Leonardo Aviles
Data Com. and Security
Paul Smith
February 19,2017

Lab 2

ICMP and Ping

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

For the first packet the src IP address is 192.168.0.104 which is my computers IP address. The destination IP address is 143.89.14.2 which is the IP address of http://www.ust.hk/.

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

ICMP packet does not have source and destination port numbers because it is meant to communicate with the server and not with a specific port number.

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 type of the first packet is type 8 with a code of 0. The other fields in this packet are checksum which is 2 bytes long. There are two identifier fields one is called (BE) which is also 2 bytes long and (LE) which is 2 bytes long. There is also a sequence number which is split into two fields (BE) and (LE) each 2 bytes long.

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 reply packet has type 0 (Echo (ping) reply) with a code of 0. The reply packet has a checksum which is 2 bytes. A identifier split into two 2 byte fields and a sequence number split into 2 2 byte fields. There is also a response time and request frame which has a value of 1.

```
C:\Users\avile>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=232ms TTL=39
Reply from 143.89.14.2: bytes=32 time=234ms TTL=39
Reply from 143.89.14.2: bytes=32 time=235ms TTL=39
Reply from 143.89.14.2: bytes=32 time=232ms TTL=39
Reply from 143.89.14.2: bytes=32 time=233ms TTL=39
Reply from 143.89.14.2: bytes=32 time=235ms TTL=39
Reply from 143.89.14.2: bytes=32 time=234ms TTL=39
Reply from 143.89.14.2: bytes=32 time=232ms TTL=39
Reply from 143.89.14.2: bytes=32 time=234ms TTL=39
Reply from 143.89.14.2: bytes=32 time=233ms TTL=39

Ping statistics for 143.89.14.2:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 232ms, Maximum = 235ms, Average = 233ms
```

Figure 1: Shows the ping command being used on www.ust.hk

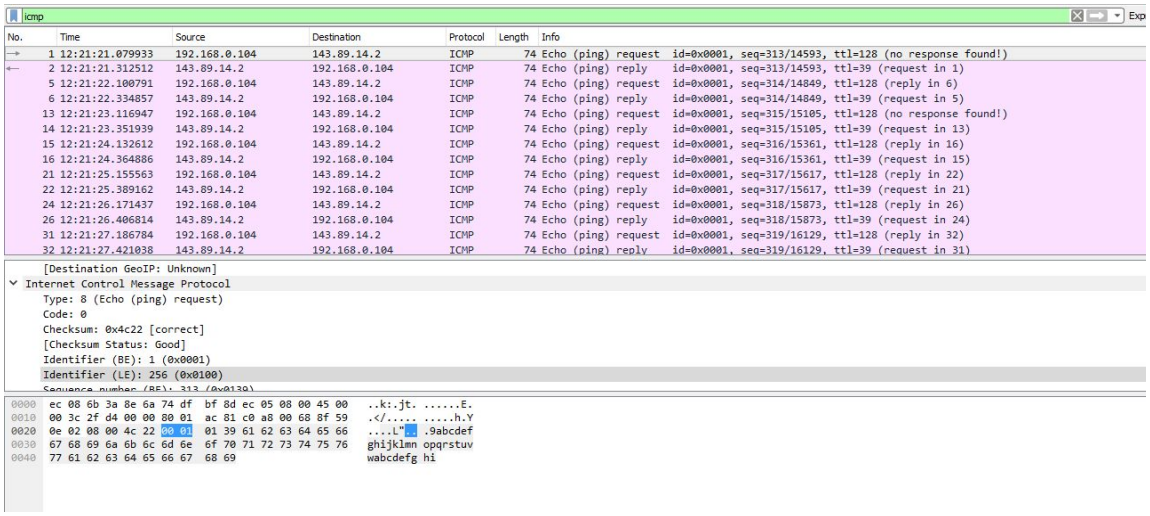

Figure 2: Shows the wireshark capture of the packet ping request

ICMP and Tracert

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

The host IP address is 192.168.0.104 while the destination IP address is 128.93.162.84.

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?

The number would 17 instead of the protocol number one we received.

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 packets are not different they both have the type,code,checksum,identifier and sequence number field.

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

The new fields area field which contains IPv4 with the src and destination IP addresses listed in the drop down menu. The type is also different with it being 11 (TTL exceeded).

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 replies from 128.93.162.84. In this packet the type is 0 (Echo (ping) reply). The response time is 94.533 ms while in the error packet there was no response time.

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?

At hop 9 to 10 there is a increase in the amount of mSeconds it takes. The time goes from 6,7,6 to a much larger 82,84,83 mSeconds. From looking up the IP addresses the location change from Canada to the United Kingdom.

```
Approximate round trip times in milli-seconds:
    Minimum = 232ms, Maximum = 235ms, Average = 233ms

C:\Users\avile>tracert www.inria.fr

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

  1     4 ms     2 ms     2 ms  192.168.0.1
  2     4 ms     3 ms     6 ms  174.141.140.1
  3     4 ms     2 ms     2 ms  10.217.99.1
  4     7 ms     7 ms     3 ms  10.217.98.1
  5     3 ms     3 ms     3 ms  38.140.149.33
  6     3 ms     4 ms     3 ms  be3164.rcr22.phl01.atlas.cogentco.com [154.54.25.141]
  7     6 ms     8 ms     7 ms  be2333.ccr42.jfk02.atlas.cogentco.com [154.54.5.1]
  8    12 ms     7 ms     6 ms  be2057.ccr21.jfk10.atlas.cogentco.com [154.54.80.178]
  9     6 ms     7 ms     6 ms  vodafone.jfk10.atlas.cogentco.com [154.54.9.22]
 10    82 ms    81 ms    79 ms  ae0-xcr1.nyh.cw.net [195.2.25.70]
 11    84 ms    84 ms    83 ms  et-10-1-5-xcr1.ptl.cw.net [195.2.24.242]
 12    88 ms    85 ms    87 ms  ae5-xcr1.prp.cw.net [195.2.10.89]
 13    95 ms   100 ms    99 ms  renater-gw-prp.cw.net [195.10.54.66]
 14    93 ms    96 ms    95 ms  te1-1-paris1-rtr-021.noc.renater.fr [193.51.177.25]
 15    95 ms    93 ms    93 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 16    95 ms   100 ms   103 ms  inria-rocquencourt-te1-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 17    94 ms    95 ms    94 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 18    94 ms    95 ms    94 ms  ezp3.inria.fr [128.93.162.84]

Trace complete.
```

Figure 3: Shows the tracert on www.inria.fr in windows command prompt

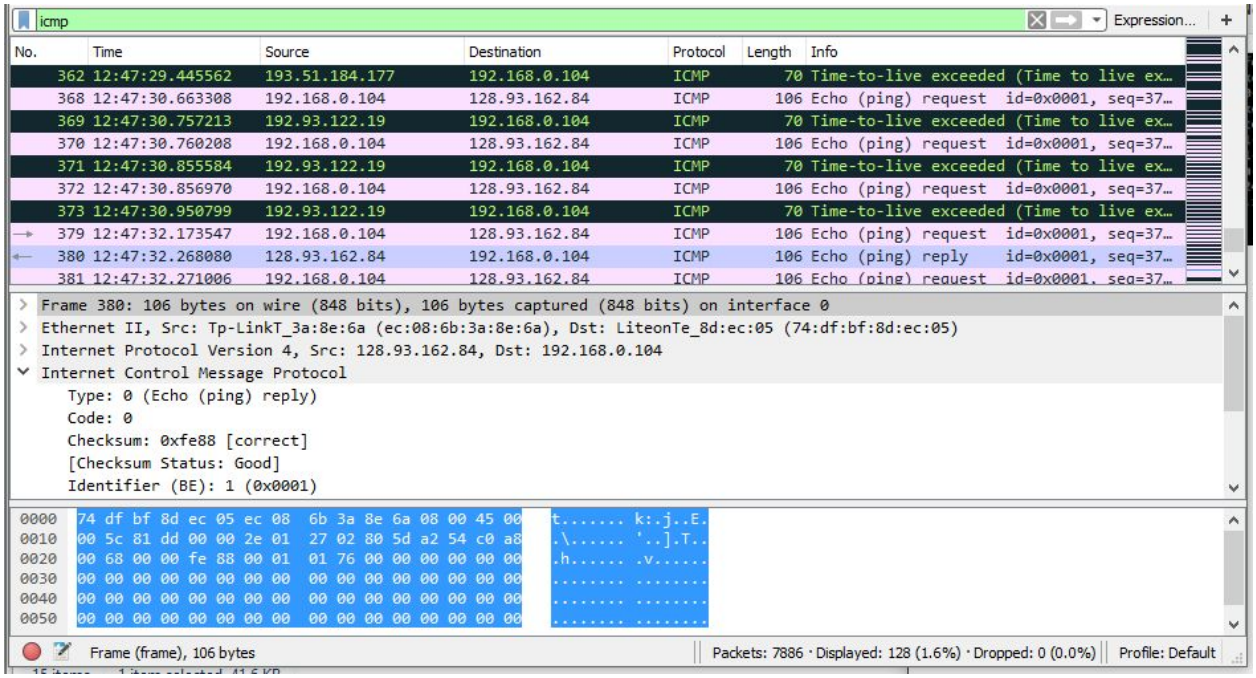

Figure 4: Shows the packet capture of tracert