湖南电子科技职业学院
HUNAN VOCATIONAL COLLEGE OF ELECTRONIC AND TECHNOLOGY

产品设计	方案设计	工艺设计
	√	

信息工程学院

毕 业 设 计

题目：恒慧中学校园网设计方案

学生姓名	陈邦本
学生学号	010425171785
班级名称	计网 G32208 班
专业名称	计算机网络技术
指导教师	龙佳

2025 年 05 月

毕业设计真实性承诺及指导教师声明

本人郑重声明：所提交的毕业设计是本人在指导教师的指导下，独立进行研究工作所取得的成果，内容真实可靠，不存在抄袭、造假等学术不端行为。除设计中已经注明引用的内容外，本设计不含其他个人或集体已经发表或撰写过的研究成果。对本毕业设计的研究做出重要贡献的个人和集体，均已在设计中以明确方式标明。如被发现设计中存在抄袭、造假等学术不端行为，本人愿承担相应的法律责任和一切后果。

学生（签名）：陈邦宇　　日　期：2025.5.10

指导教师关于学生毕业设计真实性审核的声明

本人郑重声明：已经对学生毕业设计所涉及的内容进行严格审核，确定其成果均由学生在本人指导下取得，对他人成果的引用已经明确注明，不存在抄袭等学术不端行为。

指导教师（签名）：[illegible]　　日　期：2025.5.15

（注：本页学生和指导教师须亲笔签名。）

目 录

一、校园概述

（一）背景介绍

恒慧中学位于大石桥市水源镇盖家村，服务范围涵盖赵家、水源等 10 个自然村以及鲤鱼村的部分区域，学区总人口约为 2.2 万人。目前，该校中学部拥有 61 名教师，设有 12 个教学班，容纳 570 名学生。学校配备了 5 间多媒体教室、110 台计算机终端、标准化的理化生实验室以及藏书量达 3.28 万册的图书室。为了适应教育信息化的发展需求，学校正式启动了校园网络全面升级工程，重点提升网络性能、运行稳定性及安全防护能力。

本次升级计划主要包括三大核心举措：首先，系统性更新网络基础设施，对服务器、交换机、路由器等关键设备进行升级换代，以构建稳定高效的基础网络环境；同时，扩容网络带宽，以满足日益增长的教学资源访问流量需求。其次，构建网络安全防护体系，部署企业级防火墙和入侵检测系统，建立多层防御机制以抵御网络攻击，并配备 7×24 小时网络监控机制，实现故障预警与快速响应。最后，推进教学应用的数字化升级，重点建设在线教育平台、学生信息管理系统及教学资源共享库，通过智能化工具提升教学管理效能，构建覆盖备课、授课、学情分析的全流程数字化解决方案。

此次网络改造工程预计实现三大成效：基础网络吞吐性能提升 300%，教学资源访问响应速度缩短 60%；构建符合等保 2.0 标准的安全防护体系；实现 90% 教学管理流程的数字化。核心建设内容涵盖网络基础设施升级、网络安全架构重构、教学应用生态优化三大维度。通过构建“智能网络 + 数字平台 + 安全体系”三位一体的新型校园信息化架构，为师生打造安全、流畅、智能的数字化教学环境，全面推动学校教育现代化进程。

（二）项目概述

本项目旨在打造高性能智慧校园网络体系，通过系统性改造实现网络架构优化、安全防护强化和运维能力升级。具体实施内容严格按照七大核心模块推进，保持原有段落结构进行深度优化：

网络架构设计：

采用核心 - 汇聚 - 接入三级分层架构，核心层部署双万兆主备交换机，实现99.99%的高可用性；汇聚层配置 VXLAN 技术，打通跨区域数据通道；接入层实施802.1X 认证，实现终端准入控制。通过划分 12 个业务 VLAN（包括教学 VLAN、物联网 VLAN、安防 VLAN 等），构建逻辑隔离的虚拟化网络环境，满足未来五年2000+终端接入的扩展需求。

IP 地址规划：

基于 IPv4/IPv6 双栈部署策略，采用 172.16.0.0/16 私有地址段进行精细化划分。教学区分配/24 可变长子网掩码，物联网设备采用/28 独立子网，访客网络设置 DMZ 隔离区。部署 DHCP Snooping + IP Source Guard 技术，有效防范 ARP 欺骗和 IP 地址盗用问题。

路由协议配置：

核心层启用 OSPF 动态路由协议，实现智能选路，并配置 BFD 快速检测机制，确保 50ms 内感知故障。出口网关部署策略路由（PBR），实现教育专网、互联网等多链路负载均衡，通过 SD-WAN 控制器实现教学视频流量的智能调度，保障 4K 在线课堂的流畅体验。

设备选型部署：

选用华为 S6730-H 系列核心交换机（支持 MACsec 硬件加密）、H3C WA6628X 无线 AP（内置智能射频优化）、迪普科技 UAG9000 下一代防火墙（集成 IPS/AV/WAF 三合一防护）。无线网络采用 Wi-Fi 6（802.11ax）标准，教室区域布放双频 AP，满足 60 终端并发接入，信号覆盖率超过 99%。

技术可行性验证:

搭建 1:1 模拟测试环境，完成 STP 收敛（＜800ms）、IPv6 邻居发现协议、多媒体直播时延（≤30ms）等 12 项专项测试。参照《教育行业信息系统安全等级保

护基本要求》，验证网络架构符合等保 2.0 三级标准，核心业务系统 RTO≤15 分钟。

系统测试验收：

实施四阶段验收体系：1）物理层测试（Cat6A 线缆 100%通过福禄克测试）；2）网络性能测试（iPerf3 测速达标率 100%）；3）业务压力测试（支持 800 终端并发访问）；4）安全渗透测试（通过 NSACE 三级认证）。最终形成包含 283 个检测项的验收矩阵。

运维保障体系：

构建智能运维中心（IMOC），部署 SolarWinds NPM 实现全网设备状态可视化监控。制定三级应急响应机制：1 级故障（全网中断）启动 SDN 控制器自动切换（＜1 分钟）；2 级故障（区域故障）运维团队 30 分钟内到达现场；3 级故障（单点故障）远程指导 2 小时内修复。

项目建成后，将实现三项关键指标：核心网络吞吐量从 1Gbps 提升至 10Gbps，无线接入并发能力提高 5 倍，安全威胁平均响应时间缩短至 8 分钟。通过构建弹性扩展的智能网络底座、符合等保 2.0 的安全防护体系、可视化的运维管理平台，全面支撑电子班牌、智慧课堂、虚拟实验室等新型教学应用的深化部署。

二、学校网络现状与需求分析

（一）描述网络描述

当前学校网络系统陈旧老化，许多设备已服役多年，随着技术的飞速发展，这些设备的功能已无法满足现代教学的需求。设备老化问题日益凸显，不仅故障频发导致性能下降，还可能进一步引发一系列连锁问题，如网络中断、访问延迟等，严重影响师生的日常教学和学习活动。然而，这些问题并未完全阻碍师生在课堂上获取电影、音乐等教学资源，或者访问互联网和浏览社交媒体，但网络的不稳定性和低效性确实给教学活动带来了诸多不便。

此外，学校网络在带宽方面也面临严峻挑战。随着数字化教学和在线学习的不断普及，对网络带宽的需求呈指数级增长，但现有网络带宽却难以满足各类终端设备的高负载访问需求。这不仅会导致网络拥塞，还会使访问速度大幅下降，严重影响师生的在线教学体验。

学校网络安全同样存在潜在风险。若缺乏严格的安全措施，未经授权的用户可能轻易从系统外部或内部入侵学校网络，从而导致数据泄露和信息安全受损。这种脆弱性不仅会干扰学校网络的正常运行，还可能因敏感信息的泄露或丢失而带来不可预估的风险和损失，给学校带来严重的安全隐患。

综上所述，学校网络目前面临的问题不仅包括设备老化、带宽不足和安全风险，还涉及管理挑战和扩展性不足。管理方面的缺陷可能导致网络管理员陷入繁琐的现场维护和故障排除工作中，这种低效的方式无法及时发现并解决网络问题，严重影响了正常的网络使用体验和师生的学术活动。此外，随着学校规模的扩大，网络扩展需求日益迫切，但现有设备性能不足和网络拓扑僵化限制了网络容量的扩充，难以满足未来学校的发展需求。

因此，学校亟需解决设备老化、带宽不足和安全威胁等问题，同时寻求有效的网络管理方法，增强网络的可控性和可维护性，并考虑网络的可扩展性，以确保学校网络能够满足未来发展和扩展的需求。

（二）网络需求

1.教学楼网络需求

教学楼网络必须具备高带宽和稳定性，以满足学生和教师在课堂上使用多种设备（如笔记本电脑、平板电脑和智能手机）同时在线的需求。可靠的网络连接能够有效支持教学活动的顺利开展。同时，强大的安全措施至关重要，必须有效阻止未经授权的用户访问，并检测和防范潜在的网络攻击。此外，网络设计应注重可管理性，支持远程监控和故障排除，能够及时处理网络故障和异常情况，确保网络的不间断运行。

2.行政办公室网络要求

行政办公网络需要高度安全，以防止未经授权的敏感信息泄露和限制不必要的网络访问。通过应用访问控制列表（ACL），网络管理员可以在细粒度级别管理网络流量，配置允许或限制某些类型流量通过网络设备的规则，从而更好地控制对网络资源的访问。此外，高可靠性也是行政办公网络的重要需求，通过实施冗余设备和链路以及定期进行数据备份，可以有效降低设备故障和网络中断的风险，确保管理流程的连续性和稳定性。

3.图书馆网络需求

图书馆网络需要具备高带宽和不间断的可用性，以满足大量用户同时访问电子资源和实体图书资料的需求。同时，必须建立严格的安全协议，保护用户隐私和图书馆资源的完整性，防止未经授权的访问和非法下载。此外，图书馆网络应具备良好的可扩展性，能够适应图书馆管理系统和电子资源管理系统的实施和管理，满足未来业务发展的需求。

4.宿舍网络需求

宿舍网络的主要目标是满足大量学生的互联网需求，确保高带宽、稳定性和可用性，即使在高峰使用时段也能保持良好的网络体验。在设计宿舍网络时，必须将安全性放在首位，通过实施隔离协议和采用入侵检测技术，确保个人隐私和学生设备的安全。此外，宿舍网络应允许学生自行注册并实施设备访问管理系统，简化网络接入流程，提高用户体验。

5.IT 管理部门的网络要求

IT 管理部门负责校园网络的监控和管理，必须实时监控网络设备和流量，及时发现网络故障或潜在的安全风险，并迅速采取措施确保系统稳定运行。同时，提供技术支持也是 IT 管理部门的重要职责，包括解决网络相关问题、提高整体效率以及培养用户的安全意识，以减少潜在的安全漏洞。此外，IT 管理部门还需负责网络规划与优化，持续调整和增强网络结构，以实现更高的性能水平，提升用户体验，提供优质的网络服务。

三、学校网络总体设计与规划

（一）网络结构层次

ISP（互联网服务提供商）： ISP 是学校接入互联网的关键节点，为学校提供外部网络连接，确保学校能够顺畅访问互联网资源。

BJRouter（边界路由器）： 作为学校内部网络与 ISP 之间的桥梁，BJRouter 负责管理内外网络的通信，并提供 NAT（网络地址转换）服务，将内部私有 IP 地址转换为公共 IP 地址，从而实现对外部网络的安全访问。

Firewalld（防火墙）： Firewalld 是学校内部网络的防护屏障，通过 ACL（访问控制列表）和其他安全机制，严格控制和监控网络流量，防止外部恶意攻击和非法访问，保障内部网络的安全。

CoreSwitch（核心交换机）：作为学校内部网络的核心设备，CoreSwitch 连接各个部门的交换机，提供高速数据交换和路由功能，支持 OSPF（开放式最短路径优先）协议，确保网络的稳定性和高效性。

JXLSw1、XZBGSw1、SMSw1（部门交换机）： 这些交换机连接到核心交换机，负责各个部门的网络接入，通过 VLAN（虚拟局域网）技术隔离不同部门的设备，提供定制化的网络服务，满足各部门的网络需求。

学校网络的基础架构由 ISP、BJRouter、Firewalld、CoreSwitch 以及各个部门交换机组成。ISP 作为网络的入口，提供外部连接；BJRouter 负责内外网络的通信和 NAT 转换；Firewalld 作为安全防线，保护网络免受攻击；CoreSwitch 作为核心设备，确保高速数据交换和路由；部门交换机通过 VLAN 技术实现隔离，提供定制化服务，共同构建了一个安全、高效的网络环境。

（二）学校拓扑设计

在学校网络拓扑图中，ISP 作为互联网服务提供商，承担着连接学校网络与外部互联网的关键角色。BJRouter 作为边界路由器，负责内外网络的连接，执行地址转换和路由通信。Firewalld 作为防火墙，严格监控网络流量，确保学校

网络的安全性。CoreSwitch 作为核心交换机，连接各个部门的交换机，实现高速数据传输和路由管理。各部门交换机（如 JXLSw1、XZBGSw1、SMSw1 等）通过 VLAN 技术实现设备隔离，提供定制化的网络服务，满足不同部门的网络需求。

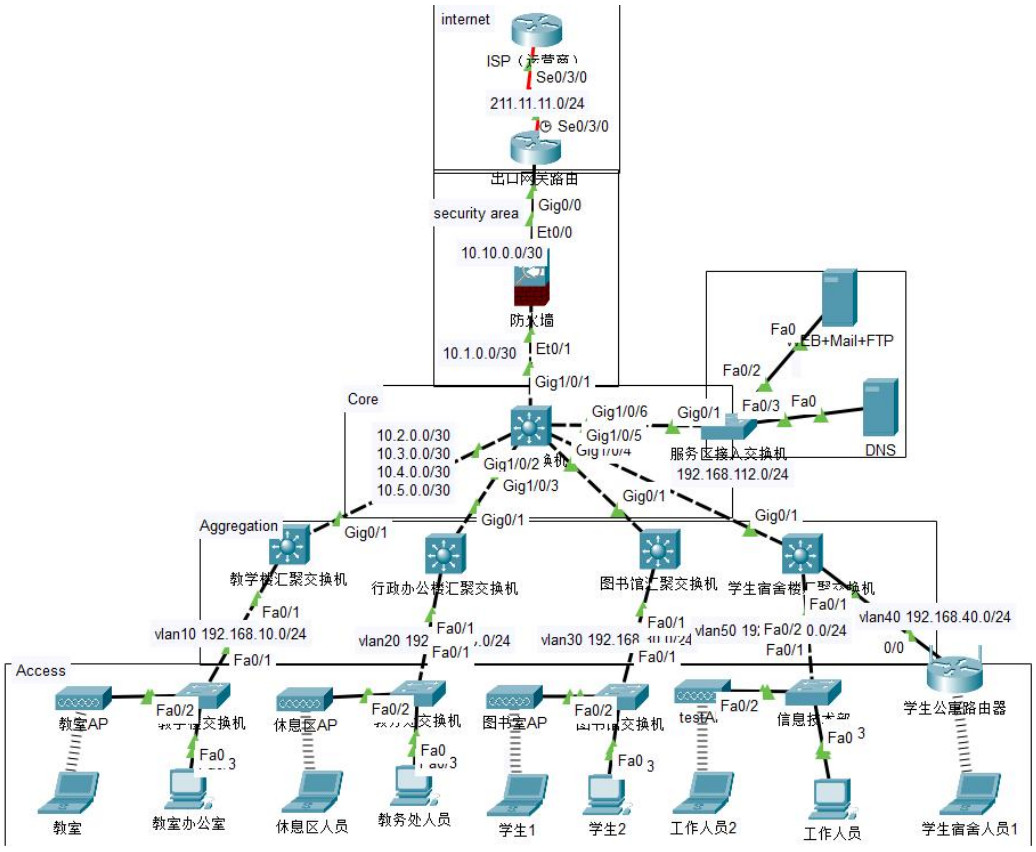


图 3.1 学校网络逻辑拓扑图

（三）IP 地址规划

IP 地址规划是构建高效网络环境的关键环节，其核心目标在于确保网络的稳定性、安全性和高效性。规划过程主要围绕两个策略展开：子网划分与地址分配。通过子网划分，可将大型网络拆分为多个小型子网，这不仅有助于避免 IP 地址的浪费，还能优化网络资源的使用效率。在实施子网划分时，需平衡每个子网的主机容量与网络功能需求，并预留空间以满足未来扩展的需要。此外，合理选择子网掩码至关重要，它直接决定了子网的规模及其后续扩展能力。为适应不断变化的网络需求，设计者需灵活选择合适的子网掩码。

在 IP 地址分配方面，应遵循逻辑性和连贯性原则，避免地址冲突和碎片化。通过将 IP 地址按逻辑顺序分组，可简化网络管理，同时根据不同区域和设备的需求，制定系统化的地址分配方案。确保每个区域拥有充足的地址供应，从而保障网络运营的连续性，支持各类终端设备开展不同级别的网络活动，实现高效、便捷的网络访问。

表 3.1 IP 地址规划表

设备	接口	IP 地址/CIDR 掩码	备注
ISP	Se0/3/0	211.11.11.2/24	连接到互联网的外部接口
BJRouter	Se0/3/0	211.11.11.1/24	连接到 ISP 的外部接口，NAT 外部接口
	G0/0	10.10.0.1/30	内部接口，NAT 内部接口
firewalld	E0/0	10.1.0.2/30	连接到 BJRouter 的内部接口
	VLAN 1	10.10.0.2/30	连接到 BJRouter 的外部接口
CoreSwitch	GigabitEthernet1/0/1	10.1.0.1/30	连接到 firewalld 的内部接口
	GigabitEthernet1/0/2	10.2.0.1/30	连接到 XZBGSw1 的内部接口
	GigabitEthernet1/0/3	10.3.0.1/30	连接到 JXLSw1 的内部接口
	GigabitEthernet1/0/4	10.4.0.1/30	连接到 JXLSw1 的内部接口
	GigabitEthernet1/0/5	10.5.0.1/30	连接到 SMSw1 的内部接口
	GigabitEthernet1/0/6	192.168.112.254/24	管理接口
JXLSw1	FastEthernet0/1	192.168.10.254/24	连接到教学楼的 VLAN
	G0/1	10.2.0.2/30	连接到 CoreSwitch 的内部接口
XZBGSw1	FastEthernet0/1	192.168.20.254/24	连接到行政办公的 VLAN
	G0/1	10.3.0.2/30	连接到 CoreSwitch 的内部接口

JXLSw1	FastEthernet0/1	192.168.30.254/24	连接到图书馆的 VLAN
	G0/1	10.4.0.2/30	连接到 CoreSwitch 的内部接口
SMSw1	FastEthernet0/1	192.168.40.254/24	连接到宿舍的 VLAN
	VLAN 50	192.168.50.254/24	管理 VLAN
	G0/1	10.5.0.2/30	连接到 CoreSwitch 的内部接口

（四）路由方案设计

在设计学校网络的路由方案时，我们对比了 OSPF（开放式最短路径优先）和 RIP（路由信息协议）两种主流路由协议，最终选择了 OSPF 作为学校的路由协议。

首先，路由收敛速度是关键考量因素。OSPF 采用链路状态路由算法，能够迅速适应网络拓扑的变化，实现快速路由收敛；而 RIP 基于距离矢量算法，依赖定时器触发路由更新，收敛速度相对较慢。

其次，网络规模的适用性也至关重要。OSPF 适用于大型复杂网络，支持分层设计和区域划分，具备良好的可扩展性和灵活性；而 RIP 更适合小型简单网络，对于大型网络拓扑不够灵活，容易导致路由器资源消耗和网络拥堵。

在路由更新频率方面，OSPF 仅在链路状态发生变化时进行更新，有效减少了更新频率和带宽消耗；而 RIP 采用周期性路由更新机制，频繁发送更新信息，增加了网络负载。

在路由选择优化方面，OSPF 通过计算链路成本选择最短路径，综合考虑了带宽、延迟等因素，能够实现路由优化和负载均衡；而 RIP 仅以跳数作为路由选择依据，未考虑实际链路质量，可能导致选择非最优路径。

最后，安全性和认证机制也是重要考量。OSPF 支持认证机制，可对路由器之间的邻居关系和路由信息进行验证，提升了网络安全性；而 RIP 缺乏认证机制，容易受到路由欺骗等安全攻击，安全性较差。

综上所述，尽管 RIP 在配置简单性和小型网络中具有一定优势，但在大型、复杂的学校网络环境下，OSPF 凭借更快的路由收敛速度、更好的可扩展性和灵活性，以及更高的安全性和性能表现，成为更适合的路由协议选择。

四、网络设备选型

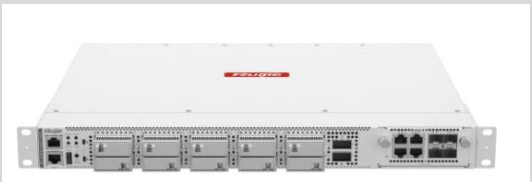
（一）路由器选型

表 4.1 RG-RSR50-X-84 设备

技术参数	参数描述
产品型号	RG-RSR50-X-84
主控板插槽	2 个
交换转发架构	独立交换网板
业务板插槽	12 个
转发性能	360-12000Mpps
交换容量	700Gbps-71Tbps

（二）交换机选型

表 4.2 RG-S7610-10SFX2CQ 设备



产品型号	RG-S7610-10SFX2CQ
整机交换容量	19T
整机包转发率	3600Mpps
CPU	四核处理器，主频 2.2GHz
BOOT ROM	16MB

FLASH Memory	16GB
SDRAM	DDR4 4GB（兼容 8GB）
扩展模块插槽	支持 1 个

表 4.3 RG-S6110-24MG4VS-UP 设备

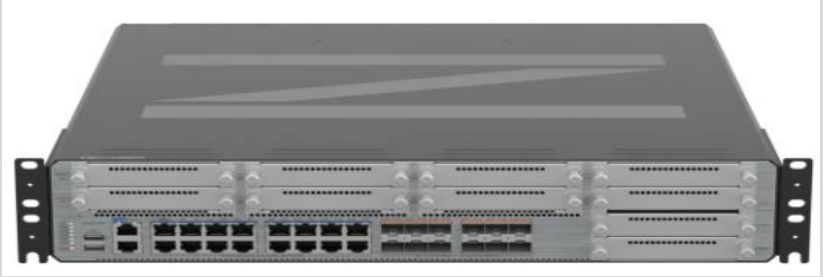
	
硬件规格	RG-S6110-24MG4VS-UP
固化业务接口	24 个 100M / 1000M / 2.5G/ 5G 自适应电口，4 个 10G / 25G SFP28 光口
模块插槽	内置电源
	2 个固化风扇
固化管理接口	1 个 MGMT 端口
	1 个 Console 端口
	1 个 USB 端口

表 4.4 RG-S5310-24GT4XS-E 设备

技术参数	参数描述
产品型号	RG-S5310-24GT4XS-E
固定端口	24 个 10/100/1000M 自适应电口，4 个 1G/10G SFP+光口；
交换容量	672Gbps/6.72Tbps
包转发率	171Mpps/309Mpps

（三）防火墙选型

表 4.5 RG-WALL 1600-Z8680 设备

	
产品型号	RG-WALL 1600-Z8680
固化业务接口	16 个 10/100/1000M 自适应以太网接口
	12 个 10G SFP+接口
固化管理接口	1 个 RJ45 的 MGMT 接口
	1 个 RJ45 的 Console 接口
	2 个 USB 3.0 接口
模块插槽	8 个扩展模块插槽

（四）无线设备选型

表 4.6 RG-AP850-AR(V3)设备

	
尺寸与重量	RG-AP850-AR(V3)
产品尺寸（宽×深×高）	230mm × 230mm × 51mm
产品重量	主机：1.0kg
	挂架：0.1kg
安装方式	吸顶、壁挂
防盗锁	暗锁、明锁

（五）服务器选型

表 4.7 RG-CS7025 设备

	
RG-CS7025 云服务器	
处理器	最大支持 2 颗 C86 架构 7300 系列处理器
内存	DDR4 RDIMM
	最高支持内存频率为 3200MHz，内存在云服务器的实际工作频率根据内存标称频率、CPU 型号及实际配置内存数量不同而不同。
内存插槽	32 个

数	
内存总容量	最大支持 2048GB（64GB*32）
对外接口	2 个 USB3.0 前置接口
	建议使用标准 VGA 线缆，否则可能会导致个别 VGA 口无法正常输出；推荐使用后置 VGA 口

五、技术介绍与可行性分析

（一）技术简介

在网络管理和安全控制领域，VLAN（虚拟局域网）、OSPF（开放最短路径优先）、NAT（网络地址转换）和 ACL（访问控制列表）等技术因其高效性和实用性而被广泛应用。这些技术是构建强大、安全且易于管理网络的关键。

VLAN（虚拟局域网）：VLAN 能够将物理网络划分为多个逻辑网络，从而减少广播流量，增强安全性，并优化网络管理。通过 VLAN，管理员可以根据用户的功能需求而非物理位置进行分组，实现更灵活的网络配置。

OSPF（开放最短路径优先）：OSPF 是一种动态路由协议，广泛应用于 IP 网络。它通过链路状态路由算法，根据最短路径高效地在 IP 网络内路由数据包。OSPF 能够快速适应网络拓扑变化，确保网络服务的高可用性和可靠性。

NAT（网络地址转换）：NAT 在节省公共 IP 地址和增强安全性方面发挥着重要作用。它通过将私有 IP 地址转换为公共 IP 地址，使多个设备能够共享一个公共 IP 地址访问互联网，同时隐藏内部网络结构，增加安全防护。

ACL（访问控制列表）：ACL 是一组规则，用于控制进出网络的流量。它可以限制对敏感区域的访问，防止未经授权的访问，并确保用户只能访问其所需的资源。ACL 可以根据 IP 地址、端口号或协议进行流量过滤，实现精确的流量控制。

（二）可行性分析

将 VLAN、OSPF、NAT 和 ACL 技术集成到网络中，不仅技术上可行，而且对于提升网络管理和安全性具有显著益处。这些技术各自解决了网络设计和运营中的特定挑战，综合使用时，能够提供全面的解决方案，打造高效、安全且易于管理的网络环境。

集成这些技术的可行性取决于当前网络架构、硬件兼容性以及管理员的技术水平。现代网络设备大多支持这些技术，因此集成过程相对简单。然而，可行性

分析还需考虑对网络性能的潜在影响以及对培训或额外资源的需求。通过合理的规划和实施，集成这些技术可以显著提升网络性能和安全性，是现代组织的理想选择。

1. VLAN（虚拟局域网）

优势：VLAN 通过将网络划分为逻辑独立的部分，增强了安全性和管理效率，降低了广播风暴的风险，并提供了灵活的配置选项。

实施方式：需要根据部门或功能需求规划 VLAN 划分，并在交换机和路由器上配置 VLAN 接口，确保流量正确转发和隔离。

2. OSPF（开放最短路径优先）

优势：OSPF 作为一种动态路由协议，能够自动适应网络拓扑变化，具备快速收敛、适应性强和分层设计等优点。

实施方式：在网络中定义 OSPF 区域，配置区域类型和参数，并启用 OSPF 进程，使路由器能够动态调整路由表。

3. NAT（网络地址转换）

优势：NAT 通过将内部私有 IP 地址转换为公共 IP 地址，隐藏了内部网络结构，解决了 IPv4 地址不足的问题。

实施方式：在边界设备上配置 NAT 规则，指定私有地址与公共地址的映射关系，使内部主机能够安全访问互联网。

4. ACL（访问控制列表）

优势：ACL 能够过滤网络流量，实现精细的访问控制，防止未经授权的访问，提高网络安全性。

实施方式：根据网络策略创建 ACL，定义允许或拒绝的流量类型，并将其应用到相应接口或 VLAN 上，确保流量受到适当控制。

六、网络测试

（一）设备连接测试

为了确保校园网络能够满足不同部门之间的资源共享和业务隔离需求，以下是对校园网络中不同部门之间连通性的详细测试描述：

部门内部连通性测试:

此测试的目的是验证同一部门内部人员之间的网络连通性。例如，教室内的人员 1 尝试通过网络访问同一教室内人员 2 的设备，以确认他们之间的通信是否正常，从而确保部门内部资源共享的顺畅性。

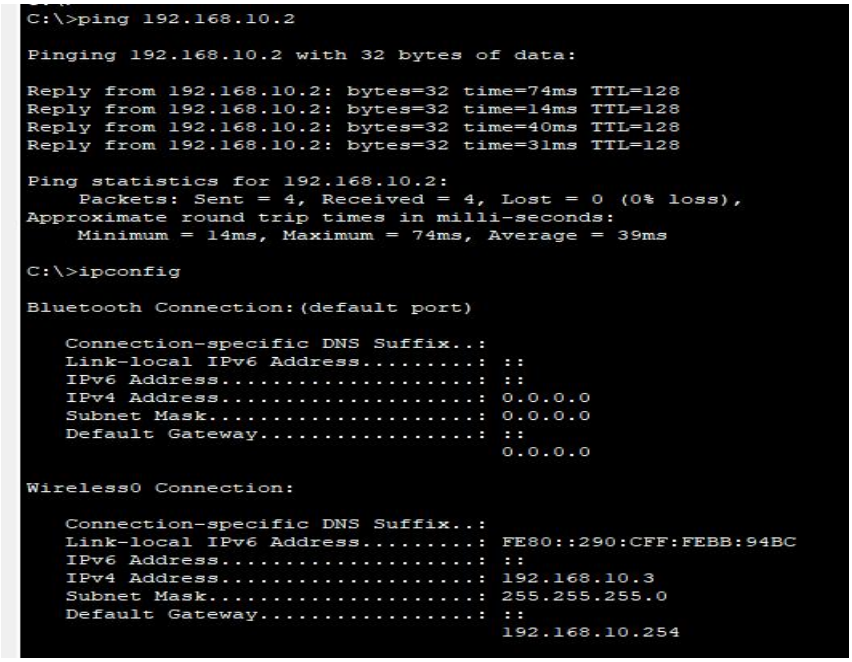


图 6.1 教室人员 1 访问教室人员 2 连通性测试

跨部门访问测试:

在此测试中，教室人员尝试访问行政办公室的网络资源，以确认是否能够跨部门访问。如果测试结果显示无法访问，则表明业务隔离措施生效，不同部门之间无法直接访问对方资源，符合安全策略要求。

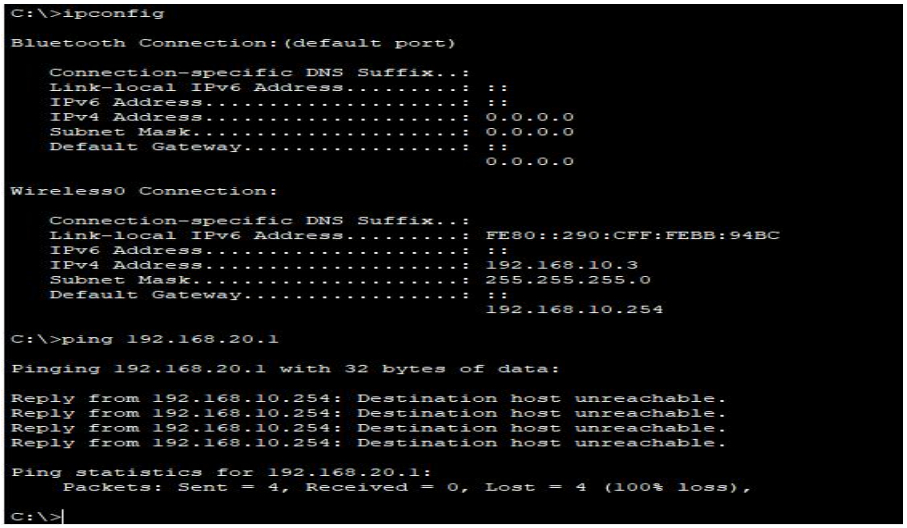


图 6.2 教室人员访问行政办公室连通性测试

图书馆网络访问测试:

此测试旨在验证学生在图书馆使用校园网络时是否能够顺利访问互联网。学生尝试访问外部网站或资源，以确认他们是否能够正常使用网络服务，从而支持他们的学习和资料查找需求。

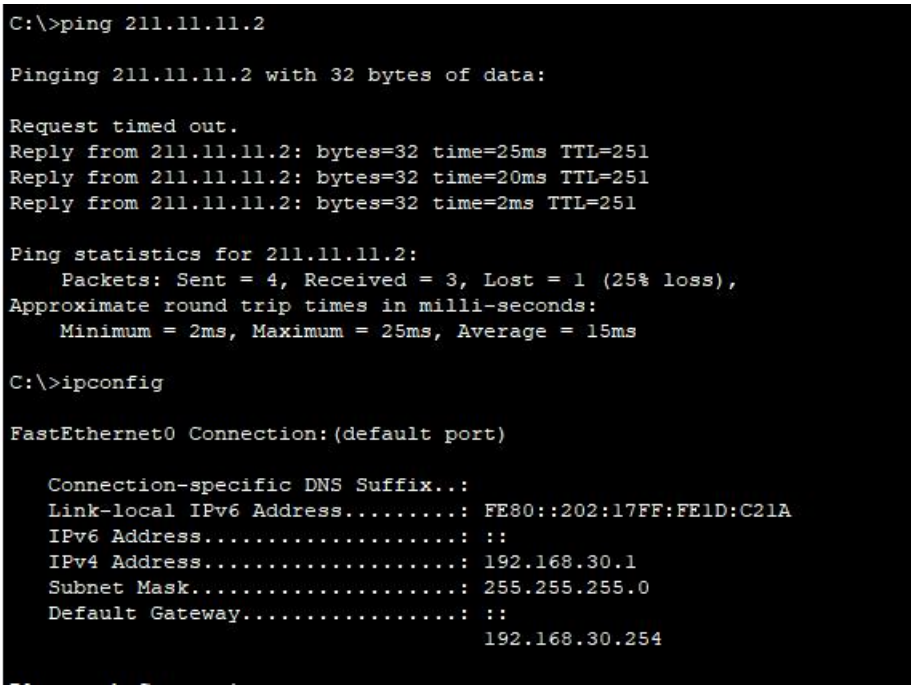


图 6.3 图书馆学生访问互联网连通性测试

IT 管理部门访问权限测试:

IT 管理部门作为网络的维护者，需要具备对学校服务器区的高权限和管理能力。通过测试 IT 管理部门是否能够顺利访问学校服务器区的网络资源，可以验证其权限设置和网络管理能力，确保网络的正常运行和维护。

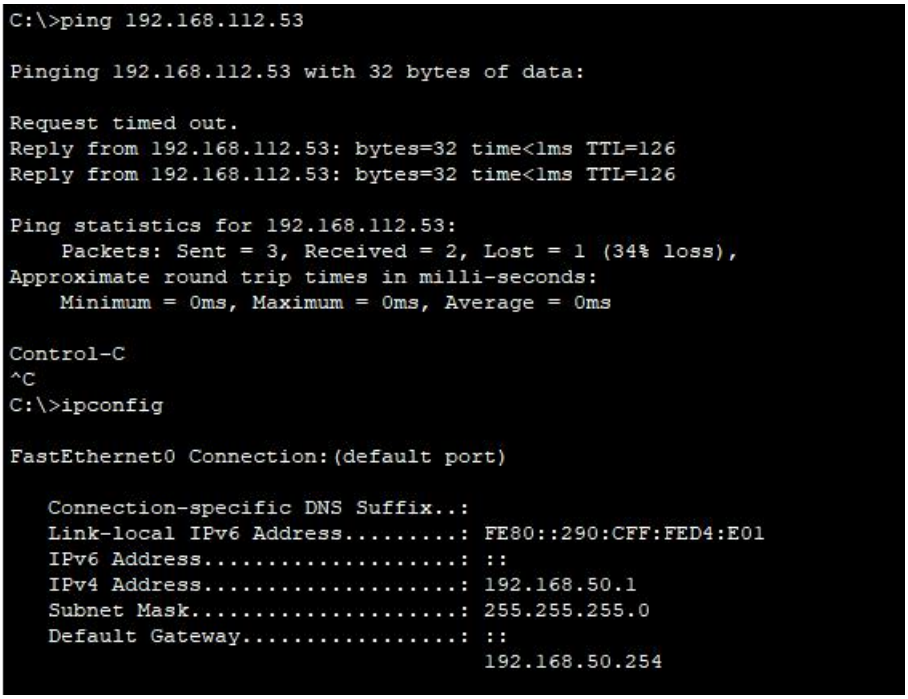


图 6.4 IT 管理部门访问学校服务器区连通性测试

（二）功能性测试

1.DHCP 分配测试

在校园网络中，DHCP 服务负责为连接到网络的设备分配 IP 地址。进行 DHCP 分配测试时，需验证各个 VLAN 的 DHCP 服务器是否正常工作，并确认设备能够成功获取 IP 地址，以确保网络接入的稳定性。

图 6.5 教务处人员自动获取 IP 地址

2.访问控制测试

校园网络通常需要根据安全策略限制不同部门或用户之间的通信。通过进行访问控制测试，可以验证 ACL 是否有效地限制了不同 VLAN 之间的通信，从而确保网络的安全性和合规性。

```
C:\>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:

Reply from 192.168.30.254: Destination host unreachable.
Reply from 192.168.30.254: Destination host unreachable.

Ping statistics for 192.168.50.1:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:17FF:FE1D:C21A
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.30.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.30.254
```

图 6.6 vlan 隔离测试

3.OSPF 路由测试

在校园网络中，OSPF 常用于实现内部路由，确保校园各个子网之间的通信。进行 OSPF 路由测试时，应检查各个路由器之间的邻居关系是否建立，并验证路由器之间的路由信息是否正确，以确保网络的连通性和稳定性。

```
CoreSwitch#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.254    1   FULL/BDR        00:00:37    10.2.0.2        GigabitEthernet1/0/2
192.168.20.254    1   FULL/BDR        00:00:37    10.3.0.2        GigabitEthernet1/0/3
192.168.30.254    1   FULL/BDR        00:00:37    10.4.0.2        GigabitEthernet1/0/4
192.168.50.254    1   FULL/BDR        00:00:37    10.5.0.2        GigabitEthernet1/0/5
CoreSwitch#
```

图 6.7 CoreSw 设备中 ospf 邻居信息

```
JXLSw1#show ip route ospf
     10.0.0.0/30 is subnetted, 5 subnets
O       10.1.0.0 [110/2] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O       10.3.0.0 [110/2] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O       10.4.0.0 [110/2] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O       10.5.0.0 [110/2] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O    192.168.20.0 [110/3] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O    192.168.30.0 [110/3] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O    192.168.40.0 [110/3] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O    192.168.50.0 [110/3] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O    192.168.112.0 [110/2] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 10.2.0.1, 02:45:19, GigabitEthernet0/1
```

图 6.8 CoreSw 设备中 ospf 路由条目

4.NAT 功能测试

如果校园网络需要通过 ISP 连接到外部网络，那么 NAT 功能就变得至关重要。通过进行 NAT 功能测试，可以验证内部网络设备是否能够成功访问外部网络资源，以确保 NAT 功能正常运行，支持校园网络的外部访问需求。

```
BJRouter#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 211.11.11.1:3     192.168.30.1:3     201.11.11.2:3      201.11.11.2:3

BJRouter#
```

图 6.9 BJR outer 设备中 nat 地址转换信息

5.HTTP 功能测试

HTTP 功能测试旨在验证校园网络内部设备是否能够成功访问外部的 HTTP 服务，例如通过网页浏览器访问网站。通过 HTTP 功能测试，可以确认网络中的 NAT 配置是否正确，并且外部网络连接是否畅通。测试过程中，可以尝试从校园网络内部的设备使用浏览器访问外部的网站，如 Google、百度等，以确认是否能够成功打开网页并正常浏览内容。

图 6.10 老师访问学校服务资源

七、应急方案

网络故障响应流程：

为确保网络故障能够得到快速有效的处理，减少对网络服务的影响，必须建立一套明确的网络故障响应流程。当网络故障发生时，首要任务是确定责任人员，由其负责故障的诊断与修复工作，同时应及时向相关用户和部门通报故障情况。

备份设备和配置：

定期对核心设备、路由器、交换机等关键网络设备进行备份，并将备份文件妥善存储于安全位置。备份内容应涵盖网络设备配置、ACL 规则、VLAN 设置等重要信息，以便在需要时能够迅速恢复网络服务。

故障排查工具和资源准备：

配备必要的故障排查工具和资源，例如网络测试仪、备用设备、备用电源等。同时，对网络运维人员进行培训，使其熟练掌握这些工具的使用方法，从而加快故障定位和修复的速度。

应急联系方式：

建立一份完整的应急联系方式清单，涵盖网络供应商、设备厂商技术支持、网络管理员等关键人员的联系方式。确保在紧急情况下能够迅速联系到相关人员并获得必要的支持。

应急网络配置：

预先制定应急网络方案，明确备用路由器、交换机等备用设备的接入方式和配置细节。在主要设备发生故障时，能够快速切换至备用设备，确保网络服务的持续可用性。

网络监控与警报系统：

部署网络监控系统，实时监控网络设备的运行状态和流量情况。同时，设置警报系统，以便在检测到网络异常时能够及时发出警报，并通知相关人员进行处理。

应急演练和培训：

定期组织网络应急演练，使网络运维人员熟悉应急处理流程和操作步骤。同时，定期开展培训，提升网络运维人员的应急处理能力和技术水平。

与供应商合作：

与网络设备供应商建立良好的合作关系，及时获取最新的设备信息、漏洞修复和技术支持。在网络设备出现严重故障或漏洞时，能够迅速获得供应商的支持和协助。

参考资料

[1]乌文波.中职学校校园网络的规划与设计[J].数码设计,2024,18(07):173-174.

[2]陈岳.园区级校园网络规划与方案设计[J].信息技术与信息化,2023(11):167-170.

[3]李思雨.高校校园网综合规划与设计[J].信息记录材料,2022,23(03):190-192.

[4]刘晓亚.校园无线网络的规划设计与部署[J].计算机时代,2024(6):122-124.

[5]钟机灵.高可靠性校园网规划与设计研究[J].电脑知识与技术,2023,16(22):74-76.

[6]王应求.高校校园网规划设计及智能化改造分析[J].现代信息科技,2022,6(04):88-90.

[7]赵新胜，等.《路由与交换技术》[M].人民邮电出版社:北京市,2023.06.

[8]谢希仁.《计算机网络第七版》[M].电子工业出版社:北京市,2023.11.

[9]林宜锋.基于 ENSP 的中学网络规划研究与设计[D].中国新通信,2023-09-20.

[10]廖伟文.广州工商学院校园网的规划及实现[D].华南理工大学,2024-10-22.