

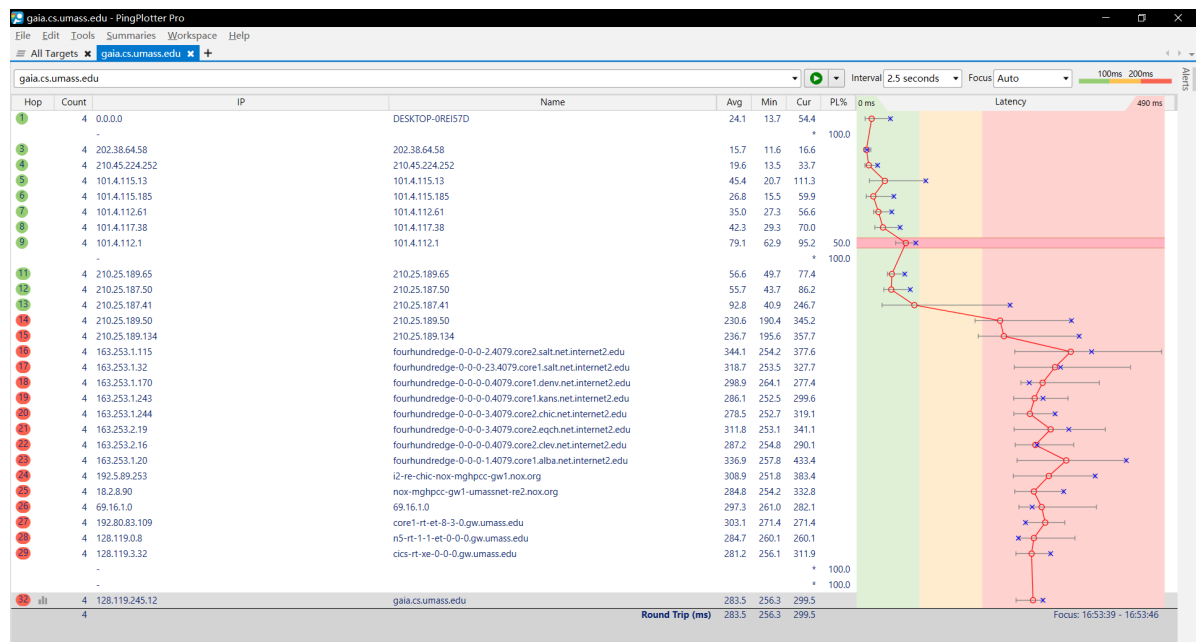
# traceroute实验

## 实验要求

Submit to [bb.ustc.edu.cn](http://bb.ustc.edu.cn)

- A pdf file named "id + name + traceroute.pdf"
- The packet trace you have captured.
- Your answers to the questions
- For Q1, you need to give the screenshot of the result after performing filter rules and packet with the application-layer protocol.
- For Q2- Q6, you need to give the corresponding screenshot and explanation.
- deadline: 2021/11/30

## traceroute:



## Q&A:

**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?**

rules:

ip.src == 114.214.246.214 && ip.dst == 128.119.245.12 && icmp && ip

screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
76	2.891278	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3805/56590, ttl=255 (no response found!)
79	2.932506	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3806/56846, ttl=1 (no response found!)
82	2.972499	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3807/57102, ttl=2 (no response found!)
85	3.011104	0.0.0.0	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
89	3.012409	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3808/57358, ttl=3 (no response found!)
94	3.053156	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3809/57614, ttl=4 (no response found!)
97	3.094980	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3810/57870, ttl=5 (no response found!)
98	3.097013	202.38.64.58	114.214.246.214	ICMP	590	Time-to-live exceeded (Time to live exceeded in transit)
99	3.097013	210.45.224.252	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
106	3.122693	101.4.115.13	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
115	3.134822	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3811/58126, ttl=6 (no response found!)
122	3.174666	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3812/58382, ttl=7 (no response found!)
126	3.214512	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3813/58638, ttl=8 (no response found!)
130	3.214540	101.4.115.185	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
139	3.254487	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3814/58894, ttl=9 (no response found!)
146	3.294805	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3815/59150, ttl=10 (no response found!)
151	3.336249	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3816/59406, ttl=11 (no response found!)
155	3.377068	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3817/59662, ttl=12 (no response found!)
156	3.387960	101.4.112.61	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
157	3.387960	101.4.117.38	114.214.246.214	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
164	3.417998	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3818/59918, ttl=13 (no response found!)
167	3.457056	114.214.246.214	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=3819/60174, ttl=14 (no response found!)

Frame 76: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{ABC4694B-568E-4E17-B5A2-2F35B1DEF686}, id 0  
 > Interface id: 0 ((Device\NPF\_{ABC4694B-568E-4E17-B5A2-2F35B1DEF686}))  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Nov 25, 2021 17:22:24.177533000 中国标准时间  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1637832144.177533000 seconds  
 [Time delta from previous captured frame: 0.000000000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 2.801278000 seconds]

0000 ac 74 09 35 8a e2 0c dd 24 fd 2e 60 08 00 45 00  
 0010 00 28 29 cb 01 72 ff 01 00 00 72 d6 f6 d6 80 77  
 0020 f5 0c 20 20 20 20 20 20 20 20 20 20 20 20 ..  
 0030 20 20 20 20 20 20

other application layer protocols:

DNS protocol.

screenshot:

No.	Time	Source	Destination	Protocol	Length	Info
56	2.400657	114.214.246.214	202.38.64.56	DNS	77	Standard query 0xa35b A gaia.cs.umass.edu
57	2.401142	114.214.246.214	202.38.64.56	DNS	77	Standard query 0x6ec5 AAAA gaia.cs.umass.edu
58	2.433547	202.38.64.56	114.214.246.214	DNS	93	Standard query response 0xa35b A gaia.cs.umass.edu A 128.119.245.12
60	2.529738	114.214.246.214	202.38.64.17	DNS	77	Standard query 0x6ec5 AAAA gaia.cs.umass.edu
71	2.885422	202.38.64.17	114.214.246.214	DNS	130	Standard query response 0x6ec5 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
100	3.099606	114.214.246.214	202.38.64.56	DNS	85	Standard query 0x721c PTR 58.64.38.202.in-addr.arpa
102	3.111312	114.214.246.214	202.38.64.56	DNS	87	Standard query 0x1940 PTR 252.224.45.210.in-addr.arpa
107	3.122693	202.38.64.56	114.214.246.214	DNS	165	Standard query response 0x721c No such name PTR 58.64.38.202.in-addr.arpa SOA ns.ustc.edu.cn
108	3.122693	202.38.64.56	114.214.246.214	DNS	130	Standard query response 0x6ec5 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
110	3.122693	202.38.64.56	114.214.246.214	DNS	165	Standard query response 0x1940 No such name PTR 252.224.45.210.in-addr.arpa SOA ns.ustc.edu.cn
116	3.136977	114.214.246.214	202.38.64.56	DNS	85	Standard query 0x6a14 PTR 13.115.4.101.in-addr.arpa
131	3.214540	202.38.64.56	114.214.246.214	DNS	170	Standard query response 0x6a14 No such name PTR 13.115.4.101.in-addr.arpa SOA DNS.EDU.CN
136	3.244567	114.214.246.214	202.38.64.56	DNS	86	Standard query 0x6314 PTR 185.115.4.101.in-addr.arpa
152	3.375653	114.214.246.214	202.38.64.17	DNS	86	Standard query 0x6314 PTR 185.115.4.101.in-addr.arpa
158	3.387960	202.38.64.56	114.214.246.214	DNS	171	Standard query response 0x6314 No such name PTR 185.115.4.101.in-addr.arpa SOA DNS.EDU.CN
160	3.401727	114.214.246.214	202.38.64.56	DNS	85	Standard query 0x12b3 PTR 61.112.4.101.in-addr.arpa
161	3.401903	114.214.246.214	202.38.64.56	DNS	85	Standard query 0x6b13 PTR 38.117.4.101.in-addr.arpa
172	3.472294	202.38.64.17	114.214.246.214	DNS	147	Standard query response 0x6314 No such name PTR 185.115.4.101.in-addr.arpa SOA DNS.EDU.CN
173	3.486487	114.214.246.214	202.38.64.56	DNS	84	Standard query 0x944a PTR 1.112.4.101.in-addr.arpa
176	3.487548	114.214.246.214	202.38.64.56	DNS	86	Standard query 0xfc79 PTR 65.189.25.210.in-addr.arpa
182	3.509539	202.38.64.56	114.214.246.214	DNS	170	Standard query response 0x12b3 No such name PTR 61.112.4.101.in-addr.arpa SOA DNS.EDU.CN
183	3.509539	202.38.64.56	114.214.246.214	DNS	170	Standard query response 0x6b13 No such name PTR 38.117.4.101.in-addr.arpa SOA DNS.EDU.CN

Frame 56: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF\_{ABC4694B-568E-4E17-B5A2-2F35B1DEF686}, id 0  
 > Interface id: 0 ((Device\NPF\_{ABC4694B-568E-4E17-B5A2-2F35B1DEF686}))  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Nov 25, 2021 17:22:23.606912000 中国标准时间  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1637832143.606912000 seconds  
 [Time delta from previous captured frame: 0.046922000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 2.400657000 seconds]

0000 ac 74 09 35 8a e2 0c dd 24 fd 2e 60 08 00 45 00  
 0010 00 3f 5f f5 00 00 80 11 00 00 72 d6 f6 d6 ca 26 ?  
 0020 40 38 e3 8f 00 35 00 2b 74 40 a3 5b 01 00 00 01  
 0030 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75  
 0040 60 61 73 73 03 65 64 75 00 00 01 00 01

## 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?

hops: 30

is this packet fragmented? yes

fragment count: 3 (见下图)





