Övning 4
EITF25 & EITF45 - 2016
Protokoll

October 29, 2016

LUNDS UNIVERSITET
Lunds Tekniska Högskola

Uppgift 1.
Nedan finns en Ethernet II-ram där Preamble, SFD och CRC är borttagna. Ramen är beskriven i hexadecimalt format. Svara på följande frågor genom att studera ramens innehåll.

1.1 Till vilken MAC-adress är ramen skickad (destinationsadress)?

1.2 Från vilken MAC-adress är ramen skickad (sändaradress)?

```
08 00 20 7c 94 1c 00 00 39 51 90 37 08 00 45 00
00 3e 36 00 00 00 80 11 da 4f 82 eb 12 7f 82 eb
12 0a 04 01 00 35 00 2a ee 6a 00 01 01 00 00 01
00 00 00 00 00 00 06 67 65 6d 69 6e 69 03 6c 64
63 02 6c 75 02 73 65 00 00 01 00 01
```

Solution 1.
The preamble and the SFD have been removed from the header, leaving the destination address (DA) and sender address (SD) at the front, with 6 bytes each.

1.1 The first consecutive 6 bytes represent the DA.

Answer: 08:00:20:7C:94:1C

1.2 The second consecutive 6 bytes represent the SA.

Answer: 00:00:39:51:90:37

Uppgift 2.
Nedan finns en Ethernet-ram som bär ett IP-paket. IP-paketet startar från den 15:e byten. Ramen är beskriven i hexadecimalt format. Svara på följande frågor genom att studera ramens innehåll:

2.1 Till vilken destinationsadress skall IP-paketet?

2.2 Från vilken sändaradress kommer IP-paketet?

2.3 Vad är längden på IP-headern?

2.4 Vilket protokoll tillhör paketets datafält?

```
08 00 20 7c 94 1c 00 00 39 51 90 37 08 00 45 00
00 3e 36 00 00 00 80 11 da 4f 82 eb 12 7f 82 eb
12 0a 04 01 00 35 00 2a ee 6a 00 01 01 00 00 01
00 00 00 00 00 00 06 67 65 6d 69 6e 69 03 6c 64
63 02 6c 75 02 73 65 00 00 01 00 01
```

Solution 2.
In the figure below, each requested component has been highlighted accordingly. In addition, the beginning of the IP packet has been emphasized.

```
08 00 20 7C 94 1C 00 00 39 51 90 37 08 00 45 00
00 3E 36 00 00 00 80 11 DA 4F 82 EB 12 7F 82 EB
12 0A 04 01 00 35 00 2A EE 6A 00 01 01 00 00 01
00 00 00 00 00 00 06 67 65 6D 69 6E 69 03 6C 64
63 02 6C 75 02 73 65 00 00 01 00 01
```

2.1 Note that the Ethernet header (which does not include Preamble and SFD) has been greyed-out. As highlighted in the figure above, the destination address is 0x82:EB:12:0A, which in decimal is 130.235.18.10.

Answer: 130.235.18.10

2.2 As highlighted in the figure above, the sender address is 0x82:EB:12:7F, which in decimal is 130.235.18.127.

Answer: 130.235.18.127

2.3 As highlighted in the figure above, the length of the ID header is 0x5 which is expressed in 32 bit words. As such the header length is 160 bits or 20 bytes. Note that this is enough space to include the destination IP address, leaving no room for options.

Answer: 160 bits

2.4 As highlighted in the figure above, the data protocol is 0x11 which corresponds to UDP.

Answer: UDP

Uppgift 3.

Nedan visas tre Ethernet-II ramar som bär IPv4-paket.Vi ska undersöka dem avseende fragmentering:

3.1 Vilka flaggor har blivit satta i de olika IPv4-paketen (i headern)?

3.2 Vad kan vi utläsa från identifikationsfältet i varje header?

```
Ram 1:
0000: 00 00 0c 07 ac 01 00 00 - 39 51 90 37 08 00 45 00
0010: 05 dc 48 00 20 00 20 01 - 94 67 82 eb 12 7f 82 eb
0020: 80 64 08 00 e3 fb 03 00 - 0c 00 61 62 63 64 65 66
0030: 67 68 69 6a 6b 6c 6d 6e - 6f 70 71 72 73 74 75 76
0040: 77 61 62 63 64 65 66 67 - 68 69 6a 6b 6c 6d 6e 6f
...

Ram 2:
0000: 00 00 0c 07 ac 01 00 00 - 39 51 90 37 08 00 45 00
0010: 05 dc 48 00 20 b9 20 01 - 93 ae 82 eb 12 7f 82 eb
0020: 80 64 61 62 63 64 65 66 - 67 68 69 6a 6b 6c 6d 6e
0030: 6f 70 71 72 73 74 75 76 - 77 61 62 63 64 65 66 67
0040: 68 69 6a 6b 6c 6d 6e 6f - 70 71 72 73 74 75 76 77
...

Ram 3:
0000: 00 00 0c 07 ac 01 00 00 - 39 51 90 37 08 00 45 00
0010: 04 2c 48 00 01 72 20 01 - b4 a5 82 eb 12 7f 82 eb
0020: 80 64 69 6a 6b 6c 6d 6e - 6f 70 71 72 73 74 75 76
0030: 77 61 62 63 64 65 66 67 - 68 69 6a 6b 6c 6d 6e 6f
0040: 70 71 72 73 74 75 76 77 - 61 62 63 64 65 66 67 68
...
```

Solution 3.

Note that the sequence includes an Ethernet header (which does not include Preamble and SFD). Furthermore, the below sequence of frame is a snapshot of a fragmented datagram in three parts, starting with offset 0 bytes and moving successively up to 2960 bytes. As all the 3 frames have the same identification, we can conclude that they are apart of the same fragmentation sequence. Note, as IP packets can arrive out of sequence, including several fragmented sequences, the ID is the only thing binds a fragmented sequence on the receiver end.

3.1 **Frame 1**

```
... 48 00 20 00 20 01 ...
```

When expressed in binary

```
00100000 00000000
```

Answer: More fragments, no fragmentation offset

Frame 2

```
... 48 00 20 B9 20 01 ...
```

When expressed in binary

```
00100000 10111001
```

Answer: More fragments, fragment offset of 1480 bytes

Frame 3

```
... 48 00 01 72 20 01 ...
```

When expressed in binary

```
00000001 01110010
```

Answer: Fragmented, last fragment, fragment offset of 2960 bytes

3.2 The Identification filed consists of 2 byte and are represented by the 5^{th} and 6^{th} bytes of the IPv4 header.

Frame 1

```
... DC 48 00 20 ...
```

Answer: 48 00

Frame 2

```
... DC 48 00 20 ...
```

Answer: 48 00, same as frame 1

Frame 3

```
... 2C 48 00 01 ...
```

Answer: 48 00, same as frame 1 & 2

Uppgift 4.
Nedan visas en UDP-header i hexadecimal form.

```
06 32 00 0D 00 1C E2 17
```

Vilken är

4.1 Källporten?

4.2 Destinationsporten?

4.3 Datagrammets totala längd?

4.4 Datafältets (payload) längd?

Solution 4.
The table below reveals the content of the 8 byte UDP header.

	Hex	Decimal
Source port	0x0632	1586
Destination port	0x000D	13
Length (bytes)	0x001C	28
Checksum	0xE217	n/a

Tabell 1: UDP header breakdown

4.1 The table above reveals that the source port is 1586.

Answer: 1586

4.2 The table above reveals that the destination port is 13, which corresponds to Daytime Protocol.

Answer: 13

4.3 The table above reveals that the total length of the datagram is 28 bytes.

Answer: 28 bytes

4.4 Subtracting the header size (8) from the total length reveals that the payload is $28 - 8 = 20$ bytes.

Answer: 20 bytes

Uppgift 5.

Nedan visas en TCP-header i hexadecimal form.

`05320017 00000001 00000000 500207FF 00000000`

Vilken är:

5.1 Källporten?

5.2 Destinationsporten?

5.3 Sekvensnumret (sequence number)?

5.4 ACK-numret (acknowledgement number)?

5.5 Headerns storlek?

5.6 Segmentets typ?

5.7 Fönsterstorleken?

Solution 5.

The table below reveals the content of the 20 byte TCP header. Note that there is no room for any options.

	Hex	Decimal
Source port	`0x0532`	1330
Destination port	`0x0017`	23
Sequence number	`0x00000001`	1
Acknowledgment number	`0x00000000`	0
Data offset and flags	`0x5002`	n/a
Window size (bytes)	`0x07FF`	2047
Checksum	`0x0000`	n/a
Urgent pointer	`0x0000`	n/a

Tabell 2: TCP header breakdown

5.1 The table above reveals that the source port is 1330.

Answer: 1330

5.2 The table above reveals that the destination port is 23, which corresponds to Telnet.

Answer: 23

5.3 The table above reveals that the sequence number is 1.

Answer: 1

5.4 The table above reveals that the ACK number is 0.

Answer: 0

5.5 From counting bytes: the size of the header is 20 bytes.

Answer: 20 bytes

5.6 As reveals in the answer to question 5.2 the destination port is 23 which implies that the packet is carrying Telnet data.

Answer: Port 23 : Telnet

5.7 The table above reveals that the windows size is 2047 bytes.

Answer: 2047 bytes

Uppgift 6.

Nedan följer utskriften i hexadecimal form av ett antal Ethernetramar. Utskriften visar inte preamble, SFD eller CRC. Ramarna innehåller TCP-segment. Rita ett händelsediagram med två tidslinjer, en för vardera värddator. Varje segment ritas som en pil från sändare till mottagare. Ange för varje segment:

6.1 Typ av TCP-segment

6.2 Sekvensnummer

6.3 ACK-nummer

6.4 Fönsterstorlek.

```
Frame 1:
0000: 00 00 0c 07 ac 01 00 08 - 74 41 af a7 08 00 45 00
0010: 00 30 88 14 40 00 80 06 - d5 dc 82 eb 12 bd 82 eb
0020: 84 43 09 93 00 17 f2 d2 - 7a 29 00 00 00 00 70 02
0030: 40 00 2f a2 00 00 02 04 - 05 b4 01 01 04 02
...

Frame 2:
0000: 00 08 74 41 af a7 00 00 - 0c 07 ac 01 08 00 45 00
0010: 00 2c 53 3a 00 00 7e 06 - 4c bb 82 eb 84 43 82 eb
0020: 12 bd 00 17 09 93 a9 65 - ab 46 f2 d2 7a 2a 60 12
0030: 0b b8 24 38 00 00 02 04 - 05 b0 00 00
...

Frame 3:
0000: 00 00 0c 07 ac 01 00 08 - 74 41 af a7 08 00 45 00
0010: 00 28 88 15 40 00 80 06 - d5 e3 82 eb 12 bd 82 eb
0020: 84 43 09 93 00 17 f2 d2 - 7a 2a a9 65 ab 47 50 10
0030: 44 40 03 69 00 00 00 00 - 00 00 00 00
...

Frame 4:
0000: 00 08 74 41 af a7 00 00 - 0c 07 ac 01 08 00 45 00
0010: 00 2b 53 3b 00 00 7e 06 - 4c bb 82 eb 84 43 82 eb
0020: 12 bd 00 17 09 93 a9 65 - ab 47 f2 d2 7a 2a 50 18
0030: 0b b8 23 e8 00 00 ff fd - 18 00 00 00
...

Frame 5:
0000: 00 00 0c 07 ac 01 00 08 - 74 41 af a7 08 00 45 00
0010: 00 2e 88 16 40 00 80 06 - d5 dc 82 eb 12 bd 82 eb
0020: 84 43 09 93 00 17 f2 d2 - 7a 2a a9 65 ab 4a 50 18
0030: 44 3d ef 3f 00 00 ff fb - 18 ff fb 1f
...

Frame 6:
0000: 00 08 74 41 af a7 00 00 - 0c 07 ac 01 08 00 45 00
0010: 00 31 53 3c 00 00 7e 06 - 4c b4 82 eb 84 43 82 eb
0020: 12 bd 00 17 09 93 a9 65 - ab 4a f2 d2 7a 30 50 18
0030: 0b b8 04 eb 00 00 ff fa - 18 01 ff f0 ff fe 1f
```

Solution 6.
We need to start by identifying the TCP packet. We have previously learnt that, without preamble and SFD, an Ethernet header is 14 bytes long. The figgure below reveals what is left after the Ethernet header has been removed.

```
00 00 0c 07 ac 01 00 08 74 41 af a7 08 00 45 00
00 30 88 14 40 00 80 06 d5 dc 82 eb 12 bd 82 eb
84 43 09 93 00 17 f2 d2 7a 29 00 00 00 00 70 02
40 00 2f a2 00 00 02 04 05 b4 01 01 04 02
```

Furthermore, the subsequent 20 byte IPv4 header reveals the source and destination IP addresses: 130.235.18.189, 130.235.132.67 respectively.

```
00 00 0c 07 ac 01 00 08 74 41 af a7 08 00 45 00
00 30 88 14 40 00 80 06 d5 dc 82 eb 12 bd 82 eb
84 43 09 93 00 17 f2 d2 7a 29 00 00 00 00 70 02
40 00 2f a2 00 00 02 04 05 b4 01 01 04 02
```

We are finally left with the actual TCP content.

```
09 93 00 17 f2 d2 7a 29 00 00 00 00 70 02
40 00 2f a2 00 00 02 04 05 b4 01 01 04 02
```

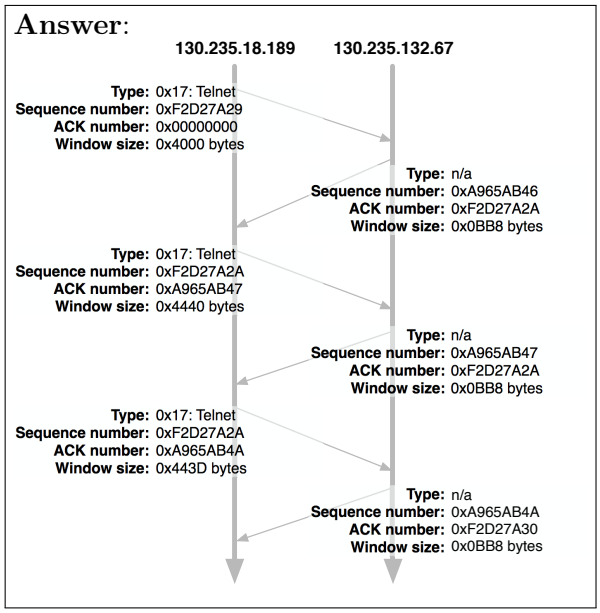
The header has the following field content:

	Hex	Decimal
Source port	0x0993	2451
Destination port	0x0017	23
Sequence number	0xF2D27A29	4073880105
Acknowledgment number	0x00000000	0
Window size (bytes)	0x4000	16384

Tabell 3: TCP header breakdown

Dissecting each frame in the same manner as above reveals that we are observing a Telnet conversation between 130.235.18.189 and 130.235.132.67.

Answer:


130.235.18.189
130.235.132.67
Type: 0x17: Telnet
Sequence number: 0xF2D27A29
ACK number: 0x00000000
Window size: 0x4000 bytes
Type: n/a
Sequence number: 0xA965AB46
ACK number: 0xF2D27A2A
Window size: 0x0BB8 bytes
Type: 0x17: Telnet
Sequence number: 0xF2D27A2A
ACK number: 0xA965AB47
Window size: 0x4440 bytes
Type: n/a
Sequence number: 0xA965AB47
ACK number: 0xF2D27A2A
Window size: 0x0BB8 bytes
Type: 0x17: Telnet
Sequence number: 0xF2D27A2A
ACK number: 0xA965AB4A
Window size: 0x443D bytes
Type: n/a
Sequence number: 0xA965AB4A
ACK number: 0xF2D27A30
Window size: 0x0BB8 bytes