TP 4 : Analyse de Trames DHCP avec Wireshark

SOMMAIRE :

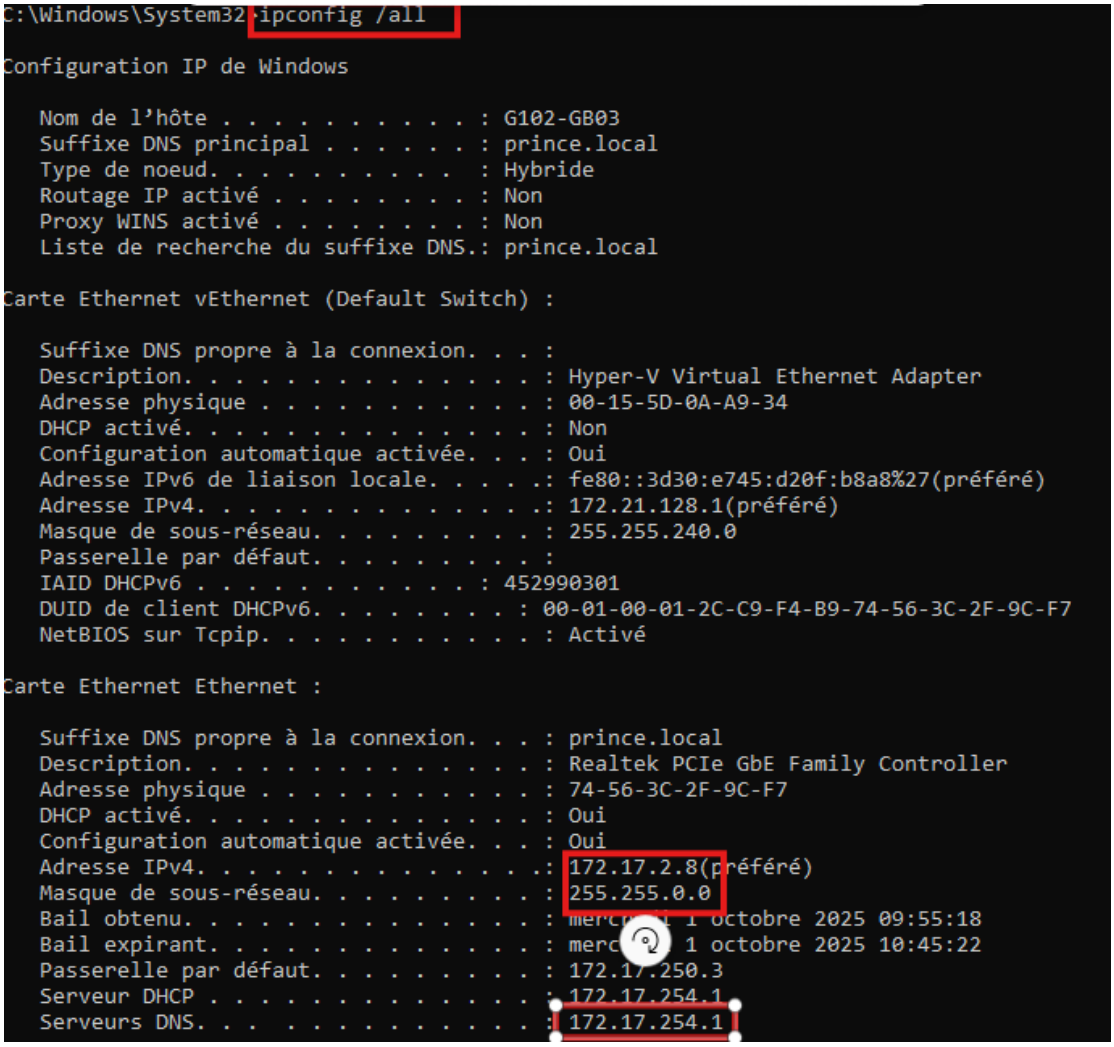
Objectifs :

L'objectif de ce TP est de **comprendre et analyser le fonctionnement du protocole DHCP (Dynamic Host Configuration Protocol)** à travers la capture et l'étude des trames réseau échangées entre un **client** et un **serveur DHCP**.
À l'aide de **Wireshark**, nous observons les différentes étapes du processus d'attribution d'adresse IP (Discover, Offer, Request, Ack) et identifions les **champs importants** des en-têtes **Ethernet, IP et UDP**.

---

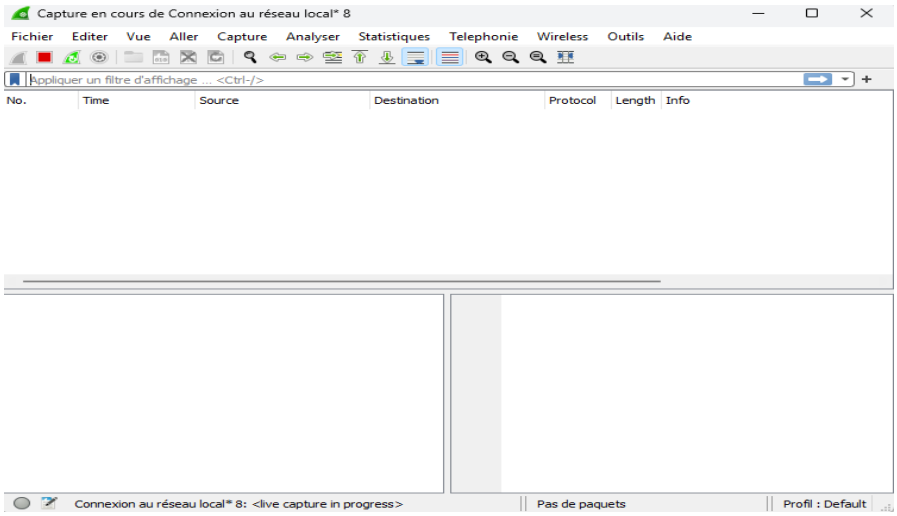
1. Processus d’acquisition d’une adresse IPv4

La commande **`ipconfig /all`** permet d’afficher **toutes les informations de configuration réseau** d’un ordinateur sous Windows.



2. Capture de trames DHCP avec Wireshark

J'initie une capture de trames réseau à l'aide de **Wireshark**. Depuis l'**invite de commandes Windows**, j'exécute ensuite les commandes successives permettant de libérer et de renouveler l'adresse IP attribuée par le serveur DHCP.

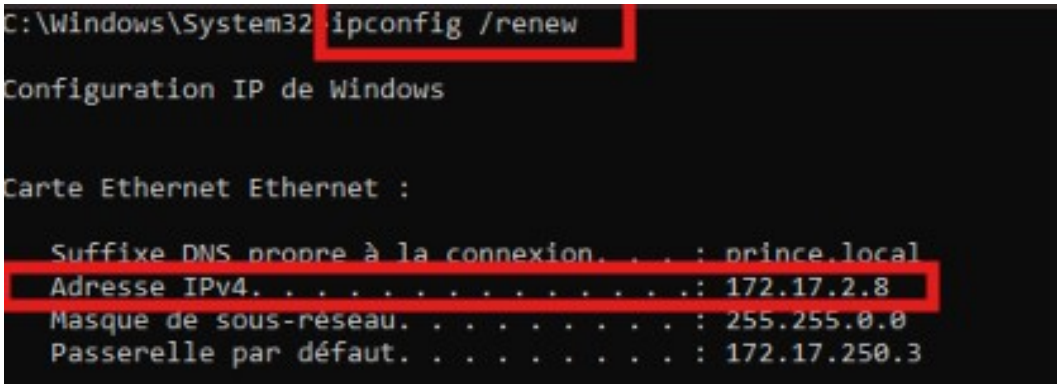


`ipconfig /release` libère l'adresse IP actuelle du poste

L'ordinateur se déconnecte temporairement du réseau, car il n'a plus d'adresse IP.

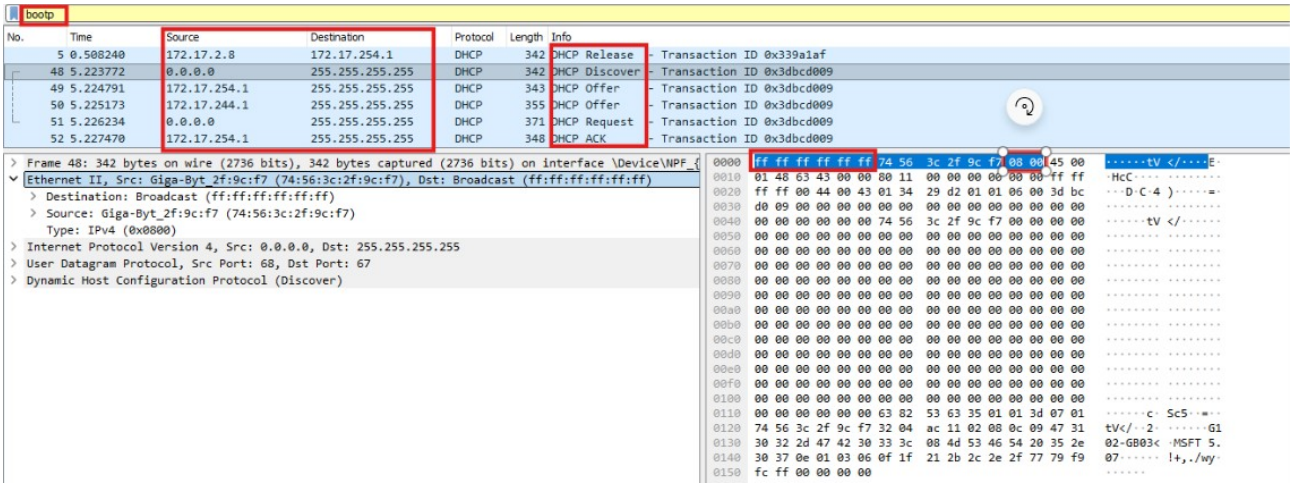
```
C:\Windows\System32>ipconfig /release

Configuration IP de Windows


Carte Ethernet vEthernet (Default Switch) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::3d30:e745:d20f:b8a8%27
   Adresse IPv4. . . . . . . . . . . . . .: 172.21.128.1
   Masque de sous-réseau. . . . . . . . . : 255.255.240.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::e973:6dc5:ff6f:f6e%13
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

`ipconfig /renew` demande ensuite une **nouvelle adresse IP** au serveur DHCP



Paramètre	Valeur
Adresse IP attribuée	172.17.2,8
DHCP activé	Oui
Masque de sous-réseau	255.255.0.0
Bail obtenu	01/10/2025 – 09:55:18
Bail expirant	01/10/2025 – 10:45:22
Passerelle	172.17.2.8
Serveur DHCP	172.17.254.1 *(serveur « ROI »)*
Serveur DNS	172.17.254.1

3. Analyse des trames DHCP



Interprétation de la capture DHCP dans Wireshark

- La **partie supérieure** de la fenêtre montre la **liste des trames capturées**, avec pour chaque paquet :
  le **numéro**, le **temps**, la **source**, la **destination**, le **protocole** et une **description** du message DHCP (Discover, Offer, Request, Ack).
  → Elle permet de suivre le **dialogue complet** entre le client et le serveur DHCP.

- La **partie centrale** affiche le **détail du paquet sélectionné**, c'est-à-dire les informations des **différentes couches du modèle TCP/IP** : **Ethernet**, **IP**, **UDP** et **DHCP**.
  → Elle sert à analyser les champs des en-têtes et à comprendre comment les données sont encapsulées.

- La **partie inférieure** montre la **trame en hexadécimal**, c'est-à-dire les **données brutes** telles qu'elles ont circulé sur le réseau.
  → Elle permet de vérifier les valeurs exactes des champs (adresses, ports, identifiants…).

Pourquoi avoir filtré `bootp` ?

Le protocole **DHCP** est en réalité une **extension du protocole BOOTP**.
En filtrant `bootp` dans Wireshark, on affiche donc **uniquement les trames DHCP/BOOTP**, ce qui permet :

- De **se concentrer sur les échanges DHCP** (Discover, Offer, Request, Ack),

4. Étude du message DHCP

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

L'adresse MAC de destination est **inconnue** et contient la **valeur maximale en hexadécimal** : `ff:ff:ff:ff:ff:ff`
Cette valeur correspond à une **adresse de broadcast**, utilisée pour diffuser la trame à **tous les hôtes du réseau local**.
Elle est employée ici car le client ne connaît pas encore l'adresse du serveur DHCP.

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

Le champ situé juste après les adresses MAC est le **champ EtherType**, qui indique le **protocole de couche supérieure** encapsulé dans la trame Ethernet.

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

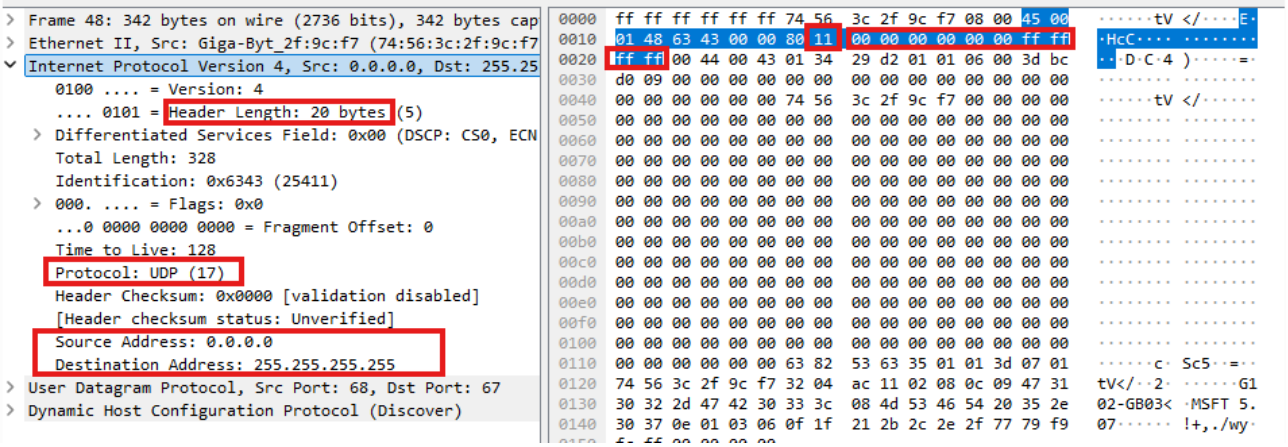
Le champ EtherType contient la valeur **0x0800**, ce qui signifie que la trame transporte un **paquet IPv4**.
Cela indique donc que la couche supérieure utilisée est le **protocole Internet (IP)**.

▪ Quels sont les protocoles inclus dans cette trame ?

Les protocoles encapsulés dans cette trame, du plus bas au plus haut niveau, sont :

- **Ethernet II** → couche liaison (couche 2)

- **IPv4** → couche réseau (couche 3)
- **UDP** → couche transport (couche 4)
- **DHCP** → couche application (couche 7)



▪ Champ qui indique le protocole de transport :

Le protocole de transport est indiqué dans le **champ “Protocole”** de l’**en-tête IP**
Sa **valeur est 17 en décimal** (soit **0x11 en hexadécimal**), ce qui correspond au **protocole UDP**.
Les messages **DHCP** transitent donc via **UDP**

- **Champs d’en-tête IP :**

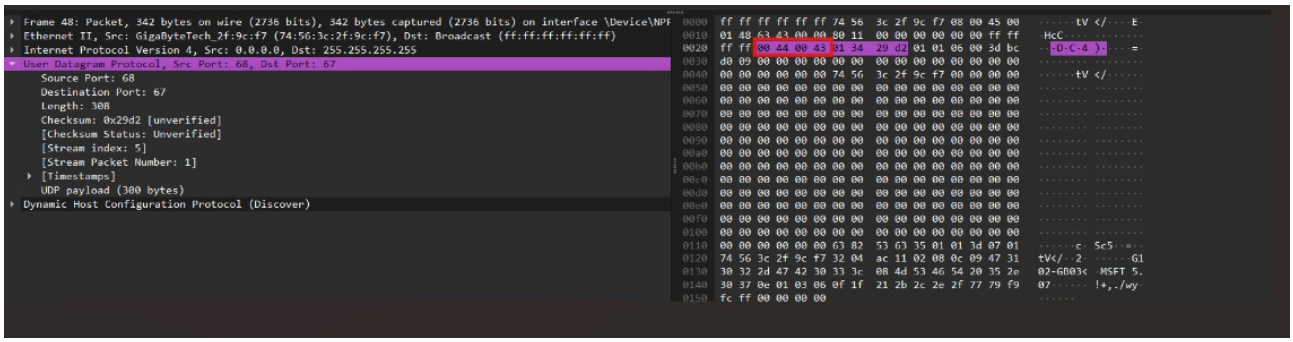
Champ	Valeur décimale	Valeur hexadécimale	Interprétation
Version	4	—	IPv4
IHL	5	0x05	Longueur d’en-tête = 5 × 4 = **20 octets**
Protocole	17	0x11	**UDP**
Adresse source	0.0.0.0	00 00 00 00	Le client n’a pas encore d’adresse IP
Adresse destination	255.255.255.255	FF FF FF FF	Adresse de **broadcast** (diffusion)

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

L’adresse IP source est **0.0.0.0**.
Cette valeur indique que le client **n’a pas encore d’adresse IP** attribuée (il n’a pas encore reçu de configuration du serveur DHCP).
Il utilise donc **0.0.0.0** comme adresse temporaire pour se présenter sur le réseau.

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

L’adresse IP de destination est **255.255.255.255**, c’est-à-dire **l’adresse de broadcast IPv4**.
Elle permet d’envoyer le message à **tous les hôtes du réseau local**, afin que le serveur DHCP puisse recevoir la requête du client même sans connaître encore son adresse IP.



Le nom du champ de l’en-tête de transport permettant le **démultiplexage de protocole** est **Le champ Port**

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

Identifier la valeur hexadécimale correspondante figurant dans le volet des octets (octets de position 0×02 et 0×03 ligne 0020) :

- **Port UDP client DHCP :** 68
- **Valeur hexadécimale :** 0x0044
- **Explication :** Ce port (68) est réservé au **client DHCP (BOOTP client)** pour l'envoi des requêtes vers le serveur.

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

- **Protocole applicatif :** DHCP
- **Nom complet :** *Dynamic Host Configuration Protocol*
- **Rôle :** Permet au client d'obtenir automatiquement une adresse IP et les paramètres réseau depuis un serveur DHCP.

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

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

- **Port UDP serveur DHCP :** 67
- **Valeur hexadécimale :** 0x0043
- **Explication :** Le port 67 est utilisé par le **serveur DHCP (BOOTP server)** pour recevoir les requêtes envoyées par les clients.

▪ **Que contient le premier champ de la section Bootstrap Protocol pour cette trame DHCP ?**

- **Valeur :** 1
- **Signification : Boot Request**
- **Explication :**

Le champ “op” (operation code) du protocole BOOTP vaut :

- **1 → Boot Request** : message émis par le **client** vers le serveur
- **2 → Boot Reply** : message émis par le **serveur** vers le client

Dans le cas d’un **DHCP Discover**, le client cherche un serveur DHCP, donc c’est bien un **Boot Request**.

▪ **Quelle est la valeur de l’option DHCP indiquant le type de message DHCP ?**

- **Valeur :** 1
- **Signification : DHCP DISCOVER**
- **Explication :**

Cette option indique le type précis du message DHCP :

- 1 → **DHCP Discover** (recherche d’un serveur)