



Jérémy Barrette – 1736976  
Alexis Vailles – 1742139

## **Rapport TP #2 : Analyseur de protocole**

Soumis à : Kadi, Mehdi  
INF3405 (01 – B1) – Réseaux informatiques  
Session Automne 2018

École Polytechnique de Montréal  
Vendredi le 16 novembre 2018

## 6. Préparation de l'environnement de travail clients virtuel

### 6.1.

Windows7\_A :



```
C:\Windows\system32\cmd.exe
Windows IP Configuration

Host Name . . . . . : test-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Description . . . . . : Intel(R) PRO/1000 MT Network Connection
    Physical Address. . . . . : 00-0C-29-65-90-B3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e54a:c9ec:c2e5:3fd6%10(Preferred)
    IPv4 Address. . . . . : 192.168.79.137(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Tuesday, November 06, 2018 9:56:24 AM
    Lease Expires . . . . . : Tuesday, November 06, 2018 10:25:59 AM
    Default Gateway . . . . . : 192.168.79.2
    DHCP Server . . . . . : 192.168.79.254
    DHCPv6 IAID . . . . . : 234884137
    DHCPv6 Client DUID. . . . . : 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90

    DNS Servers . . . . . : 192.168.79.2
    Primary WINS Server . . . . . : 192.168.79.2
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : Teredo Tunneling Pseudo-Interface
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

Tunnel adapter 6T04 Adapter:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . : Microsoft 6to4 Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```

Windows7\_B :

```
C:\Windows\system32\cmd.exe
Windows IP Configuration

Host Name . . . . . : test-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-23-61-22
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::314f:a140:9a2b:1249%10(Preferred)
IPv4 Address. . . . . : 192.168.79.136(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, November 06, 2018 9:57:04 AM
Lease Expires . . . . . : Tuesday, November 06, 2018 10:27:04 AM
Default Gateway . . . . . : 192.168.79.2
DHCP Server . . . . . : 192.168.79.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90

DNS Servers . . . . . : 192.168.79.2
Primary WINS Server . . . . . : 192.168.79.2
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.localdomain:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter 6T04 Adapter:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft 6to4 Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```

## 8. Partie DHCP (Dynamic Host Configuration Protocol)

### 8.1.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
19	0.0.0.0	IP Broadcast		346	0.000000	DHCP	C DISCOVER 192.168.79.137 test-PC	
23	192.168.79.254	192.168.79.137		346	1.049289	DHCP	R OFFER 192.168.79.137	
24	0.0.0.0	IP Broadcast		356	1.049545	DHCP	C REQUEST 192.168.79.137 test-PC	
25	192.168.79.254	192.168.79.137		346	1.049711	DHCP	R ACK	DHCP Low Lease Time (30 minutes,...

Cette manipulation fonctionne comme suit :

- 1) Windows7\_A découvre que l'adresse 192.168.79.137 est disponible (DISCOVER)
- 2) L'adresse est ensuite offerte à la machine (OFFER)
- 3) Windows 7\_A fait la requête de l'adresse (REQUEST)
- 4) L'acquisition est ensuite confirmée (ACK).

### 8.2.

Les opérations DHCP effectuées en broadcast sont les opérations DISCOVER et REQUEST. Ces opérations doivent être faites en broadcast parce que l'ordinateur cherche à contacter les serveurs DHCP disponibles sans les connaître préalablement. Il émet donc en broadcast et c'est aux serveurs de détecter le message pour y répondre.

### 8.3.

On ne peut pas utiliser le TCP pour toutes les requêtes DHCP, car il n'est pas possible d'effectuer de broadcast sur le TCP

### 8.4.

La séquence d'encapsulation est Ethernet, IP, BOOTP, IP et DHCP

[0-13]	Ethernet:	D=Ethernet Broadcast S=Vmware:A2:73:A1
[14-33]	IP:	S=0.0.0.0 D=IP Broadcast
[34-41]	UDP:	Src=bootpc Dst=bootps
[42-277]	BOOTP:	Operation=1 Boot Request Hardware Address Type=1 H
[278-341]	DHCP:	DHCP Magic Cookie=0x63825363 Data Area=(8 bytes)

(La capture d'écran pour cette question a été fournie par une autre équipe car nous n'avions pas accès aux postes de polytechnique lorsque nous avons réalisé que la capture que nous avions était incorrecte)

## 8.5.

Le rôle du DHCP offer est d'envoyer une offre DHCP au client.

## 8.6.

Wireshark packet capture showing a DHCP Offer message. The packet list shows a DHCP Offer (Type 2) at offset 0000. The packet details pane shows the following options:

- Message Type: 2 Offer [284]
- Server Identifier: 54 Server Identifier [285]
  - Option Code: 54
  - Option Length: 4 [286]
  - Address: 192.168.79.254 [287-290]
- IP Address Lease Time: 51 IP Address Lease Time [291]
  - Option Code: 51
  - Option Length: 4 [292]
  - Value: 1800 [293-296]
- Subnet Mask: 1 Subnet Mask [297]
  - Option Code: 1
  - Option Length: 4 [298]
  - Address: 255.255.255.0 [299-302]
- Domain Name: 15 Domain Name [303]
  - Option Code: 15
  - Option Length: 11 [304]

The packet bytes pane shows the raw data of the DHCP message, with the Message Type field (02) highlighted in blue.

Il s'agit du champ 284, sa valeur est de 02.

## 8.7.

Wireshark packet capture showing the Ethernet Header of the DHCP Offer message. The Destination MAC address is 00:0C:29:65:90:B3 (VMware:65:90:B3) and the Source MAC address is 00:50:56:EB:88:6F (VMware:EB:88:6F).

Destination : 00:0C:29:65:90:B3 => correspond au poste physique Windows7\_A

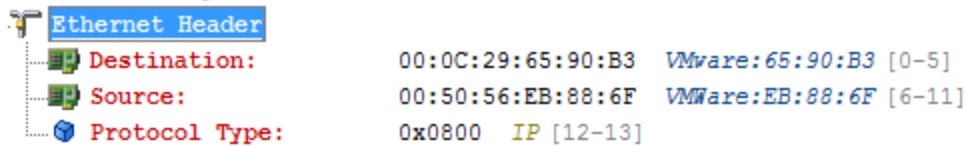
Source : 00:50:56:EB:88:6F => correspond au serveur DHCP

## 8.8.

Wireshark packet capture showing the Source IP Address of the DHCP Offer message. The Source IP Address is 192.168.79.254 [26-29].

Adresse de la source : 192.168.79.254 => appartient au serveur DHCP

## 8.9.



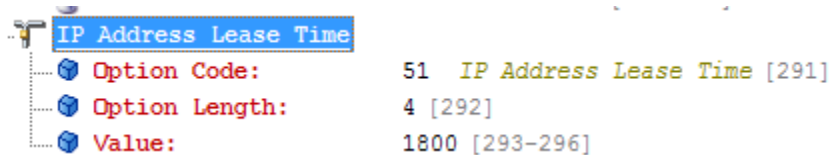
L'entête Ethernet est présente sur les octets 0 à 13, donc elle occupe un espace de 14 octets.

#### 8.10.



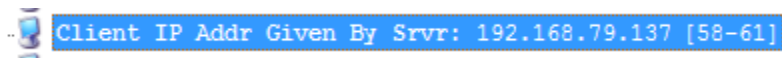
La valeur du champ Protocol Type est de 0x0800. Cette valeur signifie que c'est le protocole IP qui est utilisé.

#### 8.11.



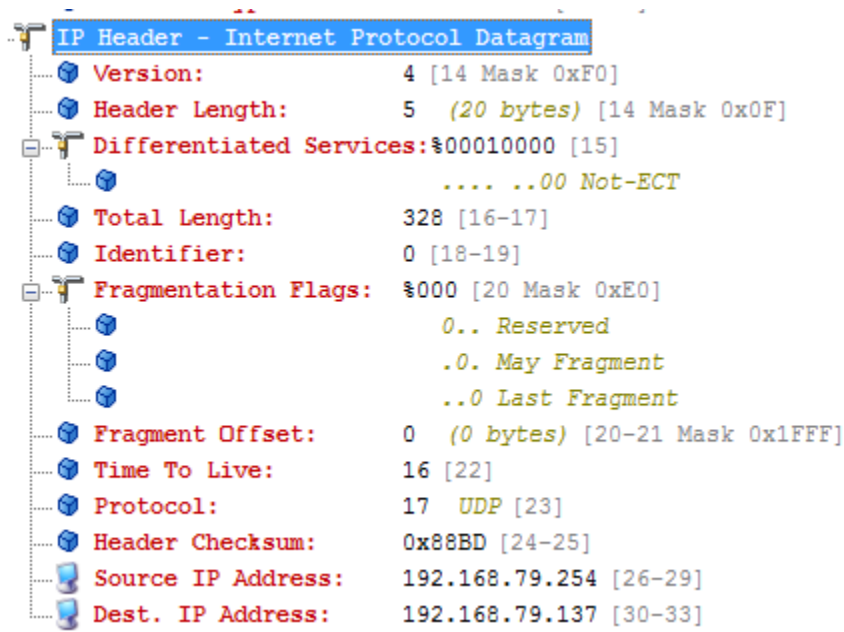
Le champ *IP Address Lease Time* correspond au temps que la machine a avant de devoir revalider son adresse avec le serveur DHCP. Il s'agit du temps dont elle dispose pour faire une requête de cette adresse, sinon elle en changera à la fin du délai.

#### 8.12.



Le champ *Client IP Addr Given By Srwr* désigne l'adresse prêtée par le serveur DHCP. Son utilité est d'informer le client de sa nouvelle IP adresse.

### 8.13.

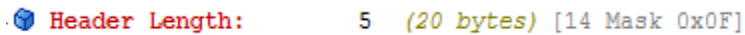


The image shows a Wireshark packet capture of an IP Header. The header is expanded, showing various fields with their values and bit masks. The fields include Version, Header Length, Differentiated Services, Total Length, Identifier, Fragmentation Flags, Fragment Offset, Time To Live, Protocol, Header Checksum, Source IP Address, and Dest. IP Address.

Field	Value	Mask
Version:	4	[14 Mask 0xF0]
Header Length:	5 (20 bytes)	[14 Mask 0x0F]
Differentiated Services:	00010000	[15]
Total Length:	328	[16-17]
Identifier:	0	[18-19]
Fragmentation Flags:	000	[20 Mask 0xE0]
Fragment Offset:	0 (0 bytes)	[20-21 Mask 0x1FFF]
Time To Live:	16	[22]
Protocol:	17 UDP	[23]
Header Checksum:	0x88BD	[24-25]
Source IP Address:	192.168.79.254	[26-29]
Dest. IP Address:	192.168.79.137	[30-33]

Il s'agit de l'entête de la trame IP.

### 8.14.



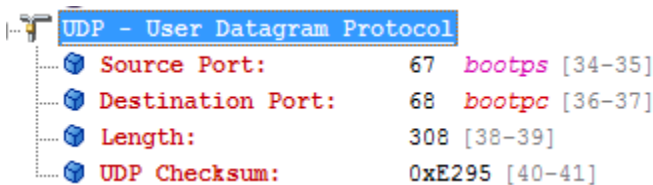
The image shows a close-up of the Header Length field in the IP Header. The value is 5, which corresponds to 20 bytes.

Field	Value	Mask
Header Length:	5 (20 bytes)	[14 Mask 0x0F]

La longueur observée est de 20 octets.

### 8.15.

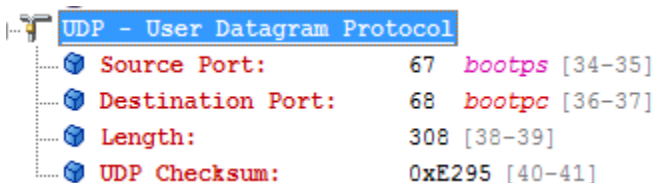
Il s'agit du protocole UDP :



The image shows a Wireshark packet capture of a UDP Header. The header is expanded, showing fields such as Source Port, Destination Port, Length, and UDP Checksum.

Field	Value	Mask
Source Port:	67 bootps	[34-35]
Destination Port:	68 bootpc	[36-37]
Length:	308	[38-39]
UDP Checksum:	0xE295	[40-41]

### 8.16.

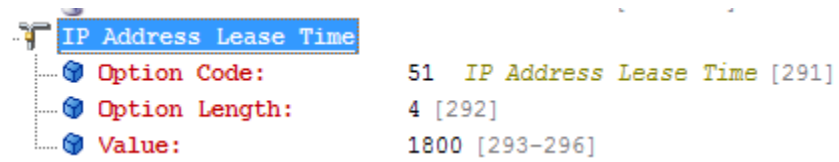


The image shows a Wireshark packet capture of a UDP Header, identical to the one in 8.15. The header is expanded, showing fields such as Source Port, Destination Port, Length, and UDP Checksum.

Field	Value	Mask
Source Port:	67 bootps	[34-35]
Destination Port:	68 bootpc	[36-37]
Length:	308	[38-39]
UDP Checksum:	0xE295	[40-41]

L'entête UDP est présente sur les octets 34 à 41, donc elle occupe un espace de 8 octets.

### 8.17.



La machine Windows 7 doit revalider son adresse IP avec le serveur DHCP au bout de 1800 secondes, soit 30 minutes.



## 9. Partie ARP (Address Résolution Protocol)

### 9.1.

Le protocole ARP a pour but d'associer une adresse IP à une adresse de niveau 2, comme une adresse MAC.

### 9.2.

```
C:\Users\Administrator>arp -a

Interface: 192.168.79.137 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.254        00-50-56-eb-88-6f    dynamic
192.168.79.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Administrator>_
```

### 9.3.

```
C:\Users\Administrator>ping 192.168.79.136

Pinging 192.168.79.136 with 32 bytes of data:
Reply from 192.168.79.136: bytes=32 time<1ms TTL=128
Reply from 192.168.79.136: bytes=32 time<1ms TTL=128
Reply from 192.168.79.136: bytes=32 time<1ms TTL=128
Reply from 192.168.79.136: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.79.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>arp -a

Interface: 192.168.79.137 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.136        00-0c-29-23-61-22    dynamic
192.168.79.254        00-50-56-eb-88-6f    dynamic
192.168.79.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Administrator>
```

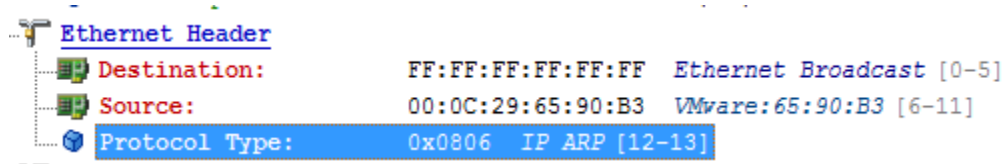
On remarque que l'adresse IP de Windows7\_B est maintenant dans le ARP de Windows7\_A.

#### 9.4.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1	VMware:65:90:B3	Ethernet Broadcast		64	0.000000	ARP Request	192.168.79.136 = ?
2	VMware:23:61:22	VMware:65:90:B3		64	0.000228	ARP Response	VMware:23:61:22 = 192.168.79.136
5	VMware:65:90:B3	VMware:23:61:22		64	0.000514	ARP Response	VMware:65:90:B3 = 192.168.79.137

On observe dans la colonne *size* que la longueur des trames est de 64 octets.

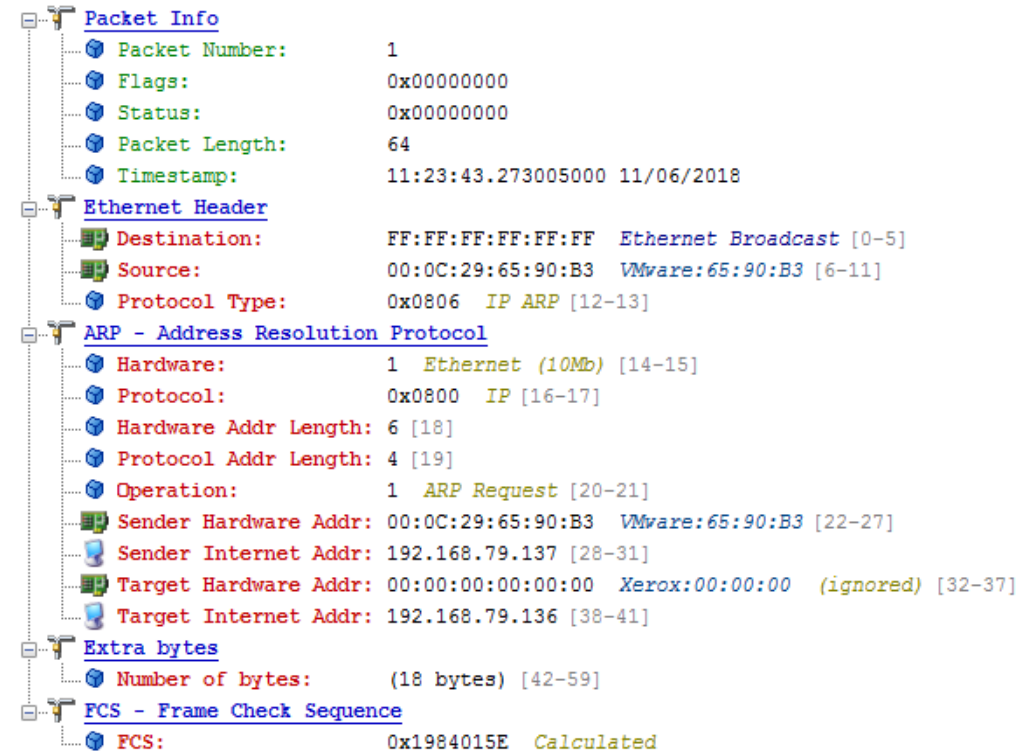
#### 9.5.



La valeur numérique est de 0x806. Cette valeur signifie que c'est le protocole IP ARP qui est utilisé.

#### 9.6.

Requête :



Réponse :

The image shows a Wireshark packet capture details pane for an ARP response packet. The tree on the left shows the hierarchy: Packet Info, Ethernet Header, ARP - Address Resolution Protocol, Extra bytes, and FCS - Frame Check Sequence. The details pane shows the following fields:

<b>Packet Info</b>		
Packet Number:	2	
Flags:	0x00000000	
Status:	0x00000000	
Packet Length:	64	
Timestamp:	11:23:43.273233000	11/06/2018
<b>Ethernet Header</b>		
Destination:	00:0C:29:65:90:B3	VMware:65:90:B3 [0-5]
Source:	00:0C:29:23:61:22	VMware:23:61:22 [6-11]
Protocol Type:	0x0806	IP ARP [12-13]
<b>ARP - Address Resolution Protocol</b>		
Hardware:	1	Ethernet (10Mb) [14-15]
Protocol:	0x0800	IP [16-17]
Hardware Addr Length:	6	[18]
Protocol Addr Length:	4	[19]
Operation:	2	ARP Response [20-21]
Sender Hardware Addr:	00:0C:29:23:61:22	VMware:23:61:22 [22-27]
Sender Internet Addr:	192.168.79.136	[28-31]
Target Hardware Addr:	00:0C:29:65:90:B3	VMware:65:90:B3 [32-37]
Target Internet Addr:	192.168.79.137	[38-41]
<b>Extra bytes</b>		
Number of bytes:	(18 bytes)	[42-59]
<b>FCS - Frame Check Sequence</b>		
FCS:	0x5FA7F9FD	Calculated

Une requête est un broadcast (pas de target), tandis que qu'une réponse est un message spécifique à une adresse connue.

## 9.7.

The image shows a Wireshark packet capture details pane for an Ethernet header. The tree on the left shows the hierarchy: Ethernet Header. The details pane shows the following fields:

























<b>Ethernet Header</b>		
Destination:	00:0C:29:65:90:B3	VMware:65:90:B3 [0-5]
Source:	00:0C:29:23:61:22	VMware:23:61:22 [6-11]
Protocol Type:	0x0806	IP ARP [12-13]

Le nœud de la source de la première réponse ARP correspond à Windows7\_B, qui répond au broadcast de Windows7\_A.

## 9.8.

Le nœud de la destination de la première réponse ARP correspond à Windows7\_A, qui est contacté par Windows7\_B.

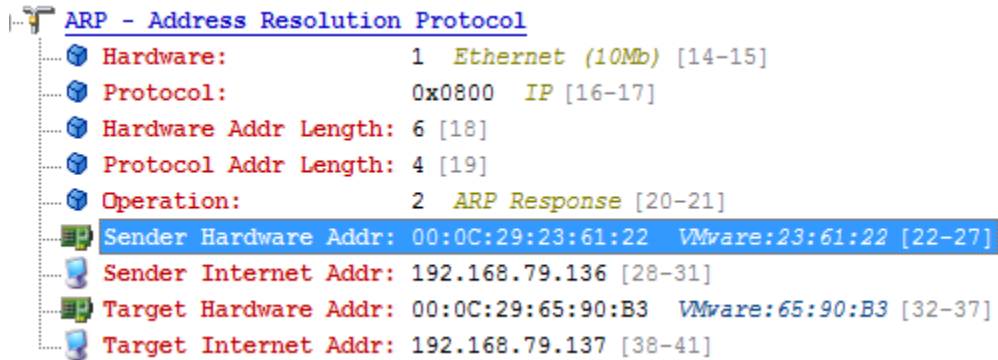
## 9.9.

	<u>Packet Info</u>	
	Packet Number:	1
	Flags:	0x00000000
	Status:	0x00000000
	Packet Length:	64
	Timestamp:	11:23:43.273005000 11/06/2018
	<u>Ethernet Header</u>	
	Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast [0-5]
	Source:	00:0C:29:65:90:B3 VMware:65:90:B3 [6-11]
	Protocol Type:	0x0806 IP ARP [12-13]
	<u>ARP - Address Resolution Protocol</u>	
	Hardware:	1 Ethernet (10Mb) [14-15]
	Protocol:	0x0800 IP [16-17]
	Hardware Addr Length:	6 [18]
	Protocol Addr Length:	4 [19]
	Operation:	1 ARP Request [20-21]
	Sender Hardware Addr:	00:0C:29:65:90:B3 VMware:65:90:B3 [22-27]
	Sender Internet Addr:	192.168.79.137 [28-31]
	Target Hardware Addr:	00:00:00:00:00:00 Xerox:00:00:00 (ignored) [32-37]
	Target Internet Addr:	192.168.79.136 [38-41]
	<u>Extra bytes</u>	
	Number of bytes:	(18 bytes) [42-59]
	<u>FCS - Frame Check Sequence</u>	
	FCS:	0x1984015E Calculated

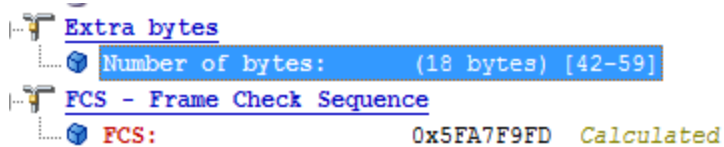
La séquence est : l'encapsulation Ethernet d'abord, et directement les informations ARP ensuite.

### 9.10.

Le champ contenant la réponse est le "Sender Hardware Addr" aux positions [22-27]. Il s'agit de l'adresse physique de l'envoyeur (Windows7\_B) qui a été contacté par son adresse internet par Windows7\_A.



### 9.11.



Il y a un espace d'octets vides additionnels (extra bytes) à la fin de la trame ARP.

Ce champ occupe  $18/64$  bytes = 28.125 %

Ce champ est nécessaire parce que la trame ARP ne fait 64 octets, soit la limite minimale d'une trame Ethernet.

## 10.1.

<b>IP Header - Internet Protocol Datagram</b>	
Version:	4 [14 Mask 0xF0]
Header Length:	5 (20 bytes) [14 Mask 0x0F]
Differentiated Services:	%00000000 [15]
	0000 00.. Default
	.... ..00 Not-ECT
Total Length:	60 [16-17]
Identifier:	4475 [18-19]
Fragmentation Flags:	%000 [20 Mask 0xE0]
	0.. Reserved
	.0. May Fragment
	..0 Last Fragment
Fragment Offset:	0 (0 bytes) [20-21 Mask 0x1FFF]
Time To Live:	128 [22]
Protocol:	1 ICMP - Internet Control Message Protocol [23]
Header Checksum:	0x0000 Checksum invalid. Should be: 0x08E4 [24-25]
Source IP Address:	192.168.79.137 [26-29]
Dest. IP Address:	192.168.79.136 [30-33]
<b>ICMP - Internet Control Messages Protocol</b>	
ICMP Type:	8 Echo Request [34]
ICMP Code:	0 [35]
ICMP Checksum:	0x4D55 [36-37]
Identifier:	0x0001 [38-39]
Sequence Number:	0x0600 [40-41]
ICMP Data Area:	(32 bytes) [42-73]
<b>FCS - Frame Check Sequence</b>	
FCS:	0xE1A1D43C Calculated

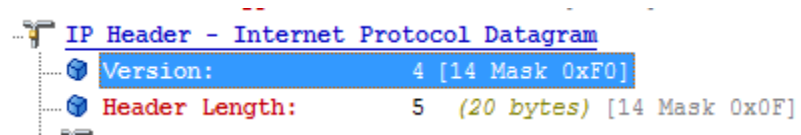
<b>IP Header - Internet Protocol Datagram</b>	
Version:	4 [14 Mask 0xF0]
Header Length:	5 (20 bytes) [14 Mask 0x0F]
Differentiated Services:	%00000000 [15]
	0000 00.. Default
	.... ..00 Not-ECT
Total Length:	60 [16-17]
Identifier:	4522 [18-19]
Fragmentation Flags:	%000 [20 Mask 0xE0]
	0.. Reserved
	.0. May Fragment
	..0 Last Fragment
Fragment Offset:	0 (0 bytes) [20-21 Mask 0x1FFF]
Time To Live:	128 [22]
Protocol:	1 ICMP - Internet Control Message Protocol [23]
Header Checksum:	0x08B5 [24-25]
Source IP Address:	192.168.79.136 [26-29]
Dest. IP Address:	192.168.79.137 [30-33]
<b>ICMP - Internet Control Messages Protocol</b>	
ICMP Type:	0 Echo Reply [34]
ICMP Code:	0 [35]
ICMP Checksum:	0x5555 [36-37]
Identifier:	0x0001 [38-39]
Sequence Number:	0x0600 [40-41]
ICMP Data Area:	(32 bytes) [42-73]
<b>FCS - Frame Check Sequence</b>	
FCS:	0x31CEF46E Calculated

Le champ est ICMP Type.

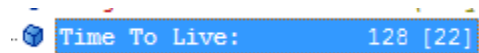
Les valeurs impliquées sont 8 (Echo Request) pour la requête et 0 (Echo Reply) pour la réponse.

## 10.2.

On utilise la version 4 :



## 10.3.



Le *Time to Live* de 128. Il s'agit de la durée maximale de transit du paquet dans le réseau.

#### 10.4.

<b>Packet Info</b>	
Packet Number:	7
Flags:	0x00000000
Status:	0x00000000
Packet Length:	78
Timestamp:	11:23:44.274070000 11/06/2018
<b>Ethernet Header</b>	
Destination:	00:0C:29:23:61:22 VMware:23:61:22 [0-5]
Source:	00:0C:29:65:90:B3 VMware:65:90:B3 [6-11]
Protocol Type:	0x0800 IP [12-13]
<b>IP Header - Internet Protocol Datagram</b>	
Version:	4 [14 Mask 0xF0]
Header Length:	5 (20 bytes) [14 Mask 0x0F]
Differentiated Services:	%00000000 [15]
	0000 00.. Default
	.... ..00 Not-ECT
Total Length:	60 [16-17]
Identifier:	4475 [18-19]
Fragmentation Flags:	%000 [20 Mask 0xE0]
	0.. Reserved
	.0. May Fragment
	..0 Last Fragment
Fragment Offset:	0 (0 bytes) [20-21 Mask 0x1FFF]
Time To Live:	128 [22]
Protocol:	1 ICMP - Internet Control Message Protocol [23]
Header Checksum:	0x0000 Checksum invalid. Should be: 0x08E4 [24-25]
Source IP Address:	192.168.79.137 [26-29]
Dest. IP Address:	192.168.79.136 [30-33]
<b>ICMP - Internet Control Messages Protocol</b>	
ICMP Type:	8 Echo Request [34]
ICMP Code:	0 [35]
ICMP Checksum:	0x4D55 [36-37]
Identifier:	0x0001 [38-39]
Sequence Number:	0x0600 [40-41]

La séquence d'encapsulation est une combinaison de protocole IP et Ethernet



## 11. Partie théorique

### 11.1.

Lien 4:


(Le commutateur n'envoie que vers l'adresse désirée)

Lien 5

A6:B7:C8:D9:E1:F2	A1:B2:C3:D4:E5:F6
132.207.29.102/24	132.207.29.103/24

Lien 6

A6:B7:C8:D9:E1:F2	A1:B2:C3:D4:E5:F6
132.207.29.102/24	132.207.29.103/24

### 11.2.

Lien 1:

A5:B6:C7:D8:E9:F1	A4:B5:C6:D7:E8:F9
132.207.29.102/24	132.207.30.102/24

Lien 2:

A4:B5:C6:D7:E8:F9	A3:B4:C5:D6:E7:F8
132.207.29.102/24	132.207.30.102/24

Lien 3:

A3:B4:C5:D6:E7:F8	A2:B3:C4:D5:E6:F7
132.207.29.102/24	132.207.30.102/24

Lien 4:

A2:B3:C4:D5:E6:F7	A1:B2:C3:D4:E5:F6
132.207.29.102/24	132.207.30.102/24

Lien 5:

A2:B3:C4:D5:E6:F7	A1:B2:C3:D4:E5:F6
132.207.29.102/24	132.207.30.102/24