**实验14\_NAT网络地址转换**

**学生姓名:林觉凯 合作同学:无**

**实验地点:济事楼330 实验时间:2024.4.8**

【**实验目的**】

NAT，网络地址转换(Network Address Translation)是一种网络技术，用于将私有网络内部的IP地址转换为公共网络上的可路由的IP地址，以便在互联网上进行通信。本实验通过对网络地址的转换，让我们了解并掌握NAT的概念和作用，理解静态NAT的配置和管理方法，掌握相关的网络地址转换技术，从而进一步了解内网和公网的区别。

【**实验原理**】

技术原理：

网络地址转换NAT (Network Address Translation) ，被广泛应用于各种类型Internet接入方式和各种类型的网络中。原因很简单，NAT不仅完美地解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

默认情况下，内部IP地址是无法被路由到外网的，内部主机要与外部网络或internet通信，IP包到达NAT路由器时，IP包头的源地址被替换成一个合法的外网IP，并在NAT转换表中保存这条记录。

当外部主机发送一个应答到内网时，NAT路由器收到后，查看当前NAT转换表，用内网地址替换掉这个外网地址。

NAT将网络划分为内部网络和外部网络两部分，局域网主机利用NAT访问网络时，是将局域网内部的本地地址转换为全局地址(外部网络或互联网合法的IP地址后转发数据包；

NAT分为两种类型：NAT(网络地址转换)和NAPT(网络端口地址转换IP地址对应一个全局地址)。

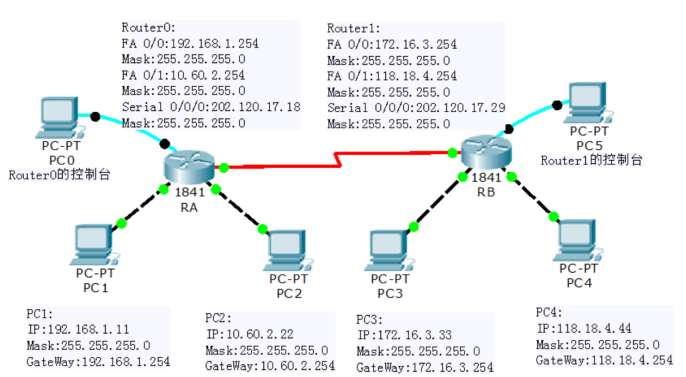
 静态NAT：实现内部地址与外部地址一对一的映射。现实中，一般都用于服务器；动态NAT：定义一个地址池，自动映射，也是一对多的。现实中，用得比较少；NAPT：使用不同的端口来映射多个内网IP地址到一个指定的外网IP地址，多对一。

【**实验设备**】

硬件设备：济事楼330机房电脑

软件设备：Windows操作系统和Cisco Packet Tracer网络仿真软件

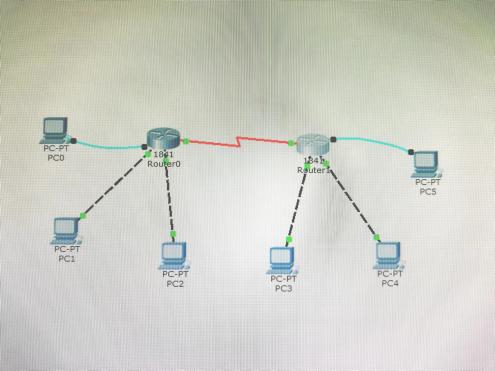
【**实验步骤**】

1.首先规划网络地址及拓扑图(如右图)；

2.配置PC机、服务器及路由器口IP地址；

3.在各路由器上配置静态路由协议，让pc间能相互ping通；

4.在路由器上配置静态NAT；

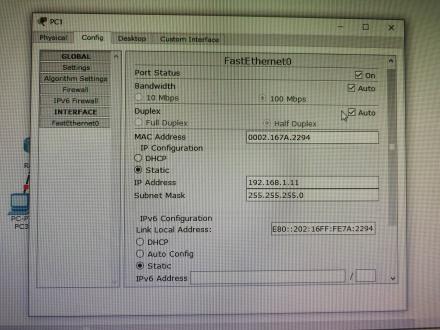
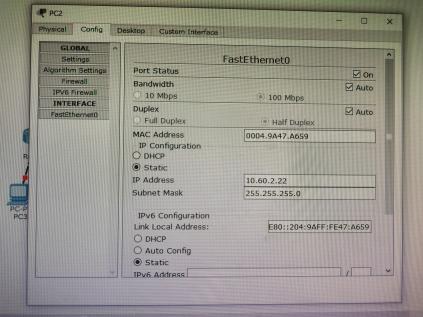
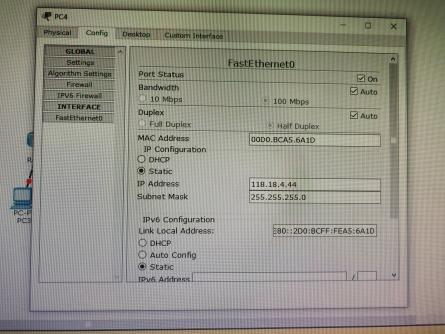
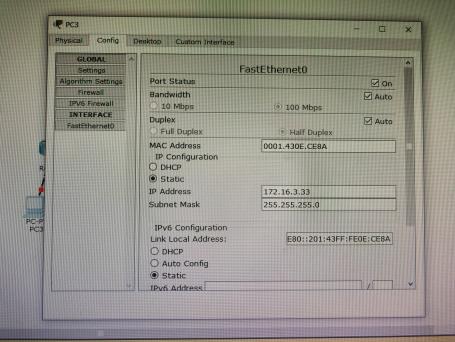
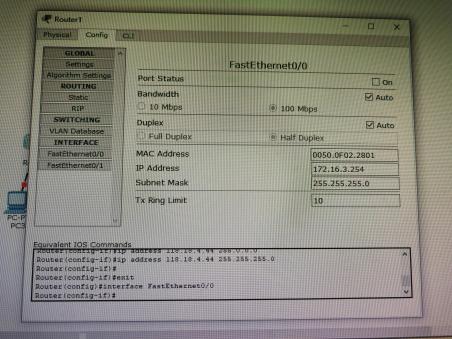
5.在路由器上定义内外部网络接口；

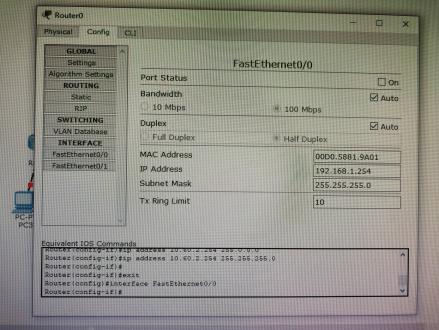
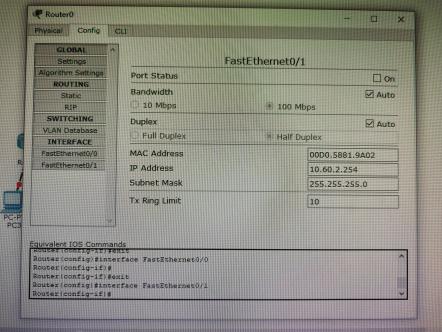
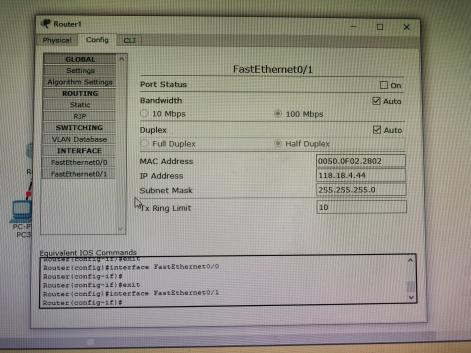
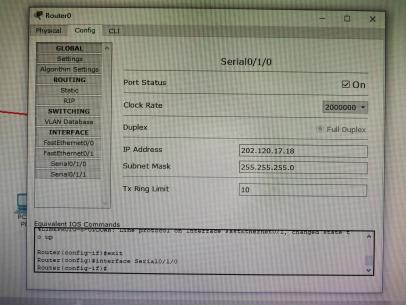
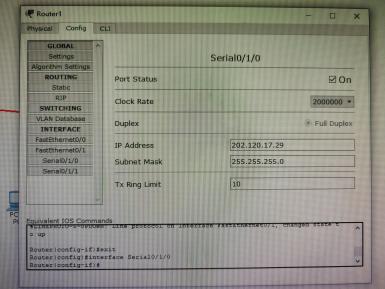
6.验证主机之间的互通性。

【**实验现象**】

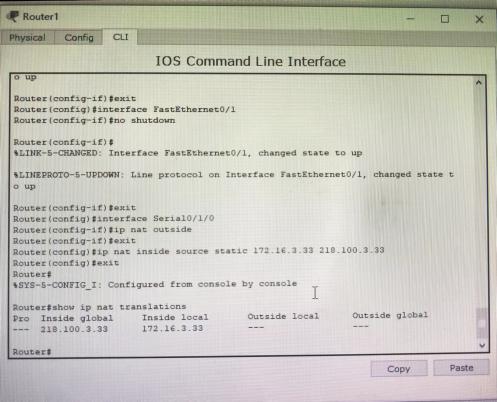
首先按照实验的要求完成拓扑图的连接。

配置相应位置的IP地址和网关内容。

配置PC1,PC2,PC3,PC4对应的IP地址、子网掩码和网关



配置Router0和Router1相关参数

配置路由器A的NAT的出入口：

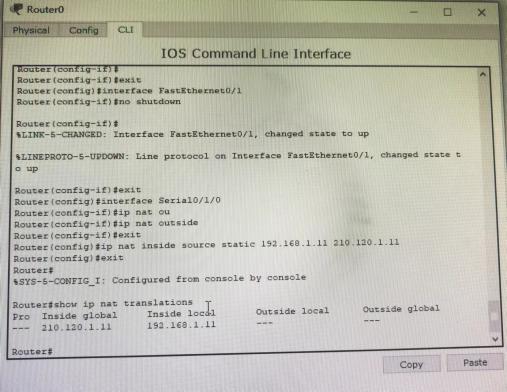
路由器A：

interface FastEthernet0/0

ip natinside

interface Serial 0/1/0

ip natoutside

路由器B：

interface FastEthernet0/0

ip natinside

interface Serial 0/1/0

ip natoutside

配置路由器的NAT转换:

 路由器A（在全局配置模式下配置NAT地址转换）

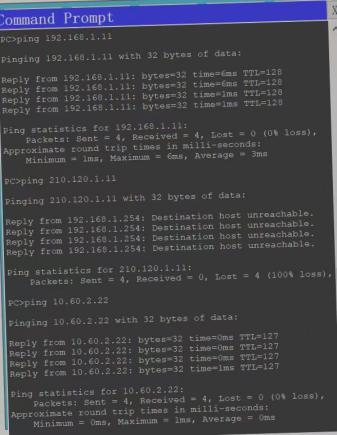
 ip nat inside source static 192.168.1.11210.120.1.11

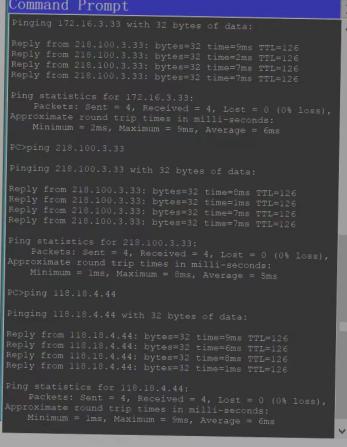
 路由器B（在全局配置模式下配置NAT地址转换）

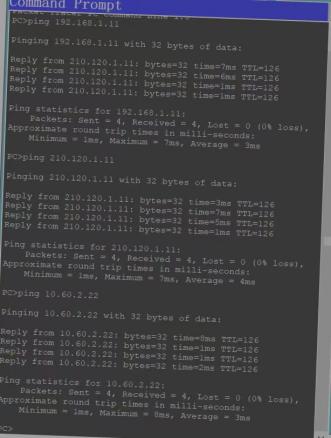
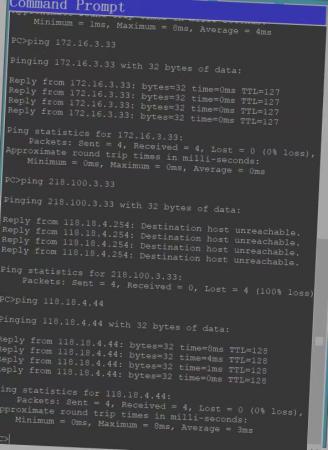
 ip nat inside source static 172.16.3.33218.100.3.33

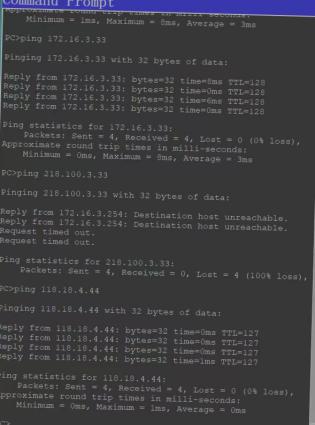
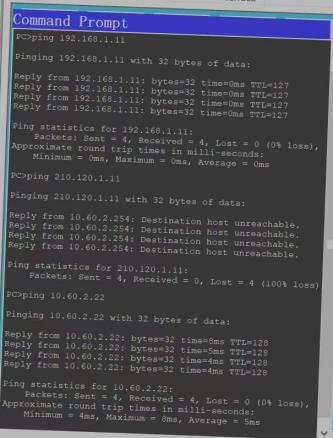
在各自PC端访问，观察现象：

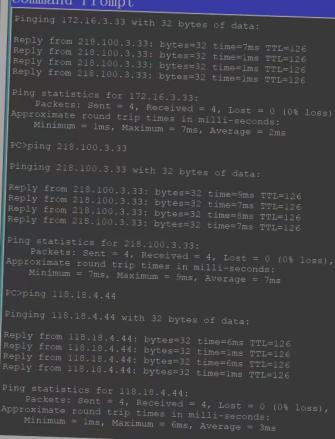
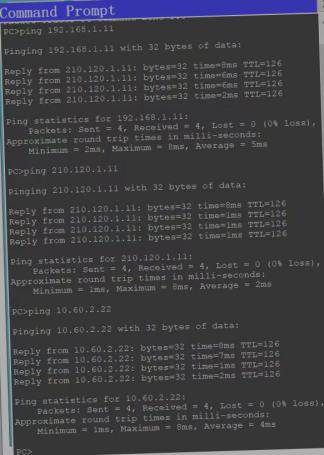
 ping 192.168.1.11 ping 210.120.1.11 ping 10.60.2.22

 ping 172.16.3.33 Ping 218.100.3.33 Ping 118.18.4.44









【**分析讨论**】

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 192.168.1.11 | 210.120.1.11 | 10.60.2.22 | 172.16.3.33 | 218.100.3.33 | 118.18.4.44 |
| PC1 | 通 | 不通 | 通 | 不通 | 通 | 通 |
| PC2 | 通 | 不通 | 通 | 不通 | 通 | 通 |
| PC3 | 不通 | 通 | 通 | 通 | 不通 | 通 |
| PC4 | 不通 | 通 | 通 | 通 | 不通 | 通 |

以上为具体ping操作的结果，我们可以发现，在同一路由器的局域网内，我们是无法ping通公网地址的，但是我们可以ping通内网的地址；在不同路由器的局域网内，我们是无法ping通内网地址的，但是可以ping通公网的地址。这是我们通过本次实验得出的结果。

192.168.1.11，对于PC1/2，ping自身收到回复；对于PC3/4，数据到达路由器B之后被截断，所以并没有到达PC3/4所在的位置。

210.120.1.11，PC1/2发送的数据包没有进入路由器就被返回，所以发送的数据包没有得到有效的回复。

10.60.2.22，PC1/2和该机器连接在同一台路由器，所以ping成功。通过两台路由器之间的连接，经过NAT的转换，也可以在PC3/4成功访问。

172.16.3.33，对应路由器2内部访问接口，PC1/2无法访问，PC34成功发送。

218.100.3.33，是路由器2的内部，PC1/2可以访问。

118.18.4.44是PC4IP地址，PC3访问成功。PC1/2也可以访问到。

此外，对于NAT在计算机网络中的具体应用，我课外查找其中包括：

家庭网络：在家庭网络中，通常使用路由器来实现NAT。当多个设备连接到同一个路由器时，路由器将分配给这些设备的私有IP地址转换为公共IP地址，以便它们可以与互联网通信。这样，家庭网络中的多个设备可以共享一个公共IP地址，从而减少了对IP地址的需求，并提高了网络的安全性。

企业网络：在企业网络中，NAT常用于将企业内部网络的私有IP地址转换为企业所拥有的少量公共IP地址。这样，内部网络中的设备可以通过单个或少量公共IP地址访问互联网，而不需要为每个设备都分配独立的公共IP地址。

虚拟专用网络(VPN)：在VPN中，NAT用于隐藏VPN客户端的真实IP地址。VPN服务器会将客户端的私有IP地址转换为VPN服务器的公共IP地址，以确保客户端的真实IP地址不会暴露给其他VPN用户或互联网。

安全性增强：NAT可以作为一种安全机制，因为它隐藏了内部网络的真实IP地址，使得外部网络无法直接访问内部网络中的设备。这种隐藏可以减少来自互联网的恶意攻击和未经授权的访问。

IPv4地址短缺问题：随着IPv4地址的短缺，NAT成为一种应对策略。通过NAT，一个公共IP地址可以映射到多个私有IP地址，从而延长了IPv4地址的可用寿命。

**实验15\_帧中继配置实验**

**学生姓名:林觉凯 合作同学:无**

**实验地点:济事楼330 实验时间:2024.4.8**

【**实验目的**】

帧中继是一种广泛用于广域网的数据传输技术。它在传输层使用数据链路层的帧来传输数据。通过本次帧中继配置实验，可以让我们了解帧中继的网络的基本概念和原理，并且通过实践的配置帧中继网络中的地址映射表，理解在帧中继网络中的帧转发过程，同时也可以通过发送数据包并观察帧中继网络的转发行为，检验地址映射和帧转发的正确性。了解帧中继在网络通信中的重要作用

【**实验原理**】

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。

帧中继连接运行在虚电路(VC)上，每条虚电路都由一个数据链路标识符DLCI标识，后者被映射到一个IP地址。

PVC：永久虚电路，是永久性连接，建立后可直接使用，无需再建立。

SVC：交换虚电路，是暂时的。Cisco IOS11.2以后版本中支持SVC.

LMI协议类型：ITU-T的Q.933附录A。ANSI的T1.617附录D。非标准兼容类型，如CISCO等。

Frame-Relay通过为每一对DTE设备分配一个数据链连接标识符DLCI。

并且用DLCI将每对Router关联起来，在路由器（CPE）和Frame-Relay交换机之间生成一条逻辑虚拟链路PVC。PVC实现多个虚拟电路在同一个物理链路上进行多路复用。

在网络服务提供商的交换设备中，为将连接标识符映射到输出端口而构建了一张表。当收到一个Frame时，交换设备分析DLCI，并将这个Frame转发到预先建立好的与其相关联的输出端口在Cisco Router上，地址映射MAP可以是手动配置的，也可以采用动态地址映射。使用动态地址映射时，根据给定的DLCI号码，Frame-Relay地址解析协议（ARP）为某一具体连接找出下一跳协议地址。Frame-Relay ARP也被认为是反向ARP。然后Router会更新它的映射列表，并使用该表中的信息将数据包转发到正确的路由。如果DLCI在该链路上被定义了，交换机将Frame转发到目的地。如果DLCI在该链上没有被定义，交换机则会丢弃该Frame。

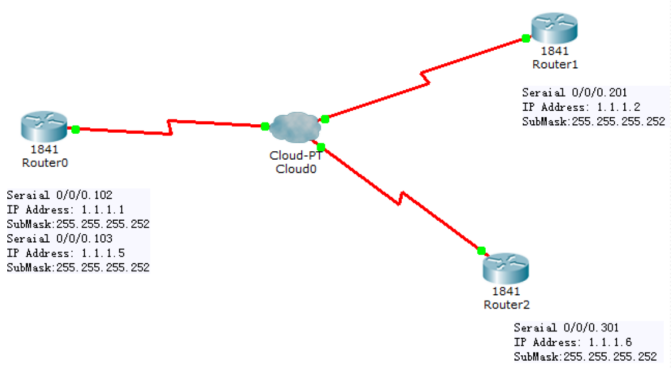
在封装接口时候Cisco是默认值，一般用于与另一个Cisco Router连接时。如果要与另一个非CiscoRouter连接，则应使用任选项“IETF”。

【**实验设备**】

硬件设备：济事楼330机房电脑

软件设备：Windows操作系统和Cisco Packet Tracer网络仿真软件

【**实验步骤**】

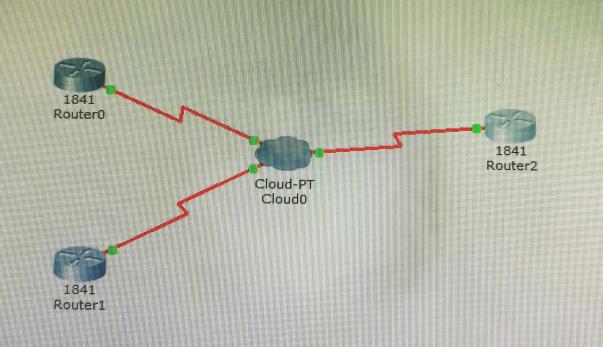
1.首先规划网络地址及拓扑图(如右图)；

2.接口IP地址配置；

3.配置Frame Relay之前检查接口间能否相互ping通；

4.在R0，R1，R2 配置 Frame Relay；

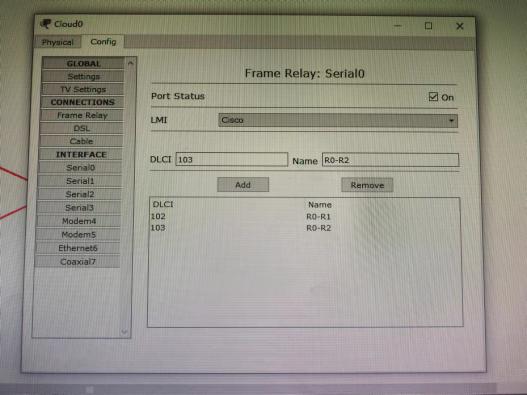
5.在R1 R2配置静态路由；

6.验证接口之间的互通性。

【**实验现象**】

首先按照实验的要求完成拓扑图的连接。

接下来配置路由器和交换机：

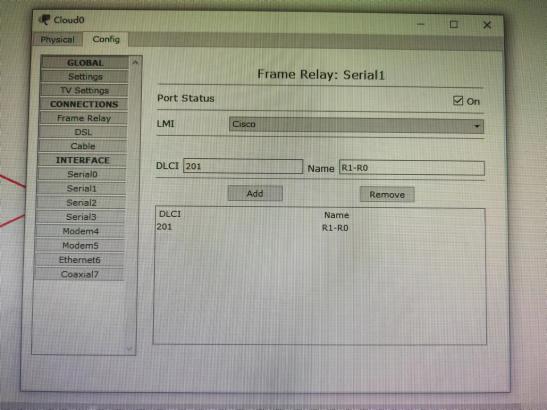
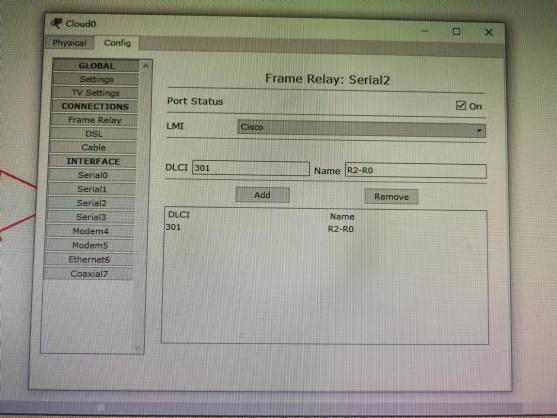
Serial0

DLCI Name

102 R0-R1

103 R0-R2

Serial1

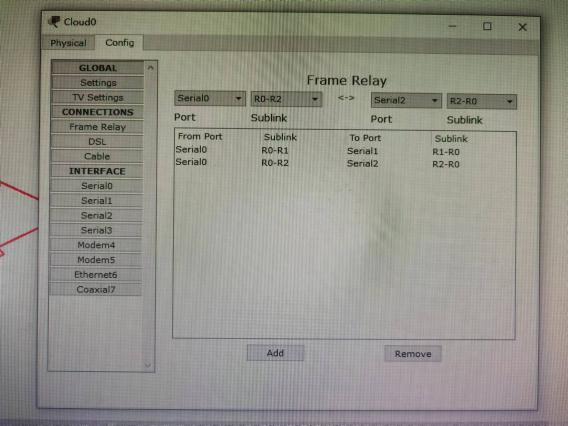
DLCI Name

201 R1-R0

Serial2

DLCI Name

301 R2-R0

From Port Sublink To Port Sublink

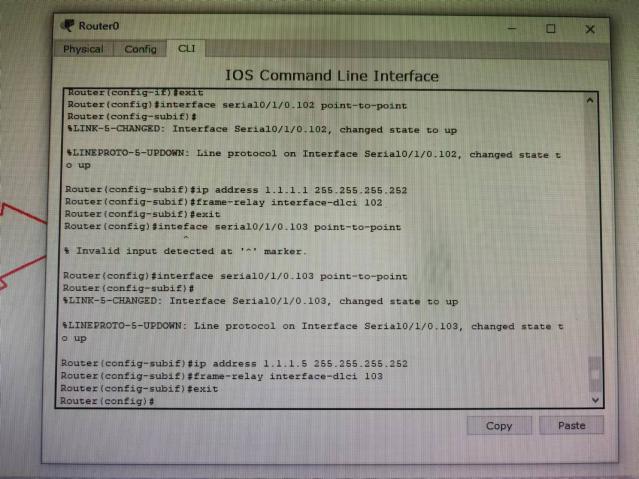
Serial0 R0-R1

Serial1 R1-R0

Serial0 R0-R2

Serial2 R2-R0

接着，我们需要在路由器中配置，一共配置三个路由器：

路由器R0配置

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

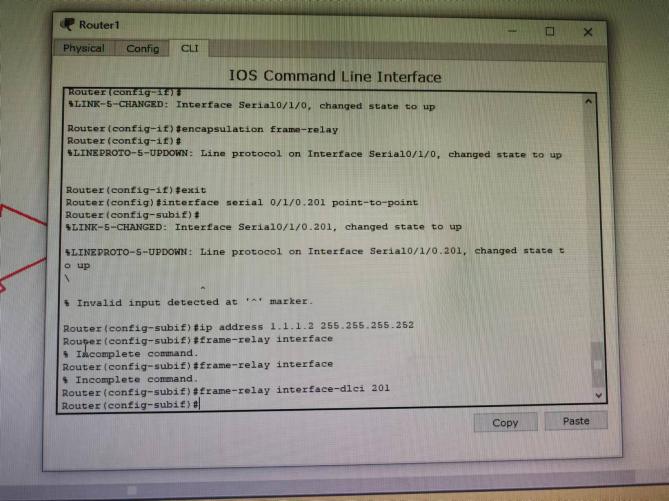
R0(config-subif)#frame-relay interface-dlci 102

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

路由器R1配置

R1>enable

R1#configure terminal

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

R1(config-if)#no shutdown

R1(config-if)#encapsulation frame-relay

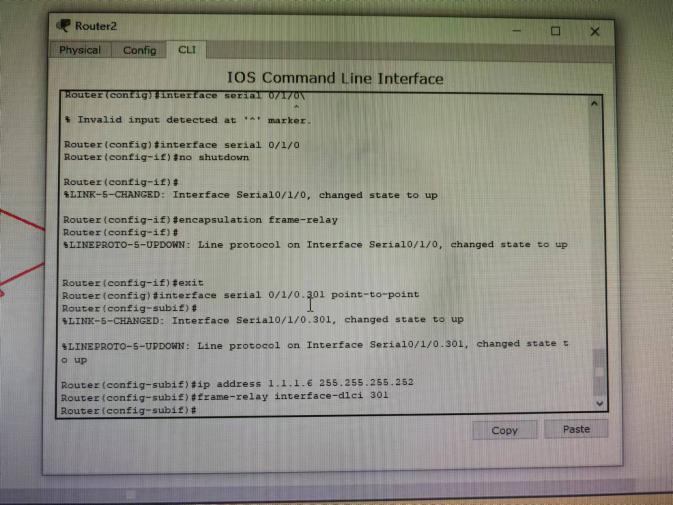
R1(config-if)#exit

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

路由器R2配置

R2>enable

R2#configure terminal

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

R2(config-if)#no shutdown

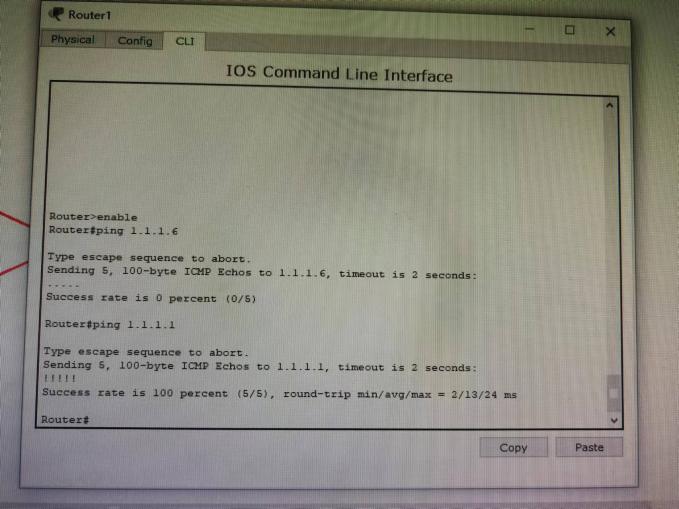
R2(config-if)#encapsulation frame-relay

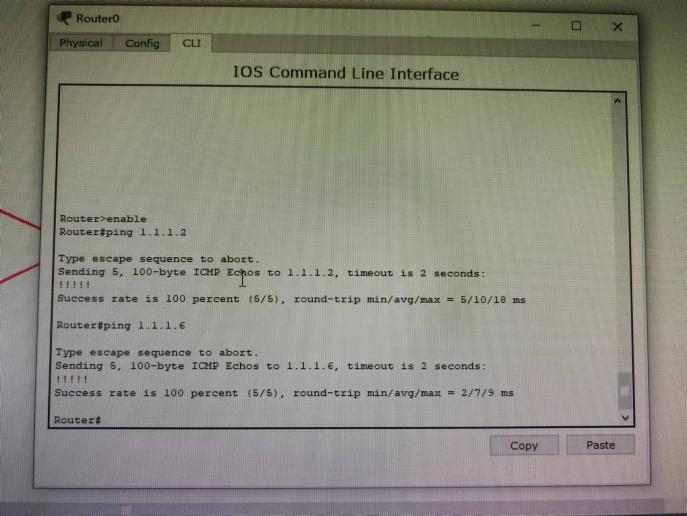
R2(config-if)#exit

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

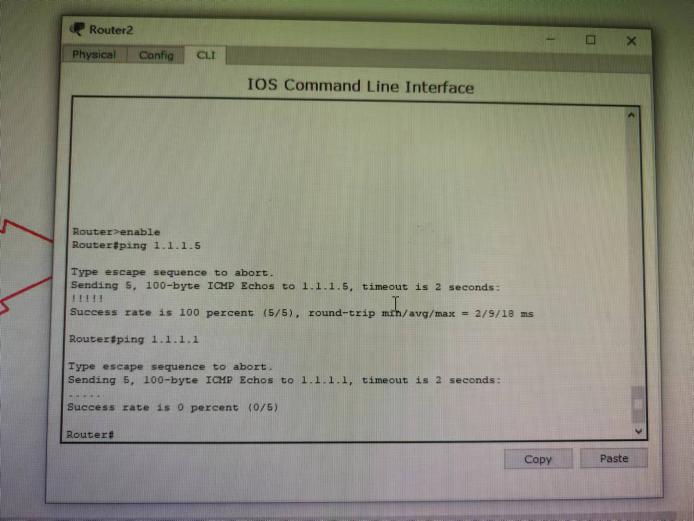
R2(config-subif)#ip address 1.1.1.6 255.255.255.252

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

接下来，我们分别对Router0、Router1和Router2进行ping操作，观察哪两个路由器之间可以被ping通。即R0，R1和R2互相ping ，测试通否？(在R1和R2配置路由前后的各自情况下)



Router0 ping Router1和Router2均成功。 Router1 ping Router0成功，

Router1 ping Router2失败。

Router2 ping Router0成功，

Router2 ping Router1失败。

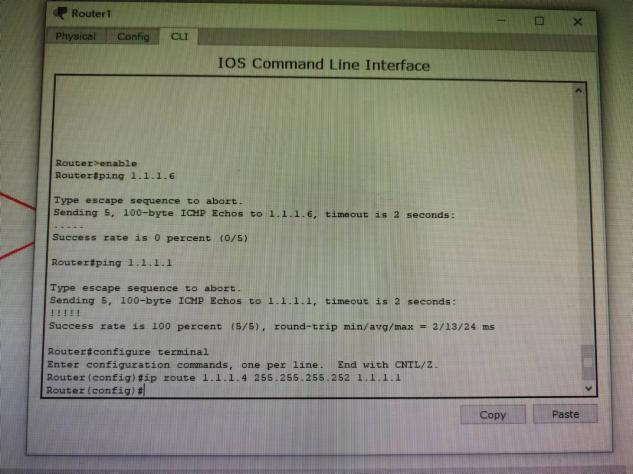
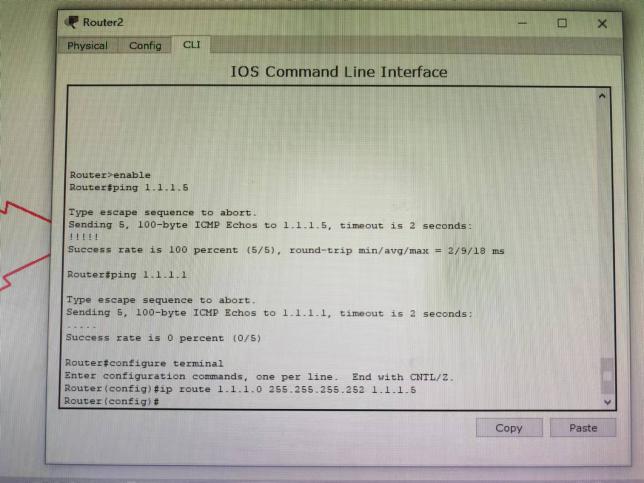
在Router1和Router2配置静态路由之后，发现二者可以互相ping成功。

Router1：

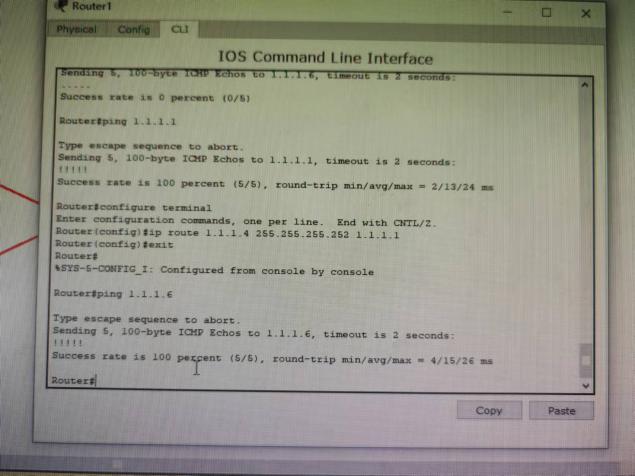
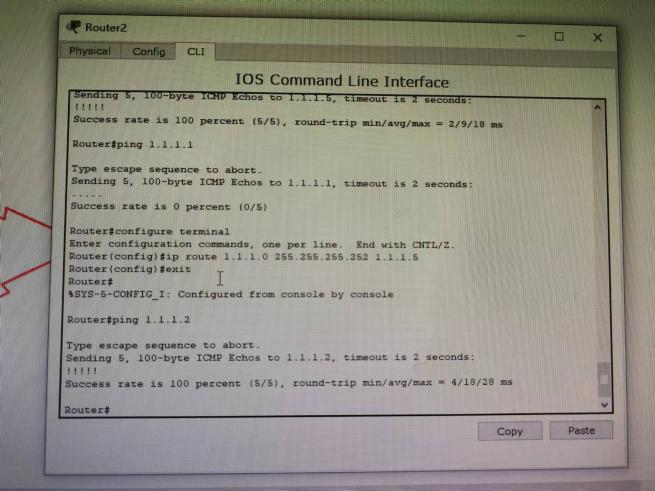
R1(config)#ip route 1.1.1.4 255.255.255.252 1.1.1.1

Router2：

R2(config)#ip route 1.1.1.0 255.255.255.252 1.1.1.5

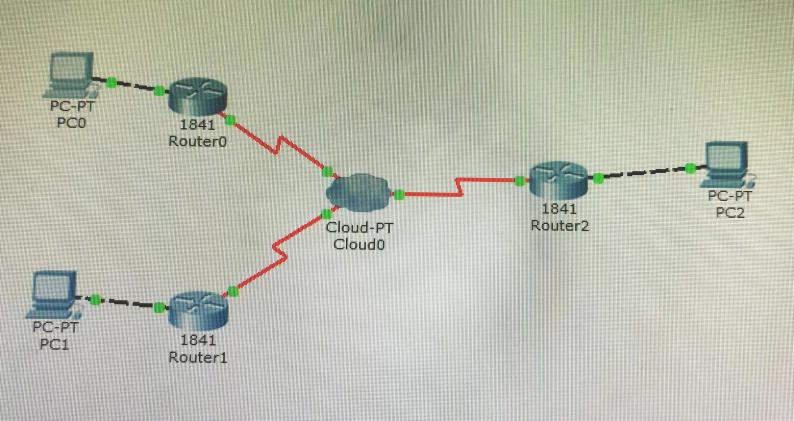


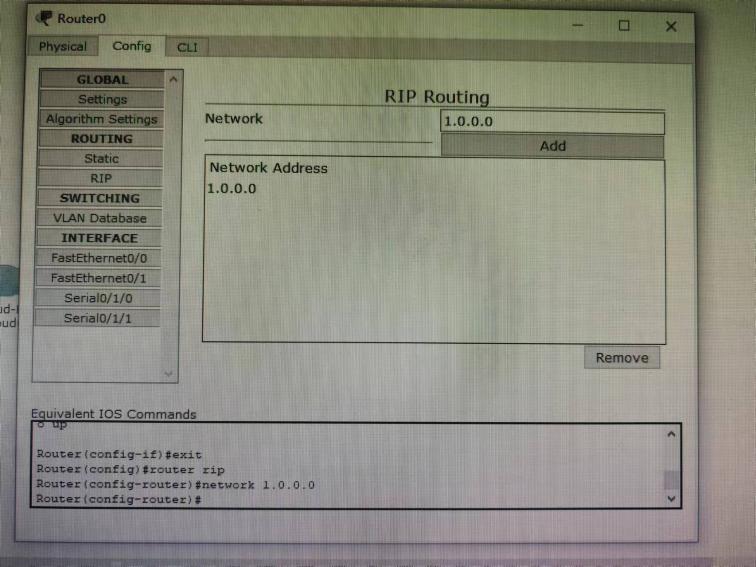
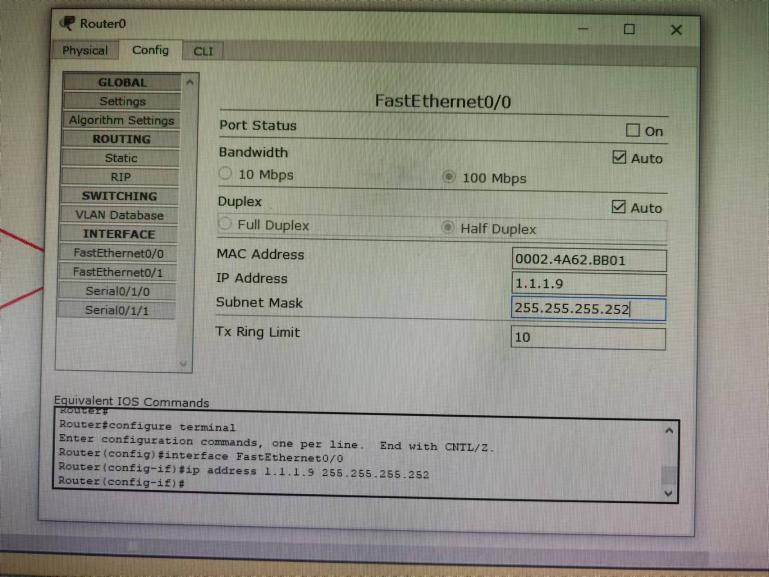
为Router1和Router2分别配置静态路由

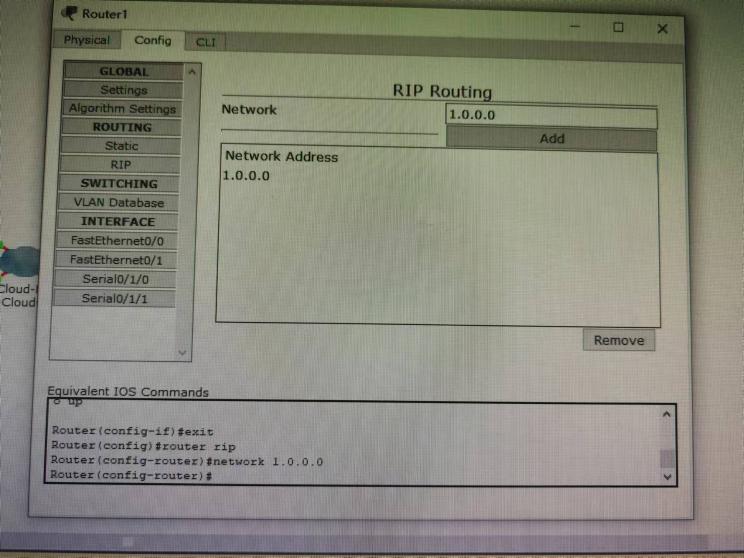
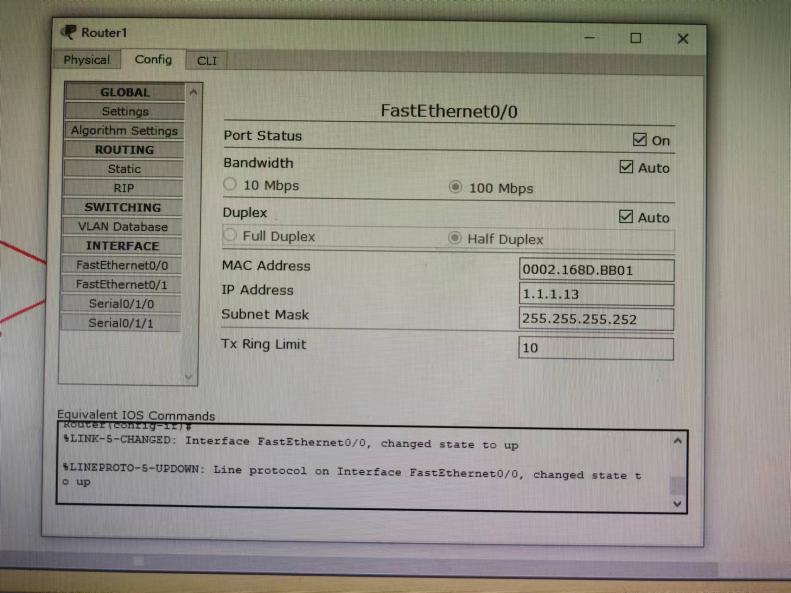


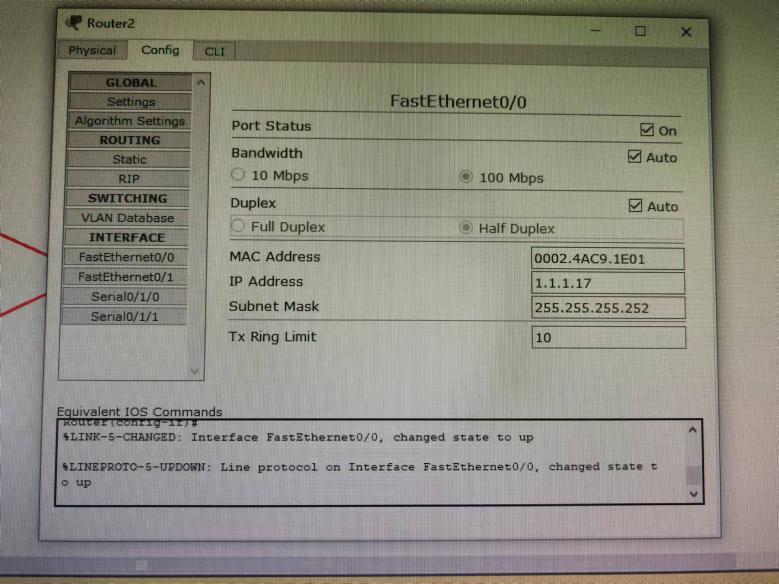
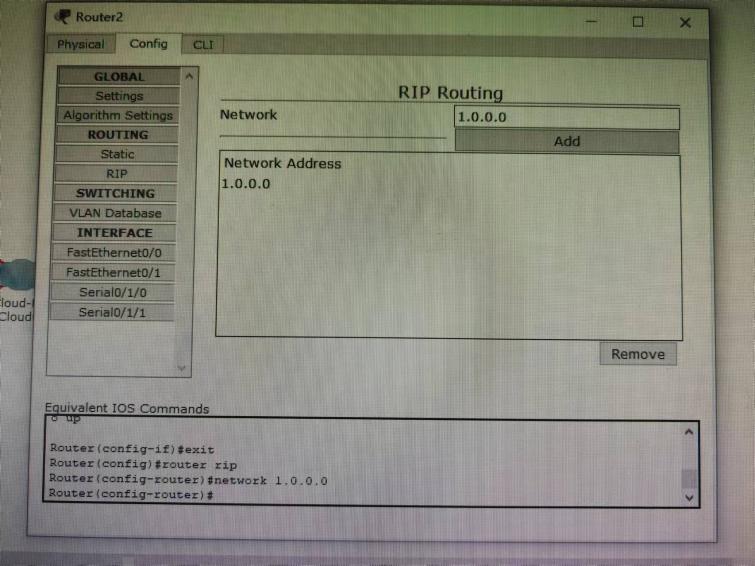
发现此时Router1和Router2可以互相ping成功。

按照要求，分别增加PC机，再次配置路由器的IP、子网掩码和RIP、各PC机器的IP、子网掩码和网关，进行ping测验并观察现象。

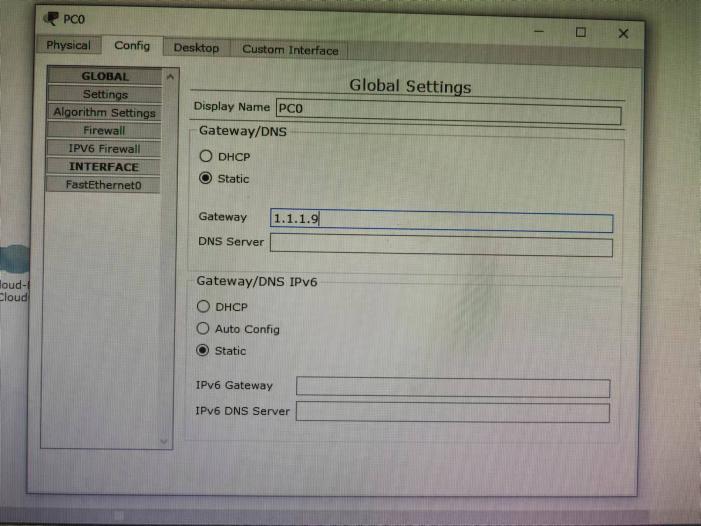
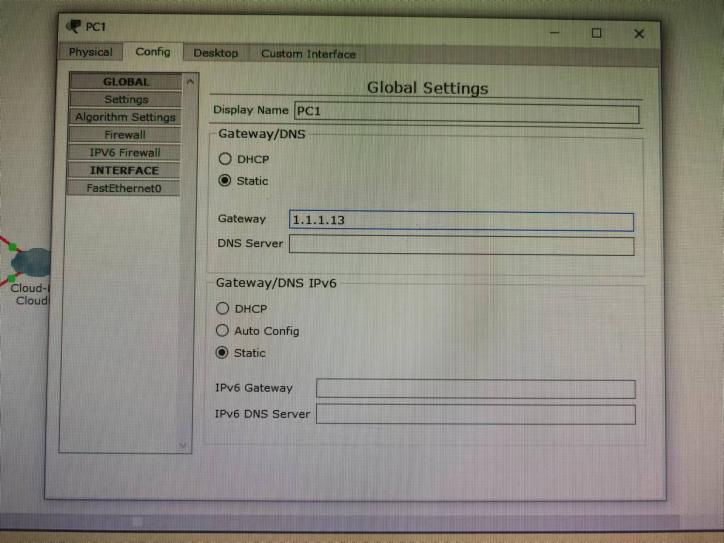
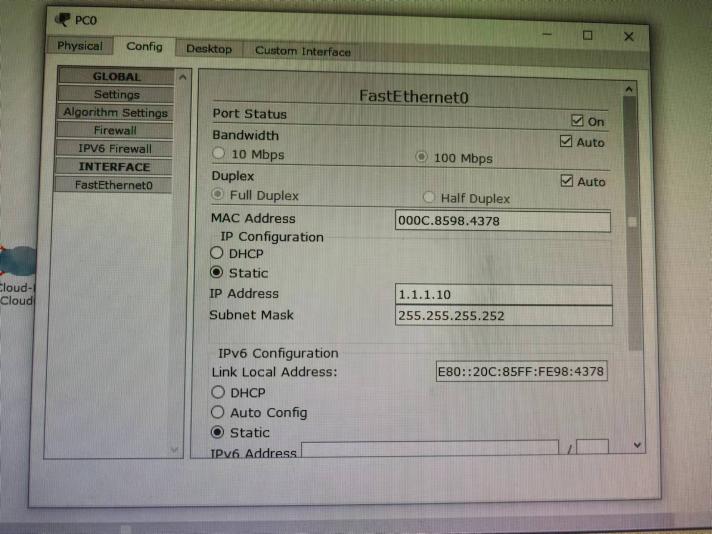


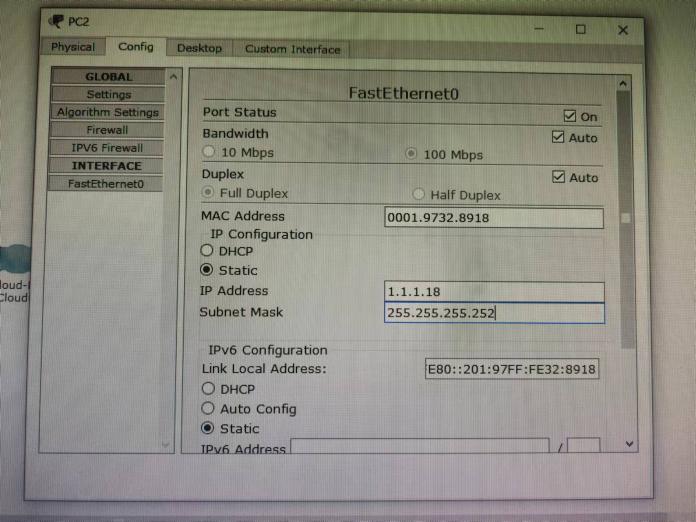
配置Router0

配置Router1

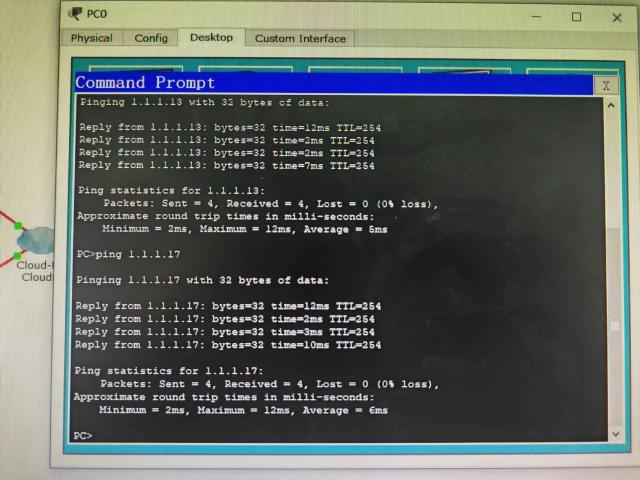
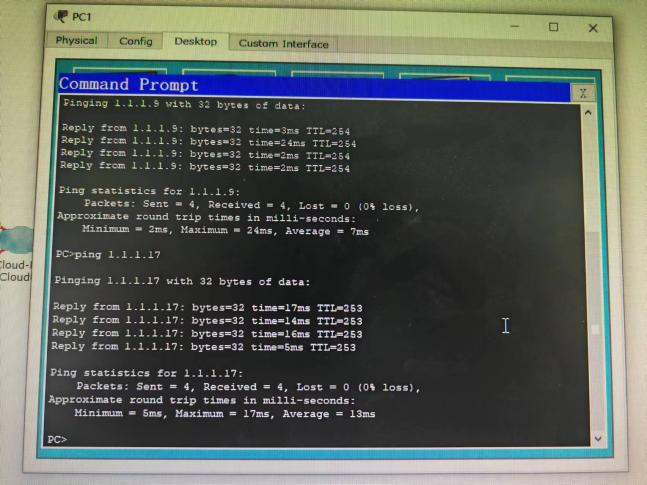
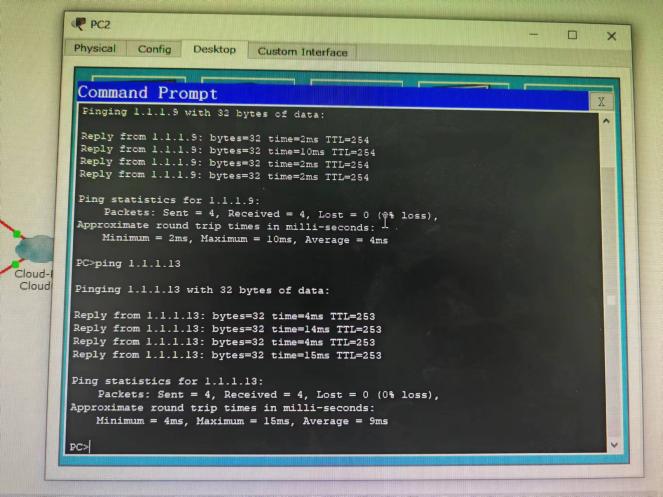
配置Router2

接下来配置各PC机器的IP、子网掩码和网关：





最后我们PC之间互相ping，发现PC之间能互相ping得通。



【**分析讨论**】

本次实验的过程较为复杂，非常锻炼我们的基础动手能力和逻辑顺序能力。在一开始时我们需要完成路由器和帧中继交换机的配置，之后我们需要在路由器中配置，在三个路由器中互相ping，并且观察能否ping得通。完成对Router1和Router2之中的静态路由的配置，看看之后能不能ping通。最后在路由器后加上相应的PC机，配置好对应的RIP之后再观察是否可以PC之间ping通。

本次实验的主题为帧中继的相关配置，说明了帧中继在网络互通之间发挥着重要的作用，主要体现在以下几个方面：

数据交换和传输: 帧中继协议允许在不同网络之间交换和传输数据帧。这种能力使得连接到不同帧中继网络的站点可以相互通信，实现数据的传输和交换。无论是连接到同一家服务提供商的网络还是不同服务提供商的网络，帧中继都能够在它们之间实现数据传输。

跨越异构网络: 帧中继可以跨越不同类型的网络，如局域网(LAN)、城域网 (MAN)或广域网(WAN)。这意味着它可以连接到各种类型和不同厂商的网络设备，实现异构网络之间的互联互通。

带宽管理和控制: 帧中继网络允许灵活地管理带宽。通过配置虚拟电路(VC) 和带宽控制，网络管理员可以根据实际需求分配和管理带宽资源。这种灵活性有助于确保每个站点在网络中都能够获得足够带宽，并且能根据需要进行动态调整。

RIP的配置使得我们本次实验中的机器可以相互ping通，可见其再网络通信中的应用还是非常广泛，也是非常重要的。

RIP是一种基于距离向量的动态路由协议，用于在计算机网络中交换路由信息，以便动态地更新路由表。它使用跳数(hop count)作为衡量路径开销的指标。每个路由器在路由表中存储到达目的网络的跳数信息，并定期将其发送到相邻路由器。当网络拓扑发生变化时，路由器会更新其路由表并向相邻路由器发送更新。RIP是一种简单的协议，易于配置和实现。它使用广播方式发送路由更新信息，这在小型网络中效率较高，但在大型网络中会产生较大的网络流量。RIP使用固定的时间间隔(通常为30秒)发送路由更新，不会根据网络拓扑变化的情况进行自适应调整。RIP受限于其跳数限制(最大跳数为15)，这限制了其适用范围，特别是在较大的网络中。