**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 夏雨轩 学号 21009201006

同作者 无

实验日期 2023 年 11 月 24 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

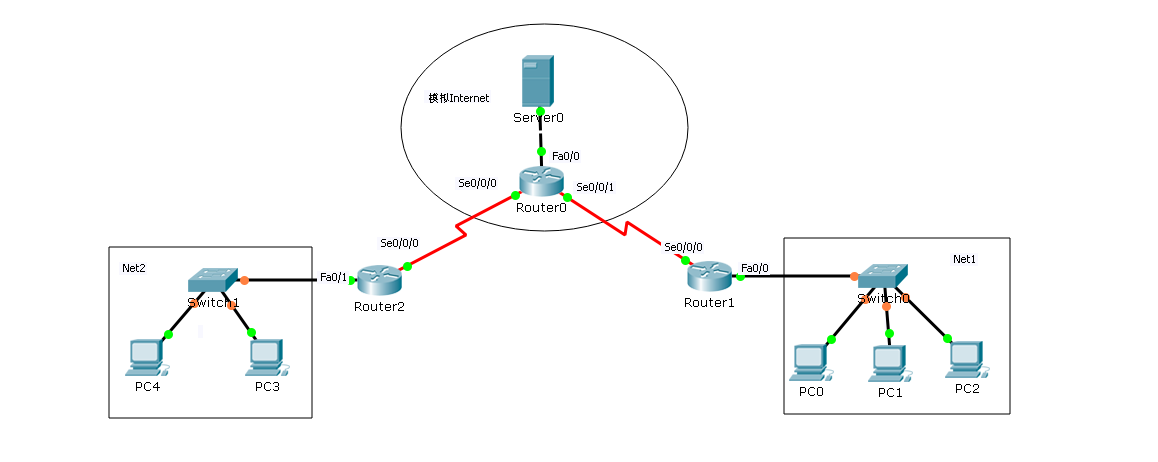
## 一、实验目的

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）

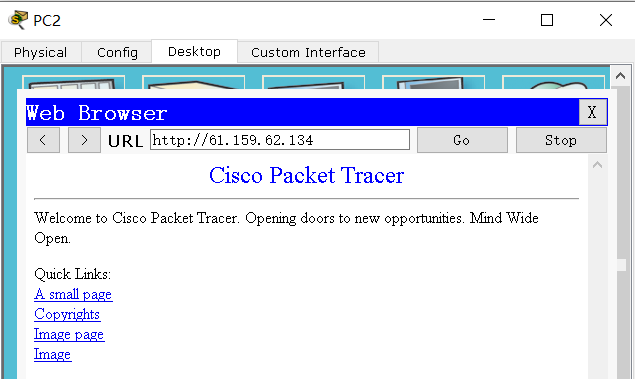
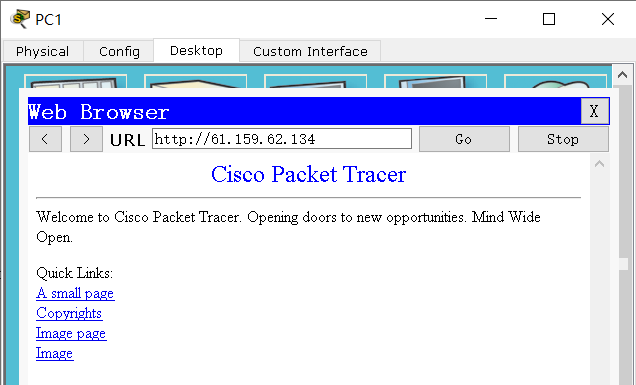
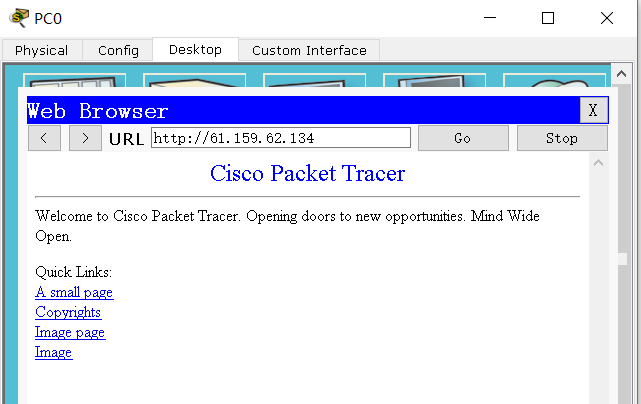
**分别在PC0~PC2中访问Web服务器**

·在Desktop打开Web Browser，在URL地址栏中输入http://61.159.62.134。

在实时模式的逻辑空间中单击 PCO，表示这一步表示选择了 PC0 这台模拟计算机。在Desktop 中打Web Browser按钮(网页浏览器)，这是一种用于浏览互联网的应用程序。

在URL地址栏中输入并回车。此时可以输入地址，看到打开的网页。这一步表示成功地在 PC0 上输入了一个网页地址，并且浏览器加载了相应的网页内容。目的是查看或与指定的网页进行交互。

按同样的方法，也分别在 PC1和PC2中访问Web服务器。

总体来说，这系列操作的目的是通过模拟环境中的不同计算机，使用Web浏览器访问特定的网页或Web服务器。是为了测试网络的连通性，验证Web服务器的可访问性，进行其他与网络浏览相关的实验和操作。

**观察NAT路由器对数据包的处理方法**

·进入Simulation模式，观察到HTTP报文的往返过程

进入Simulation(模拟)模式。这一步将软件切换到模拟模式，使用户能够模拟网络环境中的不同事件和流量。

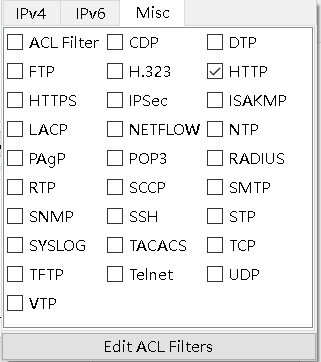
设置Event List Filters(事件列表过滤器)只显示HTTP事件。在模拟模式下，用户通过设置事件列表过滤器，选择只显示与 HTTP 相关用户打开 PC0 的 Web 浏览器，并刷新网页，这是为了触发 HTTP 请求和响应的传输。

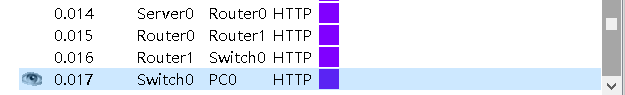
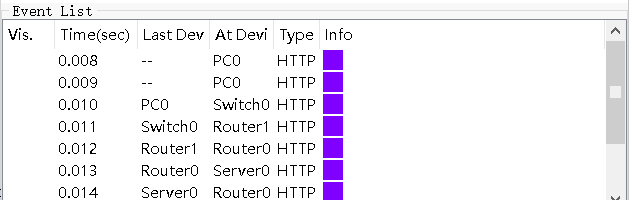
在PCO的Web Browser 中重新刷新网页，用户打开 PC0 的 Web 浏览器，并刷新网页，这可能是为了触发 HTTP 请求和响应的传输。

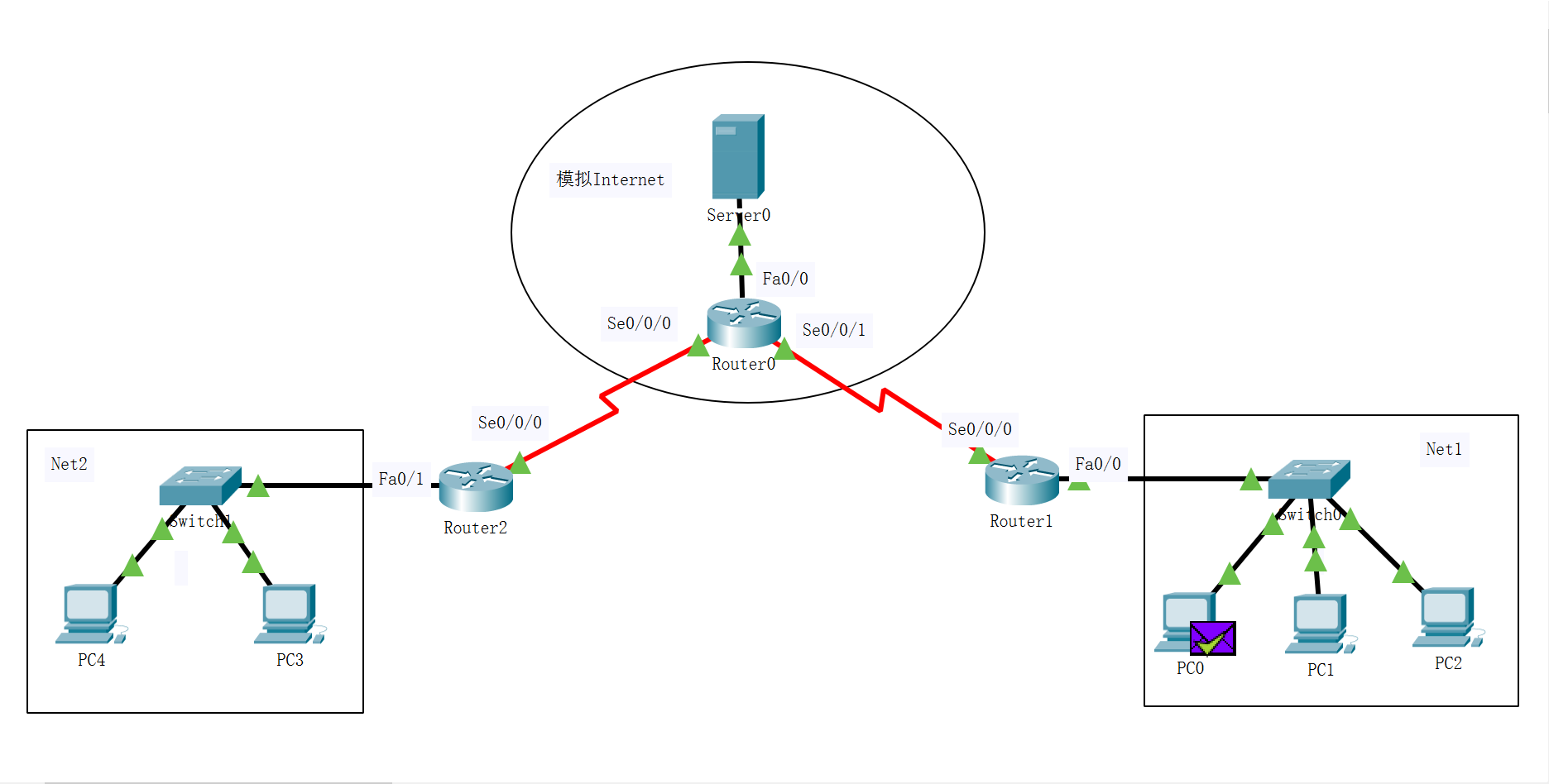
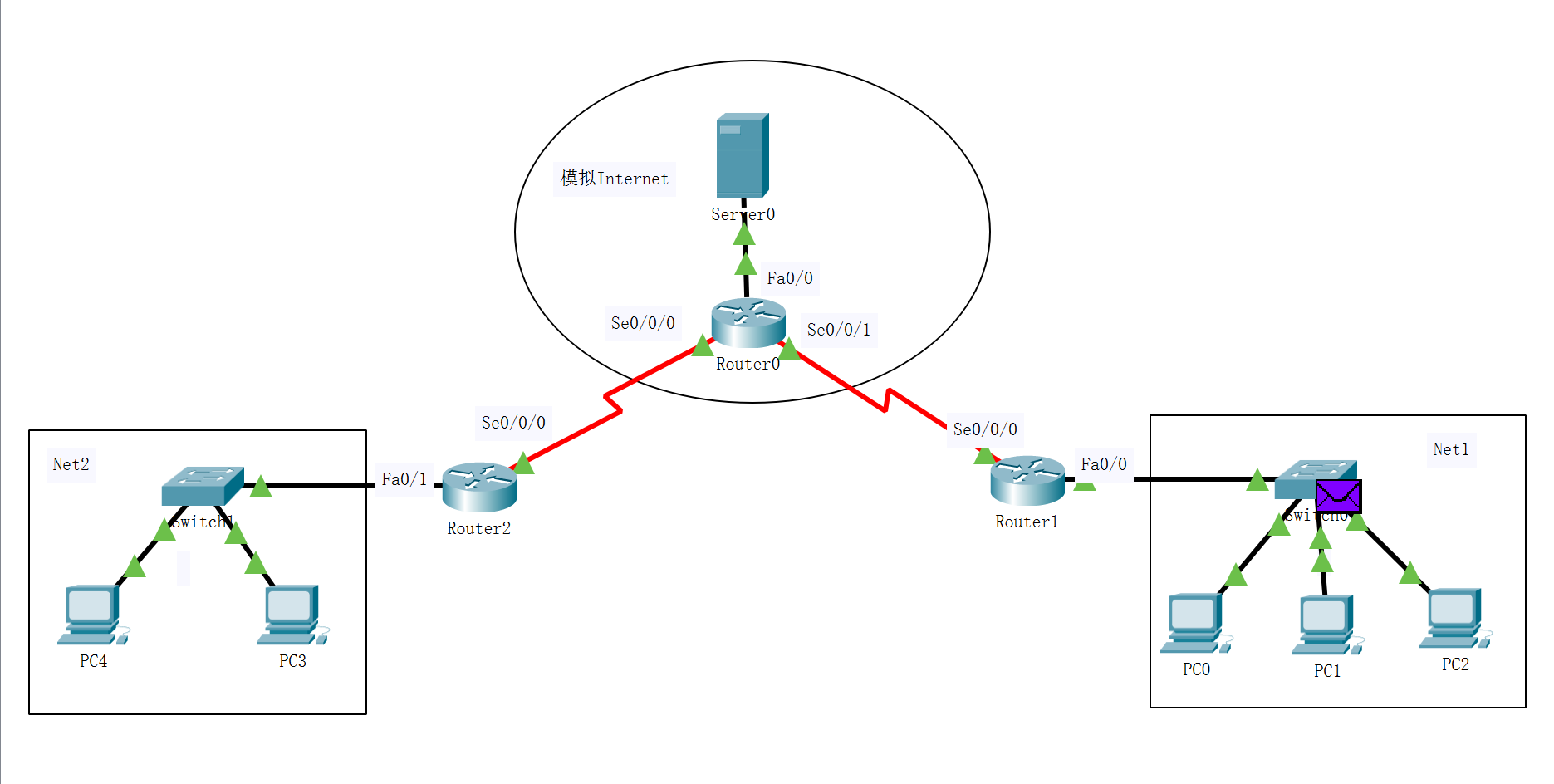
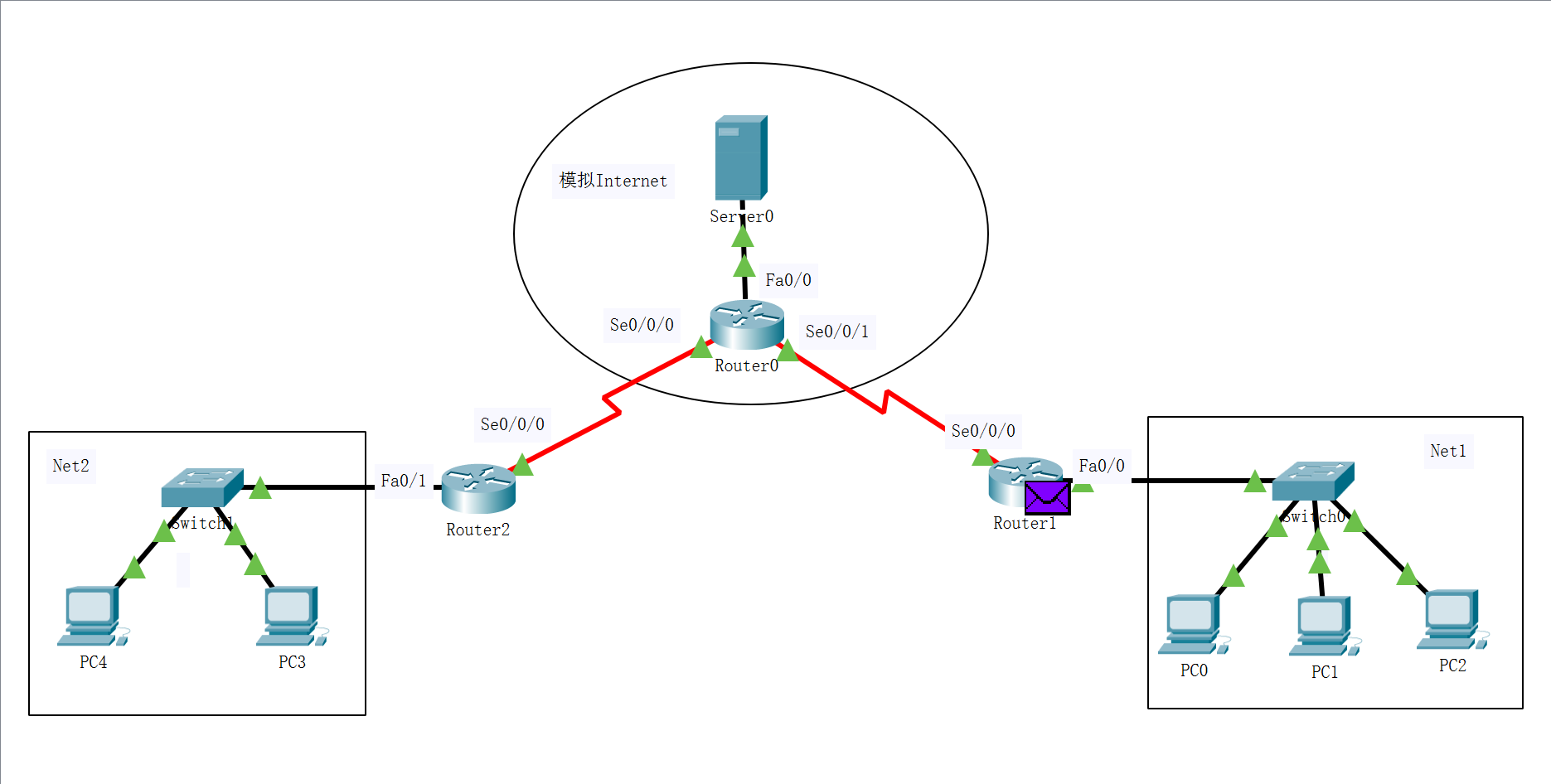
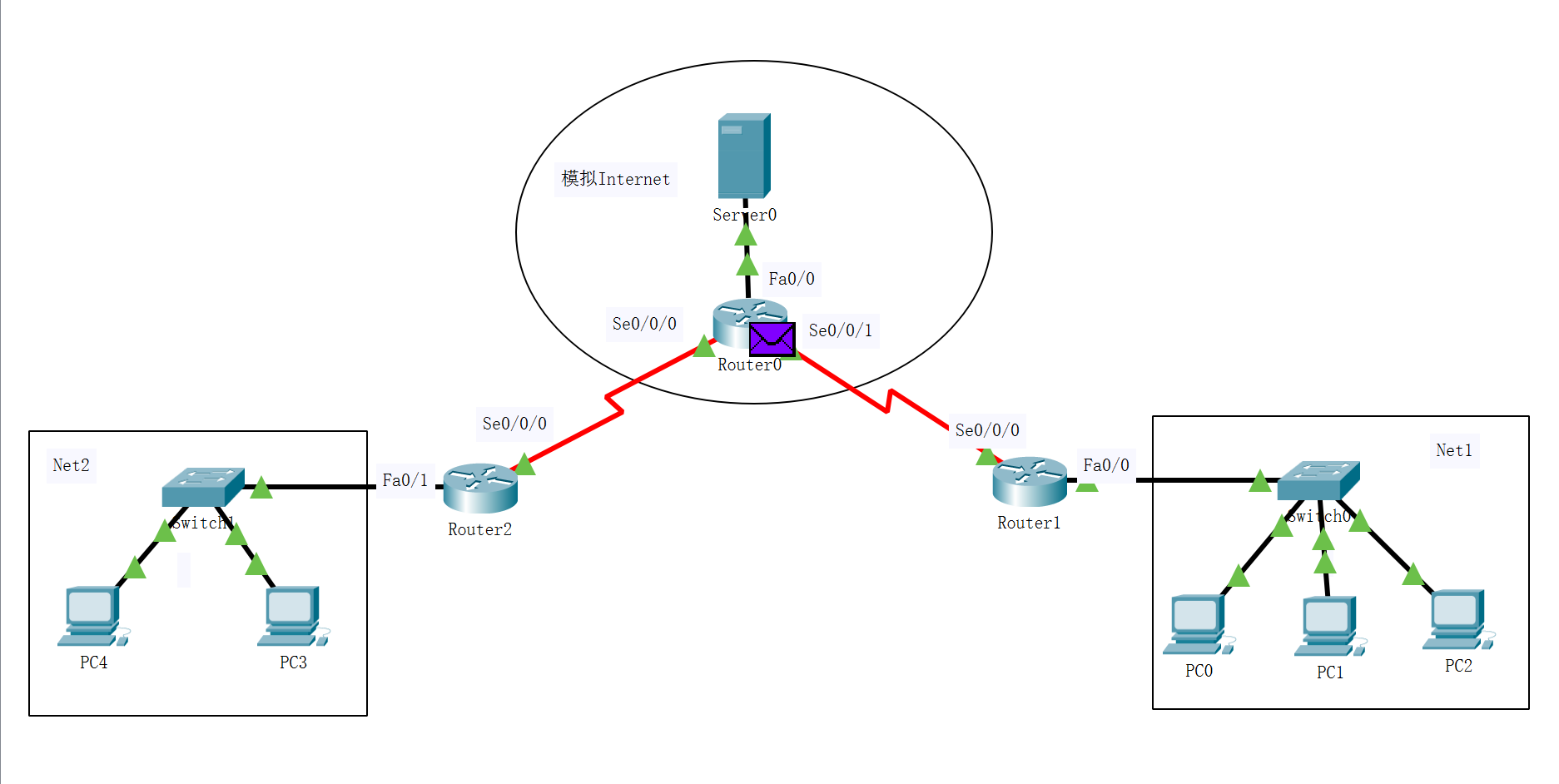
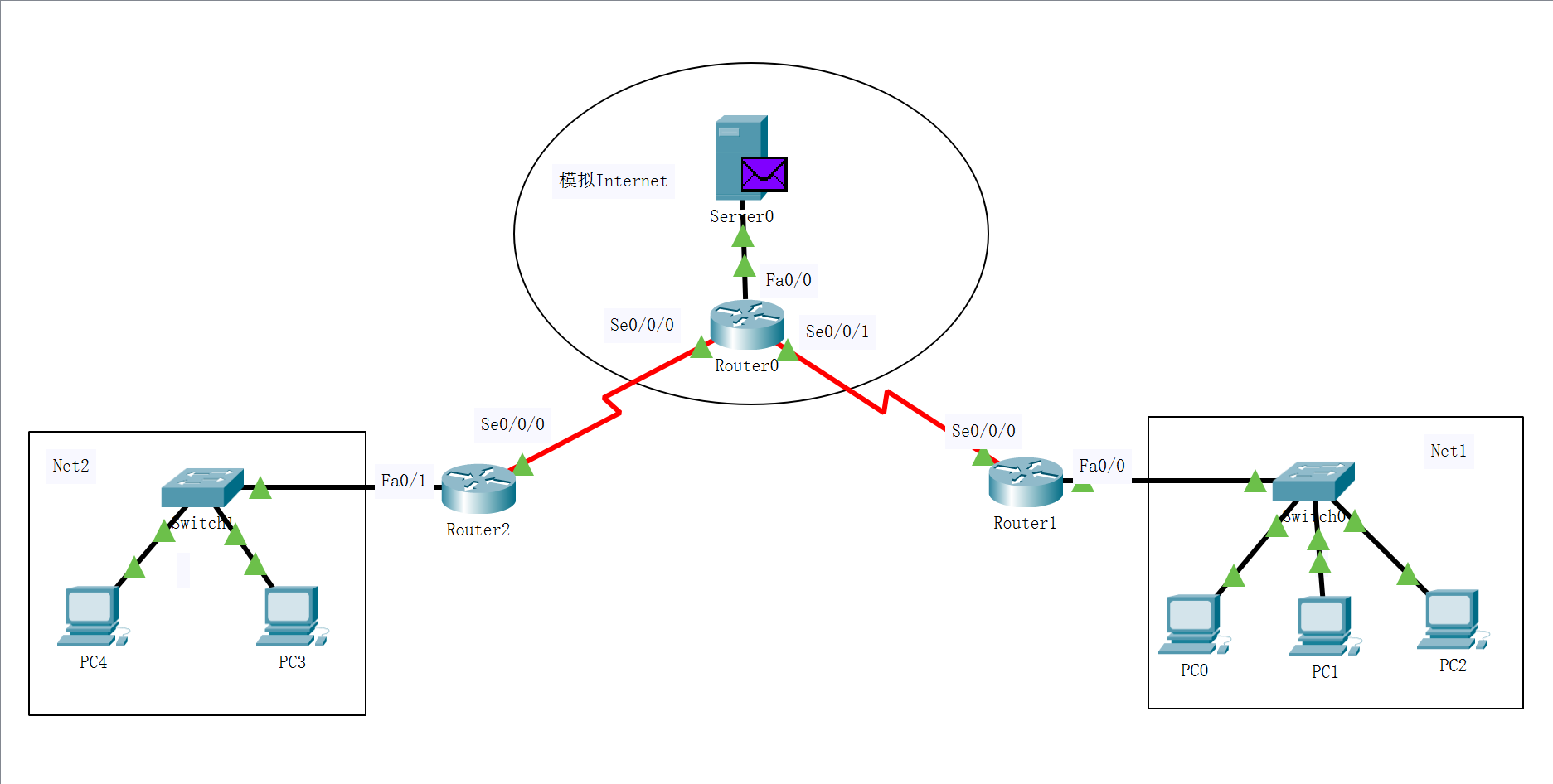
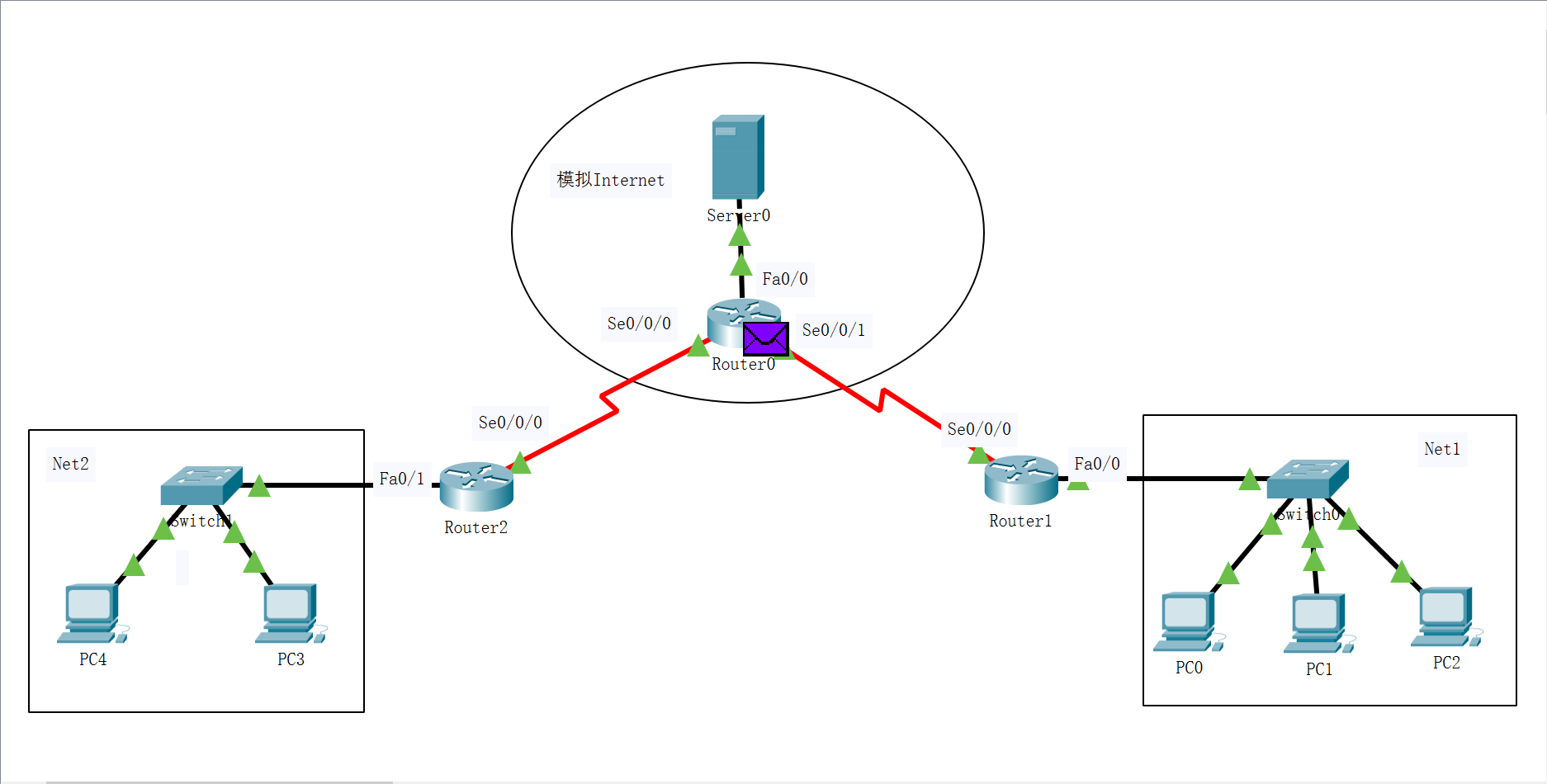
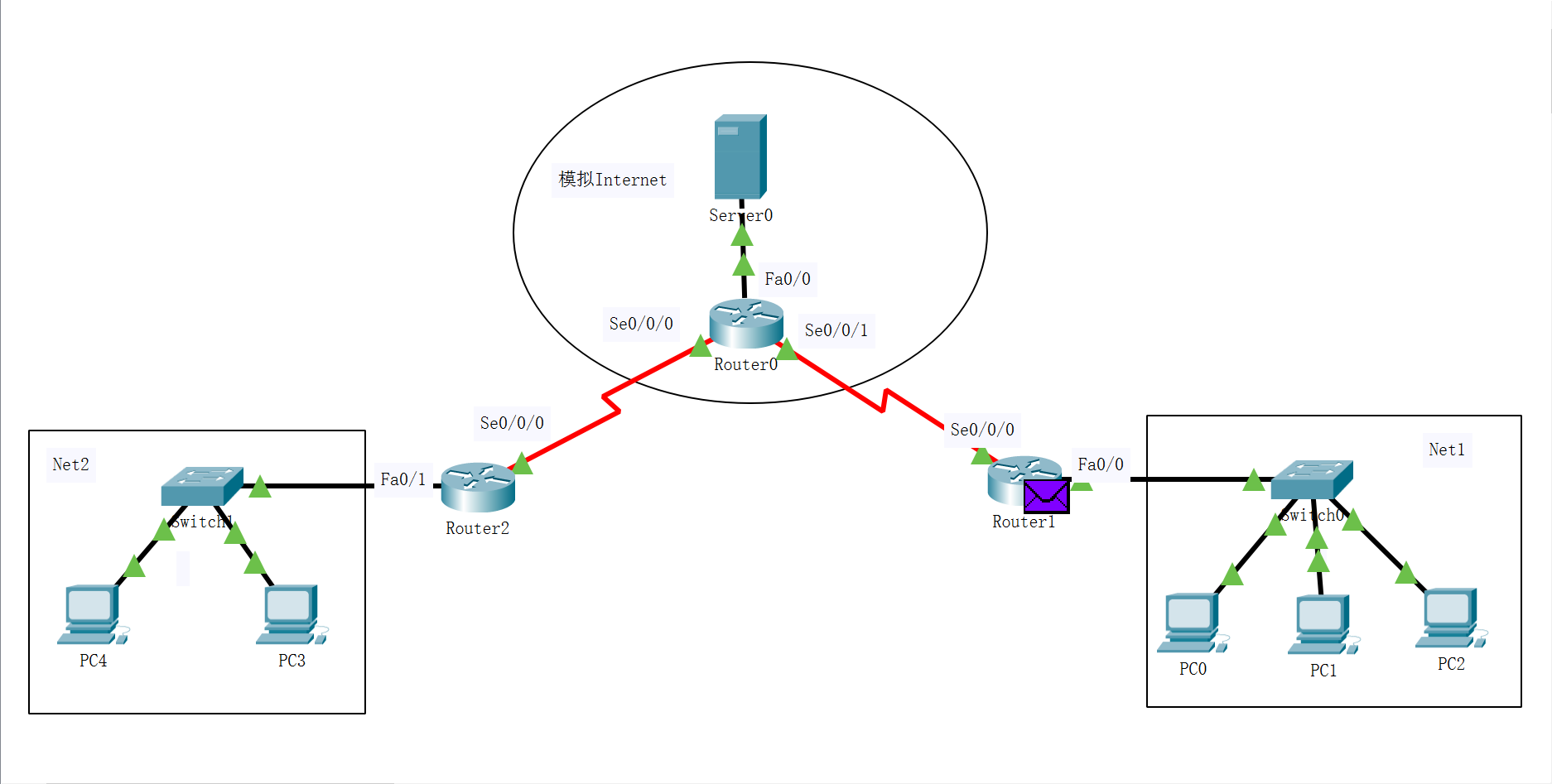
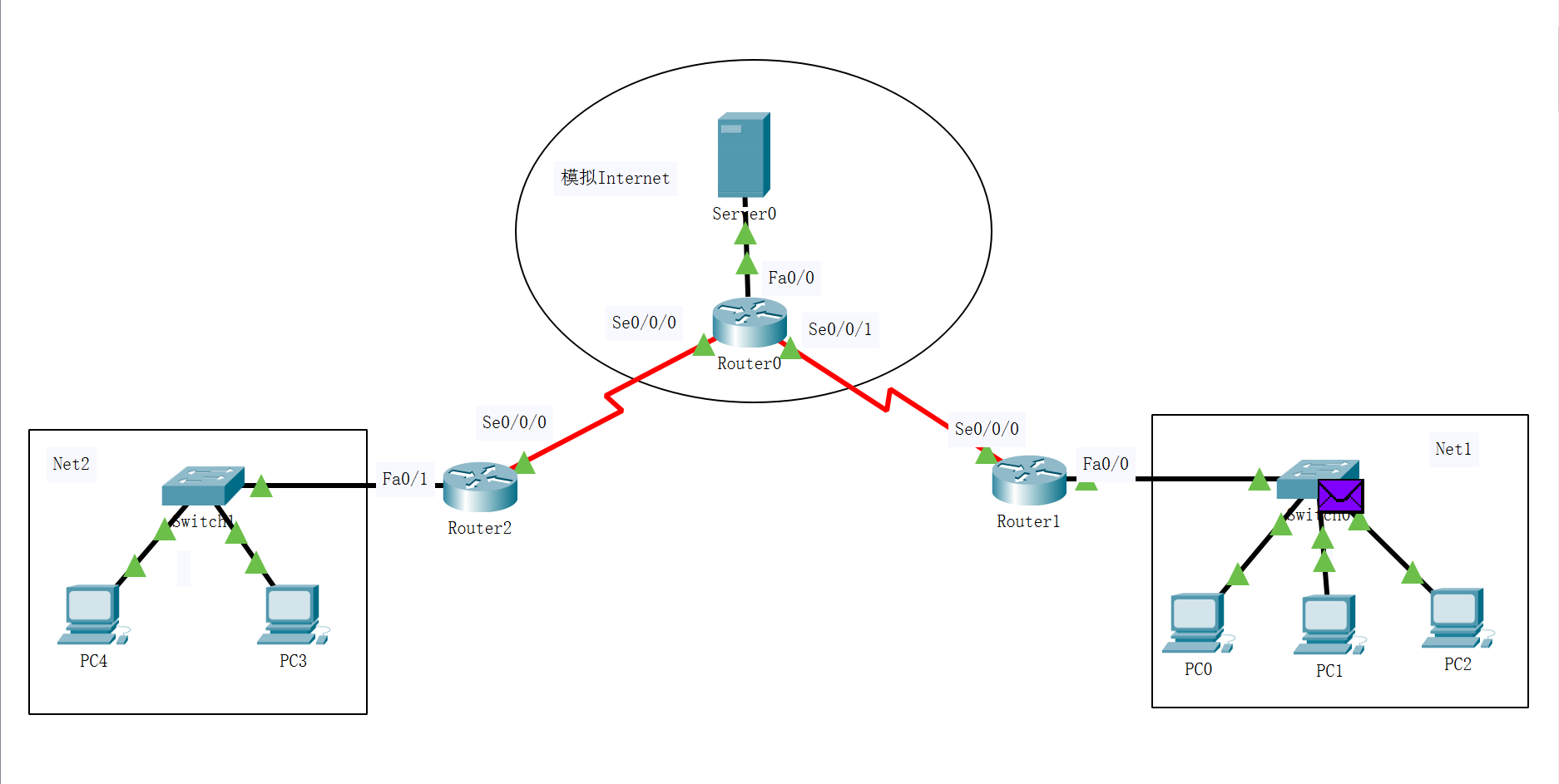
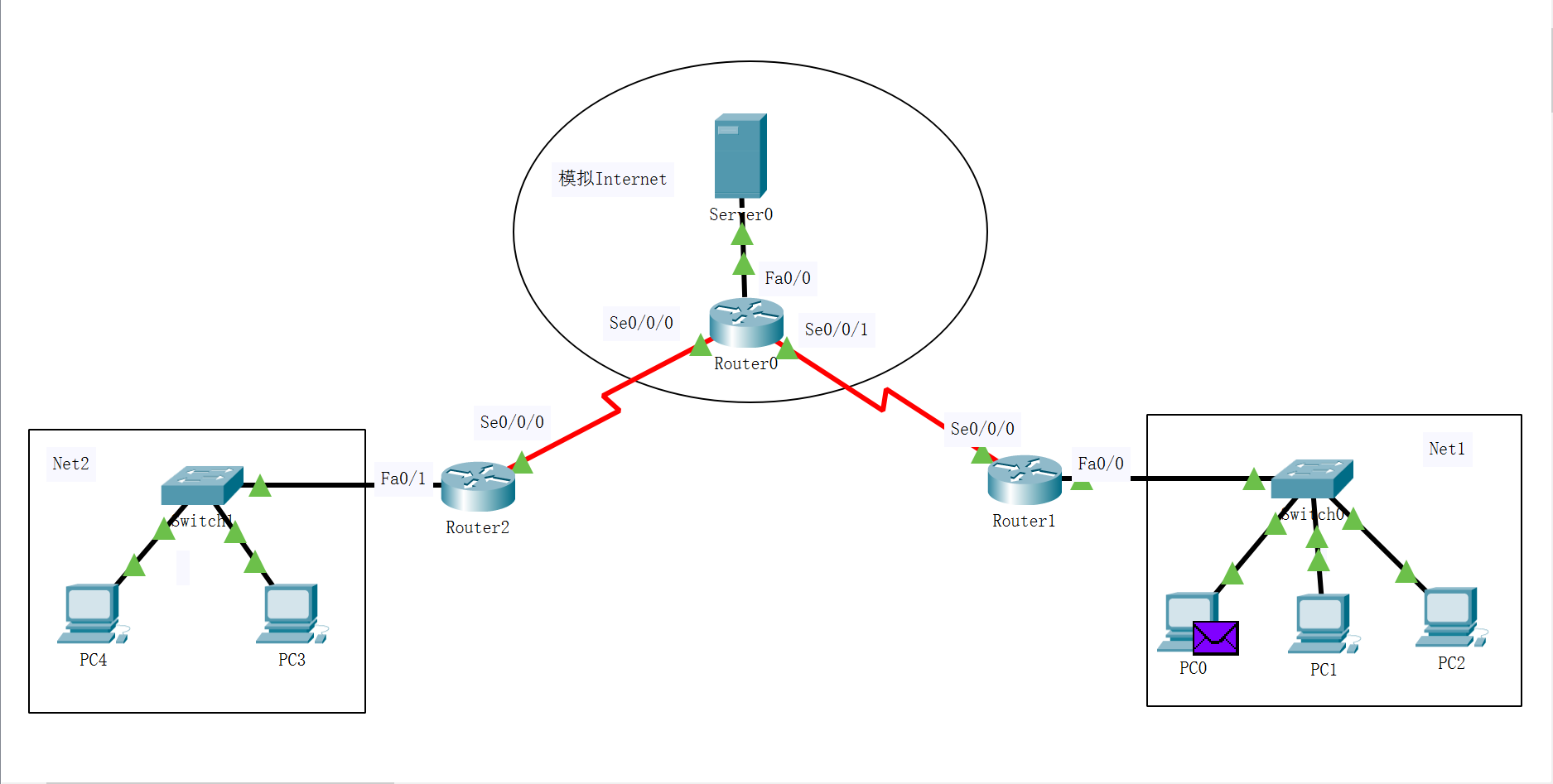
并逐步单击Capture/Forward 按以控制模拟进程，此时可观察到HTTP报文的传输往返过程。用户通过逐步单击 Capture/Forward 按钮，控制模拟过程的进行。这是为了逐步观察模拟中发生的事件，特别是与 HTTP 报文相关的事件。在模拟过程中，用户可以观察到 HTTP 报文的传输往返过程，了解请求和响应之间的交互。

当出现 Buffer Full 窗口时，停止模拟过程。

总体而言，这一系列操作的目的是在模拟环境中，通过设置过滤器、刷新网页、逐步控制模拟进程，观察并分析 HTTP 报文的传输过程。模拟环境中的 Buffer Full 窗口出现表示要进行进一步的分析。

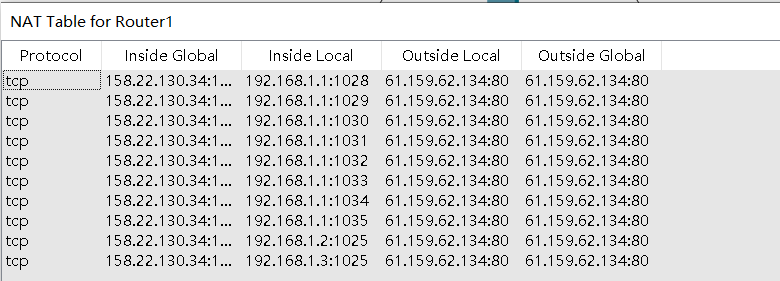






·使用检查工具（检查工具可能是网络设备提供的一种工具或命令行工具，用于检查和显示网络设备的配置、状态或其他信息。）打开Router1的NAT 地址转换表。

使用检查工具，用户打开Router1上的NAT（Network Address Translation）地址转换表。NAT是一种网络技术，用于将私有IP地址转换为公共IP地址，以实现在私有网络和公共网络之间进行通信。



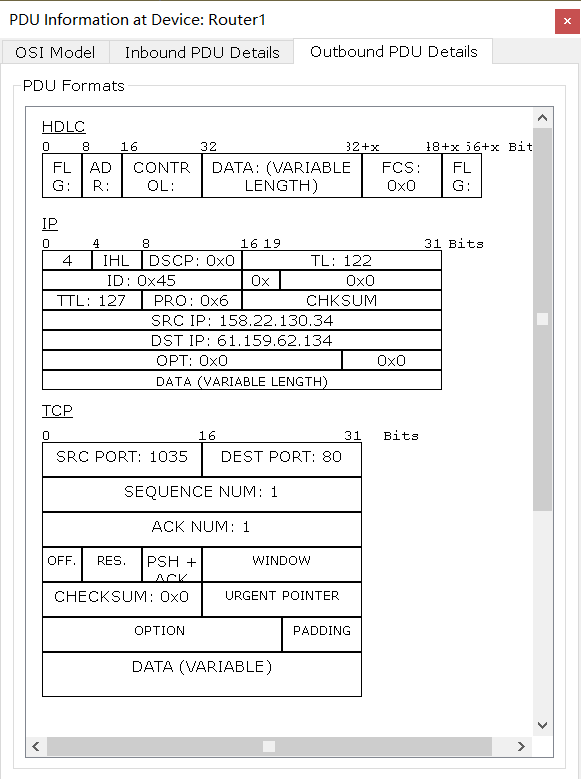
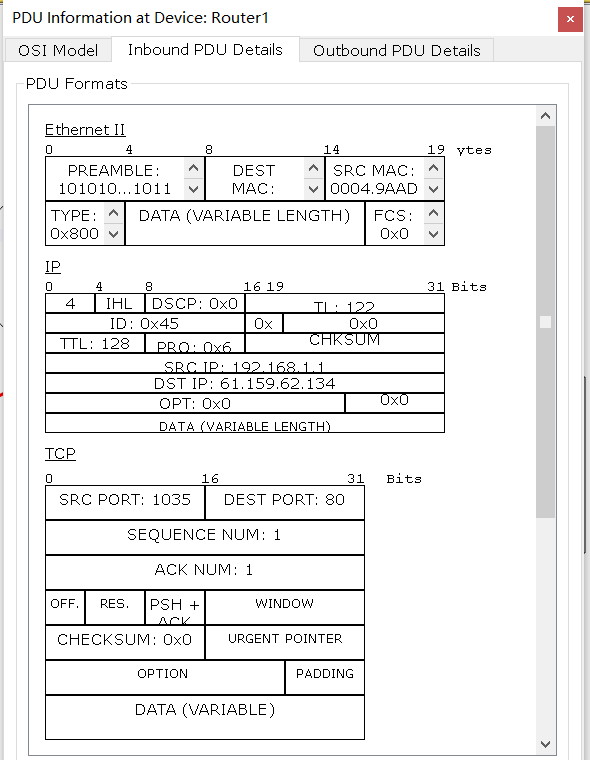
·观察数据包的处理，对比Inbound PDU Details和 Outbound PDU Details。

在Event List窗口中找到At Device中显示为Router1的事件，单击其彩色正方形。分别单击Inbound PDU Details和Outbound PDU Details选项卡，这将允许用户查看并对比进入Router1的PDU和离开Router1的PDU的详细信息。

同时查看和对比PDU内容的区别。在Inbound PDU Details选项卡中，观察PDU的内容，特别关注源和目标IP地址。然后切换到Outbound PDU Details选项卡，继续观察相同的PDU，但此时已经通过NAT进行了转换。比较两者的源目IP地址，以及可能的其他字段，观察转换规律。

我们可以发现在Inbound PDU中,该PDU的源目IP地址分别为192.168.1.1和 61.159.62.134。而在Outbound PDU中PDU的源目IP地址已经更改为158.22.130.34和61.159.62.134。同时对照NAT 地址转换表，可以发现外出数据包的源端口进行了改变，内部网络的私有IP地址转换为了公用IP地址。但目标端口没有发生改变。

进行这一系列的操作的目的是通过观察模拟环境中Router1上的PDU传输，了解NAT对PDU中源目IP地址的修改过程，并对比Inbound和Outbound PDU的内容。这有助于理解NAT如何实现私有IP地址到公共IP地址的映射，以及相应的端口转换规律。这是很重要的，因为可以通过这些信息监控和调试网络中的地址转换过程。



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）

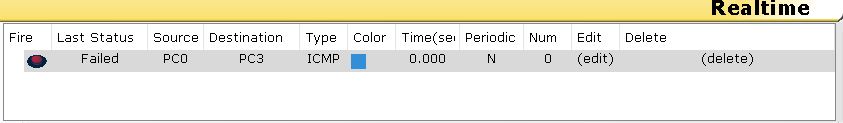
**初始化模拟**

·添加简单PDU，PC0->PC3，该过程的主要目的是初始化VPN连接。

进入实时模式。单击AddSimple PDU(添加简单PDU)按钮，然后分别单击PCO(源站点)和PC3(目标站点)，则PCO将快速向PC3发送一个包含ICMP报文的IP数据报。

PDU是在计算机网络中用于表示数据包的术语，它包含了网络通信中的一些基本信息，如源IP地址、目标IP地址、协议类型等。

初始化VPN连接主要目的是通过模拟这个简单的PDU传输，实现对VPN连接的初始化。VPN连接是一种通过公共网络（例如互联网）建立安全通信的技术。通过发送PDU，模拟数据传输的过程，是为了触发 VPN 连接的建立，进行初始化阶段的通信。

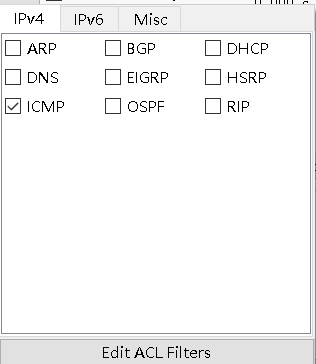


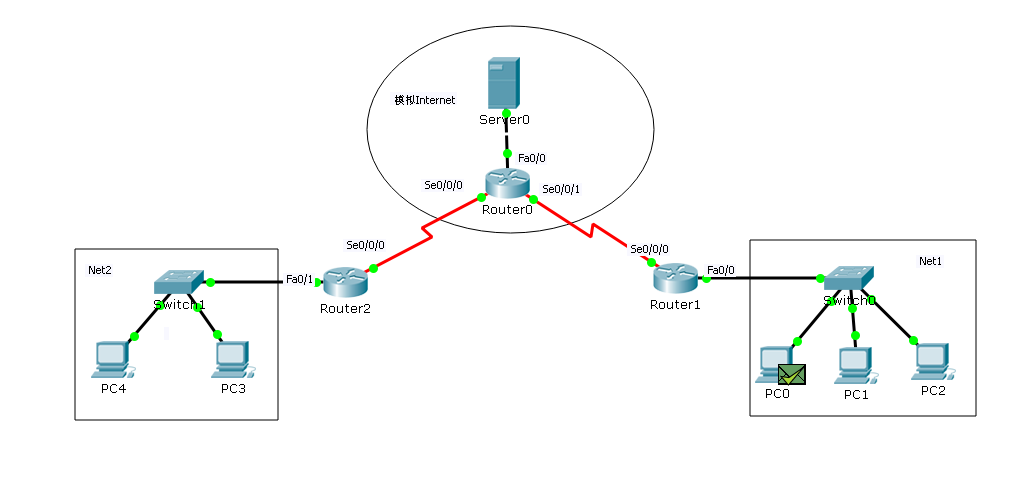
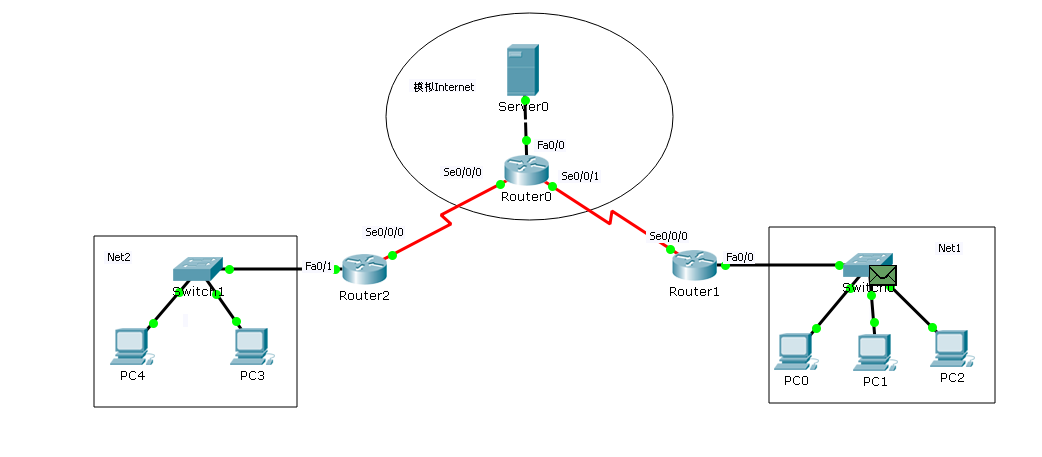
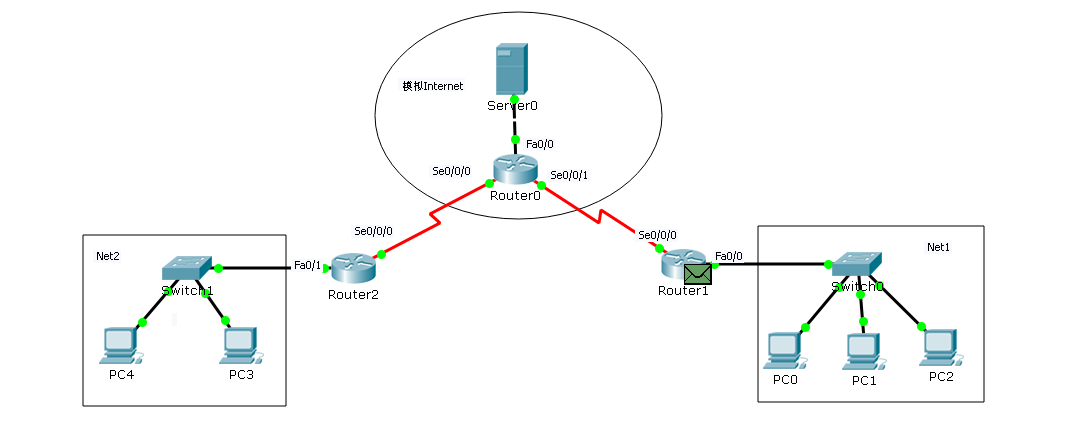
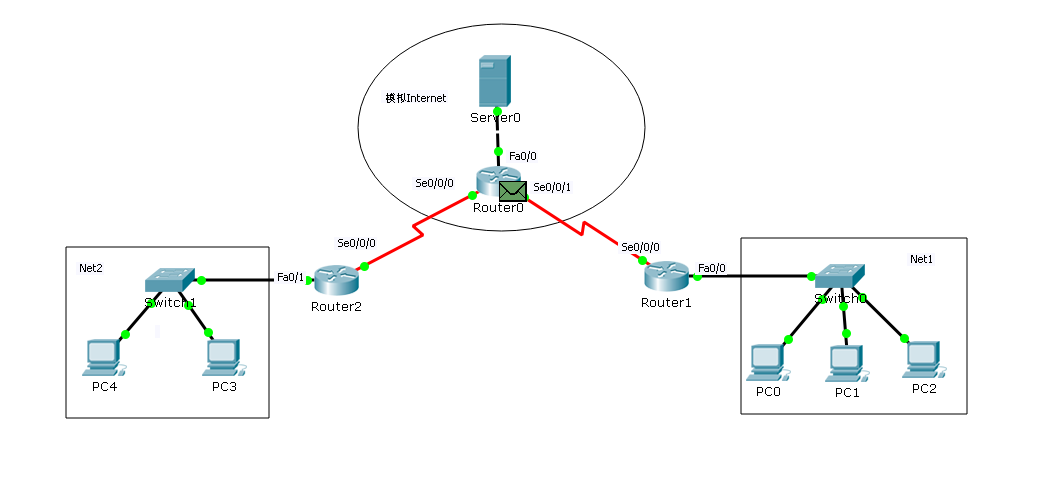
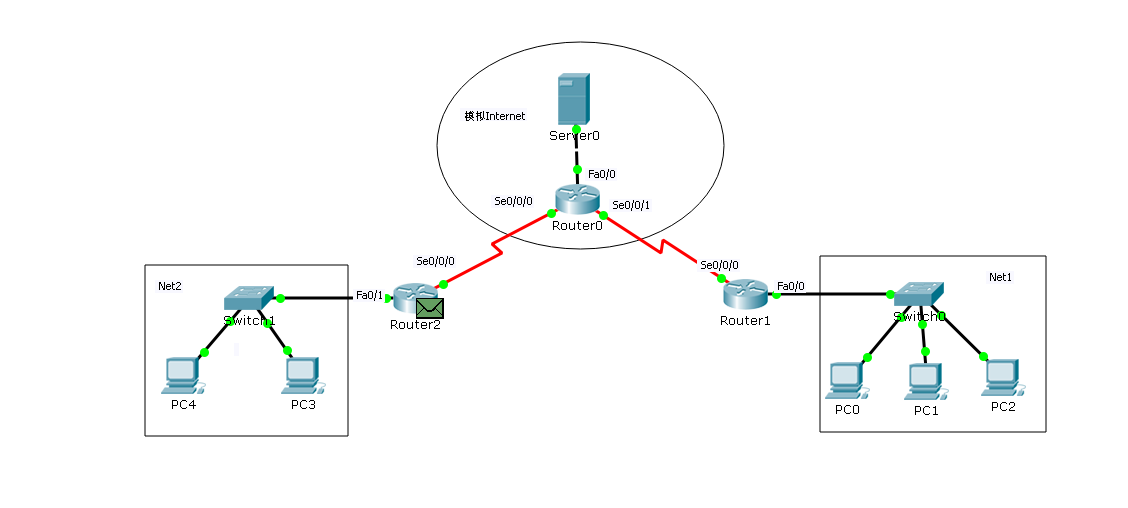
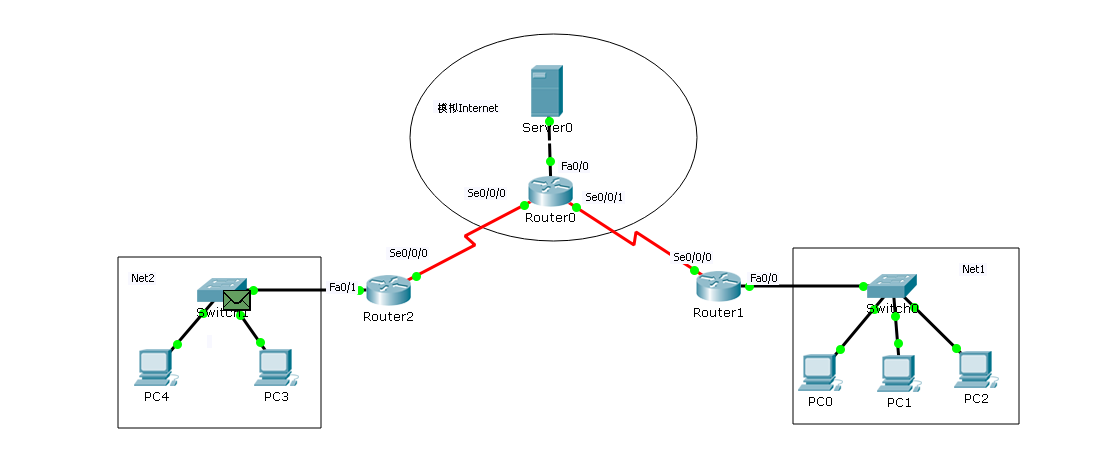
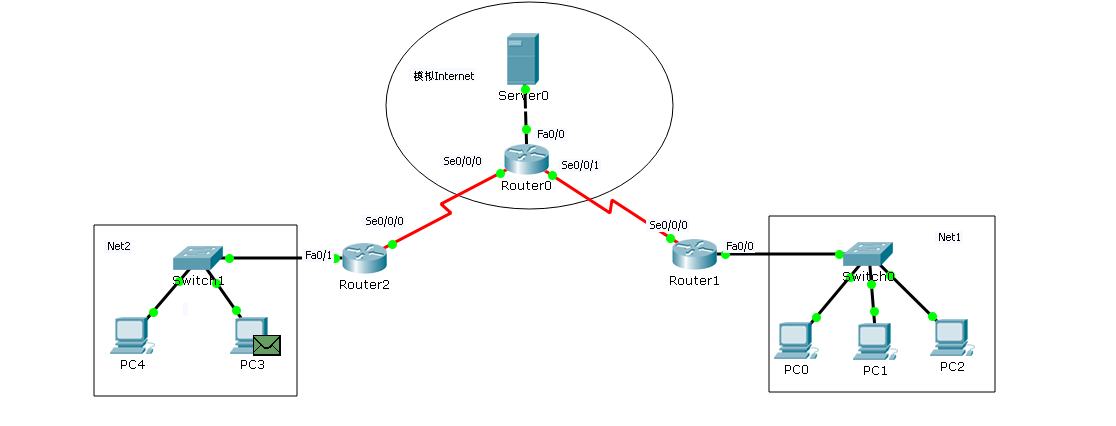
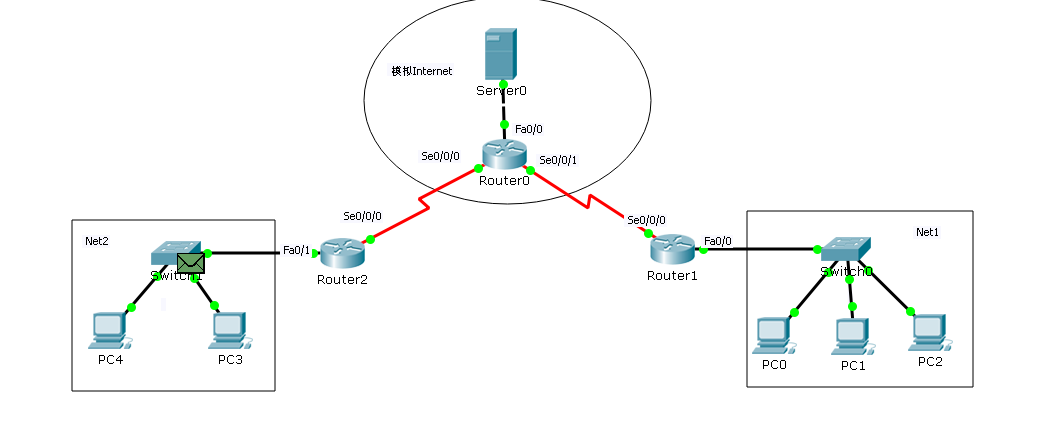
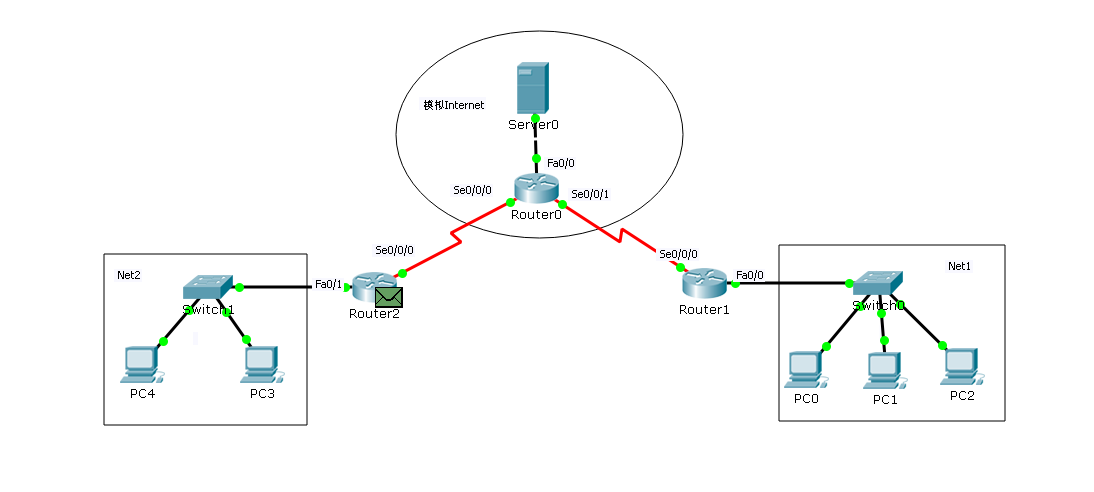
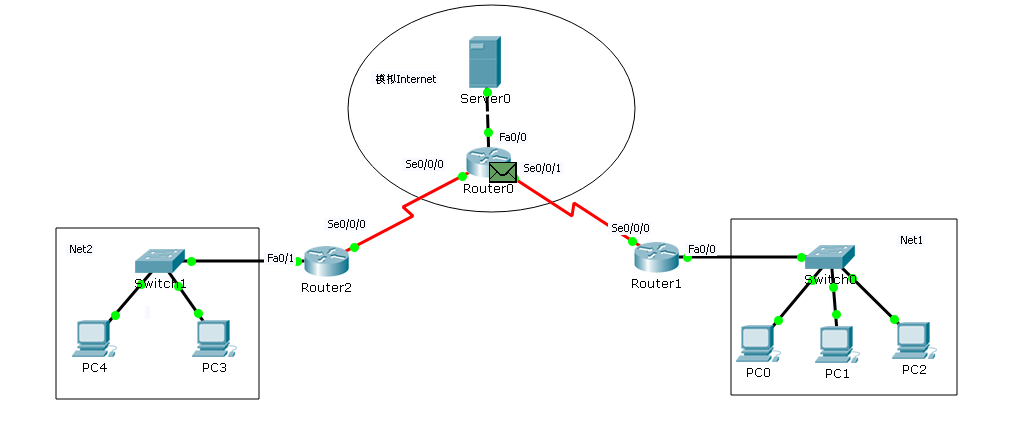
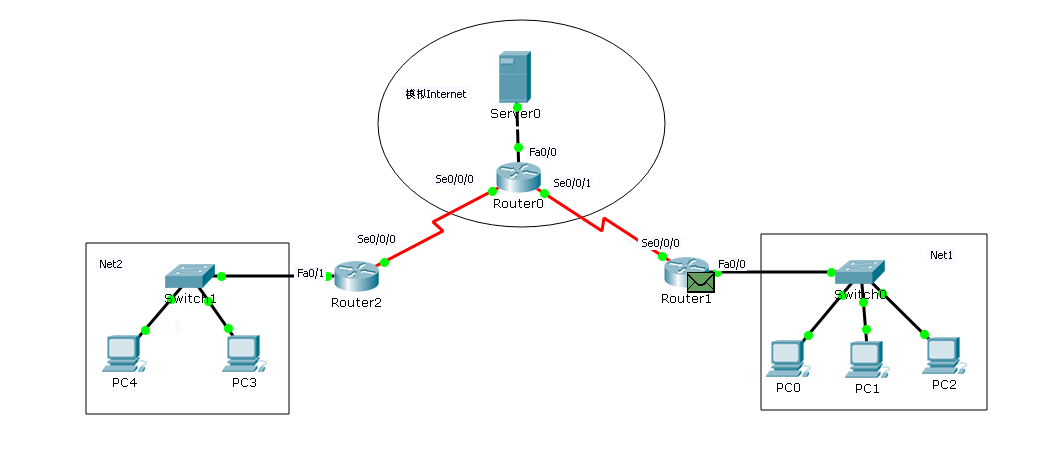
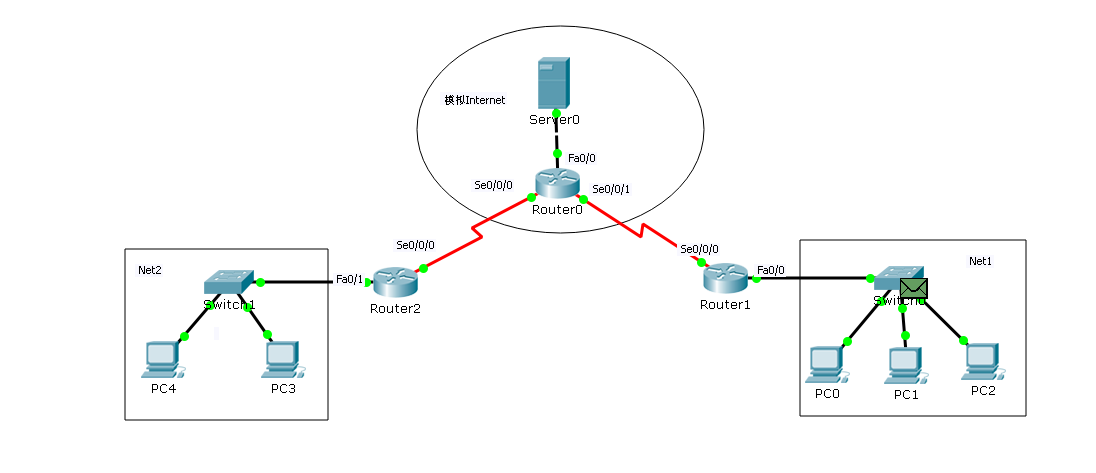
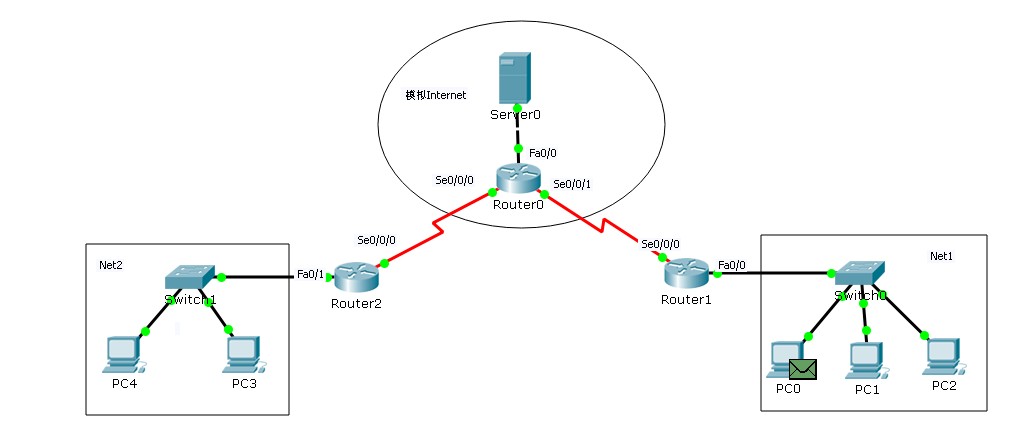
**观察VPN的隧道技术**

·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。

Auto Capture/Play按钮是模拟环境中的一个控制按钮，用于自动捕获事件和数据包，同时运行模拟。用户单击这个按钮会触发模拟环境执行预定义的操作和事件。

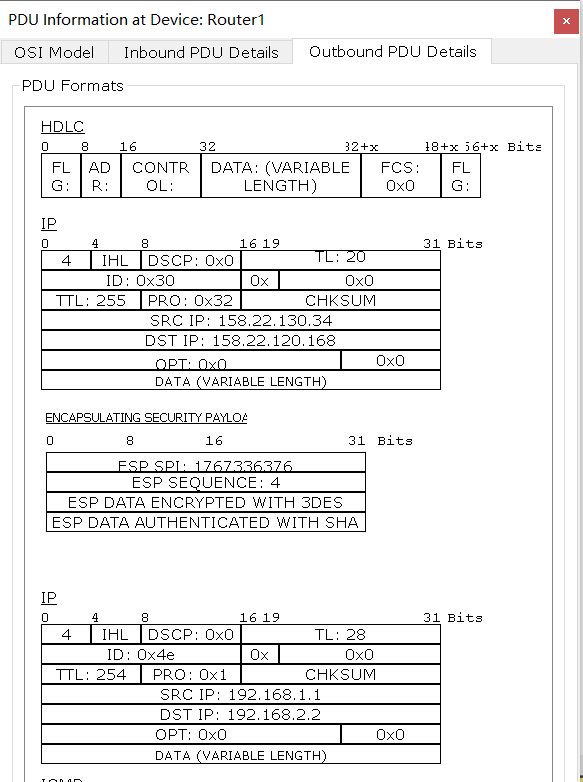
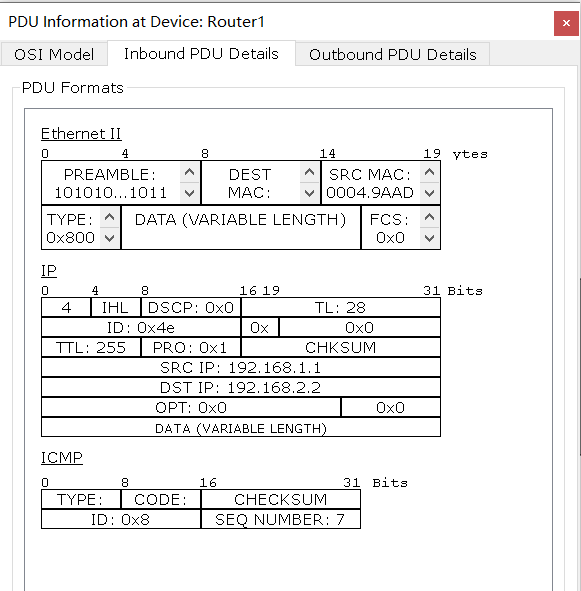
如下图截图所示，ICMP数据报的转发过程为：PC0-Switch1-Router1-Router0-Server0-Router0-Router1-Switch1-PC0。



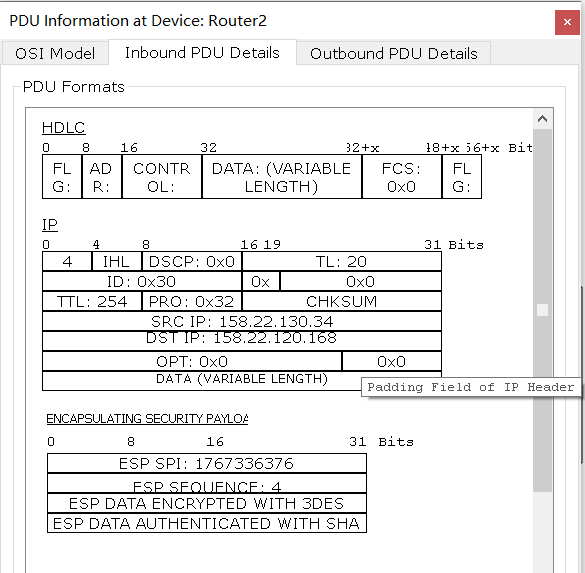


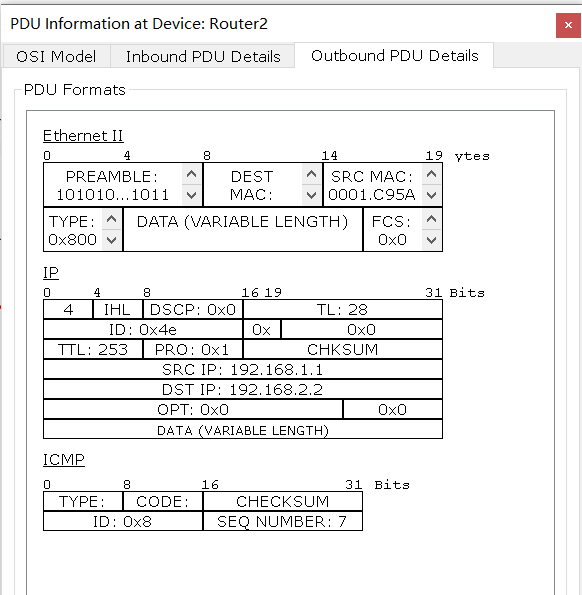
·对比VPN网关对数据包的处理结果，Inbound PDU Details和 Outbound PDU Details。

单击AutoCapture/Play(自动捕获/播放)或者Capture/Forward按钮以运行模拟，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Event List窗口中找到At Device中显示为Router的事件，单击其彩色正方形。分别单击Inbound PDU Details和Outbound PDU Details 选项卡,查看和对比PDU内容的区别。我们可以发现在Inbound PDU中,该PDU的源目P地址分别为192.168.1.1(PCO的IP地址)和192.168.22(PC3的IP地址)。而在Outbound PDU 中，PDU的源目P地址已经更改为158.22.130.34 (Routerl的 Se0/0/0的地址)和18.22120.18 (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Event List窗口中找到At Device中显示为 Router2的事件，单击其彩色正方形。分别单击Inbound PDU Details和Outbound PDU Details选项。卡以查看和对比PDU内容的区别。我们可以发现在Inbound PDU中,该PDU的源目IP地址分别为158.22.130.34(Routerl的 Se0/0/0的IP地址)和158.22.120.168 (Router2的 Se0/0/0的P 地址)。而在 Outbound PDU 中PDU的源目IP地址已经更改为192.168.1.1(PCO的P地址)和192.168.2.2(PC3的IP地址)，这说明PCO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？

NAT服务器（Router1）通过不同的端口号来识别不同主机的报文。

1. 在任务二中，VPN中采用隧道技术的原因是什么？。

因为Net1和Net2都是私有地址，无法直接通过Internet进行通信，采用隧道技术可以将源地址转换为全局地址，到达目标路由器后也很容易获得真正目标主机的ip地址。

1. Net1网络和Net2网络的IP地址能否编在同一段？

不能，这样容易造成主机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？

做任务二的时候，发现数据包传到Router2就丢弃了，但重新delete所有场景后再做一遍，就成功解决了。通过该实验，我理解了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。

