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 ?

b) Ouvrir une capture de trames (alexanor-ie.pcap) avec wireshark et filtrer avec arp
Que voit-on ?
Expliquer.

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 ?

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

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

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

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 ?

Deuxième partie

Toujours avec la même capture (les lignes correspondent au numéro de trames)
(Recherche « alexanor » sur google et requête sur le site alexanor(machaon.fr)

Filtrer avec http

a) Rappeler l'adresse IP de mon serveur

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 ?

c) Commentez les lignes 61 et 64

Développez les trames et commentez les principaux renseignements de chaque couche

d) Pour que la page s'affiche complètement quels sont les renseignements nécessaires ?

e) Pourquoi y a-t-il deux demandes d'envoi de l'image ? (lignes 91 et 237)

f) Développez la trame 2370 et essayez d'analyser comment la couche transport avec le protocole TCP a permis l'envoi de l'image