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： 中科有限公司网络规划与设计方案

学生姓名	陈瑞琪
学生学号	010425171773
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）：陈锦琪　　日　期：2025.5.12

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：2025.5.16

（注：本页学生和指导教师须亲笔签名。）

目录

一、项目概况

（一）毕业设计背景

中科有限公司作为一家新兴的高科技企业，致力于开发和提供创新的网络解决方案。随着公司业务的持续扩张，我们深刻认识到一个强大、可靠且安全的网络系统对于公司运营的重要性。因此，我们决定开展一次全面的网络规划与设计，以满足公司未来的发展需求。

目前，公司的网络系统虽然能够满足基本的业务需求，但随着公司规模的扩大和业务的增长，现有的网络设备和技术已经逐渐无法满足日益增长的需求。我们亟需一个更高性能、更高可靠性和更大带宽的网络系统来支持公司的业务发展。

网络安全是我们在网络规划与设计中的重要考量。随着网络攻击和数据泄露事件的不断增加，我们必须采取有效的安全措施来保护公司的网络资源和用户数据的安全。这包括建立防火墙、入侵检测系统、数据加密等安全机制，以及制定详细的网络安全策略和培训员工提高网络安全意识。

此外，网络的可扩展性和灵活性也是我们重点关注的方面。随着公司业务的不断发展和变化，我们需要一个可以轻松扩展和调整的网络架构，以适应新的业务需求和技术变革。这需要我们在网络规划与设计中采用模块化和可伸缩的设备和技术，以便在未来能够方便地进行升级和扩展。

（二）毕业设计意义

随着公司业务的不断发展和员工数量的持续增加，对网络的需求也在不断增长。因此，对公司的网络进行全新的规划显得尤为重要。首先，网络规划将显著提升公司网络的性能和可靠性。通过优化网络架构和配置，提升带宽和传输速度，公司员工将能够更快速、稳定地访问和传输数据，从而提高工作效率和业务运行的效率。

其次，网络规划将加强公司的网络安全保护。通过引入先进的安全技术和策略，建立完善的安全体系，可以有效防止网络攻击、病毒传播和数据泄露，保护公司的商业机密和客户数据的安全。

此外，网络规划将提高网络管理的效率和便捷性。通过合理的设备配置和网络

优化，可以提高网络的利用率和效能，提高网络管理团队的工作效率，减少人力和时间成本，降低管理风险。

最重要的是，网络规划将为公司的业务发展和创新提供有力支持。通过设计灵活的可扩展的网络架构，满足公司不断增长的业务需求，支持新业务的快速部署和应用，为公司提供一个稳定、高效、安全的网络环境，助力公司实现业务目标和长期发展。

（三）毕业设计思路

技术选型是网络规划中非常关键的一步。根据中科有限公司的需求和现状，我们需要选择适合的网络技术和标准，以满足性能、安全性和可靠性的要求。在选择网络技术和标准时，我们可以考虑使用高速以太网技术，如千兆以太网或 10 千兆以太网，以提供更高的带宽和更快的传输速度。此外，我们还可以考虑使用虚拟局域网（VLAN）技术来划分不同的网络区域，提高网络的安全性和管理性。

网络拓扑设计同样至关重要。结合中科有限公司的业务特点和发展规划，我们可以设计合理的网络拓扑结构，包括核心交换机、路由器、防火墙等设备的布置和连接方式。在设计网络拓扑结构时，我们可以考虑采用分层结构，将网络划分为核心层、汇聚层和接入层，以提高网络的可扩展性和稳定性。

根据网络规划的需求，我们需要挑选出适合的交换机、路由器、防火墙和服务器等设备，以保证其性能和可靠性达到预期。在选择硬件设备时，我们可以考虑使用知名品牌的设备，并注意其性能指标和技术参数是否符合我们的需求。

设计合理的 IP 地址规划方案也非常关键，它可以确保网络设备和终端设备的地址分配合理，能够满足中科有限公司的业务需求。在进行地址规划时，我们可以考虑使用私有 IP 地址范围，并通过子网划分来管理不同部门的网络。

根据中科有限公司的安全需求，我们需要制定完善的安全策略，包括访问控制、防火墙配置、入侵检测等措施，以保障网络的安全性和稳定性。我们可以采用多层次的安全措施，如设立访问控制列表（ACL）、配置防火墙规则、实施入侵检测系统（IDS）等，来保护网络免受恶意攻击和未经授权的访问。

通过以上规划与设计，中科有限公司将建立一个稳定、高效且安全的网络环境，为公司的业务进步和创新提供坚实的支持和保障。这将有助于提高员工的工作效率

和满意度，增强公司的竞争力和创新能力，实现长期稳定的发展。

二、 需求分析

（一）毕业设计总体需求

中科有限公司目前正处于企业网络构建的关键阶段，这一工程的核心目标是加速公司信息化进程，打造一个高度集成的智能化和数字化网络环境，从而显著提升公司的信息处理能力和运营效率。通过引入前沿信息技术，我们旨在优化企业办公与管理流程，实现自动化与智能化，满足公司对信息化建设的高标准需求。

该网络环境不仅作为基础通信平台，更是为各类应用程序提供高效、快速的信息交换平台，确保内部数据交换与外部通信的高效性、实时性与准确性。网络设计特别强调高可靠性，要求低故障率、减少意外中断，并注重降低维护成本，确保网络系统的经济性和可持续性，为公司稳定运营提供坚实技术支持。

（二）公司办公需求

公司计划在现有网络基础设施基础上进行升级与扩展。首先，采用高速光纤作为传输媒介，提升网络传输速度与稳定性。同时，构建相互独立的内网系统，提供安全的办公局域网及可访问 Internet 的网络系统，实现部门间网络信息共享与资源共享，提高办事效率与透明度。

技术方面，公司将以 IP 和 Internet 技术为主体，核心路由器为交换中心，构建多层结构的下属部门信息网络系统，提供功能齐全、技术先进、资源统一的网络应用系统。同时，引入先进的网络安全技术，如防火墙、入侵检测系统等，确保网络的安全性和可靠性。

为满足不同部门和业务需求，公司将根据实际需要划分不同子网，如办公子网、生产子网、销售子网等，提高网络管理效率与灵活性。此外，公司将建立完善的网络监控和管理系统，实现网络实时监控、故障排除与性能优化。

（三）公司设备性能需求

在网络设备选择上，公司将挑选性能稳定、安全可靠的设备，如交换机、路由器、服务器等，并考虑引入云计算、大数据等先进技术，提升网络处理能力和业务

支持能力。

公司通过全面升级和扩展企业网络，实现信息化建设目标，为企业发展提供强大信息支持。未来网络建设中，公司将持续关注新技术和新趋势，不断优化和完善网络系统，满足企业不断发展需求。

网络设计涵盖路由架构、IP 地址管理、网络安全防护、VLAN 划分及设备设置等方面。公司内联网构成基本网络设施，成为构建公司网络系统主体任务，后续工作基于此展开。信息化网络体系目标是以宽带互联网为主导，形成一体化内部办公室网络与外部宽带互联，具备 VLAN 能力，确保网络高效性与安全性。骨干网交换机需具备高效数据传输能力，整套网络包含高效三级交换特性。

骨干网络采用稳定 1000Mbps 以太网技术构建主干部分，建议选用有成功项目经验的网络供应商产品，提供通向 Internet 端口，具备优秀扩充潜力。搭建公司内局域网涉及网络技术挑选、网络布局设计、线路系统设定及详细网络计划制定。网络计划中核心、汇聚、接入层三个层次至关重要。

路由架构采用分层设计，包括核心层、汇聚层和接入层。核心层处理公司内部主要数据交换，汇聚层汇总各部门数据到核心层，接入层连接终端设备。为提高网络稳定性和可扩展性，选择高性能、高稳定性、高安全性的设备，如交换机、路由器等。

IP 地址管理采用私有 IP 地址，提高网络安全性。实施完善 IP 地址规划方案，包括子网划分、IP 地址分配等，满足不同部门和业务需求。网络安全部署防火墙、入侵检测系统、虚拟专用网等安全设备，防止数据泄露和攻击。建立完善网络安全策略和管理制度，定期进行网络安全检查和漏洞扫描。

VLAN 划分根据公司业务需求和部门划分，合理划分 VLAN，提高网络管理效率和灵活性。实施完善 VLAN 管理方案，包括 VLAN 间通信、VLAN 调整和优化等。设备设置根据网络规划方案，选择合适设备和配置参数，确保网络性能和稳定性。建立完善设备管理制度，包括设备监控、维护和更新等。

三、 局域网拓扑与 IP 地址规划设计

（一）公司网络设计需求

今夕公司部门结构：

领导办公区：5 人

人事部：5 人

综合保障中心：1 人

财务部：3 人

销售部：5 人

市场部：5 人

技术部：5 人。

公司办公楼栋拓扑图如“图 3.1”：

图 3.1 办公楼拓扑图

（二）公司方案设计策略

为实现对公司网络的有效管理与合理 IP 地址分配，我们依据不同区域及设备类型进行子网划分，并精心设计了一套 IP 地址规划方案。具体策略如下：

1. 核心子网

作为公司网络的核心枢纽，核心子网将分配给核心交换机及其他关键网络设备。鉴于其重要性，我们为其分配了较大范围的 IP 地址段，例如 192.168.0.0/16，以确保核心网络的高效运作与扩展性。

2. 办公区域子网

针对公司各办公区域，我们将分别设置独立子网，用于连接各区域内的办公设备。例如：

领导办公区子网：采用 192.168.1.0/24，满足领导办公区的网络需求。

人事部子网：采用 192.168.2.0/24，确保人事部的网络稳定。

综合保障中心子网：采用 192.168.3.0/24，保障其网络独立性。

财务部子网：采用 192.168.4.0/24，确保财务数据的安全传输。

销售部子网：采用 192.168.5.0/24，支持销售团队的网络需求。

市场部子网：采用 192.168.6.0/24，满足市场部的网络需求。

技术部子网：采用 192.168.7.0/24，为技术团队提供稳定的网络环境。

3. 特殊功能区域子网

根据公司业务需求，我们还将设置若干特殊功能区域子网，例如：

数据中心子网：采用 192.168.50.0/24，确保数据中心的高带宽与低延迟需求。

会议室子网：采用 192.168.60.0/24，满足会议室的多媒体设备连接需求。

访客网络子网：采用 192.168.70.0/24，为访客提供安全的网络访问，同时与公司内部网络隔离。

4. 网络安全与管理

为保障公司网络的安全性与稳定性，我们将部署以下措施：

防火墙与入侵检测系统：在核心子网与外部网络之间部署防火墙，同时在各子

网中配置入侵检测系统，实时监控网络流量，防止恶意攻击。

VLAN 划分：通过虚拟局域网技术，进一步隔离不同部门的网络流量，提高网络管理效率与安全性。

IP 地址管理：建立动态主机配置协议（DHCP）服务器，自动分配 IP 地址，同时为关键设备预留静态 IP 地址，确保网络配置的灵活性与稳定性。

网络监控与维护：部署网络监控系统，实时监控网络设备状态与性能指标，及时发现并解决网络问题，确保网络的高效运行。

通过以上精心设计的网络方案，我们将为今夕公司构建一个高效、稳定、安全且易于管理的网络环境，满足公司各部门的业务需求，支持公司的长期发展。

具体 IP 地址规划看“表 3.1”

表 3.1 IP 地址规划

名称	接口或 VLAN	IP 地址	备注
Switch1	VLAN10	192.168.10.0/24	财务部
	VLAN20	192.168.20.0/24	技术部
	VLAN30	192.168.30.0/24	市场部
	聚合端口 1	10.0.254.253/24	冗余链路
	f0/1	10.0.4.2/24	上联链路
Switch2	VLAN40	192.168.40.0/24	销售部
	VLAN50	192.168.50.0/24	人事部
	VLAN60	192.168.60.0/24	领导办公区
	聚合端口 1	10.0.254.254/24	冗余链路
	f0/1	10.0.5.2/24	上联链路
Router	g0/0	10.0.2.2/24	与防火墙相连
	g0/1	10.0.5.1/24	与 HXSwitch2 相连
	g0/2	10.0.4.1/24	与 HXSwitch1 相连
防火墙	VLAN1	10.0.2.1/24	与 HXRouter 相连
	VLAN2	10.0.1.2/24	与 BJRouter 相连
BJRouter	g0/0	10.0.1.1/24	与防火墙相连
	g0/1	10.0.3.2/24	与 SRouter 相连

	s0/3/0	100.100.100.1/24	与 internet
SRouter	g0/0	10.0.3.1/24	与 BJRouter 相连
	g0/1	192.168.7.254/24	服务区网关
ISP	s0/3/0	100.100.100.2/24	ISP
	g0/0	202.202.202.254/24	internet
WEB 站点		202.202.202.120/24	互联网服务
WEB 站点		192.168.7.80/24	内网 WEB 服务
DNS 服务		192.168.7.53/24	内网 DNS 服务
DHCP 服务		192.168.7.68/24	内网 DHCP 服务
Mail 服务		192.168.7.110/24	内网邮件服务
无线 SSID	财务部	192.168.0.0/24	财务部
无线 SSID	技术部	192.168.0.0/24	技术部
无线 SSID	市场部	192.168.0.0/24	市场部
无线 SSID	销售部	192.168.0.0/24	销售部
无线 SSID	人事部	192.168.0.0/24	人事部
无线 SSID	行政部	192.168.0.0/24	领导办公区

四、设备选型规划

（一）公司网络设备选型

设备选型是企业网络建设和维护的关键环节，其决策依据主要涉及以下几个重要方面：

（1）性能要求

性能要求是设备选型的核心考量因素。根据公司网络的规模和业务需求，必须明确设备所需的性能指标。例如，带宽是衡量网络传输速度的关键指标，而吞吐量则反映了设备处理数据的能力。此外，设备的处理能力直接影响其运行效率。在选择设备时，需要根据公司的实际需求和预算进行综合权衡，确保设备性能既能满足当前需求，又具备一定的扩展性。

（2）可扩展性

随着公司业务的持续发展和网络需求的不断增长，设备的可扩展性变得尤为重要。选择具有灵活升级和扩展能力的设备，可以有效应对未来可能出现的各种需求变化，确保网络的可持续发展。例如，设备应支持模块化扩展，以便在需要时增加端口或提升性能，而无需更换整个设备。

（3）可靠性和稳定性

设备的可靠性和稳定性是保障公司网络稳定运行的基础。选择具有良好可靠性和稳定性的设备，可以显著减少故障发生频率，降低维护成本，提高网络运行效率。在评估设备时，可以参考设备的平均无故障时间（MTBF）和用户评价，优先选择经过市场验证的成熟产品。

（4）安全性

在当今信息化社会，网络安全问题日益突出。因此，选择具有完善安全功能和机制的设备至关重要。设备应具备防火墙、入侵检测系统（IDS）、数据加密等安全特性，以有效保护公司网络的信息安全和数据隐私。此外，设备的安全功能应易于配置和管理，确保安全策略能够快速部署和更新。

（5）成本效益

在满足性能和功能需求的前提下，设备的成本效益也是重要的考量因素。需要选择价格合理、性价比高的设备，以确保设备选型符合预算，并实现成本的最优化。

可以通过对比不同品牌和型号的设备，综合考虑其初始购买成本、维护成本和使用寿命，选择最具性价比的设备。

（二）公司设备选择的侧重点

在选择公司网络设备时，公司将重点关注以下几个方面：

（1）品牌信誉

在选择网络设备时，公司会优先考虑具有良好品牌信誉和口碑的厂商。知名品牌通常拥有更高的生产制造标准和严格的质量控制体系，能够提供更可靠的设备。此外，知名品牌厂商通常在售后服务方面更具优势，能够提供更全面的技术支持和保障。选择知名品牌的设备，可以确保设备的质量和服务，为公司网络建设提供坚实的保障。

（2）技术支持

公司在选择网络设备时，会优先选择能够提供全面技术支持和售后服务的厂商。稳定运行的网络离不开及时的技术支持和维护服务。因此，公司会选择能够提供24/7 技术支持、快速响应故障的厂商，确保设备在需要时能够及时恢复正常运行。这样可以保证公司网络的稳定性和可靠性，提高工作效率和用户体验。

（3）产品特性

公司在选择网络设备时，会重点关注设备的产品特性和创新功能，选择符合公司网络需求的设备。公司会重点考虑设备的性能指标、安全功能、易用性以及与其他设备的兼容性，以满足公司网络的功能要求，并提升网络性能和用户体验。选择具备先进特性和创新功能的设备，可以更好地满足公司的网络需求，提高工作效率和数据安全性。

（4）合作历史

公司在选择网络设备时，会倾向选择与公司有良好合作历史和沟通顺畅的厂商。建立长期稳定的合作关系有助于厂商更好地了解公司的需求和情况，提供更贴合实际需求的解决方案，并能够更快速地响应和解决问题，推动项目合作顺利进行。选择与公司有良好合作历史的厂商，可以确保双方之间的沟通顺畅，提高合作效率和项目成功率。

（三）公司设备选型

（1）交换机

S6520X-54QC-HI 核心交换机，具备高性能、可靠性和安全性，适用于公司网络的核心和汇聚层。外观如图 4.1 所示：

图 4.1 S6520X-54QC-HI

（2）路由器

RG-RSR20-XA-36 路由器，提供高性能的路由和安全功能，适用于公司网络的边缘连接和互联网接入。外观如图 4.2 所示：

图 4.2 RG-RSR20-XA-36

（3）防火墙

H3C F1000-AI-03 系列防火墙，具有卓越的防护性能和灵活的安全策略配置，保障公司网络的安全。外观如图 4.3 所示：

图 4.3 RG-WALL 1600-Z8620

（4）无线设备

H3C BA3000C，提供高密度的无线覆盖和可靠的用户连接，适用于公司无线网络的部署。外观如图 4.4 所示：

图 4.4 H3C BA3000C

（5）服务器

H3C R4900G3 系列服务器，提供高性能的计算和存储资源，支持公司网络的各类应用和服务部署。外观如图 4.5 所示：

图 4.5 H3C R4900G3

五、关键技术介绍和实现

（一）网络使用技术说明

在公司网络建设中，我们精心挑选并采用了以下关键技术，旨在全方位提升网络的性能、安全性和管理效率：

（1）VLAN（虚拟局域网）

VLAN 技术通过在交换机上进行逻辑划分，将同一物理网络分割为多个独立的逻辑网络。这种划分方式不仅显著增强了网络的安全性，还极大地提升了管理的灵活性。借助 VLAN，我们能够实现对网络资源的精细化管理，从而优化网络的可扩展性和可维护性。例如，不同部门的网络流量可以通过 VLAN 隔离，确保数据传输的安全性和独立性。

（2）OSPF（开放最短路径优先）

OSPF 是一种先进的动态路由协议，通过计算最短路径来实现高效的路由选择。它具备快速的网络收敛能力，能够迅速适应网络拓扑的变化，并自动调整路由策略，确保数据传输的稳定性和可靠性。OSPF 的自适应性使其成为复杂网络环境中的理想选择，能够有效提升网络的整体性能。

（3）NAT（网络地址转换）

NAT 技术是实现内部网络与外部网络通信的关键技术。它通过将私有 IP 地址转换为公有 IP 地址，不仅实现了网络的互联互通，还提供了一定的安全性。NAT 可以隐藏内部网络的真实 IP 地址，防止外部网络直接访问内部设备，从而有效降低网络攻击的风险，保护公司网络的安全。

（4）HTTP（超文本传输协议）

HTTP 是一种应用层协议，广泛用于在 Web 服务器和客户端之间传输超文本数据。它是互联网上最常用的协议之一，支持全球范围内的网页浏览和数据传输。HTTP 协议的高效性和兼容性使其成为现代网络通信的基石，确保用户能够无缝访问各类网络资源。

（5）DNS（域名系统）

DNS 是互联网上的地址簿，用于将用户友好的域名解析为相应的 IP 地址。它使得用户可以通过输入易于记忆的域名来访问网站，而无需记住复杂的 IP 地址。

DNS 的高效解析能力确保了网络设备能够准确、快速地访问目标网站，极大地提升了用户体验。

（6）DHCP（动态主机配置协议）

DHCP 协议用于自动分配 IP 地址、网关和 DNS 服务器等网络参数，极大地简化了设备接入和网络管理过程。通过 DHCP，设备可以自动获取所需的网络配置信息，无需手动配置，从而提高了网络部署的效率和管理的便捷性。例如，在公司新设备接入网络时，DHCP 可以快速为其分配合适的 IP 地址，确保设备立即可用。

（7）Mail（邮件服务）

我们为公司提供了全面的电子邮件服务，用于内部和外部的邮件通信。邮件服务支持邮件的发送、接收和存储，是日常沟通和信息交流的重要工具。通过高效的邮件系统，公司员工可以方便地进行协作和沟通，提升工作效率。

（8）防火墙

防火墙是网络边界的安全守护者，用于监控和控制网络数据包的流量。它能够阻止未经授权的访问和网络攻击，确保公司网络的安全。防火墙可以过滤网络流量，限制特定端口和协议的访问，防止恶意软件和黑客入侵，保护网络中的敏感数据和关键设备。

（9）无线路由器和无线 Wi-Fi

我们部署了无线路由器和 Wi-Fi 技术，为公司员工提供无线网络覆盖。无线连接提供了更大的灵活性和便利性，使得用户可以在任何地点自由地连接到网络，使用移动设备进行上网和学习。例如，在会议室、休息区等场所，无线网络为用户提供了无缝的网络接入体验。

（10）端口聚合技术（LACP）

LACP 是一种先进的网络技术，允许将多个物理端口捆绑成一个逻辑通道，从而显著提高链路带宽和可靠性。这种技术特别适用于连接高负载设备和实现设备冗余，确保关键设备之间的稳定连接和数据传输。例如，在连接服务器和核心交换机时，LACP 可以有效提升链路的性能和稳定性。

（二）网络技术功能配置

为确保公司网络的安全性、稳定性和高效性，我们对以下关键网络功能进行了

详细配置：

1. VLAN 配置

通过划分不同 VLAN 并明确各端口的成员关系，实现了不同用户群体及设备之间的有效隔离与精细化管理。这种配置不仅增强了网络的安全性，还优化了资源分配，确保各部门网络的独立性与高效运行。

```
sw1#show running-config | begin vlan
 switchport access vlan 10
!
interface FastEthernet0/3
 switchport access vlan 20
!
interface FastEthernet0/4
 switchport access vlan 30
!
```

```
sw2#show running-config | begin vlan
 switchport access vlan 40
!
interface FastEthernet0/3
 switchport access vlan 50
!
interface FastEthernet0/4
 switchport access vlan 60
!
```

图 5.1 对应接口加入对应 VLAN

2. OSPF 配置

精心配置了 OSPF 协议，详细定义了区域、网络及邻居关系等关键参数，从而高效地建立了动态路由体系。这一配置使得网络能够自动适应拓扑变化，快速收敛，确保数据传输的稳定性和可靠性，为复杂网络环境提供了强大的路由支持。

```
sw1#show running-config | begin router ospf
router ospf 110
 log-adjacency-changes
 redistribute connected metric-type 1 subnets
 network 10.0.4.0 0.0.0.255 area 0
 network 10.0.254.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
!
end


sw1#
```

图 5.2 OSPF 配置

3. NAT 配置

根据公司网络需求，制定了精准的 NAT 转换规则，实现了内部网络与外部网络之间的无缝地址转换与严格访问控制。NAT 配置不仅保障了内部网络的安全性，还优化了对外通信效率，确保公司能够安全、高效地与外部网络交互。

```
R2#show running-config | include nat
 ip nat inside
 ip nat inside
 ip nat outside
 default-information originate
ip nat pool ZZ 100.100.100.3 100.100.100.10 netmask 255.255.255.0
ip nat inside source list 1 pool ZZ
R2#
```

图 5.3 NAT 配置

4. HTTP 服务配置

成功部署了 WEB 服务器，并对其 HTTP 服务进行了全面配置。通过优化服务器性能和安全设置，为公司提供了稳定、高效的 WEB 页面及应用访问服务，支持了公司内部及对外的多种业务需求。

File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to 今夕科技公司!
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

图 5.4 公司官网首页

5. DNS 服务配置

配置了功能强大的 DNS 服务器，并添加了全面的域名解析记录。通过精确的 DNS 设置，确保了网络设备能够快速、准确地访问目标网站，极大地提升了用户体验和网络访问效率。

DNS

DNS Service On Off

Resource Records

Name Type A Record

Address

Add Save Remove

No.	Name	Type	Detail
0	mail.jxkj.cn	A Record	192.168.7.111
1	pop3.jxkj.cn	A Record	192.168.7.111
2	stmp.jxkj	A Record	192.168.7.111
3	www.baidu.com	A Record	202.202.202.120
4	www.jxkj.cn	A Record	192.168.7.80
5	www.jzkj.com	A Record	192.168.7.80

DNS Cache

图 5.5 公司内部 DNS 服务记录配置

6. DHCP 服务配置

详细配置了 DHCP 服务器，定义了合理的地址池和租期等关键参数。通过自动化的 IP 地址分配机制，简化了设备接入流程，提高了网络管理效率，确保了公司网络的动态性和灵活性。

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.168.7.0	255.255.255.0	255	0.0.0.0	0.0.0.0
vlan60	192.168.60.254	192.168.7.53	192.168.60.0	255.255.255.0	250	0.0.0.0	0.0.0.0
vlan50	192.168.50.254	192.168.7.53	192.168.50.0	255.255.255.0	250	0.0.0.0	0.0.0.0
vlan40	192.168.40.254	192.168.7.53	192.168.40.0	255.255.255.0	250	0.0.0.0	0.0.0.0
vlan30	192.168.30.254	192.168.7.53	192.168.30.0	255.255.255.0	250	0.0.0.0	0.0.0.0
vlan20	192.168.20.254	192.168.7.53	192.168.20.0	255.255.255.0	250	0.0.0.0	0.0.0.0
vlan10	192.168.10.254	192.168.7.53	192.168.10.0	255.255.255.0	250	0.0.0.0	0.0.0.0

图 5.6 DHCP 池配置

7. 邮件服务配置

部署了高性能的邮件服务器，并对其邮件传输代理、邮件存储等核心功能进行了深度配置。通过优化邮件系统的安全性和性能，为公司提供了稳定、可靠的内部及外部邮件通信服务，满足了日常办公和业务需求。

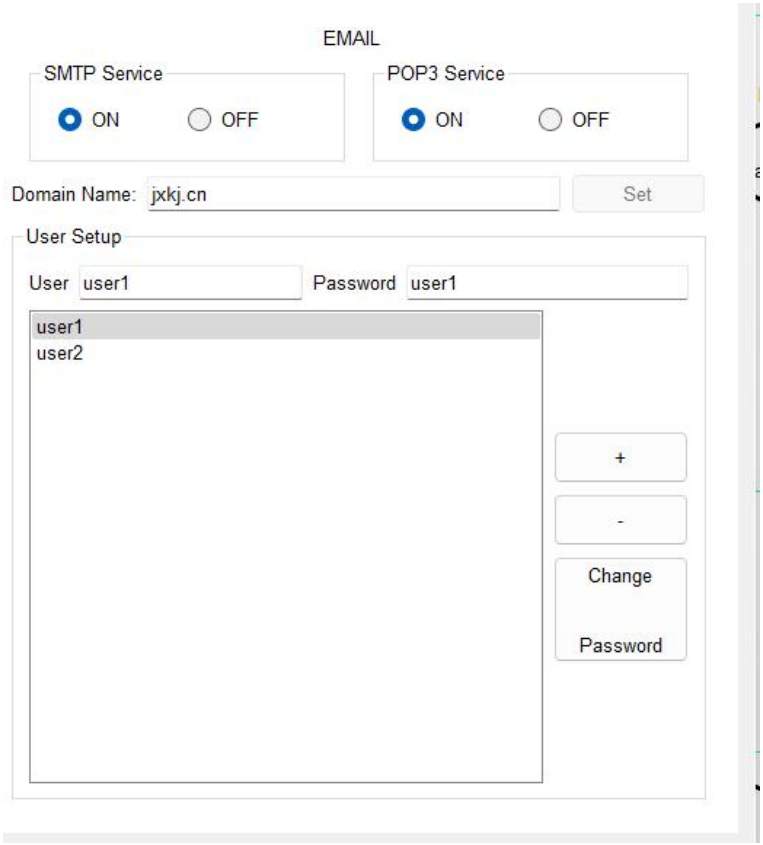

图 5.7 Mail 配置

8. 防火墙配置

制定了全面的防火墙策略和访问控制列表（ACL），精准配置了各类安全规则。通过防火墙的有效防护，阻止了未经授权的访问和潜在的网络攻击，为公司网络构

建了坚固的安全防线。

```
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.0.2.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 10.0.1.2 255.255.255.0
!
!
route outside 0.0.0.0 0.0.0.0 10.0.1.1 1
route inside 192.168.0.0 255.255.0.0 10.0.2.2 1
route outside 192.168.7.0 255.255.255.0 10.0.1.1 1
!
access-list fx extended permit icmp any any
access-list fx extended permit udp any range bootps bootpc any range bootps
bootpc
!
!
access-group fx in interface inside
access-group fx in interface outside
access-group fx out interface outside
access-group fx out interface inside
!
```

图 5.8 防火墙配置

9. 无线路由器和无线 Wi-Fi 配置

对无线路由器和 Wi-Fi 设备进行了细致配置，设置了安全的 SSID、加密方式及访客网络等参数。通过无线网络的优化，为公司员工提供了灵活、便捷的无线接入服务，满足了移动办公和学习的需求。

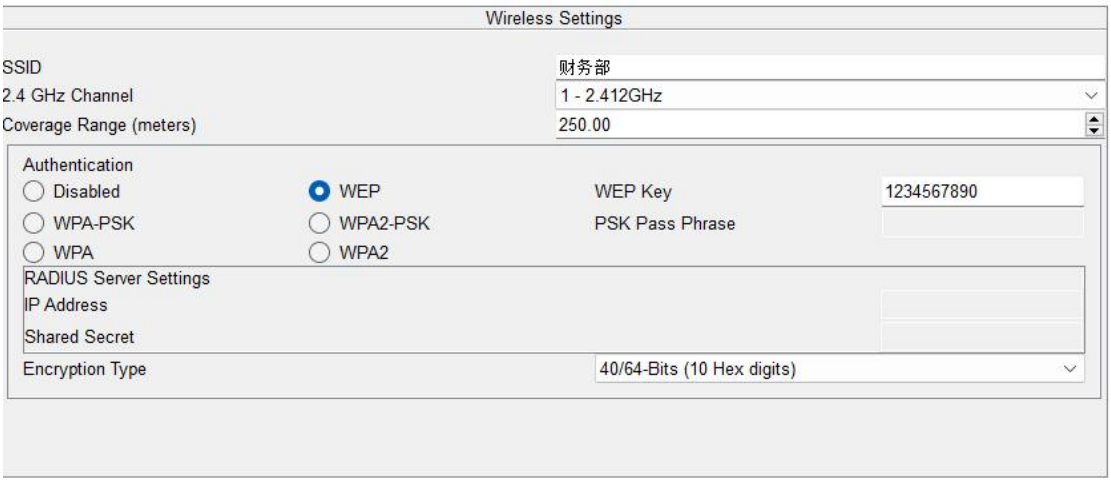

图 5.9 无线 SSID 以及认证配置

10. 端口聚合技术配置（LACP）

精心配置了端口聚合组，将多个物理端口高效捆绑为一个逻辑通道。通过 LACP 技术，显著提高了链路带宽和可靠性，确保了关键设备之间的稳定连接和高效数据传输，为高负载业务提供了有力支持。

```
interface FastEthernet0/5
 no switchport
 no ip address
 channel-group 1 mode active
 duplex auto
 speed auto
!
interface FastEthernet0/6
 no switchport
 no ip address
 channel-group 1 mode active
 duplex auto
 speed auto
!
```

图 5.10 端口聚合配置

通过以上功能配置，我们全面实现了公司网络的安全、稳定和高效运行，为公司办公和业务发展提供了坚实的网络基础。

六、技术结果测试

（一）公民网络技术测试

1. VLAN 配置验证

为确保不同网络区域的有效隔离，公司要求对 VLAN 配置进行详细验证。通过检查 VLAN 摘要信息，确认每个 VLAN 的 VLAN ID、名称、状态以及 VLAN 接口成员关系是否准确无误。这一验证步骤对于保障网络的安全性和稳定性至关重要。

```
sw1>show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/7,
Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11,
Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15,
Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19,
Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23,
Fa0/24, Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/2
20   VLAN0020                          active    Fa0/3
30   VLAN0030                          active    Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
sw1>
```

图 6.1 VLAN 摘要信息

2. OSPF 邻居关系验证

公司要求通过 OSPF 邻居关系确认动态路由协议的正确建立，以实现网络的自动路由选择。通过查看 OSPF 邻居信息，确认与邻居路由器的连接状态以及协议状态是否正常，确保路由器之间的 OSPF 邻居关系成功建立。这一验证步骤有助于优化网络的路由效率。

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.60.254    1   FULL/DR         00:00:37    10.0.5.2
GigabitEthernet0/1
192.168.30.254    1   FULL/DR         00:00:37    10.0.4.2
GigabitEthernet0/2
R1#
```

图 6.2 OSPF 邻居信息

3. NAT 转换表验证

公司要求验证 NAT 转换表，确保内部网络与外部网络的通信经过正确的地址转换。通过查看 NAT 转换表，确认 NAT 转换规则是否生效，以及内部主机与外部网络之间的地址转换是否按照预期进行。这一验证步骤对于保障网络的安全性和连通性至关重要。

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 100.100.100.3:1038 192.168.20.7:1038  202.202.202.120:80 202.202.202.120:80
tcp 100.100.100.4:1024 192.168.10.1:1024  202.202.202.120:80 202.202.202.120:80
tcp 100.100.100.4:1026 192.168.10.1:1026  202.202.202.120:80 202.202.202.120:80

R2#
```

图 6.3 NAT 转换表

4. 防火墙配置与状态验证

公司要求检查防火墙的配置和状态信息，确认安全策略和访问控制是否按照预期生效。通过查看防火墙配置和状态信息，确认已配置的安全策略是否正确，以及防火墙是否拦截了不合法的流量。这一验证步骤有助于确保网络的安全性。

```
ciscoasa#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list fx; 9 elements; name hash: 0xad2b61de
access-list fx line 1 extended permit icmp any any(hitcnt=163) 0x8e0d0535
access-list fx line 2 extended permit udp any range bootps bootpc any range
bootps bootpc(hitcnt=12) 0x7edb6265
access-list fx line 3 extended permit tcp any any eq www(hitcnt=31)
0xbde16550
access-list fx line 4 extended permit tcp any any eq domain(hitcnt=0)
0x572651c8
access-list fx line 5 extended permit udp any any eq domain(hitcnt=164)
0xa48a0cc5
access-list fx line 6 extended permit tcp any any eq smtp(hitcnt=1)
0x7076c9b8
access-list fx line 7 extended permit tcp any any eq pop3(hitcnt=2)
0x0bb4b770
access-list fx line 8 extended permit udp any any(hitcnt=25) 0x7434ca70
access-list fx line 9 extended permit tcp any any(hitcnt=23) 0x1880le9b
ciscoasa#s
```

图 6.4 访问控制列表 ACL 配置

5. 无线网络状态验证

公司要求查看无线网络的概要信息，确认无线网络覆盖和连接状态是否正常。通过查看无线网络的概要信息，了解每个接入点的状态、客户端连接数以及无线网络的整体运行情况，确保无线网络正常运行。这一验证步骤有助于优化无线网络的性能和用户体验。

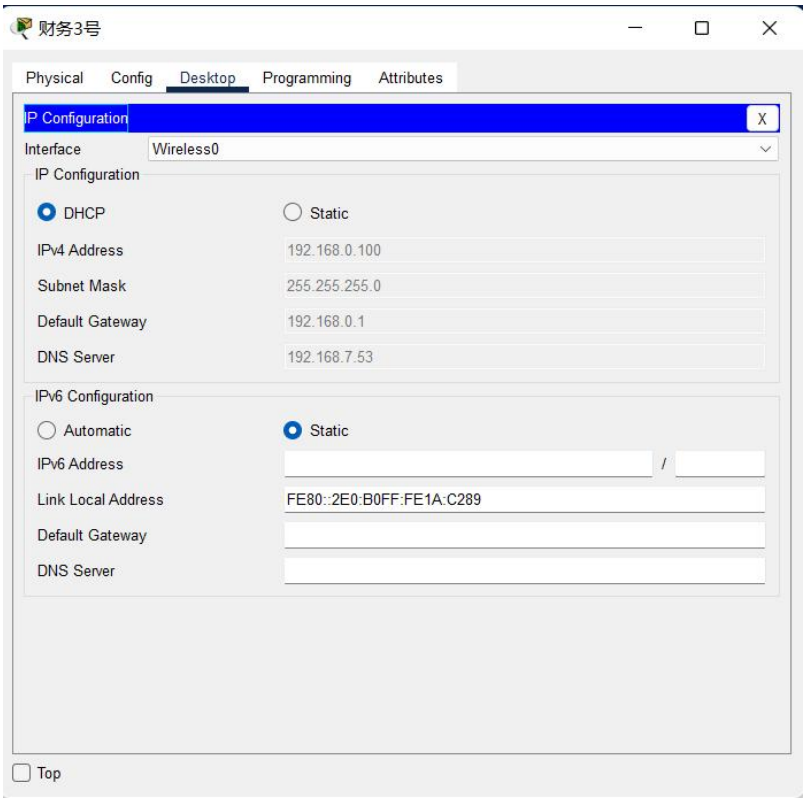

图 6.5 无线用户连接 SSID

（二）网络功能测试

1. DHCP 服务器功能验证

公司要求验证 DHCP 服务器是否成功分配 IP 地址给客户端设备，以保证网络设备能够正常接入网络。通过查看 DHCP 绑定信息，确认 DHCP 服务器已成功分配 IP 地址给客户端设备，并且了解每个 IP 地址的绑定状态。这一测试步骤对于确保网络的动态性和灵活性至关重要。

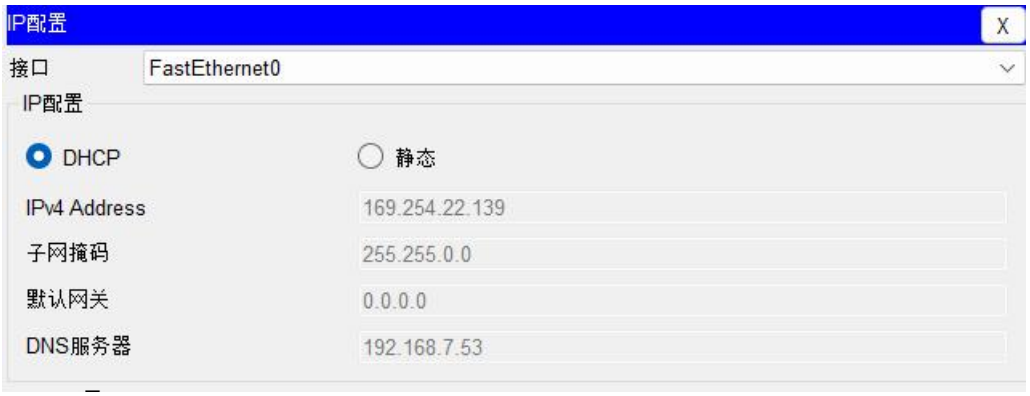

图 6.6 有线用户自动获取 IP 地址

2. DNS 服务器功能验证

公司要求使用 nslookup 命令查询域名解析结果，确认 DNS 服务器能够正确解析域名。通过执行 nslookup 命令，查询指定域名的解析结果，并确认 DNS 服务器是否能够返回正确的 IP 地址。这一测试步骤有助于确保网络设备能够准确访问目标网站。

图 6.7 使用 nslookup 命令查询域名解析结果

3. 邮件服务器功能验证

公司要求通过 telnet 命令连接到邮件服务器的 SMTP 端口，确认邮件服务器能够正常响应并发送邮件。通过 telnet 命令连接到邮件服务器的 SMTP 端口，模拟发送邮件的过程，并确认邮件服务器是否能够正常响应连接请求。这一测试步骤对于确保邮件服务的正常运行至关重要。

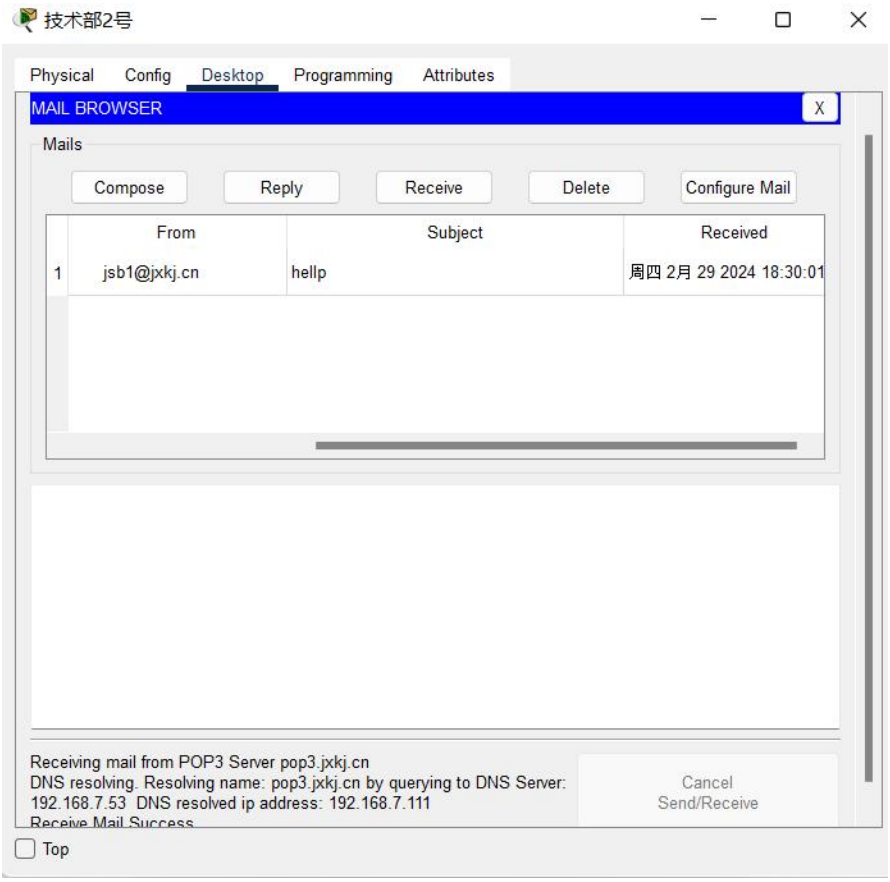

图 6.8 用户之间相互发送消息

4. 网站连通性验证

在公司网络中，测试网站是否存活通常涉及使用命令来检测其连通性和存活状态。例如，通过使用 ping 或 curl 等命令，可以快速验证网站的响应情况，确保网络的连通性。这一测试步骤有助于及时发现并解决网络问题。

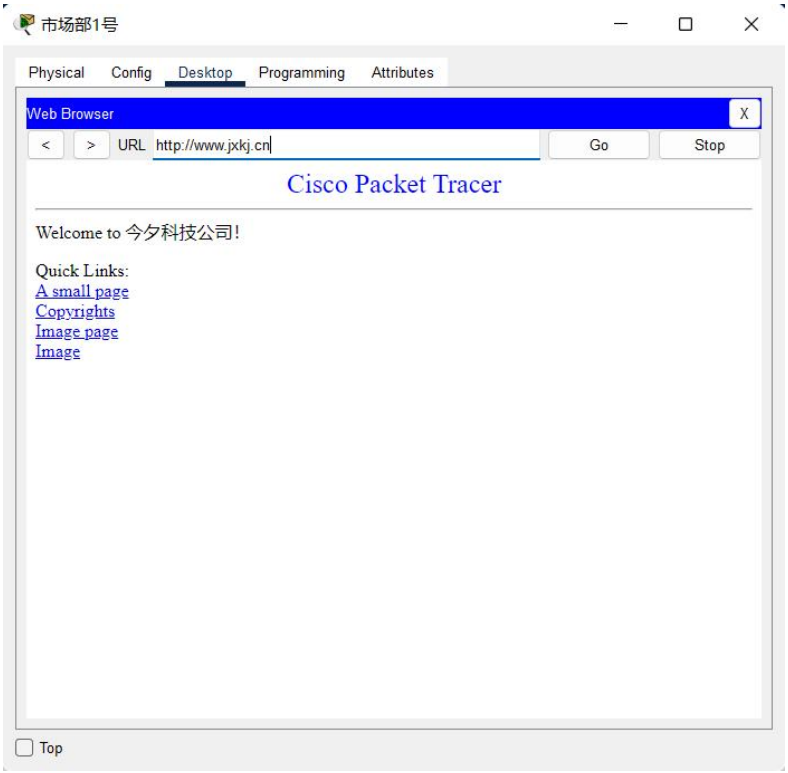

图 6.9 访问公司官网首页

七、 应急方案

（一）公司网络应急方案概述

为确保公司网络在面对网络故障、设备故障或自然灾害等突发情况时能够稳定运行，我们精心制定了一套全面且高效的应急方案。该方案的核心目标是在突发事件发生时，能够迅速、精准地采取应对措施，最大限度地降低网络服务中断时间，减少数据损失，从而保障公司的日常办公和关键信息存储不受影响。通过这一应急方案，我们致力于构建一个更加稳健、可靠的网络环境，为公司的持续运营提供坚实的技术支撑。

（二）网络设备故障应急处理

当网络设备出现故障时，我们将依据以下详细步骤进行应急处理：

（1）快速故障定位：借助先进的网络监控工具或专业命令，迅速锁定故障的具体位置与原因，为后续的处理措施提供准确依据。

（2）备用设备切换：若存在备用设备，我们将立即启动备用设备，无缝切换网络服务，确保网络连接的连续性，最大程度减少对业务的影响。

（3）技术支持求助：若故障超出自身解决能力范围，我们将第一时间联系设备厂商的专业技术支持团队，提供详细的故障信息，寻求专业的技术援助，以加快问题解决速度。

（4）故障信息记录：无论故障是否解决，我们都将详细记录故障发生的时间、现象、处理过程及最终结果，这些记录将作为后续故障分析、预防措施制定以及设备维护的重要参考依据。

通过以上严谨且高效的应急处理措施，我们能够确保在面对网络设备故障时，能够迅速响应并妥善解决，保障公司网络的稳定运行，为公司的日常运营提供坚实的网络保障。

参考资料

[1]《中小型企业局域网的设计和规划（论文）》道客巴巴，2023 年 12 月.

[2]《局域网组建教学中模块化教学法的实践》于涛，发明与创新（职业教育），2024 年第 08 期.

[3]《办公局域网组建维护和安全防护方法研究》凡荣，网络安全技术与应用，2024 年第 04 期.

[4]《计算机局域网组建和设计中防火墙技术的运用分析》郑随泰，现代职业教育，2023 年第 05 期.

[5]《小型公司局域网组建与配置》刘雪梅，信息与电脑（理论版），2024 年第 18 期.

[6]《中小企业无线局域网的规划设计研究》石河子科技，2024 年第 2 期.

[7]《中小型局域网网络工程的建设和管理》数字化用户，2024 年第 11 期.

[8]《服务于新一代新闻采集系统的超高速无线局域网组建重难点技术探析》朱江，王华，杨春，数字通信世界，2023 年第 05 期.

[9]《计算机虚拟局域网的组建与应用探究》王磊，甘肃科技纵横，2024 年第 04 期.

[10]《办公局域网组建维护和安全防护方法的分析》章杰，数码世界，2023 年第 04 期.