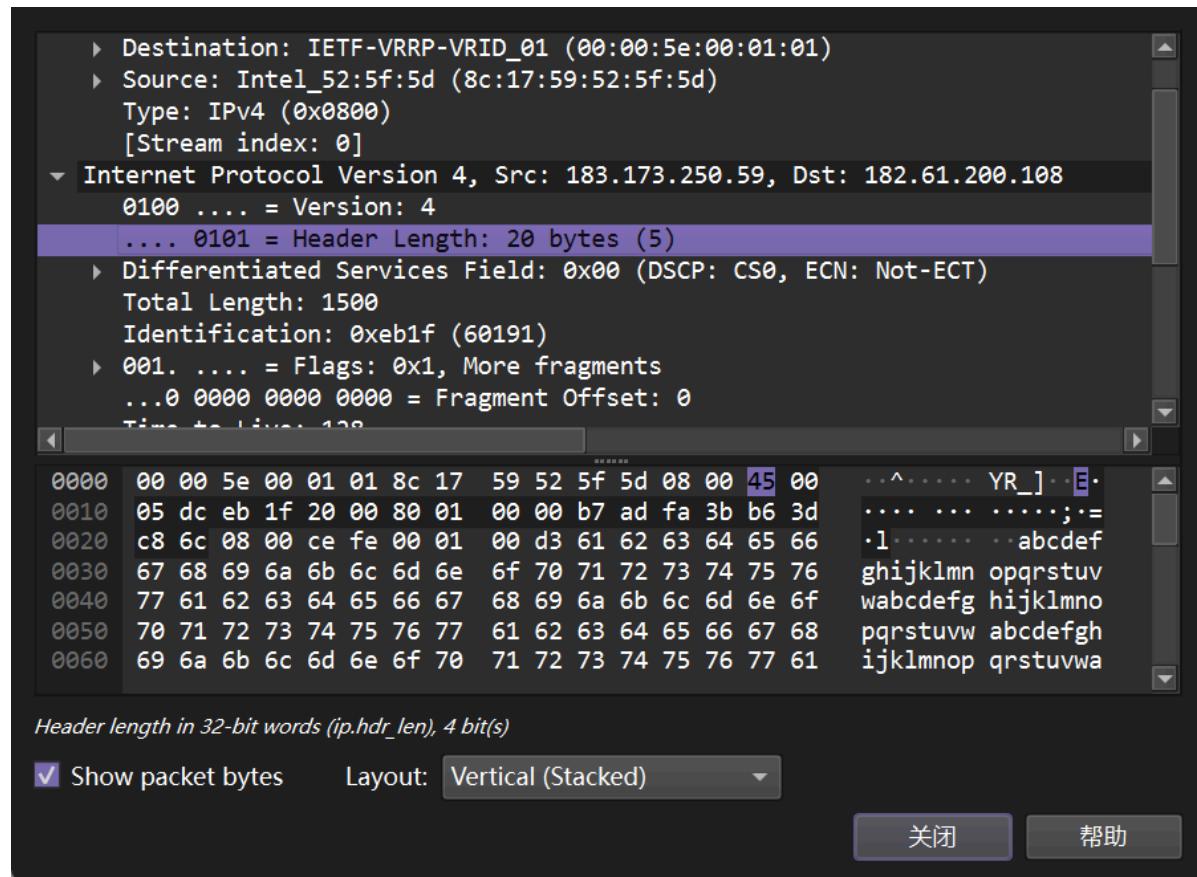


第三次实验报告

张峰源 2023010859

实验一

(1) Version字段的值是多少? IHL字段的值一般是多少? 结合 IPv4 分组头部格式可以看出 IHL 的单位是什么?



version: 4

IHL: 5, 单位为32位 (4字节)

(2) 三个分组的 Identification 值是多少？是否相等？

ip.version == 4 and ip.src == 183.173.250.59 and ip.dst == 182.61.200.108

No.	Time	Source	Destination	Protocol	Length	Info
5673	48.165636	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=eb1f) [Reassembled in #5675]
5674	48.165636	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=eb1f) [Reassembled in #5675]
5675	48.165636	183.173.250.59	182.61.200.108	ICMP	82	Echo (ping) request id=0x0001, seq=211/54016, ttl=128 (no response found!)
8311	53.079267	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=eb20) [Reassembled in #8313]
8312	53.079267	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=eb20) [Reassembled in #8313]
8313	53.079267	183.173.250.59	182.61.200.108	ICMP	82	Echo (ping) request id=0x0001, seq=212/54272, ttl=128 (no response found!)
8407	58.094558	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=eb21) [Reassembled in #8409]
8408	58.094558	183.173.250.59	182.61.200.108	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=eb21) [Reassembled in #8409]
8409	58.094558	183.173.250.59	182.61.200.108	ICMP	82	Echo (ping) request id=0x0001, seq=213/54528, ttl=128 (no response found!)

Source: Intel_52:5f:5d (8c:17:59:52:5f:5d)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 183.173.250.59, Dst: 182.61.200.108
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0xeb1f (60191)
001. = Flags: 0x1, More fragments
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
0000 00 00 5e 00 01 01 8c 17 59 52 5f 5d 08 00 45 00 ..^..... YR_] E.
0010 05 dc eb 1f 20 00 80 01 00 00 b7 ad fa 3b b6 3d ;=
0020 c8 6c 08 00 ce fe 00 01 00 d3 61 62 63 64 65 66 .l..... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f wabcdefg hijklmno
0050 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 pqrstuvw abcdefgh
0060 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 ijklmnop qrstuvwxyz

No.: 5673 · Time: 48.165636 · Source: 183.173.250.59 · Destination: 182.61.200.108 · Protocol: ICMP (1) [proto=ICMP 1, off=0, ID=eb1f] [Reassembled in #5675]

Show packet bytes Layout: Vertical (Stacked) 关闭 帮助

identification: 0xeb1f(60191), 相等。

(3) 前两个分组的Flag字段，DF和MF的值分别是？表示什么意思？

The screenshot shows the Wireshark interface with an ICMP packet selected. The top pane displays the packet details:

- Total Length: 1500
- Identification: 0xeb1f (60191)
- Flags:
 - 001. = Flags: 0x1, More fragments
 - 0.... = Reserved bit: Not set
 - .0... = Don't fragment: Not set
 - ..1. = More fragments: Set
 - ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: ICMP (1)
- Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
- Source Address: 183.173.250.59
- Destination Address: 183.61.220.128

The bottom pane shows the raw bytes of the ICMP header:

Hex	ASCII
0000	00 00 5e 00 01 01 8c 17 59 52 5f 5d 08 00 45 00
0010	05 dc eb 1f 20 00 80 01 00 00 b7 ad fa 3b b6 3d
0020	c8 6c 08 00 ce fe 00 01 00 d3 61 62 63 64 65 66
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f
0050	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68
0060	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61

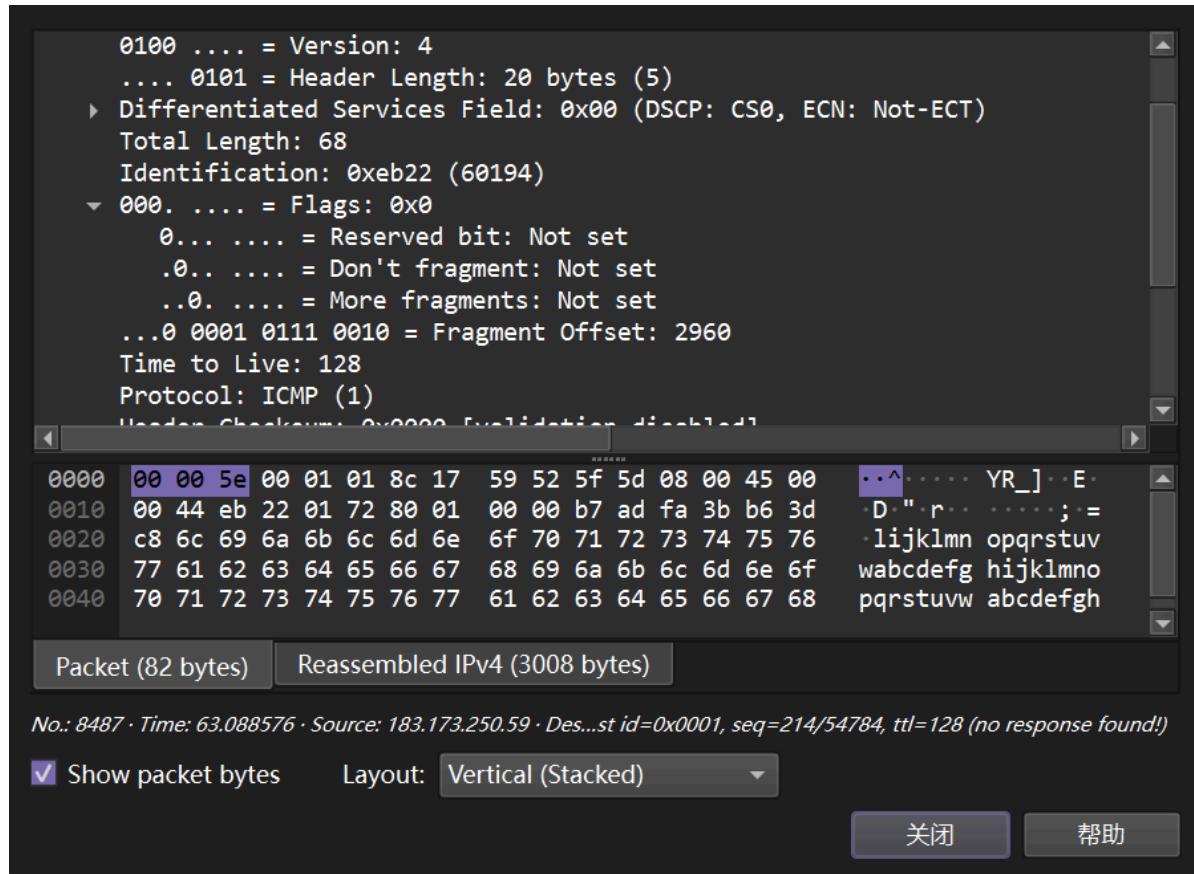
Below the bytes view, the status bar shows: No.: 5673 · Time: 48.165636 · Source: 183.173.250.59 · Destination: 183.61.220.128 · (proto=ICMP 1, off=0, ID=eb1f) [Reassembled in #5675].

At the bottom left, there is a checkbox labeled "Show packet bytes" and a dropdown menu labeled "Layout: Vertical (Stacked)". At the bottom right are two buttons: "关闭" (Close) and "帮助" (Help).

DF:0,not set, 禁止分片置零, 表允许分片

MF:1,set, 该分段后还有分片

(4) 第三个分组的Flag字段，DF和MF的值分别是？表示什么意思？



DF:0, 允许分片

MF:0, 该分片后无分片

(5) 三个分组Fragment offset的值依次为多少，以确保在乱序到达时也能正确重组出原来的分组？

...0 0000 0000 0000 = Fragment Offset: 0

...0 0000 1011 1001 = Fragment Offset: 1480

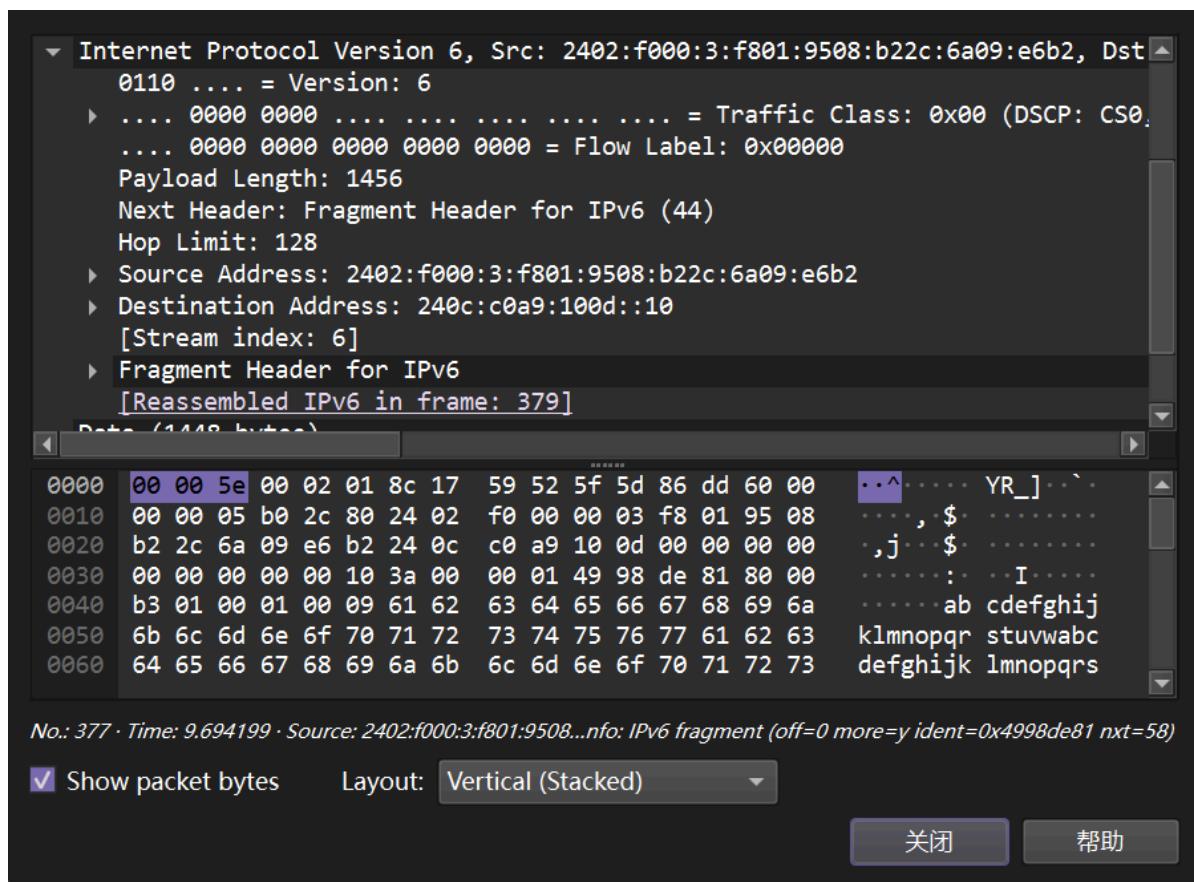
...0 0001 0111 0010 = Fragment Offset: 2960

(6) 三个分段的总的数据长度为 1500+1500+68-3*20=3008，比 ping 命令 中的参数 3000 多了 8，为什么？

答：总数据长度 3008 包含了 ICMP 头部的 8 字节。

实验二

(1) Version字段的值是多少？源地址和目 标地址分别是什么，占多少字节？



The screenshot shows the Wireshark interface with a selected IPv6 fragment header. The analysis pane displays the following details:

- Internet Protocol Version 6, Src: 2402:f000:3:f801:9508:b22c:6a09:e6b2, Dst: 240c:c0a9:100d::10 [Stream index: 6]
- Version: 6
- Traffic Class: 0x00 (DSCP: CS0)
- Flow Label: 0x000000
- Payload Length: 1456
- Next Header: Fragment Header for IPv6 (44)
- Hop Limit: 128
- Source Address: 2402:f000:3:f801:9508:b22c:6a09:e6b2
- Destination Address: 240c:c0a9:100d::10
- Fragment Header for IPv6 [Reassembled IPv6 in frame: 379]

The bytes pane shows the raw hex and ASCII data of the fragment header. The hex dump starts with 00 00 5e 00 02 01 8c 17 59 52 5f 5d 86 dd 60 00, followed by 00 00 05 b0 2c 80 24 02 f0 00 00 03 f8 01 95 08, and so on.

No.: 377 · Time: 9.694199 · Source: 2402:f000:3:f801:9508...info: IPv6 fragment (off=0 more=y ident=0x4998de81 nxt=58)

Show packet bytes Layout: Vertical (Stacked)

version: 6

源地址: 2402:f000:3:f801:9508:b22c:6a09:e6b2

目的地址: 240c:c0a9:100d::10

占16字节

(2) 观察并说明ipv6是如何进行分片的?

```
▼ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 0000 0000 0... = Offset: 0 (0 bytes)
    .... .... .... .00. = Reserved bits: 0
    .... .... .... ..1 = More Fragments: Yes
    Identification: 0x4998de81
    [Reassembled IPv6 in frame: 379]

▼ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 0101 1010 1... = Offset: 181 (1448 bytes)
    .... .... .... .00. = Reserved bits: 0
    .... .... .... ..1 = More Fragments: Yes
    Identification: 0x4998de81
    [Reassembled IPv6 in frame: 379]

▼ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 1011 0101 0... = Offset: 362 (2896 bytes)
    .... .... .... .00. = Reserved bits: 0
    .... .... .... ..0 = More Fragments: No
    Identification: 0x4998de81
▶ [3 IPv6 Fragments (3008 bytes): #377(1448), #378(1448), #379(112)]
```

将含ICMP头的共3008bytes分为了1448、1448、112三片（前两段必须是8的倍数），identification相同，前两个MF为1表示后面还有分片，最后一个为0.

(3) 观察ipv4与ipv6头部的不同点，比如前文提到的地址长度区别和分段方法区别，除此以外举出1个点辅以截图说明即可。

1.地址长度：IPv4地址长度为4字节，IPv6地址长度为16字节。

2.Ipv6含Traffic class字段，

```
▼ Internet Protocol Version 6, Src: 2402:f000:3:f801:9508:b22c:6a09:e6b2, Dst: 240c:c0a9:100d::10
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 00.. .... .... .... .... = Differentiated Services Codepoint: Default (0)
  .... .... ..00 .... .... .... .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  .... 0000 0000 0000 0000 = Flow Label: 0x00000
  Payload Length: 1456
```

DSCP (Differentiated Services Code Point) : 占 Traffic Class 字段前 6 位，用于给 IPv6 数据包分类，标记服务优先级（如语音、视频包优先转发），让网络设备提供差异化 QoS（服务质量）。

ECN (Explicit Congestion Notification) : 占后 2 位，用于显式传递网络拥塞状态，路由器拥塞时无需丢包，直接告知源主机调整发送速率，优化传输效率。

3. IPv6 不含 DF 字段。分片规则与 IPv4 完全不同：IPv6 仅由源主机分片（中间路由器不分片），且源主机会通过“路径 MTU 发现”提前适配最大传输单元，无需禁止分片；同时移除 DF 位可简化 IPv6 头部设计，提升路由器转发效率，无需像 IPv4 那样用 DF 位限制路由器分片行为。