# 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**

## 第 1 章 网络需求分析

### 1.1 项目背景

随着教育信息化进程的不断深入，中国石油大学（北京）在教学、科研和管理等方面对校园网络的依赖程度日益加深。当前，学校拥有主校区和分校区两个办公区域，传统的网络架构在面对业务多元化、用户规模扩大以及应用场景复杂化等挑战时，逐渐显露出诸多不足。

从网络架构来看，主校区和分校区目前通过 VPN 方式连接成一个局域网。然而，这种连接方式在网络性能方面存在瓶颈，例如数据传输速率受限，无法满足大量数据实时交互的需求；在安全性方面，传统 VPN 的加密和认证机制相对单一，面临着日益严峻的网络攻击威胁；在扩展性方面，难以快速适应新业务和新设备的接入需求，导致网络资源调配不够灵活。

在基础设施层面，主校区包含 2 幢 8 层教学楼、1 幢 6 层实验楼、1 幢 10 层行政楼。分校区则有 2 幢 8 层教学楼、1 幢 5 层实验楼和 1 幢 6 层行政大楼。各楼宇的功能定位不同，使得信息点分布差异显著。主校区实验楼每个实验室需布设 30 个信息点，这些信息点主要用于连接科研设备、计算机等，对网络的稳定性和带宽要求极高；行政楼机房作为核心数据处理区域，需 100 个信息点，以满足大量服务器和网络设备的接入需求；分校区计算机中心信息点达 300 个，主要服务于学生的实践教学和高性能计算任务，高密度的信息点对网络的接入能力和布线系统提出了更高要求，需要确保每个信息点都能稳定、高速地接入网络。

在网络应用方面，学校需要支持学校网站、本科教务管理系统、研究生系统等十余种应用系统。所有服务器集中部署于行政楼网络中心的数据中心，随着大模型服务器部署、私有云平台搭建以及人脸识别系统覆盖等新需求的提出，数据中心的负荷不断增加。大模型服务器在进行人工智能模型训练和推理时，需要大量的计算资源和高速的数据传输；私有云平台要为全校 2 万师生提供 100GB 存储空间的云网盘服务，支持文件共享、协作编辑等功能，对存储容量和访问速度要求极高；人脸识别系统需覆盖各楼宇出入口，实现人员身份识别和考勤管理，这就要求网络能够实时传输和处理大量的图像数据。

为了应对上述挑战，本网络方案设计致力于构建一个安全可靠、稳定高效的系统集成平台。通过优化网络架构，引入先进的技术和设备，提升校园网的性能、安全性和可管理性，为学校的长远发展提供坚实的网络基础支撑，确保教学、科研和管理等各项工作的顺利开展。

### 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需要高速、稳定的链路作为支撑。主校区现有两根光纤分别接入教育网和联通网，分校区通过 VPN 与主校区连接。考虑到未来业务的持续增长，网络带宽需求将不断增加，因此需要确保核心层与汇聚层之间采用万兆连接，以实现高速的数据传输和交换；汇聚层与接入层千兆连接，满足汇聚层对各接入层设备的流量汇聚和转发需求；桌面终端支持 10/100 兆接入，适应不同终端设备的接入速率要求，从而构建一个层次分明、带宽适配的网络架构，满足不同场景下的带宽需求。

主校区行政楼网络中心作为核心节点，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。它不仅需要通过光纤实现与教育网、公网的高速连接，获取外部资源和服务，还需要与分校区建立稳定的连接，实现两校区之间的数据共享和业务协同。分校区网络机房作为汇聚节点，负责将各楼宇的网络流量汇聚后，通过 VPN 链路传输至主校区，确保分校区的业务能够顺利接入校园网整体架构。

#### 1.2.2 无线覆盖需求

随着移动办公、在线教学和物联网设备接入等场景的普及，两校区所有教学和办公场所实现无线网络全覆盖成为必然需求。无线局域网需要具备高可靠性，确保在长时间运行中不会出现频繁的中断或故障；高并发能力，能够支持大量用户同时接入和使用，避免出现网络拥堵；无缝漫游特性，使用户在不同区域移动时能够自动切换接入点，保持网络连接的连续性；自动负载均衡功能，将用户流量合理分配到各个接入点，避免热点区域拥堵。

同时，支持 802.11ac/a/n 等主流无线协议，提供 2.4GHz 和 5GHz 双频段覆盖，能够满足不同终端设备的接入需求。2.4GHz 频段覆盖范围广，适合对传输速率要求不高的设备接入；5GHz 频段传输速率快，适合对带宽要求较高的设备，如高清视频传输、大文件下载等，从而为师生提供更加便捷、高效的无线接入服务。

#### 1.2.3 服务器与存储需求

数据中心作为校园网的核心数据处理和存储区域，部署虚拟化架构具有重要意义。通过整合学校网站、教务系统等服务器资源，能够提高硬件利用率，减少硬件设备的重复购置和闲置，降低成本；同时，提升系统可靠性，当某台物理服务器出现故障时，虚拟机能快速迁移到其他服务器上运行，确保业务不中断。

大模型服务器如 Deepseek 服务器，在人工智能、大数据分析等科研任务中发挥着关键作用。它需要具备强大的计算能力和存储资源，支持 GPU 加速和分布式计算，以满足复杂模型训练和大规模数据处理的需求。GPU 加速能够显著提高计算效率，分布式计算则可以将任务分配到多个计算节点上并行处理，缩短任务完成时间。

私有云平台为全校师生提供 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。采用主流技术路线构建云平台，能够确保其开放性和成熟可靠性，方便与其他系统进行集成和交互；同时，具备良好的扩展性，可根据业务需求动态扩展计算和存储资源，满足不断增长的数据存储和处理需求。

#### 1.2.4 网络安全需求

构建统一的安全防护体系是保障校园网安全稳定运行的关键。该体系包括防火墙、Web 防火墙、入侵检测系统、安全审计系统等。防火墙部署于网络边界，基于 IP 地址、端口、协议等规则过滤流量，阻止未经授权的访问，保护校园网内部资源免受外部攻击；Web 防火墙针对 Web 应用层攻击，如 SQL 注入、XSS 跨站脚本攻击等，对 HTTP/HTTPS 流量进行深度检测和防护，保护学校网站、教务系统等 Web 应用的安全；入侵检测系统实时监控网络流量，检测潜在的入侵行为，并发送告警信息，以便及时采取应对措施；安全审计系统对网络中的安全事件进行记录和分析，为安全管理提供依据。

统一身份认证系统支持多因子认证，如用户名 + 密码 + 短信验证码、硬件令牌或生物识别等，确保用户身份的真实性和访问权限的合理性，防止非法用户接入和访问敏感资源。安全态势感知系统对全网安全事件进行集中管理和分析，提供预警和应急响应支持，能够实时掌握网络安全状况，及时发现和处理安全隐患。

### 1.3 网络应用需求

#### 1.3.1 教学科研应用

教学科研应用是校园网的重要服务对象，需要支持在线教学平台、虚拟实验室、科研数据共享等应用。在线教学平台需要稳定的网络环境来支持视频会议、直播授课等实时业务，确保教学过程的流畅进行；虚拟实验室为学生提供了远程进行实验操作的平台，需要网络能够实时传输实验数据和控制指令；科研数据共享平台则需要高速的网络传输和安全的数据存储，方便科研人员之间的数据交流和协作。

大模型服务器为人工智能、机器学习等科研方向提供算力支持，支持模型训练、推理和部署等全流程操作。在模型训练过程中，需要处理大量的数据，对网络的带宽和稳定性要求极高；推理和部署阶段，需要快速响应用户请求，确保模型的高效运行。

#### 1.3.2 办公管理应用

办公管理应用包括办公自动化（OA）系统、一卡通系统、财务管理系统等核心业务系统。这些系统的稳定运行依赖于可靠的网络环境，确保数据传输的安全性和完整性。OA 系统用于日常办公事务的处理，如文件流转、审批等，需要网络能够及时传输和处理数据；一卡通系统涉及师生的日常生活消费和身份认证，数据的安全性和实时性至关重要；财务管理系统处理学校的财务数据，对数据的保密性和准确性要求极高。

统一身份认证系统与各业务系统无缝对接，实现单点登录，用户只需一次登录即可访问多个业务系统，提高办公效率，减少重复登录的繁琐过程。

#### 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，方便他们存储和共享教学资料、科研数据。师生可以在不同设备上随时访问和管理自己的文件，提高工作和学习效率。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，提升校园安全管理水平。通过人脸识别技术，能够准确识别人员身份，有效防止无关人员进入校园重要区域，同时自动记录人员的进出时间，为考勤管理提供便捷、准确的手段。

#### 1.3.4 未来扩展需求

网络架构需要具备良好的扩展性，以适应未来 5-10 年的业务发展需求。支持 IPv6、SDN（软件定义网络）、算力网络等新技术的平滑升级，能够确保校园网在技术不断发展的过程中保持先进性和竞争力。IPv6 解决了 IPv4 地址资源枯竭的问题，为物联网设备的大规模接入提供了可能；SDN 实现了网络的集中控制和灵活管理，提高了网络资源的调配效率；算力网络整合了网络、计算和存储资源，为人工智能、大数据分析等领域提供了强大的支持。

同时，考虑物联网设备如智能教室设备、环境监测传感器等的接入需求，构建融合化、智能化的校园网络生态。物联网设备的接入将实现校园环境的智能化管理，如智能教室的设备控制、校园环境的实时监测等，提升校园的智能化水平。

## 第 2 章 网络技术调研

### 2.1 网络互连技术

网络互连技术是实现不同网络设备、子网及网络之间通信的核心技术，其目标是确保数据在复杂网络环境中准确、高效地传输。在校园网场景中，主要涉及局域网互连、广域网互连及 VPN 技术。

#### 2.1.1 局域网互连技术

局域网（LAN）互连通常采用以太网技术，基于 IEEE 802.3 标准，支持双绞线、光纤等传输介质。以太网技术具有成熟稳定、易于扩展、成本较低等优点，是校园网局域网互连的理想选择。

校园网中核心层、汇聚层和接入层设备通过以太网交换机实现互连，采用分层架构设计，如核心层 - 汇聚层 - 接入层三层架构。通过 VLAN 划分隔离广播域，将一个较大的局域网划分为多个较小的虚拟局域网，减少广播流量的影响，提高网络性能和安全性。例如，主校区实验楼各实验室的信息点通过接入层交换机连接，再通过汇聚层交换机上联至核心层，实现楼宇内及跨楼宇的局域网通信。接入层交换机负责连接终端设备，汇聚层交换机收敛接入层的流量，核心层交换机实现高速数据转发和跨区域通信。

#### 2.1.2 广域网互连技术

广域网（WAN）互连用于连接主校区与分校区、校园网与外部网络如教育网、公网。常见技术包括光纤传输、MPLS VPN（多协议标签交换虚拟专用网络）和 SD-WAN（软件定义广域网）。

本方案中，主校区通过两根光纤分别接入教育网和联通网，分校区通过 VPN 设备与主校区连接，采用 IPsec VPN 技术实现安全的数据传输。光纤传输具有高速、稳定、抗干扰能力强等优点，是广域网互连的主要传输介质。IPsec VPN 技术工作在网络层，提供数据加密、完整性校验和访问控制，确保数据在广域网上传输的安全性。

未来可考虑引入 SD-WAN 技术，通过智能路由和流量优化提升广域网链路利用率和可靠性。SD-WAN 技术能够根据网络流量、链路质量等因素动态选择最佳的传输路径，实现流量的智能分配，提高广域网的传输效率和稳定性。

#### 2.1.3 VPN 技术

VPN 技术通过加密隧道在公共网络上构建专用通信链路，适用于分校区与主校区的互连。IPsec VPN 是目前最常用的 VPN 技术之一，它在网络层对数据进行加密和封装，为不同网络之间的通信提供安全保障。

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。通过 VPN 隧道，两校区之间的业务如统一身份认证、数据共享等能够正常运行，确保跨校区的网络通信安全可靠。

### 2.2 网络接入技术

网络接入技术负责将终端设备如 PC、手机、服务器连接到网络，分为有线接入和无线接入两类。

#### 2.2.1 有线接入技术

* **以太网接入**：采用 RJ45 接口和双绞线如超五类、六类线，支持 10/100/1000Mbps 速率，是校园网有线接入的主要方式。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，确保高速的数据传输；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，为大量数据的高速传输提供保障。
* **PoE 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，简化布线结构。例如，主校区教学楼的无线 AP 可通过 PoE 交换机供电，无需单独部署电源线，提高施工效率和美观度，同时便于设备的集中管理和维护。

#### 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，Wi-Fi 6 支持更高的传输速率，理论峰值 9.6Gbps、更大的并发连接数和更低的延迟，适用于高密度场景如教室、图书馆。主校区和分校区的无线覆盖均采用 Wi-Fi 6 技术，部署双频 2.4GHz/5GHz 无线 AP，支持 OFDMA 和 MU-MIMO 技术，提升多用户场景下的性能。OFDMA 技术将信道划分为多个子信道，同时为多个用户传输数据，提高频谱利用率；MU-MIMO 技术支持多个用户同时进行数据传输，提升系统容量。
* **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，实现无线信号的自动调优、用户漫游切换和安全策略统一配置。例如，主校区网络中心部署无线控制器，各楼宇内的瘦 AP 通过隧道协议与控制器通信，确保全校无线服务的一致性和可管理性。无线控制器可以实时监控无线 AP 的状态，自动调整信道和发射功率，避免干扰，提高无线覆盖质量。

### 2.3 网络安全技术

网络安全技术是保障校园网数据安全和业务连续性的关键，涉及边界防护、入侵检测、数据加密和身份认证等领域。

#### 2.3.1 边界防护技术

* **防火墙**：部署于网络边界如校园网与教育网、公网连接处，基于 IP 地址、端口、协议等规则过滤流量，阻止未经授权的访问。主校区出口部署下一代防火墙（NGFW），支持应用层流量识别和深度包检测（DPI），可精准识别并控制 P2P 下载、视频流媒体等非业务流量，保障关键应用带宽。下一代防火墙不仅具备传统防火墙的功能，还能对应用层流量进行深入分析，识别各种应用程序，从而实现更精细的访问控制。
* **Web 防火墙（WAF）**：针对 Web 应用层攻击如 SQL 注入、XSS 跨站脚本攻击，部署 Web 防火墙，对 HTTP/HTTPS 流量进行深度检测和防护，保护学校网站、教务系统等 Web 应用免受攻击。Web 防火墙通过分析 HTTP 请求和响应，检测和阻止恶意攻击代码，确保 Web 应用的安全运行。

#### 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，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。IDS 能够实时分析网络流量，发现异常行为并发出警报，为网络安全管理人员提供及时的预警。
* **入侵防御系统（IPS）**：与 IDS 相比，IPS 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）。IPS 通过在线部署，在检测到攻击时立即采取阻断措施，防止攻击行为对网络造成损害。

#### 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可启用 HTTPS 协议，防止数据被窃取或篡改。SSL/TLS 协议在传输层对数据进行加密，保障数据在网络传输过程中的机密性和完整性。
* **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。存储加密技术对存储在设备上的数据进行加密处理，即使设备丢失或被盗，数据也难以被破解和窃取。

#### 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。多因子认证增加了身份认证的安全性，避免因单一密码泄露导致的安全问题；LDAP 目录服务实现了用户信息的集中存储和管理，方便用户账号的创建、修改和删除。

### 2.4 数据中心

数据中心是校园网核心业务系统的载体，负责存储和处理学校的关键数据。本项目数据中心位于主校区行政楼网络中心，需满足高可靠性、可扩展性和能效管理要求。

#### 2.4.1 架构设计

采用虚拟化架构，通过 VMware vSphere 或开源的 KVM 虚拟化平台，将物理服务器资源抽象为虚拟服务器（VM），实现计算资源的动态分配和高可用性（HA）。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。通过虚拟化技术，提高了服务器资源的利用率，减少了硬件设备的数量，降低了数据中心的运营成本。

#### 2.4.2 存储系统

* **SAN 存储**：采用光纤通道（FC）或 iSCSI 协议的存储区域网络（SAN），为虚拟化平台提供集中式存储。主校区数据中心可部署全闪存阵列（AFA），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。全闪存阵列具有高速的数据访问能力，能够满足大模型训练等对存储性能要求极高的应用场景。
* **NAS 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。集群 NAS 架构具有高可用性和可扩展性，能够根据用户数量和数据量的增长动态扩展存储资源。

#### 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 / 万兆接口。部署虚拟局域网（VLAN）和访问控制列表（ACL），隔离不同业务系统的流量，如将服务器划分为 Web 服务器 VLAN、数据库服务器 VLAN 等，提高安全性。通过合理的网络设计，确保数据中心内部数据的高效传输和安全隔离。

### 2.5 云平台

#### 2.5.1 云平台选型

根据指导书要求，私有云平台选用阿里云建设，采用阿里云 Stack 解决方案，支持本地化部署和与公有云的混合云架构。阿里云 Stack 基于 OpenStack 开源技术构建，具备成熟的生态体系和丰富的功能模块，可满足学校教学、科研和管理的 IT 资源需求。阿里云在云计算领域具有丰富的经验和技术积累，其 Stack 解决方案能够提供稳定、可靠的云服务。

#### 2.5.2 架构特点

* **计算资源池**：通过虚拟化技术整合物理服务器，形成弹性计算资源池，支持虚拟机快速创建、销毁和配置调整。用户可以根据自己的需求动态申请和释放计算资源，提高资源的利用效率。
* **存储资源池**：整合 SAN 和 NAS 存储，提供块存储、对象存储和文件存储服务，支持数据备份和容灾恢复。存储资源池能够统一管理不同类型的存储设备，为用户提供多样化的存储解决方案。
* **网络资源池**：通过软件定义网络（SDN）技术实现虚拟网络的灵活配置，支持 VPC（虚拟私有云）、负载均衡和 VPN 等功能。网络资源池可以根据用户的需求快速构建虚拟网络，实现网络资源的灵活调配。
* **管理平台**：提供统一的管理界面，实现资源监控、用户管理、计费统计和自动化运维，降低管理复杂度。管理平台使管理员能够方便地管理云平台的各项资源，提高运维效率。

#### 2.5.3 搭建方案

1. **基础设施部署**：在主校区网络中心部署阿里云 Stack 物理服务器、存储设备和网络设备，采用冗余电源和散热设计，确保高可用性。基础设施的稳定运行是云平台正常工作的基础，冗余设计能够提高系统的可靠性。
2. **软件平台安装**：安装阿里云 Stack 控制节点、计算节点和存储节点软件，配置集群管理和资源调度策略。合理的软件配置能够充分发挥云平台的性能，实现资源的高效调度。
3. **服务集成**：将学校现有业务系统迁移至云平台，如教务系统、OA 系统等，通过 API 接口实现与统一身份认证系统的对接。服务集成能够实现业务系统的集中管理和统一访问，提高工作效率。
4. **容灾备份**：建立异地容灾中心，可利用分校区资源，通过数据复制技术实现关键数据的实时备份，确保业务连续性。容灾备份是保障云平台数据安全和业务稳定的重要措施。

### 2.6 主流路由器性能指标

|  |  |  |  |
| --- | --- | --- | --- |
| 产品系列 | 规格 | 性能指标 | 适用场景 |
| 华为 AR6000 系列 | 千兆模块化路由器 | - 转发速率：10Gbps- 接口类型：GE 电口 / 光口、SFP+、USB、Console- 支持 IPsec VPN、MPLS VPN- 内置防火墙、QoS 功能 | 校园网出口、广域网互连 |
| Cisco4000 系列 | 万兆集成多业务路由器 | - 转发速率：20Gbps- 接口类型：10GE 光口、USB3.0、SD 卡插槽- 支持 SD-WAN、应用层检测- 提供高密度 VPN 隧道处理能力 | 核心层出口、大型网络汇聚 |
| 新华三 ER8300G2 | 千兆企业级路由器 | - 转发速率：5Gbps- 接口类型：4 个 GE 电口（其中 2 个 Combo 口）- 支持负载均衡、策略路由- 内置入侵防御、防病毒功能 | 中小型网络出口、分校区接入 |

### 2.7 主流交换机性能指标

|  |  |  |  |
| --- | --- | --- | --- |
| 产品系列 | 规格 | 性能指标 | 适用场景 |
| 华为 S12700 系列 | 万兆核心交换机 | - 交换容量：1.44Tbps~23.04Tbps- 接口密度：48×10GE 光口 + 6×40GE 光口- 支持堆叠技术（CSS2）、BGP/OSPF 路由协议- 硬件支持 ACL、QoS 和组播协议 | 校园网核心层 |
| Cisco Catalyst9300 | 千兆 / 万兆接入交换机 | - 交换容量：400Gbps~1.2Tbps- 接口类型：24×GE 电口 + 4×10GE 光口- 支持 PoE+（802.3at），单端口供电 30W- 支持 DNA Center 智能管理 | 接入层、汇聚层 |
| 新华三 S5130 系列 | 千兆智能汇聚交换机 | - 交换容量：256Gbps~512Gbps- 接口类型：48×GE 电口 + 4×10GE 光口- 支持 IRF2 智能堆叠、RSTP/MSTP 生成树协议- 提供基于端口的 VLAN 和 QinQ 功能 | 汇聚层、中小型网络核心 |

### 2.8 主要网络安全产品性能指标

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 产品类型 | 产品系列 | 规格 | 性能指标 | 适用场景 |
| 防火墙 | 华为 USG6000 系列 | 万兆下一代防火墙 | - 吞吐量：10Gbps- 并发连接数：200 万- 支持 IPS、AV、URL 过滤等安全服务- 提供 VPN 隧道数：5000+ | 校园网出口、数据中心边界 |
| Web 防火墙 | 启明星辰 WAF 系列 | 千兆应用层防火墙 | - 吞吐量：2Gbps- 支持 HTTP/HTTPS 协议深度检测- 防护规则数：1000+- 提供 SQL 注入、XSS 攻击防御 | Web 应用防护 |
| 入侵检测系统 | 绿盟 NIDS 系列 | 万兆分布式 IDS | - 检测速率：10Gbps- 支持协议解析：2000+- 实时威胁告警：邮件、SNMP Trap- 日志存储容量：TB 级 | 核心层流量监控、数据中心安全 |
| 安全审计系统 | 奇安信天巡系列 | 千兆日志审计系统 | - 日志收集速率：10 万条 / 秒- 支持多种日志格式（syslog、SNMP、JSON）- 提供报表生成和合规性检查 | 全网安全事件审计 |

### 2.9 最新网络技术

#### 2.9.1 SDN（软件定义网络）

SDN 通过将网络控制平面与数据平面分离，实现网络流量的集中控制和动态调度。在校园网中，可通过 SDN 控制器如 ONOS、OpenDaylight 统一管理交换机、路由器等设备，实现 VLAN 自动配置、链路负载均衡和故障快速切换。例如，当核心层某条链路故障时，SDN 控制器可实时调整路由策略，将流量切换至备用链路，提高网络可靠性。SDN 技术使网络管理更加灵活高效，能够快速响应业务需求的变化。

#### 2.9.2 IPv6

随着 IPv4 地址资源的枯竭，IPv6（Internet Protocol Version6）成为下一代互联网的核心技术。IPv6 采用 128 位地址空间，可提供约 3.4×10³⁸个地址，满足物联网设备大规模接入需求。校园网需逐步部署 IPv6，支持双栈 IPv4/IPv6 技术，确保新旧系统兼容。主校区和分校区的核心设备、服务器均需支持 IPv6 协议，同时配置 DNS64/NAT64 等转换技术，实现 IPv6 网络与 IPv4 网络的互通。IPv6 的部署将为校园网的未来发展提供充足的地址空间，支持更多的智能设备接入。

#### 2.9.3 确定性网络

确定性网络旨在为工业控制、实时通信等场景提供可预测的低延迟、高可靠性网络服务。通过时间敏感网络（TSN，IEEE802.1Qcc）和软件定义网络（SDN）的结合，实现流量的精确调度和资源预留。在校园网的远程实验、虚拟现实（VR）教学等场景中，确定性网络可保障实时数据的传输质量，避免因网络延迟导致的教学体验下降。确定性网络技术能够满足对网络延迟和可靠性要求极高的应用场景，提升教学和科研的效果。

#### 2.9.4 6G 网络

6G 网络作为未来通信技术的发展方向，将融合太赫兹通信、人工智能、卫星通信等技术，提供更高的传输速率，有望达到 1Tbps、更低的延迟纳秒级和更大的连接密度。虽然 6G 尚未进入商用阶段，但校园网在规划时需预留技术升级接口，如采用支持 6G 频段的无线 AP 硬件架构，为未来科研和教学应用奠定基础。提前规划 6G 网络的部署，能够使校园网在未来的技术竞争中保持领先地位。

#### 2.9.5 算力网络

算力网络通过整合网络、计算和存储资源，实现资源的统一调度和智能化分配。在校园网中，可结合私有云平台和大模型服务器，构建算力网络基础设施，为人工智能、大数据分析等科研任务提供 “按需分配” 的算力服务。例如，科研团队可通过算力网络门户申请 GPU 算力资源，系统自动调度空闲的大模型服务器资源，提高资源利用率和科研效率。算力网络技术将实现网络、计算和存储资源的深度融合，为科研工作提供更强大的支持。

#### 2.9.6 工业互联网络

在校园网场景中，工业互联网络的应用重点在于构建智能化实验室环境与设备管理体系。通过部署边缘计算网关，可将传统实验室的 PLC 控制器、传感器、智能仪表等设备接入校园网，实现设备状态实时监控（如电压 / 电流参数、设备运行时长）、远程程序下载与调试、故障预警（温度异常报警、振动频率超限）等功能。支持 OPC UA 协议的设备可直接与数据中心的工业互联网平台对接，非标准协议设备通过边缘网关进行协议转换（如 Modbus RTU 转 MQTT），确保多源异构数据的统一采集与处理。典型应用场景包括化工学院的反应釜温度压力监控系统、机械学院的数控车床加工数据采集平台，通过工业互联网络实现实验数据的实时上传与分析，为科研实验提供精准的设备状态数据支撑。

## 第 3 章 网络方案设计

### 3.1 总体架构设计

#### 3.1.1 分层架构设计

采用 "核心层 - 汇聚层 - 接入层" 三层架构，辅以独立的安全管理层与数据中心层，形成立体化网络体系：

* **核心层**：主校区行政楼网络中心部署 2 台华为 S12700 万兆核心交换机，采用集群技术（CSS2）实现逻辑单节点，提供 1.44Tbps 交换容量，负责校区间流量调度、出口链路聚合（教育网 / 联通网双链路负载均衡）及数据中心高速互联（40GE 光纤直连数据中心核心交换机）。
* **汇聚层**：主校区每栋楼宇（教学楼、实验楼、行政楼）及分校区核心机房部署新华三 S5130 千兆汇聚交换机，通过万兆光纤上联核心层，下联接入层交换机，实现楼宇内 VLAN 汇聚、QoS 策略部署（区分教学 / 科研 / 管理流量优先级）及 ACL 访问控制（限制非授权设备跨 VLAN 访问）。
* **接入层**：采用 Cisco Catalyst 9300 系列千兆 PoE 交换机，支持 802.3at 供电，为教室 AP、办公室 PC、实验室设备提供接入服务。每个信息点配置六类非屏蔽双绞线，支持千兆到桌面，实验室等高带宽需求区域预留万兆光纤接口。

#### 3.1.2 双校区互联设计

主校区与分校区通过 2 条 10Gbps 光纤链路（教育网专线 + 联通 MPLS VPN）实现互联，部署华为 AR6000 系列路由器作为出口设备，支持 IPsec VPN 加密（AES-256 算法）与流量整形。分校区网络机房配置 1 台新华三 ER8300G2 路由器作为接入节点，通过动态路由协议（OSPF）与主校区核心层同步路由信息，确保跨校区业务（如统一身份认证、云网盘访问）的低延迟传输。

#### 3.1.3 无线覆盖架构

采用 "AC+Fit AP" 集中管理模式，主校区部署 2 台华为 AC6005 无线控制器（主备冗余），分校区部署 1 台 AC6005，单控制器支持 2000+AP 管理。无线 AP 选用华为 AP7060DN（Wi-Fi 6 双频），在教学楼教室、图书馆阅览区等高密度场景按每 80㎡部署 1 台，实现 2.4GHz（覆盖）与 5GHz（高速）信号的智能切换，支持无缝漫游（漫游中断时间 < 50ms）与负载均衡（单 AP 并发用户数≤60 人）。

### 3.2 硬件设备选型方案

#### 3.2.1 核心层设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备类型 | 型号 | 数量 | 关键参数 | 功能定位 |
| 核心交换机 | 华为 S12700E-24 | 2 台 | 交换容量 23.04Tbps，48×10GE 光口 + 6×40GE 光口，支持 CSS2 堆叠 | 校区核心互联、数据中心接入 |
| 出口路由器 | 华为 AR6600-20 | 2 台 | 转发速率 10Gbps，支持双电源冗余，集成 IPS/URL 过滤功能 | 教育网 / 公网出口连接、边界防护 |

#### 3.2.2 汇聚层设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 楼宇类型 | 设备型号 | 数量 / 栋 | 关键参数 | 部署位置 |
| 主校区教学楼 | 新华三 S5130S-52S-I | 2 台 | 48×GE 电口 + 4×10GE 光口，支持 IRF2 堆叠，PoE + 供电 | 楼层弱电间 |
| 实验楼（主 / 分校区） | Cisco Catalyst 9400L | 1 台 | 24×10GE 光口 + 8×GE 电口，支持硬件 ACL 深度检测 | 机房核心机柜 |
| 行政楼（主校区数据中心） | 华为 CE12804 | 1 台 | 32×40GE 光口，支持 EVPN-VXLAN 虚拟网络，低时延转发 | 数据中心核心区 |

#### 3.2.3 接入层设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 场景类型 | 设备型号 | 数量 / 台 | 覆盖能力 | 特殊功能 |
| 普通办公室 | Cisco Catalyst 9200L-24P | 1 台 / 80㎡ | 24×GE 电口（PoE+），支持基于 MAC 的认证 | 桌面终端接入 |
| 实验室（30 信息点 / 间） | 华为 S5735-L24P4S-A | 1 台 / 实验室 | 24×GE 电口 + 4×10GE 光口，支持端口镜像（科研流量监控） | 高速设备接入 |
| 室外区域（操场 / 广场） | 华为 AP8050DN | 按需部署 | IP68 防护等级，支持定向天线，最远覆盖 300 米 | 移动终端接入 |

#### 3.2.4 安全设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备类型 | 型号 | 部署位置 | 核心功能 | 性能指标 |
| 下一代防火墙 | 华为 USG6680 | 主校区出口 | 应用层过滤、APT 攻击检测、VPN 加速 | 吞吐量 10Gbps，并发连接数 200 万 |
| Web 防火墙 | 启明星辰 WAF-6000 | 数据中心边界 | SQL 注入防护、OWASP Top10 攻击拦截 | HTTPS 吞吐量 2Gbps，防护规则数 1000+ |
| 入侵检测系统 | 绿盟 NIDS-1800 | 核心交换机旁挂 | 全流量深度检测、威胁情报联动 | 检测速率 10Gbps，支持 2000 + 协议解析 |
| 日志审计系统 | 奇安信天巡 1000 | 安全管理区 | 全网设备日志采集、合规性分析 | 日志处理速率 10 万条 / 秒，存储容量 10TB |

### 3.3 软件系统设计方案

#### 3.3.1 网络管理平台

采用华为 iMaster NCE-Campus 作为集中管理系统，实现 "全网可视化 + 自动化运维"：

* **设备管理**：支持 2000 + 台网络设备的批量配置（通过模板下发 VLAN、QoS 策略）、实时状态监控（CPU / 内存利用率阈值告警）、固件自动升级（分批次灰度升级，避免业务中断）。
* **无线管理**：AC 控制器与 iMaster 联动，自动优化 AP 信道（避开微波炉等 2.4GHz 干扰源）、调整发射功率（根据用户密度动态平衡覆盖范围），支持微信连 Wi-Fi、Portal 认证（弹出校园网登录页面）。
* **故障诊断**：通过 AI 算法分析网络日志，自动识别链路中断、设备宕机等故障，定位至具体端口并触发工单系统，平均故障恢复时间（MTTR）缩短至 30 分钟内。

#### 3.3.2 数据中心虚拟化平台

基于 VMware vSphere 8.0 构建虚拟化集群，配置 8 台戴尔 PowerEdge R750 服务器（2× 第三代 Intel Xeon 8380 处理器，512GB 内存，4×400GB SSD），实现：

* **资源动态分配**：通过 vSphere DRS（分布式资源调度），根据 CPU / 内存利用率自动迁移虚拟机，确保物理服务器利用率维持在 60%-80%。
* **高可用性**：启用 vSphere HA（主机故障切换），虚拟机重启时间 < 2 分钟；配置 vSphere FT（容错）功能，对数据库服务器等关键业务提供零停机保护。
* **存储整合**：接入华为 OceanStor 5310 V5 全闪存阵列（100TB 可用容量，随机读写 IOPS 150 万），通过 VMFS 7 文件系统实现存储资源池化，支持虚拟机快照（每 15 分钟自动备份关键数据）。

#### 3.3.3 私有云平台部署

采用阿里云 Stack 3.0 本地化部署，构建 "一云多池" 架构：

* **计算池**：划分教学资源池（500 台通用虚拟机，配置 2vCPU+8GB 内存，用于在线教学平台）、科研资源池（200 台 GPU 虚拟机，搭载 NVIDIA A100 显卡，支持大模型训练）、管理资源池（100 台虚拟机，运行 OA、一卡通等业务系统）。
* **存储池**：对接数据中心 SAN 存储（块存储用于数据库）与 NAS 存储（文件存储用于云网盘），提供对象存储服务（OSS）用于非结构化数据（如教学视频、科研图片），单用户默认 100GB 存储空间，支持配额管理与文件版本回溯（保留最近 10 个版本）。
* **服务集成**：通过统一身份认证系统（基于 CAS 6.4）实现单点登录，用户通过 "校园信息门户" 一键访问云平台资源；开放 API 接口，支持第三方系统（如研究生管理系统）快速对接。

### 3.4 网络安全方案设计

#### 3.4.1 边界防护体系

* **出口防火墙策略**：
  + 教育网链路：允许 DNS（53 端口）、HTTPS（443 端口）、SSH（22 端口）等教育科研类流量，限制 P2P 下载（如 BitTorrent 协议）、视频流媒体（如 Netflix）等高带宽非业务流量。
  + 公网链路：仅开放 Web 服务器（80/443 端口）、邮件服务器（25/110 端口）等必要服务，采用 NAT 技术隐藏内部 IP 地址，同时配置 DDoS 攻击防护（清洗阈值 10Gbps）。
* **Web 应用防护**：在数据中心前端部署启明星辰 WAF，针对教务系统、研究生系统等 Web 应用，启用 SQL 注入防护（阻断包含 "UNION SELECT" 关键词的请求）、XSS 过滤（拦截标签）、CSRF 令牌校验（强制表单提交时携带动态令牌）。

#### 3.4.2 终端安全管理

* **准入控制（NAC）**：采用 802.1X 协议对有线终端进行认证，用户需输入校园网账号密码 + 短信验证码（双因子认证），未安装杀毒软件或系统补丁过期的设备自动引导至补丁服务器修复；无线终端通过 Portal 认证，支持微信、支付宝等第三方登录方式（需绑定学号 / 工号）。
* **设备指纹**：通过 MAC 地址、操作系统版本、安装软件列表生成终端指纹，对实验室科研设备（如大模型服务器）实施严格的访问控制策略（仅允许访问数据中心存储区与科研平台，禁止访问互联网）。

#### 3.4.3 数据安全保护

* **传输加密**：所有用户登录流量（如统一身份认证）强制使用 HTTPS 协议，数据中心内部虚拟机之间通信启用 TLS 1.3 加密，数据库连接采用 SSL 证书认证（防止中间人攻击）。
* **存储加密**：云网盘文件存储时自动进行 AES-256 加密（用户密钥与系统密钥混合加密），大模型训练数据存储于加密的 SAN 卷，物理硬盘支持 TCG Opal 加密标准（设备断电后数据自动加密）。

## 第 4 章 实施计划与预算

### 4.1 项目实施阶段划分

#### 4.1.1 需求分析与设计阶段（第 1-2 个月）

* **需求确认**：完成全校各部门（教务处、科研院、网络中心）的需求调研，修订《校园网升级技术规范书》，明确各楼宇信息点数量（主校区合计 8500 点，分校区 5500 点）、无线覆盖区域图纸（标注承重墙位置、信号盲区）。
* **方案设计**：完成网络架构图（Visio 格式）、设备部署清单（Excel 表格）、布线施工图（CAD 图纸），组织校内专家评审会，重点确认数据中心迁移方案（确保业务零中断切换）与无线 AP 部署密度（实验室区域信号强度≥-65dBm）。

#### 4.1.2 设备采购与线缆敷设阶段（第 3-5 个月）

* **招标采购**：通过公开招标确定设备供应商（建议选择华为、新华三、Cisco 等主流品牌代理商），签订采购合同（含 3 年原厂维保服务），设备到货后进行通电测试（检查端口速率、PoE 供电稳定性）。
* **综合布线**：
  + 主干线缆：主校区各楼宇间采用 12 芯单模光纤（万兆兼容），沿现有弱电井敷设，每 20 米设置固定支架；分校区教学楼到机房采用 6 芯光纤，穿越道路时使用镀锌钢管保护。
  + 水平线缆：办公室、教室信息点采用六类非屏蔽双绞线（UTP），单段长度≤90 米，端接采用 T568B 标准，模块安装高度距地 30cm（符合 GB 50311 综合布线规范）。

#### 4.1.3 设备安装与系统调试阶段（第 6-7 个月）

* **硬件部署**：
  + 核心交换机上架：安装于行政楼网络中心标准 19 英寸机柜（前后通风设计，配置冗余空调，室温控制 22±2℃），光纤连接采用标签管理（标注 "核心 - 实验楼汇聚 - 1" 等信息）。
  + 无线 AP 安装：教学楼走廊采用吸顶式安装（天线向下 45° 倾斜），实验室天花板内采用壁挂式（避开消防喷头），确保信号覆盖无死角。
* **系统配置**：
  + 网络设备：通过 iMaster NCE-Campus 批量下发配置模板，完成 VLAN 划分（教学 VLAN 100-200，科研 VLAN 300-400）、QoS 策略（视频会议流量标记 DSCP EF，优先转发）。
  + 数据中心：在 vSphere 平台创建虚拟机模板（区分 Windows Server 2022 与 CentOS 8 镜像），完成私有云平台与统一身份认证系统的对接联调（测试单点登录成功率≥99.9%）。

#### 4.1.4 测试验收与培训阶段（第 8 个月）

* **功能测试**：
  + 有线网络：测试信息点速率（千兆端口实测下载速度≥900Mbps）、VLAN 隔离（不同 VLAN 终端无法互访）、PoE 供电（AP 断电后自动切换至 PoE 供电，重启时间 < 30 秒）。
  + 无线网络：使用 AirMagnet 软件进行信号强度测试（平均接收功率≥-70dBm）、漫游测试（移动终端跨 AP 切换延迟 < 100ms）、并发测试（单 AP 接入 60 用户时网页打开时间≤3 秒）。
  + 安全系统：模拟 SQL 注入攻击（WAF 应准确拦截）、端口扫描（IDS 应触发告警）、VPN 接入（分校区终端通过 IPsec VPN 访问主校区资源，延迟≤50ms）。
* **用户培训**：
  + 管理员培训：开展 3 场技术培训（网络管理平台操作、安全设备配置、虚拟化平台运维），培训人数 50 人 / 场，考核通过率需达 80%。
  + 师生培训：制作《校园网使用手册》（含无线连接指南、云网盘操作说明），通过校园网公告、公众号推送，组织现场答疑会（每校区 2 场）。

#### 4.1.5 正式运行与优化阶段（第 9 个月起）

* **试运行监控**：部署网络性能监控工具（如 Zabbix），实时监测核心交换机 CPU 利用率（阈值≤80%）、出口链路带宽利用率（峰值≤70%），收集师生反馈（通过在线问卷，每周汇总网络使用问题）。
* **持续优化**：根据试运行数据调整无线 AP 信道（每月一次）、更新防火墙安全策略（新增业务系统时 48 小时内完成策略配置），每季度发布《校园网运行报告》，公示网络可用性（目标≥99.95%）、故障处理及时率（≥98%）。

### 4.2 项目预算估算

#### 4.2.1 硬件设备费用（合计约 1200 万元）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 设备类别 | 核心层 | 汇聚层 | 接入层 | 安全设备 | 数据中心 | 其他 |
| 预算（万元） | 200 | 350 | 250 | 200 | 180 | 20 |
| 明细 | 核心交换机 ×2、出口路由器 ×2 | 楼宇汇聚交换机 ×15、光纤模块 ×200 | 接入交换机 ×300、无线 AP×800 | 防火墙 ×2、WAF×1、IDS×1 | 服务器 ×8、全闪存阵列 ×1 | 机柜、线缆、理线架等 |

#### 4.2.2 软件系统费用（合计约 300 万元）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系统类别 | 网络管理 | 虚拟化平台 | 私有云 | 安全软件 | 其他 |
| 预算（万元） | 80 | 100 | 100 | 15 | 5 |
| 明细 | iMaster NCE-Campus 授权 | VMware vSphere 套件 | 阿里云 Stack 许可 | 病毒库升级、安全审计授权 | 操作系统正版化、数据库许可 |

#### 4.2.3 施工与服务费用（合计约 200 万元）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 项目类别 | 综合布线 | 设备安装 | 调试服务 | 培训运维 | 其他 |
| 预算（万元） | 100 | 50 | 30 | 15 | 5 |
| 明细 | 线缆敷设、桥架安装 | 机柜上架、AP 安装 | 网络配置、系统联调 | 管理员培训、3 年维保 | 第三方测试、项目管理费 |

#### 4.2.4 总预算

本项目总投资估算约**1700 万元**，具体费用可根据设备选型调整与招标结果进行动态优化，建议预留 10% 的预备费（约 170 万元）应对需求变更或不可预见风险。

### 4.3 项目风险与应对措施

#### 4.3.1 技术风险

* **风险点**：新老系统兼容性问题（如旧版教务系统不支持 IPv6）
* 应对措施：在核心交换机部署 NAT64/DNS64 转换设备，对 IPv6 终端访问 IPv4 业务进行地址转换；安排厂商技术人员对旧系统进行补丁升级，确保双栈支持。

#### 4.3.2 进度风险

* **风险点**：线缆敷设遇阻（如弱电井空间不足）
* 应对措施：施工前完成全校区弱电井勘察，制定备选路由方案（如临时租用桥架空间）；增加施工队伍人数，优先推进主干道等关键区域布线。

#### 4.3.3 安全风险

* **风险点**：设备配置错误导致网络中断
* 应对措施：实施前进行配置文件离线校验（使用网络配置合规性检查工具），重要设备配置变更需双人复核；启用 iMaster 的配置回滚功能（支持最近 10 次配置版本恢复）。

#### 4.3.4 资金风险

* **风险点**：设备采购价格超预算
* 应对措施：采用 "框架协议招标 + 分批采购" 模式，与供应商约定价格浮动条款（如超过预算 10% 时重新议价）；优先采购国产替代设备（如新华三交换机替代部分 Cisco 设备）。

### 4.4 项目预期效果

* **性能提升**：核心层万兆互联实现校区间文件传输速率≥1200MB/s，无线覆盖区域峰值速率达 1.2Gbps（5GHz 频段），云网盘上传下载速度提升 3 倍以上。
* **安全强化**：通过统一安全防护体系，网络攻击拦截率≥99%，关键业务系统（如教务系统）全年停机时间≤4 小时。
* **管理提效**：iMaster 平台实现 90% 以上的网络配置自动化，故障定位时间从平均 2 小时缩短至 15 分钟，IT 运维人力成本降低 40%。
* **业务赋能**：私有云平台与大模型服务器集群支撑 AI 科研项目算力需求，智能实验室设备接入率达 100%，为学校 "双一流" 建设提供坚实的数字基础设施保障。