

廈門大學



信息学院软件工程系

《计算机网络》实验报告

题 目 实验三 捕获并分析帧和 IP 报文

班 级 软件工程 2018 级 B 班

姓 名 彭书浩

学 号 24320182203251

实验时间 2020 年 3 月 11 日

2020 年 3 月 11 日

1 实验目的

1、捕获并分析以太网的帧，获取目标与源网卡的 MAC 地址；

2、获取本机地址

-IPCONFIG.EXE

-通过 Winsock 的 GetAddress 命令

3、获取远端 MAC 地址

-ARP

-WinPCAP

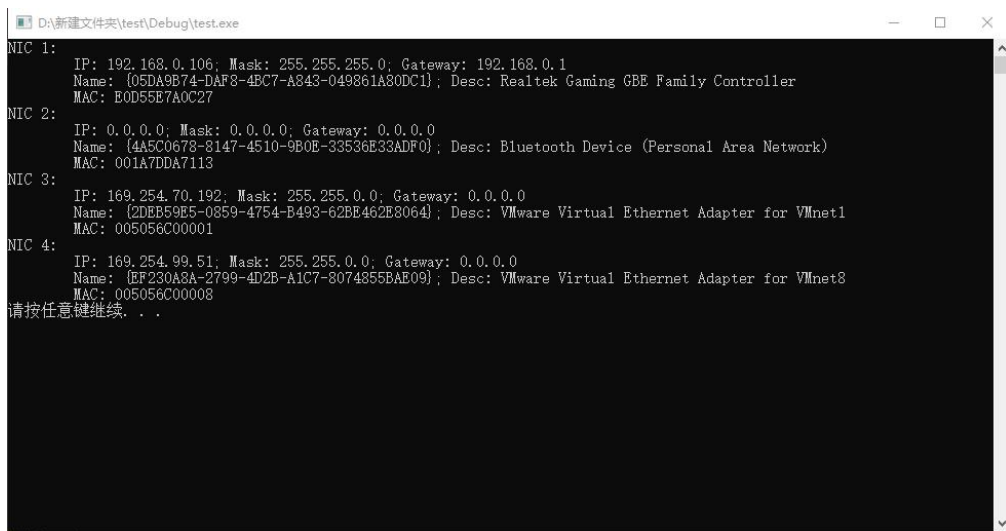
2 实验环境

Windows 10 操作系统

-WinPCAP；WireShark；科来数据包播放器

3 实验结果

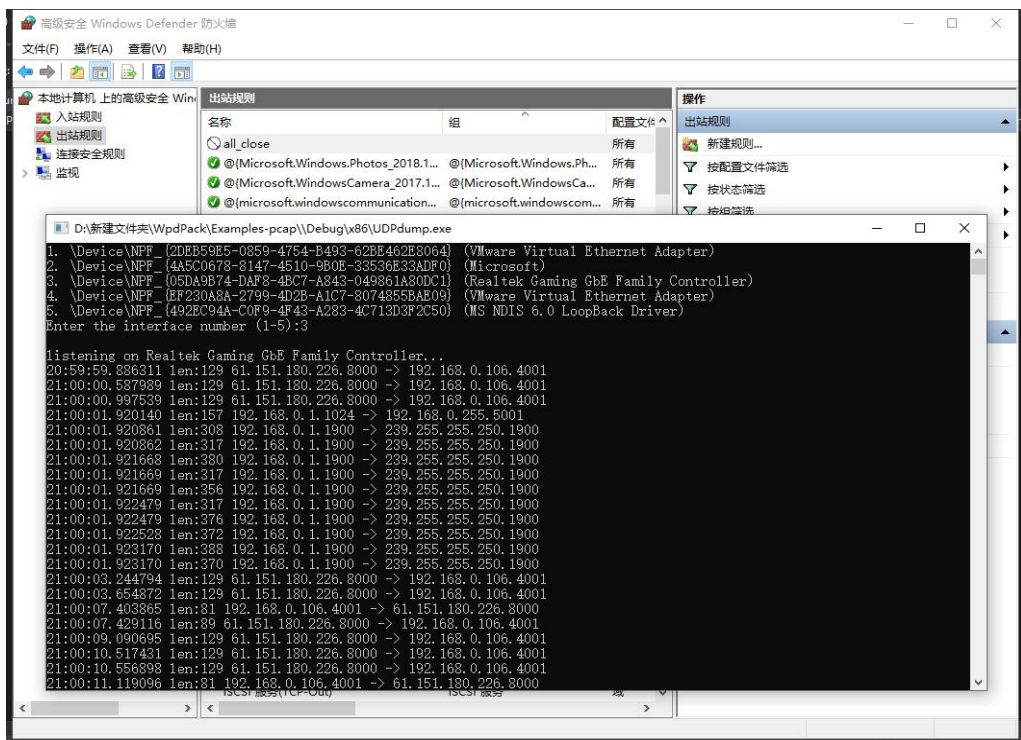
1、本机的网卡信息与 MAC 地址



```
D:\新建文件夹\test\Debug\test.exe
NIC 1:
  IP: 192.168.0.106; Mask: 255.255.255.0; Gateway: 192.168.0.1
  Name: {05DA9B74-DAF8-4BC7-A843-049861A80DC1}; Desc: Realtek Gaming GBE Family Controller
  MAC: E0D55E7A0C27
NIC 2:
  IP: 0.0.0.0; Mask: 0.0.0.0; Gateway: 0.0.0.0
  Name: {4A5C0678-8147-4510-9B0E-33536E33ADF0}; Desc: Bluetooth Device (Personal Area Network)
  MAC: 001A7DDA7113
NIC 3:
  IP: 169.254.70.192; Mask: 255.255.0.0; Gateway: 0.0.0.0
  Name: {2DEB59E5-0859-4754-B493-62BE462E8064}; Desc: VMware Virtual Ethernet Adapter for VMnet1
  MAC: 005056C00001
NIC 4:
  IP: 169.254.99.51; Mask: 255.255.0.0; Gateway: 0.0.0.0
  Name: {BF230A8A-2799-4D2B-A1C7-8074855BAE09}; Desc: VMware Virtual Ethernet Adapter for VMnet8
  MAC: 005056C00008
请按任意键继续. . .
```

2、测试 wincap 源程序的报文接收功能。

(由于本机路由器关不了 Upnp 协议, 故即使改变网络出站规则, 仍会自动发送包)



每隔1分钟左右, 路由器(192.168.1.1)就会向239.255.255.250发包:

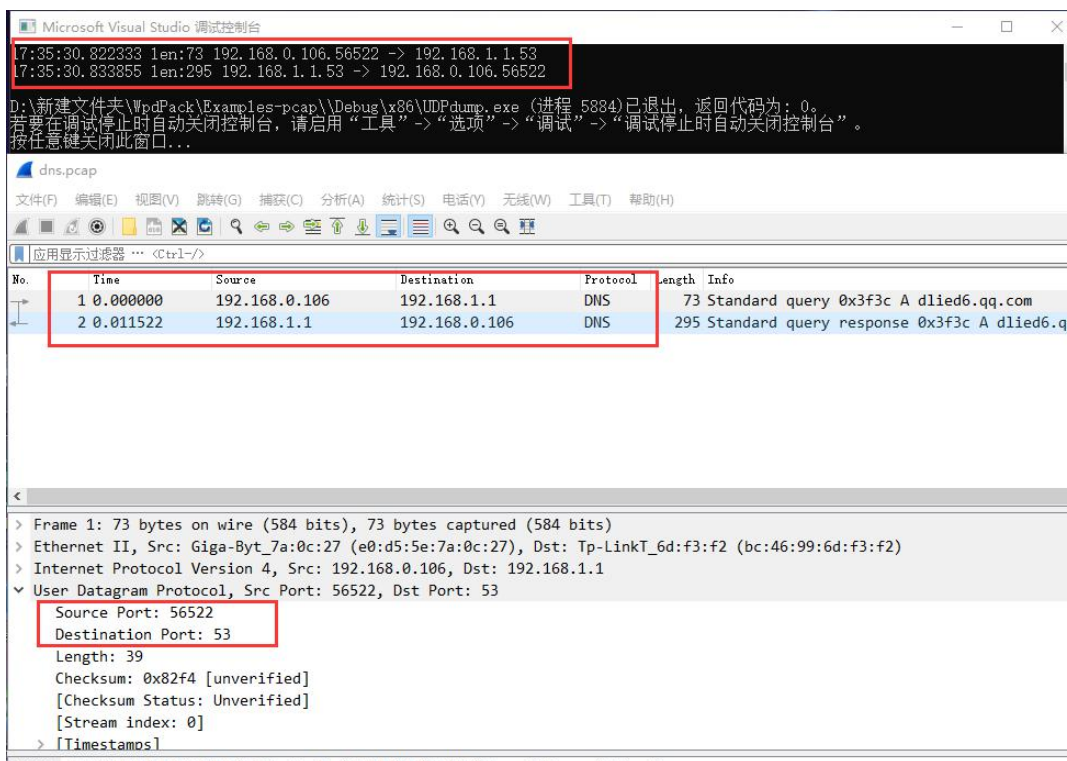
9615 995.983464000 192.168.1.1 239.255.255.250 SSDP 324 NOTIFY * HTTP/1.1

原因及解决办法:

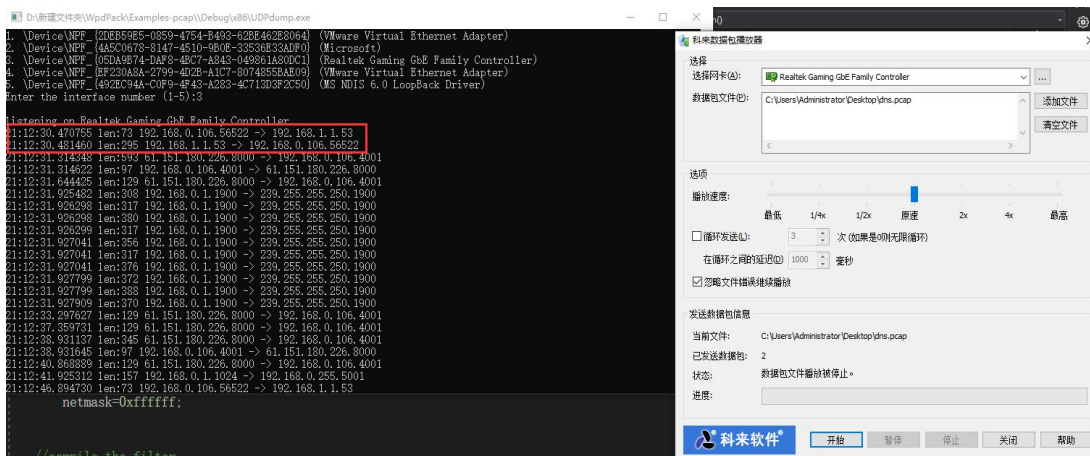
路由器上开了UPnP服务, 而这个服务会用SSDP (简单服务发现协议) 就是用239.255.255.250的多播地址端口1900来发现UPnP服务, 局域网内某台电脑上如果有UPnP服务, 每隔一段时间这台机器就会向该多播地址宣告服务在网络上可取, 而发送的方式就是基于UDP的HTTP多播方式, 关掉路由上的UPnP服务就没了。

该设置一般在路由器管理界面: 转发规则/UPnP设置。

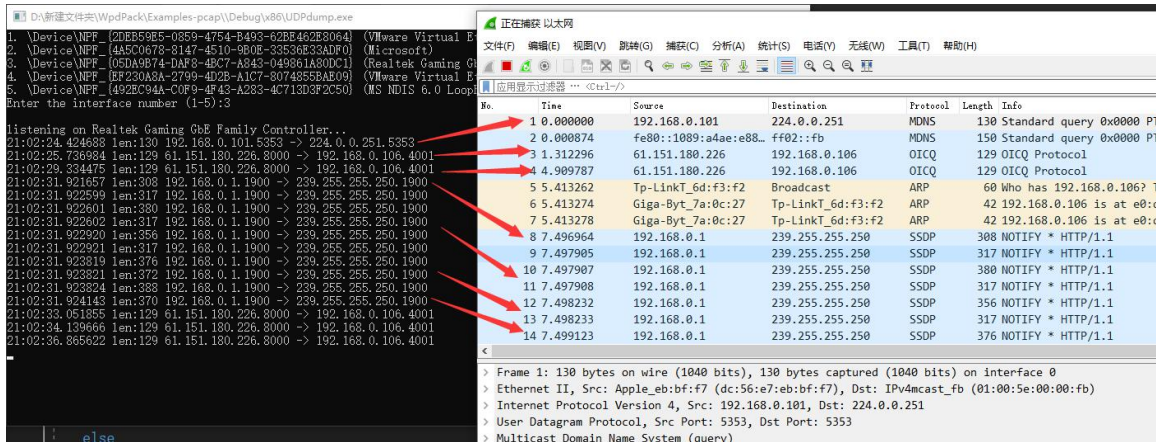
3、WireShark 生成 pcap 文件由程序读取。



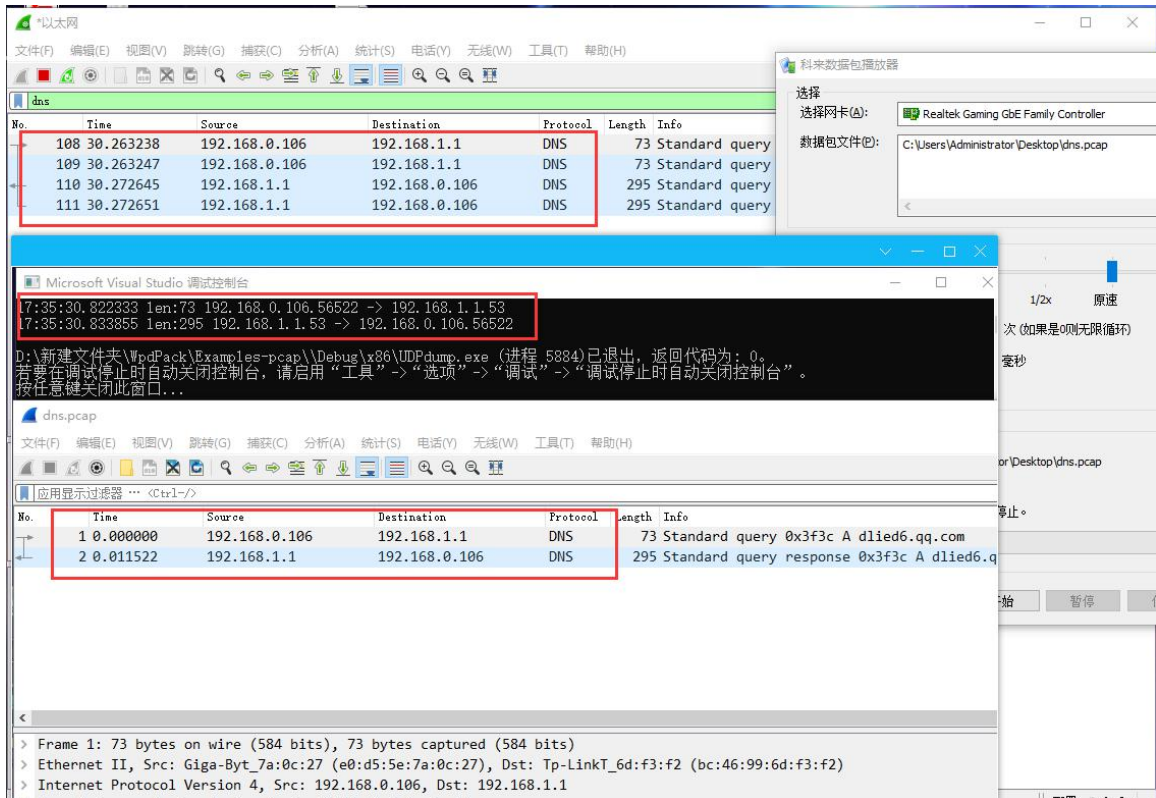
4、用科来播放器重发 pcap 文件, 由程序网卡接收。



5、出于 UPnp 服务的自动发送报文机制, 测试程序与 wireshark 接收的数据是一致的



6、使用 Wireshark 接收科来播放器发送的 pcap 报文，得到四条报文。



7、套用课件里的代码改写程序，输出结果不合预期。


```

D:\新建文件夹\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. \Device\NPF_{2DEB59E5-0859-4754-B493-62BE462E8064} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{4A5C0678-8147-4510-9B0E-33536E33ADF0} (Microsoft)
3. \Device\NPF_{05DA9B74-DAF8-4BC7-A843-049861A80DC1} (Realtek Gaming GbE Family Controller)
4. \Device\NPF_{EF230A8A-2799-4D2B-A1C7-8074855BAE09} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{492EC94A-C0F9-4F43-A283-4C713D3F2C50} (MS NDIS 6.0 LoopBack Driver)
Enter the interface number (1-5):3

listening on Realtek Gaming GbE Family Controller...
21:35:15.548768 len:73 BC 46 99 6D F3 F2 E0 D5 5E 7A 0C 27 08 00 45 00
00 3B 1B 72 00 00 80 11 00 00 C0 A8 00 6A C0 A8
01 01 DC CA 00 35 00 27 82 F4 3F 3C 01 00 00 01
00 00 00 00 00 00 64 6C 69 65 64 36 02

mac_header:
  dest_addr: BC 46 99 6D F3 F2
  src_addr: E0 D5 5E 7A 0C 27
  type: 404E

ip_header:
  ver_ihl : 45
  tos : 00
  tlen : 003B
  identification: 1B72
  flags_fo : 0000
  ttl : 80
  proto : 11
  crc : 0000
  op_pad : 00006564
  saddr: : 6A00A8C0 101A8C0 3500CADC F4822700 1778428096.16885952.889244380.-192796928.
  daddr: : 13C3F 100 00 696C6406 80959.256.0.1768711174.

21:35:15.559189 len:295 E0 D5 5E 7A 0C 27 BC 46 99 6D F3 F2 08 00 45 00
01 19 F6 4E 40 00 3F 11 C1 C9 C0 A8 01 01 C0 A8

```

8、根据错误输出结果，重读课件代码与源程序代码功能，对代码进行重写与修正，得到正确结果。

```

D:\新建文件夹\WpdPack\Examples-pcap\Debug\x86\UDPDump.exe
1. \Device\NPF_{2DEB59E5-0859-4754-B493-62BE462E8064} (VMware Virtual Ethernet Adapter)
2. \Device\NPF_{4A5C0678-8147-4510-9B0E-33536E33ADF0} (Microsoft)
3. \Device\NPF_{05DA9B74-DAF8-4BC7-A843-049861A80DC1} (Realtek Gaming GbE Family Controller)
4. \Device\NPF_{EF230A8A-2799-4D2B-A1C7-8074855BAE09} (VMware Virtual Ethernet Adapter)
5. \Device\NPF_{492EC94A-C0F9-4F43-A283-4C713D3F2C50} (MS NDIS 6.0 LoopBack Driver)
Enter the interface number (1-5):3

listening on Realtek Gaming GbE Family Controller...
22:34:59.886223 len:73
BC 46 99 6D F3 F2 E0 D5 5E 7A 0C 27 08 00 45 00
00 3B 1B 72 00 00 80 11 00 00 C0 A8 00 6A C0 A8
01 01 DC CA 00 35

mac_header:
  dest_addr: BC 46 99 6D F3 F2
  src_addr: E0 D5 5E 7A 0C 27
  type: 0800

ip_header:
  ver_ihl : 45
  tos : 00
  tlen : 003B
  identification: 1B72
  flags_fo : 0000
  ttl : 80
  proto : 11
  crc : 0000
  op_pad : DCC80035
  saddr: : C0 A8 00 6A 192.168.0.106.
  daddr: : C0 A8 01 01 192.168.1.1.

22:34:59.896142 len:295
E0 D5 5E 7A 0C 27 BC 46 99 6D F3 F2 08 00 45 00

```

4 实验总结

1、代码中采用了一个 `ntohs()` 函数，用于 16 进制数据的输出。由于数据的储存方式是字节大端序位小端序，故用此函数以原格式输出数据。

2、即使是防火墙设置了对所有程序的阻止连接，计算机仍能够和外界进行信息交换。（QQ 在规则启用前便登入未退出，规则启用后虽不能进入网站，但还是能够与 QQ 好友接收与发送消息，但是不能接受与发送图片。）

3、蓝牙适配器也是一种网卡，能被程序识别。但是使用科来播放器给蓝牙适配器发送 pcap 报文，蓝牙适配器不会接收到。

4、接收到的报文数据实际上与 mac 地址和 ip 地址等信息是一一对应的；通过对接收到的报文进行解析可以得到发送方与接收方的各种信息。