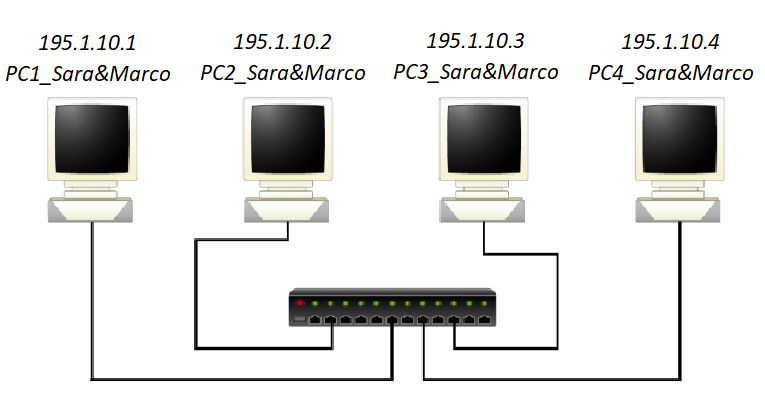
**M2-CCI Enseignement de Réseaux – Compte-Rendu du TP n.1**

Groupe BAJA Sarra – BOLLOLI Marco

Ce compte-rendu a pour objet les manipulations effectuées dans le TP n.1, et les observations et les calculs qui y étaient associés. De suite, les étapes seront présentées avec la numérotation adoptée dans l’énoncé du TP pour des raisons de clarté.

*Mise en place du réseau (2.1)*

Le réseau est mis en place à partir de 4 ordinateurs et un Hub tel que décrit dans la figure suivante.



Figure

Dans chaque ordinateur, nous n’utilisons pas l’interface réseau de la carte mère (*em0*) mais plutôt l’interface *bge0* qui est installée en plus et qui permet d’observer des collisions entre paquets.

L’interface n’étant pas associé à une adresse IP v4, nous avons procédé à le faire pour chaque ordinateur à l’aide de la commande **ifconfig <nom interface> <adresse>**. De suite le paramètres choisis :

*195.1.10.1*

*195.1.10.2*

*195.1.10.3*

*195.1.10.4*

Nous avons bien verifié, à l’aide de la meme commande ifconfig, que bge0 était correctement configurée sur chaque ordinateur (Cf. Figure 2).

Pour les quatre ordinateurs, nous observons que la valeur du Netmask est 0xffffff00. Cela est du au fait que nous avons utilisé une adresse IP de classe C, donc avec 24 bits de poids fort pour la partie réseau et 8 bits de poids faible pour la partie machine : donc en décimale le Netmask serait 255.255.255.0, et en hexadécimale, 0xffffff00.

Cela laisse 255 combinaisons pour la partie machine, donc 255 machines pourraient etre branchées sur ce réseau. En réalité, ce sont seulement 254, car justement il y a l’adresse broadcast, qui sert, entre autres, à échanger les paquets de type ARP entre ordinateurs. Comme nous pouvons le confirmer sur la Figure 2, cet adresse est la dernière adresse machine disponible parmi les combinaisons possibles dans le réseau, donc en ce cas il s’agit de 195.1.10.255.

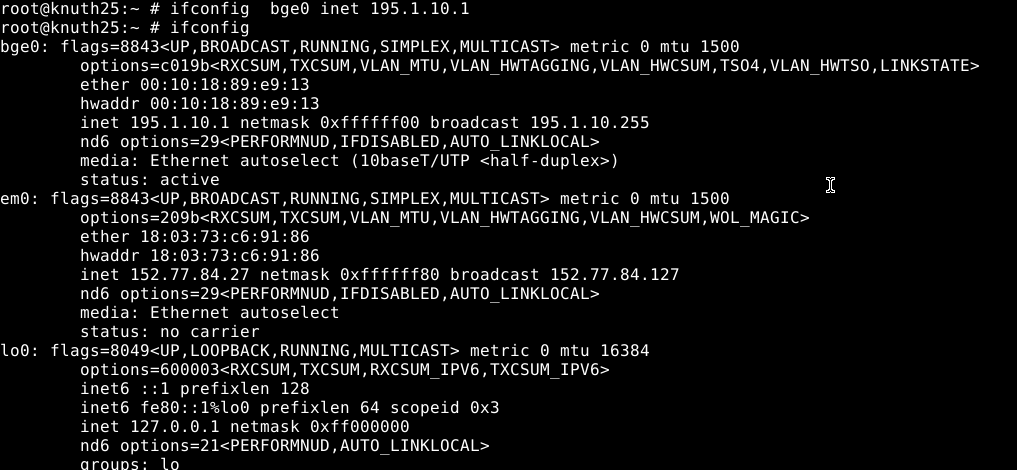


Figure 2

Une fois que nous avons vérifié le correct adressage des interfaces, les adresses sont ajoutés au fichier /etc/hosts/ de chaque ordinateur à l’aide d’un éditeur de texte, pour les faire correspondre aux noms symboliques que nous donnons aux machines au sein du réseau :

*195.1.10.1 – PC1\_Sara&Marco*

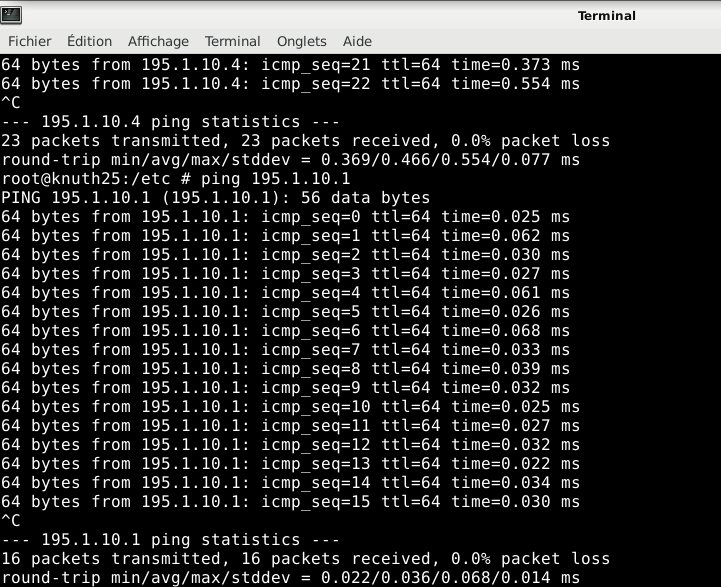
*195.1.10.2 – PC2\_Sara&Marco*

*195.1.10.3 – PC3\_Sara&Marco*

*195.1.10.4 – PC4\_Sara&Marco*

L’utilisation du caractère “&” s’est révélée, à posteriori, une erreur, car la Shell l’associe à d’autres opérations et donc, lors de la saisie du nom pour les commandes (par ex. pour **telnet –y**), cela n’était pas lu correctement, et nous avons été obligés à utiliser seulement les adresses.

Par la suite, nous avons vérifié que les ordinateurs pouvaient communiquer entre eux en lancant la commande **ping <adresse>** et la commande **telnet –y <adresse>**. Nous montrons un résultat de ping à titre d’exemple en Figure 3. La commande telnet a fonctionné aussi bien.



Figure

*Observation de l’activité du réseau (2.2)*

L’observation se fait à travers l’outil Wireshark. Nous le lançons sur *PC2* et ensuite lancons **ping** **<195.1.10.3>**. Nous pouvons donc observer le passage de paquets de communications entre le *PC2* et le *PC3*. Ceci est montré dans la figure ce dessous.

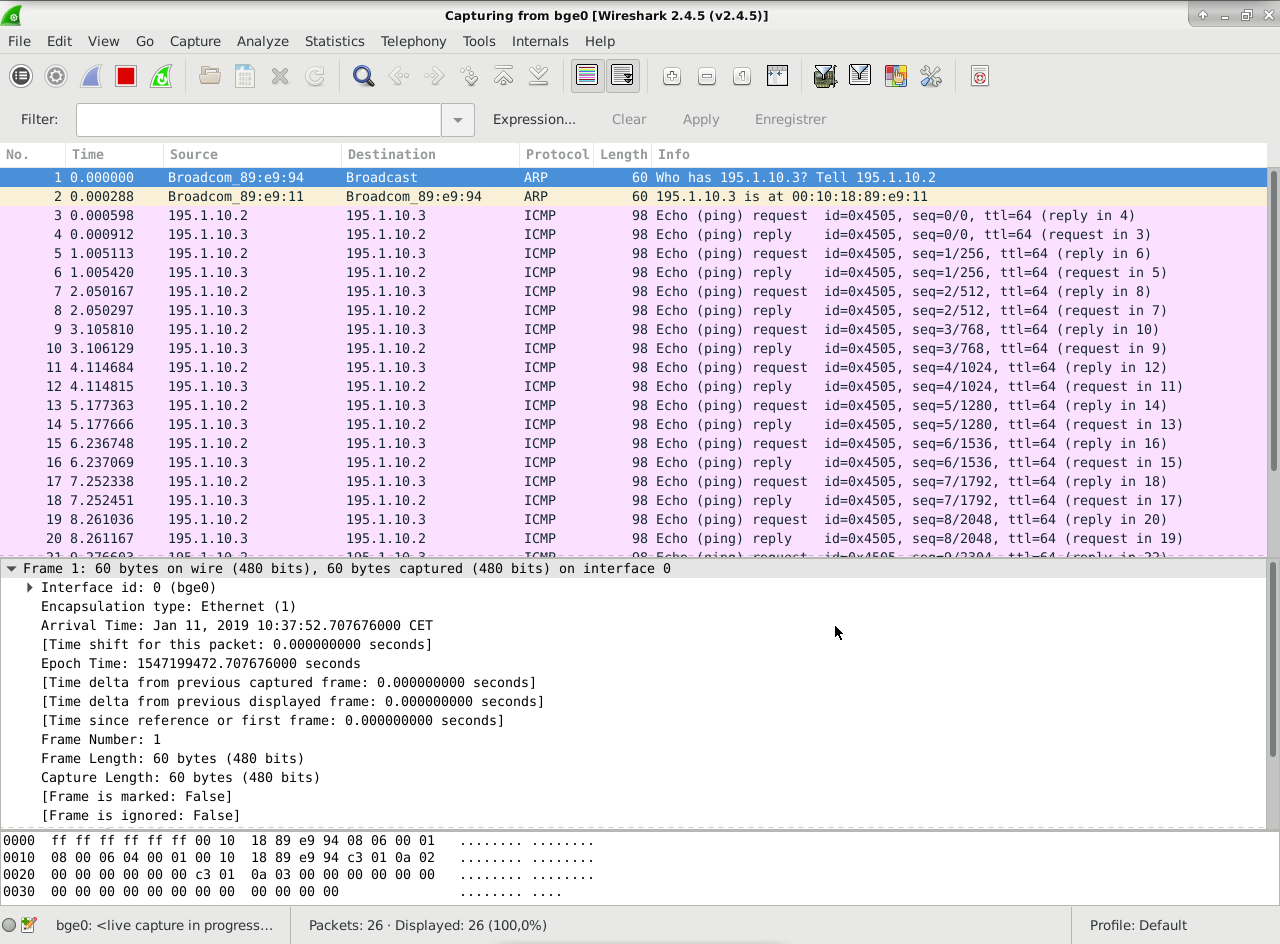
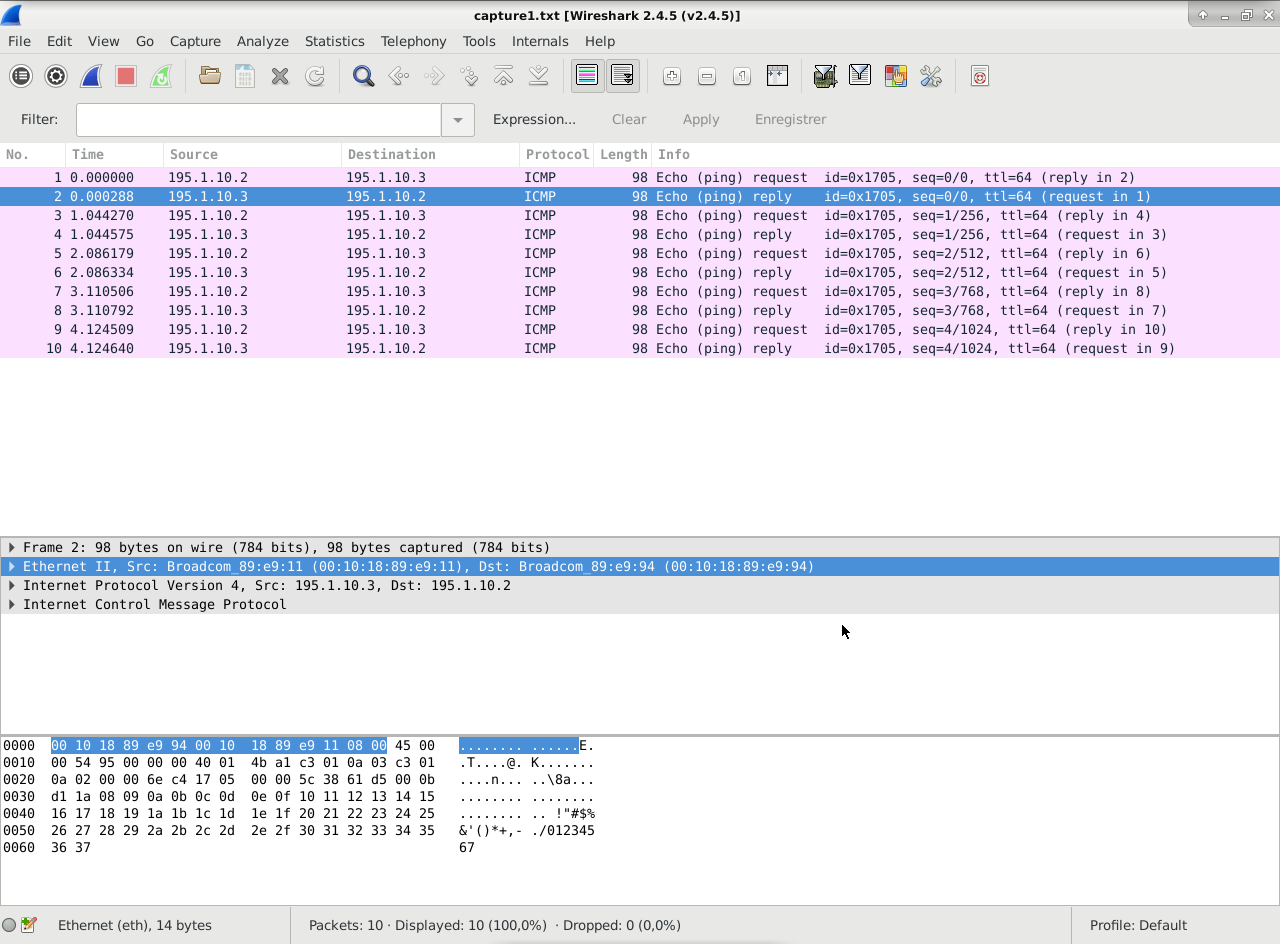


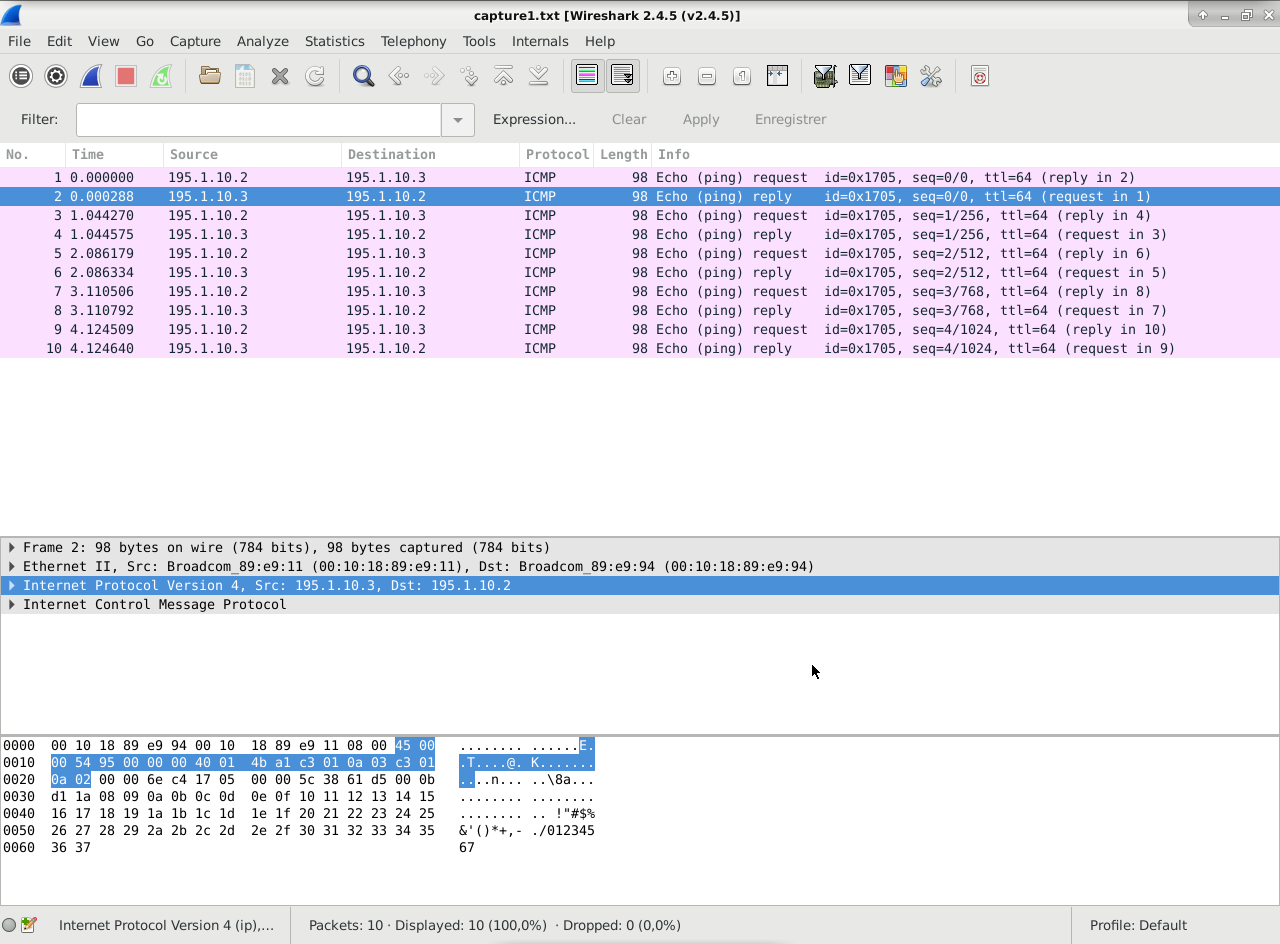
Figure 4

Cette observation nous permet de faire plusieurs remarques :

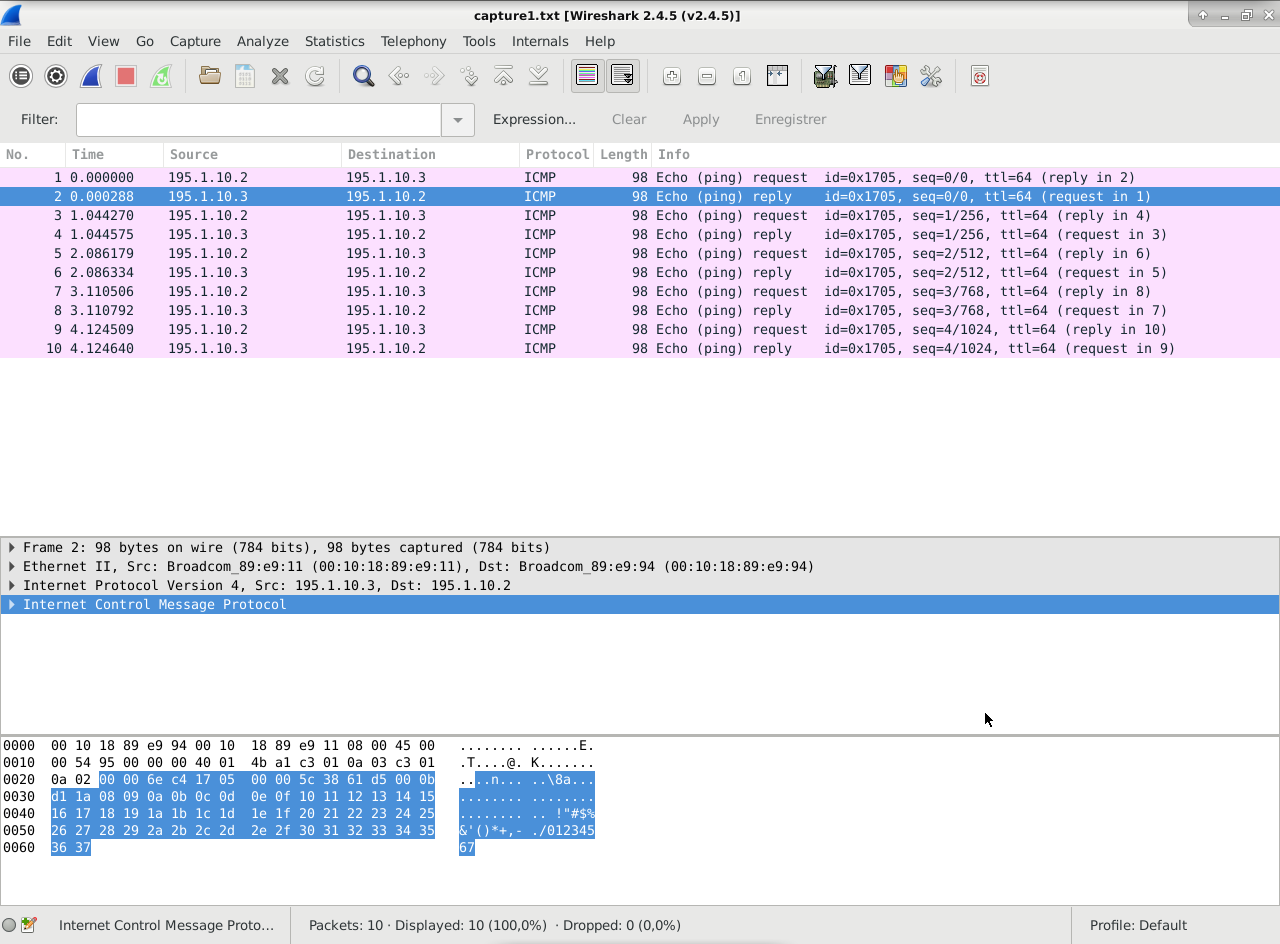
* le fonctionnement de Ping prévoit effectivement l’envoi et la réémission d’un paquet de données, de la taille minimale (64 bytes) pour Ethernet sauf si spécifié autrement.
* les paquets sont de type ICMP. Sur l’outil Wireshark nous pouvons clairement voire les différentes entetes des paquets. D’abord il y a 14 octets de l’entete Ethernet (Figure 5) , ensuite les 20 octets du protocole IP (Figure 6), et par la suite le message ICMP (Figure 7).
* Lors du premier échange de paquets, il y a au préalable l’envoi d’un message avec le protocole ARP à travers le *broadcast*. Ce protocole sert effectivement à obtenir l’adresse de l’interface interlocutrice, et à envoyer son propre adresse. Lors des captures suivantes, nous n’avons plus observé ce couple de paquets ARP, car les interfaces connaissaient leurs adresses. Pour connaitre les adresses mémorisées, il est possible de consulter la table ARP (commande **arp –an**). Nous l’avons consulté lors de la capture, et effectivement les adresses mémorisées lors des échanges parmi les différentes machines y apparaissaient.
* Si la table ARP est vidée (**arp –d –a**), la mémoire des adresse est effacé. Dans ce cas, après délétion de la table, nous avons relancé une capture et nous avons pu observer à nouveau une paire de paquets ARP.



Figure



Figure



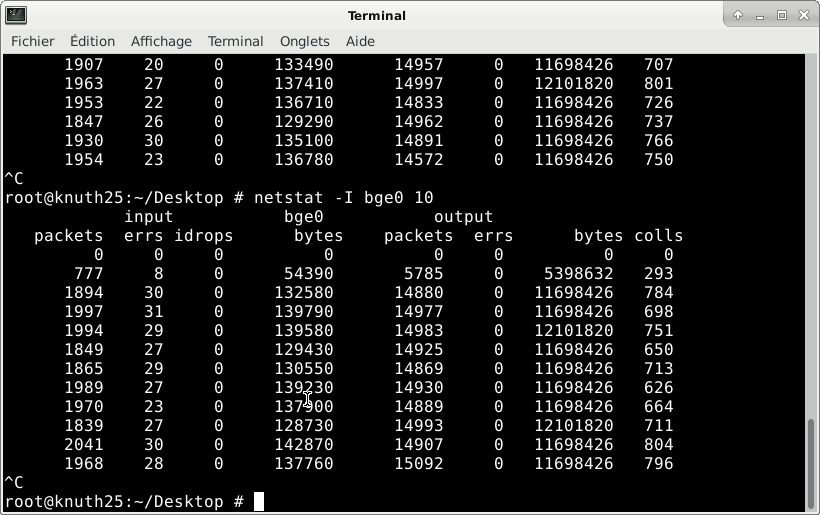
Figure

*Observation du protocole CSMA/CD (2.3)*

Nous avons utilisé l’outil Netstat pour faire des statistiques d’un transfert de paquets avec protocole UDP. Tout d’abord, nous avons fait le test entre 2 ordinateurs, *PC1* et *PC2*, *PC1* étant le client (commande **udpmt**) et *PC2* le serveur (commande **udptarget**).

Nous avons lancé d’abord la commande **netstat –I bge0 10**, pour observer le passage de paquets aux interfaces bge0 tout les 10 secondes, et ensuite les commande client-serveur.

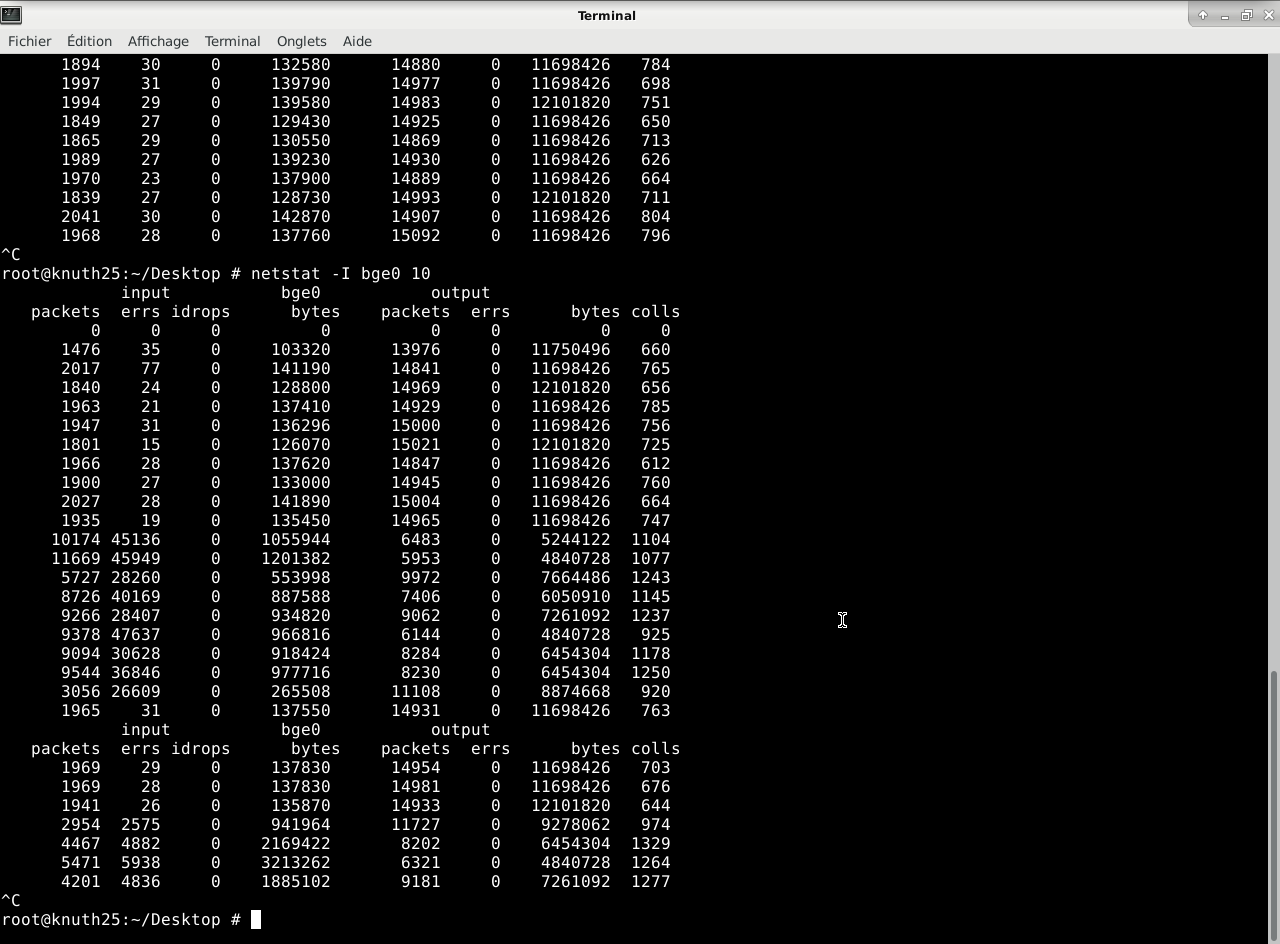
Dans la Figure 8 nous pouvons observer les statistiques pour un envoi de paquets de 64 bytes : après une première valeur de 0, due au démarrage, le nombre de bytes et de collisions au coté client augmente jusqu’à se stabiliser entre 700 et 800. Nous n’avons pas observé d’erreurs.



Figure

Si maintenant nous démarrons une deuxième connexion client-serveur entre *PC3* et *PC4*, nous pouvons observer l’impact que celle-ci a sur le nombre de collisions détectées sur *PC1* (Figure 9, centre de la page).

Effectivement nous pouvons observer que la présence de la deuxième connexion fait augmenter le nombre de collision de 700 à 1200. Le processus est, logiquement, totalement reversible, et lorsque la connexion *PC3*🡪*PC4* est terminée, nous retrouvons la valeur de 700.



Figure

Nous avons alors lance Netstat sur tous les terminaux et étudié la variation des collisions en fonction de la taille des paquets envoyés. Un récapitulatif est fourni dans la Table 1 ci-dessous.

Nous observons que les collisions se repartissent de manière statistique entre les deux serveurs, et la même chose se produit pour les deux clients.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| taille paquets  PC3🡪PC4 | taille paquets PC1🡪PC2 | collision observées à PC1 | collision observées à PC2 | collision observées à PC3 | collision observées à PC4 |
| 64 | 10 | ≈1200 | ≈1200 | ≈350 | ≈350 |
| 64 | 750 | ≈1200 | ≈1200 | ≈450 | ≈450 |
| 64 | 6000 | ≈1300 | ≈1300 | ≈700 | ≈700 |
| 6000 | 6000 | ≈1400 | ≈1400 | ≈700 | ≈700 |

Table

Nous aurions imaginé que, avec l’augmentation de la taille des paquets, le collisions diminuent, car il y a statistiquement moins de chances que deux paquets puissent se trouver en cours d’émission en même temps sur le réseau. Cependant, cette observation experimentale ne va pas dans la même direction. Nous expliquons cette différence avec le fait qu’une collision est déterminée lors du début de l’émission (ce qui arrête toute nouvelle émission), et donc un majeure nombre de collisions veut effectivement dire un majeure temps de bus pour les emissions.