Basics of Communication Engineering. COMM.100
Reyver Serna (K412764)
reyverarley.sernalerma@tuni.fi

Project Work 5: Protocol Analysis

Ethernet

Let us start with examining Ethernet frame header.

➢ **Task 5.1:** During Lecture 12, we went through in detail the content of the first Ethernet frame (frame number 15). The frame 15 has been sent by the PC and the nearest router has received it. Next, we will analyze the frame number 16.

a) What is the destination address (MAC address) of frame 16?

00 07 e9 0a 85 56 corresponding to the PC's MAC address.

b) What is the source address (MAC address) of frame 16?

00 0f f7 1e 9e c1 corresponding to the router.

c) Based on these MAC addresses, how do you know that frame 16 probably contains a response to the request contained in frame 15?

Based on these MAC addresses, we can determine that frame 16 is a response frame because fram 15 was sent from the PC to the router, and 16 is sent from the router to the PC. This is the logic to follow in a TCP/IP protocol.

d) Why these MAC addresses are specifically the MAC addresses of the PC and the router and not for example the addresses of the PC and the server?

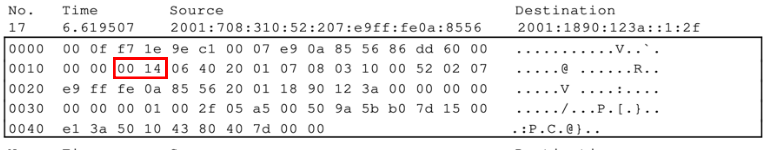
Because these are capture in the link layer in the network. Here, the PC and the router communicate on the same physical segment, meanwhile the server is on a different segment. Therefore, frames 15 and 16 show how PC and router communicate with each other because they are directly connected on the same physical network segment. The server's MAC is not visible since it is not directly involved in this communication.

IP

Let us examine next the IP header.

➢ **Task 5.2:** Analyze the IP packet inside the Ethernet frame 17.

a) What is the value in the *Payload length* field in the IP packet header inside the Ethernet frame 17?



```
No.   Time        Source                             Destination
17    6.619507    2001:708:310:52:207:e9ff:fe0a:8556  2001:1890:123a::1:2f
0000  00 0f f7 1e 9e c1 00 07 e9 0a 85 56 86 dd 60 00   ...........V..`.
0010  00 00 00 14 06 40 20 01 07 08 03 10 00 52 02 07   .....@ ......R..
0020  e9 ff fe 0a 85 56 20 01 18 90 12 3a 00 00 00 00   .....V ....:....
0030  00 00 00 01 00 2f 05 a5 00 50 9a 5b b0 7d 15 00   ...../...P.[.}..
0040  e1 3a 50 10 43 80 40 7d 00 00                    .:P.C.@}..
```

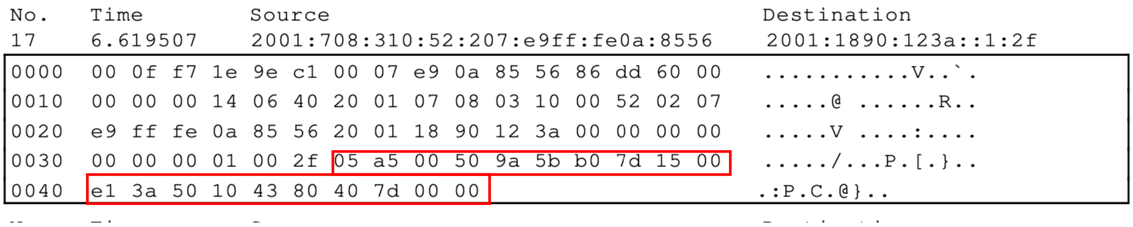
b) The content of all captured frames is represented in hexadecimal format. Convert the hexadecimal number you got in a)-part to decimal number (base-10 system).

h'00 14 is **20** in decimal.

Mathematical discloser:

$1x16^1+4x16^0 = \mathbf{20}$

c) The *Payload length* indicates the length of data field in octets. One octet is represented with two hexadecimal digits. Frame content has been presented in groups of two hexadecimal digits so that number of octets is easy to count. Include a picture of frame 17 to your report and highlight the *data field* of the IP packet. Check that the data field has correct number of octets (the number you got in b)-part). [Hint: The last field of IP packet header is *Destination address* and after that starts the data field that continues until the end of the packet.]



```
No.   Time        Source                             Destination
17    6.619507    2001:708:310:52:207:e9ff:fe0a:8556  2001:1890:123a::1:2f
0000  00 0f f7 1e 9e c1 00 07 e9 0a 85 56 86 dd 60 00   ...........V..`.
0010  00 00 00 14 06 40 20 01 07 08 03 10 00 52 02 07   .....@ ......R..
0020  e9 ff fe 0a 85 56 20 01 18 90 12 3a 00 00 00 00   .....V ....:....
0030  00 00 00 01 00 2f 05 a5 00 50 9a 5b b0 7d 15 00   ...../...P.[.}..
0040  e1 3a 50 10 43 80 40 7d 00 00                    .:P.C.@}..
```

d) How many bits the data field of that IP packet contains? [Hint: The answer of the b)-part is the number of octets, and it should be now multiplied with the number of bits in an octet. In other words, you must know how many bits one octet contains in general.]

#bits = #octects x Bits/octect

#bits = 20 octects x 8 bits/octect

#bits = **160 bits**

➢ **Task 5.3:** Analyze further the IP packet inside the Ethernet frame 17.

a) What is the value in the *Hop limit* field of the IP packet inside the Ethernet frame 17?

40

b) What does this *Hop limit* value mean in practice?

Hop limits is the maximun number of hops (routers) that a packet can cross before being dropped out. Every time a packet crossed a router the Hop Limit is decreased by one. When this number gets to zero, the packet is discarded. In that way, the packet is not circulatin in the network forever.

c) Why in the previous frame (frame number 16) the *Hop limit* of the IP packet has smaller value than the value in the IP packet of the frame 17?

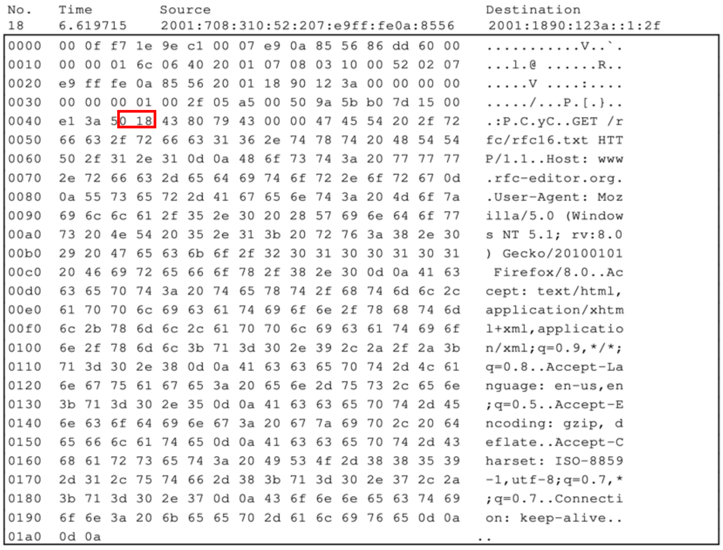
Because the Hop limit field decreases whe the packet goes through other routers in the network. Namely, the packet crossed at least six routers.

TCP

➢**Task 5.4:** Analyze the TCP segment inside the frame number 18.

a) What is the value of *Flags* field of the TCP segment in frame 18? Give the value as hexadecimal number as it is given in the *TCPIP_example_all_frames.pdf.*

0 18



```
No.   Time        Source                              Destination
18    6.619715    2001:708:310:52:207:e9ff:fe0a:8556   2001:1890:123a::1:2f
0000  00 0f f7 1e 9e c1 00 07 e9 0a 85 56 86 dd 60 00   ...........V..`.
0010  00 00 01 6c 06 40 20 01 07 08 03 10 00 52 02 07   ...l.@ ......R..
0020  e9 ff fe 0a 85 56 20 01 18 90 12 3a 00 00 00 00   .....V ....:....
0030  00 00 00 01 00 2f 05 a5 00 50 9a 5b b0 7d 15 00   ...../...P.[.}..
0040  e1 3a 50 18 43 80 79 43 00 00 47 45 54 20 2f 72   .:P.C.yC..GET /r
0050  66 63 2f 72 66 63 31 36 2e 74 78 74 20 48 54 54   fc/rfc16.txt HTT
0060  50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77   P/1.1..Host: www
0070  2e 72 66 63 2d 65 64 69 74 6f 72 2e 6f 72 67 0d   .rfc-editor.org.
0080  0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a   .User-Agent: Moz
0090  69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77   illa/5.0 (Window
00a0  73 20 4e 54 20 35 2e 31 3b 20 72 76 3a 38 2e 30   s NT 5.1; rv:8.0
00b0  29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31   ) Gecko/20100101
00c0  20 46 69 72 65 66 6f 78 2f 38 2e 30 0d 0a 41 63    Firefox/8.0..Ac
00d0  63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c   cept: text/html,
00e0  61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d   application/xhtm
00f0  6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f   l+xml,applicatio
0100  6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b   n/xml;q=0.9,*/*;
0110  71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61   q=0.8..Accept-La
0120  6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e   nguage: en-us,en
0130  3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45   ;q=0.5..Accept-E
0140  6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64   ncoding: gzip, d
0150  65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43   eflate..Accept-C
0160  68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39   harset: ISO-8859
0170  2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a   -1,utf-8;q=0.7,*
0180  3b 71 3d 30 2e 37 0d 0a 43 6f 6e 6e 65 63 74 69   ;q=0.7..Connecti
0190  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a   on: keep-alive..
01a0  0d 0a                                            ..
```

b) Convert the answer of the a)-part to binary number.

0001 1000

c) Based on previous part, which of the TCP flags have been set, i.e., which flags have binary value of 1? According to the event flow chart (slide 30 of Lecture 12), one of these flags is Push (PSH), which is related to transferring application layer data. What is the meaning of the other set flag?

The Push flag (PSH) and Acknowledgement (ACK). The later (ACK flag) recognizes the receipt of data.

➢ **Task 5.5:** Which of the frames 15–23 implement the three-way handshake of TCP? In general, what is three-way handshake, and why it is needed?

Packets 15, 16, 17.

The three-way handshake is used in TCP to establish a conenction between two devices over a network, This mehtod is used to set a reliable connection before data transmission. It consist of three steps:

1. Synchronize: a SYN packet is sent from the client to the server.
2. Synchronize- Acknoledgement (SYN-ACK): is the response from the server once the SYN packet is received. Here, it recognizes the receipt of the SYN packet and also sends it own SYN packet.
3. Acknowledgement (ACK): the client acknowledges the receipt of the SYN-ACK packet, completing the handshake.

HTTP

➢ **Task 5.6:** The HTTP request sent in the frame number 18 gets a response from the server in the frame number 20.

a) Decode the hexadecimal numbers taken from the frame (listed below) to ASCII characters:

48	54	54	50	2f	31	2e	31	20	32	30	30	20	4f	4b
H	T	T	P	/	1	.	1		2	0	0		O	K

b) What does this response from the server mean specifically?

It indicates that the server has processed the client’s request successfully, and will provide the resource. HTTP/1.1specifies the protocol beign used; 200 means the statuts code of the request, which is positive and the server will deliver. OK is the textual representation of the status code.