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：龙蕊科技公司局域网规划与设计方案

学生姓名	曾德康
学生学号	010425171772
班级名称	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。除毕业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，均已在本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）：曾德承　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）：　　日 期：2025.5.15

（注：本页学生和指导教师须亲笔签名。）

目 录

一、项目概况

（一）方案设计背景与意义

龙蕊科技公司自 2018 年成立以来，经过多年发展，已拥有 200 余亩的占地面积，员工人数突破 400 人，生产厂房面积达到 4 万余平方米，在市场中占据 45% 的份额。然而，随着公司人员规模的不断扩大以及业务的持续拓展，现有的网络规划与技术逐渐暴露出诸多不足，已难以满足日益增长的办公需求。鉴于此，公司亟待制定一套全面且高效的内部局域网优化部署解决方案。

本方案的核心目标是构建一个稳定、高效、安全且易于管理的网络平台架构，以充分满足企业办公的多样化需求，确保数据传输的稳定性、安全性和高效性。为此，我们将从整体网络需求出发，深入分析并详细阐述设计目标、设计原则、网络规划原则、网络设备选型、网络安全管理等关键要素。

通过此次优化部署，企业内部用户将能够实现流畅的相互访问，无缝共享各类资源，并保障办公通讯的顺畅无阻。同时，该网络平台架构将为企业的管理工作提供有力支撑，确保工作信息能够及时、准确地处理与传输。此外，借助双冗余负载均衡技术，我们将大幅提升企业整体运行效率，确保网络的高可用性。在网络与互联网的连接方面，我们将利用运营商现有的网络资源，为企业与外部客户搭建高效的沟通渠道，架起与世界互联互通的桥梁，助力企业更好地融入社会。在这一过程中，数据传输的安全性将得到严格保障，确保企业信息在与外界交互时万无一失。

综上所述，此次局域网优化部署对于龙蕊科技公司而言，不仅是应对当前网络困境的必要举措，更是推动企业长远发展、提升竞争力的关键一步。

（二）平面结构图

企业平面结构图如图 1.1 所示：

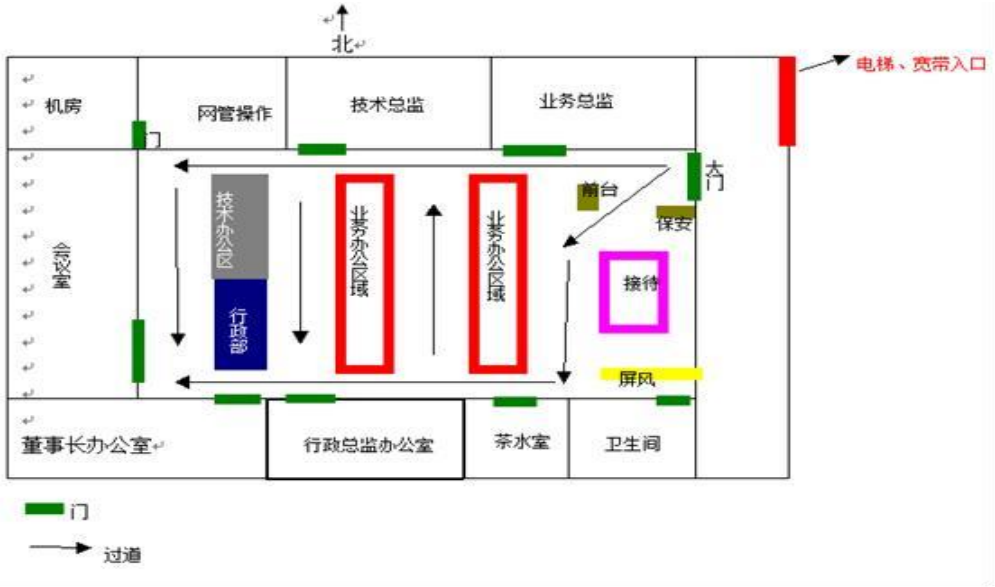

图 1.1 企业平面结构图

（三）信息点分布

为了满足龙蕊科技公司正常的业务需求，每一个区域都配置有终端，具体信息点分布如表 1.1 所示：

表 1.1 部门信息点分布情况

部门	数量	说明
市场部	42	共 1 层，分为 3 个区域，2 个区域 20 个信息点，1 个区域 2 个信息点；
财务部	24	共 1 层，分为 6 个区域，每个区域 4 个信息点；
行政部	200	共 2 层，每层设置 100 个信息点；
研发部	26	共 1 层，1 个区域 26 个信息点；
食堂	38	共 1 层，1 个区域 38 个信息点；
人事部	220	共 3 层，2 层 200 个信息点，1 层 20 个信息点；
测试部	15	共 1 层，1 个区域 15 个信息点；
总计	**565**	

二、需求分析

（一）建设目标

在 21 世纪的商业环境中，企业网络已成为企业运营的核心组成部分，其重要性在未来数年乃至更长时间内将持续凸显。企业网络是基于特定范围构建的网络系统，旨在为企业提供高效、经济的信息传输与交易处理能力，确保企业流程的有序与高效运行。同时，企业网络也是市场经济发展的必然产物，尤其在竞争激烈的市场环境中，中小企业网络建设的需求日益增长。客户对网络产品的需求正朝着多元化、高质量、高性能以及合理价格的方向发展。随着经济的快速发展和市场需求的快速变化，企业网络建设与信息技术的融合愈发紧密。

为了实现高效、稳定且安全的企业网络环境，我们计划采取以下技术措施：通过虚拟局域网（VLAN）技术实现局域网的隔离，确保各终端设备的地址分配采用静态方式，以增强网络的稳定性和可管理性；在核心设备之间部署链路聚合技术，并结合多生成树协议（MSTP）与虚拟路由冗余协议（VRRP），以显著提升办公效率；网络设备之间运行开放最短路径优先（OSPF）协议，优化网络路径选择；利用防火墙的网络地址转换（NAT）技术，确保信息安全；此外，还将搭建覆盖全公司的无线网络，进一步提高办公效率，满足员工随时随地接入网络的需求。

（二）需求描述

1.业务需求

（1）随着企业数据量和应用系统的快速增长，以及网络设备的不断增加，网络区域的扩展性成为关键考量因素。网络架构需要具备足够的灵活性和可扩展性，以适应未来业务的持续增长，确保网络能够无缝扩展，满足日益增长的业务需求。

（2）企业核心业务高度依赖网络进行数据存储与传输，因此业务活动的可用性和可靠性至关重要。同时，信息的保密性以及敏感信息的保护也是企业网络建设的核心需求，必须确保网络能够有效保障信息安全，防止数据泄露或未经授权的访问。

（3）用户在访问、传输或修改信息时，网络响应速度必须足够快，不能对业务工作造成任何影响。网络系统需要具备高效的性能，确保用户能够快速获取所需资源，提升工作效率。

（4）应用系统应具备良好的适应性，能够满足用户不断变化的需求。企业服务与应用需求需涵盖文件传输和互联网信息服务，网络架构应为这些服务提供稳定、高效的支持，确保业务流程的顺畅运行。

2.功能需求

（1）对网络进行合理规划，划分不同功能区域，确保网络架构清晰、高效，满足企业的多样化业务需求。

（2）对网络上下行流量进行精准管控，优化流量分配，避免网络拥堵，确保关键业务的优先传输，提升网络整体性能。

（3）采用双核心企业网架构，防止单点故障。同时，针对二层网络和三层网络的容灾问题，引入虚拟路由冗余协议（VRRP）技术，实现网络设备的冗余与负载均衡，确保网络的高可用性。

（4）在网络配置中，重点关注开放最短路径优先（OSPF）、多生成树协议（MSTP）、虚拟路由冗余协议（VRRP）等关键技术的合理部署与优化，以提升网络的整体性能和稳定性。

3.安全需求

（1）确保内外网访问的安全性，防止内部数据信息及网络信息外泄。网络架构需要具备强大的安全防护机制，抵御外部攻击，同时防止内部数据泄露，保障企业信息安全。

（2）避免因企业网络管理不善、员工上网行为失控或设备外联导致内网信息泄露。为此，需要对员工的上网行为进行严格管理，并设置外联告警机制，及时发现并阻止潜在的安全风险。

（3）采用网络双机热备方式，确保在出现灾难性故障时，能够快速恢复到正常运行状态，最大限度减少停机时间，保障企业业务的连续性。

三、方案设计

（一）组网设计

1.设计思路

在龙蕊科技公司的网络设计与规划过程中，我们深入研究了国内外先进的网络技术与规划理念，结合企业的实际规模、业务背景以及安全需求，明确了主干网络架构和技术方向。通过对企业的全面调研，我们确定了网络设计的核心目标：构建一个安全、高效、可扩展的网络系统，为企业的信息化发展提供坚实基础。

在设计阶段，我们严格遵循以下基本要求：首先，将设计原则与标准有机结合，确保方案的科学性和实用性；其次，优化网络结构，充分考虑未来的扩展性，为企业的发展预留空间；第三，保障网络的高性能和安全性，确保企业数据传输的稳定性和保密性；最后，支持业务的扩展和多业务融合，满足企业多样化的业务需求。

2.设计原则

随着信息化技术与企业经营的深度融合，计算机网络已成为企业信息化建设的核心。企业的信息共享和业务自动化高度依赖于网络的稳定性和安全性。因此，构建一个安全可靠、高效经济、易于管理的大型企业网络，是企业信息化发展的关键。

在方案设计中，我们严格遵循以下原则：

（1）实用性原则：通过深入的需求分析，设计出合理化的网络架构，确保网络能够满足企业的实际运行需求，同时避免过度设计，为企业节省投资成本。

（2）可靠性原则：采用 MSTP（多生成树协议）与 VRRP（虚拟路由冗余协议）相结合的技术方案，确保在第一跳路由设备出现故障时，网络仍能正常运行。同时，通过 OSPF（开放最短路径优先）路由协议实现高效的路由信息发布与计算，选择最适合的网络设备，保障网络的高可用性。

（3）先进性原则：采用先进且成熟的 TCP/IP 网络协议标准，确保网络能够适应未来发展的性能需求，保障网络的长期稳定运行。

（4）安全性原则：制定严格的安全规则，利用 NAT（网络地址转换）技术限制外部数据访问，对员工上网行为进行有效管理，严格限制非法外联等行为，全方位保护企业网络、信息及设备的安全。

（5）可扩展性原则：考虑到企业未来的发展需求，方案在架构和技术设计上充分预留了扩展空间，确保网络能够快速适应企业规模的扩大和业务的增长。

（6）可管理性原则：通过先进的设备和管理工具，实现对网络的统一管理，提升网络管理员的工作效率，同时增强网络的可管理性，确保网络运行的高效性和稳定性。

（二）VLAN 及 IP 地址规划

根据企业实际需求，VLAN 及 IP 地址规划如表 3.1 所示：

表 3.1 企业 VLAN 及 IP 地址规划表

VLAN 编号	网络地址	子网掩	区域
VLAN 10	192.168.10.0	24	市场部
VLAN 20	192.168.20.0	24	财务部
VLAN 30	192.168.30.0	24	行政部
VLAN 40	192.168.40.0	24	研发部
VLAN 50	192.168.50.5	24	食堂
VLAN 60	192.168.60.0	24	人事部
VLAN 70	192.168.70.0	24	测试部
VLAN 80	192.168.80.0	24	访客
VLAN 90	192.168.90.0	24	服务器

（三）网络设计

1.核心层设计

在核心层方案中，我们部署了两台高性能企业级核心交换机，以满足网络数据的快速转发需求。核心层作为网络的核心枢纽，上接出口路由器，共同构成网络的主干区域；下接汇聚层交换机，形成非骨干区域。内部网络通过 OSPF（开放最短路径优先）路由协议实现高效通信。

核心层作为网络的骨干部分，承担着整个网络外部访问流量的承载任务。为了简化终端设备的维护工作，核心层配置了 DHCP（动态主机配置协议）服务器，为各区域主机自动分配 IP 地址。同时，采用 VRRP（虚拟路由冗余协议）与 MSTP（多生成树协议）相结合的技术方案，其中一台设备作为主网关，另一台设备作为备用网关，确保网络的高可用性和稳定性。

2.汇聚层设计

汇聚层方案同样采用了两台企业级核心交换机，其主要职责是为接入层终端设备提供地址分配、路由服务等，并严格控制接入层对核心层及其他区域的访问，从而保障内部网络的安全性和稳定性。汇聚层与核心层的两台交换机共同构成主干区域，通过将下行网络路由信息重分布到 OSPF 路由区域，实现高效的路由管理。

数据中心和技术区是企业的重要信息区域，为了确保企业信息安全，我们采用标准的 ACL（访问控制列表）技术，禁止其他区域对数据中心区和技术区的访问。在汇聚层设计中，通过 MSTP 技术实现数据的分流负载，同时消除网络环路。其中一台设备作为主根，另一台设备作为备用根，进一步提升网络的可靠性。

3.接入层设计

接入层是终端设备接入网络并进行数据传输的关键通道。为了减少各区域终端设备之间的广播域信息传递，我们通过 VLAN（虚拟局域网）技术将各个区域划分到不同的 VLAN 中，使每个区域形成独立的网络环境。各区域之间无法直接进行数据交换，这不仅为区域管理者提供了便利，还有效保障了数据的安全性以及整体网络运行的稳定性。接入层的上行接口与汇聚层连接时，需允许所有 VLAN 通过，以确保网络的连通性。

4.出口设计

方在出口设计中，我们将网络划分为内网和外网，采用一台高性能企业级防火墙作为出口设备。内部网络通过 OSPF 路由协议与出口防火墙及内网三层设备实现高效连接。为了最大限度地节约 IP 地址资源，内网全部采用私有 IP 地址，而外网则连接互联网。

由于内网 IP 地址的安全性是网络安全的关键环节之一，我们采用了 NAT（网络地址转换）技术。通过 NAT 技术，路由器可以将局域网内所有设备的对外访问数据包转换为出接口的 IP 地址进行转发。同时，NAT 技术还可以隐藏内网主机的真实 IP 地址，仅暴露与公网连接接口的公网 IP 地址，从而有效避免外部攻击者通过内网 IP 地址发起攻击，进一步提升网络的整体安全性。

四、方案实施

（一）网络拓扑图

龙蕊科技公司的局域网主要包括核心层、汇聚层/接入层等，所有设备都汇聚到核心交换机上，方案实施采用 eNSP 模拟器进行仿真实现，企业的网络拓扑图如图 4.1 所示。

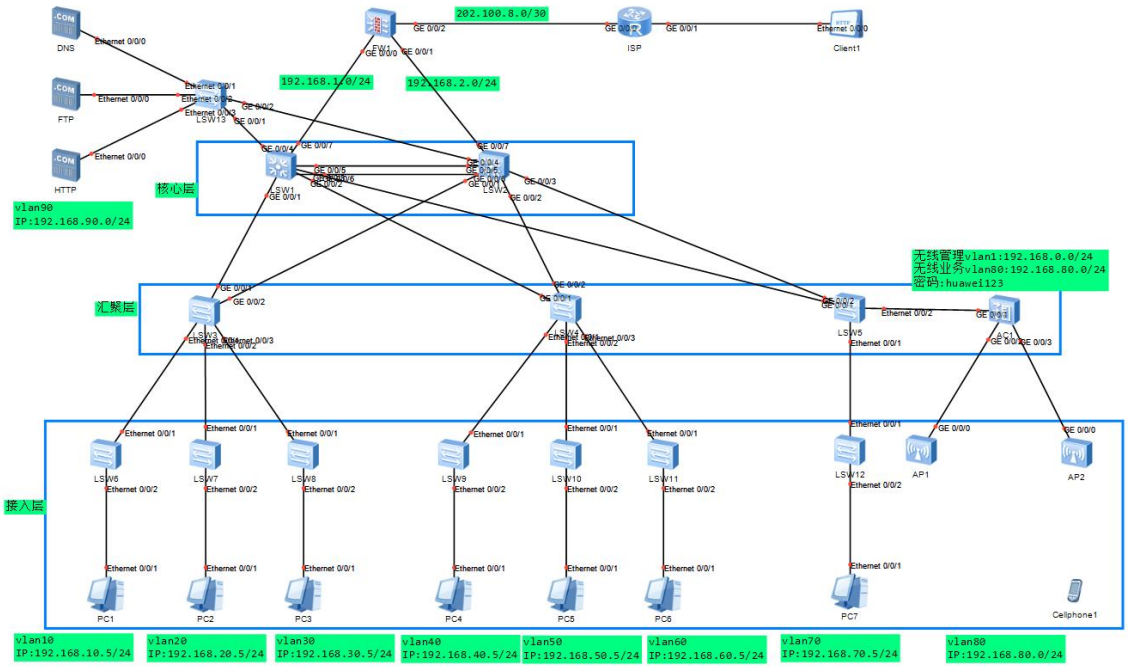

图 4.1 龙蕊科技公司网络拓扑图

（二）主要设备选型

1. 核心层

核心层设备选型如表 4.1 所示，方案仿真实现核心层交换机采用华为 S5700：

参数项	华为 S9306
产品类型	路由交换机 POE 交换机
应用层级	三层
背板带宽	6Tbps

包转发率	1152Mpps
端口结构	模块化
电源功率	1600W

表 4.1 核心层设备

2.汇聚层

汇聚层设备选型如表 4.2 所示，方案仿真实现汇聚层交换机采用华为 S3700：

表 4.2 汇聚层设备

参数项	华为 S5720-36C-EI-28S-AC
产品类型	千兆以太网交换机
应用层级	三层
背板带宽	598Gbps/5,98Tpbs
包转发率	222Mpps
端口结构	非模块化
传输速率	10/100/1000
电源功率	47.9W

3.接入层

接入层设备选型如表 4.3 所示，方案仿真实现接入层交换机采用华为 S3700：

表 4.3 接入层设备

参数项	华为 S5720-52p-SI-AC
产品类型	千兆以太网交换机
应用层级	三层
包转发率	96pps

端口结构	非模块化
传输速率	52
背板带宽	336Gbps/3.024Tpbs
传输速率	10/100/1000

4.出口路由器

出口防火墙设备选型如表 4.4 所示，方案仿真实现出口路由器采用华为 SG5500：

表 4.4 出口防火墙设备

设备类型	中小型企业级防火墙
参数项	2*GE(SFP)+10*GE
VPN 支持	支持丰富可靠的 VPN 特性
入侵检测	可第一时间获取最新威胁信息
管理	带宽管理
设备类型	中小型企业级防火墙
网络端口	2*GE(SFP)+10*GE

（三）网络关键配置

1.核心层交换机

[HXSW1]vlan batch 10 20 30 40 50 60 70 80 90 // 批量创建 VLAN 10 到 VLAN 90

[HXSW1]interface GigabitEthernet0/0/1 // 进入接口 GigabitEthernet0/0/1 的配置模式

[HXSW1-GigabitEthernet0/0/1] port link-type trunk // 将接口配置为 Trunk 模式

[HXSW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HXSW1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2 // 进入接口 GigabitEthernet0/0/2 的配置模式

[HXSW1-GigabitEthernet0/0/2] port link-type trunk // 将接口配置为 Trunk 模式

[HXSW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HXSW1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/3 // 进入接口 GigabitEthernet0/0/3 的配置模式

[HXSW1-GigabitEthernet0/0/3] port link-type trunk // 将接口配置为 Trunk 模式

[HXSW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HXSW1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/4 // 进入接口 GigabitEthernet0/0/4 的配置模式

[HXSW1-GigabitEthernet0/0/4] port link-type trunk // 将接口配置为 Trunk 模式

[HXSW1-GigabitEthernet0/0/4] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HXSW1-GigabitEthernet0/0/4]interface Eth-Trunk0 // 进入 Eth-Trunk0 的配置模式，用于配置链路聚合

[HXSW1-Eth-Trunk0] port link-type trunk // 将链路聚合接口配置为 Trunk 模式

[HXSW1-Eth-Trunk0] port trunk allow-pass vlan 2 to 4094 // 允许链路聚合接口通过 VLAN 2 到 VLAN 4094 的流量

[HXSW1]interface GigabitEthernet0/0/5 // 进入接口 GigabitEthernet0/0/5 的配置模式

[HXSW1-GigabitEthernet0/0/5] eth-trunk 0 // 将接口 GigabitEthernet0/0/5 添加到链路聚合组 Eth-Trunk0

[HXSW1]interface GigabitEthernet0/0/6 // 进入接口 GigabitEthernet0/0/6 的配置模式

[HXSW1-GigabitEthernet0/0/6] eth-trunk 0 // 将接口 GigabitEthernet0/0/6 添加到链路聚合组 Eth-Trunk0

[HXSW1-GigabitEthernet0/0/6]qu // 退出当前接口配置模式

[HXSW1]stp region-configuration // 进入 MSTP（多生成树协议）区域配置模式

[HXSW1-mst-region] region-name net // 配置 MSTP 区域名称为 "net"

[HXSW1-mst-region] instance 1 vlan 10 20 30 90 // 将 VLAN 10、20、30 和 90 映射到 MSTP 实例 1

[HXSW1-mst-region] instance 2 vlan 40 50 60 70 80 // 将 VLAN 40、50、60、70 和 80 映射到 MSTP 实例 2

[HXSW1-mst-region] active region-configuration // 激活 MSTP 区域配置，使配置生效

[HXSW1]stp instance 1 root primary // 将当前设备配置为 MSTP 实例 1 的主根桥，确保该设备在实例 1 中具有最高优先级

[HXSW1]stp instance 2 root secondary // 将当前设备配置为 MSTP 实例 2 的次根桥，确保在网络中提供冗余路径

[HXSW1]interface Vlanif10 // 进入 VLAN 接口 10 的配置模式

[HXSW1-Vlanif10] ip address 192.168.10.252 255.255.255.0 // 为 VLAN 接口 10 配置 IP 地址 192.168.10.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif10] vrrp vrid 10 virtual-ip 192.168.10.254 // 配置 VRRP（虚拟路由冗余协议）虚拟 IP 地址为 192.168.10.254，VRID 为 10

[HXSW1-Vlanif10] vrrp vrid 10 priority 115 // 设置 VRRP 组 10 的优先级为 115，优先级越高越优先成为主网关

[HXSW1]interface Vlanif20 // 进入 VLAN 接口 20 的配置模式

[HXSW1-Vlanif20] ip address 192.168.20.252 255.255.255.0 // 为 VLAN 接口 20 配置 IP 地址 192.168.20.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif20] vrrp vrid 20 virtual-ip 192.168.20.254 // 配置 VRRP 虚拟 IP 地址为 192.168.20.254，VRID 为 20

[HXSW1-Vlanif20] vrrp vrid 20 priority 115 // 设置 VRRP 组 20 的优先级为 115

[HXSW1]interface Vlanif30 // 进入 VLAN 接口 30 的配置模式

[HXSW1-Vlanif30] ip address 192.168.30.252 255.255.255.0 // 为 VLAN 接口 30 配置 IP 地址 192.168.30.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif30] vrrp vrid 30 virtual-ip 192.168.30.254 // 配置 VRRP 虚拟 IP 地址为 192.168.30.254，VRID 为 30

[HXSW1-Vlanif30] vrrp vrid 30 priority 115 // 设置 VRRP 组 30 的优先级为 115

[HXSW1]interface Vlanif40 // 进入 VLAN 接口 40 的配置模式

[HXSW1-Vlanif40] ip address 192.168.40.252 255.255.255.0 // 为 VLAN 接口 40 配置 IP 地址 192.168.40.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif40] vrrp vrid 40 virtual-ip 192.168.40.254 // 配置 VRRP 虚拟 IP 地址为 192.168.40.254，VRID 为 40

[HXSW1-Vlanif40] vrrp vrid 40 priority 115 // 设置 VRRP 组 40 的优先级为 115

[HXSW1]interface Vlanif50 // 进入 VLAN 接口 50 的配置模式

[HXSW1-Vlanif50] ip address 192.168.50.252 255.255.255.0 // 为 VLAN 接口 50 配置 IP 地址 192.168.50.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif50] vrrp vrid 50 virtual-ip 192.168.50.254 // 配置 VRRP 虚拟 IP 地址为 192.168.50.254，VRID 为 50

[HXSW1-Vlanif50] vrrp vrid 50 priority 115 // 设置 VRRP 组 50 的优先级为 115

[HXSW1]interface Vlanif60 // 进入 VLAN 接口 60 的配置模式

[HXSW1-Vlanif60] ip address 192.168.60.252 255.255.255.0 // 为 VLAN 接口 60 配置 IP 地址 192.168.60.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif60] vrrp vrid 60 virtual-ip 192.168.60.254 // 配置 VRRP 虚拟 IP 地址为 192.168.60.254，VRID 为 60

[HXSW1-Vlanif60] vrrp vrid 60 priority 110 // 设置 VRRP 组 60 的优先级为 110

[HXSW1]interface Vlanif70 // 进入 VLAN 接口 70 的配置模式

[HXSW1-Vlanif70] ip address 192.168.70.252 255.255.255.0 // 为 VLAN 接口 70 配置 IP 地址 192.168.70.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif70] vrrp vrid 70 virtual-ip 192.168.70.254 // 配置 VRRP 虚拟 IP 地址为 192.168.70.254，VRID 为 70

[HXSW1-Vlanif70] vrrp vrid 70 priority 110 // 设置 VRRP 组 70 的优先级为 110

[HXSW1]interface Vlanif80 // 进入 VLAN 接口 80 的配置模式

[HXSW1-Vlanif80] ip address 192.168.80.252 255.255.255.0 // 为 VLAN 接口 80 配置 IP 地址 192.168.80.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif80] vrrp vrid 80 virtual-ip 192.168.80.254 // 配置 VRRP 虚拟 IP 地址为 192.168.80.254，VRID 为 80

[HXSW1-Vlanif80] vrrp vrid 80 priority 110 / 设置 VRRP 组 80 的优先级为 110

[HXSW1]interface Vlanif90 // 进入 VLAN 接口 90 的配置模式

[HXSW1-Vlanif90] ip address 192.168.90.252 255.255.255.0 // 为 VLAN 接口 90 配置 IP 地址 192.168.90.252，子网掩码为 255.255.255.0

[HXSW1-Vlanif90] vrrp vrid 90 virtual-ip 192.168.90.254 // 配置 VRRP 虚拟 IP 地址为 192.168.90.254，VRID 为 90

[HXSW1-Vlanif90] vrrp vrid 90 priority 115 // 设置 VRRP 组 90 的优先级为 115

[HXSW1]dhcp enable // 启用全局 DHCP 功能，允许交换机作为 DHCP 服务器分配 IP 地址

[HXSW1]ip pool sta // 创建一个名为 "sta" 的 IP 地址池，用于分配 IP 地址

Info:It's successful to create an IP address pool // 系统提示成功创建了 IP 地址池

[HXSW1-ip-pool-sta] gateway-list 192.168.80.254 // 为 IP 地址池 "sta" 指定默认网关为 192.168.80.254

[HXSW1-ip-pool-sta] network 192.168.80.0 mask 255.255.255.0 // 指定 IP 地址池 "sta" 的网络范围为 192.168.80.0/24

[HXSW1-ip-pool-sta] dns-list 192.168.90.1 // 为 IP 地址池 "sta" 指定 DNS 服务器地址为 192.168.90.1

[HXSW1]interface Vlanif80 // 进入 VLAN 接口 80 的配置模式

[HXSW1-Vlanif80] dhcp select global // 在 VLAN 接口 80 上启用全局 DHCP 功能，允许从全局 DHCP 地址池分配 IP 地址

[HXSW1-Vlanif80]qu // 退出 VLAN 接口 80 的配置模式

[HXSW1]vlan 11 // 创建 VLAN 11

[HXSW1]interface GigabitEthernet0/0/7 // 进入接口 GigabitEthernet0/0/7 的配置模式

[HXSW1-GigabitEthernet0/0/7] port link-type access // 将接口配置为接入模式，用于连接终端设备

[HXSW1-GigabitEthernet0/0/7] port default vlan 11 // 将接口分配到 VLAN 11

[HXSW1]interface Vlanif11 // 进入 VLAN 接口 11 的配置模式

[HXSW1-Vlanif11] ip address 192.168.1.2 255.255.255.0 / 为 VLAN 接口 11 配置 IP 地址 192.168.1.2，子网掩码为 255.255.255.0

[HXSW1]ospf 1 router-id 2.2.2.2 // 启动 OSPF 进程 1，并设置 OSPF 路由器 ID 为 2.2.2.2

[HXSW1-ospf-1] area 0.0.0.0 // 进入 OSPF 区域 0 的配置模式

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255 // 将网络 192.168.1.0/24 宣告到 OSPF 区域 0

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.30.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.40.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.50.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.60.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.70.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.80.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0] network 192.168.90.0 0.0.0.255 //同上

[HXSW1-ospf-1-area-0.0.0.0]qu

2. 汇聚层交换机

[HJSW1]vlan batch 10 20 30 // 批量创建 VLAN 10、20 和 30

[HJSW1]interface Ethernet0/0/1 // 进入接口 Ethernet0/0/1 的配置模式

[HJSW1-Ethernet0/0/1] port link-type trunk // 将接口配置为 Trunk 模式，用于传输多个 VLAN 的流量

[HJSW1-Ethernet0/0/1] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HJSW1]interface Ethernet0/0/2 // 进入接口 Ethernet0/0/2 的配置模式

[HJSW1-Ethernet0/0/2] port link-type trunk // 将接口配置为 Trunk 模式

[HJSW1-Ethernet0/0/2] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HJSW1]interface Ethernet0/0/3 // 进入接口 Ethernet0/0/3 的配置模式

[HJSW1-Ethernet0/0/3] port link-type trunk // 将接口配置为 Trunk 模式

[HJSW1-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HJSW1]interface GigabitEthernet0/0/1 // 进入接口 GigabitEthernet0/0/1 的配置模式

[HJSW1-GigabitEthernet0/0/1] port link-type trunk // 将接口配置为 Trunk 模式

[HJSW1-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HJSW1]interface GigabitEthernet0/0/2 // 进入接口 GigabitEthernet0/0/2 的配置模式

[HJSW1-GigabitEthernet0/0/2] port link-type trunk // 将接口配置为 Trunk 模式

[HJSW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 4094 // 允许该 Trunk 接口通过 VLAN 2 到 VLAN 4094 的流量

[HJSW1]stp region-configuration // 进入 MSTP（多生成树协议）区域配置模式

[HJSW1-mst-region] region-name net // 配置 MSTP 区域名称为 "net"

[HJSW1-mst-region] instance 1 vlan 10 20 30 90 // 将 VLAN 10、20、30 和 90 映射到 MSTP 实例 1

[HJSW1-mst-region] instance 2 vlan 40 50 60 70 80 // 将 VLAN 40、50、60、70 和 80 映射到 MSTP 实例 2

[HJSW1-mst-region] active region-configuration // 激活 MSTP 区域配置，使配置生效

3.接入层交换机

[JRSW1]vlan batch 10 // 批量创建 VLAN 10

[JRSW1]interface Ethernet0/0/1 // 进入接口 Ethernet0/0/1 的配置模式

[JRSW1-Ethernet0/0/1] port link-type trunk // 将接口配置为 Trunk 模式，用于传输多个 VLAN 的流量

[JRSW1-Ethernet0/0/1] port trunk allow-pass vlan all // 允许该 Trunk 接口通过所有 VLAN 的流量

[JRSW1]interface Ethernet0/0/2 // 进入接口 Ethernet0/0/2 的配置模式

[JRSW1-Ethernet0/0/2] port link-type access // 将接口配置为接入模式，用于连接终端设备

[JRSW1-Ethernet0/0/2] port default vlan 10 // 将接口分配到 VLAN 10

[JRSW1-Ethernet0/0/2]

4.防火墙配置

[FW]interface GigabitEthernet0/0/0 // 进入接口 GigabitEthernet0/0/0 的配置模式

[FW-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0 // 为接口 GigabitEthernet0/0/0 配置 IP 地址 192.168.1.1，子网掩码为 255.255.255.0

[FW-GigabitEthernet0/0/0]interface GigabitEthernet0/0/1 // 进入接口 GigabitEthernet0/0/1 的配置模式

[FW-GigabitEthernet0/0/1] ip address 192.168.2.1 255.255.255.0 // 为接口 GigabitEthernet0/0/1 配置 IP 地址 192.168.2.1，子网掩码为 255.255.255.0

[FW]interface GigabitEthernet0/0/2 // 进入接口 GigabitEthernet0/0/2 的配置模式

[FW-GigabitEthernet0/0/2] ip address 202.100.8.2 255.255.255.252 // 为接口 GigabitEthernet0/0/2 配置 IP 地址 202.100.8.2，子网掩码为 255.255.255.252

[FW-GigabitEthernet0/0/2]

[FW]firewall zone trust // 进入防火墙信任区域的配置模式

[FW-zone-trust] add interface GigabitEthernet0/0/0 // 将接口 GigabitEthernet0/0/0 添加到信任区域

[FW-zone-trust] add interface GigabitEthernet0/0/1 // 将接口 GigabitEthernet0/0/1 添加到信任区域

[FW-zone-trust]

[FW]firewall zone untrust // 进入防火墙非信任区域的配置模式

[FW-zone-untrust] add interface GigabitEthernet0/0/2 // 将接口 GigabitEthernet0/0/2 添加到非信任区域

[FW]ip route-static 0.0.0.0 0.0.0.0 202.100.8.1 / 配置默认静态路由，下一跳地址为 202.100.8.1，用于访问外部网络

[FW]ospf 1 router-id 1.1.1.1 // 启动 OSPF 进程 1，并设置 OSPF 路由器 ID 为 1.1.1.1

[FW-ospf-1] default-route-advertise // 宣告默认路由到 OSPF，确保其他设备可以通过该防火墙访问外部网络

[FW-ospf-1] area 0.0.0.0 // 进入 OSPF 区域 0 的配置模式

[FW-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255 // 将网络 192.168.1.0/24 宣告到 OSPF 区域 0

[FW-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255 // 将网络 192.168.2.0/24 宣告到 OSPF 区域 0

[FW]policy interzone trust untrust outbound // 进入信任区域到非信任区域的出方向策略配置模式

[FW-policy-interzone-trust-untrust-outbound] policy 1 // 创建策略 1

[FW-policy-interzone-trust-untrust-outbound-1] action permit // 配置策略 1 的动作为允许，允许从信任区域到非信任区域的流量

[FW]nat-policy interzone trust untrust outbound // 进入信任区域到非信任区域的出方向 NAT 策略配置模式

[FW-nat-policy-interzone-trust-untrust-outbound] policy 1 // 创建 NAT 策略 1

[FW-nat-policy-interzone-trust-untrust-outbound-1] action source-nat // 配置 NAT 策略 1 的动作为源地址转换

[FW-nat-policy-interzone-trust-untrust-outbound-1] easy-ip GigabitEthernet0/0/2 // 配置使用接口 GigabitEthernet0/0/2 的 IP 地址进行 Easy IP 转换，实现内网设备访问外网

[FW-nat-policy-interzone-trust-untrust-outbound-1]qu // 退出 NAT 策略 1 的配置模式

[FW-nat-policy-interzone-trust-untrust-outbound]qu // 退出 NAT 策略配置模式

5. 无线配置

[AC]wlan // 进入无线局域网（WLAN）配置模式

[AC-wlan-view] regulatory-domain-profile name china // 创建一个名为 "china" 的监管域配置文件

[AC-wlan-regulate-domain-china] country-code cn // 设置监管域的国家代码为 "cn"（中国），以符合当地的无线法规

[AC-wlan-regulate-domain-china] quit // 退出监管域配置文件的配置模式

[AC-wlan-view] security-profile name sec_pro_wlan // 创建一个名为"sec_pro_wlan"的安全配置文件

[AC-wlan-sec-prof-sec_pro_wlan] security wpa-wpa2 psk pass-phrase huawei123 aes // 配置安全策略为 WPA/WPA2 个人模式，预共享密钥为"huawei123"，加密方式为 AES

[AC-wlan-sec-prof-sec_pro_wlan] quit // 退出安全配置文件的配置模式

[AC-wlan-view] ssid-profile name ssid_pro_wlan // 创建一个名为"ssid_pro_wlan"的 SSID 配置文件

[AC-wlan-ssid-prof-ssid_pro_wlan] ssid wlan // 设置 SSID 名称为"wlan"

[AC-wlan-ssid-prof-ssid_pro_wlan] quit // 退出 SSID 配置文件的配置模式

[AC-wlan-view] vap-profile name vap_pro_wlan // 创建一个名为"vap_pro_wlan"的虚拟接入点（VAP）配置文件

[AC-wlan-vap-prof-vap_pro_wlan] forward-mode direct-forward // 配置转发模式为直接转发

[AC-wlan-vap-prof-vap_pro_wlan] service-vlan vlan-id 80 // 将服务 VLAN 设置为 VLAN 80

[AC-wlan-vap-prof-vap_pro_wlan] security-profile sec_pro_wlan // 应用安全配置文件 "sec_pro_wlan"

[AC-wlan-vap-prof-vap_pro_wlan] ssid-profile ssid_pro_wlan // 应用 SSID 配置文件 "ssid_pro_wlan"

[AC-wlan-vap-prof-vap_pro_wlan] quit // 退出 VAP 配置文件的配置模式

[AC-wlan-view] ap-group name ap_group_wlan // 创建一个名为"ap_group_wlan"的接入点（AP）组

[AC-wlan-ap-group-ap_group_wlan] vap-profile vap_pro_wlan wlan 1 radio 0 // 在 AP 组中为无线网络 1 的无线频段 0 应用 VAP 配置文件"vap_pro_wlan"

[AC-wlan-ap-group-ap_group_wlan] vap-profile vap_pro_wlan wlan 2 radio 1 // 在 AP 组中为无线网络 2 的无线频段 1 应用 VAP 配置文件 "vap_pro_wlan"

[AC-wlan-ap-group-ap_group_wlan] regulatory-domain-profile china // 在 AP 组中应用监管域配置文件 "china"

[AC-wlan-view] ap auth-mode mac-auth // 设置接入点的认证模式为 MAC 地址认证

[AC-wlan-view] ap-id 1 ap-mac 00e0-fc18-5870 // 添加一个接入点，AP ID 为 1，MAC 地址为 00e0-fc18-5870

[AC-wlan-ap-1] ap-name wlan_ap1 // 为接入点 1 设置名称为 "wlan_ap1"

[AC-wlan-ap-1] ap-group ap_group_wlan // 将接入点 1 添加到 AP 组 "ap_group_wlan"

[AC-wlan-view] ap-id 2 ap-mac 00e0-fcd5-70d0 // 添加一个接入点，AP ID 为 2，MAC 地址为 00e0-fcd5-70d0

[AC-wlan-ap-2] ap-name wlan_ap2 // 为接入点 2 设置名称为 "wlan_ap2"

[AC-wlan-ap-2] ap-group ap_group_wlan // 将接入点 2 添加到 AP 组 "ap_group_wlan"

[AC-wlan-ap-2]q // 退出接入点 2 的配置模式

五、测试

（一）网络连通测试

通过 PC1 运行 ICMP 访问 PC3 进行连通性测试，测试如图 5.1 所示网络连通测试正常。

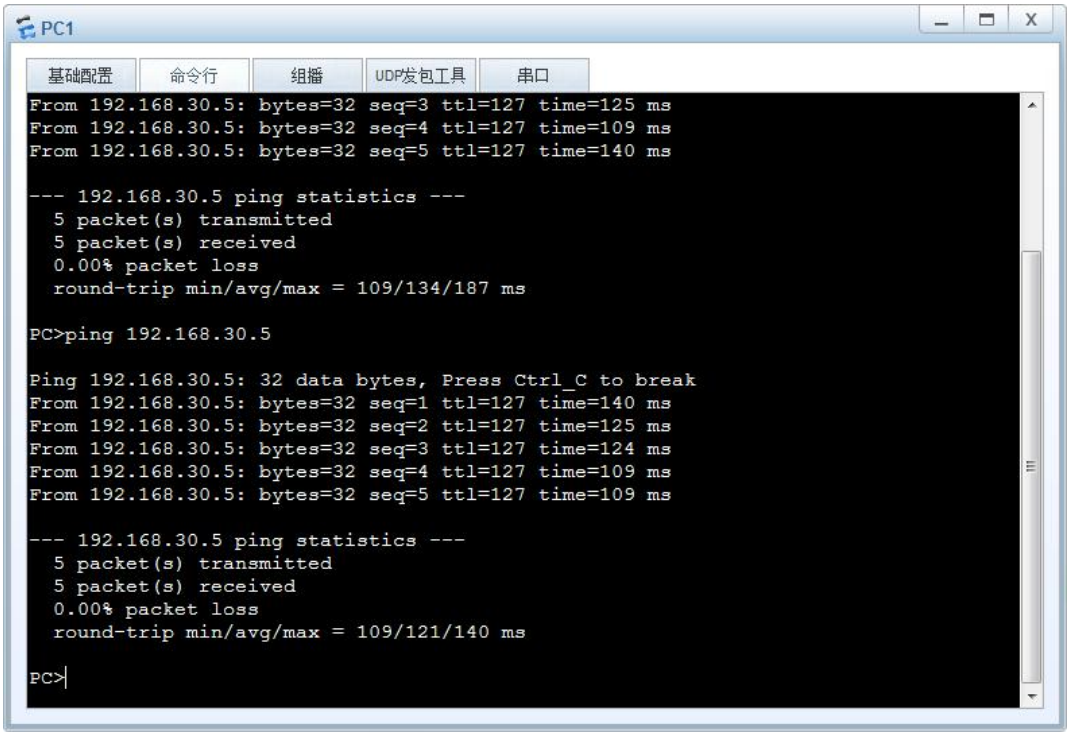

图 5.1 网络连通测试

（二）链路备份功能测试

将一台交换机宕机，通过 PC1 ping pc3 进行连通性测试，结果如图 5.2 所示网络运行正常，链路备份测试成功。

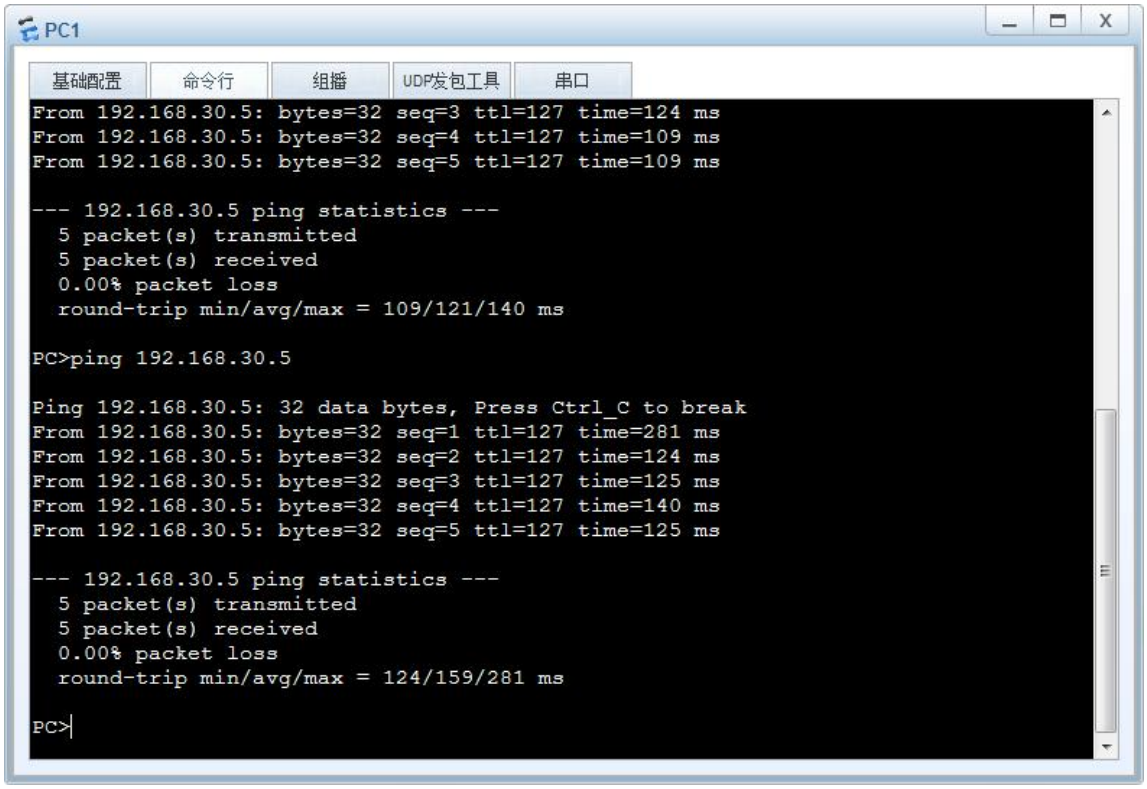

图 5.2 链路备份功能测试

（三）服务器 FTP 服务测试

通过 FTP 服务器进行文件传输，测试结果如图图 5.3 所示，文件传输成功，FTP 服务器测试成功。

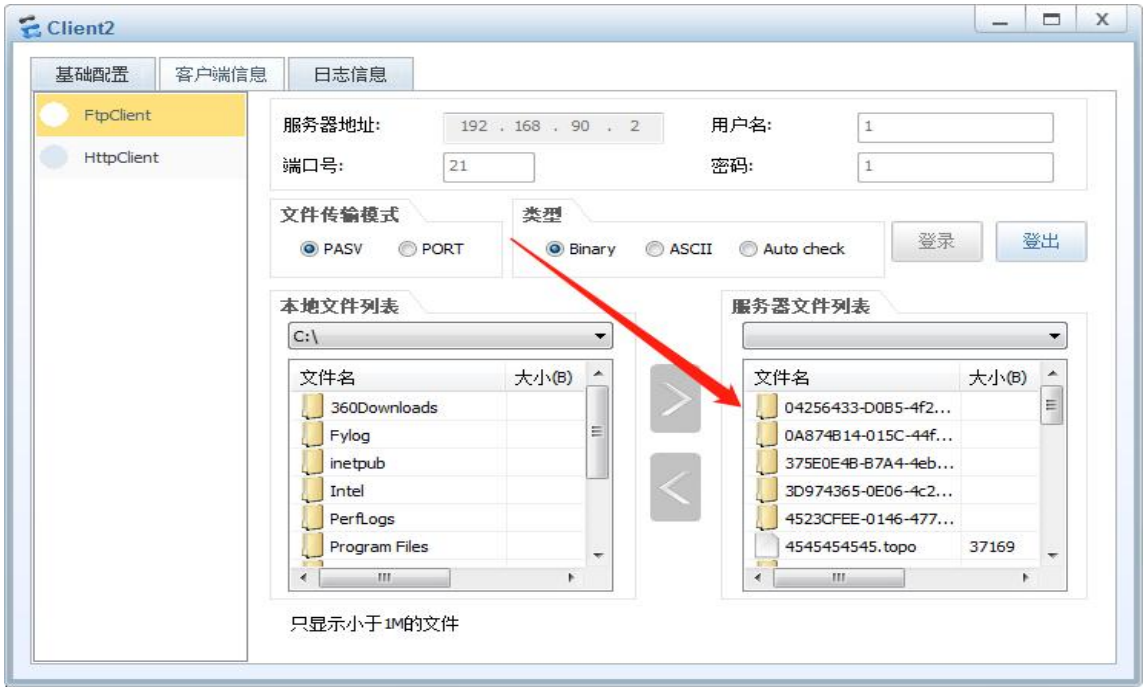

图 5.3 服务器 FTP 服务测试

（四）HTTP 服务测试

通过 HTTP 服务器进行页面访问，测试结果如图图 5.4 所示，页面访问成功，HTTP 服务器测试成功。

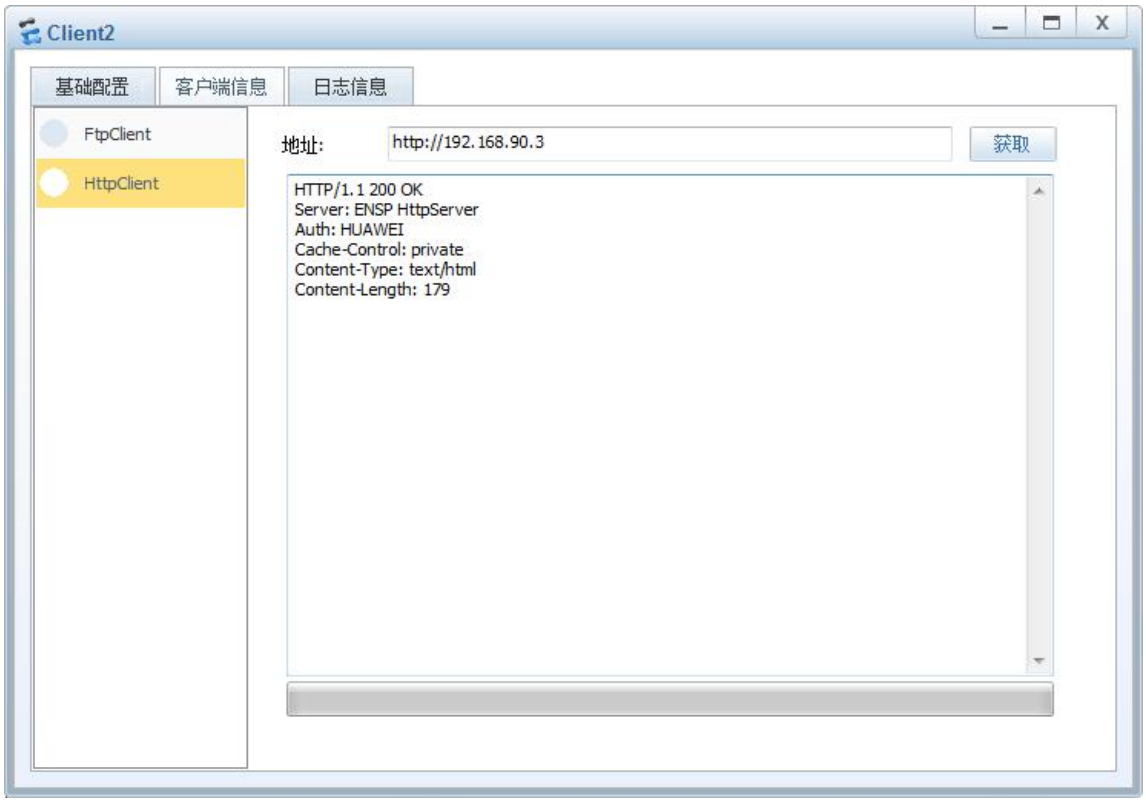

图 5.4 HTTP 服务测试

（五）无线上网连通测试

通过 STA1 运行 ICMP 访问外部网络进行连通性测试，测试如图 5.5-5.7 所示网络连通测试正常。

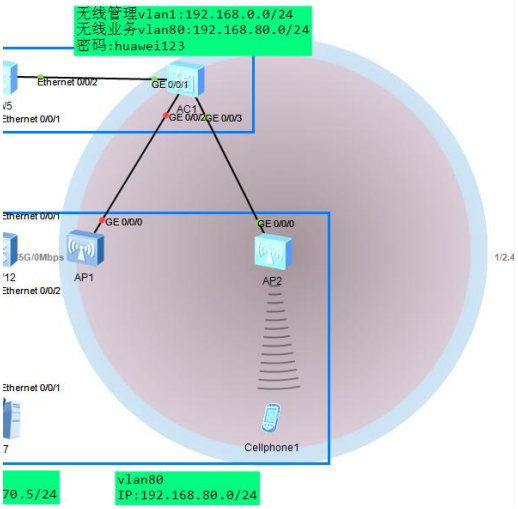

图 5.5

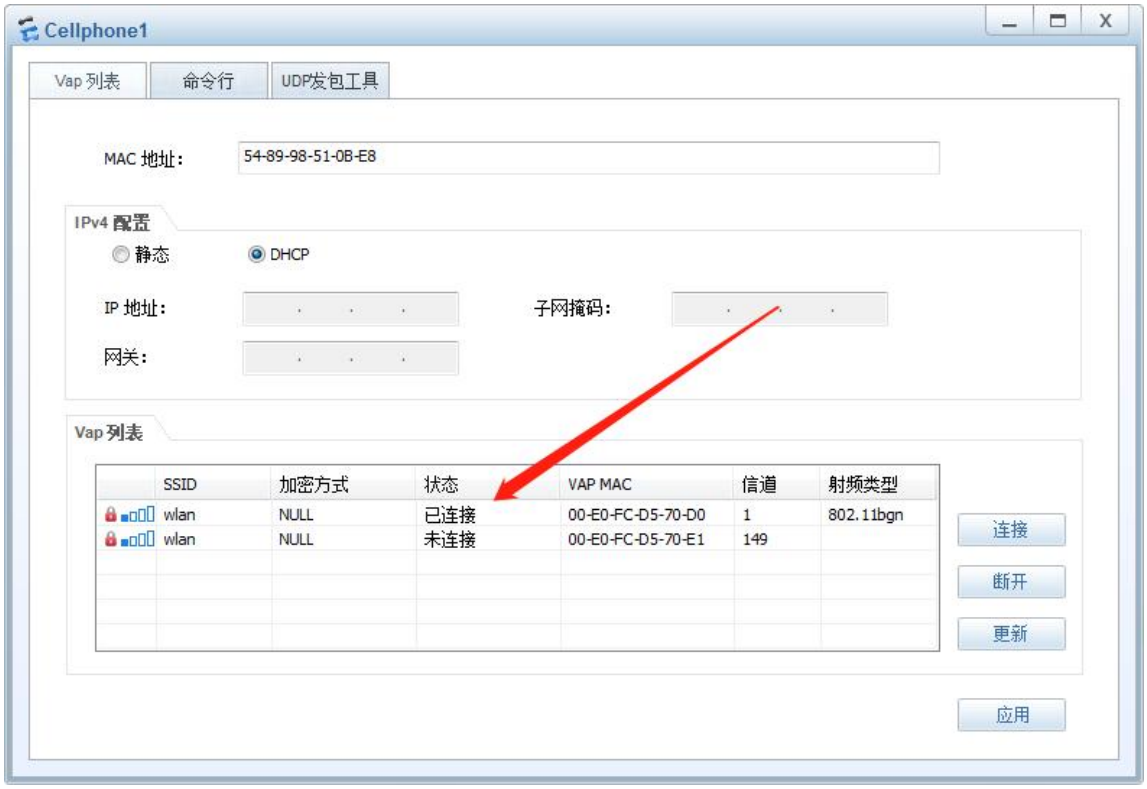

图 5.6

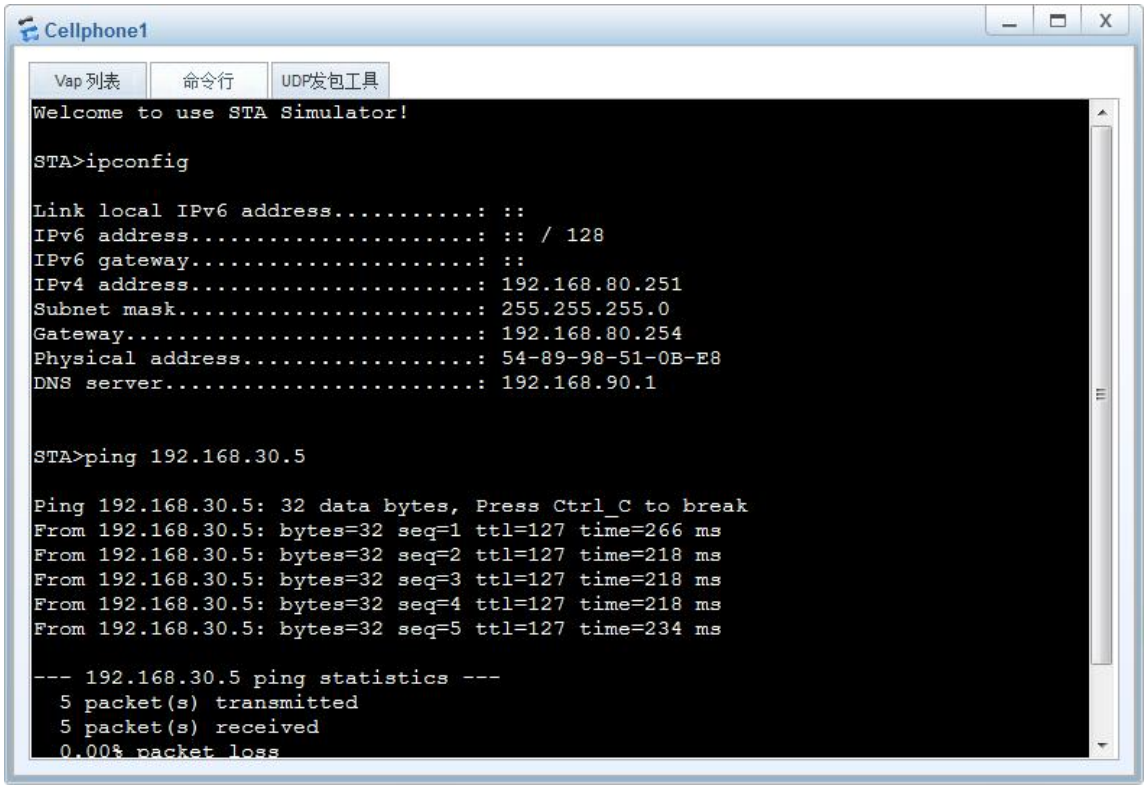

图 5.7 无线上网连通测试

（六）查看生成树

通过查看 SW1 各接口状态，测试结果如图图 5.8 所示，生成树运行正常，测试成功。

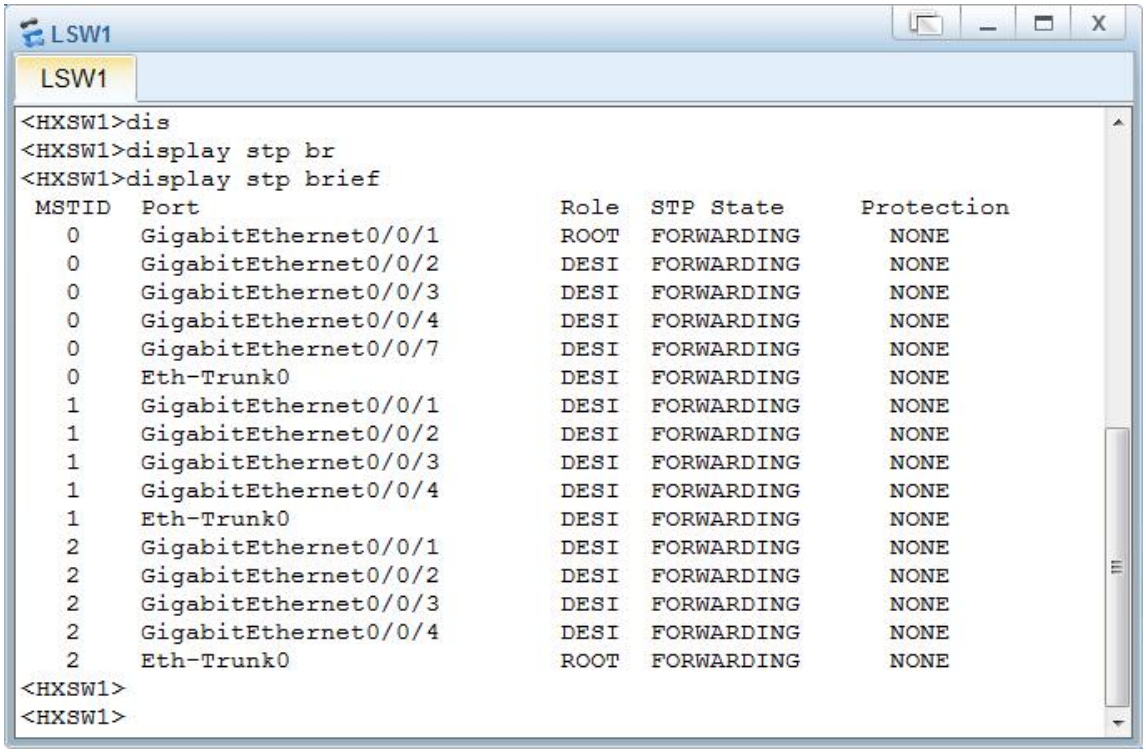

图 5.8 查看生成树

（七）查看 VRRP 及链路聚合

通过查看 SW1VRRP 状态，测试结果如图图 5.9 所示，主备运行正常，测试成功。

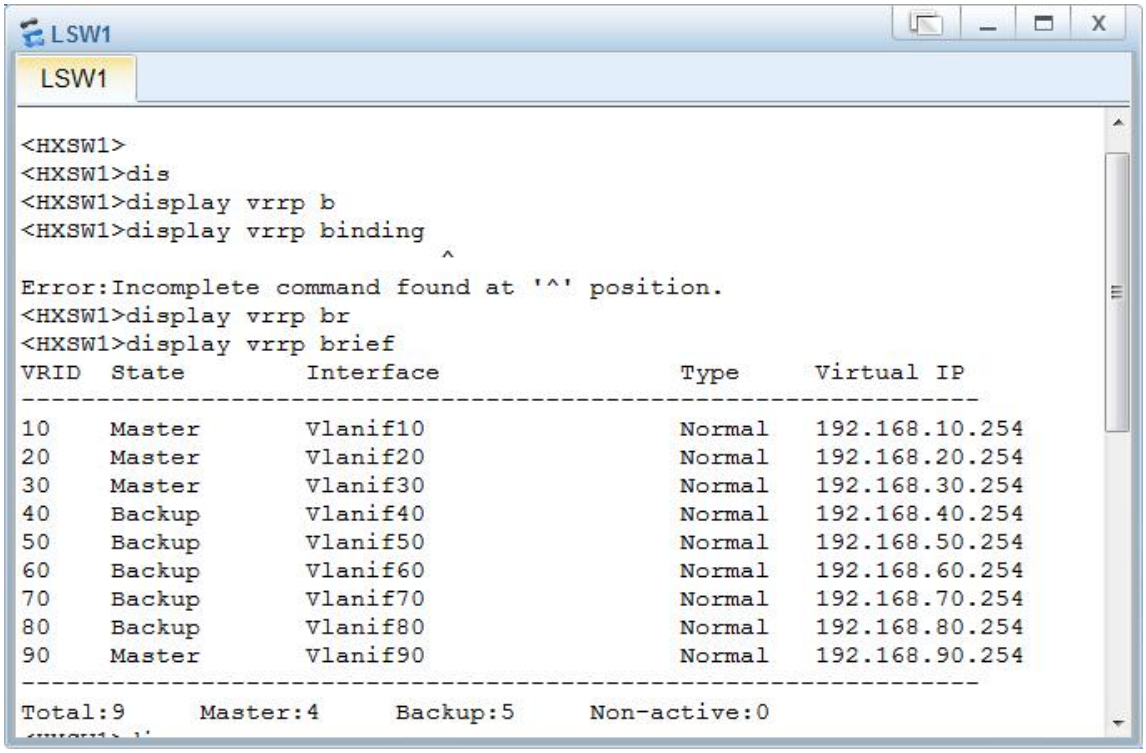

图 5.9 查看 VRRP 及链路聚合

（八）查看路由表

通过查看 FW1 的 ospf 邻居，测试结果如图图 5.10 所示，OSPF 路由协议运行正常，测试成功。

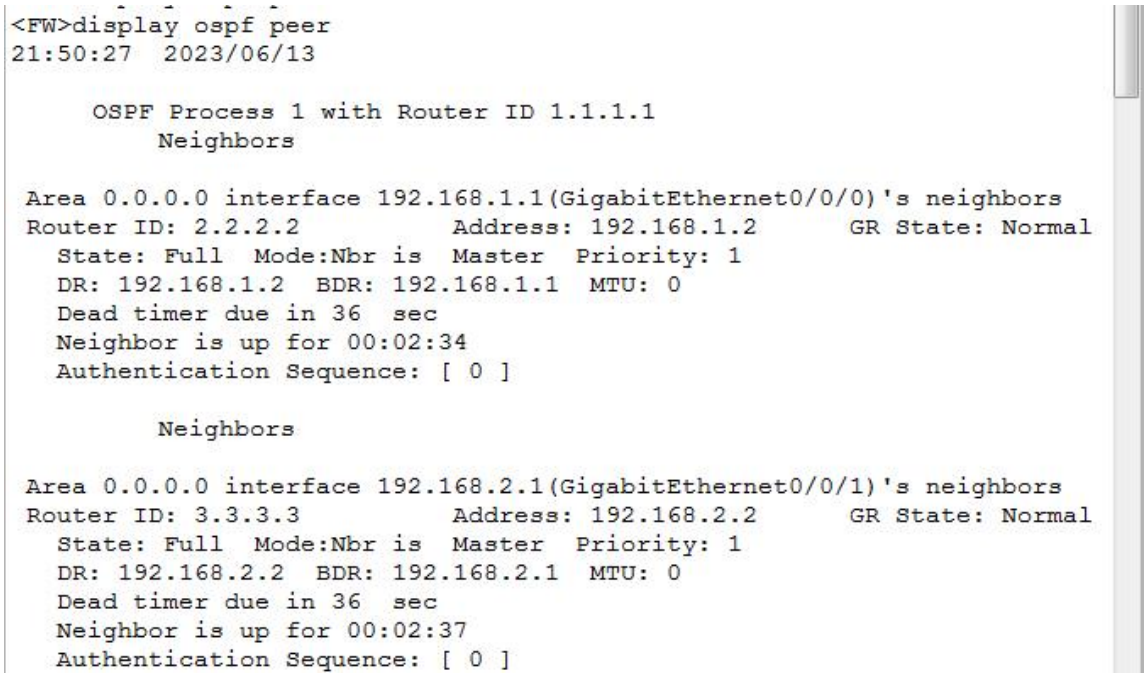

图 5.10 FW1ospf 邻居

参考资料

[1]户根勤.网络是怎样连接的[M].人民邮电出版社.2024 年.

[2]日本 Ank 软件技术公司.图解 TCP/IP 网络知识轻松入门[M].化学工业出版社.2024 年.

[3]曹雅斌.网络安全应急管理与技术实践[M].北京：清华大学出版社.2023 年.

[4]网络安全技术联盟.网络安全与攻防入门很轻松［M.清华大学出版社.2023 年.

[5]田果 刘丹宁.网络基础[M].机械工业出版社.2022 年.

[6]韩立刚.计算机网络创新教程[M].水利水电出版社.2024 年.

[7]樊胜民.网络运维从入门到精通——29 个实践项目详解[M].化学工业出版社.2023 年.

[8]H3C 网络学院系列教程.路由交换技术详解与实践 第 1 卷（下册）[M].北京：清华大学出版社.2024 年.

[9]刘建伟 等.网络安全实验教程（第 3 版[M].北京：清华大学出版社.2023 年.