网 络 工 程
本 科 实 验 报 告

实验名称：异构网络设计综合实验

学 员 姓 名	王李烜	学 号	202202001046
学 员 姓 名	廖中煜	学 号	202202001032
学 员 姓 名	王誉潞	学 号	202202001051
指 导 教 员	张军	职 称	工程师
实 验 室	306-707	实 验 时 间	2024.12.24

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 实验目的与要求

1. 实验目的：通过本实验，让学员熟悉从网络规划到方案撰写，再到工程实施及测试验收的整个过程。
2. 实验任务：设计和实现一个包含局域网和广域网的中型网络。

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。

2 需求分析

第三建筑公司大楼中需要布设网络基础设施。下面通过需求分析报告与技术分析阐明项目的实施方案。

2.1 需求分析报告书

网络工程项目需求分析报告

项目名称：第三建筑公司本部大楼网络工程项目

客户单位：第三建筑公司

承建单位：第三网络工程基础设施公司

日期：2024 年 12 月

一、项目背景

第三建筑公司（以下简称“贵公司”）目前正在规划公司总部大楼的网络基础设施，旨在建立一个高效、安全、稳定的网络环境，支持公司日常办公、项目管理、数据存储及未来业务扩展需求。由于贵公司对网络设备和技术了解有限，特委托第三网络工程基础设施公司（以下简称“我司”）进行网络规划、设计、实施及维护。

二、项目目标

本项目的主要目标是建立一个覆盖贵公司总部大楼的网络系统，确保所有员工能够顺畅访问内部资源和外部互联网。同时，网络需提供安全、可靠的运行环境，保护公司数据免受外部威胁。此外，网络设计需具备良好的扩展性，能够支持未来业务增长和技术升级。

三、需求详述

（一）网络覆盖需求

贵公司总部大楼中，网络需覆盖所有办公区域、会议室、服务器机房及公共区域。此外，需在公司大楼内提供无线网络覆盖，支持员工移动办公和访客接入。

（二）网络性能需求

网络需支持高速数据传输，确保员工能够高效访问内部服务器和外部互联网。

（三）网络安全需求

需部署防火墙，保护贵公司网络免受外部攻击。不同部门之间的网络流量需进行隔离，确保敏感数据的安全性。同时，需支持远程员工通过 VPN 安全访问公司内部资源。

（四）网络管理需求

所有网络设备需支持集中管理，方便网络管理员进行配置和监控。网络设备需记录日志，便于故障排查和安全审计。网络管理员需能够远程访问和管理网络设备。

（五）网络扩展需求

网络需预留足够的端口和带宽，以便未来增加新的设备或用户。网络设计需考虑到未来的技术升级，确保能够支持新的网络协议和设备。

（六）服务器和存储需求

需为贵公司的 Web 服务器和数据库服务器提供稳定的网络连接。同时，需确保重要数据的定期备份和快速恢复能力。

（七）终端设备需求

所有员工的电脑、打印机等设备需能够接入网络。会议室内的投影仪、视频会议设备等也需接入网络，确保会议和协作的顺利进行。

四、项目交付要求

项目交付内容包括完整的网络拓扑设计及实施方案、所有网络设备的安装、配置及调试、网络安全策略的部署及测试、网络管理系统的部署及培训，以及项目文档（包括网络拓扑图、设备配置文档、操作手册等）。项目需在合同签订后 3 个月内完成，包括设计、采购、安装、调试及测试。

五、预算要求

项目预算需在合理范围内，具体金额可根据设计方案进行调整。我司将确保在满足需求的同时控制成本，提供性价比高的解决方案。

六、其他要求

（一）培训需求

项目实施完成后，我司将为贵公司IT团队提供相关设备的操作和维护培训，确保其能够独立进行日常管理和故障排查。

（二）售后服务

我司将提供至少1年的免费售后服务，包括设备维护、故障排查及技术支持。同时，我司将提供7 × 24小时的技术支持热线，确保在出现紧急问题时能够及时响应。

2.2 技术分析

为满足公司大楼的网络需求，网络建设需采用多种先进技术。首先，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。其次，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。此外，堆叠技术用于核心交换机的冗余和扩展，确保网络的高效管理和扩展性。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。防火墙旁挂系统则通过双机热备技术，确保网络安全防护的连续性。最后，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。

公司大楼的网络建设需要多种设备来满足需求。首先，需要两台路由器（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），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，需要两台防火墙（FW1、FW2）用于网络安全防护，支持双机热备。此外，还需要若干无线接入点（AP）用于无线网络覆盖。总体来看，设备数量包括2台路由器、5台交换机、2台防火墙及若干无线接入点，确保网络的全面覆盖与高效运行。

2.3 拓扑图表

下面给出拓扑图和设备连接表，详细描述公司大楼网络的设计方案。

2.3.1 拓扑图

物理链路的拓扑图如Figure 1所示（见下页）：

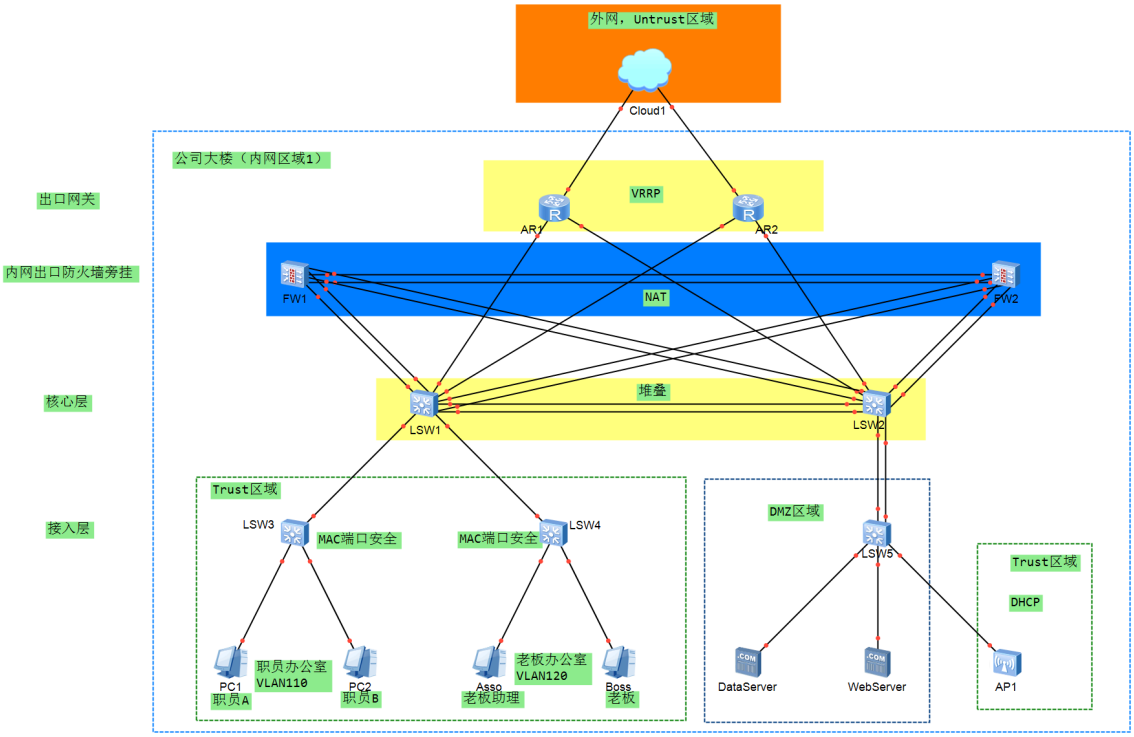


Figure 1: 实验拓扑图

核心交换机有 2 台，它们在物理上是横向而对等的关系。但由于使用了堆叠技术，核心层的 2 台交换机在逻辑上是同一个设备。此外，由于使用防火墙旁挂，所以需要把核心交换机分成内外两个 VPN 示例。而这两个 VPN 实例在逻辑上可以视为 2 个设备，故逻辑拓扑图由横向的 2 个设备变为了纵向的两个设备，如下图所示。

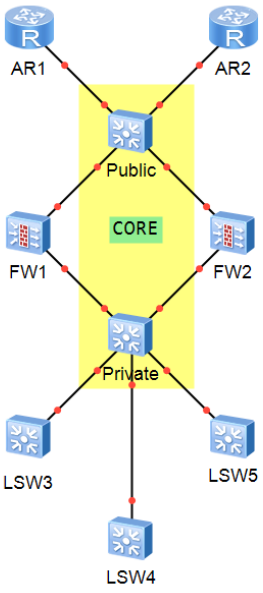


Figure 2: 逻辑拓扑图

接下来给出设备连接表（拓扑表）：

设备名称	接口	连接设备	对方接口	**IP** 地址	链路聚合 **ID**	**VLAN**	备注
LSW1	g0/0/1	LSW2	g0/0/1	-	6	-	用于与 LSW2 组建堆叠系统（iStack）
LSW1	g0/0/7	LSW2	g0/0/7	-	6	-	用于与 LSW2 组建堆叠系统（iStack）
LSW1	g0/0/3	AR1	g0/0/4	192.168.10.1/24	2	VLAN10	连接出口网关 AR1
LSW1	g0/0/4	AR2	g0/0/4	192.168.10.1/24	4	VLAN10	连接出口网关 AR2
LSW1	g0/0/5	LSW3	g0/0/3	192.168.110.1/24	-	VLAN110	连接接入层交换机 LSW3
LSW1	g0/0/6	LSW4	g0/0/3	192.168.120.1/24	-	VLAN120	连接接入层交换机 LSW4
LSW1	g0/0/8	FW1	g0/0/0	192.168.20.1/24	3	VLAN20	出口防火墙旁挂-外侧
LSW1	g0/0/9	FW1	g0/0/1	192.168.30.1/24	8	VLAN30	出口防火墙旁挂-内侧
LSW1	g0/0/10	FW2	g0/0/0	192.168.20.1/24	9	VLAN20	出口防火墙旁挂-外侧
LSW1	g0/0/11	FW2	g0/0/1	192.168.30.1/24	10	VLAN30	出口防火墙旁挂-内侧
LSW1	g0/0/13	LSW2	g0/0/13	-	-	-	用于多主检测（CORE-mad）
LSW2	g0/0/1	LSW1	g0/0/1	-	6	-	用于与 LSW1 组建堆叠系统（iStack）
LSW2	g0/0/7	LSW1	g0/0/7	-	6	-	用于与 LSW1 组建堆叠系统（iStack）
LSW2	g0/0/3	AR1	g0/0/5	192.168.10.1/24	2	VLAN10	连接出口网关 AR1
LSW2	g0/0/4	AR2	g0/0/5	192.168.10.1/24	4	VLAN10	连接出口网关 AR2
LSW2	g0/0/5	LSW5	g0/0/4	192.168.130.1/24	11	VLAN130	连接接入层交换机 LSW5
LSW2	g0/0/6	LSW5	g0/0/5	192.168.130.1/24	11	VLAN130	连接接入层交换机 LSW5
LSW2	g0/0/8	FW1	g0/0/2	192.168.20.1/24	3	VLAN20	出口防火墙旁挂-外侧
LSW2	g0/0/9	FW1	g0/0/3	192.168.30.1/24	8	VLAN30	出口防火墙旁挂-内侧
LSW2	g0/0/10	FW2	g0/0/2	192.168.20.1/24	9	VLAN20	出口防火墙旁挂-外侧
LSW2	g0/0/11	FW2	g0/0/3	192.168.30.1/24	10	VLAN30	出口防火墙旁挂-内侧
LSW2	g0/0/13	LSW1	g0/0/13	-	-	-	用于多主检测（CORE-mad）

Table 1: 核心交换机拓扑表

设备名称	接口	连接设备	对方接口	**IP** 地址	链路聚合 **ID**	**VLAN**	备注
AR1	g0/0/2	AR3	g0/0/0	-	-	-	连接内网出口 AR3
AR1	g0/0/4	LSW1	g0/0/3	192.168.10.2/24	2	-	用聚合链路连接堆叠系统
AR1	g0/0/5	LSW2	g0/0/3	192.168.10.2/24	2	-	用聚合链路连接堆叠系统
AR2	g0/0/3	AR4	g0/0/1	-	-	-	连接内网出口 AR4
AR2	g0/0/4	LSW1	g0/0/4	192.168.10.3/24	4	-	用聚合链路连接堆叠系统
AR2	g0/0/5	LSW2	g0/0/4	192.168.10.3/24	4	-	用聚合链路连接堆叠系统
AR3	g0/0/0	AR1	g0/0/2	-	-	-	连接内网出口 AR1
AR3	g0/0/1	外部路由器	未知	-	-	-	连接外部网络
VRRP	-	CORE	-	192.168.10.100/24	-	-	VRRP 网关连接 Public 区域

Table 2: 出口网关拓扑表

设备名称	接口	连接设备	对方接口	**IP** 地址	链路聚合 **ID**	**VLAN**	备注
PC1	3 号口	LSW3	g0/0/1	-	-	VLAN110	属于 VLAN110
PC2	8 号口	LSW3	g0/0/2	-	-	VLAN110	属于 VLAN110
Asso	2 号口	LSW4	g0/0/1	-	-	VLAN120	属于 VLAN120
Boss	6 号口	LSW4	g0/0/2	-	-	VLAN120	属于 VLAN120
WebServer	N/A	LSW5	g0/0/2	192.168.130.10	-	-	Web 服务器
DataServer	N/A	LSW5	g0/0/2	192.168.130.10	-	-	数据库服务器

Table 3: 终端设备与服务器拓扑表

设备名称	接口	连接设备	对方接口	**IP** 地址	链路聚合 **ID**	**VLAN**	备注
LSW3	g0/0/1	PC1	3 号口	-	-	-	Access
LSW3	g0/0/2	PC2	8 号口	-	-	-	Access
LSW3	g0/0/3	LSW1	g0/0/5	-	-	VLAN110	Trunk
LSW3	g0/0/4	LSW2	-	-	-	-	-
LSW3	g0/0/5~g0/0/7	新接入设备	不分接口	-	-	-	新接入设备端口
LSW4	g0/0/1	Asso	2 号口	-	-	-	Access
LSW4	g0/0/2	Boss	6 号口	-	-	-	Access
LSW4	g0/0/3	LSW1	g0/0/6	-	-	VLAN120	Trunk
LSW4	g0/0/4~g0/0/7	新接入设备	不分接口	-	-	-	新接入设备端口
LSW5	g0/0/2	DataServer	不分接口	192.168.130.10	-	-	Web 服务器地址
LSW5	g0/0/2	WebServer	不分接口	192.168.130.10	-	-	DNS 服务器地址
LSW5	g0/0/3	AP1	不分接口	-	-	-	-
LSW5	g0/0/4	LSW2	g0/0/5	-	-	-	-
LSW5	g0/0/5	LSW2	g0/0/6	-	-	-	-

Table 4: 接入层交换机拓扑表

设备名称	接口	连接设备	对方接口	**IP** 地址	链路聚合 **ID**	**VLAN**	备注
FW1	g0/0/0	LSW1	g0/0/8	192.168.20.2/24	3	VLAN20	出口防火墙旁挂-外侧
FW1	g0/0/1	LSW1	g0/0/9	192.168.30.2/24	8	VLAN30	出口防火墙旁挂-内侧
FW1	g0/0/2	LSW2	g0/0/8	192.168.20.2/24	3	VLAN20	出口防火墙旁挂-外侧
FW1	g0/0/3	LSW2	g0/0/9	192.168.30.2/24	8	VLAN30	出口防火墙旁挂-内侧
FW1	g0/0/4	FW2	g0/0/4	10.1.1.1/24	7	-	用于组建防火墙旁挂系统
FW1	g0/0/5	FW2	g0/0/5	10.1.1.1/24	7	-	用于组建防火墙旁挂系统
FW2	g0/0/0	LSW1	g0/0/10	192.168.20.3/24	3	VLAN20	出口防火墙旁挂-外侧
FW2	g0/0/1	LSW1	g0/0/11	192.168.30.3/24	8	VLAN30	出口防火墙旁挂-内侧
FW2	g0/0/2	LSW2	g0/0/10	192.168.20.3/24	3	VLAN20	出口防火墙旁挂-外侧
FW2	g0/0/3	LSW2	g0/0/11	192.168.30.3/24	8	VLAN30	出口防火墙旁挂-内侧
FW2	g0/0/4	FW1	g0/0/4	10.1.1.2/24	7	-	用于组建防火墙旁挂系统
FW2	g0/0/5	FW1	g0/0/5	10.1.1.2/24	7	-	用于组建防火墙旁挂系统

Table 5: 防火墙拓扑表

3 实验设备

设备名称	设备型号	设备数量	设备名称
交换机	华为 S5735	4	LSW1、LSW2、LSW3、LSW4
集线器	TPLINK TL-SG1008+	1	LSW5
路由器	华为 AR6120-S	2	AR1、AR2
防火墙	华为 USG6303E-AC	3	FW1、FW2
无线路由器	TP-LINK AX3000	1	AP
PC	联想启天 M410 Windows 10	4	PC1、PC2、Asso、Boss
PC	联想拯救者 R9000P Windows 11 23H2	1	外网主机
PC	联想拯救者 Y9000P Windows 10 24H4	1	DataServer、WebServer

另有网线、控制线若干。

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：

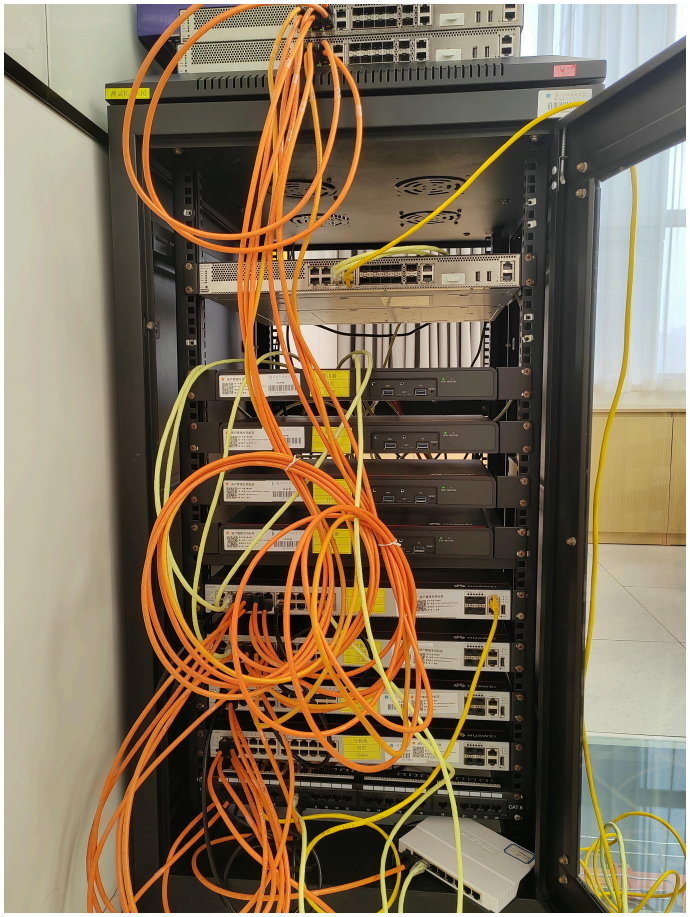


Figure 3: 机柜正面接线图

Figure 4: 机柜背面接线图

4.2 配置核心层堆叠系统基本功能

4.2.1 组建堆叠系统

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 g0/0/1、g0/0/7 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 g0/0/1 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 g0/0/7 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 g0/0/1、g0/0/7 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 g0/0/1 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 g0/0/7 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 配置核心集群的 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. 创建 Eth-Trunk1，用于连接 AR1，并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 1
[CORE-Eth-Trunk1] mode lacp
[CORE-Eth-Trunk1] quit
[CORE] interface GigabitEthernet 0/0/3
[CORE-GigabitEthernet0/0/3] Eth-Trunk 1
[CORE-GigabitEthernet0/0/3] quit
[CORE] interface GigabitEthernet 1/0/3
[CORE-GigabitEthernet1/0/3] Eth-Trunk 1
[CORE-GigabitEthernet1/0/3] quit
```

2. 创建 Eth-Trunk2，用于连接 AR2，并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 2
[CORE-Eth-Trunk2] mode lacp
[CORE-Eth-Trunk2] quit
[CORE] interface GigabitEthernet 0/0/4
[CORE-GigabitEthernet0/0/4] Eth-Trunk 2
[CORE-GigabitEthernet0/0/4] quit
[CORE] interface GigabitEthernet 1/0/4
[CORE-GigabitEthernet1/0/4] Eth-Trunk 2
[CORE-GigabitEthernet1/0/4] quit
```

3. 创建 Eth-Trunk3，用于连接 FW1（外侧），并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 3
[CORE-Eth-Trunk3] mode lacp
[CORE-Eth-Trunk3] quit
[CORE] interface GigabitEthernet 0/0/8
[CORE-GigabitEthernet0/0/8] Eth-Trunk 3
[CORE-GigabitEthernet0/0/8] quit
[CORE] interface GigabitEthernet 1/0/8
[CORE-GigabitEthernet1/0/8] Eth-Trunk 3
[CORE-GigabitEthernet1/0/8] quit
```

4. 创建 Eth-Trunk4，用于连接 FW1（内侧），并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 4
[CORE-Eth-Trunk4] mode lacp
[CORE-Eth-Trunk4] quit
[CORE] interface GigabitEthernet 0/0/9
[CORE-GigabitEthernet0/0/9] Eth-Trunk 4
[CORE-GigabitEthernet0/0/9] quit
[CORE] interface GigabitEthernet 1/0/9
[CORE-GigabitEthernet1/0/9] Eth-Trunk 4
[CORE-GigabitEthernet1/0/9] quit
```

5. 创建 Eth-Trunk5，用于连接 FW2（外侧），并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 5
[CORE-Eth-Trunk5] mode lacp
[CORE-Eth-Trunk5] quit
[CORE] interface GigabitEthernet 0/0/10
[CORE-GigabitEthernet0/0/10] Eth-Trunk 5
[CORE-GigabitEthernet0/0/10] quit
[CORE] interface GigabitEthernet 1/0/10
[CORE-GigabitEthernet1/0/10] Eth-Trunk 5
[CORE-GigabitEthernet1/0/10] quit
```

6. 创建 Eth-Trunk6，用于连接 FW2（内侧），并加入 Eth-Trunk 成员接口。

```
[CORE] interface Eth-Trunk 6
[CORE-Eth-Trunk6] mode lacp
[CORE-Eth-Trunk6] quit
[CORE] interface GigabitEthernet 0/0/11
[CORE-GigabitEthernet0/0/11] Eth-Trunk 6
[CORE-GigabitEthernet0/0/11] quit
[CORE] interface GigabitEthernet 1/0/11
[CORE-GigabitEthernet1/0/11] Eth-Trunk 6
[CORE-GigabitEthernet1/0/11] quit
```

4.2.3 配置核心集群的 VLAN 功能

经过前面的配置，核心集群上现在同时共存了 2 个 VPN 实例：Private 与 Public。它们互相隔离，表示内网与外网不能直接连通；每个实例内又需要配置多个 VLAN，并在每个 Eth 接口上限制 VLAN 的出入，借此来限制与不同用途的设备的连接。本步骤进行 VLAN 配置，并为每个 VLAN 配置 VLANIF 接口的 IP 地址。

1. 创建 VLAN 并配置 VLANIF 接口。

```
[CORE] vlan batch 10 20 30 110 120 130
[CORE] interface Vlanif 10
[CORE-Vlanif10] ip address 192.168.10.1 24
[CORE-Vlanif10] quit

[CORE] interface Vlanif 20
[CORE-Vlanif20] ip address 192.168.20.1 24
[CORE-Vlanif20] quit

[CORE] interface Vlanif 30
[CORE-Vlanif30] ip address 192.168.30.1 24
[CORE-Vlanif30] quit

[CORE] interface Vlanif 110
[CORE-Vlanif110] ip address 192.168.110.1 24
[CORE-Vlanif110] quit

[CORE] interface Vlanif 120
[CORE-Vlanif120] ip address 192.168.120.1 24
[CORE-Vlanif120] quit

[CORE] interface Vlanif 130
[CORE-Vlanif130] ip address 192.168.130.1 24
[CORE-Vlanif130] quit
```

2. 配置 Eth-Trunk 的 VLAN 允许列表
   - 配置 Eth-Trunk1 允许 VLAN10。

     ```
     [CORE] interface Eth-Trunk 1
     [CORE-Eth-Trunk1] port link-type trunk
     [CORE-Eth-Trunk1] port trunk allow-pass vlan 10
     [CORE-Eth-Trunk1] quit
     ```

   - 配置 Eth-Trunk2 允许 VLAN10。

     ```
     [CORE] interface Eth-Trunk 2
     [CORE-Eth-Trunk2] port link-type trunk
     [CORE-Eth-Trunk2] port trunk allow-pass vlan 10
     [CORE-Eth-Trunk2] quit
     ```

   - 配置 Eth-Trunk3 允许 VLAN20。

     ```
     [CORE] interface Eth-Trunk 3
     [CORE-Eth-Trunk3] port link-type trunk
     [CORE-Eth-Trunk3] port trunk allow-pass vlan 20
     [CORE-Eth-Trunk3] quit
     ```

   - 配置 Eth-Trunk4 允许 VLAN30。

     ```
     [CORE] interface Eth-Trunk 4
     [CORE-Eth-Trunk4] port link-type trunk
     [CORE-Eth-Trunk4] port trunk allow-pass vlan 30
     [CORE-Eth-Trunk4] quit
     ```

   - 配置 Eth-Trunk5 允许 VLAN20。

     ```
     [CORE] interface Eth-Trunk 5
     [CORE-Eth-Trunk5] port link-type trunk
     ```

```
[CORE-Eth-Trunk5] port trunk allow-pass vlan 20
[CORE-Eth-Trunk5] quit
```

- 配置 Eth-Trunk6 允许 VLAN30。

```
[CORE] interface Eth-Trunk 6
[CORE-Eth-Trunk6] port link-type trunk
[CORE-Eth-Trunk6] port trunk allow-pass vlan 30
[CORE-Eth-Trunk6] quit
```

- 配置 Eth-Trunk7 允许 VLAN130。

```
[CORE] interface Eth-Trunk 7
[CORE-Eth-Trunk7] port link-type trunk
[CORE-Eth-Trunk7] port trunk allow-pass vlan 130
[CORE-Eth-Trunk7] quit
```

配置完成后，通过`display vlan`命令查看 VLAN 配置信息，输出信息如下：

```
[CORE]disp vlan
The total number of VLANs is: 8
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/2(D)      GE0/0/5(U)      GE0/0/6(U)      GE0/0/12(D)
                GE0/0/13(U)     GE0/0/14(D)     GE0/0/15(D)     GE0/0/16(D)
                GE0/0/17(D)     GE0/0/18(D)     GE0/0/19(D)     GE0/0/20(D)
                GE0/0/21(D)     GE0/0/22(D)     GE0/0/23(D)     GE0/0/25(D)
                GE0/0/26(D)     GE0/0/27(D)     GE0/0/28(D)     GE1/0/2(D)
                GE1/0/6(U)      GE1/0/12(U)     GE1/0/13(U)     GE1/0/14(D)
                GE1/0/16(D)     GE1/0/17(D)     GE1/0/18(D)     GE1/0/19(D)
                GE1/0/20(D)     GE1/0/21(D)     GE1/0/22(D)     GE1/0/23(D)
                GE1/0/24(D)     GE1/0/25(D)     GE1/0/26(D)     GE1/0/27(D)
                GE1/0/28(D)     Eth-Trunk1(U)   Eth-Trunk2(U)   Eth-Trunk10(D)
                Eth-Trunk20(D)
10   common  TG:GE1/0/12(U)     Eth-Trunk1(U)   Eth-Trunk2(U)
20   common  UT:Eth-Trunk3(U)   Eth-Trunk5(U)
            TG:GE1/0/12(U)
30   common  UT:Eth-Trunk4(U)   Eth-Trunk6(U)
            TG:GE1/0/12(U)
66   common  UT:GE0/0/24(U)
            TG:GE1/0/12(U)
110  common  TG:GE0/0/5(U)      GE1/0/6(U)      GE1/0/12(U)
120  common  TG:GE0/0/6(U)      GE0/0/12(D)     GE1/0/12(U)
130  common  UT:GE1/0/5(U)      GE1/0/15(D)
            TG:GE1/0/12(U)

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
10   enable  default       enable  disable    VLAN 0010
20   enable  default       enable  disable    VLAN 0020
30   enable  default       enable  disable    VLAN 0030
66   enable  default       enable  disable    VLAN 0066
110  enable  default       enable  disable    VLAN 0110
```

```
120  enable  default       enable  disable    VLAN 0120
130  enable  default       enable  disable    VLAN 0130
```

输出中的信息与上文配置办法无异，说明各个 VLAN[1]配置生效。

4.3 配置接入层

接入层的配置比较简单，仅涉及到 VLAN。

1. 配置 LSW3：

```
<HUAWEI> system-view
[HUAWEI] sysname LSW3
[LSW3] vlan batch 110   // 创建 VLAN110

[LSW3] interface GigabitEthernet 0/0/1   // 配置连接 PC1 的接口为 Access 模式，加入 VLAN110
[LSW3-GigabitEthernet0/0/1] port link-type access
[LSW3-GigabitEthernet0/0/1] port default vlan 110
[LSW3-GigabitEthernet0/0/1] quit

[LSW3] interface GigabitEthernet 0/0/2   // 配置连接 PC2 的接口为 Access 模式，加入 VLAN110
[LSW3-GigabitEthernet0/0/2] port link-type access
[LSW3-GigabitEthernet0/0/2] port default vlan 110
[LSW3-GigabitEthernet0/0/2] quit

[LSW3] interface GigabitEthernet 0/0/3  // 配置连接 LSW1 的接口为 Trunk 模式，允许 VLAN110
通过
[LSW3-GigabitEthernet0/0/3] port link-type trunk
[LSW3-GigabitEthernet0/0/3] port trunk allow-pass vlan 110
[LSW3-GigabitEthernet0/0/3] quit
```

2. 配置 LSW4：

```
<HUAWEI> system-view
[HUAWEI] sysname LSW4
[LSW4] vlan batch 120   // 创建 VLAN120

[LSW4] interface GigabitEthernet 0/0/1   // 配置连接 Asso 的接口为 Access 模式，加入 VLAN120
[LSW4-GigabitEthernet0/0/1] port link-type access
[LSW4-GigabitEthernet0/0/1] port default vlan 120
[LSW4-GigabitEthernet0/0/1] quit

[LSW4] interface GigabitEthernet 0/0/2   // 配置连接 Boss 的接口为 Access 模式，加入 VLAN120
[LSW4-GigabitEthernet0/0/2] port link-type access
[LSW4-GigabitEthernet0/0/2] port default vlan 120
[LSW4-GigabitEthernet0/0/2] quit

[LSW4] interface GigabitEthernet 0/0/3  // 配置连接 LSW1 的接口为 Trunk 模式，允许 VLAN120
通过
[LSW4-GigabitEthernet0/0/3] port link-type trunk
[LSW4-GigabitEthernet0/0/3] port trunk allow-pass vlan 120
[LSW4-GigabitEthernet0/0/3] quit
```

3. 配置 LSW5：

[1]其中的 VLAN 66 是后来配置的，此处可忽略。

```
<HUAWEI> system-view
[HUAWEI] sysname LSW5
[LSW5] vlan batch 130   // 创建 VLAN130

[LSW5] interface GigabitEthernet 0/0/2   // 配置连接 DataServer 的接口为 Access 模式，加入 VLAN130
[LSW5-GigabitEthernet0/0/2] port link-type access
[LSW5-GigabitEthernet0/0/2] port default vlan 130
[LSW5-GigabitEthernet0/0/2] quit

[LSW5] interface GigabitEthernet 0/0/3   // 配置连接 AP1 的接口为 Access 模式，加入 VLAN130
[LSW5-GigabitEthernet0/0/3] port link-type access
[LSW5-GigabitEthernet0/0/3] port default vlan 130
[LSW5-GigabitEthernet0/0/3] quit

[LSW5] interface GigabitEthernet 0/0/4  // 配置连接 LSW2 的接口为 Trunk 模式，允许 VLAN130 通过
[LSW5-GigabitEthernet0/0/4] port link-type trunk
[LSW5-GigabitEthernet0/0/4] port trunk allow-pass vlan 130
[LSW5-GigabitEthernet0/0/4] quit
```

4.4 配置出口网关的基本功能

出口网关即为 AR1、AR2。在此步骤中，首先配置路由器使用链路聚合接口，核心交换机能够荣

1. 在 AR1 上创建 Eth-Trunk2，并加入成员接口。

```
[AR1] interface Eth-Trunk 2
[AR1-Eth-Trunk2] undo portswitch
[AR1-Eth-Trunk2] mode lacp-static
[AR1-Eth-Trunk2] quit
[AR1] interface GigabitEthernet 0/0/4
[AR1-GigabitEthernet0/0/4] Eth-Trunk 2
[AR1-GigabitEthernet0/0/4] quit
[AR1] interface GigabitEthernet 0/0/5
[AR1-GigabitEthernet0/0/5] Eth-Trunk 2
[AR1-GigabitEthernet0/0/5] quit
```

2. 在 AR1 上配置 Dot1q 终结子接口及 IP 地址，并终结 VLAN10。

```
[AR1] interface Eth-Trunk 2.100
[AR1-Eth-Trunk2.100] ip address 192.168.10.2 24
[AR1-Eth-Trunk2.100] dot1q termination vid 10
[AR1-Eth-Trunk2.100] quit
```

3. AR2 与 AR1 的配置几乎一模一样，仅有 IP 地址的设置不同。在 AR2 上创建 Eth-Trunk4，并加入成员接口。

```
[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
```

4. 在 AR2 上配置 Dot1q 终结子接口及 IP 地址，并终结 VLAN10。

```
[AR2] interface Eth-Trunk 2.100
[AR2-Eth-Trunk2.100] ip address 192.168.10.3 24
[AR2-Eth-Trunk2.100] dot1q termination vid 10
[AR2-Eth-Trunk2.100] quit
```

4.4.1 配置防火墙的基本功能

在此步骤中，首先配置防火墙使用链路聚合接口，然后配置接口的 IP 地址，最后根据接口划分安全区域。

1. 在 FW1 上配置接口与安全区域。

```
[FW1] interface Eth-Trunk 3   // 配置与 CORE 连接的接口及 IP 地址（外侧）
[FW1-Eth-Trunk3] ip address 192.168.20.2 24
[FW1-Eth-Trunk3] mode lacp-static
[FW1-Eth-Trunk3] quit
[FW1] interface GigabitEthernet 0/0/0   // 在 Eth-Trunk3 中加入成员接口
[FW1-GigabitEthernet0/0/0] Eth-Trunk 3
[FW1-GigabitEthernet0/0/0] quit
[FW1] interface GigabitEthernet 0/0/2   // 在 Eth-Trunk3 中加入成员接口
[FW1-GigabitEthernet0/0/2] Eth-Trunk 3
[FW1-GigabitEthernet0/0/2] quit

[FW1] interface Eth-Trunk 4   // 配置与 CORE 连接的接口及 IP 地址（内侧）
[FW1-Eth-Trunk4] ip address 192.168.30.2 24
[FW1-Eth-Trunk4] mode lacp-static
[FW1-Eth-Trunk4] quit
[FW1] interface GigabitEthernet 0/0/1   // 在 Eth-Trunk4 中加入成员接口
[FW1-GigabitEthernet0/0/1] Eth-Trunk 4
[FW1-GigabitEthernet0/0/1] quit
[FW1] interface GigabitEthernet 0/0/3   // 在 Eth-Trunk4 中加入成员接口
[FW1-GigabitEthernet0/0/3] Eth-Trunk 4
[FW1-GigabitEthernet0/0/3] quit

[FW1] interface Eth-Trunk 1   // 配置 FW1 与 FW2 连接的接口
[FW1-Eth-Trunk1] ip address 10.1.1.1 24
[FW1-Eth-Trunk1] mode lacp-static
[FW1-Eth-Trunk1] quit
[FW1] interface GigabitEthernet 0/0/4   // 在 Eth-Trunk1 中加入成员接口
[FW1-GigabitEthernet0/0/4] Eth-Trunk 1
[FW1-GigabitEthernet0/0/4] quit
[FW1] interface GigabitEthernet 0/0/5   // 在 Eth-Trunk1 中加入成员接口
[FW1-GigabitEthernet0/0/5] Eth-Trunk 1
[FW1-GigabitEthernet0/0/5] quit

[FW1] firewall zone trust
[FW1-zone-trust] add interface Eth-Trunk 4   // 将连接内网的 Eth-Trunk4 加入安全区域
[FW1-zone-trust] quit
```

```
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface Eth-Trunk 3   // 将连接外网的 Eth-Trunk3 加入非安全区域
[FW1-zone-untrust] quit

[FW1] firewall zone dmz
[FW1-zone-dmz] add interface Eth-Trunk 1   // 将 FW1 与 FW2 之间的接口加入 DMZ 区域
[FW1-zone-dmz] quit
```

2. 在 FW2 上配置接口与安全区域。

```
[FW2] interface Eth-Trunk 3   // 配置与 CORE 连接的接口及 IP 地址（外侧）
[FW2-Eth-Trunk3] ip address 192.168.20.3 24
[FW2-Eth-Trunk3] mode lacp-static
[FW2-Eth-Trunk3] quit
[FW2] interface GigabitEthernet 0/0/0   // 在 Eth-Trunk3 中加入成员接口
[FW2-GigabitEthernet0/0/0] Eth-Trunk 3
[FW2-GigabitEthernet0/0/0] quit
[FW2] interface GigabitEthernet 0/0/2   // 在 Eth-Trunk3 中加入成员接口
[FW2-GigabitEthernet0/0/2] Eth-Trunk 3
[FW2-GigabitEthernet0/0/2] quit

[FW2] interface Eth-Trunk 4   // 配置与 CORE 连接的接口及 IP 地址（内侧）
[FW2-Eth-Trunk4] ip address 192.168.30.3 24
[FW2-Eth-Trunk4] mode lacp-static
[FW2-Eth-Trunk4] quit
[FW2] interface GigabitEthernet 0/0/1   // 在 Eth-Trunk4 中加入成员接口
[FW2-GigabitEthernet0/0/1] Eth-Trunk 4
[FW2-GigabitEthernet0/0/1] quit
[FW2] interface GigabitEthernet 0/0/3   // 在 Eth-Trunk4 中加入成员接口
[FW2-GigabitEthernet0/0/3] Eth-Trunk 4
[FW2-GigabitEthernet0/0/3] quit

[FW2] interface Eth-Trunk 1   // 配置 FW2 与 FW1 连接的接口
[FW2-Eth-Trunk1] ip address 10.1.1.2 24
[FW2-Eth-Trunk1] mode lacp-static
[FW2-Eth-Trunk1] quit
[FW2] interface GigabitEthernet 0/0/4   // 在 Eth-Trunk1 中加入成员接口
[FW2-GigabitEthernet0/0/4] Eth-Trunk 1
[FW2-GigabitEthernet0/0/4] quit
[FW2] interface GigabitEthernet 0/0/5   // 在 Eth-Trunk1 中加入成员接口
[FW2-GigabitEthernet0/0/5] Eth-Trunk 1
[FW2-GigabitEthernet0/0/5] quit

[FW2] firewall zone trust
[FW2-zone-trust] add interface Eth-Trunk 4   // 将连接内网的 Eth-Trunk4 加入安全区域
[FW2-zone-trust] quit

[FW2] firewall zone untrust
[FW2-zone-untrust] add interface Eth-Trunk 3   // 将连接外网的 Eth-Trunk3 加入非安全区域
[FW2-zone-untrust] quit

[FW2] firewall zone dmz
[FW2-zone-dmz] add interface Eth-Trunk 1   // 将 FW2 与 FW1 之间的接口加入 DMZ 区域
[FW2-zone-dmz] quit
```

4.5 配置使内部网络互联互通

此处内网指与核心集群相连的重要设备，即 AR1、AR2、FW1、FW2。在此步骤中，需要配置核心集群与 AR1、AR2 的连接，使得核心集群能够连接路由器；其次还要配置核心集群上两个不互通的 VPN 实例与 FW1、FW2 的连接，使得两个 VPN 实例可以通过旁挂防火墙互通。

4.5.1 在路由器上部署 VRRP

在 AR1、AR2 上部署 VRRP，使得核心集群能够通过 VRRP 虚拟 IP 地址连接路由器。

- 配置 AR1：

```
[AR1] interface Eth-Trunk 2.100
[AR1-Eth-Trunk2.100] vrrp vrid 1 virtual-ip 192.168.10.100   //配置 VRRP 的虚拟 IP 地址
[AR1-Eth-Trunk2.100] vrrp vrid 1 priority 120   //提高 RouterA 的优先级，使其成为 Master
[AR1-Eth-Trunk2.100] quit
```

- 配置 AR2：

```
[AR2] interface Eth-Trunk 2.100
[AR2-Eth-Trunk2.100] vrrp vrid 1 virtual-ip 192.168.10.100   //配置 VRRP 的虚拟 IP 地址
[AR2-Eth-Trunk2.100] quit
```

4.5.2 配置 AR1 和 AR2 的路由

1. 在 AR1 上配置 OSPF。

```
[AR1] ospf 100 router-id 1.1.1.1
[AR1-ospf-100] area 0
[AR1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255    // 将连接 CORE 的网段发布到 OSPF 中
[AR1-ospf-100-area-0.0.0.0] quit
[AR1-ospf-100] quit
```

2. 在 AR2 上配置 OSPF。

```
[AR2] ospf 100 router-id 2.2.2.2
[AR2-ospf-100] area 0
[AR2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255    // 将连接 CORE 的网段发布到 OSPF 中
[AR2-ospf-100-area-0.0.0.0] quit
[AR2-ospf-100] quit
```

4.5.3 配置防火墙的路由

1. 在 FW1 上配置静态路由。

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 192.168.20.1    // 对于上行流量，缺省路由下一跳为 CORE 的 Public 接口 VLANIF20 的 IP 地址
[FW1] ip route-static 192.168.110.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN110 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
[FW1] ip route-static 192.168.120.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN120 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
[FW1] ip route-static 192.168.130.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN130 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
```

2. 在 FW2 上配置静态路由。

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 192.168.20.1    // 对于上行流量，缺省路由下一跳为 CORE 的 Public 接口 VLANIF20 的 IP 地址
[FW2] ip route-static 192.168.110.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN110 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
[FW2] ip route-static 192.168.120.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN120 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
[FW2] ip route-static 192.168.130.0 255.255.255.0 192.168.30.1   // 对于下行流量，目的地址为 VLAN130 网络，下一跳为 CORE 的 Private 接口 VLANIF30 的 IP 地址
```

4.5.4 配置核心集群的路由

核心集群上路由配置比较复杂，涉及到两个 VPN 实例，分别是 Public 和 Private。Public 用于连接路由器，Private 用于连接防火墙。在此步骤中，需要配置核心集群上的路由，使得核心集群能够连接路由器和防火墙。配置时需要仔细对照网络拓扑表，确保路由配置正确。

1. 在 CORE 上创建 VPN 实例 Public，将连接路由器的接口和连接防火墙上行口的接口绑定到 Public。

```
[CORE] ip vpn-instance Public   // 创建 Public
[CORE-vpn-instance-Public] ipv4-family
[CORE-vpn-instance-Public-af-ipv4] route-distinguisher 100:2
[CORE-vpn-instance-Public-af-ipv4] vpn-target 222:2 both
[CORE-vpn-instance-Public-af-ipv4] quit
[CORE-vpn-instance-Public] quit

[CORE] interface Vlanif 10
[CORE-Vlanif10] ip binding vpn-instance Public   // 将 CORE 连接路由器的接口 VLANIF10 绑定至 Public
[CORE-Vlanif10] ip address 192.168.10.1 24    // 将接口绑定到 Public 时，接口上的 IP 地址会被删除，需要重新配置 IP 地址
[CORE-Vlanif10] quit

[CORE] interface Vlanif 20
[CORE-Vlanif20] ip binding vpn-instance Public   // 将 CORE 连接防火墙上行口的接口 VLANIF20 绑定至 Public
[CORE-Vlanif20] ip address 192.168.20.1 24    // 将接口绑定到 Public 时，接口上的 IP 地址会被删除，需要重新配置 IP 地址
[CORE-Vlanif20] quit
```

2. 对于上行流量，在 Public 中配置静态路由，路由下一跳指向路由器 VRRP 虚拟 IP。

```
[CORE] ip route-static vpn-instance Public 0.0.0.0 0.0.0.0 192.168.10.100   // 缺省路由下一跳指向 VRRP 虚拟 IP
```

3. 对于下行流量，在 Public 中配置静态路由，路由下一跳指向防火墙上行 VRRP 1 的虚拟 IP（VRID1）。

```
[CORE] ip route-static vpn-instance Public 192.168.110.0 255.255.255.0 192.168.20.2  // 目的地址为 VLAN110 网络，下一跳指向 FW1 的上行接口
[CORE] ip route-static vpn-instance Public 192.168.120.0 255.255.255.0 192.168.20.2  //
```

```
目的地址为 VLAN120 网络，下一跳指向 FW1 的上行接口
[CORE] ip route-static vpn-instance Public 192.168.130.0 255.255.255.0 192.168.20.2  //
目的地址为 VLAN130 网络，下一跳指向 FW1 的上行接口
```

4. 对于下行流量，在 CORE 与 AR1、AR2 之间运行 OSPF 协议，用于 AR1、AR2 学习到业务网段的回程路由信息。

```
[CORE] ospf 100 router-id 1.1.1.1 vpn-instance Public
[CORE-ospf-100] area 0
[CORE-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255    // 将连接 AR1、AR2 的网
段发布到 OSPF 中
[CORE-ospf-100-area-0.0.0.0] quit
[CORE-ospf-100] import-route static       // 在 OSPF 中引入静态路由
[CORE-ospf-100] quit
```

5. 对于上行流量，在 CORE 上创建 VPN 实例 Private，将连接业务网络的接口和连接防火墙下行的接口绑定到 Private，Private 的缺省路由下一跳指向防火墙下行 VRRP 虚拟 IP（VRID2）。

```
[CORE] ip vpn-instance Private   // 创建 Private
[CORE-vpn-instance-Private] ipv4-family
[CORE-vpn-instance-Private-af-ipv4] route-distinguisher 100:1
[CORE-vpn-instance-Private-af-ipv4] vpn-target 111:1 both
[CORE-vpn-instance-Private-af-ipv4] quit
[CORE-vpn-instance-Private] quit

[CORE] interface Vlanif 110
[CORE-Vlanif110] ip binding vpn-instance Private    // 将 CORE 连接 VLAN110 的接口
VLANIF110 绑定至 Private
[CORE-Vlanif110] ip address 192.168.110.1 24    // 将接口绑定到 Private 时，接口上的 IP
地址会被删除，需要重新配置 IP 地址
[CORE-Vlanif110] quit

[CORE] interface Vlanif 120
[CORE-Vlanif120] ip binding vpn-instance Private    // 将 CORE 连接 VLAN120 的接口
VLANIF120 绑定至 Private
[CORE-Vlanif120] ip address 192.168.120.1 24    // 将接口绑定到 Private 时，接口上的 IP
地址会被删除，需要重新配置 IP 地址
[CORE-Vlanif120] quit

[CORE] interface Vlanif 130
[CORE-Vlanif130] ip binding vpn-instance Private    // 将 CORE 连接 VLAN130 的接口
VLANIF130 绑定至 Private
[CORE-Vlanif130] ip address 192.168.130.1 24    // 将接口绑定到 Private 时，接口上的 IP
地址会被删除，需要重新配置 IP 地址
[CORE-Vlanif130] quit

[CORE] interface Vlanif 30
[CORE-Vlanif30] ip binding vpn-instance Private  // 将 CORE 连接防火墙下行的接口 VLANIF30
绑定至 Private
[CORE-Vlanif30] ip address 192.168.30.1 24    // 将接口绑定到 Private 时，接口上的 IP 地
址会被删除，需要重新配置 IP 地址
[CORE-Vlanif30] quit
```

6. 在 Private 中配置缺省路由，下一跳指向防火墙下行 VRRP 2 的虚拟 IP（VRID2）。

```
[CORE] ip route-static vpn-instance Private 0.0.0.0 0.0.0.0 192.168.30.2   // 缺省路由下一跳指向 FW1 的下行接口
```

4.6 阶段性检验

上面的配置完成后，进行一个阶段性检验。配置 PC1 的 IP 地址为 `192.168.110.10/24`，网关为核心集群上 VPN 实例 Private 内的 Vlanif110 接口地址 `192.168.110.1`，然后 ping AR1、AR2 的 VRRP 虚拟 IP 地址 `192.168.10.100`，是可以通的，如图 Figure 5。如果不能，则逐级 ping，查找问题所在。

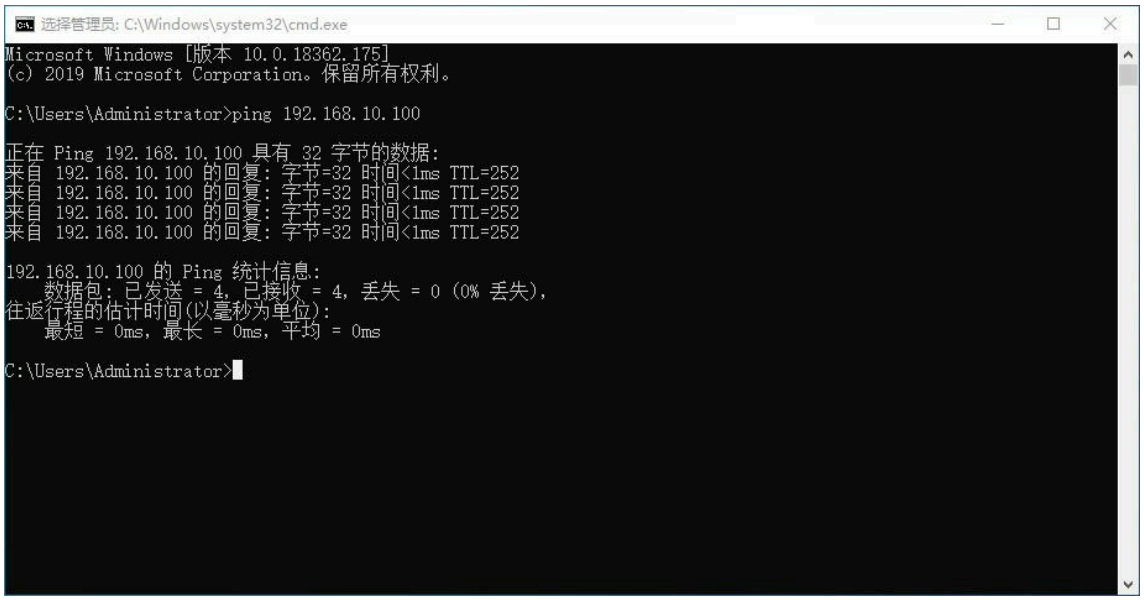


Figure 5: 阶段性检验 1

4.7 配置其他功能

4.7.1 配置出口网关的 BFD 功能

配置 AR1 和 AR2 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。

```
[AR1] bfd   // 配置全局 BFD 功能并进入全局 BFD 视图
[AR1-bfd] quit
```

```
[AR2] bfd   // 配置全局 BFD 功能并进入全局 BFD 视图
[AR2-bfd] quit
```

2. 在 AR1 上配置 OSPF 的 BFD 特性。

```
[AR1] ospf 100   // 进入 OSPF 视图
[AR1-ospf-100] bfd all-interfaces enable   // 打开 OSPF BFD 特性的开关，建立 BFD 会话
[AR1-ospf-100] quit
```

3. 在 AR2 上配置 OSPF 的 BFD 特性。

```
[AR2] ospf 100   // 进入 OSPF 视图
[AR2-ospf-100] bfd all-interfaces enable   // 打开 OSPF BFD 特性的开关，建立 BFD 会话
[AR2-ospf-100] quit
```

4. 配置 BFD 参数。

```
[AR1-ospf-100] bfd all-interfaces min-rx-interval 1000 min-tx-interval 1000 detect-
multiplier 3
[AR2-ospf-100] bfd all-interfaces min-rx-interval 1000 min-tx-interval 1000 detect-
multiplier 3
```

5. 验证 BFD 会话。

```
[AR1] display ospf bfd session all
[AR2] display ospf bfd session all
```

该命令在 AR1 上得到以下输出：

```
[AR1]disp ospf bfd session all

        OSPF Process 100 with Router ID 2.2.2.2
  Area 0.0.0.0 interface 192.168.10.3(Eth-Trunk2.100)'s BFD Sessions

NeighborId:1.1.1.1          AreaId:0.0.0.0          Interface:Eth-Trunk2.100
BFDState:up                 rx    :1000             tx       :1000
Multiplier:3                BFD Local Dis:8198      LocalIpAdd:192.168.10.3
RemoteIpAdd:192.168.10.1    Diagnostic Info:No diagnostic information

NeighborId:3.3.3.3          AreaId:0.0.0.0          Interface:Eth-Trunk2.100
BFDState:up                 rx    :1000             tx       :1000
Multiplier:3                BFD Local Dis:8197      LocalIpAdd:192.168.10.3
RemoteIpAdd:192.168.10.2    Diagnostic Info:No diagnostic information
```

注意其中的`BFDStat`字段，显示为`up`，表示 BFD 会话建立成功。

4.7.2 配置防火墙的双机热备

在防火墙上配置双机热备功能（主备备份模式），确保高可用性。FW1 作为 Master，FW2 作为 Slave。

1. 在 FW1 上配置双机热备，FW1 在备份组中作为 Master。

```
[FW1] interface Eth-Trunk 3
[FW1-Eth-Trunk3] vrrp vrid 1 virtual-ip 192.168.20.2 24 active
[FW1-Eth-Trunk3] quit
[FW1] interface Eth-Trunk 4
[FW1-Eth-Trunk4] vrrp vrid 2 virtual-ip 192.168.30.2 24 active
[FW1-Eth-Trunk4] quit
[FW1] hrp interface Eth-Trunk 1 remote 10.1.1.2   // 配置心跳口，并启用双机热备
[FW1] hrp enable
```

2. 在 FW2 上配置双机热备，FW2 在备份组中作为 Slave。

```
[FW2] interface Eth-Trunk 3
[FW2-Eth-Trunk3] vrrp vrid 1 virtual-ip 192.168.20.2 24 standby
[FW2-Eth-Trunk3] quit
[FW2] interface Eth-Trunk 4
[FW2-Eth-Trunk4] vrrp vrid 2 virtual-ip 192.168.30.2 24 standby
[FW2-Eth-Trunk4] quit
[FW2] hrp interface Eth-Trunk 1 remote 10.1.1.1   // 配置心跳口，并启用双机热备
[FW2] hrp enable
```

配置好之后，保存配置，将两台设备全部断电关机。按照 FW1 先、FW2 后的顺序开机（防火墙开机较久，约 5 分钟，可通过风扇声音判断，声音突然由大变小表示开机完成），应该可以观察到防火墙 Web 主页中的主备状态：

Figure 6: 防火墙双机热备（主，FW1）

Figure 7: 防火墙双机热备（备，FW2）

4.7.3 配置 DHCP 服务器

DHCP 服务器一般配置在接入层上，但本实验拓扑图较为简单，所以在核心集群上配置 DHCP 服务器，为 VLANIF110 和 VLANIF120 接口下的客户端分配 IP 地址和相关网络参数。

1. 配置 VLANIF110 接口的 DHCP 地址池
   - 配置 VLANIF110 接口下的客户端从接口地址池中获取 IP 地址和相关网络参数。

```
[CORE] interface vlanif 110
[CORE-Vlanif110] dhcp select interface
[CORE-Vlanif110] dhcp server gateway-list 192.168.110.1
[CORE-Vlanif110] dhcp server lease day 30
```

```
[CORE-Vlanif110] dhcp server dns-list 192.168.130.10  //内网中的 DNS 服务器地址
[CORE-Vlanif110] quit
```

2. 配置 VLANIF120 接口的 DHCP 地址池
   - 配置 VLANIF120 接口下的客户端从接口地址池中获取 IP 地址和相关网络参数。

```
[CORE] interface vlanif 120
[CORE-Vlanif120] dhcp select interface
[CORE-Vlanif120] dhcp server gateway-list 192.168.120.1
[CORE-Vlanif120] dhcp server lease day 60 // 老板一般会当得比员工久
[CORE-Vlanif120] dhcp server dns-list 192.168.130.10
[CORE-Vlanif120] quit
```

配置完成之后，配置 PC1、PC2 为自动获取 IP 地址的方式（还可配置自动获取 DNS 地址），查看 DHCP 地址池信息：

- 使用 `display ip pool` 命令查看 DHCP 地址池的配置和状态。

```
[CORE] display ip pool
------------------------------------------------------------------------------
  Pool-name        : Vlanif110
  Pool-No          : 0
  Lease            : 1 Days 0 Hours 0 Minutes
  Position         : Interface
  Status           : Unlocked
  Gateway-0        : 192.168.110.1
  Network          : 192.168.110.0
  Mask             : 255.255.255.0
  VPN instance     : Private
  Conflicted address recycle interval: -
  Address Statistic: Total       :253       Used        :2
                     Idle        :251       Expired     :0
                     Conflict    :0         Disabled    :0
```

注意到 `Used` 字段中变成 2。此时在任一台机器上查看 IP 地址和 DNS 地址，可以看到被分配的地址： `figure`

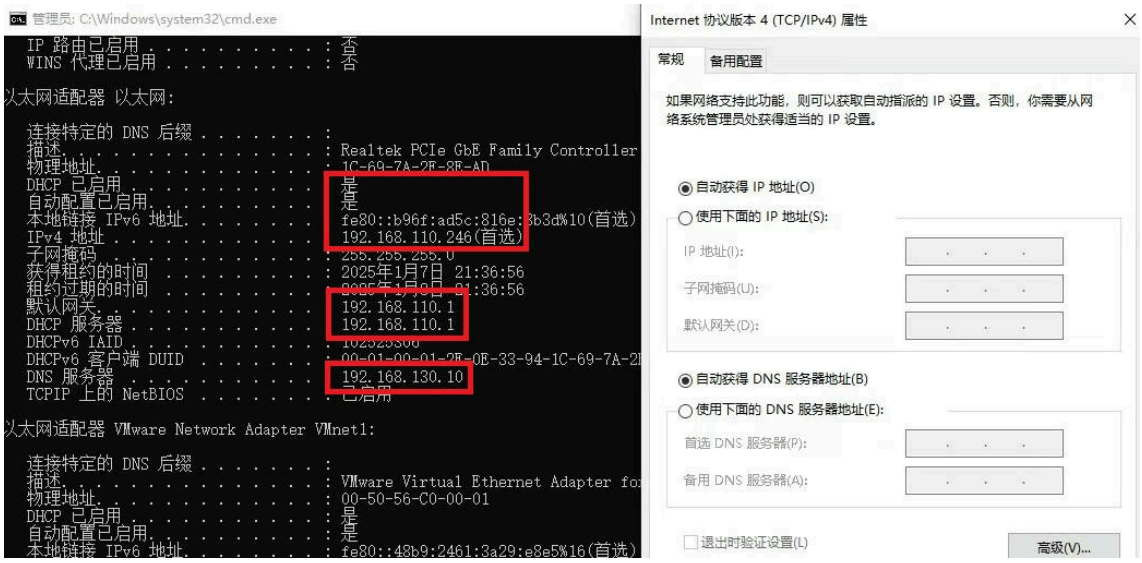


Figure 8: PC1 自动获取 IP 地址和 DNS 服务器地址

4.7.4 配置 STP 以消除网络中的环路

逻辑拓扑图 Figure 2 有更完整的版本:

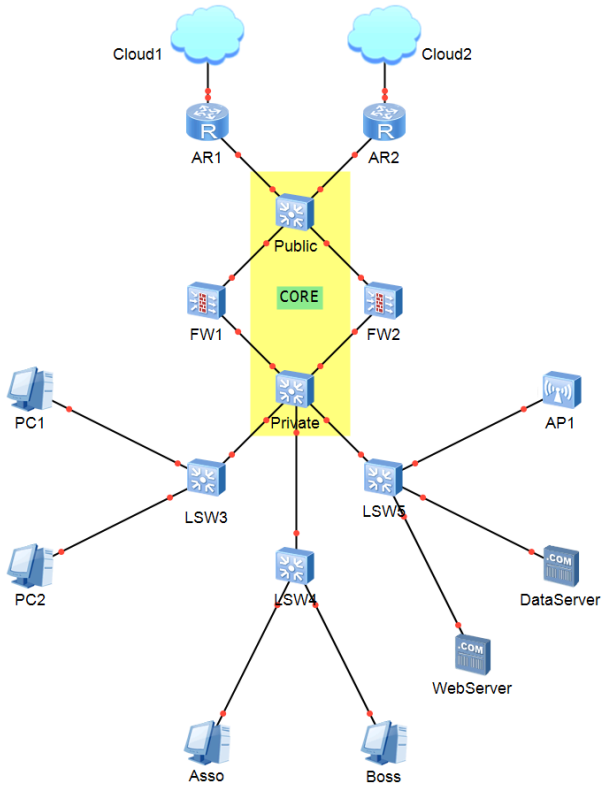


Figure 9: 逻辑拓扑图（完整）

分析逻辑拓扑图，发现此网络基本呈树形，有且仅有核心集群与 FW1、FW2 之间组成的环。因此，只需要在核心集群、防火墙上配置 STP，就可以消除网络中的环路，不需要 RSTP、MSTP 等较复杂的协议。具体来说，以阻塞 FW2 连接 Private 的端口 Eth4 为目的，配置 STP 协议。

1. 在 CORE 上启用 STP 并配置优先级。

```
[CORE] stp enable   // 启用 STP 协议
[CORE] stp mode stp   // 配置 STP 模式为标准 STP
[CORE] stp priority 0   // 设置 CORE 的 STP 优先级为 0（确保 CORE 成为根桥）
[CORE] quit
```

2. 在 FW1 上启用 STP 并配置优先级。

```
[FW1] stp enable   // 启用 STP 协议
[FW1] stp mode stp   // 配置 STP 模式为标准 STP
[FW1] stp priority 4096   // 设置 FW1 的 STP 优先级为 4096
[FW1] quit
```

3. 在 FW2 上启用 STP 并配置优先级。

```
[FW2] stp enable   // 启用 STP 协议
[FW2] stp mode stp   // 配置 STP 模式为标准 STP
[FW2] stp priority 8192   // 设置 FW2 的 STP 优先级为 8192
[FW2] quit
```

4. 在 FW2 上阻塞指定端口

```
[FW2] interface Eth-Trunk 4
[FW2-Eth-Trunk4] stp disable   // 禁用 STP 以阻塞 Eth4 端口
[FW2-Eth-Trunk4] quit
```

4.7.5 为出口网关配置 NAT

由于内网用户有上网需求，所以需要进行地址转换。这一步骤在 AR1 和 AR2 上配置 NAT 功能，包括地址池、ACL、静态映射以及 FTP ALG 功能。

1. 配置地址池和 ACL
   - 在 AR1 上配置地址池：

     ```
     [AR1] nat address-group 1 172.163.1.10 172.163.1.252
     ```

   - 在 AR2 上配置地址池：

     ```
     [AR2] nat address-group 1 172.163.3.10 172.163.3.252
     ```

   - 在 AR1 和 AR2 上创建 ACL，匹配需要上网的内网段：

     ```
     [AR1] acl 2000
     [AR1-acl-basic-2000] rule permit source 192.168.110.0 0.0.0.255
     [AR1-acl-basic-2000] rule permit source 192.168.120.0 0.0.0.255
     [AR1-acl-basic-2000] quit
     ```

     ```
     [AR2] acl 2000
     [AR2-acl-basic-2000] rule permit source 192.168.110.0 0.0.0.255
     [AR2-acl-basic-2000] rule permit source 192.168.120.0 0.0.0.255
     [AR2-acl-basic-2000] quit
     ```

   - 在 AR1 和 AR2 的路由出口引用 ACL 2000，使匹配的网段中的地址可以使用地址池中的地址进行 NAT 转换：

     ```
     [AR1] int g0/0/2
     [AR1-GigabitEthernet0/0/2] nat outbound 2000 address-group 1 no-pat
     [AR1-GigabitEthernet0/0/2] quit
     ```

     ```
     [AR2] int g0/0/3
     [AR2-GigabitEthernet0/0/3] nat outbound 2000 address-group 1 no-pat
     [AR2-GigabitEthernet0/0/3] quit
     ```

2. 配置 NAT 静态映射
   - 在 AR1 上配置 NAT 静态映射，实现外网用户通过预留的公网 IP 地址 172.163.1.9 访问内部 FTP/Web 服务器：

     ```
     ```

```
[AR1] int g0/0/2
[AR1-GigabitEthernet0/0/2] nat static protocol tcp global 172.163.1.9 21 inside
192.168.130.10 21
[AR1-GigabitEthernet0/0/2] nat static protocol tcp global 172.163.1.9 80 inside
192.168.130.10 80
[AR1-GigabitEthernet0/0/2] quit
```

- 在 AR2 上配置 NAT 静态映射，实现外网用户通过预留的公网 IP 地址 172.163.3.9 访问内部 FTP/Web 服务器：

```
[AR2] int g0/0/3
[AR2-GigabitEthernet0/0/3] nat static protocol tcp global 172.163.3.9 21 inside
192.168.130.10 21
[AR2-GigabitEthernet0/0/3] nat static protocol tcp global 172.163.3.9 80 inside
192.168.130.10 80
[AR2-GigabitEthernet0/0/3] quit
```

3. 开启 FTP 的 NAT ALG 功能

```
[AR1] nat alg ftp enable
```

```
[AR2] nat alg ftp enable
```

4. 查看 NAT 转换和静态映射的结果

4. 在 AR1 和 AR2 上查看 NAT 转换和静态映射的结果：

```
[AR1] display nat address-group 1
[AR1] display nat static
```

```
[AR2] display nat address-group 1
[AR2] display nat static
```

结果如 Figure 10 和 Figure 11 所示（见下页）：

```
[AR1]disp nat address-group 1
 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
 1       172.163.1.10    172.163.1.252
 --------------------------------------
  Total : 1
[AR1]display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------------
 Interface                       Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------------
 GigabitEthernet0/0/2         2000                                1    no-pat
 --------------------------------------------------------------------------------

  Total : 1
[AR1]disp nat static
  Static Nat Information:
  Interface  : GigabitEthernet0/0/2
    Global IP/Port     : 172.163.1.9/21(ftp)
    Inside IP/Port     : 192.168.130.10/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

    Global IP/Port     : 172.163.1.9/80(www)
    Inside IP/Port     : 192.168.130.10/80(www)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    2
[AR1]
```

Figure 10: AR1 NAT 配置结果


```
[AR1]disp nat address-group 1
 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
 1       172.163.1.10    172.163.1.252
 --------------------------------------
  Total : 1
[AR1]display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------------
 Interface                       Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------------
 GigabitEthernet0/0/2         2000                                1    no-pat
 --------------------------------------------------------------------------------

  Total : 1
[AR1]disp nat static
  Static Nat Information:
  Interface  : GigabitEthernet0/0/2
    Global IP/Port     : 172.163.1.9/21(ftp)
    Inside IP/Port     : 192.168.130.10/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

    Global IP/Port     : 172.163.1.9/80(www)
    Inside IP/Port     : 192.168.130.10/80(www)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    2
[AR1]
```


Figure 11: AR1 NAT 配置结果

4.7.6 防火墙的工作时间段切换

公司规定员工办公室工作时间内不能访问外网。因此，需要在防火墙上配置对应的安全策略，即工作时间段内`trust`不能访问`untrust`区域，策略配置如下：

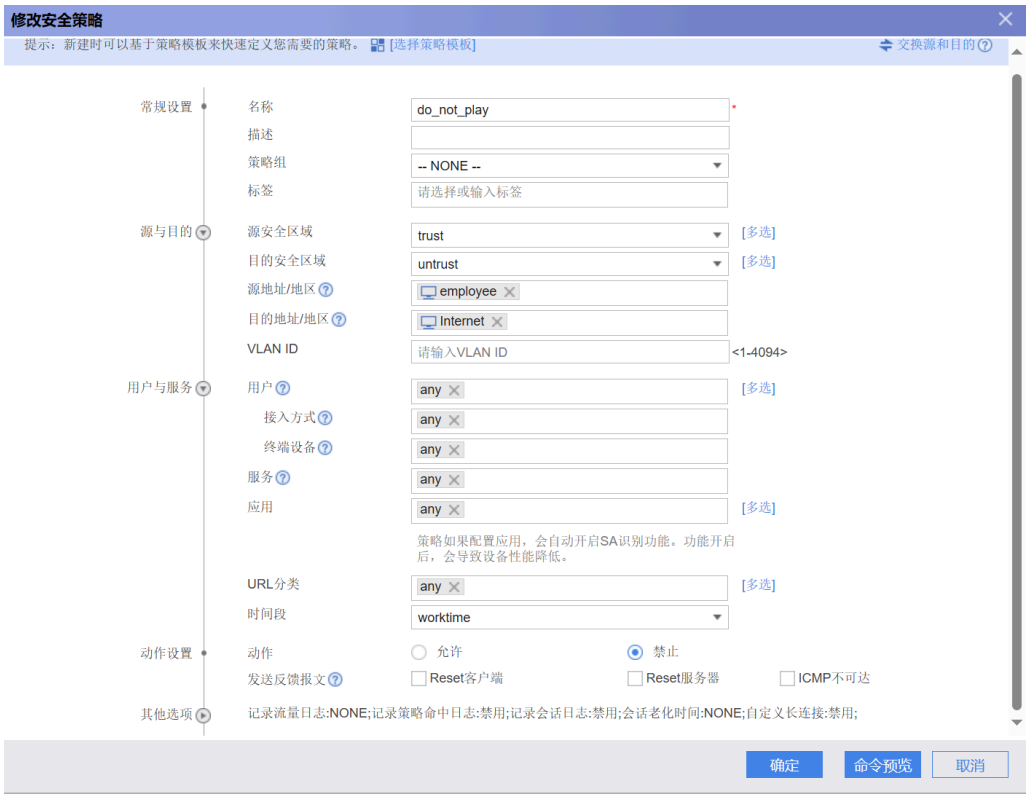


Figure 12: 配置非工作时间段内不能访问外网

4.7.7 配置端口安全

在 LSW4 上为连接到 Boss 设备的接口配置端口安全，以确保只有特定的 MAC 地址可以访问该端口。

1. 进入连接到 Boss 设备的接口配置模式。

```
[LSW4] interface GigabitEthernet0/0/2
```

2. 启用端口安全功能。

```
[LSW4-GigabitEthernet0/0/2] port-security enable
```

3. 配置粘性 MAC 地址，以便动态学习并绑定第一个连接到该端口的设备的 MAC 地址。

```
[LSW4-GigabitEthernet0/0/2] port-security mac-address sticky
```

4. 设置该端口允许的最大 MAC 地址数量为 1，确保只有一个设备可以连接到该端口。

```
[LSW4-GigabitEthernet0/0/2] port-security max-mac-num 1
```

]

4.7.8 配置 Web 服务器与 DNS 服务器

在个人笔记本电脑上配置服务器。选择 Apache24 作为 Web 服务器，选择 BIND 9 作为 DNS 服务器。Apache 的配置十分简单，而 BIND 的具体配置十分复杂，不是重点，在此不再展开。

4.7.9 配置无线路由器

初始化 AP，然后以无线网络连接到它的配置界面`tplogin.cn`（TP-Link AX3000）。随后，选择桥接模式即可。

理论成立，但实际不可行。经测试，此 AP 在选取桥接模式后，也无法真正地担任交换机的功能（两个连接同网段设备的端口间互 ping 不通）。推测在工程环境下只能作为路由器使用。而拓扑图中已经没有多余的路由器位置。即使有，也不具有适合此 AP 的功能性。所以不再继续配置此 AP。

4.8 实验后验收

检查以下项目来验证整个网络的功能：

1. 内网主机能够通过 DHCP 获取到 IP 地址；先前已验证
2. 内网主机之间可以互相通信；
3. 内网主机可以通过 IP 地址访问 Web 服务器；
4. 内网主机可以通过域名访问 Web 服务器；
5. 外网主机可以通过外网地址访问内网 Web 服务器；
6. 内网主机可以访问外网；
7. 检验防火墙安全策略；
8. 防火墙主备备份；先前已验证
9. 检验出口网关双机热备份/BFD（快速切换）；
10. 检验端口安全；

其中，第一项与第八项先前已经验证生效，后续不再专门验收。

4.8.1 内网通信

检查内网主机之间是否可以互相 ping 通。这里以 PC1 和 Boss、PC2 和 Asso 通信为例：

Figure 13: PC1 ping 通 Boss

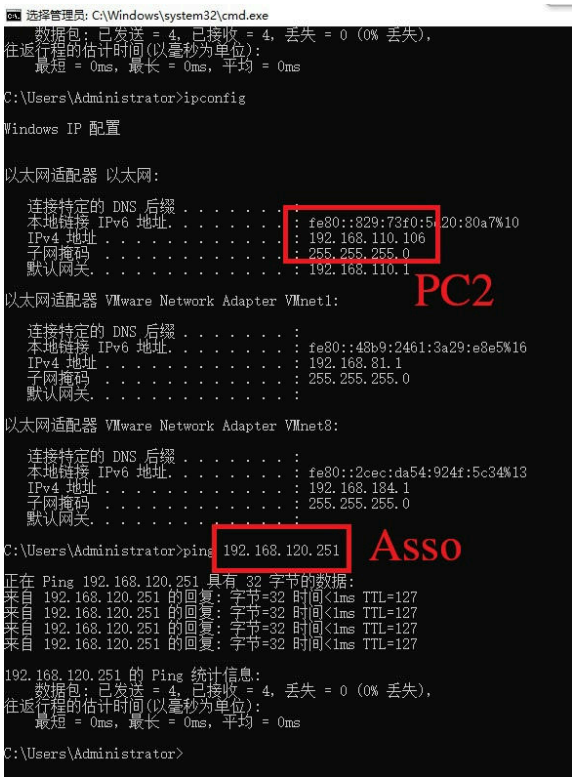


Figure 14: PC2 ping 通 Asso

4.8.2 内网访问 Web 服务器

使用主机 Asso，经由 IP 地址 192.168.130.10 访问 Web 服务器：

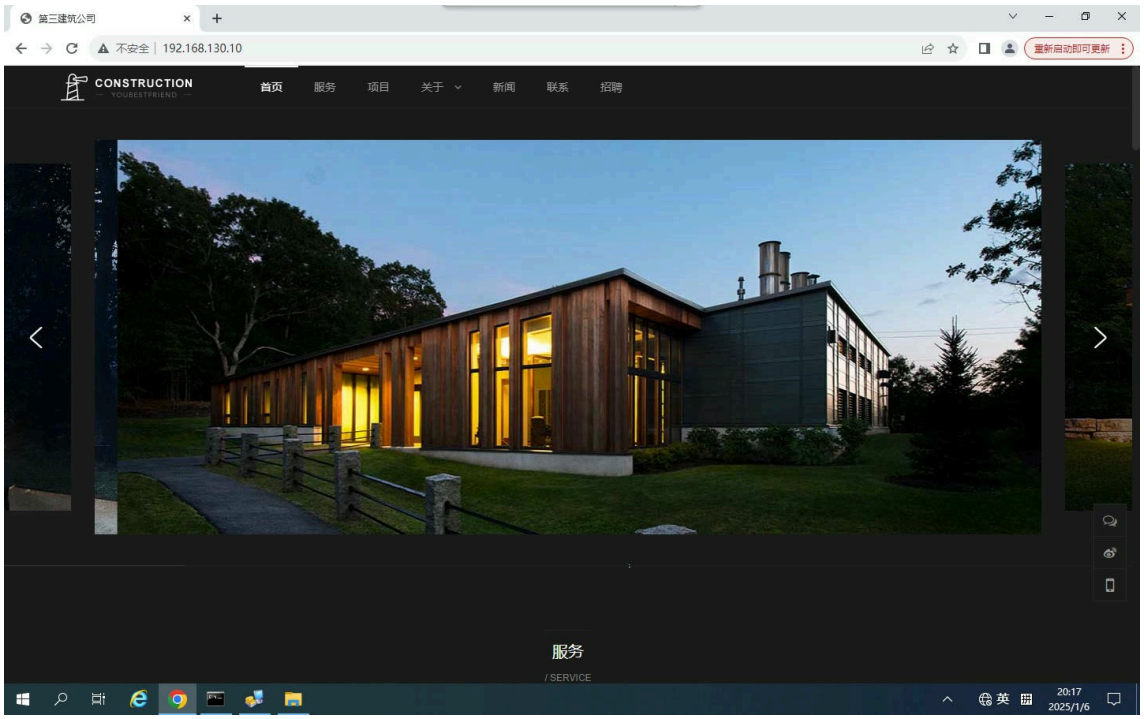


Figure 15: Asso 通过 IP 访问 Web 服务器

通过域名 www.construction.com 访问服务器：

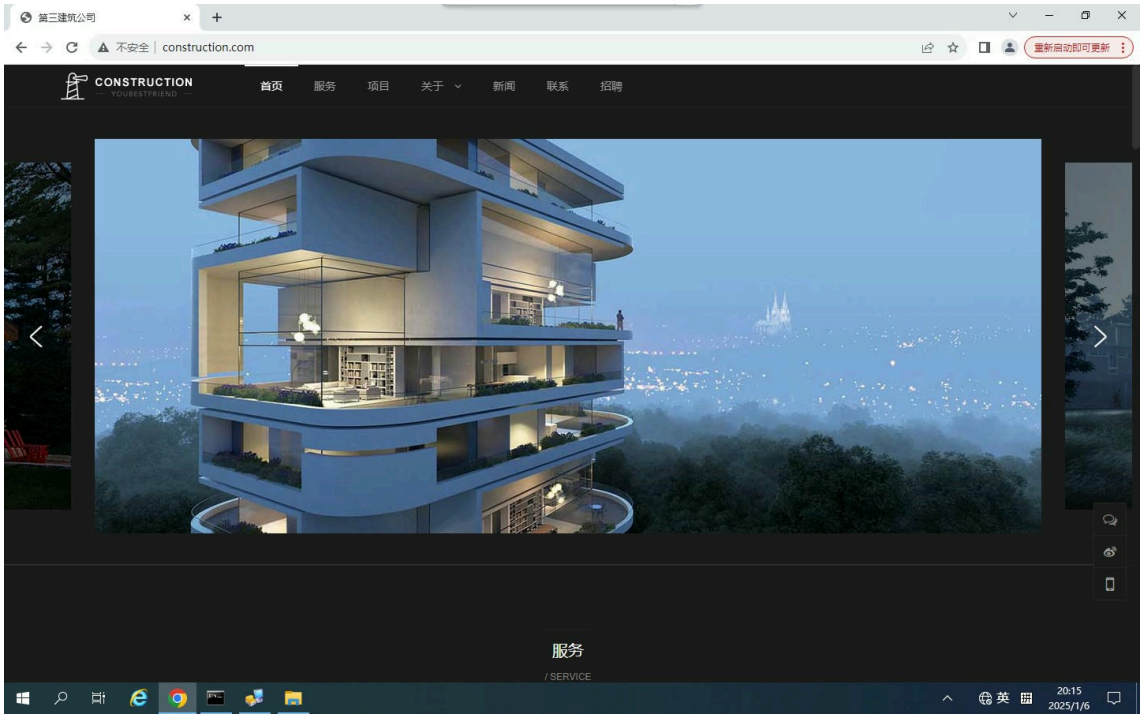


Figure 16: Asso 通过访问 Web 服务器

4.8.3 外网访问 Web 服务器

使用外网主机（地址为`172.163.5.1`），通过服务器的公网 IP 访问服务器：

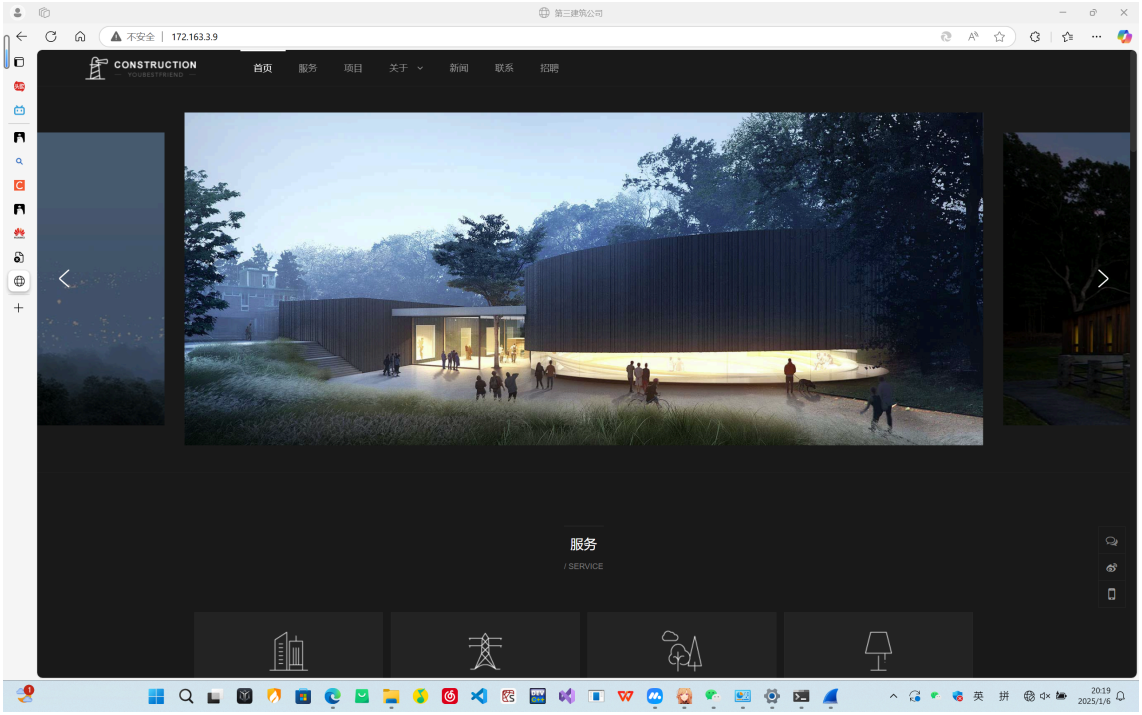


Figure 17: Asso 通过访问 Web 服务器

这还可以说明防火墙有关内外网之间的区域限制策略设置无误，即 Untrust 区域可以访问 DMZ 区域，DMZ 区域也可以访问 Untrust 区域。

4.8.4 内外网访问系列验证、NAT 验证与出口网关 BFD 验证

使用内网主机 PC1 对外网主机进行长 ping，然后再外网主机上开启抓包。途中，使用 `shutdown` 命令断开 AR1 与 CORE 的连接。在 PC1 上观察长 ping 是否断开，在外网主机上观察抓包结果中，源地址是否是经过 NAT 的转换，以及时间序列上相差多少。

运行过程如下：

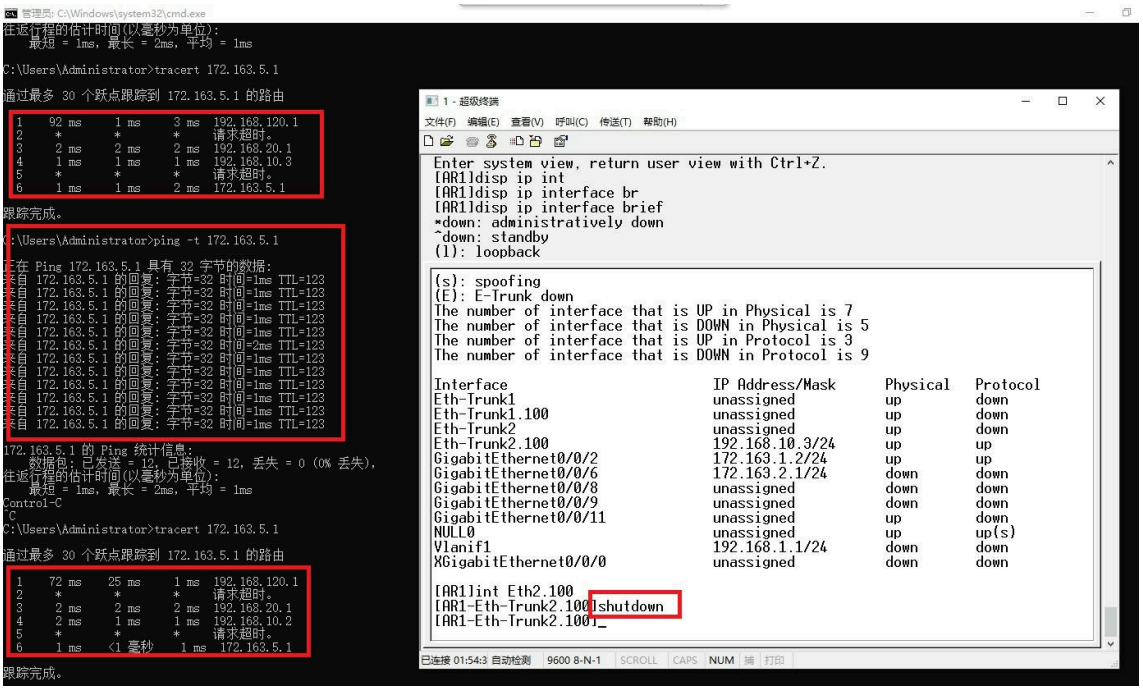
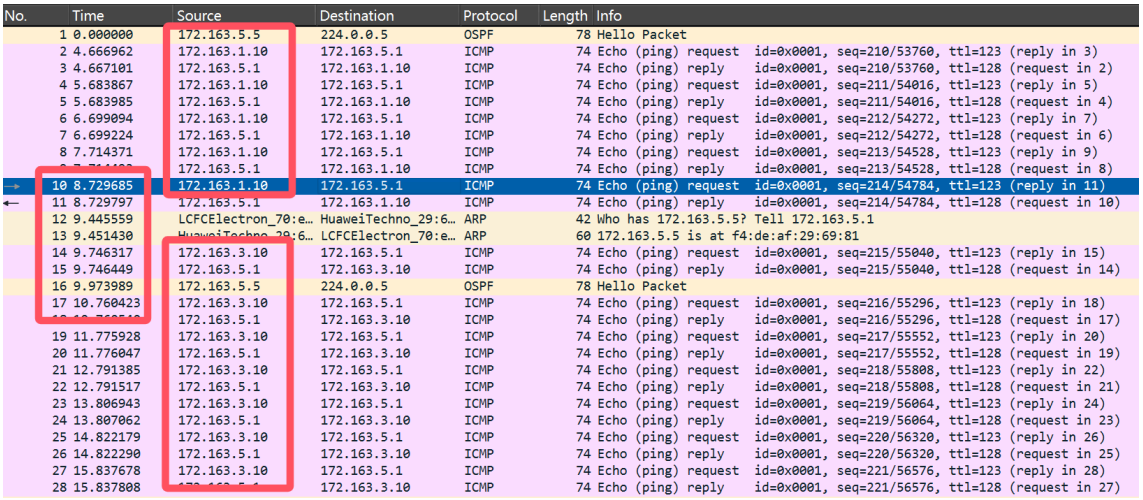


Figure 18: 长 ping 不断

从 Figure 18 中可以观察到：

- 长 ping 没有断开；
- `shutdown` 端口之前，`tracert` 命令返回的路径经过了 AR1，即 `192.168.10.3`；
- `shutdown` 端口之前，`tracert` 命令返回的路径变为经过 AR2，即 `192.168.10.2`。

进一步分析需要查看抓包结果。抓包结果如下：



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.163.5.5	224.0.0.5	OSPF	78	Hello Packet
2	4.666962	172.163.1.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=210/53760, ttl=123 (reply in 3)
3	4.667101	172.163.5.1	172.163.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=210/53760, ttl=128 (request in 2)
4	5.683867	172.163.1.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=211/54016, ttl=123 (reply in 5)
5	5.683985	172.163.5.1	172.163.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=211/54016, ttl=128 (request in 4)
6	6.699094	172.163.1.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=212/54272, ttl=123 (reply in 7)
7	6.699224	172.163.5.1	172.163.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=212/54272, ttl=128 (request in 6)
8	7.714371	172.163.1.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=213/54528, ttl=123 (reply in 9)
[illegible]	[illegible]	172.163.5.1	172.163.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=213/54528, ttl=128 (request in 8)
10	8.729685	172.163.1.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=214/54784, ttl=123 (reply in 11)
11	8.729797	172.163.5.1	172.163.1.10	ICMP	74	Echo (ping) reply id=0x0001, seq=214/54784, ttl=128 (request in 10)
12	9.445559	LCFCElectron_70:e…	HuaweiTechno_29:6…	ARP	42	Who has 172.163.5.5? Tell 172.163.5.1
13	9.451430	HuaweiTechno_29:6…	LCFCElectron_70:e…	ARP	60	172.163.5.5 is at f4:de:af:29:69:81
14	9.746317	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=215/55040, ttl=123 (reply in 15)
15	9.746449	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=215/55040, ttl=128 (request in 14)
16	9.973989	172.163.5.5	224.0.0.5	OSPF	78	Hello Packet
17	10.760423	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=216/55296, ttl=123 (reply in 18)
[illegible]	[illegible]	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=216/55296, ttl=128 (request in 17)
19	11.775928	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=217/55552, ttl=123 (reply in 20)
20	11.776047	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=217/55552, ttl=128 (request in 19)
21	12.791385	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=218/55808, ttl=123 (reply in 22)
22	12.791517	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=218/55808, ttl=128 (request in 21)
23	13.806943	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=219/56064, ttl=123 (reply in 24)
24	13.807062	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=219/56064, ttl=128 (request in 23)
25	14.822179	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=220/56320, ttl=123 (reply in 26)
26	14.822290	172.163.5.1	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=220/56320, ttl=128 (request in 25)
27	15.837678	172.163.3.10	172.163.5.1	ICMP	74	Echo (ping) request id=0x0001, seq=221/56576, ttl=123 (reply in 28)
28	15.837808	[illegible]	172.163.3.10	ICMP	74	Echo (ping) reply id=0x0001, seq=221/56576, ttl=128 (request in 27)

Figure 19: 长 ping 不断

观察 Figure 19，靠上方红框内的源地址均为 `172.163.1.10`，即 AR1 经过 NAT 转换后的外网网关地址，这说明 AR1 上的 NAT 生效；在第 8 到 9 秒之间，外网主机捕获到一个 ARP 报文，询问它的 IP 地址，这可能是 AR2 从备份状态变为了工作状态，发出 ARP 询问。随后的第 9.7s，内网主机的下一个 ping 报文到来。由于此次报文到达与上次到达间隔仅为 1s，恰好是 ping 程

序发送请求的时间间隔，由此可见 PC1 上的长 ping 丝毫没有受到影响。在这之后，ping 的源地址均为`172.163.3.10`，即 AR2 经过 NAT 转换后的外网网关地址，这说明 AR2 上的 NAT 生效。

凭此抓包结果即可验证数个配置项目。

4.8.5 防火墙安全策略系列验证

此处主要验证几条“禁止”的防火墙策略。

1. 验证非工作时间段职员办公室（PC1、PC2）无法访问外网

以 PC1 为例。验证这条策略，需要查看工作时间、非工作时间下，PC1 是否能 ping 通外网主机。

首先，在工作时间下，查看防火墙策略的命中次数：

Figure 20: 防火墙工作时段

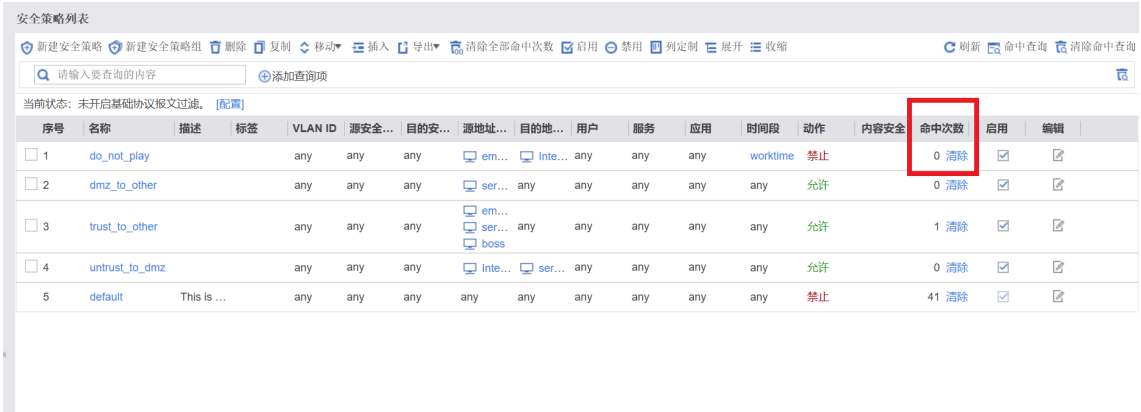


Figure 21: 防火墙工作时段策略命中次数截图（ping 前）

然后用 PC1 ping 外网，发现能够 ping 通。观察策略命中次数：

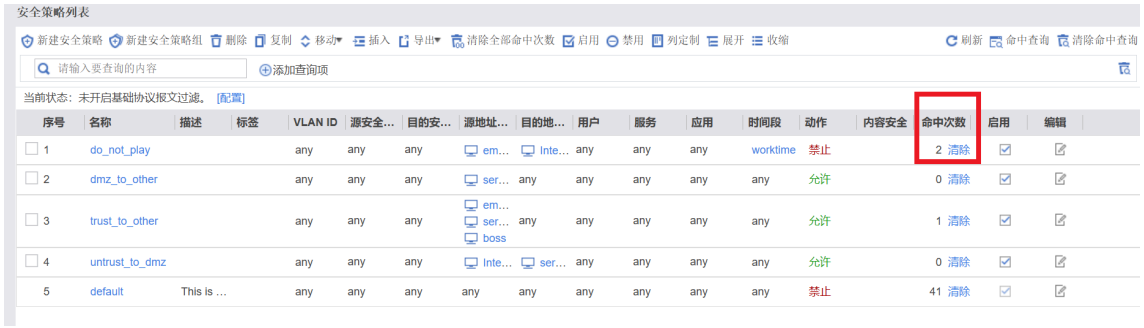


Figure 22: 防火墙工作时段策略命中次数截图（ping 后）

注意到命中次数增加。

首先，在非工作时间下，查看防火墙策略的命中次数：

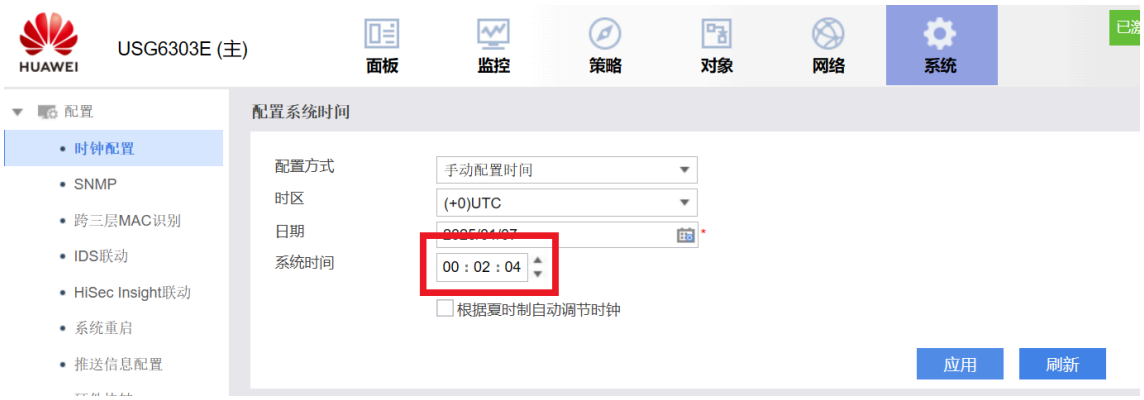


Figure 23: 防火墙非工作时段

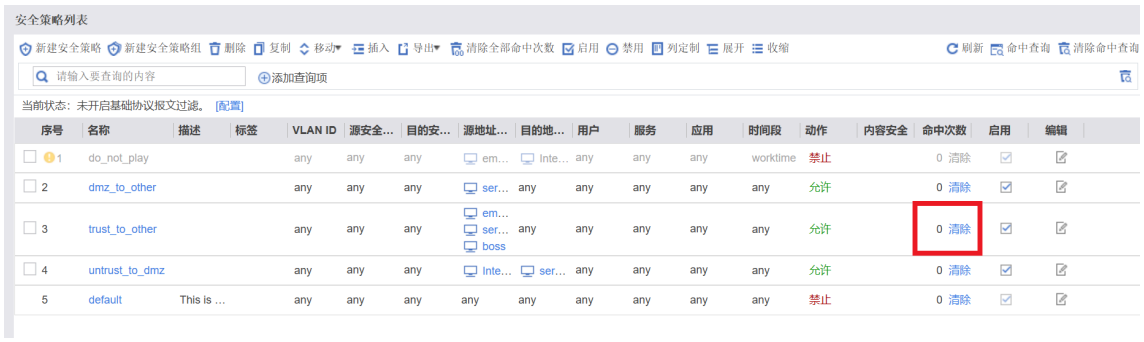


Figure 24: 防火墙非工作时段策略命中次数截图（ping 前）

然后用 PC1 ping 外网，发现能够 ping 通。观察策略命中次数：

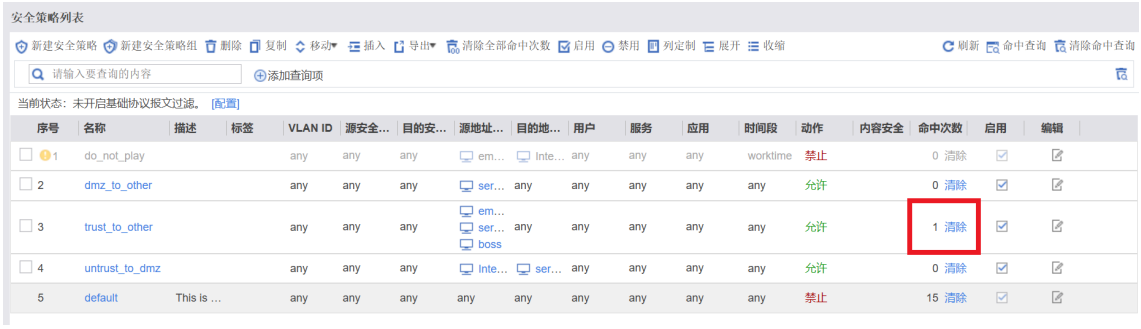


Figure 25: 防火墙非工作时段策略命中次数截图（ping 后）

注意到命中次数增加。

2. 验证外网 ping 不通内网 trust 区域

在外网主机上 ping 内网 PC1，发现无法 ping 通：

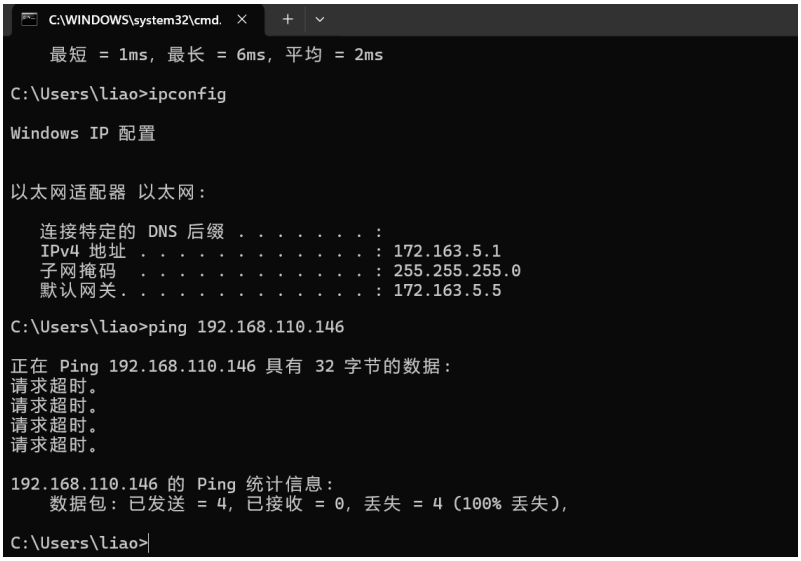


Figure 26: Untrust 区域无法访问 Trust 区域

防火墙上的验证与上面的步骤类似，此处不再展示。

4.8.6 端口安全验证

将 Boss 电脑取下，将其网线接到外网主机上。在外网主机上配置自动获取 IP 地址，然后运行 ipconfig /renew 命令后，依然无法获取到 IP 地址。

Figure 27: 配置外网主机为自动获取 IP 地址

Figure 28: 外网主机无法自动获取 IP 地址

此外，还可通过手动设置外网主机 IP 地址为 192.168.120.25/24（即 192.168.120.0/24 网段中，除 Vlanif 120 与特殊 IP 地址外的任一 IP 地址）来构成直连网络。但即便如此，ping Vlanif 120 还是会发现无法 ping 通。

至此，所有配置验证结束。

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包含局域网和广域网的中型网络，涵盖了从网络规划、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、工程验收等完整的组网工程流程。实验通过模拟第三建筑公司总部大楼的网络建设需求，详细展示了如何通过多种先进技术（如 VRRP、链路聚合、堆叠技术、VLAN、防火墙旁挂等）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，并制定了相应的项目交付要求和预算。随后，实验采用了多种网络技术来满足需求，包括虚拟路由冗余协议（VRRP）确保出口网关的高可用性，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，防火墙旁挂系统通过双机热备技术确保网络安全防护的连续性。

实验设计了详细的网络拓扑图，并通过设备连接表展示了各个设备之间的连接关系。核心交换机、路由器、防火墙、接入层交换机等设备的连接和配置都严格按照拓扑图进行。实验详细配置了核心交换机的堆叠系统、Eth-Trunk 功能、VLAN 功能等，确保核心层的高效管理和扩展性。通过堆叠技术，两台核心交换机在逻辑上形成一个设备，提升了网络的冗余性和可靠性。接入层的配置相对简单，主要涉及 VLAN 的划分和接入层交换机的配置，确保终端设备能够正确接入网络并实现部门间的隔离。出口网关的 VRRP 功能和防火墙的双机热备功能也得到配置，确保出口网关的高可用性和网络安全防护的连续性。此外，实验还配置了防火墙的安全策略，限制非工作时间的网络访问，并通过 DHCP 服务器为 VLAN 内的终端设备自动分配 IP 地址，同时配置了 NAT 功能，确保内网用户能够通过出口网关访问外网资源。

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 心得感悟

5.2.1 组长的心得感悟

本次实验自由度较大，时间跨度长，所以我选择了比较有挑战性的设计方案，也因此实现难度较大。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、防火墙的双机热备、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。

最“磨人”的当属防火墙配置问题。由于防火墙旁挂需要第二台防火墙，所以我们启用了全新的防火墙，又由于机柜上的防火墙的 MGMT 网口有些许破损，我们启用了 2 台新的防火墙，而这给我的调试带来了灾难性后果，即无论如何，配置均不生效。最后经教员指导排查，发现是防火墙未激活的问题。遂将防火墙搬到寝室内进行联网激活：

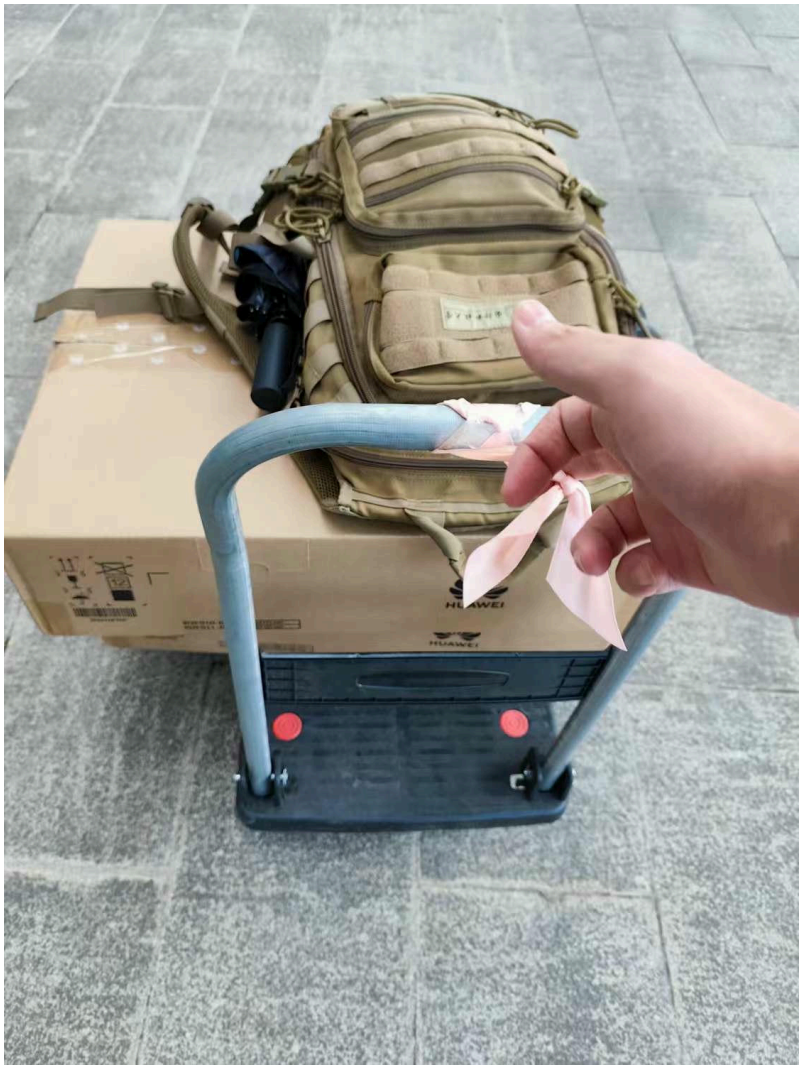


Figure 29: 搬运防火墙

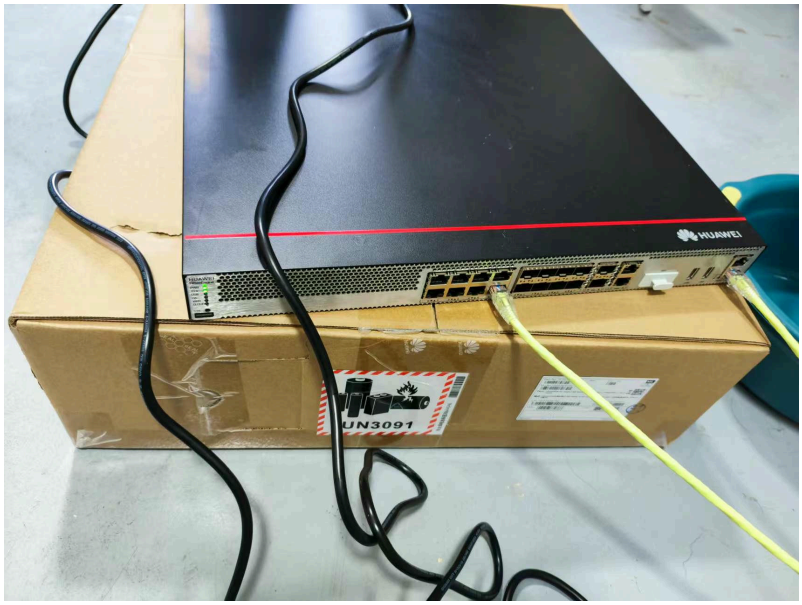


Figure 30: 激活防火墙

在将防火墙联网激活之后，一切豁然开朗，之前的问题全数解决！这一过程虽然“磨人”，但也让我深刻体会到设备初始化与激活的重要性，以及在实际工程中细节决定成败的道理。

此外，实验还让我意识到网络安全的重要性。在防火墙策略的配置和端口安全的设置上，必须严格把控，确保网络的安全性和稳定性。通过本次实验，我不仅掌握了多种网络技术的应用，还学会了如何在工程中协调各方资源，确保项目的顺利实施。总的来说，本次实验极大地提升了我的网络工程能力，为我未来的职业发展奠定了坚实的基础。

5.2.2 一把手的心得感悟

完成这次组网实验是一次难忘的体验，在团队的共同努力下，我们成功完成了实验的各项任务。

在实验中，我负责了出口路由器 AR1、AR2 的 NAT 地址转换配置。在该配置中，我们首先为内网办公区域配置了公网的动态地址池，当内网用户访问外网时，其内网地址将会转换为地址池中第一个空闲的公网地址，从而隐藏内网用户的 IP 地址。然后我们为内网的 Web 和 FTP[2]服务器配置了静态的地址转换，使得外网用户能够通过预留的公网地址 172.163.1.9 和 172.163.3.9 访问内网的 Web 服务。

通过与其他组员的密切合作，我们不仅顺利完成了任务，还在过程中学到了许多新的知识。大家在讨论和解决问题的过程中，彼此分享经验和观点，使得整个实验过程既高效又充实。

5.2.3 二把手的心得感悟

本次实验收获颇丰。通过让交换机学习老板及老板助理 PC 的 MAC 地址，限制了其他设备的接入，成功完成了 MAC 端口安全的配置，有效的增强了网络的安全性和可控性。DHCP 的配置实现了接入层 IP 地址的动态分配，让网络管理更为方便，大大减少了手动配置的工作量。在核心交换机与防火墙之间配置的 STP 成功消除了网络环路，保障了网络的稳定性，避免了因环路引发的广播风暴等问题。整个实验过程让我将理论知识与实践紧密结合，提升了网络工程实践能力，还增强了团队间的协作能力和问题解决能力。在面对复杂的网络配置问题时，我们能够共同探讨、分析并找到解决方案，这将对我们今后的学习和工作产生积极而深远的影响。

[2]最初的实验设计中，还包含实现一个 FTP 服务器。但由于时间限制，最终没有在服务器具体配置上实现，但保留了相应的特殊 NAT 转换规则。

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] 华为. 防火墙旁挂 - 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/e6367fb

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 华为. 抓包 - HUAWEI USG6000E, USG6000, USG9500, NGFW Module V500, V600 维护宝典 - 华为[EB/OL](2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000160160/6ebae75f

[16] 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

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