

Traceroute 实验报告

PB19010450 和泳毅

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?

过滤规则与结果如下：

- (ip.src==128.119.245.12&&ip.dst==114.214.221.13) ||
(ip.src==114.214.221.13&&ip.dst==128.119.245.12)

	Time	Source	Destination	Protocol	Length	Info
	255 5.015057	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad0) [Reassembled in #257]
	256 5.015057	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad0) [Reassembled in #257]
	257 5.015057	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25981/32101, ttl=255 (no response found!)
	263 5.056186	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad1) [Reassembled in #265]
	264 5.056186	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad1) [Reassembled in #265]
	265 5.056186	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25982/32357, ttl=1 (no response found!)
	266 5.060795	0.0.0.0	114.214.221.13	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
	267 5.097131	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad2) [Reassembled in #269]
	268 5.097131	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad2) [Reassembled in #269]
	269 5.097131	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25983/32613, ttl=2 (no response found!)
	277 5.138482	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad3) [Reassembled in #279]
	278 5.138482	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad3) [Reassembled in #279]
	279 5.138482	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25984/32869, ttl=3 (no response found!)
	280 5.141877	202.38.64.58	114.214.221.13	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
	285 5.178647	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad4) [Reassembled in #287]
	286 5.178647	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad4) [Reassembled in #287]
	287 5.178647	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25985/33125, ttl=4 (no response found!)
	288 5.219636	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4ad5) [Reassembled in #290]
	289 5.219636	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4ad5) [Reassembled in #290]
	290 5.219636	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=25986/33381, ttl=5 (no response found!)

128.119.245.12 是 gaia.cs.umass.edu 的 IP 地址，114.214.221.13 是本机的 IP 地址。

用“dns”规则过滤可以看到应用层协议：DNS协议，例如以下报文包含一个A类型的对域名 gaia.cs.umass.edu的查询：

	Time	Source	Destination	Protocol	Length	Info
0.	247 4.954829	114.214.221.13	202.38.64.56	DNS	77	Standard query 0x8d00 A gaia.cs.umass.edu
1.	248 4.955152	114.214.221.13	202.38.64.56	DNS	77	Standard query 0x702b AAAA gaia.cs.umass.edu
2.	249 4.986687	114.214.221.13	202.38.64.17	DNS	77	Standard query 0x8d00 A gaia.cs.umass.edu
3.	250 4.986696	114.214.221.13	202.38.64.17	DNS	77	Standard query 0x702b AAAA gaia.cs.umass.edu
4.	251 5.008425	202.38.64.56	114.214.221.13	DNS	130	Standard query response 0x702b AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
5.	252 5.008425	202.38.64.56	114.214.221.13	DNS	93	Standard query response 0x8d00 A gaia.cs.umass.edu A 128.119.245.12
6.	253 5.011071	202.38.64.17	114.214.221.13	DNS	93	Standard query response 0x8d00 A gaia.cs.umass.edu A 128.119.245.12
7.	254 5.011071	202.38.64.17	114.214.221.13	DNS	130	Standard query response 0x702b AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
8.	281 5.142859	114.214.221.13	202.38.64.56	DNS	85	Standard query 0x33f4 PTR 58.64.38.202.in-addr.arpa
9.	282 5.150967	202.38.64.56	114.214.221.13	DNS	165	Standard query response 0x33f4 No such name PTR 58.64.38.202.in-addr.arpa SOA ns
10.	296 5.232099	114.214.221.13	202.38.64.56	DNS	87	Standard query 0xe53d PTR 252.224.45.210.in-addr.arpa
11.	298 5.239185	202.38.64.56	114.214.221.13	DNS	165	Standard query response 0xe53d No such name PTR 252.224.45.210.in-addr.arpa SOA
12.	300 5.243845	114.214.221.13	202.38.64.56	DNS	85	Standard query 0x598f PTR 13.115.4.101.in-addr.arpa
13.	301 5.248656	202.38.64.56	114.214.221.13	DNS	170	Standard query response 0x598f No such name PTR 13.115.4.101.in-addr.arpa SOA DN
14.	309 5.276986	114.214.221.13	202.38.64.56	DNS	86	Standard query 0x09b2 PTR 185.115.4.101.in-addr.arpa

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
  ▼ gaia.cs.umass.edu: type A, class IN
    Name: gaia.cs.umass.edu
    [Name Length: 17]
    [Label Count: 4]
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    [Response In: 252]
```

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?

一共经过31跳达到目的地，截图如下：

Hop	Count	IP	Name
1	3	0.0.0.0	Yorick的电脑
3	3	202.38.64.58	202.38.64.58
4	3	210.45.224.252	210.45.224.252
5	3	101.4.115.13	101.4.115.13
6	3	101.4.115.185	101.4.115.185
7	3	101.4.112.61	101.4.112.61
8	3	101.4.117.38	101.4.117.38
9	3	101.4.112.1	101.4.112.1
11	3	210.25.189.65	210.25.189.65
12	3	210.25.187.50	210.25.187.50
13	3	210.25.187.41	210.25.187.41
14	3	210.25.189.50	210.25.189.50
15	3	210.25.189.134	210.25.189.134
16	3	163.253.1.115	fourhundredge-0-0-0-2.4079.core2.salt.net.int
17	3	163.253.1.32	fourhundredge-0-0-0-23.4079.core1.salt.net.ir
18	3	163.253.1.170	fourhundredge-0-0-0-0.4079.core1.denv.net.ii
19	3	163.253.1.243	fourhundredge-0-0-0-0.4079.core1.kans.net.ir
20	3	163.253.1.244	fourhundredge-0-0-0-3.4079.core2.chic.net.in
21	3	163.253.2.19	fourhundredge-0-0-0-3.4079.core2.eqch.net.ii
22	3	163.253.2.16	fourhundredge-0-0-0-0.4079.core2.clev.net.in
23	3	163.253.1.20	fourhundredge-0-0-0-1.4079.core1.alba.net.in
24	3	192.5.89.253	i2-re-chic-nox-mghpcc-gw1.nox.org
25	3	18.2.8.90	nox-mghpcc-gw1-umassnet-re2.nox.org
26	3	69.16.1.0	69.16.1.0
27	3	192.80.83.109	core1-rt-et-8-3-0.gw.umass.edu
28	3	128.119.0.8	n5-rt-1-1-et-0-0-0.gw.umass.edu
29	3	128.119.3.32	cics-rt-xe-0-0-0.gw.umass.edu
31	3	128.119.245.12	gaia.cs.umass.edu

该TTL=1的ICMP分组被分片了，分片数量为 3。因为分组的大小为 3000 字节，而MTU=1500 字节，链路不能一次性把全部的报文封装到一个片中，所以需要分片。该分组以及分片解析的截图如下：

642 7.554889 114.214.221.13 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=4af8) [Reassembled in #644]

643 7.554889 114.214.221.13 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=4af8) [Reassembled in #644]

644 7.554889 114.214.221.13 128.119.245.12 ICMP 54 Echo (ping) request id=0x0002, seq=26021/42341, ttl=1 (no response found!)

[3 IPv4 Fragments (2980 bytes): #642(1480), #643(1480), #644(20)]

[Frame: 642, payload: 0-1479 (1480 bytes)]

[Frame: 643, payload: 1480-2959 (1480 bytes)]

[Frame: 644, payload: 2960-2979 (20 bytes)]

Fragment count: 31

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.

一个3000字节的分组被分为三个独立的片，它们都包含20字节的IP首部，所以数据长度依次为1480字节、1480字节、20字节。属于同一个分组的片拥有相同的ID，并且会根据每个片在分组的位置记录偏移量offset，将除了最后一片的标志flag置为1，最后一片的标志flag置为0。在重新组装时，根据偏移量的值确定先后顺序以及相对位置，根据标志位确定分片是否结束以及完整。

532 6.499295	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP, off=1480, id=4a4) [Reassembled in #533]
533 6.499295	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=26017/41317, ttl=36 (reply in 582)
534 6.539182	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP, off=0, id=4a5) [Reassembled in #536]
535 6.539182	114.214.221.13	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP, off=1480, id=4a5) [Reassembled in #536]
536 6.539182	114.214.221.13	128.119.245.12	ICMP	54	Echo (ping) request id=0x0002, seq=26018/41373, ttl=37 (reply in 585)
537 6.543927	202.38.64.56	114.214.221.13	DNS	155	Standard query response 0x990 IP 32.1.253.163.in-addr.arpa PK fourthround-0-0-0-0-2
538 6.554969	Hangzhou35:8a:e2	Broadcast	ARP	56	Who has 211.86.146.63? Tell 211.86.144.1

具体内容如下三片：

[illegible]

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

TTL过期时路由器将会丢弃该分组并发送一个“Time to live exceeded in transit”的分组到本机ip地址。其有效载荷包含类型为11的ICMP报文，同时其中还包含该过期分组的首部信息、ICMP数据等。

4390 0.234500	114.214.221.13	160.117.243.12	ICMP	34 Echo (ping) request id=0x0002, seq=20011/39/61, ttl=30 (no response timeout)
4391 0.327403	202.38.64.37	114.214.221.13	DNS	155 Standard query response 0x375C PTR 32.4.253.163.in-addr.arpa PTR fourthround
492 0.281875	202.5.89.253	114.214.221.13	ICMP	110 Time-to-live exceeded (Time to live exceeded in transit)
493 0.282493	114.214.221.13	202.30.047.30	DNS	83 Standard query 0x375C PTR 202.30.047.30.in-addr.arpa PTR
494 0.286150	202.38.64.37	114.214.221.13	DNS	121 Standard query response 0x375C PTR 253.89.5.12.in-addr.arpa PTR i2-rech

```

Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xece6 [correct]
  [Checksum Status: Good]
  Unused: 00
  Length: 17
  [Length of original datagram: 68]
  Unused: 0000
Internet Protocol Version 4, Src: 114.214.221.13, 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: 0x4ae8 (19176)
  > Flags: 0x20, More fragments
  Fragment Offset: 0
  > Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x83d1 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 114.214.221.13
  Destination Address: 128.119.245.12
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x17ee [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]

```

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

若考虑时延最大的链路，如下两个 IP 地址所在的主机的地理距离可能很远，认为这条链路横跨太平洋。即 IP 地址从 210.25.187.41 到 210.25.189.50 的链路。

3	210.25.187.41	210.25.187.41	61.2	50.0	69.3	
3	210.25.189.50	210.25.189.50	223.6	219.2	224.0	
3	210.25.189.134	210.25.189.134	104.9	104.4	103.3	33.3
3	163.253.1.115	fourhundredge-0-0-0-2.4079.core2.salt.net.int	278.3	265.6	265.6	

6. How long is the trans-Pacific link? (given that a bit transmits 2×10^8 m/s in fiber).

若忽略传输时延，则传播时延之差为 $223.6 - 61.2 = 162.4ms$ ，
 长度为 $\frac{1}{2} \times 162.4 \times 10^{-3} \times 2 \times 10^8 = 16240km$ 。

所以该链路长度约为16240km。