**ExoLab : Etude des couches du modèle OSI**

1. Installer le logiciel « Wireshark » sur votre PC.
2. Lancez une capture de trames sur votre carte réseau.
3. Utilisez votre navigateur pour générer du trafic sur votre interface réseau. Vous devez voir apparaitre les trames capturées, dans le cas contraire sélectionnez une autre interface réseau.
4. Quelles données voyez-vous apparaitre dans la fenêtre du haut ?

Protocol, source, destination, protocol, lenght, info

1. Donner des exemples de protocoles capturés.

TCP, ARP, UDP, ICMP, DNS, DHCP

1. Sélectionnez et analyser quelques trames capturées. Toutes les couches du modèle OSI sont-elles représentées dans la fenêtre du milieu ? Expliquez.

Toutes les couches ne sont pas présentes. Cela dépend du type des protocoles utilisés. Certaines trames ne contiennent pas de données.

1. Choisissez une trame dans laquelle le protocole HTTP est présent (il faut pour cela que vous génériez du trafic avec votre navigateur). Sélectionnez ensuite dans la fenêtre du milieu les différents protocoles présents dans cette trame (Ethernet, IP, TCP, HTTP).
2. Quels sont les 2 types d’échanges entre le client et le serveur web ?

Les requetes http des client vers le serveur

Les réponses de serveur

1. Comment sont encapsulées les données HTTP pour, finalement, constituer une trame circulant sur le réseau ?

La couche application envoie les données à la couche transport(4)

La couche transport ajoute ses propres données (n°port source et destinataire)

La couche réseau (3) ajoute ses propres données (IP source et Ip destination)

La couche Ethernet (2) ajoute ses propres données (MAC source et mac destination)

La couche physique (1) envoie les bits sur le support de transmission

1. Lancer une nouvelle capture, ouvrir CMD et effectuer un ping vers le serveur google.com.
2. Effectuer un filtre sur le protocole ICMP. Quels sont les 2 types d’échanges effectués avec le protocole ICMP ? Quelle est l’adresse IP du serveur google.com ? Est-ce une adresse publique ou privée ?

La requête (echo)

La reponse(reply)

Adresse IP du serveur google.com : 142.250.201.46

C’est une adresse publique accessible sur internet

1. Lancer une nouvelle capture, ouvrir CMD et taper la commande :

***nslookup*** ac-limoges.fr

1. Quelle l’adresse IP du serveur ac-limoges.fr ?
2. Quelle est l’adresse du serveur qui a envoyé le résultat ?
3. Effectuer un filtre sur le protocole DNS.

* Que contient la requête DNS ?
* Que contient la réponse DNS ?