实验二 网络层协议分析

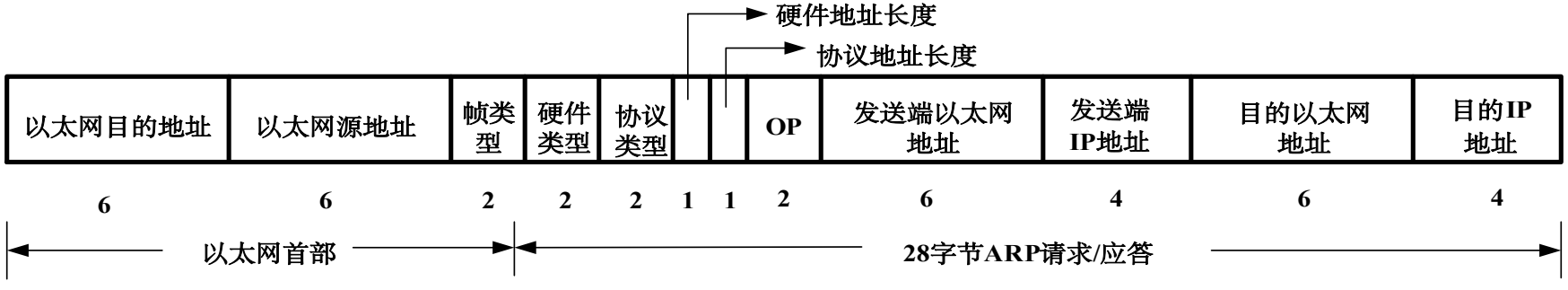
- ✓ARP协议分析
- ✓ ICMP协议分析
- ✓ IP协议分析

01 ARP

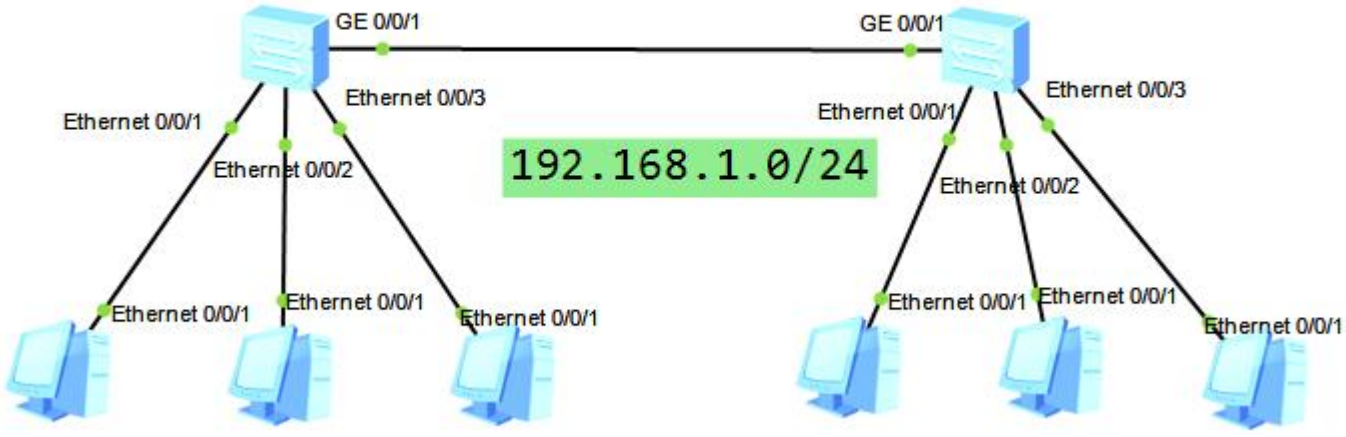
ARP，全称 Address Resolution Protocol，中文名为地址解析协议，它工作在数据链路层，在本层和硬件接口联系，同时对上层提供服务。

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


GE 0/0/1
GE 0/0/1
Ethernet 0/0/1
Ethernet 0/0/3
Ethernet 0/0/2
192.168.1.0/24
Ethernet 0/0/1
Ethernet 0/0/3
Ethernet 0/0/2
Ethernet 0/0/1
Ethernet 0/0/1
Ethernet 0/0/1
Ethernet 0/0/1
Ethernet 0/0/1
Ethernet 0/0/1

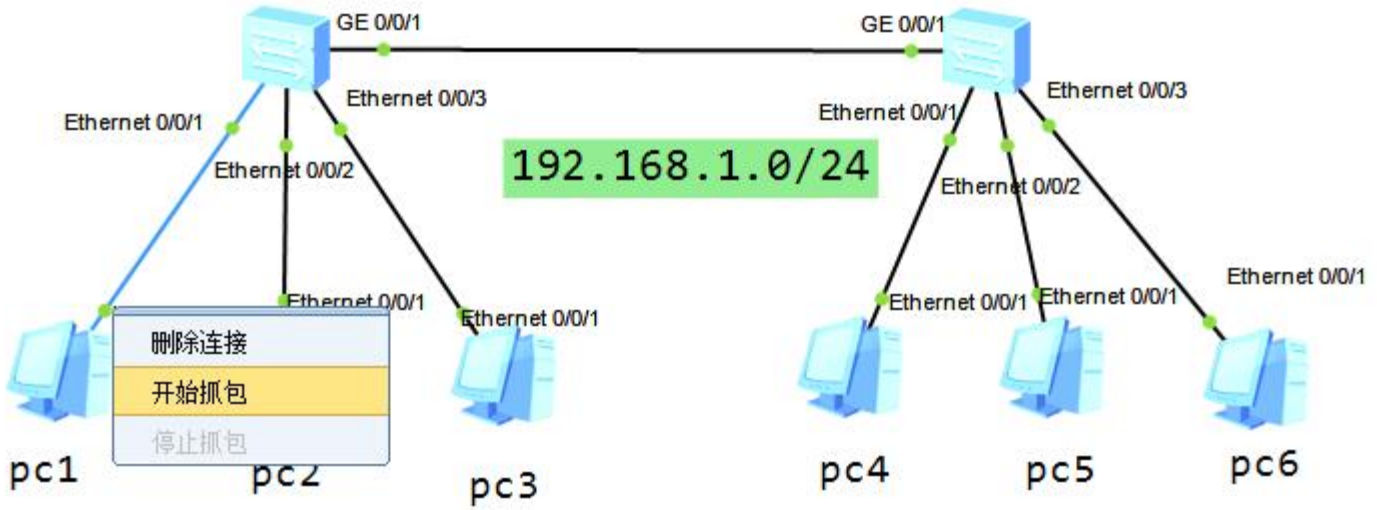
01 ARP 报文结构分析

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。

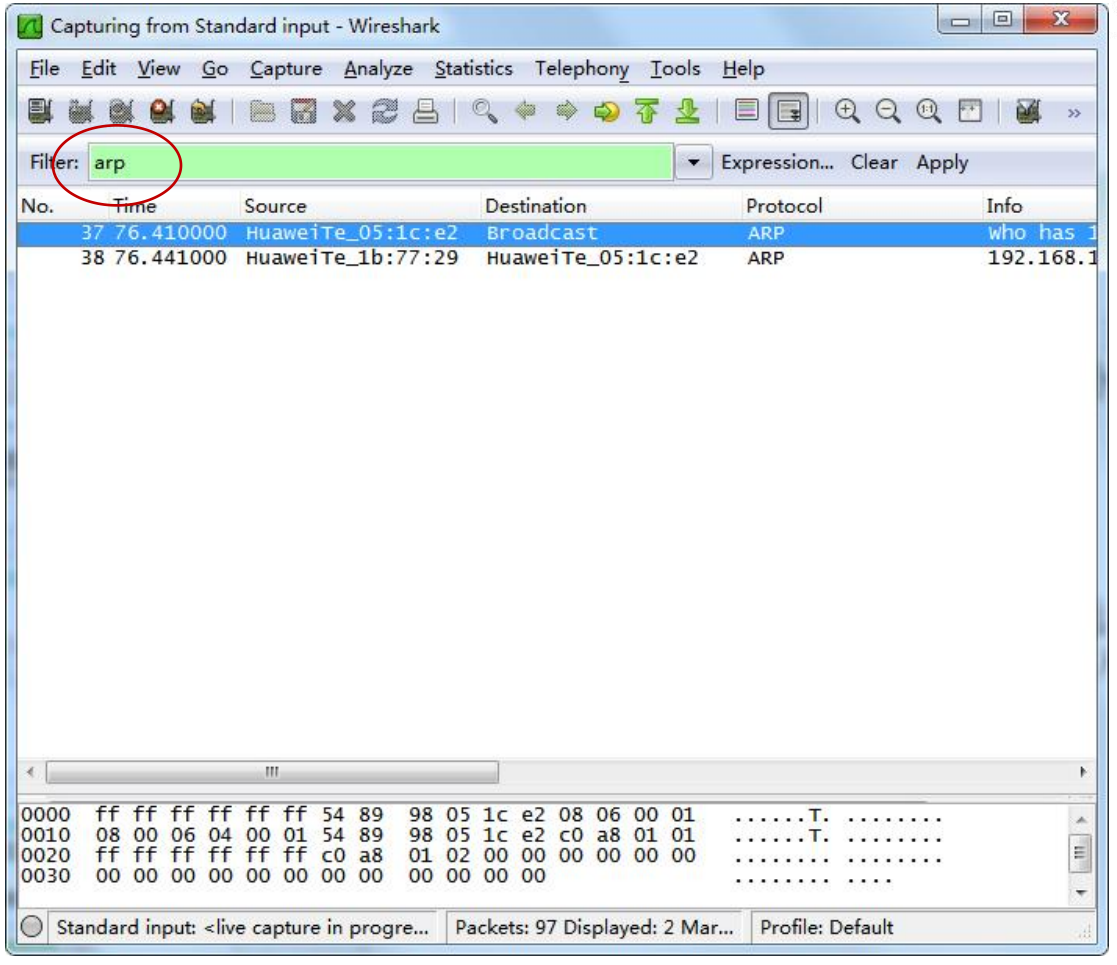


01 ARP 报文结构分析

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

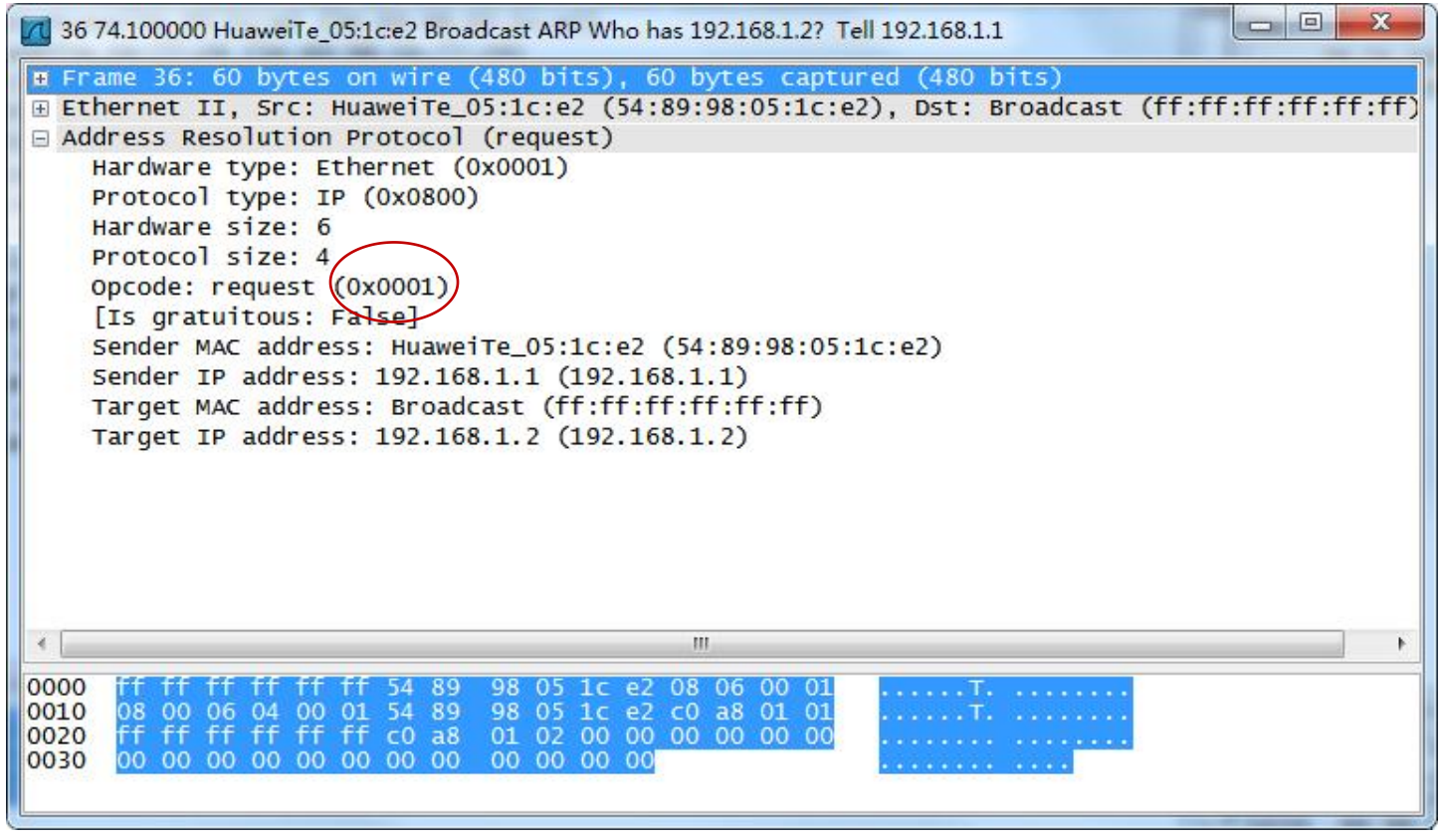
步骤 4：在Wireshark 上筛选出 PC1 的 ARP 报文
在 Wireshark 的过滤器中输入“arp”，查看PC1 收发的 ARP 报文。



01 ARP 报文结构分析

步骤 05：分析PC1 发出的ARP 请求报文结构

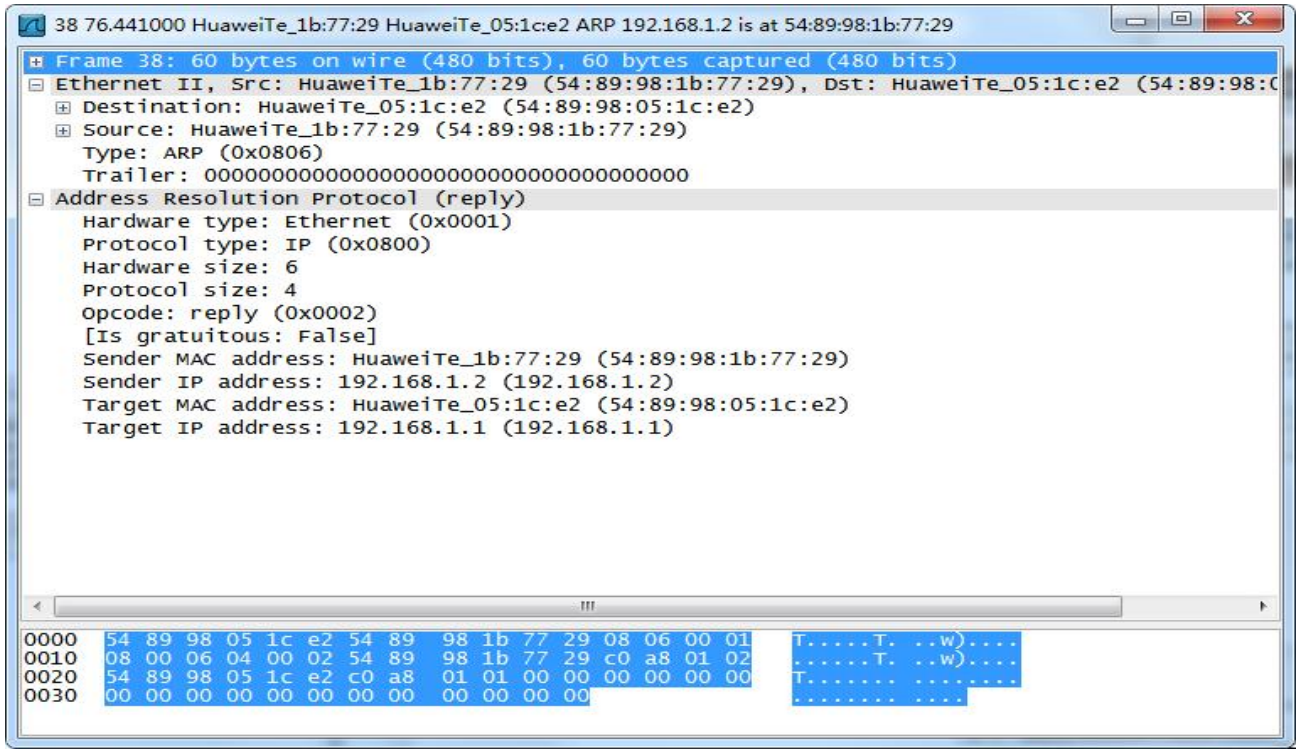
在Wireshark 中选择任意一条 ARP 请求报文进行详细分析，如图所示，将分析结果填写到实验报告表1-1。



01 ARP 报文结构分析

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。



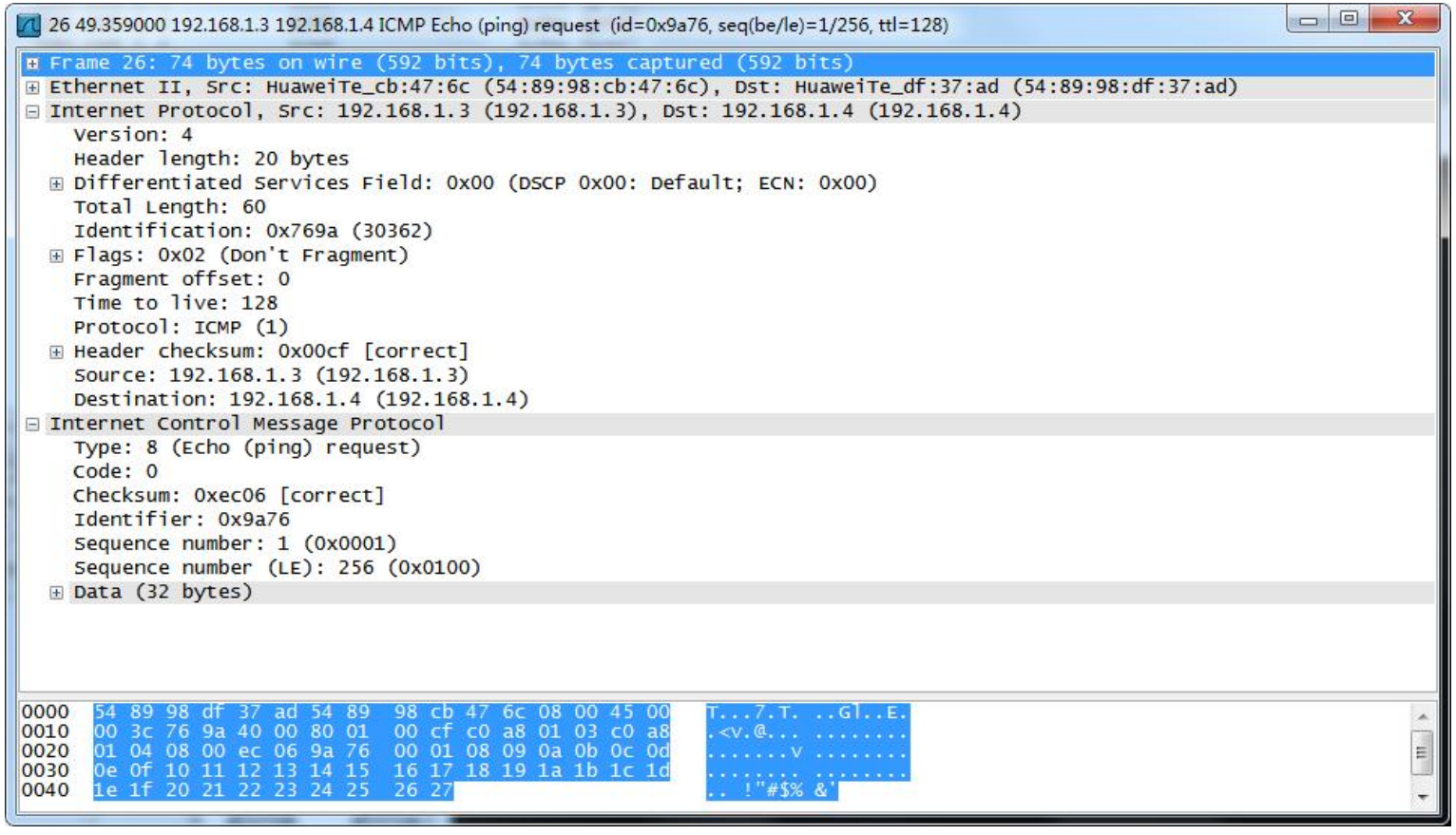
步骤 07：对比分析ARP 请求报文和响应报文结构

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

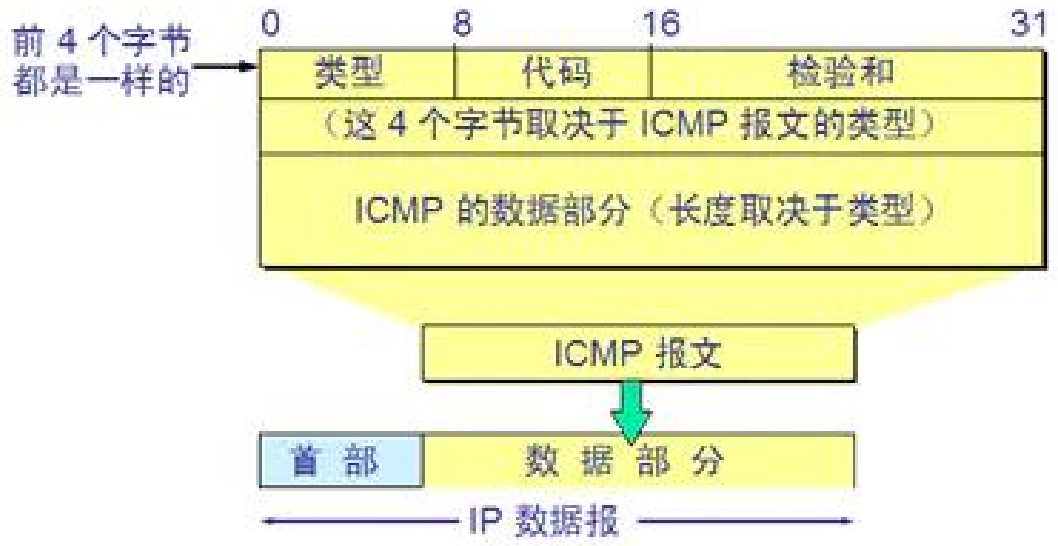
step1： 进入PC3然后执行ping指令pingPC4:

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：



02 ICMP 报文结构分析

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		

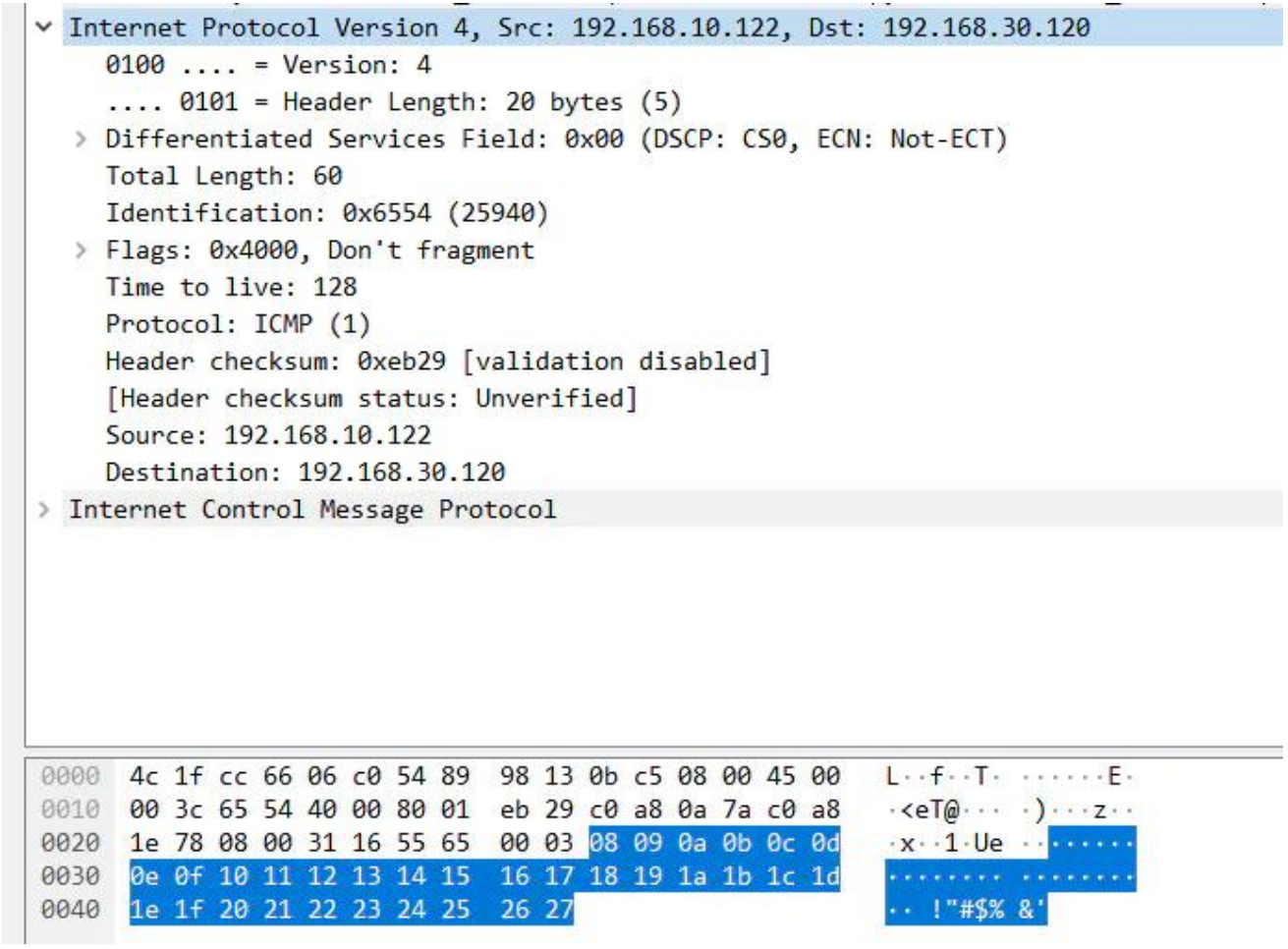
表 2-1

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。



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。

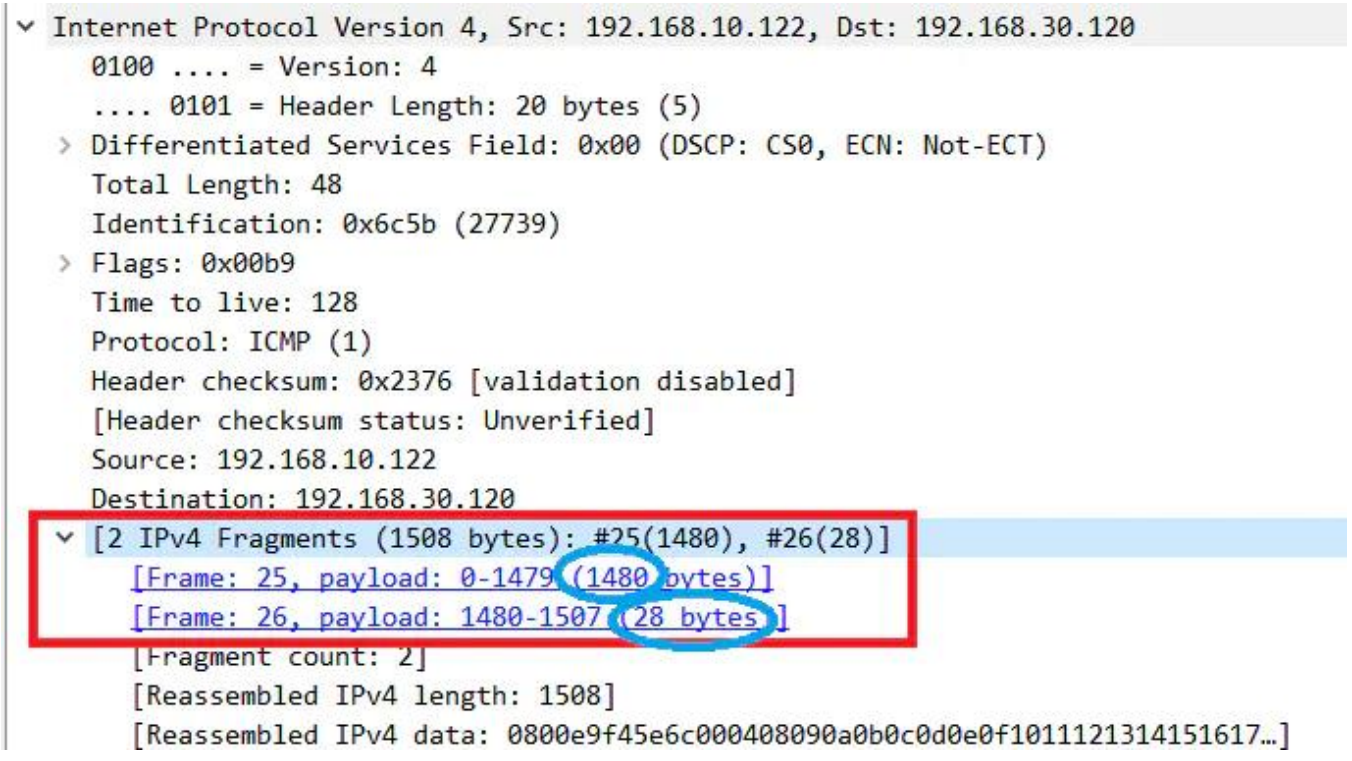
step1：进入PC3然后执行ping指令pingPC4，指定传输的数据为1500字节，进行IP分片分析。

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。



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。

完成实验，并填写实验报告。