课程讲义六+实验六：

ARP和ICMP协议分析

卢美莲

北京邮电大学

计算机学院（国家示范性软件学院）

网络体系结构中心

mllu@bupt.edu.cn

主要内容

- ARP协议原理
- ICMP协议原理
- Wireshark协议分析实验

ARP协议概述

- ARP（Address Resolution Protocol，地址解析协议）是TCP/IP协议栈中网络层的一个协议
  - 用于将IP地址转换为数据链路层的物理地址或硬件地址
  - 主要应用在以太网中
- IP数据包常通过以太网发送，但是以太网设备并不识别32位的IP地址，它们是以48位以太网地址传输以太网数据包。因此，必须把IP目的地址转换成以太网目的地址
- 以太网中一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？
  - 就是通过ARP获得的
  - ARP用于将网络中的目的IP地址解析为目的硬件地址（MAC地址），以保证通信的顺利进行

ARP协议的报头结构

ARP和RARP使用相同的报头结构

硬件类型		协议类型
硬件地址长度	协议地址长度	操作类型
源硬件地址（第0—3字节）		
源硬件地址（第4—5字节）		源协议地址（第0—1字节）
源协议地址（第2—3字节）		目标硬件地址（第0—1字节）
目标硬件地址（第2—5字节）		
目标协议地址（第0—3字节）		

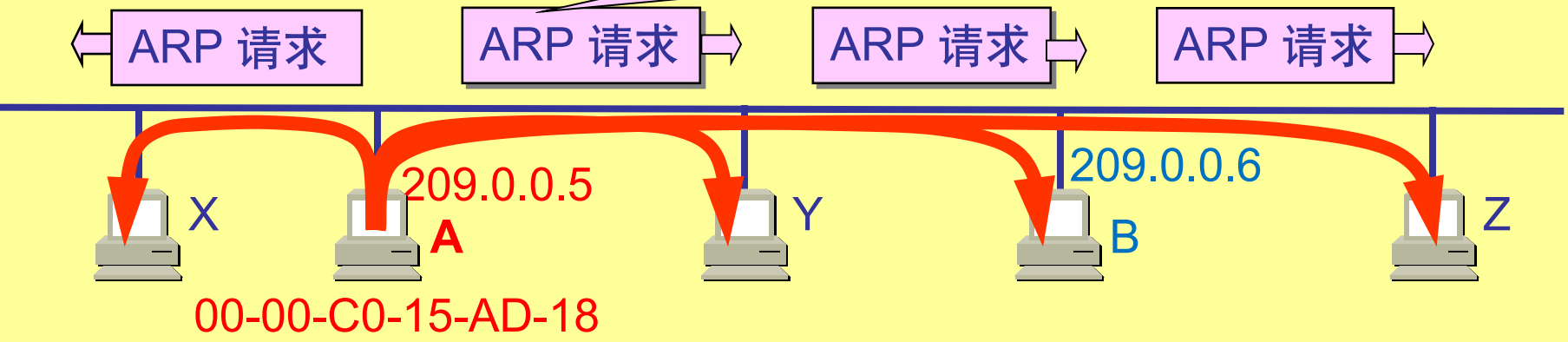
- 硬件类型：发送方想知道的硬件接口类型，以太网的值为0x0001
- 协议类型：发送方提供的高层协议类型，IP协议为0x0800
- 硬件地址长度、协议地址长度：ARP可以在任意硬件和任意高层协议的网络中使用
- 操作类型：表示该报文的类型，ARP请求为1，ARP响应为2，RAPP请求为3，RARP响应为4
- 源硬件地址、目的硬件地址：源主机和目的主机的硬件地址，如MAC地址
- 源协议地址、目的协议地址：源主机和目的主机的高层协议地址，如IP地址

ARP工作原理

1. 每台主机都会在自己的ARP缓冲区 (ARP Cache)中建立一个 ARP列表，记录表示IP地址和MAC地址的对应关系
2. 当源主机需要将一个数据包要发送到目的主机时，会首先检查自己的ARP列表中是否存在该IP地址对应的MAC地址。如果有，就直接将数据包发送到这个MAC地址；如果没有，就向本地网段发起一个ARP请求的广播包，查询此目的主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、硬件地址、以及目的主机的IP地址
3. 本地网络中所有的主机收到这个ARP请求后，会检查数据包中的目的IP地址是否和自己的IP地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的MAC地址和IP地址添加到自己的ARP列表中，如果ARP表中已经存在该IP的信息，则将其覆盖，然后给源主机发送一个ARP响应包，告诉对方自己的MAC地址
4. 源主机收到这个ARP响应包后，将得到的目的主机的IP地址和MAC地址添加到自己的ARP列表中，并利用此信息开始数据的传输。如果源主机一直没有收到ARP响应数据包，表示ARP查询失败

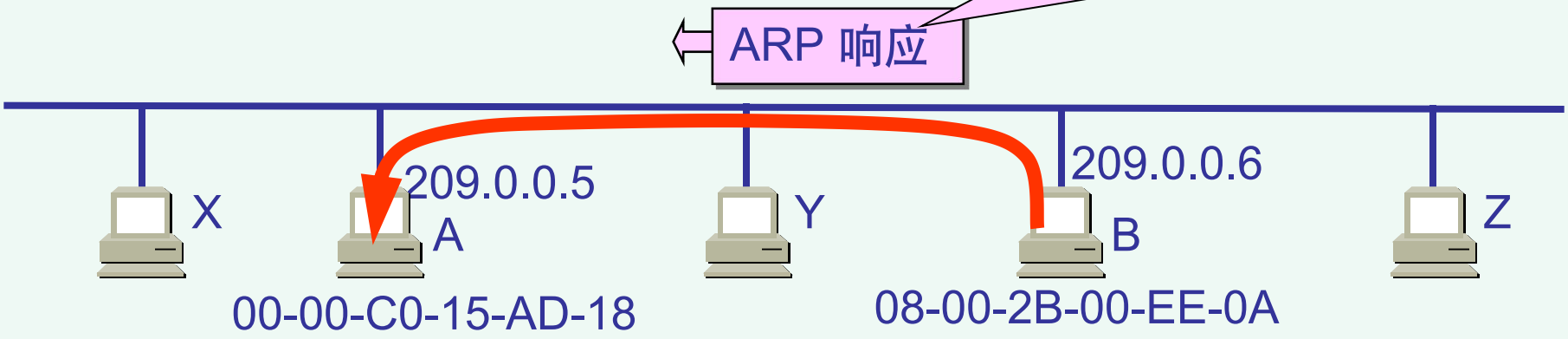
主机 A 广播发送
ARP 请求分组

我的IP地址是 209.0.0.5，硬件地址是 00-00-C0-15-AD-18
我想知道IP地址为 209.0.0.6 的主机的硬件地址



主机 B 向 A 发送
ARP 响应分组

我的IP地址是 209.0.0.6
硬件地址是 08-00-2B-00-EE-0A



ARP缓存表操作

- 在PC上可以通过命令来操作ARP缓存表
  - arp -a　列出所有的ARP缓存表项
  - arp -s　添加静态ARP缓存表项。静态ARP表项是永久性的，除非用arp -d删除
  - arp -d　删除所有的ARP缓存表项

```
C:\Users\LU-Meilian>arp -a

接口: 192.168.19.1 --- 0xe
  Internet 地址         物理地址              类型
  192.168.19.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 2.0.0.1 --- 0x15
  Internet 地址         物理地址              类型
  2.0.0.255             ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

```
接口: 192.168.189.1 --- 0x25
  Internet 地址         物理地址              类型
  192.168.189.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 192.168.1.6 --- 0x29
  Internet 地址         物理地址              类型
  192.168.1.1           e0-4b-a6-1f-77-12     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

C:\Users\LU-Meilian>
```

动态ARP缓存表的生存时间

- arp -a：观察动态arp缓存的生存时间
  - 动态arp缓存表项有有限的生存时间（2分钟/10分钟）
  - 在PC上ping某IP地址，获得该IP地址对应的MAC地址后，用arp -a观察动态arp缓存的生存时间
  - 在2分钟内未使用该arp表项的话，该表项会被自动删除；如果在2分钟内使用了该表项，会从使用之时起，该表项的生存时间再延长2分钟，直到最大生命期限10分钟为止
  - 超过10分钟最大期限后，ARP缓存表项将被删除，并且需要通过另外一个ARP请求/ARP回应来获得新的对应关系

重复IP地址检测

- ARP可以被用来检测重复的IP地址
  - 这是通过传送一种叫做无偿ARP（Gratuitous ARP）的ARP请求来完成的
  - 无偿ARP就是一个解析自己IP地址的ARP请求。在无偿ARP请求中，源IP地址和目的IP均被设置成本机的IP地址
  - 如果节点发送一个无偿ARP请求后，没有收到任何一个ARP回应帧，就可以判断没有其他节点使用与它相同的IP地址
  - 如果发送了3个无偿ARP后，都没有收到ARP回应，节点就假定此IP地址在此网络段中是唯一的
  - 如果节点发送一个无偿ARP请求后，收到ARP回应，此节点就可以判断有另外一个节点使用同样的IP地址

在配置终端IP地址时，可以通过抓包观察重复地址检测过程

主要内容

- ARP协议原理
- **ICMP协议原理**
- Wireshark协议分析实验

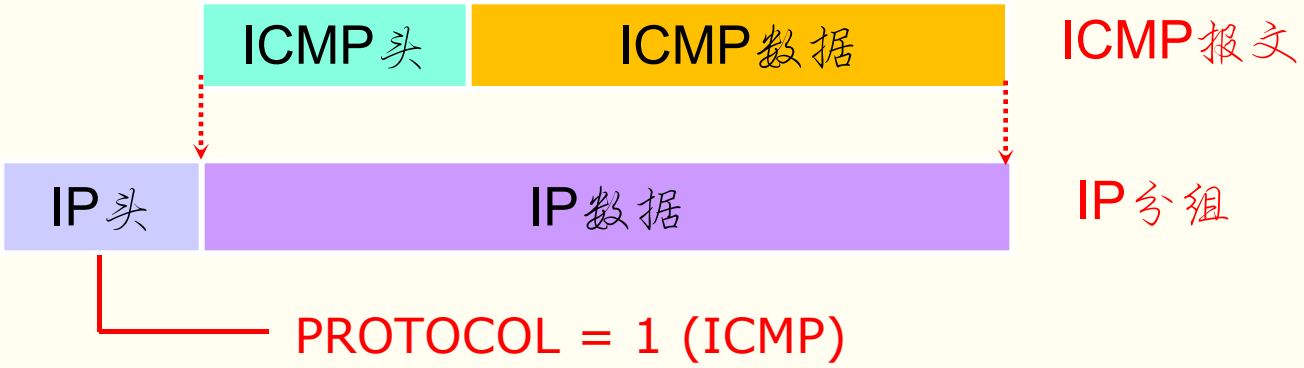
ICMP概述

- ICMP - Internet控制报文协议 (Internet Control Message Protocol)

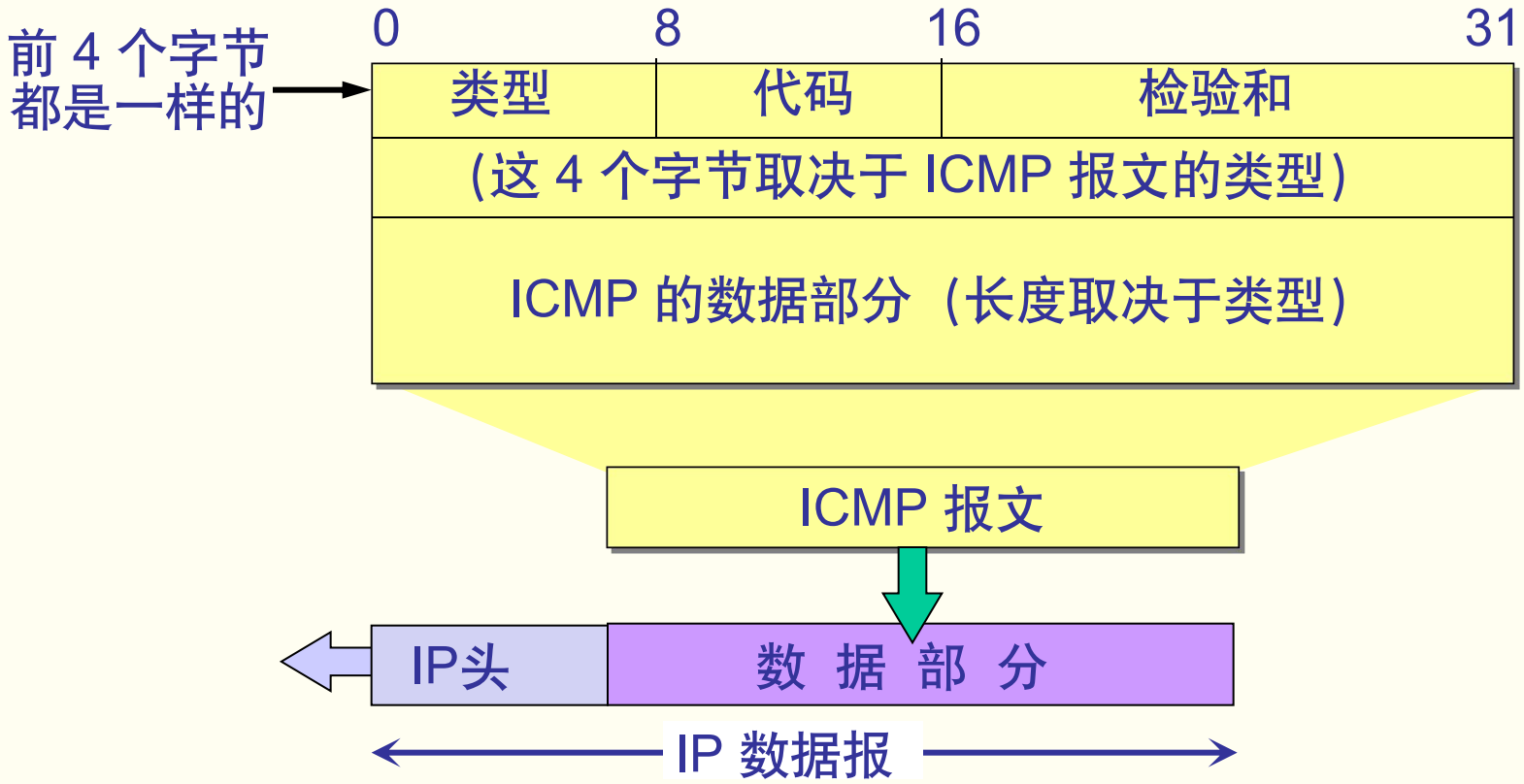
- ICMP的功能——ICMP的功能属于网络层
  - 差错报告
  - 控制
  - 信息询问 （请求/应答）

ICMP消息的封装格式

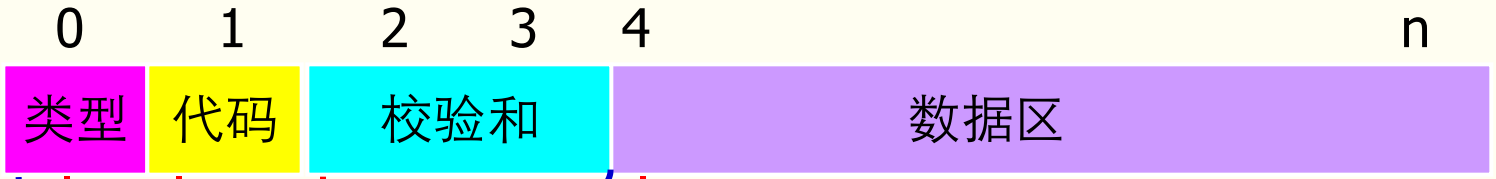
- ICMP报文封装在IP数据包中传输
  - 这是由于控制信息在网络中传输时需要跨越多个网络，需要用到网络层功能才能完成
  - ICMP的数据部分通常是出现问题的IP数据包的报头和部分内容。因此在分析ICMP数据包时通常会发现两个IP包头



ICMP 报文格式


前 4 个字节
都是一样的
0
8
16
31
类型
代码
检验和
(这 4 个字节取决于 ICMP 报文的类型)
ICMP 的数据部分（长度取决于类型）
ICMP 报文
IP头
数 据 部 分
IP 数据报

ICMP报文格式（续）



ICMP报头

包括出错数据报报头及该数据报前64比特（8字节）数据

CHECKSUM：整个ICMP报文的校验和算法同IP报头校验和的算法

CODE：提供报文类型的详细信息

三类报文

- 回送请求/响应报文
- 超时报文
- 目的主机不可达报文

TYPE: 指出ICMP报文的类型

0：回应应答	12：分组参数错
3：目的不可达	13：时间戳请求
4：源抑制	14：时间戳应答
5：路由重定向	17：地址掩码请求
8：回应请求	18：地址掩码应答
11：数据报超时	

ICMP消息格式（续）

- 回送请求/响应（ICMP Echo Request/ICMP Echo Reply）：用于探测主机地址是否存活
  - 如果主机给目的主机发送的ICMP Echo Request后收到ICMP Echo Reply，说明目的主机是存活状态
  - 如果一定时间后没有收到ICMP Echo Reply，则认为目的主机不在线
  - 检测网络是否畅通和目的主机是否可达时，会采用Ping命令，就是使用回送请求/响应机制
  - 回送请求的源IP地址和目的IP地址分别是回送响应目的IP地址和源IP地址
  - 请求类型=8，代码=0；响应类型=0，代码=0

ICMP消息格式（续）

- 超时报文（Timeout）
  - 产生超时报文的情况
    - 数据包长时间在网络中传输但是找不到目标
    - 网络拥塞导致在规定时间内无法重组数据包分段
  - 类型=11
  - 代码：

    0 = 传送超时

    1 = 分段重装超时

ICMP消息格式（续）

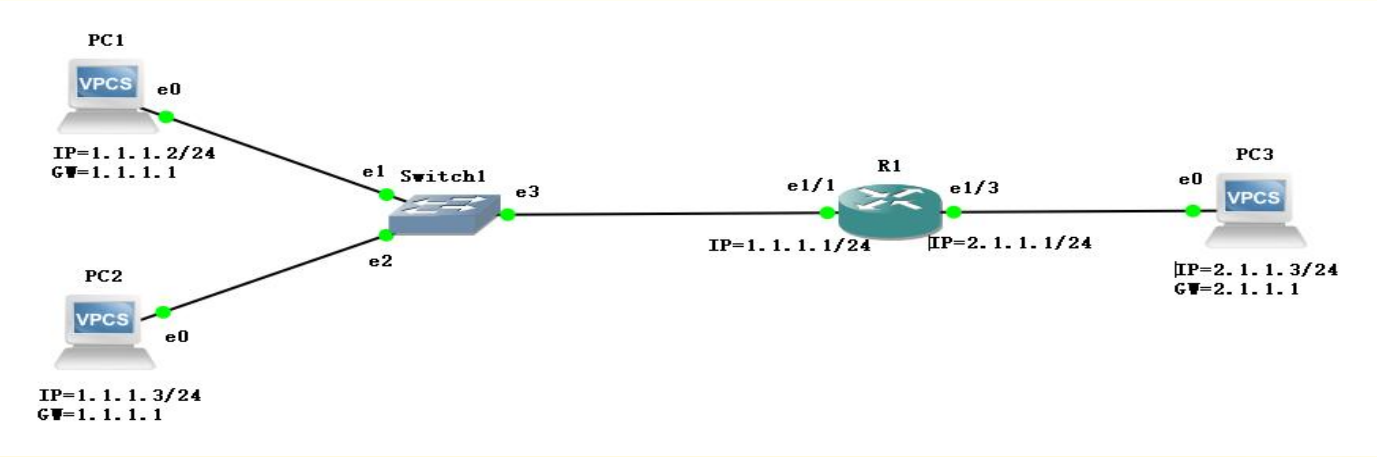
- 目标主机不可达报文
  - 在路由器或主机不能传递数据包时使用
  - 当寻找的目的主机、端口或网络等不存在时，会产生目标不可达报文
  - 类型=3
  - 代码：
    0 = 网络不可达
    1 = 主机不可达
    2 = 协议不可用
    3 = 端口不可达
    4 = 数据包太长，需要段和DF设置
    5 = 源路由失败

主要内容

- ARP协议原理
- ICMP协议原理
- **Wireshark协议分析实验**

Wireshark协议分析实验

- 实践目的
  - 掌握Wireshark协议分析工具的使用方法，能够在实际网络环境中分析ARP协议的工作过程和ICMP协议的工作原理，以及以太网中数据报的传输过程
- 实践环境
  - 真实网络环境：一台路由器、一台以太网交换机、三台带有以太网接口的PC
- 实验网络拓扑（仅供参考）



实验6.1：ARP协议分析

- 实验步骤

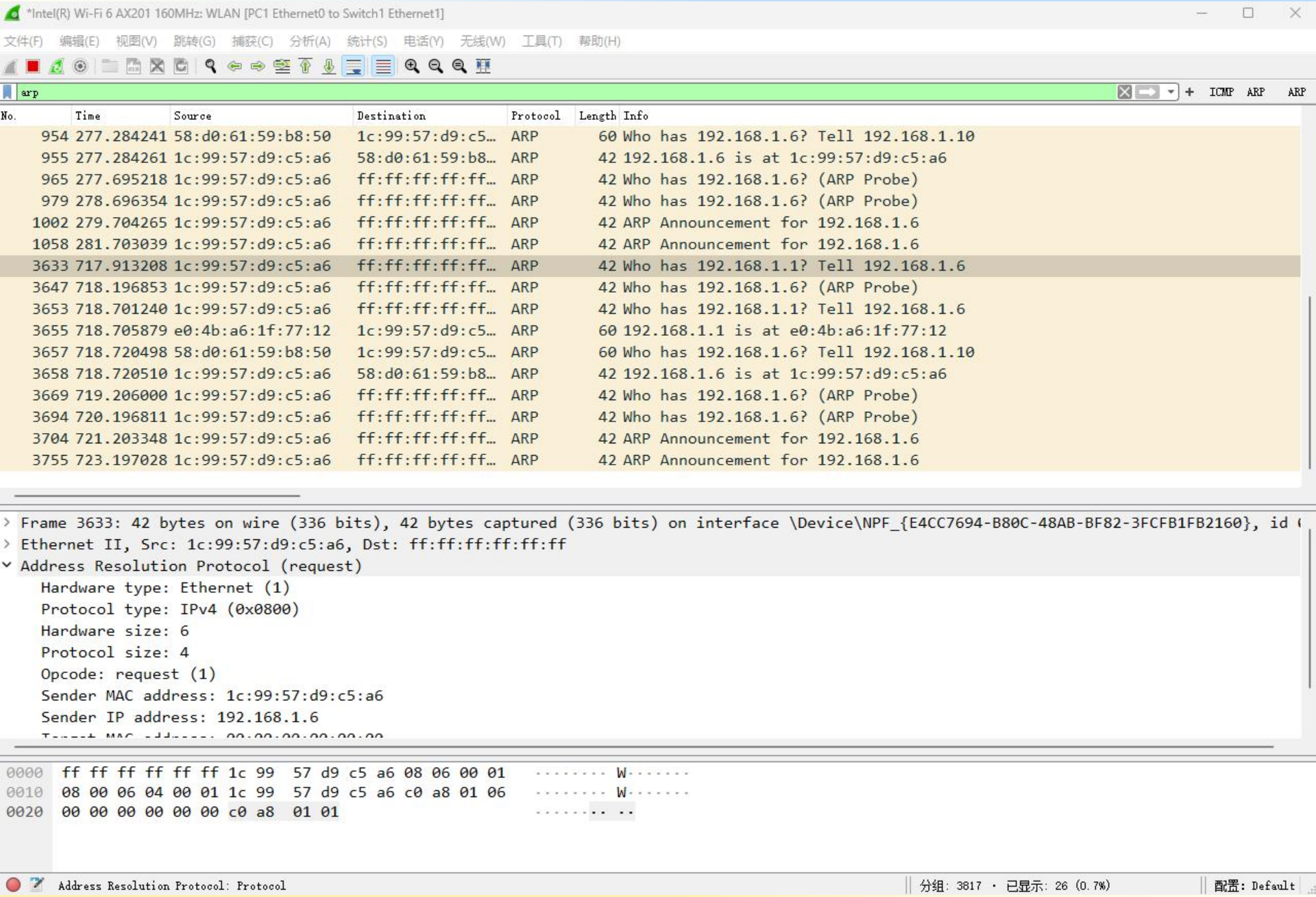
1. 在PC1和PC2上用arp -d命令删除所有ARP缓存表项
2. 在PC1上 ping PC2（ping 1.1.1.3），以触发ARP过程
3. 用Wireshark抓取ARP数据包，并分析ARP的交互过程
   - 用Wireshark抓取ARP数据包时，在显示过滤器中输入arp，就可以将所有的ARP数据包显示出来，而屏蔽掉其他数据包，便于对ARP协议进行分析
4. 在PC1和PC2上分别用arp -a观察ARP缓存表的变化情况，了解ARP解析过程

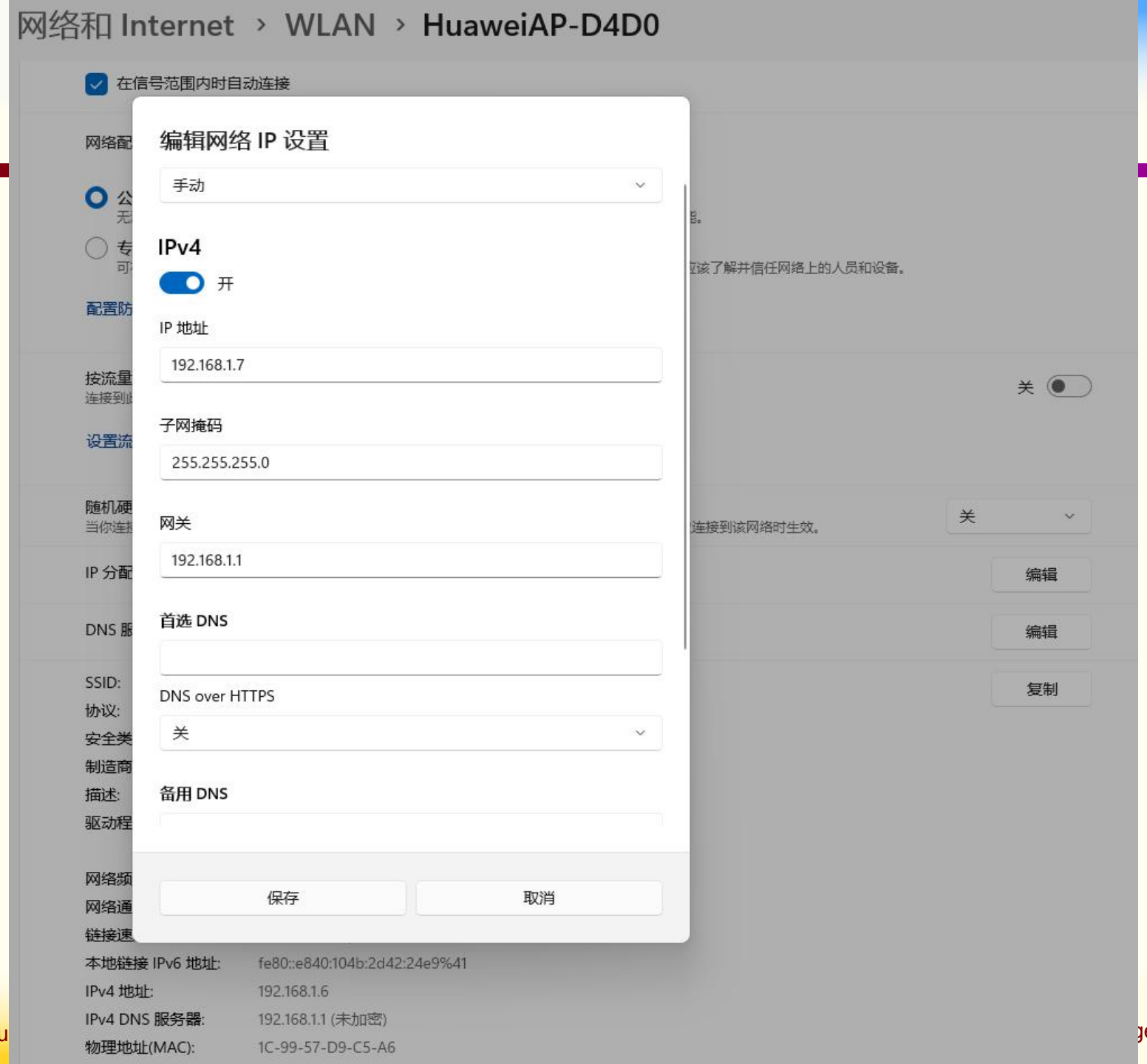
实验6.1：ARP协议分析（续）

- 实验步骤

5. 在PC1上设置IP地址1.1.1.2，然后在PC2上设置相同的IP地址，用Wireshark抓取所有的ARP包

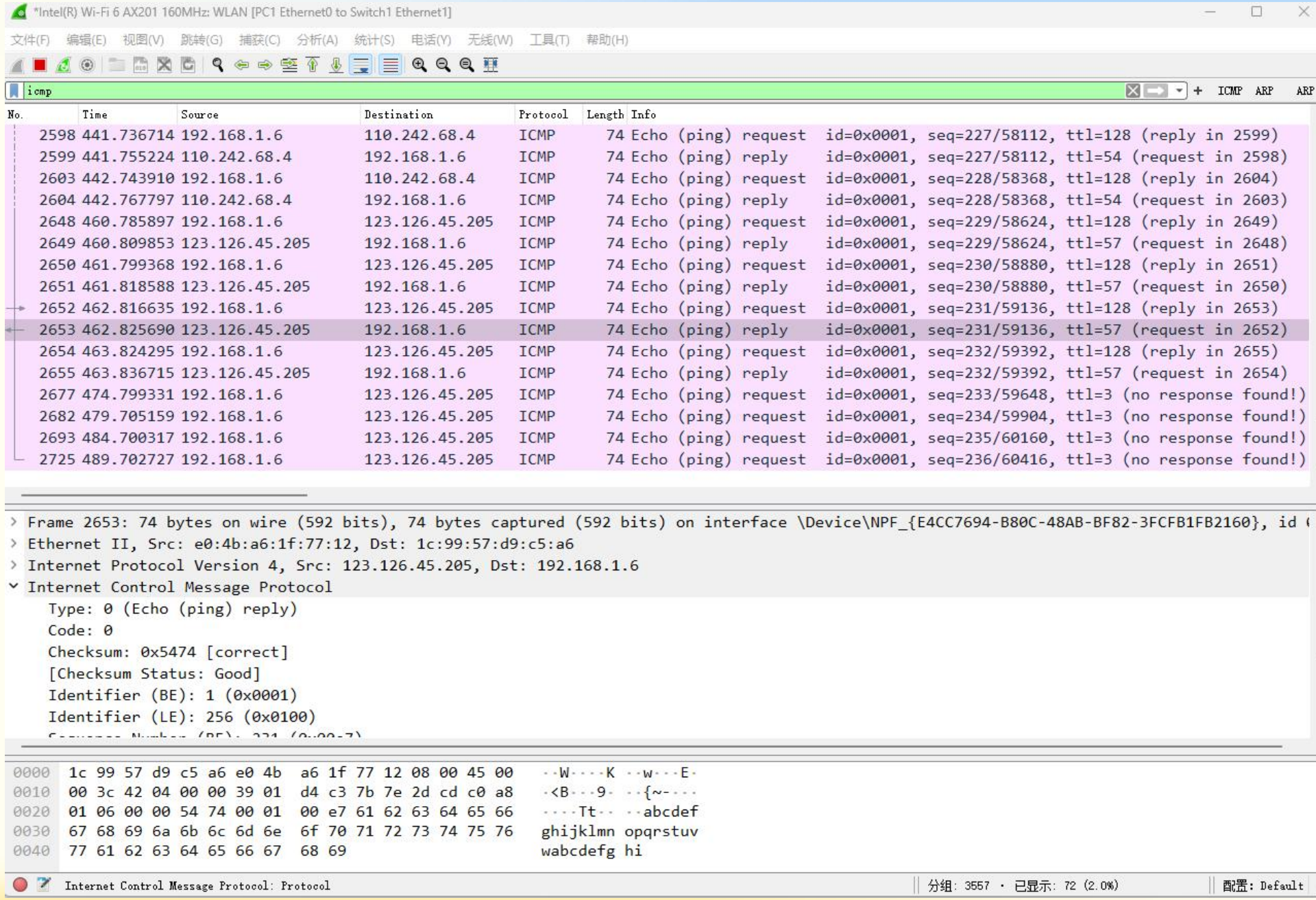
   - PC1在设置完IP地址后，会发出三次无偿ARP请求，其中的源IP地址和目的IP地址都是1.1.1.2，在一段时间内没有收到ARP响应后，认为网络上没有其他主机配置了IP地址1.1.1.2，这时PC1的TCP/IP协议栈就可以完成初始化了
   - PC2在设置完IP地址1.1.1.2后，也会发出一个无偿ARP请求，当PC1收到无偿ARP请求后，会向PC2回复ARP响应，在重复这样三次后，PC2就可以确定网络内已经有主机设置了与自己相同的IP地址1.1.1.2，就无法初始化其TCP/IP协议栈了


*Intel(R) Wi-Fi 6 AX201 160MHz: WLAN [PC1 Ethernet0 to Switch1 Ethernet1]
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
arp
ICMP ARP ARP
No. Time Source Destination Protocol Length Info
954 277.284241 58:d0:61:59:b8:50 1c:99:57:d9:c5… ARP 60 Who has 192.168.1.6? Tell 192.168.1.10
955 277.284261 1c:99:57:d9:c5:a6 58:d0:61:59:b8… ARP 42 192.168.1.6 is at 1c:99:57:d9:c5:a6
965 277.695218 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
979 278.696354 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
1002 279.704265 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
1058 281.703039 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
3633 717.913208 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.1? Tell 192.168.1.6
3647 718.196853 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3653 718.701240 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.1? Tell 192.168.1.6
3655 718.705879 e0:4b:a6:1f:77:12 1c:99:57:d9:c5… ARP 60 192.168.1.1 is at e0:4b:a6:1f:77:12
3657 718.720498 58:d0:61:59:b8:50 1c:99:57:d9:c5… ARP 60 Who has 192.168.1.6? Tell 192.168.1.10
3658 718.720510 1c:99:57:d9:c5:a6 58:d0:61:59:b8… ARP 42 192.168.1.6 is at 1c:99:57:d9:c5:a6
3669 719.206000 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3694 720.196811 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3704 721.203348 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
3755 723.197028 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
Frame 3633: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{E4CC7694-B80C-48AB-BF82-3FCFB1FB2160}, id
Ethernet II, Src: 1c:99:57:d9:c5:a6, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 1c:99:57:d9:c5:a6
Sender IP address: 192.168.1.6
0000 ff ff ff ff ff ff 1c 99 57 d9 c5 a6 08 06 00 01 ···· W·····
0010 08 00 06 04 00 01 1c 99 57 d9 c5 a6 c0 a8 01 06 ···· W·····
0020 00 00 00 00 00 00 c0 a8 01 01 ····
Address Resolution Protocol: Protocol
分组: 3817 · 已显示: 26 (0.7%)
配置: Default


网络和 Internet › WLAN › HuaweiAP-D4D0
在信号范围内时自动连接
编辑网络 IP 设置
手动
IPv4
开
IP 地址
192.168.1.7
子网掩码
255.255.255.0
网关
192.168.1.1
首选 DNS
DNS over HTTPS
关
备用 DNS
保存
取消
编辑
编辑
复制
本地链接 IPv6 地址: fe80::e840:104b:2d42:24e9%41
IPv4 地址: 192.168.1.6
IPv4 DNS 服务器: 192.168.1.1 (未加密)
物理地址(MAC): 1C-99-57-D9-C5-A6

实验6.2：ICMP协议分析

- 实验步骤
  1. 在PC1上 ping PC2
  2. 用Wireshark抓取ICMP数据包，并分析ICMP的回送请求和回送响应报文的交互过程
     - 用Wireshark抓取ICMP数据包时，在显示过滤器中输入icmp，将所有的ICMP报文显示出来，而屏蔽掉其他数据包，便于对ICMP协议进行分析
  3. 在一台能够接入Internet网络的PC上，用ping命令探测网络上较远的节点，但把TTL值设置较小，如ping -i 3 www.sina.com.cn，查看返回信息，并用Wireshark查看返回的ICMP超时信息
     - 在有些情况下，网络中不会返回ICMP超时报文
  4. 再ping其它的主机，实现不可达的返回消息


*Intel(R) Wi-Fi 6 AX201 160MHz: WLAN [PC1 Ethernet0 to Switch1 Ethernet1]
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp
ICMP ARP ARP
No. Time Source Destination Protocol Length Info
2598 441.736714 192.168.1.6 110.242.68.4 ICMP 74 Echo (ping) request id=0x0001, seq=227/58112, ttl=128 (reply in 2599)
2599 441.755224 110.242.68.4 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=227/58112, ttl=54 (request in 2598)
2603 442.743910 192.168.1.6 110.242.68.4 ICMP 74 Echo (ping) request id=0x0001, seq=228/58368, ttl=128 (reply in 2604)
2604 442.767797 110.242.68.4 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=228/58368, ttl=54 (request in 2603)
2648 460.785897 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=229/58624, ttl=128 (reply in 2649)
2649 460.809853 123.126.45.205 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=229/58624, ttl=57 (request in 2648)
2650 461.799368 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=230/58880, ttl=128 (reply in 2651)
2651 461.818588 123.126.45.205 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=230/58880, ttl=57 (request in 2650)
2652 462.816635 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=231/59136, ttl=128 (reply in 2653)
2653 462.825690 123.126.45.205 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=231/59136, ttl=57 (request in 2652)
2654 463.824295 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=232/59392, ttl=128 (reply in 2655)
2655 463.836715 123.126.45.205 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=232/59392, ttl=57 (request in 2654)
2677 474.799331 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=233/59648, ttl=3 (no response found!)
2682 479.705159 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=234/59904, ttl=3 (no response found!)
2693 484.700317 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=235/60160, ttl=3 (no response found!)
2725 489.702727 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=236/60416, ttl=3 (no response found!)
Frame 2653: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E4CC7694-B80C-48AB-BF82-3FCFB1FB2160}, id
Ethernet II, Src: e0:4b:a6:1f:77:12, Dst: 1c:99:57:d9:c5:a6
Internet Protocol Version 4, Src: 123.126.45.205, Dst: 192.168.1.6
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x5474 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
0000 1c 99 57 d9 c5 a6 e0 4b a6 1f 77 12 08 00 45 00 ··W····K ··w···E·
0010 00 3c 42 04 00 00 39 01 d4 c3 7b 7e 2d cd c0 a8 ·<B···9· ··{~-···
0020 01 06 00 00 54 74 00 01 00 e7 61 62 63 64 65 66 ····Tt·· ··abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Internet Control Message Protocol: Protocol
分组: 3557 · 已显示: 72 (2.0%)
配置: Default

实验6.3 局域网内数据传输过程

- 实验步骤

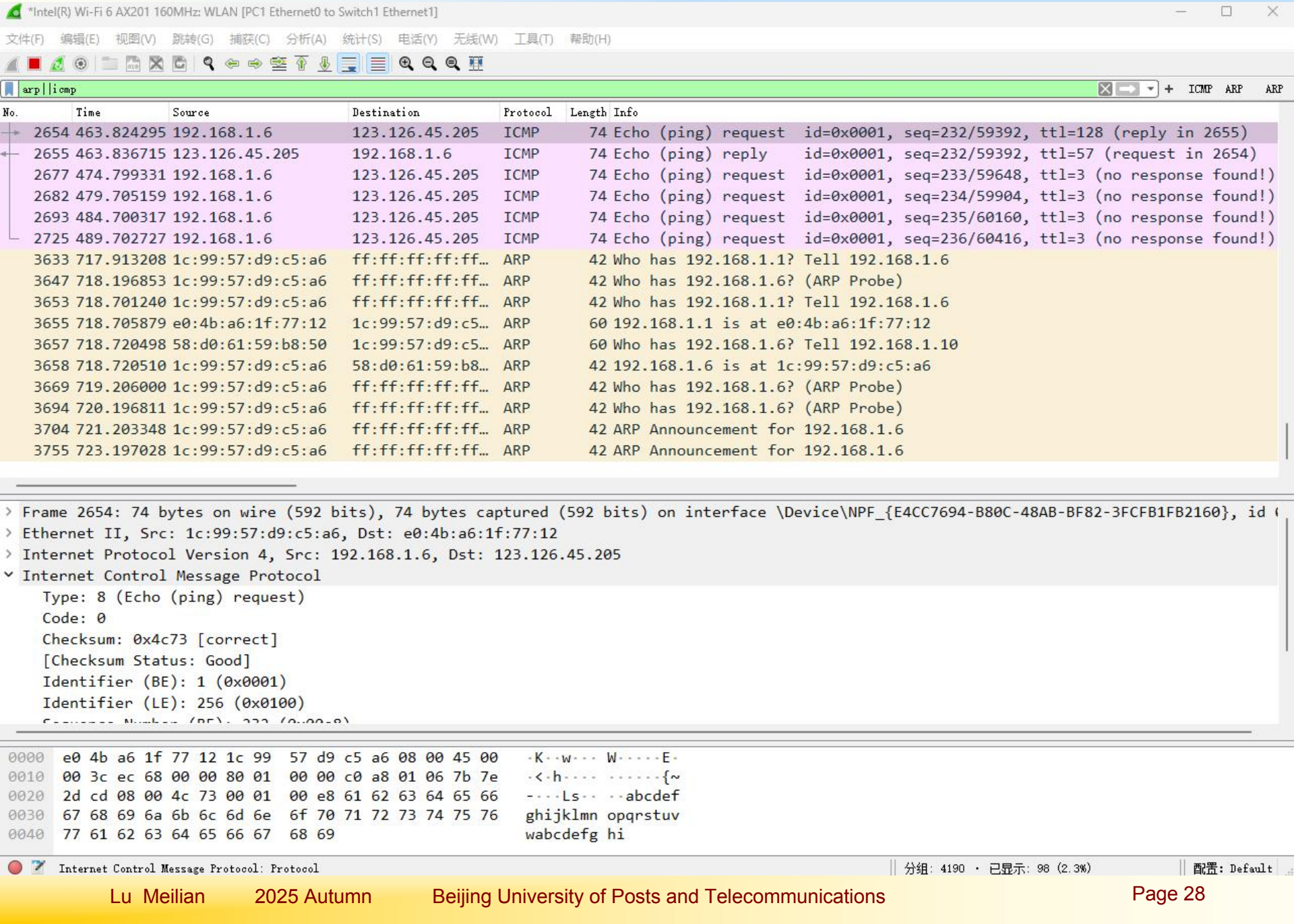
1. 在PC1和PC2上用arp -d命令删除所有ARP缓存表项
2. 在PC1上 ping PC2
3. 用Wireshark抓取PC1和PC2之间交互的所有数据包，并分析PC1向PC2发送数据的完整流程
   - 在显示过滤器中输入arp||icmp，就可以将所有的ARP和ICMP的报文显示出来，而屏蔽掉其他数据包

实验6.4 局域网间数据传输过程

实验步骤

1. 在PC1和PC3上使用arp -d命令删除所有ARP缓存表项
2. 将PC1的网关配置为1.1.1.1，PC3的网关配置为2.1.1.1
3. 在PC1上ping PC3
4. 用Wireshark抓取PC1和PC3间交互的所有数据包，并分析PC1向PC3发送数据的完整流程
   - 在抓取数据包时，需要将Wirshark安装在PC1和PC3上，并且要结合两个Wireshark抓取到的数据包进行分析
   - 同样，可以在Wireshark的显示过滤器中输入arp||icmp

注：当没有路由器设备时，想要完成局域网间的数据发送过程，可以通过ping www.sina.com.cn这样的方式来观察PC向外部网络发送数据的过程，以及路由器返回数据给PC的过程。通过这两个过程来推测出两台不在同一局域网中的PC之间的通信过程。当然由于ARP缓存的问题，这两个过程会比真正的局域网间数据发送过程少一些步骤。


*Intel(R) Wi-Fi 6 AX201 160MHz: WLAN [PC1 Ethernet0 to Switch1 Ethernet1]
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
arp||icmp
ICMP ARP ARP
No. Time Source Destination Protocol Length Info
2654 463.824295 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=232/59392, ttl=128 (reply in 2655)
2655 463.836715 123.126.45.205 192.168.1.6 ICMP 74 Echo (ping) reply id=0x0001, seq=232/59392, ttl=57 (request in 2654)
2677 474.799331 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=233/59648, ttl=3 (no response found!)
2682 479.705159 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=234/59904, ttl=3 (no response found!)
2693 484.700317 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=235/60160, ttl=3 (no response found!)
2725 489.702727 192.168.1.6 123.126.45.205 ICMP 74 Echo (ping) request id=0x0001, seq=236/60416, ttl=3 (no response found!)
3633 717.913208 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.1? Tell 192.168.1.6
3647 718.196853 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3653 718.701240 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.1? Tell 192.168.1.6
3655 718.705879 e0:4b:a6:1f:77:12 1c:99:57:d9:c5… ARP 60 192.168.1.1 is at e0:4b:a6:1f:77:12
3657 718.720498 58:d0:61:59:b8:50 1c:99:57:d9:c5… ARP 60 Who has 192.168.1.6? Tell 192.168.1.10
3658 718.720510 1c:99:57:d9:c5:a6 58:d0:61:59:b8… ARP 42 192.168.1.6 is at 1c:99:57:d9:c5:a6
3669 719.206000 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3694 720.196811 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 Who has 192.168.1.6? (ARP Probe)
3704 721.203348 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
3755 723.197028 1c:99:57:d9:c5:a6 ff:ff:ff:ff:ff… ARP 42 ARP Announcement for 192.168.1.6
Frame 2654: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E4CC7694-B80C-48AB-BF82-3FCFB1FB2160}, id
Ethernet II, Src: 1c:99:57:d9:c5:a6, Dst: e0:4b:a6:1f:77:12
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 123.126.45.205
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4c73 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
0000 e0 4b a6 1f 77 12 1c 99 57 d9 c5 a6 08 00 45 00 ·K··w··· W·····E·
0010 00 3c ec 68 00 00 80 01 00 00 c0 a8 01 06 7b 7e ·<·h···· ·····{~
0020 2d cd 08 00 4c 73 00 01 00 e8 61 62 63 64 65 66 ····Ls·· ··abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Internet Control Message Protocol: Protocol
分组: 4190 · 已显示: 98 (2.3%)
配置: Default

问题和分析

- 问题一：为什么总是得不到超时报文和目的主机不可达的报文?
  - 有些网络设备并不会产生超时报文和目的主机不可达报文。还有些网络设备会隔离ICMP报文

- 问题二：在同一网络中的两台主机为什么总是无法ping通？
  - 如果一些配置都是正确的话，通常是因为主机上开启了防火墙和杀毒软件，这些防护软件为了防止网络攻击，通常会过滤掉ICMP报文。做实验时，将这类软件关闭即可