Computer Networks Lab, Assignment 10

Suyash Gaurav

210010054

---

1 Part-1: ICMP and Ping

---

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

Src: 10.200.246.244, Dst: 10.195.250.62

```
> Frame 234: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\N
> Ethernet II, Src: Intel_24:d7:b3 (b4:0e:de:24:d7:b3), Dst: Cisco_0a:9a:f3 (44:b6:be:0a:9a:f
> Internet Protocol Version 4, Src: 10.200.246.244, Dst: 10.195.250.62
> Internet Control Message Protocol
```

Figure 1: Q1. Source, Destination

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

ICMP packets don't have source/destination ports because they're for network-layer communication, not between application-layer processes. They're identified by Type/Code combination, not ports, and are understood directly by network programs.

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?

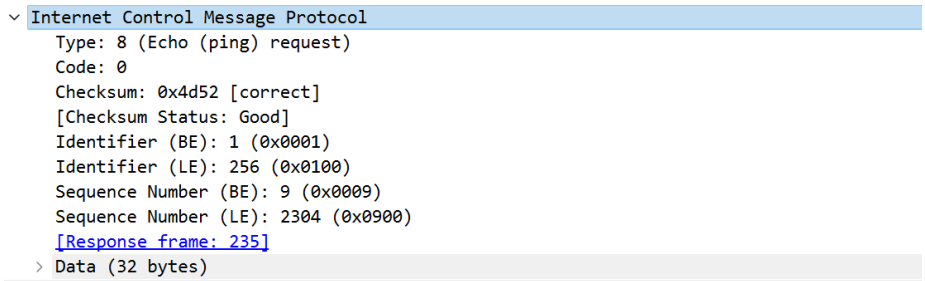

Figure 2: Q2, 3. ICMP

ICMP type: 8 (Echo (ping) request)
Code: 0
Other fields present are:

- Checksum
- Identifier (BE)
- Identifier (LE)
- Sequence Number (BE)
- Sequence Number (LE)

The size of the checksum, sequence number, and identifier fields is same i.e. **2 Bytes**.

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?

ICMP type: 0 (Echo (ping) reply) Code: 0 Other fields present are:

- Checksum
- Identifier (BE)

- Identifier (LE)
- Sequence Number (BE)
- Sequence Number (LE)

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

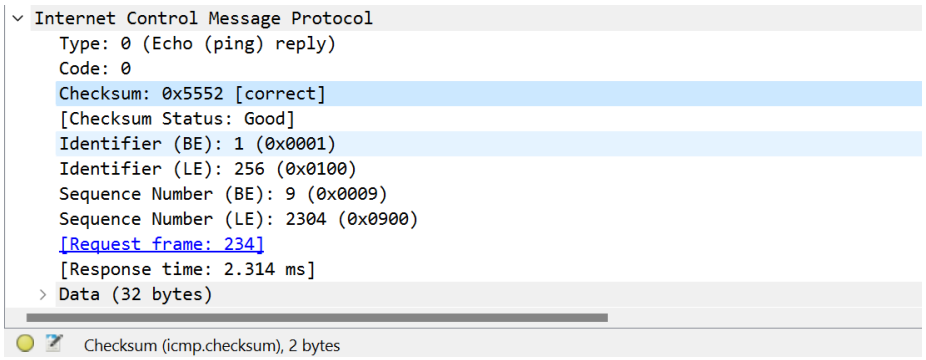

Figure 3: Q4. ICMP reply

---

2 Part-2: ICMP and Traceroute

---

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

My IP: 10.200.246.244,
target destination host IP: 142.250.183.4

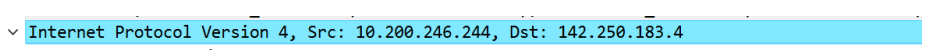

Figure 4: Q1. Source, Destination

2. If traceroute sent UDP packets, would the

IP protocol number still be 01 for the probe packets? If not, what would it be?

If ICMP sent UDP packets instead, the IP protocol number would change from 01 to 0x11. This switch reflects the different transport protocol being used (UDP instead of ICMP), which requires a different protocol number in the IP header to identify it correctly.

3. 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 ICMP echo packet is same as the ICMP ping query packets. They have the same fields and serve the same purpose.

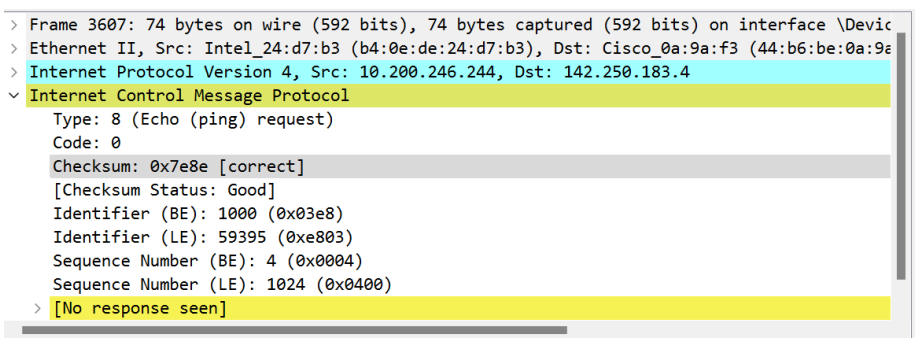

Figure 5: Q1. ICMP Packet

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

The ICMP error packet includes additional fields compared to the ICMP echo packet. Specifically, it contains the IP header and the first 8 bytes of the original ICMP

packet that caused the error. This additional information helps in diagnosing and addressing the specific issue that triggered the error.

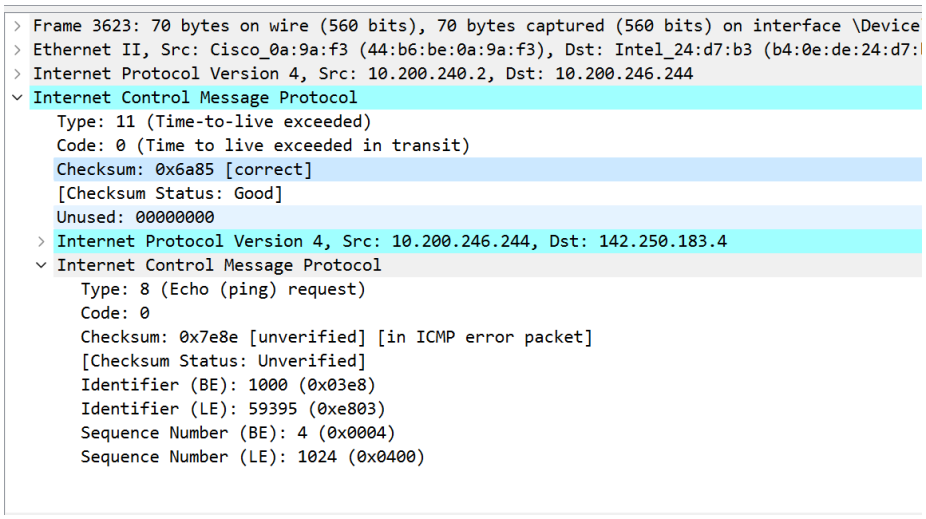

Figure 6: Q4. ICMP error

5. 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 ICMP packets received by the source host are ICMP echo reply packets (message type 0), not ICMP error packets (message type 11, TTL expired). This difference arises because these packets successfully reached the target host before the Time-to-Live (TTL) expired, thus triggering an echo reply instead of an error due to TTL expiration.

6. Within the traceroute measurements, is there a link whose delay is significantly longer than others?

The connection link between 1 and 2, 2 and 3, 4 and 5 has delay significantly longer than others.

```
suyas@Z-Sparrow:/mnt/c/Users/suyas$ sudo traceroute -I www.google.com
[sudo] password for suyas:
traceroute to www.google.com (142.250.183.4), 30 hops max, 60 byte packets
 1  Z-Sparrow.mshome.net (172.20.176.1)  0.506 ms  0.488 ms  0.487 ms
 2  10.200.240.2 (10.200.240.2)  5.821 ms  5.819 ms  5.849 ms
 3  10.240.0.1 (10.240.0.1)  53.269 ms  53.530 ms  53.528 ms
 4  10.240.240.1 (10.240.240.1)  6.127 ms  6.644 ms  6.642 ms
 5  103.120.31.121.static-chennai.powertel.in (103.120.31.121)  15.339 ms  15.000 ms  15.712 ms
 6  103.120.29.73.static-delhi.powertel.in (103.120.29.73)  18.908 ms  17.681 ms  17.674 ms
 7  103.120.29.72.static-delhi.powertel.in (103.120.29.72)  16.660 ms  16.794 ms  17.032 ms
 8  72.14.209.113 (72.14.209.113)  19.292 ms  19.298 ms  19.339 ms
 9  142.251.54.79 (142.251.54.79)  19.266 ms  19.265 ms  19.263 ms
10  142.250.239.228 (142.250.239.228)  19.983 ms  19.490 ms  19.980 ms
11  172.253.72.137 (172.253.72.137)  19.978 ms  19.976 ms  19.975 ms
12  142.250.212.0 (142.250.212.0)  38.534 ms  38.401 ms  31.167 ms
13  142.250.226.67 (142.250.226.67)  32.086 ms  32.977 ms  33.177 ms
14  142.250.214.109 (142.250.214.109)  31.986 ms  33.379 ms  33.375 ms
15  bom07s30-in-f4.1e100.net (142.250.183.4)  36.433 ms  35.973 ms  36.430 ms
```

Figure 7: Q4. Traceroute latency