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

Computer Networking and IT Security (INHN0012)

Tutorial 7

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

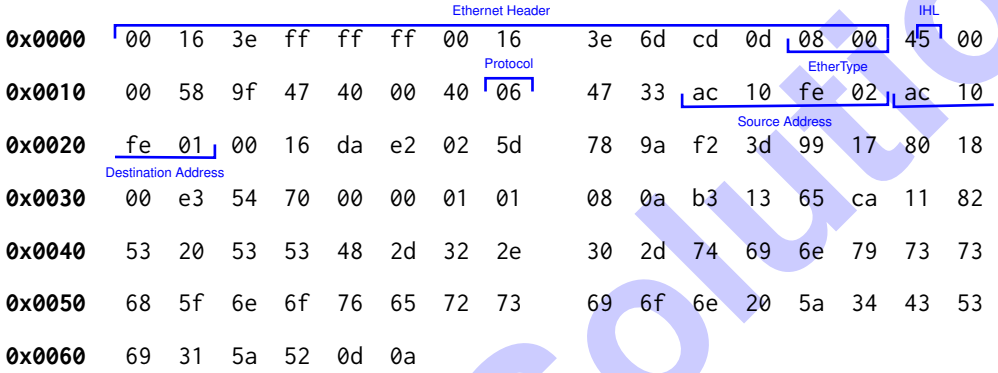

Figure 1.1: Hexdump of an Ethernet frame, without checksum, in network byte order

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.

The Ethertype specifies the type of the Layer 2 payload. The value used here `0x0800` stands for IPv4.

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

The header length in IPv4 is specified by the header field IHL. This is located in the lower nibble of the first byte of the IPv4 header and specifies the length of the header in multiples of 4 B. Thus, the length of the header is $5 \cdot 4\,\text{B} = 20\,\text{B}$.

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

e) Mark all extensions headers contained in layer 3.

The layer 3 payload is IPv4. IPv4 has no Extension Headers, only options. We know from subproblem c) that the header is 20 B long, which is the minimal length of an IPv4 header. Therefore there is nothing to mark.

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

The 3 smalles header fields are all of size 1 bit.

RES `reserved`, reserved for potential future use.

DF `do not fragment`, informs the processors that this packet shall not be fragmented

MF `more fragments`, informs that — due to a previous fragmentation — this IP packet is split into multiple fragments

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.

The value of the IPv4 header field Protocol is `0x06`. Accordingly, the L3 SDU is TCP.

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

The ASCII representation of `0x53 53 48 2d 32 2e 30` is `SSH-2.0`.

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

It is SSH (version 2.0), which is used for an encrypted console session on Linux/Unix and more recently also on Windows.

Problem 2 Subnetting

TUMexam AG is assigned the address ranges 131.159.32.0/22 and 131.159.36.0/24. The subdivision of those address ranges is left up to TUMexam AG. After a careful analysis the following requirements for the subnets and the minimal number of **usable** IP addresses are determined:

Subnet	NET 1	NET 2	NET 3	NET 4	NET 5
IPs	300	300	15	40	4

The IP address needed in for the router interface is included in those numbers.

a) Write down each first and last IP address of both given address ranges.

- 131.159.32.0/22:
  first IP: 131.159.32.0 (network address)
  last IP: 131.159.35.255 (Broadcast address)
- 131.159.36.0/24:
  first IP: 131.159.36.0 (network address)
  last IP. 131.159.36.255 (Broadcast address)

b) How many IP addresses does TUMexam AG have available? Can all of them be used to address hosts?

- 131.159.32.0/22: $2^{32-22} = 2^{10} = 1024$ addresses
- 131.159.36.0/24: $2^{32-24} = 2^{8} = 256$ addresses

There are a total of $1024 + 256 = 1280$ addresses available. However the first (network) and the last (broadcast) address of each network is not usable to address hosts. Therefore there are at maximum $1022 + 254 = 1276$ addresses available for host addressing.

c)* Is it possible to aggregate both blocks of address ranges into one single subnet?

No. The subnets are of different sizes (/22 and /24) and can therefore not be aggregated because increasing the /22 to a /21 prefix would include way more networks.
(A single subnet has always a power of two as its size, we would need one with $1024 + 256 = 1280$ addresses.)
Note: The criterion stated above is necessary, but not sufficient. Two subnets of equal size can only be aggregated iff they follow one another **and** are can be aggregated in higher-up subnet. (The last criterion is equivalent to a parent node for both subnets, if one imagines the address space as a binary tree)

d) Divide both address ranges according to the analysis in order to get subnets with fitting sizes. Use as little IP addresses as possible. A large continous address range should remain available for future use. For every subnet you should indicate:

- the size of th subnet
- the amount of usable addresses
- the subnet in prefix notation
- the subnetmask in dotted-decimal-notation
- the network and broadcast addresses

Subnet	NET 1	NET 2	NET 3
Requirement	300	300	15
Size	512	512	32
Usable	510	510	30
Prefix notation	131.159.32.0/23	131.159.34.0/23	131.159.36.64/27
Subnetmask	255.255.254.0	255.255.254.0	255.255.255.224
Network address	131.159.32.0	131.159.34.0	131.159.36.64
Broadcast	131.159.33.255	131.159.35.255	131.159.36.95

Subnet	NET 4	NET 5
Requirement	40	4
Size	64	8
Usable	62	6
Prefix notation	131.159.36.0/26	131.159.36.96/29
Subnetmask	255.255.255.192	255.255.255.248
Network address	131.159.36.0	131.159.36.96
Broadcast	131.159.36.63	131.159.36.103

To fulfill all the requirements we have to handle the subnets in order of decreasing size. Otherwise we could get into the following situation:

- Network 3 receives the address range 131.159.36.0/27.
- If we would now give network 4 the range 131.159.36.32/26 we would make a mistake. To understand this we shall take a look at the binary notation of the network address and the subnetmask: `131.159. 36.0010 0000` (IP)
  `255.255.255.1100 0000` (subnet mask)
  A bitwise AND of both numbers shows that the IP address 131.159.36.32 is part of the 131.159.36.0/26 subnet!
- We would have to give the range 131.159.36.64/26 to network 4; but then we would be left with a gap between networks 3 and 4.
- If we give the addresses out in order of decreasing subnet size, we can work around this problem. This procedure could however again contradict other criteria – for example giving out continous address ranges to single campi.