1. 实验目的
2. 局域网内相互ping对方的主机，抓取并过滤数据包，分析ip和mac地址以及抓包过程

2、学会查看和清除主机的arp缓存表，分析抓取数据包中上下行的一对包

1. 实验条件

源IP: 192.168.5.108

MAC:8c:ec:4b:cd:93:ac

目的：IP:192.168.5.122

MAC:ac:f9:70:c1:92:bd

1. 实验步骤

1、发包过程分析

1. 虚拟机通过目的ip与子网掩码相与，发现在一个网段
2. 虚拟机arp缓存表里若没有目的ip的表项，则广播arp请求包；若有则跳到（4）
3. 目的主机收到广播，发现和自己ip一样，发送arp响应包；
4. 虚拟机发送icmp请求包
5. 目的主机发送icmp响应包

2、wireshark抓包



可以看到，最开始虚拟机arp缓存里面没有192.168.5.122

（1）arp

test

第一个包源ip和mac是虚拟机，目的mac广播；

第二个包源ip和mac是目的主机，目的ip和mac是虚拟机

1. Icmp

test

第一个包源ip是虚拟机，目的ip是服务器；

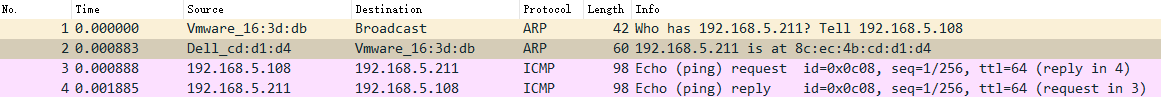
第一个包源ip是服务器，目的ip是虚拟机

3、Tcpdump:抓包

（1）抓包

tcpdump -i ens33 -ent -c 8 -s 1500 'host 192.168.5.108 and 192.168.5.132' -w ./arp1.pcap

1. 抓包结果



可以看到抓包结果和上面一样

四、结论

1、局域网ping一台主机时，若主机arp缓存表里没有目的主机的表项，则广播arp；若有，则直接发送icmp包

2、通过arp -a可以查看主机的arp缓存表，通过arp -d ip可以删除对应目的主机的ip的表项，