

我ping的一个数据包中是这样的内容，带我分析里面每一层，告诉我哪些是代表什么：

Frame 170: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
Section number: 1
Interface id: 0 (en0)
Interface name: en0
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Sep 19, 2024 14:36:18.305166000 CST
UTC Arrival Time: Sep 19, 2024 06:36:18.305166000 UTC
Epoch Arrival Time: 1726727778.305166000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.033403000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 19.881454000 seconds]
Frame Number: 170
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Apple_86:e5:d8 (9c:3e:53:86:e5:d8), Dst: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
Destination: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Source: Apple_86:e5:d8 (9c:3e:53:86:e5:d8)
.... 0. = LG bit: Globally unique address (factory default)
.... 0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 10.89.88.108, Dst: 182.61.200.7
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: 0x2a3a (10810)
000. = Flags: 0x0
0... = Reserved bit: Not set
0.. = Don't fragment: Not set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x6f65 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.89.88.108
Destination Address: 182.61.200.7
[Stream index: 9]
Internet Control Message Protocol

Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x9ace [correct]
[Checksum Status: Good]
Identifier (BE): 40228 (0x9d24)
Identifier (LE): 9373 (0x249d)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 171]
Timestamp from icmp data: Sep 19, 2024 14:36:18.305079000
CST
[Timestamp from icmp data (relative): 0.000087000 seconds]
Data (48 bytes)
Data:
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232
425262728292a2b2c2d2e2f3031323334353637
[Length: 48]

< 2/2 >



根据你提供的 ping 数据包信息，我们可以按层次逐步分析其内容。以下是每一层的详细解释：

1. 以太网层 (Ethernet II)

- **Src: Apple_86:e5 (9c:3e:53:86:e5)**: 源 MAC 地址，表示发送数据包的设备的唯一标识符。
- **Dst: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)**: 目的 MAC 地址，表示接收数据包的设备的唯一标识符。
- **Type: IPv4 (0x0800)**: 指示上层协议为 IPv4。0x0800 表示数据包承载的是 IPv4 数据。

2. 网络层 (Internet Protocol Version 4)

- **Src: 10.89.88.108**: 源 IP 地址，表示发送数据包的设备的 IP 地址。
- **Dst: 182.61.200.7**: 目的 IP 地址，表示接收数据包的设备的 IP 地址。
- **Version: 4**: IPv4 版本。
- **Header Length: 20 bytes**: IP 头部长度为 20 字节。
- **Differentiated Services Field: 0x00**: 服务类型字段，表示流量优先级和拥塞通知。0x00 表示默认服务。
- **Total Length: 84**: 数据包总长度为 84 字节。
- **Identification: 0x2a3a**: 数据包的唯一标识符，用于分片重组。
- **Flags: 0x0**: 标志字段。0x0 表示没有分片标志。
- **Time to Live: 64**: 数据包的生存时间 (TTL)，用于限制数据包的生命周期。每经过一个路由器，该值会减 1。
- **Protocol: ICMP (1)**: 上层协议为 ICMP。1 表示 ICMP 协议。
- **Header Checksum: 0x6f65**: IP 头部校验和，用于检测 IP 头部的错误。

3. 传输层 (Internet Control Message Protocol, ICMP)

- **Type: 8 (Echo (ping) request)**: ICMP 类型，8 表示 Echo 请求 (即 ping 请求)。
- **Code: 0**: ICMP 代码，0 表示没有特定代码 (仅 Echo 请求)。
- **Checksum: 0x9ace**: ICMP 校验和，用于检测 ICMP 数据的错误。
- **Identifier (BE): 40228 (0x9d24)**: 唯一标识符，用于区分不同的 ping 请求。

- **Identifier (LE): 9373 (0x249d):** 唯一标识符的低字节（小端格式）。
- **Sequence Number (BE): 0 (0x0000):** 序列号，用于区分多个 ping 请求。
- **Sequence Number (LE): 0 (0x0000):** 序列号的低字节（小端格式）。

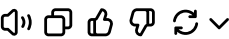
4. 数据部分 (Data)

- **Data:**
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637: 实际的负载数据部分，通常是 ping 请求的数据内容。数据部分的长度为 48 字节。

总结:

1. **以太网层:** 包含源和目的 MAC 地址，以及上层协议类型。
2. **网络层 (IP 层):** 包含源和目的 IP 地址，IP 头部信息，如总长度、标识符、TTL、协议类型等。
3. **传输层 (ICMP 层):** 包含 ICMP 类型、代码、校验和、标识符和序列号。
4. **数据部分:** 包含实际传输的数据内容。

这些信息帮助你理解数据包在网络中如何传输，并识别各层协议的作用。



```
Frame 170: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
on interface en0, id 0
  Section number: 1
  Interface id: 0 (en0)
    Interface name: en0
    Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 19, 2024 14:36:18.305166000 CST
  UTC Arrival Time: Sep 19, 2024 06:36:18.305166000 UTC
  Epoch Arrival Time: 1726727778.305166000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.033403000
seconds]
  [Time delta from previous displayed frame: 0.000000000
seconds]
  [Time since reference or first frame: 19.881454000 seconds]
  Frame Number: 170
  Frame Length: 98 bytes (784 bits)
  Capture Length: 98 bytes (784 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
前面这一部分是什么意思
```



前面的部分是Wireshark中数据包的详细描述信息，包括有关数据包捕获和解码的各种元数据。下面是对这些字段的详细解释:

Frame 170: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0

- **Frame 170:** 数据包的帧编号，是Wireshark捕获的数据包的序号。
- **98 bytes on wire (784 bits):** 数据包在网络上传输的实际字节数和比特数。
- **98 bytes captured (784 bits):** Wireshark捕获的数据包的字节数和比特数，与传输的字节数相同，表示没有丢失数据。

Section number: 1

- **Section number:** 数据包所在的抓包文件的部分编号，通常在多部分捕获文件中使用。

Interface id: 0 (en0)

- **Interface id:** 捕获数据包的接口标识符，这里是 0。
- **Interface name:** en0: 捕获数据包的接口名称，通常表示Wi-Fi接口。

Encapsulation type: Ethernet (1)

- **Encapsulation type:** 数据包的封装类型，这里是以太网 (Ethernet)，编号为 1。

Arrival Time: Sep 19, 2024 14:36:18.305166000 CST

- **Arrival Time:** 数据包到达捕获设备的时间，格式为 年月日 时分秒.微秒，时区为 CST (中国标准时间)。

UTC Arrival Time: Sep 19, 2024 06:36:18.305166000 UTC

- **UTC Arrival Time:** 数据包到达捕获设备的时间，转换为协调世界时 (UTC)。

Epoch Arrival Time: 1726727778.305166000

- **Epoch Arrival Time:** 从1970年1月1日00:00:00 UTC起的秒数，用于时间戳的内部表示。

[Time shift for this packet: 0.000000000 seconds]

- **Time shift for this packet:** 数据包的时间偏移，通常为0秒，表示数据包时间没有调整。

[Time delta from previous captured frame: 0.033403000 seconds]

- **Time delta from previous captured frame:** 与前一个捕获的数据包之间的时间差，这里是0.033403秒。

[Time delta from previous displayed frame: 0.000000000 seconds]

- **Time delta from previous displayed frame:** 与前一个显示的数据包之间的时间差，这里是0秒，表示当前数据包和上一个显示的数据包之间没有时间差异。

[Time since reference or first frame: 19.881454000 seconds]

- **Time since reference or first frame:** 自从参考帧 (通常是捕获文件的第一个数据包) 以来的时间，表示此数据包距离参考帧的时间差。

Frame Number: 170

- **Frame Number:** 数据包在捕获文件中的编号，这里是第170个数据包。

Frame Length: 98 bytes (784 bits)

- **Frame Length:** 数据包的总长度，包括以太网头和所有数据部分，长度为98字节 (784位)。

Capture Length: 98 bytes (784 bits)

- **Capture Length:** 实际捕获的数据包长度，通常等于帧长度，表示没有数据丢失。

[Frame is marked: False]

- **Frame is marked:** 数据包是否被标记。False 表示没有特别标记。

[Frame is ignored: False]

- **Frame is ignored:** 数据包是否被忽略。False 表示没有被忽略。

[Protocols in frame: eth:ethertype:ip:icmp]
]

- **Protocols in frame:** 数据包中包含的协议层次，从最底层到最上层。这里是以太网（eth）、以太网类型（ethertype）、IP（ip）、ICMP（icmp）和数据（data）。

[Coloring Rule Name: ICMP]

- **Coloring Rule Name:** 数据包在Wireshark中应用的颜色规则名称，这里是 ICMP。

[Coloring Rule String: icmp || icmpv6]

- **Coloring Rule String:** 数据包颜色规则的字符串，表示 ICMP 或 ICMPv6 协议。

这些信息帮助你了解数据包的捕获时间、数据长度、捕获的协议以及数据包的具体内容和显示设置。

```
Ethernet II, Src: Apple_86:e5:d8 (9c:3e:53:86:e5:d8), Dst:
RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
  Destination: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)
    ....0. .... = LG bit: Globally unique address (factory
default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: Apple_86:e5:d8 (9c:3e:53:86:e5:d8)
    ....0. .... = LG bit: Globally unique address (factory
default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
这一层详细分析
```



这段信息描述了以太网帧的内容。以下是对每个部分的详细分析：

**Ethernet II, Src: Apple_86:e5
(9c:3e:53:86:e5
) , Dst: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)**

这部分表示以太网帧的内容，其中包含了源和目的的MAC地址及帧类型。

Destination: RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e)

- **Destination:** 目的 MAC 地址，即数据包的目标设备的物理地址。
- **RuijieNetwor_3f:e1:1e (80:05:88:3f:e1:1e):** MAC 地址的标识符。80:05:88:3f:e1:1e 是目标设备的 MAC 地址。
- **LG bit: Globally unique address (factory default):** LG（Locally or Globally unique）位，0 表示这是一个全球唯一地址，通常是默认设置。
- **IG bit: Individual address (unicast):** IG（Individual Group）位，0 表示这是一个单播地址（即特定的唯一地址，而不是广播地址）。

**Source: Apple_86:e5
(9c:3e:53:86:e5
)**

- **Source:** 源 MAC 地址，即数据包的发送设备的物理地址。
- **Apple_86:e5
(9c:3e:53:86:e5
)**: MAC 地址的标识符。9c:3e:53:86:e5:d8 是源设备的 MAC 地址。
- **LG bit: Globally unique address (factory default):** LG 位，0 表示这是一个全球唯一地址。

- **IG bit: Individual address (unicast):** IG 位， 0 表示这是一个单播地址。

Type: IPv4 (0x0800)

- **Type:** 表示以太网帧的上层协议。 0x0800 是以太网帧中的类型字段，指示帧承载的上层协议是 IPv4。这个值告诉网络接口卡（NIC）或接收设备，接下来要解析的是 IPv4 数据包。

[Stream index: 0]

- **Stream index:** 用于标识数据流的索引。 0 表示这是第一个数据流。在Wireshark中，如果一个捕获文件中有多数据流（例如，多个TCP会话），每个数据流都会有一个唯一的索引。

总结

这一层的详细信息包括了以太网帧的基本结构：

1. **目的 MAC 地址：**表示数据包的目标设备。
2. **源 MAC 地址：**表示数据包的发送设备。
3. **类型字段：**指示上层协议，这里是 IPv4。

这些信息对于网络流量的正确路由和处理至关重要。通过分析这些字段，你可以理解数据包的传输路径以及在网络中的作用。

```
Internet Protocol Version 4, Src: 10.89.88.108, Dst: 182.61.200.7
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: 0x2a3a (10810)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x6f65 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.89.88.108
Destination Address: 182.61.200.7
[Stream index: 9]
这一层呢 是啥 详细分析
```



这部分信息是关于IPv4数据包的详细描述。下面是对每个字段的详细分析：

Internet Protocol Version 4, Src: 10.89.88.108, Dst: 182.61.200.7

这部分描述了IPv4数据包的内容。

Version: 4

- **Version:** 表示IP协议的版本号。 4 表示这是一个IPv4数据包。IPv6会用 6 表示。

Header Length: 20 bytes (5)

- **Header Length:** IP头部的长度，以字节为单位。这里是 20 bytes 。头部长度字段表示IP头部的长度，单位是32位字（即4字节）。 5 表示头部长度为5个32位字（5 × 4 = 20字节）。

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

- **Differentiated Services Field (DS Field):** 用于流量优先级和拥塞通知。0x00 表示默认服务类型。
- **DSCP: CS0:** 区分服务代码点 (DSCP), CS0 表示默认服务等级。
- **ECN: Not-ECT:** 显式拥塞通知 (ECN), Not-ECT 表示没有拥塞通知能力。

Total Length: 84

- **Total Length:** 包含IP头和数据部分的总长度, 单位为字节。这里的值 84 表示整个IP数据包的长度为84字节。

Identification: 0x2a3a (10810)

- **Identification:** 用于唯一标识IP数据包, 尤其是分片的重组。0x2a3a 是标识符的十六进制值, 10810 是其十进制值。

Flags: 0x0

- **Flags:** 标志字段, 指示是否对数据包进行分片等操作。
- **Reserved bit: Not set:** 保留位, 未设置。
- **Don't fragment: Not set:** 不分片标志, 0 表示允许分片。
- **More fragments: Not set:** 更多分片标志, 0 表示这是数据包的最后一个分片或数据包没有被分片。

Fragment Offset: 0

- **Fragment Offset:** 数据包分片的偏移量。0 表示数据包没有被分片, 或者这是第一个分片。

Time to Live: 64

- **Time to Live (TTL):** 数据包的生存时间, 表示数据包在网络中可以经过的最大路由器数量。每经过一个路由器, TTL 值会减 1。这里的 64 是初始TTL值。

Protocol: ICMP (1)

- **Protocol:** 上层协议标识符。1 表示上层协议是ICMP (Internet Control Message Protocol)。

Header Checksum: 0x6f65 [validation disabled]

- **Header Checksum:** 用于验证IP头部是否有错误的校验和。0x6f65 是校验和值, [validation disabled] 表示校验和验证被禁用。

Source Address: 10.89.88.108

- **Source Address:** 源IP地址, 即数据包的发送设备的IP地址。

Destination Address: 182.61.200.7

- **Destination Address:** 目的IP地址, 即数据包的接收设备的IP地址。

[Stream index: 9]

- **Stream index:** 数据流的索引。在Wireshark中, 数据流的索引用于标识特定的网络流或会话, 这里是 9。

总结

IPv4数据包的每个字段都提供了数据包的不同方面的信息:

1. **Version:** IP协议的版本 (IPv4)。
2. **Header Length:** IP头部的长度。
3. **Differentiated Services Field:** 服务类型字段, 用于流量优先级和拥塞控制。
4. **Total Length:** 数据包的总长度。

- 5. **Identification:** 唯一标识符，用于数据包的分片和重组。
- 6. **Flags:** 分片标志，用于数据包分片处理。
- 7. **Fragment Offset:** 分片偏移量。
- 8. **Time to Live (TTL):** 数据包的生存时间。
- 9. **Protocol:** 上层协议标识符。
- 10. **Header Checksum:** IP头部校验和。
- 11. **Source Address:** 源IP地址。
- 12. **Destination Address:** 目的IP地址。
- 13. **Stream index:** 数据流的索引。

这些字段共同决定了数据包在网络中的传输和处理方式。

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x9ace [correct]
[Checksum Status: Good]
Identifier (BE): 40228 (0x9d24)
Identifier (LE): 9373 (0x249d)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Response frame: 171]
Timestamp from icmp data: Sep 19, 2024 14:36:18.305079000
CST
[Timestamp from icmp data (relative): 0.000087000 seconds]
Data (48 bytes)
Data:
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232
425262728292a2b2c2d2e2f3031323334353637
[Length: 48]
这一层呢
```



这部分信息描述了ICMP（Internet Control Message Protocol）数据包的内容，主要用于网络诊断和错误报告。以下是对每个字段的详细分析：

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

- **Type:** ICMP消息的类型。8 表示这是一个Echo请求（ping请求），用于测试网络连接或响应时间。
- **Echo (ping) request:** 用于向目标主机发送请求，以确认目标主机是否在线以及测量响应时间。

Code: 0

- **Code:** ICMP消息的子类型。0 表示这是一个标准的Echo请求，没有附加的特定子代码。

Checksum: 0x9ace [correct]

- **Checksum:** 用于验证ICMP数据包在传输过程中是否出现错误的校验和。0x9ace 是校验和值，[correct] 表示校验和验证通过，数据包没有错误。

Identifier (BE): 40228 (0x9d24)

- **Identifier:** 用于匹配请求和响应的标识符。40228 是标识符的十进制值，0x9d24 是其十六进制值。在回显请求和回显应答中，这个值用于将请求和应答配对起来。

Identifier (LE): 9373 (0x249d)

- **Identifier (LE):** 这是标识符的低字节序表示。9373 是其十进制值，0x249d 是其十六进制值。

Sequence Number (BE): 0 (0x0000)

- **Sequence Number:** 用于标识请求的序列号，以区分多个请求。0 表示这是序列号为0的请求。

Sequence Number (LE): 0 (0x0000)

- **Sequence Number (LE):** 这是序列号的低字节序表示。0 表示序列号为0。

[Response frame: 171]

- **Response frame:** 这是对应的响应数据包的帧编号。171 表示这是响应数据包的帧编号，在这个案例中响应包的帧编号是171。

Timestamp from icmp data: Sep 19, 2024 14:36:18.305079000 CST

- **Timestamp:** 数据包中的时间戳，表示发送或接收数据包的精确时间。这个时间戳表示数据包发送的时间。

[Timestamp from icmp data (relative): 0.000087000 seconds]

- **Relative Timestamp:** 相对于捕获开始的相对时间戳，表示数据包与前一个数据包之间的时间差。0.000087000 seconds 表示相对时间差。

Data (48 bytes)

- **Data:** ICMP消息中的数据部分。这里 48 bytes 表示数据部分的长度为48字节。
 - **Data:**
08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637: 这是ICMP请求中的有效负载数据。通常用于在Ping请求中传递的数据内容。

总结

这部分数据是关于ICMP数据包的详细信息：

1. **Type:** 表示消息类型为Echo请求（ping请求）。
2. **Code:** 子类型为0，表示标准请求。
3. **Checksum:** 校验和，用于错误检测。
4. **Identifier:** 唯一标识符，用于匹配请求和响应。
5. **Sequence Number:** 序列号，用于区分多个请求。
6. **Response frame:** 响应数据包的帧编号。
7. **Timestamp:** 时间戳，表示发送或接收的时间。
8. **Data:** ICMP消息中的数据部分，用于传递实际的数据内容。

这些字段共同构成了ICMP Echo请求的详细描述，帮助确认网络连通性和测量响应时间。