《信息安全及实践》课程实验报告

学院 信息学院 专业 计算机科学与技术 年级 2020级

姓名 黄珀芝 学号 20201050331

实验时间 2022 年 11 月 5 日

实验名称 点对点IP隧道实验、IOS路由器IP Sec VPN实验

实验成绩

点对点IP隧道实验

一、实验目的

(1)拿握VPN设计过程

(2)掌握点对点IP融道配置过程

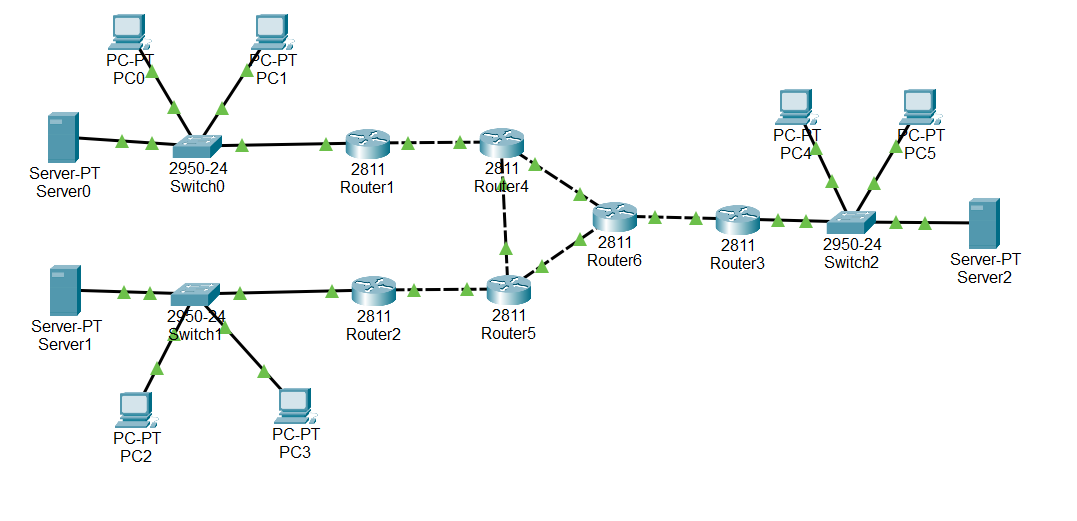
(3)握公共网络路由项建立过程

(4)握内部网络路由项建立过

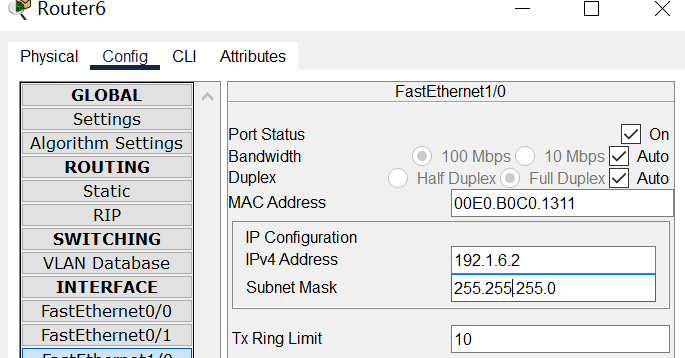
(5)验证公共网络離道两端之间的传输路径的建立过程

(6)验证基于隧道实现的内部子网之向IP分组传输过程

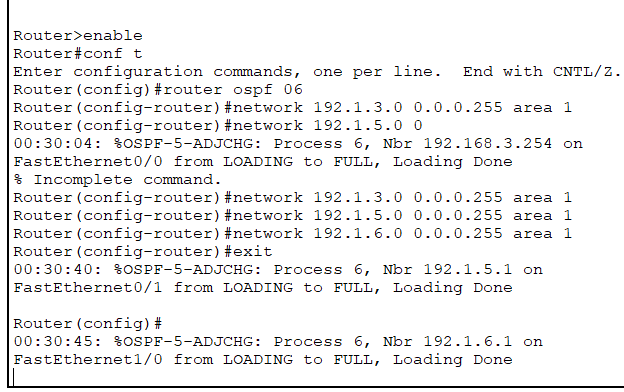
1. 实验步骤(含程序清单)
2. 完成设备放置和连接。



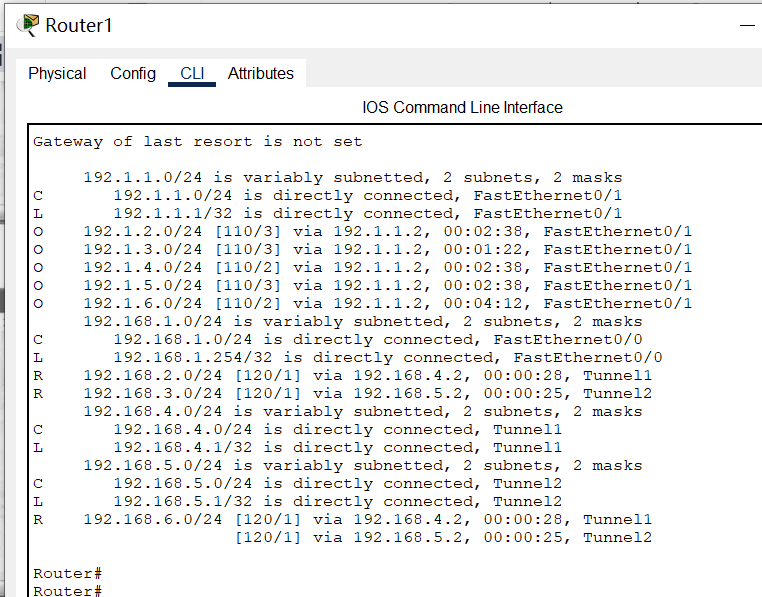
1. 为每一台路由器的各个接口配置ip地址和子网掩码，如图给出配置了router6的。

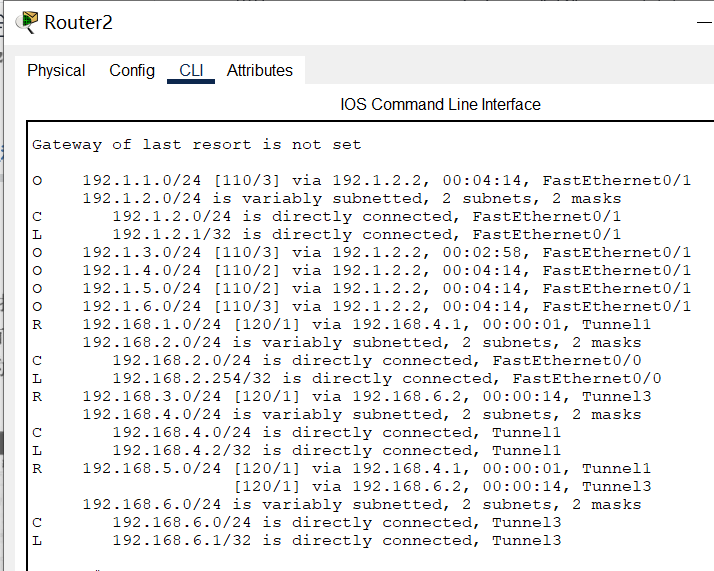


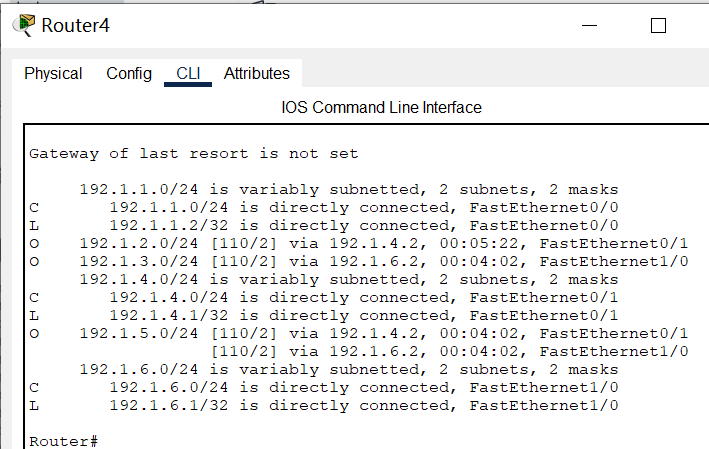
（3）在命令行接口配置方式下,完成以下功能的配置过程：定义路由器R

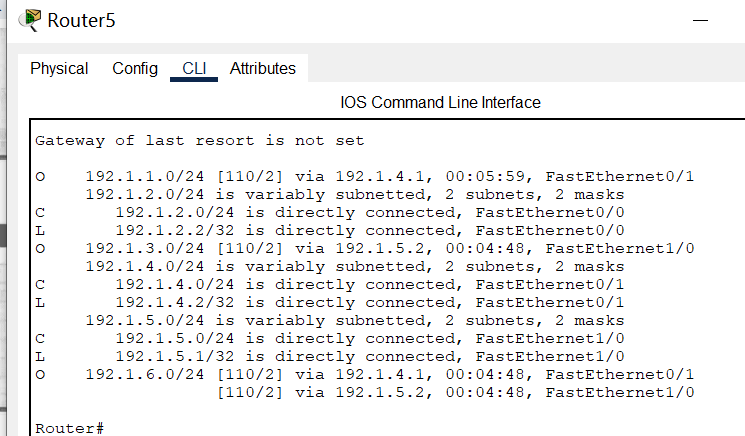
Rouet2和 Router3连接公共网络的接口之间的IP隧道:为隧道接口配置私有IP地址。路由器 Router, Router2和 Router3在直接连接的网络中,选内部网络和道接口连接的网络作为参与RIP创建动态路由项过程的网络。

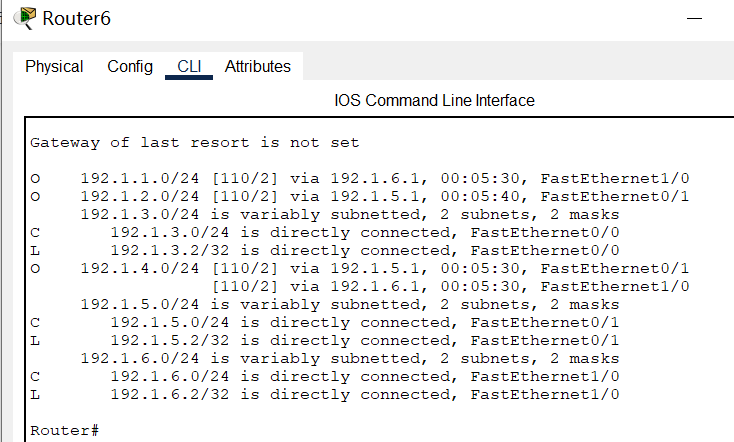
完成上述配置过程后,每一台路由器建立了完整路由表。各个路由器的完整路由表如下：







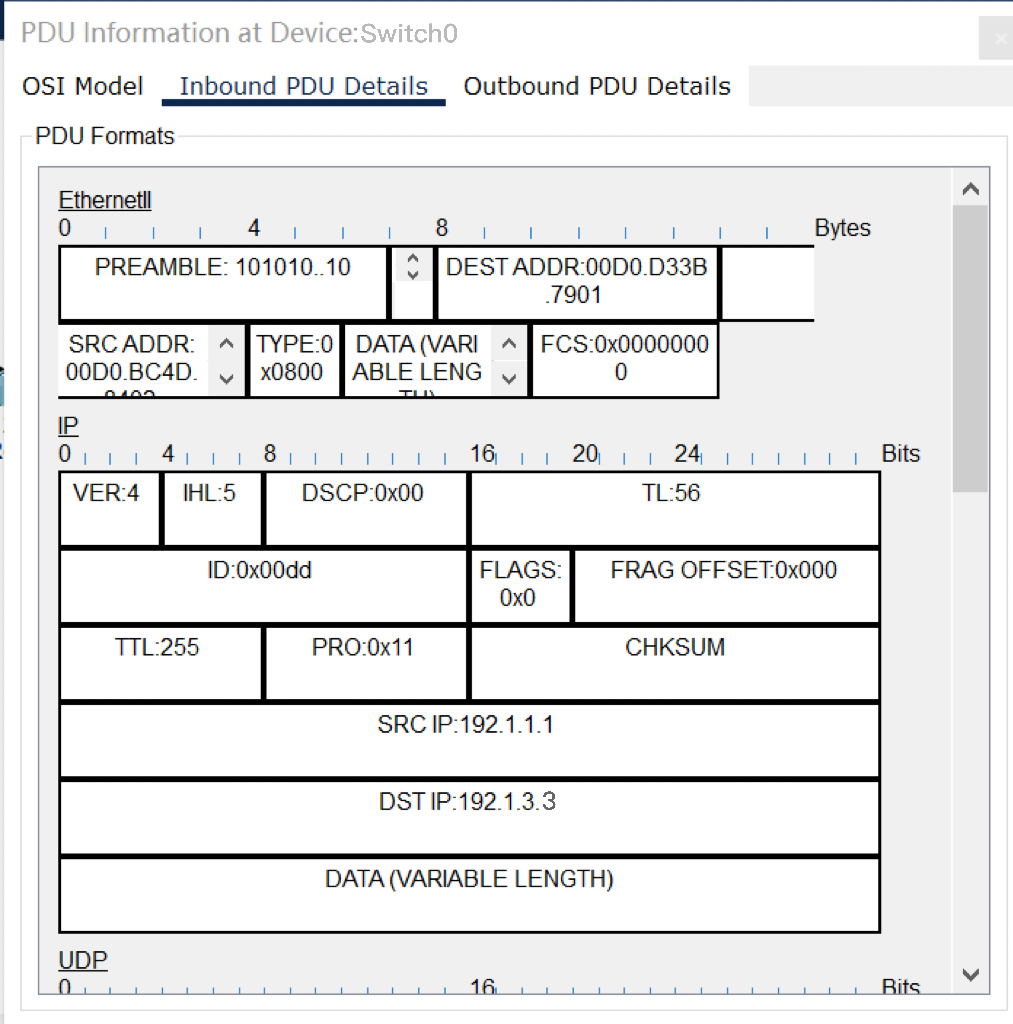


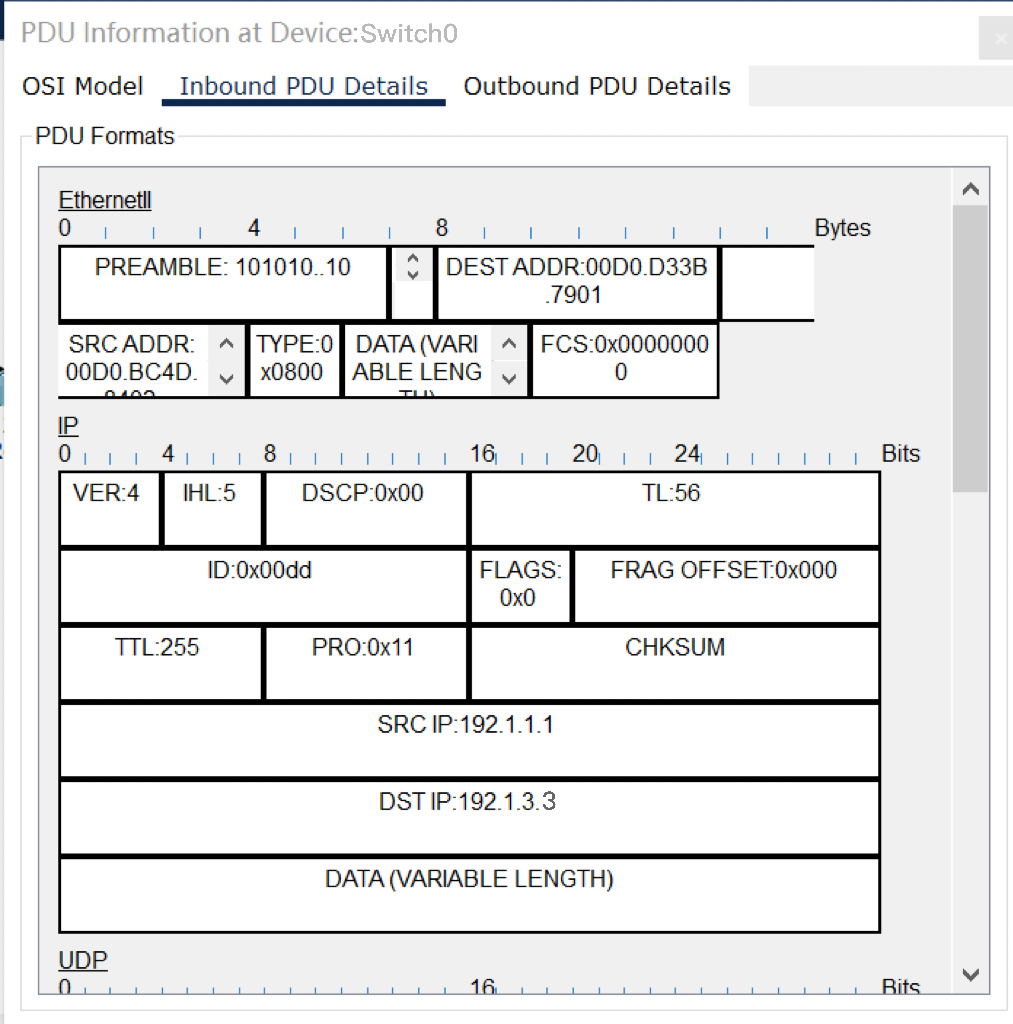


三、实验结果及分析

切换到模拟操作模式,启动PC0至Sever2的ICMP文传输过程,内部子中ICMP报文封装过程如图所示,ICMP报文封装成以PC0的私有IP地址192.168.1.1为源IP地址、以 Server2的私有IP地址192,168.3.3为目的IP地址的IP分组,公共网塔中ICMP报文封装过程如图7.10所示,以0的私有IP地址192.168.1.1为源IP地址、以 Server2的私有IP地址8.3.3为日的IP地址的1P分组封装成RE格式,并以GRE格式为净荷,封装成以R连接公共网络的接口的IP地址192.1.1.1为源IP地址,以 Router3连接公共格的接口的IP地址192.1.3.1为日的IP地址的IP分组,为了区分,将以PC0的私有IP地址192.168.1.1为源IP地址,以Server2的私有IP地址192.168.3.3为目的IP地址的IP分组称为内层IP分组,将以Routerl连接公共网落的接口的IP地址192.1.1.1为源IP地址,以 Router3连接公共网络的接口的IP地址192.1.3.1为日的IP地址的IP分组称为外层IP分组,内部网络内传输内层IP分组,公共网内传输外层IP分组。

内层ip分组格式如图：





IOS路由器IP Sec VPN实验

1. 实验目的

1) ISAKMP策略配置过程

(2)掌握 IP Sec参数配置过程

(3)验证 IP See安全关联建立过程

(4)验证封装安全净荷( Encapsulating Security Payload,ESP)报文的封装过程

(5)验证族于 IP Sec VPN的数据传输过程

1. 实验步骤(含程序清单)

(1)在第7.1节中的点对点IP隧道实验基磁上进行本实验

(2)在CLI(命令行接口)配置方式下,道两端完成安全策略配置过程,指定建立安

全传输通道使用的加密算法3DES、报文摘要算法MD5、共享密钥鉴别机制和DH组号DH2.道每一端可以配置多个安全策略,但两端必須存在匹配的安全策略,否则会终止 IP Sec安全关联建立过程。

（3)由于双方采用共享密钥鉴别方式,離道两端需要在CLI(命令行接口)配置方式下完成共享密钥配置过程, Packet Tracer只能用单个共享密钥第定所有采用共享密钥鉴别机制的隧道两端。

（4)在CLI(命令行接口)配置方式下,隧道两端完成变换集配置过程。隧道两端通过指定变换集确定 IP See安全关联使用的安全协议及各种相关算法。

(5)在CLI(命令行接口)配置方式下,通过配置分组过器指定隧道两端需要进行

安全传输的IP分组范围。

(6)在CLI(命令行接口)配置方式下,隧道两端完成加密映射配置过程。加密映射

中将 IP Sec安全关联另一端的IP地址,为 IP See配置的变换集及用于控制需要安全传输的IP分组范围的分组过器挪定在一起,如果某个端口作为多条隧道的源端口,则需要创建多个名字相同但序号不同的加密映射,每一个加密映射对应不同的隧道。

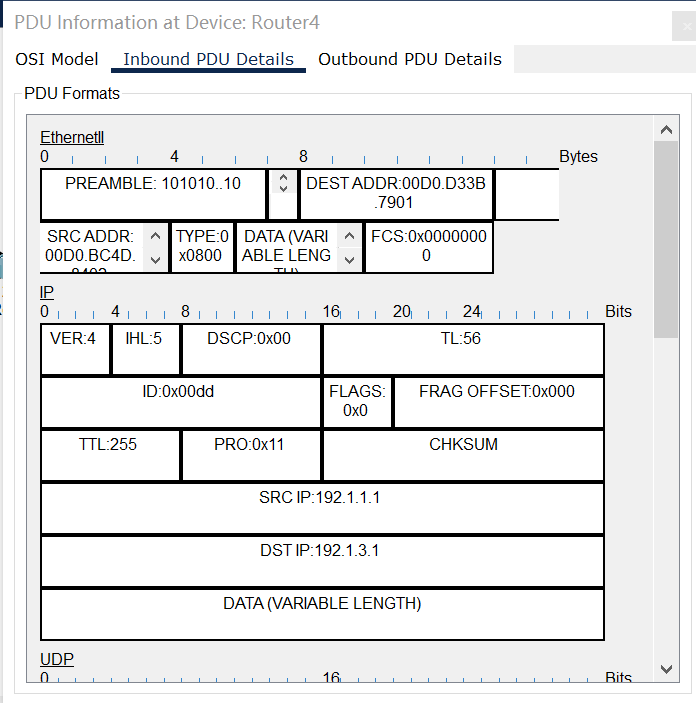
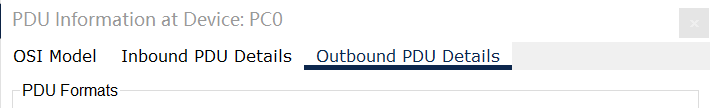
(7)在CL(命令行接口)配置方式下,完成将创建的加密映射作用到某个接口的过

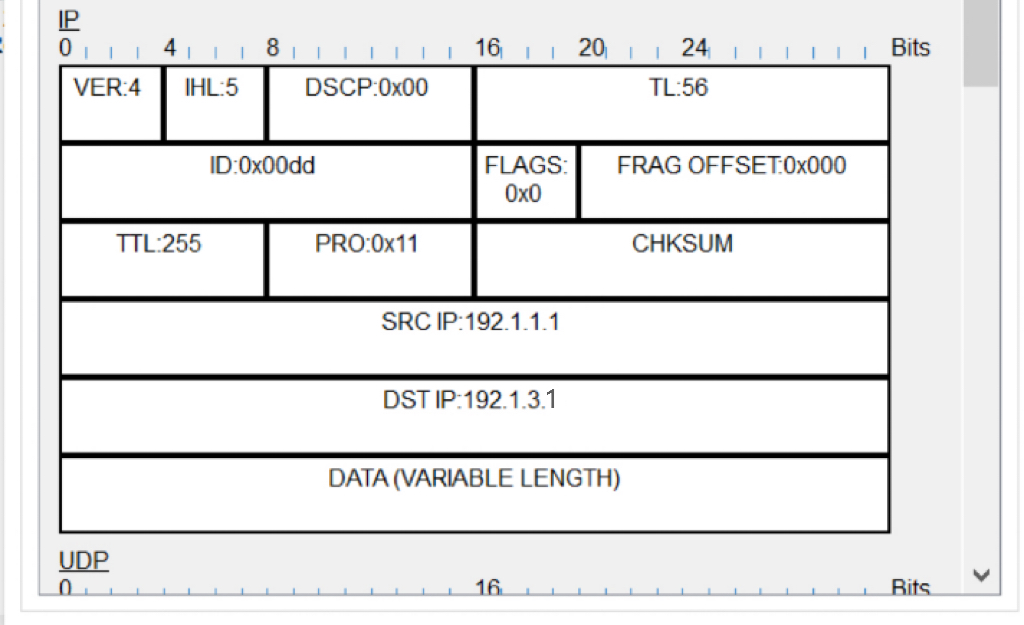
程,加密映射一且作用到某个接口上,则按照加密映射的配置,自动建立 IP See安全关联,并通过 IP Sec安全关联安全传输分组过器指定的IP分组分集。

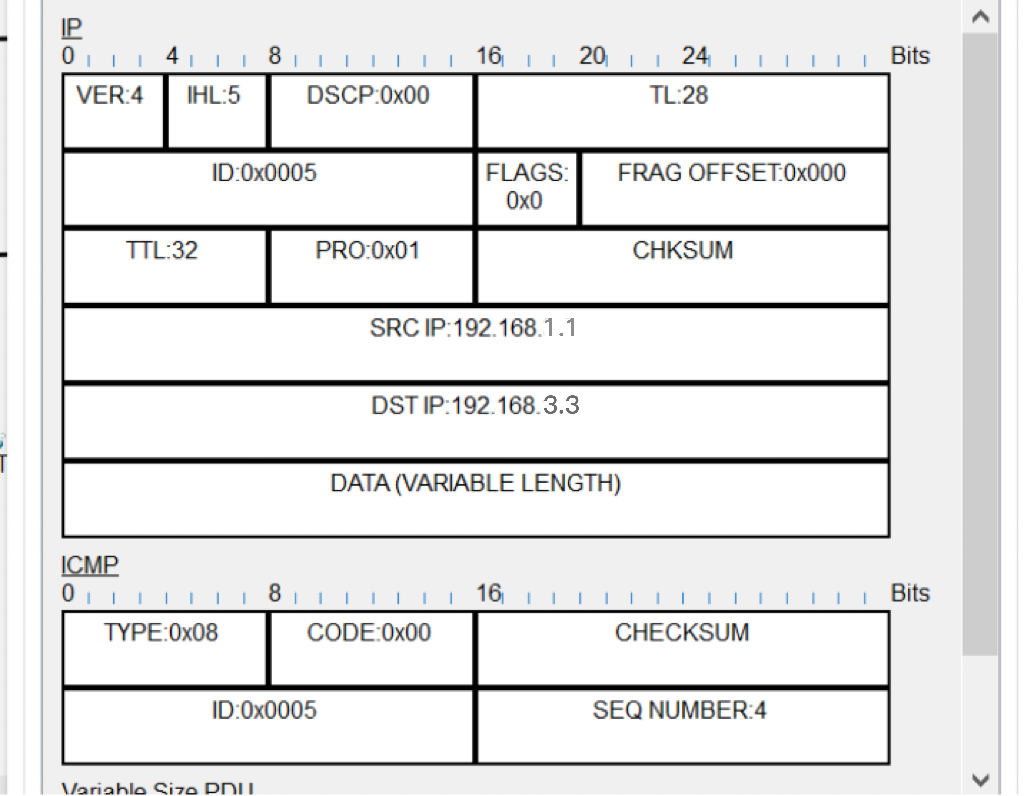
三、实验结果及分析

在道两端的接口各自创建加密映射后,離道两端通过 ISAKMP自动创建IP

Sec安全关联,内层IP分组经过陸道传输时,封装成外层IP分组,外层IP分组经过安全关联传输时,封装成ESP报文。图7.11所示是图7.2中PCO至 Server2的内层IP分组以内部网络本地IP地址192.168.1.1和192.168.3.3为源和目的IP地址,图7.12所示是该内层IP分组封装成外层IP分组的过程,它首先被封装成GRE格式,GRE格式被封装成外层IP分组。图7.13所示是外层IP分组封装成ESP报文的过程,外层IP分组作为ESP报文的净荷,ESP采用的加密算法是3DES,采用的HMAC算法是HMAC-MD5。







内层ip分组封装成外层ip分组。