無錫科技職業學院
WUXI VOCATIONAL COLLEGE OF SCIENCE AND TECHNOLOGY

有线网络改造无线网络建设

规划方案

二〇一八年八月

一、 现状分析

目前，我们校园网基础架构仍然是 2003 年建校初期建设的技术方案，近年来虽对整体的基础架构进行了不少调整优化，但是核心的骨干架构无法优化。现网中很多设备运行十多年，已趋于老化，给网络的正常运行带来巨大隐患。随着学校网络从"接入型"向"服务型"的转变，很多设备在转发性能和功能特性上已不能满足学校业务的发展，也无法支撑用户的高速接入。现有的基础设施建设已经无法满足智慧校园整体架构的发展需要，需要进行重新规划建设。

二、 建设目标

需要采用全新的架构和设备对现有校园网进行升级，升级骨干链路带宽，将接入至核心的链路升级为万兆双链路，千兆链路到用户桌面，同时可提供持续的升级能力，确保网络的高可用性和高可靠性，打造可满足学校未来 5 ~ 10 年业务需求、可运营、可管理的校园网。

由于多年业务的发展，弱电井内线路繁杂，给运维工作带来很大困难，学校希望通过本次改造对现有弱电井的线路进行梳理和整改，方便后期的运维管理。

本次有线网络改造、无线覆盖建设的战略目标为：

1. 网络可运营建设

学校网络用户众多，如果无法实现有效的运营，一方面导致无法对网络资源有效利用，造成浪费；另外一方面也将导致网络质量难以保证，使得内网师生用户的网络使用体验较差。网络可运营的建设包括网络具有运营能力，能根据业务需要实现灵活计费，根据管理要求制定精确的网络权限，并实现精准的可追溯、可查询、可分析。

2. 网络认证管理的建设

认证作为网络管理中最为主要的一层，现有网络的认证体系不够完善，不能很好保障整体网络的稳定性和安全性。此次网络建设，对网络的认证管理系统进行建设，在全网中实现有线无线一体化管理，整体网络建立扁平化网络，在校园内实现高效的实名制认证，提升整体网络的可靠性、使用性和管理性。

3. 网络骨干网络建设

此次网络建设需要对学校校园网的网络核心及汇聚进行设计，使得校园网拓

扑结构层次清晰，稳定可靠，并且具备良好的可扩展性；支持 IPV6 协议栈的演进技术；优化网络路由、增强对组播、网络流控制等方面的支持，极大地增强网络的安全性。

4. 接入层设备建设

目前我们校园网的接入层为百兆带宽，已经不能满足现有网络应用的高速传输需求。通过对校园网中骨干链路的万兆通信和冗余配置确保校园网接入层设备运行稳定性和可靠性。

5. 校园 WLAN 覆盖

校园内使用WALN覆盖以支持智能移动终端的接入是一个必然的技术趋势。此次校园网络改造建设，要在校园的重要区域，包括办公室，图书馆，教学区，操场，食堂，学生宿舍区等覆盖 WLAN，实现无线的高速上网，并且能进行区域场景间的无感知漫游。

6. Internet 出口安全及优化

学校拥有包括电信、移动、教育网等多条不同运营商的线路资源，通过部署多功能的防火墙，一方面对 Internet 的网络出口提供安全保障，增强校园内部网里的稳定性；另外一方面需要对网络资源进行合理的管理和优化，包括流量控制和出口多线路的线路负载均衡，从而充分发挥学校的网络资源，提升内部网络用户的上网体验。

7. 网络维护管理体系建设

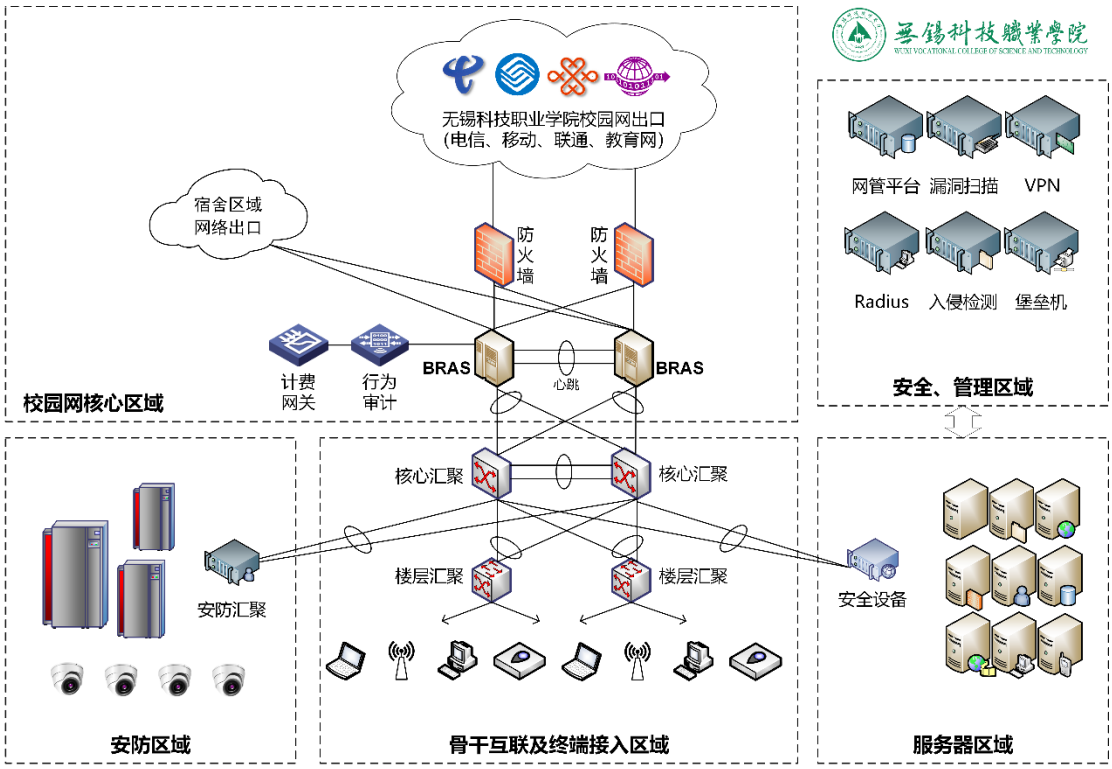
学校需要建设一个统一化的便捷网络管理平台。包括对有线、无线的集中管理，对网络定位的快速定位，对网络质量的精准分析。网络维护管理系统需要可直观数据化、图形化的分析呈现能力，并可以兼容市场多数常用的网络设备，并支持不同网络设备供应商产品。

8. 网络行为审计和非法追溯

学校校园内网络使用用户众多，角色复杂，为了更好的管理网络，做好教学辅助的工作，网络必须建设行为审计机制，具备高效的非法追溯工具，维护网络的稳定和健康，满足相关法律法规的要求。

三、 建设方案

1. 方案拓扑



2. 方案概述

改造后，全网采用实名认证，使用 BRAS 实现全网推送，并由 BRAS 统一管理整个学校上网权限，对每个实现 IPOE/PPPoE 认证的用户下发单独基于账号的 VLAN，上层使用 QinQ 实现通道共用，全网的所有上网账号实现安全隔离，上网互不影响，并对下层流量使用配置多层的 HQoS，实现精细化流量控制，可以基于时段和位置进行上网流量策略管控，为业务稳定运行设定良好框架。整网的管理方案能实现针对用户、针对应用实现精细化管理，并且管理简单，维护方便。

- **扁平化大二层网络设计**

网络核心部署 BRAS 设备来实现全网的认证管理，并且作为网关设备，下层所有汇聚和接入交换机都只启用二层转发。整个网络在逻辑上就是一个大型的二层网络，下层交换机除了启用 VLAN 之外，就只负责基础的数据转发工作，这样就去除了大量复杂和繁琐的底层设备维护工作量。

选择的 BRAS 产品在运营商、高校内广泛部署，在各种场景下的运行成熟、稳定的产品，并且要在国内有完善的厂商售后体系，确保售后响应及时度。

核心汇聚交换机、汇聚交换机除了需要提供高速的二层转发、各种安全机制，还需要支持灵活的 QinQ 技术。

- **有线无线一体化设计**

网络整体设计方案采用门户 WEB 认证，学生宿舍、特殊区域采用 PPPOE 认证。有线与无线上网账号共用，权限一致。网络层的认证设备与安全设备账号信息互通，从而实现极为简便的精细化全网管理。在用户管理、用户服务策略制定、信息安全等方面都很容易部署，很容易调整。

3. 详细设计

改造后网络架构采用扁平化组网，从网络的业务控制角度出发，以便于网络管理为目的，在该模式下将网络划分为两个大的层次：业务控制层和业务接入层。

具体设计如下：

⑴部署两台高性能多业务路由器（同时这两台设备能实现 BRAS 的功能）作为整个校园网络的业务控制层，提供用户认证、接入授权、计费、控制。核心路由器配置万兆接口，下行与校园网的核心汇聚互联，提供用户高速接入；上行与学院自己的出口万兆防火墙之间也采用万兆连接，满足互联网出口带宽要求。

⑵部署两台高性能三层交换机作为整个校园网的核心汇聚，核心汇聚配置高密度万兆接口板，通过万兆光纤和上游的核心路由、以及下游的楼宇区域汇聚之间互联，搭建万兆校园骨干网，两台核心汇聚配置成双机虚拟化，在提供高可靠性的同时简化管理。

⑶核心汇聚以及现有区域汇聚和接入层部分共同构成校园网的宽带接入层，在业务部署上，楼宇汇聚交换机负责实现 QinQ 封装，扩展 VLAN 数量，实现用户隔离。核心路由器负责终结 QinQ，提供用户接入和控制。

⑷新增一套可与核心路由（即 BRAS 设备）进行联动的 Radius 设备，在校园网（包括有线和无线环境）提供认证、授权、计费功能，在接入校园网访问外部网络时可以提供认证计费和流量控制，用户可以免费访问校内资源，需要访问其他资源时自动重定向到 Radius 上认证。

⑸在完成上述改造后，校园网出口接入多条运营商宽带线路，通过高性能万兆防火墙与两台核心路由器相连作为整个学校上网的出口；运营商为学生宿舍 PPPoE 提供的出口线路也直接接入核心路由，在各家运营商办理的宿舍有线用户根据自己办理的帐号通过策略选择各家运营商线路在运营商的 Radius 上进行计费认证。学校 Radius 不对该用户群再进行认证，仅在上网时间等方面进行一些策略控制。

(6)无线网络架构设计我们选择采用"AP 本地转发+ BRAS 认证"的架构为学院整体的 WLAN 解决方案。

使用扁平化改造新增的 2 台 BRAS 作为校内 WLAN 业务控制和认证中心，学院新增的旁路 Radius 实现用户的认证、授权和计费。无线用户的认证点放置在 BRAS 上，后台的认证系统作为用户鉴权点。

无线组网采用 AC+瘦 AP 架构，无线控制器采用冗余部署方案，保证一台控制器故障网络不可达时，另一台设备能接管故障控制器上的 AP 和 Session，用户不会出现掉线和重新认证。

4. 安全设备

习总书记指出，没有网络安全就没有国家安全。本次有线改造无线覆盖建设过程中，虽然安全设备不是必选件，但由于信息安全的重要性，这里对安全设备配备提出如下方案。

- 数据中心和互联网等在内的网络区域进行安全域划分，提高重要区域的安全等级，并且通过部署堡垒机设备，增加校内设备访问控制权限。
- 互联网区域部署 VPN 设备，校内工作人员通过 VPN 安全连接到校内网络，访问校内各种业务资源。
- 增加漏洞扫描设备建立门户网站系统的漏洞扫描与安全监测机制，加强信息系统抵御黑客攻击的能力；防止网页被挂马、被篡改。
- 通过下一代高性能防火墙增加抗 DDoS 攻击防护，提高门户网站的抗拒绝服务攻击能力，保障网站一旦被 DDoS 攻击，用户仍可访问。
- 增加 WAF 设备和 IPS 设备，对重点区域增加 Web 应用防护和入侵防护措施，确保能有针对性的提升重点区域的安全防护能力。