TP2 : Analyse de protocoles avec Wireshark

I. But de TP

Le but de ce TP est de comprendre le modèle de transmission de TCP/IP en analysant le trafic généré par l'application Web. Nous utilisons le logiciel Wireshark qui est un « sniffer » réseau qui permet de récupérer tous les paquets qui passent par l'interface réseau. Ce logiciel nous permettra de comprendre la procédure d'encapsulation/dé-encapsulation du modèle TCP/IP qui rajoute des informations (signalisation) sous forme d'entête pour contrôler la transmission de données à chaque couche de ce modèle.

Wireshark affiche les paquets entrants et sortants selon leur date de réception et de transmission par la carte réseau. Il indique l'adresse IP source, l'adresse IP destination le type du protocole concerné par ce paquet ainsi que l'entête correspondant. Il offre d'autres fonctionnalités permettant le traitement et l'analyse de ces paquets, comme le filtrage, le calcul de statistiques, la représentation des diagrammes d'échange et des statistiques sous forme graphique.

- Dans cette séance, on souhaite analyser la façon dont les applications utilisent le réseau, en particulier le Web. Le WWW définit trois éléments :
  - ✓ le nommage des objets (URL - Uniform Resource Locator)
  - ✓ le protocole de transfert d'objets (HTTP - HyperText Transfer Protocol)
  - ✓ un langage pour la spécification des documents (HTML - HyperText Markup Language).
- Quand un utilisateur clique sur un lien dans un document présenté par un navigateur (Internet Explorer, Netscape, Chrome), celui-ci (navigateur ou client http) fait appel au protocole HTTP pour charger le document correspondant au lien. HTTP ouvre une connexion TCP au niveau transport. Le protocole TCP utilise l'interconnexion au niveau IP pour échanger des segments de données avec le site Web distant. Nous observerons les échanges de données à chaque niveau de protocoles au cours de l'accès à une page Web.
- A partir des données échangées, on va identifier certains paramètres et de tracer le diagramme d'échange à chaque couche :

1. Au niveau application : la version de protocole HTTP utilisé, le type de connexion demandé à la couche transport, le type de chargement de la page web complète ainsi que les informations spécifiées et négociées entre le client et le serveur.
2. Au niveau transport, on va identifier la phase d'établissement de connexion.

2. Travail à réaliser

- Utilisez les commandes **ifconfig** (ipconfig \all sous windows) et **route –n** pour afficher la configuration de votre machine dans le réseau afin de récupérer l'adresse IP de l'interface sur laquelle vous devez lancer la capture Wireshark.
- Lancer la capture Wireshark sur l'interface repérée.
- Accédez à la page du serveur **www.ec-lyon.fr** à l'aide de votre navigateur.
- Un fois la capture terminée, arrêtez l'observation du réseau et interprétez les résultats en répondant aux questions suivantes

3. HTTP Session

Sur la capture Wireshark :

1. Observer les échanges DNS et récupérer l'adresse IP du serveur web.
2. Maintenant, observez les échanges http et donner l'adresse IP de la machine avec laquelle votre station échange les données de la page web.
3. Quels sont les différents types de protocoles impliqués dans ce transfert ?
4. Combien de connexions TCP sont ouvertes ?
5. Faîtes le diagramme des échanges au niveau du protocole http entre le client et le serveur. Quels types de messages sont échangés au niveau http ? Dans le menu de Wireshark, trouvez la fonction qui vous permet de tracer le diagramme.
6. Observez l'en-tête et le corps de la première requête -réponse.
    a. Quelle est la méthode http utilisée pour télécharger la page Web ?
    b. Quelle est le code de retour du serveur ?
    c. Quelles sont les informations spécifiées par le client (le navigateur) ?
7. Quelle est la taille de la réponse ? Quelle est la version du protocole utilisée par le serveur ?

4. TCP

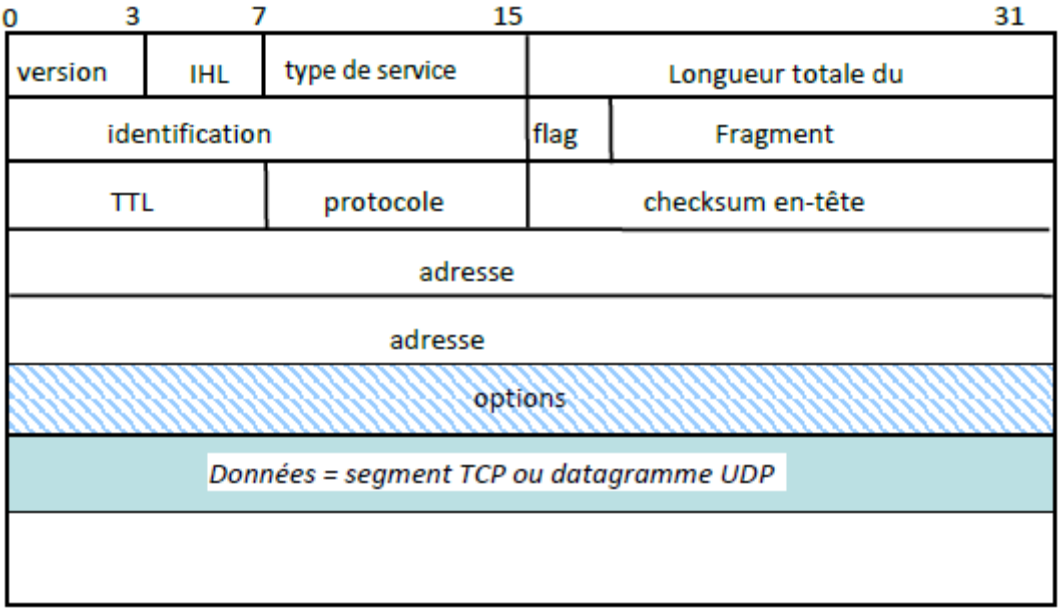
Sur la même capture, analysez le fonctionnement au niveau TCP.

1. Combien de connexions sont établies ? Donnez leurs numéros de port source et destination.
2. Quels sont les échanges au niveau du protocole TCP pour l'établissement de connexion ?
3. Repérez les commandes SYN. à quoi correspondent-ils ?
    a. Quels sont les paramètres de connexions échangés côté client et côté serveur ?
    b. Quel est le numéro de séquence initial (ISN) côté client et côté serveur ? MSS ?

5. IP

Regardez la même capture au niveau IP.

1. Comment les segments TCP sont-ils encapsulés dans des paquets IP ?
2. Quelles sont les adresses IP de ces paquets ?
3. Quelle est la longueur des paquets contenant les segments TCP de type SYN ?
4. Quelle est la longueur des paquets contenant les segments de données ?
5. Complétez le schéma de paquet IP ci-dessous pour le paquet contenant le segment d'établissement de connexion



6 Ethernet

Observez la même capture au niveau Ethernet

1. Comment les paquets IP sont encapsulés dans des trames Ethernet ?
2. Quelles sont les adresses Ethernet de ces paquets ?
3. Comment le contrôleur Ethernet sait à quel protocole il faut donner le contenu des trames pour le traitement ?