Student Information

Full Name: Ozan Akın
Id Number: 2309599

Screenshots

```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: PcsCompu_9e:fa:37 (08:00:27:9e:fa:37), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 1.1.1.1
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xfa1f [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 2]
    Timestamp from icmp data: Jan 12, 2021 17:01:56.000000000 +03
    [Timestamp from icmp data (relative): 0.917095596 seconds]
  ▶ Data (48 bytes)
```

Figure 1: ICMP Request

```
▶ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_9e:fa:37 (08:00:27:9e:fa:37)
▶ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 10.0.2.15
▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x0220 [correct]
    [Checksum Status: Good]
    Identifier (BE): 2 (0x0002)
    Identifier (LE): 512 (0x0200)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 22,623 ms]
    Timestamp from icmp data: Jan 12, 2021 17:01:56.000000000 +03
    [Timestamp from icmp data (relative): 0.939718603 seconds]
  ▶ Data (48 bytes)
```

Figure 2: ICMP Reply

```
oznakn@vbox:~$ 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    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

Figure 3: Route Table

Answers

1. (10 Points)

For ICMP request, the source is `10.0.2.15`, and the destination is `1.1.1.1`. For ICMP response, the source is `1.1.1.1`, and the destination is `10.0.2.15`.

2. (20 Points)

As seen from screenshots, the ICMP protocol uses IP protocol, not UDP or TCP. Since both ICMP and IP protocol definitions have no port info, there is no port number in the packet information.

3a. (15 Points)

The `type` info used for declaring the packet type, such as request or response. The `code` info declares basic status for request and reply packages, such as network unreachable error.

3b. (15 Points)

For `type`, 8 means ICMP Echo (ping) request, and 0 means ICMP Echo ping reply. These are written in request and reply packages. For `code`, it is always written 0, which means there is no problem.

4. (20 Points)

`98 bytes` are transferred in total with ICMP request package. `14 bytes` for Ethernet protocol header, `20 bytes` for IP header and `16 bytes` for ICMP header. Considering the `48 bytes` data, `14 + 20 + 16 + 48 = 98`.

For ICMP header, `1 byte` is used for declaring the packet type, `1 byte` for packet code, `2 bytes` for checksum, `2 bytes` for identifier, `2 bytes` for sequence number, and `8 bytes` for timestamp data. `1 + 1 + 2 + 2 + 2 + 8 = 16`.

5. (20 Points)

The first rule must be deleted to drop outgoing packages; which is the rule with destination `0.0.0.0`, and genmask `0.0.0.0`. If we look closely the destination and genmask fields, we can see both `10.0.2.0` and `169.254.0.0` are private IPs. Our target server `1.1.1.1` is only valid for the destination `0.0.0.0` with the genmask `0.0.0.0` since it is a public IP address.