Diana Margarian **22 octobre 2023**

TP 4 : ANALYSE DE TRAMES DHCP AVEC WIRESHARK

Sommaire : COMPTE RENDU

Objectifs :

1. Processus d'acquisition d'une adresse IPv4
2. Capture de trames DHCP avec Wireshark
3. Étude de la trame DHCP DISCOVER

1. Processus d'acquisition d'une adresse IPv4.

2. Capture de trames DHCP avec Wireshark

Dans cette partie je vais effectuer des captures de trames DHCP avec Wireshark.

- J'ai constaté en regardant dans mes paramètres de mon ordinateur que l'adresse IP est attribuer automatiquement par le serveur DHCP.

➔ J'ai ouvert une invite de commandes et j'ai saisi la commande ipconfig/all :

- Quelle est l'adresse IP attribuée par mon serveur DHCP ?

  L'adresse IP attribuer par mon routeur est 192.168.1.1

  L'état DHCP est activé : oui

  Masque de sous réseau est : 255.255.255.0

  Le Bail obtenu est : vendredi 20 octobre 2023

  Le Bail expirant est : samedi 21 octobre 2023

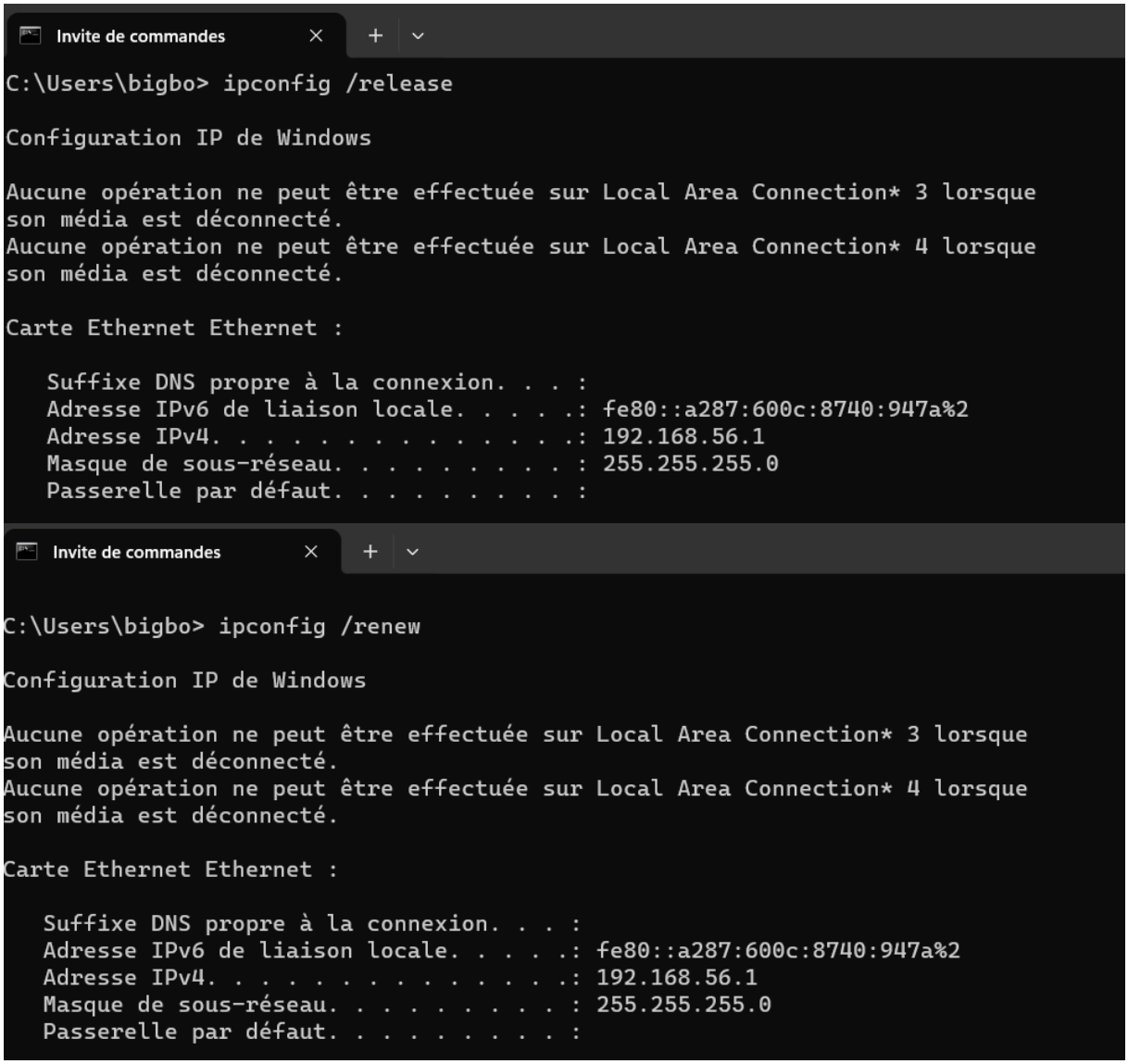
  La passerelle par défaut est : 192.168.1.1

Serveur DHCP est : 192.168.1.1

Serveur DNS est : 192.168.1.1

➔ J'ai démarré une capture de trames sur Wireshark.
➔ J'ai ouvert l'invite de commandes et j'ai tapé successivement les commandes :

- **ipconfig /release**
- **ipconfig /renew**



- A partir des renseignements obtenus à l'aide de la commande ipconfig /release, renseignez les éléments ci-dessous :

  Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : (censé être 192.168.1.1)

- A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :

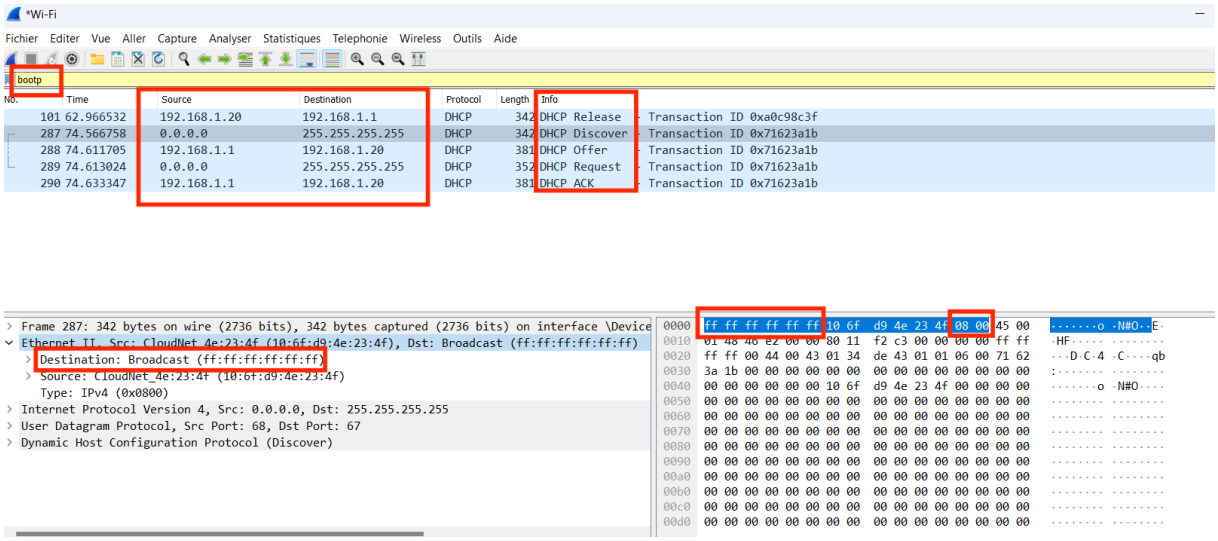
Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : (censé être 192.168.1.1)

➔ Zone Filter : bootp. La capture obtenue :

(Trame 342 DHCP Discover est sélectionnée et la section qui correspond à l'en-tête Ethernet a été développé)



4. Étude de la trame DHCP DISCOVER.

Dans cette partie de vais étudier la trame DHCP Discover

- J'ai sélectionné la section Ethernet (en-tête de trame) de la trame DHCP DISCOVER et j'ai identifié les adresses MAC source et destination dans le volet des octets :

L'adresse MAC de source est = 10 : 6f : d9 : 4e : 23 : 4f

L'adresse MAC de destination est = ff : ff : ff : ff : ff : ff

- Caractérisez l'adresse de couche 2 de destination de cette trame :

La couche 2 de destination (ff : ff : ff : ff : ff : ff) est une adresse MAC spéciale qui correspond à une diffusion nommé broadcast à toutes les machines locales. Donc la trame est destinée à être reçue par toutes les machines connectées au même réseau.

- Quel est le champ qui suit immédiatement les deux adresses MAC :

Le champ qui suit immédiatement les deux adresses MAC est le champ Type dans une trame Ethernet. Elle indique le type de protocole encapsulé dans la trame.

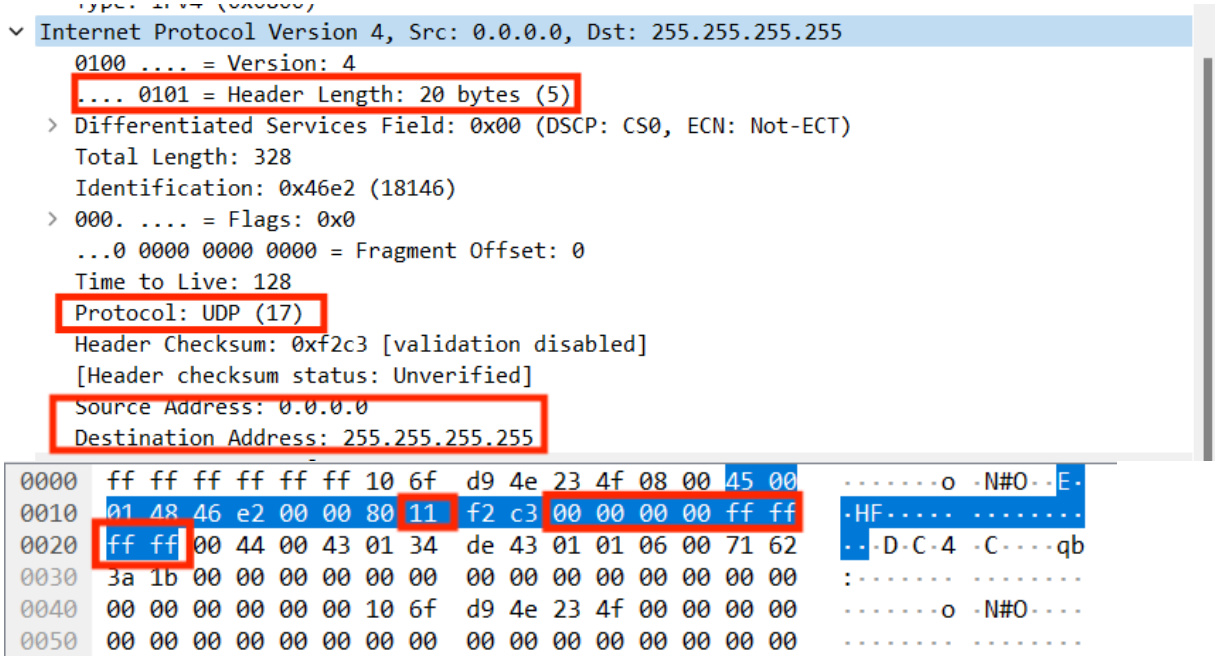
- Quelle valeur contient-il ? Que signifie-t-elle ?

Elle contient la valeur "08 00" qui correspond au champ "Type" de l'en-tête Ethernet. Elle signifie que le protocole de couche supérieure utilisé après l'en-tête Ethernet est IPv4. -> Encapsulée dans un paquet IPv4.

- Quels sont les protocoles inclus dans cette trame ?

Le protocole UDP est inclus dans cette trame.

➔ Sélectionnez comme dans la figure ci-dessous, l'en-tête IP contenu dans la trame DHCP DISCOVER.



(Et de paquet : 20 octets (le 10eme est le champ protocole et les 8 derniers sont les IP Source et IP Destination)

- Quel est le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP ? Préciser la valeur de ce champ ainsi que le nom du protocole.

- **Renseignez ci-dessous les champs d'en tête IP suivants :**

Version = valeur décimale 4 et valeur hexa 45

IHL = valeur décimale 5 et valeur hexa 45

Protocole = valeur décimale 17 et valeur hexa 11

Source address = valeur décimale 0.0.0.0 et valeur hexa 00.00.00.00

Destination address = valeur décimale 255.255.255.255 et valeur hexa ff ff ff ff

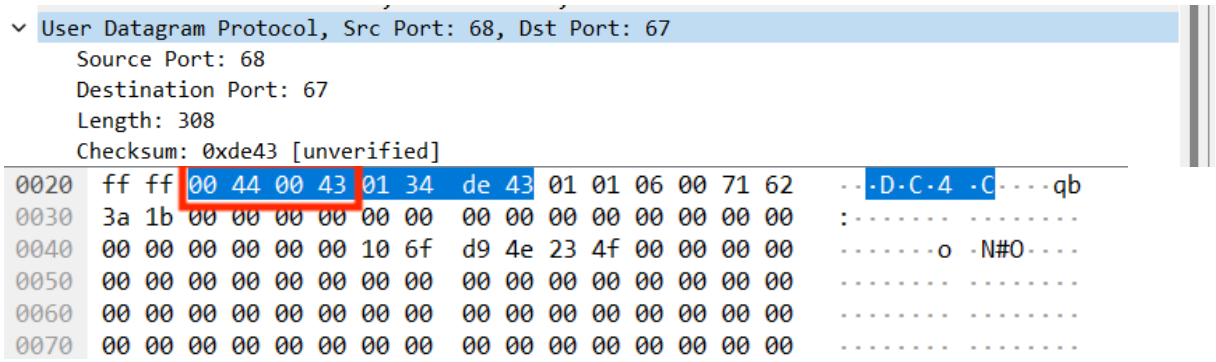
- **Que signifie la valeur contenue dans le champ adresse IP source ?**

  L'adresse IP source 00 00 00 00 est utilisé par un client DHCP pour demander une adresse IP au serveur DHCP. Elle indique donc l'absence d'une adresse IP attribuée au client.

- **Caractérisez l'adresse de couche 3 de destination de cette trame :**

  L'adresse de couche 3 destination sert à l'envoie en diffusion elle envoie à toute les machines d'un réseau local.

➔ Sélectionnez, comme dans la figure ci-dessous, l'en-tête du datagramme UDP contenu dans la trame DHCP Discover.



(Et de datagramme UDP : 8 octets (les 4 1er sont les ports Source et Destination)

- Quel est le nom du champ de l'en-tête de transport permettant le démultiplexage de protocole :

  Le champ permettant le démultiplexage des protocoles est le port destination en l'occurrence le port 67 ou 0043 correspondant à DHCP.

- Quel est le port UDP utilisé par le client DHCP ? identifier la valeur hexadécimale correspondante figurant dans le volet des octets :

  Le port utilisé par le serveur DHCP est le port source 68 ou 0044

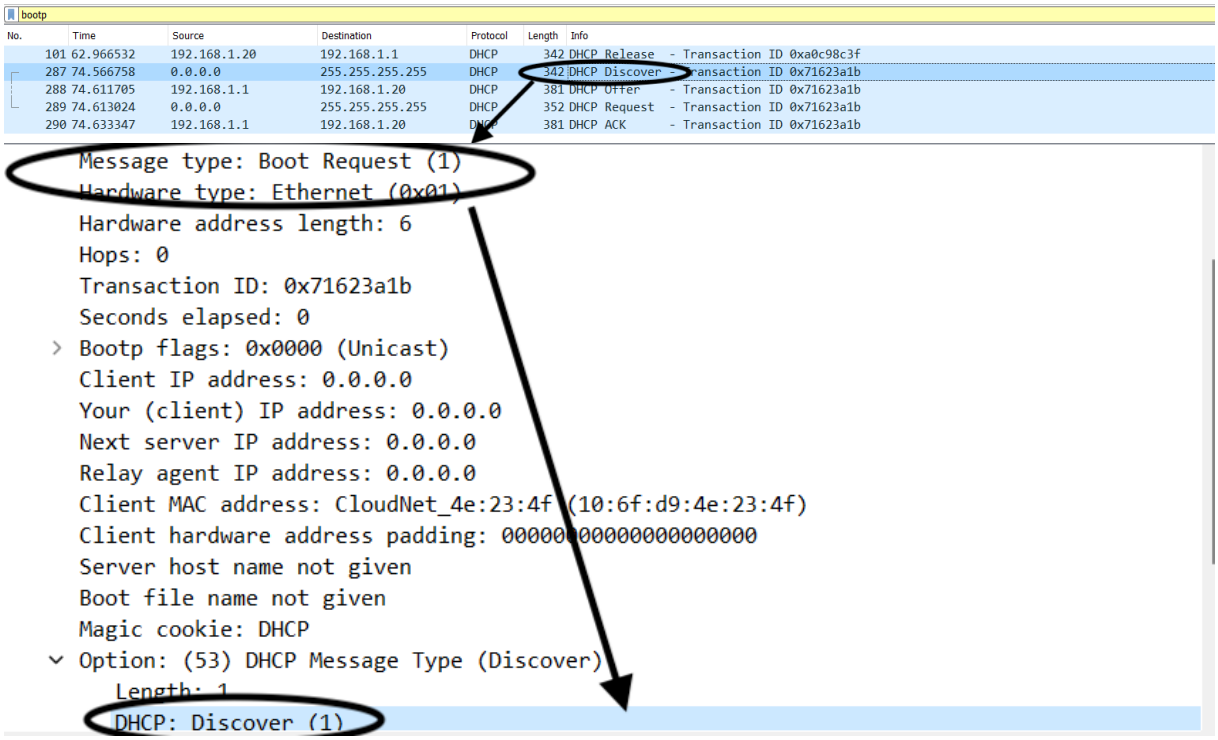
- Quel est le protocole applicatif encapsulé dans le datagramme UDP ?

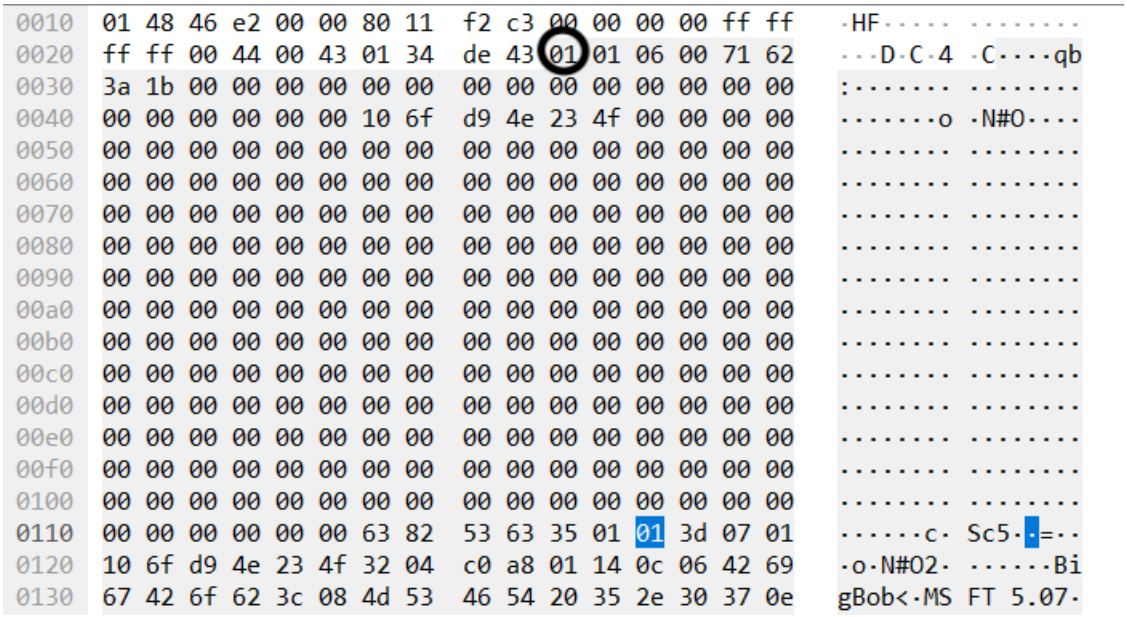
  Le protocole applicatif encapsulé dans le datagramme UDP est le protocole DHCP.

- Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client ?

  Le port utilisé par le serveur DHCP pour écouter et recevoir la requête client est le port 68 ou 0044.

➔ Sélectionnez la section Bootstrap Protocol contenu dans la trame DHCP Discover :





```
0010  01 48 46 e2 00 00 80 11  f2 c3 00 00 00 00 ff ff   ·HF····· ········
0020  ff ff 00 44 00 43 01 34  de 43 01 01 06 00 71 62   ···D·C·4 ·C····qb
0030  3a 1b 00 00 00 00 00 00  00 00 00 00 00 00 00 00   :····... ........
0040  00 00 00 00 00 00 10 6f  d9 4e 23 4f 00 00 00 00   .......o ·N#O····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ......c· Sc5··=··
0120  10 6f d9 4e 23 4f 32 04  c0 a8 01 14 0c 06 42 69   ·o·N#O2· ......Bi
0130  67 42 6f 62 3c 08 4d 53  46 54 20 35 2e 30 37 0e   gBob<·MS FT 5.07·
```

(Données applicatives BOOTP à partir de l'octet de position 0x10 ligne 0020)