Analyse des protocoles ARP& ICMP

A. Analyse de trafic ARP

1) Qu'est ce que ARP ?
2) Afficher le contenu de votre table ARP (la commande **arp –a**).
3) Expliquez dans quelle condition votre machine génère t'elle une trame ARP ?
4) Videz votre table ARP (la commande **arp –d ***)
5) Créer un filtre de façon à ce que votre analyseur de trames ne captera que les datagrammes ARP.
6) Démarrer la capture, lancer la commande « ping » vers une adresse IP choisie, puis arrêter la capture.
7) Afficher de nouveau le contenu de votre table ARP.
8) Vérifier que vous avez capturé les bonnes trames (la requête ARP émise/reçue depuis/vers votre machine). Expliquer votre démarche.
9) Expliquer comment votre analyseur arrive à détecter que les trames capturées encapsulent des datagrammes ARP (indiquer le champ utilisé et sa valeur).
10) Déterminer l'adresse Ethernet de votre machine à partir des trames capturées.
11) Vers quelle adresse Ethernet la requête ARP a été envoyée ? Interpréter cette valeur.
12) Analyser le datagramme ARP de réponse et expliquer comment votre machine arrive à déterminer l'adresse MAC relative à votre correspondant.
13) Etablir un chronogramme expliquant le fonctionnement de ARP.

B. Analyse de trafic ICMP

1) Créer un filtre de façon à ce que votre analyseur de trames ne capte que les datagrammes ICMP.
2) Démarrer la capture, lancer la commande « ping » vers une adresse IP choisie. Arrêter la capture.
3) Retrouver dans le buffer de capture les trames générées par la commande « ping ».
4) Quel type de message ICMP (en émission et en réception) a été généré par la commande ping ? Indiquer les champs spécifiques qui vous ont permis de déduire cette valeur.
5) En combien de paquets IP a été décomposée la requête émise ? Conclure.
6) Quel est le nombre de trames générées par la commande « ping » ? Montrer qu'il est cohérent avec ce qui a été affiché lors de l'exécution de la commande.
7) Expliquer comment votre analyseur arrive à détecter qu'il s'agit d'un message ICMP encapsulé dans un paquet IP, qui est lui aussi encapsulé dans une trame Ethernet.
8) Quelle est la valeur TTL des paquets relatifs aux requêtes ICMP ? Conclure.