

## Assignment 10

### Part-1

1. IP address of host: **10.240.203.43**

The IP address of the destination host is: **10.195.250.62**

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
→ 30	3.396610	10.240.203.43	10.195.250.62	ICMP	74	Echo (ping) request

2. The ICMP packet does not contain source or destination port numbers because it was created to send network-layer information between hosts and routers rather than between application-layer processes.

There is a "Type" and a "Code" in every ICMP packet. The particular message being received is identified by the Type/Code combination.

No port numbers are required to direct an ICMP message to an application layer process because the network program understands all ICMP messages.

3. For Echo (ping) request

ICMP Type: **8**

Code: **0**

Other fields present in the ICMP packet are:

- Checksum
- Identifier (BE)
- Identifier (LE)
- Sequence Number (BE)
- Sequence Number (LE)
- Timestamp from ICMP data

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
→ 30	3.396610	10.240.203.43	10.195.250.62	ICMP	74	Echo (ping) request
← 31	3.402941	10.195.250.62	10.240.203.43	ICMP	74	Echo (ping) reply

  

> Frame 30: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device	0000	f8 7a 41
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a	0010	00 3c df
> Internet Protocol Version 4, Src: 10.240.203.43, Dst: 10.195.250.62	0020	fa 3e 08
> Internet Control Message Protocol	0030	67 68 69
Type: 8 (Echo (ping) request)	0040	77 61 62
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: 31]		
> Data (32 bytes)		

The size of the checksum, sequence number, and identifier fields is **2 bytes** each.

4. For Echo (ping) reply

ICMP Type: **0**

Code: **0**

Other fields present in the ICMP packet are:

- Checksum
- Identifier (BE)
- Identifier (LE)
- Sequence Number (BE)
- Sequence Number (LE)
- Timestamp from ICMP data

The size of the checksum, sequence number, and identifier fields is **2 bytes** each.

31	3.402941	10.195.250.62	10.240.203.43	ICMP	74	Echo (ping) reply
>	Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...}					0000 14 13
>	Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: AzureWaveTec_c7:3e:39 (14:13:2a:c7:3e:39)					0010 00 3c
>	Internet Protocol Version 4, Src: 10.195.250.62, Dst: 10.240.203.43					0020 cb 2b
>	Internet Control Message Protocol					0030 67 68
>	Type: 0 (Echo (ping) reply)					0040 77 61
>	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: 30]					
>	[Response time: 6.331 ms]					
>	Data (32 bytes)					

## Part-2

1. Source IP address: **10.240.203.43**

Destination IP address: **142.250.192.68**

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
685	8.238335	10.240.203.43	142.250.192.68	ICMP	74	Echo (ping) request

2. It would be different if ICMP sent UDP packets. Instead of 01, it would be switched to **0 X 11 (= 17)**.

3. The ICMP echo packet has the **same fields** as the ping query packets.

685	8.238335	10.240.203.43	142.250.192.68	ICMP	74 Echo (ping) request
686	8.238347	10.240.203.43	142.250.192.68	ICMP	74 Echo (ping) request

  

> Frame 685: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device	0000	f8 7a 4
> Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a	0010	00 3c e
> Internet Protocol Version 4, Src: 10.240.203.43, Dst: 142.250.192.68	0020	c0 44 0
✓ Internet Control Message Protocol	0030	4e 4f 5
Type: 8 (Echo (ping) request)	0040	5e 5f 6
Code: 0		
Checksum: 0x7e6a [correct]		
[Checksum Status: Good]		
Identifier (BE): 1000 (0x03e8)		
Identifier (LE): 59395 (0xe803)		
Sequence Number (BE): 40 (0x0028)		
Sequence Number (LE): 10240 (0x2800)		
[Response frame: 695]		
> Data (32 bytes)		

4. The ICMP error packet is different from the ping query packets. It contains the **IP header** and the **first 8 bytes of the original ICMP packet** for which the error is.

57	2.065990	10.240.200.1	10.240.203.43	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
----	----------	--------------	---------------	------	---

  

> Frame 57: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device	0000	14 13 33 c7 3e 39 1c d1 e0 75 28 6e 08 00 45 c6
> Ethernet II, Src: Cisco_75:28:6e (1c:d1:e0:75:28:6e), Dst: AzureWaveTec_c7:3e:39 (14:13	0010	00 38 0f 4c 00 00 fe 01 03 ac 0a f0 c8 01 0a ff
> Internet Protocol Version 4, Src: 10.240.200.1, Dst: 10.240.203.43	0020	cb 2b 0b 00 6a 85 00 00 00 00 45 00 00 3c ef 9f
✓ Internet Control Message Protocol	0030	00 00 01 01 a4 c7 0a f0 cb 2b 8e fa c0 44 08 00
Type: 11 (Time-to-live exceeded)	0040	7e 8d 03 e8 00 05
Code: 0 (Time to live exceeded in transit)		
Checksum: 0x6a85 [correct]		
[Checksum Status: Good]		
Unused: 00000000		
> Internet Protocol Version 4, Src: 10.240.203.43, Dst: 142.250.192.68		

5. The last three ICMP packets received by the source host are messages of **Type 0 (echo reply)**, not **Type 11 (TTL expired)**. They differ because the datagrams reached the target host before the TTL expired.

6. The connection between points 3 and 4 or 9 and 10 has a much greater latency

```

paru04@LAPTOP-NVGR5VB8:~$ traceroute -I www.google.com
traceroute to www.google.com (142.250.192.68), 30 hops max, 60 byte packets
 1  LAPTOP-NVGR5VB8.mshome.net (172.23.208.1)  0.465 ms  0.449 ms  0.448 ms
 2  10.240.200.1 (10.240.200.1)  2.044 ms  2.565 ms  2.564 ms
 3  10.240.240.1 (10.240.240.1)  2.781 ms  2.781 ms  2.780 ms
 4  117.205.73.161 (117.205.73.161)  28.601 ms  28.600 ms  28.599 ms
 5  * * *
 6  * * *
 7  142.250.160.26 (142.250.160.26)  18.553 ms  24.637 ms  19.690 ms
 8  142.251.227.217 (142.251.227.217)  20.545 ms  20.541 ms  20.539 ms
 9  142.251.229.250 (142.251.229.250)  20.536 ms  20.534 ms  20.532 ms
10  64.233.174.3 (64.233.174.3)  23.752 ms  23.749 ms  23.747 ms
11  142.251.49.232 (142.251.49.232)  52.257 ms  52.255 ms  52.253 ms
12  192.178.110.207 (192.178.110.207)  52.096 ms  52.094 ms  52.071 ms
13  108.170.226.131 (108.170.226.131)  51.047 ms * *
14  bom12s16-in-f4.1e100.net (142.250.192.68)  57.473 ms  57.471 ms  57.469 ms

```