

湖南软件职业技术大学

毕业设计



基于思科设备的某教育培训机构的网络
毕业设计题目 设计方案

学 生 姓 名 宁子凡

学 生 学 号 202201110402

所 在 学 院 软件与信息工程学院

专 业 班 级 计算机网络技术 2204 班

指 导 教 师 易兰英

目 录

一、概 述	1
1.1 项目背景	1
1.2 项目目的	1
二、 需求分析	2
2.1 用户需求	2
2.2 教学需求	3
2.3 带宽需求	3
三、 项目设计	4
3.1 项目主体分析	4
3.2 网络拓扑图设计	4
3.3 网络协议	5
3.4 VLAN 划分	6
3.5 IP 地址规划	7
3.6 路由规划	9
四、 网络设备选型	11
4.1 交换机选型	11
4.2 路由器选型	13
4.3 服务器选型	14
4.4 网卡选型	15
4.5 PC 选型	16
五、 网络设备配置	17
5.1 交换机的配置	17
5.1.1 核心层交换机配置.....	17
5.1.2 汇聚层交换机配置.....	23
5.1.3 接入层交换机配置.....	26
5.2 路由器的配置	30

5.3 网络测试	33
5.4 服务器的配置	36
5.4.1 Web 服务器	36
5.4.2 FTP 服务器	38
六、 网络安全与规划	41
6.1 网络安全概述	41
6.2 网络安全规划	43
6.3 WEB 防火墙	44
6.4 数据加密策略	44
总结	46
参考文献	47
致 谢	48

一、概 述

1.1 项目背景

近年来，随着教育培训行业的快速发展，信息化手段已成为提升教学质量、优化管理流程的重要支撑。在现代教育培训机构中，依赖网络进行教学资源共享、线上课堂、远程教育和日常办公已成为常态。教育是教育事业的一个必不可少的环节，它旨在确保教育系统的正常运作，以实现其教育使命。该教育培训机构作为行业内的领先者，其网络环境面临着日益增长的设备接入数量、高带宽应用的增多及对网络稳定性、安全性要求的不断提升。然而，当前网络设施已显陈旧，难以满足现代化需求，影响了正常的教学和办公运作。

为此，该机构决定对现有网络进行全面升级，采用思科的先进设备构建高效、安全、可扩展的新型网络架构。本项目将围绕思科的网络设备优势，设计满足当前业务需求并支持未来发展的网络架构，涵盖核心层、汇聚层、接入层的设计与优化，确保网络的高性能与高可用性。

通过合理的网络分段、科学的流量管理和完善的安全策略，此设计方案将为该教育培训机构构建出一套先进的网络平台，提升教学和管理信息化水平。此设计方案不仅满足机构当前的业务需求，也为未来的教学与管理创新提供了有力的支撑，帮助教育培训机构在信息化转型中占据领先地位。

1.2 项目目的

本项目旨在为该教育培训机构构建一个高效、安全、稳定且可扩展的网络架构，以支持当前及未来的业务需求，确保日常教学和办公的顺利开展。通过优化网络性能和安全防护，提高网络管理效率，为师生提供可靠、顺畅的网络支持，进一步优化教学体验，支持共享屏幕、资源共享及远程指导等多样化的教学方式。同时，灵活的网络扩展能力将满足未来设备接入和业务发展的需求，为信息化教学创新提供坚实的技术保障。

二、需求分析

为了满足教育培训机构对高效网络性能、安全环境和灵活扩展性的需求，确保网络支持学生教师高速上网、资源共享、实验环境和多终端接入。通过加强安全策略、优化管理和便捷维护，构建可持续发展的网络环境，为现代化教学模式提供稳定的技术支撑，提升整体用户体验和教学质量。

2.1 用户需求

本项目的用户需求涵盖了多方面内容，旨在为培训机构提供一个稳定、安全、灵活、易管理的网络环境，这些需求体现了培训机构在日益数字化的教育环境中对网络性能的严格要求。

（1）稳定的网络性能：用户希望获得稳定、高速的网络连接，特别是在高并发的情况下，确保教学资源 and 日常办公应用能够流畅访问，支持高带宽和低延迟的在线学习和多媒体传输。

（2）高安全性：用户需要强有力的安全保障，采取多层次的防护措施，包括网络访问控制、入侵检测系统、加密技术等，以防范恶意攻击和数据泄露，确保师生及管理人士的个人信息、教学资源和敏感数据得到充分保护，免受各类安全威胁。

（3）灵活的扩展能力：用户希望网络具备灵活的扩展能力，能够轻松适应未来教学规模的扩大和设备接入的增加，并能快速部署新设备和新增用户，以满足长期发展的需求，同时确保系统稳定性和高效性。

（4）便捷的管理和维护：用户期望通过集中化、可视化的管理工具进行网络监控和管理，减少日常运维工作量，提高故障排查和响应效率，降低维护成本。

（5）优化教学支持：用户需求包括网络对在线课堂、远程教学、虚拟实验室等现代化教学模式的稳定支持，以便为学生和教师提供良好的教学体验，提升整体教学质量和互动效果。

2.2 教学需求

为了构建一个高效、稳定且灵活的教学环境，系统应具备一系列先进的技术功能，满足现代教学活动的多样化需求。

首先，系统应配备多媒体教室功能，支持音视频教学资源的灵活播放和互动展示，极大提升课堂的互动性和学生的参与感。通过多媒体设备，教师可以更加生动地呈现教学内容，增加课堂的趣味性，激发学生的学习兴趣。

其次，系统应集成还原盘功能，确保在设备故障或误操作情况下能够迅速恢复到原始状态，减少停机时间，保障教学连续性。这一功能有效减轻运维负担，减少系统故障对教学活动的干扰。

在实训机房主机中我们安装了教学所需各种软件，如 VMware 软件能够为教师和学生提供灵活的虚拟实验环境，提高资源利用效率，支持教学环境的快速部署和管理，满足不同课程的需求。还可以结合 PyCharm 等编程软件的支持，学生可以在机房中进行编程实践，环境搭建等，从而增强编程技能和实践能力。

最后，极域电子教室软件的集成能够实现课堂管理、远程监控与学生互动等功能，帮助教师实时掌控课堂情况，提升教学效果。极域电子教室还支持学生与教师之间的互动交流，促进课堂讨论和学习反馈，增强学生的参与感。

通过这些技术的整合，系统能够有效优化教学资源配置，提升教学质量，并为学生创造更好的学习体验。

2.3 带宽需求

在教育培训机构的网络带宽需求评估中，应考虑终端设备数量、并发用户数、主要应用场景以及峰值流量需求等因素。例如，对于支持在线教学、视频会议、多媒体课堂以及编程软件使用的机构，本教育培训机构有 500 台终端设备，每台设备的平均带宽需求为 5 Mbps，考虑到并发率为 70%，总带宽需求可估算为 $500 \times 5 \text{ Mbps} \times 0.7 = 1750 \text{ Mbps}$ 。为满足高峰期及未来扩展需求，建议预留 30%-50% 的冗余带宽，即配置不低于 2.5 Gbps 的上行带宽连接。

三、项目设计

3.1 项目主体分析

本项目的主体是为教育培训机构设计一套高效、合理的网络方案，围绕 IP 地址划分、组网架构和动态路由协议的应用展开，以满足不同区域的业务需求并保障网络的高效运行。网络按照功能需求划分为两个独立的网段：行政楼使用 192.168.0.0/24 网段，服务于办公和行政管理；实训楼的 IP 地址 172.16.0.0/24 网段，满足教学实践和学员设备接入的需要。

组网方案采用核心交换机和汇聚层交换机的分层架构，通过配置开放式最短路径优先（OSPF）动态路由协议，实现不同网段间的高效互联和快速路由收敛。OSPF 的区域化设计提升了路由的灵活性和稳定性，避免了网络拥堵问题，同时减少了路由器的资源占用。通过动态路由的引入，网络具备了较强的可扩展性和适应性，为教育培训机构的管理和教学提供了一个稳定、智能且便于维护的网络平台。

3.2 网络拓扑图设计

本网络拓扑设计分为核心层、汇聚层和接入层三个层次结构，以便于管理和提高网络的扩展性和性能。

在核心层，核心路由器连接到外网，并提供与内部各部门和服务器群的高速连接。

汇聚层负责各 VLAN 的中转和汇聚，通过交换机 HJ-SW-A、HJ-SW-B、HJ-SW-C 连接核心层和接入层，实现不同部门和楼层的网络隔离与安全管理。

在接入层，各部门和楼层的设备分布于多个 VLAN，分别通过交换机 JR-SW-A、JR-SW-B、JR-SW-C 接入，确保各 VLAN 能高效、安全地进行数据传输。整个设计还包括服务器群，以 FTP 和 WEB 服务器为代表，为网络用户提供资源访问服务。网络拓扑图如 3-1 所示：

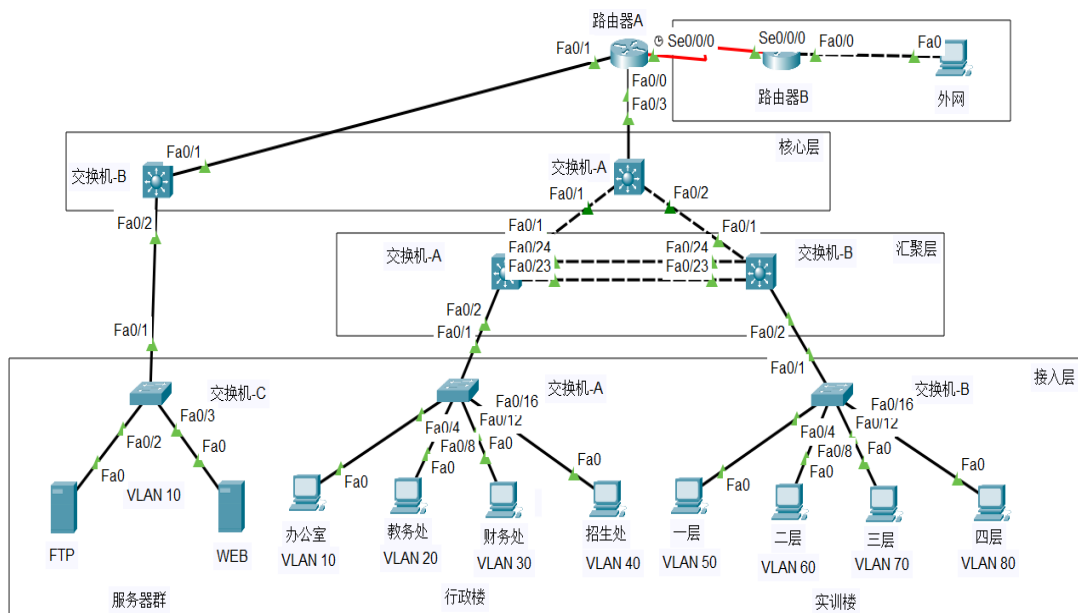


图 3-1 网络拓扑图

3.3 网络协议

网络通信协议是用于网络设备之间进行交流的标准规则，它充当不同操作系统和硬件架构之间的通用语言，确保互联网络的顺畅通信。通过这些协议，各种设备能够有效地交换信息，实现互操作性。

（1）TCP/IP 协议

Transmission Control Protocol/Internet Protocol（传输控制协议/互联网协议）是用于互联网和计算机网络的核心通信协议套件，通过分层结构实现了不同网络设备之间的有效交流。该协议主要分为四层：应用层负责提供网络服务，如 HTTP 和 FTP；传输层确保数据传输的可靠性（通过 TCP）或速度（通过 UDP）；互联网层处理数据包的寻址和路由（通过 IP）；网络接口层则管理物理连接和数据链路。TCP/IP 的设计使其能够实现多种操作系统和硬件的互操作性，确保数据在全球范围内的灵活和可靠传输，成为现代网络通信的基础。

在应用层，我们可以利用多种网络服务支持在线教学和资源共享；传输层则通过 TCP 协议确保数据的可靠传输，适应教学过程中对数据完整性和实时性的要求；互联网层负责为每个设备分配 IP 地址，实现设备之间的互联；网络接口层则保障物理连接的稳定性。

（2） OSPF 协议

Open Shortest Path First（开放最短路径优先）是一种基于链路状态算法的动态路由协议，广泛应用于中大型网络中。OSPF 通过链路成本进行高效的路由选择，优化数据传输效率，并支持区域划分，降低路由表复杂性，简化网络管理。其良好的扩展性使其能够适应培训机构未来的扩展需求，同时提供增强的安全性，通过认证机制保护路由信息，防止网络受到恶意攻击。这些优势共同构建了一个高效、可靠且安全的网络基础。

（3） NAT 协议

Network Address Translation（网络地址转换）是一种用于在计算机网络中转换 IP 地址的技术，主要用于解决 IP 地址短缺和增强内部网络安全性。

（4） DHCP 协议

Dynamic Host Configuration Protocol（动态主机配置协议）在网络中的主要功能是自动分配 IP 地址及相关网络参数，为设备提供动态、集中化的网络配置管理。它简化了网络部署和管理，避免了手动配置每个设备的繁琐过程，并提高了 IP 地址利用率，特别适合设备频繁变动或规模较大的网络环境。

（5） 链路聚合协议

Link Aggregation（链路聚合）在网络中的功能是将多条物理链路组合成一条逻辑链路，以提供更高的带宽和冗余性。通过链路聚合，网络可以实现负载分担，提升数据传输效率，同时在某条物理链路发生故障时，其余链路仍能保持连接的稳定性，从而增强网络的可靠性和可用性。

3.4 VLAN 划分

在本项目中，VLAN 通过将网络划分为行政楼、实训楼和服务器群等逻辑区域，实现了高效的网络隔离。不同部门和楼层的设备被划分到各自的 VLAN 中，从而减少了广播流量的范围，降低了网络拥堵，显著提升了整体网络的性能和稳定性。与此同时，VLAN 的应用极大地增强了数据的安全性，设计有效防止了未经授权的访问，保护了行政管理和教学数据的安全，特别是在服务器群中运行的关键业务系统。总体而言，VLAN 的引入为培训机构提供了性能优越、安全可靠、便于管理

的网络基础设施，有力支持了教学、实训和日常办公的顺利开展。如表 3-1 所示：

VLAN 号	部门	人数	子网号	子网掩码
VLAN 10	办公室	50	192.168.10.0	255.255.255.0
VLAN 20	教务处	10	192.168.20.0	255.255.255.0
VLAN 30	财务处	15	192.168.30.0	255.255.255.0
VLAN 40	招生处	5	192.168.40.0	255.255.255.0
VLAN 10	一层	160	172.16.10.0	255.255.255.0
VLAN 20	二层	160	172.16.20.0	255.255.255.0
VLAN 30	三层	160	172.16.30.0	255.255.255.0
VLAN 40	四层	160	172.16.40.0	255.255.255.0

表 3-1 VLAN 划分

3.5 IP 地址规划

IP 规划是网络设计中的关键环节，涉及为网络中的各个设备分配合理的 IP 地址，以确保网络的高效运作和管理。合理的 IP 规划需要根据网络规模、设备数量及未来扩展需求。如表 3-2 所示：

部门	VLAN	IP 地址	网关
办公室	VLAN 10	192.168.10.1/24	192.168.10.254
教务处	VLAN 20	192.168.20.1/24	192.168.20.254
财务处	VLAN 30	192.168.30.1/24	192.168.30.254
招生处	VLAN 40	192.168.40.1/24	192.168.40.254
一层	VLAN 50	172.16.10.1/24	172.16.10.254
二层	VLAN 60	172.16.20.1/24	172.16.20.254
三层	VLAN 70	172.16.30.1/24	172.16.30.254
四层	VLAN 80	172.16.40.1/24	172.16.40.254

表 3-2 部门的 IP 地址划分

培训机构向运营商申请了两个外网地址，通过 NAT 技术实现了内网用户的统一出口，确保所有用户能够顺利访问外部网络。NAT 将内网中的私有地址动态或

静态映射为公有地址，不仅有效隐藏了内网设备的真实 IP 地址，还避免了外部设备直接访问内网，从而大大提升了安全性。

外网地址池在培训机构教务系统中用于为教务系统的设备或用户动态分配公网 IP 地址，方便访问互联网资源，支持在线学习、远程管理和信息交流的需求。核心交换机 A 和路由器 A 相连端口为 10.1.1.1/30 - 10.1.1.2/30，路由器 A 与路由器 B 通过专用端口建立了连接，确保两者之间的通信顺畅。路由器 B 还通过另一个端口连接外部设备，承担内网与外网的桥梁作用。这样的配置支持路由器之间的数据交换，增强了网络的灵活性和安全性。这种设计适合需要稳定内外连接的场景。如表 3-3 所示：

描述	IP 地址	子网掩码
外网地址池	8.138.176.3-4	255.255.255.0
路由器 A 与路由器 B 相连的端口	8.138.176.1	255.255.255.0
路由器 B 与路由器 A 相连的端口	8.138.176.2	255.255.255.0
路由器 B 与外网设备相连的端口	8.138.177.254	255.255.255.0
外网设备	8.138.177.228	255.255.255.0

表 3-3 外网地址

培训机构还需要建设一个 FTP 服务器和一个 WEB 服务器，以支持教学活动的顺利进行。FTP 服务器将供内部网络使用，帮助学生和教师完成作业的上传、下载与收集，方便资料共享和作业提交。WEB 服务器将搭建教务系统，为学生和教师提供查看课程信息、安排学习任务、整理学生信息等功能，提升教学管理的效率和便利性。此外，WEB 服务器还将支持教学资源的在线浏览和管理，为培训机构的教学活动提供集中化、便捷的访问平台。如表 3-4 所示：

描述	VLAN	IP 地址	网关
FTP 服务器	VLAN 10	10.199.199.2/24	10.199.199.0
WEB 服务器	VLAN 10	10.199.199.1/24	10.199.199.0

表 3-4 服务器 IP 地址

为确保网络设备之间的有效连接，选择合适的连接线缆至关重要。以下列出

了各设备的连接情况。如表 3-5 所示：

设备	本端端口号	对端设备	对端端口号
HX-SW-A	Fa0/3	路由器 A	Fa0/0
	Fa0/1	HJ-SW-A	Fa0/1
	Fa0/2	HJ-SW-B	Fa0/1
HX-SW-B	Fa0/1	路由器 A	Fa0/1
	Fa0/2	JR-SW-C	Fa0/1
HJ-SW-A	Fa0/23-24	HJ-SW-B	Fa0/23-24
	Fa0/2	JR-SW-A	Fa0/1
HJ-SW-B	Fa0/2	JR-SW-B	Fa0/1
JR-SW-C	Fa0/2	FTP	Fa0
	Fa0/3	WEB	Fa0
JR-SW-A	Fa0/4	办公室	Fa0
	Fa0/8	教务处	Fa0
	Fa0/12	财务处	Fa0
	Fa0/16	招生处	Fa0
JR-SW-B	Fa0/4	一层	Fa0
	Fa0/8	二层	Fa0
	Fa0/12	三层	Fa0
	Fa0/16	四层	Fa0
路由器 A	Se0/0/0	路由器 B	Se0/0/0
路由器 B	Fa0/0	外网设备	Fa0

表 3-5 设备连接

3.6 路由规划

教育培训机构的路由规划考虑多个关键因素，包括网络拓扑、带宽需求、设备分布以及未来扩展性。

在网络设计初期，首先需要根据功能区域（如教室、办公区、实训室等）对

IP 地址进行合理划分，采用子网划分技术来优化地址空间的利用，避免地址冲突和浪费。合理的子网划分能够降低广播域的大小，提高网络的可管理性和性能。

在选择路由协议时，动态路由协议如 OSPF（开放最短路径优先）能够在网络拓扑发生变化时，自动重新计算路由路径，确保网络流量的最优路径选择。对于静态路由，可以在固定路径的情况下减少路由开销，提升网络的稳定性。此外，使用路由聚合（Route Aggregation）技术可以减少路由表的大小，优化路由性能。

最后，考虑到教育培训机构网络的扩展需求，路由规划应具备高度的可扩展性。通过模块化的设计和灵活的地址规划，能够方便地添加新的子网或设备而不影响现有网络的运行。如 3-6 所示：

网络地址	子网掩码	类型	下一跳/接口	度量值/更新时间
10.1.2.0	/30	直接连接	FastEthernet0/1	-
192.168.10.0	/24	直接连接	VLAN 10	-
192.168.20.0	/24	直接连接	VLAN 20	-
192.168.30.0	/24	直接连接	VLAN 30	-
192.168.40.0	/24	直接连接	VLAN 40	-
172.16.10.0	/24	直接连接	VLAN 50	-
172.16.20.0	/24	直接连接	VLAN 60	-
172.16.30.0	/24	直接连接	VLAN 70	-
172.16.40.0	/24	直接连接	VLAN 80	-
10.1.3.0	/30	ospf	通过 10.1.2.2, FastEthernet0/1	[110/2]

表 3-6 路由关系

四、网络设备选型

4.1 交换机选型

在网络设计过程中，交换机的选型对整体架构的性能、可扩展性、安全性和稳定性起着关键作用。核心层负责处理大流量数据和骨干连接所以应该选择大品牌性能强的一款，汇聚层主要负责流量汇总和路由决策可选择一款中下水品的三层交换机，接入层则提供终端设备的网络接入，选择一款多接口的二层交换机便可。

核心层交换机是网络的骨干，承担高速数据转发任务，因此需要具备高性能和可靠性。它们通常支持高带宽（如万兆、40G 或 100G），以应对大流量需求。此外，核心层交换机应具备高冗余性，确保网络高可用，避免单点故障。冗余电源、热插拔模块以及支持多路由协议（如 OSPF）是核心层交换机的必要功能。在选型时，应重点考虑设备的吞吐量和带宽，确保能够支撑网络流量。如表 4-1 所示：

Cisco Catalyst 9500-24Q		
网络分层位置	第三层	<div>产品图片</div> 
数据传输能力	高达 40 Gbps	
虚拟网络支持	支持	
接口数量	28 个	
数据交换方式	存储-转发模式，支持三层交换模式	
电力需求	400W-800W	
运行条件	工作温度：0° C - 40° C，存储温度：-40° C - 70° C	
接口说明	24 个 40G 光纤端口、4 个以太网接口	
外观规格	44.5 cm（长）x 43.74 cm（宽）x 4.4 cm（高）	
扩展能力	支持堆叠	

表 4-1 核心层交换机选型

汇聚层交换机的选型可以稍微宽松一些，但是依然需要较好的性能，它的任务主要是实现数据的转发、交换和一些策略控制。这一层的交换机需要提供足够

的带宽，以确保接入层之间能够公平共享网络资源并优化流量。汇聚层交换机可以选择中档性能的三层交换机，具备必要的路由功能，并支持流量管理和简单的安全策略。如表 4-2 所示：


Cisco Catalyst 9300-24P		
网络分层位置	第三层	<div>产品图片</div> 
数据传输能力	10/100/1000 Mbps	
虚拟网络支持	支持	
接口数量	24 个	
数据传输方式	全双工	
数据传输能力	480Gbps	
电力需求	1100W，可用的 PoE 的功率 490W	
运行条件	工作温度：0° C - 40° C，存储温度：-40° C - 70° C	
协议支持	支持现有网络大部分协议标准	
接口详情	24 个以太网接口	
外观规格	44.5 cm（长）x 43.7 cm（宽）x 4.4 cm（高）	

表 4-2 汇聚层交换机选型

接入层交换机主要负责连接终端设备，如 PC、打印机和无线接入点等，需求相对简单，因此可以选择二层交换机。二层交换机支持基本的数据转发功能，通常具备 VLAN 和端口聚合等功能，足以满足接入层的基本需求。接入层交换机通常提供多种接口类型，以下这款交换机拥有 48 个千兆以太网端口，4 个千兆光纤端口，支持大规模设备的接入。由于接入层交换机不需要处理复杂的路由功能，选择性能适中的二层交换机即可，既能保证网络的稳定性，又具备较高的性价比，适合大规模部署终端设备。如表 4-3 所示：


Cisco Catalyst 1000-48T-4G-L		
网络分层位置	第二层	产品图片
数据传输能力	10/100/1000 Mbps	
虚拟网络支持	支持	
接口数量	52 个	
数据交换方式	全双工	
背板能力	128 Gbps	
电力需求	370W	
运行条件	工作温度：0° C - 40° C，存储温度：-40° C - 70° C	
协议支持	支持现有网络大部分协议标准	
接口详情	48 个千兆以太网端口，4 个千兆光纤端口	
外观规格	44.5 cm（长）x 44.7 cm（宽）x 4.4 cm（高）	

表 4-3 接入层交换机选型

4.2 路由器选型

路由器在网络中扮演着非常重要的角色。它负责连接不同的网络，比如局域网（LAN）和广域网（WAN），使得数据可以在这些网络之间顺畅传输。路由器会根据数据包的目的地址来决定最佳的传输路径，从而实现数据的快速转发。

此外，路由器还可以管理网络流量，优化带宽使用，确保每个设备都能高效地访问网络。在安全方面，路由器通常内置防火墙功能，可以防止不良数据包入侵网络，保护网络安全。

选择合适的路由器对于提升网络性能和安全性至关重要，尤其是在教育机构这样的环境中，需要同时支持大量用户和设备的连接。因此，路由器的功能和性能直接影响到教学活动的顺利进行和信息交流的有效性。

Cisco Catalyst 8200-1N-8T-4X 路由器在整体网络中起着核心转发作用。它不仅提供高达 8 个千兆以太网端口，支持多设备同时连接，还具备高效的流量管理和优化功能，确保网络性能稳定。此外，路由器集成了先进的安全特性，能够

防御网络攻击，保护敏感数据。作为思科品牌的一部分，Catalyst 8200 系列具有卓越的可靠性和可扩展性，能够灵活适应不断变化的网络需求，确保教育机构在未来的长期投资回报。如表 4-4 所示：

Cisco Catalyst 8200-1N-8T-4X		
数据传输能力	10/100/1000 Mbps	产品图片 
虚拟网络接口	8 个千兆以太网端口	
虚拟网络支持	支持	
接口详情	2 个外部 USB2.0 闪存插槽 1 个 USB 控制台端口 1 个串行控制台端口	
电力需求	320W	
运行条件	工作温度：0° C - 40° C，存储温度：-40° C - 70° C	
外观规格	46.99 cm（长）x 43.82 cm（宽）x 4.45 cm（高）	
网络支持	支持现有网络大部分协议标准	

表 4-4 路由器选型

4.3 服务器选型

服务器的主要作用是集中存储、管理和处理数据，为用户和应用程序提供资源支持。在教育机构中，服务器可以支持在线学习平台、课程管理系统和数据库存储。其运行特征包括高可用性、稳定性和安全性，确保系统能够在高负载下持续运行，同时保护敏感数据不受威胁。此外，服务器通常支持多用户同时访问，提高工作效率。

ASUS TS100-E10-PS4 是一款经济实惠的小型塔式服务器，专为培训机构搭建内部 FTP 和教务系统。它支持最新的处理器和大容量内存，能够满足日常数据处理和存储需求。作为华硕品牌的一部分，华硕提供出色的售后服务和技术支持，确保我们在遇到问题时能够获得及时帮助。非常适合需要高效、可靠解决方案的教育机构和小型企业。如表 4-5 所示：


ASUS TS100-E10-PS4			
设备所属类型	塔式服务器	<div>产品图片</div> 	
设计与外形架构	1U		
处理器数量	支持单个 CPU		
制造技术规范	14nm		
支持的内存上限	64GB		
存储设备的大小	4 个 SATA 硬盘		
连接与通信方式	一个千兆以太网接口		
适应的工作条件	标准环境		
耗电性能指标	350W		
供电方式及配置	AC 电源		
售后保障条款	全国联保，享受三包服务，提供 3 年保修服务		

表 4-5 服务器选型

4.4 网卡选型

ASUS XG-C100C 是一款高性能 PCI Express x4 网络适配器，支持最高 10Gbps 的传输速度，兼容 5Gbps 和 2.5Gbps，适合需要高速网络的环境。它与 Windows 和 Linux 操作系统广泛兼容，并配有散热设计以保持稳定性。如表 4-6 所示：


ASUS XG-C100C		
数据流通速度	10Gbps	产品图片
核心处理单元	Intel X550-AT2 芯片	
通信媒介形式	3/4/5/6 类 UTP	
数据交互通道	PCIe 3.0 x4 接口	
协议支持规范	支持 802.3ab（1000BASE-T）标准	
推荐使用场景	工作站，服务器，台式电脑	

表 4-6 网卡选型

4.5 PC 选型

华硕破晓 X 是一款专为创意专业人士和商用用户设计的高性能台式机，搭载第 14 代英特尔酷睿 i5（i5-14400）处理器。它拥有 10 个核心和 16 个线程，能够轻松处理多任务和复杂应用程序，适合视频编辑、图形设计和数据处理等需求。

这款台式机配备 16GB 的 DDR4 内存，提供充足的运行空间，确保软件运行流畅。集成的 Intel UHD Graphics 显卡，适合日常办公和轻度的图形处理，满足一般用户的需求。

在接口方面，华硕破晓 X 设计了丰富的 I/O 接口配置，包括 2 个 USB 3.2 Gen 1、2 个 USB 3.2 Gen 2 和 4 个 USB 2.0 接口，方便连接各种外部设备，提升工作效率。如表 4-7 所示：

华硕破晓 X 14 代酷睿 i5（i5 14400）		
设备分类	商用电脑	产品图片
处理器系列	英特尔 酷睿 i5 14 代系列	
内存大小	16GB	
图形处理单元	集成显卡	
输入输出端口	2xUSB3. 2-Gen1, 2xUSB3. 2-Gen2, 4xUSB2. 0	
核心与线程	十核心/十六线程	
冷却系统方法	双风扇（系统风扇+CPU 风扇）	

表 4-7 PC 选型

五、网络设备配置

5.1 交换机的配置

5.1.1 核心层交换机配置

核心交换机 HX-SW-A 的配置如下：

(1) 交换机命名 HX-SW-A 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升交换机的安全性，防止未经授权的访问和操作。

```
Switch(config)#hostname HX-SW-A
```

```
HX-SW-A(config)#line console 0 (设置控制台密码)
```

```
HX-SW-A(config-line)#password 55665566
```

```
HX-SW-A(config-line)#login
```

```
HX-SW-A(config-line)#exit
```

```
HX-SW-A(config)#line vty 0 4 (设置远程访问密码)
```

```
HX-SW-A(config-line)#password 55665566
```

```
HX-SW-A(config-line)#login
```

```
HX-SW-A(config-line)#exit
```

```
HX-SW-A(config)#enable password 55665566 (设置特权模式密码)
```

(2) 交换机 HX-SW-A 的 Fa 0/3 端口配置 IP，将端口的交换机模式变为路由接口，并配置小网段，保持网络精简性，主要用于实现网络通信、远程管理、数据交换以及路由功能等。

```
HX-SW-A(config)#interface fastEthernet 0/3
```

```
HX-SW-A(config-if)#no switchport (将端口的交换机模式变为路由接口)
```

```
HX-SW-A(config-if)#ip address 10.1.1.1 255.255.255.252 (配置 IP 地址子网)
```

```
HX-SW-A(config-if)#no shutdown (启用接口)
```

(3) 交换机 HX-SW-A 的 Fa 0/1-2 端口配置 trunk 允许 vlan10 - 80 通过，设置接口的 trunk 封装方式为 IEEE 802.1Q 允许在同一物理链路上传输多个 VLAN

的流量，通过这种方式配置 Trunk 端口，有助于高效地支持多个 VLAN 的通信，同时也能确保网络流量的优化和管理，避免不必要的带宽浪费，并提高网络安全性。

```
HX-SW-A(config)#interface range fastEthernet 0/1-2
```

```
HX-SW-A(config-if-range)#switchport trunk encapsulation dot1q
```

```
HX-SW-A(config-if-range)#switchport trunk switchport trunk allowed vlan  
10-80
```

(4) 在交换机 HX-SW-A 创建 8 个 vlan 分别为 10 20 30 40 50 60 70 80 并配置 IP 地址作为内网网关，主要目的是为了实现不同 VLAN 之间的通信和网络分隔，同时为每个 VLAN 提供一个网关 IP 地址，便于设备与外部网络的通信。

```
HX-SW-A(config)#vlan 10
```

```
HX-SW-A(config)#vlan 20
```

```
HX-SW-A(config)#vlan 30
```

```
HX-SW-A(config)#vlan 40
```

```
HX-SW-A(config)#vlan 50
```

```
HX-SW-A(config)#vlan 60
```

```
HX-SW-A(config)#vlan 70
```

```
HX-SW-A(config)#vlan 80
```

```
HX-SW-A(config)#interface vlan 10
```

```
HX-SW-A(config-if)#ip address 192.168.10.254 255.255.255.0
```

```
HX-SW-A(config-if)#interface vlan 20
```

```
HX-SW-A(config-if)#ip address 192.168.20.254 255.255.255.0
```

```
HX-SW-A(config-if)#interface vlan 30
```

```
HX-SW-A(config-if)#ip address 192.168.30.254 255.255.255.0
```

```
HX-SW-A(config-if)#interface vlan 40
```

```
HX-SW-A(config-if)#ip address 192.168.40.254 255.255.255.0
```

```
HX-SW-A(config-if)#interface vlan 50
```

```
HX-SW-A(config-if)#ip address 172.16.10.254 255.255.255.0
```

```
HX-SW-A(config-if)#interface vlan 60
HX-SW-A(config-if)#ip address 172.16.20.254 255.255.255.0
HX-SW-A(config-if)#interface vlan 70
HX-SW-A(config-if)#ip address 172.16.30.254 255.255.255.0
HX-SW-A(config-if)#interface vlan 80
HX-SW-A(config-if)#ip address 172.16.40.254 255.255.255.0
HX-SW-A(config-if)#ex
```

(5) 交换机 HX-SW-A 配置 dhcp 自动 ip 地址分配, 是为了让交换机为连接到交换机端口的设备自动分配 IP 地址、子网掩码、默认网关等网络配置信息。DHCP 使得设备在连接到网络时能够自动获取所需的网络配置, 简化了网络管理和设备配置的工作。

```
HX-SW-A(config)#ip routing
HX-SW-A(config)#ip dhcp pool VLAN10
HX-SW-A(dhcp-config)#network 192.168.10.0 255.255.255.0 (配置地址池)
HX-SW-A(dhcp-config)#default-router 192.168.10.254 (配置网关)
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 (配置 DNS 为中国移动 DNS 服务器地址)
HX-SW-A(dhcp-config)#exit
HX-SW-A(config)#ip dhcp pool VLAN20
HX-SW-A(dhcp-config)#network 192.168.20.0 255.255.255.0 (配置地址池)
HX-SW-A(dhcp-config)#default-router 192.168.20.254 (配置网关)
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 (配置 DNS 为中国移动 DNS 服务器地址)
HX-SW-A(dhcp-config)#exit
HX-SW-A(dhcp-config)#ip dhcp pool VLAN30
HX-SW-A(dhcp-config)#network 192.168.30.0 255.255.255.0 (配置地址池)
HX-SW-A(dhcp-config)#default-router 192.168.30.254 (配置网关)
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 (配置 DNS 为中国移动 DNS
```

服务器地址)

```
HX-SW-A(dhcp-config)#exit
```

```
HX-SW-A(dhcp-config)#ip dhcp pool VLAN40
```

```
HX-SW-A(dhcp-config)#network 192.168.40.0 255.255.255.0 （配置地址池）
```

```
HX-SW-A(dhcp-config)#default-router 192.168.40.254 （配置网关）
```

```
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 （配置 DNS 为中国移动 DNS  
服务器地址）
```

```
HX-SW-A(dhcp-config)#exit
```

```
HX-SW-A(dhcp-config)#ip dhcp pool VLAN50
```

```
HX-SW-A(dhcp-config)#network 172.16.10.0 255.255.255.0 （配置地址池）
```

```
HX-SW-A(dhcp-config)#default-router 172.16.10.254
```

```
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 （配置 DNS 为中国移动 DNS  
服务器地址）
```

```
HX-SW-A(dhcp-config)#exit
```

```
HX-SW-A(dhcp-config)#ip dhcp pool VLAN60
```

```
HX-SW-A(dhcp-config)#network 172.16.20.0 255.255.255.0 （配置地址池）
```

```
HX-SW-A(dhcp-config)#default-router 172.16.20.254 （配置网关）
```

```
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 （配置 DNS 为中国移动 DNS  
服务器地址）
```

```
HX-SW-A(dhcp-config)#exit
```

```
HX-SW-A(dhcp-config)#ip dhcp pool VLAN70
```

```
HX-SW-A(dhcp-config)#network 172.16.30.0 255.255.255.0 （配置地址池）
```

```
HX-SW-A(dhcp-config)#default-router 172.16.30.254 （配置网关）
```

```
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 （配置 DNS 为中国移动 DNS  
服务器地址）
```

```
HX-SW-A(dhcp-config)#exit
```

```
HX-SW-A(dhcp-config)#ip dhcp pool VLAN80
```

```
HX-SW-A(dhcp-config)#network 172.16.40.0 255.255.255.0 （配置地址池）
```

```
HX-SW-A(dhcp-config)#default-router 172.16.40.254 （配置网关）
```

```
HX-SW-A(dhcp-config)#dns-server 218.201.96.130 （配置 DNS 为中国移动 DNS 服务器地址）
```

```
HX-SW-A(dhcp-config)#exit
```

（6）交换机 HX-SW-A 配置启用编号为 1 的 OSPF 路由进程并宣告其下方主机网段和与路由器相连端口网段，保持内外网互通。

```
HX-SW-A(config)#router ospf 1
```

```
HX-SW-A(config-router)#network 10.1.1.1 0.0.0.3 area 0
```

```
HX-SW-A(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 192.168.30.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 192.168.40.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 172.16.10.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 172.16.20.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 172.16.30.0 0.0.0.255 area 0
```

```
HX-SW-A(config-router)#network 172.16.40.0 0.0.0.255 area 0
```

核心交换机 HX-SW-B 的配置如下：

（1）交换机命名 HX-SW-B 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升交换机的安全性，防止未经授权的访问和操作。

```
Switch(config)#hostname HX-SW-B
```

```
HX-SW-B(config)#line console 0 （设置控制台密码）
```

```
HX-SW-B(config-line)#password 55665566
```

```
HX-SW-B(config-line)#login
```

```
HX-SW-B(config-line)#exit
```

```
HX-SW-B(config)#line vty 0 4 （设置远程访问密码）
```

```
HX-SW-B(config-line)#password 55665566
```

```
HX-SW-B(config-line)#login
```



```
HX-SW-B(config-line)#exit
```

```
HX-SW-B(config)#enable password 55665566（设置特权模式密码）
```

（2）交换机 HX-SW-B 的 Fa 0/1 端口配置 IP，将端口的交换机模式变为路由接口，并配置小网段，保持网络精简性，主要用于实现网络通信、远程管理、数据交换以及路由功能等。

```
HX-SW-B(config)#interface fastEthernet 0/1
```

```
HX-SW-B(config-if)#no switchport
```

```
HX-SW-B(config-if)#ip address 10.1.2.1 255.255.255.252
```

```
HX-SW-B(config-if)#no shutdown
```

（3）交换机 HX-SW-B 创建 vlan 10 并配置其 IP 地址作为内网网关，主要目的是为了实现不同 VLAN 之间的通信和网络分隔，同时为每个 VLAN 提供一个网关 IP 地址，便于设备与外部网络的通信。

```
HX-SW-B(config)#vlan 10
```

```
HX-SW-B(config-vlan)#ex
```

```
HX-SW-B(config)#interface vlan 10
```

```
HX-SW-B(config-if)#ip address 10.199.199.254 255.255.255.0
```

```
HX-SW-B(config-if)#no shutdown
```

```
HX-SW-B(config-if)#ex
```

（4）交换机 HX-SW-B 的接口 FA 0/2 配置 trunk 允许 vlan10 通过，设置接口的 trunk 封装方式为 IEEE 802.1Q 允许在同一物理链路上传输多个 VLAN 的流量，通过这种方式配置 Trunk 端口，有助于高效地支持多个 VLAN 的通信，同时也能确保网络流量的优化和管理，避免不必要的带宽浪费，并提高网络安全性。

```
HX-SW-B(config)#interface fastEthernet 0/2
```

```
HX-SW-B(config-if)#switchport trunk encapsulation dot1q
```

```
HX-SW-B(config-if)#switchport trunk allowed vlan 10
```

```
HX-SW-B(config-if)#ex
```

（5）交换机 HX-SW-B 配置启用编号为 1 的 OSPF 路由进程并宣告其下方主机网段和与路由器相连端口网段，保持内外网互通

```
HX-SW-B(config)#router ospf 1
```

```
HX-SW-B(config-router)#network 10.199.199.0 0.0.0.255 area 0
```

```
HX-SW-B(config-router)#network 10.1.2.1 0.0.0.3 area 0
```

5.1.2 汇聚层交换机配置

汇聚交换机 HJ-SW-A 的配置如下：

(1) 交换机命名 HJ-SW-A 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升交换机的安全性，防止未经授权的访问和操作。

```
HJ-SW-A(config)#line console 0 (设置控制台密码)
```

```
HJ-SW-A(config-line)#password 55665566
```

```
HJ-SW-A(config-line)#login
```

```
HJ-SW-A(config-line)#exit
```

```
HJ-SW-A(config)#line vty 0 4 (设置远程访问密码)
```

```
HJ-SW-A(config-line)#password 55665566
```

```
HJ-SW-A(config-line)#login
```

```
HJ-SW-A(config-line)#exit
```

```
HJ-SW-A(config)#enable password 55665566 (设置特权模式密码)
```

(2) 交换机 HJ-SW-A 创建 vlan 10 20 30 40，通过在汇聚层交换机上创建不同的 VLAN，网络管理员可以将不同部门或不同类型的流量隔离开来，减少网络冲突，提高管理灵活性。

```
HJ-SW-A(config)#vlan 10
```

```
HJ-SW-A(config)#vlan 20
```

```
HJ-SW-A(config)#vlan 30
```

```
HJ-SW-A(config)#vlan 40
```

```
HJ-SW-A(config)#ex
```

(3) 交换机 HJ-SW-A Fa0/1-2 端口配置 trunk 模式并放行 vlan10-80，能够承载 VLAN 10 到 VLAN 80 之间的流量，并且使用 802.1Q 标记协议来区分不同的 VLAN

流量。

```
HJ-SW-A(config)#interface range fa0/1-2
```

```
HJ-SW-A(config-if-range)#switchport trunk encapsulation dot1q
```

```
HJ-SW-A(config-if-range)#switchport mode trunk
```

```
HJ-SW-A(config-if-range)#switchport trunk allowed vlan 10-80
```

```
HJ-SW-A(config-if-range)#ex
```

(4) 交换机 HJ-SW-A Fa0/23-24 端口配置链路聚合, 通过这些配置, Fa 0/23 和 Fa 0/24 被聚合为一个逻辑端口 Port-Channel 1, 并且这个逻辑端口被配置为 Trunk 端口, 支持多个 VLAN 的流量传输, 提供了更高的带宽和冗余。

```
HJ-SW-A(config)#interface range fastEthernet 0/23-24
```

```
HJ-SW-A(config-if-range)#channel-group 1 mode on (接口添加端口通道组 1)
```

```
HJ-SW-A(config-if-range)#exit
```

```
HJ-SW-A(config)#int port-channel 1 (进入端口通道组 1)
```

```
HJ-SW-A(config-if)#switchport trunk encapsulation dot1q
```

```
HJ-SW-A(config-if)#switchport mode trunk
```

```
HJ-SW-A(config-if)#ex
```

汇聚交换机 HJ-SW-B 的配置如下:

(1) 交换机命名 HJ-SW-B 并配置控制台, 远程访问和特权模式密码保护, 这些配置能有效提升交换机的安全性, 防止未经授权的访问和操作。

```
Switch(config)#hostname HJ-SW-B
```

```
HJ-SW-B(config)#line console 0 (设置控制台密码)
```

```
HJ-SW-B(config-line)#password 55665566
```

```
HJ-SW-B(config-line)#login
```

```
HJ-SW-B(config-line)#exit
```

```
HJ-SW-B(config)#line vty 0 4 (设置远程访问密码)
```

```
HJ-SW-B(config-line)#password 55665566
```

```
HJ-SW-B(config-line)#login
```

```
HJ-SW-B(config-line)#exit
```

```
HJ-SW-B(config)#enable password 55665566（设置特权模式密码）
```

（2）交换机 HJ-SW-B 创建 vlan 50 60 70 80，通过在汇聚层交换机上创建不同的 VLAN，网络管理员可以将不同部门或不同类型的流量隔离开来，减少网络冲突，提高管理灵活性。

```
HJ-SW-B(config)#vlan 50
```

```
HJ-SW-B(config)#vlan 60
```

```
HJ-SW-B(config)#vlan 70
```

```
HJ-SW-B(config)#vlan 80
```

```
HJ-SW-B(config-vlan)#ex
```

（3）交换机 HJ-SW-B Fa0/1-2 端口配置 trunk 模式并放行 vlan10-80，能够承载 VLAN 10 到 VLAN 80 之间的流量，并且使用 802.1Q 标记协议来区分不同的 VLAN 流量。

```
HJ-SW-B(config)#int range fa0/1-2
```

```
HJ-SW-B(config-if-range)#switchport trunk encapsulation dot1q
```

```
HJ-SW-B(config-if-range)#switchport mode trunk
```

```
HJ-SW-B(config-if-range)#switchport trunk allowed vlan 10-80
```

```
HJ-SW-B(config-if-range)#ex
```

（4）交换机 HJ-SW-B Fa0/23-24 端口配置链路聚合，通过这些配置，Fa 0/23 和 Fa 0/24 被聚合为一个逻辑端口 Port-Channel 1，并且这个逻辑端口被配置为 Trunk 端口，支持多个 VLAN 的流量传输，提供了更高的带宽和冗余。

```
HJ-SW-B(config)#interface range fastEthernet 0/23-24
```

```
HJ-SW-B(config-if-range)#channel-group 1 mode on（接口添加到通道组 1）
```

```
HJ-SW-B(config-if-range)#exit
```

```
HJ-SW-B(config)#int port-channel 1（进入端口通道组 1）
```

```
HJ-SW-B(config-if)#switchport trunk encapsulation dot1q
```

```
HJ-SW-B(config-if)#switchport mode trunk
```

```
HJ-SW-B(config-if)#ex
```

5.1.3 接入层交换机配置

接入层交换机 JR-SW-A 的配置如下：

(1) 交换机命名 JR-SW-A 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升交换机的安全性，防止未经授权的访问和操作。

```
Switch(config)#hostname JR-SW-A
```

```
JR-SW-A(config)#line console 0 (设置控制台密码)
```

```
JR-SW-A(config-line)#password 55665566
```

```
JR-SW-A(config-line)#login
```

```
JR-SW-A(config-line)#exit
```

```
JR-SW-A(config)#line vty 0 4 (设置远程访问密码)
```

```
JR-SW-A(config-line)#password 55665566
```

```
JR-SW-A(config-line)#login
```

```
JR-SW-A(config-line)#exit
```

```
JR-SW-A(config)#enable password 55665566 (设置特权模式密码)
```

(2) 交换机 JR-SW-A 创建 vlan 10 20 30 40 并将交换机 JR-SW-A 的接口 F0/2-4 加入 vlan10,接口 F0/5-8 加入 vlan20,接口 F0/9-12 加入 vlan30,接口 F0/13-16 加入 vlan40,使得这些端口成为各自 VLAN 的接入端口。

```
JR-SW-A(config)#vlan 10
```

```
JR-SW-A(config-vlan)#vlan 20
```

```
JR-SW-A(config-vlan)#vlan 30
```

```
JR-SW-A(config-vlan)#vlan 40
```

```
JR-SW-A(config-vlan)#exit
```

```
JR-SW-A(config)#interface range fa0/2-4
```

```
JR-SW-A(config-if-range)#switchport mode access
```

```
JR-SW-A(config-if-range)#switchport access vlan 10
```

```
JR-SW-A(config-if-range)#exit
```

```
JR-SW-A(config)#interface range fa0/5-8
```

```
JR-SW-A(config-if-range)#switchport mode access
JR-SW-A(config-if-range)#switchport access vlan 20
JR-SW-A(config-if-range)#exit
JR-SW-A(config)#interface range fa0/9-12
JR-SW-A(config-if-range)#switchport mode access
JR-SW-A(config-if-range)#switchport access vlan 30
JR-SW-A(config-if-range)#exit
JR-SW-A(config)#interface range fa0/13-16
JR-SW-A(config-if-range)#switchport mode access
JR-SW-A(config-if-range)#switchport access vlan 40
JR-SW-A(config-if-range)#exit
```

(3) 交换机 JR-SW-A Fa0/1 端口配置 trunk 模式并放行 vlan10-40, 这样, Fa 0/1 端口可以同时承载多个 VLAN 的流量, 并使用 VLAN 标签来区分不同 VLAN 的数据。

```
JR-SW-A(config)#interface fastEthernet 0/1
JR-SW-A(config-if)#switchport mode trunk
JR-SW-A(config-if)#switchport trunk allowed vlan 10-40
JR-SW-A(config-if)#ex
```

接入层交换机 JR-SW-B 的配置如下:

(1) 交换机命名 JR-SW-B 并配置控制台, 远程访问和特权模式密码保护, 这些配置能有效提升交换机的安全性, 防止未经授权的访问和操作。

```
JR-SW-B(config)#line console 0 (设置控制台密码)
JR-SW-B(config-line)#password 55665566
JR-SW-B(config-line)#login
JR-SW-B(config-line)#exit
JR-SW-B(config)#line vty 0 4 (设置远程访问密码)
JR-SW-B(config-line)#password 55665566
```

```
JR-SW-B(config-line)#login
```

```
JR-SW-B(config-line)#exit
```

```
JR-SW-B(config)#enable password 55665566（设置特权模式密码）
```

（2）交换机 JR-SW-B 创建 vlan 50 60 70 80 并将交换机 JR-SW-A 的接口 F0/2-4 加入 vlan50,接口 F0/5-8 加入 vlan60,接口 F0/9-12 加入 vlan70,接口 F0/13-16 加入 vlan80, 使得这些端口成为各自 VLAN 的接入端口。

```
JR-SW-B(config)#vlan 50
```

```
JR-SW-B(config-vlan)#vlan 60
```

```
JR-SW-B(config-vlan)#vlan 70
```

```
JR-SW-B(config-vlan)#vlan 80
```

```
JR-SW-B(config-vlan)#exit
```

```
JR-SW-B(config)#interface range fa0/2-4
```

```
JR-SW-B(config-if-range)#switchport mode access
```

```
JR-SW-B(config-if-range)#switchport access vlan 50
```

```
JR-SW-B(config-if-range)#exit
```

```
JR-SW-B(config)#interface range fa0/5-8
```

```
JR-SW-B(config-if-range)#switchport mode access
```

```
JR-SW-B(config-if-range)#switchport access vlan 60
```

```
JR-SW-B(config-if-range)#exit
```

```
JR-SW-B(config)#interface range fa0/9-12
```

```
JR-SW-B(config-if-range)#switchport mode access
```

```
JR-SW-B(config-if-range)#switchport access vlan 70
```

```
JR-SW-B(config-if-range)#exit
```

```
JR-SW-B(config)#interface range fa0/13-16
```

```
JR-SW-B(config-if-range)#switchport mode access
```

```
JR-SW-B(config-if-range)#switchport access vlan 80
```

```
JR-SW-B(config-if-range)#exit
```

（3）交换机 JR-SW-A Fa0/1 端口配置 trunk 模式并放行 vlan10-40, 这样, Fa 0/1

端口可以同时承载多个 VLAN 的流量，并使用 VLAN 标签来区分不同 VLAN 的数据。

```
JR-SW-B(config)#interface fastEthernet 0/1
```

```
JR-SW-B(config-if)#switchport mode trunk
```

```
JR-SW-B(config-if)#switchport trunk allowed vlan 50-80
```

```
JR-SW-B(config-if)#ex
```

接入层交换机 JR-SW-C 的配置如下：

(1) 交换机命名 JR-SW-C 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升交换机的安全性，防止未经授权的访问和操作。

```
Switch(config)#hostname JR-SW-C
```

```
JR-SW-C(config)#line console 0 (设置控制台密码)
```

```
JR-SW-C(config-line)#password 55665566
```

```
JR-SW-C(config-line)#login
```

```
JR-SW-C(config-line)#exit
```

```
JR-SW-C(config)#line vty 0 4 (设置远程访问密码)
```

```
JR-SW-C(config-line)#password 55665566
```

```
JR-SW-C(config-line)#login
```

```
JR-SW-C(config-line)#exit
```

```
JR-SW-C(config)#enable password 55665566 (设置特权模式密码)
```

(2) 交换机 JR-SW-C 创建 vlan 10 并将交换机 JR-SW-C 的接口 fa0/2-3 加入 vlan10，使得端口成为 VLAN 的接入端口。

```
JR-SW-C(config)#vlan 10
```

```
JR-SW-C(config-vlan)#exit
```

```
JR-SW-C(config-if-range)#switchport mode access
```

```
JR-SW-C(config-if-range)#switchport access vlan 10
```

```
JR-SW-C(config-if-range)#exit
```

(3) 交换机 JR-SW-C Fa0/1 端口配置 trunk 模式并放行 vlan10，这样，Fa 0/1 端

口可以同时承载多个 VLAN 的流量,并使用 VLAN 标签来区分不同 VLAN 的数据。

```
JR-SW-C(config)#interface fastEthernet 0/1
```

```
JR-SW-C(config-if)#switchport mode trunk
```

```
JR-SW-C(config-if)#switchport trunk allowed vlan 10
```

5.2 路由器的配置

路由器 A 的配置如下:

(1) 路由器命名 RA 并配置控制台, 远程访问和特权模式密码保护, 这些配置能有效提升路由器的安全性, 防止未经授权的访问和操作。

```
Router(config)hostname RA
```

```
RA(config)#line console 0 (设置控制台密码)
```

```
RA(config-line)#password 55665566
```

```
RA(config-line)#login
```

```
RA(config-line)#exit
```

```
RA(config)#line vty 0 4 (设置远程访问密码)
```

```
RA(config-line)#password 55665566
```

```
RA(config-line)#login
```

```
RA(config-line)#exit
```

```
RA(config)#enable password 55665566 (设置特权模式密码)
```

(2) 路由器 A 的接口 Fa0/0 Fa0/1 Se0/0/0 端口配置 IP, 所有接口都配置了适当的 IP 地址和子网掩码, 并确保接口处于启用状态 (no shutdown)。这为路由器与其他网络设备之间的通信提供了基础配置。

```
RA(config)#int fastEthernet 0/0
```

```
RA(config-if)#ip address 10.1.1.2 255.255.255.252
```

```
RA(config-if)#no shutdown
```

```
RA(config)#int fastEthernet 0/1
```

```
RA(config-if)#ip address 10.1.2.2 255.255.255.252
```

```
RA(config-if)#no shutdown
```

```
RA(config)#interface serial 0/0/0
```

```
RA(config-if)#ip address 8.138.176.1 255.255.255.0
```

```
RA(config-if)#no shutdown
```

(3) 路由器 A 配置启用编号为 1 的 OSPF 路由进程并宣告其下方主机网段和与路由器相连端口网段, 保持内外网互通。

```
RA(config)#router ospf 1
```

```
RA(config-router)#network 10.1.1.2 0.0.0.3 area 0
```

```
RA(config-router)#network 8.138.176.0 0.0.0.255 area 0
```

```
RA(config-router)#network 10.1.2.2 0.0.0.3 area 0
```

(4) RA 上配置地址转换, 将服务器的 80 端口, 映射到 RA 的出口的 80 端口上, 首先创建 ACL 匹配内网流量, 然后使用外网地址池 8.138.176.3 和 8.138.176.4 IP 对内网流量进行动态 NAT 转换, 最后使用访问控制列表 10 匹配的内网流量, 通过 NAT 地址池 ningzifan 转换到外网 IP 并加入端口规则中, 本段命令可实现外部用户通过配置的外网 IP 访问内部服务器。

```
RA(config)access-list 10 permit 10.199.199.0 0.0.0.255 (创建 ACL)
```

```
RA(config)#ip nat outside source static tcp 10.199.199.1 80 8.138.176.1 80 (实现外部用户通过外网 IP (8.138.176.1) 访问内部服务器)
```

```
RA(config)#ip nat pool ningzifan 8.138.176.3 8.138.176.4 netmask 255.255.255.0 (使用这些公网 IP 对内网流量进行动态 NAT 转换)
```

```
RA(config)#ip nat inside source list 10 pool ningzifan overload
```

(overload: 启用地址复用, 即多个内网设备可以共享同一个公网 IP 出网)

```
RA(config)#interface fastEthernet 0/0
```

```
RA(config-if)#ip nat outside (加入内网端口规则)
```

```
RA(config-if)#ex
```

```
RA(config)#int
```

```
RA(config)#interface fastEthernet 0/1
```

```
RA(config-if)#ip nat outside (加入内网端口规则)
```

```
RA(config-if)#ex
```

```
RA(config)#interface serial 0/0/0
```

```
RA(config-if)#ip nat inside （加入外网端口规则）
```

路由器 B 的配置如下：

（1）路由器命名 RB 并配置控制台，远程访问和特权模式密码保护，这些配置能有效提升路由器的安全性，防止未经授权的访问和操作。

```
Router(config)hostname RB
```

```
RB(config)#line console 0 （设置控制台密码）
```

```
RB(config-line)#password 55665566
```

```
RB(config-line)#login
```

```
RB(config-line)#exit
```

```
RB(config)#line vty 0 4 （设置远程访问密码）
```

```
RB(config-line)#password 55665566
```

```
RB(config-line)#login
```

```
RB(config-line)#exit
```

```
RB(config)#enable password 55665566 （设置特权模式密码）
```

（2）路由器 B 的接口 Fa0/0 Se0/0/0 端口配置 IP，所有接口都配置了适当的 IP 地址和子网掩码，并确保接口处于启用状态（no shutdown）。这为路由器与其他网络设备之间的通信提供了基础配置。

```
RB(config)#interface serial 0/0/0
```

```
RB(config-if)#ip address 8.138.176.2 255.255.255.0
```

```
RB(config-if)#no shutdown
```

```
RB(config-if)#ex
```

```
RB(config)#interface fastEthernet 0/0
```

```
RB(config-if)#ip address 8.138.177.254 255.255.255.0
```

```
RB(config-if)#no shutdown
```

```
RB(config-if)#ex
```

（3）路由器 B 配置启用编号为 1 的 OSPF 路由进程并宣告其下方主机网段和与

路由器相连端口网段，保持内外网互通。

```
RB(config)#router ospf 1
```

```
RB(config-router)#network 8.138.176.2 0.0.0.255 area 0
```

```
RB(config-router)#network 8.138.177.254 0.0.0.255 area 0
```

```
RB(config-if)#exit
```

5.3 网络测试

网络测试在验收中的作用至关重要，它帮助确保网络的各项配置、性能和稳定性符合预期需求。在网络建设完成后，验收测试通过使用诸如 ping、带宽测试、延迟测量、丢包率检测等方法，验证网络设备的连接性、吞吐量和响应时间，确保网络设备间的通信畅通无阻，网络带宽和延迟满足业务要求，同时确认网络安全措施（如防火墙和访问控制）有效运行。通过这些测试，可以提前发现潜在的性能瓶颈、配置错误或硬件故障，从而确保网络能够稳定、安全地支持预期的业务应用。

ping 命令是一种网络诊断工具，用于测试设备之间的网络连接性和响应速度。通过向目标设备发送 ICMP 回显请求（Echo Request）并等待 ICMP 回显应答（Echo Reply），ping 命令可以确认目标设备是否在线，是否能够正常响应网络请求。

除了验证设备的连通性外，ping 还能够测量网络延迟（即请求和应答之间的时间差），并帮助诊断网络中的丢包情况。

通过多次 ping 测试，用户还可以检测网络的稳定性、带宽瓶颈或其他潜在问题，是网络故障排查和性能优化中常用的基础工具。

（1）办公室访问招生处和实训四层，如图 5-1 所示：

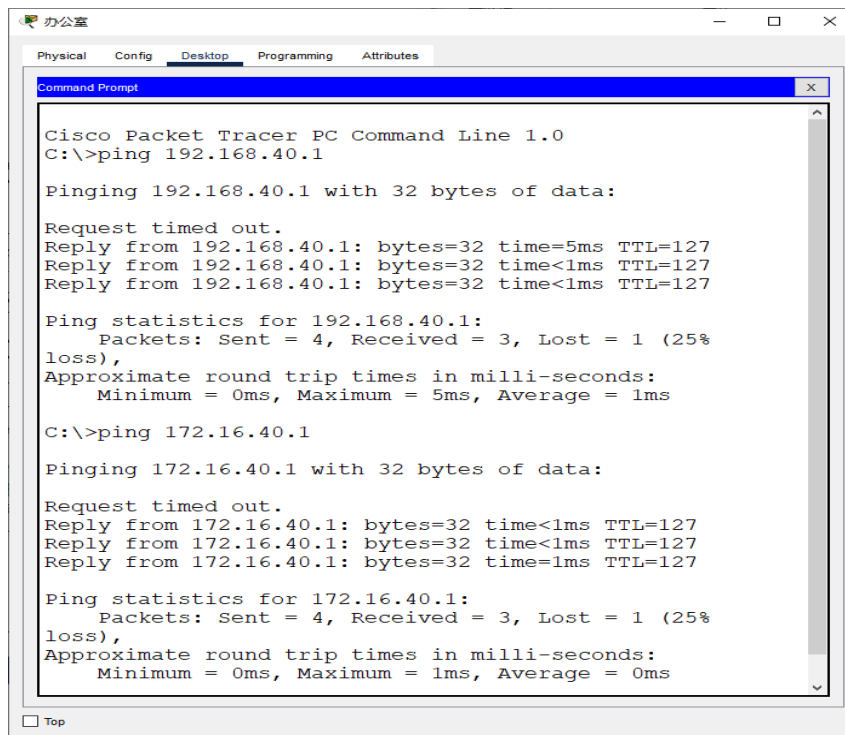


图 5-1 办公室访问招生处和实训四层

(2) 财务处访问教务处和实训二层，如图 5-2 所示：

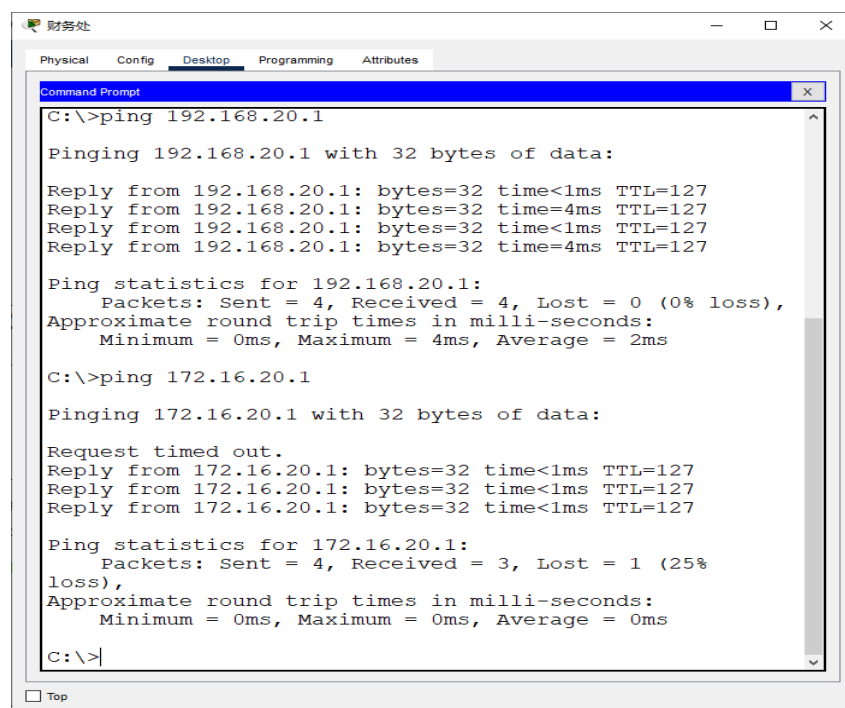


图 5-2 财务处访问教务处部和实训二层

(3) 实训三层访问实训一层和 FTP 服务器。如图 5-3 所示：

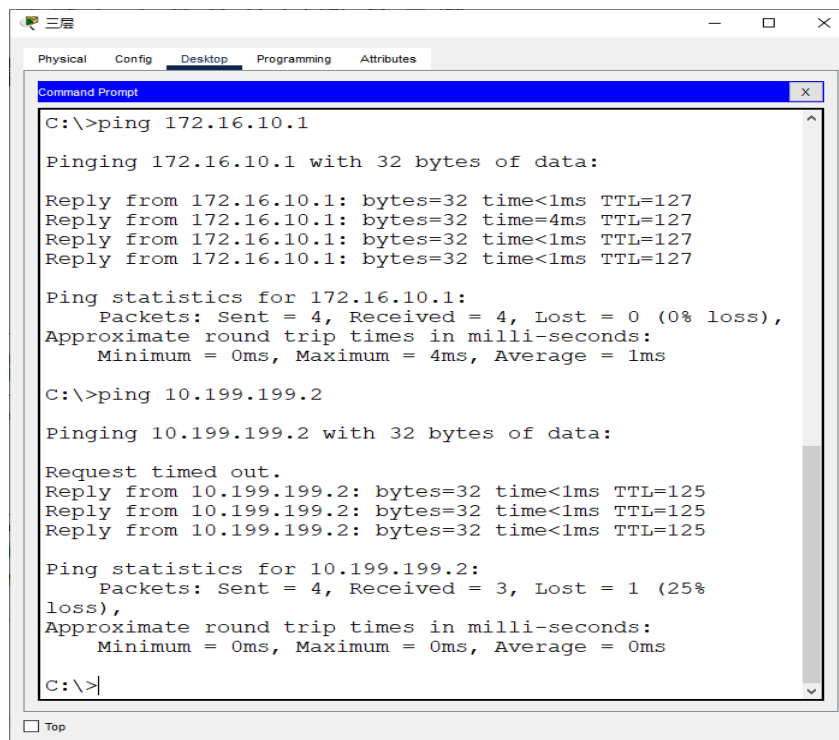


图 5-3 实训三层访问实训一层和 FTP 服务器

(4) 教务处访问 FTP 服务器和教务系统服务器。如图 5-4 所示：

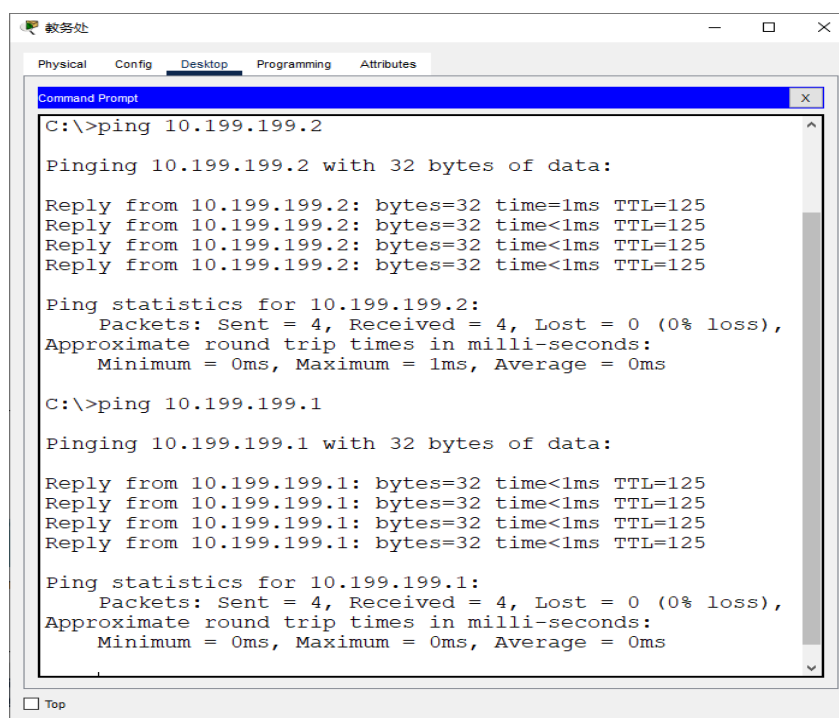


图 5-4 教务处访问 FTP 服务器和教务系统服务器

(5) 实训四层连接外网，如图 5-5 所示：

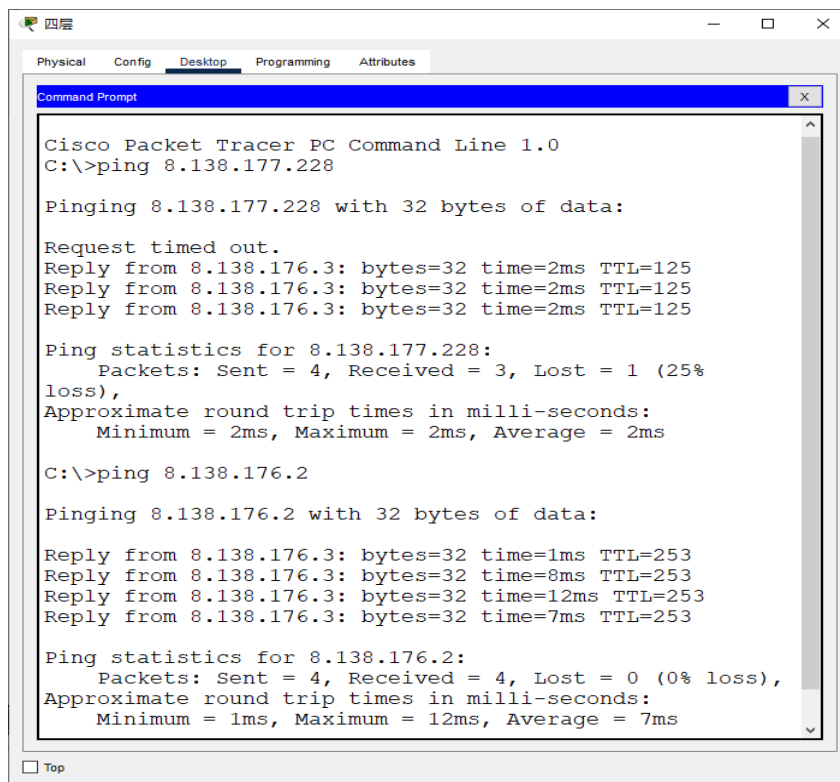


图 5-5 实训四层连接外网

5.4 服务器的配置

我们在服务器搭建了 Ubuntu 操作系统，Ubuntu 操作系统以其用户友好的界面和强大的稳定性而著称，适合新手和有经验的用户。它拥有丰富的软件库，提供广泛的应用程序和工具，使得安装和使用变得简单。此外，Ubuntu 具有强大的社区支持，用户可以轻松找到解决问题的资源和教程。其定期更新和长期支持版本（LTS）确保了系统的安全性和性能，适合个人用户、开发者和企业环境。总之，Ubuntu 结合了易用性、灵活性和安全性，成为许多用户的首选操作系统。

5.4.1 Web 服务器

WEB 服务器是一种计算机系统或软件，用于存储和传输网页内容，处理客户端请求并返回相应的网页，尤其在培训机构中，它支持在线课程、学习管理系统和资源共享，提升学习体验和管理效率。安装 Web 服务器的过程如下：

(1) 下载 Tomcat 安装包

```
[root@JW-Server]#wget https://dlcdn.apache.org/tomcat/tomcat-11/
```

--2024-11-24 00:47:58--

<https://dlcdn.apache.org/tomcat/tomcat-11/v11.0.0/bin/>

正在解析主机 dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132,
2a04:4e42::644

正在连接 dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... 已
连接。

(2) 解压 Tomcat 安装包

```
[root@JW-Server]# unzip apache-tomcat-9.0.93
```

```
Archive: apache-tomcat-9.0.93.zip
```

```
creating: apache-tomcat-9.0.93/
```

```
inflating: apache-tomcat-9.0.93/BUILDING.txt
```

```
creating: apache-tomcat-9.0.93/work/
```

(3) 安装 Java11

```
[root@JW-Server]# apt install openjdk-11-jdk
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
Reading state information... Done
```

```
Openjdk-11-jdk is already the newest version (11.0.25+9-1ubuntu1-24.04)
```

(4) 配置防火墙运行 8080 端口通过

```
[root@JW-Server]# ufw allow 8080/tcp
```

```
Skipping adding existing rule
```

```
Skipping adding existing rule (v6)
```

(5) 启动 tomcat

```
[root@JW-Server]# /opt/tomcat/apache-tomcat-9.0.93/bin# ./startup.sh
```

```
Using CATALINA_BASE: /opt/tomcat/apache-tomcat-9.0.93
```

```
Using CATALINA_HOME: /opt/tomcat/apache-tomcat-9.0.93
```

```
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.93/temp
```

```
Using JRE_HOME: /usr
```



```
Using CLASSPATH:      /opt/tomcat/apache-tomcat-9.0.93/bin/
:/opt/tomcat/apache-tomcat-9.0.93/bin/tomcat-juli.jar
USing CATALINA_OPTS:
Tomcat started.
```

(6) 测试，在浏览器中输入 `http://10.199.199.1:8080/index/`，即可查看本地网页，如图 5-6 所示：

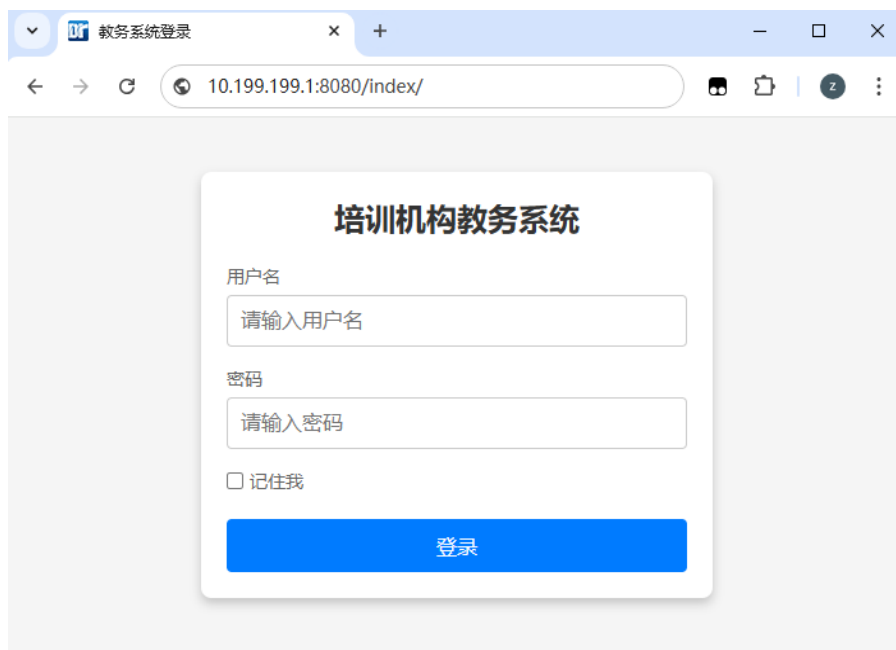


图 5-6 Web 服务器的安装

5.4.2 FTP 服务器

在培训机构中，FTP 服务器用于存储和传输教学资源、学生作业、项目文件等数据。教师可以将课件和练习资料上传至 FTP 服务器，方便学生下载学习；学生也可以提交作业至服务器，便于统一管理。由于桌面用户大多使用 Windows 操作系统，所以我们在 FTP 服务器的选择上使用 Windows Server 2016 服务器操作系统以保持良好的兼容性。安装 FTP 服务器的过程如下：

(1) 在服务器管理器添加角色和功能中勾选 FTP 服务器，并安装。如图 5-7 所示：



图 5-7 FTP 服务器的安装

(1) 打开 IIS 管理页面新建 FTP 站点，如图 5-8 所示：



图 5-8 FTP 服务器的安装

(3) 设置 FTP 服务器的各种参数，如图 5-9 所示：

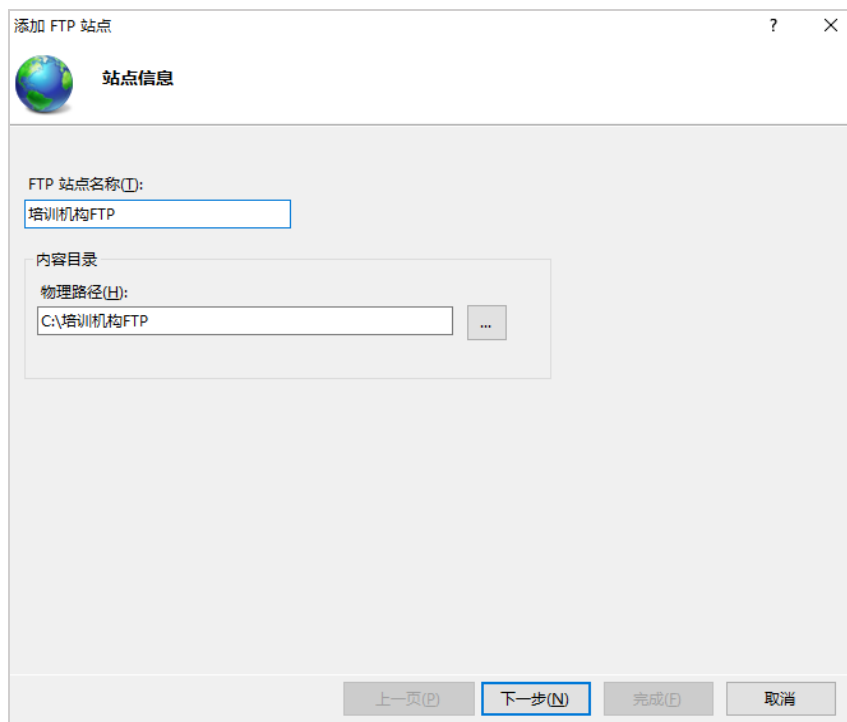


图 5-9 FTP 服务器的安装

(4) 在实训楼的计算机上登陆 `ftp://10.199.199.2/`，访问成功如图 5-10 所示：

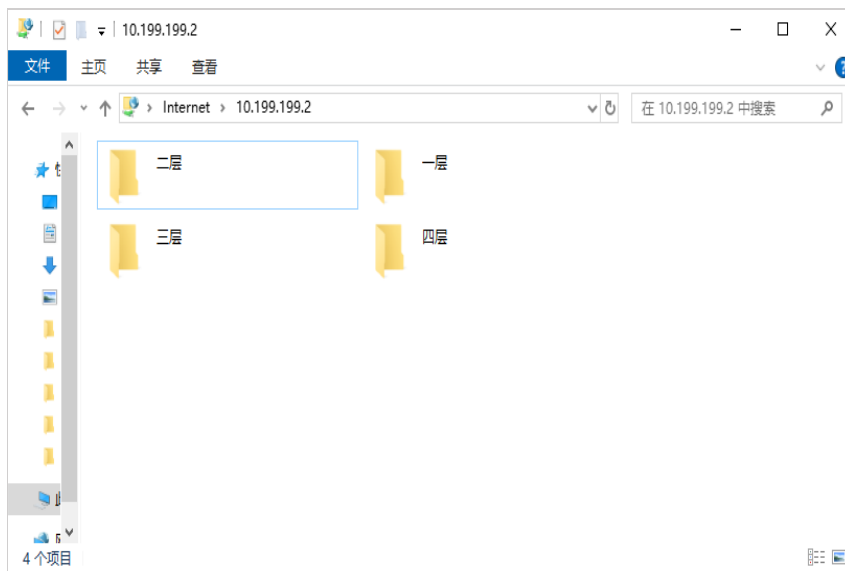


图 5-10 FTP 服务器的安装

六、网络安全与规划

6.1 网络安全概述

在当今信息化高度发展的社会，网络安全已成为各行业和领域普遍关注的焦点问题。网络的广泛应用为人们的日常生活、学习、工作带来了诸多便利，但与此同时，各种网络安全威胁也层出不穷，如恶意软件、网络攻击、数据泄露等，这些威胁不仅会导致个人隐私泄露，还可能大面积瘫痪机构的设备。主要的网络安全威胁包括以下几种：

（1）恶意软件

恶意软件包括病毒、蠕虫、木马和勒索软件等，这些软件通常是通过各种手段传播到用户设备上。病毒和蠕虫会自动复制并传播，可能导致系统崩溃或数据损坏。木马程序通常伪装成合法软件，用户一旦运行，就会被黑客控制，窃取个人信息或造成系统破坏。勒索软件则通过加密用户文件并要求支付赎金来恢复数据，这种攻击不仅对个人用户造成损失，还可能威胁到企业的业务运作和机密数据的安全。

（2）网络攻击

网络攻击是指攻击者通过网络入侵、破坏目标计算机系统或网络的行为。其中，分布式拒绝服务攻击（DDoS）是最常见的攻击类型之一，攻击者利用大量被感染的设备（如僵尸网络）向目标服务器发送海量请求，导致服务器或网站无法正常响应。DDoS 攻击不仅会影响服务的可用性，还会增加企业的运维成本。其他形式的网络攻击，如 SQL 注入、跨站脚本攻击（XSS）等，也会通过漏洞侵入系统，获取敏感数据或执行恶意操作。

（3）数据泄露

数据泄露通常发生在敏感信息（如个人身份、财务信息等）被未经授权的第三方获取的情况下。黑客可能通过各种手段，包括网络攻击、社交工程等，窃取存储在服务器、数据库中的敏感数据。泄露的个人信息可能被用于身份盗窃、诈

骗或其他非法活动，严重的泄露事件会导致用户的隐私权和财产损失。对于企业来说，数据泄露不仅会损害品牌声誉，还可能面临法律诉讼和经济处罚。

（4）社会工程攻击

社会工程攻击通过操控人类行为获取敏感信息，攻击者通常伪装成信任的人或机构来欺骗受害者。钓鱼邮件是最常见的社会工程攻击方式之一，攻击者通过伪装成合法的银行、社交媒体或公司发送邮件，引诱用户点击恶意链接或提供个人信息。伪装网站和假冒电话也常用于此类攻击，利用受害者的信任达到窃取信息的目的。社会工程攻击往往很难通过技术手段防范，因此培训用户提高警惕是防御此类攻击的有效措施。

（5）中间人攻击

中间人攻击是指攻击者在通信双方之间拦截和篡改数据的行为。攻击者可以通过监听不安全的网络（如公共 Wi-Fi）窃取敏感信息，如账号密码、银行交易信息等，或篡改通信内容，如修改银行转账金额、伪造电子邮件等。中间人攻击通常会影响到用户的隐私安全和交易安全，尤其是在未加密的网络中，攻击者更容易执行此类攻击。因此，使用加密协议（如 HTTPS）进行安全通信是防止中间人攻击的关键措施。

（6）内部威胁

内部威胁指的是来自组织内部人员的安全风险，包括员工、承包商、合作伙伴等，他们可能故意或无意地泄露敏感数据或进行破坏。这类威胁往往更加难以防范，因为内部人员通常拥有较高的访问权限。恶意内部人员可能窃取商业机密、篡改数据或破坏系统，而无意间泄露信息的员工可能在不知情的情况下成为黑客攻击的跳板。加强内部人员的安全意识、控制权限、实施访问审计等措施，有助于减少内部威胁的发生。

（7）零日攻击

零日攻击是指攻击者利用尚未公开或尚未修补的系统漏洞进行攻击。在漏洞被厂商发现并修复之前，攻击者已经利用这些漏洞对目标系统实施攻击，造成数据泄露、系统崩溃或被控制等后果。由于零日漏洞通常在公之于众之前没有补丁或防护措施，因此这些攻击尤其危险，防御难度较大。为了防范零日攻击，及时

的系统更新和漏洞扫描至关重要，此外，采用多层次的安全防护措施可以有效降低零日攻击带来的风险。

6.2 网络安全规划

网络安全策略是保护机构信息系统免受网络威胁的重要框架，涵盖访问控制、数据保护、防火墙与入侵检测、漏洞管理、日志监控、灾难恢复以及用户教育等多方面内容。通过有效实施这些策略，机构可以减少网络攻击的风险，保护数据安全，提升整体网络的抗风险能力，确保系统的稳健和业务的持续性。

（1）物理安全规划

物理安全策略旨在防范未经授权的实体访问或破坏硬件设备和设施。它涵盖对服务器、路由器、交换机等关键设备的物理保护，包括安装访问控制系统、监控摄像头、门禁管理以及确保设备远离自然灾害的防护措施。通过严格的物理安全策略，机构可以有效降低硬件损毁、数据泄露和业务中断的风险，为信息系统的稳定运行提供可靠保障。

（2）信息加密规划

信息加密通过将数据进行加密处理，保护信息在传输和存储过程中的机密性和完整性。此策略通常采用对称加密、非对称加密以及散列算法来确保敏感数据不被未授权者读取或篡改。通过在网络通信、文件存储和身份验证中引入加密技术，信息加密策略能有效抵御窃听和数据泄露等安全威胁，保障机构和用户的数据隐私。

（3）数据安全规划

数据安全策略是保护组织内外数据资源的系统性措施，旨在确保数据的机密性、完整性和可用性。该策略通常涵盖数据的访问控制、备份恢复、权限管理、数据脱敏以及传输安全等方面，以防止数据被未授权访问、篡改或丢失。通过实施数据加密、身份验证、存储隔离和定期备份等手段，数据安全策略能够抵御潜在的网络攻击、内部威胁和自然灾害，帮助维护信息系统的安全稳定，为机构的数据资产提供全面保护。

6.3 WEB 防火墙

在培训机构中，教务系统通常放到外网的，并且涉及到学生信息管理、课程安排、成绩查询等重要功能。由于其敏感性，教务系统成为黑客攻击的重点目标。Web 防火墙（WAF）在此起着至关重要的作用，主要通过检测和拦截恶意 Web 流量，防止常见的攻击手段，如 SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等，保护教务系统的安全性。

WAF 能够对教务系统进行深度流量分析，识别出潜在的安全威胁。通过实时监控 HTTP/HTTPS 请求，WAF 能够有效拦截恶意请求，防止不法分子通过漏洞获取或篡改学生和教师的个人信息、成绩数据等敏感资料。此外，WAF 还能在教务系统面临高并发访问时，提供负载均衡和流量管理功能，保证系统的稳定运行。

针对新型攻击，现代 WAF 还通过行为分析和机器学习等技术，识别未知攻击模式，并自适应更新防护规则，这使得教务系统能够在不断变化的网络环境中保持高水平的安全性。综上所述，WAF 不仅能防止常见的网络攻击，还能够保障教务系统的稳定性和数据安全，是培训机构信息化建设中不可或缺的安全防线。

6.4 数据加密策略

在现代教育和培训环境中，保护学员数据、教学资源和其他敏感信息的安全至关重要。为了确保数据的机密性、完整性和可用性，培训机构需要采用合适的加密方法来保护存储和传输中的数据。以下是对培训机构数据加密方法的设计方案：

（1）存储数据的加密：

培训机构存储的数据通常包括学员的个人信息、成绩记录、教学内容等，这些数据一旦泄露，可能会导致严重的隐私侵犯和法律风险。因此，在存储数据时，应该采用对称加密（如 AES）来保护敏感数据。具体设计如下：

数据分类：对存储数据进行分类，明确哪些数据属于敏感信息，如学员个人信息、成绩单、考勤记录等，这些数据需要进行加密存储。

加密算法：使用 AES-256 算法进行数据加密，AES 是一种对称加密算法，具有较高的安全性和处理速度。256 位密钥长度能提供更强的加密强度，适合存储

大量敏感数据。

密钥管理：密钥是对称加密中最关键的元素，必须采取安全的密钥管理策略。例如，可以使用硬件安全模块（HSM）进行密钥存储，并定期更换密钥，确保密钥不被泄露或滥用。

加密存储：所有敏感数据应以加密格式存储在数据库或文件系统中，未经授权的用户无法直接访问原始数据。

（2）传输数据的加密：

在现代教育环境中，数据在网络中传输时面临着各种潜在的安全威胁，包括中间人攻击和数据窃听。因此，必须采用非对称加密和 SSL/TLS 加密协议来保护传输数据的安全。

SSL/TLS 加密：在所有涉及学员和教师交互、成绩上传、在线学习平台访问等环节，采用 SSL/TLS 协议对数据进行加密。SSL/TLS 协议能够有效防止数据在传输过程中被窃取或篡改。网站的 HTTPS 协议就是通过 SSL/TLS 进行加密的。

（3）数据备份和恢复的加密

数据备份是确保数据在遭遇灾难或丢失时能够恢复的重要手段。为了保证备份数据的安全性，备份文件也需要进行加密处理。

备份加密：所有备份文件应使用与存储数据相同的 AES-256 算法进行加密处理，确保备份数据即使在外设或云端存储中也无法被未经授权人员访问。

备份数据完整性校验：在备份恢复过程中，使用哈希算法（如 SHA-256）对备份数据进行完整性校验，确保备份数据没有被篡改。

总 结

在即将迎来大学生活的尾声之际，我深感毕业设计不仅是学业的最后考验，更是我人生旅程中的一次重要启航。经过这段时间的学习与实践，我对未来充满了憧憬和期待。这个项目让我认识到，网络规划不仅仅是技术层面的挑战，更是对个人学习能力的承诺。

随着技术更新迭代，未来的工作中，我希望能够不断适应和融入这种变化，不仅提升自己的专业技能，更要以开放的心态去接受新知识。只有持续学习，才能在这个快速变化的世界中立于不败之地。

在这个过程中，我对人生的理解也在逐渐深化。每一个项目都是一种责任，而每一次成功与挫折都是成长的契机。我希望将这种责任感融入未来的工作中，无论身处何地，都能为团队贡献自己的力量，为国家建设贡献自己的智慧与努力。未来的道路上，我愿意与志同道合的人们携手同行，共同探索新领域，实现共同的理想。每一个小目标的实现，都是迈向更大成就的基石。

我也愈发意识到，知识的获取不仅仅是为了个人的提升，更是为了更好地服务他人。通过这次毕业设计，我感受到教育的真正意义在于为国家建设。在未来的工作中，我希望能够将自己所学运用于实践，为国家的发展贡献一份力量。“为国捧心”将成为我始终不变的信念。

在此，我要感谢所有指导我、支持我的老师和同学们。你们的鼓励和建议让我在这条旅程中不再孤单，深深地激励着我不断追求卓越。未来的我，将继续秉持着这种学习的热情和探索的勇气，迎接每一个新的挑战，成就更好的自己。

参考文献

- [1]秦智.网络系统集成[M].西安:西安科技大学出版社,2024:15-21,2.
- [2]王晓玲,马庆槐.Wbe 前端开发实训案例教程[M].北京:电子工业出版社,2023:18-25,1.
- [3]孟敬.计算机网络基础与应用[M].北京:人民邮电出版社,2024:50-52,1.
- [4]冯昊,杨海燕.网络工程规划设计与项目实训[M].北京:清华大学出版社,2022:20-21,1.
- [5]王燕.交换路由组网技术与实训指导[M].大连:大连理工大学出版社,2023:20-25,1.
- [6]杨寅春.网络安全技术[M].西安:西安电子科技大学出版社,2023:10-12,5.
- [7]彭文华,李忠.网络组网与互联[M].北京:北京理工大学出版社,2024:1-2,3.
- [8]郑东营.计算机网络技术及应用研究[M].天津:天津科学技术出版社,2022:62-63,1.
- [9]牛丽萍,李龙,郭爽.计算机应用基础与网络安全研究[M].哈尔滨:哈尔滨出版社,2023:3-2,1.
- [10]梁广民,徐磊,程越.网络互联技术[M].北京:高等教育出版社,2022.5-6,2.
- [11]王亮.网络工程技术实践[M].西安:西安电子科技大学,2022.11-12.2.
- [12]尹淑玲,温静.路由交换技术[M].武汉:华中科技大学出版社,2023.43-44,3.
- [13]陈波,于泠.防火墙技术与应用[M].北京:机械工业出版社,2024.51-54,1.
- [14]韩立刚.计算机网络创新教程[M].北京:中国水利水电出版社,2023.44-45,2.
- [15]韩少云.网络与 Linux 安全攻防/[M].西安:西安电子科技大学出版社,2022.12-14.1
- [16]黄宁著.网络可靠性及评估技术[M].北京:国防工业出版社,2022.11-12.2
- [17]廖燕玲.网络课程开发实验教程[M].武汉:华中科技大学出版社,2023.114-115.1
- [18]朱先强,杨国利,张维明.复杂网络:结构与动态演化分析[M].北京:机械工业出版社,2022.15-16.2
- [19]柳青,曾德生.计算机网络技术基础项目式教程[M].北京:中国水利水电出版社,2021.19-20.1
- [20]唐宏,伍佑明,陈华南,龚霞.可编程网络技术原理与实践[M].北京:人民邮电出版社,2023.8-9.1

致 谢

大学三年经过许多的和考试，毕业设计是三年当中最后一场考试，也是我们大学生涯谢幕的最后一场的演练，此次设计成功最离不开的是我的指导老师易兰英，是他精心指导我从最初的选题到设计的成功，都离不开他呕心沥血的教导，没有他我会走许多的弯路，其次感谢的是我的同学，是他们在我的大学生涯添上了浓墨重彩的一笔，让我见识到了同学之间的情谊和互帮互助，在我遇到困难的时候拉我一把，让我又能看见黎明前的那一刻曙光。

大学毕业就要各奔东西了，也不知什么时候才能与各位老友见面，在此还是想对各位说一声谢谢，能够出现在我青春最美好的一段时光，现在回想起过往的种种，时常让我流连忘返，例如老师在聚精会神的给我们讲课，时不时帮助同学解答各种疑难困惑问题，也有同学在上课时互相交流技术的那份激情画面，当然最让我忘不了的就是我指导老师易兰英上课的时候，有严肃认真的一幕，也有和同学们嬉笑的瞬间，但是更多的还是给各个同学严谨难题的一刻，易老师是一位非常认真负责的老师，对待同学没有保持师生之间的距离感，更多的是像一位朋友之间的情谊，在弄完课题的心累的时候与我们讲点笑话，让我们疲惫的神经得到一丝舒缓，所以我还是想对易老师说一声谢谢，谢谢你对待我们像朋友一样，谢谢你在毕业研究上给我的宝贵意见。让我在毕业设计上的出发点有了很好的思路，正是有了这些经验，才让我在毕业设计上没有迷茫，让我的专业知识很好的运用和掌握，此次毕业设计能够完成还是由衷的感谢易老师和各位同学。