**lab11\_VLAN 配置实验项目**

学生姓名：苏家铭 合作学生：莫益萌

实验地点：济世楼 330 实验时间：2023 年 10 月 25 日

**【实验目的】**

了解 VLAN 的发展原因以及基本原理，从而掌握网络的隔离性要求，进而对交换即深入学习，了解交换机的更多功能和应用。接触网络安全的相关知识，之后的 VLAN 技术的理论学习奠定基础。掌握通过交换机划分 VLAN 的方法。

**【实验原理】**

1. VLAN 是通过软件把网络按逻辑分组，按照物理上交换机端口分割，把不同地理位置的主机分割到相同的 VLAN 内，VLAN 是在交换机上实现的。VLAN 是指在一个物理网段内。进行逻辑的划分，划分成若干个虚拟局域网，VLAN 最大的特性是不受物理位置的限制，可以进行灵活的划分。VLAN 具备了一个物理网段所具备的特性。相同 VLAN 内的主机可以相互直接通信，不同 VLAN 间的主机之间互相访问必须经路由设备进行转发，广播数据包只可以在本 VLAN 内进行广播，不能传输到其他 VLAN 中。
2. VLAN 可以剞劂广播风暴问题，交换机的每个端口是一个冲突域，但不能隔离广播，而 VLAN 就是一个广播域。
3. Cisco2950 交换机设备中默认所有端口都在 VLAN1，因此需要进行配置。
4. Port VLAN 是实现 VLAN 的方式之一，它利用交换机的端口进行 VLAN 的划分。
5. Tag VLAN 是基于交换机端口的零一类型，主要用于是交换机的相同 VLAN 内的主机之间可以直接访问，同时对不同 VLAN 的主机进行隔离。Tag VLAN 遵循 IEEE802.1Q 协议的标准，在使用配置了 Tag VLAN 的端口进行数据传输时，需要在数据帧内添加 4 字节的 8021.Q 标签信息，用于标识该数据帧属于哪个 VLAN，以便于对端交换机接收数据帧后进行准确的过滤。

交换机的 VLAN 配置涉及一下命令：

* 进入 VLAN 配置模式：vlan database，只有在此模式下，才能管理 VLAN。
* 创建 vlan:vlan NO name NAME

其中，NO 代表 BLAN 组编号数字，可以任意，但必须保持唯一，NAME 表示 BLAN 别名。每个交换机都缺省包含一个编号为 1 的 VLAN，该 VLAN 不能删除，缺省情况下所有交换机端口都属于该 VLAN。

* 物理端口划归指定 VLAN：switchport access vlan NO。NO 代表 VLAN 组编号。
* 显示 VLAN 配置情况：show Vlan。
* 删除 VLAN：no vlan NO，NO 代表 VLAN 组编号。

使用交换机作为实验设备，将交换机划分成三个 VLAN，VLAN1 包含 1～8 端口，VLAN2 包含 9～16 端口，VLAN3 包含其余端口；两台计算机作为测试平台，设置成同一个子网 IP 地址。

使用 Host1 超级终端为交换机配置 VLAN

为 Host1 和 Host2 以太网卡配置同子网 IP 地址，分别是 192.168.0.12 和 192.168.0.10。

然后用双绞线将两个网卡连接到交换机端口上，不断变换交换机的端口，测试联通状况。位于同一个 VLAN 时，两个主机将会连通；位于不同 VLAN 时，两个主机无法连通。

**【实验设备】**

济世楼 330 实验室 PC 机一台

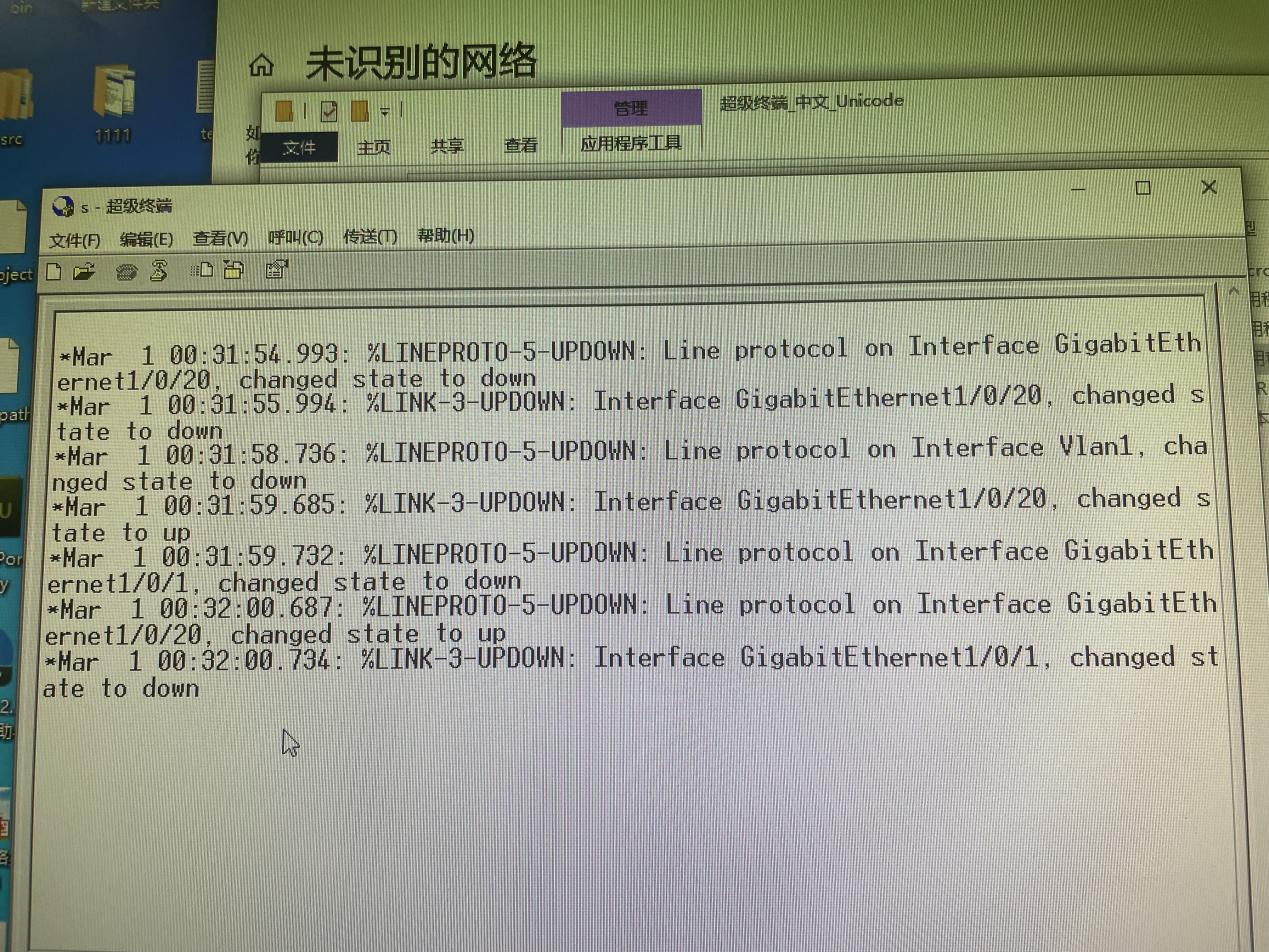
**【实验步骤】**

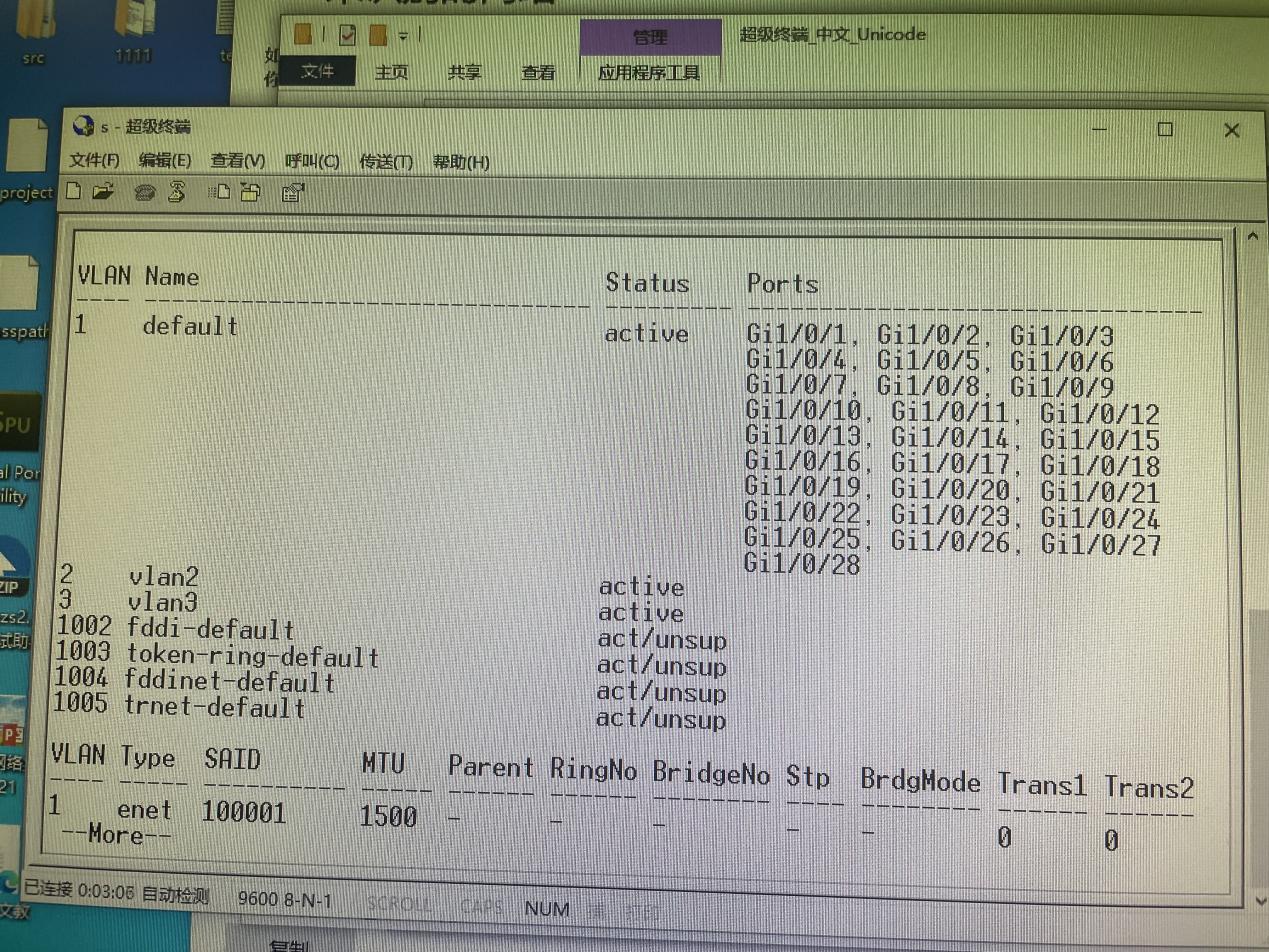
1. 按照实验环境要求，完成实验拓扑结构连接，并打开相关设备电源。
2. 设置计算机 Host1 和 Host2 网卡 IP 地址。主机网卡 IP 地址设置如下：

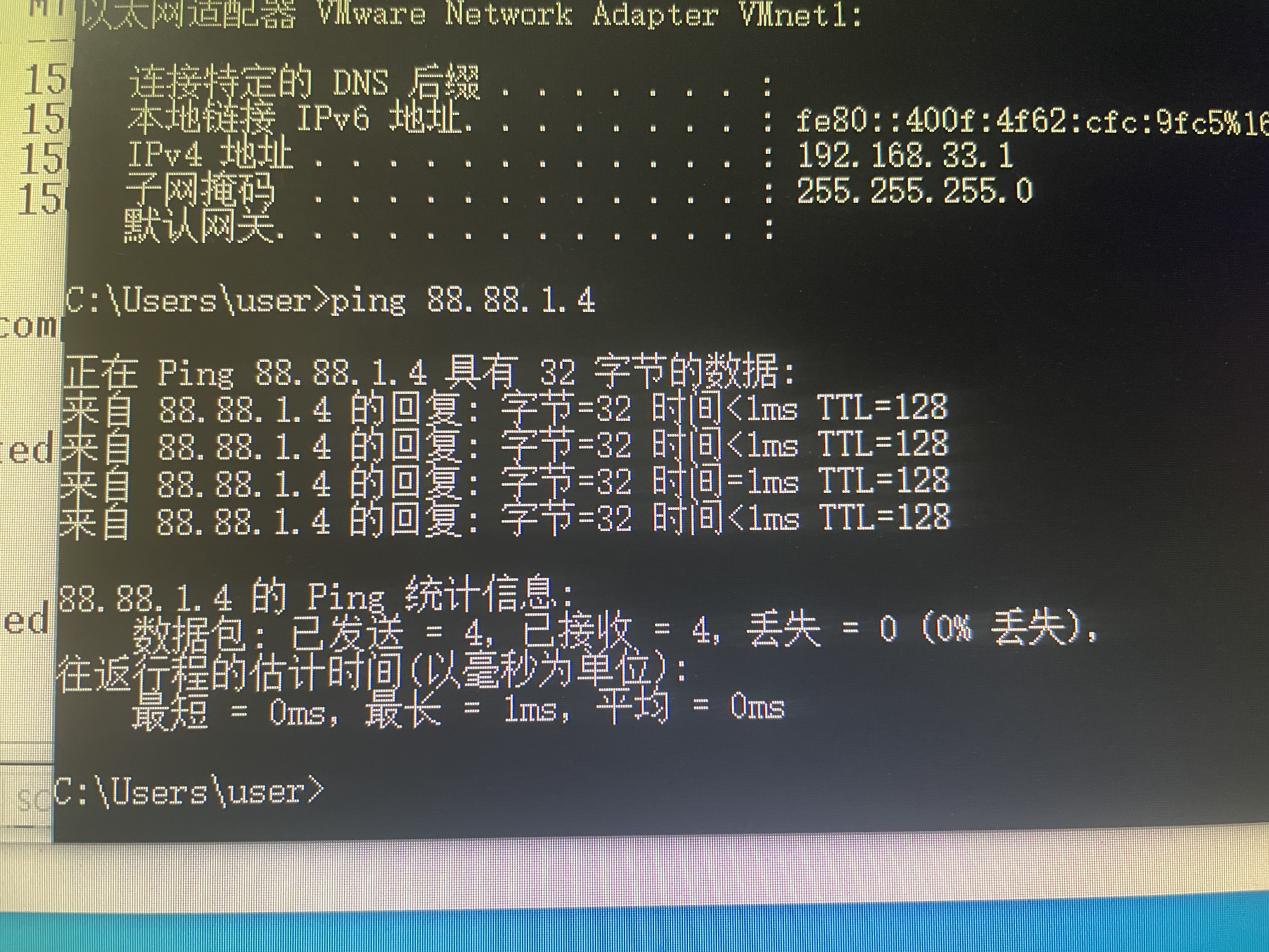
* Host1：IP 地址=192.168.0.12，子网掩码=255.255.255.0
* Host2：IP 地址=192.168.0.10，子网掩码=255.255.255.0

1. 测试初始阶段同子网主机之间连通性。用双绞线将 Host1 和 Host2 连接到交换机任意端口。从 Host1 打开命令行窗口，测试连通性，键入”ping 192.168.0.10“，连通就表示试验成功。
2. 交换机配置。启用超级终端，创建 VLAN2，并将端口 9 等划分给 VLAN2。
3. ①进入特权模式：switch>en，Enable Secret Password=cisco。
4. ②建立 VLAN2：
5. 进入 vlan 配置模式：switch#vlan database；
6. 添加 vlan2：switch（vlan）#vlan 2 name vlan；
7. 退出配置和生效：switch（vlan）#exit。
8. ③为 VLAN2 分配端口：
9. 进入配置模式：switch#config t；
10. 进入 f0/9 端口：switch（config）#int f0/9；
11. 将端口 f0/9 端口分配给 vlan2：switch（config -if）#switchport access vlan2；
12. 推出配置和生效：switch（config -if）#exit；
13. 仿照操作，将 f0/10-f/16 端口分配给 vlan2；
14. 查看 VLAN2 配置：switch# sh vlan name vlan2。
15. 重新测试不同 VLAN 之间主机连通性。将 Host1 插到端口 1，Host2 插到端口 9.Host1 打开命令行窗口，测试连通性，键入”ping 192.168.0.10“，无法连通就表示实验成功，因为两台主机分别位于 VLAN1 和 VLAN2。

**【实验现象】**







**【分析讨论】**

1. 网络风暴

通常指的是由于网络拓扑的设计和连接问题，或其他原因，导致广播在网段内大量复制，传播数据帧，导致网络性能下降，甚至网络瘫痪。

1. 如何避免

* 使用交换机和路由器：交换机可以分隔冲突域，路由器可以分隔广播域。通过合理设计网络拓扑，使用交换机将网络划分为多个较小的冲突域，减少冲突和广播的影响范围。路由器可以将广播限制在特定的网络段内，避免广播数据在整个网络中传播，减少网络风暴的风险。
* VLAN（Virtual Local Area Network）技术：通过 VLAN 可以将网络划分为多个逻辑上独立的虚拟局域网。不同的 VLAN 之间的广播和数据流量是相互隔离的，可以有效控制广播范围，减少网络风暴的影响。
* 使用广播抑制机制：一些网络设备和交换机上提供了广播抑制功能。这些功能可以限制广播报文的传播范围，从而减少网络风暴的影响。
* 配置流量控制和拥塞控制机制：通过配置合适的流量控制和拥塞控制机制，可以在网络拥塞时限制流量的传输，避免网络风暴的发生。

1. 交换机在 VLAN 中的作用

* VLAN 端口成员分配：交换机上的每个接口可以配置为特定 VLAN 的成员。通过将接口分配给不同的 VLAN，可以实现不同 VLAN 之间的隔离，确保通信只在同一 VLAN 内进行。
* VLAN 之间的通信：交换机通过使用虚拟局域网标记（VLAN tag）来区分不同 VLAN 上的数据流量。当交换机接收到带有 VLAN 标记的数据包时，它会根据标记将数据包转发到正确的 VLAN。
* VLAN 间的隔离：通过在交换机上创建不同的 VLAN，可以实现逻辑上的隔离。这意味着即使物理连接共享在同一个交换机上，不同 VLAN 的设备也无法直接通信，增加了网络的安全性和隔离性。
* VLAN 间的广播控制：交换机可以限制广播和多播流量在同一 VLAN 内传播，而不会泛洪整个网络。这样可以减少网络风暴的风险，并优化网络性能。
* VLAN 间的流量控制：通过交换机上的配置，可以实现对不同 VLAN 之间的流量优先级和带宽的控制。这有助于提供针对不同 VLAN 的流量管理和服务质量（QoS），以满足特定 VLAN 的需求。