# 石油大学校徽

# 网络方案设计

**计算机科学与技术22-3班**

**黄思源**

**2022011599**

目录

[第 1 章 网络需求分析
1](#_Toc8477)

[1.1 项目背景
1](#_Toc20141)

[1.2 网络业务需求
2](#_Toc19442)

[1.3 网络应用需求
5](#_Toc28788)

[第 2 章 网络技术调研
6](#_Toc25458)

[2.1 网络互连技术
6](#_Toc2204)

[2.2 网络接入技术
8](#_Toc32675)

[2.3 网络安全技术
9](#_Toc1067)

[2.4 数据中心
11](#_Toc8741)

[第 3 章 网络结构设计
11](#_Toc19506)

[3.1 网络分层架构设计
11](#_Toc28173)

[3.2 网络拓扑图设计
14](#_Toc25767)

[3.3 网络可靠性设计
15](#_Toc30662)

[3.4 网络设备选型​ 17](#_Toc30550)

[3.5 VLAN 划分​ 18](#_Toc13519)

[3.6 IP 地址规划和子网划分​ 18](#_Toc21273)

[3.7 路由设计（路由协议选择）​ 19](#_Toc4749)

[3.8 无线网络方案设计​ 19](#_Toc27116)

[3.9 数据中心网络方案设计​ 20](#_Toc13453)

[3.10 云平台方案设计​ 21](#_Toc27811)

[3.11 网络安全性设计​ 22](#_Toc7651)

[3.12 人脸识别系统设计 23](#_Toc22857)

[3.13 大模型服务器平台部署方案 24](#_Toc26260)

[第 4 章 网络预算
25](#_Toc14701)

[4.1 网络设备、服务器和软件系统清单及预算
25](#_Toc25892)

## 第 1 章 网络需求分析

### 1.1 项目背景

在当今时代，教育信息化正以前所未有的速度深入发展，深刻地改变着教育的模式与格局。对于高等院校而言，校园网络作为教育信息化的关键基础设施，其性能与功能的优劣直接影响着教学、科研和管理工作的质量与效率。中国石油大学（北京），作为一所肩负着为石油行业培养高素质人才使命的知名学府，在教育信息化的浪潮中，也面临着校园网络升级改造的迫切需求。

目前，中国石油大学（北京）拥有主校区和分校区两个办公区域。主校区位于 [主校区具体地址]，这里汇聚了 2 幢 8 层教学楼，承载着大量的日常教学任务，涵盖了从基础课程到专业课程的各类教学活动；1 幢 6 层实验楼，是开展科研实验和实践教学的重要场所，拥有先进的实验设备和专业的实验室环境；1 幢 10 层行政楼，集中了学校的行政管理部门，承担着学校的管理和决策职能。分校区位于 [分校区具体地址]，包含 2 幢 8 层教学楼，为分校区的学生提供了良好的教学空间；1 幢 5 层实验楼，支持着分校区的科研和实践教学工作；1 幢 6 层行政大楼，负责分校区的日常管理事务。

随着学校的不断发展，各楼宇的信息点分布呈现出显著的差异。在主校区实验楼，由于科研和实践教学的需要，每个实验室需布设 30 个信息点，以满足实验设备、计算机等的网络接入需求。行政楼机房作为学校网络和信息管理的核心区域，更是需要 100 个信息点，以保障服务器、网络设备等的稳定运行。而分校区计算机中心，由于其承担着大量的教学和科研计算任务，信息点高达 300 个。这种高密度的信息点需求，对校园网络的接入能力提出了严峻的挑战。同时，传统的布线系统也难以满足如此复杂的网络连接需求，需要进行全面的升级和优化。

在网络应用层面，学校现有的网络架构需要支持学校网站、本科教务管理系统、研究生系统等十余种应用系统。这些系统涵盖了教学管理、学生管理、行政管理等多个方面，是学校日常运行不可或缺的部分。所有服务器集中部署于行政楼网络中心的数据中心，这里是学校信息的核心枢纽，存储和处理着大量的教学、科研和管理数据。

随着人工智能、大数据等技术的快速发展，学校计划实现大模型服务器部署，以支持人工智能、机器学习等前沿科研方向的发展。这需要强大的计算能力和高速的网络支持，以满足模型训练、推理和部署等全流程操作对算力和数据传输的需求。同时，搭建私有云平台也是学校网络建设的重要任务之一，旨在为全校师生提供 100GB 存储空间的云网盘服务，支持文件共享、协作编辑和版本控制等功能，方便师生存储和共享教学资料、科研数据。此外，人脸识别系统的覆盖也是学校提升校园安全管理水平的重要举措，通过在各楼宇出入口部署人脸识别设备，实现人员身份识别和考勤管理，有效保障校园的安全。

当前，主校区和分校区现通过 VPN 方式连接成一个局域网，但这种连接方式在网络性能、安全性和扩展性方面存在明显的不足。在网络性能方面，VPN 连接的带宽有限，难以满足日益增长的教学、科研和管理数据传输需求，特别是在进行大规模数据传输、在线教学、视频会议等应用时，容易出现网络卡顿、延迟高等问题，影响教学和科研的正常进行。在安全性方面，虽然 VPN 提供了一定的加密保护，但随着网络攻击手段的不断升级，现有的安全防护措施难以有效应对各种新型网络威胁，如黑客攻击、数据泄露等。在扩展性方面，传统的网络架构难以灵活适应学校未来的发展需求，如新增楼宇、新的应用系统上线等，需要进行大规模的网络改造和升级，成本高且实施难度大。

为了应对上述挑战，构建一个安全可靠、稳定高效的系统集成平台已成为当务之急。通过优化网络架构，引入先进的网络技术和设备，如万兆以太网、SDN（软件定义网络）、云计算等，可以显著提升校园网的性能、安全性和可管理性。这不仅能够满足学校当前的教学、科研和管理需求，还能为学校的长远发展提供坚实的网络基础支撑，助力学校在教育信息化的道路上不断前行，培养更多适应时代需求的高素质人才。

### 1.2 网络业务需求

#### 1.2.1 基础网络连接需求

两校区之间的互联互通是保障学校整体教学、科研和管理工作顺利开展的关键。目前，主校区现有两根光纤分别接入教育网和联通网，这为校园网与外部网络的通信提供了基本的通道。教育网作为教育领域的专用网络，拥有丰富的教育资源和稳定的网络环境，为学校师生访问教育类网站、获取学术资源等提供了便利。联通网则提供了更广泛的公网接入，满足师生对互联网资源的多样化需求。分校区通过 VPN 与主校区连接，实现了两校区之间的局域网互通，使得分校区的师生能够访问主校区的数据中心和各类应用系统，如统一身份认证系统、教务管理系统等。

然而，随着学校业务的不断增长，对网络带宽的需求也在日益增加。考虑到未来的发展，需要确保核心层与汇聚层之间采用万兆连接。核心层作为校园网的高速交换中心，承担着大量的数据转发任务，万兆连接能够提供高速、稳定的骨干链路，确保数据能够快速、准确地在核心层与汇聚层之间传输。汇聚层与接入层千兆连接，接入层负责将终端设备连接到网络，千兆连接能够满足大多数桌面终端和服务器的接入需求，提供足够的带宽保障。桌面终端支持 10/100 兆接入，这主要是考虑到一些普通办公场景和对网络带宽需求较低的终端设备，如普通办公电脑、打印机等，10/100 兆的接入速率能够满足其基本的网络访问需求。

主校区行政楼网络中心作为核心节点，具有至关重要的地位。它不仅承担着数据中心服务器、大模型服务器及各类应用系统的接入任务，还通过光纤实现与教育网、公网及分校区的连接。数据中心服务器存储着学校的核心数据，如学生信息、教学资源、科研成果等，大模型服务器则为人工智能、大数据分析等科研任务提供强大的算力支持。各类应用系统则是学校日常教学、科研和管理工作的重要工具。通过与教育网和公网的连接，网络中心能够实现资源的共享和交互，为师生提供更丰富的网络服务。分校区网络机房作为汇聚节点，负责将各楼宇网络流量汇聚后通过 VPN 链路传输至主校区。分校区各楼宇的网络流量通过接入层和汇聚层交换机汇聚到网络机房，再通过 VPN 链路传输到主校区网络中心，实现与主校区的网络互通。

#### 1.2.2 无线覆盖需求

在当今数字化校园的建设中，无线覆盖已成为不可或缺的一部分。对于中国石油大学（北京）而言，实现两校区所有教学和办公场所的无线网络全覆盖，具有极其重要的意义。它能够支持师生移动办公，教师可以在教室、办公室、图书馆等场所随时随地访问教学资源、处理教学事务；支持在线教学，学生可以通过无线网络在课堂上参与互动教学、观看教学视频等；还能满足物联网设备接入等场景，如智能教室设备、环境监测传感器等，实现校园的智能化管理。

无线局域网需具备高可靠性，以确保在各种复杂环境下都能稳定运行。高并发能力也是关键特性之一，能够支持大量用户同时接入，特别是在教室、图书馆等人员密集区域，能够保障每个用户都能获得良好的网络体验。无缝漫游特性则允许用户在不同的无线接入点之间自由切换，而不会出现网络中断或连接不稳定的情况，确保用户在校园内移动时能够持续享受网络服务。自动负载均衡功能可以根据各个无线接入点的负载情况，自动分配用户流量，避免热点区域拥堵，提高网络资源的利用率。

同时，无线局域网需支持 802.11ac/a/n 等主流无线协议。802.11ac 协议作为新一代的无线通信标准，具有更高的传输速率和更大的并发连接数，能够满足高密度场景下的网络需求。802.11a 协议则在 5GHz 频段上提供了较高的传输速率和较少的干扰，适用于对网络质量要求较高的应用场景。802.11n 协议则具有较好的兼容性和性价比，能够满足大多数普通用户的需求。提供 2.4GHz 和 5GHz 双频段覆盖，2.4GHz 频段具有较好的穿墙能力和广泛的设备兼容性，但传输速率相对较低，且容易受到干扰；5GHz 频段则具有更高的传输速率和较少的干扰，适合高速数据传输和对网络质量要求较高的应用。通过双频段覆盖，可以满足不同终端设备的接入需求，提供更优质的网络服务。

为了满足不同终端设备的接入需求，在无线 AP 的部署上，需要根据不同区域的特点进行合理规划。在教室区域，由于人员密集且对网络稳定性要求较高，应部署高性能的无线 AP，采用双频设计，支持 802.11ac 协议，以确保每个学生都能获得稳定、高速的网络连接。在办公室区域，考虑到办公设备的多样性和对网络安全性的要求，可部署支持 802.1X 认证的无线 AP，保障办公网络的安全。在图书馆等公共场所，由于用户流动性大且对网络覆盖范围要求广，应增加无线 AP 的密度，确保整个区域都能得到良好的网络覆盖。

#### 1.2.3 服务器与存储需求

在数字化校园建设中，数据中心的建设至关重要。部署虚拟化架构是提升数据中心性能和管理效率的关键举措。通过虚拟化技术，如 VMware vSphere 或开源的 KVM 虚拟化平台，可以将物理服务器资源抽象为虚拟服务器（VM）。这使得多个虚拟服务器可以在同一台物理服务器上运行，实现了计算资源的动态分配。当某个业务系统的负载增加时，可以动态地为其分配更多的计算资源，如 CPU、内存等；当负载降低时，又可以回收多余的资源，提高资源的利用率。同时，虚拟化架构还支持服务器集群部署，当某台物理服务器出现故障时，虚拟机会自动迁移至其他服务器运行，确保业务不中断，提高了系统的可靠性。

大模型服务器（如 Deepseek 服务器）在人工智能和大数据分析等科研领域发挥着核心作用。它需具备强大的计算能力，配备高性能的 CPU，如 Intel Xeon Gold 系列处理器，拥有多个核心和高主频，能够快速处理复杂的计算任务。同时，支持 GPU 加速，配备 NVIDIA A100 等高性能 GPU，能够显著提升深度学习模型的训练速度。分布式计算能力也是大模型服务器的重要特性，通过多台服务器之间的协同工作，可以处理大规模的数据集和复杂的模型训练任务。此外，大模型服务器还需要具备丰富的存储资源，采用高速的 SSD 硬盘作为系统盘，确保系统的快速启动和运行；采用大容量的 SATA 硬盘作为数据盘，存储大量的训练数据和模型参数。

私有云平台为全校师生提供 100GB 存储空间的云网盘服务，这极大地方便了师生存储和共享教学资料、科研数据。云平台支持文件共享功能，师生可以方便地与他人分享自己的文件，促进教学和科研的交流与合作。协作编辑功能允许多人同时对一个文件进行编辑，提高了团队协作的效率。版本控制功能则可以记录文件的修改历史，方便用户在需要时恢复到之前的版本。云平台应采用主流技术路线，如基于 OpenStack 开源技术构建，确保开放性和成熟可靠性。OpenStack 具有丰富的功能模块和庞大的社区支持，能够提供稳定、可靠的云服务。同时，云平台具备良好的扩展性，通过增加物理服务器和存储设备，可以动态扩展计算和存储资源，以满足学校不断增长的业务需求。

#### 1.2.4 网络安全需求

在网络技术飞速发展的今天，网络安全已成为校园网络建设中不容忽视的重要环节。中国石油大学（北京）构建统一的安全防护体系，是保障校园网络安全稳定运行、保护师生信息和学校数据安全的必然要求。

防火墙作为网络安全的第一道防线，部署于网络边界，如校园网与教育网、公网连接处。它基于 IP 地址、端口、协议等规则对流量进行过滤，阻止未经授权的访问。主校区出口部署的下一代防火墙（NGFW），不仅具备传统防火墙的基本功能，还支持应用层流量识别和深度包检测（DPI）。通过应用层流量识别，能够精准识别各种网络应用，如 P2P 下载、视频流媒体、在线游戏等；通过深度包检测，能够对网络数据包进行深入分析，检测其中是否包含恶意代码、攻击行为等，从而精准识别并控制非业务流量，保障关键应用带宽。

Web 防火墙（WAF）主要针对 Web 应用层攻击，如 SQL 注入、XSS 跨站脚本攻击等。学校网站、教务系统等 Web 应用是学校对外展示和内部管理的重要窗口，容易成为黑客攻击的目标。部署 Web 防火墙，对 HTTP/HTTPS 流量进行深度检测和防护，能够有效保护这些 Web 应用免受攻击，确保师生能够安全地访问这些应用。

入侵检测系统（IDS）通过旁路部署方式监听网络流量，实时检测潜在的入侵行为，如端口扫描、恶意代码传播等，并发送告警信息。主校区数据中心部署 IDS，对服务器区域的流量进行监控，及时发现针对服务器的攻击尝试，为安全人员提供预警，以便采取相应的防护措施。入侵防御系统（IPS）与 IDS 相比，具备实时阻断攻击的能力，可主动拦截恶意流量。在核心层或关键链路部署 IPS，可有效应对零日漏洞攻击和高级持续性威胁（APT），保障校园网络的安全。

统一身份认证系统采用 “用户名 + 密码 + 多因子认证” 机制，多因子认证可集成短信验证码、硬件令牌或生物识别（如指纹、人脸识别）。通过与 LDAP 目录服务集成，实现用户账号的集中管理和权限分配。这确保只有授权用户可访问相应资源，防止非法用户的入侵。例如，学生只能访问与自己学习相关的教学资源，教师可以访问教学和科研相关的资源，管理员则拥有更高的权限，能够管理和配置系统。

安全态势感知系统对全网安全事件进行集中管理和分析，通过收集和分析网络设备、服务器、安全设备等产生的日志数据，实时了解网络的安全状态。当发现安全事件时，能够及时提供预警，并支持应急响应，协助安全人员快速采取措施，降低安全风险。

### 1.3 网络应用需求

#### 1.3.1 教学科研应用

在当今数字化教育时代，教学科研应用对于高校的发展至关重要。中国石油大学（北京）高度重视教学科研应用的建设，致力于为师生提供优质的网络服务，以支持在线教学平台、虚拟实验室、科研数据共享等应用的高效运行。

在线教学平台已成为现代教学的重要组成部分，它打破了时间和空间的限制，为师生提供了更加灵活的教学方式。通过在线教学平台，教师可以进行课程直播、录制教学视频、发布教学资料等，学生可以随时随地进行学习、参与讨论、提交作业等。虚拟实验室则为科研人员提供了一个虚拟的实验环境，他们可以在虚拟环境中进行实验操作、模拟实验过程，减少了实际实验的成本和风险。科研数据共享平台促进了科研人员之间的合作与交流，他们可以在平台上共享科研数据、研究成果等，推动科研工作的进展。

为了确保视频会议、远程实验等实时业务的流畅运行，学校需要采用一系列先进的技术手段。在网络带宽方面，需要保障充足的带宽资源，通过优化网络架构，确保核心层、汇聚层和接入层之间的高速连接，减少网络延迟和丢包率。在网络协议方面，采用实时传输协议（RTP）等，确保数据能够实时、准确地传输。在服务器性能方面，配备高性能的服务器，提高服务器的处理能力和响应速度。

大模型服务器在人工智能、机器学习等科研方向中扮演着关键角色。它为这些科研方向提供强大的算力支持，支持模型训练、推理和部署等全流程操作。在模型训练阶段，大模型服务器利用其强大的计算能力，快速处理大量的训练数据，加速模型的收敛速度，提高模型的准确性。在推理阶段，能够根据训练好的模型，快速对新的数据进行预测和分析。在部署阶段，将训练好的模型部署到实际应用中，为科研人员提供便捷的服务。

#### 1.3.2 办公管理应用

办公管理应用是保障学校日常办公和管理工作顺利进行的重要支撑。办公自动化（OA）系统实现了办公流程的数字化和自动化，提高了办公效率。例如，文件的审批、传阅等流程可以在 OA 系统中快速完成，减少了人工传递的时间和错误。一卡通系统集成了多种功能，如消费支付、门禁控制、考勤管理等，方便了师生的日常生活和学校的管理工作。财务管理系统则对学校的财务收支进行精细化管理，确保财务数据的准确性和安全性。

统一身份认证系统与各业务系统无缝对接，实现单点登录，这极大地提高了办公效率。师生只需使用一套账号和密码，就可以登录到各个业务系统，无需重复输入账号和密码，节省了时间和精力。同时，统一身份认证系统还加强了对用户身份的验证和管理，提高了系统的安全性。

在技术实现上，统一身份认证系统采用了 OAuth、OpenID Connect 等标准协议，与各业务系统进行集成。通过这些协议，各业务系统可以信任统一身份认证系统的认证结果，实现用户的单点登录。同时，为了确保数据传输的安全性，采用了 SSL/TLS 加密协议，对数据进行加密传输，防止数据被窃取或篡改。

#### 1.3.3 师生服务应用

云网盘服务为师生提供了高速上传下载、多终端同步功能，方便师生存储和共享教学资料、科研数据。师生可以将自己的文件上传到云网盘，随时随地进行访问和下载，不受时间和空间的限制。多终端同步功能使得师生在不同的设备上，如电脑、手机、平板等，都能同步查看和编辑自己的文件，提高了工作和学习的便利性。

人脸识别系统部署于各楼宇出入口，实现人员身份识别和考勤管理，有效提升了校园安全管理水平。通过人脸识别技术

## 第 2 章 网络技术调研

### 2.1 网络互连技术

#### 2.1.1 局域网互连技术

以太网技术作为局域网互连的核心技术，基于 IEEE 802.3 标准，在校园网中发挥着至关重要的作用。该标准经过多年的发展和完善，涵盖了多种不同的规范，以适应不同的网络需求。例如，早期的 IEEE 802.3 10Base - 5 使用粗同轴电缆，最大网段长度可达 500 米，采用基带传输方法，在早期的局域网建设中得到了广泛应用；IEEE 802.3 10Base - T 则使用双绞线电缆，最大网段长度为 100 米，因其布线方便、成本较低等优势，成为了目前最常用的以太网规范之一。随着技术的不断进步，IEEE 802.3 100Base - TX 使用两对 5 类非屏蔽双绞线（UTP）和 RJ - 45 接头，实现了 100Mbps 的传输速率，单条线缆长度可达 100 米，满足了对网络速度要求较高的场景；而 IEEE 802.3 1000Base - SX 使用多模光纤传输，传送距离可达 550 米，IEEE 802.3 1000Base - LX 使用单模光纤，在采用直径 10 微米的单模光纤时，传送距离更是可达 5000 米，这些规范为长距离、高速率的网络连接提供了可能。

在校园网中，局域网通常采用分层架构设计，主要分为核心层、汇聚层和接入层。核心层作为网络的高速交换主干，承担着大量数据的快速转发任务，要求具备极高的性能和可靠性。例如，主校区行政楼网络中心部署的核心交换机，需要具备高速的数据处理能力和大容量的缓存，以确保数据能够快速、准确地在核心层与汇聚层之间传输。汇聚层则起到了承上启下的作用，它将接入层的流量进行汇聚，并实现 VLAN 间路由、QoS 策略和安全策略执行等功能，减轻核心层的压力。以主校区教学楼的汇聚层为例，汇聚交换机需要对来自各个教室和办公室的接入层交换机的流量进行汇总，并根据不同的业务需求进行相应的处理，如为教学视频会议流量分配更高的优先级。接入层则直接连接终端设备，为用户提供网络接入服务，要求具备高密度端口和即插即用的特性。如主校区教学楼每层部署的接入交换机，需要提供足够数量的端口，以满足教室信息点和无线 AP 的接入需求。

VLAN（虚拟局域网）划分是提高网络性能和安全性的重要手段。通过 VLAN 划分，可以将一个物理局域网划分为多个逻辑上独立的虚拟局域网，每个 VLAN 之间的通信需要通过三层设备进行转发，从而隔离了广播域，减少了广播风暴的影响，提高了网络性能。同时，不同 VLAN 之间的访问可以通过访问控制列表（ACL）进行控制，增强了网络的安全性。例如，在校园网中，可以将教学区域、办公区域和服务器区域分别划分到不同的 VLAN 中。教学区域的 VLAN 可以限制对外部网络的访问，只允许访问教育网相关资源，以保障教学网络的安全和稳定；办公区域的 VLAN 可以根据不同部门进行细分，限制不同部门之间的互访，保护部门内部的数据安全；服务器区域的 VLAN 则可以设置严格的访问控制策略，只允许授权的设备进行访问，防止服务器受到攻击。

#### 2.1.2 广域网互连技术

广域网互连技术是实现主校区与分校区、校园网与外部网络连接的关键。光纤传输以其高带宽、低延迟和高可靠性的特点，成为了广域网连接的首选方式之一。主校区通过两根光纤分别接入教育网和联通网，为校园网与外部网络的通信提供了高速、稳定的通道。教育网光纤连接使得学校能够与其他教育机构进行高效的学术交流和资源共享，如参与教育网内的在线学术会议、访问教育网的学术数据库等；联通网光纤连接则为师生提供了更广泛的公网接入，满足了师生对互联网资源的多样化需求，如访问各类商业网站、在线学习平台等。

MPLS VPN（多协议标签交换虚拟专用网络）是一种基于标签交换的广域网技术，它通过在网络边缘为数据包添加标签，实现了快速的数据转发和流量工程。MPLS VPN 具有良好的扩展性和安全性，适用于大型企业和机构的广域网连接。在校园网中，如果需要实现更高级的流量管理和安全隔离，MPLS VPN 可以作为一种可选的技术方案。例如，学校可以利用 MPLS VPN 将不同的业务流量划分到不同的虚拟专用网络中，实现教学、科研和管理业务的隔离，提高网络的安全性和稳定性。

SD - WAN（软件定义广域网）是一种新兴的广域网技术，它通过软件定义的方式实现了网络的集中管理和智能路由。SD - WAN 可以根据网络的实时状态和业务需求，自动选择最佳的网络路径，实现流量的优化和负载均衡。同时，SD - WAN 还支持多种接入方式，如光纤、4G/5G 等，提高了网络的灵活性和可靠性。在本方案中，虽然目前分校区通过 VPN 设备与主校区连接，但未来随着业务的发展和网络需求的增加，引入 SD - WAN 技术具有很大的可行性。例如，当学校开展大规模的在线教学活动时，SD - WAN 可以根据实时的网络流量和带宽情况，自动调整教学视频流量的传输路径，确保教学活动的流畅进行；在应对网络故障时，SD - WAN 可以快速切换到备用链路，保障关键业务的正常运行。

#### 2.1.3 VPN 技术

VPN（Virtual Private Network，虚拟专用网络）技术通过在公共网络上构建加密隧道，实现了专用通信链路的功能，适用于分校区与主校区的互连等场景。其原理主要基于隧道技术、加密技术和身份认证技术。隧道技术是 VPN 的核心技术之一，它将原始数据包封装在新的数据包中，通过公共网络进行传输。例如，在 IPsec VPN 中，会使用 IPsec 协议对数据进行封装，在原始数据的外层添加新的协议头，这个协议头包含了 VPN 服务器和用户设备之间的连接信息，使得数据能够在公共网络中安全传输。加密技术则对传输的数据进行加密，确保数据的保密性和完整性。常见的加密算法有 AES（高级加密标准）、3DES（三重数据加密标准）等，以 AES 加密算法为例，它能够将用户的数据转换为密文形式，只有拥有正确密钥的接收方（通常是 VPN 服务器）才能将密文还原为原始数据，从而保护了数据在传输过程中的隐私和安全。身份认证技术用于确保只有授权用户可以接入网络，常见的方式有用户名 / 密码认证、数字证书认证、双因素认证等。例如，使用数字证书认证时，用户设备需要安装由认证机构颁发的数字证书，在连接 VPN 时，VPN 服务器会验证这个数字证书的有效性，只有证书有效且匹配的用户才能成功连接，有效防止了未经授权的用户接入 VPN 网络。

IPsec VPN 是目前最常用的 VPN 技术之一，工作在网络层，提供数据加密、完整性校验和访问控制等安全功能。在本项目中，分校区网络机房通过 IPsec VPN 设备与主校区行政楼网络中心建立隧道，实现两校区局域网的无缝对接。具体来说，分校区的 IPsec VPN 设备会对分校区局域网内的数据进行封装和加密，然后通过公共网络传输到主校区的 IPsec VPN 设备，主校区的设备再对数据进行解封装和解密，将数据转发到主校区局域网。这样，两校区之间的业务（如统一身份认证、数据共享）就能够在安全的环境下正常运行。同时，IPsec VPN 还可以通过配置访问控制策略，限制不同校区之间的访问权限，进一步提高网络的安全性。

### 2.2 网络接入技术

#### 2.2.1 有线接入技术

以太网接入是校园网有线接入的主要方式，采用 RJ45 接口和双绞线（如超五类、六类线），支持 10/100/1000Mbps 速率。在主校区行政楼办公室、实验室等信息点均采用六类线布线，满足千兆接入需求。六类线相比超五类线，具有更高的带宽和抗干扰能力，能够更好地支持高速数据传输。例如，在实验室中，科研人员需要传输大量的实验数据，六类线的千兆接入速率能够确保数据快速、稳定地传输，提高科研工作效率。核心层与汇聚层之间采用万兆光纤互联，确保骨干链路带宽。万兆光纤具有极高的传输速率和大容量的带宽，能够满足核心层与汇聚层之间大量数据的快速传输需求，保障校园网的整体性能。

PoE（Power over Ethernet，以太网供电）供电技术通过以太网交换机为 IP 电话、无线 AP、摄像头等设备提供电力和数据传输，简化了布线结构。其原理是利用以太网双绞线中的空闲线对或数据传输线对同时传输电力和数据。例如，在主校区教学楼的无线 AP 部署中，采用 PoE 交换机为无线 AP 供电，无需单独部署电源线，不仅提高了施工效率，还使教学楼内的布线更加简洁美观。同时，PoE 技术还便于对设备进行集中管理和维护，当无线 AP 出现故障时，可以通过 PoE 交换机快速检测和定位问题，提高了网络的可靠性和可维护性。

#### 2.2.2 无线接入技术

Wi - Fi 6（802.11ax）作为新一代无线通信标准，相比其他无线通信标准具有诸多优势。它支持更高的传输速率，理论峰值可达 9.6Gbps，能够满足高密度场景下大量用户同时接入的高速数据传输需求。例如，在学校的大型教室或图书馆等人员密集区域，众多学生同时使用电子设备进行学习和查阅资料，Wi - Fi 6 的高传输速率可以确保每个用户都能获得流畅的网络体验。更大的并发连接数也是 Wi - Fi 6 的重要优势之一，它能够支持更多的设备同时连接到同一个无线接入点，有效解决了传统无线网络在用户数量增加时容易出现的网络拥堵问题。更低的延迟使得 Wi - Fi 6 在实时应用场景中表现出色，如在线视频会议、实时游戏等，用户几乎感受不到明显的延迟，提高了应用的交互性和实时性。此外，Wi - Fi 6 采用了 OFDMA（正交频分多址）技术，将信道划分为多个子信道，允许多个用户同时在不同的子信道上进行数据传输，大大提升了多用户并发效率；MU - MIMO（多用户多输入多输出）技术则支持单 AP 同时与 8 台设备通信，进一步提高了无线网络的效率。

无线控制器（AC）+ 瘦 AP（Fit AP）架构通过无线控制器集中管理所有瘦 AP，实现了无线信号的自动调优、用户漫游切换和安全策略统一配置。主校区部署华为 iMaster NCE - Campus 无线控制器，支持管理 2000 + 瘦 AP，分校区通过隧道协议接入主控制器，实现统一配置和固件升级。无线控制器可以实时监测各个瘦 AP 的信号强度、负载情况等，自动调整无线信号的发射功率和信道，确保无线信号覆盖均匀，减少信号干扰。当用户在校园内移动时，无线控制器能够实现用户在不同瘦 AP 之间的无缝漫游切换，保证用户的网络连接不中断。在安全策略方面，无线控制器可以统一配置加密方式、认证方式等，提高了无线网络的安全性和管理效率。

### 2.3 网络安全技术

#### 2.3.1 边界防护技术

防火墙作为网络安全的第一道防线，部署于网络边界，如校园网与教育网、公网连接处。它基于 IP 地址、端口、协议等规则对流量进行过滤，阻止未经授权的访问。主校区出口部署的下一代防火墙（NGFW），不仅具备传统防火墙的基本功能，还支持应用层流量识别和深度包检测（DPI）。通过应用层流量识别，能够精准识别各种网络应用，如 P2P 下载、视频流媒体、在线游戏等；通过深度包检测，能够对网络数据包进行深入分析，检测其中是否包含恶意代码、攻击行为等，从而精准识别并控制非业务流量，保障关键应用带宽。例如，当检测到 P2P 下载软件占用大量带宽时，防火墙可以根据预设的策略，限制 P2P 下载的流量，确保教学、科研等关键业务的网络带宽不受影响。

Web 防火墙（WAF）主要针对 Web 应用层攻击，如 SQL 注入、XSS 跨站脚本攻击等。学校网站、教务系统等 Web 应用是学校对外展示和内部管理的重要窗口，容易成为黑客攻击的目标。部署 Web 防火墙，对 HTTP/HTTPS 流量进行深度检测和防护，能够有效保护这些 Web 应用免受攻击。例如，当有黑客试图通过 SQL 注入攻击教务系统时，Web 防火墙可以实时检测到恶意的 SQL 语句，并阻止攻击请求，确保教务系统的安全稳定运行。

#### 2.3.2 入侵检测与防御技术

入侵检测系统（IDS）通过旁路部署方式监听网络流量，实时检测潜在的入侵行为，如端口扫描、恶意代码传播等，并发送告警信息。主校区数据中心部署 IDS，对服务器区域的流量进行监控，及时发现针对服务器的攻击尝试。例如，当 IDS 检测到有外部 IP 对服务器进行频繁的端口扫描时，会立即发送告警信息给网络管理员，管理员可以及时采取措施，如封禁该 IP 地址，防止进一步的攻击。

入侵防御系统（IPS）与 IDS 相比，具备实时阻断攻击的能力，可主动拦截恶意流量。在核心层或关键链路部署 IPS，可有效应对零日漏洞攻击和高级持续性威胁（APT）。例如，当 IPS 检测到有恶意软件试图通过网络传播时，会立即阻断相关的网络连接，防止恶意软件扩散到校园网内的其他设备，保障校园网络的安全。

#### 2.3.3 数据加密技术

传输层加密采用 SSL/TLS 协议对数据传输过程进行加密，确保用户登录信息、敏感数据在网络传输中的安全性。例如，统一身份认证系统与各业务系统之间的通信启用 HTTPS 协议，HTTPS 协议基于 SSL/TLS 协议，对数据进行加密传输，防止数据被窃取或篡改。当用户在登录教务系统时，用户名和密码等登录信息在传输过程中被加密，即使数据被黑客截获，由于没有解密密钥，黑客也无法获取用户的真实信息。

存储加密对数据中心服务器的硬盘、云平台存储卷进行加密，防止物理设备丢失或被盗导致的数据泄露。可采用 AES - 256 等高强度加密算法，确保数据存储安全。例如，在数据中心，服务器的硬盘采用 AES - 256 加密算法对存储的数据进行加密，即使硬盘丢失或被盗，没有正确的解密密钥，攻击者也无法读取硬盘中的数据，保护了学校的关键数据安全。

#### 2.3.4 身份认证技术

统一身份认证系统采用 “用户名 + 密码 + 多因子认证” 机制，多因子认证可集成短信验证码、硬件令牌或生物识别（如指纹、人脸识别）。通过与 LDAP 目录服务集成，实现用户账号的集中管理和权限分配，确保只有授权用户可访问相应资源。例如，学生在登录校园网的各类应用系统时，除了输入用户名和密码外，还需要输入手机收到的短信验证码进行多因子认证。与 LDAP 目录服务集成后，系统可以根据用户的身份信息，如学生、教师、管理员等，分配相应的访问权限。学生只能访问与自己学习相关的教学资源，教师可以访问教学和科研相关的资源，管理员则拥有更高的权限，能够管理和配置系统，从而确保了用户身份的真实性和访问权限的合理性。

### 2.4 数据中心

#### 2.4.1 架构设计

虚拟化架构通过将物理服务器资源抽象为虚拟服务器（VM），实现了计算资源的动态分配和高可用性（HA）。采用 VMware vSphere 或开源的 KVM 虚拟化平台，多个虚拟服务器可以在同一台物理服务器上运行，每个虚拟服务器都拥有独立的操作系统和应用程序环境，相互之间互不干扰。当某个业务系统的负载增加时，虚拟化平台可以动态地为其分配更多的计算资源，如 CPU、内存等；当负载降低时，又可以回收多余的资源，提高资源的利用率。例如，在期末考试期间，教务管理系统的负载会大幅增加，虚拟化平台可以自动为教务管理系统所在的虚拟服务器分配更多的 CPU 和内存资源，确保系统能够稳定运行。

在实现高可用性方面，虚拟化架构支持服务器集群部署。当某台物理服务器故障时，虚拟机会自动迁移至其他服务器运行，确保业务不中断。以 VMware vSphere HA 技术为例，它通过心跳检测机制实时监控物理服务器的状态，当发现某台服务器出现故障时，会自动将其上的虚拟机迁移到集群内其他正常运行的服务器上，整个迁移过程对用户来说是透明的，几乎不会影响业务的正常进行。

#### 2.4.2 存储系统

SAN（Storage Area Network，存储区域网络）存储采用光纤通道（FC）或 iSCSI 协议，为虚拟化平台提供集中式存储。主校区数据中心部署的全闪存阵列（AFA），采用高速的闪存作为存储介质，具有极高的随机读写 IOPS（Input/Output Operations Per Second，每秒输入 / 输出操作次数），能够满足大模型服务器对高性能存储的需求，支持随机读写 IOPS 达百万级别。例如，在大模型训练过程中，需要频繁地读取和写入大量的数据，全闪存阵列的高性能能够确保数据的快速读写，加速模型的训练速度。

NAS（Network Attached Storage，网络附属存储）存储用于文件共享和云网盘服务，采用 NFS/CIFS 协议，支持多客户端同时访问。可通过集群 NAS 架构实现存储容量和性能的横向扩展，满足 2 万师生的存储需求。例如，当学校的师生数量增加或云网盘的使用量增长时，可以通过添加更多的 NAS 存储设备到集群中，实现存储容量的扩展，同时，集群 NAS 架构还能够提高存储系统的性能和可靠性，确保师生能够快速、稳定地访问云网盘。

#### 2.4.3 网络设计

数据中心网络采用 “核心 - 接入” 两层架构，核心交换机采用万兆光纤互联，接入交换机为服务器提供千兆 / 万

## 第 3 章 网络结构设计

### 3.1 网络分层架构设计

#### 3.1.1 核心层设计

核心层作为校园网的神经中枢，其设计目标至关重要。它肩负着实现高速数据转发的重任，要确保数据能够以最快的速度在校园网内传输，满足师生在教学、科研和办公过程中对数据实时性的高要求。多链路冗余设计则是为了保障网络的可靠性，当某条链路出现故障时，数据能够自动切换到其他备用链路进行传输，从而确保网络的不间断运行。全局流量调度功能可以根据网络的实时负载情况，合理分配网络资源，使网络资源得到最优化的利用，避免出现网络拥塞的情况。此外，核心层还需保证主校区与分校区、校园网与外部网络的高效互通，实现资源的共享和交互。

在设备部署方面，选择在主校区行政楼网络中心部署 2 台华为 S12700 万兆核心交换机。这款交换机具备卓越的性能，交换容量达 23.04Tbps，拥有 48×10GE 光口和 6×40GE 光口，能够满足万兆骨干链路的需求。通过采用集群堆叠技术（CSS2），这 2 台交换机可以形成逻辑单一设备，从而提高了设备的可靠性和管理效率。当其中一台交换机出现故障时，另一台可以立即接管其工作，确保网络的正常运行。同时，集群堆叠技术还可以实现带宽的聚合，提高网络的整体性能。

链路设计对于核心层的性能也起着关键作用。核心层与汇聚层之间采用双万兆光纤链路（主备链路），这种设计可以提供更高的带宽和更好的冗余性。当主链路出现故障时，数据可以自动切换到备用链路进行传输，保证网络的不间断运行。核心交换机与教育网、联通网出口路由器通过 10GE 光口连接，确保了校园网与外部网络的高速互联。通过 IPsec VPN 设备与分校区建立冗余隧道，实现了主校区与分校区之间的安全、可靠通信。

在功能特性方面，启用 OSPFv3 动态路由协议，支持 IPv4/IPv6 双栈。这使得校园网能够同时支持 IPv4 和 IPv6 两种协议，适应未来网络发展的趋势。配置 BGP 协议实现多运营商链路负载均衡和故障切换，当教育网或联通网的链路出现故障时，BGP 协议可以自动将流量切换到其他正常的链路，确保网络的畅通。部署硬件级 ACL 过滤非业务流量，通过设置访问控制列表，可以阻止未经授权的流量进入核心层，保障核心层的安全，提高网络的安全性和稳定性。

#### 3.1.2 汇聚层设计

汇聚层在校园网中扮演着至关重要的角色，其设计目标是收敛接入层流量，将来自各个接入层交换机的流量进行汇总，然后传输到核心层。同时，它还承担着实现 VLAN 间路由的任务，不同 VLAN 之间的通信需要通过汇聚层进行路由转发。执行 QoS 策略也是汇聚层的重要功能之一，它可以根据不同的业务需求，对流量进行分类和优先级标记，确保关键业务（如教学视频会议、科研数据传输）的带宽和延迟要求得到满足。执行安全策略可以防止网络攻击和非法访问，保护校园网的安全。通过这些功能，汇聚层有效地减轻了核心层的压力，提高了校园网的整体性能和安全性。

在主校区汇聚层，教学楼、实验楼、行政楼各部署 2 台新华三 S5130 万兆汇聚交换机。这款交换机支持 48×GE 电口 + 4×10GE 光口，交换容量达 512Gbps，具备强大的处理能力。采用 IRF2 堆叠技术实现设备冗余，当其中一台交换机出现故障时，另一台可以立即接管其工作，确保网络的正常运行。实验楼汇聚交换机额外配置 PoE 模块，为实验室设备（如可编程控制器、传感器）提供电力和数据接入，方便了实验室设备的部署和使用，减少了布线的复杂性。

在分校区汇聚层，行政大楼机房部署 2 台 Cisco Catalyst 9300 千兆汇聚交换机。该交换机支持 24×GE 电口 + 4×10GE 光口，通过单模光纤上联至主校区核心层，下联分校区各楼宇接入层，实现了分校区与主校区的连接以及分校区内部各楼宇之间的通信。

汇聚层的功能特性也十分丰富。启用 VLAN 间路由（SVI 接口），通过配置 SVI 接口，可以实现不同 VLAN 之间的通信。配置 QoS 策略区分教学、科研、办公流量优先级，根据不同业务的需求，为教学、科研、办公流量分配不同的优先级，确保关键业务的带宽和延迟要求得到满足。部署 DHCP 中继服务，为接入层终端分配 IP 地址，简化了终端设备的 IP 地址配置过程，提高了网络管理的效率。

#### 3.1.3 接入层设计

接入层是校园网与终端设备直接连接的部分，其设计目标是提供高密度端口，以满足大量终端设备的接入需求。同时，要实现即插即用功能，方便用户快速接入网络，减少用户的配置时间和操作难度。安全接入控制也是接入层的重要功能之一，通过采用各种安全技术，如 802.1X 认证、端口安全等，防止非法设备接入网络，保护校园网的安全。此外，接入层还支持有线无线一体化部署，满足用户在不同场景下的网络接入需求。

在主校区接入层，教学楼每层部署 2 台 Cisco Catalyst 9200L 千兆接入交换机（24×GE PoE + 电口）。这些交换机为教室信息点（每教室 1 个）和无线 AP 供电，支持 802.1X 端口认证，通过 802.1X 认证，可以确保只有授权的设备才能接入网络，提高了网络的安全性。实验楼每层实验室部署 4 台华为 S5735 - L24P4S - A 千兆 PoE 交换机（24×GE PoE + 电口），每个实验室 30 个信息点通过六类线接入，支持端口限速和风暴抑制。端口限速可以限制每个端口的带宽使用，防止个别设备占用过多带宽，影响其他设备的正常使用；风暴抑制可以防止网络风暴的产生，保障网络的稳定运行。行政楼办公室区域采用新华三 S5130 - 28S - GE 千兆交换机（24×GE 电口 + 4×10GE 光口），每间办公室 10 个信息点划分独立 VLAN，实现了不同办公室之间的网络隔离，提高了网络的安全性和管理效率；网络中心机房部署万兆接入交换机，支持服务器直接上联核心层，满足了服务器对高速网络连接的需求。

在分校区接入层，教学楼每层部署 2 台新华三 S5024PV3 - EI 千兆 PoE 交换机（24×GE PoE + 电口），支持每教室 1 个信息点和无线 AP 接入。计算机中心（7 层）部署 8 台华为 S6720 - 30C - EI 万兆交换机（24×10GE 光口 + 4×40GE 光口），为 300 个信息点提供万兆接入，满足了高性能计算需求，确保了计算机中心的高速数据传输。

为了增强接入层的安全性，启用端口安全（Port Security）限制单端口接入设备数量，防止非法设备接入网络。配置 DHCP Snooping 防止 IP 欺骗，通过检查 DHCP 报文的合法性，防止非法的 DHCP 服务器接入网络，保护网络的安全。部署 IP - MAC 地址绑定，将 IP 地址和 MAC 地址进行绑定，确保只有合法的设备才能使用指定的 IP 地址，增强了接入层的安全性。

#### 3.1.4 Internet 接入设计

实现校园网与教育网、公网的高速互联是校园网建设的重要目标之一。这不仅能够满足师生对教育资源和互联网资源的访问需求，还能够促进学校与外界的交流与合作。保障多链路可靠性可以确保网络的不间断运行，当某条链路出现故障时，数据能够自动切换到其他备用链路进行传输。流量优化则可以根据网络的实时负载情况，合理分配网络资源，提高网络的利用率，确保关键业务的带宽和延迟要求得到满足。

在出口架构方面，主校区部署 2 台华为 AR6000 系列万兆路由器，分别连接教育网（1000Mbps 光纤）和联通网（500Mbps 光纤）。通过 BGP 协议实现双链路负载均衡和互为备份，BGP 协议可以根据链路的带宽、延迟、可靠性等因素，自动选择最佳的链路进行数据传输。当教育网链路的负载过高时，BGP 协议可以将部分流量切换到联通网链路，实现负载均衡；当某条链路出现故障时，BGP 协议可以立即将流量切换到其他正常的链路，确保网络的畅通。

NAT 与防火墙配置也是 Internet 接入设计的重要部分。出口路由器配置动态 NAT，为校内私有 IP 地址提供公网转换，使校内设备能够访问互联网。串联华为 USG6000 下一代防火墙，对进出流量进行应用层检测，防火墙可以识别各种网络应用，如 P2P 下载、视频流媒体、在线游戏等，并根据预设的策略对这些应用进行控制。同时，防火墙还可以阻断勒索软件、钓鱼攻击等威胁，保护校园网的安全。

流量管理是保障网络性能的关键措施。通过 QoS 策略优先保障教学视频会议、科研数据传输等实时流量，为这些关键业务分配较高的带宽和较低的延迟，确保其正常运行。限制 P2P 下载、视频流媒体等非关键流量带宽，防止这些非关键业务占用过多带宽，影响关键业务的使用。部署 DNS 缓存服务器，减少外部 DNS 查询延迟，提高网络访问速度。DNS 缓存服务器可以缓存常用的域名解析结果，当用户再次访问相同的域名时，DNS 缓存服务器可以直接返回解析结果，无需再次查询外部 DNS 服务器，从而减少了查询延迟。

### 3.2 网络拓扑图设计

采用分层星型架构的网络拓扑图设计，这种架构具有清晰的层次结构和良好的扩展性。它分为核心层、汇聚层、接入层三级结构，分校区通过 VPN 链路接入主校区核心层，形成了一个有机的整体。

核心层位于主校区网络中心，以双核心交换机为中心，通过万兆光纤辐射至各楼宇汇聚层，并连接出口路由器和 VPN 设备。双核心交换机的部署提供了冗余和高性能的保障，当其中一台核心交换机出现故障时，另一台可以立即接管其工作，确保网络的正常运行。万兆光纤的高速传输能力可以满足核心层与汇聚层之间大量数据的快速传输需求，保障校园网的整体性能。出口路由器负责连接校园网与教育网、公网，实现校园网与外部网络的通信；VPN 设备则用于实现主校区与分校区之间的安全连接。

汇聚层分布于主校区和分校区各主要楼宇（如行政楼、实验楼），通过千兆 / 万兆链路下联接入层，上联核心层。汇聚层的主要作用是汇聚接入层的流量，并将其传输到核心层。同时，汇聚层还可以实现 VLAN 间路由、QoS 策略和安全策略执行等功能，减轻核心层的压力。

接入层部署于各楼层，通过双绞线连接终端设备，无线 AP 通过 PoE 交换机接入有线网络。接入层直接面向用户，为用户提供网络接入服务。双绞线的使用方便了终端设备的连接，PoE 交换机则为无线 AP 提供电力和数据传输，简化了布线结构。

分校区连接通过 IPsec VPN 隧道与主校区核心层通信，隧道带宽根据业务需求配置为 100Mbps，支持加密算法 AES - 256 和认证算法 SHA - 256。IPsec VPN 隧道的使用可以确保分校区与主校区之间的数据传输安全，防止数据被窃取或篡改。AES - 256 加密算法和 SHA - 256 认证算法提供了高强度的加密和认证，保障了数据的机密性和完整性。

在拓扑图说明中，主校区与分校区之间用虚线表示 VPN 隧道，这样可以清晰地表示出两者之间的连接方式和数据传输路径。核心层与汇聚层之间用双线表示冗余链路，表明这些链路具有冗余备份功能，当其中一条链路出现故障时，另一条链路可以继续工作，确保网络的可靠性。服务器区、无线用户区、办公区等通过不同颜色标注，这样可以清晰区分业务区域，方便网络管理和故障排查。出口处标注教育网和联通网链路带宽及安全设备部署位置，使网络管理员能够直观地了解网络出口的情况，便于进行流量管理和安全控制。

### 3.3 网络可靠性设计

#### 3.3.1 设备冗余

设备冗余是确保网络高可用性的重要手段之一。在核心层，双核心交换机堆叠部署，控制平面和数据平面冗余，这种设计可以有效地提高核心层的可靠性。控制平面负责处理网络协议和路由信息，数据平面则负责数据的转发。当单台设备故障时，由于控制平面和数据平面的冗余，流量可以自动切换到另一台设备进行转发，不会影响网络的正常运行。例如，在主校区行政楼网络中心部署的 2 台华为 S12700 万兆核心交换机，通过集群堆叠技术（CSS2）形成逻辑单一设备，实现了控制平面和数据平面的冗余，大大提高了核心层的可靠性。

在汇聚层，每楼宇部署 2 台汇聚交换机，采用链路聚合（LACP）上联核心层。链路聚合是将多个物理链路捆绑成一个逻辑链路，增加了链路的带宽和可靠性。当单台交换机或单条链路故障时，流量可以自动切换至备份设备 / 链路，确保网络的不间断运行。例如，在主校区教学楼、实验楼、行政楼各部署的 2 台新华三 S5130 万兆汇聚交换机，通过 IRF2 堆叠技术实现设备冗余，并采用链路聚合上联核心层，提高了汇聚层的可靠性。

在服务器区，关键业务服务器（如教务系统、大模型服务器）采用双网卡绑定技术，分别接入不同汇聚交换机，实现多路径冗余。双网卡绑定技术可以将两个网卡虚拟成一个网卡，增加了网络连接的带宽和可靠性。当其中一个网卡或连接的链路出现故障时，另一个网卡可以继续工作，确保服务器的网络连接不中断。例如，教务系统服务器通过双网卡分别接入不同的汇聚交换机，实现了多路径冗余，提高了教务系统的可靠性。

#### 3.3.2 链路冗余

链路冗余对于保障网络可靠性起着至关重要的作用。在核心 - 汇聚层，主校区各楼宇汇聚层与核心层之间采用双万兆光纤链路（不同物理路径），通过 OSPF 协议设置不同开销值，实现主备链路自动切换。当主链路出现故障时，OSPF 协议可以根据开销值的变化，自动将流量切换到备用链路，确保网络的正常运行。例如，主校区教学楼汇聚层与核心层之间的双万兆光纤链路，一条链路作为主链路，设置较小的开销值；另一条链路作为备用链路，设置较大的开销值。当主链路正常时，流量通过主链路传输；当主链路出现故障时，OSPF 协议会自动将流量切换到备用链路，实现主备链路的自动切换。

在分校区互联方面，除 IPsec VPN 主隧道外，预留 4G 无线备份链路。当光纤链路中断时，通过 4G 路由器自动接入公网，维持关键业务（如统一身份认证）运行。4G 无线备份链路作为备用链路，在光纤链路出现故障时，可以确保关键业务的正常运行。例如，当分校区与主校区之间的光纤链路因故障中断时，4G 路由器可以自动启动，通过 4G 网络接入公网，然后通过公网与主校区建立连接，维持统一身份认证等关键业务的运行。

#### 3.3.3 电源与散热

电源与散热是保障网络设备稳定运行的重要因素。在核心层、汇聚层设备部署于标准机柜，采用双电源模块（AC 220V+DC 48V），连接至园区 UPS 不间断电源系统。双电源模块的设计可以确保在其中一个电源模块出现故障时，设备仍然能够正常运行。UPS 不间断电源系统可以在市电中断时，为设备提供持续的电力供应，确保断电后设备持续运行 30 分钟以上。例如，在主校区行政楼网络中心的核心层和汇聚层设备，采用双电源模块，并连接至园区 UPS 不间断电源系统，提高了设备的供电可靠性。

网络中心机房配置精密空调系统，维持温度 22±2℃、湿度 50%±10%。适宜的温度和湿度对于网络设备的稳定运行至关重要。过高或过低的温度、湿度都可能导致设备故障。精密空调系统可以精确控制机房的温度和湿度，避免设备因过热导致故障。例如，在炎热的夏季，精密空调系统可以将机房温度维持在 22℃左右，确保设备在适宜的环境下运行。

#### 3.3.4 业务连续性

业务连续性对于校园网来说至关重要，它直接影响到教学、科研和管理工作的正常进行。在虚拟化平台方面，数据中心服务器采用 VMware vSphere HA 技术，当物理服务器故障时，虚拟机在 30 秒内迁移至集群内其他服务器。VMware vSphere HA 技术通过心跳检测机制实时监控物理服务器的状态，当发现某台服务器出现故障时，会自动将其上的虚拟机迁移到集群内其他正常运行的服务器上，整个迁移过程对用户来说是透明的，几乎不会影响业务的正常进行。例如，当数据中心的某台物理服务器出现硬件故障时，VMware vSphere HA 技术可以在 30 秒内将其上的虚拟机迁移到其他服务器上，确保业务的连续性。

在云平台容灾方面，阿里云 Stack 私有云平台与公有云建立灾备链路，关键数据（如师生数据、科研成果）实时同步至公有云存储，满足等保 2.0 三级备份要求。通过建立灾备链路和实时同步数据，可以确保在私有云平台出现故障时，关键数据不会丢失，业务可以快速恢复。例如，当主校区的私有云平台因自然灾害等原因出现故障时，公有云存储中的数据可以快速恢复到备用的云平台上，确保师生数据和科研成果的安全，维持业务的正常运行。

### **3.4 网络设备选型**​

#### **3.4.1 交换机**​

在交换机选型上，核心层选用华为 S12700 万兆核心交换机。该系列交换机支持高达 288 个万兆端口，交换容量可达 128Tbps，包转发率为 48000Mpps，具备出色的高速数据处理能力。采用集群堆叠技术，可将多台交换机虚拟化为一台逻辑设备，极大提升了网络的可靠性和管理效率。主校区部署 2 台进行冗余配置，分校区各部署 1 台，保障核心层数据高速转发。​

汇聚层设备，主校区教学楼汇聚层选用华为 S5735 - S - 48T4X - A，该交换机提供 48 个千兆电口和 4 个万兆光口，支持丰富的 QoS 策略和 VLAN 划分功能，可有效收敛接入层流量，每栋教学楼部署 2 台实现冗余备份。分校区办公楼汇聚层采用新华三 S5130 - 28S - SI，具备 24 个千兆电口和 4 个万兆光口，端口密度和性能能够满足分校区汇聚层需求，每栋办公楼部署 1 台。​

接入层方面，主校区宿舍区接入层部署华为 S1730 - S24T4S - A2，该交换机拥有 24 个千兆电口和 4 个千兆光口，支持 PoE 供电功能，可为无线 AP、IP 电话等设备供电，每个宿舍单元部署 1 台。分校区实验室接入层选用 Cisco Catalyst 2960X - 24TS - LL，提供 24 个千兆电口和 2 个千兆光口，具备完善的安全接入控制功能，每个实验室部署 1 台。​

#### **3.4.2 路由器**​

出口路由器选型华为 AR6600 系列，该系列路由器支持高达 100Gbps 的转发性能，具备强大的路由处理能力和丰富的广域网接口。主校区部署 2 台 AR6620 进行双机热备，作为教育网 / 公网出口路由和 VPN 网关，实现与外部网络的高速互联，并保障校园网与分校区之间通过 IPsec VPN 安全通信。分校区各部署 1 台 AR6120，作为与主校区互联的 VPN 接入设备，满足分校区网络接入需求。​

#### **3.4.3 服务器**​

数据中心虚拟化平台服务器选用戴尔 PowerEdge R750，配置为 2 颗英特尔至强第三代可扩展处理器（64 核心 / 128 线程）、512GB DDR4 内存、2 块 1.92TB NVMe SSD 系统盘和 8 块 10TB SAS 数据盘，支持 NVIDIA Tesla T4 GPU 加速卡，每台服务器可提供强大的计算和存储能力，部署 4 台构建虚拟化集群，实现计算资源的动态分配和高可用性。​

人工智能模型训练服务器采用浪潮 NF5488A5，配备 4 颗英特尔至强铂金 8380 处理器、1TB DDR4 内存、8 块 3.84TB NVMe SSD 数据盘和 8 块 NVIDIA A100 GPU 加速卡，强大的计算性能和大容量存储能够满足大模型训练的需求，部署 3 台组成高性能计算集群。​

云平台服务器选用华为 TaiShan 200 2280，基于鲲鹏 920 处理器，配置为 2 颗 64 核心处理器、256GB DDR4 内存、4 块 960GB SSD 系统盘和 12 块 4TB SAS 数据盘，部署 5 台构建阿里云 Stack 私有云平台，为校园网提供弹性计算、存储和网络资源服务。​

#### **3.4.4 网络安全设备**​

校园网出口防火墙选用华为 USG6680E - 16，该防火墙支持高达 40Gbps 的吞吐量，具备丰富的安全防护功能，包括入侵防御、病毒防护、应用控制等，部署 2 台进行双机热备，实现对进出校园网流量的全面安全防护。​

Web 应用防火墙选用启明星辰 WAF - 6000 - T32，支持高达 10Gbps 的 HTTP/HTTPS 处理能力，可有效防护 SQL 注入、跨站脚本攻击等 Web 应用层攻击，部署在数据中心服务器区前端，保障 Web 应用系统的安全。​

上网行为管理设备选用深信服 AC - 1000 - B1400，支持高达 5Gbps 的上网行为管理吞吐量，可实现对用户上网行为的审计、管控和流量管理，部署在出口防火墙之后，规范师生上网行为，保障网络资源合理使用。​

### **3.5 VLAN 划分**​

基于楼宇、部门和业务类型进行 VLAN 划分，以提高网络安全性和管理效率。行政楼 VLAN ID 设为 100，名称为 Admin - Building，涵盖行政楼所有办公区域信息点，用于行政办公业务；教学楼 VLAN ID 设为 200 - 210，名称分别为 Teaching - Building1 - Teaching - Building10，每个教学楼对应一个 VLAN，用于教学相关业务；宿舍区 VLAN ID 设为 300 - 310，名称分别为 Dormitory - Area1 - Dormitory - Area10，每个宿舍区对应一个 VLAN，用于学生宿舍网络接入；服务器区 VLAN ID 设为 400，名称为 Server - Area，用于数据中心服务器通信；访客网络 VLAN ID 设为 500，名称为 Guest - Network，为外来访客提供网络接入。​

在汇聚层和核心层交换机之间配置 Trunk 链路，允许所有 VLAN 通过，并设置 VLAN 访问控制列表（ACL），防止 VLAN 跳跃攻击，保障网络安全。​

### 3.6 IP 地址规划和子网划分​

#### **3.6.1 地址空间选择**​

内网地址段采用私有地址空间 [10.0.0.0/8](http://10.0.0.0/8" \t "https://www.doubao.com/chat/_blank)，该地址段拥有大量可用 IP 地址，能够满足校园网未来扩展需求。同时，向教育网和运营商申请 IPv4 公网地址段 [202.112.145.0/24](http://202.112.145.0/24" \t "https://www.doubao.com/chat/_blank) 和 IPv6 公网地址段 2001:da8:1234::/48，用于校园网与外部网络的通信。​

#### 3.6.2 子网划分示例​

行政楼子网地址为 [10.1.1.0/24](http://10.1.1.0/24" \t "https://www.doubao.com/chat/_blank)，子网掩码 [255.255.255.0](http://255.255.255.0/" \t "https://www.doubao.com/chat/_blank)，可用 IP 数 254 个，网关地址 [10.1.1.1](http://10.1.1.1/" \t "https://www.doubao.com/chat/_blank)，用于行政楼办公设备网络接入；教学楼 1 子网地址为 [10.2.1.0/24](http://10.2.1.0/24" \t "https://www.doubao.com/chat/_blank)，子网掩码 [255.255.255.0](http://255.255.255.0/" \t "https://www.doubao.com/chat/_blank)，可用 IP 数 254 个，网关地址 [10.2.1.1](http://10.2.1.1/" \t "https://www.doubao.com/chat/_blank)，用于教学楼 1 教学设备和师生终端接入；宿舍区 1 子网地址为 [10.3.1.0/24](http://10.3.1.0/24" \t "https://www.doubao.com/chat/_blank)，子网掩码 [255.255.255.0](http://255.255.255.0/" \t "https://www.doubao.com/chat/_blank)，可用 IP 数 254 个，网关地址 [10.3.1.1](http://10.3.1.1/" \t "https://www.doubao.com/chat/_blank)，用于宿舍区 1 学生终端接入；服务器区子网地址为 [10.4.1.0/24](http://10.4.1.0/24" \t "https://www.doubao.com/chat/_blank)，子网掩码 [255.255.255.0](http://255.255.255.0/" \t "https://www.doubao.com/chat/_blank)，可用 IP 数 254 个，网关地址 [10.4.1.1](http://10.4.1.1/" \t "https://www.doubao.com/chat/_blank)，用于数据中心服务器通信；访客网络子网地址为 [10.5.1.0/24](http://10.5.1.0/24" \t "https://www.doubao.com/chat/_blank)，子网掩码 [255.255.255.0](http://255.255.255.0/" \t "https://www.doubao.com/chat/_blank)，可用 IP 数 254 个，网关地址 [10.5.1.1](http://10.5.1.1/" \t "https://www.doubao.com/chat/_blank)，用于外来访客设备接入。​

#### **3.6.3 DHCP 部署**​

在主校区网络中心部署 2 台 Windows Server 2022 服务器作为 DHCP 服务器，采用热备模式，主服务器 IP 地址为 [10.0.0.10](http://10.0.0.10/" \t "https://www.doubao.com/chat/_blank)，辅助服务器 IP 地址为 [10.0.0.11](http://10.0.0.11/" \t "https://www.doubao.com/chat/_blank)。为每个 VLAN 创建独立的作用域，如行政楼 VLAN 作用域范围为 [10.1.1.10](http://10.1.1.10/" \t "https://www.doubao.com/chat/_blank) - [10.1.1.250](http://10.1.1.250/" \t "https://www.doubao.com/chat/_blank)，教学楼 1 VLAN 作用域范围为 [10.2.1.10](http://10.2.1.10/" \t "https://www.doubao.com/chat/_blank) - [10.2.1.250](http://10.2.1.250/" \t "https://www.doubao.com/chat/_blank) 等，并配置 DNS 服务器地址为教育网 DNS（[202.112.0.35](http://202.112.0.35/" \t "https://www.doubao.com/chat/_blank)）和公网 DNS（[114.114.114.114](http://114.114.114.114/" \t "https://www.doubao.com/chat/_blank)），实现为校园网终端自动分配 IP 地址、子网掩码、网关和 DNS 等网络参数。​

### **3.7 路由设计（路由协议选择）**​

#### **3.7.1 内部路由协议**​

校园网内部路由协议采用 OSPFv2 和 OSPFv3 双协议栈。将校园网划分为多个区域，核心层为骨干区域 Area 0，各楼宇汇聚层为非骨干区域，如行政楼区域为 Area 1，教学楼区域为 Area 2 等。在核心层和汇聚层交换机上配置 OSPF 协议，设置接口优先级和 Cost 值，优化路由路径选择。​

接入层交换机采用静态路由配置，将默认路由指向汇聚层交换机，简化接入层网络配置，提高网络稳定性和安全性。​

#### **3.7.2 外部路由协议**​

校园网出口路由器与教育网和运营商路由器之间采用 BGP 协议进行路由交换。在主校区出口路由器上配置 BGP 协议，与教育网和运营商的 BGP 邻居建立连接，获取外部路由信息，并将校园网公网路由宣告给外部网络。​

同时，在出口路由器上配置 NAT 策略，实现校园网内部私有 IP 地址与公网 IP 地址的转换，使终端设备能够访问互联网，并且为数据中心服务器配置静态 NAT，实现外部网络对服务器的访问。​

### **3.8 无线网络方案设计**​

#### **3.8.1 无线网络方案涉及的技术**​

采用 Wi - Fi 6 技术，其支持 OFDMA、MU - MIMO 等关键技术，相比 Wi - Fi 5，在多用户并发效率上提升 4 倍，传输速率最高可达 9.6Gbps，能够满足校园网大量终端设备同时接入的需求。​

无线网络架构采用 AC（无线控制器）+Fit AP（瘦 AP）模式，AC 设备选用华为 AC6805，可管理多达 1024 个 AP，实现对 AP 的集中配置、管理和监控。Fit AP 选用华为 AP7060DN - HI，支持 2.4GHz 和 5GHz 双频段，每个 AP 可同时接入 128 个用户，具备出色的覆盖能力和用户承载能力。​

运用射频优化技术，通过 AC 自动调整 AP 的发射功率、信道和频宽，避免同频干扰，优化无线信号覆盖，保障无线网络的稳定性和性能。​

#### 3.8.2 无线网络方案设计​

##### [3.8.2.1](http://3.8.2.1/" \t "https://www.doubao.com/chat/_blank) 覆盖规划​

主校区教学楼采用华为 AP7060DN - HI 进行覆盖，每间教室部署 1 台，走廊每间隔 20 米部署 1 台，实现教学楼内无缝覆盖，满足师生教学、学习和移动办公的无线网络需求。​

图书馆采用高密度部署方式，每层部署 10 台 AP7060DN - HI，确保在人员密集区域提供稳定的无线网络服务，支持师生查阅资料、在线学习等业务。​

宿舍区每栋楼部署 20 台 AP7060DN - HI，在楼道和宿舍区域合理分布，保障学生在宿舍内随时随地接入无线网络，进行娱乐、学习等活动。​

分校区办公楼每间办公室部署 1 台 AP7060DN - HI，走廊每间隔 15 米部署 1 台，实现办公楼无线网络全覆盖，满足办公人员移动办公需求。​

实验室根据实验设备和人员分布情况，每间实验室部署 2 - 3 台 AP7060DN - HI，确保实验过程中设备和人员的网络接入需求。​

##### **[3.8.2.2](http://3.8.2.2/" \t "https://www.doubao.com/chat/_blank) 安全与认证**​

无线网络设置多个 SSID，如 “CUP - Edu” 用于教学科研业务，采用 WPA2 - Enterprise 认证方式，结合统一身份认证系统，实现师生使用校园网账号密码进行认证接入；“CUP - Office” 用于办公业务，同样采用 WPA2 - Enterprise 认证；“CUP - Guest” 用于访客网络，采用短信认证或临时账号密码认证方式。​

部署无线入侵防御系统（WIPS），实时监控无线网络中的非法 AP、恶意攻击等行为，一旦检测到威胁，立即采取隔离、阻断等措施，保障无线网络安全。​

### 3.9 数据中心网络方案设计​

#### 3.9.1 架构设计​

数据中心采用虚拟化平台和大模型服务器集群架构。虚拟化平台采用 VMware vSphere 7.0，将 4 台戴尔 PowerEdge R750 服务器构建为虚拟化集群，实现计算资源的池化管理和动态分配，提高资源利用率和业务连续性。​

大模型服务器集群由 3 台浪潮 NF5488A5 服务器组成，通过高速 Infiniband 网络进行互联，支持分布式训练，满足人工智能科研项目对计算资源的高需求。​

存储架构采用 SAN（存储区域网络）和 NAS（网络附加存储）相结合的方式。SAN 存储选用华为 OceanStor 5310 V5，配置 8 块 10Gbps FC 接口，提供块存储服务，用于虚拟化平台和数据库存储；NAS 存储选用群晖 RS3621RPxs，配置 12 块 10TB 硬盘，提供文件存储服务，用于科研数据共享和备份。​

#### 3.9.2 网络设计​

服务器接入网络采用双网卡绑定模式，每台服务器配置 2 块万兆网卡，通过链路聚合技术绑定为一个逻辑接口，连接到数据中心接入层交换机，实现网络冗余和带宽提升。​

管理网络采用独立的 VLAN 进行隔离，配置专门的管理 IP 地址段，用于服务器的远程管理和监控。在数据中心接入层交换机上划分管理 VLAN，并配置 ACL 策略，限制非授权设备访问管理网络，保障管理网络安全。​

备份网络采用 10Gbps 以太网，部署专门的备份服务器和备份存储设备。数据中心服务器通过备份网络将数据定期备份到备份存储设备，采用增量备份和全量备份相结合的方式，确保数据的安全性和可恢复性。​

### **3.10 云平台方案设计**​

#### 3.10.1 阿里云 Stack 架构​

阿里云 Stack 控制节点部署在 3 台华为 TaiShan 200 2280 服务器上，采用三节点集群部署方式，实现控制节点的高可用性。每台控制节点服务器配置 2 颗鲲鹏 920 处理器、256GB 内存、960GB SSD 系统盘，运行阿里云 Stack 控制平面软件，负责云平台的资源管理、调度和监控。​

计算节点部署 2 台华为 TaiShan 200 2280 服务器，每台计算节点配置 2 颗鲲鹏 920 处理器、512GB 内存、4TB SAS 数据盘，运行虚拟化软件，为云平台提供计算资源。​

存储节点部署 5 台华为 TaiShan 200 2280 服务器，每台存储节点配置 2 颗鲲鹏 920 处理器、256GB 内存、12 块 4TB SAS 硬盘，采用分布式存储技术构建存储资源池，为云平台提供弹性存储服务。​

#### 3.10.2 功能实现​

云平台提供自助服务门户，师生通过统一身份认证登录门户，可自主申请计算、存储和网络资源，如虚拟机实例、云硬盘、虚拟网络等。平台根据用户申请自动分配资源，并提供可视化的资源管理界面，方便用户查看和管理资源使用情况。​

支持资源弹性扩展功能，当用户业务量增加时，可通过自助服务门户在线申请增加计算资源（如 CPU、内存）、存储资源（如扩容云硬盘）或网络资源（如增加带宽），平台自动进行资源分配和调整，满足业务需求。​

部署监控与告警系统，实时监控云平台的各项指标，包括服务器性能、资源利用率、网络流量等。当指标超过阈值时，系统自动发送告警信息（如邮件、短信）通知管理员，以便及时处理问题，保障云平台稳定运行。​

提供数据备份与恢复功能，采用定时备份和实时备份相结合的方式，将用户数据备份到本地存储设备和异地容灾中心。当数据丢失或损坏时，用户可通过自助服务门户申请数据恢复，平台根据备份策略快速恢复数据，保障数据安全。​

### **3.11 网络安全性设计**​

#### **3.11.1 统一身份认证设计方案**​

统一身份认证系统采用基于 LDAP（轻量级目录访问协议）的认证机制，将校园网内所有业务系统的用户信息集中存储在 LDAP 目录服务器中。师生使用统一的校园网账号密码进行认证，实现单点登录（SSO），即用户只需登录一次，即可访问所有集成统一身份认证系统的业务系统，无需重复输入账号密码。​

系统支持多因子认证方式，除了传统的账号密码认证外，还可结合短信验证码、动态令牌、生物识别（如指纹、人脸识别）等方式，进一步提高用户身份认证的安全性。同时，通过权限管理机制，根据用户角色和部门分配不同的资源访问权限，确保用户只能访问其有权限的资源。​

#### 3.11.2 网络安全系统设计方案

在边界防护体系中，部署两台华为 USG6680E - 16 防火墙组成双机热备架构，作为校园网与外部网络的安全屏障。防火墙通过精细化的访问控制策略，依据源 IP、目的 IP、端口号、协议类型等条件，对进出校园网的流量进行严格过滤，阻止非法访问请求进入校园网络。同时，启用防火墙内置的入侵防御（IPS）功能，实时监测并阻断如 DDoS 攻击、端口扫描等常见网络攻击行为；病毒防护模块可识别并查杀各类恶意软件，防止病毒在校园网内传播扩散；应用控制功能则能够对校园网内的应用流量进行管控，限制非必要应用占用网络资源，保障关键业务的网络带宽。

于数据中心服务器区前端部署启明星辰 WAF - 6000 - T32 Web 应用防火墙，针对 Web 应用系统面临的安全威胁进行专项防护。该防火墙通过深度包检测技术，对 HTTP/HTTPS 流量进行逐包分析，精准识别并拦截 SQL 注入攻击，防止攻击者通过构造恶意 SQL 语句获取或篡改数据库信息；抵御跨站脚本（XSS）攻击，避免攻击者利用 Web 应用漏洞注入恶意脚本，窃取用户敏感信息；防护文件包含漏洞，防止攻击者通过非法访问获取服务器敏感文件。此外，WAF 还支持自定义防护规则，可根据校园网 Web 应用系统的实际需求，灵活配置防护策略，进一步提升 Web 应用的安全性。

入侵检测与响应系统采用绿盟科技 NIDS - 1000 - S200 入侵检测系统，通过旁路部署的方式，实时镜像采集校园网内各关键节点的网络流量。系统基于特征检测和行为分析技术，对采集到的流量数据进行深度解析，当检测到符合已知攻击特征的流量或异常的网络行为模式时，立即触发告警机制，以邮件、短信等方式通知网络安全管理员。同时，入侵检测系统与防火墙等安全设备进行联动，一旦确认攻击行为，可自动生成并下发访问控制规则，在防火墙侧对攻击源进行阻断，实现对网络攻击的快速响应和有效处置，将攻击造成的影响降至最低。

终端安全管理方面，部署深信服 EDR 终端检测与响应系统，覆盖校园网内所有师生办公终端、教学终端以及服务器终端。该系统通过在终端设备上安装轻量级客户端，实现对终端的全方位安全防护。终端杀毒功能可实时扫描终端设备，查杀各类病毒、木马、蠕虫等恶意软件；漏洞管理模块定期对终端系统和应用程序进行漏洞扫描，及时发现并推送补丁修复建议，降低因系统漏洞被攻击的风险；准入控制功能结合 802.1X 认证技术，对新接入校园网的终端设备进行身份验证和安全检查，只有通过安全合规检查的终端设备才能获得网络访问权限，有效防止非法设备接入校园网，保障网络内部安全。

### 3.12 人脸识别系统设计

#### 3.12.1 硬件部署

在校园各关键出入口，如主校区大门、分校区大门、教学楼主入口、宿舍楼入口等位置，部署海康威视 DS - 2CD7A47FWDV2 - ZS 高清智能人脸抓拍摄像机。该摄像机采用星光级图像传感器，具备 200 万像素高清成像能力，支持宽动态范围，即使在强光、逆光等复杂光照环境下，也能清晰捕捉人脸图像。摄像机内置 AI 芯片，可实现人脸实时检测、抓拍和特征提取，支持同时检测多个目标人脸，识别准确率高达 99% 以上。摄像机通过 POE 交换机进行供电和数据传输，减少布线复杂度，同时采用光纤作为主干传输链路，确保数据传输的稳定性和高速性，满足人脸识别系统对实时性和准确性的要求。

在网络汇聚层部署华为 S5735 - S - 48T4X - A 汇聚交换机，负责将各区域摄像机的视频数据进行汇聚，并通过万兆光纤链路传输至数据中心。数据中心部署高性能的华为 OceanStor 5310 V5 存储设备，采用 RAID 6 数据冗余技术，保障人脸图像数据的安全存储。存储设备配置足够的存储空间，按照每天 24 小时不间断录像，每路摄像机视频数据存储 30 天的标准进行规划，确保人脸图像数据可长期保存，为后续查询和分析提供支持。

#### 3.12.2 数据处理与存储

人脸识别系统的数据处理核心采用商汤科技 SenseFace 人脸识别算法平台，该平台基于深度学习技术，具备强大的人脸特征提取和比对能力。系统通过对大量人脸图像数据的训练，能够准确识别不同年龄、性别、表情、姿态下的人脸特征。在数据处理流程中，摄像机抓拍的人脸图像首先传输至算法平台，平台对图像进行预处理，包括图像增强、归一化等操作，以提高图像质量；然后提取人脸特征向量，并与预先录入的人员人脸特征库进行比对，实现身份识别。算法平台支持亿级人脸特征库的快速检索和比对，可在毫秒级时间内完成一次人脸比对操作，满足校园大规模人员身份识别的需求。

数据存储方面，采用 MySQL 数据库作为人员信息和识别记录的存储载体。数据库设计包含人员基础信息表、人脸特征信息表、识别记录信息表等核心表结构。人员基础信息表存储人员姓名、学号 / 工号、部门等基本信息；人脸特征信息表存储经过算法提取的人脸特征向量；识别记录信息表记录每次人脸识别的时间、地点、识别结果等信息。为保障数据安全，对数据库中的敏感信息，如人脸特征向量进行加密存储，采用 AES - 256 加密算法，防止数据泄露和非法访问。同时，定期对数据库进行备份，采用全量备份和增量备份相结合的方式，将备份数据存储在异地容灾中心，确保数据的完整性和可用性。

#### 3.12.3 业务集成

人脸识别系统与校园考勤管理系统进行深度集成，实现智能化考勤。在教学楼和办公楼入口处部署的人脸识别设备，可自动识别师生身份，并将识别结果实时传输至考勤管理系统。考勤管理系统根据预设的考勤规则，自动记录师生的出勤情况，生成考勤报表，极大提高了考勤管理的效率和准确性，避免了传统考勤方式中存在的代签、漏签等问题。同时，系统支持异常考勤信息实时推送功能，当出现迟到、早退、未打卡等异常情况时，自动向相关人员发送短信或邮件提醒，便于及时处理考勤异常问题。

与异常告警系统集成后，人脸识别系统可有效提升校园安全管理水平。当系统识别到黑名单人员（如校外闲杂人员、危险人员等）试图进入校园或重点区域时，立即触发异常告警机制，向安保人员的手持终端和监控中心发送告警信息，同时联动现场摄像机进行跟踪拍摄，并将实时画面推送至监控中心。安保人员可根据告警信息迅速采取措施，对异常人员进行拦截和处理，有效预防安全事件的发生。此外，系统还支持自定义告警规则，可根据不同区域的安全等级和管理需求，设置不同的告警条件，如在深夜时段对宿舍楼出入口进行重点监控，一旦识别到非本楼人员进入，立即发出告警，进一步增强校园安全防护能力。

### 3.13 大模型服务器平台部署方案

#### 3.13.1 硬件配置

大模型服务器平台由 4 台浪潮 NF5488A5 服务器组成高性能计算集群，每台服务器均配备强大的硬件配置以满足大模型训练和推理的高计算需求。服务器搭载 4 颗英特尔至强铂金 8380 处理器，该处理器采用 10 纳米工艺制造，拥有 28 个物理核心，主频高达 2.3GHz，通过多核心并行计算能力，可大幅提升数据处理速度。配备 1TB DDR4 3200MHz 内存，为模型训练过程中大规模数据的加载和处理提供充足的内存空间，确保数据读写的高效性。

在图形处理能力方面，每台服务器安装 8 块 NVIDIA A100 GPU 加速卡，A100 采用先进的安培架构，拥有高达 80GB 的 HBM2e 显存，显存带宽达 2039GB/s，单精度计算性能可达 19.5 TFLOPS，双精度计算性能为 9.7 TFLOPS，强大的计算能力能够加速深度学习模型的训练和推理过程，显著缩短训练时间。存储系统配置 8 块 3.84TB NVMe SSD 硬盘，NVMe 协议的固态硬盘具备极高的读写速度，顺序读取速度可达 7000MB/s 以上，顺序写入速度可达 5000MB/s 以上，满足大模型训练过程中大量数据的快速存储和读取需求。

## 第 4 章 网络预算

### 4.1 网络设备、服务器和软件系统清单及预算

#### 4.1.1 设备与软件预算总表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类别 | 设备 / 软件名称 | 型号 / 规格 | 数量 | 单价（万元） | 总价（万元） | 备注 |
| 核心网络设备 | 华为 S12700E-24X 万兆核心交换机 | 交换容量 23.04Tbps，48×10GE 光口 + 6×40GE 光口，CSS2 堆叠，含冗余电源、光模块 | 2 台 | 25 | 50 | 主校区核心层双机冗余，具备卓越的交换性能，满足未来长时间内校园网核心层高速数据转发需求，其 CSS2 堆叠技术极大增强了设备的可靠性和稳定性 |
|  | 新华三 S5130-52S-HI 万兆汇聚交换机 | 48×GE 电口 + 4×10GE 光口，IRF2 堆叠，支持 PoE+ | 6 台 | 8 | 48 | 主校区教学楼 / 实验楼 / 行政楼汇聚，IRF2 堆叠技术实现设备冗余，PoE + 功能方便为各类终端设备供电，满足主校区各楼宇汇聚层的复杂需求 |
|  | Cisco Catalyst 9300L 汇聚交换机 | 24×GE 电口 + 4×10GE 光口，支持 SD-Access，PoE + 供电 | 2 台 | 7 | 14 | 分校区行政楼汇聚层，SD-Access 技术提升网络的智能化管理水平，PoE + 供电为分校区相关设备提供便利的电力和数据接入 |
|  | 华为 S5735-L24P4S-A 千兆 PoE 交换机 | 24×GE PoE + 电口，单端口供电 30W，支持 802.1X 认证 | 32 台 | 1.2 | 38.4 | 主校区教室 / 实验室接入层，为教室信息点和无线 AP 提供稳定的电力和网络接入，802.1X 认证增强了网络接入的安全性 |
|  | 新华三 S5024PV3-EI 千兆 PoE 交换机 | 24×GE PoE + 电口，分校区教学楼接入层 | 20 台 | 0.8 | 16 | 分校区教室 / 无线 AP 接入，满足分校区教学楼大量信息点和无线 AP 的接入需求，保障分校区教学区域网络的正常运行 |
| 出口与互联设备 | 华为 AR6320 万兆出口路由器 | 转发速率 10Gbps，支持 BGP/MPLS VPN，含 IPsec VPN license（1000 隧道数） | 2 台 | 15 | 30 | 教育网 / 联通网双出口，具备强大的路由功能和 VPN 支持能力，实现校园网与外部网络的高速、安全互联 |
|  | 深信服 M5400 VPN 网关 | 支持 IPsec/SSL VPN，用户数授权 5000+，分校区冗余互联 | 1 台 | 12 | 12 | 分校区通过 VPN 接入主校区，提供安全可靠的分校区与主校区连接通道，满足分校区师生对主校区资源的访问需求 |
| 服务器与存储 | 戴尔 PowerEdge R750 虚拟化服务器 | 2×Intel Xeon Platinum 8368，256GB DDR4，2×1.92TB SSD，双万兆网卡 | 8 台 | 8 | 64 | 数据中心虚拟化集群（含 HA 功能），为数据中心提供强大的虚拟化计算能力，HA 功能保障业务的连续性和稳定性 |
|  | 浪潮 NF5468M5 大模型服务器 | 2×Intel Xeon Gold 6348，512GB DDR4，8×NVIDIA A100 GPU，4×40GE 光口 | 2 台 | 40 | 80 | 人工智能模型训练，含 GPU 加速卡，具备强大的计算能力，满足人工智能科研领域对高性能计算的严苛需求 |
|  | 华为 TaiShan 200 云平台服务器 | 2× 鲲鹏 920 64 核，256GB DDR4，12×4TB SATA 硬盘，支持 OpenStack 集群 | 6 台 | 6 | 36 | 阿里云 Stack 私有云控制节点 + 计算节点，为私有云平台提供稳定的计算资源和控制能力，基于鲲鹏处理器的高性能和低功耗特性，保障云平台的高效运行 |
|  | 华为 OceanStor 5310 SAN 存储 | 全闪存阵列，配置 10×1.92TB SSD，支持 RAID 10，双控制器冗余 | 1 台 | 28 | 28 | 数据中心块存储，支持虚拟化平台，全闪存阵列提供极高的读写性能，RAID 10 和双控制器冗余确保数据的安全性和存储系统的可靠性 |
| 安全设备 | 华为 USG6680 下一代防火墙 | 吞吐量 10Gbps，支持 IPS/AV/URL 过滤，含 5 年威胁特征库升级服务 | 1 台 | 28 | 28 | 校园网出口安全防护，全面的安全防护功能和长期的威胁特征库升级服务，有效抵御各类网络攻击，保障校园网出口的安全 |
|  | 启明星辰 WAF-6000 Web 防火墙 | 吞吐量 2Gbps，支持 HTTP/HTTPS 深度防护，含 3 年攻击规则库更新 | 1 台 | 15 | 15 | Web 应用层安全防护（如教务系统），针对 Web 应用层攻击提供深度防护，3 年的攻击规则库更新确保对不断变化的 Web 攻击手段保持有效防护 |
|  | 绿盟 NIDS-1000 入侵检测系统 | 检测速率 10Gbps，支持 2000 + 协议解析，含日志存储 10TB | 1 台 | 18 | 18 | 核心层流量实时监控，高速的检测速率和广泛的协议解析能力，能够及时发现网络中的入侵行为，并通过 10TB 的日志存储进行安全事件的追溯和分析 |
| 无线覆盖设备 | 华为 AP7060DN Wi-Fi 6 双频 AP | 2.4GHz/5GHz 双频段，2×2 MIMO，支持 OFDMA，含 PoE 供电模块 | 120 台 | 0.3 | 36 | 主校区 + 分校区室内全覆盖，Wi-Fi 6 技术提供高速、稳定的无线网络连接，双频段和 OFDMA 技术适应不同场景和多用户并发需求，PoE 供电模块简化安装布线 |
|  | 华为 iMaster NCE-Campus 无线控制器 | 支持管理 2000 + 瘦 AP，含 AC 管理软件授权，主校区集中部署 | 1 台 | 10 | 10 | 无线 AP 集中配置与优化，强大的管理能力实现对大量瘦 AP 的集中配置和智能射频优化，保障校园无线网络的高效运行和用户体验 |
| 软件系统 | 阿里云 Stack 基础版 | 含 OpenStack 云平台、容器服务、对象存储，5 年授权费 + 技术支持 | 1 套 | 50 | 50 | 私有云平台搭建，全面的云服务功能和长期的技术支持，满足学校教学、科研和管理对云平台的多样化需求 |
|  | VMware vSphere 8.0 虚拟化套件 | 含 8 节点企业版 License，支持 HA/DRS/FT 功能 | 1 套 | 25 | 25 | 服务器虚拟化授权，提供强大的服务器虚拟化功能，HA/DRS/FT 等功能保障虚拟化环境下业务的高可用性、资源优化和容错能力 |
|  | 奇安信天珣终端安全管理系统 | 20000 点授权，含病毒查杀 / 补丁管理 / 外设管控，3 年升级服务 | 1 套 | 12 | 12 | 师生终端安全防护，全面的终端安全防护功能和 3 年的升级服务，有效保护师生终端设备免受病毒、恶意软件的侵害，规范外设使用 |
| 综合布线 | 六类非屏蔽双绞线 + 单模光纤 | 主校区 + 分校区楼宇布线，含 200 箱六类线（每箱 305 米）、50 公里单模光纤 | 1 批 | 20 | 20 | 含桥架、面板、水晶头等辅材，满足校园网千兆到桌面和万兆骨干传输的布线需求，高质量的线缆和完善的辅材确保网络布线的稳定性和可靠性 |
| 其他配件 | 光模块 / 机柜 / 理线架等 | 10GE SFP + 光模块（200 个）、42U 标准机柜（15 个）、理线架 / PDU 等 | 1 批 | 10 | 10 | 设备安装与线缆管理，充足的光模块满足网络设备之间的高速连接，标准机柜和理线架等配件保障设备安装的规范性和线缆管理的有序性 |
| 合计 | — | — | — | — | 490.4 | — |