计算机学院 计算机网络 课程实验报告

实验题目： ICMP		学号：202200130048
日期：5.7	班级： 6	姓名： 陈静雯

Email：1205037094@qq.com

实验方法介绍：

在本实验中，我们将探讨 ICMP 协议的几个方面:由 Ping 程序程序生成的 ICMP 消息;由 Traceroute 程序生成的 ICMP 消息;ICMP 报文的格式和内容。

实验过程描述：

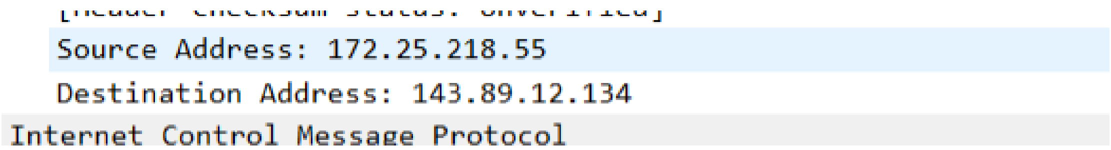
1. ICMP 和 Ping 程序
2. ICMP 和 Traceroute
3. 额外学分

结论分析：

1. What is the IP address of your host? What is the IP address of the destination host?

Host：172.25.218.55

Dst：143.89.12.134



```
    [Header checksum status: Unverified]
    Source Address: 172.25.218.55
    Destination Address: 143.89.12.134
Internet Control Message Protocol
```

2. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP 是 Internet 控制消息协议，它属于 TCP/IP 模型中的网络层协议，而非传输层协议。端口号是传输层概念，主要用于标识在同一台主机上不同应用程序之间的通信通道。ICMP 的主要职责是传递网络层的控制信息和差错报告，比如“目的地不可达”、“超时”或者“回显请求”（通常用于 ping 命令）等消息。由于这些控制信息和差错报告并不涉及到具体应用层的服务，也不需要在不同应用程序之间进行复用，因此 ICMP 报文结构中并没有设计源端口号和目的端口号字段。

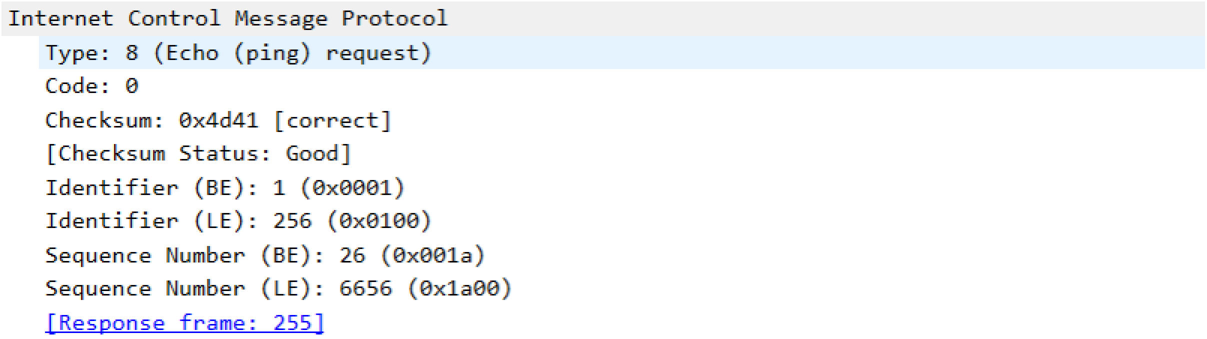
ICMP 报文包含类型（Type）和代码（Code）字段，这些字段联合起来定义了 ICMP 报文的具体用途，比如类型 8 和代码 0 表示 Echo Request（ping 请求），类型 0 和代码 0 表示 Echo Reply（ping 响应）。这样，通过类型和代码，接收方就能明确了解 ICMP 报文的意图，而无需借助端口号来进行进一步的区分。

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Type：8，code：0，

other field：checksum、identifier、sequence number，

各占两个字节，共 6 个 bytes



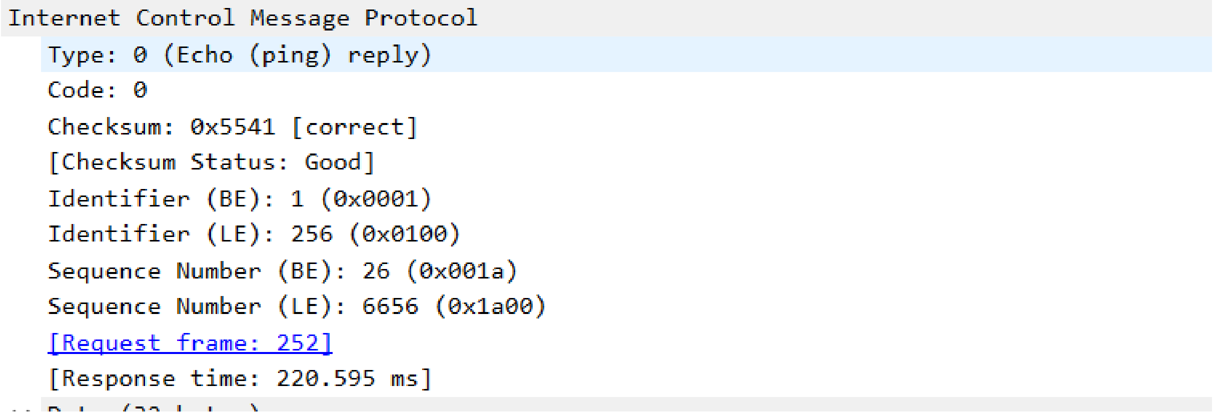
```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d41 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 26 (0x001a)
    Sequence Number (LE): 6656 (0x1a00)
    [Response frame: 255]
```

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Type：0，code：0，

other field：checksum、identifier、sequence number，

各占两个字节，共 6 个 bytes

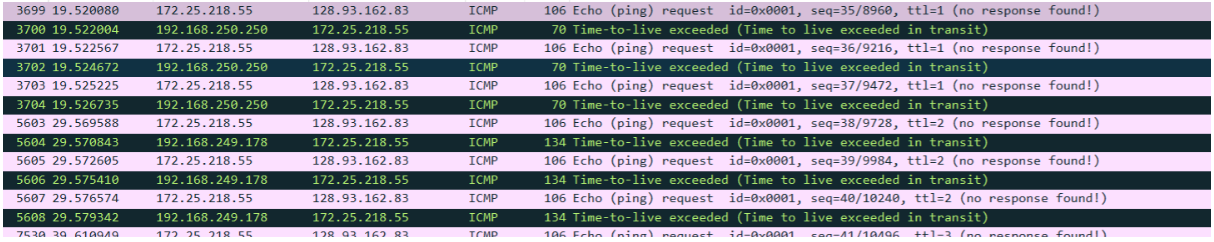


```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5541 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 26 (0x001a)
    Sequence Number (LE): 6656 (0x1a00)
    [Request frame: 252]
    [Response time: 220.595 ms]
```

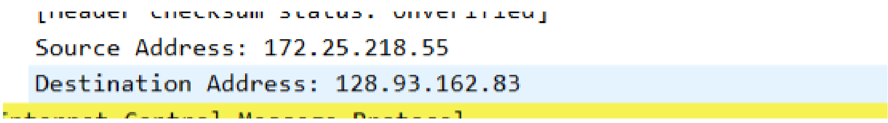
5. What is the IP address of your host? What is the IP address of the target destination host?

Host：172.25.218.55

Dst:128.93.162.83



```
3699 19.520080   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=35/8960, ttl=1 (no response found!)
3700 19.522004   192.168.250.250   172.25.218.55    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
3701 19.522567   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=36/9216, ttl=1 (no response found!)
3702 19.524672   192.168.250.250   172.25.218.55    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
3703 19.525225   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=37/9472, ttl=1 (no response found!)
3704 19.526735   192.168.250.250   172.25.218.55    ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
5603 29.569588   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=38/9728, ttl=2 (no response found!)
5604 29.570843   192.168.249.178   172.25.218.55    ICMP    134 Time-to-live exceeded (Time to live exceeded in transit)
5605 29.572605   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=39/9984, ttl=2 (no response found!)
5606 29.575410   192.168.249.178   172.25.218.55    ICMP    134 Time-to-live exceeded (Time to live exceeded in transit)
5607 29.576574   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=40/10240, ttl=2 (no response found!)
5608 29.579342   192.168.249.178   172.25.218.55    ICMP    134 Time-to-live exceeded (Time to live exceeded in transit)
7530 39.610949   172.25.218.55     128.93.162.83    ICMP    106 Echo (ping) request  id=0x0001, seq=41/10496, ttl=3 (no response found!)
```



```
    [Header checksum status: Unverified]
    Source Address: 172.25.218.55
    Destination Address: 128.93.162.83
Internet Control Message Protocol
```

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

ICMP 和 UDP 是两种不同的协议，它们在 IP 协议栈中的层级和功能各不相同。ICMP 作为网络层协议，其报文直接封装在 IP 数据包中，IP 头部的协议字段（Protocol field）用于标识承载的数据属于哪种上层协议。对于 ICMP，该字段的值通常是 1（即十进制的

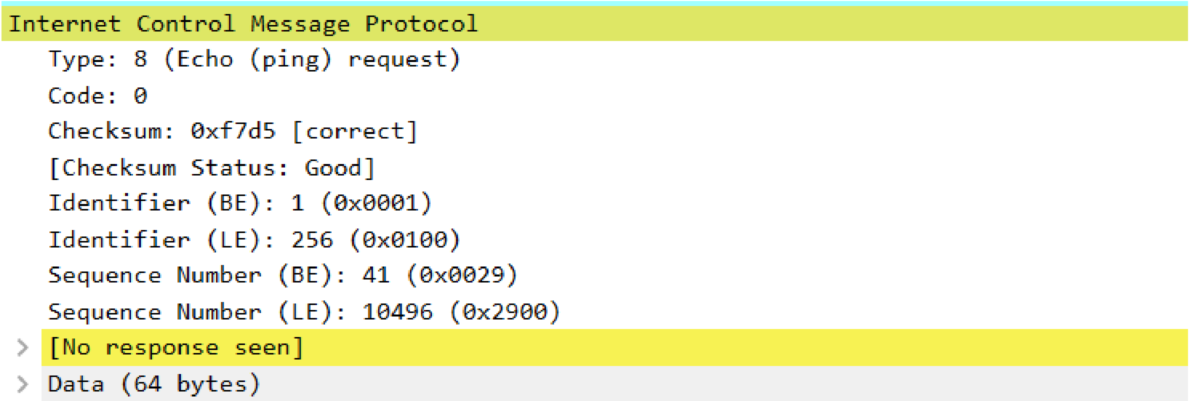
01)。

UDP 数据包是由传输层的 UDP 协议负责封装和发送的，当 UDP 数据包被进一步封装到 IP 层时，IP 头部的协议字段会标记为 17，这是 UDP 协议的协议号。

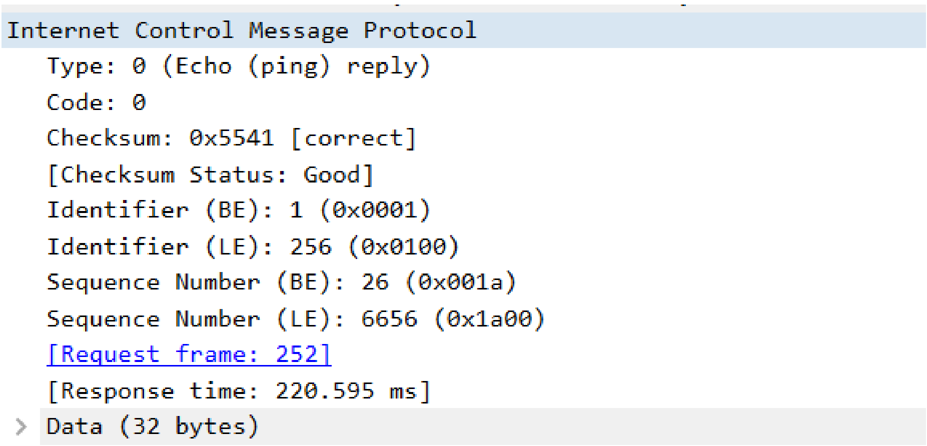
所以，如果通过 ICMP 来探测或涉及 UDP 通信的情况那么涉及 UDP 的 IP 数据包的协议号应当是 17，而非代表 ICMP 的 01。

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

有不同，type 不同，还多了一栏 no response seen



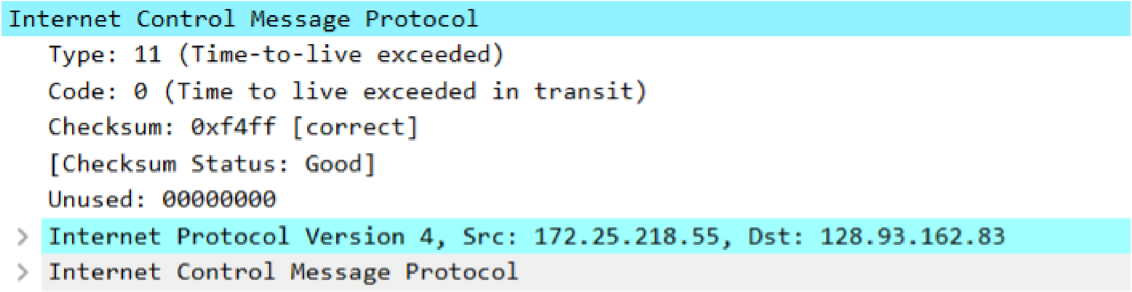
```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 41 (0x0029)
    Sequence Number (LE): 10496 (0x2900)
  > [No response seen]
  > Data (64 bytes)
```



```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5541 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 26 (0x001a)
    Sequence Number (LE): 6656 (0x1a00)
    [Request frame: 252]
    [Response time: 220.595 ms]
  > Data (32 bytes)
```

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

Unused，icmp 里还有一层 icmp 和 ipv4



```
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.25.218.55, Dst: 128.93.162.83
  > Internet Control Message Protocol
```

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

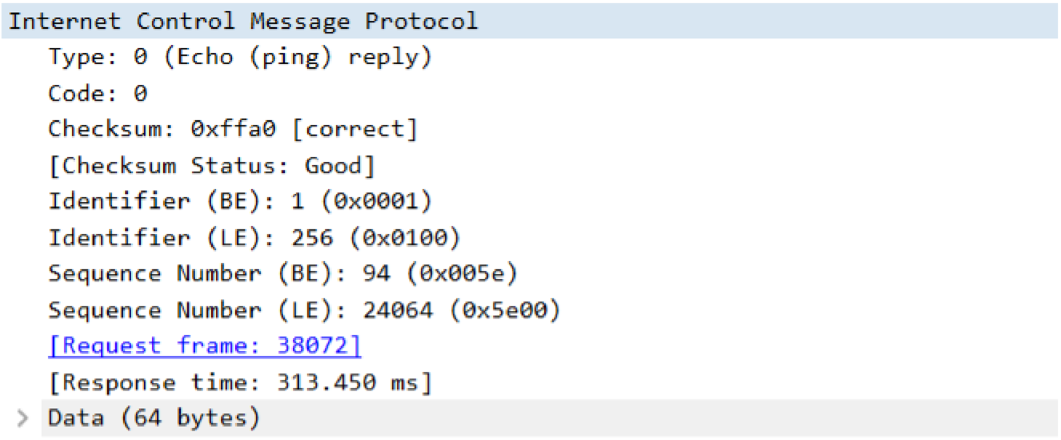
类型和代码：Echo Reply 报文的类型字段值为 0，代码字段值通常为 0，而 ICMP 错误

报文如“目的地不可达”类型字段值为 3，伴随不同的代码值来指示具体错误原因，如代码 1 表示网络不可达，代码 2 表示主机不可达等。

目的和用途：Echo Reply 报文是对之前发送的 Echo Request（如 ping 命令产生的请求）的响应，表明通信路径畅通且目的主机可达。而 ICMP 错误报文是在数据包传输过程中出现问题时生成的，用于通知发送方数据包未能成功送达的原因。

报文内容：Echo Reply 报文通常包含接收到的 Echo Request 中的某些信息，如数据负载（可能包含时间戳或其他用户自定义数据），用于确认请求并提供响应。错误报文则可能携带无法送达的数据包的 IP 头部信息，以帮助发送方识别问题所在。

发起方与响应方：Echo Reply 报文是由目标主机或路由器响应 Echo Request 而主动发送的，而错误报文则是由遇到问题的路由器或目的主机生成并返回给原始数据包的发送者。

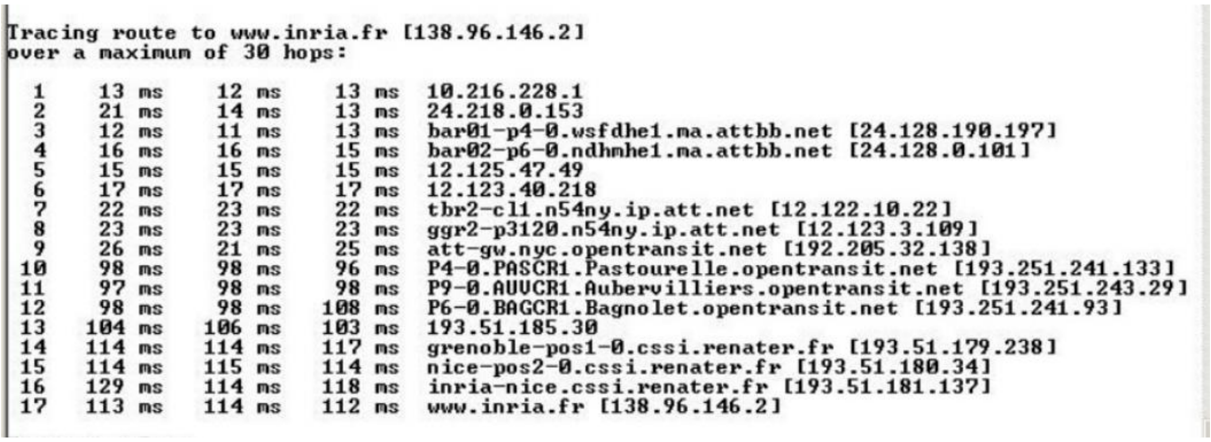


```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xffa0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 94 (0x005e)
    Sequence Number (LE): 24064 (0x5e00)
    [Request frame: 38072]
    [Response time: 313.450 ms]
  > Data (64 bytes)
```

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

从[193.251.243.29] 到[193.251.241.133]的延迟为 98 毫秒，这是整个路径中最长的延迟之一。

根据路由器名称，我们可以推测这两个路由器都属于 Open Transit Network，但它们位于不同的位置。延迟较高可能是由于物理距离造成的，也可能是由于网络连接质量或其他因素导致的。



```
Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

  1     13 ms     12 ms     13 ms  10.216.228.1
  2     21 ms     14 ms     13 ms  24.218.0.153
  3     12 ms     11 ms     13 ms  bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
  4     16 ms     16 ms     15 ms  bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
  5     15 ms     15 ms     15 ms  12.125.47.49
  6     17 ms     17 ms     17 ms  12.123.40.218
  7     22 ms     23 ms     22 ms  tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  8     23 ms     23 ms     23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  9     26 ms     21 ms     25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
 10     98 ms     98 ms     96 ms  P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 11     97 ms     98 ms     98 ms  P9-0.AUVCR1.Aubervilliers.opentransit.net [193.251.243.29]
 12     98 ms     98 ms    108 ms  P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 13    104 ms    106 ms    103 ms  193.51.185.30
 14    114 ms    114 ms    117 ms  grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 15    114 ms    115 ms    114 ms  nice-pos2-0.cssi.renater.fr [193.51.180.34]
 16    129 ms    114 ms    118 ms  inria-nice.cssi.renater.fr [193.51.181.137]
 17    113 ms    114 ms    112 ms  www.inria.fr [138.96.146.2]
```

11. 额外学分

有以下几种情况：

无响应：大多数服务只监听特定的知名端口或配置好的端口上的 UDP 连接请求。Wireshark 中只看到 UDP 请求包，而不会有对应的回复。

ICMP 端口不可达错误：目标主机收到了 UDP 数据包，但没有服务在指定的端口上监听，会返回一个 ICMP 端口不可达(Port Unreachable)错误。在 Wireshark 中，可以看到 UDP 请求之后跟着一个类型为 3 且代码为 3 的 ICMP 响应包。

结论：

1.在执行 tracert 或 traceroute 命令时，你会看到数据包到达每个路由器（或跃点）所需的时间。这些时间通常以毫秒（ms）为单位显示。如果某一步的延迟明显高于其他步骤，这可能意味着：

（1）网络拥堵：该链接上的数据流量较大，导致数据包需要等待较长时间才能通过。

（2）物理距离遥远：数据包需要经过更长的物理距离到达下一个路由器，尤其是在跨越不同地理区域时。

（3）设备性能问题：端到端链接中的某个路由器或链路可能因处理能力不足或配置不当而导致延迟增加。

（4）路由路径问题：数据包可能通过了一个非最优的路径。

2. ICMP Echo 请求报文（即 ping 查询包）通常包含以下几个关键部分：

类型（Type）：值为 8，表示这是一个 Echo Request 报文。

代码（Code）：通常为 0，对于 Echo Request 来说，代码字段辅助描述没有其他特殊信息。

校验和（Checksum）：确保报文完整性的计算值。

标识符（Identifier）：发送者设置的一个 16 位数值，用于标识发送方的进程或会话。

序列号（Sequence Number）：发送者设置的另一个 16 位数值，用于区分同一个会话中的多个 Echo Request 报文。