

**Gökhan Özeloğlu - 21627557**

**Burak Yılmaz - 21627868**

**BBM 453 Computer Networks Lab - ICMP Lab Assignment**

**Group ID: 1**

1. What is the IP address of your host? What is the IP address of the destination host?

Ans: The IP address of our host is **192.168.1.41**. The IP address of the destination host is **141.193.213.20**.

```
C:\Users\gozel>ping -n 10 www.stanford.edu

Pinging www.stanford.edu [141.193.213.20] with 32 bytes of data:
Reply from 141.193.213.20: bytes=32 time=20ms TTL=56
Reply from 141.193.213.20: bytes=32 time=19ms TTL=56
Reply from 141.193.213.20: bytes=32 time=19ms TTL=56
Reply from 141.193.213.20: bytes=32 time=17ms TTL=56
Reply from 141.193.213.20: bytes=32 time=18ms TTL=57
Reply from 141.193.213.20: bytes=32 time=18ms TTL=56
Reply from 141.193.213.20: bytes=32 time=18ms TTL=56
Reply from 141.193.213.20: bytes=32 time=20ms TTL=56
Reply from 141.193.213.20: bytes=32 time=25ms TTL=56
Reply from 141.193.213.20: bytes=32 time=18ms TTL=56

Ping statistics for 141.193.213.20:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 25ms, Average = 19ms
```

No.	Time	Source	Destination	Protocol	Length	Info
20184	54.024253	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=335/20225, ttl=128 (reply in 20185)
20185	54.045056	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=335/20225, ttl=56 (request in 20184)
20186	55.038777	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=336/20481, ttl=128 (reply in 20187)
20187	55.058598	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=336/20481, ttl=56 (request in 20186)
20190	56.051756	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=337/20737, ttl=128 (reply in 20191)
20191	56.071297	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=337/20737, ttl=56 (request in 20190)
20206	57.067991	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=338/20993, ttl=128 (reply in 20207)
20207	57.085833	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=338/20993, ttl=56 (request in 20206)
20208	58.084693	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=339/21249, ttl=128 (reply in 20209)
20209	58.103093	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=339/21249, ttl=57 (request in 20208)
20214	59.093526	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=340/21505, ttl=128 (reply in 20215)
20215	59.111972	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=340/21505, ttl=56 (request in 20214)
20216	60.103914	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=341/21761, ttl=128 (reply in 20217)
20217	60.122071	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=341/21761, ttl=56 (request in 20216)
20220	61.114156	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=342/22017, ttl=128 (reply in 20221)
20221	61.134901	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=342/22017, ttl=56 (request in 20220)
20245	62.124341	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=343/22273, ttl=128 (reply in 20246)
20246	62.150219	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=343/22273, ttl=56 (request in 20245)
20247	63.138543	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=344/22529, ttl=128 (reply in 20248)
20248	63.156776	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=344/22529, ttl=56 (request in 20247)

> Frame 20184: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{D7A6458E-FA4F-47A4-81AE-6F992169F9E7}, id 0

> Ethernet II, Src: HewlettP\_1a:d2:10 (a0:8c:fd:1a:d2:10), Dst: zte\_19:98:fe (e0:19:54:19:98:fe)

> Internet Protocol Version 4, Src: 192.168.1.41, Dst: 141.193.213.20

> Internet Control Message Protocol

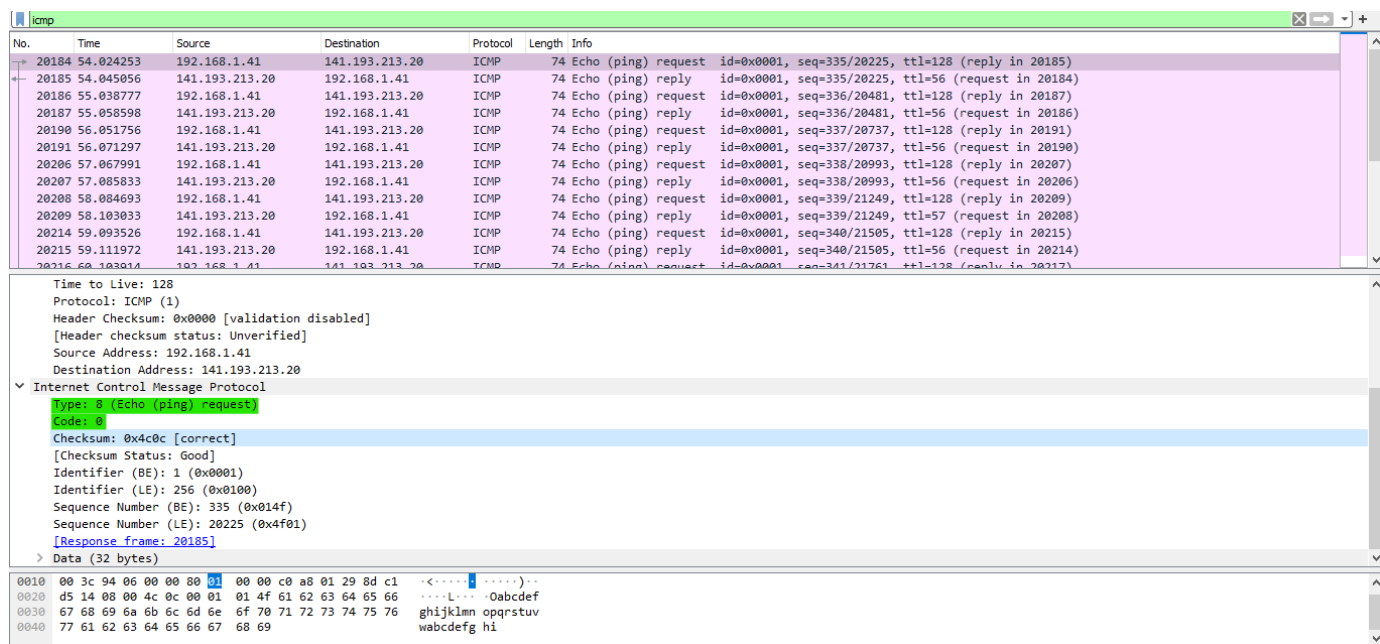
2. Why is it that an ICMP packet does not have source and destination port numbers?

Ans: It is designed for communicating network layer information between hosts and routers, not between application layer protocols. It does not exchange data so that it does not have any specific port.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this

ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Ans:



No.	Time	Source	Destination	Protocol	Length	Info
20184	54.024253	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=335/20225, ttl=128 (reply in 20185)
20185	54.045056	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=335/20225, ttl=56 (request in 20184)
20186	55.038777	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=336/20481, ttl=128 (reply in 20187)
20187	55.058598	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=336/20481, ttl=56 (request in 20186)
20190	56.051756	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=337/20737, ttl=128 (reply in 20191)
20191	56.071297	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=337/20737, ttl=56 (request in 20190)
20206	57.067991	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=338/20993, ttl=128 (reply in 20207)
20207	57.085833	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=338/20993, ttl=56 (request in 20206)
20208	58.084693	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=339/21249, ttl=128 (reply in 20209)
20209	58.103033	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=339/21249, ttl=57 (request in 20208)
20214	59.093526	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=340/21505, ttl=128 (reply in 20215)
20215	59.111972	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=340/21505, ttl=56 (request in 20214)
20216	60.103014	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=341/21761, ttl=128 (reply in 20217)

Time to Live: 128  
Protocol: ICMP (1)  
Header Checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.1.41  
Destination Address: 141.193.213.20

Internet Control Message Protocol

Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0x4c0c [correct]  
[Checksum Status: Good]  
Identifier (BE): 1 (0x0001)  
Identifier (LE): 256 (0x0100)  
Sequence Number (BE): 335 (0x014f)  
Sequence Number (LE): 20225 (0x4f01)  
[Response frame: 20185]

Data (32 bytes)

0010 00 3c 94 06 00 00 80 00 00 c0 a8 01 29 8d c1 <----->  
0020 d5 14 08 00 4c 0c 00 01 01 4f 61 62 63 64 65 66 ----L---.Oabcdef  
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv  
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

The ICMP type is **8** and the code number is **0**. Also, there are **checksum, identifier, sequence number, and data** fields. The checksum, identifier, sequence number fields have **2 bytes**.

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Ans:

No.	Time	Source	Destination	Protocol	Length	Info
20184	54.024253	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=335/20225, ttl=128 (reply in 20185)
20185	54.045056	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=335/20225, ttl=56 (request in 20184)
20186	55.038777	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=336/20481, ttl=128 (reply in 20187)
20187	55.058598	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=336/20481, ttl=56 (request in 20186)
20190	56.051756	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=337/20737, ttl=128 (reply in 20191)
20191	56.071297	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=337/20737, ttl=56 (request in 20190)
20206	57.067991	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=338/20993, ttl=128 (reply in 20207)
20207	57.085833	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=338/20993, ttl=56 (request in 20206)
20208	58.084693	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=339/21249, ttl=128 (reply in 20209)
20209	58.103033	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=339/21249, ttl=57 (request in 20208)
20214	59.093526	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=340/21505, ttl=128 (reply in 20215)
20215	59.111972	141.193.213.20	192.168.1.41	ICMP	74	Echo (ping) reply id=0x0001, seq=340/21505, ttl=56 (request in 20214)
20216	59.103014	192.168.1.41	141.193.213.20	ICMP	74	Echo (ping) request id=0x0001, seq=341/21761, ttl=128 (reply in 20217)

Protocol: ICMP (1)	
Header Checksum: 0x36f4 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 141.193.213.20	
Destination Address: 192.168.1.41	
Internet Control Message Protocol	
Type: 0 (Echo (ping) reply)	
Code: 0	
Checksum: 0x540c [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 335 (0x014f)	
Sequence Number (LE): 20225 (0x4f01)	
[Request frame: 20184]	
[Response time: 20,803 ms]	
> Data (32 bytes)	

```

0000 a0 8c fd 1a d2 10 e0 19 54 19 98 fe 08 00 45 00 .....T....E:
0010 00 3c 27 26 00 00 38 01 36 f4 8d c1 d5 14 c0 a8 <'.&..8..6.....
0020 01 29 00 00 54 0c 00 01 01 4f 61 62 63 64 65 66 .).T....0abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

```

The ICMP type is **0** and the code number is **0**. Also, there are **checksum**, **identifier**, **sequence number**, and **data** fields. The checksum, identifier, sequence number fields have **2 bytes**.

5. What is the IP address of your host? What is the IP address of the target destination host?

Ans:

```

C:\Users\gozel>tracert www.stanford.edu

Tracing route to 89wyd637cdel.wpeproxy.com [141.193.213.21]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    hgw.local [192.168.1.1]
  2   1 ms     1 ms     1 ms     212.156.201.194.static.turktelekom.com.tr [212.156.201.194]
  3   5 ms     6 ms     5 ms     81.212.2.197.static.turktelekom.com.tr [81.212.2.197]
  4   1 ms     1 ms     1 ms     07-antalya-xrs-t2-2---07-antalya-t3-4.statik.turktelekom.com.tr [81.212.217.190]
  5  14 ms    15 ms    14 ms    00-gayrettepe-xrs-t2-2---07-antalya-xrs-t2-2.statik.turktelekom.com.tr [212.156.117.23]

  6  14 ms    16 ms    15 ms    31.210.9.177
  7  15 ms    15 ms    22 ms    31.210.12.6
  8  15 ms    15 ms    15 ms    141.193.213.21

Trace complete.

```

No.	Time	Source	Destination	Protocol	Length	Info
31	1.790742	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=399/36609, ttl=1 (no response found!)
32	1.791452	192.168.1.1	192.168.1.41	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
33	1.792205	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=400/36865, ttl=1 (no response found!)
34	1.792943	192.168.1.1	192.168.1.41	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
35	1.793657	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=401/37121, ttl=1 (no response found!)
36	1.794318	192.168.1.1	192.168.1.41	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
925	7.344956	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=402/37377, ttl=2 (no response found!)
926	7.346181	212.156.201.194	192.168.1.41	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
927	7.348992	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=403/37633, ttl=2 (no response found!)
928	7.349357	212.156.201.194	192.168.1.41	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
929	7.350928	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=404/37889, ttl=2 (no response found!)
930	7.352174	212.156.201.194	192.168.1.41	ICMP	94	Time-to-live exceeded (Time to live exceeded in transit)
1440	8.357204	192.168.1.41	141.193.213.21	ICMP	106	Echo (ping) request id=0x0001, seq=405/38145, ttl=3 (no response found!)

> Time to Live: 1	
Protocol: ICMP (1)	
Header Checksum: 0x0000 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.1.41	
Destination Address: 141.193.213.21	
▼ Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Code: 0	
Checksum: 0xf66f [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 399 (0x018f)	
Sequence Number (LE): 36609 (0x8f01)	
> [No response seen]	
> Data (64 bytes)	

0020	d5 15 08 00 f6 6f 00 01 01 8f 00 00 00 00 00 00	.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Internet Control Message Protocol: Protocol | Packets: 7787 · Displayed: 51 (0.7%) · Dropped: 0 (0.0%) | Profile: Default

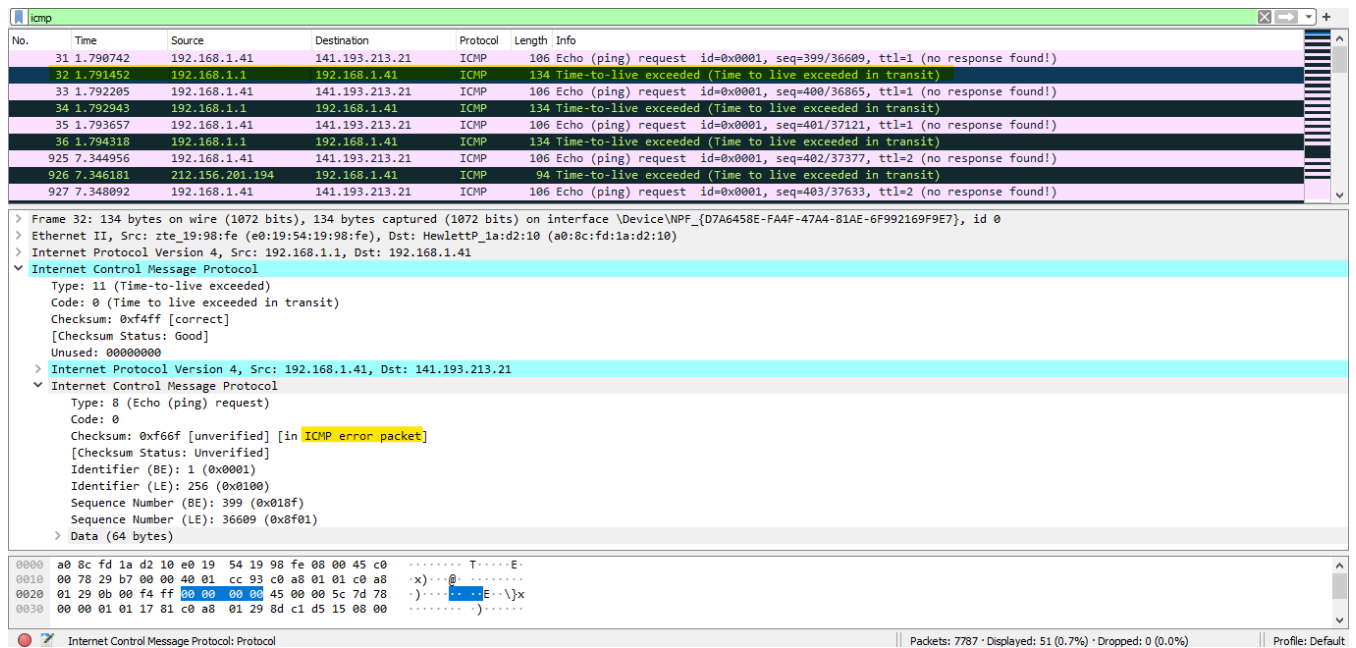
The IP address of our host is **192.168.1.1**. The IP address of the destination host is **141.193.213.21**.

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

Ans: No. It would be different if ICMP sent UDP packets. It would be **0x11** instead of 01.

7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP ping packet. What is included in those fields?

Ans:



It contains the IP header and the first 8 bytes of the original ICMP packet that the error is for.

8. Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in your figure, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Ans:

```
C:\Users\gozel>tracert stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  1  1 ms  <1 ms  <1 ms  hgw.local [192.168.1.1]
  2  1 ms  <1 ms  1 ms  212.156.201.194.static.turktelekom.com.tr [212.156.201.194]
  3  2 ms  2 ms  2 ms  81.212.2.197.static.turktelekom.com.tr [81.212.2.197]
  4  2 ms  1 ms  1 ms  07-antalya-xrs-t2-2---07-antalya-t3-4.statik.turktelekom.com.tr [81.212.217.190]
  5  15 ms  14 ms  14 ms  00-gayrettepe-xrs-t2-2---07-antalya-xrs-t2-2.statik.turktelekom.com.tr [212.156.117.23]

  6  14 ms  14 ms  14 ms  00-ebgp-gayrettepe-k---00-gayrettepe-xrs-t2-2.statik.turktelekom.com.tr [81.212.202.19]

  7  52 ms  51 ms  51 ms  301-fra-col-2---00-gayrettepe-xrs-t2-2.statik.turktelekom.com.tr [212.156.101.196]
  8  58 ms  52 ms  51 ms  ipv4.decix-frankfurt.core1.fra1.he.net [80.81.192.172]
  9  58 ms  58 ms  58 ms  100ge1-1.core1.par2.he.net [72.52.92.13]
 10 135 ms 134 ms 135 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 11 192 ms 192 ms 193 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 12 192 ms 193 ms 193 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 13 193 ms 193 ms 193 ms  woa-west-rtr-v13.SUNet [171.66.255.132]
 14  *  *  *  Request timed out.
 15 194 ms 193 ms 193 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

There is a link that has significantly longer delays between steps 4-5 and 9-10. This could occur because of the distance.