实验3 Wireshark 软件使用与协议分析

3.1-----ARP协议分析

一．实验目的

学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包；掌握以太网 MAC 帧的基本结构，掌握 ARP 协议的特点及工作过程。

二．实验内容

使用 Wireshark 抓取局域网的数据包并进行分析：

1. 学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。
2. 观察 MAC 地址：了解 MAC 地址的组成，辨识 MAC 地址类型。
3. 分析以太网帧结构：观察以太网帧的首部和尾部，了解数据封装成帧的原理。
4. 分析 ARP 协议：抓取 ARP 请求和应答报文，分析其工作过程。

三．实验原理

3.1 Wireshark 简介

Wireshark 软件是目前全球使用最广泛的开源网络数据包分析工具（前身为 Ethereal），由 Gerald Combs 编写并于 1988 年获开源许可发布。网络数据包分析是指进入网络通信系统、捕获和解码网络上实时传输数据以及搜集统计信息的过程。通过 Wireshark 对网络数据进行分析，我们能够了解网络是如何运行的、数据包是如何被转发的、应用是如何被访问的；能够分析各层网络协议的性能、掌握通信主体的运行情况，确认带宽分配和时延大小、查看应用的快慢并改进优化，识别网络中存在的攻击或恶意行为、解决网络异常和故障。Wireshark 可以在 Windows、Linux 和 macOS 操作系统中运行，具备友好的图形界面、丰富的统计及图表分析功能。

3.2 以太网 MAC 帧格式

本实验基于使用最广泛的有线局域网（以太网 Ethernet II）， 以太网的帧结构如 表1.1–1所示。其中，MAC 地址（Media Access Control Address，媒体存取控制位址）或称物理地址（Physical Address），用于在网络中标识网卡。MAC 地址的长度为 48 位 (6 个字节)，通常表示为 12 个 16 进制数，如：00-16-EA-AE-3C-40。其中前 3 个字节的 16 进制数 00-16-EA 代表网络硬件制造商的编号、即组织唯一标志符 (OUI)，它由 IEEE 分配；而后 3 个字节的 16 进制数 AE-3C-40 代表该制造商所生产的某个网络产品 (如网卡) 的系列号。

表 1.1-1

前导字符	目的MAC地址	源 MAC 地址	类型	IP 数据报	帧校验
8 字节	6 字节	6 字节	2 字节	46-1500 字节	4 字节

3.3 ARP 协议及数据报格式

地址解析协议（Address Resolution Protocol，ARP），主要作用是将 IP 地址解析为 MAC 地址。当某主机或网络设备要发送数据给目标主机时，必须知道对方的网络层地 址（即 IP 地址），而且在数据链路层封装成帧时，还必须有目标主机（或下一跳路由器） 的 MAC 地址。本实验重点观察最简单的情形：同一个网段内，

主机 A 要向主机 B 发送信息时，ARP 解析的过程（主机 A 和 B 不在同一网段的情况请参阅课本相关内容）。

3.4 实验方法及手段

使用 Wireshark 软件在有线局域网中捕捉相关网络操作的数据包，运用观察对比、 计算验证、分析统计等方法，掌握以太网 MAC 帧和 IP 数据报的结构以及 ARP 协议的 工作原理。

四．实验条件

PC 机一台，连入局域网； Wireshark 软件，建议 3.0 以上版本。

五．实验步骤

5.1 WireShark 基本使用

1. 通过 Wireshark 官网下载最新版软件，按默认选项安装。
2. 运行 Wireshark 软件，程序界面会显示当前的网络接口列表，双击要观察的网络接口，开始捕捉数据包，Wireshark 软件选择网络接口的界面如图1.1–2所示。
3. 点击工具栏上的红色方块按钮停止捕捉。
4. 菜单、工具栏、状态栏和主窗口如图1.1–3所示，可以根据需要通过菜单“视图” 以及“编辑/首选项/外观”的相关选项对基本设置进行更改。例如图1.1–4中的语 言、字体缩放、颜色、布局等项目。
5. 使用“显示过滤器”可以方便地从捕获的数据包中筛选出要观察的数据包。显示 过滤器支持若干的过滤选项：源 MAC、目的 MAC、源 IP、目的 IP、TCP/UDP 传输协议、应用层协议（HTTP, DHCP）、源端口 Port、目的端口 Port 等。在显示过滤器栏中输入过滤表达式（更详细的显示过滤语法可以查看 WireShark 的官方文档 1），例如下面的命令：

```
arp //显示 arp 协议报文，例如图1.1–5
ip.src == a.b.c.d && icmp //显示源地址为 a.b.c.d 的 icmp 报文
```

6. 通过主菜单“文件”/“导出特定分组”（如图1.1–6），可以保存捕获的网络数据 （也可以先选中某些包，只保存部分数据）。
7. 如果只想捕捉特定的数据包，可以使用菜单“捕获”/“捕获过滤器”选定想要 的类型（如图1.1–7）。例如，选择“IPv4 only”，Wireshark 只抓取 ipv4 类型的数 据包。Wireshark 过滤器官方文档提供了更加全面详细的语法和常用示例 2。
8. Wireshark 还提供了丰富的统计功能供用户选用，如图1.1–8。更多文档可以查询 Wireshark 使用帮助。

5.2 观察 MAC 地址

以太网帧IG/LG位解释-Wireshark

启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关和 ping 同网段的一台主机，分析本机发出的数据包。重点观察以太网帧的 Destination 和 Source 的 MAC 地址，辨识 MAC 地址类型，解读 OUI 信息、I/G 和 G/L 位。

OUI（Organizationally Unique Identifier）信息是指 MAC 地址的前三个字节。这三个字节表示设备制造商的标识符。OUI 信息可以帮助你确定设备的制

I/G 位（Individual/Group）表示数据包的目的地。如果 I/G 位设置为“1”，则表示数据包的目的地是单个设备；如果 I/G 位设置为“0”，则表示数据包的目的地是一组设备。IG位区分MAC地址是个人地址还是团体（因此是IG）地址。换句话说，0的IG位表示这是一个单播MAC地址，1的IG位表示多播或广播地址。

G/L 位（Global/Local）表示 MAC 地址的范围。如果 G/L 位设置为“1”，则表示 MAC 地址是全局唯一的；如果 G/L 位设置为“0”，则表示 MAC 地址是本地管理的。LG位（有时也称为UL位）和IG位都位于每个MAC地址中最重要的字节中，其中IG位是该字节中最小的位，LG位是该字节中第二小的显著位。

```
ip.src == a.b.c.d && icmp //显示源地址为 a.b.c.d 的 icmp 报文

Frame 2701: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on
interface en0, id 0

Ethernet II,
Src: Apple_7b:91:fc (f4:d4:88:7b:91:fc),
Dst: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
    Destination: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
        Address: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
    Source: Apple_7b:91:fc (f4:d4:88:7b:91:fc)
        Address: Apple_7b:91:fc (f4:d4:88:7b:91:fc)
        .... ..0. .... .... .... .... = LG bit: Globally unique address
(factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address
(unicast)
    Type: IPv4 (0x0800)

Internet Protocol Version 4,
Src: 192.168.3.48,
Dst: 192.168.3.1

Internet Control Message Protocol
```

5.3 分析以太网的帧结构

选择其中一个数据包，点击 Ethernet II 展开（图1.1–9），查看 MAC 帧的各个字段。

前导字符	目的MAC地址	源 MAC 地址	类型	IP 数据报	帧校验
8 字节	6 字节	6 字节	2 字节	46-1500 字节	4 字节

```
0000   b0 cc fe 03 dd 5a f4 d4 88 7b 91 fc 08 00 45 00   .....Z...{....E.
------目的MAC地址6B-------;---源MAC地址6B----;类型2B;
0010   00 54 a3 e1 00 00 40 01 4f 46 c0 a8 03 30 c0 a8   .T....@.OF...0..
0020   03 01 08 00 66 a1 18 8a 00 00 63 a6 72 70 00 03   ....f.....c.rp..
0030   b7 b7 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040   16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
```

```
0050   26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060   36 37                                            67
```

5.4 ARP 协议分析

1. 使用 arp –d 命令（其语法见图1.1–10），清空本机的 ARP 缓存，开启 Wireshark， ping 本机的同网段地址，在显示过滤器条框中输入“arp”，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

```
❯ sudo arp -a -d
Password:
192.168.3.1 (192.168.3.1) deleted
192.168.3.44 (192.168.3.44) deleted
192.168.3.49 (192.168.3.49) deleted
192.168.3.66 (192.168.3.66) deleted
192.168.3.90 (192.168.3.90) deleted
192.168.3.93 (192.168.3.93) deleted
192.168.3.95 (192.168.3.95) deleted
192.168.3.98 (192.168.3.98) deleted
192.168.3.104 (192.168.3.104) deleted
192.168.3.105 (192.168.3.105) deleted
192.168.3.107 (192.168.3.107) deleted
192.168.3.255 (192.168.3.255) deleted
224.0.0.251 (224.0.0.251) deleted
239.255.255.250 (239.255.255.250) deleted
```

ARP 报文结构示意图

0 - 7	8 - 15	16 - 23	24 - 31
硬件类型		协议类型	
硬件地址长度	协议长度	操作码	（请求为1，响应为2）
源硬件地址			
源协议地址			
目的硬件地址			
目的协议地址			

- 硬件类型：指明了发送方想知道的硬件接口类型，以太网的值为 1。
- 协议类型：表示要映射的协议地址类型。IP 地址的类型值为 0x0800。
- 硬件地址长度和协议地址长度：分别指出硬件地址和协议地址的长度，以字节为单位。在以太网中，它们的值分别为 6 和 4。
- 操作码（op）：用来表示这个报文的类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4。

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
```

```
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_7b:91:fc (f4:d4:88:7b:91:fc)
    Sender IP address: 192.168.3.48
    Target MAC address: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
    Target IP address: 192.168.3.1

Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
    Sender IP address: 192.168.3.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.3.48
```

2. 使用 arp -d 命令，清空本机的 ARP 缓存。开启 Wireshark，ping 与本机网段不同的 IP 地址或域名，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

```
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_7b:91:fc (f4:d4:88:7b:91:fc)
    Sender IP address: 192.168.3.48
    Target MAC address: HuaweiDe_03:dd:5a (b0:cc:fe:03:dd:5a)
    Target IP address: 192.168.3.1

Internet Protocol Version 4, Src: 39.156.66.10, Dst: 192.168.3.48
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable
Transport (0)
    Total Length: 84
    Identification: 0x179f (6047)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 52
    Protocol: ICMP (1)
    Header Checksum: 0x418c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 39.156.66.10
```

```
    Destination Address: 192.168.3.48
```

六. 思考题 实验心得与体会

> 使用了显示过滤器后，Wireshark 的抓包工作量会减少吗?

不会

> MAC 帧的长度和 IP 数据报的长度有怎样的关系？请用你的数据记录进行验证。

MAC 帧长度为 14 字节，IP 数据报 20 字节

> ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的 ARP 报文有何不同，为什么?

当一台主机在发送数据包时，无论是向局域网内的其他主机还是向局域网外的主机发送数据包，都会产生 ARP 报文。在发送数据包之前，主机需要确定对方主机的物理地址，因此会发送 ARP 报文来请求对方的物理地址。在 ARP 报文中，局域网内的主机之间交换的是 IP 地址和物理地址的映射关系，而局域网外的主机之间交换的是网关的 IP 地址和物理地址的映射关系。

3.2-----IP与ICMP分析

一．实验目的

IP 和 ICMP 协议是 TCP/IP 协议簇中的网络层协议，在网络寻址定位、数据分组转 发和路由选择等任务中发挥了重要作用。本实验要求熟练使用 Wireshark 软件，观察 IP 数据报的基本结构，分析数据报的分片；掌握基于 ICMP 协议的 ping 和 traceroute 命令及其工作原理。

二．实验内容

启动 Wireshark，捕捉网络命令执行过程中本机接受和发送的数据报。

1. 执行 ping 命令，观察 IP 数据报和 ICMP 询问报文的结构：通过 Wireshark 监视 器观察捕获流量中的 ICMP 询问报文和 IP 数据报的结构。注意比较 ICMP 请求 帧与回应帧，及其 IP 头部数据字段的异同。
2. 改变 ping 命令的参数，观察 IP 数据报分片：更改 ping 命令参数 MTU，使其发 出长报文以触发 IP 数据报分片，再观察 IP 数据报的结构变化。
3. 执行 Traceroute 命令，观察 ICMP 差错报文的结构，并分析其工作原理：使用 Linux 操作系统提供的 traceroute 命令（或者 Windows 系统提供的 tracert 命令）， 捕获和分析该命令所产生的 IP 数据报，特别注意相关的 ICMP 差错报文。结合 捕获的具体数据，画出命令执行过程中数据交互的示意图，掌握 traceroute 的工 作原理。

三．实验原理

3.1 IP 协议及数据报格式

网际互连协议（Internet Protocol，IP），是 TCP/IP 体系中的网络层协议，可实现大规 模的异构网络互联互通，为主机提供无连接的、尽力而为的数据包传输服务。在网际协 议第 4 版（IPv4）中，IP 数据报是一个可变长分组，包括首部和数据两部分 (如图1.2–1)。 首部由 20～60 字节组成，包含与路由选择和传输有关的重要信息，其各字段意义如下：

1. 版本（4 位）：该字段定义 IP 协议版本，所有字段都要按照此版本的协议来解释。
2. 首部长度（4 位）：该字段定义数据报协议头长度，表示协议首部具有 32 位字长 的数量，最小值为 5，最大值为 15。
3. 服务（8 位）：该字段定义上层协议对处理当前数据报所期望的服务质量，并对 数据报按照重要性级别进行分配。前 3 位为优先位，后面 4 位为服务类型，最后 1 位没有定义。这 8 位可用于分配优先级、延迟、吞吐量以及可靠性。
4. 总长度（16 位）：该字段定义整个 IP 数据报的字节长度，包括协议首部和数据， 其最大值为 65535 字节。
5. 标识（16 位）：该字段包含一个整数，用于标识当前数据报。当数据报分片时， 标识字段的值被复制到所有的分片中。
6. 标记（3 位）：该字段由 3 位字段构成，其中最低位（MF）控制分片：若存在下 一个分片则值为 1；否则置 0 代表该分片是最后一个。中间位（DF）指出数据报 是否可进行分片，若置 1 则不允许该数据报进行分片。第三位即最高位保留不 使用，值为 0。
7. 分片偏移（13 位）：该字段指出数据分片在源数据报中的相对位置，以 8 字节为 长度单位。
8. 生存时间（8 位）：该字段是计数器，转发该数据报的路由器依次减 1 直至减少为 0。
9. 协议（8 位）：该字段指出在 IP 层处理后，由哪种上层协议接收该数据报。
10. 头部校验和（16 位）：该字段帮助确保 IP 协议头的正确性。计算过程是先将校 验和字段置为 0，然后将整个头部每 16 位划分为一部分，并将各部分相加，其计算结果取反码，填入校验和字段中。
11. 源地址（32 位）：源主机的 IP 地址。
12. 目的地址（32 位）：目标主机的 IP 地址。

0 - 3	4 - 7	8 - 15	16 - 31
版本	首部长度	服务	总长度
标识	标记		分片偏移(19-31)
生存时间	协议	头部校验和	
源地址			
目的地址			
选项字段（长度可变）			填充（24-31）
数据			

一个 IP 包从源主机传输到目标主机可能需要经过多个传输媒介不同的网络。每种 网络对数据帧都设置了一个最大传输单元 (MTU) 的限制（例如以太网的 MTU 是 1500 字节）。因此，当路由器在转发 IP 包时，如果数据包的大小超过了出口链路网络的 MTU 时，需将对该 IP 数据报进行分片，才能在目标链路上顺利传输。每个 IP 分片将独立传 输，直到所有分片都到达目的地后，目标主机才会把他们重组成一个完整的 IP 数据报。在 IP 数据报的分片与重组过程中，以下三个首部字段发挥了重要作用：

1. 标记的后两位：最低位记为 MF（More Fragment），MF = 1 代表还有后续分片， MF = 0 表示此为原始数据报的最后分片。次低位 DF（Don't Fragment），用来控 制数据报是否允许分片。DF = 1 表示该数据报不允许分片；DF = 0 允许分片。
2. 标识符：用于目的主机将 IP 数据报的各个分片重装成原来的数据报。
3. 片偏移：以 8 字节为单位，目的主机在重装 IP 数据报时需要根据该字段提供偏 移量进行排序。这是因为数据分片的独立传输使各分片的到达顺序难以确定。

3.2 ICMP 协议及报文格式

因特网控制报文协议（Internet Control Message Protocol，ICMP），用于 IP 主机、路由器之间传递控制消息。控制消息是指网络是否连通、主机是否可达、路由是否可用等网络本身的控制管理消息，对网络正常运行起着重要的作用。

ICMP 报文的类型可以分为 ICMP 差错报文和 ICMP 询问报文两种（其结构如图1.2–2）。ICMP 差错报告报文主要有终点不可达、源站抑制、超时、参数问题和路由重定向 5 种。ICMP 询问报文有回送请求和应答、时间戳请求和应答、地址掩码请求和应答以 及路由器询问和通告 4 种。其常见的类型与代码如表1.2–1所示。

本实验涉及以下两个常用网络命令，都属于 ICMP 协议的典型应用。

表 1.2-1 ICMP 各类型报文的格式

类型	代码	描述(Description)	查询类(Query)	差错类(Error)
0	0	Echo Reply 回送应答	√	×
3	1	Host Unreachable 主机不可达	×	√
3	2	Protocol Unreachable 协议不可达	×	√
3	3	Port Unreachable 端口不可达	×	√
3	4	Fragmentation Needed and Don't Fragment was Set 分片需要但设置了不分片比特	×	√
8	0	Echo Request 回送请求(Ping Request)	√	×
11	0	TTL equals 0 during transit 传输期间生存时间为 0	×	√

ping 命令，是测试网络最有效的工具之一。它是由主机或路由器执行 ping 命令 向一个特定的目的主机发送一份 ICMP 回显请求（Echo request）报文，并等待 其返回 ICMP 回显应答（Echo Reply）。ping 命令可以检测网络的连通性，简单 估测数据报的往返时间（Round Trip Time），确定是否有数据包丢失或损坏，从而帮助分析网络故障。ping 命令格式和常用参数罗列如下：

```
# ping [-t] [-al [-n count〕 [-1 length] [-f] [-i tt1] [-v tos]
# [-r count〕 [-s count〕 [-j computer-list]
# [-k computer-list]
# [-w timeout] destination-list

-a 将地址解析为计算机名。
-n count 发送 count 指定的 ECHO 数据包数。默认值为 4。
-1 length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是
65,527。
-f 在数据包中发送“不要分片”标志，避免数据包被路由上的网关分片。
-i tt1 将“生存时间”字段设置为 tt1 指定的值。
```

3.3 实验方法和手段

1. 使用 Wireshark 软件，捕获本机在 ping 和 traceroute 网络命令执行过程中接收和 发出的全部数据流量。

2. 合理设置过滤条件，观察 IP 数据报和 ICMP 报文，着重分析报文首部和内容变 化，从而掌握协议的工作原理。
3. 调整 ping 命令的参数，观察并分析 IP 数据报分片情况。
4. 结合所捕获的数据报，画出 traceroute 命令过程中数据交互示意图。

四．实验条件

装有 Wireshark 软件的 PC 机一台，处于局域网环境。 参考资料：

- J.F Kurose and K.W. Ross, Wireshark Lab: ICMP v8.0
- Wireshark 官方过滤器语法指导书
- IP 协议的 RFC

五．实验步骤

5.1 ping 命令

本机（示例 IP 为 192.168.1.251）启动 Wireshark 软件，选择要监听的网络接口（如 eth0、wlan0）；然后在终端发起网络命令：ping IP 地址/域名。

1. 在 Wireshark 监视器中设置过滤条件。例如图1.2–3设置过滤条件为 icmp，则显 示出所捕获的 ICMP 数据包。

2. 点击 Internet Protocol Version 4 展开（如图1.2–4），查看 IP 数据报，特别观察 IP 数据报的首部字段及其内容。

```
Internet Protocol Version 4, Src: 192.168.3.1, Dst: 192.168.3.48
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable
Transport (0)
    Total Length: 84
    Identification: 0x94d0 (38096)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x5e57 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.3.1
    Destination Address: 192.168.3.48
```

3. 点击 Internet Control Message Protocol 展开（如图1.2–5），查看 ICMP 报文，并解释回显（Echo Request 和 Echo Reply）报文的首部字段。

ICMP 报文是 Internet 控制消息协议的缩写，是用于在 IP 网络中传输控制消息的协议。ICMP 报文包括很多种类型的报文，其中最常见的是回显（Echo）报文。

回显报文分为两种：回显请求（Echo Request）报文和回显应答（Echo Reply）报文。回显请求报文是发送方发送的报文，回显应答报文是接收方发送的报文。

- 类型（Type）字段：用于表示报文类型，其中回显请求报文的类型值为 8，回显应答报文的类型值为 0。
- 代码（Code）字段：用于表示报文类型的更细分的信息，对于回显报文来说，该字段的值通常为 0。
- 校验和（Checksum）字段：用于对报文进行校验，以确保报文在传输过程中没有被破坏。
- 标识符（Identifier）字段：用于唯一标识一个回显请求报文，以便回显应答报文能够与其对应。
- 序列号（Sequence Number）字段：用于标识回显请求报文的序列号，同时也可以用来确定回显应答报文与回显请求报文的对应关系。
- 数据（Data）字段：回显报文中的数据部分，通常包含一些简单的信息或者是回显请求报文中的数据的副本。

回显报文通常用于测试主机之间的网络连通性，也可用于测量网络延迟。当发送方发送回显请求报文时，接收方会收到该报文并回复回显应答报文。发送方收到回显应答报文后，就可以计算出回显请求报文到达接收方的时间，从而测量网络延迟。

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x7c83 [correct]
    [Checksum Status: Good]
    Identifier (BE): 8371 (0x20b3)
    Identifier (LE): 45856 (0xb320)
    Sequence Number (BE): 2 (0x0002)
    Sequence Number (LE): 512 (0x0200)
    [Response frame: 1550491]
    Timestamp from icmp data: Dec 24, 2022 15:35:10.090222000 CST
    [Timestamp from icmp data (relative): 0.000091000 seconds]
    Data (48 bytes)

Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8483 [correct]
    [Checksum Status: Good]
    Identifier (BE): 8371 (0x20b3)
    Identifier (LE): 45856 (0xb320)
    Sequence Number (BE): 2 (0x0002)
    Sequence Number (LE): 512 (0x0200)
    [Request frame: 1550490]
    [Response time: 1.947 ms]
    Timestamp from icmp data: Dec 24, 2022 15:35:10.090222000 CST
    [Timestamp from icmp data (relative): 0.002038000 seconds]
    Data (48 bytes)

0000   f4 d4 88 7b 91 fc b0 cc fe 03 dd 5a 08 00 45 00   ...{.......Z..E.
0010   00 54 94 d0 00 00 40 01 5e 57 c0 a8 03 01 c0 a8   .T....@.^W......
0020   03 30 00 00 84 83 20 b3 00 02 63 a6 ab ae 00 01   .0.... ...c.....
0030   60 6e 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   `n..............
0040   16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
```

```
0050   26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060   36 37                                            67
```

4. 清空 Wireshark 监控器，重新发起网络命令（如图1.2–6）：`ping [IP 地址/域名] –l #length`，并解释对比前后两次执行 ping 命令的结果。其中，`–l #length` 确定 echo 数据报的长度为 #length，其默认值为 32 字节，且小于 65,527 字节。

当比较两次执行 ping 命令的结果时，如果使用了 "-l #length" 参数，并且指定的长度不同，那么两次执行的结果可能会有所差异。这是因为，回显数据报的长度越大，网络中传输的数据就越多，因此可能会影响网络的性能。例如，如果第一次执行 ping 命令时使用的是默认的 32 字节长度，而第二次执行 ping 命令时使用了长度为 64 字节的回显数据报，那么第二次执行的结果可能会比第一次执行的结果差。

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x9eeb [correct]
    [Checksum Status: Good]
    Identifier (BE): 4278 (0x10b6)
    Identifier (LE): 46608 (0xb610)
    Sequence Number (BE): 5 (0x0005)
    Sequence Number (LE): 1280 (0x0500)
    [Request frame: 1567879]
    [Response time: 3.458 ms]
    Timestamp from icmp data: Dec 24, 2022 15:45:00.409067000 CST
    [Timestamp from icmp data (relative): 0.003762000 seconds]
    Data (3992 bytes)
```

5. 可以多次改变 #length 的大小（例如 1000 字节、2000 字节和 4000 字节），观察 IP 数据报何时会分片？请解释 IP 数据报分片的原因和具体情况。提示：请先确认该网络的 MTU，可在 Wireshark 记录中查找“IPv4 fragments”项目。

如下方例子所示，在1480, 2960 处进行了分片，分片的原因是 IP 数据报的长度超过了网络的 MTU，因此需要将 IP 数据报分片，以便在网络中传输。

```
[3 IPv4 Fragments (4008 bytes): #1567781(1480), #1567782(1480),
#1567783(1048)]
    [Frame: 1567781, payload: 0–1479 (1480 bytes)]
    [Frame: 1567782, payload: 1480–2959 (1480 bytes)]
    [Frame: 1567783, payload: 2960–4007 (1048 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 4008]
    [Reassembled IPv4 data:
0800b57d10b6000363a6adfa00061f5d08090a0b0c0d0e0f10111213141516171819 1a1b…]
```

IP 数据报是用于在网络中传输数据的数据包，它是由 IP 首部和数据部分组成的。IP 首部中包含有关数据报的源地址、目的地址、生存时间（TTL）、标识、分片偏移量等信息。数据部分则是数据报中的具体内容，可以包含任意的数据。如果一个数据报的长度超过了网络中所能支持的最大长度，那么该数据报就需要进行分

片（Fragmentation）。分片是指将一个大的数据报分成多个较小的数据报，分别发送到目的地。分片后的每一个数据报的 IP 首部都会有一个分片偏移量字段，用于表示该数据报在原始数据报中的相对位置。

IP 数据报分片的原因有以下几种：

- 网络中传输的数据报最大长度有限：不同的网络技术和协议有着不同的最大数据报长度限制，如果一个数据报的长度超过了这个限制，就需要进行分片。
- 网络中的路由器不支持较大的数据报：在网络中传输数据时，数据报可能会经过多个路由器，如果某个路由器不支持较大的数据报，就需要将数据报进行分片。
- 网络环境中存在丢包：在网络中传输数据时，由于各种原因，数据报可能会丢失。为了减少丢包的可能性，可以将数据报进行分片，并分别发送多个数据报，从而减少丢包的影响。

5.2 traceroute 命令

本机（示例 IP 为 192.168.1.251）启动 Wireshark 软件，选择要监听的网络接口（如 eth0、wlan0）；然后在终端发起网络命令：traceroute IP 地址/域名。

1. 启动 Wireshark 软件，选择要监听的网络接口，设置过滤条件 icmp（如图1.2–7）。
2. 在终端中使用 traceroute 命令，目的主机是外网的一台设备（如图1.2–8，示例 IP 为 210.34.0.1）。
3. 点击 Internet Control Message Protocol 展开，查看 ICMP 差错报文，观察并解释 ICMP 报文结构和字段内容。

```
icmp.type == 3

Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xdfdc [correct]
    [Checksum Status: Good]
    Unused: 00000000
    Internet Protocol Version 4, Src: 192.168.3.48, Dst: 192.168.3.98
    User Datagram Protocol, Src Port: 3722, Dst Port: 3722

ICMP 差错报文的类型包括：类型 3（目的不可达）、类型 4（源站超时）、类型 5（路由器重定向）和类型 11（TTL 超时）。可以根据需要修改过滤器来查看不同类型的 ICMP 差错报文。
```

ICMP 报文包括两部分：首部和数据部分。

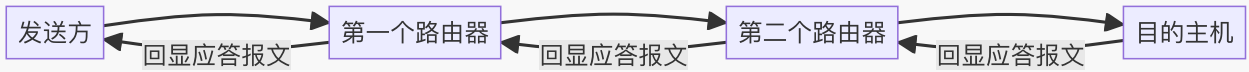
ICMP 首部包括类型、代码、校验和三个字段。类型字段指定了 ICMP 报文的类型，代码字段提供了进一步的信息，校验和字段用于校验 ICMP 报文的完整性。

ICMP 报文的数据部分则取决于 ICMP 报文的类型。例如，回显请求（Echo Request）报文包含标识符、序列号和数据三个字段，回显应答（Echo Reply）报文则包含标识符、序列号和数据三个字段。差错报文则包含有关错误的更多信息。

1. 结合 ICMP 报文记录画出数据交互示意图，并描述 tracert 工作原理。

在终端中使用 traceroute 命令时，traceroute 会向目的主机发送一个回显请求报文，并记录发送时间。目的主机会收到回显请求报文并发送一个回显应答报文，traceroute 会收到回显应答报文并记录响应时间。根据

发送时间和响应时间的差值，traceroute 就可以计算出数据包在网络中传输的时间。



1. 发送方向目的主机发送回显请求报文
2. 第一个路由器收到回显请求报文，并向目的主机发送回显请求报文
3. 第二个路由器收到回显请求报文，并向目的主机发送回显请求报文
4. 目的主机收到回显请求报文，并发送回显应答报文
5. 第二个路由器收到回显应答报文，并向发送方发送回显应答报文(英文：Echo Reply)
6. 第一个路由器收到回显应答报文，并向发送方发送回显

六．实验心得与体会

本次实验学习了网络工具，如 ping、traceroute、Wireshark 等，这些工具可以帮助我们检测网络连通性、排查网络故障、分析网络数据包等。了解了网络协议的工作原理，如 TCP/IP 协议、ICMP 协议等。我们学习了网络协议的报文格式，如 IP 数据报、TCP 报文段、ICMP 报文等。通过这些知识，我们可以更好地理解网络数据在传输过程中的处理流程，以及网络故障时的原因分析。