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

姓名 学号

同作者

实验日期 2023 年 11 月 25 日

成 绩

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）

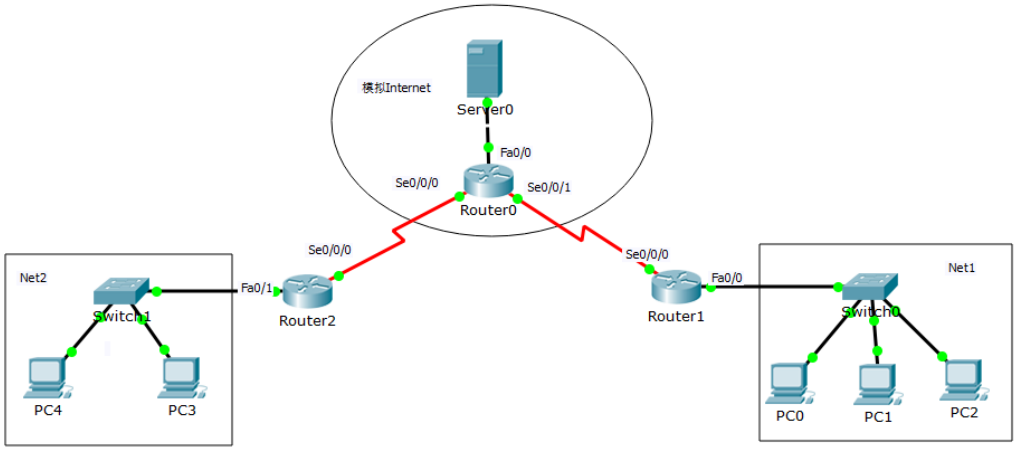
VPN与NAT协议分析

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



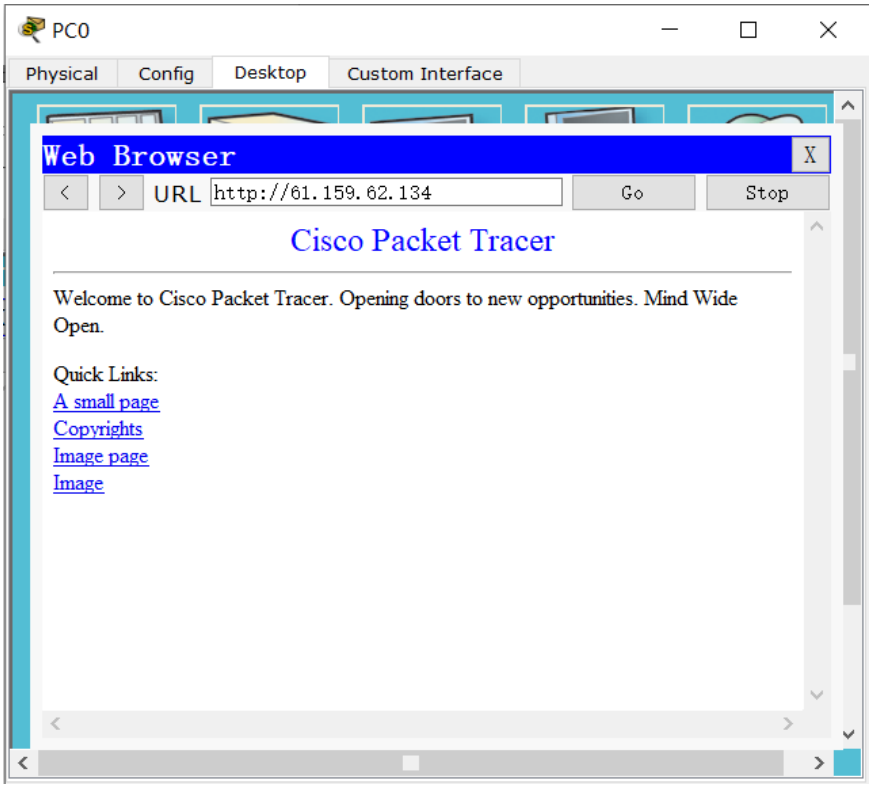
2. 给出实验中使用的 IP 配置表

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
Router0	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	-

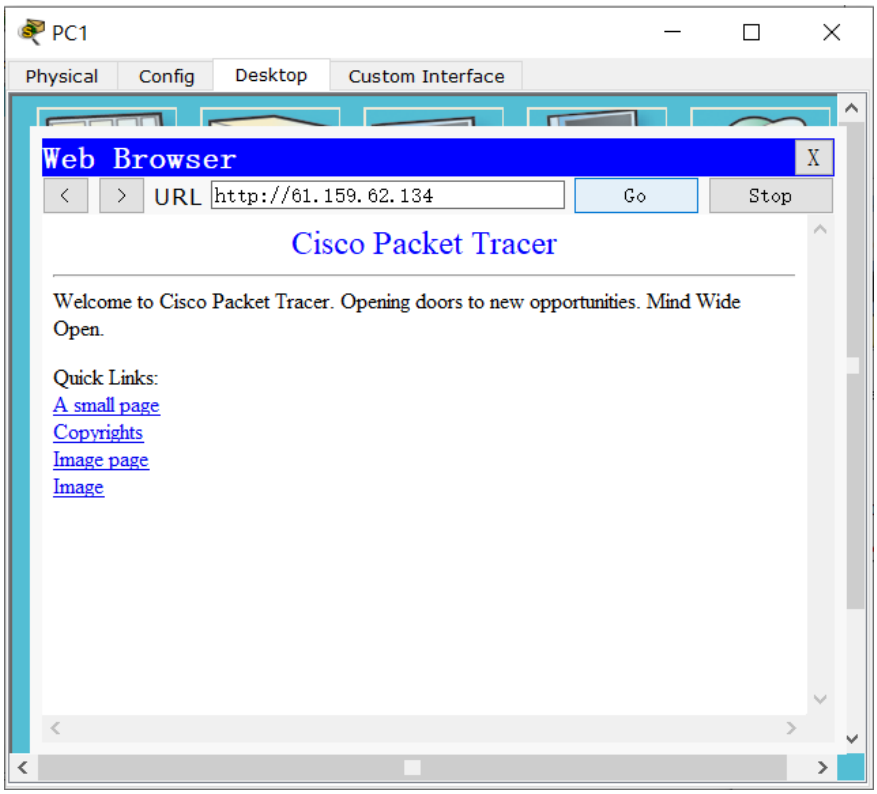
设备	接口	IP 地址	掩码	默认网关
Router1	Fa0/0	192.168.1.254	255.255.255.0	-
	Se0/0/0	158.22.130.34	255.255.255.0	-
Router2	Se0/0/0	158.22.120.168	255.255.255.0	-
	Fa0/0	61.159.62.12	255.0.0.0	-
Server	Fa0	61.159.62.134	255.0.0.0	61.159.62.12

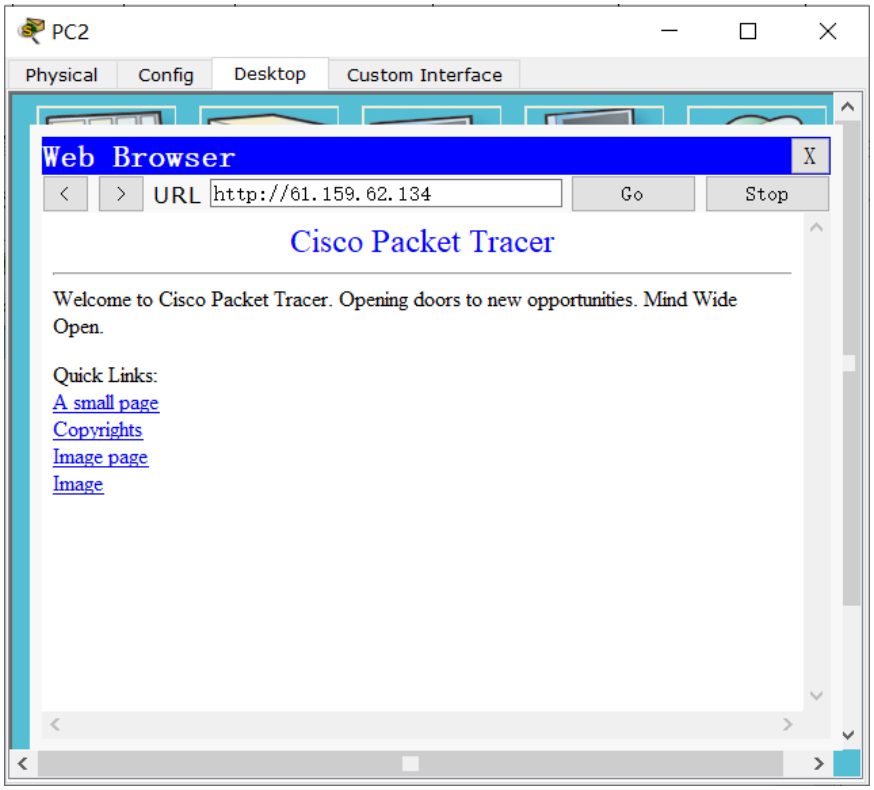
3. 任务一：观察学习 NAT 的工作原理。

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：



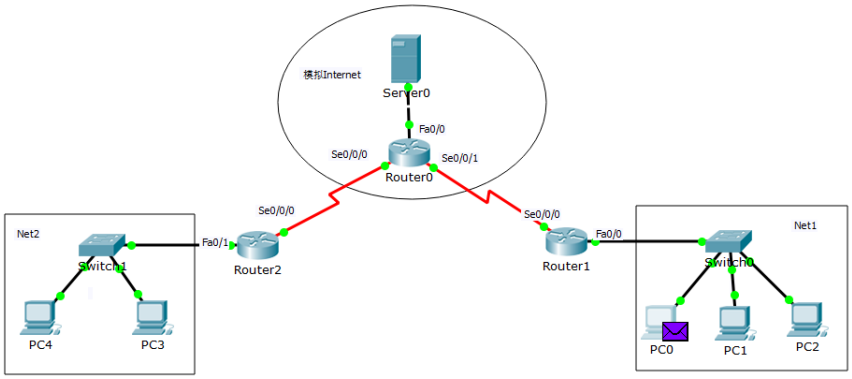
按照同样的方法，在 PC1、PC2 中访问 http://61.159.62.134，结果如下：

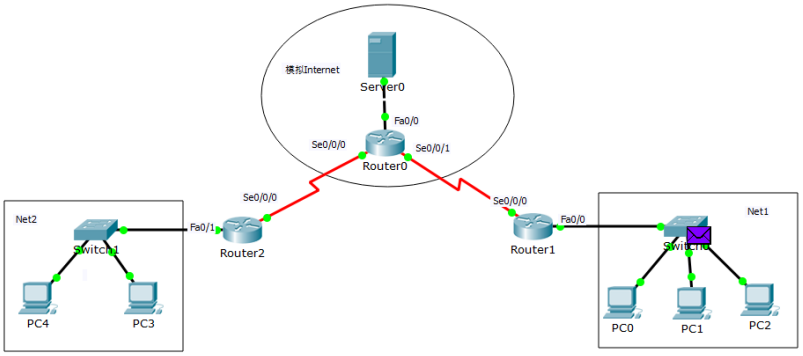


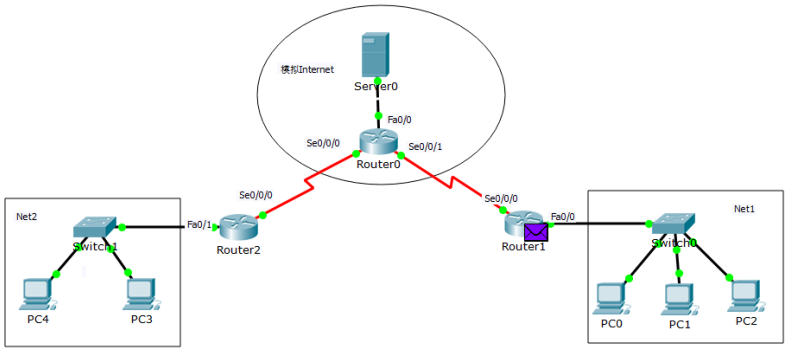


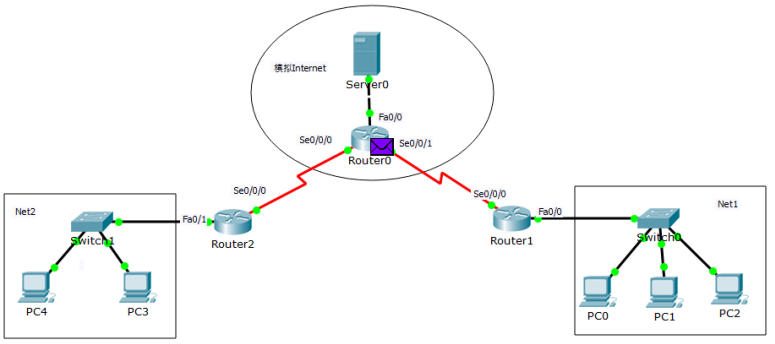
由图可知，三台主机均能正常访问 Web 服务器。

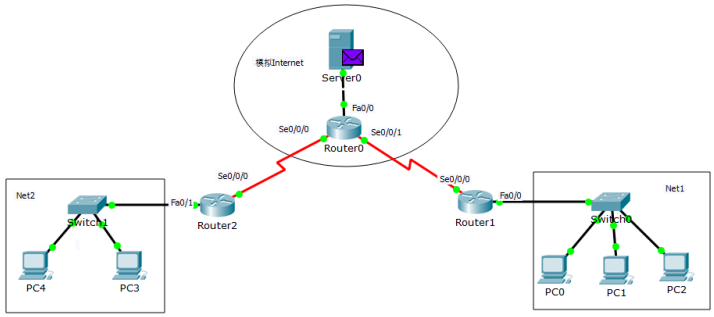
此时进入模拟模式，设置事件过滤器仅显示 HTTP 事件，重新在 PC0 中访问 http://61.159.62.134，点击 Auto Capture/Forward 按钮，观察 HTTP 报文传输过程，传输过程如下：

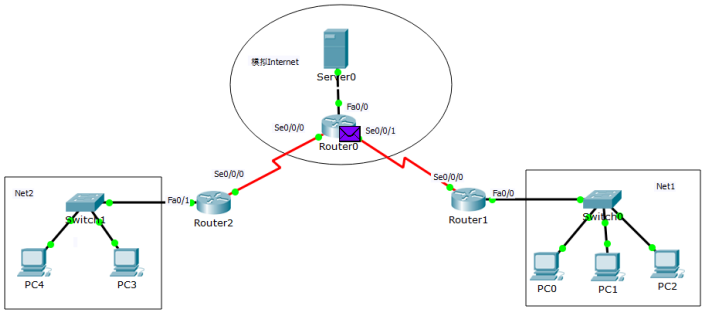

模拟Internet
Server0
Fa0/0
Se0/0/0
Router0
Se0/0/1
Se0/0/0
Fa0/1
Router2
Net2
Switch1
PC4
PC3
Se0/0/0
Fa0/0
Router1
Net1
Switch0
PC0
PC1
PC2

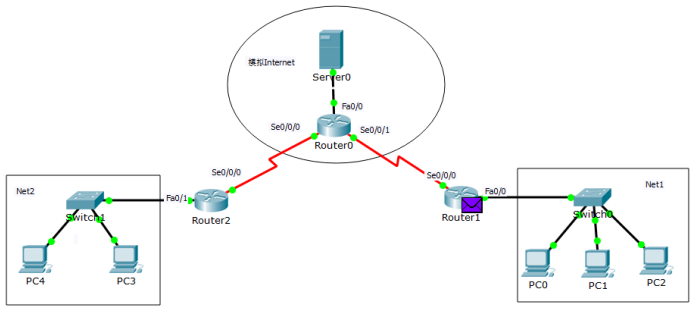

模拟Internet
Server0
Fa0/0
Se0/0/0
Router0
Se0/0/1
Se0/0/0
Fa0/1
Router2
Net2
Switch1
PC4
PC3
Se0/0/0
Fa0/0
Router1
Net1
Switch0
PC0
PC1
PC2

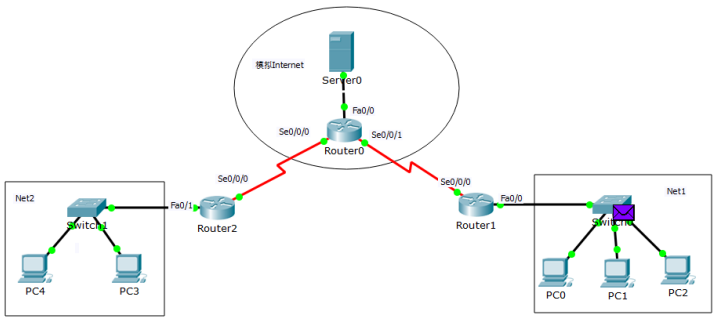

模拟Internet
Server0
Fa0/0
Se0/0/0
Router0
Se0/0/1
Se0/0/0
Fa0/1
Router2
Net2
Switch1
PC4
PC3
Se0/0/0
Fa0/0
Router1
Net1
Switch0
PC0
PC1
PC2

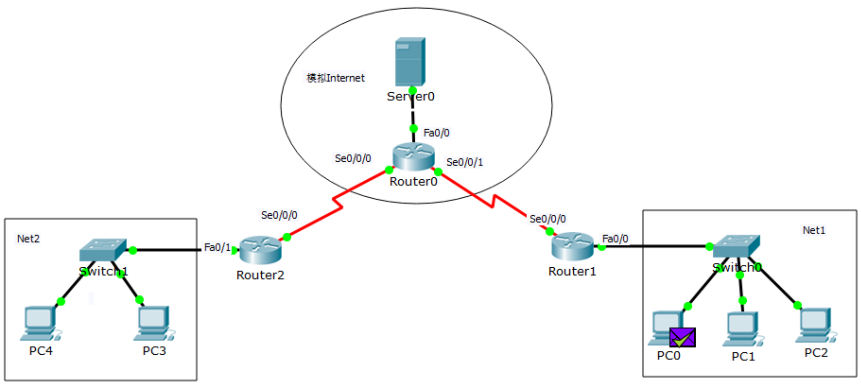

模拟Internet
Server0
Fa0/0
Se0/0/0
Router0
Se0/0/1
Se0/0/0
Fa0/1
Router2
Net2
Switch1
PC4
PC3
Se0/0/0
Fa0/0
Router1
Net1
Switch0
PC0
PC1
PC2


模拟Internet
Server0
Fa0/0
Se0/0/0
Se0/0/1
Router0
Se0/0/0
Fa0/1
Router2
Se0/0/0
Fa0/0
Router1
Net2
Switch1
PC4
PC3
Net1
Switch0
PC0
PC1
PC2


模拟Internet
Server0
Fa0/0
Se0/0/0
Se0/0/1
Router0
Se0/0/0
Fa0/1
Router2
Se0/0/0
Fa0/0
Router1
Net2
Switch1
PC4
PC3
Net1
Switch0
PC0
PC1
PC2


模拟Internet
Server0
Fa0/0
Se0/0/0
Se0/0/1
Router0
Se0/0/0
Fa0/1
Router2
Se0/0/0
Fa0/0
Router1
Net2
Switch1
PC4
PC3
Net1
Switch0
PC0
PC1
PC2

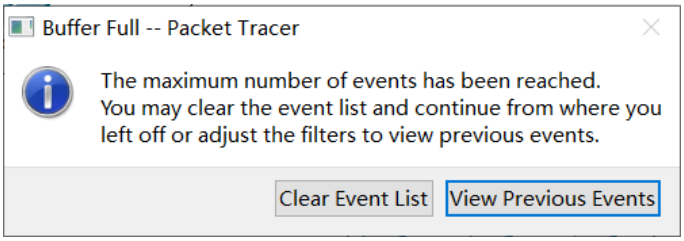

模拟Internet
Server0
Fa0/0
Se0/0/0
Se0/0/1
Router0
Se0/0/0
Fa0/1
Router2
Se0/0/0
Fa0/0
Router1
Net2
Switch1
PC4
PC3
Net1
Switch0
PC0
PC1
PC2


模拟Internet
Server0
Fa0/0
Se0/0/0
Se0/0/1
Router0
Se0/0/0
Fa0/1
Router2
Se0/0/0
Fa0/0
Router1
Net2
Switch1
PC4
PC3
Net1
Switch0
PC0
PC1
PC2

Event List

Vis.	Time(sec)	Last Dev	At Devi	Type	Info
	0.312	--	PC0	HTTP	
	0.313	--	PC0	HTTP	
	0.314	PC0	Switch0	HTTP	
	0.315	Switch0	Router1	HTTP	
	0.316	Router1	Router0	HTTP	
	0.317	Router0	Server0	HTTP	
	0.318	Server0	Router0	HTTP	
	0.319	Router0	Router1	HTTP	
	0.320	Router1	Switch0	HTTP	
	0.321	Switch0	PC0	HTTP	

等待出现缓冲区满的提示，查看事件列表。



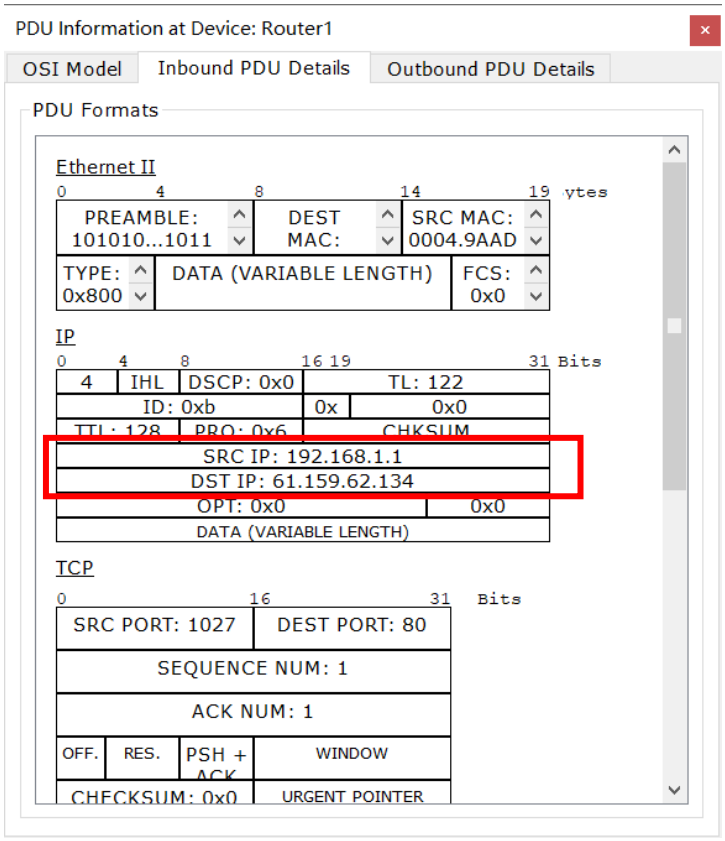
使用检查工具查看 Router 1 的 NAT 地址转换表如下：

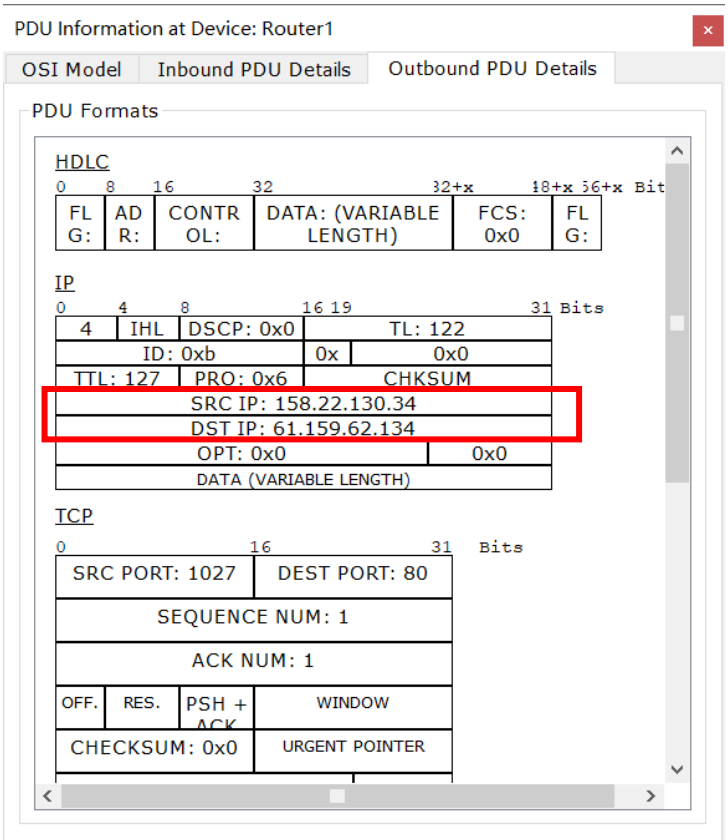
NAT Table for Router1

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	158.22.130.34:1025	192.168.1.1:1025	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1027	192.168.1.1:1026	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1027	192.168.1.1:1027	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1024	192.168.1.2:1025	61.159.62.134:80	61.159.62.134:80

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：

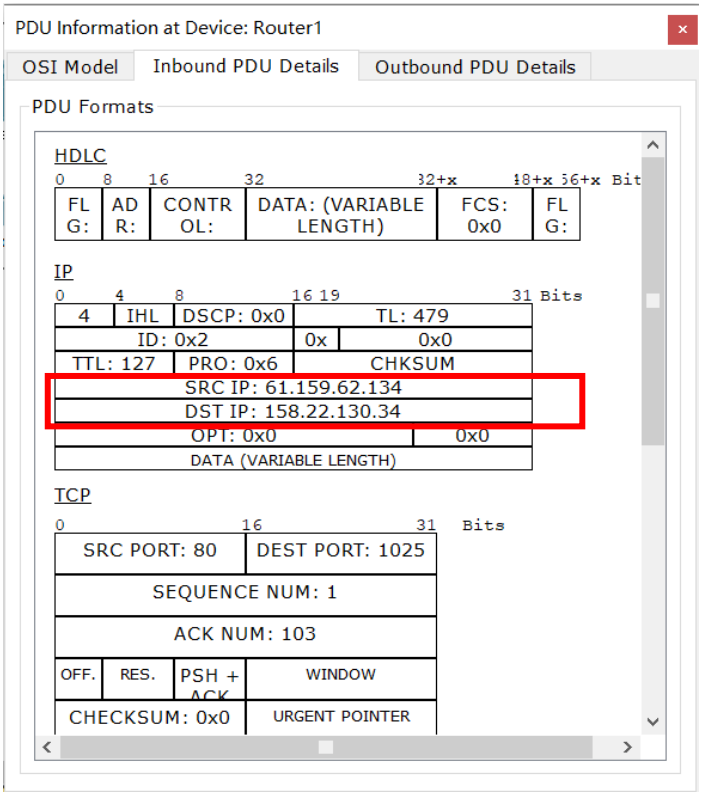


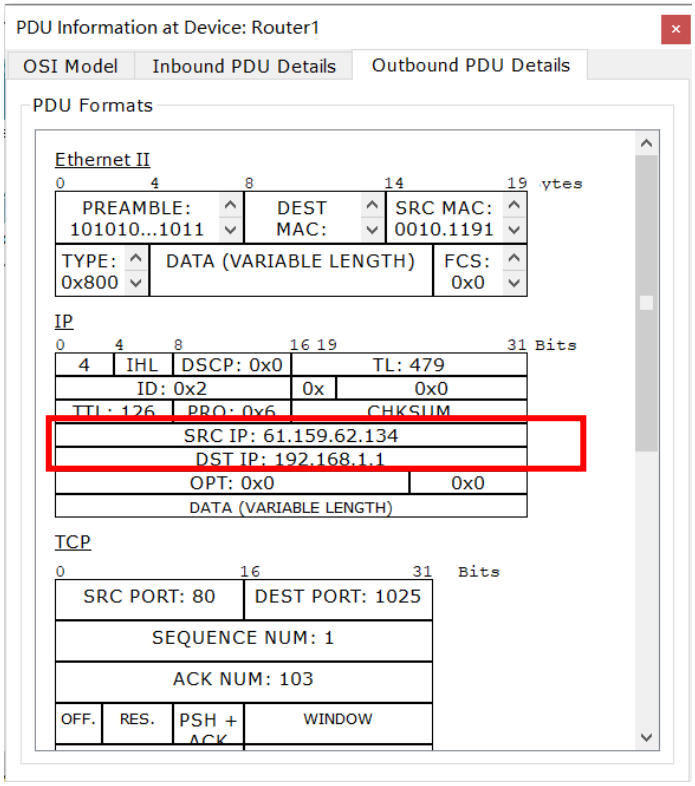


由图可知，报文的源 IP 地址从进入时的私有 IP192.168.1.1，转换为全局

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

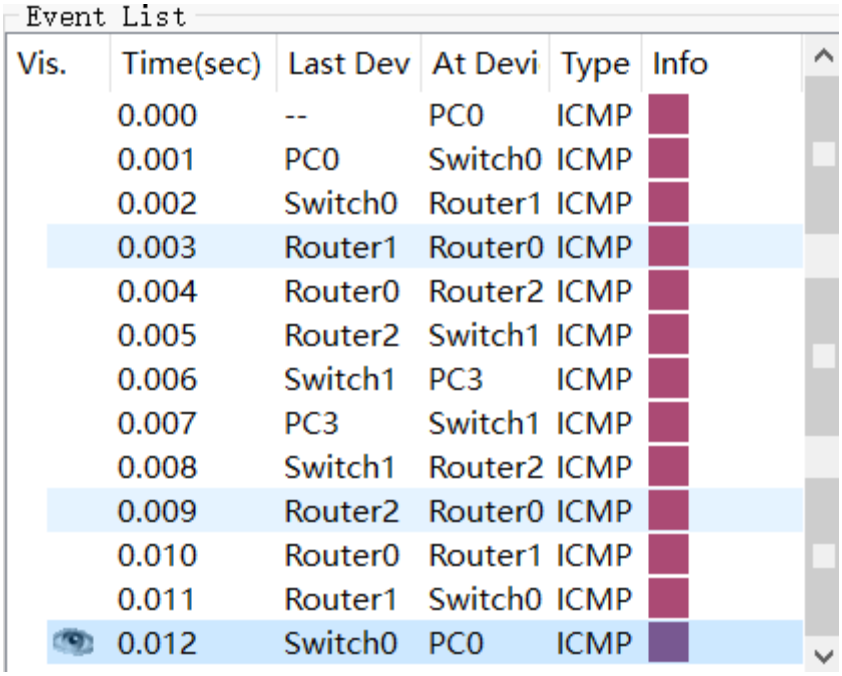
私有 IP192.168.1.1，而源 IP 并未改变。

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。

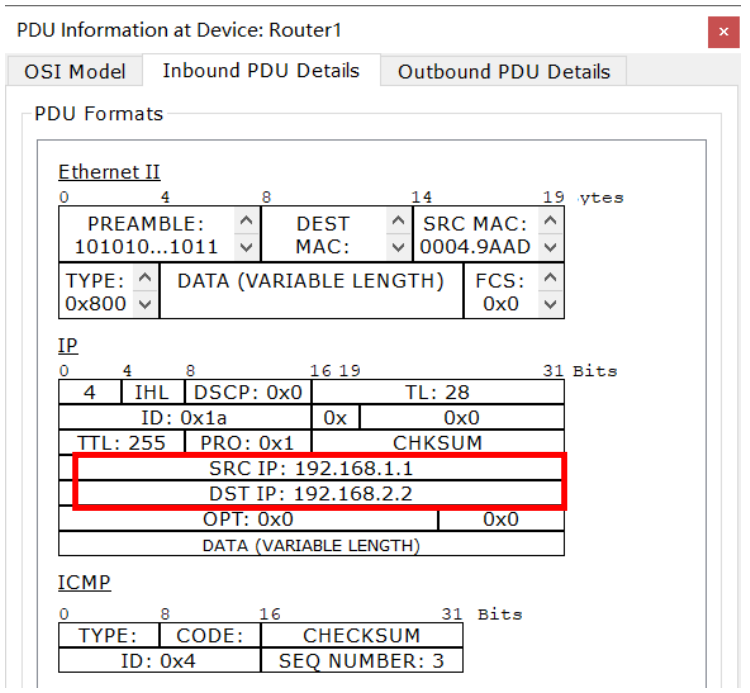
4. 任务二：观察学习 VPN 工作原理。

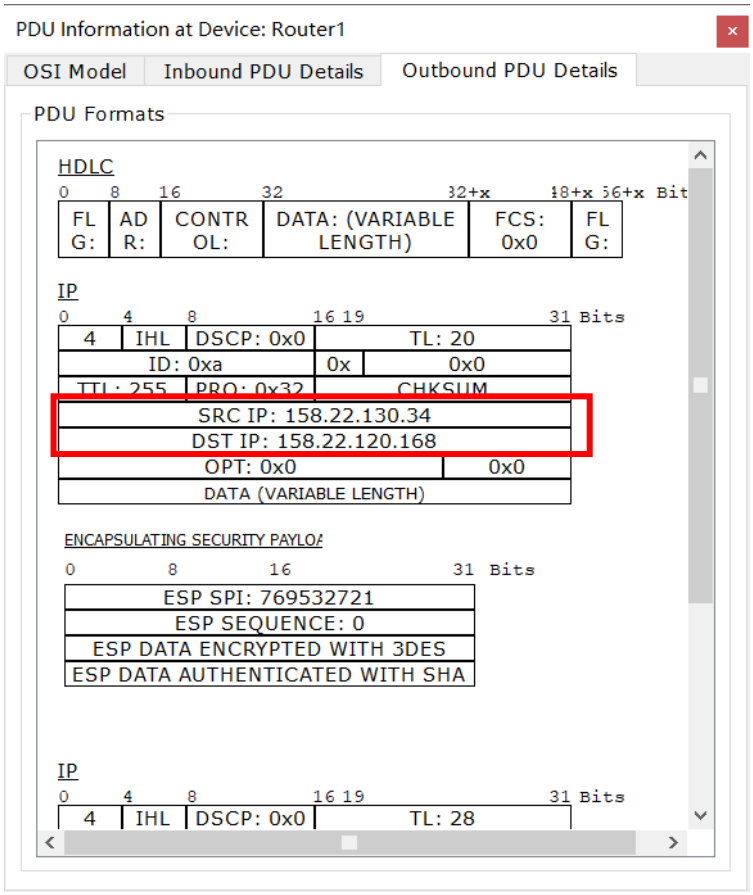
首先进入实时模式，点击添加简单 PDU 按钮，再点击 PC0、PC3，添加从 PC0 至 PC3 的简单 PDU，再切换至模拟模式，设置事件列表过滤器仅显示 ICMP 事件，点击 Auto Capture/Play，使得数据包自动完成转发。转发完成后查看其转发过程如下：



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。

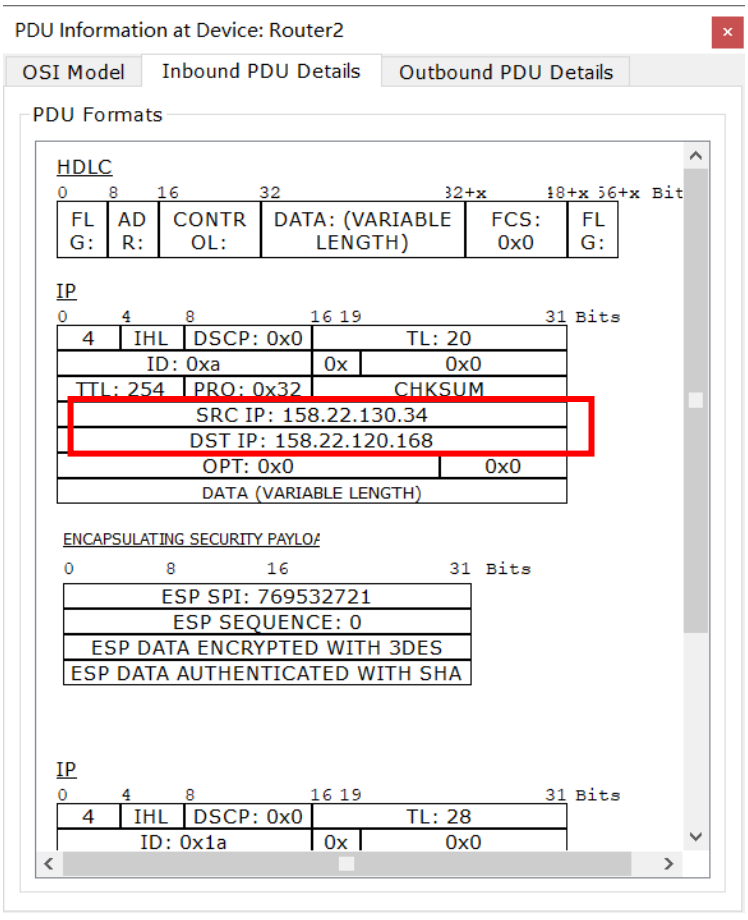
此时查看 PC0 向 PC3 发送数据包过程中 At Device 为 Router 1 的事件，点击 info 标签，分别查看其 Inbound PDU Details 和 Outbound PDU Details 选项卡如下：

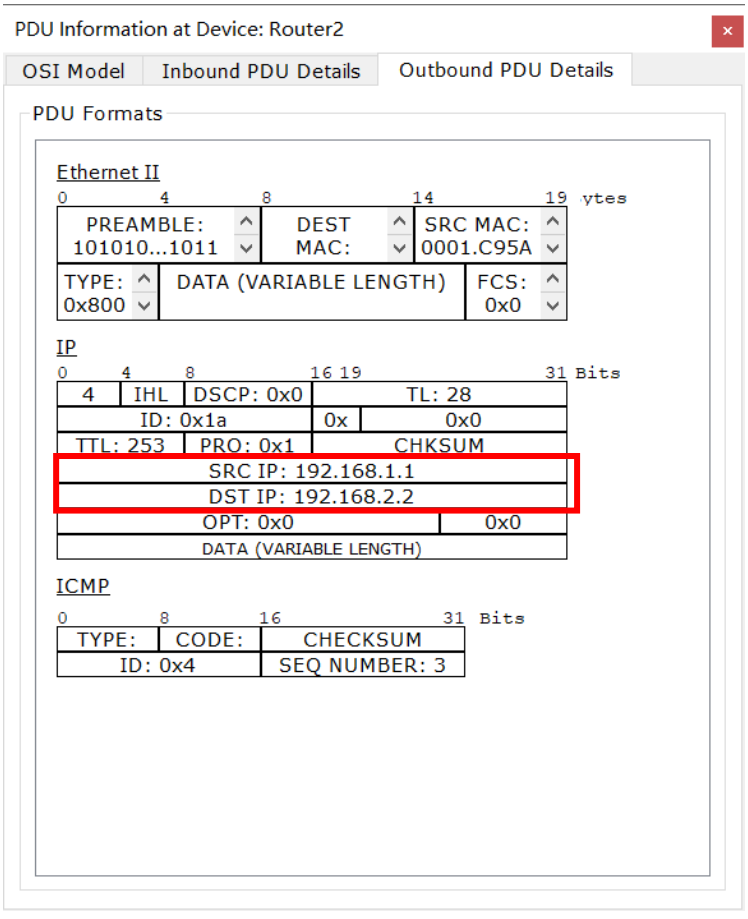




由图可知，随着 Router 1 的转发，源 IP 与目的 IP 均从私有地址转换为对应的全局地址，且原有 IP 数据报被封装在该数据包中。

按照同样的方法查看 Router 2 中的 PDU 的信息如下：


PDU Information at Device: Router2
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
HDLC
0 8 16 32 32+x 48+x 56+x Bit
FLG: | ADR: | CONTROL: | DATA: (VARIABLE LENGTH) | FCS: 0x0 | FLG:
IP
0 4 8 16 19 31 Bits
4 | IHL | DSCP: 0x0 | TL: 20
ID: 0xa | 0x | 0x0
TTL: 254 | PRO: 0x32 | CHKSUM
SRC IP: 158.22.130.34
DST IP: 158.22.120.168
OPT: 0x0 | 0x0
DATA (VARIABLE LENGTH)
ENCAPSULATING SECURITY PAYLOA
0 8 16 31 Bits
ESP SPI: 769532721
ESP SEQUENCE: 0
ESP DATA ENCRYPTED WITH 3DES
ESP DATA AUTHENTICATED WITH SHA
IP
0 4 8 16 19 31 Bits
4 | IHL | DSCP: 0x0 | TL: 28
ID: 0x1a | 0x | 0x0


PDU Information at Device: Router2
OSI Model
Inbound PDU Details
Outbound PDU Details
PDU Formats
Ethernet II
0 4 8 14 19 ytes
PREAMBLE: 101010...1011 | DEST MAC: | SRC MAC: 0001.C95A
TYPE: 0x800 | DATA (VARIABLE LENGTH) | FCS: 0x0
IP
0 4 8 16 19 31 Bits
4 | IHL | DSCP: 0x0 | TL: 28
ID: 0x1a | 0x | 0x0
TTL: 253 | PRO: 0x1 | CHKSUM
SRC IP: 192.168.1.1
DST IP: 192.168.2.2
OPT: 0x0 | 0x0
DATA (VARIABLE LENGTH)
ICMP
0 8 16 31 Bits
TYPE: | CODE: | CHECKSUM
ID: 0x4 | SEQ NUMBER: 3

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。

2. 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。

3. 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。

4. 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。