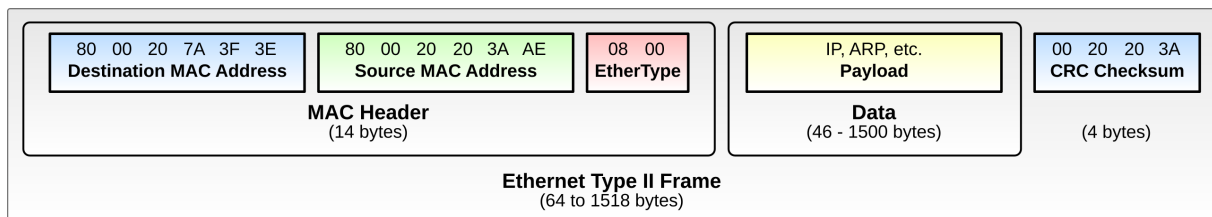# Travaux Dirigés 1

1 Reminder

Figure 1: The most common Ethernet frame format.
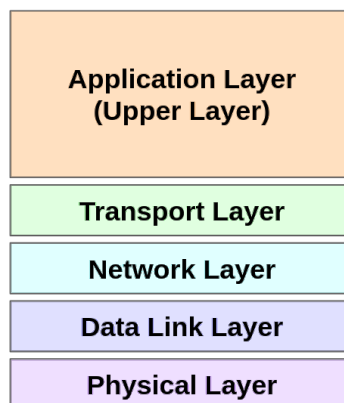

Figure 2: TCP/IP Model.

2 Packet Analysis

2.1 First Packet

One network equipement receive the following Ethernet frame:

```
1  1    0000    cc f3 a5 d2 3c 0c 58 91 cf 52 75 bd 08 00 45 00
2  2    0010    01 9f a0 db 40 00 40 06 76 5f c0 a8 2b 9b 5d b8
3  3    0020    d8 22 c3 26 00 50 95 55 26 ce fb c8 09 53 80 18
4  4    0030    01 f6 b8 85 00 00 01 01 08 0a e0 26 d8 56 e8 72
5  5    0040    c2 46 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31
6  6    0050    0d 0a 48 6f 73 74 3a 20 65 78 61 6d 70 6c 65 2e
7  7    0060    6f 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a
8  8    0070    20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31
```

```
 9  9   0080   31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b
10  10  0090   20 72 76 3a 37 38 2e 30 29 20 47 65 63 6b 6f 2f
11  11  00a0   32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78
12  12  00b0   2f 37 38 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74
13  13  00c0   65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61
14  14  00d0   74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61
15  15  00e0   70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71
16  16  00f0   3d 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c
17  17  0100   2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70
18  18  0110   74 2d 4c 61 6e 67 75 61 67 65 3a 20 66 72 2c 66
19  19  0120   72 2d 46 52 3b 71 3d 30 2e 38 2c 65 6e 2d 55 53
20  20  [...]
21  21  0170   69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d
22  22  0180   0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72
23  23  0190   65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 53
24  24  01a0   65 63 2d 47 50 43 3a 20 31 0d 0a 0d 0a
```

2.2   Layer 2 Analysis

Identify the header

Identify the destination address

Identify the source address

Identify the EtherType

Identify the payload

Identify the CRC

2.3   Layer 3 Analysis

Ethertype (decimal)	Ethertype (hex)	Description	Reference
2048	0x0800	Internet Protocol version 4 (IPv4)	RFC 7042
2054	0x0806	Address Resolution Protocol (ARP)	RFC 7042
35597	0x86DD	Internet Protocol version 6 (IPv6)	RFC 7042

Table 1: Common Ethertype.

Identify the protocol used for Layer 3.

2.4   Second Frame

```
1  0000   ff ff ff ff ff ff 58 91 cf 52 75 bd 08 00 45 00
2  0010   00 54 00 00 40 00 40 01 4e 66 c0 a8 2b 9b ff ff
3  0020   ff ff 08 00 ac 1b 02 6f 00 9c 9f 1d 42 61 00 00
```

```
4 0030    00 00 a7 87 01 00 00 00 00 00 10 11 12 13 14 15
5 0040    16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
6 0050    26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
7 0060    36 37
```

Identify the header

Identify the destination address

Identify the source address
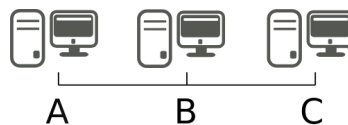
Identify the EtherType

Identify the payload

Identify the CRC

Discussion: The destination address looks a bit special. What is its role?

3 ARP Protocol

3.1 Topology

We have three computers, or network nodes, connected with a simple Ethernet link:

- A: `AA:11:22:33:44:55`
- B: `BB:11:22:33:44:55`
- C: `CC:11:22:33:44:55`

A has already communicated with B recently.

3.2 Tasks

1. Write A's ARP Table.

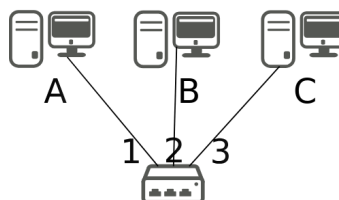| Host	Address	TTL
_____	_____	60

2. Describe the value A will put in its packets as source and destination to reach B.

3. Remind the role of the TTL field.

3.3   Updating Table

1. How can A send a packet to C?

2. Describe the values A will put in its packets as source and destination to reach C.

3. How could B try to impersonate C and receive its data?

4   CAM

4.1   Topology

We have our same three computers, or network nodes. Instead of being connected using the same physical link, frames pass through a switch:

- A: `AA:11:22:33:44:55`, connected to switch port 1

- B: `BB:11:22:33:44:55`, connected to switch port 2

- C: `CC:11:22:33:44:55`, connected to switch port 3

A has already communicated with B recently (and got a response).

4.2   Tasks

1. Write the switch CAM table.

Host	Address
_____	_____

2. How can A send a packet to C? What will the switch do?

3. Update the switch table if necessary.

Host	Address
_____	_____

4. Let's say B wants to listen to traffic from A to C, how can it proceed?