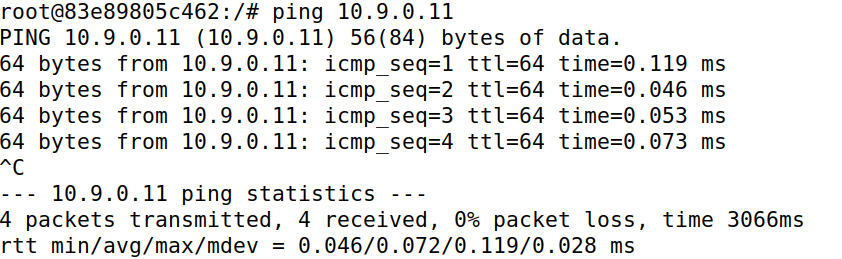
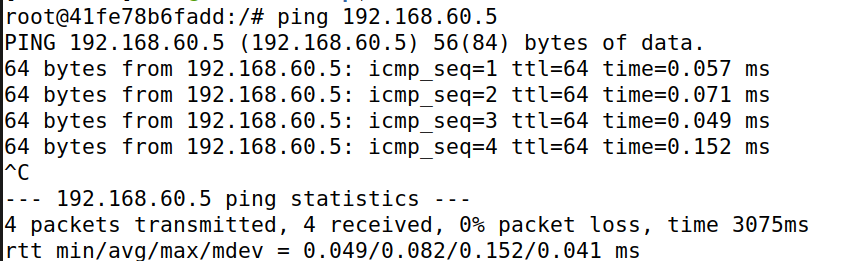
**VPN Lab: The Container Version**

学号：57118223 姓名：齐天一

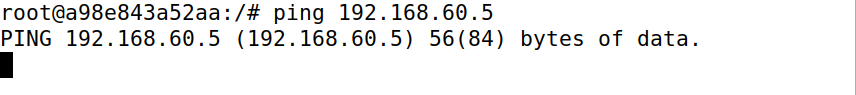
**Task1：**

（1）在主机V ping 路由

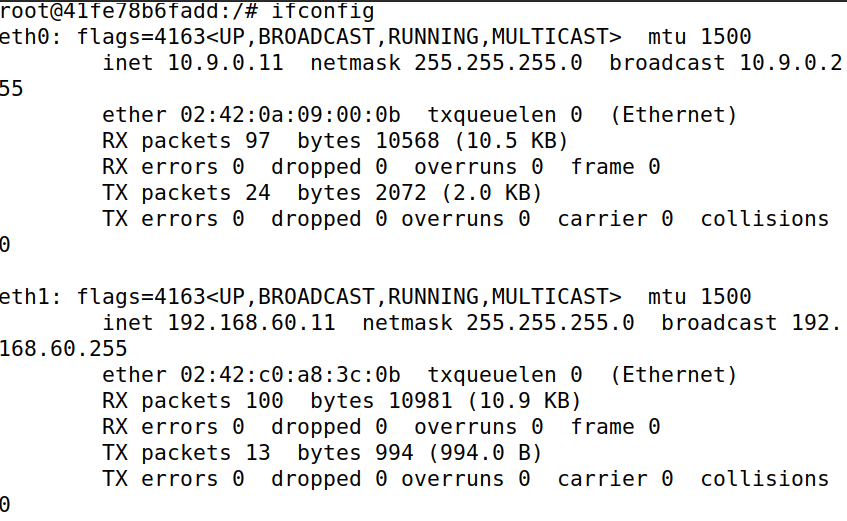
（2）在路由上ping主机V



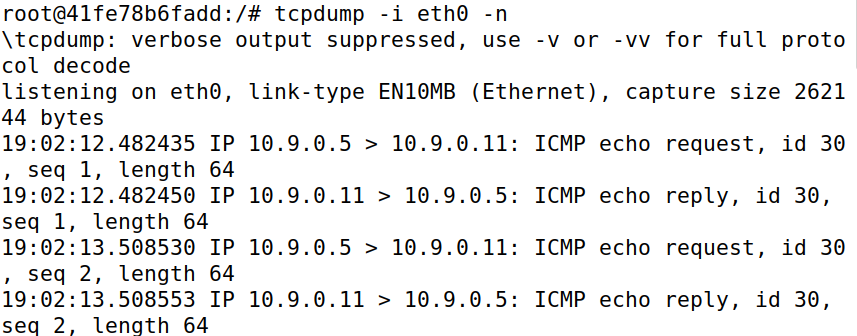
1. 主机U ping主机V



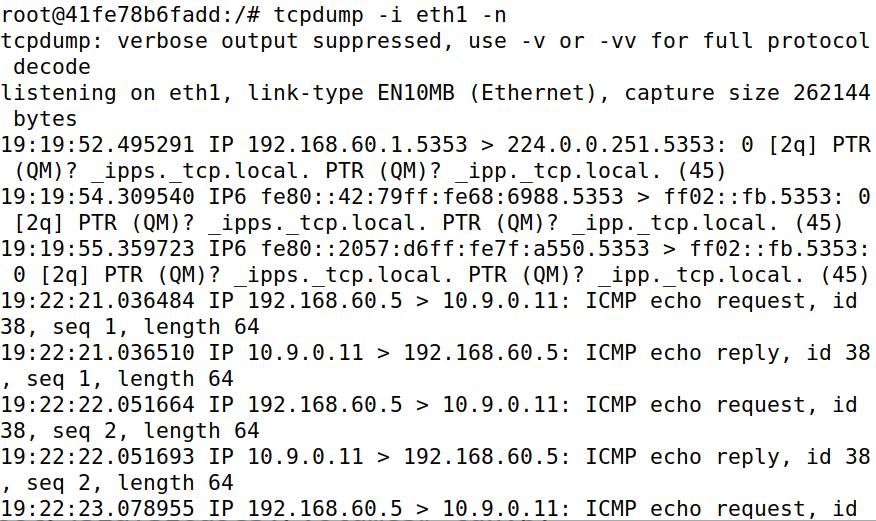
1. 在路由上查看端口对应的ip地址



1. 在路由器的eth0端口开启tcpdump监听，同时在主机U ping 路由器



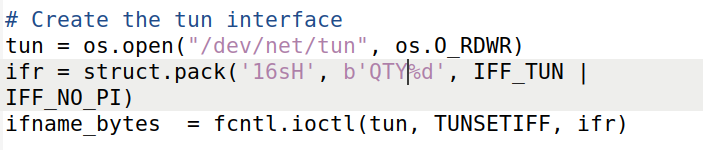
1. 在路由器测eth1端口



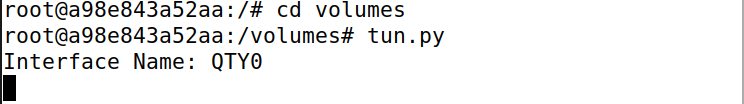
**Task2：**

**Task2.a**

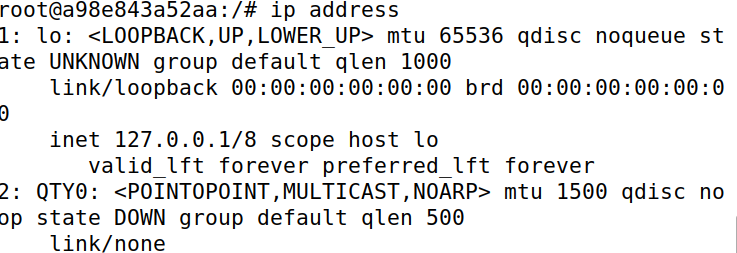
1. 修改程序，自行定义端口号



（2）在主机U上运行程序



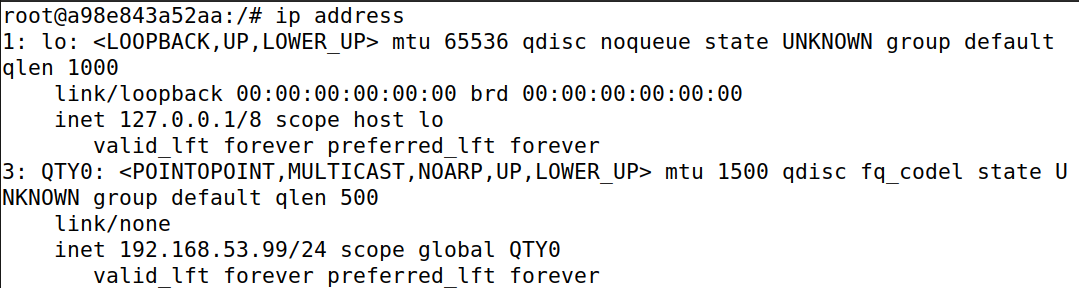
（3）使用ip address查看，可以看到修改成功



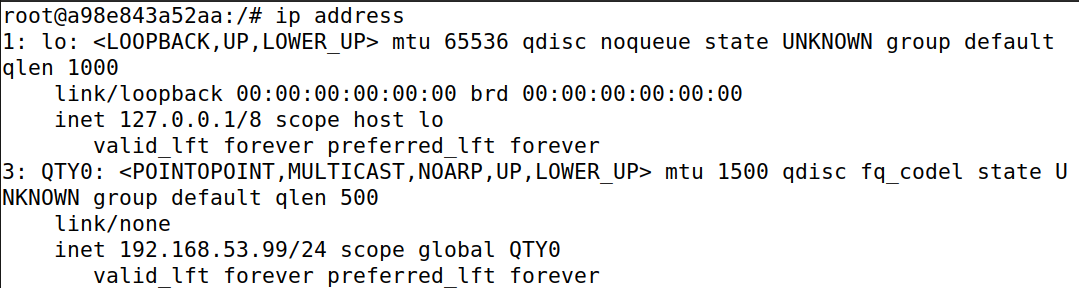
**Task2.b**

1. 在while循环前增加两条语句用于分配ip，并重新运行程序

IMG_256

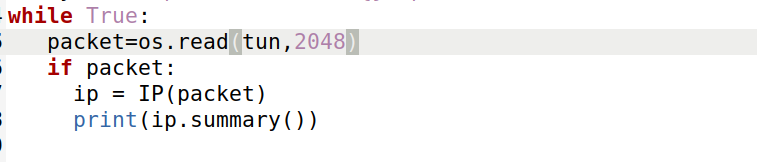


（2）在主机U输入ip address 查看

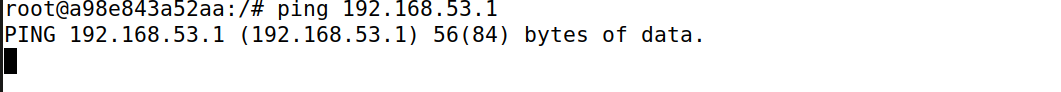


**Task2.c**

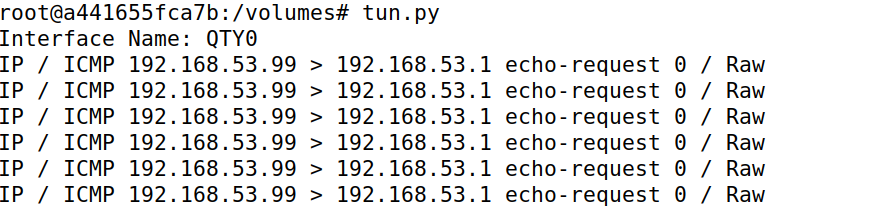
1. 修改while循环如下



（2）重新运行程序并ping192.168.53.1

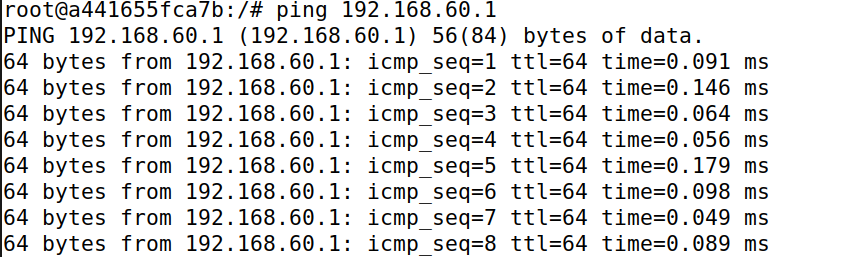


可以看到ping不通，查看QTY0端口

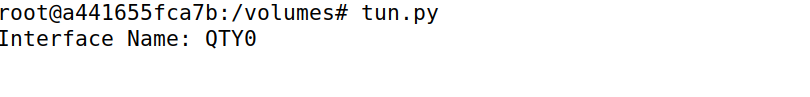


这说明icmp请求都是从QTY0端口发出，且都被QTY0端口捕获了。

（3）尝试ping 192.168.60.1



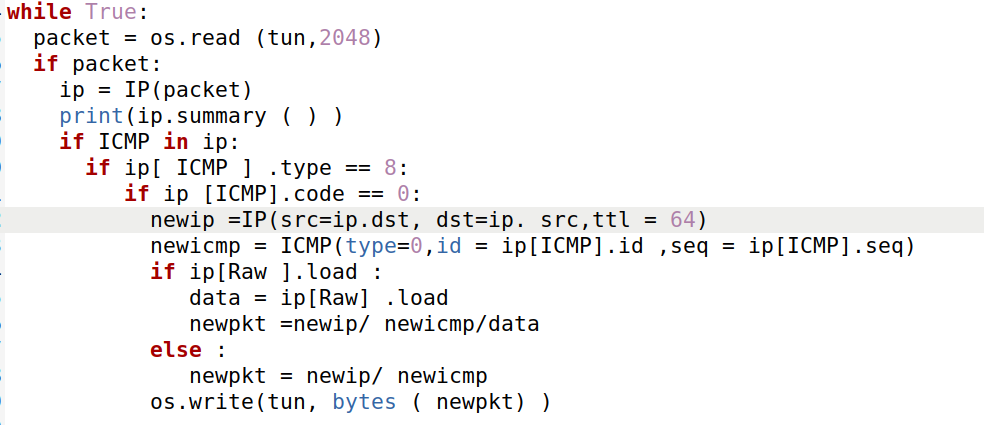
查看QTY0端口



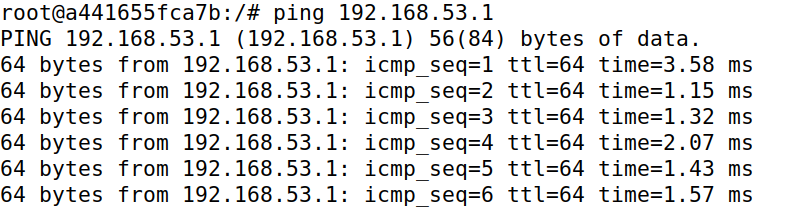
造成这种现象的原因是发给192.168.60.1的报文不经过QTY0端口，所以不会被捕获。

**Task2.d:**

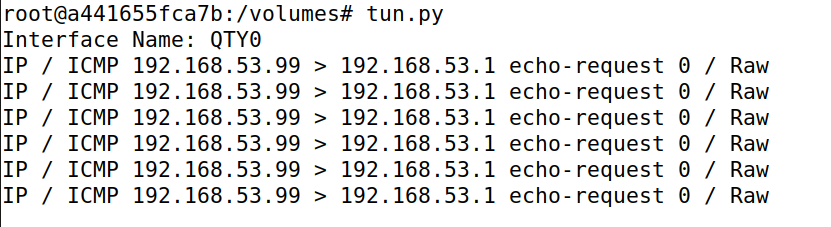
1. 修改程序如下



1. 运行程序，并重新ping 192.168.53.1,发现可以ping通

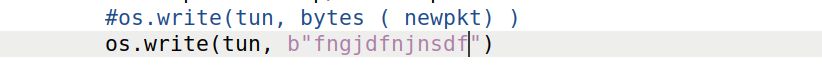


查看QTY0端口

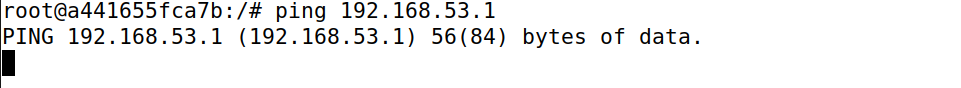


可以看到发送的报文被成功地伪造成了request报文，说明程序正确。

（3）修改写入语句，改成写入任意语句

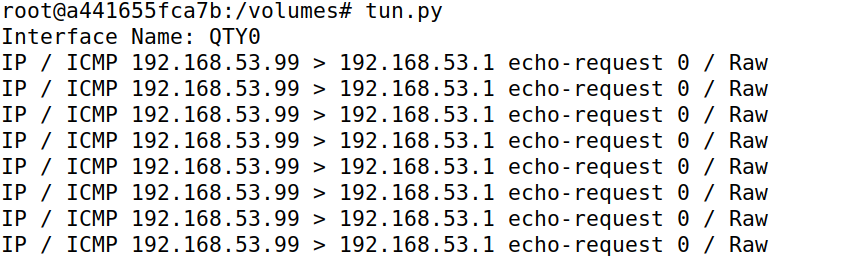


1. 重新运行程序并ping 192.168.53.1



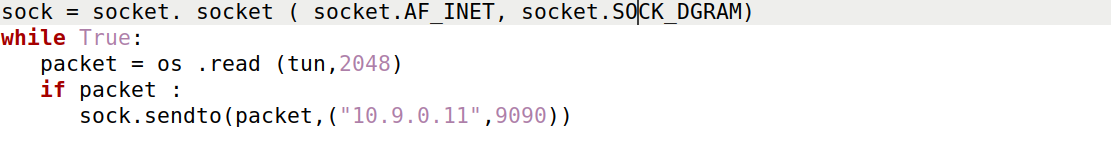
可以发现此时ping不通了。

查看QTY0端口：

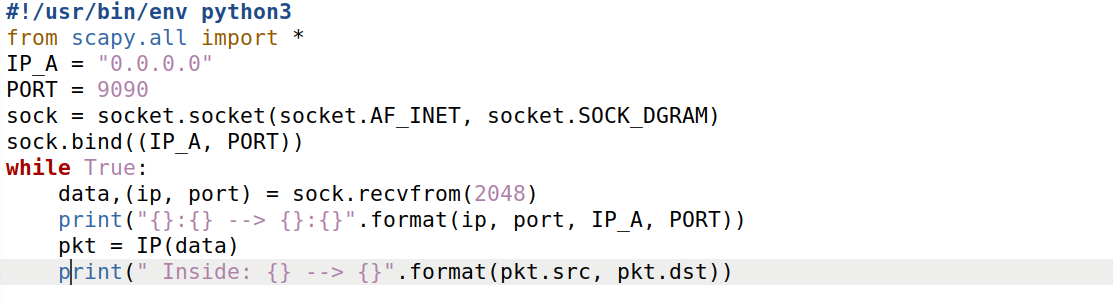


可以看到，报文被成功发送并接受，但没有进行处理。猜测是由于不符合报文的格式，所以被丢弃了。

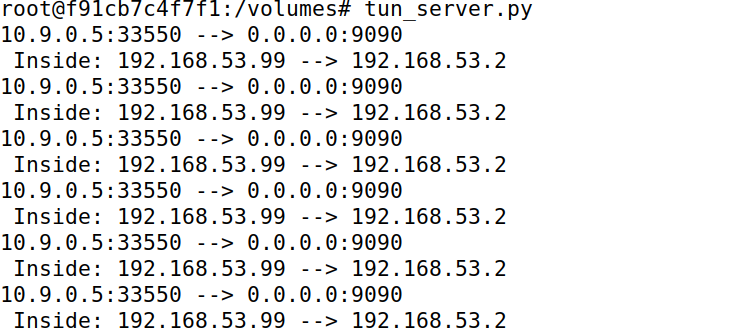
**Task3**  
（1）编写客户端程序如下（修改task3代码的while部分）：



编写服务器端程序如下：



1. 在服务器路由上运行服务器程序，在主机U上运行客户端程序
2. 在主机U上ping 192.168.53.0/24网段，并在服务器端查看：



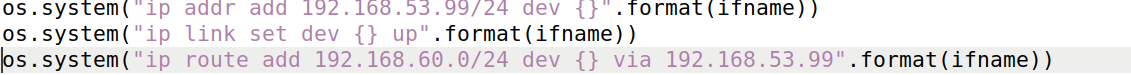
可以看到服务器成功捕获了报文，说明程序转发正确。

（4）在主机U上ping主机V

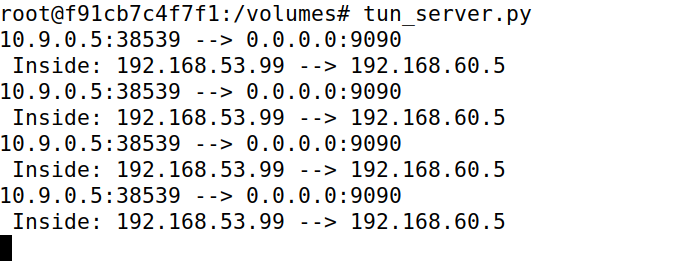
Q_V97JJKTK$UWH6083_4SCY

可以看到ping不通,这是因为路由器中没有 响应的路由

（5）修改客户端代码，增添如下代码用于自行增添路由



（6）重新运行程序，并在主机Uping主机V，并查看服务器端的效果：



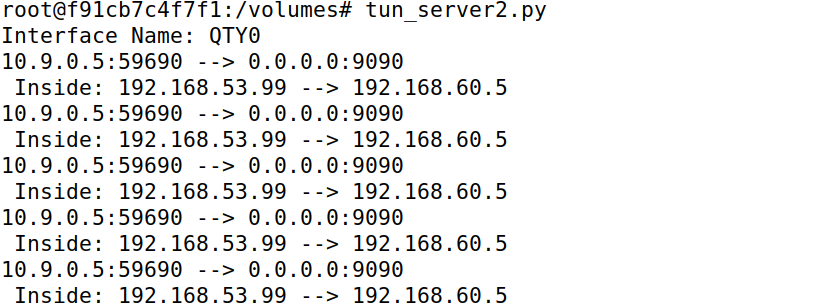
可以看到成功捕获了报文，说明成功地通过隧道传输了报文。

**Task4**

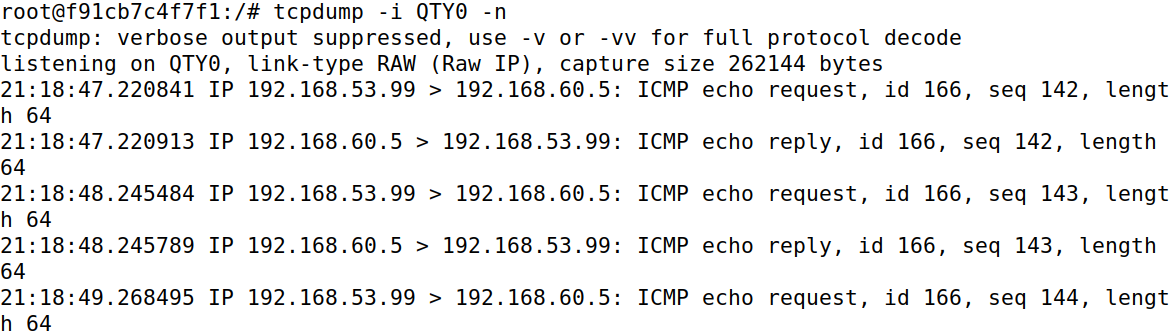
1. 仿照task2中tun程序编写新的服务端程序



（2）重新执行task3中的步骤，并查看服务器端的效果

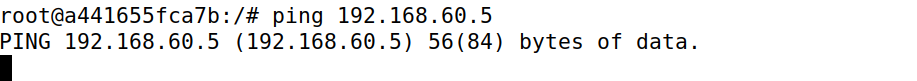


（3）在服务器端使用tcpdump监听端口



可以看到icmp请求成功到达了主机V、

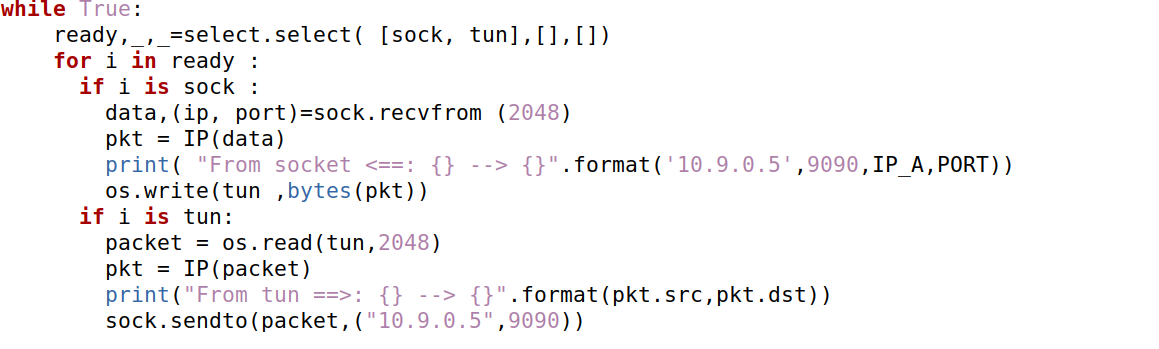
1. 查看主机U端



可以看到，没有收到响应报文，说明此时隧道只是单向的，不能由主机V发送到主机U。

**Task5**

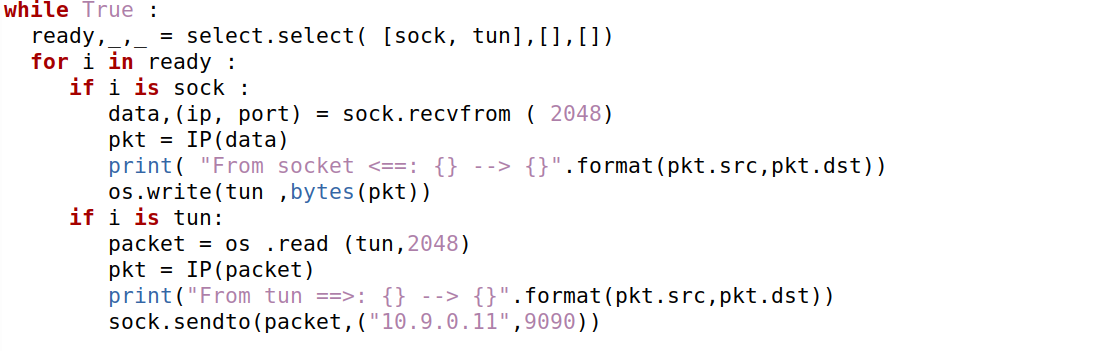
1. 修改服务端代码，其中关键部分如下



当报文是来自socket端口，说明是隧道的流量，将其转发给9090；

当报文是来自tun端口，说明是从主机U发来的报文，将其转发给主机V

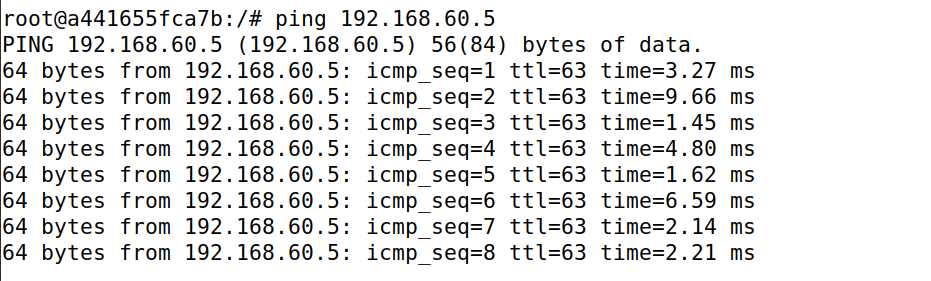
1. 修改客户端代码，其中关键部分如下



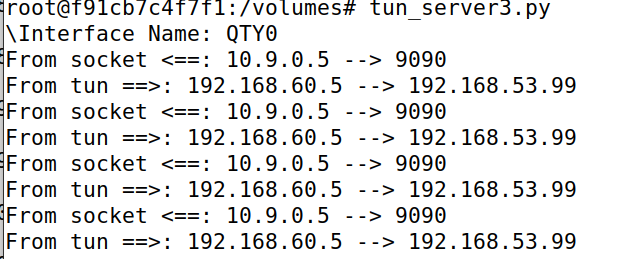
如果报文来自socket端口，说明是主机U发送的，将其转发给隧道；

如果报文来自tun端口，说明是来自隧道（主机V发送的），将其转发给主机U。

1. 重复Task3中的操作，在主机V上ping主机U

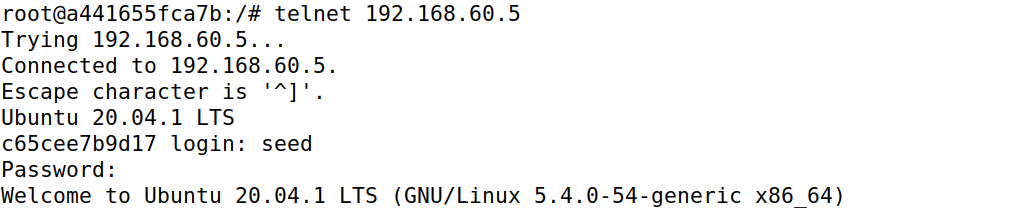
  
可以看到，此时已经能够ping通，说明能够收到响应报文。

1. 查看服务器端的情况



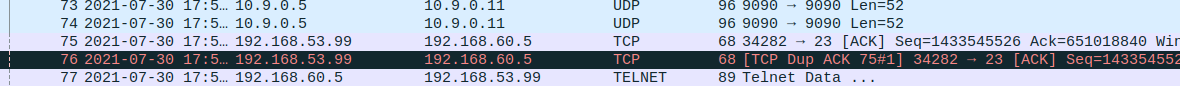
可以看到双方交互的报文在服务器上通过的情况，说明实现了成功实现了隧道的双向功能。

（5）在主机U上发起对主机V的telnet请求

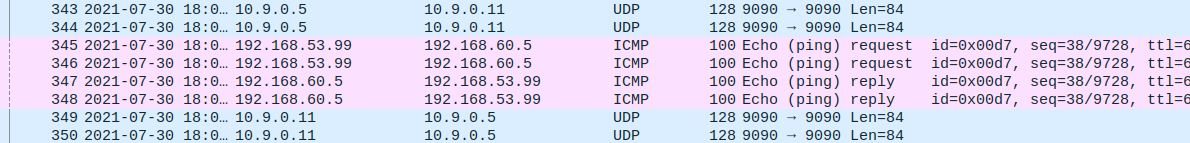


可以看到telnet成功。

（6）主机U在telnet后输入数据，并使用wireshark观察

可以看到报文会先通过隧道到达服务器，再通过服务器发送到主机V

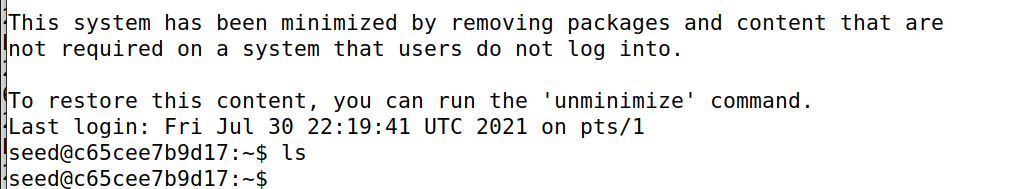
1. 在主机U上ping主机V，并使用wireshark观察



可以看到同样，报文会通过隧道到达服务器，由服务器通过正常方式发送icmp报文给主机V，同时主机V发送icmp响应报文给服务器，最后再由隧道传回到主机U。

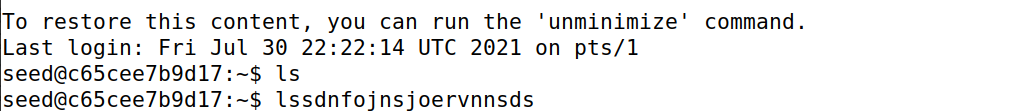
**Task6**

（1）主机U上进行telnet，同时中断服务器程序



会发现中断后无法输入任何字符了

1. 重启服务器程序

此时可以重新输入字符了，同时之前中断时输入的字符也出现了。

造成这种现象的原因是：

中断服务器程序使得通道功能失效，因此双方无法进行通讯，在发送方发出的报文会驻留在缓冲区，一旦通道在短时间内恢复，缓冲区中的内容将会重新发送出去，从而被显示出来。