Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

Computer Networking and IT Security (INHN0012)

Tutorial 9

Problem 1 Wireshark

Given is the hexdump in Figure 1.1 in network byte order of an Ethernet frame without checksum, which is to be analyzed in the following

```
0x0000   00 16 3e ff ff ff 00 16    3e 6d cd 0d 08 00 45 00
0x0010   00 58 9f 47 40 00 40 06    47 33 ac 10 fe 02 ac 10
0x0020   fe 01 00 16 da e2 02 5d    78 9a f2 3d 99 17 80 18
0x0030   00 e3 54 70 00 00 01 01    08 0a b3 13 65 ca 11 82
0x0040   53 20 53 53 48 2d 32 2e    30 2d 74 69 6e 79 73 73
0x0050   68 5f 6e 6f 76 65 72 73    69 6f 6e 20 5a 34 43 53
0x0060   69 31 5a 52 0d 0a
```

Figure 1.1: Hexdump of an Ethernet frame, without checksum, in network byte order

Note: To solve this task, information from the cheatsheet is necessary.

a)* In figure 1.1 mark the start and the end of the Ethernet header.

b) Reason, by highlighting and describing relevant header fields, which protocol is used at layer 3.

c)* Describe how the length of the header on layer 3 is determined. Mark and name relevant sections in figure 1.1.

d)* Mark all layer 3 adresses and name them.

e) Mark all extensions headers contained in layer 3.

f) Name and describe the 3 smallest header fields of layer 3. Indicate the size of those fields.

g) If there is an L3 SDU, state its type and justify the statement. Otherwise, state your thought process and discuss how this situation could occur.

h) The bytes at offset `0x0042` and following are payload of layer 4. Specify the ASCII representation of the first 7 B of the payload.

i) What application layer protocol is this probably and what is this protocol used for?

Problem 2 TCP Sequence Numbers

In the following, we consider a data transfer between a PC and a web server in order to understand the concept of TCP sequence and acknowledgement numbers.

a)* What is the meaning of the *Maximum Segment Size* (MSS), and what is the difference compared to the *Maximum Transmission Unit* (MTU)?

b)* Calculate the MSS for both IPv4 and IPv6 over Ethernet (MTU = 1500 B). Assume that no options or extension headers are used.

The PC now requests a text document hosted on the web server using HTTP 1.1 over IPv6. For this purpose, it sends a request with a length of $L_{\text{Request}} = 430\,\text{B}$. The web server answers the request with the HTTP response header in its own segment with $L_{\text{Response}} = 160\,\text{B}$. After the initial segment, the server sends the text file with a length of $L_{\text{Data}} = 3080\,\text{B}$, which it divides into multiple segments due to its size (*Segmentation*).

c) How many data segments will the web server send back to the client?

d) Determine the payload size in the data segments.

In the following, we want to trace the progression of all transmitted segments and consider the used sequence and acknowledgement numbers, the flags, and the payload length in each of these segments. The PC and the server choose `8999` and `1839` as their initial sequence numbers. Note that the sequence numbers in segments always refer to the sender's own initial sequence number, whereas the acknowledgement numbers always refer to the peer's initial sequence number.

First, the PC initiates the connection establishment and issues the HTTP request. The server then responds with the HTTP response, which contains only the header, and subsequently sends the data segments. After it has sent all segments, the server also initiates the connection teardown. Assume that each data segment is acknowledged individually and immediately with an own acknowledgement segment.

e) Complete the connection establishment in the diagram.

f) Complete the data of the segments for transmitting the HTTP request and the HTTP response.

g) Add the segments for transmitting the data and the corresponding acknowledgements.

h) Complete the connection teardown in the diagram.