**TP1 Analyse du protocole DHCP avec Wireshark**

**Objectif**: étudier le protocole DHCP, qui assure l'attribution automatique de configuration IP, par l'analyse de trames avec Wireshark.

**Condition de réalisation :**

Ordinateur portable (Wifi) ou fixe relié au réseau du lycée avec le logiciel Wireshark installé.

**1. configuration et test du réseau**

Votre ordinateur doit être en adressage automatique et disposer du logiciel Wireshark.

**2. Capture de trames du protocole DHCP**

Les commandes suivantes seront utilisées dans **votre ordinateur Windows** dans l’invite de commande. Si vous utilisez un autre OS utilisez les commandes équivalentes.

**ipconfig /all** : affiche la configuration complète des connexions réseau.

**ipconfig /release** : permet de libérer l'adresse IP attribuée par le DHCP

**ipconfig /renew** : permet de renouveler l'adresse IP attribuée par le DHCP.

* Lancez la commande **ipconfig /all**. Notez l'adresse MAC de l’ordinateur : **5C-FB-3A-19-E2-EE**
* Lancez la capture de trame avec Wireshark.
* Lancez la commande **ipconfig /release** pour libérer l'adresse IP
* Lancez la commande **ipconfig /renew** pour renouveler l'adresse IP.
* Arrêtez la capture dès que la configuration IP est obtenue.

Une image contenant texte, Police, nombre, logiciel

Description générée automatiquement

Appliquer le filtre « dhcp » ou « bootp » sur wireshark pour ne garder que les trames liées au DHCP.

* **Combien de trames sont échangées entre le serveur DHCP et le client pour l’obtention d’une adresse IP ?**

**4.**

* **Quels sont les types de trames échangées ?**

Vous allez étudier ces trames successivement en recherchant les valeurs des champs suivant (remplir les tableaux)

**Trame DHCP n°1**:

|  |  |
| --- | --- |
| Mac source | 5c :fb :3a :e2 :ed |
| Mac destination | FF.FF.FF.FF.FF |
| IP source | 0.0.0.0 |
| IP destination | 255.255.255.255 |
| Protocole de transport utilisé | UDP |
| Port source | 68 |
| Port destination | 67 |
| Nom du protocole de la couche application | DHCP |
| Type de message | Discover |

*A quoi correspond l'adresse Mac de destination ?*

**Trame DHCP n°2 :**

|  |  |
| --- | --- |
| Mac source | 00:15:5d:fa:d5:03 |
| Mac destination | 5c:fb:3a:19:e2:ed |
| IP source | 172.25.227.254 |
| IP destination | 172.25.227.20 |
| Protocole de transport utilisé | UDP |
| Port source | 67 |
| Port destination | 68 |
| Nom du protocole de la couche application | DHCP |
| Type de message | offer |

*Quels sont les paramètres de configuration offert par le serveur DHCP ?*

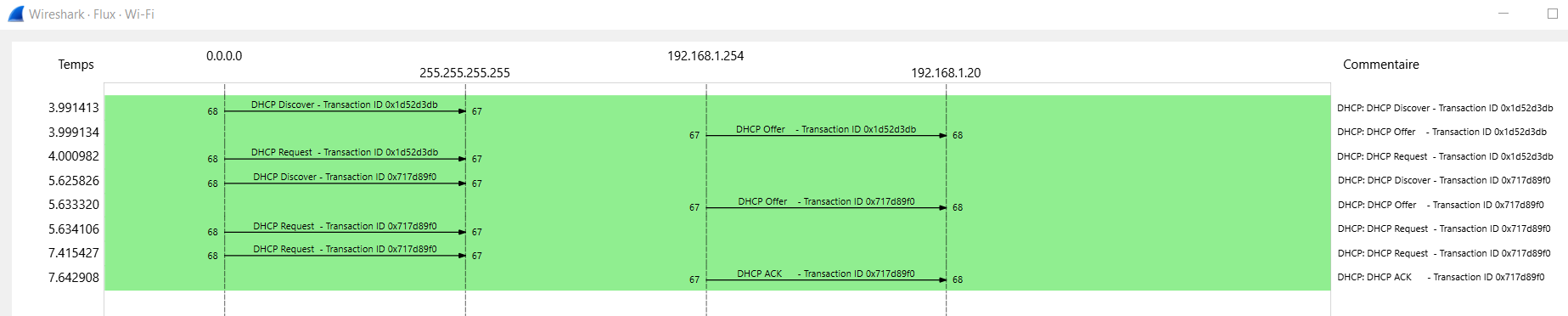
*Quelle est la durée du bail ?*

**Trame DHCP n° 3 :**

|  |  |
| --- | --- |
| Mac source | 5c:fb:3a:19:e2:ed |
| Mac destination | ff:ff:ff:ff:ff:ff |
| IP source | 0.0.0.0 |
| IP destination | 255.255.255.255 |
| Protocole de transport utilisé | UDP |
| Port source | 68 |
| Port destination | 67 |
| Nom du protocole de la couche application | DHCP |
| Type de message | Request |

**Trame DHCP n°4 :**

|  |  |
| --- | --- |
| Mac source | 00:15:5d:fa:d5:03 |
| Mac destination | 5c:fb:3a:19:e2:ed |
| IP source | 172.25.227.254 |
| IP destination | 172.25.227.20 |
| Protocole de transport utilisé | UDP |
| Port source | 67 |
| Port destination | 68 |
| Nom du protocole de la couche application | DHCP |
| Type de message | ACK |

Aller dans le menu « statistiques » puis « graphique des flux ». Afficher le graphique des flux correspondant à votre capture puis commenter le.

A quoi correspond « transaction ID » ?

Les ID de transaction sont des identifiants uniques pour chaque transaction, comme un numéro de confirmation de commande.