

XXX 学院无线校园网

建 设 方 案

郑州向心力通信技术股份有限公司

日 期：2017 年

目录

1	公司概况	3
2	项目概况	10
3	方案设计	12
4	敏捷基础网络方案	15
5	WLAN 规划设计.....	18
6	设备简介	29
7	方案优势	30
8	客户价值	35
9	设备清单	36
10	类似项目案例一览表	36

1 公司概况

✚ 郑州向心力通信技术股份有限公司

地址：郑州市高新区莲花街 5 号 B 区 B 座

行业：通信及 IT&软件

电话：（86）37167008600 员工数量：720

网址：www.centfor.com 邮箱地址：info@centfor.com

✚ 业务概要

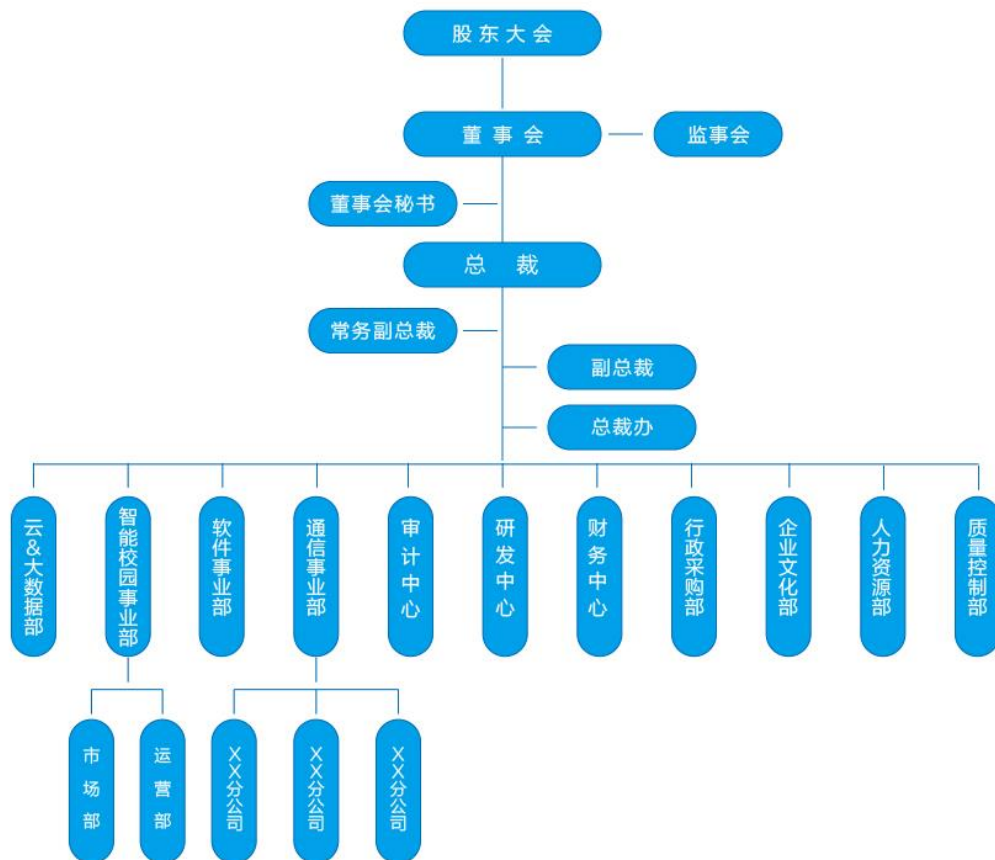
郑州向心力通信技术股份有限公司是中国卓越的通信及 IT&软件综合服务提供商，拥有八年的通信及 IT&软件服务经验。公司成立于 2000 年 10 月 1 日，前身为“向心力信息技术股份有限公司”注册资本为陆仟壹佰万圆整，在 2010 年重新注册为“郑州向心力通信技术股份有限公司”。总部设在中国河南郑州。随着公司规模不断扩大，公司海外业务范围涉及 20 多个国家，在中国香港设有全资子公司，并在中国大陆设有多个分支机构。2004 年初始向心力开始开拓海外市场，目前已设立亚太、拉美地区部，公司选派优秀员工奔赴印度尼西亚、阿根廷、巴西、葡萄牙、西班牙、印度、罗马尼亚等地区为客户提供专业的技术服务。

✚ 其业务领域涵盖：

- IT 系统集成服务
- 软件开发及服务外包服务
- 通信产品网络建设服务
- 通信产品网络规划优化服务
- 通信产品工程勘察服务
- 通信产品运行维护服务
- 通信产品机房搬迁、整改服务
- 通信产品技能提升培训服务
- 通信行业咨询服务

集团架构

向心力组织结构图



向心力技术秉承“立足国内、放眼全球”的战略发展思路，“专注于通信、IT 行业技术服务、持续为客户创造价值”的经营理念，以坚实的技术实力，对客户业务范围充分理解，以及高效的实施队伍，为全球通信运营商、设备提供商、大型集团客户等，提供全面业务的解决方案，定制化或产品化的专业通信及 IT&软件服务。在全球电信运营商及集团企业等拥有大量的成功案例。

公司文化

✚ 我们的愿景

向心力技术将整合全球通信及 IT&软件资源，立足中国，以通信及 IT&软件为核心，持续提升员工的职业化素养，开拓全球的通信及 IT&软件市场，以广泛的战略合作联盟为基础，全力打造中国通信及 IT&软件服务外包行业的洲际航母，与客户、投资者和我们的团队一起分享创造价值的喜悦。

✚ 使命

帮助客户持续盈利

核心价值观

客户	以感恩之心服务于客户，赢得客户尊重
员工	我们是一个团队
工作	一次性把工作做好；持续改进
创新	唯有创新，方能生存

经营理念

团队、服务、贡献、发展

核心竞争力

高效率、弹性、面向客户需求的供应链和管理平台

1.1.1 部门简介

智慧校园事业部概况

致力于为高校系统集成解决方案。专注于提供包括：无线覆盖投资运营、实训室建设、网络、服务器、存储与虚拟化管理、数据保护、信息安全、视频监控等在内的企业信息化服务与技术支持高校。

部门成立以来，一直以客户为导向、以服务为基础，不断优化产品、市场、技术、服务等全方位的支持体系，为客户提供企业级的、最有价值的软硬件产品、专业的 IT 解决方案。提供包括咨询、工程规划与实施、IT 系统优化和管理、技术培训等多层次的服务和专业的技术支持。

业务领域涵盖

智慧校园、通信服务、软件开发、IT 系统集成及服务外包。

人员素质

作为一流的信息安全服务提供商，向心力十分重视技术支持与售后服务，并且拥有一大批精通技术且实践经验丰富的技术支持人员。

- 两年以上的技术支持与服务工作经验
- 三年以上的计算机系统集成经验，针对各项集成技术都有深入的了解
- 对待工作认真负责，信守“客户至上”的原则
- 大学本科以上学历

技术支持与服务

雄厚的资源

向心力软件事业部承担着向心力及合作伙伴的产品和系统的技术支持与维护，通过

向心力维修服务网和热线支持服务网等多种形式，向用户提供及时优质的服务。向心力维修中心及客户服务支持中心随时为客户排忧解难，与厂商配合，做到备件更换及时、维修及时。

充足的研发力量和技术储备

作为知名的信息安全服务提供商，向心力时刻注意跟踪计算机领域最新技术，组织了专门的研发队伍，有针对性的对各类创新计算机产品进行研究和开发工作，并且及时购买代表技术趋势的新产品设备，组建相应试验环境，确保公司的技术人员在第一时间内掌握最新技术和产品的使用。另外，公司每年都会投入大量资源与设备厂商合作，有针对性的组织大规模技术人员培训，提高技术人员的素质，确保为用户提供高质量的系统集成和技术支持服务。

良好的合作伙伴关系

随着计算机领域的行业划分越来越细，即使是大型的专业公司也不可能在所有方面均处于领先地位，为了给用户提供最优秀的整体解决方案，向心力与世界上众多的计算机、信息安全、软件公司保持着良好的合作关系，如华为、飞想、锐捷、3COM、IBM、HP、Compaq、SUN、VMWare、Oracle、Juniper 等。通过与厂商建立共同的业务关系，包括合作开发、共同的市场和销售方案以及综合的技术支持模式等，向心力和主要的合作伙伴能够提供对关键业务的整体解决方案，以满足客户的各种需要，在技术支持与服务过程中需要与设备厂商协调时，向心力将具有明显的便利条件。

丰富的系统技术支持与售后服务经验

向心力承担过多个大型信息系统的建设工作，在系统实施过程中以及后期的技术支持工作中，我们的技术支持人员同各级技术人员进行了广泛的交流，积累了大量的技术支持和售后服务经验。

充足的备件资源

在多年的网络安全系统建设过程中，为了保证网络安全系统的可靠、正常运行，向心力建立了相应的备品备件库，已经准备了充足的备件资源。如果向心力能够有幸成为此次工程的信息安全服务提供商，我们可以充分发挥现有优势，合理调配各地资源，组建大规模的系统技术支持队伍和备品备件体系。

部分荣誉和大事记

- ◆ 2016 年 3 月 30 日，向心力公司荣获河南省住房和城乡建设厅颁发的电子与智能化工程专业承包贰级资质
- ◆ 2015 年 7 月 1 日，向心力公司顺利通过 ISO27001 信息安全管理体系认证

- ◆ 2015 年 2 月，向心力公司荣获河南省软件服务业协颁发的 2014 年度河南省优秀软件企业证书
- ◆ 2015 年 2 月，向心力公司的“向心力信息化项目管理系统 V1.0”荣获河南省软件服务业协颁发的 2014 年度河南省优秀软件产品证书
- ◆ 2015 年 1 月，向心力公司荣获中国信息安全认证中心颁发的信息安全风险评估一级服务资质
- ◆ 2014 年 12 月被河南省电子学会授予 2014 年河南省电子信息行业科技创新先进单位
- ◆ 2013 年 3 月 12 日，向心力公司顺利通过了由河南省科学技术厅、财政厅、河南省国家税务局、地方税务局四部门联合组织的 2012 年度高新技术企业认证
- ◆ 2013 年 1 月 18 日，向心力公司荣获中华人民共和国工业和信息化部颁发的通信信息网络系统集成企业甲级资质证书
- ◆ 2012 年 2 月 8 日，向心力软件研发中心开工奠基
- ◆ 2011 年 11 月 28 日，向心力公司通过“防雷工程专业施工/设计丙级资质单位”评定
- ◆ 2010 年 12 月 7 日，向心力公司安全生产许可证获批
- ◆ 2010 年 11 月 19 日，向心力公司通过“通信信息网络系统集成企业(乙级)”资质认证
- ◆ 2010 年 9 月 20 日，经工业和信息化部审核、河南省住房和城乡建设部批准，我公司喜获“通信工程施工总承包三级”资质
- ◆ 2010 年 8 月，郑州向心力通信技术股份有限公司被推选为河南省电子学会理事单位
- ◆ 2010 年 7 月，向心力经过国家工信部核定，获得计算机信息系统集成企业二级资质。
- ◆ 2010 年 5 月，向心力被郑州市科学技术局授予“郑州市移动应用工程技术研究中心”。
- ◆ 2010 年 3 月，向心力经过中国信息安全测评中心审核，正式通过了国家信息安全服务资质(安全工程类一级)认证，此证书的颁发表明对我司安全保障能力的权威认可。
- ◆ 2010 年 2 月 4 日，向心力荣升华为公司“2009 年度金牌合作伙伴”，同时

荣获“2009 年度 WCDMA 3G 网络建设奖”

- ◆ 2009 年前三季度销售合同金额首次突破亿元。
- ◆ 2009 年 10 月，向心力公司被郑州市人民政府授予“高校毕业生就业见习基地”牌匾。
- ◆ 2009 年元月，成功获得美国卡纳基—梅隆大学软件工程研究所 CMMI Level 3 的认证。
- ◆ 2009 年元月，“郑州向心力通信技术有限公司”更名为“郑州向心力通信科技股份有限公司”，标志着向心力股份制改制成功。
- ◆ 2008 年 11 月，向心力公司通过河南信息产业厅的“双软”认证。
- ◆ 2008 年 11 月，被郑州市政府认定为 50 户高成长型高新技术企业和郑州市重点服务外包企业。
- ◆ 2008 年 10 月 1 日，黑龙江代表处、吉林代表处正式成立。
- ◆ 2008 年 10 月，河南省政协副主席龚立群到向心力公司考察工作，对向心力自主创业给予了肯定，并对向心力的发展寄予厚望。
- ◆ 2008 年 6 月，向心力公司正式入驻中国郑州经济技术开发区河南信息产业园，办公面积达 3100 多平方米。
- ◆ 2008 年 5 月，汶川 8.0 级地震，牵动着向心力人的心，公司及员工向灾区捐款 15 万元，表达对灾区人民的祝福，承担起企业公民的责任。
- ◆ 2008 年 2 月，在服务业发展会上，省委书记人大常委会主任徐光春在听取了软件服务代表性企业向心力技术董事长赵国庆的汇报后，对向心力公司给予了高度评价，并对公司未来的发展寄予厚望；
- ◆ 2007 年 12 月，向心力技术与印度知名软件企业 Cellent 公司，签订战略合作协议，合作方向主要包括软件服务外包业务、高端客户业务开拓等；
- ◆ 2007 年 11 月，向心力技术作为服务外包企业重要代表应邀参加中国郑州国际服务外包高层论坛；
- ◆ 2007 年 10 月，向心力技术与美国独资软件企业速索公司签订了战略合作协议；
- ◆ 2007 年 9 月，郑州市委书记王文超亲切接见向心力技术董事长赵国庆，并对向心力技术作为河南软件服务代表企业的未来发展寄予了厚望；
- ◆ 2007 年 1 月，向心力技术获得通信信息网络系统集成企业乙级资质证书；
- ◆ 2006 年 12 月，向心力技术成为华为技术有限公司最大的通信工程服务外包

商，同时也成为中国最大的专业通信技术服务提供商；

- ◆ 2005 年初，向心力技术与华为技术有限公司共同成立中国唯一的 3G 培训实习外场；
- ◆ 2004 年初，向心力技术宇信培训中心，成为华为技术有限公司授权培训中心，致力为通信领域培养专业技术人才；
- ◆ 2004 年 07 月，向心力技术通过中国检验认证集团质量认证，并获得 ISO9001 证书；
- ◆ 2003 年 05 月，向心力技术被授予高新技术企业称号；

我们的优势

- ◆ 专业化的核心管理团队，拥有丰富的技术经验；
- ◆ 充满朝气的团队，员工平均年龄 27 岁，70%为本科及以上学历；
- ◆ 丰富的行业经验和技术服务水平，在服务器、存储、视频会议、安全等领域尤为突出；
- ◆ 丰富的厂商资源及产品线，广泛的业务合作伙伴；
- ◆ 严格的质量控制体系与知识产权保护；
- ◆ 公司总部设在河南郑州，有充足的资源来保障项目的顺利实施和售后技术支持。客户背景

2 项目概况

本次项目主要针对学院现有的办公楼、宿舍楼、广场、餐厅及其周边区域实现 WLAN 信号的全覆盖，要求 WLAN 网络能够提供稳定的信号覆盖，高效的数据传输，同时 WLAN 网络要和学校当前的网络进行互通，并且实现学校整体网络的统一管理，运维。

本文档以下内容将依照上述需求，对 WLAN 网络建设提供技术建议书。

2.1 解决方案理念概述

针对网络面临的新挑战，华为提出了敏捷网络解决方案来支持网络的高速发展。

敏捷网络的设计理念包括：

- 具有敏捷结构的网络方案

-无阻塞架构

华为的解决方案中，使用全千兆的方案，来支撑网络流量的爆炸式增长，满足未来虚拟化和云计算的带宽需求。无阻塞的网络架构保证网络的业务质量。

-有线无线一体化运营

华为设计的解决方案中，运维管理非常方便，支持有线/无线网络统一管理，同时可靠性极高，给用户最好的上网体验。

- 优化运维解决方案

使用 eSight 网管，可实现对整网的拓扑管理、网络资源管理、性能管理、故障管理和配置管理。eSight 提供强大的报表功能，为判断运维趋势、发现问题提供了强有力的支持。

- IPv6 平滑演进方案

华为全系列 IPv6 产品均为自主核心技术，提供双栈过渡技术、隧道互联技术和地址转换技术保证 IPv4 到 IPv6 的平滑过渡。

2.2 设计原则

漯河食品职业学院 WLAN 网络系统将本着以下原则进行设计建设：

- 超前性与实用性结合

网络技术发展迅猛，如果设备缺乏先进性，设备可能很快落后甚至被淘汰，但也不能过分超前，以避免造成投资的浪费。为此，在网络建设中，需注意超前性与实用性结合，确保投资有效，使之能真正发挥出相应的作用。

- 安全性与可靠性

在网络建设中，安全性是整个网络建设中的重中之重，要通过各种技术确保系统应用的安全性以及内容的安全性。同时，要求系统本身具有高度的可靠性，这样才能保证网络客户的应用

- 可管理性

网络管理是一个长期的投资，在网络建设中对网络可管理是一项重要的应用原则，通过选择全网的可管理性软件，减少日常维护费用。

- 可扩展性

网络不但需要能够满足当前需要，随着后续业务的改变、技术的发展，未来网络需要承载更多的业务及提供更多的优质服务。所以，网络的可扩展性是网络建设中必须提前规划的重点。

3 方案设计

3.1 网络架构设计原则

XXX 学院 WLAN 网络系统的架构设计，需遵循如下原则：

- 层次化

将网络划分为核心层、接入层。每层功能清晰，架构稳定，易于扩展和维护。

- 模块化

将网络中的每个区域或者每个功能区划分为一个模块，模块内部的调整涉及范围小，易于进行问题定位。

- 冗余性

关键设备采用冗余设计；关键链路采用 Trunk 方式冗余备份或者负载分担；关键设备的电源、主控板等关键部件冗余备份。提高了整个网络的可靠性。

- 可管理性和可维护性

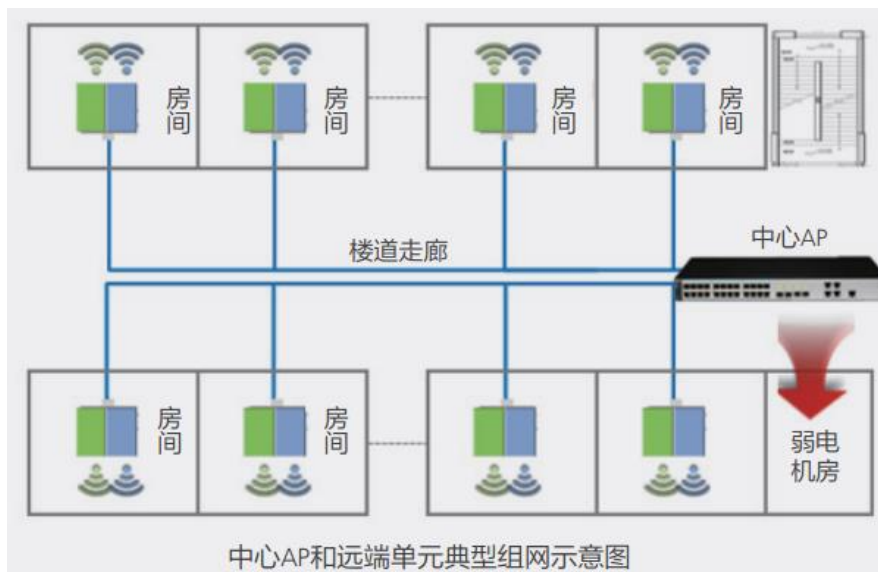
为了易于管理，可选择适用于全网的网管软件来管理网络。为了便于维护，应尽可能选取集成度高、模块可通用的产品。

3.2 网络架构设计

3.2.1 设计方案



网络架构设计



如上图所示，组网说明如下：

WLAN 网络核心区：主要部署 WLAN 网络核心交换机，无线控制器，网管平台。在本方案中，建议部署华为集成无线控制器的 S12710 核心交换机和 eSight 网管平台。由 S12710 核心交换机负责 WLAN 网络所有的数据的转发，同时与学校现网联通，在学校的网络管理策略框架内与现网数据进行交换。eSight 负责 WLAN 网络所有设备的管理和维护，如果有必要，可以将学校现网一并纳入，实现有线网络和无线网络的统一管理。

AP 信号覆盖：室内覆盖采用华为的 AP9430 敏捷分布式无线覆盖。

3.2.2 组网优势

采用上述方案的组网方式，具有如下优势：

- 网络架构各个区域模块化，网络可独立维护。
- 采用分层拓扑，架构稳定，易于扩展和维护。
- 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。
- 重要节点及链路层冗余设计，保证网络的可靠性。
- 支持各种终端接入，统一管理，一张 IP 网络承载所有业务。

4 敏捷基础网络方案

基础区域网络是整个网络的枢纽，覆盖整个网络，连接着各个区域。承担了内部数据流量和对外数据流量，在逻辑上成为可靠性、安全设计的中心。

4.1 基础网络整体规划

基础网络区域建议采用核心层、接入层的架构模型，具有如下的优势：

- 二层设计

基础网络部分逻辑上采用了扁平化的大二层结构，不需要维护复杂的网络架构与协议。

- 层次化设计

有核心层接入层，每层功能清晰，架构稳定，易于扩展和维护。

- 模块化设计

每一个模块为单个业务网络系统，模块内部调整涉及范围小，定位问题也容易。

- 冗余性设计

关键节点冗余性设计，适当的冗余性提高可靠性，过度的冗余不便于运行维护。

- 对称性设计

网络的对称性便于业务部署，拓扑直观，便于设计和分析。

4.2 VLAN 规划

VLAN 概述

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。

基于网络内拥有比较多不同的业务类型，并且不同类型网络使用者也有很大差别，因此进行 VLAN 的合理规划将可以帮助建设一个稳定运作的网络。

按功能划分 VLAN

在网络中，可以按功能将 VLAN 划分为以下几种：

- 管理 VLAN

网络中的交换机需要划分管理 VLAN，在管理 VLAN 中配置 IP 地址，以便日常维护。管理 VLAN 要与用户 VLAN 严格区分。

- 用户 VLAN

用户 VLAN 指为终端接入用户划分的 VLAN，针对网络中不同区域，划分不同的 VLAN；以满足 VLAN 内用户的直接互访需求。如果有访问控制的需求，建议使用 MUX VLAN 技术，实现 VLAN 内部用户部分互通，部分隔离。

- Voice VLAN

Voice VLAN 是为用户的语音数据流划分的 VLAN，用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，便于对语音流进行有针对性的 QoS 配置，提高语音流量的传输优先级，保证通话质量。

- Guest VLAN

网络中用户在通过 802.1x 等认证之前接入设备会把该端口加入到一个特定的 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，只能访问有限的网络资源。用户从处于 Guest VLAN 的服务器上可以获取 802.1x 客户端软件，升级客户端或执行其他应用升级程序（例如：防病毒软件、操作系统补丁程序等）。认证成功后，端口离开 Guest VLAN 加入用户 VLAN，用户可以访问其特定的网络资源。

- Multicast VLAN

Multicast VLAN 即组播 VLAN，组播交换机运行组播协议时需要组播 VLAN 来承载组播流。组播 VLAN 主要是用来解决当客户端处于不同 VLAN 中时，上行的组播路由器必须在每个用户 VLAN 复制一份组播流到接入组播交换机的问题。

VLAN 规划原则

VLAN 划分的基本原则如下：

- 要严格区分业务 VLAN 和管理 VLAN。
- 按照不同的管理区域划分 VLAN,不仅方便隔离用户，也方便日常维护。
- 同一区域也要按照不同的业务类型来划分 VLAN,比如按照不同的接入方式来划分 VLAN。
- VLAN 需连续分配，以保证 VLAN 资源合理利用。
- 预留一定数目 VLAN 方便后续扩展。

4.3 IP 地址规划

IP 地址规划原则

IP 地址规划的基本原则如下：

- 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

连续地址在层次结构网络中易于进行路径叠合，大大缩减路由表，提高路由算法的效率。

- 扩展性

地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。

- 实意性

好的 IP 地址规划使每个地址具有实际含义，看到一个地址就可以大致判断出该地址所属的设备

IP 地址分类

- 业务地址

数据中心和 DMZ 区域中，服务器可能部分使用公网 IP 地址，需要将这些网段发布到公网。

内网用户的地址由核心交换机或者 DHCP 服务器统一分配。可以通过配置地址池来按用户所在区域分配 IP 地址。

内部用户中，为打印机、IP 电话等哑终端（IT 设备）分配固定 IP 地址，为网络设备划分固定 IP 地址，与终端用户的 IP 地址严格区分。

- Loopback 地址

为了方便管理，会为每一台路由器创建一个 Loopback 接口，并在该接口上单独指定一个 IP 地址作为管理地址。

Loopback 地址务必使用 32 位掩码的地址。

- 互联地址

互联地址是指两台网络设备相互连接的接口所需要的地址，设备互联的网段一般聚合后发布，而且没有必要发布给终端用户。

5 WLAN 规划设计

5.1 WLAN 覆盖需求分析

随着智能终端的飞速发展和普及，WLAN 覆盖已经是难以阻挡的趋势。根据不同的场景和不同的业务需求，对于 WLAN 覆盖的要求也有差异，需要根据差异性选择不同的 WLAN 设备进行部署，以达到最好的使用效果。

5.1.1 场景需求分析

主要覆盖场景中，笔记本、台式计算机、智能手机、平板电脑等多种类型 WIFI 无线终端，802.11a、802.11b、802.11g、802.11n 等多种标准的终端均可便捷接入，满足终端接入覆盖需求。

重点区域

重点覆盖区，满足 100% 用户并发，接入速率不低于 2Mbps；

双频覆盖，2.4GHz 和 5GHz 边缘场强均大于 -60dBm。

一般区域

一般覆盖区，满足 30% 用户并发，用户同时接入上网，并发接入速率不低于 1Mbps；

双频覆盖，2.4GHz 和 5GHz 边缘场强均大于 -75dBm。

5.1.2 无线应用需求分析

服务质量 QoS

无线漫游：覆盖区域内无线漫游，用户终端从一个 AP 覆盖范围移动到另一个 AP 覆盖范围，无需重新登录和认证；

精细化控制：不同的角色拥有不同的权限，且不同的角色之间要隔离，限制不同的角色互访（根据实际情况确定）；

多用户调度：AP 能感知接入用户数量，灵活调整物理信道竞争参数，降低碰撞几率，避免过多的用户接入同一 AP，保障服务质量和体验。

安全防护

无线安全加密：无线信号是开放的，任何人都可以接受到，存在数据被窃听，篡改等安全隐患，WLAN 无线网络需要支持 WEP、WPA/WPA2、WAPI 等加密认证方式，充分保证用户重要信息的私密性，数据传输的安全性。

无线入侵防护：为了更好的保证网络的安全性和可靠性，WLAN 无线网需要支持泛洪攻击、Spoof 攻击、暴力 PSK 破解、Weak IV 等 WIDS/WIPS 安全防护。

稳定可靠

AP 设备：室外 AP 设备的防尘、防水的防护等级达到 IP67 要求，同时 AP 自身内置 5kV 防雷器，减少工程施工和网络运维的困难。

AC 设备：AC 支持 1+1 热备份，解决 AC 单点故障问题。

网络链路：本地转发模式下，若遇到 CAPWAP 隧道中断、AC 故障、控制链路错误等问题时，AP 可进入半自治状态，继续对终端业务数据进行转发，业务不中断，保障用户体验。

认证

认证方式：认证系统需要支持 Portal、MAC、802.1x、PPPOE 等多种认证方式，以满足不同场景下，不同群体的接入认证需求。

与有线网络兼容

WLAN 网络必须考虑与有线网络之间的兼容，实现与现有系统使用同一个账号、密码进行认证，并获取相同的访问权限

运行维护

网络监控：通过网管软件查看当前设备物理拓扑，直接显示设备间连接关系，监控设备及链路状态。通过 WLAN 业务拓扑监控无线设备告警、状态、网络设备逻辑结构，包括 AC、AP、终端用户、非法 AP 的逻辑连接关系及其详细信息，并在拓扑提供一定故障诊断处理能力。

故障恢复：通过网管远程批量重启 AP，恢复 AP 配置。通过网管快速完成 AP 替换，替换后业务不变。

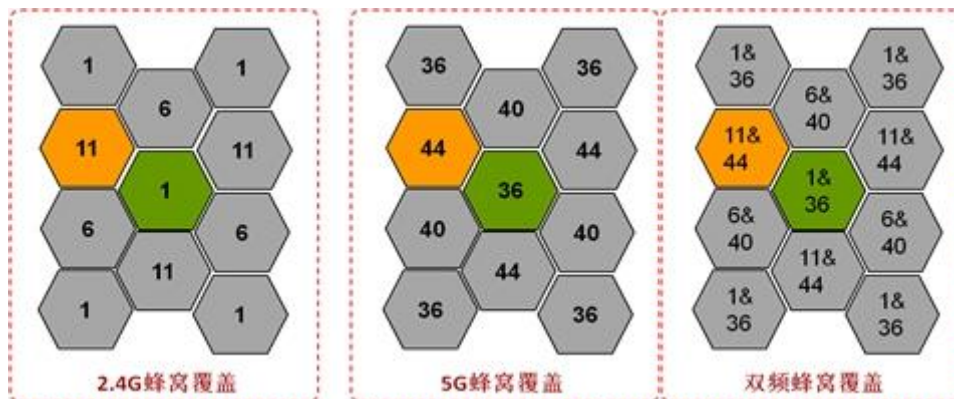
5.2 频点划分

为保证信道之间不相互干扰，无线网必须对 WLAN 信道进行统一规划并实施。WLAN 系统主要应用两个频段：2.4GHz 和 5.0GHz。2.4G 频段具体频率范围为 2.4~2.4835GHz 的连续频谱，信道编号 1~14，非重叠信道共有三个，一般选取 1、6、11 这三个非重叠信道。5.0G 频段分配的频谱并不连续，主要有两段：5.15~5.35GHz、

5.725GHz~5.85GHz。不重叠信道在 5.15~5.35GHz 频段有 8 个，分别为 36、40、44、48、52、56、60、64；在 5.725GHz~5.85GHz 频段有 4 个，分别为 149、153、157、161，可以根据实际部署情况，选择相应的非重叠信道。

5.3 信道覆盖

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



5.4 链路预算

WLAN 链路预算一般经过边缘场强确认，空间损耗计算，覆盖距离计算等步骤。边缘场强确认是指：在 WLAN 工程部署中，要求重点覆盖区域内的 WLAN 信号到达用户终端的电平不低于-75dBm。这样可以保障用户与 AP 的协商速率以及收发数据质量。

空间损耗计算通常采用如下公式： $Pr[dB] = Pt[dB] + Gt[dB] - Pl[dB] + Gr[dB]$ 。其中： $Pr[dB]$ 为最小接收电平，即为 AP 在不同传输速率下的接收灵敏度； $Pt[dB]$ 为最大发射功率； $Gt[dB]$ 为发射天线增益； $Gr[dB]$ 为接收天线增益； $Pl[dB]$ 为路径损耗（包括空间传播损耗、馈线传播损耗、墙体/玻璃阻挡损耗）。实际部署中终端天线增益不可知，为方便计算常忽略接收天线增益，而采用如下公式：到达用户端的信号电平=AP 发射功率+AP 天线增益-路径损耗。路径损耗主要指 WLAN 信号的空间损耗，空间损耗= $92.4+20\lg f+20\lg d$ （f: GHz, d: km）。由公式推算可知：

空间传输距离	100m	200m	300m	400m	500m	600m	1000m	100m
2.4GHz 信号 的空间衰减 (dBm)	80	86	89.5	92	94	95.5	100	80
5.8GHz 信号 的空间衰减 (dBm)	87.6	93.6	97.1	99.6	101.6	103.1	107.6	87.6

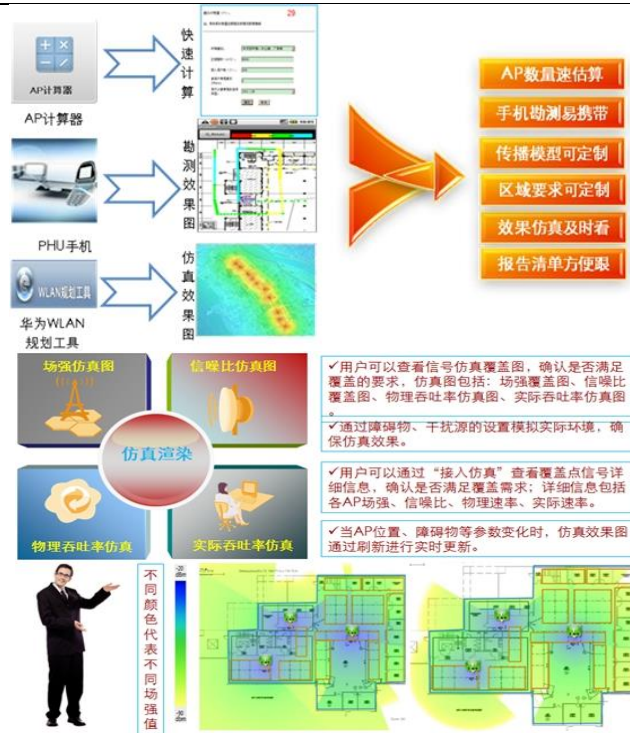
为便于理解链路估算的过程，这里给出一个室外场景覆盖和室内场景覆盖的预算案例：根据 WLAN 覆盖边缘场强的要求，到达终端用户的信号电平不低于 -75dBm ，500mW AP 的输出电平 27dBm ，天线增益 11dBi ，距离 AP 500m 处信号的衰减量 94dBm ，由于 $27+11-94=-56\text{dBm}$ ，大于 -75dBm ，因此在通常情况下，AP 的覆盖范围为 500m。由于数据通信是双向的，终端的信号发射功率相对 AP 较弱，综合考虑，一般建议室外 AP 的覆盖范围为 200m~300m。有些场景需要利用无线 AP 设备做桥接，华为 AP 桥接可以按照 3km~5km 规划。

根据 WLAN 覆盖边缘场强的要求，到达终端用户的信号电平不低于 -75dBm ，100mW AP 的输出电平 20dBm ，天线增益 4dBi ，距离 AP 60m 处信号的衰减量 90dBm ，由于 $20+4-90=-66\text{dBm}$ ，大于 -75dBm ，因此在正常情况下，室内 AP 的覆盖范围为 60m。考虑到室内环境复杂，无线信号需要穿越墙体等障碍物，一般建议覆盖半径为 20m 左右。

5.5 规划工具

无论是室内还是室外，精细地覆盖规划都是一件非常有挑战的工作。很多项目的无线网络规划设计完全参照经验进行设计，与现网环境不能有机结合，不但缺乏科学的依据，准确率也不高，且规划效率低下。粗放的覆盖规划不能充分发挥 WLAN 的性能，并且也给后期维护优化带来更多的工作量，增加后期成本。

华为提供专业的规划服务工具，可以提供从规划、建设和优化全流程的工具支撑，大大提升覆盖规划的效率和准确性。



5.6 SSID 和漫游规划

SSID 规划

AP 可以配置多个 SSID，华为单频 AP 可支持 16 个 SSID，双频 AP 可支持 32 个 SSID。通过配置多个 SSID，AC 针对不同的 SSID 下发不同的策略，SSID 根据策略进行终端与业务管理。无线网络可按照用户群体划分不同的 SSID。

SSID 和 VLAN 的映射

通常，以太网中管理 VLAN 和业务 VLAN 是分离的。业务 VLAN 主要用于区分不同的业务类型或用户群体。在 WLAN 网络中 SSID 也同样可以承担相应的工作。因此，在 SSID 的规划中必须综合考虑 VLAN 与 SSID 的映射关系。业务 VLAN 应根据实际业务需要与 SSID 匹配映射关系，映射关系有 1:1、1:N、N:1、N:N 四种。

漫游规划

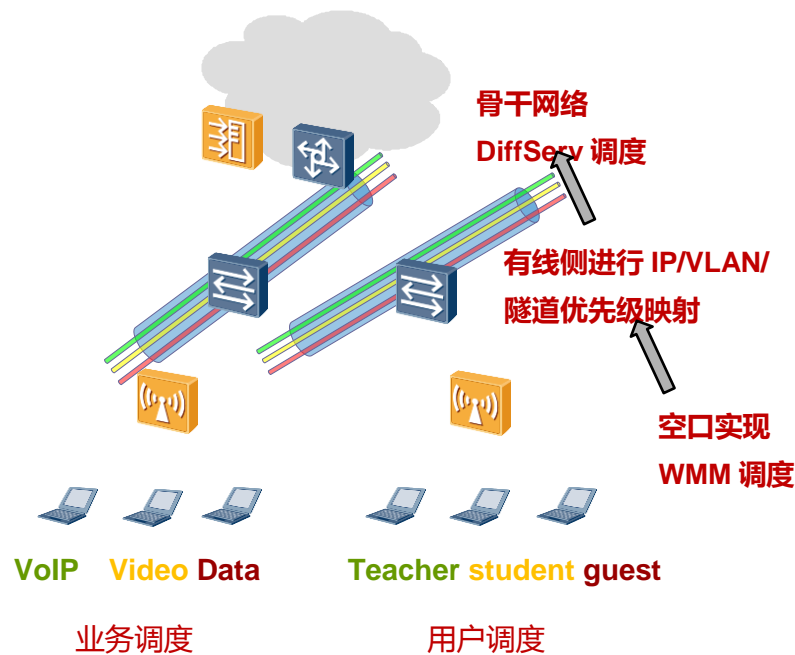
漫游是指用户在部署了 WLAN 网络的场所移动时，用户终端可以从一个 AP 的覆盖范围移动到另一个 AP 的覆盖范围，用户无需重新登录和认证。

WLAN 网络漫游中需要了解以下两点：

- 1、漫游过程中 SSID 必须一致，且使用相同的安全设置。
- 2、漫游中选择连接哪个 AP 是无线客户端的动作，这个切换的时机和快慢受无线客户端的芯片或设置的影响，所以在漫游切换过程中会出现不同的终端切换性能有差异。

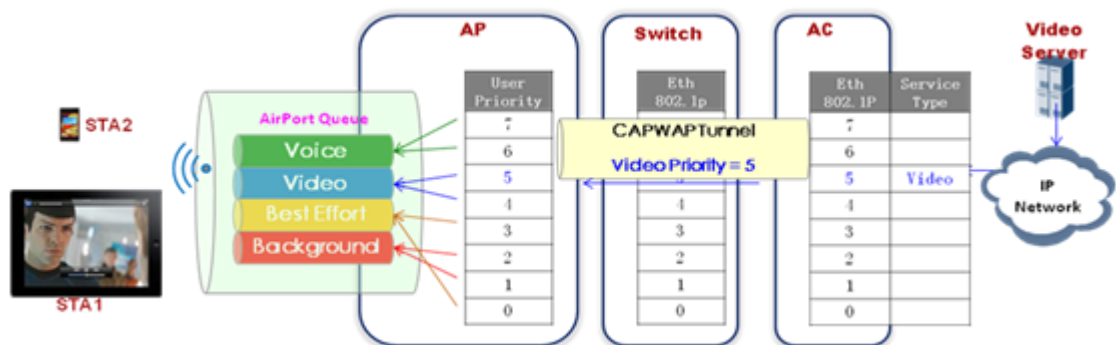
5.7 WLAN 业务 QoS 规划

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。如下图所示，在网络中，常采用无线空口做 WMM 调度，有线侧进行优先级映射，网络做 DiffServ 调度的方式，最大程度优化网络发生拥塞时的核心业务和 VIP 用户服务质量。QoS 部署一方面需要从业务的角度实现端到端的 QoS 保障，另一方面出于管理的需要能够对用户或者单 AP 的带宽进行管理，比如访客用户的带宽不超过 300kbps，某个 AP 上 SSID-Guest 的总流量限速 20Mbps 等。



WLAN 业务 QoS

报文在 WLAN 网络中传输时需要经过有线网络和无线网络两个部分，QoS 的设计要保障端到端的性能。华为 Native AC 可以做到 5 级 Qos 调度，满足业务服务质量要求。以视频流为例，端到到的方案流程如下图所示：



视频服务器通过 IP 网络将广播报文发送给 AC，并打上优先级：Erthnet 802.1p 优先级为 5。

AC 通过 CAPWAP 隧道将报文发送给 AP。AC 需要将 Earthnet 优先级映射到隧道的

优先级。

在保证效率的同时，为了提升稳定性，AP 上先将组播报文转为单播报文，然后将报文从有线的优先级映射到无线的优先级。

不同的业务进入不同的空口队列，并且获取到不同的空口 EDCA 参数，从而对不同优先级的业务实现差异性调度，保障 QOS 性能。

5.8 WLAN 带宽管理

出于管理的需要，运维人员往往需要系统地对用户或者单 AP 的带宽进行管理，比如要求访客用户的带宽不超过 512kbps，其他用户上网获得的带宽不超过 1Mbps，WLAN 解决方案能够提供基于用户，基于 AP（VAP）或者基于某 SSID 的带宽管理。

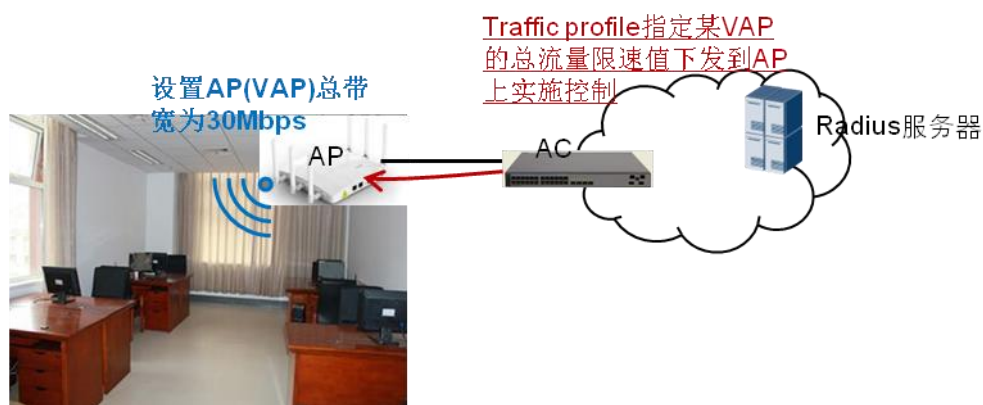
基于用户的带宽管理

基于用户的带宽管理包含基于某个特定用户的带宽管理以及基于用户组（角色）的带宽管理。基于用户的带宽管理需要 Radius 服务器参与，在认证后 Radius 下发用户带宽或者用户组给 AC，AC 通知 AP 进行相应的带宽控制

基于 AP 的带宽管理

出于管理的目的，有时需要对某个具体的 AP 进行带宽管理，如限制某个办公室里的 AP 带宽为 30Mbps，可以通过配置 Traffic profile 里的 VAP Limit Rate 实现带宽管理，如下图所示。

WLAN 基于 AP 的带宽管理



基于 SSID 的带宽管理

为来自网络外的访客提供上网服务不是建设 WLAN 的主要目的，一般需要对访客 SSID 的容量做限制，以保障内部用户的带宽和业务体验。

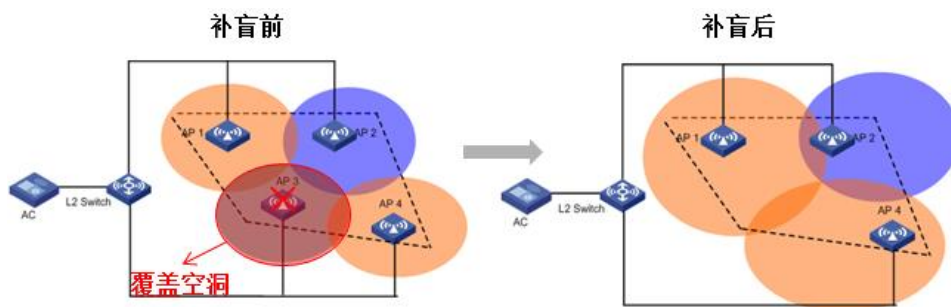
5.9 WLAN 可靠性规划

WLAN 网络的稳定性被普遍关注。一方面是设备的稳定性，AC 能够实现倒换后用户无感知的 Session 级的备份以及常年工作在室外的 AP 在恶劣环境下的适应能力等都是 WLAN 网络可靠性关注的重点。另一方面，AP 的调优特性可以在个别 AP 故障或者性能恶化时自动调优，以提升 WLAN 网络的稳定性。

自动调优

当 AP 射频环境出现恶化，某个 AP 故障或新增扩容 AP 时，需要启动射频自动调优，以增强系统的可靠性和稳定性。建议选择同时支持局部调优和全局调优的 AP 设备。局部调优可方便的应用于扩容新 AP、单点 AP 故障或者微波炉等局部环境变化而引起的信道环境变化场景，如下图所示。全局调优更多的应用于新建 WLAN 网络或者大面积信道环境恶化场景。

局部调优



当 AP3 掉电或故障时，其邻近 AP1 和 AP4 自动感知，并调整发射功率，从而达到补盲的效果。AP3 重新上线后，其邻居 AP1 和 AP4 的自动的调整发射功率，避免 AP 与邻居因覆盖区域重叠造成 AP 间相互干扰。

负载均衡

无线客户端一般会根据 AP 信号强度 (RSSI) 选择 AP，这很容易导致大量的客户端仅仅因为某个 AP 信号较强而连接到同一个 AP 上。由于 WLAN 是基于 CSMA/CA 机制，实现多用户接入，当单台 AP 接入用户数过多时，用户吞吐率性能会出现急剧下降且稳定性无法保证。负载均衡特性可以按照用户数量和用户流量，将用户分配到同一组但负载不同的 AP 上，从而实现不同 AP 之间的负载分担，避免出现某个 AP 负载过高而使其性能不稳的情况。

5.10 WLAN 安全性规划

空口安全

空口安全主要来自非法 rogue 设备，空口监听和恶意攻击三个方面，如下图所示。

空口安全威胁



Rogue 设备

网络中可能出现的 Rogue 设备包括 Rogue AP, Rogue Client, Ad-hoc 设备，这些设备对运维的 WLAN 网络会带来诸多的安全隐患，如干扰，用户和非法 AP 建立连接等。WLAN WIDS 方案支持对网络中的 Rogue 设备（包括 AP, Client, Ad-hoc）的进行检测、识别以及反制功能。下面分别从非法设备的监听，识别，判断以及反制四个方面详细阐述，。

侦听周边设备

AP 有三种工作模式：接入模式混，监听模式和合模式。

接入模式只提供覆盖功能，不提供非法设备监听功能；监听模式只监听，不能接入业务；而混合模式可以在接入业务的同时进行监听。

推荐 AP 工作在混合模式，在接入业务的同时监听周边设备，低成本部署。

设备类型识别

AP 通过监听 Beacon, Association Request, Association Response 协议报文和数据报文来识别 Rogue 设备是哪种设备（AP/Ad hoc/Client）。

监控 AP 搜集到无线设备后，维护一个无线设备信息列表，并把这些信息上报给 AC，在 AC 上根据一定的规则进行 Rogue 设备判断。

Rogue 设备判断

当 AP 设备工作在混合模式或者监听模式时可以实现对整个网络的监控，监控设备包括 AP、Client、Ad hoc 终端、无线网桥等。

Rogue 设备反制

检测到 Rogue 设备后，可以使能防范、反制功能。反制功能，根据反制的模式，监测模式 AP 从无线控制器下载攻击列表，并对 Rogue 设备采取措施，阻止其工作。

对 Rogue AP 的反制：监测 AP 通过使用 Rogue AP 设备的地址发送假的广播解除认

证帧来对 Rogue AP 设备进行反制，抑制无线用户和非法 AP 建立链接。

对 Rogue Client、Ad hoc 设备的反制：监测 AP 通过使用 Rogue Client、Ad hoc 设备的 BSSID、MAC 地址发送假的单播解除认证帧，对指定非法 Client 的进行反制。

Rogue 设备管理可以与定位功能集合，如在地图上可以查询或者实时显示 Rogue 设备的位置，为网管人员对网络监管和排障定位提供便捷。



恶意攻击

针对恶意攻击，WLAN 要拥有多种方式。下面针对最常用的 flood 攻击，Weak IV 攻击，Spoof 攻击方式，方案需要具备防御规划和措施。

Flood 攻击检测：

当“恶意用户”发送大量的“连接请求报文”至 AP 时，这些报文会被 AP 转发到 AC 设备上进行处理，这样会对内部网络造成冲击。

启动 Flood attack 检测，AC 会检测到来自于该恶意用户的 Flood 攻击，AP 会将来自于该用户的报文将全部被丢弃，从而实现了对于网络的安全防御。

Weak IV 攻击检测：

对于 Client 的数据报文，如果该报文使用了 WEP 加密算法，需要启动 IV 检测；AC 根据 IV 的安全性策略判断是否存在 Weak IV 攻击。

Spoof 攻击检测：

这种攻击的潜在攻击者将以其他设备的名义发送攻击报文。

恶意 AP 或者恶意用户发送一个欺骗的解除认证报文会导致无线客户端下线。

AC 接受到这种报文时将立刻被定义为欺骗攻击，并阻止该用户。

空口窃听

空口监听往往是网络中那些充满好奇心的用户经常尝试破解的点，需要考虑对空口数据进行加密。常用的空口加密方式有 WEP, WPA/WPA2, WAPI 等。在最新的实现中，不管是 WPA1 还是 WPA2 都可以使用 802.1X，使用 802.1X 时称为 WPA 企业版，不使用 802.1X 时称为 WPA 个人版，或者叫 WPA-PSK 版。

在实际网络部署中，空口加密通常和用户认证一起考虑，在本方案中推荐使用 Portal+PSK 方式部署，加密方式推荐采用 CCMP，在网络侧进行配置。

5.11 WLAN 用户安全

用户安全可以分为合法用户非法地访问其范围以外的资源和非法用户的接入网络两部分。

非法访问

在网络中根据需要，往往划分了不同的 SSID 供不同的用户群使用，如外部用户 SSID-Guest，内部用户 SSID-xx University。出于信息安全的需求，往往需要保证来访的访客不能访问内部的资源。同时内部的不同角色之间可能需要授予不同访问权限。这些可以通过用户组的方式来实现。

用户访问授权

用户访问授权可以在本地网络设备授权，也可以通过 AAA 服务器进行远端授权。一般来说本地授权多用于 SOHO 或者小型园区的网络架构，并不适合网络规模较大的园区架构。园区网络中多用远端授权的方式，即通过 AAA 服务器完成。

WLAN 用户认证成功后，Radius 服务器下发用户分组，将用户进行分类，每个用户分组可以关联对应的 ACL 规则，通过用户分组和 ACL 规则的关联，实现对每类用户进行 ACL 授权信息控制，即同类用户获得相同的授权信息。Radius 服务可以利用现网的 AAA 也可以新建。

用户隔离

访客系统推荐使用集中转发的方式，可以增强对访客用户的控制。

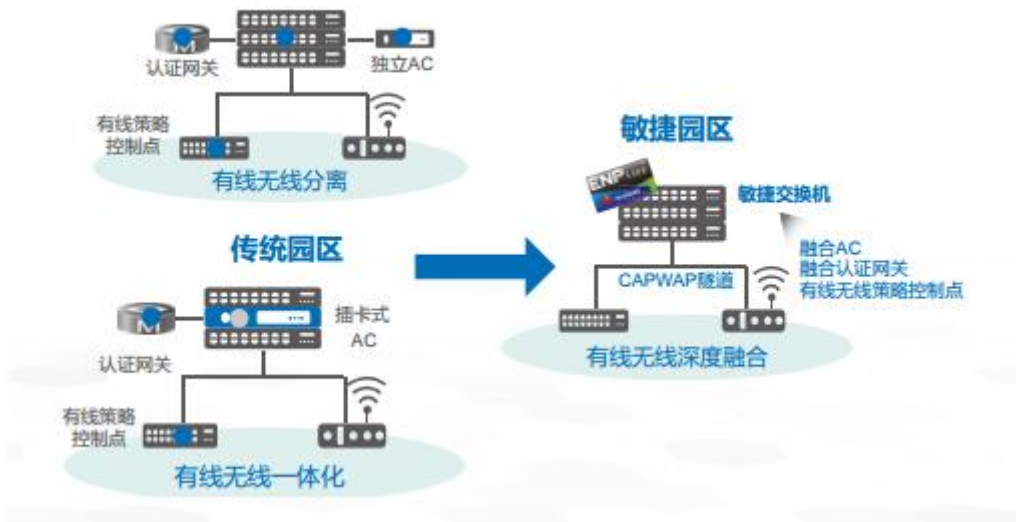
当外部访客用户和内部用户都采用集中转发时，外部访客用户使用的 SSID-Guest 与内部用户 SSID-civil aviation flight University 之间是天然隔离的。

当外部访客用户使用集中转发，内部用户都采用本地转发时，外部访客用户使用的 SSID-Guest 与内部用户 SSID-civil aviation flight University 之间也是天然隔离的。

6 设备简介

7 方案优势

7.1 有线无线深度融合：性能卓越，运维便捷



传统网络中常见的无线部署方式有独立 AC 或插卡式 AC，有线和无线网络在转发和控制层面上是分离的。随着 802.11ac 时代的到来和 BYOD 移动办公的逐渐普及，AC 设备由于转发能力、端口速率等各方面的限制将逐渐成为性能瓶颈。同时由于有线和无线网络用户认证和策略管理分别在交换机和 AC 单独维护，给 IT 管理人员的配置、管理带来极大的工作量。

华为创新性提出有线无线深度融合的理念，将有线网络和无线网络互相取长补短，形成有线、无线两张网络在用户使用体验、管理体验两个方面的趋同和极致优化，帮助企业获得一致的使用和管理体验。

融合转发：有线无线统一转发，性能卓越

利用敏捷交换机提供的全可编程能力，无线功能已经作为一个特性内置到有线板卡中，有线和无线网络转发、控制、管理层面都融为一体。这种网元层面的融合有效的解决了有线和无线网络独立控制和转发的现状。交换机的交换能力和可扩展性完全消除了 AC 设备或插卡集中转发控制的流量瓶颈，敏捷交换机整机转发能力可达 T bit。用户不需要单独购买 AC 设备或者插卡，节省投资。

融合管理：一台设备管理一个园区，极致简化管理

传统的无线园区网中由于众多接入交换机和 WLAN AP 的存在，节点数较多，管理复杂。敏捷园区通过 SVF（Super Virtual Fabric）超级虚拟交换网技术，创新性地将盒

式接入交换机虚拟化为核心 / 汇聚交换机的远端虚拟板卡，将 AP 虚拟化为核心 / 汇聚交换机的虚拟端口，将原来“核心 / 汇聚 + 接入交换机 + AP”的网络架构虚拟化为一台设备，实现设备、业务、用户管理层面的统一和简化。

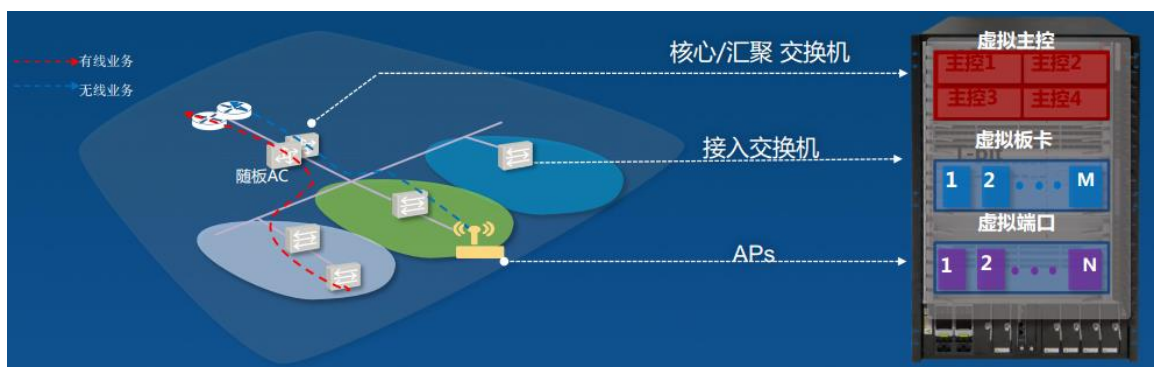
融合策略：有线无线用户统一管理，一致体验

传统的无线园区网中，有线无线的认证点是分离的，用户难以统一管理和认证。敏捷交换机融合 WLAN AC 后，将有线无线的接入认证点集中在敏捷交换机的敏捷板卡上，实现有线无线用户统一认证，业务统一管理。借助于敏捷交换机与接入层交换机之间的管理隧道（CAPWAP 隧道），实现认证点与策略执行点之间的策略联动，简化海量接入层交换机的配置维护，实现不认证用户无法二层接入，保障安全性。同时，认证点交换机可以精确感知接入层设备、链路状态，用户接入端口、位置等信息，从而当网络出现问题时能够快速定位故障点，提升运维管理效率。

有线无线深度融合，通过融合转发、融合管理、融合策略，实现了有线无线网络及业务的统一管理，保障有线无线用户体验的同时，极致简化园区的运维管理。

7.2 超级虚拟化，有线无线一体化，极简运维

华为公司推出的 SVF 是一种纵向虚拟化技术，将控制设备（SVF-Parent）以下的接入设备（SVF-Client）进行虚拟化，把众多接入交换机 AS 视为有线端口的集合，无线 AP 视为无线接口的集合，在垂直方向将 SVF 管理区域内的汇聚层设备和接入层设备虚拟化成一台逻辑设备，减少网络管理节点，实现网络集中统一控制和管理。

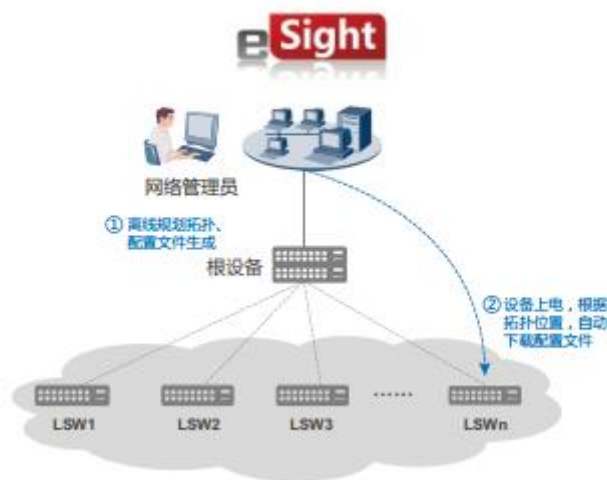


- 集中控制：控制设备（SVF-Parent）和接入设备（SVF-Client）虚拟化为一台逻辑设备，统一设备的管理平面、控制平面、转发平面，减少设备的管理层级和节点数目。
- 零配置接入：控制设备上集中配置，接入设备“0”配置，连上线自动加入 SVF 系统，自动获取配置、版本/补丁等文件，实现即插即用。
- 简化维护：控制设备上统一执行版本/补丁升级；统一查询 AS 的端口状态、CPU

及内存占用率等信息；统一对有线/无线用户进行管理。

SVF 系统面向业务的模板化配置，不仅智能化，而且更加贴近用户的理解。只要在控制设备集中配置，无需登陆到接入设备逐一配置，系统自动识别各接入设备及其端口角色，把配置自动下发到所有接入设备，避免了接入设备的重复配置工作量，大幅提高工作效率。

7.3 零配置部署：实现网络全自动部署，提升效率



传统网络部署需要手工通过命令行、或 Web 管理等方式，逐台配置设备，对于规模较大的园区，手工重复工作量大，配置繁琐。而近年来出现的一些自动化配置方案，虽然部分降低了设备配置的工作量，但依然没有解决两个问题：第一是网络规划与部署分离，当网络部署与初始规划不一致时难以第一时间发现；第二是需要人工采集设备 MAC/ESN 等相关信息，不能实现全自动部署。

华为敏捷网络零配置部署（Zero Touch Provisioning，简称 ZTP）方案基于统一的网络管理平台，通过在 eSight 网管上进行网络规划、部署和运维管理，设备根据规划的网络拓扑，上电后自动从网管获取配置文件，实现即插即用，极大提升网络设备部署效率。

7.4 无线信号全覆盖，随时随地便捷接入

面对复杂的室内结构场景，如学生宿舍、医院病房、酒店套间、办公区会议室等场景，华为推出了全新的敏捷分布式 Wi-Fi 方案，将有源射频模块安装在各个房间内，通过网线连接到中心接入点（AP）。与传统的通过馈线将 WLAN 天线安装到多个隔间的方法，敏捷分布式 Wi-Fi 有以下优势：



- 覆盖无死角：中心 AP 和远端射频模块之间，通过网线入室部署，无穿墙衰减与馈线损耗，
- 信号覆盖更优:业务可靠性高：中心 AP 支持断链逃生，AP 与 AC 链路中断，无线用户不受影响；
- 部署管理方便：远端射频模块由中心 AP 自动管理，部署便捷，管理方便；
- 投资回报率高：射频模块无需占用控制器 License，减少接入点数量，节省用户投资

7.5 网络全生命周期管理



无线园区的运维，相对于传统的有线园区，成本显著上升。首先是大量的 WLAN AP 增加了网络的节点数；其次，WLAN 使用空气作为传播媒介，而园区建筑内存在各种阻挡物会导致信号反射或衰减影响覆盖能力；再次，WLAN 的特点决定了用户非均匀分布时有可能出现部分用户无法接入的情况，需要排查问题所在。

无线园区全生命周期管理，从 WLAN 规划开始，在 WLAN 接入开通、日常网络监控和故障排查方面，均实现了高度的自动化和智能化，使得管理员能够快速简单地帮助园区内网络用户取得最佳的业务体验。

可视 WLAN 网规：专属工具，快速、准确、简单

网管集成专业网规软件，简单高效地进行可视化的网络规划，帮助建网周期缩短 30%，后期网络运维问题减少 20%；

敏捷配置：三步快速开通 Wi-Fi 接入

高效的敏捷配置方案，只需要三步就可以完成 WLAN 的部署，实现快速开通 Wi-Fi 接入，可提升 10 倍以上的工作效率；

日常监控：基于用户体验的 360 度网络监控

实时获取用户接入速率 / 接入成功率 / 接入掉线率等指标，通过大数据分析得出全网健康度指数，针对异常情况给出根本原因及排障建议，实现用户体验监控；

快速排障：移动化运维，网络故障快速定位

对于用户无法接入等问题，可基于报障用户快速搜索定位，从终端、空口、AP、AC、连通性、AAA、DHCP 等多维度进行诊断，给出关键 KPI 信息和修复建议。在智能手机上安装 eSightMobile 移动运维巡检工具后，可随时随地检测 WLAN 覆盖情况，感知用户体验，指导故障排除。

8 客户价值

华为敏捷 WLAN 解决方案凝聚了客户对未来网络的核心诉求，以用户为中心，自动部署网络资源、自动定位故障、网络管理更加精细友好。从网络基础机制上消除了传统网络缺乏体验保证、部署低效、单点安全防护和响应慢的问题，从业务被动适应网络转变为网络主动适应业务，从而构建一个业务友好的网络。让视频马赛克、语音模糊、上网慢以及远程办公、移动办公的糟糕体验不再困扰客户；从网络状态不可知、网络管理困难，转变为主动感知优化网络；让业务插上软件定义的翅膀，帮助客户以领先 4 倍的业务演进速度取得产业内的持续领先。

华为敏捷 WLAN 解决方案的终极目标是帮助客户实现无距离障碍的自由沟通的梦想，让人与人、人与物、人与信息的沟通，不再受任何因素的干扰和限制，变得自由、舒适和高效，让体验、运维和效率得到彻底的解放。

9 设备清单

10 类似项目案例一览表

序号	高校客户名称	合同期	主要内容及范围	负责人	备注
1	XX 大学	2015.5.9- 2018.3.8	无线 AP、交换机、控制器、POE 交换机		
2	XX 大学	2017.3.1- 2025.2.28	网络核心设备、无线终端、综合布线		