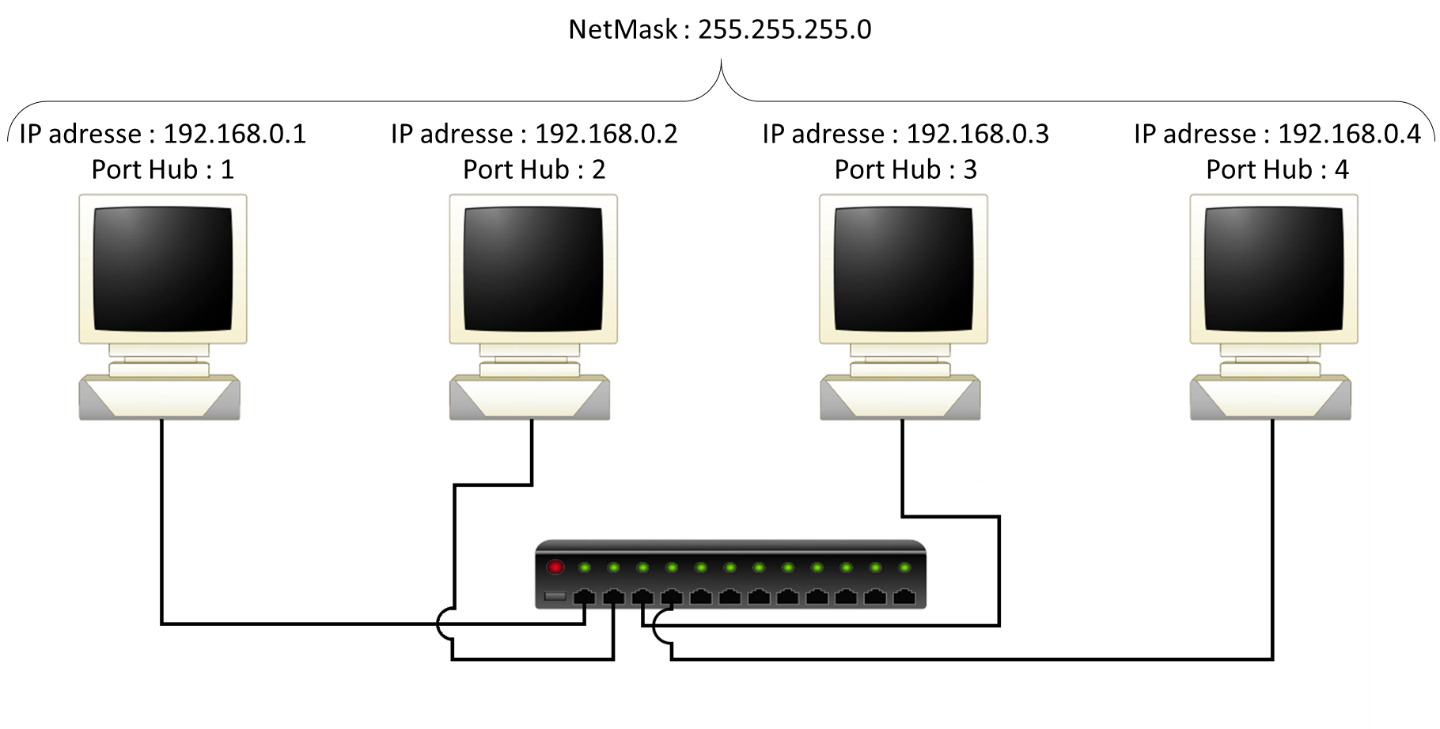
Cheick CISSOKO M2 Pro CCI

Gaëtan LAGIER

Eric THIERRY

**CR réseau TP1**

1) Schéma du réseau utilisé au cours de la séance :



2) NetMask et adresse broadcast :

Netmask : FFFFFF00 (255.255.255.0), c’est le masque de réseau pour des adresses IP de classe C. Ce qui est équivalent à 192.168.0.X/24. Sur un réseau comme nous avons défini, l’adresse broadcast correspond à la dernière adresse possible sur ce réseau soit 192.168.0.255

3) Ping et paquet ICMP :

Machines utilisées pour la commande ping :

Machine A :

* Adresse IP : 192.168.0.3 (nom symbolique res3)

Machine B :

* Adresse IP : 192.168.0.2 (nom symbolique res2)

Commande ping exécutée sur Machine A : ping res2

Un paquet de type ICMP provenant de la machine A est envoyé sur le réseau en tant que requête. Quand la machine B (res2) reçoit le paquet elle en renvoie un en réponse à destination de la machine A.

La commande ping permet de savoir si les deux machines peuvent communiquer. Elle indique en plus le temps d’aller-retour d’un paquet entre les deux machines sur le réseau.

4) Paquet de type ARP :

Pour un ordinateur ayant sa table ARP vide, si un paquet A est envoyé sur le réseau depuis cette machine, on aura alors un paquet de type ARP envoyé en broadcast. Le paquet est alors à destination de toutes les machines présentes sur le réseau local. Le paquet ARP contient l’adresse de destination contenue dans le paquet A. Le paquet ARP demande l’adresse Ethernet correspondant à l’adresse IP de destination.

Le paquet ARP a pour adresse source l’adresse Ethernet de l’ordinateur envoyant le paquet A. L’adresse de destination est l’adresse Ethernet broadcast. Quand le paquet ARP est reçu par la machine recherchée, cette dernière envoie un paquet ARP contenant son adresse Ethernet (source) et l’adresse Ethernet (destination) de l’ordinateur désirant envoyer le paquet A.

5) Collisions :

Utilisation des utilitaires netstat et udpmt afin de visualiser les collisions sur le réseau. On utilise udpmt pour envoyer des paquets de tailles diverses entre deux machines de notre réseau local. Netstat permet d’observer le réseau, il est lancé sur la machine envoyant les paquets pour pouvoir détecter les collisions. Seule la machine qui envoie les paquets pourra détecter les collisions.

Nous observons une moyenne de 800 collisions, avec des intervalles de 10 sec pour netstat et des paquets de 1472 octets envoyé par udpmt. Il n’y a pas de détection d’erreur. Avec une taille de 64 octet par paquet, on observe une très légère baisse du nombre de collisions en comparaison des paquets de 1472 octets.

­6) Collisions avec plus de trafic sur le réseau :

Il n’y a pas d’augmentation du nombre de collision, quel que soit la taille des paquets utilisés.

7) Variations du nombre de collisions en fonction de la taille des paquets :

Le protocole CSMA/CD permet de réduire le nombre de collision suivant deux principes, émission seulement quand le support est libre (CSMA) et détection des collisions (CD). La détection est possible car la machine écoute le support tout en émettant. Si une différence est observée c’est qu’il y a eu collision.

Seule la machine qui a émis le paquet est capable de détecter la collision. Ainsi pour une détection efficace des collisions, il faut que le temps d’émission soit supérieur ou égale au temps d’aller-retour sur le réseau. Ce qui implique une taille minimale des paquets à envoyer sur le réseau. Comme c’est la machine émettrice qui détecte les collisions si les paquets sont petits elle ne sait pas s’il y a eu collision de son paquet avec un autre avant qu’il ne soit arrivé à la machine de destination.

Pour les questions 5) et 6), il n’était pas évident de voir une variation du nombre de collisions en fonction de la taille des paquets. Pour faciliter cette observation, il faudrait un temps de propagation plus grand donc une distance de câble plus longue, 200 m serait une taille intéressante.

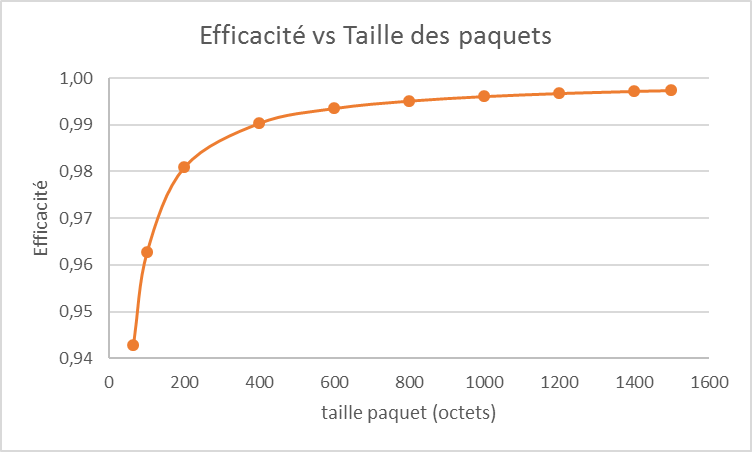
8) Temps de propagation et efficacité :

Le réseau que nous avons créé, était composé de câbles d’environ 3m entre chaque ordinateur et le hub. Ainsi la longueur du réseau était d’environ 6m. Pour calculer le temps de propagation on utilise l’équation suivante :

Les caractéristiques de notre réseau Ethernet sont : L = 6 m et v = 108 m/s donc Tprop = 60 ns

L’efficacité du réseau est obtenue grâce à l’équation suivante :

Sur notre réseau nous avons mesuré un débit maximum de 9571 kbits/s



La taille de notre réseau étant très petite on l’efficacité évolue très peu avec la taille des paquets.

9) Partage du débit :

Le partage du débit est à peu près équitable car les machines parlent sur le réseau seulement s’il est libre, elle dispose ainsi du débit maximal à chaque envoie de paquet. C’est le protocole CSMA/CD qui gère cette équité.

10) Débit vs taille des paquets :

Mesure du débit pour des paquets de tailles diverses (10, 20, 100, 1000, 1472, 1473, 2800 et 3000 octets)

