POLYTECHNIQUE MONTRÉAL

INF3405 - Réseaux Informatiques

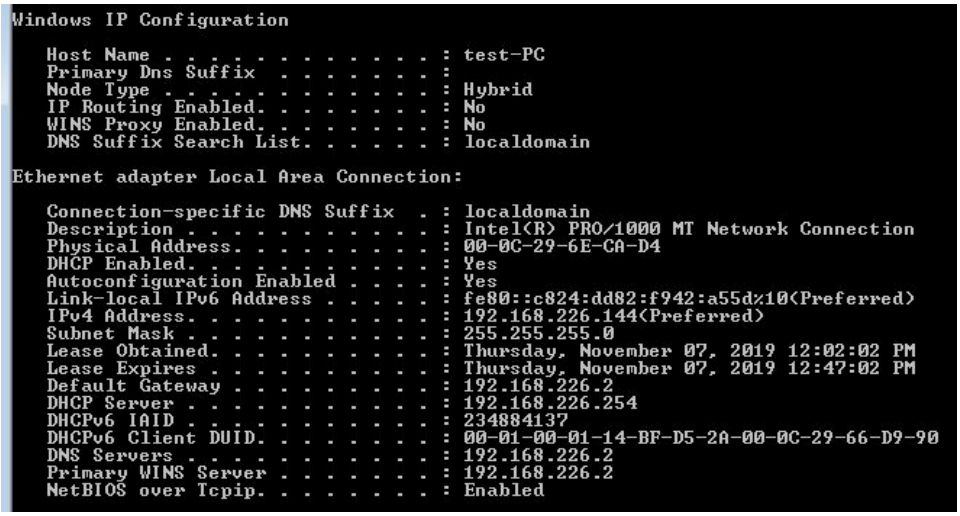
Travail pratique No 2

Analyseur de protocoles

Jeremy Boulet - 1896107
Duc-Thien Nguyen - 1878502

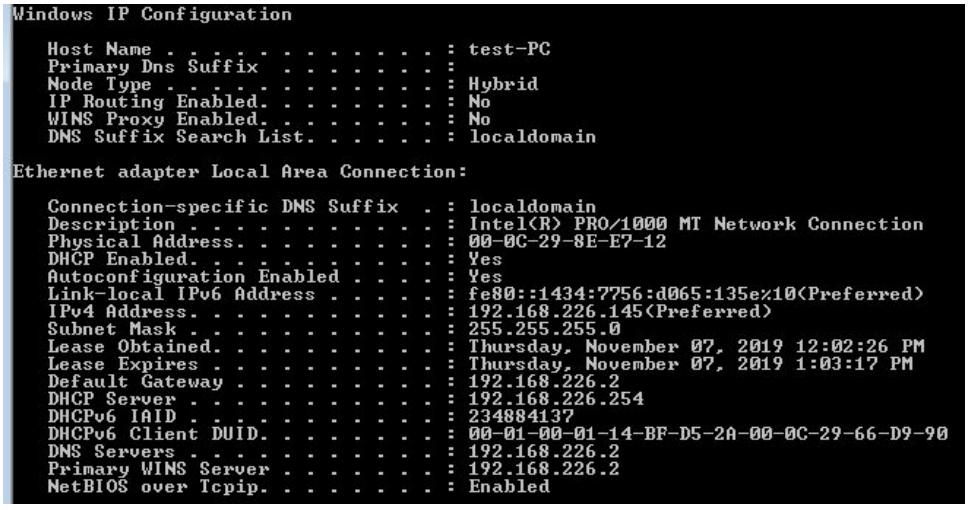
6.1

Windows7_A



Nom du poste: test-PC
IPV4: 192.168.226.144
Masque: 255.255.255.0
MAC: 00-0C-29-6E-CA-D4
Passerelle: 192.168.226.2

Windows7_B



Nom du poste: test-PC
IPV4: 192.168.226.145
Masque: 255.255.255.0
MAC: 00-0C-29-8E-E7-12
Passerelle: 192.168.226.2

Question 8

8.1

Lorsqu'un nous avons fait le "/release", nous avons manuellement enlevé l'adresse IP de la VM.

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary	Expert
82	0.0.0.0	IP Broadcast		346	0.000000	DHCP	C DISCOVER 192.168.226.144 test-PC	
83	192.168.226.254	192.168.226.144		346	0.000160	DHCP	R OFFER 192.168.226.144	
84	0.0.0.0	IP Broadcast		356	0.000386	DHCP	C REQUEST 192.168.226.144 test-PC	
85	192.168.226.254	192.168.226.144		346	0.000559	DHCP	R ACK	DHCP Low Lease Time (30
127	192.168.226.1	192.168.226.254		364	2.603474	DHCP	C REQUEST L4708-12	
128	192.168.226.254	192.168.226.1		346	2.603593	DHCP	R ACK	DHCP Low Lease Time (30

En faisant "/renew", le DHCP client fait un broadcast DISCOVER vers un serveur DHCP pour la demande de paramètre TCP/IP. Ensuite, le serveur DHCP fait un unicast OFFER vers le client pour proposer les paramètres TCP/IP. Le client va ensuite fait un broadcast REQUEST vers le serveur qui contient l'acceptation d'une proposition et par défaut, va refuser le reste des propositions. Enfin, le serveur fait un unicast ACKNOWLEDGE des paramètres TCP/IP au client complétant la séquence.

8.2

Ce sont les observations, nous pouvons voir que les requête DISCOVER et REQUEST sont faites en broadcast. Certaines doivent être en broadcast, car le client veut envoyer une demande à tous les serveurs DHCP potentiel.

8.3

Il est impossible d'utiliser les TCP, car les DHCP utilise UDP au lieu puisque la communication est faite sans une connection. Avec TCP, il doit avoir une connection établie en premier lieu pour ensuite faire les communication.

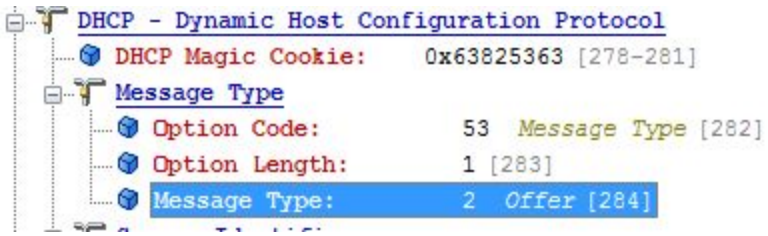
8.4

Séquence: Ethernet - IP - UDP - BootP - DHCP - FCS

8.5

Le rôle de la trame DHCP Offer est de donner au client l'adresse Ip à être assigné avec et un bail pour sa durée d'utilisation.

8.6



Dans le champ de Message Type -> Message Type -> 2 [Offer]

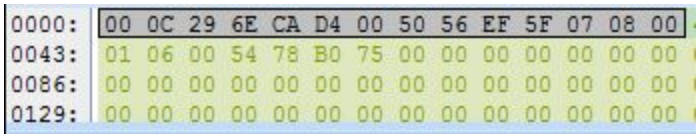
8.7

Destination: Le poste Windows7_A
Source: Le poste qui assigne l'adresse IP

8.8

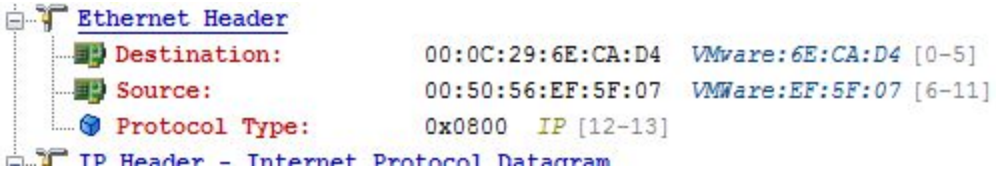
La machine qui assigne l'adresse IP: 192.168.226.254

8.9



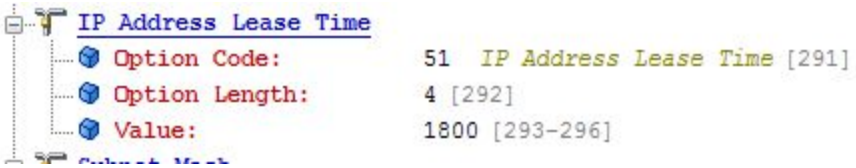
La taille est de 14 Octets

8.10



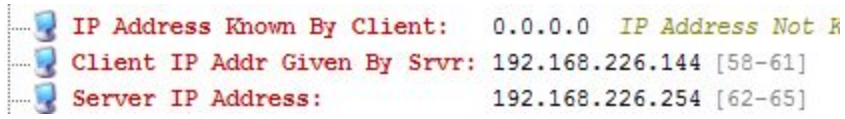
La valeur du protocole est: 0x0800, cela signifie que nous travaillons avec une adresse IP

8.11



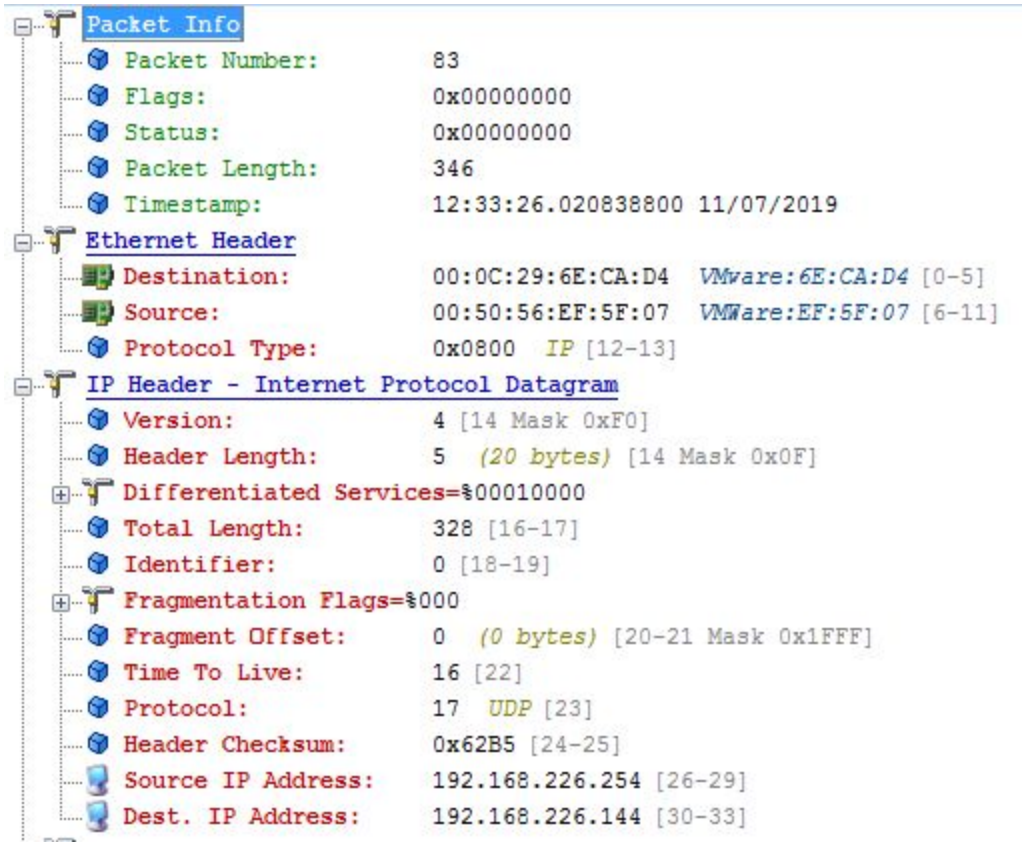
Ça signifie la durée du baille de l'adresse IP dans notre cas:
Value: 1800

8.12



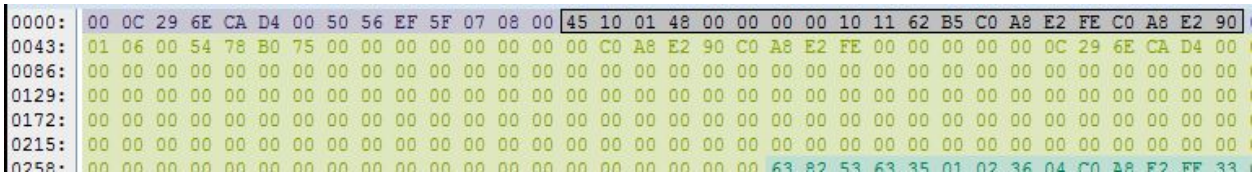
C'est l'adresse IP que le DCHP serveur donne à son client: 192.168.226.144

8.13



Niveau 3: IP Header - Internet Protocol Datagramme

8.14

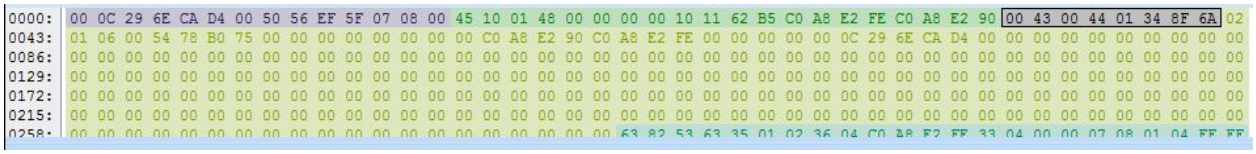


Taille: 20 octets

8.15

Niveau 4: UDP - User Datagram Protocol

8.16



Taille: 8 octets

8.17

1800

Question 9

9.1

La ARP cache est utilisé pour garder en mémoire les liens entre les adresses MAC et les adresses IP.

9.2

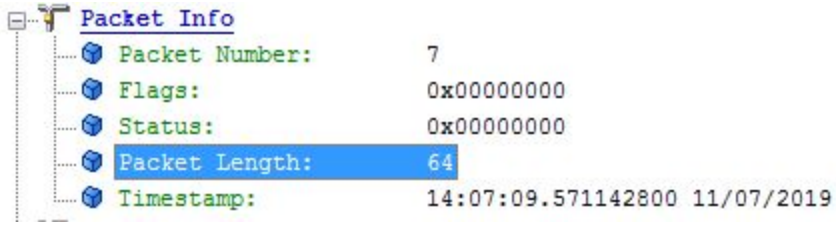
```
C:\Users\Administrator>arp -a

Interface: 192.168.226.144 --- 0xa
  Internet Address      Physical Address      Type
  192.168.226.2         00-50-56-f1-51-9e     dynamic
  192.168.226.145       00-0c-29-8e-e7-12     dynamic
  192.168.226.254       00-50-56-ef-5f-07     dynamic
  192.168.226.255       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 192.168.226.145

C:\Users\Administrator>arp -a

Interface: 192.168.226.144 --- 0xa
  Internet Address      Physical Address      Type
  192.168.226.2         00-50-56-f1-51-9e     dynamic
  192.168.226.254       00-50-56-ef-5f-07     dynamic
  192.168.226.255       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

Packet	Source	Destination	Flags	Size	Relative Time	Protocol	Summary
1	VMware:6E:CA:D4	VMWare:F1:51:9E		64	0.000000	ARP Request	192.168.226.2 = ?
2	VMWare:F1:51:9E	VMware:6E:CA:D4		64	0.000189	ARP Response	VMWare:F1:51:9E = 192.168.226.2
3	VMware:6E:CA:D4	Ethernet Broadcast		64	28.073414	ARP Request	192.168.226.145 = ?
4	VMware:8E:E7:12	VMware:6E:CA:D4		64	28.073677	ARP Response	VMware:8E:E7:12 = 192.168.226.145
5	VMware:6E:CA:D4	VMware:8E:E7:12		64	35.999987	ARP Request	192.168.226.145 = ?
6	VMware:8E:E7:12	VMware:6E:CA:D4		64	36.000260	ARP Response	VMware:8E:E7:12 = 192.168.226.145
7	VMware:6E:CA:D4	Ethernet Broadcast		64	0:01:07.183365	ARP Request	192.168.226.145 = ?
8	VMware:8E:E7:12	VMware:6E:CA:D4		64	0:01:07.183730	ARP Response	VMware:8E:E7:12 = 192.168.226.145
9	VMware:8E:E7:12	VMware:6E:CA:D4		64	0:01:11.969096	ARP Request	192.168.226.144 = ?
10	VMware:6E:CA:D4	VMware:8E:E7:12		64	0:01:11.969163	ARP Response	VMware:6E:CA:D4 = 192.168.226.144
11	VMware:6E:CA:D4	Ethernet Broadcast		64	0:01:55.460144	ARP Request	192.168.226.2 = ?
12	VMWare:F1:51:9E	VMware:6E:CA:D4		64	0:01:55.460296	ARP Response	VMWare:F1:51:9E = 192.168.226.2

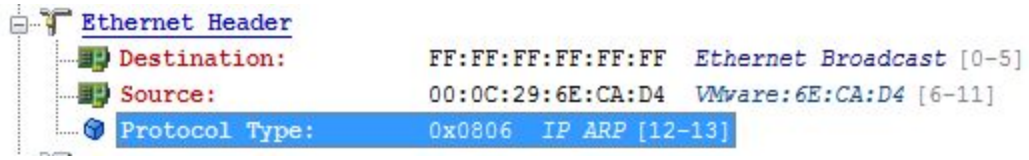
Même après avoir supprimer le IP de Windows7_B de Windows7_A, lorsque nous faisons ping, l'IP de B apparaît dans le ARP de A.

9.4



Taille: 64 octets

9.5

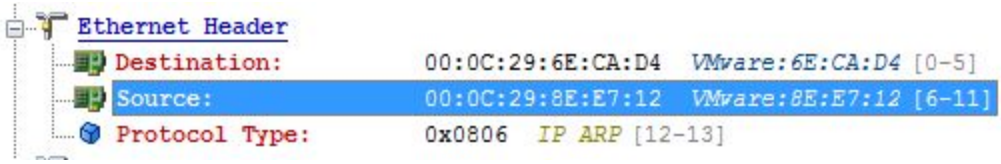


Valeur: 0x0806, ce qui signifie IP ARP

9.6

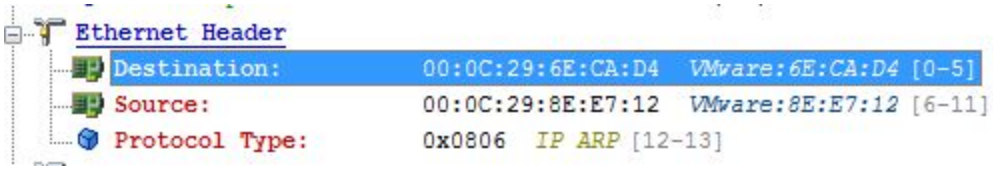
Le champs Operation pour une requête a une valeur de 1, tandis que pour une réponse, la valeur est 2.

9.7



C'est l'adresse Mac de Windows7_B.

9.8



C'est l'adresse Mac de Windows7_A.

9.9

Séquence: Ethernet - ARP - Data - FCS

9.10

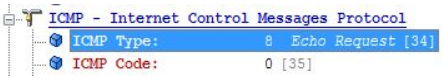
Le champ **Target Hardware Address** contient l'adresse physique qui se trouve dans la réponse.

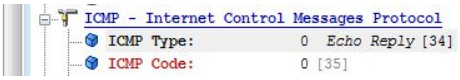
9.11

Puisque la réponse est trop petite, le trame n'est pas à 64 octets, alors il faut du padding pour pouvoir remplir l'espace disponible. Dans notre cas, le padding est de 18 octets de 64. Ceci qui correspond à environ 28% de la taille de la trame.

Question 10

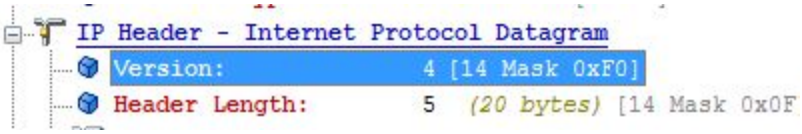
10.1





Le champs ICMP Type pour une requête a une valeur de 8, tandis que pour une réponse, la valeur est 0.

10.2



Version: 4

10.3

La valeur es 128. Elle sert à indiquer si un paquet a été sur un réseau pour une longue durée et celle-ci sera ignorée.

10.4

Séquence: Ethernet - IP - ICMP - FCS

Question 11

11.1

Puisque le répéteur ne change pas le message, l'état de l'entête sera le même pour les liens 4,5,6.

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

11.2

Pour liens 4 et 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	132.207.29.101

Pour lien 3

MAC Destination	A3:B4:C5:D6:E7:F8
MAC Source	A2:B3:C4:D5:E6:F7
IP source	132.207.29.101
IP destination	132.207.0.101

Pour lien 2

MAC Destination	A4:B5:C6:D7:E8:F9
MAC Source	A3:B4:C5:D6:E7:F8
IP source	132.207.0.101
IP destination	132.207.30.101

Pour lien 1

MAC Destination	A5:B6:C7:D8:E9:F1
MAC Source	A4:B5:C6:D7:E8:F9
IP source	132.207.30.101
IP destination	132.207.30.102