Matthew Kehoe CS 356 4/13/17

ICMP Lab

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

Local host :	192.168.1.11
Destination:	143.89.14.2

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

ICMP runs the Network Layer, port numbers are only needed at the Transport Layer which is above Network. Therefore ICMP does not use port numbers.

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?

Type: 8 (Echo (ping) request)
Code: 0

Checksum = 2B
Sequence = 2B
Identifier = 2B

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?

Type: 0 (Echo (ping) reply)
Code: 0

Checksum = 2B
Sequence = 2B
Identifier = 2B

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

Local Host : 192.168.1.11
Destination: 128.93.162.84

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?

Linux uses UDP for traceroute.
Protocol: UDP (17)

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

Ping messages have a body length of 32b, traceroute messages have a body length of 64b. Other than that the two are the same.

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

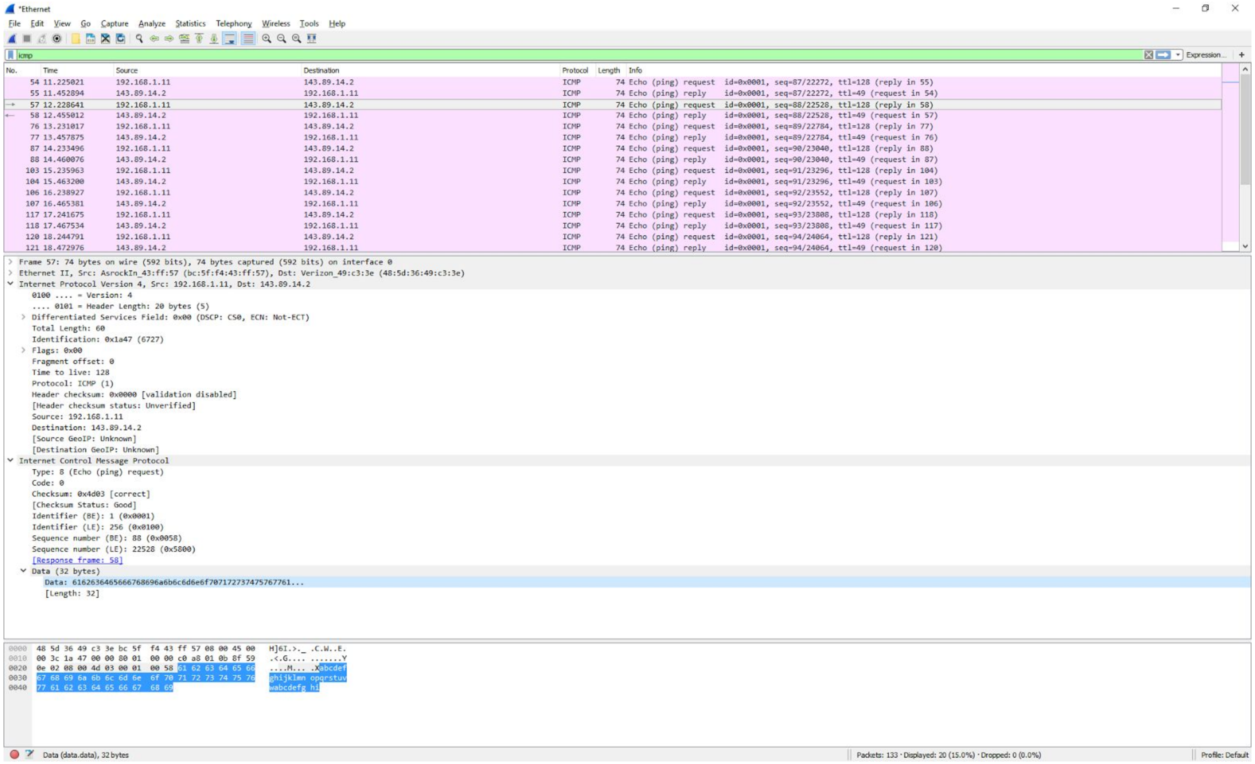
The TTL error packet includes the original ICMP packet headers as well as the error headers in its message.

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three packets received are not errors because they have reached their destination. The destination router then sends a reply back, rather than a TTL error.

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, 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?

There is a gap between
12 ms 11 ms 11 ms vodafone-gw.customer.alter.net [204.148.1.254]
82 ms 81 ms 91 ms ae0-xcr1.nyh.cw.net [195.2.25.70]
The first host 204.148.1.254 is located in Manhattan
The second host 195.2.25.70 is located in London


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

icmp

```
No.  Time       Source        Destination   Protocol Length Info
 54 11.225021   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=87/22272, ttl=128 (reply in 55)
 55 11.452894   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=87/22272, ttl=49 (request in 54)
 57 12.228641   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=88/22528, ttl=128 (reply in 58)
 58 12.455012   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=88/22528, ttl=49 (request in 57)
 76 13.231017   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=89/22784, ttl=128 (reply in 77)
 77 13.457875   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=89/22784, ttl=49 (request in 76)
 87 14.233496   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=90/23040, ttl=128 (reply in 88)
 88 14.460076   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=90/23040, ttl=49 (request in 87)
103 15.235963   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=91/23296, ttl=128 (reply in 104)
104 15.463200   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=91/23296, ttl=49 (request in 103)
106 16.238927   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=92/23552, ttl=128 (reply in 107)
107 16.465381   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=92/23552, ttl=49 (request in 106)
117 17.241675   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=93/23808, ttl=128 (reply in 118)
118 17.467534   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=93/23808, ttl=49 (request in 117)
120 18.244791   192.168.1.11  143.89.14.2   ICMP      74 Echo (ping) request  id=0x0001, seq=94/24064, ttl=128 (reply in 121)
121 18.472976   143.89.14.2   192.168.1.11  ICMP      74 Echo (ping) reply    id=0x0001, seq=94/24064, ttl=49 (request in 120)
```

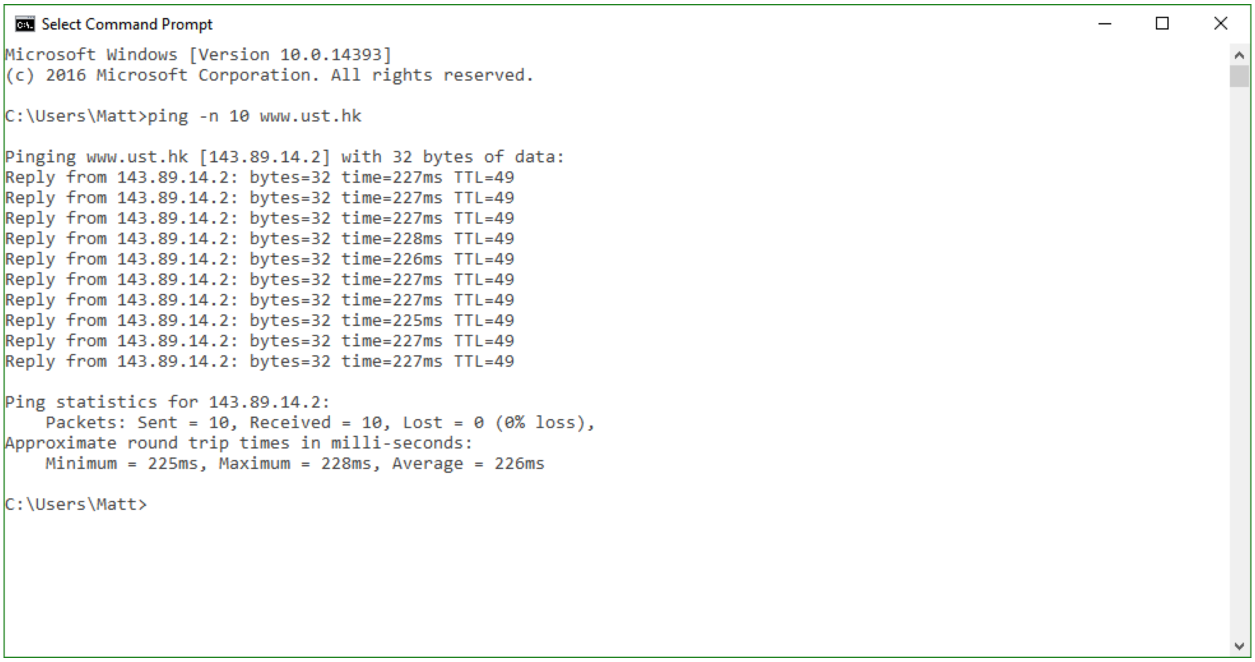
```
> Frame 57: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: AsrockIn_43:ff:57 (bc:5f:f4:43:ff:57), Dst: Verizon_49:c3:3e (48:5d:36:49:c3:3e)
v Internet Protocol Version 4, Src: 192.168.1.11, Dst: 143.89.14.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x1a47 (6727)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.11
    Destination: 143.89.14.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d03 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 88 (0x0058)
    Sequence number (LE): 22528 (0x5800)
    [Response frame: 58]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...
      [Length: 32]
```

```
0000  48 5d 36 49 c3 3e bc 5f  f4 43 ff 57 08 00 45 00   H]6I.>._ .C.W..E.
0010  00 3c 1a 47 00 00 80 01  00 00 c0 a8 01 0b 8f 59   .<.G.... .......Y
0020  0e 02 08 00 4d 03 00 01  00 58 61 62 63 64 65 66   ....M... .Xabcdef
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
```

Data (data.data), 32 bytes

Packets: 133 · Displayed: 20 (15.0%) · Dropped: 0 (0.0%)

Profile: Default



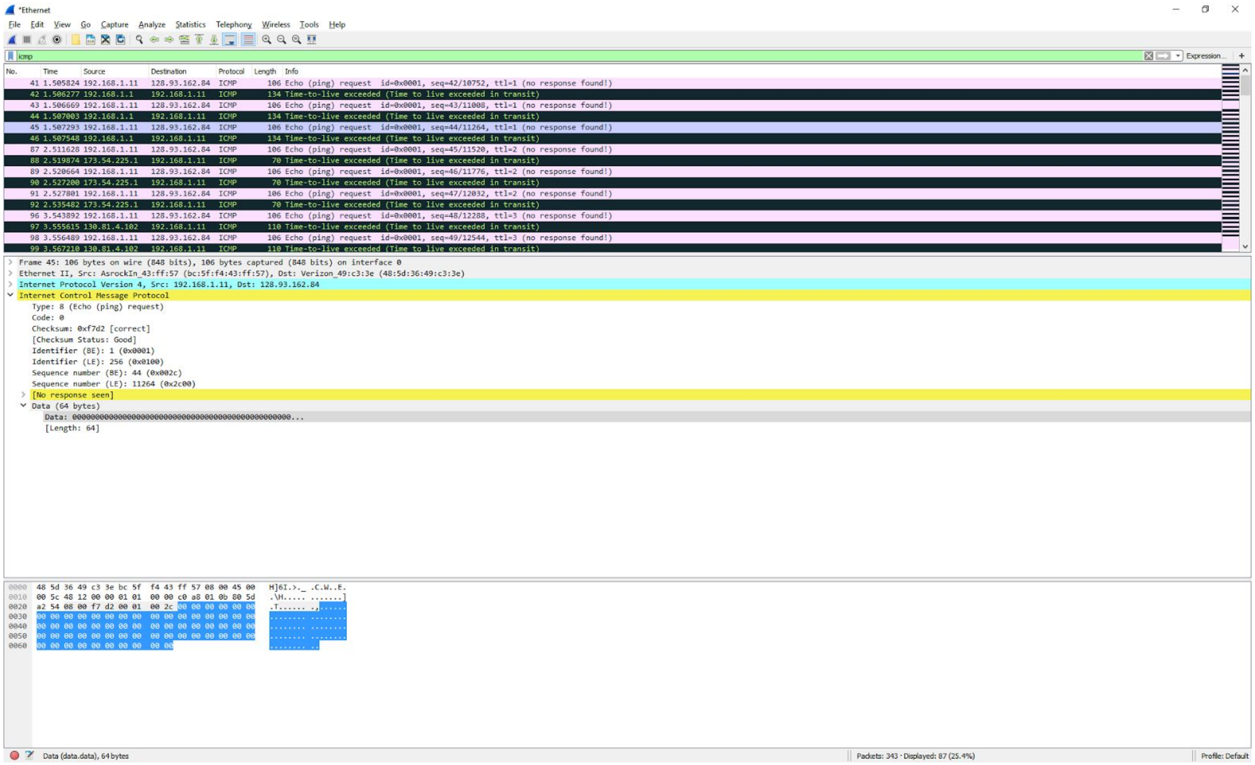
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Matt>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.14.2] with 32 bytes of data:
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=228ms TTL=49
Reply from 143.89.14.2: bytes=32 time=226ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=225ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49
Reply from 143.89.14.2: bytes=32 time=227ms TTL=49

Ping statistics for 143.89.14.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 225ms, Maximum = 228ms, Average = 226ms

C:\Users\Matt>
```


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

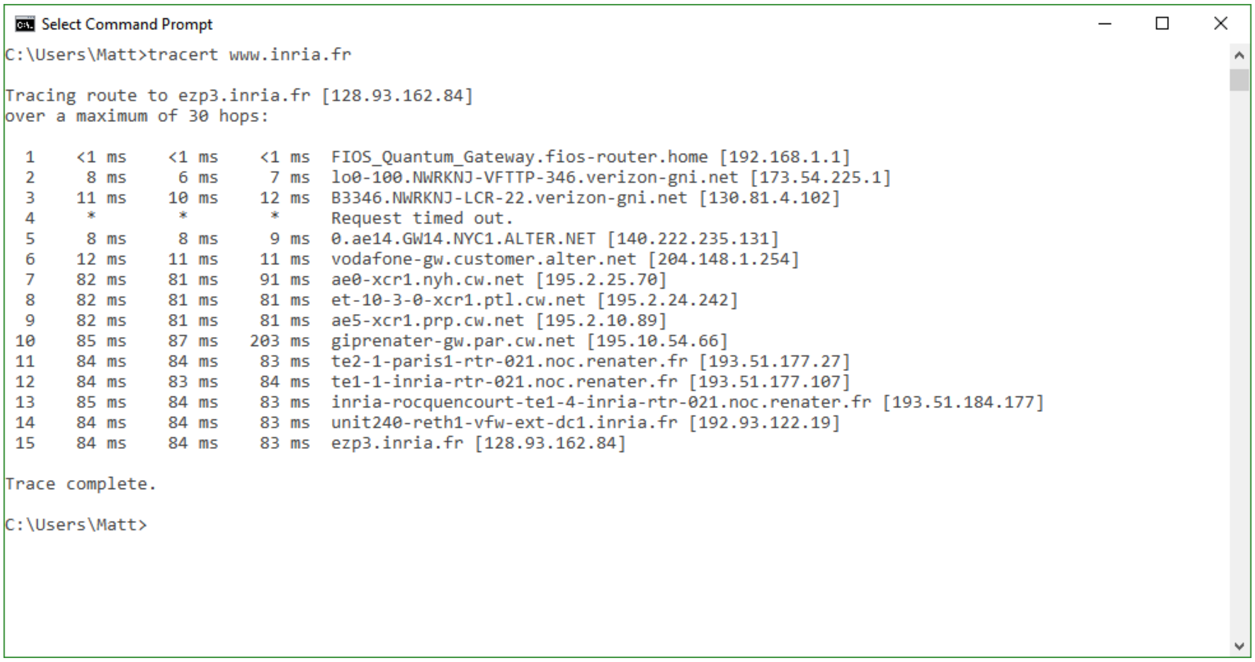
```
icmp
```

```
No.  Time     Source        Destination    Protocol Length Info
  41 1.505824 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=42/10752, ttl=1 (no response found!)
  42 1.506277 192.168.1.1   192.168.1.11   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  43 1.506669 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=43/11008, ttl=1 (no response found!)
  44 1.507003 192.168.1.1   192.168.1.11   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  45 1.507293 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=44/11264, ttl=1 (no response found!)
  46 1.507548 192.168.1.1   192.168.1.11   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
  87 2.511628 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=45/11520, ttl=2 (no response found!)
  88 2.519874 173.54.225.1  192.168.1.11   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  89 2.520664 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=46/11776, ttl=2 (no response found!)
  90 2.527200 173.54.225.1  192.168.1.11   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  91 2.527801 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=47/12032, ttl=2 (no response found!)
  92 2.535482 173.54.225.1  192.168.1.11   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  96 3.543892 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=48/12288, ttl=3 (no response found!)
  97 3.555615 130.81.4.102  192.168.1.11   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
  98 3.556489 192.168.1.11  128.93.162.84  ICMP     106 Echo (ping) request  id=0x0001, seq=49/12544, ttl=3 (no response found!)
  99 3.567210 130.81.4.102  192.168.1.11   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 45: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: AsrockIn_43:ff:57 (bc:5f:f4:43:ff:57), Dst: Verizon_49:c3:3e (48:5d:36:49:c3:3e)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.93.162.84
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7d2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 44 (0x002c)
    Sequence number (LE): 11264 (0x2c00)
  > [No response seen]
  v Data (64 bytes)
      Data: 000000000000000000000000000000000000000000000000...
      [Length: 64]
```

```
0000  48 5d 36 49 c3 3e bc 5f  f4 43 ff 57 08 00 45 00   H]6I.>._ .C.W..E.
0010  00 5c 48 12 00 00 01 01  00 00 c0 a8 01 0b 80 5d   .\H..... .......]
0020  a2 54 08 00 f7 d2 00 01  00 2c 00 00 00 00 00 00   .T...... .,......
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   ........ ........
0060  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

```
Data (data.data), 64 bytes          Packets: 343 · Displayed: 87 (25.4%)          Profile: Default
```



```
C:\Users\Matt>tracert www.inria.fr

Tracing route to ezp3.inria.fr [128.93.162.84]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  FIOS_Quantum_Gateway.fios-router.home [192.168.1.1]
  2     8 ms     6 ms     7 ms  lo0-100.NWRKNJ-VFTTP-346.verizon-gni.net [173.54.225.1]
  3    11 ms    10 ms    12 ms  B3346.NWRKNJ-LCR-22.verizon-gni.net [130.81.4.102]
  4     *        *        *     Request timed out.
  5     8 ms     8 ms     9 ms  0.ae14.GW14.NYC1.ALTER.NET [140.222.235.131]
  6    12 ms    11 ms    11 ms  vodafone-gw.customer.alter.net [204.148.1.254]
  7    82 ms    81 ms    91 ms  ae0-xcr1.nyh.cw.net [195.2.25.70]
  8    82 ms    81 ms    81 ms  et-10-3-0-xcr1.ptl.cw.net [195.2.24.242]
  9    82 ms    81 ms    81 ms  ae5-xcr1.prp.cw.net [195.2.10.89]
 10    85 ms    87 ms   203 ms  giprenater-gw.par.cw.net [195.10.54.66]
 11    84 ms    84 ms    83 ms  te2-1-paris1-rtr-021.noc.renater.fr [193.51.177.27]
 12    84 ms    83 ms    84 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 13    85 ms    84 ms    83 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 14    84 ms    84 ms    83 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 15    84 ms    84 ms    83 ms  ezp3.inria.fr [128.93.162.84]

Trace complete.

C:\Users\Matt>
```