**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和NAT协议分析**

网络与信息安全 学院 2118021 班

成 绩

姓名 学号

同作者

实验日期 2023 年 11 月 25 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） |

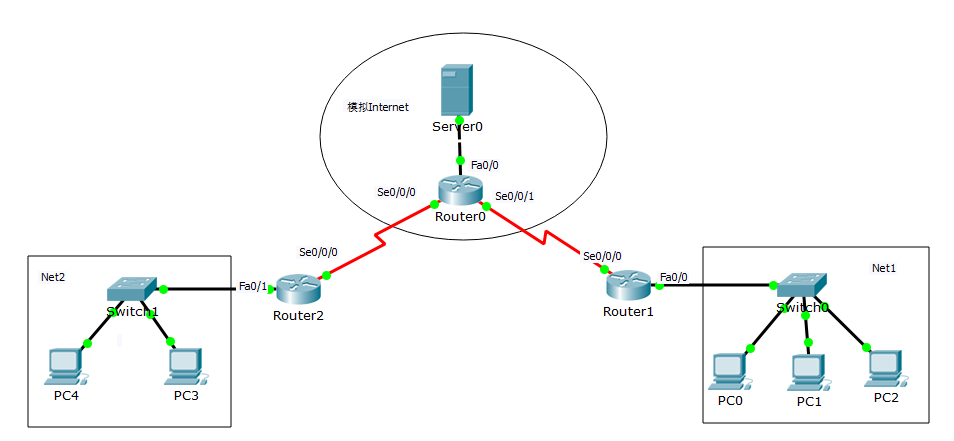
# VPN与NAT协议分析

## 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

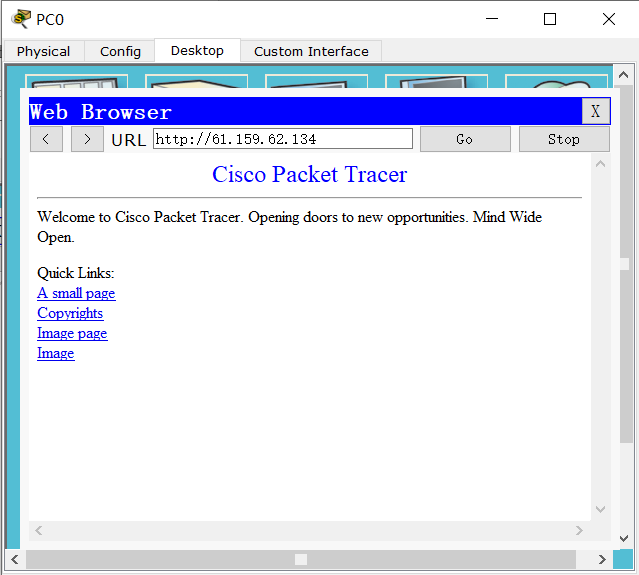


1. 给出实验中使用的IP配置表

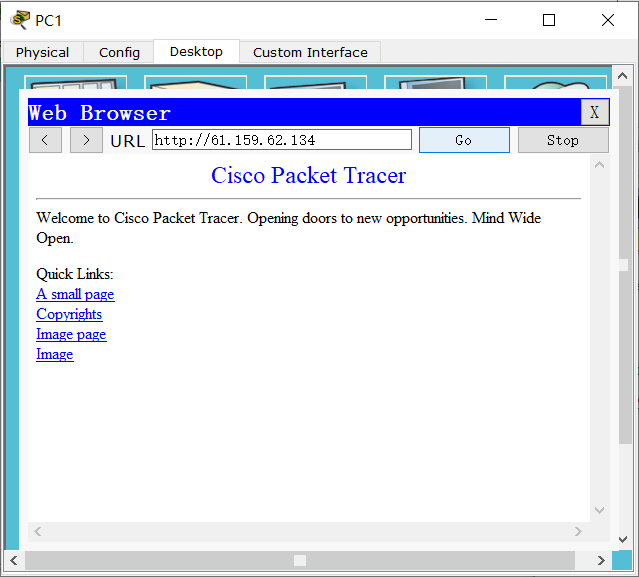
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备** | **接口** | **IP地址** | **掩码** | **默认网关** |
| PC0 | Fa0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.254 |
| PC1 | Fa0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.254 |
| PC2 | Fa0 | 192.168.1.3 | 255.255.255.0 | 192.168.1.254 |
| PC3 | Fa0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.254 |
| PC4 | Fa0 | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 |
| RouterO | Fa0/0 | 61.159.62.12 | 255.0.0.0 | - |
| Se0/0/0 | 158.22.120.169 | 255.255.255.0 | - |
| Se0/0/1 | 158.22.130.33 | 255.255.255.0 | - |
| **设备** | **接口** | **IP地址** | **掩码** | **默认网关** |
| Routerl | Fa0/0 | 192.168.1.254 | 255.255.255.0 | - |
| Se0/0/0 | 158.22.130.34 | 255.255.255.0 | - |
| Router2 | Se0/0/0 | 158.22.120.168 | 255.255.255.0 | - |
| Fa0/0 | 61.159.62.12 | 255.0.0.0 | - |
| Server | Fa0 | 61.159.62.134 | 255.0.0.0 | 61.159.62.12 |

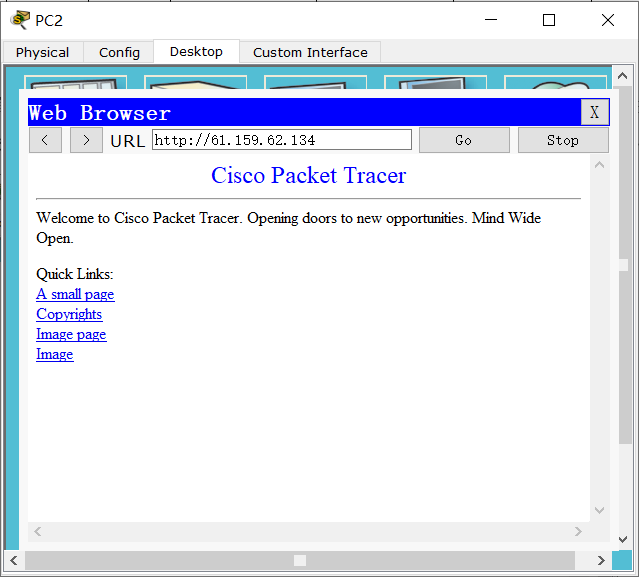
1. 任务一：观察学习NAT的工作原理。

首先在实时模式下，点击PC0，选择Desktop中的Web Browser，在地址栏输入Server 0的IP地址http://61.159.62.134，访问目标网页，结果如下：



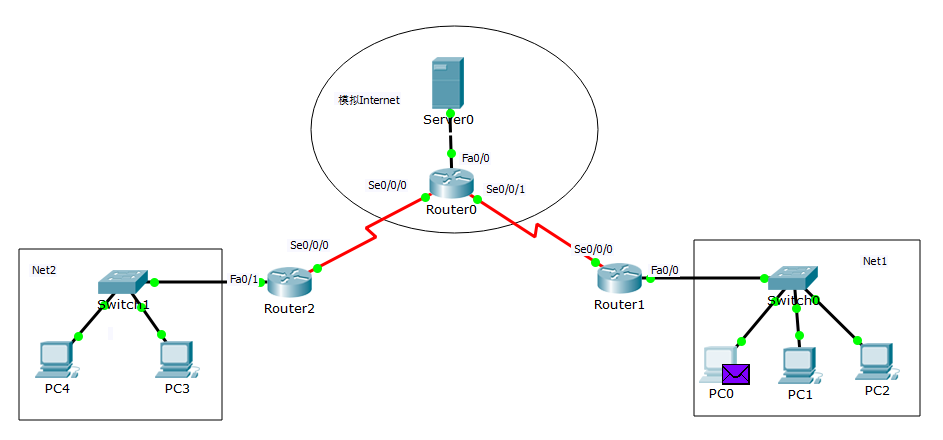
按照同样的方法，在PC1、PC2中访问http://61.159.62.134，结果如下：

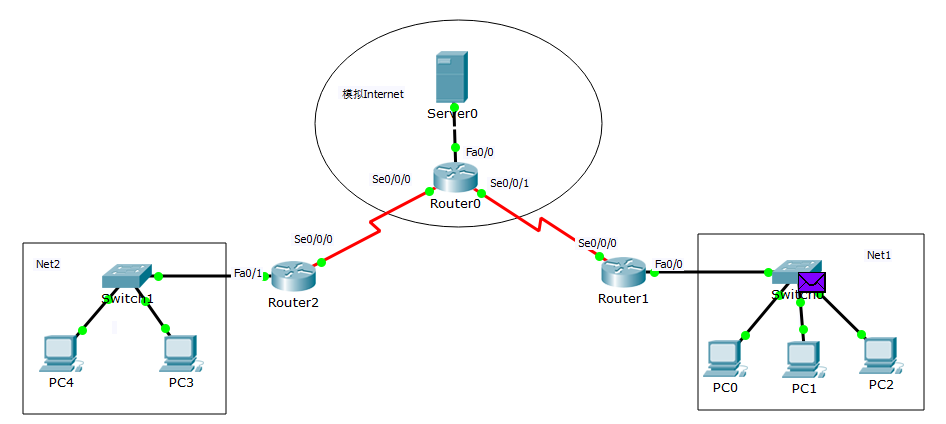


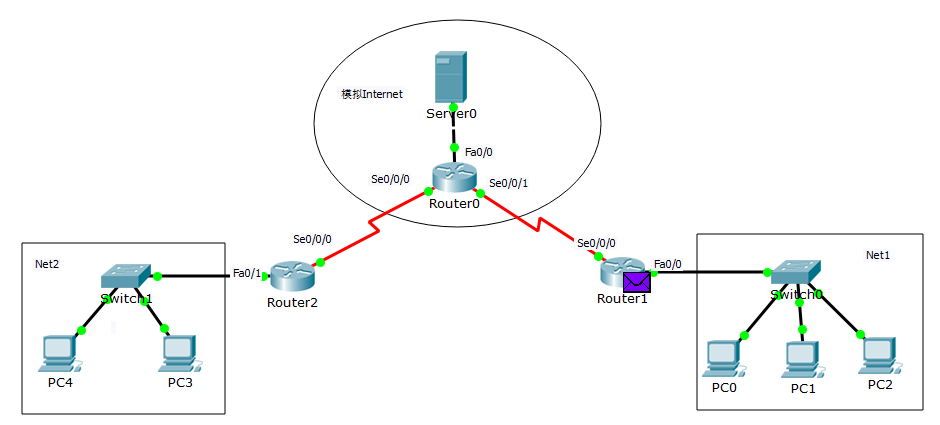


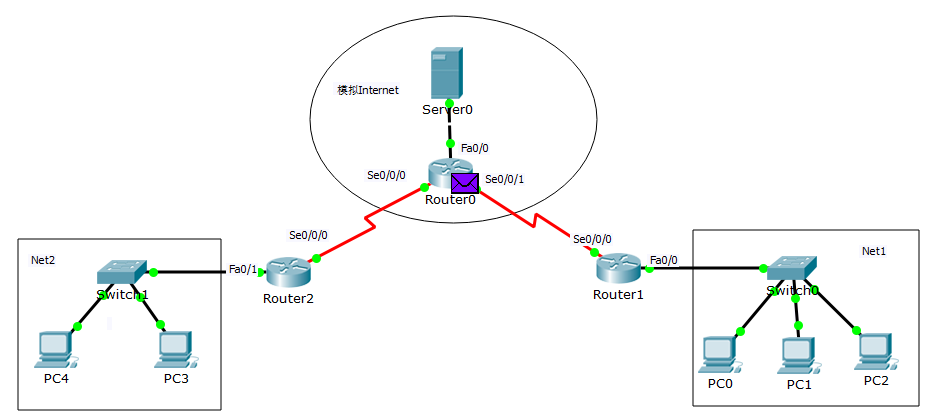
由图可知，三台主机均能正常访问Web服务器。

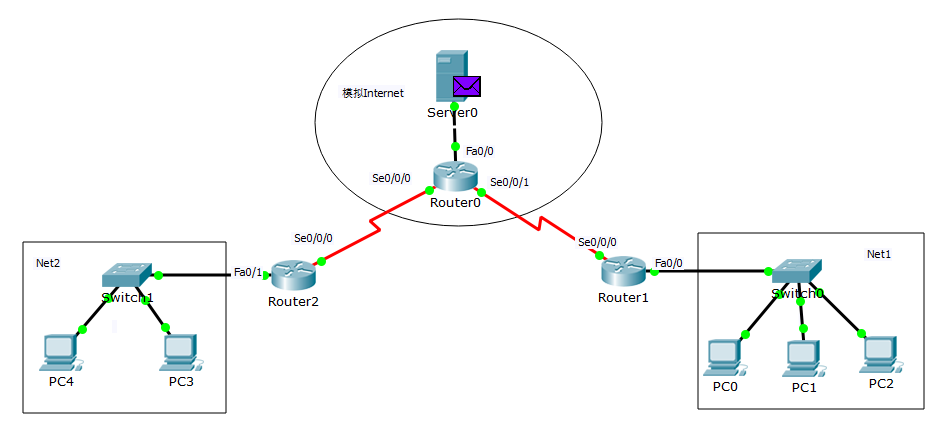
此时进入模拟模式，设置事件过滤器仅显示HTTP事件，重新在PC0中访问http://61.159.62.134，点击Auto Capture/Forward 按钮，观察HTTP报文传输过程，传输过程如下：

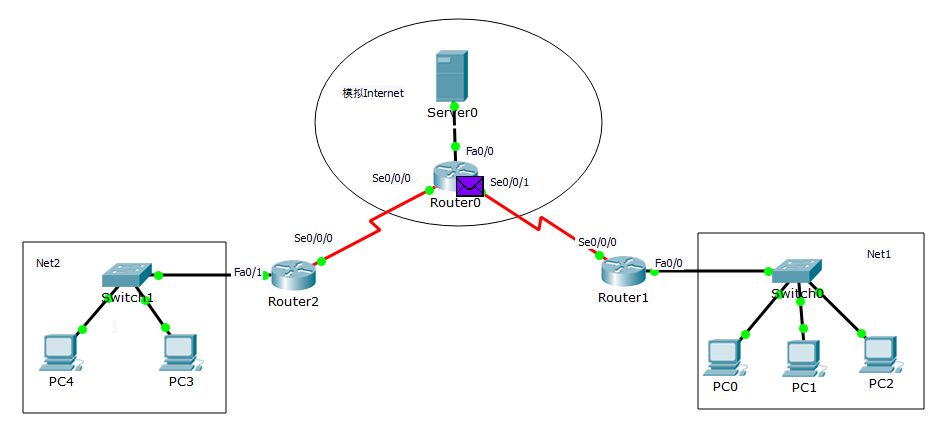


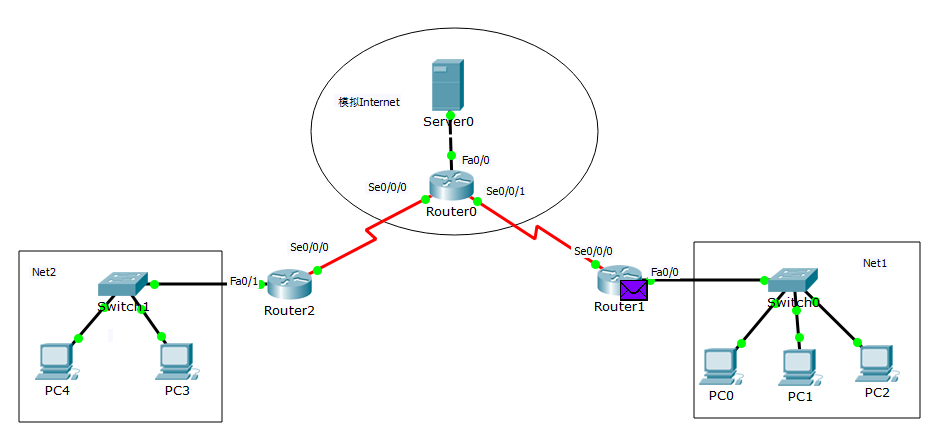


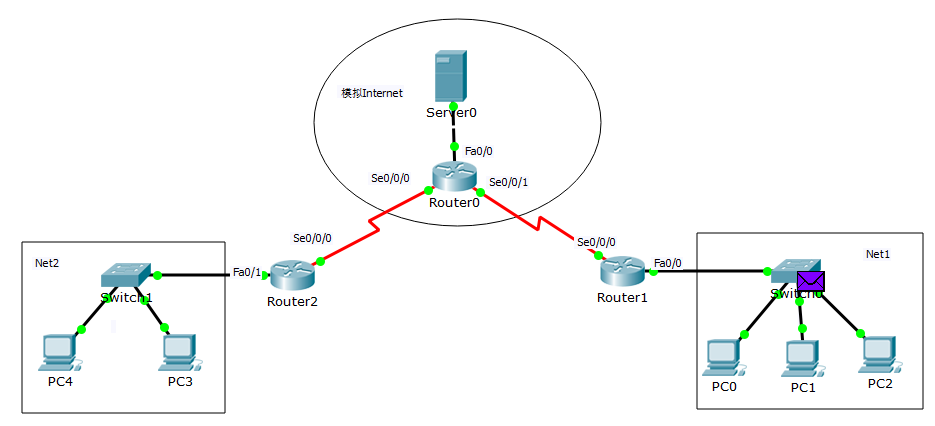


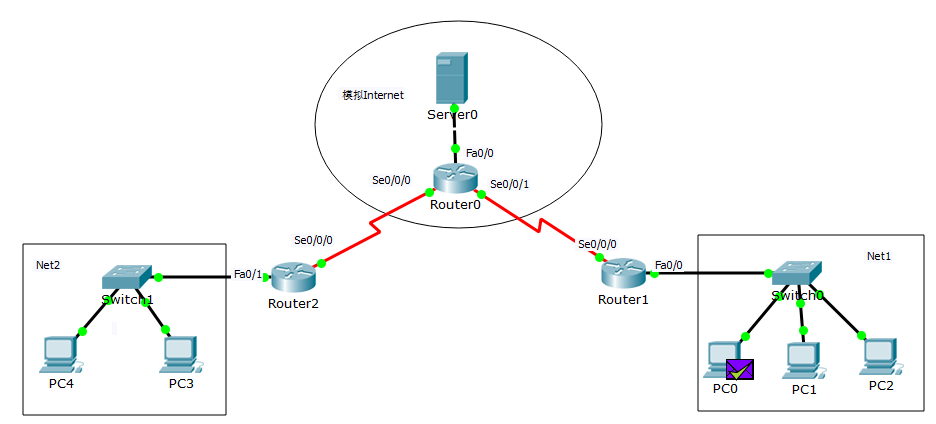


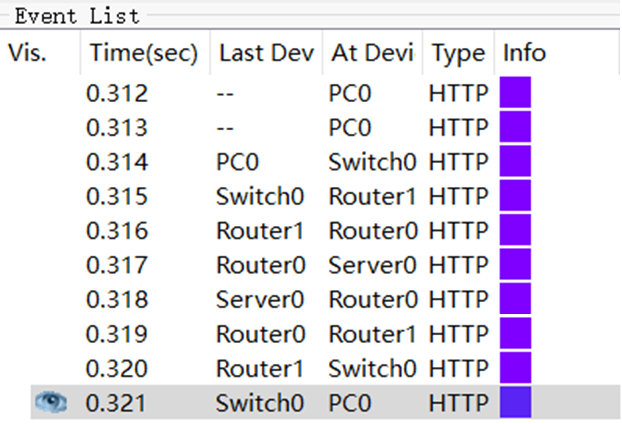




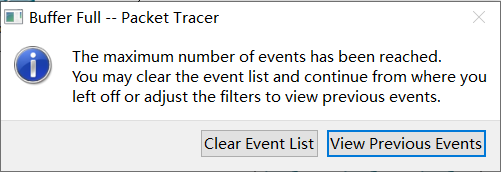




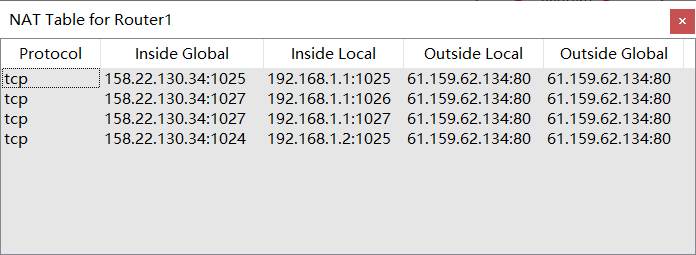




等待出现缓冲区满的提示，查看事件列表。

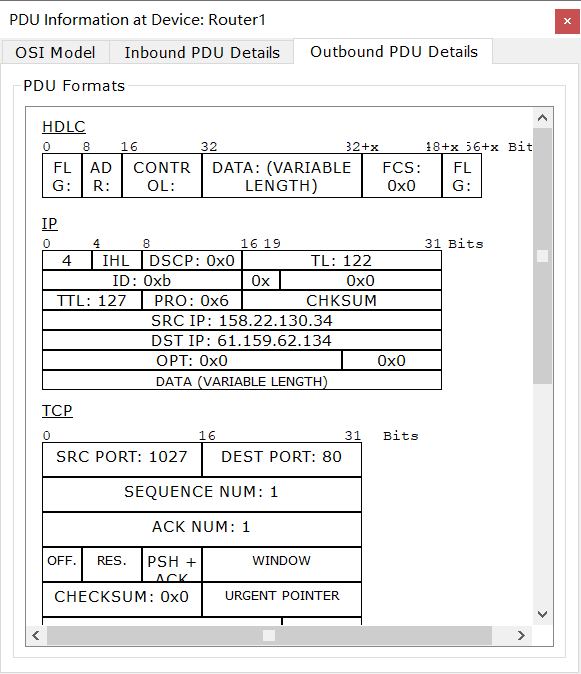
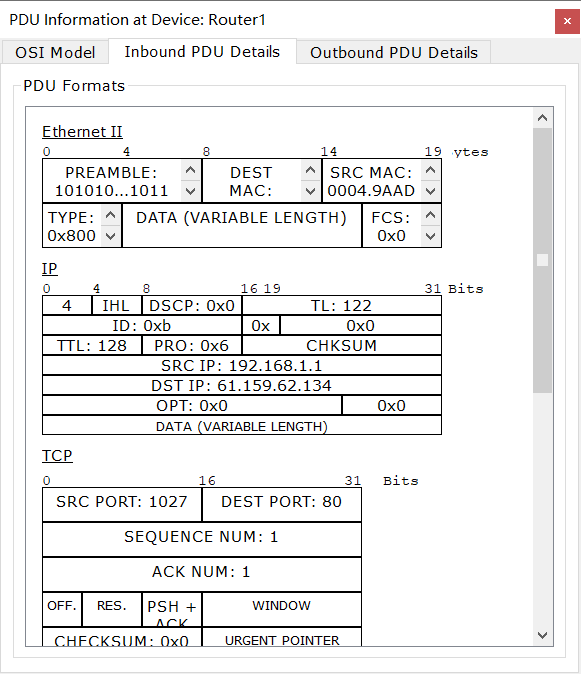


使用检查工具查看Router 1的NAT地址转换表如下：



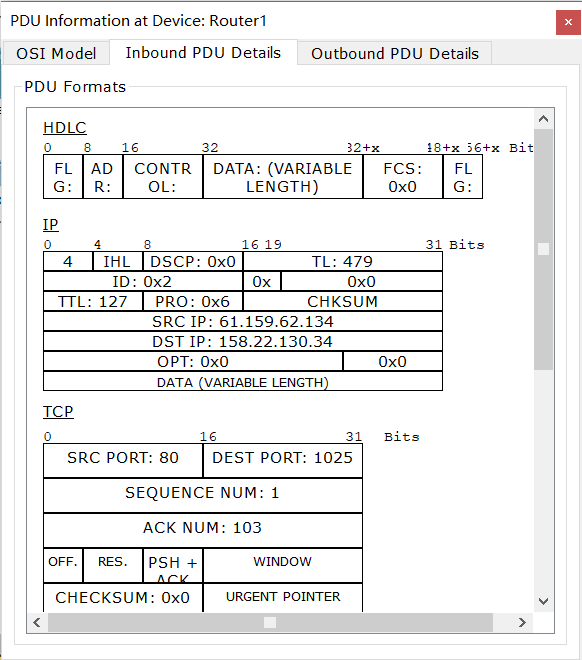
在事件列表中查看到达Router 1的事件，点击查看详细内容。在弹出对话框中分别点击Inbound PDU Details 和Outbound PDU Details 选项卡。

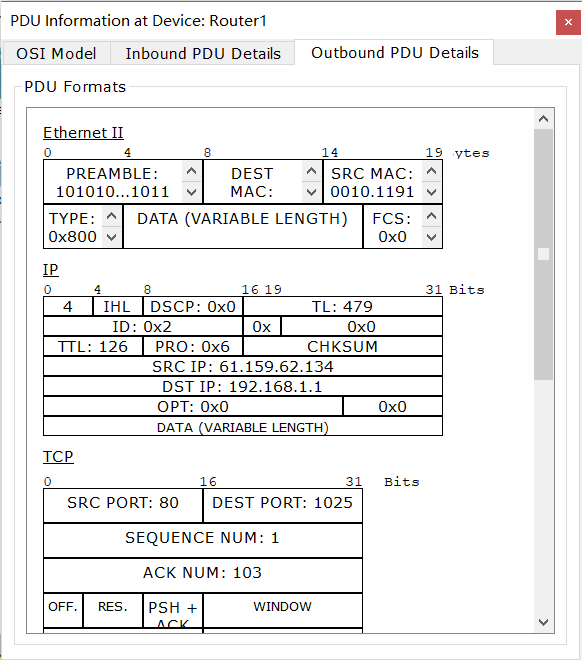
首先查看报文从PC0发送至server端时，router1中的ip地址转换情况，查看其内容如下：



由图可知，报文的源IP地址从进入时的私有IP192.168.1.1，转换为全局IP158.22.130.34，而目的IP并未改变。

之后查看报文从server端返回PC0时时，router1中的ip地址转换情况，查看其内容如下：





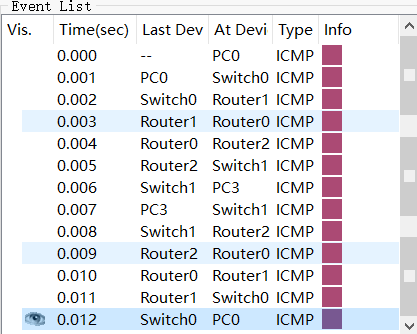
由图可知，报文的目的IP地址从进入时的全局IP158.22.130.34，转换为私有IP192.168.1.1，而源IP并未改变。

参照Router 1的NAT地址转换表可知，Router 1在报文发送至server0时，将switch0处的私有IP地址根据端口相应转换为对应全局IP地址；而在报文从server0返回switch0时，将全局IP地址根据端口相应转换为对应私有IP地址，从而使得具有私有IP的PC也能够访问互联网。

由此可以得到，NAT协议是一种将私有地址转化为合法IP地址的转换技术，将专用IP地址转换为全局IP地址，解决专用IP地址访问Internet的问题。

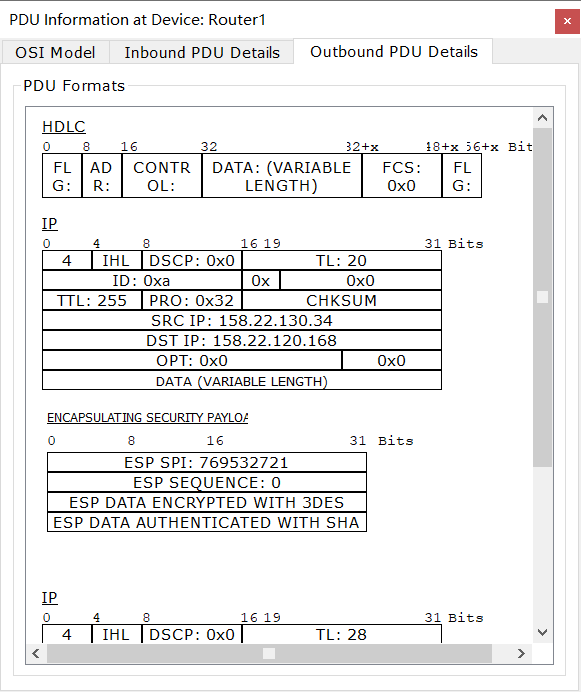
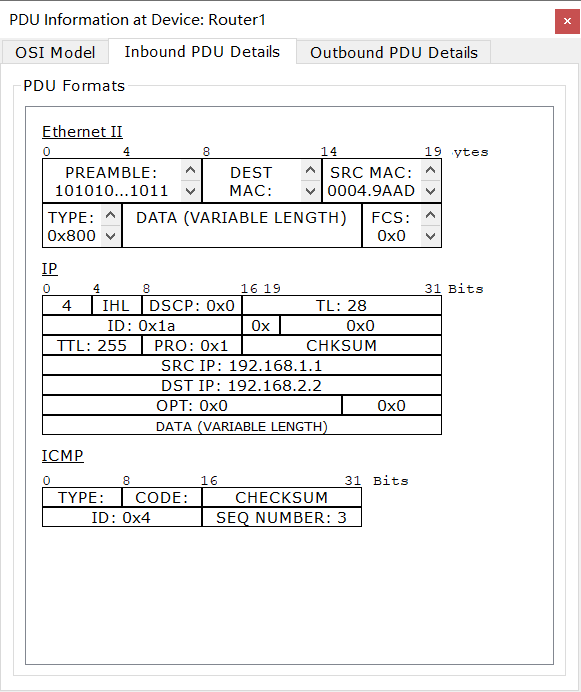
1. 任务二：观察学习VPN工作原理。

首先进入实时模式，点击添加简单PDU按钮，再点击PC0、PC3，添加从PC0至PC3的简单PDU，再切换至模拟模式，设置事件列表过滤器仅显示ICMP事件，点击Auto Capture/Play，使得数据包自动完成转发。转发完成后查看其转发过程如下：



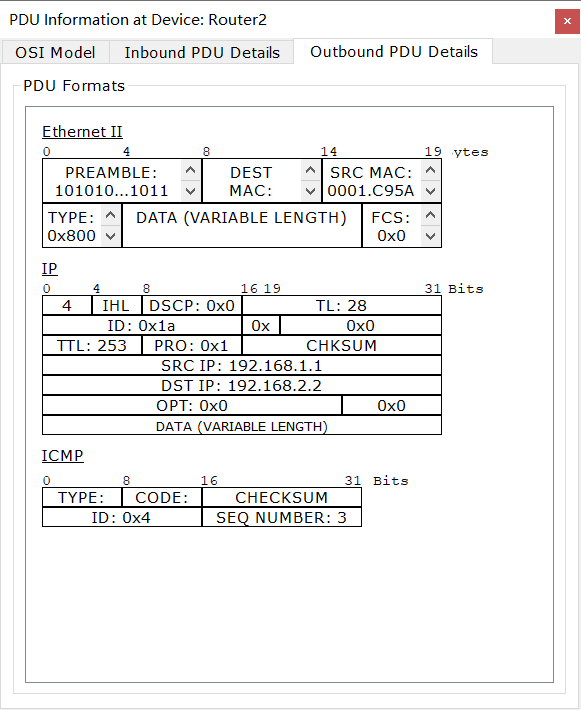
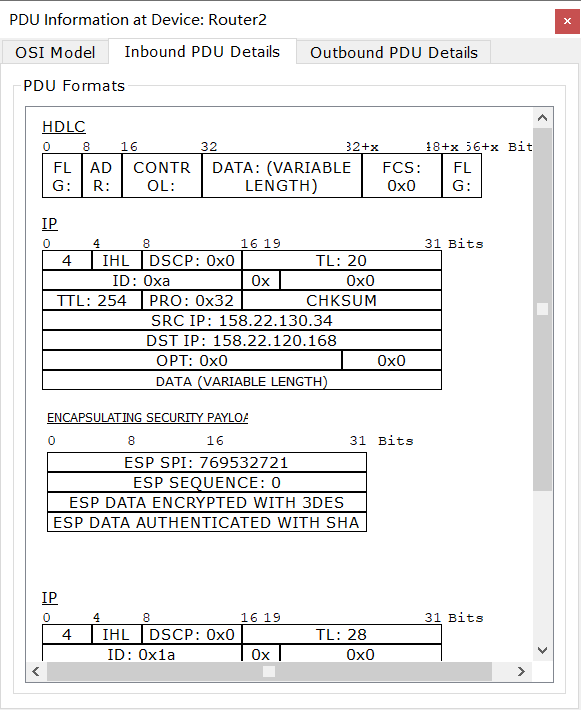
由转发过程可知，该数据包通过交换机转发至互联网中，再经由路由器转发至目的主机所在网络的交换机，最终到达目的主机。

此时查看PC0向PC3发送数据包过程中At Device为Router 1的事件，点击info标签，分别查看其Inbound PDU Details 和 Outbound PDU Details 选项卡如下：



由图可知，随着Router 1的转发，源IP与目的IP均从私有地址转换为对应的全局地址，且原有IP数据报被封装在该数据包中。

按照同样的方法查看Router 2中的PDU的信息如下：



由图可知，此时通过Router 2的转发，源IP与目的IP从全局地址转换为私有地址，即被封装的数据报被解封，从而能够找到对应目的主机。

通过该实验可以知道，虚拟专用网络（Virtual Private Network, VPN）是一种常用于连接企业或机构内部网络的通信方法，它利用已加密的IP隧道技术来达到IP地址转换、保密、身份认证等网络服务，通过将双方的专用IP地址转换为公有IP地址，使两个使用专用IP地址的局域网透过公用的Internet连网。

## 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？

根据使用的端口号，区分不同主机。由于在NAT转换表中记录有IP地址转换规则，由表可知，Router 1根据不同端口转换IP地址，从而区分不同主机的报文。

1. 在任务二中，VPN中采用隧道技术的原因是什么？。

因为Net1与Net2两个网络中主机均采用私有地址，不能直接在互联网上通信，因此在通信时需要借助隧道技术，将私有地址转换为全局地址，从而实现通过互联网的通信。

1. Net1网络和Net2网络的IP地址能否编在同一段？

不能。由于两个网络通过互联网通信，不能避免IP地址冲突问题。若编在同一网段，可能造成两个网络中不同主机的IP地址发生冲突。

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？

在理解NAT与VPN时，需要结合相应转换表，查看相应转换关系才能对这两种技术有准确地理解。

通过本次实验，借助虚拟环境观察到NAT与VPN具体的转换过程，对其原理以及使用原因有了进一步的理解与认识。