



# POLYTECHNIQUE MONTRÉAL

## LE GÉNIE EN PREMIÈRE CLASSE

Réseaux Informatiques  
INF3405

Laboratoire 3

**Présenté par:**

Ibrahima Séga Sangaré (1788085)

et

Khalil Benani (1566707)

**Soumis à:**

Bilal Itani

7.1 Exécutez la commande ipconfig /all dans une fenêtre de commande (Command Prompt) : Menu Démarrer (start), cmd pour le client et start, run cmd pour le serveur. Inscrivez le nom de votre poste, l'adresse IPv4, le masque de sous-réseau, l'adresse MAC, la passerelle par défaut pour vos deux systèmes virtuels. (0.5 pt)

|         | Nom du poste   | IPv4           | Masque        | Adresse Mac       | Passerelle par défaut |
|---------|----------------|----------------|---------------|-------------------|-----------------------|
| Client  | test-PC        | 192.168.44.99  | 255.255.255.0 | 00-0C-29-22-C2-E0 | 192.168.44.198        |
| Serveur | ServeurWindows | 192.168.44.205 | 255.255.255.0 | 00-0C-29-A6-08-42 | 192.168.44.198        |

8.1 Présentez une capture d'écran des paquets DHCP que vous avez capturés à l'aide de l'outil Omnipeek. À la lumière vos observations, expliquez en détail le mécanisme d'attribution d'une nouvelle adresse IP à un client qui veut se joindre à un réseau. (2 pts)

| Packet | Source         | Destination   | Flags | Size | Relative Time | Protocol | Summary                       |
|--------|----------------|---------------|-------|------|---------------|----------|-------------------------------|
| 1      | 192.168.44.213 | IP Broadcast  |       | 294  | 0.000000      | DHCP     | C INFORM                      |
| 2      | 192.168.44.205 | IP Broadcast  |       | 346  | 0.000289      | DHCP     | R ACK                         |
| 3      | 192.168.44.213 | IP Broadcast  |       | 346  | 0.000334      | DHCP     | R ACK                         |
| 4      | 192.168.44.218 | IP Broadcast  |       | 346  | 0.000335      | DHCP     | R ACK                         |
| 5      | 192.168.44.224 | IP Broadcast  |       | 346  | 0.000335      | DHCP     | R ACK                         |
| 6      | 192.168.44.202 | IP Broadcast  |       | 346  | 0.000336      | DHCP     | R ACK                         |
| 7      | 192.168.44.206 | IP Broadcast  |       | 346  | 0.000359      | DHCP     | R ACK                         |
| 8      | 192.168.44.4   | IP Broadcast  |       | 346  | 0.000369      | DHCP     | R ACK                         |
| 9      | 192.168.44.221 | IP Broadcast  |       | 346  | 0.000575      | DHCP     | R ACK                         |
| 10     | 192.168.44.223 | IP Broadcast  |       | 346  | 0.000650      | DHCP     | R ACK                         |
| 11     | 192.168.44.216 | IP Broadcast  |       | 346  | 0.000651      | DHCP     | R ACK                         |
| 12     | 192.168.44.217 | IP Broadcast  |       | 346  | 0.000651      | DHCP     | R ACK                         |
| 13     | 192.168.44.219 | IP Broadcast  |       | 346  | 0.000652      | DHCP     | R ACK                         |
| 14     | 192.168.44.227 | IP Broadcast  |       | 346  | 0.000670      | DHCP     | R ACK                         |
| 15     | 192.168.44.207 | IP Broadcast  |       | 346  | 0.000671      | DHCP     | R ACK                         |
| 16     | 192.168.44.215 | IP Broadcast  |       | 346  | 0.000672      | DHCP     | R ACK                         |
| 38     | 0.0.0.0        | IP Broadcast  |       | 346  | 11.701760     | DHCP     | C DISCOVER 192.168.44.99 test |
| 42     | 192.168.44.198 | 192.168.44.99 |       | 346  | 12.027979     | DHCP     | R OFFER 192.168.44.99         |
| 43     | 0.0.0.0        | IP Broadcast  |       | 356  | 12.028214     | DHCP     | C REQUEST 192.168.44.99 test  |
| 44     | 192.168.44.198 | 192.168.44.99 |       | 346  | 12.035419     | DHCP     | R ACK                         |

Pour attribuer une adresse IP au client lorsqu'il doit rejoindre le réseau, le client envoie un paquet DHCP DISCOVER au serveur. Le client a 0.0.0.0 comme adresse IP au départ. Le serveur lui répond en lui envoyant le message DHCP OFFER pour assigner une adresse IP non liée ainsi que des informations des configurations pour TCP et IP pour la passerelle par défaut et le masque de sous-réseau. Le client accepte le premier paquet qu'il reçoit pour la configuration de son adresse IP.

8.2 En se basant sur vos observations en 8.1, quelles opérations DHCP se sont effectuées en broadcast? Selon vous, pourquoi certaines de ces opérations doivent absolument être faites en broadcast? (1.5 pts)

Les messages qui sont effectués en broadcast concernent Discover, Ack, Inform, Request. Ces messages sont en broadcast car le client ne possède pas d'adresse IP au départ. Il envoie donc un paquet à tous les serveurs pour qu'il reçoivent le message Offer par exemple ou être informé.

8.3 Donnez la séquence d'encapsulation des protocoles utilisés pour le paquet DHCP DISCOVER. Pour vous aider, présentez une capture d'écran du contenu du paquet DHCP DISCOVER. (0.25 pt)

The screenshot shows a DHCP Discover packet in Wireshark. The packet structure is as follows:

- DHCP - Dynamic Host Configuration Protocol**
  - DHCP Magic Cookie:** 0x63825363 [278-281]
  - Message Type**
    - Option Code:** 53 *Message Type* [282]
    - Option Length:** 1 [283]
    - Message Type:** 1 *Discover* [284]
  - Client Identifier**
    - Option Code:** 61 *Client Identifier* [285]
    - Option Length:** 7 [286]
    - Hardware Type:** 1 [287]
    - Hardware Address:** 00:0C:29:22:C2:E0 *Vmware:22:C2:E0* [288-293]
  - Requested IP Address**
    - Option Code:** 50 *Requested IP Address* [294]
    - Option Length:** 4 [295]
    - Address:** 192.168.44.99 [296-299]
  - Host Name Address**
    - Option Code:** 12 *Host Name Address* [300]
    - Option Length:** 7 [301]
    - String:** test-PC [302-308]
  - Vendor Class Identifier**
    - Option Code:** 60 *Vendor Class Identifier* [309]
    - Option Length:** 8 [310]
- Parameter Request List**
  - Option Code:** 55 *Parameter Request List* [319]
  - Option Length:** 12 [320]
  - Requested Option:** 1 *Subnet Mask* [321]
  - Requested Option:** 15 *Domain Name* [322]
  - Requested Option:** 3 *Routers* [323]
  - Requested Option:** 6 *Domain Name Servers* [324]
  - Requested Option:** 44 *NetBIOS (TCP/IP) Name Servers* [325]
  - Requested Option:** 46 *NetBIOS (TCP/IP) Node Type* [326]
  - Requested Option:** 47 *NetBIOS (TCP/IP) Scope* [327]
  - Requested Option:** 31 *Perform Router Discovery* [328]
  - Requested Option:** 33 *Static Routes* [329]
  - Requested Option:** 121 [330]
  - Requested Option:** 249 [331]
  - Requested Option:** 43 *Vendor Specific Information* [332]
- DHCP Option End**
  - Option Code:** 255 [333]
  - Data Area:** (8 bytes) [334-341]

8.4 Serait-il possible d'utiliser le protocole TCP de la couche 4 pour toutes requêtes DHCP? Si oui, dites comment, sinon pourquoi est-il impossible d'utiliser TCP pour les requêtes DHCP? (1.5 pts)

**Il serait impossible d'utiliser le protocole TCP car le TCP empêche les opérations de broadcast par définition.**

Ouvrir la trame DHCP OFFER pour les questions qui suivent. 8.5 Quel est le rôle de la trame DHCP offer ? (1 pt)



1-

|   |                |                             |
|---|----------------|-----------------------------|
| <b>DHCP - Dynamic Host Configuration Protocol</b> |                |                             |
| DHCP Magic Cookie:                                | 0x63825363     | [278-281]                   |
| <b>Message Type</b>                               |                |                             |
| Option Code:                                      | 53             | Message Type [282]          |
| Option Length:                                    | 1              | [283]                       |
| Message Type:                                     | 2              | Offer [284]                 |
| <b>Server Identifier</b>                          |                |                             |
| Option Code:                                      | 54             | Server Identifier [285]     |
| Option Length:                                    | 4              | [286]                       |
| Address:  | 192.168.44.198 | [287-290]                   |
| <b>IP Address Lease Time</b>                      |                |                             |
| Option Code:                                      | 51             | IP Address Lease Time [291] |
| Option Length:                                    | 4              | [292]                       |
| Value:  | 14400          | [293-296]                   |
| <b>Subnet Mask</b>                                |                |                             |
| Option Code:                                      | 1              | Subnet Mask [297]           |
| Option Length:                                    | 4              | [298]                       |
| Address:  | 255.255.255.0  | [299-302]                   |
| <b>DHCP Option End</b>                            |                |                             |
| Option Code:                                      | 255            | [303]                       |
| Data Area:  | (38 bytes)     | [304-341]                   |
| <b>FCS - Frame Check Sequence</b>                 |                |                             |
| FCS:  | 0xE0207CEC     | Calculated                  |

La trame DHCP OFFER permet au serveur de répondre à un client qui lui a envoyé un message DHCPDiscover. DHCP Offer contient les informations de configuration de TCP et IP en plus du masque sous-réseau et la passerelle par défaut.

8.6 Quel champ, dans le paquet, indique que ce message est un DHCP offer ? Spécifiez le champ et sa valeur. (0.25 pt)

|   |            |                    |
|---|------------|--------------------|
| <b>DHCP - Dynamic Host Configuration Protocol</b> |            |                    |
| DHCP Magic Cookie:                                | 0x63825363 | [278-281]          |
| <b>Message Type</b>                               |            |                    |
| Option Code:                                      | 53         | Message Type [282] |
| Option Length:                                    | 1          | [283]              |
| Message Type:                                     | 2          | Offer [284]        |
| <b>Server Identifier</b>                          |            |                    |

8.7 À quel poste correspond l'adresse MAC dans le champ Destination de l'entête Ethernet? Et celui du champ Source? (0.5 pt)

|   |                   |                       |
|---|-------------------|-----------------------|
| <b>Ethernet Header</b>                        |                   |                       |
| Destination:                                  | 00:0C:29:22:C2:E0 | VMware:22:C2:E0 [0-5] |
| Source:                                       | 00:19:D1:25:2E:45 | Intel:25:2E:45 [6-11] |
| Protocol Type:                                | 0x0800            | IP [12-13]            |
| <b>IP Header - Internet Protocol Datagram</b> |                   |                       |

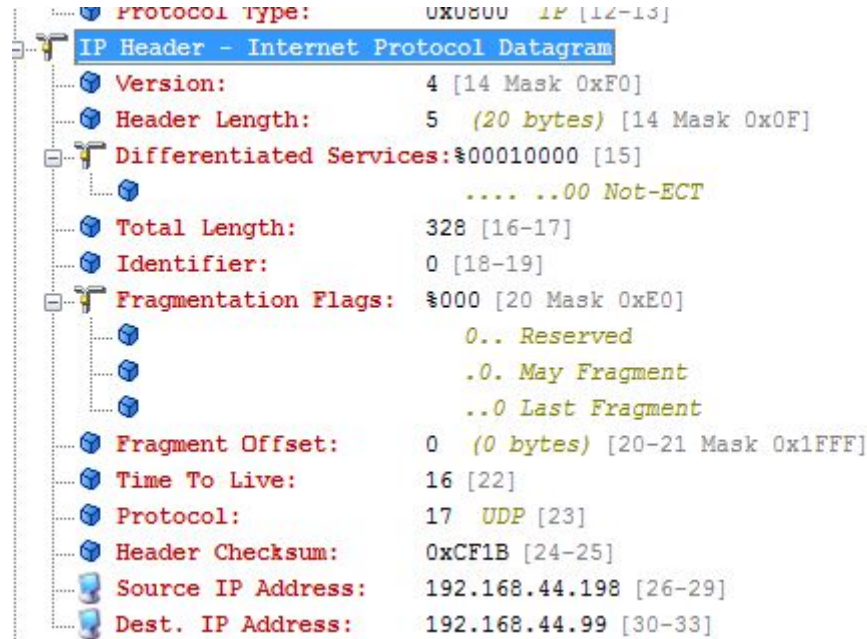
L'adresse MAC du champ destination dans l'entête correspond à celle du client comme vu dans la réponse à la question 7.1

8.8 Quelle est la valeur du champ Protocole Type et que signifie-t-elle ? (0.25 pt) 8.9 Quelle est la taille de l'entête Ethernet que vous observez? (0.25 pt)

|                |        |            |
|----------------|--------|------------|
| Protocol Type: | 0x0800 | IP [12-13] |
|----------------|--------|------------|

La valeur est 0x800 et permet d'indiquer le type de protocole de commutation de paquets utilisé. Dans ce cas, il s'agit du protocole IP.

8.10 Quelle est l'entête suivante de la trame (niveau 3 du modèle OSI) ? (0.25 pt)



8.11 À quelle machine appartient l'adresse IP source? (0.25 pt)

Il s'agit de l'adresse IP (passerelle par défaut en réalité) du serveur étant donné que le client est le destinataire.

8.12 Quelle est la taille de l'entête de niveau 3 du modèle OSI que vous observez? (0.25 pt)

**20 octects**

8.13 Nommez le protocole de niveau supérieur (niveau 4 du modèle OSI) utilisé par DHCP. (0.25 pt)



8.14 Quelle est la taille de l'entête de niveau 4 du modèle OSI que vous observez? (0.25 pt)

**8 octect**

8.15 Dans l'entête DHCP, quelle est la signification du champ IP Address Lease Time ? (0.25 pt)

IP Address Lease Time est la durée du bail de l'adresse IP

8.16 Dans combien de temps la machine Windows 7 doit-elle revalider avec le serveur DHCP son adresse IP? (0.25 pt)

**14400s**

8.17 Que désigne le champ Client IP Addr Given By Svr? Quelle est l'utilité de ce champ? (0.25 pt)

Ce champ spécifie l'adresse IP que le serveur à attribuer au client après une demande de la part de ce dernier avec DHCP.

9.1 Dans votre client clone of Windows 7, et dans une fenêtre de commande (DOS), exécutez la commande arp -a qui permet d'afficher le contenu de votre cache ARP. Quelle est l'utilité de la cache ARP? (1.25 pts)

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

Interface: 192.168.44.99 --- 0xa
Internet Address      Physical Address      Type
10.0.80.109           00-0c-29-71-de-25    dynamic
192.168.44.40         00-0c-29-30-02-43    dynamic
192.168.44.57         00-0c-29-71-de-25    dynamic
192.168.44.118        00-0c-29-e5-bd-db    dynamic
192.168.44.198        00-19-d1-25-2e-45    dynamic
192.168.44.205        00-0c-29-a6-08-42    dynamic
192.168.44.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    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
```

La cache ARP permet au module ARP de déterminer l'adresse MAC d'une autre machine sur le même réseau ethernet. Il y a une correspondance entre les adresses IP et les adresses MAC.

Si l'adresse de votre serveur clone of ServeurWindows y apparaît, enlevez-la avec la commande arp -d 192.168.44.2xx. Vérifiez qu'elle n'y est plus. Démarrez l'analyseur de protocole.

```
C:\Users\Administrator>arp -d 192.168.44.205

C:\Users\Administrator>arp -a

Interface: 192.168.44.99 --- 0xa
Internet Address      Physical Address      Type
10.0.80.109           00-0c-29-71-de-25    dynamic
192.168.44.40         00-0c-29-30-02-43    dynamic
192.168.44.57         00-0c-29-71-de-25    dynamic
192.168.44.118        00-0c-29-e5-bd-db    dynamic
192.168.44.198        00-19-d1-25-2e-45    dynamic
192.168.44.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    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
```

9.2 Lancez une commande qui permet de vérifier votre connectivité avec le serveur clone of ServeurWindows. Arrêtez l'analyseur de protocole et sauvegardez la capture réalisée. Lancez à nouveau la commande arp -a. Que remarquez-vous ? (0.25 pt)

|     |                    |                    |     |     |           |                   |                                  |
|-----|--------------------|--------------------|-----|-----|-----------|-------------------|----------------------------------|
| 1   | 192.168.44.41      | 192.168.44.255     |     | 247 | 0.000000  | SMB               | C Browser Host Announcement L47  |
| 2   | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 1.224044  | 802.1             |                                  |
| 3   | Cisco:A2:CE:01     | 01:00:0C:00:00:00  | *   | 94  | 1.833376  | 00-00-0C-00-00-03 |                                  |
| 4   | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 2.238778  | ARP Request       | 192.168.20.1 = ?                 |
| 5   | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 3.216440  | 802.1             |                                  |
| 6   | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 3.236137  | ARP Request       | 192.168.20.1 = ?                 |
| 7   | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 4.233556  | ARP Request       | 192.168.20.1 = ?                 |
| 8   | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 5.212853  | 802.1             |                                  |
| 9   | FE80::C9D3:F98:... | FF02::1:2          |     | 153 | 7.065914  | UDP               | Src= 546,Dst= 547 ,L= 87         |
| 10  | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 7.205426  | 802.1             |                                  |
| 11  | VMware:22:C2:E0    | Ethernet Broadcast |     | 64  | 8.269077  | ARP Request       | 192.168.44.205 = ?               |
| 12  | VMware:A6:08:42    | VMware:22:C2:E0    |     | 64  | 8.269294  | ARP Response      | VMware:A6:08:42 = 192.168.44.205 |
| 13  | 192.168.44.99      | 192.168.44.205     |     | 78  | 8.269314  | PING Req          | Echo: 192.168.44.205             |
| 14  | 192.168.44.205     | 192.168.44.99      |     | 78  | 8.269705  | PING Reply        | Echo Reply: 192.168.44.99        |
| 15  | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 9.200305  | 802.1             |                                  |
| 16  | 192.168.44.99      | 192.168.44.205     |     | 78  | 9.271724  | PING Req          | Echo: 192.168.44.205             |
| 17  | 192.168.44.205     | 192.168.44.99      |     | 78  | 9.272347  | PING Reply        | Echo Reply: 192.168.44.99        |
| 18  | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 9.962028  | ARP Request       | 192.168.20.1 = ?                 |
| 19  | 192.168.44.99      | 192.168.44.205     |     | 78  | 10.275001 | PING Req          | Echo: 192.168.44.205             |
| 20  | 192.168.44.205     | 192.168.44.99      |     | 78  | 10.275184 | PING Reply        | Echo Reply: 192.168.44.99        |
| 21  | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 10.411852 | ARP Request       | 192.168.20.198 = ?               |
| 22  | 192.168.44.110     | 192.168.44.255     |     | 247 | 10.852477 | SMB               | C Browser Host Announcement L47  |
| 23  | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 10.959457 | ARP Request       | 192.168.20.1 = ?                 |
| 24  | Cisco:AD:6D:45     | Mcast 802.1d Br... | *   | 64  | 11.195161 | 802.1             |                                  |
| 25  | 192.168.44.99      | 192.168.44.205     |     | 78  | 11.276383 | PING Req          | Echo: 192.168.44.205             |
| 26  | 192.168.44.205     | 192.168.44.99      |     | 78  | 11.276557 | PING Reply        | Echo Reply: 192.168.44.99        |
| 27  | Intelorate:2A:D... | Ethernet Broadcast |     | 64  | 11.409297 | ARP Request       | 192.168.20.198 = ?               |
| ... | ...                | ...                | ... | ... | ...       | ...               | ...                              |



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

Interface: 192.168.44.99 --- 0xa
Internet Address      Physical Address      Type
10.0.80.109           00-0c-29-71-de-25     dynamic
192.168.44.40         00-0c-29-30-02-43     dynamic
192.168.44.57         00-0c-29-71-de-25     dynamic
192.168.44.118        00-0c-29-e5-bd-db     dynamic
192.168.44.198        00-19-d1-25-2e-45     dynamic
192.168.44.205        00-0c-29-a6-08-42     dynamic
192.168.44.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     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
```

l'adresse du serveur est la encore.

9.3, appliquez le filtre ARP à votre nouvelle capture. Dans l'analyseur de protocole, quelle est la longueur (size) des trames ARP ? (0.25 pt)

28 octet

```
ARP - Address Resolution Protocol
  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:29:22:C2:E0 VMware:22:C2:E0 [22-27]
  Sender Internet Addr: 192.168.44.99 [28-31]
  Target Hardware Addr: 00:00:00:00:00:00 Xerox:00:00:00 (ignored) [32-37]
  Target Internet Addr: 192.168.44.205 [38-41]
```

9.4 Quelle est la valeur numérique du champ Protocol type de l'en-tête Ethernet (Ethertype) d'une trame ARP ? Que signifie-t-elle ? (0.5 pt)

**Ethernet:** IP can use **Ethernet** and many other protocols. The assigned Ethernet type for IP is 0x800.

9.5 Quelle est la séquence d'encapsulation d'une requête ARP ? (0.25 pt)

Séquence d'encapsulation ARP :

- Packet Info
- Ethernet Header
- ARP
- Extra bytes
- FCS Frame Check Sequence

9.6 En se basant sur le contenu d'un paquet ARP Request et ARP Response, qu'est-ce qui différencie une requête ARP d'une réponse ARP dans le protocole ARP ? (0.25 pt)

**Une requête ARP concerne toutes les machines du réseau ( broadcast. On ne tient pas compte de l'adresse du destinataire. Tandis que la réponse provient de la machine du destinataire de la requête.**

9.7 Quel champ de la réponse ARP possède l'information recherchée par la requête ARP lancée par un client d'un réseau? (0.25 pt)

**Le champ de la réponse ARP possède l'information recherchée par la requête ARP : est le sender Hardware Addr**

1-

9.8 Qu'est-ce qu'il y a de particulier à la fin des données d'une trame ARP juste avant le champ FCS (CRC de 32 bits) ? Quel pourcentage de la taille de la trame ce champ occupe-t-il? Pourquoi ce champ est-il nécessaire dans les requêtes ARP? (0.5 pt)

**Il s'agit des extra bytes. Le pourcentage correspondant est  $18 \times 100 / 64 = 28,12\%$**

9.9 À quel nœud réseau correspond l'adresse MAC de la source de la réponse ARP? (0.25 pt)

**Adresse MAC source : 00:0c:29:30:02:43 . C'est l'adresse MAC du serveur DHCP**

9.10 À quel nœud réseau correspond l'adresse MAC de la destination de la réponse ARP? (0.25 pt)

**Adresse Mac destination : 00:0C:29:20:B1:20. C'est l'adresse du client ( clone du Windows 7)**

10.1 Toujours dans l'analyseur de protocoles avec les mêmes données de capture pour la partie ARP, quelle est la séquence d'encapsulation d'une trame PING ? (0.5 pt)

**La séquence d'encapsulation :**

- Packet Info
- Ethernet Header
- IP Header - Internet Protocol Datagram
- ICMP - Internet Control Messages Protocol
- FCS - Frame Check Sequence

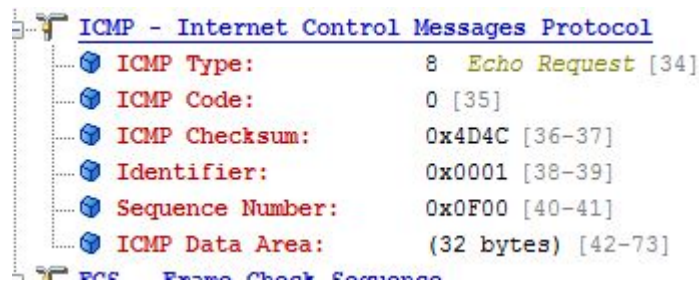
10.3 Quelle est la version du protocole IP utilisée ? (0.5 pt)

**Il s'agit du protocole IPv4**

10.4 Quelle est la valeur du champ TTL (Time To Live). À quoi sert ce champ ? (0.5 pt)

**Un paquet avec un TTL de moins de 128 indique que le paquet a le plus probablement traversé un routeur.**

10.5 Quel est le champ ICMP qui différencie les requêtes par rapport aux réponses PING et quelles sont les valeurs impliquées ? (0.5 pt)



**c'est le champ Identifier et sa valeur est de 0x001 (1 octet)**

11.1 Un ingénieur travaillant sur l'ordinateur « A » décide d'envoyer une requête PING vers l'ordinateur « B » afin de vérifier si l'ordinateur « B » est accessible sur le réseau. Sachant que le réseau en entier est câblé, donner l'état de l'entête Ethernet et IP du paquet contenant la requête PING à chaque lien (1, 3, 4 ,5 et 6). Utiliser le format de paquet ci-dessous. (2 pts)



1-

|                            |                                |
|----------------------------|--------------------------------|
| MAC destination: --        | MAC Source: A1:B2:C3:D4:E5:F6  |
| IP source : 132.207.29.102 | IP destination: 132.207.30.102 |

3-

|                            |                                |
|----------------------------|--------------------------------|
| MAC destination: --        | MAC Source: A1:B2:C3:D4:E5:F6  |
| IP source : 132.207.29.102 | IP destination: 132.207.29.101 |

4-

|                            |                               |
|----------------------------|-------------------------------|
| MAC destination: --        | MAC Source: --                |
| IP source : 132.207.29.101 | IP destination: 132.207.0.101 |

5-

|                           |                                |
|---------------------------|--------------------------------|
| MAC destination: --       | MAC Source: --                 |
| IP source : 132.207.0.101 | IP destination: 132.207.30.101 |

6-

|                            |                                |
|----------------------------|--------------------------------|
| MAC destination: --        | MAC Source: A5:B6:C7:D8:E9:F1  |
| IP source : 132.207.30.101 | IP destination: 132.207.30.102 |

11.2 Ce même ingénieur, toujours depuis l'ordinateur « A » décide d'envoyer une requête PING vers l'ordinateur « C » pour vérifier si lui aussi est accessible sur le réseau. Donner l'état de l'entête Ethernet et IP du paquet contenant la requête PING à chaque lien (1 et 2). Utiliser le même format de paquet qu'en 11.1 (2 pts)

|                                    |                                |
|------------------------------------|--------------------------------|
| 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 |

|                                    |                                |
|------------------------------------|--------------------------------|
| 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 |