1. 实验目的
2. 跨网段ping一台实验室主机，分析ip和mac地址以及抓包过程
3. 删除默认路由，观察ping的现象并解释
4. 实验条件

源IP: 192.168.5.10

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

网关：192.168.4.1

目的：IP:172.21.23.5

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

网关：172.21.16.1

1. 实验步骤

1、发包过程分析

1. 主机通过目的ip与子网掩码相与，发现不在一个网段
2. 若主机arp缓存里有网关的mac，跳到（4）；否则主机在局域网进行ARP广播
3. 网关发现主机发送的目的ip和自己相同，并向主机发送arp响应
4. 主机发送icmp请求报文给主机所在的网关（源ip是主机，目的ip是服务器，源mac是主机，目的mac是网关）
5. 路由器发现目的ip不在直连网段，并根据路由表找到下一跳路由172.21.16.1
6. 172.21.16.1的arp缓存表里有服务器的表项。
7. 172.21.16.1转发icmp请求报文给主机（源ip是主机，目的ip是服务器，源mac是172.21.16.1，目的mac是服务器）
8. 服务器发送icmp响应报文给主机

2、抓包结果

主机ping服务器172.21.23.5

1. Arp（主机arp缓存表里没有网关表项，能抓到arp）

arp

第一个包源ip是本机，目的ip是网关；源mac是本机，目的mac是网关

第二个包源ip是网关，目的ip是本机；源mac是网关，目的mac是主机

1. Icmp

icmp

第一个为上行包，源ip是本机，目的ip是服务器；

第一个为下行包，源ip是服务器，目的ip是本机

服务器ping主机

1. Arp(arp缓存表里有上次转包的缓存，不用发arp包，所以抓不到)
2. icmp

test

3、删除服务器的默认路由：

route del default gw 172.21.16.1

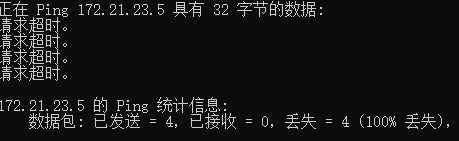
（1）服务器ping主机

test

现象：服务器ping不通主机，抓不到icmp包

原因：默认路由删除后，服务器就无法和动态路由外的网络通信，icmp包不能通过默认路由器发送出去，所以抓不到icmp包

（2）主机ping服务器



test

现象：主机ping不通服务器，能抓到请求包，抓不到响应包

原因：因为主机通过网关能够发送请求包，但是icmp包达到服务器后，由于默认路由表已经删除，所以响应包发不出去

4、通过另一台服务器登入这台服务器并添加默认路由：

route add default gw 172.21.16.1

现象：主机和服务器能相互ping通

1. 实验结论
2. 跨网段ping一台实验室服务器时，需要通过网关或者路由器。源ip和目的ip在包中不变，源mac和目的mac为局域网内的主机或者路由器
3. 删除服务器的默认路由表后，主机ping不通服务器，能抓到请求包，但是抓不到响应包；服务器ping不通主机，也抓不到请求包。添加默认路由表后可以相互ping通