Couche de Liaison (partie 1 - Découverte de Scapy)

Objectifs
1. Apprendre à utiliser l'outil scapy
2. Appliquer les connaissances acquises dans la partie théorique à une couche de liaison conçue par vous-même implémentant l'algorithme ARQ envoyer-et-attendre.

Déroulement
Veuillez répondre aux questions et rendre le pdf de ce fichier par mail à marcos.rubinstein@heig-vd.ch et mohammad.azadifar@heig-vd.ch au plus tard le 19.10.2016 avant le cours.

1. Qu'est-ce que scapy ?

2. Dans quel langage scapy est-il écrit ? Quelle version de ce langage est utilisée ?

3. Des PDU's de quelles couches peut-on forger avec scapy ?

4. Donnez la commande pour lister les protocoles supportés par scapy

5. Sur quels systèmes d'exploitation peut-on installer scapy ?

6. Installez scapy sur linux avec la commande `sudo apt-get install scapy`

7. Forgez une trame Ethernet avec adresse de destination broadcast et transmettez-la en utilisant la commande appropriée de scapy tenant compte du fait qu'une trame Ethernet est un PDU de la couche 2. Montrez ce que vous avez écrit en ligne de commande.

8. Capturez la trame que vous avez transmise au point antérieur avec wireshark et montrez une capture d'écran du détail de la trame en mettant en évidence les champs importants.

9. Normalement, on transmet des trames d'un ordinateur à un autre. Dans le cas des questions 6 et 7, vous avez transmis une trame depuis un ordinateur et vous l'avez capturée sur le même ordinateur. Comment est-ce possible ? Expliquez.

10. Utilisez un câble Ethernet pour connecter deux machines. Transmettez une trame Ethernet depuis l'une des machines comme dans le point 6 mais avec l'adresse MAC du destinataire (pas en broadcast). Capturez-la depuis l'autre machine et montrez une capture d'écran.

11. Forgez une trame Ethernet avec le mot « Hello » dans le payload (ce qui correspond au champ de données dans une trame Ethernet). Transmettez-la en utilisant scapy et capturez-la. Vous devez voir le mot « Hello » dans votre capture. Montrez les commandes et la capture.

12. Décrivez, analysez et testez ce qu'il se passe si on utilise send() au lieu de sendp() pour la trame Ethernet que vous avez forgée.

Pour les points 10 et 11, veuillez montrer au professeur ou à l'assistante que cela fonctionne, afin d'obtenir les points pour les questions.