Première Partie

Cette partie traite de la configuration des interfaces réseau.

1. Au moyen de la commande historique et multiplateforme ifconfig, vous listez les interfaces réseau de votre machine en donnant leurs noms.

2. Vous commentez pour chaque interface les différents drapeaux (UP, BROADCAST, RUNNING, MULTICAST, LOOPBACK), la valeur et la signification du MTU vis à vis des paquets IP.

(MTU : taille max de paquet. UP et RUNNING : interface en fonctionnement/ BROADCAST : adresse broadcast valide / MULTICAST : supporte le multicast / LOOPBACK : interface loopback)

3. Listez les interfaces physiques dont vous disposer en vous aidant du nom de l'interface et en vérifiant via la commande dmesg les interfaces découvertes par le noyau.

(eth0 et eth1)

4. Déduisiez en le rôle des autres interfaces.

(interfaces virtuelles notemment pour les vm)

5. Pour l'interface eth0 justifiez que l'adresse IP de cette interface est une adresse non routée.

(entre 172.16.0.0 et 172.31.255.255 : adresses non routées)

6. A quelle classe d'adresse de réseau appartient elle ?

(classe b)

7. Donnez l'adresse du sous réseau auquel appartient l'interface eth0.

(172.31.1.0)

8. Combien de sous réseaux sont ils possibles sur ce réseau ?

(256-2=254 : de 172.31.1.x à 172.31.254.x car 172.31.0.x et 172.31.255.x sont reservées)

9. Combien de machines sont elles possibles sur chaque sous réseau ?

(256-2=254 : de 172.31.1.1 à 172.31.1.254 car 172.31.1.0 et 172.31.1.255 sont reservées)

10. Expliquez comment a été calculé l'adresse de broadcast correspondant.

11. Donnez la commande ifconfig qui a permis de configurer cette interface.

(ifconfig eth0 172.31.1.72 netmask 255.255.255.0 broadcast 172.31.1.255)

12. Expliquez pourquoi cette commande n'est pas saisie par l'administrateur de la machine.

(machine configurée automatiquement)

Seconde partie

Nous nous intéressons à analyser la table de routage de notre machine.

1. Expliquez l'entrée 172.31.1.0 de votre table ? Est ce une route directe ou indirecte ? Que permet elle de faire ? Justifiez en terme de factorisation de la table de routage.

(route directe (ne passe par aucun routeur). Elle permet d'atteindre toutes les machines du sous-réseau. S'il n'y avaitpascette entrée, ondevrait avoir dans la table de routage les adresses de toutes les machines du sous-réseau ==> "factorisation" de la table de routage)

2. Vérifiez que cette entrée permet d'atteindre la machine de votre voisin. Donnez la commande que vous utilisez et la trace.

(faire un ping sur l'adresse de la machine de votre voisin)

3. Justifiez que c'est bien cette entrée de la table de routage qui est utilisée pour atteindre la machine de votre voisin.

4. Expliquez à quoi correspond l'entrée 0.0.0.0 ? Est ce une route directe ou indirecte ? Selon vous de combien d'interfaces physique dispose la passerelle associée ?

(route indirecte. Il s'agit de la route par défaut. La passerelle associée dispose d'un minimum de 2 interfaces physique (une vers internet et l'autre ou les autres vers le ou les réseaux locaux))

5. Justifiez que c'est bien cette entrée qui est utilisée lorsque vous cherchez à atteindre la machine 216.58.204.227.

(on cherche à aller sur internet : on passe forcément par la route par défaut (car cette adresse n'est connue ni de la machine ni du sous reseau))

Troisième partie

Analyse de trace et du routage.

1. Grâce à la commande /usr/sbin/arp -a trouver une adresse IP de votre sous réseau qui n'est pas présente dans le cache arp.

(prendre une adresse correspondant à une machine allumée de la salle mais qui ne soit pas celle pingée précedemment)

2. Lancez une capture wireshark et pour capturer ce qui circule sur votre sous résau et justifiez l'interface sur laquelle vous faites la capture.

(eth0 car c'est l'interface utilisée par le sous-réseau)

3. Faites un ping sur une machine de votre sous réseau qui n'est pas dans le cache arp.

4. Vous donnez la capture d'écran montrant une requête ARP suivie d'une requête ICMP.

5. Expliquez pourquoi il y une requête ARP à destination de l'adresse MAC ff:ff:ff:ff:ff:ff:ff:ff pour résoudre l'adresse IP que vous avez pinguée ? Justifiez que cette requête atteint bien toutes les machines du réseau ethernet ? Est ce que la réponse est sûre ?

(cette adresse MAC est l'adresse MAC de broadcast donc ça atteint bien toutes les machines du sous-réseau. La réponse n'est pas sûr, car la 1ere machine qui répond sera prise pour le destinataire)

6. En analysant la requête ICMP justifiez que celle-ci a bien utilisée la route établie pour le sous réseau grâce à l'adresse MAC de la destination et en justifiant par rapport au type de route (directe ou indirecte) ?

7. Vous lancez une capture sur l'interface de votre route par défaut.

8. Vous faites un ping 216.58.204.227 et vous donnez la copie d'écran de la capture associée à ce ping.

9. Vous donnez l'adresse MAC de la destination de la requête ICMP correspondant.

10. Vous vérifiez grâce au cache ARP qu'il s'agit bien de l'adresse MAC de votre routeur par défaut.

11. Vous en concluez que la route utilisée pour atteindre 216.58.204.227 est bien votre route par défaut via les adresses IP et MAC de destination de cette requête ICMP.