TP sur le réseau

Les outils utiles :
1) cmd.exe (invite de commandes se trouve sur c:\\windows\system32
Et sur mon site dans isn puis réseau
2) Wireshark portable
3) Capture de trames
4) lire des tables de routage (présentation)
5) liste de commandes

Première partie

a) Utiliser la commande arp –a (arp seule donne l'aide sur cette commande)
Qu'obtient-on ?
Quel est le protocole qui est utilisé ?
A quel niveau du modèle TCP-IP intervient-il ?

On obtient une table ou cache arp qui donne toutes les machines connectées sur le même réseau local avec la correspondance adresse logique (IP privée) et adresse MAC (adresse physique)
C'est le protocole arp qui est utilisé : il permet d'obtenir l'adresse physique de la première machine à qui on envoie directement les trames ethernet.
C'est la couche liaison (couche 2 de bas niveau) qui rajoute dans son en-tête l'adresse physique du destinataire et l'adresse physique de la source

b) Ouvrir une capture de trames (alexanor-ie.pcap) avec wireshark et filtrer avec arp
Que voit-on ?
Expliquer.
Lorsque la machine (192.168.0.1) fait une requête sur un site quelconque il doit connaître l'IP de la machine à qui il va envoyer les trames.
Sa table de routage lui indique une route par défaut : celle du routeur (coté réseau local).
Sauf qu'il doit connaître l'adresse physique qui correspond à cette IP d'où le protocole arp avec « who has »
La réponse lui est alors envoyée. (lignes 18 et 19)

c) Utiliser la commande ping
ping -4 www.google.fr
Quel renseignement a-t-on ?
A quoi sert le TTL ?
Quel est le protocole utilisé ?

Le premier renseignement est l'adresse IP du serveur google.
Le TTL (time to live) est aussi donné.
Le protocole utilisé est ICMP qui gère les envois de message en cas de problème de transmission.
Echo-request utilisé par un ping sur un site permet seulement de savoir si la transmission se fait correctement sur ce site.
Le TTL est décrémenté de 1 à chaque passage d'un nœud (routeur).
A 0 le message est détruit et le protocole ICMP envoie un message d'erreur à la machine source.

d) utiliser la commande tracert -4 www.google.fr
Qu'obtient-on ?
Quel protocole est utilisé et à quel niveau du modèle TCP se trouve-t-il ?

On a la route complète avec les nœuds intermédiaires pour aller entre les 2 machines.
Ce sont les IP qui sont utilisées.

Il s'agit du protocole IP qui s'occupe du routage et de l'adressage.
Ce protocole est sur la couche 3 : réseau

e) Filtrer avec le protocole DNS
Quelle est l'adresse du serveur DNS utilisé ?
quelles IP a-t-il déterminées ?
Avec Whois en ligne retrouver les renseignements de ces IP

Le serveur DNS a pour adresse 212.27.54.252
google 74.125.24.104
alexanor 84.246.225.167
On retrouve bien google d'une part et le groupe elb d'autre part qui héberge mon site

f) utiliser la commande route print -4
Qu'obtient-on ?

On obtient une table de routage qui selon une destination donnée sous forme d'adresse IP dit à quelle machine il faut l'envoyer et à partir de quelle interface de votre machine.
Sur un réseau local c'est la route par défaut qui est utilisée (l'adresse 0.0.0.0) et l'envoi se fait sur le routeur directement relié (passerelle)

Utiliser la présentation « lire des tables de routage » et regarder le chemin des trames à partir de la page 17.
Essayer de comprendre l'erreur.
Au niveau des trames envoyées d'une machine à l'autre que se passe-t-il ?

Une trame envoyée par la machine source est à chaque nœud transformée.
Seules les adresses physiques (destination -source) changent avec le protocole arp.
En effet, ce sont ces adresses qui sont utilisées pour communiquer entre 2 machines directement reliées et dans un même réseau.
Par contre les adresses IP (destinataire-source) ne changent pas.
Quand une machine reçoit une trame par une interface d'une carte réseau, l'adresse MAC du destinataire est examinée, si c'est la sienne il remet la trame à la couche réseau (3) après décapsulation et l'adresse IP du destinataire est examinée, sinon elle ne fait rien.
L'adresse IP permet de savoir à quelle machine il faudra transmettre la trame.
Si c'est la sienne elle remet la trame à la couche supérieure (couche transport) après décapsulation.
Sinon elle utilise sa table de routage pour savoir à qui remettre la trame.
On regarde la première entrée et on applique le masque on obtient alors une adresse réseau si c'est celle qui est indiquée (à gauche) la route est alors trouvée (à droite) sinon on passe à l'entrée en dessous et une fois l'adresse IP du prochain nœud trouvée il suffit de déterminer son adresse MAC par le protocole arp.
La couche réseau encapsule alors la trame en mettant l'adresse mac du destinataire et sa propre adresse mac (source), les adresses IP sont inchangées.

<u>Deuxième partie</u>
Toujours avec la même capture
(Recherche « alexanor » sur google et requête sur le site alexanor(machaon.fr)

Filtrer avec http (les lignes correspondent au numéro de trames)

a) *Rappeler l'adresse IP de mon serveur* :
   84.246.225.167

Les lignes concernées pour le chargement de ma page d'accueil sont :
29 33 61 64 73 85 91 237 277 682 2370 2382 2387
Du protocole HTTP il y a la méthode get et des codes de statut (moved permanently :301 et OK :200)

b) Que signifient-ils ?
get est la demande du client pour que le serveur lui envoie la page d'accueil.
moved permanently est une réponse du serveur : dans le cas présent www.alexanor.eu se trouve en fait à www.machaon.fr
OK est une réponse du serveur qui signifie qu'il a bien envoyé l'objet demandé.

c) Commentez les lignes 61 et 64
Développez les trames et commentez les principaux renseignements de chaque couche
Le client demande la page d'accueil du site machaon.fr (61)
Le serveur lui a envoyé cette page(64)
Sur la couche liaison on retrouve les adresses mac de ma carte ethernet et de l'interface de ma freebox
Sur la couche réseau les adresses IP privée de ma machine IP (ce n'est pas celle-là qui circule mais celle publique de ma freebox)
Sur la couche transport les numéros de port (80 pour le protocole http côté serveur)
Dans la trame 64 on retrouve le texte complet de la page d'accueil.

d) Pour que la page s'affiche complètement quels sont les renseignements nécessaires ?
Le fichier html : ligne 64
Le fichier css : ligne 85
L'image de fond : ligne 682
L'image du papillon alexanor : ligne 2370
L'icône : ligne 2387

e) Pourquoi y a-t-il deux demandes d'envoi de l'image ? (lignes 91 et 237)
Lors du premier envoi il y a eu des erreurs liées au protocole TCP de la couche transport.
TCP signifie Transmission Control Protocol.
f) Développez la trame 2370 et essayez d'analyser comment la couche transport avec le protocole TCP a permis l'envoi de l'image
La taille de l'image est de 1 887 430 octets, or chaque trame ne peut excéder 1500 octets (en fait 1460 octets de données que l'on nomme MTU ou Maximum Transmission Unit)
Ainsi il a fallu 1293 trames pour l'envoi de cette image.
La première 240 et la dernière 2370 (on peut filtrer par TCP pour les voir toutes).
Le protocole TCP consiste à gérer et à contrôler l'envoi des paquets, s'assurer de la bonne réception, les réassembler etc...
C'est un protocole sûr.