

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.**

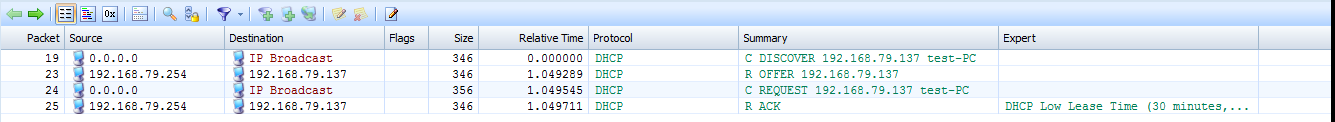
Windows7\_A :



Windows7\_B :



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

**8.1.**

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.**

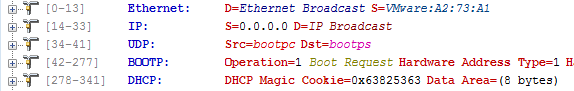
Les opérations DHCP effectuées en broadcast sont les opérations DISCOVER et REQUEST. Ces opérations doivent être faites en broadcast parce que l'ordinateur cherche à contacter les serveurs DHCP disponibles sans les connaitre préalablement. Il émet donc en broadcast et c'est aux serveurs de détecter le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

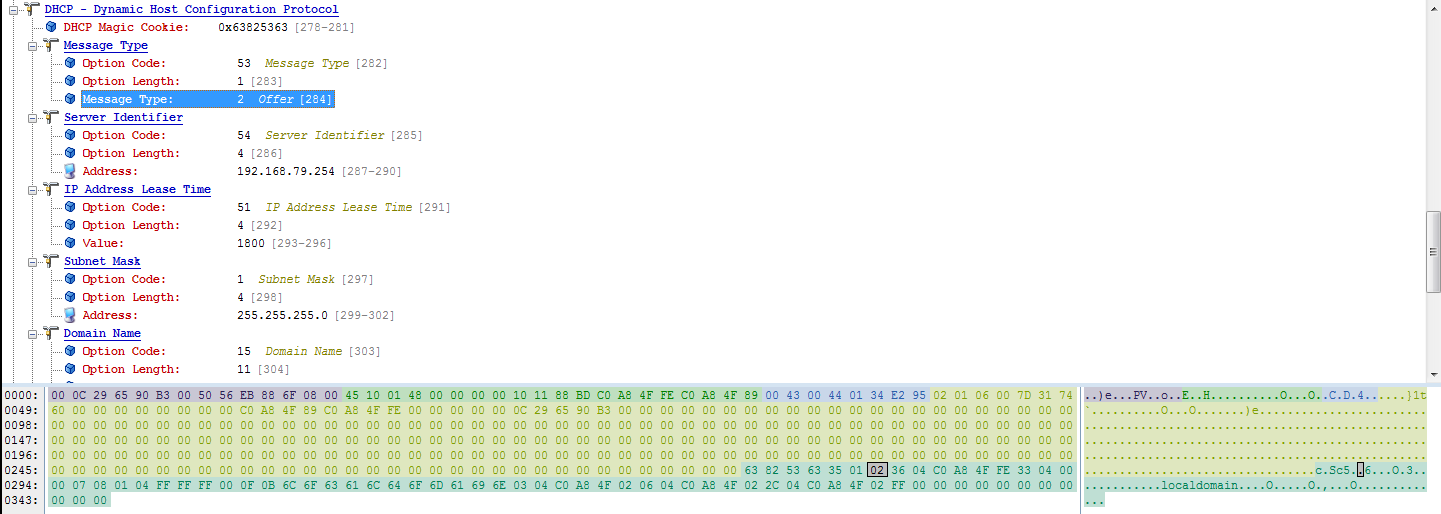


(La capture d'écran pour cette question a été fournie par une autre équipe car nous n'avions pas accès aux postes de polytechnique lorsque nous avons réalisé que la capture que nous avions était incorrecte)

**8.5.**

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

**8.6.**

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

**8.7.**



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

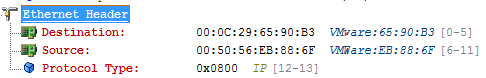
Source : 00:50:56:EB:88:6F => correspond au serveur DHCP

**8.8.**



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

**8.9.**



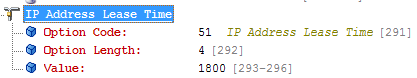
L’entête Ethernet est présente sur les octets 0 à 13, donc elle occupe un espace de 14 octets.

**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.**



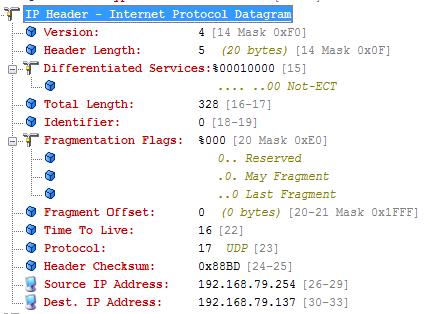
Le champ ***IP Address Lease Time*** correspond au temps que la machine a avant de devoir revalider son adresse avec le serveur DHCP. Il s’agit du temps dont elle dispose pour faire une requête de cette adresse, sinon elle en changera à la fin du délai.

**8.12.**



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

**8.13.**



Il s’agit de l’entête de la trame IP.

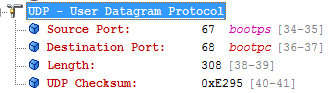
**8.14.**



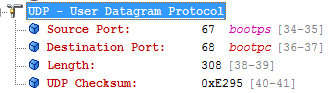
La longueur observée est de 20 octets.

**8.15.**

Il s’agit du protocole UDP :

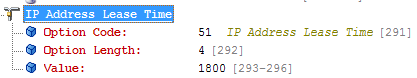


**8.16.**



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)

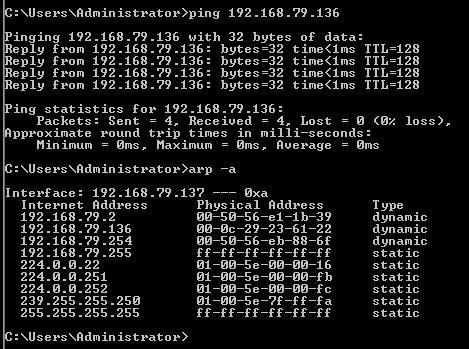
**9.1.**

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

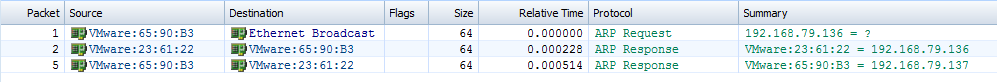
**9.2.**



**9.3.**

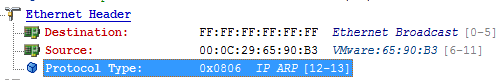


On remarque que l’adresse IP de Windows7\_B est maintenant dans le ARP de Windows7\_A.

**9.4.**

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

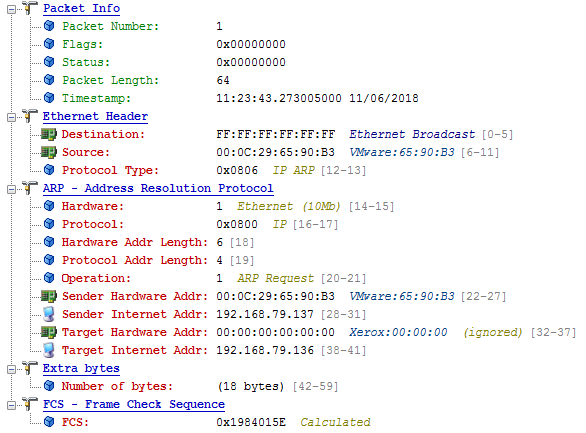
**9.5.**



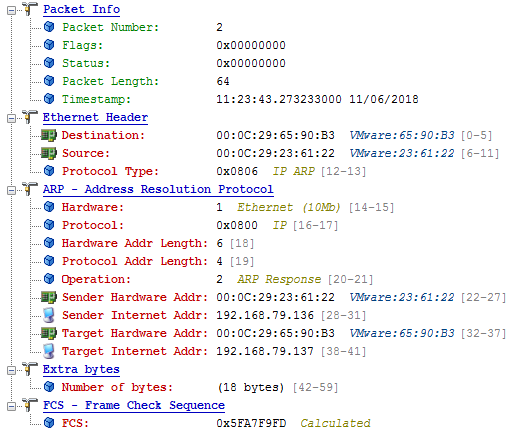
La valeur numérique est de 0x806. Cette valeur signifie que c’est le protocole IP ARP qui est utilisé.

**9.6.**

Requête :

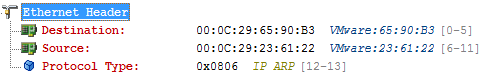


Réponse :



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

**9.7.**

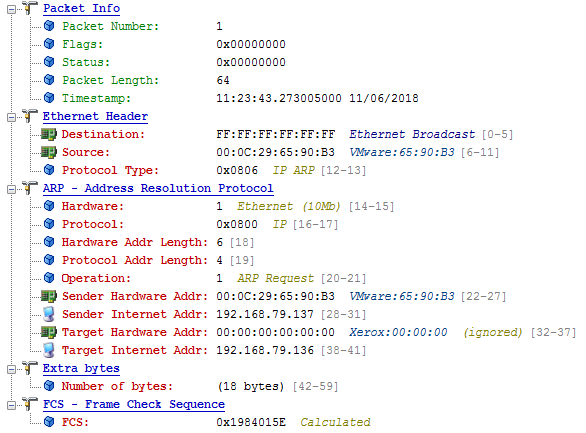


Le nœud de la source de la première réponse ARP correspond à Windows7\_B, qui répond au broadcast de Windows7\_A.

**9.8.**

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

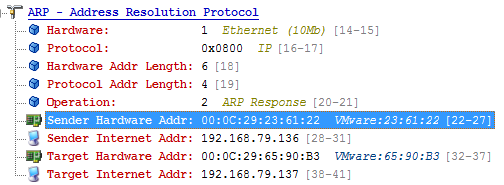
**9.9.**



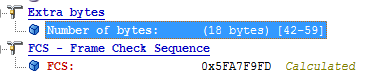
La séquence est : l’encapsulation Ethernet d’abord, et directement les informations ARP ensuite.

**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.**

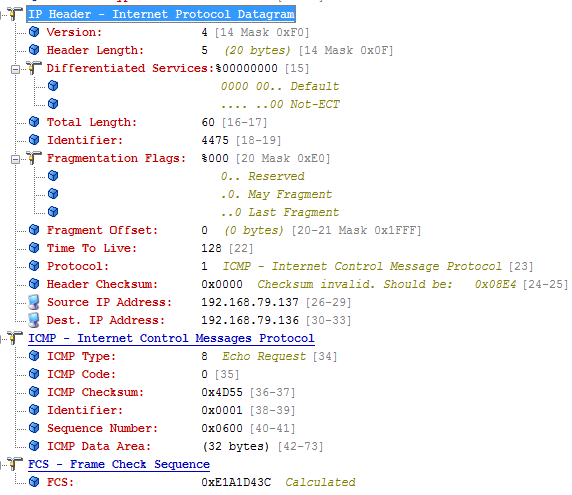


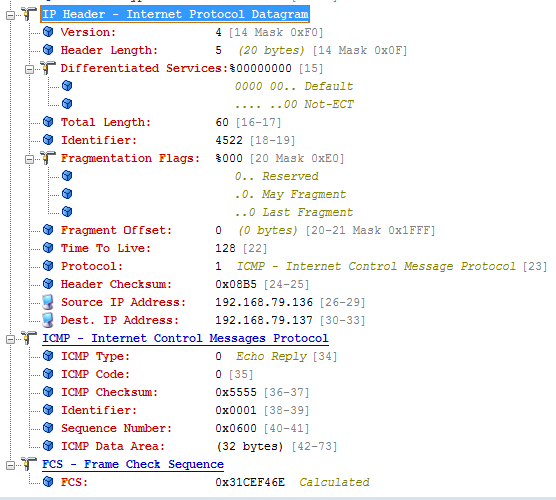
Il y a un espace d’octets vides additionnels (extra bytes) à la fin de la trame ARP.

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.**





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 :

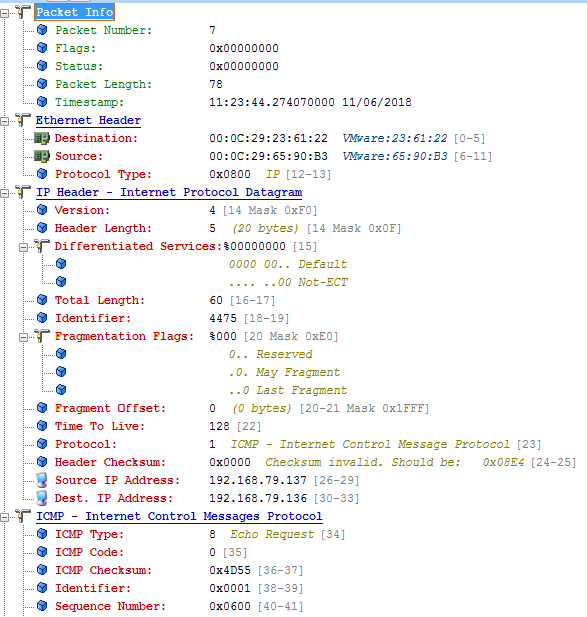


**10.3.**



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

**10.4.**



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 |

