

# Lab 4 - Internet Control Message Protocol

## Computer Networks

Thang Huu Nguyen - 1713239

September, 2019

```
thang@thang:~$ ping -c 10 google.com
PING google.com (172.217.163.238) 56(84) bytes of data.
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=1 ttl=55 time=28.9 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=2 ttl=55 time=27.6 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=3 ttl=55 time=27.7 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=4 ttl=55 time=28.6 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=5 ttl=55 time=28.1 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=6 ttl=55 time=30.1 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=7 ttl=55 time=31.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=8 ttl=55 time=45.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=9 ttl=55 time=31.0 ms
64 bytes from hkg12s18-in-f14.1e100.net (172.217.163.238): icmp_seq=10 ttl=55 time=32.1 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 27.614/31.055/45.084/4.905 ms
```

## 1 ICMP and Ping

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
61	1.268255185	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
65	1.297191064	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
87	2.269772786	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
90	2.297350633	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
103	3.271618667	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
104	3.299353736	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
124	4.273579657	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
125	4.302196312	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
165	5.275425252	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
166	5.303496554	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
188	6.276796714	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
190	6.306901922	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
213	7.278190612	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
215	7.309159099	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply
235	8.279439835	172.17.25.115	172.217.163.238	ICMP	98	Echo (ping) request
236	8.304400000	172.217.163.238	172.17.25.115	ICMP	98	Echo (ping) reply

  

▶ Frame 61: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0  
 ▶ Ethernet II, Src: LiteonTe\_0f:f2:dc (94:e9:79:0f:f2:dc), Dst: 0e:fa:bd:15:43:69 (0e:fa:bd:15:43:69)  
 ▶ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 172.217.163.238  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 84  
 Identification: 0x5278 (21112)  
 ▶ Flags: 0x4000, Don't fragment  
 Time to live: 64  
 Protocol: ICMP (1)  
 Header checksum: 0xd1e4 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 172.17.25.115  
 Destination: 172.217.163.238

**Answers:** The IP address of my host is 172.17.25.115. And the IP address of the destination host is 172.217.163.238.

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

**Answers:** An ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer between source hosts and routers, not between application-layer processes. Each ICMP packet has a particularly **type** and **code** which combination identifies the specific message being received.

## 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?

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xa334 [correct]
  [Checksum Status: Good]
  Identifier (BE): 8010 (0x1f4a)
  Identifier (LE): 18975 (0x4a1f)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Response frame: 65]
  Timestamp from icmp data: Sep 26, 2019 20:33:21.000000000 +07
  [Timestamp from icmp data (relative): 0.037329324 seconds]
  ▶ Data (48 bytes)
```

**Answers:**

- The ICMP type number is 8.
- The ICMP code number is 0.
- The ICMP request packet also has Checksum, Identifier, Sequence number, Timestamp and Data fields.
- The Checksum, Sequence number and Identifier are two bytes each.

## 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?

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xab34 [correct]
  [Checksum Status: Good]
  Identifier (BE): 8010 (0x1f4a)
  Identifier (LE): 18975 (0x4a1f)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Request frame: 61]
  [Response time: 28.936 ms]
  Timestamp from icmp data: Sep 26, 2019 20:33:21.000000000 +07
  [Timestamp from icmp data (relative): 0.066265203 seconds]
  ▶ Data (48 bytes)
```

**Answers:**

- The ICMP type number is 0.
- The ICMP code number is 0.
- The ICMP reply packet also has Checksum, Identifier, Sequence number, Timestamp, Data fields.
- The Checksum, Sequence number and Identifier are two bytes each.

## 2 ICPM and Traceroute

```
thang@thang:~$ sudo traceroute --icmp google.com
[sudo] password for thang:
traceroute to google.com (172.217.163.238), 30 hops max, 60 byte packets
 1 * * *
 2 adsl.hnpt.com.vn (203.210.144.132) 27.900 ms 27.919 ms 27.918 ms
 3 172.17.5.65 (172.17.5.65) 27.929 ms 27.928 ms 27.926 ms
 4 static.vnpt.vn (113.171.48.125) 27.897 ms 27.897 ms 27.894 ms
 5 static.vnpt.vn (113.171.44.113) 47.096 ms 47.098 ms 47.102 ms
 6 static.vnpt.vn (113.171.50.230) 47.042 ms 52.084 ms 52.102 ms
 7 static.vnpt.vn (113.171.32.23) 52.100 ms 52.105 ms 52.111 ms
 8 * * *
 9 108.170.241.65 (108.170.241.65) 55.017 ms 35.854 ms 35.816 ms
10 172.253.64.111 (172.253.64.111) 35.810 ms 35.810 ms 38.451 ms
11 hkq12s18-in-f14.1e100.net (172.217.163.238) 38.441 ms 38.440 ms 38.438 ms
```

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

```
▼ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 172.217.163.238
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb6dd (46813)
  ▶ Flags: 0x0000
  ▶ Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0xec97 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.17.25.115
    Destination: 172.217.163.238
```

**Answers:** The IP address of my host is 172.17.25.115. And the IP address of the target destination host is 172.217.163.238.

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?

```
▼ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 216.58.220.206
  0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x01a8 (424)
  ▶ Flags: 0x0000
  ▶ Time to live: 1
    Protocol: UDP (17)
```

**Answers:** If ICMP sent UDP packets instead, The IP protocol number not still be 01 for the probe packets. It would be 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?

```

▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x5d22 [correct]
  [Checksum Status: Good]
  Identifier (BE): 9559 (0x2557)
  Identifier (LE): 22309 (0x5725)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  ▶ [No response seen]
  ▶ Data (32 bytes)

```

**Answers:** The ICMP echo packet has the most fields as the ping query packets, but it has no timestamp field.

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

```

▼ Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x6a85 [correct]
  [Checksum Status: Good]
  ▶ Internet Protocol Version 4, Src: 172.17.25.115, Dst: 172.217.163.238
  ▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x5d1f [unverified] [in ICMP error packet]
    [Checksum Status: Unverified]
    Identifier (BE): 9559 (0x2557)
    Identifier (LE): 22309 (0x5725)

```

**Answers:** The ICMP error packet is not the same as the ICMP normal packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

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?

**Answers:** The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

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?

```

thang@thang:~$ sudo traceroute --icmp www.lnr1a.fr
[sudo] password for thang:
traceroute to www.lnr1a.fr (128.93.162.84), 30 hops max, 60 byte packets
 1 * * *
 2 adsl.hnpt.com.vn (203.210.144.132) 9.013 ms 9.564 ms 9.574 ms
 3 172.17.5.65 (172.17.5.65) 14.716 ms 14.748 ms 14.751 ms
 4 static.vnpt.vn (113.171.14.97) 9.551 ms 10.965 ms 10.981 ms
 5 static.vnpt.vn (113.171.7.225) 12.336 ms 12.342 ms 12.345 ms
 6 static.vnpt.vn (113.171.50.230) 12.268 ms 5.734 ms 7.806 ms
 7 * * *
 8 et-16-0-0-0-pastr3--opentransit.net (193.251.242.78) 151.685 ms 153.843 ms 153.896 ms
 9 hundredglge0-0-0-9-partr2--opentransit.net (193.251.131.166) 153.905 ms 153.915 ms 153.212 ms
10 ae1-cr0-par9-ip4-gtt.net (77.67.73.1) 231.137 ms 231.173 ms 231.173 ms
11 xe-0-3-3-cr4-par7-ip4-gtt.net (141.136.109.82) 229.559 ms 230.010 ms 231.124 ms
12 renater-gw-tx1-gtt.net (77.67.123.206) 232.281 ms 228.714 ms 229.115 ms
13 te1-1-lnria-rtr-021.noc.renater.fr (193.51.177.107) 231.305 ms 231.328 ms 231.331 ms
14 lnria-rocquencourt-te1-4-lnria-rtr-021.noc.renater.fr (193.51.184.177) 229.904 ms 228.022 ms 228.026 ms
15 unit240-reth1-vfw-ext-dcl-lnria.fr (192.93.122.19) 230.555 ms 229.018 ms 234.480 ms
16 e2p3.lnr1a.fr (128.93.162.84) 235.292 ms 235.762 ms 228.737 ms

```

**Answers:** There is a link between steps 6 and 7 that has a significantly longer delay. This is a transatlantic link from Vietnam to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.