**实验报告要求（本页最后提交实验报告时需删除！）**

1. **文件命名要求：**

班级-学号-姓名-实验报告.docx 如：通信2201-42024111-张三-实验报告.docx

1. **文档要求：**

实验目的：参考教材

实验仪器：本次实验用到的设备，如1台交换机，3台PC机

实验原理：根据教材自己总结实验所用原理

实验内容与步骤：详细说明实验过程，所有**验证结果（show、ping、抓包）**需要截图。

**注意**：每台设备配置前，必须先**修改设备名**：姓名首字母缩写\_设备名简写编号，在截图时，必须体现设备名。

如：张三同学的实验中，交换机命名：ZS\_SW1、ZS\_SW2；

李四同学的实验中，路由器命名：LS\_R1、LS\_R2



实验结果与分析：分析实验结果的原因，如分析ping通或不通的原因、抓包分析

问题思考和解决方法：对本次实验的思考，以及实现过程中遇到的问题及解决方法，必要时需截图说明

1. **交作业时间与方式：**

时间：2023年 5月26日

方式： 发送邮件至：通信1-2 班：sy1\_ustb@126.com

通信3-4 班：sy2\_ustb@126.com

**北京科技大学实验报告**

学院： 计算机与通信工程学院 专业：通信工程 班级： 通信2102

姓名： 罗伟东 学号： U202142092 实验日期： 2023年 4月 23日

# 实验名称：实验一 单台交换机划分VLAN

**实验目的：**

**（1）了解VLAN原理**

**（2）掌握使用交换机划分VLAN的方法**

**（3）了解如何验证VLAN的划分**

**实验仪器：**

**二层交换机 S2126（1 台）**

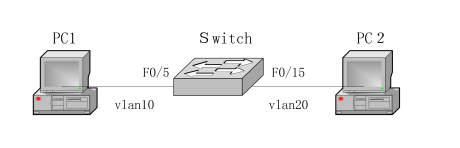
**主机 2 台**

**实验原理：**

1. **VLAN是虚拟局域网，是指网络中的站点不拘泥于所处的物理位置，而可以根据需要灵活地加入不同的逻辑子网中的一种网络技术。那也就意味vlan可提高网络安全性和灵活性，vlan可以阻止数据截取，缩小广播的传输范围。降低处理广播所占有的设备的CPU和内存资源。部署原则有两点：首先是按照行政机构划分vlan；然后是vlan号与ip子网要一一对应的。**
2. **交换机的管理方式基本分为两种：带内管理和带外管理。带外管理是通过交换机的Console口管理交换机，不占用交换机的网络接口，特点是需要使用配置线缆，近距离配置。第一次配置交换机时必须利用Console端口进行配置。带内管理是占用交换机的一个通信接口，通过telnet方式管理交换机，可以远距离配置。交换机管理主要通过命令行完成。交换机的命令行操作模式，主要包括：用户模式、特权模式、全局配置模式、端口模式等几种。各种模式提供一组命令，实现特定的一组功能。**
3. **为了防止二层广播域过大造成安全影响和性能影响，我们通常会在交换机上部署vlan来实现二层网络的隔离，vlan技术通过花粉不同的逻辑区域实现二层网络的隔离。主机本身没有关于vlan的概念，而在交换机通信的过程中要通过数据帧加上pvid来区分所vlan，因此要求Access链路收到一个pvid的帧时打上tag，在发送给主机的时候剥离tag。**

**实验内容与步骤：**

**1.实验拓扑图**



**2.实验步骤：**

**1.连线：**

**在机房将PC1和交换机F 0/5端口相连，将PC2和交换机的F0/15端口相连**

**2.创建vlan**

**在锐捷实验平台上输入以下命令行**

**Switch>enable**

**Switch#config terminla**

**switch(Config)#**

**switch(Config)#vlan 10 !创建 vlan 10**

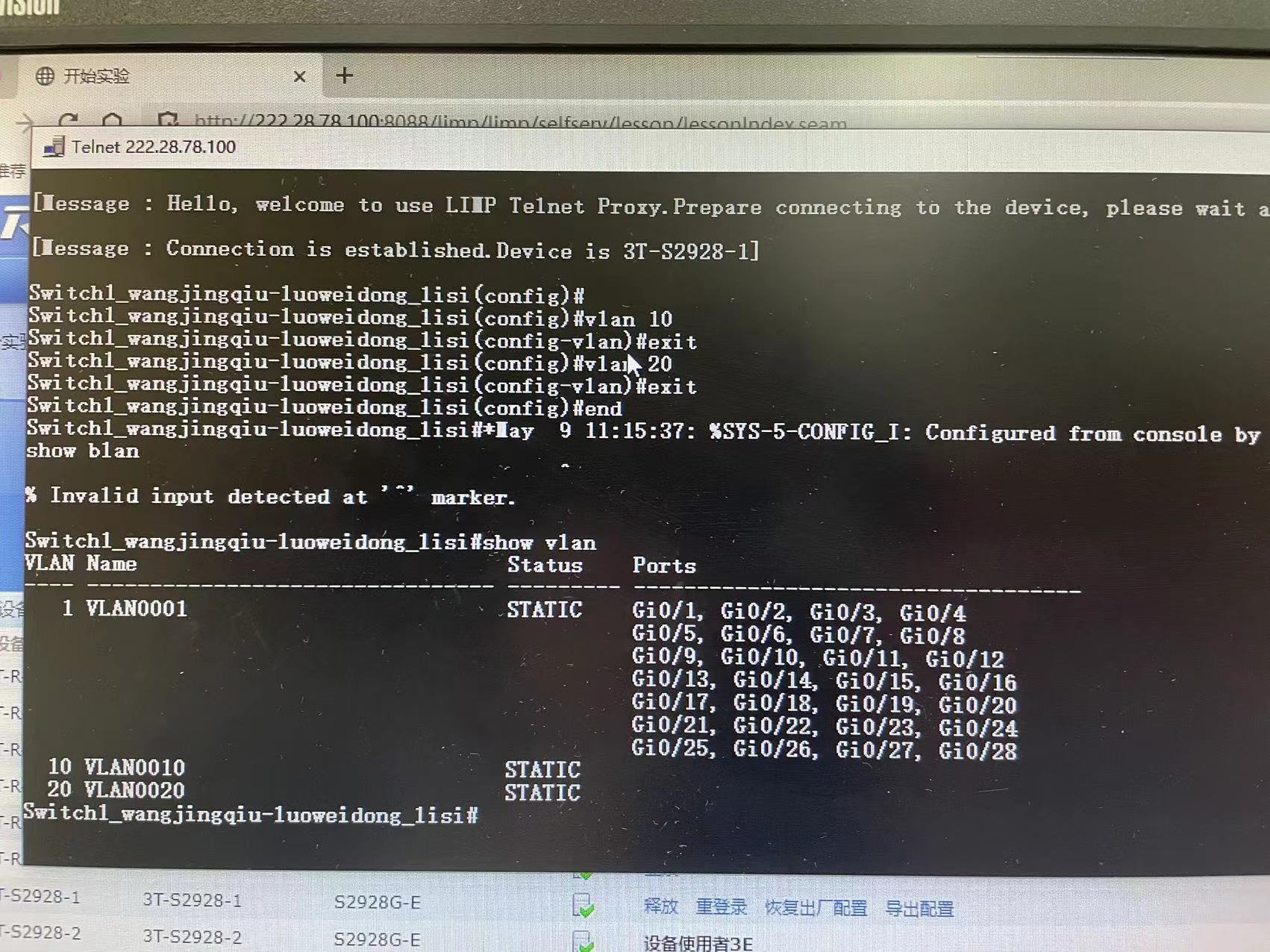
**switch(Config-Vlan10)#exit**

**switch(Config)#vlan 20 !创建 vlan 20**

**switch(Config-Vlan20)#exit**

**switch(Config)#end**

**switch#show vlan !查看配置的 Vlan 信息**

****

**3.给vlan添加端口**

**switch(Config)#**

**switch(Config)#interface range fastEthernet 0/1-10 ! 将端 Fa0/1 至 Fa0/10 划分到VLAN 10**

**switch(config-if-range)#switchport mode access !定义端口为访问连接模式**

**switch(config-if-range)#switchport access vlan 10**

**switch(config-if-range)#exit**

**switch(config)# interface range fastEthernet 0/11-15 !将端口Fa0/11至Fa0/15划分到 VLAN 20**

**switch(config-if-range)#switchport mode access**

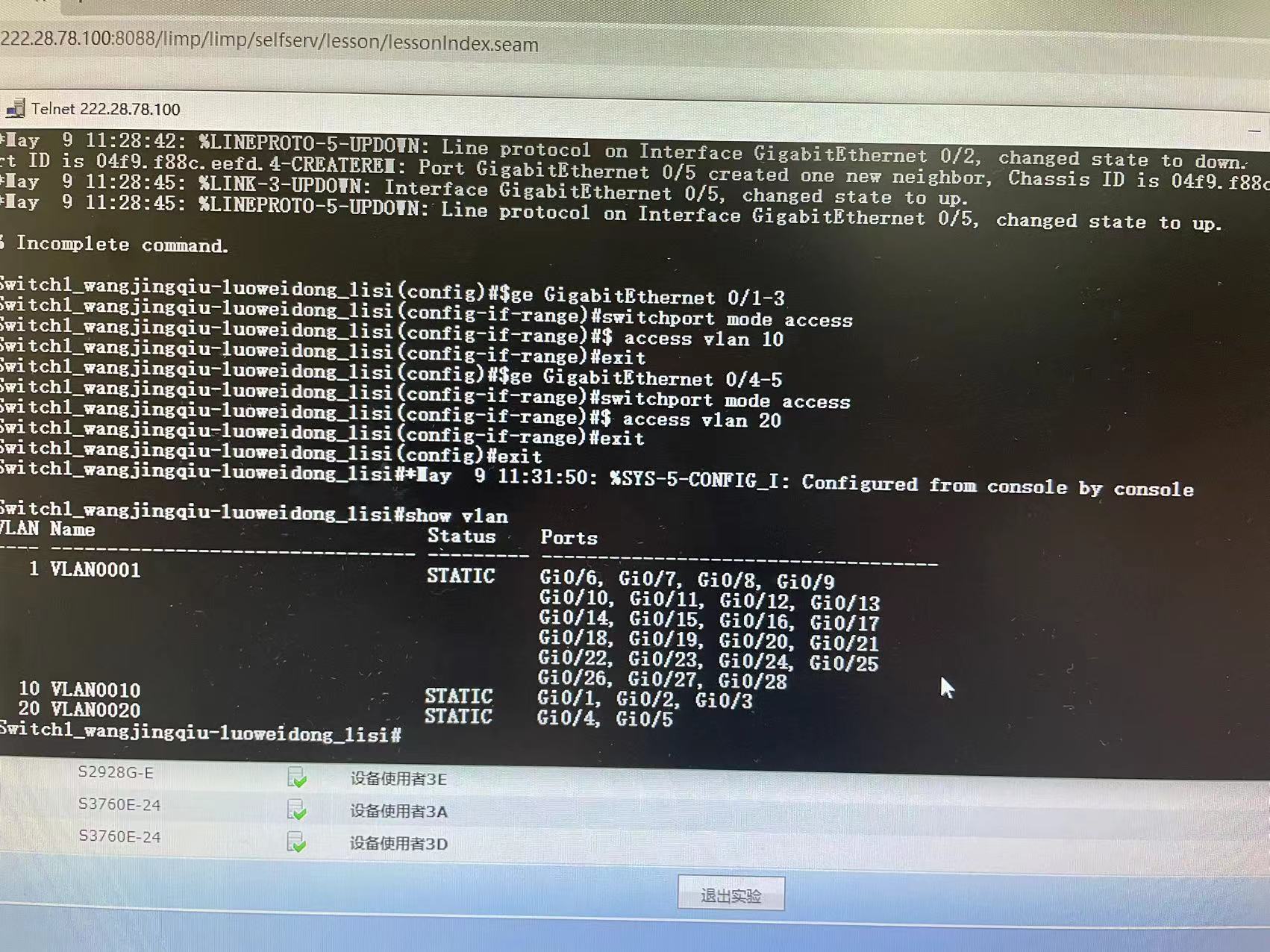
**switch(config-if-range)#switchport access vlan 20**

**switch(config-if-range)#exit**

**switch(config)#exit**

**4.查看配置**

**switch#show vlan**

****

**然后看到时交换机中有三个vlan分别是vlan1，vlan10，vlan20，在交换机中vlan1是默认存在的，没有受到划分的端口都在vlan1下面，然后其他就按照上面的命令行都划分好了。**

**5.配置网卡地址**

**在两台主机上：**

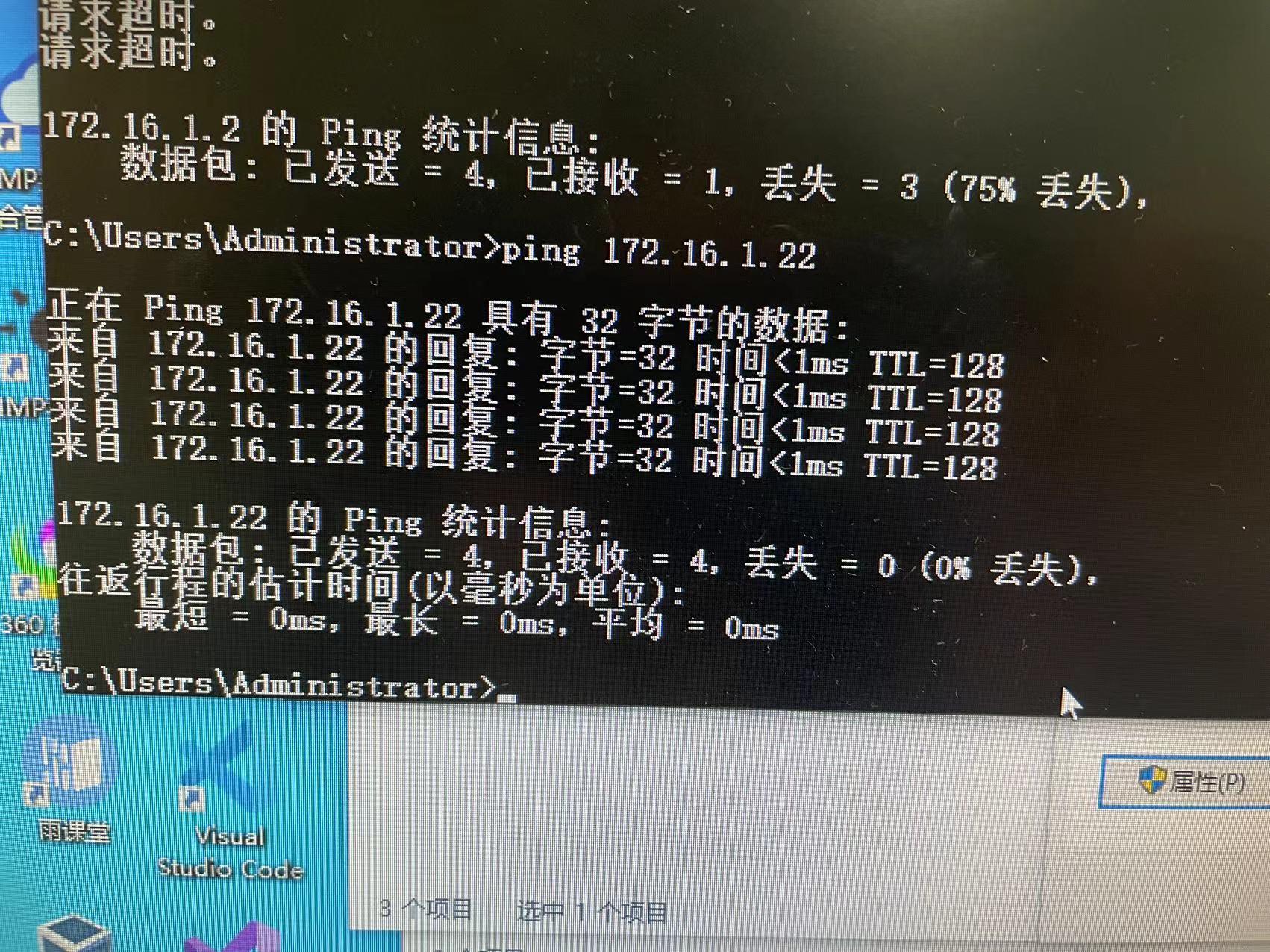
**PC1中的“网络实验”网卡ip地址为**172.16.1.11/24

**PC2中的“网络实验”网卡ip地址为**172.16.1.22/24

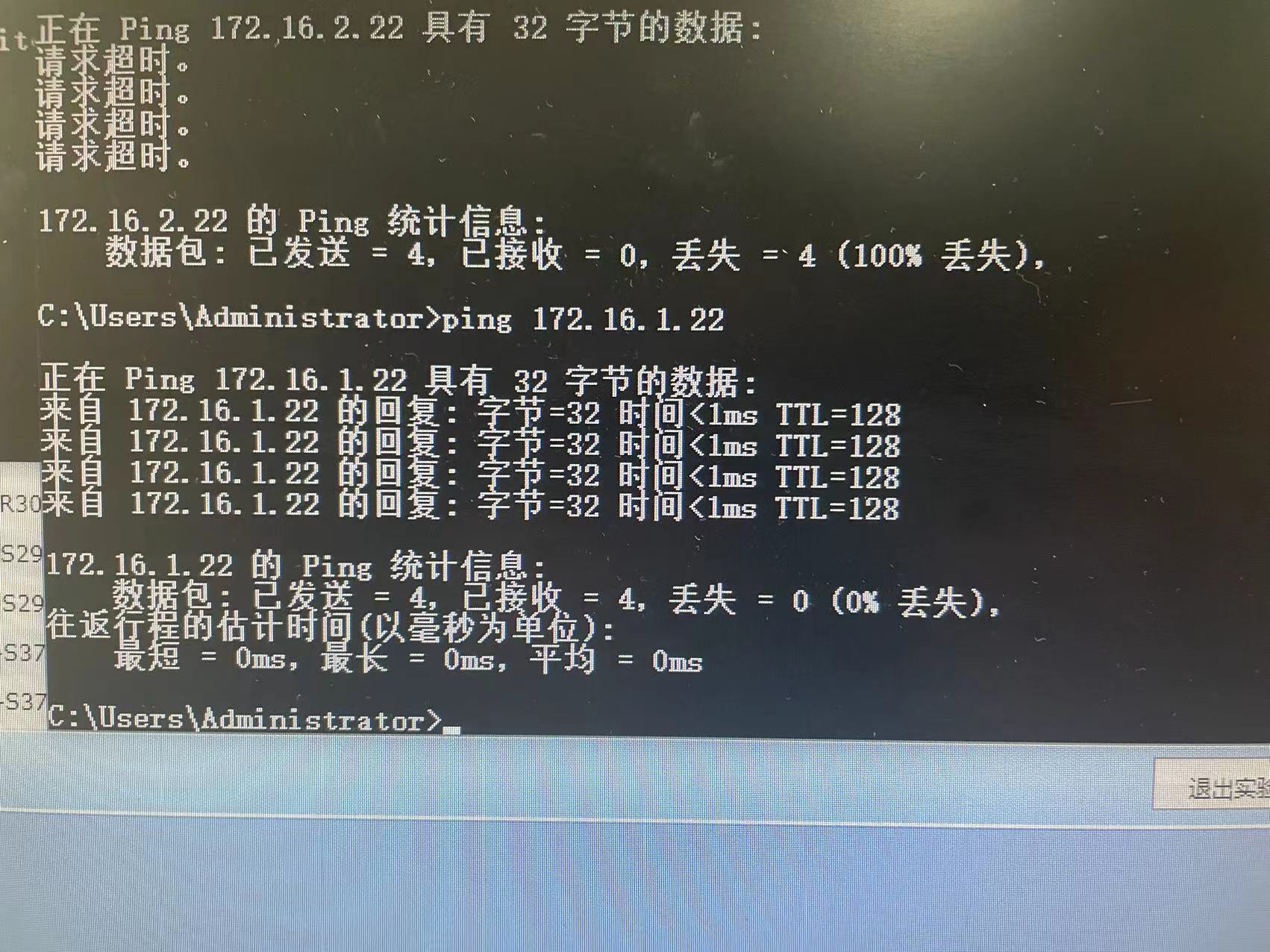
**在PC段的命令行下输入ipconfig，查看刚刚配置的地址设置是否生效。**

**6.验证**

**保证PC1和PC2在一个vlan下面，在PC1命令行输入 ping 172.16.1.1.22**

****

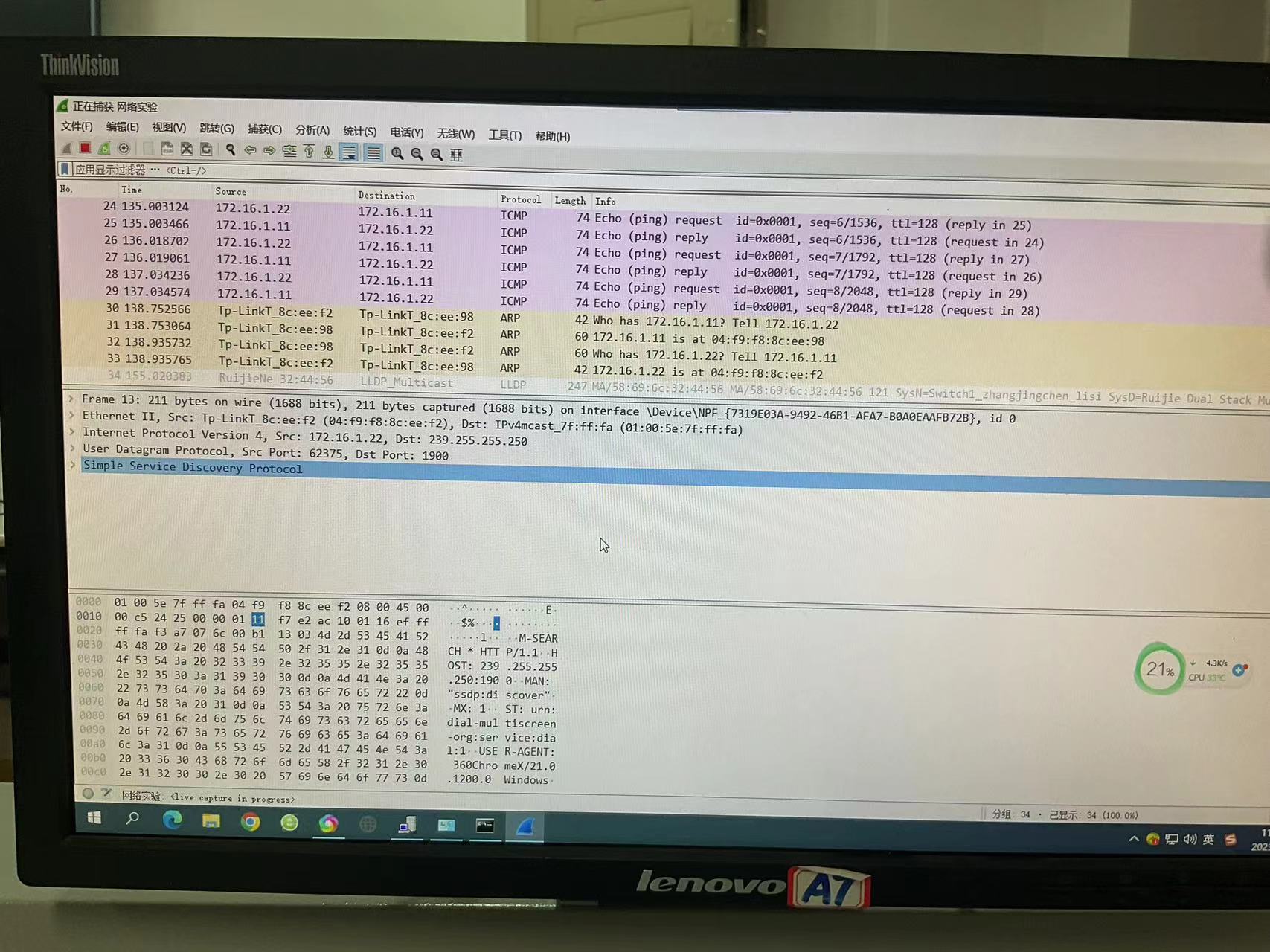
**PC1连接交换机的F0/5端口，PC2链接交换机的F0/15端口，在PC1命令行输入 ping 172.16.1.1.22**

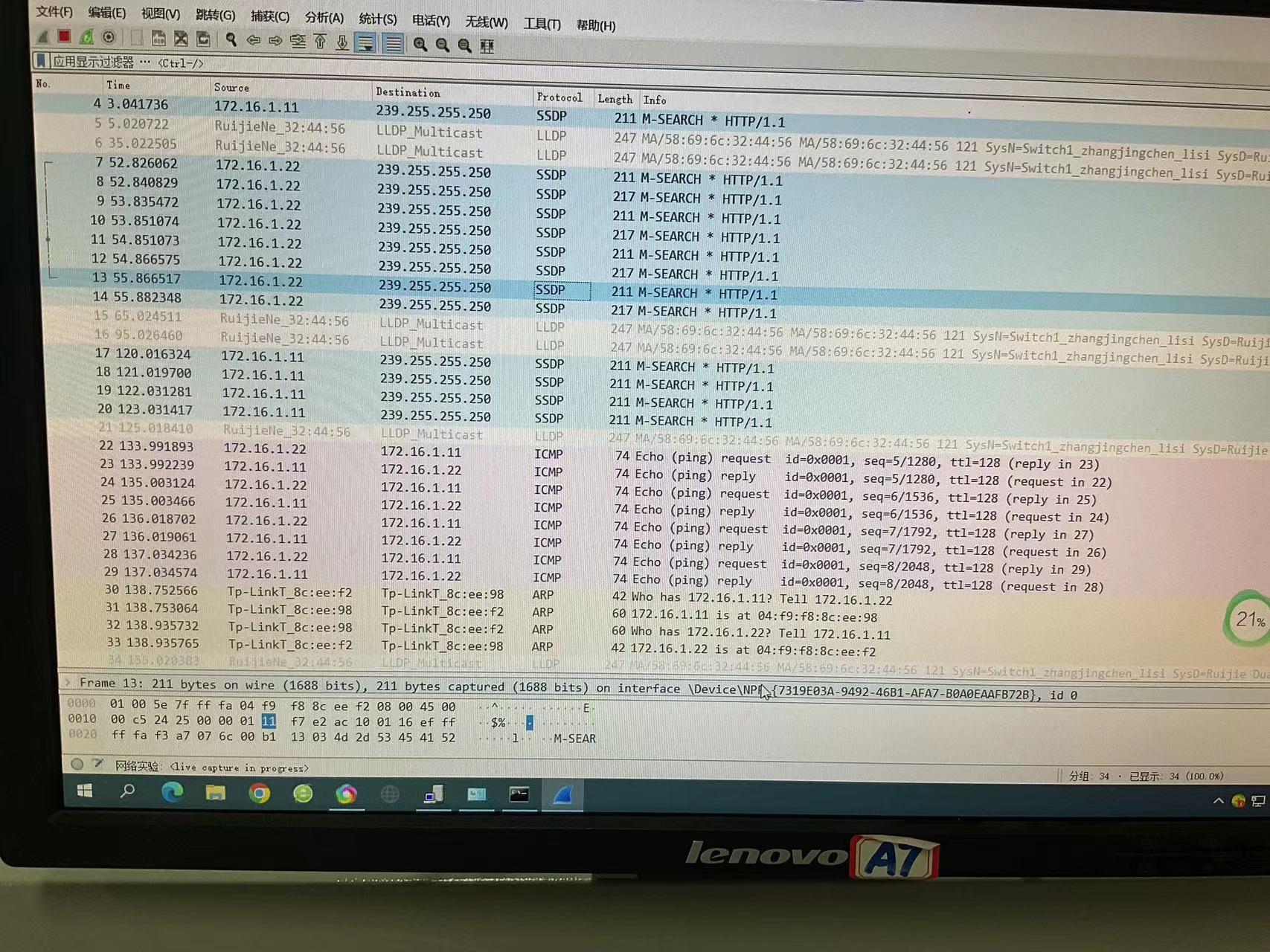
****

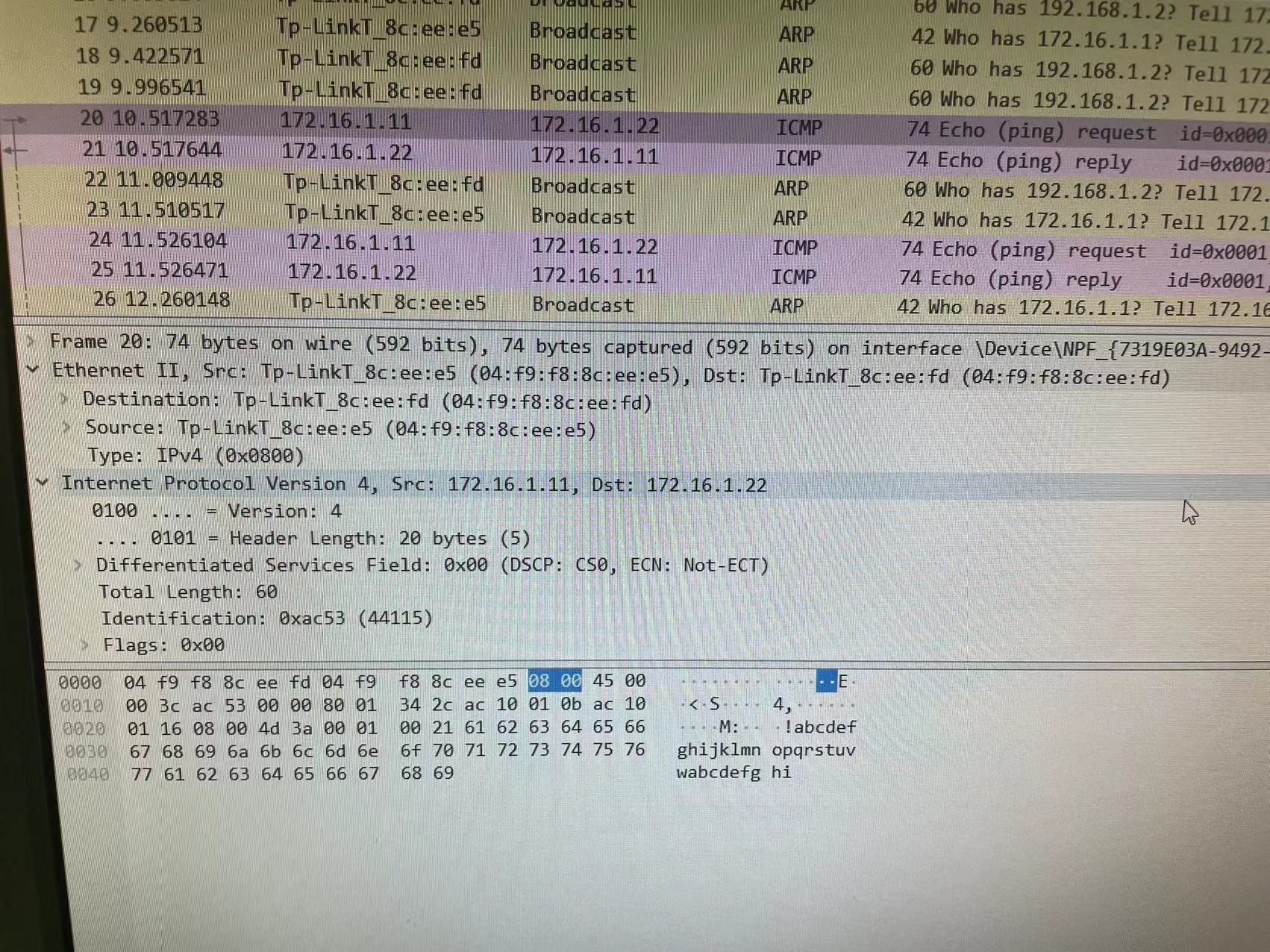
**PC1连接交换机的F0/5端口，PC2链接交换机的F0/20端口，在PC1命令行输入 ping 172.16.1.1.22**

**7.wireshark抓包分析**

**打开 Wireshark 软件，捕获→选项下，选中“网络实验”网卡，点击“开始”，启动抓包软件。再次执行 PC1 ping PC2 操作，抓取 ICMP 报文，点击捕获→停止，对抓取的报文进行分析。**

****

****

****

**实验结果与分析：**

**在实验一中，PC1在同一个vlan下可以成功ping通PC2，在不同的vlan下则是不能ping通。为了实现互通划分vlan，修改ip地址，将不同vlan下的主机ip地址改为与其网关vlanif相同的网段，经过上述修改后，不同vlan之间的通信时候传数据包先发送给vlanif接口的虚拟网关，由交换机进行转发，由此次实验也验证并了解了两种不同的access和trunk工作方式的却别以及部署位置的不同，对课堂上的知识进行了验证。**

**为了实现加环己的互通，在交换机上面配置了两个虚拟接口，将这两个接口分别作为两个vlan内主机的网关。**

**问题思考和解决方法：**

**1.** **第 6 步抓包实验中，有没有 ARP 协议的请求和回答报文？怎样才能产生 ARP 协议的报文？**

**在抓包实验中，有ARP协议的请求和回答报文，产生ARP报文的方式有发送ARP请求，接受ARP请求并且回复，主动发送ARP相应，更新ARP缓存。**

**2.** 使用 wireshark 软件抓包，抓取一组 ICMP 请求和应答的报文

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 请求报文序号 | 源 MAC | 目的 MAC | 源 IP | 目的 IP | Type | Code |
| 20 | 04:f9:f8:8c:ee:fd | 04:f9:f8:8c:ee:e5 | 172.16.1.11 | 172.16.1.22 | 8 | 0 |
| 回答报文序号 | 源 MAC | 目的 MAC | 源 IP | 目的 IP | Type | Code |
| 21 | 04:f9:f8:8c:ee:e5 | 04:f9:f8:8c:ee:fd | 172.16.1.22 | 172.16.1.11 | 0 | 0 |

3.在实验过程中，有没有遇到什么问题，是怎么解决的？

（1）首先就是接线接错端口，还有配置ip地址的端口错了。然后就是后面发现了，即使改正。

（2）然后就是两台PC在同一个vlan下有时候无法ping通，老师给的解决方法就是将校园网禁用。

# 实验名称：实验二 通过三层交换机实验Vlan间路由

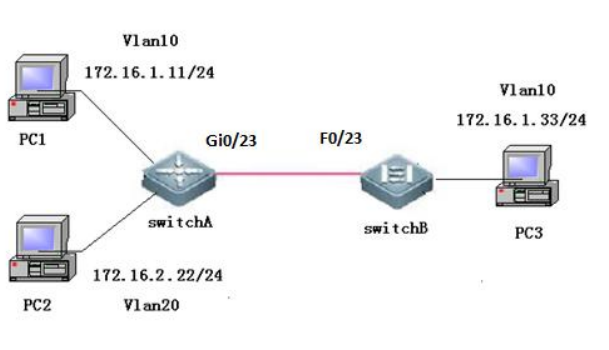
**实验目的：**

* + - 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 S2126（1 台），三层交换机 S3750（1 台），主机 3 台。**

**实验原理：**

**1.实验拓扑图**



2. 为了防止二层广播域过大造成的安全影响和性能影响，我们通常会在交换机上部署VLan来实现二层网络的隔离，Vlan技术通过划分不同的逻辑区域实现二层网络的隔离。 Vlan可以基于端口，基于MAC地址等划分，通常我们选择基于端口划分。部署了Vlan的交换机与主机之间的链路成为access链路，部署了vlan的交换机之间的链路成为Trunk链路。 主机本身没有任何关于Vlan的概念，而在交换机通信过程中需要通过为数据帧加上pvid来区分所属Vlan。因此要求Access链路在收到一个没有pvid的帧时为其打上tag，在发送给主机时剥离tag。以此来实现Vlan控制。有些特性丰富的交换机除了上述两种接口外还支持混合接口，用来对数据帧的转发进行更精细的控制，在本实验中不涉及。

**实验内容与步骤：**

1.连线：

将二层交换机A的G0/23端口和三成交换机B的F0/23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；

2.二层交换机中创建vlan，并且添加端口：

switchA(Config)#

switchA(Config)#vlan 10

switchA (Config-Vlan)# exit

switchA (Config)# interface G0/1

switchA (Config-if)#switchport access vlan 10

switchA (Config-if)#exit

switchA (Config)#vlan 20

switch A(Config-Vlan)#exit

switchA(config)# interface G0/2

switch (Config-if)# switchport access vlan 20

switch (Config-if)#exit

3.三层交换机B创建vlan，并且添加端口

switchB(Config)#vlan 10

switchB (Config-Vlan)# exit

switchB (Config)# interface fastethernet 0/1

switchB (Config-if)#switchport access vlan 10

switchB (Config-if)#exit

switchB(Config)#vlan 20

switchB(Config-Vlan)# exit

switchB(Config)#

4.将会两个交换机相连的F0/23端口定义为Trunk模式

switchA(Config)#interface Fastethernet 0/23

switchA(Config-if)#switchport mode trunk ！将 F0/23 端口定义为 Trunk 模式

switchA(Config-if)#end

switchA#show interface f 0/23 switchport !查看端口的转发模式

交换机B操作相同

5.设置网卡地址：

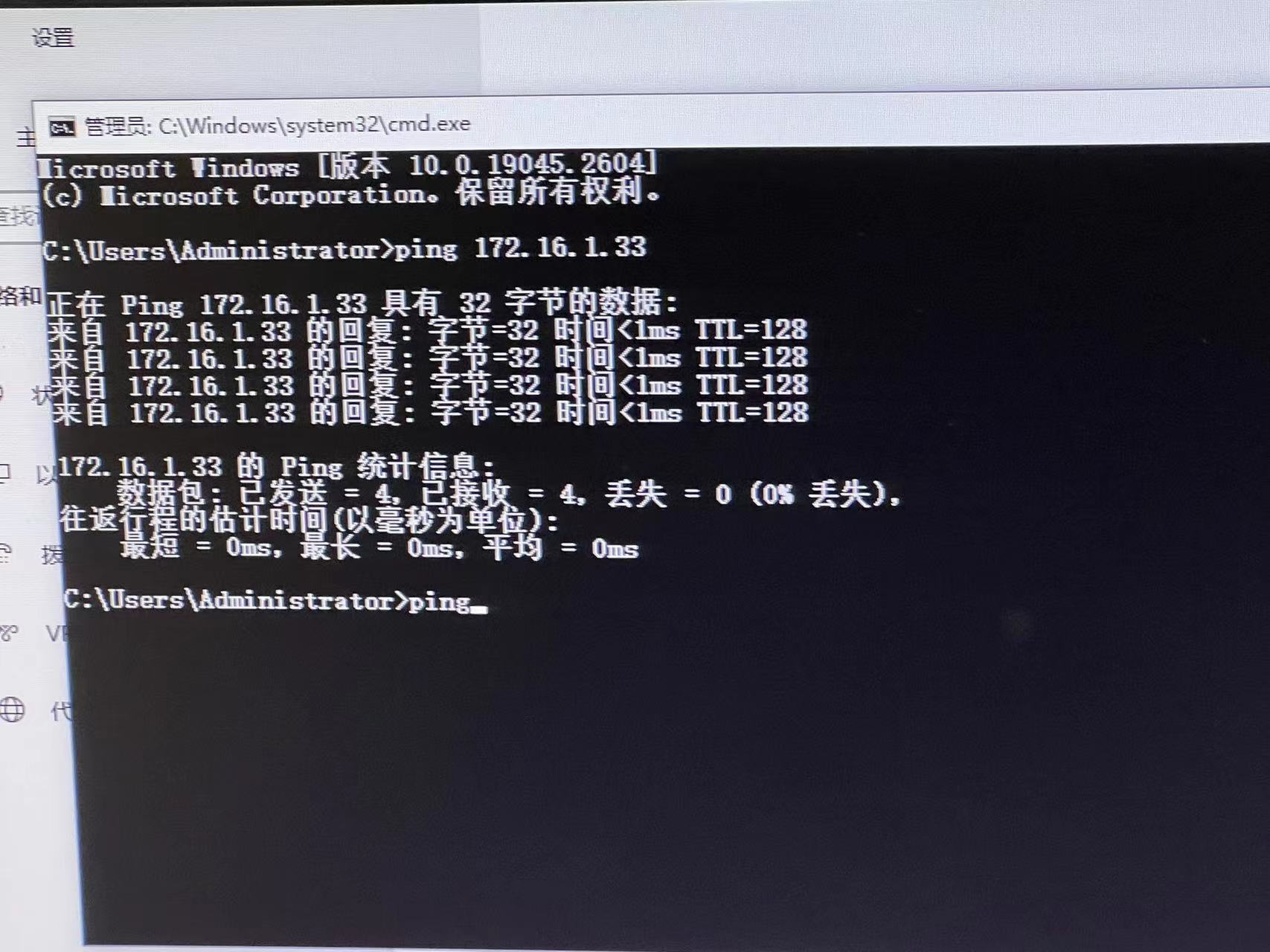
配置 PC1“网络实验”网卡的 IP 地址为：172.16.1.11/24，网关设为 172.16.1.254；

配置 PC2“网络实验”网卡的 IP 地址为：172.16.2.22/24，网关设为 172.16.2.1。

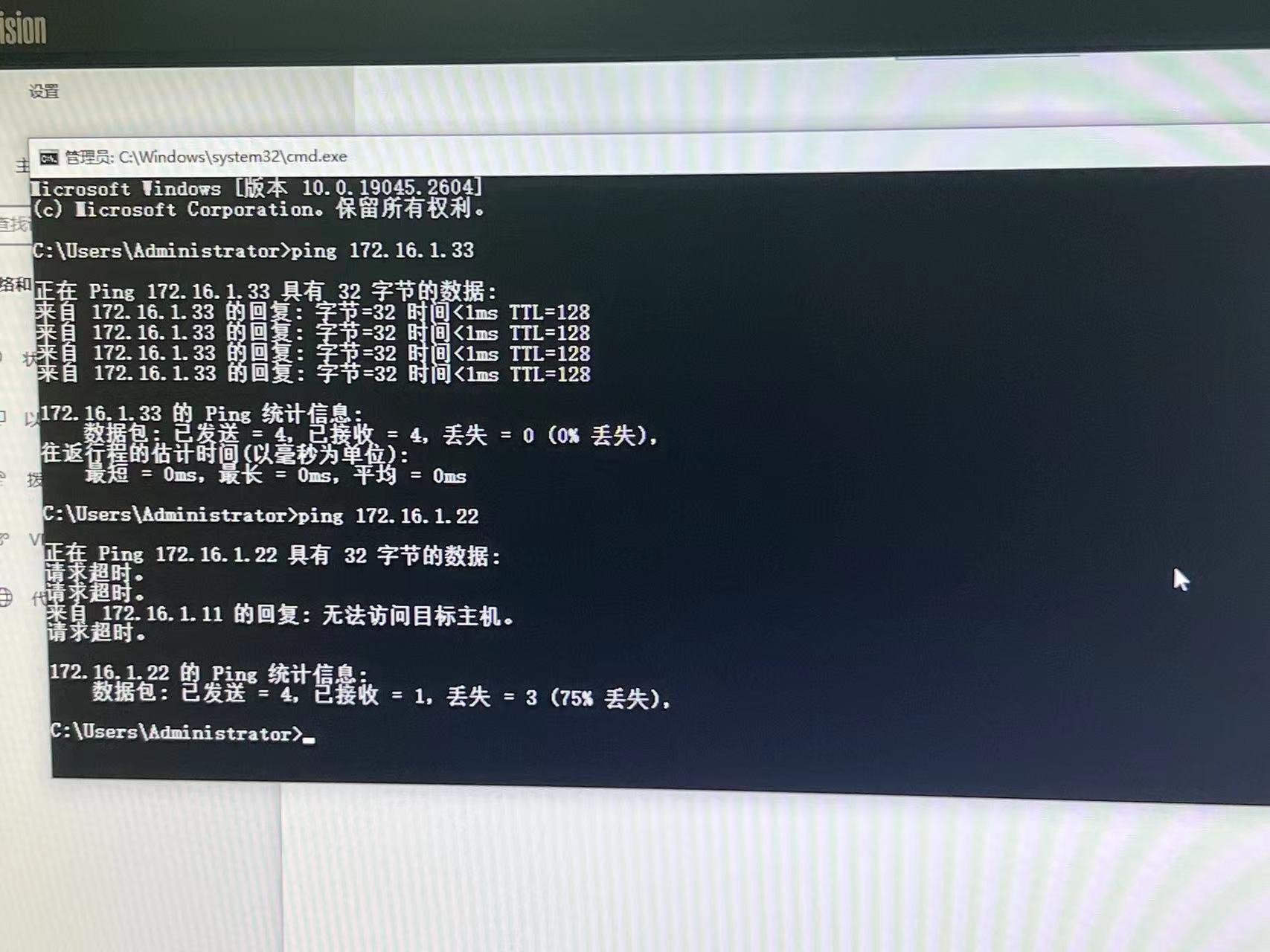
配置 PC3“网络实验”网卡的 IP 地址为：172.16.1.33/24，网关设为 172.16.1.254。

6.验证 PC1 和 PC3 能连通，但 PC1 和 PC2 不能连通，PC2 和 PC3 也不能连通。

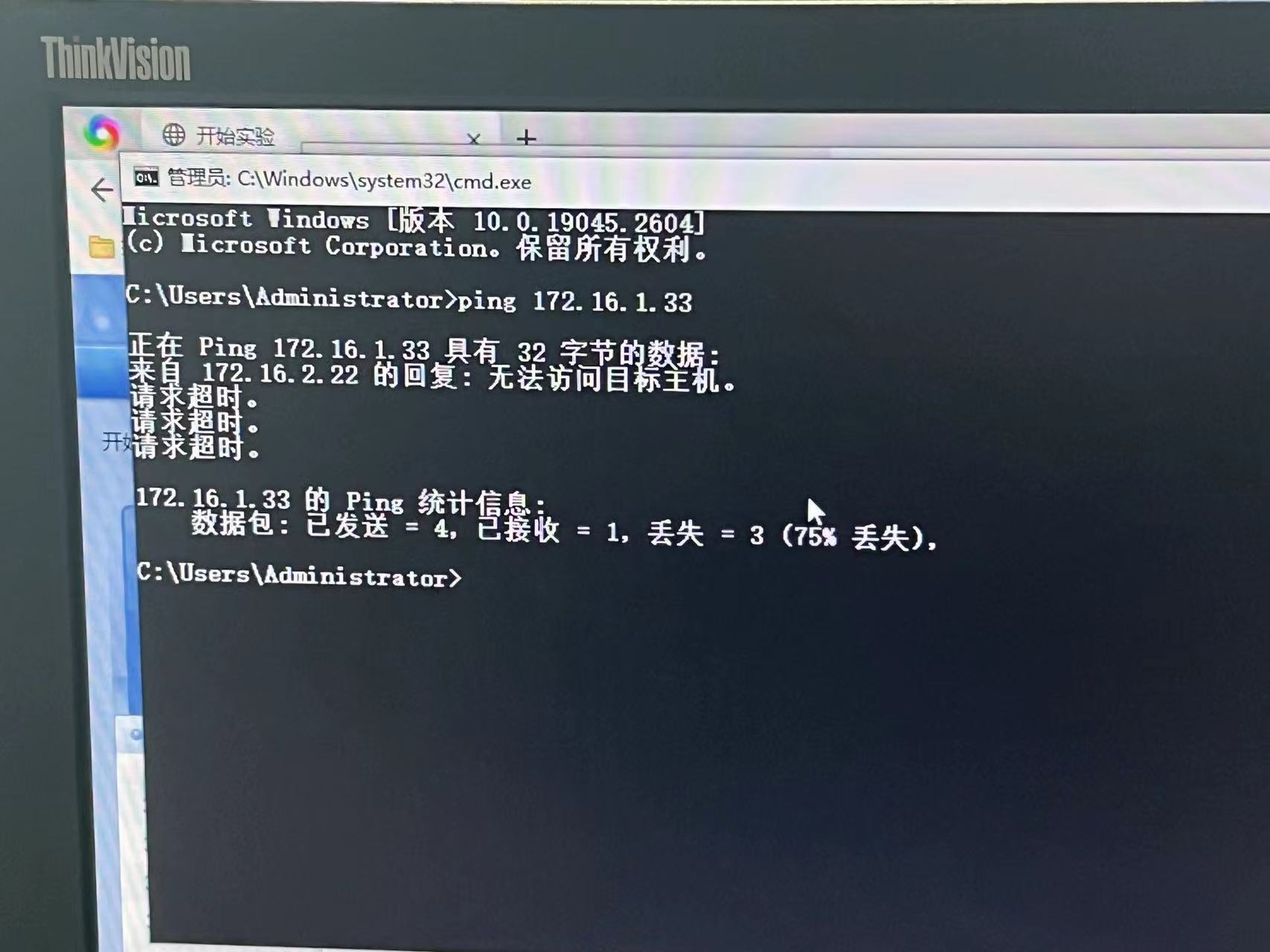
(1) 在 PC1 命令行下输入：ping 172.16.1.33，查看现象；



(2) 在 PC1 命令行下输入：ping 172.16.1.22，查看现象；



(3) 在 PC2 命令行下输入：ping 172.16.1.33，查看现象；



7.在三层交换机上设置vlan地址

switchB(Config)#int vlan 10

switchB(Config-if)#ip address 172.16.1.254 255.255.255.0 !配置虚接口 vlan10 地址 switchB(Config-if)#exit

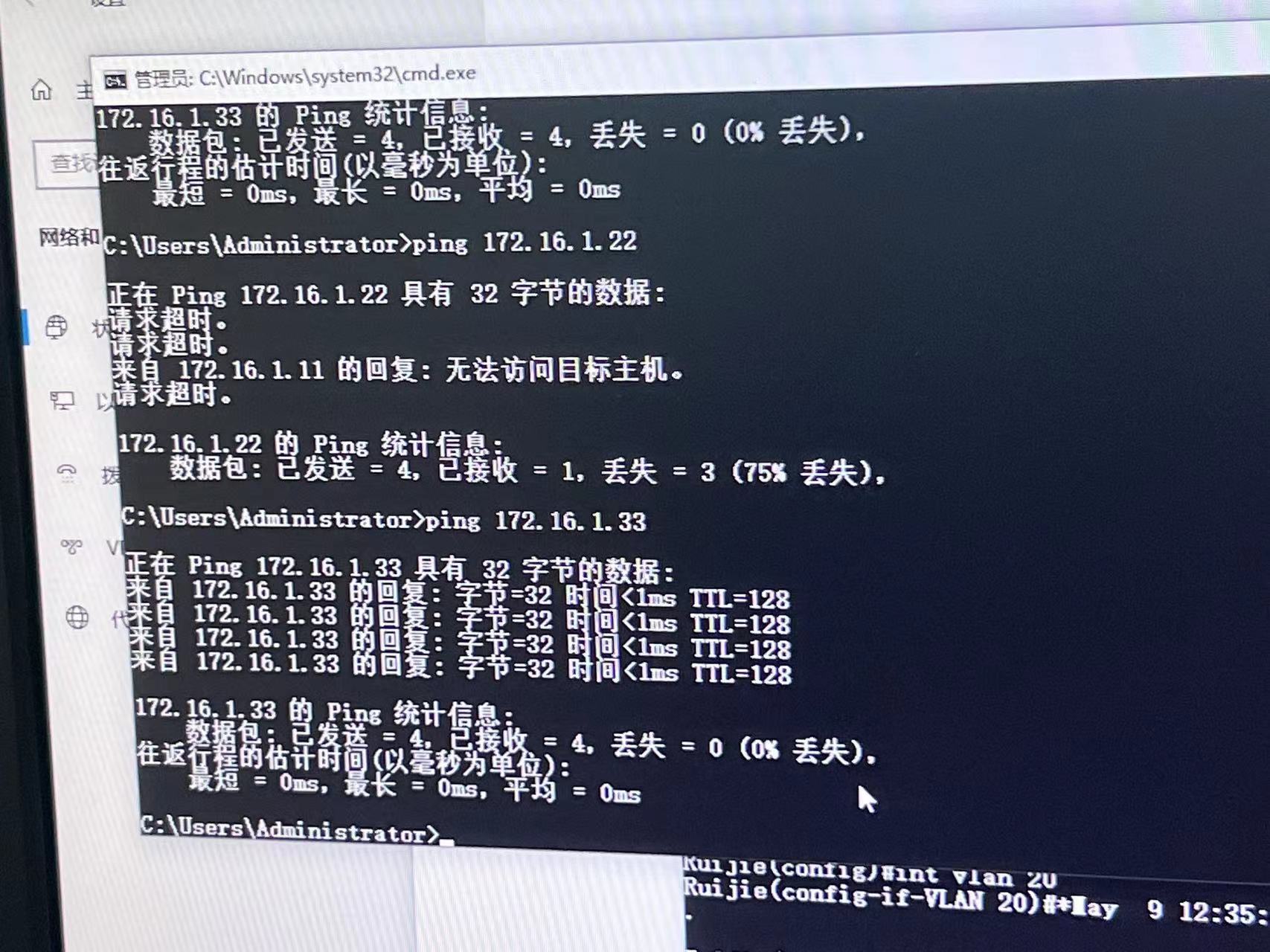
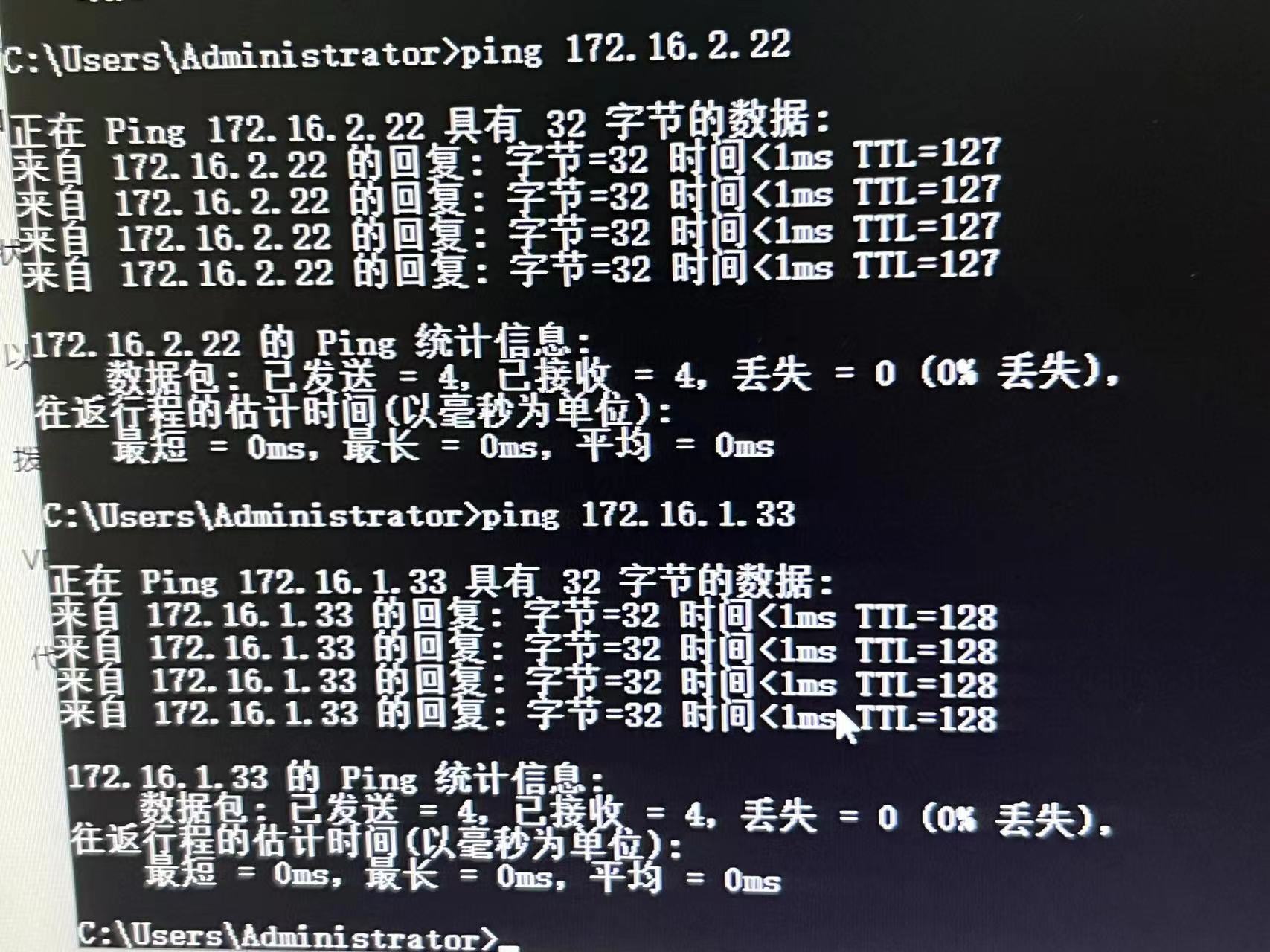
switchB(Config)#int vlan20

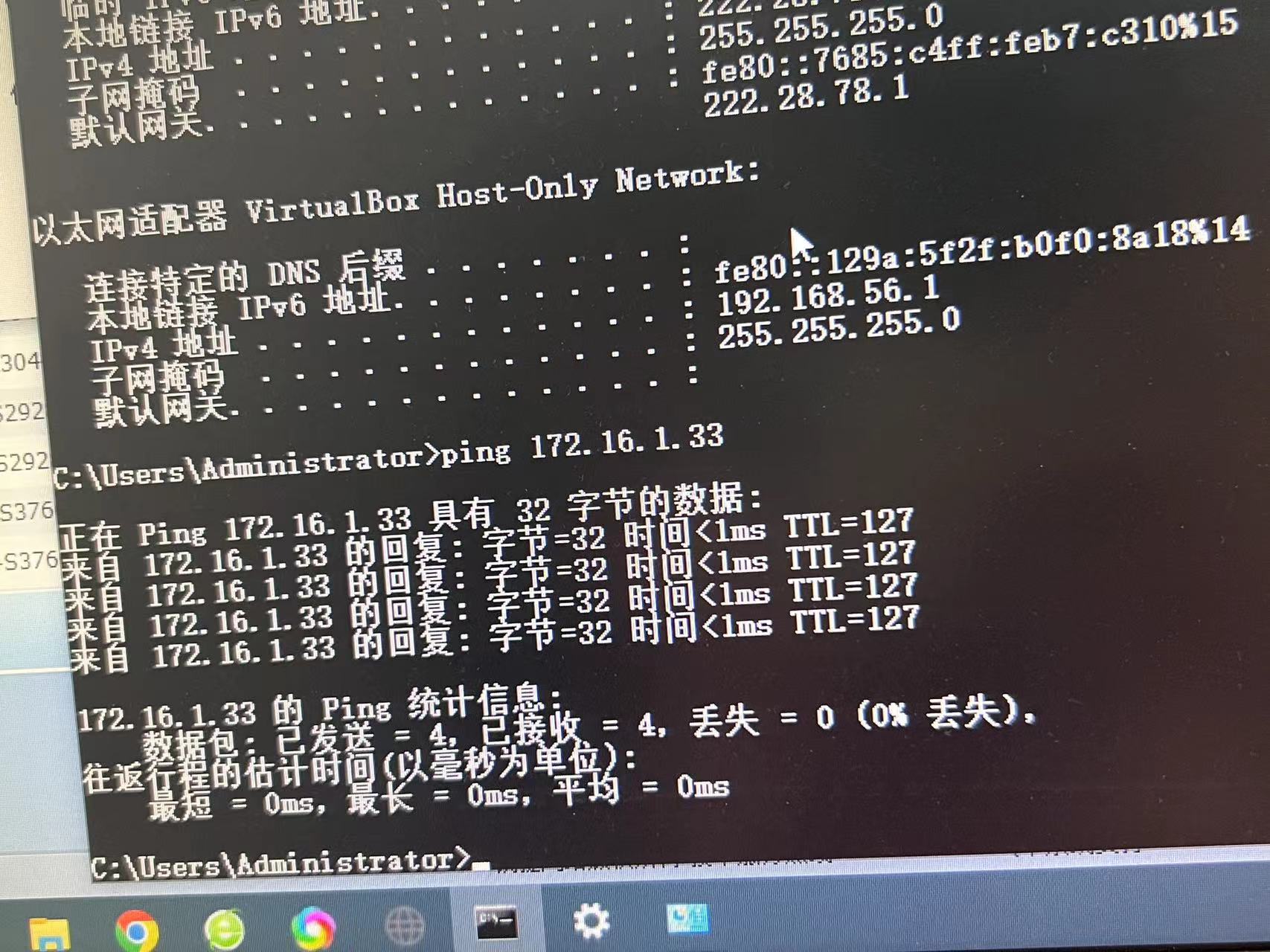
switchB(Config-if)#ip address 172.16.2.1 255.255.255.0 !配置虚接口 vlan20 地址 switchB(Config-if)#end

switch#show ip interface brief

8.检验连通性

验证 PC1 和 PC3 能连通，PC1 和 PC2 也能连通，PC2 和 PC3 也能连通。

1. 在 PC1 命令行下输入：ping 172.16.1.33，查看现象；
2. 在 PC1 命令行下输入：ping 172.16.2.22，查看现象；
3. 

（3） 在 PC2 命令行下输入：ping 172.16.1.33，查看现象；

**实验结果与分析：**

**1.首先就是在三层交换机上还没有设置vlan地址，ip地址的时候，三台PC是无法连通的，**

**后面给三层交换机设置了vlan和ip地址之后才能相互之间连通。为什么会这样呢？是因为在默认的情况下，三台PC是处于不同的广播域中，无法直接进行ping通，后面我们给他加上了vlan的接口，将三层交换机开启了路由功能，然后不同vlan下的PC就可以互相ping通了。**

**问题思考和解决方法：**

**1.三层交换机如何开启路由功能？**

**（1）在三层交换机中创建vlan，并且添加端口，然后将两个交换机的端口定义为Trunk模式**

**（2）进入vlan接口配置后，配置ip地址**

**（3）IP routing开启路由功能**

（4）配置路由

（5）保存配置

2.交换机虚拟接口（Switch Virtual Interface，SVI），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？

switchB(Config)#int vlan 10

switchB(Config-if)#ip address 172.16.1.254 255.255.255.0 !配置虚接口 vlan10 地址 switchB(Config-if)#exit

switchB(Config)#int vlan20

switchB(Config-if)#ip address 172.16.2.1 255.255.255.0 !配置虚接口 vlan20 地址 switchB(Config-if)#end

分别进入不同的vlan，然后开始配置ip地址。

# 实验名称：实验三 最简路由器组网

**实验目的：**

**1、掌握路由器命令行各种操作模式的区别，以及模式之间的切换；**

**2、掌握路由器端口的常用配置参数；**

**3、查看路由器系统和配置信息，掌握当前路由器的工作状态。**

**实验仪器：**

Router 路由器（1 台）、主机（2 台）、直连线（2 条）。

**实验原理：**

(1) 在因特网中是基于广播方式传输数据的，即所有的物理信号都要经过同一网段的所有设备。

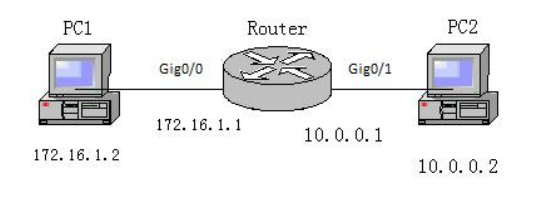
(2) 网卡可设置成混杂模式，在这种模式下网卡能接收到一切通过它的数据，能不管实际上的数据的目的地址是不是它。计算机直接传输的数据是大量的二进制数据，因此一个网络监听程序还必须使用特定的网络协议来分解嗅探到的数据，嗅探器通过解析数据包头部的各字段含义，能够识别出这个数据片段对应于哪个协议，实现正确得解码。

（3）将多个网络设备连接到路由器上，模拟真实的网络环境。可以使用有线或无线方式进行连接，也可以同时使用两种方式。

（4）在完成路由器的配置和设备的连接后，可以开始测试网络连接。可以使用 ping 命令，检查网络设备之间是否可以正常通信，并观察数据包的转发情况。

**实验内容与步骤：**

1.连线



2. 配置路由器ip地址

配置路由器的 Gig0/0 以太网口地址为 172.16.1.1 255.255.255.0；

配置路由器的 Gig0/1 以太网口地址为 10.0.0.1 255.0.0.0

Ruijie> enable

Ruijie#show ip interface brief

Ruijie# configure terminal

Ruijie (config)# interface gi 0/0

Ruijie (config-if)# ip address 172.16.1.1 255.255.255.0

Ruijie(config-if)# no shutdown

Ruijie(config-if)#exit

Ruijie (config)# interface gi 0/1

Ruijie(config-if)# ip address 10.0.0.1 255.0.0.0

Ruijie(config-if)# no shutdow



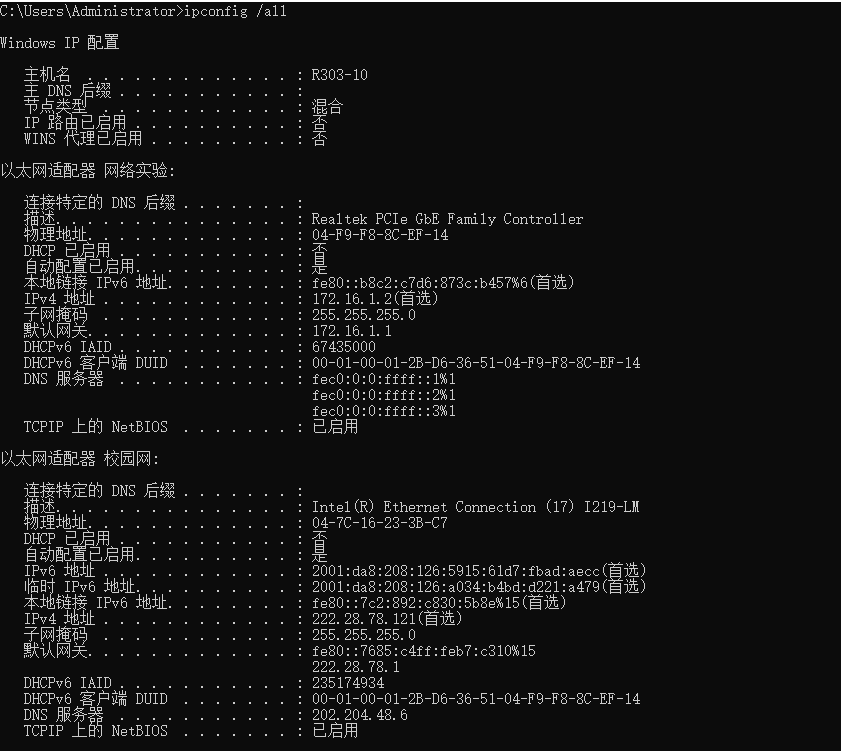
3.PC上ip地址的配置

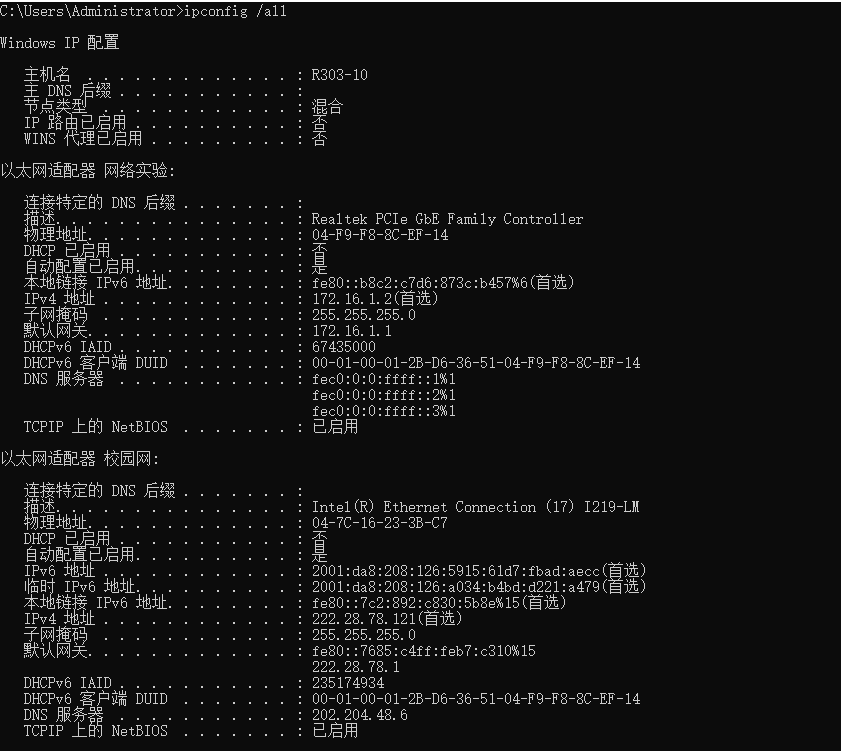
右键点击 PC 机上“网上邻居”，选择“属性”，找到“网络实验”，右键点击“属 性”，选择“TCP/IP”，可配置 IP 地址和相应掩码。

配置 PC1 的“网络实验”接口地址为 172.16.1.2/24，网关接口为 172.16.1.1；

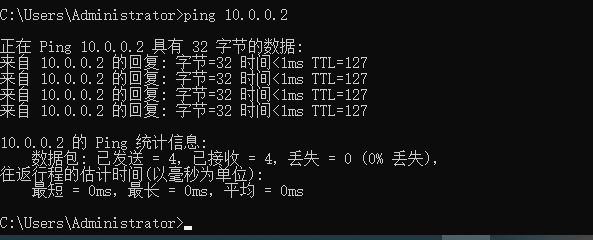
配置 PC2 的“网络实验”接口地址为 10.0.0.2/8，网关接口为 10.0.0.1；

在 PC 机的命令行状态下执行 ipconfig /all 命令查看配置是否生效

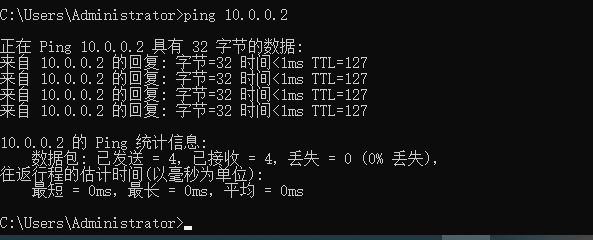




**在 PC1 命令行下输入命令 ping 10.0.0.2**



**在 PC2 命令行下输入命令 ping 172.16.1.2**



**5.修改路由器端口地址，重复过程**

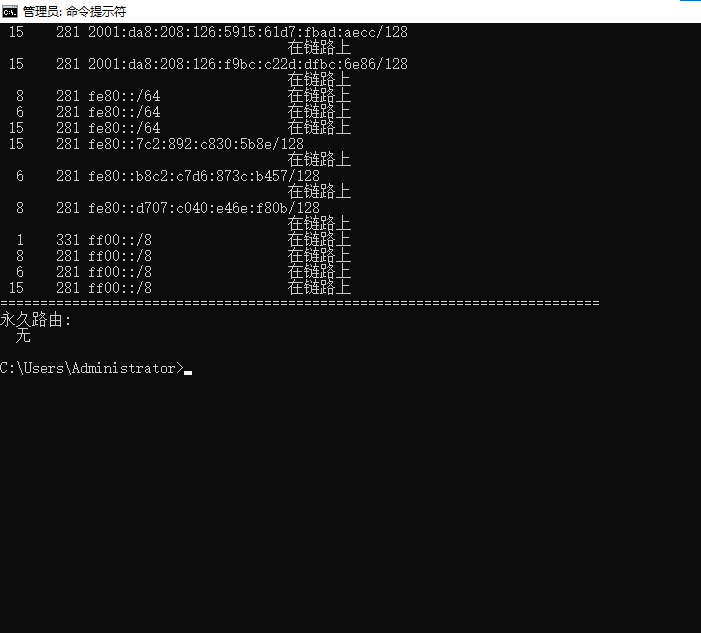
**路由器的 Gig0/1 以太网口地址修改为 172.16.1.3 255.255.255.0；**

**并将 PC2 的“网络实验”接口地址修改为 172.16.1.4/24，网关接口为 172.16.**

**6.查看路由表**







**4.实验结果与分析：**

**按照一开始的做法，是可以ping通的，因为PC1将数据传到路由器上，然后路由器接收到PC1的数据包之后，路由器根据PC1提供的目的地址查找路由表，根据路由表中的信息，路由器会数据包发送给目的主机PC2，所以可以PING通。但是在第六步中改变路由器的端口和pc网关之后，两个端口的网络号变成一样的，发生了冲突，最后导致无法配置成功。**

**问题思考和解决方法：**

1. **第五步中ping的命令可以执行成功，因为PC1将数据传到路由器上，然后路由器接收到PC1的数据包之后，路由器根据PC1提供的目的地址查找路由表，根据路由表中的信息，路由器会数据包发送给目的主机PC2，所以可以PING通。**
2. **第六步中，路由器配置不成功，改变路由器的端口和pc网关之后，两个端口的网络号变成一样的，发生了冲突，最后导致无法配置成功。**
3. **如果不配置PC机的网关，执行ping命令的时候会发现ping不通。**
4. **不可以ping通，两台主机相互ping无法成功，是因为在路由器的路由表中，没有配置相对应的路由，导致当有数据包传送时，路由器无法找到对应的目的地址，无法传送。**

# 实验名称：实验四 静态路由实验

**实验目的：**

**1、深入掌握 IP 协议和路由原理；**

**2、掌握静态路由配置方法；实验仪器：**

**实验原理：**

**1.实验拓扑图如下：**



* + - 1. 1、静态路由静态路由是由管理员在路由器中手动配置的固定路由。配置静态路由需要注意以下几点。（1）需要有目标IP（2）需要有与静态路由直接相连的下一路由器接口的IP地址或静态路由的本地接口。（3）静态路由是由管理员手动设置的，除非管理员干预，否则静态路由不会发生变化。静态路由特点（1）允许对路由的行为进行精准的控制。（2）静态路由是单向的。（3）静态路由器的缺点就是缺乏灵活性。

2、静态路由是指由用户或网络管理员手工配置的路由，当网络拓扑结构或链路状态发生变化时，需要手工去修改路由表的相关信息，在默认情况下，静态路由是私有的，不会传递给其他路由器，也不通过路由器发通告消息，从而节省网络带宽和路由器的运算资源。静态路由是单向的，适合小型网络或结构比较稳定的网络。

**实验内容与步骤：**

**1.为路由器添加串口模块**

**2.配置路由器接口地址：**

配置路由器 R0 的 Gig0/0 以太网口地址为 172.16.1.1 255.255.255.0；

配置路由器 R0 的串口 Serial 0/1/0 地址为 172.16.2.1 255.255.255.0；串口需要配置时钟频率。

Router0> enable

Router0# configure terminal

Router0 (config)# interface gi 0/0

Router0(config-if)# ip address 172.16.1.1 255.255.255.0

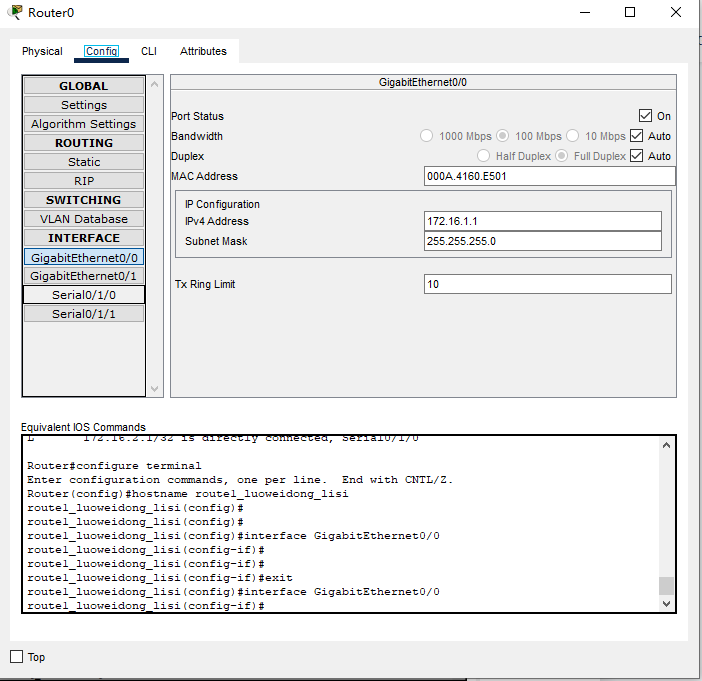
Router0 (config-if)# no shutdown

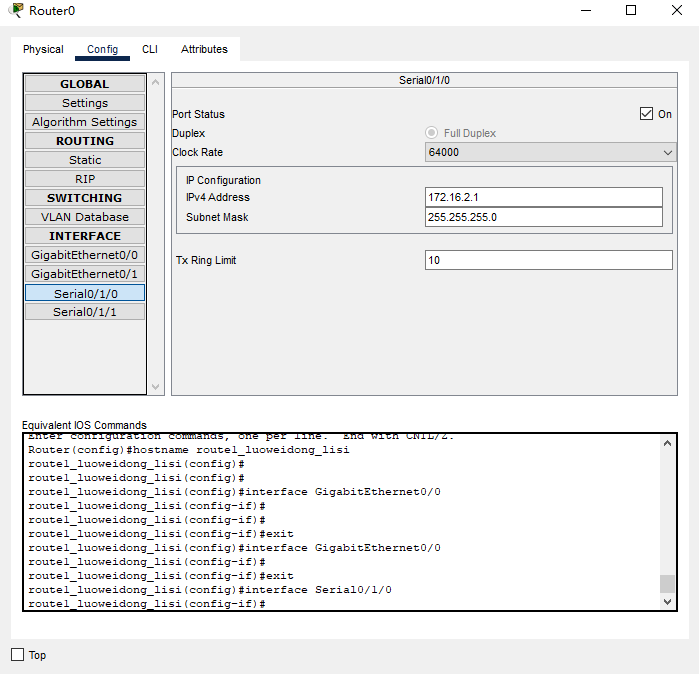
Router0 (config)# interface serial 0/1/0

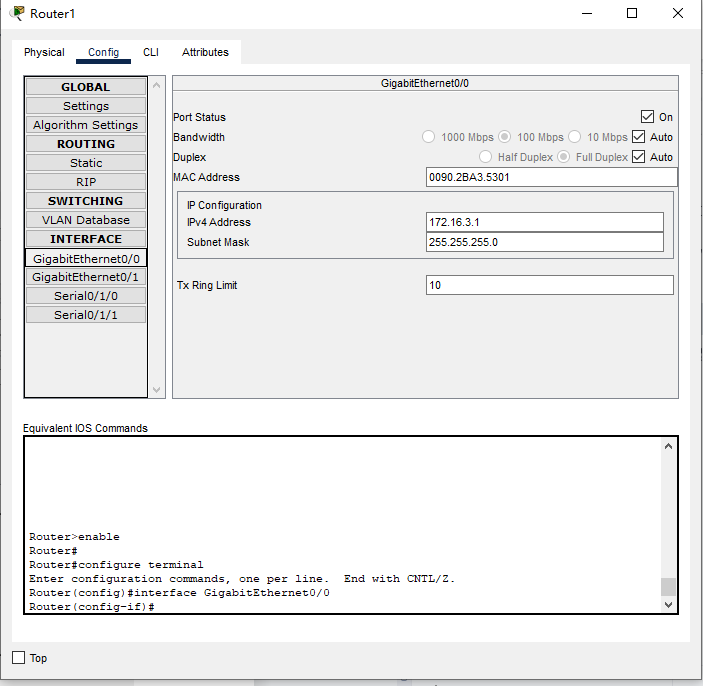
Router0 (config-if)# ip address 172.16.2.1 255.255.255.0

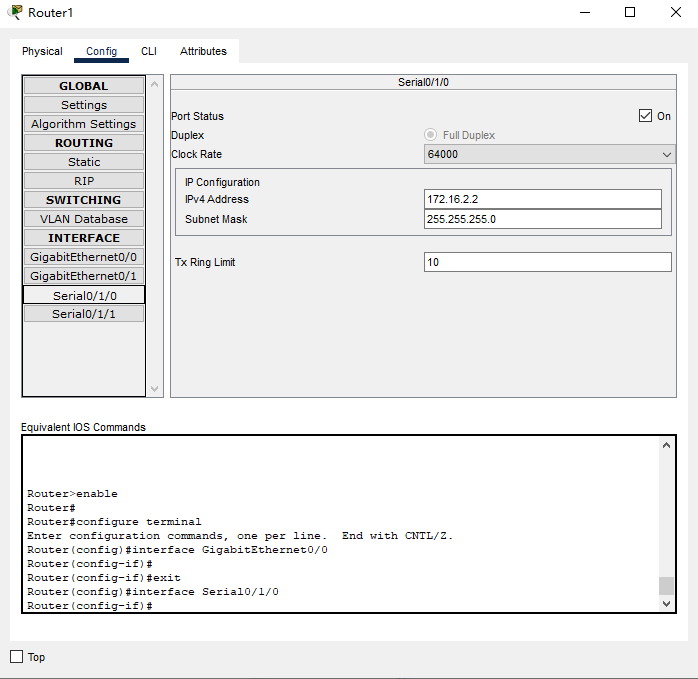
Router0 (config-if)# clock rate 64000 配置 Router0 的时钟频率（DCE）

Router0 (config-if)# no shutdown



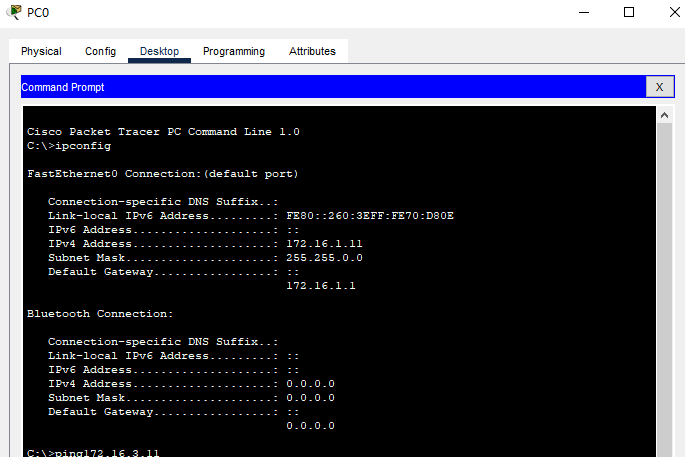




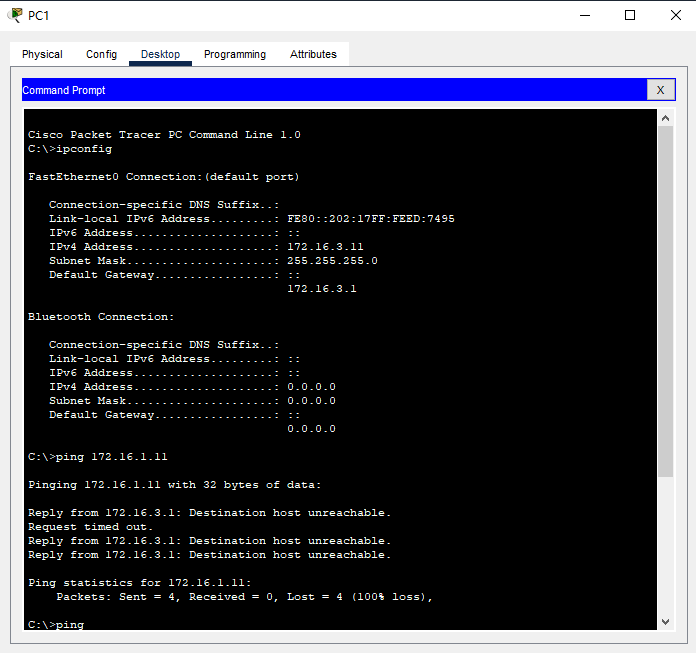


4.PC机ip地址配置

配置 PC0 的地址为 172.16.1.11/24，网关接口为 172.16.1.1；



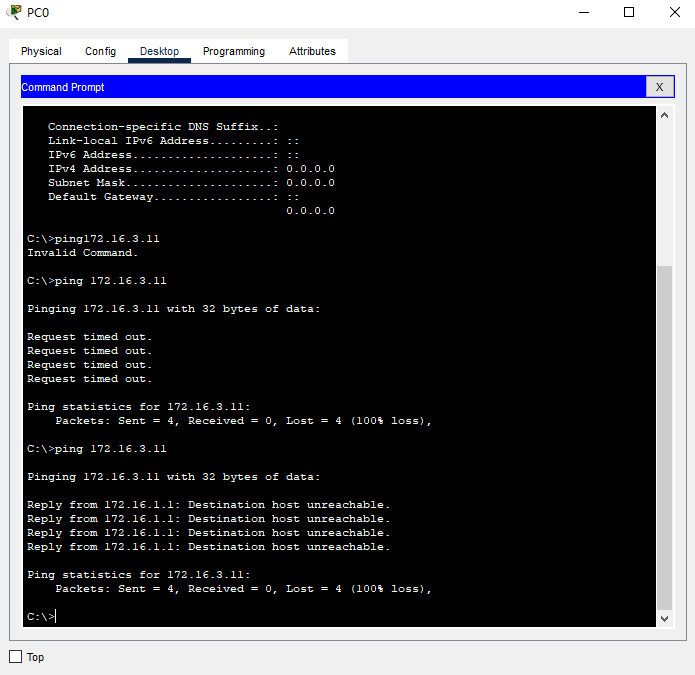
配置 PC1 的地址为 172.16.3.11/24，网关接口为 172.16.3.1；



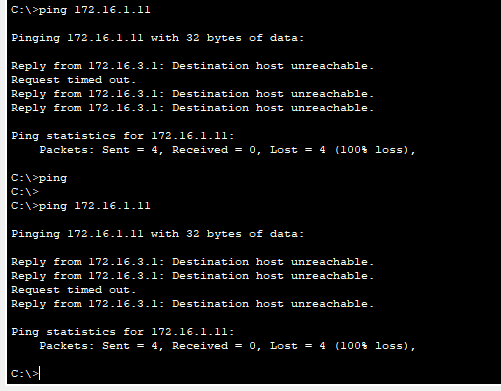
在 PC 机的命令行状态下执行 ipconfig 命令查看配置是否生效。

4.查看实验结果

**在 PC0 命令行下输入命令 ping 172.16.3.11**

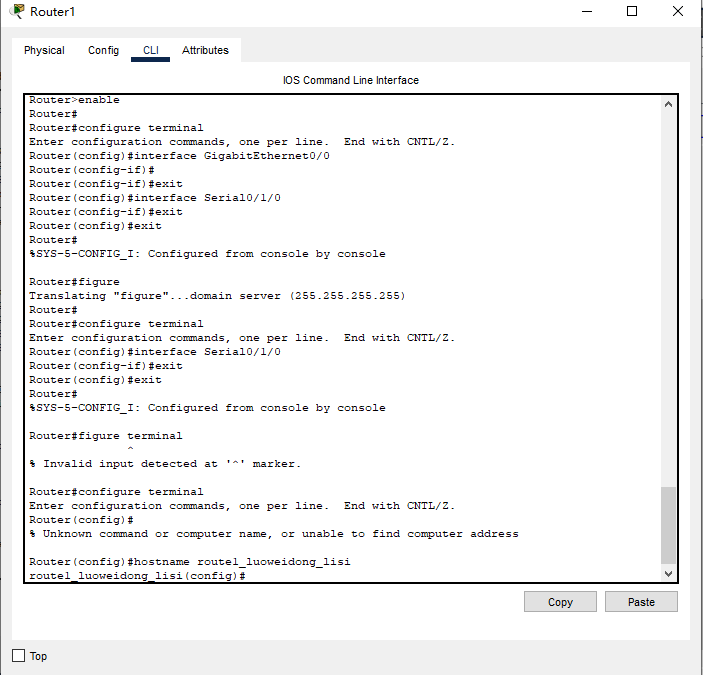


**在 PC1 命令行下输入命令 ping 172.16.1.11**



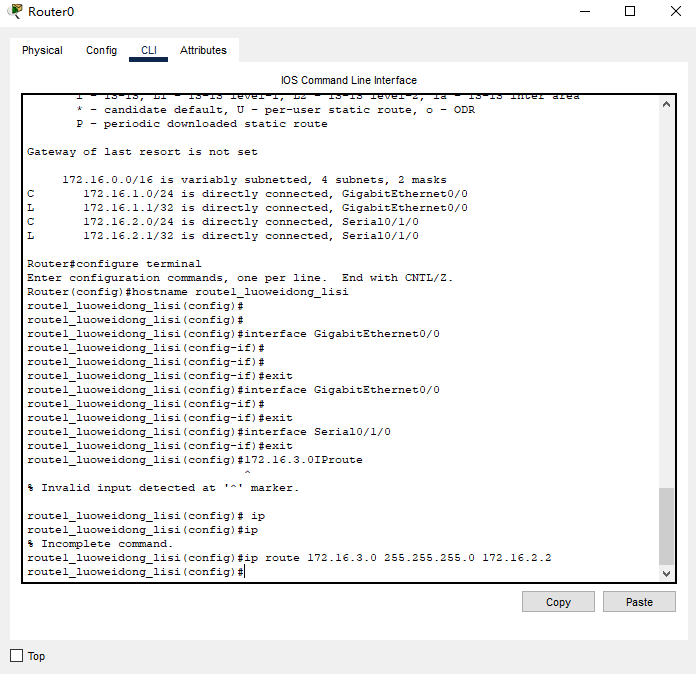
**观察现象，记录是否成功。**

**在路由器上的“router#”模式（特权用户模式）下，使用“show ip route**

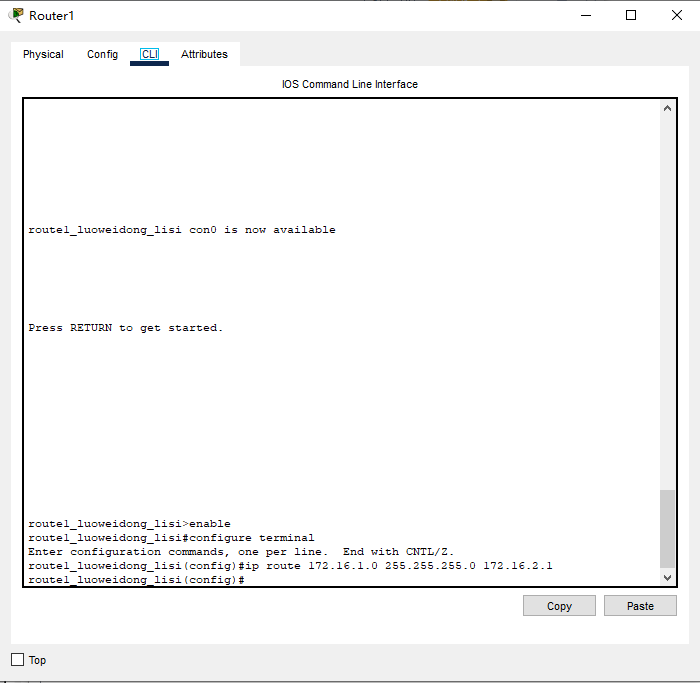


**5.写入静态路由表**

在 Router0 上配置路由 R0 (config)# ip route 172.16.3.0 255.255.255.0 172.16.2.2

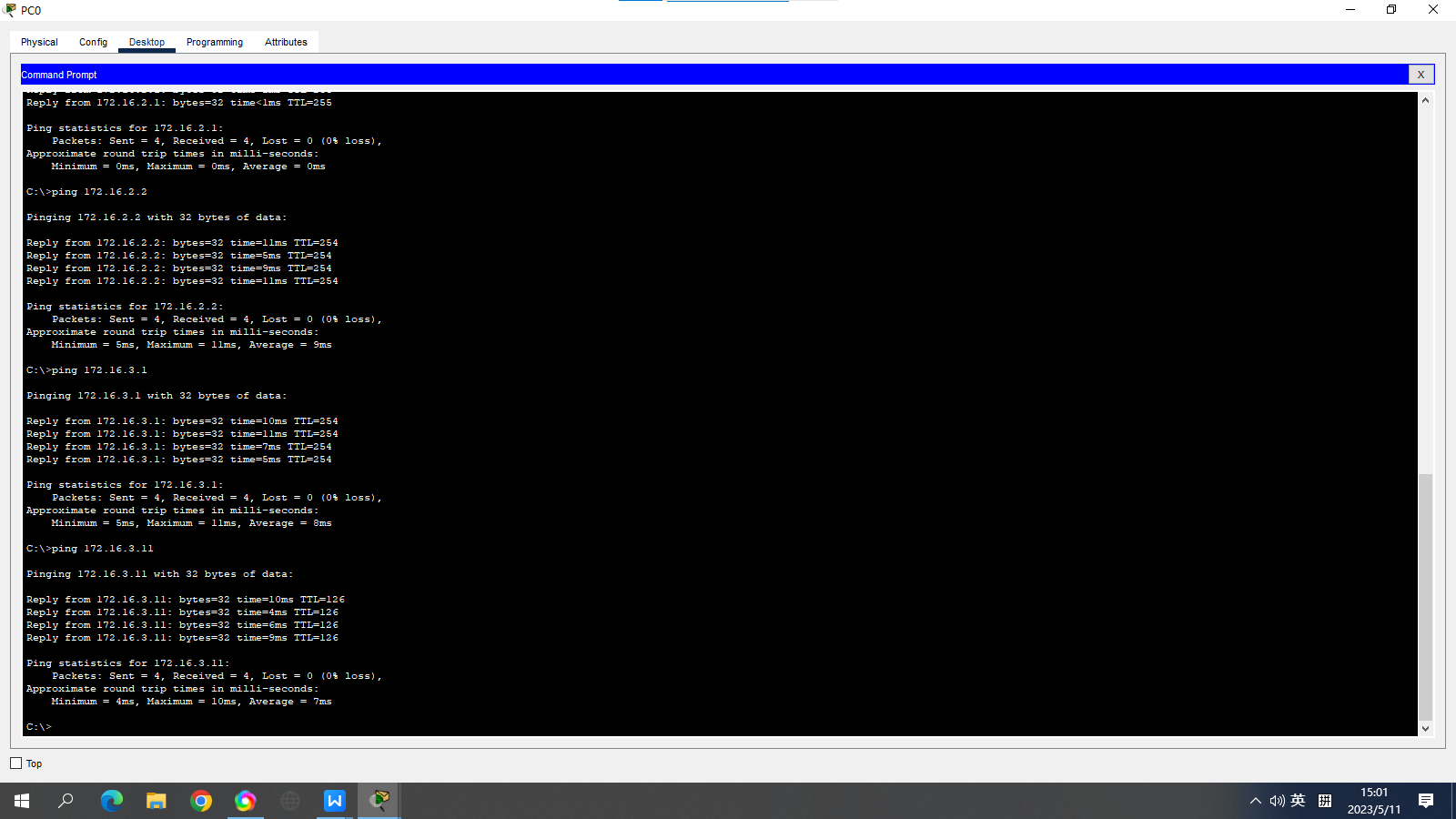


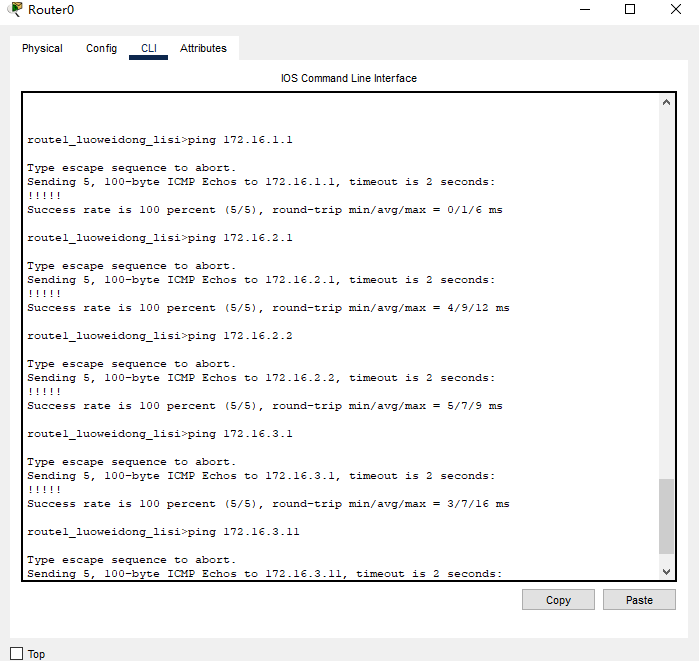
在 Router1 上配置路由 R1 (config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1

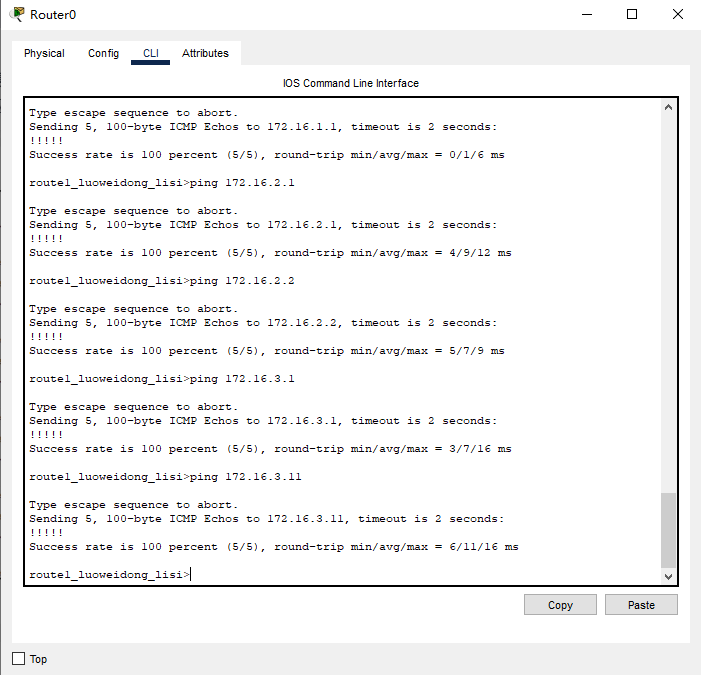


**6.分段测试**







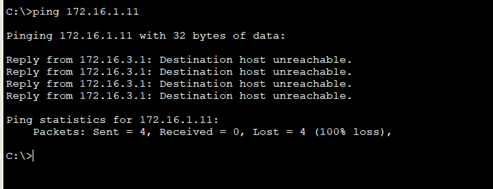


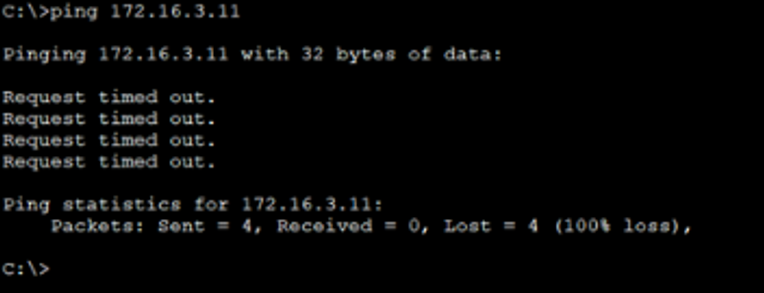
**实验结果与分析：**

**一开始ping的时候，两台PC是无法ping通的，是因为在路由器的路由表中，没有相应的路由和目的IP地址，所以当有数据包传送的时候，路由器无法找到对应的目的地址，所以最后无法发传送。而在后面配置好了静态路由表之后两台PC之间才可以互相ping通。**

**问题思考和解决方法：**

1. **在步骤四中PC0pingPC1无法ping通，是因为在路由器的路由表中，没有相应的路由和目的IP地址，所以当有数据包传送的时候，路由器无法找到对应的目的地址，所以最后无法发传送。**
2. **步骤七中，路由表中有五条，但是之前之后四条，多了一个172.16.1.0/24[1/0]via 172.16.2.1**
3. **R1上取消静态路由之后**





后面找不到目的地址，所以无法ping通。

# 实验名称：实验五 RIP 动态路由实验

**实验目的：**

**1、深入掌握动态路由原理；**

**2、掌握动态路由 RIP 配置方法；**

**3、掌握 RIP 路由工作原理。**

**实验仪器：**

Router 路由器（3 台）、主机（3 台）

**实验原理：**

Internet划分成不同的自治系统（Autonomous System，简称AS），每个AS由单一的管理机构决定内部的路由选择策略，在AS之间使用另外的路由交换方式。一般在AS内部使用的路由选择协议叫做IGP，或者叫做Intra-AS协议；在自治系统之间交换路由信息的协议叫做EGP，或者叫做Inter-AS协议。现在Internet上主要采用的EGP叫做BGP。

RIP（Routing Information Protocol）协议标准包括只支持分类IPv4地址的的RIPv1（RFC1058）和支持无类IPv4地址的RIPv2（RFC2453）以及支持IPv6的RIPng（RFC2080）三个版本。

RIP协议的工作原理如下：1.每个路由器都会定期广播自己的路由表，即向相邻路由器发送路由信息。2.接收到其他路由器广播的路由表后，每个路由器会将该路由表与自己的路由表进行比较，选择距离更短的路径更新到自己的路由表中。3.当路由器的路由表发生变化时，向相邻路由器发送更新信息，以便其他路由器能够及时更新路由表。4.如果某个路由器在一定时间内没有收到相邻路由器的更新信息，则认为该路由器已经失效，删除该路由器的信息。

在缺省情况下，RIP以30秒为周期向邻居发送响应报文；如收到邻居的请求报文，则应立即发送响应报文。假设有“目的为N，下一跳为R”的路由，经过180秒未收到关于N的任何更新信息，将该路由的metric置为16（不可达），如果再经120秒后仍未收到该路由的任何更新信息，则在路由表中删除该路由。

因为距离向量算法只和邻居交换信息，对目标采用估值等做法，会产生收敛慢、“坏消息传得慢”和“累加到无穷”等问题，一般采用“水平分割”（split-horizon）、“毒性反转”（poison-reverse，也叫带毒性反转的水平分割）、“触发更新”（triggered update）等方法提高可靠性。

水平分割：如果某路由条目下一跳是某邻居，则在向该邻居发送更新报文时不包含该路由条目信息。

毒性反转：如果某路由条目下一跳是某邻居，则在向该邻居发送更新报文时将该路由条目的metric值置为16。

触发更新：如果路由表发生改变（增加、删除或更新路由），立即发送更新报文而不等默认更新周期到来。

**实验内容与步骤：**

1.为路由器添加串口模块，并且按照拓扑图正确接线。

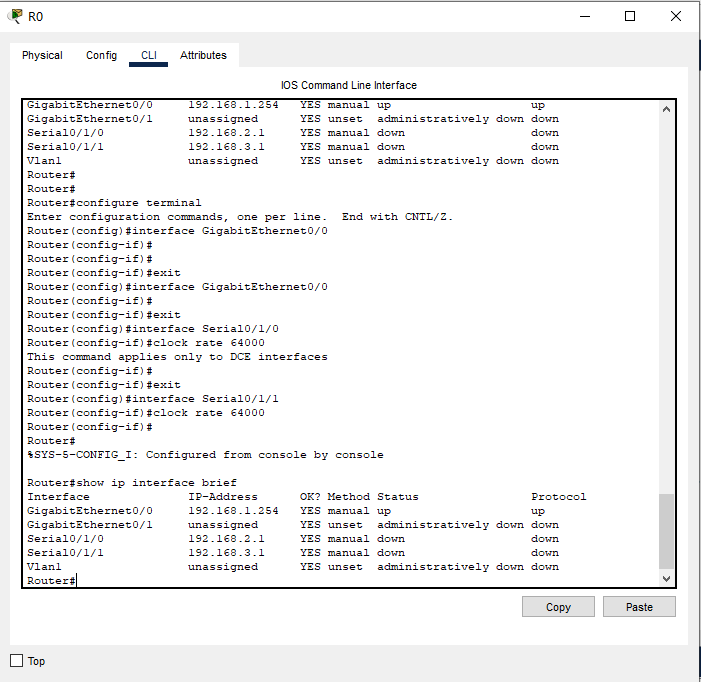
2.配置路由器R0接口网址

路由器 R0 的 Gi0/0 以太网口地址为 192.168.1.254 255.255.255.0；

路由器 R0 的串口 Se0/1/0 地址为 192.168.2.1 255.255.255.0；

路由器 R0 的串口 Se0/1/1 地址为 192.168.3.1 255.255.255.0；

配置完成后，使用 show ip interface brief 命令进行检查。



R0> enable

R0# configure terminal

R0 (config)# interface Gi 0/0

R0 (config-if)# ip address 192.168.1.254 255.255.255.0

R0 (config-if)# no shutdown

R0 (config)# interface Se0/1/0

R0 (config-if)# ip address 192.168.2.1 255.255.255.0

R0(config-if)#clock rate 64000

R0 (config-if)# no shutdown

R0 (config)# interface Se0/1/1

R0 (config-if)# ip address 192.168.3.1 255.255.255.0

R0(config-if)#clock rate 64000

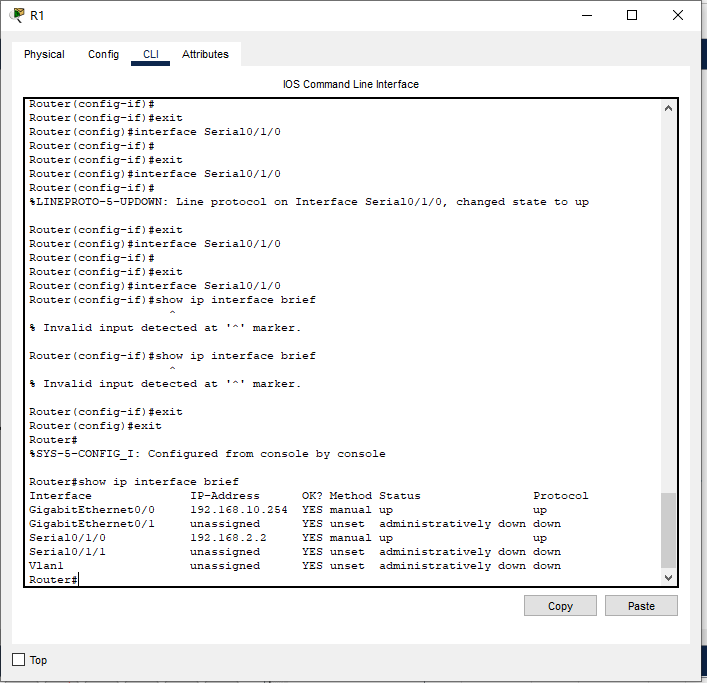
R0 (config-if)# no shutdown

**3.配置路由器R1的接口地址**

**路由器 R1 的 Gi0/0 以太网口地址为 192.168.10.254 255.255.255.0；**

**路由器 R1 的串口 Se0/1/0 地址为 192.168.2.2 255.255.255.0；**

**配置完成后，使用 show IP interface brief**

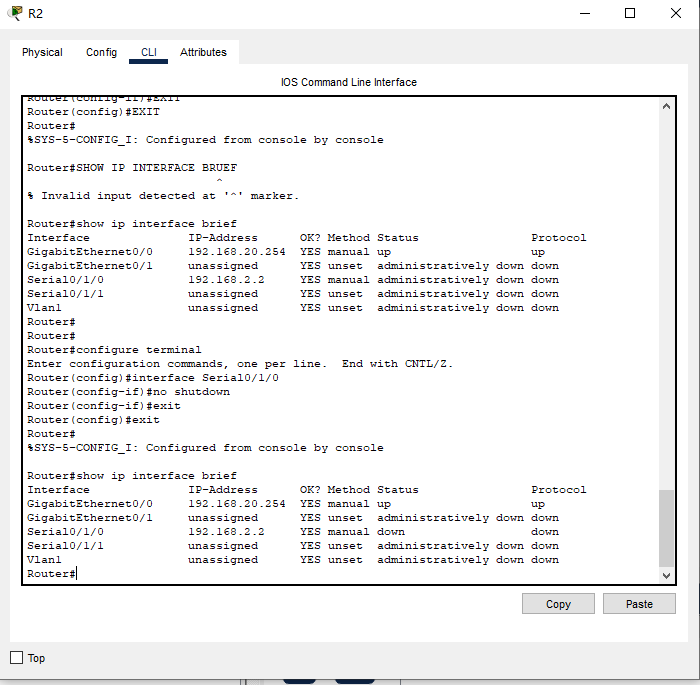


**4.配置路由器R2的接口地址**

**路由器 R2 的 Gi0/0 以太网口地址为 192.168.20.254 255.255.255.0；**

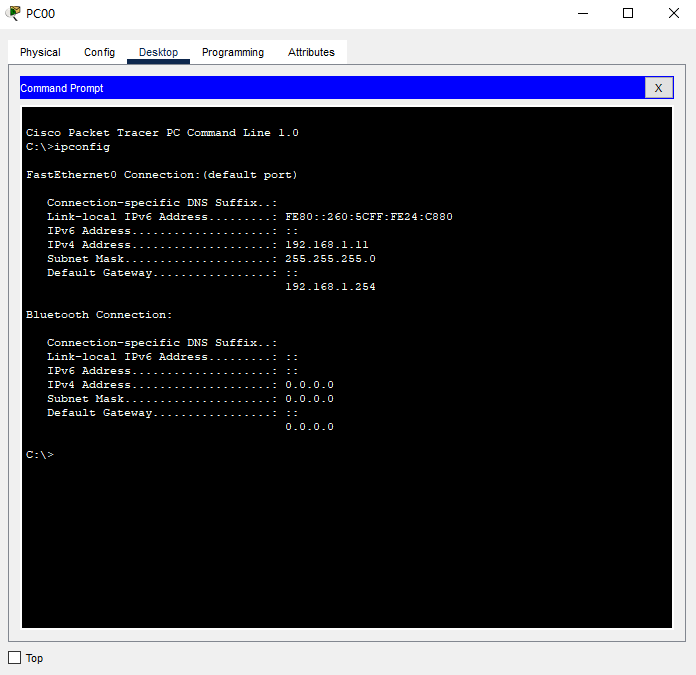
**路由器 R2 的串口 Se0/1/0 地址为 192.168.3.2 255.255.255.0；**

**配置完成后，使用 show IP interface brief**

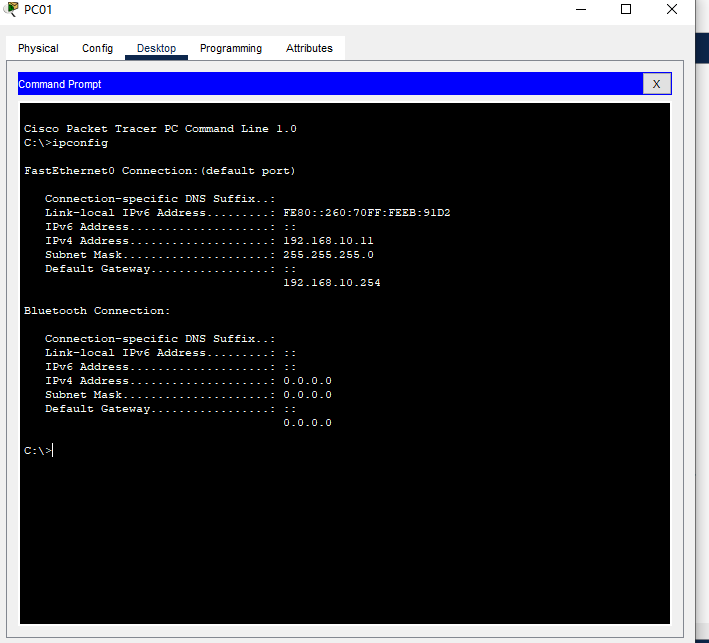


**5.PC机ip地址配置**

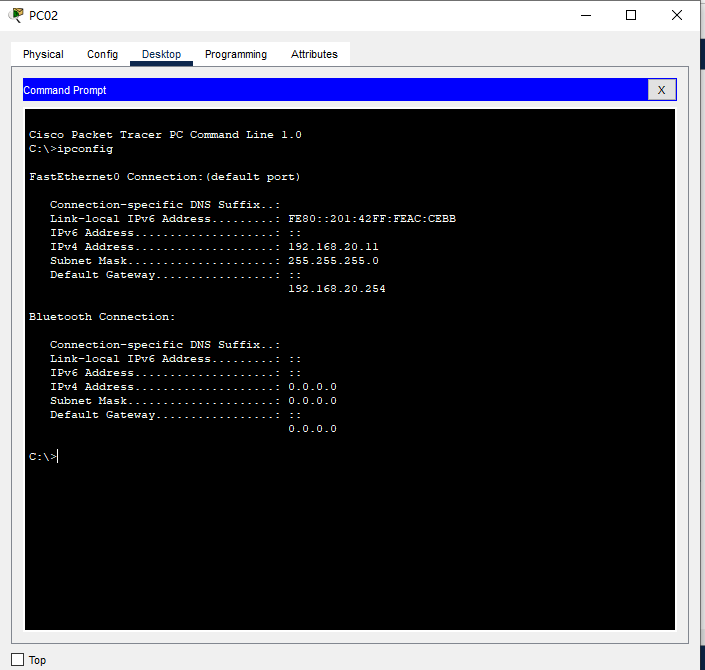
配置 PC0 的 IP 地址为 192.168.1.11/24，网关接口为 192.168.1.254；



配置 PC1 的 IP 地址为 192.168.10.11/24，网关接口为 192.168.10.254；



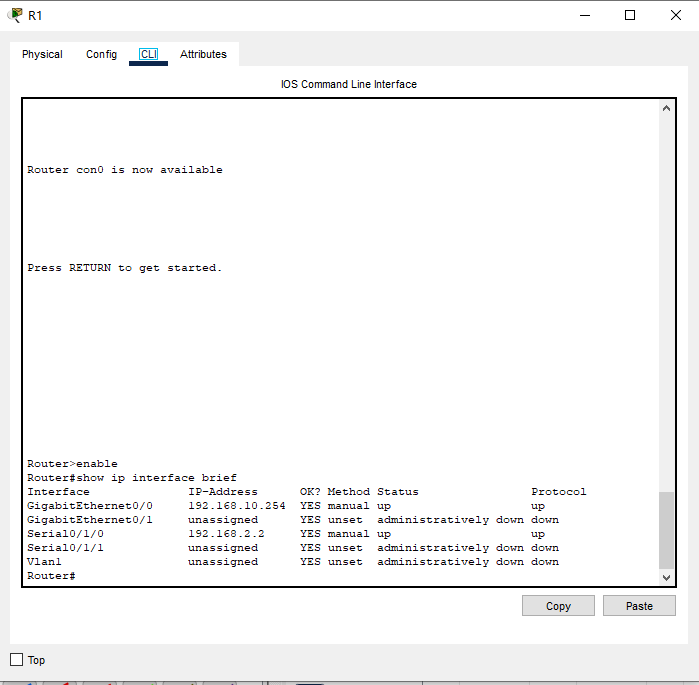
配置 PC2 的 IP 地址为 192.168.20.11/24，网关接口为 192.168.20.254；



在 PC 机的命令行状态下执行 ipconfig 命令查看配置是否生效。

**6.动态路由协议RIP设置**

（1）RIP 路由协议配置之前，show ip route 查看当前路由表



（2）路由器 R0 上 3 个网段在 RIP 路由区域

R0(config)#router rip ！进入 RIP 路由模式

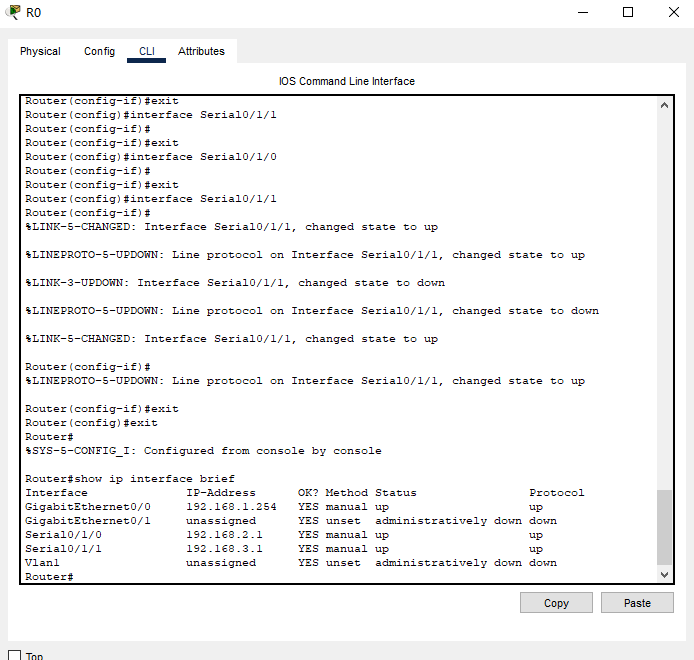
R0(config-router)#version 2 ！启用 RIPv2

R0(config-router)#no auto-summary !关闭自动汇总功能

R0(config-router)#network 192.168.1.0

R0(config-router)#network 192.168.2.0

R0(config-router)#network 192.168.3.0



路由器 R1 上 2 个网段在 RIP 路由区域。

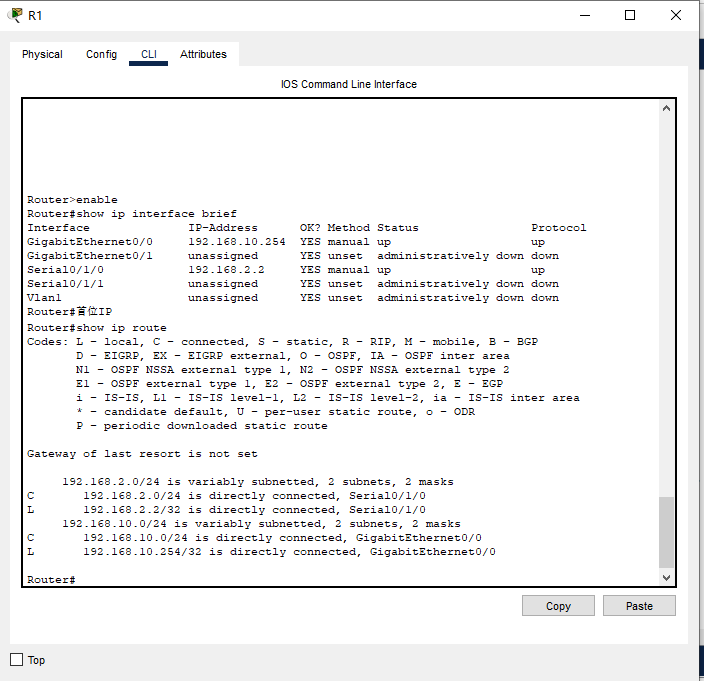
R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#no auto-summary

R1r(config-router)#network 192.168.10.0

R1(config-router)#network 192.168.2.0



路由器 R2 上 2 个网段在 RIP 路由区域。

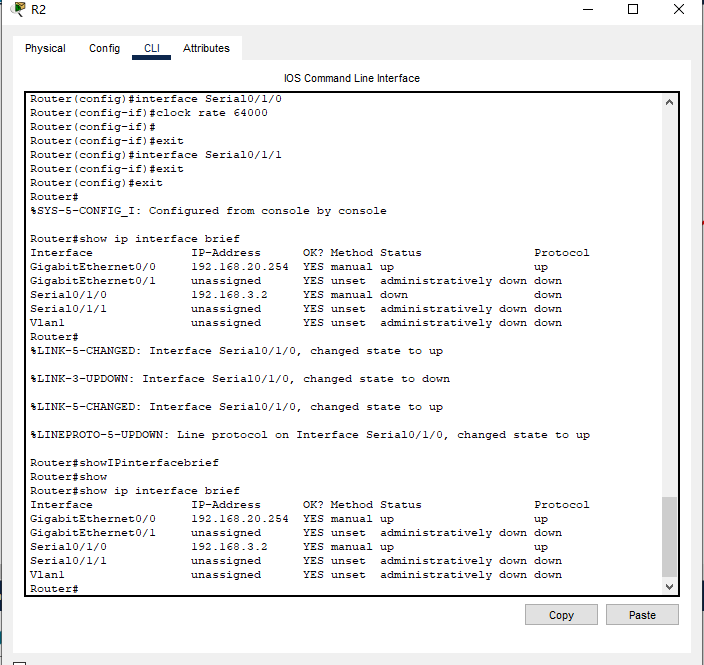
R2(config)#router rip

R2(config-router)#version 2

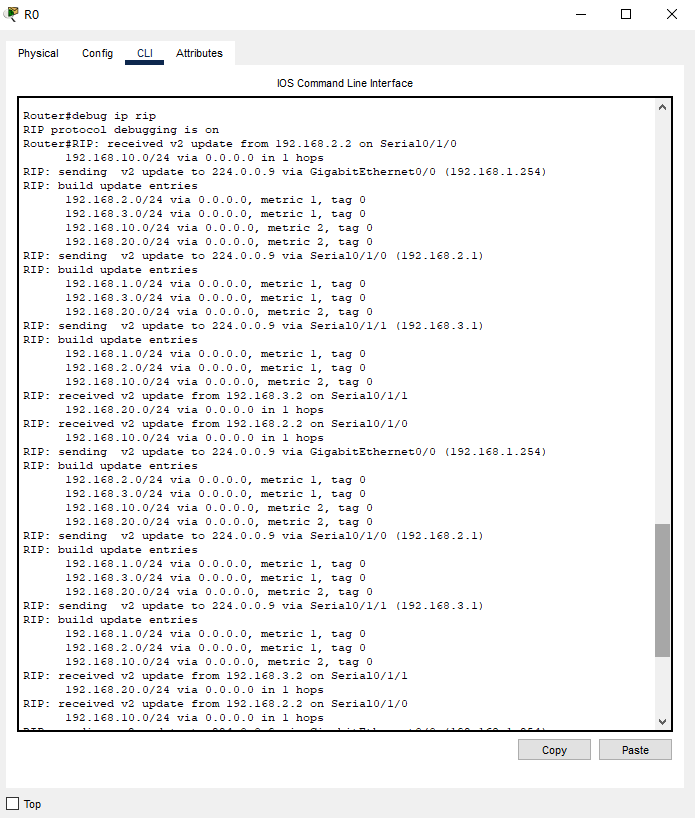
R2(config-router)#no auto-summary

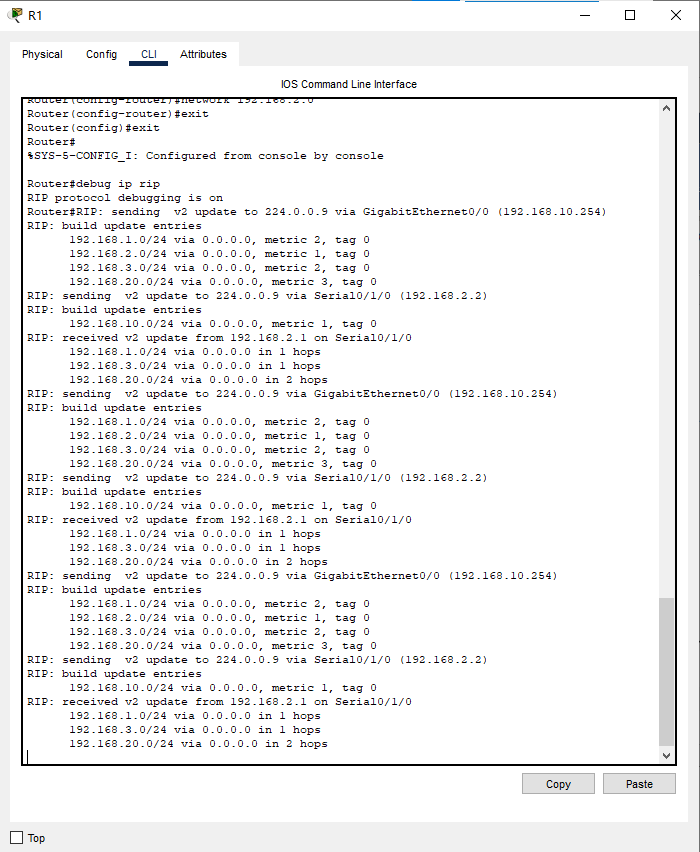
R2(config-router)#network 192.168.20.0

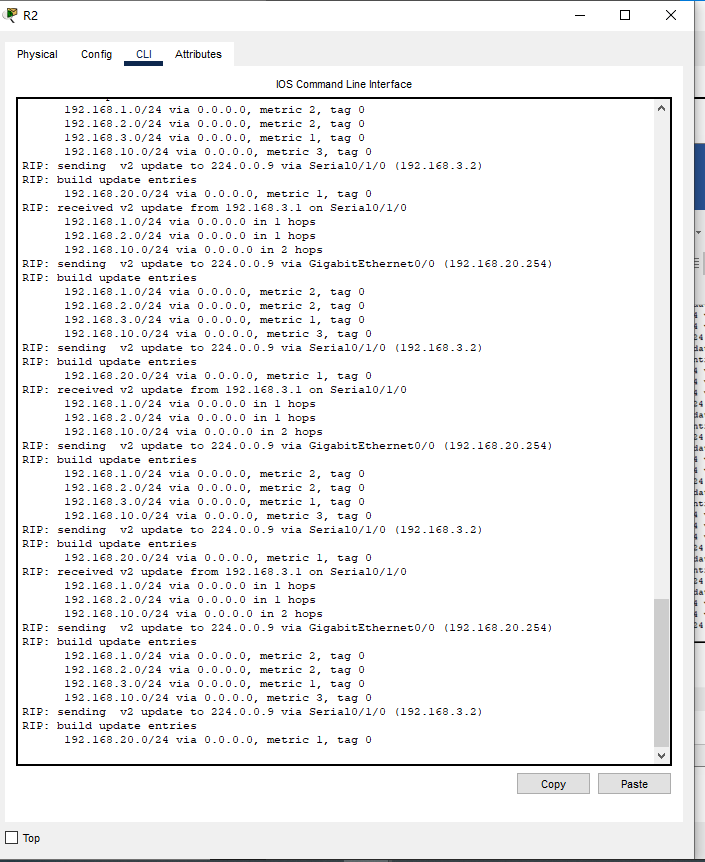
R2(config-router)#network 192.168.3.

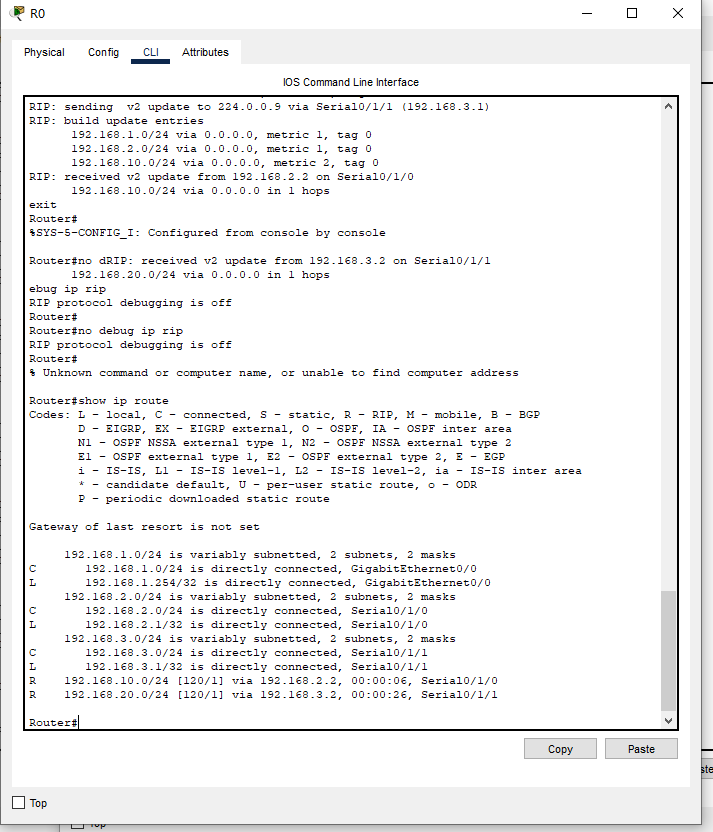


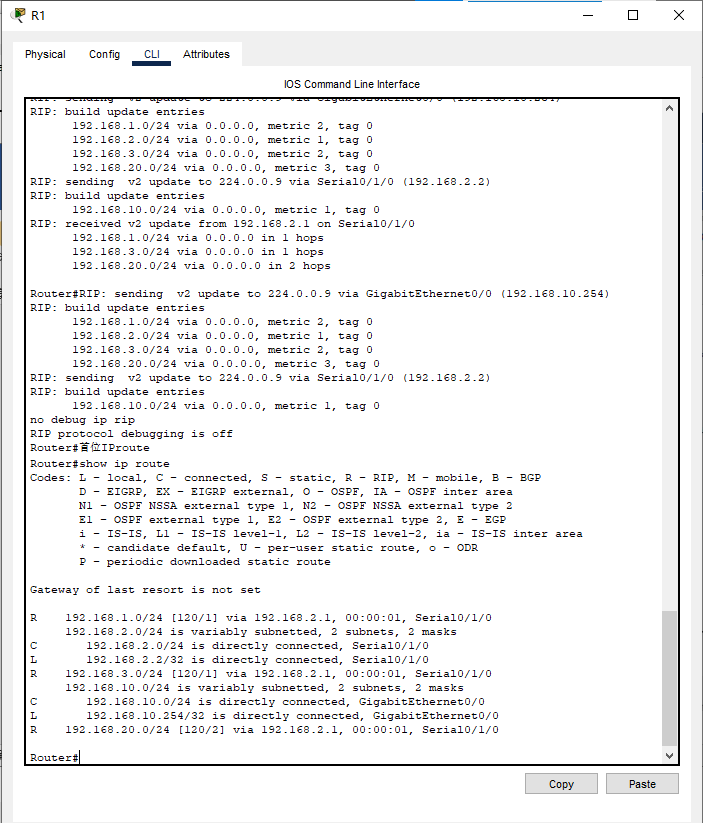
1. 路由器配置结束后，输入debug IP rip命令查看交互信息

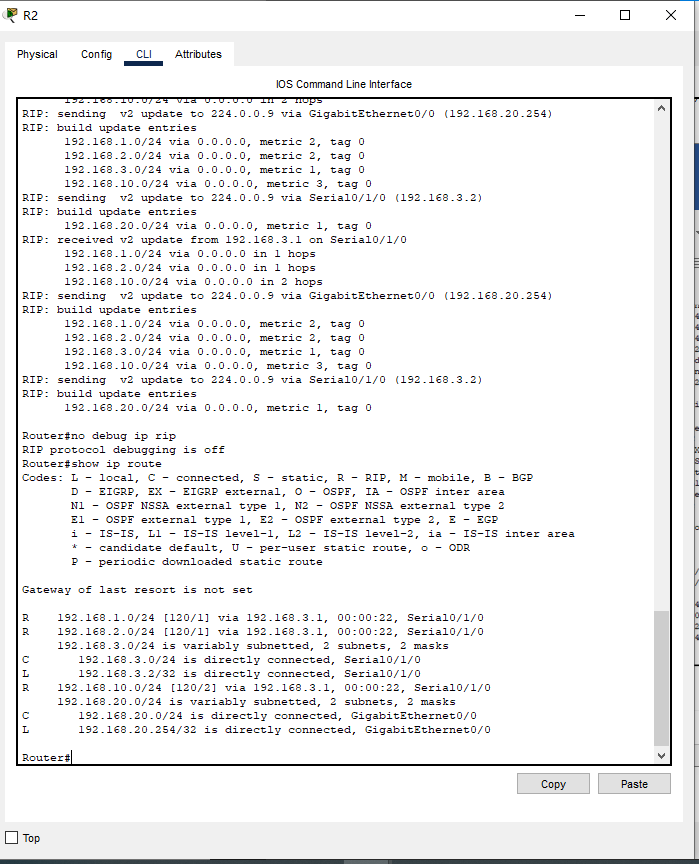






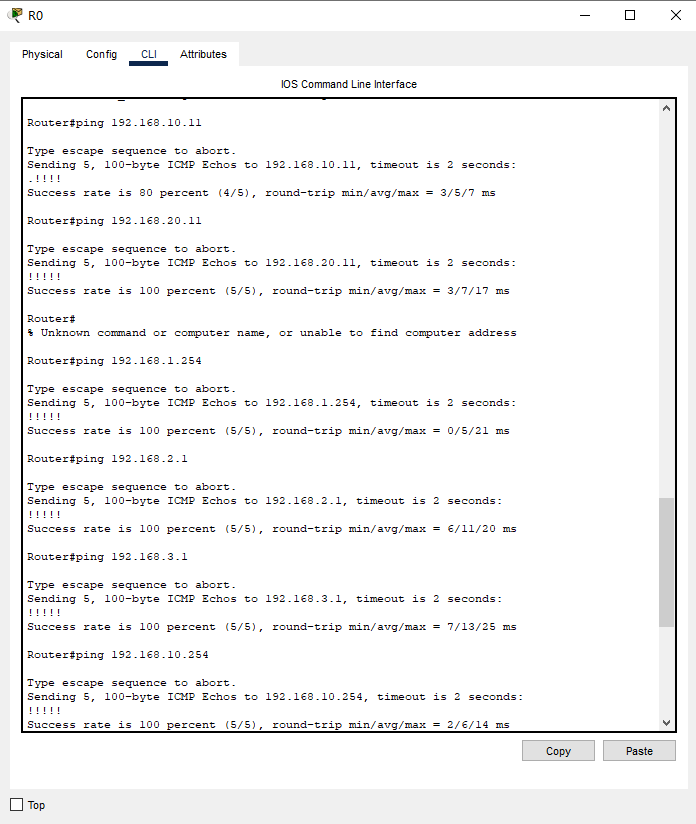


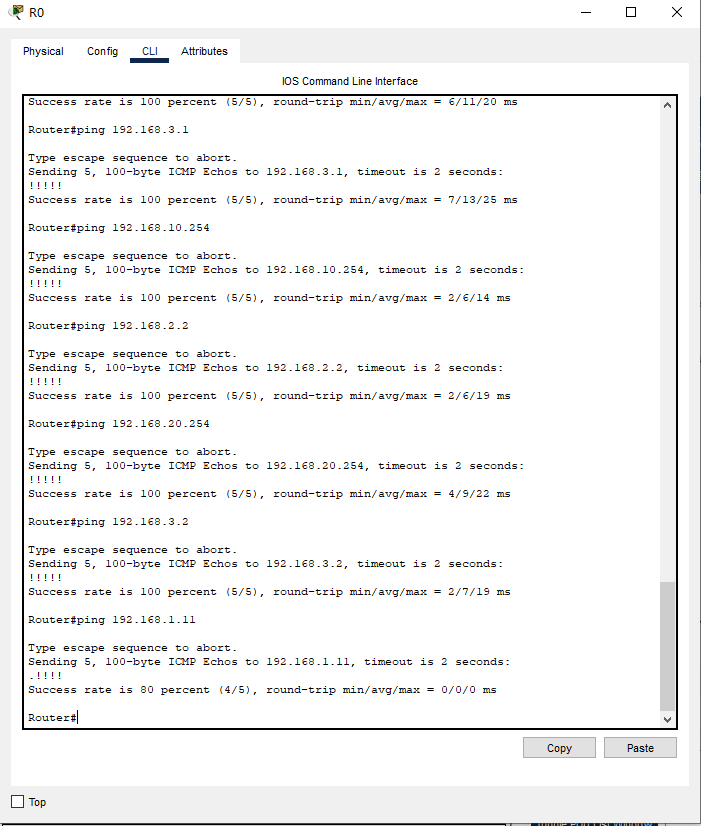




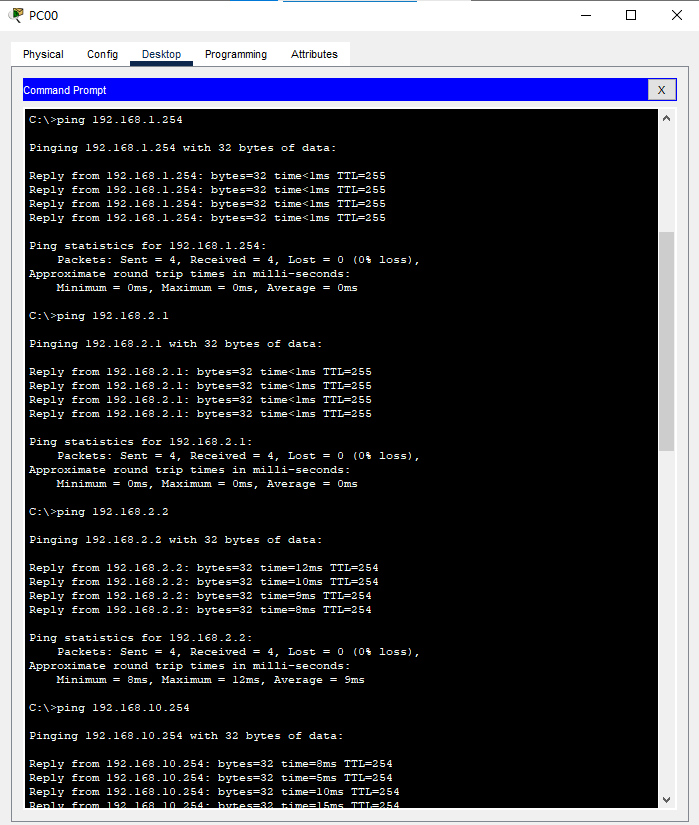
**7.查看路由表**

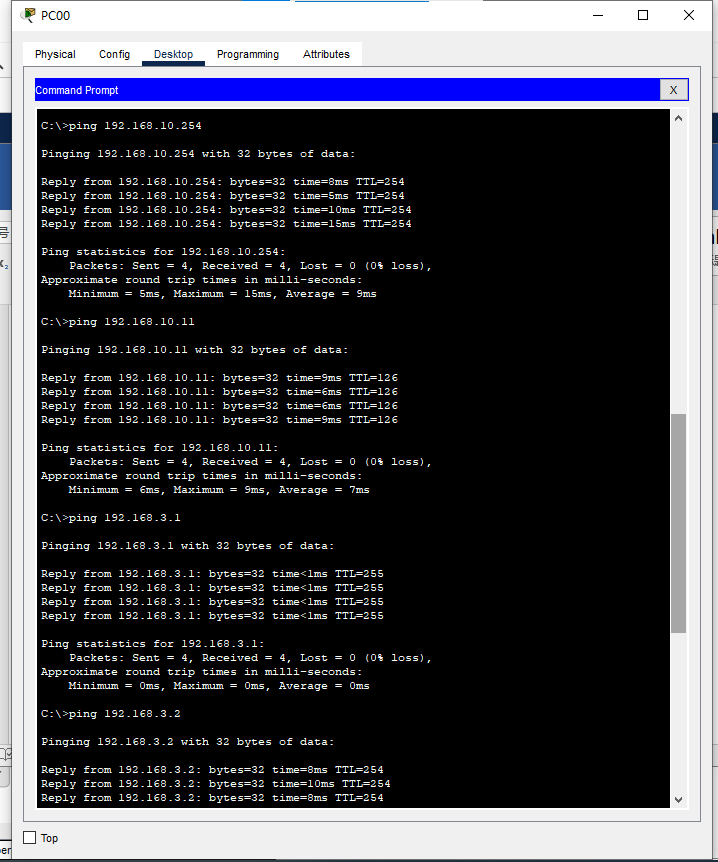
**（1）在路由器上进行ping测试**

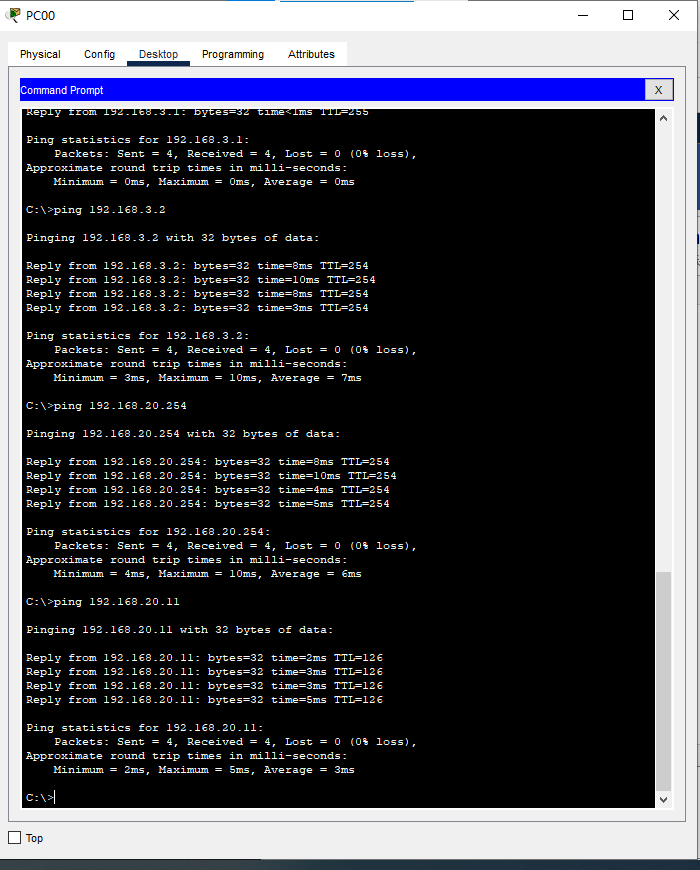




**（2）在PC上进行ping测试**







**实验结果与分析：**

**首先在PC和路由器上分别进行ping通测试，结果都可以ping通，是因为路由器在最开始启动RIP协议的时候，以广播的形式向相邻的路由器发送请求报文，相邻路由器收到报文之后，修改路由器表，然后又重复地向相邻的路由器发送修改报文，到最后，所有路由器都获得了最新的路由信息，所以，ping的时候可以找到对应的目的地址，可以ping通。**

**问题思考和解决方法：**

1. **学到了192.168.1.0和192.168.20.0这两个路由条目**
2. **本次实验中实现了全网全通**

# 实验名称：实验六 OSPF 动态路由实验

**实验目的：**

1、深入掌握动态路由原理；

2、掌握动态路由 OSPF 配置方法；

3、掌握 OSPF 路由工作原理。

**实验仪器：**

Router 路由器（2 台）、主机（2 台）、三层交换机（1 台）

**实验原理：**

OSPF协议是一种ISP，实际部署中分为主干的Area 0和其他Area，不同Area交互信息必须要经过主干区域，若非主干区域没有物理连接到主干区域则需要配置Vlink。

链接主干区域与非主干区域的路由器称为ABR，用于将1类和2类lsa转化为3类LSA发布出去，每个路由器有本自治系统内唯一的RouterID，默认为最大的端口IP地址。维护自己的LSDB，在广播二层网络和NBMA网络中，每一个二层域选举一个DR和BDR用于LSDB的同步。

OSPF报文封装在IP分组中，IP分组的协议字段的值为89。

OSPF采用最短路径算法，拓扑计算与路由计算不独立。路由器通过收集全网链路状态信息，每台路由器独立计算路由，来保证全网路由可达。

OSPF的基本工作过程如下：

（1）路由器周期向自己连接的链路发送Hello报文，Hello报文的作用是：

a. 和邻居路由器建立近邻（adjacent）关系，以互相发送LSA。

b. 确定邻居仍然正常（keep-alive）。

c. 在广播网络或NBMA网络中，选举指定路由器DR，以生成Network-LSA。

（2）建立近邻关系的邻居间交换数据库描述DD报文，标记自己没有的LSA。

（3）通过链路状态请求报文LSR向邻居请求自己没有的LSA。

（4）接收包含LSA的链路状态更新LSU报文，发送链路状态确认LSAck。

（5）如果链路状态改变，发送链路状态更新LSU，变化的LSA在区域内泛洪（flooding）扩散。

**实验内容与步骤：**

1.为路由器添加串口模块，按照拓扑图正确组网

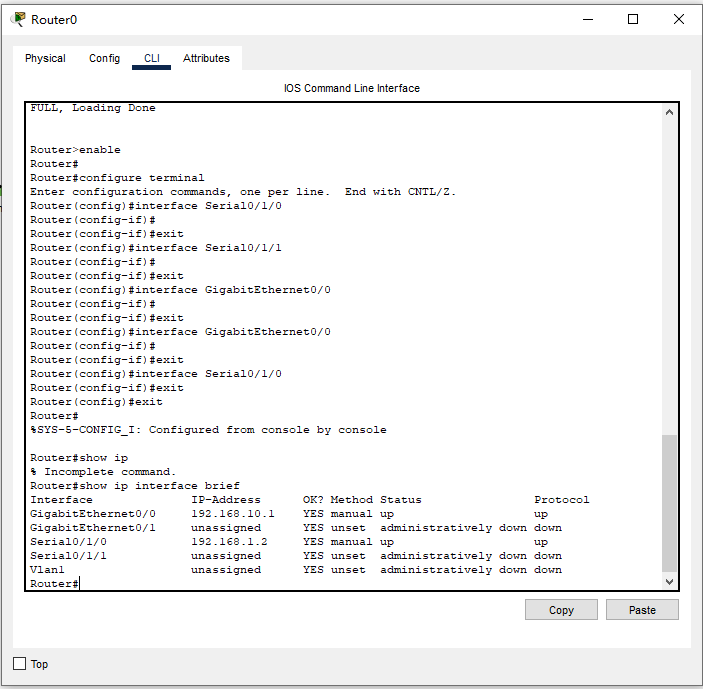
2.配置路由器接口地址

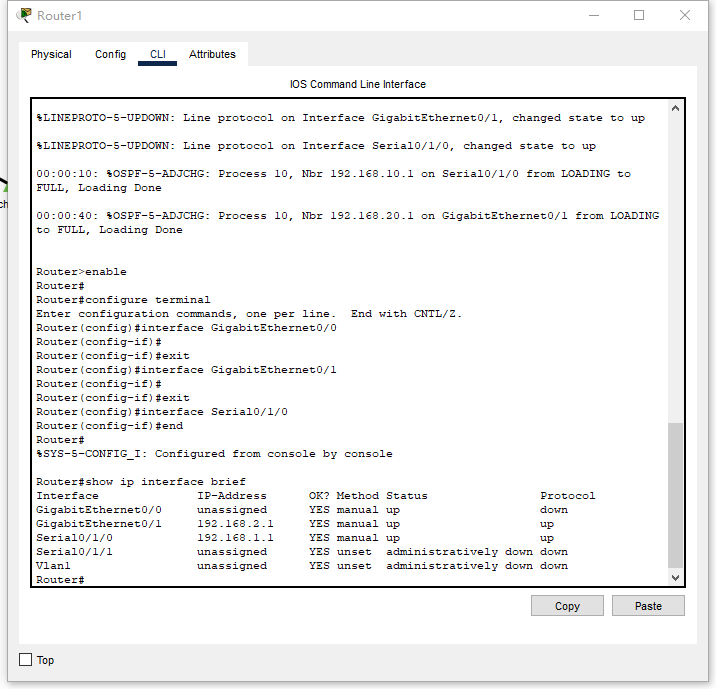
路由器 RouterA 的 Gi0/0 以太网口地址为 192.168.10.1 255.255.255.0；

路由器 RouterA 的串口 Se0/1/0 地址为 192.168.1.2 255.255.255.0；

路由器 RouterB 的配置与 RouterA 类似。配置完成后，

使用 show ip interface brief 命令进行检查。





RouterA> enable

RouterA# configure terminal

RouterA (config)# interface Gi 0/0

RouterA (config-if)# ip address 192.168.10.1 255.255.255.0

RouterA (config-if)# no shutdown

RouterA (config)# interface Se0/1/0

RouterA (config-if)# ip address 192.168.1.2 255.255.255.0

RouterA(config-if)#clock rate 64000

RouterA (config-if)# no shutdown

3.三层交换机配置

Switch(config)#interface f0/1

Switch(config-if)#switchport access vlan 20

Switch(config-if)#exit

Switch(config)#interface f 0/24

Switch(config-if)#switchport access vlan 200

Switch(config-if)#exit

Switch(config)#interface vlan 20

Switch(config-if)#ip address 192.168.2.2 255.255.255.0

Switch(config-if)#no shut

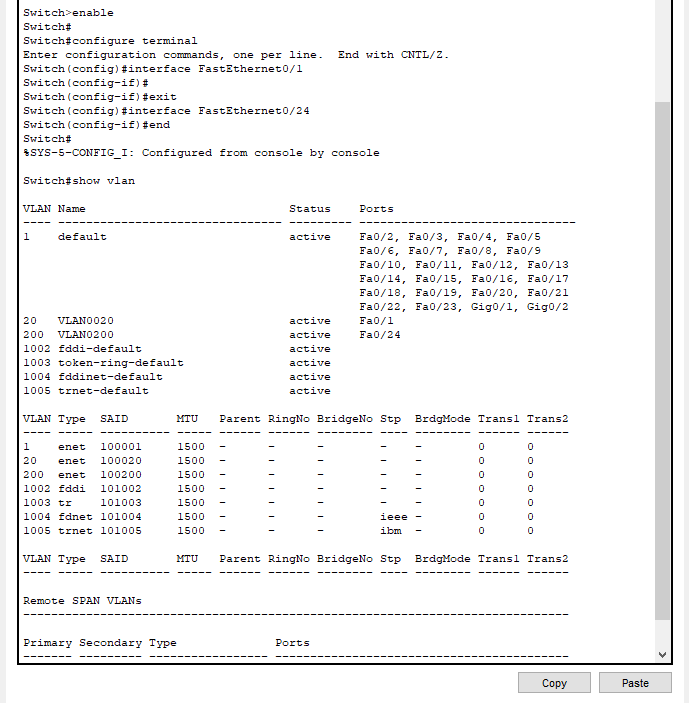
Switch(config-if)#exit

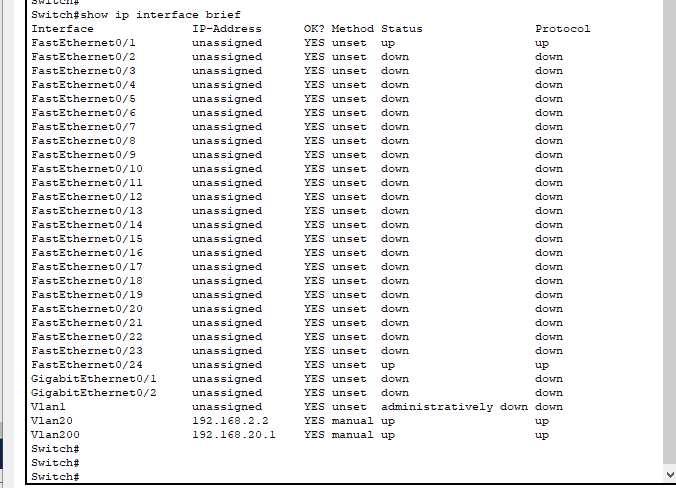
Switch(config)#interface vlan 200

Switch(config-if)#ip address 192.168.20.1 255.255.255.0

Switch(config-if)#no shut

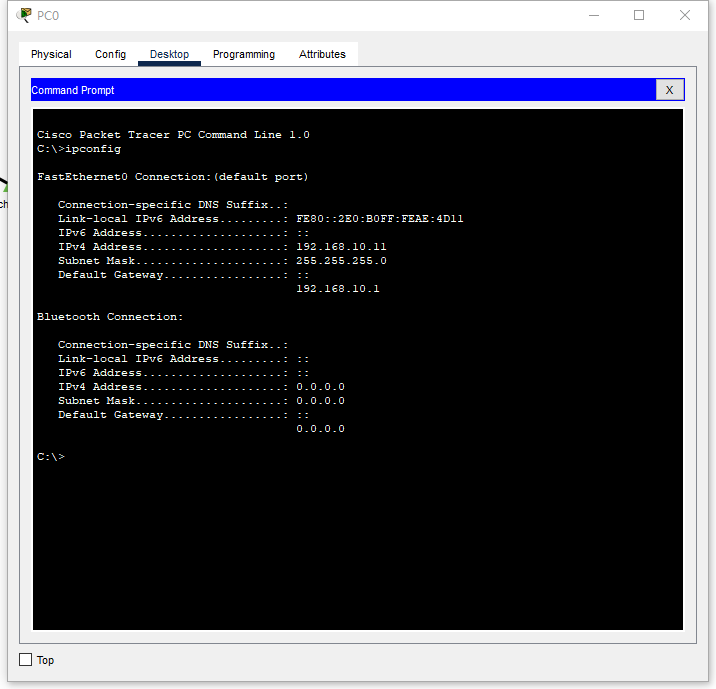
配置完成后，使用命令 show vlan、show ip interface brief



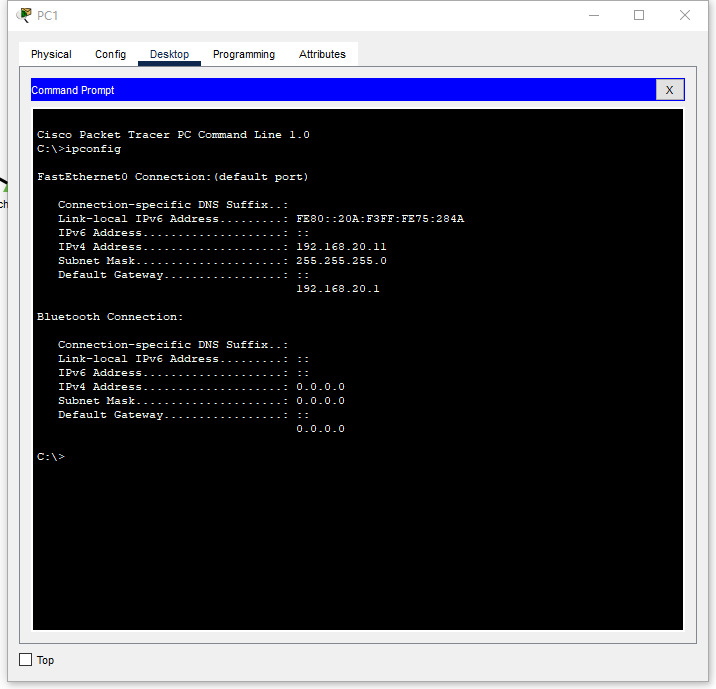


4.PC机ip地址配置

配置 PC0 的 IP 地址为 192.168.10.11/24，网关接口为 192.168.10.1；



配置 PC1 的 IP 地址为 192.168.20.11/24，网关接口为 192.168.20.1；



5.动态路由协议OSPF的设置

路由器 RouterA 上的 2 个网段都在 Area0 区域。

RouterA(config)#router ospf 10

RouterA(config-router)#network 192.168.1.0 0.0.0.255 area 0

RouterA(config-router)#network 192.168.10.0 0.0.0.255 area 0 路由器

RouterB 左侧在 Area0 区域，右侧在 Area1 区域。

Router(config)#router ospf 10

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0

Router(config-router)#network 192.168.2.0 0.0.0.255 area 1

交换机上的 2 个网段都在 Area1 区域。

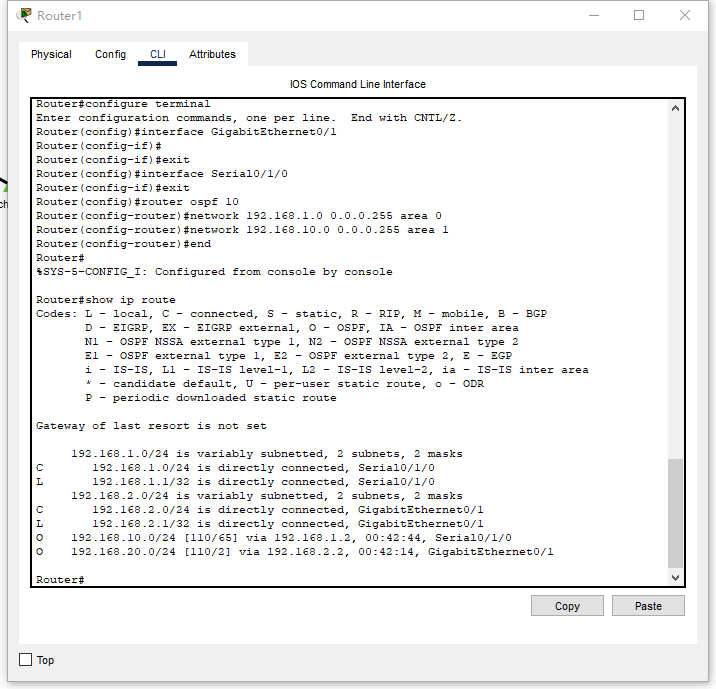
Switch(config)#router ospf 10

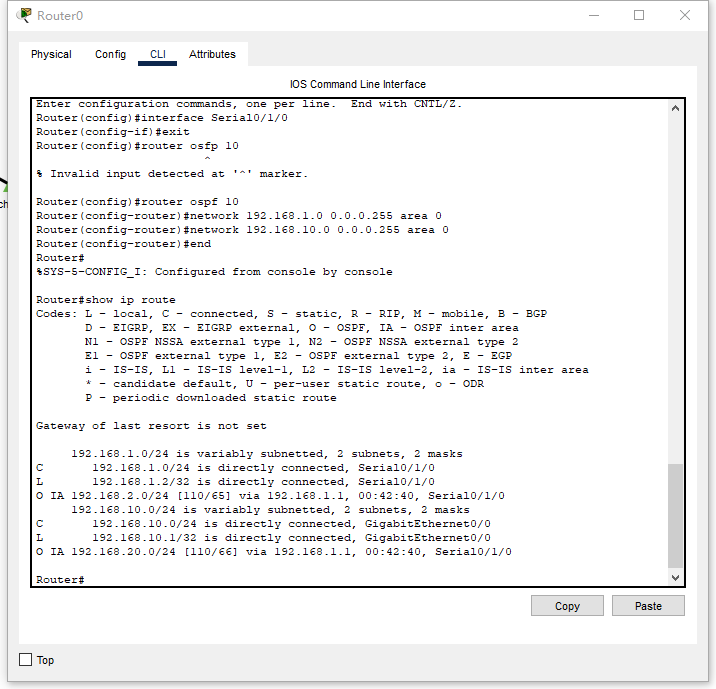
Switch(config-router)#network 192.168.2.0 0.0.0.255 area 1

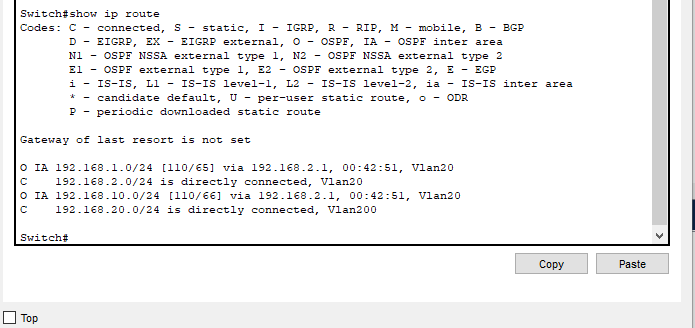
Switch(config-router)#network 192.168.20.0 0.0.0.255 area 1

Switch(config-router)#end

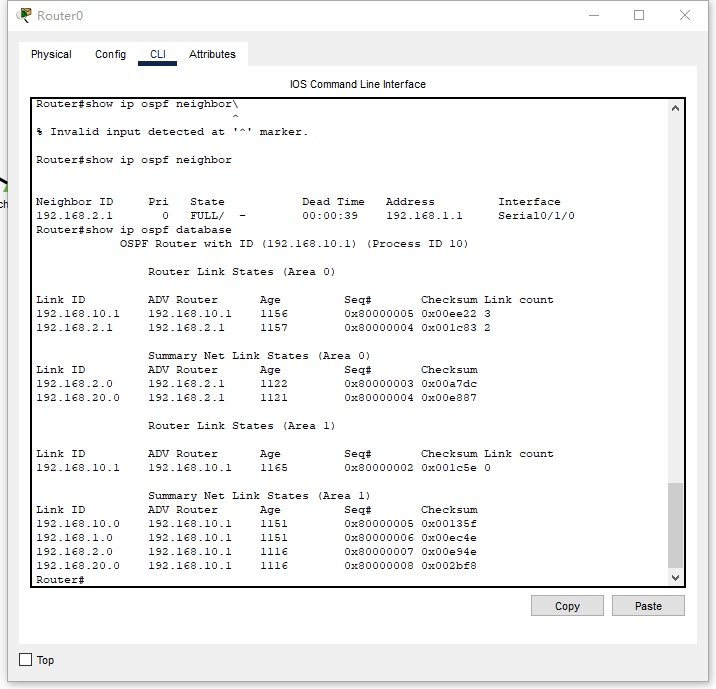
6.查看路由表



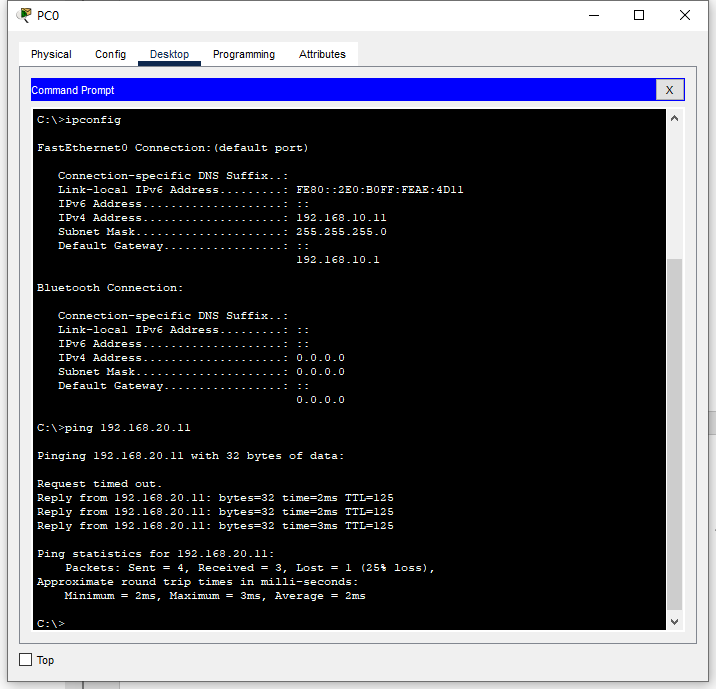




7.查看ospf信息



8.ping测试连通性



**实验结果与分析：**

**在ping通测试中，直接从PC0pingPC1都可以ping通，因为OSPF路由协议可以学习到对应的网段和路由，所有的都可以ping通。**

**问题思考和解决方法：**

**通过本次实验，我学习到了OSPF协议的基本原理和关于OSPF是如何工作的。**

OSPF的基本工作过程如下：

（1）路由器周期向自己连接的链路发送Hello报文。

（2）近邻关系的邻居间交换数据库描述DD报文，标记自己没有的LSA。

（3）通过链路状态请求报文LSR向邻居请求自己没有的LSA。

（4）接收包含LSA的链路状态更新LSU报文，发送链路状态确认LSAck。

（5）如果链路状态改变，发送链路状态更新LSU，变化的LSA在区域内泛洪（flooding）扩散。

OSPF协议可以避免二层重复报文的出现，减少对带宽的占用，和课上讲到了的理论差不多。