



École Polytechnique de Montréal  
Département de génie informatique et génie logiciel

**INF3405**  
**Réseaux informatiques**  
**Automne 2018**

Travail pratique #2  
Analyseurs de protocoles

Soumis par :  
Son-Thang Pham (1856338)  
Gabriel Côté-Jones (1771119)

Soumis à :  
Dion-Paquin Émilie

Section (04)  
16 novembre 2018

# Préparation de l'environnement de travail client / serveur virtuel

## 6.1

### Windows7\_A

Nom de votre poste : L4708-27

Adresse IPv4 : 192.168.79.139

Masque de sous-réseau : 255.255.255.0

Adresse MAC : 00-0C-29-F8-4C-81

Passerelle par défaut : 192.168.79.2

```
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-F8-4C-81
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2dd4:f3b3:3493:cb64%10(Preferred)
IPv4 Address. . . . . : 192.168.79.139(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 05, 2018 5:52:42 AM
Lease Expires . . . . . : Monday, November 05, 2018 6:22:28 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
```

### Windows7\_B

Nom de votre poste : L4708-27

Adresse IPv4 : 192.168.79.140  
Masque de sous-réseau : 255.255.255.0  
Adresse MAC : 00-0C-29-01-99-7A  
Passerelle par défaut : 192.168.79.2

```
C:\Users\Administrator>ipconfig/all

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-29-01-99-7A
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::5c57:3ddc:2f93:c198%10(Preferred)
    IPv4 Address. . . . . : 192.168.79.140(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, November 05, 2018 5:52:44 AM
    Lease Expires . . . . . : Monday, November 05, 2018 6:22:29 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:

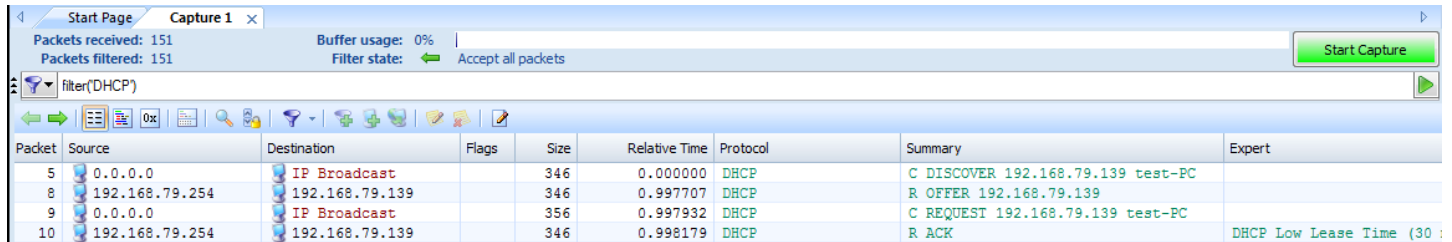
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Teredo Tunneling Pseudo-Interface
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes

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
```

## 8. Partie DHCP (Dynamic Host Configuration Protocol) (9.5 points)

### 8.1



The image shows a Wireshark packet capture window titled 'Capture 1'. The filter is set to 'filter(DHCP)'. The packet list shows four packets:

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
5	0.0.0.0	IP Broadcast		346	0.000000	DHCP	C DISCOVER 192.168.79.139 test-PC	
8	192.168.79.254	192.168.79.139		346	0.997707	DHCP	R OFFER 192.168.79.139	
9	0.0.0.0	IP Broadcast		356	0.997932	DHCP	C REQUEST 192.168.79.139 test-PC	
10	192.168.79.254	192.168.79.139		346	0.998179	DHCP	R ACK	DHCP Low Lease Time (30 :)

- 1- Le client commence par « broadcaster » un DHCP DISCOVER pour trouver un DHCP server dans le même sous-réseau.
- 2- Ensuite, le DHCP server reçoit ce « broadcast » et puis « broadcast » un DHCP OFFER au client avec une nouvelle adresse IP.
- 3- Le client récupère ce « broadcast » et « broadcast » à son tour un DHCP REQUEST au server pour obtenir son propre adresse IP.
- 4- Le server répond en « broadcastant » un DHCP ACK et donne toutes les informations nécessaires au client pour qu'il puisse changer les informations nécessaires dont l'adresse IP.

### 8.2

Tous les opérations sont effectuées en broadcast.

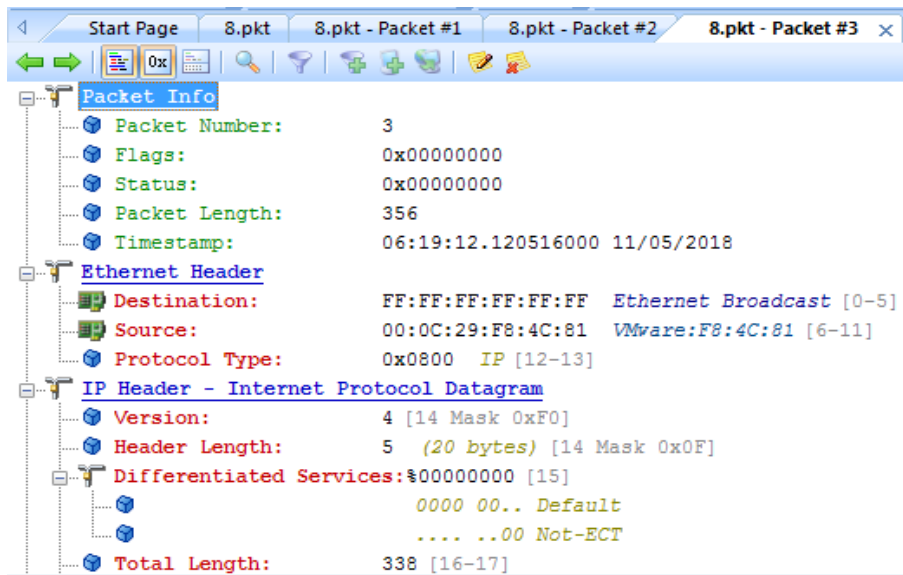
Le DHCP DISCOVER doit être effectué en broadcast. Il se fait en broadcast dans le but de découvrir les serveurs DHCP dans le sous-réseau et les avertir de son besoin de paramètres IP.

Le DHCP OFFER et DHCP ACK peuvent être fait en « broadcast » ou en « unicast » dépendamment des implantations.

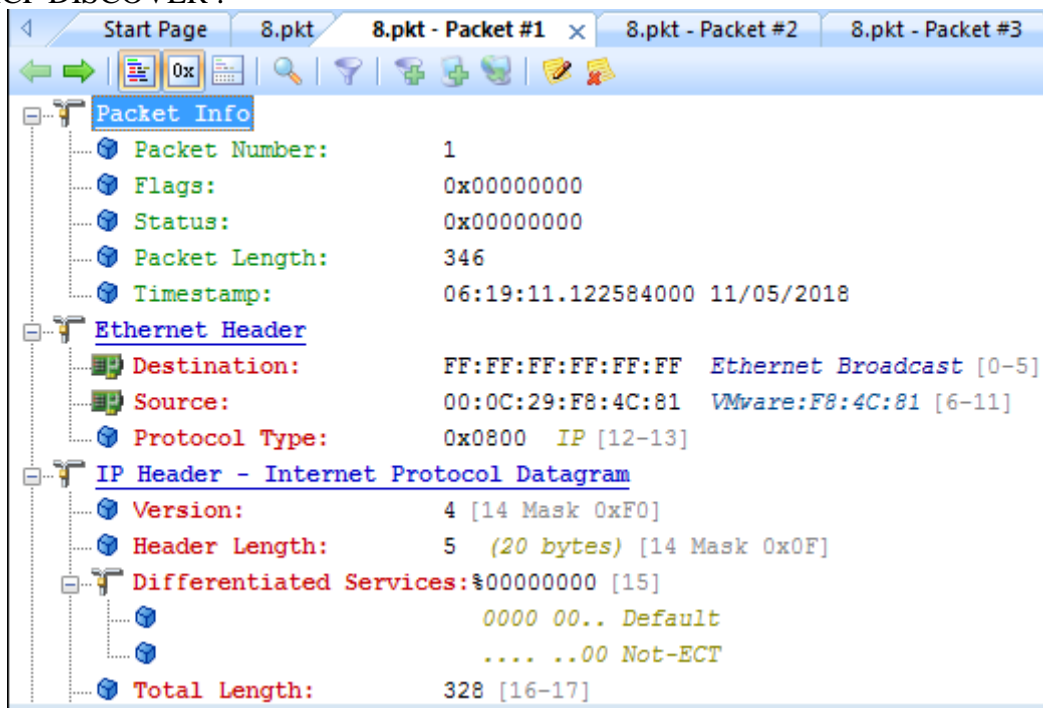
Le DHCP REQUEST doit absolument être « broadcaster » puisqu'il se peut qu'il y ait plusieurs DHCP servers dans le réseau. En « broadcastant » le DHCP REQUEST, tous les serveurs qui ont « broadcasté » un DHCP OFFER pourront savoir le choix du client et libérer l'adresse IP réservée.

Dans notre situation, le DHCP DISCOVER et DHCP REQUEST sont effectués en broadcast.

Le DHCP REQUEST :



Le DHCP DISCOVER :



8.3

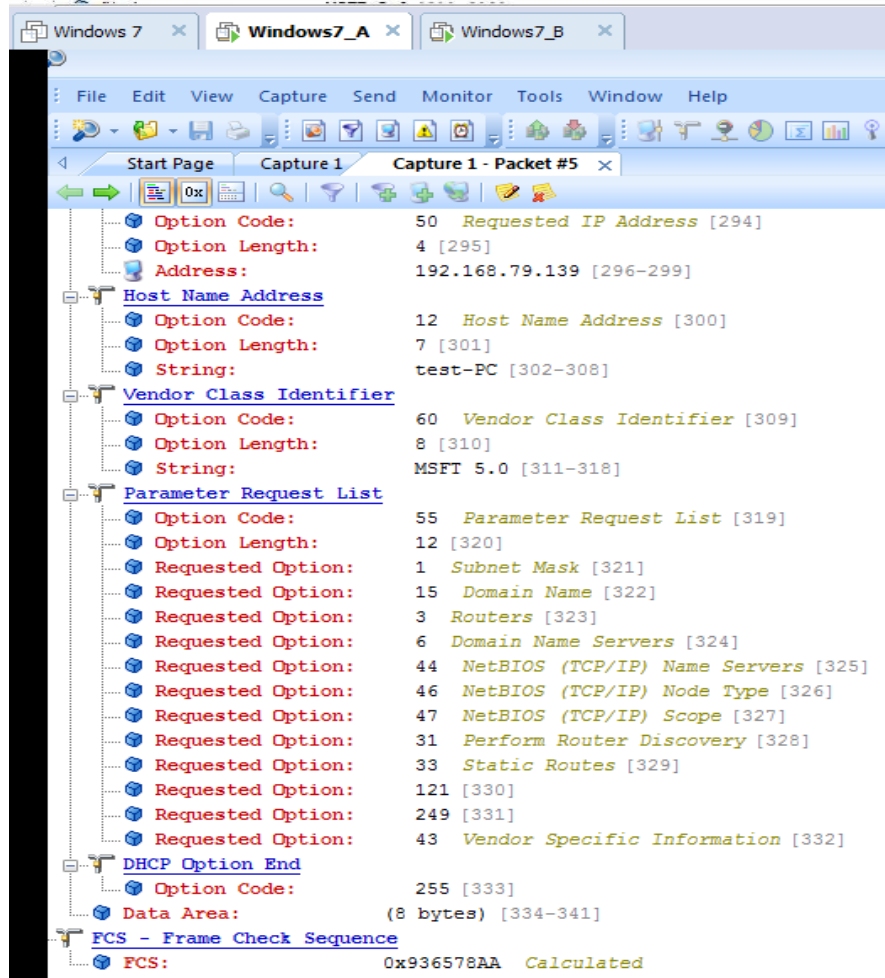
Non, il n'est pas possible d'utiliser le protocole TCP de la couche 4 pour toutes les requêtes DHCP. Comme le client n'a pas nécessairement d'adresse IP quand il fait une requête au DHCP et ne possède pas nécessairement d'adresse destination, il est impossible pour le protocole TCP qui nécessite ces adresses d'être utilisées.

## 8.4

L'encapsulation est DHCP-BootP-UDP-IP-Ethernet

The image shows a Wireshark packet capture analysis of a DHCP BootP request. The interface displays the packet list, packet details, and packet bytes panes. The packet list shows a single packet (Packet #5) of length 346 bytes, timestamped 06:19:11.122584000 on 11/05/2018. The packet details pane shows the following structure:

- Packet Info:**
  - Packet Number: 5
  - Flags: 0x00000000
  - Status: 0x00000000
  - Packet Length: 346
  - Timestamp: 06:19:11.122584000 11/05/2018
- Ethernet Header:**
  - Destination: FF:FF:FF:FF:FF:FF Ethernet Broadcast [0-5]
  - Source: 00:0C:29:F8:4C:81 VMware:F8:4C:81 [6-11]
  - Protocol Type: 0x0800 IP [12-13]
- IP Header - Internet Protocol Datagram:**
  - 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: 328 [16-17]
  - Identifier: 4086 [18-19]
  - Fragmentation Flags: 0000 [20 Mask 0xE0]
    - 0.. Reserved
    - .0. May Fragment
- Fragmentation Flags:**
  - .0. May Fragment
  - ..0 Last Fragment
- Fragment Offset:** 0 (0 bytes) [20-21 Mask 0xFFFF]
- Time To Live:** 128 [22]
- Protocol:** 17 UDP [23]
- Header Checksum:** 0x29B0 [24-25]
- Source IP Address:** 0.0.0.0 [26-29]
- Dest. IP Address:** 255.255.255.255 IP Broadcast [30-33]
- UDP - User Datagram Protocol:**
  - Source Port: 68 bootpc [34-35]
  - Destination Port: 67 bootps [36-37]
  - Length: 308 [38-39]
  - UDP Checksum: 0x0145 [40-41]
- BootP - Bootstrap Protocol:**
  - Operation: 1 Boot Request [42]
  - Hardware Address Type: 1 Ethernet (10Mb) [43]
  - Hardware Address Length: 6 bytes [44]
  - Hops: 0 [45]
  - Transaction ID: 4115058281 [46-49]
  - Seconds Since Boot Start: 0 [50-51]
  - BootP Flags: 0x0000 [52-53]





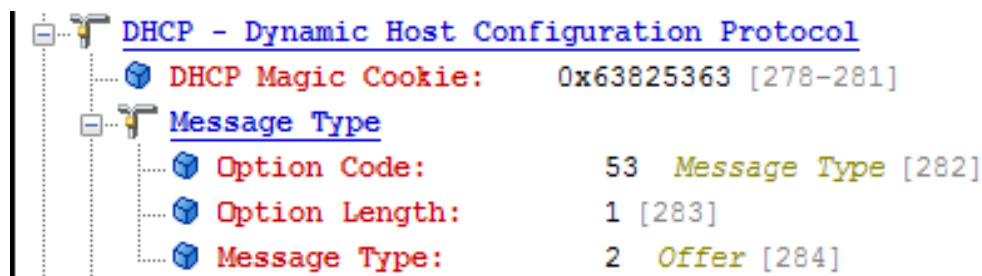
0000:	FF FF FF FF FF 00 0C 29 F8 4C 81 08 00 45 00 01 48 0F F6 00 00 80 11 29 B0 00 00 00 00 FF FF FF FF 00 44 00 43 01 34 01 45 01	.....).L..E..H.....).D.C.4.E.
0043:	01 06 00 F5 46 CE 69 00	...F.i.....).L.....
0086:	00 00	.....
0129:	00 00	.....
0172:	00 00	.....
0215:	00 00	.....
0258:	00 00	.....c.Sc5..=.....).L.2...O..
0301:	07 74 65 73 74 2D 50 43 3C 08 4D 53 46 54 20 35 2E 30 37 0C 01 0F 03 06 2C 2E 2F 1F 21 79 F9 2B FF 00 00 00 00 00 00 00 00 00	.test-PC<.MSFT 5.07...../..!y+.....
0344:	00 00	..

8.5

Le DHCP OFFER envoie les informations du réseau tel que l'adresse IP proposée, le masque de sous-réseau, le IP de la passerelle par défaut, le IP de l'adresse DNS, etc.

8.6

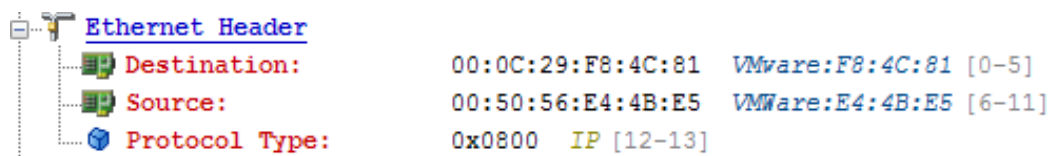
Le champ « Message Type » spécifie exactement que c'est le DHCP Offer. Sa valeur est : 2 Offer (284)



8.7

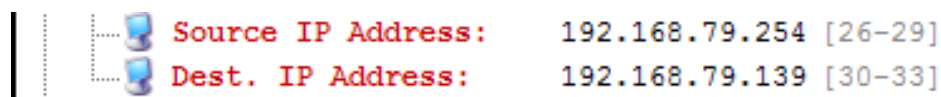
La destination correspond à l'adresse MAC de la machine Windows\_7A

La source correspond à l'adresse MAC du serveur DHCP.



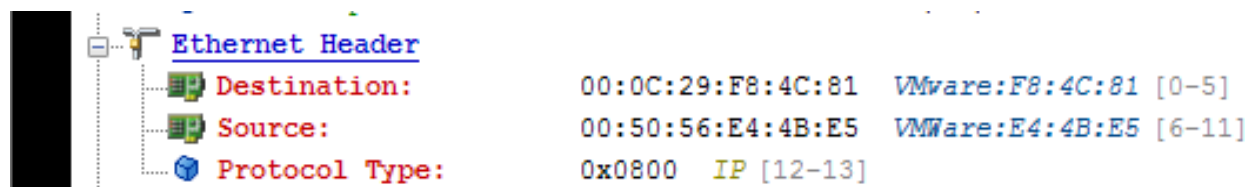
8.8

Elle appartient au DHCP server.



8.9

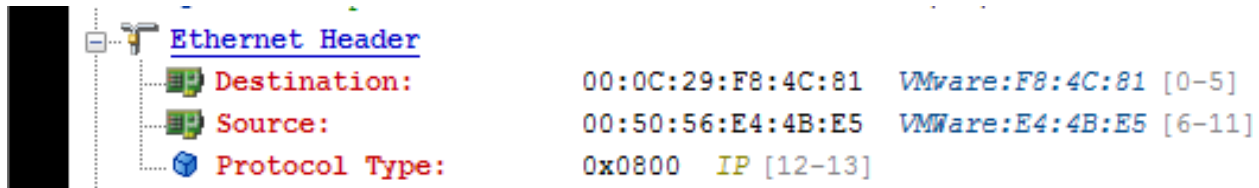
L'entête Ethernet occupe 14 octets.





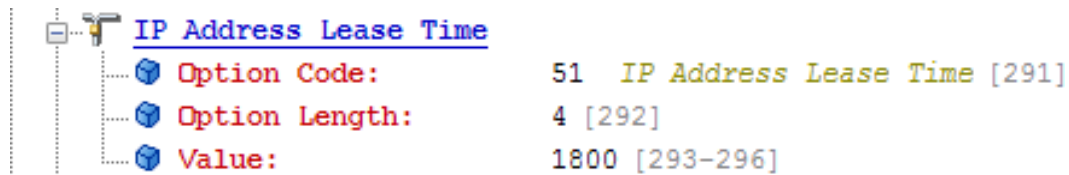
### 8.10

La valeur du champ Protocole Type est de 0x0800 et représente le paquet IPv4.



### 8.11

Elle signifie le période de temps que l'adresse IP nous est alloué. A la fin de ce temps, s'il n'est pas renouvelé, cette adresse IP peut être utilisé par un autre utilisateur.



### 8.12

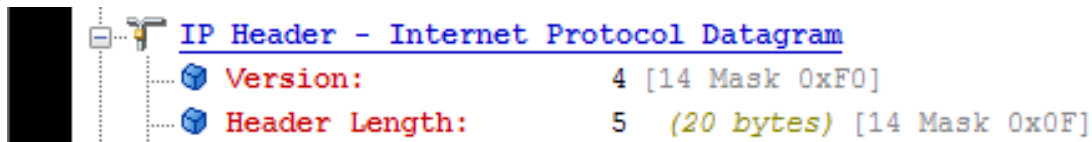
Ce champ représente l'adresse IP que le server (DHCP) a offert au client. Cette adresse est importante pour que l'adresse puisse se connecter au server.

### 8.13

C'est l'entête de la trame IP (IP Header).

### 8.14

La taille est de 20 octets.

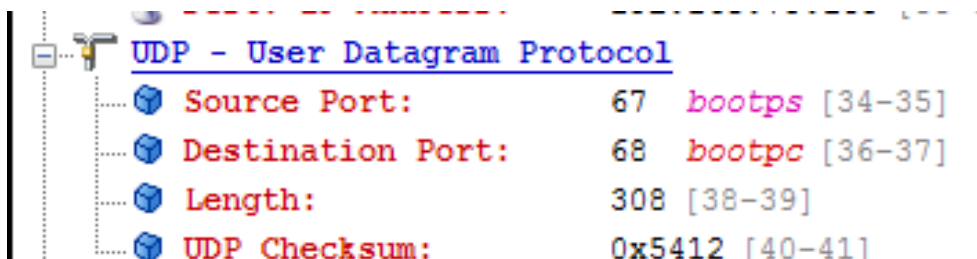


### 8.15

C'est le protocole UDP.

### 8.16

La taille est de 8 octets.



### 8.17

Dans 1800 secondes. (Voir capture 8.11)

## 9. Partie ARP (Address Resolution Protocol) (4 points)

9.1

La cache ARP garde en mémoire des couples IPv4-MAC. Le protocole ARP utilise cette cache pour obtenir l'adresse MAC associée à une adresse IP quel qu'on sans quoi il doit broadcast un ARP request pour l'obtenir.

9.2

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

Interface: 192.168.79.139 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.140         00-0c-29-01-99-7a    dynamic
192.168.79.254         00-50-56-e4-4b-e5    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>arp -d 192.168.79.140

C:\Users\Administrator>arp -a

Interface: 192.168.79.139 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.254         00-50-56-e4-4b-e5    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
```

9.3

L'adresse IP de Windows 7B réapparaît.

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

Interface: 192.168.79.139 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.140         00-0c-29-01-99-7a    dynamic
192.168.79.254         00-50-56-e4-4b-e5    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>arp -d 192.168.79.140

C:\Users\Administrator>arp -a

Interface: 192.168.79.139 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.254         00-50-56-e4-4b-e5    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>ping 192.168.79.140

Pinging 192.168.79.140 with 32 bytes of data:
Reply from 192.168.79.140: bytes=32 time<1ms TTL=128
Reply from 192.168.79.140: bytes=32 time<1ms TTL=128
Reply from 192.168.79.140: bytes=32 time<1ms TTL=128
Reply from 192.168.79.140: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.79.140:
    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: 192.168.79.139 --- 0xa
Internet Address      Physical Address      Type
192.168.79.2          00-50-56-e1-1b-39    dynamic
192.168.79.140         00-0c-29-01-99-7a    dynamic
192.168.79.254         00-50-56-e4-4b-e5    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
```

## 9.4

Elles sont de 64 octets.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
4	VMware:F8:4C:81	Ethernet Broadcast		64	0.000188	ARP Request	192.168.79.2 = ?
5	VMware:E1:1B:39	VMware:F8:4C:81		64	0.000293	ARP Response	VMware:E1:1B:39 = 192.168.79.2
12	VMware:F8:4C:81	Ethernet Broadcast		64	20.711798	ARP Request	192.168.79.140 = ?
13	VMware:01:99:7A	VMware:F8:4C:81		64	20.712100	ARP Response	VMware:01:99:7A = 192.168.79.140
16	VMware:F8:4C:81	VMware:01:99:7A		64	20.712388	ARP Response	VMware:F8:4C:81 = 192.168.79.139

## 9.5

Elles sont toutes de 0x0806 IP ARP[12-13] et représente simplement le protocole d'adresse de révolution (address resolution protocole).

## 9.6

La destination est de type ethernet broadcast pour la requête ARP tandis que la réponse ne l'est pas. Le numéro d'opération indiquant request or response diffère également. D'autres champs comme « Target Hardware Addr » et « Target Internet Addr » sont également différents.

Request:

<b>Packet Info</b>	
Packet Number:	4
Flags:	0x00000000
Status:	0x00000000
Packet Length:	64
Timestamp:	06:56:04.793264000 11/05/2018
<b>Ethernet Header</b>	
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast [0-5]
Source:	00:0C:29:F8:4C:81 VMware:F8:4C:81 [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:	1 ARP Request [20-21]
Sender Hardware Addr:	00:0C:29:F8:4C:81 VMware:F8:4C:81 [22-27]
Sender Internet Addr:	192.168.79.139 [28-31]
Target Hardware Addr:	00:00:00:00:00:00 Xerox:00:00:00 (ignored) [32-37]
Target Internet Addr:	192.168.79.2 [38-41]
<b>Extra bytes</b>	
Number of bytes:	(18 bytes) [42-59]
<b>FCS - Frame Check Sequence</b>	
FCS:	0x6FFECE5E Calculated

Response:



9.7

Le nœud source correspond à Windows7\_B.

9.8

Le nœud source correspond à Windows7\_A.

9.9

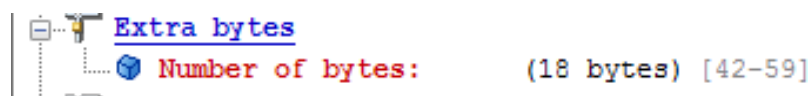
ARP-Ethernet

9.10

Le champ « Sender Hardware Addr ».

9.11

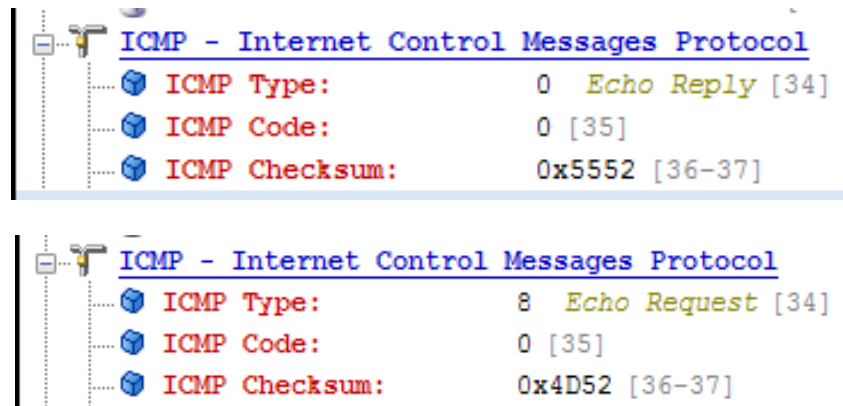
Nous pouvons observer la section « Extra bytes » avec une valeur de 18 bytes. Elle occupe 28.125% de la taille de la trame. Ce champ est nécessaire parce que la trame ARP ne fait 64 octets qui est le minimum d'une trame Ethernet.



## 10. Partié PING (2 points)

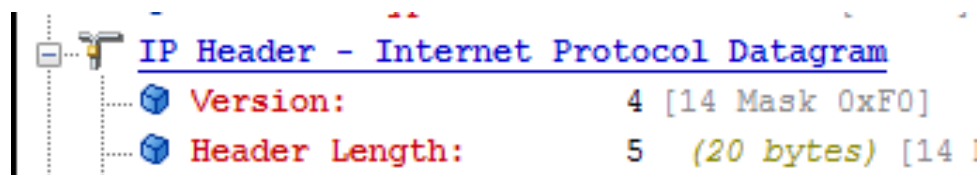
### 10.1

Le champ est le ICMP type et les valeurs impliquées sont « 0 Echo Reply » pour la réponse et « 8 Echo Request » pour la requête.



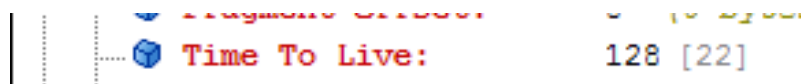
### 10.2

La version du protocole IP utilisée est la version 4.



### 10.3

La valeur du champ TTL est de 128. Ce champ indique la durée maximale de transit d'un paquet IP dans le réseau. La durée de vie est représentée par un compteur qui est décrémenté d'un à chaque routeur (la plupart des routeurs ne supportent pas la décrément en secondes).



### 10.4

ICMP-IP-Ethernet

## 11. Partie théorique (4 points)

### 11.1.

Le paquet ne passe pas par le lien 4. Après utilisation du mask sur l'adresse IP destination, il se rend compte que l'ordinateur à ping est dans le même réseau.

#### lien 5

MAC destination : A2:B3:C4:D5:E6:F7	MAC source : A1:B2:C3:D4:E5:F6
IP source : 132.207.29.102	IP destination : 132.207.29.103

#### lien 6

MAC destination : A6:B7:C8:D9:E1:F2	MAC source : A2:B3:C4:D5:E6:F7
IP source : 132.207.29.102	IP destination : 132.207.29.103

### 11.2.

#### lien 5

MAC destination : A2:B3:C4:D5:E6:F7	MAC source : A1:B2:C3:D4:E5:F6
IP source : 132.207.29.102	IP destination : 132.207.30.102

#### lien 4

MAC destination : A2:B3:C4:D5:E6:F7	MAC source : A1:B2:C3:D4:E5:F6
IP source : 132.207.29.102	IP destination : 132.207.30.102

#### lien 3

MAC destination : A3:B4:C5:D6:E7:F8	MAC source : A2:B3:C4:D5:E6:F7
IP source : 132.207.29.102	IP destination : 132.207.30.102

#### lien 2

MAC destination : A4:B5:C6:D7:E8:F9	MAC source : A3:B4:C5:D6:E7:F8
IP source : 132.207.29.102	IP destination : 132.207.30.102

#### lien 1

MAC destination : A5:B6:C7:D8:E9:F1	MAC source : A4:B5:C6:D7:E8:F9
IP source : 132.207.29.102	IP destination : 132.207.30.102