网 络 工 程 课 程 设 计
实 验 报 告

实验名称： 异构网络设计综合实验

学 员 姓 名	程景愉	学 号	202302723005
培 养 类 型	计算机类	年 级	大三
专 业	网络工程	所 属 学 院	计算机学院
指 导 教 员	张军	职 称	工程师
实 验 室	306-707	实 验 时 间	2025.10.28

国防科技大学教育训练部制

《本科实验报告》填写说明

实验报告内容编排应符合以下要求：

（1）采用 A4（21cm×29.7cm）白色复印纸，单面黑字。上下左右各侧的页边距均为 3cm；缺省文档网格：字号为小 4 号，中文为宋体，英文和阿拉伯数字为 Times New Roman，每页 30 行，每行 36 字；页脚距边界为 2.5cm，页码置于页脚、居中，采用小 5 号阿拉伯数字从 1 开始连续编排，封面不编页码。

（2）报告正文最多可设四级标题，字体均为黑体，第一级标题字号为 4 号，其余各级标题为小 4 号；标题序号第一级用“一、”、“二、”……，第二级用“（一）”、“（二）”……，第三级用“1.”、“2.”……，第四级用“（1）”、“（2）”……，分别按序连续编排。

（3）正文插图、表格中的文字字号均为 5 号。

目录

图目录

1 实验目的

通过对常用的组网设备（包括交换机、路由器、防火墙）、常见的网络服务系统（Web 服务、Proxy 服务、Smtp & Pop3 服务、DNS 服务等）的安装与配置与调试实验，加深对上述设备和系统工作原理的理解，初步掌握其安装配置方法，为将来从事网络工程建设打下基础。

2 实验概述

一个完整的组网工程包括需求分析、方案设计、设备选型与采购、硬件安装与配置、软件安装与配置、系统测试与联调、工程验收等若干个环节，其中硬件与应用系统安装、配置工作量大，技术含量高，是信息系统集成或网络工程的关键环节，其中既涉及到技术上的问题，也涉及到工程组织、协调配合上的问题，一个网络工程师只有通过多次工程的实际锻炼，不断积累经验、吸取教训才能提高自己的水平。

3 需求分析

设计并构建一个小型的校园网络平台, 并在该平台上构建INTERNET 服务平台, 该网络工程建成后，将具有以下服务功能:

1. 具有内部 Web 服务功能；
2. 具有外部 Web 服务代理功能 ；
3. 具有邮件收发功能；
4. 具有对内部核心子网安全保护功能；
5. 具有内部域名解析功能；
6. 具有简单的网络管理功能。

3.1 技术分析

为满足校园的网络需求，网络建设需采用多种先进技术。首先，通过链路聚合技术（Eth-trunk）提升网络带宽和链路可靠性，特别是在核心层与接入层之间。其次，需使用虚拟路由冗余协议（VRRP）确保出口网关的高可用性，防止单点故障。VLAN 技术用于划分不同部门的安全区域，确保网络流量的隔离与安全性。MAC 地址绑定用于确保网络设备的安全性。STP 技术用于防止网络环路。此外，无线网络覆盖技术用于支持移动办公和访客接入，确保网络的全面覆盖。

该小型校园的网络建设需要多种设备来满足需求。首先，选择两台路由器（AR1、AR2）作为出口网关，支持 VRRP 协议。其次，核心层需要两台支持堆叠技术的交换机（LSW1、LSW2 使用普通线缆堆叠），用于连接各个接入层交换机和防火墙。接入层需要多台交换机（LSW3、LSW4、LSW5）用于连接终端设备，如 PC、服务器等。防火墙方面，需要一台防火墙（FW）用于网络安全防护，支持分时访问。此外，还需要无线接入点（AP）用于无线网络覆盖。总体来看，本次实验设备包括 4 台路由器、4 台交换机、1 台防火墙、三台 PC 及一块树莓派（用于模拟服务器与提供 AP），确保实验网络的全面覆盖与高效运行。

3.2 实验环境

软件清单:

软件名称	软件功能
Apache HTTP Server	提供 Web 服务
Poste.io Mail Server	提供邮件服务（SMTP/POP3）
Vsftpd	提供 FTP 服务
Wireshark	网络数据包分析工具
PuTTY	SSH/Telnet 远程终端工具
EndeavourOS Linux	树莓派操作系统
Huawei eNSP	网络设备模拟与配置工具

硬件设备:

设备名称	设备型号	设备数量	设备名称
交换机	华为 S5735	4	CORE(LSW1 + LSW2)、 LSW3、LSW4
路由器	华为 AR6120-S	4	R1、R2、R3、R_NEW
防火墙	华为 USG6303E-AC	1	FW
树莓派	Raspberry Pi Model 4B	1	server
PC	联想启天 M410 Windows 10	3	PC1、PC2、PC3

另有网线、控制线若干。

3.3 任务分工

任务	分工	时间
结构设计与构思	程景愉	10.22
服务器配置	程景愉	10.23-10.28
交换机路由器配置	程景愉	10.23-10.28
防火墙配置	程景愉	10.23-10.28
调试	程景愉	10.29
实验测试	程景愉	11.1-11.2
进阶实验	程景愉	11.7-11.8

3.4 拓扑图表

下面给出拓扑图和设备连接表，详细描述该小型校园网络的设计方案。

3.4.1 拓扑图

物理链路的拓扑图如 Figure 1 所示（见下页）：

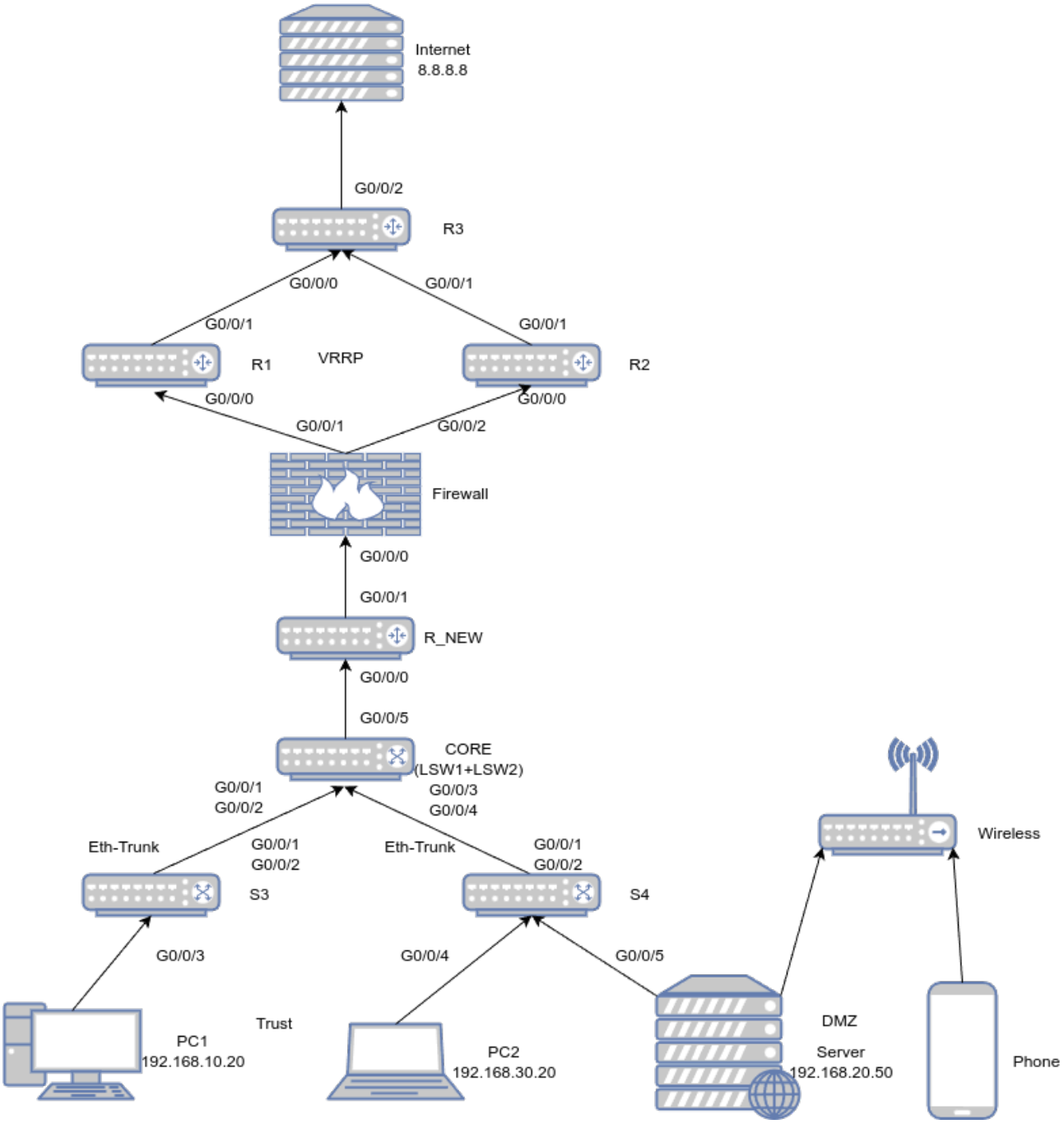

Figure 1: 实验拓扑图

实验示意图如 Figure 2 所示（见下页）:

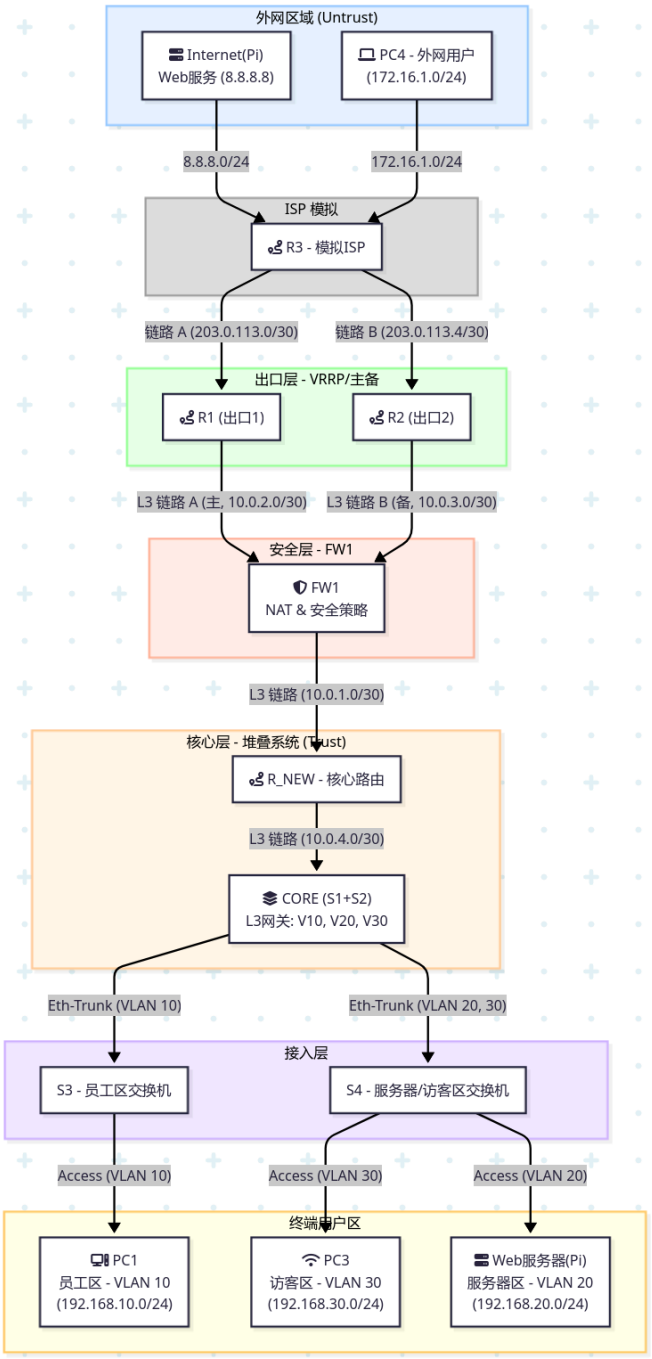

Figure 2: 实验示意图

接下来给出设备连接表（拓扑表）：

设备	接口	IP 地址	掩码	网关	备注
VLANs					
CORE	Vlanif 10	192.168.10.254	/24	-	员工区 (V10) 网关
CORE	Vlanif 20	192.168.20.254	/24	-	服务器区 (V20) 网关
CORE	Vlanif 30	192.168.30.254	/24	-	访客区 (V30) 网关
终端					
PC1	Eth0/0/1	192.168.10.x	/24	192.168.10.254	(DHCP)
Server(Pi)	Eth0/0/1	192.168.20.50	/24	192.168.20.254	(静态)
PC3	Eth0/0/1	192.168.30.x	/24	192.168.30.254	(DHCP)
PC4	Eth0/0/1	172.16.1.10	/24	172.16.1.254	(静态)
Internet(Pi)	Eth0/0/1	8.8.8.8	/24	8.8.8.1	(静态)
P2P 链路					
FW1	G1/0/0	10.0.1.1	/30	-	To R_NEW (Trust)
R_NEW	G0/0/0	10.0.1.2	/30	-	To FW1
R_NEW	G0/0/1	10.0.4.1	/30	-	To CORE
CORE	G(Stack)0/0/1	10.0.4.2	/30	-	To R_NEW
FW1	G1/0/1	10.0.2.2	/30	-	To R1 (Untrust)
R1	G0/0/0	10.0.2.1	/30	-	To FW1
FW1	G1/0/2	10.0.3.2	/30	-	To R2 (Untrust)
R2	G0/0/0	10.0.3.1	/30	-	To FW1
R1	G0/0/1	203.0.113.2	/30	-	To R3 (主)
R3	G0/0/0	203.0.113.1	/30	-	To R1
R2	G0/0/1	203.0.113.6	/30	-	To R3 (备)
R3	G0/0/1	203.0.113.5	/30	-	To R2
R3	G0/0/2	172.16.1.254	/24	-	To PC4
R3	G0/0/3	8.8.8.1	/24	-	To Internet(Pi)

Figure 3: IP 地址表（以实际实验为准）

4 实验步骤及结果

4.1 设备连接

将所有设备按照拓扑图连接好，确保每个设备的接口都正确连接：

Figure 4: 机柜正面接线图

Figure 5: 机柜背面接线图

注：以上为验收前拍摄的图片，验收后有返回机房进行实验补充如交换机堆叠与邮件服务器部署，实际情况以报告内容为准。

4.2 接入层 (S3, S4) 与核心层 (CORE) L2/L3 基本功能配置

4.2.1 组建堆叠系统

堆叠功能在验收后补充进行，原因是一开始以为必须有专用堆叠线缆导致无法实验，后查询华为文档发现支持普通线缆堆叠。在此处配置开始之前，必须明确：本设备的逻辑堆叠端口 stack-port 0/1 对应的物理端口，必须连接邻设备的逻辑堆叠端口 stack-port 0/2 对应的物理端口，否则堆叠组建不成功。

1. 配置逻辑堆叠端口并加入物理成员端口。

- 配置 LSW1 的业务口 g0/0/20、g0/0/21 为物理成员端口，并加入到相应的逻辑堆叠端口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSW1
[LSW1] interface stack-port 0/1
[LSW1-stack-port0/1] port interface g0/0/20 enable
Warning: Enablingstack function may cause configuration loss on the
interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait.
[LSW1-stack-port0/1] quit
[LSW1] interface stack-port 0/2
[LSW1-stack-port0/2] port interface g0/0/21 enable
Warning: Enablingstack function may cause configuration loss on the
interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait.
[LSW1-stack-port0/2] quit
```

- 配置 LSW2 的业务口 g0/0/20、g0/0/21 为物理成员端口，并加入到相应的逻辑堆叠端口。

```
<HUAWEI> system-view
[HUAWEI] sysname LSW2
[LSW2] interface stack-port 0/1
[LSW2-stack-port0/1] port interface g0/0/20 enable
Warning: Enablingstack function may cause configuration loss on the
interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait.
[LSW2-stack-port0/1] quit
[LSW2] interface stack-port 0/2
[LSW2-stack-port0/2] port interface g0/0/21 enable
Warning: Enablingstack function may cause configuration loss on the
interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait.
[LSW2-stack-port0/2] quit
```

2. 配置堆叠 ID 和堆叠优先级
   - 配置 LSW1 的堆叠优先级为 200。

```
[LSW1] stack slot 0 priority 200
Warning: Do not frequently modify the Priority because it will make the
stack split. Continue? [Y/N]:y
```

   - 配置 LSW2 的堆叠 ID（即 Slot）为 1。

```
[LSW2] stack slot 0 renumber 1
Warning: All the configurations related to the slot ID will be lost
after the slot ID is modified.
Do not frequently modify the slot ID because it will make the stack
split. Continue? [Y/N]:y
Info: Stack configuration has been changed, and the device needs to
restart to make the configuration effective.
```

3. 在每台设备上、在用户界面下输入`save`命令，保存配置信息。
4. 关闭设备并按顺序启动

- 关闭 LSW1、LSW2。
- 先启动 LSW1，等待 2 分钟左右，控制机能够登录到 LSW1 之后，再启动 LSW2。

5. 检验配置结果 使用`display stack`命令查看堆叠状态，输出信息如下：

```
[CORE]disp stack
Stack mode: Service-port
Stack topology type: Ring
Stack system MAC: 6012-3c9a-5ff0
MAC switch delay time: 10 min
Stack reserved VLAN: 4093
Slot of the active management port: --
Slot      Role        MAC Address      Priority   Device Type
--------------------------------------------------------------
0         Master      6012-3c9a-5ff0   200        S5735S-S24T4S-A
1         Standby     642c-acc1-5970   100        S5735S-S24T4S-A
```

输出展示了堆叠的状态信息，包括堆叠模式、堆叠拓扑类型、堆叠系统MAC地址、MAC切换延迟时间、堆叠保留VLAN、激活管理端口的槽位、各个槽位的角色、MAC地址、优先级和设备类型。其中，槽位 0 的 Priority 为 200，槽位 1 的 Priority 为 100，在竞争中槽位 0 最终会成为 Master 角色，槽位 1 为 Standby 角色。按照顺序上电能够保证设备快速进入事先规定好的角色。

配置完成后，两台设备将组成一个堆叠系统，逻辑上看成一个设备，标号为 CORE，称为核心集群。在后续的配置中，将以 CORE 作为设备名称。

4.2.2 配置员工区交换机

员工区交换机 S3 主要负责连接员工的终端设备（如 PC1），并通过核心集群与其他网络区域进行通信。为了确保网络的高效性和安全性，需要对 S3 进行基本的 VLAN 和链路聚合配置。下面开始配置 S3 的基本信息和 VLAN：

```
[S3] sysname S3
[S3] vlan batch 10

# 配置 Eth-Trunk 到 CORE
[S3] interface Eth-Trunk 1
[S3] port link-type trunk
[S3] port trunk allow-pass vlan 10
[S3] mode lacp-static  # 静态LACP
[S3] quit

[S3] interface GigabitEthernet 0/0/1
[S3] eth-trunk 1
[S3] quit
[S3] interface GigabitEthernet 0/0/2
[S3] eth-trunk 1
[S3] quit

# 配置接入端口 (PC1)
[S3] interface GigabitEthernet 0/0/3
[S3] port link-type access
[S3] port default vlan 10
```

```
[S3] stp edged-port enable  # 边缘端口，快速转发
[S3] quit
```

4.2.3 配置服务器/访客区交换机

服务器/访客区交换机 S4 主要负责连接服务器和访客的终端设备（如 PC3），并通过核心集群与其他网络区域进行通信。为了确保网络的高效性和安全性，需要对 S4 进行基本的 VLAN 和链路聚合配置。下面开始配置 S4 的基本信息和 VLAN：

```
[S4] sysname S4
[S4] vlan batch 20 30

# 配置 Eth-Trunk 到 CORE
[S4] interface Eth-Trunk 1
[S4] port link-type trunk
[S4] port trunk allow-pass vlan 20 30
[S4] mode lacp-static
[S4] quit

[S4] interface GigabitEthernet 0/0/1
[S4] eth-trunk 1
[S4] quit
[S4] interface GigabitEthernet 0/0/2
[S4] eth-trunk 1
[S4] quit

# 配置接入端口 (Server)
[S4] interface GigabitEthernet 0/0/3
[S4] port link-type access
[S4] port default vlan 20
[S4] stp edged-port enable
[S4] quit

# 配置接入端口 (PC3)
[S4] interface GigabitEthernet 0/0/4
[S4] port link-type access
[S4] port default vlan 30
[S4] stp edged-port enable
[S4] quit

# 配置接入端口 (R_NEW)
[S4] interface GigabitEthernet 0/0/5
[S4] port link-type access
[S4] port default vlan 40
[S4] stp edged-port enable
[S4] quit
```

4.2.4 配置核心堆叠交换机的 Eth-Trunk 功能和接口 IP 地址

此步骤是要将核心集群与其他设备相连的物理链路聚合起来，以提高链路的带宽和可靠性。

1. 配置 CORE 网关

```
[CORE] vlan batch 10 20 30 40

[CORE] interface Vlanif 10
[CORE] ip address 192.168.10.254 255.255.255.0
[CORE] quit

[CORE] interface Vlanif 20
[CORE] ip address 192.168.20.254 255.255.255.0
[CORE] quit

[CORE] interface Vlanif 30
[CORE] ip address 192.168.30.254 255.255.255.0
[CORE] quit

[CORE] interface Vlanif 40
[CORE] ip address 10.0.4.1 255.255.255.252
[CORE] quit
```

2. 配置 Eth-Trunk 到 S3

```
[CORE] interface Eth-Trunk 1
[CORE] port link-type trunk
[CORE] port trunk allow-pass vlan 10
[CORE] mode lacp-static
[CORE] quit
[CORE] interface GigabitEthernet 1/0/1
[CORE] eth-trunk 1
[CORE] quit
[CORE] interface GigabitEthernet 2/0/1
[CORE] eth-trunk 1
[CORE] quit
```

3. 配置 Eth-Trunk 到 S4

```
[CORE] interface Eth-Trunk 2
[CORE] port link-type trunk
[CORE] port trunk allow-pass vlan 20 30
[CORE] mode lacp-static
[CORE] quit
[CORE] interface GigabitEthernet 1/0/2
[CORE] eth-trunk 2
[CORE] quit
[CORE] interface GigabitEthernet 2/0/2
[CORE] eth-trunk 2
[CORE] quit
```

4. 配置 CORE 接口到 R_NEW

```
[CORE] interface GigabitEthernet 1/0/3
[CORE] port link-type access
[CORE] port default vlan 40
[CORE] quit
```

4.3 接入层安全配置 (S3, S4)

接入层的配置比较简单，主要涉及到 VLAN, MAC 地址绑定。

1. 配置 S3：

```
[S3] dhcp enable
[S3] dhcp snooping enable
[S3] dhcp snooping enable vlan 10

# 信任上联到 CORE 的 Trunk 口
[S3] interface Eth-Trunk 1
[S3] dhcp snooping trusted
[S3] quit

# 配置 PC1 端口安全
[S3] interface GigabitEthernet 0/0/3
[S3] port-security enable
[S3] port-security max-mac-num 1  # 只允许1个MAC地址
[S3] port-security protect-action restrict # 丢弃并告警
[S3] quit
```

2. 配置 S4：

```
[S4] dhcp enable
[S4] dhcp snooping enable
[S4] dhcp snooping enable vlan 20 30

# 信任上联到 CORE 的 Trunk 口
[S4] interface Eth-Trunk 1
[S4] dhcp snooping trusted
[S4] quit

# 配置 Server 端口安全
[S4] interface GigabitEthernet 0/0/3
[S4] port-security enable
[S4] port-security max-mac-num 1
[S4] port-security protect-action restrict
[S4] quit

# 配置 PC3 端口安全
[S4] interface GigabitEthernet 0/0/4
[S4] port-security enable
[S4] port-security max-mac-num 1
[S4] port-security protect-action restrict
[S4] quit
```

4.4 OSPF 路由配置

本次实验我将使用 OSPF Area 0 作为内部骨干区域，Area 1 作为外部 ISP 区域。

1. 在 CORE 上配置路由

```
[CORE] ospf 1 router-id 1.1.1.1
[CORE] area 0
[CORE] network 192.168.10.0 0.0.0.255
[CORE] network 192.168.20.0 0.0.0.255
[CORE] network 192.168.30.0 0.0.0.255
[CORE] network 10.0.4.0 0.0.0.3
[CORE] quit
[CORE] quit
```

2. 在 R_NEW 上配置路由

```
[R_NEW] sysname R_NEW
[R_NEW] interface GigabitEthernet 0/0/0
[R_NEW] ip address 10.0.1.2 255.255.255.252
[R_NEW] quit
[R_NEW] interface GigabitEthernet 0/0/1
[R_NEW] ip address 10.0.4.1 255.255.255.252
[R_NEW] quit

[R_NEW] ospf 1 router-id 2.2.2.2
[R_NEW] area 0
[R_NEW] network 10.0.1.0 0.0.0.3
[R_NEW] network 10.0.4.0 0.0.0.3
[R_NEW] quit
[R_NEW] quit
```

3. 在 R1 (出口 1 - 主) 上配置路由

这里我在验收后补充实验时选择改为使用`ospf cost`来替代`VRRP`实现冗余备份功能，增强网络系统的健壮性。

```
[AR2] interface Eth-Trunk 2
[AR2-Eth-Trunk2] undo portswitch
[AR2-Eth-Trunk2] mode lacp-static
[AR2-Eth-Trunk2] quit
[AR2] interface GigabitEthernet 0/0/4
[AR2-GigabitEthernet0/0/4] Eth-Trunk 2
[AR2-GigabitEthernet0/0/4] quit
[AR2] interface GigabitEthernet 0/0/5
[AR2-GigabitEthernet0/0/5] Eth-Trunk 2
[AR2-GigabitEthernet0/0/5] quit
```

1. 在 R2 (出口 2 - 备) 上配置路由

```
[R2] sysname R2
[R2] interface GigabitEthernet 0/0/0
[R2] ip address 10.0.3.1 255.255.255.252
[R2] quit
[R2] interface GigabitEthernet 0/0/1
[R2] ip address 203.0.113.6 255.255.255.252
[R2] ospf cost 100 # **关键：设置高 cost，作为备路**
[R2] quit
```

```
[R2] ospf 1 router-id 4.4.4.4
[R2] area 0
[R2] network 10.0.3.0 0.0.0.3
[R2] quit
[R2] area 1
[R2] network 203.0.113.4 0.0.0.3
[R2] quit
[R2] quit
```

2. 在 R3 (ISP 模拟) 上配置路由

```
[R3] sysname R3
[R3] interface GigabitEthernet 0/0/0
[R3] ip address 203.0.113.1 255.255.255.252
[R3] quit
[R3] interface GigabitEthernet 0/0/1
[R3] ip address 203.0.113.5 255.255.255.252
[R3] quit
[R3] interface GigabitEthernet 0/0/2
[R3] ip address 172.16.1.254 255.255.255.0
[R3] quit
[R3] interface GigabitEthernet 0/0/3
[R3] ip address 8.8.8.1 255.255.255.0
[R3] quit

[R3] ospf 1 router-id 5.5.5.5
[R3] area 1
[R3] network 203.0.113.0 0.0.0.3
[R3] network 203.0.113.4 0.0.0.3
[R3] network 172.16.1.0 0.0.0.255
[R3] network 8.8.8.0 0.0.0.255
[R3] quit
[R3] ospf 1
[R3] default-route-advertise always
[R3] quit
```

4.4.1 配置出口网关的 BFD 功能

配置 R1 和 R2 之间的 BFD 功能，用于快速检测链路故障并触发 OSPF 路由收敛。

1. 配置全局 BFD 功能。

```
[R1] bfd
[R1-bfd] quit
```

```
[R2] bfd
[R2-bfd] quit
```

2. 在 R1 上配置 OSPF 的 BFD 特性。

```
[R1] ospf 100   // 进入 OSPF 视图
[R1-ospf-100] bfd all-interfaces enable   // 打开 OSPF BFD 特性的开关，建
```

```
立 BFD 会话
[R1-ospf-100] quit
```

3. 在 R2 上配置 OSPF 的 BFD 特性。

```
[R2] ospf 100   // 进入 OSPF 视图
[R2-ospf-100] bfd all-interfaces enable   // 打开 OSPF BFD 特性的开关，建
立 BFD 会话
[R2-ospf-100] quit
```

4. 配置 BFD 参数。

```
[R1-ospf-100] bfd all-interfaces min-rx-interval 1000 min-tx-interval 1000
detect-multiplier 3
[R2-ospf-100] bfd all-interfaces min-rx-interval 1000 min-tx-interval 1000
detect-multiplier 3
```

此时，R1 和 R2 之间已经建立了 BFD 会话，可以使用 `display bfd session` 命令查看 BFD 会话状态。

4.5 DHCP 中继与服务器配置

4.5.1 CORE 的 DHCP 中继配置

```
[CORE] dhcp enable
# 全局启用中继
[CORE] dhcp relay server-ip 10.0.1.1  # 指向 FW1 的 Trust 接口 IP

# 在 Vlanif 上启用
[CORE] interface Vlanif 10
[CORE] dhcp select relay
[CORE] quit

[CORE] interface Vlanif 30
[CORE] dhcp select relay
[CORE] quit
```

4.5.2 FW1 防火墙上的 DHCP 服务配置

此步骤在 FW1 的 Web-UI 中完成：

1. 导航到 网络 > DHCP > DHCP 服务器 > DHCP 地址池。
2. 新建 地址池 (VLAN 10)：

   地址池名称: VLAN10_Staff

   网段: 192.168.10.0

   掩码: 255.255.255.0

   网关: 192.168.10.254

   DNS 服务器: 8.8.8.8 (或 ISP 的 DNS)

地址池范围: 192.168.10.100 到 192.168.10.200

3. 新建 地址池 (VLAN 30)：

   地址池名称: VLAN30_Guest

   网段: 192.168.30.0

   掩码: 255.255.255.0

   网关: 192.168.30.254

   DNS 服务器: 8.8.8.8

   地址池范围: 192.168.30.100 到 192.168.30.200

确保 DHCP 服务器功能已在 Trust 区域接口上启用（通常默认启用）。

4.6 防火墙 (FW1) 的基本功能配置

4.6.1 接口与区域配置

1. 导航到 网络 > 接口。

   配置 GigabitEthernet1/0/0 (to R_NEW):

   安全区域: Trust

   IP 地址: 10.0.1.1 / 30

   安全区域：DMZ

   IP 地址: 192.168.20.0/24

   配置 GigabitEthernet1/0/1 (to R1):

   安全区域: Untrust

   IP 地址: 10.0.2.2 / 30

   配置 GigabitEthernet1/0/2 (to R2):

   安全区域: Untrust

   IP 地址: 10.0.3.2 / 30

Figure 6: 防火墙接口配置

4.6.2 防火墙的 OSPF 配置

```
[FW1] ospf 1 router-id 6.6.6.6
[FW1-ospf-1] area 0
[FW1-ospf-1-area-0.0.0.0] network 10.0.1.0 0.0.0.3
[FW1-ospf-1-area-0.0.0.0] network 10.0.2.0 0.0.0.3
```

```
[FW1-ospf-1-area-0.0.0.0] network 10.0.3.0 0.0.0.3
[FW1-ospf-1-area-0.0.0.0] quit
[FW1-ospf-1] quit
[FW1] quit
```

4.6.3 安全策略 (内网上网)

导航到 策略 > 安全策略。

新建 策略:

名称: Trust_to_Untrust_Allow

源区域: Trust

目的区域: Untrust

源地址: Any (或 192.168.0.0/16)

目的地址: Any

服务: Any

动作: Permit

Figure 7: 安全策略配置

4.6.4 SNAT (源 NAT) 策略 (内网上网)

导航到 策略 > NAT 策略 > 源 NAT。

新建 策略:

源区域: Trust

目的区域: Untrust

源地址: 192.168.0.0 / 16 (覆盖所有内网 VLAN)

目的地址: Any

动作: 源 NAT

转换模式: 出接口地址 (这样流量走 R1 就 NAT 成 R1 接口 IP，走 R2 就 NAT 成 R2 接口 IP)。
注意：这里 FW1 的出接口是 10.0.2.2 和 10.0.3.2，这还不是实验中设计的公网 IP。

Figure 8: NAT 策略配置

拓扑缺陷与解决： 我设计的拓扑中，FW1 在 R1/R2 之后，SNAT 需要做两次。

FW1 (Web-UI): Trust -> Untrust (192.168.x.x -> 10.0.2.2/10.0.3.2)

R1/R2 (CLI): 需要再做一次 NAT (192.168.x.x -> 203.0.113.x)

为解决问题，在 R1/R2 上配置 SNAT :

```
[R1] acl 3000
[R1-acl-adv-3000] rule 5 permit ip source 192.168.0.0 0.0.255.255
[R1-acl-adv-3000] quit
[R1] interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1] nat outbound 3000
[R1-GigabitEthernet0/0/1] quit

[R2] acl 3000
[R2-acl-adv-3000] rule 5 permit ip source 192.168.0.0 0.0.255.255
[R2-acl-adv-3000] quit
[R2] interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1] nat outbound 3000
[R2-GigabitEthernet0/0/1] quit
```

FW1 上的 SNAT (Web-UI): (如上所述) Trust -> Untrust，源: 192.168.0.0/16，动作: NAT (出接口地址)。

4.6.5 分时访问策略配置

导航到 对象 > 时间段。

新建 时间段:

名称: Work_Time

类型: 周期

星期: 勾选 周一 到 周五

时间: 08:00:00 到 17:00:00

导航到 策略 > 安全策略。

修改 之前的 Trust_to_Untrust_Allow 策略:

源地址: 更改为 192.168.10.0/24 (仅员工区)

时间段: 选择 Work_Time

新建一条策略 (服务器/访客全天可上):

名称: Server_Guest_Allow

源区域: Trust

目的区域: Untrust

源地址: (创建一个地址组包含 192.168.20.0/24 和 192.168.30.0/24)

动作: Permit

将此策略拖到 Work_Time 策略下方。

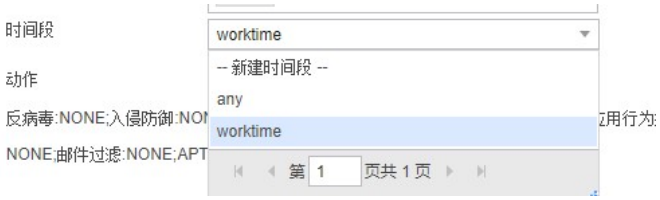

Figure 9: 分时访问策略配置

4.7 树莓派服务器的配置

树莓派在本次实验中设置静态 IP 地址为 `192.168.20.50/24`，充当 Web 服务器，FTP 服务器与邮件服务器的角色，同时还提供 AP 实现无线接入功能。

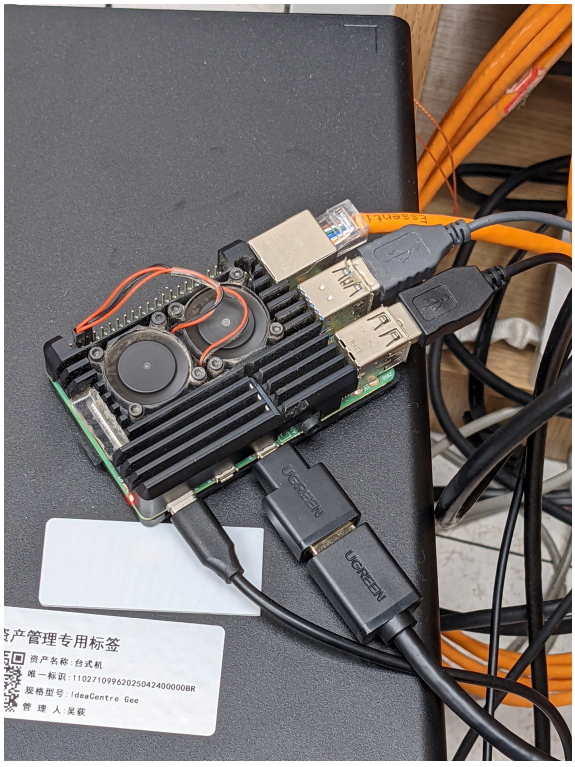

Figure 10: 实验中的 Raspberry Pi 4B 服务器

4.7.1 配置 Web 服务器

我的树莓派安装了 EndeavourOS 系统，使用 Apache 作为 Web 服务器。配置步骤如下：

1. 安装 Apache：

```
sudo pacman -Syu apache
```

2. 启动并设置 Apache 开机自启：

```
sudo systemctl start httpd
sudo systemctl enable httpd
```

3. 配置防火墙允许 HTTP 流量：

```
sudo ufw allow 80/tcp
```

4. 测试 Web 服务器：在浏览器中输入树莓派的 IP 地址 `http://192.168.20.50`，能看到 Apache 的默认页面，则表示 Web 服务启动成功。

5. 设计网页：使用 Httrack 将 www.nudt.edu.cn 网页镜像下载到 `/var/www/html` 目录下，替换默认的 `index.html` 文件。

Figure 11: Web 服务器页面

4.7.2 配置 FTP 服务器

在树莓派上安装并配置 vsftpd 作为 FTP 服务器，步骤如下：

1. 安装 vsftpd：

```
sudo pacman -Syu vsftpd
```

2. 启动并设置 vsftpd 开机自启：

```
sudo systemctl start vsftpd
sudo systemctl enable vsftpd
```

3. 配置防火墙允许 FTP 流量：

```
sudo ufw allow 21/tcp
```

4. 配置 vsftpd： 编辑配置文件 `/etc/vsftpd.conf`，确保以下参数被正确设置：

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
```

5. 重启 vsftpd 服务使配置生效：

```
sudo systemctl restart vsftpd
```

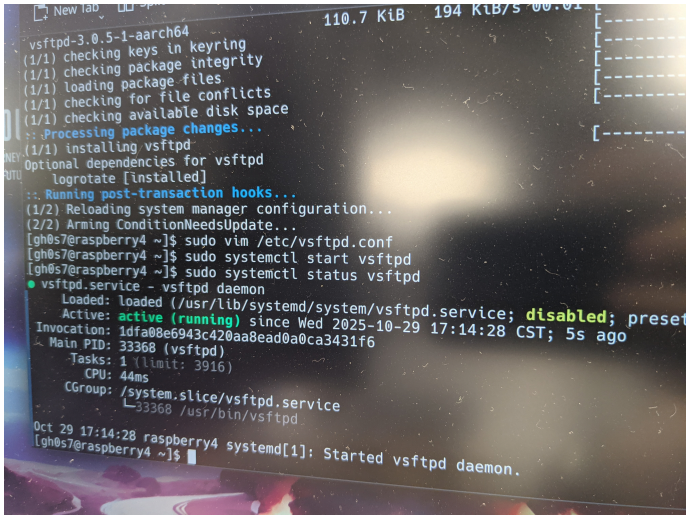

Figure 12: FTP 服务工作状态

1. 测试 FTP 服务器： 使用 FTP 客户端连接到树莓派的 IP 地址 `192.168.20.50`，并使用有效的用户名和密码进行登录。

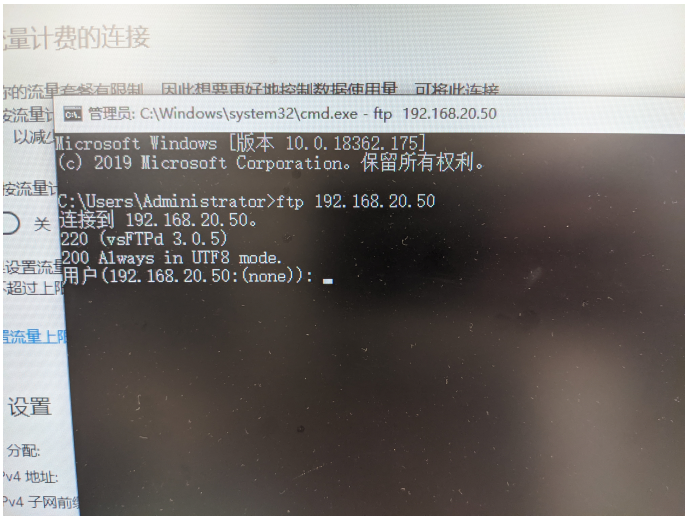

Figure 13: FTP 登录测试

由于树莓派已经开启了 SSH 服务，所以可以使用 SFTP 协议进行文件传输更为方便。

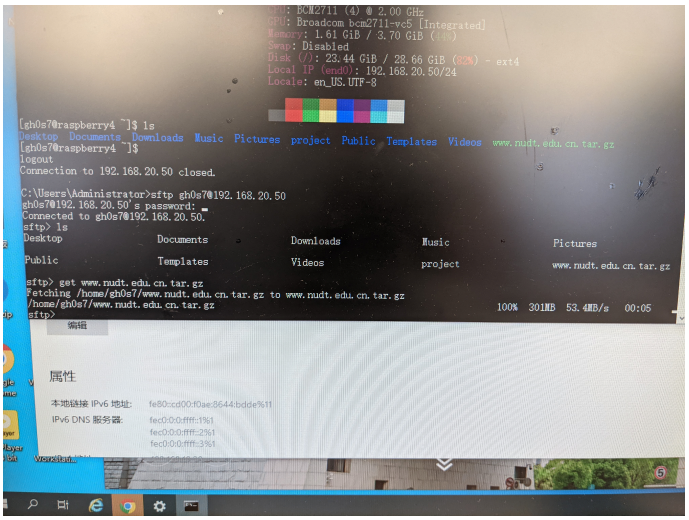

Figure 14: SFTP 传输测试

4.7.3 配置邮件服务器

本人拥有在公网服务器部署个人专有邮箱经验（地址为`chengjingyu@hifuu.ink`这里的`hifuu.ink`为我个人持有域名），也曾参与学校超算俱乐部邮件服务器建设（邮件地址为`scc@nudt.cc`，网站地址为`mail.nudt.cc`），这里选择在树莓派上拉取 poste.io 镜像进行快速部署。

1. 安装 Docker：

```
sudo pacman -Syu docker
sudo systemctl start docker
sudo systemctl enable docker
```

2. 拉取 poste.io 镜像并运行容器：

```
sudo docker run -d \
  --name mailserver \
  -p 25:25 -p 8080:80 -p 443:443 -p 587:587 -p 993:993 \
  -v /path/to/data:/data \
  analogic/poste.io
```

3. 配置防火墙允许邮件相关端口流量：

```
sudo ufw allow 25/tcp
sudo ufw allow 587/tcp
sudo ufw allow 993/tcp
```

4. 访问 poste.io 的 Web 界面进行邮箱配置：在浏览器中输入 `http://192.168.20.50`，按照提示完成域名绑定和邮箱账户创建。

5. 测试邮件服务器：在 poste.io 配置创建的邮箱账户，发送和接收测试邮件。

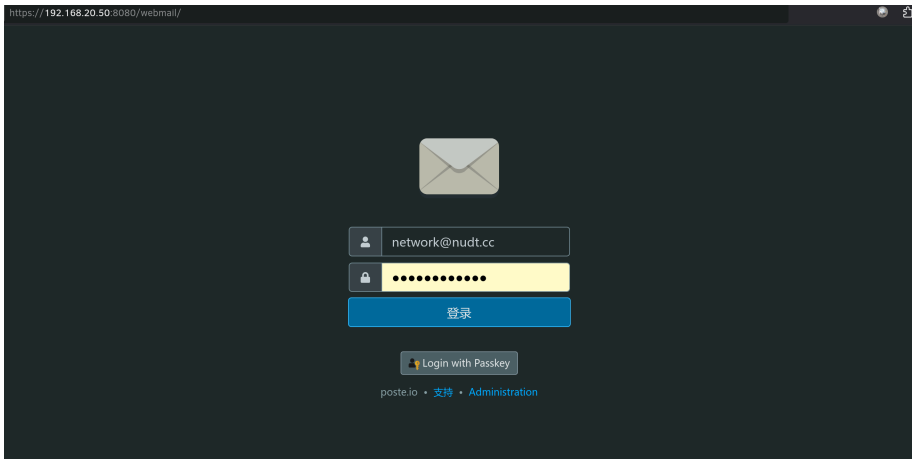

Figure 15: 邮件服务器登录界面

4.7.4 配置无线接入点 (AP)

在树莓派上配置无线接入点 (AP) 功能，使其能够为内网设备提供无线网络连接。步骤如下：

1. 安装 hostapd 和 dnsmasq：

```
sudo pacman -Syu hostapd dnsmasq
```

2. 配置 hostapd：编辑 `/etc/hostapd/hostapd.conf` 文件，添加以下内容：

```
interface=wlan0
driver=nl80211
ssid=gh0s7-hotap
hw_mode=g
channel=6
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
```

```
wpa_passphrase=********
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
```

3. 配置 dnsmasq： 编辑 `/etc/dnsmasq.conf` 文件，添加以下内容：

```
interface=wlan0
dhcp-range=192.168.20.100,192.168.20.200,255.255.255.0,24h
```

4. 启动并设置 hostapd 和 dnsmasq 开机自启：

```
sudo systemctl start hostapd
sudo systemctl enable hostapd
sudo systemctl start dnsmasq
sudo systemctl enable dnsmasq
```

5. 使用手机连接无线网络：在手机上搜索并连接到 SSID `gh0s7-hotap`，输入密码后即可连接成功，连接后即可访问 Web 服务器等资源。

Figure 16: 无线接入点连接成功

4.8 实验测试

4.8.1 测试方案

检查以下项目来验证整个网络的功能：

测试项目	操作与期望
应用-DHCP	PC1 与 PC3 应分别自动获取 192.168.10.x 与 192.168.30.x 网段地址，验证 DHCP 地址池与绑定策略。
连通性	PC1 依次 ping 192.168.10.254、192.168.20.50、192.168.30.x 以及 8.8.8.8，确认网关、内网服务器、跨 VLAN 路由与外网连通均正常。
应用-Web	PC1 访问 http://192.168.20.50，页面需正确展示树莓派 Web 服务内容。
应用-FTP	PC1 使用 FTP 客户端连接 192.168.20.50，凭有效账号完成登录与文件传输。
应用-邮件	在 PC1 上配置邮件客户端，完成测试邮件的发送与接收，验证 SMTP/IMAP 正常。
可靠性-多路径	PC1 持续 ping 8.8.8.8，手动 shutdown R1 外网口后应仅短暂中断并自动切换至 R2，undo shutdown 后可按 OSPF 策略回切。
可靠性-Eth-Trunk	PC1 持续 ping 192.168.10.254，断开 S3 与 CORE 的 Eth-Trunk1 任意链路时业务不中断，证明链路聚合冗余有效。
安全-分时访问	在 FW1 修改 Work_Time 至当前时间之外后，PC1 ping 8.8.8.8 应被阻断，而 PC3 与 Server 仍可外联，恢复时间策略后 PC1 恢复访问。
安全-端口安全/DHCP	在 S3 上调换 PC1 端口或新增私设 DHCP 服务器，应无法接入网络且不会影响既有终端地址获取。
安全-VLAN 隔离	PC1 ping PC3 应被隔离，而 PC3 ping Server 需可达，以验证 VLAN 与 ACL 策略。

4.8.2 测试结果

经过全面测试，网络的各项功能均正常运行，具体测试结果如下：

测试项目	结果结论
DHCP 功能	PC1 与 PC3 均成功获取对应网段地址，地址池与绑定策略正常。

测试项目	结果结论
连通性	PC1 可稳定访问网关、内网服务器、跨 VLAN 终端及外网公共地址，整体连通性良好。
Web 访问	PC1 可正常打开树莓派 Web 服务并显示完整页面。
FTP 访问	PC1 成功建立 FTP 会话并完成文件传输，认证与数据通道均正常。
邮件服务	客户端成功配置并完成收发测试邮件，SMTP/IMAP 服务表现稳定。
多路径冗余	R1 外网口故障时仅出现瞬时抖动，随后自动切换至 R2，恢复后可根据 OSPF 策略回切。
Eth-Trunk 冗余	断开 Eth-Trunk1 单链路时 PC1 ping 无丢包，聚合链路保障生效。
分时访问策略	非工作时段阻断 PC1 的外网访问，PC3 与 Server 不受限，策略符合预期。
端口安全与 DHCP	冒用终端无法接入，私设 DHCP 也未造成地址冲突，安全策略有效。
VLAN 隔离	PC1 ping PC3 被隔离，PC3 可访问 Server，隔离策略与允许路径均正确。

总体而言，网络设计和配置达到了预期目标，确保了网络的高效性、安全性和稳定性。所有测试均通过，网络系统运行良好。

5 实验总结

5.1 内容总结

本次实验的主要目标是设计和实现一个综合性强的中小型网络，涵盖了从网络规划、方案设计、硬件安装与配置、软件安装与配置、系统测试与联调、工程验收等完整的组网工程流程。实验通过模拟某学校的校园网络建设需求，详细展示了如何通过多种先进技术（如链路聚合、堆叠技术、VLAN、OSPF 等）来构建一个高效、安全、稳定的网络环境。实验首先进行了详细的需求分析，明确了网络覆盖、性能、安全、管理、扩展、服务器和存储、终端设备等方面的需求。随后，实验采用了多种网络技术来满足需求，包括 BFD 协议确保出口网关的健壮性，链路聚合技术（Eth-trunk）提升网络带宽和链路可靠性，堆叠技术用于核心交换机的冗余和扩展，VLAN 技术用于划分不同部门的安全区域等等。

实验通过多个阶段的验证，确保网络的各项功能正常运行。包括内网主机之间的通信、内网主机访问 Web 服务器、外网主机访问内网服务器、防火墙安全策略的验证、出口网关的双机热备验证等。

5.2 困难挑战

首先是笔者由于是唯一一个单人实验小组，需要独自完成从需求分析到最终测试的所有环节，工作量较大且任务繁重。其次，在配置过程中遇到了多种技术挑战，例如核心交换机的堆叠配置、路由配置等，这些都需要深入理解设备的工作原理和配置命令。此外，实验中还需要处理各种突发问题，如设备间的兼容性问题、配置错误导致的网络故障等，这些都考验了笔者的问题解决能力和应变能力。

在解决问题的过程中，我尤其要感谢教辅学长，张军老师与 Deepseek 的悉心指导与帮助。他们不仅在技术上给予了我宝贵的建议，还在思路上启发了我，让我能够更好地理解网络设计与配置的核心理念。通过这次实验，我不仅提升了自己的技术能力，也增强了独立解决问题的信心和能力。

5.3 心得感悟

本次实验自由度较大，时间跨度长，我选择了比较有综合性的设计方案同时也需要个人独立完成，因此实现难度较大。在配置的过程中，遇到了很多困难，但也让我对网络设备的运行机制有了更深的理解。从需求分析到方案设计，再到设备配置和测试验收，每一个环节都需要严谨的态度和细致的操作。实验中的每一步配置都充满了挑战，尤其是在核心交换机的堆叠配置、各设备之间的 OSPF 配置，防火墙的 NAT 的配置等方面，我遇到了不少困难，但也因此积累了宝贵的实践经验。

参考文献

[1] 华为. S5735-L, S5735S-L, S5735S-L-M 业务口堆叠支持情况 - S300, S500, S2700, S5700, S6700 V200R021C00, C01 配置指南-设备管理 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1100212502/d9806384.

[2] 华为. S5735-L, S5735S-L, S5735S-L-M 业务口堆叠支持情况 - S300, S500, S2700, S5700, S6700 V200R021C00, C01 配置指南-设备管理 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1100212502/493f7e15.

[3] 华为. 什么是堆叠？为什么需要堆叠？ - 华为[EB/OL]. (2024-11-07). https://info.support.huawei.com/info-finder/encyclopedia/zh/%E5%A0%86%E5%8F%A0.html.

[4] 华为云. 网工最容易混淆的Ethernet、trunk、Eth-Trunk、E-Trunk，四者之间有什么区别？-云社区-华为云[EB/OL]. (2024-11-07). https://bbs.huaweicloud.com/blogs/386900.

[5] 未知. awesome-selfhosted[EB/OL]. (2024-11-07). https://awesome-selfhosted.net/.

[6] CSDN. 华为交换机查看端口相关信息常用命令_华为交换机查看端口状态命令-CSDN博客[EB/OL]. (2024-11-07). https://blog.csdn.net/zhongguoYPT/article/details/130771351.

[7] EOLINK. 华为设备堆叠配置命令（查看华为堆叠命令）-eolink官网[EB/OL]. (2024-11-07). https://www.eolink.com/news/post/24989.html.

[8] 华为. 集群/堆叠通用部署 - S300, S500, S2700, S3700, S5700, S6700, S7700, S7900, S9700 系列交换机 典型配置案例（V200） - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000069491/4af18100#ZH-CN_TOPIC_0177315553.

[9] 华为. 出口网络设计 - 云园区网络解决方案 V100R022C00 大中型园区网络设计与部署指南（虚拟化场景）- 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1100278208/4d9ef478.

[10] 华为. 清除堆叠配置 - S1720, S2700, S3700, S5700, S6700, S7700, S7900, S9700 系列交换机 常用操作指南（V200） - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000057409?section=j00l.

[11] 华为. 添加和删除堆叠成员端口 - CloudEngine S5700, S6700 V600R022C10 配置指南-虚拟化 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1100302422/cbd1d1a0.

[12] 华为. 配置通过 Telnet 登录设备 - 配置通过 Telnet 登录设备 - S300, S500, S2700, S5700, S6700 V200R022C00 配置指南-基础配置 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1100277061/b3180b88.

[13] CSDN. 单向能ping通，反向不通故障解决过程_单向ping通 反向不通-CSDN博客[EB/OL]. (2024-11-07). https://blog.csdn.net/wj31932/article/details/89634302.

[14] 51CTO. 华为防火墙 VRRP 双机热备的原理及配置详解_51CTO博客_华为防火墙双机热备[EB/OL]. (2024-11-07). https://blog.51cto.com/u_14154700/2427616.

[15] USG6310 PC 能 ping 通防火墙，防火墙无法 ping 通 PC[EB].