**【实验名称】：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】**

**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。**

**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**

**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。**

**交换机配置。启用超级终端，创建VLAN2，并将端口9等划分给VLAN2。**

**①进入特权模式：switch>en,Enable Secret Password=cisco.**

**②建立VLAN2：**

**进入vlan配置模式：switch#vlan database；**

**添加vlan2：switch（vlan）#vlan 2 name vlan；**

**退出配置和生效：switch（vlan）#exit。**

**③为VLAN2分配端口：**

**进入配置模式：switch#config t；**

**进入f0/9端口：switch(config)#int f0/9;**

**将端口f0/9端口分配给vlan2：switch(config -if)#switchport access vlan2；**

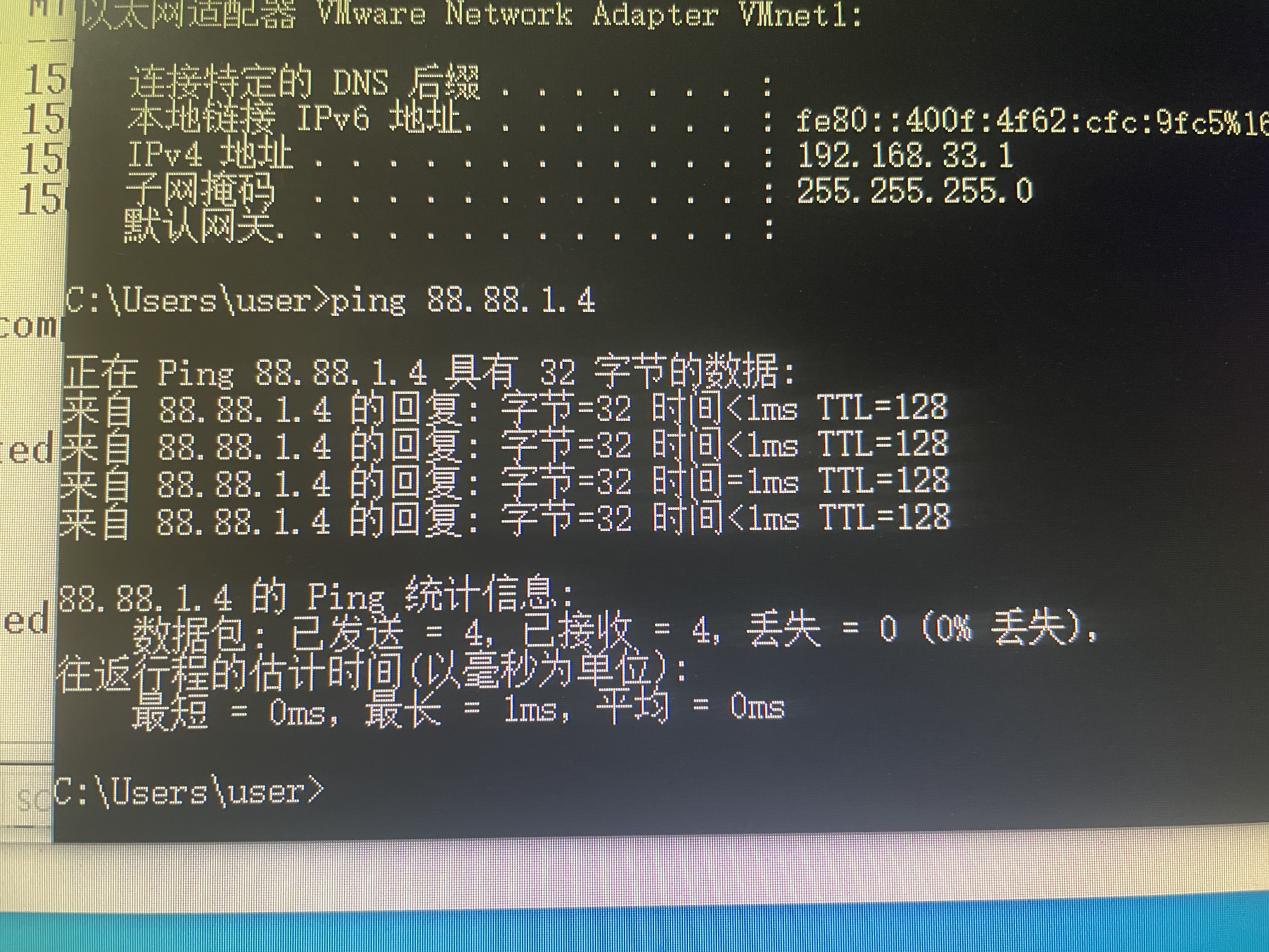
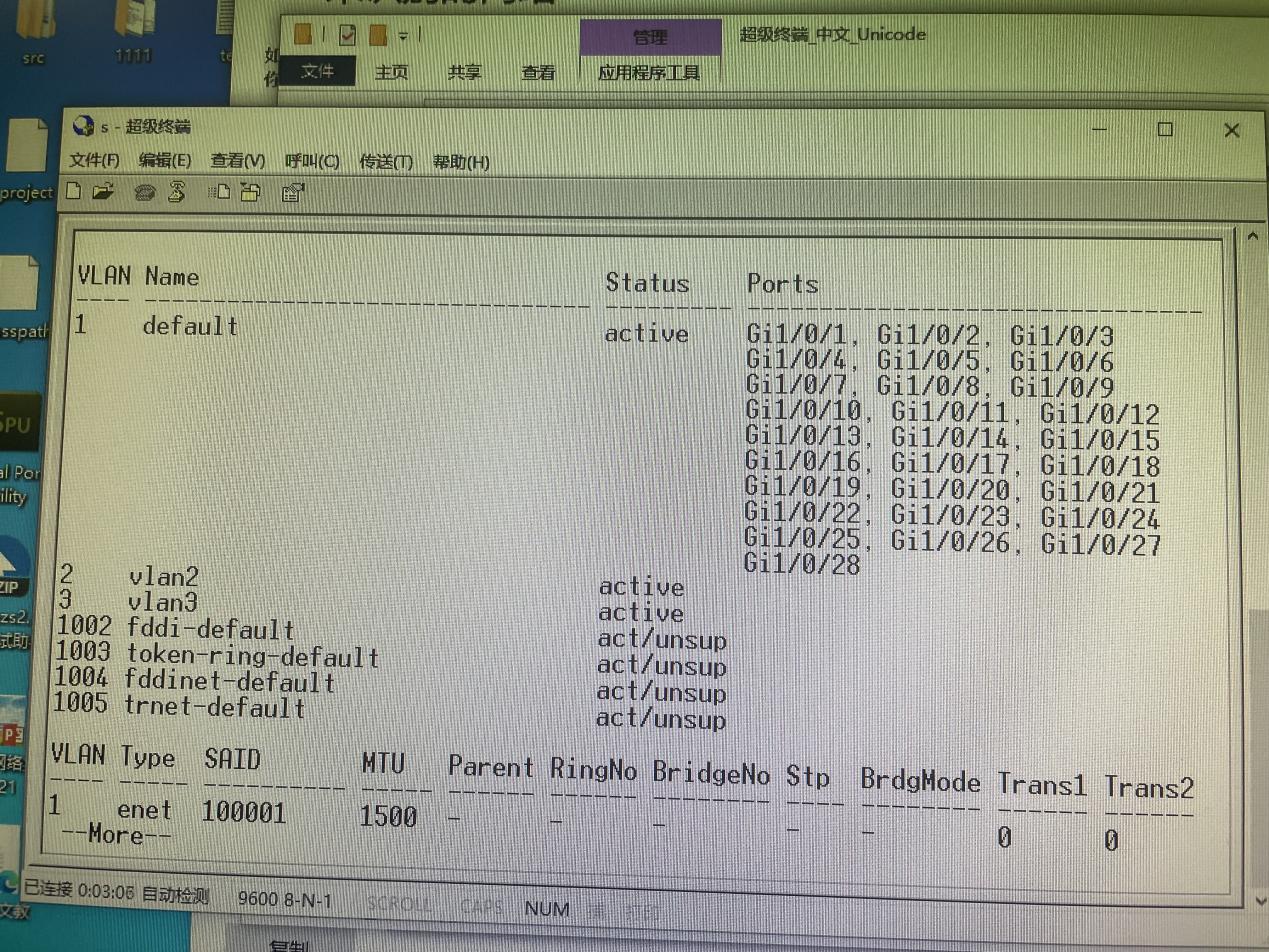
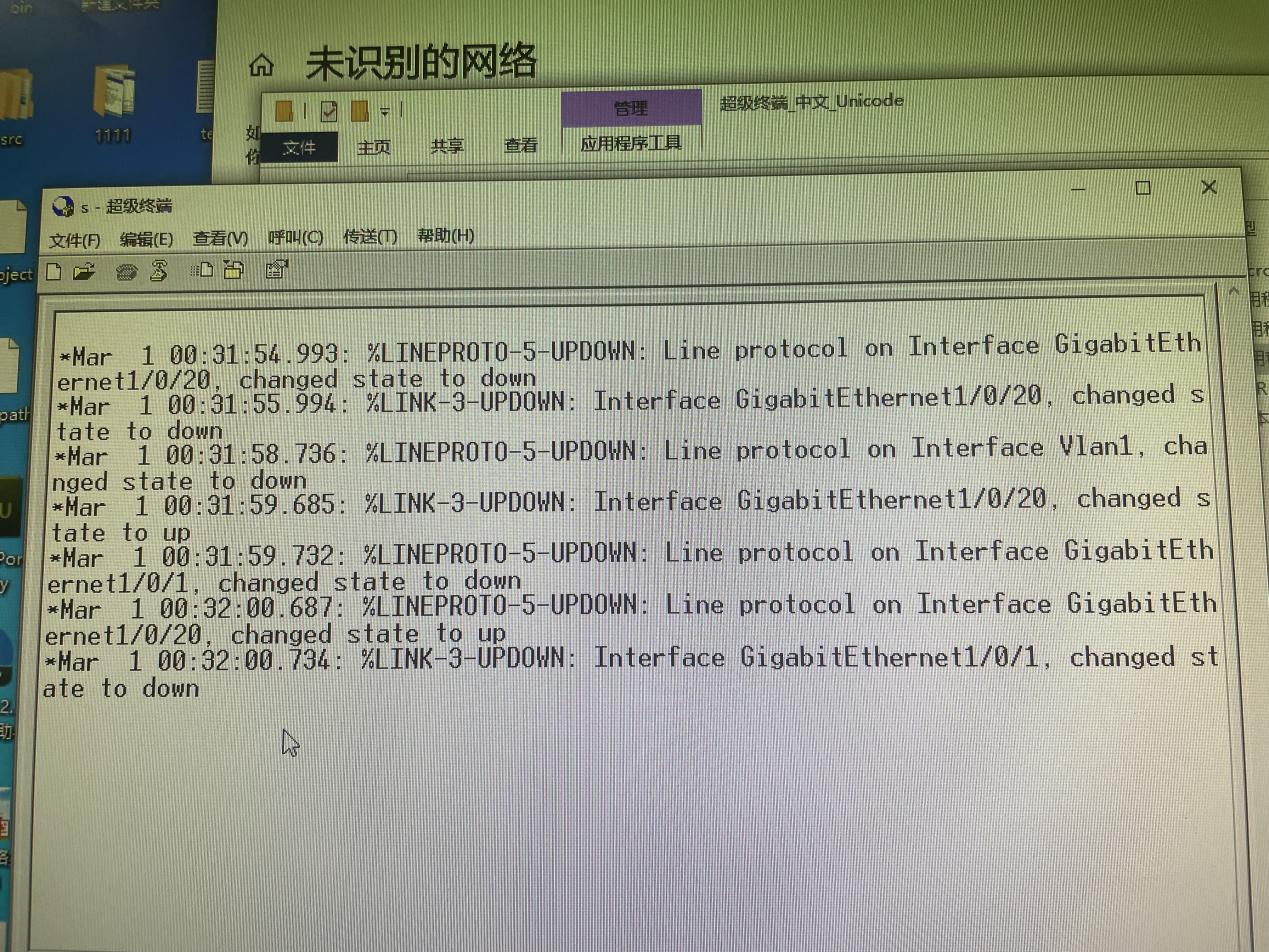
**推出配置和生效：switch(config -if)#exit;**

**仿照操作，将f0/10-f/16端口分配给vlan2；**

**查看VLAN2配置：switch# sh vlan name vlan2。**

**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。**