**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 12 月 7 日

本次实验中的实验三不进行实际操作，通过阅读实验指导书了解相关知识。

**实验名称：**

实验四：跨交换机实现相同VLAN互访

**实验目的：**

（1）了解IEEE802.1q的实现方法

（2）了解交换机接口的trunk模式和access模式

（2）掌握链路聚合的原理及配置方法

**实验仪器：**

二层交换机1台

三层交换机1台

主机4台

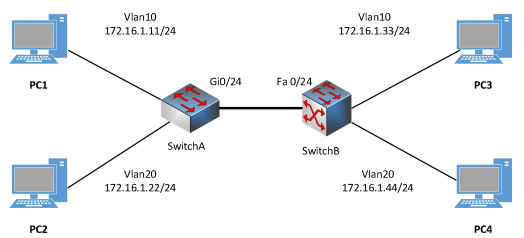
**实验原理：**

交换机通过MAC地址进行数据转发，引入VLAN之后，在MAC地址表中增加vlan信息，也就是交换机会维护一个本地vlan的MAC地址表。在进行数据转发时，首先在同一个vlan的MAC地址表中根据目的MAC查找转发端口，若查找到进行转发；若查找不到则向此vlan的网关发送，由网关向其他网段（vlan）进行转发。

引入Vlan后，交换机的端口按用途分为访问连接端口（Access Link）和干路连接端口（Trunk Link），访问连接端口（Access Link）连接 PC 机，只属于某一个Vlan，Trunk端口连接交换机和交换机，属于所有Vlan共有。这与之前在实验三中学到的基础知识是一致的。

为了提高交换机的传输带宽，可以将交换机之间的多个端口互联，也就是链路聚合，这在我们之前的实验验证广播风暴时介绍过。同样，也可能会出现广播风暴问题，因此要求我们先进行交换机端口聚合的配置，然后再进行连线。

本次实验要实现两个交换机之间两对端口的聚合，属于vlan 10的PC1和PC3之间能连通，属于vlan 20的PC2和PC4之间能连通，PC1和PC4之间不能连通。下图是本实验的网络拓扑结构图。



在实验过程中，我对端口连接模式不熟悉（理论课上目前还没有讲授），因此我查阅资料([什么是VLAN？VLAN是如何工作的？ - 华为 (huawei.com)](https://info.support.huawei.com/info-finder/encyclopedia/zh/VLAN.html))，学习了关于端口连接模式的相关知识，主要有三种连接模式：access、trunk、hybrid。

**a、access接口**

Access接口一般用于和不能识别Tag的用户终端（如用户主机、服务器）相连，或者不需要区分不同VLAN成员时使用。

在一个VLAN交换网络中，以太网数据帧主要有以下两种形式：

1、无标记帧（Untagged帧）：原始的、未加入4字节VLAN标签的帧。

2、有标记帧（Tagged帧）：加入了4字节VLAN标签的帧。

Access接口大部分情况只能收发Untagged帧，且只能为Untagged帧添加唯一VLAN的Tag。交换机内部只处理Tagged帧，所以Access接口需要给收到的数据帧添加VLAN Tag，也就必须配置缺省VLAN。配置缺省VLAN后，该Access接口也就加入了该VLAN。当Access接口收到带有Tag的帧，并且帧中VID与PVID相同时，Access接口也能接收并处理该帧。在发送带有Tag的帧前，Access接口会剥离Tag。

**b、trunk接口**

Trunk接口一般用于连接交换机、路由器、AP以及可同时收发Tagged帧和Untagged帧的语音终端。它可以允许多个VLAN的帧带Tag通过，但只允许属于缺省VLAN的帧从该类接口上发出时不带Tag（即剥除Tag）。

Trunk接口上的缺省VLAN，有的厂商也将它定义为native VLAN。当Trunk接口收到Untagged帧时，会为Untagged帧打上Native VLAN对应的Tag。

**c、hybrid接口**

Hybrid接口既可以用于连接不能识别Tag的用户终端（如用户主机、服务器）和网络设备（如Hub），也可以用于连接交换机、路由器以及可同时收发Tagged帧和Untagged帧的语音终端、AP。它可以允许多个VLAN的帧带Tag通过，且允许从该类接口发出的帧根据需要配置某些VLAN的帧带Tag（即不剥除Tag）、某些VLAN的帧不带Tag（即剥除Tag）。

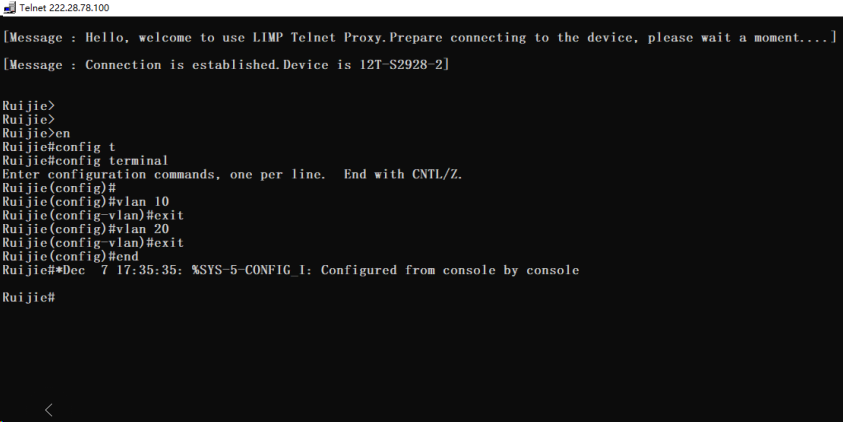
**实验内容与步骤：**

**（1）连线**

将PC1和交换机A的G0/1端口相连；将PC2和交换机A的G0/2端口相连；将PC3和交换机B的F0/1端口相连；将PC4和交换机B的F0/2端口相连。

**（2）创建vlan，两台交换机的配置相同**

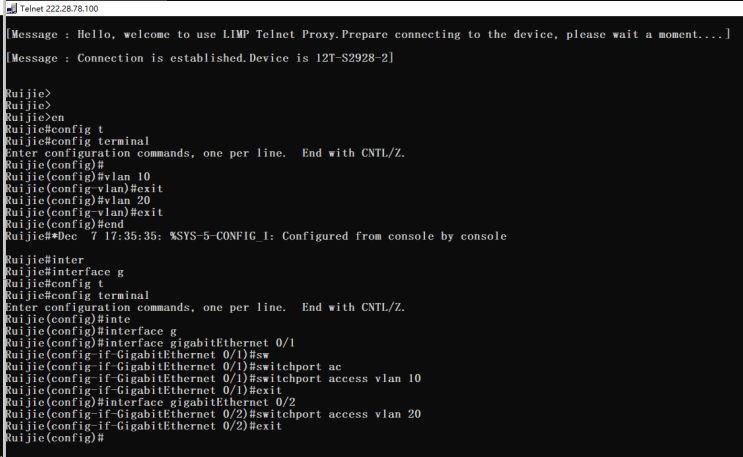
在二层交换机上创建vlan 10和vlan 20这两个VLAN。



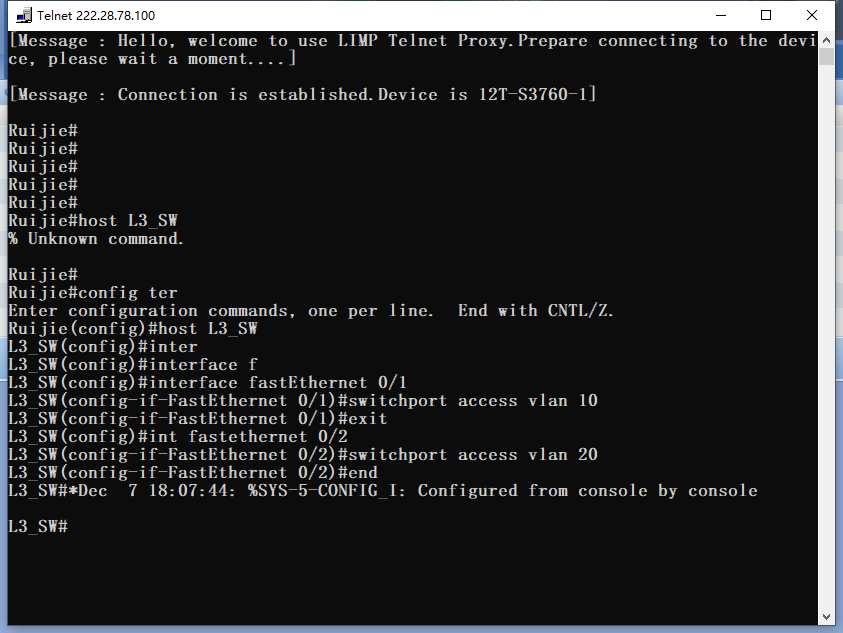
**（3）为VLAN添加端口**

具体来说，二层交换机的G0/1和G0/2分别属于vlan 10和vlan 20；三层交换机的F0/1和F0/2分别属于vlan 10和vlan 20。

在二层交换机上的配置如下。

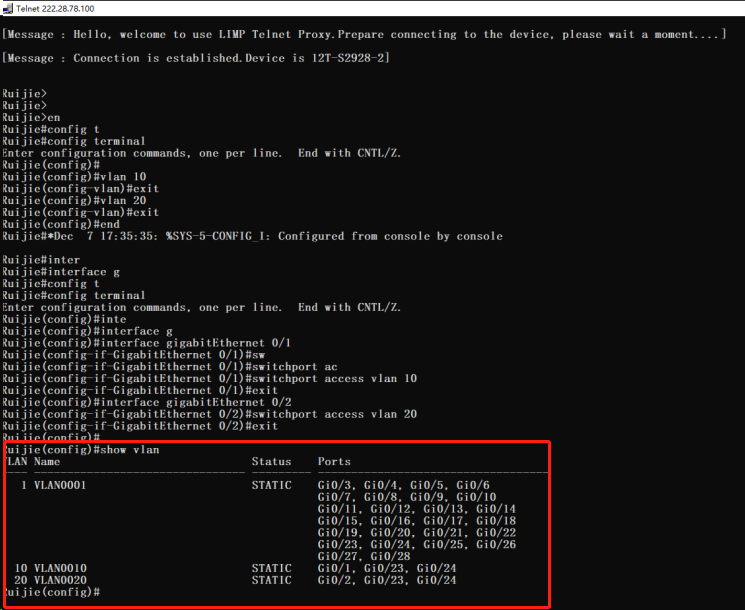


在三层交换机上的配置如下。

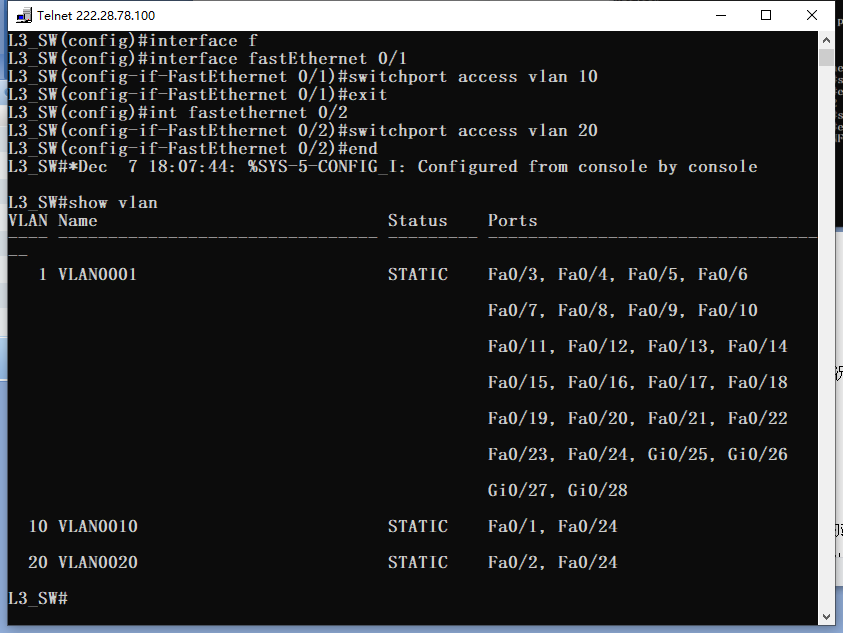


**（4）通过show vlan查看配置情况**

查看二层交换机的配置情况。



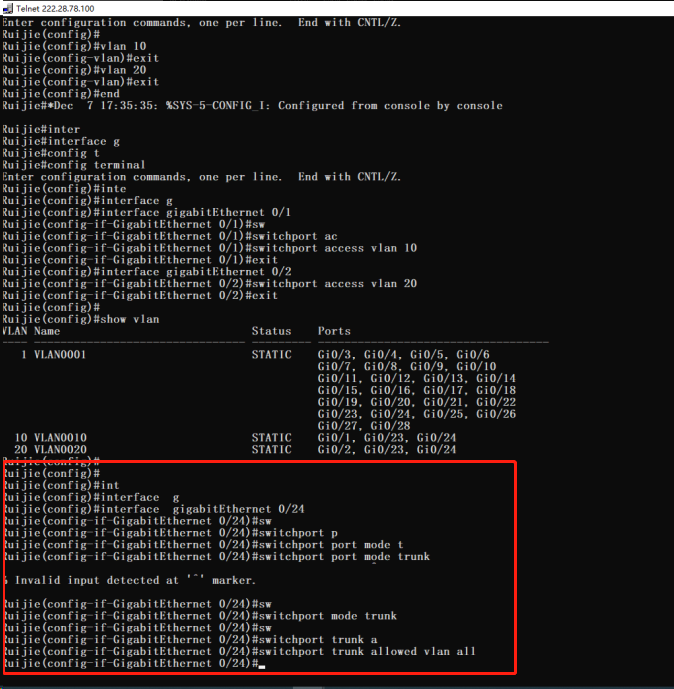
查看三层交换机的配置情况。



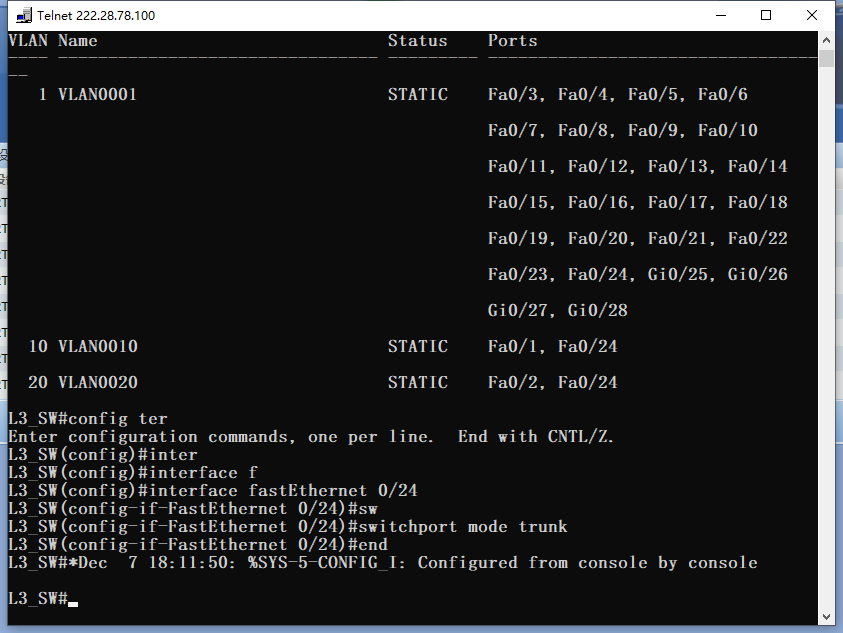
**（5）配置交换机与交换机相连的端口**

主要是配置G0/24和F0/24端口为trunk模式，然后再次查看vlan，会发现trunk被加入vlan 10和vlan 20中。

配置二层交换的的G0/24端口。

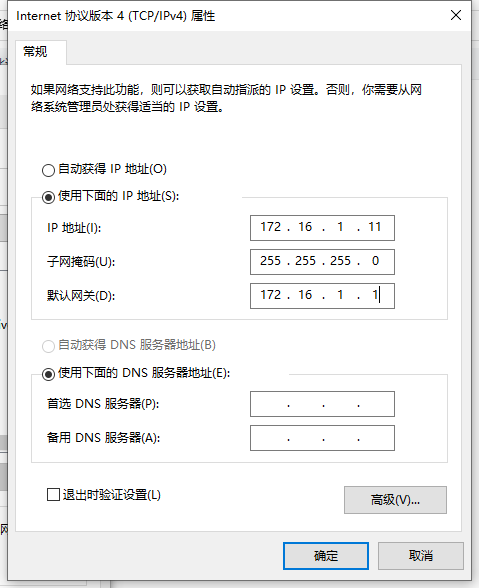


配置三层交换机的F0/24端口。



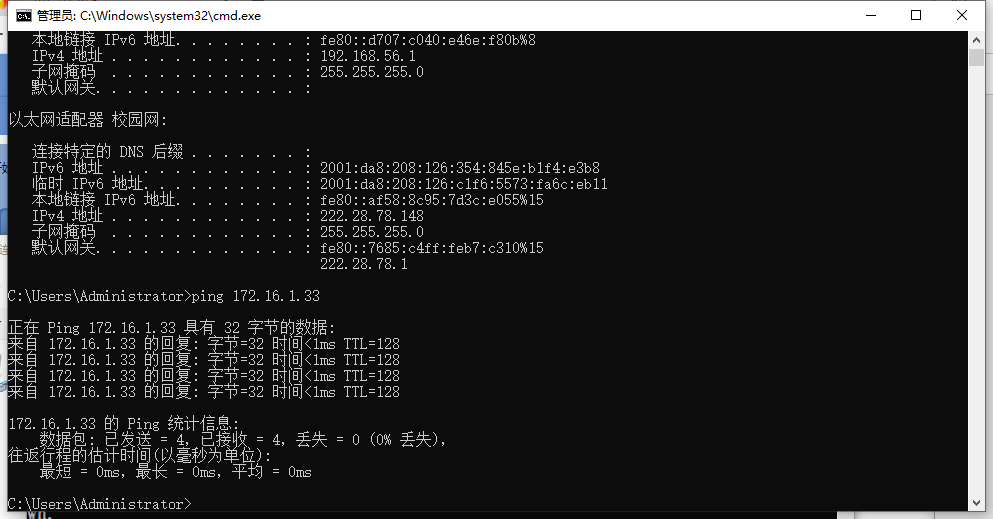
**（6）配置四台主机的网卡**

受限于报告篇幅，这里只展示PC1的网卡配置情况。

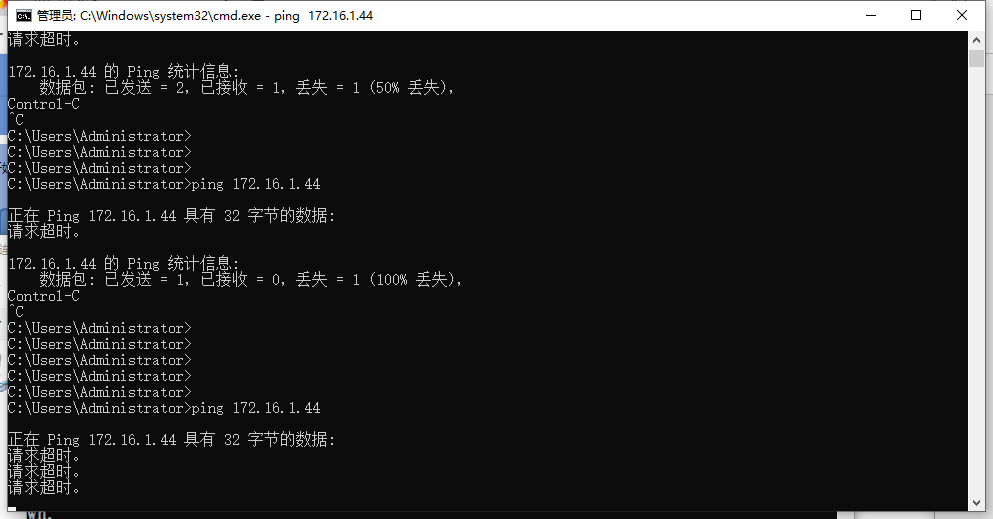


**（7）四台主机之间相互ping，验证连通性**

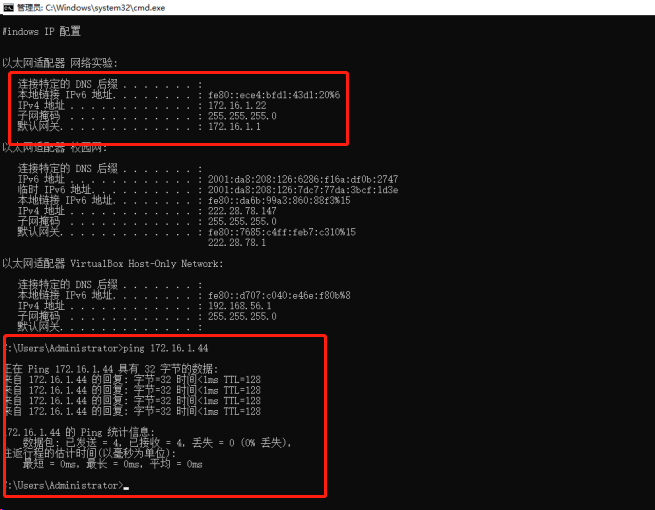
PC1 ping PC3



Pc1 ping pc4



PC2 ping PC4



在这一步中，需要填写一个测试表格，因此将这个表格作为实验数据进行记录，在后续的实验数据环节会进行展示。

**（8）下面进行选作内容，抓取vlan id报文**

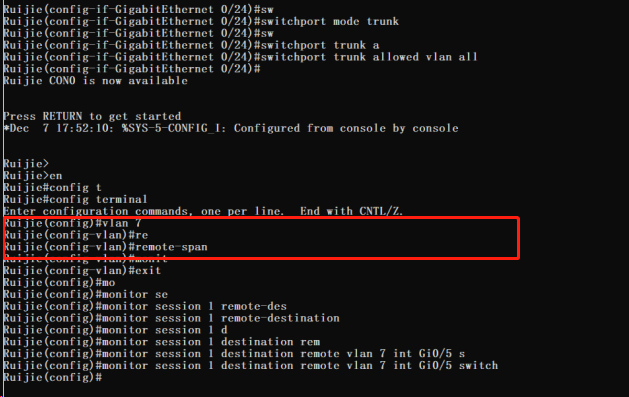
端口镜像分为本地端口镜像和远程端口镜像，一个端口镜像（SPAN）会话只能有一个目的端口（监控端口），但是可以有多个源端口（被监控端口）。这一部分主要是通过对监控口进行抓包，获得vlan报文，并进行分析。

**（9）端口镜像，使用Wireshark分析802.1q报文**

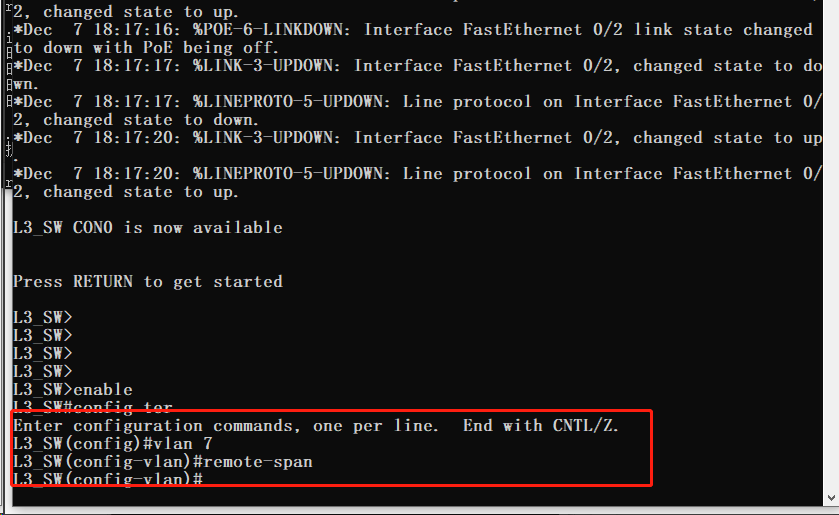
在二层交换机上选定一个端口G0/5作为监控口，将三层交换机的F0/1口，映射到二层交换机的G0/5，监控端口和被监控端口不在同一台设备上，称为远程端口镜像。

**A、交换机A和交换机B创建vlan 7作为远程镜像的网络号，交换机之间相连的模式设置为trunk模式。**

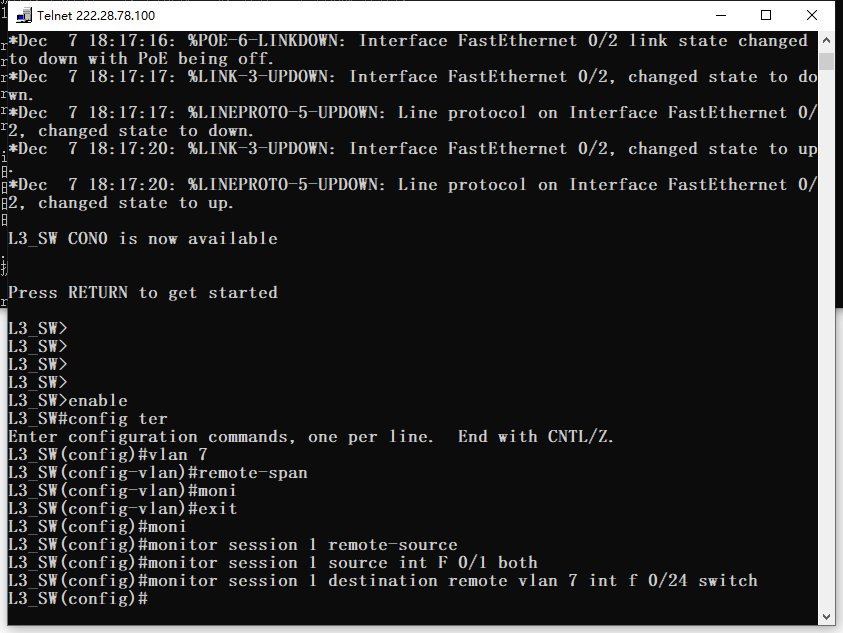
设置二层交换机。



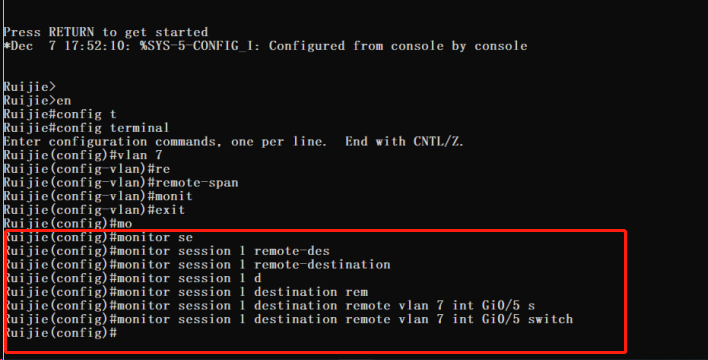
设置三层交换机。



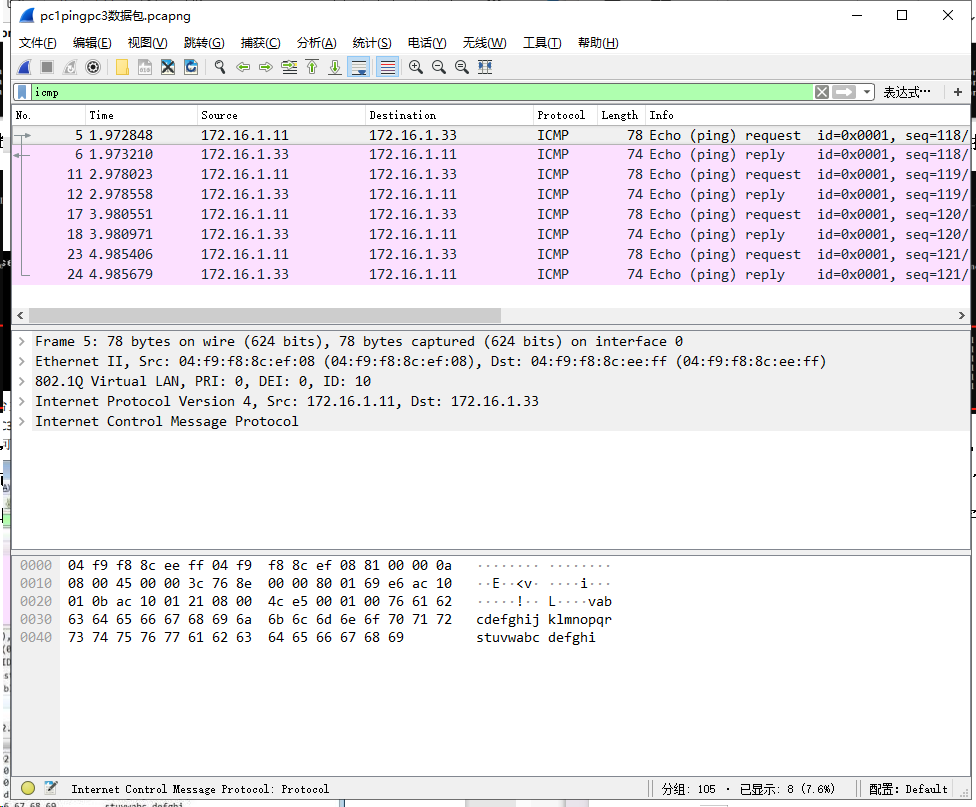
**B、三层交换机上制定源端口F0/1和输出端口F0/24**



**C、二层交换机上选定G0/5作为监控口，为端口镜像的目的端口。**



**D、二层交换机G0/5连接一台主机，打开Wireshark抓包软件，抓取“网络实验”网卡的数据包。执行 PC1pingPC3 操作，它们同属于VLAN10，能够连通，停止抓包，展开报文的数据链路层，可以发现，VLANID字段出现在报文里面。**



针对所抓取的报文，作为实验数据，会在实验数据处理环节进行详细分析。

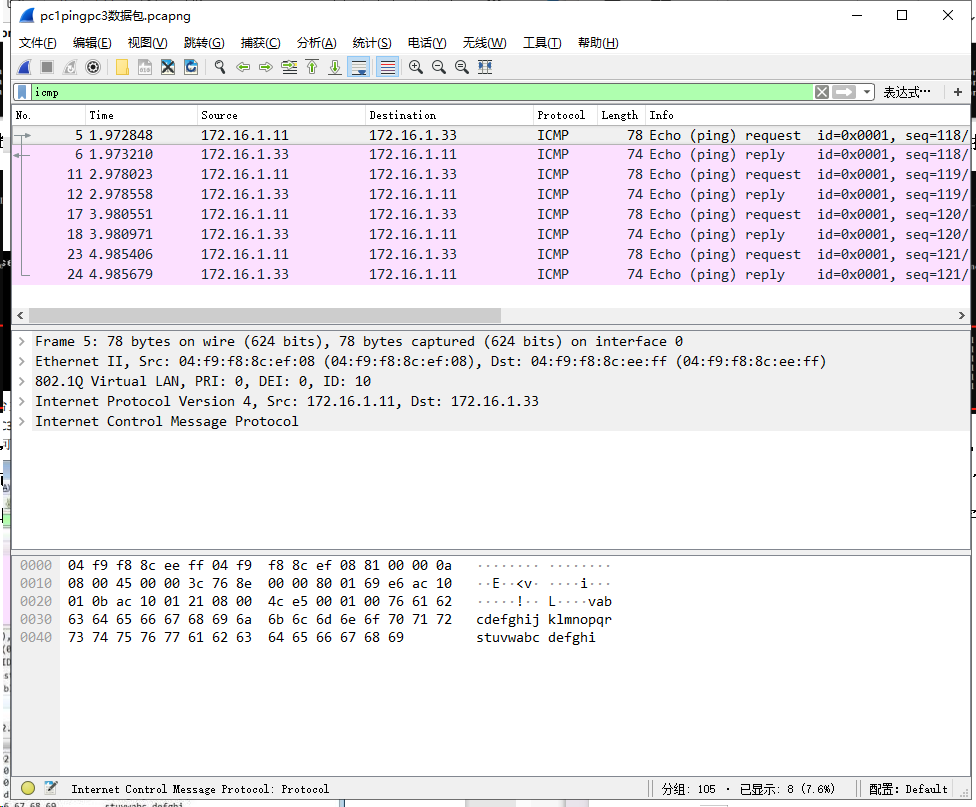
**实验数据：**

**（1）测试连通性实验数据**

实验中测试连通性环节，需要PC1-PC4之间相互测试连通性，将测试结果整理成为下面的表格（表格中\*表示不测试自己到自己的连通性）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 从  到 | PC1 | PC2 | PC3 | PC4 |
| PC1 | \* | × | √ | × |
| PC2 | × | \* | × | √ |
| PC3 | √ | × | \* | × |
| PC4 | × | √ | × | \* |

**（2）抓取vlan报文实验数据**



**实验数据处理：**

**（1）针对连通性测试的实验数据**

此时，PC1与PC3同属于vlan 10，PC2与PC4同属于vlan 20，因此同属于一个vlan的主机可以连通，不属于同一个vlan的主机不可以连通。在后续的实验中，我们会通过三层交换机的路由模块或路由器来实现不同vlan间的通信。

**（2）针对抓取的vlan数据包**

对其中的第一个icmp报文内容进行分析。

|  |
| --- |
| Frame 5: 78 bytes on wire (624 bits), 78 bytes captured (624 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: Dec 7, 2023 17:50:19.359412000 中国标准时间  [Time shift for this packet: 0.000000000 seconds]  Epoch Time: 1701942619.359412000 seconds  [Time delta from previous captured frame: 0.468257000 seconds]  [Time delta from previous displayed frame: 0.000000000 seconds]  [Time since reference or first frame: 1.972848000 seconds]  Frame Number: 5  Frame Length: 78 bytes (624 bits)  Capture Length: 78 bytes (624 bits)  [Frame is marked: False]  [Frame is ignored: False]  [Protocols in frame: eth:ethertype:vlan: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:ee:ff (04:f9:f8:8c:ee:ff)  Destination: 04:f9:f8:8c:ee:ff (04:f9:f8:8c:ee:ff)  Address: 04:f9:f8:8c:ee:ff (04:f9:f8:8c:ee:ff)  .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)  .... ...0 .... .... .... .... = IG bit: Individual address (unicast)  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: 802.1Q Virtual LAN (0x8100)  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10  000. .... .... .... = Priority: Best Effort (default) (0)  ...0 .... .... .... = DEI: Ineligible  .... 0000 0000 1010 = ID: 10  Type: IPv4 (0x0800)  Internet Protocol Version 4, Src: 172.16.1.11, Dst: 172.16.1.33  0100 .... = Version: 4  .... 0101 = Header Length: 20 bytes (5)  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  Total Length: 60  Identification: 0x768e (30350)  Flags: 0x0000  0... .... .... .... = Reserved bit: Not set  .0.. .... .... .... = Don't fragment: Not set  ..0. .... .... .... = More fragments: Not set  Fragment offset: 0  Time to live: 128  Protocol: ICMP (1)  Header checksum: 0x69e6 [validation disabled]  [Header checksum status: Unverified]  Source: 172.16.1.11  Destination: 172.16.1.33  Internet Control Message Protocol  Type: 8 (Echo (ping) request)  Code: 0  Checksum: 0x4ce5 [correct]  [Checksum Status: Good]  Identifier (BE): 1 (0x0001)  Identifier (LE): 256 (0x0100)  Sequence number (BE): 118 (0x0076)  Sequence number (LE): 30208 (0x7600)  [Response frame: 6]  Data (32 bytes)  Data: 6162636465666768696a6b6c6d6e6f707172737475767761...  [Length: 32] |

（一）基本信息

接口ID: 0，指示捕获此数据包的网络接口。

到达时间: 2023年12月7日 17:50:19 中国标准时间，数据包到达接口的时间。

帧编号: 5，表示这是捕获的第五个数据包。

帧长度: 78字节（624位），数据包的总长度。

捕获长度: 78字节，实际捕获的数据长度。

（二）以太网II

目的地址 (Dst): 04:f9:f8:8c:ee:ff，接收此数据包的设备的MAC地址。

源地址 (Src): 04:f9:f8:8c:ef:08，发送此数据包的设备的MAC地址。

类型: 802.1Q虚拟局域网 (VLAN)。

（三）802.1Q虚拟局域网 (VLAN)

优先级 (PRI): 0，表示最佳努力传输。

DEI: 0，表示帧不是通过拥塞的路径发送的。

ID: 10，表示此帧属于VLAN ID为10的虚拟局域网。

（四）互联网协议版本4 (IPv4)

源IP地址: 172.16.1.11。

目的IP地址: 172.16.1.33。

总长度: 60字节。

生存时间 (TTL): 128，数据包在网络中的最大跳数。

协议: ICMP (1)，表示承载的是一个ICMP数据包。

（五）互联网控制消息协议 (ICMP)

类型: 8，表示这是一个回声请求（ping请求）。

代码: 0，与回声请求类型相关的特定代码。

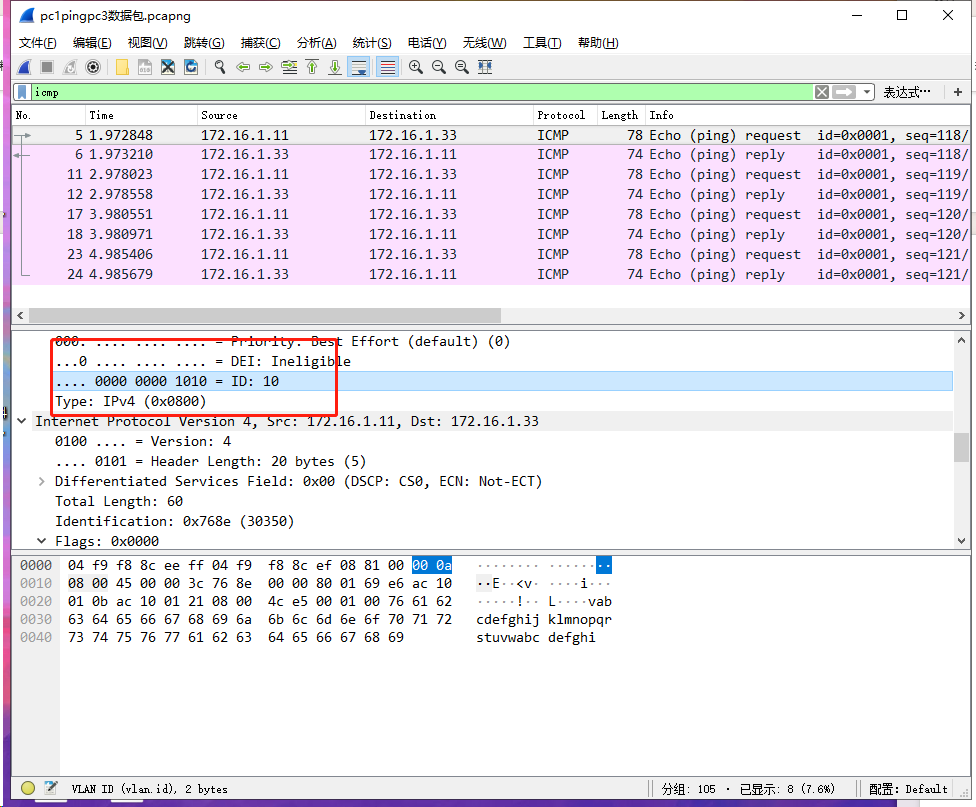
校验和: 0x4ce5，用于验证ICMP消息的完整性。

标识符: 1（大端序），256（小端序）。

序列号: 118（大端序），30208（小端序）。

数据: 32字节的数据，通常用于ping请求的有效载荷。

最后，可以在802.1Q部分找到vlan id。



**实验结果与分析：**

下面，针对实验指导书中的思考问题进行回答。

**（1）二层交换机和三层交换机如果删除vlan配置，PC1-PC4之间能否连通？**

删除VLAN配置后，PC1-PC4之间的连通性取决于它们是否在同一IP子网以及网络设备的配置。如果它们在同一IP子网内，并且物理连接正确，那么它们应该能够相互通信。如果它们在不同的IP子网，可能需要额外的路由配置。

**（2）Vlan是什么技术？与IP子网有什么异同？**

VLAN是一种网络技术，用于在数据链路层创建多个逻辑子网络，这些子网络在物理上可能分布在不同的交换机或网络设备上。VLAN的主要目的是提高网络的效率和安全性，通过逻辑上分隔网络来控制流量和限制广播域。

**相似点：**两者都用于创建网络中的逻辑分隔，提高网络的管理效率和安全性。

**不同点：**

操作层级不同：VLAN工作在数据链路层，而IP子网工作在网络层。

隔离方式不同：VLAN是通过交换机端口的配置来实现逻辑隔离，而IP子网是通过IP地址和子网掩码来实现。

通信机制不同：VLAN间的通信需要路由器或三层交换机来实现跨VLAN通信，而不同子网间的通信本质上是通过路由器进行的。

**（3）Trunk如何识别不同的Vlan数据？它能解决不同交换机之间相同Vlan之间的通信问题，它可以解决不同交换机不同Vlan之间的通信问题吗？**

在Trunk链接上，数据包被标记以指示它们属于哪个VLAN。这通常通过在以太网帧中插入一个特殊的VLAN标识符（称为VLAN ID）来实现，这个过程称为帧标签化。最常用的标签化方法是IEEE 802.1Q标准。在802.1Q VLAN标签中，VLAN ID被插入到原始帧的以太网头部和帧的有效载荷之间。

对于不同VLAN之间的通信，仅仅有Trunk链接是不够的，因为VLAN本质上是隔离的。要使不同VLAN之间的设备通信，需要路由器或具有路由功能的三层交换机来进行跨VLAN的路由。这种情况下，路由器或三层交换机的一个接口会连接到一个Trunk链接，该设备负责从一个VLAN接收数据，然后根据目的IP地址将数据路由到另一个VLAN。

**实验名称：**

实验五：通过三层交换机实现Vlan间路由

**实验目的：**

（1）拓展对交换机VLAN划分的认识

（2）熟悉三层交换机端口的路由功能

**实验仪器：**

二层交换机1台

三层交换机1台

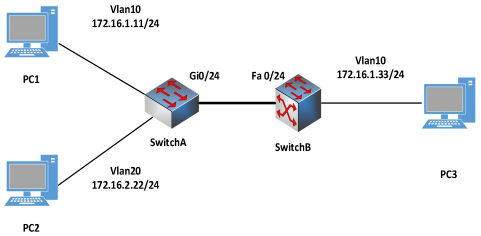
主机3台

**实验原理：**

二层交换机划分vlan后，不同vlan之间无法通信，因此可以通过配置三层交换机来实现不同vlan之间的通信。在企业网络连接的时候，二层接入交换机与三层汇聚交换机往往使用星形拓扑连接在一起，汇聚的三层交换机作为中心节点存在。

Vlan和普通物理网络一样，通常和一个IP子网联系在一起，同一个Vlan的网络号相同，不同Vlan拥有不同的网络号，在三层交换机中定义虚拟交换机接口SVI，也就是各个Vlan的网关，通过三层交换机的路由模块实现不同Vlan之间的通信。

本实验要实现同一Vlan跨交换机进行通信，即拓扑中PC1和PC3之间的通信；不同Vlan通过三层交换机端口的路由功能也能实现通信，即拓扑中PC2和PC3之间的通信。网络拓扑结构如下。

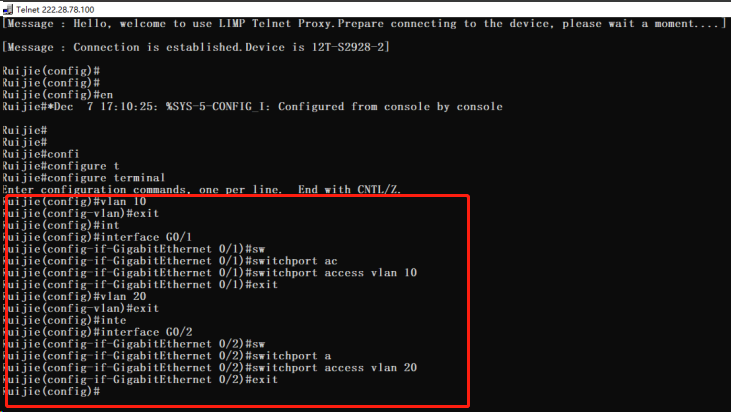


**实验内容与步骤：**

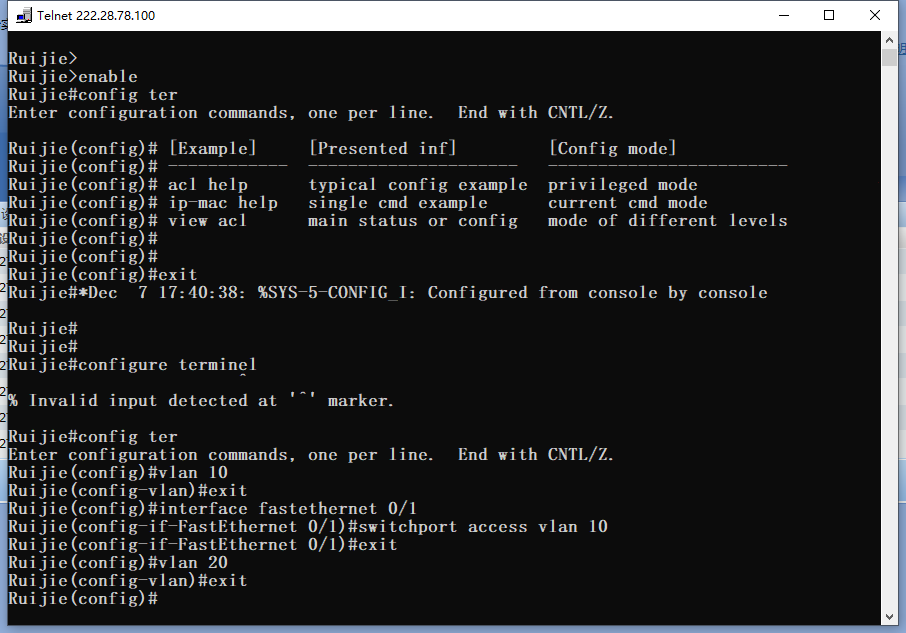
**（1）连线**

将二层交换机A的G0/24端口和三层交换机B的F0/24端口相连。将PC1和二层交换机A的G0/1端口相连；将PC2和二层交换机A的G0/2端口相连；将PC3和三层交换机B的F0/1端口相连。

**（2）在二层交换机A中创建vlan，并添加端口**

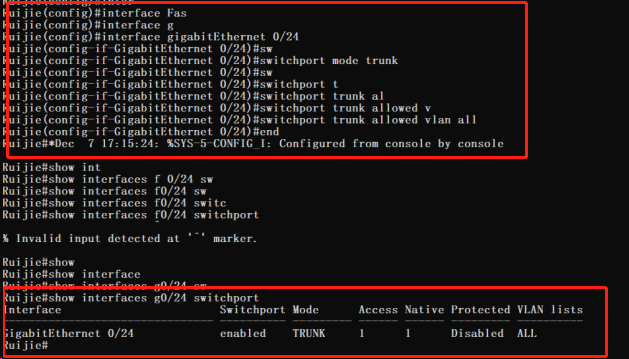


**（3）在三层交换机B中创建vlan，并添加端口**

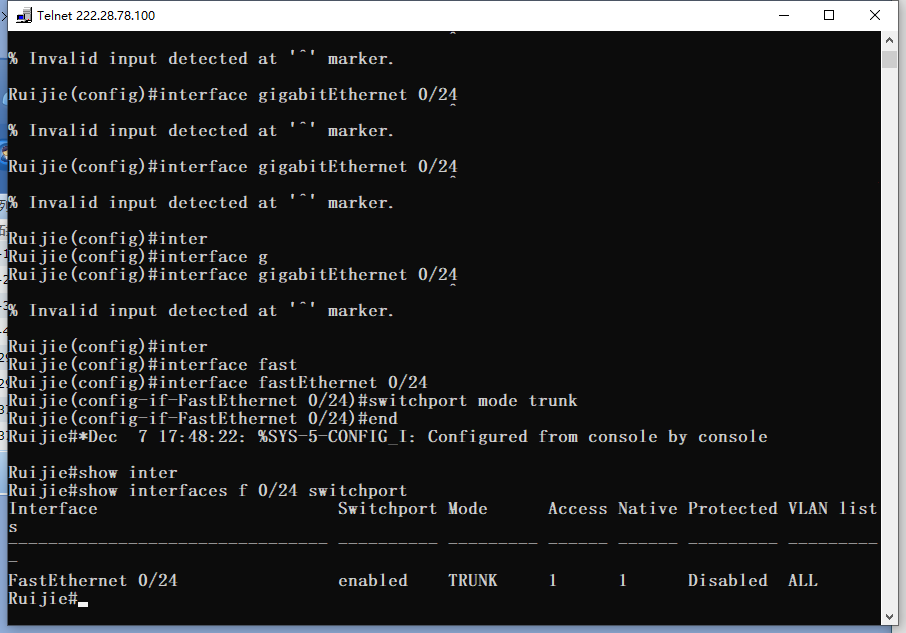


**（4）将两个交换机相连的F0/24定义为Trunk模式**

设置二层交换机。

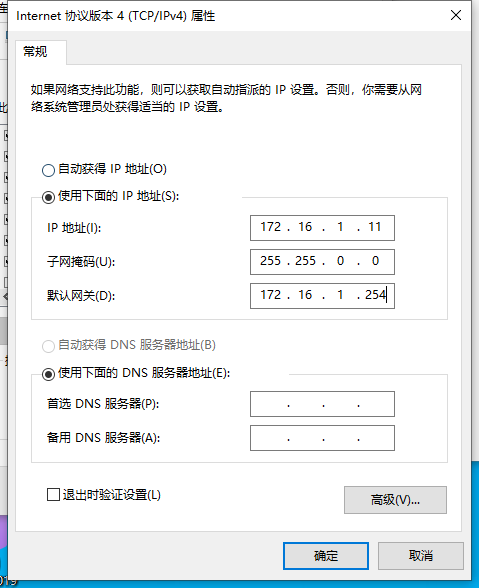


设置三层交换机。



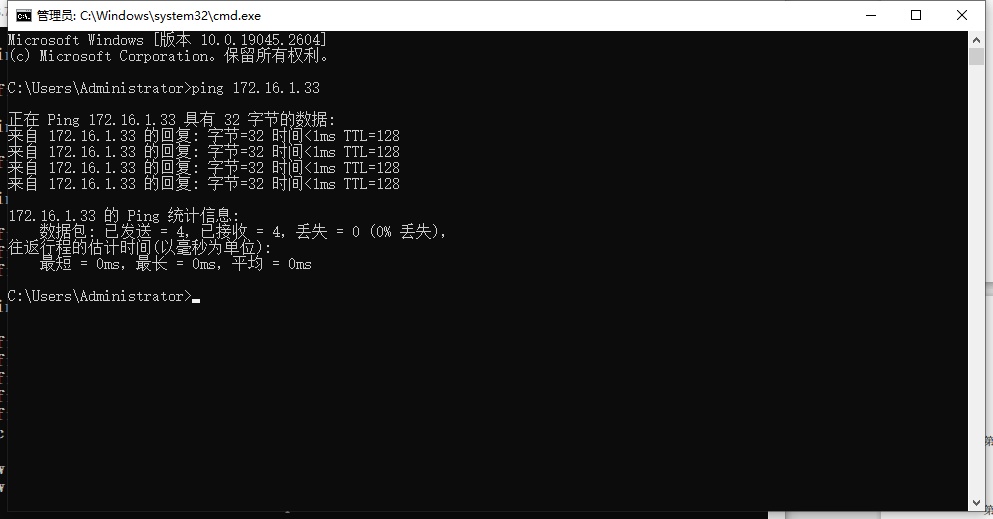
**（5）设置网卡地址**

受限于报告篇幅，展示PC1的网卡配置情况。

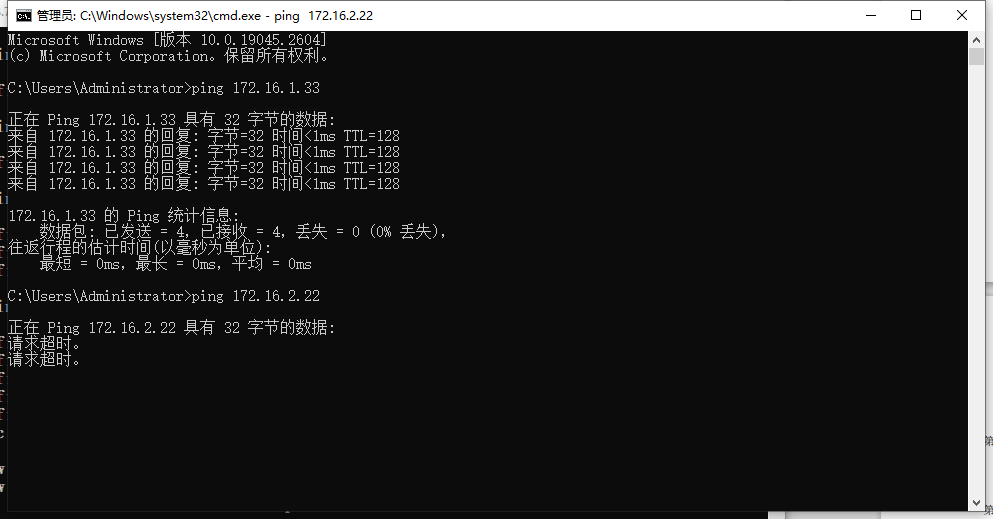


**（6）PC之间相互ping，验证连通性**

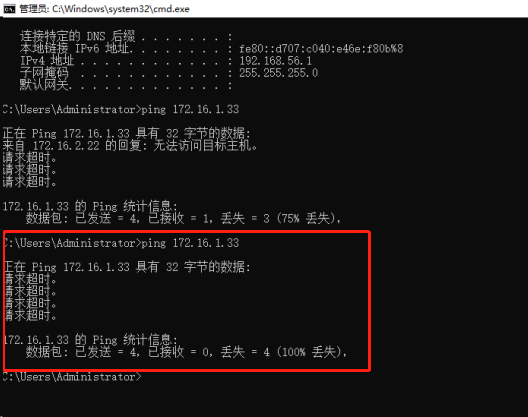
PC1 ping PC3，连通



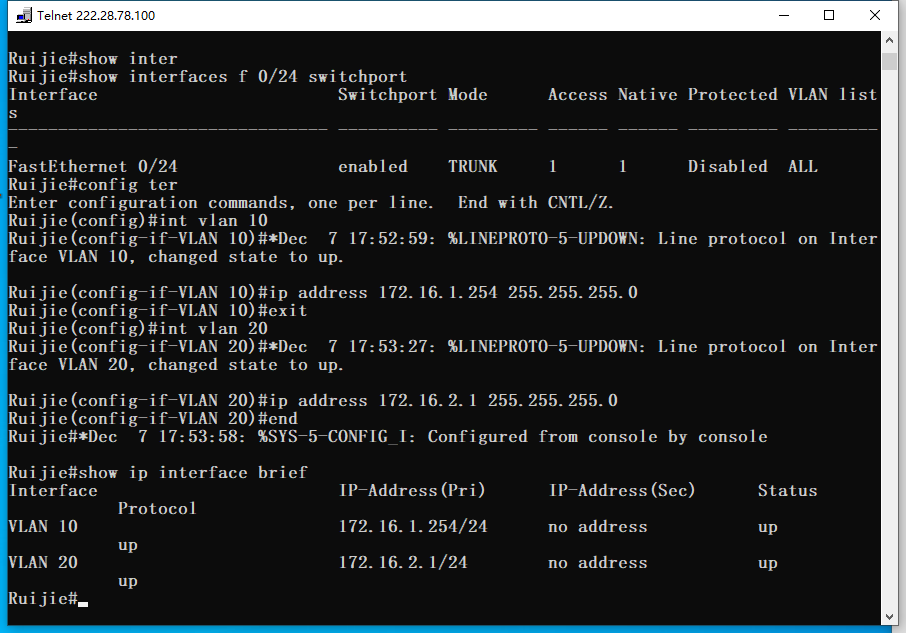
PC1 ping PC2，不连通



PC2 ping PC3，不连通

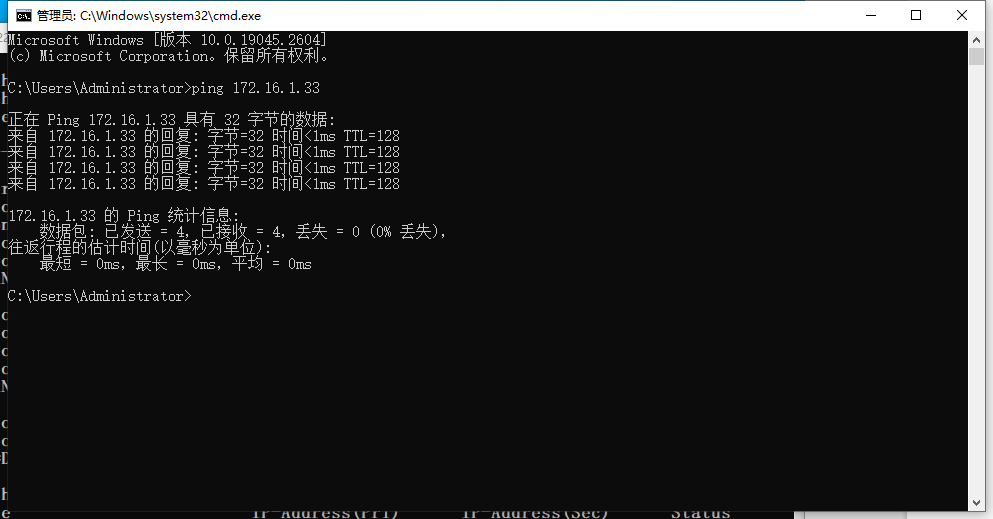


**（7）在三层交换机上设置Vlan地址**

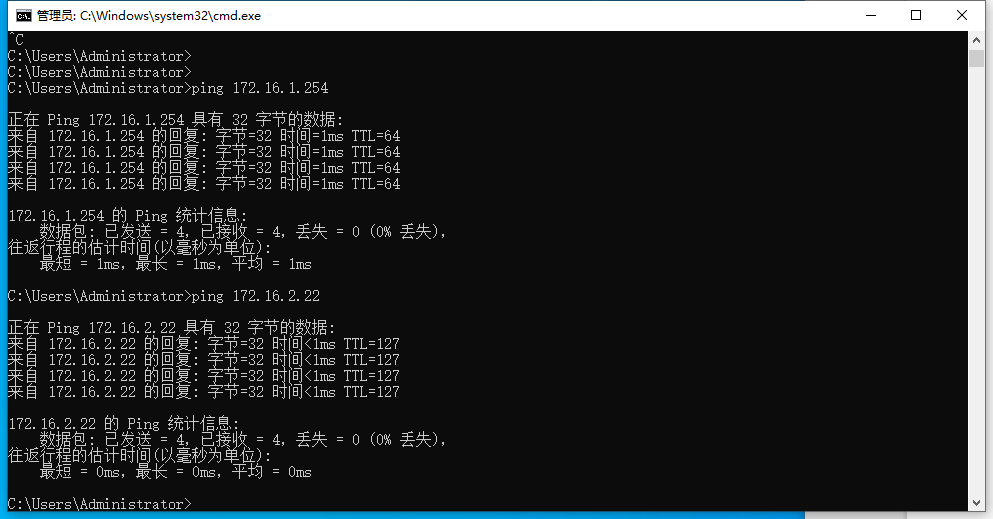


**（8）验证连通性**

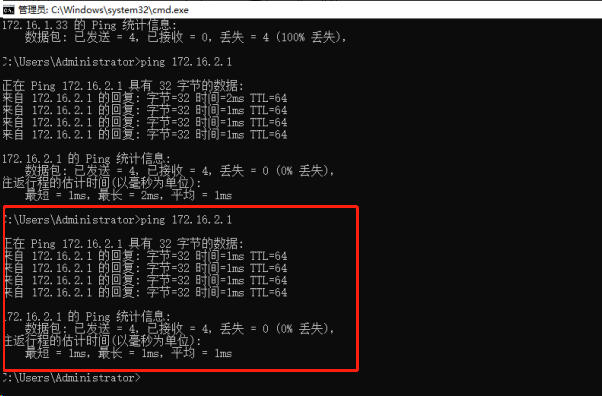
PC1 ping PC3，连通



PC1 ping PC2，连通



PC2 ping PC3，连通



**实验数据：**

本次实验没有涉及到重要的实验数据，因此将实践过程以图片的形式进行记录，记录进入实验过程中。

**实验数据处理：**

由于本次实验未涉及重要数据，因此无需进行实验数据处理。

**实验结果与分析：**

在这个环节，针对实验指导书中的思考问题进行分析。

**（1）二层交换机和三层交换机有什么区别？**

二层交换机更多用于局域网内部的数据转发，基于MAC地址工作，适用于较小或简单的网络环境。

三层交换机则结合了交换机和路由器的功能，不仅能处理局域网内的数据转发，还能进行跨网络的路由，基于IP地址工作，适用于需要复杂路由和大型网络环境。

**（2）交换机虚拟接口，也称为VLAN接口，是一种逻辑的三层接口，类似路由器子接口，其接口IP地址作为对应VLAN主机的默认网关。三层交换机如何配置VLAN的IP地址？**

下面以配置vlan 10的地址为例，进行回答。

在特权模式下：

|  |
| --- |
| config ter !进入配置模式  int vlan 10  ip address 172.16.1.254 255.255.255.0 !配置虚接口vlan 10地址  exit |

**实验名称：**

实验六：通过路由器实现Vlan间路由（单臂路由）

**实验目的：**

（1）进一步掌握交换机中不同VLAN之间的数据传输

（2）掌握如何使用路由器实现Vlan间路由

**实验仪器：**

二层交换机1台

路由器1台

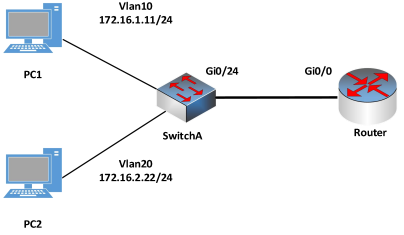
主机2台

**实验原理：**

二层交换机划分的Vlan，不同Vlan之间无法通信，在路由器的快速以太接口上，为每个Vlan创建一个对应的逻辑子接口，同时设置逻辑子接口的IP地址，封装制定的802.1q协议与对应的Vlan关联。由于是直连网络，路由器会自动在路由表为各个Vlan添加路由，将对应逻辑子接口的IP地址设成Vlan默认网关，就能实现Vlan间的路由转发。这种方式通常也被称为单臂路由。

路由器和交换机之间应以Trunk链路方式连接，路由器的不同接口所连接的Vlan必须不同，例如路由器F1/0所连接的交换机中有Vlan10、Vlan20，路由器的另一个接口F1/ 1连接的交换机中不能再有Vlan10、Vlan20，可以有Vlan30、Vlan40等，因为路由器的接口必须连接不同的网络，路由器的功能就是实现不同网络之间的数据转发。

本次实验要实现PC1和PC2之间的通信，网络拓扑结构如下。

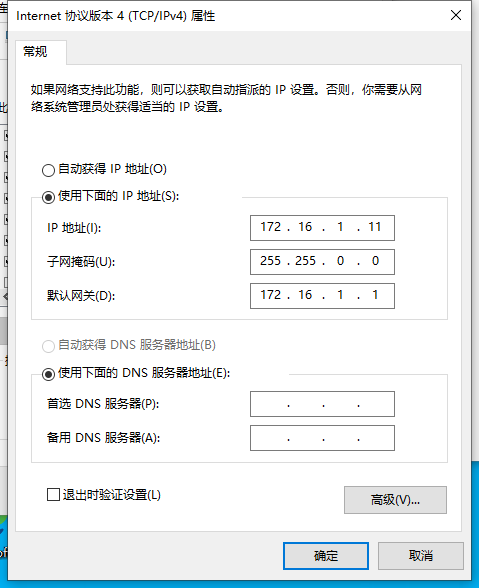


**实验内容与步骤：**

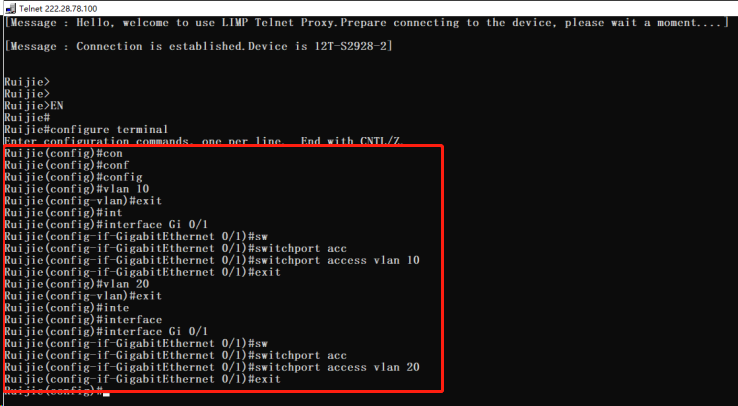
**（1）连线**

将二层交换机的G0/23端口和路由器的F0/0端口相连。将PC1和二层交换机的G0/1端口相连；将PC2和二层交换机A的G0/2端口相连。

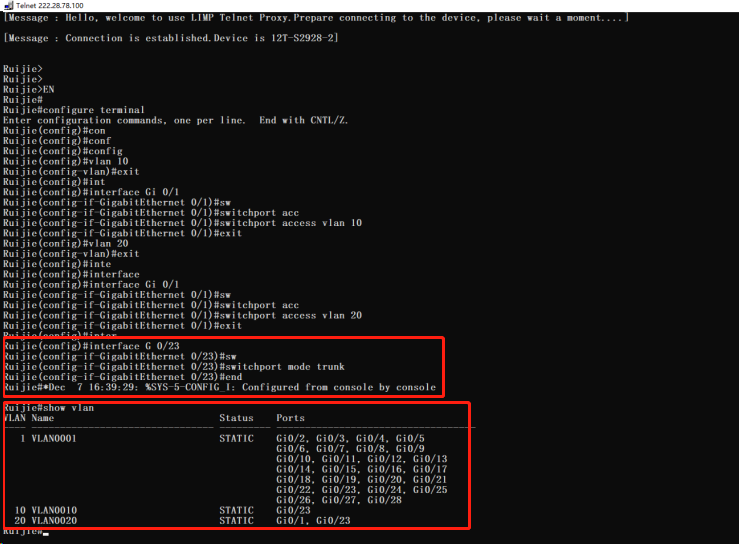
**（2）设置PC的网卡地址**



**（3）在二层交换机中创建vlan，并添加端口**

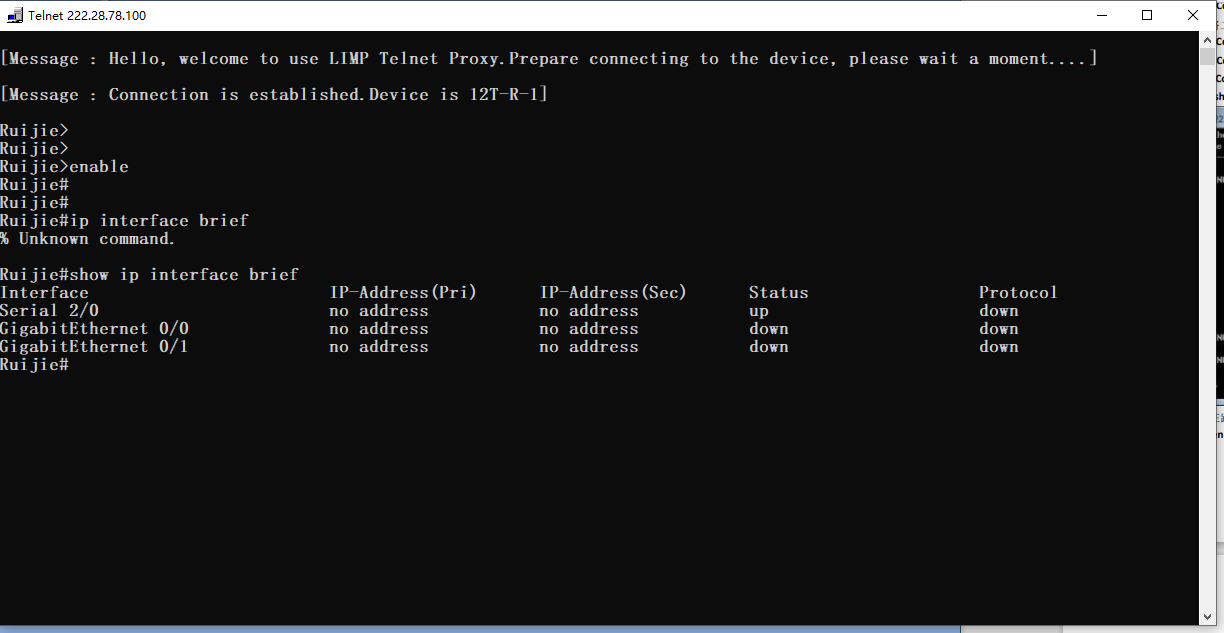


**（4）将二层交换机的G0/23端口射程干道模式**

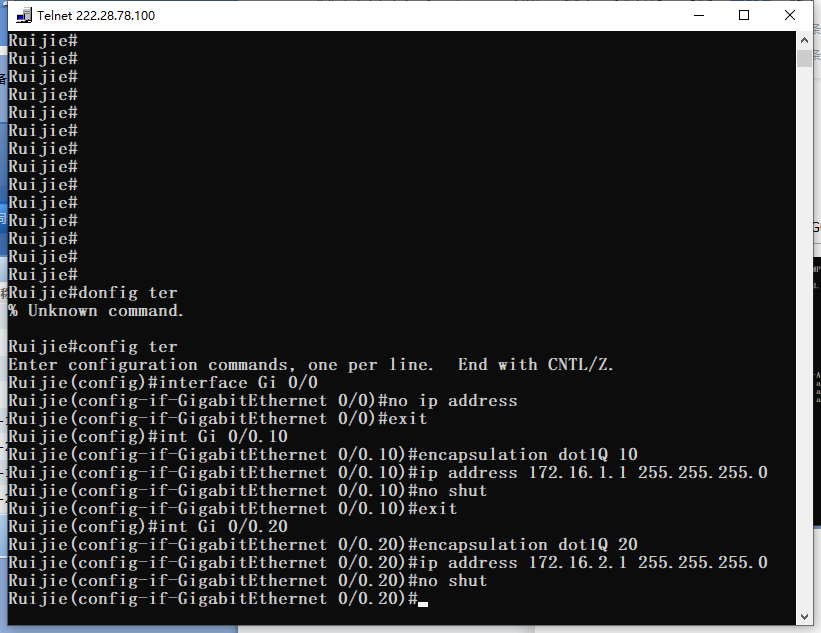


**（5）在路由器上配置G0/0的子接口**

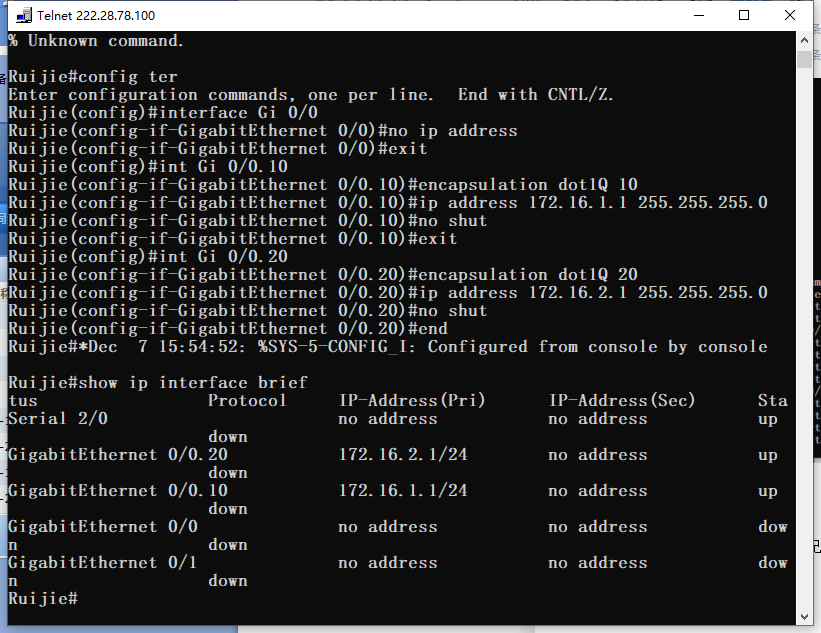
查看路由器的端口命名方式和状态

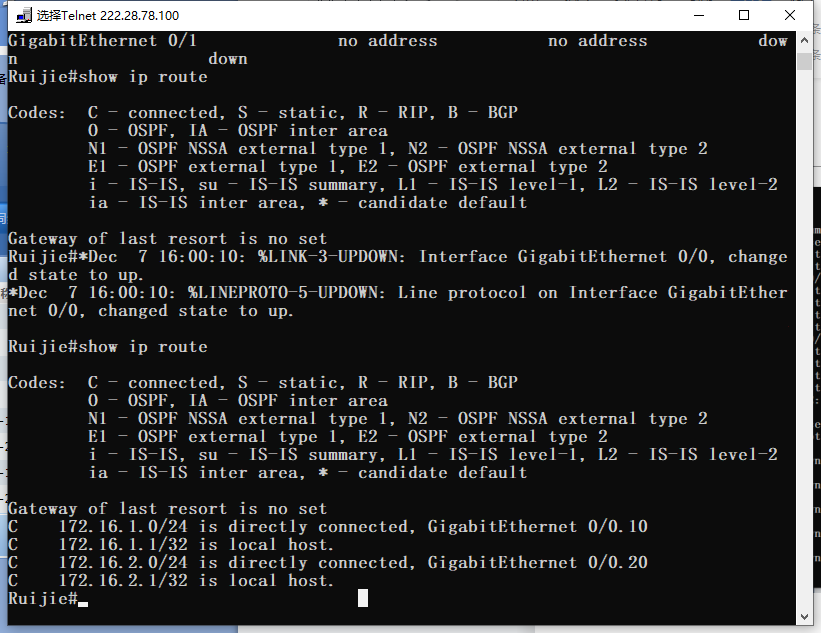


配置G0/0子接口



**（6）验证路由器上的配置并查看路由器上的路由表**





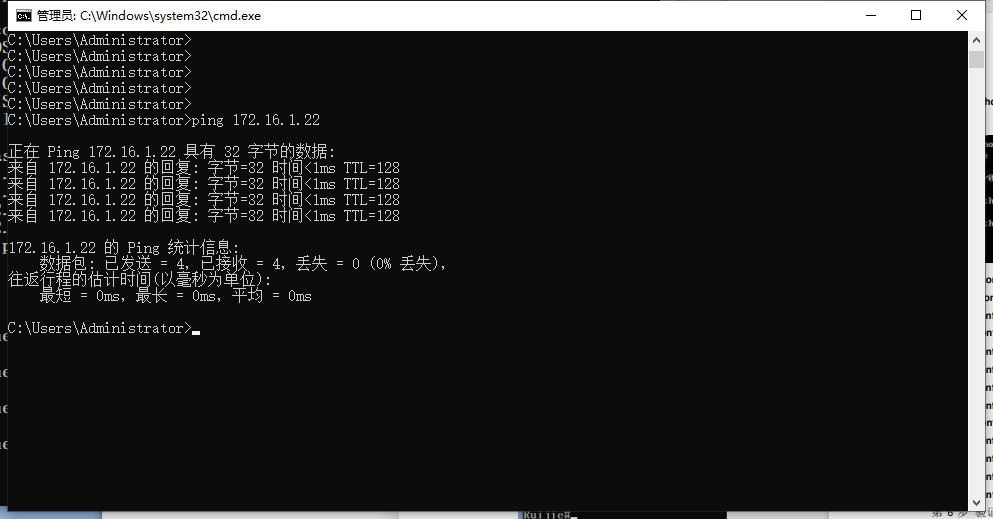
**（7）测试Vlan间的连通性**

PC1 ping PC1的网关

PC1 ping PC2的网关



PC1 ping PC2



**实验数据：**

本次实验没有涉及重要的实验数据，部分实验记录以图片的形式放置在实验过程部分。

**实验数据处理：**

由于未涉及实验数据，因此无需进行实验数据处理。

**实验结果与分析：**

在这个环节，将针对实验指导书中的思考问题进行回答。

**（1）交换机Acess口和Trunk口两种模式如何选择？**

在实验过程中，我对端口连接模式不熟悉（理论课上目前还没有讲授），因此我查阅资料([什么是VLAN？VLAN是如何工作的？ - 华为 (huawei.com)](https://info.support.huawei.com/info-finder/encyclopedia/zh/VLAN.html))，学习了关于端口连接模式的相关知识，主要有三种连接模式：access、trunk、hybrid。

**a、access接口**

Access接口一般用于和不能识别Tag的用户终端（如用户主机、服务器）相连，或者不需要区分不同VLAN成员时使用。

在一个VLAN交换网络中，以太网数据帧主要有以下两种形式：

1、无标记帧（Untagged帧）：原始的、未加入4字节VLAN标签的帧。

2、有标记帧（Tagged帧）：加入了4字节VLAN标签的帧。

Access接口大部分情况只能收发Untagged帧，且只能为Untagged帧添加唯一VLAN的Tag。交换机内部只处理Tagged帧，所以Access接口需要给收到的数据帧添加VLAN Tag，也就必须配置缺省VLAN。当Access接口收到带有Tag的帧，并且帧中VID与PVID相同时，Access接口也能接收并处理该帧。在发送带有Tag的帧前，Access接口会剥离Tag。

**b、trunk接口**

Trunk接口一般用于连接交换机、路由器、AP以及可同时收发Tagged帧和Untagged帧的语音终端。它可以允许多个VLAN的帧带Tag通过，但只允许属于缺省VLAN的帧从该类接口上发出时不带Tag（即剥除Tag）。

Trunk接口上的缺省VLAN，有的厂商也将它定义为native VLAN。当Trunk接口收到Untagged帧时，会为Untagged帧打上Native VLAN对应的Tag。

**c、hybrid接口**

Hybrid接口既可以用于连接不能识别Tag的用户终端（如用户主机、服务器）和网络设备（如Hub），也可以用于连接交换机、路由器以及可同时收发Tagged帧和Untagged帧的语音终端、AP。它可以允许多个VLAN的帧带Tag通过，且允许从该类接口发出的帧根据需要配置某些VLAN的帧带Tag（即不剥除Tag）、某些VLAN的帧不带Tag（即剥除Tag）。

**（2）路由器子接口封装802.1Q需要与相应VLAN封装一致，并正确配置网关和子网掩码，请给出配置命令，可以以VLAN10示例。**

|  |
| --- |
| enable !进入特权模式  config ter !进入配置  interface Gi 0/0 !清除Gi 0/0端口的ip设置  no ip address  exit  int Gi 0/0.10 !配置子接口Gi0/0.10  encapsulation dot1Q 10 !封装802.1Q协议并与vlan10关联  ip address 172.16.1.1 255.255.255.0 !配置ip地址和掩码  no shut !开启端口  exit |