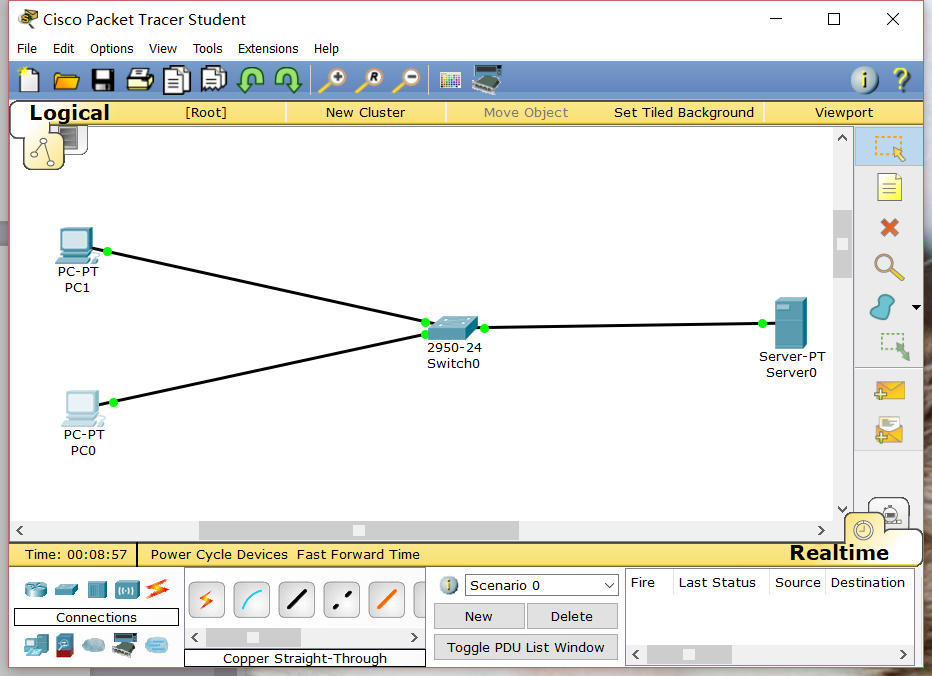
# 作业二

# 实验4-4 免费ARP

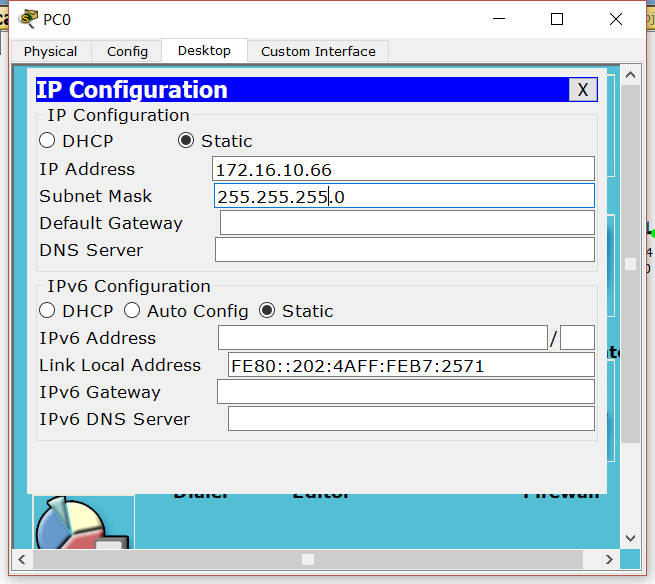
# （1）、在Packet Tracer6.0中观察免费ARP

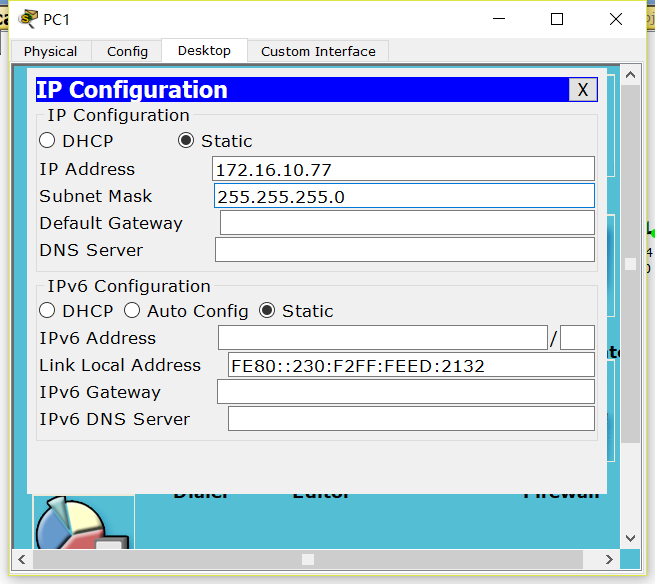
1. 设置好IP地址以及完成拓扑结构的连接设置

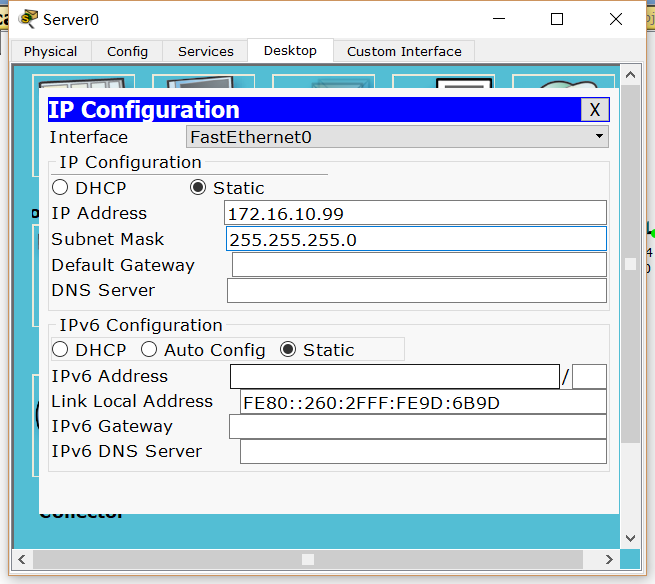
- 进行拓扑连接



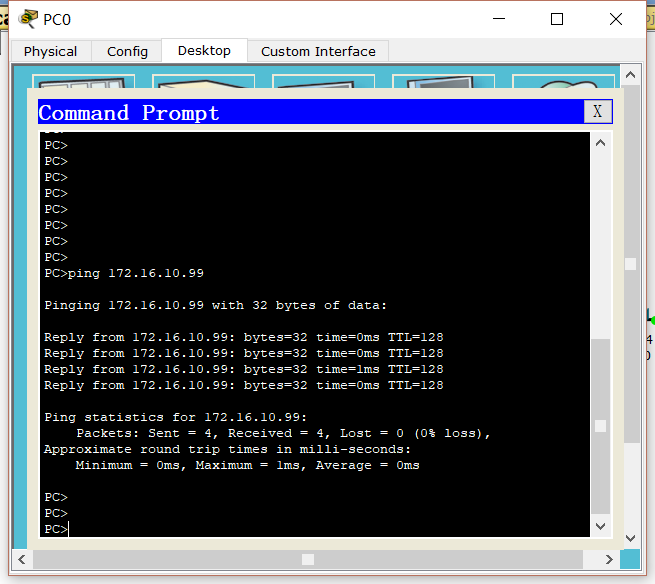
- 设置IP地址

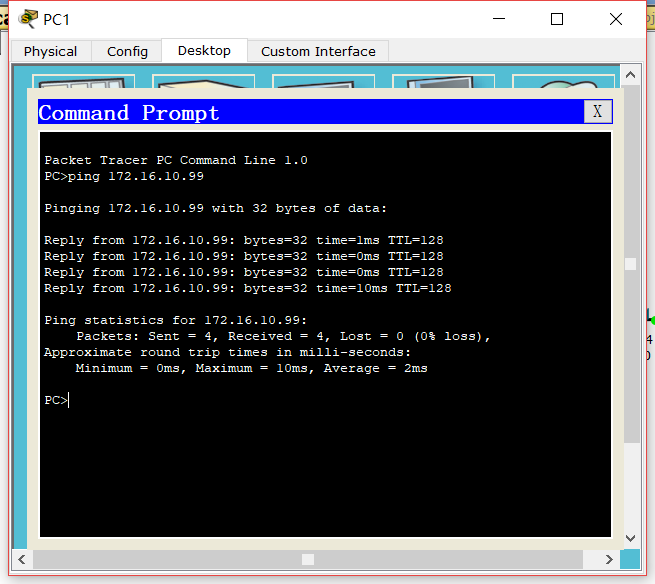






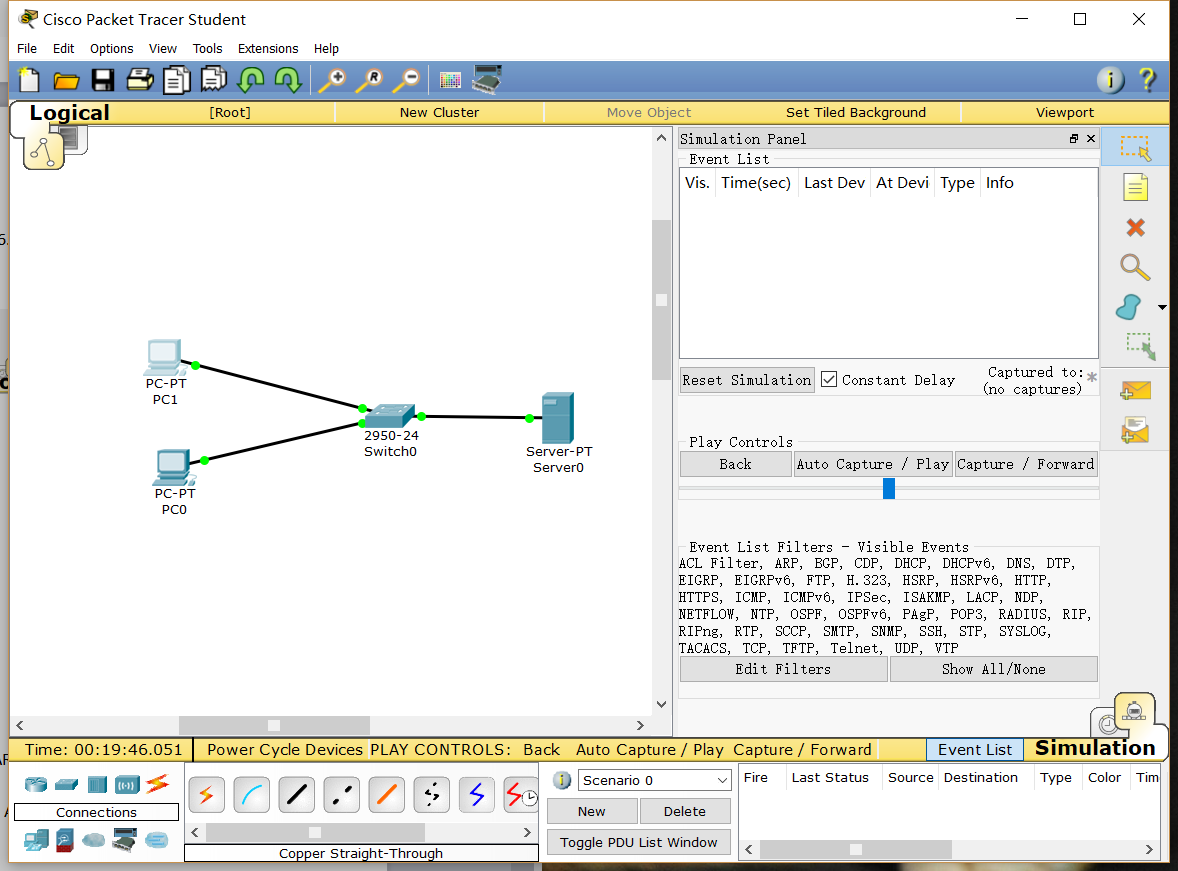
1. 在pc0和pc1上Ping server0.这将在各个机器上建立ARP表，查看ARP表并记录



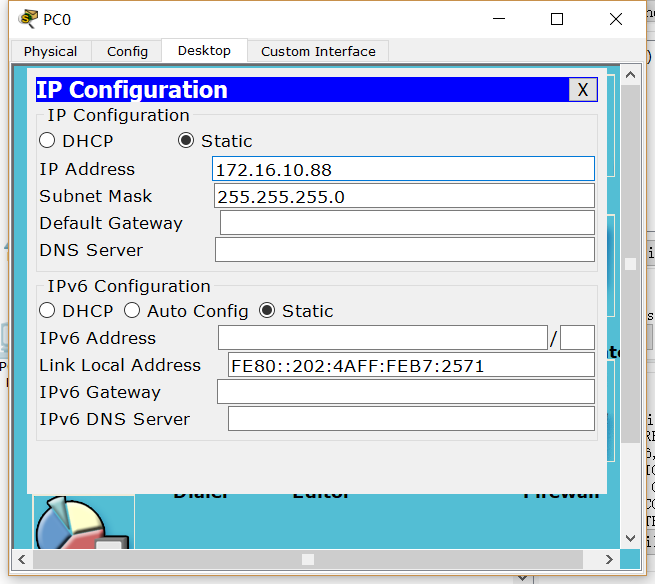


1. 切换到模拟方式，修改PC0的ip地址，如修改为172.16.10.88

- 将模式切换成**simulation**

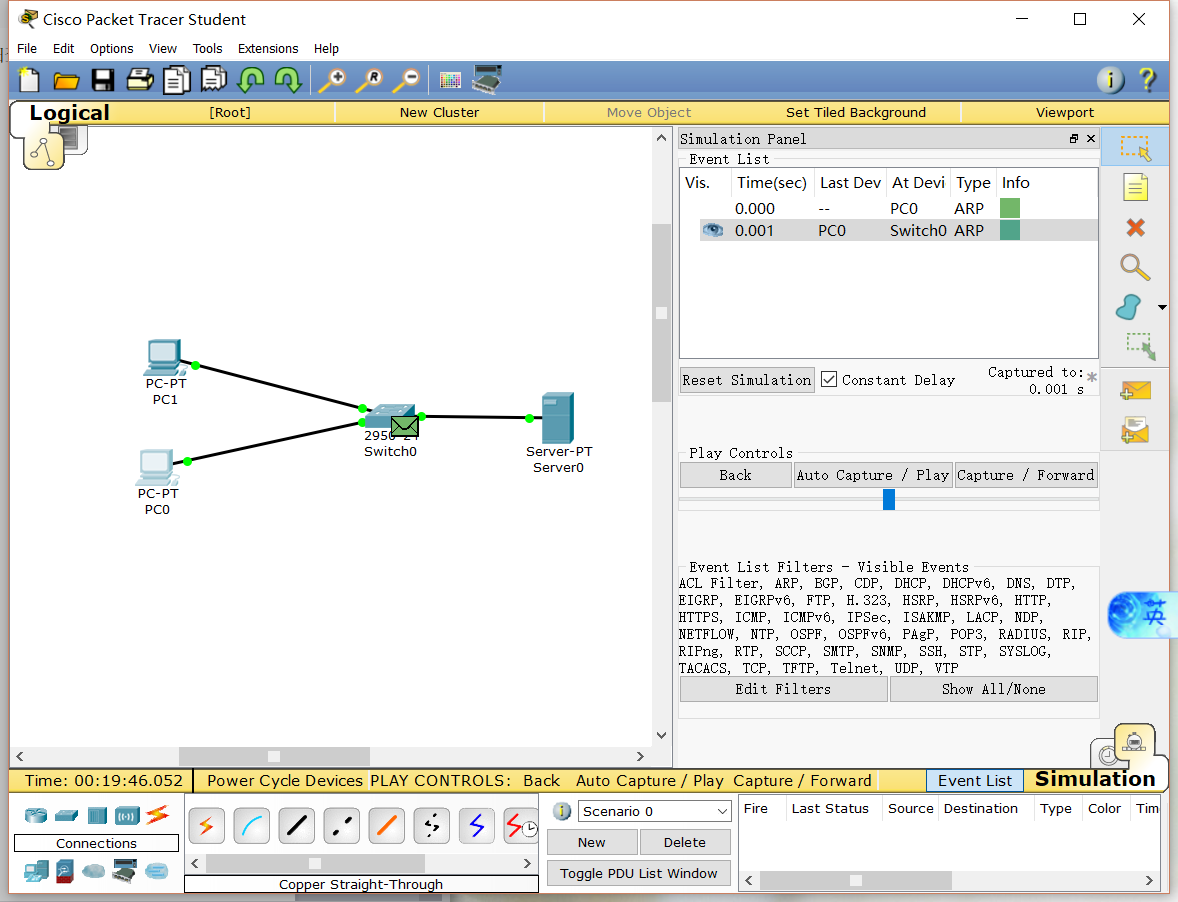


- 在desktop中的Ipconfiguration中修改pc0的ip地址

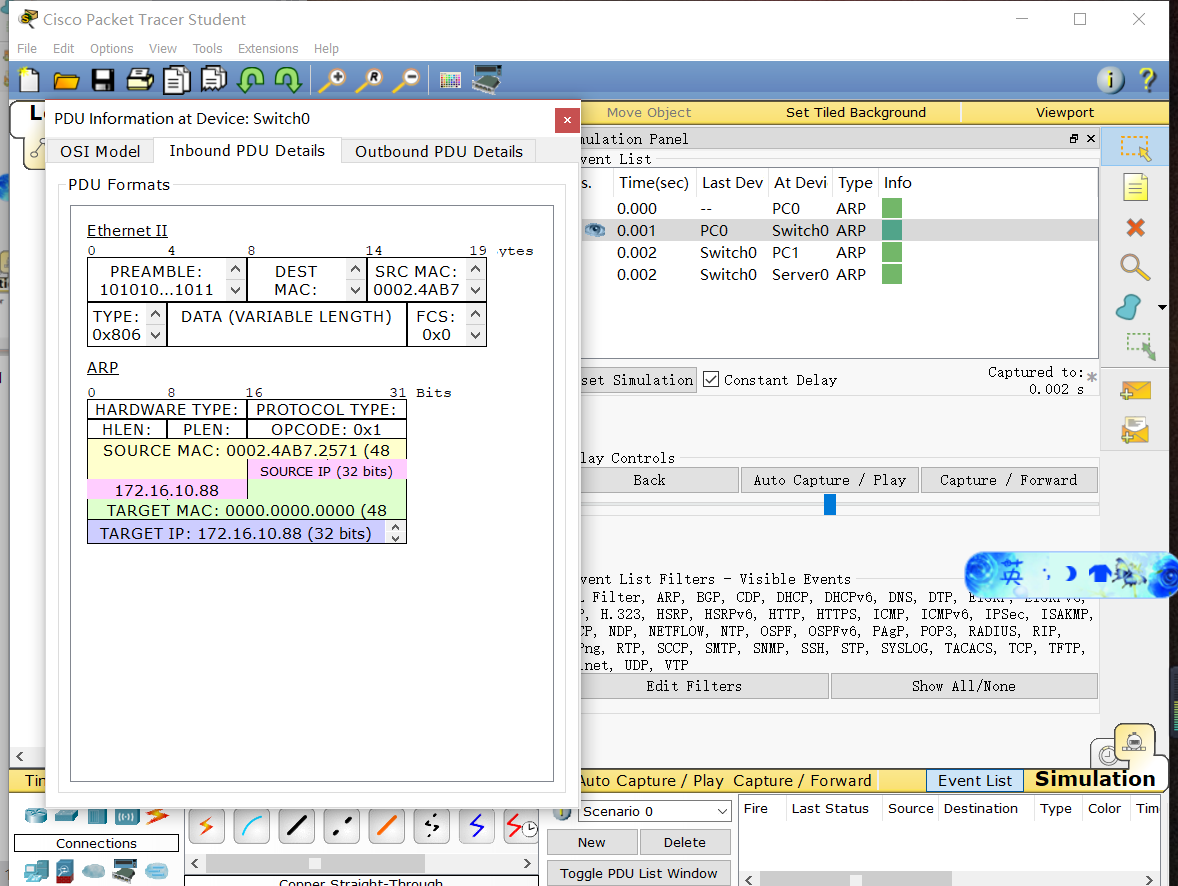


1. 单击capture/forward按钮，立刻可观察到pc0发出的ARP包，仔细查看pdu信息和处理说明。

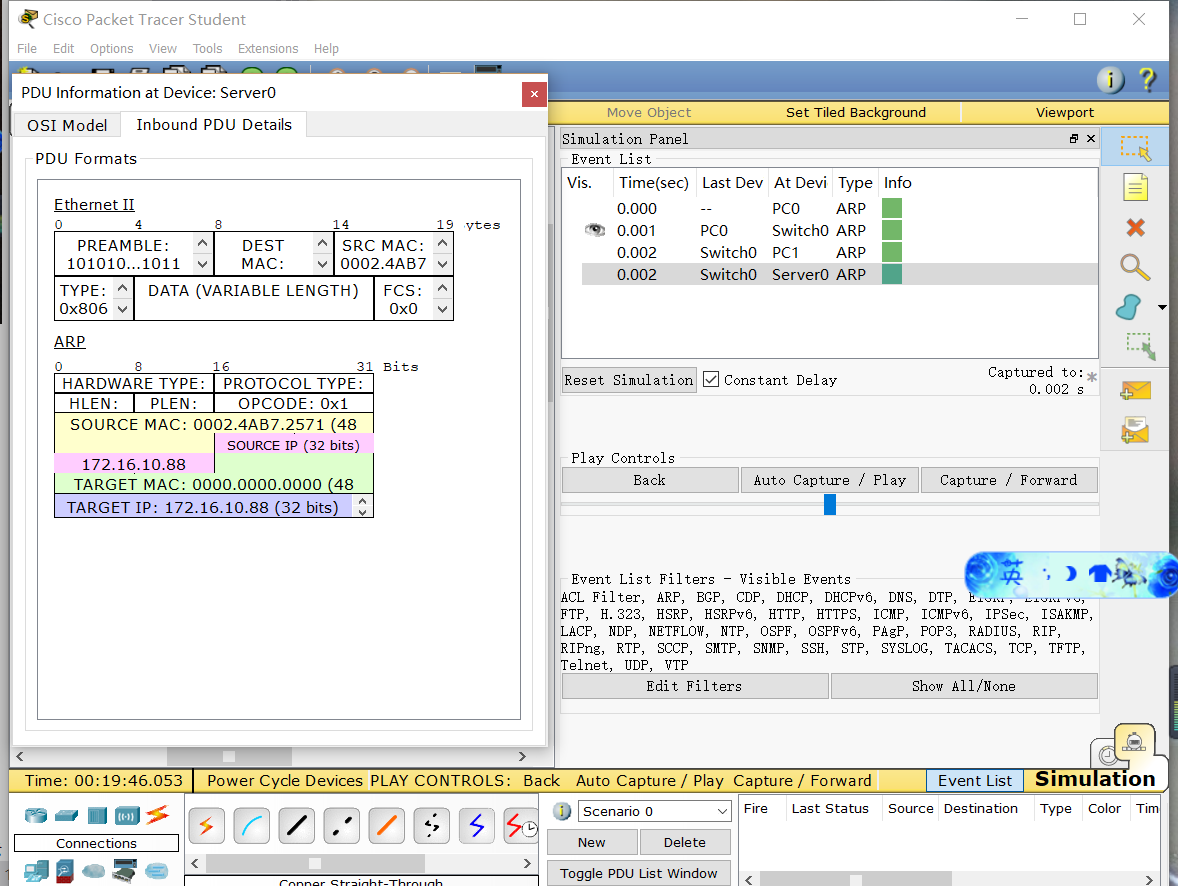
- 单击capture/forward按钮，立刻可观察到pc0发出的ARP包



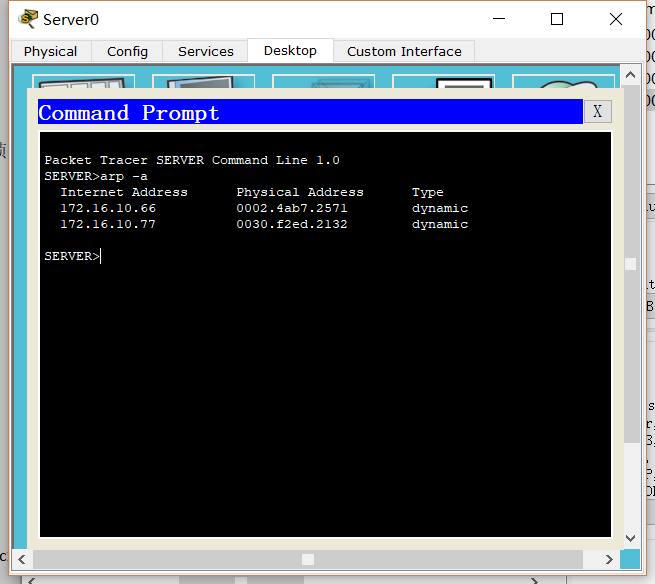
- 仔细查看pdu信息和处理说明，此处会看到Pc0发出的arp报文中发送端的ip地址和目的端ip地址是一样的，这就是gratuitous arp reauest。



- 继续在server0上观察，可以看到服务器ARP处理时，丢弃了这个帧而没有回应。

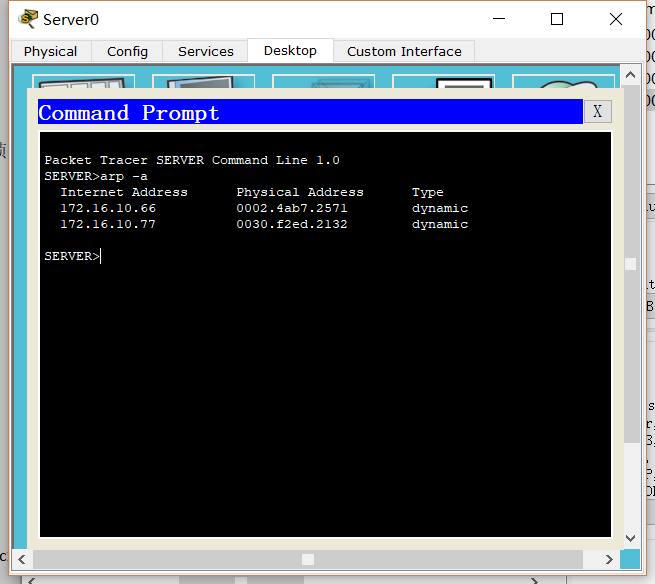


- 查看PDU处理说明，因为服务器上ARP表中没有相应的IP地址，因而丢弃了这个帧。这是协议默认对免费ARP的处理方式。



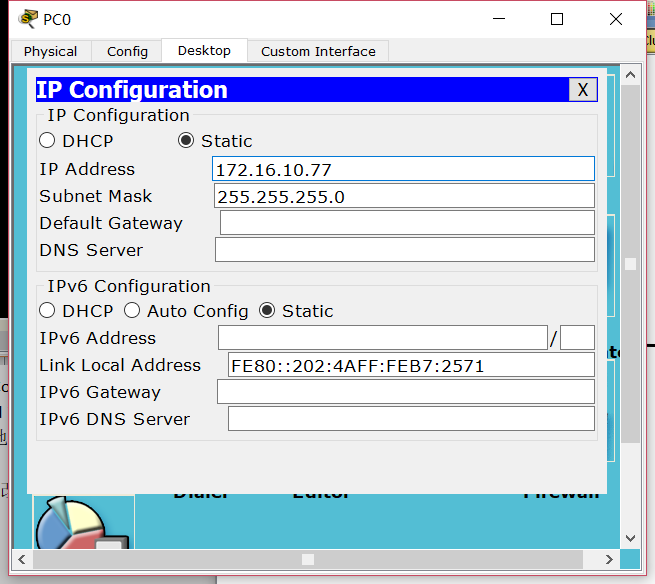
# （2）、免费ARP带来的漏洞

1. 接上续实验，首先在server0上运行arp命令，确认其ARP表的内容包含有pc0和pc1两台机器的ARP表项内容

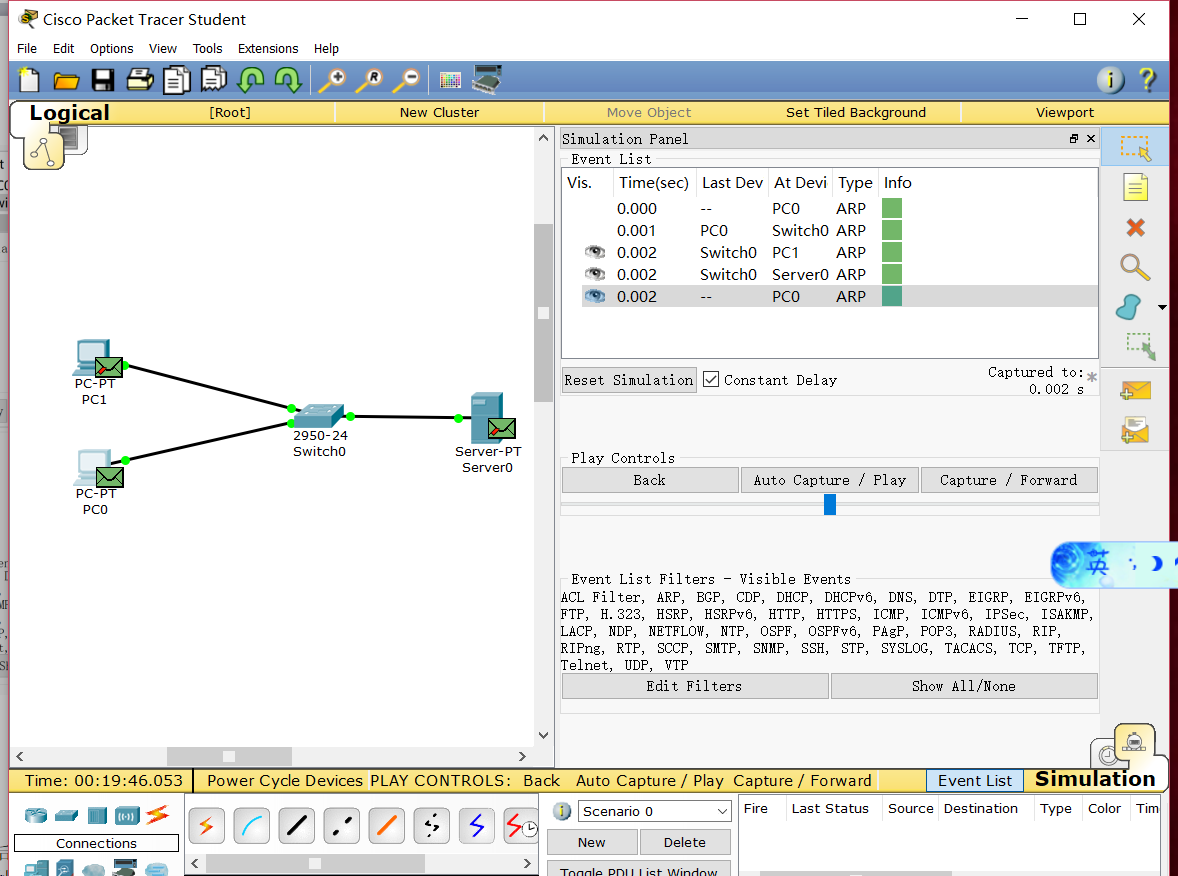


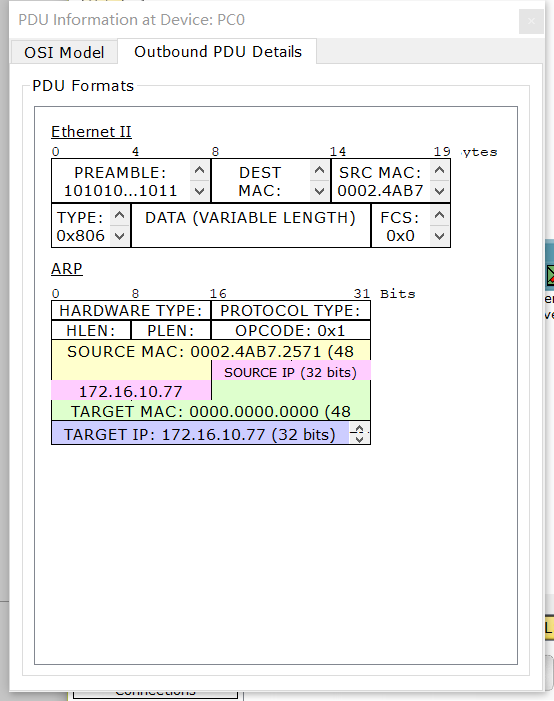
1. 切换到模拟方式，然后在PC0上打开DESKTOP选项卡，双击选择其中的IP Configuration，修改IP地址为172.16.10.77，马上切换到模拟窗口，单击capture/forward按钮，观察PC0向局域网内发送免费ARP广播，其源IP地址为PC1的地址，源MAC地址为PC0自己的地址。

- 在PC0上打开DESKTOP选项卡，双击选择其中的IP Configuration，修改IP地址为172.16.10.77

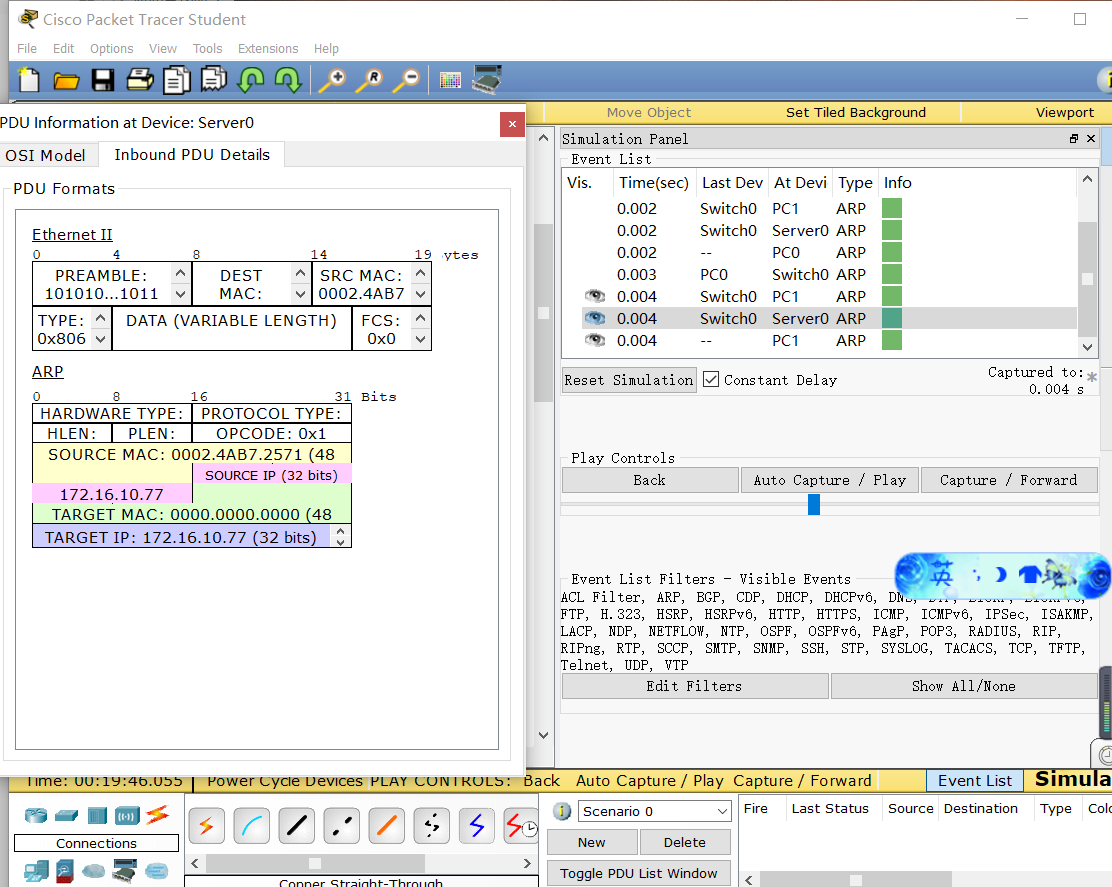


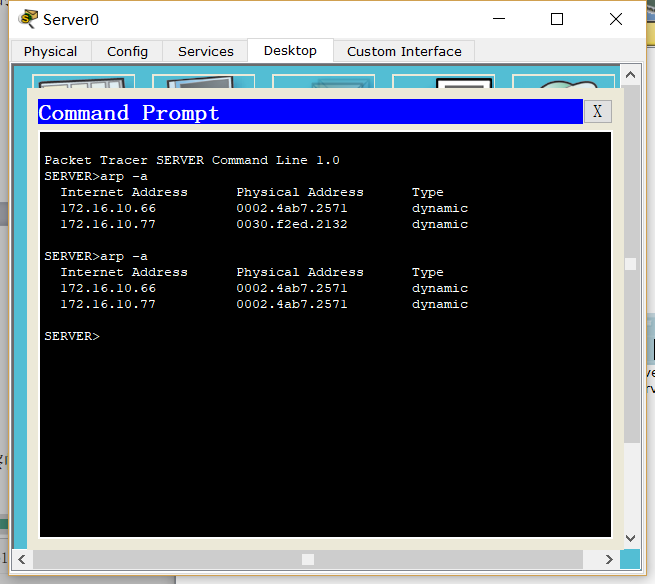
- 单击capture/forward按钮，观察PC0向局域网内发送免费ARP广播，其源IP地址为PC1的地址，源MAC地址为PC0自己的地址。



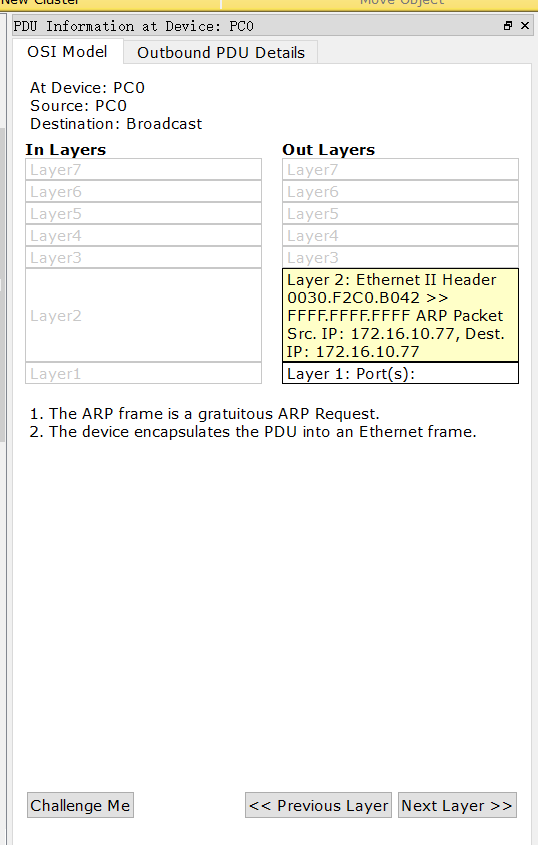


1. 在server0上收到数据帧后，查看PDU information,观察协议的处理过程。然后在server0上查看ARP表是否将自己ARP缓存中PC1的MAC地址改为PC0的MAC地址，如果是，就形成了MAC地址欺骗，记录实验结果。

- 在server0上查看ARP表已将自己ARP缓存中PC1的MAC地址改为PC0的MAC地址，形成了地址欺骗。

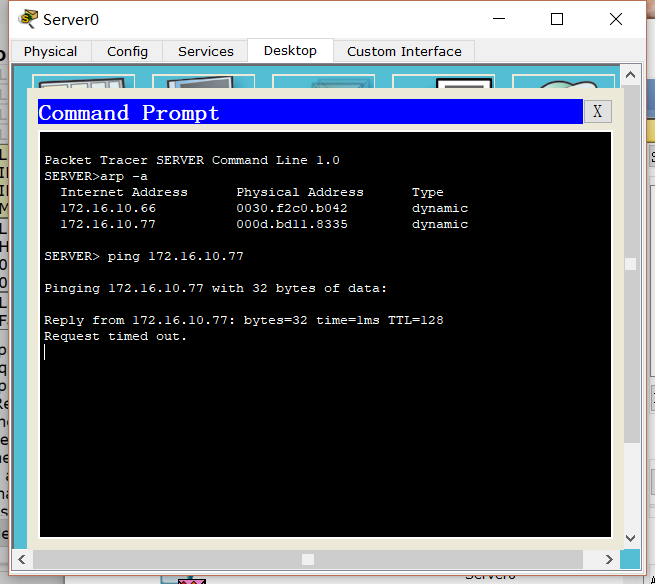


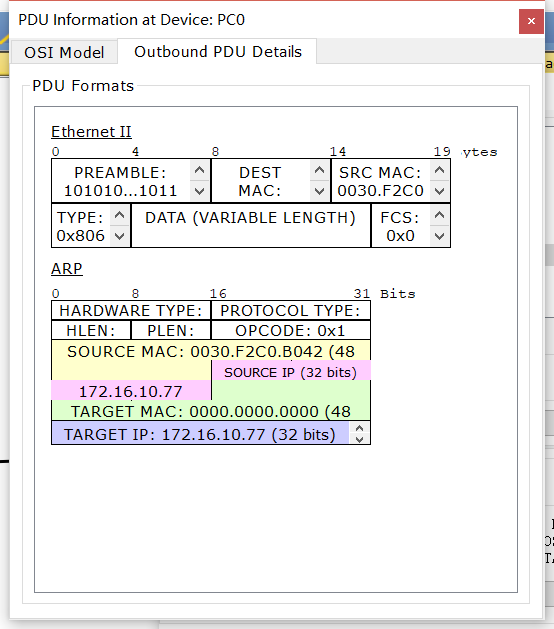
1. 当pc0发出的免费ARP到达PC1时，PC1会发出对免费ARP的响应报文，其目标地址为0.0.0.0，以通知全部网络节点IP地址172.16.10.77已被使用。注意观察帧的IP地址和MAC地址。

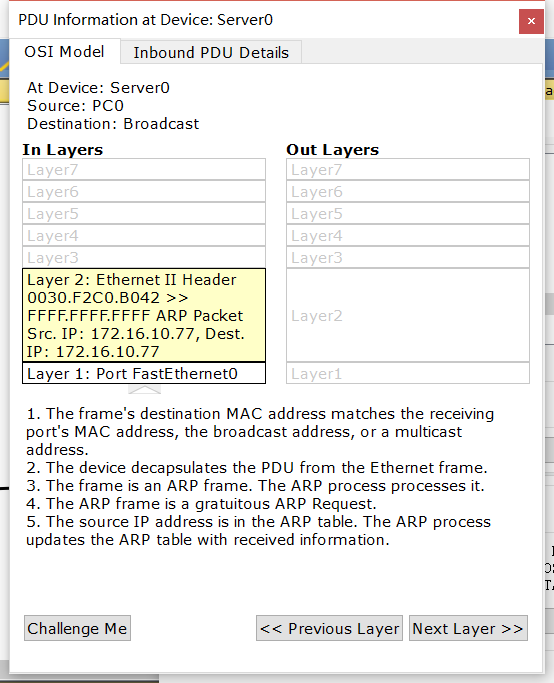


1. 模拟方式下在Server上运行以下命令

SERVER>ping 172.16.10.77







PC0发出的免费ARP到达PC1后，PC1会通知全部网络节点IP地址172.16.10.77已被使用；

联系图三的MAC地址信息以及ICMP回显请求（ICMP Message Type:8）可知server0已向pc0发出回显请求，但没有收到回显应答报文（ICMP Message Type:0）.

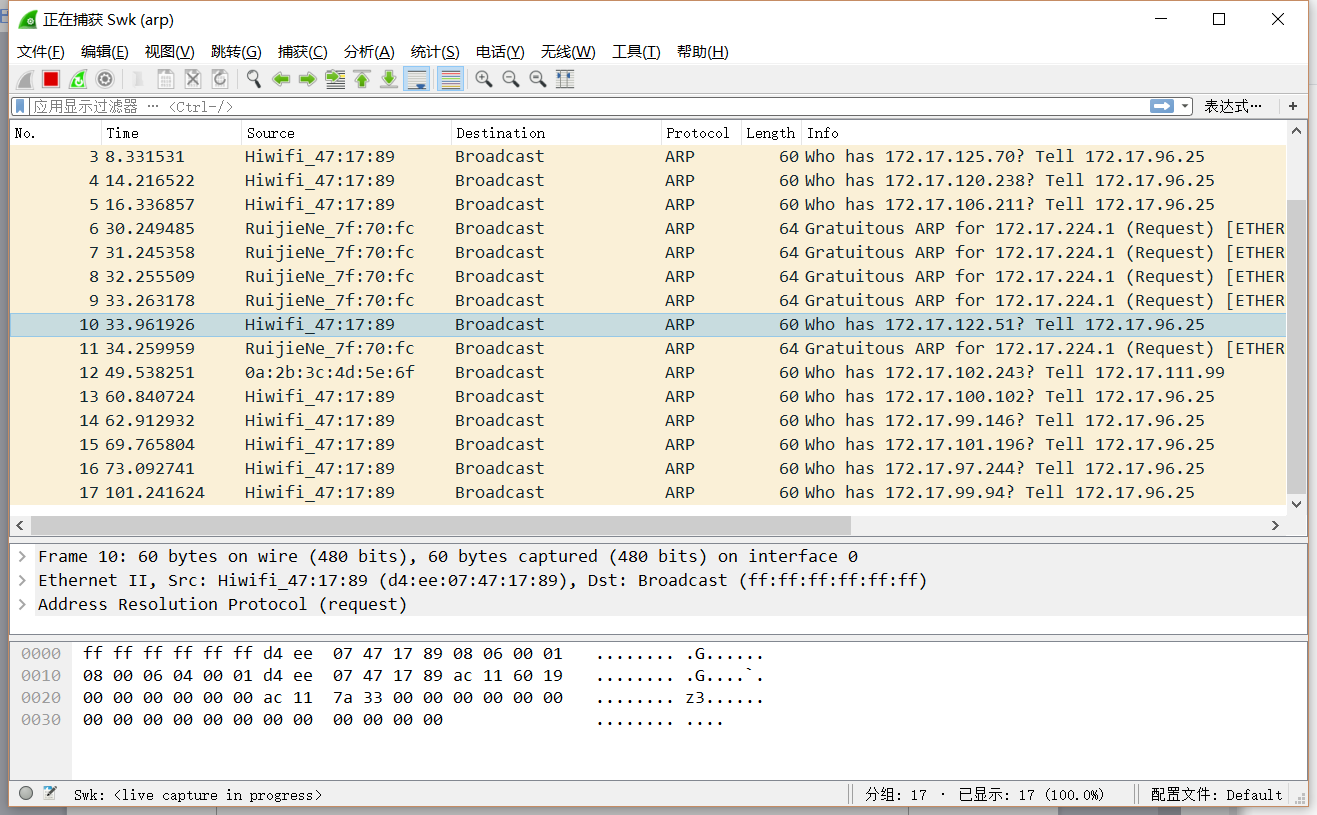
# （3）、用Wireshark1.10观察免费ARP

1. 要在真实网络环境中观察到免费ARP，需要有局域网环境，也可以参考图4.3，建立网络。

- 启用自动分配IPv4地址

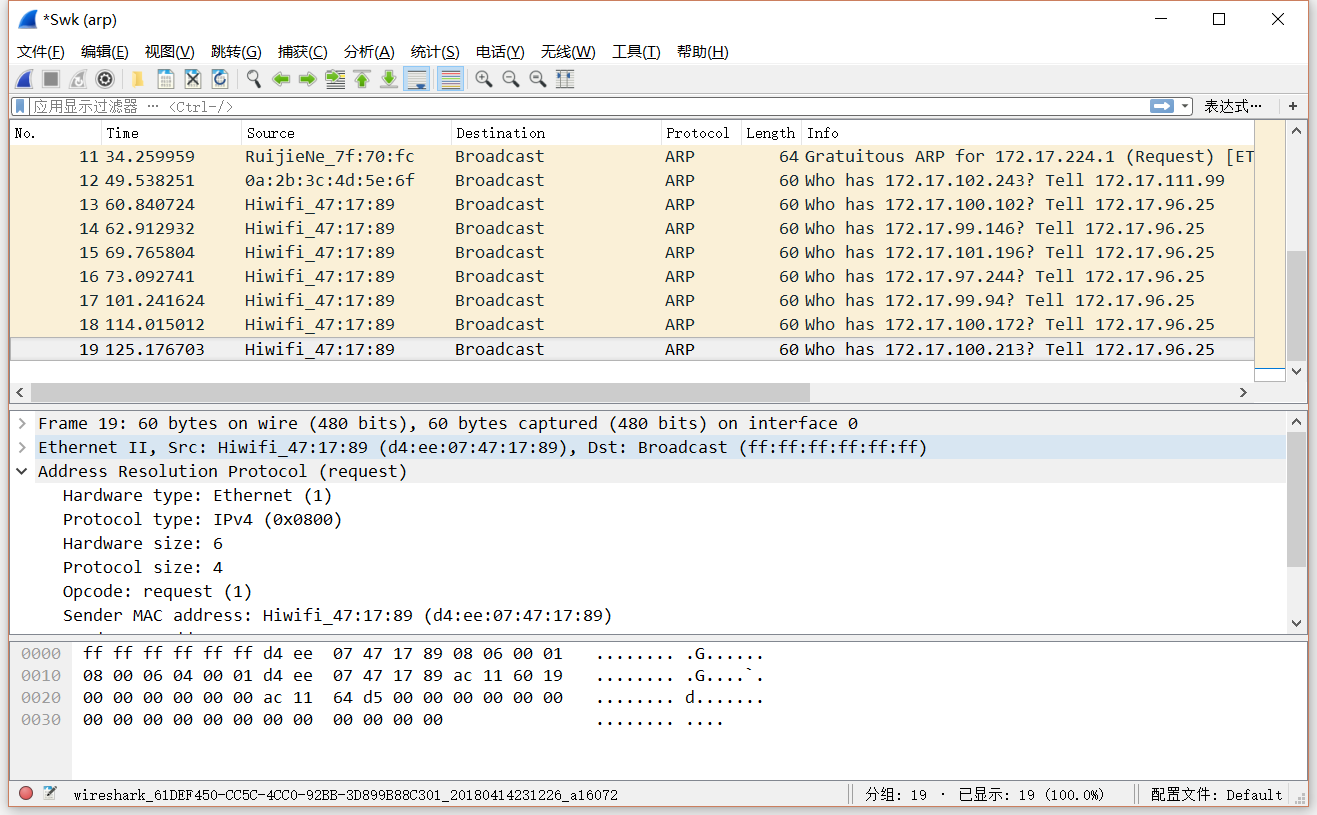


1. 在windows主机上运行Wireshark，选择本地网卡后启动抓包。为观察方便，在显示过滤器栏输入“arp”，以便只察看ARP数据。



1. 启停网络中的主机或其他网络设备，观察在Wireshark中捕获的数据包中的免费arp，分析其报文结构和内容。

- 观察到来自本机“自问自答”的免费arp。



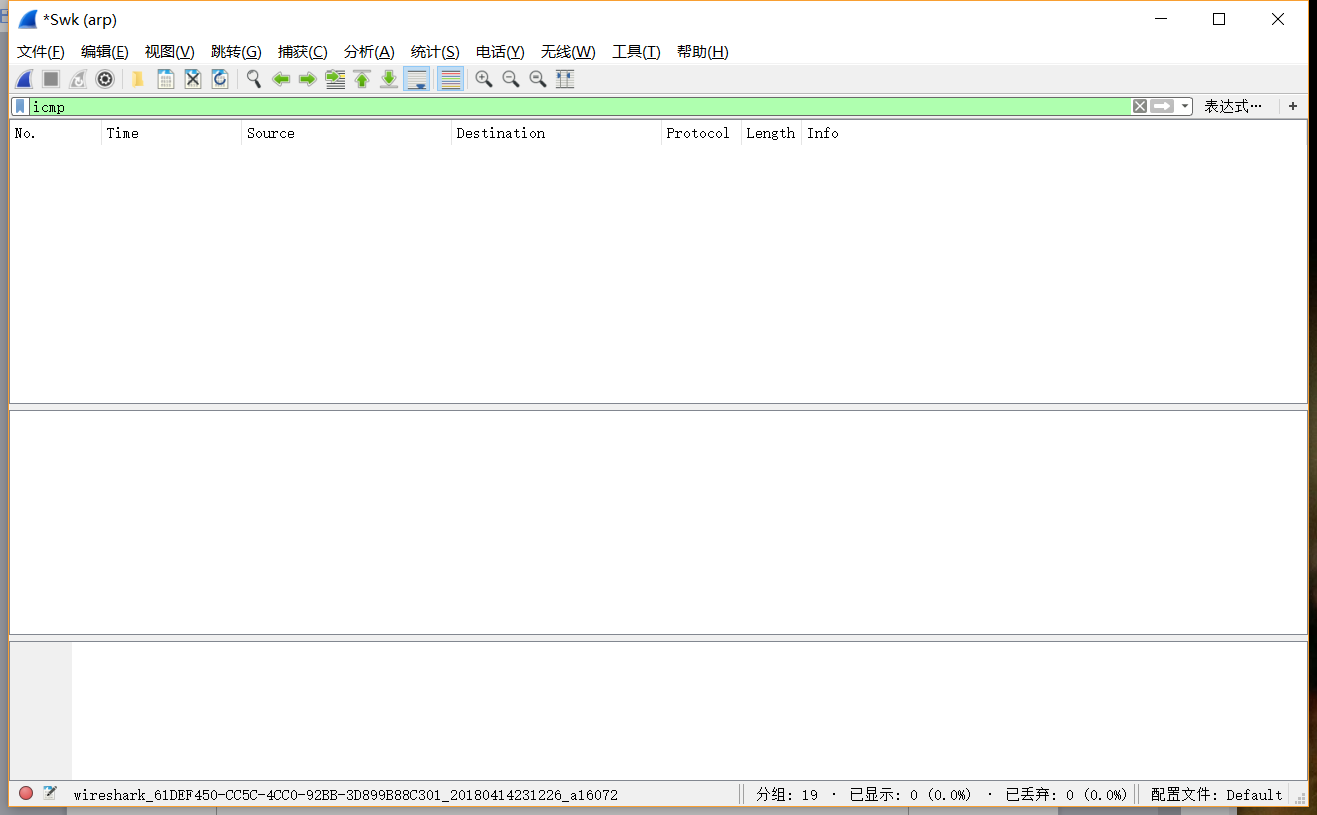
思考：各实验主机对收到的免费ARP都做了哪些处理，为什么？

由于免费arp是以广播形式发送到各个主机，所以当主机收到免费arp后，ip地址相同的主机则回应，Ip地址不同则不用理会。所以免费arp的功能是检测Ip地址冲突。

# 实验5-4 traceroute程序

# 基于ICMP的traceroute工作过程

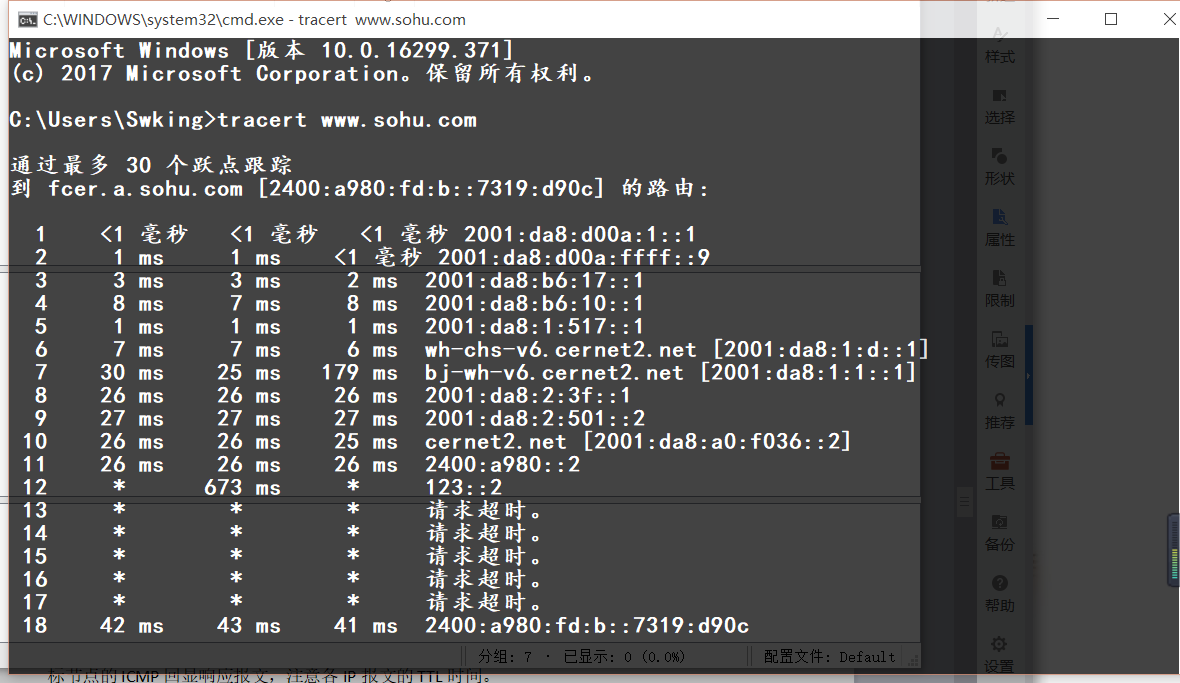
1. 在一台能够连接Internet的Windows主机上，启动Wireshark，设置过滤器为ICMP.



1. 在Windows命令行运行下列命令。

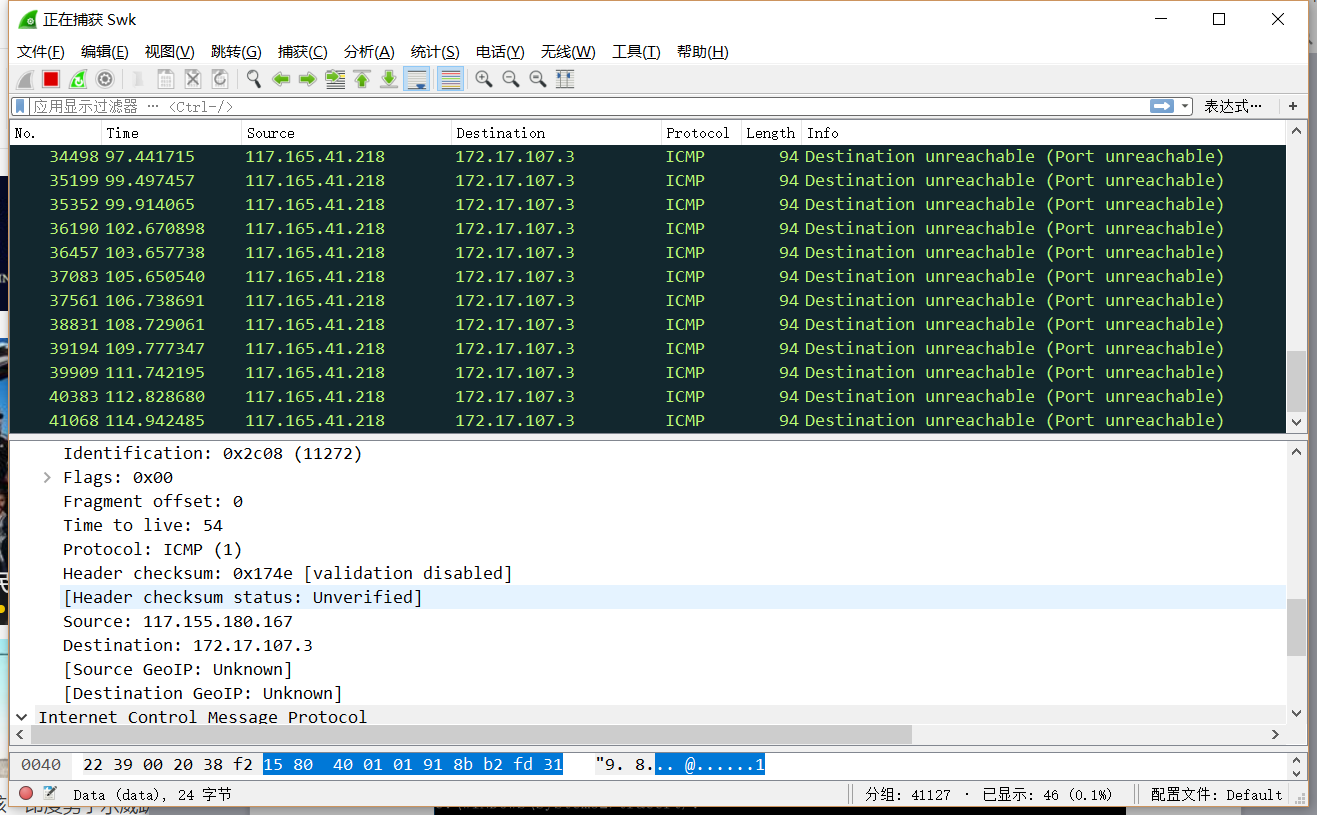
C:\>tracert [www.sohu.com](http://www.sohu.com)。观察命令执行过程中输出的跟踪跃点的内容。

- 从左到右依次表示为生存周期（每经过一个节点自增1）->三个ICMP包的返回时间->途径路由器的IP地址

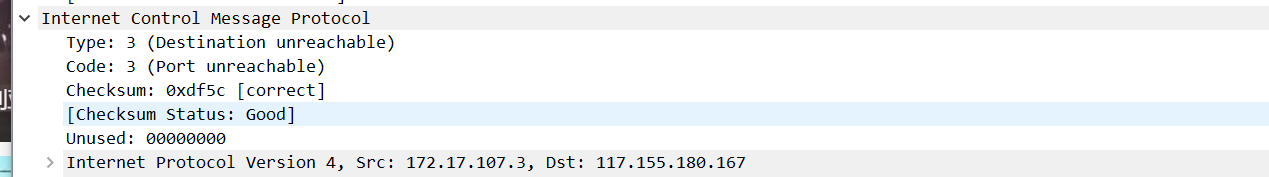


1. 对照分析捕获的tracert程序发出的ICMP回显请求报文、ICMP超时差错报文、到达目标节点的ICMP回显响应报文，注意各IP报文的TTL时间。

- 回显请求报文



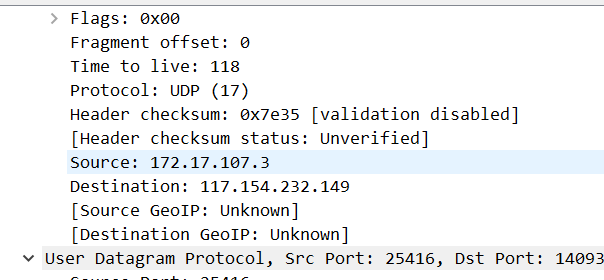
- TTL超时报文(TTL=64,TYPE=3,CODE=3)



Q:不是说ICMP TTL-expired差错报文中TTL为 1或0吗？为什么这里显示64？

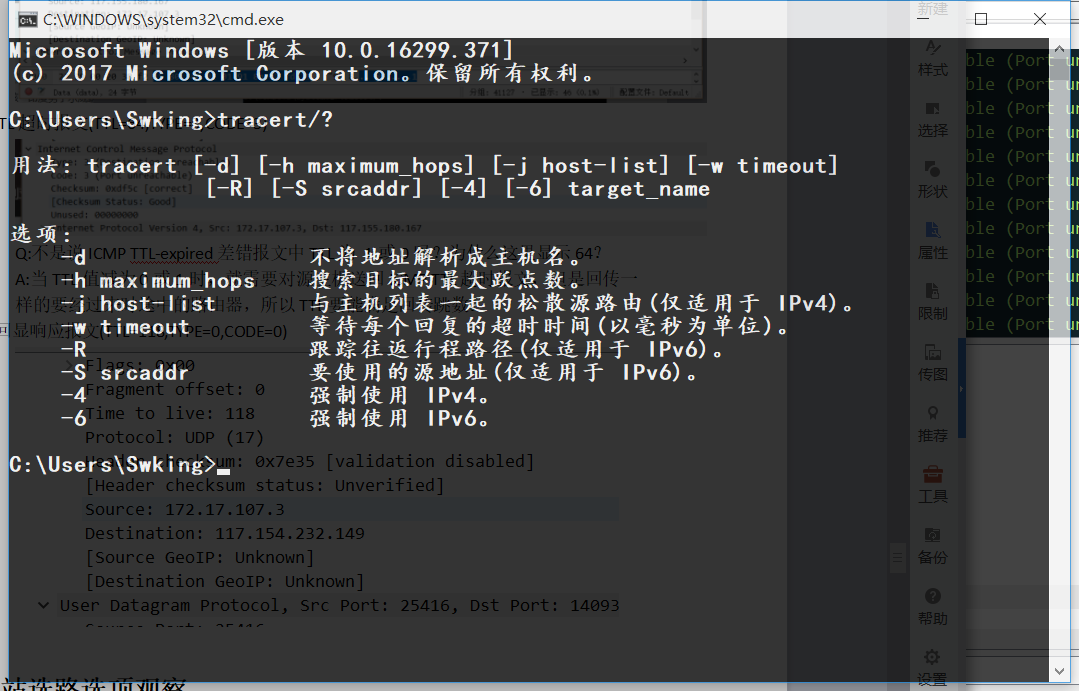
A:当TTL值减为0或1时，就需要对源主机送回ICMP TTL超时报文，但是回传一样的要经过来时途中的路由器，所以TTL要能满足回传跳数。

- 回显响应报文(TTL=118,TYPE=0,CODE=0)



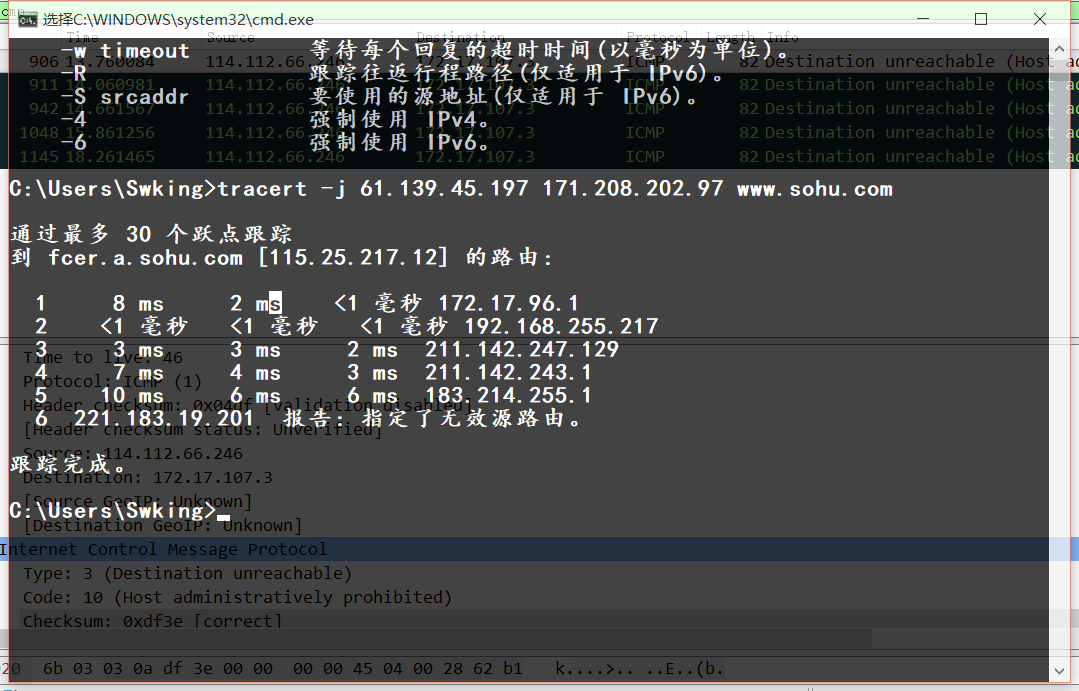
# IP源站选路选项观察

1. 执行命令tracert/?查看程序的参数选项，了解宽松的源路由的命令格式



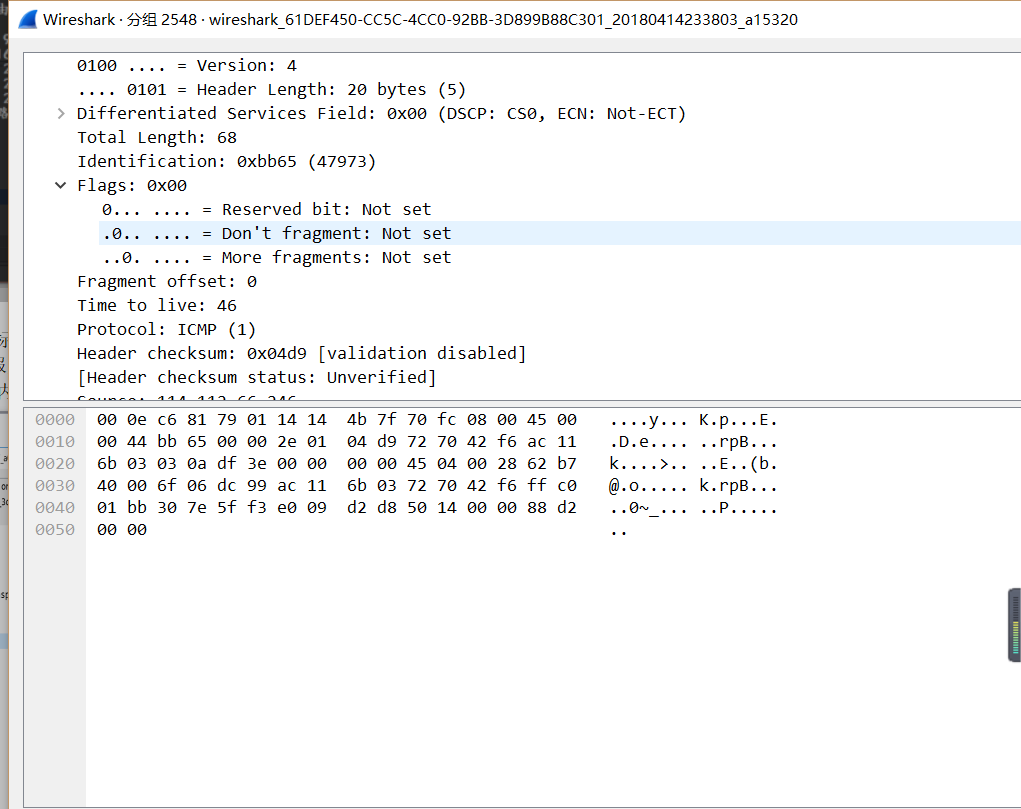
1. 接续上面的实验，在其命令输出的去往[www.sohu.com](http://www.sohu.com)的路径上，选择两个路由器地址，如61.139.45.197，171.208.202.97，作为指定的源路由（去往目的地的路径可能不唯一，以实际执行命令时得到的信息为准），执行下列命令。

C:/>tracert -j 61.139.45.197 171.208.202.97 [www.sohu.com](http://www.sohu.com)



可以看到，并没有在规定生存周期内到达目标地址，而且返回请求超时，在某些途径的节点（路由器）上，限制了类型11的ICMP报文（ICMP报文是防火墙最常见的限制） 。

1. 查看捕获的ICMP回显请求报文中IP选项的内容，记录选项里code、ptr的值，记录选项中IP地址的内容。



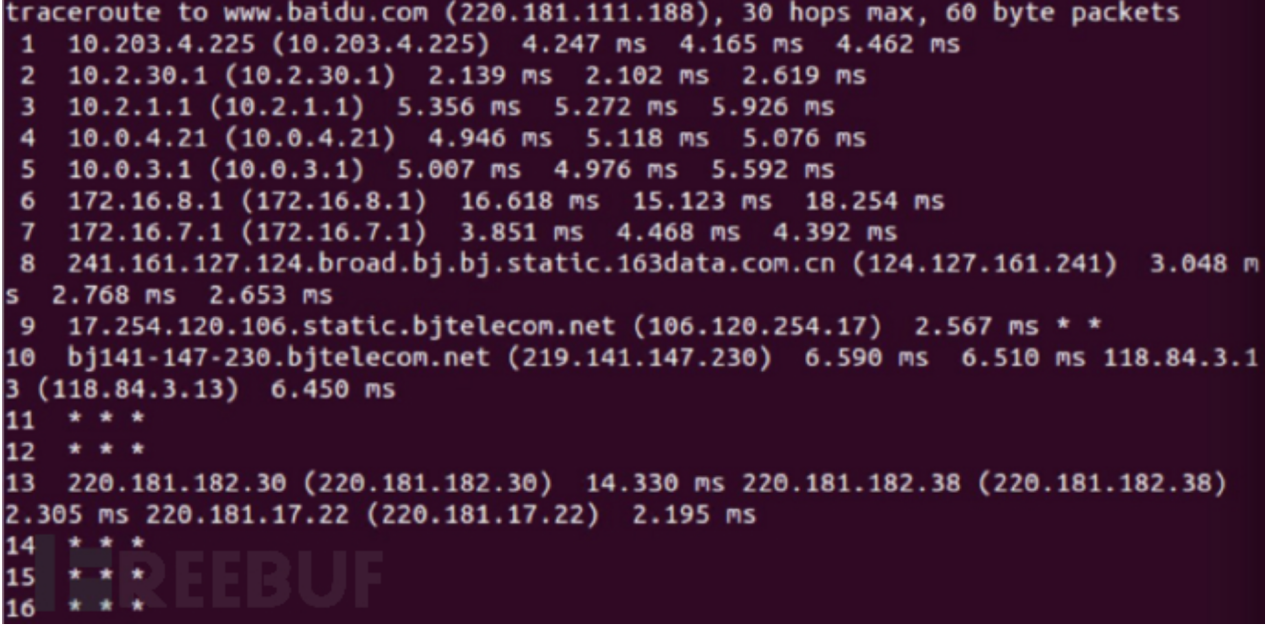
由于不少路由器对带IP源站选路选项的报文都做了限制，所以没能捕获ICMP回显响应报文。

## 思考：

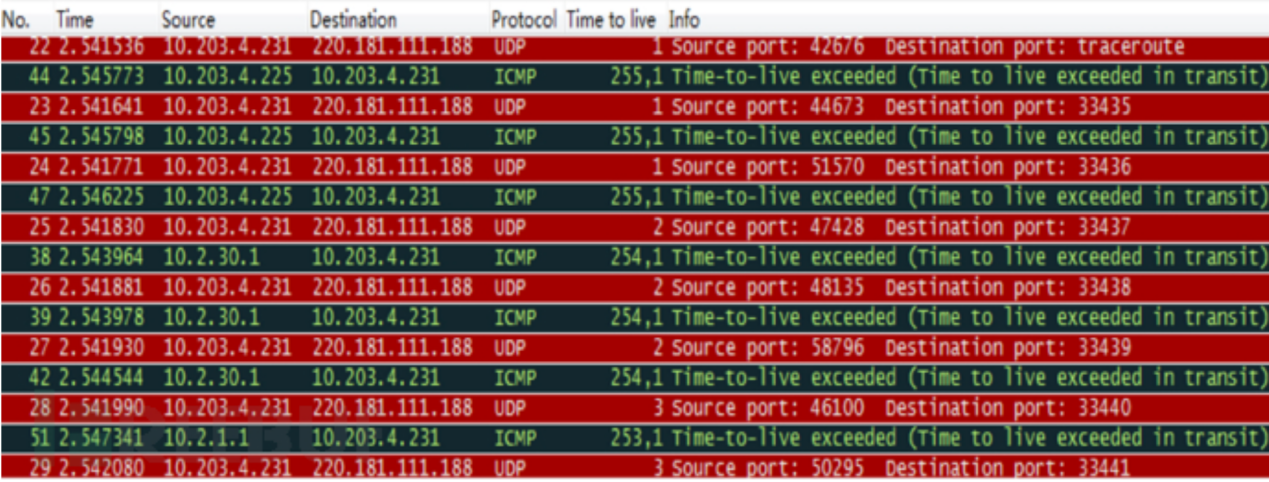
1. 如何能够观察到基于UDP的traceroute实现？(没装虚拟机，直接百度的)

Linux系统使用UDP包进行探测，目标端口号默认为33434，每次探测目标端口号加1。Traceroute故意使用了一个大于 30000 的目标端口号，以保证目标地址收到数据包后能够返回一个“端口不可达”的 ICMP 报文，于是源地址就可将端口不可达报文当作跟踪结束的标志。

- traceroute www.baidu.com



- 抓包



源地址10.203.4.244向目的地址119.75.218.70发送UDP数据包，每跳默认发送3个，TTL设置为1；数据包遇到路由器之后，被丢弃，返回Time tolive exceeded超时通知，解析出路由器IP地址10.203.4.225。源地址再发数据包，设置TTL=2，从而解析出第二跳路由10.2.30.1。同理，解析出第三跳路由10.2.1.1。与终端显示的信息相符。

1. 如何根据带有源站选路的traceroute命令的输出，画出到目的节点的拓扑路径？

