



INF3405 – Réseaux informatiques

Automne 2019

TP 2 : analyseur de protocoles

Groupe 3

2038408 – Clément Prime

1879536 – Jacob Dorais

Soumis à : Bilal Itani

18 Novembre 2019

Introduction

L'objectif de ce laboratoire était de comprendre les divers types de paquets qui circulent dans un réseau, de visualiser l'encapsulation des données et d'analyser des échanges réseaux. Pour cela nous avons dû préparer un environnement de travail composé de client virtuel. On retrouve dans les images 1, 2 et 3 des captures d'écran de notre travail. On y retrouve un client A virtuel avec l'adresse IP 192.168.226.136 et un client virtuel B avec l'adresse IP 192.168.226.137. La commande *ipconfig* nous donne de plus les informations suivantes :

Poste	Client A	Client B
Adresse IPv4	192.168.226.136	192.168.226.137
Adresse MAC	00-0C-29-33-4F-FF	00-0C-29-5F-F9-9 ^E
Masque de sous-réseau	255.255.255.0	255.255.255.0
Passerelle par défaut	192.168.226.2	192.168.226.3

Tableau 1. Information sur les clients A et B

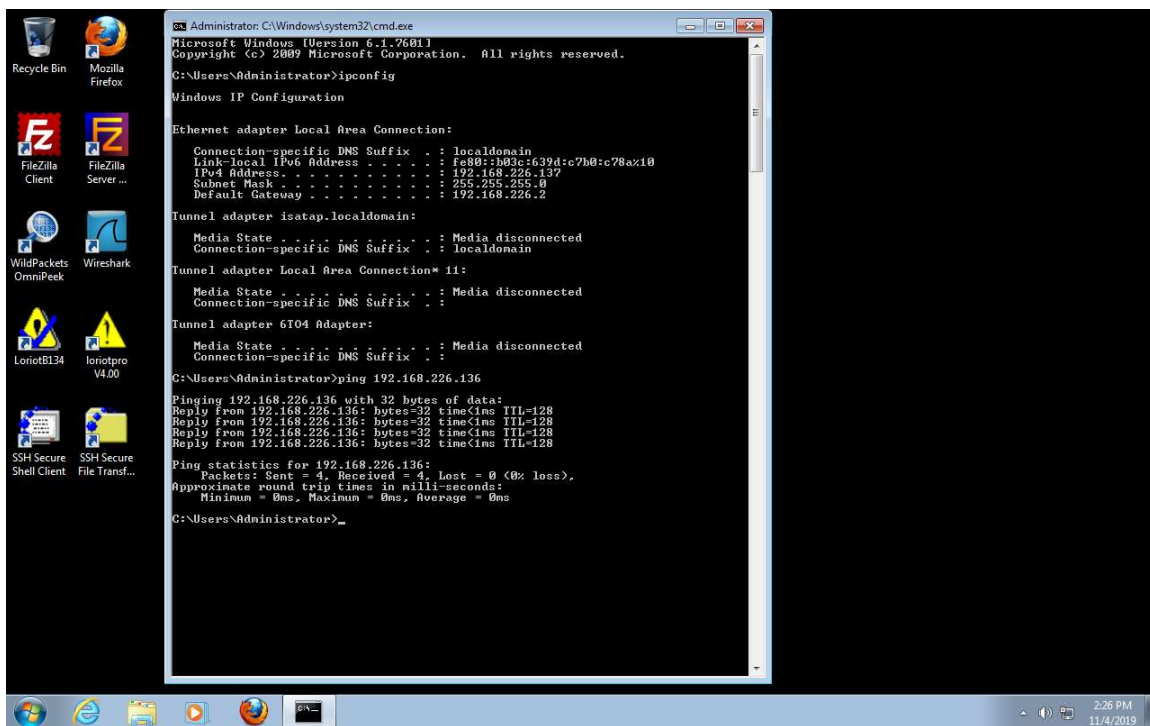


Image 1. Ping du client B vers le client A

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : test-PC
Primary Dns Suffix . . . . . : localdomain
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-29-33-4F-FF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::bd0d:726f:7186:56ed%10(Preferred)
IPv4 Address. . . . . : 192.168.226.136(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 04, 2019 2:22:19 PM
Lease Expires . . . . . : Monday, November 04, 2019 2:53:04 PM
Default Gateway . . . . . : 192.168.226.2
DHCP Server . . . . . : 192.168.226.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90

DNS Servers . . . . . : 192.168.226.2
Primary WINS Server . . . . . : 192.168.226.2
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 . : localdomain
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 . : localdomain
Description . . . . . : Microsoft 6t04 Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```

Windows could not activate
Click this message to find out more.

2:31 PM
11/4/2019

Image 2. *Ipconfig* du client A

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : test-PC
Primary Dns Suffix . . . . . : localdomain
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-29-33-4F-9E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b03c:639d:c7b0:c78a%10(Preferred)
IPv4 Address. . . . . : 192.168.226.137(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 04, 2019 2:23:59 PM
Lease Expires . . . . . : Monday, November 04, 2019 2:54:44 PM
Default Gateway . . . . . : 192.168.226.2
DHCP Server . . . . . : 192.168.226.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-BF-D5-2A-00-0C-29-66-D9-90

DNS Servers . . . . . : 192.168.226.2
Primary WINS Server . . . . . : 192.168.226.2
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 . : localdomain
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 . : localdomain
Description . . . . . : Microsoft 6t04 Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Administrator>
```

2:29 PM
11/4/2019

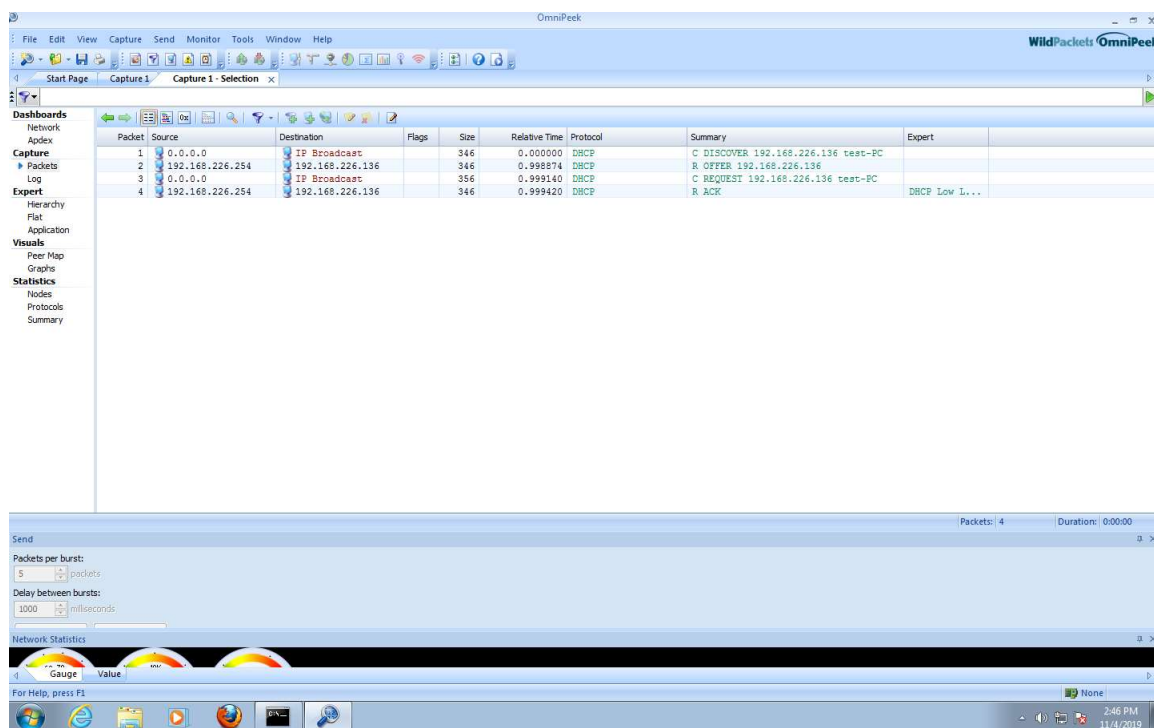
Image 3. *Ipconfig* du client B

Par la suite, on va utiliser l'analyseur de protocoles Omnipeek pour analyser la transmission de différents messages sur le réseau.

A. Partie DHCP

Question 1 :

Tout d'abord, on va analyser une communication DHCP. Pour cela, on effectue une commande permettant la demande d'une nouvelle adresse sur le réseau. Après avoir filtrer les paquets transmis via DHCP sur Omnipeek, on obtient le résultat de l'image 4.



Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
1	0.0.0.0	IP Broadcast		346	0.000000	DHCP	C DISCOVER 192.168.226.136 test-PC	
2	192.168.226.254	192.168.226.136		346	0.998974	DHCP	R OFFER 192.168.226.136	
3	0.0.0.0	IP Broadcast		356	0.999140	DHCP	C REQUEST 192.168.226.136 test-PC	
4	192.168.226.254	192.168.226.136		346	0.999420	DHCP	R ACK	DHCP Low I...

Image 4. Communication DHCP

Selon le résultat obtenu, l'attribution d'une nouvelle adresse IP à un client qui veut rejoindre un réseau se fait de la manière suivante :

- Le client envoie un paquet à tous les participants du réseau pour dire qu'il souhaite une nouvelle adresse.
- Le serveur répond à ce client en lui proposant une adresse IP et MAC libre.
- Le client informe tous les participants du réseau du choix de sa nouvelle adresse.
- Le serveur confirme alors la bonne réception du message.

Question 2 :

Les opérations effectuées en broadcast sont le DISCOVER et le REQUEST envoyés par le client. Ces opérations doivent être effectuées en broadcast car au début, le client ne connaît pas l'adresse du serveur, il doit envoyer son message à tout le réseau.

Question 3 :

Il est impossible d'utiliser le protocole TCP pour les requêtes DHCP car ces requêtes servent justement à configurer les paramètres TCP/IP au client.

Question 4 :

On retrouve plus en détail le message DISCOVER envoyé par le client sur les images 5, 6, 7 et 8.

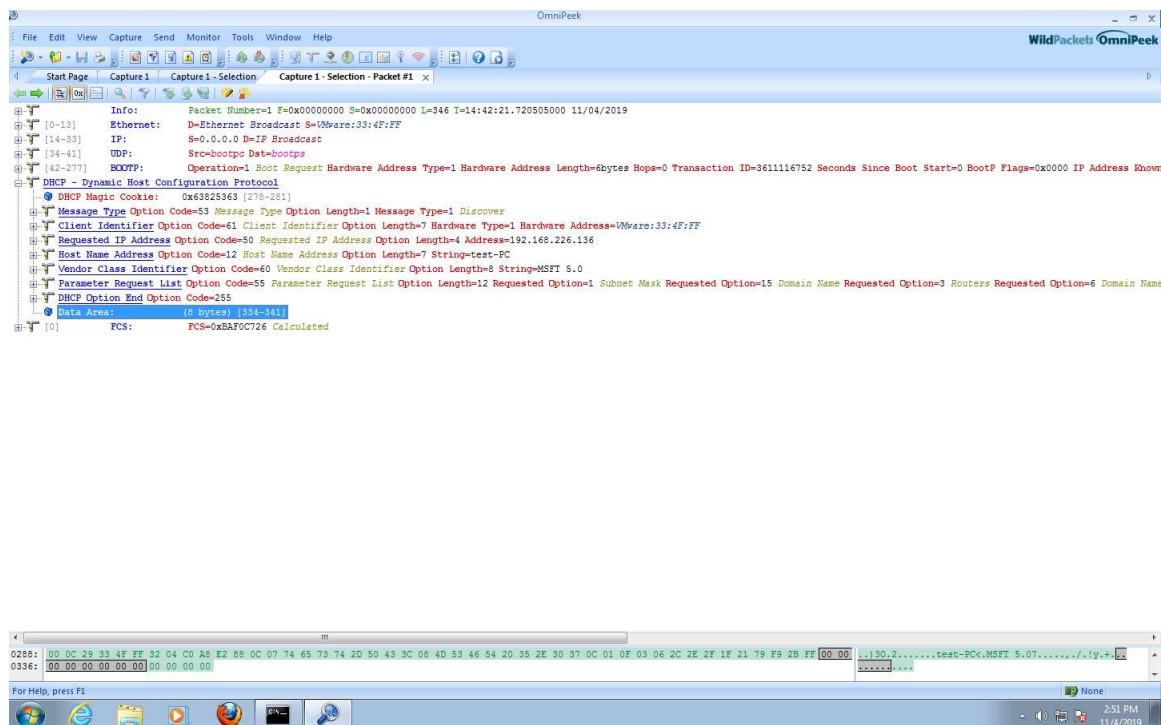
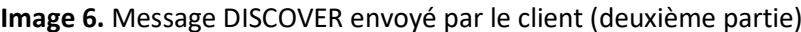


Image 5. Message DISCOVER envoyé par le client (première partie)



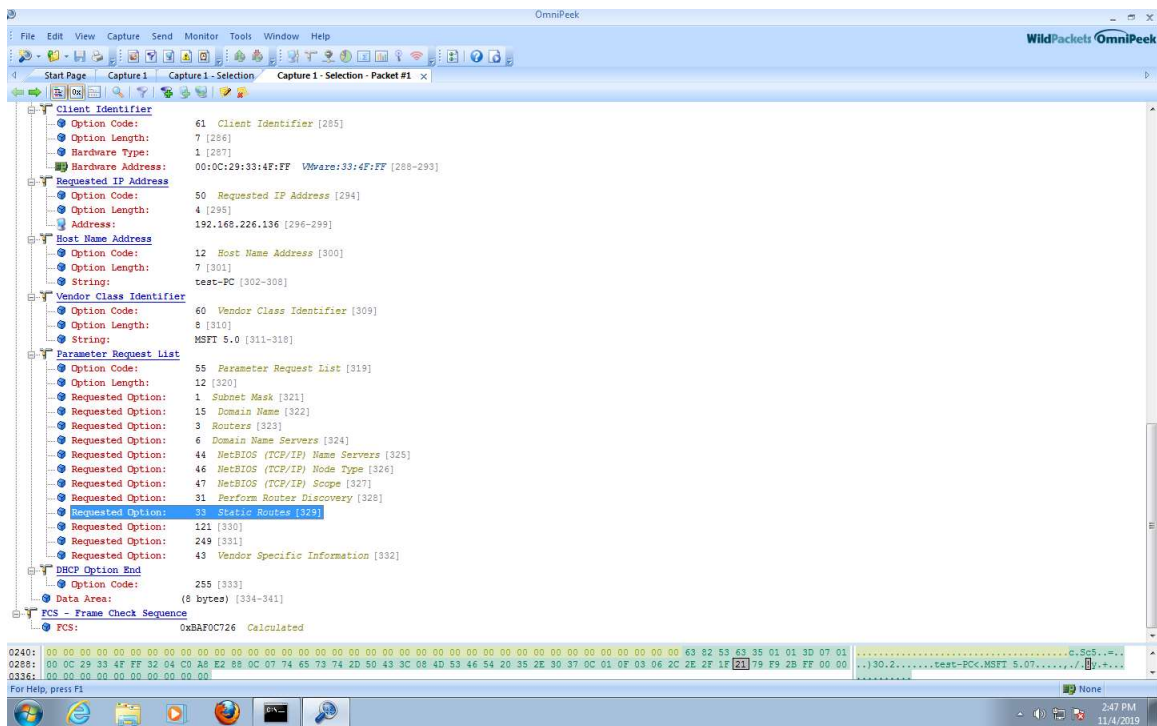


Image 8. Message DISCOVER envoyé par le client (quatrième partie)

Question 5 :

Sur les images 9, 10 et 11, on retrouve cette fois le message OFFER envoyé par le serveur.

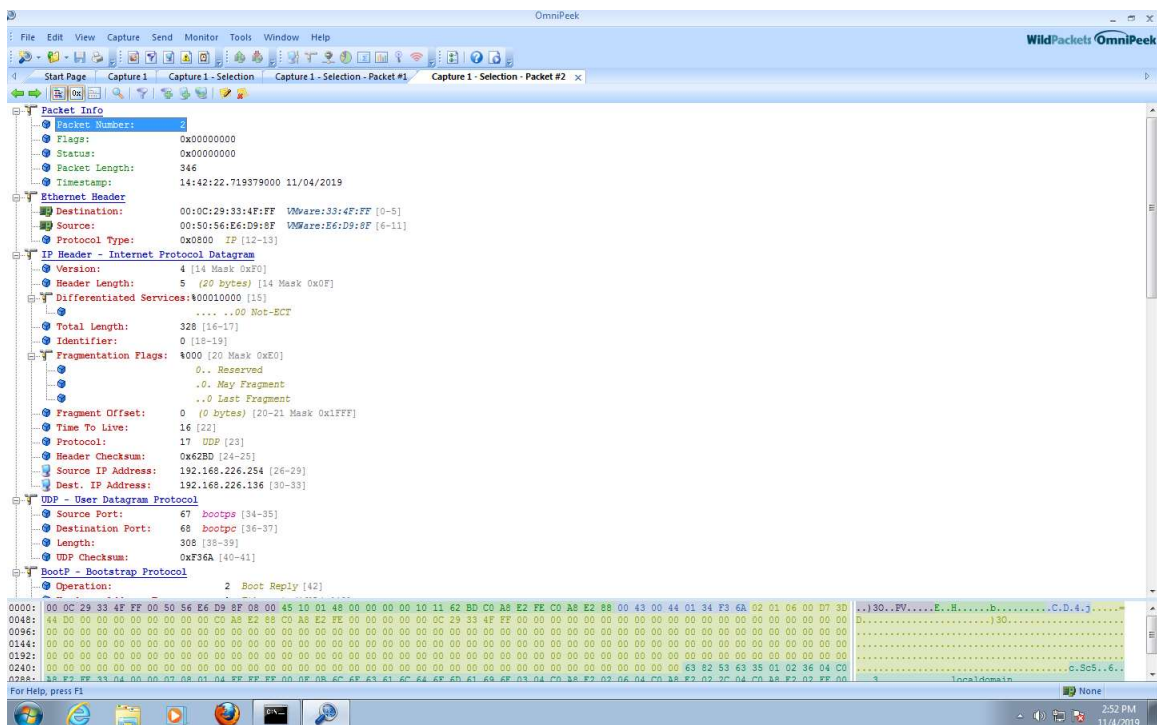


Image 9. Message OFFER envoyé par le serveur (première partie)

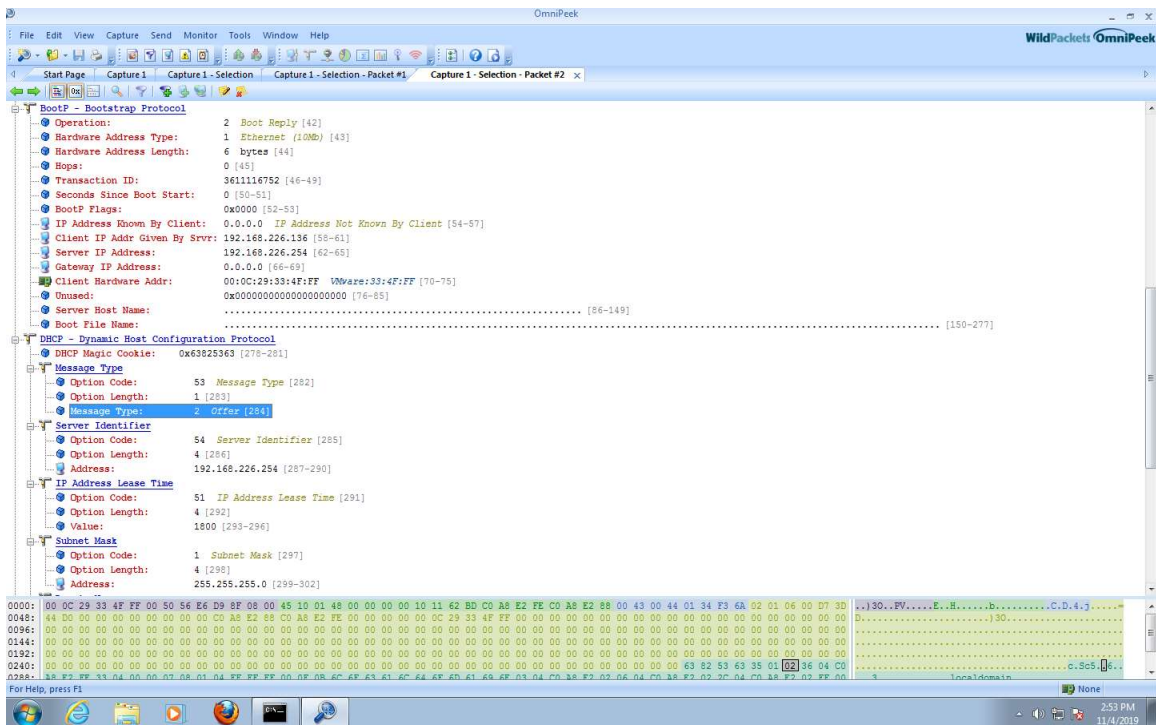


Image 10. Message OFFER envoyé par le serveur (deuxième partie)

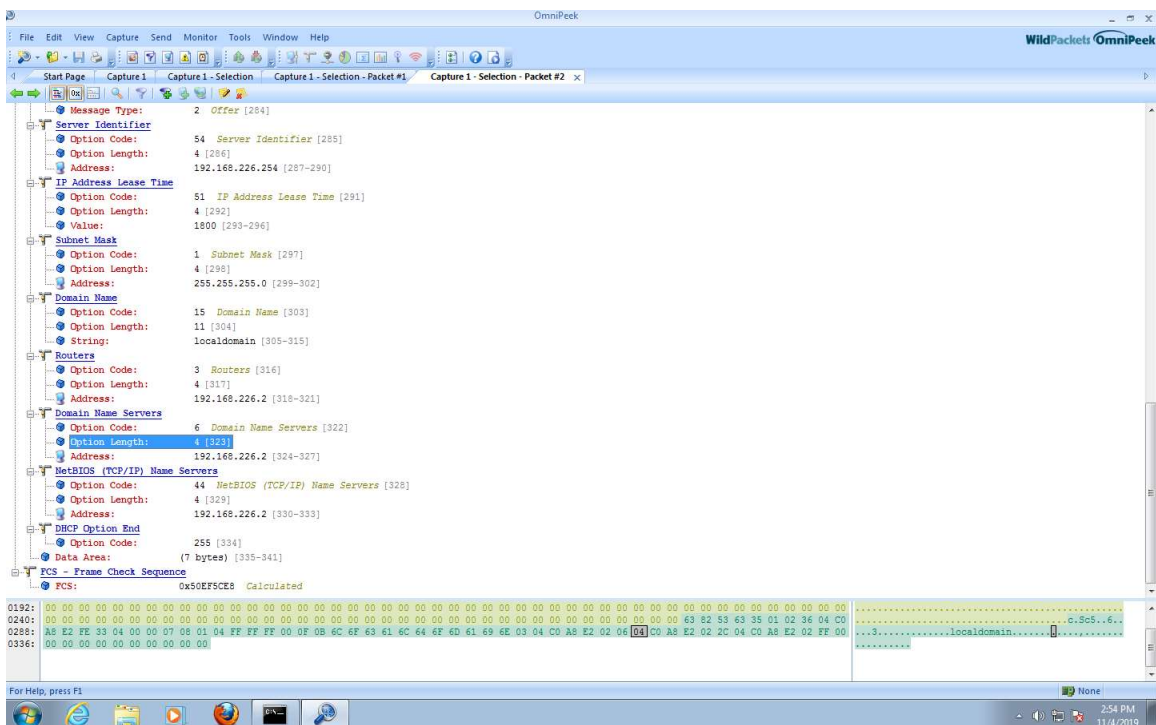


Image 11. Message OFFER envoyé par le serveur (troisième partie)

Le DHCP offer permet de proposer au client des paramètres TCP/IP. Ce paquet peut provenir de plusieurs serveurs.

Question 6 :

Le champ qui indique que le message est un DHCP offer est le « message type » qui indique alors la valeur 2.

Question 7 :

L'adresse MAC de la destination est celle du client et celle de la source est celle du routeur.

Question 8 :

L'adresse IP source est cependant celle du serveur.

Question 9 :

L'en-tête Ethernet fait ici 13 octets.

Question 10 :

La valeur du champ « Protocole Type » est 0x0800, cela signifie que le protocole utilisé est le protocole IP.

Question 11 :

Le champ « IP Address Lease Time » permet de définir le temps d'utilisation de l'adresse IP par le client. Cela est nécessaire pour ne pas se retrouver à cours d'adresse IP disponible.

Question 12 :

Le champ « Client IP Addr Given By Svr » correspond à une adresse IP disponible qui sera proposée au client.

Question 13 :

L'en-tête suivante de la trame est le Protocol IP.

Question 14 :

Sa taille est de 19 octets.

Question 15 :

L'en-tête suivante de la trame est le Protocol UDP.

Question 16 :

Sa taille est de 7 octets.

Question 17 :

Le Lease Time étant de 1800 secondes, le client devra revalider son adresse IP au bout de 30 minute.

B. Partie ARP

Question 1 :

La cache ARP est une table qui associe les adresses IPv4 avec les adresses MAC des machines connues. Il est important pour les machines de connaître les adresses MAC des autres machines, car c'est avec ceux-ci qu'elles vont communiquer. Il faut donc savoir leurs adresses IP si elles se trouvent dans le même réseau.

Question 2 :

Pour analyser la partie ARP, on doit d'abord supprimer l'adresse MAC du client B au niveau du client A. L'image 12 montre le résultat.

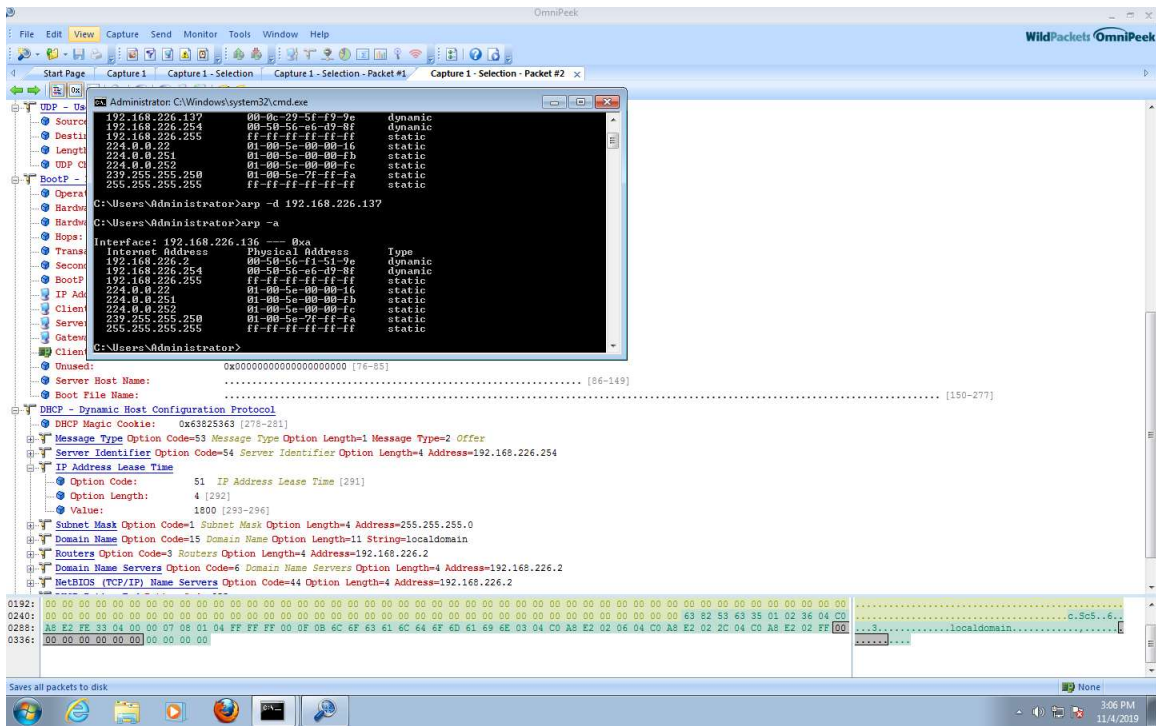


Image 12. Contenu de la cache ARP du client A après suppression de l'adresse MAC du client B

Question 3 :

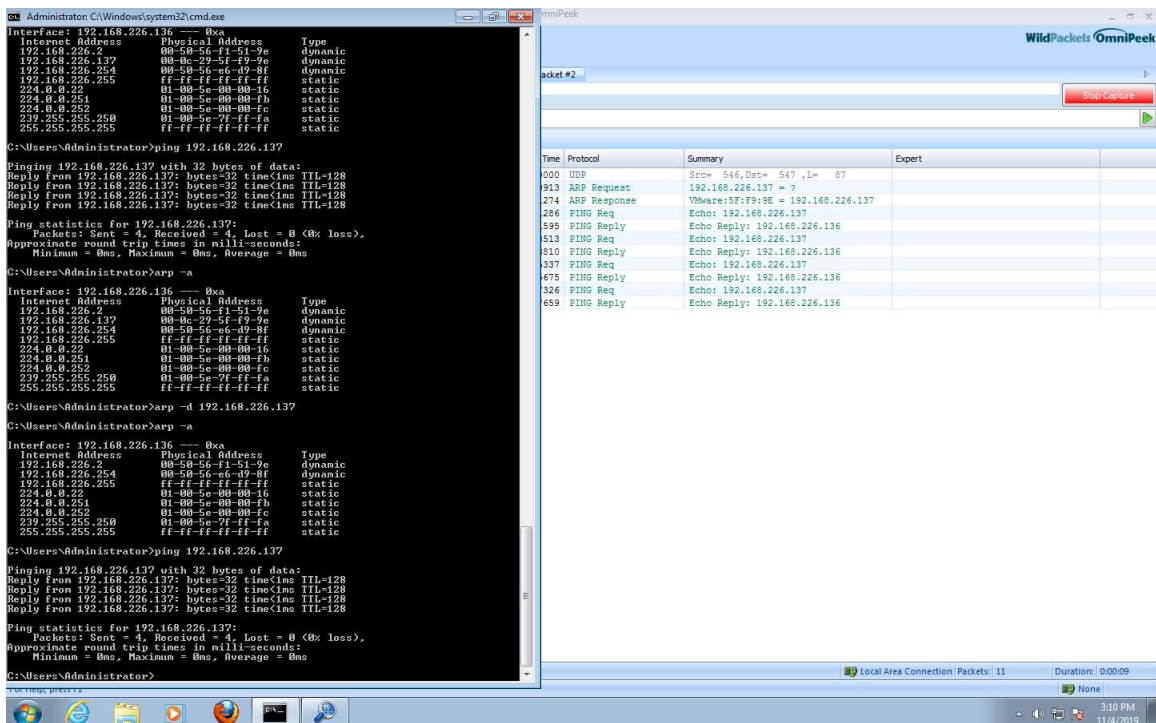
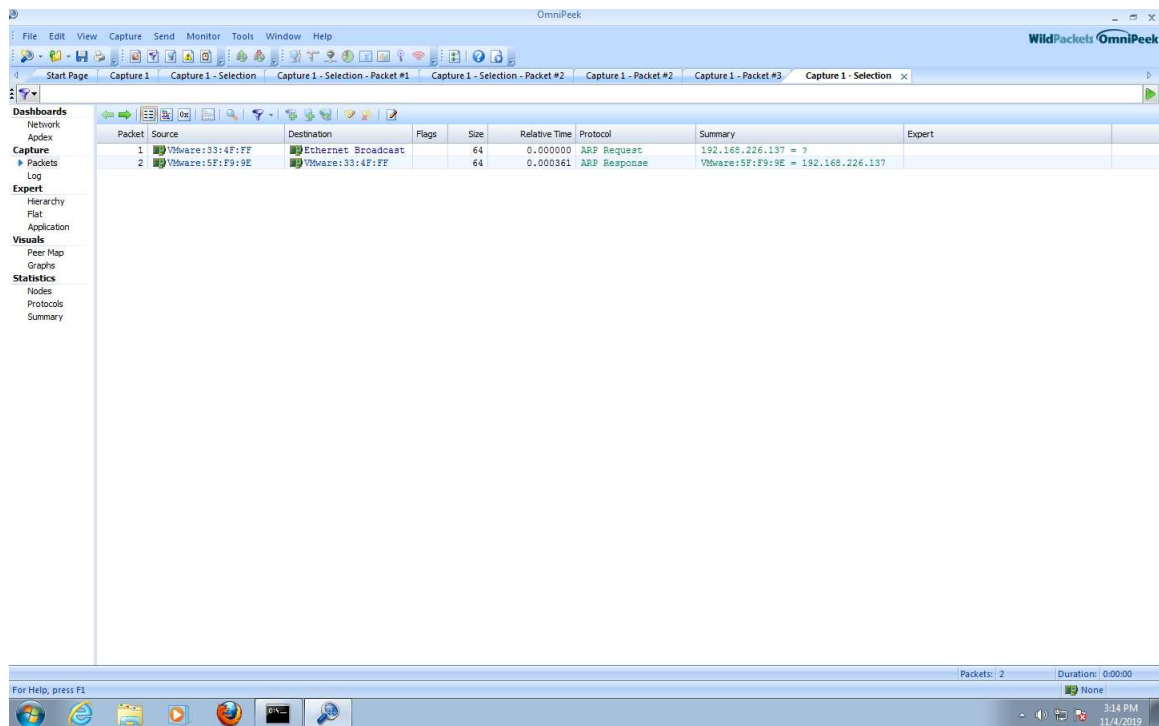


Image 13. Ping du client A vers le client B

Nous remarquons que la machine B (192.168.226.137) est présente dans notre table arp au début, ensuite nous la supprimons, elle n'est plus là et après un ping, elle réapparaît dans notre table.

Question 4 :



The screenshot shows the OmniPeek network analysis tool interface. The main window displays a list of captured packets. The first packet is an ARP Request from VMware:33:4F:FF to Ethernet Broadcast, with a size of 64 bytes and a relative time of 0.000000. The second packet is an ARP Response from VMware:5F:F9:9E to VMware:33:4F:FF, with a size of 64 bytes and a relative time of 0.000361. The summary column for the second packet shows 'VMware:5F:F9:9E = 192.168.226.137'. The left sidebar shows various dashboard options like Network, Apex, Capture, Packets, Log, Expert, Hierarchy, Flat, Application, Visuals, Peer Map, Graphs, Statistics, Nodes, Protocols, and Summary. The bottom status bar indicates 2 packets captured over a duration of 0:00:00.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
1	VMware:33:4F:FF	Ethernet Broadcast		64	0.000000	ARP Request	192.168.226.137 = ?	
2	VMware:5F:F9:9E	VMware:33:4F:FF		64	0.000361	ARP Response	VMware:5F:F9:9E = 192.168.226.137	

Image 14. Communication ARP entre le client A et le client B

La longueur des trames ARP est de 64 octets, c'est-à-dire, la longueur minimale des trames Ethernet.

Question 5 :

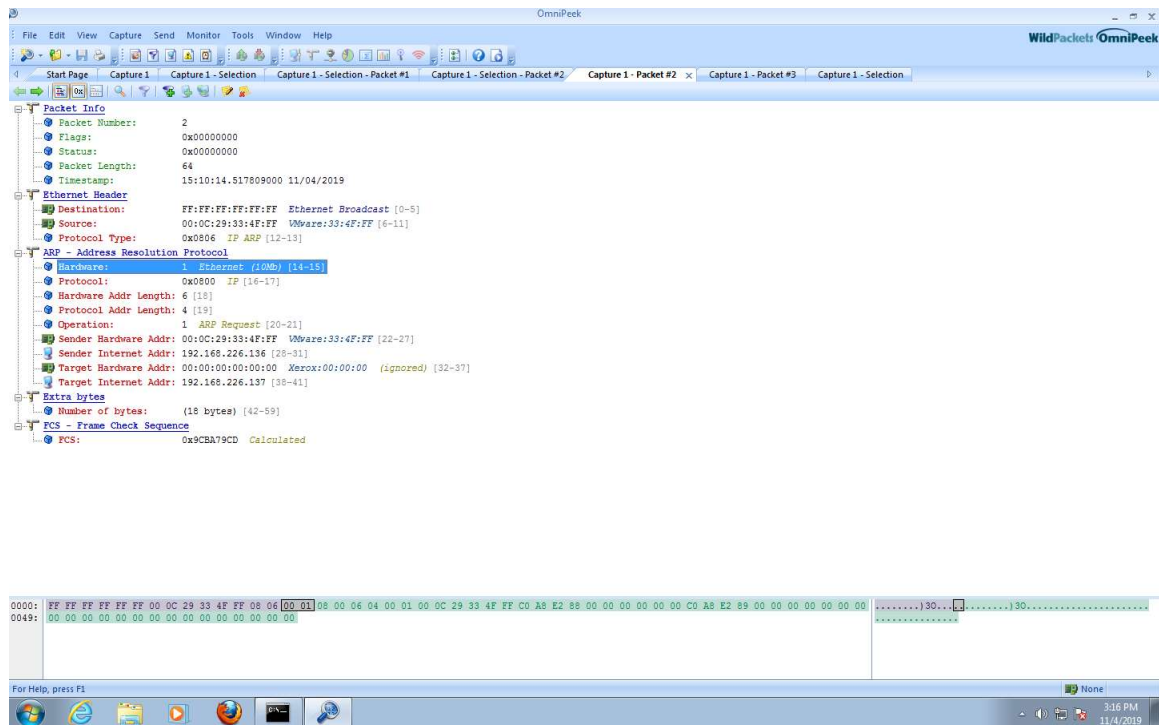


Image 15. ARP request

Le protocole type dans l'entête Ethernet est 0x806, qui signifie que c'est ARP. La valeur est de 2054 en décimale.

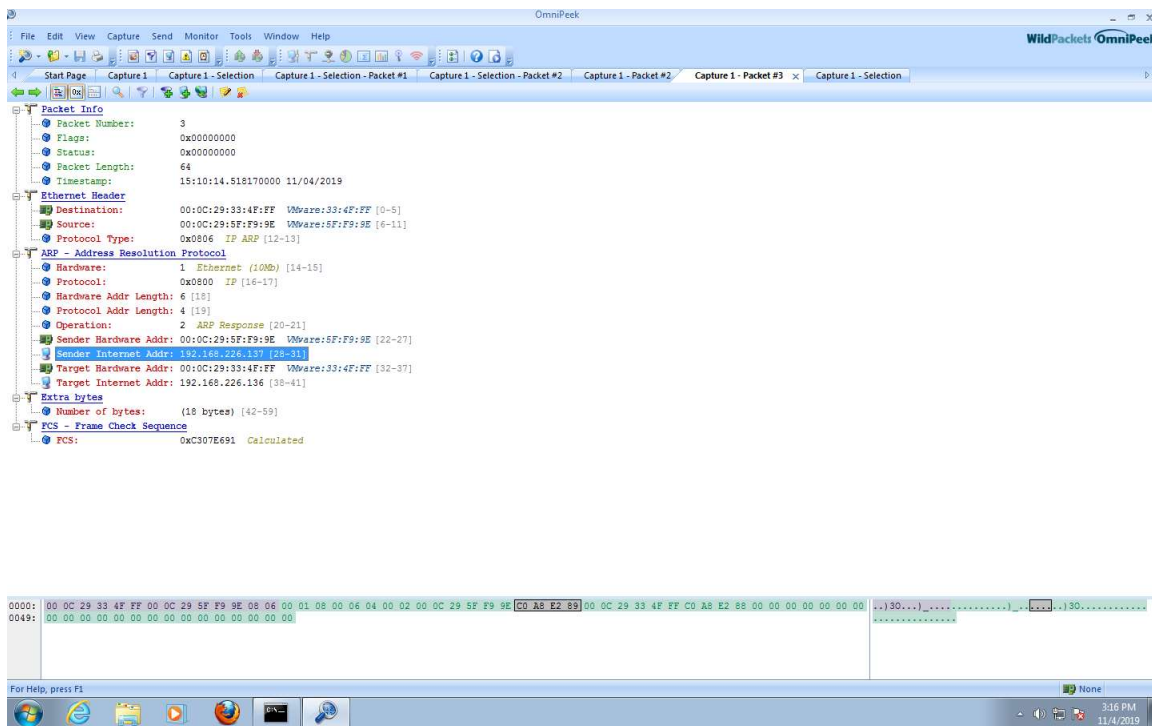


Image 16. ARP response

Question 6 :

La différence entre la requête ARP et la réponse ARP est que la requête est envoyée sur le broadcast, donc à tout le monde sur le réseau. La requête contient l'adresse IP destinée, ainsi les machines qui écoutent sur le réseau vérifient leur adresse IP et si c'est la même, elles envoient une réponse directement à la machine qui a envoyé la requête, car assurément son adresse MAC et son adresse IP fourni dans la requête.

Question 7 :

Dans la réponse, l'adresse MAC source (sender hardware address) est celle de la machine B, celle qui a envoyé la réponse.

Question 8 :

Dans la réponse, l'adresse MAC de destination (target hardware address) est celle de la machine A, à qui s'adresse la réponse.

Question 9 :

La séquence d'encapsulation est : Ethernet – ARP – data.

Question 10 :

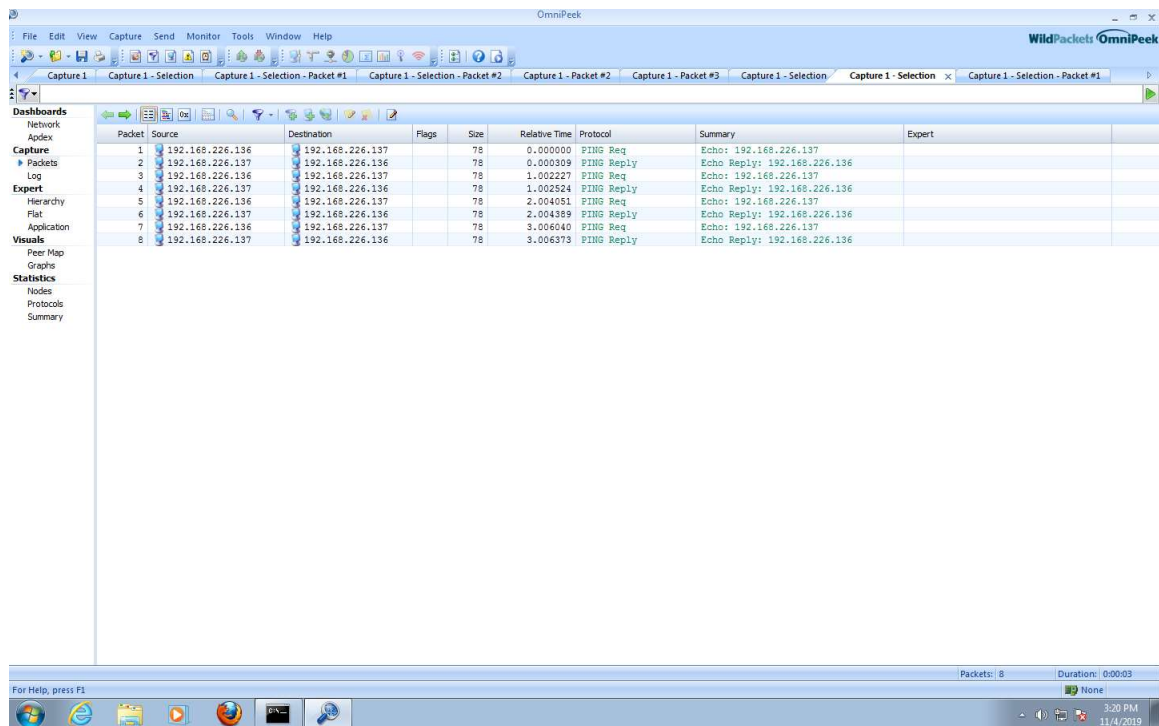
L'information recherchée par la requête ARP se trouve dans le champ sender hardware address de la réponse, car maintenant, dans notre cache arp on peut associer une adresse physique à l'adresse IP.

Question 11 :

Juste avant la séquence FCS, il y a 18 octets de données vides (à 0). ces octets représentent 28.12% de la trame. Ce champ est nécessaire, car il agit comme remplissage pour que la trame ait la taille de trame minimal de 64 octets. Effectivement, sans ces données vides, la trame ne serait que de 46 octets.

C. Partie PING

Question 1 :



The screenshot displays the WildPackets OmniPeek interface with a network capture of ICMP PING traffic. The main pane shows a list of 8 packets. The left sidebar contains navigation options like Dashboards, Network, Capture, Expert, Visuals, and Statistics. The bottom status bar indicates 8 packets captured over a duration of 0:00:03.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
1	192.168.226.136	192.168.226.137		78	0.000000	PING Req	Echo: 192.168.226.137	
2	192.168.226.137	192.168.226.136		78	0.000309	PING Reply	Echo Reply: 192.168.226.136	
3	192.168.226.136	192.168.226.137		78	1.002227	PING Req	Echo: 192.168.226.137	
4	192.168.226.137	192.168.226.136		78	1.002524	PING Reply	Echo Reply: 192.168.226.136	
5	192.168.226.136	192.168.226.137		78	2.004051	PING Req	Echo: 192.168.226.137	
6	192.168.226.137	192.168.226.136		78	2.004359	PING Reply	Echo Reply: 192.168.226.136	
7	192.168.226.136	192.168.226.137		78	3.006040	PING Req	Echo: 192.168.226.137	
8	192.168.226.137	192.168.226.136		78	3.006373	PING Reply	Echo Reply: 192.168.226.136	

Image 17. Communication ICMP entre le client A et le client B

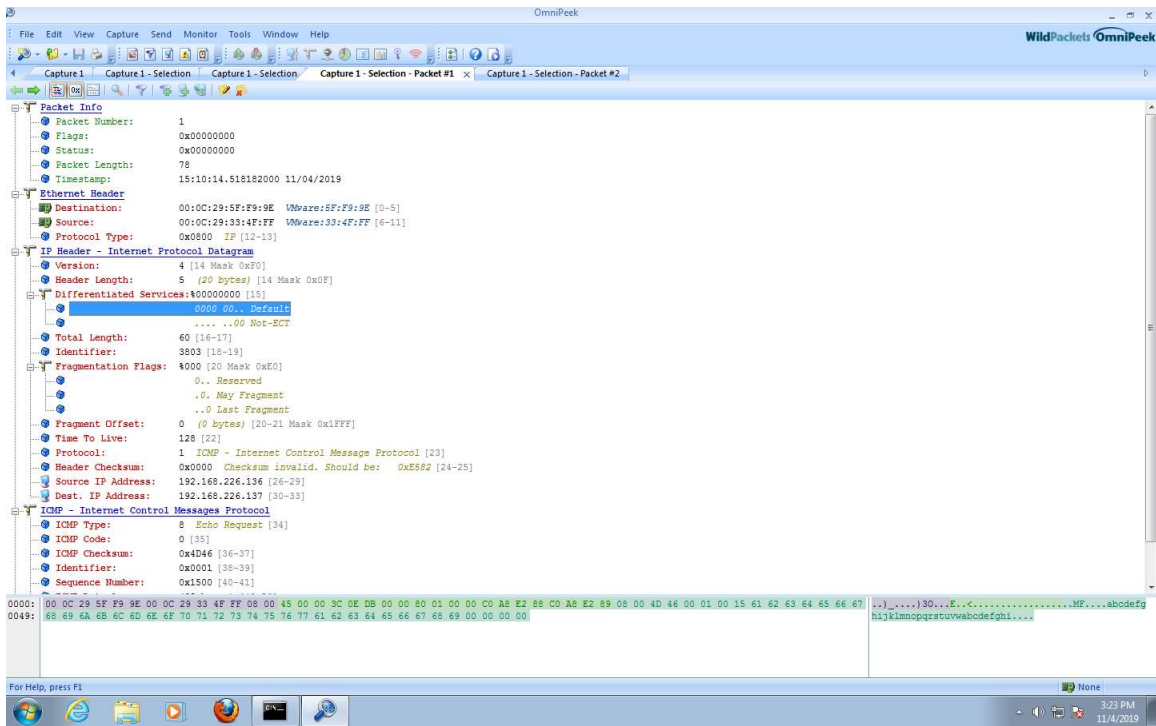


Image 18. Requête ICMP (partie 1)

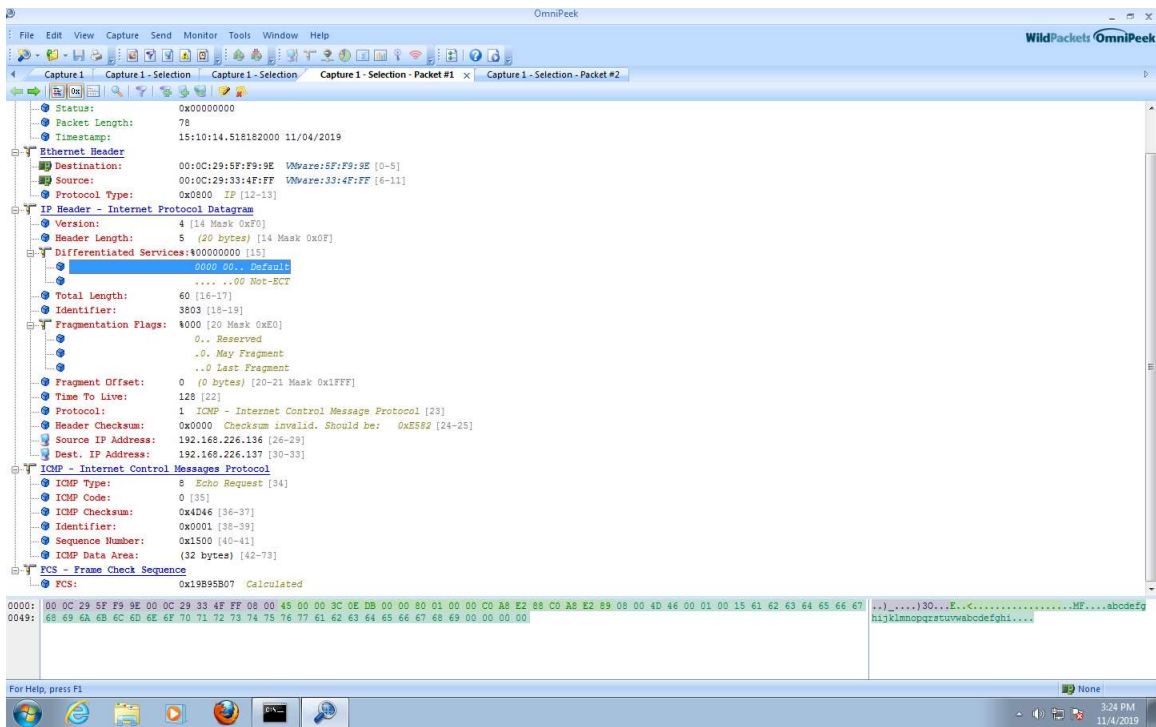


Image 19. Requête ICMP (partie 2)

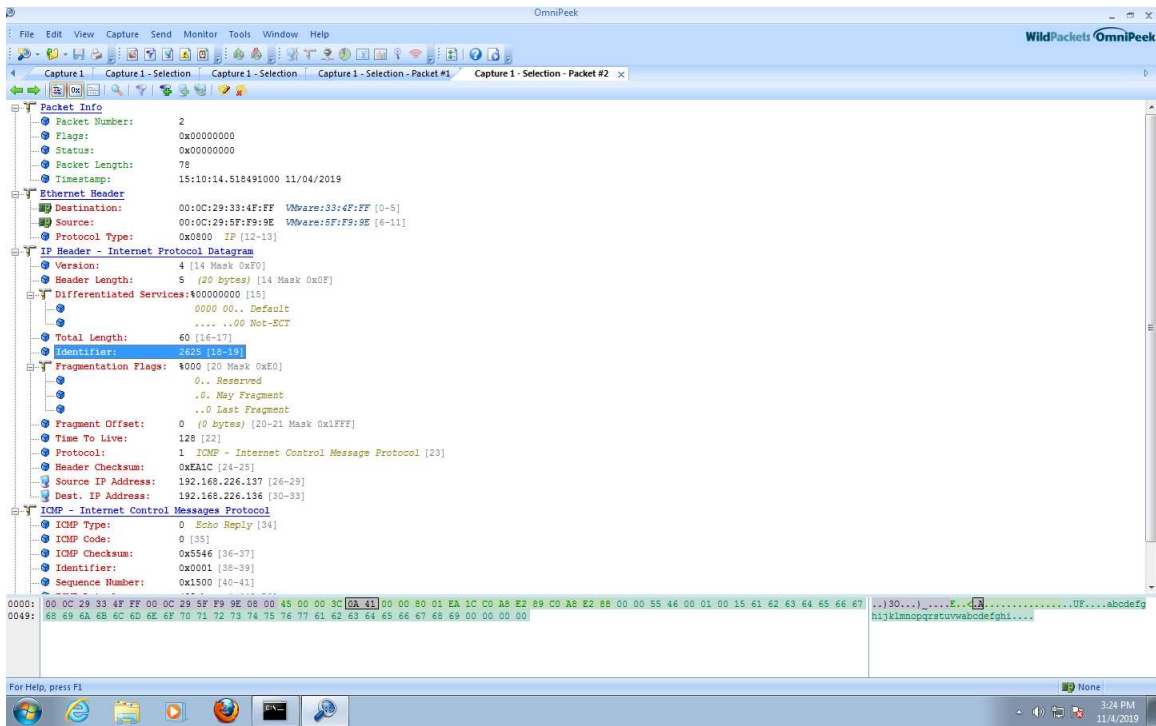


Image 20. Requête ICMP (partie 3)

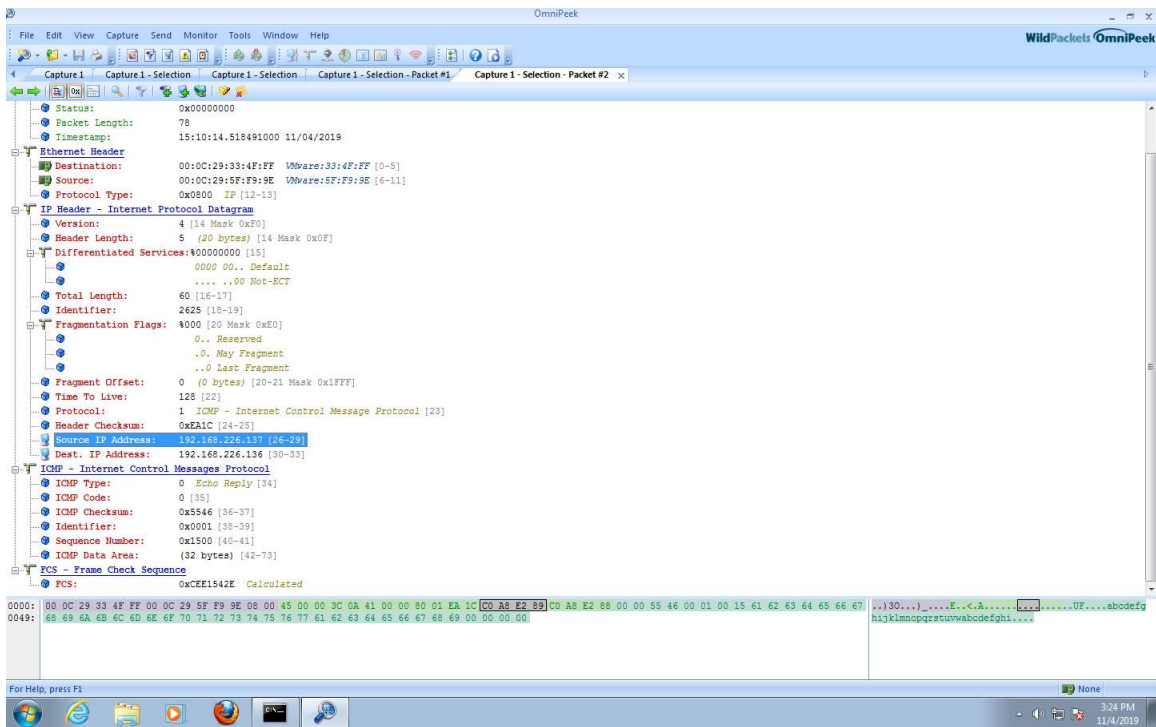


Image 21. Requête ICMP (partie 4)

Ce qui différencie le ping des autres requêtes dans l'entête ICMP est le champ ICMP Type qui est à 8 pour les requêtes ping et à 0 pour les réponses ping.

Question 2 :

La version IP du protocole est la version 4, comme indiqué dans l'entête IP sous le champ « version ».

Question 3 :

La valeur du champs TTL est à 128. Ce champ sert à éviter d'être envoyé en boucles si il y a des cycles dans le réseautage. La manière dont il fonctionne est qu'il est d'abord mis à une valeur par défaut. Celle-ci change en fonction de l'implémentation, mais on retrouve souvent 128 ou 255. Lorsque le message parvient à une machine, un commutateur par exemple, il diminue la valeur de 1, dans notre cas, elle serait passé de 128 à 127 et le ré-envoie. Donc, c'est le nombre maximal de nœud que le message perd traverser.

Question 4 :

La séquence d'encapsulation est : Ethernet – IP – ICMP.

D. Partie théorique

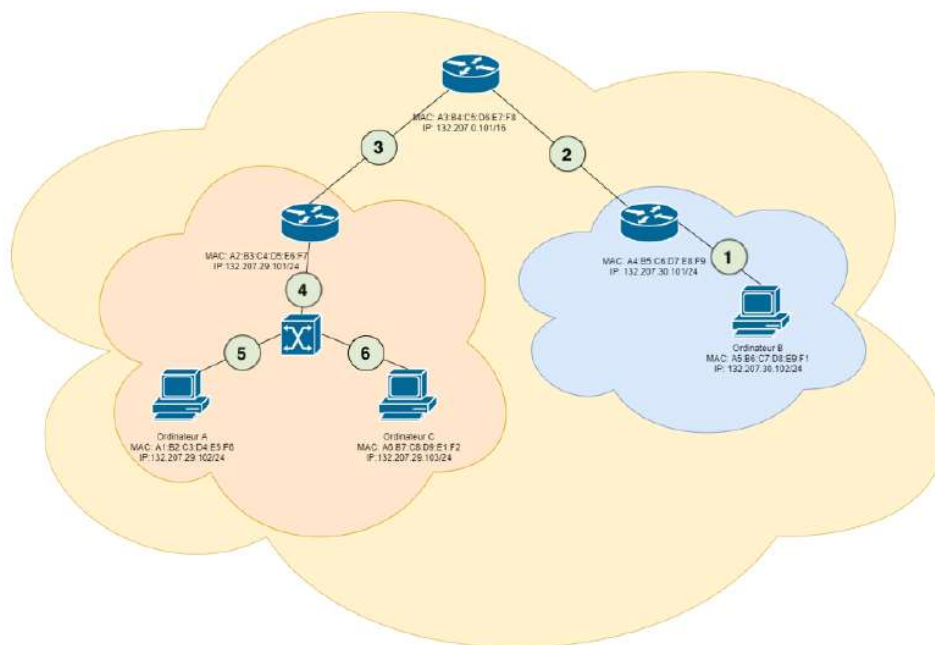


Image 22. Schéma d'une configuration réseau quelconque

Question 1 :

Pour les liens 4-5 et 6, ce sera pareil, car les répéteurs ne font que répéter les messages tels qu'ils le sont.

MAC destination : A6-B7-C8-D9-E1-F2

MAC source : A1-B2-C3-D4-E5-F6

ip source : 132.207.29.102

ip destination : 132.207.29.103

Question 2 :

Dans cette situation, on trouve les résultats suivants.

- lien 5 et 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

conclusion

Nous avons d'abord créé un environnement de travail virtuel avec deux machines dans le même sous-réseau, nous avons testé et compris les requêtes DHCP, ping, ARP à l'aide du logiciel omnipeek qui nous a permis d'analyser tous les paquets entrant et sortant. Cela nous a permis de mieux comprendre l'encapsulation des paquets des différentes requêtes.