Travaux Pratiques 3
Analyse de trames et fonctionnement des protocoles TCP/IP

L'objectif de ce TP est d'observer le fonctionnement des protocoles à travers l'analyse de trames Ethernet capturées grâce au logiciel Wireshark. Vous utiliserez *Wireshark* pour consulter les paquets fournis. Pour cela, vous pouvez vous reporter à cette introduction à l'analyse de trames.

1. Récupérez et décompressez l'archive `captures.zip` disponible sur Moodle. Celle-ci contient les captures de trames sur lesquelles vous allez travailler.
2. **Le protocole IP et ses associés**
   (a) Ouvrez le fichier `capture1.pcapng` et répondez aux questions suivantes :
      i. Quel est le protocole transporté par cette trame Ethernet et à quoi sert-il ?
      ii. Quelle est l'adresse MAC de destination utilisée par la trame numéro 1 ? pourquoi ?
      iii. Quelle est l'adresse MAC de destination utilisée par la trame numéro 2 ? pourquoi ?
      iv. Quelle est l'adresse IP pour laquelle cette requête à été émise ?
      v. Cette requête a été déclenchée par un `ping` de la machine `192.168.1.5` vers la machine `210.10.10.1`. Expliquez pourquoi ce n'est pas cette adresse IP qui est dans la requête et à quoi correspond l'adresse recherchée.
   (b) Ouvrez le fichier `capture2.pcapng` et répondez aux questions suivantes :
      i. Quels sont les protocoles présents dans cette capture ?
      ii. Quelle commande a déclenché cette communication ?
      iii. Quelle est la taille totale du paquet ?
      iv. Quelle est la taille de l'en-tête IP ?
      v. En supposant que la machine qui répond (trame 2) à utilisé un TTL initial de 64, combien de routeurs séparent les deux machines ?
   (c) Ouvrez le fichier `capture3.pcapng` et répondez aux questions suivantes :
      i. Quelle erreur est signalée par ce paquet ICMP ? qu'est-ce qui a provoqué cette erreur ?
      ii. Quelles sont les adresses des machines source et destination de la communication pour laquelle il y a eu un problème ?
      iii. Quelles est le type d'application qui était concerné ?
      iv. Quelle est l'adresse IP de la machine qui a signalé l'erreur et quel type de machine est-ce ?

   Pour la suite des captures, il est nécessaire de modifier la configuration de Wireshark : Edit → Preferences → Protocols.
   — pour IP, désactiver `Reassemble fragmented IP datagrams`
   — pour TCP désactiver `Relative sequence numbers and window scaling`

   (d) Ouvrez le fichier `capture4.pcapng`. Celui-ci correspond à un envoi de paquet ICMP request qui a été fragmenté. A partir de ces trames, répondez aux questions suivantes :

i. A quel niveau est géré la fragmentation ?

ii. Retrouvez le déplacement (*fragment offset*) dans la deuxième trame. A quoi correspond ce champs ? Déduisez-en la quantité de données qui se trouve dans la première trame.

iii. Trouvez le MTU du réseau qui transporte ces trames

iv. Comment être sûr que la dernière trame contient bien le dernier fragment ?

3. **La couche 4 : UDP et TCP**

(a) Ouvrez le fichier `capture5.pcapng` et répondez aux questions suivantes :

i. Quel est le protocole transporté par IP.

ii. Trouvez le port source et destination.

iii. Retrouvez la taille des données transportées. A partir des informations présentes dans l'en-tête IP, déduisez la taille de l'en-tête UDP.

(b) Ouvrez le fichier `capture6.pcapng` et répondez aux questions suivantes :

i. Quel est le protocole transporté par IP ?

ii. À quoi correspond l'échange observé et à quoi sert-il ?

iii. Quels sont les numéros de segment initiaux utilisés par chaque partie ?

iv. Au vu de l'échange, quel sera le *Maximum Segment Size* utilisé pour la communication TCP ? A quoi correspond cette valeur par rapport au MTU ?

(c) Ouvrez le fichier `capture6.pcapng` et répondez aux questions suivantes :

i. Quel est le numéro de séquence indiqué dans le premier segment ?

ii. Quel est le numéro d'acquittement dans le second segment ? Expliquez la différence.

iii. Quel drapeau est positionné dans l'entête TCP quand il y a des données ?

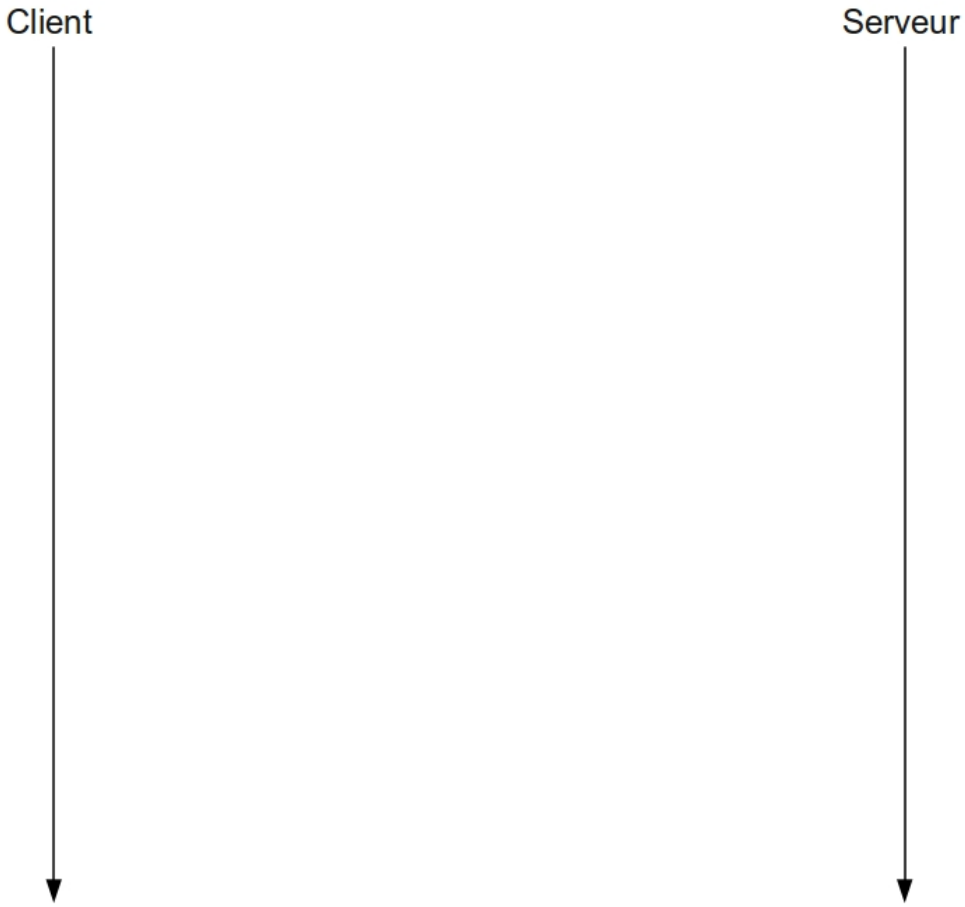
(d) Ouvrez le fichier `capture7.pcapng` et répondez aux questions suivantes :

i. A quoi correspond l'échange observé ?

4. **Interaction avec un service**

Récupérer sur Moodle l'archive `Serveur.jar`. Lancer ensuite le programme Java Serveur-Main contenu dans l'archive au moyen de la commande `java -jar Serveur.jar`

5. Lire le manuel de la commande `netstat`. Trouver le numéro de port sur lequel ce programme attend les connexions.
6. Avec la commande `nc` connectez vous sur le serveur et trouver la séquence de message nécessaire (i.e., **le protocole**) afin qu'il vous délivre une clé.
7. Tracez un diagramme temporel complet d'une session TCP avec ce serveur



8. Lire l'article de blog qui traite du contrôle de congestion de TCP.