## CENG 435 - Data Communications and Networking Fall 2022-2023 ${\rm THE-4}$

Sezgin, Mustafa e2380863@ceng.metu.edu.tr

January 2, 2023

## **ICMP**

1. For the ICMP request package shown in Figure 1, the source host IP address is 172.26.128.47, and the destination host IP address is 1.1.1.1. For the ICMP reply package shown in Figure 2, the source host IP address is 1.1.1.1, and the destination host IP address is 172.26.128.47.

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
  Ethernet II, Src: Microsof_6e:76:42 (00:15:5d:6e:76:42), Dst: Microsof_7a:11:ef (00:15:5d:7a:11:ef)
  Internet Protocol Version 4, Src: 172.26.128.47, Dst: 1.1.1.1

    Internet Control Message Protocol

    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa2ae [correct]
     [Checksum Status: Good]
    Identifier (BE): 115 (0x0073)
    Identifier (LE): 29440 (0x7300)
     Sequence Number (BE): 1 (0x0001)
     Sequence Number (LE): 256 (0x0100)
     [Response frame: 2]
     Timestamp from icmp data: Jan 2, 2023 15:08:50.000000000 Turkey Standard Time
     [Timestamp from icmp data (relative): 0.220974000 seconds]
       Data: 8cdd040000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
       [Length: 48]
 0010 00 54 a8 5e 40 00 40 01 63 ff ac 1a 80 2f 01 01 0020 01 01 08 00 a2 ae 00 73 00 01 52 c9 b2 63 00 00
                                                                 ·T·^@·@· c···/··
                                                                 · · · · · · · s · · R · · c · ·
       00 00 8c dd 04 00 00 00 00 00 10 11 12 13 14 15
 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                                 &'()*+,- ./012345
Show packet bytes
                                                                                                 Close Help
```

Figure 1: ICMP request packet details

2. ICMP packets do not contain any port number. This is because ICMP is a host-to-host protocol that does not communicate with processes and, therefore, does not need any port number. It is a part of the network layer.

```
Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 Ethernet II, Src: Microsof_7a:11:ef (00:15:5d:7a:11:ef), Dst: Microsof_6e:76:42 (00:15:5d:6e:76:42)
 Internet Protocol Version 4, Src: 1.1.1.1, Dst: 172.26.128.47
v Internet Control Message Protocol
   Type: 0 (Echo (ping) reply)
   Code: 0
   Checksum: Oxaaae [correct]
   [Checksum Status: Good]
   Identifier (BE): 115 (0x0073)
   Identifier (LE): 29440 (0x7300)
   Sequence Number (BE): 1 (0x0001)
   Sequence Number (LE): 256 (0x0100)
   [Request frame: 1]
   [Response time: 10.194 ms]
   Timestamp from icmp data: Jan 2, 2023 15:08:50.000000000 Turkey Standard Time
   [Timestamp from icmp data (relative): 0.231168000 seconds]
  V Data (48 bytes)
     Data: 8cdd04000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b...
     [Length: 48]
      00 15 5d 6e 76 42 00 15
                               5d 7a 11 ef 08 00 45 00
                                                           ·]nvB··
                                                                  ]z - - - E
      00 54 97 a2 00 00 36 01 be bb 01 01 01 01 ac 1a
9929
     80 2f 00 00 aa ae 00 73
                               00 01 52 c9 b2 63 00 00
                                                         ·/····s ··R···c··
     00 00 8c dd 04 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050
     26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
                                                         &'()*+,- ./012345
                                                                                      Close Help
```

Figure 2: ICMP reply packet details

- 3. (a) The type field is used to identify the type of the packet, which can be "echo reply", "echo request", "destination unreachable", "TTL expired", "bad IP header", etc.
  - (b) The code field is used to provide additional information regarding the type of the packet. It is not always used. For example, if the type is "destination unreachable", the code can mean "network unreachable", "host unreachable", "protocol unreachable", "network unknown", etc.
  - (c) The type of the ICMP request packet shown in Figure 1 has the value 8, which means it is an "Echo (ping) request" packet. The type of the ICMP reply packet shown in Figure 2 has the value 0, which means it is an "Echo (ping) reply" packet. The code fields of both packets have the value of 0 and they do not have any meaning when the type is 0 or 8.
- 4. As seen in Figure 1, ICMP request has a payload data of size 48 bytes, and the total size of the frame is 98 bytes, including all the headers. The size of each field in the header of an ICMP packet is as follows.

type: 1 bytecode: 1 byte

checksum: 2 bytesidentifier: 2 bytes

• sequence number: 2 bytes

timestamp: 8 bytespayload: varying size

5. The routing table can be seen in Figure 3. The IP address 1.1.1.1 does not match any of the rules and, therefore, packets are forwarded to the default interface according to the default rule. Removing the default rule would cause the outgoing packets to drop.

```
П
                                                                           X

↑ sezgin@DESKTOP-23TDFK3: 

×

                             + ~
sezgin@DESKTOP-23TDFK3:~$ ping -c 10 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=10.5 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=10.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=10.8 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=54 time=10.9 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=54 time=10.6 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=54 time=11.1 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=54 time=10.3 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=54 time=10.4 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=54 time=10.9 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=54 time=10.9 ms
  - 1.1.1.1 ping statistics --
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 10.312/10.710/11.072/0.243 ms
sezgin@DESKTOP-23TDFK3:~$
sezgin@DESKTOP-23TDFK3:~$ ip route
default via 172.26.128.1 dev eth0
172.26.128.0/20 dev eth0 proto kernel scope link src 172.26.128.47
sezgin@DESKTOP-23TDFK3:<mark>~$</mark>
```

Figure 3: ping Packets and Routing Table

- 6. (a) The 48-bit Ethernet address ofmy computer is 00:15:5d:6e:77:1b.
  - (b) The 48-bit destination address in the Ethernet frame is also 00:15:5d:6e:77:1b, which belongs to my computer.
  - (c) The type fields in layer 2 of ICMP packets are all 0x0800, which means IPv4. For other packets:
    - 0x0800 (IPv4) for most of the packets
    - 0x86dd (IPv6) for some of the packets
    - 0x0806 (ARP) for Address Resolution Protocol packets