**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 数据链路层和网络层协议分析 指导教师 潘冰

实验项目编号 实验项目类型 实验地点

学生姓名 孙靖 学号 2019053750

学院 智能科学与工程/人工智能产业学院 系 专业 信息安全

实验时间 年 月 日 午～ 月 日 午

1. **实验目的**
2. 理解链路层、网络层主要协议格式，以及协议的工作原理
3. 理解网关和子网掩码概念
4. 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程
5. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。

**二、实验内容**

1. 用嗅探器捕获数据包。
2. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
3. 分析PING、TRACERT、ARP命令的工作过程
4. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。

**三、实验原理**

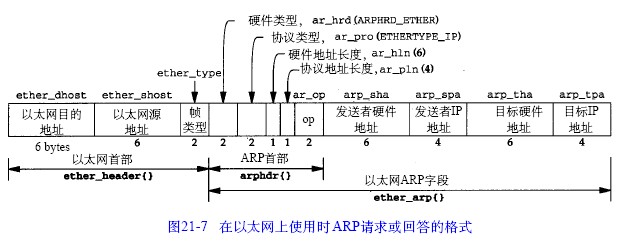
**1、网络嗅探器**

Wireshark是一个网络数据包分析软件。通过该软件可以获取网络数据包，并能进行统计分析网络数据包数据。运行Wireshark时需要将网卡设为**混合模式**。

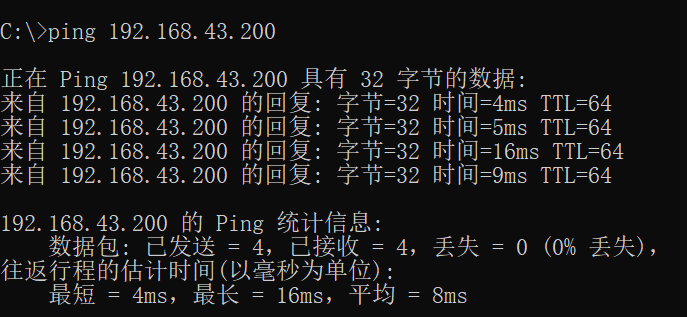
如果在交换环境里对其他主机进行嗅探，需要对交换机端口进行映射。

**2、协议**

**以太网上使用的ARP协议格式**



1. **实验步骤**
2. 安装Wireshark
3. 以太网协议分析



1.Header Length:IPv4的首部长度。

2.Differentiated Services Field（区分服务）:用来获得更好的服务， 用来指定特殊的数据包处理方式。

3.Total Length:指首部和数据的总长度。

4.Identification：IPv4在存储器中维持一个计数器，每产生一个数据包，计数器加一，把值赋给该字段。

5.Flags：目前只有两位有意义。最低位为1表示后面“还有分片”的数据报，为0表示这已经是最后一个数据片；中间一位为1表示“不能分片”，为0才允许分片。

片偏移：13位，较长的分组在经过通信链路中因为分组过大进行分片，分片后在原分组中的相对位置。片偏移以8字节为偏移单位

6.Time to Live（生存时间）：表示数据包在网络中的寿命，英文缩写是TTL（Time To Live），功能是“跳数限制”。

7.Protocol：指出此数据包携带数度的协议。

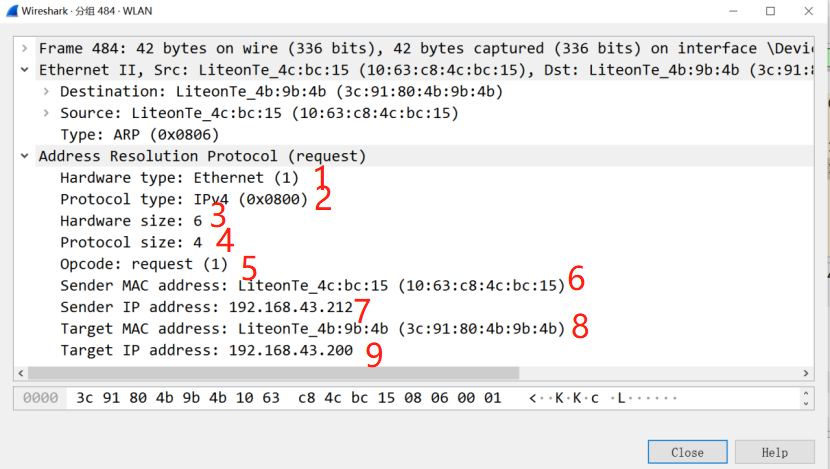
8.Header checksum（首部效验和）：数据包每经过一个路由器，路由器都要重新计算一下首部检验和，若首部未发生变化，则此结果必为0，于是就保留这个数据报。这个字段只检验数据报的首部，但不包括数据部分。

9.Source：发送数据包方IPv4地址。

10.Destinatio：接受方IPv4地址。

选项字段：1字节到40字节不等。长度可变，支持排错，测量，安全等措施

1. ARP协议分析



(1).Hardware type（网卡类型）：以太网（Ethernet）是1。我们常见的网络都是以太网

(2).Protocol type：查询中提供的网络地址的类型，IPv4是0x0800。

(3).Harware size：网卡地址长度，以太网网卡是6字节。

(4).Protocol size：查询中提供的网络地址的的长度，IPv4是4字节。

(5).Opcode：查询包值为1，响应包值为2。

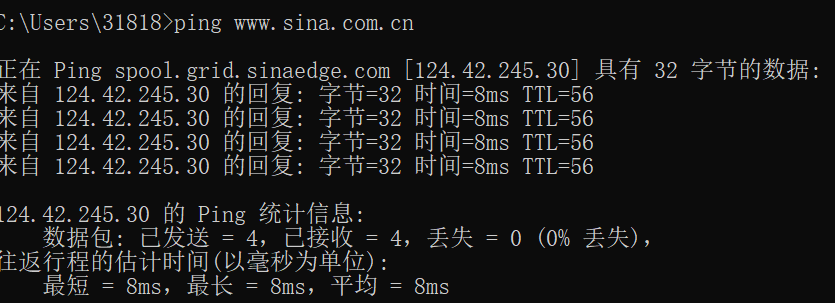
(6).Sender MAC address：发送者的Mac地址。

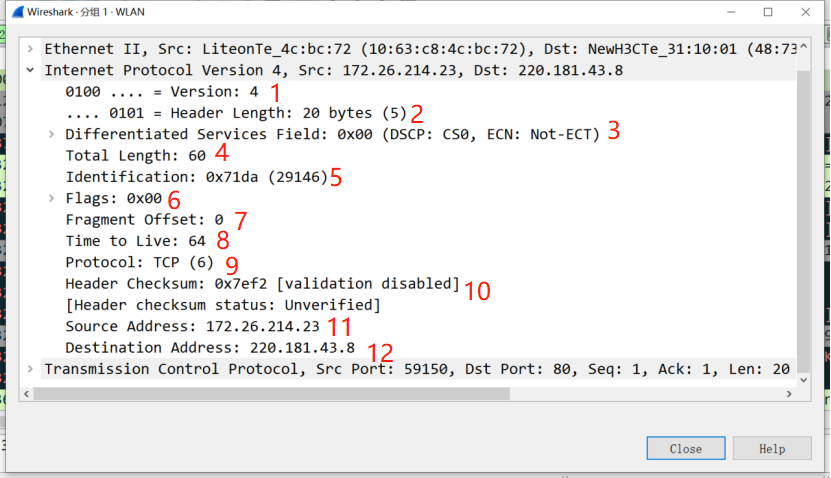
(7).Sender IP address：发送者的IP地址。

(8).Target MAC address：接收者的Mac地址，指向性查询包是MAC地址表中记录的mac，广播性查询包是00:00:00:00:00:00。（注意区分ARP头和Eth头，指向性查询包Eth头的dst mac是MAC地址表中记录的mac，而广播性查询包是ff:ff:ff:ff:ff:ff）。

(9).Target protocol address：要查询目标的mac地址的ip。

4、IP协议分析





(1).版本(4bit)。ip报文中，版本占了4位，用来表示该协议采用的是那一个版本的ip，相同版本的ip才能进行通信。

(2).首部长度(4bit)。该字段表示整个ip包头的长度，其中数的单位是4字节。即二进制数0000-1111（十进制数0-15），其中一个最小长度为0字节，最大长度为60字节。一般来说此处的值为0101，表示头长度为20字节。

(3).区分服务(8bit)。该字段用来获得更好的服务，在旧标准中叫做服务类型，但实际上一直未被使用过。1998 年这个字段改名为区分服务。只有在使用区分服（DiffServ）时，这个字段才起作用。在一般的情况下都不使用这个字段。

(4).总长度(16bit)。该字段指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 65535 字节。总长度必须不超过最大传送单元 MTU。

(5).标识(16bit)。标识(identification)占 16 位，它是一个计数器，用来产生数据报的标识。

(6).标志(3bit)。标志(flag)占 3 位，目前只有前两位有意义。标志字段的最低位是 MF (More Fragment)。MF=1 表示后面“还有分片”。MF=0 表示最后一个分片。标志字段中间的一位是 DF (Don't Fragment) 。只有当 DF=0 时才允许分片。

(7).片偏移(13 bit)。该字段指出较长的分组在分片后某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。

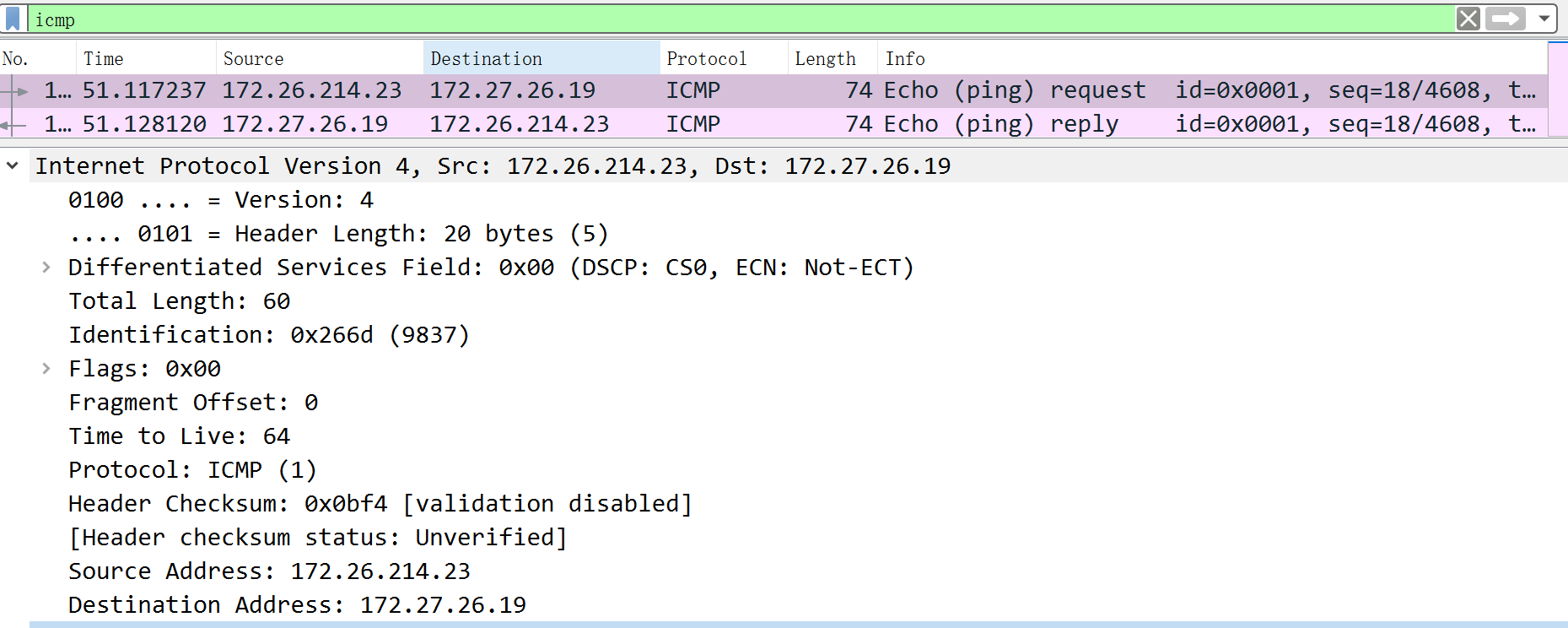
(8).生存时间(8 bit)。记为 TTL (Time To Live)数据报在网络中可通过的路由器数的最大值。

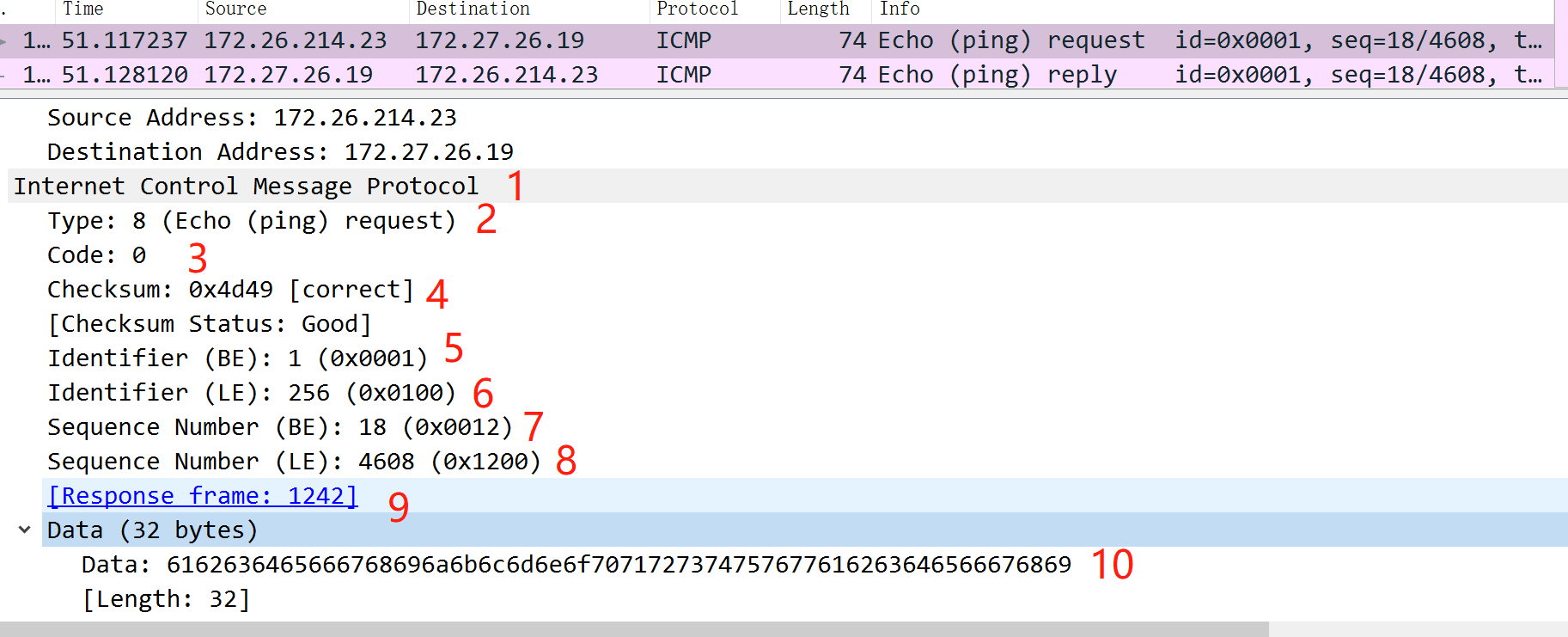
(9).协议(8 bit)。该字段指出此数据报携带的数据使用何种协议以便目的主机的 IP 层将数据部分上交给哪个处理过程。

(10).首部检验和(16 bit)。该字段只检验数据报的首部不检验数据部分。

(11).源地址/目的地址(32bit)。

1. ICMP协议分析





(1).ICMP协议

(2).请求报文类型

(3).请求报文代码

(4).校验和

(5).标识符BE

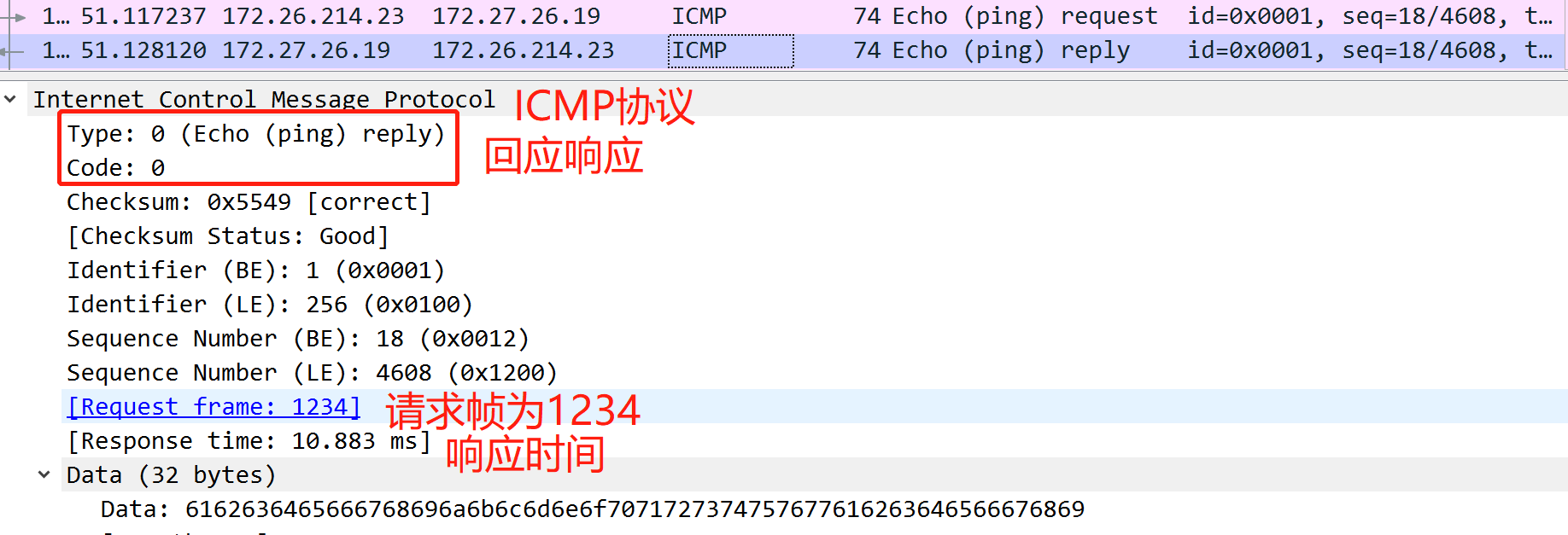
(6).标识符LE

(7).序列号BE

(8).序列号LE

(9).响应帧为1242

(10).数据



1. **思考**

1、为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

ping127。0.0.1的地址数据包根本就没到网口，所以抓不到，ping本机应该能收到。

2、在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

Request timed out：

　　（1） 对方已关机，或者网络上根本没有这个地址：比如在上图中主机A中PING 192.168.0.7 ,或者主机B关机了，在主机A中PING 192.168.0.5 都会得到超时的信息。

　　（2）对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的，当然不存在也是返回超时的信息。

　　（3）对方确实存在，但设置了ICMP数据包过滤（比如防火墙设置）。

(4）错误设置IP地址

Destination host Unreachable：

　　（1） 对方与自己不在同一网段内，而自己又未设置默认的路由，比如上例中A机中不设定默认的路由，运行Ping 192.168.0.1.4就会出现“Destination host Unreachable”。

　　（2）网线出了故障