Traceroute 实验报告

PB19030861 王湘峰

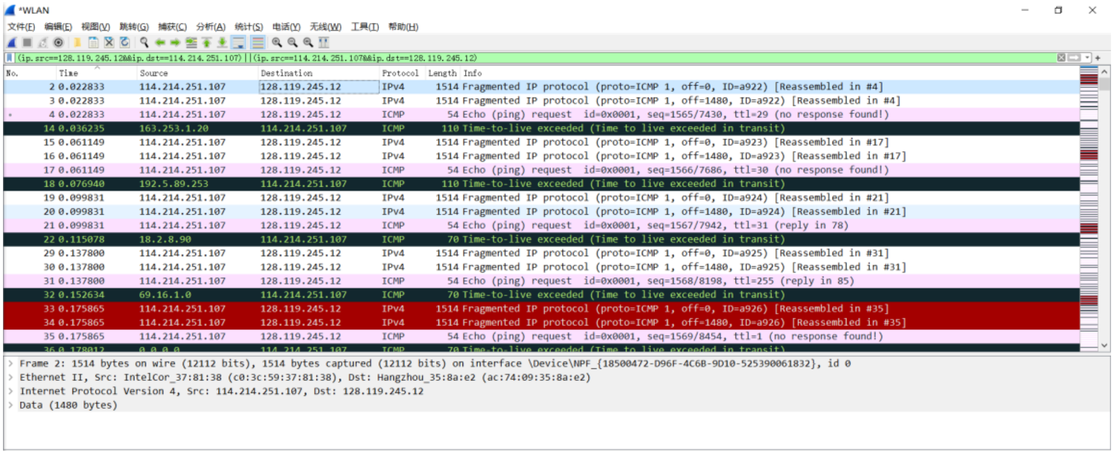
Questions

1. **Display the rules to filter the IP and ICMP packets between source host and destination host. Are there any other Application-layer protocols when you traceroute gaia.cs.umass.edu?**

   答：过滤规则为：(ip.src==128.119.245.12&&ip.dst==114.214.251.107) || (ip.src==114.214.251.107&&ip.dst==128.119.245.12)

   其中 128.119.245.12 是 gaia.cs.umass.edu 的 IP 地址，

   114.214.251.107 是本机的 IP 地址。下图为过滤后的图标：

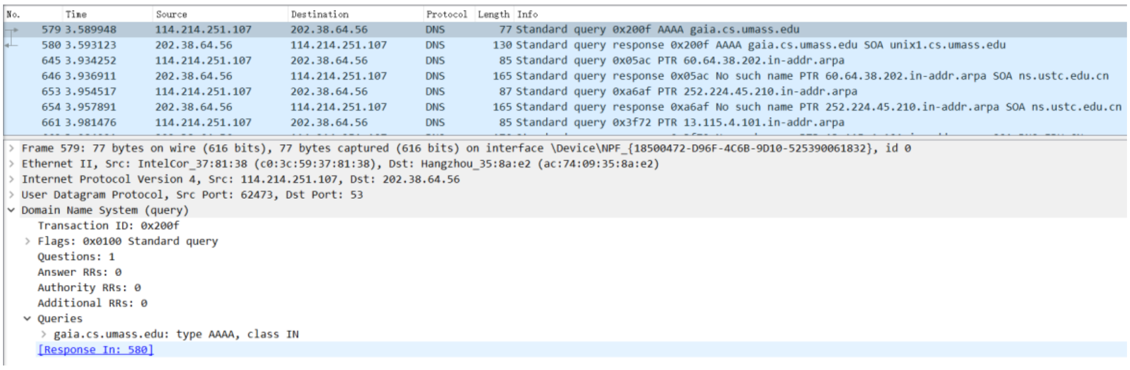

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
(ip.src==128.119.245.12&&ip.dst==114.214.251.107)||(ip.src==114.214.251.107&&ip.dst==128.119.245.12)
```

```
No.   Time        Source            Destination       Protocol  Length Info
    2 0.022833    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a922) [Reassembled in #4]
    3 0.022833    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a922) [Reassembled in #4]
    4 0.022833    114.214.251.107   128.119.245.12    ICMP        54 Echo (ping) request  id=0x0001, seq=1565/7430, ttl=29 (no response found!)
   14 0.036235    163.253.1.20      114.214.251.107   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   15 0.061149    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a923) [Reassembled in #17]
   16 0.061149    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a923) [Reassembled in #17]
   17 0.061149    114.214.251.107   128.119.245.12    ICMP        54 Echo (ping) request  id=0x0001, seq=1566/7686, ttl=30 (no response found!)
   18 0.076940    192.5.89.253      114.214.251.107   ICMP       110 Time-to-live exceeded (Time to live exceeded in transit)
   19 0.099831    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a924) [Reassembled in #21]
   20 0.099831    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a924) [Reassembled in #21]
   21 0.099831    114.214.251.107   128.119.245.12    ICMP        54 Echo (ping) request  id=0x0001, seq=1567/7942, ttl=31 (reply in 78)
   22 0.115078    18.2.8.90         114.214.251.107   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   29 0.137800    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a925) [Reassembled in #31]
   30 0.137800    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a925) [Reassembled in #31]
   31 0.137800    114.214.251.107   128.119.245.12    ICMP        54 Echo (ping) request  id=0x0001, seq=1568/8198, ttl=255 (reply in 85)
   32 0.152634    69.16.1.0         114.214.251.107   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   33 0.175865    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a926) [Reassembled in #35]
   34 0.175865    114.214.251.107   128.119.245.12    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a926) [Reassembled in #35]
   35 0.175865    114.214.251.107   128.119.245.12    ICMP        54 Echo (ping) request  id=0x0001, seq=1569/8454, ttl=1 (no response found!)
   36 0.178012    0.0.0.0           114.214.251.107   ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
```

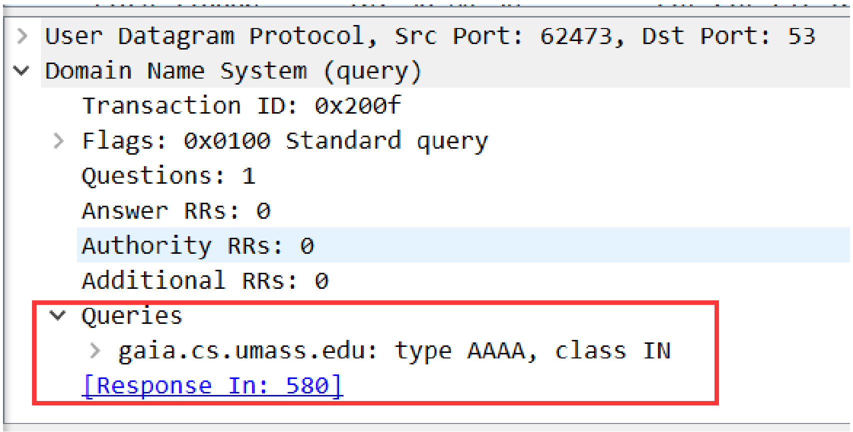
```
> Frame 2: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{18500472-D96F-4C6B-9D10-525390061832}, id 0
> Ethernet II, Src: IntelCor_37:81:38 (c0:3c:59:37:81:38), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.251.107, Dst: 128.119.245.12
> Data (1480 bytes)
```

应用层协议只发现了 DNS 协议：



```
No.   Time        Source            Destination       Protocol  Length Info
  579 3.589948    114.214.251.107   202.38.64.56      DNS         77 Standard query 0x200f AAAA gaia.cs.umass.edu
  580 3.593123    202.38.64.56      114.214.251.107   DNS        130 Standard query response 0x200f AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  645 3.934252    114.214.251.107   202.38.64.56      DNS         85 Standard query 0x05ac PTR 60.64.38.202.in-addr.arpa
  646 3.936911    202.38.64.56      114.214.251.107   DNS        165 Standard query response 0x05ac No such name PTR 60.64.38.202.in-addr.arpa SOA ns.ustc.edu.cn
  653 3.954517    114.214.251.107   202.38.64.56      DNS         87 Standard query 0xa6af PTR 252.224.45.210.in-addr.arpa
  654 3.957891    202.38.64.56      114.214.251.107   DNS        165 Standard query response 0xa6af No such name PTR 252.224.45.210.in-addr.arpa SOA ns.ustc.edu.cn
  661 3.981476    114.214.251.107   202.38.64.56      DNS         85 Standard query 0x3f72 PTR 13.115.4.101.in-addr.arpa
```

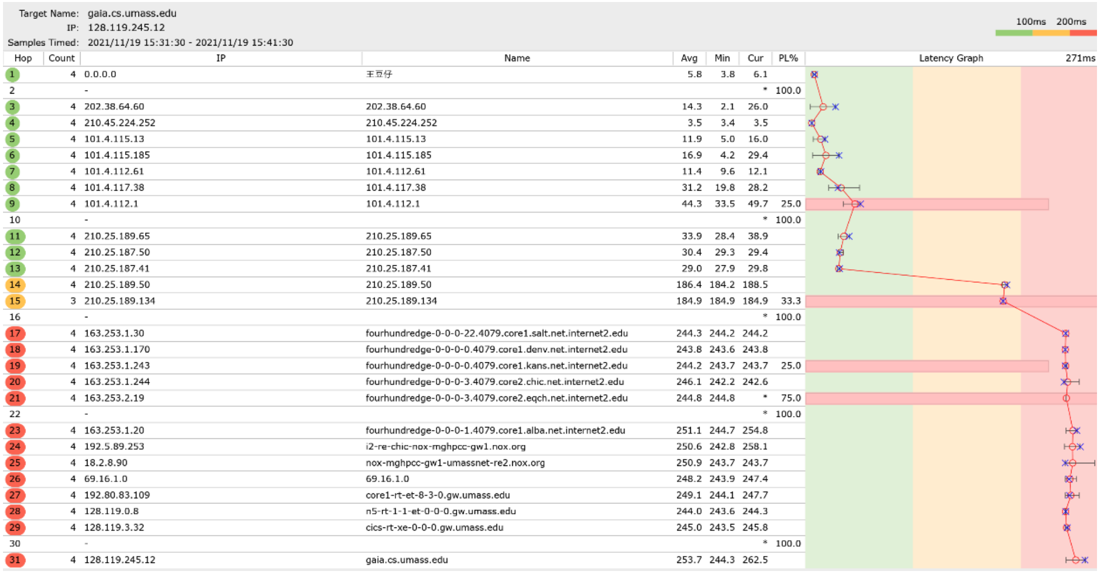
```
> Frame 579: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{18500472-D96F-4C6B-9D10-525390061832}, id 0
> Ethernet II, Src: IntelCor_37:81:38 (c0:3c:59:37:81:38), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 114.214.251.107, Dst: 202.38.64.56
> User Datagram Protocol, Src Port: 62473, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x200f
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > gaia.cs.umass.edu: type AAAA, class IN
    [Response In: 580]
```



```
> User Datagram Protocol, Src Port: 62473, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x200f
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > gaia.cs.umass.edu: type AAAA, class IN
    [Response In: 580]
```

2. **How many hops between source and destination? Find the first ICMP Echo Request packet that has TTL=1, is this packet fragmented? If yes, how many fragments, and why is the packet fragmented?**

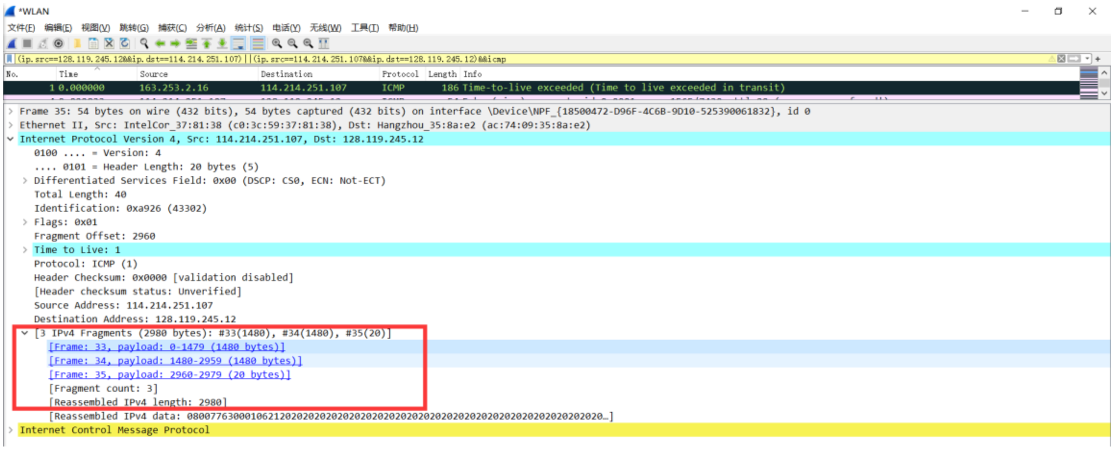
答：一共经历了31跳达到目的地。



Target Name: gaia.cs.umass.edu
IP: 128.119.245.12
Samples Timed: 2021/11/19 15:31:30 - 2021/11/19 15:41:30

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	4	0.0.0.0	王豆仔	5.8	3.8	6.1	
2		-				*	100.0
3	4	202.38.64.60	202.38.64.60	14.3	2.1	26.0	
4	4	210.45.224.252	210.45.224.252	3.5	3.4	3.5	
5	4	101.4.115.13	101.4.115.13	11.9	5.0	16.0	
6	4	101.4.115.185	101.4.115.185	16.9	4.2	29.4	
7	4	101.4.112.61	101.4.112.61	11.4	9.6	12.1	
8	4	101.4.117.38	101.4.117.38	31.2	19.8	28.2	
9	4	101.4.112.1	101.4.112.1	44.3	33.5	49.7	25.0
10		-				*	100.0
11	4	210.25.189.65	210.25.189.65	33.9	28.4	38.9	
12	4	210.25.187.50	210.25.187.50	30.4	29.3	29.4	
13	4	210.25.187.41	210.25.187.41	29.0	27.9	29.8	
14	4	210.25.189.50	210.25.189.50	186.4	184.2	188.5	
15	3	210.25.189.134	210.25.189.134	184.9	184.9	184.9	33.3
16		-				*	100.0
17	4	163.253.1.30	fourhundredge-0-0-0-22.4079.core1.salt.net.internet2.edu	244.3	244.2	244.2	
18	4	163.253.1.170	fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu	243.8	243.6	243.8	
19	4	163.253.1.243	fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu	244.2	243.7	243.7	25.0
20	4	163.253.1.244	fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu	246.1	242.2	242.6	
21	4	163.253.2.19	fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu	244.8	244.8	*	75.0
22		-				*	100.0
23	4	163.253.1.20	fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu	251.1	244.7	254.8	
24	4	192.5.89.253	i2-re-chic-nox-mghpcc-gw1.nox.org	250.6	242.8	258.1	
25	4	18.2.8.90	nox-mghpcc-gw1-umassnet-re2.nox.org	250.9	243.7	243.7	
26	4	69.16.1.0	69.16.1.0	248.2	243.9	247.4	
27	4	192.80.83.109	core1-rt-et-8-3-0.gw.umass.edu	249.1	244.1	247.7	
28	4	128.119.0.8	n5-rt-1-1-et-0-0-0.gw.umass.edu	244.0	243.6	244.3	
29	4	128.119.3.32	cics-rt-xe-0-0-0.gw.umass.edu	245.0	243.5	245.8	
30		-				*	100.0
31	4	128.119.245.12	gaia.cs.umass.edu	253.7	244.3	262.5	

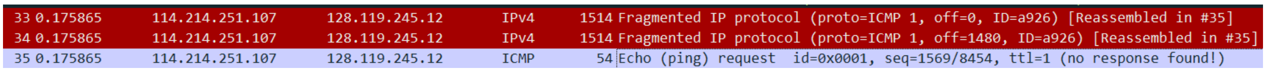
该分组被切片了，分片数量为 3；由于我们在 Pingplotter 中设置的 packet 大小为 3000 字节，但是链路的 MTU 只有 1500 字节，所以链路不能一次性把全部的报文封装到一个片中，于是 packet 被分为了三个较小的片。


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
(ip.src==128.119.245.12&&ip.dst==114.214.251.107)||(ip.src==114.214.251.107&&ip.dst==128.119.245.12)&&icmp
No.   Time       Source          Destination      Protocol Length Info
    1 0.000000   163.253.2.16    114.214.251.107  ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
> Frame 35: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{18500472-D96F-4C6B-9D10-525390061832}, id 0
> Ethernet II, Src: IntelCor_37:81:38 (c0:3c:59:37:81:38), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
v Internet Protocol Version 4, Src: 114.214.251.107, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xa926 (43302)
  > Flags: 0x01
    Fragment Offset: 2960
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.251.107
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #33(1480), #34(1480), #35(20)]
      [Frame: 33, payload: 0-1479 (1480 bytes)]
      [Frame: 34, payload: 1480-2959 (1480 bytes)]
      [Frame: 35, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: 080077630001062120202020202020202020202020202020202020202020202020202020…]
> Internet Control Message Protocol
```

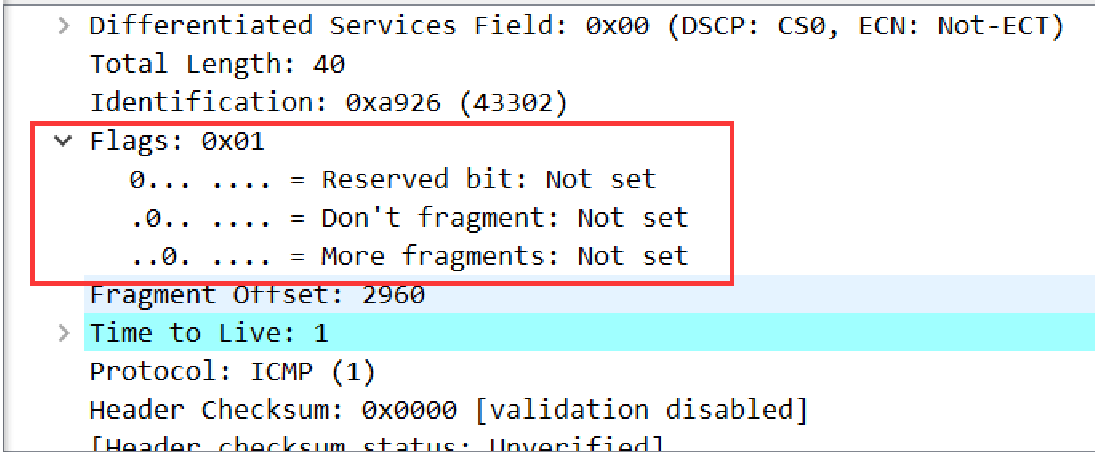
3. **How the packets are fragmented and reassembled? For each fragment, how to know if it is the last fragment, and how many bytes are contained in each fragment? Print the packets and answer by highlighting the relevant fields.**

答：该数据包被分为三个独立的片，其中两个**数据**长度为 1480 字节，一个**数据**长度为 20 字节。他们的首部中加入了偏移量的信息，在重新组装的时候根据偏移量的值确定先后顺序，以此来保证组装后的数据是有序的。每个片中的 flag 字段表示了该片是否为最后一个，更进一步地，flag=0 代表是最后一个包，flag=1 代表不是最后一个。



```
33 0.175865   114.214.251.107   128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a926) [Reassembled in #35]
34 0.175865   114.214.251.107   128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a926) [Reassembled in #35]
35 0.175865   114.214.251.107   128.119.245.12   ICMP     54 Echo (ping) request  id=0x0001, seq=1569/8454, ttl=1 (no response found!)
```

上图是被分成三个片的报文

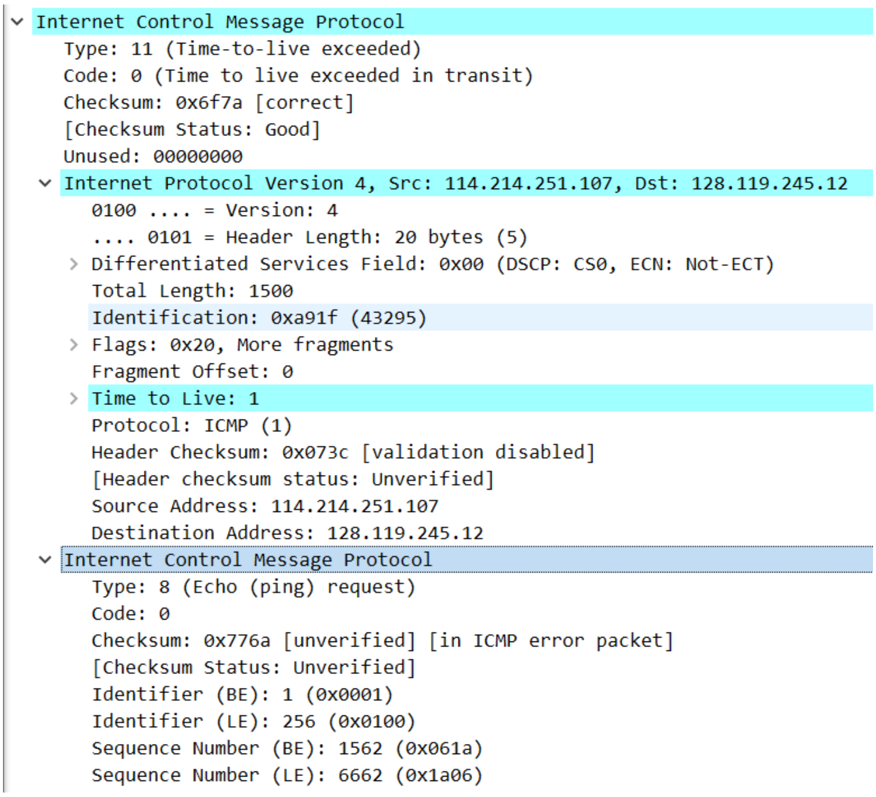


```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xa926 (43302)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

上图为最后一个片的 flag 字段，more fragment = 0，代表该报文是最后的一个片。

4. **What packet is returned from the router when TTL expires? What is contained in the payload of the packet?**

   答：当 TTL 减为 0 时，路由器将会丢弃该分组并发送一个“Time to live exceeded in transit”的分组作为通知。该分组的 ICMP 中的 type 字段被设置为“11”，即代表转发跳数已达到 TTL；同时 ICMP 中还包含着被丢弃分组首部的信息，包括被丢弃分组的 IPv4 数据和 ICMP 数据。

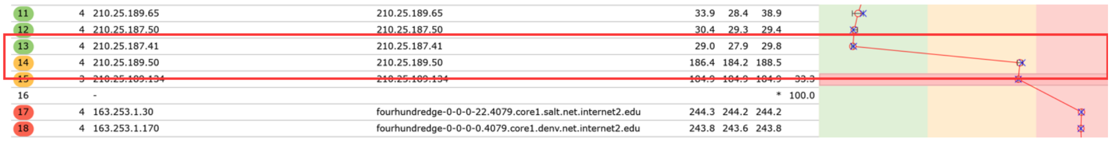


```
⌄ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6f7a [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ⌄ Internet Protocol Version 4, Src: 114.214.251.107, Dst: 128.119.245.12
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 1500
      Identification: 0xa91f (43295)
    > Flags: 0x20, More fragments
      Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x073c [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 114.214.251.107
      Destination Address: 128.119.245.12
  ⌄ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x776a [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 1562 (0x061a)
      Sequence Number (LE): 6662 (0x1a06)
```

（可以看到，通知报文的 ICMP 中包含着丢弃分组的 IPv4 和 ICMP 信息）

5. **Which link crosses the Pacific, give the router addresses at the two ends of the link? Explained your reason.**

   答：IP 地址从 210.25.187.41 到 210.25.189.50 的链路。



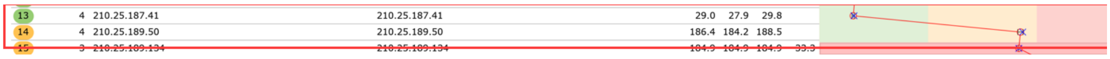
11	4	210.25.189.65	210.25.189.65	33.9	28.4	38.9	
12	4	210.25.187.50	210.25.187.50	30.4	29.3	29.4	
13	4	210.25.187.41	210.25.187.41	29.0	27.9	29.8	
14	4	210.25.189.50	210.25.189.50	186.4	184.2	188.5	
~~15~~	~~3~~	~~210.25.189.134~~	~~210.25.189.134~~	~~184.9~~	~~184.9~~	~~184.9~~	~~33.3~~
16	-					*	100.0
17	4	163.253.1.30	fourhundredge-0-0-0-22.4079.core1.salt.net.internet2.edu	244.3	244.2	244.2	
18	4	163.253.1.170	fourhundredge-0-0-0.4079.core1.denv.net.internet2.edu	243.8	243.6	243.8	

直观上，从时延的角度可以看出这两个 IP 地址所在的主机的地理距离很远， 因此这条链路横跨太平洋。

6. **How long is the trans-Pacific link? (given that a bit transmits**

2×10^8 m/s in fiber).

答：



13	4	210.25.187.41	210.25.187.41	29.0	27.9	29.8		
14	4	210.25.189.50	210.25.189.50	186.4	184.2	188.5		
15	3	210.25.189.134	210.25.189.134	184.9	184.9	184.9	33.3	

若忽略传输时延，则单项传播时延为186.4 − 29 = 157.4ms

$$Length = 157.4 \times 10^{-3}s \times 2 \times 10^8 m/s \times \frac{1}{2} = 1.574 \times 10^7 m = 15740km$$

链路长度大约为15740km。