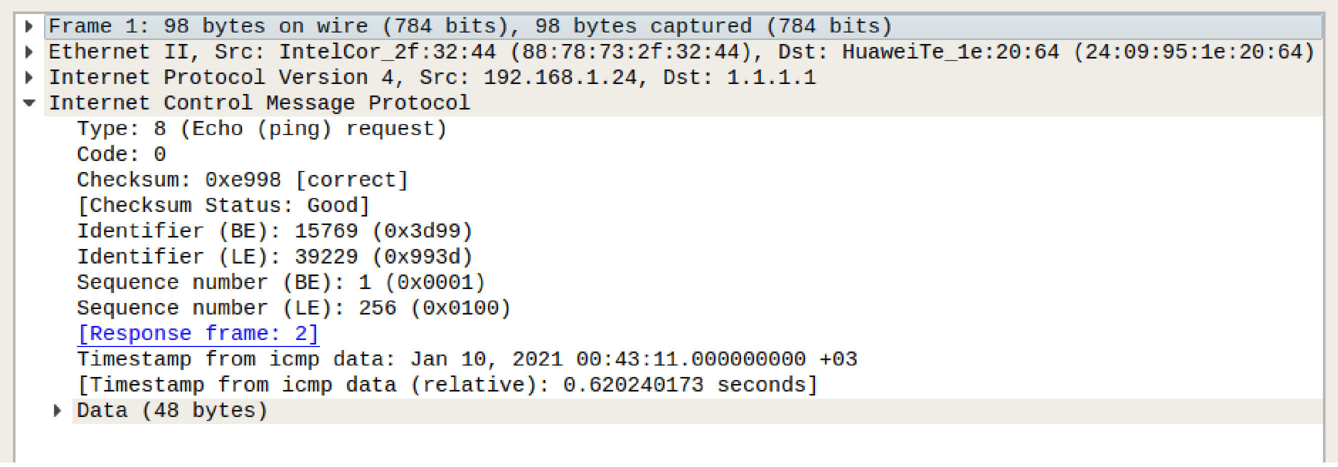
Student Information

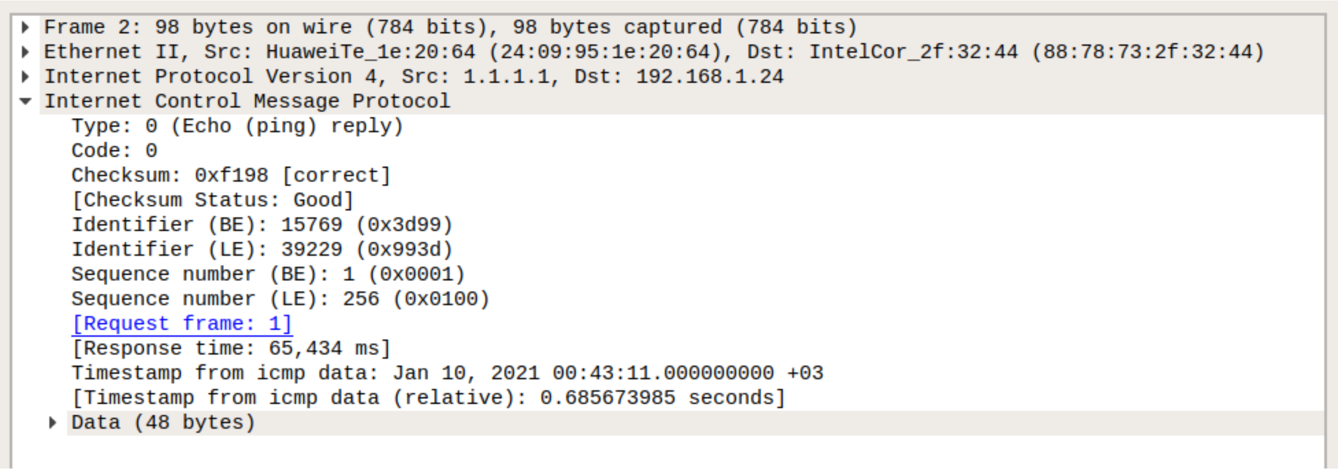
Full Name: Doruk Gerçel
Id Number: 2310027

Screenshots



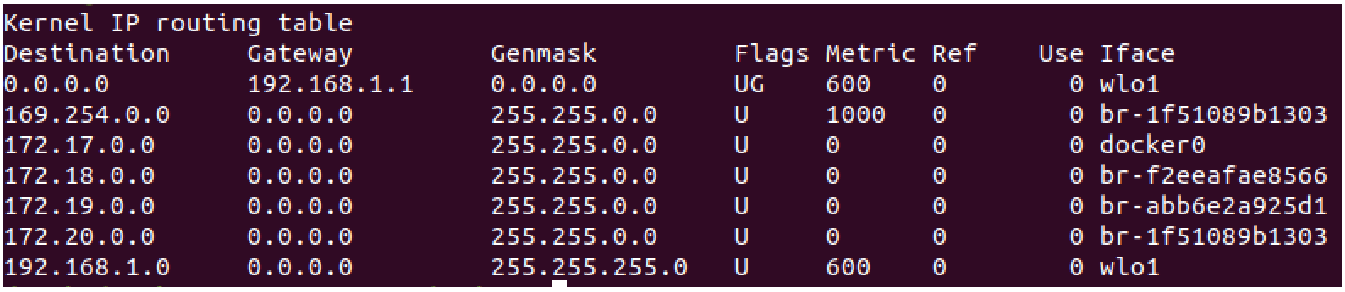
```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: IntelCor_2f:32:44 (88:78:73:2f:32:44), Dst: HuaweiTe_1e:20:64 (24:09:95:1e:20:64)
▸ Internet Protocol Version 4, Src: 192.168.1.24, Dst: 1.1.1.1
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe998 [correct]
    [Checksum Status: Good]
    Identifier (BE): 15769 (0x3d99)
    Identifier (LE): 39229 (0x993d)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 2]
    Timestamp from icmp data: Jan 10, 2021 00:43:11.000000000 +03
    [Timestamp from icmp data (relative): 0.620240173 seconds]
  ▸ Data (48 bytes)
```

Figure 1: ICMP Request Screenshot



```
▸ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: HuaweiTe_1e:20:64 (24:09:95:1e:20:64), Dst: IntelCor_2f:32:44 (88:78:73:2f:32:44)
▸ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.1.24
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xf198 [correct]
    [Checksum Status: Good]
    Identifier (BE): 15769 (0x3d99)
    Identifier (LE): 39229 (0x993d)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 65,434 ms]
    Timestamp from icmp data: Jan 10, 2021 00:43:11.000000000 +03
    [Timestamp from icmp data (relative): 0.685673985 seconds]
  ▸ Data (48 bytes)
```

Figure 2: ICMP Reply Screenshot



```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlo1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 br-1f51089b1303
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-f2eeafae8566
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-abb6e2a925d1
172.20.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-1f51089b1303
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
```

Figure 3: Routing Table Screenshot

Answers

1. (10 Points)

In the ICMP Request packet, the IP address of the source host is '192.168.1.24' (IP address of my computer) and the IP address of the destination host is '1.1.1.1' (IP address of the Cloudfare's DNS service server). In the ICMP Reply packet, the IP address of the source host is '1.1.1.1' and the IP address of the destination host is '192.168.1.24'. This change of the source and destination IP addresses between the request and reply packets, makes sense as the reply packet is a response to the request packet, therefore the source and destination IP addresses swap places.

2. (20 Points)

Port numbers are included in the Transport Layer protocol headers. As we know, Network Layer is under the Transport Layer in the Internet Protocols stack, therefore a Network Layer protocol won't include port numbers. As ICMP is also a Network Layer protocol, it doesn't contain any source or destination port numbers. (Although ICMP is carried by the IP datagrams, it is still a part of Network Layer.) Also ICMP's primary usage is to control the Network Layer functions between the hops (hosts and routers), therefore it is sufficient for ICMP to exchange Network Layer datagrams (there is no need for these packets to reach upper layers of Internet Protocols stack, therefore there is no need for them to include any port numbers).

3a. (15 Points)

'Type' field of the ICMP message is used in-order to indicate the type of the ICMP packet, according to the number this field contains. 'Code' field can actually be considered as a 'subtype' field as-well, because this field gives additional information about the type of the ICMP, and changes meaning according to the 'Type' field of the ICMP protocol. Therefore this field identifies the kind of the ICMP package with the given type. Also as this field changes meaning according to the value of the 'Type' field, number of variations of 'Code's for each 'Type' of ICMP is different. Therefore 'Type' and 'Code' fields together identifies the ICMP package.

3b. (15 Points)

In ICMP Request packet, value of the 'Type' field is '8' and value of the 'Code' field is '0'. This value pair indicates that this is a 'Echo (Ping) request' message (makes sense as this message is sent from my computer as a ping request). In the ICMP Reply packet, value of the 'Type' field is '0' and value of the 'Code' field is '0'. This value pair indicates that this is a 'Echo (ping) reply' message (makes sense as this message is sent from the server as a ping response to my ping request).

4. (20 Points)

In ICMP request packet 98 bytes are transferred in total.

14 bytes are used for protocol 'Ethernet 2's header +
20 bytes are used for protocol 'IPv4's header +
1 byte is used for the 'Type' field of ICMP packet +
1 byte is used for the 'Code' field of ICMP packet +
2 bytes are used for the 'Checksum' field of ICMP packet +
2 bytes are used for the 'Identifier' field of ICMP packet +
2 bytes are used for the 'Sequence Number' field of ICMP packet +

8 bytes are used for the 'Timestamp from ICMP data' field of ICMP packet +
48 bytes are used for data (payload) =
98 total bytes

Ethernet 2 is a Link Layer protocol, and its header carries the relevant link layer information for the packet. IPv4 is a Network Layer protocol, and its header carries the relevant network layer information for the packet. 'Type' field and 'Code' field together in the ICMP header are used to identify the type and kind of the ICMP packet (Type:8 and Code:0 in my request packet). 'Checksum' field is necessary for the data integrity and checking the corruption of the packet (Checksum:0xe998 in my request packet). 'Identifier' and 'Sequence Number' fields are used to match both request and reply messages with each other (Identifier:15769 and Sequence Number:1 in my request packet). 'Timestamp' includes data about time and date information, and is necessary for synchronization (Timestamp: Jan 10, 2021 00:43:11.0000 in my request packet).

5. (20 Points)

From the first question we know that destination address of the packets that we send (ICMP Request packet) is '1.1.1.1' (Figure 1). When we look at the Routing Table (Figure 3) we can see that these packets are directed to my home modem (can be observed as Gateway's address is '192.168.1.1', and this is the IP address of my home modem). I observed that as the destination address '1.1.1.1' match 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'), therefore it is directed to the Gateway '192.168.1.1' (actually it is the default gateway). Therefore if I remove this first rule from my Routing Table, I won't be able to send any ping request. Also as this first rule represents the default gateway for all the outgoing packets (as '0.0.0.0/0' achieves the longest prefix match with every packet that doesn't match with other routing addresses), all the outgoing packet will be dropped when the first rule is removed.