# TP 4- Analyse des trames DHCP avec Wireshark

Nesrine EL AHMADI

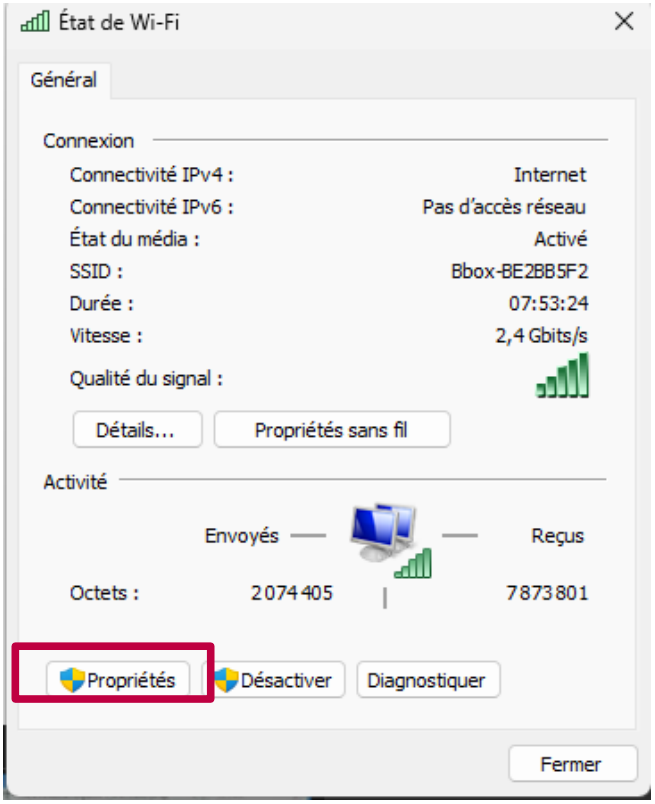
**BTS SIO**

## Table des matières

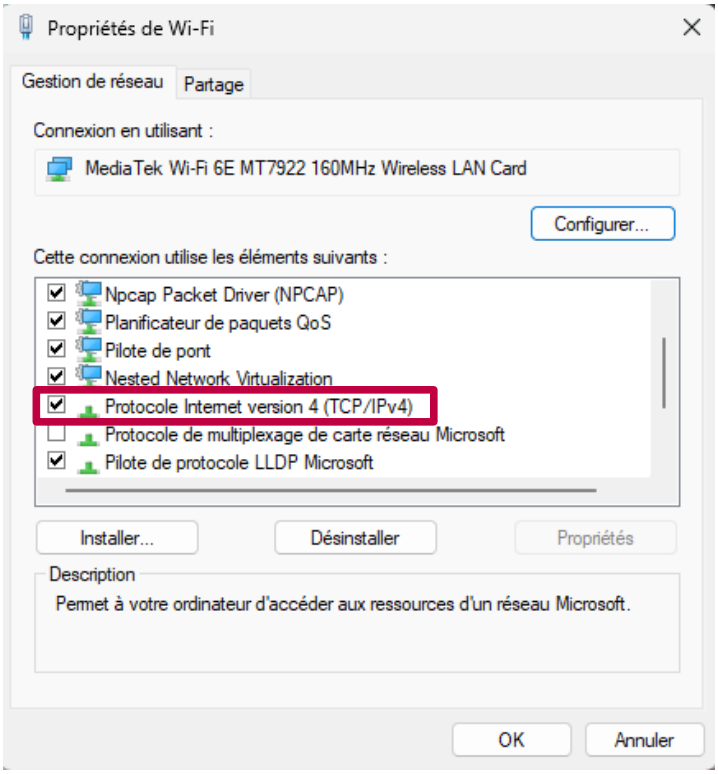
1. Capture de trames DHCP avec Wireshark.....2
2. Étude de trame DHCP DISCOVER.....11

# 1. Capture de trames DHCP avec Wireshark

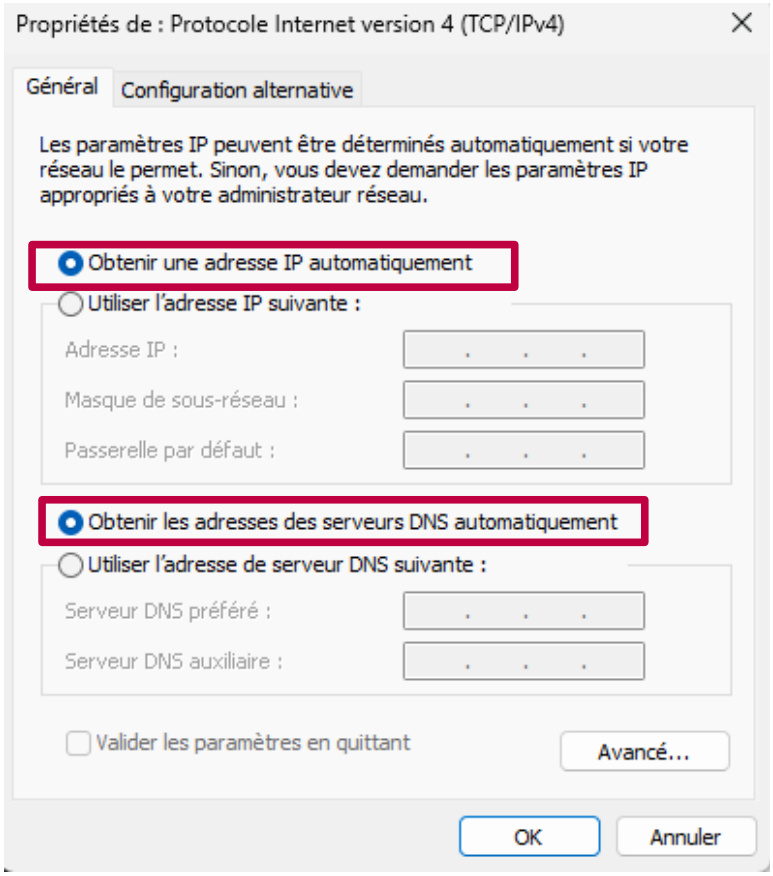
On modifie les propriétés TCP/IPv4 de manière à obtenir automatiquement les paramètre IP du serveur DHCP  ( Capture 1, 2 et 3) .




*Capture 1*

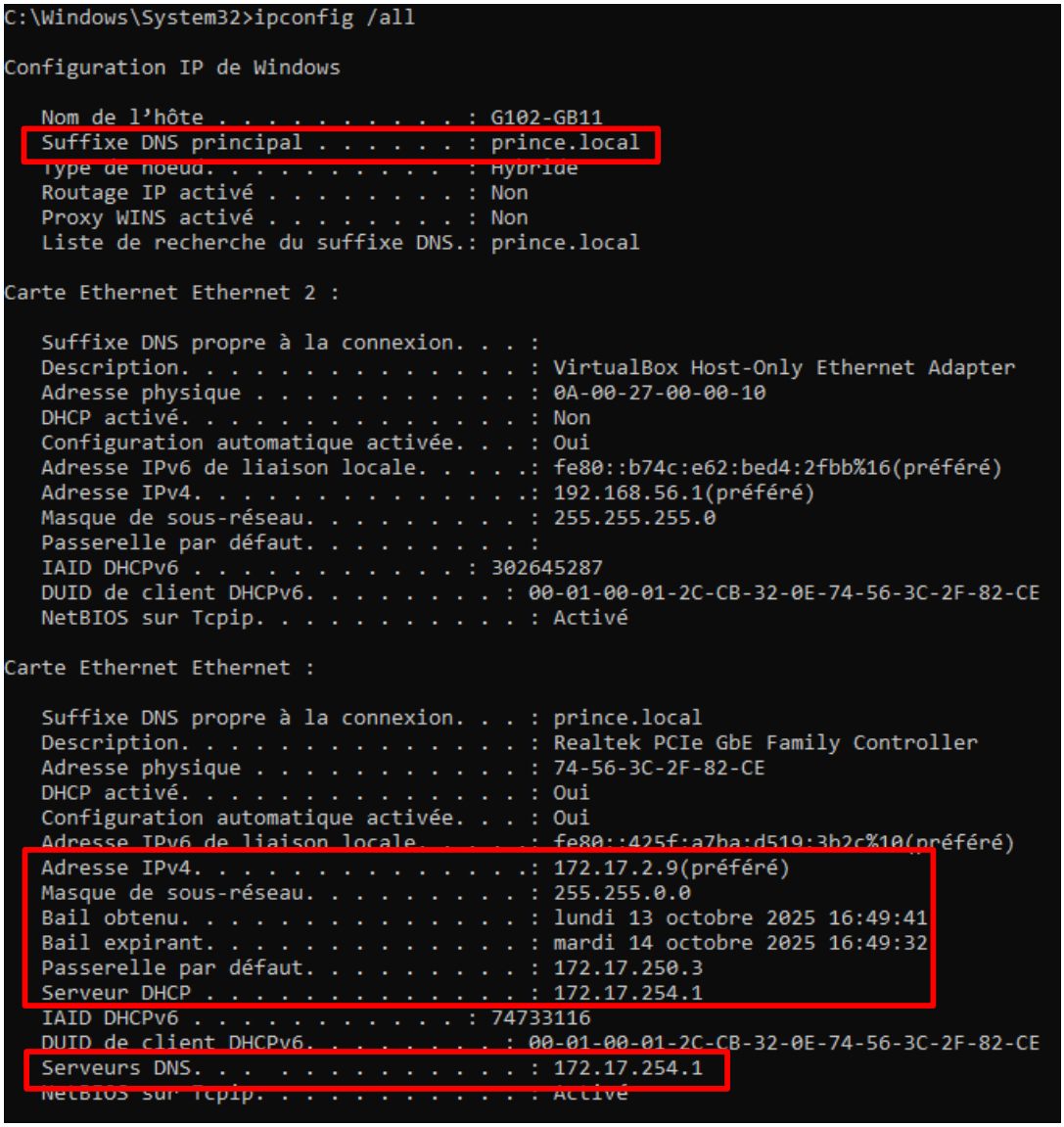



*Capture 2*

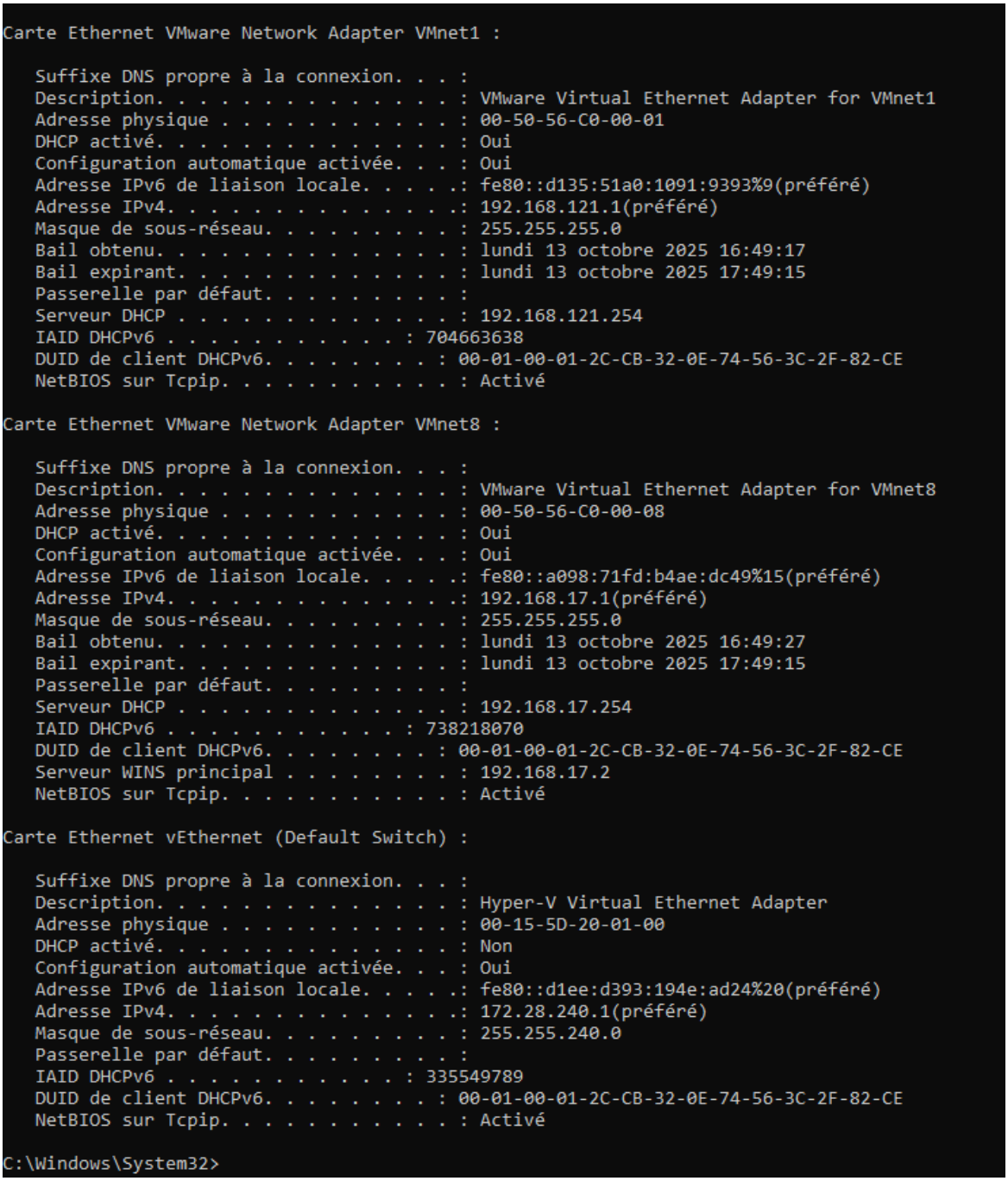

Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Configuration alternative
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
Masque de sous-réseau :
Passerelle par défaut :
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

*Capture 3*

→On exécute la commande **ipconfig /all** dans l'invite de commande( capture 4).




*Capture 4*




## *Capture 4*

---Quelle est **l'adresse IP** attribuée par le **serveur DHCP** a votre poste de travail ?

- Adresse IP : 172.17.2.9

---D'autres éléments sont inscrits :

- DHCP activé : OUI
- Masque de sous- réseau : 255.255.0.0

▪ Bail obtenu : lundi 13 octobre 2025 16:49:41

▪ Bail expirant : mardi14 octobre 2025 16:49:32

▪ Passerelle par défaut : 172.17.250.3

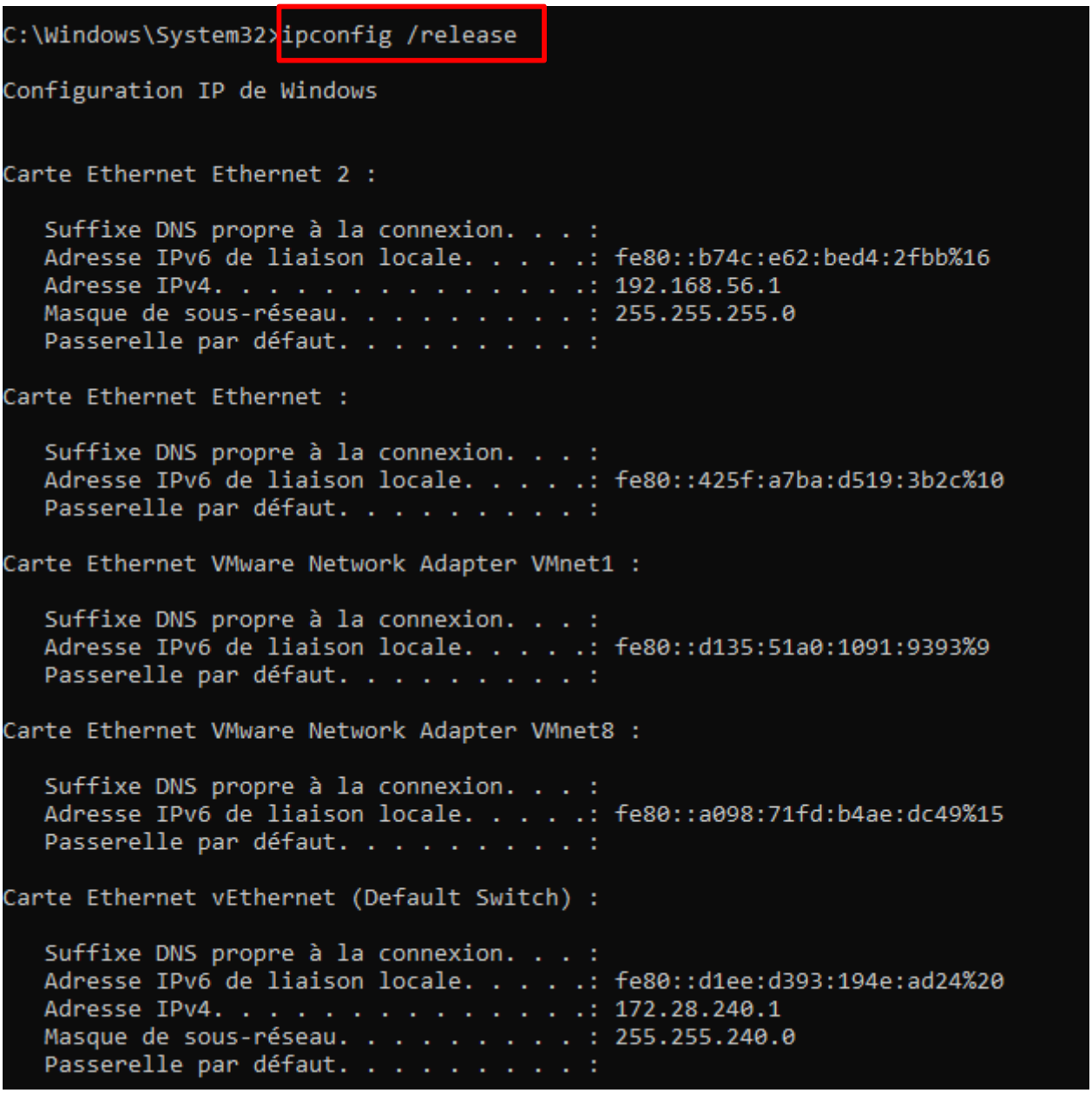
▪ Serveur DHCP :172.17.254.1

Serveur DNS :172.17.254.1

→On exécute la commande **ipconfig** a titre de comparaison (capture 5).

```
C:\Windows\System32>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::b74c:e62:bed4:2fbb%16
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::425f:a7ba:d519:3b2c%10
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.9
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.3

Carte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d135:51a0:1091:9393%9
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.121.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::a098:71fd:b4ae:dc49%15
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.17.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d1ee:d393:194e:ad24%20
   Adresse IPv4. . . . . . . . . . . . . .: 172.28.240.1
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . :
```

→Après avoir exécuté  la commande **ipconfig /release** dans l'invite de commande on obtiens certaines  informations ( capture 6 ) :




*Capture 6*

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : ?

→ On exécute ensuite la commande **ipconfig /renew** ( capture 7 ) et obtiens :

```
C:\Windows\System32>ipconfig /renew

Configuration IP de Windows


Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::b74c:e62:bed4:2fbb%16
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : prince.local
   Adresse IPv6 de liaison locale. . . . .: fe80::425f:a7ba:d519:3b2c%10
   Adresse IPv4. . . . . . . . . . . . . .: 172.17.2.9
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 172.17.250.3

Carte Ethernet VMware Network Adapter VMnet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d135:51a0:1091:9393%9
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.121.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::a098:71fd:b4ae:dc49%15
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.17.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet vEthernet (Default Switch) :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
```

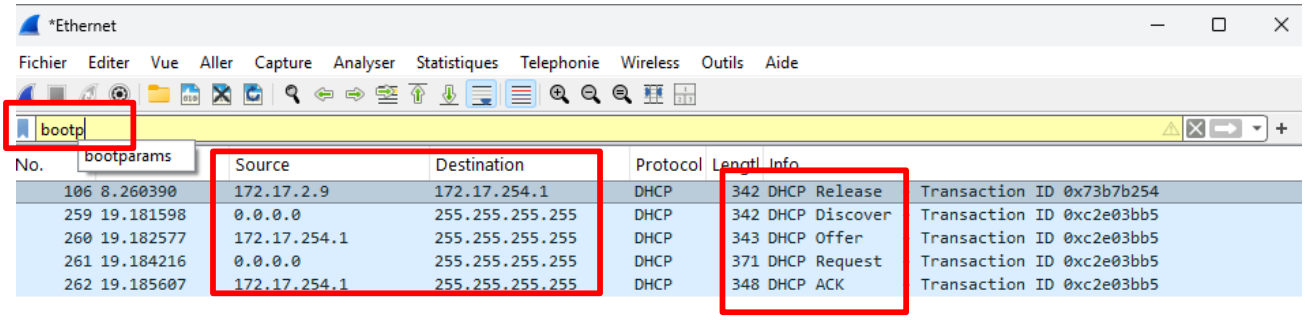
*Capture 7*

Adresse IPv4 : 192.168.56.1

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : ?

→ On a fait une **capture de trames a l'aide de Wireshark** tout en générer un peu de trafic entre le poste de travail et le serveur DHCP. On a ensuite limité l'affichage des trames a celle encapsulant les protocoles DHCP ( Capture 8 ) .

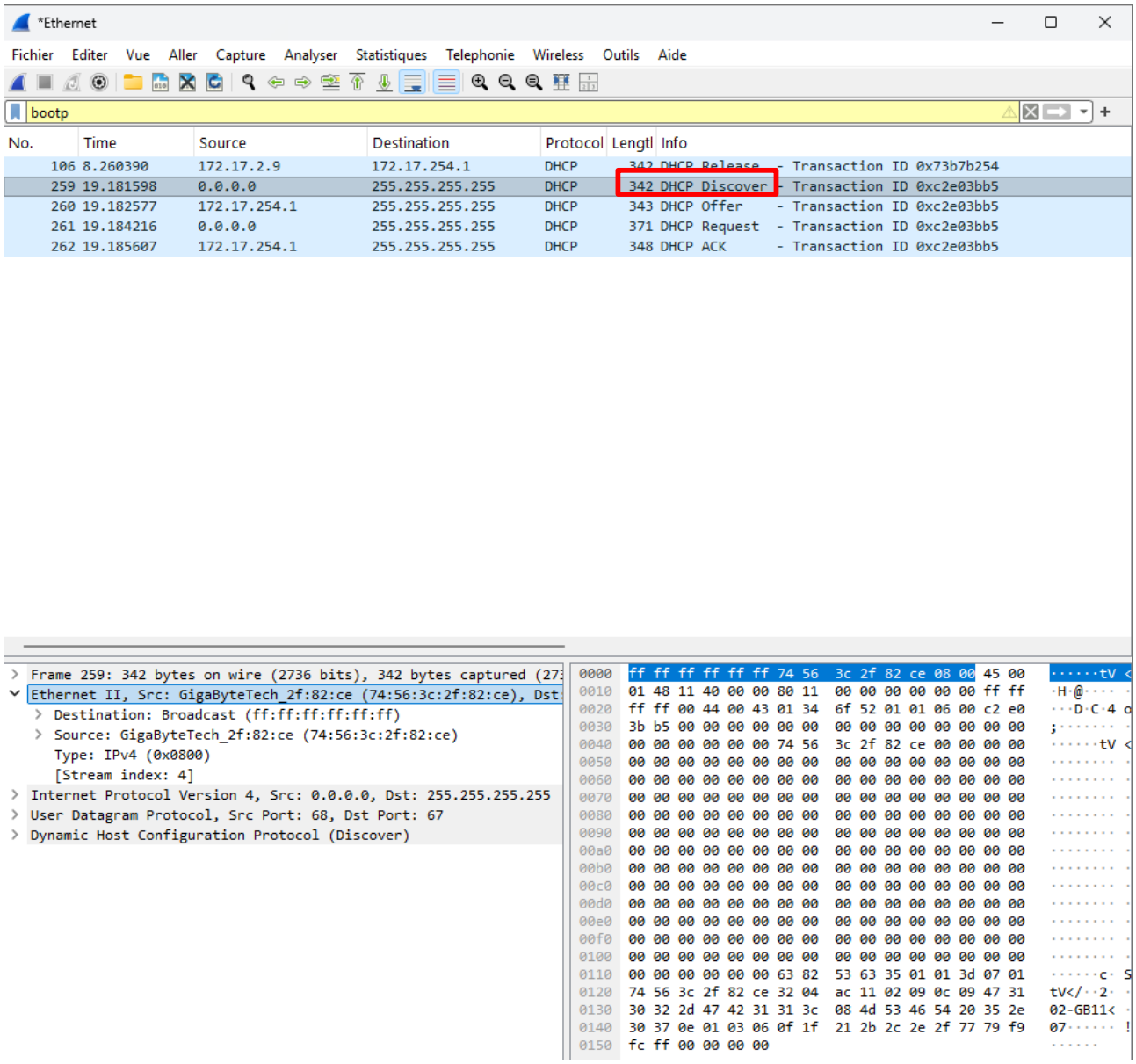



*Capture 8*

On obtient plusieurs trames comme **DHCP RELEASE** ( généré par la commande ipconfig /release), **DHCP DISCOVER** (conséquence de la commande ipconfig / renew), **DHCP OFFER** ( réponse du serveur ), **DHCP REQUEST** (réponse du client pour faire valider son adresse IP) et la trame **DHCP ACK** ( pour confirmer l'attribution)

## 2. Étude de trame DHCP DISCOVER

→ On s'intéresse a la trame **DHCP DISCOVER** et on développe l'en-tête Ethernet ( capture 9)




*Capture 9*

**---A l’aide de la l’en-tête de trame DHCP DISCOVER on identifie l’adresse MAC source et destination.**

- MAC source : 74:56:3c:2f:82:ce
- MAC destination: ff:ff:ff:ff:ff:ff

**--- Caractérisez l’adresse de couche 2 de destination de cette trame :**

C’est une adresse en broadcast c’est  dire qu’elle est diffusé a tout le monde afin de savoir a qui est ce qur l’addresse MAC appartient appartient.

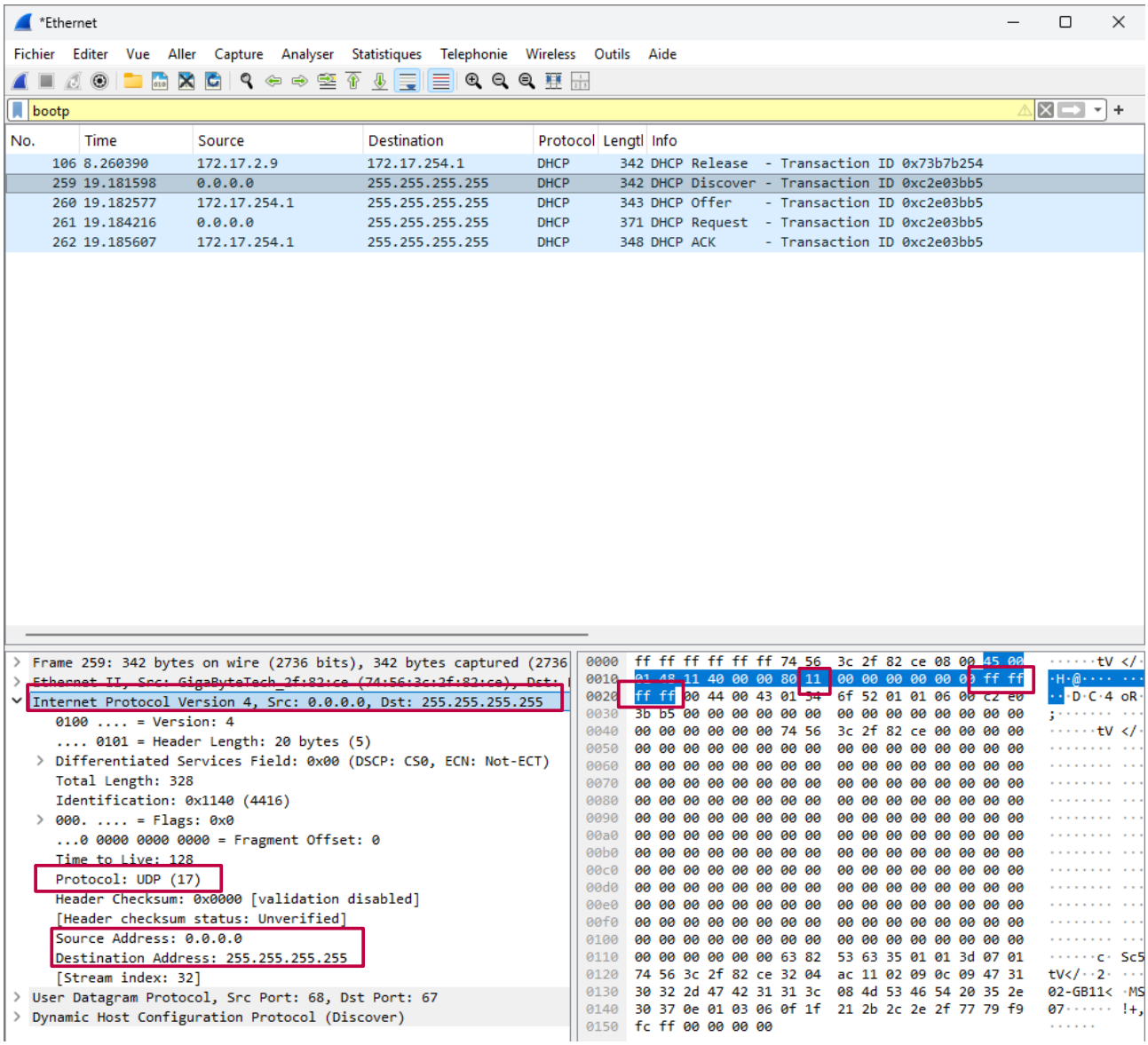
**--- Quel est le champ qui suit immédiatement les deux adresses MAC ? Quelle valeur contient-il ? Que signifie t-elle ?**

Ce qui se trouve juste après les deux adresse MAC est le champ Ethertype ( de 2 octets ) permettant le démultiplexage. Celui nous indique le protocole supérieur encapsulé dans la trame. Dans ce cas sa valeur est de 0x0800 donc IPv4.

**---Quels sont les protocoles inclus dans cette trames ?**

Dans une trame DHCP, plusieurs protocoles sont encapsules. Tout commence par Ethernet  qui transporte les adresses MAC et le champs Ethertype qui nous informe que le protocole supérieur encapsulé dans la trame est le protocole IPv4. Ensuite le datagramme UDP qui assure le transport entre les ports 67 et 68. Enfin, le protocole DHCP est encapsulé au niveau applicatif.

→ On sélectionne **l'en-tête IP** contenu dans la trame DHCP Discover ( Capture 10 )




*Capture 10*

---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 .

▪C'est le champ protocole qui nous indique le protocole de couche 4 qui est encapsulé dans le paquet IP.

Champ d’en-tête IP :

▪Version : 4 ( IPv4)

▪IHL (val.déci ) : 20 octets (en hexadécimal) :0x14

▪Protocole ( val.déci ) :17 (en hexadécimal) : 0x11

▪Source adresse (val. Déci. ) : 0.0.0.0 (client sans IP) (en hexadécimal) : 00 00 00 00

▪Destination adresse (val déci ) : 255.255.255.255 (en hexadécimal) : FF FF FF FF

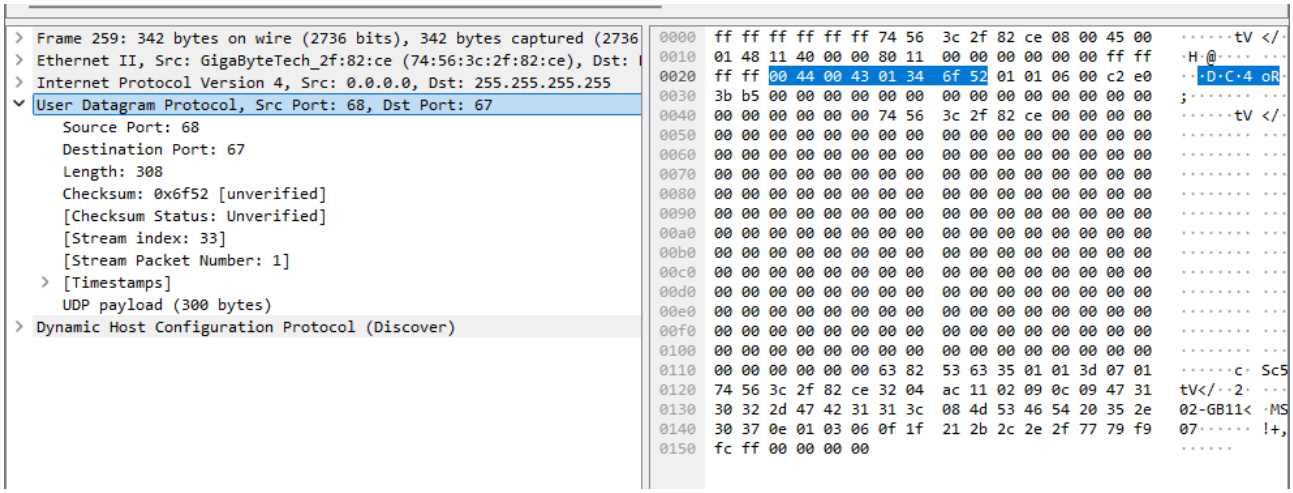
**---Que signifie la valeur contenue dans le champ Adresse IP source ?**

▪Elle indique que le client ne possède pas encore d’adresse IP. Il envoie une requête DHCP pour obtenir dynamiquement une configuration réseau l’adresse 0.0.0.0 est utilisé temporairement pour la communication avec le serveur DHCP.

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

▪L’adresse de couche 3 destination une adresse de broadcast . Elle permet d’envoyer sa requête a tous les hôtes du réseau, notamment le serveur DHCP sans connaître leur adresse IP .

→ On sélectionne **l’en-tête du datagramme UDP** contenue dans la trame DHCP DISCOVER (capture 11)




*Capture 11*

---**Quel est le nom de l’en-tête de transport permettant le démultiplexage de protocoles ?**

▪C’est l’en-tête de segment ou ici datagramme car le protocole après le démultiplexage est UDP et on parle de datagramme UDP.

**--- Quel est le port UDP utilisé par le client DHCP ?**

▪C’est le port 68 qui est utilisé par le client DHCP pour envoyer sa requête DHCP. ( La requête vient du client)

**---Identifier la valeur hexadécimale correspondante figurant dans le volet des octets :**

→ 00 44

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

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

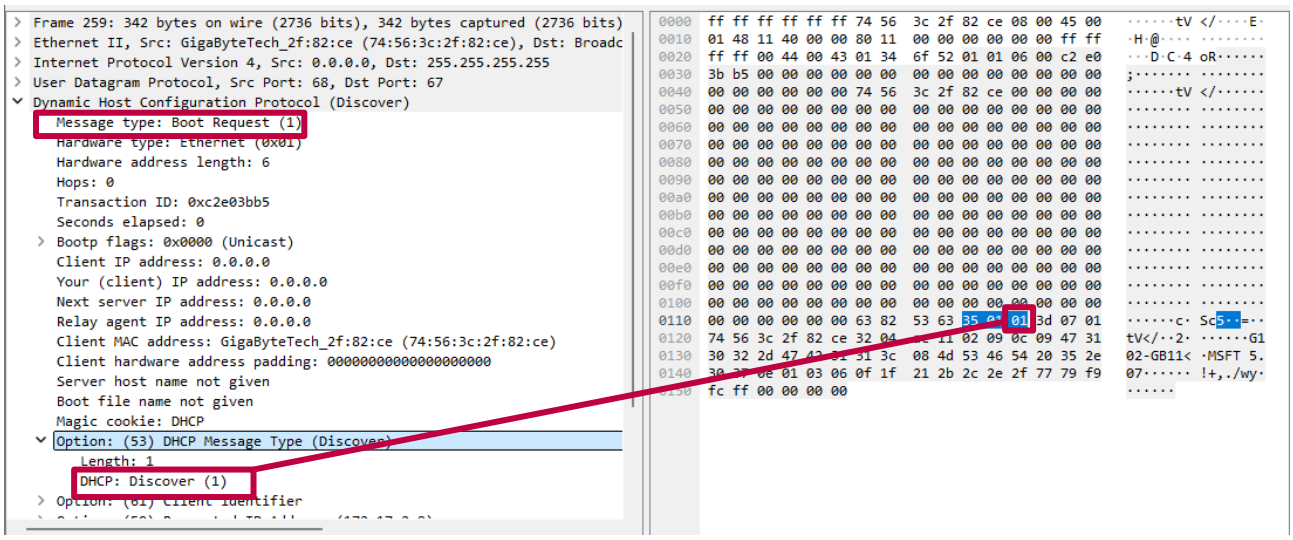
**---Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client ?**

C’est le port 67 (utilisé par le serveur )

**---Identifier la valeur hexadécimale correspondante figurant dans le volet des octets.**

→ 0x0043

→ On sélectionne la section Bootstrap Protocole contenu dans la trame DHCP DISCOVER ( Capture 12 )




*Capture 12*

La valeur 1 montre que le message est un Boot Request. Si elle avait était de 2 ca signifierai qu'il sagit d'un boot Reply.