**西安电子科技大学**

**组网与运维综合实验 课程实验报告**

**实验名称 VPN与NAT协议分析**

网络与信息安全 学院 2118021 班

成 绩

姓名 盖乐 学号 21009200991

同作者

实验日期 2023 年 11 月 29 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# VPN与NAT协议分析

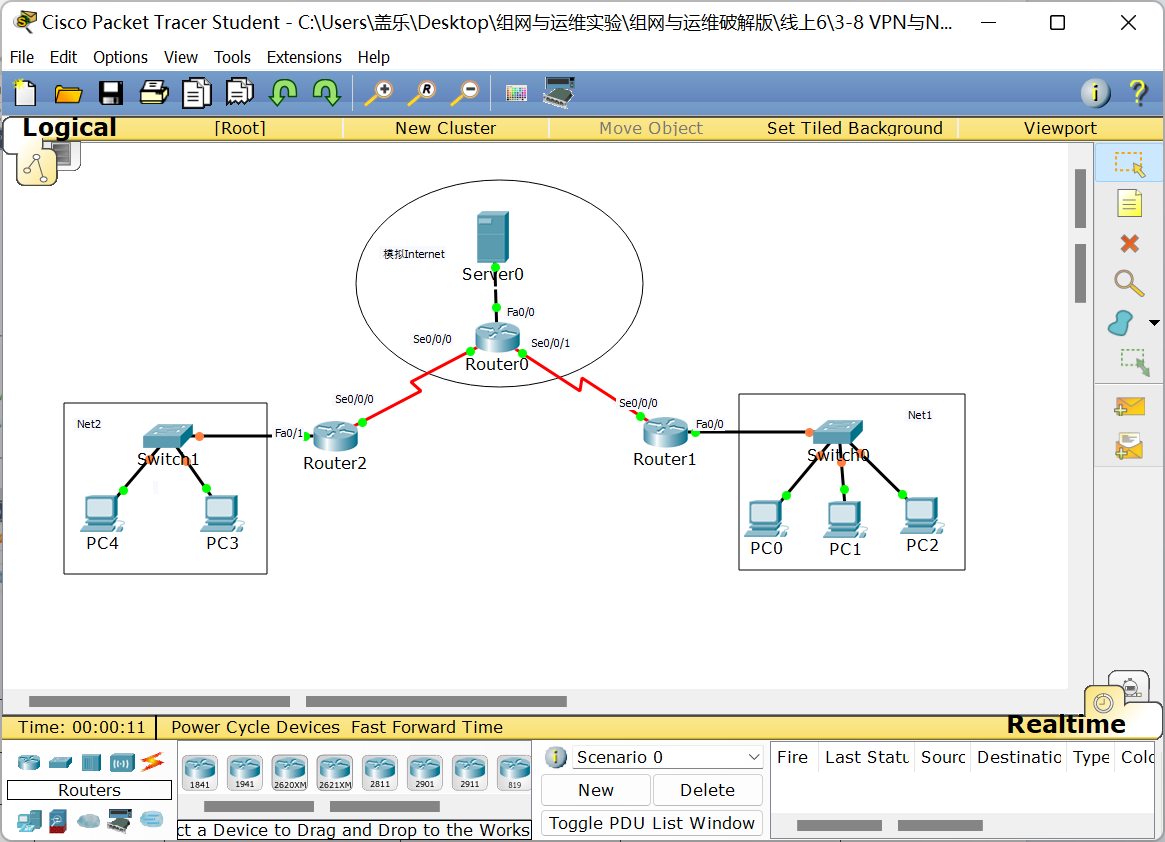
## 一、实验目的

1. 理解VPN使用的IP隧道技术的工作原理。
2. 理解NAT技术的工作原理。

## 二、实验步骤

1. 给出实验中用到的拓扑图

（不能从老师的资料中截图，从自己的界面里截图）



1. 给出实验中使用的IP配置表

（不能从老师的资料中截图，自己制表）

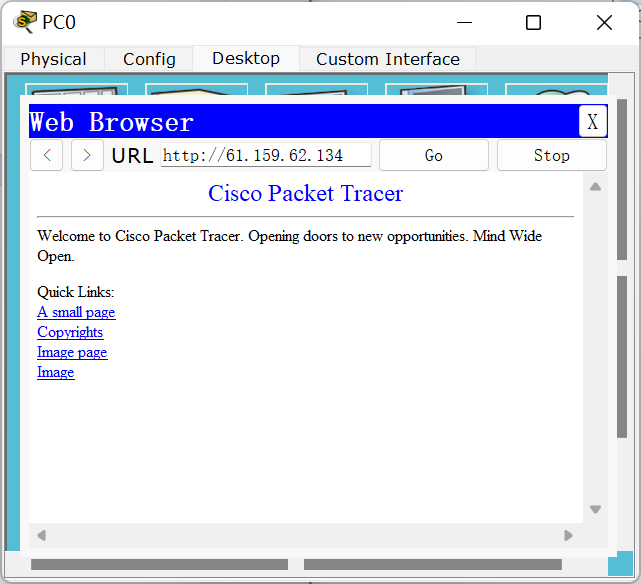
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 掩码 | 默认网关 |
| PC0 | Fa0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.254 |
| PC1 | Fa0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.254 |
| PC2 | Fa0 | 192.168.1.3 | 255.255.255.0 | 192.168.1.254 |
| PC3 | Fa0 | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 |
| PC4 | Fa0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.254 |
| Router1 | Fa0/0 | 192.168.1.254 | 255.255.255.0 | - |
| Router1 | Se0/0/0 | 158.22.120.34 | 255.255.0.0 | - |
| Router2 | Se0/0/0 | 158.22.120.168 | 255.255.0.0 | - |
| Router2 | Fa0/1 | 61.159.62.12 | 255.0.0.0 | - |
| Server0 | Fa0 | 61.159.62.134 | 255.0.0.0 | 61.159.62.12 |

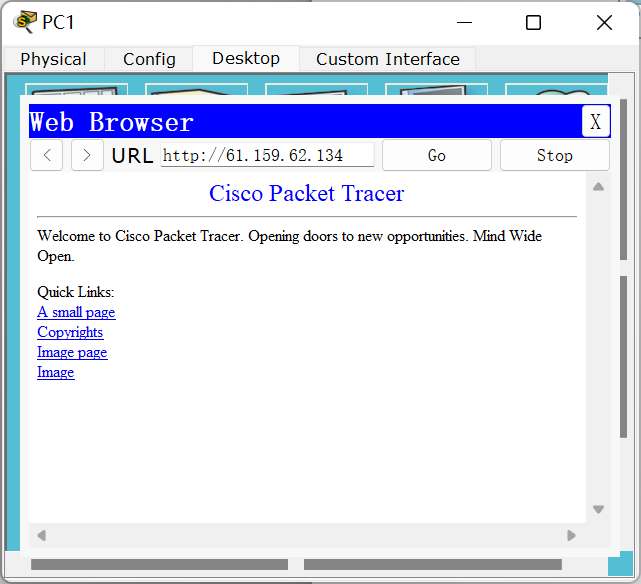
1. 任务一：观察学习NAT的工作原理。

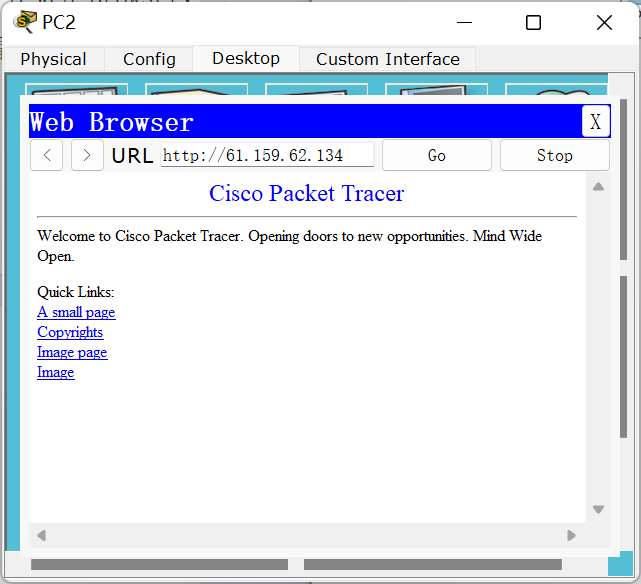
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

步骤一：分别在PC0-PC2中访问Web服务器

• 实时模式下，在PC0、PC1、PC2 Desktop中打开Web Browser，在URL地址栏中输入<http://61.159.62.134>，可以看到打开的网页

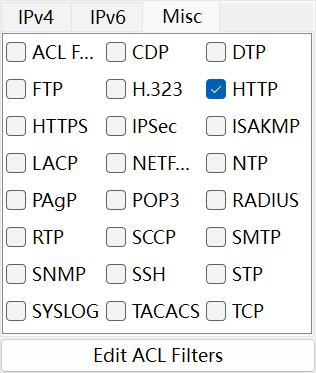




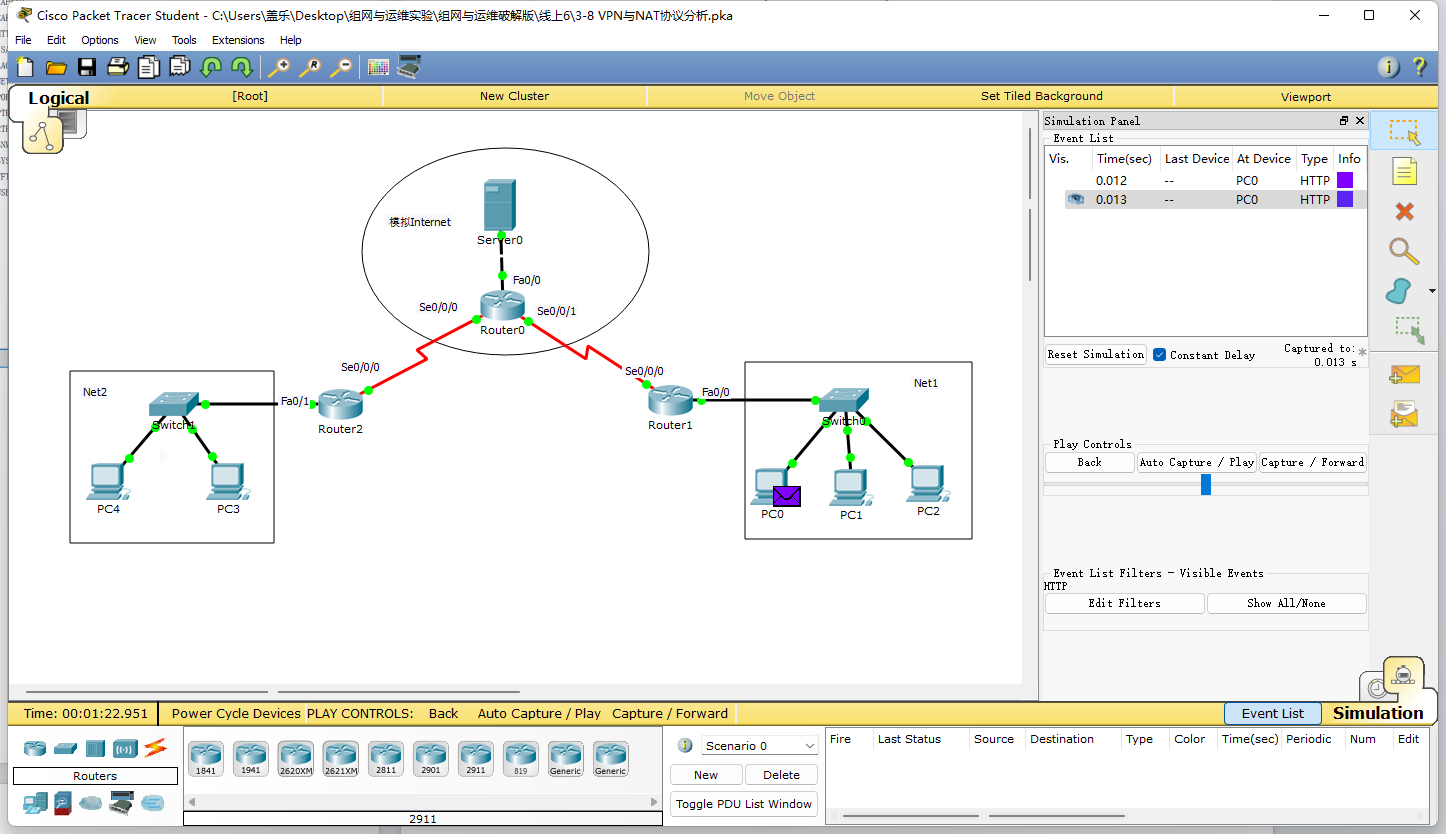


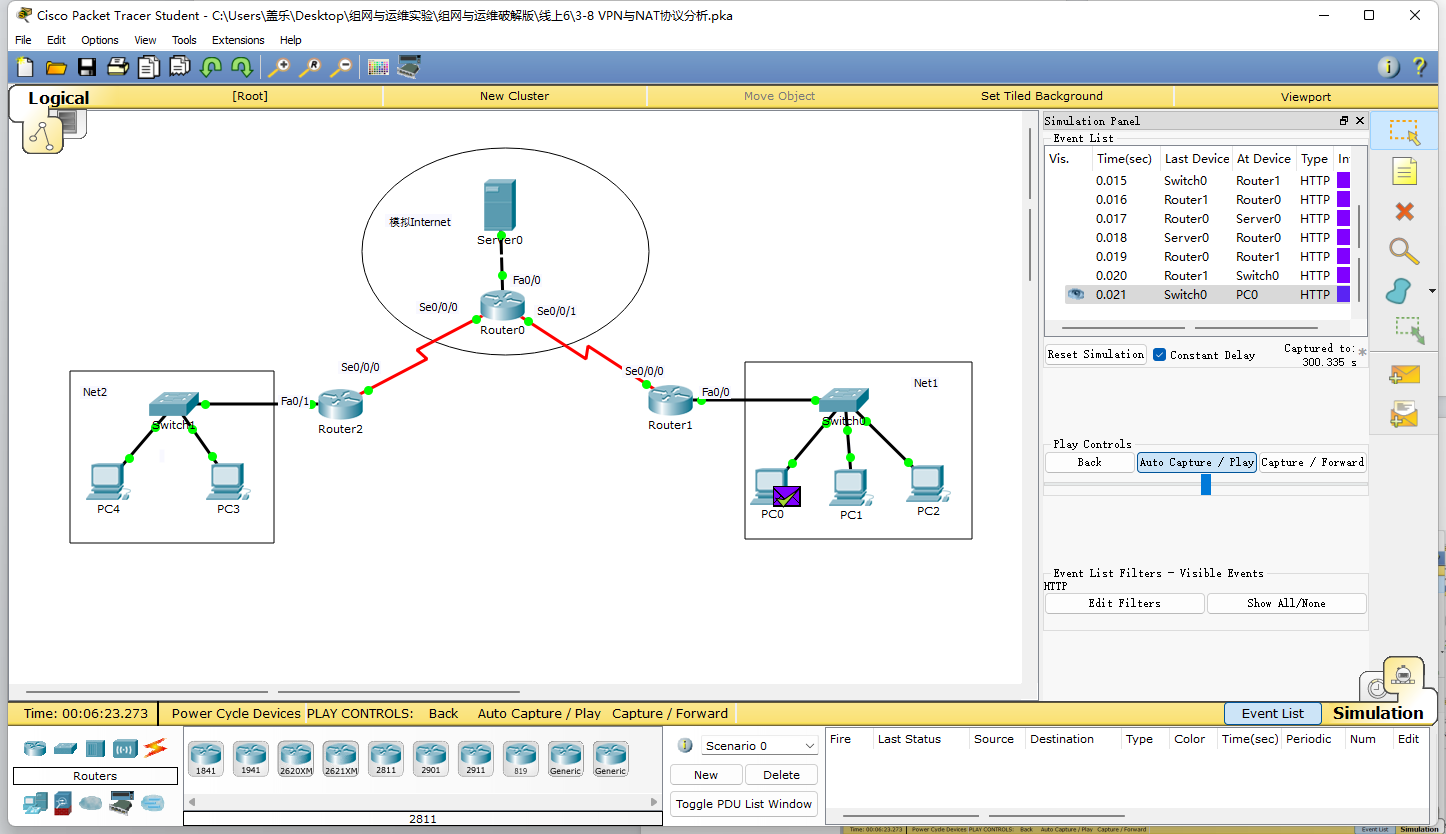
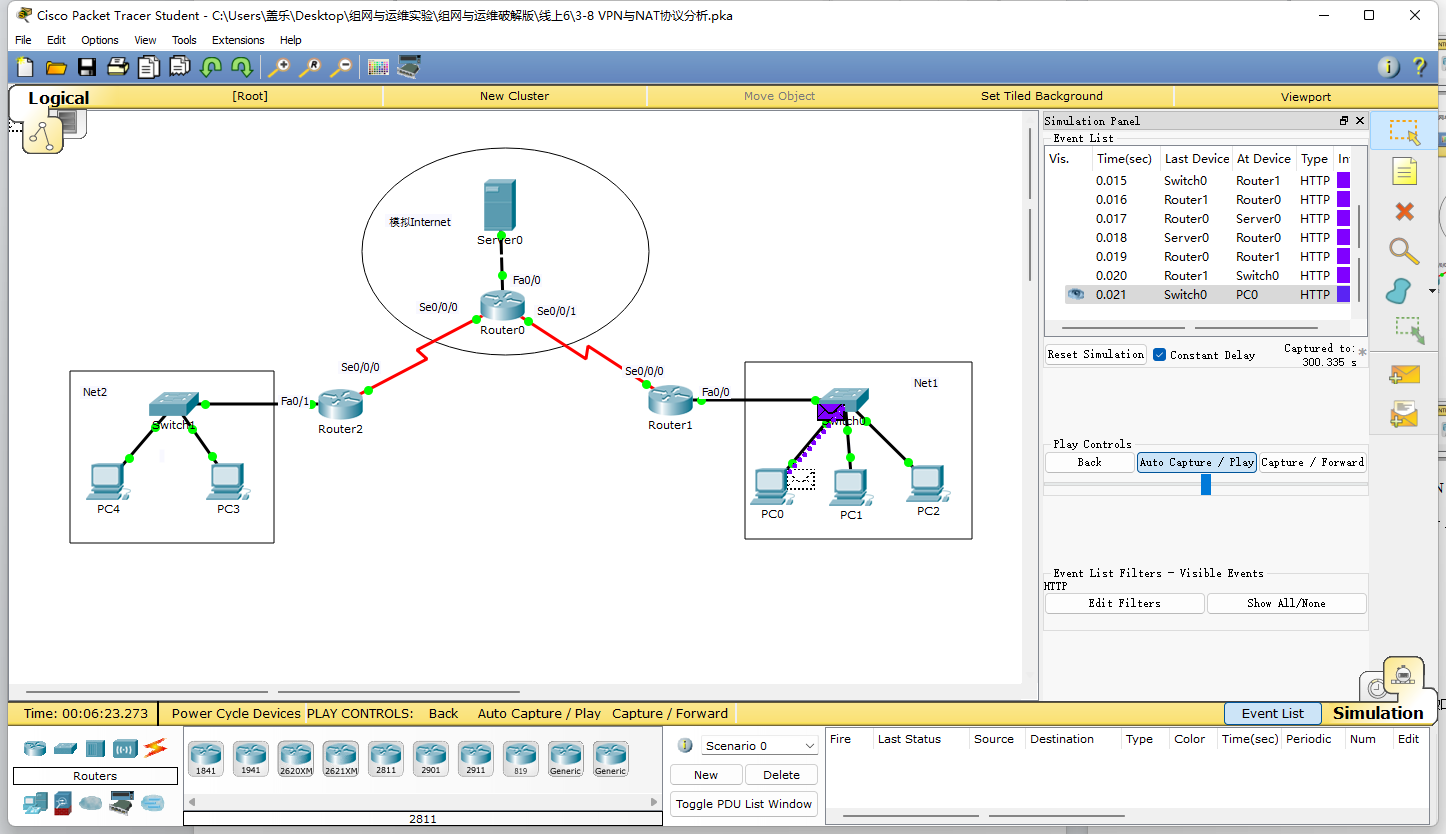
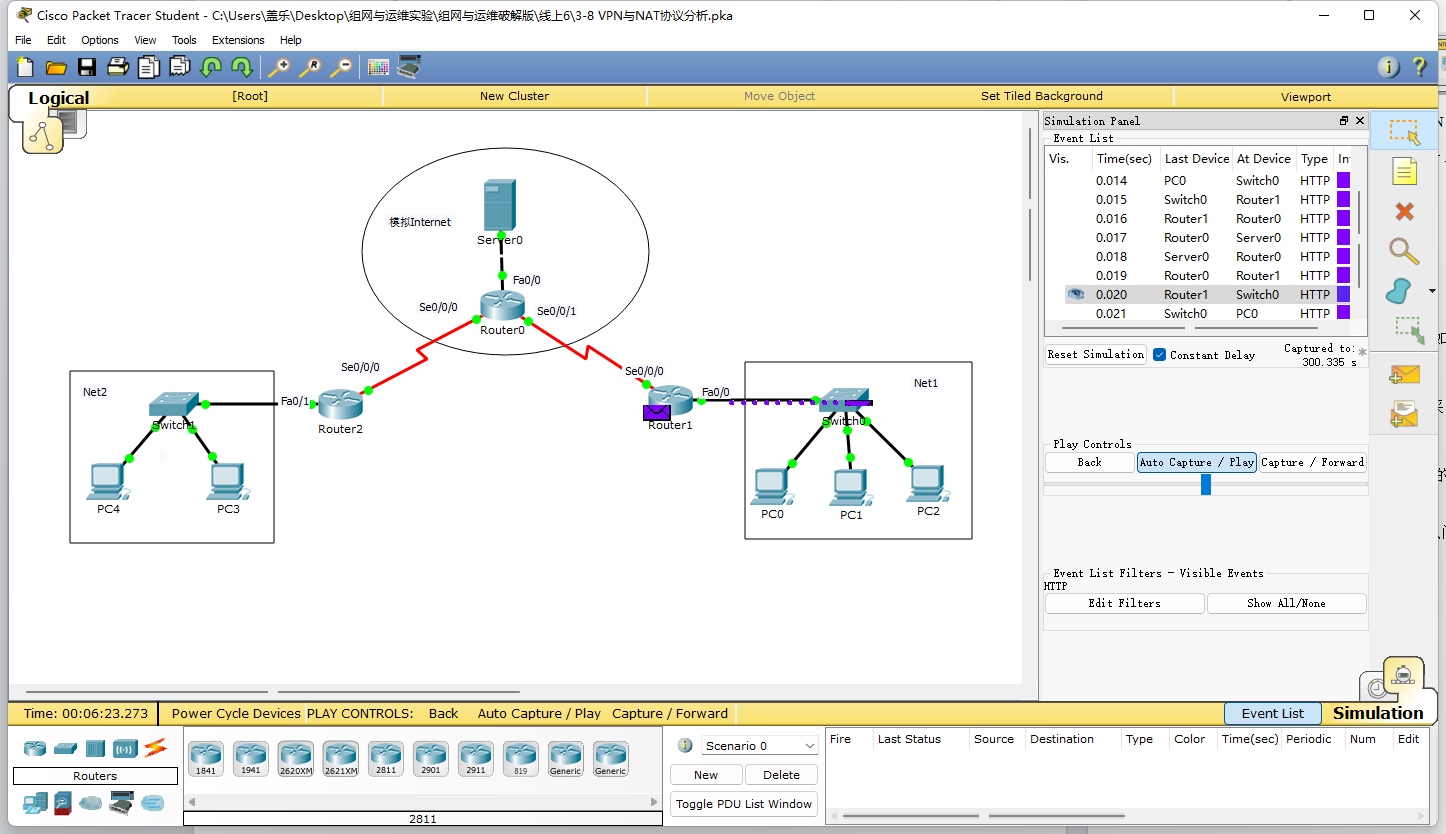
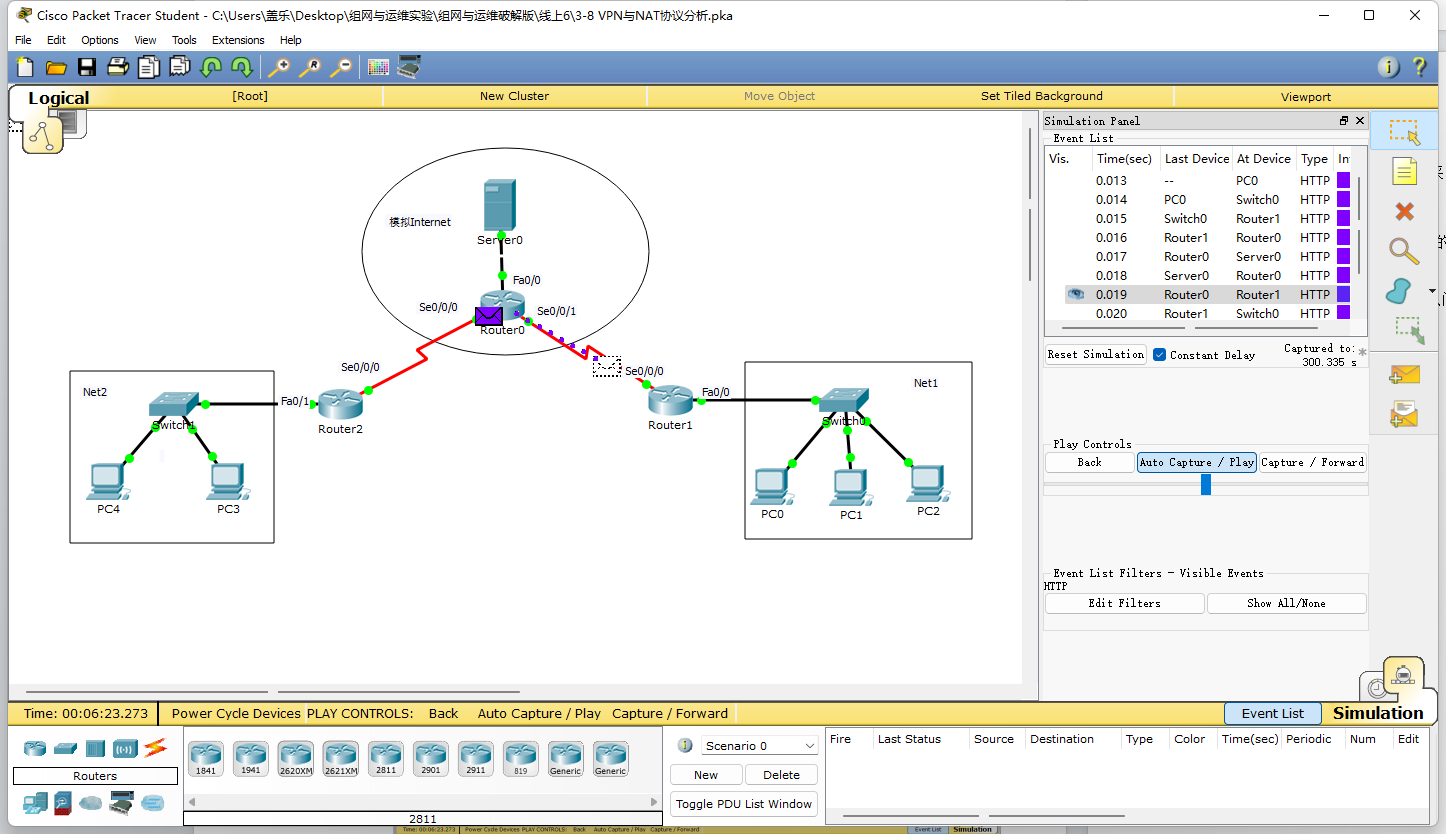
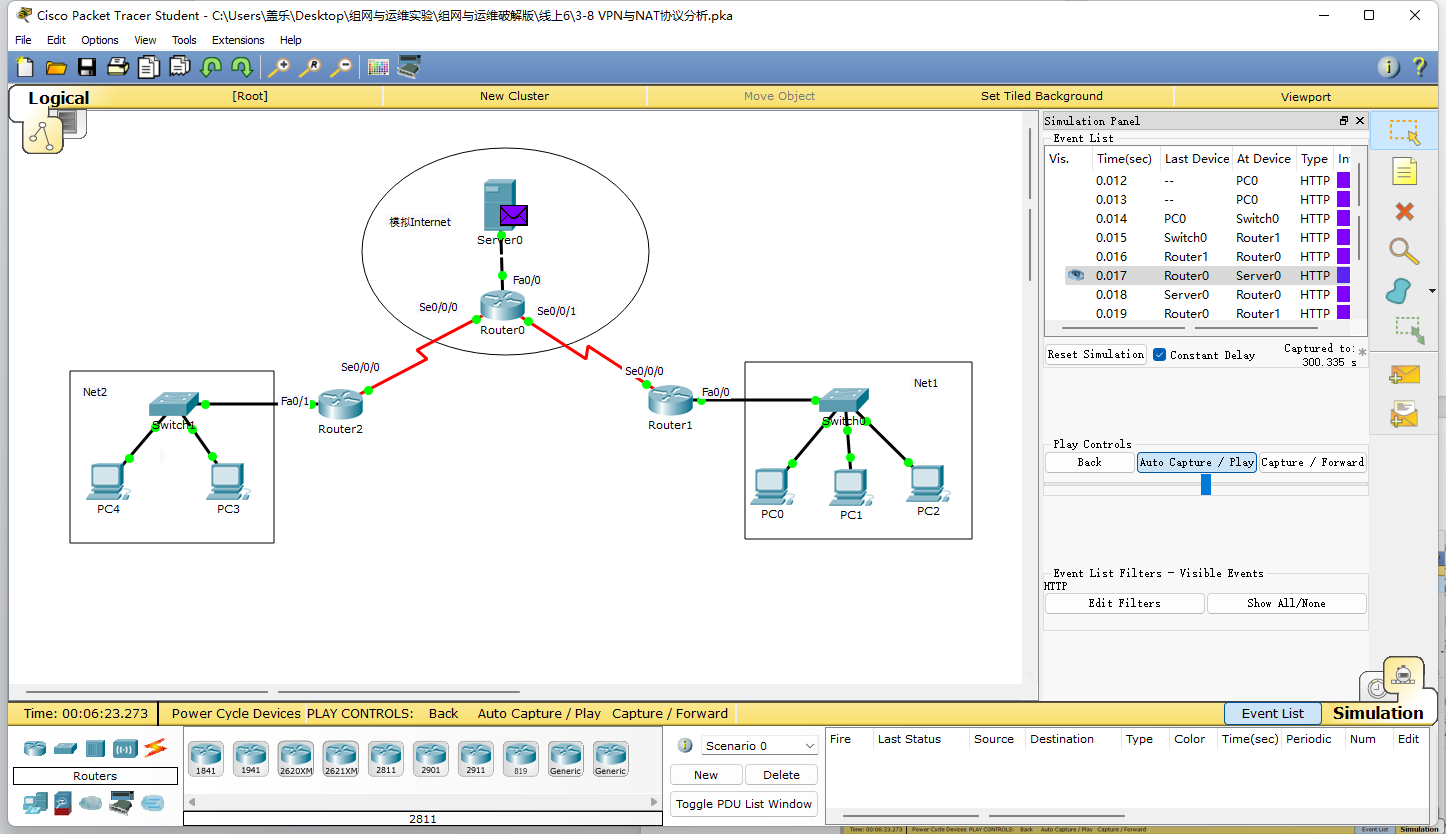
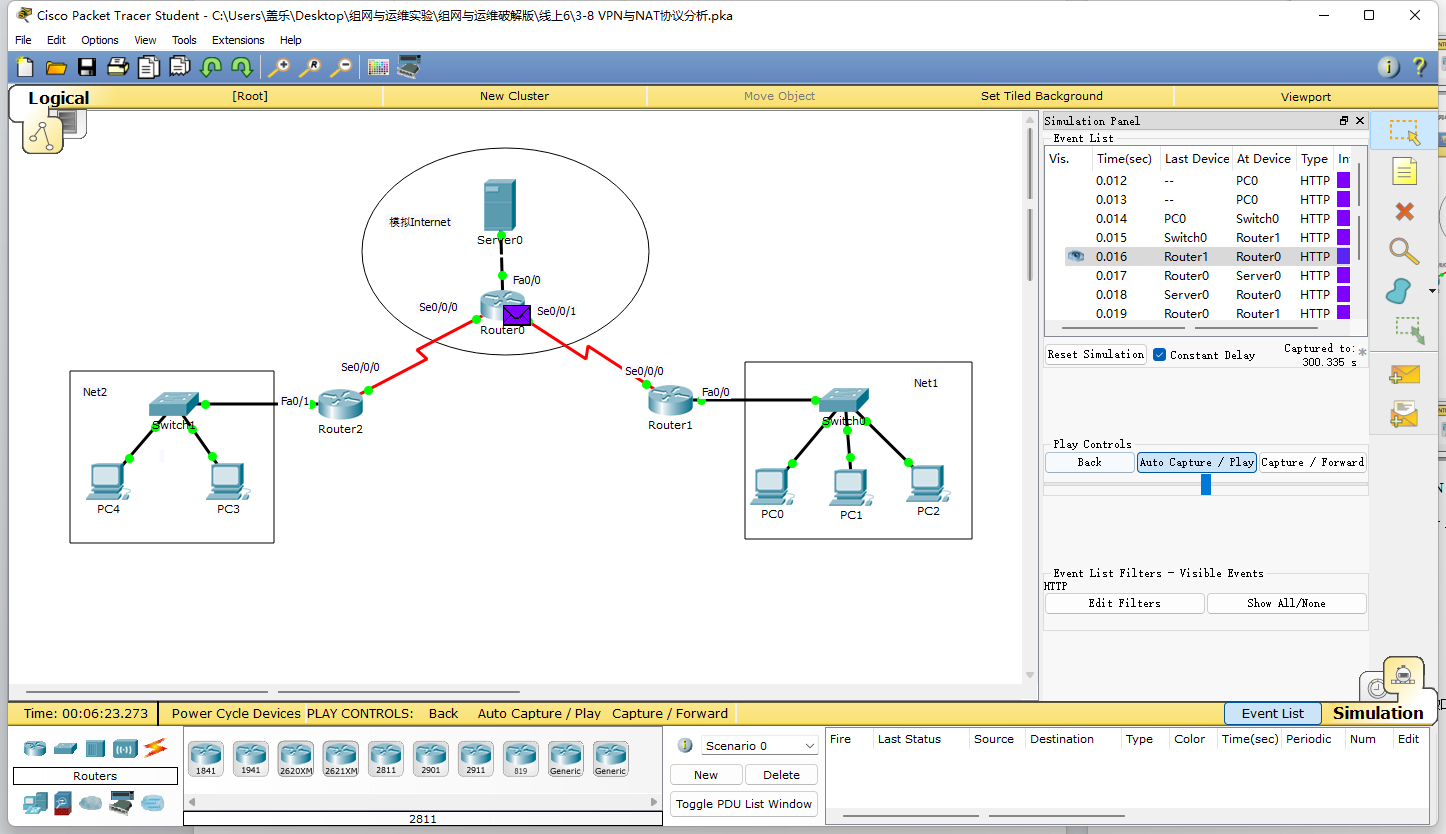
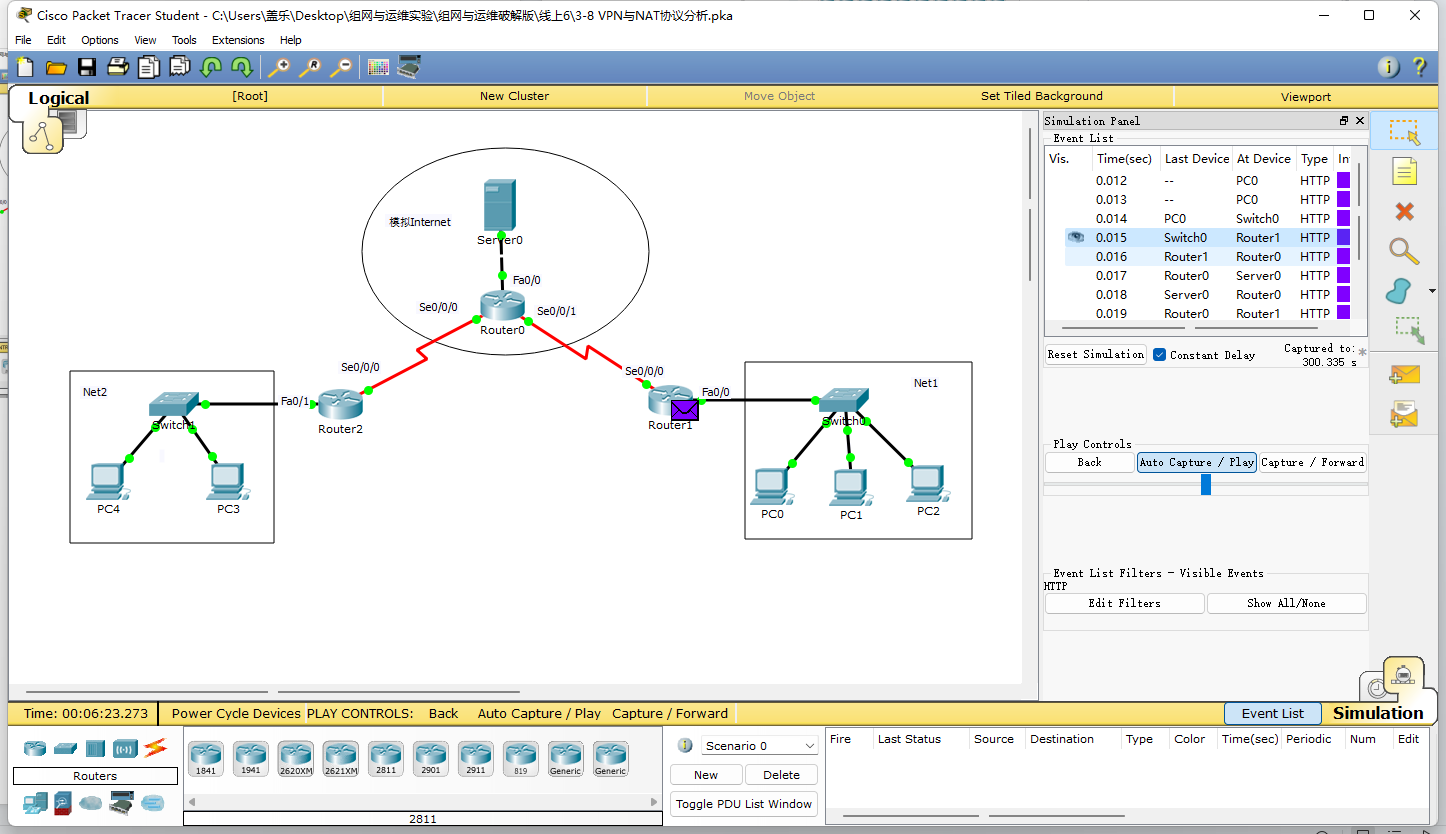
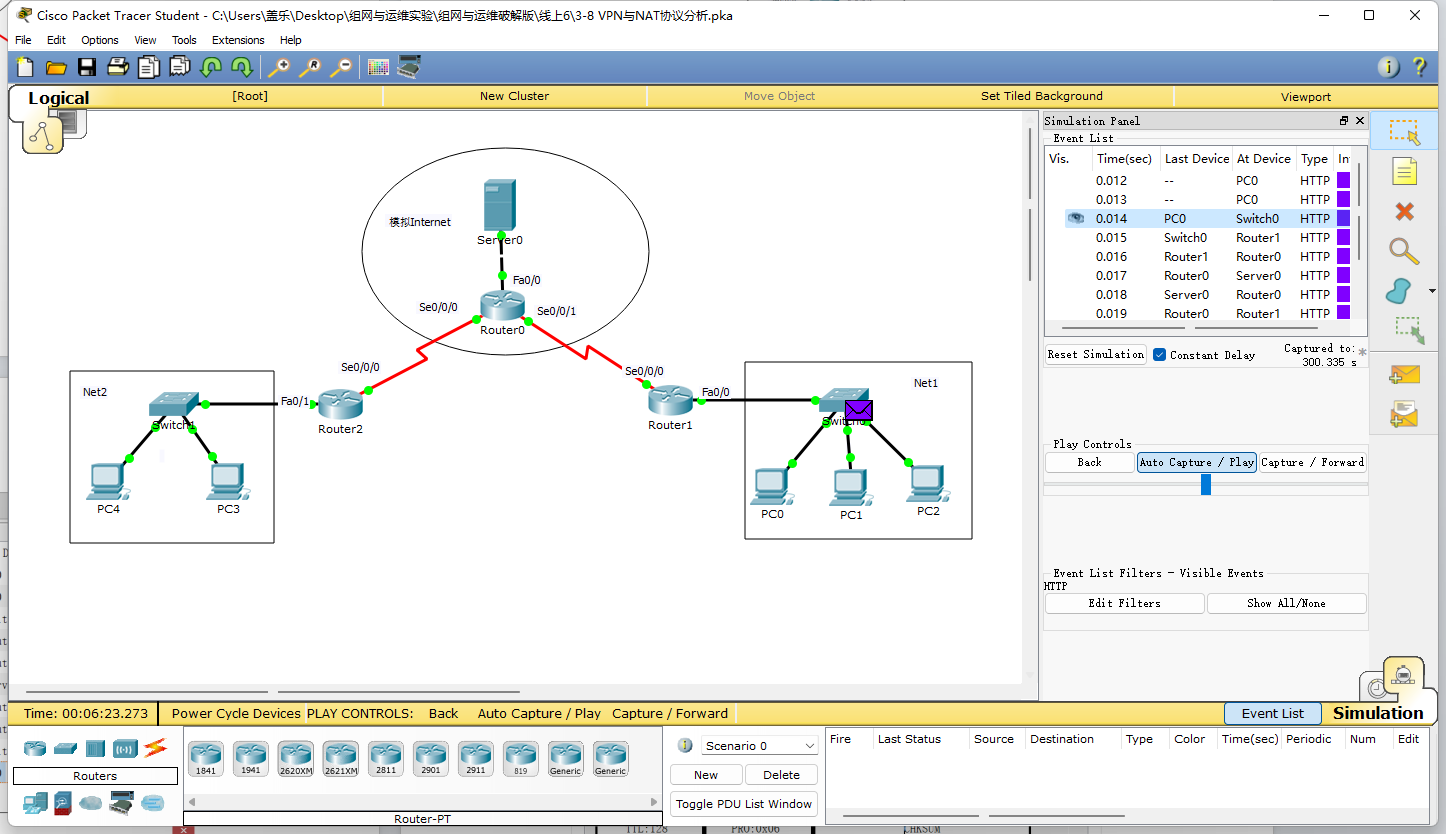
步骤二：观察NAT路由器对数据包的处理方法

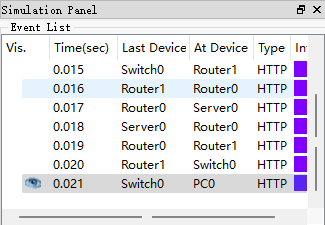
• 进入模拟模式，设置事件列表只显示HTTP事件，观察NAT路由器对数据包的处理方法。



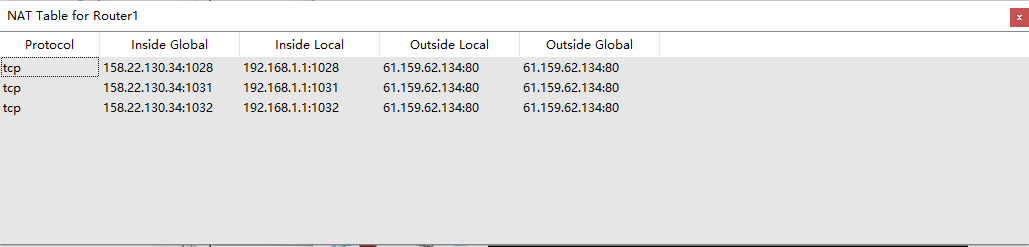
PC0刷新网页，并逐步单击Capture / Forward，以模拟进程，观察到HTTP报文的往返过程。



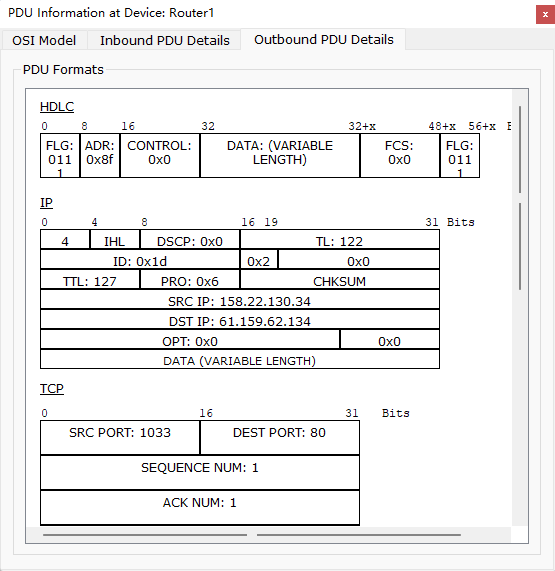
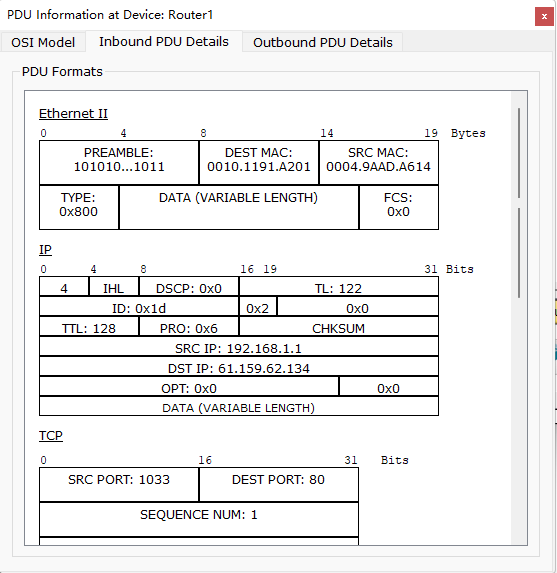




• 使用检查工具打开Router1的NAT 地址转换表。

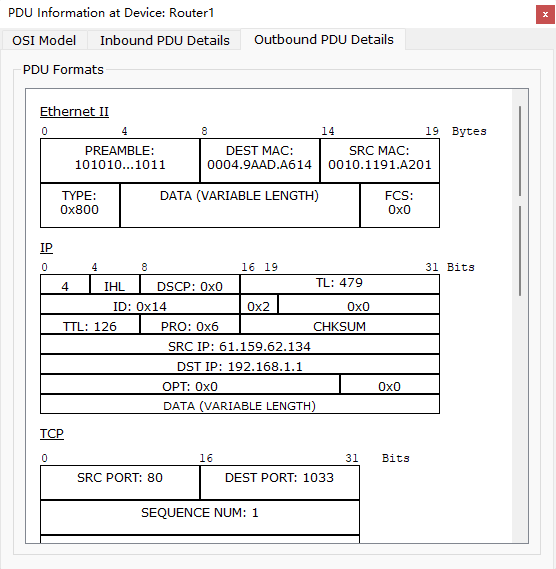
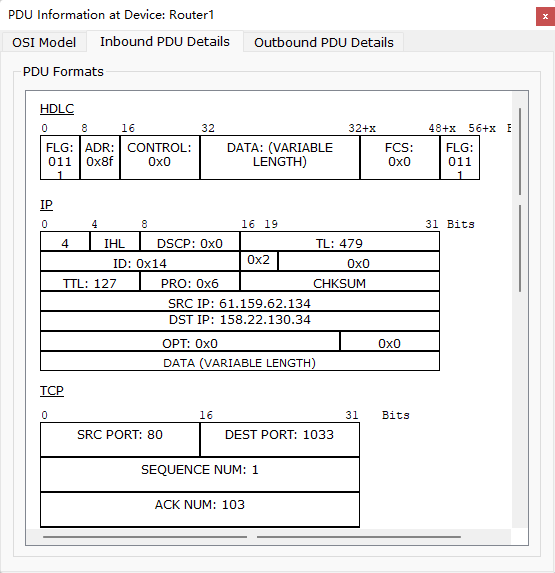


• 观察数据包的处理，点击At Device为Router1的事件，对比Inbound PDU Details和 Outbound PDU Details。



可以看到，Inbound PDU中源IP地址为192.168.1.1，目的IP地址为61.159.62.134；而Outbound源IP地址更改为158.22.130.34，即把PC0的私有地址，改为公有IP地址。而目的 IP 地址不变

回送报文时：



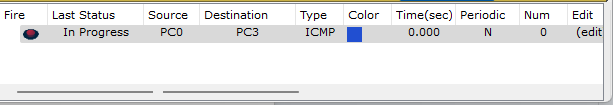
可以看到，Inbound PDU中源IP地址为61.159.62.134，目的IP地址为158.22.130.34；而Outbound源IP地址不变，目的IP地址更改为192.168.1.1，即把公有IP地址改为PC0的私有地址。

1. 任务二：观察学习VPN工作原理。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

步骤一：初始化模拟

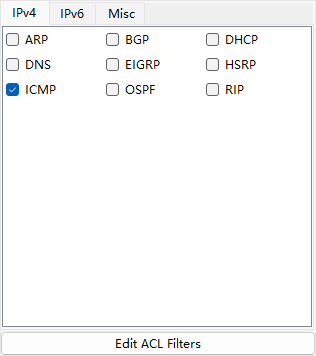
• 实时模式下，添加PC0到PC3的简单PDU



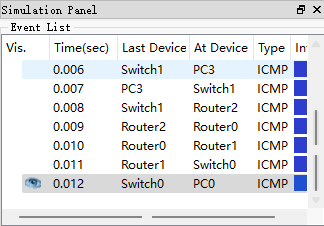
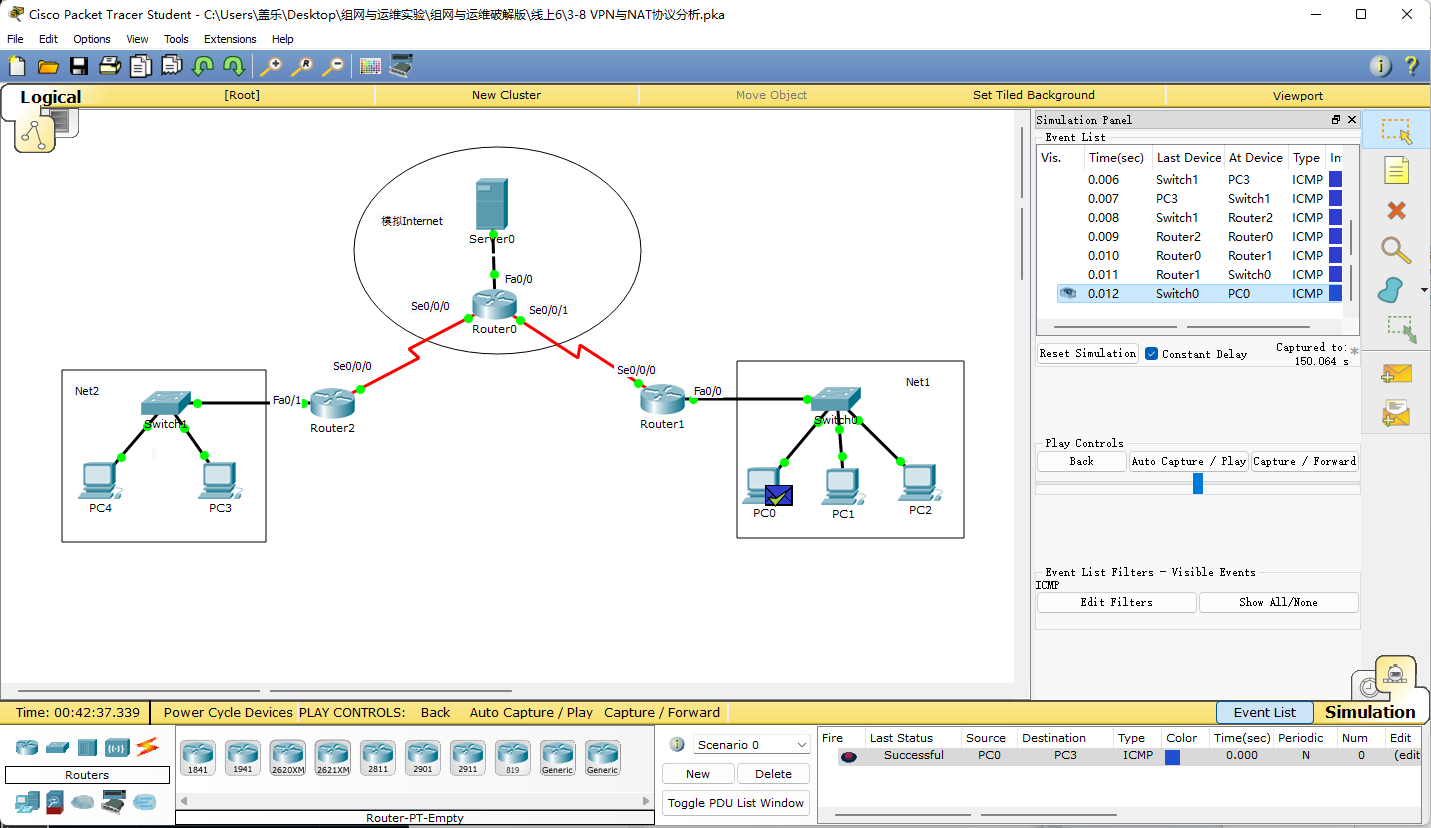
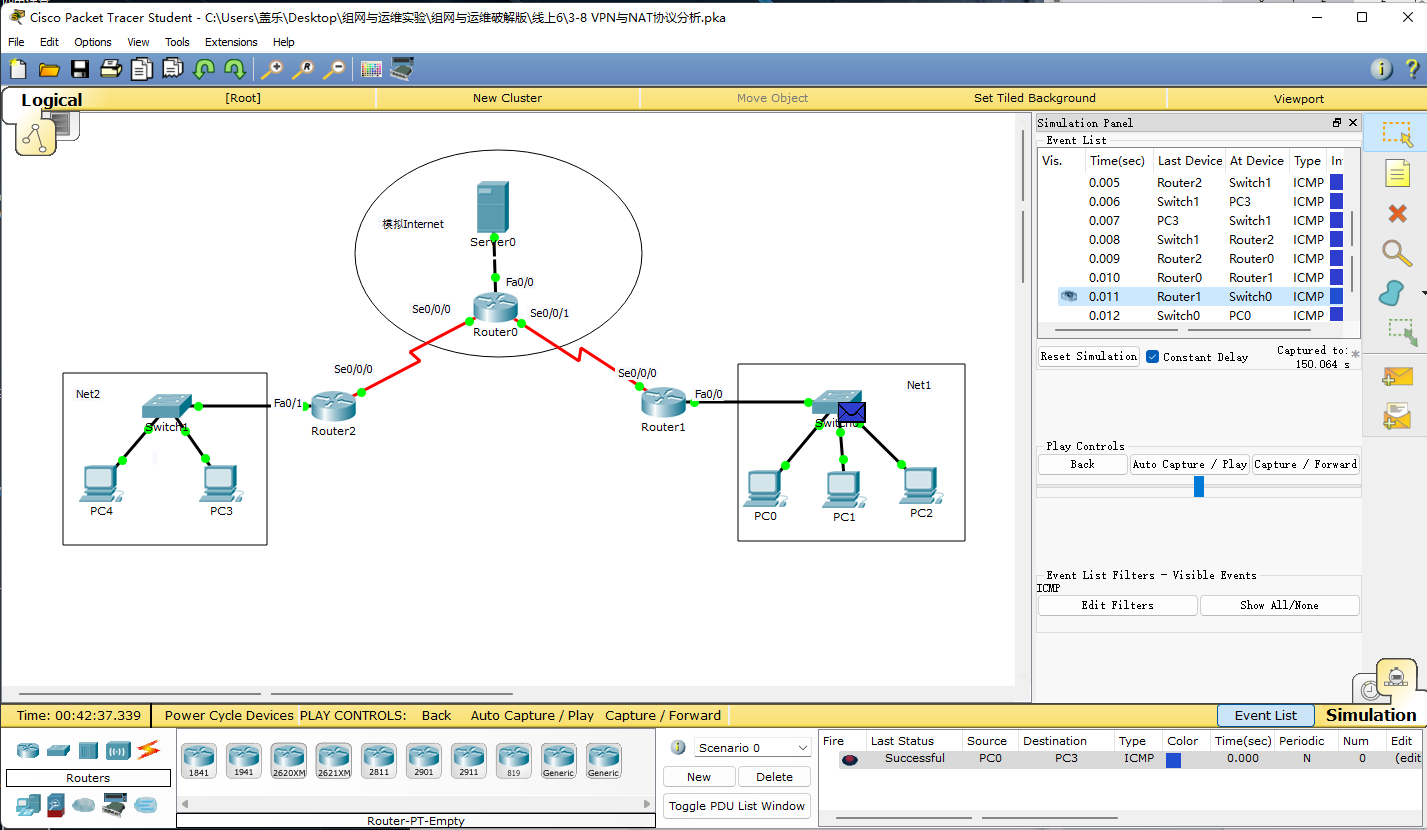
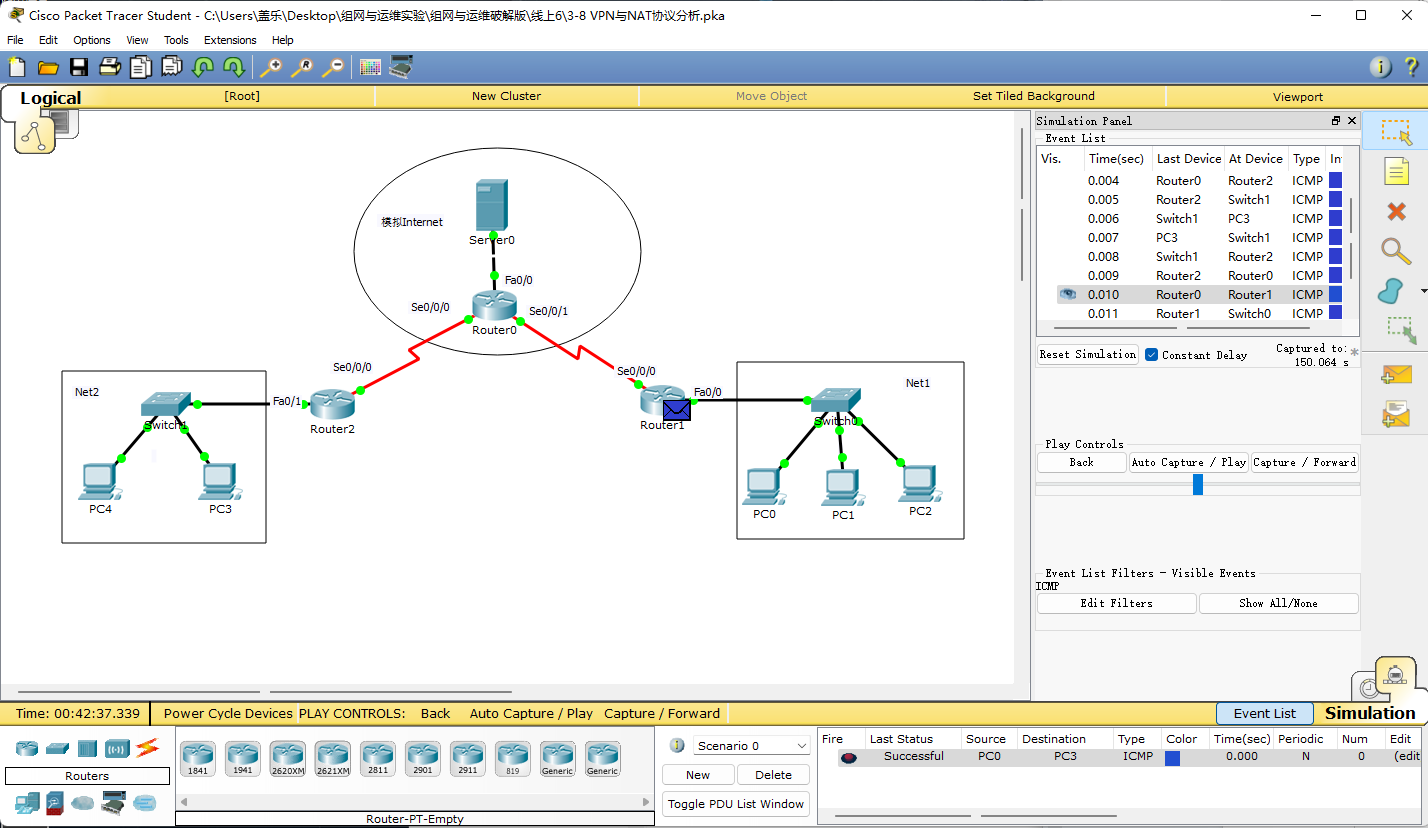
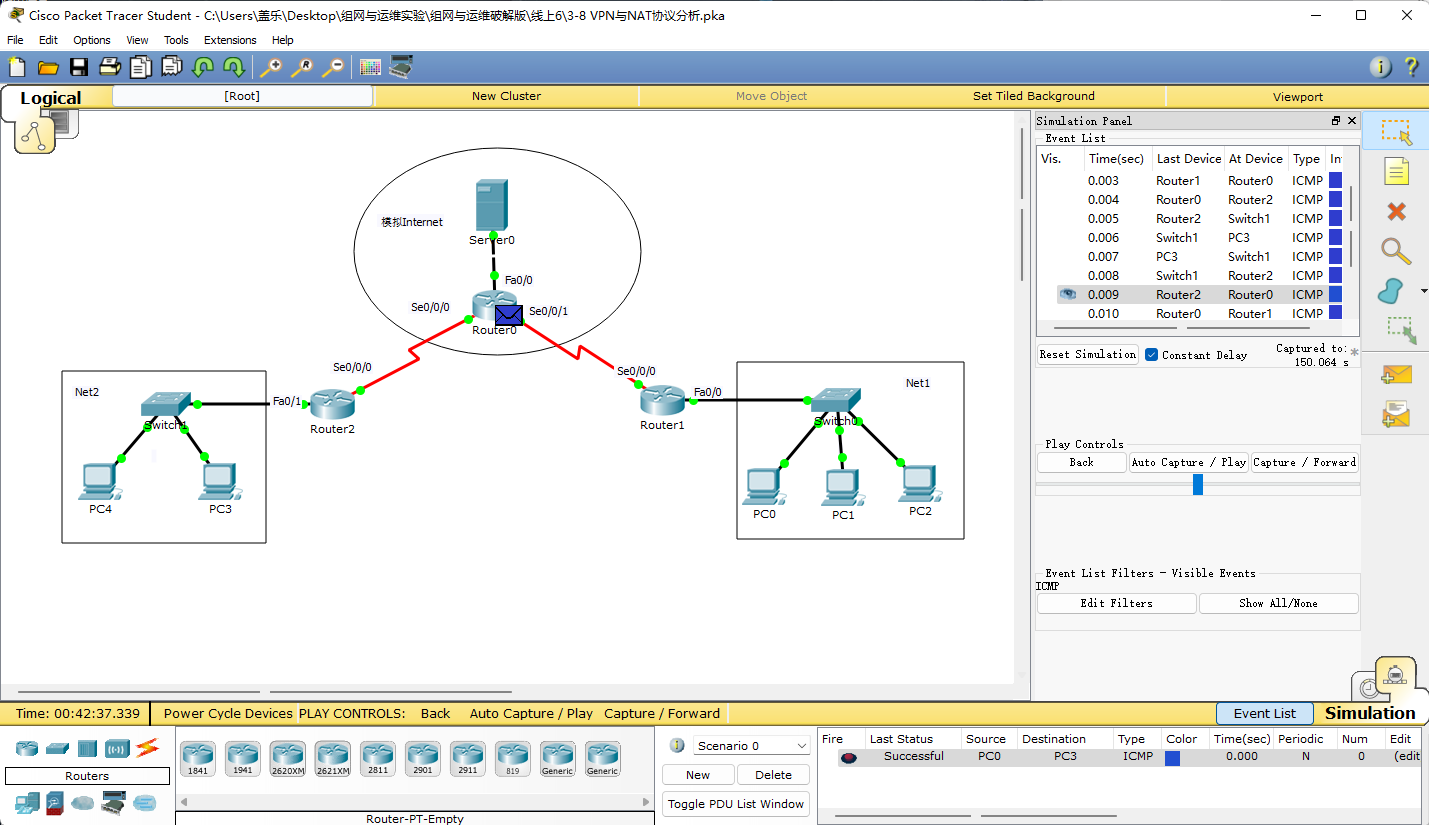
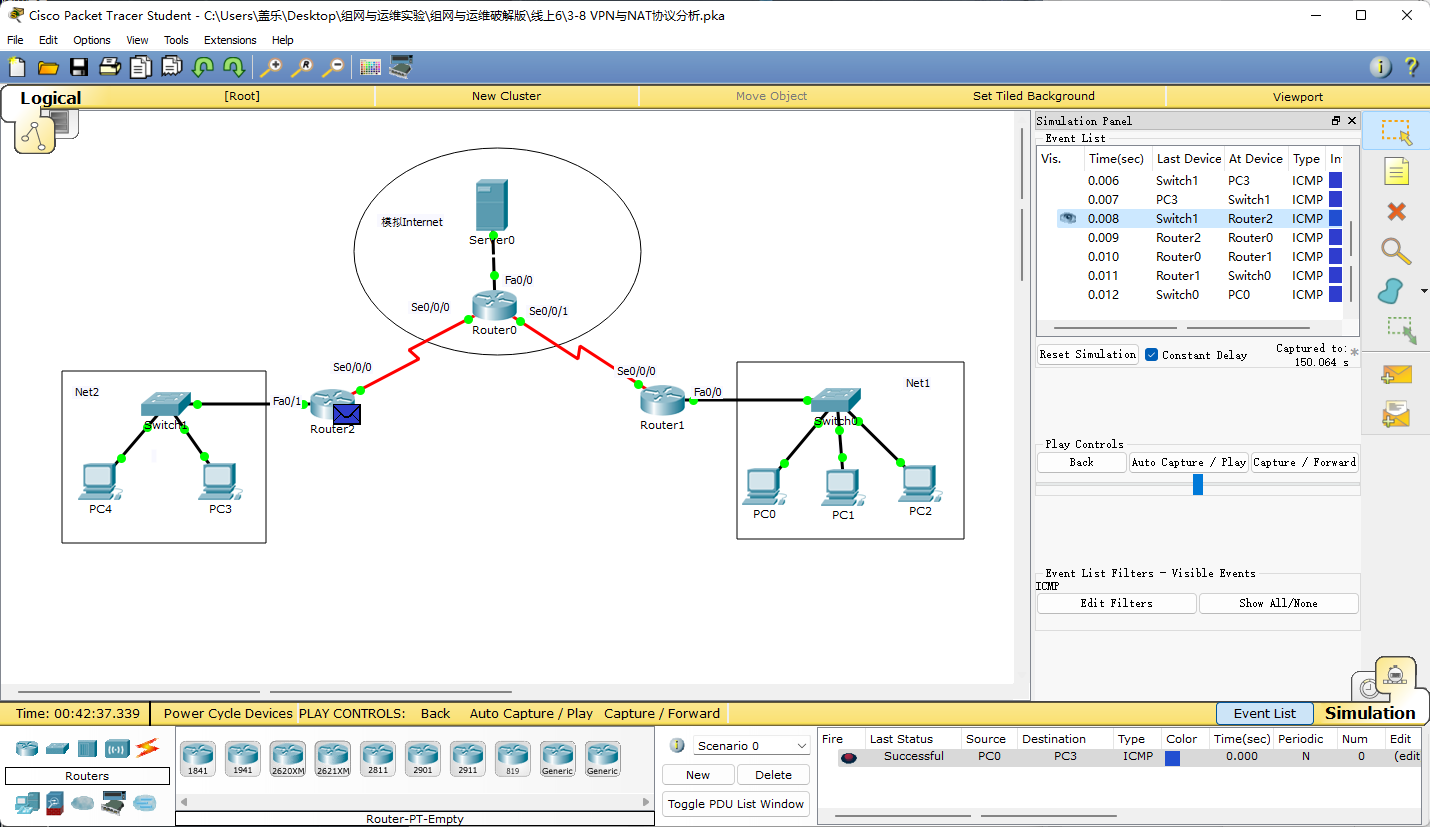
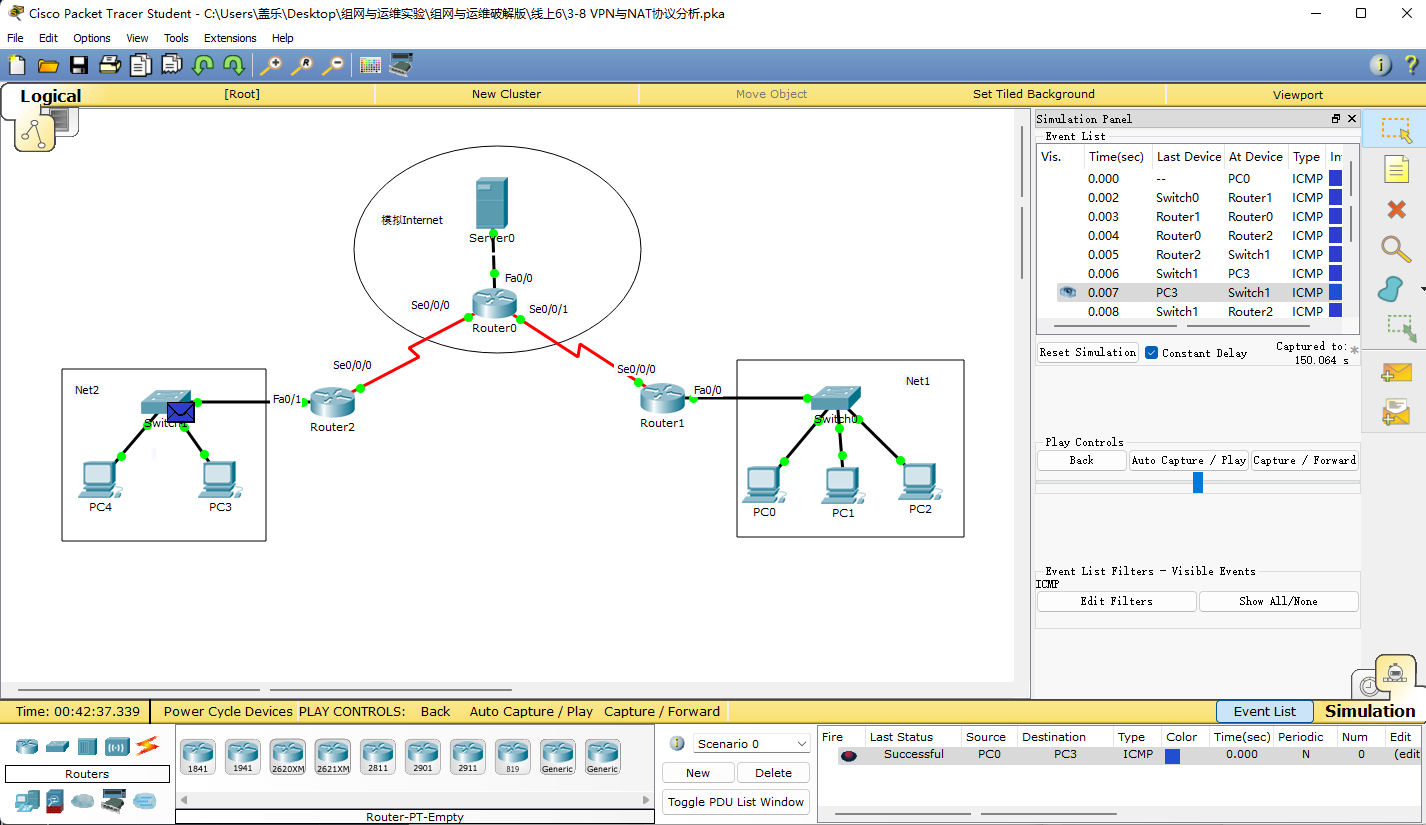
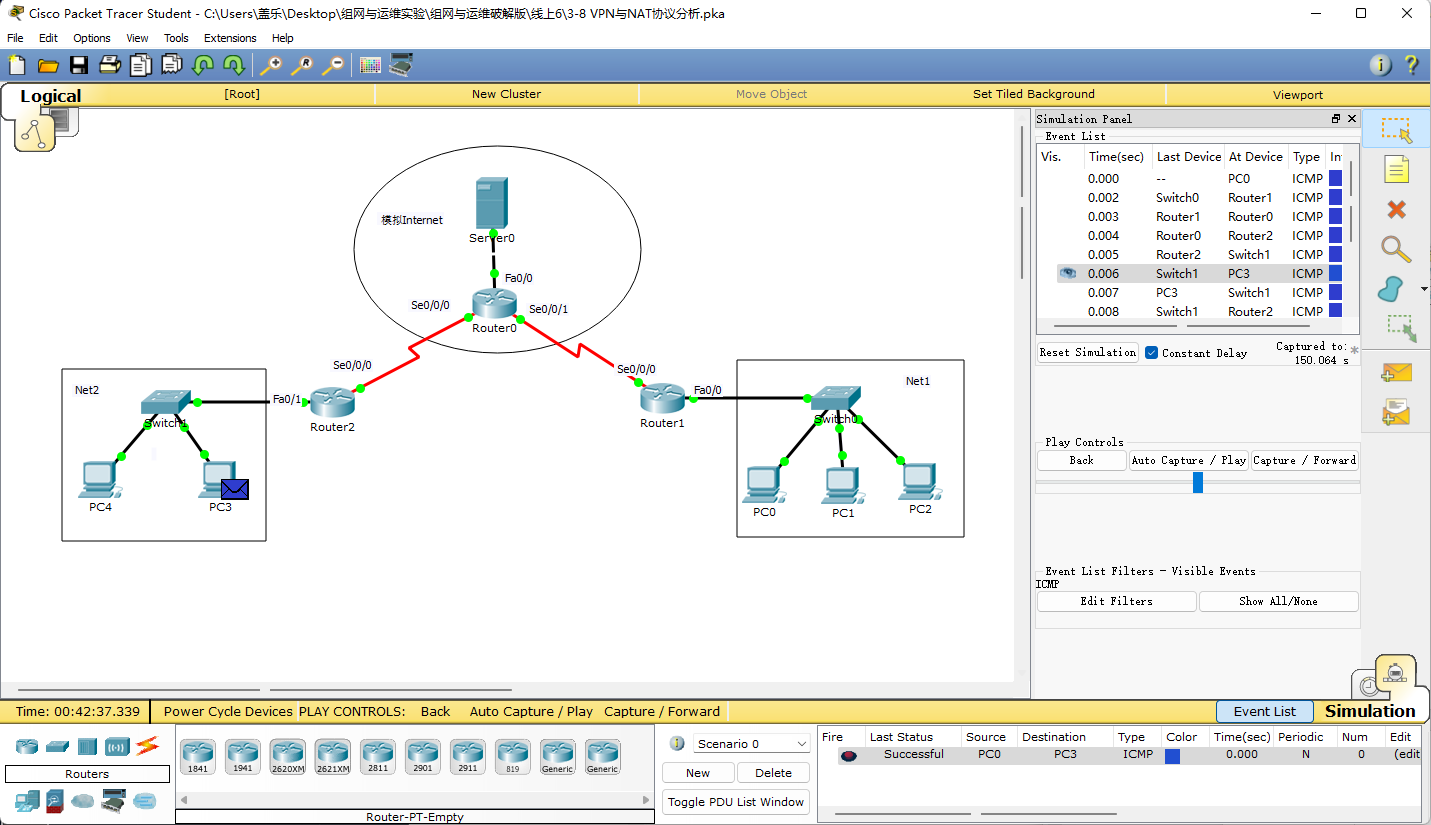
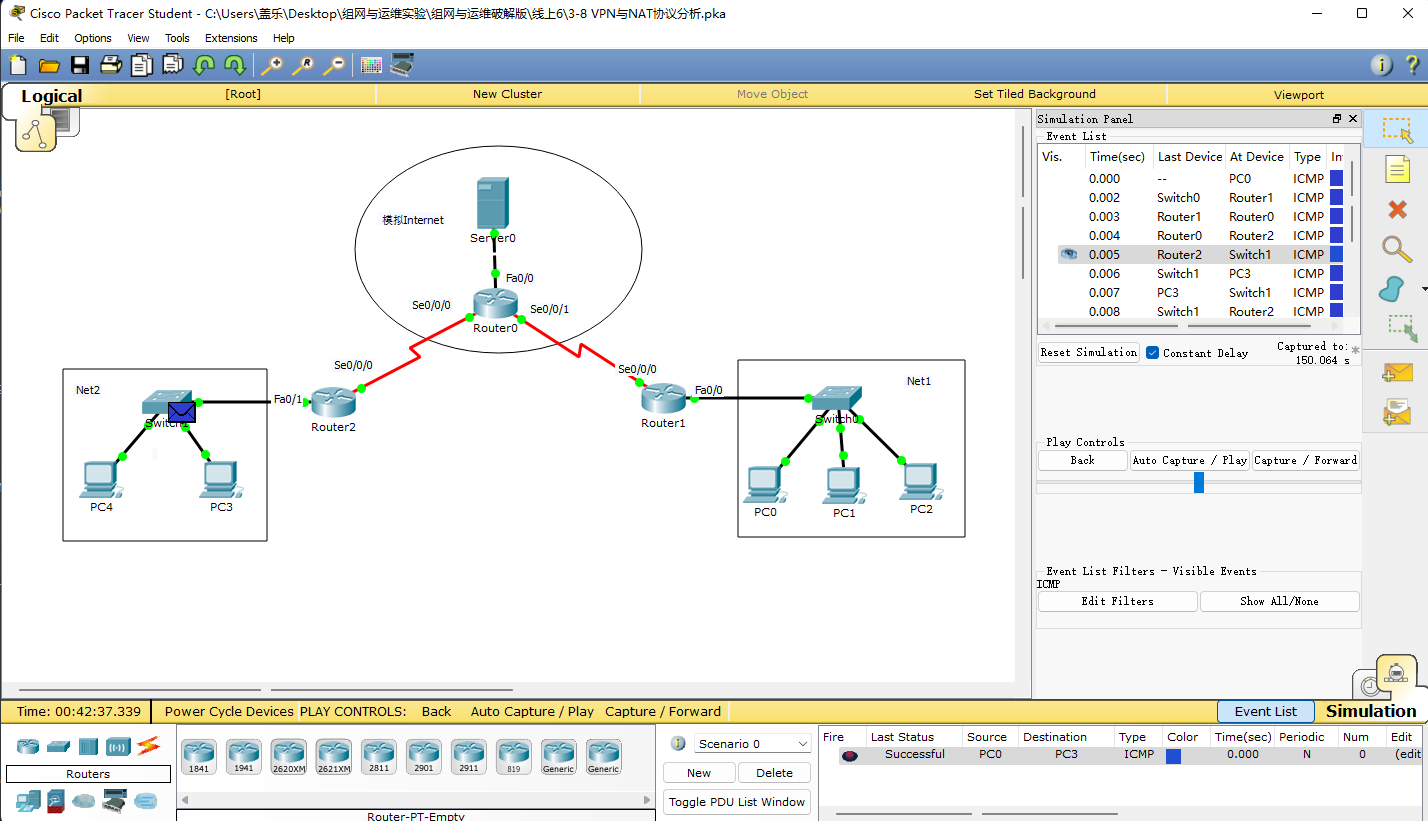
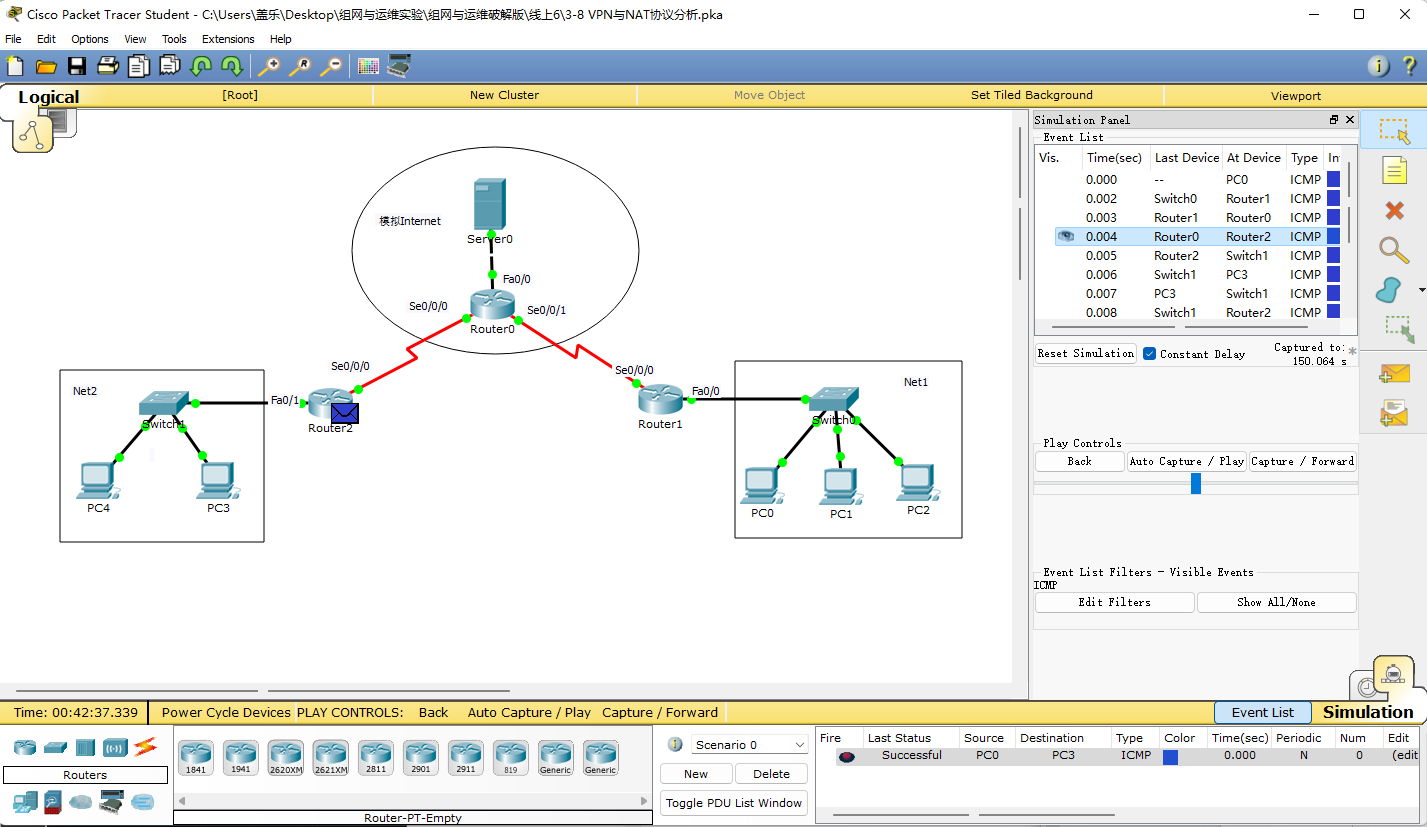
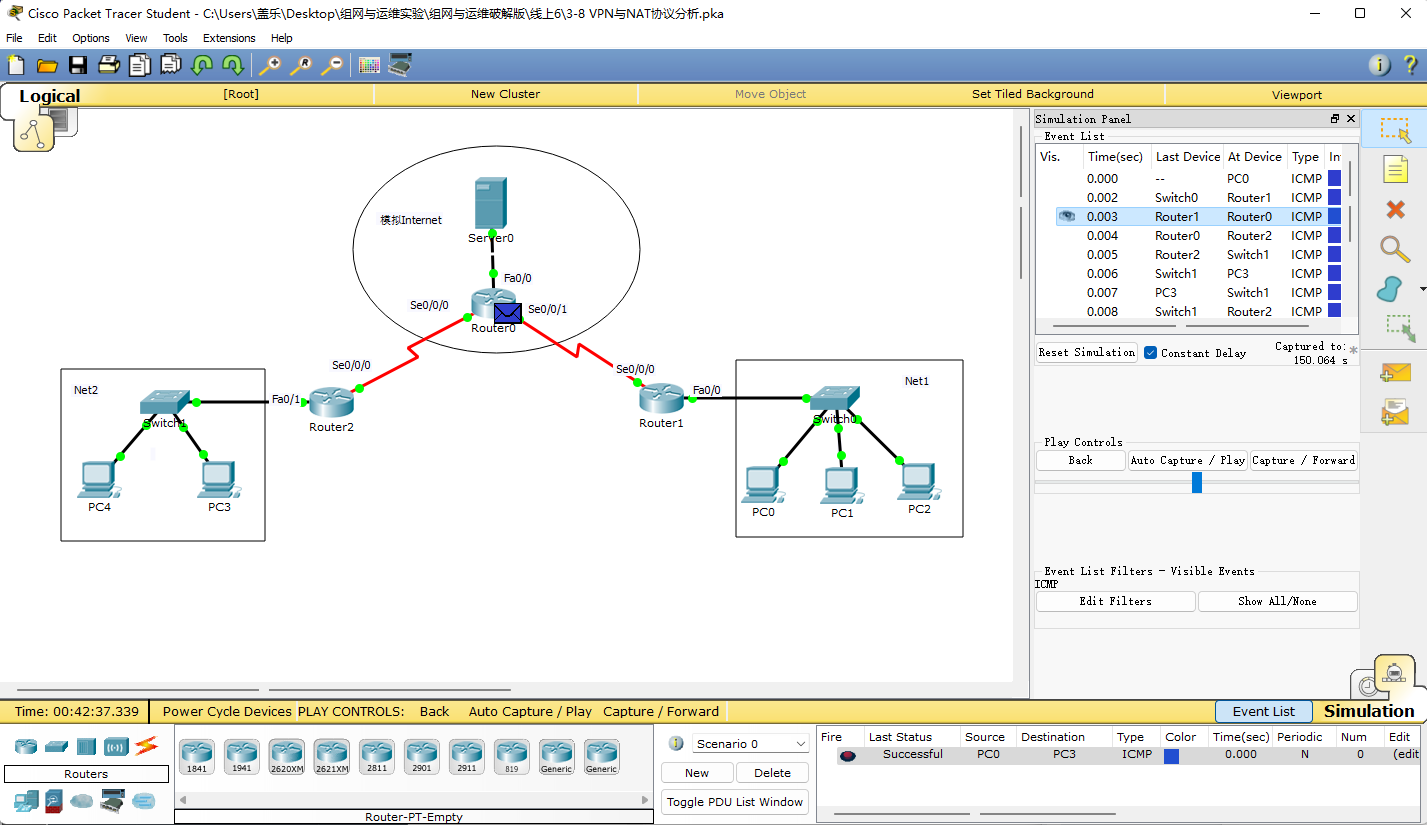
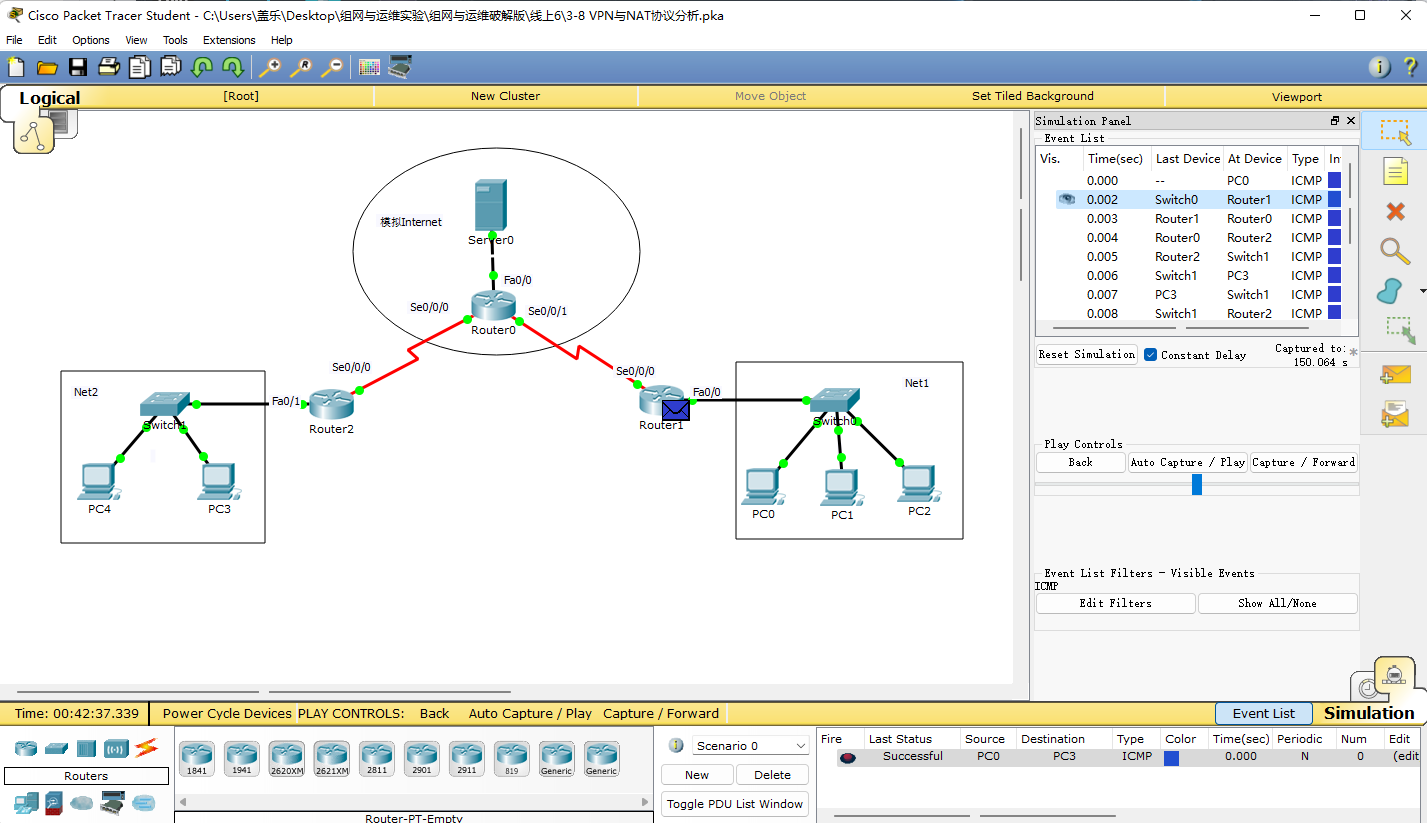
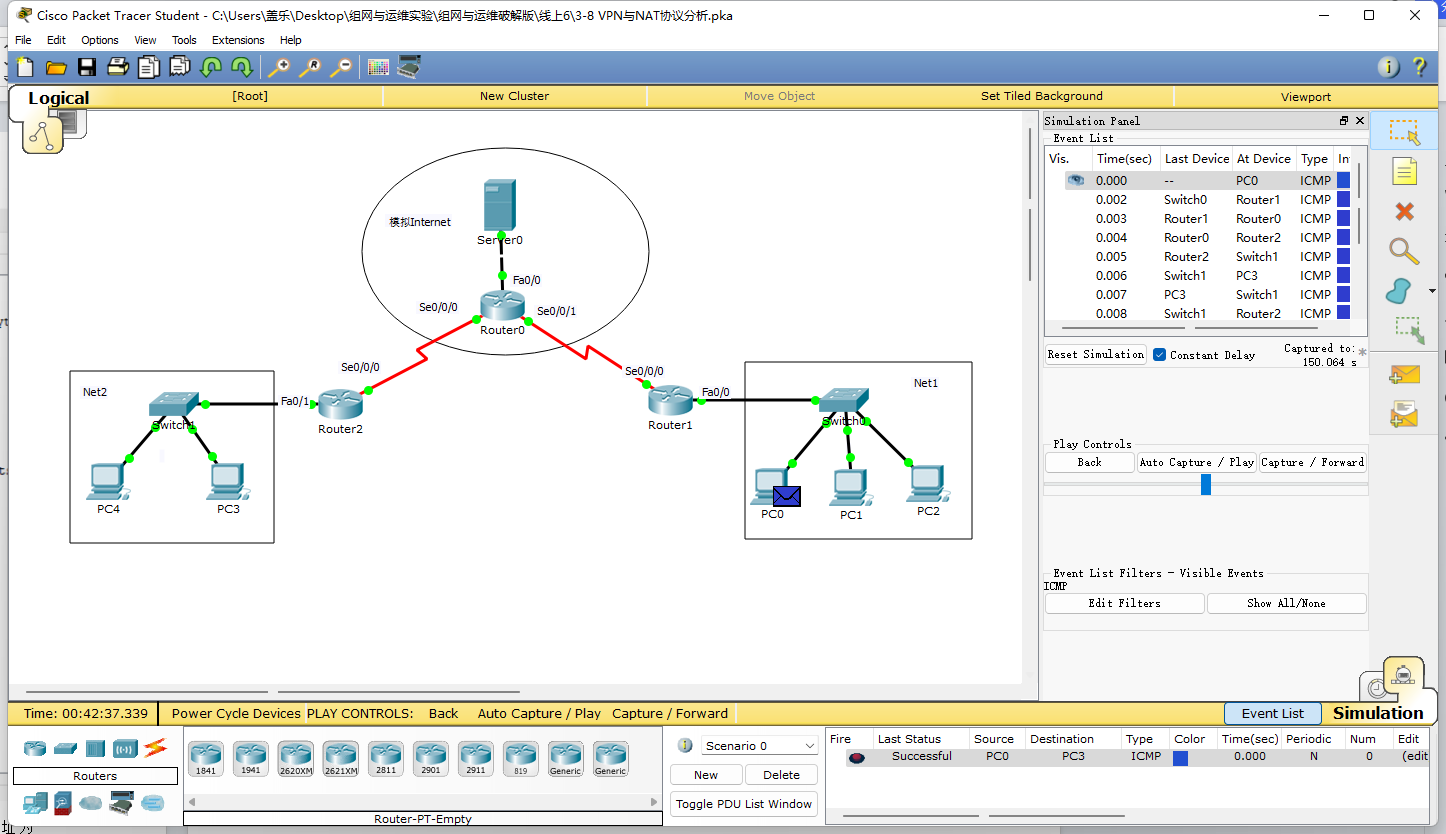
• 该过程的主要目的是初始化VPN连接

步骤二：观察VPN的隧道技术

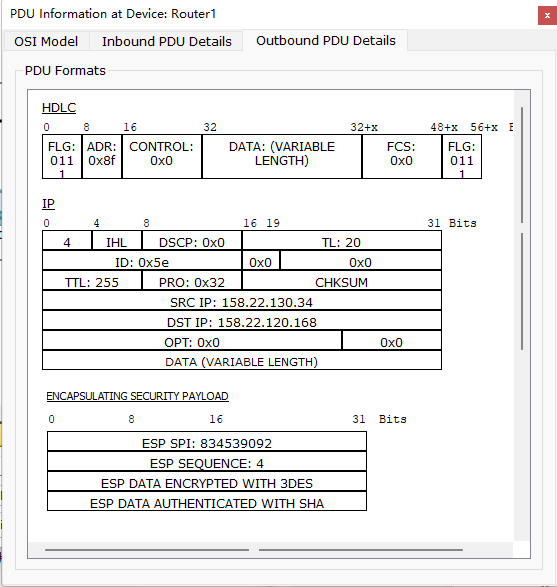
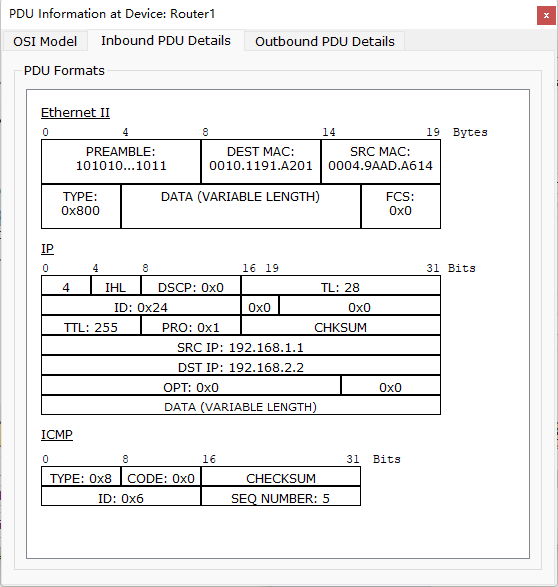
• 切换到模拟模式，设置事件列表只显示ICMP事件



• 单击Auto Capture/Play运行模拟，并捕获事件和数据包。此时，可观察到ICMP数据报的转发过程。

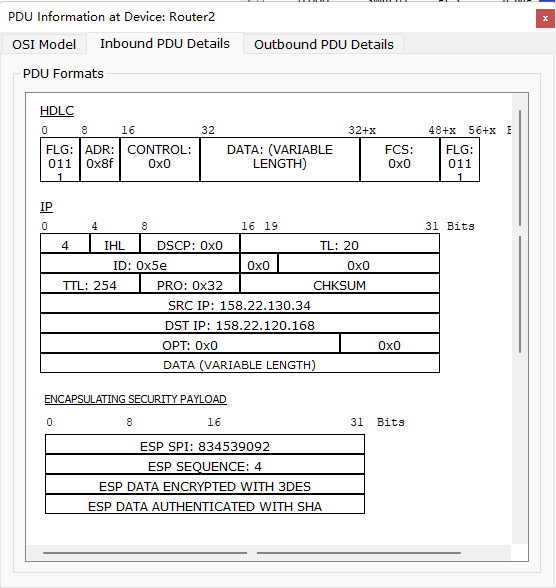
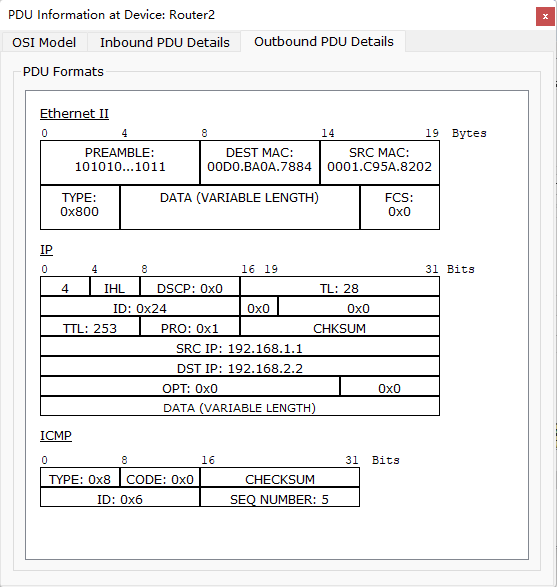


• 在事件列表中找到 At Device 显示为 Router1 的事件查看。



可以发现在Inbound PDU中，该PDU的源目IP地址分别为192.168.1.1（PC0的IP地址）和192.168.2.2（PC3的IP地址）。而在Outbound PDU中，PDU的源目IP地址已经更改为158.22.130.34（Router1的Se0/0/0的IP地址）和158.22.120.168（Router2的Se0/0/0的IP地址），并且原IP包已经被重新封装在新的IP包中，这就是隧道技术的工作原理。

• 在事件列表中找到 At Device 显示为 Router2 的事件查看。

可以发现在Inbound PDU中，该PDU的源目IP地址分别为158.22.130.34（Router1的Se0/0/0的IP地址）和158.22.120.168（Router2的Se0/0/0的IP地址）。而在Outbound PDU中，PDU的源目IP地址已经更改为192.168.1.1（PC0的IP地址）和192.168.2.2（PC3的IP地址），这说明PC0发送的IP包被Router2重新解封出来。

## 三、思考与总结

1. 在任务一中，Router1如何区分Server0返回给不同主机的HTTP报文？

答：NAT 服务器(Router1)通过不同的端口号来识别不同的主机的报文。

1. 在任务二中，VPN中采用隧道技术的原因是什么？。

答：PC0 和 PC3 使用的都是私有地址，无法直接进行通信，采用隧道技术可以将源地址和目的地址转换为全局地址。

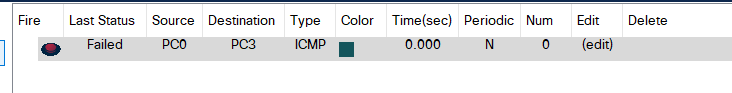
1. Net1网络和Net2网络的IP地址能否编在同一段？

答：不可以，在同一个网段容易造成两个网络下主机的IP地址冲突。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

①观察NAT工作原理时，发现在模拟模式下无法直接访问连接，切换到实时模式访问再切换回模拟模式解决问题。

②本次实验还是和之前几次线上实验一样存在数据包转发过程中异常的情况，和预期情况不符，来回切换数次实时模式和模拟模式后解决问题。



通过本次实验，我学习了NAT和VPN协议，理解了VPN使用的IP隧道技术的工作原理以及理解了NAT技术的工作原理。