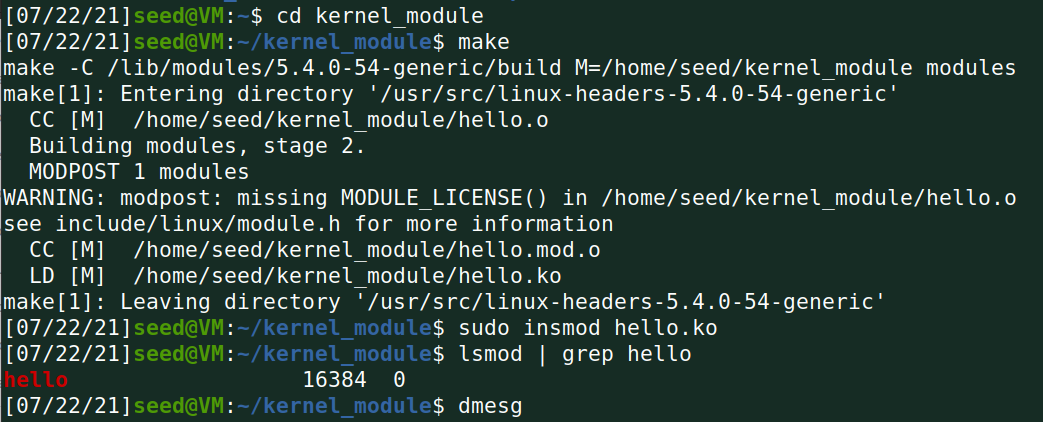
**Firewall Exploration Lab**

**57118215程文泽**

**Task 1: Implementing a Simple Firewall**

**Task 1.A: Implement a Simple Kernel Module**

使用make命令编译内核模块，随后安装内核模块，查看模块是否已载入内核，然后卸载模块，最后使用dmesg命令查看内核日志缓冲区，可以看到模块输出的信息。



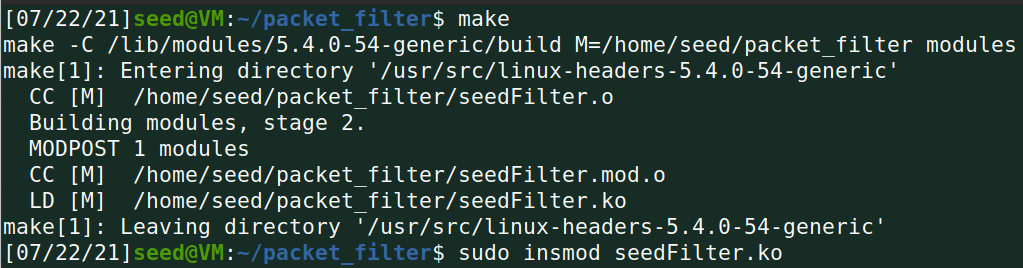


****

**Task 1.B: Implement a Simple Firewall Using Netfilter**

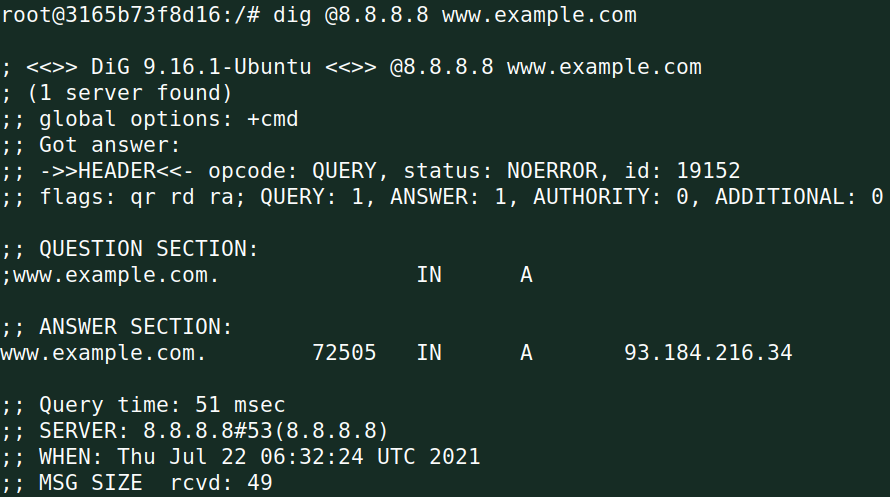
**1.**

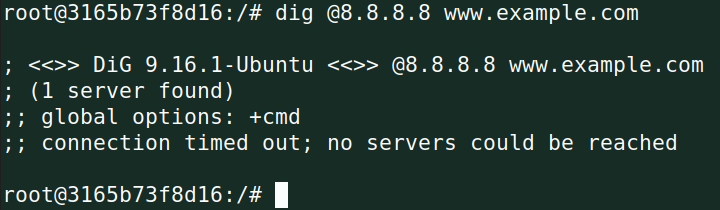
编译模块如下：



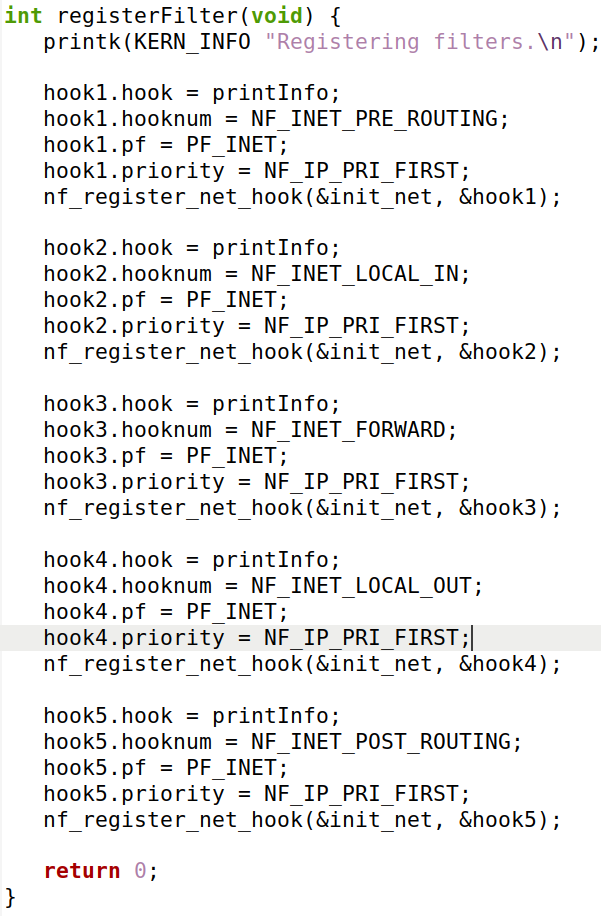


编译前后在主机10.9.0.5里运行dig命令，结果如下，可以看到编译后的防火墙正常工作，发出DNS请求被阻止

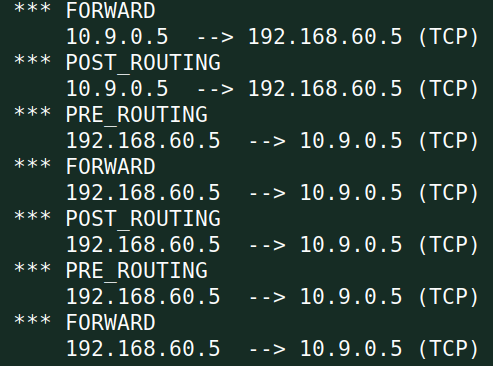
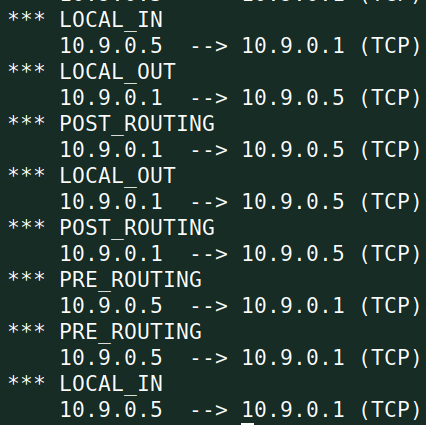




**2.**



首先在主机10.9.0.5里telnet自己网段中主机10.9.5.1，使用dmesg命令查看结果如下，无FORWARD。再telnet其他网段主机192.168.60.5，查看结果如下，出现了FORWARD,

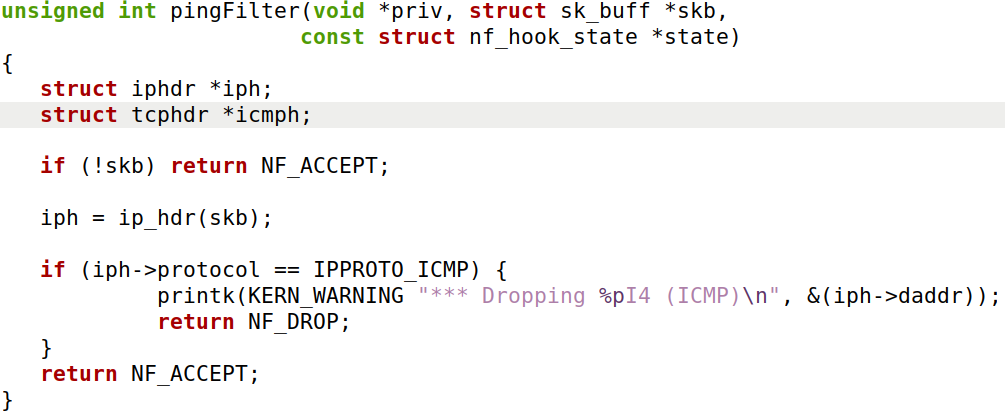


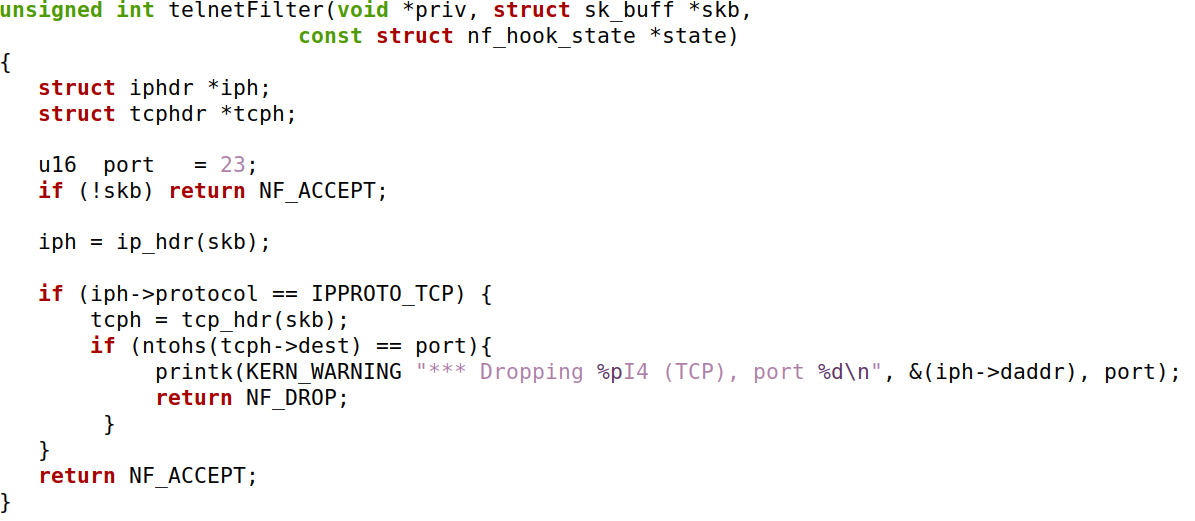
从以上结果可以看出，LOCAL\_IN和LOCAL\_OUT适用于本地主机接收和发送数据包时，POST\_ROUTING适用于本地数据包产生后发送给目的地PRE\_ROU

TING适用于来自目的地址数据包发给本地，FORWARD适用于路由器转发数据包。

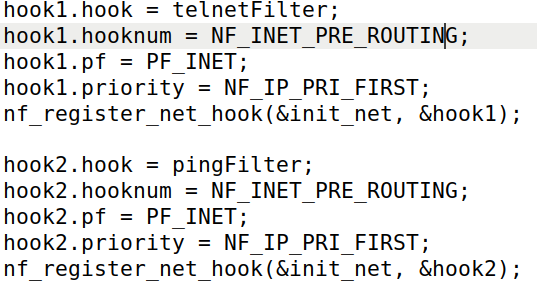
**3.**

两个hook函数代码如下：

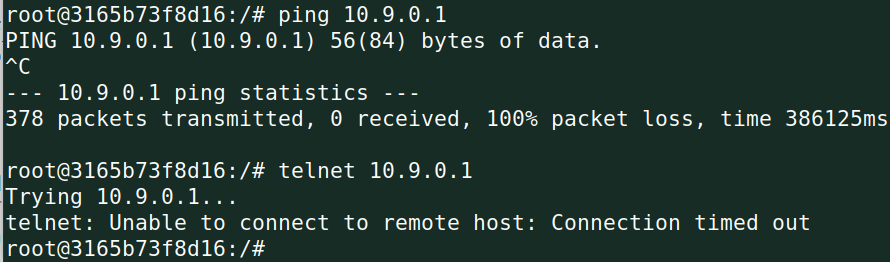




选择NF\_INET\_PRE\_ROUTING作为共同的钩子



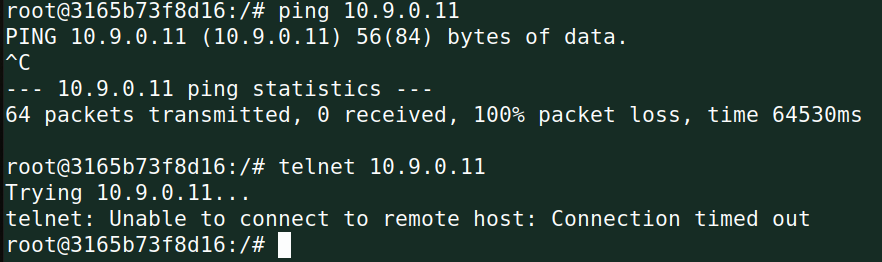
在主机10.9.0.5上，进行以下操作，结果如下：



**Task 2: Experimenting with Stateless Firewall Rules**

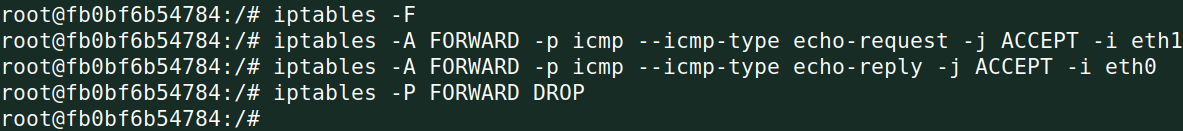
**Task 1.A: Implement a Simple Kernel Module**

如果按照实验手册的命令进行设置，在主机10.9.0.5里ping路由器和telnet路由器都无法成功，这是第一条规则是允许路由器接收ICMP回复报文，第二条规则是允许路由器发出ICMP请求报文，第三条规则是默认路由器不接收任何报文，第四条规则是默认路由器不输出任何报文，因为ping路由器，路由器接收到的是请求报文，输出的是回复报文，所以无法成功。

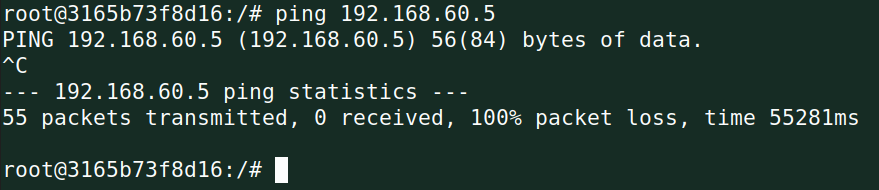


**Task 2.B: Protecting the Internal Network**

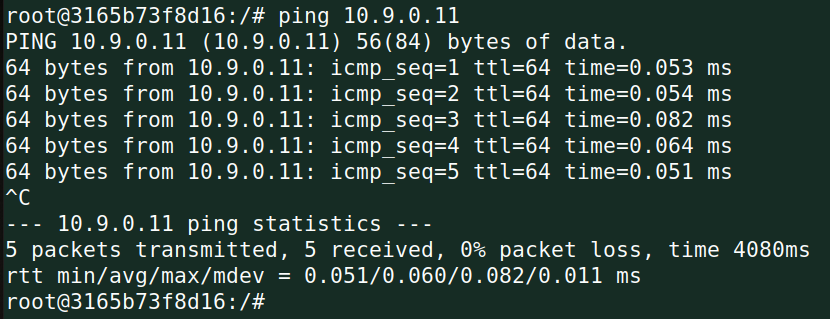
路由器里设置的规则如下：



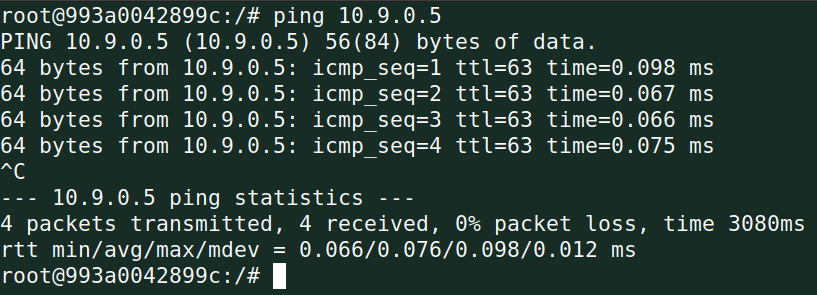
1. Outside hosts cannot ping internal hosts



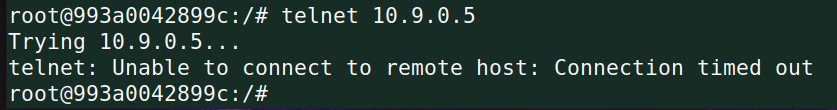
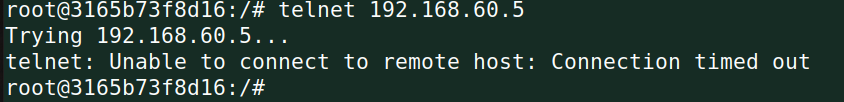
1. Outside hosts can ping the router



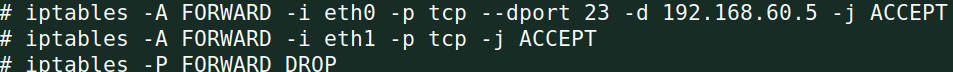
1. Internal hosts can ping outside hosts



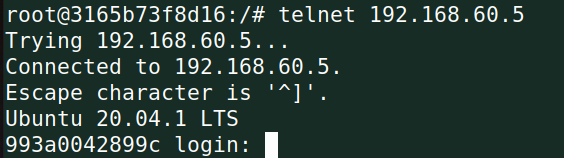
1. All other packets between the internal and external networks should be blocked.

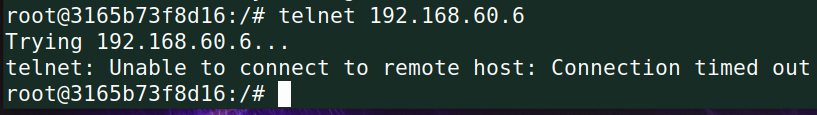


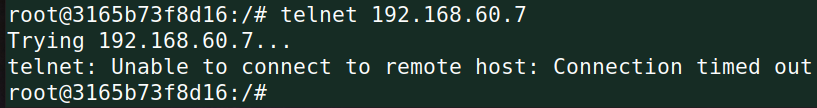
**Task 2.C: Protecting Internal Servers**



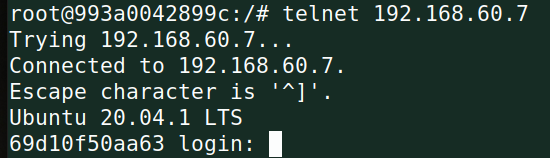
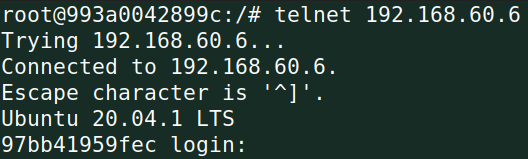
1. All the internal hosts run a telnet server (listening to port 23). Outside hosts can only access the telnet server on 192.168.60.5, not the other internal hosts.
2. Outside hosts cannot access other internal servers.



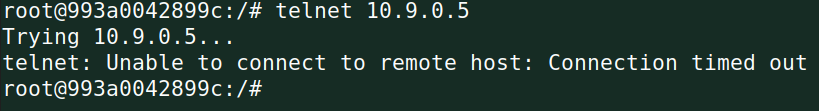


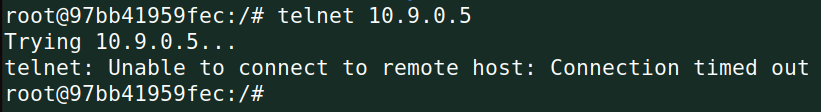


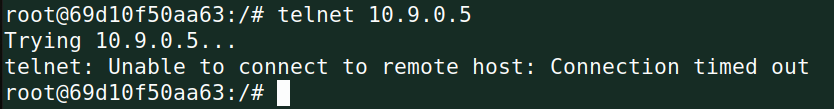
1. Internal hosts can access all the internal servers.



1. Internal hosts cannot access external servers.



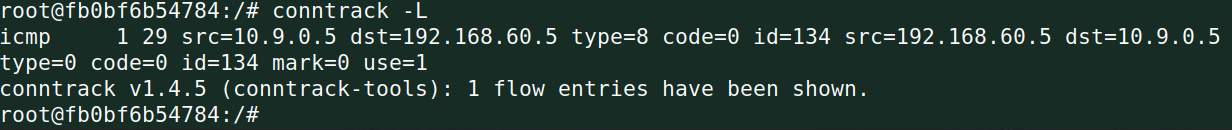




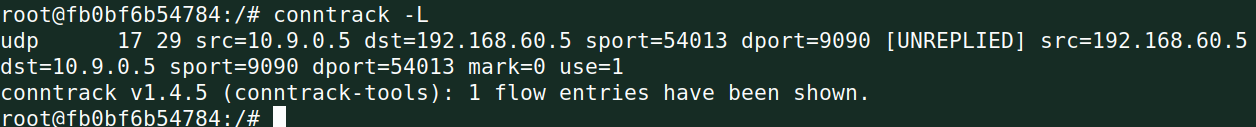
**Task 3: Connection Tracking and Stateful Firewall**

**Task 3.A: Experiment with the Connection Tracking**

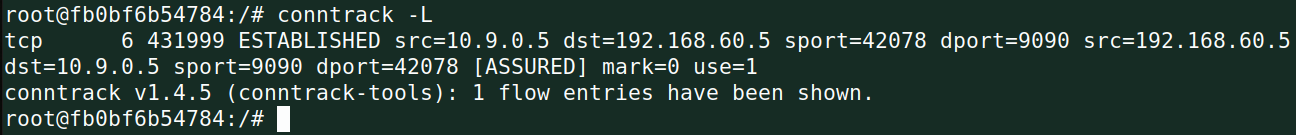
ICMP experiment：建立了一个ICMP连接，持续时间为29秒



UDP experiment：建立了一个UDP连接，持续时间为29秒

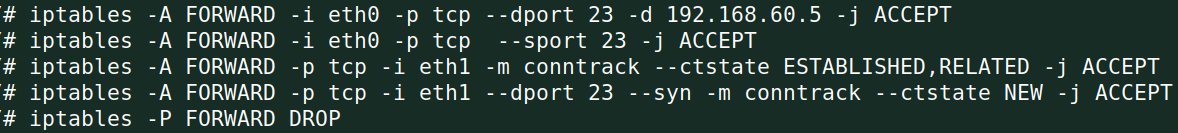


TCP experiment：建立了一个TCP连接，持续时间为431999秒



**Task 3.B: Setting Up a Stateful Firewall**

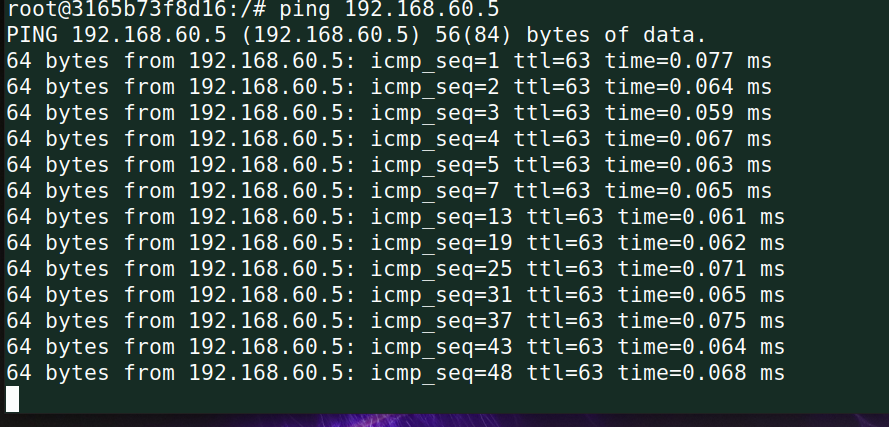
使用跟踪连接修改规则如下：



不使用跟踪连接规则相对于使用跟踪连接规则更少，但使用跟踪连接更加安全。

**Task 4: Limiting Network Traffic**

运行实验册上两条命令后，在主机10.9.0.5里ping主机192.168.60.5，可以看到，在连续接收到了多个回复后，需要等一会儿时间才能接收到下一个回复报文，

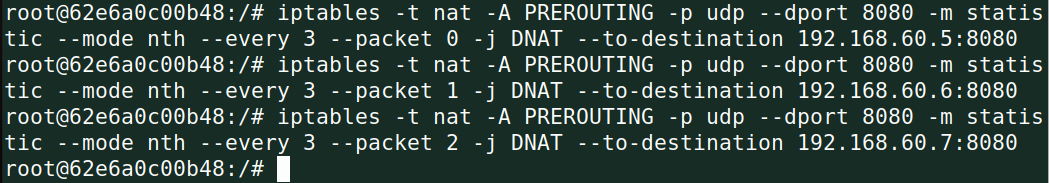


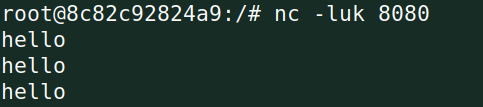
如没有第二条规则，就会连续收到回复报文，因此可以看到如果没有第二条规则，第一条的规则的限制就无法体现出来。

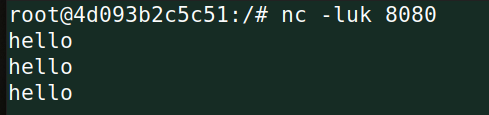
**Task 5: Load Balancing**

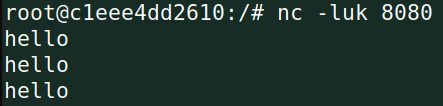
**Using the nth mode (round-robin)**

规则添加如下，在主机10.9.0.5里运行命令，在192.168.60.0网段中各个主机得到如下结果，这些规则的意思就是发至路由器的每3个udp报文中，其中一个修改目的地址为192.168.60.5，发给主机192.168.60.5，其中一个修改目的地址为192.168.60.6，发给主机192.168.60.6，最后一个修改目的地址为192.168.60.7，发给主机192.168.60.7。









**Using the random mode**

规则添加如下，在主机10.9.0.5里运行命令，在192.168.60.0网段中各个主机得到如下结果，这些规则的意思就是发至路由器的udp报文中，其中0.33333的概率修改目的地址为192.168.60.5，发给主机192.168.60.5，0.33333的概率修改目的地址为192.168.60.6，发给主机192.168.60.6，0.33333的概率修改目的地址为192.168.60.7，发给主机192.168.60.7。

