*Wireshark Lab : DHCP*

**Objectif :** Observer le fonctionnement du protocole DHCP et analyser les différents échanges entre un client et un serveur DHCP à l'aide de Wireshark.

1. **Relâchement de l'adresse IP avec ipconfig /release**
   - **Action :** Dans la fenêtre de commande (cmd), entrez la commande ipconfig /release.
   - **But :** Cette commande force votre machine à libérer son adresse IP actuelle. En réponse, l'adresse IP de votre interface réseau sera mise à 0.0.0.0 (si le client est configuré en DHCP).

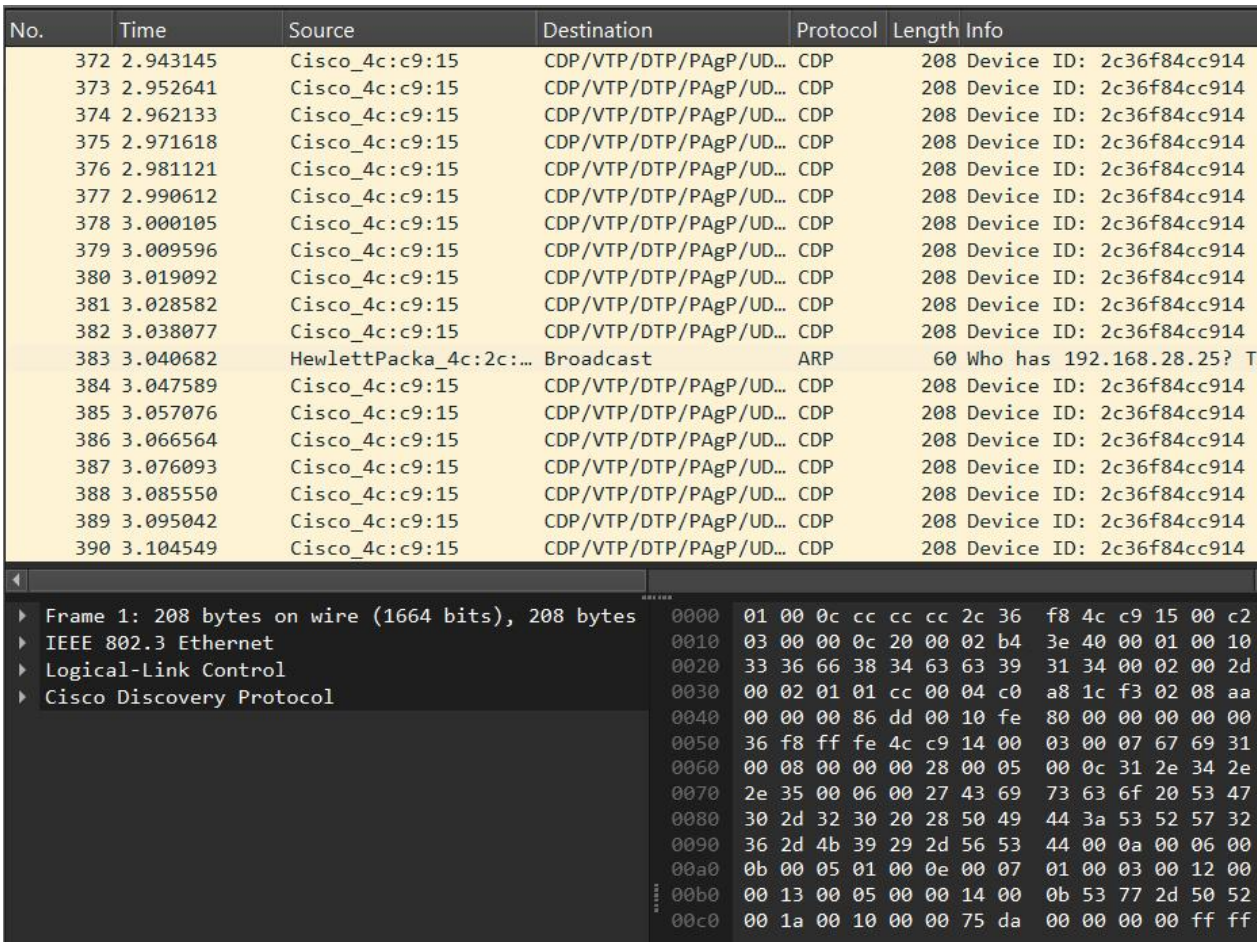
```
C:\Users\laulf>ipconfig /release

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion au réseau local* 1 lorsq
son média est déconnecté.
Aucune opération ne peut être effectuée sur Connexion au réseau local* 2 lorsq
son média est déconnecté.
Aucune opération ne peut être effectuée sur Wi-Fi lorsque
son média est déconnecté.
Aucune opération ne peut être effectuée sur Connexion réseau Bluetooth lorsque
son média est déconnecté.

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::5054:97d3:8464:98ad%3
   Passerelle par défaut. . . . . :

Carte réseau sans fil Connexion au réseau local* 1 :

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

Carte réseau sans fil Connexion au réseau local* 2 :

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

Carte réseau sans fil Wi-Fi :

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

Carte Ethernet Connexion réseau Bluetooth :

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

2. **Lancer Wireshark**

- **Action :** Démarrez Wireshark et sélectionnez l'interface réseau appropriée pour capturer les paquets
- **But :** Vous allez capturer tous les paquets transitant par votre machine, y compris ceux liés à DHCP.

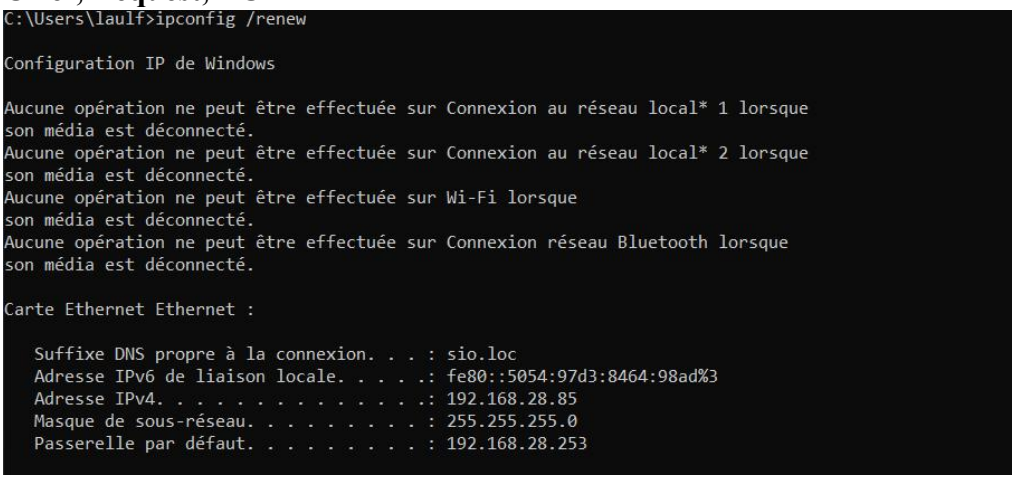
**3. Commencer la capture des paquets**

- **Action :** Démarrez la capture sur Wireshark en cliquant sur l'interface réseau appropriée.
- **But :** Cela permettra d'enregistrer tous les paquets réseau, ce qui inclut les échanges DHCP.




**4. Lancer la commande ipconfig /renew**

- **Action :** Dans la fenêtre de commande (cmd), entrez ipconfig /renew.
- **But :** Cette commande force la machine à envoyer une requête DHCP pour obtenir une nouvelle adresse IP. Le processus DHCP de quatre étapes sera lancé : **Discover, Offer, Request, ACK**.



**5. Vérifier la nouvelle adresse IP avec ipconfig**

- **Action :** Après l'échange DHCP, entrez ipconfig dans la fenêtre de commande.
- **But :** Vérifiez que votre machine a reçu une nouvelle adresse IP attribuée par le serveur DHCP.

**6. Effectuer un deuxième ipconfig /renew**

- **Action :** Tapez à nouveau ipconfig /renew dans la fenêtre de commande.
- **But :** Demander une nouvelle adresse IP au serveur DHCP. Cela vous permet de voir s'il y a un changement ou non (par exemple, si l'adresse IP a été renouvelée ou réattribuée).

**7. Effectuer un ipconfig /release**

- **Action :** Tapez ipconfig /release dans la fenêtre de commande.
- **But :** Relâchez à nouveau l'adresse IP attribuée à votre machine.

**8. Effectuer un ipconfig /renew à nouveau**

- **Action :** Exécutez à nouveau ipconfig /renew pour demander une nouvelle adresse IP après avoir libéré l'adresse précédente.
- **But :** Cela permet de voir si le serveur DHCP attribue la même ou une nouvelle adresse IP.

**9. Stopper la capture Wireshark**

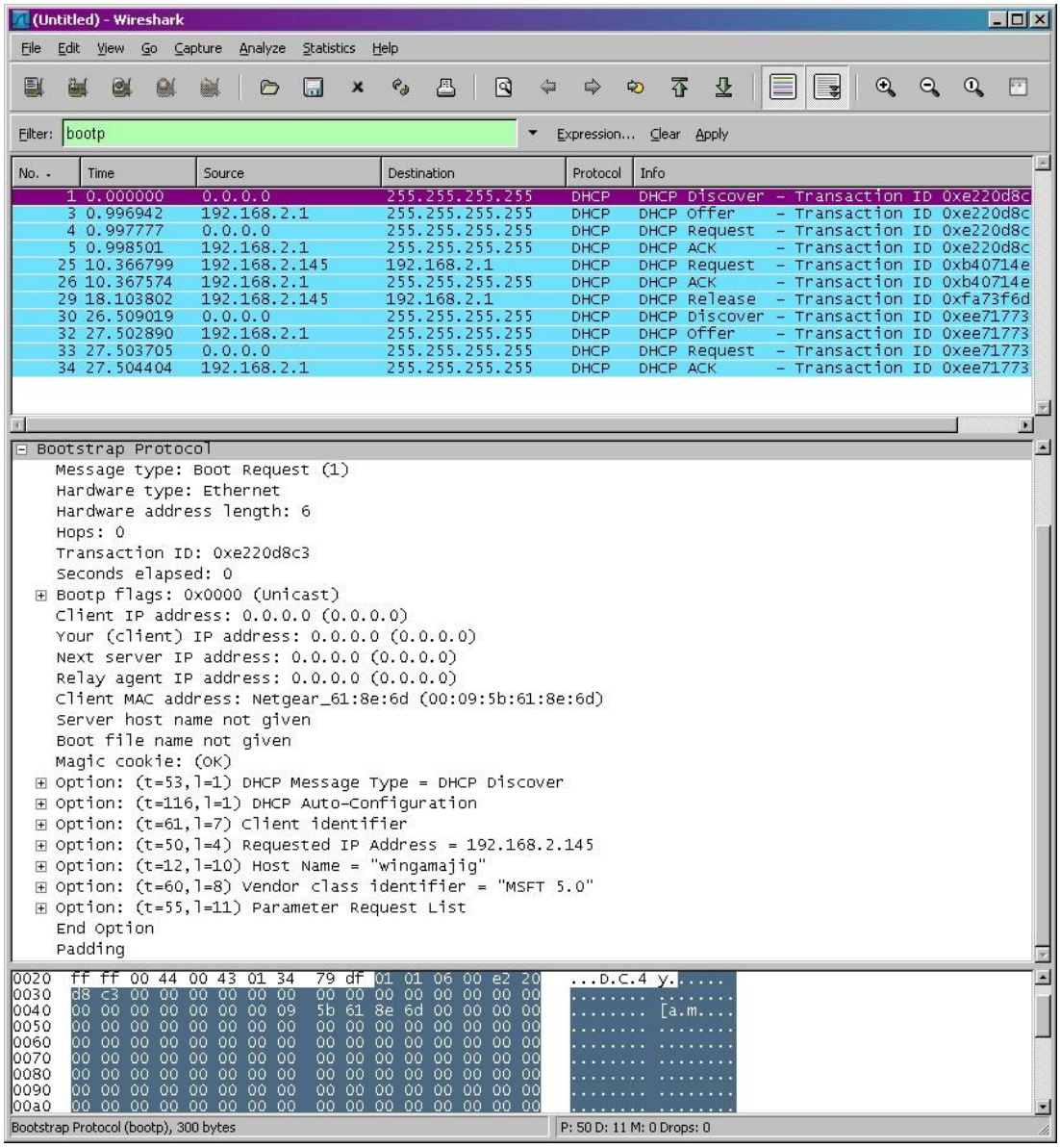
- **Action :** Une fois que vous avez effectué toutes les étapes ci-dessus et observé les paquets échangés, arrêtez la capture dans Wireshark.
- **But :** Cela vous permet d'analyser les paquets capturés et de répondre aux questions suivantes.

**Filtrage des paquets DHCP dans Wireshark**

- **Filtre Wireshark :** Dans la barre de filtre en haut de Wireshark, entrez dhcp ou bootp pour filtrer et ne visualiser que les paquets DHCP.
- **Ports utilisés par DHCP :** DHCP utilise les ports UDP **67** (serveur) et **68** (client).

Vous devriez observer les échanges de paquets suivants :

- **DHCP Discover** (Client → Serveur)
- **DHCP Offer** (Serveur → Client)
- **DHCP Request** (Client → Serveur)
- **DHCP ACK** (Serveur → Client)



Faites une capture d'écran et répondez aux questions suivantes :

**1. DHCP utilise-t-il UDP ou TCP ?**

- **Réponse :** Dhcp utilise UDP

**2. Diagramme des quatre premiers paquets (Discover/Offer/Request/ACK)**

1. **DHCP Discover :**
    - **Source :** 0.0.0.0
    - **Destination :** 255.255.255.255
    - **But :**
2. **DHCP Offer :**
    - **Source :** 192.168.28.253
    - **Destination :** 192.168.28.85
    - **But :**
3. **DHCP Request :**
    - **Source :** 0.0.0.0
    - **Destination :** 2555.255.255.255
    - **But :**
4. **DHCP ACK :**
    - **Source :** 192.168.28.253
    - **Destination :** 192.168.28.85
    - **But :**

**3. Quelle est l'adresse Ethernet de votre hôte ?**

- **Réponse :** 255.255.255.255

**4. Différence entre le message DHCP Discover et le message DHCP Request**

- Le message **DHCP Discover :** demande
- Le message **DHCP Request :** accept

**5. Valeur du Transaction-ID dans les quatre premiers paquets DHCP**

- **Transaction-ID** :0x49b4e6f0

**6. Valeur IP dans les datagrammes IP pendant l'échange (avant l'attribution de l'adresse IP)**

- **Réponse :** 0xa1d6

**7. Quelle est l'adresse de votre serveur DHCP ?**

- **Réponse :** 192.168.18.253

**8. Quelle adresse IP vous est proposée dans le message DHCP Offer ?**

- **Réponse (**"Yours DHCPOFFER" ou "Your IP address") :

**9. Y a-t-il un relais entre l'hôte et le serveur DHCP ?**

- **Réponse (Gateway IP address) :255.255.255.0**

**10. Objectif du masque dans le message DHCP Offer**

- **Réponse :**

**11. Intérêt du « lease time »**

- **Réponse : c'est le temps d'on l'offre du dhcp reste actif cela permet au dhcp de pouvoire attribuer l'adresse a un autre poste si il y a trop de client par rapport aux ip**

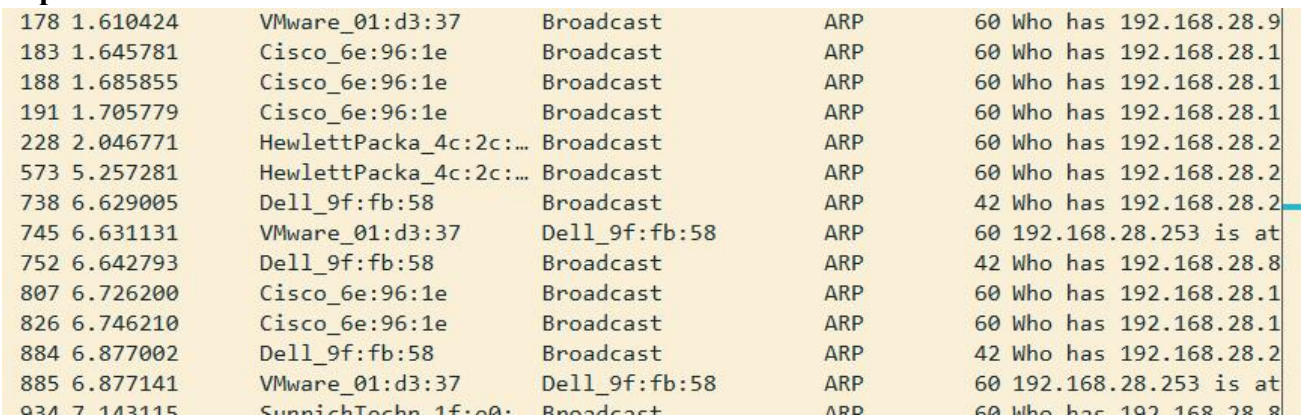
- **Sa valeur : 51 2 hours**

**12. Objectif du message DHCP Release**

- **Réponse :** cela permet au dhcp derevoquer un adresse pour la reatribuer

**13. Désactivez le filtre bootp. A-t-il eu des échanges ARP pendant l'échange DHCP ?**

- **Réponse :** oui



| | | | | | |
|---|---|---|---|---|---|
| 178 | 1.610424 | VMware_01:d3:37 | Broadcast | ARP | 60 Who has 192.168.28.9 |
| 183 | 1.645781 | Cisco_6e:96:1e | Broadcast | ARP | 60 Who has 192.168.28.1 |
| 188 | 1.685855 | Cisco_6e:96:1e | Broadcast | ARP | 60 Who has 192.168.28.1 |
| 191 | 1.705779 | Cisco_6e:96:1e | Broadcast | ARP | 60 Who has 192.168.28.1 |
| 228 | 2.046771 | HewlettPacka_4c:2c:… | Broadcast | ARP | 60 Who has 192.168.28.2 |
| 573 | 5.257281 | HewlettPacka_4c:2c:… | Broadcast | ARP | 60 Who has 192.168.28.2 |
| 738 | 6.629005 | Dell_9f:fb:58 | Broadcast | ARP | 42 Who has 192.168.28.2 |
| 745 | 6.631131 | VMware_01:d3:37 | Dell_9f:fb:58 | ARP | 60 192.168.28.253 is at |
| 752 | 6.642793 | Dell_9f:fb:58 | Broadcast | ARP | 42 Who has 192.168.28.8 |
| 807 | 6.726200 | Cisco_6e:96:1e | Broadcast | ARP | 60 Who has 192.168.28.1 |
| 826 | 6.746210 | Cisco_6e:96:1e | Broadcast | ARP | 60 Who has 192.168.28.1 |
| 884 | 6.877002 | Dell_9f:fb:58 | Broadcast | ARP | 42 Who has 192.168.28.2 |
| 885 | 6.877141 | VMware_01:d3:37 | Dell_9f:fb:58 | ARP | 60 192.168.28.253 is at |
| 934 | 7.143115 | SunnichTechn_1f:e0: | Broadcast | ARP | 60 Who has 192.168.28.8 |