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

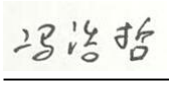
题目：怀化人民医院网络规划与设计方案

学生姓名	冯浩哲
学生学号	010425171760
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）：  日　期：2025.5.11

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：2025.5.16

（注：本页学生和指导教师须亲笔签名。）

目 录

一、项目概况

（一）设计背景及意义

随着科技的飞速发展，信息技术在各个领域都发挥着至关重要的作用，其影响力日益显著。网络技术在过去 20 年中经历了迅猛的发展，尤其是在近几年，网络产品的年产值以大约 3%的速度持续增长。为了适应时代的发展，医院网络技术也在不断更新换代，医院对网络的依赖程度越来越高。无论是日常办公、医疗服务还是医疗设备的运行，都与网络紧密相连，且对网络的性能要求也在不断提升。

互联网的普及极大地推动了医院网络化的发展。信息技术的进步不仅促进了社会的整体发展，还深刻改变了人们的生活方式。网络已经渗透到生活的方方面面，从娱乐消遣到网络购物，再到日常工作，网络已成为人们生活中不可或缺的一部分。然而，随着科技的不断进步和生活节奏的加快，传统的网络技术已无法满足现代医院的需求。医院作为提供医疗服务的重要场所，对网络的依赖尤为显著。计算机在医院的广泛应用，使得一个安全可靠的网络成为医院高效运作的关键。因此，对医院网络进行优化和改进显得尤为迫切。

21 世纪是信息时代，也是互联网时代。为了适应时代的发展，医院必须不断更新技术，提升网络性能。医院网络信息化在医护人员的工作和医疗活动中扮演着至关重要的角色。随着医院规模的不断扩大，网络的稳定性和安全性对医院的运营至关重要。一个中型医院如果网络无法正常运行，不仅会给医院内部带来巨大损失，还会影响对患者的护理和治疗。为了确保医院网络的正常运行，加强网络的安全管理，完善网络信息建设，提高医护人员的工作效率和医院的管理水平，必须建立一个高性能、高速度、实用性强、高效可靠的双核心、双链路的医院网络。这样的网络不仅能满足医院的需求，还能更好地服务患者，提升患者满意度。

（二）医院基本情况介绍

网络技术在社会、经济和文化等多个领域都扮演着重要角色，并产生了深远的影响。国内医院也需要进一步强化自身的网络信息化建设，以促进信息资源在医疗和医院内部管理中的高效利用，提高医生、医护人员和患者的满意度。以某中型医院为例，设计一个安全、稳定、高效的医院网络方案。该医院分为综合大楼、行政部、门诊部、住院部和功能科室五大部分。其中，行政部、门诊部、住院部和功能

科室的网络核心位于综合大楼。行政部分为财务部和办公室，门诊部和住院部分为内外两科，功能科室包括胃镜室、B 超室和 CT 室。

根据医院内部的规划，门诊部设定 100 个信息点，功能科室每个科室设定 30 个信息点，住院部设定 100 个信息点，行政部每个部门设定 50 个信息点。为每个信息点分配合理的 IP 地址，确保不同部门能够轻松接入现有网络。随着医院规模的不断扩大，医护人员办公、临床医疗和运营管理对医院网络的需求也在不断增加。为了满足医生和患者的需求，必须建立一个高性能、高速度、实用性强、高效可靠的医院网络。

通过以上设计，医院网络不仅能够满足当前的业务需求，还具备良好的扩展性和安全性，为医院的长期发展提供坚实的技术支持。

二、需求分析

（一）建设目标

本方案旨在根据医院的结构规模和业务需求，构建一个高效、安全、可靠的网络系统。网络设计采用三级架构：核心层、汇聚层和接入层，以满足医院不同区域的网络需求。医院整体划分为综合大楼、行政部、住院部、门诊部和功能科室五大区域。其中，行政部进一步细分为财务部和办公室；住院部分为内科和外科；门诊部同样分为内科和外科；功能科室则包括胃镜室、CT 室和 B 超室等。在设计过程中，我们首先进行了 IP 地址规划和 VLAN 划分，以实现网络的高效管理和隔离。通过 DHCP 协议自动分配 IP 地址、网关和 DNS 服务器，确保设备能够快速接入网络。采用 OSPF 协议实现不同网段间的互联互通，利用 ACL 技术保护财务部等关键部门的信息安全。结合 VRRP 和 MSTP 技术，实现网络的负载均衡、路由冗余和环路避免。出口防火墙采用 NAT 技术，实现与 Internet 的安全连接。最终，利用华为 eNSP 模拟器对医院网络环境进行模拟测试，确保网络设计的可行性和稳定性。

（二）需求分析

1、 应用需求分析

网络的连通性对医院的日常运营至关重要。医院内部的办公、文件传输与共享、患者信息管理以及医疗设备的连接等都依赖于一个安全、高效、稳定的网络环境。根据医院的服务和应用需求，网络应满足以下几个关键方面：

（1）文件传输服务

为确保医院各部门之间能够高效共享文件，我们部署了 FTP 服务。FTP 服务器存储了丰富的数据信息，医护人员可以根据自身需求随时获取所需文件，极大地方便了日常工作。

（2）互联网信息服务

医院各部门需要访问互联网以查询资料、学习新知识等。因此，网络设计中采用了 NAT 技术实现与外网的连通。同时，通过 Web 服务器（IIS）共享 Internet 上的信息资源，方便医护人员获取所需资料。

（3）多媒体辅助和远程治疗

医院需要具备数据、图像、语音和视频等多媒体通信能力，以支持远程治疗和多媒体辅助诊断。网络设计提供了足够的带宽，以满足大量用户的需求，并尽可能降低网络传输延迟。通过 DHCP 协议，设备能够快速获取网络配置，提高网络传输速度。

2、 安全性与管理分析

医院的工作性质特殊，网络安全性至关重要。保护医生和患者的个人隐私、确保财务部和办公部的信息安全是医院的重要责任。为此，网络设计采用了以下技术。

（1）访问控制列表（ACL）

通过 ACL 技术，对不同数据设置不同的访问级别，限制和开放不同人员对数据的访问权限，确保关键信息的安全。

（2）虚拟路由冗余协议（VRRP）

采用 VRRP 技术实现网络的路由冗余，确保在主路由器故障时，备用路由器能够无缝接管，保障网络的高可用性。

（3）数据备份与镜像技术

利用备份和镜像技术提高数据的完整性和可靠性，防止数据丢失或损坏。

（4）网络管理与维护

运营管理人员需定期检查网络状态，进行病毒扫描、程序漏洞修复等工作，确保网络的安全性和高效运行。

3、 实用性与经济性分析

随着医院规模的不断扩大，网络改造需要投入大量的时间和资源。因此，医院网络的设计必须兼顾实用性和经济性。实用性体现在网络的易于管理和维护、便于扩展，降低使用和操作难度，使更多人能够掌握网络技术。经济性则要求在建设过程中节约资金，确保网络具有一定的扩展性，以便在后续改造中只需进行少量改动即可满足新的需求，从而节省资源和费用。在保证实用性的基础上，同时确保经济性，将有力推动医院网络的信息化发展。

通过以上设计和分析，医院网络不仅能够满足当前的业务需求，还具备良好的扩展性和安全性，为医院的长期发展提供坚实的技术支持。

三、方案设计

（一）网络拓扑结构设计

一个优秀的设计方案应当采用分层结构，通过不同层次的划分来提升网络的可扩展性，并简化网络架构。根据医院的规模和业务需求，我们将医院划分为综合大楼、行政部、住院部、门诊部和功能科室五个主要区域。全网采用光纤连接，构建了一个合理的三级网络结构：核心层、汇聚层和接入层。为了确保医院网络的全面互通、资源共享以及安全访问，需要对相关设备进行合理的配置与管理。

1、 核心层设计

本方案的核心层配置了两台三层交换机和两台路由器，构建了一个双核心、双链路的网络架构，显著增强了网络的可靠性和稳定性。在路由设计方面，选用了 OSPF 动态路由协议，该协议具有快速收敛的特点，能够高效地实现与汇聚层及外部网络的连接。同时，结合 VRRP 和 MSTP 技术，不仅增强了路由设备的可用性，还实现了路由网关的冗余和负载均衡，无需对网络结构进行大规模改造，有效降低了管理成本，显著提升了网络性能。此外，通过 ACL 技术为不同部门设置了不同级别的访问权限，打造了一个强大的数据传输中心，为用户提供安全、可靠的网络服务。同时，采用 DHCP 协议自动分配 IP 地址。核心层的拓扑结构如图 3.1 所示：

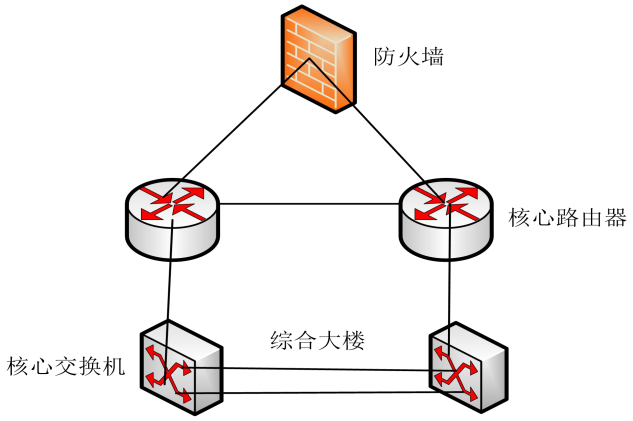


图 3.1 核心层拓扑结构图

2、 汇聚层设计

汇聚层采用了三层交换机，并设计了双链路连接，确保了网络的高可靠性和稳定性。在汇聚层交换机上应用了 MSTP 技术，有效减少了环路的产生，进一步保障了网络的可靠性，并对同一部门进行了 VLAN 划分。汇聚层交换机不仅要处理来自

接入层设备的所有通信流量，还要为上行链路到核心层提供支持，因此必须具备高性能和高效的交换速率。

3、 接入层设计

在该医院网络设计中，将医院的各个部门分别划分到独立的 VLAN 中，所有 VLAN 在核心交换机上进行 VRRP 冗余备份。同时，在汇聚层交换机上运用 MSTP 技术，将多个 VLAN 分配到不同的实例中，确保了网络的负载均衡。接入层向下能够为桌面设备提供高质量的接入速率，向上则能够将流量高效汇聚到核心层。以门诊部为例，其拓扑结构如图 3.2 所示：

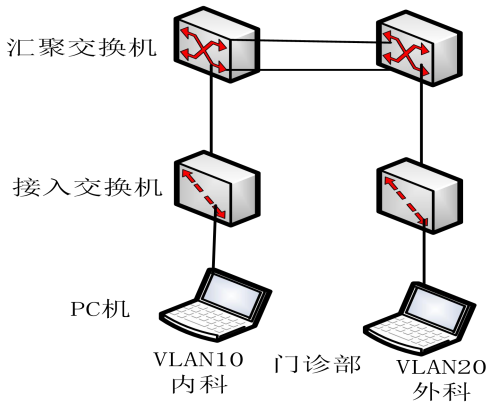


图 3.2 接入层拓扑结构图

4、 出口方案设计

由于需要与 Internet 连接，出口处必须配置防火墙解决方案，并制定严格的安全策略。这些策略允许内网访问外部网络，同时实现不同网络之间的隔离与访问控制，从而提高网络的整体安全性。通过 NAT 技术实现与 Internet 的互联，能够将局域网内部的私有 IP 地址转换为外部合法的 IP 地址，提高了 IP 地址的使用效率，同时避免了来自网络外部对内网的攻击，确保了主机能够从内部网络透明地访问外部网络。出口方案的拓扑结构如图 3.3 所示：

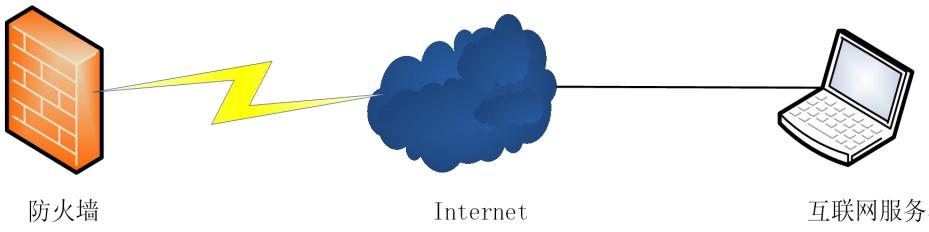


图 3.3 出口拓扑结构图

（二）网络拓扑结构

依据网络方案的规划和需求，采用双核心、双链路结构，利用相应的网络配置命令，模拟真实的医院网络环境。整个网络采用核心层、汇聚层和接入层的三层结构模式进行设计，主要由以下四部分组成：交换模块、接入模块、远程访问模块以及服务器群。具体的医院网络拓扑结构如图 3.4 所示：

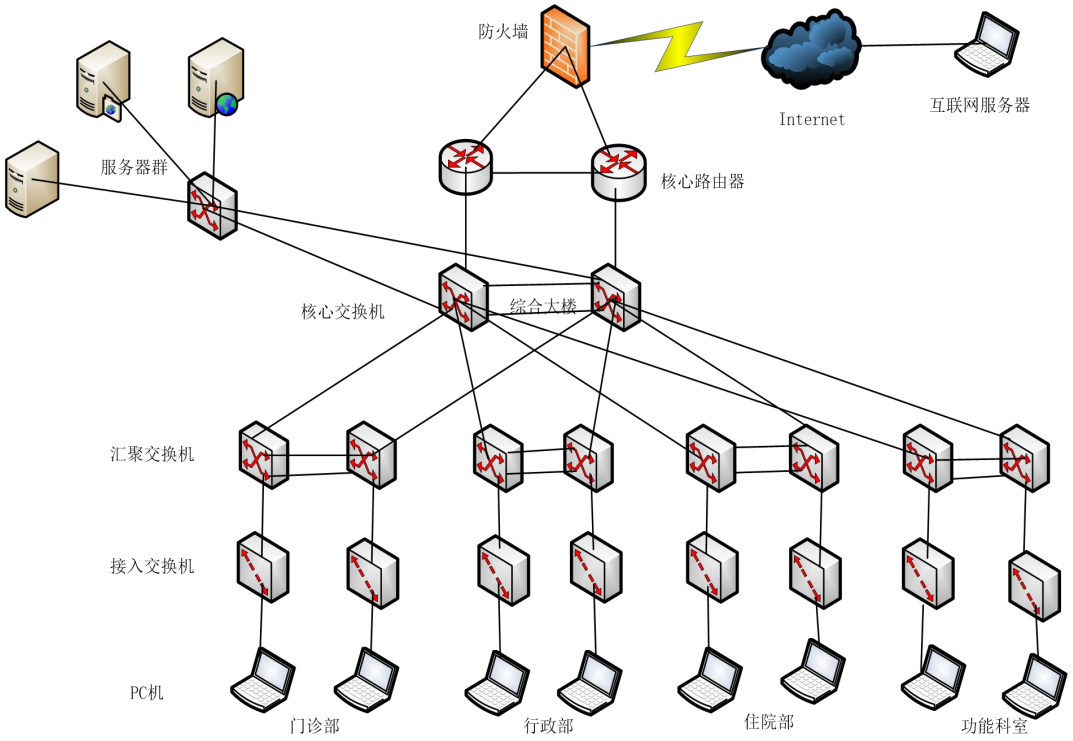


图 3.4 医院网络拓扑结构图

通过以上设计，医院网络不仅能够满足当前的业务需求，还具备良好的扩展性和安全性，为医院的长期发展提供了坚实的技术支持。

四、方案实施

（一）网络拓扑图

在第三章的分析设计基础上，利用华为 eNSP 模拟器搭建了一个医院网络方案的拓扑图。该拓扑图详细展示了医院网络的结构和设备连接关系，为后续的设备配置和功能测试提供了基础。具体的拓扑图如图 4.1 所示：

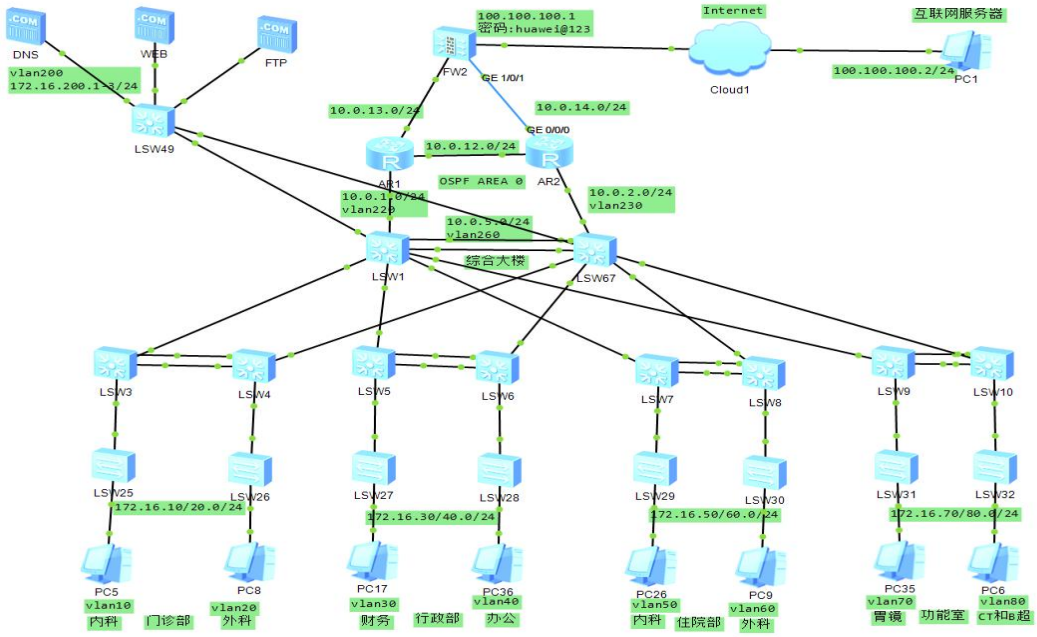


图 4.1 医院网络拓扑图

（二）设备选型

在本次设计中，设备选型是确保网络性能和稳定性的关键环节。选型时不仅要考虑网络的带宽速率，还需确保设备之间的兼容性和匹配性。具体选型的设备及其参数如表 4.1 所示：

表 4.1 设备清单

设备	型号	数量
三层交换机	eNSP S5700-28C-HI	9
二层交换机	eNSP S3700-26C-HI	8
路由器	eNSP AR2240	2
防火墙	eNSP USG6000V	1
PC 机	惠普	若干
服务器	eNSP Sever	3
传输介质	直通线、交叉线、光纤	若干

（三）VLAN 及 IP 地址规划

为了提高网络的稳定性和安全性，我们将医院的各个部门（如财务部、办公室、住院部、内外科、功能科室等）分别划分到独立的 VLAN 中，并为每个 VLAN 分配相应的 IP 地址段。通过划分 VLAN，可以有效防止广播风暴，将广播域限制在单个 VLAN 内部，减少广播通信对其他 VLAN 的影响。同时，VLAN 的划分增强了网络的安全性，不同 VLAN 之间的报文传输相互隔离，降低了机密信息泄露的风险。具体的 VLAN 划分和 IP 地址规划如表 4.2 所示：

表 4.2 VLAN 划分和 IP 划分表

VLAN	部门	IP 网段	子网掩码	默认网关
VLAN 10	门诊部-内科	172.16.10.0/24	255.255.255.0	172.16.10.1
VLAN 20	门诊部-外科	172.16.20.0/24	255.255.255.0	172.16.20.1
VLAN 30	财务部	172.16.30.0/24	255.255.255.0	172.16.30.1
VLAN 40	办公室	172.16.40.0/24	255.255.255.0	172.16.40.1
VLAN 50	住院部-内科	172.16.50.0/24	255.255.255.0	172.16.50.1
VLAN 60	住院部-外科	172.16.60.0/24	255.255.255.0	172.16.60.1
VLAN 70	胃镜室	172.16.70.0/24	255.255.255.0	172.16.70.1
VLAN 80	CT室、B超室	172.16.80.0/24	255.255.255.0	172.16.80.1
VLAN 200	服务器群	172.16.200.0/24	255.255.255.0	172.16.200.1
VLAN 220	核心路由1	10.0.1.0/24	255.255.255.0	10.0.1.1
VLAN 230	核心路由2	10.0.2.0/24	255.255.255.0	10.0.2.1
VLAN 260	综合大楼	10.0.5.0/24	255.255.255.0	10.0.5.1

（四）总公司网络方案实现

1、 核心层交换机配置

核心层是整个网络的核心部分，负责实现网络的高效传输和优化。本方案的核心层位于综合大楼内，采用两台三层交换机和两台核心路由器，通过不同链路划分 VLAN，利用 OSPF 协议实现网段间的连接。同时，采用 ACL 技术保护财务部的信息安全，通过 VRRP 技术实现路由冗余功能，并使用 DHCP 协议自动分配 IP 地址。这些技术共同构建了一个双核心、双链路的医院网络核心结构，确保网络的高可用性和稳定性。具体拓扑结构如图 4.2 所示：

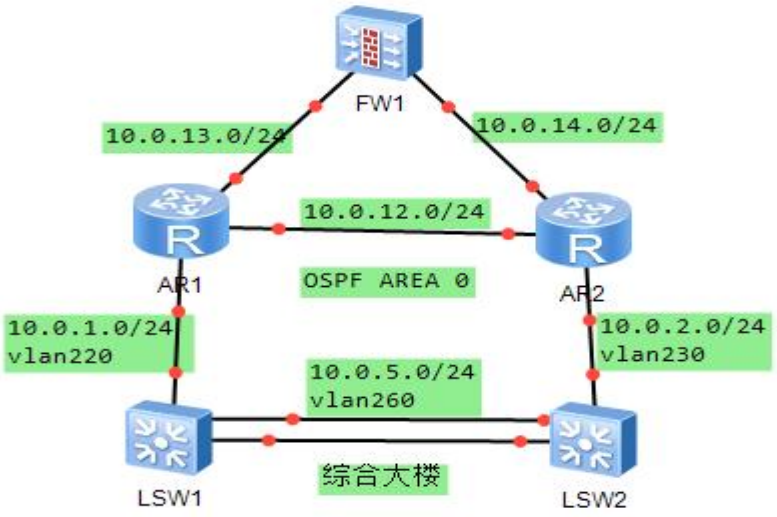


图 4.2 核心层网络结构

(1) DHCP 配置

在核心层交换机中，采用了 DHCP 协议，自动获取 IP 地址、网关和 DNS，以 LSW1 三层交换机配置为例，配置如下：

#[LSW1]ip pool pool10　　//创建 DHCP 地址池并分配相应的 IP 地址网关及 DNS

#[LSW1-ip-pool-pool10]gateway-list 172.16.10.1　# 设置 DHCP 地址池 pool10 的默认网关为 172.16.10.1

#[LSW1-ip-pool-pool10]network 172.16.10.0 mask 255.255.255.0　# 定义 DHCP 地址池 pool10 的网络范围为 172.16.10.0/24，指定子网掩码为 255.255.255.0，用于分配 IP 地址

#[LSW1-ip-pool-pool10]dns-list 172.16.200.1　# 设置 DHCP 地址池 pool10 的 DNS 服务器地址为 172.16.200.1，使客户端能够通过此 DNS 服务器解析域名

(2) OSPF 配置

在核心层配置 OSPF 协议，实现不同网段之间的互通，宣告相邻网段路由，以 LSW1 三层交换机配置为例，配置如下：

#[LSW1]ospf 1　　//配置 ospf 并宣告网段

#[LSW1-ospf-1]area 0.0.0.0　# 进入 OSPF 进程 1 的区域 0（骨干区域）

#[LSW1-ospf-1]network 10.0.1.0 0.0.0.255　# 在 OSPF 进程 1 的区域 0 中宣告网络 10.0.1.0/24，使该网络中的设备能够参与 OSPF 路由计算

#[LSW1-ospf-1]network 10.0.5.0 0.0.0.255 # 在 OSPF 进程 1 的区域 0 中宣告网络 10.0.5.0/24

#[LSW1-ospf-1]network 172.16.0.0 0.0.255.255 # 在 OSPF 进程 1 的区域 0 中宣告网络 172.16.0.0/16

在核心路由器中使用了 OSPF 协议与静态路由协议以及对路由器进行主备份配置，提高了网络的可靠性，以 AR1 为例具体配置如下：

#[AR1]ospf 1 //配置 ospf

#[AR1-ospf-1]default-route-advertise always //ospf 进入默认路由

#[AR1-ospf-1]area 0.0.0.0 # 进入 OSPF 进程 1 的区域 0（骨干区域）

#[AR1-ospf-1]network 10.0.1.0 0.0.0.255 # 在 OSPF 进程 1 的区域 0 中宣告网络 10.0.1.0/24

#[AR1-ospf-1]network 10.0.12.0 0.0.0.255

#[AR1]ip route-static 0.0.0.0 0.0.0.0 10.0.13.2 //配置默认路由主

#[AR1]ip route-static 0.0.0.0 0.0.0.0 10.0.12.2 preference 70 //配置默认路由备

(3) VRRP 配置

为了实现医院网络的路由冗余和负载均衡，我们在核心层的路由器和交换机上配置了 VRRP（虚拟路由冗余协议）。VRRP 通过将一组路由器组织成一个虚拟路由器，并为其配置虚拟 IP 地址，确保即使在当前使用的首跳设备故障时，网络通信仍能保持连通性。在本方案中，通过配置优先级，将 LSW1 设置为主设备，LSW2 设置为备份设备，以实现 VRRP 功能。

现通过配置优先级，将 LSW1 作为主设备，LSW2 作为备份设备进行 VRRP 的配置。

主设备 LSW1 部分配置如下：

#[LSW1]interface Vlanif10 //配置 VRRP 主，并配置接口 DHCP 全局下发

#[LSW1-Vlanif10]ip address 172.16.10.2 255.255.255.0

#[LSW1-Vlanif10]vrrp vrid 10 virtual-ip 172.16.10.1 //配置虚拟网关

#[LSW1-Vlanif10]vrrp vrid 10 priority 120

#[LSW1-Vlanif10]dhcp select global

备份设备 LSW2 部分配置如下：

#[LSW2]interface Vlanif10 //配置 VRRP 备

#[LSW2-Vlanif10]ip address 172.16.10.3 255.255.255.0

#[LSW2-Vlanif10]vrrp vrid 10 virtual-ip 172.16.10.1

#[LSW2-Vlanif10]dhcp select global

(4) MSTP 配置

在核心设备配置 MSTP 的优先级，现将 LSW1 作为主核心设备划分两个实例，分为 instance1 和 instance2，将 LSW2 作为备份核心设备同样划分两个实例，分为 instance1 和 instance2。具体配置如下：

#[LSW1]stp instance 1 priority 0 # 在交换机 LSW1 上，将生成树协议（STP）实例 1 的优先级设置为 0

#[LSW1]stp instance 2 priority 4096 # 在交换机 LSW1 上，将生成树协议（STP）实例 2 的优先级设置为 4096

#[LSW2]stp instance 1 priority 4096 # 在交换机 LSW2 上，将生成树协议（STP）实例 1 的优先级设置为 4096

#[LSW2]stp instance 2 priority 0 # 在交换机 LSW2 上，将生成树协议（STP）实例 2 的优先级设置为 0

(5) ACL 配置

在核心层，我们采用了 ACL（访问控制列表）技术来增强网络的安全性。ACL 分为标准 ACL 和扩展 ACL 两种类型，本设计中使用的是标准 ACL。通过对财务部应用 ACL 技术，限制其他部门对财务部的访问，从而确保财务部信息的安全性。以财务部与住院部内科为例，具体的 ACL 配置如下：

#[LSW1]acl number 3001

#[LSW1-acl-adv-3001]rule 10 deny ip source 172.16.30.0 0.0.0.255 destination 172.16.50.0 0.0.0.255

#[LSW1-acl-adv-3001]drop-profile default

#[LSW1-acl-adv-3001]traffic-filter vlan 30 inbound acl 3001

2、 汇聚层交换机配置

汇聚层采用三层交换机，并通过双链路连接以增强网络的可靠性和稳定性。在汇聚层中，为每个部门创建独立的 VLAN，确保各部门网络的隔离与安全。同时，

配置 MSTP（多生成树协议）实例，以优化网络流量的分配。具体的模拟结构如图 4.3 所示：

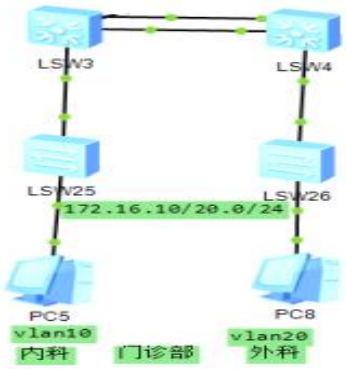


图 4.3 汇聚层网络结构

(1) VLAN 划分：

现以 LSW3 三层交换机为例，对医院部门进行 VLAN 的划分，具体配置如下：

#[LSW3]interface GigabitEthernet0/0/1

#[LSW3-GigabitEthernet0/0/1]port link-type access

#[LSW3-GigabitEthernet0/0/1]port default vlan 10　//将接口划分到 VLAN10

#[LSW3-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2

#[LSW3-GigabitEthernet0/0/1]port link-type access

#[LSW3]interface GigabitEthernet0/0/24 //进入接口将接口配置为中继端口

#[LSW3-GigabitEthernet0/0/24]port link-type trunk　# 将交换机 LSW3 的 GigabitEthernet0/0/24 接口配置为 Trunk 模式

#[LSW3-GigabitEthernet0/0/24]port trunk allow-pass vlan 2 to 4094　# 配置 Trunk 接口 GigabitEthernet0/0/24 允许通过的 VLAN 范围为 VLAN 2 到 VLAN 4094

(2) MSTP 配置：

MSTP 能够将多个 VLAN 整合到一个集合中，即将一个或多个 VLAN 划分为一个实例。这种配置不仅能够快速收敛，还能使不同 VLAN 的流量沿着各自的路径分发，从而提供多个数据转发路径、负载均衡，并避免环路的产生。以 LSW3 为例，MSTP 的具体配置如下：

#[LSW3]stp mode mstp　//将交换机配置成 MSTP 模式

#[LSW3]stp region-configuration　//进入 MSTP 模式

#[LSW3-mst-region]instance 1 vlan 10　40　# 在 MSTP（多生成树协议）区域配置中，将 VLAN 10 和 VLAN 40 映射到实例 1

#[LSW3-mst-region]instance 2 vlan 50　80

#[LSW3-mst-region]active region-configuration

3、 接入层交换机配置

接入层采用二层交换机，与各主机进行连接。每个部门划分到一个独立的网段，并处于单独的 VLAN 中。同时，对每个部门进行了 IP 地址的规划。以门诊部为例，具体的模拟结构如图 4.4 所示：

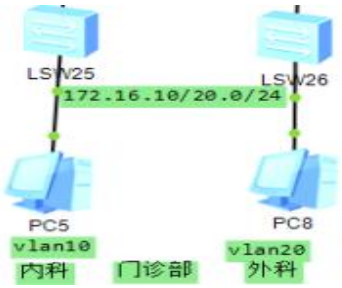


图 4.4 接入层网络结构

4、 出口防火配置

出口防火墙的设计显著提升了网络的安全性。对其进行内外网络的访问控制配置，并采用静态路由协议进行主备份路由的设置。同时，利用 NAT（网络地址转换）技术实现与外网的连接。具体的模拟结构如图 4.5 所示：

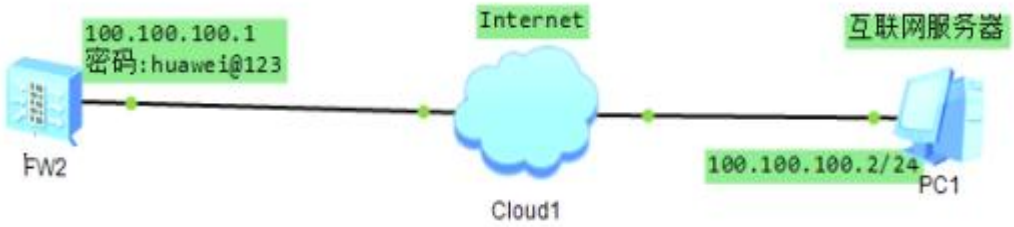


图 4.5 网络出口结构

(1) 防火墙具体配置如下：

#[FW2]firewall zone trust　//将内网接口加入 trust 区域

#[FW2-zone-trust]set priority 85

#[FW2-zone-trust]add interface GigabitEthernet0/0/0

#[FW2-zone-trust]add interface GigabitEthernet1/0/0

#[FW2-zone-trust]add interface GigabitEthernet1/0/1

#[FW2]firewall zone untrust //将外网接口加入 untrust 区域

#[FW2-zone-untrust]set priority 5

#[FW2-zone-untrust]add interface GigabitEthernet1/0/2

#[FW2-zone-dmz]firewall zone dmz

#[FW2-zone-dmz]set priority 50

#[FW2]ip route-static 172.16.0.0 255.255.0.0 10.0.13.1 //配置主静态路由

#[FW2]ip route-static 172.16.0.0 255.255.0.0 10.0.14.1 preference 70 //配置备静态

(2) NAT 技术配置

在出口防火墙设计中，采用 NAT 技术并通过 NAT 池的方式进行配置。NAT 技术主要用于实现内部网络主机访问外部网络的功能。当内网主机需要访问外网时，NAT 技术可以将内部主机的私有地址转换为外部网络的公有地址。多个私有地址可以共用一个公网地址，有效解决了 IP 地址不足的问题，同时保证了网络的互通性并节省了公网地址。配置相应的安全策略，允许内网访问外部网络，实现内外网的连通。具体配置如下：

#[FW2]nat address-group test 0 //进行 NAT 地址池配置

#[FW2]mode pat

#[FW2]section 0 100.100.100.3 100.100.100.5

#[FW2]security-policy //配置安全策略允许 172.16 内网访问外部

#[FW2-security-policy]rule name souce_nat

#[FW2]source-zone trust

#[FW2-destination-zone-trust]destination-zone untrust

#[FW2-destination-zone-trust]source-address 172.16.0.0 16

#[FW2-destination-zone-trust]action permit

#[FW2-destination-zone-trust]traffic-policy

#[FW2-destination-zone-trust]policy-based-route

5、 服务器配置

根据医院的需求，为该网络方案配置了相应的服务器，包括 DNS 服务器、WEB 服务器和 FTP 服务器。具体的模拟结构如图 4.6 所示：

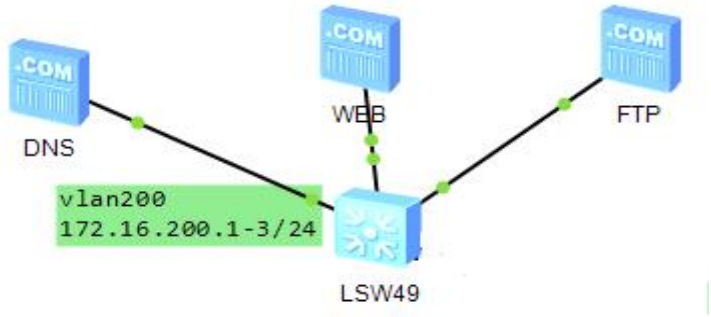


图 4.6 服务器群

(1) DNS 服务器

DNS 服务器能够实现域名和 IP 地址的相互映射。在该设计中，为 DNS 服务器配置了相应的 IP 地址、子网掩码和网关，并为医院配置了域名。相关配置如图 4.7 和图 4.8 所示：

图 4.7 DNS 服务器配置

图 4.8 域名配置

(2) WEB 服务器：

网络服务器中，Web 服务器（IIS）扮演着重要角色，它能够共享 Internet 上的各类信息资源。医护人员能够通过 Web 服务器便捷地查询所需信息，这不仅提升了工作效率，还节省了宝贵的时间。针对本方案的 Web 服务器，我们进行了细致的配置，确保其能够高效运行。相关配置详情如图 4.9 所示：

图 4.9 WEB 服务器配置

(3) FTP 服务器：

FTP 服务器作为文件传输的核心设备，存储着大量的数据信息。在本设计中，FTP 服务器未设置权限限制，用户可以根据自身需求随时下载所需文件。我们为 FTP 服务器配置了相应的 IP 地址、子网掩码和网关，确保其能够稳定运行。具体配置情况如图 4.10 所示：

图 4.10 FTP 服务器配置

五、测试

（一）核心层测试

1、 DHCP 服务测试

为了验证DHCP服务的正常运行，我们将PC机的IP地址获取方式设置为DHCP。通过在 PC 机上输入 ipconfig 命令，可以在命令行中查看到成功获取的 IP 地址、网关及 DNS 信息。以 PC5 为例，使用 ipconfig 命令进行测试，测试结果显示 PC5 成功获取了 IP 地址、网关和 DNS 信息，表明 DHCP 服务运行正常。测试结果如图 5.1 和图 5.2 所示：

图 5.1 设置 DHCP

```
Welcome to use PC Simulator!

PC>ipconfig

Link local IPv6 address.....: fe80::5689:98ff:fe9a:7fdd
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 172.16.40.254
Subnet mask.....: 255.255.255.0
Gateway.....: 172.16.40.1
Physical address.....: 54-89-98-9A-7F-DD
DNS server.....: 172.16.200.1
```

图 5.2 测试获取 IP、网关、DNS

2、 OSPF 协议测试

在核心层，我们采用了 OSPF 协议来实现各网段之间的互联互通。以 LSW1 三层交换机为例，通过执行 display ospf peer 命令，可以查看 OSPF 邻居表。如图 5.3 所示，OSPF 邻居表状态显示为 full，这表明 LSW1 交换机上的各个网段已经全部连通，OSPF 协议运行正常。

```
<LSW1>dis ospf peer

       OSPF Process 1 with Router ID 172.16.10.2
            Neighbors

 Area 0.0.0.0 interface 10.0.1.1(Vlanif220)'s neighbors
 Router ID: 10.0.13.1        Address: 10.0.1.2
   State: Full  Mode:Nbr is  Slave  Priority: 1
   DR: 10.0.1.1  BDR: 10.0.1.2  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 5
   Neighbor is up for 00:01:13
   Authentication Sequence: [ 0 ]

            Neighbors

 Area 0.0.0.0 interface 10.0.5.1(Vlanif260)'s neighbors
 Router ID: 172.16.10.3      Address: 10.0.5.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.5.2  BDR: 10.0.5.1  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 5
   Neighbor is up for 00:01:13
   Authentication Sequence: [ 0 ]
```

图 5.3 OSPF 邻居表

（二）汇聚层测试

1、 VRRP 测试

在核心层中，我们利用 VRRP 技术实现了网络的路由冗余，确保网络的高可用性。以 LSW1 交换机为例，通过执行 display vrrp brief 命令，可以查看 VRRP 配置的简化信息。具体信息如图 5.4 所示，显示了 VRRP 的运行状态和配置参数，验证了 VRRP 技术的有效性：

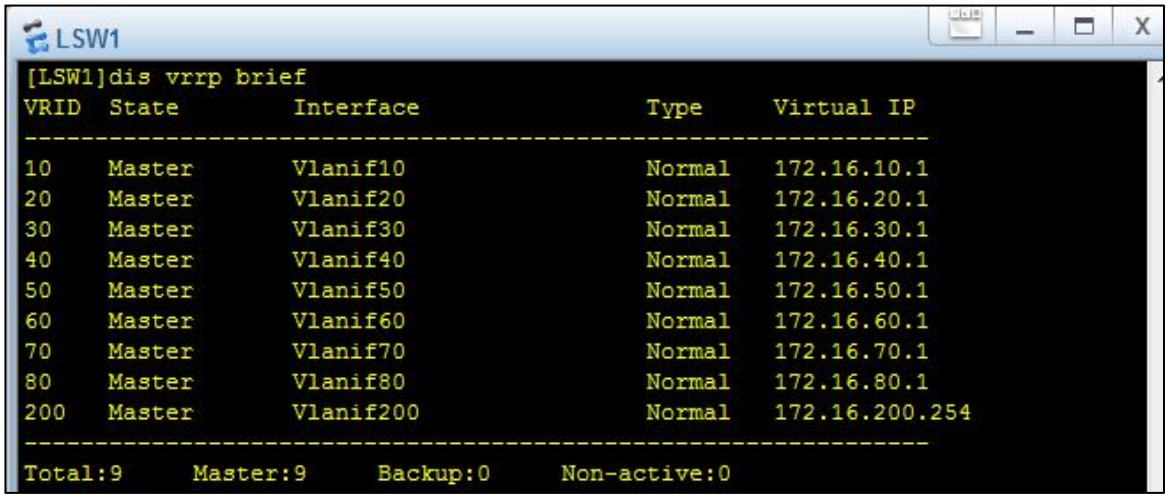


图 5.4 VRRP 配置信息

2、 VLAN 测试

在汇聚层，我们为每个部门分配了相应的 VLAN，以实现网络的隔离和管理。以门诊部为例，在交换机 LSW3 上为门诊部内科分配了 VLAN10。通过执行 display this 命令，在接口 g0/0/1 上查看 VLAN 的分配情况。测试结果显示，VLAN10 已成功分配给门诊部内科，网络配置正确。具体结果如图 5.5 所示：

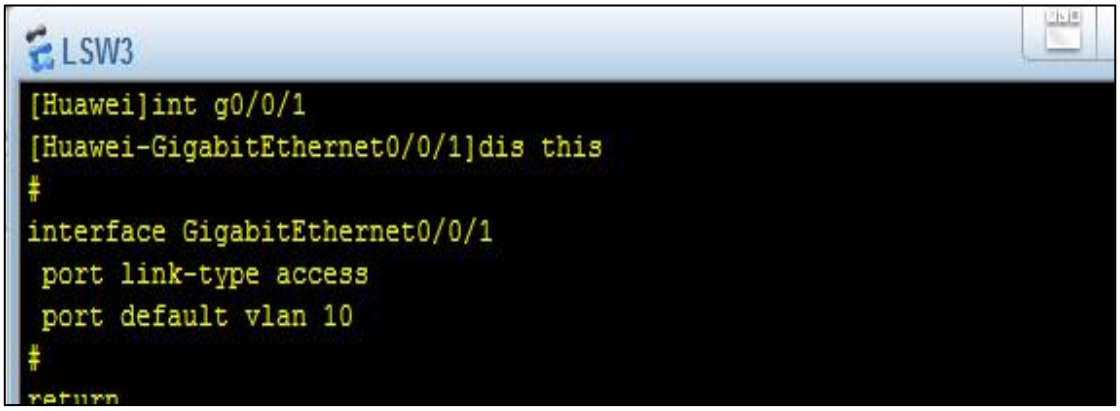


图 5.5 VLAN 的分配

3、 MSTP 测试

在汇聚层，我们配置了 MSTP 技术，以优化网络流量的分配，避免环路的产生。以 LSW3 汇聚交换机为例，通过执行 display stp brief 命令，可以查看 MSTP 的简化配置。配置 MSTP 区域后，所有相关数据均处于 forwarding 转发状态，表明 MSTP 配置成功，网络运行稳定。具体结果如图 5.6 所示：

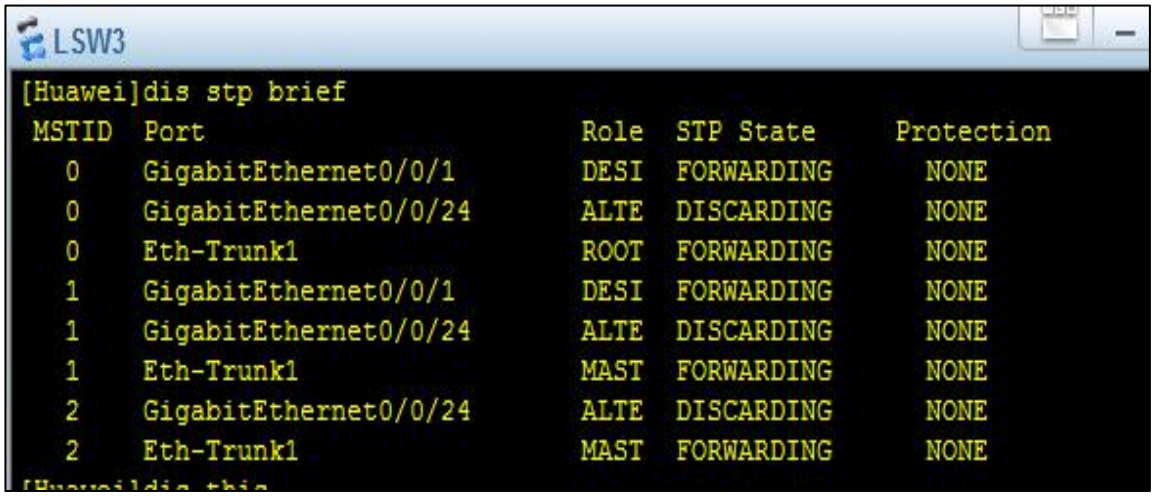


图 5.6 MSTP 的分配

（三）接入层测试

1、 VALN 测试

为了测试不同 VLAN 之间的连通性，我们选择了 VLAN10 中的主机 PC5 与 VLAN80 中的主机 PC6 进行互 ping 测试。测试结果显示，PC5 发送的数据包全部被 PC6 接收，数据传输的最长延迟为 187ms，最短延迟为 171ms，平均延迟为 180ms。这表明不同 VLAN 之间的通信正常，网络配置有效。具体测试结果如图 5.7 所示：

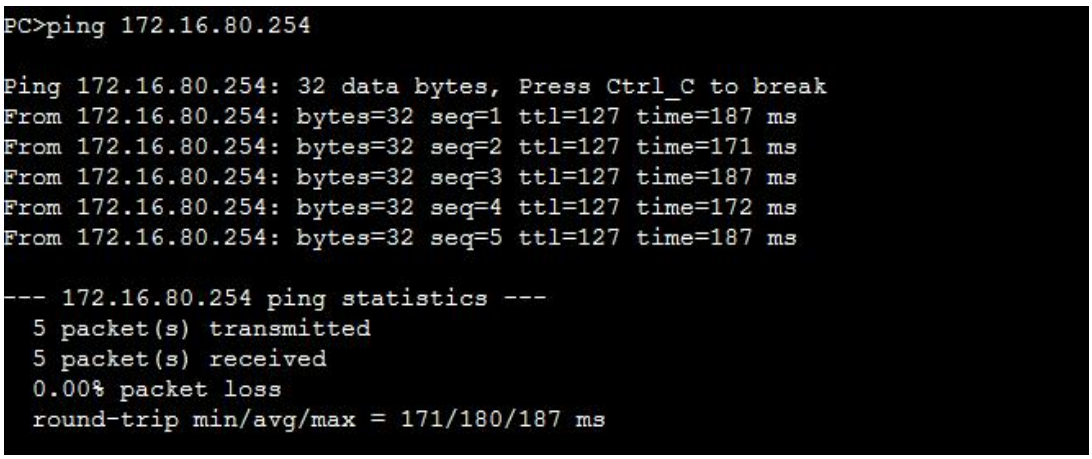


图 5.7 不同 VLAN 主机连通性

2、 ACL 测试

为了验证 ACL 技术对主机连通性的影响，我们对医院财务部设置了访问权限，以保护其重要信息文件的安全性。以办公室的主机 PC36 与财务部的主机 PC17 为例，进行互 ping 测试。测试结果显示，PC36 发送的 5 个数据包全部被 PC17 接收，数据传输的最长延迟为 218ms，最短延迟为 171ms，平均延迟为 193ms。这表明 ACL

配置正确，既保护了财务部的信息安全，又允许合法访问。具体测试结果如图 5.8 所示：

```
PC>ping 172.16.30.254

Ping 172.16.30.254: 32 data bytes, Press Ctrl_C to break
From 172.16.30.254: bytes=32 seq=1 ttl=127 time=218 ms
From 172.16.30.254: bytes=32 seq=2 ttl=127 time=187 ms
From 172.16.30.254: bytes=32 seq=3 ttl=127 time=203 ms
From 172.16.30.254: bytes=32 seq=4 ttl=127 time=171 ms
From 172.16.30.254: bytes=32 seq=5 ttl=127 time=187 ms

--- 172.16.30.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 171/193/218 ms
```

图 5.8 访问控制列表技术与主机连通性

为了确保财务部数据的安全性，其他部门的主机被限制访问财务部的主机。以住院部内科的主机 PC26 为例，尝试使用 ping 命令访问财务部的主机 PC17。结果显示，数据包超时且未被接收，表明访问限制生效，如图 5.9 所示：

```
PC>ping 172.16.30.254

Ping 172.16.30.254: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 172.16.30.254 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

图 5.9 访问控制列表技术与主机连通性

（四）出口测试

在出口防火墙配置中，采用 NAT 技术实现内外网的连通性。通过执行 display nat address-group 命令，可以查看 NAT 技术的配置结果。NAT 技术将内网的私有 IP 地址转换为外网的公有 IP 地址，从而实现局域网主机对外部网络的访问。具体配置如图 5.10 所示：

```
[USG6000V1]display nat address-group
NAT address-group information:
  Total 1 address-group(s)
nat address-group test 0
 reference count: 1
 mode pat
 status active
 section 0 100.100.100.3 100.100.100.5
```

图 5.10 出口 NAT 技术配置信息

NAT 技术将网络划分为内部网络和外部网络两部分。当内网主机通过 NAT 访问外部网络时，其本地地址会被转换为合法的互联网 IP 地址。以内网主机 PC8 与外网主机 PC1 的连接为例，连通情况如图 5.11 所示：

```
PC>ping 100.100.100.2

Ping 100.100.100.2: 32 data bytes, Press Ctrl_C to break
From 100.100.100.2: bytes=32 seq=1 ttl=125 time=188 ms
From 100.100.100.2: bytes=32 seq=2 ttl=125 time=109 ms
From 100.100.100.2: bytes=32 seq=3 ttl=125 time=110 ms
From 100.100.100.2: bytes=32 seq=4 ttl=125 time=156 ms
From 100.100.100.2: bytes=32 seq=5 ttl=125 time=141 ms

--- 100.100.100.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 109/140/188 ms
```

图 5.11 测试与外网连通性

（五）服务器测试

1、 DNS 服务器测试

为了验证 DNS 服务器的连通性，使用主机 PC5 对 DNS 服务器 172.16.200.1 进行 ping 测试。测试结果显示，主机 PC5 发送的数据包被 DNS 服务器全部接收，表明 DNS 服务器运行正常，如图 5.12 所示：

```
PC>ping 172.16.200.1

Ping 172.16.200.1: 32 data bytes, Press Ctrl_C to break
From 172.16.200.1: bytes=32 seq=1 ttl=254 time=265 ms
From 172.16.200.1: bytes=32 seq=2 ttl=254 time=156 ms
From 172.16.200.1: bytes=32 seq=3 ttl=254 time=110 ms
From 172.16.200.1: bytes=32 seq=4 ttl=254 time=125 ms
From 172.16.200.1: bytes=32 seq=5 ttl=254 time=140 ms

--- 172.16.200.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 110/159/265 ms
```

图 5.12 DNS 服务器测试

2、 FTP 服务器测试

为了验证 FTP 服务器的连通性，使用主机 PC9 对 FTP 服务器 172.16.200.3 进行 ping 测试。测试结果显示，主机 PC9 发送的数据包被 FTP 服务器全部接收，表明 FTP 服务器运行正常，如图 5.13 所示：

```
PC>ping 172.16.200.3

Ping 172.16.200.3: 32 data bytes, Press Ctrl_C to break
From 172.16.200.3: bytes=32 seq=1 ttl=254 time=172 ms
From 172.16.200.3: bytes=32 seq=2 ttl=254 time=187 ms
From 172.16.200.3: bytes=32 seq=3 ttl=254 time=156 ms
From 172.16.200.3: bytes=32 seq=4 ttl=254 time=141 ms
From 172.16.200.3: bytes=32 seq=5 ttl=254 time=172 ms

--- 172.16.200.3 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 141/165/187 ms
```

图 5.13 FTP 服务器测试

3、 WEB 服务器测试

为了验证WEB服务器的连通性，使用主机PC8对WEB服务器www.yiyuan.com进行ping测试。测试结果显示，主机PC8发送的数据包被WEB服务器全部接收，表明WEB服务器运行正常，如图5.14所示：

```
PC>ping www.yiyuan.com

Ping www.yiyuan.com [172.16.200.2]: 32 data bytes, Press Ctrl_C to break
From 172.16.200.2: bytes=32 seq=1 ttl=254 time=202 ms
From 172.16.200.2: bytes=32 seq=2 ttl=254 time=140 ms
From 172.16.200.2: bytes=32 seq=3 ttl=254 time=202 ms
From 172.16.200.2: bytes=32 seq=4 ttl=254 time=125 ms

--- 172.16.200.2 ping statistics ---
  4 packet(s) transmitted
  4 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 125/167/202 ms
```

图 5.14 WEB 服务器测试

通过以上测试，我们全面验证了网络配置的有效性和稳定性，确保了医院网络的高效运行和数据安全。

参考资料

[1] 吴冠朋.医院数据中心建设中网络规划研究与应用[J].智能计算机与应用,2024,11(02):40-43+49.

[2] 蔡立明.医院网络与信息安全体系建设探讨[J].网络安全技术与应用,2024,(11):116-117.

[3] 王东辰.浅谈智慧医院网络规划与设计[J].企业科技与发展,2023,(05):58-60.

[4] 徐毅,高山,姚富进,等.北京小汤山医院战备院区应急网络规划与实施[J].中国数字医学,2024,15(06):15-18.

[5] 时晨,赵洪钢,余瑞丰,李国栋.基于 eNSP 的高可靠性企业园区网设计与仿真[J].实验室研究与探索,2024,39(02):112-117.

[6]刘晓明.现代大型医院的网络式规划与模块化设计探索[J].中外建筑,2024,(02):139-141.

[7] 黄国伟.ACL 技术在局域网中的应用[J].计算机产品与流通,2024,(07):63.

[8] 张蕾,韩作为,舒婷.医疗事业单位网络安全管理风险研究与思考[J].中国卫生质量管理,2023,28(2):61-64.

[9] 杨礼.基于 eNSP 的 DHCP 原理设计与分析[J].2024,(01):85-90.

[10] 梁宾,宋蓓蓓.VLAN 之间通信方案设计与仿真实验[J].电子测试,2023,(Z1):88-90.