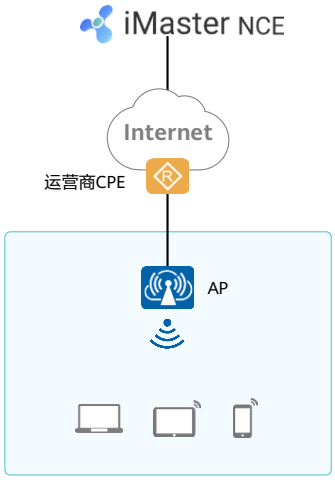
组网方案设计原则（1）

网络规模	出口安全述求	组网关键需求	组网推荐	细分组网推荐
面积<50 ㎡，最大同时在线终端数<50。	低	• 仅无线用户接入。 • 单Internet出口。	单设备组网	AP
	低	• 有线和无线用户接入。 • 需要以太上行或者3G/LTE上行。		AR
面积<300 ㎡，最大同时在线终端数<200。	低	• 仅提供无线接入。 • 需要以太上行或者3G/LTE上行。	出口网关+AP组网	AR+AP
	高	• 需要有线、无线认证接入，多Internet上行。 • URL过滤/IPS/安全防御/AV反病毒等高安全诉求。		FW+AP

组网方案设计原则（2）

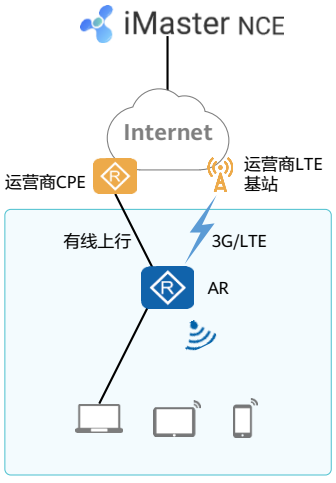
网络规模	出口安全述求	组网关键需求	组网推荐	细分组网推荐
面积<3000 ㎡，最大同时在线终端数<2000。	低	• 有线无线接入，需要多Internet上行。	出口网关+L2SW+AP组网	AR+L2SW+AP
	高	• 有线无线接入，多Internet上行。 • URL过滤/IPS/安全防御/AV反病毒等高安全诉求。		FW+L2SW+AP
面积<3000 ㎡，最大同时在线终端数<2000。	低	• 有线无线接入，多Internet上行。 • 酒店、宿舍等房间密集型场景。	出口网关+L2SW+分布式AP组网	AR+L2SW+中心AP+RU
	高	• 有线无线接入，多Internet上行。 • 出口设备存在双机热备需求。 • URL过滤/IPS/安全防御/ AV反病毒等高安全诉求，适用于酒店、宿舍等房间密集型场景。		AR+L2SW+中心AP+RU

组网方案：单AP组网



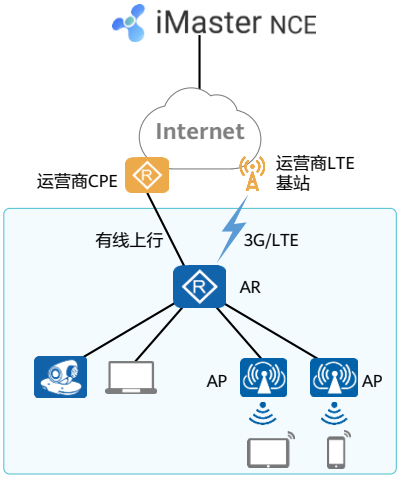
- 方案简介：
  - 单AP组网，AP作为终端用户的网关及园区出口设备。
- 适用场景：
  - 小型连锁门店（如：便利店、加油站）等，面积＜50㎡。
  - 最大同时在线终端数＜50个。
  - 仅需支持无线用户接入。

组网方案：单AR组网



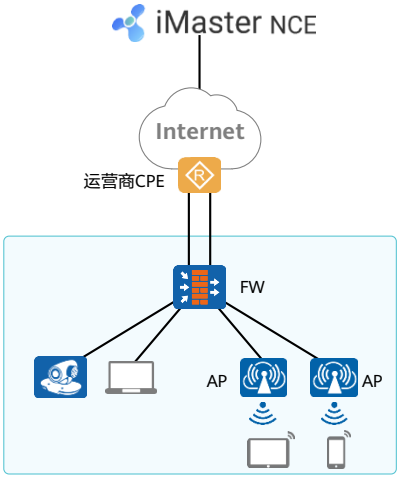
- 方案简介：
  - 单AR组网，AR作为网关提供无线和有线终端接入。
- 适用场景：
  - 小型便利店、服装店等，面积＜50㎡。
  - 最大同时在线终端数＜50个。
  - 需支持有线、无线终端接入，需支持有线上行或3G/LTE上行。

组网方案：AR+AP组网场景



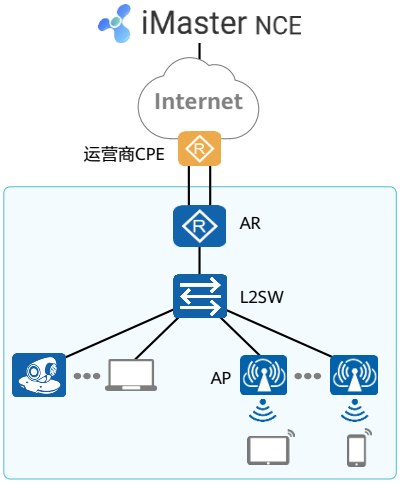
- 方案简介：
  - 需要多个AP满足无线覆盖需求；AR作为用户网关且提供出口特性，如WAN接入、DHCP、NAT等。
- 适用场景：
  - 中小型的服装门店、商超等，门店面积＜300㎡。
  - 最大同时在线终端数＜200个。
  - 需要多AP覆盖，支持有线上行或者3G/LTE无线上行。

组网方案：FW+AP组网场景



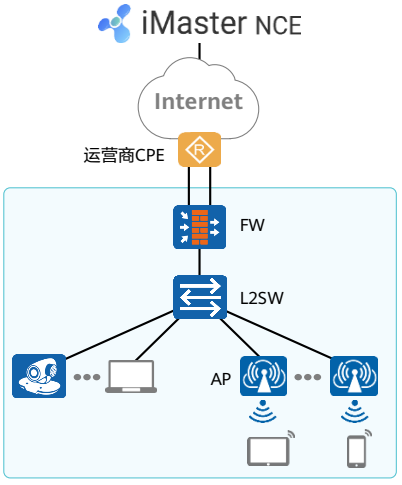
- 方案简介：
  - 需要多个AP满足无线覆盖需求；FW作为用户网关且提供出口特性，比如：WAN接入、DHCP、NAT等。
- 适用场景：
  - 中小型的体验门店、物流门店、保险门店等，门店面积＜300㎡，最大同时在线终端数＜200个。
  - 需要多AP覆盖，需要支持URL过滤、IPS、安全防御、AV反病毒等高级安全功能，同时需要支持多链路上行。

组网方案：AR+L2SW+AP



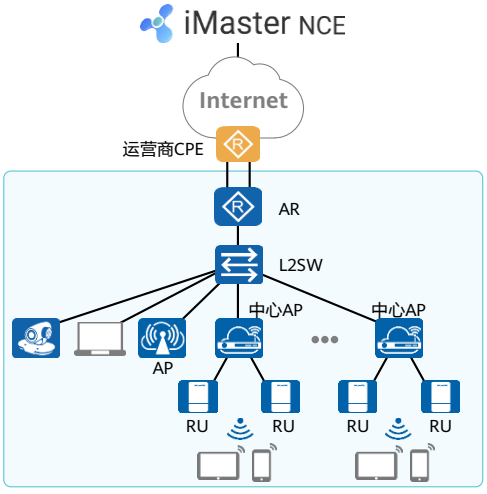
- 方案简介：
  - 通过L2SW PoE扩展接入多个AP提供无线覆盖；
  - 出口网关AR设备提供出口特性，比如：WAN接入、DHCP、NAT等，且作为用户网关；
  - L2SW提供PoE扩展接入和有线终端接入功能，通过部署AP提供站点里的无线终端接入。
- 适用场景：
  - 中小型的服装门店、零售商店等，门店面积＜3000 ㎡，最大同时在线终端数＜2000个。
  - 需多AP覆盖，通过PoE LSW扩展AP的接入，出口支持多链路上行。

组网方案：FW+L2SW+AP



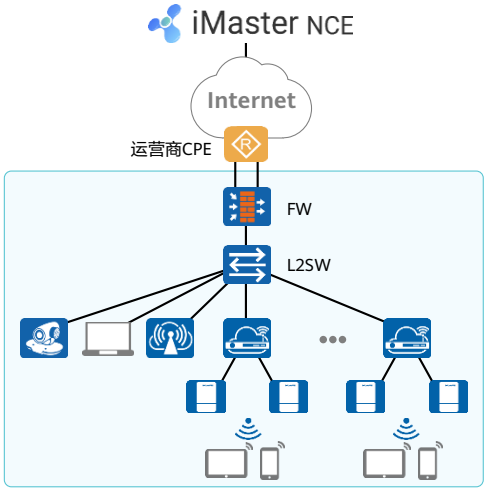
- 方案简介：
  - 通过L2SW PoE扩展接入多个AP提供无线覆盖，FW提供出口特性，比如：WAN接入、DHCP、NAT等， ，且作为用户网关；L2SW提供PoE扩展接入和有线终端接入功能， AP提供站点里的无线终端接入。
- 适用场景：
  - 中小型的体验门店、物流门店、保险门店等，门店面积＜3000 ㎡，最大同时在线终端数＜2000个。
  - 需要多AP覆盖，需要支持URL过滤、 IPS、 安全防御、 AV反病毒等高级安全功能，同时需要支持多链路上行。

组网方案：AR+L2SW+中心AP+RU



- 方案简介：
  - 可免网规，每个房间独立放置RU，AR提供出口特性，如：WAN接入、DHCP、NAT等，L2SW可做有线接入或者作为汇聚的二层交换机，中心AP可提供RU PoE接入和管理，RU提供WLAN无线能力。
- 适用场景：
  - 多房间建筑模式的场景，比如：宿舍、酒店等，门店面积＜3000 ㎡，最大同时在线终端数＜2000个，可以免网规，每个房间独立信号，出口需要支持多链路上行。

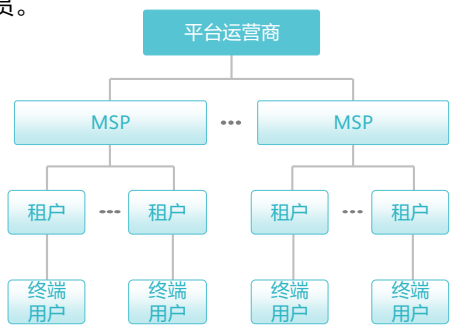
组网方案：FW+L2SW+中心AP+RU



- 方案简介：
  - 可免网规，每个房间独立放置RU。
  - FW提供出口特性，如：WAN接入、DHCP、NAT等。
  - L2SW可做有线接入或者作为汇聚的二层交换机。
  - 中心AP可提供RU PoE接入和管理，RU提供WLAN无线能力。
- 适用场景：
  - 多房间建筑模式的场景，比如：宿舍、酒店等，门店面积＜3000 ㎡，最大同时在线终端数＜2000个，需要支持URL过滤、IPS、安全防御、AV反病毒等高级安全功能，同时需要支持多链路上行。

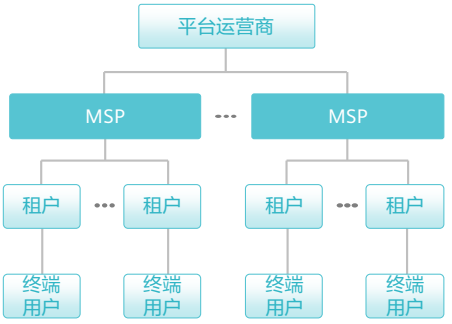
CloudCampus角色 - 平台运营商

- 平台运营商（Operator）是平台管理员或者系统管理员。
- 账号：安装iMaster NCE时由平台运营商自行创建。
- 职责：
  - 安装和维护iMaster NCE
  - 管理MSP/租户
  - 全网设备数量与服务统计
  - 基础网络增值服务



CloudCampus角色 - 网络管理服务提供商

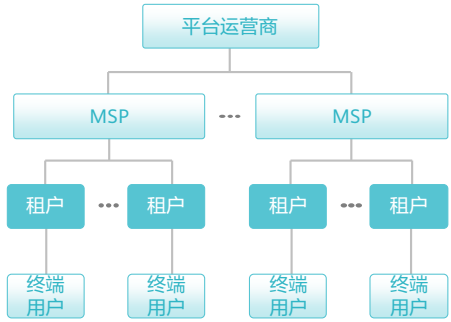
- 网络管理服务提供商（MSP，Managed Service Provider）也称为云管理服务经销商，具有比较专业的网络建设和维护能力。
- 账号：由平台管理员或系统管理员创建。
- 职责：
  - 销售CloudCampus园区方案。
  - 对租户的网络进行监控、定期云巡检，发现异常，评估风险和问题。
  - 如果租户管理员具备一定的IT能力，可以自行部署和运维园区网络，则MSP管理员只做一些简单的开局协助工作。
  - 如果租户管理员不具备一定的IT能力，可向MSP申请代建代维服务，经过授权后由MSP进行代建代维租户的园区网络。



组网方案设计 | 网络设计 | QoS设计 | 安全设计 | 运维管理设计

CloudCampus角色 - 租户

- 租户（Tenant）是园区网络的管理和维护人员，基于自身的业务发展需要出资购买云化设备和服务，组建网络。
- 账号：
  - 由MSP管理员创建。
  - 仅华为公有云部署场景下支持租户自注册。
- 职责：
  - 建设和维护园区网络，根据具备的IT能力分为2种场景：
    - 租户管理员自行部署和运维园区网络，这种场景称为：租户自建自维。
    - 租户管理员向MSP申请代建代维服务，这种场景称为：MSP代建代维。

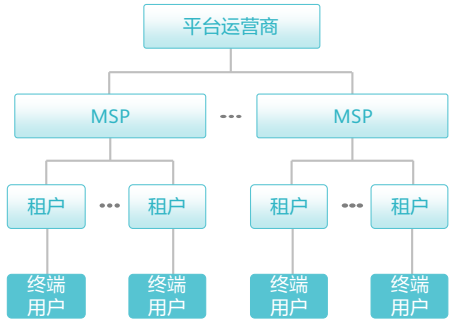


HUAWEI

- CloudCampus支持分权分域：
  - 所谓分权分域，即按照角色、职责和所管理的区域为用户进行授权，将待操作的权限和范围控制到最合理的区间，减小误操作和越级操作引发的业务安全问题的发生概率。分权分域不合理或未进行分权分域，不仅会影响运维效率，更可能会引起用户操作到非管辖范围的网元或执行非本级别用户可被允许的危险操作，从而导致人为因素引发的业务中断。
  - 分权分域以后，平台、MSP、租户在非授权的情况下，不能执行别的机构或者层次的功能。各级超级管理员只能对本级机构起作用，不能越权操作其他机构的权限。比如，平台超级管理员对MSP级的系统管理员没有任何操作权限，MSP级超级管理员不能对租户级超级管理员或者系统管理员进行操作。
- 对租户网络的授权管理范围的设计原则如下：
  - MSP管理员：MSP管理员分配网络管理和配置权限，如果租户向MSP申请代维服务，MSP可直接对租户业务进行维护，此时MSP管理员具备管理全部设备范围的权限。
  - 租户管理员：租户管理员具有网络设备状态查看权限和网络设备配置权限。建议对有运维能力的管理员下发网络设备配置权限；对于无运维能力的管理员下发网络设备状态查看权限，并授权给MSP管理员进行网络维护的权限。租户管理员可以管理的设备范围建议基于站点的范围进行授权，不同的租户管理员可以管理不同的站点设备。租户授权给MSP时，不支持分域，授权会将全部站点的权限授予MSP管理员。

CloudCampus角色 - 终端用户

- 终端用户（End User）是园区网络的最终使用者，例如员工或访客等。
- 账号：NA
- 职责：NA



站点设计

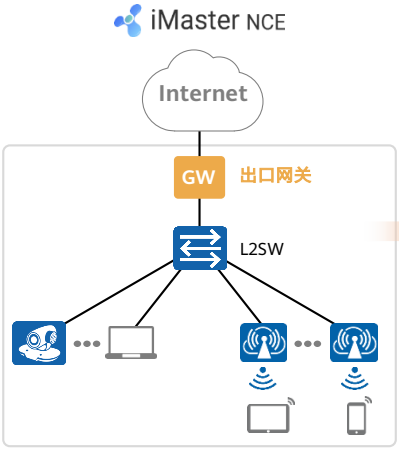
CloudCampus中的站点

站点是智简园区中一个抽象的概念，可以定义为一个独立的网络，比如一个分支机构或者一个独立的园区网络。

站点设计：考虑管理和运维的便利性

- 可以按照物理位置属性将一个独立的分支划分为一个站点，比如银行的一个金融网点或者高校的一个校区。
- 每个站点可以配置独立的租户管理员进行网络运维，也可以统一通过MSP管理员进行运维管理。
- 对于中型园区来说，站点也不宜划分的太多，否则会增加站点间互连的复杂性和管理的复杂性。

站点物理网络设计：出口设计



出口网关设备的选择：

- 高安全应用场景，采用防火墙设备。
- 家庭酒店、小型零售、分支等，可采用AR设备。
- 微型门店仅部署单台AP时，采用AP设备。

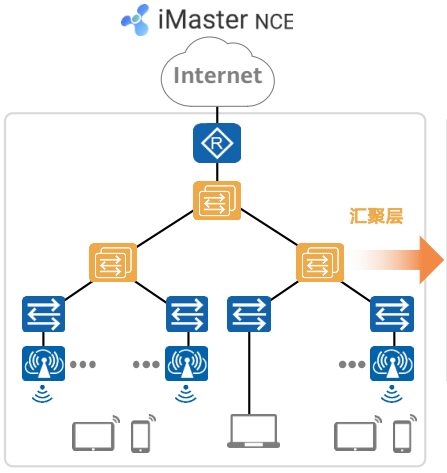
出口组网设计：

- 若网络规模较大，推荐出口采用防火墙或者AR双机组网。推荐多运营商出口链路备份。
- 若网络规模相对较小，推荐出口采用单设备组网，出口采用单运营商链路即可。

出口设备部署主要功能：

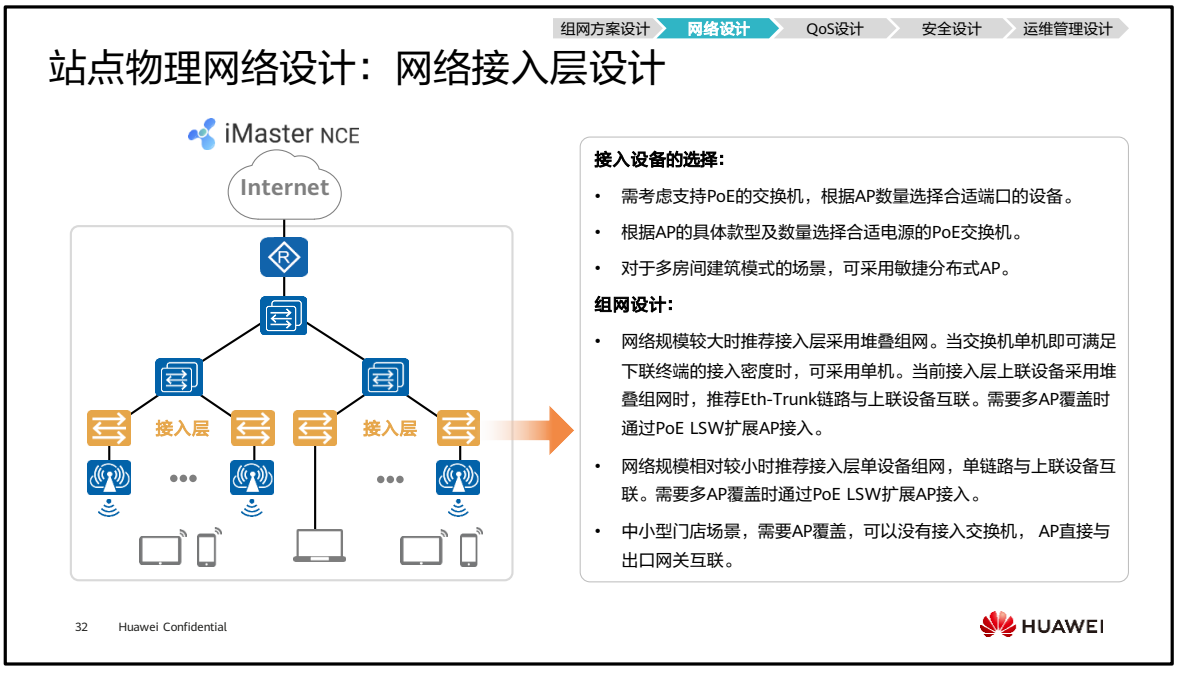
- 需要配置基本的VPN功能、WAN口/拨号接入功能。
- 对于安全有需求的场景，可以部署安全防火墙功能。

站点物理网络设计：网络核心汇聚层设计

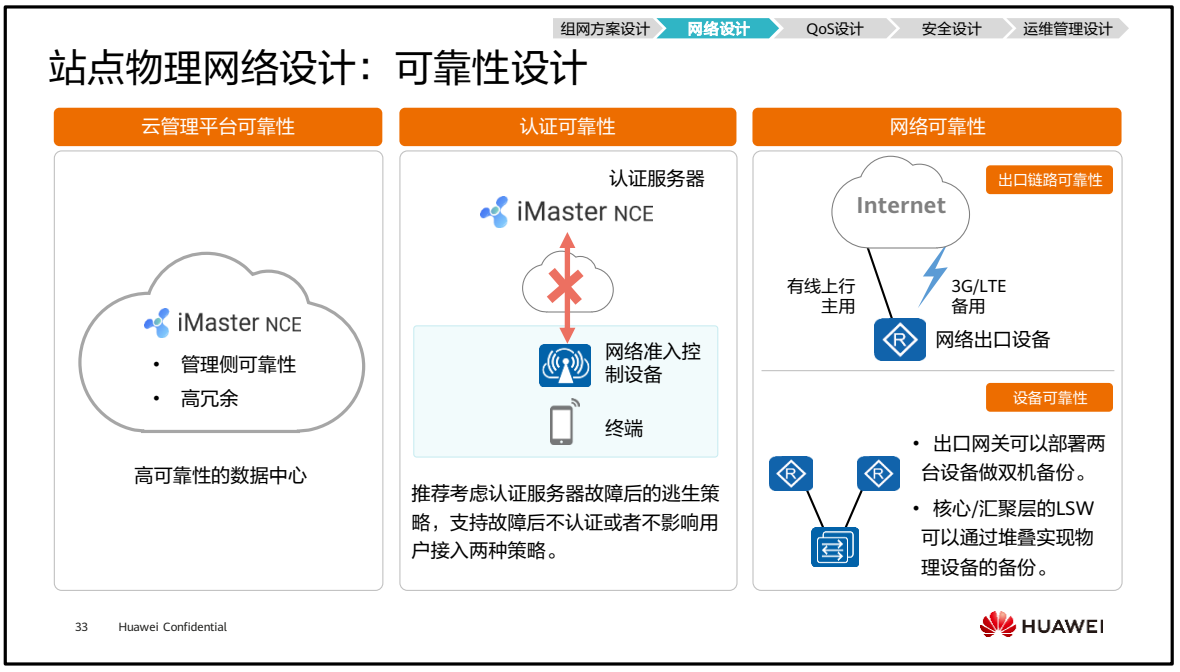


网络汇聚层（含核心层）的设计需要考虑如下方面：

- 若网络规模较大，推荐汇聚层采用堆叠组网。若汇聚层有两层，汇聚层之间通过Eth-Trunk链路互联。推荐出口设备作为用户网关。
- 若网络规模相对较小，推荐汇聚层单设备组网，也可以根据网络的规模和可靠性需求，选择堆叠组网。推荐出口设备作为用户网关。
- 对于小型商超、门店等，网络规模更小，可以没有汇聚层设备。

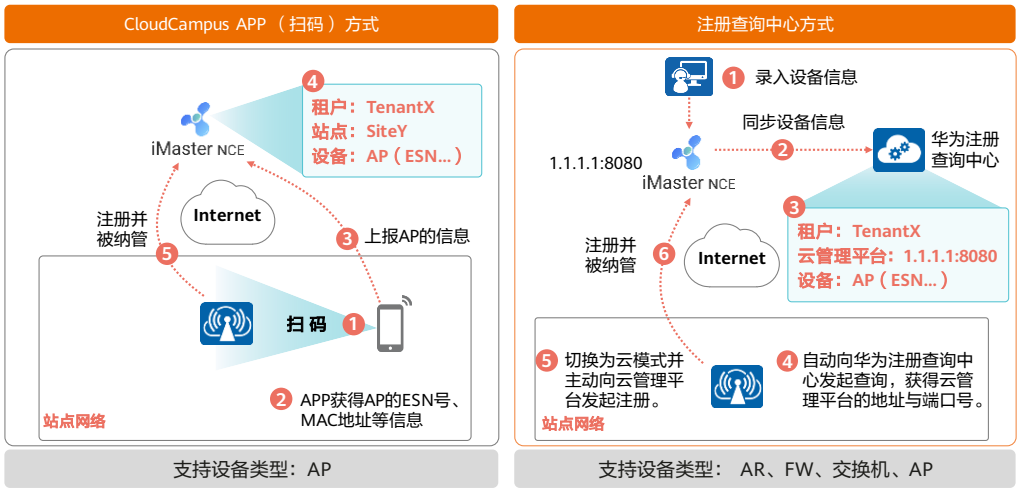


- 接入设备的选择：
  - 需考虑支持PoE的交换机，根据接入AP的数量，选择合适端口的设备。
  - 需考虑接入AP的数量和PoE交换机可以提供的功率关系： AP的功率大概在十几到二十瓦左右，PoE交换机单电源提供的功率一般在三百多瓦，所以要根据AP的具体款型，选择合适电源的PoE交换机。
  - 对于酒店、宿舍等多房间建筑模式的场景时，采用中心AP， 提供RU PoE接入和管理，RU提供WLAN无线能力。
- 组网设计：
  - 对于中型的商超、普教场景，网络规模较大，推荐接入层采用堆叠组网。当接入单机即可满足下联终端的接入密度时，可接入层采用单机组网。当前接入层上联设备采用堆叠组网时，推荐Eth-Trunk链路与上联设备互联。需要多AP覆盖，通过PoE LSW扩展AP接入。
  - 对于酒店、中小型商超、中型门店等场景，网络规模相对较小，推荐接入层单设备组网，单链路与上联设备互联。需要多AP覆盖，通过PoE LSW扩展AP接入。
  - 中小型门店场景，需要AP覆盖，可以没有接入交换机， AP直接与出口网关互联。



- iMaster NCE-Campus部署在云上，管理侧的可靠性由iMaster NCE-Campus提供。由于iMaster NCE-Campus部署在具有高可靠性的数据中心，同时云管理软件具有高冗余的特点，因此在网络设计中重点考虑网络的可靠性。
- 认证可靠性：对于设备与认证服务器对接的场景，推荐考虑认证服务器故障后的逃生策略，目前支持故障后不认证或者不影响用户接入两种策略。
- 网络的可靠性主要涉及链路的可靠性、设备的可靠性。
  - 出口链路可靠性：一般场景多为单链路出口，则不用考虑多链路的备份，对于高可靠场景，则需要部署多链路出口，对链路进行主备配置。
  - 园区内部链路可靠性：一般可以使用Eth-Trunk技术来保证链路的可靠性，建议交换机堆叠组网采用跨设备Eth-Trunk来保证链路可靠性。
  - 设备的可靠性：出口网关设备可以部署两台设备做双机备份，核心/汇聚层的LSW设备，可以通过堆叠实现物理设备的备份。

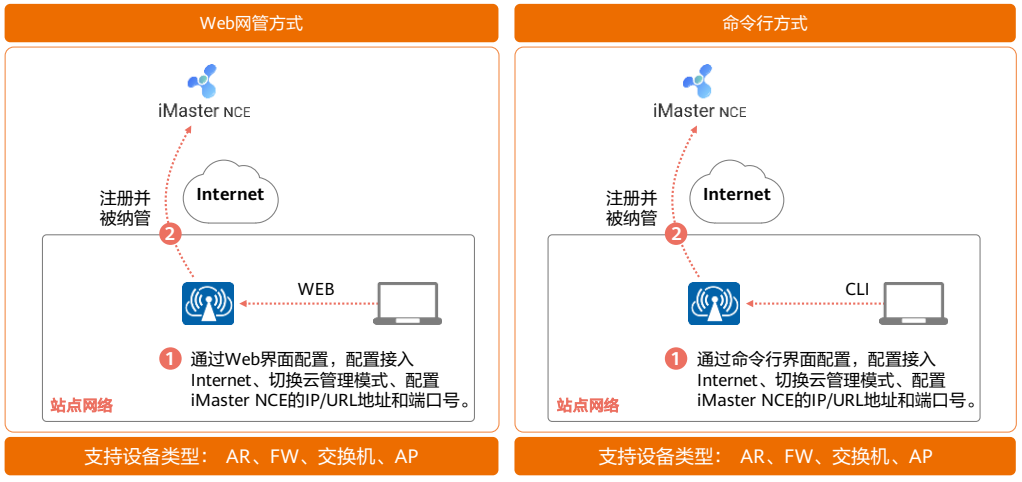
网络开局设计：开局方式（1）



HUAWEI

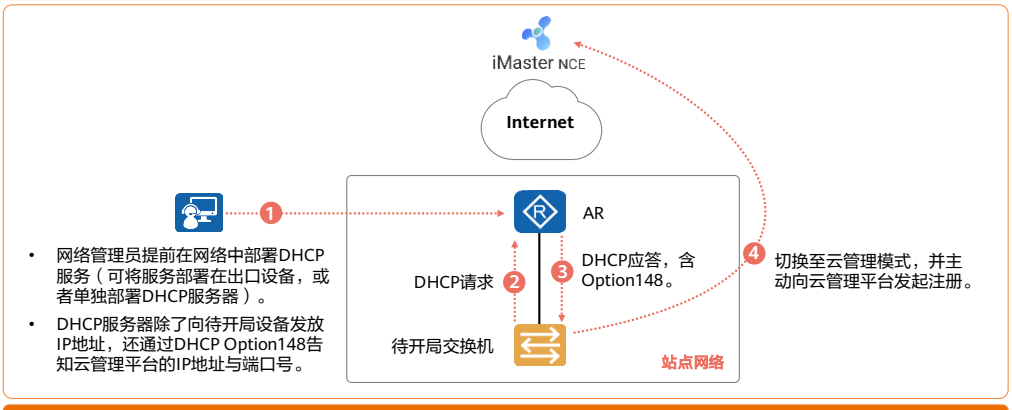
- 注册查询中心是华为在Internet上设立的公有云服务，可以理解为一个云上平台。主要用于实现用户网络设备的即插即用。对于网络设备的开局配置而言，最重要的是向iMaster NCE发起注册并被纳管。华为CloudCampus支持公有云部署模式、MSP自建云部署模式，因此在Internet上可能存在多个iMaster NCE的实例，那么网络设备开机接入网络后，如何知道该向哪一个iMaster NCE发起注册呢?
- 华为设立了注册查询中心，用户可以选择注册查询中心方式来实现CloudCampus华为公有云或MSP自建云场景下的网络设备即插即用。用户首先在iMaster NCE上录入待管理网络设备的信息，其中包括设备的SN号等。iMaster NCE将该信息同步给华为注册查询中心，注册查询中心会维护相关信息。当用户购买的华为云管理网络设备以出厂的方式接入网络并获取IP地址后，会主动向注册查询中心发起查询。设备在出厂时已经预置注册查询中心的域名，该域名全球统一，设备通过不同地区的DNS服务器发起解析请求并得到各地的注册查询中心地址。此后注册查询中心会将设备对应的iMaster NCE的IP地址等信息返回给设备，于是设备便能向该地址发起注册申请，完成纳管过程。

网络开局设计：开局方式（2）



网络开局设计：开局方式（3）

DHCP Option148方式



- 网络管理员提前在网络中部署DHCP服务（可将服务部署在出口设备，或者单独部署DHCP服务器）。
- DHCP服务器除了向待开局设备发放IP地址，还通过DHCP Option148告知云管理平台的IP地址与端口号。

支持设备类型： AR、交换机、AP

网络开局设计：出口网关设备开局方式推荐

场景	出口网关的推荐开局方式		
	AR	防火墙	AP
华为公有云部署或者MSP自建云部署场景，出口网关设备只能通过静态配置方式或PPPoE方式获取IP地址。	Web网管开局	Web网管开局	CloudCampus APP方式开局
本地部署场景，出口网关设备无法通过DHCP方式获取外网接口IP地址。	Web网管开局	Web网管开局	CloudCampus APP方式开局
华为公有云部署场景，出口网关设备可直接通过DHCP获取外网接口IP地址。	注册查询中心开局	注册查询中心开局	注册查询中心开局
本地部署场景，出口网关设备可直接通过DHCP获取外网接口IP地址，且DHCP服务器可配置Option148参数。	DHCP Option148开局 或 Web网管开局	Web网管开局	DHCP Option148开局

网络开局设计：内网（LAN侧）设备开局注册

- LAN侧网络主要指LSW和AP，这些设备都部署在内网中。
- 公有云部署时，推荐部署使用注册查询方式开局。
- 对于不想将设备信息同步给注册查询中心的企业，也可以采用DHCP Option开局方式。

组网场景		LAN侧设备开局方式	
		LSW	AP
华为公有云部署	网络中不能配置DHCP option	注册查询中心	
	网络中可以配置DHCP option	注册查询中心/DHCP option	
MSP自建云部署	网络中不能配置DHCP option	WEB网管	CloudCampus APP开局
	网络中可以配置DHCP option	注册查询中心/DHCP option	

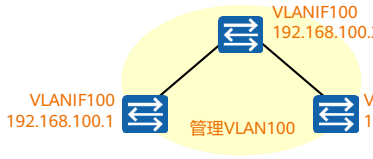
基础业务设计：VLAN设计

- VLAN编号建议连续分配，以保证VLAN资源合理利用。
- 建议预留一定数量的VLAN以方便后续扩展。
- VLAN划分需要区分业务VLAN、 管理VLAN和互联VLAN。
- 最常用的划分方式是基于接口的方式，根据不同的设计原则，将接入交换机不同接口划分到不同的VLAN， 从而实现不同业务类型用户的隔离需求。

业务VLAN设计

- 按地理区域划分VLAN
- 按逻辑区域划分VLAN
- 按人员结构划分VLAN
- 按业务类型划分VLAN

管理VLAN设计



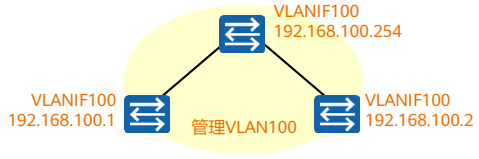
通常，二层交换机使用VLANIF接口地址作为管理地址。建议所有的二层交换机使用同一管理VLAN， 管理IP地址处于同一网段。

HUAWEI

- 业务VLAN不建议采用VLAN1。

基础业务设计：IP地址规划

管理IP地址

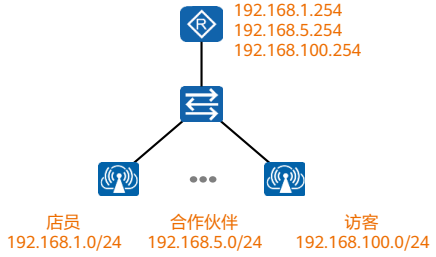


二层设备使用VLANIF地址作为管理IP地址，建议网关以下的所有二层交换机使用同一IP网段。

互联IP地址

互联IP地址推荐使用30位掩码的IP地址，核心设备可使用主机地址较小的IP地址。

业务IP地址



业务IP地址是服务器、主机以及网关的IP地址。

- 网关IP地址推荐统一使用相同的末位数字，如.254。
- 各业务IP地址范围要清晰区分，每一类业务终端IP地址连续、可聚合。
- 建议使用掩码为24位的IP地址段。

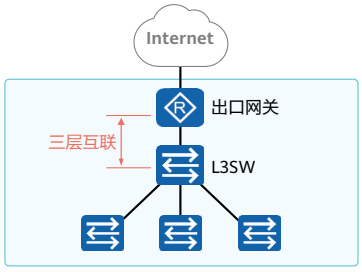
HUAWEI

- 业务IP地址是服务器、主机以及网关的IP地址。网关IP地址推荐统一使用相同的末位数字，比如：.254都是表示网关。各业务IP地址范围要清晰区分，服务器和客户端的IP地址范围也要清晰区分，每一类业务终端IP地址连续、可聚合。考虑到广播域范围及规划的简易程度，建议为每个业务地址段预留掩码为24位的IP地址段，如果业务终端超出200个，再为其顺延一个掩码为24位的IP地址段。

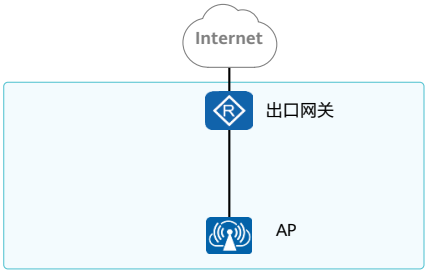
- IP地址分配时可以动态IP分配或者静态IP绑定。在中小型园区中， IP地址具体的分配原则如下：
- 出口网关设备： WAN侧接口的IP地址由运营商进行分配，可以通过静态IP地址、DHCP、 或者PPPoE方式分配，对于出口网关的IP地址需要提前与运营商沟通获取。
- 服务器、特殊终端设备（打卡机、打印服务器、 IP视频监控设备等）建议采用静态IP地址绑定方式分配。
- 用户终端：用户办公用PC、IP电话等设备建议通过在网关设备上部署DHCP Server后，统一通过DHCP方式动态分配。

基础业务设计：IP地址分配方式设计（2）

LAN侧网络设备



当出口网关与L3SW对接时，用于实现对接的互联IP地址建议通过静态的方式手工配置。



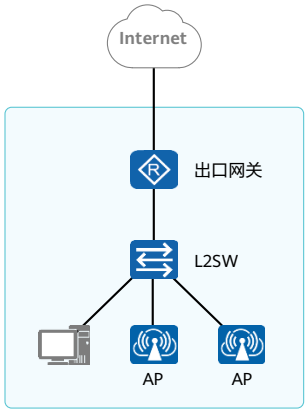
AP设备的IP地址建议通过在网关设备上部署DHCP Server后，统一通过DHCP方式动态分配。

HUAWEI

组网方案设计 网络设计 QoS设计 安全设计 运维管理设计

路由设计

- 园区内部的路由设计：
  - AP设备：通过DHCP分配IP地址后默认会生成一条缺省路由。
  - 交换机、网关设备：通过静态路由即可满足需求，无需部署复杂的路由协议。
- 园区出口的路由设计：
  - 建议在出口设备上配置静态路由来满足需求。



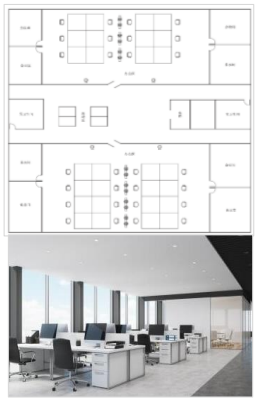
HUAWEI

- 中小型单园区网络的路由设计包括园区内部的路由设计及园区出口与Internet/广域设备之间的路由设计。
- 园区内部的路由设计：主要满足园区内部设备/终端的互通需求，并且可以与外部路由交互。由于中小型单园 区的网络规模比较小，网络结构也比较简单。
  - AP设备：通过DHCP分配IP地址后默认会生成一条缺省路由。
  - 交换机、网关设备：通过静态路由即可满足需求，无需部署复杂的路由协议。
- 园区出口的路由设计：出口路由设计主要满足园区内部用户访问Internet和广域网的需求。出口设备与 Internet或者WAN连接时，建议在出口设备上配置静态路由来满足需求。

WLAN设计：WLAN网规工具

- 云网规缩减规划时间，基于内置经验库确保信号覆盖。

① 获取平面图



② 进入华为在线WLAN网规工具：WLAN Planner
https://serviceturbo-cloud-cn.huawei.com/serviceturbocloud/dist/#/toolappmarket

1.环境设置
2.区域设置
3.设备布放
4.信号仿真
5.导出报告

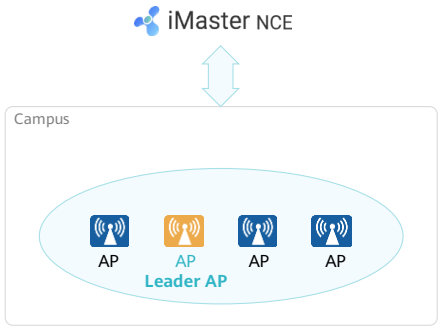
③ 在华为WLAN云网规工具中，用户可以通过简单的5步来完成WLAN网络规划。

④ 使用网规报告指导现场施工
网规结果可导入iMaster NCE。

HUAWEI

- 网规是WLAN工程实施过程中很重要的一个环节，网规设计通常包括如下几个部分：
  - 网络覆盖设计，确定信号覆盖的指标要求与原则。
  - 网络容量设计，基于业务模型与终端行为，确定单用户的带宽诉求，再基于AP的能力确定AP的数量。
  - AP和交换机布放设计，基于布放原则确定部署位置。
  - AP信道设计，进行相邻区域AP的信道规划，以降低同频与邻频干扰。
  - AP供电与走线设计。
- WLAN设计涉及以上多个维度的设计内容，篇幅所限，本文档不展开介绍，读者可参考设计指南学习相关内容。
  https://e.huawei.com/cn/material/networking/campusnetwork/d26a8e9cc9c243a58c8484159680e7a1
- 华为提供了WLAN在线云网规工具，指导用户通过简单的步骤完成WLAN网规操作。

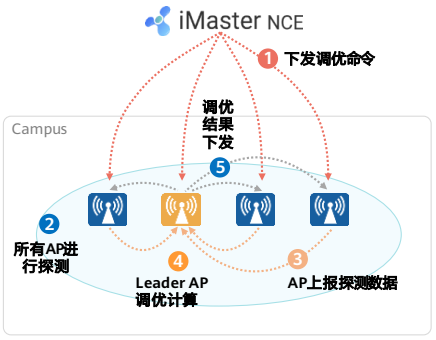
WLAN设计：云管理场景下的Leader AP



- 云AP本质是胖AP。一些WLAN业务如调优需要集中处理，需要一个类似AC的全局控制角色。
- Leader AP，就是在一组AP里面选举一个能力比较强的AP作为Leader AP，负责整个组的全局的业务功能。
- Leader AP负责的业务：调优、负载均衡等。
- Leader选举后，其他AP都会和Leader AP 建capwap链路，以便发送调优、负载均衡的消息。
- Leader AP由云AP自选举。

- 云AP和传统AC调优的核心算法逻辑一致，都是通过AP探测、收集周围邻居射频、干扰信息，然后上报调优计算引擎，计算引擎计算完毕后，将各AP分配的信道、功率下发给对应的AP。
- 和传统AC不同的是，传统网络的调优计算引擎是部署在AC上，云网络的调优计算引擎是部署在Leader AP上。
- 云款型AP的射频调优依赖于一个AP组的Leader AP（选举产生），而Leader AP的管理能力（支持管理的AP数量）是有限的，对于AP数量超过单个Leader AP的管理能力时（不同款型AP的管理能力有差异，例如AP4050DN-E为50个AP，AP6050DN为128个AP），需要进行网络规划（通过规划AP的管理VLAN以实现分组，当一个管理VLAN下的AP数量较多时，会自动划分为多个组）。
- 射频调优是对一个连续区域的无线网络进行调优的，因此建议AP分组时按照例如楼层的方式进行分组，确保一个组内的AP是同一个区域的，保证调优效果。

WLAN设计：云管理场景下的射频调优方式选择



- 支持三种射频调优方式：
  - 自动模式：指定设备根据调优时间与间隔进行周期性的全局调优。
  - 手动模式：设备不会主动进行调优，用户需在iMaster NCE上手动对站点内的AP进行全局或者局部调优。
  - 定时模式：指定设备仅在每天指定时刻触发全局调优。
- AP上根据配置模式执行相应的调优探测，切换信道扫描周边邻居信息。
- AP在探测期间，每隔10s会将探测到的数据上报Leader AP。
- Leader AP每5分钟计算一次调优，共计算3次以达到算法收敛的效果。
- Leader AP将调优结果下发到组内的各个AP，包括计算好的信道、功率等。

- 定时调优时可以选择开启智能无线射频调优，利用分析器对无线网络历史数据进行分析，对网络中的干扰源进行预测。设备在对网络调优时能够提前避让开网络中可能存在的干扰源，提升整个无线网络的质量。
- 在开局阶段，建议在完成AP部署并上线后，进行一次手动调优，以自动完成AP的信道与功率规划。

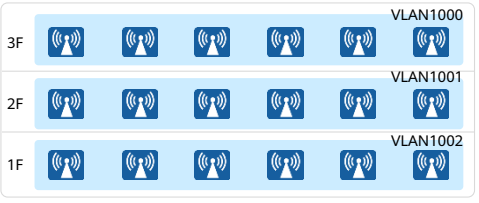
WLAN设计：云管理场景下的AP分组设计

- Leader AP的管理能力（支持管理的AP数量）是有限的。
- 对于AP数量超过单个Leader AP的管理能力时，需要进行网络规划（通过规划AP的管理VLAN以实现分组，当一个管理VLAN下的AP数量较多时，会自动划分为多个组）。
- 射频调优是对一个连续区域的无线网络进行调优的，因此建议AP分组时按照例如楼层的方式进行分组，确保一个组内的AP是同一个区域的，保证调优效果。

随机分组

当超过规格限制时，如果不进行干预，则AP会随机建组，影响调优效果。

根据管理VLAN分组



连续区域内（例如相邻的AP、同楼层的AP）通过规划管理VLAN，划分到同一个组里，每个组内选举自己的Leader AP。

HUAWEI

WLAN设计：信道及频宽选择

AP信道选择

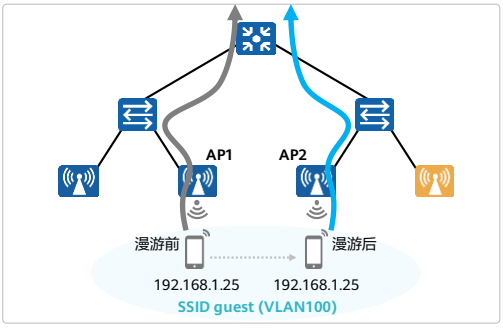
- **对于2.4G频段：**建议选择1、6、11信道集，如果AP部署比较密集的场景，建议选择1、5、9、13。
- **对于5G频段：**当AP使用单5G射频时，建议相邻AP高低频信道错开，当AP使用双5G射频时，则建议两个5G射频分别在低频与高频进行信道规划。

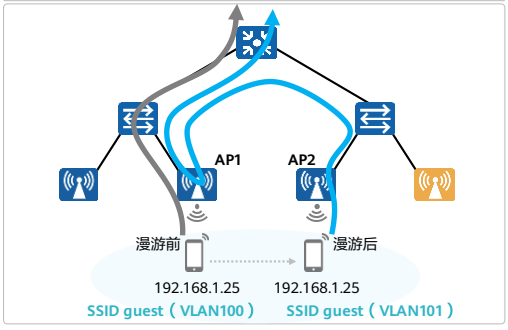
频宽选择

- **对于2.4G频段：**只能选择20M频宽。
- **对于5G频段：**推荐使用40M频宽。

WLAN设计：云管理场景下的无线漫游设计

AP数量小于50，终端数量小于1000	AP数量大于50，终端数量大于1000
1. 采用二层漫游，用户在同一个2层网络内的AP间进行漫游，漫游前后业务VLAN不变。 2. 二层漫游的特点：同一个站点下，两个AP的SSID、业务VLAN相同。	• 采用三层漫游，用户漫游前后的两个AP的业务VLAN不同，不在同一个二层业务域，且对应不同的业务网关。 • 三层漫游的特点：同一个站点下，两个AP的SSID/认证相同、业务VLAN不相同。

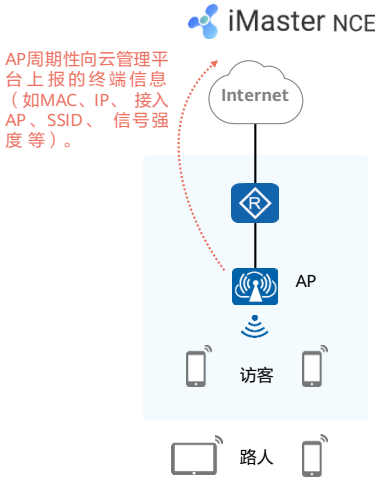




HUAWEI

- 对于802.11r快速漫游，支持与华为终端基于端管协同机制，提供增强的漫游机制，可减小漫游切换时延与丢包，建议开启802.11r快速漫游功能时也开启该增强功能。
- 说明：
  - 无线漫游仅支持在同一个站点内的AP间进行。
  - 二层漫游域比较大时，会有广播泛滥的风险，建议在控制器上配置广播报文限速（缺省为256pps）。
  - 每个AP仅支持64个三层漫游流量迂回的用户，当三层漫游的用户比较多时，会导致漫游失败，需下线重新上线。
  - 由于三层漫游的流量会迂回到终端首次接入的AP上或者与首次接入AP在同一二层域内的其他AP上，因此针对网络入口处的AP，建议规划在一个比较大的二层域中，以便三层漫游后的流量迂回，可以分担到更多的AP上。

WLAN设计：增值业务设计（客流分析）



在企业运营与管理中，通常希望能够更多地掌握客流信息，以更好的优化经营；WLAN无线网络可以获取使用和接入WLAN的顾客的更多信息和特征，以便企业：

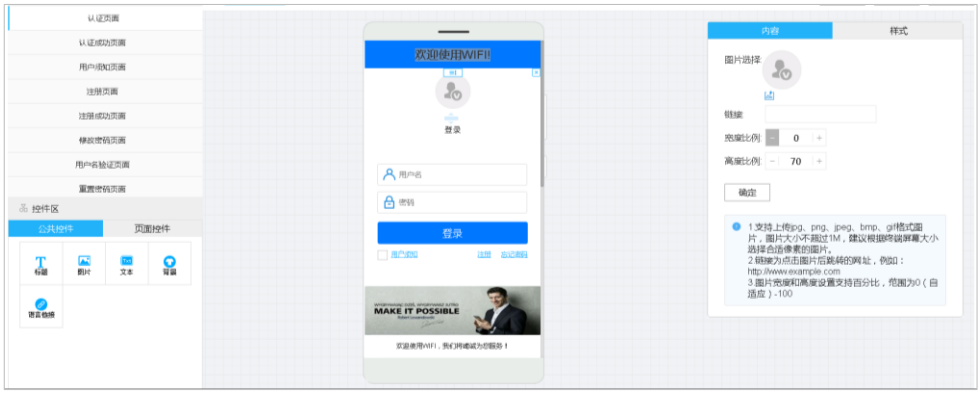
- 掌握客流情况与规律，合理安排市场活动。
- 掌握人流的热点区域，作为租金制定的参考，提高了管理效率与精度。
- 掌握顾客到访的频率，获取高忠诚度的客户，开展促销活动。

- 支持进行客流量统计，包括各时刻的客户流量以及客流量变化趋势。
- 客流分析中，支持识别区分路人与访客，并支持统计访客比例。
- 客流分析中，支持对访客驻留时间的统计与分析。
- 客流分析中，支持对顾客忠诚度的分析（即回头客的重复访问率）。

HUAWEI

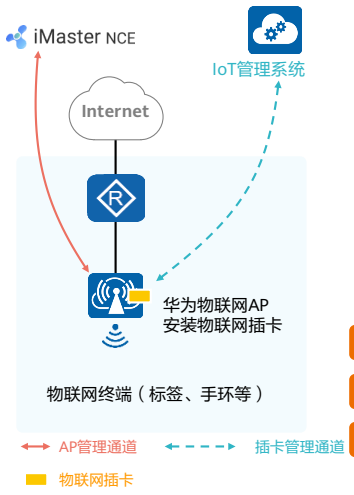
- 客流分析需要AP周期性的向iMaster NCE-Campus上报终端信息（如MAC、IP、接入AP、SSID、信号强度等），因此需要在iMaster NCE-Campus上AP设备所属的站点设置中开启上报终端位置的开关。如果使用终端信息可能存在数据信息安全的风险，则请关闭此开关。
- 客流分析功能缺省是基于站点维度的。如果需要查看站点内部分设备的结果，可以采用设置Tag的方法，对AP进行标示。一台AP可以标记多个Tag，便于使用者从多个角度查看结果。如租户A商场，其B专卖店入口区域的AP，可以设置以下标签：A\B\入口，后续对商场站点中的无线AP的查看和终端行为分析都可以基于Tag维度进行。
- 华为智简园区中小型网络支持跟第三方终端行为管理软件对接，通过第三方软件，可以提供更详细的终端画像、行为分析等业务。华为提供了对接接口，第三方软件可以根据华为的接口进行适配，通过大数据进行客户行为分析，以便进行商业推广。如果有需要可以联系华为。

WLAN设计：增值业务设计（商业Portal推送）



企业可以基于该能力快速简单的定制出适合自己的Portal门户页面，从而进行品牌推广、广告推送等增值业务。

WLAN设计：增值业务设计（IoT融合方案）



- 华为物联网云AP提供管道层能力，一是提供标准的Mini-PCI-E扩展槽位与USB接口，供物联网模块接入；二是提供上行的数据通道。
- 合作伙伴提供提供满足华为接口规范的物联网插卡模块，通过Mini-PCI-E接口或者USB接口接入华为物联网云AP。
- 合作伙伴提供终端层能力，包括各种标签、手环等，与物联网插卡进行交互。

降成本	Wi-Fi与IoT多网融合	解决了站点设计与供电问题
简部署	AP提供站址及通信管道	业务开通简单
可扩展	Mini-PCI-E扩展槽位+USB	物联网插卡安装便捷

HUAWEI

- 华为WLAN在IoT物联网领域，构建基于管道的技术平台和生态系统，充分发挥合作伙伴在IoT领域的专业优势，实现多网融合，给客户带来最大效益。
  - 华为物联网云AP提供管道层能力，一是提供标准的Mini-PCI-E扩展槽位与USB接口，供物联网模块接入；二是提供上行的数据通道。
  - 合作伙伴提供接入层能力，提供满足华为接口规范的物联网插卡模块，通过Mini-PCI-E接口或者USB接口接入华为物联网云AP。
  - 合作伙伴提供终端层能力，包括各种标签、手环等，与物联网插卡进行交互。
  - 华为物联网云AP只提供通道能力，转发插卡模块的上下行数据，不处理具体的物联网业务协议。
- 与传统的IoT方案相比， WLAN的IoT融合方案具有如下优势：
  - 物联网基站与AP共站址，多网融合，解决了站点规划与供电问题，降低部署成本。
  - AP提供上行数据通道，统一入口和统一管理，降低部署复杂度。
  - AP提供管道层的能力，具备灵活可扩展的特点。

准入控制设计：认证技术对比表

对比项	Portal认证	MAC认证	802.1X认证
客户端需求	不需要	不需要	需要
优点	部署灵活	无需安装客户端	安全性高
缺点	安全性不高	需登记MAC地址，管理复杂	部署不灵活
适用场景	通常适用于流动性较大，终端类型复杂的访客用户网络认证。	打印机、传真机等哑终端接入认证的场景。	通常适用于对安全要求较高的办公用户的网络认证。

准入控制设计：云管理的Portal认证适配多种应用场景（1）

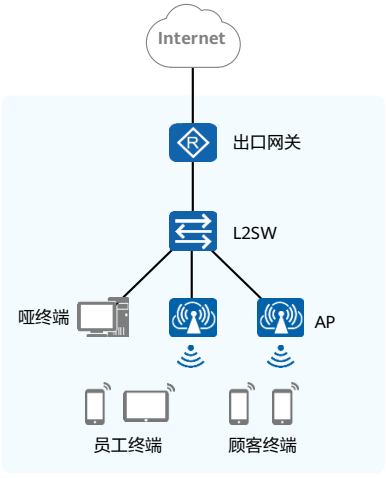
认证方式	特点	依赖条件	适用场景
用户名密码认证	使用租户管理员创建的用户名密码或者终端用户自注册来完成接入认证。	-	管理员创建帐号适用于用户群体相对固定，企业员工可以使用此类方式。 用户自注册方式需要审批，适用于确认访客访问权限场景，比如会员等。
匿名认证	无需任何帐号，直接接入网络，控制器中自动将访客登录的帐号显示为匿名帐号。	-	适用网络开放，需要免费为顾客提供上网服务的场景。
短信认证	终端用户输入手机号作为账户，并点击获取密码按钮，系统自动注册相应的访客帐号和密码信息，并通过短信通知终端用户的密码来完成接入认证。	需要配置短信服务器。	适用访客认证，通过短信认证，可以提高访客身份有效性，商家将更便捷的获得用户信息，与之形成互动。

准入控制设计：云管理的Portal认证适配多种应用场景（2）

认证方式	特点	依赖条件	适用场景
社交媒体认证	通过与微信或者Facebook进行对接联动，确保终端用户在不另外注册帐号的情况下使用自己的社交媒体帐号和密码在业务管理器的页面进行认证，通过认证之后可获得接入网络的权限。	如果是微信认证，企业具有自己微信公众号平台，要求微信公众平台与iMaster NCE之间网络互通。 企业必须向Facebook公司申请自己独立的Facebook帐号，以便获得Facebook公司的合法授权。	微信认证适用于商场门店提供一键关注微信公众号免费上网的场合。 Facebook适用于海外门店提供免费上网场景。
Passcode认证	用户通过在推送的页面上输入Passcode 并完成的接入认证。	-	接入方式较简单，适用门 店访客场景。

组网方案设计 网络设计 QoS设计 安全设计 运维管理设计

准入控制设计：最佳实践



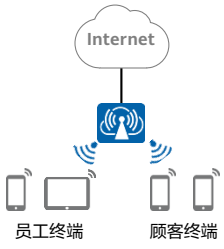
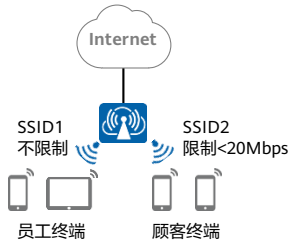
- 顾客建议采用Portal认证，认证点可以根据组网情况在接入AP、AR或者FW中选择。
- 员工可采用Portal认证或者802.1X认证，认证点建议选择接入设备。
- 企业办公哑终端通过有线接入，对于该部分企业办公哑终端，建议采用MAC认证方式，认证点可以选择接入交换机。

HUAWEI

- 对于上述认证类型建议均选择接入设备作为认证点。
- 接入设备作为认证点的优势：
  - 多接入设备分别承载用户认证，比集中认证压力小。
  - 认证点更靠近终端，更安全。
  - 配置规划简单，如果认证点上移，还要考虑认证点设备的性能规格，用户在接入层二层隔离的需求，以及802.1X协议报文在接入层的透传配置问题。

QoS设计：限速

- 在中小型园区网络解决方案中，支持三种限速方案：

基于单用户流量的限速	基于SSID的限速	基于ACL的限速
		
适用于需针对于每个用户流量进行精细化管控的场景，比如：限定VIP用户、企业员工和访客能够获取不同的带宽。	适用于对连接特定服务的所有用户进行综合管控场景，比如：限定所有访客用户的带宽不能超过20 Mbps。	适用于对符合特定特征的流量进行管控的场景，比如：限制网络中的FTP流量等。

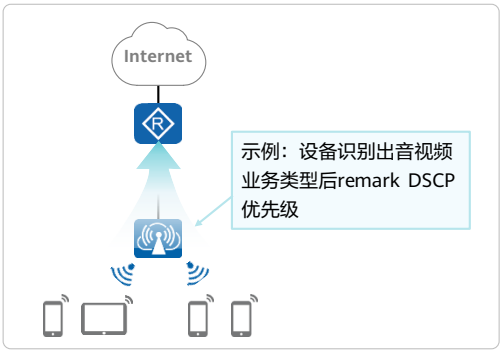
HUAWEI

- 限速的目的是为了防止个别用户或者应用占用了大量的带宽资源，使得其他用户或者应用在使用网络时无法获得充足的带宽资源而影响用户体验。

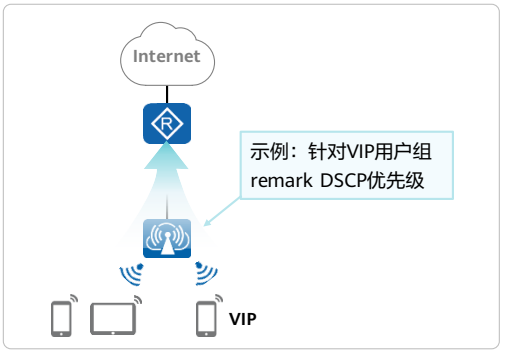
QoS设计：无线QoS（无线队列映射）

- 通过优先级设置方式将用户的流量映射到不同的无线队列中，可以保证语音、视频等对网络参数敏感的业务得到优先调度的机会。

基于应用类型修改DSCP优先级

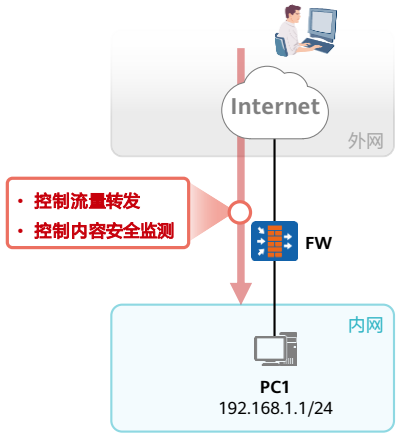


基于用户组remark DSCP设置报文优先级



安全设计：基本概念（安全策略）

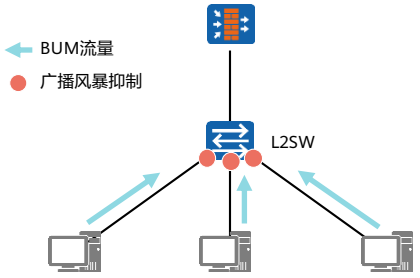
- 设备能够识别出流量的属性，并将流量的属性与安全策略的条件进行匹配。
- 如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作。
- 如果动作为“允许”，则对流量进行内容安全检测。最终根据内容安全检测的结论来判断是否对流量进行放行。
- 如果动作为“禁止”，则禁止流量通过。
- 内容安全一体化检测是指使用设备的智能感知引擎对一条流量的内容只进行一次检测和处理，就能实现包括反病毒、入侵防御、URL过滤、DNS过滤、文件过滤、内容过滤、应用行为控制、邮件过滤、APT防御在内的内容安全功能，通过各种内容安全功能来保证网络安全。



- 安全策略是防火墙的核心功能，在中小型园区通常无需划分过多的安全区域，为了简化配置，建议将WAN侧接口加入到untrust域，LAN侧接口加入到trust域，且放行域间流量。传统防火墙根据五元组（源地址、目的地址、源端口、目的端口、协议类型）来控制流量在安全区域间的转发。华为下一代防火墙的安全策略不仅可以完全替代包过滤的功能，还进一步实现了基于用户和应用的流量转发控制，而且还可以对流量的内容进行安全检测和处理。下一代防火墙的安全策略可以更好的适应新时代网络的特点，满足新时代网络的需求。

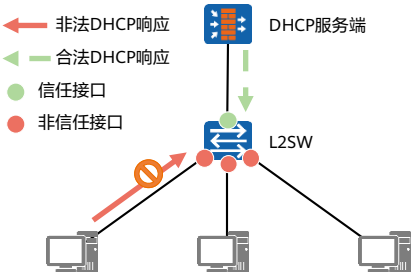
安全设计：内网有线网络安全设计（1）

开启广播风暴控制



在接入层下行接口，部署广播、组播、未知单播报文的抑制，可有效减少广播风暴。

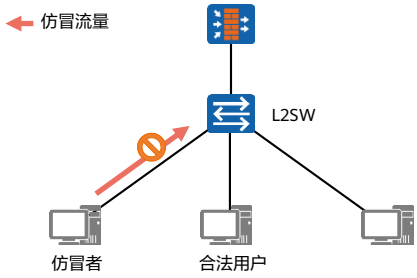
开启DHCP Snooping



开启DHCP Snooping，直接或者间接连接管理员信任的DHCP服务器的接口需要设置为信任接口，其他接口设置为非信任接口，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址。

安全设计：内网有线网络安全设计（2）

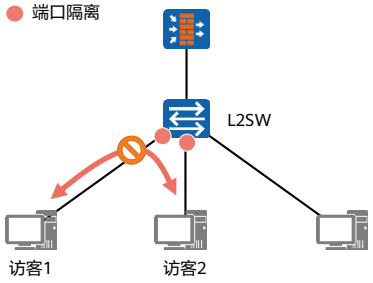
开启IPSG和DAI



IP源防攻击（IPSG）可防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址来访问网络或者攻击网络。

启用DAI后设备会将ARP报文对应的源IP、源MAC、接口、VLAN信息和绑定表中的信息进行比较，丢弃非法ARP报文。

开启端口隔离

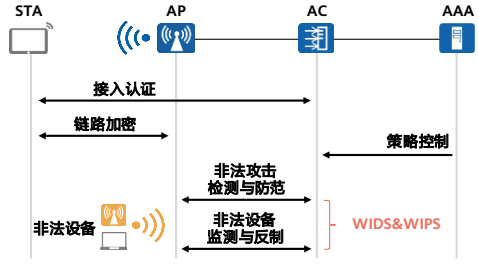


建议在接入交换机连接终端的接口上配置端口隔离，加强用户通信安全，同时避免无效的广播报文影响用户业务。

HUAWEI

安全设计：内网无线网络安全设计（无线空口安全）

WIDS与WIPS功能



为了防止非法设备或者干扰设备的入侵，可开启WIDS与WIPS功能，对网络的非法设备进行检测与反制。

非法攻击检测功能

为了防止WLAN网络受到非法攻击，建议在公共场所以及普教等对安全要求高的场景，启用非法攻击检测功能，对泛洪攻击、弱向量和欺骗攻击等进行检测，自动添加攻击者到动态黑名单中，并发送告警信息及时通知管理员。

HUAWEI

- WIDS（Wireless Intrusion Detection System， 无线入侵检测系统）。WIDS可以检测出非法的AP、无线网桥、无线用户终端、Ad-hoc设备，以及信道重合的干扰AP。
- WIPS（Wireless Intrusion Prevention System， 无线干扰防御系统）。WIPS可以断开合法用户与仿冒AP的WLAN连接，也可以断开非法用户终端和Ad-hoc的接入，实现对非法设备的反制。
- 无线入侵检测系统用于实现对非法终端、恶意的用户攻击和入侵无线网络的行为进行安全检测。无线入侵防护系统是基于WIDS基础上的，进一步保护企业无线网络安全，如阻止企业网络和用户不被非法设备的非授权访问，以及提供网络系统的攻击防护。
- WIDS&WIPS技术相关概念：
  - Rogue AP（非法AP）：网络中未经授权或者有恶意的AP，它可以是私自接入到网络中的AP、未配置的AP、邻居AP或者攻击者操作的AP。
  - Rogue Client（非法客户端）：网络中未经授权或者有恶意的客户端，类似于Rogue AP。
  - Rogue Wireless Bridge（非法无线网桥）：网络中未经授权或者有恶意的网桥。
  - Monitor AP（监控AP）：网络中用于扫描或监听无线介质，并试图检测无线网络中的攻击。
  - Ad-hoc mode（Ad-hoc模式）：把无线客户端的工作模式设置为Ad-hoc模式，Ad-hoc终端可以不需要任何设备支持而直接进行通讯。

安全设计：内网无线网络安全设计（终端接入安全）

- WLAN的802.11标准定义提供了WEP、WPA、WPA2和WPA3等安全策略机制。每种安全策略体现了一整套安全机制，包括无线链路建立时的链路认证方式、无线用户上线时的用户接入认证方式和无线用户传输数据业务时的数据加密方式。

安全机制	特点
WEP	需要预先配置相同的静态密钥，无论从加密机制还是从加密算法本身都很容易受到安全威胁，一般不推荐使用
WPA/WPA2	WPA和WPA2在安全性上几乎没有差别，WPA/WPA2分为企业版和个人版： WPA/WPA2企业版需要使用认证服务器，推荐在大中型园区网络中供企业员工接入使用。 WPA/WPA2个人版提供了简化的模式，不需要认证服务器，推荐在大中园区中功供访客接入使用， 采用WPA/WPA2-PPSK（Private PSK）个人版增强网络安全性的同时兼顾便捷性
WPA3	相较于WPA/WPA2，WPA3主要在以下几个方面有所改进： 新增支持WPA3-SAE，提供更安全的握手协议。理论上SAE握手协议能够提供前向保密，即使攻击者知道了网络中的密码，也不能解密获取到流量。而在WPA2网络中，在得到密码后就可以解密之前获取的流量。所以，WPA3的SAE握手协议在这方面做出了很大的改进。 加强了算法强度，支持安全套件Suite B，也就是WPA3支持256位密钥的AES-GCM和384位曲线的椭圆曲线加密。

- 和WPA/WPA2类似，根据不同的使用场景和安全性要求，WPA3也可以分为企业版和个人版，即WPA3-SAE和WPA3-802.1X。
- 由于WPA2仍在广泛使用，为了能兼容暂时不支持WPA3的终端能接入WPA3网络，Wi-Fi联盟规定了WPA3的过渡模式，即WPA3和WPA2在未来的一段时间里可以共存。该模式仅针对WPA3个人版，WPA3企业版不支持过渡模式。

运维管理设计： iMaster NCE-CampusInsight

AS-IS：以设备为中心的网络管理

- **以设备为中心**，无法感知用户体验。
- **“救火式”响应**，无法识别潜在故障。
- 依靠专业工程师**现场定位故障。**

TO-BE：以用户体验为中心的AI智能运维

体验可视化：基于Telemetry秒级数据采集，每用户每应用每时刻体验可视。

分钟级潜在故障识别和根因定位。

- 基于动态基线、大数据关联等识别潜在故障。
- KPI关联分析和协议回放，精准定位问题根因。

网络预测性调优：通过AI智能分析AP的负载趋势，完成无线网络的预测性调优闭环。

利用算法提升效率，通过场景化的持续学习和专家经验，智能运维将运维人员从复杂的告警和噪声解放出来，使运维更加自动化和智能化。

运维管理设计：基于预测性和AI提升用户和业务体验

实时体验可视

1. **每区域：**通过7维评价体系，直观呈现整网或每个区域的网络状况及用户体验。
2. **每用户：**实时呈现每个用户的全旅程网络体验（谁、何时、连接至哪个AP、体验、问题），故障可回溯。
3. **每应用：**实时语音与实时视频应用体验感知，快速智能定界问题设备，分析质差根因。

分钟级故障定位

1. **主动问题识别：**经过华为20万+终端持续训练的AI算法，主动识别85%的网络潜在问题。
2. **分钟级故障定位：**基于故障推理引擎，分钟级问题定界并识别问题根因，给出有效的修复建议。
3. **智能故障预测：**利用AI学习历史数据动态生成基线，通过和实时数据对比分析从而预测可能发生的故障。

智能网络调优

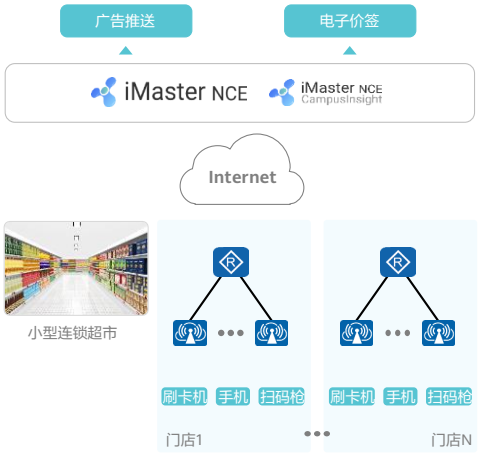
1. **实时仿真反馈：**基于楼层设备的邻居和射频信息，实时评估无线网络信道冲突情况，并给出优化建议。
2. **预测性调优：**基于历史数据的分析识别边缘AP、预测AP的负载趋势，进行无线网络的预测性调优并查看调优前后的增益对比，整网性能提升50%+（Tolly认证）。

开放及生态

HUAWEI

目录

零售行业场景 - 小型连锁



客户需求:

- 门店面积小，分布广，新增门店快速上线。
- 无专业运维人员，出现问题难以短时间内定位问题。
- 门店内人工替换纸质价签速度慢，易出错。

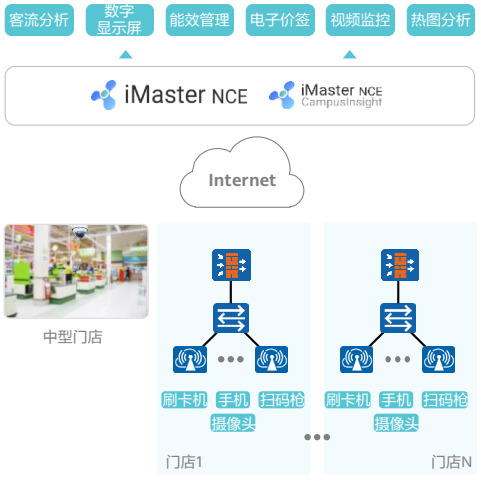
解决方案:

- 扫码开局实现分钟级的无线网络快速上线，云管理平台实现从开局到运维的一站式管理。访客通过portal认证接入网络，支持定制化的广告推送。
- 通过物联网AP内置的物联网插槽实现IoT与WiFi的融合部署，统一规划，共站址回传，电子价签对接超市管理和ERP系统，动态显示并实现实时变价，缺货预警等交互功能。
- 支持对无线扫码枪等无线终端进行批量导入，快速完成海量终端接入。

客户价值:

- 两网合一，融合部署，统一规划，节省投资。
- 价签实时或定时刷新，响应快、零出错、降成本。

零售行业场景 - 中型门店



客户需求:

- 无线终端接入类型多，应用种类多元化。
- 如何有效的支撑销售增长，带来商业上的价值。
- 如何更好的节省人力成本。

解决方案:

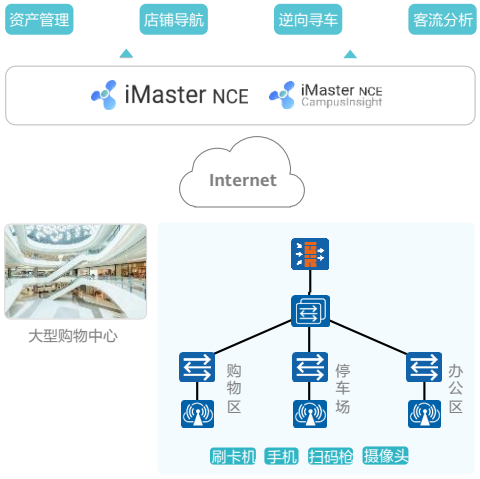
- 采用FW作为出口网关，SW+AP提供有线无线网络接入需求，同时利用交换机给AP和终端设备供电。
- 无线网络实时的将信息上报给大数据分析平台，分析出顾客的喜好习惯，精准的推送广告信息，辅助货物陈列。
- 通过数字显示屏实时展示打折信息，支持在线比价和自助结账。

客户价值:

- 接入设备给摄像头供电节省布线成本，视频监控保障财物安全。
- 帮助客户通过大数据分析系统做运营决策，提升销售业绩，通过精准推送，增加客户粘性。

HUAWEI

零售行业场景 - 大型购物中心



客户需求:

- 有线无线设备统一管理，满足不同类型的终端接入，简化运维。
- 大型购物中心寻车难，影响购物体验。

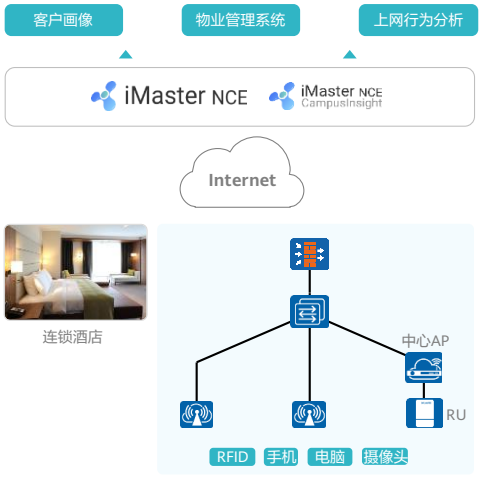
解决方案:

- 采用强核心+接入+AP设备统一进行管理，同时满足突发流量的带宽需求。
- 支持Portal、短信和社交媒体认证；支持MAC认证，保证哑终端（电话、打印机、摄像头）的接入安全。
- WLAN网络通过AP探测采集RSSI场强信息，上报给RTLS，RTLS采用事先建立的指纹库，计算出终端的位置，提供寻车、店铺导航等服务。

客户价值:

- 简化管理无需专业人员进行运维。
- 增强用户购物体验，实现精准营销，同时保障重要资产安全可控。

酒店行业场景 - 连锁酒店



客户需求:

- 无专业技术人员，多个连锁酒店希望远程统一管理、业务快速上线。
- 网络安全合规，满足当地法律法规要求。
- 顾客上网体验好。网络故障能够快速响应，提升顾客满意度。
- 通过网络能给酒店带来增值业务应用，如客户画像、上网行为分析等。

解决方案:

- 采用华为公有云云管理方案，统一管理。通过CloudCampus APP工具完成工勘，网规，开局，验收，运维各个环节远程管理，业务快速上线。
- 采用FW作为出口网关，通过上网行为管理实现安全合规。敏分AP方案。
- 结合Campusinsight实现智能运维。
- 网络数据实时上报给大数据分析平台，从而实现客户画像等增值应用。

客户价值:

- 节省部署成本。网络状态实时监控，故障排障快。
- 丰富的北向接口对接多种应用，一方面提高酒店业务体验，另一方面利用大数据分析给酒店带来盈利。

普教行业场景 - 中小学校园网

- 客户需求：
  - 教委或教育局实现分级分域管理，集中管理和运维区域内多所学校，且需要可视化、简单易懂、易操作的管理平台。
  - 满足校园多种场景的无线覆盖，且基于不用角色进行灵活认证计费。
  - 实现智慧教室，提高教学体验；实现健康监测、电子考勤等增值业务的统一管理。
- 解决方案：
  - 采用华为公有云云管理方案，教委或教育局作为租户，各学校作为站点通过分权分域方式进行管理。
  - AP提供丰富的款型，满足教室、宿舍、礼堂、体育场馆等多场景无线接入。
  - AP提供物联网插槽，实现Wi-Fi与物联网融合，同时，网络数据实时上报给大数据分析平台，从而实现各种数字化业务应用。
- 客户价值：
  - 设备即插即用，远程部署网络，节省部署成本。学校本地无需布署网管等服务器，节约投资成本。
  - 云平台提供丰富的北向接口对接多种应用，方便教委按需订阅。

思考题

1. 已知某中小型门店面积<300㎡，最大同时在线终端数<200。该门店需要多个AP满足无线覆盖需求；同时具有URL过滤/IPS/安全防御/AV反病毒等高安全诉求。则该门店可采用以下哪个组网方案？（　）

   A. 单AP组网

   B. 出口网关FW+AP

   C. 出口网关AR+AP组网

   D. 出口网关FW+L2SW+AP组网

- BD

本章总结

- 华为CloudCampus中小型园区网络解决方案架构分为三层： 多租户网络、iMaster NCE和增值SaaS平台。
- 本章介绍了CloudCampus解决方案，并针对各个场景全面地介绍了CloudCampus中小型园区网络设计，涵盖组网方案设计，网络设计，QoS设计，安全设计以及运维管理设计。最后列举了典型的中小型园区行业场景案例。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

CloudCampus大型园区网络方案部署

VXLAN虚拟化园区网络

HUAWEI

前言

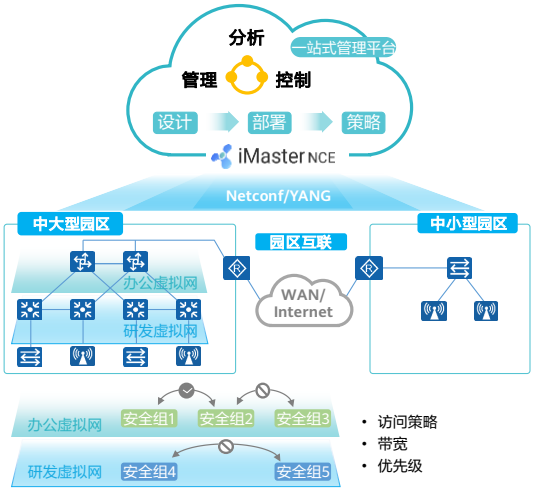
- 区别于传统园区关注独立的单台设备，虚拟化网络关注全网的整体业务体验，通过iMaster NCE-Campus和VXLAN技术，实现网络资源能够任意灵活调度。通过虚拟化技术，将物理网络资源进行池化处理，形成可供业务层任意调动的全网资源池，供iMaster NCE-Campus灵活分配。同时，在一个物理网络上虚拟出多个逻辑上独立的虚拟网络，分别承载多种不同的业务，拥有相对独立的网络资源，做到了业务与网络解耦，方便业务管理。
- 本课程将介绍CloudCampus VXLAN虚拟化园区网络方案部署流程及典型部署案例。

目标

- 学习完本课程后，您将能够：
  - 描述CloudCampus VXLAN虚拟化园区网络方案部署流程
  - 部署典型CloudCampus VXLAN虚拟化园区网络方案
  - 配置iMaster NCE-Campus，完成CloudCampus VXLAN虚拟化园区网络管理及维护

目录

园区网络一站式自动驾驶解决方案



网络开通”快”，部署效率提升

- **设备即插即用：**设备极简开局，场景导航，模板配置。
- **网络极简部署：**网络资源池化，一网多用，业务自动化发放。

业务发放”快”，用户体验提升

- **业务随行：**图形化策略配置，用户漫游权限不变，体验不变。
- **终端智能识别：**终端接入防仿冒，终端智能识别准确率高。
- **智能HQos：**基于应用调度和整形，带宽精细化管理。

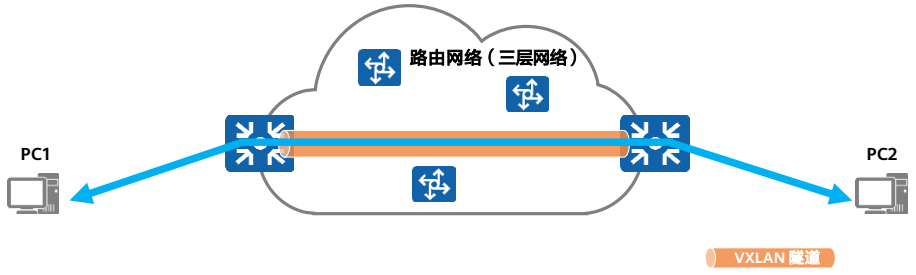
智能运维“快”，整网性能提升

- **实时体验可视：**每时刻、每用户、每区域的网络体验可视。
- **精准故障分析：**主动识别85%的典型网络问题并给出建议。
- **智能网络调优：**基于历史数据的无线网络预测性调优。

HUAWEI

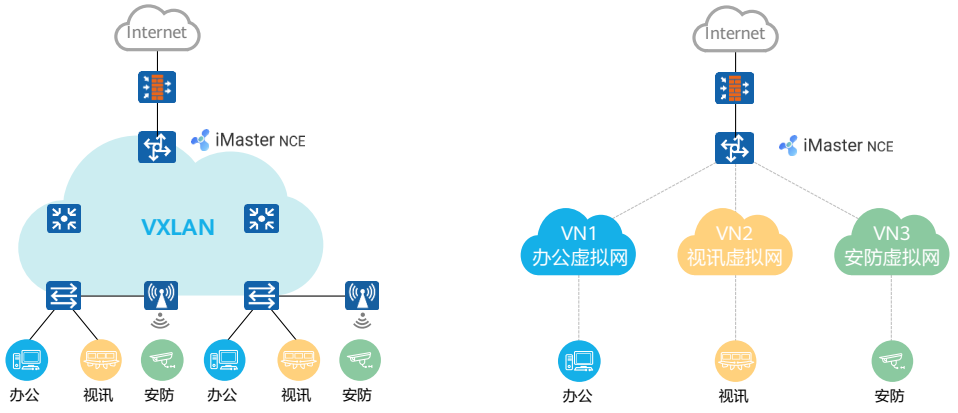
VXLAN简介

- VXLAN在本质上属于一种VPN技术，能够在任意路由可达的网络上叠加二层虚拟网络，通过VXLAN网关实现VXLAN网络内部的互通，同时，也可以实现与传统的非VXLAN网络的互通。
- VXLAN通过采用MAC in UDP封装来延伸二层网络，将以太报文封装在IP报文之上，通过路由在网络中传输，无需关注虚拟机的MAC地址。且路由网络无网络结构限制，具备大规模扩展能力。



在园区网络中引入VXLAN技术

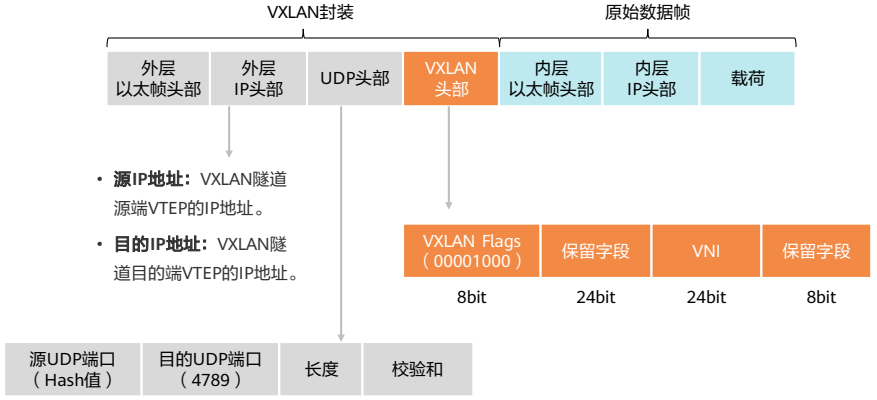
- 一张网承载多种业务，物理网络部署自动化，虚拟网络开通自动化，业务策略发放自动化。



HUAWEI

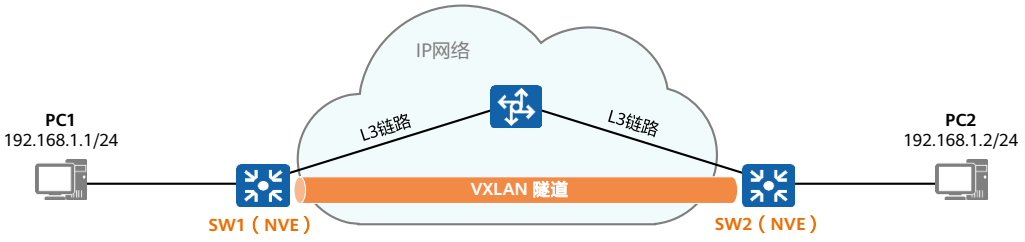
- 通过引入虚拟化技术，在园区网络中基于一张物理网络创建多张虚拟网络（VN，Virtual Network）。不同的虚拟网络应用于不同的业务，例如办公、研发或物联网等。
- 通过iMaster NCE实现全网设备集中管理，管理员通过图形化界面实现网络配置。
- iMaster NCE将管理员的网络业务配置意图“翻译”成设备命令，通过NETCONF协议将配置下发到各台设备，实现网络的自动驾驶。

VXLAN的报文格式



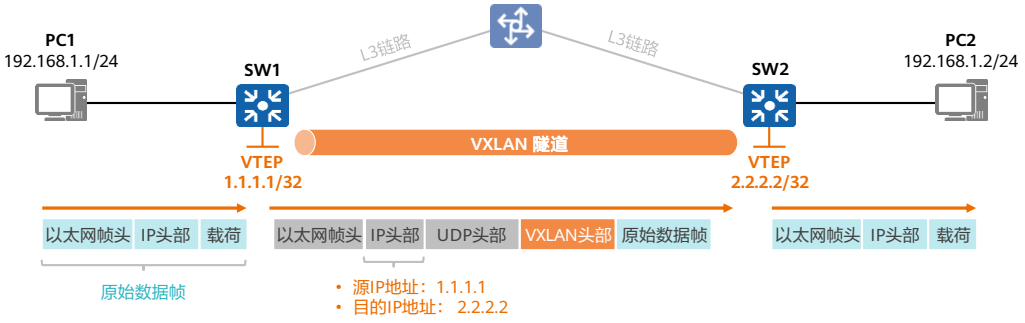
VXLAN基本概念：NVE

- NVE（Network Virtualization Edge，网络虚拟边缘）：
  - 是实现网络虚拟化功能的网络实体，可以是硬件交换机也可以是软件交换机。
  - NVE在三层网络上构建二层虚拟网络，是运行VXLAN的设备。图中SW1和SW2都是NVE。



VXLAN基本概念：VTEP

- VTEP（VXLAN Tunnel Endpoints， VXLAN隧道端点）：
  - VTEP是VXLAN隧道端点，位于NVE中，用于VXLAN报文的封装和解封装。
  - VXLAN报文（的外层IP头部）中源IP地址为源端VTEP的IP地址，目的IP地址为目的端VTEP的IP地址。



HUAWEI

- 一对VTEP地址就对应着一条VXLAN隧道。
- 在源端封装报文后通过隧道向目的端VTEP发送封装报文，目的端VTEP对接收到的封装报文进行解封装。
- 通常情况下使用设备的Loopback接口地址作为VTEP地址。

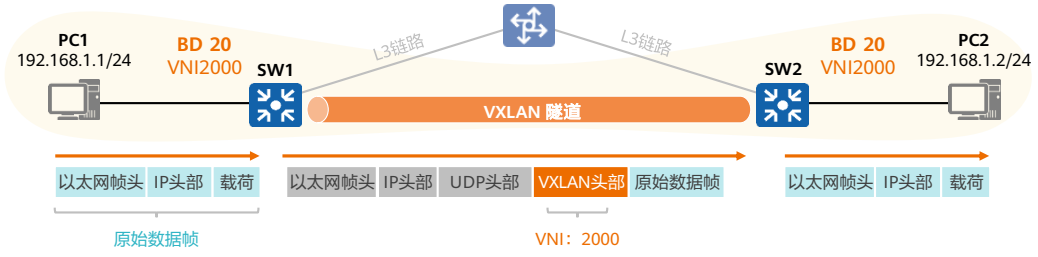
VXLAN基本概念：VNI与BD

VNI（VXLAN Network Identifier，VXLAN网络标识）：

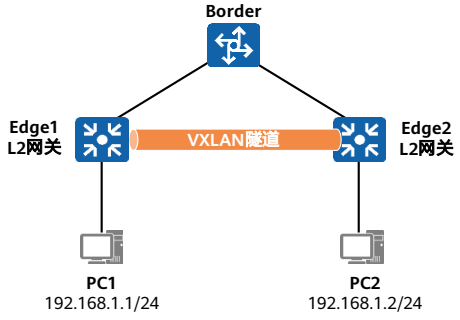
- 类似VLAN ID，用于区分VXLAN段。不同VXLAN段的虚拟机不能直接二层相互通信。
- 一个租户可以有一个或多个VNI，VNI长度为24bit。

BD（Bridge Domain）：

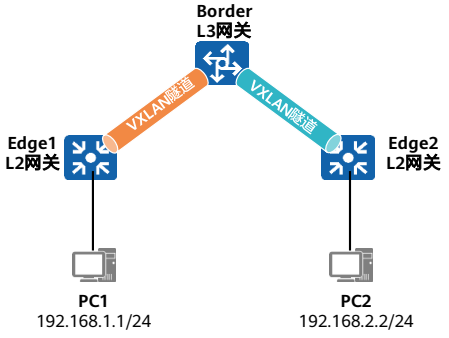
- 类似传统网络中采用VLAN划分广播域，在VXLAN网络中一个BD就标识一个大二层广播域。
- VNI以1:1方式映射到BD，同一个BD内的终端可以进行二层互通。



VXLAN概念：VXLAN二层网关、三层网关

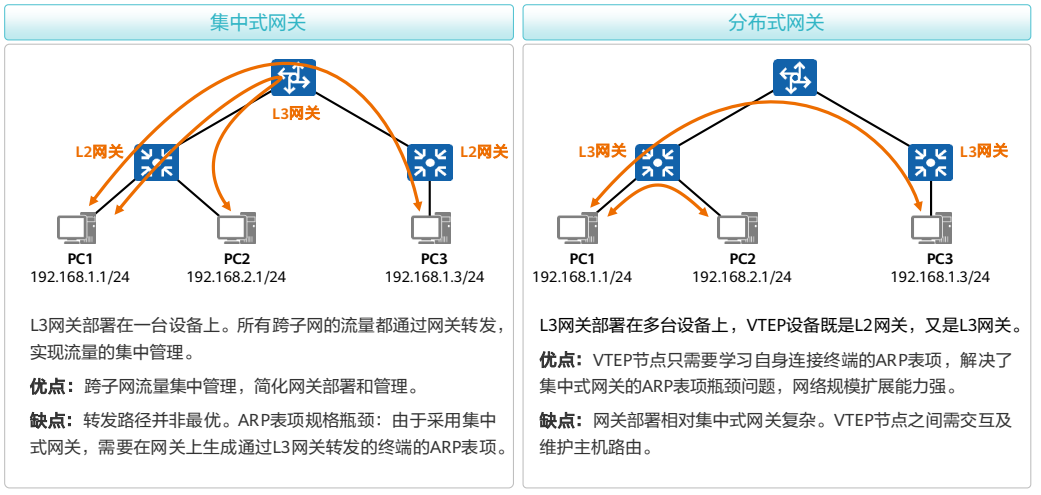


二层（L2）网关：实现流量进入VXLAN虚拟网络，也可用于同一VXLAN虚拟网络的同子网通信。



三层（L3）网关：用于VXLAN虚拟网络的跨子网通信以及外部网络（非VXLAN网络）的访问。

VXLAN概念：集中式与分布式网关



- 大中型园区场景中，智简网络虚拟化方案基于用户网关的位置，主要分为集中式网关和分布式网关两种，iMaster NCE-Campus在创建Fabric时，可以选择采用哪种网关方案。
- 集中式网关方案中，用户网关集中部署在Border节点，所有跨子网的流量都经过Border节点进行转发；分布式网关方案中，用户网关部署在多个Edge节点上，跨子网的流量通过Edge节点转发。

VXLAN隧道的建立方式

- VXLAN隧道由一对VTEP IP地址确定，报文在VTEP设备进行封装之后在VXLAN隧道中依靠路由进行传输。在进行VXLAN隧道的配置之后，只要VXLAN隧道的两端VTEP IP是三层路由可达的，VXLAN隧道就可以建立成功。

手工方式

- 手工在设备上完成配置，建立VXLAN隧道。
- 需要在隧道两端的设备上分别配置源端VTEP与目的端VTEP的IP地址、VNI等。

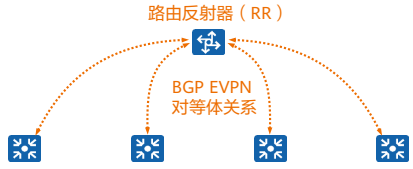
BGP EVPN方式

- 在设备上使能BGP EVPN，设备之间建立BGP EVPN对等体关系。
- 通过BGP EVPN实现VXLAN隧道的按需、自动建立。

HUAWEI

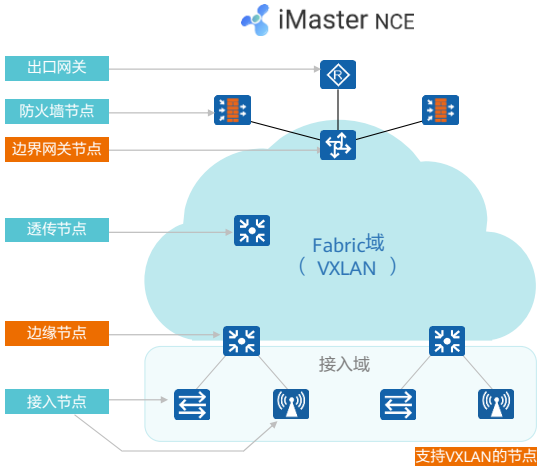
- EVPN（Ethernet Virtual Private Network）通过扩展BGP协议新定义了几种BGP EVPN路由，这些BGP EVPN路由可以用于传递VTEP地址和主机信息，因此EVPN应用于VXLAN网络中，可以使VTEP发现和主机信息学习从数据平面转移到控制平面。

BGP EVPN概述

BGP EVPN	使用BGP EVPN作为控制面协议
• MP-BGP（多协议BGP）对BGP-4进行了扩展，来达到在不同网络中应用的目的。 • EVPN（Ethernet Virtual Private Network）通过扩展BGP协议新定义了几种BGP EVPN路由（在MP_REACH_NLRI属性中新定义了几种NLRI，称作EVPN NLRI）。 • 这些BGP EVPN路由可以用于传递VTEP地址和主机信息，因此EVPN应用于VXLAN网络中，可以使VTEP发现和主机信息学习从数据平面转移到控制平面。	• 基于iMaster NCE的网络自动化方案使用BGP EVPN作为控制面协议。 • 设备将被使能BGP EVPN，并建立BGP EVPN对等体关系。 • 设备之间通过BGP EVPN路由通告完成VXLAN控制面的相关工作。 • VXLAN隧道通过BGP EVPN自动建立，转发表项通过BGP EVPN动态刷新。 

- 为保证IBGP对等体之间的连通性，需要在IBGP对等体之间建立全连接关系。假设在一个AS内部有n台设备，那么建立的IBGP连接数就为n(n-1)/2。当设备数目很多时，设备配置将十分复杂，而且配置后网络资源和CPU资源的消耗都很大。在IBGP对等体间使用路由反射器（Route Reflector，RR）可以解决以上问题。
- 路由反射器相关的基本概念如下：
  - 路由反射器RR（Route Reflector）：允许把从IBGP对等体学到的路由反射到其他IBGP对等体的BGP设备。
  - 客户机（Client）：与RR形成反射邻居关系的IBGP设备。在AS内部客户机只需要与RR直连。
  - 非客户机（Non-Client）：既不是RR也不是Client的IBGP设备。在AS内部Non-Client与RR之间，以及所有的Non-Client之间仍然必须建立全连接关系。
- 同一集群内的Client只需要与该集群的RR直接交换路由信息，因此Client只需要与RR之间建立IBGP连接，不需要与其他Client建立IBGP连接，从而减少了IBGP连接数量。Client将路由通告给RR后，后者会将该路由反射给所有其他的Client。

园区虚拟网络中的网络节点

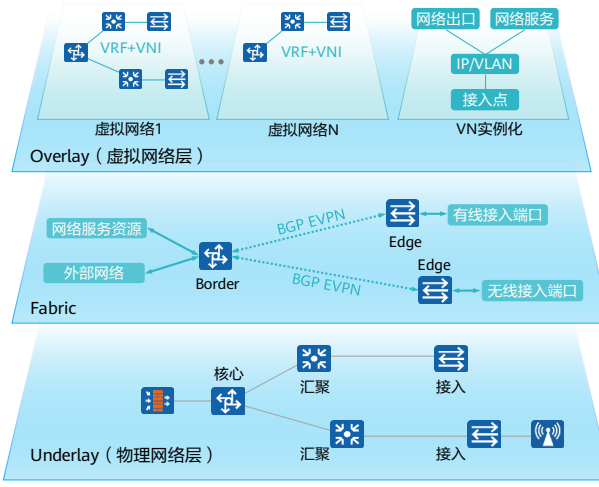


- **出口网关（External Gateway）：**园区网络的出口设备，可以是AR路由器或防火墙。
- **防火墙（Firewall）节点：**部署L4~L7安全策略时需该节点。可旁挂部署，或部署在园区出口处。
- **边界网关（Border）节点：**用于实现Fabric和外部网络之间的互联互通。一般为核心交换机。
- **边缘（Edge）节点：**Fabric边缘设备，用于连接用户侧设备及Fabric。有线用户的数据从边缘节点进入VXLAN封装。
- **传输（Transparent）节点：**Fabric的透传节点，无需支持VXLAN。
- **接入节点：**包含有线接入节点和无线接入节点，一般就是接入交换机及AP设备。其中，有线接入节点可以和Edge节点合一，即VXLAN到接入；另一种组网方式是有线接入节点无需支持VXLAN，并与上联的VXLAN边缘节点建立策略联动。

HUAWEI

- 策略联动是通过在网关设备上统一管理用户的访问策略并且在网关设备和认证接入设备执行用户的访问策略，来解决大型园区策略强度与复杂度之间矛盾的一种解决方案。
- 部署策略联动后，认证接入设备可以自动透传BPDU报文、实时上报用户下线和用户接入位置，同时认证控制设备联动认证接入设备，使其执行用户的访问策略，从而实现了对用户访问网络的控制。

园区虚拟网络架构



- **Fabric：**对Underlay网络抽象后的资源池化网络。在创建实例化的虚拟网络（VN）时，可以选取Fabric中的网络资源。
- **虚拟网络（VN）：**Virtual Network，通过将Fabric实例化，能够构建逻辑上隔离的虚拟网络实例。一个VN对应一个隔离网络（业务网络），比如研发专网。

HUAWEI

- 在大中型园区网络场景中，如果需要通过虚拟化方案做到业务和网络解耦，在不改变基础网络的情况下，实现一网多用和业务的灵活、快速部署，这就对园区的虚拟网络架构提出了异于传统网络的要求。本页展示园区虚拟网络架构，Underlay即为物理网络层，Overlay为基于VXLAN技术构建在Underlay之上的虚拟网络层。
- Fabric组网中，对VXLAN隧道端点VTEP（VXLAN Tunnel Endpoints）做了进一步的角色划分：
  - Border：Fabric网络的边界网关节点，对应实体为物理网络设备，提供Fabric网络与外部网络间的数据转发。一般将支持VXLAN的核心交换机作为Border。
  - Edge：Fabric网络的边缘节点，对应实体为物理网络设备，接入用户的流量从这里进入Fabric网络。一般将支持VXLAN的接入交换机或汇聚交换机作为Edge。

Fabric包含的资源池以及创建VN时资源调用的对应表

Fabric包含的资源池	创建VN时如何调用资源池中的资源
VN资源池，主要是指Overlay能创建的VN数量。	创建VN，每创建一个VN就相当于使用了一个VN资源。
VLAN资源池，VN接入终端、与外部互联等场景使用，配置Fabric全局资源池时规划。	在VN中创建用户网关时，设置的用户VLAN为Fabric全局资源池中的资源。
BD/VNI资源池，VN中划分的二层广播域，对应的VBDIF接口作为用户子网网关接口，配置Fabric全局资源池时规划。	在VN中创建用户网关时，会自动从BD/VNI资源池中调用资源，创建BD广播域及对应的VBDIF接口。
用户接入点资源池，配置Fabric的接入管理时规划，包括接入点绑定的认证方式。	在VN中配置用户接入时，可选取已规划的接入点资源。
外部出口池，指VN可以使用的外部资源，配置Fabric时主要创建两类： 外部网络，用于VN与外部互通。 网络服务资源，用于VN与认证服务器、DHCP服务器等互通。	创建VN时，可选取外部网络和网络服务资源。

目录

部署规划：网关方案选择

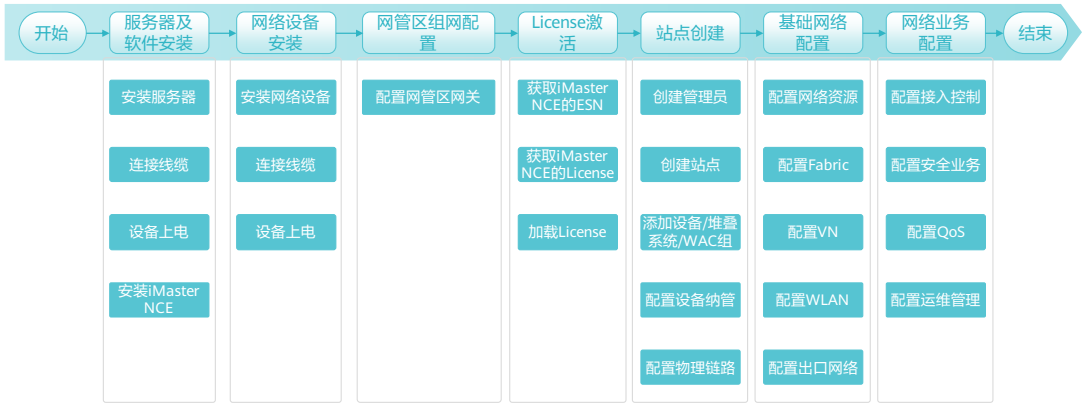
- 在智简园区网络虚拟化方案设计中，首先需要确定采用哪种网关方案。网关方案确定后，就可以基于已选择的网关方案，对园区整体网络进行端到端的设计。

对比项	集中式网关	分布式网关
用户网关位置	Border	Edge
运维部署	用户网关集中部署在Border节点，且Border节点通常启用随板WAC功能，配置无线业务，运维部署相对简单。	用户网关分散部署在Edge节点，且Edge节点通常启用随板WAC功能，所有Edge节点都要配置无线业务，运维部署相对较复杂。
终端规模	≤50000（根据集中式网关设备的数量和规格计算）。终端规模不超过50000时优先推荐。	≤100000（根据分布式网关设备的数量和规格计算）。终端规模超过50000时优先推荐。

部署规划：两种网关方案推荐的组网规划

网关方案	Border位置	Edge位置	WAC类型及位置	无线数据转发模式	适用场景
集中式	核心	接入	随板WAC，位于核心设备	隧道转发	新建网络，终端规模≤50000。
集中式	核心	汇聚	随板WAC，位于核心设备	隧道转发	改造网络，终端规模≤50000，可以利旧不支持VXLAN的接入交换机。
集中式	核心	接入	独立WAC，旁挂核心设备	隧道转发	改造网络，终端规模≤50000，可以利旧独立WAC设备。
集中式	核心	汇聚	独立WAC，旁挂核心设备	隧道转发	改造网络，终端规模≤50000，可以利旧独立WAC设备和不支持VXLAN的接入交换机。
分布式	核心	汇聚	随板WAC，位于汇聚设备	隧道转发	新建网络/改造网络，50000<终端规模≤100000，接入交换机不需要支持VXLAN。

大中型园区网络虚拟化方案部署流程图



- 由于大中型园区网络的规模较大、业务较复杂，因此部署过程也相对复杂，本页展示的部署流程指的是一般流程，并非所有的大型园区网络都严格按照该流程进行部署。
- 本课程后续的内容将聚焦部署流程中的关键操作。

目录

服务器及软件安装（1）

安装iMaster NCE-Campus	安装iMaster NCE-CampusInsight
iMaster NCE • iMaster NCE-Campus支持三种部署场景：企业私有云部署场景、华为公有云部署场景和MSP自建云部署场景。 • 大中型园区通常采用企业私有云部署场景，即企业自行安装iMaster NCE-Campus。 • 《iMaster NCE-Campus 产品文档》	iMaster NCE CampusInsight • iMaster NCE-CampusInsight支持独立部署、与iMaster NCE-Campus集成部署两种部署方式。 • 智简园区网络解决方案推荐采用与iMaster NCE-Campus集成部署方式。 • 《iMaster NCE-CampusInsight产品文档》

- iMaster NCE-CampusInsight支持独立部署、与iMaster NCE-Campus集成部署两种部署方式。独立部署场景下，网络设备的功能（如数据上报等）需要在各设备上通过命令行进行配置。与iMaster NCE-Campus集成部署场景下，网络设备的配置可以通过iMaster NCE-Campus自动化下发，同时，iMaster NCE-Campus还可以配合iMaster NCE-CampusInsight实现路径跟踪、故障定界等功能。智简园区网络解决方案推荐采用与iMaster NCE-Campus集成部署方式，为了避免iMaster NCE-CampusInsight与iMaster NCE-Campus之间网络不稳定，建议iMaster NCE-CampusInsight与iMaster NCE-Campus部署在同一位置，如同一数据中心或同一机房。

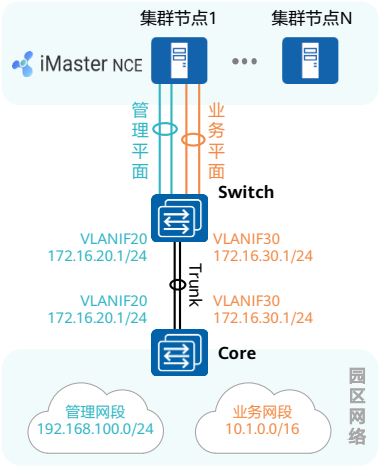
服务器及软件安装（2）

安装CloudCampus APP

华为应用市场下载

- 对于AP设备，在安装时需要将其实际安装的点位上传至iMaster NCE-Campus，以便后续高效的运维，以及提供基于终端位置的增值服务。可通过CloudCampus APP完成AP设备信息录入和上传。
- 除了支持开局功能外，CloudCampus APP还支持Wi-Fi体验测试、测速、视频测试等功能。
- CloudCampus APP的获取方式：
  - 安卓系统的用户请在华为应用市场搜索关键字“CloudCampus”，选择“CloudCampus APP”下载安装。
  - 扫描二维码下载。

网络管理区网关部署



- 在服务器安装了iMaster NCE-Campus等软件后，还需要对网络管理区网关进行配置，一方面需要保证各软件服务器集群的每个网络平面内能够互通，另一方面也需要确保各软件部件能够与园区网络互通。
- 在典型的场景中，iMaster NCE-Campus采用双网络平面，并且需要与Underlay的管理网段和Overlay的业务网段互通。

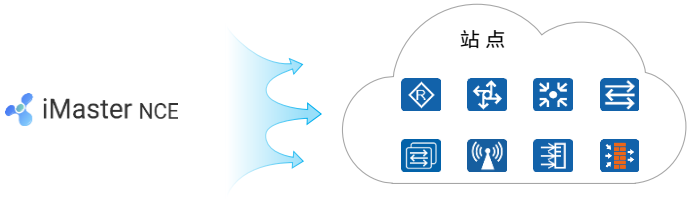
HUAWEI

- 大中型园区网络虚拟化方案中，在服务器安装了iMaster NCE-Campus等软件后，还需要对网络管理区网关进行配置，一方面需要保证各软件服务器集群的每个网络平面内能够互通，另一方面也需要确保各软件部件能够与园区网络互通。
- 本页主要介绍简单网络管理区组网的网关如何配置，如果部署iMaster NCE-Campus等软件的网络管理区是一个数据中心网络，具体服务器侧组网及网关配置可参考数据中心网络解决方案。
- 在本例中，VLAN20及VLAN30是Switch与Core交换机之间的互联VLAN。由于管理平面及业务平面的流量分离处理，因此采用两个单独的互联VLAN。

目录

创建站点

- 创建站点是把同一管理范围内的网络设备添加到iMaster NCE-Campus中纳管，这些设备汇总成一个管理集合，方便在iMaster NCE-Campus上进行统一管理。大中型园区网络中管理的设备类型通常选择交换机和WAC。
- 创建站点时，可以同步完成“添加设备”的任务，也可以在站点创建完成后再单独实施“添加设备”的任务。

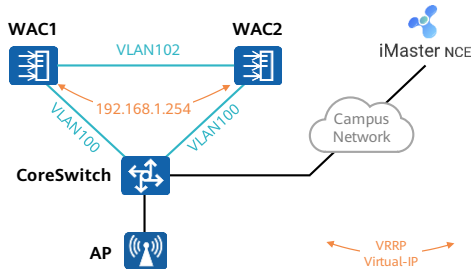


- 大中型园区网络中，WLAN一般采用WAC+Fit AP架构，Fit AP由WAC进行统一配置管理。WAC被iMaster NCE-Campus纳管后，可以直接在iMaster NCE-Campus上跳转到WAC的Web网管界面对Fit AP进行管理。

- 为了便于用户管理设备和提升业务部署效率，同一个租户下，同一个网络的设备可以规划到一个站点中。
- 在iMaster NCE-Campus中创建站点，以便进行统一运维管理。创建站点当前支持如下两种方式：
  - 单个创建：对于添加少量站点的场景，可以单个创建。
  - 批量创建：对于添加大量站点的场景，可以批量创建。云站点暂不支持批量创建。

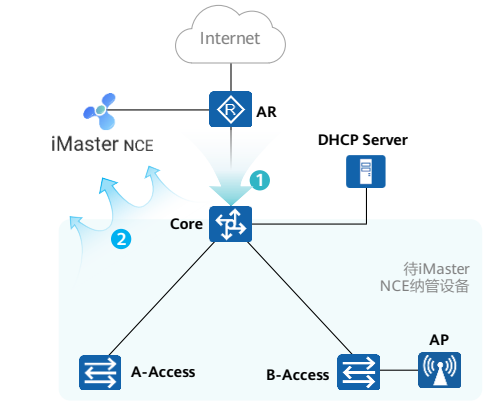
添加WAC组

- 如果WAC选用的是独立WAC设备，并配置双机热备，如果需要被iMaster NCE-Campus纳管，首先成员设备需要添加到站点中；同时，还需要通过命令行的方式提前配置好双机热备功能。配置完成后，再通过iMaster NCE-Campus向站点添加WAC组。



站点设计 | 设备管理 | 网络规划 | Fabric管理 | VN管理 | 业务部署

案例：站点创建与设备即插即用



1 DHCP Offer 2 设备自动向iMaster NCE发起注册

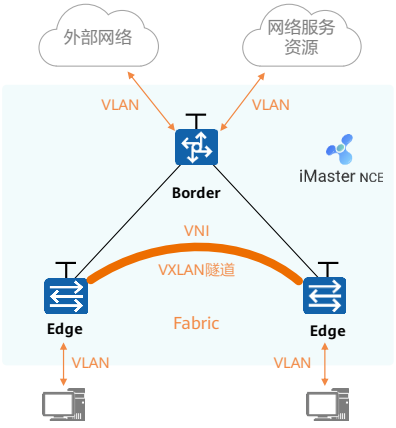
- 站点创建：
  - 在iMaster NCE上，通过批量导入功能，将设备及站点信息导入控制器，完成站点创建，以及站点设备添加。
- 设备即插即用（现场操作）
  - 用户将网络中的交换机和AP进行连线、上电。
  - 交换机通过AR完成IP地址获取、iMaster NCE地址/端口获取，然后向iMaster NCE发起注册，并被纳管。
- 设备管理（iMaster NCE）
  - 可查看设备注册状态。
  - 可查看网络物理拓扑。

HUAWEI

- 用户痛点：传统的网络开局方式需要工程师在现场对网络设备进行逐台调试，配置工作量大，效率低下。
- 本用例将展示CloudCampus解决方案的网络设备即插即用特性（采用DHCP Option方案实现交换机的即插即用，在本例中，需要提前在AR路由器上完成DHCP服务及相关参数的配置）。
- 通过本步骤，园区中的交换机可以直接以出厂状态完成开局配置，并被iMaster NCE纳管，大大降低了用户的配置工作量。

配置网络资源：配置Fabric全局资源池

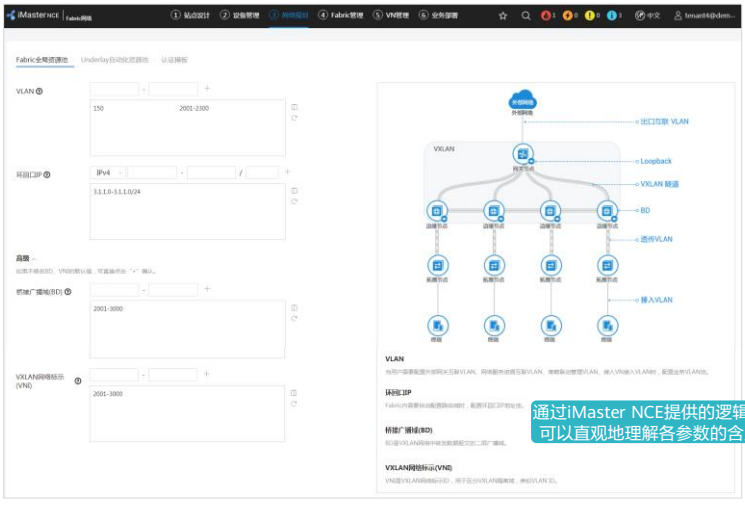
- 创建Fabric前，要提前规划Fabric全局资源池，包含BD/VNI、VLAN和Loopback接口IP地址资源。



任务描述	详细操作步骤
配置Fabric全局资源池	1. 配置VLAN资源，包括创建VN时使用的业务VLAN，以及Fabric创建外部网络和网络服务资源时使用的互联VLAN。 2. 配置Loopback地址资源，VXLAN控制面采用BGP EVPN，不同Border/Edge间建立BGP对等体时使用。 3. 配置BD/VNI资源，VN中二层广播域隔离使用。

站点设计 > 设备管理 > 网络规划 > Fabric管理 > VN管理 > 业务部署

案例：配置Fabric全局资源池

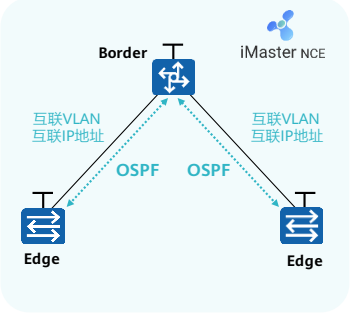


HUAWEI

- Fabric全局资源参数说明：
  - VLAN：当用户终端需要配置外部网关互联VLAN、网络服务资源互联VLAN、策略联动管理VLAN、接入VN接入VLAN时，配置业务VLAN池。
  - 环回口IP：使能Underlay自动化时，配置环回口IP资源池。环回口IP地址作为VXLAN隧道的VTEP IP。
  - 桥接广播域：在VXLAN网络中，将虚拟广播域VN对应的VNI以1:1方式映射到桥接广播域BD，BD成为VXLAN网络的实体，通过BD转发流量。
  - VXLAN网络标识：VXLAN网络标识VNI类似VLAN ID，用于区分VXLAN段。

配置网络资源：配置Underlay自动化资源池

- Underlay自动化资源池是Underlay网络进行OSPF路由编排时使用到的地址池。



任务描述	详细操作步骤
配置Underlay自动化资源池	1. 配置互联VLAN资源。 2. 配置互联IP资源。

- 配置Fabric时，可以同时打开网络域编排开关实现Underlay网络的自动部署，实现建立Fabric BGP-EVPN 所需的VLANIF接口、Loopback接口、VTEP IP、路由等配置的自动发放，完成Underlay网络的自动配置。iMaster NCE-Campus会从该资源池内自动分配相关资源给设备。

站点设计 设备管理 网络规划 Fabric管理 VN管理 业务部署

案例：配置Underlay自动化资源池

HUAWEI

- Underlay自动化资源参数说明：
  - 互联VLAN：Fabric内参与Underlay自动路由编排的设备互联时，配置互联VLAN资源池
  - 互联IP：Fabric内参与Underlay自动路由编排的设备互联时，配置互联IP资源池

配置用户接入认证模板

- 在大中型园区虚拟化方案中，Fabric的接入管理会对认证控制点配置，配置时绑定的认证模板资源需要提前规划设计。
- 在iMaster NCE-Campus上配置的认证模板资源一般包括RADIUS服务器模板、Portal服务器模板和用户认证模板。

任务描述	详细操作步骤
创建RADIUS服务器模板	1. 选择RADIUS服务器类型。推荐采用iMaster NCE-Campus内置的RADIUS服务器。 2. 配置RADIUS服务器地址。如果采用iMaster NCE-Campus内置的RADIUS服务器，则不需要配置。
创建Portal服务器模板	1. 选择Portal服务器类型。推荐采用iMaster NCE-Campus内置的Portal服务器。 2. 配置Portal服务器地址。如果采用iMaster NCE-Campus内置的Portal服务器，则不需要配置。 3. 配置Portal服务器URL。如果采用iMaster NCE-Campus内置的Portal服务器，则不需要配置。
创建用户认证模板	1. 选择用户认证方式，常用的包括802.1X认证、MAC认证和Portal认证。一个模板可以包含多种认证方式。 2. 选择需要绑定的RADIUS服务器模板或者Portal服务器模板。

创建Fabric

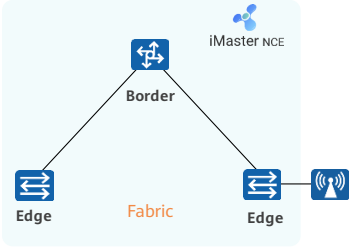
- Fabric是使用VXLAN技术构建在物理网络之上的资源池化网络。
- Fabric首先需要创建，完成基本组网的配置，包括Border和Edge设备的选取、VXLAN控制面BGP EVPN的配置等。另外，Underlay网络路由自动编排功能也是在Fabric创建时开启。

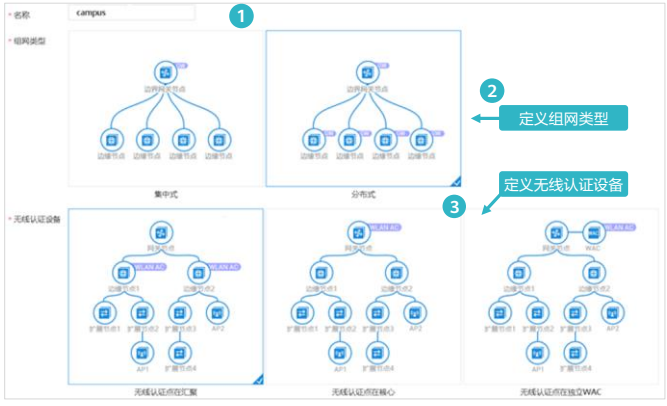
任务描述	详细操作步骤
创建Fabric	1. 选择网关类型，包括集中式和分布式两种。 2. 选择作为Border和Edge节点的设备。如果Fabric采用的VXLAN到汇聚组网，一般还会选取接入交换机作为扩展节点。 3. （可选）配置Fabric网络风暴抑制。为了减小网络风暴风险，建议配置。 4. （可选）开启上报终端识别信息功能。配置终端识别功能时，需要开启。 5. 开启Underlay网络路由自动编排功能。 6. 配置BGP EVPN。建议将作为Border节点的核心交换机配置为路由反射器。

站点设计 > 设备管理 > 网络规划 > Fabric管理 > VN管理 > 业务部署

案例：创建Fabric（1）

- 基于iMaster NCE的图形化界面创建一个新的Fabric：



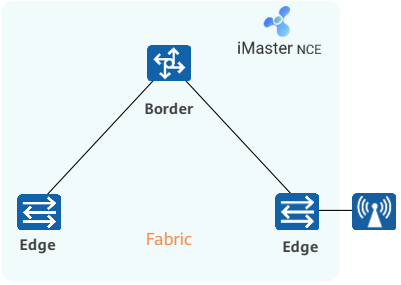


HUAWEI

- Fabric网络由一组核心-汇聚-接入节点设备互联组成，提供无差异接入能力，实现一台接入设备可以同时接入不同的网络业务，节省了成本提供了网络设备的利用效率。
- 园区虚拟网络通过Overlay虚拟化技术（VXLAN），实现多个虚拟网络统一承载在同一个Fabric网络上，并能够支持业务的灵活部署。
- 组网类型：Fabric的组网部署模式：
  - 集中式：Fabric中网关设备是集中的，访问外网和内网的流量都经过集中式的网关。此时，只有边界网关节点可以作网关。
  - 分布式：Fabric中网关设备是分布式的，访问外网和内网的流量经过不同的网关。此时，边界网关节点、边缘节点都可以作网关。

案例：创建Fabric（2）

- 向Fabric中添加设备，并定义设备角色：



- 选择特定的站点，以及相应的设备。
- 指定设备在Fabric里的节点角色。

HUAWEI

- 角色：指定设备在Fabric网络中所属的角色，包含边界网关节点、边缘节点、扩展节点。缺省为扩展节点。

案例：创建Fabric（3）

- 通过iMaster NCE完成Underlay网络自动化部署：

- 自动配置路由域：开启该功能后，自动配置underlay网络。用户可以指定自动配置路由域的站点，并指定OSPF路由参数，当前支持的参数如下：
  - 域：单域为所有设备均属于area 0；多域为边界网关节点属于area 0，其余每个边缘节点与边界网关节点为一个area。
  - 网络类型：指定OSPF的网络类型，可以选择broadcast、p2mp或者p2p。
  - 加密：设置相邻设备之间的加密方式，可以选择hmac-sha256、md5或者无。
  - Key：接口密文验证的验证字标识符，必须与对端的验证字标识符一致。整数形式，取值范围是1～255。
  - 密码：指定密文验证字，字符串格式，不支持空格，长度为1～255。
  - 确认密码：确认密文验证字。
  - OSPF平滑启动：开启OSPF GR功能。
- AS号：指定该Fabric网络中BGP协议的AS号。
- 完成本步骤后，用户成功地基于园区物理网络构建了一个Fabric网络，并且通过iMaster NCE自动地完成了Underlay网络配置（网络设备之间的互联，以及OSPF协议配置等），为后续创建VN构建了底座。

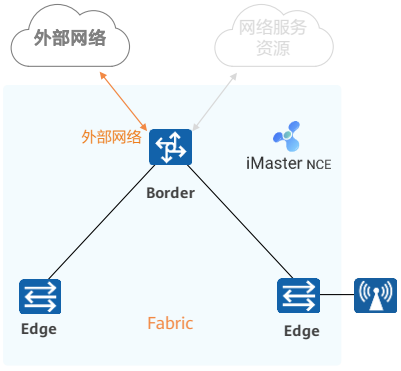
创建Fabric的外部网络

- 在Fabric网络的资源模型设计中，通过在Border节点创建外部网络，使得园区内部终端能够访问外部Internet等。
- 外部网络资源定义了三种类型，如果用户网关位于Fabric内，主要采用L3共享出口或者L3独占出口两种类型。
  - L3共享出口：Fabric网络的多个VN共享L3出口，与出口设备互通。L3共享出口可以节省VLAN和IP等用于互联的资源，适用于不同VN间安全控制策略要求较低的场景。
  - L3独占出口：Fabric网络的每个VN独占一个L3出口，与出口设备互通。此时，防火墙通常会划分多个安全区域与L3独占出口一一对应，到达防火墙的不同VN间业务子网流量是隔离的。如果不同VN间需要在防火墙实现互访，可以在不同安全区域间配置安全策略，配置的安全策略还能够控制互访的应用端口、限制带宽等。

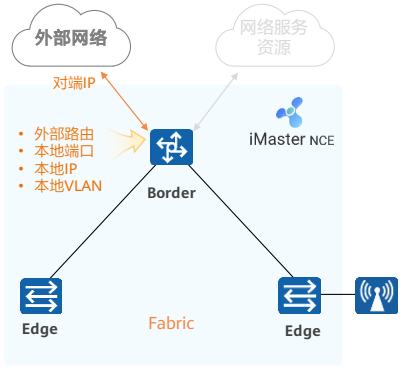
任务描述	详细操作步骤
创建外部网络	1. 选择外部网络资源类型 2. 配置互联的物理接口 3. 配置互联的VLAN和IP地址 4. 配置互联的路由协议

案例：创建Fabric的外部网络（1）

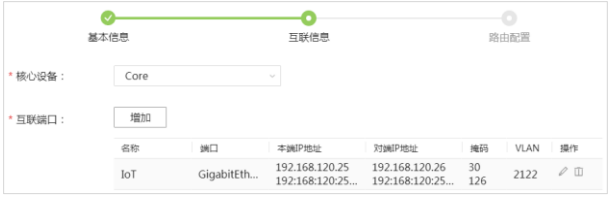
- 创建一个新的Fabric外部网络，定义名称，定义该外部网络是否用于连接Internet（是否采用默认路由作为外部路由），亦可自定义外部路由。



案例：创建Fabric的外部网络（2）



配置该外部网络对应的互联信息：



配置该外部网络对应的路由信息：

HUAWEI

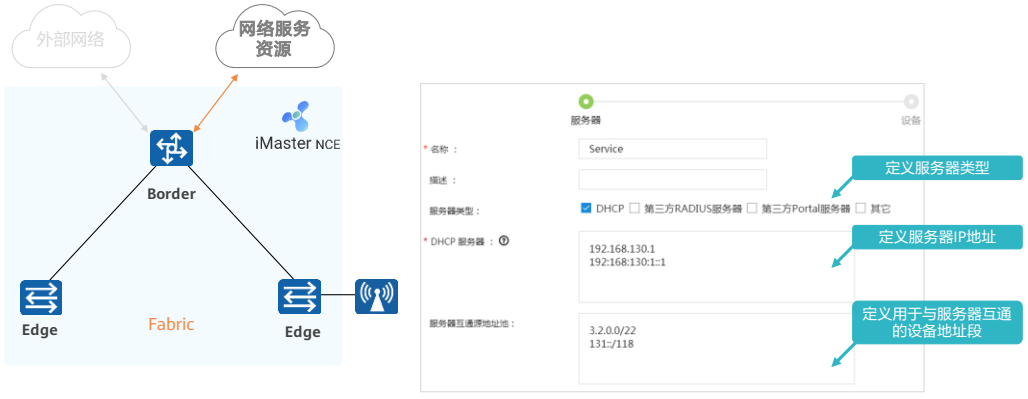
创建Fabric的网络服务资源

- 在Fabric网络的资源模型设计中，通过在Border节点创建网络服务资源，使得园区内部业务终端能够访问网络管理区的服务资源，比如DHCP服务器、准入服务器等。
- 网络服务资源可以创建多个，也可以一个网络服务资源模型包含多个服务资源的访问地址。
- 如果网络管理区需要访问的服务资源较少，建议这些服务资源都规划在一个网络服务资源模型中。这样，可以节省互联的VLAN和IP地址资源，简化网络管理区侧的路由配置。

任务描述	详细操作步骤
创建网络服务资源	1. 配置服务资源的访问地址，如DHCP服务地址、iMaster NCE-Campus的南向地址。 2. 选择互联场景，包括与服务器直连、与交换机直连两种。 3. 配置互联的物理接口。 4. 配置互联的VLAN和IP地址。

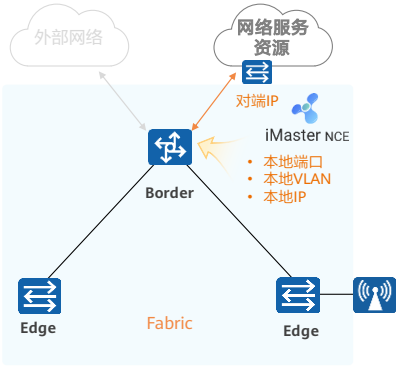
案例：创建Fabric的网络服务资源（1）

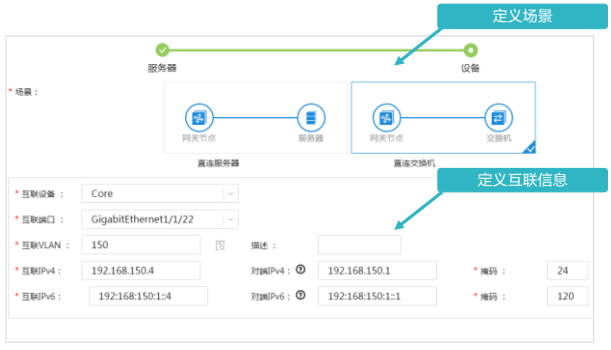
- 创建一个新的Fabric网络服务资源，定义其名称，定义所连接的服务器类型及地址：



案例：创建Fabric的网络服务资源（2）

- 创建一个新的Fabric网络服务资源，定义其名称，定义所连接的服务器类型及地址。





HUAWEI

配置Fabric接入管理

- Fabric的接入管理主要是配置认证控制点，对接入点资源进行规划，供VN创建时选用。
- 其中，有线接入点资源指的是终端接入的交换机端口，无线接入点资源指的是终端接入的SSID。
- Fabric接入管理中，对交换机的接入端口定义了3种连接类型。
  - Fabric扩展AP：华为瘦AP，可以通过iMaster NCE-Campus进行管理。
  - Fabric扩展接入交换机：华为交换机，可以通过iMaster NCE-Campus进行管理。
  - 终端（PC、哑终端、非Fabric扩展交换机/AP）：用户终端、不支持iMaster NCE-Campus管理的交换机和AP、支持iMaster NCE-Campus管理但不支持Fabric扩展的交换机。
- 在不同的网关方案中，Fabric接入管理的配置会有差异。

案例：配置Fabric接入管理

HUAWEI

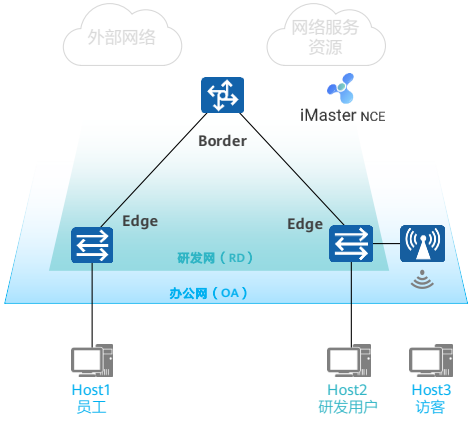
创建VN

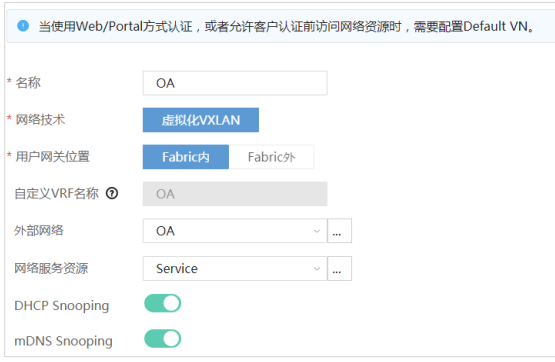
- Fabric创建完成后，就可以选取其中的网络资源，创建VN实例。不同的VN代表不同用户的业务，通过VN实现业务隔离的目的。

任务描述	详细操作步骤
创建VN	1. （可选）选择外部网络。通常会选取，用于VN与外部网络互通。 2. （可选）选择网络服务资源。通常会选取，用于VN与网络服务资源互通。 3. 配置用户网关，有手动指定和自动分配两种方式可选择。 4. 配置有线接入，选取Fabric接入管理配置好的接入端口资源，并将端口加入到用户网关中配置的业务VLAN。 5. 配置无线接入，选择接入无线用户子网的WAC设备，然后用户网关中配置的业务VLAN会下发到该设备。该步骤需要WAC设备为Fabric接入管理配置的认证控制点，适用于分布式网关方案有线无线统一认证控制点的场景。

案例：创建VN（1）

- 创建一个新的VN，定义VN的名称、用户网关位置，并可配置VN所使用的外部网络及网络服务资源：



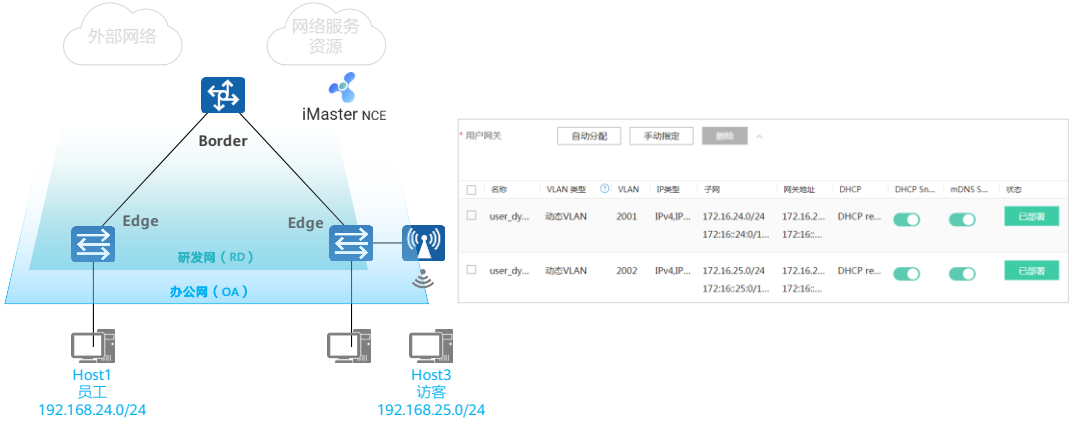


HUAWEI

站点设计 > 设备管理 > 网络规划 > Fabric管理 > VN管理 > 业务部署

案例：创建VN（2）

- 定义VN的用户网段。

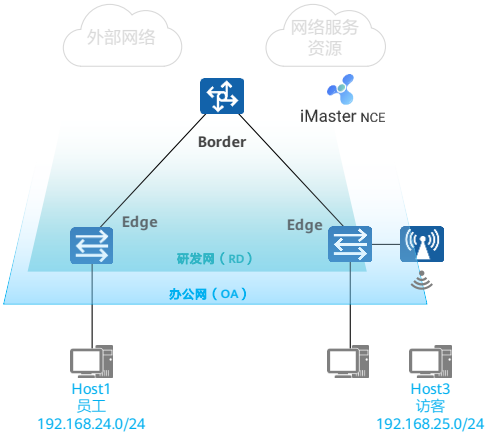


HUAWEI

- 本步骤为VN创建用户网段，网络管理员可以通过手动绑定的方式逐个创建网段，也可以通过自动分配方式批量创建网段。

站点设计 > 设备管理 > 网络规划 > Fabric管理 > VN管理 > 业务部署

案例：创建VN（3）



定义VN的有线接入端口：

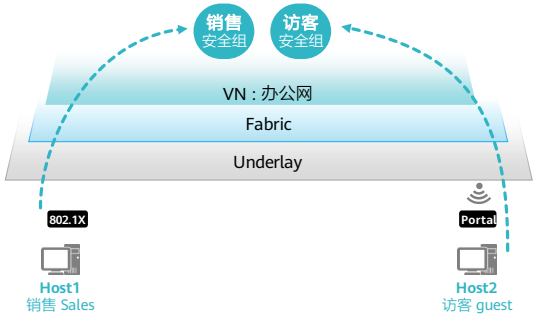
定义VN的无线接入：

HUAWEI

- 本步骤定义VN的有线接入端口及无线接入点。

业务随行：创建安全组

- 安全组是权限控制的实体单元，将不同的用户或网络服务类资源分配在不同安全组，通过配置之间的访问权限来实现网络内用户权限的管理。安全组分为静态安全组和动态安全组，动态安全组为给用户授权的安全组，静态安全组为网络服务类资源分配的安全组。



- 安全组是指网络中通信对象的集合。安全组既可以根据5W1H条件授权给用户，符合5W1H条件的用户授权到指定安全组，也可以通过静态绑定IP地址的方式定义安全组。安全组授权通过华为私有的radius属性(26-160)下发。
- 动态授权加入的成员优先级高于静态绑定的成员，例如：静态的将IP1的用户绑定到安全组1，同时通过radius授权该用户到安全组2，最终设备将会将该用户归入安全组2。
- 缺省支持unknown组和any组，unknown表示未知用户，未认证的用户或者资源指定为unknown组，any组表示任意用户或资源，通常用来配置默认规则。any组只能做目的组，不支持配置为源组。

- 安全组和资源组定义完成之后，租户管理员就可以基于组来定义全网的权限策略。策略矩阵用于承载组间策略的配置。策略矩阵定义完毕后，可以基于策略矩阵配置源安全组到目的安全组或者资源组的策略。
- 组间权限策略主要控制组到组之间的访问权限。当一个源安全组存在到多个目的组的策略时，需要通过优先级区分对不同策略的匹配顺序，比如目的组为资源组的时候，由于目的地址可能存在重复，所以需要通过手动调整策略的优先级实现对某策略的优先匹配。

配置用户接入与认证：802.1X认证

- 802.1X协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级验证用户身份并控制其访问权限。
- iMaster NCE-Campus作为RADIUS服务器时，802.1X认证的服务器侧配置如下。

任务描述	详细操作步骤
配置802.1X认证	1. 添加用户账号 2. 配置认证规则 3. 配置授权结果和授权规则

案例：添加账号

- 对于企业员工接入场景，可以使用用户名密码认证方式实现终端用户接入。
- 在Portal认证和802.1x认证过程中，终端用户需要填写如下帐号作为认证信息。
- 账号：包括用户名和密码。由租户管理员在iMaster NCE-Campus上预先发放。

案例：配置认证规则

配置认证规则可以对接入网络的客户端和用户进行认证，保证网络的安全。

HUAWEI

- 配置认证规则可以对接入网络的客户端和用户进行认证，保证网络的安全。
- iMaster NCE-Campus存在缺省认证规则default，使用本地数据源进行认证，缺省模板支持修改，可以修改为使用第三方数据源进行认证。

- 配置Portal认证、802.1X认证和MAC认证时，用于配置终端用户认证通过后所获得的权限集、流量限速策略、过滤策略等。适用于认证点在FW、AR、AP、LSW、WAC的场景，可以针对特定的用户群完成配置。
- iMaster NCE-Campus存在缺省授权结果允许接入和拒绝接入，缺省模板绑定所有站点，不可修改和删除。

- 对于通过认证的用户进行授权时，需要根据授权规则匹配用户，为符合规则的用户提供特定的权限集合。
- iMaster NCE-Campus存在缺省授权规则default，授权结果为拒绝接入，缺省模板支持修改，可以修改为其他授权结果。
- 终端用户认证通过后具备哪些权限由授权结果指定，认证通过后满足配置的授权规则，表示匹配授权策略，授权结果对匹配该授权规则的终端用户生效。如果所有授权规则均不设置，表示适用于所有认证通过后的终端用户。

配置用户接入与认证：Portal认证

- Portal认证通常也称为Web认证，一般将Portal认证网站称为门户网站。用户上网时，必须在门户网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源。
- iMaster NCE-Campus作为Portal服务器和RADIUS服务器时，Portal认证的服务器侧配置如下：

任务描述	详细操作步骤
配置Portal认证	1.添加用户账号。 2.配置认证规则。 3.配置授权结果和授权规则。
（可选）配置MAC免认证策略	如需用户终端在首次Portal认证通过后的一段时间内，可以基于MAC免认证，需要在用户控制策略中配置此功能。

- Portal认证通常包含四个基本要素：用户终端、认证控制点、Portal服务器和认证服务器。
  - 用户终端：安装有运行HTTP/HTTPS协议的浏览器的主机。
  - 认证控制点：通常为支持Portal认证的网络设备。
  - Portal服务器：为用户终端提供免费门户服务和认证界面，与接入设备交互用户终端的认证信息。
  - 认证服务器：用于实现对用户进行认证、授权和计费，通常为RADIUS服务器。

WLAN配置（以分布式网关为例）

- 配置无线用户子网
  - 目前，在部署分布式网关方案中，如果Fabric采用VXLAN到汇聚，Edge设备作为随板WAC，有线无线业务子网统一在Edge接入VN，创建VN时，可配置无线业务子网的网关等。
- 配置AP在WAC上线
  - 目前，在部署分布式网关方案中，如果Fabric采用VXLAN到汇聚，Edge设备作为随板WAC，AP通过策略联动管理VLAN与Edge建立CAPWAP隧道，然后在Edge上线。配置接入管理时，会进行策略联动功能的配置。
- 配置无线业务
  - 目前，在部署分布式网关方案中，如果Fabric采用VXLAN到汇聚，Edge设备作为随板WAC，有线无线认证控制点统一在Edge，配置用户接入认证模板时规划的模板资源，可以在配置接入管理的无线接入时向Edge下发。

思考题

1. iMaster NCE-Campus支持哪些站点创建方式?
2. Fabric全局资源池中，用户可以录入以下哪些参数?（ ）
   A. VLAN
   B. 环回口IP
   C. 桥接广播域
   D. VXLAN网络标识

1. 单个创建：对于添加少量站点的场景，可以单个创建。批量创建：对于添加大量站点的场景，可以批量创建。

2. ABCD

本章总结

- 本课程系统介绍了CloudCampus大型园区网络方案部署（VXLAN虚拟化园区网络）部署流程，同时，通过穿插案例帮助学员完成解决方案功能特性理解，掌握部署技能。
- 通过本课程的学习，搭配基于实际环境的练习，学员将能独立完成CloudCampus大型园区网络方案部署（VXLAN虚拟化园区网络）方案部署，并具备网络运维及管理能力。

学习推荐

- 智简园区网络解决方案 V100R019C10 产品文档
  - https://support.huawei.com/hedex/hdx.do?docid=EDOC1100141274&lang=zh&id=library_change_preview&from=HedExLite

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

CloudCampus中小型园区网络方案部署

HUAWEI

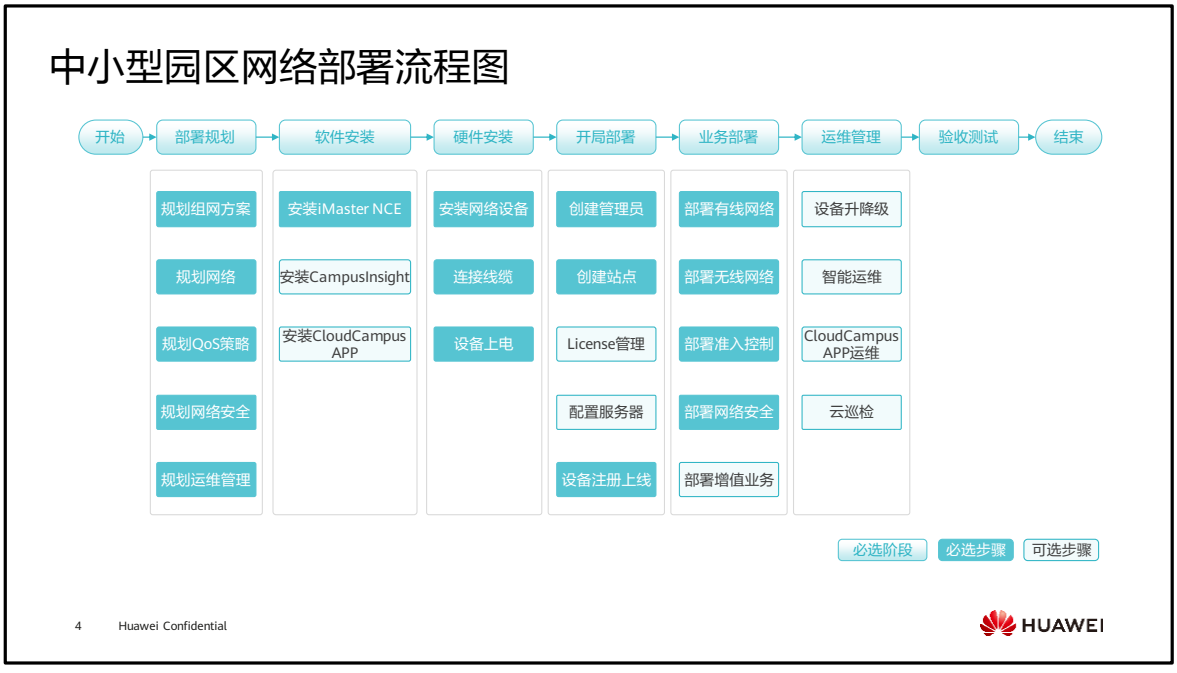
前言

- 随着技术和行业数字化的发展，尤其是连锁门店、分支办公等中小场景业务正逐步通过云化管理的网络接入到企业内部来。根据IDC报告，2014~2018年，传统Wi-Fi年度增长率仅为5%，而云化Wi-Fi为38%；传统交换机与接入路由器年度增长率仅为2%，而云化交换机与接入路由器达到61%。
- 从以上数据可见，云化管理的网络已经成为中小型园区网络建设的趋势，通过采用云化方案，企业可以获得管理效率的提升，网络能够更加快速的支撑新的业务开拓。
- 本课程将介绍CloudCampus中小型园区网络方案部署流程及典型部署案例。

目标

- 学习完本课程后，您将能够：
  - 描述CloudCampus中小型园区网络方案部署流程
  - 部署典型CloudCampus中小型园区网络方案
  - 配置iMaster NCE，完成CloudCampus中小型园区网络管理及维护

目录



- 在“部署规划”中，“规划网络”项目包括管理员角色、站点、物理网络、开局方式、基础业务、WLAN业务、网络准入控制等规划项。

目录

部署规划概述

HUAWEI

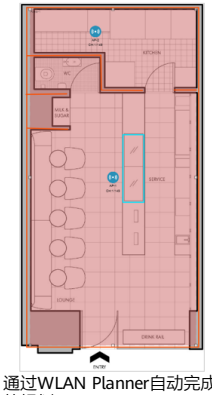
- 中小型园区网络设计与规划包含多项内容，例如LAN侧组网方案设计、网络设计、QoS设计、安全设计、运维管理设计等。
- 本文档仅介绍WLAN网络规划。其余内容在HCIE WLAN认证课程《CloudCampus中小型园区网络方案》已经系统介绍，此处不再赘述。

部署规划：WLAN网规

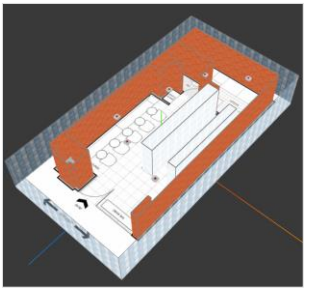
1 访问华为云化WLAN网规工具（WLAN Planner）

1.环境 2.区域 3.部署 4.仿真 5.报表

2 在华为WLAN云网规工具中，用户可以通过简单的5步来完成WLAN网络规划



3 通过WLAN Planner自动完成AP布放规划

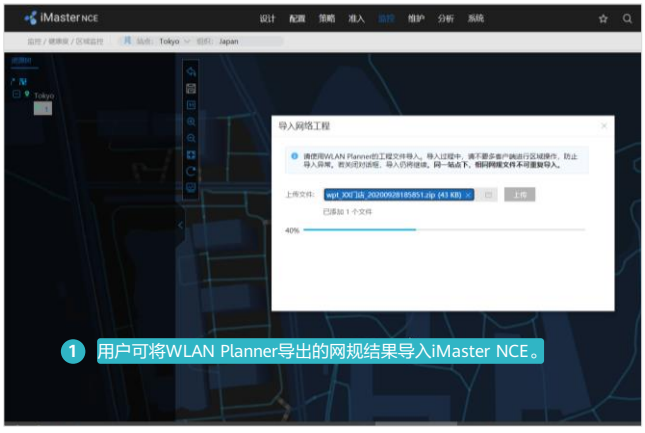


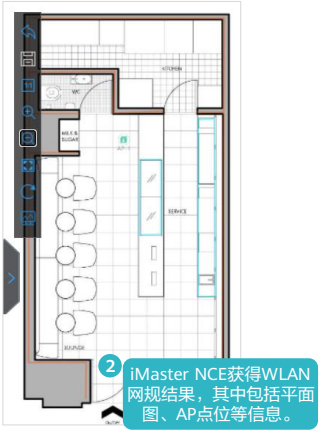
4 查看3D网规结果，模拟终端移动，查看漫游数据。导出网规结果。

HUAWEI

- 华为提供了云网规工具WLAN Planner，用户可基于该工具轻松完成WLAN网规工作，获得AP的布放规划，更可将网规结果导入iMaster NCE。
- WLAN Planner：https://serviceturbo-cloud-cn.huawei.com/serviceturbocloud/dist/#/toolsummary?entityId=d59de9ac-e4ef-409e-bbdc-eff3d0346b42

将WLAN Planner网规结果导入iMaster NCE





HUAWEI

目录

软件安装：iMaster NCE

- iMaster NCE支持华为公有云部署、MSP自建云部署和本地部署三种部署场景：

安装场景	场景描述	iMaster NCE所有者	iMaster NCE运营者
华为公有云部署场景	华为公司将iMaster NCE安装在华为公有云上，华为公司拓展MSP（Managed Service Provider，管理服务提供商），由MSP销售云管理服务，最终客户（租户）购买并使用云管理服务。	华为	华为公司的系统管理员（admin）
MSP自建云部署场景	MSP向华为购买iMaster NCE（软件和License文件）并自行安装，MSP拓展其下级渠道商，即下级MSP，由其下级MSP销售云管理服务，最终客户（租户）购买并使用云管理服务。	MSP	MSP作为系统管理员（admin）
本地部署场景	企业向华为购买iMaster NCE（软件和License文件）并自行安装，企业内部员工（租户）使用云管理服务。	企业	企业作为系统管理员（admin）

- iMaster NCE 产品文档：
  - https://support.huawei.com/enterprise/zh/network-management-and-analysis-software/imaster-nce-campus-pid-250852420/doc

软件安装：CampusInsight及CloudCampus APP

安装CampusInsight	CloudCampus APP的获取方式
iMaster NCE CampusInsight **根据iMaster NCE-CampusInsight安装指导完成软件安装。**	• 安卓系统的用户请在华为应用市场搜索关键字“CloudCampus”，选择“CloudCampus APP”进行下载安装。 • 扫描二维码下载。 华为应用市场下载

HUAWEI

- iMaster NCE-CampusInsight安装指导：
  - https://support.huawei.com/hedex/hdx.do?docid=EDOC1100154774&lang=zh&idPath=24030814%7C250382819%7C250382820%7C250987490%7C250872285

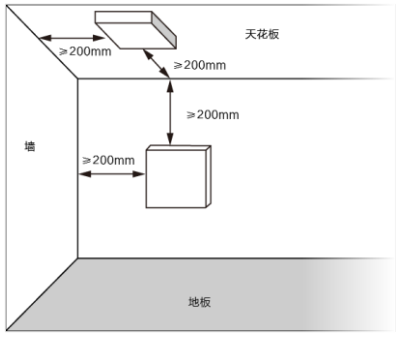
硬件安装

- 根据部署规划时的网络设备安装点位设计、设备间互联等信息，完成网络设备的硬件安装、连线、上电等操作。

室内AP一般是通过钣金安装件直接贴在墙壁或者天花板安装，设备的具体安装位置由工勘确定，设备出线端距离墙壁至少预留200mm空间。

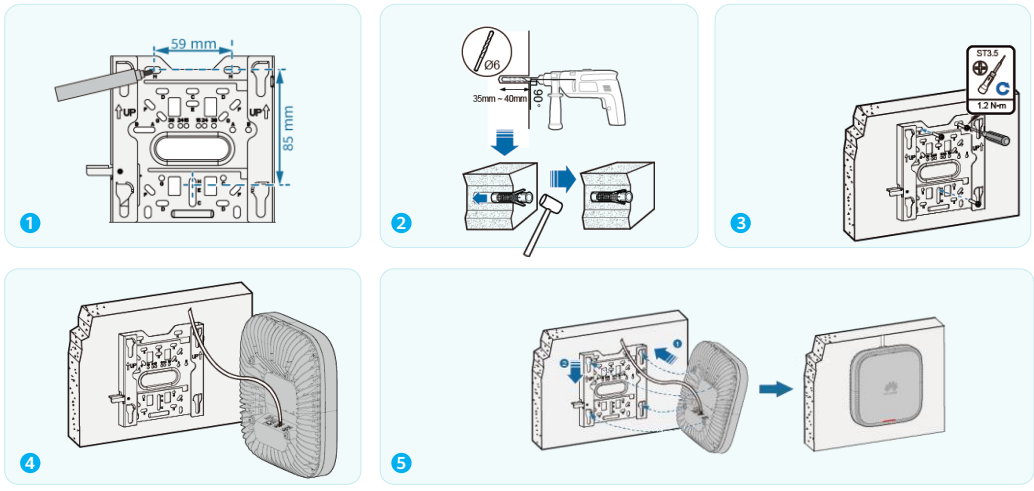
确定安装位置时的原则如下：

- 尽量减少AP和用户终端间的障碍物（如：墙壁）数量。
- 使AP远离可能产生射频干扰的电子设备。
- 严禁在积水、渗水、滴漏、结露等环境下安装。
- 严禁将设备安装在高温、阳光直射、多尘、有害气体、易燃、易爆、易受电磁干扰及电压不稳、震动大或强噪声的环境中。



- 此处以AP设备的安装为例，其他设备的硬件安装方式请参考产品文档。
- 室内安装场景天线防干扰布放距离通用要求：
  - 天线间距7m以上
  - 距离运营商4G天线5m以上
  - 远离可能产生天线干扰的其他电子设备（如微波炉等）
- 对于内置天线的设备，对天线的布放距离要求即为对设备的布放距离要求。

硬件安装（AP的挂墙安装方式）



HUAWEI

- 挂墙安装方式对墙体要求如下：
  - 墙体需能承受设备和钣金安装件总重量的4倍而不被破坏。当设备和钣金安装件总重量小于1.25kg时，墙体承重需不低于5kg。
  - 当螺钉的紧固力矩达到3.5N*m时，螺钉不会出现打转失效，并且墙面不会出现裂纹或损坏。
- 挂墙安装方式需要使用安装件和配套的膨胀螺栓，具体安装步骤如下。
  - 将钣金安装件紧贴墙面，调整好安装位置，用记号笔标出定位点。
  - 用6mm的电钻头在定位点打孔，钻孔的深度为35mm～40mm，然后安装膨胀螺管，使膨胀螺管与墙面齐平。
  - 将钣金安装件贴紧墙面，用十字螺丝刀依次将3个膨胀螺钉分别拧进膨胀螺管中，使钣金安装件与墙面紧固。
  - 连接并理顺线缆。
  - 按照图示扣紧设备，当听到“咔哒”声后，说明AP已固定至锁止位。
- 设备安装好后，确保按压扳手已回弹到位。安装放置的空间尽量根据前文所述的安装空间要求，以便后期的维护操作。
- 当AP安装在迪厅、酒吧等震动较剧烈的场景时，须用M3×12螺钉拧紧至钣金安装件上，防止AP因震动而脱落，螺钉紧固力矩为0.5N·m。正常场景此螺钉可不用安装。

目录

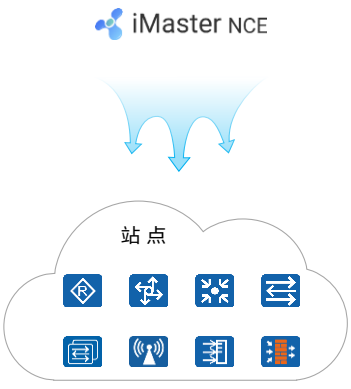
开局部署：创建管理员

- 园区网络实施前需要先创建好相应的管理员角色，由该管理员去实施部署园区网络的工作。
- MSP（Managed Service Provider，管理服务提供商）和租户角色在创建后，即缺省拥有唯一一个该级别的超级管理员帐号，使用该超级管理员帐号，可以创建多个同级别的管理员帐号。

租户自建自维	MSP代建代维
1. 租户管理员自己现场安装云化设备，注册云化设备上线。 2. 租户管理员使用自己的帐号登录iMaster NCE，进行业务部署。	1. MSP管理员帮助租户在现场安装云化设备，注册云化设备上线。 2. 租户管理员使用自己的帐号登录iMaster NCE，打开“授权给MSP”开关并设置授权范围；或者MSP管理员在创建租户管理员时，打开“授权给MSP”开关，默认授权“Tenant Administrator”角色的权限。 3. MSP管理员使用自己的帐号登录iMaster NCE，在首页的“租户列表”中选择申请代建代维且已授权的租户。 4. 单击租户名称进入代建代维界面，MSP管理员帮助租户进行业务部署。

- 如果租户管理员具备一定的IT能力，可以自行部署和运维园区网络，这种场景我们称为“租户自建自维”，租户管理员是主要实施者，MSP管理员只做一些简单的开局协助工作。反之，租户管理员可以向MSP申请代建代维服务，经过授权后由MSP进行代建代维租户的园区网络，这种场景我们称为“MSP代建代维”，MSP管理员是主要实施者。
- 本课程中各组网场景下的部署思路和流程都是以租户自建自维为例来描述的，租户管理员是主要实施者；如果是MSP代建代维场景，MSP管理员是主要实施者，换个角色完成相同的任务。

开局部署：创建站点（1）



- 创建站点就是把同一管理范围内的网络设备添加到iMaster NCE中纳管，这些设备汇总成一个管理集合，方便在iMaster NCE上进行统一管理。
- 创建站点的工作包含两部分：
  - 创建站点
  - 添加设备

HUAWEI

- 站点通常对应一个总部或者分支，是网络和使用网络用户的统称，也是管理中小型园区网络的基本单元。为了便于租户管理设备和提升业务部署效率，同一个租户下，同一个网络中的设备可以规划到一个站点中。

开局部署：创建站点（2）

单个创建

批量创建

1 从iMaster NCE下载模板文档（Excel）

2 在模板文档中填充站点及设备信息

站点名称	园区设备类型	设备款型	设备ESN	设备名称
Sitename	LSW,AP	S5730-36C-PWH-HI	***	
		S5730-36C-PWH-HI	***	
		S5731-H24P4XC	***	
...	...	...	...	...

3 将文档导入iMaster NCE

批量完成站点创建、设备导入

HUAWEI

- 为了便于用户管理设备和提升业务部署效率，同一个租户下，同一个网络的设备可以规划到一个站点中。
- 在iMaster NCE中创建站点，以便进行统一运维管理。创建站点当前支持如下两种方式：
  - 单个创建：对于添加少量站点的场景，可以单个创建。
  - 批量创建：对于添加大量站点的场景，可以批量创建。云站点暂不支持批量创建。
- 在iMaster NCE中可以从已有的站点克隆新的站点，以减少重复配置。

注册上线：出口网关的推荐开局方式

场景	出口网关的推荐开局方式		
	AR	防火墙	AP
华为公有云部署或者MSP自建云部署场景，出口网关设备只能通过静态配置方式或PPPoE方式获取IP地址。	Web网管开局	Web网管开局	CloudCampus APP方式开局
本地部署场景，出口网关设备无法通过DHCP方式获取外网接口IP地址。	Web网管开局	Web网管开局	CloudCampus APP方式开局
华为公有云部署场景，出口网关设备可直接通过DHCP获取外网接口IP地址。	注册查询中心开局	注册查询中心开局	注册查询中心开局
本地部署场景，出口网关设备可直接通过DHCP获取外网接口IP地址，且DHCP服务器可配置Option148参数。	DHCP Option148开局 或 Web网管开局	Web网管开局	DHCP Option148开局

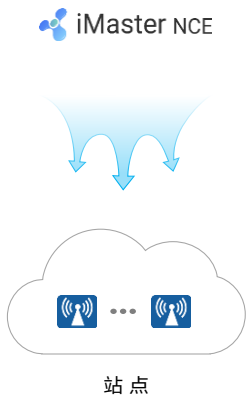
注册上线：LAN侧设备开局方式

- LAN侧网络主要指LSW和AP，这些设备都部署在内网中。
- 公有云部署时，推荐部署使用注册查询方式开局。
- 对于不想将设备信息同步给注册查询中心的企业，也可以采用DHCP Option开局方式。

组网场景		LAN侧设备开局方式	
		LSW	AP
华为公有云部署	网络中不能配置DHCP option	注册查询中心	
	网络中可以配置DHCP option	注册查询中心/DHCP option	
MSP自建云部署	网络中不能配置DHCP option	WEB网管	CloudCampus APP开局
	网络中可以配置DHCP option	注册查询中心/DHCP option	

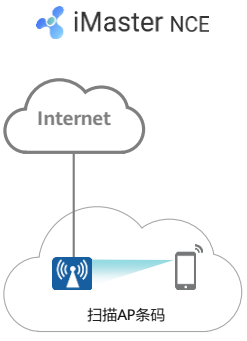
AP开局

- 对于AP设备，在安装时需要将其实际安装的点位上传至iMaster NCE，以便后续高效的运维，以及提供基于终端位置的增值服务。
- 可通过CloudCampus APP完成AP设备信息录入和上传。
- 安卓版CloudCampus APP配置AP两种部署方式：
  - 单AP开局：建议使用快速开局。用户不需要手动输入连接管理SSID密码、登录设备密码。
  - 多AP开局：建议使用网规开局。网规开局分为扫码部署和管理SSID部署。



- 除了支持开局功能外，CloudCampus APP还支持Wi-Fi体验测试、测速、视频测试等功能。

案例1：单AP快速开局

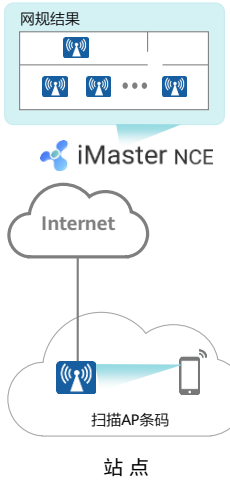


站 点

1. 连接AP上电。
2. 登录CloudCampus APP。
3. 选择“快速开局”，然后选择待安装AP所属的站点。
4. 快速部署AP。
5. 按照界面提示信息做好准备工作，单击“下一步”。
6. **扫码，录入AP的ESN号以及MAC地址。**
7. 完成扫码，单击“下一步”。自动连接AP离线管理SSID并自动登录AP。
8. 进行AP开局配置，完成参数设置后单击“下一步”。
9. AP注册。
10. 创建SSID。根据实际需求创建SSID，如有可用SSID，也可以直接跳过。进入“一键验收”页面。
11. 选择需要验收的SSID，单击“一键验收”。
12. 硬件安装。
13. 验证AP部署是否成功。

HUAWEI

案例2：AP网规开局 - 扫码部署

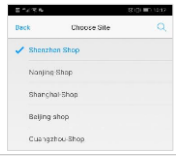


1 将WLAN网规结果导入iMaster NCE（关联对应站点）

2 登录CloudCampus APP

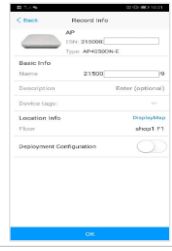
录入iMaster NCE的服务器域名或IP地址、用户名及密码。

3 在APP上选择站点

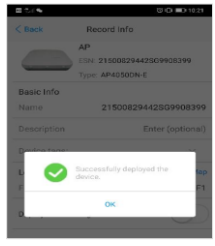


4 选择AP位置&扫描AP的ESN条码

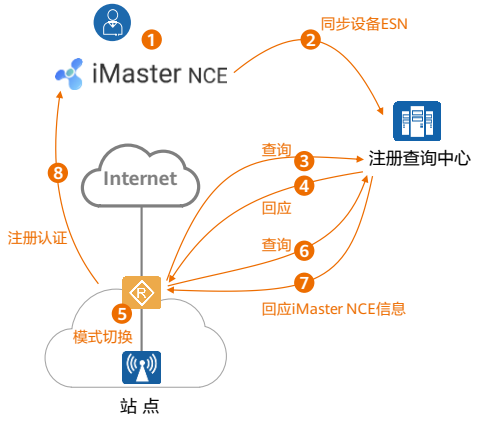
5 确认AP的信息



6 部署成功

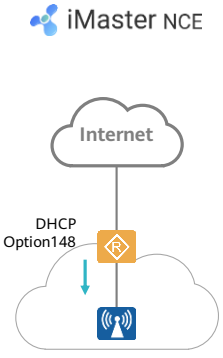


案例3：AR做出口网关场景（AR通过注册查询中心开局）



1. 管理员向iMaster NCE导入新的待纳管设备的信息，包括设备的ESN、设备类型等。
2. iMaster NCE向注册查询中心上传新的待纳管设备的ESN以及对应的iMaster NCE的信息。
3. AR接入Internet后，向注册查询中心发送查询报文，报文携带自身的ESN信息。
4. 注册查询中心回应查询，报文中会携带云管理模式的信息。
5. 设备根据回应报文中的信息，从传统模式切换到云管理模式。
6. 云化设备与注册查询中心之间建立一个HTTP2.0的双向认证连接。设备通过该连接发送查询报文，报文携带自身的ESN信息。
7. 注册查询中心发送回应报文，携带该设备对应的iMaster NCE信息。
8. 云化设备向iMaster NCE注册认证，实现云化设备即插即用。

案例4：AR做出口网关场景（AR配置DHCP option148）



通过配置DHCP服务及Option148，能够实现AR下联的LAN侧设备零配置开局（Option148方式）

HUAWEI

目录

部署有线网络：LAN网络

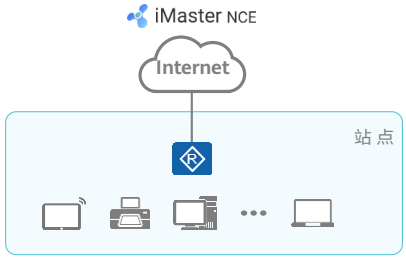
- 中小型园区网络中一般用户数量较少，建议使用出口网关设备或者交换机设备作为DHCP服务器给用户动态分配IP地址，从用户侧至出口网关路径上的接口，均需要将对应的VLAN放通。
  - 出口网关是FW或者AR的场景，建议由出口网关作为DHCP服务器。
  - 对于单AP的组网场景，可直接使用AP作为DHCP服务器给用户分配地址。

任务名称	任务描述
在FW上配置子网	通过iMaster NCE-Campus在防火墙上配置DHCP服务器功能，防火墙下层接入的设备能从防火墙自动获取IP地址，从而实现与防火墙上行网络的互通。
在AR上配置子网	在AR上配置DHCP服务，使下行网络中的设备能自动获取IP地址，从而实现与AR上行网络的互通。
在SW上配置子网	通过iMaster NCE-Campus可以在指定交换机上配置DHCP服务器功能，交换机的DHCP服务器功能与管理VLAN互斥。
在AP上配置子网	如果终端以NAT方式接入AP，则以AP作为默认网关，从AP动态获取IP地址。缺省情况下，以NAT方式接入AP的终端设备自动获取到的IP地址为10.1.1.2～10.1.1.254，所属VLAN ID为3911。用户可以直接使用默认值，也可以按需调整配置。

案例1：配置AR的LAN网络业务（1）

- 在“LAN”页签中设置网络配置模式。
- 如果需要为同一站点里的不同AR设备配置相同的DHCP参数，请选用“本地Internet接入”。
- 如果需要为同一站点里的不同AR设备配置不同的DHCP参数，请选用“多分支互联”。

单击“创建”，设置LAN侧子网参数（下一页）



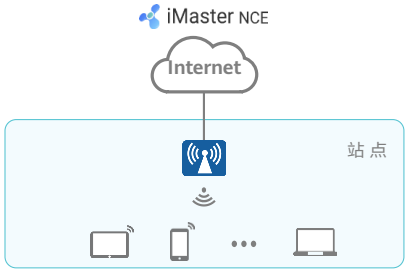
HUAWEI

案例1：配置AR的LAN网络业务（2）

接右图 >>

案例2：配置AP的LAN网络业务

- 如果终端以NAT方式接入AP，则以AP作为默认网关，从AP动态获取IP地址。
- 缺省情况下，以NAT方式接入AP的终端设备自动获取到的IP地址为10.1.1.2～10.1.1.254，所属VLAN ID为3911。用户可以直接使用默认值，也可以按需调整配置。



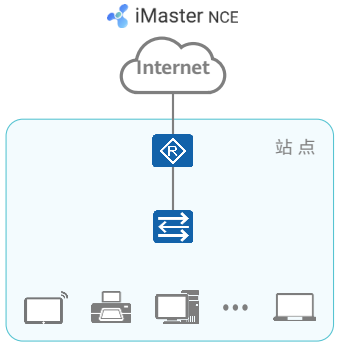
HUAWEI

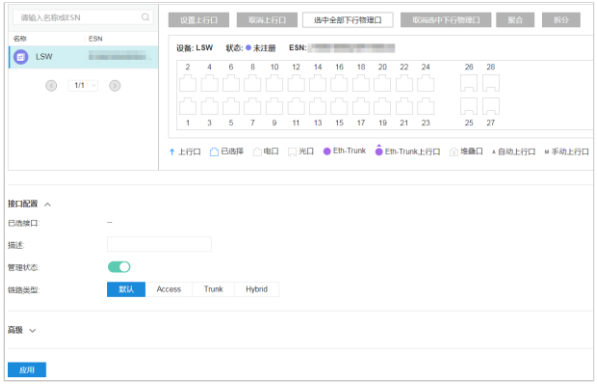
部署有线网络：接口

- 设备接口的初始状态下均是只能通过VLAN1，为了不同类型的用户之间二层隔离且能和网关通信，需要将设备的接口加入对应的业务VLAN。
  - 直连用户的接口建议配置成Access类型，如接口下同时连接了IP Phone和PC，需要将接口配置成Hybrid类型，并将IP Phone业务的VLAN配置成Tagged VLAN，PC业务的VLAN配置成Untagged VLAN，缺省VLAN为PC业务的VLAN。
  - 设备之间互联的接口建议配置成Trunk或者Hybrid类型。
  - 交换机连接AP的接口需要配置成Trunk类型，并且配置缺省VLAN为AP的管理VLAN。

案例1：配置交换机的物理接口

- 在交换机上配置网口，使其接入到有线网络中。配置的接口必须与安装连线时选用的网络接口相匹配。

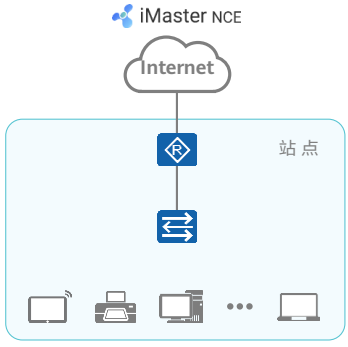




HUAWEI

案例2：配置AP的LAN网络业务

- 在AR上配置NAT，使下行网络中的设备能以AR的WAN口IP地址访问Internet。



部署有线网络：NAT

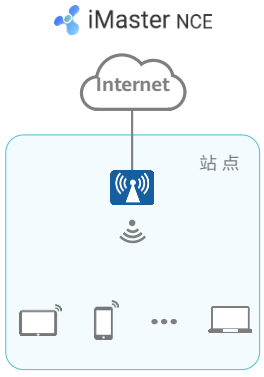
任务名称	任务描述
在FW上配置NAT	FW设备做出口网关时支持基于出接口地址方式的NAT（又称为Easy IP），下行网络中的设备能以FW的WAN口公网IP地址访问Internet。
在AR上配置NAT	AR设备做出口网关时支持基于出接口地址方式的NAT（又称为Easy IP），下行网络中的设备能以AR的WAN口公网IP地址访问Internet。
在AP上配置NAT	单AP的组网场景下，配置SSID时在“基本配置”页面中“网络连接方式”选择“NAT”。
在AP上配置NAT日志开关	NAT日志是设备在做NAT时生成的信息记录，该信息包括：报文的源IP地址、源端口、目的IP地址、目的端口、转换后的源IP地址、转换后的源端口以及NAT的时间信息和用户执行的操作等。网络管理员可以通过查看NAT日志实时定位用户通过NAT访问网络的情况，增强了网络的安全性。通过开启对应的开关可以设置将NAT日志输出至日志服务器。

- NAT网络地址转换（Network Address Translation）是一种将私有（保留）地址转化为合法IP地址的转换技术，可以将IPv4报文头中的地址转换为另一个地址。通常情况下，利用NAT技术将IPv4报文头中的私网地址转换为公网地址，可以实现位于私网的多个用户使用少量的公网地址同时访问Internet。因此，NAT技术常用来解决随着Internet规模的日益扩大而带来的IPv4公网地址短缺的问题。
- 在中小型园区网络中，往往只有出口网关设备有公网IP地址，当园区中的用户需要访问Internet时，必须在出口网关上进行NAT地址转换，所以需要在iMaster NCE-Campus上对出口网关使能NAT功能。
  - 中小型园区网络中，最常见的出口网关是AR或者FW，直接在网络中使能出口网关的NAT功能即可。
  - 对于单AP的组网场景，需要在AP的SSID中配置“网络连接方式”为NAT。

部署无线网络：SSID

- 在WLAN网络中，SSID用来表示不同的无线网络，在手机等终端上搜索可接入的无线网络时，显示出来的网络名称就是SSID，终端用户可选择相应的SSID接入网络，每个SSID可以指定一种认证方式，从而实现对无线接入的终端用户准入控制。
- 每个SSID只能指定一种认证方式，终端用户接入网络时选择的无线网络就决定了所采用的认证方式，但是可以按照不同的用户角色或者不同的业务类型规划多个SSID，可以采用不同的认证方式。比如：商铺场景可针对三种不同的无线业务，规划3个SSID：
  - SSID1用于员工的无线办公。
  - SSID2用于访客的Internet上网。
  - SSID3用于扫描枪等哑终端接入。对于非面向终端用户的SSID，比如：用于扫描枪接入的SSID，可以设置为隐藏SSID的方式，避免被普通用户搜索到。

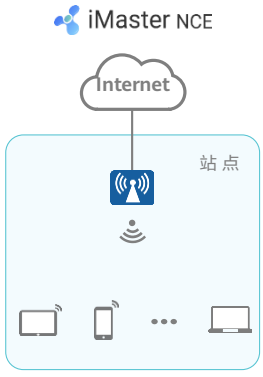
案例1：部署用于员工无线办公的SSID（802.1X认证）



配置WLAN的基本参数

HUAWEI

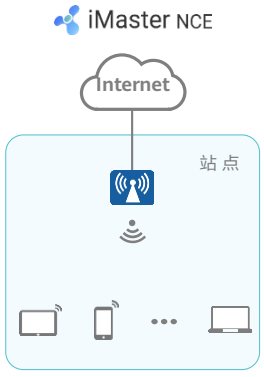
案例1：部署用于员工无线办公的SSID - 配置安全认证

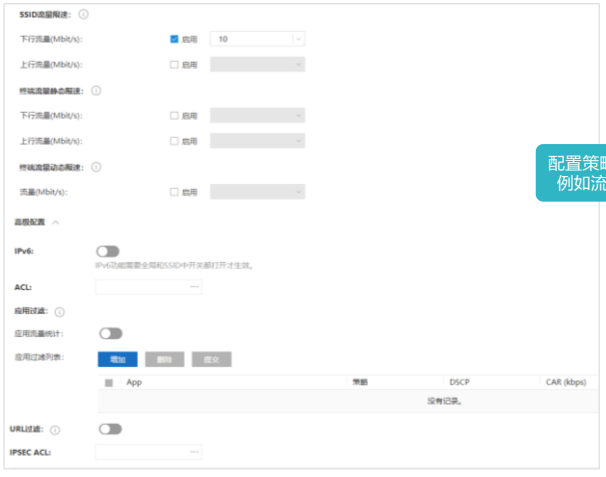


配置安全认证（802.1X认证），使用iMaster NCE作为Radius服务器。

HUAWEI

案例1：部署用于员工无线办公的SSID - 配置策略控制

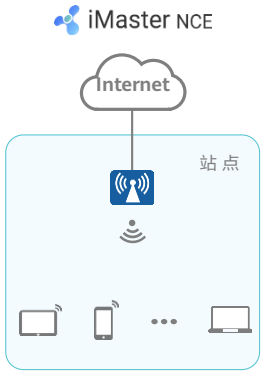


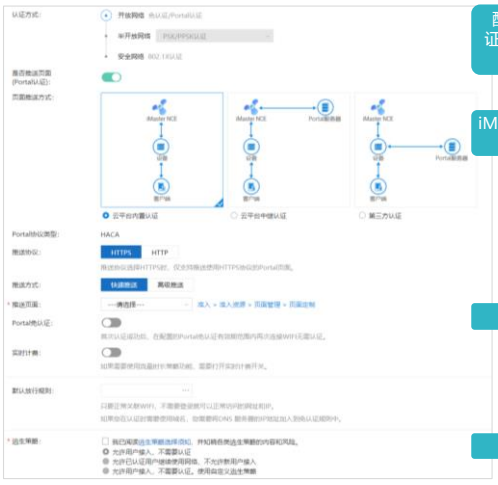


配置策略控制参数，例如流量限速等。

HUAWEI

案例2：部署用于访客上网的SSID（Portal认证）





配置安全认证（Portal认证），使用iMaster NCE作为Portal服务器。

iMaster NCE支持多种Portal页面推送方式

支持Portal页面定制

支持逃生策略

HUAWEI

部署无线网络：射频调优

- WLAN技术以射频信号作为传输介质。为了避免信号互相干扰，相邻AP必须使用非重叠信道传输无线信号。通过调整信道和功率，可以使各AP的信道和功率保持相对平衡，保证整个网络整体工作在最佳状态。
- 在AP上按实际需要配置握手协议模式、空口扫描参数和天线增益等，可以合理控制AP的无线网络覆盖区域、减少射频干扰和数据传输冲突。通过为射频功能配置定时开启/关闭策略，可以降低不必要的能耗。
- 射频调优有三种调优模式：
  - 自动调优：指定AP设备根据调优时间与间隔（缺省起始时刻03:00:00，间隔1440min）进行周期性的全局调优。
  - 定时调优：指定AP设备在每天指定时刻触发全局调优。
  - 手动调优：AP设备不会主动进行调优，用户需在iMaster NCE-Campus上手动对站点内的AP进行全局或者局部调优。

调优模式建议：

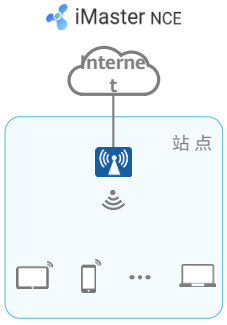
- 开局阶段，在完成AP部署并上线后，进行一次手动调优，以自动完成AP的信道与功率规划。
- 网络正常运行阶段，推荐使用定时调优，在业务空闲的时间段，定时对网络进行调优，以减少对业务的影响。

部署网络安全

- 随着网络技术的普及以及网络应用的多样性，网络攻击行为出现的越来越频繁。为了提高网络安全，建议通过配置安全策略加强AP的防范能力。
  - 将一些与设备相连的固定上行设备或信任用户的MAC地址配置为静态MAC表项，可以保证其安全通信。
  - 配置无线安全策略，检测和反制非法AP，保护企业网络和用户不被无线网络上未经授权的设备访问。
  - 启用攻击防范，通过分析上送CPU处理的报文内容和行为，判断报文是否具有攻击特性，并配置对具有攻击特性的报文执行一定的防范措施。
  - 通过如下方法对允许接入到AP的终端设备进行限制：
    - 黑名单（MAC地址）
    - 白名单（MAC地址或OUI）
  - 通过广播报文和IGMP组播报文限速，使AP的广播报文和IGMP组播报文速率限制在合理的范围内，防止这些报文占用过多网络资源。

部署安全策略

- 防火墙FW的基本作用是对进出网络的访问行为进行控制，保护特定网络免受“不信任”网络的攻击，但同时还必须允许两个网络之间可以进行合法的通信。FW实现访问控制就是通过安全策略技术来实现的。
- 安全策略是FW的核心特性，它的作用是对通过FW的数据流进行检验，只有符合安全策略的合法流量才能通过FW进行转发。



HUAWEI

- 安全策略是由匹配条件（例如五元组、用户、时间段等）和动作组成的控制规则，FW收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，并将流量的属性与安全策略的匹配条件进行匹配。如果所有条件都匹配，则此流量成功匹配安全策略。流量匹配安全策略后，设备将会执行安全策略的动作。

部署增值业务：商业Portal推送

- 企业给访客提供WLAN网络服务时，通常是采用Portal认证的方式，包括用户名/密码、匿名认证、短信认证、Facebook认证以及Passcode认证等，这些认证方式需要系统推送相关的Portal页面供终端用户进行认证的交互操作，每套推送页面中包含了认证页面、用户须知页面和注册页面，租户管理员可以指定其中一个作为推送的第一个页面。
- 对于每种认证方式，iMaster NCE支持提供内置的页面格式，也可以根据需要定制修改Portal页面具体的内容。

基于内置模板定制	基于自定义模板定制
1. 只需要做少量、简单的编辑就可以完成页面的定制。 2. 只支持中、英文两种语言；如需更多语言，可基于自定义模板进行定制。 3. 内置模板定制支持如下三种方式： ① 方式一：基于内置模板，简单修改。 ② 方式二：基于内置模板，创建新的页面。 ③ 方式三：下载模板，定制页面后再上传。	1. 具有更大的发挥空间。 例如：定制更多语言的页面，设计页面布局，配置页面上呈现的文字及样式。 2. 系统默认支持四种语言模板： ① 中文 ② 英文 ③ 德文 ④ 西班牙文

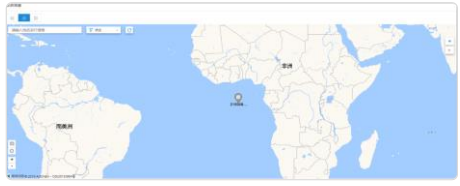
- 企业可以基于该能力快速简单的定制出适合自己的Portal门户页面，从而进行品牌推广、广告推送等增值业务。
- Portal页面定制分为两种：
  - 基于内置模板定制：
    - 在这种定制模式下，您只需要做少量、简单的编辑就可以完成页面的定制。例如：修改页面中呈现的文字，修改语言种类、推送协议，更换背景图片。
    - 基于内置模板定制的页面，只支持中、英文两种语言；如需更多语言，您可以基于自定义模板进行定制。
    - 内置模板定制支持如下三种方式：方式一：基于内置模板，简单修改；方式二：基于内置模板，创建新的页面；方式三：下载模板，定制页面后再上传。
  - 基于自定义模板定制：
    - 在这种定制模式下，您可以具有更大的发挥空间。例如：定制更多语言的页面，设计页面布局，配置页面上呈现的文字及样式。
    - 系统默认支持四种语言模板：中文、英文、德文、西班牙文。在语言模板中，可以按语言、按页面配置每个页面上需要呈现内容。

目录

监控：站点

- 网络业务发放后，用户需要监控站点设备的在线状态、网络资源状态等信息，便于维护人员掌握设备的数据状况，防范异常。
- 在iMaster NCE主菜单中选择“监控> 健康度 > 站点” 。

查看云管设备健康度、网络健康度和终端丢包率。



基于室外地图查看设备部署状态

•••

以列表方式查看站点内所有设备状态

查看站点健康度、管设备状态、告警、云管设备健康度统计信息

监控WAN统计信息

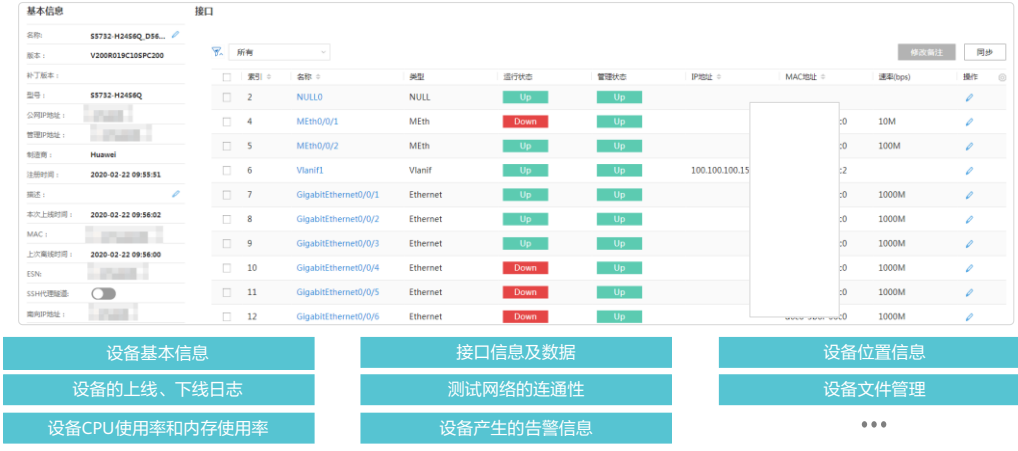
•••

HUAWEI

- 查看云管设备健康度、网络健康度和终端丢包率。
  - 云管设备健康度分数 =（1-异常设备/设备总数）*100。
  - 网络健康度分数（WIFI），即射频健康度分数=(1 – 异常射频数 / 总射频数) * 100。
  - 网络健康度分数（WAN）= 站点所有链路质量的平均值（sitelqm）*10。

监控：设备

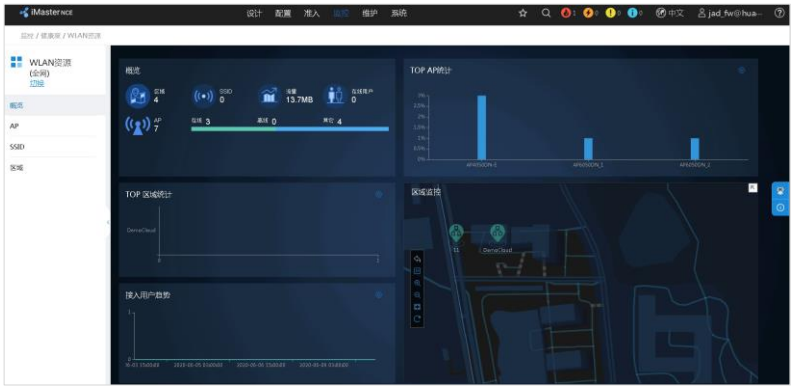
- 选择“监控 > 健康度 > 设备360”，进入设备监控页面。点击相应设备，可进入设备的管理页面：



- 可查看设备名称、版本号、补丁版本、型号、公网IP地址、制造商、注册时间、描述、本次上线时间、MAC、上次离线时间、ESN、SSH代理隧道、南向IP地址和性能数据上报端口等基本信息。
- 可监控接口相关数据。
- 可查看设备的上线、下线日志。
- 可结合地图查看设备所在位置。
- 可进行Ping/Ping self、Trace、虚拟电缆探测操作，测试网络的连通性。
- 可对设备文件进行管理。
- 可查看设备CPU使用率和内存使用率。
- 可查看此设备产生的告警信息。

监控：WLAN资源

- iMaster NCE-Campus支持查看区域内WLAN网络重要的指标项，通过多指标的关联分析，帮助用户更好的了解区域内WLAN网络的整体运行状况。

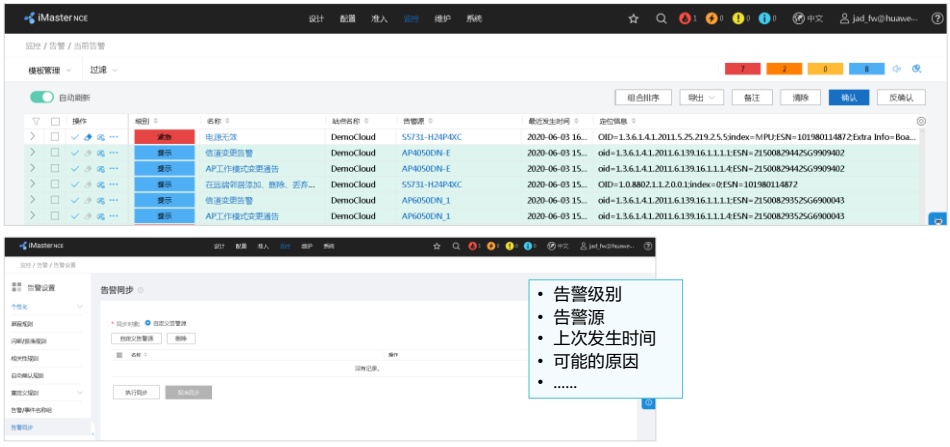


HUAWEI

- 查看区域内WLAN网络重要的指标项（包括TOP AP统计、TOP区域统计、接入用户趋势、AP信息、SSID信息等）

告警

- 用户可通过设置告警/事件规则，制定符合自身需求的告警/事件监控策略，提升故障解决效率。



目录

CloudCampus APP现场验收（1）

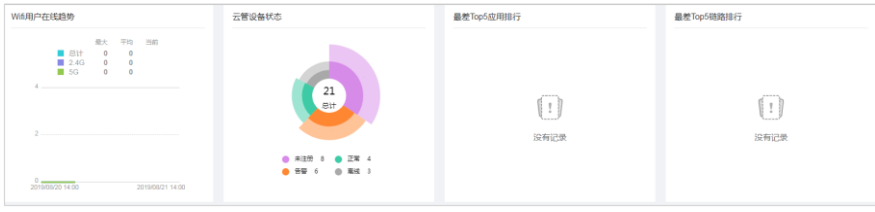
- Wi-Fi体检：通过Wi-Fi体检可以快捷地从WiFi覆盖、业务体验、网络安全三方面检测Wi-Fi。适用于不依赖于图纸的测试，可以随时随地检测Wi-Fi，并支持导出报告。

CloudCampus APP现场验收（2）

- 漫游验收：在租户现场的整个区域行走并持续打点，确认终端设备可以在AP之间正常使用漫游功能。

登录iMaster NCE-Campus验收

查看W-Fi用户在线趋势、云设备状态、最差Top5应用排行和最差Top5链路排行



查看异常云设备列表和告警信息

HUAWEI

思考题

1. 用户在iMaster NCE上配置AP业务时，针对SSID的认证方式，可以选择(　　)。
   A. 开放网络（免认证/Portal认证）
   B. 半开放网络（PSK/PPSK认证）
   C. 安全网络（802.1X认证）

- ABC

本章总结

- 本课程系统介绍了CloudCampus中小型园区网络方案部署流程，其中包括软硬件安装、开局部署、业务部署、运维管理及验收测试。
- 通过本课程的学习，搭配基于实际环境的练习，学员将能独立完成CloudCampus中小型园区网络方案部署，并具备网络运维及管理能力。

学习推荐

- 智简园区网络解决方案 V100R019C10 产品文档
  - https://support.huawei.com/hedex/hdx.do?docid=EDOC1100141274&lang=zh&id=library_change_preview&from=HedExLite

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

WLAN故障排除

HUAWEI

前言

- WLAN在提供方便的网络接入的同时，出现故障的风险也相对较高，构建无线局域网后，网络工程师必须准备就绪，随时调查可能发生的问题。
- 本章结合资深工程师的排错经验，重点讲解WLAN故障排除思路和部分辅助工具。帮助广大工程师在遇到故障时，能够有办法去定位和排除故障。

目标

- 学完本课程后，您将能够：
  - 描述WLAN网络的故障处理思路
  - 描述WLAN故障排查辅助软件的使用
  - 掌握通过WLAN报文分析进行故障定位的方法

目录

通用故障处理流程

- 故障处理往往被认为是一份很复杂、很困难且对工程师要求较高的工作，想要高效排除故障，在对各种技术原理、产品特性掌握到位后，还需要清楚一般处理流程，才能有条不紊的展开工作。

确认故障

- ✓ 确认故障现象
- ✓ 确认复现情况
- ✓ ...

评估故障

- ✓ 评估故障等级
- ✓ 评估故障排除时间
- ✓ ...

收集资料

- ✓ 收集网络信息
- ✓ 收集配置信息
- ✓ 收集设备日志
- ✓ ...

故障排除

- ✓ 定位故障
- ✓ 排除故障
- ✓ 业务测试
- ✓ 输出报告
- ✓ ...

常见的WLAN故障现象

AP上线故障

AP掉线、版本升级失败等导致AP无线上线故障。

STA上线故障

STA无法上线。

认证问题

用户认证出现问题。

信号问题

信号导致的服务问题。

其它接入问题

其它问题导致用户无法接入WLAN网络。

网速&丢包&延迟&漫游等服务质量问题

用户可以接入网络，但是体验不好。

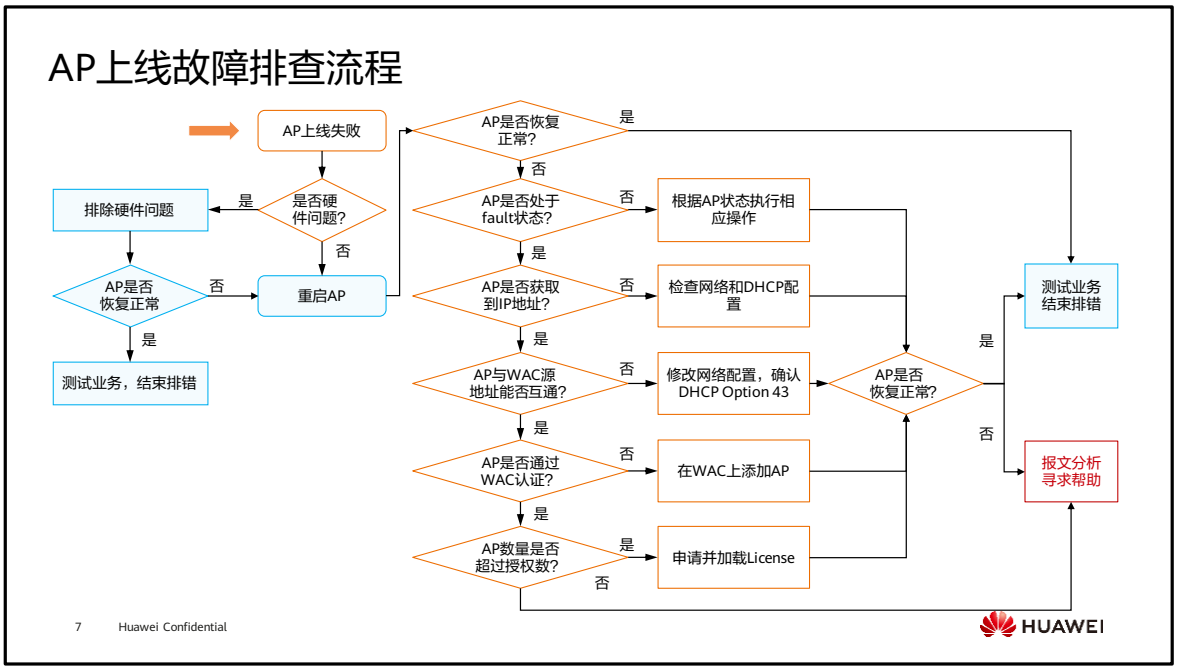
组网可靠性问题

组网可靠性存在问题，故障引发业务受损，导致业务受到影响。

其它原因

未知原因导致WLAN网络故障。

AP上线故障

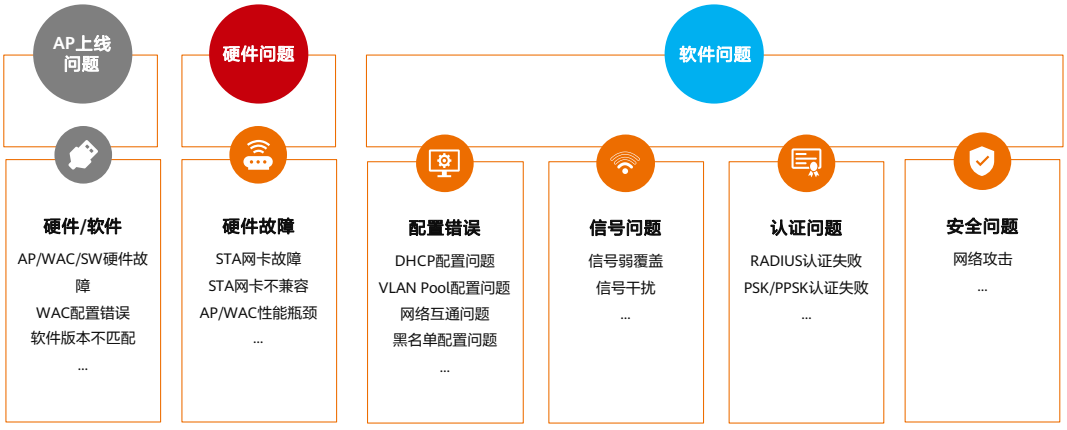


- AP的故障排查是基于AP上线流程来进行的，WLAN工程师务必要对CAPWAP隧道建立流程非常熟悉，才能有效的进行排查。

AP上线故障排查常用命令

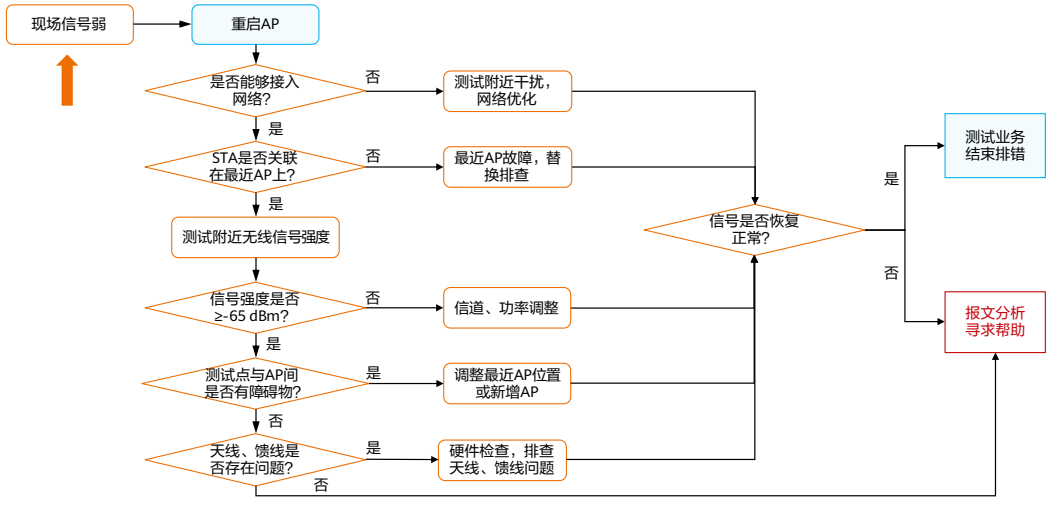
- **display ap** { **all** | **ap-group** ap-group }
  - 主要用于查看AP的IP地址以及状态信息，重点关注AP是否正常获取到IP地址，AP状态是否正常。
- **display ap online-fail record**
  - 主要用于查看AP上线失败的原因，然后可以根据具体原因采取相应的措施。
- **trace enable brief/trace object mac-address** *ap-mac-address*
  - 对AP进行业务流程诊断，重点关注查看上线信息中是否存在异常情况。
- **display mac-address** *mac-address*
  - 主要用来查看AP的网关设备能否正常学习到AP的MAC地址，便于检查网络的连通性。
- **display license resource usage**
  - 主要用来查看WAC可纳管的AP数量是否达到了上限。

STA上线故障



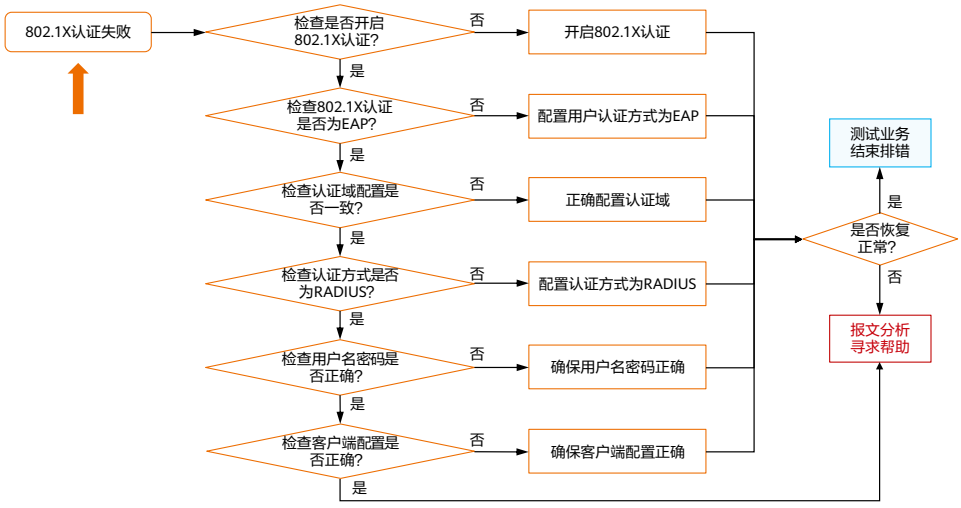
STA上线故障 - 信号问题

信号问题一般排查流程



STA上线故障 - 认证问题

802.1X认证故障排查流程



802.1X认证故障排查技巧 - 查看是否开启了802.1X认证

- 查看认证模板"HCIE-WLAN"下是否引用了802.1X接入模板"HCIE-WLAN"。

```
<WAC> system-view
[WAC] authentication-profile name HCIE-WLAN
[WAC-authentication-profile-HCIE-WLAN] display this
#
authentication-profile name HCIE-WLAN
 dot1x-access-profile HCIE-WLAN
```

- 如果未引用802.1X接入模板，则在认证模板视图下引用802.1X接入模板。

```
[WAC-authentication-profile-HCIE-WLAN] dot1x-access-profile HCIE-WLAN
```

- 查看VAP模板"HCIE-WLAN"下是否引用了认证模板"HCIE-WLAN"。

```
[WAC-wlan] vap-profile name HCIE-WLAN
[WAC-wlan-vap-prof-HCIE-WLAN] display this
#
 forward-mode tunnel
 service-vlan vlan-id 101
 ssid-profile 1
 security-profile 1
 authentication-profile HCIE-WLAN
```

- 如果未引用认证模板，则在VAP模板视图下引用认证模板。

```
[WAC-wlan-vap-prof-HCIE-WLAN] authentication-profile HCIE-WLAN
```

802.1X认证故障排查技巧 - 检查用户认证方式是否为EAP

- 802.1X认证包括EAP、CHAP和PAP三种方式，需保证客户端与服务器均支持该种方式，否则用户无法通过认证。
- 手机等移动终端仅支持EAP方式，所以设备上也应配置为EAP方式，EAP方式为设备的默认配置。
- 查看802.1X接入模板下配置的用户认证方式。

```
<WAC> display dot1x-access-profile configuration name HCIE-WLAN
  Profile Name                    : HCIE-WLAN
  Authentication method           : EAP
  Re-Authen                       : Disable
  Client-no-response authorize    : -
  Max retry value                 : 2
  Reauthen Period                 : 3600s
  Client Timeout                  : 5s
  Bound authentication profile    : HCIE-WLAN
```

- 如果认证方式不是”EAP”，则配置为”EAP”。

```
<WAC> system-view
[WAC] dot1x-access-profile name HCIE-WLAN
[WAC-dot1x-access-profile-HCIE-WLAN] dot1x authentication-method eap
```

802.1X认证故障排查技巧 - 检查认证域配置是否正确

- 在802.1X认证配置中，需要配置AAA方案，可以包括认证方案模板、计费方案模板、授权方案模板和业务方案模板。认证方案选用RADIUS认证，还需要配置RADIUS服务器模板，设置和服务器对接的参数。
- 查看认证模板下的配置方式，方案直接引用到认证模板。

```
[WAC] authentication-profile name HCIE-WLAN
[WAC-authentication-profile-HCIE-WLAN] display this
#
authentication-profile name HCIE-WLAN
 dot1x-access-profile HCIE-WLAN
 authentication-scheme radius
 accounting-scheme radius
 radius-server radius
#
```

- 域引用到认证模板。

```
[WAC-aaa] domain radius
[WAC-aaa-domain-radius] display this
#
 domain radius
  authentication-scheme radius
  accounting-scheme radius
  radius-server radius
#
```

```
[WAC] authentication-profile name HCIE-WLAN
[WAC-authentication-profile-HCIE-WLAN] display this
#
authentication-profile name HCIE-WLAN
 dot1x-access-profile HCIE-WLAN
 access-domain radius
#
```


HUAWEI

- 实现上述配置有两种方式。
  - 将方案直接引用到认证模板。
  - 先将方案引用到域，再将域引用到认证模板。
- 如果两种方式同时配置，则方案直接引用到认证模板的方式，优先级更高。所以先查看认证模板下的配置方式，再进入到对应的视图下查看配置是否正确。

802.1X认证故障排查技巧 - 检查认证方式和用户名密码

- 若不使用认证域进行认证，需要检查认证模板下绑定的认证方案模板下配置的认证方式是否为RADIUS认证。
- 若使用认证域进行认证，需要检查认证域下绑定的认证方案模板下配置的认证方式是否为RADIUS认证。
- 通过命令行查看认证方案模板下认证方式。

```
[WAC-aaa] authentication-scheme radius
[WAC-aaa-authen-radius] display this
#
 authentication-scheme radius
  authentication-mode radius
#
```

- 执行命令**test-aaa**查看设备与RADIUS服务器是否可达，并可验证用户名密码是否正确。

```
[WAC] test-aaa test huawei123 radius-template radius
```

- 执行命令后，根据提示信息判断：
  - 若提示信息显示为"Account test succeed"，则说明设备与RADIUS服务器链路正常，且测试用户名密码正确。
  - 若提示信息显示为"User name or password is wrong"，则说明设备与RADIUS服务器链路正常，但用户名密码信息错误，需要检查用户名密码信息。
  - 若提示信息显示为"Account test time out"，则说明认证设备与RADIUS服务器不可达或RADIUS服务器模板配置不正确。

802.1X认证故障排查技巧 - 信息收集

- 收集trace信息。

```
[WAC] trace object ip-address ip-address
[WAC] trace enable
```

- 收集完成后，删除trace实例。

```
[WAC] undo trace object all
[WAC] undo trace enable
```

- 查看用户上线失败原因。

```
[WAC] diagnose
[WAC-diagnose] display aaa online-fail-record all
```

- 查看用户下线原因。

```
[WAC] diagnose
[WAC-diagnose] display aaa offline-fail-record all
```

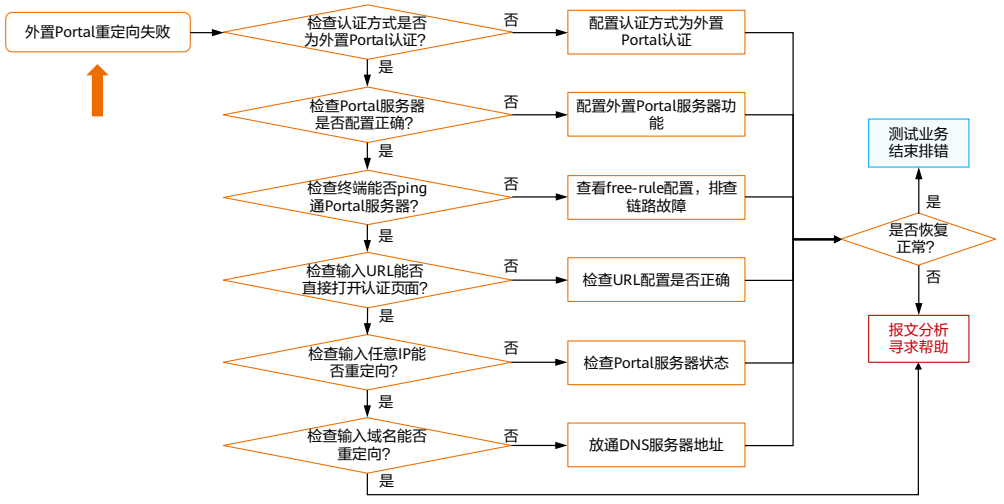
- 查看用户异常下线原因。

```
[WAC] diagnose
[WAC-diagnose] display aaa abnormal-offline-record all
```

- 查看dot1x计数信息。

```
[WAC] display dot1x
```

外置Portal重定向页面失败排查流程



Portal重定向失败 - 检查Portal认证配置是否正确

- 通过命令行查看Portal接入模板下是否开启外置Portal服务器功能。

```
[WAC] portal-access-profile name local_portal_access_profile
[WAC-portal-access-profile-local_portal_access_profile] display this
#
portal-access-profile name local_portal_access_profile
 web-auth-server portal direct
```

- 查看Portal接入模板是否绑定在认证模板下。

```
[WAC] authentication-profile name portal_authen_profile
[WAC-authentication-profile-portal_authen_profile] display this
#
authentication-profile name portal_authen_profile
 portal-access-profile local_portal_access_profile
 free-rule-template default_free_rule
#
```

- 查看认证模板是否绑定在VAP模板下。

```
[WAC-wlan-view] vap-profile name portal_authen_test
[WAC-wlan-vap-prof-portal_authen_test] display this
#
 forward-mode tunnel
 service-vlan vlan-id 200
 ssid-profile portal_authen_test
 authentication-profile portal_authen_profile
#
```

Portal重定向失败 - 检查Portal服务器是否配置正确

- 查看外置Portal服务器配置。

```
[WAC] display web-auth-server configuration
 Listening port: 2000
 Portal: version 1, version 2
 Include reply message : enabled
 ------------------------------------------------------------------------------
 Web-auth-server Name : portal
 IP-address           : 192.168.13.1
 Shared-key           : %^%#xZD=PF^$,"+n#W3@LRoB!x^~Hco42X\p@UJaw]h#%^%#
 Source-IP            : -
 Port / PortFlag      : 50100 / NO
 URL                  : http://192.168.13.1:8080/PortalServer
 URL Template         : portal
 Redirection          : Enable
 Sync                 : Disable
 Sync Seconds         : 0
 Sync Max-times       : 0
 Detect               : Disable
 Detect Seconds       : 60
 Detect Max-times     : 3
 Detect Critical-num  : 0
 Detect Action        :
 Bound Portal profile : portal_test
 ------------------------------------------------------------------------------
1 Web authentication server(s) in total
```

Portal重定向失败 - 检查终端是否能ping通Portal服务器

- 若不能ping通外置Portal服务器地址，则检查free-rule是否在AP上应用。

```
[AP] diagnose
[AP-diagnose] display portal free-rule
------------------------------------------------------------------------------
Dynamic free rule
 destination ip 10.10.10.10 mask 255.255.255.255 source ip x.x.x.x mask 255.255.255.255 vlan x
Total 1
------------------------------------------------------------------------------
......
```

- 查看终端网关是否有指向外置Portal服务器的路由，若没有，请添加路由。
- 查看Portal服务器是否有指向终端网关的路由，若没有，请添加路由。

Portal重定向失败 - URL跳转测试

- 在终端浏览器直接输入外置Portal服务器URL，查看能否打开认证页面。
- 若不能打开认证页面，则检查设备上外置Portal服务器URL配置是否正确。
- 若是在web-auth-server模板下配置了URL模板，则执行命令display url-template查看配置是否正确。

```
[WAC] display url-template name portal
 Name                  : portal
 URL                   : http://192.168.13.1:8080/PortalServer
 Start mark            : ?
 Assignment mark       : =
 Isolate mark          : &
 AC IP                 :
 AC MAC                :
 AP IP                 :
 AP MAC                :
 SSID                  :
 User MAC              :
 Redirect URL          :
 User IP address       :
 Sysname               :
 Delimiter             :
 Format                :
.....
```

Portal重定向失败 - 检查URL中参数配置是否正确

- 对接第三方Portal服务器时，URL中可能需要携带指定参数，Portal服务器可根据URL中的参数获取到用户终端的信息，并根据获取到的用户终端信息为不同用户提供不同的WEB认证界面。
- 设备支持在URL中携带的参数包括AC的系统名称、AC的IP地址、AC的MAC地址、AP的IP地址、AP的MAC地址、用户关联的SSID、用户的IP地址、用户的MAC地址和用户访问的原始URL地址等参数。
- 当URL中需要携带参数时，只能通过URL模板配置。

```
[WAC] url-template name portal
[WAC-url-template-portal] url-parameter ac-ip acip ap-ip apip user-mac usermac
```

Portal重定向失败 - IP地址跳转测试

- Portal认证时，在浏览器中输入任意IP地址（非免认证规则放通的地址），都可以跳转到Portal认证页面进行认证。
- 在终端浏览器输入任意IP地址（非免认证规则放通的地址），查看能否重定向出Portal认证页面。
- 在终端浏览器输入HTTPS协议的网站时无法打开重定向页面，需要使能Portal认证HTTPS重定向功能。

```
[WAC] portal https-redirect enable
```

- 若不能重定向出Portal认证页面，则在AC上通过命令行查看Portal服务器状态。

```
<WAC> display server-detect state
Web-auth-server     :portal
Total-servers       :1
Live-servers        :1
Critical-num        :0
Status              :Normal
IP-address          Status
192.168.13.1        UP
```


HUAWEI

- 用户访问HTTPS协议的网站触发Portal认证时，浏览器会弹出安全提示，需要用户点击继续才能完成Portal认证。
- 执行HSTS的浏览器或网站不能进行重定向。
- 如果用户发送的HTTPS请求报文的目的端口号是非知名端口（443），则不能进行重定向。
- AC上通过命令行查看Portal服务器状态。
  - 若服务器状态为Abnormal，需要确认Portal服务器侧是否支持探测及是否开启探测。
  - 若服务器支持探测，则需要开启探测。
  - 若服务器侧不支持探测，则需要在设备侧通过以下命令行关闭探测。
    - [WAC] **web-auth-server portal**
    - [WAC-web-auth-server-portal] **undo server-detect**

Portal重定向失败 - 检查DNS相关配置

- 如果直接输入IP地址能够重定向出认证页面，但输入域名无法重定向，查看DNS服务器IP地址是否加入到免认证规则中。
- 查看DNS服务器IP是否加入到免认证规则中。

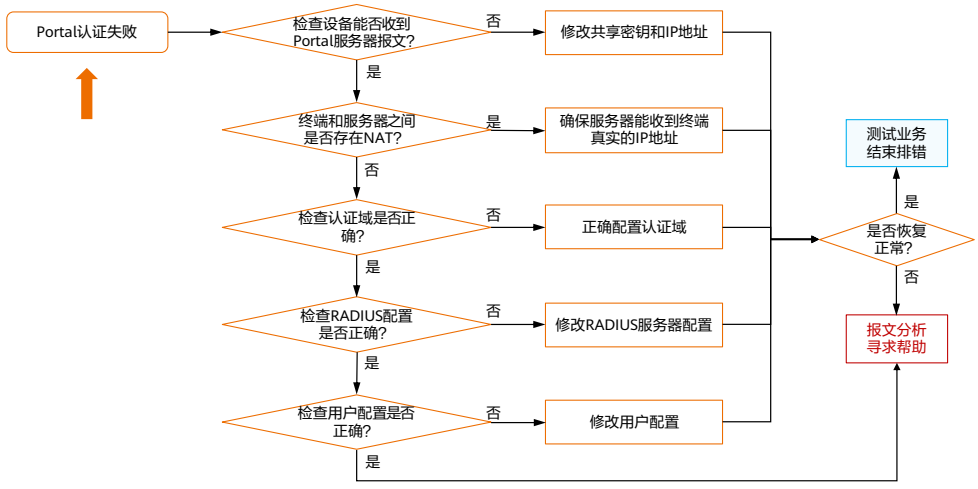
```
[WAC] free-rule-template name portal_free_rule
[WAC-free-rule-portal_free_rule] display this
#
free-rule-template name portal_free_rule
 free-rule 1 destination ip 10.72.55.101 mask 255.255.255.255
#
```

- 在AP上收集Portal模块debug信息。

```
<AP> debugging portal all
<AP> terminal debugging
<AP> terminal monitor
```


- 用户访问HTTPS协议的网站触发Portal认证时，浏览器会弹出安全提示，需要用户点击继续才能完成Portal认证。
- 执行HSTS的浏览器或网站不能进行重定向。
- 如果用户发送的HTTPS请求报文的目的端口号是非知名端口（443），则不能进行重定向。
- AC上通过命令行查看Portal服务器状态。
  - 若服务器状态为Abnormal，需要确认Portal服务器侧是否支持探测及是否开启探测。
  - 若服务器支持探测，则需要开启探测。
  - 若服务器侧不支持探测，则需要在设备侧通过以下命令行关闭探测。
    - [WAC] **web-auth-server portal**
    - [WAC-web-auth-server-portal] **undo server-detect**

Portal认证失败排查流程



Portal认证故障排查技巧 - 检查是否收到服务器的请求报文

- 检查设备是否收到Portal服务器发送的请求报文及报文是否正确。
- 在诊断视图下通过命令查看Portal请求报文计数是否有增加。

```
[WAC] diagnose
[WAC-diagnose] display web statistics
  MAX session number     : 0
  Current session number : 0 head = 4, tail = 3
  ......
  Packet error Totol          :0
  Challenge req error         :0
  Auth req error              :0
  Logout req error            :0
  Info req error              :0
  Auth ntf error              :0
  Discover req error          :0
  IPChange ack error          :0
  Cut ack error               :0
  Recv auth req               :0
  Recv Auth ntf               :0
  Recv Logout req             :0
  Recv Challenge req          :0
......
```

- 外置Portal服务器决定了认证方式是PAP方式还是CHAP方式，若是PAP方式，查看Recv auth req计数是否增加，若是CHAP方式，查看Recv Challenge req计数是否增加，如果报文计数增加，则表明正确收到Portal服务器侧报文。

HUAWEI

- 如果报文计数没有增加则进行以下操作。
  - 检查Portal服务器侧报文是否正确发送。
    - 检查Portal服务器侧是否添加设备地址。以Controller服务器为例，若服务器未添加设备IP地址，在认证页面输入用户名密码，认证页面显示认证成功，但用户访问网络时将会再次重定向出Portal认证页面，产生该现象的原因是Controller服务器未向设备发送Portal请求，出现假认证，用户未在设备上认证成功。若Portal服务器侧未添加设备地址，请配置添加。
    - 检查Portal服务器侧接收和发送报文的端口号，是否分别与设备侧一致，若不一致请重新配置端口号。
  - 查看Packer error number计数是否有增加，若有增加，表明收到的Portal报文有误，可以尝试如下操作。
    - 检查Portal服务器侧和设备侧配置的shared key是否一致，若不一致，在设备侧通过命令行修改shared key。
      - [WAC] **web-auth-server portal**
      - [WAC-web-auth-server-portal] **shared-key cipher** *xxxx*
  - 检查Portal服务器发送报文的源IP地址与设备侧配置的server ip是否一致，若不一致，在设备侧通过命令行修改server ip。
      - [WAC] **web-auth-server portal**

- [WAC-web-auth-server-portal] **server-ip** *X.X.X.X*

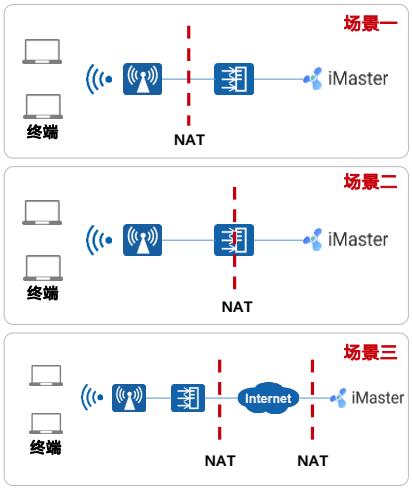
Portal认证故障排查技巧 - 检查客户网络是否配置NAT转换

- 如果终端与Portal服务器之间存在NAT，Portal服务器可能无法获取终端的真实IP地址，会导致Portal服务器无法根据终端IP地址找到接入控制设备，进而导致终端Portal认证失败。
- 场景一：NAT业务部署在AP与AC之间。
- 场景二：NAT业务部署在AC。
  - 解决方法：配置AC向Portal服务器发送终端的真实地址。

```
[WAC] url-template name url1
[WAC-url-template-url1] url http://172.18.1.1:8080/portal
[WAC-url-template-url1] url-parameter user-ipaddress userip
```

- 场景三：Portal服务器和AC之间经过两次NAT。
  - 解决方法：配置AC向Portal服务器发送终端和AC的真实地址。

```
[AC] url-template name url1
[AC-url-template-url1] url http://172.18.1.1:8080/portal
[AC-url-template-url1] url-parameter user-ipaddress userip ac-ip acip
```



Portal认证故障排查技巧 - 检查RADIUS服务器配置是否正确

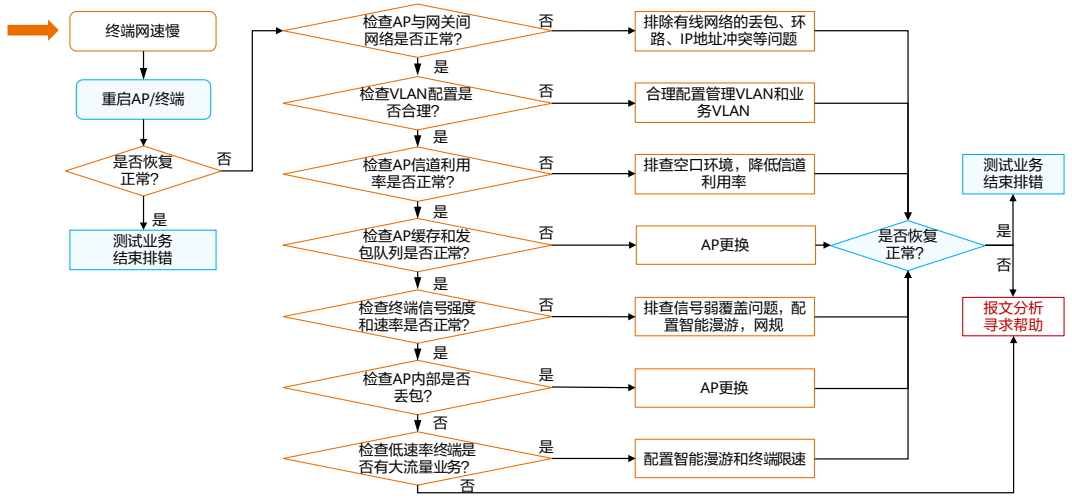
- 如果配置通过远端Radius服务器认证，那么需要查看Radius服务器模板下共享秘钥、端口号是否与服务器上的一致。

```
[WAC] display radius-server configuration
----------------------------------------------------------------------------------------------
Server-template-name            :radius
Protocol-version                :standard
Traffic-unit                    :B
Shared-secret-key               :%^%#-YBtX+C'@-Q\&L>T~OE~0E%XSH:~
Timeout-interval(in second)     :5
Retransmission                  :3
EndPacketSendTime               :3
Dead time(in minute)            :5
Domain-included                 :Original
NAS-IP-Address                  :0.0.0.0
Calling-station-id MAC-format   :xxxx-xxxx-xxxx
Called-station-id MAC-format    :XX-XX-XX-XX-XX-XX
Server algorithm                :master-backup
Authentication Server 1         :192.168.13.1  Port:1812  Weight:80[UP]
                                Vrf:- LoopBack:NULL
                                Source IP: ::
Accounting Server 1             :192.168.13.1  Port:1813  Weight:80[UP]
                                Vrf:- LoopBack:NULL
                                Source IP: ::
----------------------------------------------------------------------------------------------
```

- 由于显示的共享密钥为密文，无法直接看出RADIUS服务器模板下的共享密钥是否与服务器上的一致，建议根据服务器使用的密钥，重新配置RADIUS服务器模板下的共享密钥，使它们保持一致。

STA网速慢/丢包/漫游等用户体验故障

STA网速慢故障排查流程



STA网速慢排查技巧 - 确认故障范围

- 通过ping包确认故障范围。
  - 从STA ping网关，出现丢包、 延迟过高等问题，故障在网关以下网络。
  - 从STA ping网关正常，但是ping外网不稳定，故障在网关与外网之间网络。
- AP与网关间的有线网络是否正常。
  - 网关与PoE交换机的Ping包稳定，需开始排查无线侧网络问题。
  - 网关与PoE交换机的Ping包不稳定，需排查网关与交换机间的网络问题。
- 业务VLAN和管理VLAN配置是否合理。
  - 不论是哪种转发模式，都建议业务VLAN与管理VLAN分离。

STA网速慢排查技巧 - 检查AP的信道利用率

- 检查AP的信道利用率是否正常。一般情况下，如果信道利用率超过60%，则可能会对用户造成网络波动。

```
<Huawei> display radio all
CH/BW: Channel/Bandwidth
CE: Current EIRP (dBm)
ME: Max EIRP (dBm)
CU: Channel utilization
------------------------------------------------------------------------------
AP ID Name          RfID Band Type     Status  CH/BW  CE/ME  STA  CU
------------------------------------------------------------------------------
2    1051-7250-bd20 0    2.4G bgn      on        1/20M  17/17  0   37%
2    1051-7250-bd20 1    5G   an11ac   on       36/20M  17/17  0   12%
------------------------------------------------------------------------------
Total: 2
```

- 导致信道利用率高的原因和解决方法如下：
  - 无线网络环境干扰严重，此时，需要对AP的信道进行合理的规划，降低干扰。可以手动将信道切换至信道利用率低的信道，或者在无业务影响时进行调优操作。
  - 网络中组播、广播报文很多，此时，需要查看网络中的组播、广播报文的情况。

HUAWEI

- 检查AP的信道利用率是否正常。
  - WLAN网络中所有终端共享带宽，相互竞争带宽资源，如果周围环境中无线终端很多，或网络中有很多广播、组播报文（组播、广播报文都是低速率发送，消耗空口资源多），相互抢占信道的情况就会很严重，最终导致信道利用率高，无线网络不稳定，出现ping包延迟大、丢包等情况。

STA网速慢排查技巧 - 检查AP系统报文缓存资源

- 检查AP系统报文缓存资源的剩余可用buffer资源是否正常。
  - AP的转发模块和Wi-Fi收发包模块共用一个buffer资源池，如果buffer资源不足，会出现丢包的情况。
  - 在AP上执行命令display memory-pool info查看AP系统报文缓存资源，确认剩余可用buffer资源是否正常。
  - 如果AP剩余可用的buffer资源在100以下，则认为AP的buffer资源不足，会出现丢包的情况，建议更换更强性能的AP或寻求帮助。

```
[AP-diagnose] display memory-pool info
...
Show PBuf Buffer Pool info :
============== BufMan Info ====================
BufMan Shm Addr[0x42600000], Shm Size[0x1e00000], L1 Num[64], L1 in use[6]
Buffer Num[13358], each buffer has [0x900] bytes
L1 stack info:
      Offset = 0x130, L2Offset = 0xd728, num = 128, SP = 38
L1 stack info:
      Offset = 0x3d0, L2Offset = 0xd728, num = 16, SP = 0
L1 stack info:
      Offset = 0x424, L2Offset = 0xd728, num = 0, SP = 0
L2 stack info:
      Offset = 0xd728, len = 0x4000
      front = 13014, rear = 2630, available = 6000
...
```

STA网速慢排查技巧 - 检查AP的发包队列

- 检查发包队列是否存在拥塞或者被占满的情况。
  - 报文到达AP Wi-Fi驱动模块后，会先缓存在队列中等待调度发送，如果Wi-Fi驱动模块缓存队列被占满或者拥塞严重，则会出现丢包、延迟大的情况。
  - 在AP上查看AP的Wi-Fi驱动模块发包队列情况，确认发包队列是否存在拥塞或者被占满的情况。
  - 一般情况下，Wi-Fi驱动模块的缓存队列基本处于0占用的状态，不会持续处于被占用的情况，所以如果上述显示信息中的加粗字段数字维持在100以上，则说明队列出现了拥塞的情况。

```
[AP-diagnose] display lmac txq-buf radio 1
Hardware tx queue statistic:
-------------------------------------------------------------------------------------------------------------
          Txq0      Txq1      Txq2      Txq3      Txq4      Txq5      Txq6      Txq7
Total     0         0         0         0         0         0         0         0
...
-------------------------------------------------------------------------------------------------------------
Software tid queue statistic:
-------------------------------------------------------------------------------------------------------------
          Tid0      Tid1      Tid2      Tid3      Tid4
Total     0         0         0         0         0
...
-------------------------------------------------------------------------------------------------------------
Qos queue statistic:
-------------------------------------------------------------------------------------------------------------
          BE        BK        VI        VO
Total     0         0         0         0
-------------------------------------------------------------------------------------------------------------
```


- AP Wi-Fi驱动模块的缓存队列出现拥塞，肯定是被某些终端占用了，常见的如终端信号弱、离开Wi-Fi覆盖区域等场景，都会导致发给此终端的报文无法顺利发出，而堵塞在AP的缓存队列中。
- 对于仅支持11ac类型的AP，如AP5x30xN，查看AP的Wi-Fi驱动模块发包队列情况。
  - V200R007及之后本命令行：**display wifi txq-buf radio** *radio-id*。
- 对于仅支持11n类型的AP，如AP6x10xN，查看AP的Wi-Fi驱动模块发包队列情况。
  - V200R006C20及之后版本命令行：**display wifi txq-buf radio** *radio-id*。

STA网速慢排查技巧 - 查看终端占用队列情况

- 如果AP Wi-Fi驱动模块的缓存队列出现拥塞，查看每个终端占用队列的具体情况。

[AP-diagnose] **display lmac sta-statistics queue-status radio** *1*

----------STA:aab8-3cdb-f2fc----------

Tx tid queue info:

Base info:

Tid num	: 0	1	2	3	4	5	6	7	8
Hardware txq ID	: 1	0	0	1	2	2	3	3	11
Tid flag	: 0x65	0x1	0x1	0x1	0x1	0x1	0x65	0x1	0x1007
Tid start sn	: 1	0	0	0	0	0	1233	0	0
Negotiate window size	: 64	1	1	1	1	1	64	1	1
Software retry failure	: 0	0	0	0	0	0	0	0	0
Failure count	: 0	0	0	0	0	0	0	0	0
MPDU count	: 0	0	0	0	0	0	0	0	0
Retrans MPDU count	: 0	0	0	0	0	0	0	0	0
MPDU byte	: 0	0	0	0	0	0	0	0	0
Retrans MPDU byte	: 0	0	0	0	0	0	0	0	0
MSDU num	: 0	0	0	0	0	0	0	0	0
MSDU byte	: 0	0	0	0	0	0	0	0	0
MPDU total num	: 0	0	0	0	0	0	0	0	0
Window credit	: 64	1	1	1	1	1	64	1	1

.....

- 发给终端的报文有多个优先级，每个优先级对应一个队列。如上所示的显示信息中，列出了当前AP对应射频上关联的所有终端在每一个队列中占用的buffer数量（num_mpdu_in_frameq），如果该参数的数值维持在20以上，则说明该终端占用了发包队列。

HUAWEI

- AP Wi-Fi驱动模块的缓存队列出现拥塞，肯定是被某些终端占用了，常见的如终端信号弱、离开Wi-Fi覆盖区域等场景，都会导致发给此终端的报文无法顺利发出，而堵塞在AP的缓存队列中。
- 对于仅支持11ac类型的AP，如AP5x30xN，查看AP的Wi-Fi驱动模块发包队列情况。
  - V200R007及之后本命令行：**display wifi txq-buf radio** *radio-id*
- 对于仅支持11n类型的AP，如AP6x10xN，查看AP的Wi-Fi驱动模块发包队列情况。
  - V200R006C20及之后版本命令行：**display wifi txq-buf radio** *radio-id*

STA网速慢排查技巧 - 查看组播和广播报文信息

- WLAN网络中发送组播、广播报文时，因为报文不会重传，所以为了确保接收端的收包成功率，都是以较低速率发送。如果网络中有大量的组播、广播报文往空口发送，会导致空口资源浪费严重，信道利用率持续升高，影响无线终端正常的上网体验，出现延迟大、丢包的情况。
- 在AP上查看AP对应接口上接收到的组播和广播报文的统计信息，观察组播、广播报文增长速率。可以多执行几次，观察报文统计计数增长的情况。

```
<AP> display interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
......
Input:  610 packets, 90015 bytes
  Unicast:                13,  Multicast:             244
  Broadcast:              352,  Jumbo:                0
  Discard:                0,  Total Error:            0
...
Output:  457 packets, 207021 bytes
  Unicast:    0,  Multicast:              457
  Broadcast:  0,  Jumbo:                  0
  Discard:    0,  Total Error:            0
...
    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization :    0%
    Output bandwidth utilization :   0%
```

- 如果广播或组播报文的增长速率超过100 pps，说明该接口接收到的广播、组播报文较多。在交换机或WAC的接口下配置接口二层隔离、广播和组播限速功能；在WAC的流量模板下配置用户二层隔离功能等。

HUAWEI

- 在交换机或WAC的接口下配置接口二层隔离功能。以WAC为例。
  - [WAC] **interface GigabitEthernet** *0/0/1*
  - [WAC-GigabitEthernet0/0/1] **port-isolate enable**
  - [WAC-GigabitEthernet0/0/1] **quit**
- 在WAC的流量模板下配置用户二层隔离功能。
  - [WAC-wlan-view] **traffic-profile name** *default*
  - [WAC-wlan-traffic-prof-default] **user-isolate l2**
- 在交换机或WAC上开启接口的广播和组播报文限速功能。以WAC为例。
  - [WAC] **interface GigabitEthernet** *0/0/1*
  - [WAC-GigabitEthernet0/0/1] **broadcast-suppression packets** *1000*
  - [WAC-GigabitEthernet0/0/1] **multicast-suppression packets** *1000*

STA网速慢排查技巧 - 检查终端的信号强度和速率

- 通过rf-ping命令检查问题终端的信号强度和速率是否正常。
- 无线终端信号强度弱，会导致收、发包出现重传的情况。无线通信系统的速率是动态变化的，重传会导致发送端降速来确保通信成功率。
  - 在WAC上执行命令rf-ping -c number sta-mac，查看问题终端的信号强度和速率，确认无线侧通信是否顺畅。

```
[WAC] wlan
[WAC-wlan-view] rf-ping -c 5 183d-a27a-0570
Info: RfPing start, press CTRL+C to break.
 Tx rate=130.0 Mbps, Reply from 183d-a27a-0570: RSSI=-43 dBm time < 1 ms
 Tx rate=130.0 Mbps, Reply from 183d-a27a-0570: RSSI=-44 dBm time=1 ms
 Tx rate=130.0 Mbps, Reply from 183d-a27a-0570: RSSI=-44 dBm time=1 ms
 Tx rate=130.0 Mbps, Reply from 183d-a27a-0570: RSSI=-43 dBm time < 1 ms
 Tx rate=130.0 Mbps, Reply from 183d-a27a-0570: RSSI=-43 dBm time < 1 ms
 5 packets transmitted, 5 received, 0% packet loss, time < 1 ms, RSSI -43 dBm
```

  - 如上所示的显示信息中，需要关注发包速率（Tx rate）和信号强度（RSSI）。
  - 在信号强度正常的情况下，如果速率反复变化，说明网络中存在无线干扰，需要对AP进行信道规划和功率调整。
  - 如果终端信号强度低于-70 dBm，说明终端信号强度弱，需要查看Wi-Fi网络覆盖是否存在盲区，如果存在，需要补盲解决。同时还需要查看AP是否分布密集，如果是，建议调整功率或者调整AP位置，保证漫游体验。

STA网速慢排查技巧 - 检查关联终端

- 查看终端是否关联到远端AP。
  - 如果邻居列表中存在SNR比STA当前关联的AP的SNR高，则说明终端可能关联到了远端AP，建议开启智能漫游功能。

```
<WAC> display station sta-mac b878-2eb4-2689
--------------------------------------------------------------------------------
...
The upstream SNR(dB)                    : 80.0
...
Neighbor list:
----------------------------------------------
AP name             RfID  SNR     RCPI
----------------------------------------------

----------------------------------------------
total: 0
...
--------------------------------------------------------------------------------
```

STA网速慢排查技巧 - 检查是否关闭WMM功能

- 在WAC上查看AP的射频模板，检查是否关闭了WMM功能。如果WMM功能被关闭，当前终端的速率只能为802.11g的速率，此时，需要开启WMM功能。

```
<WAC> display radio-5g-profile name default
------------------------------------------------------------------
.....
WMM switch                          : disable
.....
------------------------------------------------------------------
<WAC> system-view
[WAC] wlan
[WAC-wlan-view] radio-5g-profile name default
[WAC-wlan-radio-5g-prof-default] undo wmm disable
```

STA网速慢排查技巧 - 检查低速率终端业务

- AP关联的低速率终端收发大量数据时，可能会导致该AP下的其它用户无法正常上网，该终端停止业务后，其它用户恢复正常。
  - 通过**display station ap-id** *X*查看该AP下是否存在建链速率低的终端。

```
<WAC> display station ap-id 3
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------------------------------------------
STA MAC          AP ID   Ap name          Rf/WLAN  Band  Type  Rx/Tx   RSSI  VLAN  IPv4 address    SSID     Status
--------------------------------------------------------------------------------------------------------------------
14cf-9208-9abf   0       1047-8007-6f80   0/2      2.4G  11n   65/58   -70   10    10.10.10.253    huawei   Normal
--------------------------------------------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0
```

  - 在有业务的情况下，如果终端的建链速率（Tx或Rx）小于30 Mbps，说明该终端的建链速率低。
  - 通过**命令display station statistics sta-mac** *sta-mac*查看该终端下的统计。

```
<WAC> display station statistics sta-mac 14cf-9208-9abf
-------------------------------------------------------------------------
  Packets sent to the station                          : 7
  Packets received from the station                    : 40
  Bytes sent to the station                            : 1170
  Bytes received from the station                      : 3911
  Wireless data rate sent to the station(kbps)         : 0
  Wireless data rate received from the station(kbps) : 0
......
```

  - 一般认为，如果终端流量超过10 M，说明该终端在进行大流量业务。具体还需要结合实际网络情况来判断。

HUAWEI

- 为保证其它终端能够正常上网，可以通过如下方法进行处理：
  - 对单个终端进行限速，具体的限制速率请结合实际网络情况来配置。
    - [WAC-wlan-view] **traffic-profile name** *p1*
    - [WAC-wlan-traffic-prof-p1] **rate-limit client up** *2000*
    - [WAC-wlan-traffic-prof-p1] **rate-limit client down** *2000*
  - 开启智能漫游功能。
    - [WAC-wlan-view] **rrm-profile name** *wlan-rrm*
    - [WAC-wlan-rrm-prof-wlan-rrm] **smart-roam enable** //从V200R008版本开始，智能漫游功能默认是开启的，如被关闭，可以执行命令**undo smart-roam disable**开启。

STA网速慢排查技巧 - 检查中间设备是否存在ARP丢包

- 如果中间设备ARP丢包严重，会导致通信双方无法及时学习到对方的ARP表项，出现网络时通时断的异常情况。
  - 在中间设备（如交换机）上执行命令display cpu-defend statistics wired，检查中间设备ARP CPCAR丢包情况。

```
<LSW> display cpu-defend statistics wired
-------------------------------------------------------------------------------
Packet Type              Pass Packets        Drop Packets
-------------------------------------------------------------------------------
8021X                    0                   0
arp-miss                 0                   0
arp-reply                0                   0
arp-request              6                   0
Capwap                   0                   0
capwap-association       0                   0
capwap-discovery         0                   0
capwap-echo              0                   0
capwap-keepalive         0                   0
dhcp-client              0                   0
```

  - 如果ARP Request包的丢包率超过50%，说明该中间设备ARP丢包严重。
- 解决方法：
  - 在设备当前CPU利用率不高的情况下，可以增大ARP Request报文上送CPU的限制速率。
  - 配置攻击溯源功能，避免网络中有终端存在ARP泛洪攻击行为。

STA网速慢排查技巧 – 解决中间设备是否存在ARP丢包

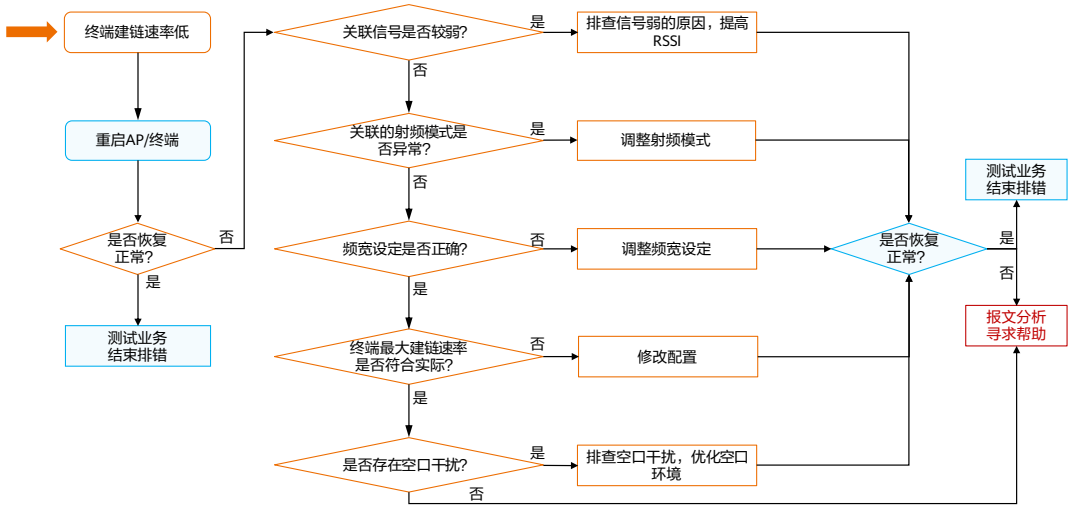
- 增大ARP Request报文上送CPU的限制速率。

```
<LSW> system-view
[LSW] cpu-defend policy test                                          //创建策略
[LSW-cpu-defend-policy-test] packet-type arp-request rate-limit 256 wired   //调整ARP Request报文的限制速率
[LSW-cpu-defend-policy-test] quit                                     //应用策略
[LSW] cpu-defend-policy test
```

- 配置攻击溯源功能。

```
[LSW] cpu-defend policy test
[LSW-cpu-defend-policy-test] auto-defend protocol arp                 //设置攻击溯源检查阈值为50pps，如果超过该阈值，则认为被攻击。
[LSW-cpu-defend-policy-test] auto-defend threshold 50
[LSW-cpu-defend-policy-test] auto-defend action deny timer 60         //检测到攻击后，直接丢弃报文并将终端加入黑名单60s。
[LSW-cpu-defend-policy-test] quit
[LSW] cpu-defend-policy test                                          //应用策略
```

STA建链速率低排查流程



STA建链速率低排查技巧 - 查看STA关联的信号强度

- AP射频的发射功率过低、终端离AP较远、终端与AP天线间有遮挡等因素都会影响终端关联信号的强度。
  - 在WAC上执行命令**display station all | include** *mac-address*，查看终端的RSSI和协商速率。

```
<WAC> display station all | include cc3d-828a-bfec
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------------------------------------
STA MAC          AP ID  AP name  Rf/WLAN  Band  Type    Rx/Tx     RSSI  VLAN  IP address    SSID
--------------------------------------------------------------------------------------------------------------
cc3d-828a-bfec  25       ap1        0/1      2.4G  11n     123/98    -46    500   10.1.1.253    r6c10-test
--------------------------------------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0
```

  - 命令行中显示的RX值和终端上显示速率在一个数量级上，可能会有小的差异。
  - 如果终端关联的RSSI值小于-75dBm，请尝试如下处理：
    - 调整AP发射功率：在WAC上执行命令**display radio ap-id** *ap-id*，查看AP射频的发射功率是否为最大功率。
    - 如果AP射频的发射功率不是最大功率，请在WAC上执行命令**eirp** *eirp*，调整AP射频的发射功率为最大值，使终端关联时RSSI变大。

- 检查终端与AP天线间的距离是否过远，以及终端与AP天线间是否有遮挡。
- 一般终端与AP天线间的距离大于50 m认为比较远，会造成无线传播损耗过大；终端与AP天线之间如果有遮挡，会造成终端检测到的AP信号较弱。
- 如果有上述原因造成RSSI过低，可以通过移动终端位置等方法，使终端关联时RSSI变大，一般建议在-65 dBm以上。

STA建链速率低排查技巧 - 查看终端关联的详细信息

- 终端关联的射频模式、AP配置的加密方式、终端支持的空间流、配置的频宽都与协商速率有必然联系，需要查看终端关联后这些指标信息。

```
[WAC-wlan-view] display station sta-mac cc3d-828a-bfec
--------------------------------------------------------------------------------
Station MAC-address                    : cc3d-828a-bfec
Station IP-address                     : 10.1.1.253
Station gateway                        : 10.1.1.1
Associated SSID                        : r6c10-test
Station online time(ddd:hh:mm:ss)      : 000:06:30:19
......
Station's radio mode                   : 11ax
Station's AP Name                      : cc53-b5ee-39e0
Station's Radio ID                     : 0
Station's Authentication Method        : WPA2-PSK
Station's Cipher Type                  : AES
Station's User Name                    : cc3d828abfec
Station's Vlan ID                      : 500
Station's Channel Band-width           : 160MHz
Station's asso BSSID                   : cc53-b5ee-39e0
Station's state                        : Asso with auth
Station's QoS Mode                     : WMM
Station's HT Mode                      : HT160
Station's MCS value                    : 15
Station's Short GI                     : nonsupport
......
```

STA建链速率低排查技巧 - 检查射频模式和频宽设定是否正确

- 检查AP是否配置了固定的终端关联射频模式。
- 查看Station's radio mode字段。如果AP配置了固定的终端关联射频模式，请按如下方法恢复终端关联射频模式为缺省模式，即2.4G频段下为802.11b/g/n/ax模式，5G频段下为802.11n/ac/ax模式。

```
[WAC-wlan-view] radio-2g-profile name huawei
[WAC-wlan-radio-2g-prof-huawei] display this
#
  radio-type dot11ax
[WAC-wlan-radio-2g-prof-huawei] undo radio-type
[WAC-wlan-radio-2g-prof-huawei] quit
```

- 如果终端已达到配置频宽的最大建链速率，可以修改频宽，以达到下一个频宽的建链速率。
  - 查看Station's Channel Band-width和Station's HT Mode字段。如果配置的终端频宽不合理，请按如下方式修改终端频宽。例如，支持802.11ac的终端，建议配置频宽为80mhz。

```
[WAC-wlan-view] ap-id 25
[WAC-wlan-ap-25] radio 1
[WAC-wlan-radio-25/1] channel 160mhz 149
```

  - 由于空口干扰等因素，终端实际建链速率可能低于最大建链速率。
  - 如果终端和AP都支持802.11ax协议，可以配置160mhz的频宽。
  - 配置频宽时，需要配置AP支持的频宽，比如非11ax的AP不支持配置160mhz的频宽等。

STA建链速率低排查技巧 - 检查终端是否处在节电状态

- 当终端处于节电状态时，发包时延会增加，时延大小在正常情况下和Beacon间隔的配置相关，Beacon间隔配置越低则时延越小，反之时延越大。

```
<WAC> display station sta-mac 482c-a042-8227
--------------------------------------------------------------------------------
Station MAC-address                  : 482c-a042-8227
Station IP-address                   : FE80::D287:F82B:9D2C:827C
                                     : 10.10.10.49
Station gateway                      : 10.10.10.1
Associated SSID                      : Huawei
Station online time(ddd:hh:mm:ss)    : 000:00:03:36
......
Station current state
......
 Power save mode enabled             : YES
```

STA建链速率低排查技巧 - 查看空口是否存在干扰

- 终端与AP协商的速率受空口环境的影响，当空口干扰比较大时，协商速率会降低，显示速率也会比较低。
- 在WAC上查看AP的信道利用率来判断空口干扰程度。

```
[WAC-wlan-view] display radio ap-id 25
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
--------------------------------------------------------------------------------
AP ID    Name    RfID  Band  Type   Status  CH/BW     CE/ME   STA    CU
--------------------------------------------------------------------------------
25       ap1     0     2.4G  11ax   on        8/20M   29/29   1      21%
25       ap1     1     5G    11ax   on      165/20M   23/30   0      4%
--------------------------------------------------------------------------------
Total:2
```

STA建链速率低排查技巧 - 查询空口环境的干扰

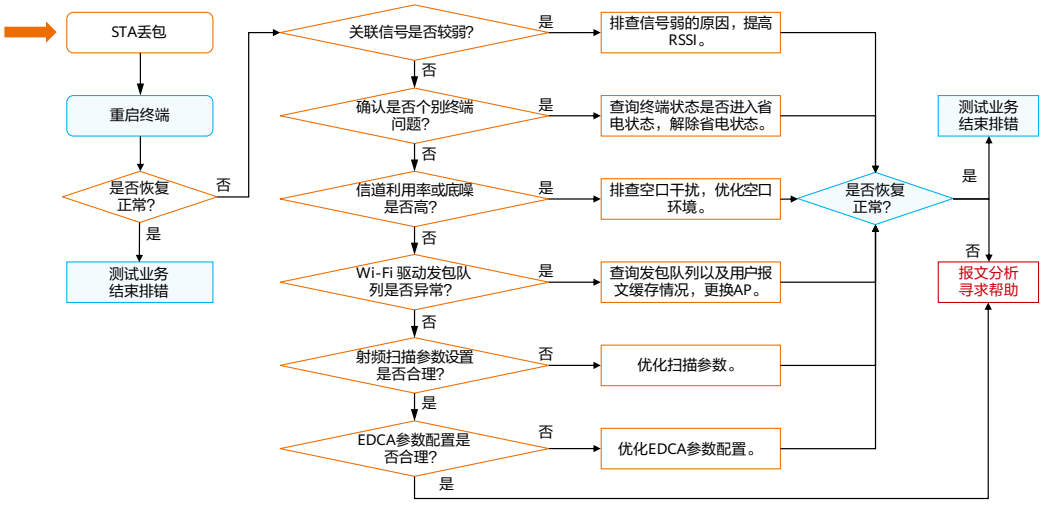
- 如果查询到AP的信道利用率大于50%，则信道利用率比较高，空口干扰比较大。
- 根据查询到的当前各信道干扰设备的个数及强度，可以判断各个信道的优劣。

```
<WAC> display ap radio-environment ap-id 13 radio 0
Info: This operation may take a few seconds. Please wait for a moment.done.
......
Radio:                  0
ScanChannel:            1
WorkChannel:            1
ScanCycle:              1
--------------------------------------------------------------------------------
Ch      NF      CU(%)   CommIf(%) AdjaceIf(%) SINR    #APs
--------------------------------------------------------------------------------
1       -105    75      19        -           245     57
......
--------------------------------------------------------------------------------
Total: 13
--------------------------------------------------------------------------------
Ch      MAC                 Type    RSSI    SSID
--------------------------------------------------------------------------------
1       c88d-833a-8d41      I       -65     Huawei
......
--------------------------------------------------
Total: 177
```


HUAWEI

- p: permit
- i: interference
- Ch: Channel
- NF: Noise Floor
- CommIf: Common-Channel Interference
- AdjaceIf: Adjacent-Channel Interference
- #AP: Number of APs detected
- 首次查询时没有空口环境扫描结果显示，需要再次执行该命令。
- 执行此命令，AP射频的扫描开关开启后，会对AP空口性能有一定影响。命令执行五分钟后，如果期间没有重复执行命令，则AP射频的扫描开关会自动关闭。
- 不指定参数radio radio-id时，查询的是AP上所有射频的空口环境信息。

STA丢包故障排查流程



STA丢包故障排查技巧 - 确认ping包在Wi-Fi无线侧收发正常

- WAC诊断视图下开启基于用户的station-trace功能，进行ping包测试，确认ping包在Wi-Fi无线侧收发是否正常。
  - 开启station-trace功能。

    ```
    [WAC-diagnose] station-trace sta-mac 482c-a042-8227
    ```

  - 进行ping包测试。

    ```
    <7>Aug 11 2020 15:02:30.0.1 0032-4516-4100 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f72d-6365):SeqNo[10] [ICMP] Ping request from
    [192.168.110.2] to [192.168.110.214] id[44094] seq[1] payload[56] Receive from fwd
    <7>Aug 11 2020 15:02:30.40.1 0032-4516-4100 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f72d-6365):SeqNo[10] [ICMP] Ping request from
    [192.168.110.2] to [192.168.110.214] id[44094] seq[1] payload[56] elapsed[23 ms] send to rt ok format :1 seqType:6 eof:0 total_mpdu_num:0
    <7>Aug 11 2020 15:02:30.40.2 0032-4516-4100 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f72d-6365):SeqNo[10] [ICMP] Ping request from
    [192.168.110.2] to [192.168.110.214] id[44094] seq[1] payload[56] elapsed[23 ms] send to air ok
    <7>Aug 11 2020 15:02:30.40.3 0032-4516-4100 WSRV/7/BTRACE:(BTRACE)(WLAN_AP)(94e6-f72d-6365):SeqNo[9] [ICMP] Ping reply from
    [192.168.110.214] to [192.168.110.2] id[44094] seq[1] payload[56] send to np ok
    ```

- 如果信息中没有出现Receive from fwd，则说明ping request报文没有从转发模块发送到WiFi模块，此时有线侧出现问题的可能性比较大。
- 如果信息中出现Receive from fwd打印，但是没有出现send to air ok，则说明WiFi模块没有成功将报文发送给用户，问题出现在无线侧。
- 如果信息中出现send to np ok，则说明用户已经回应了ping response报文，并上送到转发模块，此时有线侧出现问题的可能性比较大。
- 如果信息中确认ping request报文已经成功发给用户，但是没有出现send to np ok打印，则说明问题出现在无线侧。

- SeqNo[xxx]：表示该ping包内携带的序列号，通过该序列号可以将trace和某个具体ping报文对应起来。
- Receive from fwd：表示Wi-Fi侧收到转发侧发给用户的ping request报文。
- send to rt ok：表示Wi-Fi侧PMAC模块成功将ping request报文发送给SMAC模块。
- send to air ok：表示Wi-Fi侧成功将ping request报文通过空口发送给用户。
- send to np ok：表示Wi-Fi将ping response报文成功送到转发侧，后面将会由转发侧处理，并通过AP网口送到有线侧网络设备。
- send to air fail, reason code: 0：表示接收响应帧超时了，需要进一步分析。

STA丢包故障排查技巧 - 确认终端的信号强度以及建链速率

- WAC上通过命令行查询终端关联信息，确认AP接收到终端的信号强度以及建链速率是否合理。

```
[WAC-wlan-view] display station sta-mac 8844-7748-3c81
------------------------------------------------------------------------------
Station MAC-address                     : 8844-7748-3c81
Station IP-address                      : 192.168.150.162
Station gateway                         : 192.168.150.1
Associated SSID                         : WLAN-TEST
Station online time(ddd:hh:mm:ss)       : 000:00:00:57
The upstream SNR(dB)                    : 44.0          //信号强度
The upstream aggregate receive power(dBm) : -51.0
Station connect rate(Mbps)              : 58            //建链速率
.....
```

- 如果信号强度或建链速率很低，均可能会导致丢包。正常办公场景下，要求信号强度不低于-70dBm，建链速率不低于13Mbps，如果低于该水平，则需进行排查以及优化。
  - 首先确认终端所在位置AP部署是否合理，是否存在盲区，如果存在的话，则需要增加AP进行补盲。
  - 如果不存在盲区，则查看STA是否接入到离其较远的AP，如果是，可通过如下配置进行优化：
    - 如果当前终端接入的远端AP发射功率过高，可以进入AP视图下进行发射功率微调。
    - 配置强制低RSSI用户下线功能。

HUAWEI

- 发射功率微调。

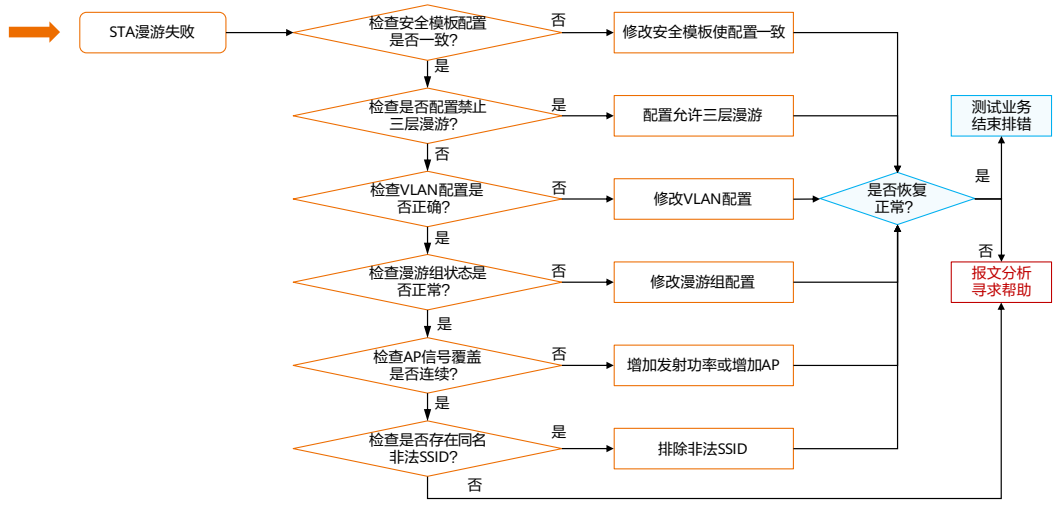
```
[WAC-wlan-view] ap-id 19
[WAC-wlan-ap-19] radio 1
[WAC-wlan-radio-19/1] eirp 20
[WAC-wlan-radio-19/1] display this
#
 vap-profile test2 wlan 1
 vap-profile test4 wlan 2
 channel 160mhz 149
 eirp 20
#
```

- 具体调整多少，需要进行实际测试，可以在满足覆盖的基础上尽量往下调整，调整时建议将附近区域的AP根据情况进行同步调整。
- 配置强制低RSSI用户下线功能。

```
[WAC-wlan-view] rrm-profile name default
[WAC-wlan-rrm-prof-default] smart-roam enable //从V200R008C10版本开始，智能漫游及快速强制用户下线功能默认开启
[WAC-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold snr 20
```

- 配置的阈值需要根据网络覆盖情况进行适当调整，比如AP部署较密的区域，建议配置较高阈值，反之建议配置较低阈值。

STA漫游失败排查流程



STA漫游故障排查技巧 - 检查安全模板配置和三层漫游功能

- 进入安全模板视图重新配置密钥，保证漫游前后AP的安全模板配置一致。

```
[WAC-wlan-view] security-profile name default
[WAC-wlan-sec-prof-default] security wpa2 psk pass-phrase huawei123 aes
```

- 检查是否配置了禁止三层漫游。

```
[WAC] display vap-profile name default
--------------------------------------------------------------------------------
......
Service VLAN ID          : 101
Service VLAN Pool        : -
Permit VLAN ID           : -
Auto off service switch  : disable
Auto off starttime       : -
Auto off endtime         : -
STA access mode          : disable
STA blacklist profile    :
STA whitelist profile    :
Home agent               : ap
VLAN mobility group      : 2
Layer3 roam              : enable
......
```

- 可根据业务需要决定是否禁止三层漫游，执行undo layer3-roam disable命令可取消禁止三层漫游。

```
[WAC-wlan-vap-prof-default] undo layer3-roam disable
```

STA漫游故障排查技巧 - 检查漫游组状态是否正常

- 在Master Controller AC上执行命令**display mobility-group**查询漫游组成员状态是否normal，如果漫游组成员状态不是normal，则会导致AC间漫游失败。

```
<WAC> display mobility-group name roam
--------------------------------------------------------------------------------
AC ID           State          IP address
--------------------------------------------------------------------------------
1               Normal         192.168.10.3
2               Fault          192.168.10.4
--------------------------------------------------------------------------------
```

- 如果漫游组成员状态是"fault"，查看当前漫游组的配置信息是否正确。

```
[WAC] mobility-group name mobility
[WAC-mc-mg-mobility] display this
#
  member ip-address 192.168.10.1
  member ip-address 192.168.10.2
#
```

STA漫游故障排查技巧 - 检查功率配置是否合理

- 如果功率配置过小，容易造成信号覆盖盲点。此时，需要在射频视图下执行eirp命令增大发射功率。
- 如果功率配置过大（如满功率），容易导致终端关联远端AP而出现漫游不灵敏。此时，需要在射频视图下执行**eirp**命令适当降低发射功率或者配置智能漫游功能。

<WAC> **display radio ap-id** *25*
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization

AP ID	Name	RfID	Band	Type	Status	CH/BW	CE/ME	STA	CU
25	ap-yuan	0	2.4G	bgn	on	8/20M	29/29	1	21%
25	ap-yuan	1	5G	an11ac	on	165/20M	23/30	0	4%

Total:2

STA漫游故障排查技巧 - 检查周边是否存在同名的非法SSID

- 确定发生漫游失败问题的AP ID后， 在AC上执行命令**display ap neighbor ap-id** *ap-id* , 查看Uncontrol AP中是否存在同名的非法SSID。如果存在则需要关闭此非法SSID信号。

<WAC> **display ap neighbor ap-id** *0*
Radio: Radio ID of AP
.....
Uncontrol AP:

Radio	BSSID	Channel	RSSI(dBm)	Last Update Time	SSID
0	d0d0-4b22-df00	1	-50	2019-08-24/15:32:18	
0	c4b8-b4f0-6980	1	-44	2019-08-24/15:31:06	
0	**10c1-72dd-12e0**	**11**	**-41**	**2019-08-24/15:28:27**	**test**
0	9c50-ee45-6240	1	-54	2019-08-24/15:32:06	

Total: 4

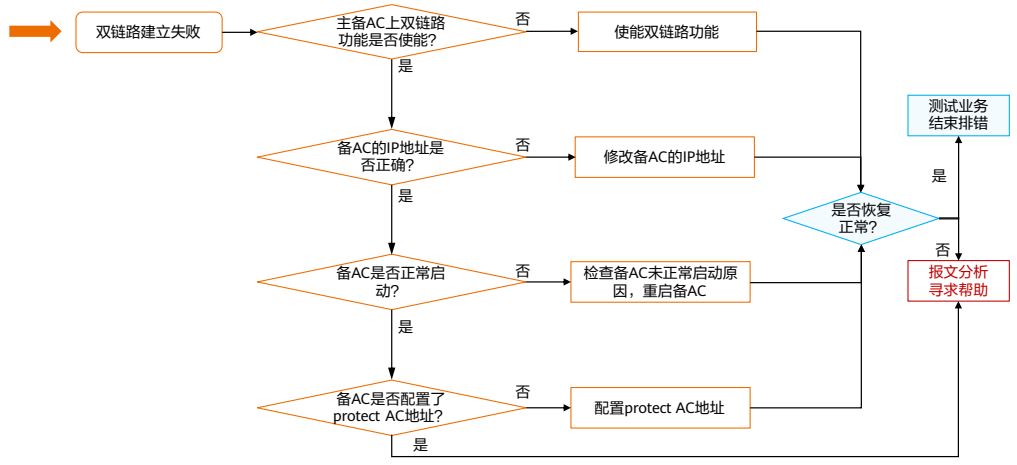
STA漫游故障排查技巧 - 信息收集

- 将终端在两个AP间移动，执行命令**display station roam-track**查看终端的漫游轨迹，如果漫游轨迹显示正常则问题解决，如果仍然漫游失败，请收集漫游时系统的日志和诊断日志并收集如下故障诊断信息，然后寻求技术支持。

命令	使用说明
[WAC] **trace enable** [WAC] **trace object mac-address**	查看STA上线或者漫游全流程跟踪信息。
[WAC] **display station online-fail-record** [WAC] **display station offline-record**	查看用户上线失败或下线原因。
[WAC-diagnose] **display wlan wsta block-sta-number all** [WAC-diagnose] **display wlan wsta online-statistics** [WAC-diagnose] **display wlan wsta online-fail-record by-mac** [WAC-diagnose] **display wlan wsta peak-statistics**	查看用户上线失败或下线原因码。
[WAC-diagnose] **display diagnostic-information**	获取系统的一键诊断信息，该信息包括版本、补丁版本、当前配置和已保存配置 、异常、部分日志等。

WLAN可靠性问题

AC双链路建立失败排查流程



HUAWEI

AC双链路建立失败 - 检查主备AC上双链路开关和源IP地址

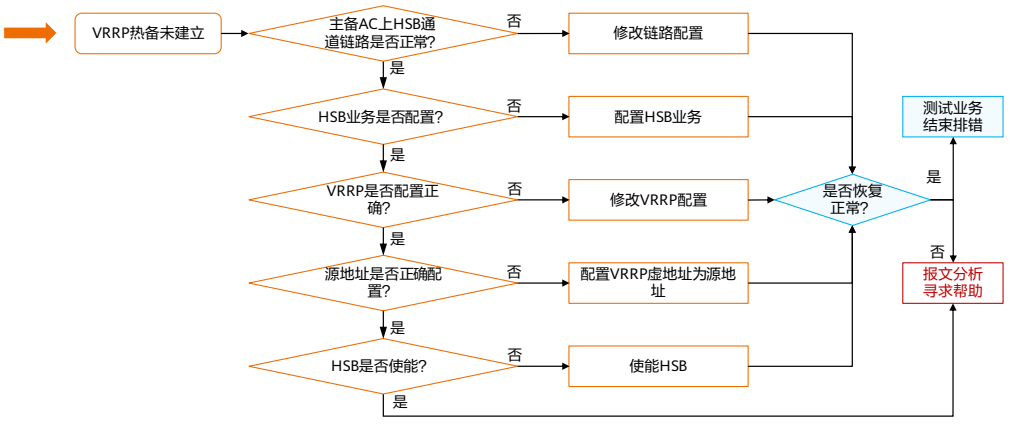
- 在主备AC上执行display ac protect命令，查看配置中双链路功能是否使能，如果未使能，请执行ac protect enable命令开启双链路功能。

```
[WAC] display ac protect
------------------------------------------------------------------
Protect state                 : disable
Protect AC                    : -
Priority                      : 0
Protect restore               : enable
Coldbackup kickoff station: disable
------------------------------------------------------------------
```

- 在备AC上执行**display capwap configuration**命令，如果源地址为IP地址，则直接显示；如果为VLANIF，则查看对应的VLANIF地址。

```
[WAC] display capwap configuration
  ------------------------------------------------------------------
  Source interface                                : -
  Source ip-address                               : 10.1.1.111
  Echo interval(seconds)                          : 25
  Echo times                                      : 6
  Control priority(server to client)              : 7
  Control priority(client to server)              : 7
  Control-link DTLS encrypt                       : disable
  DTLS PSK value                                  : ******
  PSK mandatroy match switch                      : enable
  Control-link inter-controller DTLS encrypt      : disable
  Inter-controller DTLS PSK value                 : ******
  IPv6 status                                     : disable
```

VRRP热备故障排查流程



HUAWEI

VRRP热备故障排查技巧 - 检查主备AC的HSB通道是否正常

- 登录主AC，查看主备AC之间的链路是否畅通。
- 执行display hsb-service 0命令查看链路状态是否为Connected。Connected表示链路畅通，Disconnected表示链路已断开，需检查链路使其恢复Connected状态。

```
[WAC] display hsb-service 0
Hot Standby Service Information:
-------------------------------------------------------------------
  Local IP Address          : 10.1.1.1
  Peer IP Address           : 10.1.1.2
  Source Port               : 10241
  Destination Port          : 10242
  Keep Alive Times          : 5
  Keep Alive Interval       : 2
  Service State             : Connected
  Service Batch Modules     :
-------------------------------------------------------------------
```

VRRP热备故障排查技巧 - 检查VRRP虚地址和CAPWAP源地址

- 分别登录主备AC，查看VRRP状态和虚地址。

```
[WAC] display vrrp brief
Total:1    Master:1    Backup:0    Non-active:0
VRID       State        Interface      Type         Virtual IP
------------------------------------------------------------------------------
2          Master       Vlanif1360     Normal       10.1.1.6
```

- 检查CAPWAP源地址是否配置正确。

```
[WAC] display capwap configuration
  ------------------------------------------------------------------
  Source interface                                : -
  Source ip-address                               : 10.1.1.111
  Echo interval(seconds)                          : 25
  Echo times                                      : 6
......
```

- 发现地址错误，需在AC上修改CAPWAP源地址为VRRP虚地址。

VRRP热备故障排查技巧 - 收集信息

命令	功能
<WAC> **display hsb statistics hsb-group 0 event** <WAC> **display hsb statistics hsb-service 0 event**	进入用户视图，收集hsb event信息，将控制台打印的信息收集起来。
<WAC> **display hsb statistics hsb-service 0 packet**	进入用户视图，收集hsb packet信息，将控制台打印的信息收集起来。
[WAC-diagnose] **display wlan debuginfo type** *1* **from** *0* **to** *1000*	进入用户视图，收集WDEV日志信息，将控制台打印的信息收集起来。
[WAC-diagnose] **display wlan debuginfo type** *8* **from** *0* **to** *1000*	进入用户视图，收集WSRV日志信息，将控制台打印的信息收集起来。
<WAC> **save logfile**	保存诊断日志
[WAC-diagnose] **info-center create logbook xx.xml**	创建诊断日志的字典文件
[WAC-diagnose] **display wlan wsrv backup elmt** *1000*	进入诊断视图，查看指定模块备份处理信息，包括序列化、反序列化和处理的统计信息。

疑难故障处理 - 报文分析

- 当出现未知原因导致网络故障，报文分析是一种有效的辅助手段，来定位故障根因。
- 现网问题具有突发性、个体性、时效性等特点，只有实时采集现网报文并进行报文分析才可能定位出故障的根本原因。

有线网络报文

通过网线直连抓包，获取设备通过网线传输的报文。

普通网络互通问题，AP上线失败，STA上线失败，认证失败等等问题均可通过有线报文分析来定位故障。

无线网络报文

通过特定网卡空口抓包，获取无线交互报文。

无线环境干扰、无线攻击、非法AP、无线报文协商异常、AP信号异常、STA上线故障等问题均可通过无线报文分析来定位故障。

目录

CloudCampus APP

- 网络质量诊断：
  - CloudCampus APP的Wi-Fi体检功能，能够协助工程师，尽快定位WLAN网络存在的故障，并提供一定的解决方案参考，非常实用。

iMaster NCE-Campus

- iMaster NCE-Campus集成了网络管理功能，能够高效管理全网设备，一旦发生任何故障，会自动检测且第一时间产生告警，并提示故障原因，协助工程师高效进行故障排查。

CampusInsight：个障分析 & 群障分析

- 园区网络运维过程中，管理员遇到的问题主要分为两类：
  - 个体性问题：比如终端配置错误导致的个体接入失败等。
  - 群体性问题：比如认证服务器问题导致的批量认证失败，AP覆盖不足导致的批量用户信号强度差等。

个体性问题解决方案

1、每指标：秒级数据采集&异常检测。

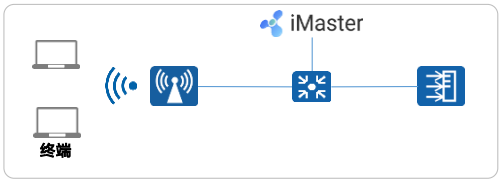
2、每用户：协议级接入过程分析、全旅程回放&体验分析、音视频应用质量感知。

群体性问题解决方案

三大类问题识别：智能识别连接类、空口性能类、漫游类问题。

有线网络报文分析案例 - 故障背景

- 案例场景：
  - 如图所示WLAN组网，客户使用Portal认证，客户端接入网络网络时，正常弹出Portal页面，也提示认证成功，但是终端没有获取任何权限，无法访问网络。
- 故障分析：
  - Portal页面正常弹出，也出现了认证成功的提示，说明Portal认证数据交互正常，仅仅是授权出现了问题，应该排查授权模板的相关配置。
  - 排查授权模板，但没有发现任何错误配置。
  - 此案例并不符合Portal认证失败的案例情况，为节省时间，此时可以抓包查看报文协商情况，来判断具体是什么原因导致。



有线网络报文分析案例 - 报文分析

- 通过报文捕获，得到了WAC与Portal服务器之间的交互报文，Portal认证交互过程如下：

No.	时间	源地址	目的地址	协议	长度	信息
232	50.674904	192.168.20.1	192.168.1.199	PORTAL	60	PORTAL REQ_CHALLENGE
949	60.682857	192.168.20.1	192.168.1.199	PORTAL	60	PORTAL REQ_LOGOUT
.....						
➢ Frame 949: 60 bytes on write (480 bits), 60 bytes captured (480 bits) on interface 0						
➢ Ethernet Ⅱ, Src: HuaweiTe_87:8b:4f (48:46:fb:87:8b:4F), Dst: HuaweiTe_53:d8:d6 (58:60:5f:53:d8:d6)						
Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.1.199						
➢ User Datagram Protocol, Src Port: 65165 (65165), Dst Port: 2000 (2000)						
➢ Portal Proto						
Versoin: Portal Ver1 (1)						
MsgType: REQ_LOGOUT						
AuthType: CHAP (0)						
.....						
UserIP: 192.168.100.254						
UserPort: 0						
ErrCode: 1 //Errcode为1，即为超时，即设备没有给出回应，需进一步分析没有回应的原因。						
.....						

有线网络报文分析案例 - debug日志分析

- 通过报文分析可以直观看到，有个错误代码1，代表的是设备没有回应挑战报文，需定位没有回应的原因。
- Debug Portal报文：

```
<WAC> debugging web all
<WAC>
Jan 16 2021 10:38:56. 950. 2+08:00 192.168.1.199 WEB/7/DEBUG:
Received packet from socket  (length = 32 Vrf = 0)
Version                 : 2
Type                    : challenge request
Method                  : chap
SeriaNo                 : 25927
RequestID               : 0
UserIP                  : 192.168.100.254
......

<WAC>
Jan 16 2021 10:38:56. 950. 2+08:00 192.168.1.199 WEB/7/DEBUG:
[Web-Err] Web check md5 failed.
<WAC>
Jan 16 2021 10:38:56. 950. 5+08:00 192.168.1.199 WEB/7/DEBUG:
[Web-Err] The shared-key configured on the device must be the same as the one configured  on the portal server.
```

- Debug的报文提示，MD5校验失败，可能是预共享密钥不正确。
- 但重新配置密钥，故障现象并没有解除。

有线网络报文分析案例 - debug日志与报文对比

- 结合报文和debug日志，发现有一个参数不同，Portal服务器上报文的Portal协议版本号是1，但是在WAC上提示的Portal协议版本号是2。

➢ **Portal Proto**
Versoin: Portal Ver1 (1)　//Portal协议共有3个版本：1.0、2.0、9.0，其中V9.0为内部Portal协议。
MsgType: REQ_LOGOUT
AuthType: CHAP (0)
.....

```
<WAC>
Jan 16 2021 10:38:56. 950. 2+08:00 192.168.1.199 WEB/7/DEBUG:
Received packet from socket  (length = 32 Vrf = 0)
Version                 : 2
Type                    : challenge request
Method                  : chap
SeriaNo                 : 25927
RequestID               : 0
UserIP                  : 192.168.100.254
.....
```

- 修改Portal协议版本，问题解决。
- 结论：
  - 较为复杂的故障排查，可以通过报文捕获来获取报文协商过程中的信息，并结合日志、表项等信息，来帮助定位故障根因。

空口报文分析

- WLAN网络介质的特殊性导致仅仅网口抓包不足以解决全部故障，工程师还需掌握对空口报文进行捕获以及分析的能力。
- 在空口报文分析前，工程师需要掌握进行空口报文捕获和分析，可以解决什么问题。

按STA上线过程分析

01 → 阶段1：网络发现，不进行网络探测
报文：无

02 → 阶段2：有探测，但不关联。
报文：Probe

03 → 阶段3：关联失败
报文： Probe, authentication, association

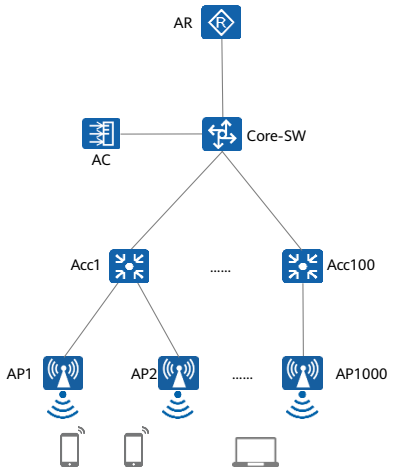
04 → 阶段4：认证失败
报文：Probe, authentication, association, PSK/EAP

05 → 阶段5：DHCP失败
报文：Probe, authentication, association, EAP, KEY, DHCP

06 阶段6：传输数据、漫游以及休眠等
报文：Probe, authentication, reassociation, PMK, 11r, data

空口报文分析案例 - 故障背景

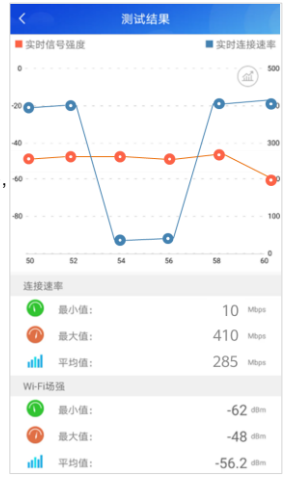
- 案例背景：某WLAN项目已完成部署，但在进行WLAN网络稳定性测试时发现，PC网络速率每过10分钟都会下降到10Mbps左右，间隔2~5s后网速恢复正常，但使用手机却没有该问题。
- 初步分析，WLAN网络正常，但出现网络速率波动，且呈现的比较规律，可能故障点：
  - 空口环境干扰，需排查现场是否有规律开启的大功率无线设备。
  - 信号强度不稳定，需进行信号故障排查。
  - PC端网卡故障。



空口报文分析案例 - 故障分析

- 初步排查：
  - 空口环境正常，并无大功率无线设备，且底噪正常。
  - 信号强度有所波动，但在正常波动范围，且信号波动并未对网速造成影响。
  - 仍需确定是否是PC端网卡故障或者兼容性问题引起。
- 空口抓包：
  - 在空口捕获无线报文，分析速率骤降时间点无线报文情况，发现是PC网卡进入了省电模式，禁用网卡再启用网卡，使PC网卡退出省电模式，故障恢复。

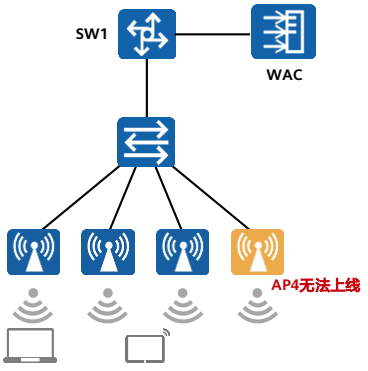
➢ **802.11 MAC Header**	
Version	: 0 [0 Mask 0x03]
Type	: %10 Data [0 Mask 0x0C]
Subtype	: %1100 QoS Null (No Data) [0 Mask 0xF0]
– **Frame Control Flags**	**: %00010001 [1]**
	0... .... Non-strict order
	.0.. .... Non-Protected Frame
	..0. .... No More Data
	...1 .... Power Management – power save mode
	.....



目录

案例1：AP上线失败

- 案例背景：某公司网络中有1台WAC，2台交换机，以及4台AP。其中DHCP地址池部署在核心交换机SW1上，WLAN组网为三层旁挂组网，转发模式为直接转发，在设备调测过程中发现AP4无法正常上线，需排查该故障。



案例1：AP上线失败故障排查 - 检查AP状态

- 分析过程：第一步，登陆WAC设备，通过命令：display ap all查看当前WAC上AP的运行情况。

```
[WAC-wlan-view]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
fault: fault            [1]
nor  : normal           [3]
--------------------------------------------------------------------------------
ID   MAC            Name Group   IP          Type            State STA Uptime
--------------------------------------------------------------------------------
0    00e0-fc97-6b20 ap1  default 10.1.1.250 AP8130DN-W      nor   0   3M:3S
1    00e0-fcb0-0610 ap2  default 10.1.1.251 AP8130DN-W      nor   0   2M:56S
2    00e0-fc0d-6a60 ap3  default 10.1.1.253 AP8130DN-W      nor   0   2M:38S
3    00e0-fc61-22c0 ap4  default -           AP8130DN-W      fault 0   -
--------------------------------------------------------------------------------
Total: 4
```

- 发现ap4处于fault状态，则应该查看AP是否获取到IP地址。

案例1：AP上线失败故障排查 - 检查AP的IP地址及路由可达性

- 由于DHCP服务器在核心交换机上，则在核心交换机上查看IP地址分配情况。

```
<SW1>display ip pool name ap used | in 00e0-fc61-22c0
 ------------------------------------------------------------------------------
  Network section :
  ------------------------------------------------------------------------------
  Index            IP               MAC               Lease   Status
  ------------------------------------------------------------------------------
   251      10.1.1.252    00e0-fc61-22c0       192      Used
  ------------------------------------------------------------------------------
```

- 可以看到AP是正常获取到了IP地址的，在WAC上用CAPWAP源地址去访问AP的地址：

```
<WAC>ping -a 10.1.1.254 10.1.1.252
  PING 10.1.1.252: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.252: bytes=56 Sequence=1 ttl=255 time=60 ms
    Reply from 10.1.1.252: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 10.1.1.252: bytes=56 Sequence=3 ttl=255 time=60 ms
    Reply from 10.1.1.252: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.1.1.252: bytes=56 Sequence=5 ttl=255 time=40 ms

  --- 10.1.1.252 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    00.00% packet loss
    round-trip min/avg/max = 40/52/60 ms
```

- 能够正常访问，则需关注是否WAC的licence不足导致AP无法上线。

案例1：AP上线失败故障排查 - 检查AP的licence及交互报文

```
<WAC> display license resource usage
 Activated License: -
 FeatureName    | ConfigureItemName      | ResourceUsage

 CRFEA1          LH85WLANAP01             3/256
<WAC>
```

- 可以看到WAC上有充足的licence资源，可以获取AP与WAC的交互报文来帮助分析。
- 查看AP与WAC的交互报文。

No.	时间	源地址	目的地址	协议	长度	信息
1868	1258.579000	10.1.1.252	255.255.255.255	CAPWAP-Control	397	CAPWAP-Control - Discovery Request
1935	50.682857	10.1.1.252	255.255.255.255	CAPWAP-Control	397	CAPWAP-Control - Discovery Request
1996	53.838915	10.1.1.252	255.255.255.255	CAPWAP-Control	397	CAPWAP-Control - Discovery Request
2069	103.467834	10.1.1.252	255.255.255.255	CAPWAP-Control	397	CAPWAP-Control - Discovery Request

- 可以看到，AP获取到10.1.1.252的IP地址后，一直在寻找WAC，WAC也收到了discovery request报文，但是没有回复，说明直接丢弃了该报文，可能是WAC上的策略导致了该故障的产生。

案例1：AP上线失败故障排查 - 检查AP的流策略及WLAN策略

- 查看WAC上的流策略信息及ACL。

```
<WAC> display traffic policy
<WAC>
<WAC> display acl all
 Total quantity of nonempty ACL number is 0
<WAC>
```

- 没有发现任何流策略的配置，继续查看WLAN的策略。

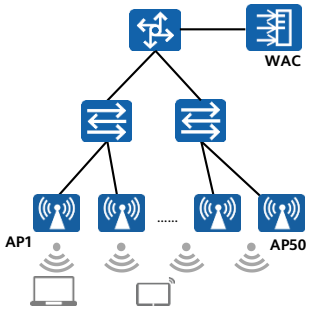
```
<WAC> display ap blacklist
------------------------------------------------------------------------------
ID     MAC
------------------------------------------------------------------------------
0      00e0-fc61-22c0
------------------------------------------------------------------------------
Total: 1
```

- 发现原来在WAC上配置了静态AP黑名单，去掉该黑名单设置后，AP4也正常上线了。

```
[WAC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment. Done.
-------------------------------------------------------------------------------------------------
ID   MAC             Name      Group   IP          Type          State  STA Uptime
-------------------------------------------------------------------------------------------------
3    00e0-fc61-22c0  ap4       default 10.1.1.252  AP8130DN-W    nor    1s
-------------------------------------------------------------------------------------------------
Total: 4
```

案例2：用户体验不佳故障排查 - 故障背景

- 案例背景：A公司内部网络中，员工多次反馈大会议室的无线网络不稳定，上网偶尔出现卡顿，影响线上会议进行，需要进行故障排查。



案例2：用户体验不佳故障排查 - 检查AP的空口环境

- 分析过程：第一步，尝试接入网络，能够正常接入，且关联到了最近位置的AP。
- 查看空口环境的质量。

```
<WAC> display ap radio-environment ap-id 13 radio 0
Radio:       0
ScanChannel:  1
WorkChannel:  1
ScanCycle:    1
--------------------------------------------------------------------------------
Ch  NF   CU(%) CommIf(%)  AdjaceIf(%) SINR   #APs
--------------------------------------------------------------------------------
1  -105   75          19              -          245       57
--------------------------------------------------------------------------------
Total: 69
--------------------------------------------------------------------------------
Ch    MAC               Type  RSSI  SSID
--------------------------------------------------------------------------------
1     c88d-833a-8d41 i     -72    Huawei-Employee
--------------------------------------------------------------------------------
Total: 50
```

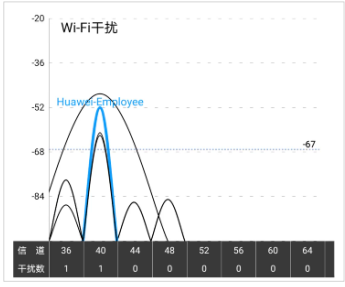
  - 发现空口质量不佳，且信号强度低于-65 dBm，初步判断需进行信道、功率调整，再使用CloudCampus APP检查周边空口环境。

案例2：用户体验不佳故障排查 - 使用工具检查空口环境

- 使用CloudCampus APP辅助检测结果一致，需进行信道及功率调整。

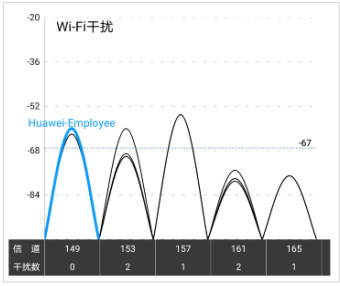
Wi-Fi干扰

同频干扰数	1 （推荐值：≤2）
同频最大干扰	-47dBm （推荐值：≤-75dBm）
邻频干扰数	1 （推荐值：≤5个）
邻频最大干扰	-78dBm （推荐值：≤-65dBm）
信噪比	38dB （推荐值：≥25dB）
当前信道受干扰强度	73 （推荐值：≤40）
解决方案	当前网络干扰严重，可以使用看干扰功能，重新选择工作信道。
Tips	当您手机、电脑的WiFi信号满格时仍然觉得网络卡顿时，这时候大部分的元凶就是【WiFi干扰】。干扰通常有WiFi设备的干扰、非WiFi干扰（运营商4G天线的干扰、蓝牙设备、微波炉等）。WLAN网络需要远离干扰，同时合理规划AP的功率和信道！



案例2：用户体验不佳故障排查 - 检查调整后网络质量

- 调整信道和功率后，网络恢复正常。



网络延迟

网关	10.166.236.1
Ping网关延迟	25.6ms （推荐值：≤80ms）
Ping地址1	www.baidu.com
ping延迟	58.4ms （推荐值：≤200ms）
解决方案	您网络延迟这么低，您的网络就是解决方案啊！
Tips	低延迟是业务体验的基本指标，语音会议、VR互动等要求更低的网络时延保证用户体验。

互联网性能

服务器	China Mobile Group Zhejiang Co.,Ltd
下载速度	68.36Mbps （推荐值：≥12.0Mbps）
上传速度	119.25Mbps （推荐值：≥6.0Mbps）
解决方案	当前网速极佳，邀请好基友来一把王者荣耀
Tips	不同的业务体检有不同的网络带宽推荐。我们建议：语音会议（2Mbps），网站访问（4Mbps），课堂直播（12Mbps），FTP下载（16Mbps），VR互动（50Mbps）。

网页体验

网址	www.baidu.com
DNS解析时间	126ms
TCP连接时间	272ms
HTTP请求时间	635ms
白屏时间	1205ms
总时间	2471ms （推荐值：≤3000ms）
解决方案	网页加载时间极快，网页体验很不错哦。
Tips	网页加载是一个带宽要求低、延迟响应要求不高的基本业务，网络维护人员需要关注。（注意当测试间隔很短时，DNS和TCP耗时会因为浏览器缓存机制，测试结果为0）。

网页时间参数关系

思考题

1. AP有哪些认证方式？默认的认证方式是哪种？怎么修改认证方式？
2. Portal认证重定向页面失败，包含哪两个部分？

HUAWEI

- 不认证、MAC认证、SN认证；MAC认证；在WLAN视图下，使用ap auth-mode XXX修改。
- 重定向Portal URL过程、访问Portal页面过程。

本章总结

- 本课程通过三个部分来介绍WLAN网络的故障排查，第一个部分侧重于解释常见的WLAN故障排查思路及方法，第二个部分介绍了一些能够帮忙WLAN工程师进行故障排查的工具，最后介绍了一些故障排查案例，希望通过该课程能够帮助考生掌握故障排查的技巧。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

智能运维

HUAWEI

前言

- 华为iMaster NCE-CampusInsight（园区网络分析器），颠覆传统聚焦资源状态的监控方式，将人工智能应用于运维领域，基于已有的运维数据（设备性能指标、终端日志等数据），通过大数据、人工智能算法及更多高级分析技术，将网络中的用户体验数字化，辅助客户及时发现网络问题，改善用户体验。
- iMaster NCE-CampusInsight采用Telemetry技术实时采集网络设备的性能指标和日志数据，基于真实业务流量发现网络异常。通过大数据平台，对数据进行统一采集、存储和分析，具有高效的大数据处理能力。

目标

- 学完本课程后，您将能够：
  - 描述园区网络智能运维的痛点及需求
  - 描述CampusInsight的逻辑架构、外部接口
  - 描述CampusInsight的应用场景及部署模式
  - 描述CampusInsight的主要功能特性及应用
  - 完成CampusInsight的主要操作

目录

WLAN运维面临的挑战

精准检测

传统运维基于SNMP分钟级采集数据，一旦发生问题，故障发生时刻数据无法实时获取，且缺少方便的回溯手段。

问题定位分析“难”

体验感知

传统运维仅监控设备指标，有可能指标正常，但用户体验不好，缺少用户和网络的关联分析。

用户体验衡量“难”

问题识别

传统运维往往等到用户投诉了，才知道网络发生了问题，无法有效主动识别、分析潜在影响用户感知的问题。

问题主动识别“难”

园区网络运维需求：AI智能运维

AS-IS：以设备为中心的网络管理

- **以设备为中心**，无法感知用户体验
- **“救火式”响应**，无法识别潜在故障
- 依靠专业工程师**现场定位故障**

TO-BE：以用户体验为中心的AI智能运维

体验可视化：基于Telemetry秒级数据采集，每用户每应用每时刻体验可视。

分钟级潜在故障识别和根因定位

- 基于动态基线、大数据关联等识别潜在故障。
- KPI关联分析和协议回放，精准定位问题根因。

网络预测性调优：通过AI 智能分析AP的负载趋势，完成无线网络的预测性调优闭环。

利用算法提升效率，通过场景化的持续学习和专家经验，智能运维将运维人员从复杂的告警和噪声解放出来，使运维更加自动化和智能化

CampusInsight：基于预测性和AI提升用户和业务体验

实时体验可视

1. **每区域：**通过多维的有线+无线网络健康度，直观呈现整网或每个区域的网络状况及用户体验。
2. **每用户：**实时呈现每个用户的全旅程网络体验（谁、何时、连接至哪个AP、体验、问题），故障可回溯。
3. **每应用：**实时语音与实时视频应用体验感知，快速智能定界问题设备，分析质差根因。

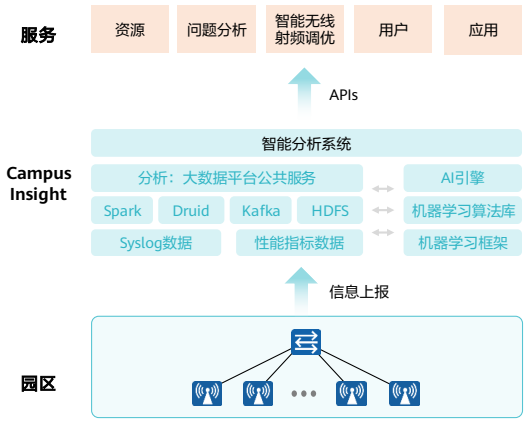
分钟级故障定界

1. **主动问题识别：**经过华为20万+终端持续训练的AI算法，主动识别85%的网络潜在问题。
2. **分钟级故障定位：**基于故障推理引擎，分钟级问题定界并识别问题根因，给出有效的修复建议。
3. **智能故障预测：**利用AI学习历史数据动态生成基线，通过和实时数据对比分析从而预测可能发生的故障。

智能网络调优

1. **实时仿真反馈：**基于楼层设备的邻居和射频信息，实时评估无线网络信道冲突情况，并给出优化建议。
2. **预测性调优：**基于历史数据的分析识别边缘AP、预测AP的负载趋势，进行无线网络的预测性调优并查看调优前后的增益对比，整网性能提升50%+（Tolly认证）。

CampusInsight：逻辑架构



业务服务：面向场景提供数据分析服务

- **问题识别：**连接/空口性能/漫游/设备四类问题的智能识别。
- **接入分析&性能体验：**连接问题以及性能体验问题分析。
- **用户&网络画像：**用户旅程回放，AP详情分析。
- **应用分析：**音视频质量感知。

数据分析：大数据平台和数据分析服务

- **数据存储：**预处理实时流、分布式处理离线流、数据存储服务。
- **数据分析：**模式识别、AI引擎、数据汇聚&查询。

数据采集：秒级采集性能指标以及日志

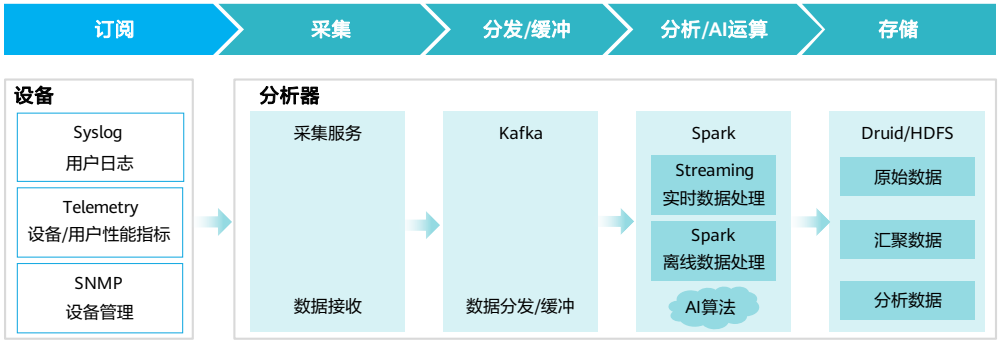
- **数据采集：**用户、射频、AP、交换机、用户日志等多维度数据。

CampusInsight：外部接口

- CampusInsight南向接口实现CampusInsight与设备之间的对接，完成CampusInsight对设备的管理功能。CampusInsight支持的南向接口类型，包括：SNMP、HTTP2+ProtoBuf、Syslog。

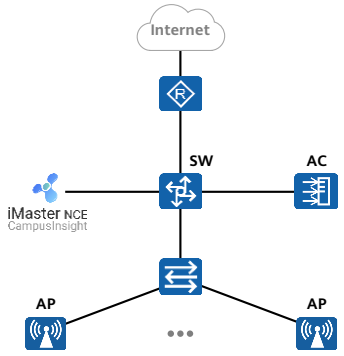
SNMP	HTTP2+ProtoBuf	Syslog
• 支持标准的SNMPv2c/v3。 • 通过SNMP可以实现CampusInsight与网络设备的连接，用于接入网络设备。 • SNMP基于TCP/IP的应用层网络管理协议，使用UDP作为传输层协议，能管理支持代理进程的网络设备。	• 采用HTTP2+ProtoBuf接口采集设备性能指标报文。 • HTTP2协议安全层通过SSL、TLS进行通信信道的认证和加密。 • ProtoBuf是由Google开发的一种数据序列化协议（类似于XML、JSON、hessian），能够将数据进行序列化，并广泛应用在数据存储、通信协议等方面。	• 系统日志（Syslog）协议是在一个IP网络中转发系统日志信息的标准。 • 工业标准协议，可用它记录设备的日志。 • CampusInsight通过Syslog协议接收设备上报的日志数据。

CampusInsight：数据处理流程



数据订阅后，由采集服务完成秒级数据的采集；经过高吞吐的分布式消息系统的缓冲和分发；由各业务服务完成基于AI算法、专家经验的数据分析和运算；最后将处理后的数据保存至快速的、列式分布式数据存储系统中，并通过页面进行功能展示。

CampusInsight应用场景：独立部署模式（本地部署）



场景描述

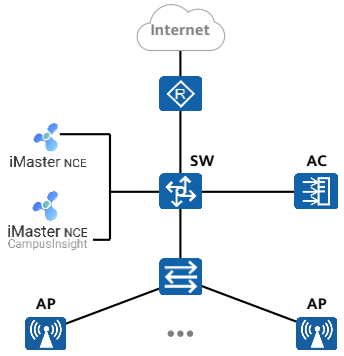
- CampusInsight独立部署，即以独立的平台在网络中部署。
- 支持园区企业无线和有线网络设备的智能分析。

组网说明

支持的组网如下：

- 所有AC（包含独立AC设备、随板AC及ACU）+ Fit AP
- 所有AC（包含独立AC设备、随板AC及ACU）+ 中心AP + RU
- 交换机和WLAN设备混合组网

CampusInsight应用场景：CloudCampus模式（本地部署）



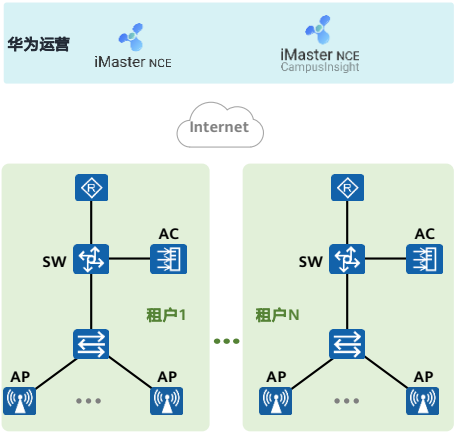
场景描述

- CampusInsight与iMaster NCE-Campus共部署。
- 企业购买华为云管理平台（iMaster NCE-Campus和CampusInsight）部署在数据中心，由运维人员负责云管理平台和园区网络的维护，供园区内部使用。
- 企业从华为服务团队购买相关license。

组网说明

- 支持华为云交换机、云AC和云AP设备的管理和智能分析，具体设备款型参见规格清单。
- 用户在企业自建的数据中心部署CampusInsight和iMaster NCE-Campus，通过iMaster NCE-Campus对设备进行纳管，CampusInsight从iMaster NCE-Campus同步设备等管理信息。

CampusInsight应用场景：CloudCampus模式（华为公有云）



场景描述

- iMaster NCE-Campus和CampusInsight由华为云管理运营团队统一运维维护，提供SaaS服务给最终用户（租户）。
- 租户网络设备通过运营商网络接入华为云管理平台。

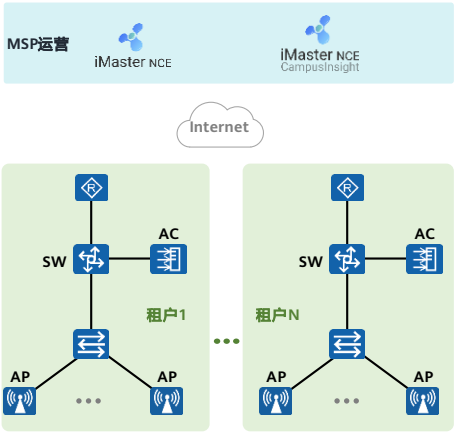
组网说明

- 支持华为云交换机、云AC和云AP设备的管理和智能分析，具体设备款型参见规格清单。
- 华为云管理运营团队在华为数据公有云部署CampusInsight和iMaster NCE-Campus，通过iMaster NCE-Campus对设备进行纳管，CampusInsight从iMaster NCE-Campus同步设备等管理信息。

HUAWEI

- SaaS：software as a service，软件即服务

CampusInsight应用场景：CloudCampus模式（MSP自建云）



场景描述

- MSP购买iMaster NCE-Campus和CampusInsight等软件做运营，软件可以部署在其数据中心或者公有云IaaS。
- MSP发展租户，向租户提供SaaS服务。
- 租户网络设备通过运营商网络接入MSP数据中心或者公有云IaaS。

组网说明

- 支持华为云交换机、云AC和云AP设备的管理和智能分析，具体设备款型参见规格清单。

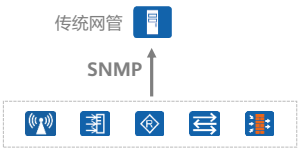
HUAWEI

- IaaS：infrastructure as a service，基础设施即服务

目录

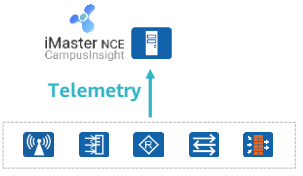
基于Telemetry技术，满足实时分析诉求

SNMP



- 协议发展停滞 ： SNMP是为有限的处理能力设计的网管协议；
- 基于轮询技术 ： 分钟级轮询周期，无法满足实时管理的业务诉求；
- 刚性数据结构：固定的数据结构定义，完成一次有效采集需要多个数据请求。

Telemetry



- 基于HTTP2 + ProtoBuf。
- 基于订阅发布、按需使用。
- 高效的编解码技术，一次获取多个数据，实现秒级数据获取能力。

准实时数据获取能力，是分析器挖掘数据的关键依赖。

无线网络Telemetry指标监控

- 基于Telemetry技术，监控无线侧关键KPI指标。从AP、射频、用户三个维度呈现无线侧的网络质量，主动识别弱信号覆盖、高干扰、高信道利用率等空口性能类问题。

实时数据呈现

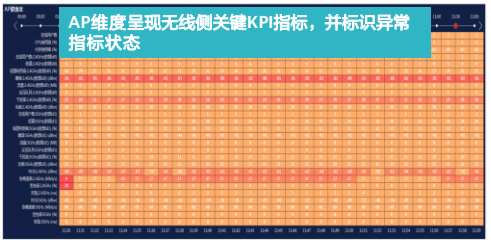
支持呈现无线侧关键KPI指标，并标识异常指标状态。

问题自动识别

结合AI算法、相关性分析、异常模式等自动识别空口性能类问题。

无线网络Telemetry Metrics采集

测量对象	测量指标	支持的设备类型	默认采样精度
AP	CPU利用率、内存利用率、在线用户数	AP	1分钟
射频	在线用户数、信道利用率、噪声、流量、反压队列、干扰率、功率	AP	1分钟
用户	RSSI、协商速率、丢包率、时延	AP	1分钟



HUAWEI

有线网络Telemetry指标监控

- 分析有线网络设备Telemetry特性采集的设备、接口等性能Metrics数据，主动监控、预测网络异常。

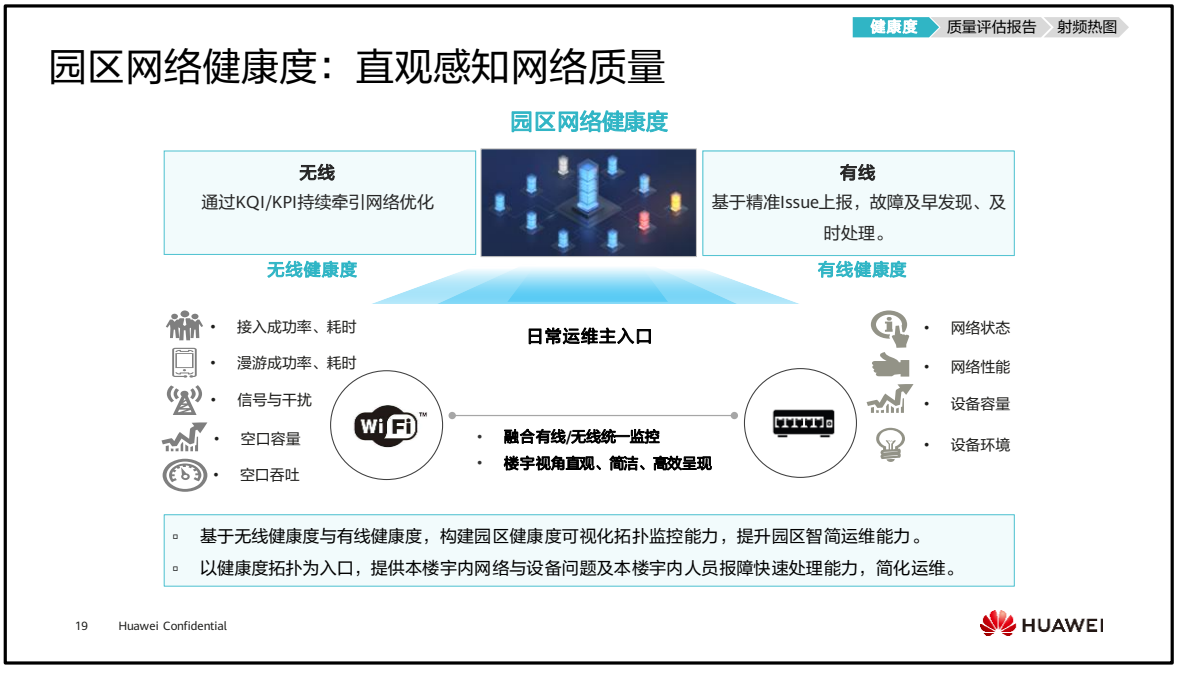
关键指标实时呈现	基于动态基线的异常检测
支持有线侧关键指标实时呈现，包含TopN、历史趋势等多种呈现方式。	使用AI算法对设备的CPU/内存利用率等指标进行基线预测。通过和动态基线的对比，在业务中断前识别网络指标的劣化。

有线网络Telemetry Metrics采集

测量对象	测量指标	支持的设备类型	默认采样精度
设备/单板	CPU利用率	交换机、AC	1分钟
	内存利用率	交换机、AC	1分钟
接口	广播、组播及单播报文的收、发数量；收、发丢包数；收、发错包数等	交换机、AC	1分钟

HUAWEI

目录



- KQI：key quality indicator，关键质量指标。

楼宇拓扑：基于楼宇呈现关键KPI及网络问题

楼宇视角，直观、简洁问题呈现

- ✓ 您的网络出现状态问题
  设备离线、端口闪断、AP离线等问题。
- ✓ 您的网络出现接入问题
  用户出现批量认证失败等问题。
- ✓ 您的网络出现拥塞问题
  网络出现端口拥塞、队列拥塞等问题。
- ✓ 您的网络出现误包问题
  网络端口出现误包超过阈值、误包数持续增长等问题。

多维网络健康度评估模型，全方位评价网络体验

无线网络健康度评估模型

三个维度，六个子类，直观呈现无线网络质量

- **接入体验**：用户是否能正常接入网络。
- **漫游体验**：用户移动过程中是否顺畅，没有卡顿。
- **吞吐体验**：无线网络是否存在干扰，是否需要扩容。

分类	评估指标	根因指标
接入体验	接入成功率	关联/认证/DHCP成功率
	接入耗时	关联/认证/DHCP耗时
漫游体验	漫游达标率	漫游成功率/漫游耗时
吞吐体验	信号与干扰	信号强度达标率、干扰达标率
	容量健康度	信道利用率达标率/用户数达标率
	吞吐达标率	非5G优先占比/空口拥塞达标率/物理层带宽

有线网络健康度评估模型

分析10+类监控对象，30+项指标数据，直观呈现有线网络质量

- **设备环境**：物理器件是否有状态异常
  整机、单板、风扇、电源、文件系统故障等。
- **设备容量**：感知设备资源数量或容量是否够用
  ARP/MAC/FIB等表项容量、ACL资源、存储器容量等。
- **网络状态**：网络接口是否有状态异常
  接口闪断、接口假死、光模块异常等。
- **网络性能**：数据传输异常，影响吞吐
  接口拥塞、队列拥塞、接口误包等。

案例1：无线网络健康度

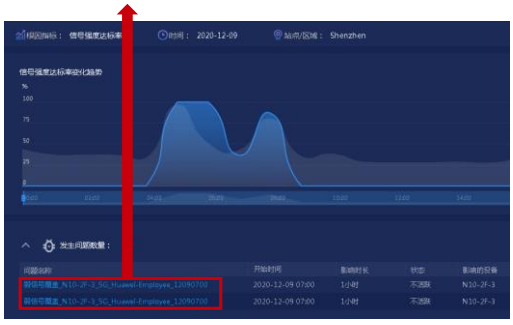
- 某局点运维人员使用CampusInsight无线网络健康度，发现深圳园区网络质量评估明显低于其他园区。对其进行维度分析，发现深圳园区接入成功率、覆盖、吞吐达标率得分均低于行业Benchmark。运维人员进行维度钻取分析，发现问题原因，将问题修复解决。

1、菜单选择**“健康度”**，选择**“无线健康度”**进入。

2、达标率排名中，深圳园区达标率低于其他园区。点击**“Shenzhen”柱状图**，页面刷新为深圳园区质量评估数据。

3、查看6大维度数据，发现信号与干扰维度质量评估是“良”，低于行业Benchmark。点击**信号强度达标率指标**，钻取查看问题。

4、在信号强度达标率分析页面，看到发生了两次弱信号覆盖的Issue。点击Issue的“问题名称”超链接，跳转到Issue详情界面，查看具体问题。



HUAWEI

案例2：有线网络健康度

- 某局点运维人员使用CampusInsight有线网络健康度，发现网络性能维度存在异常。运维人员通过详情查看，发现异常的监控项，进入对应的问题分析页面查看具体问题根因，将问题修复解决。

1、菜单选择**“健康度”**，选择**“有线健康度”**进入。

2、发现**“网络性能”**存在异常，点击**“查看详情”**。

3、查看异常的检测项，对于异常的问题，通过**“问题分析”**进入具体分析页面，查看问题原因与修复建议，闭环问题。

质量评估报告：实时或定期生成，优化有据可依

- CampusInsight提供专业评估报告服务，基于“全网概况”、“指标详情”、“整改建议”实时或周期自动生成网络质量评估报表，提供可量化的网络体验。

全网概况

资源概况、用户概况、质量概况，全网信息一目了然。

指标详情

依据质量评估体系七大维度指标，统计站点质量排名，识别站点质量变化趋势。

整改建议

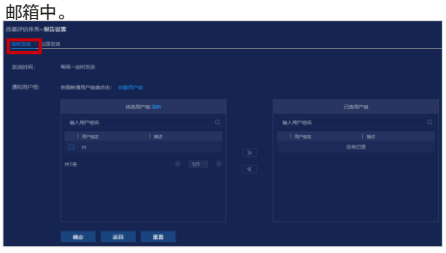
识别网络Top问题根因，提供修复建议指导用户持续提升网络质量。

HUAWEI

案例3：质量评估报告

1、菜单选择**“健康度”**，进入**“无线健康度”**页面，点击右上角**“报告导出”**。

2、**“定时发送”**：选择报告的**“发送时间”**与**“通知用户组”**，报告会按照设置的周期，定时发送到用户设置的邮箱中。



3、**“立即发送”**：选择报告的**“起止时间”**与**“接收方式”**，报告立即生成。（立即下载：浏览器直接提供下载；邮件发送：报告立即发送到指定用户邮箱）。

射频热图：网络覆盖仿真直观可视

比规划：部署无线网络覆盖与规划是否一致?
基于网络开通后射频真实功率、功率仿真覆盖范围。

看影响：需要增加一扇隔离墙，网络有影响吗?
通过增加故障物，仿真对无线覆盖影响。

少干扰：需要修改设备配置，会干扰其它设备吗?
修改设备配置，如功率、信道后，实时仿真设备间是否产生干扰。

能力	描述
按强度	仿真楼层各个位置Wi-Fi覆盖信号强度
按速率	仿真楼层各个位置Wi-Fi访问可达到速率值
按信道	仿真楼层各个位置在指定信道上覆盖信号强度及冲突情况

HUAWEI

- CampusInsight的业务拓扑能统计状态、接入、拥塞以及误包四大类问题，在拓扑上基于站点、区域、楼宇、楼层可视呈现用户数、流量及各类问题，通过搜索快速查看用户经过的楼栋回放，帮助用户快速确认园区网络问题。
- 在CampusInsight的业务拓扑中，可以进入“Wlan拓扑”查看网络的射频热图。

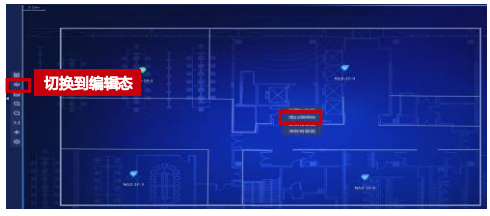
案例4：射频热图（1）

- 某公司会议室资源紧张，需要在办公场所隔出会议室，施工设计方向公司IT部门咨询：增加会议室，是否对办公Wi-Fi产生影响。IT人员通过射频热图，编辑会议室墙、玻璃门等故障物，根据仿真结果进行AP补盲或调整。

1、点击菜单**“业务拓扑”**，进入**“Wlan拓扑”**。

2、左树层级选择**“Shenzhen”**-**“N10”**-**“N10-1F”**。

3、切换到编辑态，右键选择**“增加障碍物”**。

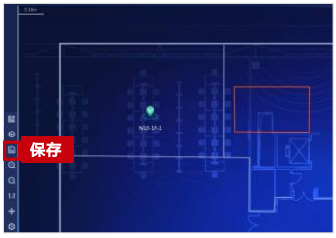


HUAWEI

案例4：射频热图（2）

4、形状选择“**折线**”、类型“**砖墙1**”或“**木门**”。

5、拓扑绘制会议室（如图方块，绘制完鼠标左键双击退出障碍物编辑），点击“保存”。



6、进入监控态，选择“**按强度**”，点击“**刷新**”查看是否存在盲区，根据仿真结果进行优化调整。

价值

当无线环境或设备信号配置发生变更后，通过射频热图，基于无线信号传播模型，仿真无线覆盖情况，主动识别覆盖盲区与冲突影响区域，为网络补盲及网络配置调整提供依据。

目录

CampusInsight：个障分析 & 群障分析

- 园区网络运维过程中，管理员遇到的问题主要分为两类：
  - 个体性问题：比如终端配置错误导致的个体接入失败等。
  - 群体性问题：比如认证服务器问题导致的批量认证失败，AP覆盖不足导致的批量用户信号强度差等。

个体性问题解决方案

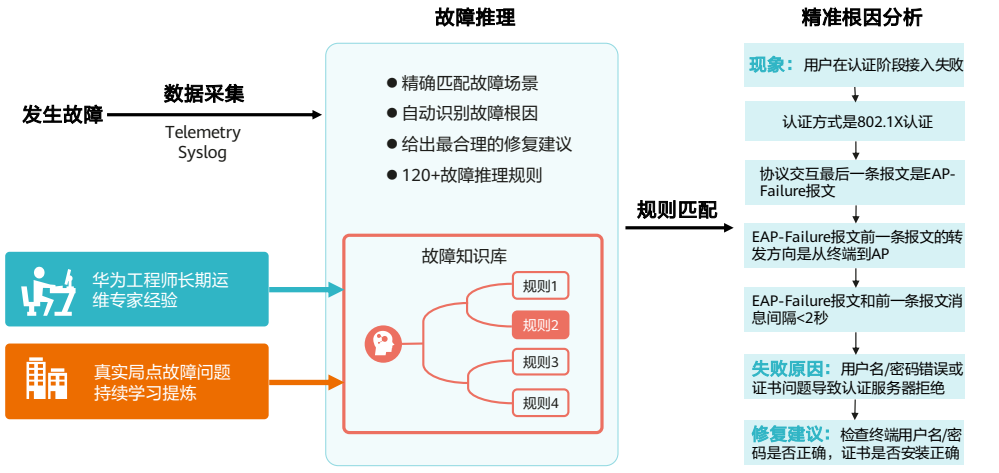
1、每指标：秒级数据采集&异常检测。

2、每用户：协议级接入过程分析、全旅程回放&体验分析、音视频应用质量感知。

群体性问题解决方案

三大类问题识别：智能识别连接类、空口性能类、漫游类问题。

CampusInsight：故障推理



HUAWEI

CampusInsight：从四个方面智能分析个体性问题

挑战	需求
1. 无法有效分析“接入失败发生在哪个阶段”。 2. 无法有效分析“用户去了哪里、体验怎么样”。 3. 无法有效感知“应用质量”。	端到端识别单个用户的网络体验问题并提供根因分析。

解决方案和客户价值

旅程分析 用户旅程 （无线+有线）	**接入分析** 协议回放 （无线+有线）	针对网络运维过程中遇到的用户个体性故障，CampusInsight从接入网络、使用旅程、体验质量、应用感知四个方面进行分析，将协议过程打开分析、用户旅程可视化回放、质差体验关联分析并感知音视频应用质量，助力管理员运维网络，精准保障VIP用户体验。
体验分析 质差用户相关性分析 （无线）	**应用分析** 音视频应用质量感知 （无线+有线）	

用户旅程：每用户每时刻实时体验可视

Step1 体验概览

看看整体的体验指标有没有问题?

Step2 体验趋势

看看体验趋势有没有波动或劣化?

Step3 旅程回放

看看每个时刻，接入了哪个AP，体验如何，发生了什么问题?

HUAWEI

案例5：Wi-Fi用户体验可视（1）

- 某局点领导报障，称Wi-Fi体验不佳。运维人员使用用户旅程功能，发现领导在咖啡厅时丢包很高，信号差，并出现了“弱信号覆盖”Issue。

1、菜单选择 **“用户”**。

2、点击搜索框，按用户名搜索**“XXX”**，点击**检索按钮**。

3、点击**MAC地址超链接**，跳转到用户旅程页面（页面内演示步骤见下一页）。

HUAWEI

案例5：Wi-Fi用户体验可视（2）

1、首先查看用户连接Wi-Fi体验概览，发现用户Wi-Fi体验指标中，**平均丢包率**较高，超过了15%。

2、查看用户Wi-Fi体验趋势，发现用户连接Wi-Fi的一段时间体验发生了明显的劣化，**信号很差**（小于-65 dBm），对应时间段的**丢包率很高**（超过5%）。

3、在用户的Wi-Fi旅程回放中，看到用户在接入AP“N10-2F-3”时，出现了**弱信号覆盖问题**，此时信号很差，丢包率非常高。

价值

CampusInsight用户旅程功能，聚焦用户真实的Wi-Fi体验，将每一个设备都作为传感器，精准地回放用户接入Wi-Fi网络的整个旅程，谁，什么时间，去哪里接入了哪个AP，体验如何，遇到了什么问题，全部都一目了然。

协议回放：分钟级定位接入故障根因

解决接入类问题，只需“三看”

1. **看状态：终端接入成功了没?**
   查看会话的接入结果，确认是否出现接入类问题。
2. **看交互：每一步协议交互正常么?**
   查看关联、认证、DHCP协议交互过程，确定异常阶段。
3. **看根因：问题根因是什么?**
   查看问题的大概率根因和修复建议。

HUAWEI

案例6：定位无线接入问题（1）

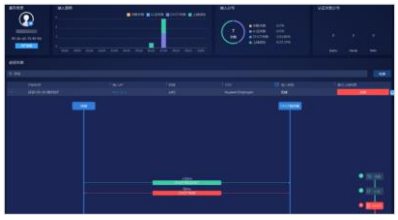
- 某局点用户报障，Wi-Fi无法正常接入。运维人员通过CampusInsight协议回放功能，定位出问题根因是由于DHCP地址池满了，导致给手机终端分配IP地址失败。修改对应配置，扩充DHCP地址池可用地址范围后问题解决。

1、菜单选择**“协议回放”**。

2、点击**切换用户按钮**。

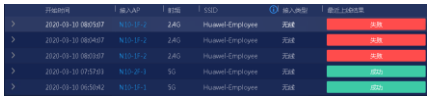
3、点击搜索框，按用户名搜索**“XXX”**，点击**选择按钮**。

4、页面刷新为案例相关数据。



案例6：定位无线接入问题（2）

1、首先能够确定，用户在此时出现了接入失败的问题。在Session List中选择一条接入失败的会话（直接点击）



2、查看用户接入过程，发现用户的关联、认证都已经成功，但DHCP过程出现了异常。点击DHCP按钮，呈现DHCP交互的过程。

3、在DHCP交互过程中，可以看到终端向DHCP Server发送了DHCP请求，但DHCP Server**回复了NAK的异常报文**。

4、系统分析出问题原因：**DHCP地址池中没有可供分配的IP地址**。建议扩充地址池可用范围

价值

CampusInsight协议回放能力，能够基于用户接入Wi-Fi三阶段（关联、认证、DHCP）进行协议级别的精细化分析，细化各阶段协议交互的详情，提供用户接入问题的根因与修复建议，是解决Wi-Fi连不上问题的一个强有力的武器。

用户Wi-Fi体验劣化相关性分析

Step1 AI识别

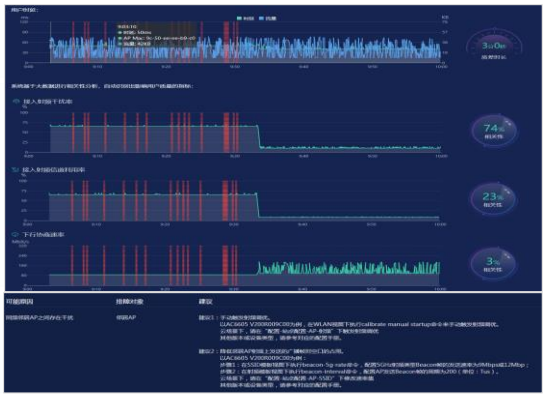
使用AI算法进行离群检测，识别Wi-Fi体验劣化用户。

Step2 AI分析

使用相关性分析算法，分析出相关性最大的网络指标，锁定问题根因。

Step3 AI闭环

根据华为工程师长期运维专家经验，给出最合理的问题闭环修复建议。



Wi-Fi连接质量不好？“全AI”分析！

HUAWEI

个障分析 旅程分析 接入分析 体验分析 应用分析

音视频应用质量感知

关键技术

- **主动感知音视频质量：**通过SIP Snooping技术主动感知SIP+RTP音视频流，实时探测音视频会话的建立与结束，自动启用eMDI技术监控分析会话过程中的音视频流质量，识别质差音视频流。
- **质差音视频根因分析：**分析音视频MOS值与空口指标（信号强度、干扰率、信道利用率、协商速率、反压队列计数等）、有线口指标（端口丢包率、缓存占用等）、设备类指标（CPU、内存占用率）的相关性，识别质差根因。
- **会话异常掉线根因分析：**自动分析音视频会话异常掉线的根因，包括漫游异常、Wi-Fi去关联、网络侧指标劣化、信令交互异常等。

HUAWEI

- 案例描述：
  - 运维人员查看办公区音视频会话列表，发现有员工的会话质量较差。查看质差会话详情，定界到问题出现在员工的接入AP上。点击相关性分析，发现由于信道配置不合理，邻居AP对该AP造成了干扰。通过调整信道，解决了空口干扰问题，音视频会话质量恢复到正常。
- 约束限制：
  - 仅支持IPv4场景下非加密的SIP信令+RTP承载的音视频应用。例如：HUAWEI Video Phone 8950。
  - 交换机仅特定款型支持音视频业务分析，AP仅特定款型支持音频业务分析，具体规格请参见CampusInsight规格清单中“HUAWEI设备支持规格清单”sheet页。
  - 支持交换机V200R013C00SPC500及以上版本及AP V200R010C00及以上版本。
  - 路径分析仅支持开启了云形态的交换机及AP。

CampusInsight：智能分析三类无线群体性问题

场景和需求

1. 数字化时代，“救火式”运维、事后处置难以保障业务体验。
2. 需要有更智能的手段自动识别潜在故障，并精准定位根因，从而降低故障响应时间。

识别潜在故障：故障响应时间从小时级降至分钟级

连接类

- 关联失败
- 关联慢
- 认证失败
- 认证超时
- 认证慢
- DHCP失败
- DHCP慢
- 用户网关不可达

空口性能类

- 弱覆盖
- 高信道利用率
- 高干扰
- 非5G优先
- 终端容量
- 空口拥塞

漫游类

- 乒乓漫游
- 漫游异常

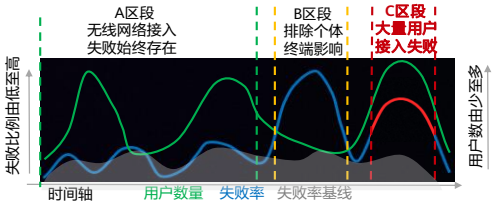
CampusInsight：智能识别三类典型问题

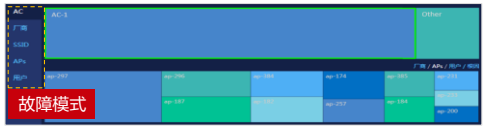
类型	描述	问题
连接类	快速识别关联、认证、DHCP三个阶段出现的群体性失败、慢等各类用户接入网络过程的问题。针对每个问题，通过故障知识库快速精准识别问题根因并给出修复建议。	认证失败
		认证超时
		认证慢
		关联失败
		关联慢
		DHCP失败
		DHCP慢
		用户网关不可达
性能类	实时监控无线空口性能数据，并融入华为专家经验，智能识别用户在接入无线网络后，影响用户上网体验的六类无线空口问题，并对应给出修复建议。	弱覆盖
		高干扰
		高信道利用率
		空口拥塞
		非5G优先接入
		终端容量
漫游类	分析用户在多个AP间的上、下线流程，智能识别用户在移动过程中的上网体验问题，并对应给出修复建议。	乒乓漫游
		漫游异常

连接类问题分析

关键技术

- **异常识别：**网络接入行为的异常检测。
  - 正常失败非故障场景（如右图A区段）：无线网络用户接入失败始终存在，然而它们不一定是故障。
  - 问题终端去噪（如右图B区段）：排除个体终端自身因素影响。异常终端导致失败率冲高，虽然超出基线但不是问题。
  - 机器学习智能识别“双高”（如右图C区段）：智能识别影响范围大的群体性问题，“失败用户数高”与“失败比例高”同时发生的“双高”问题。
- **模式识别：**相同的问题现象可能有不同的原因，通过识别模式找出可能的原因。将接入失败终端的相关特征进行抽象，运用聚类算法进行特征分析。
- **根因分析：**基于终端上线日志，提炼可能的故障根因并给出修复建议，帮助运维人员实现问题闭环。





HUAWEI

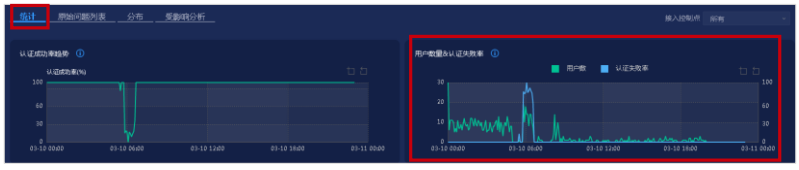
案例7：连接类问题分析（1）

- 局点运维人员某天中午接到用户保障，抱怨早上上班时段出现手机无法接入网络，直到10点左右才逐渐恢复正常。经IT人员最终定位，发现是RADIUS服务器性能较差，在上班高峰时段无法及时处理大量认证请求，导致认证失败，后更换更高性能的服务器后故障消失。

1、菜单选择**“问题分析”**。

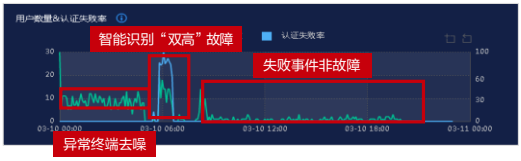
2、点击**连接类页签**，点击选择**“认证超时”**卡片，进入认证失败Issue视图。

3、点击**统计**查看右侧**“用户数量&认证失败率”**的统计分析图（具体分析见下一页）。



案例7：连接类问题分析（2）

4、点击**统计**查看右侧**“用户数量&认证失败率”**的统计分析图。



6、查看**失败事件**及**可能原因分析**。

分析器给出可能原因：**服务器异常**或接入控制器点与服务器连接异常，建议登录认证服务器进一步检查。

5、切换至**原始问题列表**，点击**问题名称超链接**，跳转到Issue详情页面。

价值

由于无线网络受信号覆盖、物理环境遮挡、无线干扰等因素影响，用户接入失败的事件持续存在。CampusInsight基于用户接入数据分析，识别异常终端，去除无效失败事件，使用机器学习算法智能识别系统中“双高”现象，及时准确识别网络中的群体性连接类故障，结合专家经验给出合理修复建议。

- 用户数量&认证失败率统计分析：
  - 异常终端去噪：某些时段也出现认证失败率冲高，经分析为异常终端发起大量认证请求，失败率100%，此种场景非网络问题引起，噪声数据需要去除（用户回访，发现是新员工，未安装公司Wi-Fi证书，频繁重认证导致出现大量失败事件）。
  - 智能识别“双高”故障：早上8点，无线接入用户数突增时，认证失败率冲高到70%（RADIUS服务器性能问题无法及时响应认证请求），出现典型的“双高”现象，表明大量用户出现认证失败，即出现群体性故障。
  - 失败事件非故障：由于无线用户接入的不稳定性（用户移动，经过盲区等），各个时段用户认证失败现象持续存在，但不影响用户实际体验，自动重新接入后即恢复正常。

弱信号覆盖Issue解决信号覆盖类问题

Step1 问题发现

智能识别弱信号覆盖问题。

Step2 问题分析

问题信息辅助分析。

Step3 问题原因

根据建议辅助排障。

“智能识别”弱信号覆盖，“足不出户”轻松搞定问题。

HUAWEI

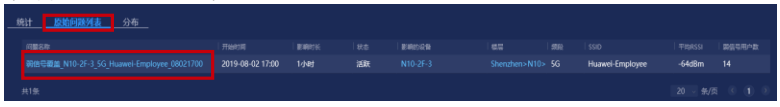
案例8：弱信号覆盖问题分析（1）

- 某局点运维人员通过CampusInsight检测到多条弱信号覆盖Issue，通过Issue详情分析出问题射频下大部分用户信号都比较弱，且该射频功率较高，导致较多终端远端关联到该射频。运维人员根据修复建议处理后，问题解决。

1、菜单选择**“问题分析”**。

2、点击**空口性能页签**，点击选择**“弱信号覆盖”**卡片，进入弱信号覆盖Issue视图。

3、点击**原始问题列表**查看Issue列表，选择第一个Issue，点击**问题名称超链接**，跳转到Issue详情页面（页面内演示步骤见下一页）。



案例8：弱信号覆盖问题分析（2）

1、AP“N10-2F-3”出现了弱信号覆盖的Issue。查看该AP下用户的信号强度分布，发现在Issue发生的时段内，**80%以上的用户信号强度均出现异常，低于-65 dBm**（以华为IT长期运维经验来看，信号强度低于-65 dBm会影响用户体验）

2、查看该AP的射频功率配置，发现在Issue发生时段内，该AP的**5GHz射频功率配置过高，配置值为30**（按照华为IT长期运维经验，5G射频功率一般配置为13）。功率配置过高，会使远处的终端关联进来，造成远端关联，出现弱信号覆盖现象。

3、分析器给出Issue的可能原因，是由于**AP射频功率配置过大导致**，建议降低对应功率配置。

价值

弱信号覆盖是很常见的一种Wi-Fi网络问题，由于网规不合理、配置不合理等原因，造成大部分接入用户的信号很差，Wi-Fi体验下降。CampusInsight能够自动识别这种问题，通过用户RSSI模式、射频功率等指标辅助分析，给出问题的原因和修复建议。

高干扰Issue解决干扰类问题

Step1：智能识别

智能识别，主动发现网络中高干扰问题。

Step2：关联分析

高干扰Issue相关指标关联分析。

Step3：定位排障

辅助可能原因与建议，定位问题根因并排障。

“救火式”运维变为“主动运维”

HUAWEI

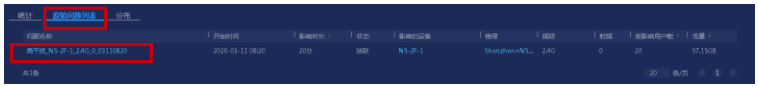
案例9：高干扰问题分析（1）

- 某局点运维人员通过CampusInsight检测到高干扰Issues，通过Issues详情关联分析发现有邻居AP造成严重的同频干扰，运维人员根据修复建议处理后，问题解决。

1、菜单选择**“问题分析”**。

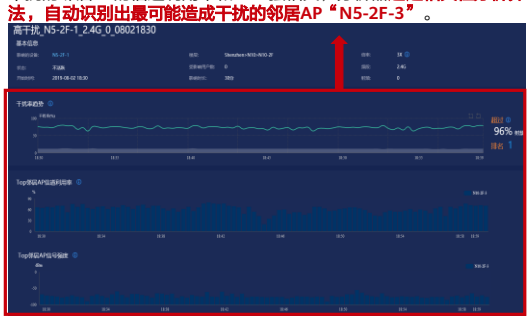
2、点击**空口性能页签**，点击选择**“高干扰”**卡片，进入高干扰Issue视图。

3、点击**原始问题列表**查看Issue列表，选择第一个Issue，点击**问题名称超链接**，跳转到Issue详情页面（页面内演示步骤见下一页）。

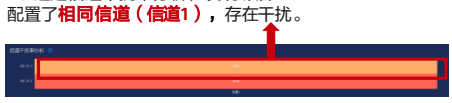


案例9：高干扰问题分析（2）

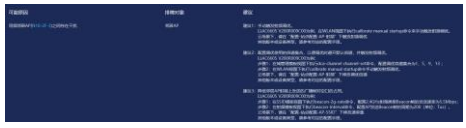
1、AP“N5-2F-1”出现了高干扰Issue。由于AP的干扰率与对它造成干扰的邻居AP的信道利用率和RSSI强相关，分析器**通过相关性分析算法，自动识别出最可能造成干扰的邻居AP“N5-2F-3”**。



2、通过信道干扰率分析，发现邻居AP“N5-2F-3”配置了**相同信道（信道1），**存在干扰。



3、分析器给出Issue的可能原因，是由于**同频邻居AP“N5-2F-3”**，建议进行射频调优。



价值

高干扰问题是Wi-Fi网络中非常常见的问题，会出现网络延迟大、网络卡顿等问题，一定程度上影响接入用户的Wi-Fi体验。
CampusInsight能够主动发现网络中出现高干扰问题，通过相关性算法与大数据分析，找到问题最有可能的原因，并给出修复建议。

目录

AI加持的智能无线射频调优，提升整网性能

场景1：人工调优

约**20%**客户会选择手工规划信道等，但面临的挑战：

- 手工规划不是最优
- 无法实时感知
  网络环境复杂，干扰变化大

实时仿真反馈

结合环境变化实时反馈，提供预测、仿真工具，驱动网络优化

场景2：自动调优

约**80%**会采用设备自动调优，但面临的挑战：

- 均衡调优未考虑负载
- 仅感知当前状态
  无法感知历史负载与干扰

预测性调优

基于大数据+AI，提供业务权重的权衡调优能力。

场景1：基于神经网络仿真反馈给出最佳信道规划建议

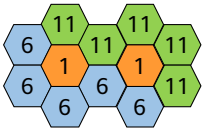
问题现象

IT工程师对员工报障区域进行网络优化，却发现优化后，周边区域又产生报障，持续多天多次调整，结果还是不尽如人意，越调越差，引发网络不稳定。

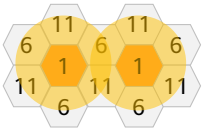
挑战

依赖专家经验调优，专业要求高；分析工作量大，人工无法从整网视角规划无线网络。

技术根因



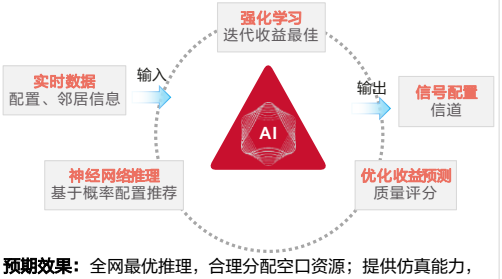
信道规划不合理导致AP相互干扰



信道为1的两个AP过近导致AP相互干扰

AP配置需充分考虑AP间、周边干扰、距离等影响，大部分调优只能保证本地最优，无法提供全网综合评估、确保整网最优。

无线网络仿真反馈方案



预期效果：全网最优推理，合理分配空口资源；提供仿真能力，基于收益得分评估，先确认后下发。

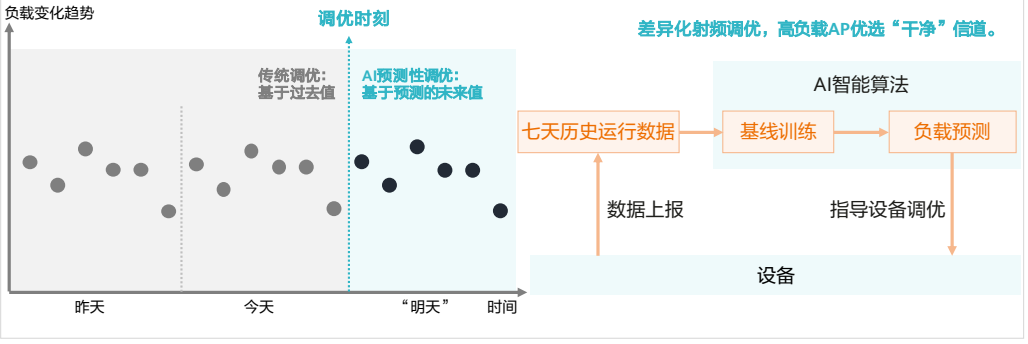
HUAWEI

场景2：基于AI的预测性调优（1）

挑战：如何利用AP负载数据，高效利用频谱资源

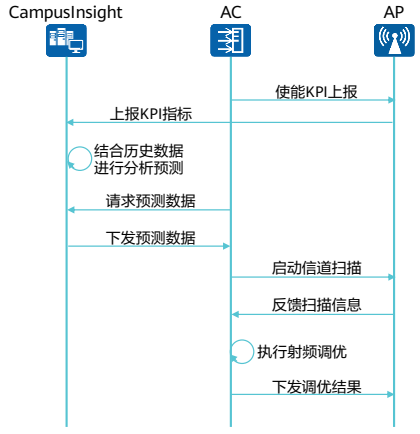
无线网络环境中每个AP的繁忙程度不同，如何准确预测每个AP的负载趋势，差异化作出整网的预测性调优?

方案：多种预测模型集成，准确预测AP负载，差异化射频调优



场景2：基于AI的预测性调优（2）

AP/AC等设备和CampusInsight交互原理图



- 通过KPI上报功能，AP可以将网络指标数据上报到CampusInsight，由后者进行汇总和分析预测。
- 在下次触发定时调优时，设备可以结合实时信道质量和CampusInsight提供的预测数据进行网络调优，使调优结果能有效规避非持续存在的干扰源、更加符合业务需要。

HUAWEI

- 在食堂、办公区、候车点、咖啡厅等存在明显人流的场景中，对于部署在人流附近的AP，往往存在较多短暂接入又迅速离开的STA。AP的空口资源会被此类STA大量占用，从而导致性能下降，而此类STA自身的上网体验也会由于上网方式的无谓切换而受到影响。为了方便表述，将处于这种状态的AP称之为“边缘AP”，将短暂接入又迅速离开的STA称之为“游牧STA”。CampusInsight可以根据AP上报的网络指标数据判断它是否为边缘AP，并在下次射频调优中通过调整AP的发射功率来抑制游牧STA的接入，改善AP射频的健康度。

案例10：基于AI的预测性调优（1）

- 某公司无线网络办公区升级改造，员工临时搬迁到C4栋楼临时集中办公，导致C4楼栋人员增多，网路负载加大，员工抱怨无线网络越来越卡，通过开启“智能无线射频调优”，自动识别C4办公楼内的高负载区域，针对性调整AP频宽，员工带宽得到提升，体验良好。

1、菜单选择**“智能无线射频调优”-“大数据调优”**。

2、开启**“智能无线射频调优”**（建议提前开启，提升数据训练的准确度）。

3、点击“下一步”，在“负载优化”中发现“C4-3F”识别出较多的**高负载AP**。

HUAWEI

案例10：基于AI的预测性调优（2）

4、开启大数据调优后第二天，C4三楼片区的AP经过大数据调优后，学生带宽提升到**257Mbps（提升50%），平均信道利用率降为3.4%（下降50%）。**

5、查看调优详情，C4三楼的高负载AP的5G频宽，**从20Mhz调整为40Mhz，员工上网体验提升，不再出现卡顿。**
注：AP频宽加大，用户的带宽会同步提升

价值

智能无线射频调优基于系统持续采集的真实用户的海量数据信息，运算AI算法智能识别系统中“高负载AP”、“边缘AP”，提供决策数据进行差异化的系统调优，实现真正意义上的网随人动。

思考题

1. CampusInsight可以实现以下哪些功能？（　）
   A. 网络健康度评估
   B. 无线用户体验可视
   C. 协议回放定位无线接入问题
   D. 分钟级故障定位

- ABCD

本章总结

- CampusInsight是华为推出的园区网络分析器，使用大数据分析技术和机器学习算法，旨在通过每时刻每用户的数据分析，提供卓越的网络服务保障体验。
- CampusInsight能够实现实时体验可视、分钟级故障定位、智能网络调优，本课程介绍了CampusInsight的主要功能及应用案例，包括有线无线网络健康度、个障及群障分析、智能调优等。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI

大型WLAN组网实践

HUAWEI

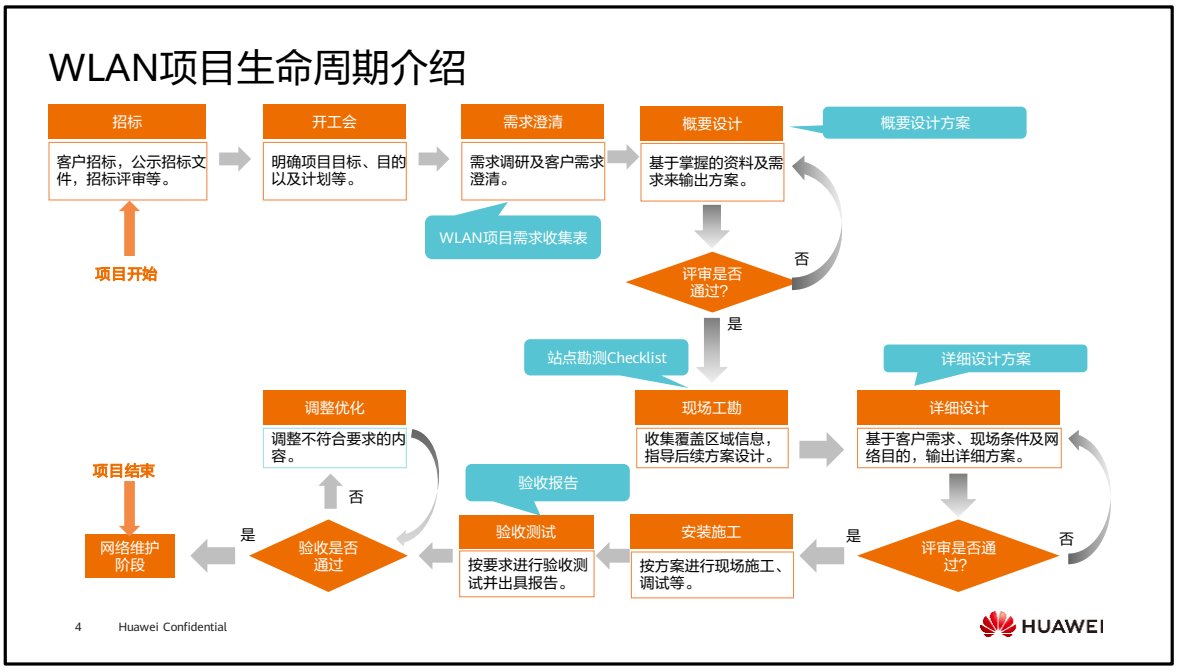
前言

- 一个标准的WLAN项目生命周期应该包含：需求澄清、概要设计、现场勘测、详细设计、网络部署、网络优化等环节。
- 在掌握WLAN领域的相关技术及解决方案后，职业化的WLAN网络工程师需端到端看护WLAN项目生命周期中的各个里程碑，并输出专业化的工程交付件，例如现场工勘报告、HLD及LLD等。这些都是构建高品质WLAN园区网络的重要保障。

目标

- 学完本课程后，您将能够：
  - 描述WLAN规划及交付流程
  - 描述WLAN项目交付件标准以及内容
  - 熟悉WLAN项目的设计、交付以及运维

目录



- 一般网络项目的服务流程分为需求澄清、概要设计、站点勘测、详细设计、安装调测、优化和验收。

目录

WLAN项目需求收集表 - 室内

内容	说明	结果
法律法规限制	确认网络所在地遵循法律法规限制，需要使用哪个国家码。	国家码: _____
平面图纸	需要提供有比例的平面图纸。如果客户没有图纸，需要提前进行图纸绘画。	□CAD图纸 □JPEG比例图纸 □非比例图纸 □无图纸
覆盖方式	描述覆盖的方式。	□室内分布 □室内放装
带宽需求	总带宽需求=总用户数*并发率*每用户带宽需求。	总用户数: _____ 每用户带宽需求:_____ 并发率:_____ 总带宽: _____
覆盖区域	结合工勘和建筑图纸，明确WLAN 建网的主要覆盖区域和次要覆盖区域，重点针对用户集中上网区域做覆盖规划。	主要覆盖区域: _____、_____、_____... 次要覆盖区域: _____、_____、_____... 特殊覆盖区域: _____、_____、_____...
场强需求	具体描述对于重点场强需求、边缘场强需求、干扰场强需求和外泄场强的具体要求。	重点场强: _____ 边缘场强: _____ 干扰场强: _____ 外泄场强: _____
组网方式	初步描述用户希望方式。	□AC直连 □AC旁挂 □不关注
配电方式	确认客户是否明确要求哪种供电方式，现场有哪些可以使用的供电区域和设施。	□PoE交换机供电 □交流适配器供电 □PoE适配器供电 □不关注
业务类型	描述业务的主要类型。	□日常办公（Email，FTP）□视频 □语音
终端类型	确认终端类型和数量，普通终端如手机、PAD、笔记本电脑，特殊终端如扫码枪、收银机等。	手机:_____ PAD:_____ 笔记本电脑: _____ 扫码枪: _____ 收银机: _____
安全策略	接入加密方式及认证方式。	SSID是否隐藏: _____ 加密方式: _____
交换机位置	WLAN上行有线侧交换机的位置。确认PoE供电距离是否符合要求。	
客户验收项及标准	客户对WLAN网络验收的特殊要求。	

WLAN项目需求收集表 - 室外

内容	说明	结果
法律法规限制	确认网络所在地遵循法律法规限制，需要使用哪个国家码。	国家码: _____
坐标&图纸	需要室外覆盖区域的坐标和边界或者提供带比例的平面图纸。	经度: _____ 维度: _____ 范围说明:_____ 带比例尺图纸: _____
带宽需求	根据用户的业务类型和占比，来分析单用户所需带宽，再推算总带宽。	总用户数: _____ 每用户带宽需求:_____ 并发率:_____ 总带宽: _____
覆盖区域	结合工勘和建筑图纸，明确WLAN建网的主要覆盖区域和次要覆盖区域，重点针对用户集中上网区域做覆盖规划。	主要覆盖区域:_____、_____、_____... 次要覆盖区域:_____、_____、_____...
场强需求	具体描述对于重点场强需求、边缘场强需求、干扰场强需求和外泄场强的具体要求。	重点场强: _____ 边缘场强: _____ 干扰场强: _____ 外泄场强: _____
障碍物	具体描述障碍物的类型、位置，尽量描述障碍物的高度。	楼房高度: ___树木高度:___ 绿化带高度:___
AP可安装位置	现场可安装设备的位置，如电线杆、监控杆，是否可自行立杆。	□电线杆 □监控杆 □树木 □自行立杆
配电方式	确认客户是否明确要求哪种供电方式，现场有哪些可以使用的供电区域和设施。	□PoE交换机供电 □交流适配器供电 □PoE适配器供电
业务类型	描述业务的主要类型。	□视频 □语音 □浏览网页
终端类型	确认终端类型和数量，普通终端如手机、PAD、笔记本电脑、IP摄像头等。	手机:____ PAD:____ 笔记本电脑: _____ 摄像头: _____ 其他: _____
设备类型	是否有802.11ax产品要求等。	□无要求 □802.11ax □ 802.11ac
交换机位置	WLAN上行有线侧交换机的位置，确认是否有室外部署机柜，室内部署交换机需确认PoE供电距离是否符合要求。	□室内部署交换机 □室外部署交换机
客户验收项及标准	客户对WLAN网络验收的特殊要求。	

WLAN网络规划概要设计方案 - HLD

方案架构	内容	描述
项目概述	项目背景	客户信息及本项目的信息
	网络建设目标	网络建设的目标
需求分析	网络现状	现有的网络结构图及简介
	覆盖目标	WLAN网络所要覆盖的建筑情况（建筑平面图及照片）：各个区域的功能，人员的分布信息，覆盖的要求。
	业务需求	WLAN网络应用的业务，每用户的带宽需求。
	特殊要求	用户对WLAN网络验收的特别要求。
网络设计	产品介绍	WLAN所使用的AC、AP产品功能介绍以及选择该产品的原因。
	组网结构	WLAN网络的组网结构图，需要标示出管理流量，业务流量的方向等信息，简要说明采用该结构的原因。
	容量规划	描述各用户的带宽要求，上网的并发率，总带宽需求，AP的个数估计。 AP上层交换机的上下行带宽需求。
	AP位置规划	AP位置规划所遵循的规划，如AP的覆盖半径、覆盖的人数。 各个楼层区域的AP分布图，AP、AC的放置方式。
	设备需求	各个楼层各个区域的AP、AC、PoE交换机的型号、数量。 各型号设备的数量汇总信息。
	信号仿真图	RF仿真图：场强、吞吐量等信息。

WLAN站点勘测信息采集表 - 室内

建筑覆盖类型	室内放装型/室内合路型/室外放装	
覆盖区域描述	记录覆盖楼层数量，需要覆盖楼层或特定区域（在建筑图纸标注）。	
	记录各AP覆盖楼层或区域。	
覆盖容量描述	估计特定区域人数，是否有大会议室，会展中心等，记录人数及分布情况。	
	记录用户的业务类型，现场询问客户避免与前期的需求调查有所偏差。	
建筑信息	业主提供的建筑图纸与现场是否一致，记录不同之处。	
	图纸中需要把房间号标示出来，比如弱电井位置、交换机可安装位置等。	
建筑材质及损耗	墙/门/窗/天花板	结合建筑图纸描述材质及测试以后的损耗。
干扰源	内部干扰源	结合建筑图纸描述清楚干扰源的来源、位置与强度。
	外部干扰源	结合建筑图纸描述清楚干扰源的来源、位置与强度。
走线规则	总体走线规则	描述总体的走线规则。从交换机到AP之间网线路由经业主同意，需要穿墙打孔位置业主是否同意。是否有条件隐蔽走线，或使用PVC线槽，经客户同意。
	特殊走线规则	对于一些特殊情况下的走线规则进行处理，如果不涉及可忽略
勘测描述	设备安装位置	在建筑图纸标注各AP适合安装位置，交换机安装位置，网络走线路由标注，照片存档。
	电源确认	交换机安装位置是否具有电源插座。
		AP使用PoE供电是否有障碍，是否考虑独立供电。
	内部建筑结构	对房屋结构拍摄足够数量的照片。主要关注屋内是否新增了明显的障碍物。
	传输资源	交换机安装处是否具备上层汇聚传输资源（汇聚设备上连口带宽）。
业主要求	不同业主可能存在一些特定的需求，需沟通清楚，让业主确认信息无误。	

WLAN站点勘测信息采集表（室内）

WLAN站点勘测信息采集表 - 室外

站点位置	海拔高度		经纬度	
直接可视			加抱杆可视	
工程站点地址				
覆盖区域描述	描述覆盖区域情况，定向站按扇区覆盖方向描述覆盖区域，如街道，景区，小区等。			
	对周围环境按顺时针拍照备案（推荐每60度一张），并对扇区主覆盖方向拍照备案。			
站点环境描述	描述站点天面情况，是否有其他通信系统共站，周边是否有其他通信系统，拍照备案。			
天馈系统描述	描述天馈系统类型，根据覆盖目标确定天线方位角等工参。			
勘测描述	设备安装位置	抱杆，挂墙还是铁塔。		
	电源确认	交换机安装位置是否具有电源插座。		
		AP能否使用PoE供电。		
	走线确认	若交换机在室内部署，从交换机到AP之间网线路由经业主同意，需要穿墙打孔位置业主是否同意。		
		是否有条件隐蔽走线，或使用PVC线槽，经客户同意。		
各运营商覆盖情况	运营商网络的覆盖情况，频点使用情况，逐一记录，预计安装位置测试点抓屏保存。			
业主要求				
安装环境准备遗留问题备注	物业准入：			
	电源：			
	汇聚传输：			

WLAN网络规划详细设计方案 - LLD

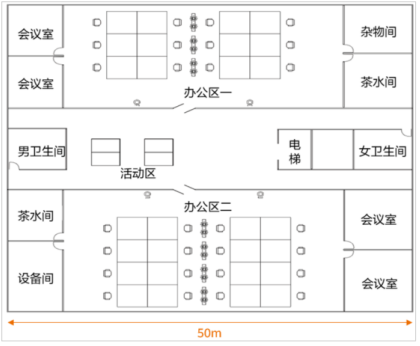
方案架构	内容	描述
项目概述	项目背景	客户信息及本项目的信息
	网络建设目标	网络建设的目标
需求分析	网络现状	现有的网络结构图及简介
	覆盖目标	WLAN网络所要覆盖的建筑情况（建筑平面图及照片）：各个区域的功能，人员的分布信息，覆盖的要求。
	业务需求	WLAN网络应用的业务，每用户的带宽需求。
	特殊要求	用户对WLAN网络验收的特别要求。
勘测数据	自由空间损耗	WLAN信息在自由空间的损耗的实测数据，应包含10米、20米、50米、100米等的场景。
	建筑穿透损耗	建筑内各种材质的门、窗、墙的穿透损耗实测数据。
	干扰源信息	干扰源的位置、信号强度、频率。
网络设计	产品介绍	WLAN所使用的AC、AP产品功能介绍以及选择该产品的原因。
	组网结构	WLAN网络的组网结构图，需要标示出管理流量，业务流量的方向等信息，简要说明采用该结构的原因。
	容量规划	描述各用户的带宽要求，上网的并发率，总带宽需求，AP的个数估计。AP上层交换机的上下行带宽需求。
	AP位置规划	AP位置规划所遵循的规划，如AP的覆盖半径、覆盖的人数。各个楼层区域的AP分布图，AP、AC的放置方式。
	设备需求	各个楼层各个区域的AP、AC、PoE交换机的型号、数量；各型号设备的数量汇总信息。
	信号仿真图	RF仿真图：场强、吞吐量等信息。
部署建议	线缆路由	在建筑图标示出的线缆位置走向信息。
	安装要求	线缆的长度、间距、及PVC的安装要求。
需求分析	AC&AP部署	AC的部署位置、及要求。AP安装在天花板、壁挂的步骤及要求。

目录

室内WLAN项目背景

- 某公司新办公区WLAN网络部署，经过与XXX项目接口人详细沟通，该项目情况如下：
  - 建筑图纸见右图所示，建筑的长度为50米，单用户的业务类型分析见下表。
  - 无线WLAN网络应覆盖项目所在的室内区域，办公室、会议室、活动区为重点覆盖区域，卫生间、茶水间、设备间和杂物间等为普通覆盖区域，电梯不覆盖。
  - 整个办公区可以容纳400人，两个办公区，每个办公区200人。
  - 活动区人数不超过100人，并发率60%，各会议室最大接入人数不超过30人，并发率50%。
  - 无线网络需支持802.11ax标准，活动区域为镂空设计。

业务类型	单业务基线速率（Mbps）		占比
	优异	良好	
网页浏览	8	4	40%
流媒体（1080P）	16	12	13%
流媒体（4K）	50	22.5	10%
VoIP（Voice）	0.25	0.125	10%
电子白板	32	16	5%
电子邮件	32	16	5%
文件传输	32	16	5%
即时通讯	0.5	0.25	12%

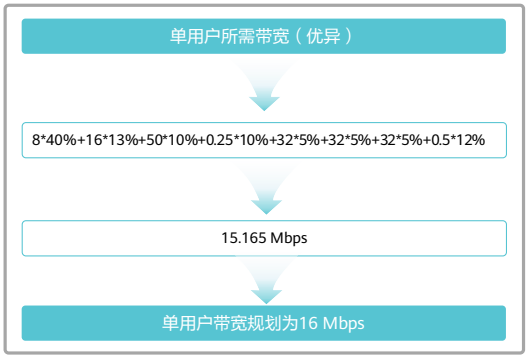


单用户所需带宽分析

- 基于用户的业务类型及占比，可以计算出平均每位用户的带宽需求，有了单用户的单宽需求后，不仅可以计算WLAN网络的总带宽，也有助于AP设备选型及AP数量计算。

业务类型	单业务基线速率（Mbps）		占比
	优异	良好	
网页浏览	8	4	40%
流媒体（1080P）	16	12	13%
流媒体（4K）	50	22.5	10%
VoIP（Voice）	0.25	0.125	10%
电子白板	32	16	5%
电子邮件	32	16	5%
文件传输	32	16	5%
即时通讯	0.5	0.25	12%

优异与良好表示用户在使用某业务时不同带宽情况下的体验。
该项目全部使用优异的用户体验结果来规划用户带宽。



WLAN项目需求收集表

- 结合单用户带宽，完善WLAN项目需求收集表。

澄清内容	结果
法律法规限制	国家码: CN
平面图纸	JPEG比例图纸，建筑长度为50米
覆盖方式	室内放装
带宽需求	单办公区：总用户数：200；每用户带宽需求：16 Mbps；并发率：70%
	会议室：总用户数：30；每用户带宽需求：16 Mbps；并发率：50%
	活动区：总用户数：100；每用户带宽需求：16 Mbps；并发率：60%
覆盖区域	主要覆盖区域：办公区、会议室、活动区 次要覆盖区域：茶水间、卫生间、杂货间、设备间
场强需求	重点覆盖区域场强：≥-65 dBm；次要覆盖区域场强：≥-80 dBm； 边缘场强：≤-80 dBm；干扰场强：-60 dBm；外泄场强：无要求
组网方式	AC旁挂组网 + 直接转发
配电方式	AP使用PoE交换机供电
终端类型	普通手机和笔记本，支持2*2MIMO，2.4GHz频宽支持40 MHz，5GHz频宽支持80 MHz
安全策略	员工认证方式：802.1X；访客认证方式：Portal
交换机位置	WLAN上行有线侧交换机的位置，PoE供电距离符合要求
客户验收项及标准	无特殊要求

WLAN设备选型 & 计算AP数量

- 在规划WLAN网络时，首先考虑到的是满足AP跟无线网卡信号的交互，以及用户可有效的接入网络。
  - 客户要求支持802.11ax标准，且每位用户的带宽为16 Mbps，同时，同一个办公区域人数达到100人，并发率为70%，按每人2台终端来规划（活动区只考虑一台终端），则单办公区的终端数量：单办公区总终端数量=100*2*70%=140个终端。
  - 参考华为Wi-Fi 6 AP在满足单用户16 Mbps带宽需求的前提下，双频最大并发14个终端，三频最大并发23个终端，也就是需要双频AP 20个或者三频AP 7个，基于成本和场景考虑，决定使用支持三射频AP AirEngine 5760-51（注意AP需配置RTU licence升级来支持8空间流），节省预算的同时，减少AP的部署数量。
  - 初步规划，单办公区部署13个AP，每个会议室部署2个AP，活动区域由于形状狭长，且无法吸顶布放AP，预计部署3~6个AP。
  - 需纳管AP数量不超过50个，WAC可以使用AirEngine 9700S-S接入控制器。
  - 接入交换机需为AP提供电源，故需选购PoE交换机，由于全是室内AP，交换机支持PoE即可，本案例使用CloudEngine S5731-H24P4XC，电源也许采购PoE电源。

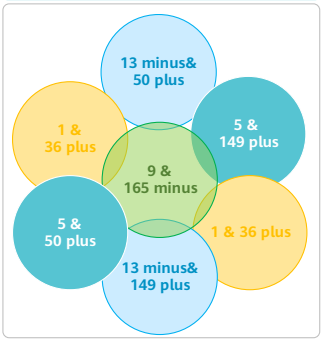
Wi-Fi 6 AP在不同带宽下的最大并发终端数

序号	用户接入带宽	单频最大并发终端数	双频最大并发终端数	三频最大并发终端数
1	2 Mbps	42	72	114
2	4 Mbps	24	41	65
3	6 Mbps	18	29	47
4	8 Mbps	15	24	39
5	16 Mbps	9	14	23

WLAN网络AP信道设计

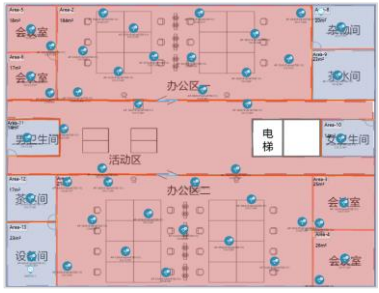
- 信道频宽规划：
  - 2.4 GHz，由于用户带宽需求为16 Mbps，AP部署密度较密，使用40 MHz会导致临频或同频干扰，所以将使用20 MHz频宽。
  - 5 GHz的信道资源丰富，足以满足使用40 MHz的条件，目前支持80 MHz频宽的终端设备较少，所以将使用40 MHz频宽。
- 室内部署可用信道：
  - 2.4 GHz信道：1、5、9、13（不考虑802.11b兼容情况）
  - 5 GHz频段信道：36~64、149~165（不同国家或地区，可用信道不同，规划前必须确认清楚）
- AP功率：
  - 默认AP将开启AP功率自动调整功能。

全向覆盖示意：



使用WLAN Planner进行网络规划

- 障碍物绘制（粗略估计）。
  - 外层墙体等为240 mm混凝土。
  - 卫生间、设备间外层、会议室相邻墙体为240 mm加厚砖墙。
  - 会议室、办公区的墙体均为120 mm加厚砖墙。
  - 门均为40 mm实木门。
- 区域绘制。
  - 重点覆盖区域：办公区、会议室、活动区；信号强度≥ -65 dBm。
  - 次要覆盖区域：杂物间、茶水间、卫生间、设备间；信号强度≥ -80 dBm。
  - 设定区域覆盖人数、带宽需求及终端类型。
- AP以及接入交换机点位设定。
  - AP点位可以自动部署，也可手动部署，障碍物与区域设定的越详细，AP自动布放就越准确。
  - 干扰源未知（需工勘）
  - 一台交换机部署于设备间，另一台部署在杂物间。

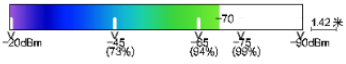


- AP参数设定。
  - AP的安装高度，默认吸顶安装，高度为2.6 m，活动区域壁挂安装AP，高度为2.5 m。
  - 活动区域AP朝向需综合调整，使得整个活动区域被最少数量的AP覆盖。

使用WLAN Planner进行信号仿真

- 基于输入的建筑大小、障碍物、AP设备以及干扰源情况进行信号仿真，根据初步规划的AP数量，进行微调，确定最终AP数量以及点位。
  - AP可以自动布放，但可能布放不合理，可以先进行自动布放，然后手动调整数量和点位。
  - AP布放需注意活动区不能吸顶布放，只能壁挂部署，壁挂部署AP需调整好天线角度，室内壁挂可微调AP朝向。

材料名称	材料类型	材料数量
AP	AirEngine5760-51	45
交换机	S5731-S24P4X	2



WLAN网络规划概要设计方案 - HLD

方案架构	内容	描述
项目概述	项目背景	为了提高办公效率，给办公室进行WLAN网络覆盖，覆盖区域面积大约为2500 m²，覆盖总人数为400人左右，前期客户选定一个试点区域完成了WLAN覆盖设计和报价，客户满意该方案，目前开展项目后续事宜。
	网络建设目标	完成新办公区WLAN网络覆盖，满足客户的业务需求。
需求分析	网络现状	新建WLAN网络，层高约2.6米，镂空层高度为15米，现在室内覆盖区域有2个其他无线信号。
	覆盖目标	全部使用室内型AP，除活动区域外，均使用吸顶部署。 重点区域：重点覆盖区域：两个办公区域，四个会议室，一个活动区；信号强度≥ -65 dBm。 次要覆盖区域：两个茶水间，两个卫生间，一个设备间，一个杂货间；信号强度≥ -80 dBm。
	业务需求	正常上网业务，场强、带宽、漫游等无特殊要求。但需要通过划分SSID等方式，实现带宽控制。
	特殊要求	针对WLAN无线网络的QoS设计，员工的带宽为16 Mbps，访客的带宽限制为2 Mbps。
网络设计	产品介绍	WAC：AirEngine 9700S-S； AP：AirEngine 5760-51；交换机：CloudEngine S5731-H24P4XC
	组网结构	附图
	容量规划	单用户带宽需求为16 Mbps。 每个办公区域有200人，每人2台终端，并发率70%。每个会议室有30人，每人2台终端，并发率50%。 每个活动区域有100人，每人1台终端，并发率60%。其他区域仅需考虑6人，每人1台终端，并发率50%。
	AP位置规划	单办公区部署13个AP，每个会议室部署2个AP，活动区域由于形状狭长，且无法吸顶布放AP，预计部署3~6个AP。
	设备需求	AirEngine 9700S-S：1； AirEngine 5760-51：38个；CloudEngine S5731-H24P4XC：2个
	信号仿真图	RF仿真图：场强、吞吐量等信息。

WLAN站点勘测

- 现网工勘的主要目的是获取现场的实际环境信息，如干扰源、障碍物衰减、楼层高度、新增障碍物和弱电井等信息，配合建筑图纸来确定AP选型、安装位置和方式、供电走线等设计。
- 现场工勘需要借助多项工具辅助才能完成，工勘前需要准备好工勘工具，常见工具主要有：

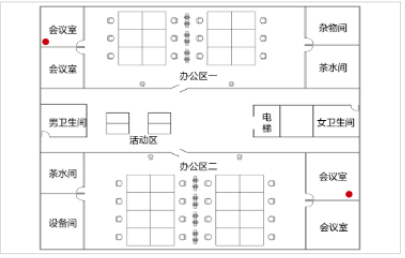
类型	名称	说明
软件工具	WLAN Planner	WLAN Planner是由华为推出的专业无线网络规划工具，用于网规环境设置、设备布放、无线信号仿真和网规报告输出等，帮助用户轻松完成网规设计。 在工勘任务开始前，需要先用WLAN Planner设计一版网规初稿，根据初稿的结果，指导工勘时特别关注的注意点。网规初稿的设计思路与网规设计一致，区别在于网规初稿设计时没有工勘的采集数据做参考。
	CloudCampus APP	CloudCampus APP内置工勘模块，且支持找AP、查终端、看干扰等多个功能。使用APP执行如下任务： • 查看当前无线环境信道使用情况。 • 测试障碍物衰减，记录障碍物位置、类型和衰减值。 • 在图纸上增加图片和文字类的标注信息。 • 修改图纸比例尺、楼层属性。
	高德地图/Google Earth	在部署室外网络场景时使用，用于标记AP经纬度、查看障碍物、确认项目现场环境等。
硬件工具	室内测距仪	在部署室内网络场景时使用，用来测量AP安装位置高度、AP和障碍物间距、场馆长宽高信息等。
	相机	记录站点环境情况，如AP安装环境，WDS场景站点障碍物信息等。
	测试用AP（含配套电源及支架）	室内场景配合CloudCampus APP进行障碍物衰减测试，建议携带。 请注意携带测试FAT AP时，需要同时携带： • 电池：用于给测试AP供电。 • 落地支架：要求支架可升至2 m，用于模拟AP吸顶安装场景。
其他工具	建筑图纸	提前打印建筑图纸，方便现场工勘使用。

WLAN站点勘测信息采集表

建筑覆盖类型	室内放装型	
覆盖区域描述	仅需要覆盖一个楼层 重点覆盖区域：两个办公区域，四个会议室，一个活动区。	
	次要覆盖区域：两个茶水间，两个卫生间，一个设备间，一个杂货间。	
覆盖容量描述	每个办公区域有200人，每人2台终端，并发率70%；每个会议室有30人，每人2台终端，并发率50%；每个活动区域有100人，每人1台终端，并发率60%，其他区域仅需考虑6人，每人1台终端，并发率50%。	
建筑信息	业主提供的建筑图纸与现场一致	
	设备间与杂货间均可用来放置交换机	
	楼层高度为2.6m，活动区域镂空，高度超过15米，无法吸顶部署。	
建筑材质及损耗	墙/门/窗/天花	外层墙体等为240 mm混凝土，卫生间、设备间外层、会议室相邻墙体为240 mm加厚砖墙，会议室、办公区的墙体和门均为12 mm加厚玻璃，卫生间门均为40 mm实木门。
干扰源	内部干扰源	仅有两个内部干扰源，已在图纸上标记，处于桌上，高度1米，2.4GHz功率21 dBm，5 GHz功率24 dBm，天线增益均为4 dBi。
走线规则	走线规则	从交换机到AP之间网线路由均走天花板吊顶内部穿透，需隐蔽走线，可打孔。
勘测描述	设备安装位置	一台交换机安装在设备间，一台交换机安装到杂货间，AP部署位置可参考WLAN Planner规划。
	电源确认	交换机安装位置具有电源插座，AP可使用PoE电源。
	内部建筑结构	桌、椅等高度都正常，对于信号干扰不大，可忽略。
	传输资源	交换机安装处具备上层汇聚传输资源
业主要求	员工和访客的SSID需要分开，访客带宽限制为2 Mbps。	
安装环境准备	物业准入：	已获取物业许可

WLAN工勘信息分析

- 图中建筑，左右墙体距离为50米，图中红点为现场的干扰源位置，2个干扰源均为2.4GHz和5GHz双频设备，规划时需设置好干扰源的高度、功率以及频段。



- 在现场测试自由空间信号衰减情况。

距离	1 m	2 m	5 m	10 m	15m	20 m	40 m	80 m	100 m
2.4G	46 dB	53.5 dB	63.5 dB	71 dB	75.4	78.5 dB	86 dB	93.6 dB	96 dB
5G	53 dB	62 dB	74 dB	83 dB	88.3	92 dB	101 dB	110.1 dB	113 dB

- 最终信号场强 = AP发射功率 + 天线增益 – 传输距离衰减值 – 障碍物信号衰减。
- 忽略其他衰减的情况下计算，信号传输距离在20米时，信号场强为（5.8 G）：AP发射功率（20 dBm） +天线增益（全向3 dBi）–传输距离衰减值（92 dB）–障碍物信号衰减（0 dB）= -69 dBm。所以规划AP点位时，需注意AP间距不应超过20米，当有障碍物时，需注意减少AP布放间距。

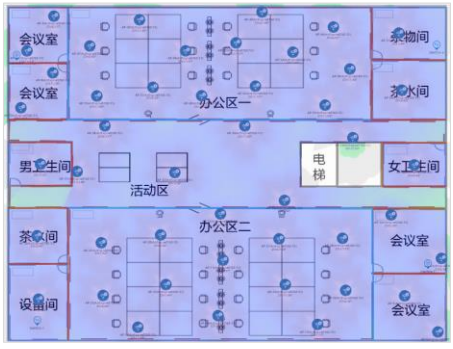
使用WLAN Planner进行网络规划（基于工勘结果）

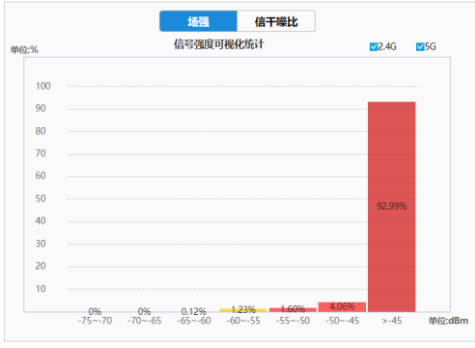
- 障碍物调整。
  - 外层墙体等为240 mm混凝土。
  - 卫生间、设备间外层、会议室相邻墙体为240 mm加厚砖墙。
  - 会议室、办公区的墙体和门均为12 mm加厚玻璃。
  - 卫生间门均为40 mm实木门。
- 区域调整。
  - 重点覆盖区域：办公区、会议室、活动区；信号强度≥ -65 dBm。
  - 次要覆盖区域：杂物间、茶水间、卫生间、设备间；信号强度≥ -80 dBm
  - 设定区域覆盖人数、带宽需求及终端类型。
- 干扰源、AP以及接入交换机点位设定。
  - AP点位可以自动部署，也可手动部署，障碍物与区域设定的越详细，AP自动布放就越准确。
  - 干扰源按工勘确定位置、高度、功率及天线信号强度来设定。
  - 一台交换机部署于设备间，另一台部署在杂物间。

- AP参数设定。
  - AP的安装高度，默认吸顶安装，高度为2.6 m，活动区域壁挂安装AP，高度为2.5 m。
  - 活动区域AP朝向需综合调整，使得整个活动区域被最少数量的AP覆盖。

使用WLAN Planner进行信号仿真

- 基于输入的建筑大小、障碍物、AP设备以及干扰源情况进行信号仿真，根据初步规划的AP数量，进行微调，确定最终AP数量以及点位。
  - AP可以自动布放，但可能布放不合理，可以先进行自动布放，然后手动调整数量和点位。
  - AP布放需注意活动区不能吸顶布放，只能壁挂部署，壁挂部署AP需调整好天线角度，室内壁挂可微调AP朝向。





WLAN项目详细设计方案LLD（1）

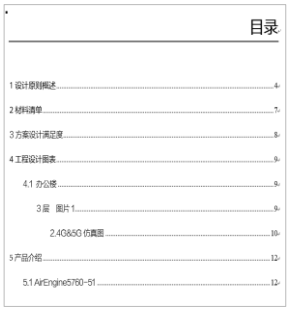
方案架构	内容		描述
项目概述	项目背景		为了提高办公效率，给办公室进行WLAN网络覆盖，覆盖区域面积大约为2500 m^2，覆盖总人数为400人左右，前期客户选定一个试点区域完成了WLAN覆盖设计和报价，客户满意该方案，目前开展项目后续事宜。
	网络建设目标		完成新办公区WLAN网络覆盖，满足客户的业务需求。
需求分析	网络现状		新建WLAN网络，层高约2.6米，镂空层高度为15米，现在室内覆盖区域有2个其他无线信号。
	覆盖目标		全部使用室内型AP，除活动区域外，均使用吸顶部署。 重点区域：重点覆盖区域：两个办公区域，四个会议室，一个活动区；信号强度≥ -65 dBm。 次要覆盖区域：两个茶水间，两个卫生间，一个设备间，一个杂货间；信号强度≥ -80 dBm。 每个办公区域有200人，每人2台终端，并发率70%。 每个会议室有30人，每人2台终端，并发率50%。 每个活动区域有100人，每人1台终端，并发率60%。 其他区域仅需考虑6人，每人1台终端，并发率50%。
	业务需求		正常上网业务，场强、带宽、漫游等无特殊要求。但需要通过划分SSID等方式，实现带宽控制。
	特殊需求		针对WLAN无线网络的QoS设计，员工的带宽为16 Mbps，访客的带宽限制为2 Mbps。
勘测数据	传输损耗数据	自由空间损耗	20 m距离会导致信号强度小于-65 dBm，重点覆盖区域需注意。
		穿透损耗	240 mm混凝土2.4GHz的衰减为25 dB，5 GHz的衰减为30 dB。240 mm砖墙2.4GHz的衰减为15 dB，5GHz的衰减为25 dB。80 mm有色厚玻璃2.4 GHz的衰减为8 dB，5 GHz的衰减为10 dB。40 mm木门2.4 GHz的衰减为3dB，5GHz的衰减为4 dB。
	干扰源		2.4 GHz支持802.11n，功率为25 dBm，信道1。5 GHz支持802.11ac wave2，功率为28 dBm，信道149。 安装高度为1 m。

WLAN项目详细设计方案LLD（2）

方案架构	内容		描述
网络设计	组网结构		附上WLAN网络的组网结构图。
	容量规划		每位用户16 Mbps，单AP规划接入23位用户。
	AP位置规划		附AP点位图。
	安全策略		员工接入网络认证需使用802.1X认证，访客使用Portal认证。
	设备需求		AP使用38个AirEngine5760-51，PoE交换机使用2台S5731-S24P4X。
	信号仿真图		附图
	参数规划	信道规划	附WLAN物料清单，AP参数规划。
		VLAN规划	附管理VLAN、业务VLAN、互联VLAN，设备管理VLAN表。
		IP规划	附设备各接口IP地址表。
		命名规则	附设备型号、位置及设备名称。
		参数汇总	QoS、SNMP参数
部署建议	线缆部署	线缆铺设	附线缆走线图。
		安装要求	天花板走线，可钻孔。
	设备部署	AC部署	AC部署在设备间，上架部署。
		AP部署	AP按点位图部署，镂空区壁挂部署。
		测试用例设计	附测试用例。

输出WLAN网络规划方案

- 完成WLAN方案的规划和设计后，输出网规方案和物理清单：
  - 《Test WLAN规划报告》


目录

1 设计原则概述 4
2 材料清单 7
3 方案设计满足度 8
4 工程设计图表 9
4.1 办公楼 9
3层 图片1 9
2.4G&5G 仿真图 10
5 产品介绍 12
5.1 AirEngine5760-51 12

  - 《Test 物料清单》

区域	楼层	物料类型	物料型号	数量	BOM编码	备注
汇总		室内AP	AirEngine5760-51	38		
		交换机	S5731-S24P4X	2		
办公楼	楼层汇总	室内AP	AirEngine5760-51	38		
		交换机	S5731-S24P4X	2		
	3层图片1	室内AP	AirEngine5760-51	38		
		交换机	S5731-S24P4X	2		

AP名称	AP型号	射频类型	输出功率	信道	天线高度(米)	方位角°	下倾角°	.....
AP-1	AirEngine 5760-51	2.4 G	18 dBm	13	2.6	0	0	
		5 G	24 dBm	60	2.6	0	0	
		5 G	21dBm	157	2.6	0	0	
AP-2	AirEngine 5760-51	2.4 G	18 dBm	9	2.6	0	0	
		5 G	24 dBm	52	2.6	0	0	
		5 G	21 dBm	149	2.6	0	0	

完善WLAN详细设计方案LLD

- 基于《WLAN项目规划方案》和用户需求，输出《WLAN详细设计方案LLD》，包含：

事项	说明
设备清单	设备具体型号、数量、功能描述、可用于采购的编码以及设备到货周期等。
设备基本信息	机架号、设备类型、设备型号、设备名称、设备IP、管理协议、用户名密码等。
机柜逻辑布局	不同机架中不同设备的安装位置，需标注功率和重量等。
网络拓扑	项目的逻辑拓扑以及物理接线图。
网络侧连接表	设备功能、本端设备、本端端口、本端接口带宽、本端接口类型、本端Eth-Trunk ID、本端IP。 对端设备、对端端口、对端接口带宽、对端接口类型、对端Eth-Trunk ID、对端IP。
IP地址规划	设备、管理地址、互联地址、业务VLAN、业务地址等。
其他信息	设备名称、协议、协议参数等。

WLAN项目详细设计方案LLD（1）

方案架构	内容		描述
项目概述	项目背景		为了提高办公效率，给办公室进行WLAN网络覆盖，覆盖区域面积大约为2500 m^2，覆盖总人数为400人左右，前期客户选定一个试点区域完成了WLAN覆盖设计和报价，客户满意该方案，目前开展项目后续事宜。
	网络建设目标		完成新办公区WLAN网络覆盖，满足客户的业务需求。
需求分析	网络现状		新建WLAN网络，层高约2.6米，镂空层高度为15米，现在室内覆盖区域有2个其他无线信号。
	覆盖目标		全部使用室内型AP，除活动区域外，均使用吸顶部署。 重点区域：重点覆盖区域：两个办公区域，四个会议室，一个活动区；信号强度≥ -65 dBm。 次要覆盖区域：两个茶水间，两个卫生间，一个设备间，一个杂货间；信号强度≥ -80 dBm。 每个办公区域有200人，每人2台终端，并发率70%。 每个会议室有30人，每人2台终端，并发率50%。 每个活动区域有100人，每人1台终端，并发率60%。 其他区域仅需考虑6人，每人1台终端，并发率50%。
	业务需求		正常上网业务，场强、带宽、漫游等无特殊要求。但需要通过划分SSID等方式，实现带宽控制。
	特殊需求		针对WLAN无线网络的QoS设计，员工的带宽为16 Mbps，访客的带宽限制为2 Mbps。
勘测数据	传输损耗数据	自由空间损耗	20m距离会导致信号强度小于-65 dBm，重点覆盖区域需注意。
		穿透损耗	240 mm混凝土2.4 GHz的衰减为25 dB，5 GHz的衰减为30 dB。240 mm砖墙2.4 GHz的衰减为15 dB，5 GHz的衰减为25 dB。80 mm有色厚玻璃2.4 GHz的衰减为8 dB，5 GHz的衰减为10 dB。40 mm木门2.4 GHz的衰减为3 dB，5 GHz的衰减为4 dB。
	干扰源		2.4 GHz支持802.11n，功率为25 dBm，信道1。5 GHz支持802.11ac wave2，功率为28 dBm，信道149。 安装高度为1 m。

WLAN项目详细设计方案LLD（2）

方案架构	内容		描述
网络设计	组网结构		附上WLAN网络的组网结构图。
	容量规划		每位用户16 Mbps，单AP规划接入23位用户。
	AP位置规划		附AP点位图。
	安全策略		员工接入网络认证需使用802.1X认证，访客使用Portal认证。
	设备需求		AP使用38个AirEngine5760-51，PoE交换机使用2台S5731-S24P4X。
	信号仿真图		附图
	参数规划	信道规划	附WLAN物料清单，AP参数规划。
		VLAN规划	附管理VLAN、业务VLAN、互联VLAN，设备管理VLAN表。
		IP规划	附设备各接口IP地址表。
		命名规则	附设备型号、位置及设备名称。
		参数汇总	QoS、SNMP参数
部署建议	线缆部署	线缆铺设	附线缆走线图。
		安装要求	天花板走线，可钻孔。
	设备部署	AC部署	AC部署在设备间，上架部署。
		AP部署	AP按点位图部署，镂空区壁挂部署。
		测试用例设计	附测试用例。

部署和调试

- 在完成网络方案的设计且通过评审后，需开始进行网络部署和调试。

注意事项	说明
设备安装	按照图纸上AP点位进行安装
	本项目中均为室内AP，大部分吸顶部署，活动区域覆盖AP需挂墙安装，安装需注意天线朝向
	WAC设备上架，注意部分型号需提前准备挂耳和特殊电源线缆。
	需检查设备牢固性、强弱电分离情况（强弱电线缆距离10 cm以上）以及标签的完整性等。
设备调试	配置调试在模拟器或镜像环境中完成，进行配置的可行性验证。
	设备命名建议包含：所在机房、机架、设备功能、层次、型号以及编号等内容，便于识别。
	若设备存在配置，应做好备份。

网络优化

- 网络调试和部署完成后，需对现场WLAN网络质量进行内部校验，不符合要求的部分需进行网络优化。重点需要优化：
  - AP信道和功率自动调优。
  - 漫游优化。
  - 用户限速校验。
  - 会议室高密的AP Beacon周期调整。
  - 访客区域的STA老化时间调整。
  - 低信号用户强制下线。
  - ...

验收（交付）测试

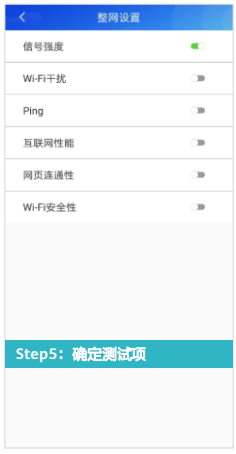
验收标准	验收内容	说明
信号覆盖验收准则	覆盖区域场强要求	对用户主要上网区域的信号覆盖强度要求在-40~-65 dBm之间。
	边缘场强要求	要求信号覆盖的90%区域内信号质量良好，覆盖区域内边缘场强大于-75 dBm。
	同频干扰场强要求	在用户上网房间内，如果存在同频AP场强干扰，要求干扰源小于-80 dBm。
	信噪比要求	信噪比大于20 dB
基本业务验收准则	网络时延波动	通过ping包方式验证网络时延波动，波动在允许范围以内。
		总时延在允许范围以内
		Ping丢包率小于5%
	吞吐量要求	信号覆盖良好区域，单用户下载基本能够达到下发的理论值。
	AP间要求漫游	STA在各AP覆盖区域间漫游，不中断业务，2 Mbps下载速率应感知不到波动。

CloudCampus APP验收

- 若无特殊需求，也可使用CloudCampus APP进行验收。

Step1：点击工具—验收
Step2：使用support网站账号登录
Step3：点击想要编辑的工程

Step4：在“验收”视图选择楼层，选择右上角设置



Step5：确定测试项

Step6：找到图纸上自身处于的实际物理位置，点击打点

HUAWEI

网络建设项目验收报告

- 工程文档:
  - 《网络规划表》
  - 《网络建设方案》
  - 《项目安装报告》
  - 《项目实施报告》

客户单位（甲方）	**A公司**	
项目实施单位（乙方）	X网络技术公司	
项目实施服务内容	于2021年12月10日完成到货验收	☑是 □否 □不涉及
	完成设备硬件安装和软件调测	☑是 □否 □不涉及
	完成产品维护现场讲解和培训	☑是 □否 □不涉及
	完成业务上线/割接	☑是 □否 □不涉及
	工程文档、工程帐号和密码已移交客户，并提醒客户修改帐号和密码	☑是 □否 □不涉及
	客户在实施前已对工程实施方案进行了确认	☑是 □否 □不涉及
	项目实施进度和人力投入满足客户要求	☑是 □否 □不涉及
	试运行情况	☑是 □否 □不涉及
甲方签章: **日期: 年 月 日**		**服务方签章:** **日期: 年 月 日**

室外WLAN项目背景

- 某市中心步行街，经过与社区的接口人详细沟通，该项目情况如下：
  - 项目图纸如右图，是典型的室外WLAN覆盖场景，步行街长200米。
  - 无线WLAN网络应重点覆盖区域只有步行街，商铺不覆盖。
  - 步行街每天的人流量最大为800人，并发率为60%，每位游客的平均业务类型见右表，本项目仅需考虑优异的网络体验。
  - 无线网络需支持802.11ax标准，仅需支持5GHz频段，频宽为40 MHz。
  - 交换机可以部署在任意商铺2楼；步行街位置不能新增线杆，AP只能壁挂在商铺外墙。
  - 游客的终端类型仅需考虑手机，认证方式均为Portal认证，且客户希望游客漫游过程中，不需要反复进行Portal认证。

业务类型	单业务基线速率（Mbps）		占比
	优异	良好	
网页浏览	8	4	40%
流媒体（1080P）	16	12	20%
VoIP（Voice）	0.25	0.125	20%
游戏	2	1	10%
即时通讯	0.5	0.25	10%

WLAN站点勘测信息分析

- 现场工勘信息汇总如下：
  - 外层墙体等为240 mm混凝土，但室外AP无需穿透障碍物，AP可壁挂到墙体上。
  - 各家商铺都自有Wi-Fi网络，现场存在大量干扰源，如右图所示干扰源标注，干扰源布置高度0.85米，2.4GHz功率21 dBm，5 GHz功率24 dBm。
  - 交换机可以布置在商铺二楼任意位置，AP可以使用PoE供电。
  - 商铺3和商铺8的外墙有装饰物，无法壁挂AP和天线。
  - 自由空间的信号衰减测试见右图。

距离 (m)	2.4G路径损耗 (dB)	5G路径损耗 (dB)
50	76.4	84
100	84.2	91.9
200	92	99.7
300	96.6	104.2
500	102.4	110
800	107.7	115.4
1000	110.2	117.9

WLAN项目输出件

- 基于以上场景输出室外WLAN网络规划，输出内容需包含：
  - WLAN项目需求收集表

  - WLAN项目工勘信息收集表

  - 概要设计方案HLD

  - 详细设计方案LLD

思考题

1. 室内场景的WLAN网络规划与室外场景的差别是什么?
2. 信道规划时，应该考虑哪些因素？为什么?
3. 现场勘测干扰源时，应该注意什么?

HUAWEI

- 室内场景的WLAN网络规划与室外场景的差别是什么?
  - 室内场景仅需要室内建筑平面图，室外场景仅有平面图可能不够还需要坐标。
  - 室内场景可以轻松测试信号衰减情况，室外场景障碍物过大，往往需避开障碍物或者预估障碍物高度，提高天线位置。
  - 室外场景还需考虑供电、线缆布线、防水、防雷、防尘、天线选型等等问题
- 信道规划时，应该考虑哪些因素？为什么?
  - 干扰，最简单的应该避开同频和临频干扰，比如1, 5, 9, 13，149~165等，同时应该注意法律法规限制，不同国家规定不同，比如中国室外5GHz频段不可以使用36信道，室内可以。
  - 频宽，20MHz，40MHz，80MHz以及160MHz，不同场景需求不同，更大的频宽更适合对带宽有高要求的用户。
  - 功率，往往和信道规划一起，过大功率也会带来不必要的干扰问题。
- 现场勘测干扰需注意记录干扰的高度、频段、频宽、功率、朝向等信息，便于部署AP的时候减少干扰。

本章总结

- WLAN项目生命周期中，均需标准流程及相应交付件保障规范运作。通过专业工具完成简单高效的无线网络规划；主动运维，从整体到局部的用户360质量感知；端到端故障诊断，从而达到对无线网络的高效排障。
- 本章侧重WLAN项目的生命周期介绍，目的是让考生熟悉在WLAN项目的不同阶段需要工程师去完成或者输出哪些交付件，交付件应该包含哪些内容，考生应该熟悉WLAN Planner等规划工具的使用，才能高效完成不同WLAN项目的规划与设计。

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

HUAWEI