**北京科技大学实验报告**

学院：计通学院 专业：信息安全 班级：信安211

姓名：李晓坤 学号：U202141863 实验日期： 2023年 11 月 30 日

**实验名称：**

实验一：交换机的基本操作

**实验目的：**

（1）了解交换机配置的方法

（2）掌握CLI配置环境

（3）掌握交换机的基本配置

另外，受限于报告篇幅，对报告中部分图片进行裁剪，不影响结果展示。

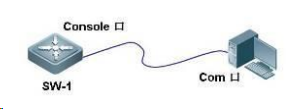
**实验仪器：**

交换机1台、主机1台

**实验原理：**

交换机工作在数据链路层的网络连接设备，基本功能是在多个计算机或网段之间交换数据。交换机内部的CPU会在每个端口成功连接时，通过将MAC地址和端口对应，形成一张MAC表。交换机在数据链路层进行数据转发时，根据数据包的 MAC地址决定数据转发的端口，而不是简单的向所有的端口进行转发，因此，交换机可用于划分数据链路层广播，即冲突域；但它不能划分网络层广播，即广播域。具体来说，当交换机接收到一个数据帧时，它首先会记录数据帧的源端口和源MAC地址的映射，然后将数据帧的目的MAC地址与系统内部的动态查找表进行比较，并根据比较结果将数据包发送给相应的目的端口。若数据包的目的 MAC 层地址不在查找表中，则将包广播到每个端口。

基于Cisco互连网操作系统对交换机进行配置，以CLI的形式对交换机进行配置和管理。基本网络拓扑结构如下：



**实验内容与步骤：**

**（一）基本操作部分**

（1）查看设备选型并登录

通过实验室的计算机登陆实验平台，看到本小组的设备，其中有路由器、二层交换机、三层交换机。这里我选择12T-S2928-1，即第十二组的第一台二层交换机。



（2）熟悉交换机的配置模式，登陆进入所选择的交换机，然后开始配置

a、通过enable进入特权模式

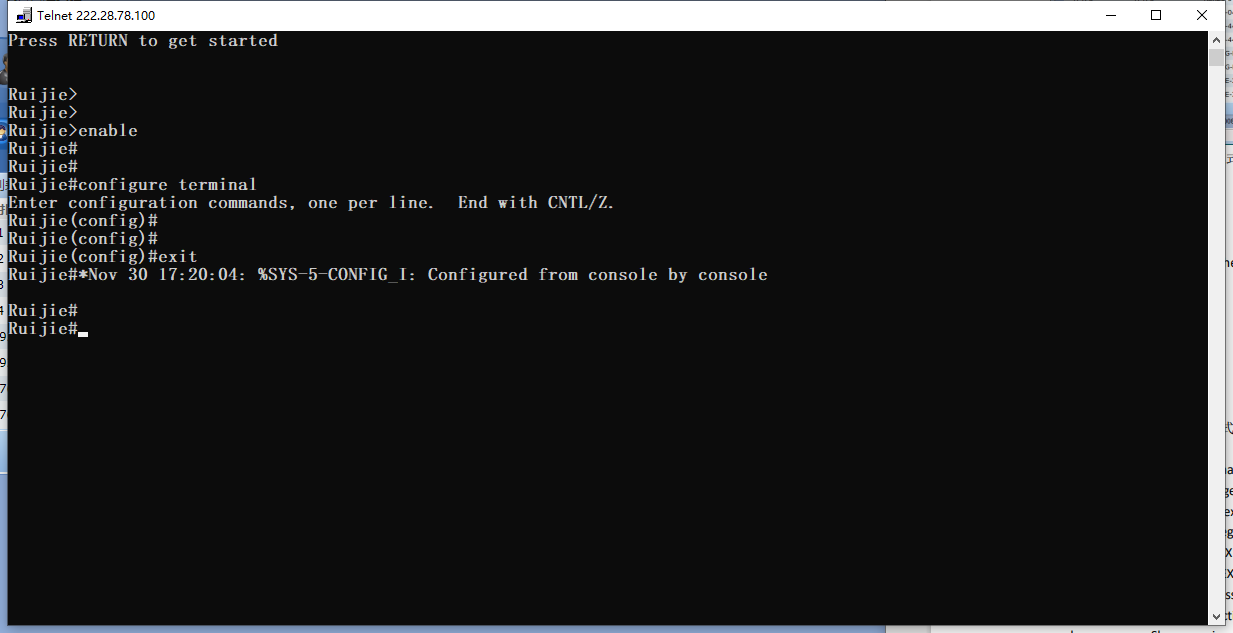
b、通过configure terminal进入全局配置模式

c、通过interface Gigabitethernet 0/5进入交换机f0/5的接口模式

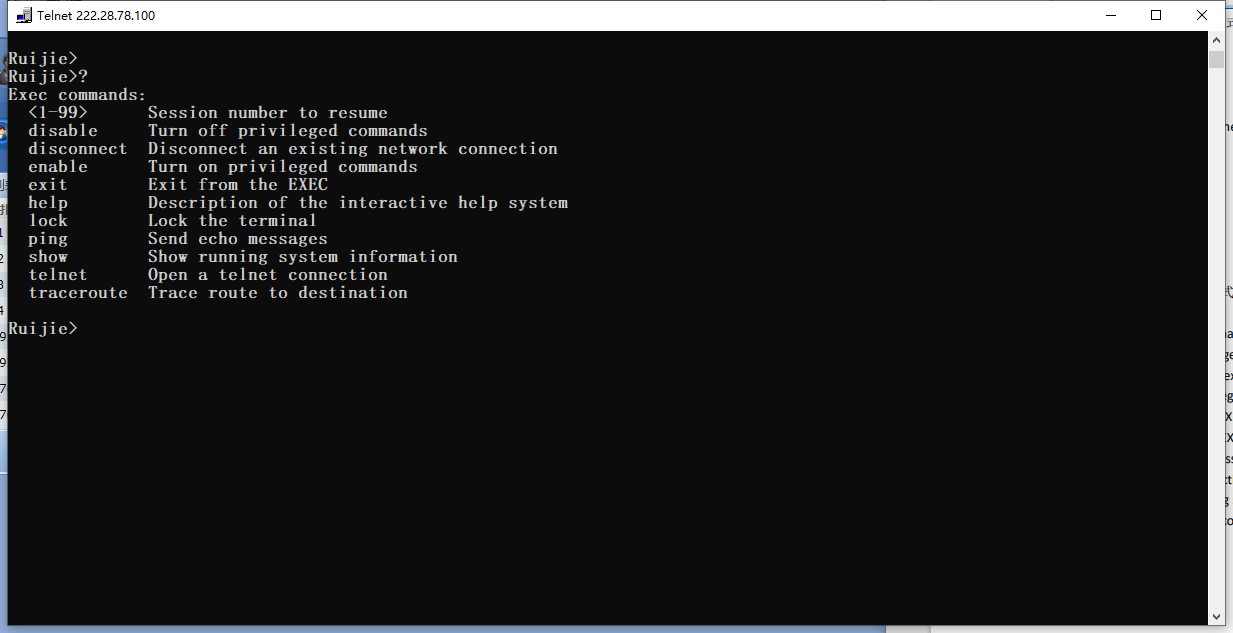
d、通过exit返回上一级操作模式

e、通过end直接退回到特权模式

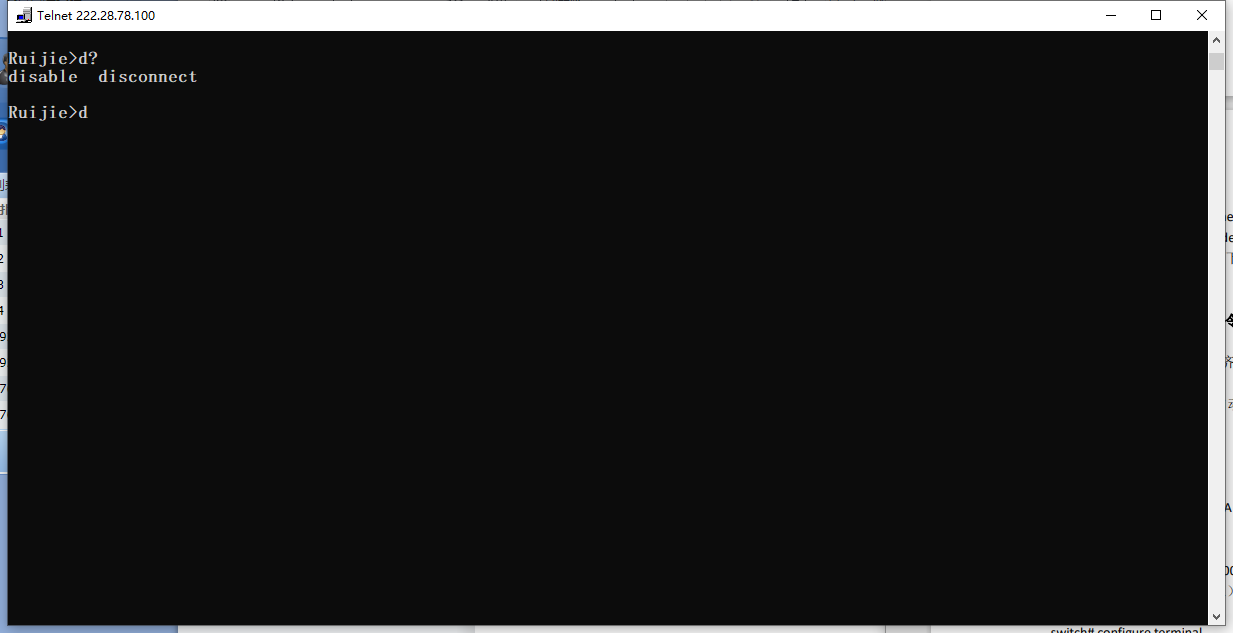
本环节主要测试了上述指令，熟悉了交换机的配置模式，部分中间截图如下：

（3）命令行快捷指令

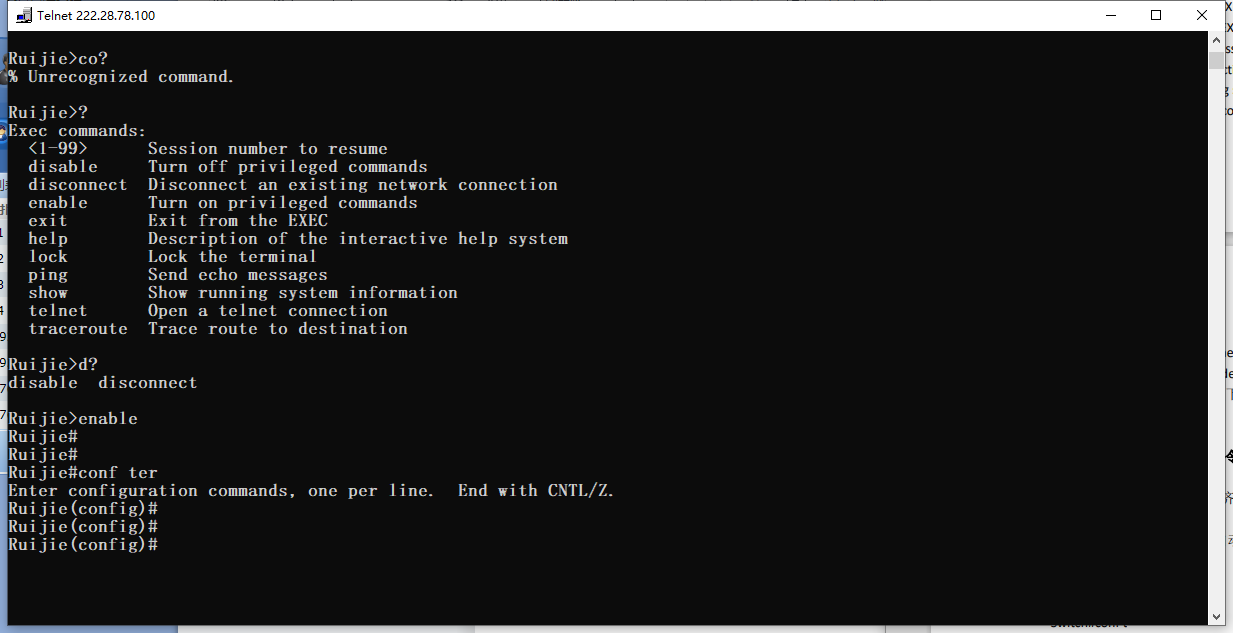
a、通过？查看当前模式下所有可执行的命令



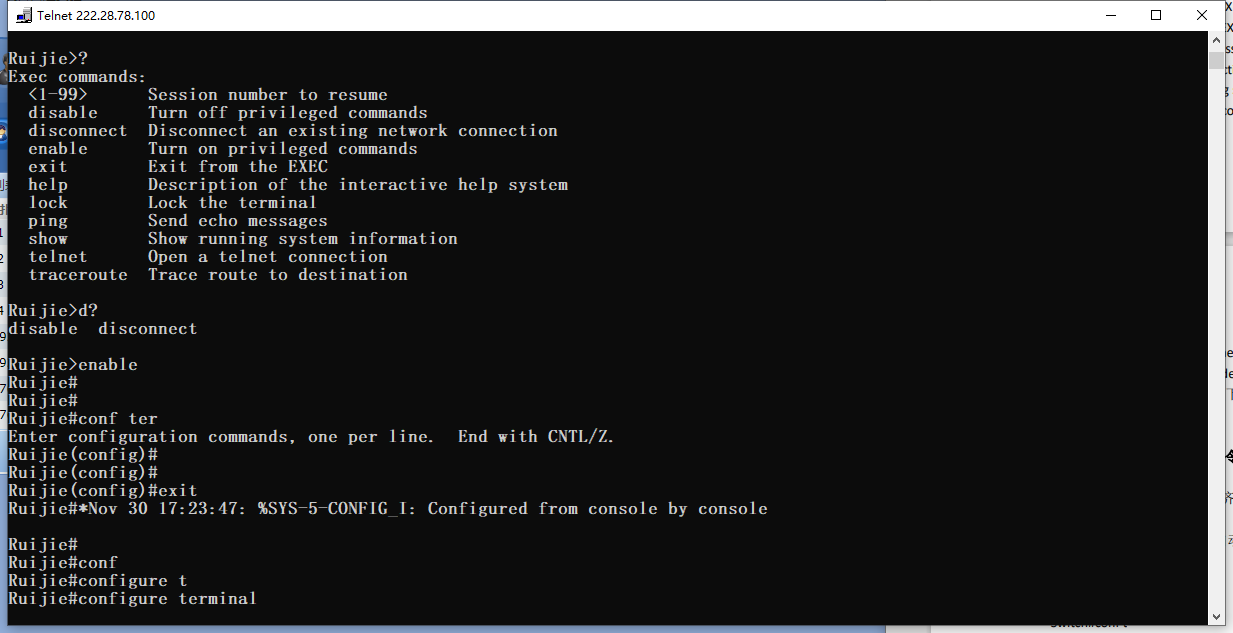
b、通过d？查看当前模式下所有d开头的命令



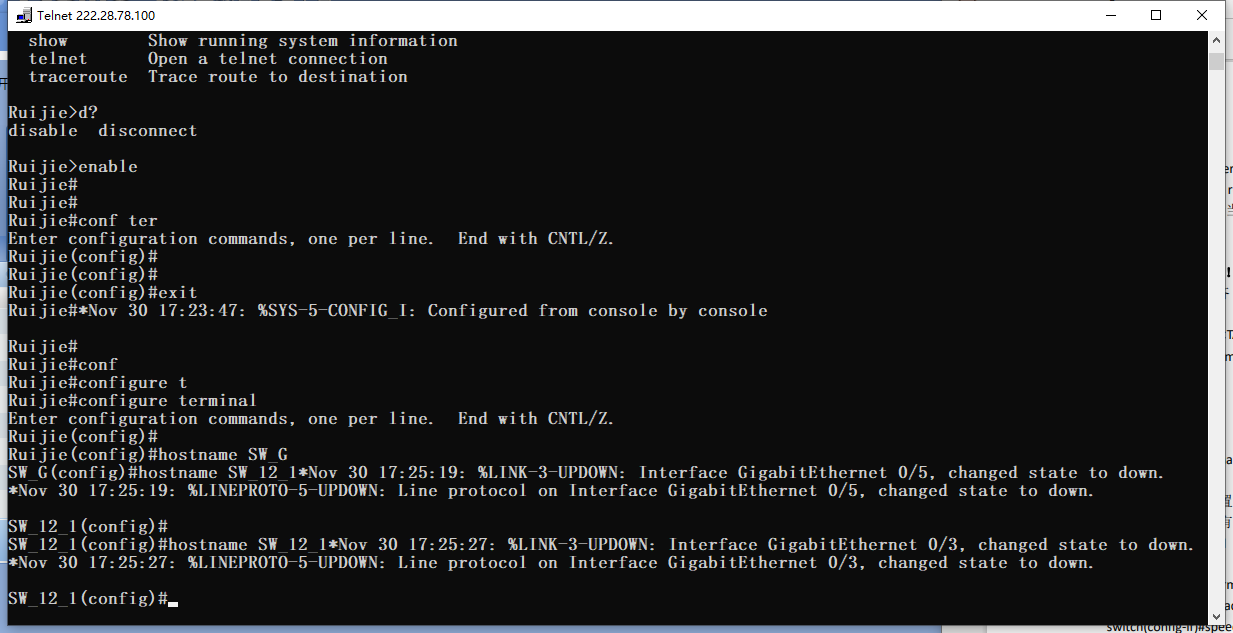
c、通过命令简写conf ter进入全局配置模式



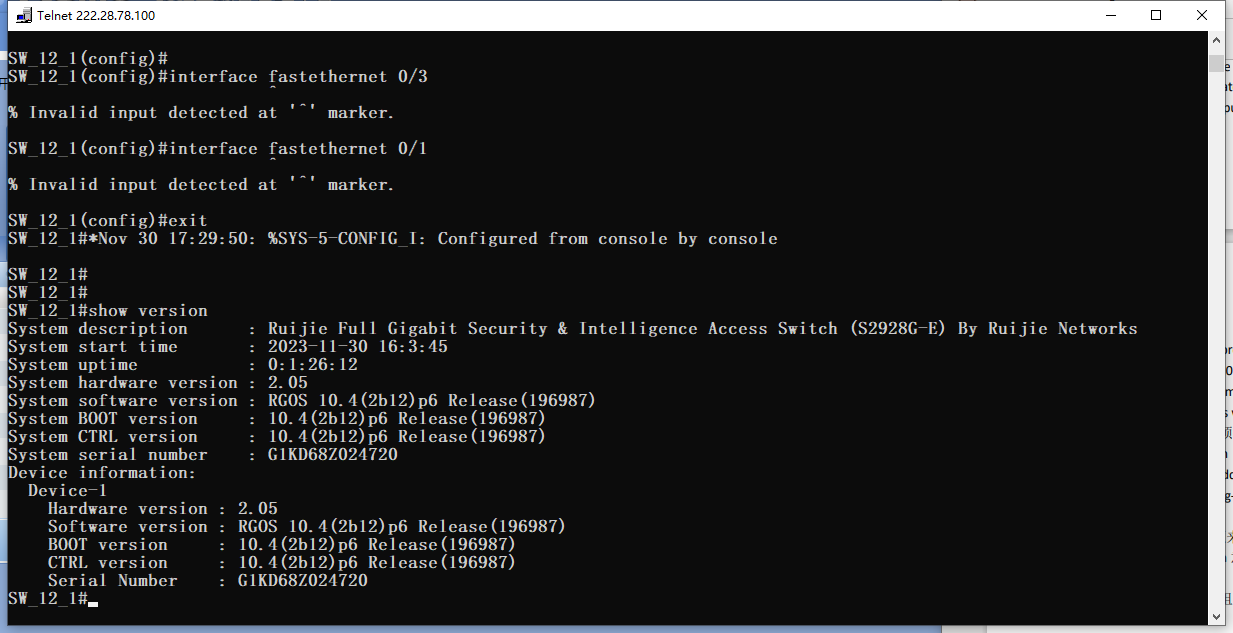
d、通过conf+TAB补全成configure



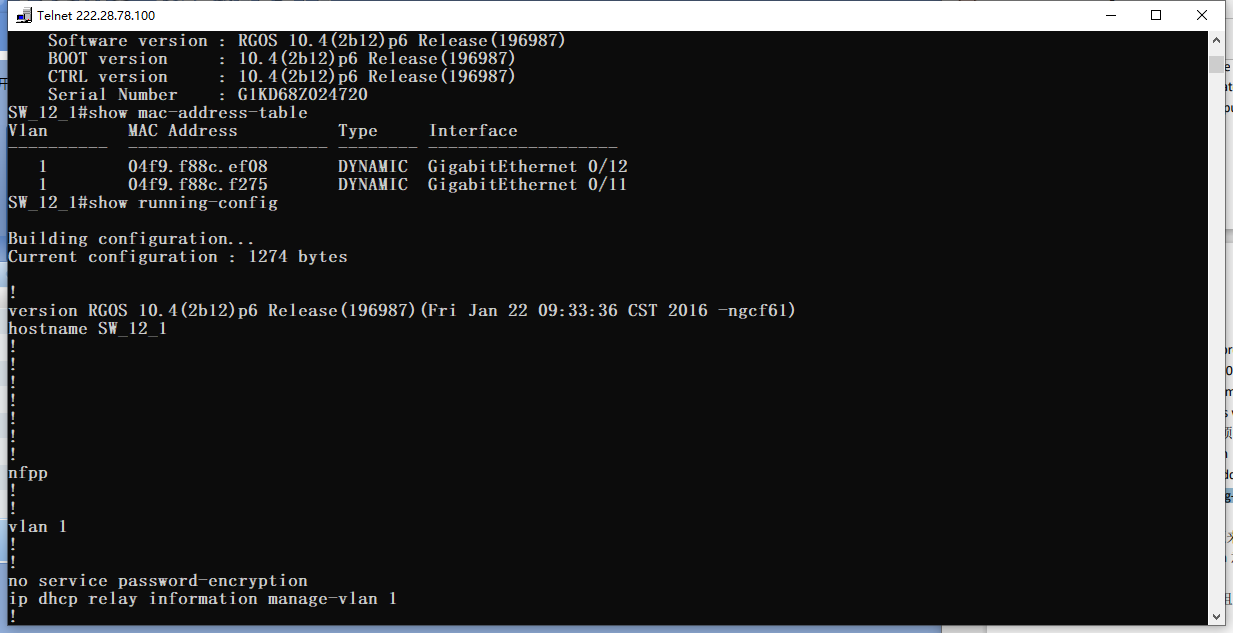
e、通过hostname+name将设备名称修改为name（需要注意该操作在特权模式下进行），我这里修改为了SW\_12\_1，表示第十二组的第一个二层交换机。



f、通过show version查看交换机版本信息

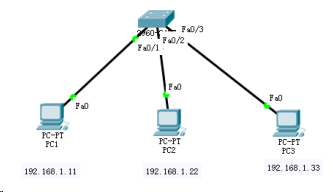


g、通过show mac-address-table查看当前交换机的MAC地址表，通过show running-config查看当前生效的配置

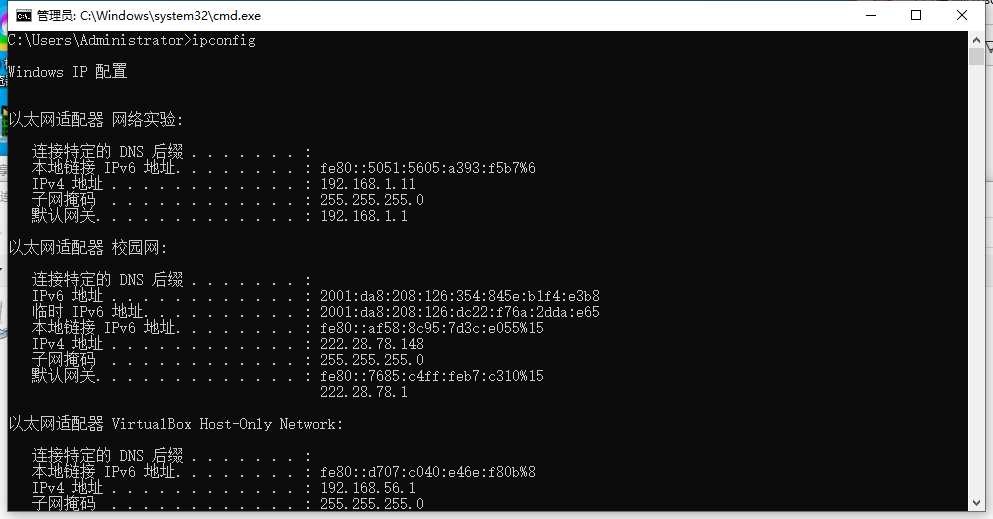
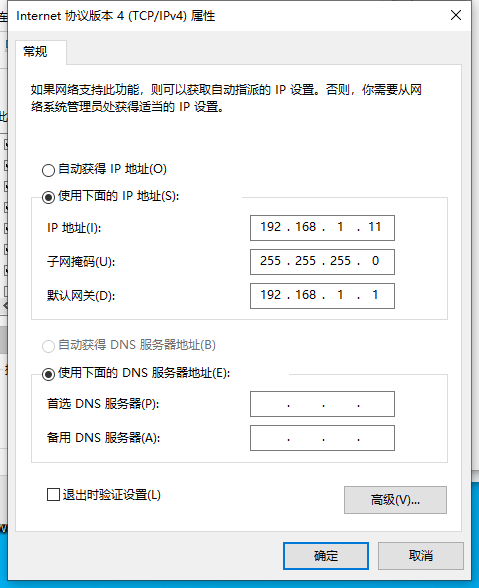


**（二）组建局域网，查看MAC表的生成过程**

在这个过程中，搭建局域网的网络拓扑结构如下所示：



（1）配置“网络时延”网卡地址，采用静态地址，在网络-属性下进行设置，设置完毕后通过cmd命令ipconfig查看。



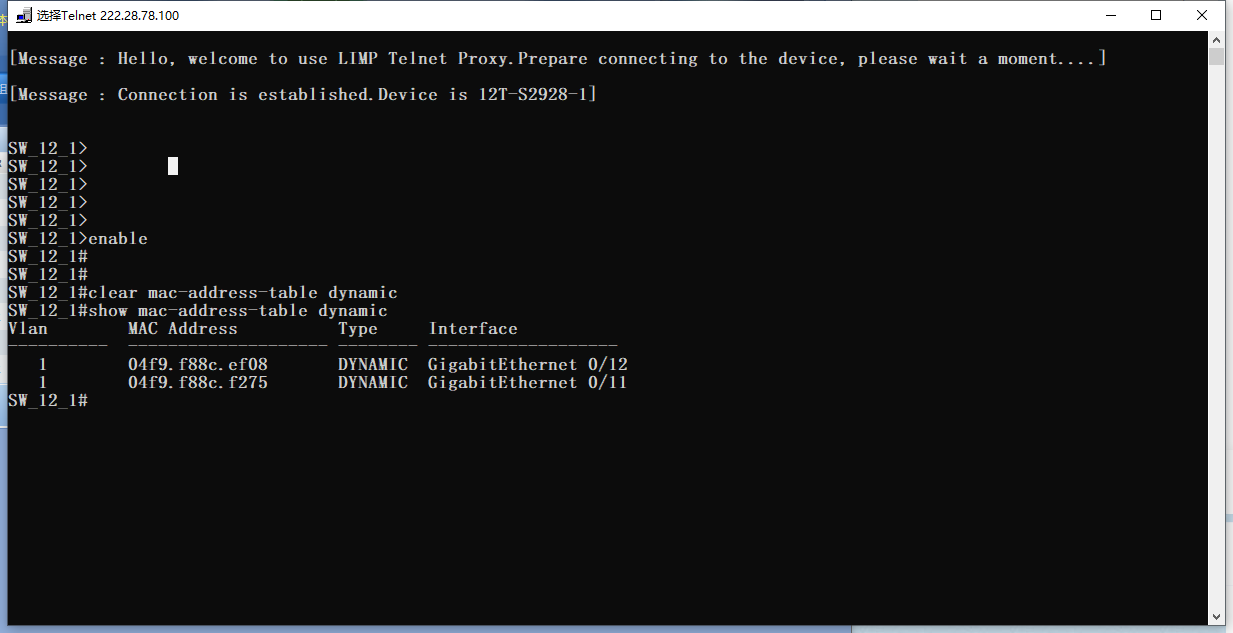
（2）将两台PC与一台交换机相连

a、通过clear mac-address-table命令清除MAC表内容

b、通过show mac-address-table命令查看MAC表为空

（3）PC1 ping PC2

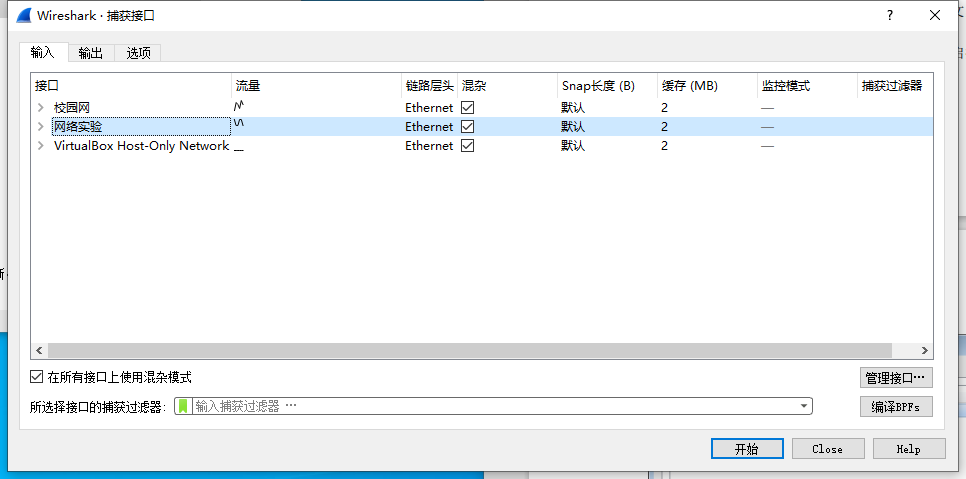
（4）再次过show mac-address-table命令查看MAC表内容如下：



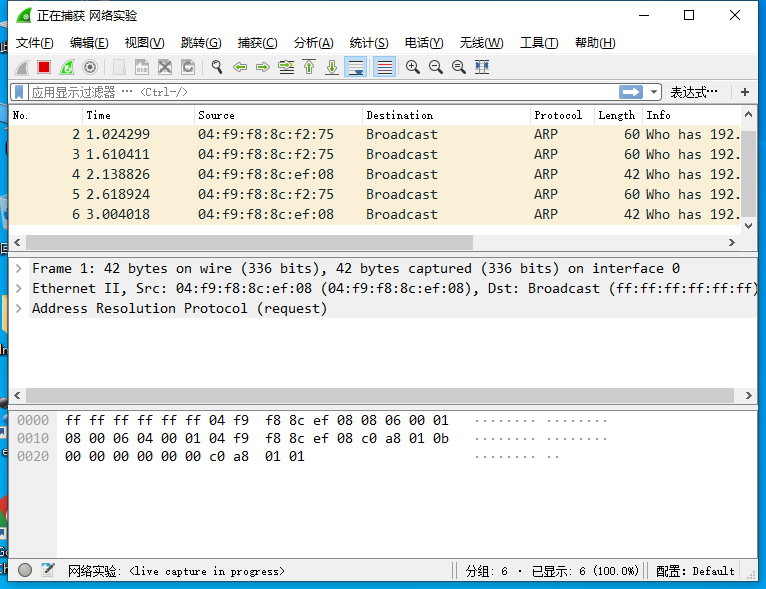
PC1 发出的报文，首先到达交换机，交换机从数据帧的源地址学习，完成 F0/1-MAC1 的映射，PC2 回复的报文，到达交换机后，交换机完成 F0/2-MAC2 的映射。在报告后续的总结中会对其进行分析。

（5）Wireshark抓包分析

在wireshark软件下，修改捕获网卡，选择“网络实验”，然后准备进行两次抓包。

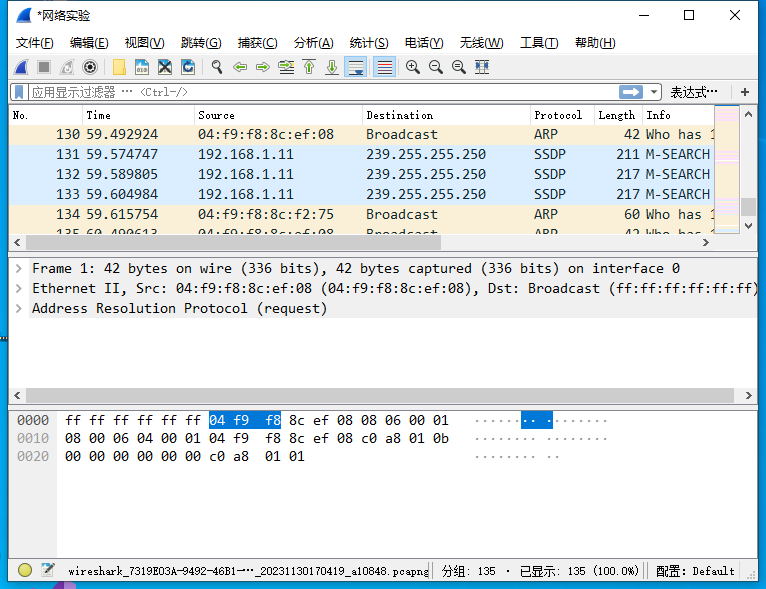


a、第一次抓包时，直接启动抓包，在抓包期间执行PC1 ping PC2的操作，停止抓包得到如下的ICMP报文。



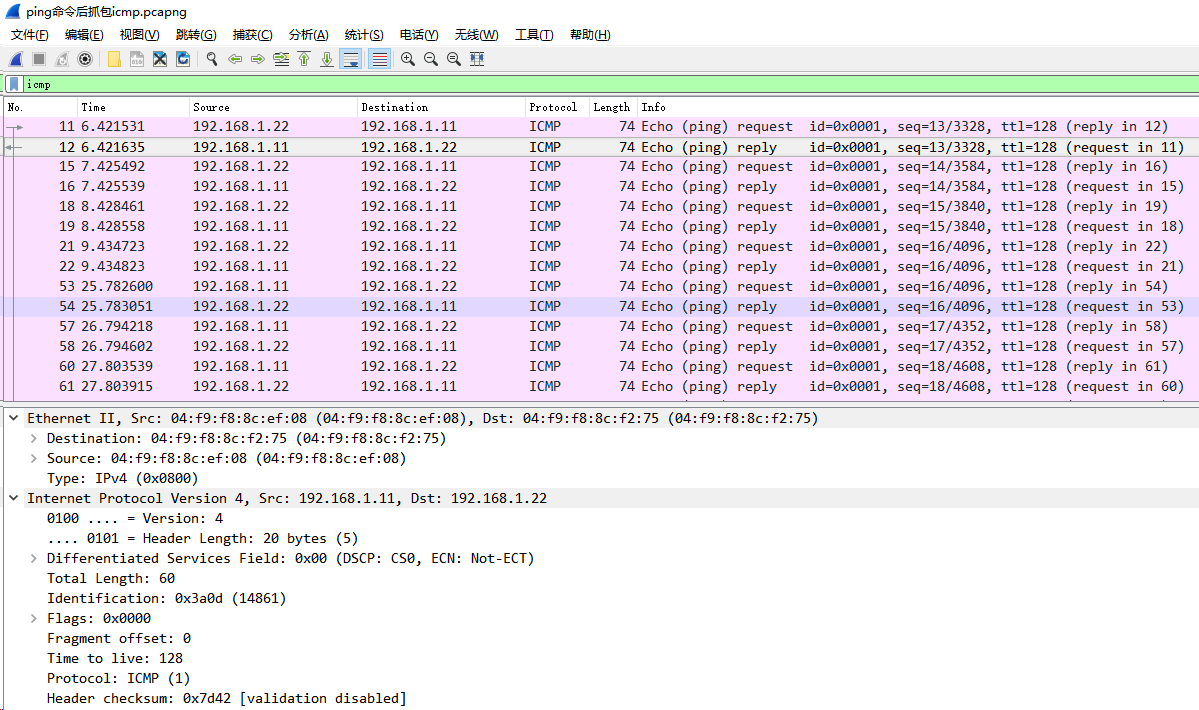
b、在命令行中执行ARP -d命令，开始抓包，在抓包期间执行PC1 ping PC2的操作，停止抓包得到如下的ICMP报文。

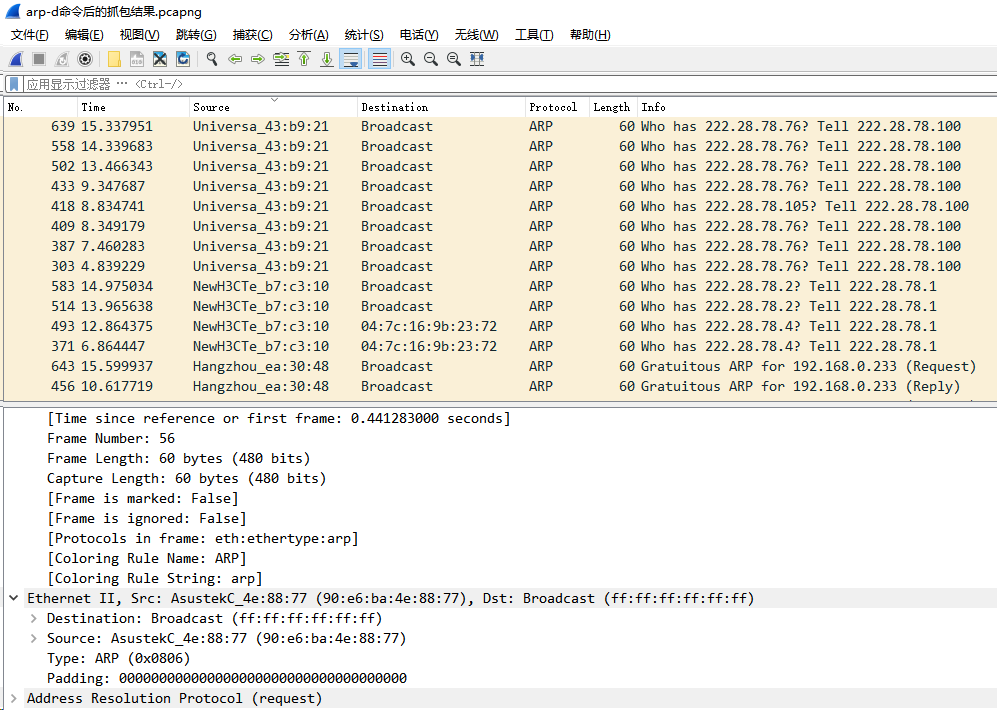




**实验数据：**

由于本次实验主要熟悉交换机的配置过程、常用命令以及MAC表的形成过程，因此本次实验中得到的实验数据主要是wireshark数据包。受限于报告篇幅，不能够全部展示数据包内容，因此只展示部分截图。在后续的实验数据处理环节，会对数据包进行简要分析。





**实验数据处理：**

在这个环节，将对所捕获的某个数据包的关键内容进行简要分析。

|  |
| --- |
| Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  Interface id: 0 (\Device\NPF\_{7319E03A-9492-46B1-AFA7-B0A0EAAFB72B})  Interface name: \Device\NPF\_{7319E03A-9492-46B1-AFA7-B0A0EAAFB72B}  Encapsulation type: Ethernet (1)  Arrival Time: Nov 30, 2023 17:04:26.271453000 中国标准时间  [Time shift for this packet: 0.000000000 seconds]  Epoch Time: 1701335066.271453000 seconds  [Time delta from previous captured frame: 0.000104000 seconds]  [Time delta from previous displayed frame: 0.000104000 seconds]  [Time since reference or first frame: 6.421635000 seconds]  Frame Number: 12  Frame Length: 74 bytes (592 bits)  Capture Length: 74 bytes (592 bits)  [Frame is marked: False]  [Frame is ignored: False]  [Protocols in frame: eth:ethertype:ip:icmp:data]  [Coloring Rule Name: ICMP]  [Coloring Rule String: icmp || icmpv6]  Ethernet II, Src: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08), Dst: 04:f9:f8:8c:f2:75 (04:f9:f8:8c:f2:75)  Destination: 04:f9:f8:8c:f2:75 (04:f9:f8:8c:f2:75)  Source: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08)  Address: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08)  .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)  .... ...0 .... .... .... .... = IG bit: Individual address (unicast)  Type: IPv4 (0x0800)  Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.22  0100 .... = Version: 4  .... 0101 = Header Length: 20 bytes (5)  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 60  Identification: 0x3a0d (14861)  Flags: 0x0000  Fragment offset: 0  Time to live: 128  Protocol: ICMP (1)  Header checksum: 0x7d42 [validation disabled]  [Header checksum status: Unverified]  Source: 192.168.1.11  Destination: 192.168.1.22  Internet Control Message Protocol  Type: 0 (Echo (ping) reply)  Code: 0  Checksum: 0x554e [correct]  [Checksum Status: Good]  Identifier (BE): 1 (0x0001)  Identifier (LE): 256 (0x0100)  Sequence number (BE): 13 (0x000d)  Sequence number (LE): 3328 (0x0d00)  [Request frame: 11]  [Response time: 0.104 ms]  Data (32 bytes) |

这个Wireshark捕获的数据包是一个ICMP的回显应答。

**（1）Ethernet II帧头：**

源MAC地址：04:f9:f8:8c:ef:08

目标MAC地址：04:f9:f8:8c:f2:75

以太网类型：IPv4 (0x0800)

**（2）IPv4头部：**

源IP地址：192.168.1.11

目标IP地址：192.168.1.22

协议类型：ICMP (1)

**（3）ICMP协议：**

类型：0（回显应答）

代码：0

校验和：0x554e

标识符：1（0x0001）

序列号：13（0x000d）

数据：32字节

**（4）时间信息：**

抵达时间：Nov 30, 2023 17:04:26.271453000 中国标准时间

捕获到达时间：1701335066.271453000 秒

帧长度：74字节

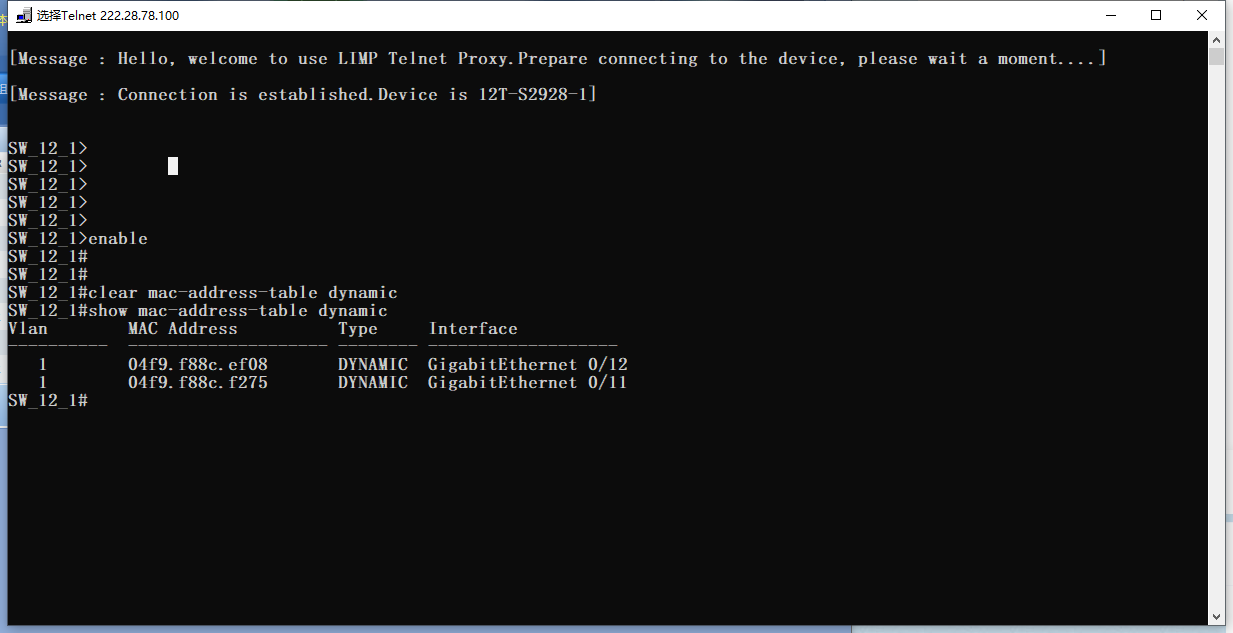
捕获长度：74字节

捕获接口：\Device\NPF\_{7319E03A-9492-46B1-AFA7-B0A0EAAFB72B}

**实验结果与分析：**

在这个环节，对实验指导书中的总结与分析进行回答。

**（1）给出交换机MAC地址表的截图，交换机MAC地址表是如何建立的？**



当交换机接收到一个帧时，它会查看帧中的源MAC地址，并记录该地址与接收到该帧的端口的对应关系。如果这个源MAC地址已经存在于MAC地址表中，交换机会更新该条目的时间戳。如果该源MAC地址不在表中，交换机会添加一个新的表项。

当交换机接收到一个帧时，它会查看目标MAC地址，并在MAC地址表中查找对应的条目。如果找到了，交换机就知道了要将帧发送到哪个端口。如果在表中找不到目标MAC地址的对应条目，交换机会将帧广播到所有端口（除了接收到该帧的端口之外），以确保目标设备能够收到。

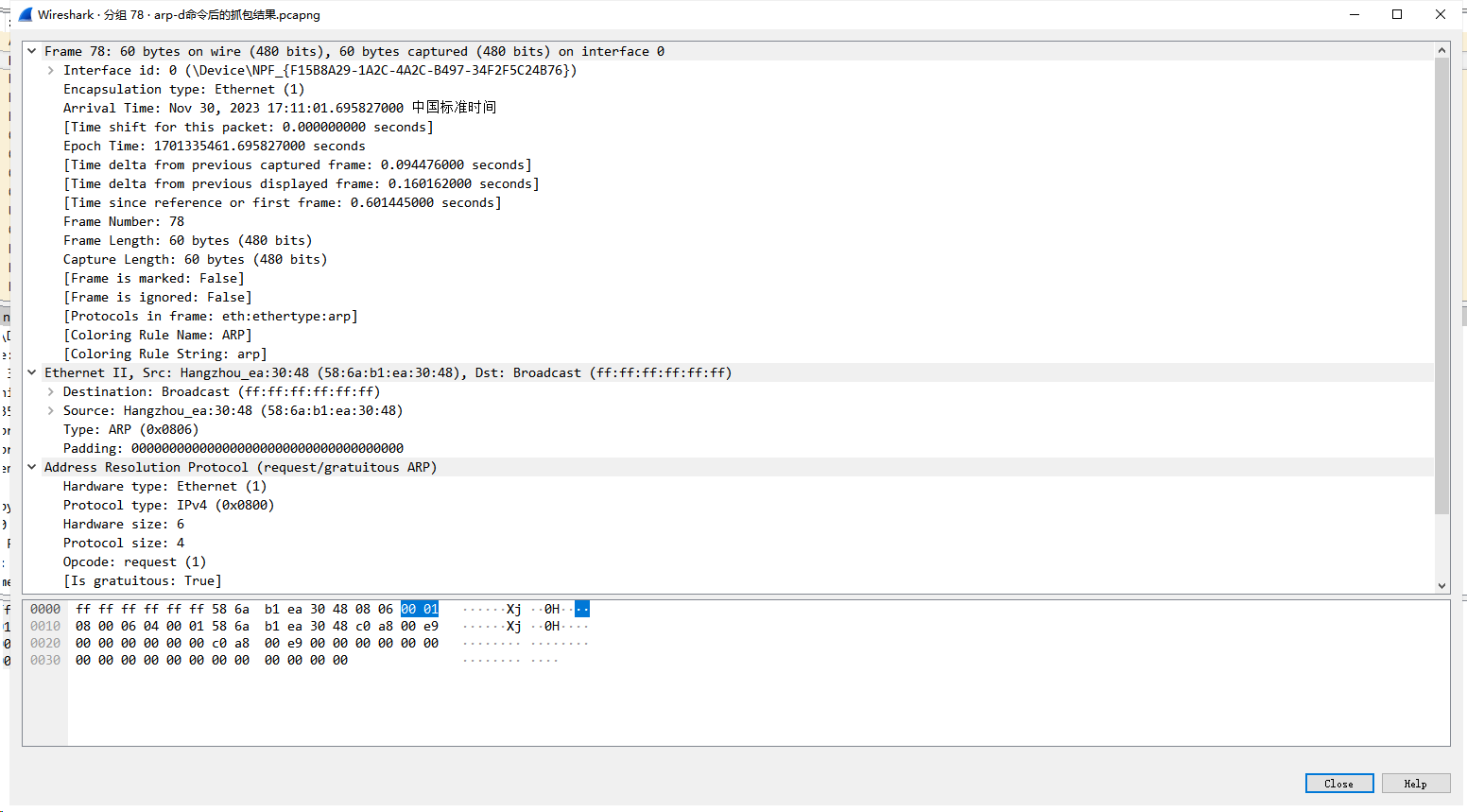
**（2）使用wireshark软件抓包，抓取一组ICMP请求和应答的报文，完成下表。**

使用之前的操作中抓取到的报文进行该问题的解答，具体分析过程在数据处理环节已经进行。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 请求报文序号 | 源MAC | 目的MAC | 源IP | 目的IP | Type | Code |
| 11 | 04:f9:f8:8c:f2:75 | 04:f9:f8:8c:ef:08 | 192.168.1.22 | 192.168.1.11 | IPv4 (0x0800) | Echo (ping) request (Type: 8, Code: 0) |
| 回答报文序号 | 源MAC | 目的MAC | 源IP | 目的IP | Type | Code |
| 12 | 04:f9:f8:8c:ef:08 | 04:f9:f8:8c:f2:75 | 192.168.1.11 | 192.168.1.22 | IPv4  (0x0800) | Echo (ping) reply (Type: 0, Code: 0) |

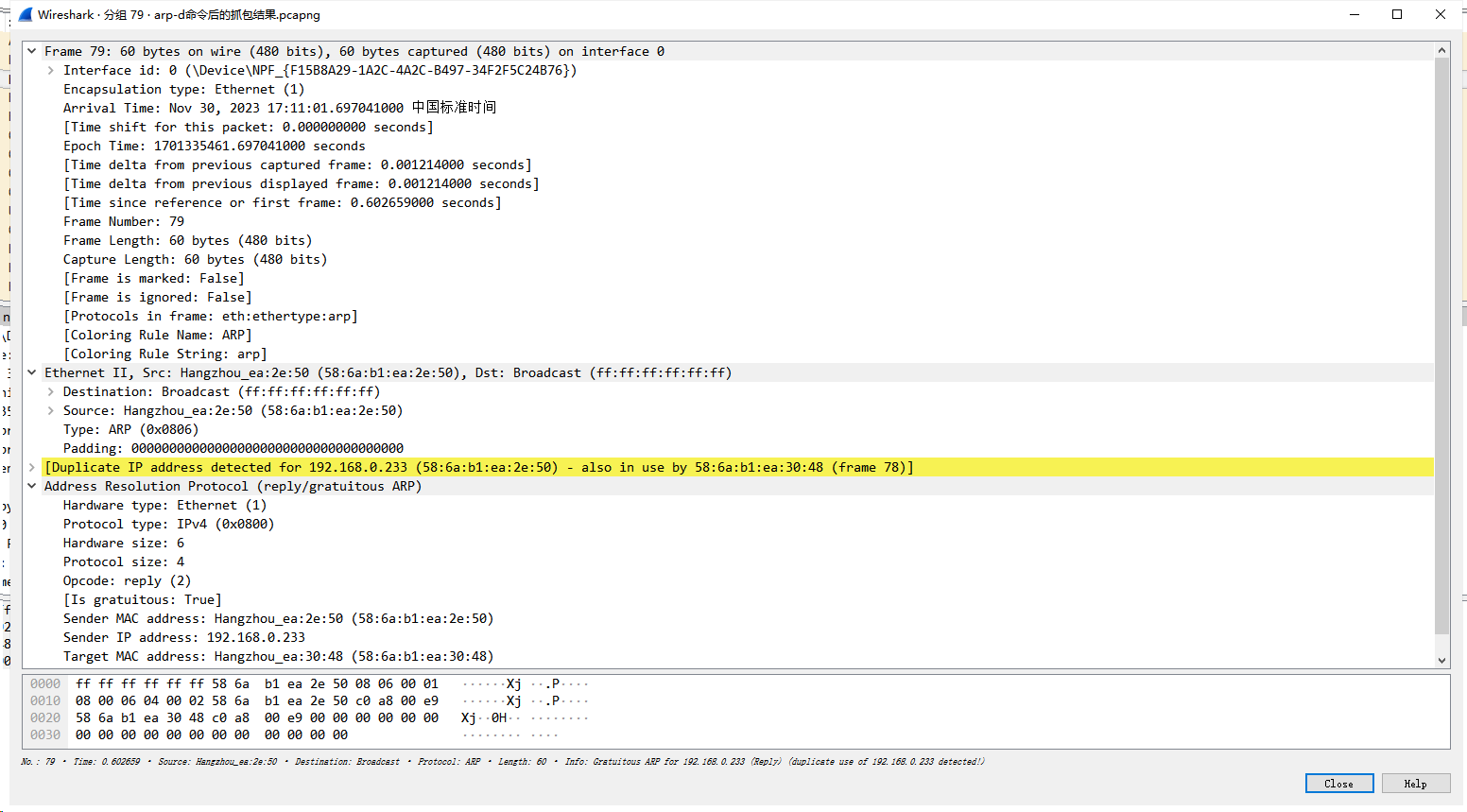
**（3）对通过arp -d命令后的ping命令住区的ARP数据包进行分析。**

a、展开第一条ARP请求报文，截图显示链路层和ARP协议详细信息



目的MAC是ff:ff:ff:ff:ff:ff ，说明arp请求是广播帧；源MAC地址是Hangzhou\_ea:30:48 (58:6a:b1:ea:30:48) ，说明是设备Hangzhou\_ea:30:48 (58:6a:b1:ea:30:48) 发出的ARP请求。ARP请求帧询问IP地址为192.168.0.233 对应的MAC地址。

b、展开第二条ARP应答报文，截图显示链路层和ARP协议详细信息



源MAC地址是Hangzhou\_ea:2e:50 (58:6a:b1:ea:2e:50)，说明是设备Hangzhou\_ea:2e:50 (58:6a:b1:ea:2e:50) 发出的arp应答。目的地址是ff:ff:ff:ff:ff:ff 说明arp应答是广播 帧， arp请求的IP地址为192.168.0.233 所对应的MAC地址为Hangzhou\_ea:30:48 (58:6a:b1:ea:30:48) 。

**北京科技大学实验报告**

学院：计通学院 专业：信息安全 班级：信安211

姓名：李晓坤 学号：U202141863 实验日期： 2023 年 11 月30 日

**实验名称：**

实验二：广播风暴与生成树

**实验目的：**

（1）了解广播风暴产生的原因

（2）掌握交换机生成树的配置方法

（3）理解根交换机和根端口选举规则

**实验仪器：**

交换机1台

主机2台

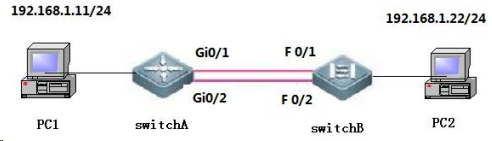
**实验原理：**

为了提高网络的可靠性和健壮性，通常设置冗余链路，即备份链路。当主链路出现故障时，备份链路自动启动，避免网络发生单点故障。但这也带来一个问题，就是在二层网络中产生了环路，数据帧会在网络中循环，占用带宽资源，从而形成广播风暴，最终导致链路中断。

生成树协议在网络中提供冗余链路并解决交换网络中的环路问题。常使用SPA生成树算法，在网络中生成没有环路的树形网络。该算法将交换网络冗余的备份链路逻辑上断开，当主链路出现故障时，自动切换到备份链路上，保证数据正常转发。

生成树协议常见的版本有STP、RSTP、MSTP。其中，STP收敛时间长，RSTP在STP上增加了替换端口和备份端口，分别作为根端口和指定端口的冗余端口，从而实现快速收敛。

本实验用到的网络拓扑结构如下：



**实验内容与步骤：**

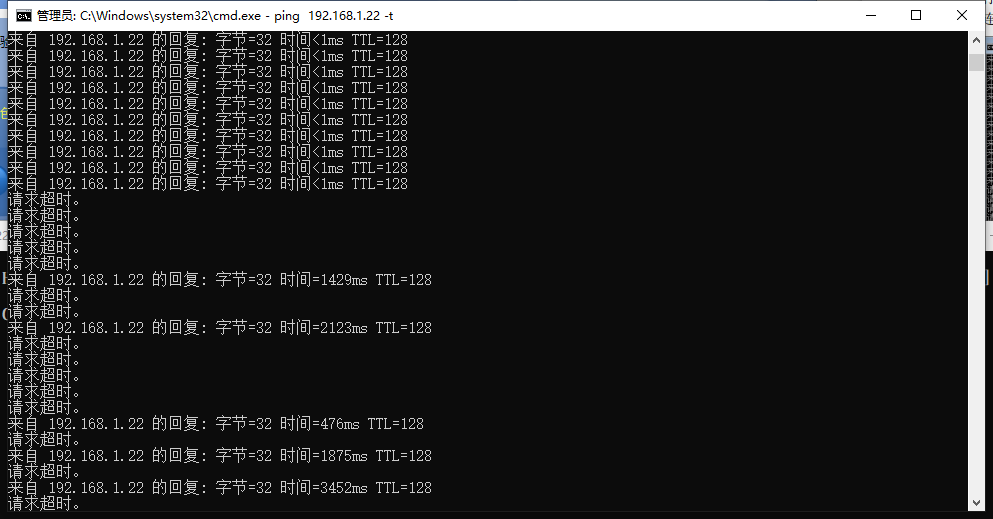
（1）配置两台交换机的主机名、管理IP地址和Trunk

该环节主要通过特权模式下的hostname、interface等命令进行设置。主要是将两台交换机分别重命名为L2-SW、L3-SW；ip地址设置为192.168.1.2、192.168.1.1；子网掩码设置为255.255.255.0；端口模式设置为Trunk。

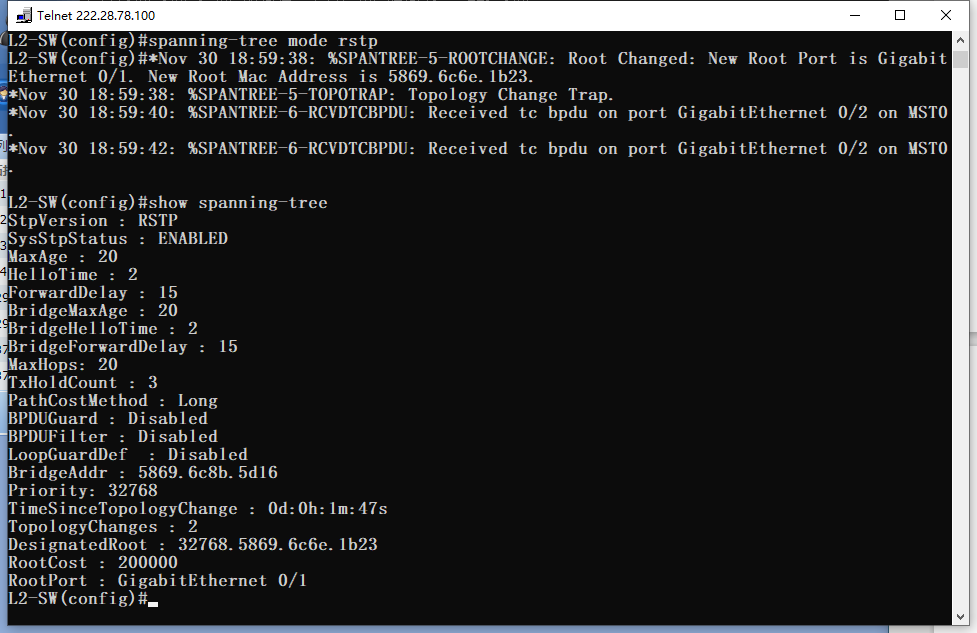
（2）接线，交换机之间将G0/1- F0/1相连，二层交换机将G0/5与PC1机相连，三层交换机将F0/5与PC2机相连；G0/2- F0/2稍后再连接。具体的连接方式与前文的网络拓扑结构相同。

（3）不启用生成树协议，PC1 ping PC2，能够连通。

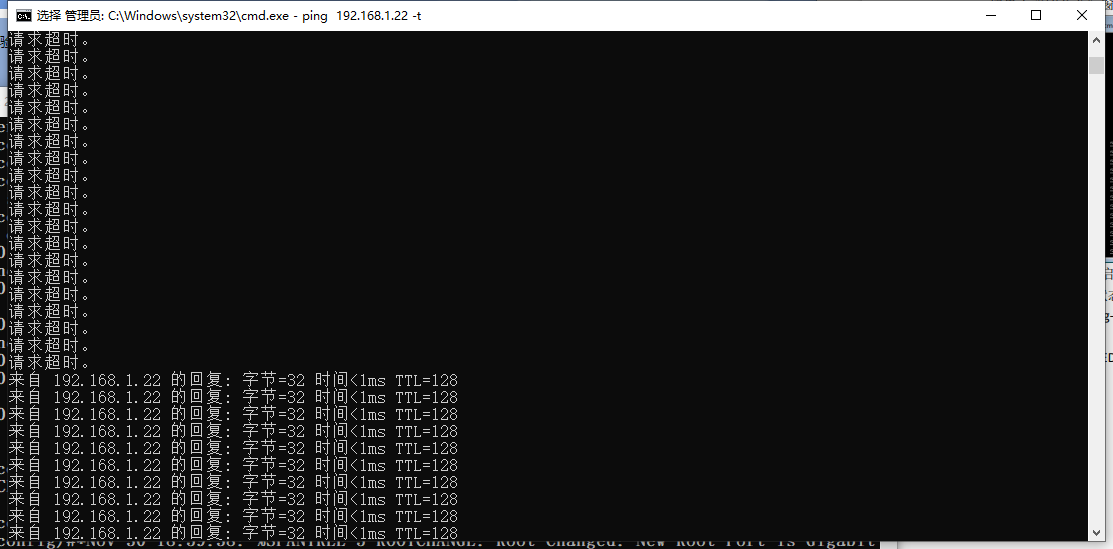
（4）此时，启用备份链路，一段时间后观察到请求超时，产生广播风暴现象。



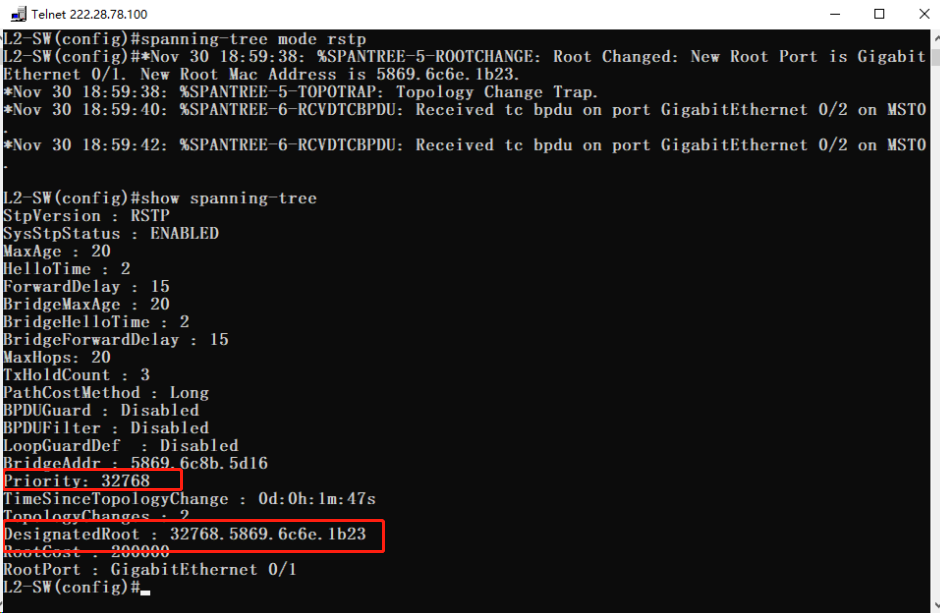
（5）接下来通过spanning-tree和spanning-tree mode rstp命令启用生成树协议并修改生成树协议类型为RSTP。



（6）一段时间后观察到链路由中断变为连通。



（7）通过show spanning-tree 命令查看两台交换机上的生成树工作状态，记录此时的priority字段。

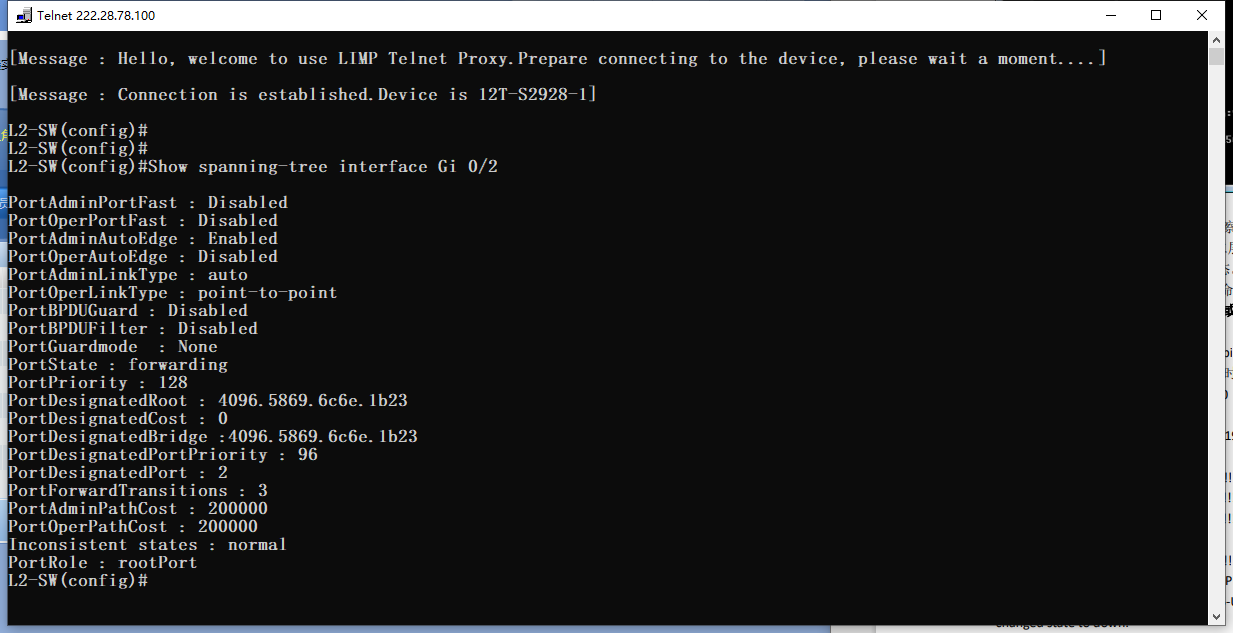


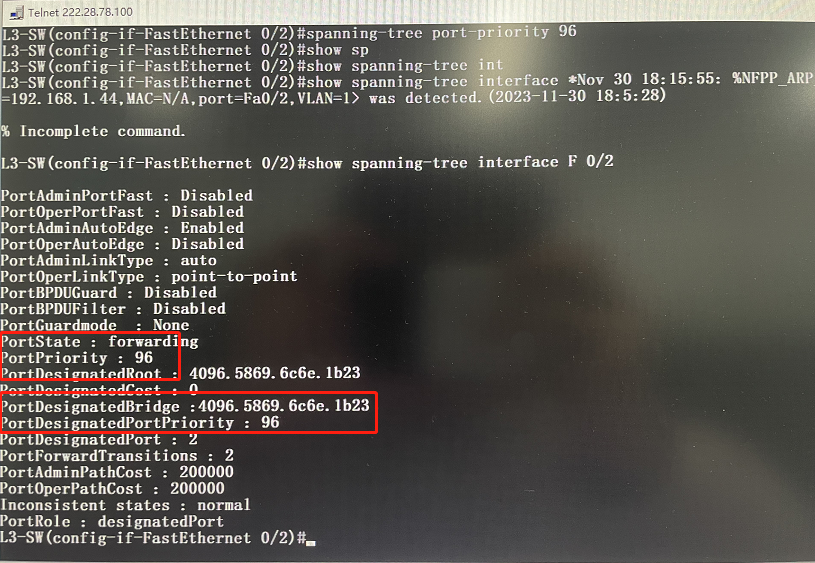
可以看到两台交换机已经正常启用RSTP协议，两台交换机的桥优先级都是32768，然后比较MAC地址，L2\_5869.6c8b.5d16<L3\_5869.6c8b.5d20，由于 MAC 地址较小，L2-SW被选举为根桥，L3\_SW在自己的生成树设置根桥为L2-SW。两台交换机上计算路径成本的方法都是长整型。

根桥选定后，其他交换机都成为非根桥，每台交换机需要选举一条到根桥的根路径，相应的端口就是根端口，若有多条路径到达根桥，比较各条路径累加的开销 COST，带宽大的链路开销值低，累加值 COST 最低得路径是根路径。L3-SW上Fa0/1和Fa0/2都与根桥相连，路径开销也相同，端口号Fa0/1比Fa0/2小，Fa0/1被选为根端口。所有根端口都为指定端口，参与数据的转发，Fa0/2端口为非指定端口，将被阻塞，无法装法数据。

（8）指定三层交换机为根网桥，指定二层交换机的 Gi0/2 端口为根端口。

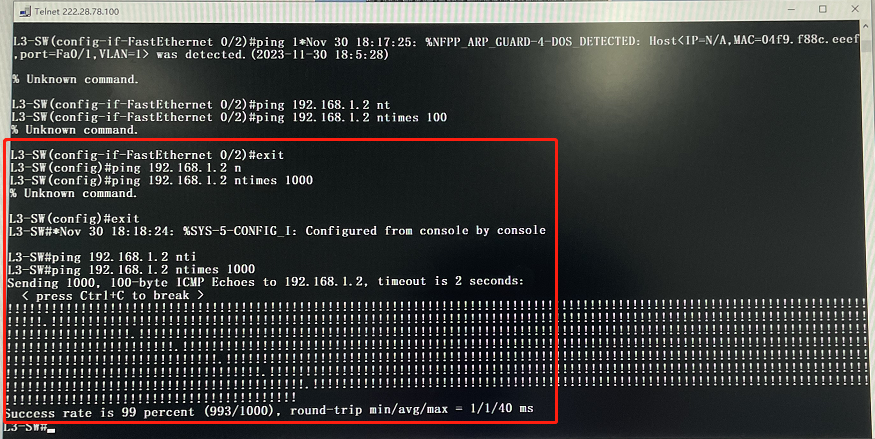
这一操作主要通过命令spanning-tree priority xxxx进行设置优先级，设置完毕后通过命令show spanning-tree进行查看。

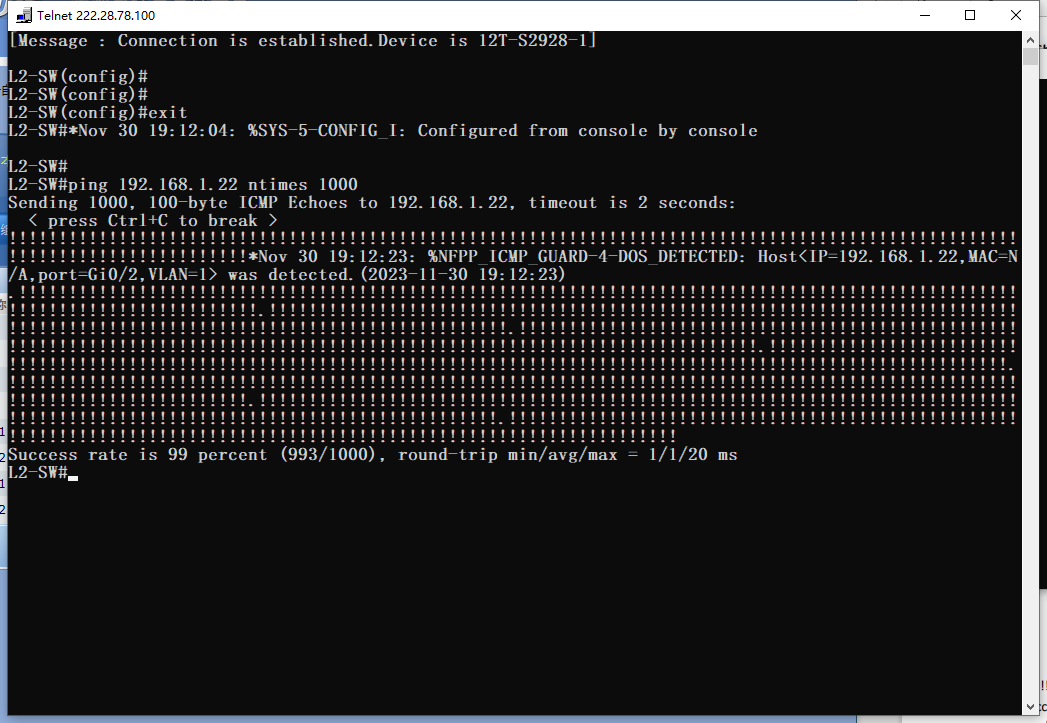




（9）验证配置，在三层交换机 L3-SW上长时间的ping二层交换机L2-SW，其间断开L2-SW上的根端口Gi0/2，这时观察替换端口能够在多长时间内成为转发端口。

该操作主要通过例如ping 192.168.1.2 ntimes 1000进行。





从中可以看到替换端口变成转发端口的过程中，丢失了7个 ping 包，中断时间小于60ms。

当网络主链路发生故障时，网络拓扑结构会发生变化，处于阻塞状态的端口，通过 BPDU报文侦听了解到这一变化，端口状态立刻从阻塞转变到学习状态，完成 MAC地址表的建立后，端口转变为转发状态。一个端口从禁用到转发大约需要50 秒，用于生成树协议了解整个网络的拓扑结构。

**实验数据：**

该实验为验证性实验，已将中间过程以图片的形式进行记录，具体见前述的报告内容。

**实验数据处理：**

由于实验数据均为图片，无需处理，在实验过程中已将其进行分析。

**实验结果与分析：**

该环节解释实验指导书中的思考问题部分。

**（1）广播风暴产生的原因是什么？它有什么危害？**

广播风暴是网络中发生广播消息传播过度，导致网络中的设备被不必要的广播消息淹没的现象。产生广播风暴的主要原因包括：

a、网络环路：当网络中存在环路时，广播消息可能在网络中无限循环，导致广播风暴。

b、网络设备故障：某个网络设备故障可能导致它不正确地转发广播消息，使得广播消息在网络中无限传播。

c、网络设计不当：不良的网络设计或配置错误可能导致广播消息无法正确处理，从而引发广播风暴。

广播风暴可能导致以下危害：

a、网络拥塞：大量不必要的广播消息会占用网络带宽，导致网络拥塞，影响正常的数据传输。

b、性能下降：广播风暴会导致网络设备过度负荷，使其性能下降，影响正常的网络通信。

c、服务不可用：在极端情况下，广播风暴可能导致网络服务不可用，使网络中的设备无法正常通信。

d、网络不稳定：广播风暴可能导致网络不稳定，影响用户正常的网络体验。

**（2）根交换机也称为根桥，它的选举规则是什么？**

a、Bridge ID比较：每个交换机都有一个唯一的Bridge ID，由优先级和MAC地址组成。生成树协议中，Bridge ID越小，优先级越高。交换机会比较所有相邻交换机的Bridge ID，选择具有最小Bridge ID的交换机作为根交换机。

b、优先级比较：如果有多个交换机具有相同的最小Bridge ID，那么将比较它们的优先级。交换机的优先级是一个16位的值，默认值为32768。优先级越低，优先级越高。

c、MAC地址比较：如果两个交换机具有相同的Bridge ID和优先级，那么将比较它们的MAC地址。MAC地址越小，优先级越高。

**（3）非根交换机，怎样选举根端口？**

a、根路径成本比较：非根交换机的每个端口都会计算到根交换机的路径成本。路径成本是从该端口到根交换机的总带宽代价。端口选择具有最低路径成本的路径作为根端口。

b、根路径成本相同的情况下，比较桥优先级：如果存在多个端口具有相同的最低路径成本，那么将比较相邻交换机的桥优先级。桥优先级越低的交换机将优先选择为根端口。

c、桥优先级相同的情况下，比较本地端口优先级：如果相邻交换机的桥优先级相同，那么将比较本地端口的优先级。本地端口优先级越低的端口将被选择为根端口。

d、端口号比较：如果以上都相同，将比较端口号。端口号越小的端口将被选择为根端口。