

CS-315 COMPUTER NETWORKS LAB-10 (ICMP)

Part-1

No.	Time	Source	Destination	Protocol	Length	Info
78	3.754211	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 80)
80	3.757916	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=62 (request in 78)
107	4.770877	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 108)
108	4.777686	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=62 (request in 107)
136	5.783747	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 137)
137	5.785531	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=62 (request in 136)
143	6.808201	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 144)

> Frame 78: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D330...}	0000	b0 8b d0 60 ff ff 20 c1 9b 1f 79 8a 08 00 45 00	...
> Ethernet II, Src: Intel_1f:79:8a (20:c1:9b:1f:79:8a), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)	0010	00 3c 5f 42 00 00 80 01 00 00 0a c8 5d f7 0a c3	<_B.....]
> Internet Protocol Version 4, Src: 10.200.93.247, Dst: 10.195.250.62	0020	fa 3e 08 00 4d 57 00 01 00 04 61 62 63 64 65 66	>...MW...abcdef
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi
Code: 0			
Checksum: 0x4d57 [correct]			
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 4 (0x0004)			
Sequence Number (LE): 1024 (0x0400)			
[Response frame: 80]			
> Data (32 bytes)			

1. The IP address of my host = 10.200.93.247
The IP address of the destination host = 10.195.250.62
2. ICMP is a network layer protocol so it requires only source and destination IP address and does not require source and destination port numbers, which are required only for transport layer protocols.
3. From the screenshot above, the ICMP Type is 8 (Echo (ping) request) and the code is 0. The other fields that this ICMP packet has are Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE) and Sequence Number (LE). As we can see, the checksum, sequence number and identifier field values have 4 hexadecimal digits, which is 16 bits or 2 bytes. Hence, the checksum, sequence number and identifier fields are of 2 bytes in size each.
4. From the screenshot below, for the ping reply packet, the ICMP Type is 0 (Echo (ping) reply) and the code is 0. The other fields that this ICMP packet has are Checksum, Identifier (BE), Identifier

(LE), Sequence Number (BE) and Sequence Number (LE). As we can see, the checksum, sequence number and identifier field values have 4 hexadecimal digits, which is 16 bits or 2 bytes. Hence, the checksum, sequence number and identifier fields are of 2 bytes in size each.

No.	Time	Source	Destination	Protocol	Length	Info
78	3.754211	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 80)
80	3.757916	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=62 (request in 78)
107	4.770877	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 108)
108	4.777686	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=62 (request in 107)
136	5.783747	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 137)
137	5.785531	10.195.250.62	10.200.93.247	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=62 (request in 136)
143	6.808201	10.200.93.247	10.195.250.62	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 144)

> Frame 80: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{D330}	0000	20 c1 9b 1f 79 8a f8 7a 41 13 2a c2 08 00 45 00	...y...z A*...E
> Ethernet II, Src: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2), Dst: Intel_1f:79:8a (20:c1:9b:1f:79:8a)	0010	00 3c c9 e4 00 00 3e 01 45 1c 0a c3 fa 3e 0a c8	-<...> E...>..
> Internet Protocol Version 4, Src: 10.195.250.62, Dst: 10.200.93.247	0020	5d f7 00 00 55 57 00 01 00 04 61 62 63 64 65 66]...UW...abcdef
> Internet Control Message Protocol	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 0 (Echo (ping) reply)	0040	77 61 62 63 64 65 66 67 68 69	wabdefg hi
Code: 0			
Checksum: 0x5557 [correct]			
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 4 (0x0004)			
Sequence Number (LE): 1024 (0x0400)			
[Request frame: 78]			
[Response time: 3.705 ms]			
> Data (32 bytes)			

Part-2

Windows, by default, uses ICMP for traceroute command.

No.	Time	Source	Destination	Protocol	Length	Info
467	35.369802	216.239.43.137	10.200.93.247	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
473	36.365082	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=9 (no response found!)
474	36.387499	142.251.55.121	10.200.93.247	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
475	36.390808	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=39/9984, ttl=9 (no response found!)
476	36.411125	142.251.55.121	10.200.93.247	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
477	36.412549	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=40/10240, ttl=9 (no response found!)
478	36.433190	142.251.55.121	10.200.93.247	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
487	37.421996	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=41/10496, ttl=10 (reply in 488)
488	37.444637	142.250.196.68	10.200.93.247	ICMP	106	Echo (ping) reply id=0x0001, seq=41/10496, ttl=58 (request in 487)
489	37.446236	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=42/10752, ttl=10 (reply in 490)
490	37.468239	142.250.196.68	10.200.93.247	ICMP	106	Echo (ping) reply id=0x0001, seq=42/10752, ttl=58 (request in 489)
491	37.469879	10.200.93.247	142.250.196.68	ICMP	106	Echo (ping) request id=0x0001, seq=43/11008, ttl=10 (reply in 492)
492	37.491241	142.250.196.68	10.200.93.247	ICMP	106	Echo (ping) reply id=0x0001, seq=43/11008, ttl=58 (request in 491)

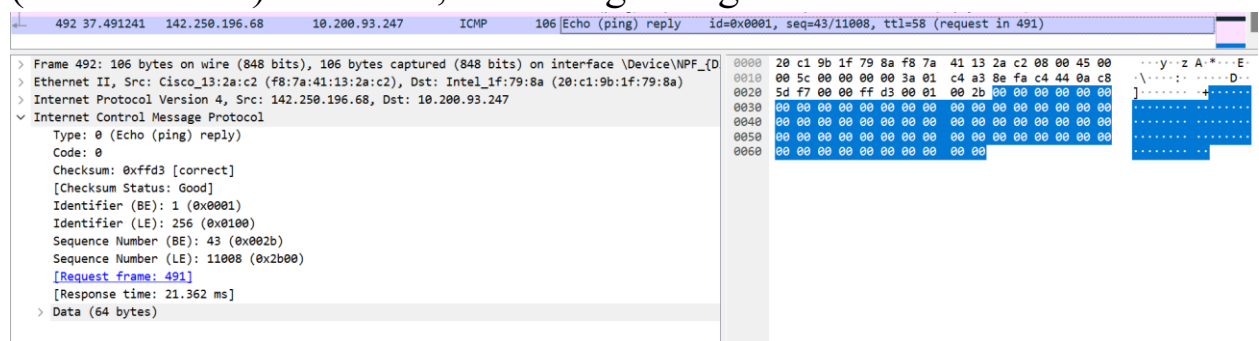
> Frame 487: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{D	0000	b0 8b d0 60 ff ff 20 c1 9b 1f 79 8a 08 00 45 00	...y...E
> Ethernet II, Src: Intel_1f:79:8a (20:c1:9b:1f:79:8a), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)	0010	00 5c 21 c4 00 00 0a 01 00 00 0a c8 5d f7 8e fa	.\ ...}]..
> Internet Protocol Version 4, Src: 10.200.93.247, Dst: 142.250.196.68	0020	c4 44 08 00 f7 d5 00 01 00 29 00 00 00 00 00 00	.D.....)
> Internet Control Message Protocol	0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Type: 8 (Echo (ping) request)	0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Code: 0	0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Checksum: 0xf7d5 [correct]	0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 41 (0x0029)			
Sequence Number (LE): 10496 (0x2900)			
[Response frame: 488]			
> Data (64 bytes)			

1. The IP address of my host = 10.200.93.247
The IP address of the destination host = 142.250.196.68
2. No, the protocol number would be 17 which is the assigned protocol number for UDP. The protocol number would be 1 in the case of ICMP packets.
3. No, the above screenshot shows that this packet is similar to the ICMP ping query packets in the first part as both have the same fields. The type and code fields in both also have the same values (8 and 0 respectively).
4. Yes, it has more fields. The extra fields are 'Unused', the IP layer of the echo request and the ICMP layer of the echo request which includes the fields: type, code, checksum, identifier and sequence number just as any other ICMP packet. Also, the type is changed to 11 (Time-to-live exceeded).

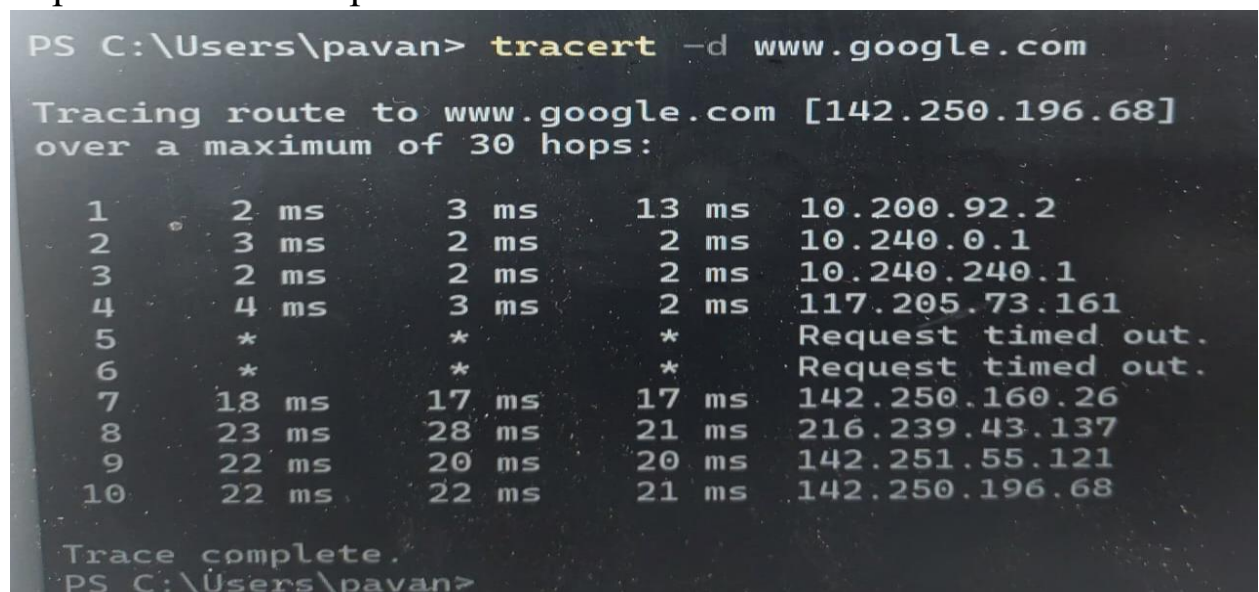
```
> Internet Protocol Version 4, Src: 142.251.55.121, Dst: 10.200.93.247
- Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xf4ff [correct]
  [Checksum Status: Good]
  Unused: 00000000
> Internet Protocol Version 4, Src: 10.200.93.247, Dst: 142.250.196.68
- Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf7d6 [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 40 (0x0028)
  Sequence Number (LE): 10240 (0x2800)
> Data (64 bytes)
```

5. These packets are different from the ICMP error packets as we can see the Type is 0 (Echo (ping) request) unlike 11 (Time-to-live exceeded) in the error packets. Also, unlike the error packets, they do not have an IP layer and an ICMP layer for the echo reply. They do not have the extra 'Unused' field like the error packets. These packets are different from the ICMP error packets in the sense that

they are responses from the destination host (www.google.com) indicating that the packet has reached the destination. These packets are different from ICMP error packets because they are ICMP Echo Reply packets confirming that the destination host has received the ICMP Echo Request. In contrast, ICMP error packets are packets sent by intermediate routers along the path when they encounter issues forwarding packets to the destination. These packets indicate problems such as unreachable destination, TTL (Time-to-Live) exceeded, or routing changes.



6. Yes, as we can see from the screenshot below, the delay of the link around 4-5-6-7(from hop 4 to hop 7) is significantly longer than others. The delay is noticeably higher compared to the previous ones, indicating a potential bottleneck or increased latency in that particular segment of the network. Delay increased from 2ms in hop 4 to 17ms in hop 7.



Part-3

```
PS C:\AlphaParadise\1.CSE\SEM6\COMPUTER NETWORKS\CS-315_Computer_Networks_Lab\lab10> python .\210010050_client.py
```

```
-----  
PING SEQ NO: 1  
Response from server: PING 1 WED MAR 20 21:01:42 2024  
RTT: 0.003004312515258789 seconds  
-----
```

```
PING SEQ NO: 2  
Response from server: PING 2 WED MAR 20 21:01:42 2024  
RTT: 0.0 seconds  
-----
```

```
PING SEQ NO: 3  
Response from server: PING 3 WED MAR 20 21:01:42 2024  
RTT: 0.0010037422180175781 seconds  
-----
```

```
PING SEQ NO: 4  
Response from server: PING 4 WED MAR 20 21:01:42 2024  
RTT: 0.0009989738464355469 seconds  
-----
```

```
PING SEQ NO: 5  
Request timed out  
-----
```

```
PING SEQ NO: 6  
Request timed out  
-----
```

```
-----  
PING SEQ NO: 6  
Request timed out  
-----
```

```
PING SEQ NO: 7  
Request timed out  
-----
```

```
PING SEQ NO: 8  
Response from server: PING 8 WED MAR 20 21:01:45 2024  
RTT: 0.0010001659393310547 seconds  
-----
```

```
PING SEQ NO: 9  
Response from server: PING 9 WED MAR 20 21:01:45 2024  
RTT: 0.001001596450805664 seconds  
-----
```

```
PING SEQ NO: 10  
Response from server: PING 10 WED MAR 20 21:01:45 2024  
RTT: 0.001008749008178711 seconds  
-----
```

```
Ping Statistics  
-----
```

```
Packet loss rate: 30.0%  
Average RTT: 0.0011453628540039062 seconds
```