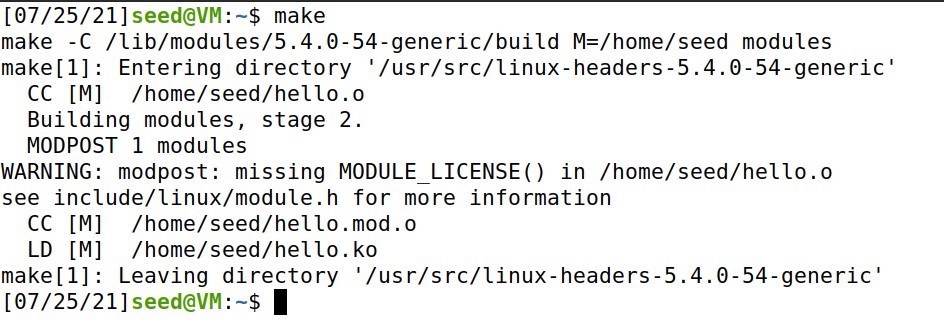
**Firewall Exploration Lab**

# **Task1**

# Task1.A

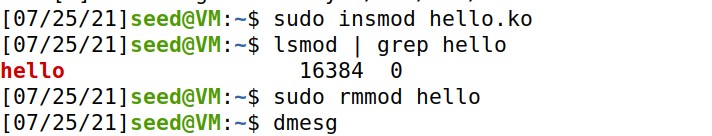
根据实验所给代码进行 make。



make 后得到的全部文件如下。



用 insmod 命令载入模块，用 lsmod 命令查看，用 rmmod 命令将其从内核中卸载，用 dmesg 命令查看日志。



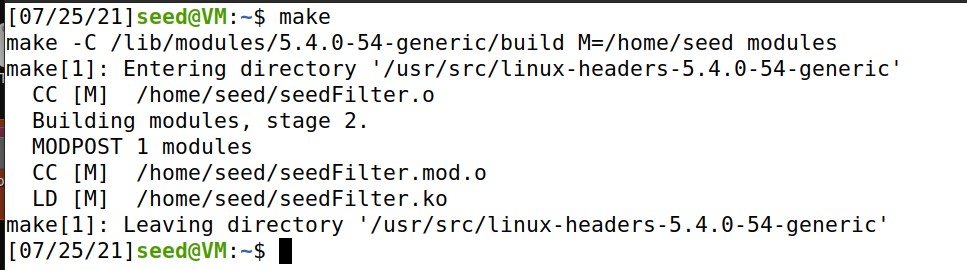
成功出现了期望的结果。

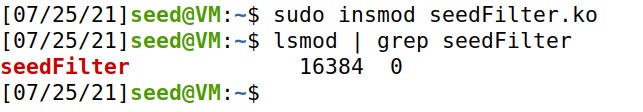


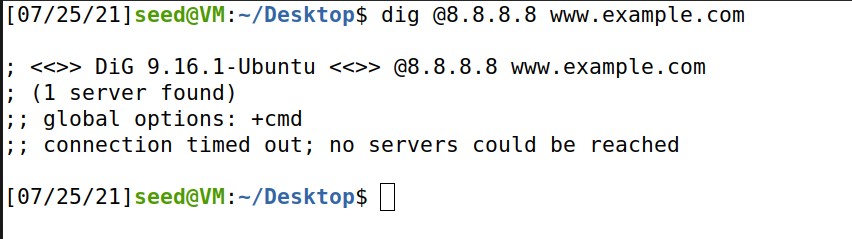
Task1.B

Task1.B.1

用所给代码进行 make。

 用 insmod 命令载入模块，用 lsmod 命令查看。

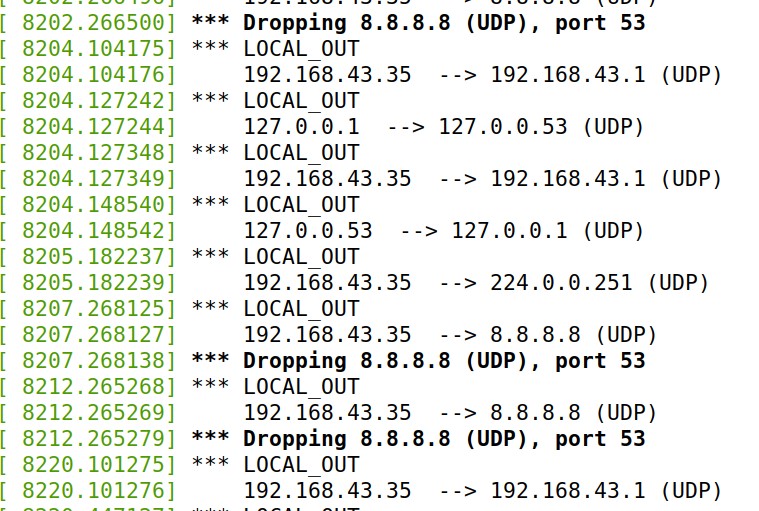
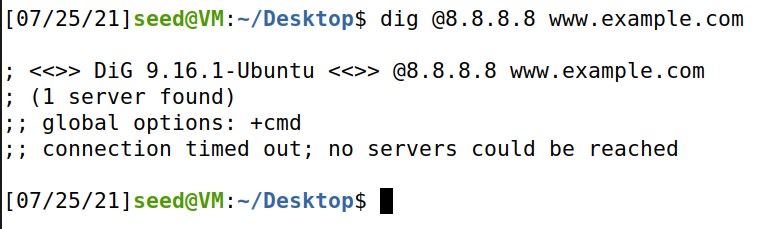
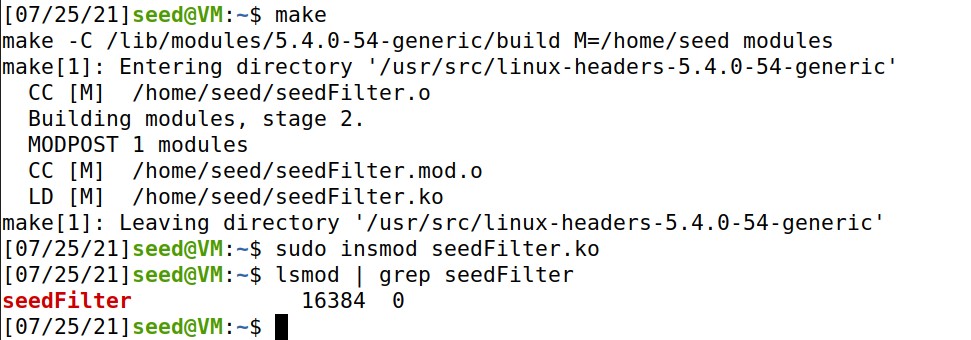
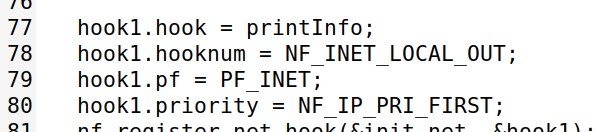
 发送请求，发现请求被阻塞，达到预期结果。



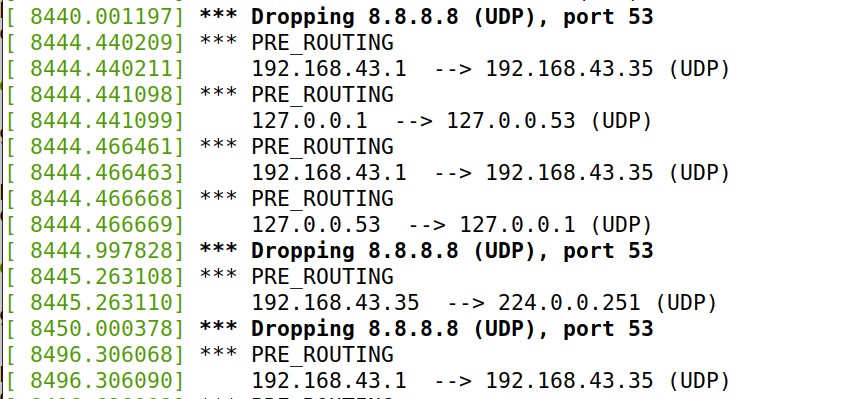
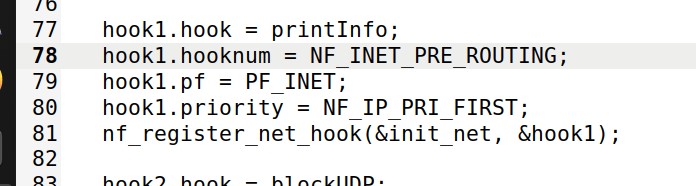
Task1.B.2

# 将 printfo 挂在不同 hook 上，先修改第 78 行处代码，然后重新 make 并加载内核，再发送请求，最后看日志，结果如下。

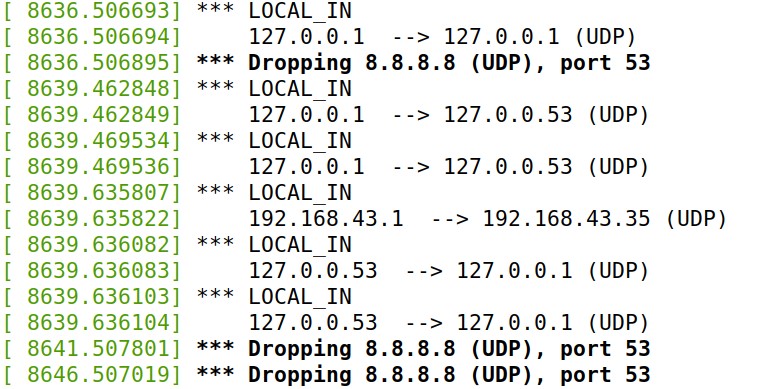
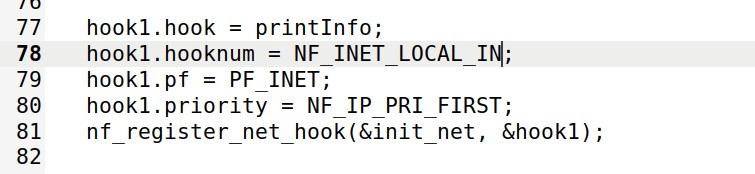
NF\_INET\_LOCAL\_OUT：在数据包以其方式离开主机之前调用。



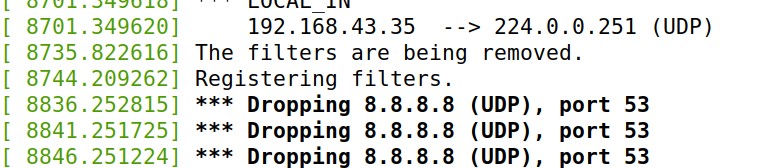
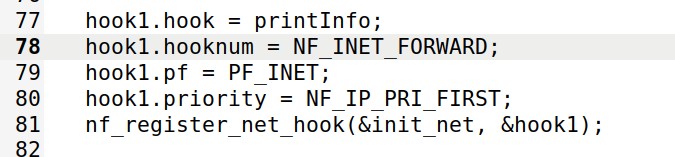
NF\_INET\_PRE\_ROUTING:在做出任何路由决策之前调用。



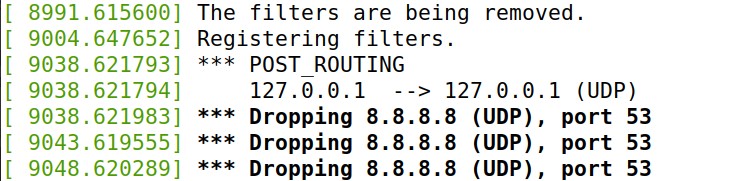
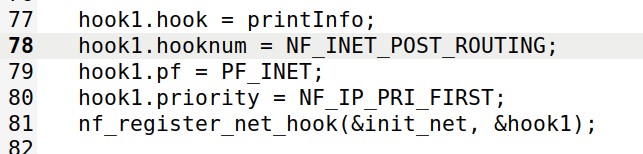
NF\_INET\_LOCAL\_IN:在发送到网络堆栈之前调用。



NF\_INET\_FORWARD:向其他主机转发报文时调用。

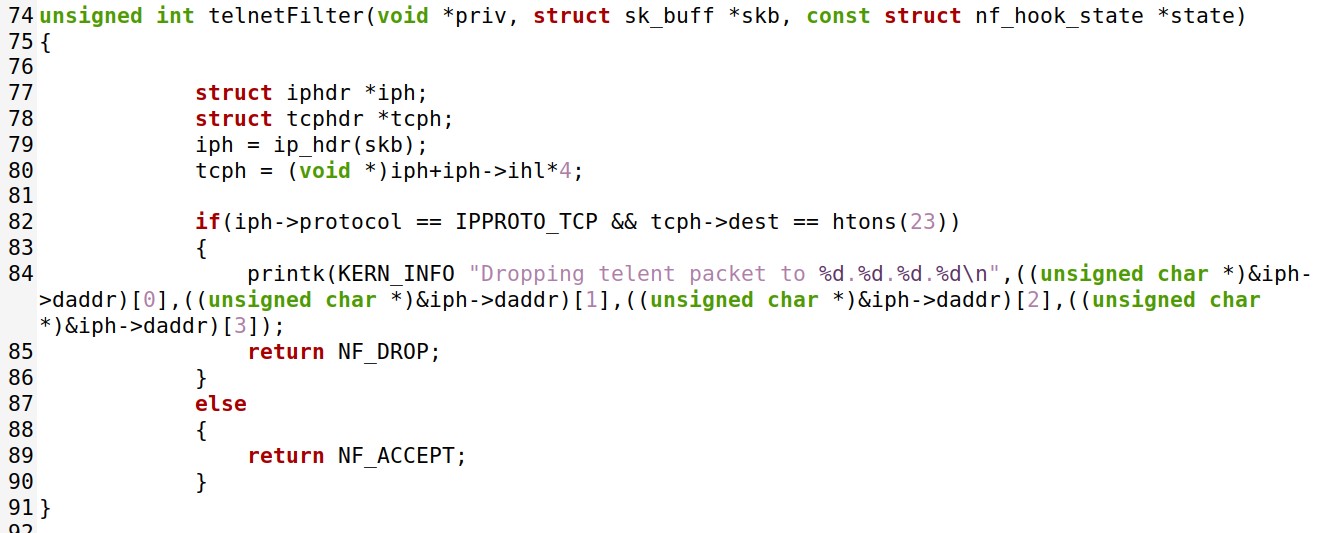


NF\_IP\_POST\_ROUTING:数据包离开主机并进入不同的网络之后调用。



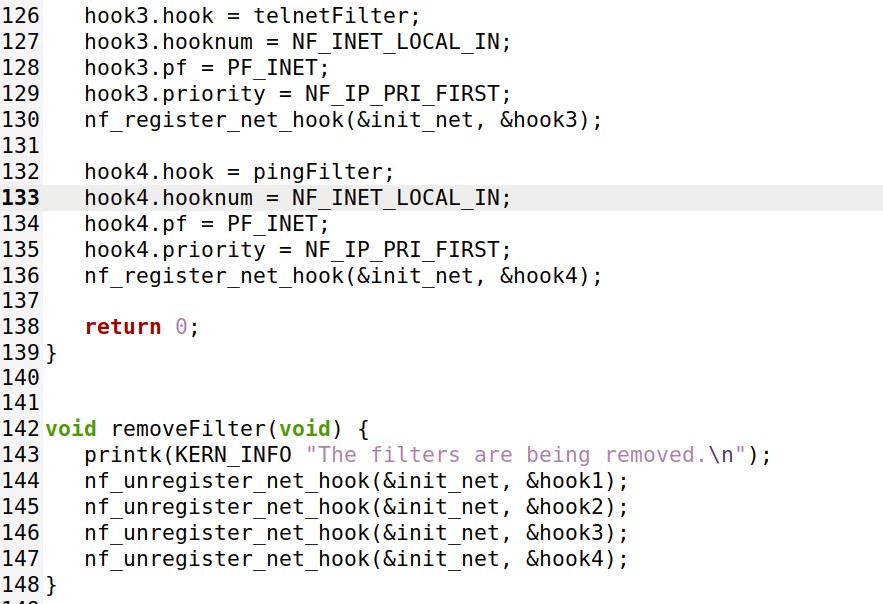
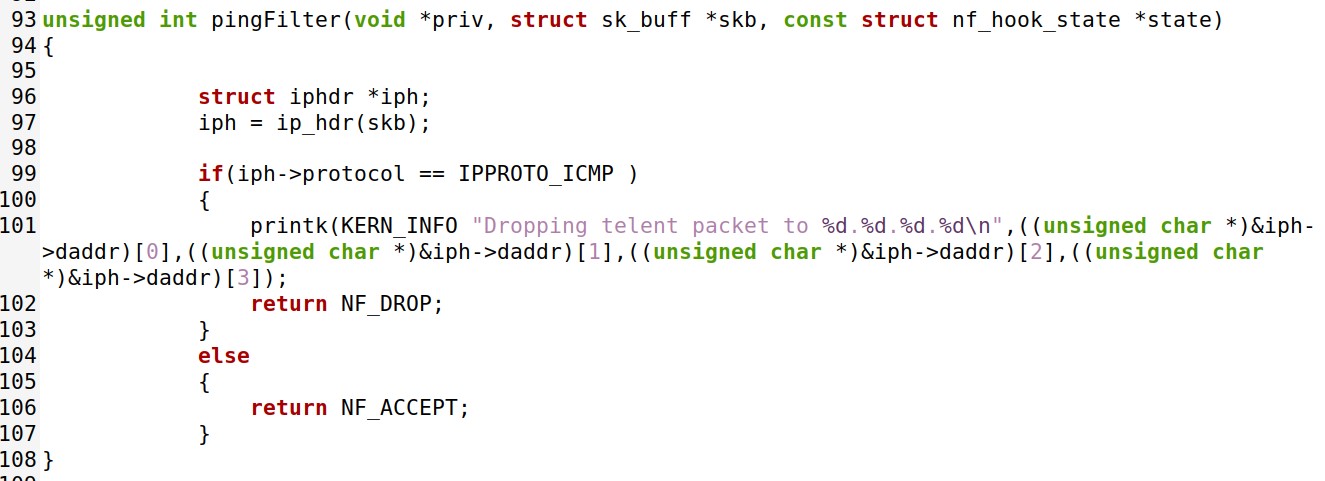
Task1.B.3

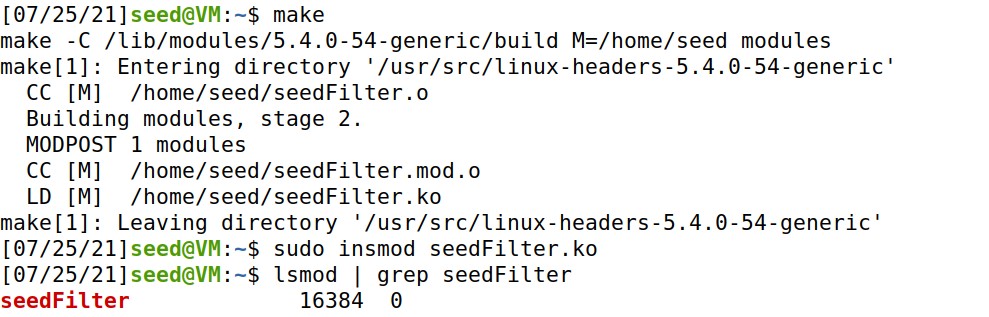
下面代码是实现防止其他计算机 telnet 到 VM 的 hook。

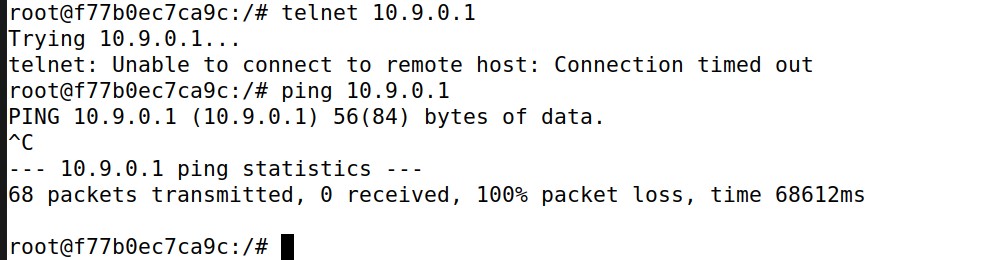


下面代码是实现防止其他计算机 ping 到 VM 的 hook。

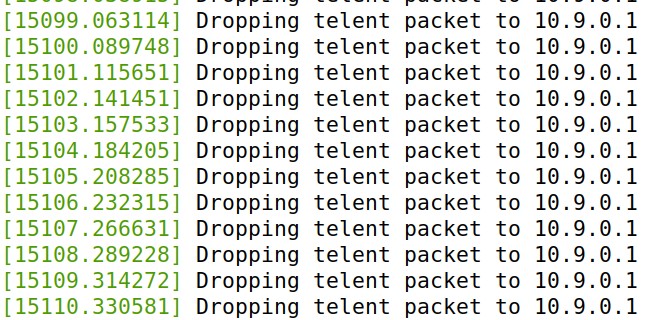
编译并加载内核。



 此时 telnet 和 ping 均未成功。



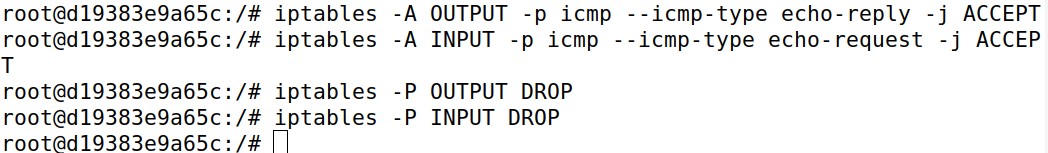
查看日志发现 telnet 包都被 drop 掉了。

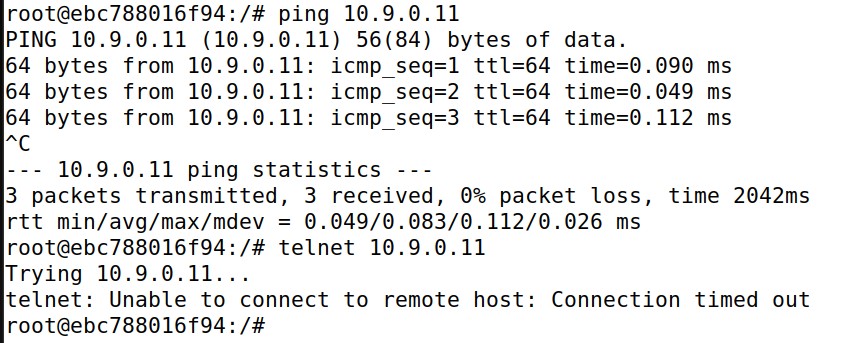


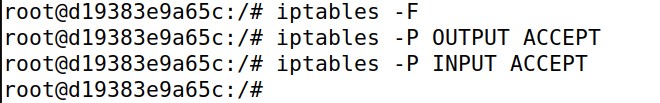
**Task2**

Task2.A

在路由器里设置如下规则。

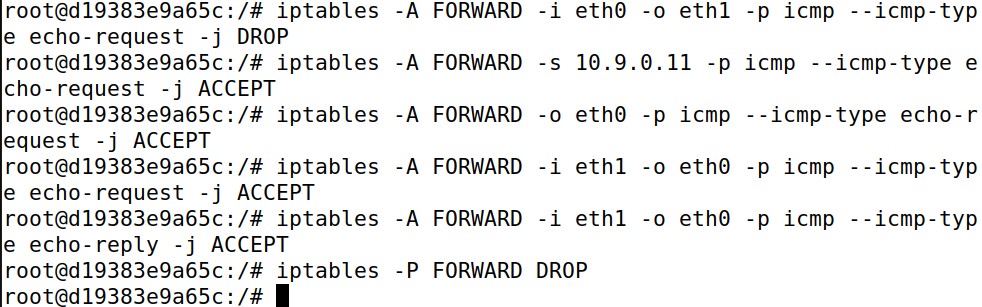


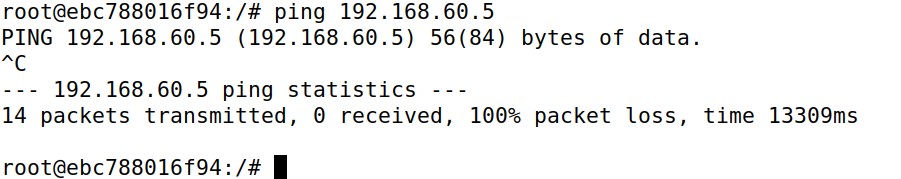
此时从 10.9.0.5 ping 路由器能通，但是 telnet 不行。  清除写入的规则。

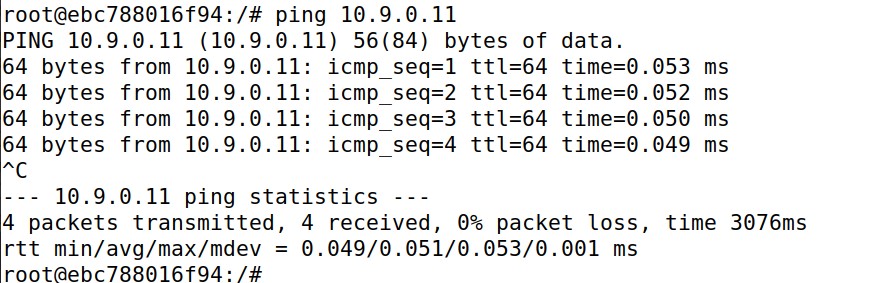


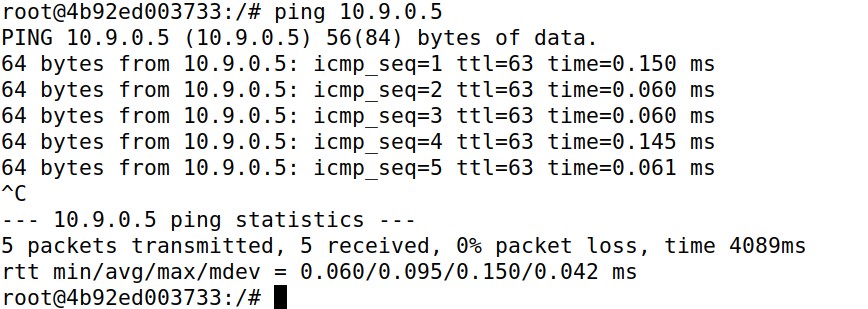
Task2.B

在路由器里设置如下规则。

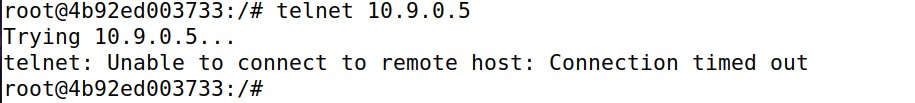
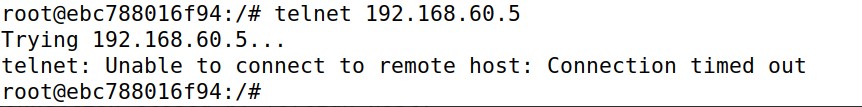
 此时，外部主机不能 ping 内网。

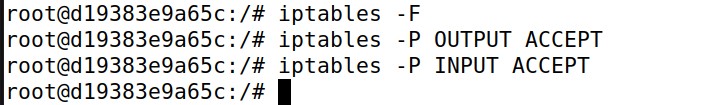
 外部主机可以 ping 路由器。

 内部主机可以 ping 外网。

 无论是内网 telnet 外网还是外网 telnet 内网都失败。

清除规则。

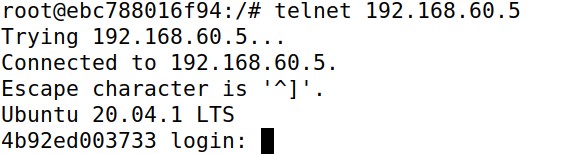


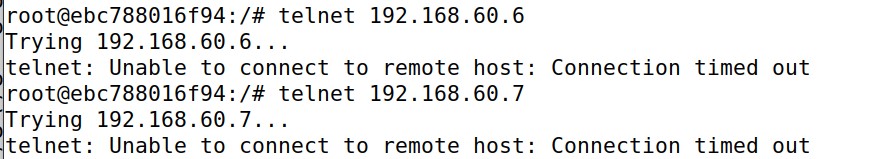


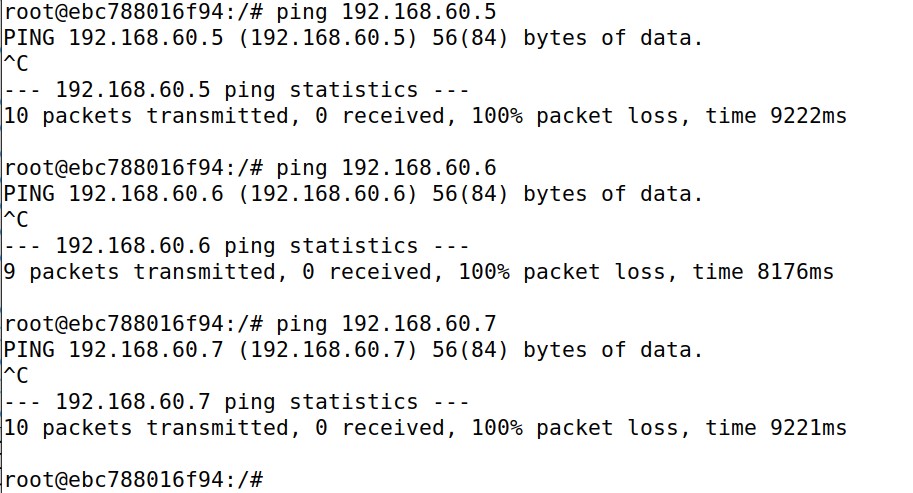
Task2.C

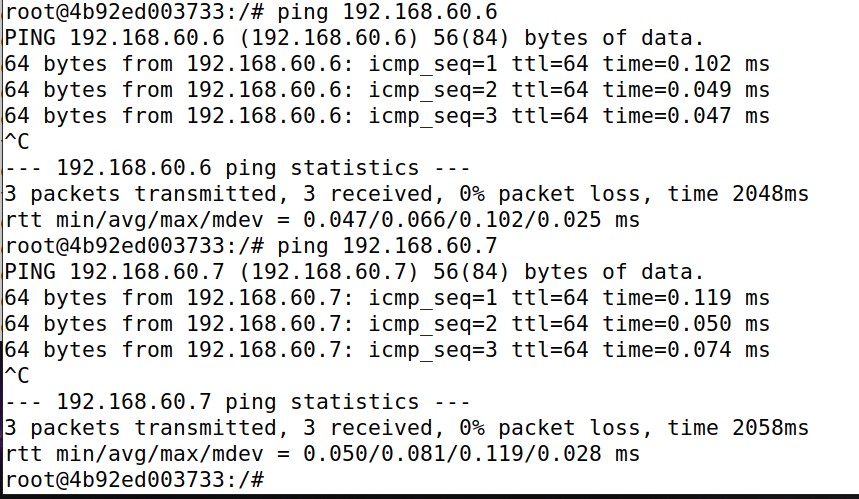
在路由器里设置如下规则。

 外网主机能 telnet 192.168.60.5。

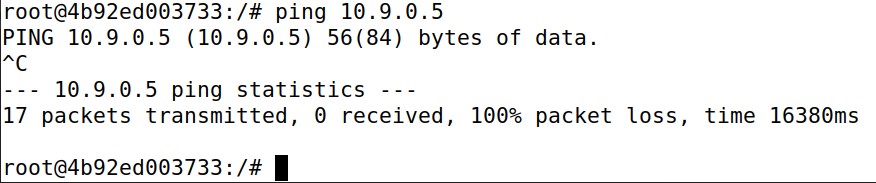
 外网主机不能 telnet 内网其他主机。

 外网主机无法 ping 内网主机。

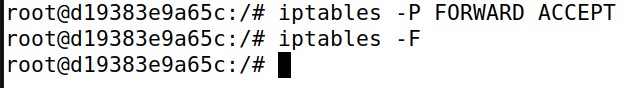
 内网主机可以 ping 所有内网主机 。



内网主机无法访问外网主机。

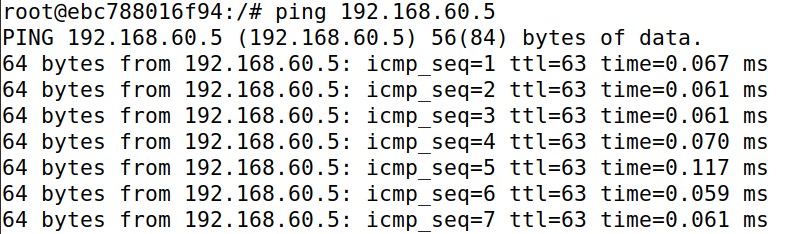


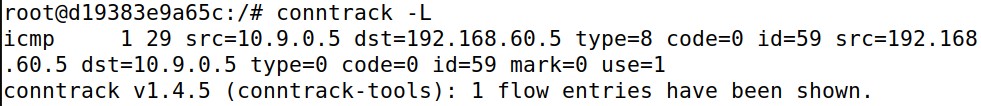
清除规则。

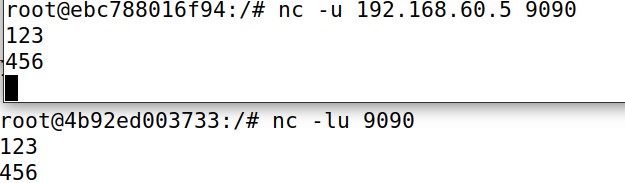


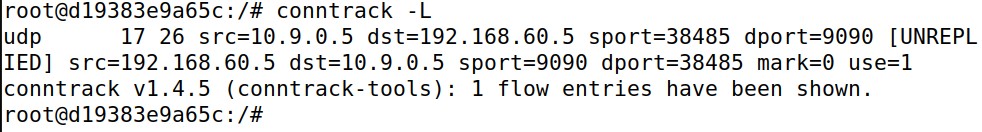
**Task3**

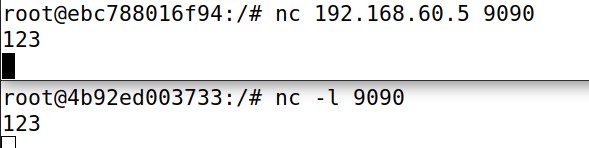
Task3.A

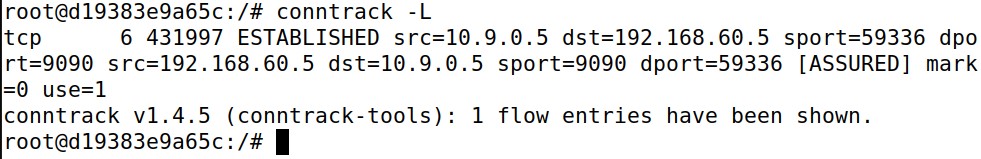
在 10.9.0.5 上 ping192.168.60.5。  在路由器上查看跟踪信息，可知持续时间为 30s。

 在 192.168.60.5 上开一个 UDP 服务器，在 10.9.0.5 上发送报文。

 查看路由器跟踪信息，可知持续时间为 30s。

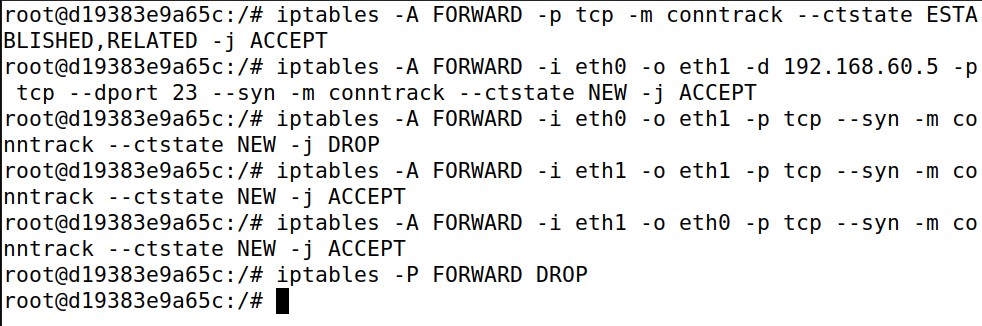
 在 192.168.60.5 上开一个 TCP 服务器，在 10.9.0.5 上发送报文。

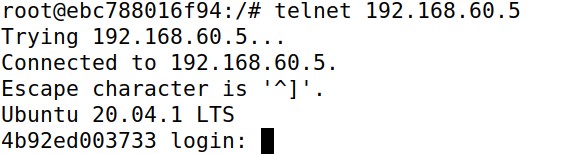
 查看路由器跟踪信息，可知持续时间为 432000s。

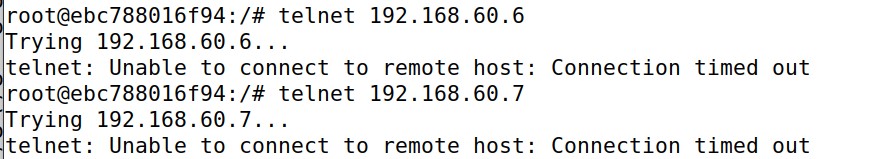


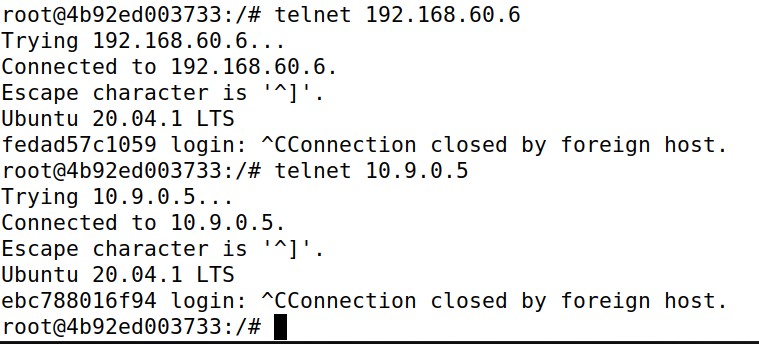
Task3.B

在路由器里设置如下规则。

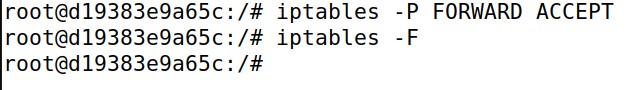
 外部主机可以 telnet192.168.60.5。

 外部主机不能 telnet 到内网其他主机。

 内网主机可以 telnet 到任意内网或外网主机。

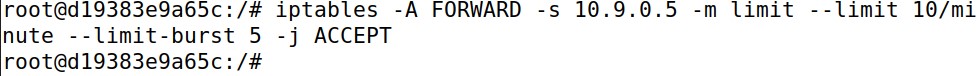


清除规则。

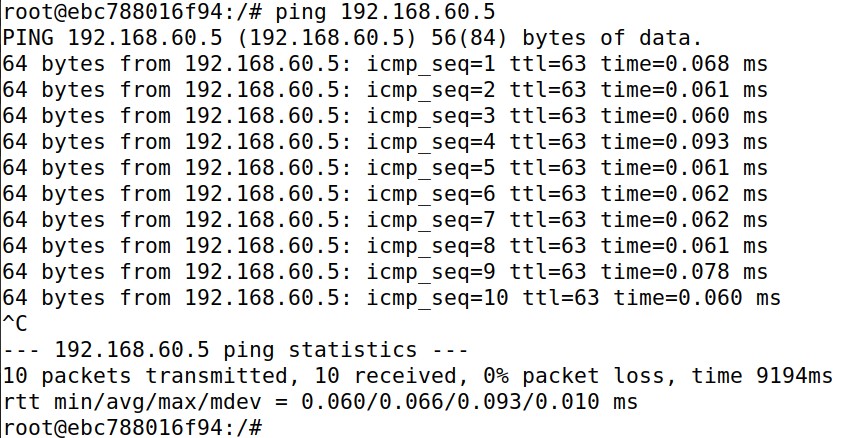


**Task4**

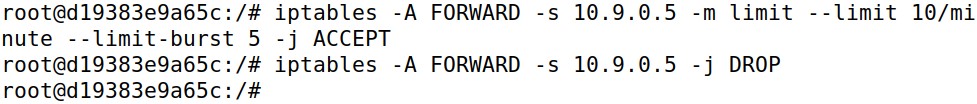
在路由器里设置如下规则。



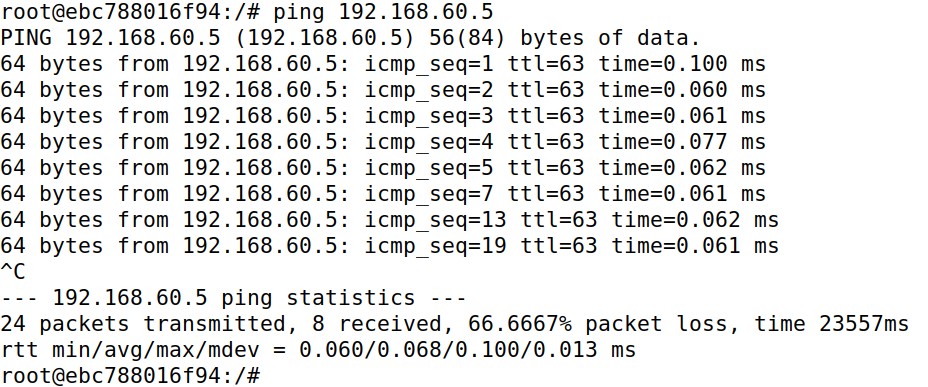
在 10.9.0.5 上 ping192.168.60.5，没有丢包现象。



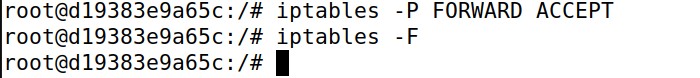
在路由器里加入第二条规则。



继续在 10.9.0.5 上 ping192.168.60.5，能 ping 通但有丢包现象。



清除规则。

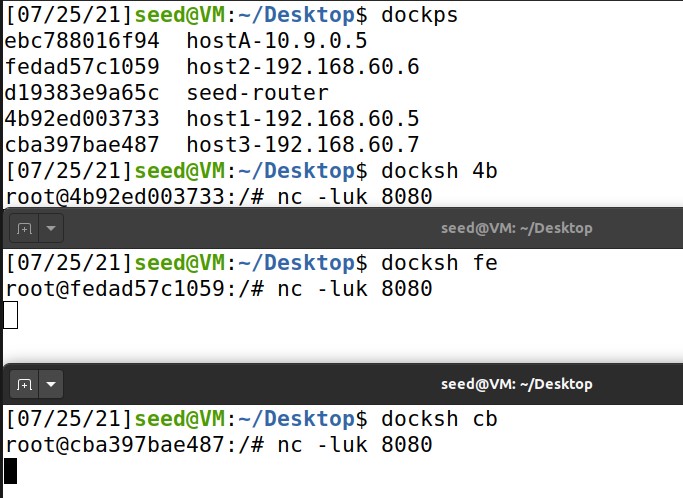


**Task5**

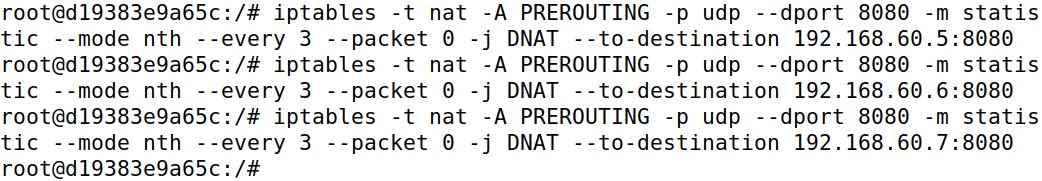
轮询模式：

在 192.168.60.5, 192.168.60.6, 192.168.60.7 上 8080 端口都开一个

UDP 服务器。

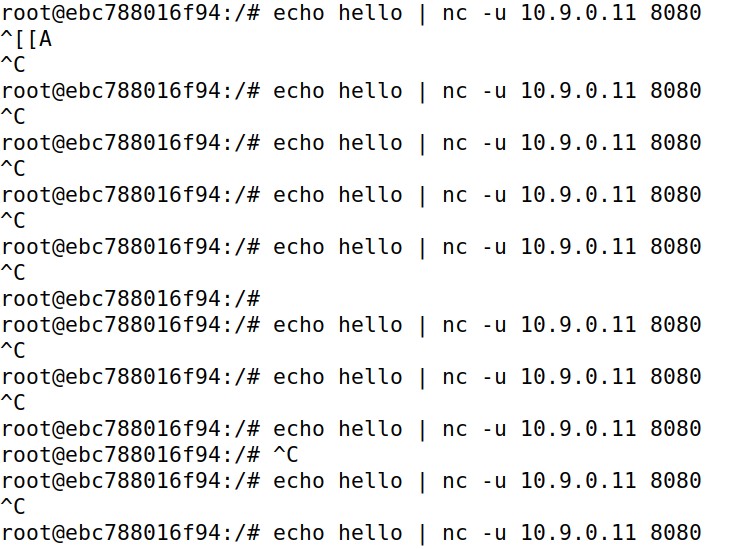


在路由器里设置如下规则。

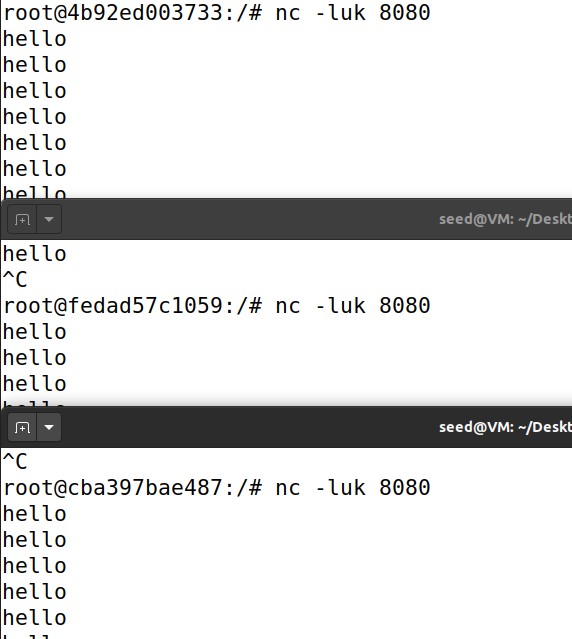


在 10.9.0.5 上输入足够多的 echo hello | nc -u 10.9.0.11 8080，观察三

个服务器 hello 的数量。



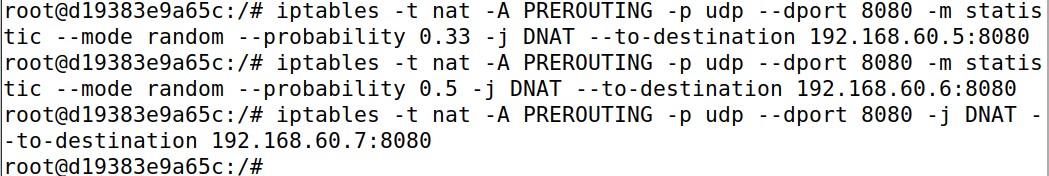
在输入了 75 次 echo hello | nc -u 10.9.0.11 8080 后，192.168.60.5， 192.168.60.6，192.168.60.7 里的 hello 数量为 50：15：10。



清除规则。

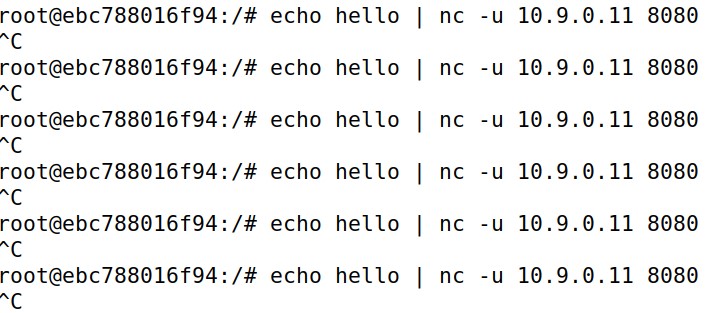


随机模式：在路由器里设置如下规则。

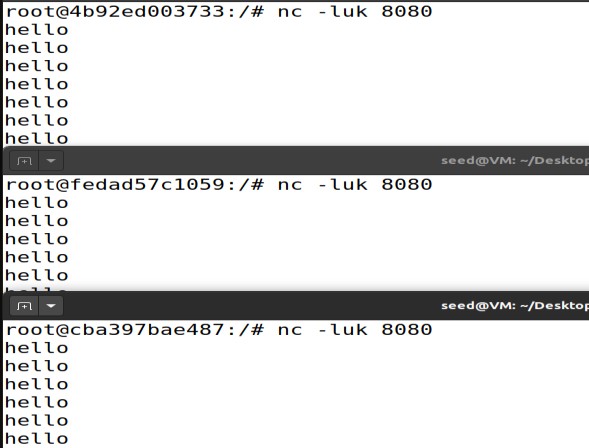


在 10.9.0.5 上输入足够多的 echo hello | nc -u 10.9.0.11 8080，观察三

个服务器 hello 的数量。



在输入了 84 次 echo hello | nc -u 10.9.0.11 8080 后，192.168.60.5， 192.168.60.6，192.168.60.7 里的 hello 数量为 54：19：11。



清除规则。

