

武汉大学国家网络安全学院教学实验报告

课程名称	网络程序设计			成 绩		教师签名	
实验名称	数据链路层数据操作及 ARP			实验序号		实验日期	
姓 名		学号		专 业		年级-班	
<p>一、实验目的及实验内容</p> <p>（本次实验所涉及并要求掌握的知识；实验内容；必要的原理分析）</p> <p>实验目的：熟悉数据链路层数据的获取方法，能够从数据链路层获取网络层、传输层和应用层的数据，掌握 ARP 协议</p>							<p>小题分：</p>
<p>二、实验环境及实验步骤</p> <p>（本次实验所使用的器件、仪器设备等的情况；具体的实验步骤）</p> <p>实验环境：Ubuntu18.04LTS</p> <p>实验步骤：编写 arp 程序并验证</p>							<p>小题分：</p>
<p>三、实验过程分析</p> <p>（详细记录实验过程中发生的故障和问题，进行故障分析，说明故障排除的过程及方法。根据具体实验，记录、整理相应的数据表格、绘制曲线、波形等）</p>							<p>小题分：</p>
<p>1、arp 封装格式</p> <pre> 17 18 struct arppacket 19 { 20 struct arphdr ar_head; 21 unsigned char ar_sha[ETH_ALEN]; 22 struct in_addr ar_sip; 23 unsigned char ar_tha[ETH_ALEN]; 24 struct in_addr ar_tip; 25 }__attribute__((packed)); 26 </pre> <p>注意：要禁用 gcc 的结构体对齐</p> <p>2、遍历网卡，通过 ip&mask 获取正确网卡 通过 SIOCGIFADDR 获取网卡 ip 地址</p>							

```

ifrPtr = ((struct ifreq*)buf) + i;
if(ioctl(fd, SIOCGIFADDR, ifrPtr) == -1)
{
    perror("get ip address error\n");
    exit(-1);
}
netaddr = ((struct sockaddr_in*)&(ifrPtr->ifr_addr))->sin_addr;

```

通过 SIOCGIFNETMASK 获取网卡掩码

```

if(ioctl(fd, SIOCGIFNETMASK, ifrPtr) == -1)
{
    perror("get netmask error\n");
    exit(-1);
}
netmask = ((struct sockaddr_in*)&(ifrPtr->ifr_netmask))->sin_addr;

```

找到正确网卡之后，填充网卡信息

```

if((pingaddr.s_addr & netmask.s_addr) == (netaddr.s_addr & netmask.s_addr))
{
    hwaddr.sll_family = PF_PACKET;
    hwaddr.sll_protocol = htons(ETH_P_ARP);
    hwaddr.sll_hatype = ARPHRD_ETHER;
    hwaddr.sll_pkttype = PACKET_OTHERHOST;
    hwaddr.sll_halen = ETH_ALEN;

    if(ioctl(fd, SIOCGIFINDEX, ifrPtr) == -1)
    {
        perror("get net interface index error\n");
        exit(-1);
    }
    hwaddr.sll_ifindex = ifrPtr->ifr_ifindex;

    if(ioctl(fd, SIOCGIFHWADDR, ifrPtr) == -1)
    {
        perror("get net interface hwaddr error\n");
        exit(-1);
    }
    memcpy(hwaddr.sll_addr, ifrPtr->ifr_hwaddr.sa_data, ETH_ALEN);

    flag = 1;
    break;
}

```

其中 SIOCGHWADDR 获取网卡 MAC 地址

3、构建发送的 arp 报文

```
// send arp
char ef[ETH_FRAME_LEN];
struct ethhdr *p_eth = (struct ethhdr*)ef;
memset(p_eth->h_dest, 0xff, ETH_ALEN);
memcpy(p_eth->h_source, hwaddr.sll_addr, ETH_ALEN);
p_eth->h_proto = htons(ETH_P_ARP);

struct arppacket *p_arp = (struct arppacket*)(ef + ETH_HLEN);
p_arp->ar_head.ar_hrd = htons(ARPHRD_ETHER);
p_arp->ar_head.ar_pro = htons(ETH_P_IP);
p_arp->ar_head.ar_hln = ETH_ALEN;
p_arp->ar_head.ar_pln = 4;
p_arp->ar_head.ar_op = htons(ARPOP_REQUEST);
memcpy(p_arp->ar_sha, hwaddr.sll_addr, ETH_ALEN);
p_arp->ar_sip = netaddr;
memset(p_arp->ar_tha, 0, ETH_ALEN);
p_arp->ar_tip = pingaddr;
```

4、绑定网卡，发送 arp 报文，接收回送报文

```
if(bind(fd, (struct sockaddr*)&hwaddr, sizeof(struct sockaddr_ll)) == -1)
{
    perror("bind network error\n");
    exit(-1);
}

write(fd, ef, 60);
while(1)
{
    read(fd, ef, sizeof(ef));
    struct arppacket *recv_arp = (struct arppacket*)(ef+ETH_HLEN);
    if(recv_arp->ar_tip.s_addr == netaddr.s_addr)
    {
        printMac("mac: ", recv_arp->ar_sha);
        break;
    }
}
return 0;
```

5、运行截图

```
hs@hs-X556UQK: ~/图片/网络程序设计/exper8
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
hs@hs-X556UQK:~/图片/网络程序设计/exper8$ make
gcc -o arp arp.c
hs@hs-X556UQK:~/图片/网络程序设计/exper8$ sudo ./arp 192.168.100.254
[sudo] hs 的密码:
mac: b8-4d-ee-0d-42-08
hs@hs-X556UQK:~/图片/网络程序设计/exper8$ arp 192.168.100.254
地址          类型      硬件地址      标志  Mask      接口
_gateway      ether     b8:4d:ee:0d:42:08  C      接口
_gateway      ether     b8:4d:ee:0d:42:08  C      enp2s0
hs@hs-X556UQK:~/图片/网络程序设计/exper8$
```

<p>四、实验结果总结</p> <p>（对实验结果进行分析，完成思考题目，总结实验的新的体会，并提出实验的改进意见）</p>	<p>小题分：</p>
<p>1、创建原始套接字的方式发生了更改</p> <pre>// create sock_packet socket int fd = socket(PF_PACKET, SOCK_RAW, htonl(ETH_P_ARP)); if(fd == -1) { perror("create socket error\n"); exit(-1); }</pre> <p>2、结构体禁用对齐</p> <pre>struct arppacket { struct arphdr ar_head; unsigned char ar_sha[ETH_ALEN]; struct in_addr ar_sip; unsigned char ar_tha[ETH_ALEN]; struct in_addr ar_tip; }__attribute__((packed));</pre> <p>3、sockaddr 可以转换成 sockaddr_in，但是不可以转换成 sockaddr_ll sockaddr 的数据部分前 6 字节对于 MAC</p> <pre>if(ioctl(fd, SIOCGIFHWADDR, ifrPtr) == -1) { perror("get net interface hwaddr error\n"); exit(-1); } memcpy(hwaddr.sll_addr, ifrPtr->ifr_hwaddr.sa_data, ETH_ALEN);</pre>	