e2264653-report

by ismail sahin

Submission date: 10-Jan-2021 09:56PM (UTC+0300)

Submission ID: 1485311881

File name: 22117_ismail_sahin_e2264653-report_157888_870658300.pdf (138.26K)

Word count: 434

Character count: 1885

Student Information

Full Name: İsmail ŞAHİN Id Number: 2264653

Screenshots

```
⊕ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

⊕ Ethernet II, Src: QuantaCo_ab:380:7a (54:3b:23:ab:30:7a), Dst: Tp-LinkT_6a:52:ec (30:b5:c2:6a:52:ec)

⊕ Internet Fortecool Version 4, Src: 192.168.1.108, Dst: 1.1.1.1

■ Internet Control Message Protocol

Type: 8 (Ecno (ping) request)

Code: 9

Checksum: Status: 60001

[Oheksum: Status: 6000]

[Ioentifier (EE): 2 (0x0200)

Sequence number (EE): 12 (0x0200)

Sequence number (EE): 12 (0x0200)

Sequence number (EE): 256 (0x0100)

[Essponse remain: 12 256 (0x0100)

[Essponse remain: 12 256 (0x0100)

[Timestamp From Loop data: Jan 18, 2021 16:28:49.000000000 +03

[Timestamp From Loop data (relative): 8.61044648 seconds]

⊕ Data (48 bytes)
```

Figure 1: ICMP request

```
☐ Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
☐ Ethernet II, Src: Tp-Linkf_6a:E2:ec (80:B5:C2:6a:E2:ec), Dst: QuantaCo_ab:38:fa (54:ab:3a:ab:38:fa)
☐ Internet Potocol Version 4, Src: 1.1.1.1, Dst: 192.168.1.108
☐ Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x907a [correct]
[Checksum Status: 6000]
Identifar (E8): 2 (0x0002)
Identifar (E8): 2 (0x0002)
Identifar (E8): 2 (0x0002)
Identifar (E8): 2 (0x0002)
Sequence number (E8): 1 (0x0001)
Sequence number (E1): 256 (0x1000)
[Request Trame: 1]
[Response time: 50,782 ms]
Ilmestemp from Long data: Jan 10, 2021 16:20:49.00000000 +03
[Timestamp from Long data (relative): 0.661228005 seconds]
□ Data (48 bytes)
```

Figure 2: ICMP reply

```
ismail@ismail-laptop:~$ route -n
Kernel IP routing table
Destination
                                                 Flags Metric Ref
                                                                     Use Iface
                Gateway
                                Genmask
0.0.0.0
                192.168.1.1
                                0.0.0.0
                                                 UG
                                                       100
                                                              Θ
                                                                       0 enp2s0
0.0.0.0
                                0.0.0.0
                                                       20600 0
                192.168.1.1
                                                 UG
                                                                       0 wlp3s0
169.254.0.0
                0.0.0.0
                                255.255.0.0
                                                U
                                                       1000
                                                              0
                                                                       0 enp2s0
                                                              0
192.168.1.0
                0.0.0.0
                                255.255.255.0
                                                 U
                                                       100
                                                                       0 enp2s0
192.168.1.0
                0.0.0.0
                                255.255.255.0
                                                       600
                                                              0
                                                                       0 wlp3s0
```

Figure 3: Routing Table

Answers

1. (10 Points)

For Request Pocket:

IP of the source host: 192.168.1.108 IP of the destination host: 1.1.1.1

For Reply Pocket:

IP of the source host: 1.1.1.1

IP of the destination host: 192.168.1.108

2. (20 Points)

An ICMP pocket does not have a source and destination port because, port numbers are used in transport layer protocols (UDP, TCP, etc.). ICMP is for communication twork layer. ICMP communicate between hosts and routers. I does not communicate between applications or processes.

3a. (15 Points)

"type" and "code" fields are used for to idetify ICMP messages. These gives information about its content. Thanks to these fields these messages can be interpretted.

3b. (15 Points)

For Request Pocket:

Type: 8 (Echo (ping) request)

Code:0

As we see in the type field it is 8. It means that this pocket is an Echo Request message. Code field is is 0. That means that there is no code. Some other type messages can have code field, this specifies the messages.

For Reply Pocket:

Type: 0 (Echo (ping) reply)

Code:0

As we see in the type field it is 0. It means that this pocket is an Echo Reply message. Code field is is 0. That means that there is no code.

4. (20 Points)

14 bytes are used for protocol Ethernet's header + 20 bytes are used for protocol IP's header + 1 byte is used for ICMP header's type field + 1 byte is used for ICMP header's code field + 2 bytes is used for ICMP header's checksum field + 4 bytes are used for rest of ICMP header(it can change type and code of packet) + 48 bytes are used for data field of ICMP + 8 bytes are used for timestamp field of ICMP = 98 total bytes

5. (20 Points)

If we remove first rule which destination is 0.0.0.0 and Iface is enp2s0, outgoing pockets will be dropped and we cannot send any ping requests. Because first two rules are default rules of our routing table and becouse of my using enp2s0 interface, I use first rule. When we send our pings, destination address is 1.1.1.1 and this does not match with any other rule out of first one and all packets go through this rule. So, if I remove this rule from table, all outgoing packets dropped and I cannot send any ping request.

e2264653-report

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

/100

Instructor

PAGE 1

PAGE 2



Comment 1

why are they used there?