CENG435 – Homework 4

Utku Güngör – 2237477

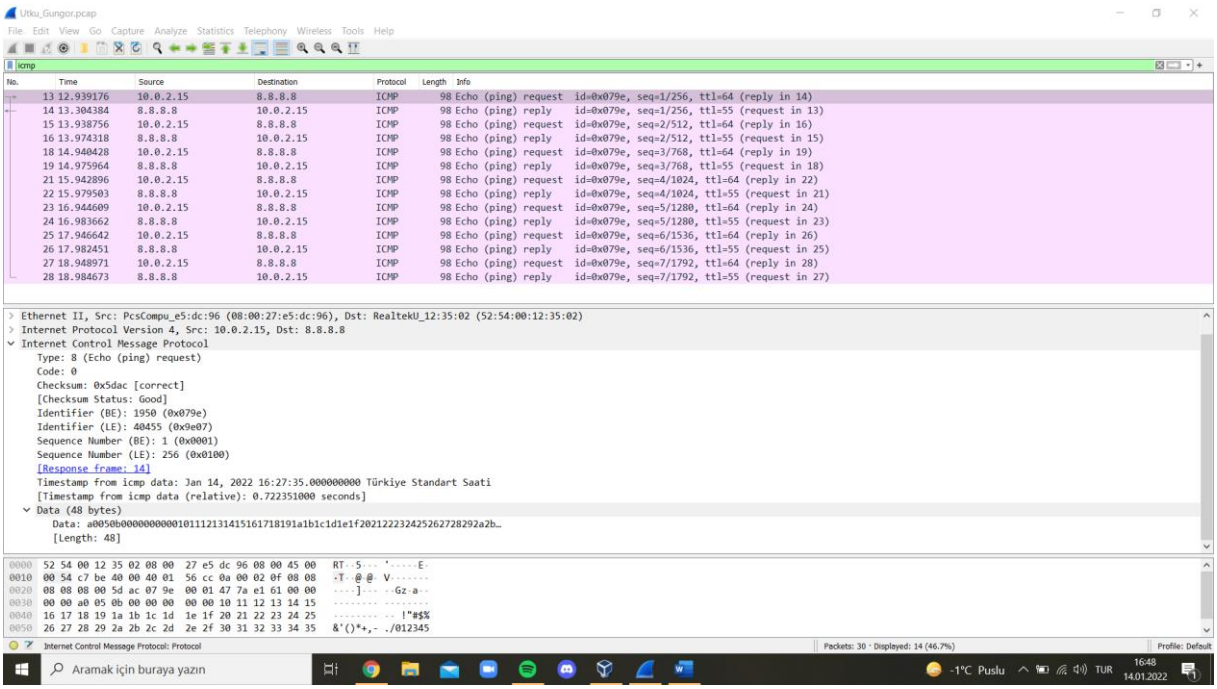

Figure 1: ICMP Request Packet Details

Figure 2: ICMP Reply Packet Details

```
mininet@the3:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    20100  0        0 enp0s3
0.0.0.0         10.0.3.2        0.0.0.0         UG    20101  0        0 enp0s8
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
10.0.3.0        0.0.0.0         255.255.255.0   U     101    0        0 enp0s8
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s8
```

Figure 3: Routing Table

1) For the request packets:
   Source IP: 10.0.2.15
   Destination IP: 8.8.8.8

   For the reply packets:
   Source IP: 8.8.8.8
   Destination IP: 10.0.2.15

2) Because the purpose of the ICMP packet is to establish a communication of network-layer information between hosts and routers, hence application layer is not included in this protocol [1]. Port numbers are a feature of transport layer protocols such as TCP and UDP, and ICMP is a part of internetworking layer(IP). So, there is no port number in ICMP.

3) **a)** "Type" byte specifies the type of the ICMP message. As you can see in part (c), type 8 is used for requests whereas type 0 is for reply messages. There are some other types that contain more specific information about the error condition.
   b) "Code" field reports more detail about the message(errors, explanations, etc.), and changes meaning according to the 'Type' field of the ICMP protocol so that we can have a more clear understanding of the request or the reply message. Therefore this field identifies the kind of ICMP package with the given type. There are many codes to describe different situations.
   c) In ICMP Request packet,'Type' field is '8' and 'Code' field is '0'. This value pair shows that this is a 'Echo (Ping) request' message.
   In the ICMP Reply packet, 'Type' field is '0' and 'Code' field is '0'. This value pair shows that this is a 'Echo (ping) reply' message.

4) **For Ethernet:** 6 bytes for source + 6 bytes for destination + 2 bytes for the type = total 14 bytes
   For Internet Protocol: 20 bytes for the header = total 20 bytes
   For ICMP: 1 byte for the type field + 1 byte for the code field + 2 bytes for the checksum field + 2 bytes for identifier + 2 bytes for sequence number + 8 bytes for timestamp + 48 bytes for the data = total 64 bytes

   14 + 20 + 64 = **98 bytes** are transferred in total.

5) Since we need to remove a rule, we need to choose a rule that allows the transition of outgoing packets.
   According to the first rule, packets coming from the source IP address with ICMP protocol and type with echo-request are accepted. If we remove this rule which has 0.0.0.0 as the destination field and enp0s3 as the Iface field, since packets cannot be directed to the Gateway 10.0.2.2, outgoing packets will be dropped and ping requests cannot be sent. From question 1, our destination IP is 8.8.8.8 for ping requests, so it matches with the '0.0.0.0/0' as the longest prefix (the first row in the table with Destination '0.0.0.0' and Genmask '0.0.0.0'). And if we remove the first rule, packets will not be able to be sent via this rule and they will be dropped.

REFERENCES

- (2021, February 16). *Exploring ICMP Port Number with Example*. Howtouselinux. https://www.howtouselinux.com/post/icmp-port-number