**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：**

实验十：OSPF动态路由

**实验目的：**

（1）深入掌握动态路由原理

（2）掌握动态路由OSPF的配置方法

（3）掌握OSPF路由工作原理

**实验仪器：**

Router路由器1台、主机2台、三层交换机1台

**实验原理：**

首先通过[网络基础之动态路由协议（OSPF）\_display ospf routing-CSDN博客](https://blog.csdn.net/weixin_51326240/article/details/109487773)学习相关基础知识。OSPF是最短路径优先协议，属于典型的链路状态路由协议和内部网关协议。OSPF网络中的每一个路由器维护一个链路状态数据库，即每一台路由器都保存了张哥网络的拓扑结构。基于链路状态数据库，通过最短路径算法，路由器能够构造出路由表。

其特点包括：

（1）可适应大规模网络，不受物理跳数的限制。对于小规模网络，RIP是首先路由协议，当网络规模扩大，具有10台以上路由器时，就需要OSPF 路由协议了。

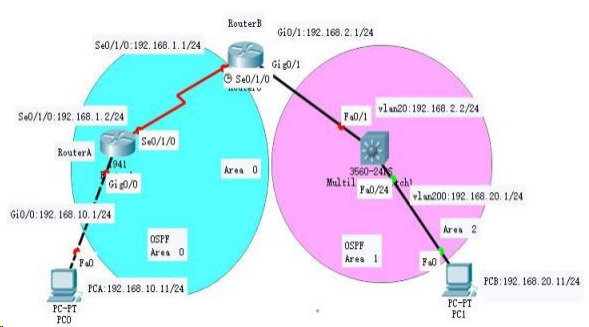
（2）OSPF路由变化收敛速度快，协议自身网络开销较小。

（3）最短路径采用SPF算法，避免了路由环路。

（4）以开销作为度量值，带宽越高，开销越小。

（5）支持区域划分。

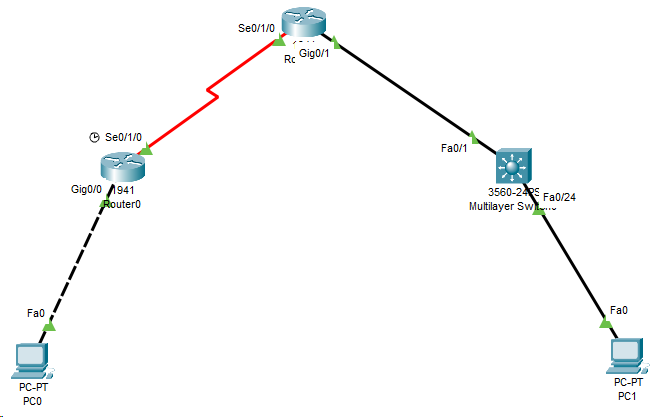
OSPF划分区域的目的是为了控制链路状态信息LSA泛洪的范围、减小链路状态数据库 LSDB 的大小、改善网络的可扩展性、快速地收敛。当网络包含多个区域时，OSPF协议规定，必须有一个Area 0区域，通常也叫做骨干区域，其他所有区域都必须与骨干区域物理或逻辑上相连。本次实验的网络拓扑结构如下。



**实验内容与步骤：**

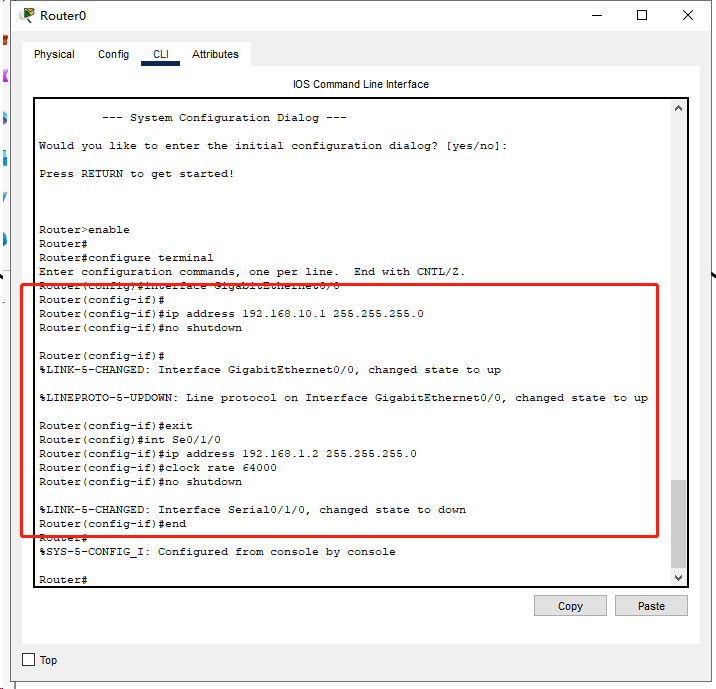
**（1）线缆连接**

为路由器增加串口模块，按照网络拓扑图组网。

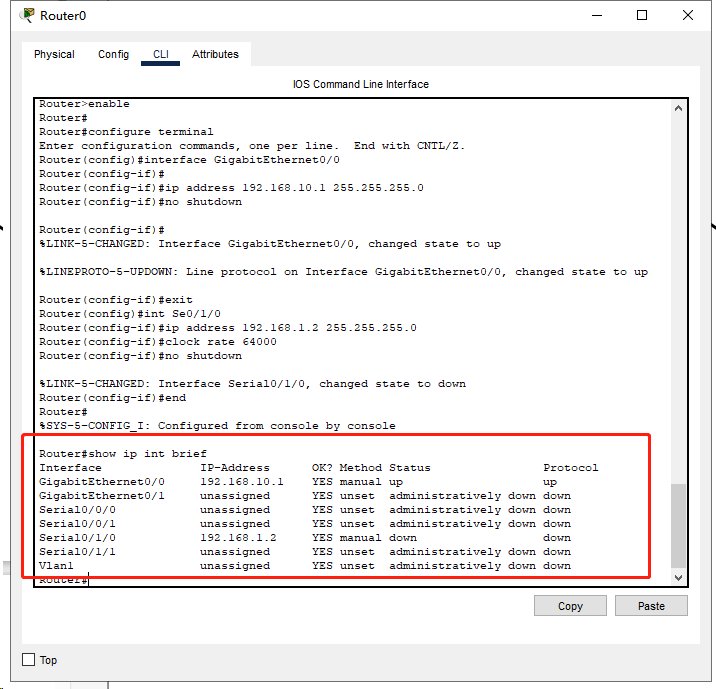


**（2）配置路由器接口地址**

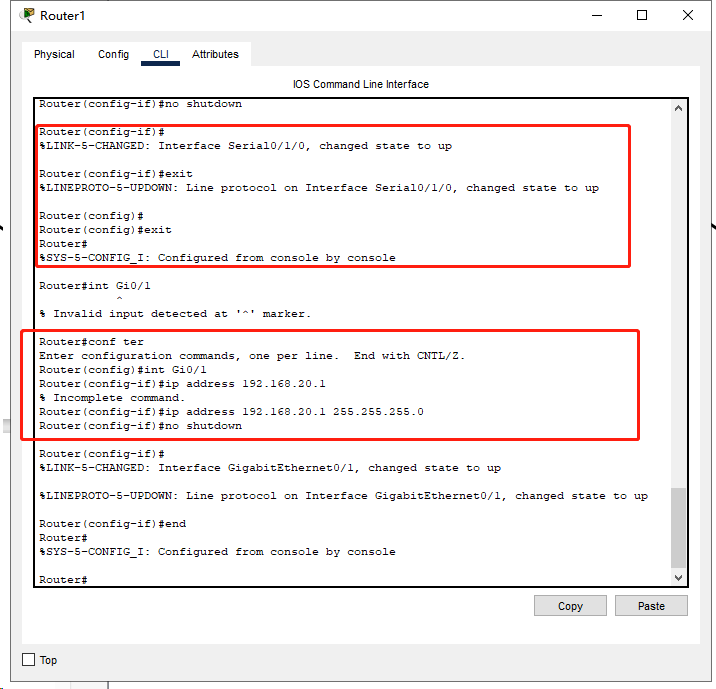
配置Router0



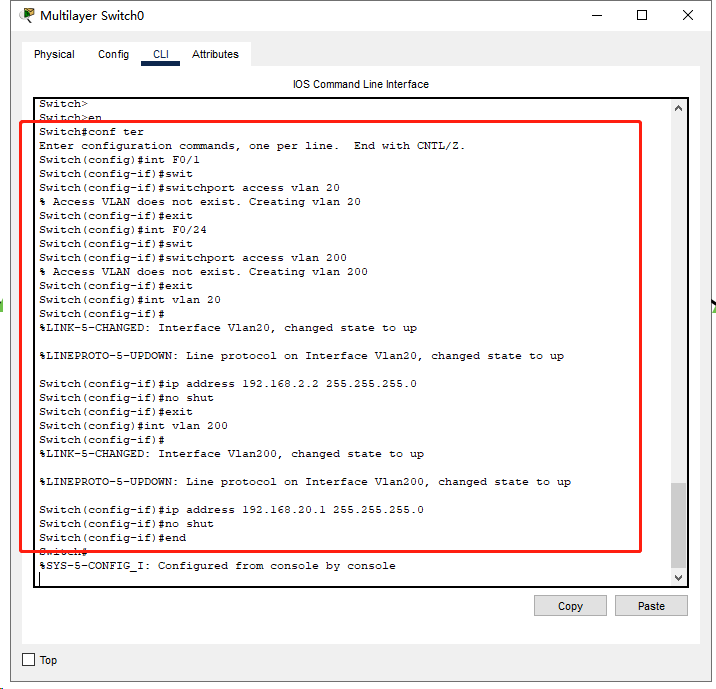
查看Router0



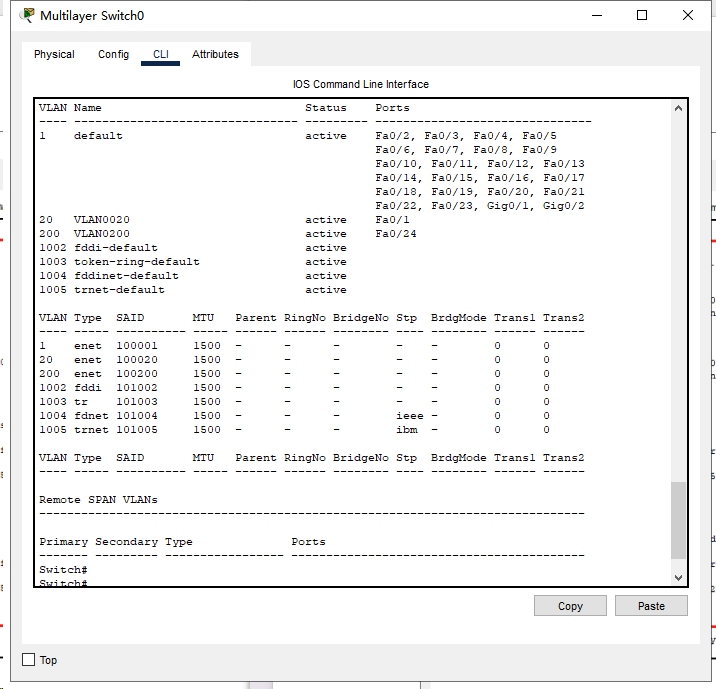
配置Router1

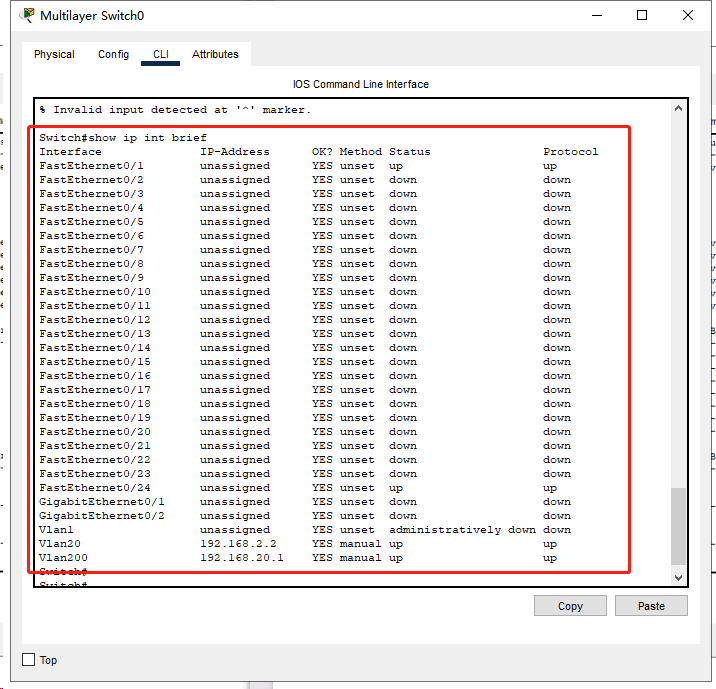


**（3）配置三层交换机**



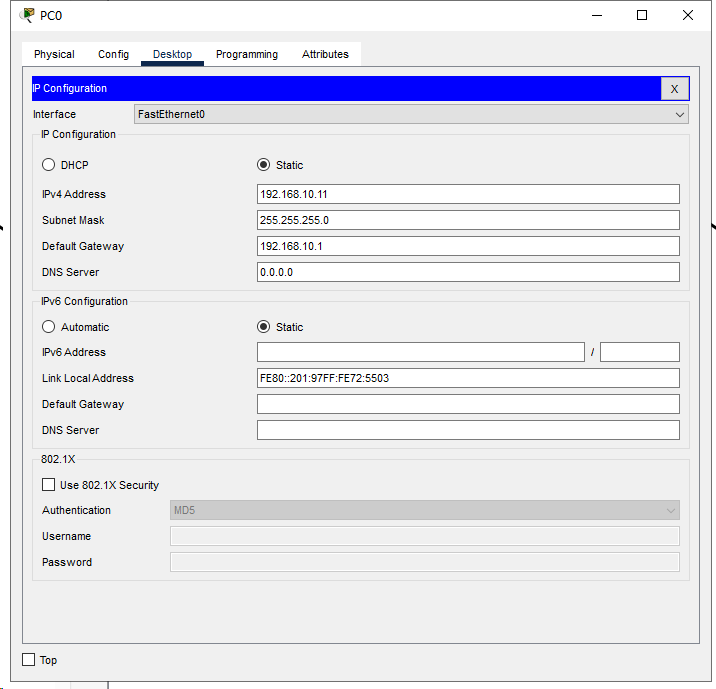
通过命令检查配置情况



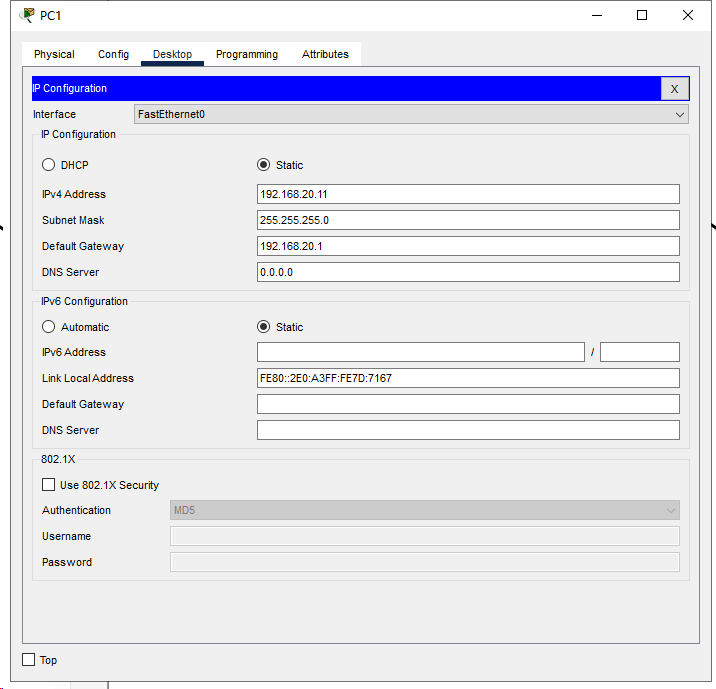


**（4）配置PC机的IP地址**

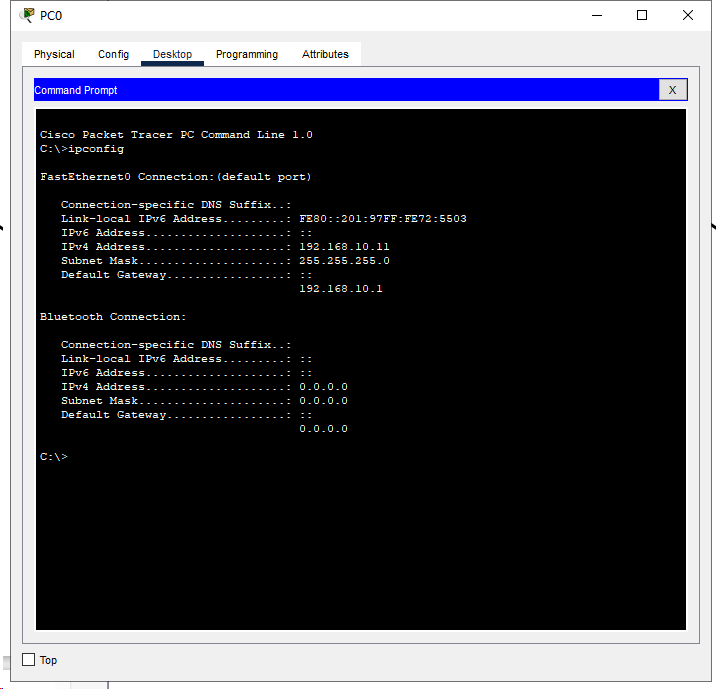
PC0

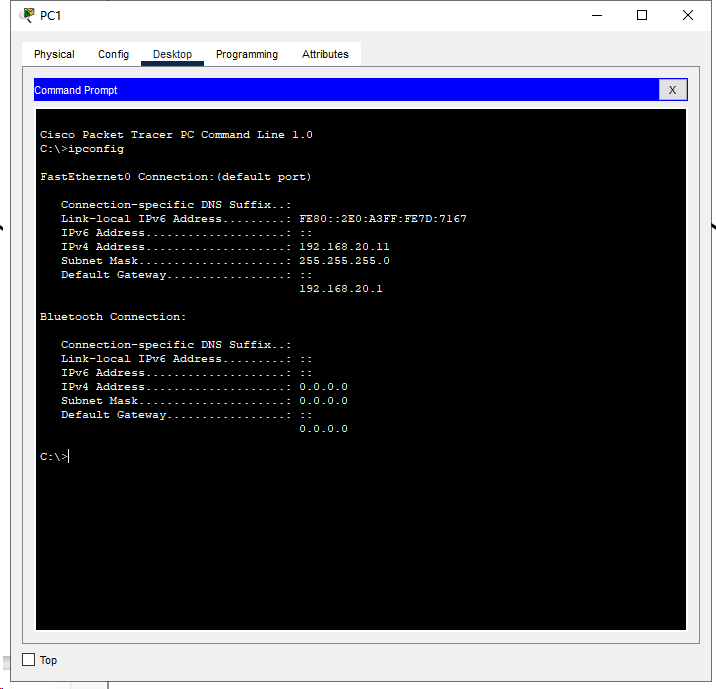


PC1



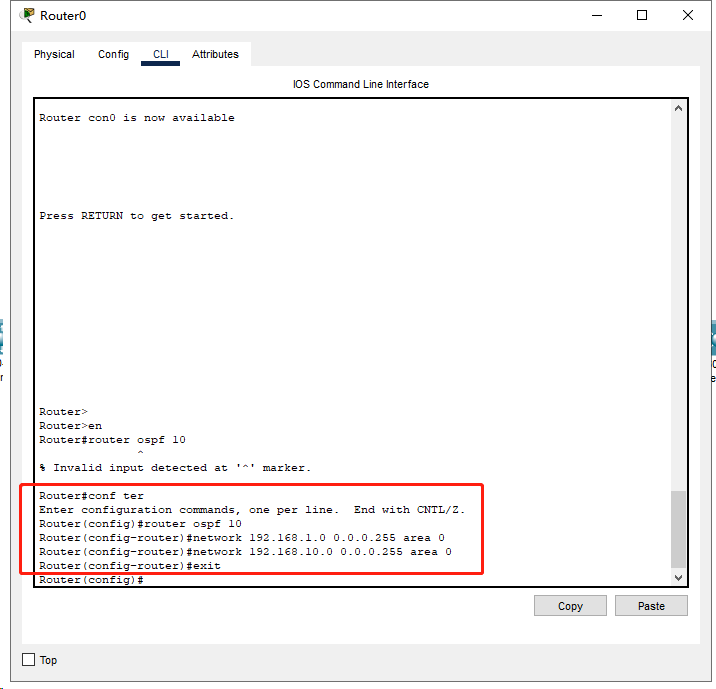
查看是否生效



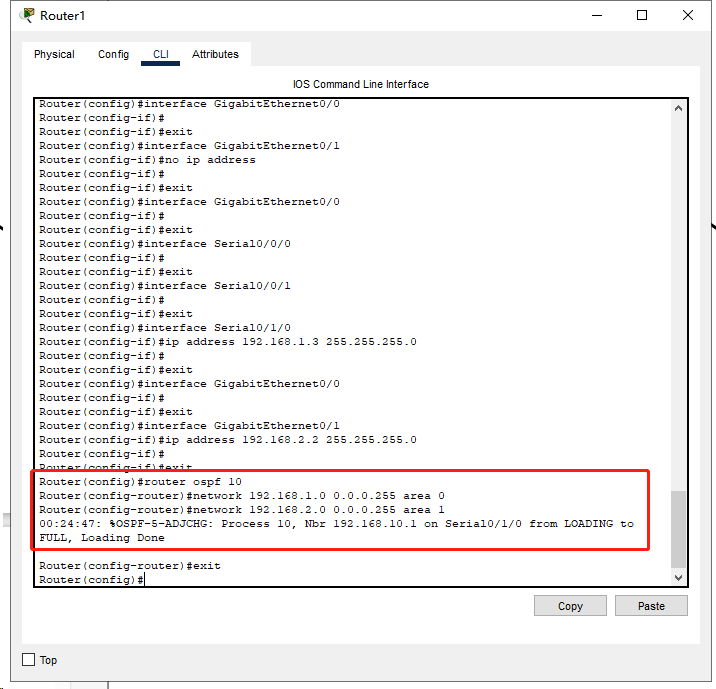


**（5）配置动态路由协议OSPF**

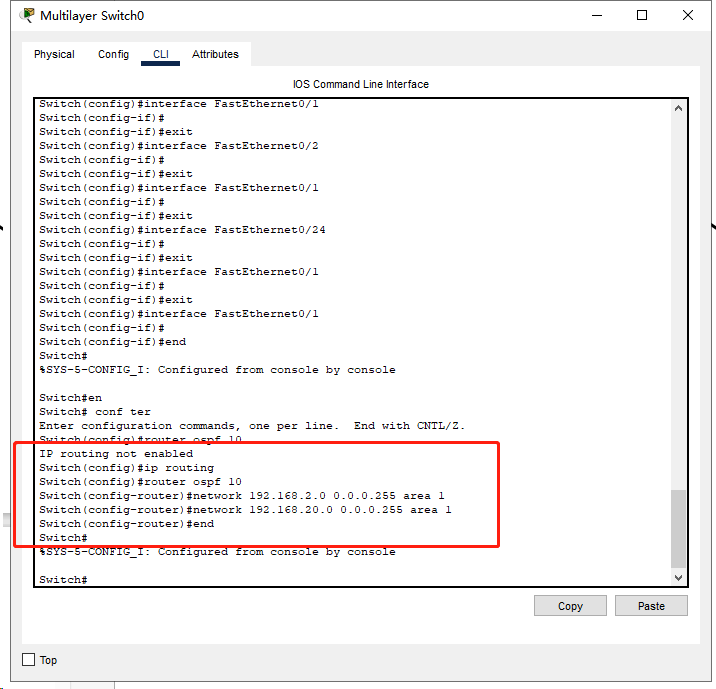
路由器Router0，两个网段都在Area0区域



路由器Router1，左侧在Area0区域，右侧在Area1区域

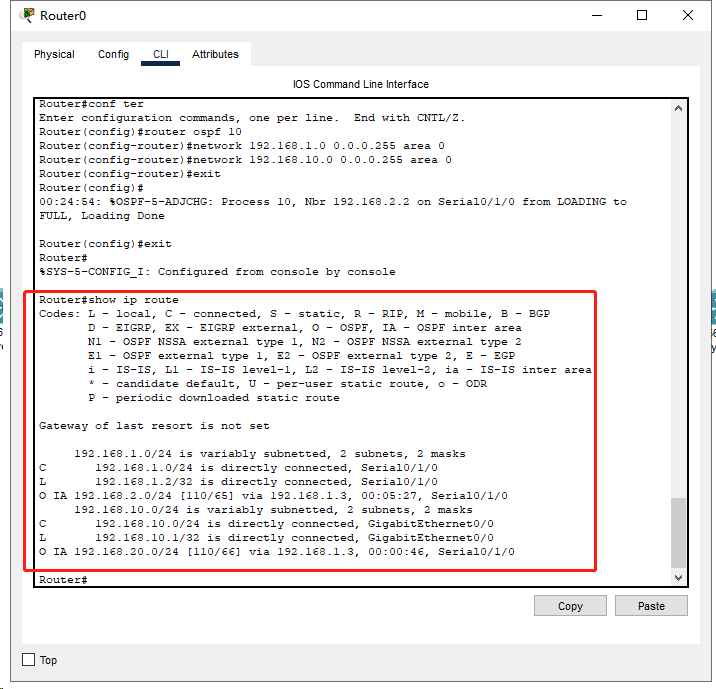


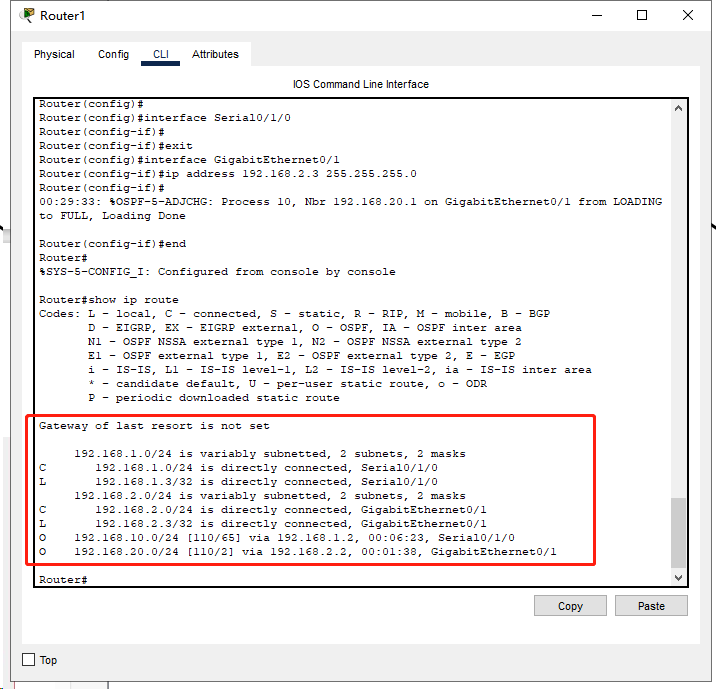
交换机Switch，两个网段都在Area1区域

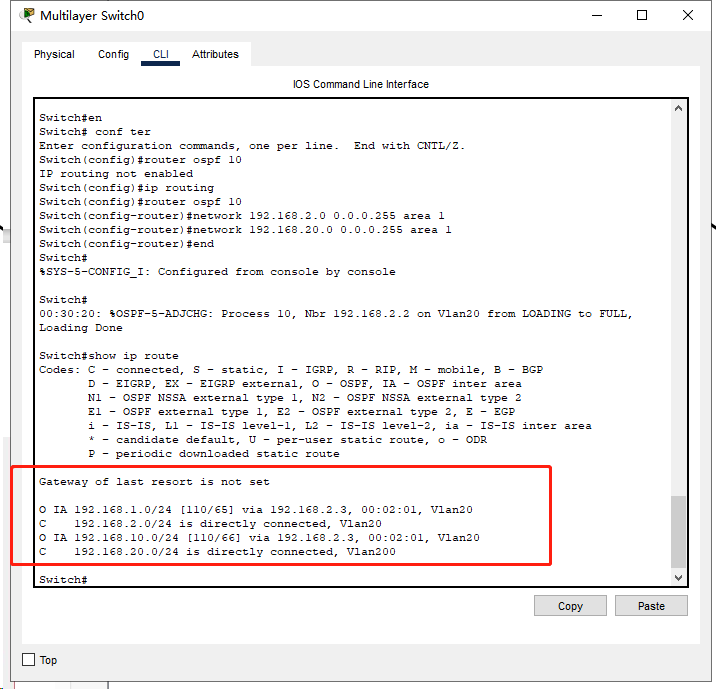


**（6）查看路由表**

查看路由器或交换机上的路由表，每台设备上的路由表都有四个网段。

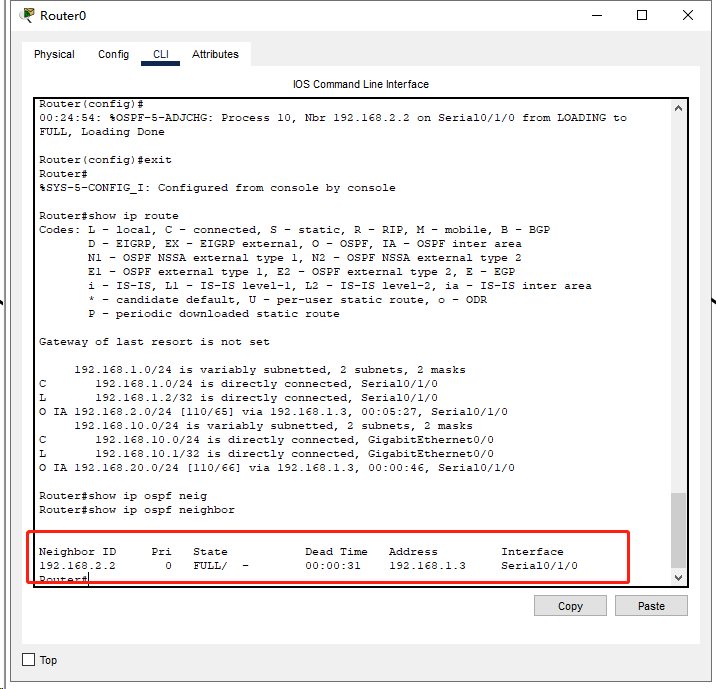




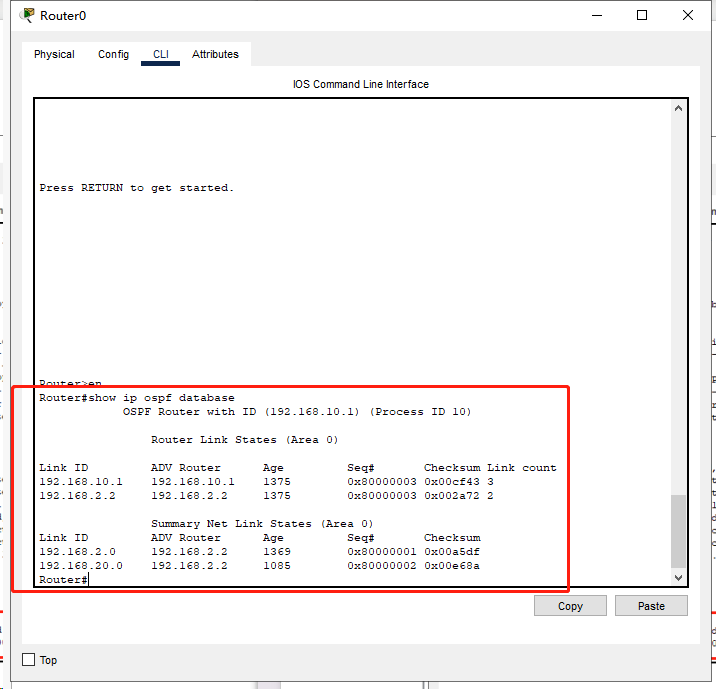


**（7）查看OSPF信息**

在Router0上查看OSPF邻居Router1，状态位full，因为两个路由器之间是点对点的链路，所以没有选举DR和BDR，邻居存活的时间为31s，邻居IP地址和Router0的连接端口也列出来了。

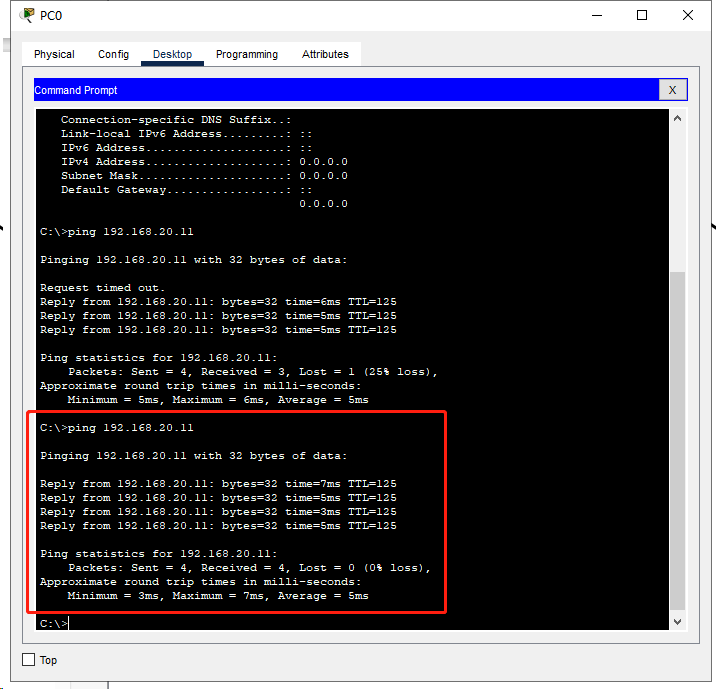


在Router0上查看OSPF数据库，显示Router0和Router1的IP地址，因为没有配置OSPF ID，路由器选择活动中端口地址中IP最大的作为自己的ID。



**（8）ping命令测试连通性**

PC0 ping PC1



**实验数据：**

本次实验无重要实验数据，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：**

由于本次实验未涉及重要的实验数据，因此无需进行数据处理。

**实验结果与分析：**

在这个环节，将针对实验指导书中的部分思考问题进行回答。

**（一）本实验拓扑图一共包含4个网段，划分Area0和Area1两个区域，尝试修改OSPF路由配置，将4个网段同时划入一个区域，看看PC0和PC1是否能够连通？**

在OSPF配置中，如果将4个网段同时划入一个OSPF区域（Area），这些网段将会共享相同的OSPF路由信息，但是仍然需要注意其他几个因素以确保PC0和PC1能够连通：（1）相邻路由器配置（2）IP地址配置（3）路由器行为

**（二）怎样理解和验证，同一网络中的路由器拥有一个相同的链路状态数据库（LSDB）？**

通过show ip ospf database查看各路由器，验证其链路状态数据库相同。

**实验名称：**

实验十一：基于思科模拟器的路由重分布实验

**实验目的：**

（1）掌握路由配置方法

（2）掌握不用路由协议之间转换的原则

（3）掌握静态路由或直连路由在动态路由重分布的方法

**实验仪器：**

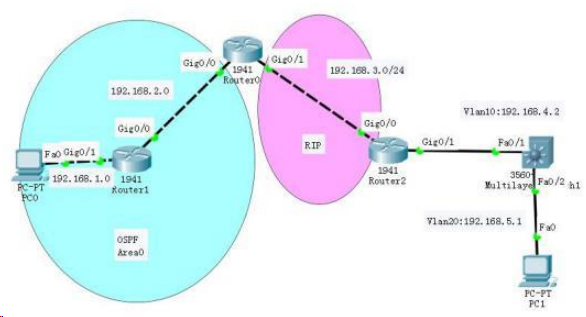
路由器3台、三层交换机1台、直连线若干、主机2台

**实验原理：**

某企业拥有3台路由器和1台三层交换机，企业内部采用了RIP和OSPF两种动态路由协议，同时网络中有去往192.168.5.0/24网段的静态路由，PC1所在末梢网络，有去往外部网络的默认路由，请正确配置网络设备，使得网络内部的每台设备都能通信。

路由重分布能让路由器交换路由信息，从而实现多种路由协议之间的路由信息共享。实施路由重分布的路由器为边界路由器（ASBR），该路由器上启用了多种路由协议，它们位于2个或多个自治系统的边界上。因路由协议自身的差异，在路由重分布时需要考虑不同路由协议的度量值和管理距离，度量值主要用于确定最佳路径，管理距离主要确定路由的来源。RIP路由以跳数作为路径的度量值，OSPF 路由以链路状态作路径的度量值，路由重分布的原则，就是度量值要进行合理的转换。OSPF在RIP中重分布时，要用metric折合成跳数，RIP在OSPF中重分布时，跳数也折合成链路状态的度量值。如果度量值分配不正确，路由重分布将会失败。

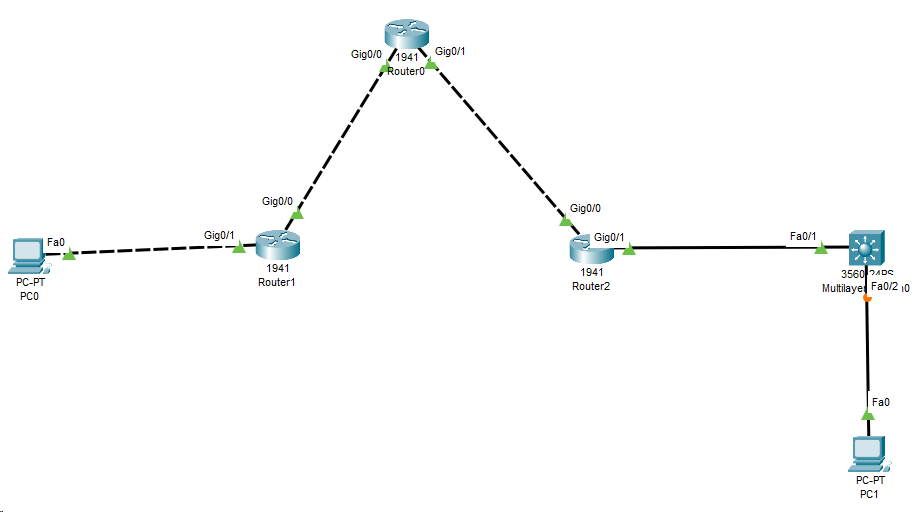
静态路由在RIP中重分布时，如果不指定度量值，默认是1跳。直连路由在RIP中重分布时，如果不指定度量值，默认也是1跳。静态路由和直连路由在OSPF中重分布时，如果不指定度量值，默认是20，类型为2，默认子网不进行重分布，所以一般要加上参数subnets，子网也可以重分布。本次实验的网络拓扑结构图如下。



**实验内容与步骤：**

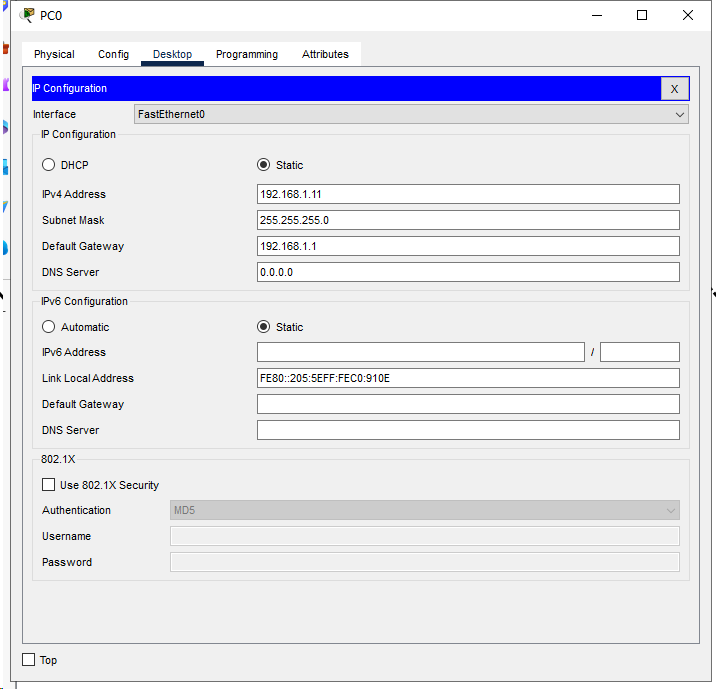
**（1）连线**

选择路由器和交换机，按照网络拓扑结构连线。

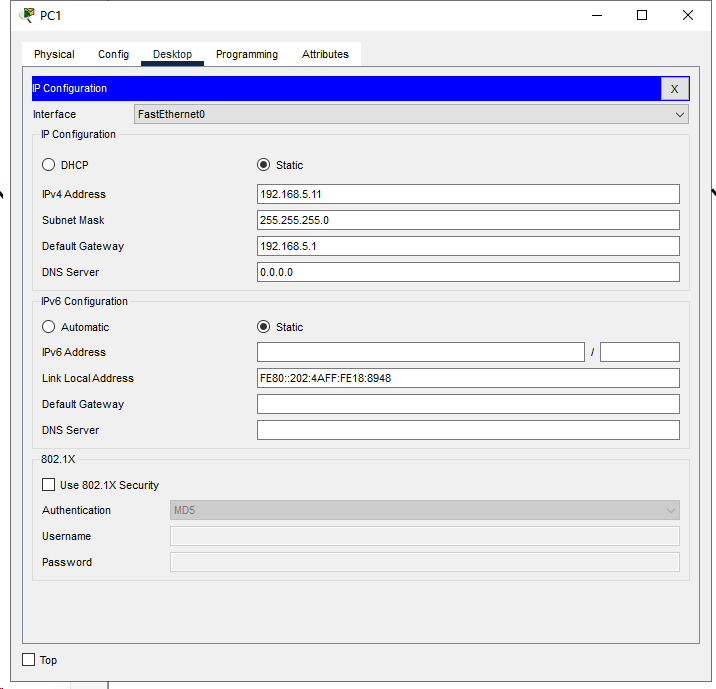


**（2）配置主机网卡地址**

PC0

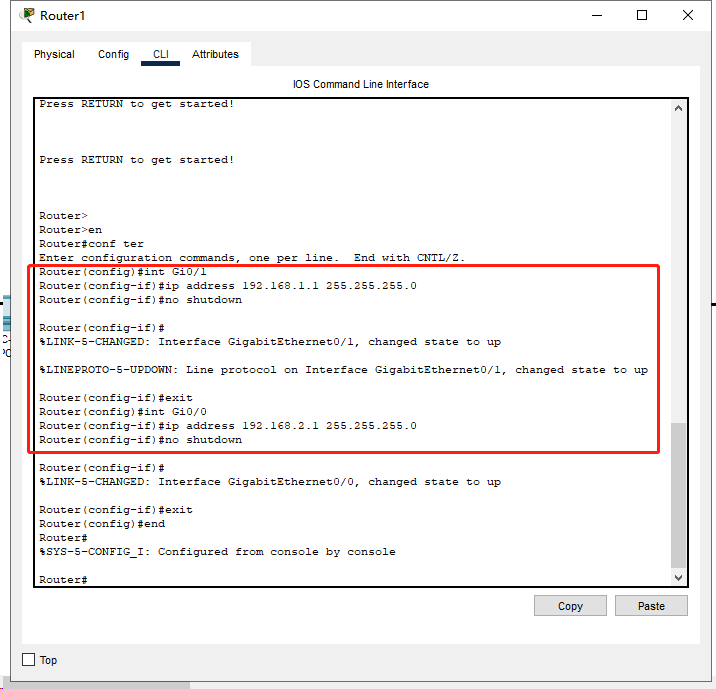


PC1

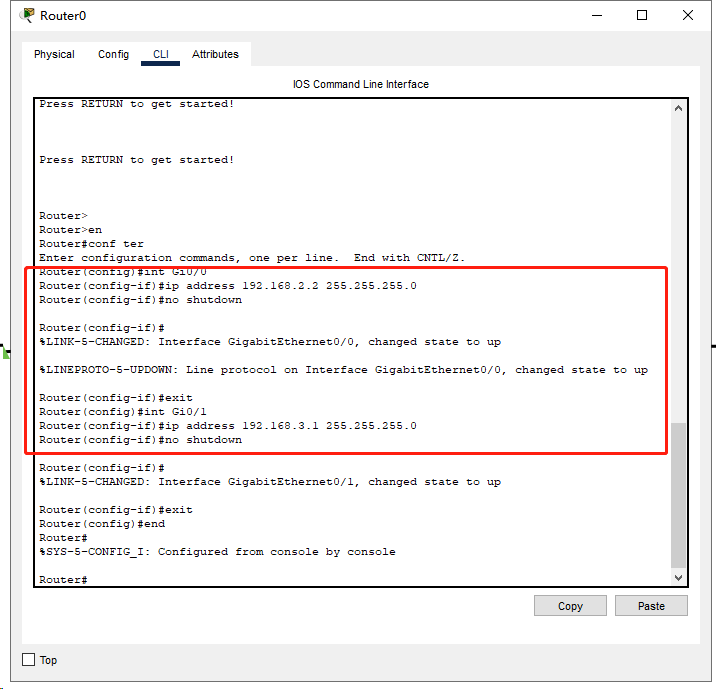


**（3）配置路由器的端口地址**

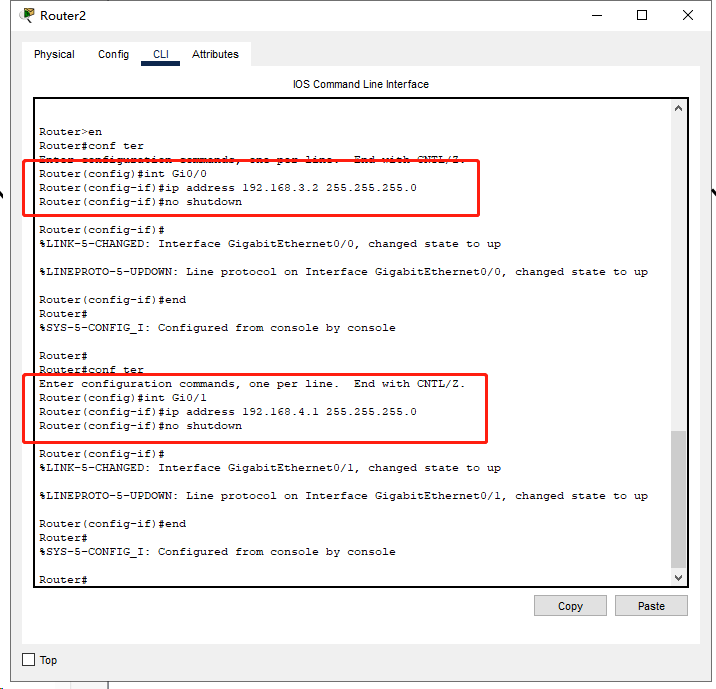
R1



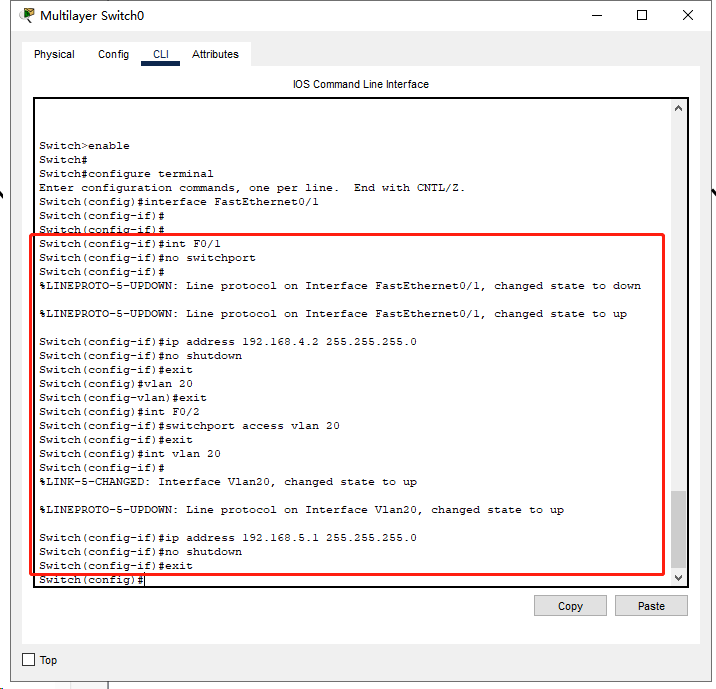
R0

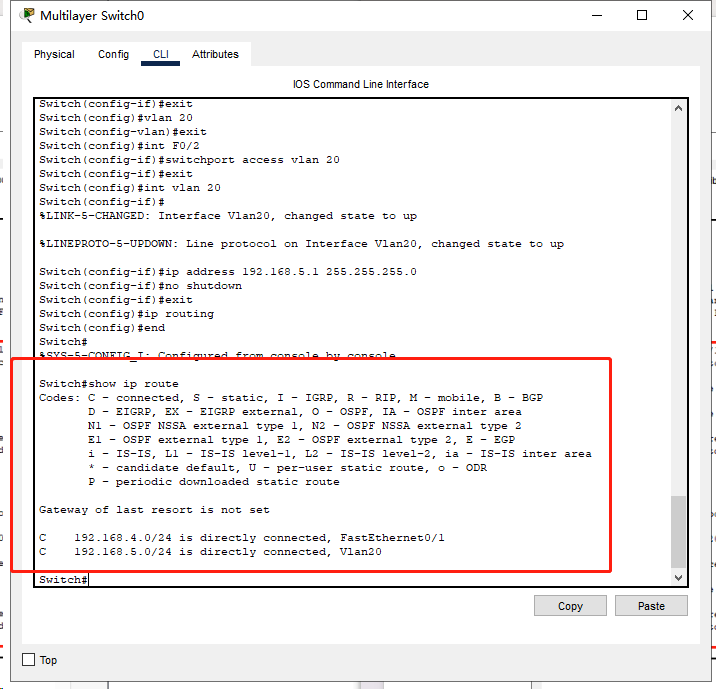


R2



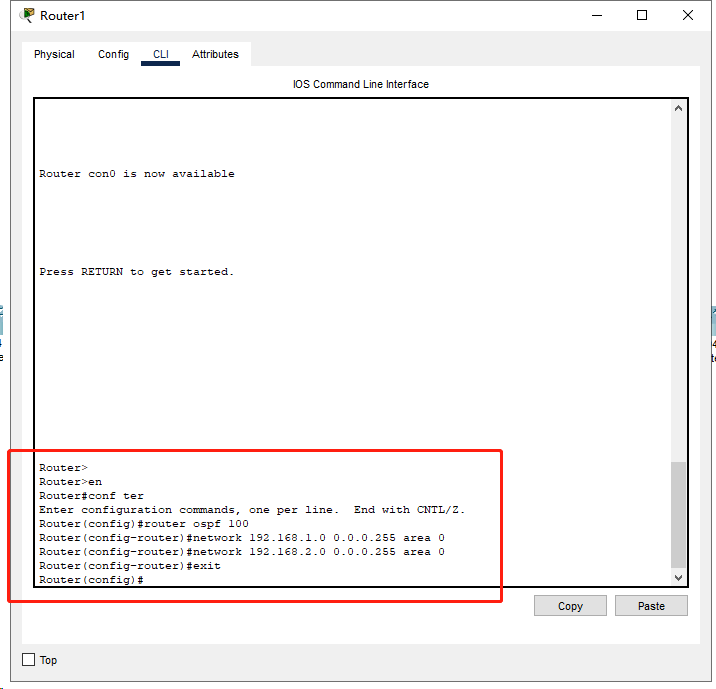
**（4）配置交换机的端口地址**



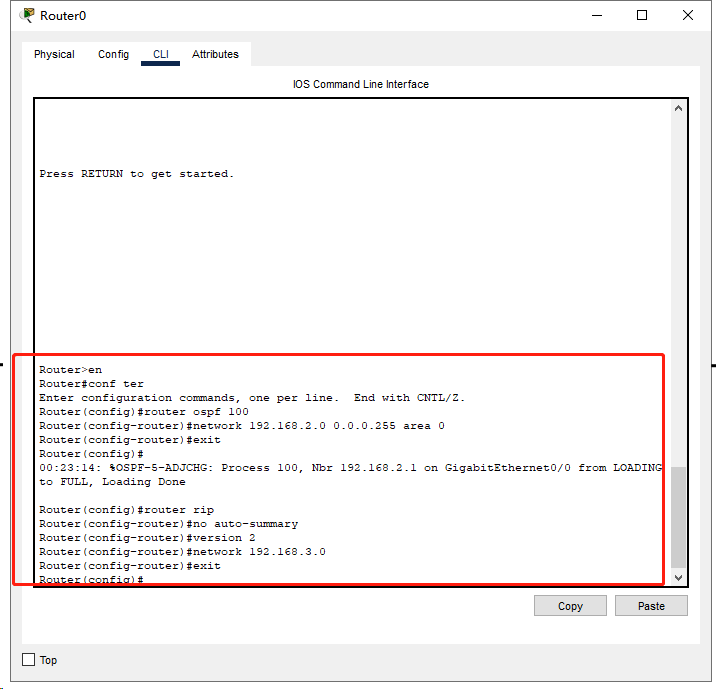


**（5）配置路由（重分布之前）**

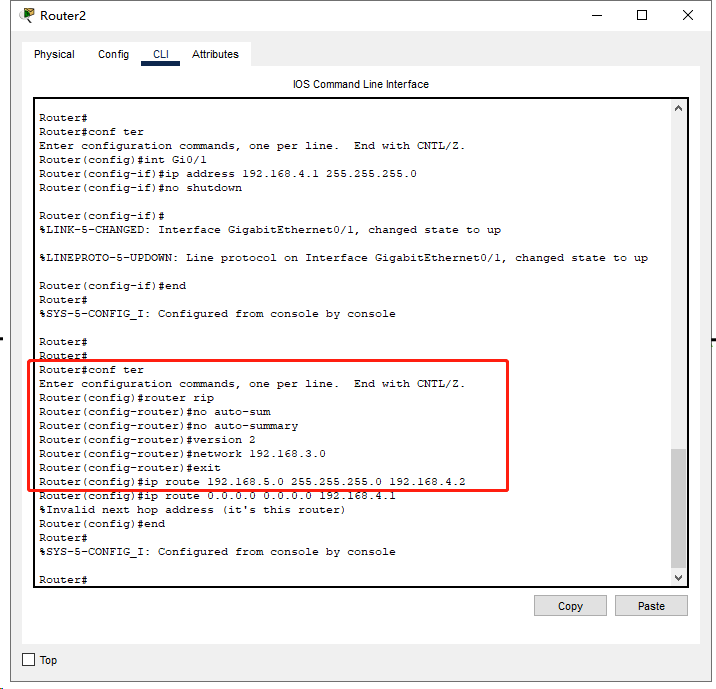
R1



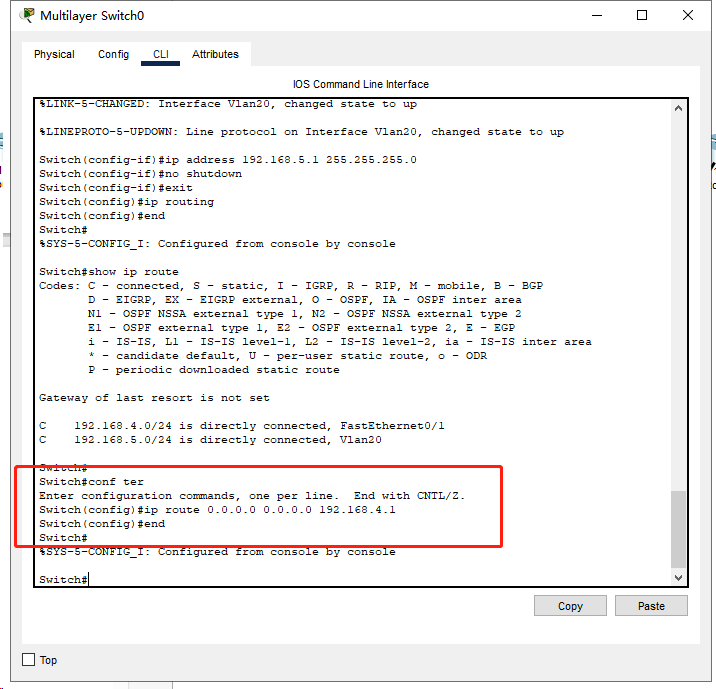
R0

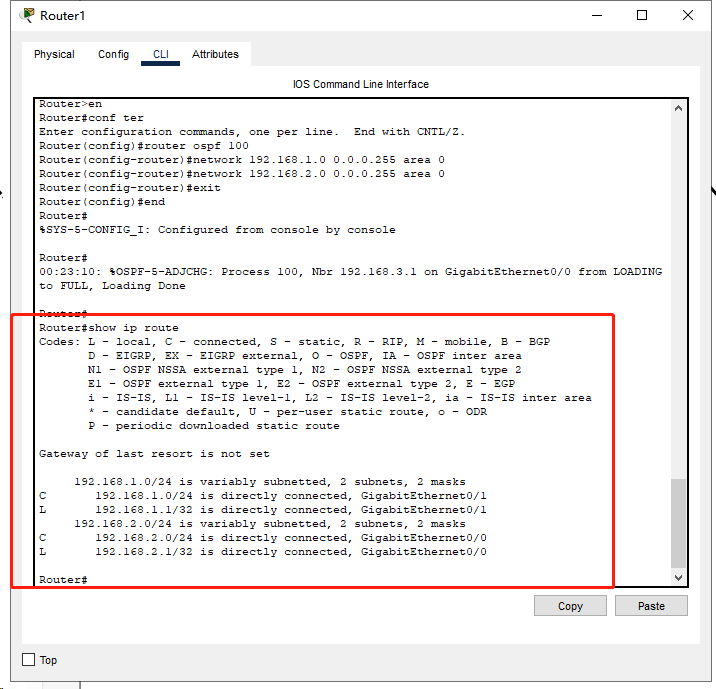


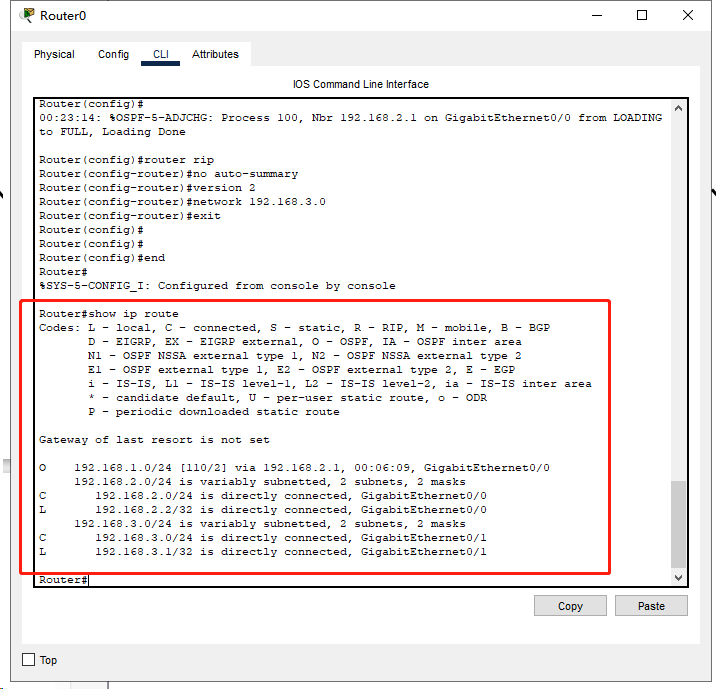
R2

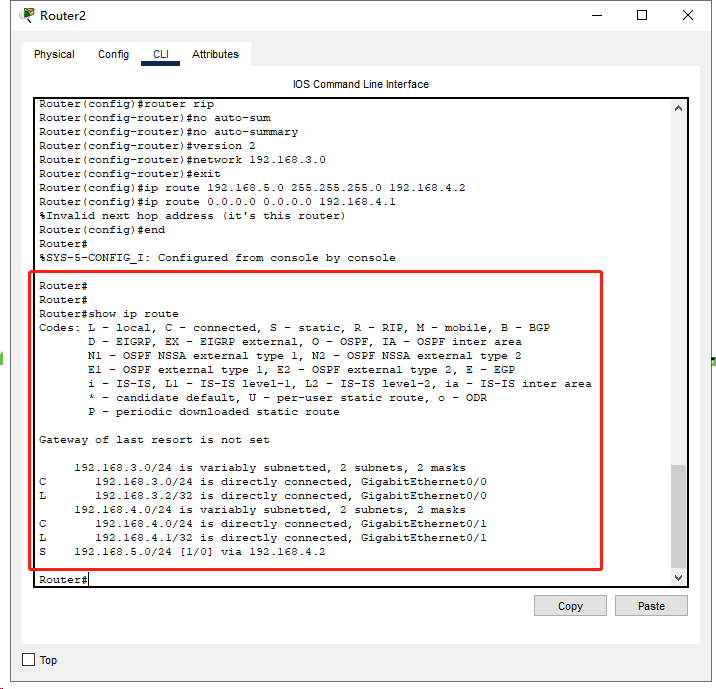


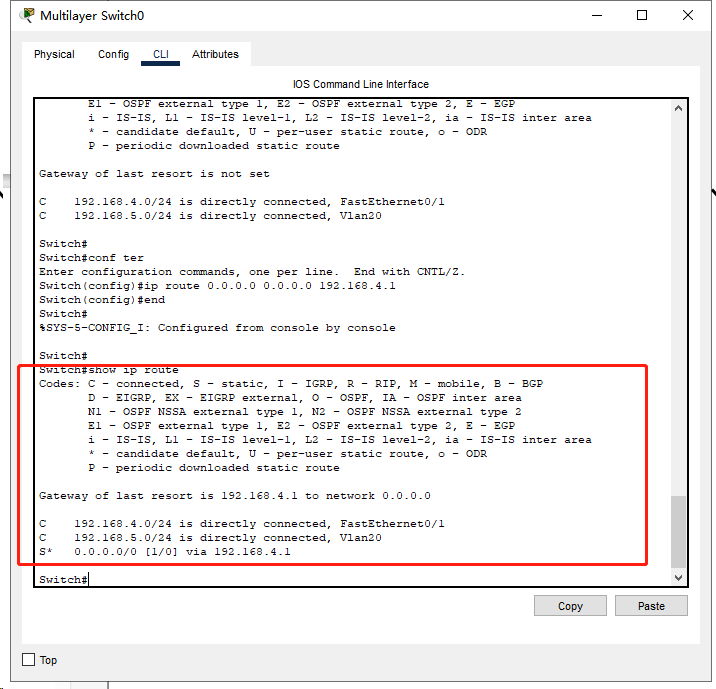
switch





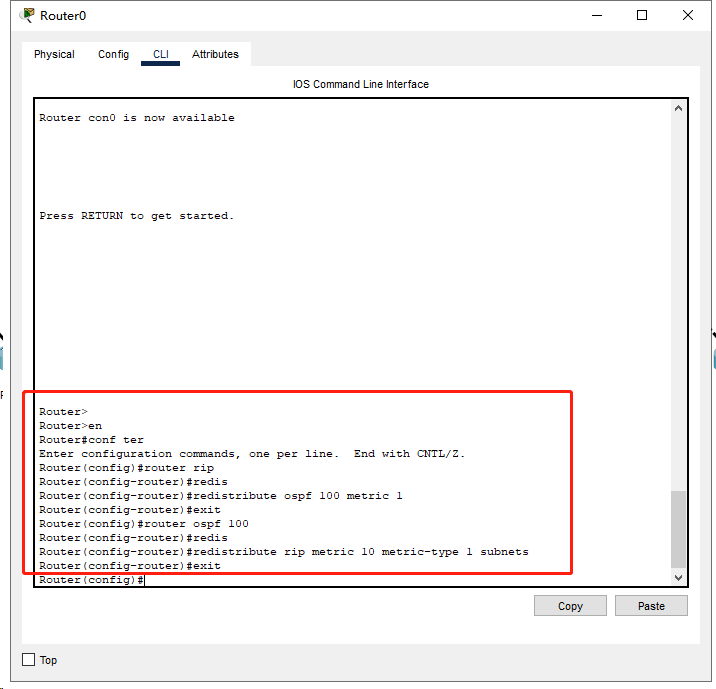




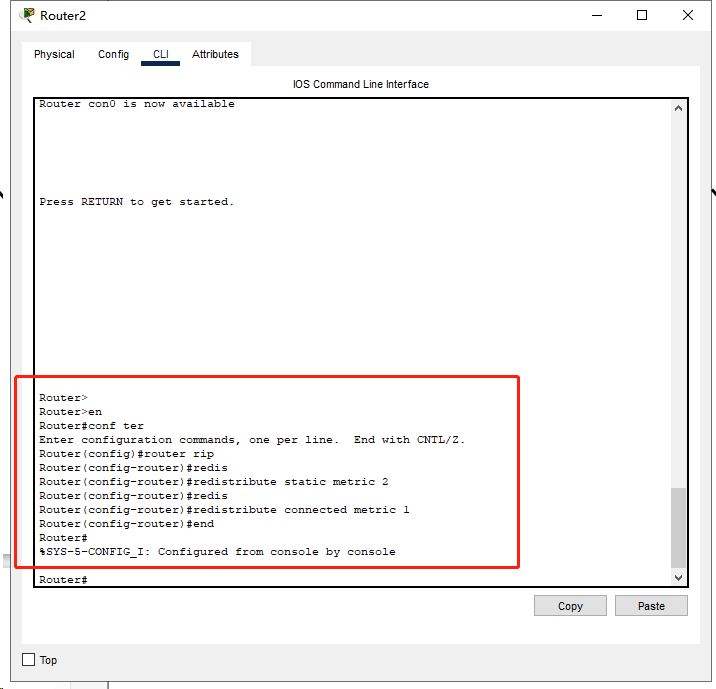


**（6）路由重分布**

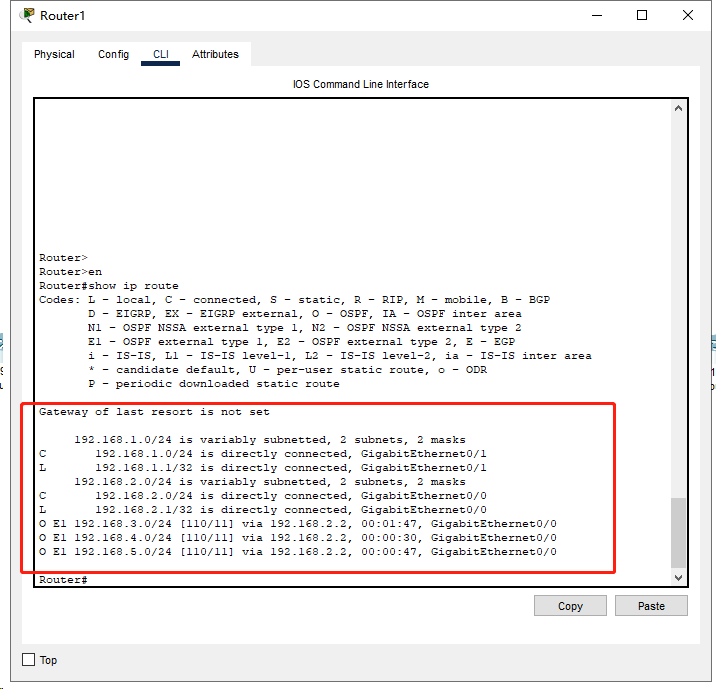
R0

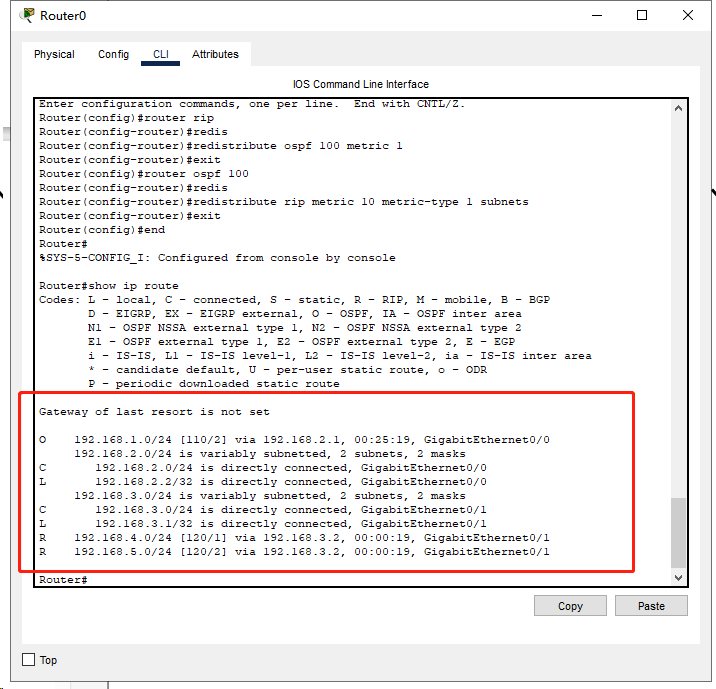


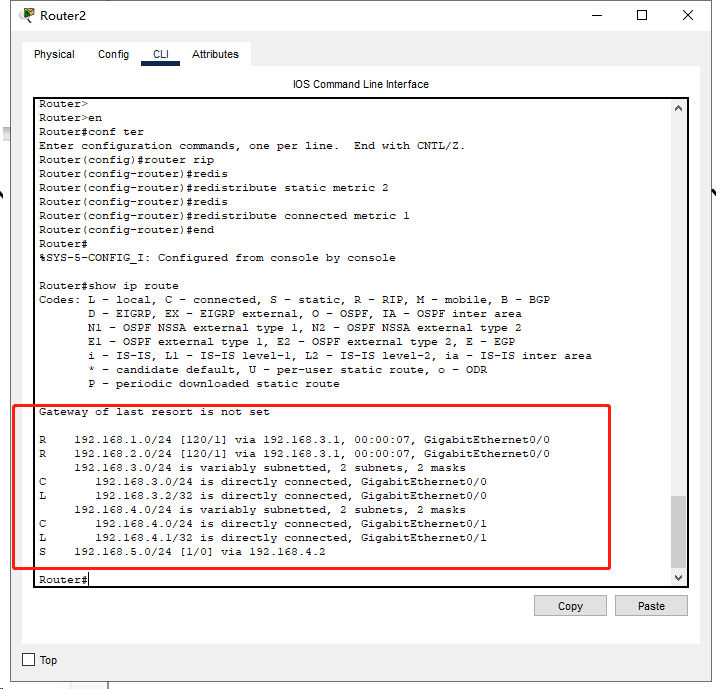
R2

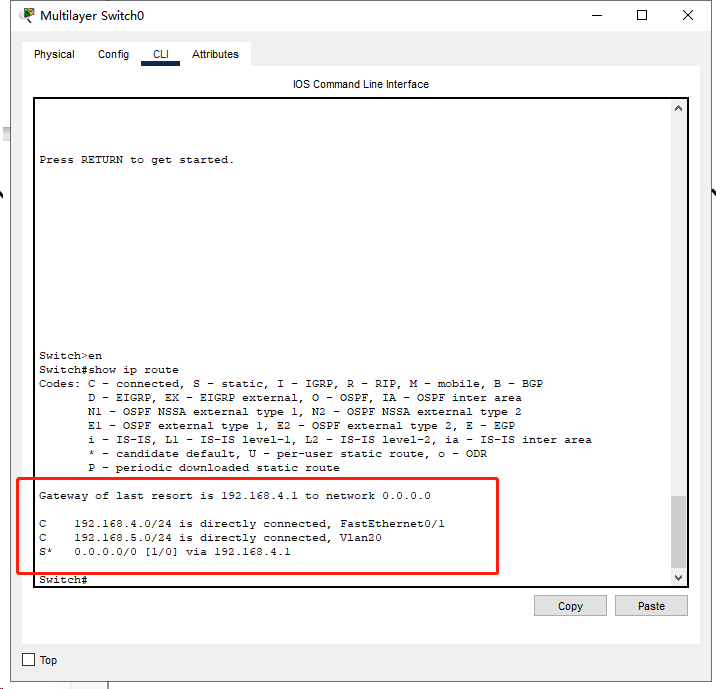


查看配置情况



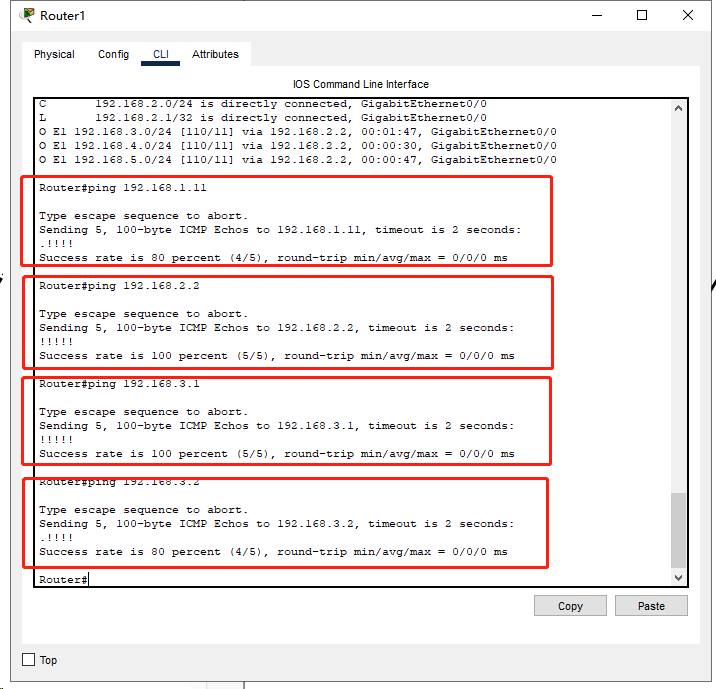


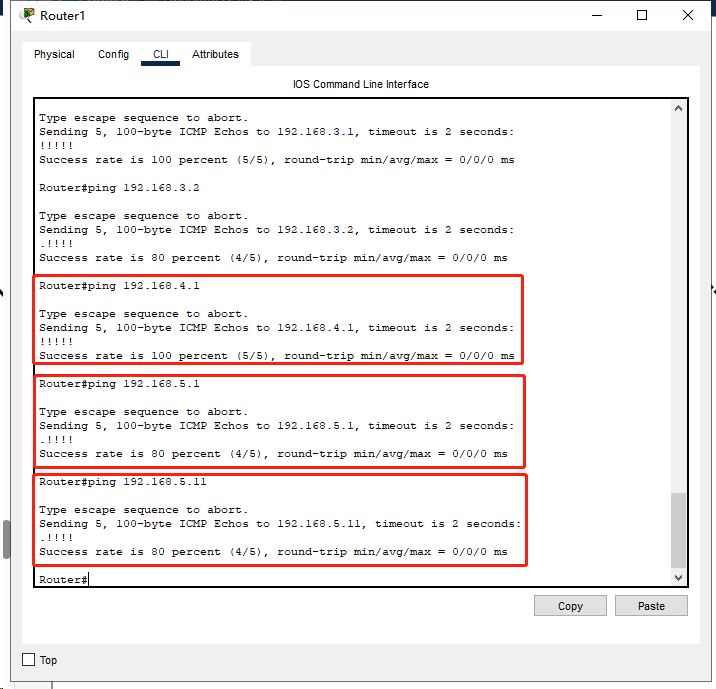




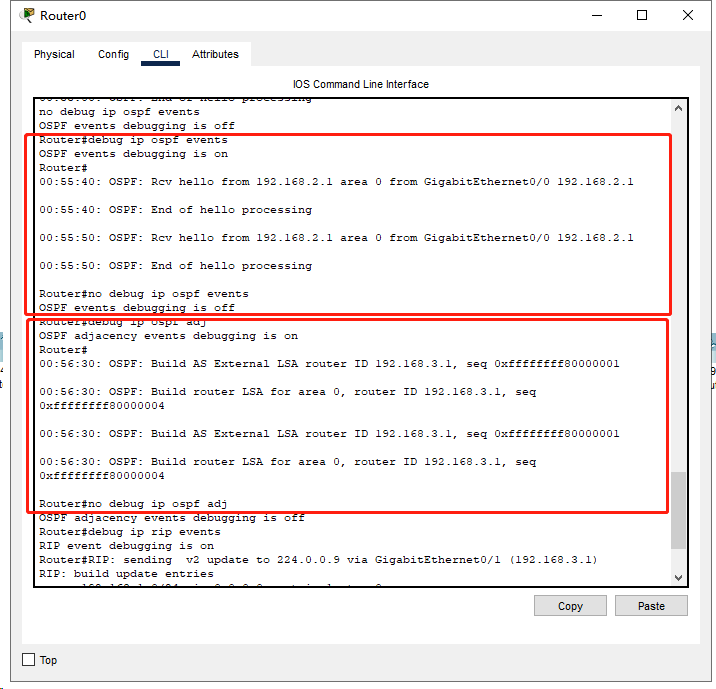
**（7）测试连通性**

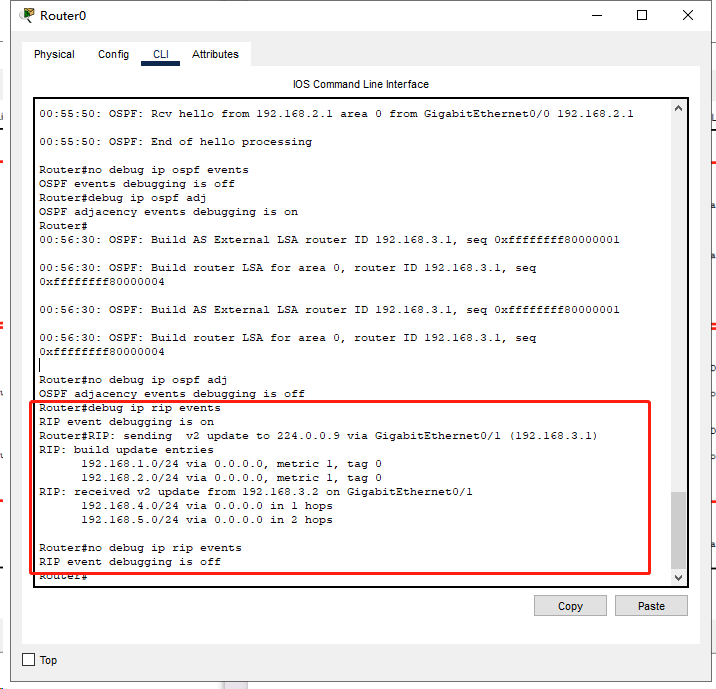
在Router1上进行，按照从左到右的顺序，每一个节点都能连通。





**（8）debug命令测试**





**实验数据：**

本次实验无重要实验数据，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：**

由于本次实验未涉及重要的实验数据，因此无需进行数据处理。

**实验结果与分析：**

本实验为验证性实验，无需进行分析。

**实验名称：**

实验十二：基于思科模拟器的NAT实验

**实验目的：**

（1）掌握如何向外网发布内网的服务器

（2）掌握NAT源地址转换和目的地址转换的区别

**实验仪器：**

路由器2台、二层交换机1台、V.35线缆1对、主机4台

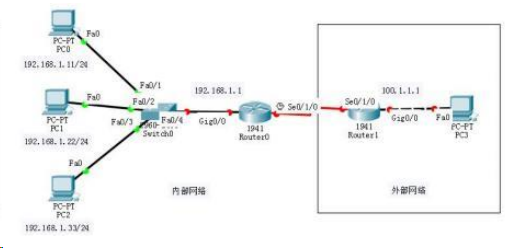
**实验原理：**

计算机网络理论课前段时间刚好学习了NAT网络地址转换，因此借着这个实验再次熟悉NAT。网络地址转换NAT，能帮助解决IP地址资源紧缺的问题，而且使得内外网隔离，提高一定的网络安全保障。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了全局地址后转发数据包。

NAT分为两种类型：网络地址转换NAT和网络地址端口转换NAPT。NAT是实现转换后一个本地IP地址对应一个全局地址。NAPT 是实现转换后多个本地IP地址对应一个全局IP地址，并用不同的端口号进行区分。

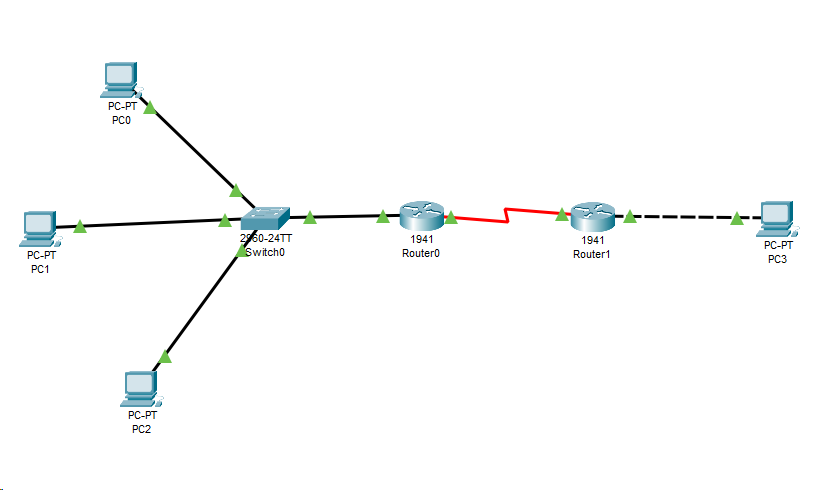
在传统的路由交换网络中可以使用路由器实现NAT转换，近年来大多使用防火墙来完成。使用路由器实现NAT 时，常常会发现路由器的性能下降，这是因为每一个经过路由器的数据包都要进行NAT地址转换，这必然消耗系统的CPU资源，而且转换的中间结果还要暂时保存在内存中以便于回应数据的恢复。防火墙的主要功能就是完成这种复杂任务，它的性能不像路由器那样下降明显。

本实验要实现内网网段192.168.1.0/24的地址转换，假设只有50个公网地址，地址池是200.1.1.100/24-200.1.1.150/24，假设外网服务器地址为100.1.1.X/ 16。本次实验的网络拓扑结构如下所示。



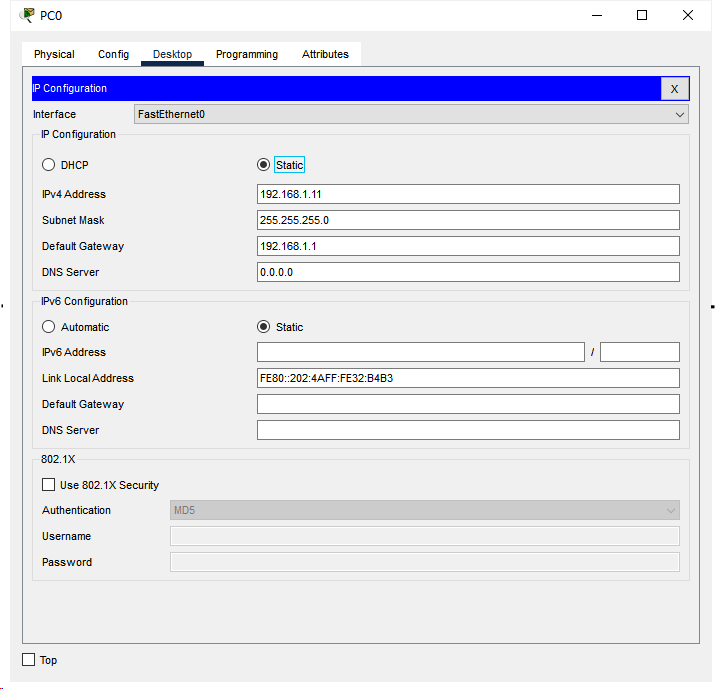
**实验内容与步骤：**

**（1）关闭电源，将HWIC-2T模块拖拽到空卡槽，为路由器添加串口并连线组网**

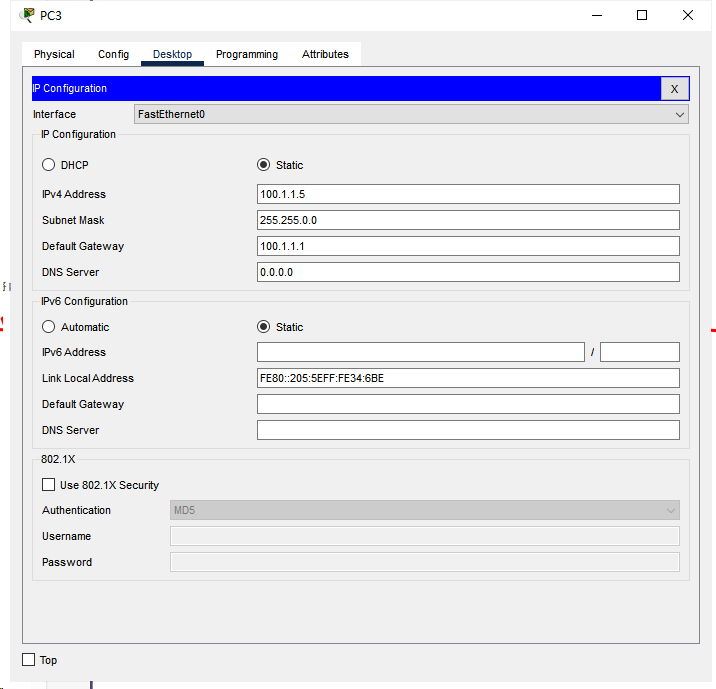


**（2）配置网卡地址**

PC0

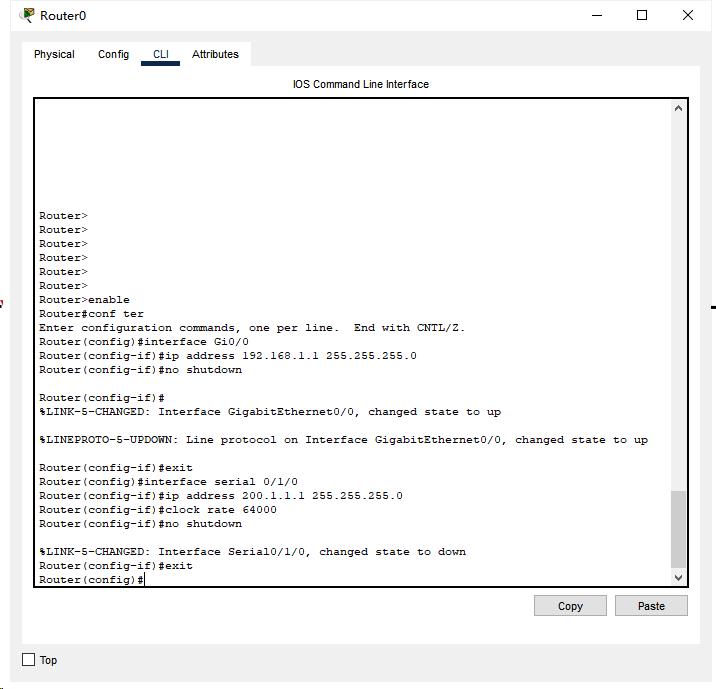


PC3

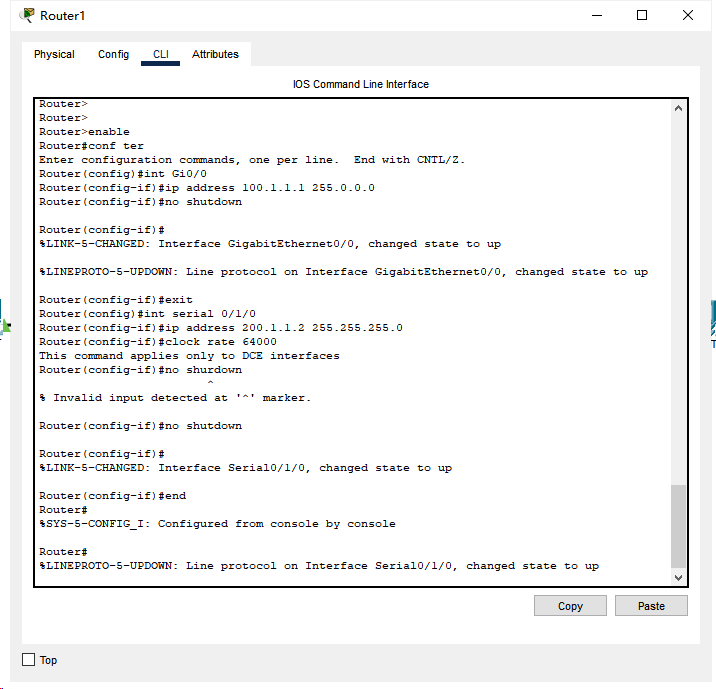


**（3）配置路由器**

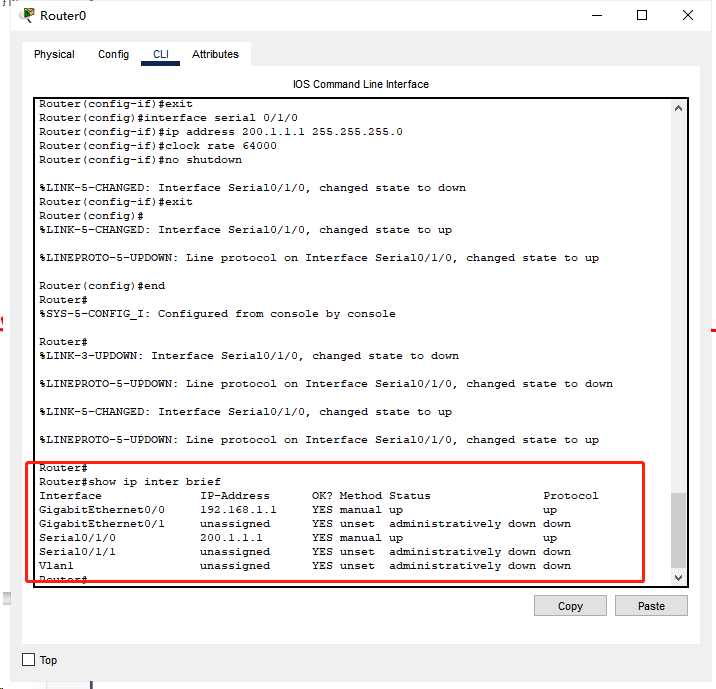
配置R0



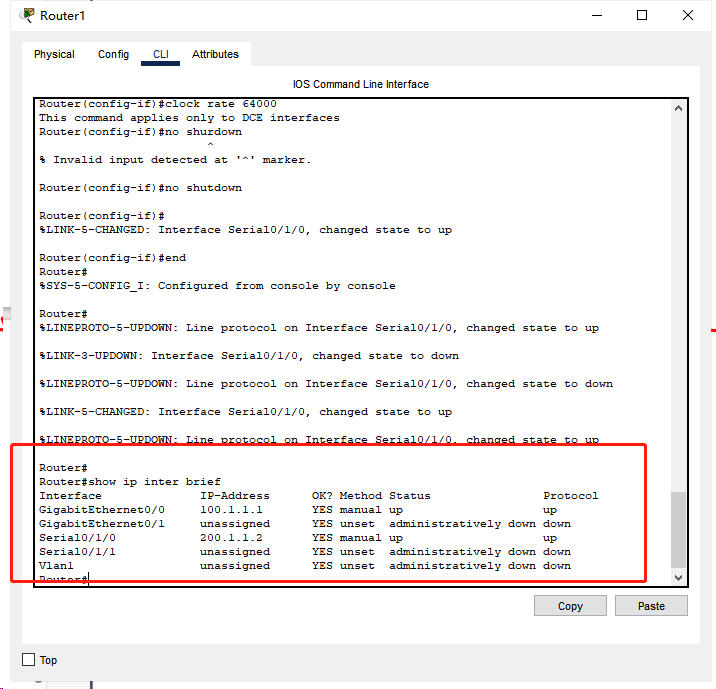
配置R1



查看R0

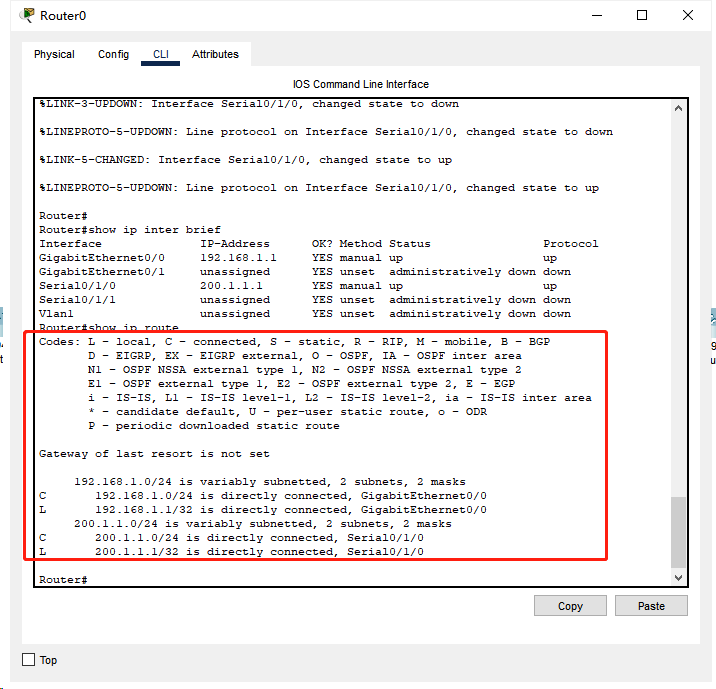


查看R1

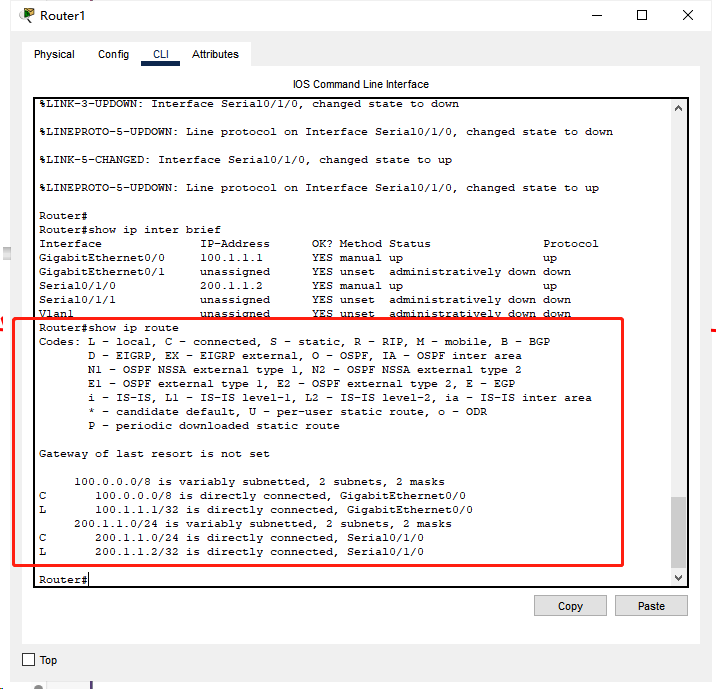


**（4）配置R0默认路由**

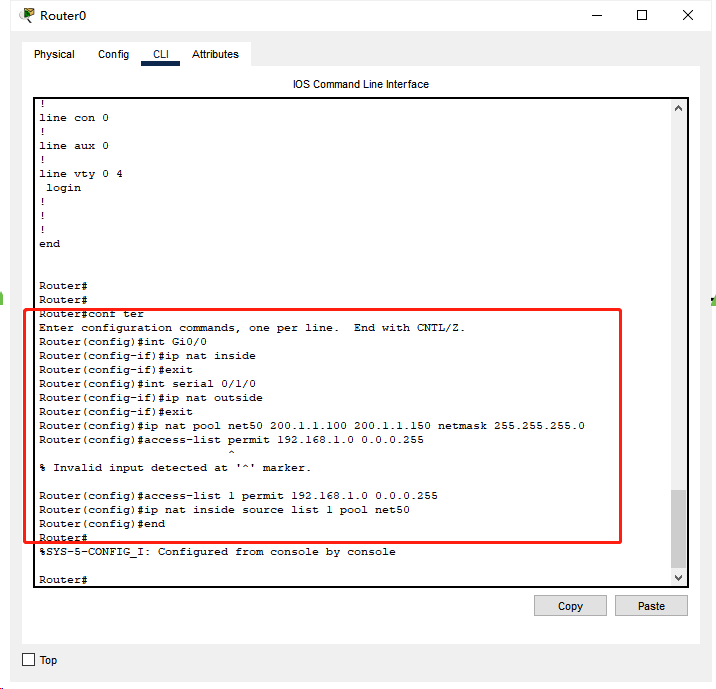
查看R0路由表



查看R1路由表

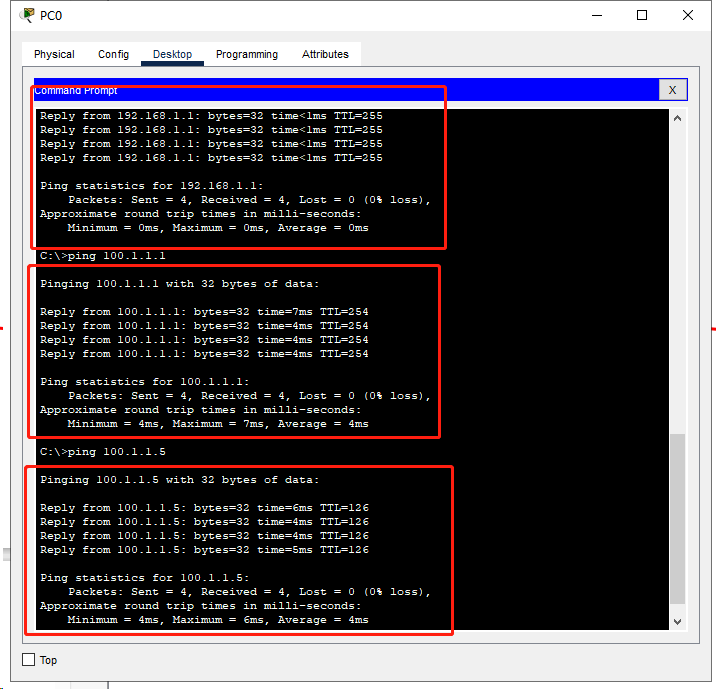


**（5）在R0上配置NAT**

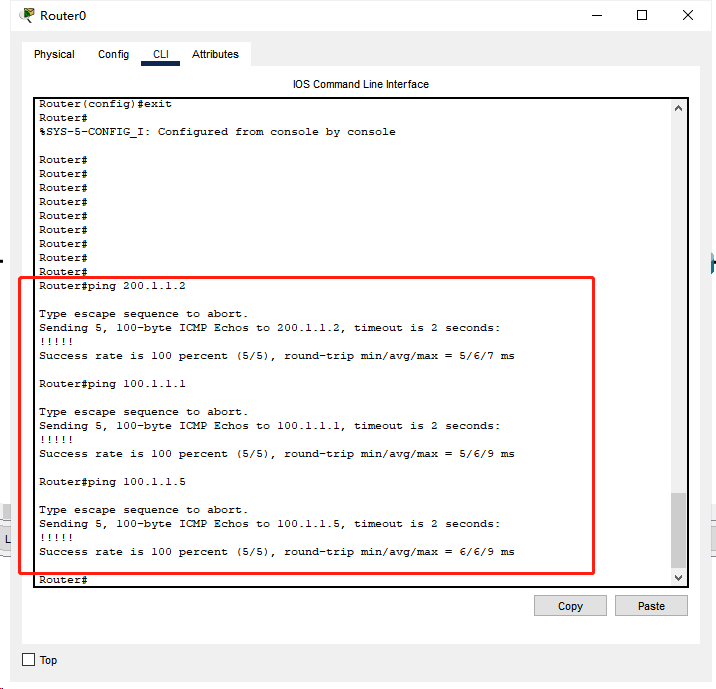


**（6）验证测试**

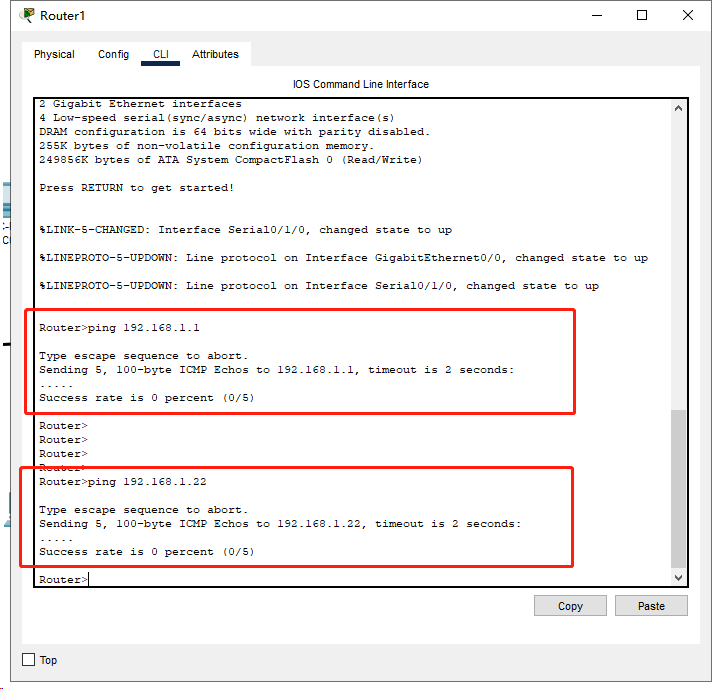
PC ping 各个节点



R0 ping各个节点

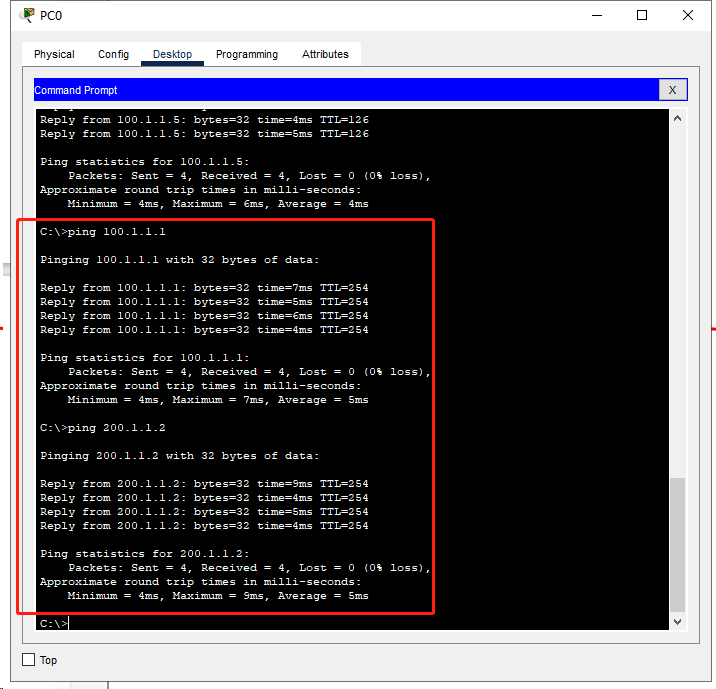


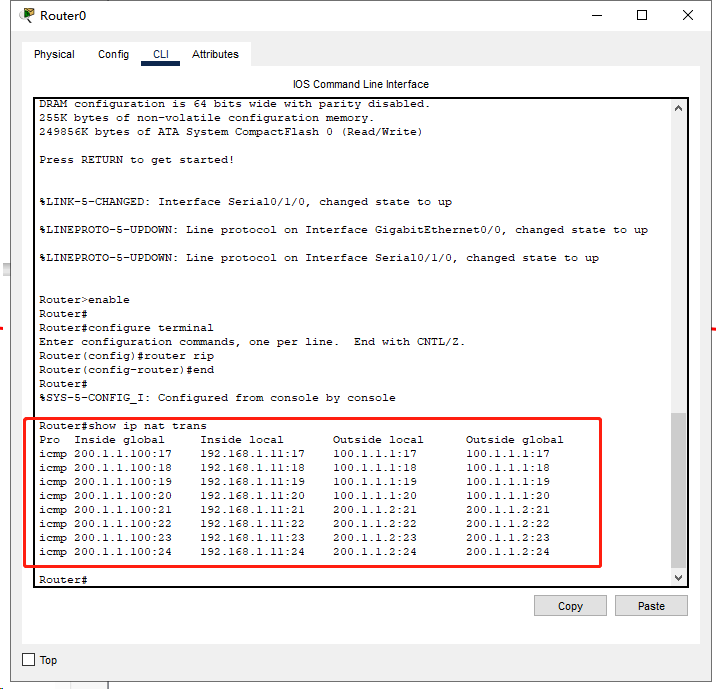
R1 ping各个节点



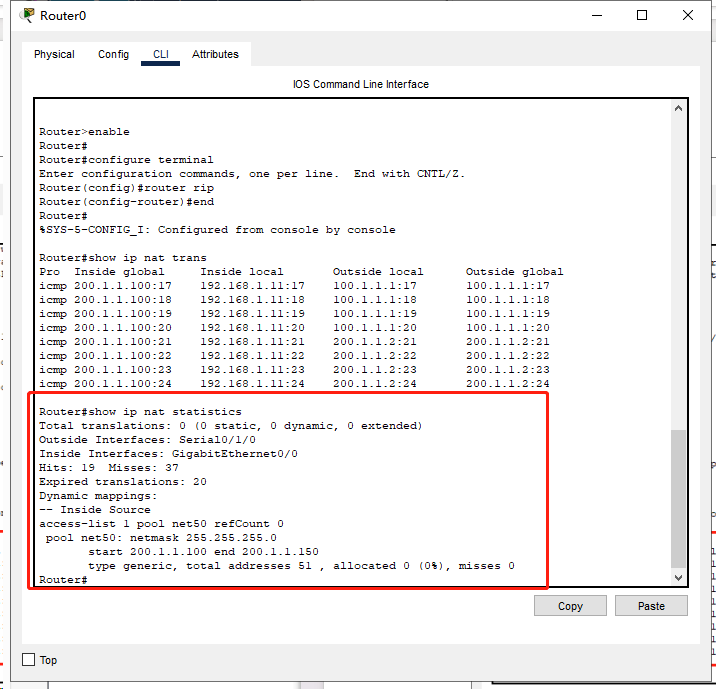
**（7）查看配置**

PC ping外部服务器，查看地址转换情况





**（8）查看地址转换的统计情况**



**实验数据：**

本次实验无重要实验数据，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：**

由于本次实验未涉及重要的实验数据，因此无需进行数据处理。

**实验结果与分析：**

在这个环节，将针对实验指导书中的部分思考问题进行回答。

**（一）什么情况下使用静态NAT？什么情况下使用动态 NAT？为什么？**

（1）静态NAT使用场景

服务器映射：静态NAT通常用于将特定的私有IP地址映射到一个固定的公有IP地址。这对于需要在互联网上提供服务的服务器是很常见的情况，例如Web服务器、邮件服务器等。

安全性需求：当需要确保内部网络中的特定设备总是使用相同的公有IP地址时，可以使用静态NAT。这有助于提高网络的安全性，因为外部网络无法直接了解内部网络中的实际IP地址。

特殊应用场景：在某些特殊的网络架构中，可能需要固定的一对一映射，这时静态NAT是比较合适的选择。

（2）动态NAT使用场景

共享公共IP地址：动态NAT通常用于将多个私有IP地址映射到较小的一组公有IP地址。这样可以实现多个内部设备共享少量的公共IP地址，从而实现节省IP地址资源。

临时连接：当内部网络中的设备需要临时访问互联网时，动态NAT允许它们动态地获得一个可用的公共IP地址。

适应网络变化：动态NAT适用于内部网络中IP地址分配需要根据网络负载或其他条件动态变化的情况。

**（二）是否需要将内网所在网段或路由在外部网络的边界路由器上共享？为什么？**

尽可能减少在外部网络的边界路由器上共享内网网段或路由信息。

信息泄露风险：将内网网段或路由信息共享到外部网络可能增加信息泄露的风险。知晓内部网络结构的信息可能使得潜在攻击者更容易进行目标识别和网络侦察。

攻击表面减小：限制在外部网络共享内网路由信息可以减小网络的攻击表面。攻击者需要更多的努力来了解网络拓扑，减少了潜在的攻击机会。

内网隔离：通过限制在边界路由器上共享内网路由信息，可以更好地实现内外网的隔离。内部网络的拓扑结构不被外部网络直接知晓，有助于提高整体网络的安全性。

防范网络扫描：外部网络如果能够知道内部网络的路由信息，可能会更容易进行网络扫描，进而发现潜在的攻击目标。限制共享有助于减少这类潜在的威胁。

安全策略实施：内外网之间的安全策略更容易实施和维护，因为外部网络无法直接了解内部网络的结构和地址。