le compte-rendu du TP N°2 et TP N°3 réalisés sur Wireshark

YOUSSEF HACHIMI

ARI

GROUP 2

N : 31

2024/2025 EST BM

Travaux Pratiques : TP 2

Exercice 1 : Examiner la trame Ethernet

a) Que signifie cette ligne ?

la trame capturée est une **trame Ethernet II**. Cela signifie que le protocole de liaison de données utilisé est **Ethernet**, et le format de trame est compatible avec Ethernet II, qui est couramment utilisé pour les réseaux IP.

b) Décrivez les informations définies dans cette ligne.

Les informations de cette ligne incluent :

- **Destination:** Adresse MAC de destination (souvent une passerelle, un routeur ou un autre périphérique).
- **Source:** Adresse MAC de la carte réseau de l'ordinateur ayant généré la trame.
- **Type:** Identifie le protocole de couche supérieure utilisé. Par exemple :
    - 0x0800 pour IPv4
    - 0x0806 pour ARP
    - 0x86DD pour IPv6

c) Quelle est l'adresse MAC de la carte réseau de l'ordinateur et celle de la passerelle par défaut ?

Pour trouver ces adresses :

- L'adresse **MAC source** correspond à la carte réseau de votre ordinateur.
- L'adresse **MAC destination** correspond à celle de la passerelle par défaut (vérifiez dans la trame capturée).

Exemple :

- **MAC source** : 00:1A:2B:3C:4D:5E
- **MAC destination** : 5E:4D:3C:2B:1A:00

d) Quel est le type de protocole de couche supérieure utilisé ?

Le type est indiqué dans le champ Type.

Si c'est une trame ICMP, cela signifie que le protocole de couche supérieure est **ICMP**.

Exercice 2 : Analyse du protocole IP

6. Quelles sont les couches OSI présentes dans les trames capturées ?

Les couches OSI visibles dans Wireshark pour une trame IP incluent

- **Couche 2 (Liaison)** : Ethernet .
- **Couche 3 (Réseau)** : IP.
- **Couche 4 (Transport)** : TCP, UDP ou ICMP.
- **Couche 7 (Application)** : HTTP, DNS, etc
- **7. Quelle est la version d'IP utilisée ?**

La version d'IP se trouve dans le champ **Version** de l'en-tête IP :

- 4 pour IPv4.
- 6 pour IPv6.

8. Quelle est la taille de l'en-tête IP ?

La taille de l'en-tête IP se trouve dans le champ **Header Length**. Elle est mesurée en multiples de 4 octets.

9. Quelle est la taille des données ?

La taille des données se calcule ainsi :

Taille des données = Longueur totale - Taille de l'en-tête IP

10. Le paquet IP est-il fragmenté ? Justifiez votre réponse.

Vérifiez dans le champ **Flags** de l'en-tête IP :

- Si le bit **MF (More Fragments)** est activé, le paquet est fragmenté.
- Si le champ **Fragment Offset** est non nul, c'est également une indication de fragmentation.

11. Quelle est la valeur du champ TTL ? Justifiez votre réponse.

Le champ **TTL (Time to Live)** est une valeur initialisée par l'expéditeur pour limiter le nombre de sauts qu'un paquet peut effectuer avant d'être détruit.

- Elle diminue de 1 à chaque passage par un routeur. Si elle atteint 0, le paquet est abandonné.

12. Quel est le protocole de niveau supérieur ? Par quelle valeur est-il identifié ?

Le protocole de niveau supérieur est indiqué dans le champ **Protocol** de l'en-tête IP.

- 6 pour TCP.
- 17 pour UDP.
- 1 pour ICMP.

13. Pouvez-vous retrouver les valeurs hexadécimales des adresses IP source et destination ?

Oui, les adresses IP source et destination apparaissent dans la section **Internet Protocol Version 4**

Exercice 3 : Analyse d'une connexion TCP

4. Combien y a-t-il de segments d'ouverture et de fermeture de la connexion ?

- L'ouverture d'une connexion TCP se fait en **3 étapes** (Handshake)
    1. **SYN**
    2. **SYN-ACK**
    3. **ACK**
- La fermeture d'une connexion se fait en **4 segments** :
    1. **FIN** (par le client).
    2. **ACK** (par le serveur).
    3. **FIN** (par le serveur).
    4. **ACK** (par le client).

5. Quels sont les numéros de port utilisés ? Justifiez votre réponse.

http : 80 , https : 403

- Le **port source** est un port aléatoire attribué par le client.
- Le **port destination** est le port du service auquel vous vous connectez

6. Vérifiez l'évolution des numéros de séquence et d'acquittements.

- Les numéros de séquence indiquent la position des octets transmis dans la connexion. 1000

- Les numéros d’acquittement (ACK) confirment la réception des octets par l’autre partie. 1001

7. Suivez le flux TCP avec "Follow TCP Stream".

Les numéros de port ne sont pas utilisés dans ICMP. À la place, les champs Type et Code définissent le rôle des messages ICMP.