RÉSEAUX – NETWORK I
EXERCICES

Exercice 0

1. Connectez-vous au serveur « ssh » « marion.szpieg.fr » avec votre compte.
2. Taper la commande « history -c », afin d'effacer votre historique du TP précédent.
3. Avec la commande « mkdir », créer un répertoire « tprx1 » dans votre home directory.
4. Vérifier avec la commande « ls » que le répertoire a bien été créé.
5. Avec la commande « cd », se placer dans le répertoire tprx1.

Exercice 1 : retrouver des informations sur le réseau (ifconfig / ipconfig sur Windows)

1. Taper la commande « ifconfig ».
   Dans la suit de l'exercice, on ne s'intéressera qu'au premier paragraphe.
2. Adresse MAC :
   a) A quel endroit peut-on lire une adresse MAC ?
   b) Comment reconnaît-on que s'en est est une ?
   c) A votre avis, elle représente l'adresse MAC de la carte réseau de quelle machine ?
3. Adresse IP :
   a) A quel endroit peut-on lire une adresse IP?
   b) Comment reconnaît-on que s'en est est une ?
   c) A votre avis, elle représente l'adresse IP que quoi ?
4. Dans la 1ère ligne, on peut lire MTU 1500. Expliquez ce que cela signifie.

Exercice 2 (arp)

1. Taper la commande « arp -n ».
2. Que voit-on ? Comparer avec ce qu'on avait avec l'exercice précédent. Que peut-on en conclure ?

Exercice 3 : interpeller une machine (ping)

1. Taper la commande « ping -c2 192.168.1.43 » et valider.

Remarque : la commande « ping » envoie un paquet à une machine et récupère la réponse. L'option « -c2 » précise qu'on ne veut envoyer que 2 paquets (sinon la commande envoie des paquets les uns après les autres tant qu'on ne lui dit pas d'arrêter).

2. Commenter le résultat qui s'affiche à l'écran

Exercice 4 (arp)

1. Taper de nouveau la commande « arp -n ».
2. Quelle est la différence avec l'exercice 2 ? A votre avis, pourquoi ?

Remarque : la commande « arp » signifie « Adresse Resolution Protocole » permet en fait de récupérer l'adresse MAC de la machine appelée par son adresse IP.

Exercice 5 : capturer les paquets (sera utile pour plus tard!)

On va apprendre à capturer des paquets pour ensuite les analyser. **Attention, ne pas utiliser la commande « ping » jusqu'à ce que je vous le demande !**

1. Après que j'ai effacé le cache de la commande « arp », taper de nouveau « arp -n » pour vérifier qu'il n'y a plus qu'une seule adresse.
2. Taper la commande « tcpdump arp or icmp -w ping.cap& » et valider deux fois.

Cette commande va copier (tcpdump) tous les paquets qu'elle va voir passer avec « arp » ou avec « ping » (message ping est transporté par le protocole icmp) à l'intérieur du fichier ping.cap (« -w »).

Le symbole « & » signifie que le processus va s'exécuter en arrière plan, afin de pouvoir avoir la main et taper les ligne de commande avec ping et arp.

Remarque : pour vérifier qu'effectivement cette commande tourne en arrière plan, vous pouvez taper la commande « jobs »

3. Attendre que je retape le ping, puis le faire vous-même.
4. Taper la commande « fg » pour rappeler le processus en arrière plan.
5. Enfin, appuyer sur les touches Ctrl + C pour tuer le processus.

Si cela a bien fonctionné, il faut que vous ayez capturé un nombre de paquets différent de 0. (55:40)

6. Taper la commande « ls -l ping* » et vérifier que le fichier ait une taille supérieure à 0 octet.

Exercice 6 : récupérer le paquet capturé

1. Pour pouvoir récupérer le paquet que vous venez de capturer, ouvrir un 2^{e} terminal (sans se connecter au serveur ssh!).
2. Vérifier qu'il n'y a pas d'accent dans le chemin absolu de votre home directory. (Sinon, créer un répertoire à la racine).
3. Taper la commande « scp lfclxx@marion.szpieg.fr:ping.cap chemin-absolu-du-répertoire-destination », rentrer votre mot de passe quand il vous sera demandé.

Exercice 7: analyser un paquet capturé (avec Wireshark)

1. Télécharger puis ouvrir le document pinglight.pcap déposé dans le classroom.
2. L'ouvrir avec Wireshark.
3. Relier les différentes informations de la fenêtre du haut avec les lignes de commandes tapées dans le terminal.

Exercice 8 : sortir du serveur

Avant de vous déconnecter taper la commande suivante : « history>/home/lfclxx/tprx1/rx1hist.txt.

Pour quitter le serveur « marion.szpieg.fr » tapez « exit » (à faire pour éviter de faire tourner la session « pour rien » svp).