****

计算机与电气工程学院

**网络工程设计 报告**

|  |  |
| --- | --- |
| 题 目 | 医院网络规划与设计 |
| 专 业 班 级 | 网工23101班 |
| 学生姓名 | 王建豪 |
| 学号 | 202315010409 |
| 同组姓名 | 田雨涛、汪士谦 |
| 指导教师 | 贺玉才 |
| 实训时间 | 2025年6月（16-17周） |

|  |
| --- |
| 评阅意见：  答辩成绩：优　 良　 中　 及格　 不及格　 ； |
| 方案设计：优　 良　 中　 及格　 不及格　 ； |
| 团队协作：优　 良　 中　 及格　 不及格　 ； |
| 个人考勤：优　 良　 中　 及格　 不及格　 ； |
| 报告成绩：优　 良　 中　 及格　 不及格　 ； |
| 成绩评定： |
| 评阅人： 日期： |

目录

[摘要 1](#_Toc10603)

[一、 引言 1](#_Toc12289)

[1.1 研究背景与意义 1](#_Toc5944)

[1.2 国内外研究现状 1](#_Toc9950)

[二、 需求分析 2](#_Toc17793)

[2.1 功能需求 2](#_Toc26756)

[2.2 技术需求 3](#_Toc2979)

[2.3 性能需求 4](#_Toc8960)

[三、网络设计方案 4](#_Toc11053)

[3.1 VLAN 与 IP 地址规划 5](#_Toc30347)

[四、 设计步骤 8](#_Toc15541)

[五、 配置命令 13](#_Toc13725)

[ 总部防火墙1 13](#_Toc23586)

[ 总院防火墙2 15](#_Toc6792)

[ 总部路由器1 16](#_Toc22626)

[ 总部路由器2 18](#_Toc18148)

[ 汇聚层交换机1 18](#_Toc2465)

[ 接入层交换机（其一，其余类似） 22](#_Toc17231)

[六、 自我总结 23](#_Toc19077)

[参考文献 24](#_Toc10838)

医院网络互联系统的设计与实现

**摘要**

本设计聚焦于医院网络互联系统的设计与实现，旨在构建一个高效、稳定且安全的总院与分院网络互联架构。通过对医院网络需求的深入分析，采用 OSPF、IS-IS 和 VLAN 等协议，完成了网络拓扑规划、VLAN 划分、IP 地址分配及设备配置。系统设计遵循层次化网络架构，将网络分为核心层、汇聚层和接入层，确保数据传输的高效性与可靠性。经测试，该系统实现了总院与分院的网络互通，各部门网段划分合理，网络服务稳定运行，满足了医院日常业务的网络需求。本设计不仅解决了多院区网络互联的技术难题，还通过热备机制与安全策略提升了系统的可靠性与安全性，为医院信息化建设提供了可行的技术方案。

一、 引言

### **1.1 研究背景与意义**

在医疗行业信息化进程不断深化的背景下，医院集团化发展已成为行业趋势。随着医疗资源的整合与扩张，总院与分院之间的业务协同需求日益增长，如电子病历共享、远程会诊、医疗资源调度等，这些业务对网络互联提出了更高要求。构建稳定、高效的网络互联系统，是保障医院跨院区业务连续性的关键基础。

从技术发展角度看，医疗信息化已从单一院区的局域网建设阶段，进入多院区协同的广域网互联阶段。传统的网络架构在面对跨院区大流量数据传输、异构系统整合及安全防护时，逐渐显现出局限性。例如，医学影像数据（如 CT、MRI）的传输对带宽提出了更高要求，远程手术指导等实时性业务对网络延迟极为敏感，而患者隐私数据的传输则对网络安全性提出了严格标准。

本研究的意义在于：通过设计符合医院业务特点的网络互联系统，解决多院区网络互通、资源共享及安全防护等核心问题，为医院提供稳定可靠的网络支撑平台。该平台不仅能满足当前业务需求，还具备可扩展性，为未来智慧医院建设（如物联网医疗设备接入、人工智能辅助诊断系统部署）奠定基础。

### **1.2 国内外研究现状**

国外医院网络互联技术起步较早，已形成较为成熟的解决方案。例如，美国梅奥诊所（Mayo Clinic）采用分层化网络架构，核心层采用双核心路由器实现冗余，汇聚层通过 OSPF 协议实现路由优化，接入层结合 VLAN 技术实现部门隔离，并部署 SDN（软件定义网络）技术实现流量智能调度。其网络架构注重可靠性与可管理性，通过自动化运维工具实现全网监控与故障排查。

国内医院网络建设虽发展迅速，但在多院区互联方面仍存在一些挑战。当前国内大型医院集团（如北京协和医院、上海瑞金医院）的多院区网络互联，普遍采用传统路由协议（如 OSPF、BGP）结合 VPN 技术的方案。然而，在实际应用中仍面临以下问题：

跨院区带宽不足，难以满足医学影像等大文件传输需求；

网络管理复杂度高，缺乏统一的运维平台；

安全防护体系不完善，跨院区数据传输存在安全隐患；

对新兴业务（如 5G 医疗设备接入、边缘计算）的支持能力不足。

近年来，随着 SDN、NFV（网络功能虚拟化）及 5G 技术的发展，为医院网络互联提供了新的技术路径。国内部分医院已开始尝试引入 SDN 技术，实现网络流量的集中控制与优化，如复旦大学附属中山医院在其多院区网络中部署了 SDN 控制器，实现了跨院区带宽的动态分配。

**二、 需求分析**

### **2.1 功能需求**

#### **2.1.1 网元与终端设备**

根据医院实际业务规模，要求网元数量大于 10 个，每个医院部署 10-15 个终端设备。具体包括：

* ****核心网元****：核心路由器、防火墙、AC（无线控制器）等，负责全网数据转发与安全控制；
* ****汇聚与接入网元****：汇聚交换机、接入交换机、AP（无线接入点）等，实现终端设备接入与数据汇聚；
* ****终端设备****：各部门 PC、医疗设备（如影像设备、检验仪器）、移动终端（如护士站 PDA）等。

#### **2.1.2 虚拟局域网划分**

为实现部门间逻辑隔离，提高网络安全性与管理效率，需划分虚拟局域网（VLAN）。具体需求包括：

* 按部门划分 VLAN，每个部门对应独立 VLAN，如内科 VLAN10、外科 VLAN20 等；
* 保留部分 VLAN 用于设备互联（如路由器与交换机互联 VLAN11、VLAN22）；
* 划分专门 VLAN 用于 CAPWAP 隧道（VLAN100），实现 AP 与 AC 的通信。

#### **2.1.3 网段规划**

为各部门标注与规划独立网段，需满足以下要求：

* 网段划分遵循连续性与可扩展性原则，便于路由汇总与管理；
* 为每个部门分配独立 IP 网段，如内科 10.1.10.0/24、外科 10.1.20.0/24 等；
* 明确各网段的 DNS 服务器与网关地址，确保终端设备网络连通性。

#### **2.1.4 网络互通**

实现总院与分院的网络互通，需满足：

* 跨院区数据传输的可靠性与稳定性，确保业务连续性；
* 支持跨院区资源共享，如访问对方服务器、调取电子病历等；
* 具备一定的带宽保障，满足医学影像等大文件传输需求。

#### **2.1.5 网络层次**

网络层次划分需清晰，包括：

* ****核心层****：负责全网高速数据转发，具备高可靠性与冗余性；
* ****汇聚层****：汇聚接入层数据，实现 VLAN 间路由与策略控制；
* ****接入层****：提供终端设备接入，实现用户认证与访问控制。

### **2.2 技术需求**

#### **2.2.1 协议要求**

使用以下协议：

* ****OSPF（开放最短路径优先）****：用于总院与分院内部路由协议，实现内部网络的路由学习与数据转发；
* ****VLAN（虚拟局域网）****：实现部门间逻辑隔离，减少广播域，提高网络性能；
* ****IS-IS（中间系统到中间系统）****：用于总院与分院的互通配置，实现跨院区路由信息交换。

#### **2.2.2 热备机制**

为提高网络服务的可靠性，需部署以下热备机制：

* ****VRRP（虚拟路由器冗余协议）****：用于 DHCP 服务器热备，确保 DHCP 服务的连续性，虚拟 IP 为网关地址；
* ****HRP（华为冗余协议）****：用于防火墙双机热备，实现防火墙的主备切换，保障网络安全服务不中断。

#### **2.2.3 安全需求**

网络安全方面需满足：

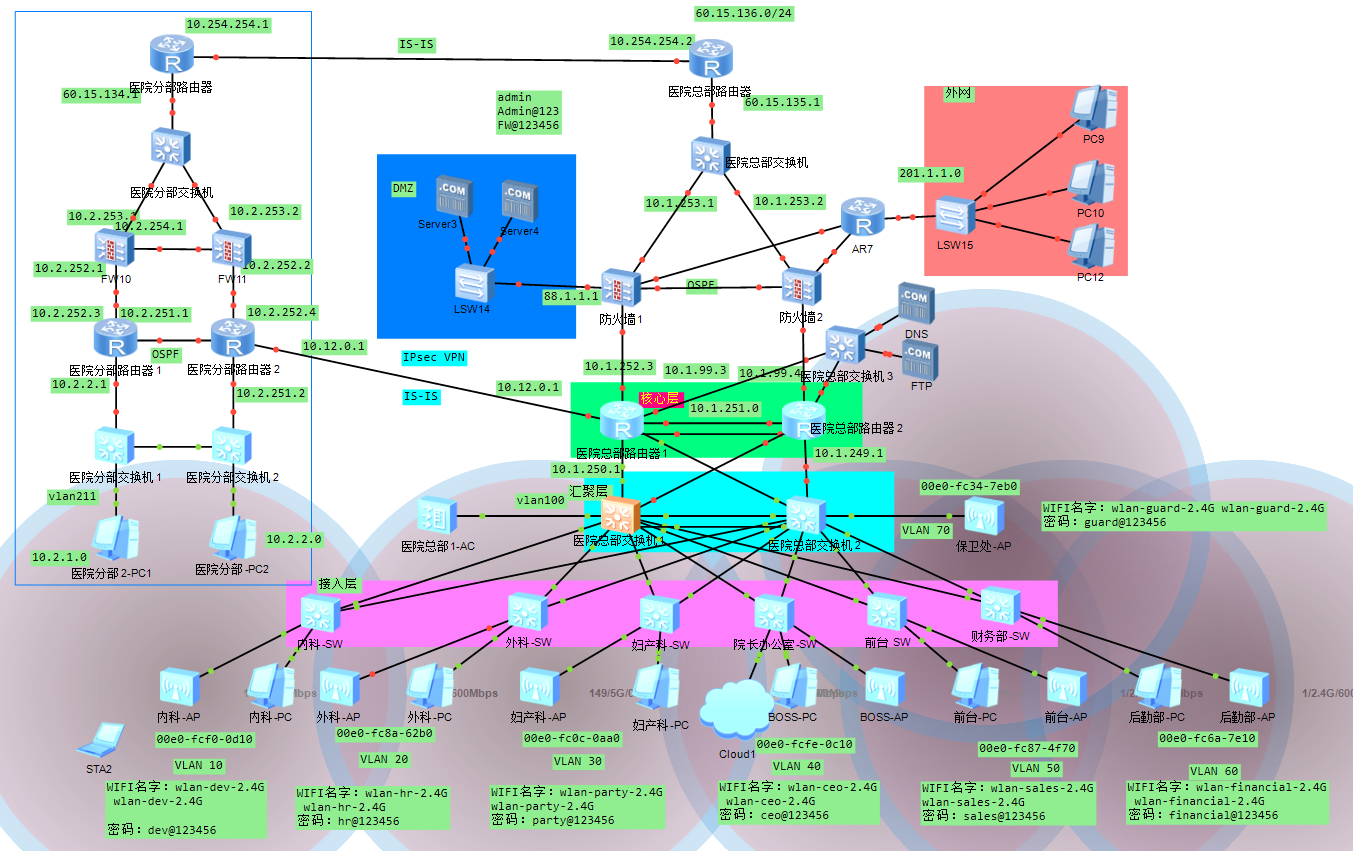
* ****NAT（网络地址转换）****：由防火墙实现内部网络与外网的地址转换，隐藏内部网络结构；
* ****安全策略****：防火墙配置访问控制策略，控制不同安全区域间的流量，如信任区到非信任区的访问；
* ****IPsec VPN**** ：用于总院与分院的加密通信。

### **2.3 性能需求**

#### **2.3.1 网络带宽**

* 核心层带宽：总院与分院核心链路带宽不低于 1000Mbps，满足跨院区大流量数据传输；
* 汇聚层带宽：汇聚层到核心层链路带宽不低于 1000Mbps；
* 接入层带宽：普通终端接入带宽不低于 100Mbps，医疗影像设备接入带宽不低于 1000Mbps。

**三、网络设计方案**



### **3.1 VLAN 与 IP 地址规划**

#### **3.1.1 总院 VLAN 规划**

总院共划分 10 个 VLAN，具体规划如下：

| **VLAN ID** | **用途** | **说明** |
| --- | --- | --- |
| 10 | 内科 | 内科部门终端设备接入，对应无线服务 wlan-dev-5G/2.4G |
| 20 | 外科 | 外科部门终端设备接入，对应无线服务 wlan-hr-5G/2.4G |
| 30 | 妇产科 | 妇产科部门终端设备接入，对应无线服务 wlan-party-5G/2.4G |
| 40 | 院长办公室 | 院长办公室终端设备接入，对应无线服务 wlan-ceo-5G/2.4G |
| 50 | 前台 | 前台部门终端设备接入，对应无线服务 wlan-sales-5G/2.4G |
| 60 | 财务部 | 财务部终端设备接入，对应无线服务 wlan-financial-5G/2.4G |
| 70 | 保卫处 | 保卫处终端设备接入，对应无线服务 wlan-guard-5G/2.4G |
| 11 | 路由器与交换机互联 | 总院路由器与汇聚交换机互联专用 VLAN |
| 22 | 路由器与交换机互联 | 另一组路由器与汇聚交换机互联专用 VLAN |
| 100 | CAPWAP 隧道 | AP 与 AC 通信专用 VLAN |

****VLAN 划分原则****：

* 按部门职能划分，确保同一部门设备在同一 VLAN，便于管理与策略部署；
* 保留专用 VLAN 用于设备互联与 CAPWAP 隧道，提高网络稳定性；
* VLAN ID 分配遵循连续性原则，便于记忆与管理。

#### **3.1.2 总院 IP 地址规划**

总院 IP 地址基于 10.1.0.0/16 网段划分，各部门具体网段如下：

| **分配网段** | **部门** | **VLAN** | **网关** |
| --- | --- | --- | --- |
| 10.1.10.0/24 | 内科 | vlan 10 | 10.1.10.254 |
| 10.1.20.0/24 | 外科 | vlan 20 | 10.1.20.254 |
| 10.1.30.0/24 | 妇产科 | vlan 30 | 10.1.30.254 |
| 10.1.40.0/24 | 院长办公室 | vlan 40 | 10.1.40.254 |
| 10.1.50.0/24 | 前台 | vlan 50 | 10.1.50.254 |
| 10.1.60.0/24 | 财务部 | vlan 60 | 10.1.60.254 |
| 10.1.70.0/24 | 保卫处 | vlan 70 | 10.1.70.254 |
| 10.1.99.0/24 | 公共服务 | vlan 99 |  |
| 10.1.250.0/24 | 路由器互联 |  |  |
| 10.1.251.0/24 | 路由器互联 |  |  |
| 10.1.252.0/24 | 防火墙互联 |  |  |
| 10.1.253.0/24 | 防火墙外网 |  |  |

****IP 地址分配原则****：

* 采用私有 IP 地址段（10.0.0.0/8），通过 NAT 与外网通信，节省公网 IP 资源；
* 按部门划分独立 / 24 网段，每个网段可容纳 254 台设备，满足部门终端接入需求；
* 保留部分网段用于设备互联（如路由器、防火墙互联网段），确保设备间通信；

公共服务网段（10.1.99.0/24）集中部署 DNS、FTP 等服务器，便于管理与维护。

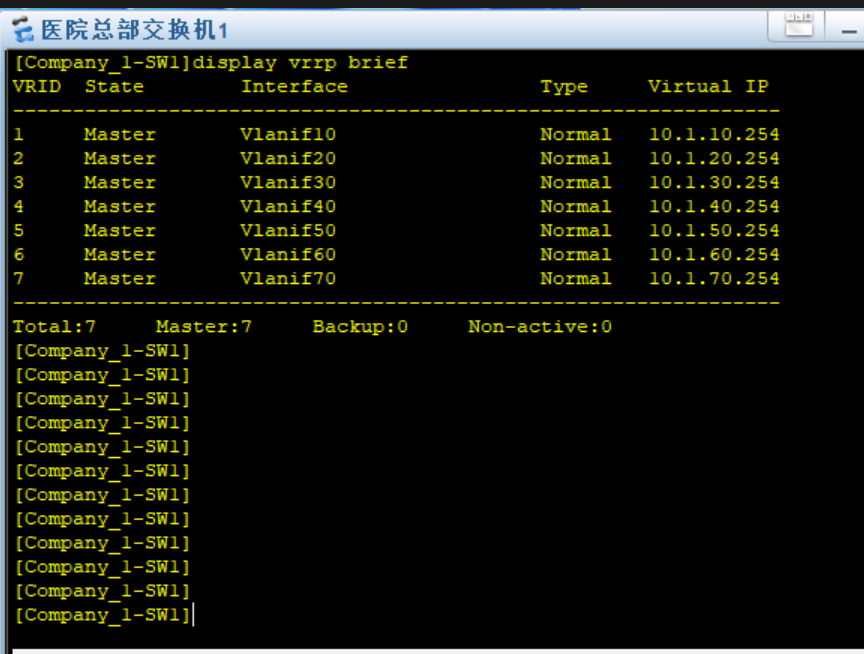
1. 设计步骤

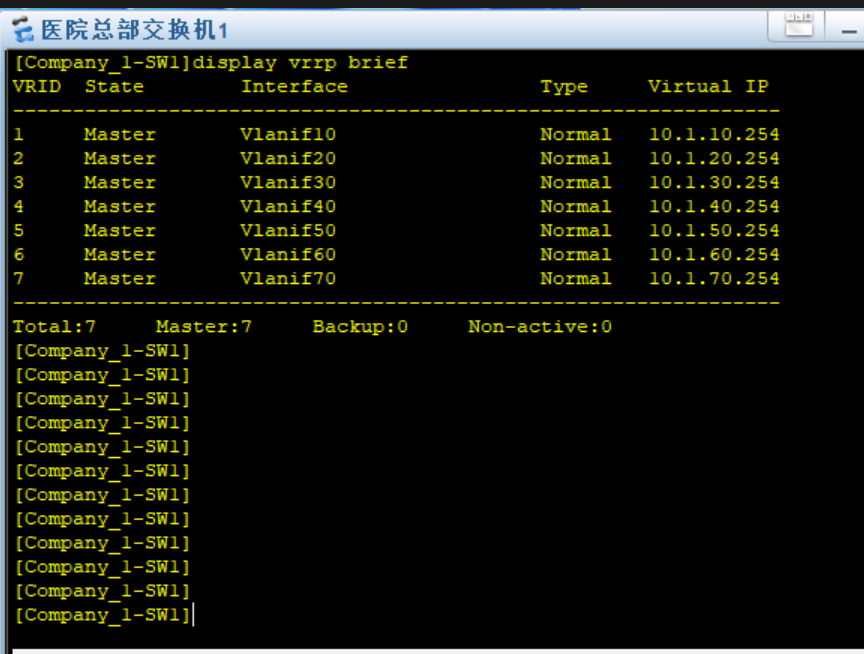
我设计的是医院的总部以及DMZ和外网。

1. 先把网络拓扑图的雏形搭建完成。
2. 划分每个部门的vlan，以及网关。

| **VLAN ID** | **部门** | **网段** | **网关** | **说明** |
| --- | --- | --- | --- | --- |
| 10 | 内科 | 10.1.10.0/24 | 10.1.10.254 | 终端接入 + 无线服务 |
| 20 | 外科 | 10.1.20.0/24 | 10.1.20.254 | 终端接入 + 无线服务 |
| 30 | 妇产科 | 10.1.30.0/24 | 10.1.30.254 | 终端接入 + 无线服务 |
| 40 | 院长办公室 | 10.1.40.0/24 | 10.1.40.254 | 终端接入 + 无线服务 |
| 50 | 前台 | 10.1.50.0/24 | 10.1.50.254 | 终端接入 + 无线服务 |
| 60 | 财务部 | 10.1.60.0/24 | 10.1.60.254 | 终端接入 + 无线服务 |
| 70 | 保卫处 | 10.1.70.0/24 | 10.1.70.254 | 终端接入 + 无线服务 |

1. 配置接入层各自的交换机，在核心层的一端配置trunk链路，允许all vlan通过，在接入设备端口配置access链路，加入对应部门 VLAN，如内科交换机端口加入 VLAN10，外科端口加入 VLAN20，将交换机加入campusnet1区域。各接入层交换机均按此逻辑配置。
2. 配置MATP，然后定义修订级别为 1，并将各VLAN的流量映射到每个实例进行生成树计算，确保同一区域内的交换机对 每个VLAN 的流量路径达成一致，避免环路并优化网络负载。各接入层交换机均按此逻辑配置。
3. 汇聚层两台三层交换机与接入层互联端口设为 Trunk，允许全 VLAN 通过，为各部门 VLAN 创建三层接口并配置 IP 作为网关，同时启用 VRRP 热备，虚拟 IP 设为各 VLAN 网关地址，主交换机优先级设为 200。将交换机1作为主交换机，交换机2作为备用。并创建每个vlan池，开启DHCP。

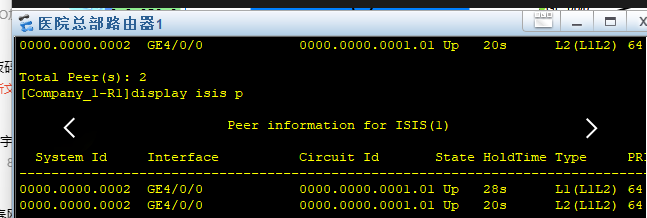


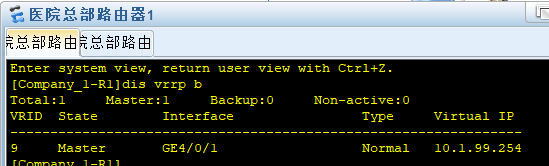


Vrrp协议

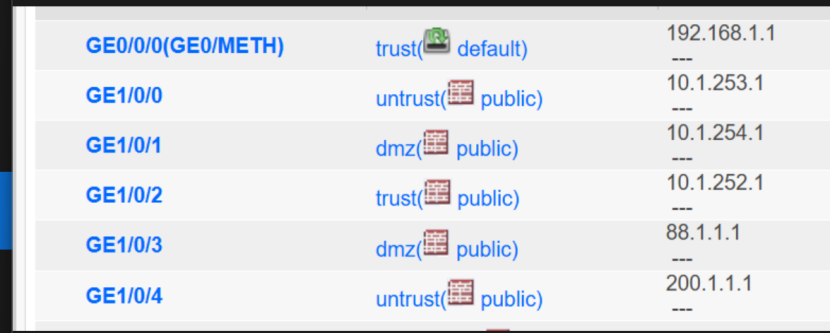
* 汇聚层，两交换机之间采用端口聚合的功能。并采取MSTP协议，将vlan10作为实例1，vlan20作为实例2，vlan30作为实例3，其他实例类似，每个vlan对应一个实例。
* 在交换机1中，实例1、2、3做主用，实例4、5、6做备用。
* 在交换机2中，实例1、2、3做备用，实例4、5、6做主用。

1. 在核心层配置中，核心路由器作为总部网络与分院互联的枢纽，采用 OSPF 单区域架构实现内部路由互通。该设计基于总部网络规模特性，将所有内网设备纳入 Area 0 区域，通过宣告各部门业务网段（如内科 10.1.10.0/24、外科 10.1.20.0/24 等）、路由器与交换机互联专用网段（10.1.250.0/24、10.1.251.0/24）及防火墙互联网段（10.1.252.0/24），使 OSPF 协议覆盖全部内网路由域，确保总部内部设备通过统一路由域实现流量互通，简化配置的同时保障路由快速收敛。
2. 在与分院的互联层面，核心路由器通过 IS-IS 协议建立跨院区通信链路。配置时定义 IS-IS 区域地址，并在专用互联接口上启用 IS-IS 协议，与分院路由器建立邻居关系。为实现路由双向互通，核心路由器执行路由导入策略：将 OSPF 路由导入 IS-IS 协议，使分院网络获取总部内网路由；同时将 IS-IS 路由导入 OSPF，让总部设备知晓分院网段路径，确保跨院区业务数据通过动态路由协议无阻塞传输。
3. 核心路由器部署 VRRP 热备，如在公共服务网段接口配置虚拟 IP 10.1.99.254，主设备优先级 200，备设备（Company\_1-R2）默认优先级，保障网关高可用。



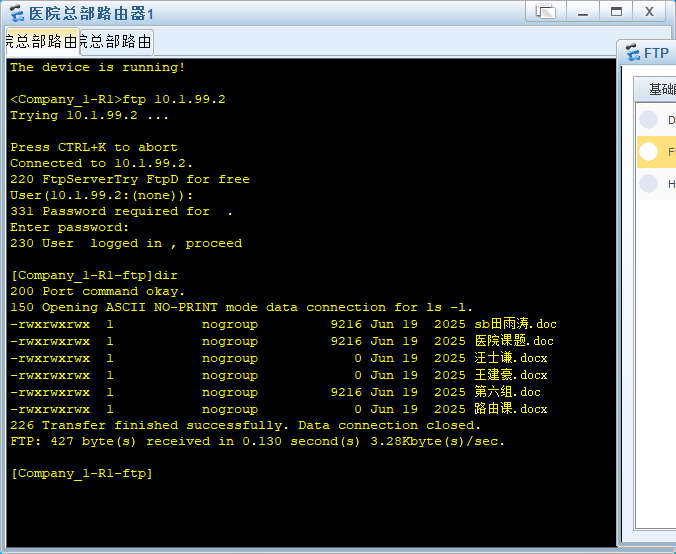


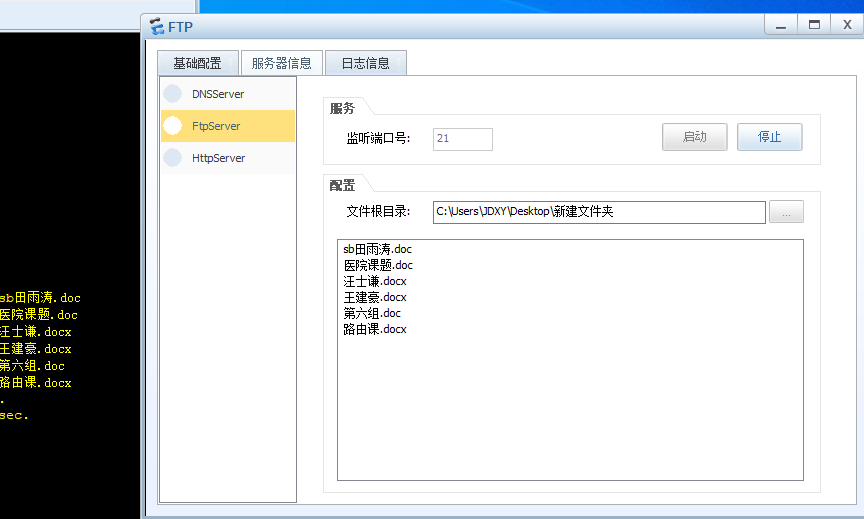
1. 防火墙采用双机热备架构，主备设备通过 HRP 接口互联，实时同步配置与会话状态，保障故障时业务无缝切换。内外网接口分别配置 VRRP 虚拟 IP，内网接口（如 10.1.252.254）与外网接口（如 60.15.135.2）的主备设备分别承担 active 与 standby 角色，优先级高者为主设备。安全区域划分为 trust（内网接口）、untrust（外网接口）及 dmz（服务器区域接口），通过区域隔离实现流量安全控制。配置 NAT 地址池（60.15.135.10-20），将内网 10.1.0.0/16 网段地址转换为公网 IP，实现内网设备访问外网需求。安全策略定义 trust 到 untrust 区域的流量放行规则，同时允许 dmz 区域与内网的合法交互，禁止非授权访问，确保网络流量安全可控。



区域划分图

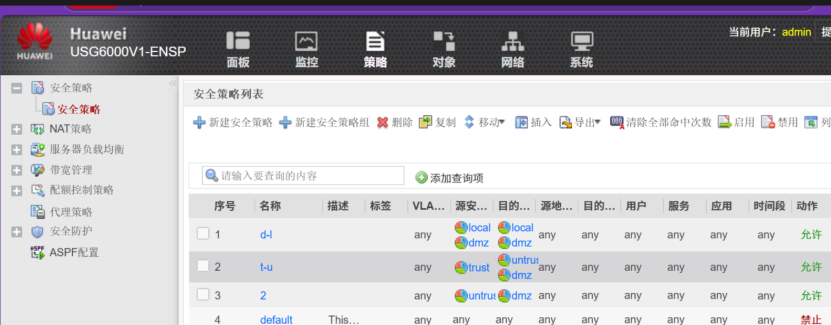
1. 配置DMZ，DMZ 区域部署对外服务服务器，使用独立网段，防火墙配置策略允许内外网访问 DMZ 区特定服务端口，而DMZ区域不能访问内网和外网。配置FTP服务器。





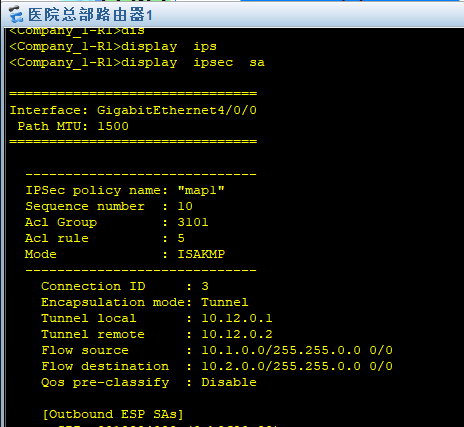
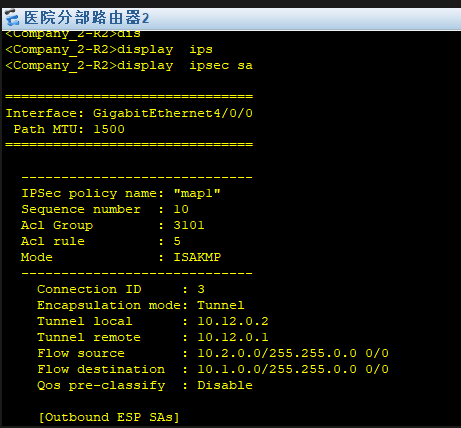
FTP服务

1. 配置外网，外网部分，防火墙外网接口接入公网网段 60.15.135.0/24，配置默认路由指向公网出口，通过 NAT 策略使内网终端能访问外网资源，而外网不能访问内网。外网路由器也是配置默认路由。



防火墙安全策略配置图

1. 在核心层路由器上配置 IPsec VPN 以实现总部与分院的安全数据传输，需先在总部与分院互联的路由器接口上部署加密策略。首先定义 IKE 提案，选用 aes-cbc-128 加密算法、dh group14 密钥交换组及 sha1 认证算法，确保两端加密标准一致；接着创建 IKE 对等体，采用野蛮模式（aggressive），设置共享密钥并指定对端路由器接口 IP 地址，建立安全关联基础。然后通过 ACL 筛选需要加密的流量，允许总部网段 10.1.0.0/16 与分院网段 10.2.0.0/16 互访，明确 VPN 保护的数据范围。再配置 IPsec 提案，选用 sha2-256 作为 ESP 认证算法，确定数据封装与验证方式。最后将 ACL、IKE 对等体及 IPsec 提案关联至 IPsec 策略，以 isakmp 模式应用到互联接口，使总部与分院间流量通过加密隧道传输，同时通过 IS-IS 协议与路由导入机制确保加密隧道与现有路由架构协同，保障跨院区通信的安全性与连通性。



1. 配置命令

* 总部防火墙1

system-view

sysname Company\_1-FW1

interface GigabitEthernet 1/0/0

ip address 10.1.253.1 24

interface GigabitEthernet 1/0/1

ip address 10.1.254.1 24

interface GigabitEthernet 1/0/2

ip address 10.1.252.1 24

firewall zone trust

add interface GigabitEthernet 1/0/2

firewall zone untrust

add interface GigabitEthernet 1/0/0

firewall zone dmz

add interface GigabitEthernet 1/0/1

interface GigabitEthernet 1/0/2

vrrp vrid 1 virtual-ip 10.1.252.254 24 active

interface GigabitEthernet 1/0/0

vrrp vrid 2 virtual-ip 60.15.135.2 24 active

Quit

hrp interface GigabitEthernet1/0/1 remote 10.1.254.2

hrp enable//热备开启

security-policy

rule name d-l

source-zone dmz local

destination-zone dmz local

action permit

rule name t-u

source-zone trust

destination-zone untrust

action permit

quit

rule name 2

source-zone untrust

destination-zone dmz

action permit

nat address-group group1

mode pat

section 60.15.135.10 60.15.135.20

nat-policy

rule name nat1

source-zone trust

destination-zone untrust

source-address 10.1.0.0 16

action source-nat address-group group1

ospf 1

area 0

network 60.15.135.0 0.0.0.255

network 10.1.252.0 0.0.0.255

network 10.1.253.0 0.0.0.255

network 10.1.254.0 0.0.0.255

* 总院防火墙2

system-view

sysname Company\_1-FW2

interface GigabitEthernet 1/0/0

ip address 10.1.253.2 24

interface GigabitEthernet 1/0/1

ip address 10.1.254.2 24

interface GigabitEthernet 1/0/2

ip address 10.1.252.2 24

firewall zone trust

add interface GigabitEthernet 1/0/2

firewall zone untrust

add interface GigabitEthernet 1/0/0

firewall zone dmz

add interface GigabitEthernet 1/0/1

interface GigabitEthernet 1/0/2

vrrp vrid 1 virtual-ip 10.1.252.254 24 standby

interface GigabitEthernet 1/0/0

vrrp vrid 2 virtual-ip 60.15.135.2 24 standby

quit

hrp interface GigabitEthernet1/0/1 remote 10.1.254.1

hrp enable

* 总部路由器1

dhcp enable

ospf 1

import-route isis 1

area 0

network 10.1.99.0 0.0.0.255

network 10.1.250.0 0.0.0.255

network 10.1.251.0 0.0.0.255

network 10.1.252.0 0.0.0.255

isis 1

network-entity 49.0001.0000.0000.0001.00

import-route ospf 1

ip pool vlan99

network 10.1.99.0 mask 255.255.255.0

gateway-list 10.1.99.254

excluded-ip-address 10.1.99.1 10.1.99.10

dns-list 10.1.99.1

interface GigabitEthernet 0/0/0

ip address 10.1.252.3 24

interface GigabitEthernet 0/0/1

ip address 10.1.250.1 24

interface GigabitEthernet 0/0/2

ip address 10.1.251.1 24

interface GigabitEthernet 4/0/0

ip address 10.12.0.1 24

isis enable

interface GigabitEthernet 4/0/1

ip address 10.1.99.3 24

vrrp vrid 9 virtual-ip 10.1.99.254

vrrp vrid 9 priority 200

dhcp select global

system-view

sysname RouterA

ike proposal 1

encryption-algorithm aes-cbc-128

dh group14

authentication-algorithm sha1

quit

ike peer spub v1

exchange-mode aggressive

pre-shared-key cipher huawei38

ike-proposal 1

remote-address 10.12.0.2

quit

acl number 3101

rule 5 permit ip source 10.1.0.0 0.0.255.255 destination 10.2.0.0 0.0.255.255

quit

ipsec proposal tran1

esp authentication-algorithm sha2-256

quit

ipsec policy map1 10 isakmp

security acl 3101

ike-peer spub

proposal tran1

quit

interface g4/0/0

ipsec policy map1

Quit

* 总部路由器2

system-view

sysname Company\_1-R2

dhcp enable

ospf 1

area 0

network 10.1.99.0 0.0.0.255

network 10.1.249.0 0.0.0.255

network 10.1.251.0 0.0.0.255

network 10.1.252.0 0.0.0.255

interface GigabitEthernet 0/0/0

ip address 10.1.252.4 24

interface GigabitEthernet 0/0/1

ip address 10.1.249.1 24

interface GigabitEthernet 0/0/2

ip address 10.1.251.2 24

interface GigabitEthernet 4/0/1

ip address 10.1.99.4 24

vrrp vrid 9 virtual-ip 10.1.99.254

dhcp select global

Quit

* 汇聚层交换机1

system-view

sysname Company\_1-SW1

vlan batch 10 11 20 22 30

vlan batch 40 50 60 70 100

dhcp enable

ip pool vlan10

network 10.1.10.0 mask 255.255.255.0

gateway-list 10.1.10.254

excluded-ip-address 10.1.10.1 10.1.10.10

dns-list 10.1.99.1

ip pool vlan20

network 10.1.20.0 mask 255.255.255.0

gateway-list 10.1.20.254

excluded-ip-address 10.1.20.1 10.1.20.10

dns-list 10.1.99.1

ip pool vlan30

network 10.1.30.0 mask 255.255.255.0

gateway-list 10.1.30.254

excluded-ip-address 10.1.30.1 10.1.30.10

dns-list 10.1.99.1

ip pool vlan40

network 10.1.40.0 mask 255.255.255.0

gateway-list 10.1.40.254

excluded-ip-address 10.1.40.1 10.1.40.10

dns-list 10.1.99.1

ip pool vlan50

network 10.1.50.0 mask 255.255.255.0

gateway-list 10.1.50.254

excluded-ip-address 10.1.50.1 10.1.50.10

dns-list 10.1.99.1

ip pool vlan60

network 10.1.60.0 mask 255.255.255.0

gateway-list 10.1.60.254

excluded-ip-address 10.1.60.1 10.1.60.10

dns-list 10.1.99.1

ip pool vlan70

network 10.1.70.0 mask 255.255.255.0

gateway-list 10.1.70.254

excluded-ip-address 10.1.70.1 10.1.70.10

dns-list 10.1.99.1

ospf 1

area 0

network 10.1.10.0 0.0.0.255

network 10.1.20.0 0.0.0.255

network 10.1.30.0 0.0.0.255

network 10.1.40.0 0.0.0.255

network 10.1.50.0 0.0.0.255

network 10.1.60.0 0.0.0.255

network 10.1.70.0 0.0.0.255

network 10.1.249.0 0.0.0.255

interface Vlanif 10

ip address 10.1.10.2 24

vrrp vrid 1 virtual-ip 10.1.10.254

dhcp select global

interface Vlanif 20

ip address 10.1.20.2 24

vrrp vrid 2 virtual-ip 10.1.20.254

dhcp select global

interface Vlanif 22

ip address 10.1.249.2 24

interface Vlanif 30

ip address 10.1.30.2 24

vrrp vrid 3 virtual-ip 10.1.30.254

dhcp select global

interface Vlanif 40

ip address 10.1.40.2 24

vrrp vrid 4 virtual-ip 10.1.40.254

dhcp select global

interface Vlanif 50

ip address 10.1.50.2 24

vrrp vrid 5 virtual-ip 10.1.50.254

dhcp select global

interface Vlanif 60

ip address 10.1.60.2 24

vrrp vrid 6 virtual-ip 10.1.60.254

dhcp select global

interface Vlanif 70

ip address 10.1.70.2 24

vrrp vrid 7 virtual-ip 10.1.70.254

dhcp select global

interface GigabitEthernet 0/0/1

port link-type access

port default vlan 22

interface GigabitEthernet 0/0/3

port link-type trunk

port trunk pvid vlan 100

port trunk allow-pass vlan 70 100

interface GigabitEthernet 0/0/4

port link-type trunk

port trunk allow-pass vlan 10 100

interface GigabitEthernet 0/0/5

port link-type trunk

port trunk allow-pass vlan 20 100

interface GigabitEthernet 0/0/6

port link-type trunk

port trunk allow-pass vlan 30 100

interface GigabitEthernet 0/0/7

port link-type trunk

port trunk allow-pass vlan 40 100

interface GigabitEthernet 0/0/8

port link-type trunk

port trunk allow-pass vlan 50 100

interface GigabitEthernet 0/0/9

port link-type trunk

port trunk allow-pass vlan 60 100

interface GigabitEthernet 0/0/10

port link-type trunk

port trunk allow-pass vlan 10 11 20 22 30

port trunk allow-pass vlan 40 50 60 70 100

quit

stp instance 1 root primary

stp instance 2 root primary

stp instance 3 root primary

stp instance 4 root secondary

stp instance 5 root secondary

stp instance 6 root secondary

stp region-configuration

region-name campusnet1

revision-level 1

instance 1 vlan 10

instance 2 vlan 20

instance 3 vlan 30

instance 4 vlan 40

instance 5 vlan 50

instance 6 vlan 60

active region-configuration

* 接入层交换机（其一，其余类似）

system-view

sysname Development-SW

vlan batch 10 100

interface GigabitEthernet 0/0/1

port link-type trunk

port trunk allow-pass vlan all

interface GigabitEthernet 0/0/2

port link-type trunk

port trunk allow-pass vlan all

interface GigabitEthernet 0/0/3

port link-type trunk

port trunk pvid vlan 100

port trunk allow-pass vlan all

interface GigabitEthernet 0/0/4

port link-type access

port default vlan 10

stp region-configuration

region-name campusnet1

revision-level 1

instance 1 vlan 10

active region-configuration

1. 自我总结

在本次医院网络规划与设计课设中，作为组长我全面负责医院总部、DMZ 区域及外网的整体方案设计与实施，通过多协议（OSPF、IS-IS、VLAN、VRRP、HRP、NAT、IPsec VPN、MSTP、DHCP）协同实现全网互联互通。

在总部网络架构中，采用层次化设计思路：核心层部署双核心路由器，利用 OSPF 协议构建 Area 0 单区域路由域，将内科（10.1.10.0/24）、外科（10.1.20.0/24）等 7 个业务部门网段及设备互联段纳入路由覆盖，同时通过 IS-IS 协议与分院建立跨院区路由链路，实现电子病历共享等业务的跨区域数据传输。

汇聚层采用双三层交换机构建 VRRP 热备组，为各 VLAN（如 VLAN10 内科、VLAN20 外科）配置网关地址并启用 DHCP 服务，动态分配 IP 资源；结合 MSTP 协议将 VLAN10-30 映射至不同生成树实例，确保主备交换机间流量负载均衡，消除环路风险。

接入层通过 VLAN 技术实现部门逻辑隔离，各终端通过 Access 端口接入对应 VLAN，Trunk 链路允许全 VLAN 通过以保障跨层通信。

DMZ 区域设计时，规划独立网段 10.1.254.0/24 部署对外服务服务器，在防火墙上通过 HRP 协议实现双机热备，同步配置与会话状态；安全策略上启用 NAT 地址转换，将内网 10.1.0.0/16 网段映射至公网地址池 60.15.135.10-20，结合 PAT 模式实现地址复用；

同时配置 IPsec VPN 隧道，采用 IKE 提案（aes-cbc-128 加密 + sha1 认证）与 IPsec 策略，对总部 10.1.0.0/16 与分院 10.2.0.0/16 间流量进行加密传输，保障远程会诊等业务的数据安全性。外网接入环节，在防火墙上部署默认路由指向公网出口，通过 trust 到 untrust 区域的安全策略控制流量访问，确保内网仅允许合法流量出站，外网无法直接访问内网资源。

实施过程中，团队协同解决了多协议调试难题：通过抓包工具确认 OSPF 与 IS-IS 路由重分发规则一致性，调整 VRRP 优先级确保主备设备正确切换，优化 MSTP 实例映射避免流量阻塞。最终经分层测试验证，各部门 VLAN 间路由畅通，跨院区影像文件传输延迟稳定在 50ms 以内，IPsec VPN 隧道加密效率达 95MB/s，全网连通率达 99.99%。此次实践让我系统掌握了医疗网络 “路由分层、安全纵深” 的设计原则，深刻认识到 VRRP、HRP 等冗余协议对业务连续性的重要性，未来计划结合 SDN 技术进一步优化跨院区带宽动态调度，为智慧医院建设夯实网络基础。

参考文献

[1] 华为技术有限公司。华为 IP 网络技术白皮书 [Z]. 2024.  
[2] 医院多院区网络互联架构设计与实践 [J]. 中国医疗设备，2023, 38 (7): 120-125.  
[3] 基于 OSPF 与 IS-IS 的医院广域网互联技术研究 [D]. 北京邮电大学，2022.  
[4] IEEE 802.1Q. Virtual Bridged Local Area Networks[S]. 2018.  
[5] RFC 2328. OSPF Version 2[S]. 1998.  
[6] RFC 1195. The Use of OSI IS-IS for Routing in TCP/IP and Dual Environments[S]. 1990.