6.1 Exécutez la commande ipconfig /all dans une fenêtre de commande (Command Prompt) : Menu Démarrer (start), cmd pour le client. Inscrivez le nom de votre poste, l’adresse IPv4, le masque de sous-réseau, l’adresse MAC, la passerelle par défaut pour vos deux systèmes virtuels. (0.5 pt)

Poste : L4708-12

**Windows7\_A**

Adresse IPv4 : 192.168.79.139

Masque du sous-réseau = 255.255.255.0

Adresse MAC : 00-0C-29-6E-CA-D4

Passerelle par défaut : 192.168.79.2

**Windows7\_B**

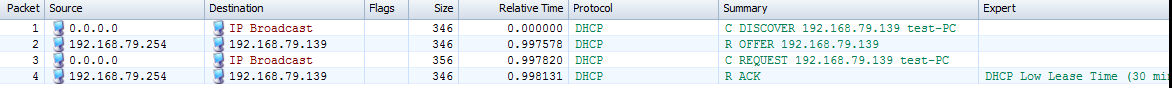
Adresse IPv4 : 192.168.79.140

Masque du sous-réseau = 255.255.255.0

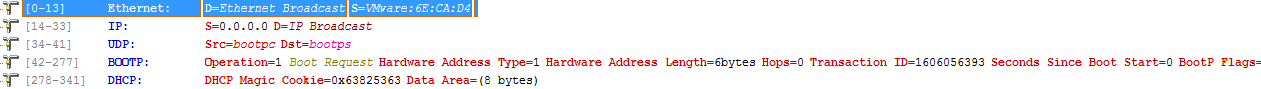
Adresse MAC : 00-0C-29-8E-E7-12

Passerelle par défaut : 192.168.79.2

8.1) Présentez une capture d’écran des paquets DHCP que vous avez capturés à l’aide de l’outil Omnipeek. À la lumière vos observations, expliquez en détail le mécanisme d’attribution d’une nouvelle adresse IP à un client qui veut se joindre à un réseau. (2 pts)



8.2 Donnez la séquence d’encapsulation des protocoles utilisés pour le paquet DHCP DISCOVER. Présentez une capture d’écran du contenu du paquet DHCP DISCOVER. (0.25 pt)



8.3 En se basant sur vos observations en 8.1, quelles opérations DHCP se sont effectuées en broadcast? Selon vous, pourquoi certaines de ces opérations doivent absolument être faites en broadcast? (1.5 pts)

8.4 Serait-il possible d’utiliser le protocole TCP de la couche 4 pour toutes requêtes DHCP? Si oui, dites comment, sinon pourquoi est-il impossible d’utiliser TCP pour les requêtes DHCP? (1.5 pts)

8.5 Quel est le rôle de la trame DHCP offer ? (1 pt)

8.6 Quel champ, dans le paquet, indique que ce message est un DHCP offer ? Spécifiez le champ et sa valeur. (0.25 pt)

8.7 À quel poste correspond l’adresse MAC dans le champ Destination de l’entête Ethernet? Et celui du champ Source? (0.5 pt)

8.8 À quelle machine appartient l’adresse IP source? (0.25 pt)

8.9 Quelle est la taille de l’entête Ethernet que vous observez? (0.25 pt)

8.10 Quelle est la valeur du champ Protocole Type et que signifie-t-elle ? (0.25 pt)

8.11 Dans l’entête DHCP, quelle est la signification du champ IP Address Lease Time ? (0.25 pt)

8.12 Que désigne le champ Client IP Addr Given By Srvr? Quelle est l’utilité de ce champ? (0.25 pt)

8.13 Quelle est l’entête suivante de la trame (niveau 3 du modèle OSI) ? (0.25 pt)

8.14 Quelle est la taille de l’entête de niveau 3 du modèle OSI que vous observez? (0.25 pt)

8.15 Nommez le protocole de niveau supérieur (niveau 4 du modèle OSI) utilisé par DHCP. (0.25 pt)

8.16 Quelle est la taille de l’entête de niveau 4 du modèle OSI que vous observez? (0.25 pt)

8.17 Dans combien de temps la machine Windows 7 doit-elle revalider avec le serveur DHCP son adresse IP? (0.25 pt)

9. Partie ARP (Address Résolution Protocol) (4 points)

9.1 Quelle est l’utilité de la cache ARP? (1 pts)

9.2 Dans votre client Windows7\_A, et dans une fenêtre de commande (DOS), exécutez la commande arp –a qui permet d’afficher le contenu de votre cache ARP ? Si l’adresse de Windows7\_B y apparaît, enlevez-la avec la commande arp –d 192.168.xx.xxx. Vérifiez qu’elle n’y est plus. (0.25 pts)

Démarrez l’analyseur de protocole.

9.3 Lancez une commande qui permet de vérifier votre connectivité avec Windows7\_B. Arrêtez l’analyseur de protocole et sauvegardez la capture réalisée. Lancez à nouveau la commande arp -a. Que remarquez-vous ? (0.25 pt)

9.4 Dans l’analyseur de protocole, cliquez avec le bouton droit de votre souris sur un paquet dont le champ ‘protocole type’ indique ARP request ou ARP Response. Sélectionnez ensuite l’option ‘Make Filter’. Dans la boîte de dialogue qui apparaît, cliquez sur le bouton Protocol et choisissez l’option ARP. Cliquez ensuite sur le bouton Both Direction et choisissez l’option both directions. Dans le champ address 1, vérifiez que l’adresse est la MAC de votre client (Windows7\_A). Si ce n’est pas le cas, remplacez la valeur du champ par la MAC de votre client. Dans le champ address 2 cochez l’option Any Address. Dans le champ Filter inscrivez filtre\_ARP. Cliquez sur le bouton OK pour valider les opérations effectuées. En suivant les étapes indiquées juste avant la question 8.1, appliquez le fitre filtre ARP à votre nouvelle capture. Dans l’analyseur de protocole, quelle est la longueur (size) des trames ARP ? (0.25 pt)

64

9.5 Quelle est la valeur numérique du champ Protocol type de l’en-tête Ethernet (Ethertype) d'une trame ARP ? Que signifie-t-elle ? (0.5 pt)

0x0806 IP ARP

9.6 En se basant sur le contenu d’un paquet ARP Request et ARP Response, qu’est-ce qui différencie une requête ARP d’une réponse ARP dans le protocole ARP ? (0.25 pt)

9.7 À quel nœud réseau correspond l’adresse MAC de la source de la réponse ARP? (0.25 pt)

9.8 À quel nœud réseau correspond l’adresse MAC de la destination de la réponse ARP? (0.25 pt)

9.9 Quelle est la séquence d’encapsulation d’une requête ARP ? (0.25 pt)

9.10 Quel champ de la réponse ARP possède l’information recherchée par la requête ARP lancée par un client d’un réseau? (0.25 pt)

Toujours dans l’analyseur de protocoles avec les mêmes données de capture pour la partie ARP, appliquer le filtre ICMP aux paquets de la capture sauvegardée afin de conserver uniquement les paquets de type PING.

10.1 Quel est le champ ICMP qui différencie les requêtes par rapport aux réponses PING et quelles sont les valeurs impliquées ? (0.5 pt)

10.2 Quelle est la version du protocole IP utilisée ? (0.5 pt)

10.3 Quelle est la valeur du champ TTL (Time To Live). À quoi sert ce champ ? (0.5 pt)

10.4 Quelle est la séquence d’encapsulation d'une trame PING ? (0.5 pt)