

**Capture, Filtrage et Analyse de trames ETHERNET
avec le logiciel Wireshark**
- correction -

Wireshark est un programme informatique libre de droit, qui permet de capturer et d'analyser les trames d'information qui transitent par les interfaces de communication du terminal sur lequel il s'exécute. *Wireshark* est ainsi apparenté aux logiciels appelés « Sniffer » ou « analyseur de trafic ». Il est multi-OS et téléchargeable sur le site www.wireshark.com.

Avec *Wireshark*, il est possible de capturer des trames Ethernet en temps réel directement sur les Cartes de communication du terminal, de sauvegarder les résultats de cette capture dans des fichiers qui peuvent être analysés ultérieurement hors ligne. *Wireshark* supporte un très grand nombre de protocoles de communication et de formats de fichiers de capture : Ethernet, ARP, IP, TCP/UDP, HDLC, etc ... libpcap/tcpdump, Sun's snoop/atmsnoop, Lanalyzer, MS Network Monitor, HPUX nettl, AIX iptrace, Cisco Secure IDS, etc....

Durant ce TP, nous allons :

1. lancer le programme Wireshark,
2. capturer et analyser une trame Ethernet
3. définir des filtres pour la capture et la visualisation des trames
4. Enregistrer le résultat de cette capture dans un fichier

Etape 5 : Répondre aux questions suivantes :

5.1 Lancer la machine virtuelle « client linux fedora » puis la machine virtuelle « Serveur linux fedora »

5.2 taper sur la console du serveur la commande « ifconfig » (voir le manuel man pour la syntaxe de la commande ifconfig). Il faut taper la commande « \$ifconfig -a » pour obtenir les différents paramètres de configuration réseaux

```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Ahmed>ipconfig /all

Carte réseau sans fil Connexion réseau sans fil :

    Suffixe DNS propre à la connexion. . . : wifi.univ-paris5.fr
    Description. . . . . : Intel(R) Centrino(R) Wireless-N 1030

    Adresse physique . . . . . : 4C-80-93-6C-DE-1E
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::b120:8a9f:dc3b:deac%13(préfére
)
    Adresse IPv4. . . . . : 172.30.44.201(préfére)
    Masque de sous-réseau. . . . . : 255.255.240.0
    Bail obtenu. . . . . : mardi 17 novembre 2015 14:29:11
    Bail expirant. . . . . : mardi 17 novembre 2015 16:29:22
    Passerelle par défaut. . . . . : 172.30.32.1
    Serveur DHCP . . . . . : 1.1.1.1
    IAID DHCPv6 . . . . . : 357335187
    DUID de client DHCPv6. . . . . : 00-01-00-01-1C-97-6F-94-24-B6-FD-0F-FA
-C7
    Serveurs DNS. . . . . : 193.51.86.4
    Serveur WINS principal . . . . . : 172.20.143.3
    NetBIOS sur Tcpip. . . . . : Activé
```

- Combien d'interfaces trouvez-vous ? nous trouvons deux interfaces eth0 et lo » (sous linux). Sous windows, nous avons 4 interfaces : Wifi, Bluetooth, Ethernet, VPN.

- A quoi correspond l'interface « eth0 », l'interface « lo » ? L'interface eth0 correspond à la première interface Ethernet du serveur. L'interface « lo » correspond à l'interface de boucle locale (127.0.0.1) servant aux communications internes du terminal.

- Identifier les adresses Ethernet (eth0) du serveur. 4C-80-93-6C-DE-1E

- Identifier les adresses IP et le masque réseaux du serveur. 172.30.44.201 et mask 255.255.240.0

Il faut ajouter l'option « /all » ou « -a » pour obtenir l'adresse physique (MAC) :

- Quel est le type d'adresse IP (publique/privée) utilisé par le serveur ? ce sont des adresses IP privée de classe C (sous linux). De Classe B (sous Windows).

- Répéter les mêmes opérations avec le poste client.

	Adresse IP	masque	adresse MAC
VM Client	192.168.57.101	255.255.255.0	08:00:27:A5:AE:4A
VM Serveur	192.168.57.100	255.255.255.0	08:00:27:06:36:6E

5.3 sur le poste Client, lancer le logiciel Wireshark sur votre interface Ethernet (eth0) en mode « administrateur (root) », au moyen de la commande : `$> sudo wireshark&`

5.4 sur le poste Client, taper une commande de type « ping » à destination du serveur et capturer environ 30 secondes de trafic sur le poste serveur (voir le manuel man pour la syntaxe de la commande ping).

`$> ping 192.168.57.100` sur le poste client

Ping est une commande système qui permet de tester la disponibilité d'un hôte (PC, serveur, routeur, imprimante, ...) utilisant le protocole de communication IP.

Ping transmet des requêtes ICMP (ICMP echo), et l'hôte distant doit répondre avec des réponses ICMP (ICMP reply)

```
C:\Users\Ahmed>ping 192.168.57.100
```

```
Pinging 192.168.57.100 with 32 bytes of data:
```

```
Reply from 192.168.57.100: bytes=32 time=42ms TTL=255
```

```
Reply from 192.168.57.100: bytes=32 time=3ms TTL=255
```

```
Reply from 192.168.57.100: bytes=32 time=2ms TTL=255
```

```
Reply from 192.168.57.100: bytes=32 time=21ms TTL=255
```

```
Ping statistics for 192.168.57.100:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds (ces moyennes sont affichées après un arrêt de l'affichage avec CTRL+C):
```

```
    Minimum = 2ms, Maximum = 42ms, Average = 17ms
```

```
C:\Users\Ahmed>ping 172.30.32.1
```

```
Envoi d'une requête 'Ping' 172.30.32.1 avec 32 octets de données :
```

```
Réponse de 172.30.32.1 : octets=32 temps=98 ms TTL=255
```

```
Réponse de 172.30.32.1 : octets=32 temps=96 ms TTL=255
```

```
Réponse de 172.30.32.1 : octets=32 temps=107 ms TTL=255
```

```
Réponse de 172.30.32.1 : octets=32 temps=65 ms TTL=255
```

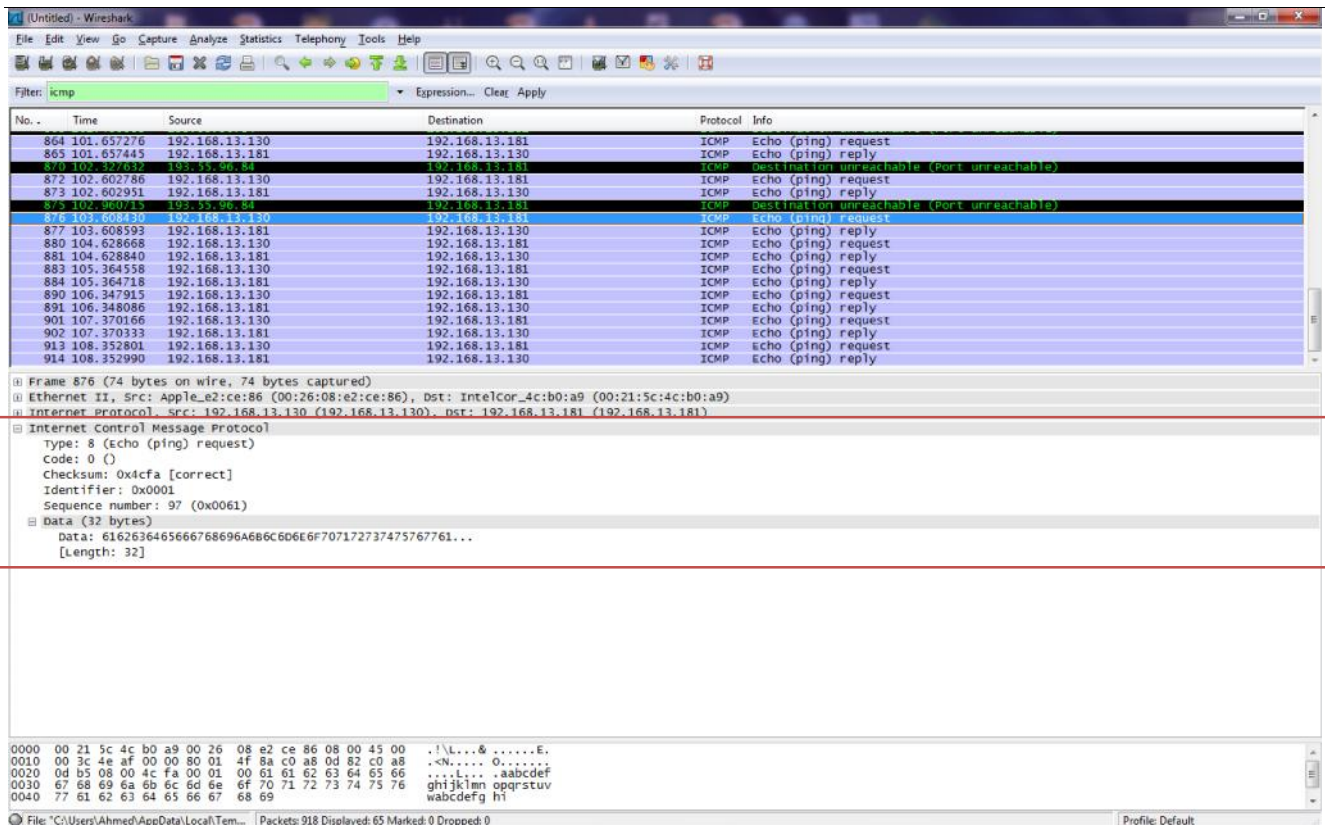
```
Statistiques Ping pour 172.30.32.1:
```

```
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

```
Durée approximative des boucles en millisecondes :
```

```
    Minimum = 65ms, Maximum = 107ms, Moyenne = 91ms
```

4 ICMP echo et 4 ICMP request (ping) ont été échangés entre le client et le serveur:



5.5 Combien de types de trames avez-vous capturé ? nous capturons deux (2) types de paquets ICMP et deux (2) types de trames ARP. Soit au total 4 types différents.

Sous windows :

8 trames = 4 trames ICMP echo + 4 trames ICMP reply

Sous unix :

Des dizaines de trames ICMP echo et reply en boucle jusqu'à l'arrêt de l'affichage avec CTRL+C

5.6 filtrer votre capture pour ne sélectionner que les trames « icmp ». Puis analyser la première trame et indiquer la valeur des champs suivants :

- en tête Ethernet : champ « TYPE »
- en tête IP : champ « protocole »
- en tête ICMP : champ « TYPE » et champ « IDENTIFIER »

Le premier paquet ICMP est de type « echo request » (ping request), le second paquet ICMP est une réponse à l'écho, et s'appelle ICMP echo reply (ping reply) .

Pour ce premier paquet ICMP echo nous trouvons avec Wireshark les valeurs de champs Ethernet, IP et ICMP suivants :

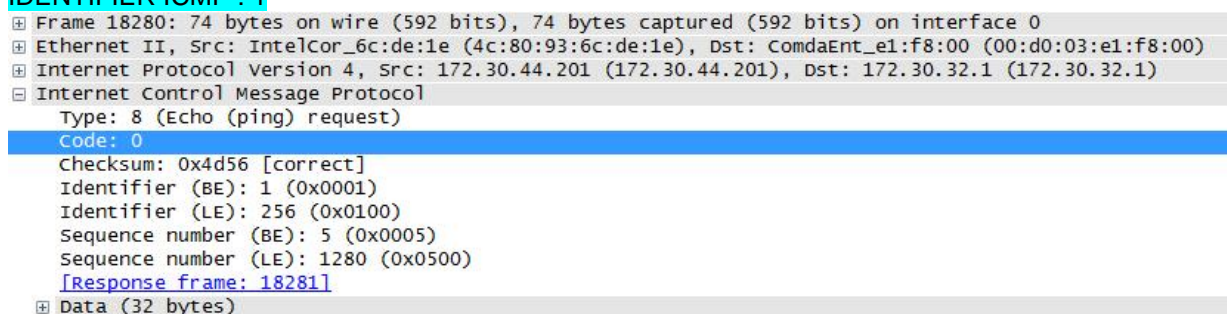
TYPE Ethernet (2 octets en Hexa) : x0800 (signifiant le contenu de la trame est un paquet IP)

PROTOCOL IP (1 octet en décimal) : 1 (signifiant que le contenu du paquet IP est un paquet ICMP)

TYPE ICMP : 8 (signifiant que le message ICMP est de type Echo request)

CODE icmp : 0

IDENTIFIANT ICMP : 1



Wireshark capture of ICMP Echo (ping) requests and replies. The packet list shows multiple 'Destination unreachable' messages. The packet details pane for frame 68 shows the Ethernet II, IP, and ICMP layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
2	0.001999	192.168.13.72	192.168.13.176	ICMP	Destination unreachable
68	5.724273	192.168.13.176	192.168.13.1	ICMP	Echo (ping) request
69	5.726266	192.168.13.1	192.168.13.176	ICMP	Echo (ping) reply
79	6.135764	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
83	6.726595	192.168.13.176	192.168.13.1	ICMP	Echo (ping) request
84	6.729064	192.168.13.1	192.168.13.176	ICMP	Echo (ping) reply
86	6.874945	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
98	7.623504	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
106	7.728576	192.168.13.176	192.168.13.1	ICMP	Echo (ping) request
107	7.730459	192.168.13.1	192.168.13.176	ICMP	Echo (ping) reply
117	8.682665	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
118	8.729653	192.168.13.176	192.168.13.1	ICMP	Echo (ping) request
119	8.731688	192.168.13.1	192.168.13.176	ICMP	Echo (ping) reply
129	9.436432	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
142	10.182995	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
149	10.935845	193.55.96.84	192.168.13.176	ICMP	Destination unreachable
154	11.686314	193.55.96.84	192.168.13.176	ICMP	Destination unreachable

Frame 68 (74 bytes on wire (58 bytes captured) on interface 0:00:00:00:00:00):
 Ethernet II, Src: IntelCor_4c:b0:a9 (00:21:5c:4c:b0:a9), Dst: Netgear_ff:d2:ba (00:09:5b:ff:d2:ba)
 Destination: Netgear_ff:d2:ba (00:09:5b:ff:d2:ba)
 Source: IntelCor_4c:b0:a9 (00:21:5c:4c:b0:a9)
 Type: IP (0x0800)
 Internet Protocol, Src: 192.168.13.176 (192.168.13.176), Dst: 192.168.13.1 (192.168.13.1)
 Internet Control Message Protocol

0000 00 09 5b ff d2 ba 00 21 5c 4c b0 a9 08 00 45 00 ...! \L....E.
 0010 00 3c 21 c1 00 00 80 01 7c fe c0 a8 0d b0 c0 a8 .<!. |.....
 0020 0d 01 08 00 4d 4c 00 01 00 0f 61 62 63 64 65 66ML.. ..abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
 0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

Ils est possibles d'identifier la source de ce test ping : en retrouvant son adresse physique et IP (08:00:27:06:36:6E et 192.168.57.100)

5.7 Recherchez sur Internet le document RFC 1700. Quelle information mentionne t il en relation avec la trame Ethernet ? le message ICMP ?

Les RFC (Request For Comment) sont les documents de specifications des protocoles de l'Internet (et Intranet). Ils signifient « RFC pour Request For Comments » et sont numérotés. Le RFC 1700 correspond aux numéros des types de paquets et les numéros des codes d'opération des protocoles de l'Internet (IP, ICMP, TCP, etc ...)

Le RFC 1700 a été remplacé par le RFC 3232

HISTORIC

J. Reynolds

J. Postel

ISI

October 1994

 group: groupe, groupement, cercle, bande, famille, grouper, se grouper, former un groupe, classer, diviser
[Désactiver](#)

Obsoletes IENs: 127, 117, 93

Category: Standards Track

Status of this Memo

OVERVIEW

This RFC is a snapshot of the ongoing process of the assignment of protocol parameters for the Internet protocol suite. To make the current information readily available the assignments are kept up-to-date in a set of online text files. This RFC has been assembled by catinating these files together with a minimum of formatting "glue". The authors appologize for the somewhat rougher formatting and style than is typical of most RFCs.

Les Filtres sont:

```
ip.addr==192.168.57.100 (afficher tous les paquets ayant pour adresses IP sources ou destination 192.168.57.100)
```

ip.src==192.168.57.100 (afficher tous les paquets ayant pour adresse IP source 192.168.57.100)

Wireshark Filter Expression - Profile: Default

Field name	Relation	Value (Ethernet or other MAC address)
eth.dst - Destination (Destination Hardware Address)	is present	192.168.13.181

OK Cancel

Filter: arp

No.	Time	Source	Destination	Protocol	Info
121	8.090024	10.1e:01:e9:90:10	b1:b0:a5:c0	ARP	who has 192.168.13.146?
122	9.308607	f8:1e:df:e9:96:1b	Broadcast	ARP	who has 192.168.13.146?
123	9.310860	Apple_0e:ba:0e	Broadcast	ARP	Gratuitous ARP for 192.168.13.146?
130	9.717303	Apple_0e:ba:0e	Broadcast	ARP	Gratuitous ARP for 192.168.13.146?
131	9.718956	Apple_0e:ba:0e	Broadcast	ARP	who has 192.168.13.72?
132	10.130045	Apple_0e:ba:0e	Broadcast	ARP	who has 169.254.255.255?

Frame 131 (42 bytes on wire, 42 bytes captured)

Ethernet II, Src: Apple_0e:ba:0e (00:25:bc:0e:ba:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (0x0001)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (0x0001)

[Is gratuitous: False]

Sender MAC address: Apple_0e:ba:0e (00:25:bc:0e:ba:0e)

Sender IP address: 192.168.13.187 (192.168.13.187)

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

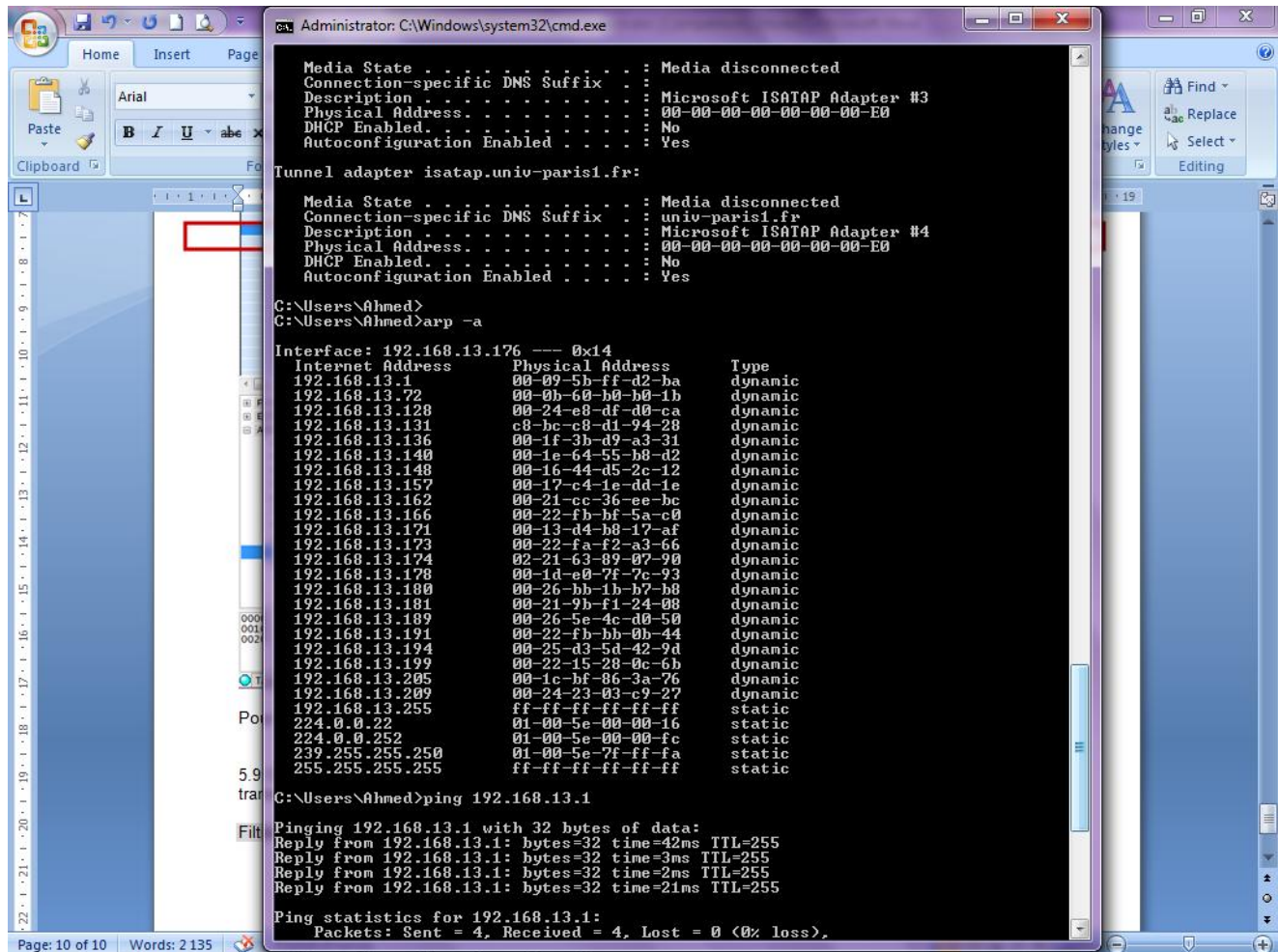
Target IP address: 192.168.13.72 (192.168.13.72)

5.9 Décrivez la procédure (commandes systèmes, filtres wireshark) permettant de capturer et de filtrer les trames Ethernet transportant uniquement un paquet ARP ayant pour origine (émission) le poste serveur.

ARP signifie Address Resolution Protocol. Ce logiciel de communication permet de trouver l'adresse Physique (MAC) d'un hôte sur le même réseau local (ex. DNS, routeur par défaut, un serveur web local, une imprimante réseau ...) connaissant son adresse IP.

L'ordinateur envoie une requête ARP et il reçoit une réponse ARP.

Pour visualiser toutes les adresses physiques (MAC) déjà obtenues, il suffit de taper la commande « arp -a ».



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays the output of the following commands:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : univ-paris1.fr
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.univ-paris1.fr:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : univ-paris1.fr
Description . . . . . : Microsoft ISATAP Adapter #4
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Ahmed>
C:\Users\Ahmed>arp -a

Interface: 192.168.13.176 --- 0x14
Internet Address      Physical Address      Type
192.168.13.1          00-09-5b-ff-d2-ba     dynamic
192.168.13.72         00-0b-60-b0-b0-1b     dynamic
192.168.13.128        00-24-e8-df-d0-ca     dynamic
192.168.13.131        c8-bc-c8-d1-94-28     dynamic
192.168.13.136        00-1f-3b-d9-a3-31     dynamic
192.168.13.140        00-1e-64-55-b8-d2     dynamic
192.168.13.148        00-16-44-d5-2c-12     dynamic
192.168.13.157        00-17-c4-1e-dd-1e     dynamic
192.168.13.162        00-21-cc-36-ee-bc     dynamic
192.168.13.166        00-22-fb-bf-5a-c0     dynamic
192.168.13.171        00-13-d4-b8-17-af     dynamic
192.168.13.173        00-22-fa-f2-a3-66     dynamic
192.168.13.174        02-21-63-89-07-90     dynamic
192.168.13.178        00-1d-e0-7f-7c-93     dynamic
192.168.13.180        00-26-bb-1b-b7-b8     dynamic
192.168.13.181        00-21-9b-f1-24-08     dynamic
192.168.13.189        00-26-5e-4c-d0-50     dynamic
192.168.13.191        00-22-fb-bb-0b-44     dynamic
192.168.13.194        00-25-d3-5d-42-9d     dynamic
192.168.13.199        00-22-15-28-0c-6b     dynamic
192.168.13.205        00-1c-bf-86-3a-76     dynamic
192.168.13.209        00-24-23-03-c9-27     dynamic
192.168.13.255        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
239.255.255.255       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Ahmed>ping 192.168.13.1

Pinging 192.168.13.1 with 32 bytes of data:
Reply from 192.168.13.1: bytes=32 time=42ms TTL=255
Reply from 192.168.13.1: bytes=32 time=3ms TTL=255
Reply from 192.168.13.1: bytes=32 time=2ms TTL=255
Reply from 192.168.13.1: bytes=32 time=21ms TTL=255

Ping statistics for 192.168.13.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

5.9 Décrivez la procédure (commandes systèmes, filtres wireshark) permettant de capturer et de filtrer les trames Ethernet transportant uniquement un paquet ARP.

Filtre : arp

5.10 modifier l'adresse IP et le masque de réseau de votre serveur linux fedora avec les valeurs 172.24.0.2 et 255.255.0.0 (consulter le manuel système Linux/unix, « \$> man ifconfig »

> ifconfig eth0 172.24.0.2 netmask 255.255.0.0