**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17 日

**实验名称：**

实验七：最简网络互连

**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

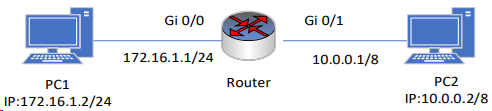
（3）查看路由器系统和配置信息，掌握当前路由器的工作状态

**实验仪器：**

Router路由器1台、主机2台、直连线2条

**实验原理：**

依据实验指导书，熟悉路由器的命令行操作，修改“网络实验”网卡的IP地址，并给路由器接口配置IP地址。本实验的网络拓扑结构如下。



**实验内容与步骤：**

**（1）路由器基本配置**

该步骤主要是熟悉路由器的几个命令：模式切换命令；show命令：show ip route， show interface，show running-config，show ip interface brief等；IP地址配置命令：ip address；Ping命令；No命令。

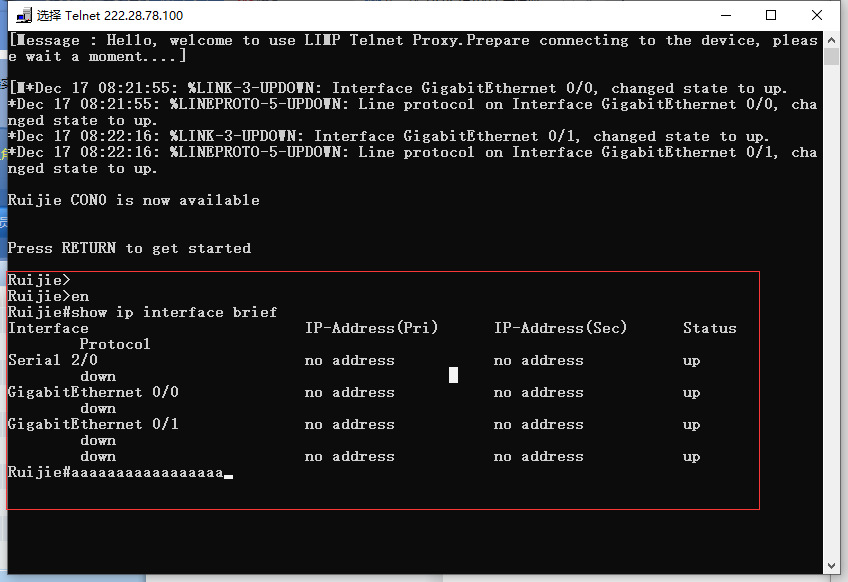
**（2）线缆连接**

将两台PC机与同一台路由器相连。

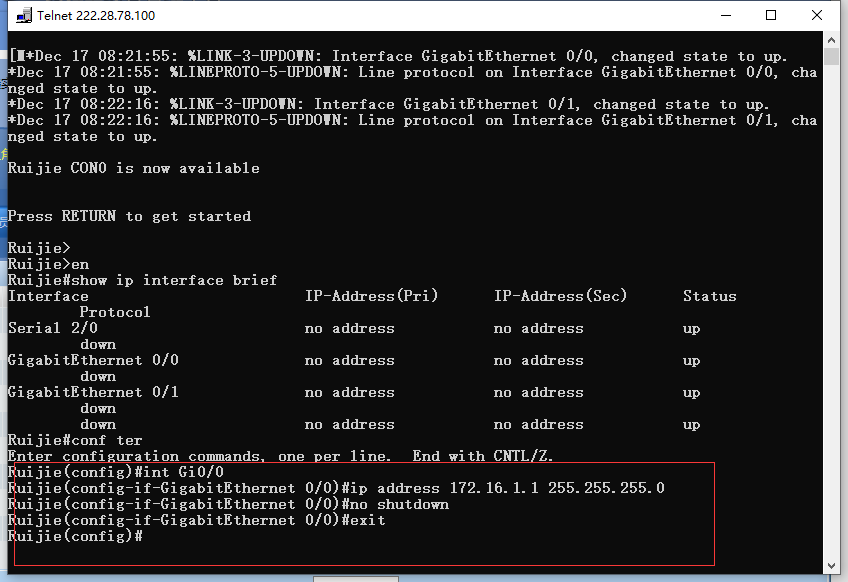
**（3）通过命令行配置路由器IP地址**

这一步骤通过实验室机房电脑中的实验平台进行。

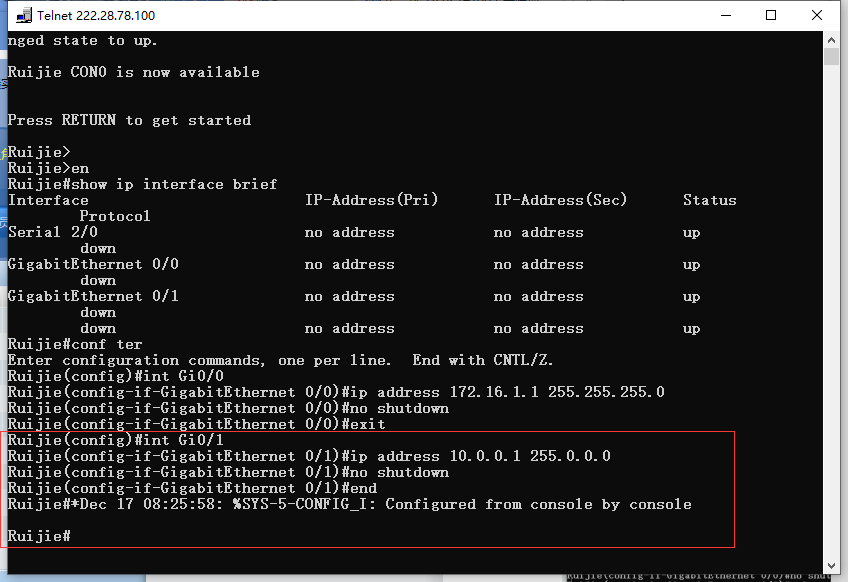
A、查看端口命名及状态



B、配置G0/0端口地址

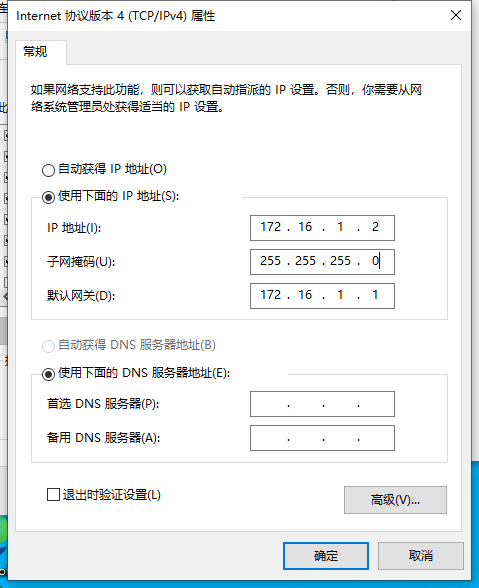


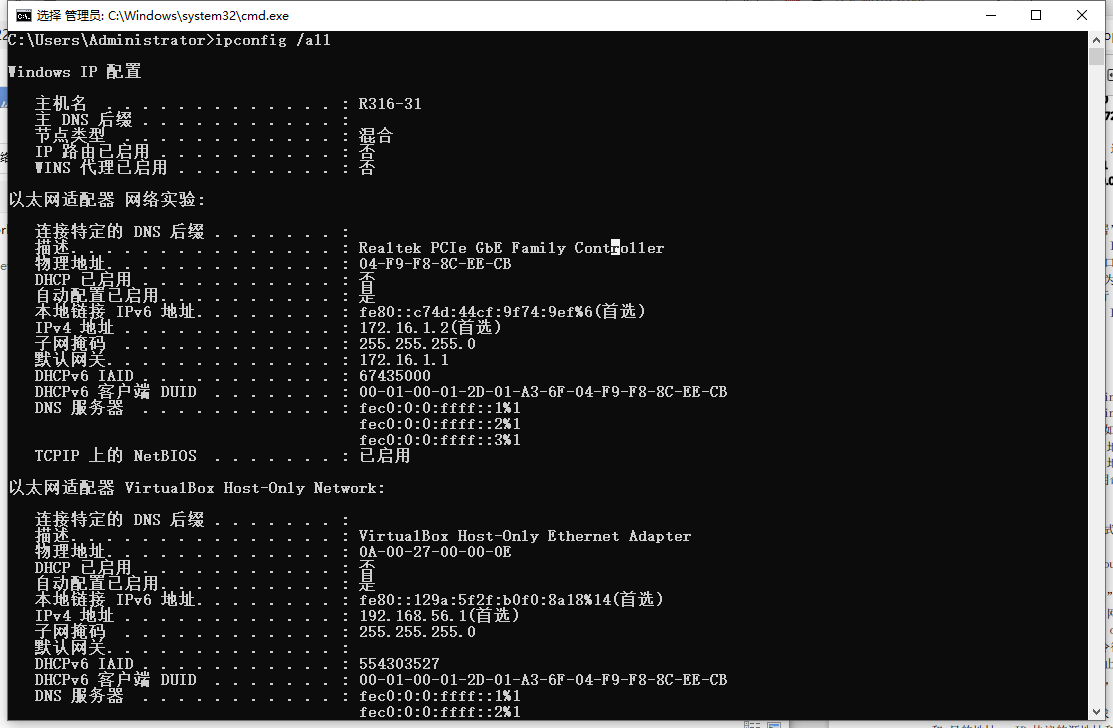
C、配置G0/1端口地址



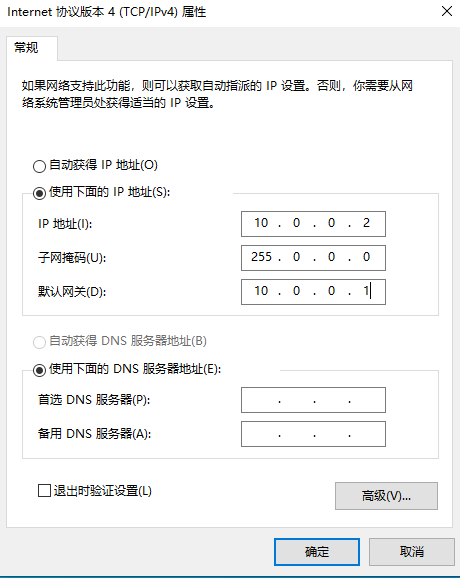
**（4）PC机IP地址配置**

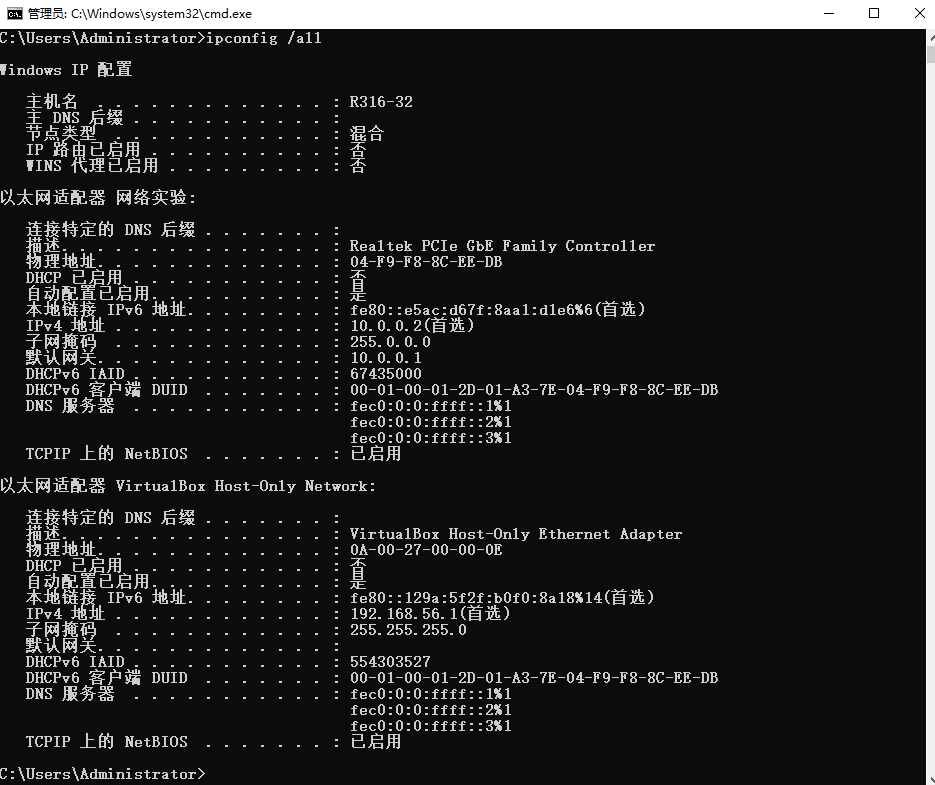
A、PC1





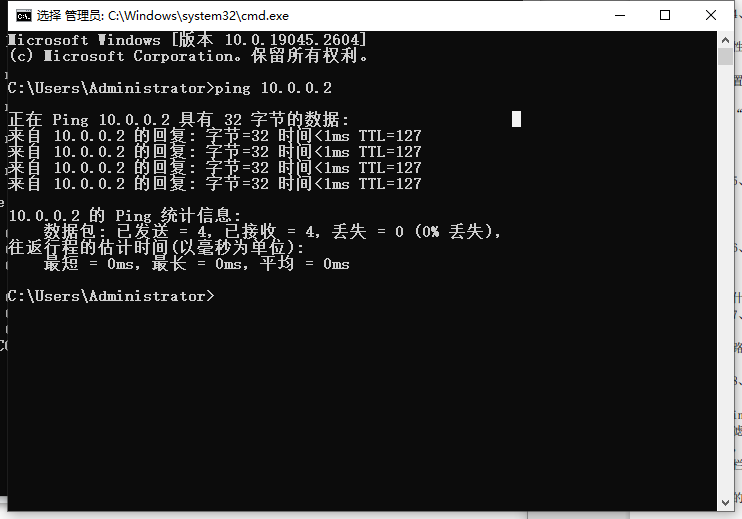
B、PC2



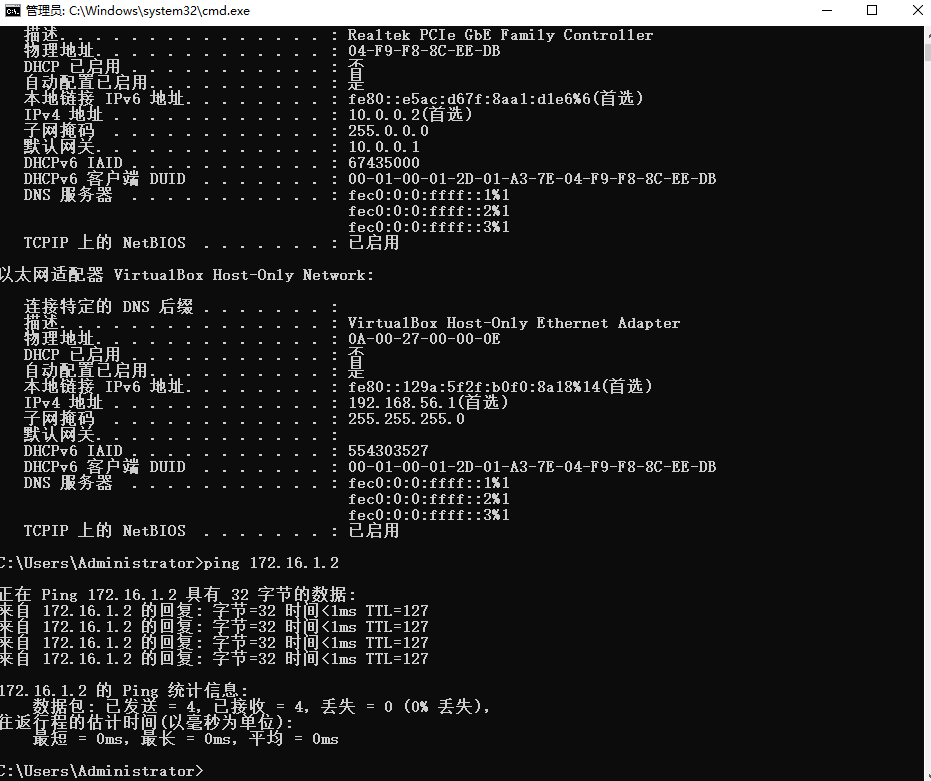


**（5）查看实验结果**

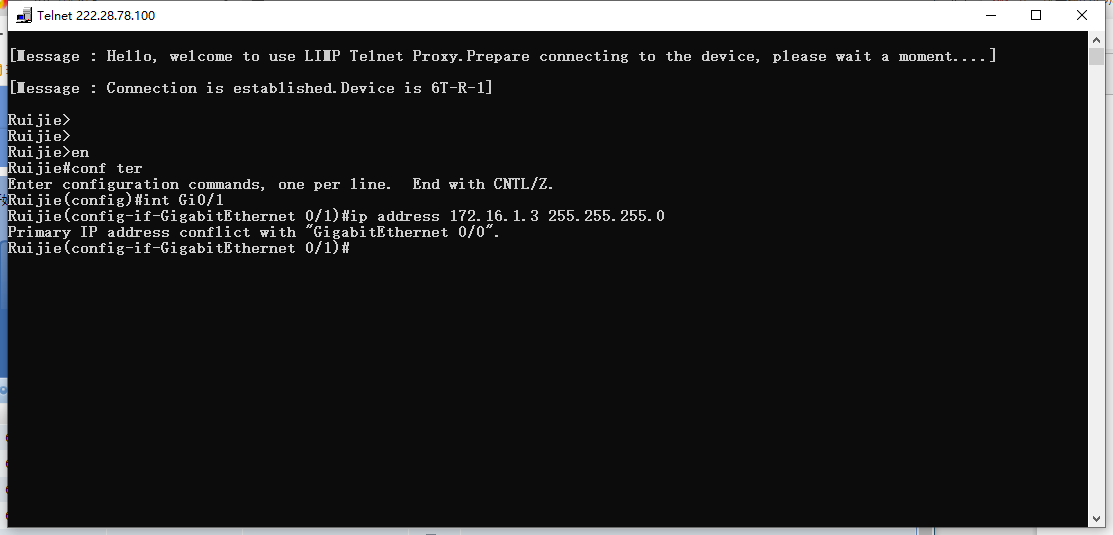
A、PC1 ping PC2，连通



B、PC2 ping PC1，连通



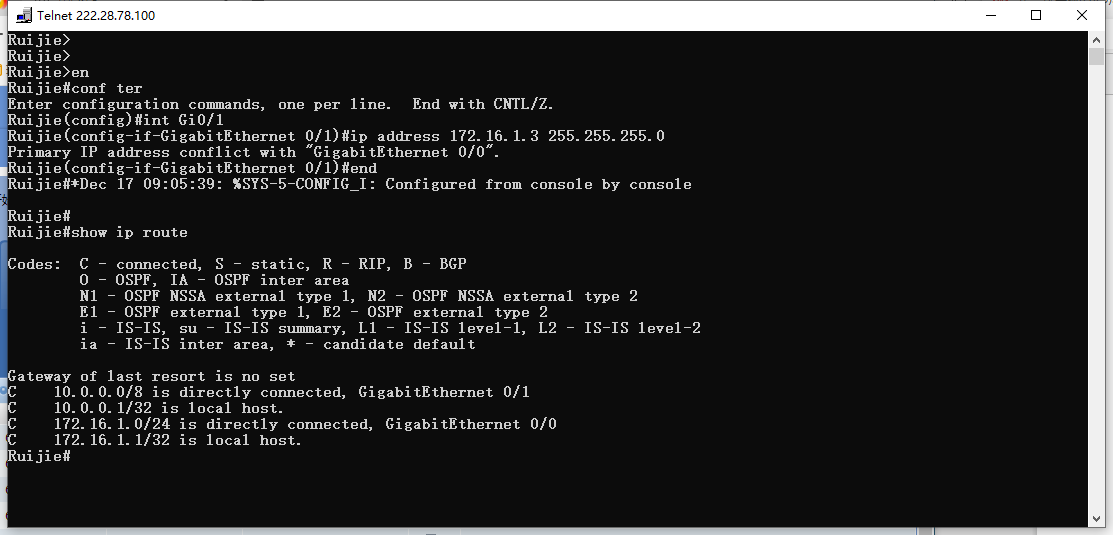
**（6）修改路由器的端口地址并查看配置**



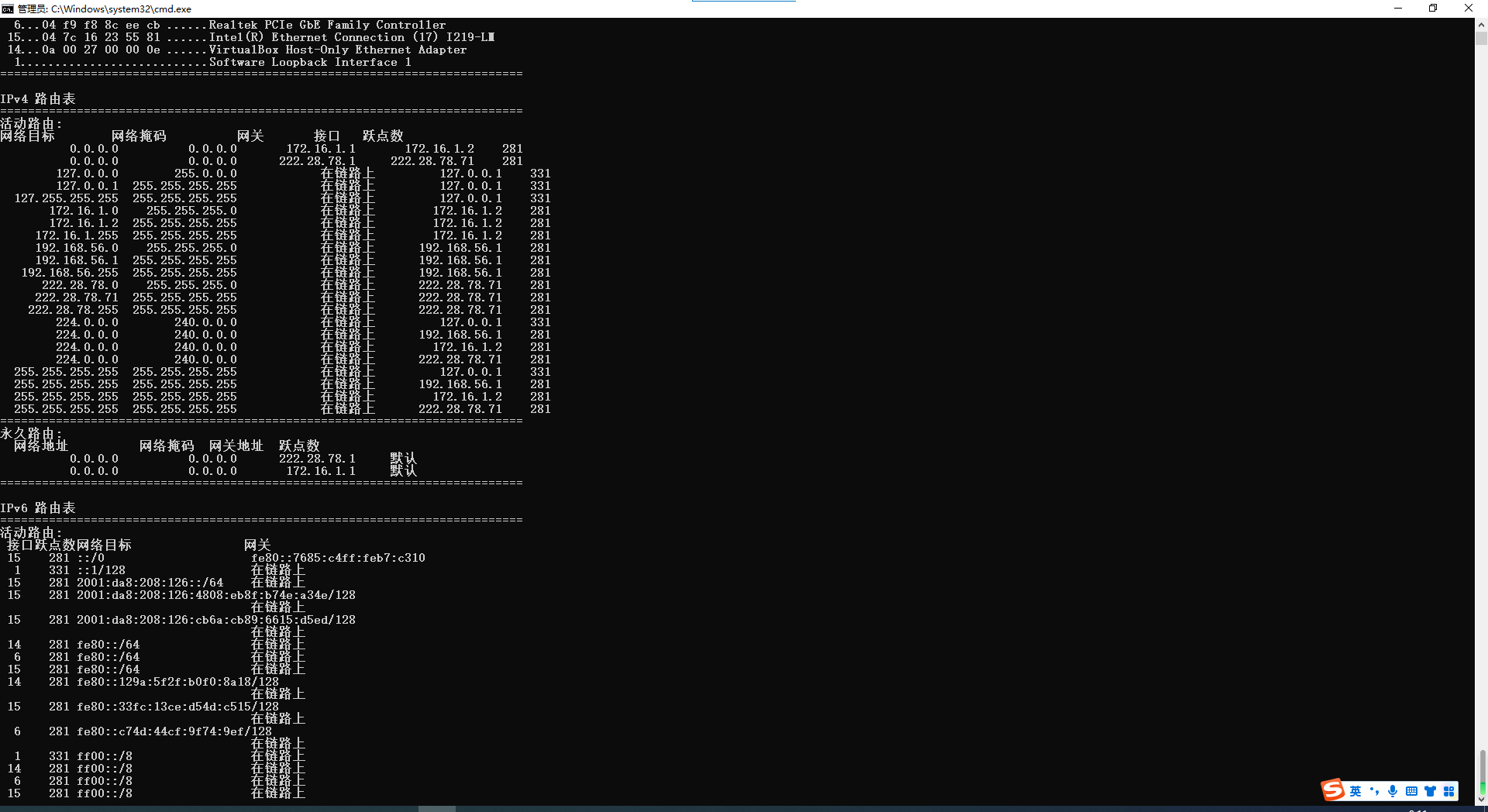
修改失败，这部分的分析将在数据分析环节进行。

**（7）查看路由表**

A、路由器

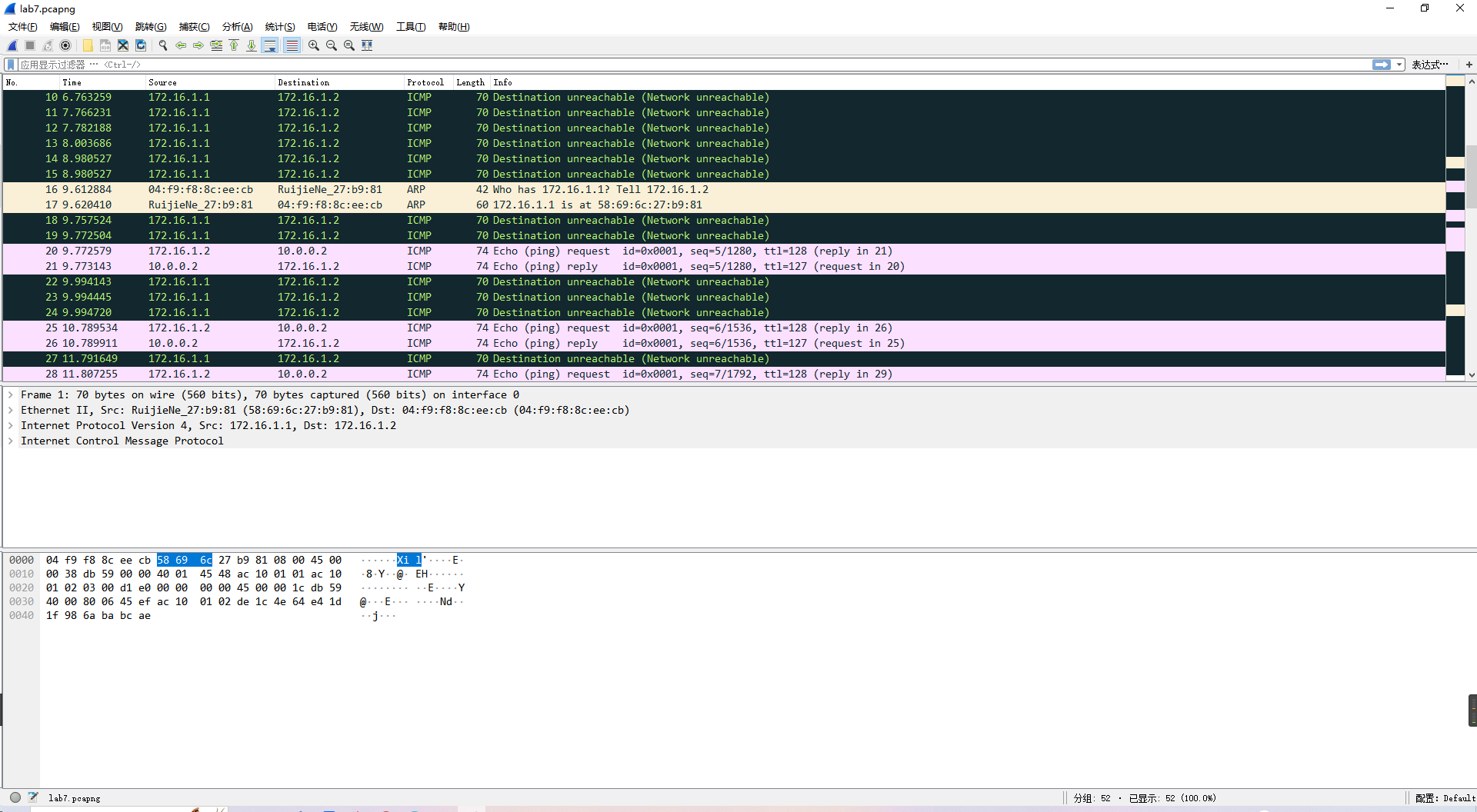


B、PC



**（8）抓包**

PC1与PC2相互ping的同时进行抓包，获得实验数据包，在后续的实验步骤总将进行分析。



**实验数据：**

在这一部分，主要实验数据是所抓取的ARP数据包与ICMP数据包，在后续的实验数据处理环节，会对该数据包进行分析，并完成实验指导书中的表格。

**实验数据处理：**

**（一）实验步骤6修改路由器端口地址失败的原因**

经分析，我认为修改失败的原因有两个：

（1）路由表冲突。路由器使用路由表来确定数据包的下一跳，如果两个端口设置在同一个IP地址域下，路由器将无法正确选择下一跳。这样可能导致数据包在网络中迷失，无法到达其目的地。

（2）网络隔离受影响。不同的网络段用于隔离不同的逻辑网络，以提高网络安全性和性能。如果两个端口设置在同一个IP地址域下，就会破坏这种隔离，可能导致未经授权的访问和潜在的安全问题。

**（二）实验步骤8数据包分析**

针对抓取的报文，选择一组arp请求和应答报文以及icmp请求和应答报文进行分析，填写下面的表格。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段值 | ARP请求报文 | ARP应答报文 | ICMP请求报文 | ICMP应答报文 |
| 链路层Destination | RuijieNe\_27:b9:81 (58:69:6c:27:b9:81) | 04:f9:f8:8c:ee:cb (04:f9:f8:8c:ee:cb) | RuijieNe\_27:b9:81 (58:69:6c:27:b9:81) | 04:f9:f8:8c:ee:cb (04:f9:f8:8c:ee:cb) |
| 链路层  Source | 04:f9:f8:8c:ee:cb (04:f9:f8:8c:ee:cb) | RuijieNe\_27:b9:81 (58:69:6c:27:b9:81) | 04:f9:f8:8c:ee:cb (04:f9:f8:8c:ee:cb) | RuijieNe\_27:b9:81 (58:69:6c:27:b9:81) |
| 网络层Sender MAC Address | 04:f9:f8:8c:ee:cb | 58:69:6c:27:b9:81 | 04:f9:f8:8c:ee:cb | 58:69:6c:27:b9:81 |
| 网络层Sender IP Address | 172.16.1.2 | 172.16.1.1 | 172.16.1.2 | 10.0.0.2 |
| 网络层Target MAC Address | 58:69:6c:27:b9:81 | 04:f9:f8:8c:ee:cb | 58:69:6c:27:b9:81 | 04:f9:f8:8c:ee:cb |
| 网络层Target IP Address | 172.16.1.1 | 172.16.1.2 | 10.0.0.2 | 172.16.1.2 |

**实验结果与分析：**

在这一环节，将针对实验指导书中的思考问题进行回答。

**（1）在第五步中，ping命令执行是否成功，为什么？**

ping命令执行成功。在实验涉及的连接和配置模式下，正确形成路由表，完成相应的转发功能。

**（2）在第六步中，路由器配置是否成功，有何提示信息？**

提示信息：端口地址冲突

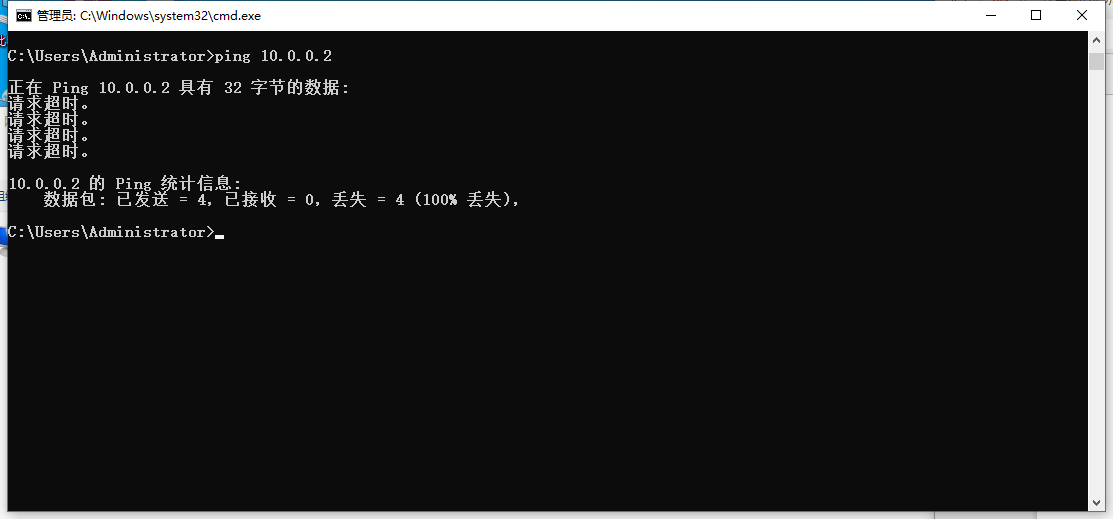
经分析，我认为修改失败的原因有两个：

A、路由表冲突。路由器使用路由表来确定数据包的下一跳，如果两个端口设置在同一个IP地址域下，路由器将无法正确选择下一跳。这样可能导致数据包在网络中迷失，无法到达其目的地。

B、网络隔离受影响。不同的网络段用于隔离不同的逻辑网络，以提高网络安全性和性能。如果两个端口设置在同一个IP地址域下，就会破坏这种隔离，可能导致未经授权的访问和潜在的安全问题。

**（3）如果不配置PC机的网关，执行ping命令时可以观察到什么现象？为什么？**

当PC1 ping PC2时显示请求超时



如果没有配置默认网关，操作系统可能不知道如何将数据包发送到目标主机。默认网关是当主机要访问不在本地子网的目标时，数据包应该发送到的路由器的IP地址。如果没有默认网关，主机无法找到到达目标主机的路由，因此ping请求会超时。

**实验名称：**

实验八：静态路由实验

**实验目的：**

（1）深入掌握IP协议和路由原理

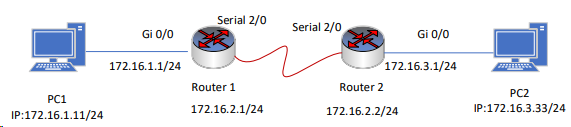
（2）掌握静态路由原理和RIP路由协议原理

**实验仪器：**

Router路由器2台、主机2台、直连线2条

**实验原理：**

静态路由指的是由用户或者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的时候，需要手动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。有关静态路由的部分知识参考了文章[静态路由（也许是目前最全的）-CSDN博客](https://blog.csdn.net/qq_34238567/article/details/119810775)进行学习。本次实验的拓扑结构如下所示。



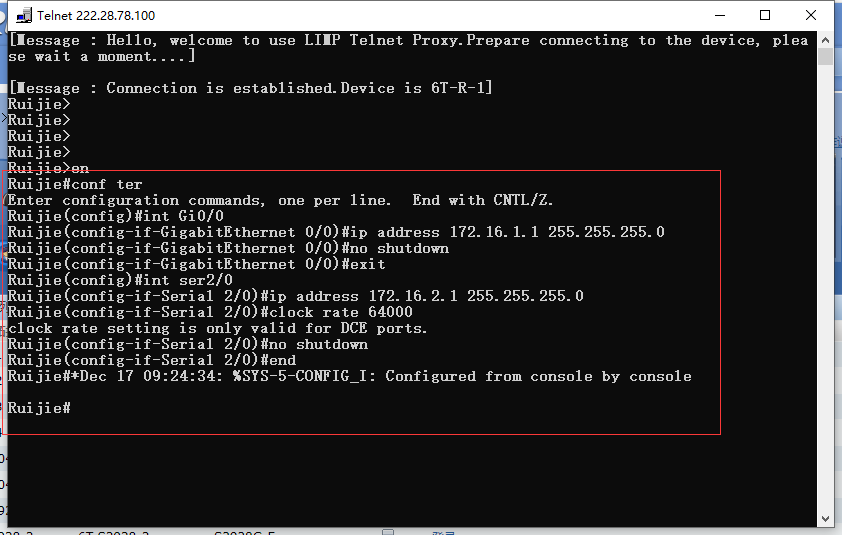
**实验内容与步骤：**

**（1）线缆连接**

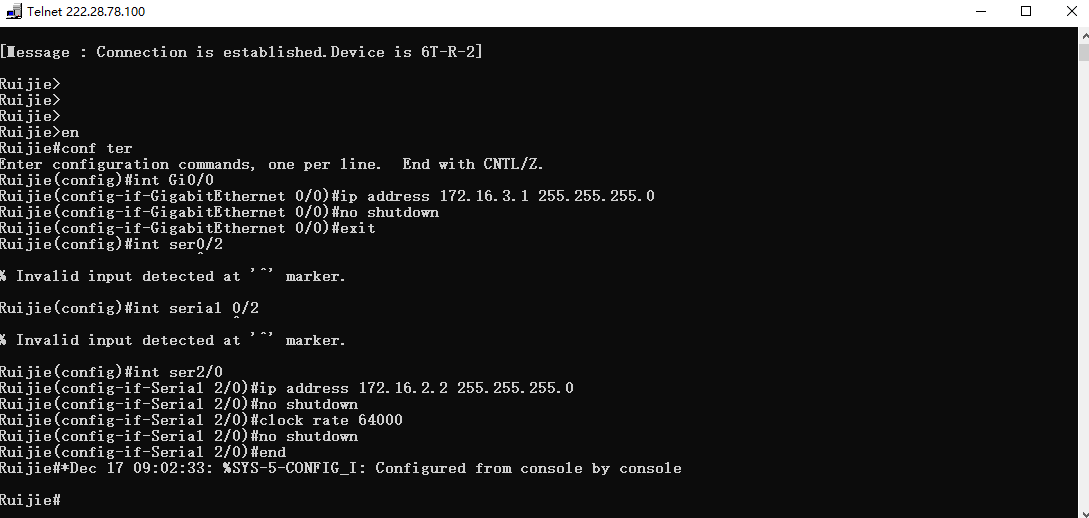
由于路由器与路由器的串口线已经接好，因此将两台PC分别与两个路由器相连。

**（2）配置路由器接口地址**

A、配置R1

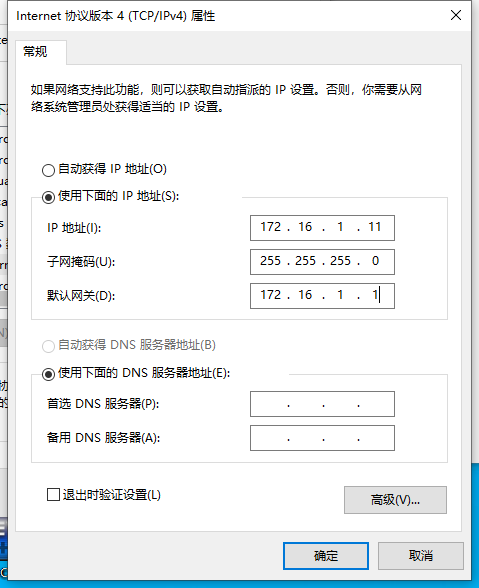


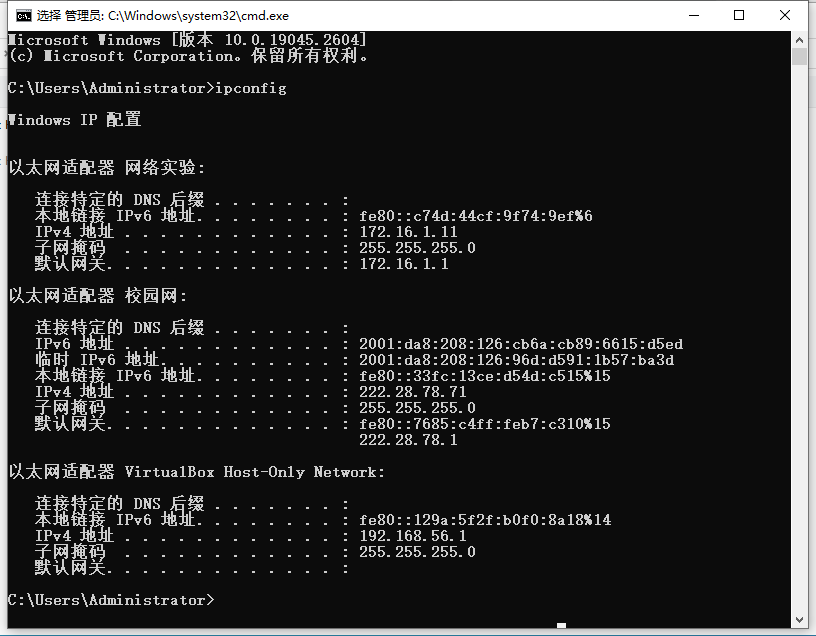
B、配置R2



**（3）配置PC机IP地址**

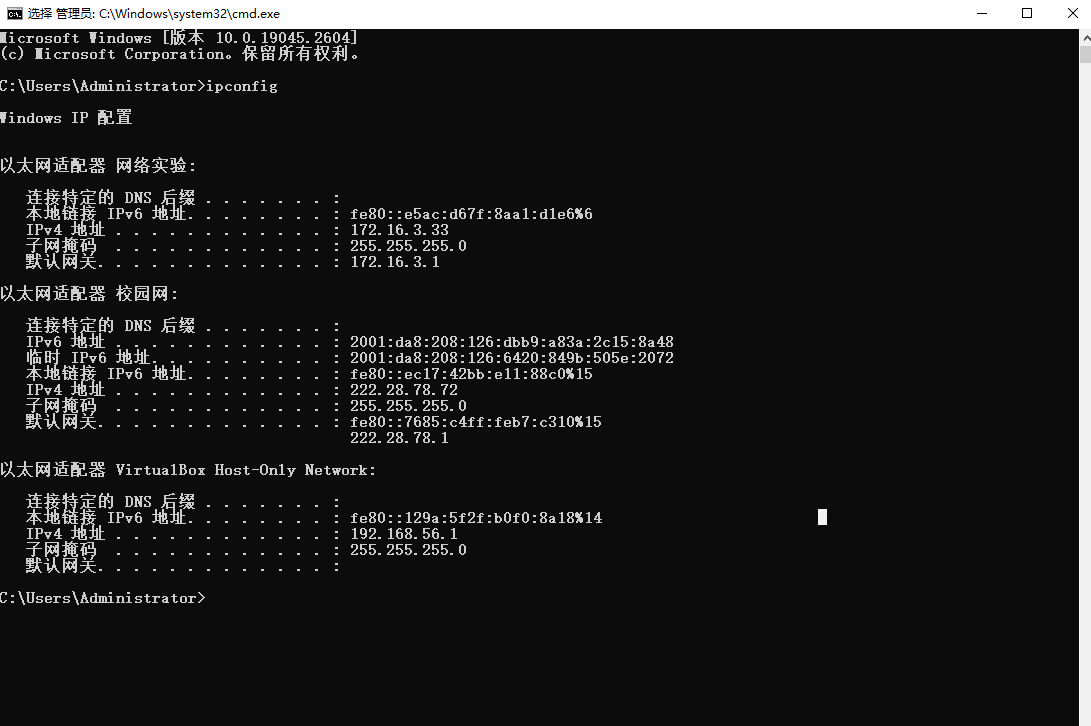
A、PC1





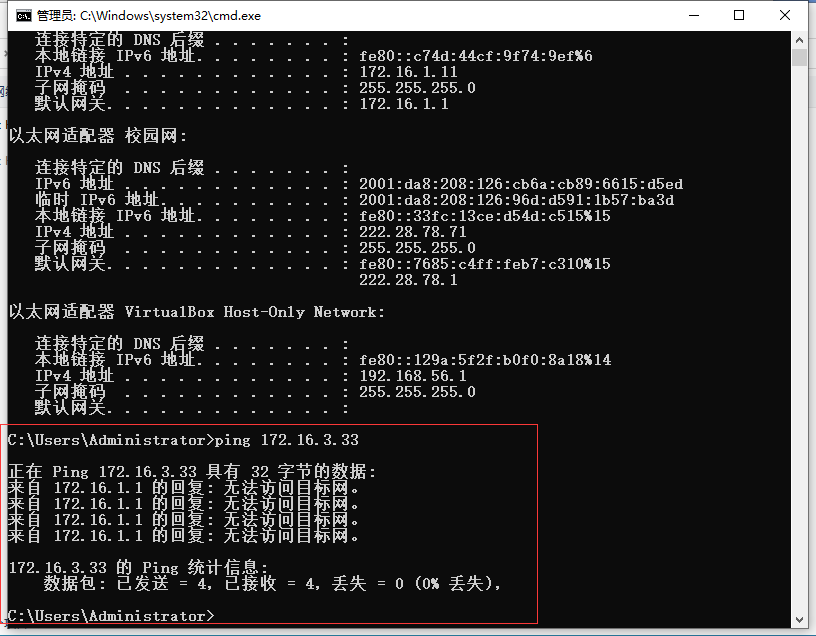
B、PC2



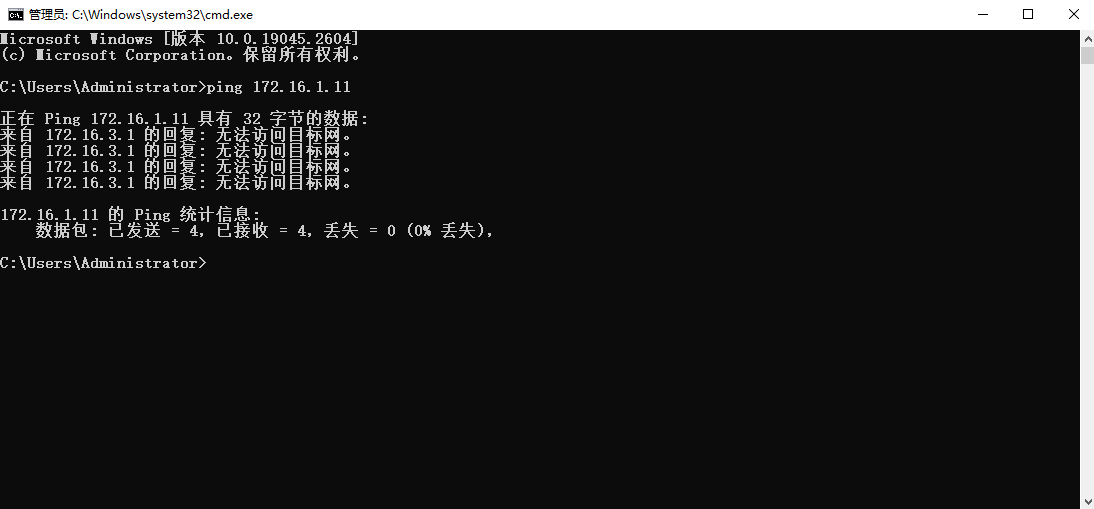


**（4）查看实验结果**

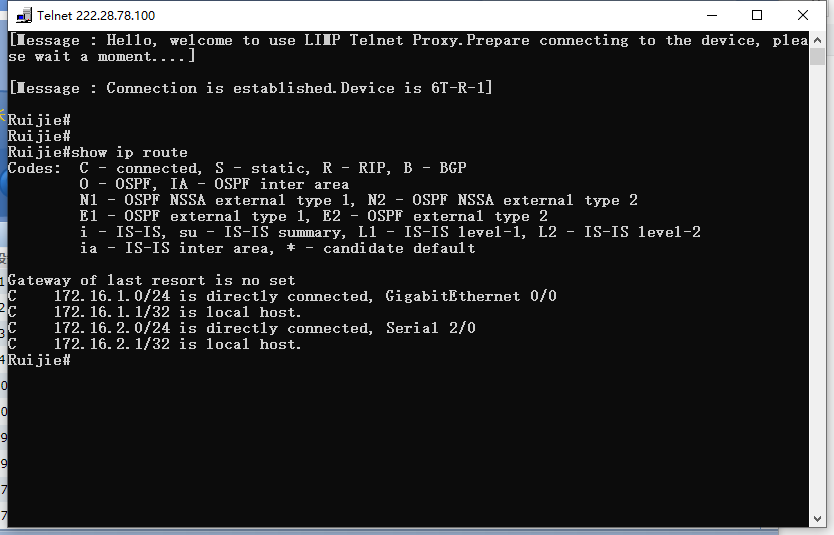
A、PC1 ping PC2，不通



B、PC2 ping PC1，不通

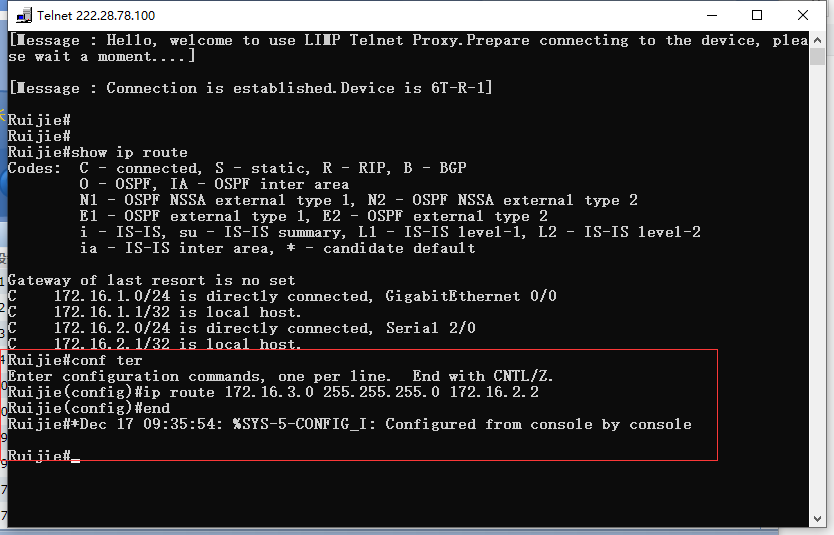


C、查看路由表

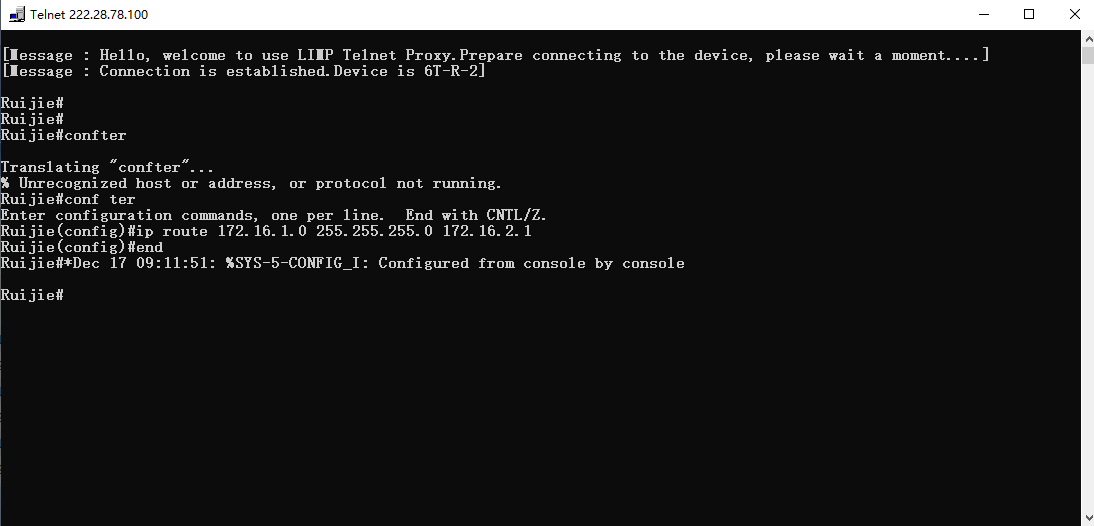


**（5）写入静态路由表**

A、配置R1

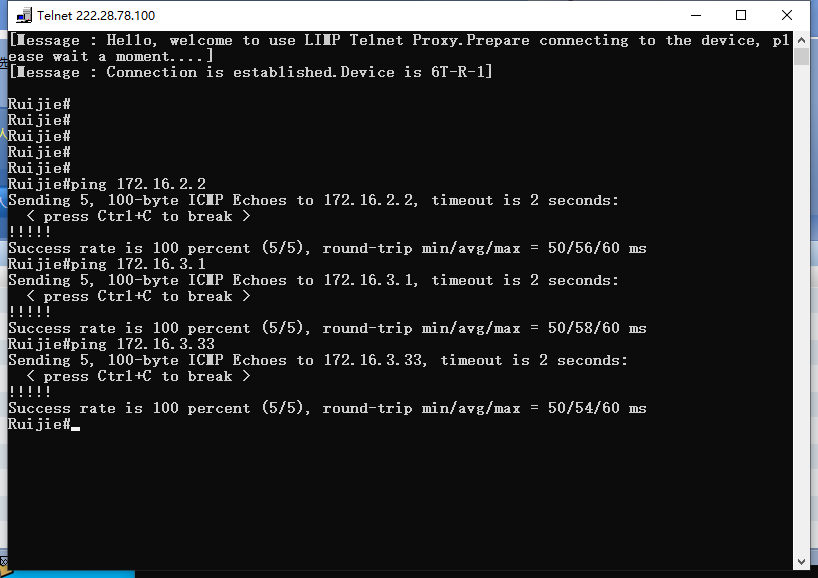


B、配置R2

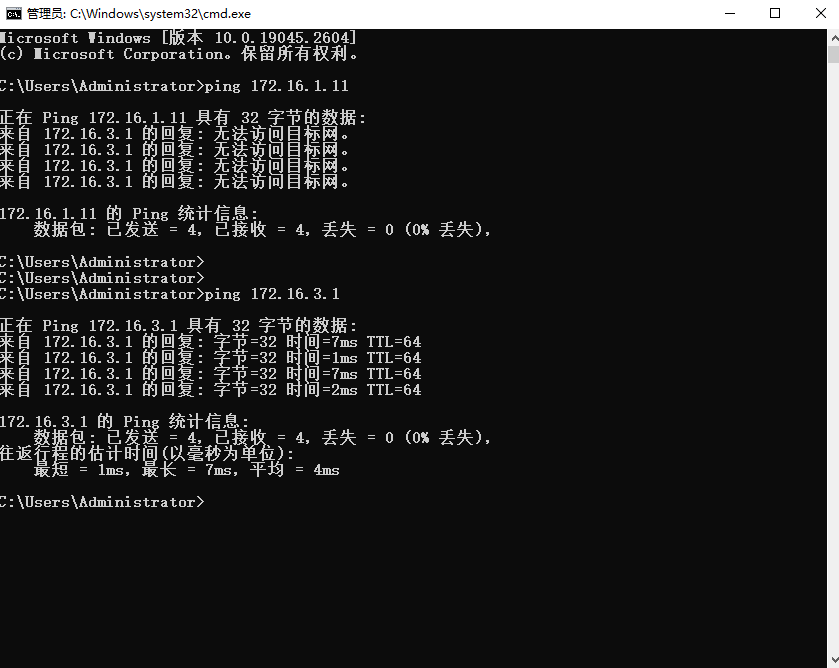


**（6）分段进行测试**

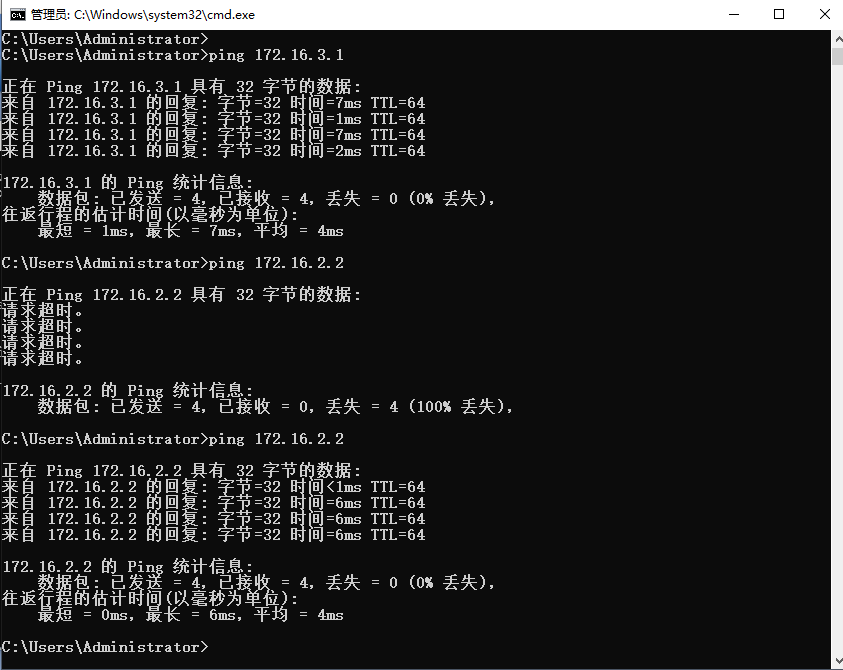
A、路由器ping各段，均能连通



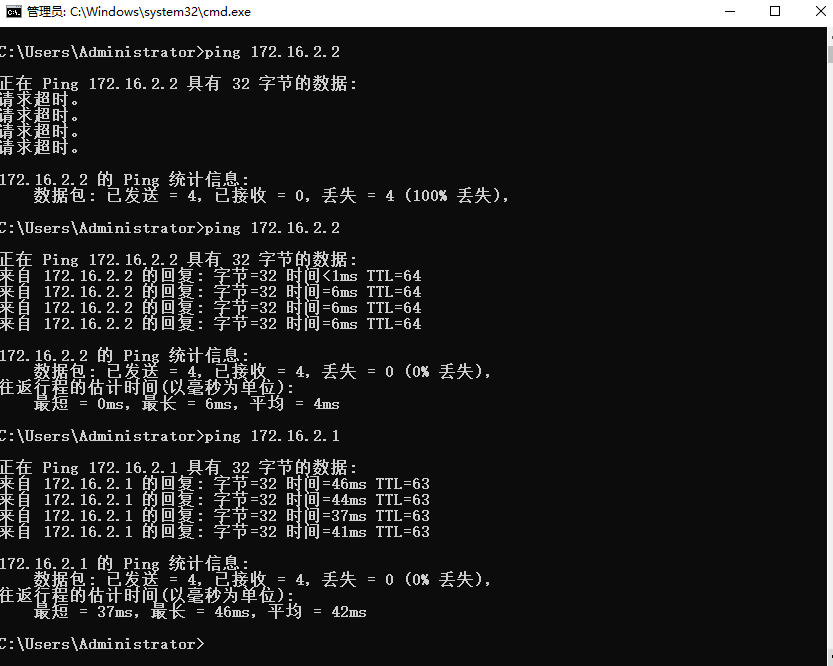
B、PC2 ping自己网关



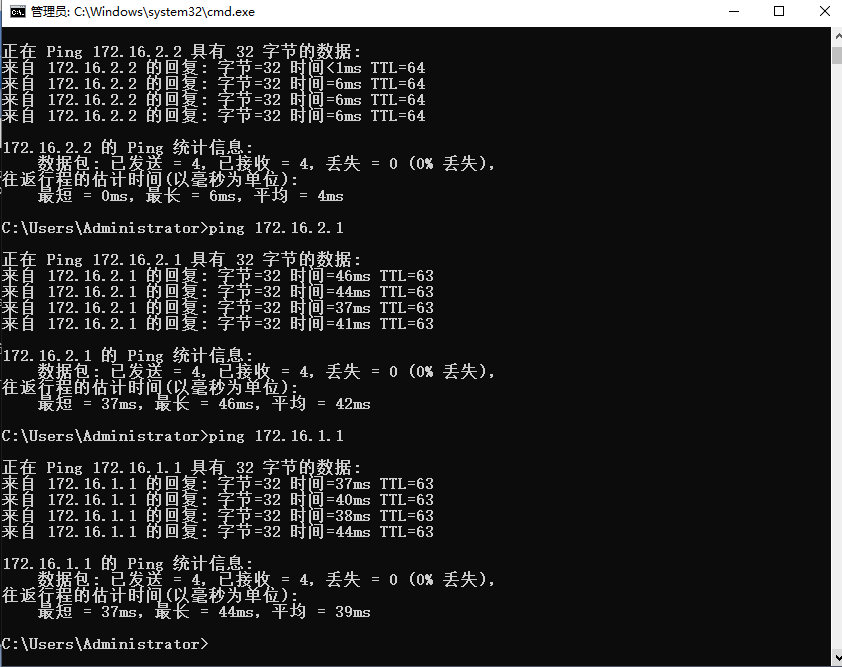
C、Router2串口



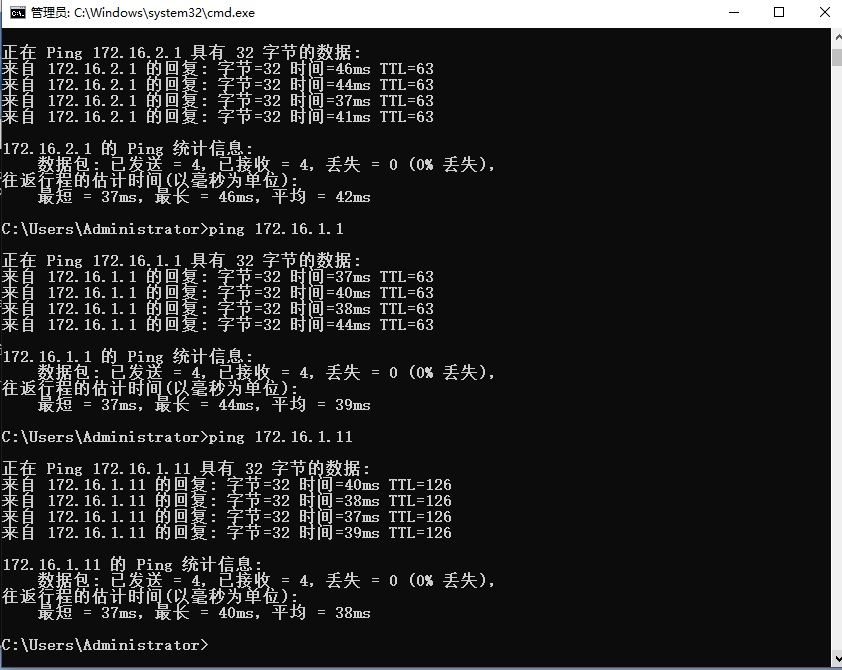
D、Router1串口



E、PC1网关

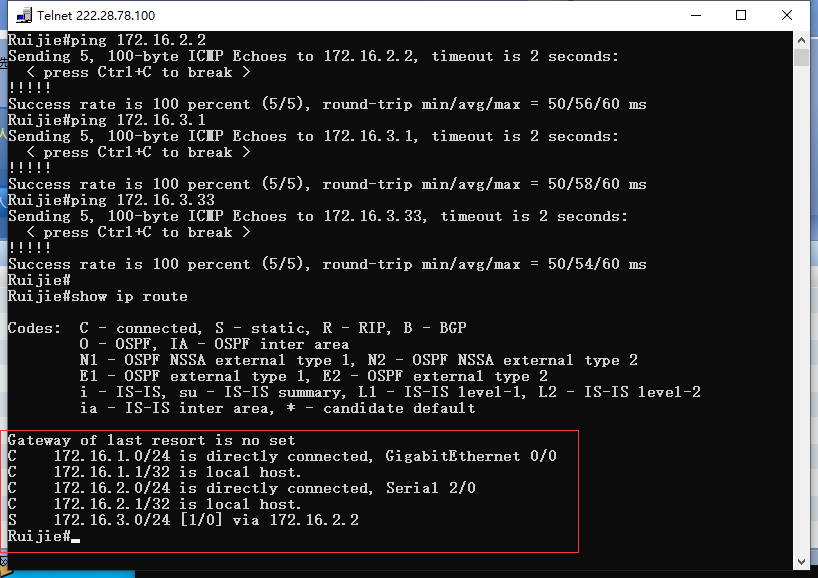


F、PC1

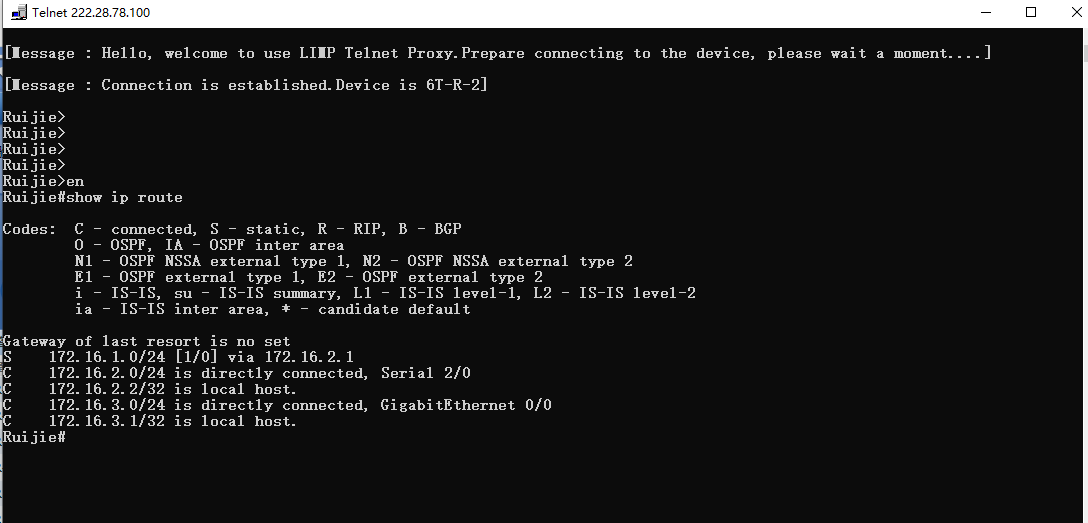


**（7）查看路由表**

A、R1路由表



B、R2路由表



**实验数据：**

本次实验偏向于验证性实验，没有涉及实验数据，相关实验记录均以图片的形式展示于实验步骤中。

**实验数据处理：**

由于本次实验未涉及到实验数据，因此无需进行实验数据处理。

**实验结果与分析：**

在这个环节，针对实验指导书中的部分思考问题进行回答。

**（1）步骤4中，PC1 ping PC2能否成功？为什么？路由表中有几个条目？**

不通，此时路由表中有4（2）个条目，均为直连。未配置路由信息，路由器不知道应该将数据包如何转发。

**（2）步骤7中，路由表中有几个条目？与步骤四中的路由表有什么不同？**

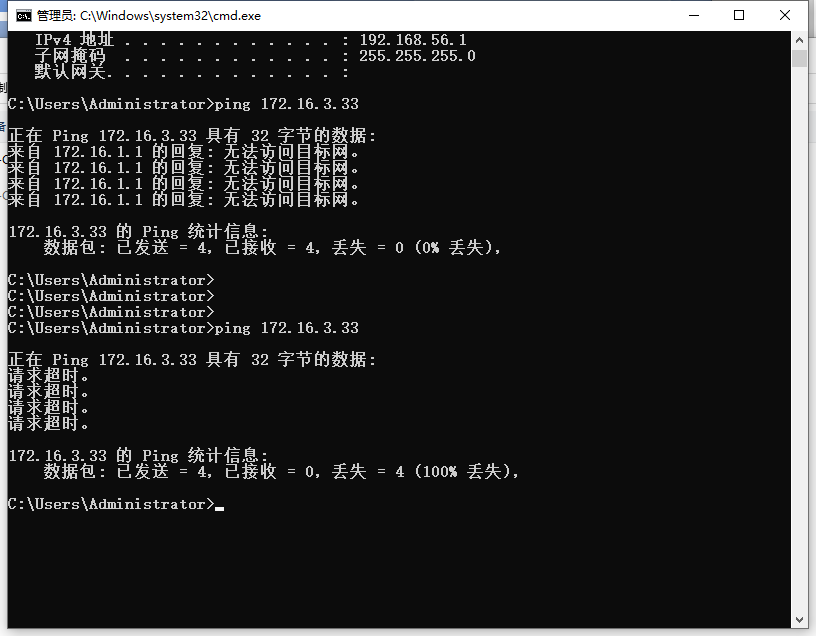
在步骤4的基础上增加了S即静态路由配置信息，通过该条目，路由器知道了：目的网络是172.16.3.0/24，则下一跳为172.16.2.2，成功进入另一个自治系统。

**（3）静态路由实验，拓扑结构为：PC1━R1━R2━PC2。静态路由具有方向性，如果一个方向上配置，另一个方向上不配置，会产生不同的实验结果。保留路由器R1上的静态路由，删除路由器R2上的静态路由。执行PC1pingPC2，再执行 PC2pingPC1，能否连通？记录实验结果，截图显示。**

A、删除配置



B、PC1 ping PC2超时

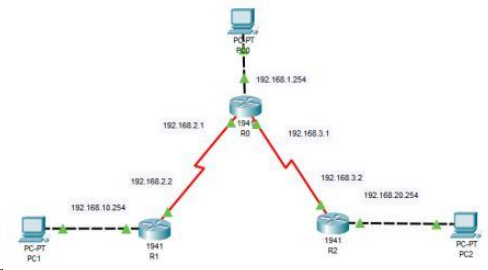


C、PC2 ping PC1不可达



结果分析：修改配置之后，R1中留有路由信息，R2无路由信息，也就是说，R1知道目的网络是172.16.3.0/24的下一跳是172.16.2.2，但R2不知道目的网络是172.16.1.0/24的下一跳是172.16.2.1。所以，当PC1 ping PC2时，请求报文能到达PC2，但是响应报文无法到达PC1，显示超时；当PC2 ping PC1时，请求报文无法到达PC1，显示不可达。

**（4）下图中，路由器的每个接口都给了IP地址，使用静态路由连接每个网段，请给出每个路由器上静态路由的配置命令，采用下一跳地址的方式，保证全网全通。**



结合课上边老师的讲解，应进行8个条目的配置：

A、R0

iP route 192.168.10.0 255.255.255.0 192.168.2.2 10网段

ip route 192.168.20.0 255.255.255.0 192.168.3.2 20网段

B、R1

ip route 192.168.1.0 255.255.255.0 192.168.2.1 1网段

ip route 192.168.3.0 255.255.255.0 192.168.2.1 3网段

ip route 192.168.20.0 255.255.255.0 192.168.2.1 20网段

C、R2

ip route 192.168.1.0 255.255.255.0 192.168.3.1 1网段

ip route 192.168.2.0 255.255.255.0 192.168.3.1 2网段

ip route 192.168.10.0 255.255.255.0 192.168.3.1 10网段

**实验名称：**

实验九：动态路由RIP

**实验目的：**

（1）深入掌握IP协议和路由原理

（2）掌握静态路由原理和RIP路由协议原理

**实验仪器：**

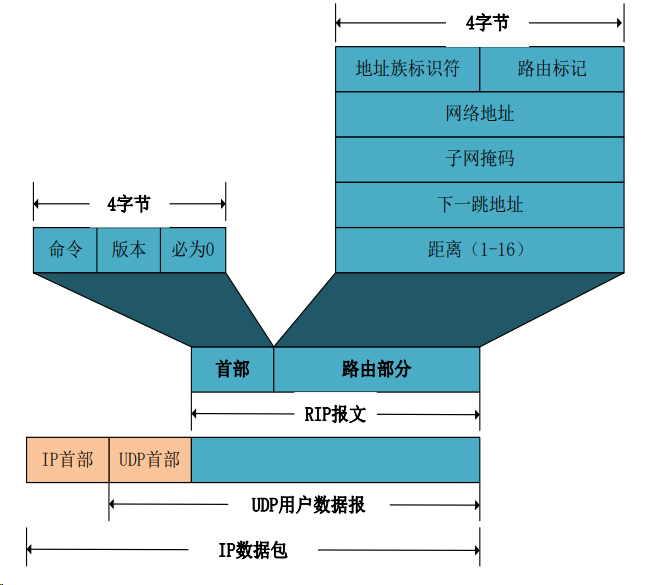
Router路由器2台、三层交换机1台、主机2台、直连线3条

**实验原理：**

首先通过文章[RIP动态路由原理与实验详解（动态路由协议概述与分类，RIP协议工作原理）\_什么是rip动态路由协议-CSDN博客](https://blog.csdn.net/CN_TangZheng/article/details/102644103)来学习动态路由的相关知识。

RIP协议有两个版本，RIPv1和RIPv2。RIPv1属于有类路由协议，不支持VLSM（变长子网掩码），RIPv1是以广播的形式进行路由信息的更新的，广播地址为 255.255.255.255。RIPv2属于无类路由协议（CIDR），支持VLSM（变长子网掩码），RIPv2以组播的形式进行路由信息的更新的，组播地址是224.0.0.9。

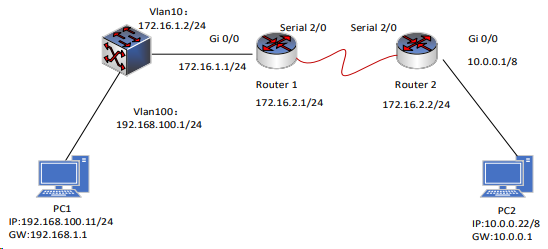
RIPv1和RIPv2运行版本不一样，两者同时工作时，学不到对方的路由，RIPv1只发送RIPv1报文，接收RIPv1报文；RIPv2只发送RIPv2报文，接收RIPv2报文。



如上图所示为RIPv2版本的报文格式。RIP报文由首部和路由部分组成，采用UDP报文传输；首部占4个字节，命令字段指出报文的意义，1表示请求路由信息，2表示对请求路由信息的的响应或未被请求而发出的路由更新报文。RIPv2路由部分由若干条路由信息组成，每个路由信息需要20个字节，地址族标识符用来标识所使用的地址协议，路由标记填入自治系统号，一个 RIP报文最多包含25条路由条目。

RIPv2是一种无类别路由协议，相比于RIPv1，它具有功能上的增强和对错误的抵抗能力，实验指导书中有详细说明，这里不再赘述。

RIP协议具有“好消息”传播得快，“坏消息”传播得慢的特点，它最大的优点是实现简单，开销较小，但是它的最大使用距离为15，限制了网络的规模。通常情况下，RIP每隔30秒向外发送一次更新报文，如果设备经过180秒没有收到来自对端的路由更新报文，则将所有来自此设备的路由信息标志为不可达，路由进入不可达状态后，120秒内仍未收到更新报文，就将这些路由从路由表中删除。如下图是本次实验的网络拓扑结构图。

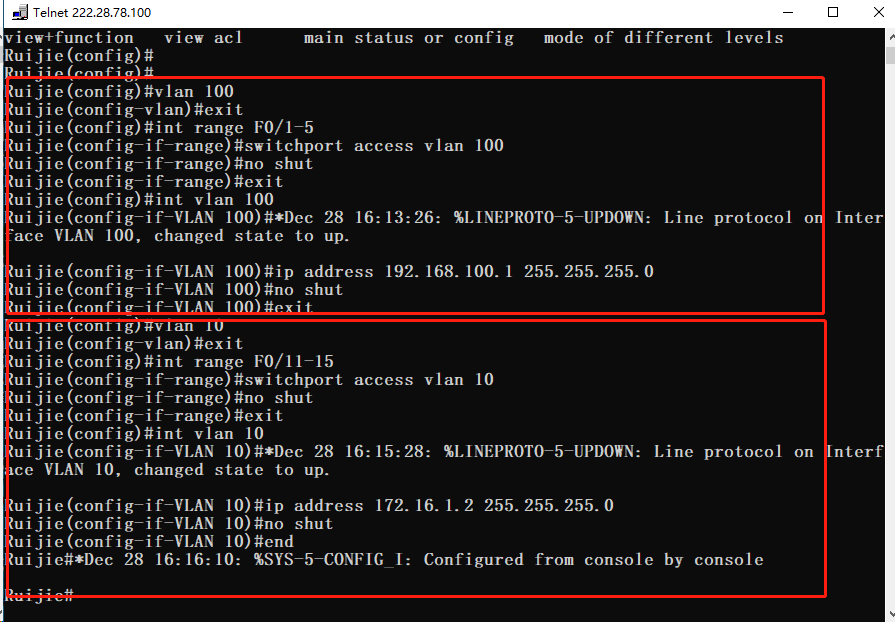


**实验内容与步骤：**

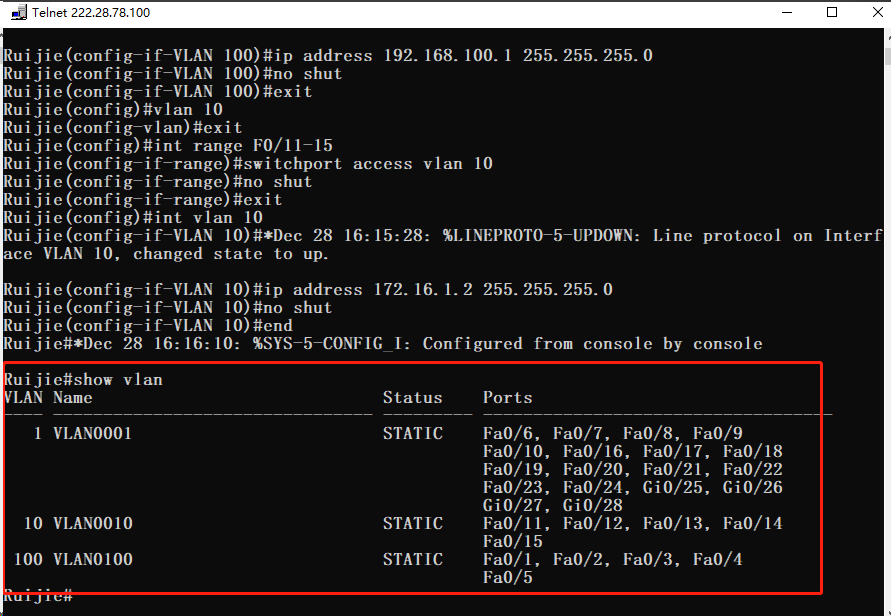
**（1）线缆连接**

由于路由器之间已经连接好，因此需要将交换机、PC与路由器相连。

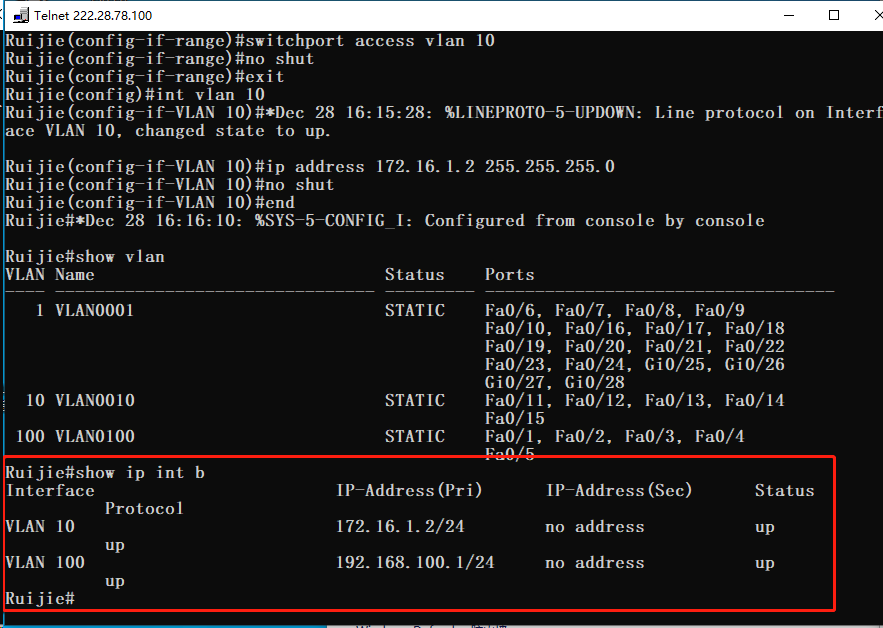
**（2）交换机创建Vlan，并进行端口的划分**



查看端口划分情况

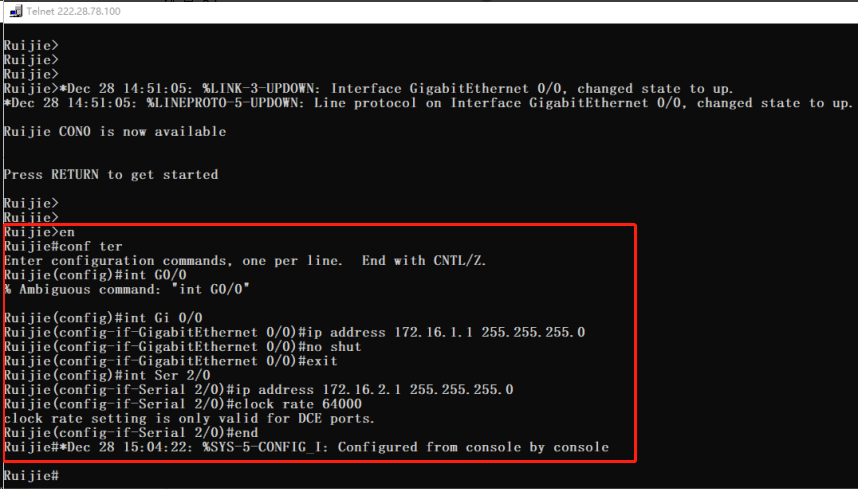


查看IP地址是否正确

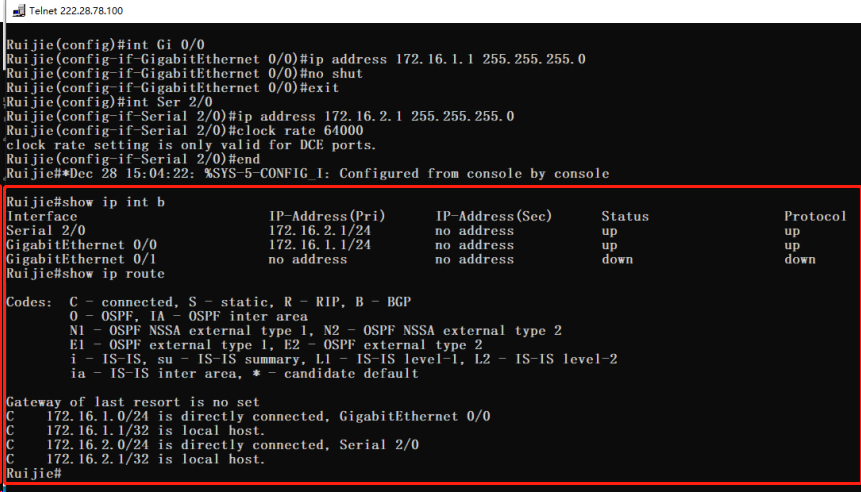


**（3）配置路由器端口IP地址**

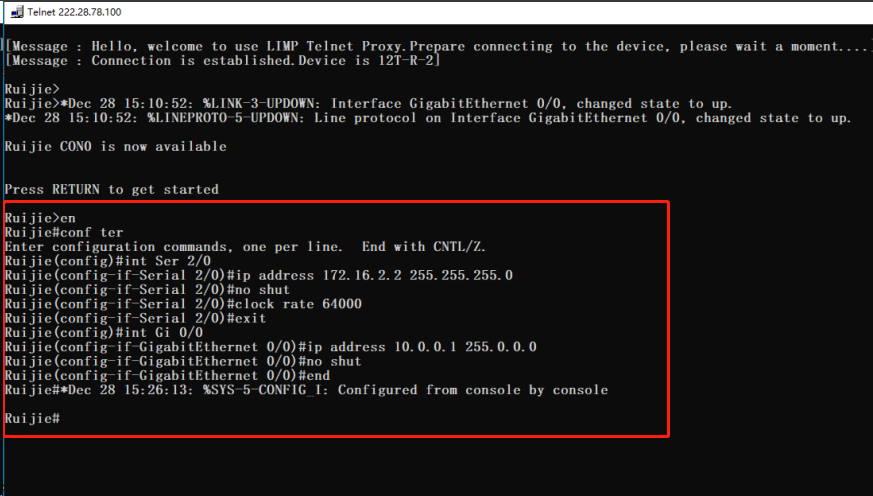
配置R1



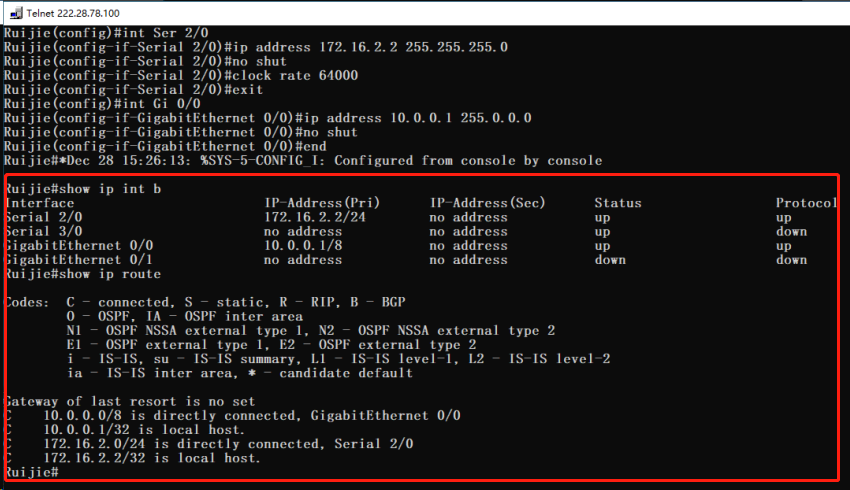
查看R1



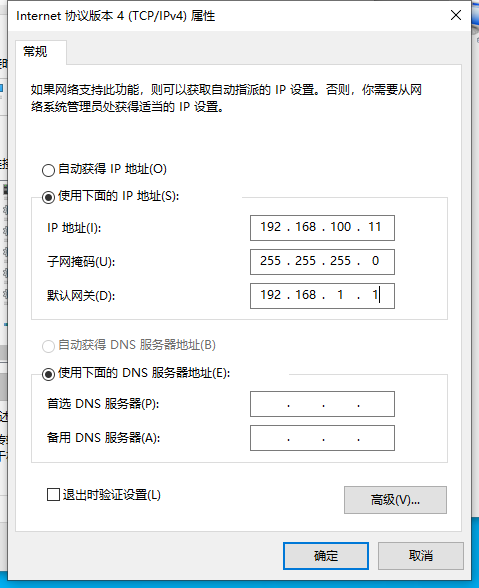
配置R2



查看R2

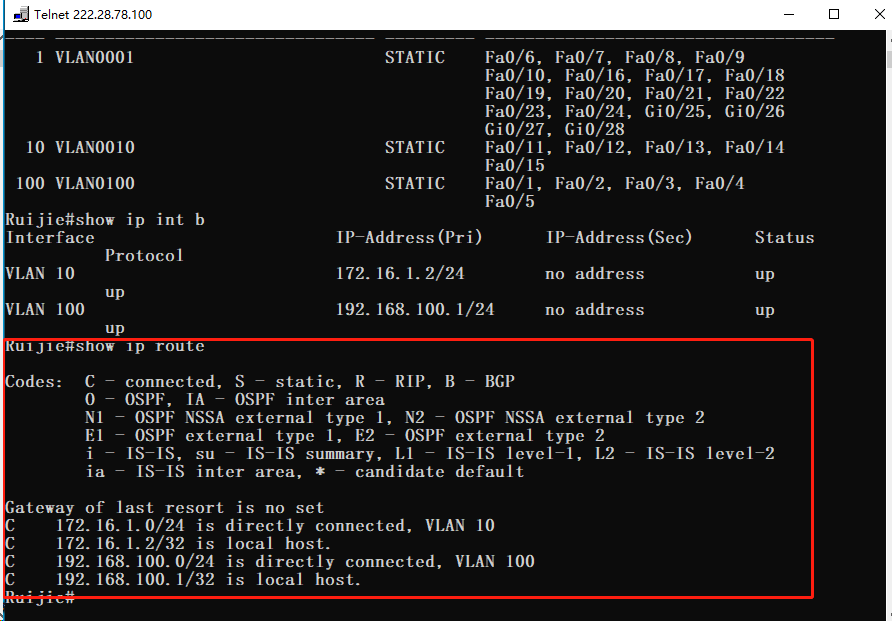


配置PC1和PC2

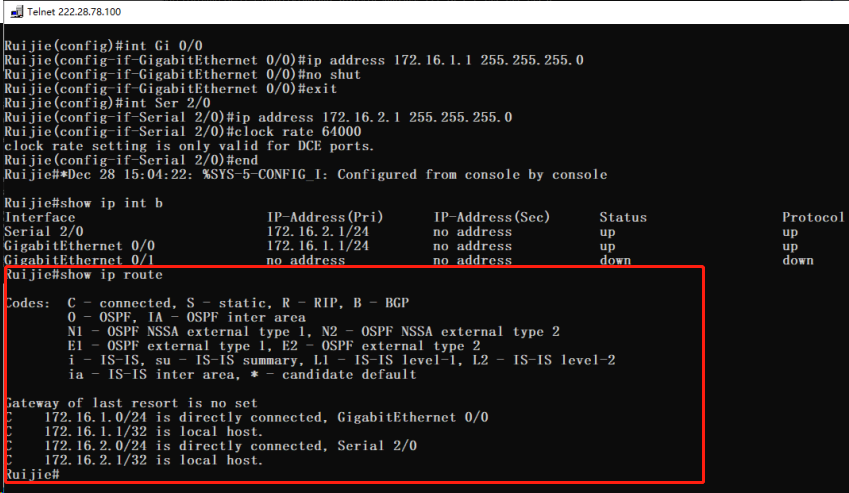


**（4）通过命令查看交换机和路由器的路由表**

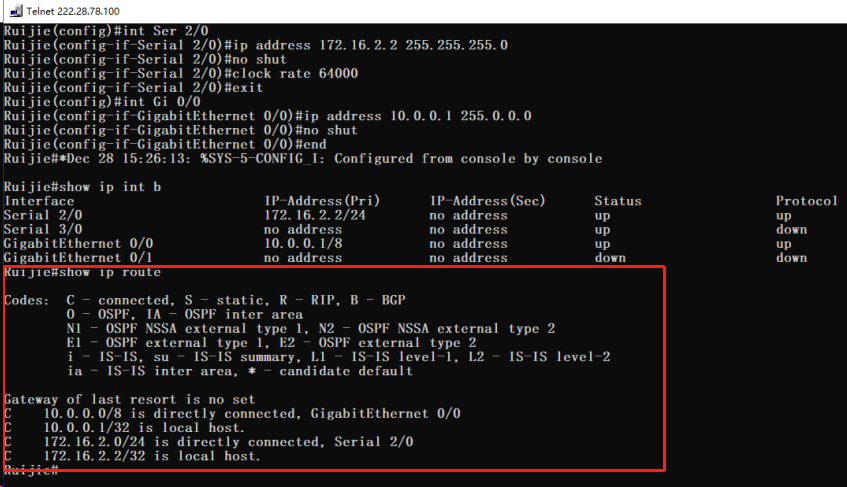
交换机



路由器R1

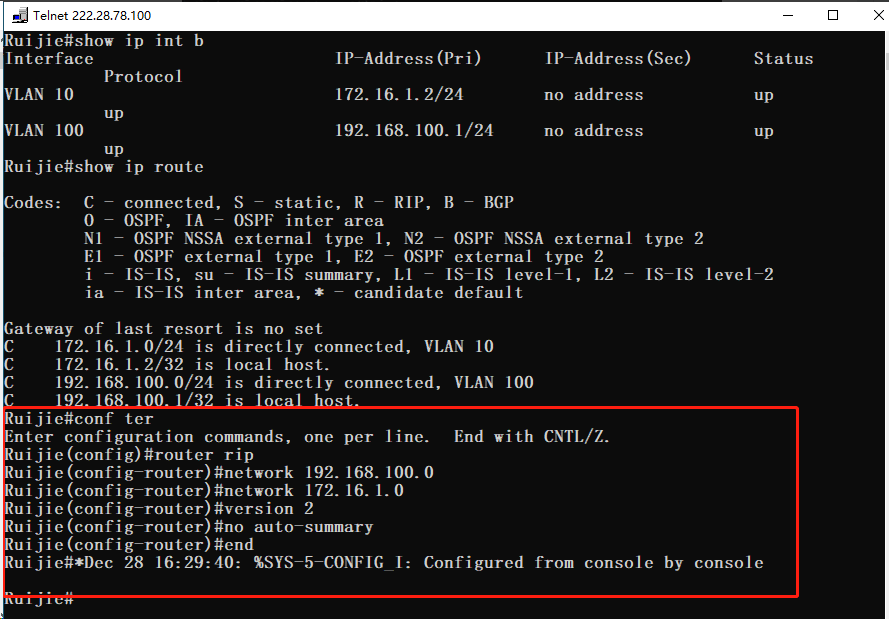


路由器R2

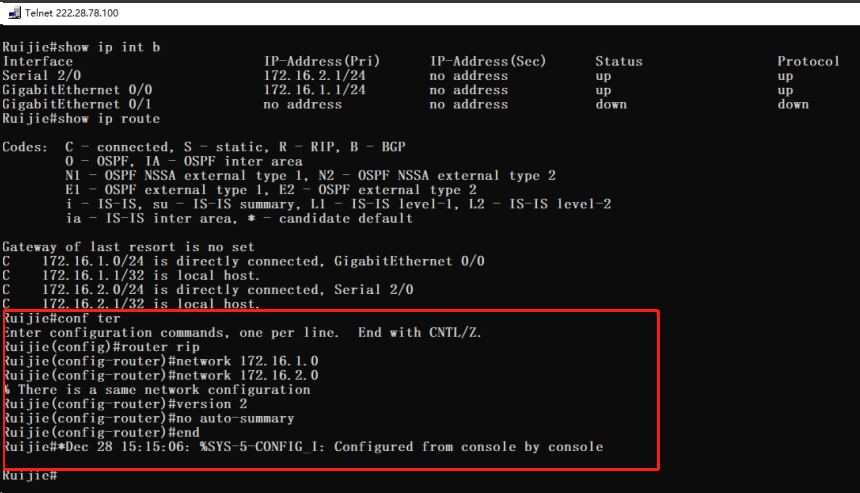


**（5）配置动态路由RIP**

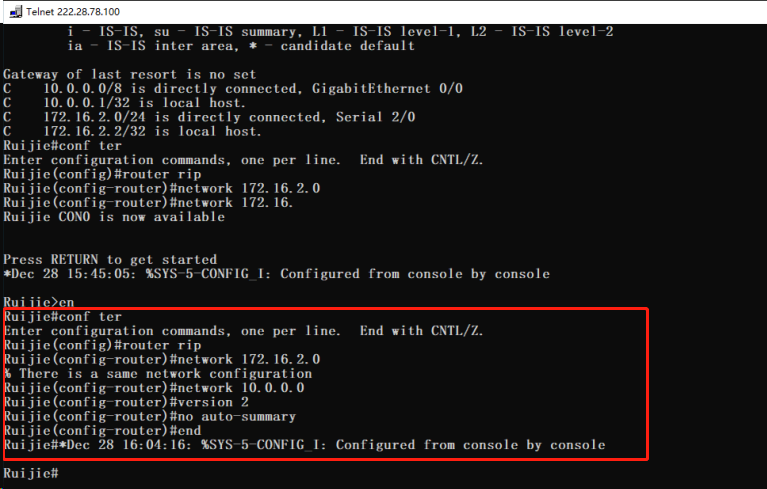
**A、三层交换机配置RIPv2协议**



**B、Router1配置RIPv2协议**



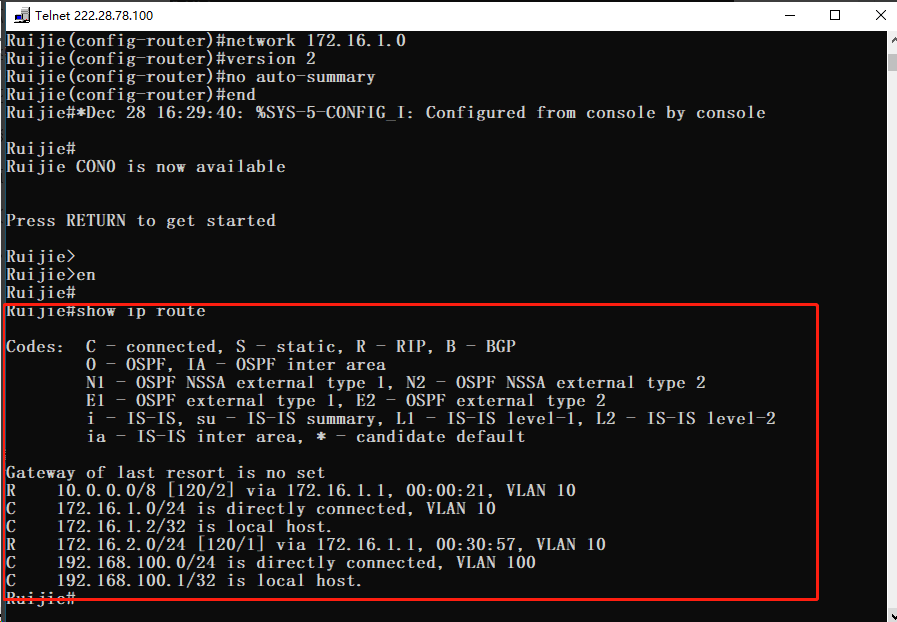
**C、Router2配置RIPv2协议**



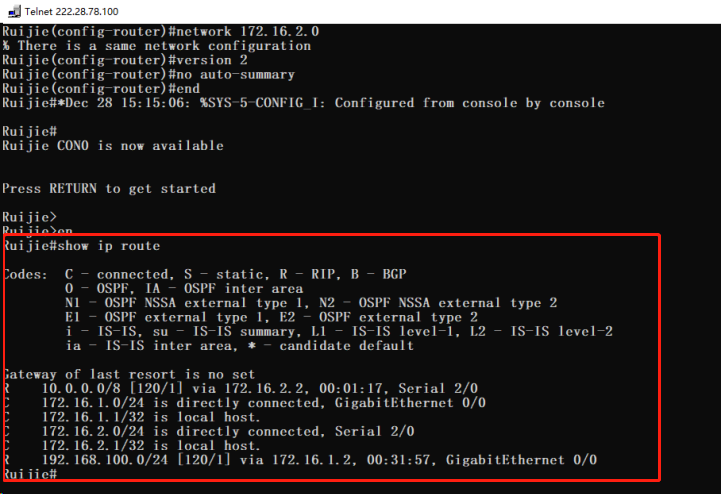
**（6）测试**

**A、查看RIP路由**

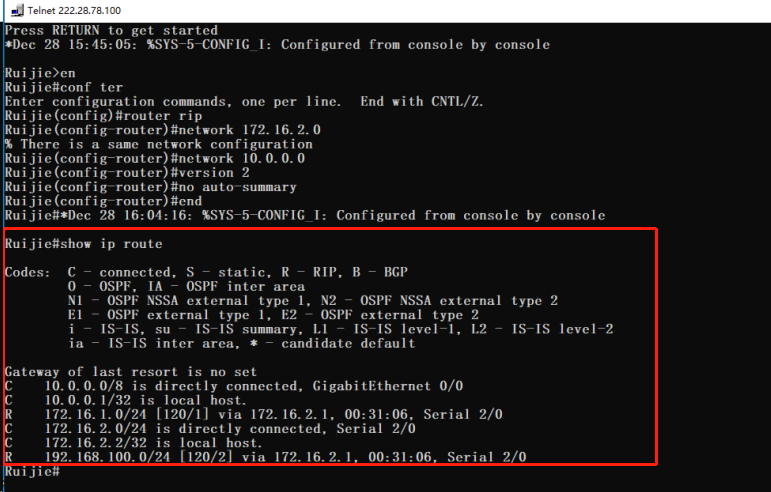
交换机



路由器R1

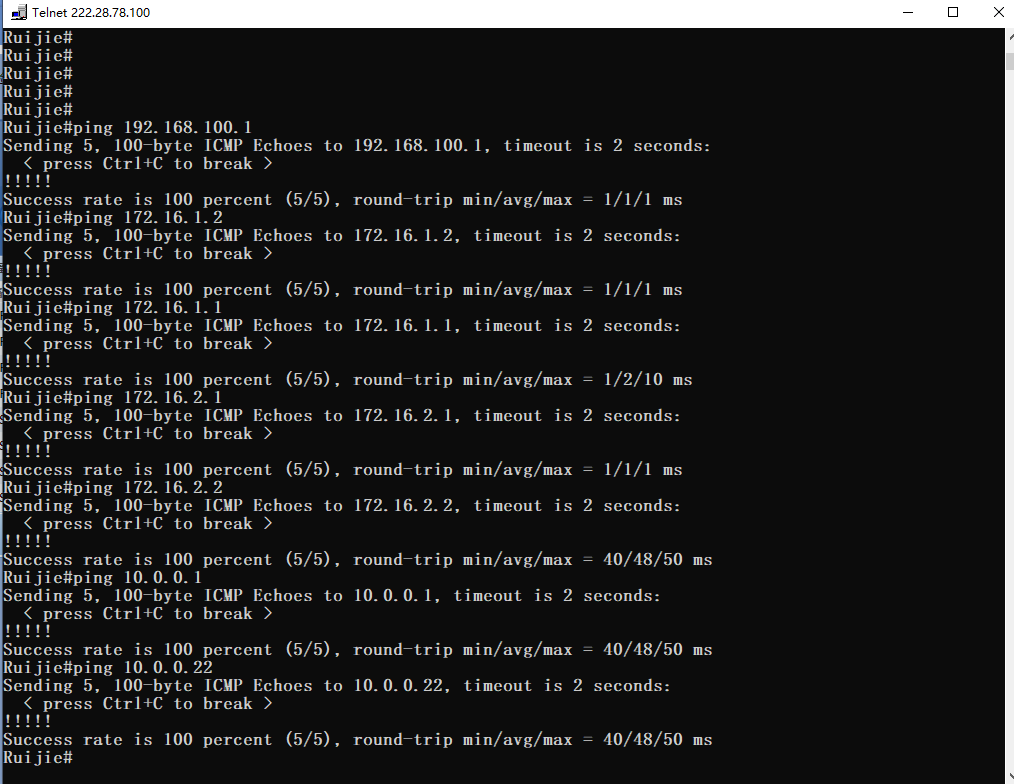


路由器R2



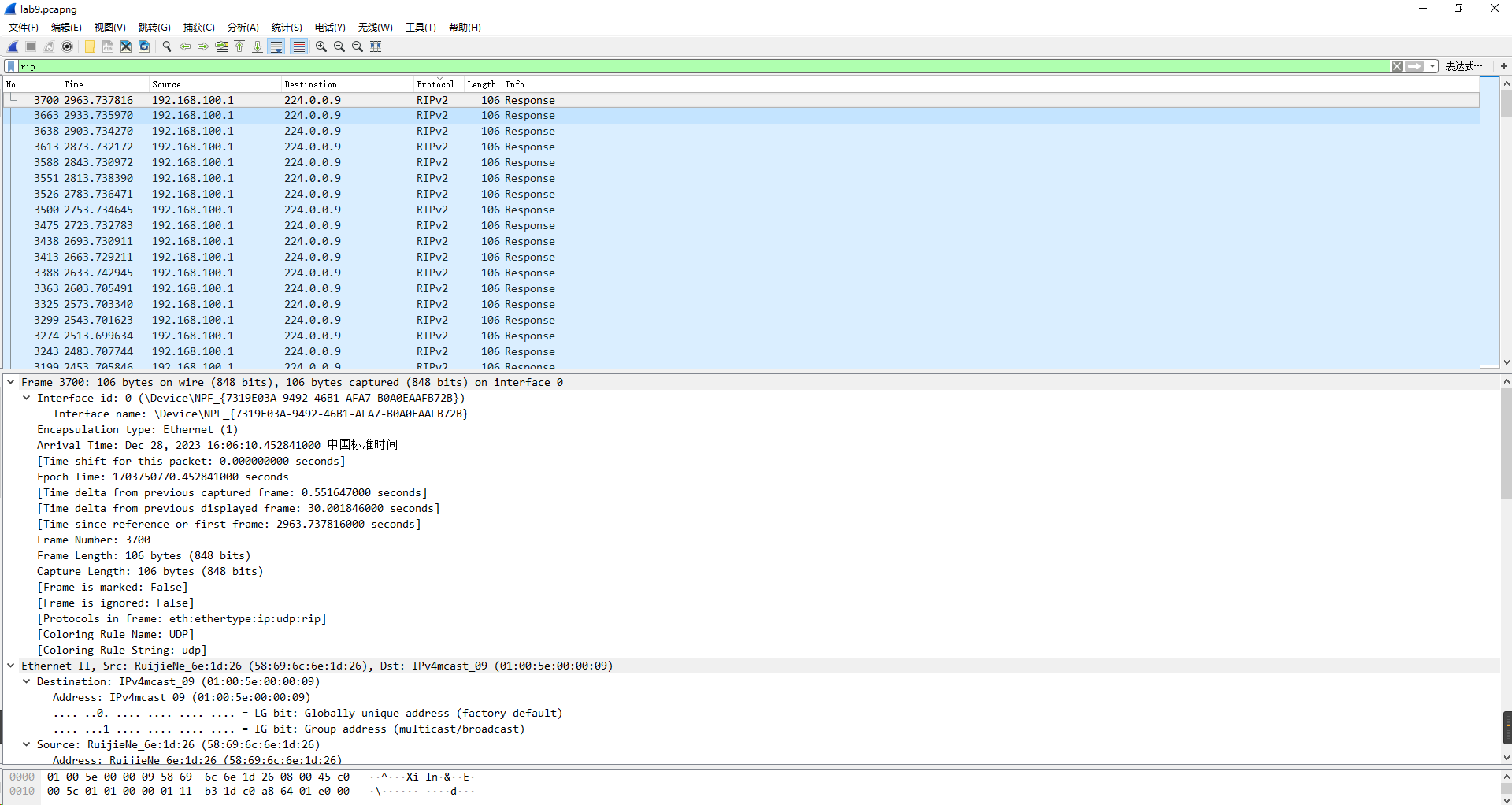
**B、分段进行Ping命令测试**

由近及远进行测试，测试结果如下。



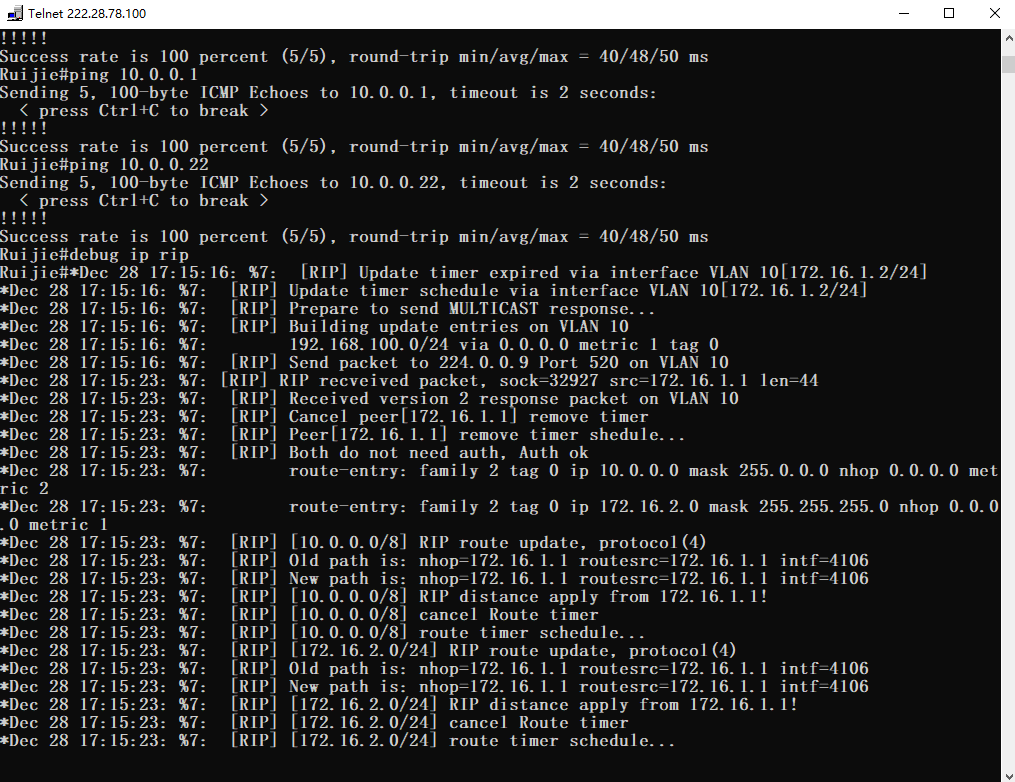
**（7）利用wireshark分析RIP通告报文，过滤显示所有RIP报文**

利用wireshark进行抓包，得到如下的数据包，将在数据处理环节进行分析。

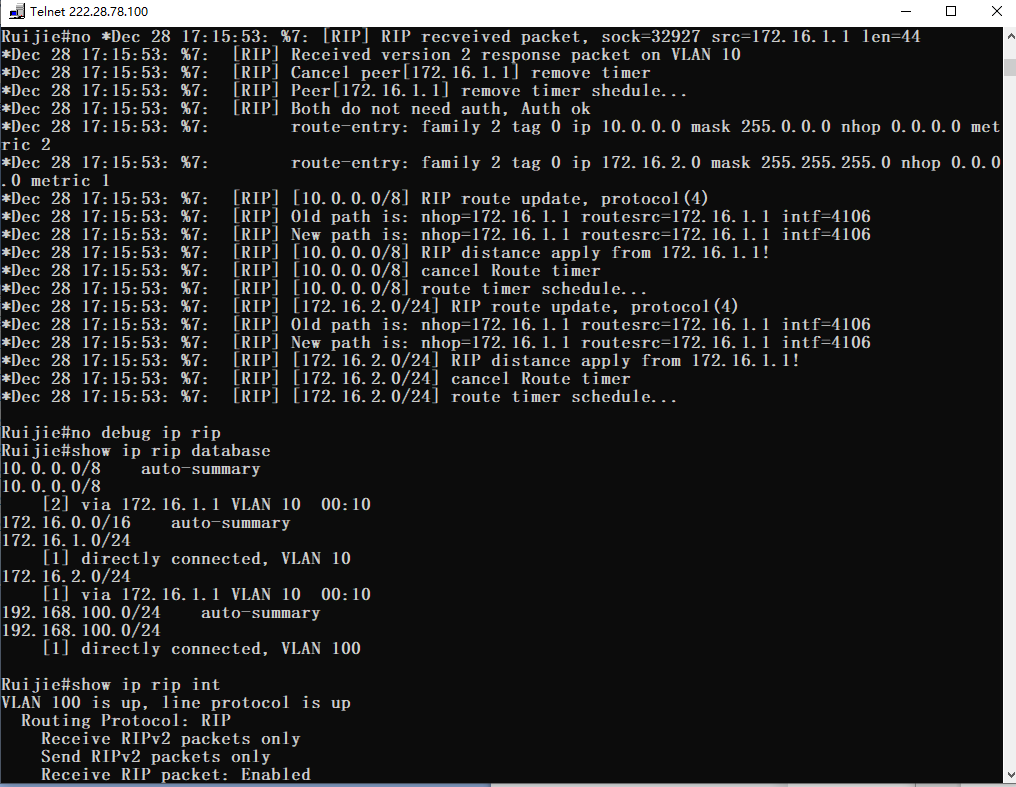


**（8）查看路由器更新情况和RIP路由信息**

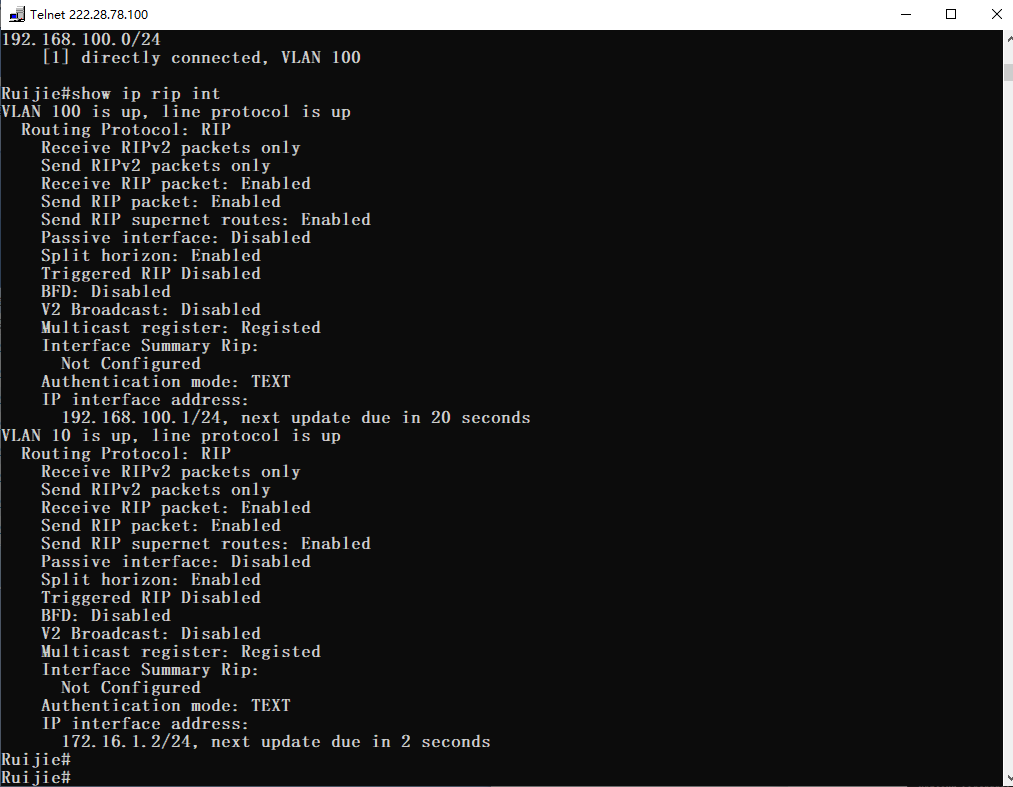
debug ip rip



show ip rip database



show ip rip interface



**实验数据：**

本次实验的实验数据主要有数据包一份，将在实验数据处理环节进行分析，部分实验步骤以图片的形式记录于实验步骤中。

**实验数据处理：**

对于数据包，对其中一个进行分析。

|  |
| --- |
| Frame 3700: 106 bytes on wire (848 bits), 106 bytes captured (848 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 28, 2023 16:06:10.452841000 中国标准时间  [Time shift for this packet: 0.000000000 seconds]  Epoch Time: 1703750770.452841000 seconds  [Time delta from previous captured frame: 0.551647000 seconds]  [Time delta from previous displayed frame: 30.001846000 seconds]  [Time since reference or first frame: 2963.737816000 seconds]  Frame Number: 3700  Frame Length: 106 bytes (848 bits)  Capture Length: 106 bytes (848 bits)  [Frame is marked: False]  [Frame is ignored: False]  [Protocols in frame: eth:ethertype:ip:udp:rip]  [Coloring Rule Name: UDP]  [Coloring Rule String: udp]  Ethernet II, Src: RuijieNe\_6e:1d:26 (58:69:6c:6e:1d:26), Dst: IPv4mcast\_09 (01:00:5e:00:00:09)  Destination: IPv4mcast\_09 (01:00:5e:00:00:09)  Address: IPv4mcast\_09 (01:00:5e:00:00:09)  .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)  .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)  Source: RuijieNe\_6e:1d:26 (58:69:6c:6e:1d:26)  Address: RuijieNe\_6e:1d:26 (58:69:6c:6e:1d:26)  .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)  .... ...0 .... .... .... .... = IG bit: Individual address (unicast)  Type: IPv4 (0x0800)  Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.9  0100 .... = Version: 4  .... 0101 = Header Length: 20 bytes (5)  Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)  1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)  Total Length: 92  Identification: 0x0101 (257)  Flags: 0x0000  0... .... .... .... = Reserved bit: Not set  .0.. .... .... .... = Don't fragment: Not set  ..0. .... .... .... = More fragments: Not set  Fragment offset: 0  Time to live: 1  Protocol: UDP (17)  Header checksum: 0xb31d [validation disabled]  [Header checksum status: Unverified]  Source: 192.168.100.1  Destination: 224.0.0.9  User Datagram Protocol, Src Port: 520, Dst Port: 520  Source Port: 520  Destination Port: 520  Length: 72  Checksum: 0x9268 [unverified]  [Checksum Status: Unverified]  [Stream index: 4]  Routing Information Protocol  Command: Response (2)  Version: RIPv2 (2)  IP Address: 10.0.0.0, Metric: 3  Address Family: IP (2)  Route Tag: 0  IP Address: 10.0.0.0  Netmask: 255.0.0.0  Next Hop: 0.0.0.0  Metric: 3  IP Address: 172.16.1.0, Metric: 1  Address Family: IP (2)  Route Tag: 0  IP Address: 172.16.1.0  Netmask: 255.255.255.0  Next Hop: 0.0.0.0  Metric: 1  IP Address: 172.16.2.0, Metric: 2  Address Family: IP (2)  Route Tag: 0  IP Address: 172.16.2.0  Netmask: 255.255.255.0  Next Hop: 0.0.0.0  Metric: 2 |

网络数据包的分析报文，主要内容包括以太网帧头部信息、IPv4头部信息、UDP头部信息以及RIP)数据。

**（1）以太网帧头部信息（Ethernet II）:**

源MAC地址（Source）: 58:69:6c:6e:1d:26

目标MAC地址（Destination）: 01:00:5e:00:00:09

类型（Type）: IPv4 (0x0800)

**（2）IPv4头部信息:**

源IP地址（Source）: 192.168.100.1

目标IP地址（Destination）: 224.0.0.9

版本（Version）: 4

头部长度（Header Length）: 20字节

区分服务字段（Differentiated Services Field）: 0xc0，表示DSCP为CS6（Class Selector 6），ECN（Explicit Congestion Notification）未启用。

总长度（Total Length）: 92字节

标识（Identification）: 0x0101

标志（Flags）: 0x0000，表示禁止分段

分段偏移（Fragment offset）: 0

存活时间（Time to live）: 1

协议（Protocol）: UDP (17)

校验和（Header checksum）: 0xb31d

**（3）UDP头部信息:**

源端口（Source Port）: 520

目标端口（Destination Port）: 520

长度（Length）: 72字节

校验和（Checksum）: 0x9268

**（4）Routing Information Protocol (RIP) 数据:**

命令（Command）: Response (2)

版本（Version）: RIPv2 (2)

**对于每个RIP路由项：**

**第一项:**

IP地址（IP Address）: 10.0.0.0，度量（Metric）: 3

地址族（Address Family）: IP (2)

路由标签（Route Tag）: 0

子网掩码（Netmask）: 255.0.0.0

下一跳（Next Hop）: 0.0.0.0

**第二项:**

IP地址: 172.16.1.0，度量: 1

地址族: IP (2)

路由标签: 0

子网掩码: 255.255.255.0

下一跳: 0.0.0.0

**第三项:**

IP地址: 172.16.2.0，度量: 2

地址族: IP (2)

路由标签: 0

子网掩码: 255.255.255.0

下一跳: 0.0.0.0

**实验结果与分析：**

在这个环节，将针对实验指导书中的部分思考问题进行回答。

**（1）水平分割、毒性逆转、触发更新分别是什么意思？**

水平分割、毒性逆转和触发更新都是为了防止路由环路产生的方法。

A、水平分割：由于路由器可能收到它自己发送的路由信息，而这种信息是无用的。因此路由器在路由信息传送过程中，不再把路由信息发送到接收到此路由信息的接口上，从而在一定程度上避免了环路的产生。

B、毒性逆转：毒性逆转是一种改进的水平分割，路由器从某个接口上接收到某个网段的路由信息之后，并不是不往回发送信息了，而是发送，只不过是将这个网段的跳数设为无限大，再发送出去。收到此种的路由信息后，接收方路由器会立刻抛弃该路由，而不是等待其老化时间到。这样可以加速路由的收敛。

C、若网络中没有变化，则按通常的30秒间隔发送更新信息。但若有变化，路由器就立即发送其新的路由表，这个过程叫做触发更新。

**（2）RIPv2与RIPv1相比，在哪些方面做了改进？**

RIPv2与RIPv1相比的改进主要是为了适应更加复杂的网络环境和提高路由协议的性能。

A、支持无类别域间路由（CIDR）：RIPv2支持CIDR，这使得更有效地利用IP地址空间成为可能。CIDR允许网络管理员使用不同长度的子网掩码，而不仅仅是类似于RIPv1的固定子网掩码。

B、支持VLSM：RIPv2允许使用不同的子网掩码长度，以实现更灵活的网络设计。这允许在同一网络上使用不同大小的子网。

C、支持路由认证：RIPv2引入了对路由更新的认证机制，通过认证可以确保接收到的路由信息是可信的。这有助于防范路由欺骗和其他安全问题。

D、支持多播：RIPv2可以使用多播地址来发送路由更新，而不是像RIPv1那样使用广播。这提高了网络的可扩展性和效率，特别是在大型网络中。

E、支持下一跳地址：RIPv2可以在路由更新中包含下一跳地址信息，这有助于避免在网络中产生死循环，并提高路由选择的准确性。

F、支持分割广播域：RIPv2支持将网络分割成不同的广播域，这有助于减少广播风暴的潜在影响。

**（3）RIPv2采用什么报文通告信息，端口号是多少？分析抓取到的RIPv2的通告信息，叙述路由器R2的路由表的建立过程。**

根据报文分析，RIPv2使用UDP协议进行路由信息的通告，UDP端口号为520。

**UDP头部信息:**

源端口（Source Port）: 520

目标端口（Destination Port）: 520

这表明RIPv2的通告信息通过UDP的520端口进行传输。通过抓取到的RIPv2通告信息来叙述路由器R2的路由表建立过程：

**报文中的RIPv2信息:**

命令（Command）: Response (2)

版本（Version）: RIPv2 (2)

**路由表项1:**

IP地址（IP Address）: 10.0.0.0，度量（Metric）: 3

地址族（Address Family）: IP (2)

路由标签（Route Tag）: 0

子网掩码（Netmask）: 255.0.0.0

下一跳（Next Hop）: 0.0.0.0

**路由表项2:**

IP地址: 172.16.1.0，度量: 1

地址族: IP (2)

路由标签: 0

子网掩码: 255.255.255.0

下一跳: 0.0.0.0

**路由表项3:**

IP地址: 172.16.2.0，度量: 2

地址族: IP (2)

路由标签: 0

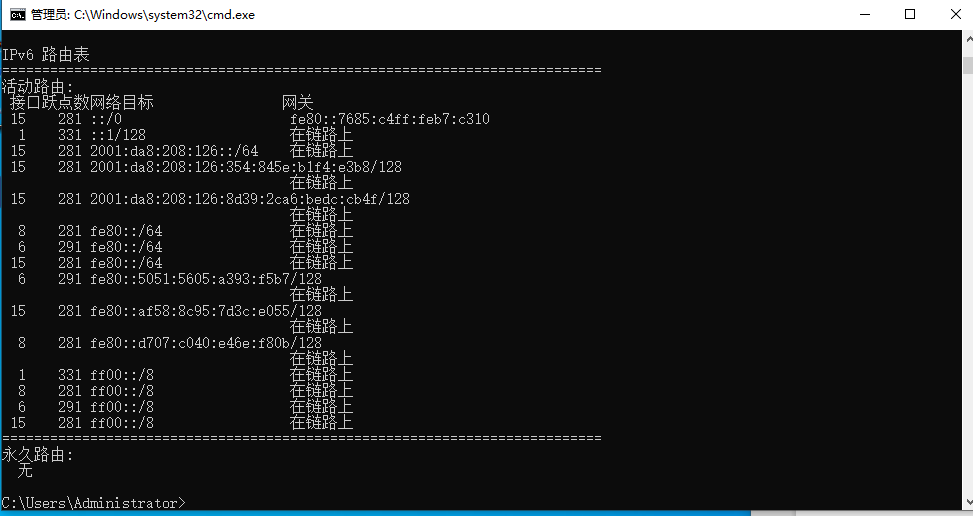
子网掩码: 255.255.255.0

下一跳: 0.0.0.0

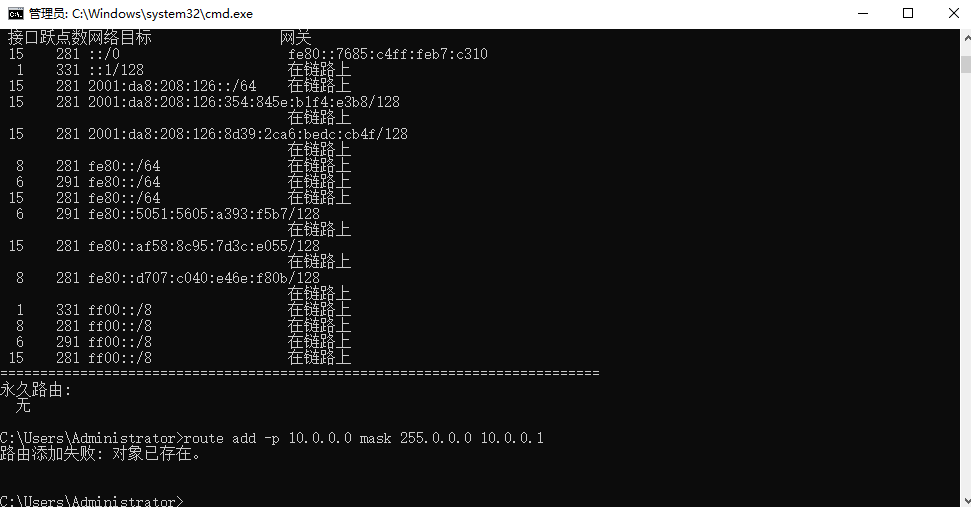
这些信息表示R2路由器收到了一份RIPv2 Response，其中包含了三个路由信息。根据RIPv2的工作原理，当一个路由器收到RIPv2通告时，它会将收到的路由信息添加到自己的路由表中。在这里，R2学到了三个路由，每个路由都包含有关网络地址、子网掩码、度量和下一跳的信息。

**附加题目：不禁用校园网卡的情况下，实现PC1 ping通PC2，以及实现PC1 ping通校园网**

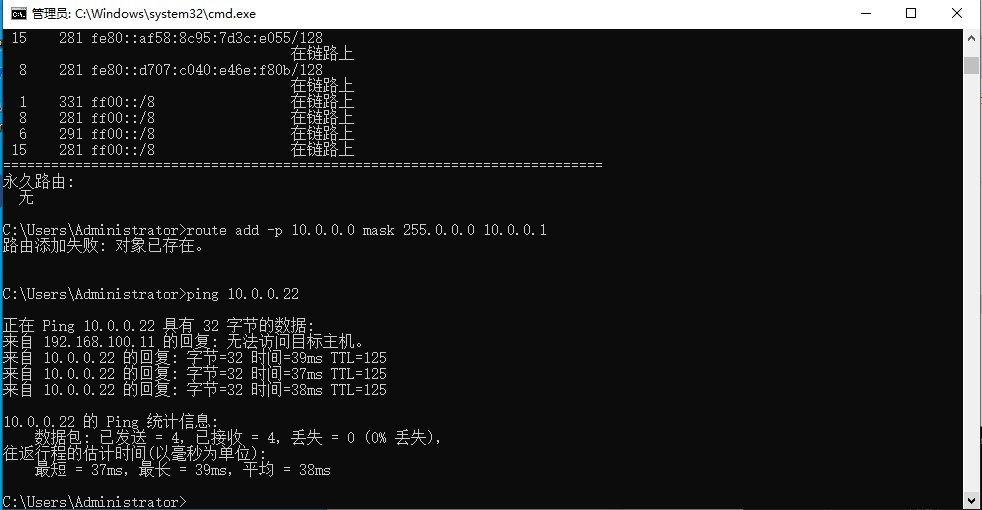
**A、通过route print查看路由信息**



**B、通过route add添加路由信息**



**C、不禁用校园网卡PC1 Ping PC2**



**D、不禁用校园网卡PC1 ping校园网**

