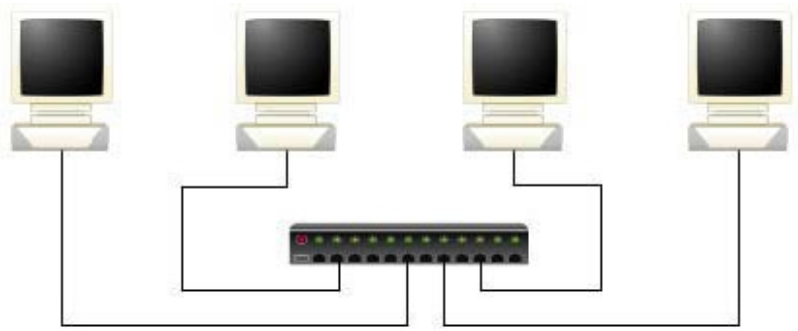
BOSC Julie

TP de Réseau n°1

Assemblage d'un réseau - Observations

L3 Miage Groupe 1

1 Raccordement du matériel



2 Configuration des machines

a) Configuration de l'interface

Nous avons configurer les machines au niveau « systéme », afin qu'elles se reconnaissent et qu'elles puissent dialoguer.
Notre réseau a été rendu operationelle en lançant manuellement la commande « ifconfig »,

ifconfig <nom de l'interface> <adresse INTERNET>

Exemple : ifconfig xl0 192.168.0.4

b) Choix des adresses INTERNET des machines

L'adresse Internet est constitué de deux parties :

192.168.0.4

Une partie réseau : Adresse du réseau Une partie machine : Adresse de la machine

Exemple : ifconfig xl0 192.168.0.1 pour le premier ordinateur
ifconfig xl0 192.168.0.2 pour le deuxième ordinateur
ifconfig xl0 192.168.0.3 pour le troisième ordinateur
ifconfig xl0 192.168.0.4 pour le quatrième ordinateur

c) Marquage de l'interface à l'état « marche »

L'interface est initialisée et configurée, on peut la marquer « prête à l'emploi », pour cela on lance la commande suivante :

ifconfig <nom de l'interface> up

Exemple : ifconfig xl0 up

Pour désactiver cette interface, il suffit de taper la commande suivante :

ifconfig <nom de l'interface> down

Exemple : ifconfig xl0 down

d) Contrôle de l'état des interfaces

A tout moment, on peut controler l'état des interfaces à partir de la commande :

ifconfig <nom de l'interface>

Exemple : ifconfig xl0

Cette commande permet de voir quelle interface (nom) est en marche (UP), de connaître l'adresse Internet associé à l'interface (inet ...) ainsi que l'adresse Ethernet de la machine (ether...). Le « status » permet de savoir si la carte est branchée à un réseau.

e) Configuration par modification des fichiers de configuration

Dans une situation réelle, on modifie des fichiers de configurations que les machines lisent automatiquement au moment du boot.

Pour cela on doit modifier le fichier rc.conf, celui se situant /etc/rc.conf.
Pour ouvrir le fichier on utilise la commande :
nedit /etc/rc.conf

On doit rajouter la ligne :
ifconfig_xl0= « inet 192.168.1.1 netmask 255.255.255.0 »

f) Association adresse / nom symbolique

On peut associer un (ou plusieurs) nom symbolique aux adresses Internet.

Pour cela on doit modifier le fichier hosts, celui se situant /etc/hosts.
Pour ouvrir le fichier on utilise la commande :
nedit /etc/hosts

On rajoute les lignes suivantes à la fin du fichier:
192.168.0.1 Jo
192.168.0.2 Alex
192.168.0.3 Romain
192.168.0.4 Julie

3 Contrôle du Réseau

a) Utilisation du ping

Pour vérifier que les machines sont bien connectées et bien configurées, on a utilisé un outil

standard : « ping » qui permet de vérifier qu'une machine distante répond bien quand on lui envoie un paquet.

ping <adresse internet de la machine distante>
ou ping <nom symbolique donné dans le fichier hosts>

Exemple : ping 192.168.0.2 est équivalent à ping Alex

Cette comande affiche à l'écran une ligne donnant le temps d'aller/retour qui recommence toutes les secondes jusqu'à l'on tape ctrl - C.

Exemple des lignes qui s'affichent à l'écran :

64 bytes from 192.168.0.2 : icmp_seq = 0 ttl=64 time=0.386 ms
64 bytes from 192.168.0.2 : icmp_seq = 1 ttl=64 time=0.379 ms
64 bytes from 192.168.0.2 : icmp_seq = 2 ttl=64 time=0.408 ms
.
.
.
64 bytes from 192.168.0.2 : icmp_seq = 47 ttl=64 time=0.380 ms

---------- Alex ping statistics ----------

48 packets transmitted, 48 packets received, % packet loss round-trip
min/avg/max/stddev = 0.369/0.387/0.486/0.020 ms

Avec ttl = La taille du paquet
time = Le temps d'aller/retour
icmp-seq = Le numéro du paquet

b) Procédure de login sur une machine distante

L'application « telnet » permet à un utilisateur de se logger sur une machine distante. Chaque machine dispose d'un login qui s'appelle « guest » autre que le root qui est l'administrateur.

telnet <nom de la machine distante>

Exemple : telnet Jo
login : guest
password : guest

Une fois le login accepté, on peut travailler sur la machine distante de la même façon que localement.

L'application « telnet » crée une connexion entre les deux machines à travers laquelle les commandes tapées sur la machine locale sont transférées pour être exécutées sur la machine distante. Les résultats obtenus sur celle-ci seront également transférés à travers cette même connexion pour être affichés sur l'écran de la machine locale.

Pour quitter l'application « telnet », il suffit de taper la commande « exit ».

4 Observation de l'activité du Réseau

Après avoir configuré les machines et vérifié au niveau utilisateur que le « réseau fonctionne correctement », on va maintenant "écouter" le câble Ethernet et regarder ce qui se passe quand on lance des commandes comme ping et telnet.

L'outil qui permet d'observer le réseau s'appelle ethereal.

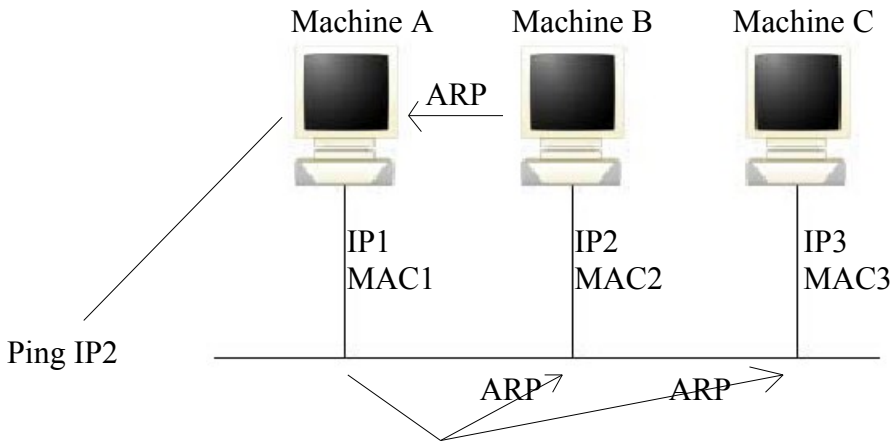
a) Observation de la commande ping

On a lancé sur une des machines (la machine d'adresse 192.168.0.1) « ethereal » et sur une autre on a tapé ping 192.168.0.2.

On remarque que la commande ping utilise des paquets de type IMCP.
On a pas obervé tout de suite d'autres paquets (de type ARP : Address Resolution Protocol).
On a donc vidé la table ARP grâce à la commande : arp - d –a et on a pu observé les paquets de type ARP.

Après que l'on a vidé le tableau des paquets apparaissent dans « ethereal » ce qui permet de dire que chaque machine identifie maintenant l'adresse ethernet de l'autre.
On souhaite afficher le contenu de la table ARP pour cela on utilise la commande : arp –a.

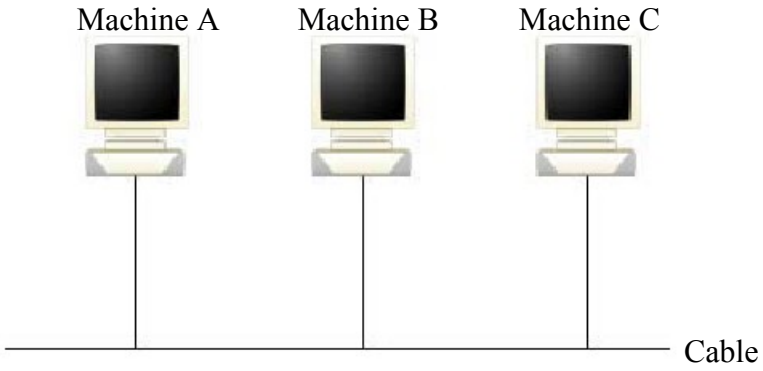
<u>Analyse et interprétation des paquets de type ARP</u> :



La machine A souhaite « pinger » la machine B.
Chaque machine a une adresse Ethernet et cette adresse posséde une adresse MAC.
La machine A connaît IP2 mais pas MAC2, la machine A va donc envoyer un message ARP à toutes les machines.
La machine C, ignore le message.
La machine B envoie son adresse MAC2 par un message ARP, la machine A peut donc « pinger » la machine B.
La machine A garde les adresses IP2 correspondant au machine dans une table.
Ensuite quand la machine A resouhaite « pinger » la machine B, elle ne renvoie pas de message ARP.

Donc les paquets ARP n'apparaissent pas à chaque fois parce qu'une fois que les deux machines se sont identifiés, le tableau ARP n'a pas besoin d'être rempli à nouveau.

b) Observation du protocole CSMA/CD



Protocole d'accès au cable :

S'il n'y a aucun signal sur le cable, la machine A envoie une trame.
S'il y a un signal, la machine A attend

Si deux machines souhaitent envoyer une trame en même temps, il y a collision sur la cable. Chaque machine arrête son émission et attend un laps de temps aléatoire, avant de tenter de re-émettre toute la trame.

Si elles envoient denouveau une trame en même temps, il y a denouveau collision.

Pour réaliser la manipulation, on a lancé l'outil netstat sur une machine(192.168.0.1) grâce a la commande :

netstat -I xl0 1

Notons que les utilitaires utilisés ci-dessous se trouvent dans le fichier cd/root/impt-tools.

Grâce a cette commande, on peut observer le ombre de paquets emis, reçus et surtout le nombre de collisions observées sur cette interface à intervalles d'une seconde.
Ensuite, on a ouvert une seconde fenêtre et utilisé la commande suivante :

udpmt -s <taille du paquet> -p <port serveur> <serveur>

Exemple : udpmt –s 60 –p 1025 192.168.0.2

La commande udpmt affiche un rapport regroupant différentes statistiques (instant émission, nombre de paquets émis durant l'intervalle, nombre totale de paquets émis, débit mesuré durant l'intervalle, débit moyen sur les 10 dernières secondes et le débit moyen depuis le début)

Sur une deuxième machine, on a lancé la commande suivante auparavant :

udptarget -p <port serveur>

Exemple : udptarget –p 1025

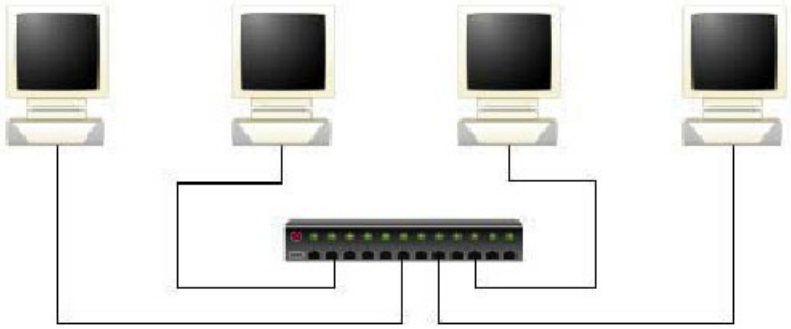
La commande udptarget affiche les débits constatés en réception.

Notons que le port serveur doit être compris entre]1024;65535[.

On a constaté que la taille des paquets augmente quand le nombre de collisions augmente.
De plus la machine ne voit les collisions que lorsqu'elle est en train d'émettre.

Au niveau du serveur, on a un nombre d'erreurs qui apparait lors de chaque collision (sequence error).

udpmt --> udptarget udpmt --> udptarget



5 Analyse des performances du Réseau

a) Mesure du débit réel

On a lancé sur une première machine la commande udpmt pour envoyer des paquets vers une autre machine, puis sur une troisième machine l'utilitaire ethereal.

Le champ « longueur de paquet » :
packet lenght = 642 bytes

Le champ « longueur d'entêtes » :
header lenght = 20 bytes

En regardant la trame effectuée par « ethereal », on note que le nombre d'octets de données est de 197 octets alors que le nombre d'octets total des paquets est de 239 octets.
Le débit réel est de 197 octets et le débit effectif est de 239 octets.

Le pourcentage est de 82,43 %.

b) Mesure en utilisant des commutateurs

On a remplacé le hub par un commutateur.

On constate qu'avec un hub on a toujours le même débit moyen sur les différentes machines.
Ceci peut être expliqué par le fait que le hub fait des circuits à deux ports.