**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 数据链路层和网络层协议分析 指导教师 潘冰

实验项目编号 实验项目类型 实验地点 计算机网络实验室

学生姓名 赖智聪 学号 2019051118

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 11 月 9 日 上 午～ 11 月 9 日 上 午

|  |
| --- |
| **一、实验目的** |
| * 理解链路层、网络层主要协议格式，以及协议的工作原理 * 理解网关和子网掩码概念 * 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程 * 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。 |

|  |
| --- |
| **二、实验环境** |
| 计算机2台，交换机一台。 |
| **三、实验内容**   1. 用嗅探器捕获数据包。 2. 分析以太网帧、ARP协议、IP协议、ICMP协议格式 3. 分析PING、TRACERT、ARP命令的工作过程 4. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。   本机ip    Mac：    一．ARP协议分析    断网一分钟后再联网，能够捕获相应ARP报文：  第一个ARP包：该包是广播发送的ARP请求分组，想要获得本机的IP地址。    第二个ARP包：如下图所示，可见该包是ARP响应分组，发送者是本机，目的地是之前请求该地址的路由器的地址。同时可见两个ARP包的协议字段使用的都是IPv4。    随后再次查看arp高速缓存，可见已经加入了本机的ip地址及mac地址：    随后再次ping，没有ARP报文，而隔了5分钟再ping，则有。  二．IP协议及ICMP协议分析  使用ping向另一台主机发送检测报文，捕获得到的数据包如图所示：  因为使用了过滤，只显示请求时的报文：可见address字段是对方的mac地址，source字段是本机的mac地址，类型是IPv4。    对IP数据报文的分析：  IP数据包如下图所示，  最开始的45表示版本是IPv4，首部长度是5字节，对应IP首部的版本和首部长度；  区分服务字段：对应数值00，因为一般情况下不使用该字段；  总长度：00 3c表示该报文的总长度；  标识字段：bd b8为该报文的标识；  标志字段及片偏移字段：00 00；  生存时间：40；表示还可以通过64个路由器；  协议字段：01，表示使用ICMP服务，这也和该报文是ping得到的报文相对应；  首部检验和：77 13；  源地址：c0 a8 2b f3；  目的地址：0a a0 4e ba； |
| 接下来是ICMP报文分析：  报文如下图所示。其类型是08，表示是询问报文，随后的代码字段为00，接下来是检验和4d 2a，随后的00 01 00 31取决于ICMP报文的类型。剩下的部分即是ping是所发送的数据。 |
|  |
| 当指定了长度时（-l 2000），如下图所示：  可见数据包被分片，并且flags字段的more fragment字段是1： |
| 使用tracert：    不可达的：由type字段为3，即表示不可达。    成功到达的：由类型为8可推知为回送回答。      类型为11，表示超时了。    Tracert工作原理为：先发送一个TTL为1的数据报，路由器收到该数据报后TTL的值为0，会发送一个ICMP报文给源主机，从而源主机知道了路由信息。随后源主机依次增加发送报文的TTL，从而得知相应的路由信息。 |
|  |

**四、实验及分析**

思考题

1.当ARP高速缓存里存在相应IP地址项时，则无法捕获ARP报文，因为此时并没有发送ARP报文，而是直接从ARP高速缓存里取得IP地址对应的MAC地址；而当高速缓存里没有IP地址时，则会发送ARP报文。

2．因为该地址定向到本机，没有发送ICMP报文；不能。

3.超时是因为对方关机，或自己和对方不在同一网段，通过路由也找不到对方，或者对方设置了ICMP数据包过滤，或者设置了错误的IP地址。目的主机不可达是因为自己和对方不在同一网段，而自己也没有设置默认路由，或者网线出故障。

5.使用ping可以连通，因为两台主机在同一网段；A向B发消息时，因为通过掩码运算后和B不在同一网段，所以捕获不到ICMP报文；B向 A发送PING时，B的子网掩码和主机A的IP地址做相与会发现A在B的网段里面，所以B会向A发送请求报文，但是当B向A发应答报文时，B的IP地址与子网掩码运算后发现B和A不在一个网段，因此不会发送应答报文。

**五、实验总结**

通过实验，更好地了解了IP协议的原理，以及ARP，ICMP协议的原理及应用。