IP

林宸昊 PB20000034

1.
```
Frame 42: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{28F4B2F8-01FA-4861-94AA-BAA450D5F52E}, id 0
  Interface id: 0 (\Device\NPF_{28F4B2F8-01FA-4861-94AA-BAA450D5F52E})
      Interface name: \Device\NPF_{28F4B2F8-01FA-4861-94AA-BAA450D5F52E}
      Interface description: WLAN
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 11, 2022 21:28:38.850365000 中国标准时间
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1668173318.850365000 seconds
  [Time delta from previous captured frame: 0.036961000 seconds]
  [Time delta from previous displayed frame: 0.036961000 seconds]
  [Time since reference or first frame: 3.917436000 seconds]
  Frame Number: 42
  Frame Length: 70 bytes (560 bits)
  Capture Length: 70 bytes (560 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: IntelCor_14:76:ed (34:cf:f6:14:76:ed), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
  Destination: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
      Address: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_14:76:ed (34:cf:f6:14:76:ed)
      Address: IntelCor_14:76:ed (34:cf:f6:14:76:ed)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 114.214.185.201, Dst: 202.38.64.246
  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: 56
  Identification: 0x2f80 (12160)
  Flags: 0x00
      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: 1
    > [Expert Info (Note/Sequence): "Time To Live" only 1]
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 114.214.185.201
  Destination Address: 202.38.64.246
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x34ec [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 337 (0x0151)
  Sequence Number (LE): 20737 (0x5101)
  [No response seen]
  Data (28 bytes)
```

   - IP地址：114.214.185.201

2.
```
Protocol: ICMP (1)
```

   - 协议字段与上层协议字段均为1；

3.
```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCI
Total Length: 56
```

   - header length = 20 bytes;
   - payload = total length - header length = 36 bytes;

4.
```
Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
```

   - MF = 0, Fragment offset = 0, 未分段；

5.
   - Identification，Header Checksum always changed;

6.
   - 必须保持不变：

     > *Version：通信双方使用版本必须一致；*
     >
     > *Header Length：首部长度，用于说明首部字节数且唯一确定；*
     >
     > *DSCP：默认为0，不启用分区服务；*

   - 保持不变：

     > *ECN：为0，表示非ECT能力传输；*
     >
     > *Total Length：已在抓包前固定；*
     >
     > *Fragment offset：分片偏移，相对于原始报文开头的偏移量，同一个包中不会更改；*
     >
     > *Src，Dst：源地址和目标地址作为发送接收端不会更改；*
     >
     > *Protocol：都是ICMP协议；*

   - 必须更改：

     > *Identification：用于唯一标识某个报文以及其所有分片；*
     >
     > *TTL：经过的每个路由器都会将此字段减1，等于0时不再传送直接丢弃；*
     >
     > *Header Checksum：每一次路由器都会将重新计算出的首部检验和与此比较，不一致会直接丢弃；*

7.
```
3048 63.106079     202.38.64.246        114.214.185.201      ICMP      554 Echo
```
```
> Frame 3048: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on i
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_14:76:e
v Internet Protocol Version 4, Src: 202.38.64.246, Dst: 114.214.185.201
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x44e6 (17638)
```
```
2946 60.453271     202.38.64.246        114.214.185.201      ICMP      554
```
```
> Frame 2946: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_14
v Internet Protocol Version 4, Src: 202.38.64.246, Dst: 114.214.185.201
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x44e3 (17635)
```

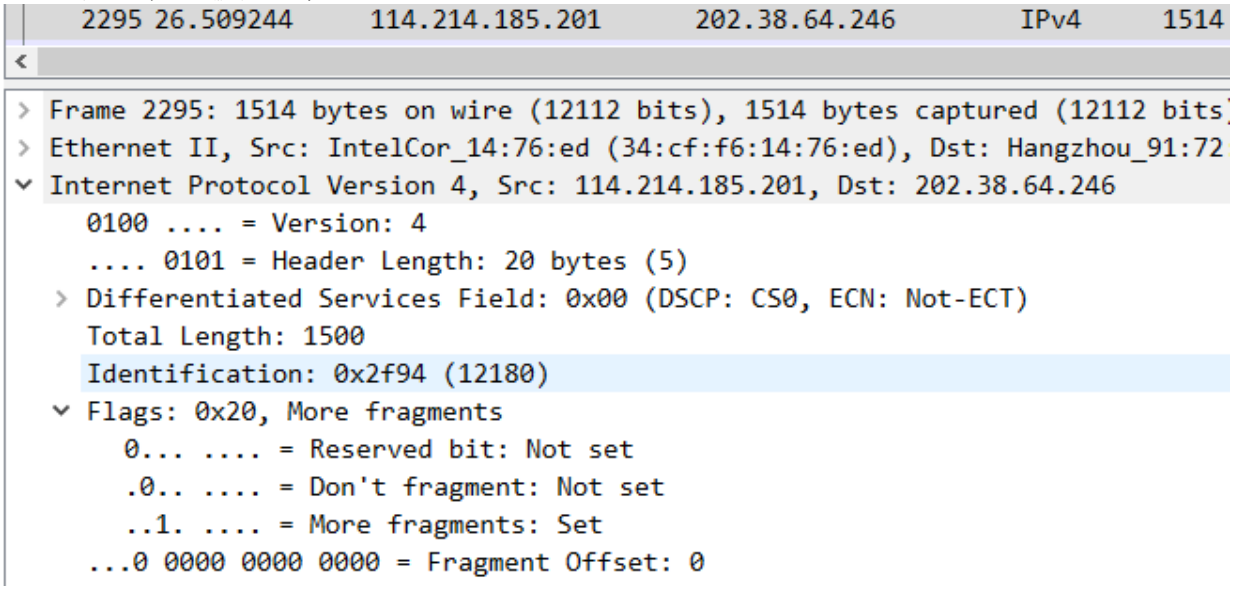
   每一个报文都有独特标识，会持续改变，使得报文可以被唯一确定；

8.

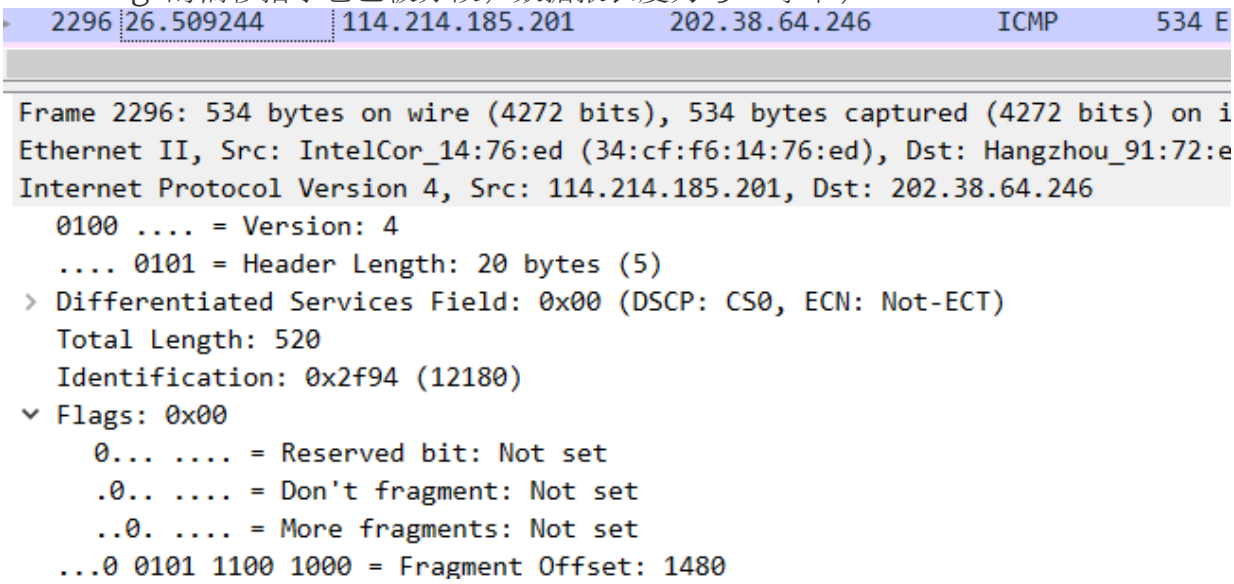
```
Identification: 0x2f92 (12178)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 254
```

9. ◦ ID字段改变，TTL字段保持不变，因为预设默认值都相同，超时代表均被扣减至0，最后一个路由器会发送icmp信息包括此TTL，因此都是一样的；
10.
```
v [2 IPv4 Fragments (1980 bytes): #2295(1480), #2296(500)]
    [Frame: 2295, payload: 0-1479 (1480 bytes)]
    [Frame: 2296, payload: 1480-1979 (500 bytes)]
    [Fragment count: 2]
```

◦ 如图，已被分段；

11. 
```
2295 26.509244     114.214.185.201      202.38.64.246        IPv4      1514
<
> Frame 2295: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: IntelCor_14:76:ed (34:cf:f6:14:76:ed), Dst: Hangzhou_91:72
v Internet Protocol Version 4, Src: 114.214.185.201, Dst: 202.38.64.246
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x2f94 (12180)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
```

◦ Flags的偏移指示它已被分段，数据报长度为1500字节；

12. 
```
2296 26.509244     114.214.185.201      202.38.64.246        ICMP      534 E

Frame 2296: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on i
Ethernet II, Src: IntelCor_14:76:ed (34:cf:f6:14:76:ed), Dst: Hangzhou_91:72:e
Internet Protocol Version 4, Src: 114.214.185.201, Dst: 202.38.64.246
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 520
  Identification: 0x2f94 (12180)
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment Offset: 1480
```

◦ 根据Flags偏移可以确定这不是第一个数据段，MF指示后面已经没有数据段了；

13. ◦ Flags， Header Checksum；
14.
```
[3 IPv4 Fragments (3480 bytes): #2731(1480), #2732(1480), #2733(520)]
[Frame: 2731, payload: 0-1479 (1480 bytes)]
[Frame: 2732, payload: 1480-2959 (1480 bytes)]
[Frame: 2733, payload: 2960-3479 (520 bytes)]
```

◦ 三个；

15. ◦ Total Lengths, ID, Header Checksum