**【实验名称】：帧中继配置实验**

**学生姓名：陈嘉瑞 合作学生： 无**

**实验地点：济事楼330网络实验室 实验时间：2023年10月23日**

**【实验目的】**

广域网是另一类主要有限物理网络，可以实现跨地域的网络连接，承担着骨干传输网络作用，只有ISP(Internet Service Provider，互联网服务提供商)才会拥有，如中国电信、移动等，普通企业很难见到此类设备。本实验利用路由器模拟帧中继交换机，用于远程连接两个以太网，实现网络互连。

（1）了解广域网基本概念

（2）区分二层路由和三层路由基本概念

（3）熟悉帧中继交换机永久虚电路及配置步骤

**【实验原理】**

广域网跨越地域，由多个包交换机( Packet Switch )组成，包交换机分布在各个地域上，相互之间用高速通信线路直接相连，具有远距离、高性能，承担骨干网络作用。包交换机是广域网组成核心，控制着数据的传输。物理网络分一跳网络和多跳网络。一跳网络就是指数据从源节点直接到达目标节点，以太网就是典型的一跳网络。多跳网是指数据从源节点发送给目标节点的途中，需要经过其他网络节点才能到达，中间节点称为路由节点，广域网是典型的多跳网络。广域网路由算法和 IP 路由算法是完全一样，但两者实现细节不同，基于所属网络协议层层次不同，业界将物理网络路由称为二层路由，IP网络路由则称为三层路由。

广域网连接到互联网，也需要进行类似以太网的地址解析，但方式不同，广域网采用面向连接通信，使用电路号作为通信标识，因此需要将电路号同IP地址建立映射， IP数据包封装时就可以通过映射表进行转换。

帧中继是一种重要、流行的WAN连接标准，它是ITU-T和ANSI制定的种标准。它是一种面向连接的数据链路技术。这提高性能和效率进行了简化，帧中继用使用更可靠的光纤和数字网络，依靠高层协议进行纠错。

几个需要了解的概念如下：

①DLCI (数据链路连接标识)

DLCI是一种电路号，用于标识帧中继源和目的设备间的逻辑链路。DLCI是帧中继网络中的第2层地址。路由器将IP数据包通过帧中继网络转发到下一跳路由器时，必须知道IP地址和DLCI的映射关系才能进行帧的封装。有两种方法可以获得该映射，一种是静态映射，由管理员手工输人；另一种是动态映射。默认时，路由器帧中继接口开启动态映射功能。

②PVC (永久虚电路)

永久虚电路是指人工建立的链路，通过设置帧中继交换机静态路由表实现。一对进出的链路可以配置成一条永久虚电路。

③LMI (本地管理接口)

一种信令标志，负责设备管理，实现帧中继设备之间的连接管理，本地管理接口类型分 cisco , ansi 和q939a三种，配置时需要将帧中继交换机和路由器相连端口设置成同一种接口类型。

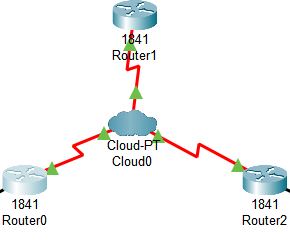
**【实验设备】**

一台装有Windows10操作系统的电脑、Cisco Packet Tracer实验软件。

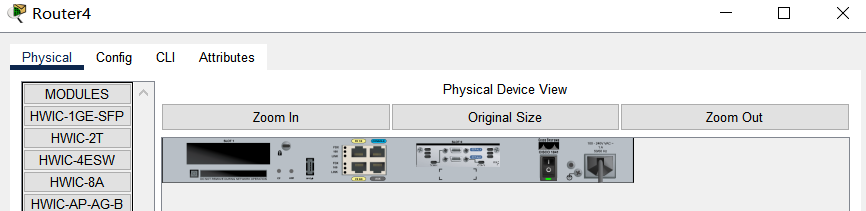
**【实验步骤及现象】**

1. **首先规划网络地址及拓扑图；**

按下图拓扑结构进行连接



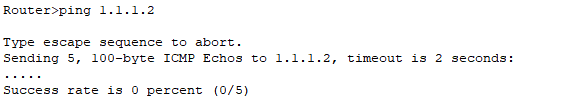
1. **硬件配置**



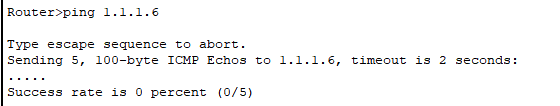
首先关闭路由器电源，拖动左侧HWIC-2T设备至图中红色框位置，重新打开电源。

1. **配置Frame Relay之前检查接口间能否相互ping通；**

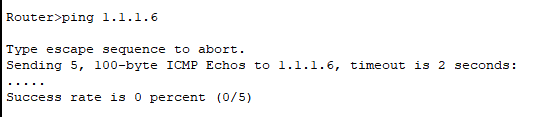
R0 ping R1



R0 ping R2



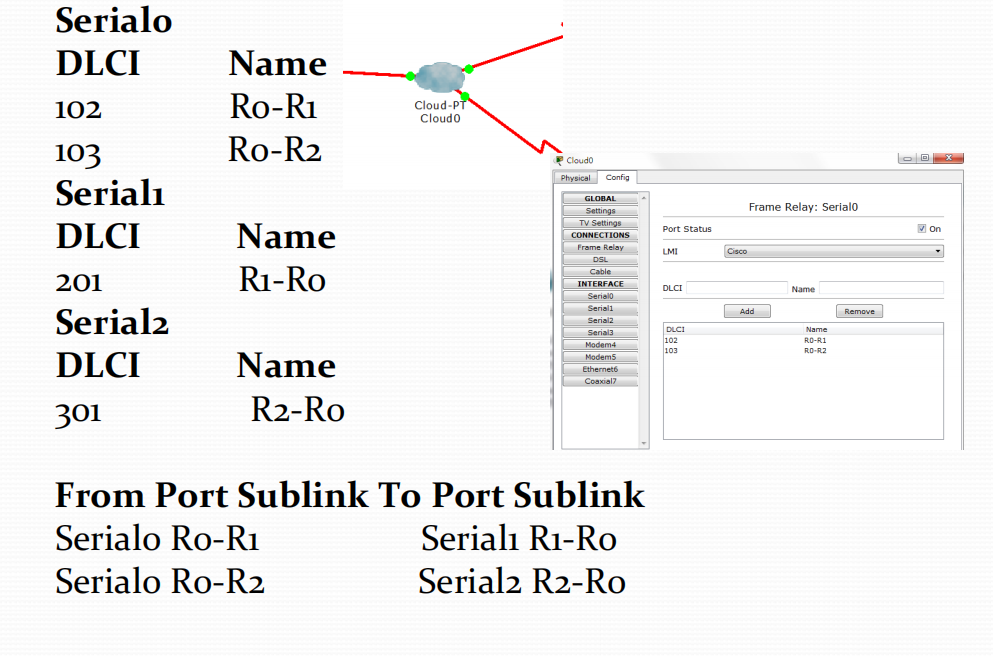
R1 ping R2



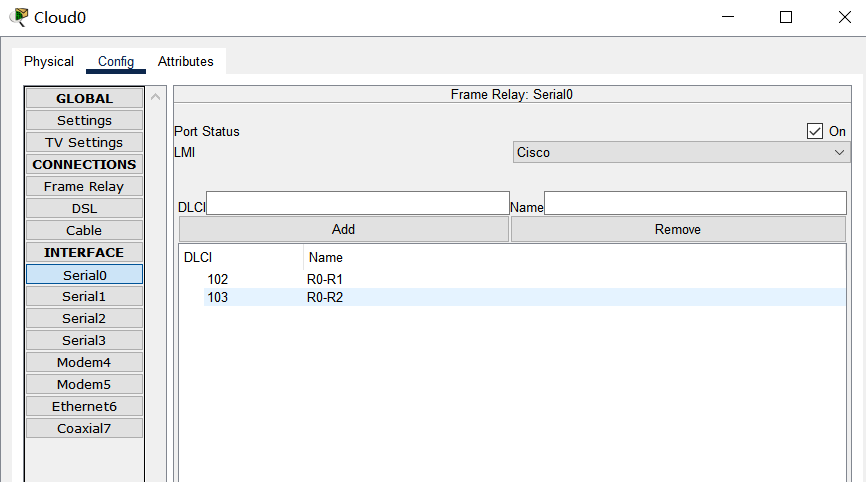
三次ping均失败，符合预期。

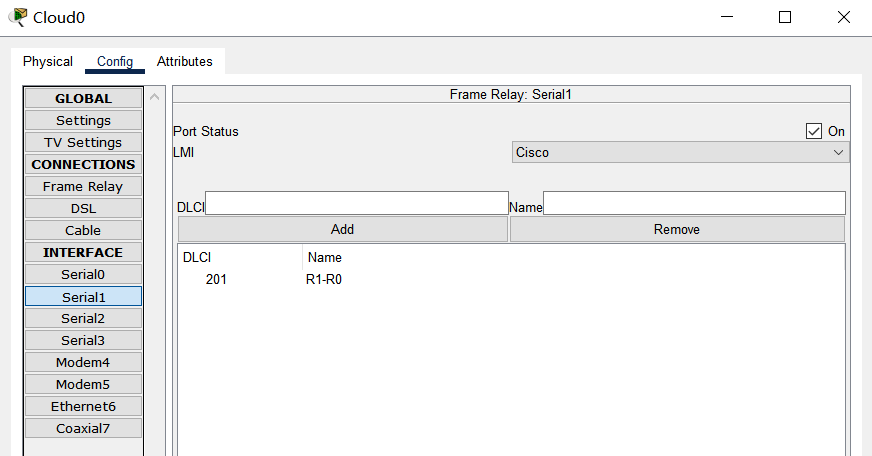
1. **配置帧中继交换机**

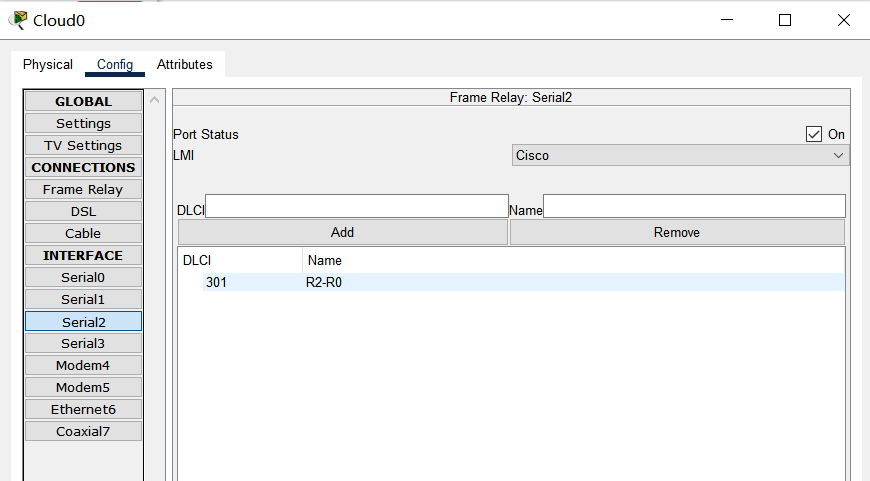
按课件中要求进行配置：

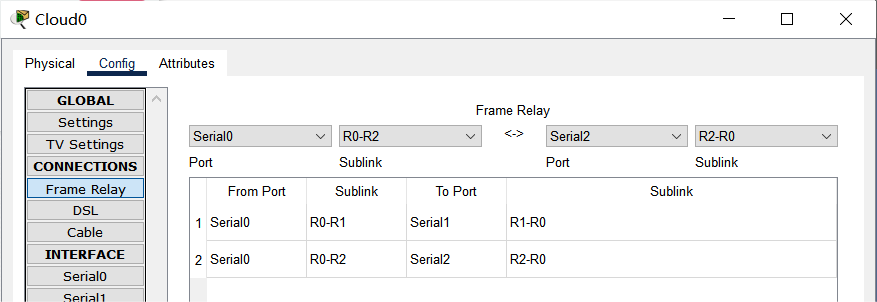


配置效果如下：









1. **在R0，R1，R2 配置 Frame Relay；**
2. **配置R0**

配置命令：

R0>enable

R0#configure terminal

R0(config)#interface Serial 0/0/0

R0(config-if)#no shutdown

R0(config-if)#encapsulation frame-relay

R0(config-if)#exit

R0(config)#interface Serial 0/0/0.102 point-to-point

R0(config-subif)#ip address 1.1.1.1 255.255.255.252

R0(config-subif)#frame-relay interface-dlci 102

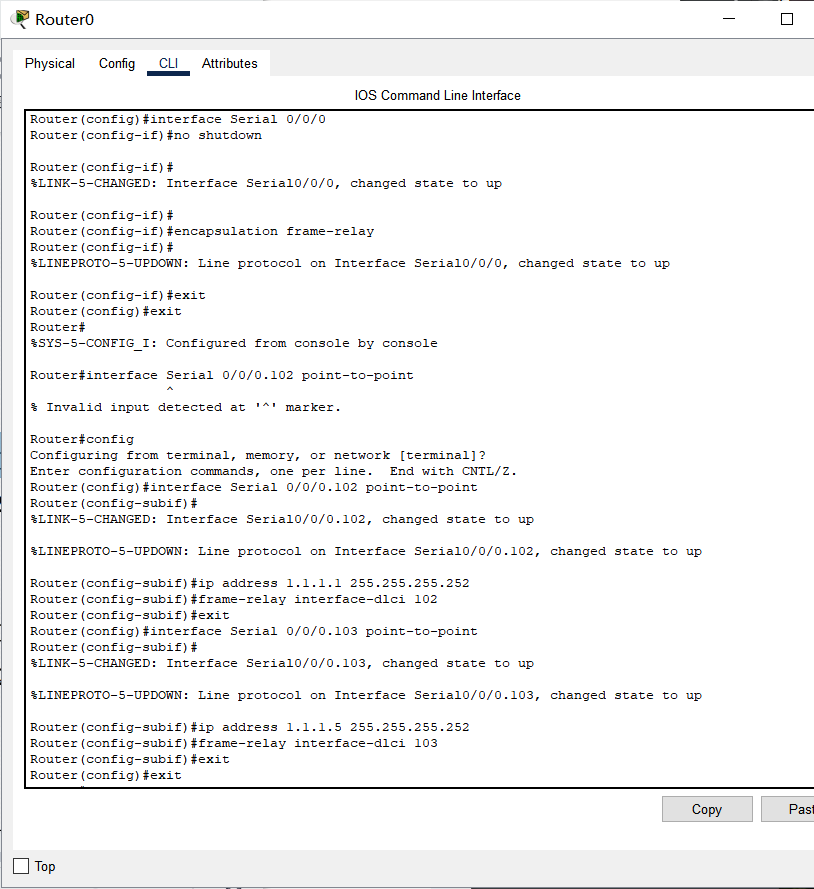
R0(config-subif)#exit

R0(config)#interface Serial 0/0/0.103 point-to-point

R0(config-subif)#ip address 1.1.1.5 255.255.255.252

R0(config-subif)#frame-relay interface-dlci 103

采用命令行方式配置：



1. **配置R1**

配置命令：

R1>enable

R1#configure terminal

R1(config)#interface Serial 0/0/0

R1(config-if)#no shutdown

R1(config-if)#encapsulation frame-relay

R1(config-if)#exit

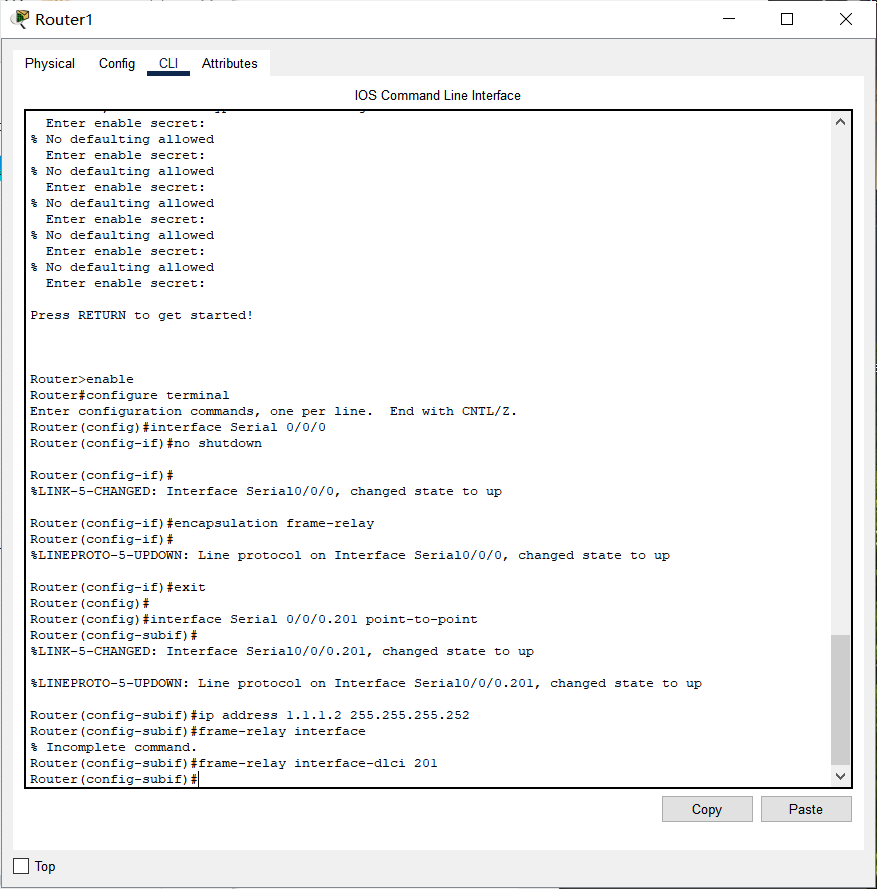
R1(config)#interface Serial 0/0/0.201 point-to-point

R1(config-subif)#ip address 1.1.1.2 255.255.255.252

R1(config-subif)#frame-relay interface

R1(config-subif)#frame-relay interface-dlci 201

采用命令行方式配置：



1. **配置R2**

配置命令：

R2>enable

R2#configure terminal

R2(config)#interface Serial 0/0/0

R2(config-if)#no shutdown

R2(config-if)#encapsulation frame-relay

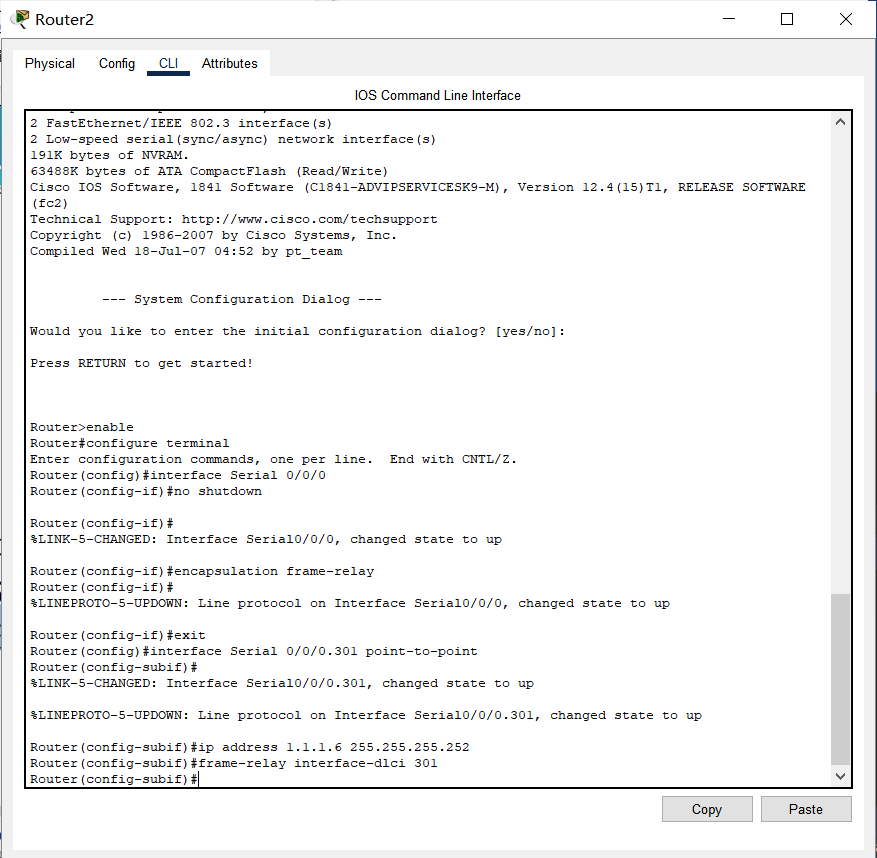
R2(config-if)#exit

R2(config)#interface Serial 0/0/0.301 point-to-point

R2(config-subif)#ip address 1.1.1.6 255.255.255.252

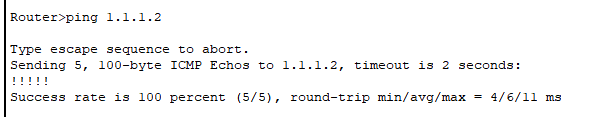
R2(config-subif)#frame-relay interface-dlci 301

采用命令行方式配置：

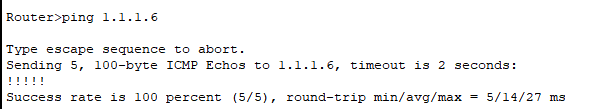


1. **配置静态路由前检查路由器之间是否能互相ping通**

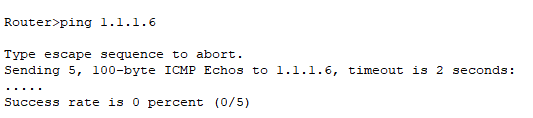
配静态路由前 R0 ping R1：



配静态路由前 R0 ping R2：



配静态路由前 R1 ping R2：

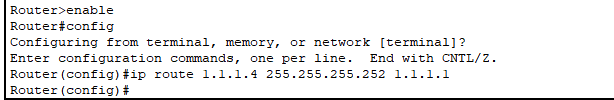


可以发现，配置静态路由前R0可以ping通R1和R2，但是R1和R2之间无法ping通

1. **在R1 R2配置静态路由；**

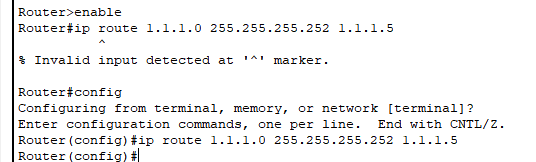
配置R1静态路由：

R1(config)#ip route 1.1.1.4 255.255.255.252 1.1.1.1



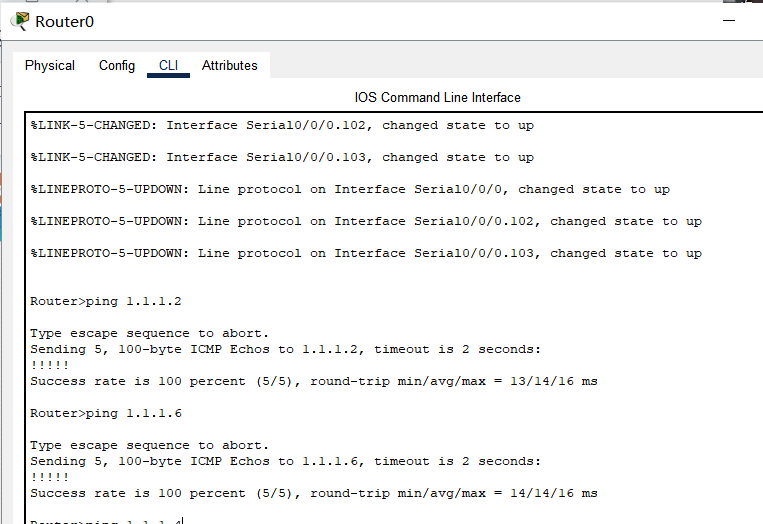
配置R2静态路由：

R2(config)#ip route 1.1.1.0 255.255.255.252 1.1.1.5

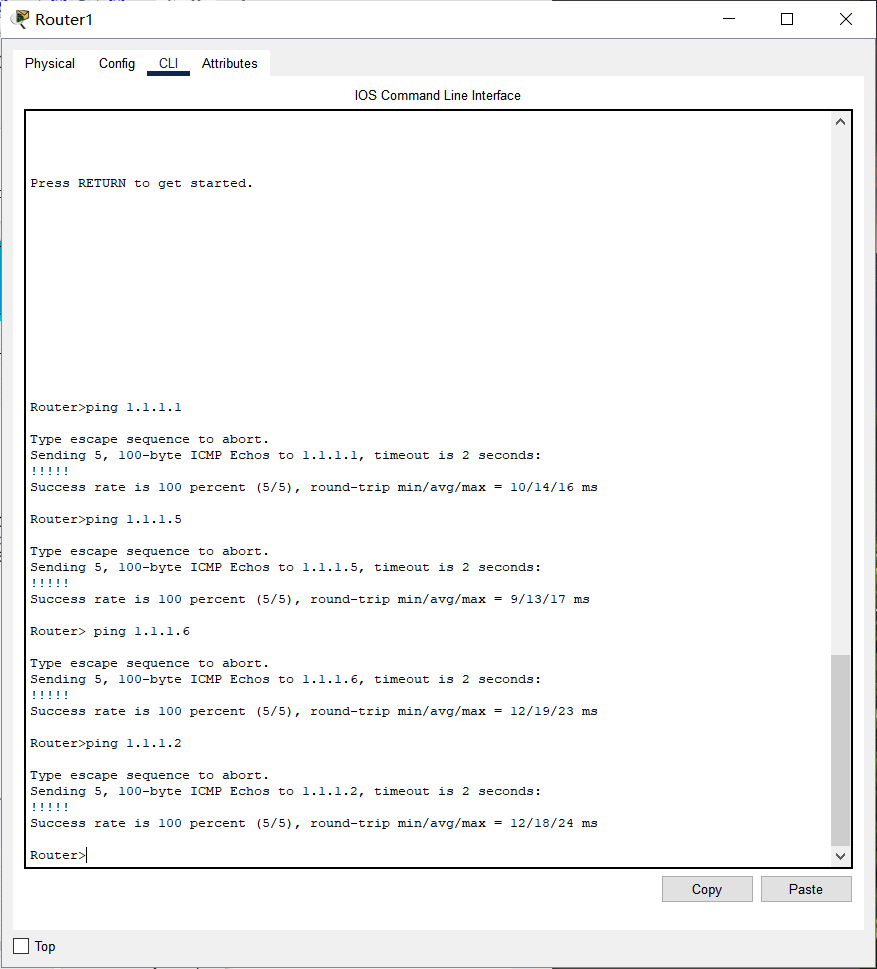


1. **验证接口之间的互通性。**

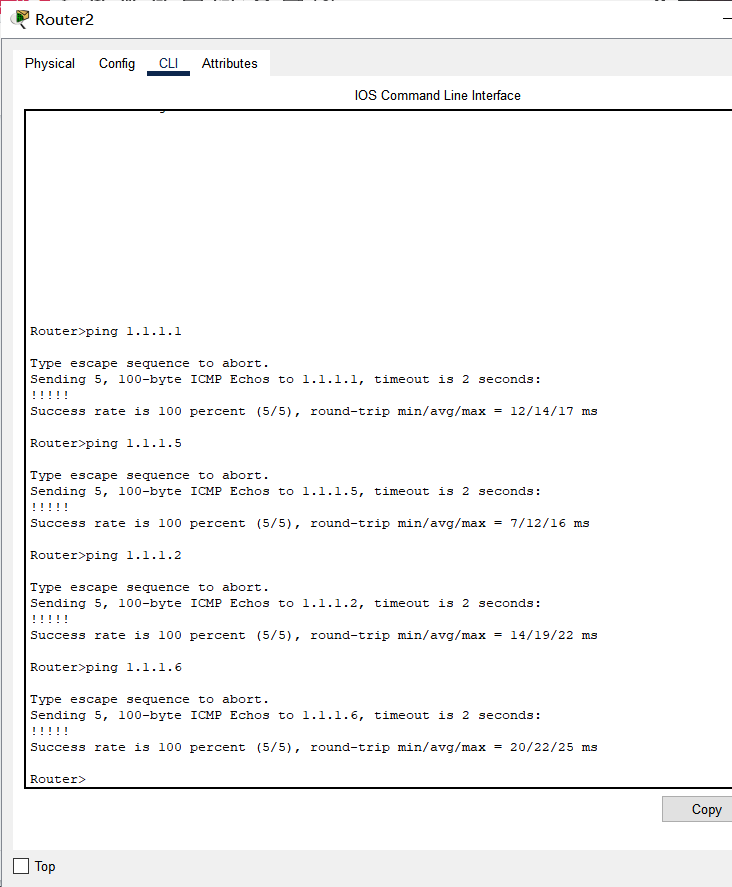
R0 ping R1、R0 ping R2：



R1 ping 各个端口：



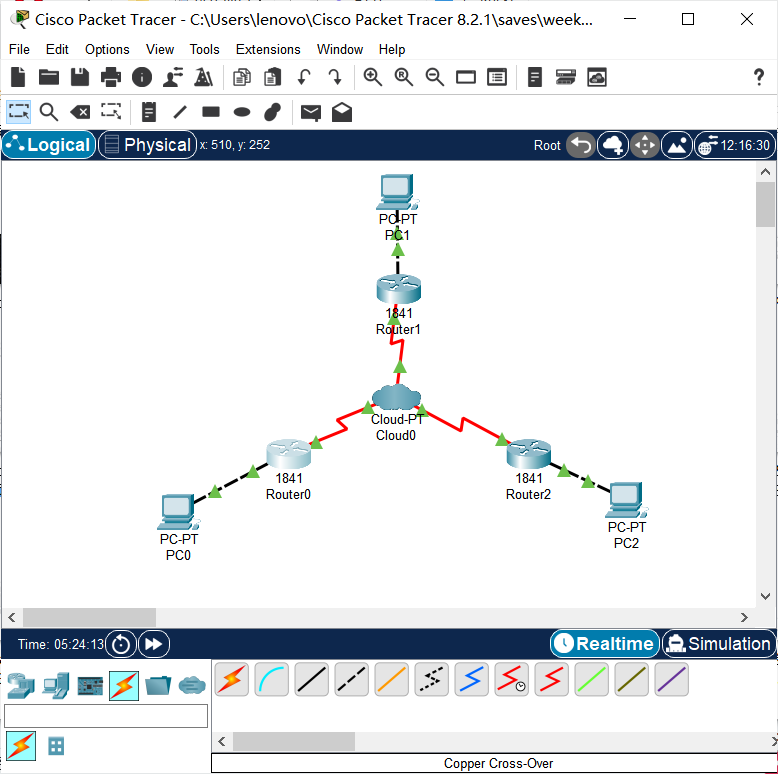
R2 ping 各个端口：



此时各个端口之间都能互相ping通

1. **添加三台PC并配置**

**（1）向拓扑结构中添加三台PC，拓扑结构变为如下所示：**



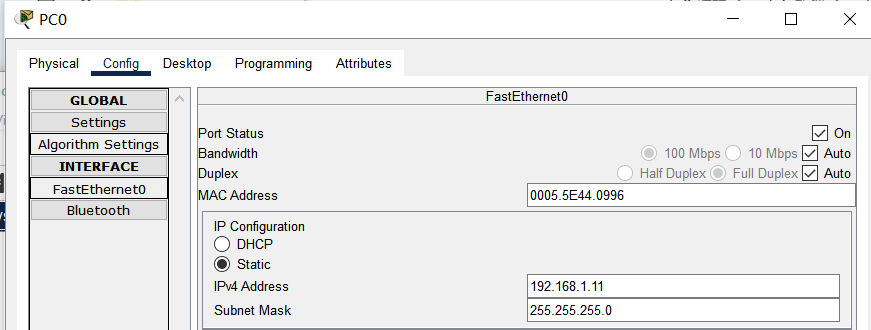
**（2）对PC进行配置**

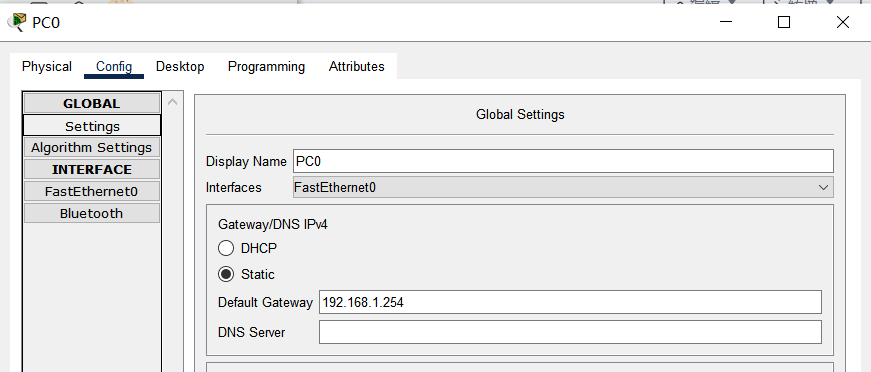
配置PC0的IP及网关：

IP：192.168.1.11

子网掩码：255.255.255.0

网关：192.168.1.254





下面两个PC配置方式与上面相同：

配置PC1的IP及网关：

IP：10.60.2.22

255.255.255.0

10.60.2.254

配置PC2的IP及网关：

172.16.3.33

255.255.255.0

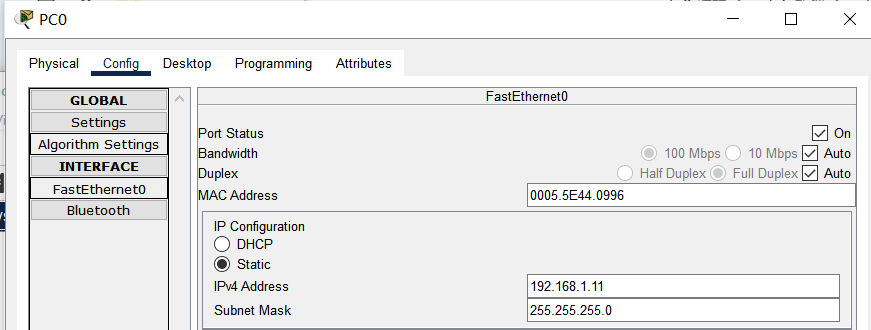
172.16.3.254

**（2）对Router进行配置**

配置Router0的f0/0端口IP及子网掩码

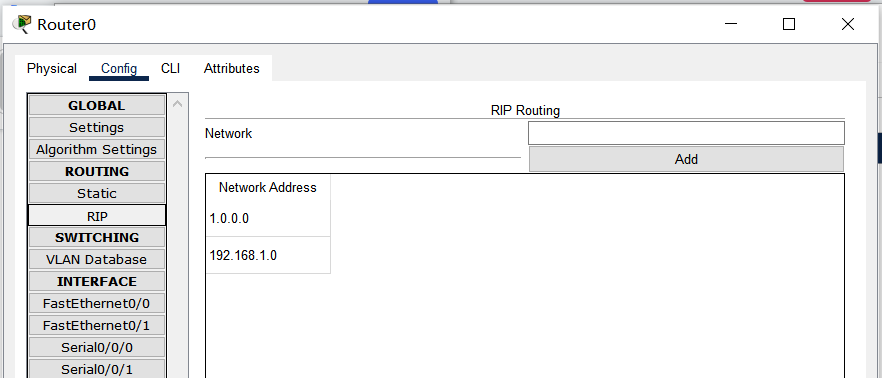
IP：192.168.1.254

子网掩码：255.255.255.0



配置Router0的RIP：

添加两个网络：1.0.0.0和192.168.1.0



下面两个Router配置方式与上面相同：

配置Router1的f0/0端口IP及子网掩码

IP：10.60.2.254

子网掩码：255.255.255.0

配置Router1的RIP：

添加两个网络：1.0.0.0和10.0.0.0

配置Router2的f0/0端口IP及子网掩码

IP：172.16.3.254

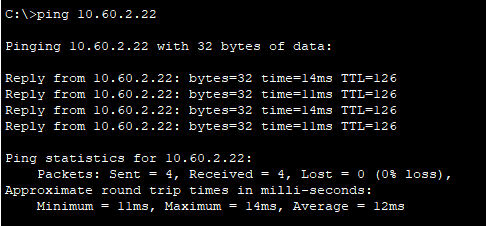
子网掩码：255.255.255.0

配置Router2的RIP：

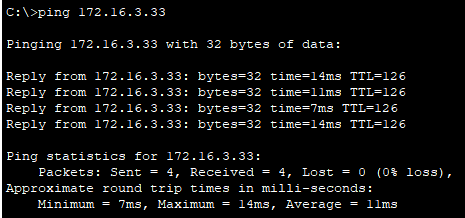
添加两个网络：1.0.0.0和172.16.0.0

1. **测试PC之间能否ping通**

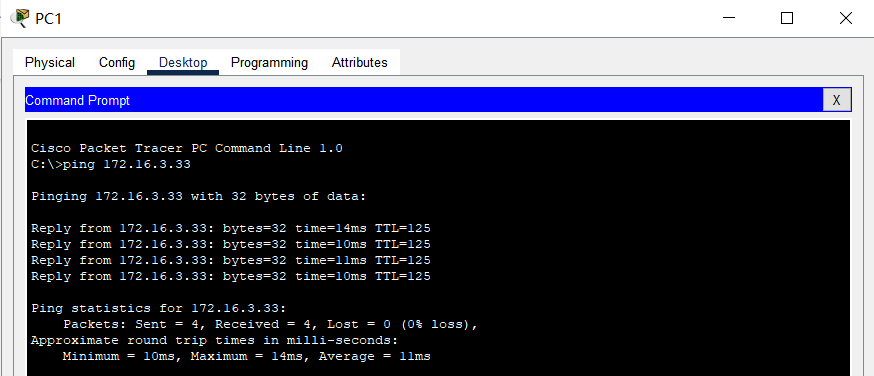
PC0 ping PC1



PC0 ping PC2



PC1 ping PC2



三台PC之间都能互相ping通

**【分析讨论】**

1.连线时的接口、串口选择

F0/0是快速以太网接口，用来连接交换机或电脑，Serial0/0是串行接口，路由器连接路由器要用路由器上的Serial端口连接。这里注意用直通线连接PC和路由器

2.PC的配置

在使用PC端测试连通性时遇到了较大麻烦，由于课件上并未说明所加PC的配置方法，因此在连好线，给PC配好IP、子网掩码和网关、给路由器对应接口配好IP和子网掩码之后尝试ping其他主机，发现ping失败。最后解决方法是，配置路由器的RIP。

RIP是一种基于距离向量的动态路由协议，它允许路由器动态地了解网络拓扑结构，并根据网络中其他路由器发送的更新信息选择最佳的路由。配置RIP就能让发送到f0/0端口的消息自动选择Serial0端口向外发送。

在配置RIP时，需要添加Serial端口和F0/0端口所在网络，将两个子网添加进去之后，到达路由器的数据包就可以正常对外转发了。

3.静态路由的配置

Router1的IP是1.1.1.2，Router2的IP是1.1.1.6，但是配置两个路由器的静态路由时，目标地址却是1.1.1.4和1.1.1.0，这点一开始没太仔细思考，后来发现是因为子网掩码是255.255.255.252，这样点分十进制转换为二进制表示，最后一组的最后两位是0，也就是说1.1.1.6地址就在1.1.1.4网络下，1.1.1.2就在1.1.1.0网络下。

4.硬件的配置

一开始按拓扑连接好后，路由器之间还是ping不通，后来发现是因为缺少了HWIC-2T模块，只有给路由器加上这个模块才能正常工作。采用的是2端口串行广域网接口卡，可以应用于CISCO 1800,2800,3800系列访问路由器，范围广泛，主要针对中小企业设计，在保证了高性能的同时，价格也非常合理。

**【实验名称】：ACL访问控制实验**

**学生姓名：陈嘉瑞 合作学生： 无**

**实验地点：济事楼330网络实验室 实验时间：2023年10月23日**

**【实验目的】**

包过滤机制是路由器基本处理机制，加入过滤规则，可以实施基本的网络安全控制。阻隔访问敏感网站和关键主机，均可以使用访问控制列表作为过滤规则实施。学习访问控制列表，不但可以了解基本网络安全知识，而且还可以提高路由器使用水平。本实验利用路由器的访问控制列表功能，使得特定的 IP 地址不能访问，实现网络安全管理任务。

1. 了解路由器包过滤基本原理。
2. 了解访问控制列表实施原理。
3. 利用控制列表实施网络安全。

**【实验原理】**

ACLs 的全称为接入控制列表(Access Control Lists)，也称为访问列表（Access Lists），俗称为防火墙，在有的文档中还称之为包过滤。ACLs 通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过或丢弃，从而提高网络可管理性和安全性；

IP ACL分为两种：标准IP访问列表和扩展IP访问列表，编号范围分别为1～99、1300～1999，100～199、2000～2699；标准IP访问列表可以根据数据包的源IP地址定义规则，进行数据包的过滤；扩展IP访问列表可以根据数据包的源IP、目的IP、源端口、目的端口、协议来定义规则，进行数据包的过滤；IP ACL 基于接口进行规则的应用，分为：入栈应用和出栈应用；

路由器包过滤机制是指路由器在转发IP数据包时，需要对每一个IP数据包头部进行分析，检查头部是否损坏并用于计算路由，为转发服务。

访问控制列表( Access Control Lists : ACL )，是指路由器在包过滤时，以IP数据包头部中的信息，诸如以源地址和目的地址等数据域作为规则条件，制订访问控制规则，只允许让满是条件的IP数据包通过，达到访问控制的目的，从而提高网络可管理性和安全性。

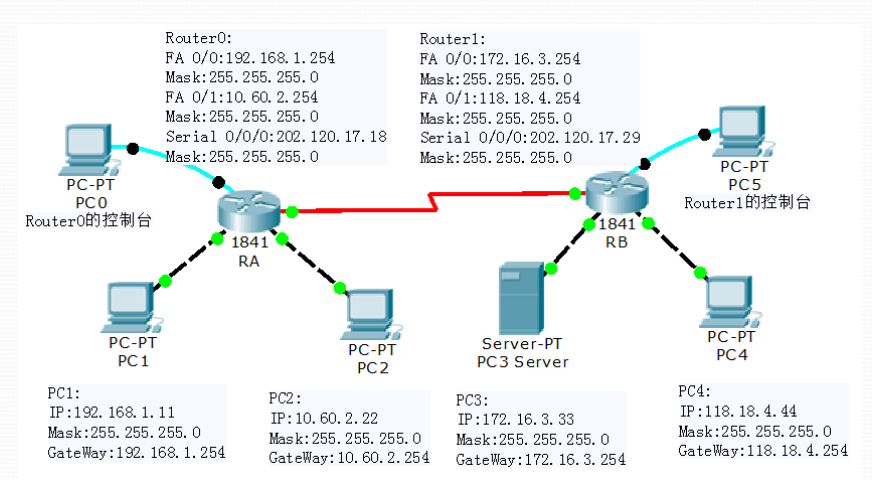
在工程应用中，可以设置规则不允许访问某些网站，比如禁止访问一些不健康网站；也可以对自身网络中某段地址进行保护，比如保护网站服务器。典型的 Web 应用，一般有 Web服务器和数据库两种服务器，Web服务器必须让外界直接访问，但数据库服务器就不应让外部直接访问，避免遭受攻击。通过访问控制列表，可以允许外部网能访问Web服务器地址，但不允许访问数据库服务器地址。

**【实验设备】**

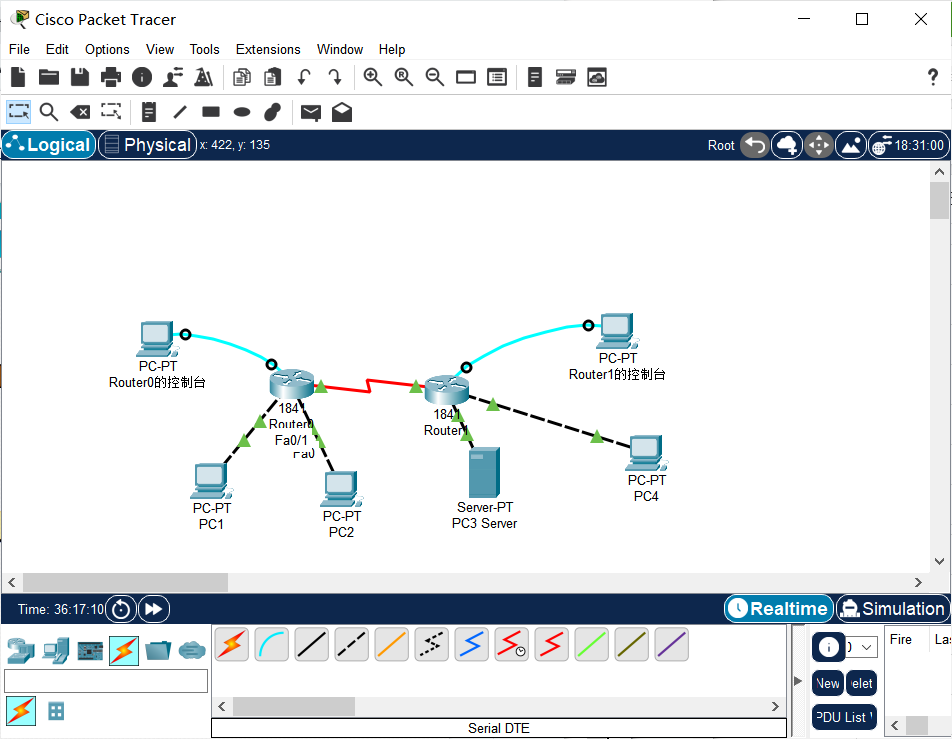
个人笔记本电脑、Cisco Packet Tracer实验软件。

**【实验步骤】**

1.首先规划网络地址及拓扑图，按下图进行设备连接；

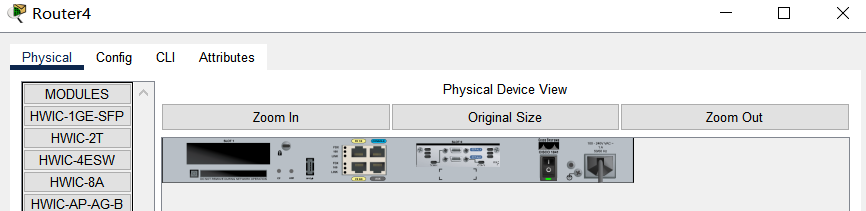


连接好后的网络拓扑图如下：



为路由器添加HWIC-2T模块：

先将路由器电源关闭，将左侧模块栏HWIC-2T模块拖动至右侧，再打开电源。

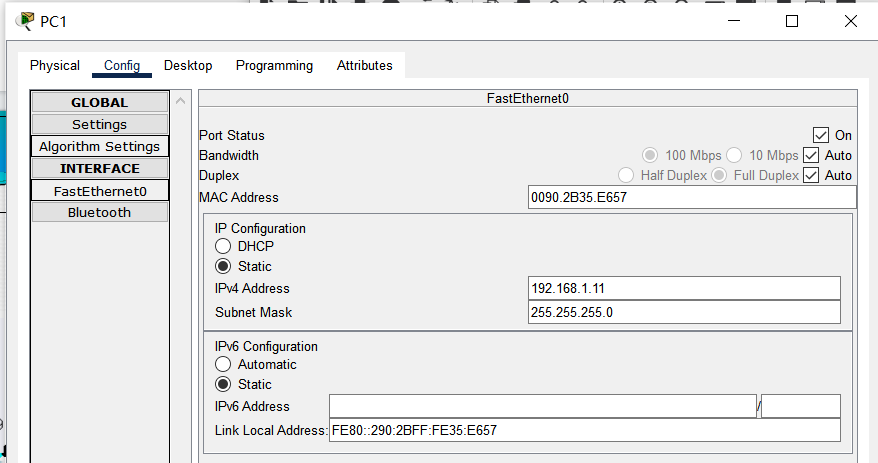


2.配置PC机、服务器及路由器口IP地址；

配置PC1的FastEthernet0端口：

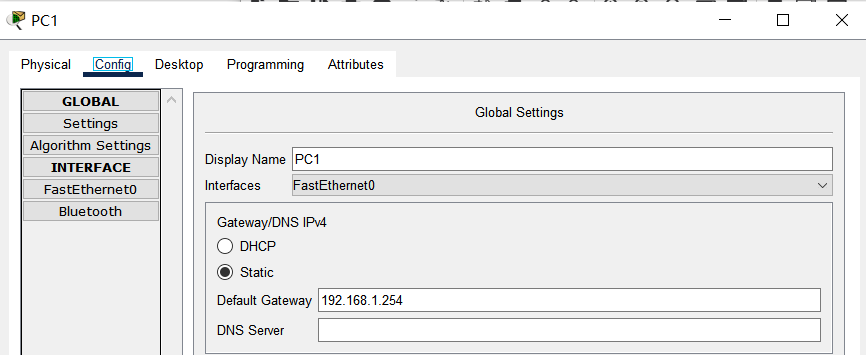
IP地址：192.168.1.11

子网掩码：255.255.255.0



配置PC1网关：

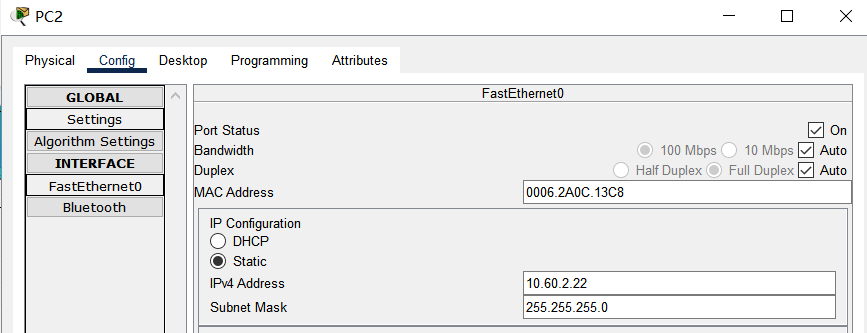
网关：192.168.1.254



配置PC2的FastEthernet0端口：

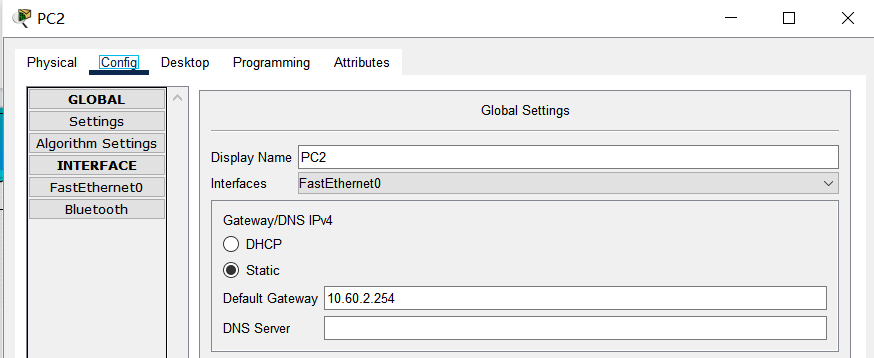
IP地址：10.60.2.22

子网掩码：255.255.255.0



配置PC2网关：

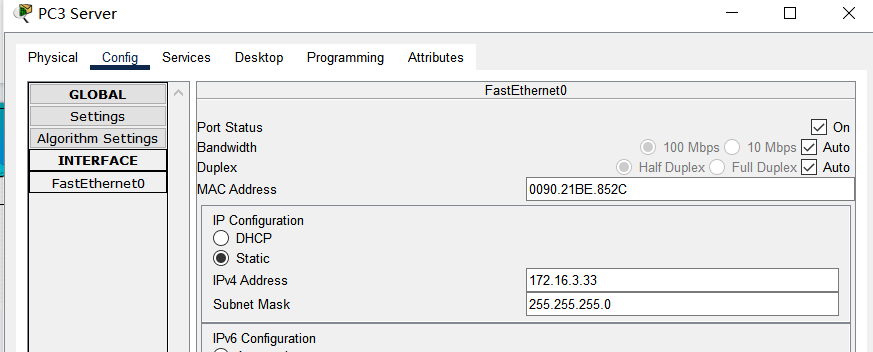
网关：10.60.2.254



配置PC3 server的FastEthernet0端口：

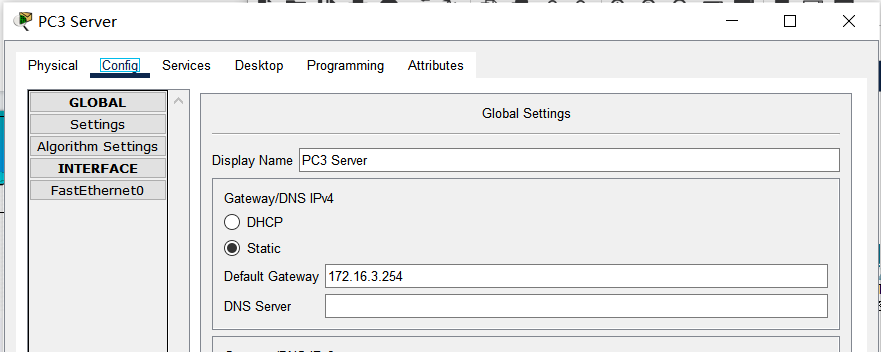
IP地址：172.16.3.33

子网掩码：255.255.255.0



配置PC3 server网关：

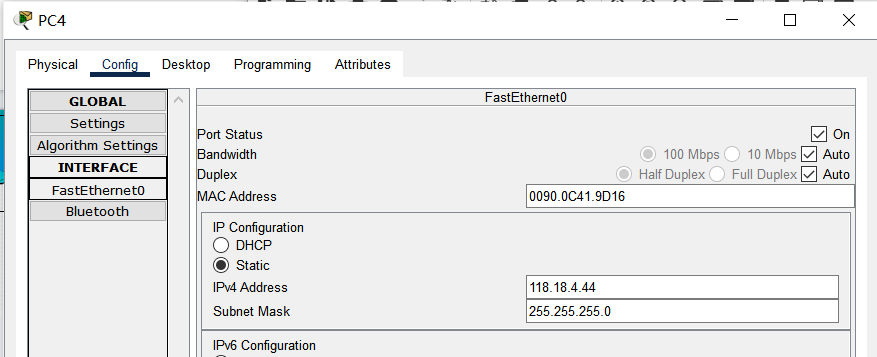
网关：172.16.3.254



配置PC4的FastEthernet0端口：

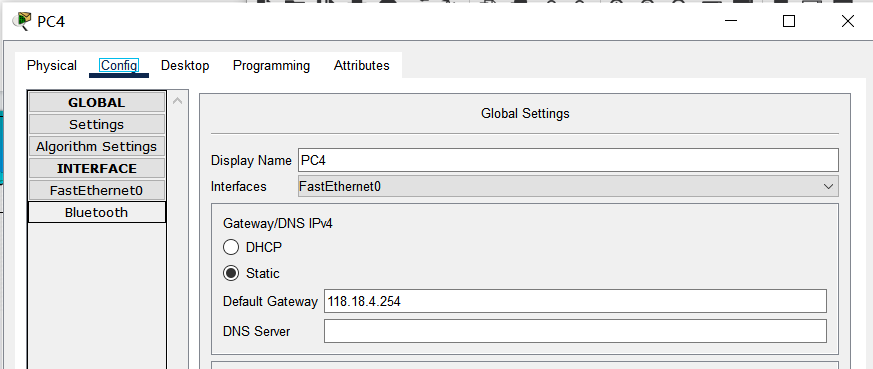
IP地址：118.18.4.44

子网掩码：255.255.255.0



配置PC4网关：

网关：118.18.4.254

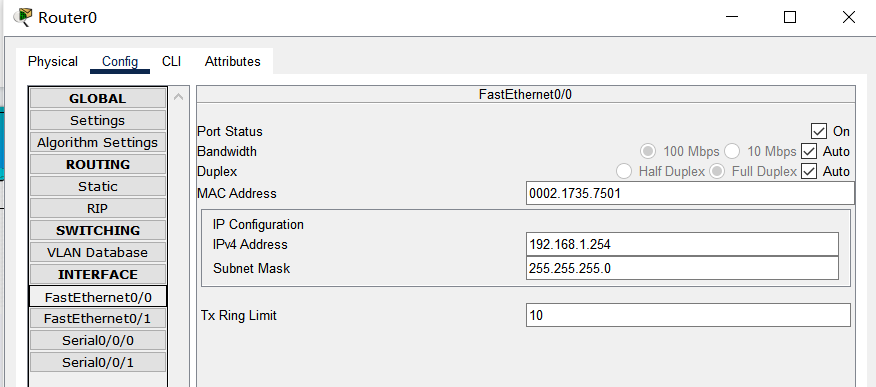


3.配置路由器的端口地址；

配置Router0的f0/0端口：

IP：192.168.1.254

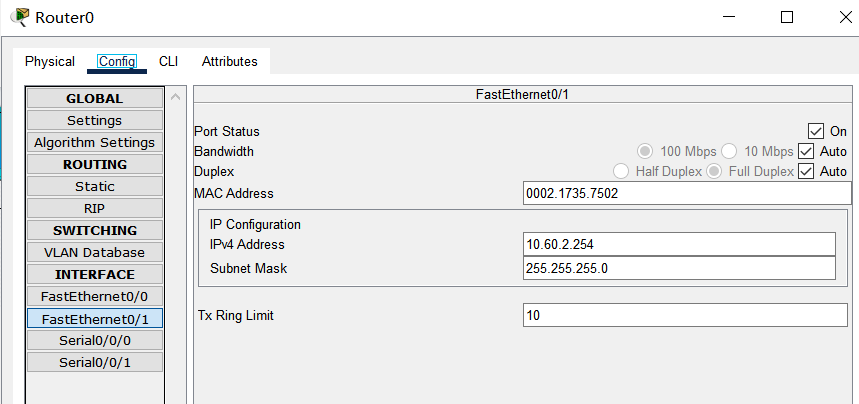
子网掩码：255.255.255.0



配置Router0的f0/1端口：

IP：10.60.2.254

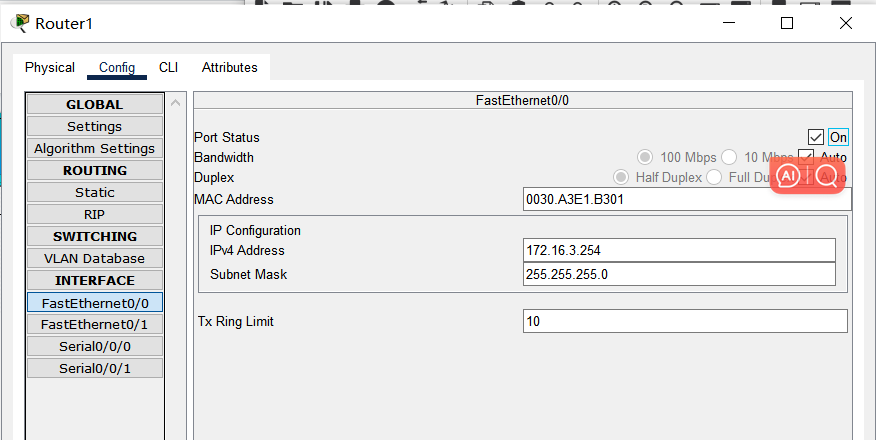
子网掩码：255.255.255.0



配置Router1的f0/0端口：

IP：172.16.3.254

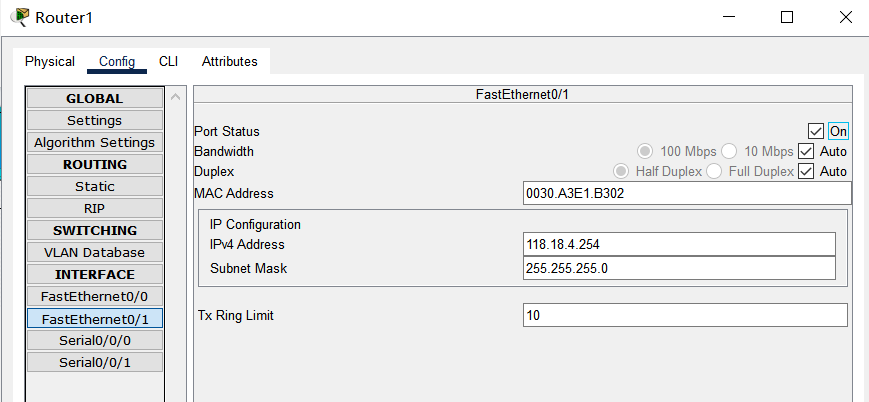
子网掩码：255.255.255.0



配置Router1的f0/1端口：

IP：118.18.4.254

子网掩码：255.255.255.0



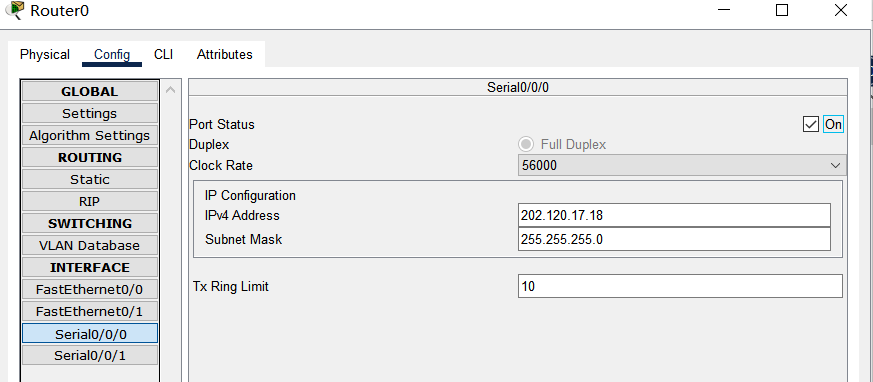
4.配置路由器的串口端口地址；

配置Router0的串口端口：

IP:202.120.17.18

子网掩码：255.255.255.0

Clock Rate:56000

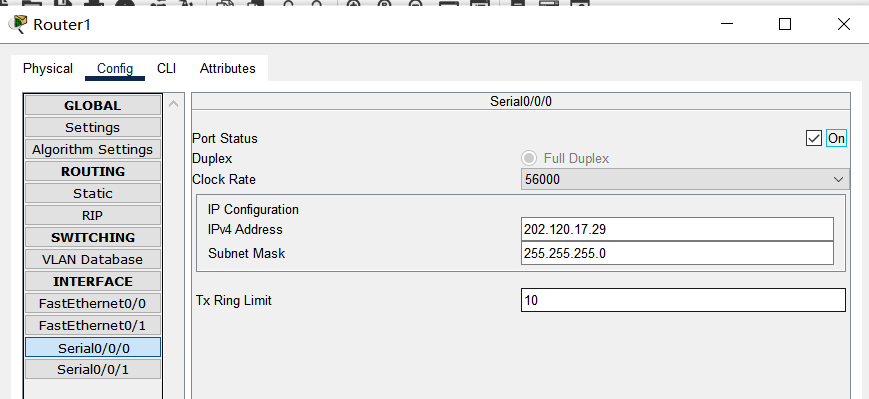


配置Router1的串口端口：

IP:202.120.17.29

子网掩码：255.255.255.0

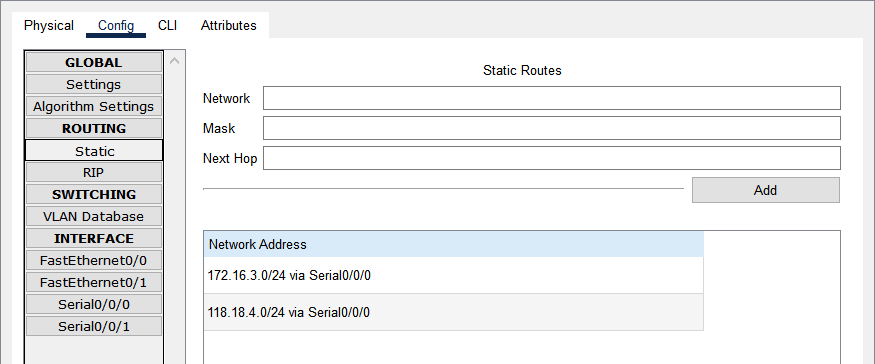
Clock Rate:56000



5.配置路由器的静态路由表

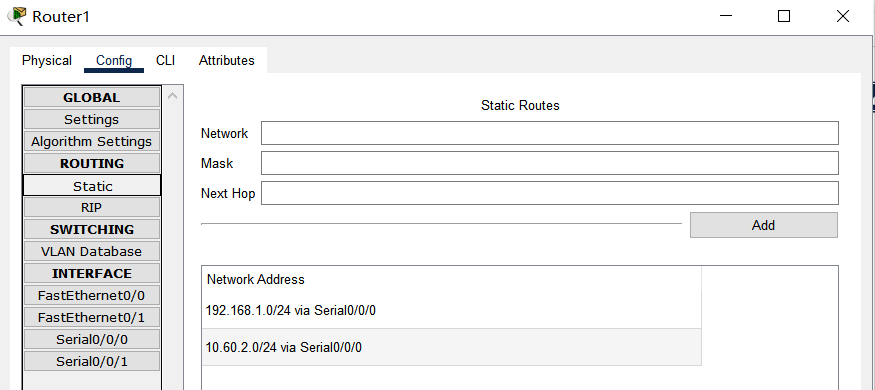
配置Router0静态路由：

router0静态路由



配置Router1静态路由：

router1静态路由



4.PC1 PC2 PC3server PC4互相ping进行测试

5.在RB上配置ACL；

在Router1上配置，拒绝来自PC1的ping，允许PC1通过tcp访问PC3 server

键入以下命令：

a.拒绝ping包：

access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33

b.允许www访问：

access-list 101 permit tcp host 192.168.1.11 host 172.16.3.33 eq www

6.在RB接口上应用ACL；

将ACL应用到端口：

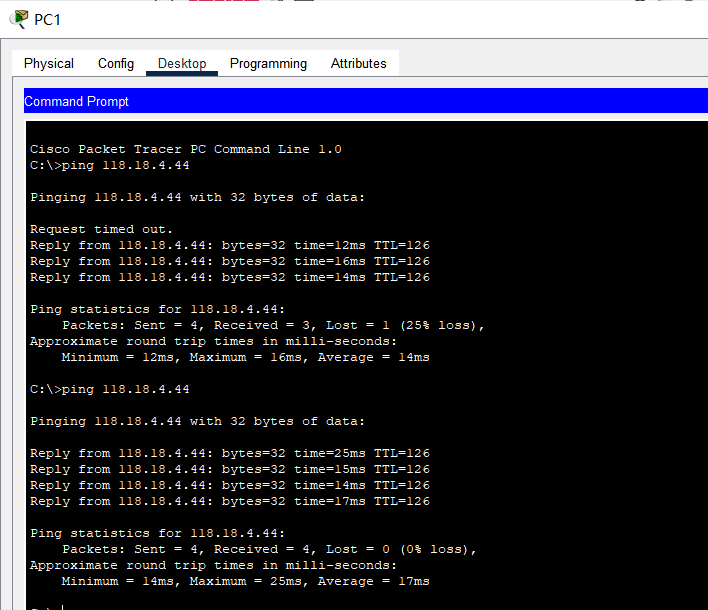
ACL引用到端口

7.验证主机之间的互通性及WWW访问。

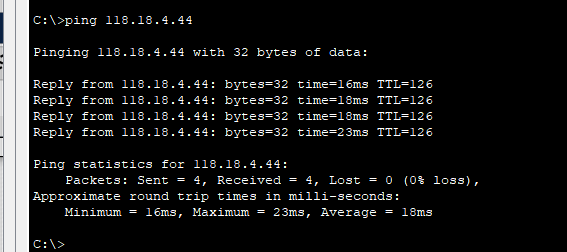
**【实验现象】**

（1）在配置ACL前PC之间互相ping：

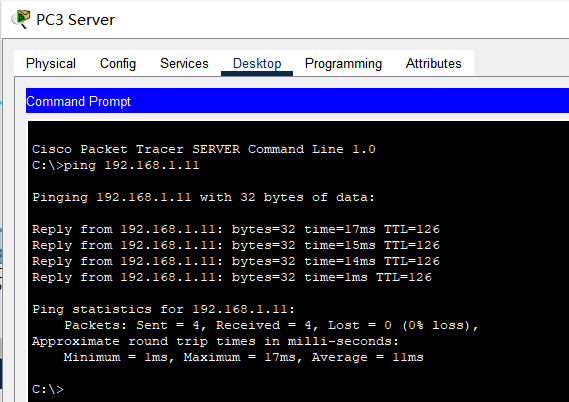
PC1 ping PC4

****

PC2 ping PC4

****

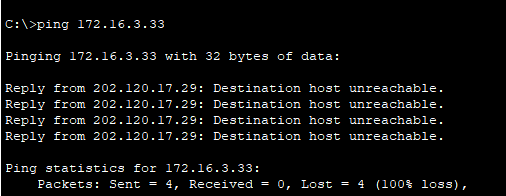
PC3 ping PC1

****

可以看出，在配置ACL前，PC之间可以互相ping通

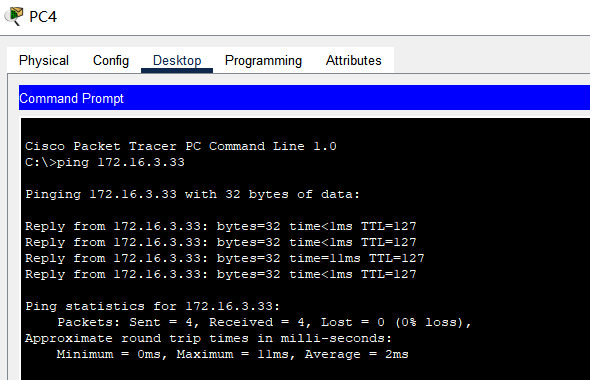
（2）在配置ACL之后PC之间互相ping：

PC1 ping PC3

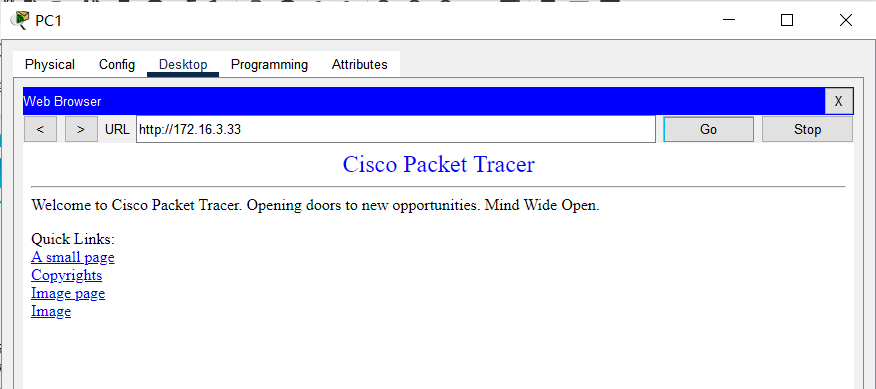
****

此时PC1无法ping通PC3

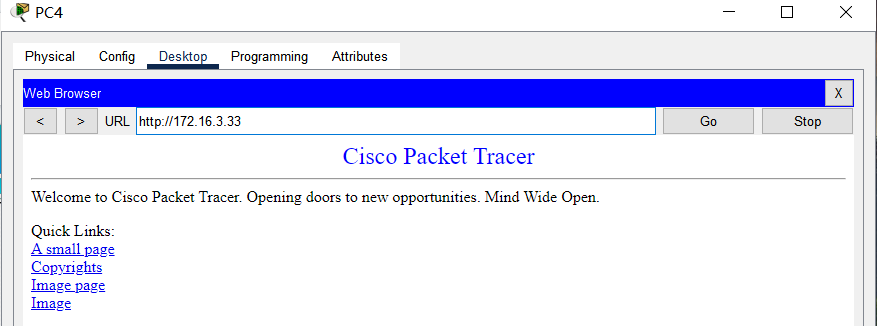
PC4 ping PC3

****

PC1 http 访问PC3

****

PC4 http 访问PC3

****

可以看出，由于Router1禁止了PC1与PC3 server之间的ping请求，所以PC1与PC3之间ping测试失败，而由于配置了允许PC1通过tcp方式访问PC3 server，因此我们可以通过在网址栏以http方式访问PC3服务器。其他PC由于没有设置禁止访问，因此还可以正常访问PC3 server

**【分析讨论】**

1. 有一个现象，当两台PC之间配置好后第一次ping时，第一个数据包会丢失，如果之后再重新发起ping请求，就不会出现这个问题。下面以R1、R2为例解释：R2尝试给R1发出第一个ICMP报文时，由于没有R1的MAC地址，这第一个报文其实并没有封装完成，卡在数据链路层就没了，所以第一个报文其实已经“胎死腹中”，而同时会发出ARP报文去获取R1的MAC地址，后续的4个报文由于收到ARP回应已经有了R1的MAC地址，可以直接封装发出，于是就通了。
2. 包过滤机制是路由器基本处理机制，加入过滤规则，可以实施基本的网络安全控制。阻隔访问敏感网站和关键主机，均可以使用访问控制列表作为过滤规则实施。通过本实验，我学习了访问控制列表，了解了基本网络安全知识，也提高了路由器使用水平。本实验利用路由器的访问控制列表功能，使得特定的 IP 地址不能访问，实现网络安全管理任务。
3. 注意，本实验也需要为路由器添加HWIC-2T模块才能连接两台路由器，否则没有对应接口，无法连通。