网 络 工 程
本 科 实 验 报 告

实验名称： 虚拟局域网（VLAN）配置

学 员 姓 名	程景愉	学 号	202302723005
培 养 类 型	无军籍	年 级	2023
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	2025.09.17

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

能根据需求划分和配置 VLAN，实现 VLAN 的基本功能。 了解端口安全的作用，掌握端口安全的配置方法。

2 实验原理

2.1 VLAN

虚拟局域网（VLAN）是一种将局域网划分为多个逻辑上的局域网的技术。VLAN 技术可以将不同的用户、不同的网络设备、不同的网络数据流分隔开，提高网络的安全性和管理性。VLAN 技术可以实现以下功能：

- 逻辑划分：将一个物理局域网划分为多个逻辑局域网，不同的逻辑局域网之间相互隔离，提高网络的安全性。
- 广播控制：VLAN 可以控制广播域的范围，减少广播风暴，提高网络的性能。
- 管理灵活：VLAN 可以根据网络的需求随时调整，提高网络的管理灵活性。
- 负载均衡：VLAN 可以将不同的用户、不同的网络设备、不同的网络数据流分隔开，实现负载均衡。

2.2 链路聚合

链路聚合是一种将多个物理链路聚合成一个逻辑链路的技术。链路聚合技术可以实现以下功能：

- 增加带宽：可以将多个物理链路聚合成一个逻辑链路，增加带宽，提高网络的性能。
- 提高可靠性：可以将多个物理链路聚合成一个逻辑链路，提高网络的可靠性。
- 负载均衡：可以将多个物理链路聚合成一个逻辑链路，实现负载均衡。

2.3 端口安全

端口安全是一种保护网络安全的技术，可以防止未经授权的设备接入网络。端口安全技术可以实现以下功能：

- 限制 MAC 地址：可以限制接口学习的 MAC 地址数量，防止未经授权的设备接入网络。
- 防止 ARP 攻击：可以防止 ARP 攻击，提高网络的安全性。
- 防止 MAC 地址冲突：可以防止 MAC 地址冲突，提高网络的稳定性。

3 实验环境

3.1 实验背景

本实验模拟某公司网络场景。公司规模较大，员工 200 余名，内部网络是一个大的局域网。公司放置了多台接入交换机（如 S1 和 S2）负责员工的网络接入。接入交换机之间通过汇聚交换机 S3 相连。公司通过划分 VLAN 来隔离广播域，由于员工较多，相同部门的员工通过不同交换机接入。为了保证在不同交换机下相同部门的员工能互相通信，需要配置交换机之间链路为干道模式，以实现相同 VLAN 跨交换机通信。

3.2 实验设备

设备名称	设备型号	设备数量
交换机	华为 S5735	2
PC	联想启天 M410 Windows 10	4

另有网线若干，控制线 2 条。

4 实验步骤及结果

4.1 实验拓扑

按实验背景，绘制拓扑图如下：

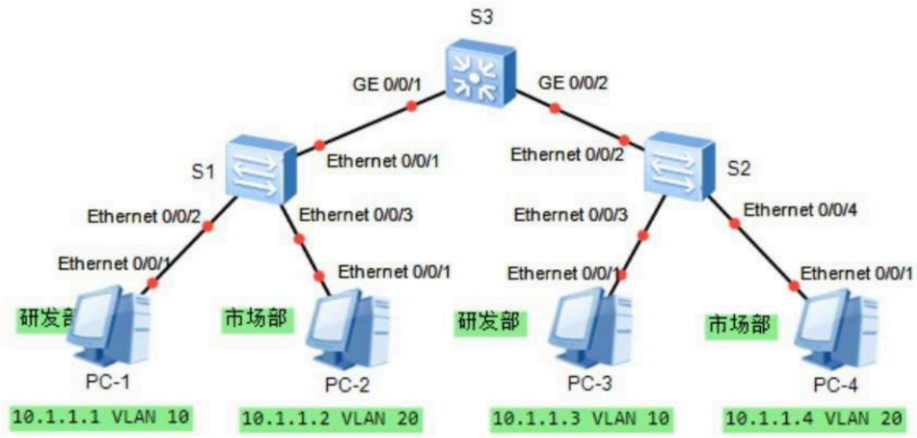

Figure 1: 实验拓扑图

4.2 按照拓扑图接线

按照拓扑图接线，将 PC1、PC2、PC3、PC4 分别连接到 LSW1、LSW2 上。图中手握的三根线是用于链路聚合的网线。

Figure 2: 接线图

4.3 配置前检验

设置 PC1、2、3、4 的 IP 地址，分别为 `192.168.10.{1, 2, 3, 4}`。设置 PC1、2 的网关为 `192.168.10.5`，设置 PC3、4 的网关为 `192.168.10.6`。使用 `ipconfig` 命令查看 PC 的 IP 地址和网关地址，以 PC1 为例，查看结果如下：

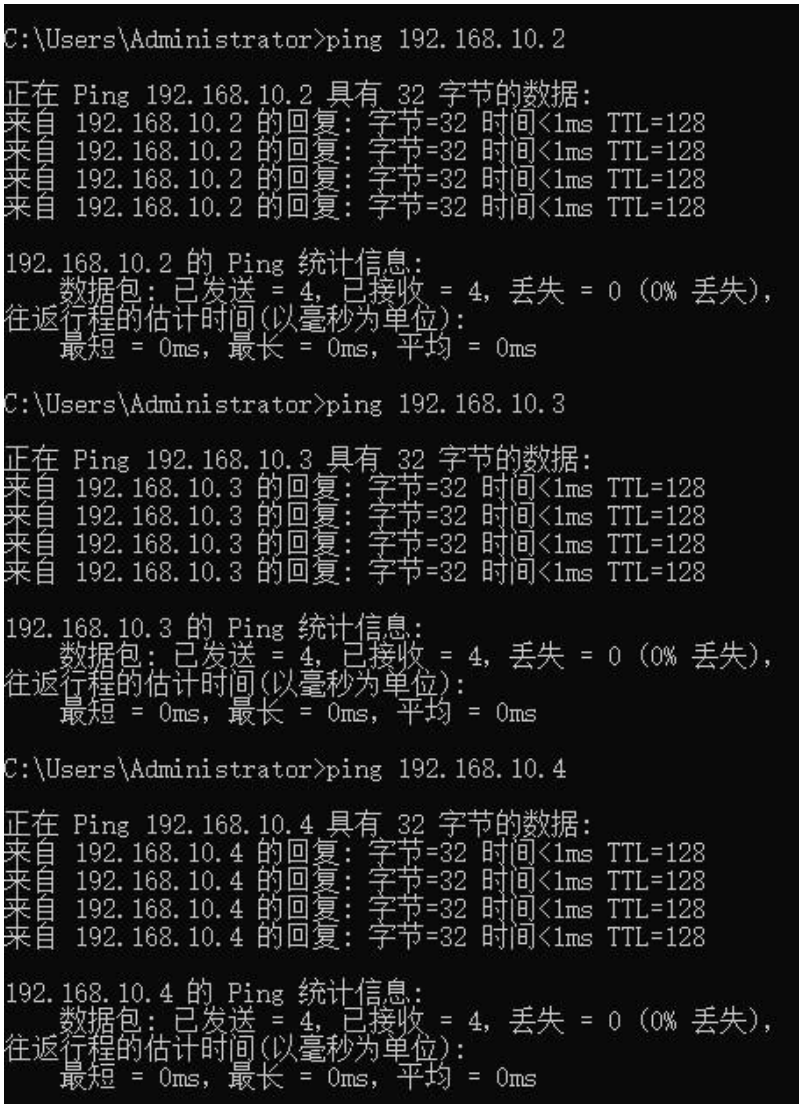

Figure 3: 配置前检验

说明 PC1 的 IP 地址、网关地址已经设置成功。 然后，在 PC1 上 ping PC2、PC3、PC4，查看是否能够 ping 通。结果如下:

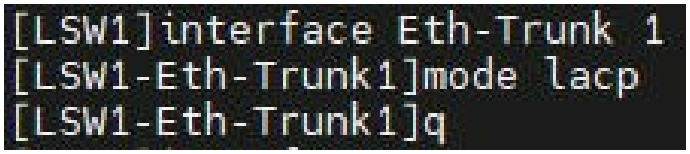

Figure 4: 配置前检验结果

说明 PC1 能够 ping 通 PC2、PC3、PC4，网络连接正常。下面开始进行 VLAN 配置。

4.4 配置 VLAN

下列许多步骤在 LSW1 和 LSW2 上都有相同的操作，这里只列出 LSW1 上的操作步骤。

4.4.1 配置各个接口的 VLAN 属性

创建 VLAN 并将接口加入 VLAN。将与 PC1、PC2 相连接口的接口类型设置为 access。将 PC1 划分到 VLAN 10，将 PC2 划分到 VLAN 20。

```
[LSW1]interf
[LSW1]int g0/0/1
[LSW1-GigabitEthernet0/0/1]int g0/0/3
[LSW1-GigabitEthernet0/0/3]eth-
[LSW1-GigabitEthernet0/0/3]eth-trunk 1
Info: This operation may take a few seconds. Please wait a moment.
Info: The operation is successful.
[LSW1-GigabitEthernet0/0/3]int g0/0/5
[LSW1-GigabitEthernet0/0/5]int g0/0/4
[LSW1-GigabitEthernet0/0/4]eth-trunk 1
Info: This operation may take a few seconds. Please wait a moment.
Info: The operation is successful.
[LSW1-GigabitEthernet0/0/4]q
```

Figure 5: 配置 VLAN 属性(1)

配置 Eth-Trunk1 接口允许 VLAN10 和 VLAN20 通过。

```
[LSW1]lacp priority 100
[LSW1]in
[LSW1]int e
[LSW1]int Eth-Trunk 1
[LSW1-Eth-Trunk1]max active
[LSW1-Eth-Trunk1]max active-linknumber 2
[LSW1-Eth-Trunk1]q
```

Figure 6: 配置 VLAN 属性(2)

验证配置结果，查看各交换机的 Eth-Trunk 信息，查看链路是否协商成功。

```
[LSW1]int g0/0/3
[LSW1-GigabitEthernet0/0/3]lacp pr
[LSW1-GigabitEthernet0/0/3]lacp priority 100
[LSW1-GigabitEthernet0/0/3]int g0/0/4
[LSW1-GigabitEthernet0/0/4]lacp priority 100
[LSW1-GigabitEthernet0/0/4]q
```

Figure 7: LSW1 的 Eth-Trunk 信息

```
[LSW1]vlan ba
[LSW1]vlan batch 10 20
Info: This operation may take a few seconds. Please wait for a moment...done.
[LSW1]int g0/0/1
[LSW1-GigabitEthernet0/0/1]port
[LSW1-GigabitEthernet0/0/1]port lin
[LSW1-GigabitEthernet0/0/1]port link-t
[LSW1-GigabitEthernet0/0/1]port link-type ac
[LSW1-GigabitEthernet0/0/1]port link-type access
Info: This operation may take a few seconds. Please wait for a moment...done.
[LSW1-GigabitEthernet0/0/1]port de
[LSW1-GigabitEthernet0/0/1]port default vlan 10
[LSW1-GigabitEthernet0/0/1]q
[LSW1]int g0/0/2
[LSW1-GigabitEthernet0/0/2]port link-type ac
[LSW1-GigabitEthernet0/0/2]port link-type access
Info: This operation may take a few seconds. Please wait for a moment...done.
[LSW1-GigabitEthernet0/0/2]port de
[LSW1-GigabitEthernet0/0/2]port default vlan
[LSW1-GigabitEthernet0/0/2]port default vlan 30
[LSW1-GigabitEthernet0/0/2]port default vlan 20
[LSW1-GigabitEthernet0/0/2]q
```

Figure 8: LSW2 的 Eth-Trunk 信息

通过以上显示信息可以看到，LSW1 的系统优先级为 100，高于 LSW2 的系统优先级。Eth-Trunk 的成员接口中 GigabitEthernet0/0/3、GigabitEthernet0/0/4 成为活动接口，处于“Selected”状态，接口 GigabitEthernet0/0/5 处于“Unselect”状态，同时实现 2 条链路的负载分担和 1 条链路的冗余备份功能。

4.4.2 阶段性检验

在 PC1 上 ping PC2、PC3、PC4，查看是否能够 ping 通。预期结果为 PC1 可以 ping 通 PC3，无法 ping 通 PC2、4。结果如下：

```
[LSW1]int eth
[LSW1]int Eth-Trunk 1
[LSW1-Eth-Trunk1]port li
[LSW1-Eth-Trunk1]port link-type t
[LSW1-Eth-Trunk1]port link-type trunk
Info: This operation may take a few seconds. Please wait for a moment...done.
[LSW1-Eth-Trunk1]port tru
[LSW1-Eth-Trunk1]port trunk a;;
[LSW1-Eth-Trunk1]port trunk all
[LSW1-Eth-Trunk1]port trunk allow-pass vlan 10 20
Info: This operation may take a few seconds. Please wait a moment.done.
[LSW1-Eth-Trunk1]q
```

Figure 9: 阶段性检验(1)

上述结果说明 PC1 可以 ping 通 PC3，无法 ping 通 PC2、4，VLAN 配置成功。网工系的学生与网安系的学生电脑之间无法通信，满足了苞米要求。

4.5 添加网关

网工系的学生做了一个网工实验，他们 PC 的 IP 地址发生了变化，从 `192.168.10.x/24` 变为了 `192.168.20.x/24`，如下图所示：

```
[LSW1]disp eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                   WorkingMode: LACP
Preempt Delay: Disabled     Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 642c-acc1-65e0
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName          Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/3   Selected 1GE      100     1      305     10111100  1
GigabitEthernet0/0/4   Selected 1GE      100     2      305     10111100  1
GigabitEthernet0/0/5   Unselect 1GE      32768   3      305     10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri   SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/3   32768    6012-3c9a-61f0  32768   1      305     10111100
GigabitEthernet0/0/4   32768    6012-3c9a-61f0  32768   2      305     10111100
GigabitEthernet0/0/5   32768    6012-3c9a-61f0  32768   3      305     10110000
```

Figure 10: 新的拓扑图

现在网工系与网安系之间展开交流，要求网安系的 PC1、PC3 能够访问网工系的 PC2、PC4。为此，需要在交换机上配置网关。本实验选择在 LSW1 上配置网关。

4.5.1 配置 PC 默认网关

在 PC2、PC4 上配置默认网关为 `192.168.20.6`（以 PC2 为例）：

```
C:\Users\Administrator>ping 192.168.10.2

正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。

192.168.10.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

C:\Users\Administrator>ping 192.168.10.3

正在 Ping 192.168.10.3 具有 32 字节的数据:
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=128

192.168.10.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>ping 192.168.10.4

正在 Ping 192.168.10.4 具有 32 字节的数据:
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。
来自 192.168.10.1 的回复: 无法访问目标主机。

192.168.10.4 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

Figure 11: 配置 PC 默认网关(1)

使用 `ipconfig` 命令查看 PC 的网关地址，以 PC2 为例，查看结果如下:

```
[LSW1]int g0/0/1
[LSW1-GigabitEthernet0/0/1]port-s
[LSW1-GigabitEthernet0/0/1]port-security enable
Info: This operation may take a few seconds. Please wait a moment.
[LSW1-GigabitEthernet0/0/1]port-security mac-
[LSW1-GigabitEthernet0/0/1]port-security mac-address st
[LSW1-GigabitEthernet0/0/1]port-security mac-address sticky
[LSW1-GigabitEthernet0/0/1]port-s
[LSW1-GigabitEthernet0/0/1]port-security max
[LSW1-GigabitEthernet0/0/1]port-security max-mac-num 1
[LSW1-GigabitEthernet0/0/1]q
```

Figure 12: 配置 PC 默认网关(2)

说明 PC2 的 IP 网关地址已经设置成功。PC4 同理。

4.5.2 配置 VLAN 网关

配置 VLANIF 接口，作为学生 PC 的网关。在 LSW1 上配置 VLANIF10 接口的 IP 地址为 `192.168.10.5/24`，配置 VLANIF20 接口的 IP 地址为 `192.168.20.6/24`。

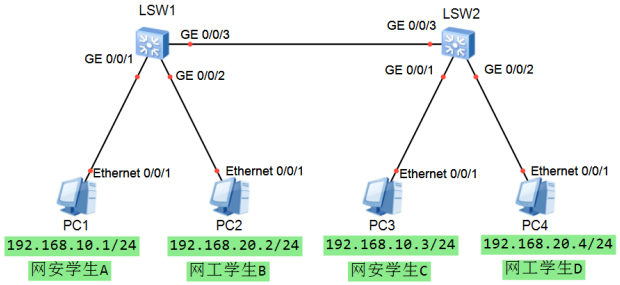

Figure 13: 配置 VLAN 网关(1)

配置好之后使用 `display interface Vlanif <index>`命令查看 VLANIF 接口的状态，查看结果如下：

Figure 14: 配置 VLAN 网关(2)

可以看到 IP 已经正确配置，且状态为 UP。

4.5.3 阶段性检验

在 PC1 上 ping PC2、PC3、PC4，查看是否能够 ping 通。预期结果为全通。结果如下：

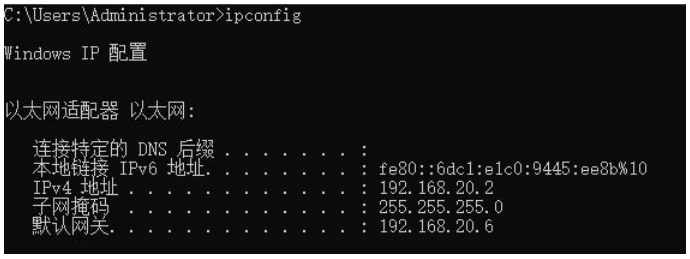

Figure 15: 阶段性检验(2)

上述结果说明 PC1 可以 ping 通 PC2、PC3、PC4，VLAN 配置成功。网工系的学生与网安系的学生电脑之间可以通信。

4.6 引入接口安全

网工系与网安系的交流活动中，有外部人员参与。为了保证网络安全，需要对接口进行安全配置，防止外部人员使用外部设备接入网络。

4.6.1 配置接口安全

将接口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 的最大 MAC 地址数设置为 1。以 LSW1 的 GigabitEthernet0/0/1 为例，配置如下：

```
[LSW1]int vlanif 10
[LSW1-Vlanif10]ip addr 192.168.10.5
                       ^
Error:Incomplete command found at '^' position.
[LSW1-Vlanif10]ip addr 192.168.10.5 24
[LSW1-Vlanif10]int vlanif 20
[LSW1-Vlanif20]ip addr 192.168.20.6 24
[LSW1-Vlanif20]q
```

Figure 16: 配置接口安全(1)

配置好之后，让 PC1 与 PC2、PC3、PC4 进行一次 ping 通信，让交换机学习每个 PC 的 MAC 地址。用 `ipconfig /all` 命令查看 PC 的 MAC 地址，以 PC1 为例，查看结果如下：

```
[LSW1]dis int vlanif 10
Vlanif10 current state : UP
Line protocol current state : UP
Last line protocol up time : 2024-11-30 16:28:13
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.10.5/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 642c-acc1-65eb
Current system time: 2024-11-30 16:56:22
    Input bandwidth utilization  : --
    Output bandwidth utilization : --

[LSW1]dis int vlanif 20
Vlanif20 current state : UP
Line protocol current state : UP
Last line protocol up time : 2024-11-30 16:30:54
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.20.6/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 642c-acc1-65e6
Current system time: 2024-11-30 16:56:26
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Figure 17: 配置接口安全(2)

可以看到 PC1 的 MAC 地址为 `1C-69-7A-2F-8E-43`。 在 LSW1 上运行 `display mac-address` 命令查看交换机学习到的 MAC 地址，查看结果如下：

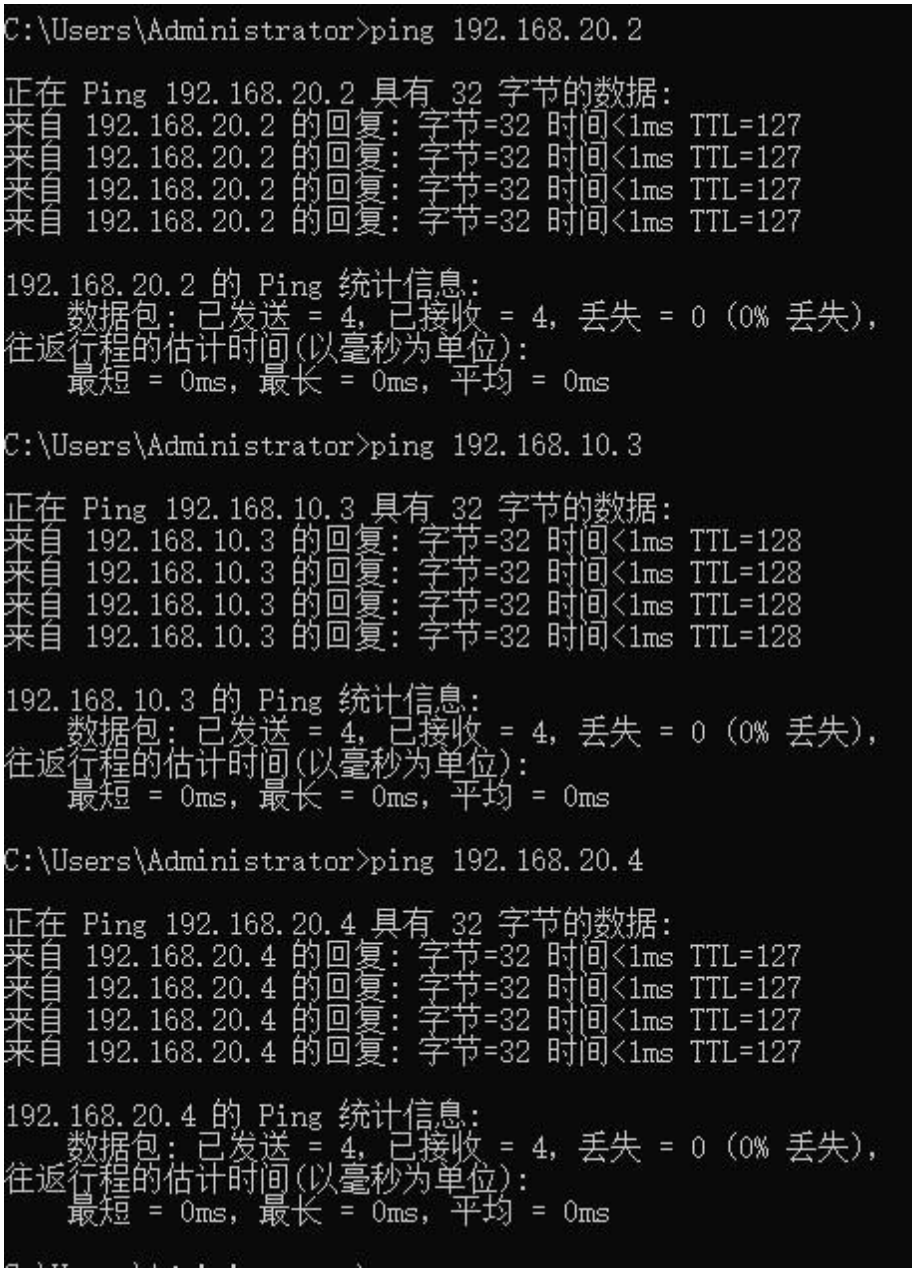

Figure 18: 配置接口安全(3)

可以看到交换机学习到了PC1的MAC地址。

4.6.2 检验接口安全配置

模拟外部人员进入网安系, 将PC1用于接入交换机LSW1的网线取下, 改用个人笔记本电脑接入LSW1:

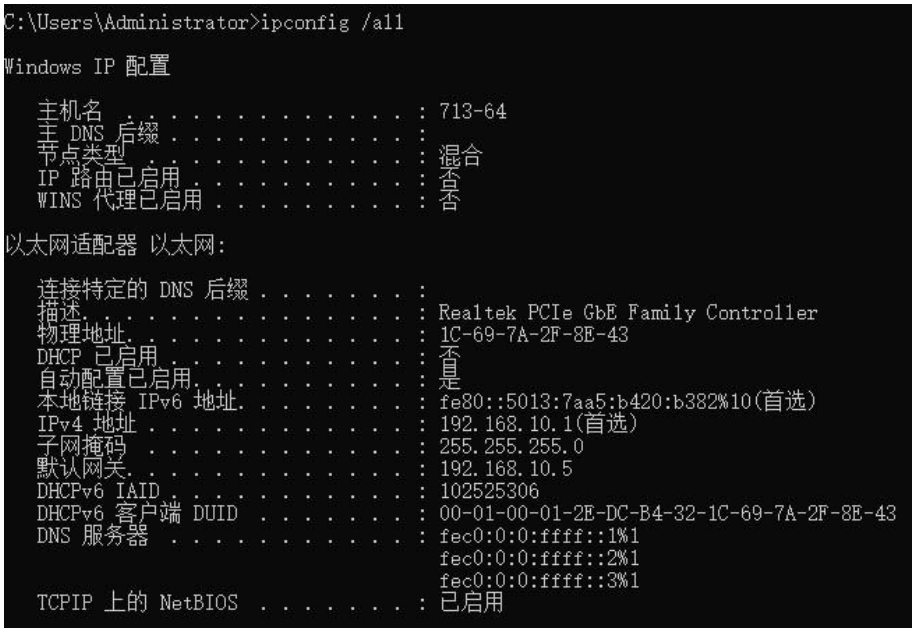

Figure 19: 检验接口安全配置(1)

将 IP 地址与默认网关设置为与 PC1 相同:

Figure 20: 检验接口安全配置(2)

然后分别 ping PC2、PC3、PC4，看是否能够正常通信。预期结果为无法通信。结果如下:

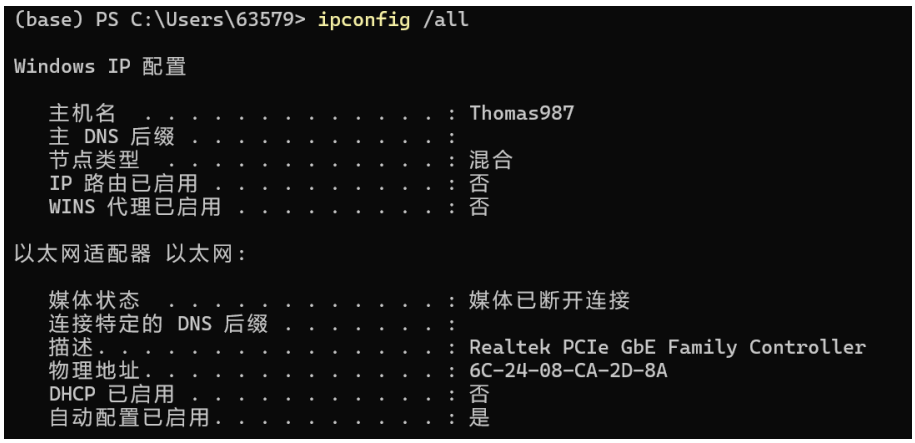

Figure 21: 检验接口安全配置(3)

个人笔记本电脑无法与任何 PC 通信，交换机出色地完成了苞米任务。

5 实验总结

5.1 内容总结

通过本次实验，我深入了解了虚拟局域网（VLAN）和端口安全配置的基本原理和实际操作。具体来说，我完成了以下几项任务：

1. VLAN 配置：
   - 学习了 VLAN 的基本概念和作用，掌握了如何根据需求划分和配置 VLAN。
   - 通过实际操作，将一个物理局域网划分为多个逻辑局域网，实现了不同 VLAN 之间的隔离，提高了网络的安全性和管理性。
2. 链路聚合：
   - 了解了链路聚合技术的基本原理，掌握了如何将多个物理链路聚合成一个逻辑链路。
   - 通过实际操作，实现了链路聚合，增加了带宽，提高了网络的性能和可靠性。
3. 端口安全配置：
   - 学习了端口安全的作用和配置方法，掌握了如何通过端口安全配置来防止未经授权的设备接入网络。
   - 通过实际操作，模拟了外部人员尝试接入网络的场景，验证了端口安全配置的有效性。

5.2 心得感悟

本次实验，我选择了 MobaXterm 作为 Serial 会话的发起终端，而非 Hypertrm。虽然两者没有本质区别，但后者具有更加现代化的界面，方便查看输入、输出。其次，在完成基础的 VLAN 配置后，我尝试学习课上讲到的其他技术，并在实验中成功利用。较为遗憾的是，由于没有技术搭建较好的测试与应用环境，没有尝试使用 Hybrid 类型接口配置基于 MAC 的 VLAN。在实验中，我遇到了许多问题，但通过查阅资料、请教老师和同学，最终解决了问题。通过本次实验，我不仅学会了网络配置的方法，还提高了解决问题的能力。

参考文献

[1] 华为. S600-E 系列交换机 典型配置案例 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000141427/f36b09a2.

[2] 华为. S600-E 系列交换机 典型配置案例 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000141427/82710693.

[3] 华为. 配置端口安全示例 - S600-E 系列交换机 典型配置案例 - 华为[EB/OL]. (2024-11-07). https://support.huawei.com/enterprise/zh/doc/EDOC1000141427/6b53bfef.