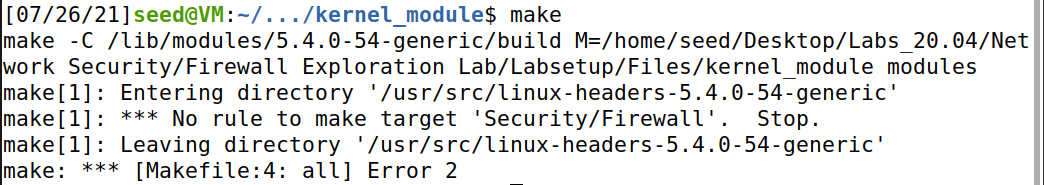
57118127孙博

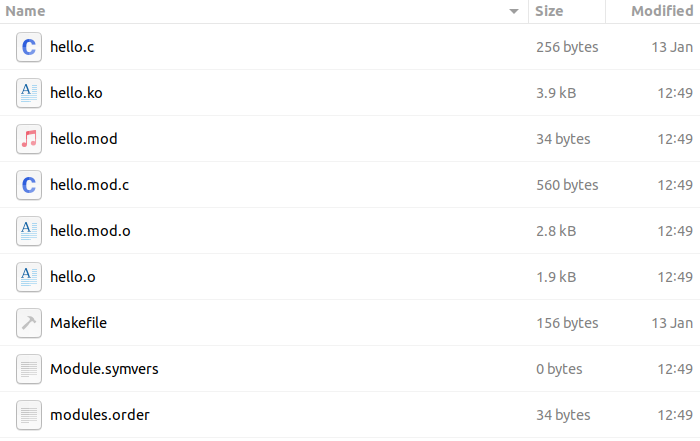
**Task1**

**1.A**

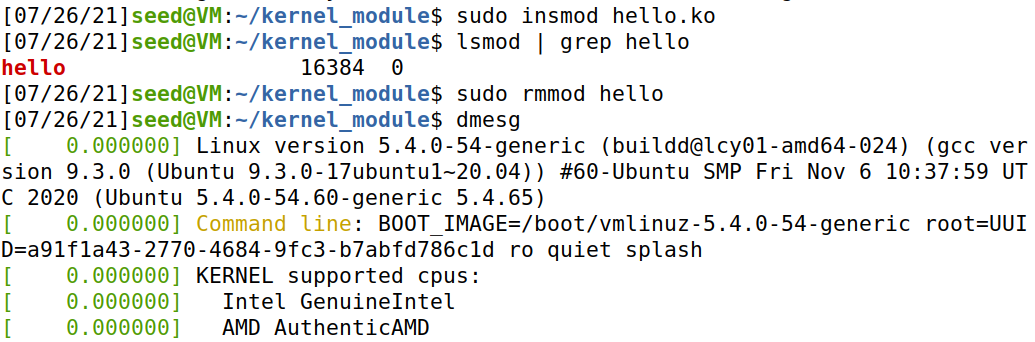
将文件夹移动到无空格的目录下，然后make



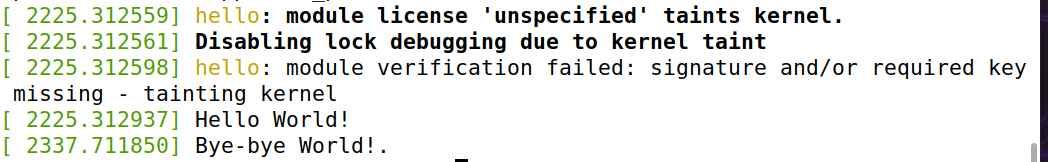
Make后文件夹中文件如下



输入指令添加模块

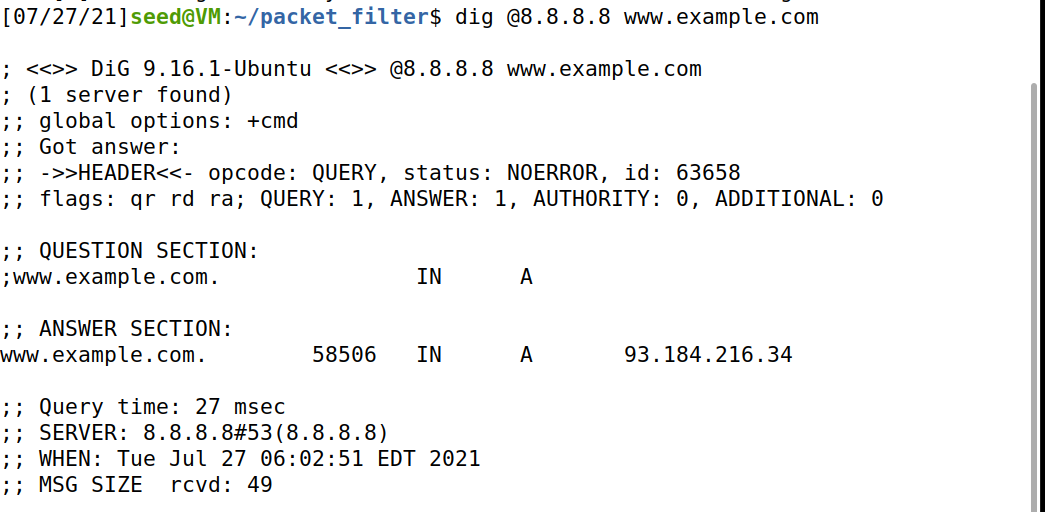


安装成功

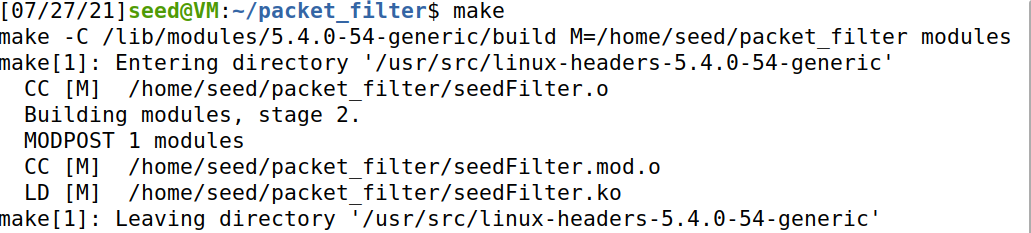


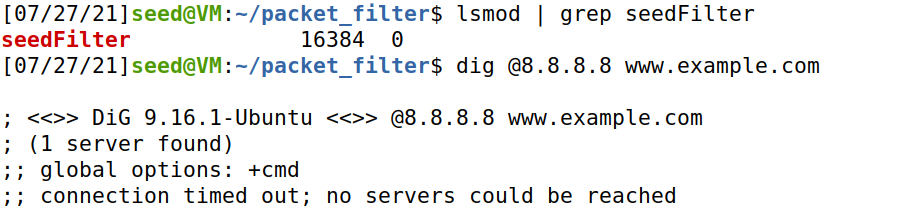
**1.B.1**

攻击前用dig指令查看



将packet\_filter编译并加载模块

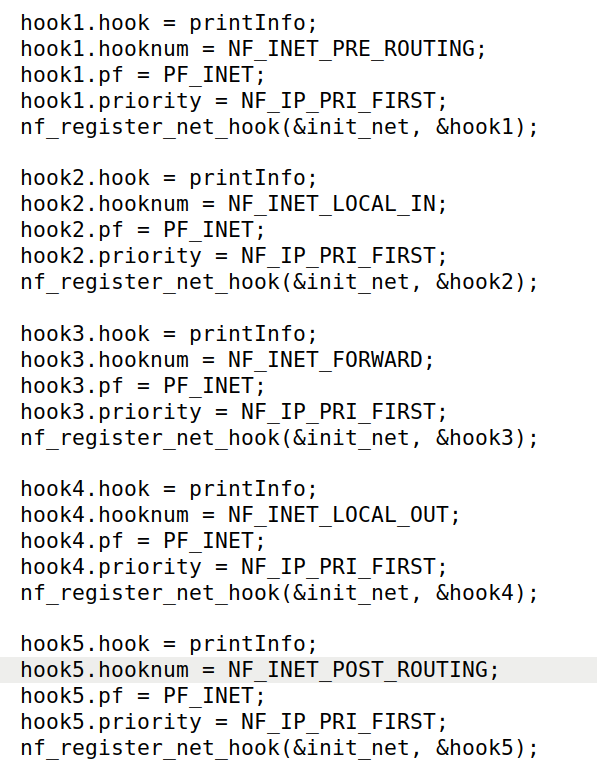


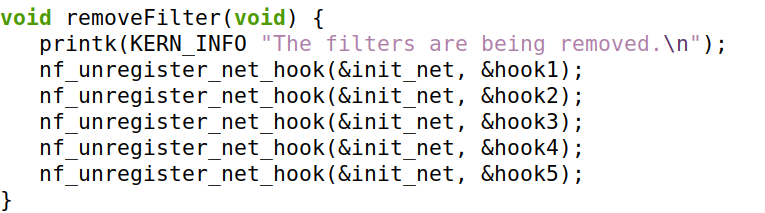


再次dig后发现无法连接，请求被阻塞

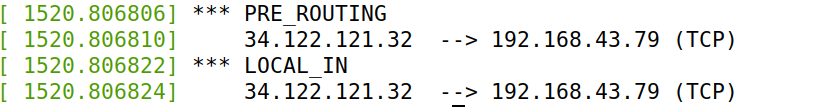
**1.B.2**

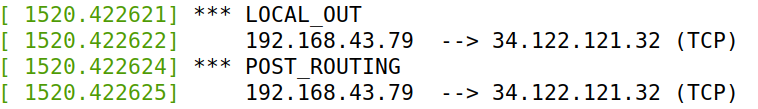
修改程序，新增hook并将其与printlnfo关联





用dmesg查看日志





并未出现NF\_INET\_FORWARD的活动，hook函数调用时刻如下

NF\_IP\_LOCAL\_OUT:在数据包以其方式离开主机之前。

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

NF\_IP\_PRE\_ROUTING:在做出任何路由决策之前

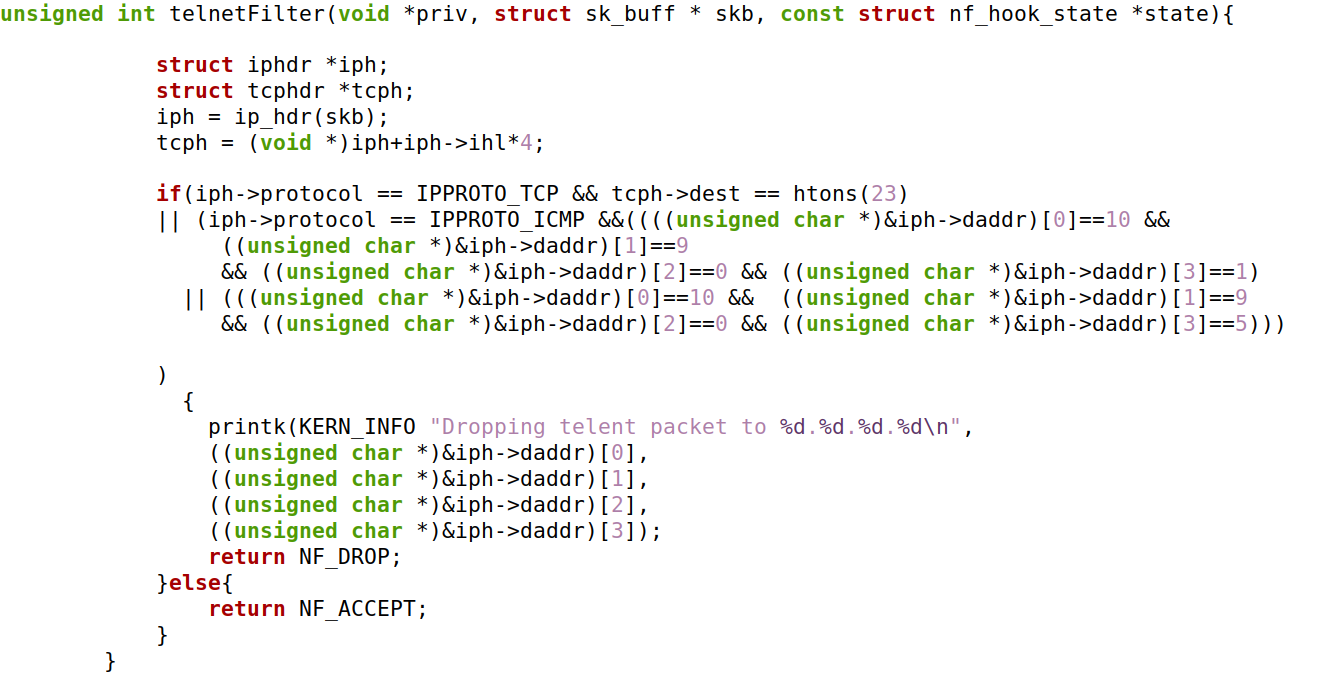
NF\_IP\_LOCAL\_IN:在发送到网络堆栈之前

NF\_IP\_FORWARD:向其他主机转发报文。

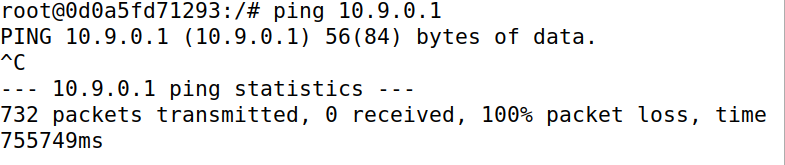
**1.B.3**

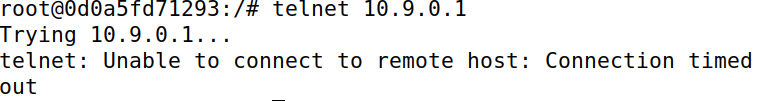
增加两个函数，分别用于拦截icmp报文和telnet报文

构造代码的主要部分如下

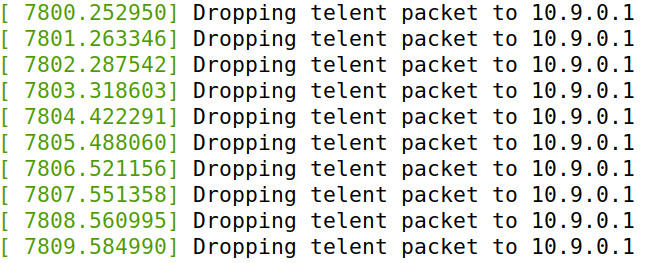


测试发现在hostA上ping和telnet都无法成功





Dmesg部分结果如下

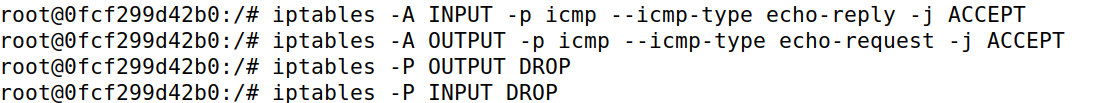


**Task2**

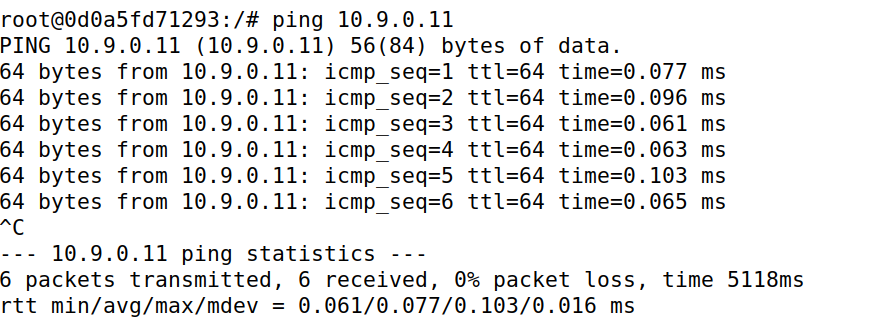
**A**

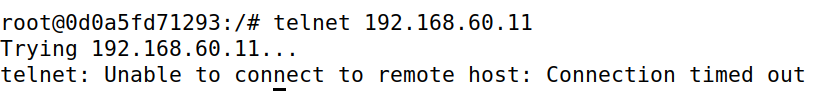
防止外部机器访问路由器机器，除了ping

首先在路由器上设置以下规则

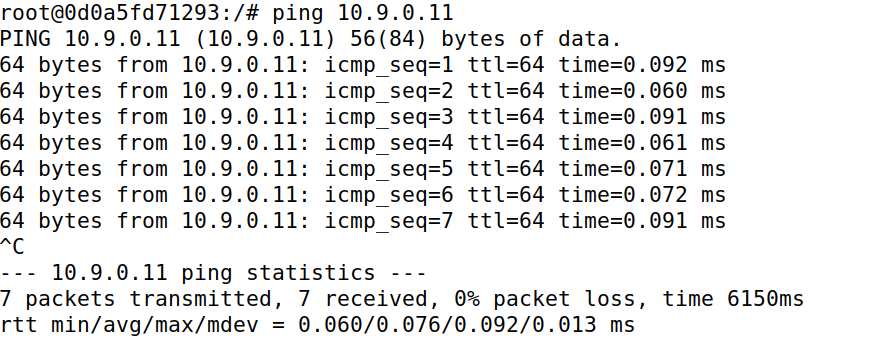


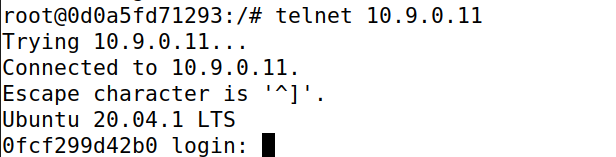
发现从10.9.0.5上能ping通路由器，但telnet失败





取消上述规则，发现ping和telnet均成功

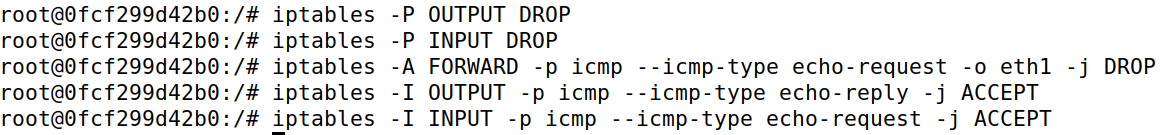




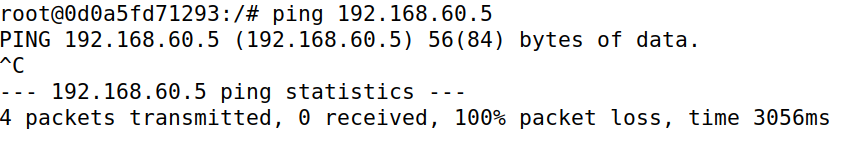
**B**

在路由器上设置防火墙规则来保护内部网络192.168.60.0/24

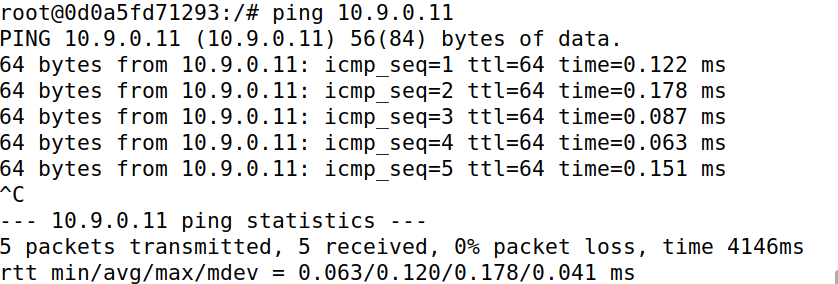
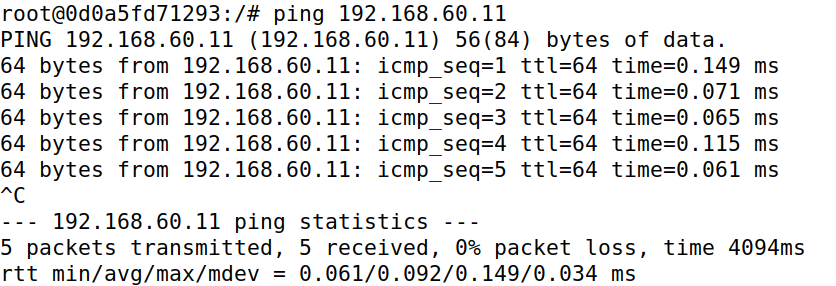
输入如下命令



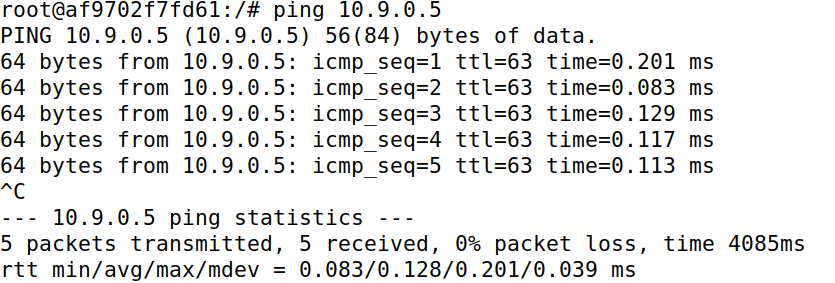
1. 外部主机ping不通内部主机，即从10.9.0.5ping到内网全部丢失



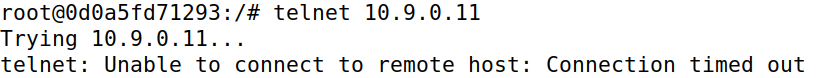
1. 外部主机可以ping通router，10.9.0.5分别ping router的eth0和eth1接口IP



1. 内部主机可以ping通外部主机即内部主机192.168.60.5可以ping通10.9.0.5



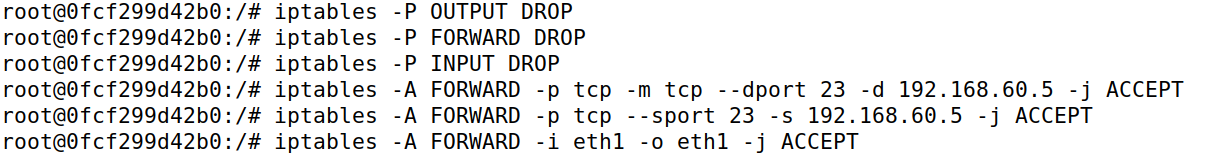
1. 内网其他包会被阻塞，即尝试发送tcp包的telnet无法连接



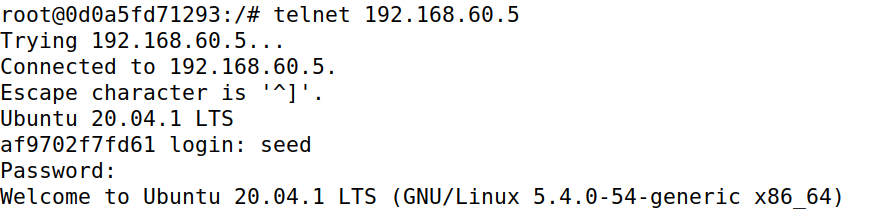
**C**

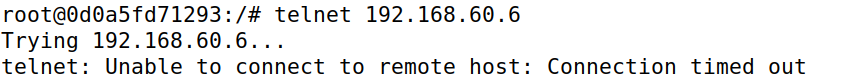
保护内部网络(192.168.60.0/24)内的TCP服务器

输入如下命令

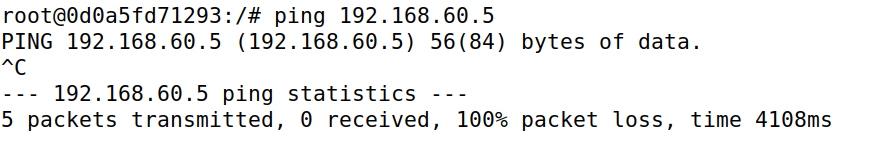


1. 外部主机只能访问192.168.60.5上的telnet服务器，不能访问其他内部主机。

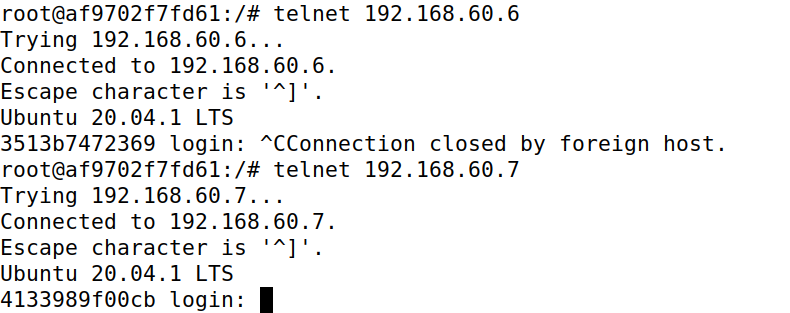


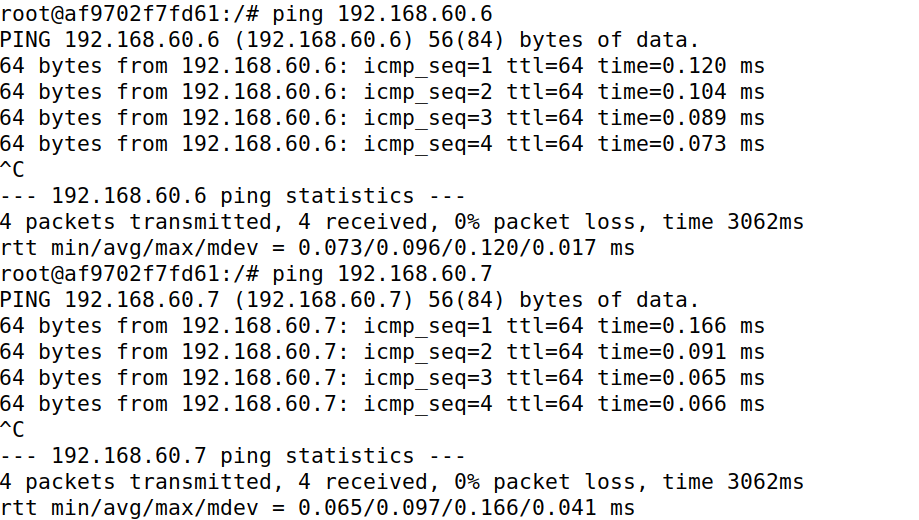


1. 外部主机不能访问内部服务器

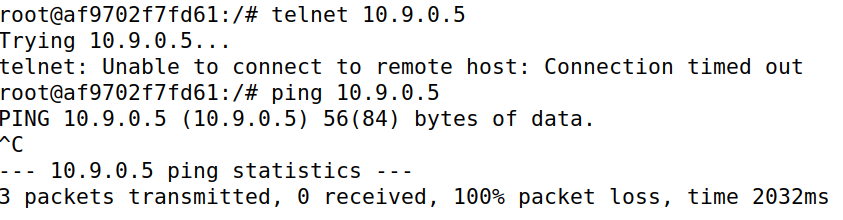


1. 内部主机可以访问所有内部服务器





1. 内部主机不可以访问外部服务器

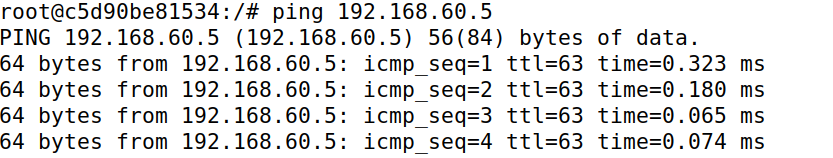


**Task3**

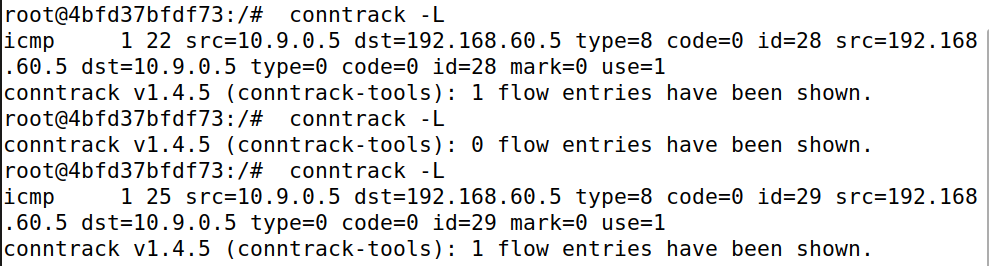
**A**

ICMP

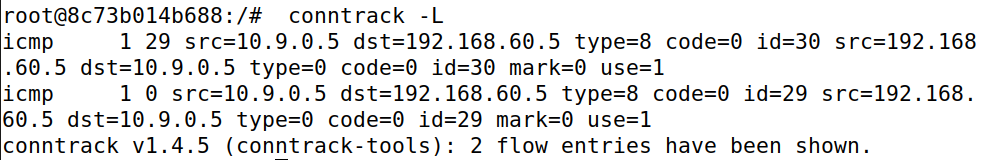
1)在10.9.0.5上ping 192.168.60.5主机



2)查看追踪信息可以看到一个icmp持续时间为30s，如果停止icmp，则会进入倒计时直至减少到0。

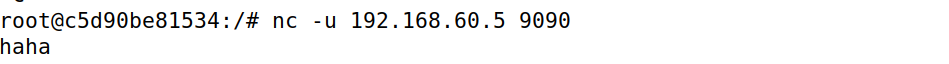


如果30s内再次ping，则会显示两个flow。

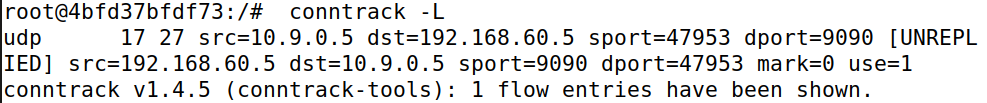
****

**UDP**

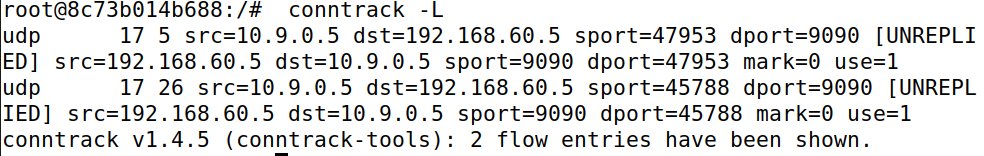
1)在主机10.9.0.5上输入指令



2)查看追踪信息

时间同样为30s，且停止登录后会倒计时到0。

同样，30s内再次连接会出现两条记录。



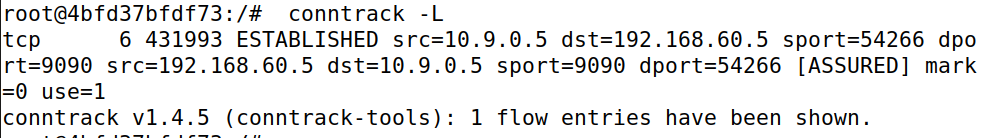
**TCP**

1)在当前机和目标主机上输入指令，建立连接

J%I3OETI%ZB~3WO%~SU``1W

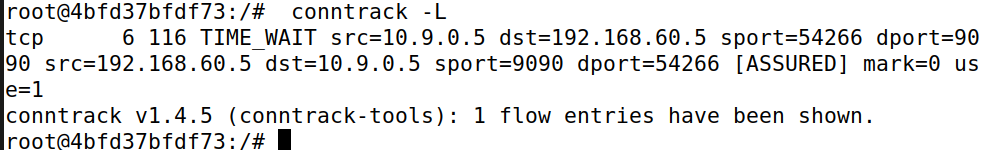
{JY{V]6A5DLBFY2_8)]N{$D

2)查看追踪



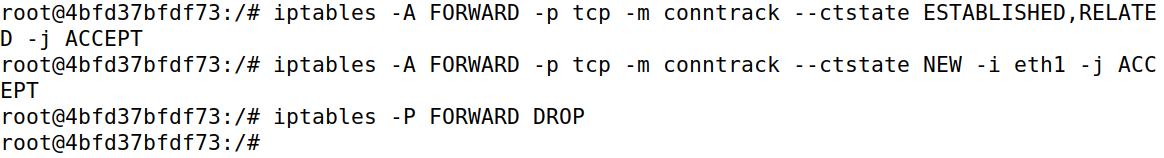
可以看到，存活时间在430000s以上

3)结束连接，可以看到记录仍然存在，但只存在120s，120s倒计时结束后将消失。



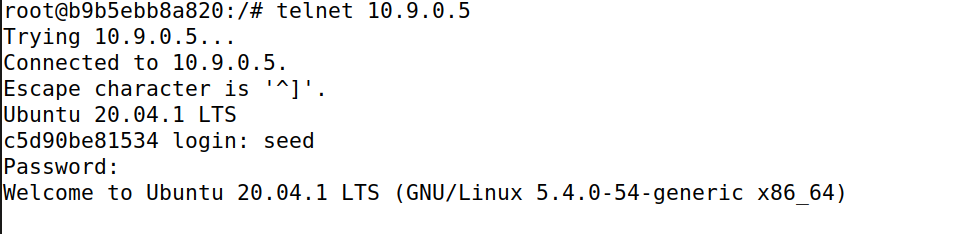
**B**

1)编写规则如下

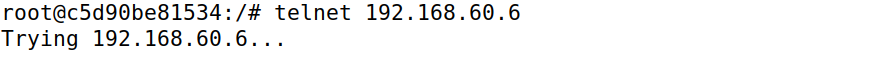


2)测试

内网telnet外网，成功

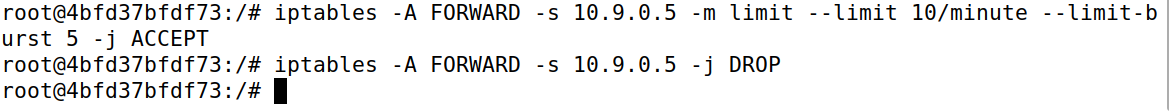


外网telnet内网，无法连接

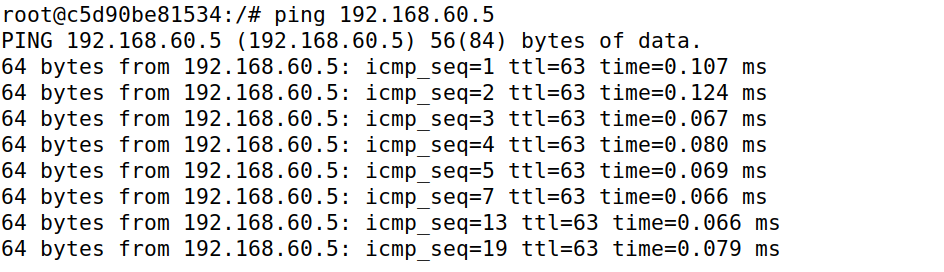


**Task4**

1)在路由器输入规则

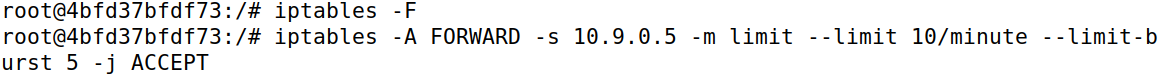


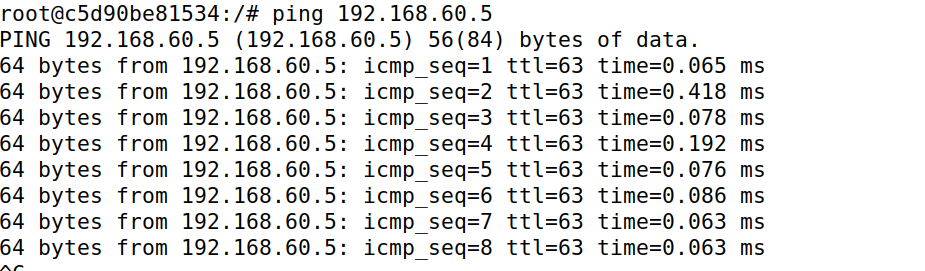
2)在10.9.0.5主机尝试ping



可以看到，前几个报文速度非常快，后面速度较慢，平均6s一个，说明规则发挥了作用

3)去掉第二条规则，再次尝试ping





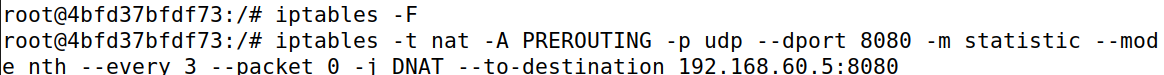
可以看到，报文发送速度很快，并没有减慢到每分钟10个，说明规则失效了。

这是因为没有第二条规则将报文设置为默认DROP，所有报文（无论是否满足第一个规则）都会从默认的ACCEPT规则通过，从而导致第一条规则也失效。

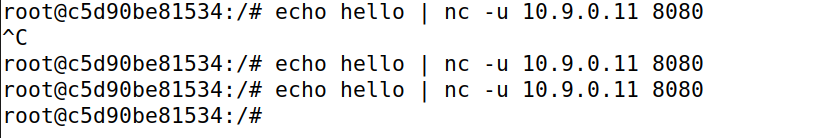
**Task5**

**轮询：**

1)在路由器上输入规则



2)在192.168.60.5上开启nc -luk 8080 监听，在10.9.0.5处连接并输入hello

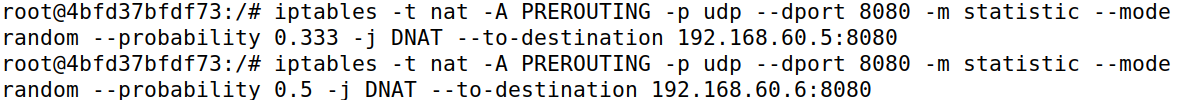


3)在192.168.60.5上查看，可以看到发送者没发送3次，接收者再会收到1次路由器转发的报文，说明路由规则正确。

M_4KF_28S%NY~XG38UZUXER

**随机：**

1)指定规则如下

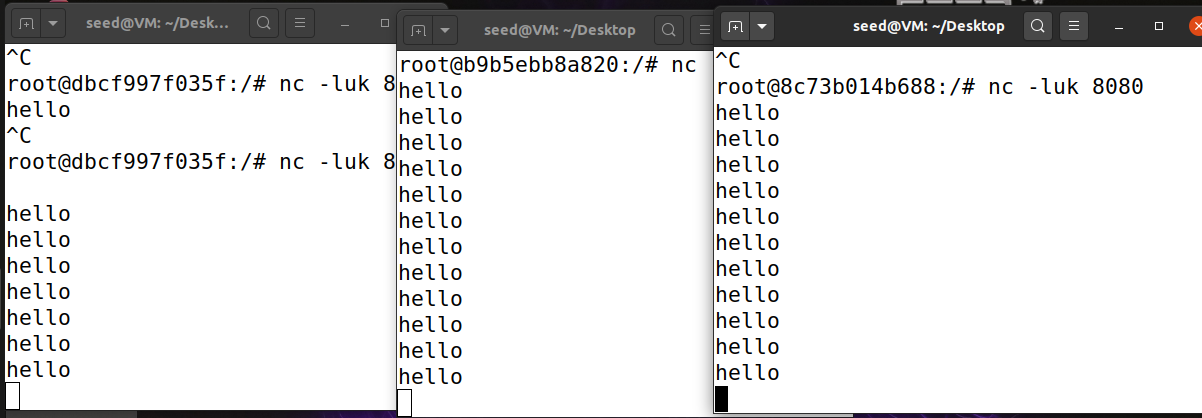


~_BL}FJJ6)V[G7)K_ZN2~CG

其中第一个的概率为0.333，第二个概率则应当在第一个规则没命中基础上考虑，即为0.5，

当前两个没有命中，则默认命中第三条

2)在三台主机上都输入nc -luk 8080打开监听，在10.9.0.5主机上建立连接并不断输入hello，得到三台主机上的输出结果如下：



可以看到路由确实实现了分发，由于样本数量太少，不能做到每个主机上收到的报文各1/3,但总体上符合负载均衡的要求。