Licence 2 - Informatique

Mise en évidence du protocole ARP

Objectifs :	Découvrir le protocole arp et l'utilisation des messages de diffusion à travers des commandes simples et un analyseur de trame
Conditions de réalisation :	Environnement : linux et wireshark.
Durée :	3H

1.Compte rendu :

Un compte rendu est à rédiger et à rendre sur moodle à la fin de chaque TP. Un des comptes rendus sera noté pour calculer la moyenne. Le premier compte rendu est là pour vous habituer à rédiger et ne sera pas évalué.
Un compte rendu est un document rédigé en français et sans faute d'orthographe. Il permet à la relecture de comprendre ce qui a été fait. En relisant votre compte rendu, nous devons pouvoir nous dire que vous avez tout compris sur les attentes du TP.
Il est structuré. Il contient donc vos noms, des titres et une pagination.
Il permet également de refaire les manipulations facilement. Les commandes doivent pouvoir être visualisées distinctement et être copiées/collées.
Vous pouvez mettre des copies d'écran mais celles-ci doivent être commentées et pertinentes.
Je vous conseille de créer un modèle de document pour vous faciliter le travail pour les prochains Tps.

2.Configuration préalable

Vous allez utiliser les machines virtuelles linux appelées « Réseaux 192 » pour ce TP. Sur cette machine, vous pouvez avoir des droits administrateurs en faisant préfixer vos commandes de sudo. En contrepartie, aucune sauvegarde n'est réalisé sur cette machine et lors du redémarrage, elle est réinitialisée.

Ces machines possèdent plusieurs interfaces réseaux :

- ens160 qui est l'interface connectée et qui possède une adresse IP en 10.192.x.y/16. C'est celle que vous allez utiliser pour ce TP
- ens192 et ens224 sont des interfaces non configurées. Nous ne les utiliserons pas pour ce TP.
- Les autres interfaces sont des interfaces dépendant d'autres logiciels ou d'autres configuration. Vous ne devez pas vous y intéresser.

3.Les commandes ping et ifconfig

1. À quoi servent les commandes ifconfig puis ifconfig -a ?
Afin de vérifier votre configuration réseau nous allons effectuer quelques tests à l'aide de la commande ping. Tous les tests suivants devront être positifs. Expliquez le rôle de chacun des tests :

- ping 127.0.0.1

- ping 10.192.12.1
- ping 10.192.0.255
- ping boa01
- ping www.framasoft.org

2. Testez une adresse IP non utilisée sur le réseau (par exemple 12.13.14.15). Que peut-on déduire de la réponse ? Le poste existe-t-il ? Le poste est-il éteint ?

4.Les adresses MAC

Vos machines ont trois cartes réseaux. Quelles sont leurs adresses MAC ? Rechercher à quel fabriquant elles appartiennent à l'aide de cette adresse.
L'adresse MAC d'une machine enseignante est : c0:b6:f9:c5:69:8f. Quel est son constructeur ?

5.Le protocole ARP

Deux stations doivent utiliser les adresses Ethernet (MAC) pour dialoguer, il faut donc un moyen pour passer de l'adresse IP à l'adresse MAC et vice versa. C'est le rôle du protocole ARP (Adress Resolution Protocol) et RARP (Reverse Adress Resolution Protocol)

Dans chaque machine il existe une table de correspondance entre les adresses MAC et les adresses IP, c'est le cache arp qui est visualisable à l'aide de la commande arp.

1. Affichez le cache ARP à l'aide de la commande arp, notez le résultat en expliquant le rôle de chaque colonne.
2. Faites un ping sur une autre machine d'un de vos camarades, Utilisez les messages privés de Discord pour échanger cette information.
3. Affichez de nouveau le cache arp (notez le résultat), que contient le cache ARP à l'issue du PING ? Pourquoi ?

Vous devrez utiliser la commande man arp pour répondre correctement aux questions suivantes.

4. Videz le cache arp. À l'aide de quelle commande ?
5. Notez l'adresse MAC de la machine de votre voisin
6. Ajoutez manuellement cette entrée arp dans le cache à l'aide de la commande arp –s. Donnez l'instruction exacte qu'il faut passer.
7. Affichez votre cache arp pour vérifier quel est le type de l'entrée ? Expliquer la différence. Testez cette adresse avec un ping

6.Association MAC↔IP

Nous allons voir maintenant que nous pouvons associer manuellement une adresse MAC à une adresse IP
1. Utilisez la commande arp -s pour modifier l'adresse matérielle d'une machine par défaut (donnez lui par exemple 08-00-02-22-22-20 qui est une adresse inexistante)
2. Faites un ping sur cette machine et expliquez le résultat de la commande.
3. Comment supprimer cette entrée incorrecte ?
4. Expliquez le résultat.

On peut également tromper arp avec une adresse MAC existante mais mal associée

5. Prenez l'adresse MAC d'un poste,
6. Prenez l'adresse IP d'un autre poste,
7. Affectez avec arp l'adresse IP à l'adresse MAC relevée,
8. Testez l'adresse IP avec ping.
9. Expliquez le résultat.

7.Explication d'un ping avec l'analyseur de trame wireshark.

Nous allons maintenant voir les mécanismes qui se mettent en jeu quand on fait un simple ping.
À l'aide des manipulations que vous venez d'effectuer :
1. Quand se déclenche le protocole ARP sur le réseau ?
2. Comment fonctionne-t-il ? Décrire son fonctionnement à l'aide d'un algorithme.
3. Quel protocole utilise la commande ping ? Dans quels modes ?
4. Écrivez **tout** ce qui se passe quand vous faites un ping 10.192.0.255 en ayant vidé votre cache arp au préalable.