

Corrigé 2.10 Analyse de trames

1. Trame n°1

Il s'agit bien sûr d'une trame de résolution ARP.

```
*****
FRAME: Base frame properties
  FRAME: Time of capture = 23/10/2003 20:52:10
  FRAME: Time delta from previous physical frame: 1181699 microseconds
  FRAME: Frame number: 12
  FRAME: Total frame length: 42 bytes
  FRAME: Capture frame length: 42 bytes
  FRAME: Frame data: Number of data bytes remaining = 42 (0x002A)
ETHERNET: EType = ARP
  ETHERNET: Destination address = FFFFFFFFFFFF
  ETHERNET: Source address = 02BFC0A801C9
  ETHERNET: Ethernet Type : 0x0806 (ARP)
ARP_RARP: ARP: Request, Target IP: 192.168.1.201
  ARP_RARP: Hardware Type = Ethernet (10Mb)
  ARP_RARP: Protocol Type = 2048 (0x800)
  ARP_RARP: Hardware Address Length = 6 (0x6)
  ARP_RARP: Protocol Address Length = 4 (0x4)
  ARP_RARP: Opcode = Request
  ARP_RARP: Sender's Hardware Address = 02BFC0A801C9
  ARP_RARP: Sender's Protocol Address = 192.168.1.200
  ARP_RARP: Target's Hardware Address = 000000000000
  ARP_RARP: Target's Protocol Address = 192.168.1.201
```

2. Trame n°2

Cette trame constitue la réponse ARP à la trame précédente.

```
*****
FRAME: Base frame properties
  FRAME: Time of capture = 23/10/2003 20:52:15
  FRAME: Time delta from previous physical frame: 851224 microseconds
  FRAME: Frame number: 17
  FRAME: Total frame length: 42 bytes
  FRAME: Capture frame length: 42 bytes
  FRAME: Frame data: Number of data bytes remaining = 42 (0x002A)
ETHERNET: EType = ARP
  ETHERNET: Destination address = 02BFC0A801C9
  ETHERNET: Source address = 02BFC0A801C9
  ETHERNET: Ethernet Type : 0x0806 (ARP)
ARP_RARP: ARP: Reply, Target IP: 192.168.1.201
  ARP_RARP: Hardware Type = Ethernet (10Mb)
  ARP_RARP: Protocol Type = 2048 (0x800)
```

```

ARP_RARP: Hardware Address Length = 6 (0x6)
ARP_RARP: Protocol Address Length = 4 (0x4)
ARP_RARP: Opcode = Reply
ARP_RARP: Sender's Hardware Address = 00A003243819
ARP_RARP: Sender's Protocol Address = 192.168.1.201
ARP_RARP: Target's Hardware Address = 02BFC0A801C9
ARP_RARP: Target's Protocol Address = 192.168.1.200

```

3. Trame n°3

Il s'agit de la première trame envoyée par un ordinateur client DHCP (DHCP DISCOVER) ; ici, l'ordinateur est un serveur Windows 2003.

```

Trame  Heure  Adr MAC src  Adr MAC dst  Protocole  Description  Autre adr src  Autre adr
dst  Entrer une autre adresse
17  10.234717  LOCAL  *BROADCAST  DHCP  Discover          (xid=2846EA72)  0.0.0.0
255.255.255.255

```

FRAME: Base frame properties

```

FRAME: Time of capture = 23/10/2003 20:50:27
FRAME: Time delta from previous physical frame: 210303 microseconds
FRAME: Frame number: 17
FRAME: Total frame length: 342 bytes
FRAME: Capture frame length: 342 bytes
FRAME: Frame data: Number of data bytes remaining = 342 (0x0156)

```

ETHERNET: EType = Internet IP (IPv4)

```

ETHERNET: Destination address = FFFFFFFF
ETHERNET: Source address = 02BFC0A801C9
ETHERNET: Ethernet Type : 0x0800 (Internet IP (IPv4))

```

IP: Protocol = UDP - User Datagram; Packet ID = 148; Total IP Length = 328; Options = No Options

```

IP: Version = IPv4; Header Length = 20
IP: 0100.... = IP Version 4
IP: ....0101 = Header Length 20
IP: Type of Service = Normal Service
IP: 000..... = Precedence - Routine
IP: ...0.... = Normal Delay
IP: ....0... = Normal Throughput
IP: .....0.. = Normal Reliability
IP: .....0. = Normal Monetary Cost
IP: Total Length = 328 (0x148)
IP: Identification = 148 (0x94)
IP: Fragmentation Summary = 0 (0x0)
IP: .0..... = May fragment datagram if necessary
IP: ..0..... = Last fragment in datagram
IP: ...0000000000000 = Fragment Offset 0 (0x0000)
IP: Time to Live = 128 (0x80)
IP: Protocol = UDP - User Datagram
IP: Checksum = 14610 (0x3912)

```

```

IP: Source Address = 0.0.0.0
IP: Destination Address = 255.255.255.255
UDP: Src Port: Bootstrap Protocol Client (68); Dst Port: Bootstrap Protocol Server (67);
Length = 308 (0x134)
UDP: Source Port = Bootstrap Protocol Client
UDP: Destination Port = Bootstrap Protocol Server
UDP: Total length = 308 (0x134)
UDP: UDP Checksum = 0x2A3B
DHCP: Discover          (xid=2846EA72)
DHCP: Op Code           (op)      = 1 (0x1)
DHCP: Hardware Type     (htype)   = 1 (0x1) 10Mb Ethernet
DHCP: Hardware Address Length (hlen) = 6 (0x6)
DHCP: Hops              (hops)    = 0 (0x0)
DHCP: Transaction ID    (xid)     = 675736178 (0x2846EA72)
DHCP: Seconds           (secs)    = 5 (0x5)
DHCP: Flags             (flags)   = 128 (0x80)
DHCP: 1..... = Broadcast
DHCP: Client IP Address (ciaddr) = 0.0.0.0
DHCP: Your IP Address (yiaddr) = 0.0.0.0
DHCP: Server IP Address (siaddr) = 0.0.0.0
DHCP: Relay IP Address (giaddr) = 0.0.0.0
DHCP: Client Ethernet Address (chaddr) = 02BFC0A801C9
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = 99.130.83.99
DHCP: Option Field (options)
DHCP: DHCP Message Type = DHCP Discover
DHCP: Auto-Configuration = (Length: 1) 01
DHCP: Client-identifier = (Type: 1) 02 bf c0 a8 01 c9
DHCP: Requested Address = 192.168.1.101
DHCP: Host Name = srv2k3
DHCP: Client Class information = (Length: 8) 4d 53 46 54 20 35 2e 30
DHCP: Parameter Request List = (Length: 11) 01 0f 03 06 2c 2e 2f 1f 21 f9 2b
DHCP: End of this option field

```

```

00000: FF FF FF FF FF FF 02 BF C0 A8 01 C9 08 00 45 00
00010: 01 48 00 94 00 00 80 11 39 12 00 00 00 00 FF FF
00020: FF FF 00 44 00 43 01 34 2A 3B 01 01 06 00 72 EA
00030: 46 28 05 00 80 00 00 00 00 00 00 00 00 00 00
00040: 00 00 00 00 00 00 02 BF C0 A8 01 C9 00 00 00 00

```

4. Trame n°4

Il s'agit d'un ping 172.16.0.2 (aller seul - ICMP echo) à partir de l'ordinateur 172.16.0.100. Comme la trame fait moins de 64 octets et que nous sommes sur un réseau Ethernet, observez les données ajoutées en fin de trame (mises en gras ci-dessous).

```

Trame  Heure  Adr MAC src  Adr MAC dst  Protocole  Description  Autre adr src  Autre adr
dst  Taper une autre adresse
1135  9.452838  LOCAL  0050FC203A4A  ICMP  Echo: From 172.16.00.100 To
172.16.00.02  ULYSSE  172.16.0.2

```

```

Frame: Base frame properties
  Frame: Time of capture = 05/01/2004 8:51:6.904
  Frame: Time delta from previous physical frame: 70095 microseconds
  Frame: Frame number: 1135
  Frame: Total frame length: 74 bytes
  Frame: Capture frame length: 74 bytes
  Frame: Frame data: Number of data bytes remaining = 74 (0x004A)

ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol
  ETHERNET: Destination address : 0050FC203A4A
  ETHERNET: Source address : 0050FC0B9A80
  ETHERNET: Frame Length : 74 (0x004A)
  ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)
  ETHERNET: Ethernet Data: Number of data bytes remaining = 60 (0x003C)
IP: ID = 0x946F; Proto = ICMP; Len: 60
  IP: Version = 4 (0x4)
  IP: Header Length = 20 (0x14)
  IP: Precedence = Routine
  IP: Type of Service = Normal Service
  IP: Total Length = 60 (0x3C)
  IP: Identification = 37999 (0x946F)
  IP: Flags Summary = 0 (0x0)
    IP: .....0 = Last fragment in datagram
    IP: .....0. = May fragment datagram if necessary
  IP: Fragment Offset = 0 (0x0) bytes
  IP: Time to Live = 128 (0x80)
  IP: Protocol = ICMP - Internet Control Message
  IP: Checksum = 0x4DCB
  IP: Source Address = 172.16.0.100
  IP: Destination Address = 172.16.0.2
  IP: Data: Number of data bytes remaining = 40 (0x0028)
ICMP: Echo: From 172.16.00.100 To 172.16.00.02
  ICMP: Packet Type = Echo
  ICMP: Echo Code = 0 (0x0)
  ICMP: Checksum = 0xB657
  ICMP: Identifier = 768 (0x300)
  ICMP: Sequence Number = 37892 (0x9404)
  ICMP: Data: Number of data bytes remaining = 32 (0x0020)

00000:  00 50 FC 20 3A 4A 00 50 FC 0B 9A 80 08 00 45 00      .Pü :J.Pü.__.E.
00010:  00 3C 94 6F 00 00 80 01 4D CB AC 10 00 64 AC 10      .<"o._.M..d.
00020:  00 02 08 00 B6 57 03 00 94 04 61 62 63 64 65 66      ....W.."abcdef
00030:  67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76      ghijklmnopqrstuv
00040:  77 61 62 63 64 65 66 67 68 69                      wabcdefghi
*****

```

5. Trame n°5

C'est la réponse ping à la requête précédente.

L'ordinateur 172.16.0.2 envoie un ICMP echo reply.

Trame Heure Adr MAC src Adr MAC dst Protocole Description Autre adr src Autre adr
dst Taper une autre adresse
1136 9.452838 0050FC203A4A LOCAL ICMP Echo Reply: To 172.16.00.100 From
172.16.00.02 172.16.0.2 ULYSSE IP

Frame: Base frame properties

Frame: Time of capture = 05/01/2004 8:51:6.904

Frame: Time delta from previous physical frame: 0 microseconds

Frame: Frame number: 1136

Frame: Total frame length: 74 bytes

Frame: Capture frame length: 74 bytes

Frame: Frame data: Number of data bytes remaining = 74 (0x004A)

ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol

ETHERNET: Destination address : 0050FC0B9A80

ETHERNET: Source address : 0050FC203A4A

ETHERNET: Frame Length : 74 (0x004A)

ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)

ETHERNET: Ethernet Data: Number of data bytes remaining = 60 (0x003C)

IP: ID = 0x407E; Proto = ICMP; Len: 60

IP: Version = 4 (0x4)

IP: Header Length = 20 (0x14)

IP: Precedence = Routine

IP: Type of Service = Normal Service

IP: Total Length = 60 (0x3C)

IP: Identification = 16510 (0x407E)

IP: Flags Summary = 0 (0x0)

IP:0 = Last fragment in datagram

IP:0. = May fragment datagram if necessary

IP: Fragment Offset = 0 (0x0) bytes

IP: Time to Live = 255 (0xFF)

IP: Protocol = ICMP - Internet Control Message

IP: Checksum = 0x22BC

IP: Source Address = 172.16.0.2

IP: Destination Address = 172.16.0.100

IP: Data: Number of data bytes remaining = 40 (0x0028)

ICMP: Echo Reply: To 172.16.00.100 From 172.16.00.02

ICMP: Packet Type = Echo Reply

ICMP: Echo Code = 0 (0x0)

ICMP: Checksum = 0xBE57

ICMP: Identifier = 768 (0x300)

ICMP: Sequence Number = 37892 (0x9404)

ICMP: Data: Number of data bytes remaining = 32 (0x0020)

00000: 00 50 FC 0B 9A 80 00 50 FC 20 3A 4A 08 00 45 00 .Pü.____.Pü :J..E.
00010: 00 3C 40 7E 00 00 FF 01 22 BC AC 10 00 02 AC 10 .<@~..ÿ."....
00020: 00 64 00 00 BE 57 03 00 94 04 61 62 63 64 65 66 .d..W..".abcdef
00030: 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
00040: 77 61 62 63 64 65 66 67 68 69 wabcdefghi

6. Trame n°6

Il s'agit de la toute première trame http envoyée par un client web à un serveur pour préciser quelles sont ses caractéristiques. Nous avons mis en gras les éléments remarquables de cette trame.

Trame Heure Adr MAC src Adr MAC dst Protocole Description Autre adr src Autre adr
dst Taper une autre adresse

260 1.982693 LOCAL 0050FC203A4A HTTP GET Request (from client using port 6450)

ULYSSE 172.16.0.2

Frame: Base frame properties

Frame: Time of capture = 05/01/2004 8:50:59.434

Frame: Time delta from previous physical frame: 0 microseconds

Frame: Frame number: 260

Frame: Total frame length: 332 bytes

Frame: Capture frame length: 332 bytes

Frame: Frame data: Number of data bytes remaining = 332 (0x014C)

ETHERNET: ETYPE = 0x0800 : Protocol = IP: DOD Internet Protocol

ETHERNET: Destination address : **0050FC203A4A**

ETHERNET: Source address : **0050FC0B9A80**

ETHERNET: Frame Length : 332 (0x014C)

ETHERNET: Ethernet Type : **0x0800** (IP: DOD Internet Protocol)

ETHERNET: Ethernet Data: Number of data bytes remaining = 318 (0x013E)

IP: ID = 0x8E4F; Proto = TCP; Len: 318

IP: Version = 4 (0x4)

IP: Header Length = 20 (0x14)

IP: Precedence = Routine

IP: Type of Service = Normal Service

IP: Total Length = 318 (0x13E)

IP: Identification = 36431 (0x8E4F)

IP: Flags Summary = 2 (0x2)

IP:0 = Last fragment in datagram

IP:1. = Cannot fragment datagram

IP: Fragment Offset = 0 (0x0) bytes

IP: Time to Live = **128** (0x80)

IP: Protocol = TCP - Transmission Control

IP: Checksum = 0x12E4

IP: Source Address = **172.16.0.100**

IP: Destination Address = **172.16.0.2**

IP: Data: Number of data bytes remaining = 298 (0x012A)

TCP: .AP..., len: 278, seq: 742229665-742229943, ack:2463308205, win:64240, src: 6450 **dst: 80**

TCP: Source Port = 0x1932

TCP: Destination Port = **Hypertext Transfer Protocol**

TCP: Sequence Number = 742229665 (0x2C3D86A1)

TCP: Acknowledgement Number = 2463308205 (0x92D319AD)

TCP: Data Offset = 20 (0x14)

TCP: Reserved = 0 (0x0000)

TCP: Flags = 0x18 : .AP...

TCP: ..0..... = No urgent data

TCP: ...1.... = Acknowledgement field significant

TCP:1... = Push function

TCP:0.. = No Reset

TCP:0. = No Synchronize

TCP:0 = No Fin

TCP: Window = 64240 (0xFAF0)

TCP: Checksum = 0x1F2F

TCP: Urgent Pointer = 0 (0x0)

```

TCP: Data: Number of data bytes remaining = 278 (0x0116)
HTTP: GET Request (from client using port 6450)
HTTP: Request Method = GET
HTTP: Uniform Resource Identifier = /
HTTP: Protocol Version = HTTP/1.1
HTTP: Undocumented Header = Accept: */*
HTTP: Undocumented Header = Accept-Language: fr
    HTTP: Undocumented Header Fieldname = Accept-Language
    HTTP: Undocumented Header Value = fr
HTTP: Undocumented Header = Accept-Encoding: gzip, deflate
    HTTP: Undocumented Header Fieldname = Accept-Encoding
    HTTP: Undocumented Header Value = gzip, deflate
HTTP: Undocumented Header = If-Modified-Since: Tue, 09 Apr 2002 18:56:58 GMT
    HTTP: Undocumented Header Fieldname = If-Modified-Since
    HTTP: Undocumented Header Value = Tue, 09 Apr 2002 18:56:58 GMT
HTTP: Undocumented Header = If-None-Match: "7f626-b4a-3cb3397a"
    HTTP: Undocumented Header Fieldname = If-None-Match
    HTTP: Undocumented Header Value = "7f626-b4a-3cb3397a"
HTTP: Undocumented Header = User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
    HTTP: Undocumented Header Fieldname = User-Agent
    HTTP: Undocumented Header Value = Mozilla/4.0 (compatible; MSIE 5.01; Windows
NT 5.0
    HTTP: Undocumented Header = Host: 172.16.0.2
    HTTP: Undocumented Header Fieldname = Host
    HTTP: Undocumented Header Value = 172.16.0.2
HTTP: Undocumented Header = Connection: Keep-Alive
    HTTP: Undocumented Header Fieldname = Connection
    HTTP: Undocumented Header Value = Keep-Alive

00000: 00 50 FC 20 3A 4A 00 50 FC 0B 9A 80 08 00 45 00   .Pü :J.Pü.__.E.
00010: 01 3E 8E 4F 40 00 80 06 12 E4 AC 10 00 64 AC 10   .>_O@._.ä..d.
00020: 00 02 19 32 00 50 2C 3D 86 A1 92 D3 19 AD 50 18   ...2.P,=_i'.P.
00030: FA F0 1F 2F 00 00 47 45 54 20 2F 20 48 54 54 50   ú./..GET /< HTTP
00040: 2F 31 2E 31 0D 0A 41 63 63 65 70 74 3A 20 2A 2F   /1.1..Accept: */
00050: 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61   *..Accept-Langua
00060: 67 65 3A 20 66 72 0D 0A 41 63 63 65 70 74 2D 45   ge: fr..Accept-E
00070: 6E 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64   ncoding: gzip, d
00080: 65 66 6C 61 74 65 0D 0A 49 66 2D 4D 6F 64 69 66   eflate..If-Modif
00090: 69 65 64 2D 53 69 6E 63 65 3A 20 54 75 65 2C 20   ied-Since: Tue,
000A0: 30 39 20 41 70 72 20 32 30 30 32 20 31 38 3A 35   09 Apr 2002 18:5
000B0: 36 3A 35 38 20 47 4D 54 0D 0A 49 66 2D 4E 6F 6E   6:58 GMT..If-Non
000C0: 65 2D 4D 61 74 63 68 3A 20 22 37 66 36 32 36 2D   e-Match: "7f626-
000D0: 62 34 61 2D 33 63 62 33 33 39 37 61 22 0D 0A 55   b4a-3cb3397a"..U
000E0: 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C   ser-Agent: Mozil
*****

```