

实验二 网络层协议分析

✓ ARP协议分析

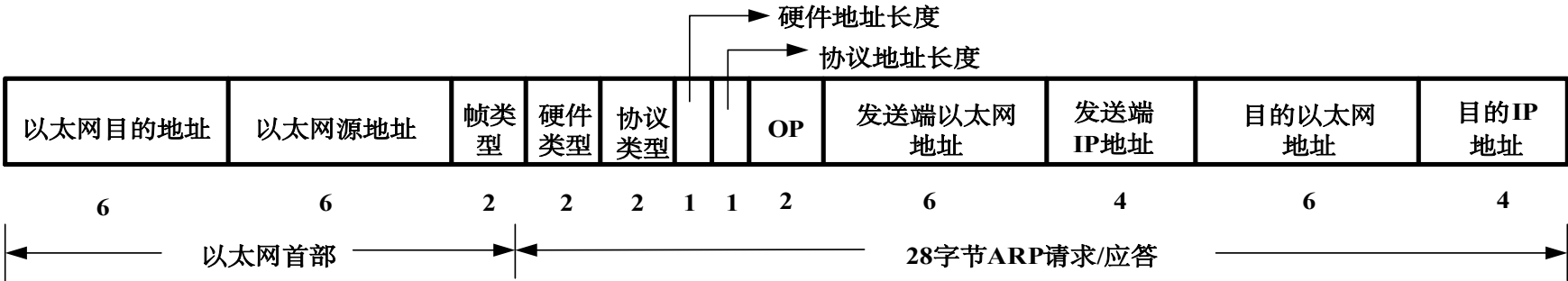
✓ ICMP协议分析

✓ IP协议分析

ARP，全称 Address Resolution Protocol，中文名为地址解析协议，它工作在数据链路层，在本层和硬件接口联系，同时对上层提供服务。

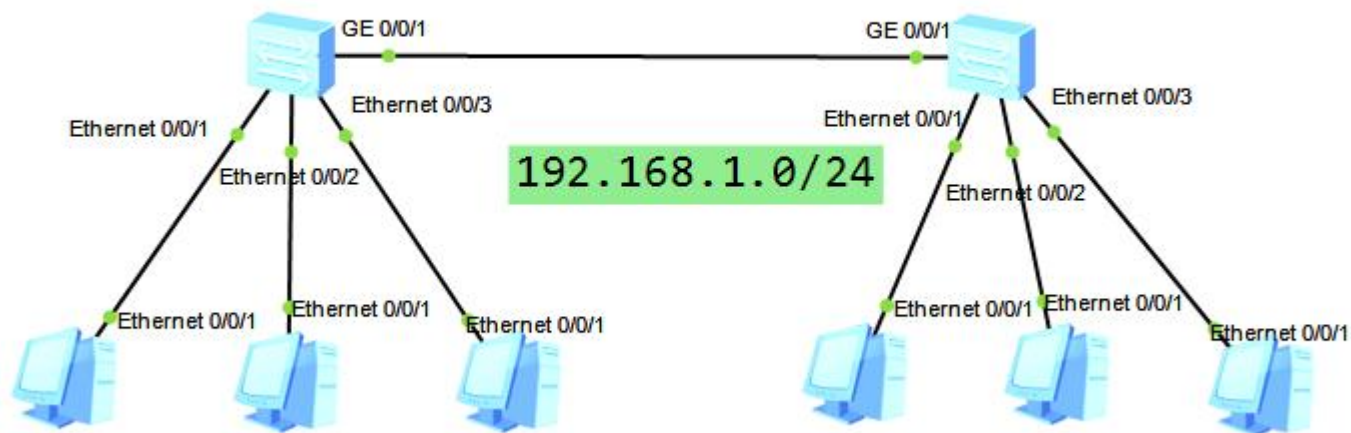
IP 数据包常通过以太网发送，以太网设备并不识别 32 位 IP 地址，它们是以 48 位以太网地址传输以太网数据包。因此，必须把 IP 目的地址转换成以太网目的地址。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。ARP 协议用于将网络中的 IP 地址解析为的硬件地址（MAC 地址），以保证通信的顺利进行。

✨ ARP的数据帧格式：



01

拓扑结构

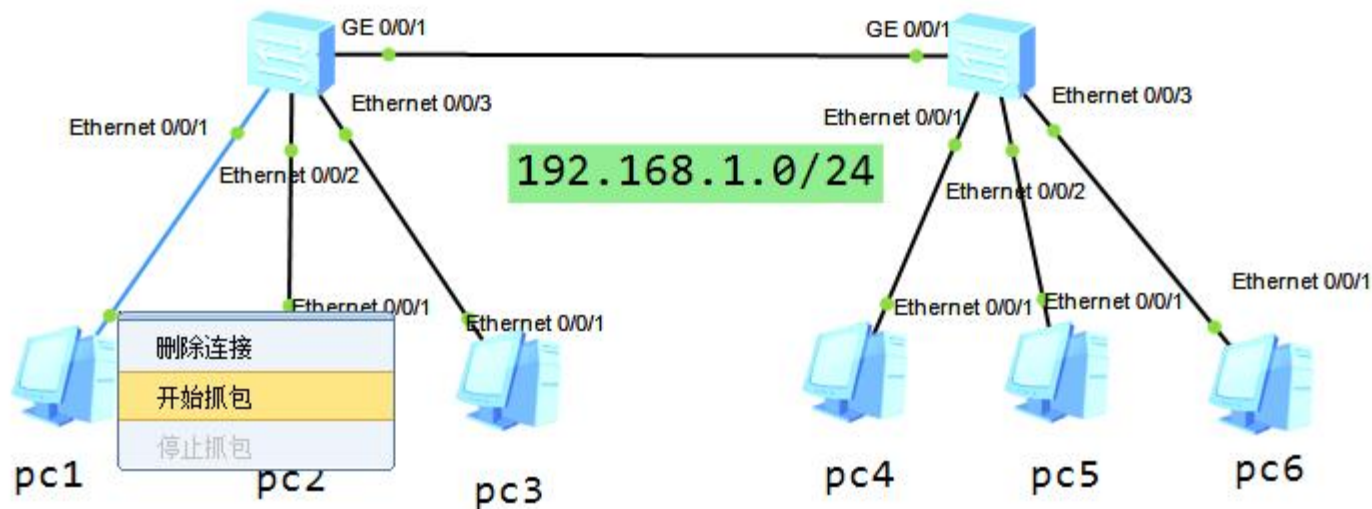


步骤 1: 清空主机 pc1 的 ARP 表
在 pc1 终端上, 通过命令清空 ARP 表。

参考命令:

`clear arp`

步骤 2: 使用Wireshark 记录主机 pc1 的所有通信报文
右击 pc1与链路, 选择“开始抓包”进行抓包, 结果如图 1-1 所示。



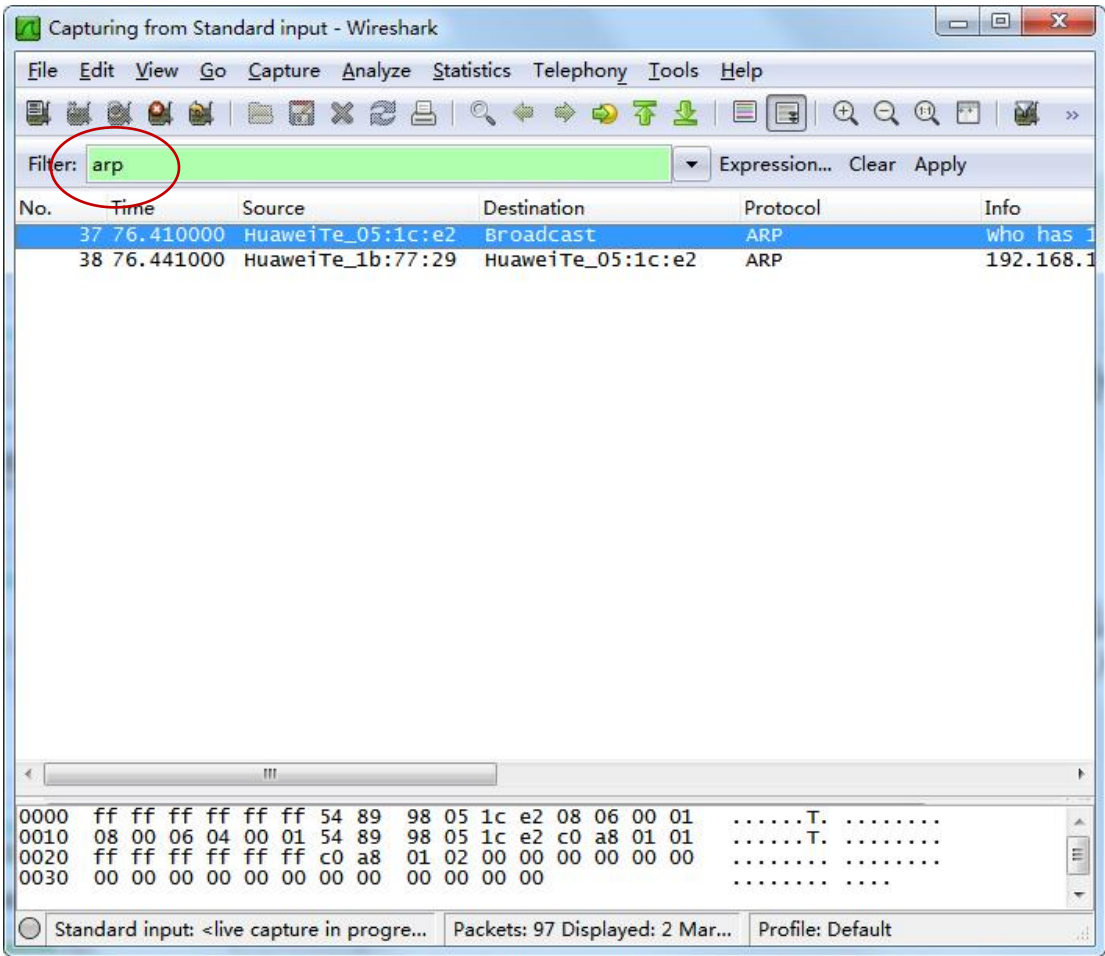
01

ARP 报文结构分析

步骤 3: 在主机PC1 上 Ping 主机PC2
在PC 终端上, 执行 Ping 命令。

参考命令:
ping 192.168.1.2

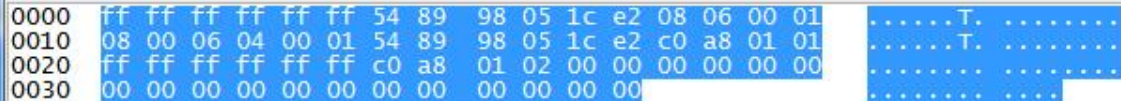
步骤 4: 在Wireshark 上筛选出
PC1 的 ARP 报文
在 Wireshark 的过滤器中输入
“arp”, 查看PC1 收发的 ARP
报文。



01



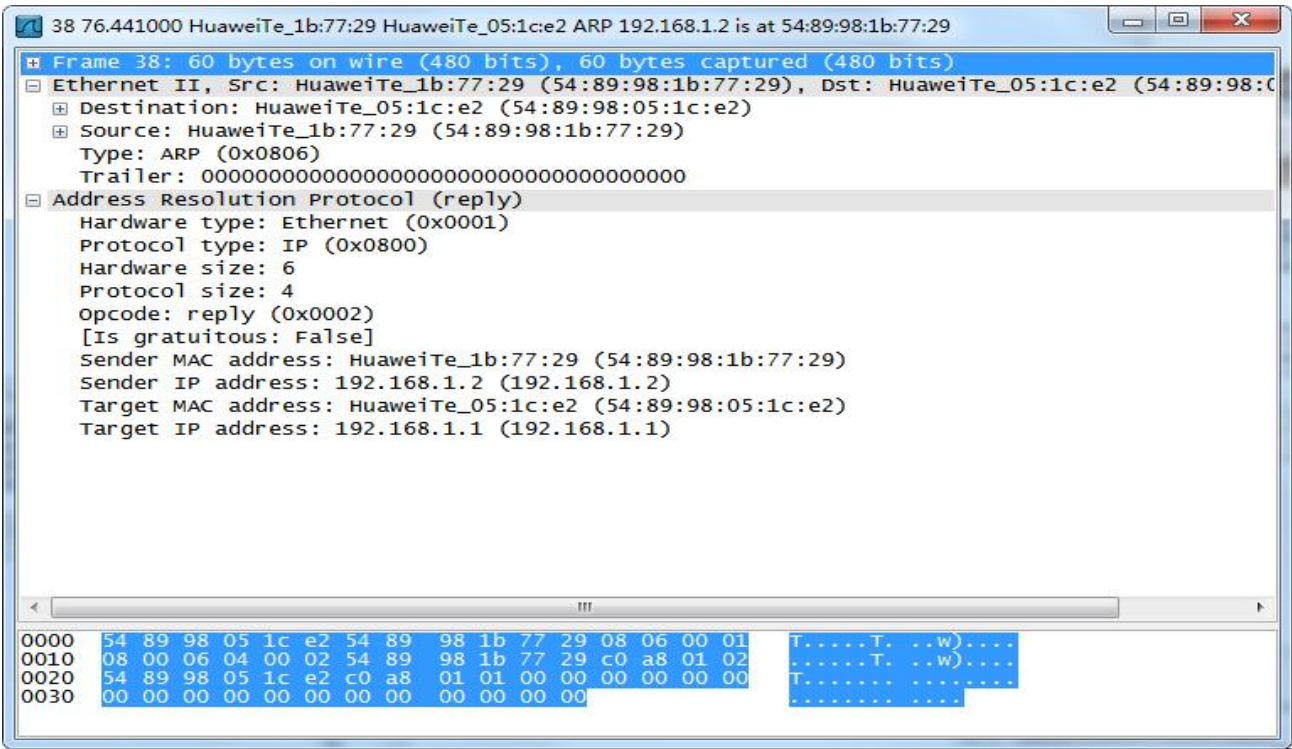
三、详细分析 如何





步骤 06：分析PC1 收到的ARP 响应报文结构

在 Wireshar 中选择任意一条响应报文进行详细分析，如图所示，分析结果填写到实验报告表 1-2。



步骤 07：对比分析ARP 请求报文和响应报文结构

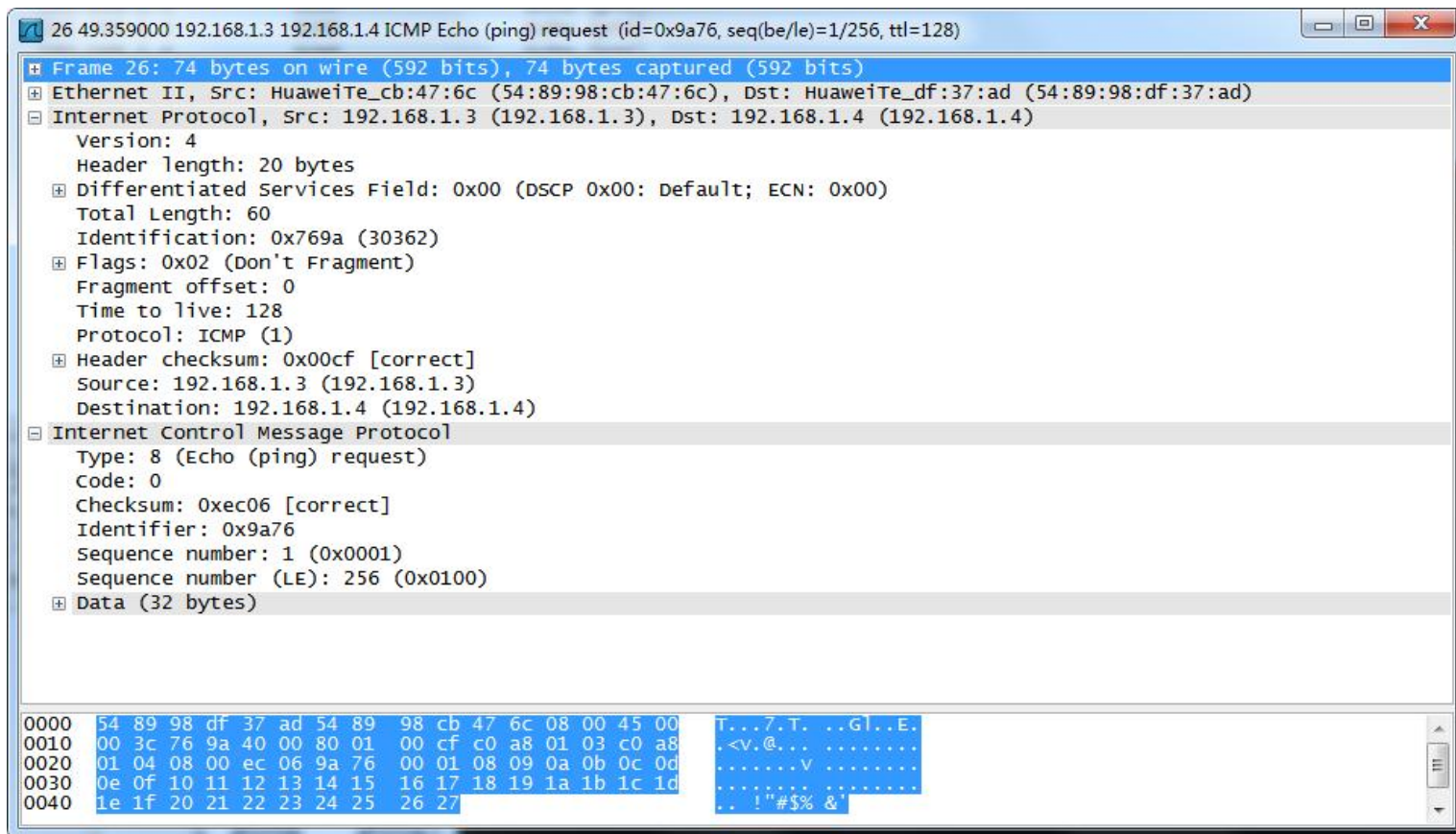
比较ARP 请求报文与响应报文的 5 个关键差别，并填写表 1-3。

02

ICMP 报文结构分析

step1: 进入PC3然后执行ping指令pingPC4:

利用Wireshark工具对PC3的Ethernet 0/0/1接口进行数据抓包，ICMP报文信息如图所示:



02 ICMP 报文结构分析



?



将截获到的ICMP报文信息与ICMP报文格式进行对比分析，ICMP报文格式如图所示：



分析 ICMP 报文内容，填写实验报告表 2-1。

PC3 ping PC4 进行连通性测试，并将测试结果填入实验报告表 2-2 中。

字段	大小（以字节为单位）	含义
Type		
Code		
Checksum		
Identifier		
Sequence		

表 2-1

报文分析点	源主机	目的主机	type	code	Identifier(BE)Identifier(LE)	Sequence(BE)Sequence(LE)	通信结果
1	Host-3	Host-4					
	Host-4	Host-3					

表 2-2

03

IP 报文结构分析

step1: 在ICMP协议分析的基础上进行IP协议的分析，利用Wireshark工具对PC3的Ethernet 0/0/1接口进行数据抓包，IP报文信息如图所示。

Internet Protocol Version 4, Src: 192.168.10.122, Dst: 192.168.30.120

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x6554 (25940)

> Flags: 0x4000, Don't fragment

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0xeb29 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.10.122

Destination: 192.168.30.120

> Internet Control Message Protocol

0000	4c 1f cc 66 06 c0 54 89 98 13 0b c5 08 00 45 00	L..f..T.E.
0010	00 3c 65 54 40 00 80 01 eb 29 c0 a8 0a 7a c0 a8	..<eT@... ..)....z..
0020	1e 78 08 00 31 16 55 65 00 03 08 09 0a 0b 0c 0d	..x..1.Ue
0030	0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
0040	1e 1f 20 21 22 23 24 25 26 27	.. !"# \$% &'

03

IP 报文结构分析

将截获到的IP报文信息与IP报文格式进行对比分析，IP报文格式如图所示。



step1: 进入PC3然后执行ping指令pingPC4，指定传输的数据为1500字节，进行IP分片分析。
命令如下：
ping 192.168.1.4 -l 1500

03 IP 报文结构分析

step3: 利用Wireshark工具对PC3Ethernet 0/0/1接口进行数据抓包，IP报文信息参考如下。

```
Internet Protocol Version 4, Src: 192.168.10.122, Dst: 192.168.30.120
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 48
  Identification: 0x6c5b (27739)
  > Flags: 0x00b9
  Time to live: 128
  Protocol: ICMP (1)
  Header checksum: 0x2376 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.10.122
  Destination: 192.168.30.120
  [2 IPv4 Fragments (1508 bytes): #25(1480), #26(28)]
    [Frame: 25, payload: 0-1479 (1480 bytes)]
    [Frame: 26, payload: 1480-1507 (28 bytes)]
  [Fragment count: 2]
  [Reassembled IPv4 length: 1508]
  [Reassembled IPv4 data: 0800e9f45e6c000408090a0b0c0d0e0f1011121314151617...]
```

由图可知，1500字节的数据被分成了1480字节和28字节。（UDP首部8字节，所以实际需要传输1500+8字节）。因此当MTU为1500字节的情况下，传输数据超过1500-20-8=1472字节时需要进行IP分片。

03 IP 报文结构分析



完成实验，并填写实验报告。

