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

要求学员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 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：

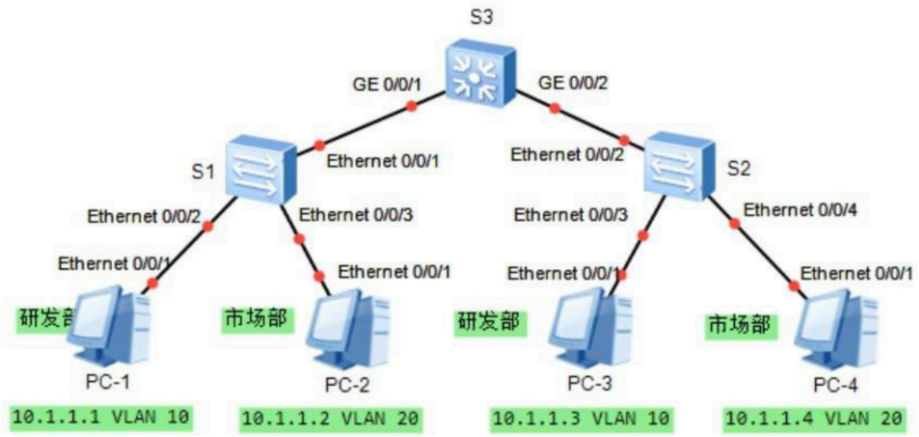

Figure 1: 实验拓扑图

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。

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 `10.130.81.{210, 211, 212, 213}`。设置 PC 的网关均为 `10.130.81.1`。以 PC1 为例，配置如下：

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。结果显然是 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]vlan batch 10 20
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Figure 4: 将 VLAN 进行划分

配置 VLAN10 和 VLAN20 接口属性为 access。

```
Username:admin
Password:
Info: Lastest accessed IP: Invalid IP address  Time: 2025-09-17 12:58:46  Failed
: 0

Info: Smart-upgrade is currently disabled. Enable Smart-upgrade to get recommend
ed version information.
<LSW1>sys
Enter system view, return user view with Ctrl+Z.
[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 link
[LSW1-GigabitEthernet0/0/1]port link-typ
[LSW1-GigabitEthernet0/0/1]port link-type ac
[LSW1-GigabitEthernet0/0/1]port link-type access
[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 access
[LSW1-GigabitEthernet0/0/2]port default vlan 20
[LSW1-GigabitEthernet0/0/2]q
[LSW1]
```

Figure 5: 配置 VLAN 属性(1)

配置 trunk 接口允许 VLAN10 和 VLAN20 通过。

```
[LSW1]int g0/0/3
[LSW1-GigabitEthernet0/0/3]port link-type tr
[LSW1-GigabitEthernet0/0/3]port link-type trunk
[LSW1-GigabitEthernet0/0/3]port trunk all
[LSW1-GigabitEthernet0/0/3]port trunk allow-pass vlan 10 20
[LSW1-GigabitEthernet0/0/3]q
[LSW1]_
```

Figure 6: 配置 VLAN 属性(2)

接下来需要验证配置结果，查看链路是否协商成功。

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：

```
C:\Users\Administrator>ping 10.130.81.213

正在 Ping 10.130.81.213 具有 32 字节的数据:
来自 10.130.81.213 的回复: 字节=32 时间<1ms TTL=128
来自 10.130.81.213 的回复: 字节=32 时间<1ms TTL=128
来自 10.130.81.213 的回复: 字节=32 时间<1ms TTL=128
来自 10.130.81.213 的回复: 字节=32 时间<1ms TTL=128

10.130.81.213 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 10.130.81.211

正在 Ping 10.130.81.211 具有 32 字节的数据:
来自 10.130.81.212 的回复: 无法访问目标主机。

10.130.81.211 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
Control-C
^C
C:\Users\Administrator>ping 10.130.81.210

正在 Ping 10.130.81.210 具有 32 字节的数据:
请求超时。

10.130.81.210 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 0, 丢失 = 1 (100% 丢失),
Control-C
```

Figure 7: 阶段性检验(1)

上述结果说明 PC2 可以 ping 通 PC4，无法 ping 通 PC1、2，VLAN 配置成功。

4.5 配置 VLANIF 接口实现三层路由通信

现在两部门之间展开交流，要求 PC1，2，3，4 能够互相访问。为此，需要在交换机上配置 VLANIF 接口以及网关地址。

4.5.1 配置 PC 默认网关

进行该实验时先调整 PC3,4 的 IP 地址，从 `10.130.81.x/24` 变为了 `10.130.91.x/24`。并在 PC3、PC4 上调整网关为 `10.130.91.1`。以 PC3 为例，配置如下：

Figure 8: PC3 进行 IP 地址调整

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 `10.130.81.1/24`，配置 VLANIF20 接口的 IP 地址为 `10.130.91.1/24`。 具体命令如下：

```
[LSW1] int vlanif 10
[LSW1-Vlanif10] ip addr 10.130.81.1
[LSW1-Vlanif10] int vlanif 20
[LSW1-Vlanif20] ip addr 10.130.91.1
```

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

```
[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
```

Figure 9: vlanif10 接口状态

```
[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
```

Figure 10: vlanif20 接口状态

说明 IP 已经正确配置，且状态为 UP。

4.5.3 阶段性检验

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

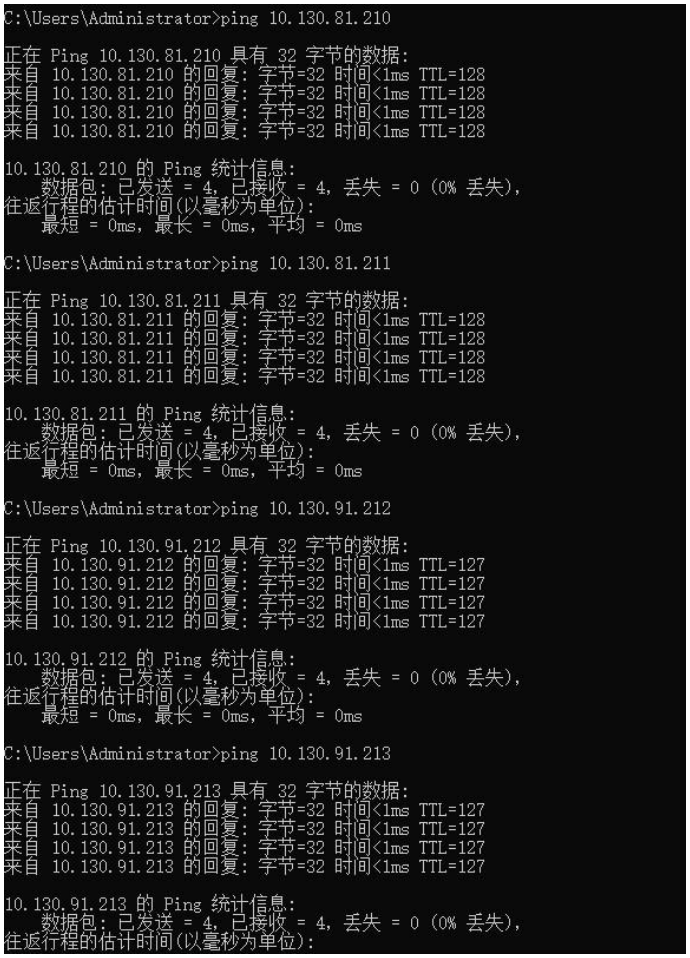

Figure 11: 阶段性检验(2)

上述结果说明 PC1 可以 ping 通 PC2、PC3、PC4，VLANIF 配置成功。两个部门的电脑之间可以通信。

4.6 引入接口安全

两个部门的交流活动中，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 g0/0/1
[LSW1-GigabitEthernet0/0/1]port-security enable
Info: This operation may take a few seconds. Please wait a moment.
[LSW1-GigabitEthernet0/0/1]poet
Sep 22 2025 13:12:20 LSW1 L2IFPPI/4/PORTSEC_ACTION_ALARM:OID 1.3.6.1.4.1.2011.5.
25.42.2.1.7.6 Interface (7/1) GigabitEthernet0/0/1 receive insecure MAC address,
 and the port status is: 1. (1:restrict;2:protect;3:error-down)
Sep 22 2025 13:12:20 LSW1 L2IFPPI/4/PORTSEC_ACTION_HAVEMAC_ALARM:OID 1.3.6.1.4.1
.2011.5.25.315.3.2 Interface 7 receive insecure MAC address. (MacAddr=[1c.69.7a.
2f.8f.22 (hex)], VLAN=20, VsiName=, Portindex=1, InterfaceName=GigabitEthernet0/
0/1, the port status is: 1. (1:restrict;2:protect;3:error-down))
[LSW1-GigabitEthernet0/0/1]por
Sep 22 2025 13:12:23 LSW1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.191.
3.1 configurations have been changed. The current change number is 13, the chang
e loop count is 0, and the maximum number of records is 4095.
[LSW1-GigabitEthernet0/0/1]port-security mac-address sticky
[LSW1-GigabitEthernet0/0/1]port-security mac-ad
Sep 22 2025 13:12:43 LSW1 DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011.5.25.191.
3.1 configurations have been changed. The current change number is 14, the chang
e loop count is 0, and the maximum number of records is 4095.
[LSW1-GigabitEthernet0/0/1]port-security max-
Sep 22 2025 13:12:46 LSW1 L2IFPPI/4/PORTSEC_ACTION_ALARM:OID 1.3.6.1.4.1.2011.5.
25.42.2.1.7.6 Interface (7/1) GigabitEthernet0/0/1 receive insecure MAC address,
 and the port status is: 1. (1:restrict;2:protect;3:error-down)
Sep 22 2025 13:12:46 LSW1 L2IFPPI/4/PORTSEC_ACTION_HAVEMAC_ALARM:OID 1.3.6.1.4.1
.2011.5.25.315.3.2 Interface 7 receive insecure MAC address. (MacAddr=[1c.69.7a.
2f.8f.22 (hex)], VLAN=20, VsiName=, Portindex=1, InterfaceName=GigabitEthernet0/
0/1, the port status is: 1. (1:restrict;2:protect;3:error-down))
[LSW1-GigabitEthernet0/0/1]port-security max-mac-num 1
[LSW1-GigabitEthernet0/0/1]_
```

Figure 12: 配置接口安全

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：

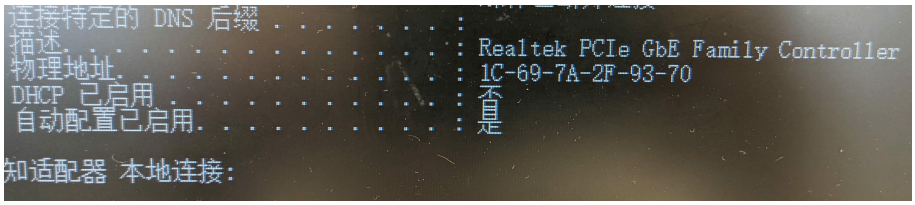

Figure 13: 查看 PC1 的 MAC 地址

可以看到 PC1 的 MAC 地址为 `1C-69-7A-2F-93-70`。 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：

```
[LSW1]display mac-address
------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                      Learned-From        Type
------------------------------------------------------------------------------
1c69-7a2f-8f2e 10/-/-                           GE0/0/2             dynamic
1c69-7a2f-8f6c 10/-/-                           GE0/0/1             sticky
1c69-7a2f-9370 20/-/-                           GE0/0/3             dynamic

------------------------------------------------------------------------------
Total items displayed = 3
```

Figure 14: 验证交换机学习到的 MAC 地址

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，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，并将 IP 地址与默认网关设置为与 PC1 相同。

然后分别 ping PC2、PC3、PC4，结果均无法正常 ping 通，查看交换机的 MAC 地址表，发现并没有学习到个人笔记本电脑的 MAC 地址，说明接口安全配置成功。

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. 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，我在完成基础的 VLAN 配置后，我尝试学习课上讲到的安全技术，并在实验中成功利用。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.