

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

No.	Time	Source	Destination	Protocol	Length	Info
1	12:21:21.079933	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=313/14593, ttl=128 (no response found!)
2	12:21:21.312512	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=313/14593, ttl=39 (request in 1)
5	12:21:22.100791	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=314/14649, ttl=128 (reply in 6)
6	12:21:22.334857	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=314/14649, ttl=39 (request in 5)
13	12:21:23.116947	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=315/15105, ttl=128 (no response found!)
14	12:21:23.351939	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=315/15105, ttl=39 (request in 13)
15	12:21:24.132612	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=316/15361, ttl=128 (reply in 16)
16	12:21:24.364886	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=316/15361, ttl=39 (request in 15)
21	12:21:25.155563	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=317/15617, ttl=128 (reply in 22)
22	12:21:25.389162	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=317/15617, ttl=39 (request in 21)
24	12:21:26.171437	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=318/15873, ttl=128 (reply in 26)
26	12:21:26.406814	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=318/15873, ttl=39 (request in 24)
31	12:21:27.186784	192.168.0.104	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=319/16129, ttl=128 (reply in 32)
32	12:21:27.421038	143.89.14.2	192.168.0.104	ICMP	74	Echo (ping) reply id=0x0001, seq=319/16129, ttl=39 (request in 31)

  

[Destination GeoIP: Unknown]	
Internet Control Message Protocol	
Type:	8 (Echo (ping) request)
Code:	0
Checksum:	0x4c22 [correct]
[Checksum Status:	Good]
Identifier (BE):	1 (0x0001)
Identifier (LE):	256 (0x0100)
Sequence number (BE): 313 (0x0130)	

  

0000	ec 08 bb 3a 8e 6a 74 df bf 8d ec 05 08 00 45 00	..k:jt. ....E.
0010	00 3c 2f d4 00 00 00 01 ac 81 c0 a8 00 68 8f 59	./.....h.Y
0020	0e 02 08 00 4c 22 00 01 01 39 61 62 63 64 65 66	....L. .9abcdef
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

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](http://www.inria.fr) in windows command prompt

No.	Time	Source	Destination	Protocol	Length	Info
362	12:47:29.445562	193.51.184.177	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live ex...
368	12:47:30.663308	192.168.0.104	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=37...
369	12:47:30.757213	192.93.122.19	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live ex...
370	12:47:30.760208	192.168.0.104	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=37...
371	12:47:30.855584	192.93.122.19	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live ex...
372	12:47:30.856970	192.168.0.104	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=37...
373	12:47:30.950799	192.93.122.19	192.168.0.104	ICMP	70	Time-to-live exceeded (Time to live ex...
→ 379	12:47:32.173547	192.168.0.104	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=37...
← 380	12:47:32.268080	128.93.162.84	192.168.0.104	ICMP	106	Echo (ping) reply id=0x0001, seq=37...
381	12:47:32.271006	192.168.0.104	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=37...

  

> Frame 380: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0	
> Ethernet II, Src: Tp-LinkT_3a:8e:6a (ec:08:6b:3a:8e:6a), Dst: LiteonTe_8d:ec:05 (74:df:bf:8d:ec:05)	
> Internet Protocol Version 4, Src: 128.93.162.84, Dst: 192.168.0.104	
v Internet Control Message Protocol <div>             Type: 0 (Echo (ping) reply)             <div>               Code: 0               <div>                 Checksum: 0xfe88 [correct]                 <div>                   [Checksum Status: Good]                   <div>                     Identifier (BE): 1 (0x0001) </div> </div> </div> </div> </div>	
0000	74 df bf 8d ec 05 ec 08 6b 3a 8e 6a 08 00 45 00
0010	00 5c 81 dd 00 00 2e 01 27 02 80 5d a2 54 c0 a8
0020	00 68 00 00 fe 88 00 01 01 76 00 00 00 00 00 00
0030	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
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 4: Shows the packet capture of tracert