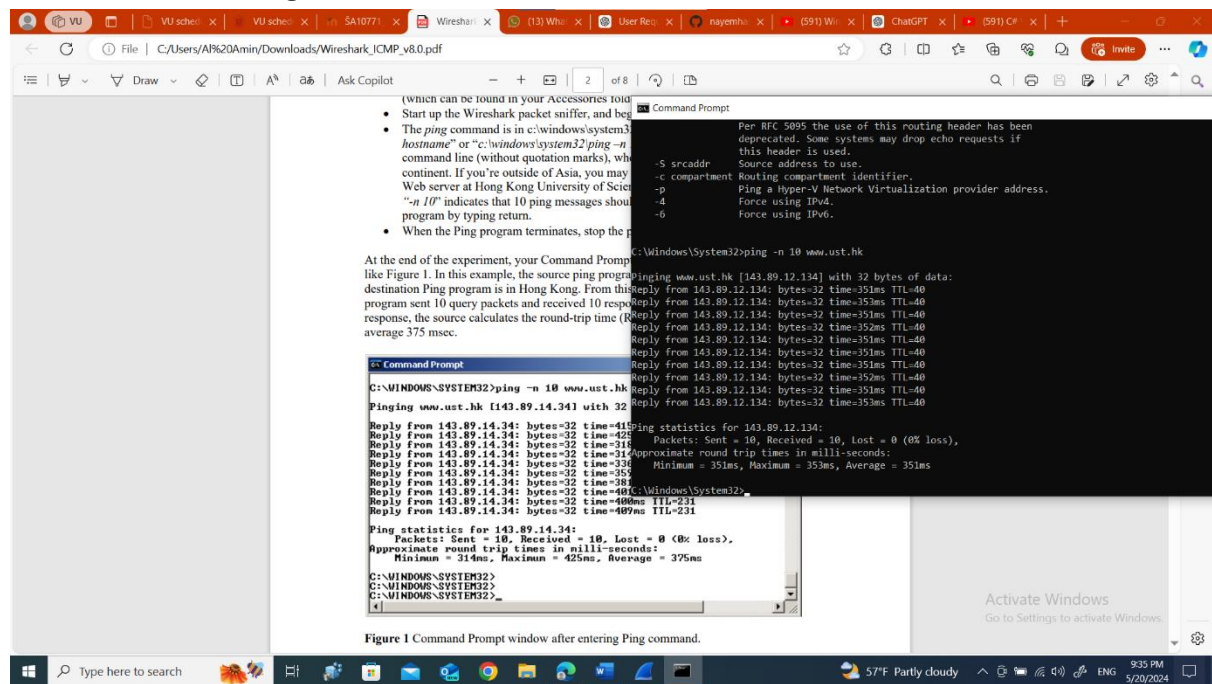


Start wireshark and give this command to cmd.



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

No.	Time	Source	Destination	Protocol	Length	Info
746	52.772392	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 751)
751	53.124203	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=40 (request in 746)
762	53.799005	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 769)
769	54.151882	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=40 (request in 762)
782	54.814106	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 790)
790	55.165745	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=40 (request in 782)
800	55.830447	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 804)
804	56.182144	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=40 (request in 800)
818	56.845430	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 826)
826	57.197034	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=40 (request in 818)
834	57.860224	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 843)
843	58.211767	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=40 (request in 834)
855	58.875659	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 859)
859	59.227281	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=40 (request in 855)
875	59.891192	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 881)
881	60.243420	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=40 (request in 875)
895	60.906651	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 905)
905	61.258473	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=40 (request in 895)
916	61.921934	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 925)

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

Ans. It does not require any source port .

icmp							
No.	Time	Source	Destination	Protocol	Length	Info	
746	52.772392	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
751	53.124203	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
762	53.799005	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
769	54.151882	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
782	54.814106	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
790	55.165745	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
800	55.830447	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
804	56.182144	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
818	56.845430	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
826	57.197034	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
834	57.860224	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
843	58.211767	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
855	58.875659	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
859	59.227281	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
875	59.891192	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
881	60.243420	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
895	60.906651	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,
905	61.258473	143.89.12.134	10.126.39.124	ICMP	74	Echo (ping) reply	id=0x0001,
916	61.921934	10.126.39.124	143.89.12.134	ICMP	74	Echo (ping) request	id=0x0001,

> Frame 746: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{759AB686-F2}

> Ethernet II, Src: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)

> Internet Protocol Version 4, Src: 10.126.39.124, Dst: 143.89.12.134

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d5a [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[\[Response frame: 751\]](#)

> Data (32 bytes)

- 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?

The screenshot shows a Wireshark packet capture on a Wi-Fi interface. The packet list on the left shows several ICMP Echo (ping) requests and replies. The selected packet is a request (No. 746) from 10.126.39.124 to 143.89.12.134. The packet details pane on the right shows the following fields:

- Frame 746: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{759A8686-F2}
- Ethernet II, Src: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)
- Internet Protocol Version 4, Src: 10.126.39.124, Dst: 143.89.12.134
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xd45a [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 1 (0x0001)
 - Sequence Number (LE): 256 (0x0100)
 - [Response frame: 751]
 - Data (32 bytes)

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The ASCII part shows the letters 'E' and 'Y'.

- 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?

The screenshot shows the same Wireshark packet capture. The selected packet is a reply (No. 751) from 143.89.12.134 to 10.126.39.124. The packet details pane on the right shows the following fields:

- Frame 751: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{759A8686-F2}
- Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
- Internet Protocol Version 4, Src: 143.89.12.134, Dst: 10.126.39.124
- Internet Control Message Protocol
 - Type: 0 (Echo (ping) reply)
 - Code: 0
 - Checksum: 0x555a [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 1 (0x0001)
 - Sequence Number (LE): 256 (0x0100)
 - [Request frame: 746]
 - [Response time: 351.811 ms]
 - Data (32 bytes)

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII. The ASCII part shows the letters 'E' and 'Y'.

Now ICMP and Traceroute

The screenshot shows a Windows desktop with a Wireshark packet capture of ICMP Echo (ping) requests. The packet list shows several ping requests from 10.126.39.124 to 128.93.162.83, all of which are marked as "Time to live exceeded" or "Destination unreachable". The packet details pane shows the ICMP Echo (ping) request structure, including the type (8), code (0), checksum, identifier (1), sequence number (1), and sequence number (1). The packet bytes pane shows the raw data of the ICMP Echo request.

Command Prompt output:

```
C:\Windows\System32>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:
  0  5 ms  4 ms  4 ms  10.126.32.1
  1  5 ms  5 ms  5 ms  158.129.162.1
  2  5 ms  4 ms  4 ms  193.219.95.1
  3  21 ms  30 ms  5 ms  193.219.62.5
  4  7 ms  7 ms  7 ms  193.219.153.25
  5  7 ms  6 ms  6 ms  193.219.153.25
  6  49 ms  49 ms  49 ms  193.219.153.25
  7  49 ms  49 ms  49 ms  193.219.153.25
  8  49 ms  49 ms  49 ms  193.219.153.25
  9  49 ms  49 ms  49 ms  193.219.153.25
 10  49 ms  49 ms  49 ms  193.219.153.25
 11  49 ms  49 ms  49 ms  193.219.153.25
 12  49 ms  49 ms  49 ms  193.219.153.25
 13  51 ms  51 ms  51 ms  193.219.153.25
 14  50 ms  51 ms  50 ms  193.219.153.25
 15  50 ms  50 ms  50 ms  193.219.153.25
 16  52 ms  50 ms  50 ms  193.219.153.25
 17  51 ms  51 ms  51 ms  193.219.153.25
 18  51 ms  51 ms  51 ms  193.219.153.25

Trace complete.
```

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

The screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests and responses. The packet list shows several ping requests from 10.126.39.124 to 128.93.162.83, all of which are marked as "Time to live exceeded" or "Destination unreachable". The packet details pane shows the ICMP Echo (ping) request structure, including the type (8), code (0), checksum, identifier (1), sequence number (1), and sequence number (1). The packet bytes pane shows the raw data of the ICMP Echo request.

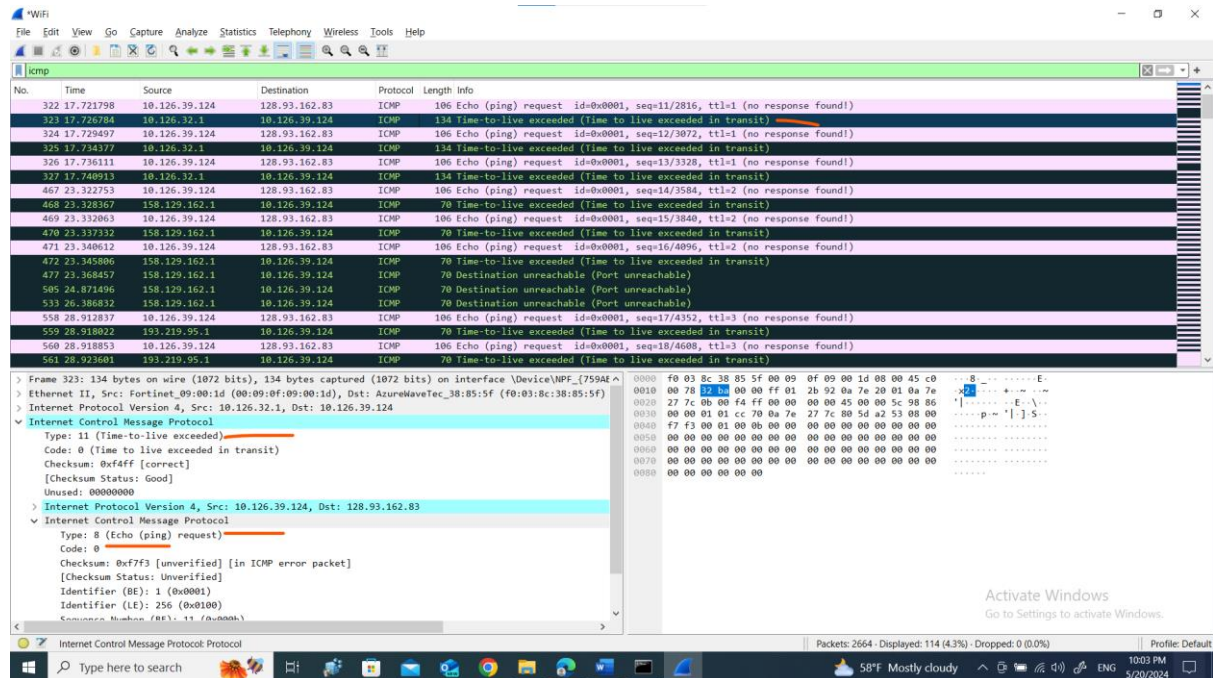
Wireshark packet details:

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xf7f3 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 11 (0x000b)
Sequence Number (LE): 2816 (0x0b00)
[No response seen]
Data (64 bytes)
```

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. (0x11) of 17.

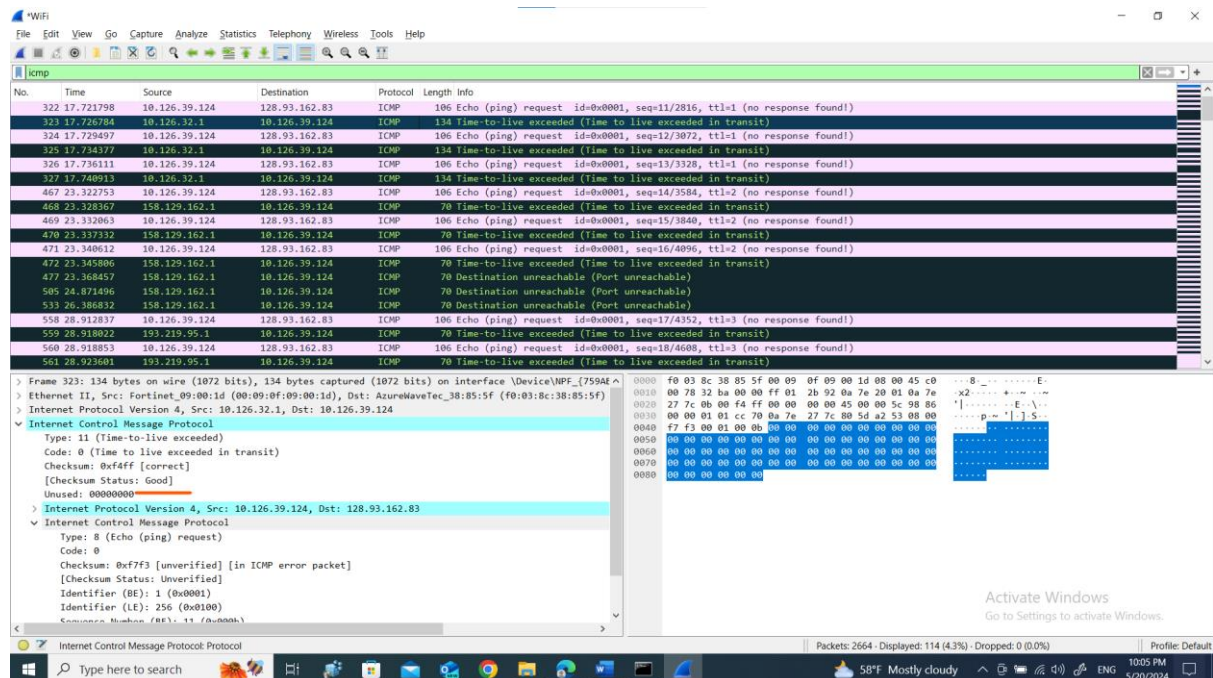
7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?



The screenshot shows a Wireshark capture of ICMP packets. The packet list on the left shows several ICMP Echo (ping) requests. Packet 323 is selected, and the details pane on the right shows the following structure:

- Frame 323: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF... (759AE...)
- Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
- Internet Protocol Version 4, Src: 10.126.32.1, Dst: 10.126.39.124
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf7f3 [unverified] [in ICMP error packet]
 - [Checksum Status: Unverified]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 11 (0x000b)

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 screenshot shows a Wireshark capture of ICMP packets. The packet list on the left shows several ICMP Echo (ping) requests. Packet 472 is selected, and the details pane on the right shows the following structure:

- Frame 323: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF... (759AE...)
- Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
- Internet Protocol Version 4, Src: 10.126.32.1, Dst: 10.126.39.124
- Internet Control Message Protocol
 - Type: 11 (Time-to-live exceeded)
 - Code: 0 (Time to live exceeded in transit)
 - Checksum: 0xf4ff [correct]
 - [Checksum Status: Good]
 - Unused: 00000000
- Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.93.162.83
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf7f3 [unverified] [in ICMP error packet]
 - [Checksum Status: Unverified]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 11 (0x000b)

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 screenshot shows a Wireshark packet capture of ICMP Echo (ping) requests and replies. The last three packets (1191, 1189, 1186) are replies with status 'no response found!'. The packet details pane for packet 1182 shows the ICMP Echo (ping) reply structure:

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0xffff [correct]
- Checksum Status: Good
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 62 (0x003e)
- Sequence Number (LE): 15872 (0x3e00)
- Request frame: 1176
- Response time: 51.220 ms
- Data (64 bytes)

10. Within the traceroute 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?

The screenshot shows the output of the 'tracert www.inria.fr' command in a Windows Command Prompt. The output shows a series of hops with approximate round trip times in milliseconds. The final hop (18) shows a significantly longer delay (51 ms) compared to the others.

```

Approximate round trip times in milli-seconds:
    Minimum = 351ms, Maximum = 353ms, Average = 351ms

C:\Windows\System32>tracert www.inria.fr

Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  10.126.32.1
  1  5 ms  4 ms  4 ms  158.129.162.1
  2  5 ms  5 ms  5 ms  193.219.95.1
  3  5 ms  4 ms  4 ms  193.219.62.5
  4  21 ms 30 ms 5 ms  193.219.153.25
  5  7 ms  7 ms  7 ms  litnet.rt2.kau.lt.geant.net [62.40.125.105]
  6  7 ms  6 ms  6 ms  ae6.mx1.poz.pl.geant.net [62.40.98.169]
  7  49 ms 49 ms 50 ms  ae7.rtl.pra.cz.geant.net [62.40.98.51]
  8  49 ms 49 ms 49 ms  ae6.rtl.fra.de.geant.net [62.40.98.158]
  9  46 ms 43 ms 43 ms  ae5.mx1.gen.ch.geant.net [62.40.98.183]
 10  49 ms 49 ms 49 ms  ae7.mx1.par.fr.geant.net [62.40.98.239]
 11  49 ms 50 ms 50 ms  renater-lb1-gw.mx1.par.fr.geant.net [62.40.124.70]
 12  51 ms 51 ms 51 ms  hu0-4-0-0-ren-nr-orsay-rtr-091.noc.renater.fr [193.51.180.131]
 13  50 ms 51 ms 50 ms  te-0-0-0-13-ren-nr-jouy-rtr-091.noc.renater.fr [193.55.204.199]
 14  50 ms 50 ms 50 ms  te2-8-inria-rtr-021.noc.renater.fr [193.51.180.125]
 15  52 ms 50 ms 50 ms  inria-rocquencourt-vl1631-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 16  51 ms 51 ms 51 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 17  51 ms 51 ms 51 ms  prod-inriafr-cms.inria.fr [128.93.162.83]
 18  51 ms 51 ms 51 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

```