曲阜师范大学 WLAN 规划
建设方案

中科软科技股份有限公司

2016 年 9 月 18 日

目录

1 项目背景

曲阜师范大学1955年创建于济南，始称山东师范专科学校。1956年5月，被教育部批准升格为曲阜师范学院，同年9月迁址曲阜，开启了兴办本科教育的历程。1970年9月至1974年4月，与曲阜师范大学文科合并成为新的曲阜师范大学。1974年4月恢复曲阜师范学院建制。1981 年，被山东省人民政府确立为重点建设的六所高校之一；同年，被批准为全国首批招收研究生的高校。1982年，取得硕士学位授予权。1985年11月，学校更名为曲阜师范大学。2002年，建设日照校区。2003年，取得博士学位授予权。2004年，获得教育部本科教学水平评估优秀成绩。2012年，入选山东省应用型人才培养特色名校。2014年，入选惠普国际软件人才及产业基地项目共建高校。建校60多年来，学校积淀形成了“学而不厌、诲人不倦”的校训精神，共为社会培养了48万名毕业生，目前已经发展成为一所拥有曲阜和日照两个校区、学科门类齐全、培养体系完善、办学条件优良、教学科研具有相当实力、师资力量比较雄厚的省属重点大学。

2016 年是“十三五”发展的开局之年。站在新的起点上，曲阜师范大学将以“创新、协调、绿色、开放、共享”发展理念为指导，聚焦“双一流”目标，加快改革步伐，深化内涵建设，彰显特色优势，全面提升办学实力和水平，向着建设国际有影响、国内先进、省内一流大学的目标不断奋进，为山东省和国家经济社会发展做出新的更大的贡献。

本项目对于曲阜师范大学的意义重大，信息化基础设施作为招生、日常教学管理和办公的重要配套设施，其重要性也进一步得到凸显。同时，考虑到曲阜师范大学在国内教育行业中的领先地位，信息化技术和应用也一直走在前列。因此本次作为信息化基础的无线网络建设，不仅需要按时高质量交付以满足招生和教学管理的基本需要，同时需要体现一定的技术领先性，为教育行业信息化应用提供新的范本。

1.1建设需求分析

无线局域网（WLAN）技术于20世纪90年代逐步成熟并投入商用，既可以作传统有线网络的延伸，在某些环境也可以替代传统的有线网络。无线局域网具有以下显著特点：

- 简易性：WLAN 网桥传输系统的安装快速简单，可极大的减少敷设管道及布线等繁琐工作；

- 灵活性：无线技术使得 WLAN 设备可以灵活的进行安装并调整位置，使无线网络达到有线网络不易覆盖的区域；
- 综合成本较低：一方面 WLAN 网络减少了布线的费用，另一方面在需要频繁移动和变化的动态环境中，无线局域网技术可以更好地保护已有投资。同时，由于 WLAN 技术本身就是面向数据通信领域的 IP 传输技术，因此可直接通过千兆自适应网口和学校内部 Intranet 相连，从体系结构上节省了协议转换器等相关设备；
- 扩展能力强：WLAN 网桥系统支持多种拓扑结构及平滑扩容，可以十分容易地从小容量传输系统平滑扩展为中等容量传输系统；

现在移动办公，便捷办公，尤其是智能手机、平板电脑等的大量使用带来了大量的无线需求，无线网络在日常办公、学习、生活的环境中，无疑是要比传统的有线网络更加方便的。基于无线网络，学校教师生可以不再局限于有线网络的固定位置，而可以在校园任何位置方便的接入到网络内，这将给大家日常的办公学习带来极大的便利，基于此，考虑在曲阜师范大学曲阜校区和日照校区部署无线校园网。

本次无线网建设物理上与有线网保持相对隔离，由汇聚交换机、无线控制器、无线 AP、POE 交换机及相应管理系统等构建成无线接入网，接入校园网络核心，建立与有线网络相对隔离的全校无线网络。

2 总体设计原则

2.1高性能

所选无线产品硬件设计上严格依据业界同等技术最高性能标准进行设计，从阻容到主处理器芯片，每一个元器件都经过严格质量认证和技术认证，严格选用一流供应商的元器件，保证元器件的性能和品质；软件产品开发必须采用优化的平台进行开发，产品必须经过严格的功能和性能测试，并达到标准。

本次无线接入 AP 采取先进的 802.11ac wave2 协议标准，能提供整机千兆接入能力，是相同环境下 802.11n 产品 3 倍左右。

2.2先进性

采用先进的无线网络架构设计，无线控制器+无线 AP 的 FIT AP 架构，通过无线控制器实现对所有 AP 的统一管理，所有的关于无线网络的配置都可以通过配置无线控制器来统一完成，大大降低 IT 部门的工作量，降低运维成本。此外无线控制器还可以通过堆叠技术不断进行升级，增加可以管理的 FIT AP 的数量以完成任务。

无线校园网提供可供实际应用的稳定网络通讯服务，可以有效地从覆盖范围、接入密度、运行稳定等方面提供更高性能的移动云接入服务并协助用户实现最佳无线网络 TCO。

所选产品及其组网技术已达到国际先进水平，并具备技术前瞻性，至少保证校园无线网络 5 年不落后。

2.3安全性

校园无线网络系统的设计必须贯彻安全性原则，以防止来自网络内部和外部的各种破坏。贯彻安装性原则体现在以下方面：

- 设备采用的是扩频技术；
- 提供了射频信道的加密；
- 用户可以通过设备自己的网桥或另加独立加密设备实现更高的安全性；
- 网络内部对网络资源访问的授权、认证、控制以及审计等安全措施；防止网络内部的用户对网络资源的非法访问和破坏。

网络的安全性对网络设计是非常重要的，合理的网络安全控制，可以使应用环境中的信息资源得到有效的保护。必须有效的控制用户对网络的访问，灵活的实施网络的安全控制策略。在校园无线网络中，无线网络用户在接入无线网络前，必须要经过认证以及授权，防止非法用户的接入。

无线接入点之间的信息必须要经过加密处理，以防止非法用户窃听、篡改。FIT AP 具有多层物理 MAC 地址，每个用户群都可以与同一 AP 的不同 MAC 地址通信，使用户与 AP 之间变成单通道通信，从而延长了移动设备的使用时间，提高了用户的工作效率。FATAP 不仅有内存与数据处理芯片等高成本部件，而且都具有 IP 地址，成为黑客攻入整个局域网的窗口和整个网络的安全漏洞。集中架构下的 FIT AP 只具有多层 MAC 地址而没有窗口地址，对 WLAN 交换机的多重保护使黑客难获取它的 IP 地址，从而实现了真正的二层加密，大大提高了局

域网安全的门槛。

同时校园无线支持无线入侵检测 WIDS 特性，非常适合大型 WLAN 校园网络，可以对整个校园 WLAN 网络中的异常设备进行监视，并且可以根据需要对非法的设备进行防攻击处理，例如非法 AP、非法无线终端、非法无线网桥等。支持无线攻击防护系统 WIPS,能够实现检测并禁用非法设备、检测并规避 DOS 攻击、检测并规避表项攻击、检测并反制仿冒攻击等主要功能。

无线产品率先实现了校园网的无线 SAVI 技术，不仅无线用户需要进行认证，无线接入设备也要能够了解每一个用户的在线状态，了解其对应的 MAC、密钥等信息，因此对于无线网络的 SAVI，应该采用区别于有线的一些处理机制。无线 SAVI 的实现，使得高校在无线、有线全业务领域实现了安全可控可追溯的技术，通过这个方法，校园 IPv6 用户再也不能被恶意修改客户端或者被黑客控制，从而减少了校园信息化管理的安全风险。

2.4可用性

在产品生产上，采用业界先进的 IPD CMMI4.0 集成产品开发流程，有严格的质量管理体系，从全流程的每一个环节控制产品质量，从而保证产品的成熟可用性。

无线控制器支持 1:1 备份或者虚拟化技术强调业务的不间断性,即发现故障并完成切换的速度。AP 同时同主备两台 AC 建立链路，发生主备切换时 AP 不需要重新连接；可以在毫秒级发现故障并完成切换，保障用户业务不间断；如果有特殊需要，两台互为备份的 AC 也可以配置成负载均担的方式。

同时也可以支持 N+1 备份方式，提供多种故障恢复和冗余备份机制；提供各种网络负载分担机制；设备需具有一定程度的智能特性，以提高网络的可用性。

校园无线支持频谱防护技术防止蓝牙、微波炉等非 WIFI 设备对信号质量的干扰；当识别出干扰源的类型时，将会将会发出告警，并显示干扰的类型、干扰的信道、干扰强度、占空比等信息，并可以进一步定位干扰所在位置，便于及时排除。频谱分析还能监控整个网络的空口性能的情况，并适时发出告警。

频谱分析和抗干扰技术结合，能够使得整个网络在无需人工介入的情况下，及时规避干扰信道，从而保证网络的可用性。

2.5管理性

本次无线方案提供界面友好、易于操作的管理方式，为网络管理者提供多种易于使用的故障定位手段，对用户的接入提供灵活、安全的管理手段；使所建的无线网络可以适应多种环境的变化，可动态地保证良好的应用效果。

无线产品支持国际标准的网络管理协议 SNMP，TFTP，以及通过 Telnet、WEB 进行远程管理和监控。通过网络管理软件实时监测无线网络设备的运行状态，网络设备的故障事件报警，网络流量统计分析等。网管软件的应用可以提高网络管理的效率，减轻网络管理人员的负担。网络管理的目标是实现零管理，基于策略的管理方式，网络管理是通过制定统一的策略，由管理策略服务器进行全局控制的。并可对网络中的其它设备进行统一管理，真正实现有线无线一体化管理。基于 Web 的网管界面，是便捷网管的发展趋势，灵活的操作方式简化了管理人员的工作。

新型无线校园网应具备简易管理效果，减少运维，通过新技术自动化等功能实现的快速部署与配置上线。

同时结合移动互联网趋势，为学校无线提供云端管理和管理应用 APP，更加灵活、管理便捷。

2.6扩展性

随着技术不断发展，新的标准和功能不断增加，无线网络设备可以通过网络进行升级，以提供更先进、更多的功能。以方便未来更灵活的扩展。

无线控制器设备具备技术前瞻性和向后兼容性，支持虚拟化技术，组网灵活，易于扩展。

也可以通过一个集中的无线网管平台实现对所有的 AP 功能的配置和管理；同时整个系统可以根据用户的需要进行规模上的扩展，扩展后所有功能和管理的模式保持不变。

2.7开放性

本次无线校园网采用的技术支持为国际标准或业界标准，不使用某个厂商的专用技术和协议，以保证网络设备的互通性，网络发展的一致性，增强网络的兼容性，以达到网络的互连与开放有利于网络的投资保护。

为确保将来不同厂家设备、不同应用、不同协议连接，整个网络从设计、技术和设备的

选择，必须支持国际标准的网络接口和协议，以提供高度的开放性。

无线接入点必须支持 IEEE802.11a/b/g/n/ac 等主流无线传输协议。本次项目所投产品以 802.11ac 协议为主；

支持国际通用的网络管理协议：SNMP（V1、V2、V3），同时支持通过 Windows 平台上的配置工具：Telnet、WEB 进行选程管理。

2.8经济性

本次所选产品具有较高的性价比，在符合用户需求的前提下选择性能合适的产品。

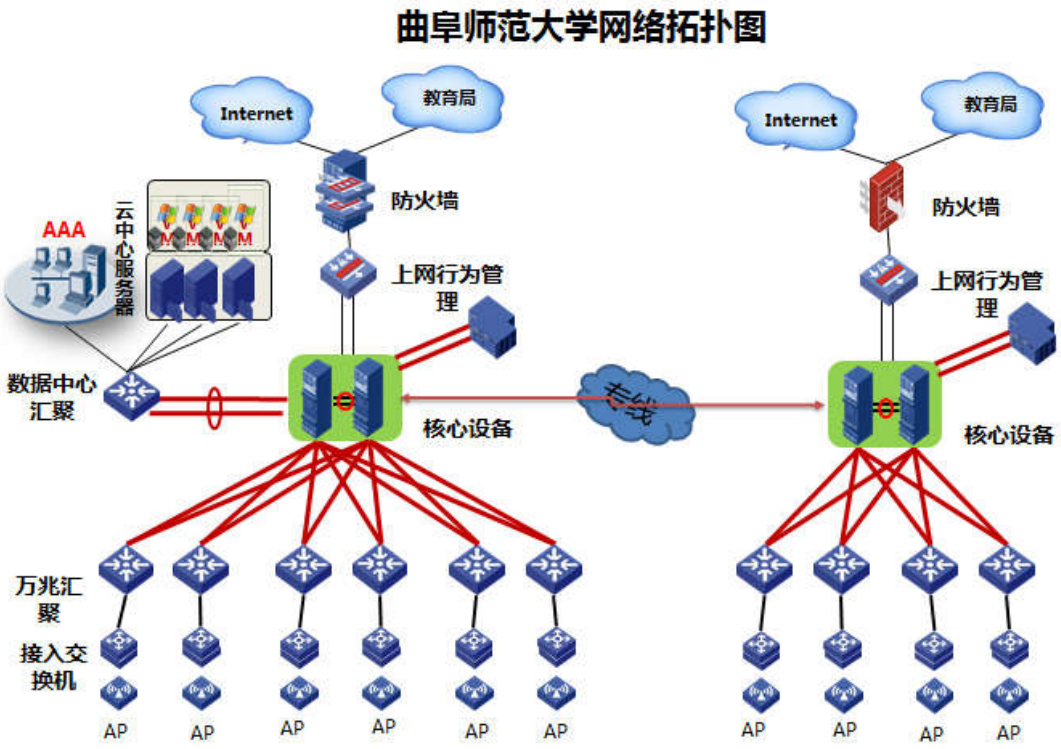
网络规划与有线网络有良好的兼容性，在采用先进技术的前提下，最大可能地保护已有投资，并能在已有的网络上扩展多种业务。

2.9合理性

为了实现校园无线网络的合理分布，考虑实现无线网络的不同情况和特点以及目前学生教室笔记本电脑、移动终端等设备用户数量日益增多的情况，本次项目采取合理的布网方式满足现在以及未来发展的需要。从无线方案选择、产品选型、认证方式、无线安全、融合管理、无线定位部署等方面进行合理化方案设计。

3 校园无线网络整体设计

3.1方案整体拓扑架构



本次建设曲阜校区和日照校区 WLAN 无线覆盖网络拓扑图，两校区使用专线互联。

无线控制器通过双万兆与核心交换机直接连接，达到高速率的转发。并且通过核心交换机下行接入各个建筑单体的楼宇汇聚交换机。为了简化网络部署，简化网络管理，并提高故障恢复的速度，核心交换机采用多虚一交换架构互联，无线控制器同样采用虚拟化部署方式，将 2 台无线控制器设备虚拟化成一台分布式设备，增加网络的健壮性及简化网络管理性。

3.2校园出口安全设计

3.2.1出口安全方案

校园互联网出口安全设备承担着为用户提供高速通道、并给整个校园网的安全防护提供保障。随着用户对于网络带宽的要求不断提升、移动终端的大量普及，以及运营商互联网线路资费的逐步降低，要求互联网出口具备高性能、高可扩展能力。同时，考虑到传统安全部署模式串接故障点多、不易维护、不易投资保护

的缺陷，建设采用高融合架构的安全统一网关。使校园出口更加稳定、可靠的运行。

为了保证校园出口高性能，校园网出口首先在网络通道上无瓶颈，其次确保安全业务处理无瓶颈。通过独立的多块交换网板，实现转发路径的无阻塞和易扩展，确保网络通道上无瓶颈；安全业务处理模块，采用 NGFW 设计模式，可在单个模块上实现防火墙、入侵防御、应用控制、负载均衡等多业务功能，避免多个模块串接的部署复杂、故障点问题。

3.3认证计费方案设计

3.3.1运营商与校园账号绑定方案

高校与多运营商合作运营的主要特点是：

1、 校园网接入多个运营商的路由出口

2、 每个运营商还有各自独立的账号和认证计费系统

3、 按照选择哪个运营商则走哪个运营商链路的原则，用户的运营商账号认证之后自动路由至运营商链路

4、 原则上需要两次认证过程，第一次是校园网认证，第二次是运营商准出认证

根据以上特点，关键是需要解决一次登录和基于运营商账号的路由选择，后者解决了，即可解决运营商账号的认证问题。

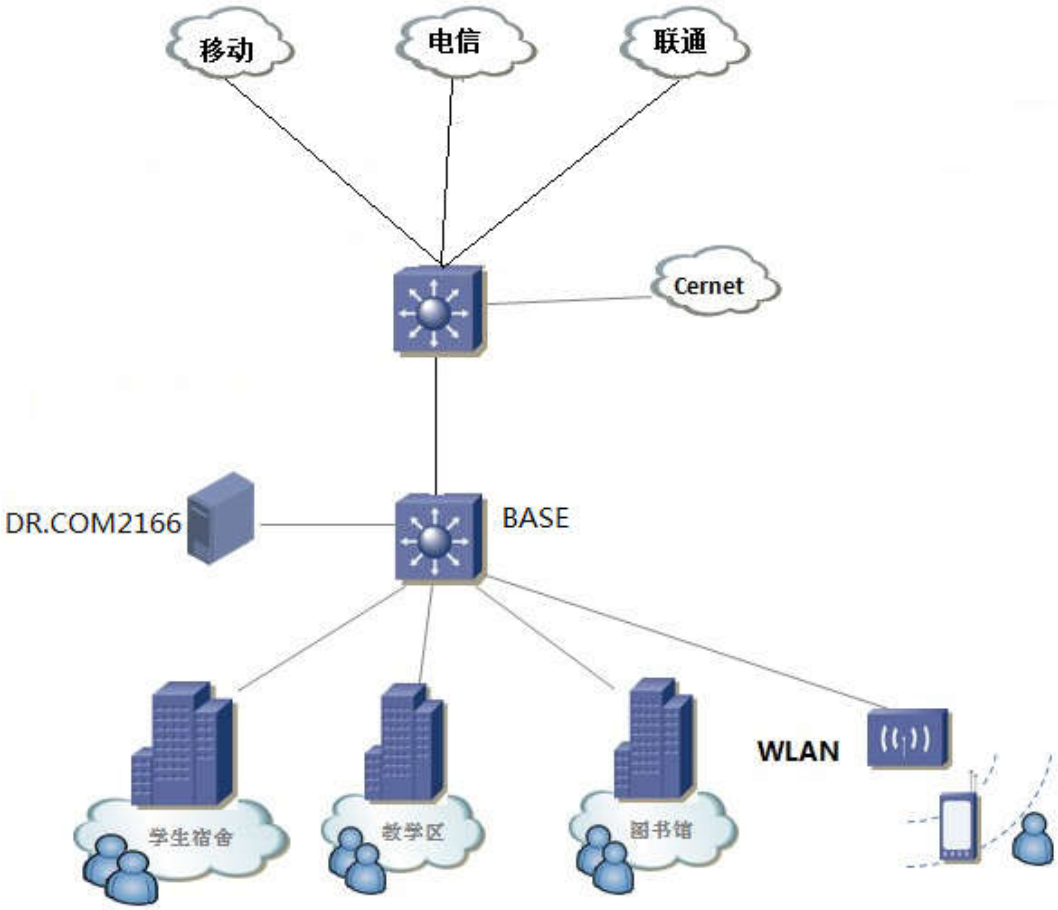
本方案建议：

1、 校园网认证和运营商准出认证均采用 Dr.COM 2166 产品，利用 Dr.COM 2166 的灵活的用户策略和认证联动功能，实现校园与运营商的统一认证需求。

2、 运营商开通运营商的账号时，连接校园端的 Dr.COM 校园认证计费系统， 将用户的校园账号与运营商账号进行绑定，这样校园用户直接使用校园账号认证，选择相应的运营商出口，即可由 Dr.COM 2166 完成绑定的运营商账号认证。

3、 用户的运营商账号密码修改后，与校园认证系统运营商的认证平台需有与校园认证系统账号密码同步的接口。

组网拓扑：



组网说明：

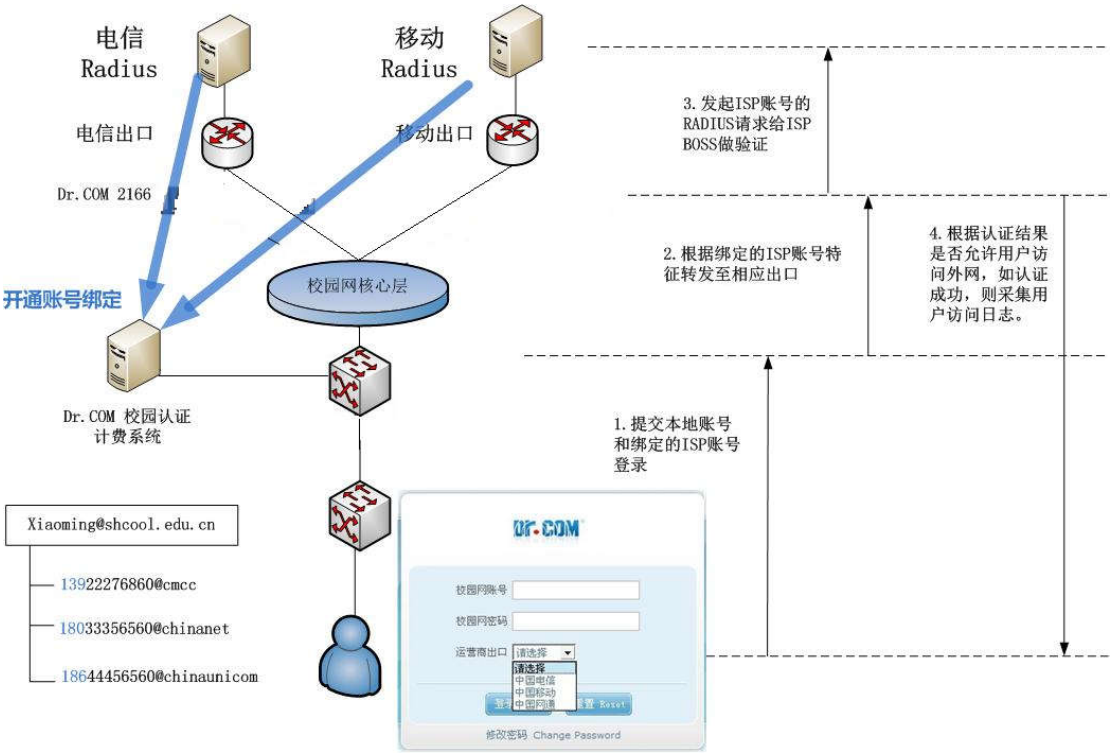
校园总出口部署 Dr.COM 2166 B-RAS 实现统一认证，并根据用户选择将用户流量发送到对应运营商链路；使用 Dr.COM 2166 可与运营商的 BOSS 系统通过 Radius 方式实现认证计费，有线网内使用 WEB Portal 或客户端认证方式，无线网使用 Dr.COM 2166 B-RAS 内置推送的 WEB Portal 认证。

方案优势：

经过绑定后，Dr.COM 客户端与 Dr.COM 2166 的 WEB 登录功能，支持只输入校园账号并选择运营商出口后，即可完成校园网认证和运营商准出认证。如下图：

Dr.COM 2166 可根据用户绑定的运营商账号特征做策略路由，转发至相应的运营商出口链路， Dr.COM 2166 与运营商认证计费后台完成认证计费功能。网络出口处的 Dr.COM 2166 可采集所有用户原始话单，可供学校与运营商对账。

工作原理图如下：



Dr.COM 校园认证计费系统需要校方开放权限给运营商，在运营商开通用户账号时，连接 Dr.COM 校园认证计费系统对校园账号进行绑定，Dr.COM 校园认证计费系统支持一个校园账号最多绑定 4 个运营商账号。运营商可通过接口或校园自服务系统页面方式进行操作。

需要说明的是，本方案建议合作的所有运营商均支持通过校园认证计费系统绑定校园账号，否则没有绑定的运营商账号，需要用户手动输入，用户的体验达不到最优的效果。

部署的 Dr.COM 2166 的主要作用：

通过 Radius Proxy 功能配合校园网准入的 Dr.COM 2166 B-RAS 实现一次登录，并对用户的互联网访问实现行为审计和接入控制。

1 每个运营商的地址范围不一样，不可能在校园网在用户选择运营商账号之前就分配用户，因此需要网络出口部署 BRAS 作 NAT 地址转换，一方面帮助运营商节省公网地址资源，另一方面便于学校统一管理校园网的 IP 地址段。

2 由于出口做了 NAT 地址转换，Dr.COM 2166 可提供基于公网 IP 的 NAT 转换前的私网 IP 互联网访问日志采集。

3 记录用户每个运营商互联网使用的原始话单，利于合作运营对账。

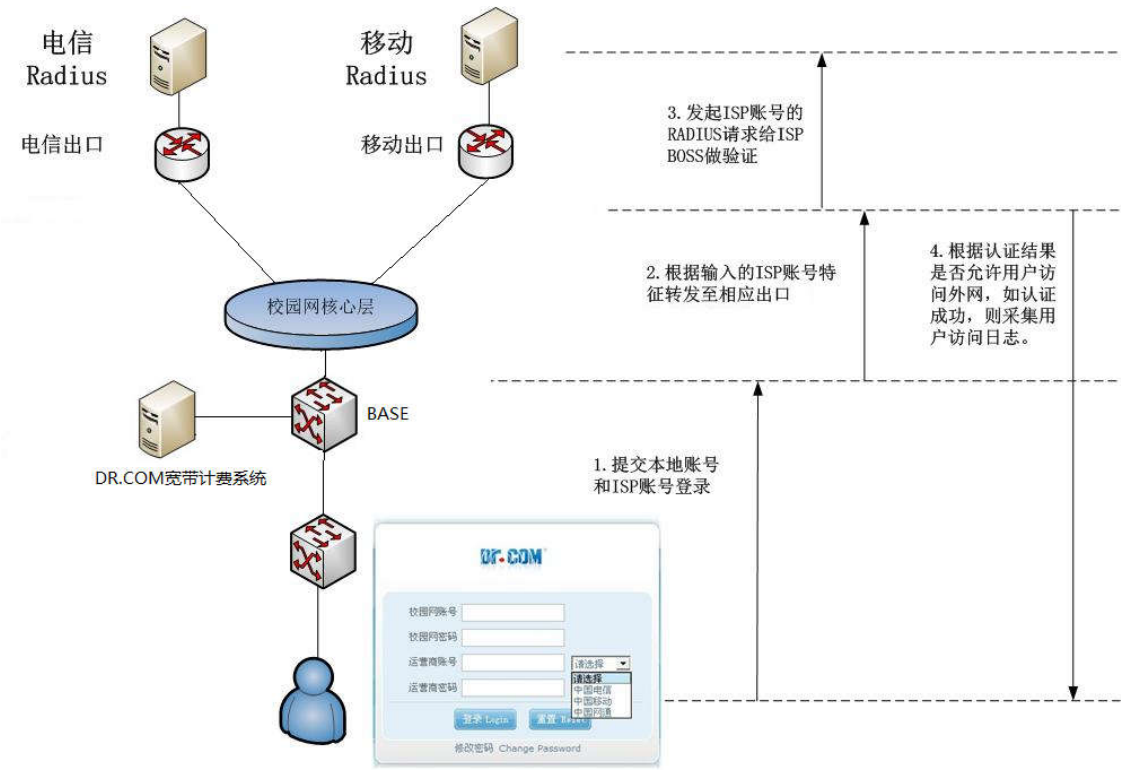
3.3.2运营商与校园账号无绑定方案

如果运营商无法连接校园认证计费系统实现校园账号绑定，则需要用户输入校园账号和运营商账号。

Dr.COM 客户端与 Dr.COM 2166 B-RAS 的 WEB 登录功能，支持一次登录实现两次认证，即用户在一个登录界面输入校园账号和运营商账号，即可完成校园网认证和运营商准出认证。登录界面可由学生自主选择运营商，如下图：

Dr.COM 2166 B-RAS 可根据用户选择的运营商账号特征，转发至相应的运营商出口链路，由运营商的出口链路上的 Dr.COM 2166 B-RAS 与运营商认证计费后台完成认证计费功能。网络出口处的 Dr.COM 2166 B-RAS 可采集所有用户原始话单，可供学校与运营商对账。

工作原理图如下：

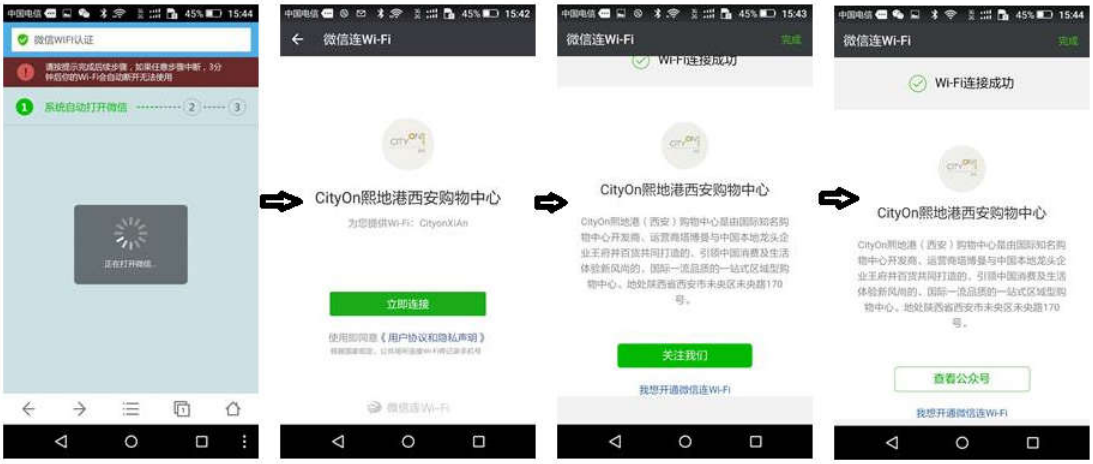


3.3.3产品配置清单

序号	名称	产品规格描述	品牌	数量	备注
1	Dr.COM Billingware 宽带运营平台（软件）	包含策略管理、用户管理、自服务平台、统计报表输出、接口等模块 最大可管理用户数：5 万	Dr.COM	1	城市热点
2	Dr.COM 2166 B-RAS 认证服务器（软件）	提供用户认证、记账功能功能，防代理私接和用户 url 访问日志采集功能	Dr.COM	1	城市热点

3.3.4 基于无线的微信认证

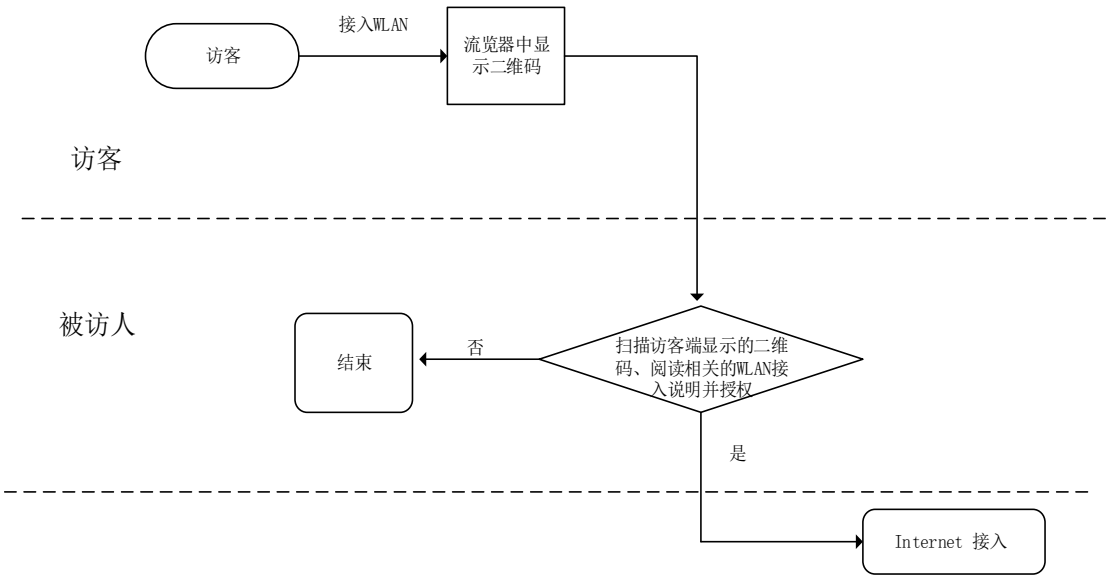
微信连 Wi-Fi 是解决传统 Wi-Fi 连接授权认证的一个新功能，其代替传统 web 认证需要用户输入用户名、密码等信息的过程，并在微信界面给予有安全性认证的 Wi-Fi 服务提供商一个信息展示广告位的入口，以充实其商业化价值，通过微信加关注，做到广告、通知等统一推送。学校可通过 WiFi 这一入口来推广微信公众号。微信连 WiFi 流程如下



3.3.5 基于无线访客管理

✓ **无线访客管理------协助扫码**

来访人员接入学校 WLAN 考虑访客的快速便捷性建议采用协助扫码认证方式，由学校老师帮助扫访客无线终端上二维码进行无线访客授权接入学校 WLAN 网络。访客扫码认证快速接入 WLAN 网络。



✓ **无线访客管理------动态密码认证**

学校老师组织学术研讨会、会议中心、集体活动等场景，无线终端接入 WLAN 时，输入相应的个人身份信息（姓名、单位、手机号等），在输入该场景中放置的动态密码上显示的数字即可接入无线。（可以对接学校签到系统）

✓ **无线学生管理------学号和学号后四位为密码**

学校学生采用方便简单实用性强的 web 认证方式准入无线网络，将学生学号做为学生上网账号，学号后 4 位作为学生初始密码，初始密码可以通过系统进行修改。将学生信息通过 excel 表格导入到系统中进行存储。

✓ **无线教师管理-------教师工号密码**

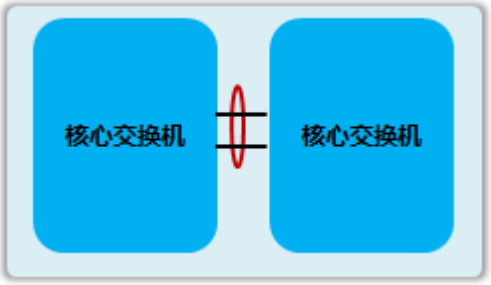
学校老师采用方便简单实用性强的 web 认证方式准入无线网络，将老师工号做为老师上网账号，工号后 4 位作为老师初始密码，初始密码可以通过系统进行修改。老师信息通过 excel 表格导入到系统中进行存储，如果学校有 AD 可以直接对接，将 AD 作为账号源进行 WiFi 认证。

3.4 校园核心交换机设计

3.4.1核心交换机方案

校园网核心交换区承载全网各区域间高速路由交换，保证平台之间数据高速通讯，2 台核心 10G 互联横向虚拟化，提高网络的稳定性、冗余性、可扩展性等。

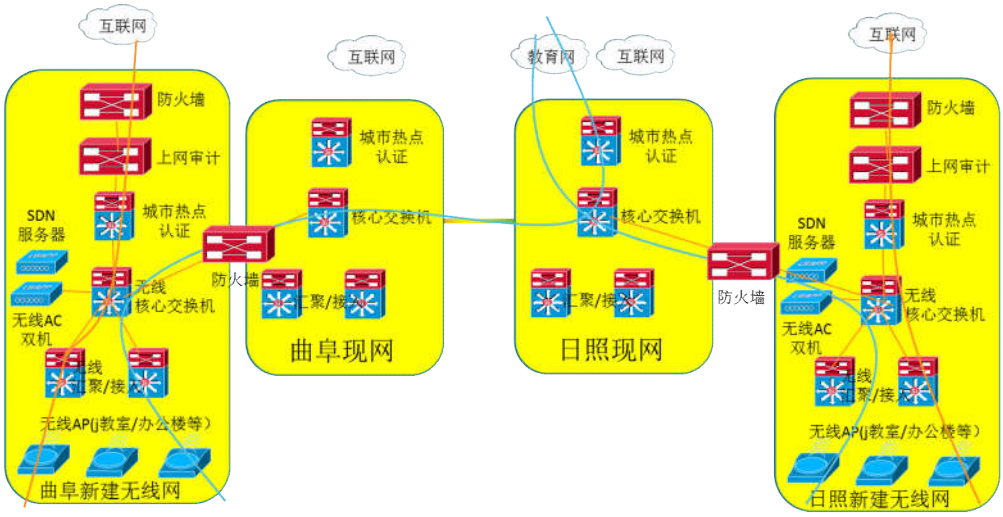
如图：



在校园网组网架构中，核心骨干层设备担负着连接各个万兆汇聚设备和部分接入的工作，同时通过骨干设备的互联，将分布在各物理位置网络连接在一起形成一套完整的网络。由于骨干层设备担负着整个网络的流量。骨干设备和链路的稳定性将直接影响整个网络的可靠运行。

高端核心交换机，将网络的控制层和数据转发层进行分离，大幅简化了网络的管理及维护难度，更为重要的是实现了网络流量的灵活控制，采用无单点故障设计，关键部件，如电源等采用冗余设计；采用先进的 CLOS 架构，无源背板避免了机箱出现单点故障；所有单板和电源模块支持热插拔功能；采用先进的 CLOS 多级多平面交换架构，可以提供持续的带宽升级能力，支持数据中心大二层技术、纵向虚拟化和一虚多技术，支持 EVB 和 FCOE，并完全兼容 40GE 和 100GE 以太网标准。核心设备支持横向虚拟化，和纵向虚拟化技术，进一步融合 MPLS VPN、IPv6、应用安全、应用优化，无线，多种网络业务，提供不间断转发、不间断升级、优雅重启、环网保护等多种高可靠技术。

3.5 现网互通方案及安全性设计



现有网络有学校各业务系统，为实现无线网络与现网的互联互通，方案设计为无线核心与现网核心交换互相对接，实现网络的互联互通，在互联的设备间添加下一代防火墙设备实现应用层的安全管控。

部署方式：

1.曲阜校区新增 2 台防火墙，组成“防火墙 HA1”双活架构

2.日照校区新增 2 台防火墙，组成“防火墙 HA2”双活架构

3.曲阜校区“防火墙 HA1”通过虚拟化技术，虚拟出曲阜“虚拟防火墙 HA1”

4.日照校区“防火墙 HA2”通过虚拟化技术，虚拟出日照“虚拟防火墙 HA2”

主要功能包括：

1.新建无线网络-有线现网互通的安全防护及应用识别

2.通过 IPSec 加密隧道技术，保护曲阜-日照日照间，身份认证信息的加密传输，确保师生的身份信息不被泄露

3.通过应用识别及 QoS 结合技术，制定曲阜-日照间的关键应用优先传送策略，确保带宽有限的前提下，选课、一卡通等现有关键应用的传输

4.通过防火墙硬件虚拟化技术，虚拟出校区间的安全防火墙，用于曲阜-日照间的安全防护，同时大幅度节省保护投资。

现有网络有学校各业务系统，为实现无线网络与现网的互联互通，方案设计为无线核心与现网核心交换互相对接，实现网络的互联互通，在互联的设备间添加下一代防火墙设备实现应用层的安全管控。

根据移动互联网的高速发展，网络安全问题愈发显著，现今的网络安全管控已不再是 IP 或端口的管控，而是基于用户、访问内容、用户行为的安全管控。

状态防火墙的数据过滤功能曾经对阻断不需要的应用非常有效，因多数应用是使用具体且不变的端口与协议传输通过网络的。如果管理员认为一项应用不安全，便可以修改防火墙策略阻断相关的端口与协议，阻止用户的访问。但是，传统的基于端口的防御不再有效了。原因在于，比如阻断 80 端口可以屏蔽对整个 web 的访问，这根本不是如今大多数企业的选择了。一些传统的网络安全技术已经落后于网络威胁的进化了，参见下图：

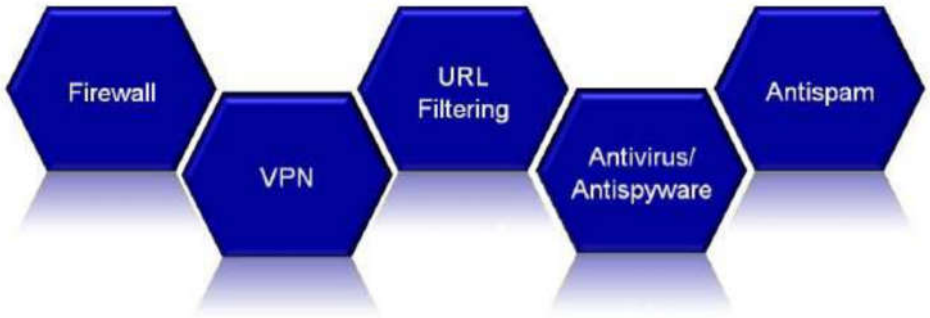
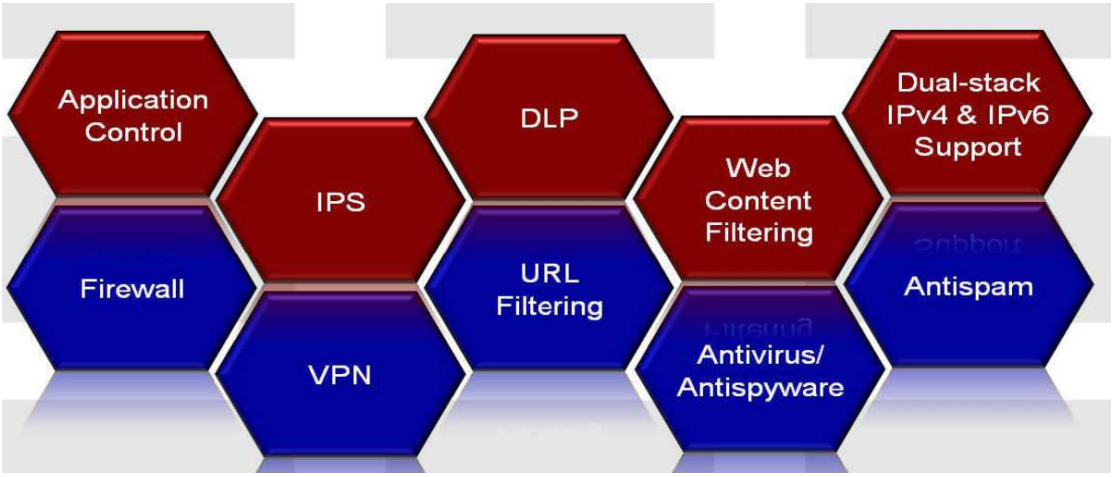


图1：传统网络安全技术是必需的但不完整

越来越多的公司或机构意识到传统的安全解决方案例如防火墙、入侵检测系统以及基于主机的病毒防御已经不足以防御新的更巧妙的攻击。潜在的数据泄漏与损失正在逐年增加，网络罪犯正在寻求新的方法突破一下一代网络安全防御防御。另外，政府与法律规定例如 PCI DSS， HIPPAA 与 HITECH 法案开始约束行业内员工的行为，公司的高管以及 IT 技术人员开始关心公司内部员工从内网网络访问与下载的内容。 安全平台具备所有被认可的下一代网络所需安全技术，能够防御最新的威胁。图 2 为一些下一代网络安全技术。

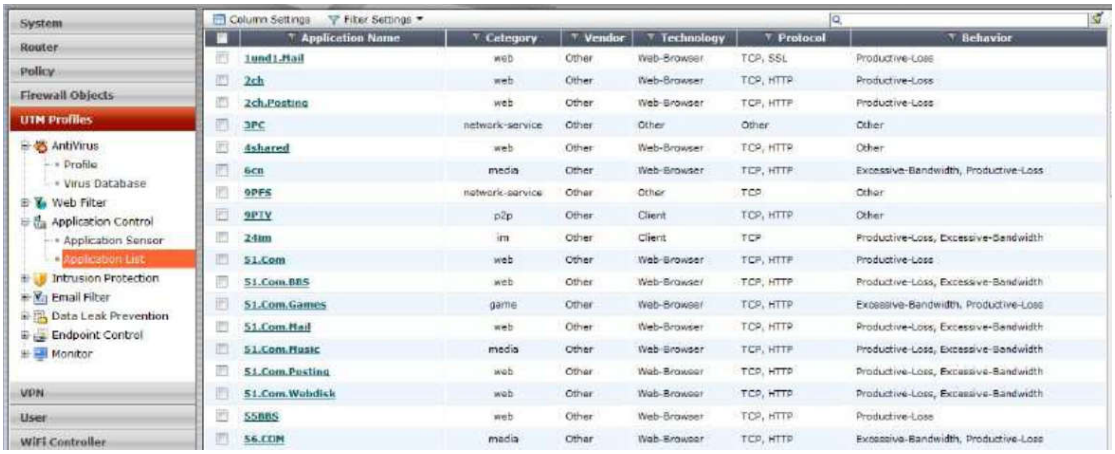


包括功能有应用控制、IPS、数据丢失防御（DLP）、网页内容过滤、双栈支持以及传统防火墙具备的 VPN、URL 过滤、防病毒/防间谍、反垃圾邮件等技术。

3.5.1安全控制-应用控制

对下一代防火墙的主要应用需求与驱动就是应用控制。为了防止数据丢失与防御新的威胁，有效控制旧有的应用以及新出现的基于互联网的应用是必需的。下一代应用控制功能必须能够检测、监控并控制应用，并在网关与终端之间管理与这些应用相关的网络流量，无论这些应用使用任何的端口与协议。另外，应用与终端用户之间需要建立关联以保证在访问应用之前能够执行安全策略。

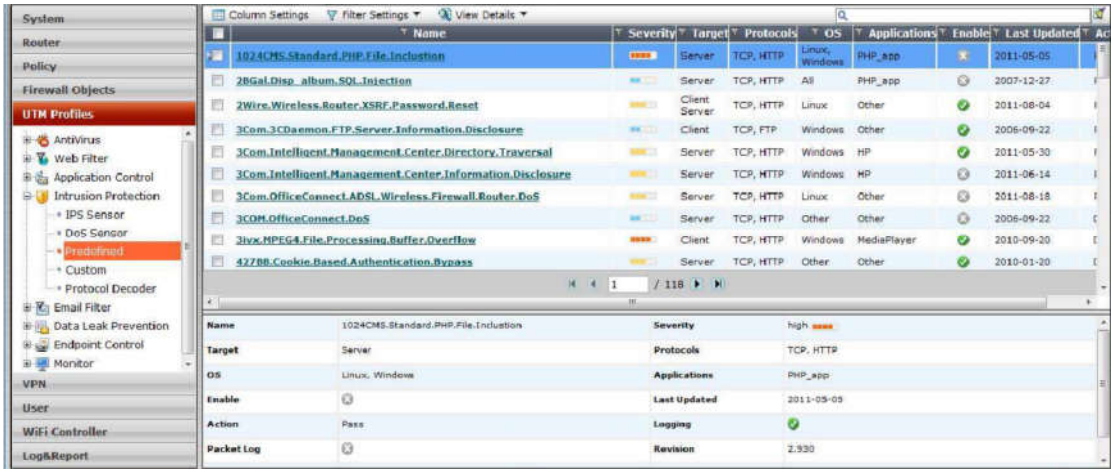
应用控制功能，可以基于应用分类、行为分析与终端用户关联来检测并限制网络与终端的应用。网络管理员可以对运行于下一代网络与终端的应用定义并执行相应的策略，实现对基于 web2.0 应用的细粒度的管理与控制，例如 Facebook，Skype，Twitter 与 Salesforce.com，且无论这些应用使用的何种端口与协议。



3.5.2安全控制-入侵检测系统（ IPS）

大范围的更新与补丁需要升级与维护，下一代网络的管理与维护是复杂而耗时的事情。每一次漏洞补丁的发布，大型企业的网络得花费数周甚至一个月的时间去更新修复所有受影响的系统。 研发安全平台设备中的 IPS 系统可以提供网络中已知漏洞防御或“零日漏洞”的更新服务，使未修复的系统免于攻击。

IPS 系统提供了广泛的功能，可用于监控或阻断恶意网络活动，包括预定义与用户定制特征、协议解码、带外模式（或单臂 IPS 模式）、数据包日志记录与 IPS 传感器功能等。通过 IPS 传感器可以迅速且集中的配置与部署 IPS 工具。所有的设备平台中，都具有 IPS 功能，防御网络边缘或网络核心的重要业务应用受到来自外部或内部的威胁。



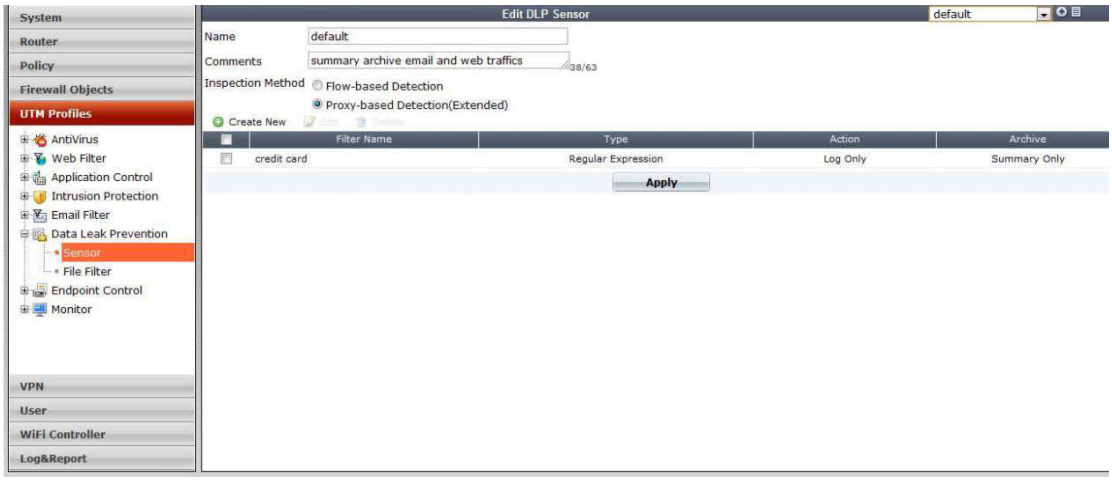
3.5.3安全控制-数据丢失防御（DLP）

受信任的雇员频繁向未信任的网络发送敏感数据，无论是故意或无意性质的。 Fortinet 公司的 DLP 技术使用成熟的模式匹配与用户识别技术，检测与防御未授权的敏感信息通信与文件穿透网络边界而泄漏。 DLP 功能包括文件与文件源的指纹识别、多重检测模式（基于代理与数据流模式）、加强模式匹配与数据存档。

许多的通信协议，包括 HTTP、 HTTPS、 FTP、 FTPS、邮件通信协议（ POP3, POP3S, IMAP,

IMAPS,
SMTP, 与 SMTPS）、 NNTP 与即时消息通信（ AIM, ICQ, MSN, 和 Yahoo!），这些流量都可以作为敏感数据信息进行监控。Fortinet 公司研发的 DLP 功能可以基于文本字符串以及加强的模式匹配包括通配符与 Perl 正则表达式进行搜索内容。例如，模式匹配可以用于扫描包含敏感个人信息例如社会保险与信用卡信息的网络流量。

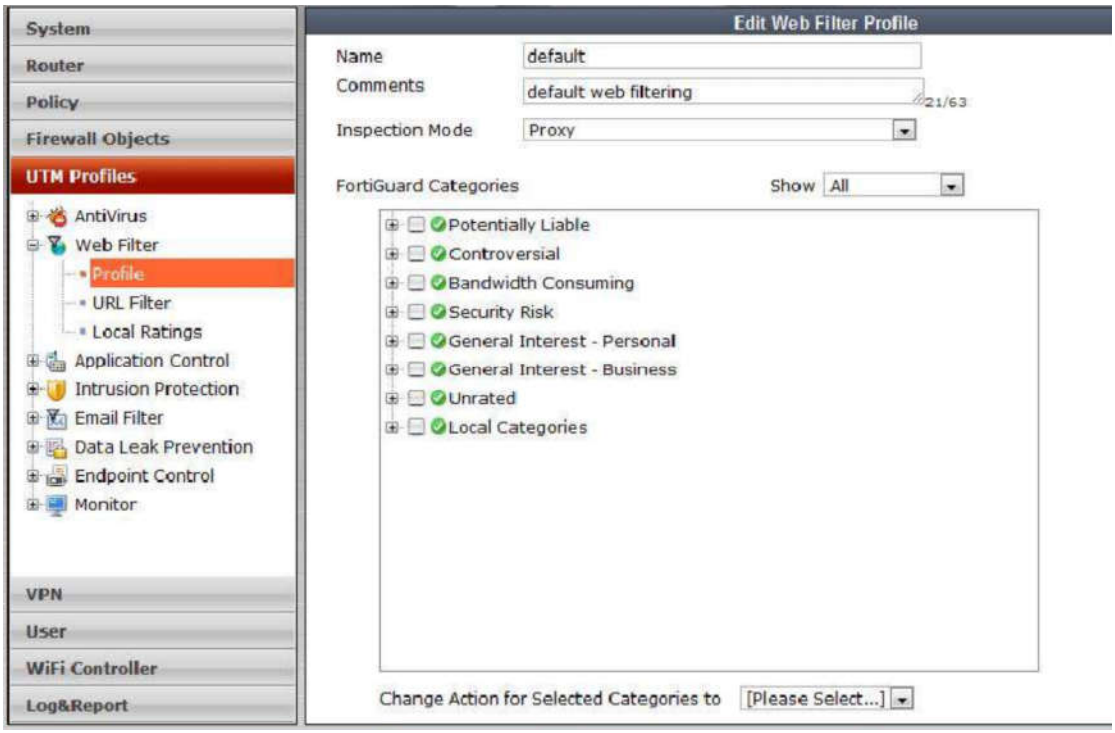
下一代网络安全防御一旦发现匹配，敏感内容将被阻断、通过或存档，并生成潜在泄漏通知。 DLP 也可以用于阻断出入网络的敏感信息。例如，屏蔽包含在垃圾邮件信息中的敏感内容， DLP 可以加强对进入网络数据的保护。



3.5.4安全控制-网页内容过滤

网页内容过滤解决方案，最初是传统的URL屏蔽名单形式的，进一步地扩展并与Fortinet公司研发的其他安全功能结合，嵌入到所有的 FortiGate 加固安全设备中应用。网页内容过滤技术使 web 流量能到达到细粒度的检测识别与控制管理的程度。通过网页内容过滤技术，FortiGate 设备可以使用多重预定义与用户定义的种类区别并过滤 web 流量。

为了加速 web 流量与内容检测，所有的 FortiGate 安全平台都支持 WCCP 协议（ Web CacheCommunication Protocol），该协议允许 FortiGate 设备作为一个路由器与缓存引擎操作。作为路由器，FortiGate 设备从客户端 web 浏览器截获 web 浏览请求并将其转发到缓存引擎。然后，缓存引擎将 web 内容返回到客户端。作为 WCCP 缓存服务器时， FortiGate 能够与其他 WCCP 路由器通信以缓存 web 内容，根据所需将所请求的内容返回到客户端 web 流量器。通过 FortiGate 设备管理接口，可以轻松配置网页内容过滤功能。



3.5.5安全控制-双栈道 IPv4 与 IPv6 支持

随着 IPv4 地址空间的耗尽，越来越多的组织正在迁移到 IPv6，下一代互联网通信协议。IPv6 彻底的改变了 IP 地址的供应，从 40 亿 IPv4 地址到 340 万万万亿 IPv6 地址（ 2^128 地址）。 IPv6 同时也保证了比 IPv4 基础之上的功能的增强包括更好的安全性、更好的地址查询、有效的路由与服务质量。 IPv6 架构包括诸多功能与优势尤其有利全球化的端到端的通信。

当更多的内容与服务提供商开始转换到 IPv6 的地址时，公司与企业机构必须部署网络安全设备能够提供与 IPv4 架构下的同等的 IPv6 架构的安全防御水平。有一些机制可以使只兼容 IPv6 的设备与之兼容 IPv4 的设备与网络之间进行通信。两种最常用的是双栈道与通道机制。双栈道更可取，因为它允许安全设备能够处理基于 IPv4 与 IPv6 的数据包。通道机制，在另一方面，将一个 IPv6 数据包包裹在 IPv4 数据包头中，允许设备转发数据包但是不进行检测。这样的 IPv6 支持限制也意味着通道机制不能检测恶意代码或不需要的内容，直接允许不需要的内容穿越网络。

3.6应用园区网设计

应用园区网方案应满足两个特征是柔性网络和软件定义。

3.6.1 柔性网络

柔性一方面指网络架构本身非常灵活，业务部署（应用/终端）可以做到与位置无关；另一方面指彻底改变传统网络通道就绪，终端和人根据位置匹配通道的模式，将人和应用作

为中心，所有网络的资源跟随人和应用移动，柔性具体涵义包括如下几个亮点：

3.6.2 无状态网络

传统网络存在的问题：传统网络划分 L3 网段时往往与位置紧密关联。一个企业要根据不同的办公室，不同的楼层/楼栋划分不同 L3 网段，这种模式下要想实现用户移动（比如员工出差、工位搬迁）非常困难。因为用户移动往往要跨越不同 L3 网段，IP 地址必须进行更换，往往会丧失原先的权限，给工作带来麻烦。

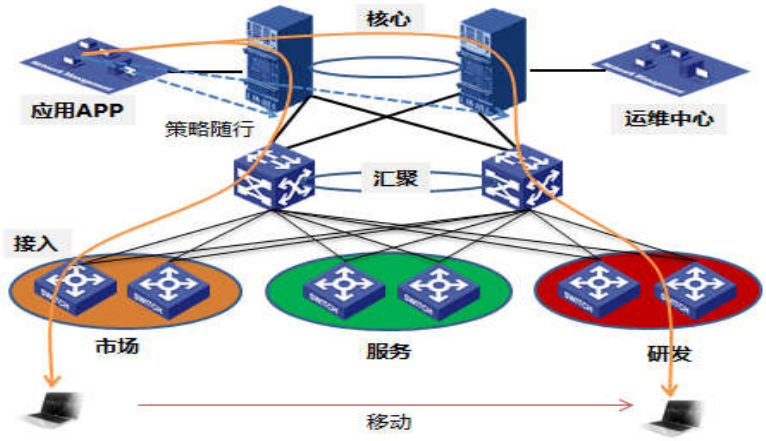
无状态网络的核心是位址分离；传统的网络，IP 地址即是终端的标识，同时也是终端位置的标识，因为 IP 确定意味做它必须位于某个三层网关的所在的位置。应用园区方案中“位址分离”位指位置，址指 IP 地址，位址分离就是 IP 地址与位置解耦，让 IP 地址可以在任意位置接入，无需改变网络的配置。

3.6.3 用户策略随行

策略随行：指用户移动到哪里，用户的体验不变；一般上要实现策略随行，都需要对用户进行分组，传统的分组方式与地理位置紧耦合，同一个用户组位于一个办公区，一个楼层或者一个大楼之内，很难跨越地理的局限。这样用户一旦移动起来，策略实施就非常复杂，想达到策略跟随或者体验一致也非常困难。

应用园区方案策略随行的核心就是“名址绑定”，名址绑定就是用户和 IP 地址一一对应；传统网络用户名和 IP 地址是难以做到绑定的，一方面 DHCP 的方式并不能保证单用户每次获取相同的 IP，静态地址分配的方式又不能保障用户在移动过程中保持相同 IP 能够在不同的位置进行正常的网络连接；应用园区方案中无状态网络本身提供了 IP 任意位置访问的能力，再配合名址绑定实现用户位置发生了变化， IP 地址段也没有变，甚至 IP 地址没有变，针对 IP 的策略也没有变，而这种针对 IP 的策略其实就是针对用户的策略，最终实现了用户的策略随行。

除了用户和 IP 绑定，在某些场合可能不需要做非常强的捆绑，应用园区可以提供业务和 IP 网段的绑定，或者用户组和 IP 网段的绑定，比如：视频监控终端尽管分布在全网任意位置，但可以将其 IP 全部分配在某一个网段之内；又比如财务的人员可能也分布在网络不同的位置，我们也可以将其分配在同一个网段内；最终实现通过 IP 段标识用户组或业务组。



策略随行

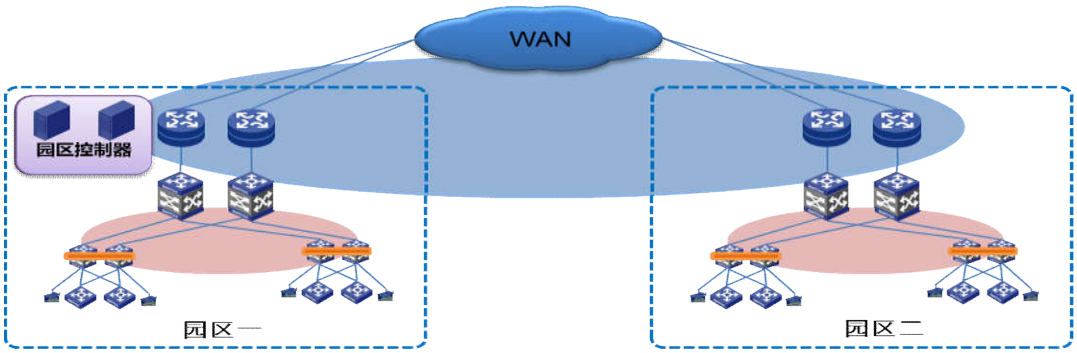
3.6.4 网随人动

传统园区网络首先是通道就绪，终端根据最初的规划，接入到相关接入交换机的端口，从而实现 VLAN 等权限和终端的匹配，一方面不能够解决用户和终端任意位置接入权限分配的问题，另外终端接入位置也受限制。

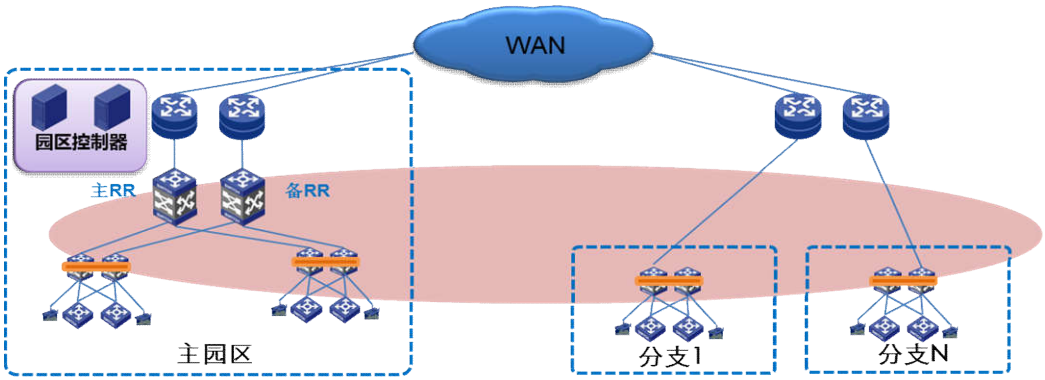
应用园区将人和应用作为核心，所有网络的资源跟随人和应用移动，用户在哪里接入、资源就下发到哪里，真正体现柔性网络的网随人动的特点。

3.6.5 无差别网络

园区分支无差别：应用园区 无状态网络、用户策略随行、网随人动不仅仅可以在单园区实现，还可以跨园区、在园区分子之间实现，满足业务、用户在更大范围内移动化办公，符合现代企业常见的多分支架构。



跨园区组网

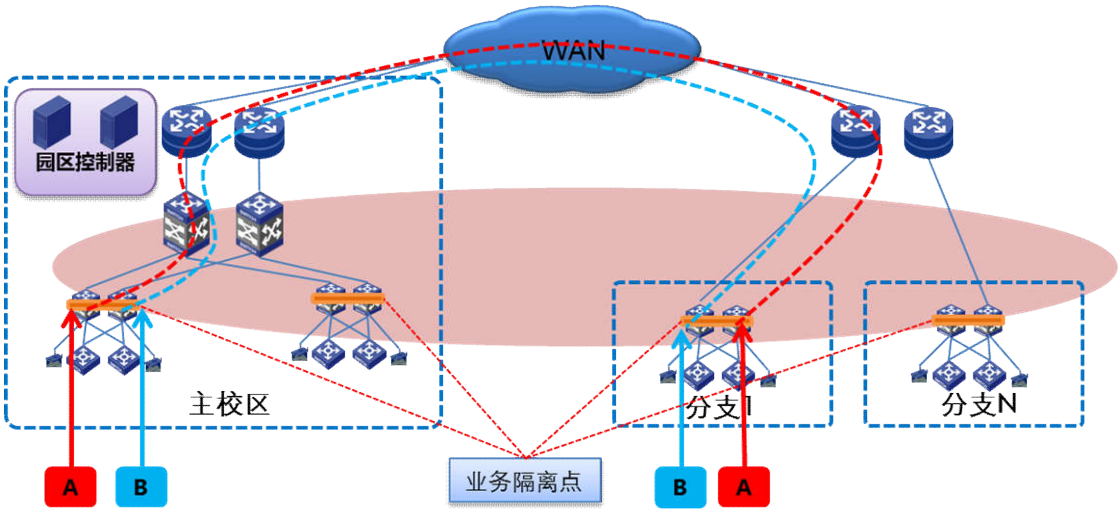


园区分支无差别组网

3.6.6 网络虚拟通道隔离

整网采用 overlay 的技术，天然具备跨广域网的通道隔离能力，相比 MPLS 的隔离方式，VXLAN 的隔离只需要在端点（VTEP）做隔离，不需要全网隔离，端点之间只需要 IP 互通既可。一方面让整个运维节点大幅减少，另一方面端点之间支持多运营商连接，负载均衡可以直接通过 ECMP 来实现，让整个组网清晰、运维更简单。

在隔离方式上，应用园区提供两种隔离方式，一是类似 MPLS 的 VRF 隔离，每个用户组在 VTEP 节点分配不同的 VRF，VRF 之间在路由层面实现隔离，每个用户在 VRF 内通过 VLAN 映射成不同的 VXLAN，最终实现在通道内通过 VXLAN 数据传输，实现隔离。二是 ACL 的隔离方式，因为每个用户组在 IP 分配的时候已经分配在不同的网段，因此不同用户组在接入之后获取的是不同网段的 IP，ACL 隔离相对比较简单，一条 ACL 就可以实现不同用户组之间的网络隔离。



3.7软件定义网络与大数据平台设计

软件定义：主要是通过 SDN 的思想，将网络控制平台集中，实现网络运维极简，真正将网管人员从低价值劳动中解放出来，具体有一下几个亮点：

3.7.1 软件定义网络业务按需交付

业务指 4-7 层服务，如防火墙，IPS，ACG 等，传统网络中部署 4-7 层服务存在哪些问题呢？用一句话总结，就是 4-7 层服务节点不能和位置解耦，这些节点成为网络拓扑的一个网元，和基本网络部分紧耦合，服务节点的增删改都会导致网络拓扑发生较大的变化，需要不停地调整网络的配置以适应，导致维护非常困难。比如下图中传统的两种服务节点部署方式，一种是 in line 方式，一种是旁挂方式。In line 方式的问题在于串接在整个转发路径上，其中任何一个节点都容易成为性能瓶颈，而且对于不想过服务节点的流量无法绕开，造成带宽的浪费，让本就捉襟见肘的性能更雪上加霜；旁挂方式的问题在于要逐跳配置复杂的策略路由，一旦网络节点增删改，或者进行服务节点的替换，就需要调整很多策略路由的配置，而且理解困难，又复杂又容易出错。

应用园区方案引入了 SDN 服务链功能，把园区传统的通过策略路由方式的复杂引流策略转换为一种简单的按需使用，自由编排的引流方式来快速实现。这种实现方式可以为用户提供灵活的、可编程的、弹性的软硬件一体化解决方案。这种方案的优势是：可以根据用户的需求，提供定制化或个性化的软硬一体化基础设施服务，可以支持如 NFV 等新技术，也可以兼容传统安全，是真正为用户提供兼具可靠性、高性能以及可编程的稳健解决方案。

此外在园区控制器 Campus Director 上直观的图形化拖拽方式，使得用户可以从业务视角出发进行服务编排。定义一条流的起点和终点，中间直观地拖拽插入需要经过的 4-7 层组件，然后一键下发，Campus Director 将把这个图形化界面翻译成网络语言配置到网络设备上，真正实现随心所欲地部署。

3.7.2 软件定义网络设备自动部署

设备开箱，上电后自动加载版本，加载配置，网管人员零干预启动。自动部署的核心是因为应用园区的网络将整网的接入设备配置完全整合变成一份完全相同的配置文件，同时汇聚层设备也进行整合，变成一份相同的配置。这大大简化预配置文件编写的复杂度， 使得各层次设备配置模板化，自动部署的成本很难度大大降低，同时也避免了人为误操作的风险，使得自动部署从理论变成现实。

3.7.3 大数据平台架构设计

大数据平台重点完成海量数据的统一存储、管理、信息共享和数据资源服务提供，并作为应用系统的支撑，针对不同的业务建立不同的专题，建立完善的数据采集、加载、存储、分析和应用展示的架构体系。

大数据平台采用混搭架构，其核心主要包含四个部分，分别是：前置系统、ETL 数据平台、数据仓库和统一数据服务接口。其中：

- 前置系统：将采集的全部数据按源系统的数据格式临时存储，屏蔽对源系统的干扰，为数据检查和 ETL 数据处理做好准备。
- ETL 平台：通过进行高效数据抽取、数据清洗、数据转换、数据校验、数据加载等，完成对数据、数据和互联网数据从数据源向目标数据仓库转化的过程。
- 数据仓库：通过数据仓库存储管理大数据平台中所涉及的所有数据进行存储、分析，并能够支撑应用层的业务需要，进行查询、统计和展现的实现。
- 统一数据服务接口：统一数据服务接口是高性能服务接口，为上层应用提供统一的数据服务，满足数据查询、数据互操作、数据交换、数据分析、目录服务、综合查询、信息比对等业务应用的需要。

3.7.4 大数据平台技术设计

整个大数据平台从技术和功能的角度可以分为数据源层、数据准备层、数据接入管理层、数据存储共享层、数据服务接口层和数据应用层六个部分。

数据源层：数据来源层为整个系统提供数据。系统不直接从数据来源系统抽取数据，而是通过数据准备层，以保证数据源业务系统的安全。

数据准备层：从源系统通过桥接、导入/导出、ETL 等方式，采集的全部数据，并按源系统的数据格式临时存储，为数据检查和 ETL 数据处理做好准备。

数据接入管理层：高效进行数据的抽取、清洗、转换、校验、加载等处理，对于少量或适量的结构化数据可利用传统 ETL 进行处理，海量的结构化、半结构化、非结构化数据可利用云化 ETL（Hadoop）进行处理。

数据存储管理层：大数据平台的数据存储层。数据存储管理层实现平台采集和产生的大数据存储，包括结构化数据存储、半结构化数据和非结构化数据存储。其中具有高价值密度

的结构化数据使用 MPP 数据库集群以数据仓库的方式来负责存储管理，低价值密度的音视频、互联网等半结构化和非结构化大数据以 Hadoop 的 HBase、HDFS 分布式存储系统负责存储管理。大数据存储管理层对 MPP 数据库集群和 Hadoop 平台实现了融合，整合了列存储、智能索引、多副本、Mapreduce、Hive 等大数据处理技术对信息资源服务的大数据进行统一的存储管理。

数据服务接口层：提供高性能服务接口，为上层应用提供统一的数据服务。

数据应用层：面向大数据平台的各类业务应用。通过对各业务系统所产生的各类结构化、非结构化大数据进行统一整理、分类、存储、专题分类等处理操作，从而达到将原始的无法使用的大数据化零为整，使之成为有序、专题化、可统一查询分析的价值数据目标。以大数据平台为基础，用户的大数据平台应用可以更快更方便的开发建设，应用的种类可以更加多样化，特别是对结构化和非结构化数据的综合价值挖掘更加有效和深入。

3.8大数据平台方案的优势

3.8.1 数据资源统一管理、高度共享

通过云计算、大数据技术，实现对各类数据源各种类型的结构化、半结构化和非结构化跨域数据的统一管理和高度共享，面对不对增长的数据规模和不断深化的工作，大数据平台帮助实现一套平台应对各类数据，系统采用模块化分层设计，以最低的工作复杂度实现最高性能的大数据处理效能。

3.8.2 海量数据低成本存储管理

通过分布式计算和存储以及 Hadoop + MPP 的混搭结构，有效支撑海量数据。基于 MPP 数据库集群的大数据综合应用平台，数据存储采用先进的列存储架构，能够实现最高 1:20 的数据压缩，帮助用户最大程度的节省硬件存储投资和后续的电能消耗。

MPP 数据库集群基于低成本高性能的 X86-64 PC 服务器构建，运行于开源 Linux 操作系统。相比基于小型机+磁阵的解决方案，大数据存储管理硬件成本大幅降低。智能索引自动建立，数据库维护简单，降低后期 DBA 数据库维护的难度和成本。

3.8.3 高可用、动态扩展

通过合理配置能够有效实现均衡负载，充分发挥每一个节点的计算能力，提升整个系统

的协同效率；基于安全组的备份策略，能够保证节点在发生故障时，不影响系统对外提供服务的连续性。

MPP 数据库集群支持上百个计算节点，能够有效处理 PB 级数据。基于 MPP+Shared Nothing 的分布式数据处理架构，面对数据规模不断扩增时可通过平滑扩容实现容量和性能的提升。整个过程高度自动化，无须停止集群服务，保证服务连贯性。

3.8.4 深度精细化的业务数据支撑

有效管理和整合海量数据，实现对各类数据的多维深入分析；高效的数据分析能力，帮助客户应对复杂性强、效率及实时性要求高的场景；高效的运算性能和海量数据的快速查询响应能力，以及 100%的查询召回率的全文索引支持，为上层多维分析、即席查询、复杂统计分析等分析应用提供完善可靠的数据支撑，帮助用户挖掘数据潜在价值，辅助科学决策。

3.9校园无线网场景设计

侧重实际应用，覆盖校园内区域，为教学、图书馆、办公及学习、生活、交流提供切实可用的、稳定的无线网络环境。

采取先进通行的协议标准，即目前无线局域网普遍采用 802.11 系列标准，无线局域网提供 802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ac Wave2 标准的联网支持，提供可供实际应用的稳定网络通讯服务。

实现室内无线网络的合理分布，考虑室内实现无线网络的不同情况和特点以及目前学生教室手提电脑用户数量日益增多的情况，应采取合理的布网方式满足现在以及未来发展的需要。

办公楼宇采用终结者 AP 为主，部分办公室按照结构需室内布点，大教室、会议室等采用室内布点，选择高密型 AP 进行覆盖。

在实施无线覆盖工程时，如无特别说明，以考虑信号覆盖范围为主，且单个 AP 的并发用户数及每用户无线上网带宽需要作为工程的重要因素予以考虑。

所有学生宿舍楼宇主要采用室内方式进行覆盖，每房间部署一个终结者 AP。

无线系统须具备对无线 AP 进行统一控制、管理的软硬件平台，软硬件控制、管理平台所提供的 AP License 数量与实际 AP 数量相匹配并易于扩充。

考虑到所属地区的气候特点，冬天低温，夏天雨水多，潮湿等特点，因此，对于室外使

用的 AP 设备，必须使用专业的室外型设备，并且有专门的防雷击措施来保护 AP 设备以及与 AP 相连的交换机设备。

3.9.1无线控制器核心设计

核心层：无线控制器作为整个无线网接入的管理控制以及转发完成以下的功能：

- 将无线 AP 进行统一地址管理和分配；
- 对所有无线终端进行地址分发和管理；
- 作为无线认证的终结节点；
- 无线广播域或组播域的边界；
- 在无线层实施功能区内、功能区之间的安全访问策略。

3.9.2无线接入层设计

接入层：提供 Layer2 的网络接入，通过 VLAN 划分实现接入的隔离。在接入层设计时，应考虑以下几点：

- 接入层接入端口规划容量应根据实际使用情况考虑扩展性,具备可堆叠特性；
- 各功能分区的接入层相对独立；
- 不同类型的接入层应各自分开，连接到对应功能区的汇聚层；
- 采用 POE 供电，PoE 供电方式更加灵活、方便，可以省却本地供电的繁琐工程；对 AP 的开关控制也更方便。

3.9.3无线 AP 设计

无线 AP：作为无线终端与校园网连接的桥梁。

- 与无线终端建立稳定无线连接；
- 对热点区域进行无线信号覆盖；
- 对热点区域内无线用户进行隔离；
- 与无线控制器建立无线数据通信隧道；
- 对热点区域进行信号采集和扫描。

3.9.4漫游方案设计

WLAN的用户存在一个天生的特点就是移动，当用户移动时，要求网络在保证安排的前提一下不间断的向用户提供服务。

二层漫游：在同一个子网内的AP间漫游。

三层漫游：在不同子网内的AP间漫游。

跨AC漫游：在不同AC间漫游。

3.9.5基于位置的页面推送方案

基于位置的页面推送可以实现无线网多业务运营，吸引更多用户，达到垂直运营的目的。基于位置的页面推送原理如下如图所示，无线控制器或 BRAS 可以将用户的位置信息比如 SSID、VLAN 等属性上报给 Portal Server，由 Portal Server 区分不同的用户进行不同页面的推送。

1. 用户 Portal 认证前，Portal server 推送基于位置的页面。
2. 用户输入用户名和密码后，发起 Portal 认证过程，AC/BRAS 通过 Radius 协议到 AAA 对用户鉴权。AAA 返回携带用户 Profile ID 的报文。
3. BRAS 通过 Portal 协议和 Portal 服务器交互，将 Profile ID 传送给 Portal 服务器。
4. Portal 服务器查找本地数据库，根据 Profile ID 推送相关页面。如对 Profile 为 VIP 用户推送 VIP 用户相关广告和信息，如针对 Profile 为女士推送化妆品和时装促销信息。

3.10 校园无线大数据应用

对于学校生活中的“大数据”国内已经有许多高校在进行率先应用，如华东师大的”餐饮预警“系统，根据学生的餐饮消费情况进行统计如果低于全校学生每顿饭消费均额的 60%，这些同学就会进入进一步核查的名单，之后进行精确的分析考察后会进行关注关怀等。某学生就由于就餐的减少而收到了这样一条短信“同学，发现你上个月餐饮消费较少，不知是否有经济困难？”。甚至某些大三大四学生由于将餐费拿去买考研资料而并不知道学校还有书费补贴，这时候预警系统也可以反映出来。也是体现了学校的一个人文关怀。

3.10.1 基于无线大数据可以开展的应用

大数据可以在两个层面提供应用：1、数据层面：将校园其他业务系统的数据导入大数据平台，融合校园其他业务系统的数据，做数据建模。2、应用层面：与高校业务系统相结合，提供基于位置的服务。

利用无线大数据可以做一下应用：

辅助决策：提供领导关注的面板，如就业率、生源地分析、消费分析、学生生活轨迹、上网行为等

教学管理：个性化教学、无线考勤、学风检查、空闲自习室查询

安全管理：失联预警、访客统计及跟踪、区域热力图

学生成长轨迹：学生成长轨迹、成长树、成长模板、数据名片

广告投放：基于位置的广告投放、根据用户行为精准广告投放

3.10.2 基于大数据的用户上网行为审计

随着互联网业务的不断丰富，网络带宽的持续升级，传统 X86 架构的行为审计已达到性能瓶颈，单台设备无法满足目前的的需求，只能通过关闭精细审计功能委屈求全，避免影响转发。因此大数据平台作为开放式架构的数据平台非常适合做大数据行为审计。大数据平台采用了 Hadoop 应用平台，海量数据查询速度提高数十倍

精细化的行为审计，完全符合公安部 82 号令和非经的要求，符合法律法规。同时精准的行为分析为每人提供了人物画像。

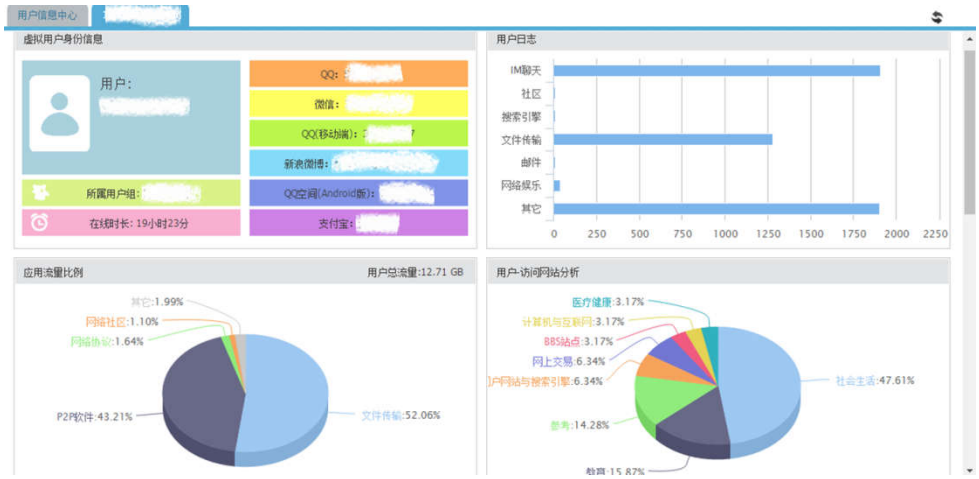


图 4-用户信息中心

图片 5-用户时间轴

3.10.3 基于大数据的定位行为轨迹分析

随着无线通信技术的发展及数据处理能力的提高，基于位置的服务成为最具潜力的互联网业务之一。特别是复杂的室内环境下，如会议室、报告厅、图书馆、超市、体育场等环境中，快速准确地获得移动终端或其持有者、设施与物品在室内的位置信息，并提供位置服务的需求变得日益迫切。

曲阜师范大学创新应用与定位正在相互融合、相互促进。通过无线通信及相关参数测量确定移动终端位置，而定位信息又可以用来支持位置业务和优化网络管理，提高位置服务质量和网络性能。所以，在各种不同的无线网络中快速、准确地获取移动位置信息的定位技术及其定位系统已经成为当前的研究热题，本次建设的无线系统需充分考虑曲师大无线定位技术的支持能力。

无线定位的应用领域概括起来可以包括四方面内容：1、导航，通过了解移动物体在坐标系中的位置，指导移动物体成功到达目的地；2、跟踪，实时了解物体所处位置和移动轨迹；3、虚拟现实，直观展示定位物体的位置和方向；4、基于位置的各种增值服务如基于位置的安全控制、广告推送等。各种无线定位技术也主要围绕这几方面开展应用。

在室内定位技术中，Wi-Fi 定位的精度为米级，相比 RFID、蓝牙等达到亚米级定位精度的技术，要逊色很多。很多人认为定位精度越高，定位所带来的价值越高。事实上，定位精度的提高势必带动成本的提高。此外，就目前的室内定位需求，如商场客流分析统计、基于位置区域的广告推送、定位拓扑监控等，米级的定位精度意味着抬头就能看见，已可以满足大部分需求。并且除了 Wi-Fi，其他技术都必须单独铺设信号发生器，有些还要求重新在前端部署信号接收装备，给大面积商用带来了很大的阻力。而 Wi-Fi 芯片在各类智能终端（智能手机、平板电脑）中已广泛普及，通过现有的 Wi-Fi 设备，可快速完成定位目标。因此，从技术的成熟度及规模应用的现实角度考虑，Wi-Fi 定位技术是当前最主流、也是最具发展潜力的定位技术手段之一。

基于有线无线统一管理框架，可以通过整网拓扑关系，直观定位 AP 设备直连的有线设备及业务传输路径（如图 1 所示），达到虚拟现实效果；在 AP 列表中定位相连的有线设备和有线接入端口，并可以直接进入有线端口界面进行分析，便于运维人员迅速定位设备问题，同时提供对端口的快捷操作，若有 AP 设备挂死则可以通过对 PoE 交换机接口进行关断处理，实现 AP 的启动，具有实用价值。同时提供对 AP 设备的 GIS 定位功能（如图 2 所示），直观展示部署了 AP 的热点所处的地理位置，实时反映热点的告警状态。

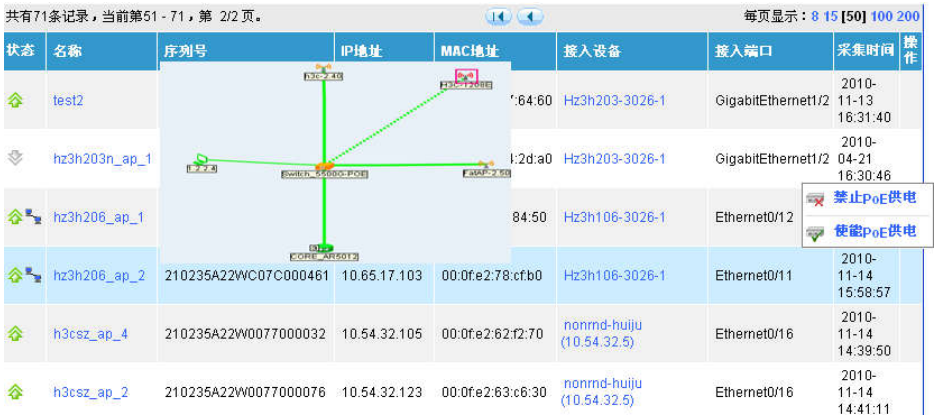


图 1 无线 AP 物理位置拓扑与接入关系定位

图 3 在 google 地图中定位无线 AP 设备

无线终端的定位、实时跟踪

无线定位解决方案提供基于 CUPID 定位手段，可以在拓扑中定位用户所在的物理位置、实时跟踪。CUPID 定位原理类似于军事领域用到的雷达测距。这时候，我们可以把 AP 看成雷达。AP 发射电磁波给设备终端，记录下发射起始时间，当终端侧收到该信号后，会发送返回信号给 AP，同时记录下返回时间。往返时间这时候就是关键因素，双向传播时间有了，计算距离就成了很简单的事情，那定位也就水到渠成了。如果想要定位精度好的话，我们可以计算出终端和多个 AP 的距离，经过简单算法，就可以计算出终端的准确位置。信信号波动完全不影响定位，当无线环境好的时候，定位精度可达 2-3m。

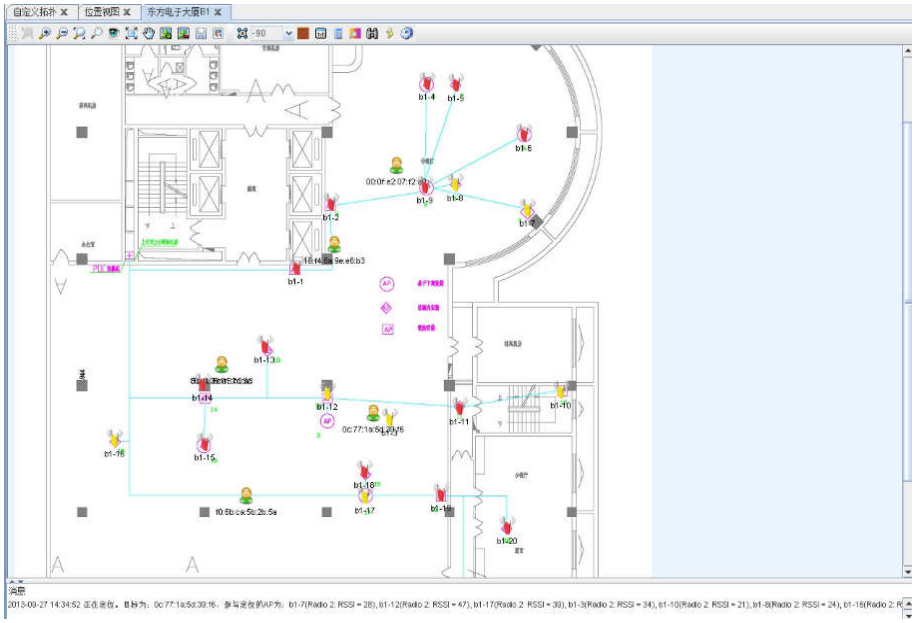


图 3 无线定位效果图

基于位置的（人流）数据分析

基于位置的数据分析包括区域监控和停留时间统计。前者可针对某一区域对用户密度进

行监控移动轨迹记录（如图 4 所示），可通过地图显示和记录用户的移动轨迹流量统计，可按照时间段统计某区域的用户密度变化历史查询，可输入历史时间查询某处区域的用户密度（如图 5 所示）。停留时间统计记录用户的运动轨迹和停留时间，可按照日、周、月、年等不同时间粒度进行分析统计偏好分析，根据用户的行走路线和停留时间挖掘用户的偏好行为和消费习惯。

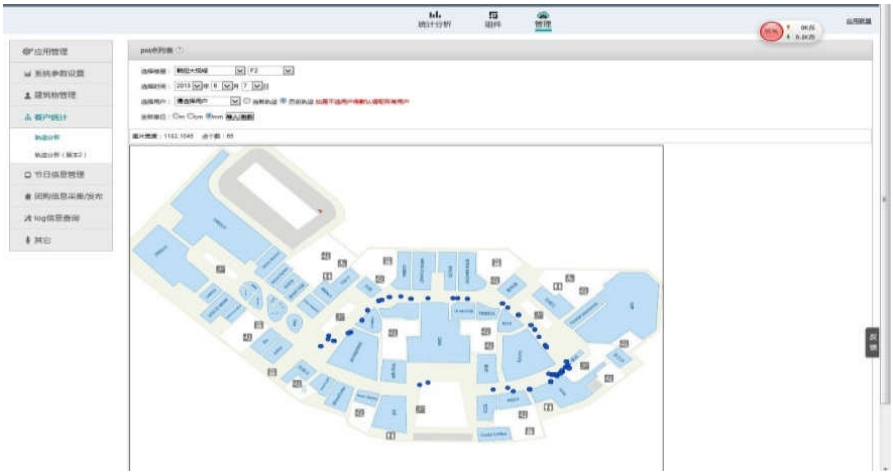


图 4 单用户轨迹图

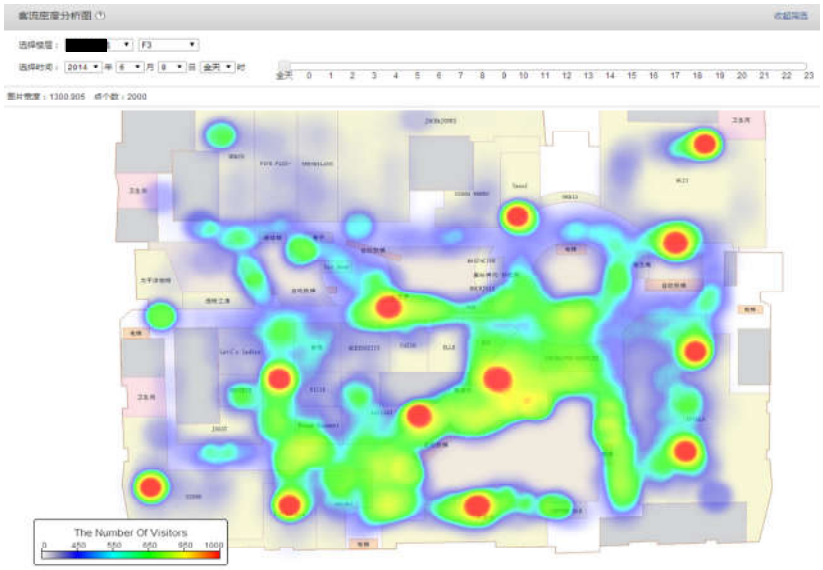


图 5 区域热图分析

3.10.4 基于无线位置的访客 PORTAL 推送

个性化认证系统与无线设备对接实现象不同位置推送不通的 portal 页面、不同的认证是方式（短信认证、微信认证、用户名等认证方式）。可在不通无线场景中灵活设置适用该场景的无线接入方式。

3.10.5 基于无线大数据的精准页面推送

地理位置定位 利用 Wi-Fi 热点地理位置可定位的特点来开展广告服务，广告主通过选择特定的地域和热点来推送广告，使广告主的广告能吸引最有可能购买其产品的潜在客户。同时，广告主还可以针对不同地理区域制定相应的特价促销或优惠活动方案，使广告的投放更加精准，更有针对性，能将定制化的信息推送到 Wi-Fi 用户，进行有效的广告宣传。

此次无线网络的搭建还可以开展商业活动，基于位置的广告页面推送，例如学生走到一家校内店铺或图书馆，可以根据不同的店面或位置弹出不同的页面信息。更方便的为学生提供信息推送。

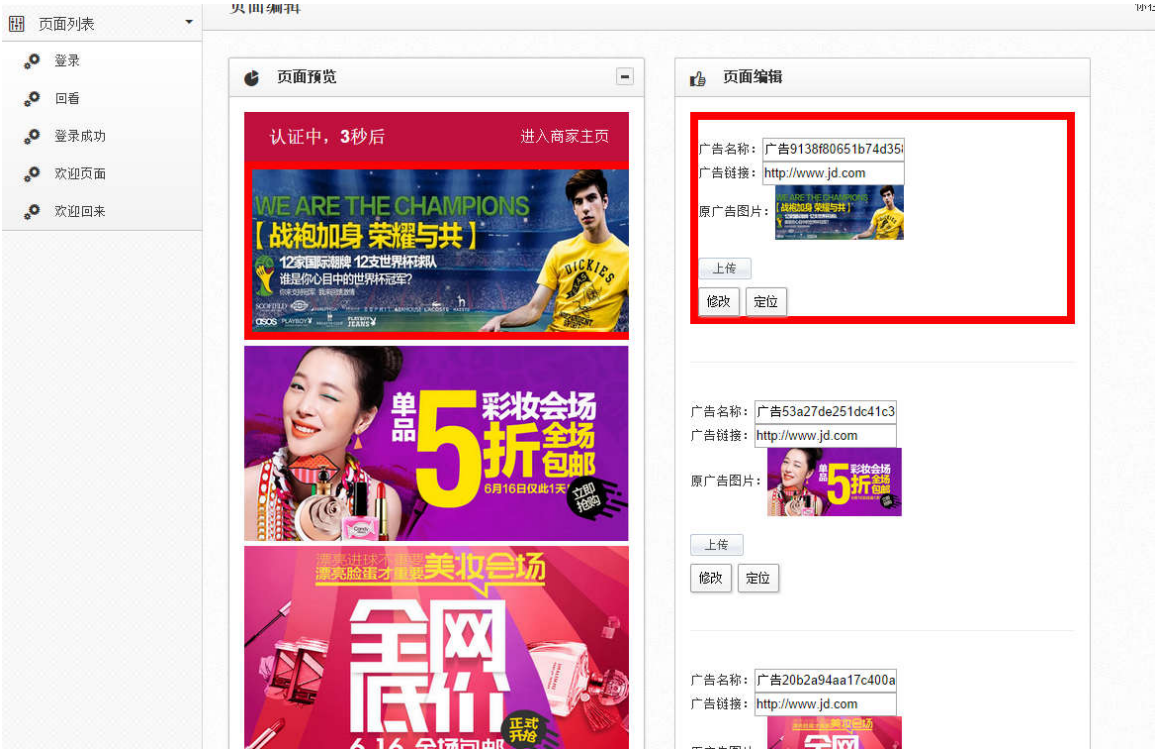
系统提供多个标准的公共 Portal 模版，其中包括页面框架、布局、样式。系统允许企业管理员在选择某个公共模版的基础上根据自身需求调整文字和图片，保存成形成供自己使用的个性化 Portal 页面主题。系统对个性化 Portal 页面主题的数量不做限制。

内容上传

提供内容上传页面，企业管理员填写待上传内容的相关信息（内容名称、描述、分类、上传路径）后，选择本地需要上传的图片等内容。

内容分为文字、图片、静态网页、音频和视频等多种类型，用户可新增、查询、删除内容。

内容上传完毕后可对内容配置 URL 连接属性，配置该属性后，当鼠标点击内容时会跳转到相应的连接页面，这里可以与第三方页面实现互通。



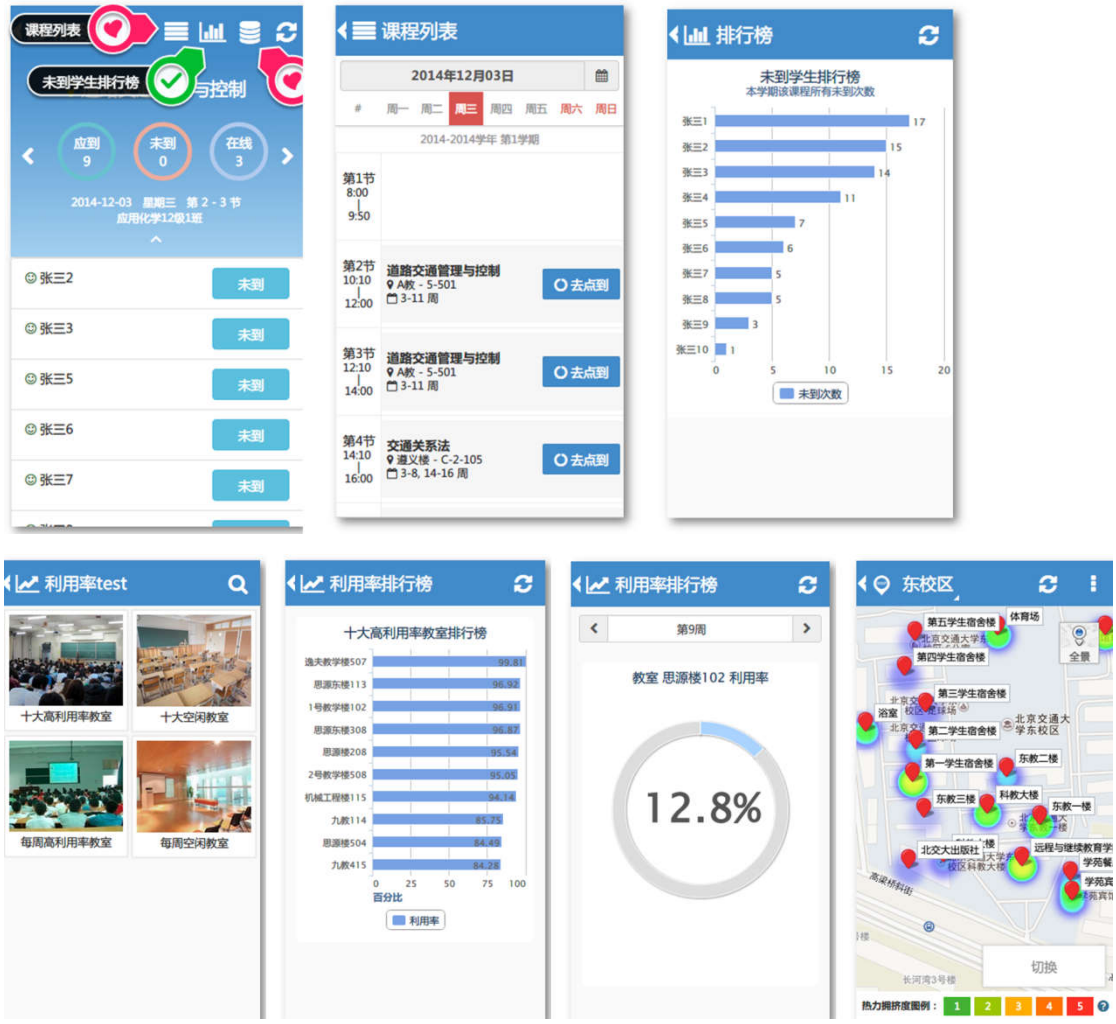
3.10.6 结合学校系统定制化开发

可以实现基于位置的安全控制，通过设置控制区域，判断移动终端进入进出，对进入该区域的客户推送短信告警，并知会后台管理人员及保安系统实时监控该名人员，追踪用户的运动轨迹、深入分析其网络行为，及时发现安全隐患。可实现基于不同类型终端、不同用户角色、不同时间点、基于不同位置的安全策略控制。

支持基于 REST 的 API，通过 REST API，允许 Web 应用程序开发人员能够轻松快速的开发位置感知的应用程序。与 SOAP API 相比，REST API 有更好的性能、可扩展性、简易性、可修改性、可见性、便携性和可靠性。可以根据 MAC 或 IP 查询某个移动终端的当前位置信息、或所有终端的当前位置信息。并且 REST API 还可以提供终端 MAC、终端类型、用户信息等内容，便于曲师大基于位置信息或终端信息进行增值业务开发，例如：

- 通过位置汇总人员密集度，通过热图展示给学生，学生可根据显示寻找到无人的自习室
- 学校 RTLS 系统辅助学校完成课程热图分析，帮助学生找寻丢失的移动终端等；
- 寻找特定的无线客户端的当前位置。

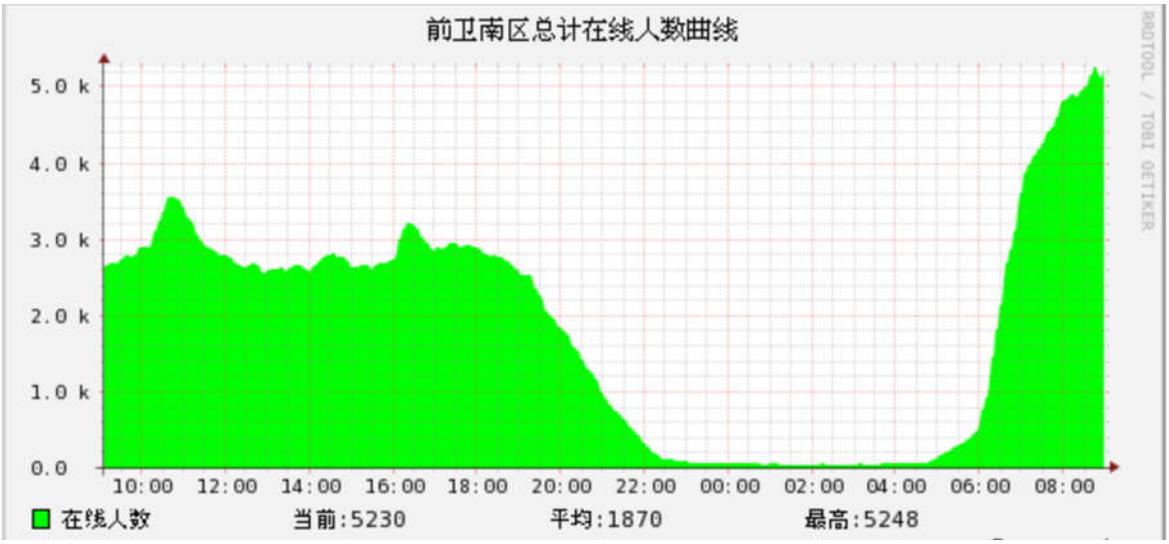
校园应用示例：

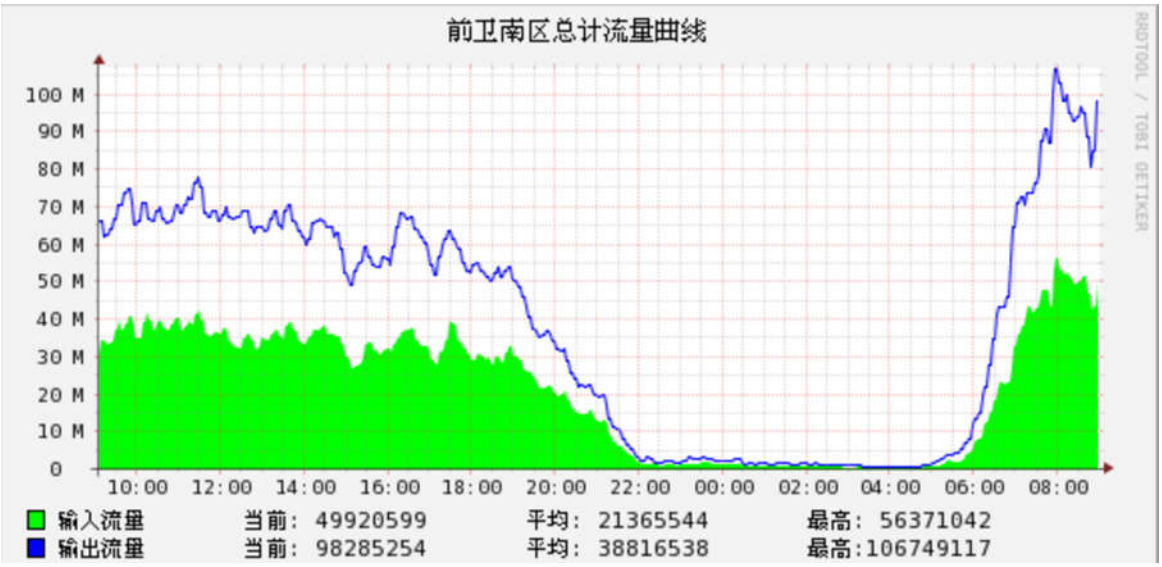


3.11校园无线服务网站建设

校园无线系统规模大、运维管理工作量大，项目建设的进展、无线覆盖的范围、无线 AP 设备列表、教职工的使用指南、客户端下载等信息需要及时的公布，以便于更好的服务于广大师生。系统建设概要建议如下：

另，系统可开放必要的信息，例如流量信息图，例如





3.12统一网管平台方案

网络管理产品以保障安全生产，提高网络服务质量管理为目标，定位于建立有效的网络管理流程体系，从快速故障定位和排除、 设备性能检测、 网络流量和容量分析， IT 运维流程等方面切入，全面监控网络运行，快速故障发现和恢复，规范网络运维，保障不间断地提供 IT 服务。

充分利用校方现有网管平台，在同一网管平台上实现如下的功能，包括资产管理， 性能监控，故障管理，拓扑管理， IP 地址管理，服务台管理， 配置备份， 配置分发， 巡检管理， 网流分析， 通告管理， 业务关联， 分析报表等功能。

系统可监测并管理常见的网络设备、服务器、数据库、中间件、虚拟化资源、通用服务等 IT 资源，支持 SNMP、CLI（Telnet、SSH）、WMI、JMX、CORBA 等远程非代理监测和 Agent 代理监测 两种手段，还支持分布式采集、集中管理模式，为业务网络提供 7X24 不间断监测服务。

集中监控

系统架构设计从下往上分为采集层、处理层和展现层：

- **采集层**

包括分布式采集探针和各监测采集模块，通过采集层获取所有被管资源的实时运行信息并送入处理层进行数据分析和处理。

探针分布式采集主要面向服务器、应用系统、业务系统的采集，可以完成分管区域的数据收集处理，从而有效地减轻了集中管理服务器的负载。

- **处理层**

通过统一事件平台和统一性能管理对采集层所采集的数据进行统一处理和分析，按照事件和性能进行处理，并将处理好的标准数据送入性能管理数据库。

- **展现层**

通过拓扑、报表等多种图形化方式直观、全面的展现被管资源的实时运行信息，帮助管理人员全面了解所辖范围内 IT 资源的运行情况

3.12.1 资产管理

资产管理模块支持对网络中资产信息的系统管理，并且通过事件关联，Netcool 网管系统中的故障事件能自动和资产数据关联，从而方便用户查找故障相关的设备/线路等丰富信息。

设备信息管理

- 自动采集：系统可以自动定时探测设备信息：设备名、序列号、IOS 版本、端口信息、模块信息、CDP 连接表等。

- 即时采集：用户触发采集动作，系统即时发起探测获取谁呗信息；
- 手工录入：对于无法采集的信息，如设备维保日期、机房、机柜、配线架等，可进行手工维护；
- 所有信息支持 Excel 格式的导入导出；

资产信息的权限维护

- 可设定用户组、用户和 CI 项的管理关系，特定区域的设备由特定的维护人员进行管理
- 支持只读，可写权限分配；
- 支持按数据内容进行模糊匹配；
- 查询网络设备的软件版本历史变更记录

信息业务关联

- 系统为开放型设计，支持用户数据表和内容的动态扩充，适应用户变化的需求；
- 可灵活定制表描述文件，支持子表关联，实现可视化查询和管理；
- 可定制字段的呈现方式，按不同定制条件显示颜色；
- 可视化定制资产展现树；

资产动态更新

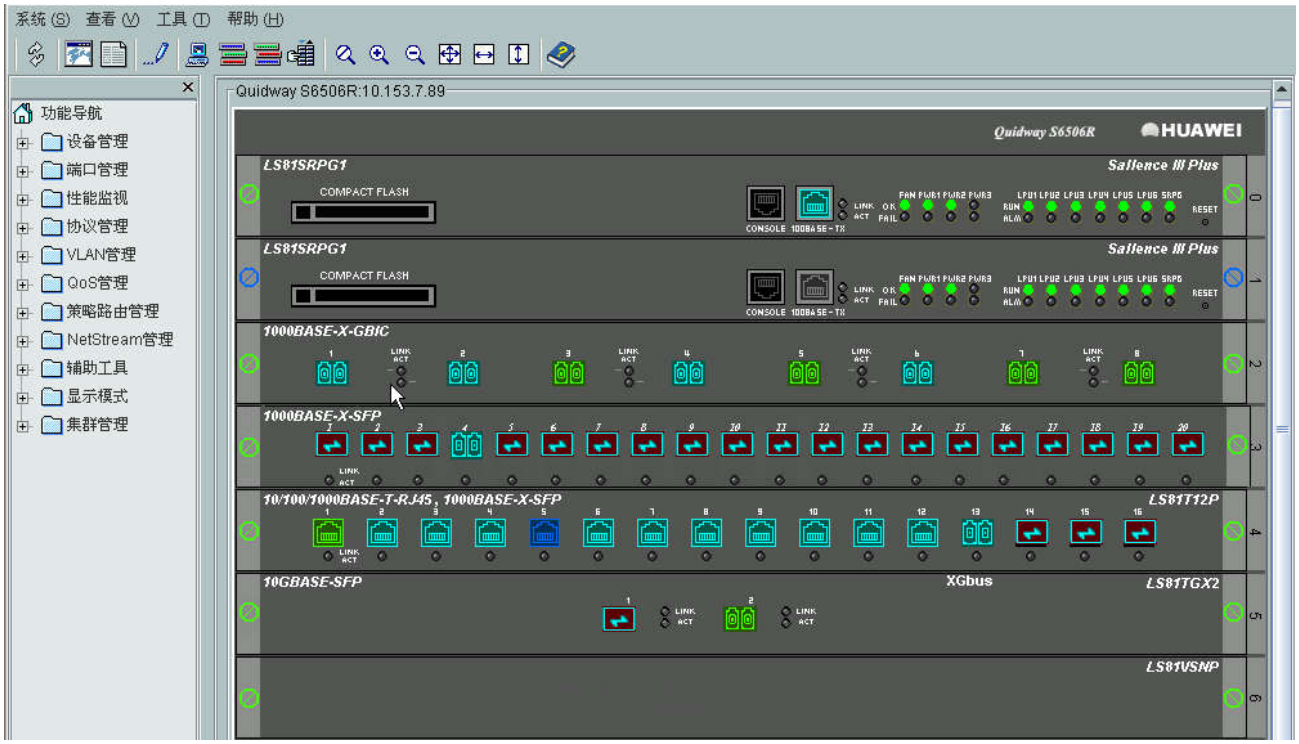
- 增加资产对象：可以按照当前的资源模型生成相应的资源对象；
- 删除资产对象：在网管人员确认下可以删除该资源对象；
- 资产属性的变更：可以根据资产属性的变更情况自动更新相应资产的属性信息；并当关键属性变更时，产生相应的变更通知事件；

资产信息查询

- 可根据条件对所有资产信息进行模糊查询；
- 可查询 CI 项的历史变化信息。

3.12.2 配置管理

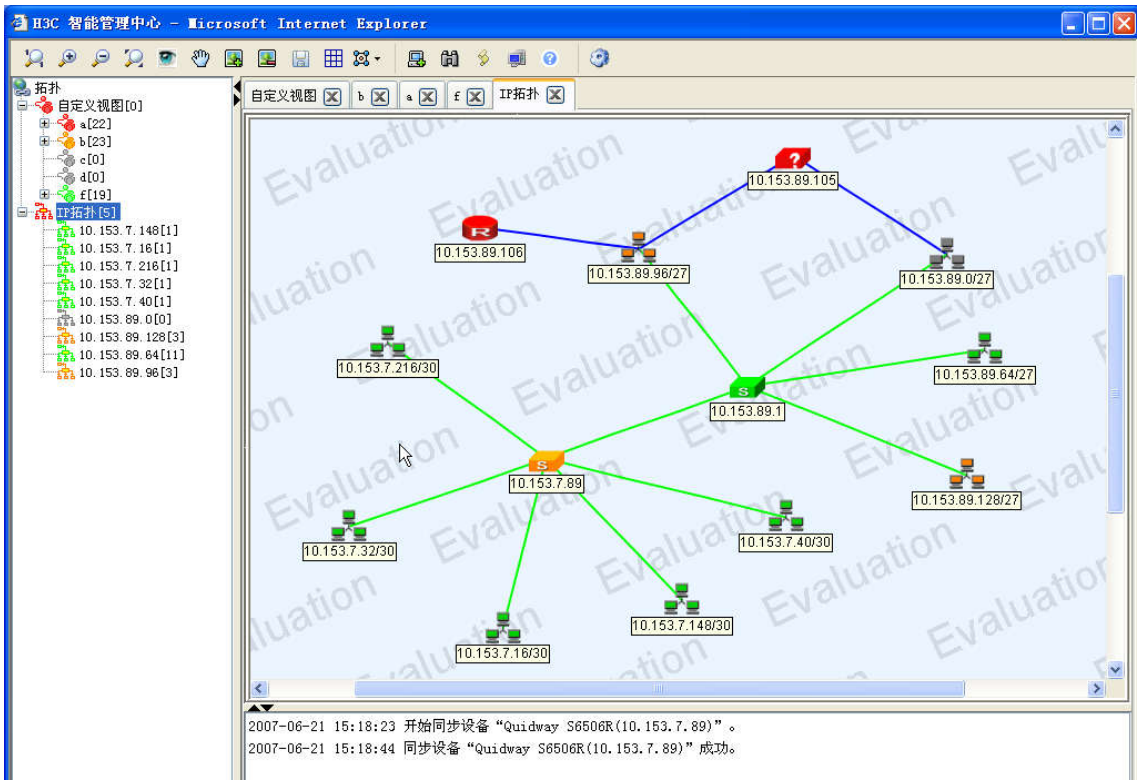
全网资源的统一部署、管理和调配中心，包括对路由器、交换机、安全、无线、语音、存储、服务器、PC、UPS 等设备类型，实现了故障、性能、拓扑、配置等管理内容，成为业务融合联动的基础。



iMC 设备面板管理

设备标签	Quidway S6506R
IP地址	10.153.7.89
设备状态	重要
系统名称	Quidway S6506R
制造厂商	Huawei
系统运行时间	289天11小时20分9秒
未确认告警	紧急0，重要4，次要6，警告0
CPU利用率-[CPU:.0]	13.0%
CPU利用率-[CPU:.1]	14.0%
CPU利用率-[CPU:.2]	14.0%
CPU利用率-[CPU:.3]	7.0%
CPU利用率-[CPU:.4]	6.0%
CPU利用率-[CPU:.5]	5.0%
CPU利用率-[CPU:.6]	12.0%
CPU利用率-[CPU:.7]	5.0%
内存利用率-[内存:.0]	41.58%
内存利用率-[内存:.1]	41.51%
内存利用率-[内存:.2]	23.66%
内存利用率-[内存:.3]	61.12%
内存利用率-[内存:.4]	61.89%
内存利用率-[内存:.5]	27.34%
内存利用率-[内存:.6]	23.45%
内存利用率-[内存:.7]	19.94%
设备响应时间	5.0ms
设备不可达比例	0.0%
总在线用户数	1

iMC 设备状态管理


H3C 智能管理中心 - Microsoft Internet Explorer
拓扑
自定义视图[0]
a[22]
b[23]
c[0]
d[0]
f[19]
IP拓扑[5]
10.153.7.148[1]
10.153.7.16[1]
10.153.7.216[1]
10.153.7.32[1]
10.153.7.40[1]
10.153.89.0[0]
10.153.89.128[3]
10.153.89.64[11]
10.153.89.96[3]
自定义视图
b
a
f
IP拓扑
10.153.89.105
10.153.89.106
10.153.89.96/27
10.153.89.0/27
10.153.7.216/30
10.153.89.64/27
10.153.89.1
10.153.7.89
10.153.89.128/27
10.153.7.32/30
10.153.7.40/30
10.153.7.148/30
10.153.7.16/30
2007-06-21 15:18:23 开始同步设备“Quidway S6506R(10.153.7.89)”。
2007-06-21 15:18:44 同步设备“Quidway S6506R(10.153.7.89)”成功。

iMC 拓扑管理

iMC 设备性能管理

iMC 对象告警设置

身份与接入管理

支持 LAN、WAN、WLAN、VPN 认证接入，实现接入业务的统一、集中管理；支持智能卡、证书等强认证功能，支持多种方式的端点准入控制和基于身份的网络服务，实现用户与资源和业务的融合管理。

端点安全准入管理

在身份接入基础上，支持终端安全准入控制，支持安全状态评估、网络中安全威胁定位、安全事件感知及保护措施执行等，预防因未打补丁、病毒泛滥、ARP 攻击、异常流量、非法软件安装和运行等因素可能带来的安全威胁，并可根据终端的安全状态实现终端下线、隔离、提醒、监控等多种控制策略。从端点接入上保证每一个接入网络的终端的安全，从而保证网络安全。

MPLS VPN 管理

实现网络资源与 MPLS VPN 业务的统一管理，除基础的网络设备管理外，还包括 MPLS VPN 业务部署、业务监控、业务审计等内容，为客户提供了端到端的全流程业务管理功能。

ACL 管理

ACL 管理实现了 ACL 这种网络重要资源的集中管理，通过全网 ACL 的视图，方便的展示给用户一个网络中 ACL 部署情况的蓝图；ACL 部署功能实现了全网 ACL 的批量配置和下发，有效减轻了用户日常的管理工作量；此外，ACL 管理还提供了 ACL 模板、ACL 规则优化等功能。

智能配置中心

可以帮助管理员方便的对设备配置文件和软件文件进行集中管理，包括配置文件的备份、恢复以及批量更新、设备软件的备份和升级等功能；同时提供设备配置的基线化版本管理，可以对配置文件的变化进行比较跟踪。

网络流量分析系统

实现各种网络流量信息统计和分析功能，能够让客户及时了解各种网络应用占用的带宽、消耗的网络资源和 TopN 流量的来源，并提供丰富的网络流量分析报表。可以使用支持 NetStream 的路由器和交换机提供网络流量信息，也可以使用 DIG 探针采集器对网络流量信息进行采集。

3.12.3 巡检管理

巡检参数

- 支持 TELNET/SSH 方式登录；
- 允许用户自行设置命令和策略；
- 巡检参数：调用资产列表，用户将巡检策略和设备/端口关联，设置巡检时间；
- 巡检频率：可设置时间策略，定期触发；

巡检模板

- 系统支持命令行方式设备登录和巡检，命令比较支持正则表达式匹配，并可设定计算表达式；
- 可设定工作时段和非工作时段阀值标准；

阀值比较方式：

- 数字比较（大于，小于，数字增量异常）
- 字符处比较（出现某个字符，不出现某个字符）
- 文本比较（与上一次比较，表格数据比较，行数变化，内容变化等）
- 系统运行时间异常

巡检管理

- 通过预先设置的基准规则,自动对设备进行配置、运行参数等方面的批量定期检查，一旦发现有不合规或超过预设阀值的现象，则发出告警到 Netcool 平台；
- 自动化巡检系统能对所有支持 Telnet 或 SSH 协议的设备进行检查；
- 管理/启动自动巡检功能。通过运行 Telnet 脚本采集网络设备数据；若巡检结果异常，发送 syslog 到 Netcool 网管平台。
  - 可以自定义巡检任务
  - 可以针对不同设备，定义不同的巡检命令集、巡检时间策略等
  - 支持手动触发巡检
  - 巡检报告可以自动和上期报告比对，将差异内容以显著颜色标示
  - 支持多厂商巡检，如思科、H3C、F5 之类设备
  - 巡检报告生成可查询和下载，巡检报告以 Excel 方式下载，罗列巡检结果，标识异常数据
  - 历史巡检查询，可保存 30 天以上数据（数据保存周期可配置）

3.12.4 广域网链路监控

监控方式

- 接收并解析中心路由器 syslog，通过 Netcool 平台发出告警；
- 探测中心路由器广域网端口状态，当端口状态变为 down 时发出告警到 Netcool 平台；
- 监控广域网链路流量，对流量值进行智能分析，建立动态基线和突变基线，当实时值偏离动态基线或突变基线时，发出预警信息至 Netcool 平台；
- 定时从中心路由器向对端路由器广域网地址发起 Polling，分析 Polling 结果，发出链路中断或丢包告警至 Netcool 平台。

信息丰富

- 在资产信息管理模块中，维护广域网链路的信息：专线用途、专线带宽、专线号、专线运营商、报修电话、对端联系人、对端联系方式、线路名称，线路分类，线路类型，骨干网线路名，线路月租费，对端端口类型，对端机构，服务商 ID 等；
- 发生广域网链路中断或流量超过阀值时，自动将资产管理中的信息丰富到事件中，减少监控人员排障时间。

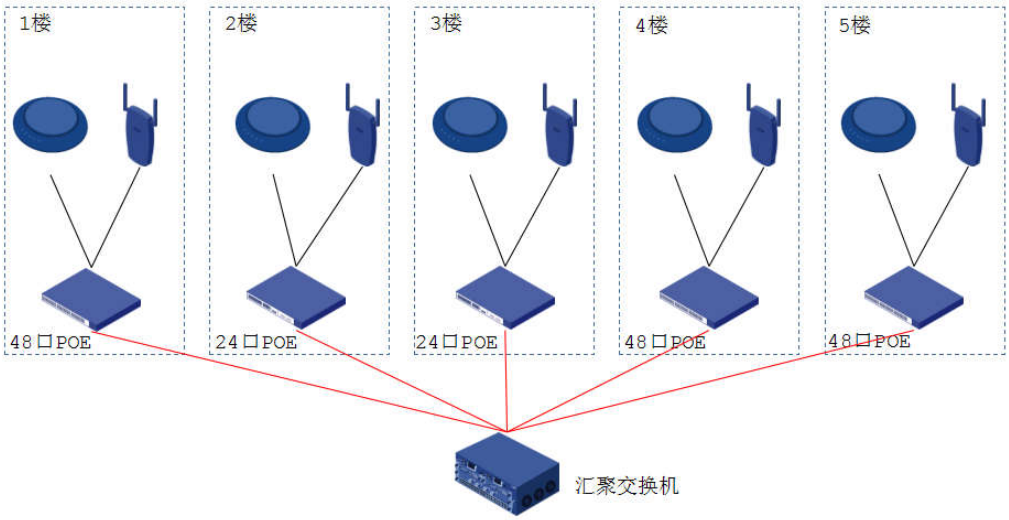
备份关系管理

连接到分支行的广域网专线存在两条或两条以上时，系统支持对链路进行备份关系管理，对单条链路的故障和多条链路同时故障的情况进行分级别告警。

- 在资产管理系统中，维护链路的备份关系
- 系统通过比对 Netcool 事件平台的广域网链路事件与资产系统中的备份关系，当发现同一分支行的多条链路同时发生故障时，将故障事件进行升级。

4 两校区无线热点图

本次方案建设为校园无线网，包括 2 套无线控制器（含 AP 授权）、3800 个室内外 AP、POE 交换机、无线汇接设备、一套有线、无线综合运维管理系统，及配套光纤模块等。



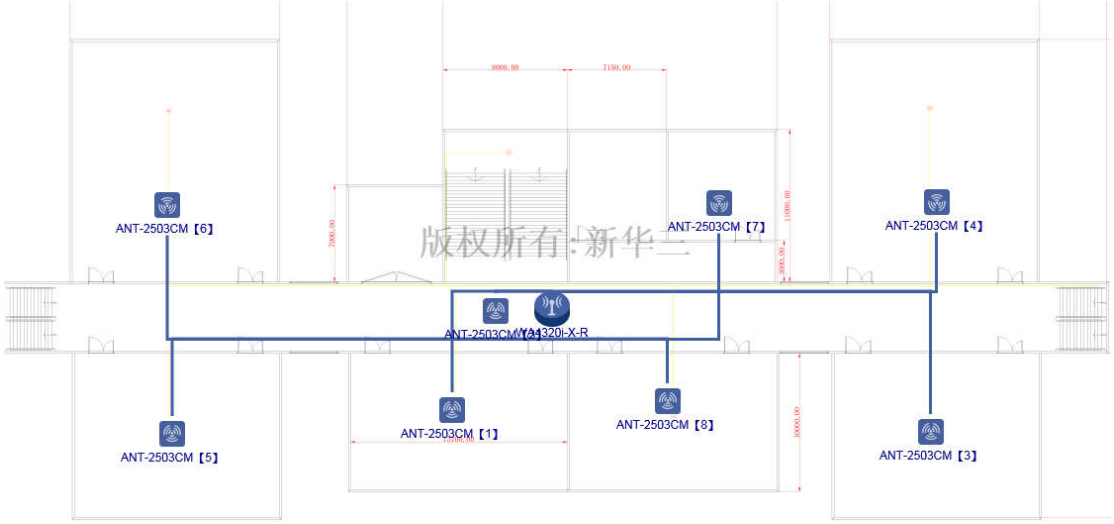
汇聚拓扑示意图

本次无线网建设物理上与有线网保持相对隔离，由汇聚交换机、无线控制器、无线 AP、POE 交换机及相应管理系统等构建成无线接入网，接入校园网络核心，建立与有线网络相对隔离的全校无线网络。

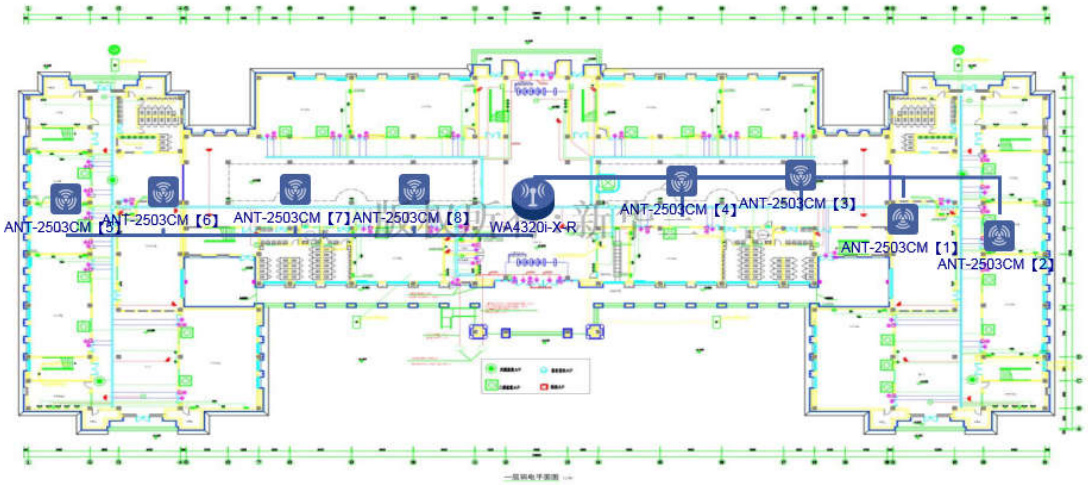
4.1曲阜校区

曲阜校区校园无线网覆盖范围包括：外国语学院、教育学院、数学学院、成教学院、化学院、激光院、物理学院、孔子会堂、国学院、书法学院、书法艺术实训中心、科技实验大楼、老办公楼、校史馆、体育学院、篮球馆、文史大楼、老西联教室、生命科学院、综合教学楼、第二食堂、计算机基础实验中心、校医室、大学生交流中心、学术交流中心、教工活动中心等。

曲阜校区大学生活动中心：



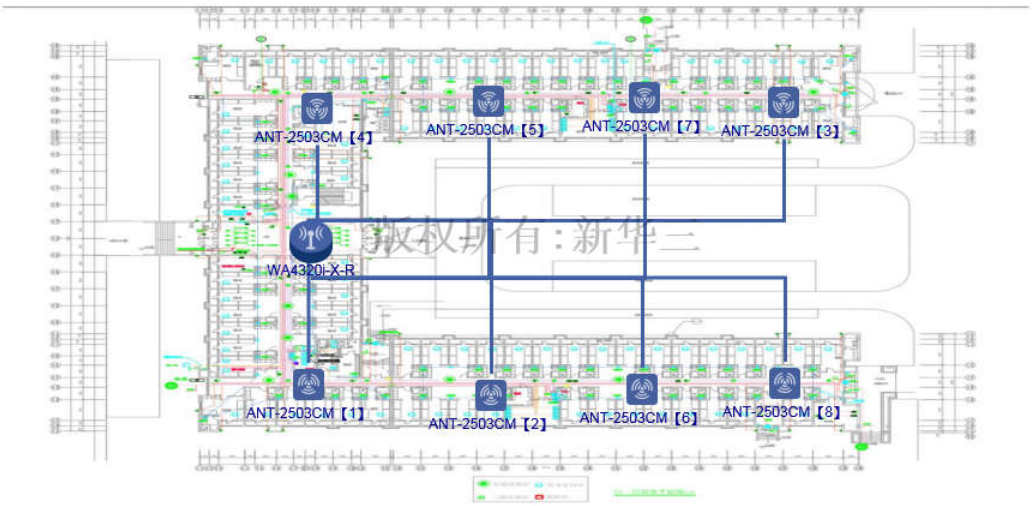
曲阜校区科技实验楼：



4.2 日照校区

日照校区无线网覆盖范围包括：S 楼、图书馆、实验中心、大学生活动中心、太阳广场、日月广场、校园绿地、网球场、篮球馆、足球场、会馆、国际学院、经济学院、美术学院法学院、信息科学与工程学院、音乐学院。

日照校区实验中心：



5 无线建设监理及验收

5.1监理团队组成

组建各参建单位、部门以项目经理为主导和相关责任领导挂帅的高效统一管理架构。相关主体单位为建设单位的工程主管部门和相关维护部门、采购部门，监理单位、设计单位、施工单位、设备厂家等。

通过建立高效统一的项目团队，加强了对项目的整体控制力度；方便解决了调动各方人员，协调多方关系，使各方全力参与和配合； 对于项目实施中需调度资金、物资、设备等多的问题解决起来更是得心应手。在项目前期，为了使项目团队沟通协作更顺畅还可组织各单位项目经理培训，加强掌握该工程项目管理机制和特点。先进性和实用性

本期工程项目相关的专业较多，涉及单位多，项目工程量大，工程复杂，项目实施团队中成立专项信息管理小组是相当必要的。信息的及时、准确、高效对工程的整体及细节控制都可以起到相当重要的作用。

5.2监理工作内容

监理小组负责收集该工程每天、每周的进度信息及相关工程（如核心网工程、无线设备安装、综合布线等）进度信息，以及工程中遇到的各种大小问题（如配套传输进度不匹配，设备、材料到货不及时，施工日进度不理想，敏感站点，设计图变更等）。通过对信息和计

划的分析对比，为工程整体或阶段细节计划的安排调整提供依据。同时还可提高工程生产率，有效地控制不必要的施工“停工、误工、窝工”等的情况。

为了进一步加强信息总控对工程的有效性，我们还建立一个信息共享的平台，及时通报相关参建单位。比如，每日、周召开一次工程例会和合署办公、项目日周报等方式保持高效的沟通，通报工程进展情况、协商处理存在的问题，明确职责任务。

为确保工程质量，充分发挥好项目团队和专家团队的作用。采取每天安排多支质量巡检队伍（含建设单位、厂家、监理、施工等组成）不间断地进行现场巡检，将现场发现的问题及时要求施工单位进行整改，必要时现场还可由专家实地指导，形成巡检报告通报各施工单位队伍，有效地提高工程施工质量。

5.3监理施工规范

设备安装

壁挂式机柜（机箱、网络箱）安装时底部距地面距离宜在 1. 2~1.5 米之间，内部应无多余扎带头、线头和其他杂物，机柜表面应无污渍，安装完成后将机柜内外擦拭干净；

室内 AP 安装

AP 的安装位置便于网线、电源线、馈线的布线，便于维护和更换；

AP 的安装位置距离地面的高度不应小于 1.5 米；

AP 设备安装在弱电井内、墙面时，为防止 AP 被盗，建议将 AP 安装高度在 2 米以上，并在固定架加锁或是将 AP 安装在专用防盗机箱之中，并保持良好通风，保持工作环境清洁无灰尘；

AP 与以太网交换设备之间布线距离不能超过 80m；

AP 安装位置的四周有特殊设备，如微波炉、无绳电话等干扰源，建议 AP 离开此类干扰源 3 米；

如果吊顶为石膏板或木质，可将 AP 安装在 吊顶内，但必须做好固定，在附近须留有检修口；

室外 AP 安装

1、室外型 AP 安装时必须接地，AP 的保护地、天馈防雷器、电源 PE 保护地、室外射频电缆、天线支撑件的接地点应分开并且接触良好，不得有松动现象，并作防氧化处理（加涂防锈漆、银粉、黄油

2、室外 AP 设备必须牢固安装在支撑架上,其高度和位置符合设计方案的规定；

3、室外 AP 应避免安装在易积水的位置；室外 AP 设备与馈线之间接头处应采取防水措施（使用防水胶泥缠绕），未接线的出线孔应用防水塞封堵；

4、安装在楼顶屋面的 AP，应选择无日光直晒或直晒时间较短的位置，必要时采取相应防护措施；

5、天线实际安装位置、角度、型号应与工程设计要求相符；

6、天线必须使用天线的专用支架，牢固固定，支架做好防雷连接；

7、天线与跳线的接头应连接紧固，并用防水胶泥和防水胶布作防尘和防水处理；

8、避雷针的位置应与 AP 安装的抱杆分开，将避雷针焊接在专用抱杆顶端，再将抱杆采用 40mm×4mm 的扁钢与防雷地网相连；

9、在平原地区，避雷针的保护角小于 45°，高山及多雷地区，天线的避雷针保护角要小于 30°，且其防雷接地（避雷针等装置的接地）应与机房的保护接地共用一组接地体；

10、将天线远离微波炉和 2GHz 无线电话。因为这些设备和天线的工作频率相近，会产生强烈干扰信号，从而干扰天线和 AP 设备的正常工作。

室外空旷区域总体宜按照蜂窝网状布局执行，尽量提高频率复用效率，将信号均匀分布，控制每个 AP 覆盖区域的重叠区域。

线缆布放

五类线接头应符合设计和施工操作规程，布放前必须核对缆线标示内容是否正确，缆线中间不允许有接头；

五类线必须按照设计文件的要求合理布放。布放时要求走线合理，绑扎牢固，走线应自然平直，不得产生扭绞、打圈接头等现象，不应受到外力的挤压和损伤；

制作五类线缆长度应留有余量。交接间、设备间对绞电缆预留长度为 0.5-1.5 米，有特殊要求的应按设计要求预留长度；

五类线的绑扎：在管道内、弱电井和吊顶内隐蔽走线时绑扎间距不应大于 40 cm；在管道开放处和明线布放时，绑扎间距不应大于 30cm。五类线必须用扎带牢固绑；

五类线的弯曲半径应符合：非屏蔽 4 对对绞电缆的弯曲半径应至少为电缆外径的 4 倍；屏蔽 4 对对绞电缆的弯曲半径应至少为电缆外径的 6-10 倍；主干对绞电缆的弯曲半径应至少为电缆外径的 10 倍；

五类线宜穿管或沿金属电缆桥架敷设，管路的截面利用率应为 25%～30%，线槽的截面利用率不应超过 50%；

单一五类线的布放长度不能超过 100 米，如实际单一布放长度大于 100 米应采用其他合适方案解决；

五类线应避免与强电、高压管道、消防管道等一起布放，确保其不受强电、强磁等源体的干扰。

五类线进入室内时需做好防水处理，做防水弯；

5.4监理技术规范

射频规范：

1、对于室外区域干扰宜采用调整(定向)天线方向角，避免天线主瓣对准干扰源的方式或调整功率。

2、在一个 AP 覆盖区内直序扩频技术最多可以提供 3 个不重叠的信道同时工作。考虑到制式的兼容性，相邻区域频点配置时宜选用 1，6，11 信道。频点配置时首先应对目标区域现场进行频率检测，对于覆盖区域内已有 AP 采用的信道，应尽量避免采用。

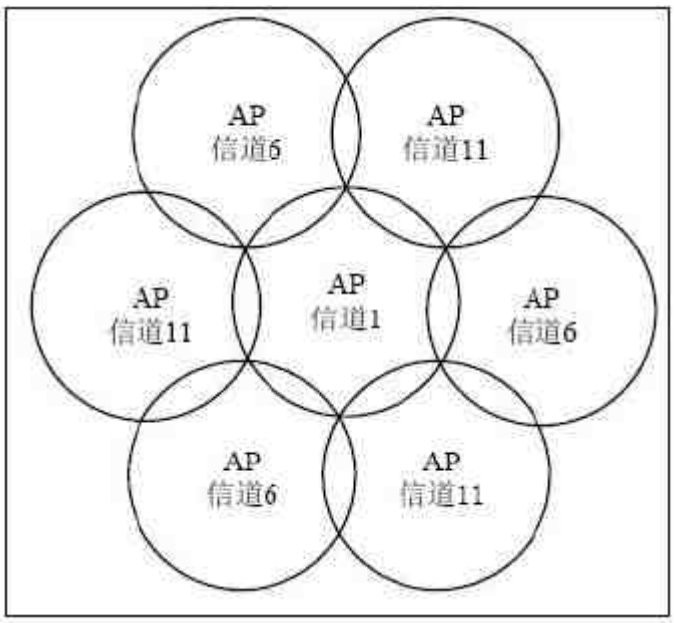
3、AP 部署时需对覆盖区域进行频率清查，掌握频率干扰及占用情况，进行频点选择和干扰规避。无线干扰控制措施：

4、在一个 AP 覆盖区内直序扩频技术最多可以提供 3 个不重叠的信道同时工作。考虑到制式的兼容性，相邻区域频点配置时宜选用 1，6，11 信道。

5、频点配置时首先应对目标区域现场进行频率检测，对于覆盖区域内已有 AP 采用的信道，应尽量避免采用。

6、对于室内区域存在多套室内覆盖系统的情况，应充分考虑其他通信系统使用的频段，设计时预留必要的保护频带，以满足干扰保护比的要求。

7、室外 AP 覆盖区频点配置时，为了实现 AP 的有效覆盖，避免信道间的相互干扰，在信道分配时宜引入移动通信系统的蜂窝覆盖原理。对 1，6，11 信道进行复用，见下图：



容量规范：

房间内要求无线信号在室内任何空间信号强度 2.4G、 5G 同时不低于-70 dbm，丢包率小于 1% 。室外环境无线信号在无线蜂窝覆盖边缘信号强度 2.4G、5G 同时不低于-75 dbm 。同时为了达到信号稳定，同频率、同信道的干扰信号强度不得高于-60 dbm。

网页打开速度测试≤1s。在目标覆盖区域内 95％以上的位置，接收信号电平≥-75dBm；在 AP 接入点附件（<5 米）信噪比应不小于 25dB；在目标覆盖区域内，以 64 字节数据包对 AP 网关进行 Ping 测试，平均时延≤50ms，丢包率≤3%；在目标覆盖区域内，单用户接入 AP 进行局域网内 10 次 ping 测试时，应全部联通；覆盖区域内单用户上行或下行单向吞吐率应不低于 300Kbps。

3)目标覆盖区域内 95%以上的位置，公共服务标识的信号强度不低于-75dBm。目标覆盖区域内 95%以上位置，用户终端接收到 i-jining 下行信号信噪比大于 20 dB。

5.5工程实施

5.5.1工程实施内容

针对本次项目项目实施内容如下：

- 制定参与本次工程的资源计划，并按工程进度要求派出现场实施的项目小组。
- 对机房现场进行勘查，提供机房环境需求，协调用户按工程进度完成现场准备工作。
- 完成设备现场开箱验货。

- 完成各局点网络设备物理安装工作。
- 进行设备的上电验收测试并确认设备版本信息
- 安装地用户运维培训。
- 按照设计方案和实施方案，完成本次项目中所有网络设备的调试工作。
- 协助用户完成项目初验
- 如涉及第三方网络产品，编制第三方项目的集成计划，包括：第三方设备硬件验收清单、工程技术文档、工程施工文档等。

5.5.2工程实施计划

设备装调总体计划包含两个方面：其中之一是安装调试进度计划；另一个是安装调试过程计划。

对于安装调试进度，我们依据曲阜师范大学本次项目总体进度要求，在规定时限内完成网络设备的安装调试及网管软件的安装调试，实现系统的试运行。

安装调试过程计划包含对于具体实施环节、具体设备的实施计划，在制定系统设备的安装调试计划时，由专门的技术人员和曲阜师范大学信息部门的业务人员一起制定软硬件系统的测试计划。

5.5.3 设备安装调试

本项目所涉及的设备安装调试要遵守 IT 设备装调的一般性原则，同时由于地市应用的特殊性，还要遵循在地市公司施工的特殊原则。

完备的装调准备——在设备装调前，由公司技术管理人员派发设备装调任务；

装调方案审议——对于不同的设备，由工程师制定相应的装调步骤方案、参数设置方案等，由项目经理和相关实施人员共同讨论，分析设备装调的具体细节和实施难点；

装调的专业性——严格控制设备装调的参与人员，杜绝非技术人员单独操作；

装调的程序性——详细记录设备装调报告，记录装调问题以便及时解决和备案；

设备安装调试准备工作

设备装调的前期要进行充分的准备，在本项目设备装调的准备工作主要有设备的测试准备、全部设备的编码分类统计工作。

考虑到在本项目中会涉及大量设备，为了统一管理和系统实施及维护的便利性，我们建议对网络设备进行统一编码，建立设备档案。使用设备全名的汉语拼音字头、设备所属机构代码、设备类别等进行混合编码，同时在设备编码对照表中附加设备产品序列号字段、设备装调工程师字段、设备维护描述字段等辅助信息。这样可以方便的从编码表中定位设备品名、设备的物理位置、设备使用情况等重要信息，既方便了系统的运营维护、又对本项目的设备管理提供了具体的有益的帮助。

网络设备的安装调试方案

网络系统的安装调试是本项目的主导环节，本公司的技术人员对于主流网络系统设备的安装调试和使用都有较强的技术积累，并且拥有一批技术过硬的工程师。他们具有丰富的现场实施经验，这些优势都有助于网络设备在本项目中的安装调试工作。

网络调试准备及设备初检

网络系统的安装调试准备工作相对较多，详细、精心的准备工作可以使安装调试达到事半功倍的效果。

网络拓扑结构的确定

根据本项目的总体方案，确定设备的物理位置及连接关系。

网络地址的分配

根据本项目的总体的网络地址划分原则、细化省内所有网络设备及其它主机/工作站等设备的IP地址划分。

路由协议的选择

根据总体方案的设计，选择各层次的网络传输路由协议。

主要设备配置细节规划

对于网络交换设备、网络路由设备等做出相对具体的配置范本。

网络设备使用的外部环境准备

这个准备工作主要由曲阜师范大学信息部门完成，本公司可以协助完成，主要涉及广域网链路的申请。

网络设备安装调试过程：

网络设备安装调试工作是本项目建设的重要步骤，也是工程升级成功的基本保证。在网络设备现场安装调试前必须做好各项准备工作，其中最重要的是实施方案和实施环境的准备。对于实施环境，要满足设备使用的基本要求，同时各种线路应该全部进场(包括专线线

路、局域网线路)。本公司希望提前得到各种线路准备情况的说明，涉及专线的申请参数表、各通讯线路在配线架上的位置。

网络设备的现场安装调试涉及运营商端的应用环境和网络连接，由本公司拟定网络连接拓扑方案、网络路由选择方案、网络安全设备配置方案、网络调试计划等文件与曲阜师范大学信息部门及合作运营商的相关人员共同商讨审定，审定的内容包括技术的可行性、人员时间安排、调试测试手段等。这些文档将做为本公司所提交的必要文档的一部分交由曲阜师范大学信息部门留存。

网络设备安装调试的参与人员：

（1） 曲师大大学信息部门的技术人员

（2） 本公司项目实施小组的技术人员

（3） 网络运营商的技术人员

（4） 第三方设备厂家配合技术人员；

安装环境的确定和测试：

首先要确定网络设备安装的位置，如在网络机柜上的高度、设备上下空间、网络连接线的位置、网络走线方法。测试网络设备安装地点的环境，主要涉及通风散热和用电安全；测试网络线缆的通断情况和传输衰减。要求布线施工人员提交布线测试报告，并抽检局域网线路（或全部测试）。线缆测试方法如下：

（1） 使用简易线缆测试设备测试线路的通断情况；

（2） 使用专用线路测试仪测试网线传输衰减；

网络设备的安装调试：

（1） 完成网络设备的上架固定；

（2） 完成网络线缆的连接；

（3） 连接网络设备配置终端；

（4） 系统安全上电；

（5） 按照网络设备调试方案进行通讯参数和地址参数的调整

（6） 设置网络设备的路由参数

（7） 设置网络设备 QOS 相关参数

（8） 设置网络设备的安全性相关参数

在网络设备调试过程中，记录各参数的调整情况，保存网络设备配置文件。

网络设备连通性测试：

网络设备连通性测试主要采用Ping命令手段，通过Ping方案设计中所要求的不同目标网段或目标地址来测试网络的连通性，通过考察Ping命令的返回信息分析判断网络连通行性能：如分析相应时间、丢包率等，并做相应调整以达到通讯性能最佳。通过TraceRoute命令考察通讯连接的路由路径，对路由跳数进行分析，来调整路由方式使得连接发起方与连接目标方的路由跳数最少。

在这个网络安装调试阶段可以保留网络设备接收Telnet登陆和Ftp文件传输，这样可以方便网络设备在本项目实施过程中的参数调整。在运行阶段为保证安全性再封死对该类连接请求的响应。

5.5.4系统调试方案

在完成上述集成工作之后，需要对所有节点进行联调，以确保整个系统的正常运行。

子系统联调记录：

在联调阶段，要详细记录各子系统运行参数，确保及时发现问题及尽快解决。具体工作包括：

1)记录/分析交换机工作状态

从交换机中提取交换机的工作日志和相关的统计数据，如：流量、丢包、拥塞等。

2)记录/分析路由器工作状态

从路由器中提取路由器的工作日志和相关的统计数据，如：流量、丢包、线路通/断等。

3)记录/分析广域网链路工作状态

从路由器中提取有关广域网端口的工作日志和相关的统计数据，如：流量、丢包等，根据提取的数据分析网络链路状态。

4)记录/分析局域网工作状态

从交换机中提取交换机的工作日志和相关的统计数据，如：网络利用率、流量、丢包等，结合局域网出现的有关现象，分析局域网的工作状态。

5)记录/分析主机工作状态

从主机中提取主机的工作日志，结合日常维护工作的记录，分析主机的工作状态，如CPU、内存、IO队列、磁盘队列、网络吞吐率等。

6)记录/分析软件系统工作状态

从系统中提取各种应用软件的工作日志，结合日常维护工作的记录，分析应用软件的工作状态。

7)工作日志

在系统联调期间，要详细、严格记录联调过程中发生的问题，无论是对设备的调整，还是系统出现故障。应当每天下午或晚上，按照上面所描述的步骤进行系统数据的收集和分析。可以及时发现系统运行中发生的异常和故障，准确定位，并及时解决。

5.5.5校园无线网络调优方案

无线电的传播，包括发射、接收、干扰、以及传播路径等。无线电波与普通建筑物对象（包括墙壁、金属甚至人）的相互作用可能影响能量传播的方式，进而影响特定系统所能达到的范围和覆盖区域。根据所遇障碍物的数量和类型，典型的 WLAN 系统可以覆盖的范围或半径有所不同。通过使用多个 AP，可以扩展覆盖范围，从而在更大区域内提供无约束的真正移动和漫游。

对于普通室内部署而言，一般情况下，只需要一个 AP 或通过简单叠加 AP 即可，无需对 AP 的布放数量和位置进行仔细的勘测和计算。

但对 WLAN 室内复杂应用和室外应用而言，如对体育场、学生宿舍、会议室等覆盖应用，只有在对覆盖地点进行勘测和指标计算后，才能确定出 AP、天线及其他器件的型号和数量。同时通过勘测和指标计算，也才能确定 AP 布放的位置、天线的方位角等工程设计参数，是作为产品配置的重要素材，也是工程安装初步的指导资料。

无线工勘及实施重难点

（1)在无线网络工前勘测时，首先应该考虑的是使 AP 与网卡之间无线信号的有效交互，因此无线信号覆盖范围是 AP 选点首要考虑的因素。其次是接入用户的有效带宽，为了保证各用户具有一定的带宽,需要将每个 AP 下的同时接入的用户控制在一定数量下，通常一个 AP 推荐接入用户数为 30 人左右。

（2）在进行天线选择时，需尽量考虑到信号分布的均匀，对于重点区域和信号碰撞点，需要考虑调整天线方位角和下倾角；

（3）AP 天线安装的位置应确保天线主波束方向正对覆盖目标区域，保证良好的覆盖效果。

（4）相同频点的 AP 的覆盖方向尽可能错开，避免同频干扰。

（5）即使无线信号能通过门、窗直射穿透，纵向最多也只能覆盖 2-3 个房间。

（6）被覆盖的区域应该尽可能靠近 AP 的天线，被覆盖区域与 AP 的天线尽可能直视，

（7）由于负责工堪的工程师，是需要对实际施工的工程师负责。也就是说，负责工堪的工程师在工堪的时候需要为负责施工的工程师做一些考虑，主要考虑的问题就是安装 AP

的理想位置是否能够进行实际施工：

是否安装 AP 后是否破坏客户的室内外装潢；

AP 安装位置是否有合适的供电设备；

AP 安装位置与上联网络设备距离是否在 100M 以内；

AP 在此处的安装工艺应该是怎么样的；

10.2 用户安全管理重难点分析

曲阜师范大学大学整个校园无线网络建设要重点考虑对于内网接入进行有效的控制，如果外来人员或未经核实的人员只要关联上学校广播的 SSID 即可接入校园网，且在内部访问不受任何限制，学校虽然是一个开放的机构但是学校依旧有自己的应用系统比如财务系统、考试系统、科研管理系统等，如果不能做到一个很好的控制，它的安全性将是一个巨大的隐患，同时学校内部大量的学生也是一个相对来说控制能力不强、容易被煽动的群体，一旦未经审核的反动言论、谣言、不法网站无限制的流入校园网内部，这将对学生、学校、社会起到一个反面作用而这些都是我们不希望也不允许看到的，在这次无线建设中也需要重点考虑曲阜师范大学大学的无线认证管理。

介于以上的问题分析，考虑到曲阜师范大学的网络现状，重点部署进行有线无线一体化的认证，即将无线认证的网关统一到核心 BRAS 设备（在 BRAS 改造中重点考虑），实现一步认证，避免两次认证给用户使用带来的不便。

5.5.6无线系统调优重难点分析

无线网络优化步骤

无线网络优化一般按照确定标准、分析问题、信号侧优化、数据侧优化、测试效果五个步骤进行。而在实际的项目中，根据具体问题的不同，相关步骤可能需要循环进行。

确定标准：确定无线网络验收的一般标准，例如某运营商网络验收标准为主要覆盖区域信号强调不低于-70dBm，一般覆盖区域信号强调不低于-75dBm，丢包率不高于 3%等；

分析问题：分析造成现有无线网络使用问题的内在原因，如客户端无法打开 Portal 认证页面、或无线上网速度太慢的根本原因可能是丢包严重或数据发送数率较低；

信号侧优化：按照无线覆盖的一般原则（如蜂窝覆盖）完成工程安装规范、设备功率、信道、覆盖方式方面的调整，以保证无线信号强度与质量的要求；

数据侧优化：在信号侧优化的基础上，如有必要，需要深入分析用户数据类型及应用

特点，并做出有针对性的参数、配置调整；

测试效果：以一般验收标准测试优化后的网络效果，如信号强度、丢包率是否满足要求，在此基础上最终以客户应用模式的标准和实际业务模型进行测试，保证实际应用的稳定。

信道设置

802.11 协议在 2.4GHz 频段定义了 14 个信道，每个频道的频宽为 22MHz。两个信道中心频率之间为 5MHz。信道 1 的中心频率为 2.412GHz，信道 2 的中心频率为 2.417GHz，依此类推至位于 2.472GHz 的信道 13 。信道 14 是特别针对日本所定义的，其中心频率与信道 13 的中心频率相差 12 MHz。

为了最大程度的利用频段资源，可以使用 1、6、11；2、7、12；3、8，13；4、9、14 这四组互相不干扰的信道来进行无线覆盖。

信号穿透损坏估测

在 WLAN 工程中，需要通过现场勘查的方式了解建筑物和周围各种物质的材质，并估测其对无线信号的影响，从而来确定 WLAN 设备的安装位置。例如将 AP 置于相对较高的位置，可以有效地消除 AP 与无线终端之间的固定或移动的遮挡物，从而能够保证 AP 与无线终端之间信号的有效交互，提高 WLAN 的覆盖质量，保障 WLAN 网络的畅通。

2.4GHz 电磁波对于各种建筑材质的穿透损耗的经验值如下：

1、隔墙的阻挡（砖墙厚度 100-300mm）：20-40dB；

2、楼层的阻挡：20dB 以上；

3、木制家具、门和其它木板隔墙的阻挡：2-15dB；

5、厚玻璃（12mm）：10dB

同时，在衡量墙壁等对于 AP 信号的穿透损耗时，需考虑 AP 信号入射角度。

功率调整

WLAN 系统使用的是 CSMA/CA 公平信道竞争机制，在这个机制中，STA 在有数据发送时，首先监听信道，如果信道中没有其他 STA 在传输数据，则首先随机退避一个时间，如果在这个时间内没有其他 STA 抢占到信道，STA 等待完后可以立即占用信道并传输数据。WLAN 系统中每个信道的带宽是有限的，其有限的带宽资源会在所有共享相同信道的 STA 间平均分配。

为避免 AP 间的同频干扰，必要时应对同信道的 AP 功率进行适当的调整，保证客户端在一个位置可见的同信道 AP 较强信号只有一个，同时要满足信号强度的要求（例如不低于 -75dBm）。

数据侧优化

开启无线用户二层隔离功能，减少非必要的广播报文对空口带宽的影响；

基于无线用户进行空口限速，将空口有限资源进行合理分配；

调整管理帧的发送间隔、取消对某些无效管理帧的回应，以减少管理报文对有效带宽的影响；

关闭低速率应用，在满足覆盖范围的前提下，可以关闭低速率应用以提高空口的带宽利用率；

将无线客户端的电源管理属性设置为最高值，以增强无线终端的工作性能，提高数据下载的效率与稳定性。

5.6WLAN 项目验收

项目验收阶段是指在 AP 及天线安装完毕，以及 AC、链路资源、IP、VLAN、服务器等各类资源都已经准备就绪状态下启动的网络配置和业务上线工作。项目实施方在项目开局前需要完成工程实施和设备到货部署的工作，以及各类资源的申请和准备工作。在项目开局前，督导服务交付方需要进行现场工程界面规范性的检查，以及各种资源准备情况。

工程界面规范性检查可以发现工程施工不规范以及没有按照设计方案进行施工的问题，及时发现及时整改，于业务上线前消除工程和硬件部署隐患。规范性部署检查涉及 AP 位置是否合理、天线位置是否合理（自有天线间是否隔开 4-6 米，离 3G/4G 天线是否 2 米开外，天线是否入室，天线位于对信号衰减强的金属、陶瓷和钢筋混凝土等建筑格局中是会造成信号盲区，还是出于信号隔离考虑）、网线质量是否合格（必须超五类及以上）、走线是否规范（使用线匝，平整，网线和电源线分离，色调协调等）、接地是否规范、防水加固是否到位以及机房温度和湿度等环境因素是否合理。资源检查方面包括光纤是否充足、DHCP 地址池是否足够、出口带宽是否充足、管理 IP 是否足够、服务器是否到位、服务器配置是否满足要求、License 是否到位、AP 安装位置对应交换机和热点的信息是否完整、测试工具是否齐全等等。

工程实施阶段所做的设备到货、设备安装、服务器安装、布线、信息记录以及各种资源申请和准备在开局前必须仔细检查核对，对于不合规的方面，督导交付方需要提出修改建议，并记录备案，同时督促项目实施方进行整改和资源补充。

开局和软调优化是业务上线的具体实现操作，两个动作间需要一个基本的测试环节，并

由此评估和决定优化软调策略。

1、指导开局操作：

（1）指导实施方进行设备的基础配置，包括交换机、AC/AP、BAS 等设备及相关版本升级和 License 注册工作，并协助进行配置检查、描述信息增添以及设备工作状态分析；

（2）指导安装服务器及相关软件（包括管理软件、AAA 以及 Portal 等系统）；

（3）指导进行网络的连通性测试，确保链路完整通畅，并指导进行全部 AP 注册上线；

2、指导基本功能元素测试

（1）指导进行基本的信号覆盖测试和关联测试。选取覆盖目标场景中容易出现信号死角和盲区的区域进行信号强度测试，以-65dBm 为评估标准进行测试评估。进行终端关联的测试，验证无线加密是否生效。现场按照实际业务发生时的地理轨迹进行漫游测试，采用笔记本、手机智能终端以及用户业务终端分别进行测试，评估终端在漫游切换过程中的信号变换。在不同楼层进行信号强度测试，大致了解不同楼层之间的信号泄漏情况。

（2）登录 AP，查看 ChannelBusy，分析信道繁忙程度是否合理；开启”dot11bg calibrate-power 以及 dot11a calibrate-power ”,然后通过命令“display wlan ap name apname rrm-status”查看和该 AP（apname）同一信道的 AP 可见性（SignalStrength），整体评估系统内部信号可见性和泄漏状况。

（3）测试单用户 AP 带宽状况（IxChariot、迅雷、FTP），评估带宽合理性。验证认证、权限控制、可靠性配置以及与各类服务器业务对接项目（Portal、iMC、LDAP 等）。

3、指导调优

（1）协助进行信号覆盖整体性评估，选择合适软调手段。针对信号的软调优化手段主要围绕优化速率配比、降低管理报文开销、收缩协议报文范围、频谱导航、功率调整、降低较差链路终端的影响、优化信道分布及相互影响等几个方面展开；

（2）协助进行数据层面的整体性评估，选择合适软调手段。数据层面的优化应涉及抵消 P2P 流量冲击、保证每用户感知、保证优先 SSID 带宽、防止来自有线的影响、组网优化、每 Radio 接入用户数优化等。

（3）除信号和数据层面的优化外，在满足特别需求和资源扩充方面还可以考虑很多综合的手段，比如漫游导航、Radio 及服务定时开启关闭、组播优化、链路扩容、室分系统改造等。

（4）优化完成后，需进行抽样性测试，在信号、带宽、接入体验、认证体验和网络使用体验等方面进行对比评估，分析优化效果，并决策进一步优化方向和方法。

优化指导这个阶段的工作主要以软调优化为主，而一般软调优化需要建立在硬件优化的基础上才会发挥出应有的效果，所以前期的部署设计及工程实施至关重要。

项目验收督导

项目验收是项目转入维护阶段的最后一环，也是涉及项目结款的关键一环，更重要的是这个工作是保证网络上线后能否顺利满足用户业务需求的最后一个可控环节。

本服务旨在进行项目验收环节进行监督和指导，是形成对业务上线能否顺利运转以及网络是否可以支撑未来一定时间业务可靠运行的闭环手段。服务交付方不决定验收通过与否，但承担严格审查验收行为以及对于验收不通过项目提出指导解决方案并进行反馈的责任。原则上，交付方应指导项目实施方诚信可靠地去完成项目验收，并就验收期间发生的事宜反馈原厂。

验收项目内容及标准的确定一般是客户方决定的，大多数情况下客户会就验收内容和标准与项目实施方进行协商和确认，这种情况下，督导交付人应指导实施方对验收内容和标准进行合理性评估，针对不合理地方提出理由，给出修改意见，协助进行与客户的沟通，确定修改结果。

验收进行时，需要进行现场工作的监控和指导工作，并指导实施方输出验收报告。验收督导工作应着重于以下几个技术层面：

（1）信号覆盖强度应不低于-65dBm，并结合行业特色进行调整，比如对于医疗病房查房等医务，目标覆盖区域信号强度应不低于-60dBm。

（2）每用户带宽应符合承诺值。由于验收环节发生时用户使用情况的不确定，即用户数及分布情况可能随项目验收时间点的不同而变化，所以验收时主要把控单 AP（Radio 卡）下单用户的带宽是否合理；

（3）用户使用网络的体验。既要关注网络丢包率、延时、信号波动以及无线漫游成功率等稳定性因素，又要关注业务使用状况的实际体验，比如使用中的无线掉线问题发生情况、业务异常中断问题、业务反应迟钝等问题。

（4）确认在稳定性、认证、计费、管理等方面的验证落地，对于无线网络尤其要关注 Portal 认证、无感知认证方案、802.1X 认证、AC 备份机制、绿色节能策略、无线定位策略以及对接第三方平台等方面是否完备实现。

服务交付方应该把关验收质量，对于出现的问题及时给予闭环指导，如果评估发现的问

题严重程度涉及较大的资源投入，应该及时反馈原厂进行协调处理。

总结汇报及归档

H3C WiFi 网络部署督导服务交付方应该就勘测指导及 AP 布点方案复核、无线整体方案审核、项目开局和调优指导和项目验收督导四个环节部分提交相关工作记录和方案文档，并进行项目督导服务工作的总结，提交总结报告。

所有记录、文档和总结报告应提交原厂项目接口人归档。