山东大学

SHANDONG UNIVERSITY

山东大学（青岛校区）

校园网建设规划

计算机科学与技术学院 2017 级菁英班

刘建东(201700130011)

张　腾(201700301030)

指导老师：张华忠　　助教：张涵

摘要

本校园网规划项目从山东大学（青岛校区）的实施背景出发，结合网络工程规划的设计原则，针对山东大学（青岛校区）的应用需求、性能需求，梳理了校园网整体规划的思路和方向。在章节上分成五大部分，一是校园网整体规划概述，包括施工背景和需求分析以及设计原则；二是校园网物理层设计细节，包括分三大层设计和对应层设备选型以及综合布线系统相关设计；三是校园网逻辑层设计细节，包括 IP 地址规划和虚拟网络隔离划分设计；四是校园网安全措施与运维管理，包括网络安全面临的问题和管理方面的五大内容；五是网络建设项目的投资估算，包括具体设备和线缆采购规模和价格总估以及后期运维成本。

本校园网规划项目对于山东大学青岛校区的意义重大，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。该项目作为信息化基础的网络建设，不仅以安全稳定的网络满足学校招生和教学管理的基本需求，同时通过引入 SDN 等技术，体现一定的技术领先性，解决传统校园网在网络部署、运维和管理等方面长期存在的诸多问题。

关键词：校园网，三层网络结构，扁平化大二层，网络规划，网络安全

目录

第一章 校园网整体规划概述

1.1 校园网实施背景

山东大学青岛校区位于青岛市即墨鳌山卫镇，南依崂山，东临黄海。校区规划面积 3000 亩，规划建设 137.12 万平米，一期 70 万平米，可满足 10000 名学生和 2000 名教职工学习、生活和教学科研的需要。目前有六个学院、八个研究机构入驻。由济南、威海、青岛三地八校区形成“山东大学系统”，使山东大学成为中国地区最大、系统相对最完善的高校，也将带动山东大学进入全新时代，向创建世界一流大学迈进。

图表 1 山东大学(青岛校区) 鸟瞰图

1.2 校园网设计原则

1.2.1 实用性

校园网的建设都是从实际出发的，以实际情况为前提考虑现有的资源和情况来建设一个满足广大师生的需求。并且为将来校园网络的维护管理尽可能的考虑进去，不能脱离实际。

1.2.2 可靠性

可靠性是指在一定的条件下和时间内完成规定任务的能力。如果没有办法完成那么就是一个失败的网络设计。这样就要时时刻刻防止网络出现故障，保证一天 24 小时的能够正常运行。为了达到网络的可靠性，就必须从系统的结构设计等方方面面给予考虑，必要时设计冗余备份，这是处理网络涂法时间最快最好的办法，可快速的回复整个网络。

1.2.3 安全性

安全性不管在什么网络都是必须要重点考虑在内的，而校园网中包含了各种的学习资料、师生信息和各种的数据库信息。这些都是高校的重要数据，一旦遭到破坏后果会非常的严重。所以校园网的安全性是非常重要的，主要运用的技术有 VLAN 技术、访问控制列表、加密技术等，这些是必须进行实施的。

1.2.4 拓展性

为校园网将来的发展做准备，是对未来网络的提升打下基础。不仅在网络设备上有很好的拓展性，包括在网络整体的拓展，所以路由协议的选择以及路由的规划很好重要。

1.2.5 先进性

在设计规划的时候采用先进的技术以及设备，这既可以满足网络的需求，又可以提高校园网的应用水平，还对未来的扩张保留了一定的潜力，这是非常需要的，能够很好地延长校园网的使用寿命。

1.2.6 可维护性

任何一个网络一旦建成就必须要对其进行维护，在设计网络的时候就要求对以后的网络监测、调试等考虑周全。

1.2.7 经济性

高校建设校园网毕竟资金有限，在任何设备的选取和设计都要选取最佳的方案，建网时选取性价比较高的网络技术和网络设备，更好地节约资金。

1.3 网络应用的需求分析

1.3.1 振声苑

多媒体教室、远程教学、无线网络、教学云桌面终端、标准化考场

1.3.2 宿舍

无线网络、门禁、用户限速、端口隔离（每一个信息点独自使用一个交换机端口并通过 VLAN 方式相互隔离，提高网络安全性）

1.3.3 行政楼

视频会议、远程访问、无线网络、全校监控

1.3.4 实验楼

无线网络、数据备份、动态地址分配

1.3.5 图书馆

计算机查询、资源检索、书籍阅读、视频会议

1.3.6 食堂

校园卡消费，自助查询终端

1.3.7 体育馆

校园卡信息读取、修改、接入带宽限制

1.3.8 医务室

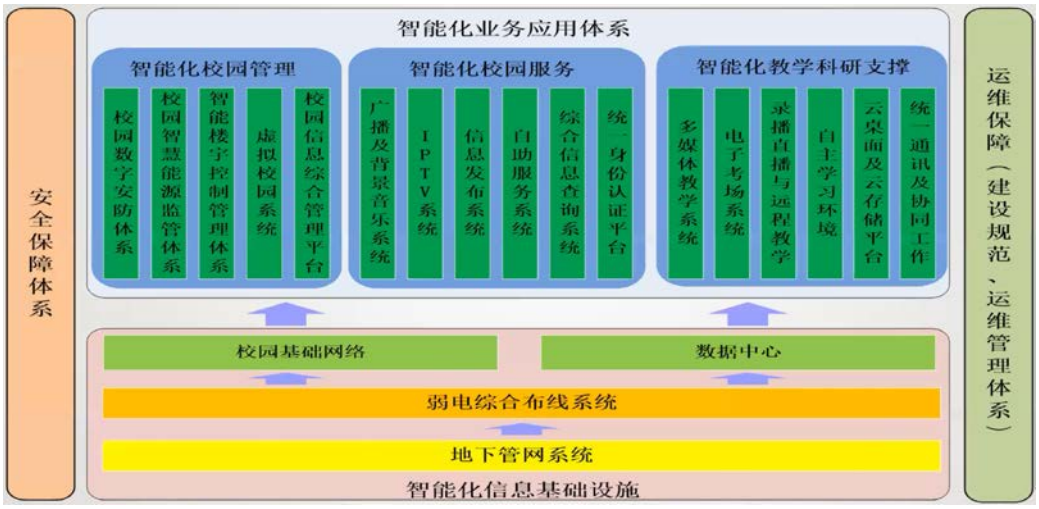
校园卡信息读取、修改、接入带宽限制

1.3.9 校道

监控、紧急报警、校园广播音柱

1.3.10 其他

提供集中业务控制设备，所有终端既需实名制认证上网，同时也实现了与账号及 IP 地址的自动绑定，确保了用户无论采取什么方式接入，始终获得相同的带宽保障、服务质量和安全策略，打破了业务接入与物理位置紧耦合的僵化网络服务模式，使得精细化策略管理得以有效实施。



图表 2 智慧化校园业务应用体系

1.4 网络性能的需求分析

1.4.1 校园卡消费

校园卡为校园内最主要的支付工具，因此对响应时间有很高的要求，因此限制校园卡在 1s 之内响应。

1.4.2 个人终端联网数目

考虑个人常用的设备为手机、电脑以及可能会配备的平板，因此限制个人终端联网数目为 3 个。

1.4.3 个人终端联网限速

师生生活用途网速：下行 500KB/s~4MB/s，上行 500KB/s~2MB/s。

师生科研用途网速：下行 2MB/s~12.5MB/s，上行 2MB/s~10MB/s。

1.4.4 视频会议最高像素支持

视频会议是校园内主要需求之一，行政楼、实验楼日常开会均可能涉及到视频会议，因此对视频会议所支持的最高像素也有较高的要求，因此至少需要支持 2k 像

素的视频会议。

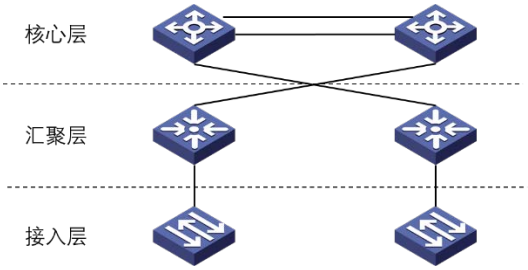
1.4.5 门禁刷卡

校园卡除了支付以外还有一个很重要的功能是身份认证，校园内教职工每天都会涉及大量的身份认证，对认证速度有较高的需求，因此将门禁认证速度限定在 1s 内响应。

第二章 校园网物理层设计及设备选型

2.1 校园网物理分层设计

为了简化校园网络的设计、提高网络的可管理型和可拓展性，一个好的校园网方案应该采用分层的方法进行设计，不同的层可能工作在 OSI 模型的不同层次上。在确定校园网使用三层网络结构后，要对着三层分别进行详细的设计。



图表 3 三层网络架构图

2.1.1 核心层

校园网的绝对主干，其主要作用是尽可能快地交换数据。校园网的其他部分都是由核心层拓展延伸而出的。如果核心层的设备停止工作，整个校园网都会瘫痪。要求核心层具有高效性、可靠性、低延时性、冗余性、容错性、可管理性、适应性等特点，核心交换机的路由处理系统、交换网络、内部总线、风扇、电源系统等关键部件均采用冗余备份设计，能提供 7 × 24 小时的可靠服务。

在我们设计的青岛校区网络拓扑图中，我们在核心交换机与核心路由器处都进行了冗余备份设计，即将两台交换机或路由器虚拟化成一台使用。

2.1.2 汇聚层

汇聚层具有实施策略、安全、工作组接入、VLAN 之间的路由、源地址或目的地址过滤等多种功能。汇聚层将工作站先做汇聚再接入核心层，是接入层和核心层的“中介”，可以减轻核心层设备的负荷。为了满足网络隔离和分段的要求，一般在

汇聚层采用能够支持三层交换技术和 VLAN 技术的交换机。

在汇聚层方面，我们在青岛校区中各大楼宇处放置了汇聚交换机，用于各楼宇与校区核心交换机之间的数据传输与通信。

2.1.3 接入层

本地网段的工作站通过接入层接入网络。如果减少接入层中某一网段的工作站数量，就能够向其工作组提供更高速的带宽。接入层可以使用不支持三层交换技术和 VLAN 技术的普通交换机。

在接入层方面，我们对于各楼宇功能的不同放置了不同数量的交换机并且分场景地根据各场景的特性选择了不同的无线接入设备，用于接入层的数据传输与通信。

在图书馆、N 区科研楼等处的接入层我们进行了分块，分别为有线接入交换机、设备管理网接入交换机、POE 交换机。这三类交换机将网络分成了三类，分别是有线网、无线网、设备管理网（为监控、门禁提供独立的接入设备）。

而学生宿舍的接入层比上述图书馆、科研楼的三类接入层还多一类，就是无线汇接器。我们在学生宿舍中设计的 AP 并不带路由功能，所有房间内的小 AP 最终汇聚到无线汇接器上。而走廊的 AP 自带路由功能，不同于宿舍中的 AP。

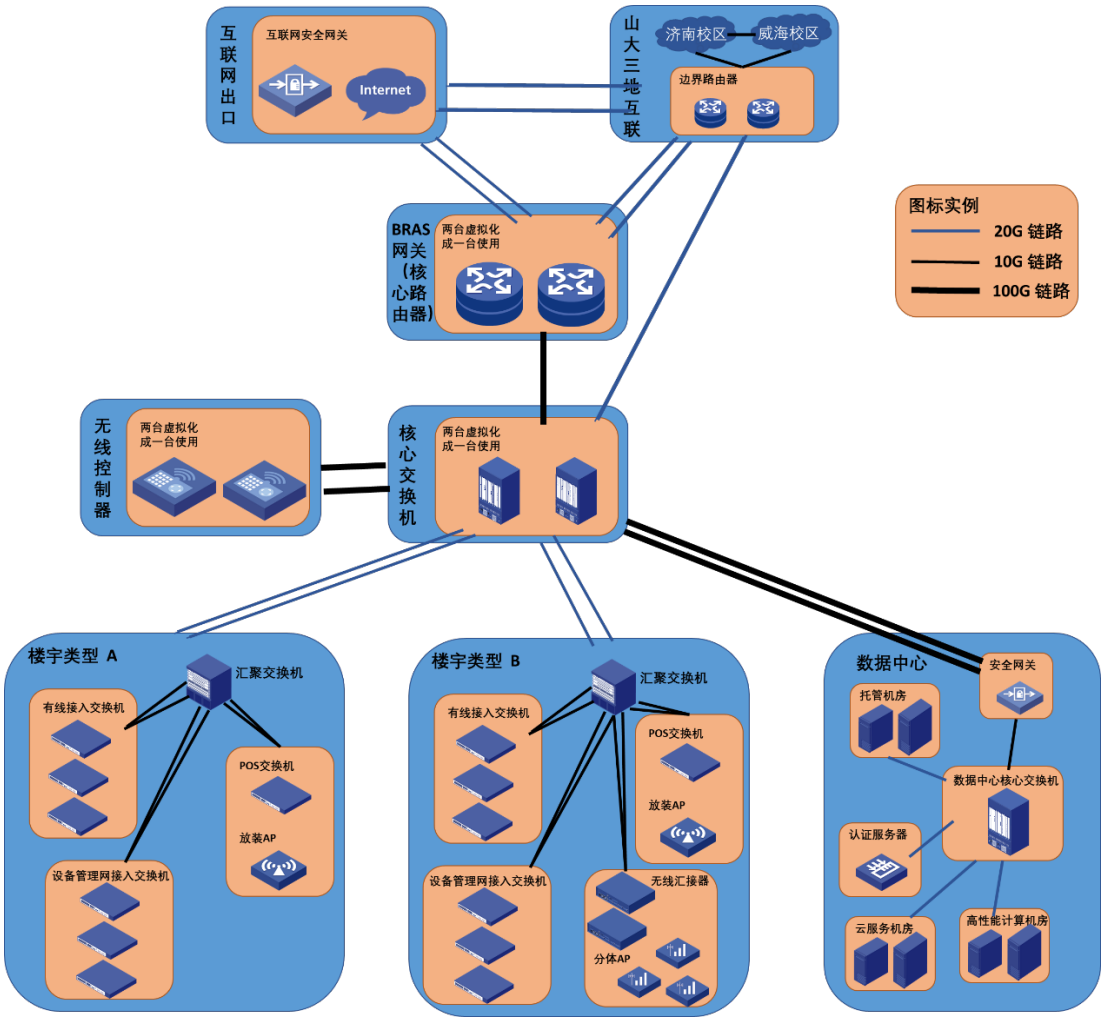
由此我们实现了分场景地对于校内不同功能建筑设计不同的接入层方案，实现更有效地数据传输与通信。

2.3 校园网拓扑结构及设备选型

2.3.1 校园网拓扑结构

网络拓扑结构是指用各种传输介质互相连接各种设备的物理布局，指构成网络的成员之间物理的（即真实的）或逻辑的（即虚拟的）排列方式。换句话说，网络拓扑就是网络的形状，用来描述网络设备的连通性。

拓扑图中，楼宇类型 A 有：图书馆、K 区 N 区科研楼、食堂、振声院、华岗苑、会文南(北)楼、博物馆等；楼宇类型 B 有：学生公寓凤凰居、专家公寓等。



图表 4 青岛校区网络拓扑图

2.3.2 核心层设备选型

核心层设备主要是核心路由器和核心交换机，核心路由器主要用于 BARS 统一认证系统。对于核心路由器，我们采用的是 Juniper MX960-PREMIUM3-AC 型号的核心路由器，该路由器是一款以太网优化的边缘路由器，同时具有数据交换和电信级以太网路由的功能，它凭借 JUNOS 操作系统，使运营商能够更加高效地无缝部署以太网并加速下一代网络部署。

除此之外，MX960 路由器是专为 ISP 等大中型网络设计的高以太网密度业务路由器，可以提供丰富的路由功能，支持各种运营商应用，包括高速 Inetrnet Peering、MPLS VPN 以及下一代宽带 Multiplay 业务。并且 MX960 路由器的高度只有 16U，最多提供 12 个 40 Gbps 插槽并支持 Juniper 全新的 DPC 卡，交换容量为 2640 Gbps，整机的吞吐能力为 1320 Gbps，最多可以支持 480 个全线速千兆以太网端口或 132 个全线速万兆以太网端口。

不仅如此，MX960 路由器可以提供多种以太网服务，常见的有：

1. 本地支持多点连接的虚拟专用局域网服务（VPLS)。

2. 本地支持点对点虚拟租用专线（VLL）服务。

3. 支持以太网中的全部 MPLS VPN 业务。

4. IPTV 系统的视频分发服务。

5. 实现校园网边缘的以太网汇聚，支持高密度 1G 和 10GE 配置。

6. 提供多达 480 个 1GE 端口或 48 个 10GE 端口，以最大限度提高以太网的密度，并为 MSE 应用提供全面的 L2 和 L3 VPN 支持。

由于该核心路由器的诸多高效特性以及校园网络建设的需求，我们最终选择了这款路由器。在路由交换机方面，我们选择了 H3C S12518 作为核心交换机，该交换机支持 10/100/1000/ 10000 Mbps 的传输速率，包转发率达到了 5400Mpps，采用了模块化的端口结构，扩展模块包括 2 个主控板槽位数、18 个业务板槽位数和 9 个交换网板槽位数，传输模式为全双工。

考虑到校区师生的巨大需求，以及校园网络的复杂性，核心交换机必须要支持多种网络标准。而在网络标准方面，H3C S12518 支持 IEEE 802.3ae、IEEE 802.3、IEEE 802.3u、IEEE 802.3x、IEEE 802.3ad、IEEE 802.3z、IEEE 802.1Q、IEEE 802.1p 等多种网络标准。不仅如此，在 QOS 方面，该交换机支持 Diff-Serv QoS，支持 SP/SDWRR 等队列调度机制、支持精细化的流量监管（粒度可达 1K）、支持流量整形、支持拥塞避免、支持优先级标记 Mark/Remark、支持 802.1p、TOS、DSCP、EXP 优先级映射，支持 VOQ 等。在组播管理方面，该交换机支持 PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP、Any-RP 等路由协议，支持 IGMP V1/V2/V3、IGMP V1/V2/V3 Snooping，支持 PIM6-DM、PIM6-SM、PIM6-SSM，支持 MLD V1/V2、MLD V1/V2 Snooping，支持组播策略和组播 QoS，支持交换网和业务板两级组播复制功能，达到最优的组播性能。

而在最为关键的安全管理方面，该交换机表现也十分出色，其支持用户分级管理和口令保护，支持 SSHv，为用户登录提供安全加密通道，支持可控 IP 地址的 FTP 登录和口令机制，支持标准和扩展 ACL，可以对报文进行过滤，防止网络攻击。还支持防止 ARP、未知组播报文、广播报文、未知单播报文、本机网段路由扫描报文、TTL=1 报文、协议报文等攻击功能。以及支持 MAC 地址限制、IP+MAC 绑定功能，支持 uRPF 技术，防止基于源地址欺骗的网络攻击行为，支持 802.1x，支持 Portal 认证，支持 Radius，支持 OSPF、RIPv2 及 BGP4 报文的明文及 MD5 密文认证，支持安全网管 SNMPv3、SSHv2，支持未知单播、组播、广播报文抑制，支持主备数据

备份机制。

基于上述诸多的优秀性能，以及考虑到校区师生的需求以及校区网络建设的实际情况，我们最终选择了这款交换机作为校区的核心交换机。

图表 5 **核心路由器** Juniper MX960

单价：970000/台　　型号：Juniper MX960-PREMIUM3-AC

图表 6 **核心交换机** H3C S12518

单价：250000/台　　型号：H3C S12518

2.3.3 汇聚层设备选型

汇聚层交换机必须为三层、具有路由功能的交换机，此处我们采用了 H3C S7502E 的交换机作为楼宇汇聚交换机。在网络标准方面，该交换机支持 IEEE 802.1P、IEEE 802.1Q、IEEE 802.1d、IEEE 802.1ad、IEEE 802.3x、IEEE 802.3ad、IEEE 802.3、IEEE 802.3z、IEEE 802.3ae、IEEE 802.3af、IEEE 802.3at 等常见网络标准。

在 QOS 方面，该交换机每单板最大支持 16K ACL，支持标准和扩展 ACL，支持基于 VLAN 的 ACL，支持 Ingress/Egress ACL、Ingress/Egress CAR（粒度可达 8Kbps），支持两级 Meter 能力，支持 VLAN 聚合 CAR、MAC 聚合 CAR 功能，支持流量整形，支持 802.1P/DSCP 优先级 Mark/Remark，支持层次化 QoS（H-QoS），支持三级队列调度，支持每端口 8 队列，支持拥塞避免机制（包括 Tail-Drop、WRED）。除此之外，在组播管理方面，该交换机支持 IGMPv1/v2/ v3，支持 IGMPv1/v2/v3 Snopping，

支持 IGMP Filter，支持 IGMP Fast leave，支持 PIM-SM/PIM-DM/PIM-SSM，支持 MSDP 等。

并且在网络管理方面，支持 FTP、TFTP、Xmodem，支持 SNMP v1/v2/v3，支持 sFlow 流量统计，支持 RMON，支持 NTP 时钟，支持 NetStream 流量统计功能，支持电源智能管理，支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测。基于此，我们选择了这款交换机作为汇聚层交换机。

图表 7 汇聚交换机 H3C S7502E

单价：35000/台　　型号：H3C S7502E

2.3.4 接入层设备选型

接入层主要是为终端用户提供网络的接入口。由于使用交换机的数量很多，虽然不需要过多的配置，但由于接入层的数据流最多，也因为从安全和网络的数据流量等方面的考虑，因此要采用网络接口数多、能做安全策略的交换机。

因此采用了 H3C 的 S5130-54C-HI 交换机，这个型号的交换机一共有 52 个端口，其中有 48 个 10/100/1000Base-T 自适应以太网端口以及 4 个万兆 SFP+口。能实现高级 QOS，其中包括支持对端口接收报文的速率和发送报文的速率进行限制，支持报文重定向，支持 CAR 功能，每个端口支持 8 个输出队列，支持端口队列调度（SP、WRR、SP+WRR），支持报文的 802.1p 和 DSCP 优先级重新标记。

不仅如此，在组播管理方面，该交换机支持 IGMP Snooping /MLD Snooping，支持组播 VLAN。在网络管理方面，支持 XModern/FTP/TFTP 加载升级，支持命令行接口（CLI）、Telnet、Console 口进行配置，支持 SNMPv1/v2/v3，WEB 网管，支持 RMON 告警、事件、历史记录、支持 iMC 智能管理中心，支持系统日志、分级告警、调试信息输出，支持 HGMPv2，支持 Ping、Tracert，支持 VCT 电缆检测功能，支持 DLDP 单向链路检测协议，支持 Loopback-detection 端口环回检测，支持电源、风扇、温度告警，支持 BFD，支持 H3C UIS Manager 统一管理软件，可提供跨服务器、存储、网络以及虚拟化的全融合管理，简化部署安装，优化运维管理。

在安全管理方面，该交换机支持用户分级管理和口令保护，支持 802.1X 认证/集中式 MAC 地址认证，支持 Triple 认证，支持 Guest VLAN，支持 RADIUS 认证，支持 SSH 2.0，支持端口隔离，支持端口安全，支持 MAC 地址学习数目限制，支

持 IP 源地址保护，支持 ARP 入侵检测功能，支持 IP+MAC+端口多元组绑定，支持 EAD。因此该交换机拥有多种的安全和加密策略，可以很好地保护接入层用户的安全。

除此之外，该交换机还有大量的优秀特点来支撑校区师生的日常网络需求。在链路聚合方面，该交换机支持 GE/10GE 端口聚合，支持动态聚合，支持跨设备聚合端口特性，支持 IEEE802.3x 流量控制（全双工），支持基于端口速率百分比的风暴抑制，支持基于 PPS/BPS 的风暴抑制。并且支持 SFLOW 形式的流量统计，支持 IPv4 静态路由、RIPv1/v2，支持 IPv6 静态路由、RIPng，支持 OSPFv1/v2、OSPFv3。并且支持端口镜像，支持远程端口镜像 RSPAN，支持流镜像。基于该交换机在上述多个方面的优良特性，最终采用了这个交换机。

图表 8 接入层交换机 H3C S5130-54C

单价：15000/台　　型号：H3C S5130-54C-HI

2.3.5 其他设备选型

无线控制器：

在无线控制器方面，我们选择了 H3C 的 EWP-WX5560H 作为我们的千兆无线控制器，该设备可以管理 6144 个无线设备，无线传输速率达到了 1450Mbps，吞吐量达到了 100G，可插拔电源并实现了 1+1 冗余备份，支持各类安全规范，在安全性方面表现极佳，并且支持功能之多远超业内同类型无线控制器，因此我们选择了这款设备作为青岛校区的无线控制器。

图表 9 无线控制器 H3C EWP-WX5560H

单价：118000/台　　型号：H3C EWP-WX5560H

互联网安全网关：

在互联网安全网关方面，我们选择了迪普科技的 DPX8000-A12 作为我们的核心互联网安全网关，该设备的整机交换容量达到了 6480Gbps，业务槽位数达到了 10 个，整机安全业务处理能力达到了 400Gbps，单板最大安全业务处理能力达到了 40Gbps，支持各类安全技术。

该设备作为业界第一款深度业务交换网关。集业务交换、网络安全、应用交付三大功能于一体。并且作为一个 100G 高性能平台，支持未来 40GE 和 100GE 以太网标准，提供高性能业务单板，最大可提供 400G 整机深度业务处理能力。

除此之外，该设备还有丰富的业务扩展能力。支持应用防火墙、IPS、流量控制、安全审计、应用交付、异常流量清洗/检测、漏洞扫描系统和 Web 应用防火墙等深度业务功能的按需扩展。并且还有领先的虚拟化能力。DPX8000 以资源化方式，将一个个相互独立的功能单一的物理设备形成一个或多个逻辑对象，所有策略配置和管理均基于逻辑对象进行实施，不仅大大提高了业务组网能力，并使得可靠性、无缝升级能力大大增强。

正是由于以上诸多优越性能与特性，我们最后选择了该设备作为整个青岛校区的互联网安全网关。

图表 10 **安全网关** DPX-8000-A12

单价：360000/台　　型号：迪普科技 DPX-8000-A12

2.4 无线网络设计

2.4.1 无线网络设计

无线网络设计的目标是建设一个覆盖办公、教学、科研以及生活区域的无线网络。因此在设计山东大学青岛校区的无线网络时要充分考虑网络的先进性、稳定性、可用性和安全性，要满足如下功能：

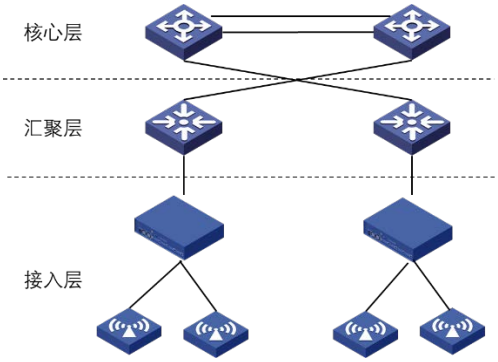
（1）无线网络采用 802.11n 技术，并兼容 IEEE802.11a/b/g，这样可以满足不同标准的在校师生无线用户进行网络连接，并使得无线网络可以达到充分使用。

（2）建设达到教学楼、办公、科研、管理等区域都有无线的 AP，并设立 1 个 SSID 并使学校能够自助管理，通过学校的 SSID 直接连接到现有的校园网。

（3）设计校园网，使之能够实现无缝连接，互联网络的速度为万兆以上，使用者在走动的同时能够自动切换不同区域的无线频率。

（4）建立一个专门的无线管理系统，方便校园网的管理。

无线网网络系统采用“无线控制器 AC+FIT AP”的组网架构。和有线网络一样，采用三层（核心层、汇聚层、接入层）拓扑结构部署，核心层在图书馆，并采用双机热备份的方式，以保证可靠性。无线网络拓扑图如下所示。



图表 11 无线网络分层图

根据青岛校区未来的规划，一共会有 60 栋楼房，设计需要的 AP 数量如下表所示。

楼名	AP 数量	楼名	AP 数量
学生公寓（6 栋）	3240	专家公寓（8 栋）	4320
学生创新创业服务中心	160	校医院	50
学生食堂	40	足球场	5
体育馆	200	博物馆	150
操场	5	振声苑	480
N 教学科研综合楼（6 栋）	700	K 教学科研综合楼（6 栋）	700
图书馆	500	会文南楼	132
会文北楼	132	J 工程技术研究院（2 栋）	400
J 学院办公楼（2 栋）	400	G 工程技术研究院（6 栋）	1200
M 高等研究院（4 栋）	800	D 工程技术研究院（5 栋）	1000
学生会堂	1500	国际交流中心	2040
篮球场	5	校园道路	300

2.4.2 无线设备选型

根据使用场景的不同，我们需要对使用场景进行分类，对特定场景使用特定的 AP 类型。我们将使用场景一共分为了四大类，分别是室外、大教室和报告厅、办公室和走廊以及宿舍和办公区域。

室外 AP：

在室外，我们选择了 H3C 的 EWP-WA2620X 作为无线 AP 的接入设备。选择该设备的主要原因是该设备在用户性能、降低同频干扰、信号传输范围、数据传输能力等方面有着远超同类产品的能力。而且支持 PoE 供电，同时支持 2.4-2.483Ghz、5.725-5.850Ghz 的工作频段。

图表 12 室外定向 AP H3C EWP-WA2620X

单价：3685/台　　型号：H3C EWP-WA2620X

大教室与报告厅：

在大教室与报告厅场景中，我们选择了 H3C 的 EWP-WA4330-ACN-FIT 作为无线接入设备。选择这个设备的主要原因是该设备内置天线，有三个工作频段，分别是 5.725GHz-5.850GHz、5.47~5.725GHz、5.15~5.35GHz，并且支持 802.3af / 802.3at 兼容供电。在性能、效率、功能等方面都远超同类产品。

图表 13 室内三频分装 AP H3C EWP-WA4330-ACN-FIT

单价：3500/台　　型号：H3C EWP-WA4330-ACN-FIT

办公室与走廊：

在办公室与走廊场景中，我们选取了 H3C 的 WA4320-ACN-C 作为无线接入设备。选取这个设备的主要原因在于该设备价格合适，有 2 个工作频段，分别是 2.4G 和 5G，适用于 90-120 ㎡ 区域的无线覆盖，带机量为 40-60 台无线设备，无线速率达到了 800M。因此在性价比以及功能等方面，该设备远超同类产品，因此我们选择了这款设备作为该场景下的无线接入设备。

图表 14 **室内双频分装** AP H3C WA4320-ACN-C

单价：1200/台　　型号：H3C WA4320-ACN-C

宿舍与办公区域：

在宿舍与办公区域场景下，我们选取了 H3C 的 WA4320H-ACN 作为无线接入设备。选取该设备的主要原因在于该设备带机量、价格及性能都比较适合宿舍这个场景。该设备带机量为 15 台无线设备，有 2 个工作频段，分别是 2.4GHz 和 5GHz，支持各类网络标准并且在安全性能方面也有较好的表现。因此我们选择了这款设备作为该场景下的无线接入设备。

图表 15 **室内双频分装** AP H3C WA4320H-ACN

单价：2500/台　　型号：H3C WA4320H-ACN

宿舍内部：

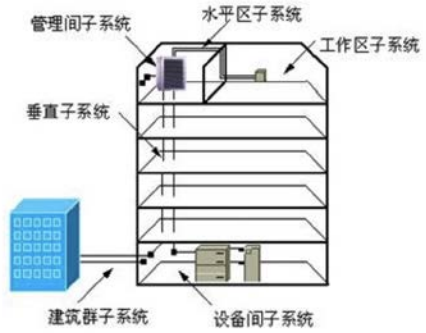
在宿舍内部我们选取了 H3C 的 WTU430H-IOT 作为无线接入设备。不同于走廊上的无线 AP，该 AP 为分体式 AP，即不自带路由功能，所有房间内的小 AP 最终汇聚到无线汇接器处。该产品内置全向天线，支持 5.725~5.850GHz、5.47~5.725GHz、5.15~5.35GHz 三个工作频段，在其它方面也表现不错，因此我们选择了该设备作为宿舍内部的无线接入设备。

图表 16 宿舍内部分体 AP H3C WTU430H-IOT

单价：1200/台　　型号：H3C WTU430H-IOT

2.5 综合布线系统的设计

当前，在综合布线领域被广泛遵循的标准是 EIA/TIA-568A，即 Commercial Building Telecommunication Wiring Standard。在 EIA/TIA-568A 标准中，综合布线系统分成了六个子系统，包括工作区子系统、水平子系统、垂直子系统、管理间子系统、设备间子系统和建筑群子系统，如下图所示。



图表 17 综合布线系统组成

图中每个部分相互独立，可以单独设计和施工。更改其中某个子系统时，不会影响其他子系统，易于系统扩展和重新组合，也便于查找和排除故障。

2.5.1 工作区子系统

工作区子系统又称为服务区子系统，是工作人员利用终端设备进行工作的地方。一个工作区的服务面积可以按 5-10 ㎡ 估算，或按照不同的应用场合调整面积大小。工作区子系统由水平布线系统的信息插座延伸到工作站终端设备的整个区域。工作区子系统的布线由插座开始，服务器或工作站可通过双绞线直接与信息插座相连。

工作区电缆通常都是短的、柔软的线缆，这种电缆的最大传输距离为 5m。因此，从 RJ-45 插座到终端设备之间所用的双绞线，一般不要超过 5m。此外还需注意，RJ-45 插座必须安装在墙壁上或不易碰到的地方，插座距离地面 30cm 以上。

2.5.2 水平子系统

水平子系统又称配线子系统，它从工作区的信息插座开始到管理子系统的配线架，用于将信息点与垂直子系统连接起来。水平子系统由工作区的信息插座、每层配线设备至信息插座的配线电缆、楼层配线设备和跳线等组成的，一般呈星型拓扑结构。

水平子系统一般采用 3 类 UTP 双绞线（传输速率为 16Mps）和 5 类 UTP 双绞线（传输速率为 100Mbps），布线的总长度一般不超过 90m，除了 90m 水平电缆外，工作区和管理子系统的接插线和跨接电缆的总长度最多可达 10m，共计不超过 100m。水平布线时，应确定线路走向和路径，使用路径最简短、施工最方便的线路。

2.5.3 垂直子系统

垂直子系统又称干线子系统，是整个建筑物综合布线系统的关键链路。他的主要功能是将设备间子系统和各楼层的管理子系统连接起来，提供建筑物内垂直干线电缆的路由。简单的说，就是实现数据终端设备、交换机和各管理子系统之间的连接。

干线子系统一般要为建筑物服务 5-10 年，支持的业务很宽，在布线标准中，可以选用的线缆也有很多种，主要由：4 对 5 类对绞线（UTP 或 FTP），100 Ω 大对数对绞线电缆（UTP 或 FTP），150 Ω（STP-A）对绞线电缆，50/125 μm 多模光纤，8.3-10/125 μm 单模光纤。

2.5.4 设备间子系统

设备间子系统是综合布线系统中为各类信息设备提供信息管理、信息传输服务的，所有楼层的资料都由光缆或线缆传送至此。设备间是一种特殊类型的交接间，但又与交接间有一些差异，设备间一般为整栋建筑物或者整个建筑群提供服务，而交接间只为移动大型建筑的某层中的某一部分提供服务。

设备间应处于干线综合体的最佳网络中间位置，并尽量靠近建筑物电缆引入区和网络接口，以使干线路径最短。设备间室温应保持在 10℃-30℃ 之间，相对湿度保持在 60%-80%，有良好的通风。此外，设备间还应拥有消防系统，使用防火防盗门，并安装至少能耐火 1 小时的导火墙。

2.5.5 管理子系统

管理子系统由交连、互联和输入/输出组成，是水平子系统电缆端接的场所，也是垂直子系统电缆端接的场所。每个设备间和交接间都有管理子系统，应该说，管

理子系统是对综合布线系统实施灵活管理、维护的关键部分。

管理子系统应有足够的空间放置配线架和网络设备，便于将来扩充，室内配线架的配线对数由管理的信息点数决定。

2.5.6 建筑群子系统

建筑群子系统是将一个建筑物中的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上，它提供楼群之间通信设施所需的硬件，其中有电缆、光缆和防止电缆的浪涌电压进入建筑物的电器保护设备。建筑群子系统由连接各建筑物之间的综合布线电缆、建筑群配线设备和跳线等组成。

第三章 校园网逻辑层设计

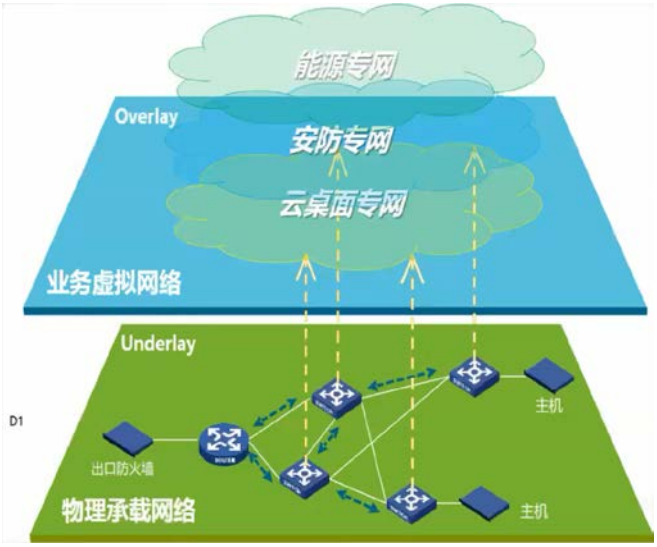
3.1 校园网逻辑分层设计

3.1.1 SDN 架构校园网

校园网逻辑分层设计上，可采用新华三基于 SDN+VxLAN 技术的 ADCampus 应用驱动型校园网方案，即在校园网物理结构基础之上，可采用 SDN+VxLAN 技术，构建一个 Overlay 的分布式扁平化逻辑大二层业务承载网。通过 SDN 控制器进行业务预定义，每中智能化业务都获得独一无二的 VxLAN ID，并在汇聚层实现 VRF 的自动创建以及与 VxLAN ID 的关联。

智能化业务与 IP 地址组实现一对一映射，网络属性与业务结合更直观，IP 即用户、网段即业务。借助 VxLAN 的分布式网关特性，业务终端在任何位置接入网络均不需要更改 IP 地址。通过提前收集的信息，SDN 控制器可以自动使用 MAC 地址作为智能化终端的接入账号和密码，实现终端的接入认证，且能够在系统中实现终端类型、业务、IP 地址和 MAC 地址的绑定。

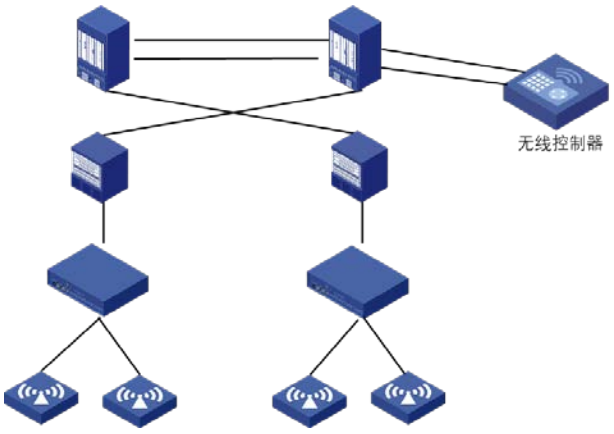
扁平化的大二层网络，整体简化了网络结构，网络中大量的接入、汇聚作为逻辑二层设备只需要做简单的 VLan 划分、端口隔离配置即可，不需要过多管理，核心设备作三层网关，启用路由、认证、安全相关功能，日常维护中，管理员只需要维护核心设备即可，大大降低了网络的运维难度，简化了工作量。



图表 18 校园网虚拟业务专网

3.1.2 有线无线一体化组网

考虑到无线终端数目的爆炸式增长，一个用户多终端情况，本地转发可以降低无线控制器的表项压力与性能要求，满足近 7000 台 802.11ac ware2 时代无线高带宽接入，流量不迂回。并且，基于 SDN 架构的校园网天然解决跨网漫游问题，用户移动后 IP 不发生变化，天然支持用户的无缝漫游，用户体验不会造成损失，更好地发挥本地转发的性能优势。另外，考虑到无线流量的增长趋势，如果采用独立组网，多年后有线网设备流量减少，造成设备利用率不足，统一组网，迎合校园流量从有线为主导无线趋势的过渡，设备充分利用。



图表 19 基于 SDN 架构实现本地转发无缝漫游

3.2 IP 地址和虚拟业务网划分与设计

在一个大规模校园网里， 其下会有许多二级单位和楼宇建筑，合理的 VLAN 及 IP 地址规划，既可提高网络的整体性能，还能大大减轻网管人员的工作量。

3.2.1 IP 地址设计

规划校园网的 VLAN 及 IP 地址时，必须和校园网的拓扑结构、路由策略、建筑分布、部分区域等因素紧密相连，相互对应。

山东大学（青岛校区）目前共招入六个学院及两个研究生院的师生，按每学院 1000 人计算，每人同时可以使用三台设备上网，因此个人可变 IP 应每学院分配至少 3000 个，同时图书馆电脑（约 100 台）应分配独立固定的 IP，各学院楼每层约有 8 个实验室，每个实验室分配约 60 台电脑，同时学院楼约有 100 名教职工固定电脑需求，所以每个学院楼应有至少 1500 个可用 IP。

学院	用途	IP 网段	子网掩码
生命科学学院	总 IP 网段	172.16.0.0~172.18.255.255	255.16.0.0
	师生动态 IP	172.16.128.0~172.16.255.255	255.255.192.0
	其他人员 IP	172.17.128.0~172.17.255.255	255.255.192.0
	院楼有线 IP	172.18.128.0~172.18.255.255	255.255.192.0
信息学院	总 IP 网段	172.19.0.0~172.21.255.255	255.16.0.0
	师生动态 IP	172.19.128.0~172.19.255.255	255.255.192.0
	其他人员 IP	172.20.128.0~172.20.255.255	255.255.192.0
	院楼有线 IP	172.21.128.0~172.21.255.255	255.255.192.0
法学院	总 IP 网段	172.22.0.0~172.24.255.255	255.16.0.0
	师生动态 IP	172.22.128.0~172.22.255.255	255.255.192.0
	其他人员 IP	172.23.128.0~172.23.255.255	255.255.192.0
	院楼有线 IP	172.24.128.0~172.24.255.255	255.255.192.0
计算机科学与技术学院	总 IP 网段	172.25.0.0~172.27.255.255	255.16.0.0
	师生动态 IP	172.25.128.0~172.25.255.255	255.255.192.0
	其他人员 IP	172.26.128.0~172.26.255.255	255.255.192.0
	院楼有线 IP	172.27.128.0~172.27.255.255	255.255.192.0
环境学院	总 IP 网段	172.28.0.0~172.30.255.255	255.16.0.0
	师生动态 IP	172.28.128.0~172.28.255.255	255.255.192.0
	其他人员 IP	172.29.128.0~172.29.255.255	255.255.192.0
	院楼有线 IP	172.30.128.0~172.30.255.255	255.255.192.0
政管学院	总 IP 网段	172.31.0.0~172.33.255.255	255.16.0.0
	师生动态 IP	172.31.128.0~172.31.255.255	255.255.192.0
	其他人员 IP	172.32.128.0~172.32.255.255	255.255.192.0
	院楼有线 IP	172.33.128.0~172.33.255.255	255.255.192.0
其他公用	总 IP 网段	172.34.0.0~172.36.255.255	255.16.0.0

IP	师生动态 IP	172.34.128.0~172.34.255.255	255.255.192.0
	其他人员 IP	172.35.128.0~172.35.255.255	255.255.192.0
	院楼有线 IP	172.36.128.0~172.36.255.255	255.255.192.0

图表 20 IP 地址划分表

3.2.2 虚拟业务网及其隔离划分

青岛校区的学院、部门众多，对于每个不同的学院、部门以及楼宇进行虚拟业务网的划分，每个虚拟网内部通信不经过网络层，通信速度较快，个别区域网瘫痪也不会影响其他区域网。

建设一个统一的业务承载网，主要关注其隔离能力和网络安全性。列举三种虚拟网络隔离划分技术：

①VLAN 技术：属于成熟技术，能够跨楼宇位置逻辑划分网络，起到隔离作用，但子网内地址必须连续，无法再进行划分，只是做一个二层网络的隔离，在三层的隔离需要结合 ACL 访问控制进行隔离 VLAN 间的访问。由于 VLAN Header 头部限长是 12bit，导致 VLAN 的限制个数是 4096 个。

②MPLS VPN 技术：该技术普遍应用于运营商，可作专线技术，网络隔离性强，但技术原理复杂，增加运维难度。

③VXLAN 技术：该技术近几年大规模用于数据中心建设，主要用于各独立租户隔离，同时各租户还可根据各业务划分 VLAN。适用于业务多，终端常挪动的需求情况。可以跨越三层，仅要求核心层设备和汇聚层设备支持，对接入层设备要求低，在楼宇交换机上都有 VXLAN 网关，结合 SDN 能自动化的配置，部署简单。

用途 \ 技术	VLAN 技术	MPLS VPN 技术	VXLAN 技术
隔离强度	一般	较强	强
部署难度	简单	复杂	简单
应用对象	楼宇、部门广播域的隔离	财务专网、人事专网等	数据中心、云服务、原 VLAN 的应用对象

图表 21 三种虚拟网络隔离划分技术对比

综合运用三种技术，根据不同的学院、部门以及楼宇进行划分，定义规则如下：

①第 1、2 位表示单位，如 01xx 表示凤凰居 S 楼。

②第 3、4 位表示内部分组，如 0101 表示凤凰居 S1 楼。

VLAN 编号	所属部门	VLAN 编号	所属部门
VLAN 01xx	国际交流中心 A1	VLAN 0201~0215	学生宿舍 B1~B5、食堂 B6、B7、学生宿舍 B8~B12、风雨操场 B15

VLAN 0301	学生会堂 C1	VLAN 0401~0405	工程技术研究院 D1-D5
VLAN 05xx	振声院 E	VLAN 0601-0604	华岗院 F（行政办公室、法学院、政治学与公共管理学院）
VLAN 0701-0706	工程技术研究院 G1-G6	VLAN 08xx	图书馆 H1
VLAN 0901-0906	教学科研楼 K（海洋研究院 K3、环境科学学院 K5）	VLAN 1001-1008	教学科研楼 N（微生物研究研究 N1、生命科学学院 N2N8、计算机科学与技术学院 N3、信息科学与工程学院 N5）
VLAN 11xx	体育综合馆 Q1、体育场 Q2	VLAN 1201-1213	学生公寓 S1-S13
VLAN 1301-1315	专家公寓 T1-T15	VLAN 1401-1407	科研孵化器 Y1-Y7
VLAN 15xx	博物馆	VLAN 16xx	宣传部
VLAN 17xx	人事处	VLAN 18xx	学生处
VLAN 19xx	公安处	VLAN 20xx	教务处
VLAN 21xx	党委部	VLAN 22xx	校工会
VLAN 23xx	校团委	VLAN 24xx	财务处
VLAN …	其他	…	…

图表 22 虚拟业务网划分

3.4 校园网其他服务设计

建设现代信息化的高等院校，不仅仅要组建网络，还包括校园的现代数字化信息化建设，青岛校区校园网建设完成后，必须建设相关的必要服务，真正实现网络的信息化。

3.4.1 一卡通系统设计

对接济南校区一卡通系统，使在校师生能在学习内部进行各种日常消费，包括食堂、超市、图书馆、校车等。它为数字化校园提供信息采集的基础工程。

3.4.2 数据中心设计

建设青岛校区数据中心需要以下设备：服务器系统、存储系统、数据中心机房环境建设

3.4.3 WWW 服务

WWW(World Wide WEb)万维网是 Internet 上被广泛应用的一种信息服务技术。WWW 采用的是 B/S 结构，整理和存储各种 WWW 资源，并响应客户端软件的请求，把所需的信息资源通过浏览器传送给用户。通过 WWW 技术建立山东大学青岛校区的主页，及时发布校内各种信息。

3.4.4 FTP 服务

匿名 FTP 是目前 Internet 上进行资源共享的主要途径之一。它的特点是访问方便，操作简单，容易管理。Internet 上有许多的资源都是以 FTP 的形式提供给大家使用的，包括各种文档、软件工具包等等。

3.4.5 E-Mail 服务

邮件服务是 Internet 上使用人数最多且最频繁的应用之一。目前大部分的邮件系统都基于 STMP 协议，通过存储转发式的非定时通信方式完成发送、接受邮件等基本功能。普通用户通过使用自己的用户名、口令可以开启邮箱完成阅读、存储、回信、转发、删除邮件等操作。

3.4.6 网上教学平台

网上教学平台实现了网上教学、网上讨论、网上批改作业、网上课件制作、网上备课、网上答疑等功能，适合开展研究性学习，从而为学校创建了一个标准的、统一的网络教学空间。由于教学平台易用性好，操作简便，有效地位教师消除了利用网络开展教学所面对的技术障碍，并为推广应用提供了便利条件。在网络教学过程中，学生拥有学习的自主权利，教师通过间接引导和任务布置来实现教学目的，实现跨越时空的教学互动。

3.4.7 教务管理系统

为提高学校的教学管理水平，实施教学管理的现代化和规范化，教务管理系统的建设势在必行。教务管理系统在充分利用教学管理资源、提高教学管理效率和保证教学质量方面发挥了积极的作用。一个完整的教务管理系统应该包括考试管理系统、成绩管理系统、教学评价管理熊、选课管理系统、排课管理系统、计划管理系统、基本信息管理子系统、学生管理系统、教材管理系统和审核管理系统等等。

除此之外，校园网还应有 OA 系统、VOD 应用服务、VPN 服务等，这些服务需要在学习的发展过程中完善。

第四章 校园网安全和管理

4.1 校园网面临的安全问题

网络是一个脆弱的实体，不仅要面对自身系统的不安全性，如 TCP/IP 协议的不安全、网络物理链路的不安全，同时还需要面对网络使用者、网络恶意程序和网络使用者操作系统不安全等威胁。校园网面临的安全威胁，主要可分为 4 类：网络物理安全威胁、人为无意失误威胁、人为恶意攻击威胁和软件漏洞隐患威胁。

4.1.1 网络物理安全威胁

信息安全首先需要保障信息的物理通道的安全性，物理安全是网络安全不可缺少的组成部分。物理安全的主要目的是：保护学校的交换机、路由器、工作站、各种网络服务器打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线窃听攻击；确保网络设备一个良好的电磁兼容工作环境；建立完备的机房安全管理制度，妥善保管备份磁带和文档资料；保护裸露的线路不受雨水影响或不被老鼠咬断。

4.1.2 人为无意失误威胁

人为的无意失误威胁主要有：网络管理人员配置不当造成的安全漏洞，使得入侵者可以通过端口扫描技术获得相应的端口信息；网络管理人员安全意识不强，随意让非网管人员在网络中心机房走动；口令选择不慎，没有定期更换口令；用户将自己的账号随意转借他人或与别人共享账号。

4.1.3 人为恶意攻击威胁

人为恶意攻击威胁是校园网络所面临的的最大威胁，黑客攻击和计算机犯罪都属于这一类威胁。人为的恶意攻击威胁主要表现在：计算机病毒、特洛伊木马以及其他恶意程序代码。

4.1.4 软件漏洞隐患威胁

软件不可能百分之百的无缺陷、无漏洞，这些缺陷和漏洞恰恰是黑客进行攻击的首选目标。大部分软件的“后门”是由于软件编程人员设计时考虑不完善，或是为了方面自己调试程序而造成的，一般不为外人所知，可一旦“后门”被发现，造成的后果不堪设想。校园网中的操作系统一般为 Windows 系统和 Linux 系，Windows 系统的广泛使用，Windows 系统的缺陷不时被发现，相应的补丁程序也不断被更新，校园网的网管人员应该及时为服务器打上补丁程序，还应提醒教师和学生用户及时

打上补丁。

4.2 校园网安全防范措施

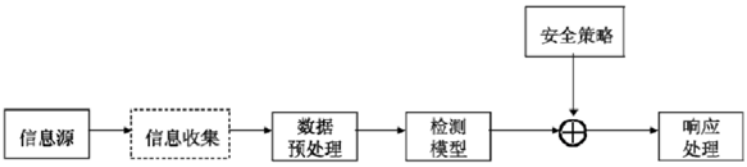
网络安全策略主要体现在网络协议方面和网络层的安全性。网络协议的漏洞、网络设备配置的疏忽、网络技术选择的不当，都会造成网络安全问题。在这个层面上，采用的安全策略主要有防火墙、入侵检测系统、入侵防御系统、身份认证、VLAN、ACL、NAT、IP-MAC 绑定等技术。

4.2.1 防火墙技术

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的边界上构造的保护屏障，是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关，从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

4.2.2 入侵检测系统

虽然防火墙应用起来非常方便，但还是存在许多不足，比如防火墙的动态性能较差，不能很好地实现对数据的实时监控。入侵检测系统（IDS）作为动态安全的核心技术之一，是防火墙的合理补充，也是安全防御体系的一个重要组成部分。入侵检测是指通过从计算机网络或计算机系统工程中若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时做出响应的安全技术。通过入侵检系统的部署可以扩展系统管理员的安全管理能力，帮助系统检测和防范网络攻击，提高信息安全基础结构的完整性。



图表 23 入侵检测的一般过程

4.2.3 入侵防御系统

入侵防御系统 (IPS) 可提供主动防护，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失。IPS 是通过直接嵌入到网络流量中实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，

有问题的数据包，以及所有来自同一数据流的后续数据包，都能在 IPS 设备中被清除掉。

IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器，每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

4.2.4 身份认证技术

身份认证是校园网安全系统中一个非常重要的环节，没有身份认证，或是身份认证失败，就无法在网络安全系统中进行访问控制和攻击检测。

SDN 控制器可以自动使用 MAC 地址作为智能化终端的接入账号和密码，实现终端的接入认证，且能够在系统中实现终端类型、业务、IP 地址和 MAC 地址的绑定。

4.3 校园网络管理的五大内容

4.3.1 网络故障管理

网络故障管理是网络管理中最基本的功能之一。常见的网络故障原因有路由器访问列表配置不正确、交换机的 VLAN 设置不正确、服务器用户权限的设置不正确、各种服务器的服务选项配置不正确、计算机网卡配置不正确等。

当网络中某个组成部分失效时，网络管理器必须迅速查找到故障并及时排除。通常不大可能迅速隔离某个故障，因为网络故障的产生原因往往相当复杂，特别是当故障是由多个网络组成共同引起的。在此情况下，一般先将网络修复，然后再分析网络故障的原因，分析故障原因对于防止类似故障的再发生相当重要。网络故障管理包括也故障监测、报警、排错、分析等方面。

4.3.2 网络配置管理

网络配置是指制作能够使设备正常运行的数据（如硬件数据、对接数据、信令数据、路由数据、号码分析数据），并将这些数据设定到设备的一种操作。因此，网络配置通常也称为“数据配置”。

对设备运行的数据进行增加、删除、修改、查询、存储、备份、恢复等操作，即为配置管理。配置管理是设备有效管理和维护的重要工具。

4.3.3 网络性能管理

网络性能管理是指评价系统资源的运行状况及通信效率等系统性能。其能力包

括监视和分析被管网络及其所提供服务的性能机制，性能分析的结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志。性能管理的功能包括以下几个方面：

① 性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量，对于每个被管对象，定时采集性能数据，自动生成性能报告

② 阀值控制：可对每一个被管对象的每一条属性设置网值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行岗值设置。可通过设置岗值检查开关控制阀值检查和告警，提供相应的阀值管理和溢出告警机制。

③ 性能分析：对历史数据进行分析、统计和整理，计算性能指标，对性能状况做出判断，为网络规划提供参考。

④ 可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

⑤ 实时性能监控：提供了一系列实时数据采集、分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

4.3.4 网络计费管理

网络计费管理的主要目的是跟踪和控制用户对网络资源的使用，并把有关信息存储在运行日志的数据库中，为收费提供依据。

4.3.5 网络安全管理

网络安全包括组成网络系统的硬件、软件及其在网络上传输信息的安全性，使其不致因偶然的或者恶意的攻击遭到破坏，网络安全既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。除此之外，网络安全管理要注意方面的有：路由（配置 ACL)、交换(绑定端口、MAC）的安全设置等、防止路环、防范泛洪、ASA 的设置等。

4.4 网络管理的手段

校园网络的管理需要选择并购买网络管理软件，用于校园网络管理人员对校园网络进行日常管理与维护。由此如何选择适合的网络管理软件尤为重要。

为了实现“按需建构”的理念：一. 基于灵活的组件化结构。二. 用户根据不同的管理需要以及网络情况选择不同的组件。选择的网络管理软件应有如下功能： 网络集中监视、故障管理、性能监控、服务器监视管理、设备配置文件管理、设备软件

升级管理、集群管理、堆叠管理、故障定位与地址反查、RMON 管理。

第 5 章 网络建设项目投资估算

根据上述接入层、汇聚层、核心层设备选型以及无线设计部分的设备选型，我们可以得到下述青岛校区校园网规划预算表。

设备名	数量/台	型号	单价/元	总价/元
核心路由器	2	Juniper MX960	970000	1940000
核心交换机	2	H3C S12518	250000	500000
安全网关	2	DPX-8000-A12	360000	720000
无线控制器	3	H3C EWP-WX5560H	118000	354000
汇聚交换机	120	H3C S7502E	35000	4200000
接入层交换机	1860	H3C S5130-54C	15000	27900000
室外定向 AP	315	H3C EWP-WA2620X	3685	1160775
室内三频分装 AP	2812	H3C EWP-WA4330-ACN-FIT	3500	9842000
室内双频分装 AP	4162	H3C WA4320-ACN-C	1200	4994400
室内双频分装 AP	4150	H3C WA4320H-ACN	2500	10375000
宿舍分体 AP	6560	H3C WTU430H-IOT	1200	7872000
光缆	50000m	GYXTW	2.90	145000
总计	70,003,175 元			

图表 24 校园网建设预算表