

Mercier Tony  
Jones Marie

## TP 2 : Liaisons de données

### Capture de Trames

Q1 :

ifconfig -a affiche l'état des interfaces réseaux, qu'elles soient actives ou non.

Q2 :

Les interfaces eth0 et lo sont actuellement actives.

Q3 :

L'interface eth0 nous permet de communiquer avec d'autres machines puisqu'elle est en Multicast.

Q4 :

MAC : 98:90:96:bb:8d:7d

IP : 192.168.5.67

Q6 :

time représente le temps mis pour entre l'envoi du paquet et la réception de l'accusé.

Q7 :

Pour nous, les adresses IP sont utilisées, tout d'abord parce qu'elles sont plus courtes, ce qui limite les erreurs de transmission d'information sur ces adresses.

De plus, les adresses IP sont toujours lues de la même façon, ce qui n'est pas forcément le cas avec les adresses MAC.

Enfin, l'adresse MAC est fixe et unique alors que l'adresse IP pourra plus facilement s'adapter si il y a besoin de la changer pour diverses raisons : conflit avec une autre machine, changement de logiciel ...

Q8 :

Les paquets envoyés sont les signaux, et les paquets reçus sont des accusés de réception.

Le protocole utilisé est le protocole IP et plus particulièrement le protocole ICMP .

Q9 :

Le protocole IP correspond à la couche Réseau.

### Ethernet

Q1 :

Le code du protocole est 01, ce qui correspond au protocole ICMP.

Q2 :

Les deux premiers champs de la trame correspondent à la version du protocole IP et à la longueur de l'entête.

Q3 :

Nous sommes en full duplex et la vitesse est de 100 Megabit/secondes.

Ces informations sont utiles lors de la présentation. En effet, c'est à ce moment que l'on va transmettre les données et c'est à ce moment où l'on va avoir besoin de savoir combien de données

vont être émises et comment.

Q4 :

Lorsque l'on lance la commande mii-tool, celle-ci affiche qu'il n'y a plus de lien vers eth0.

Et lorsque l'on lance la commande ifconfig -a, l'interface eth0 n'est plus active, elle n'est plus en "RUNNING".

Q5 :

On constate, en utilisant la commande ifconfig -a, que la connexion lo, qui est la connexion locale, donc avec un voisin est désormais active.

## Concentrateur

Q1 :

On constate que l'on reçoit les messages adressés aux autres machines.

Les données qui sont émises par ma machine, sont également reçues par celle-ci.

Q2 :

Le mode promiscuous sert à recevoir tous les messages, pas seulement ceux adressés à notre machine.

Q3 :

Les interfaces connectées au hub sont en half-duplex. Cela signifie que l'émission et la réception de données ne peut se faire en même temps, au risque de créer une collision.

Q4 :

La topologie physique est une topologie en étoile alors que la topologie logique est de type bus.

Q5 :

Avant la manipulation :

- débit atteint : 10 Megabit/s
- nombre de collisions : 0

Après la manipulation :

- débit atteint : 6.52 Mbit/s
- nombre de collisions : 278

## Commutateur

Q1 :

On constate que le message envoyé d'une machine à une autre n'est détecté qu'une seule fois par la machine qui n'est pas concerné par ce message.

Cette fois-ci nous sommes connectés en full duplex. Cela signifie que l'on peut transmettre tout en recevant des messages sans risquer de collisions.

La topologie physique et la topologie logique sont des topologies en étoile.

Avant la manipulation : 10 Mbit/s

-débit :

- nombre de collisions : 0

Après la manipulation :

- débit atteint : 93.9 Mbit/s

-nombre de collisions : 0

Q2 :

Les adresses MAC affichées sont les mêmes que nos machines et les ports sont bien ceux auxquels nous sommes connectés sur le switch.

Le switch a obtenu ces adresses lors de l'envoi d'un message. Il a fait correspondre l'adresse IP à l'adresse MAC. Le rôle de la table de commutation est d'associer chaque adresse MAC d'une machine au port

à laquelle elle est connectée sur le switch afin de ne pas passer par des machines intermédiaires pour transmettre un message.

Q3 :

Le switch a besoin de connaître l'adresse MAC , mais n'a pas besoin de l'adresse IP.

Le hub fait parti de la couche physique sur alors que le switch fait parti de la couche liaison.

Q4 :

Le switch est plus avantageux car il permet de transmettre un message directement à la machine concerné. De plus, si l'on change d'adresse IP ( ce qui arrive fréquemment) il n'est pas nécessaire de reconfigurer

la table de commutation car il connaîtra déjà l'adresse MAC (qui est unique ). Cela permet également d'éviter la saturation du réseau.

Q5 :

On constate que toutes les machines reçoivent le message. Il s'agit d'un broadcast, il est donc normal que toutes les machines aient reçu le message. L'adresse est FF:FF:FF:FF:FF:FF ( il s'agit de l'adresse Broadcast).

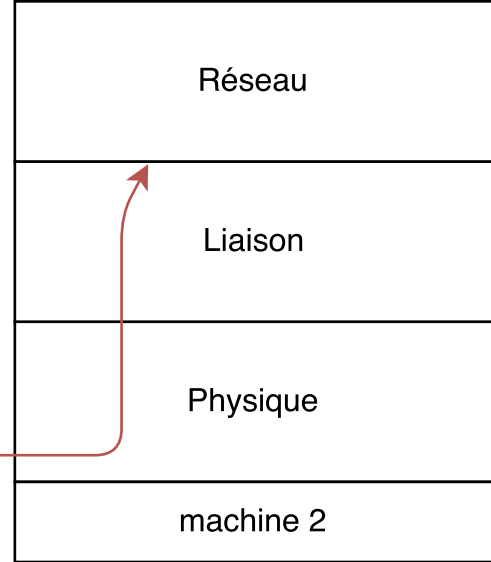
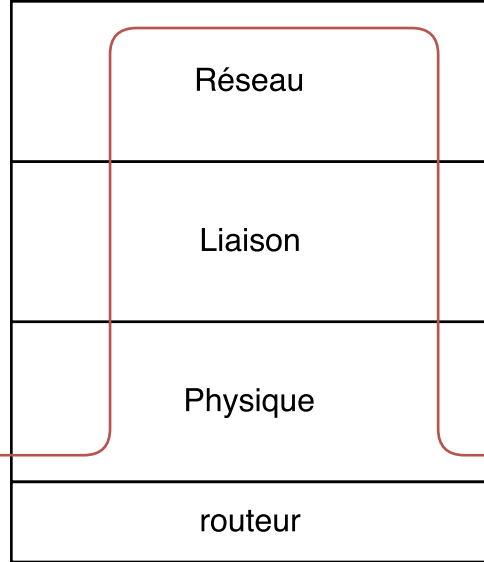
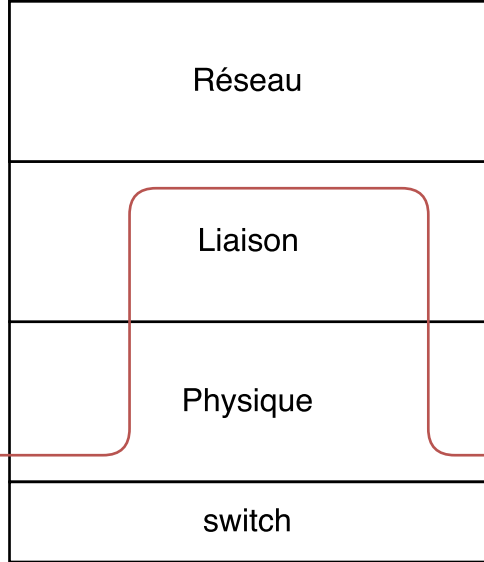
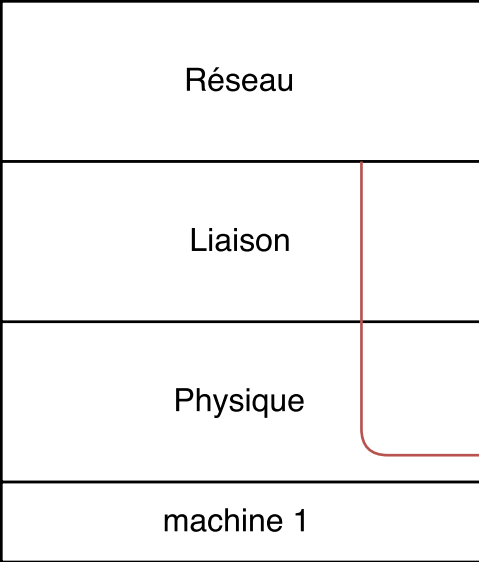
Routeur :

Q6 :

L'adresse MAC de la source reste inchangée. En revanche l'adresse MAC de la destination, qui est celle dont l'IP a changé, n'est pas la même pour l'envoi du paquet. L'adresse de la source correspond à l'adresse de la machine, mais celle de la destination correspond à l'interface reliant le switch au routeur.

Q8 :

On constate que les machines sur le réseau 192.168.5.0 reçoivent toutes le broadcast. En revanche, les machines sur le réseau 192.168.1.0 ne reçoivent rien.



Q9 :

On constate que les machines du réseau 192.168.5.0 ne reçoivent pas le message. Concernant la machine sur le réseau 192.168.1.0, la réponse reçue provient de l'adresse 192.168.1.200 qui est l'adresse de l'interface du routeur.

Q10 :

On constate que les machines du réseau 192.168.5.0 reçoivent bien le message. Les paquets reçus proviennent d'une machine ayant l'IP 255.255.255.255 . Ce mode de transfert est désactivé par défaut car il est alors possible d'envoyer des messages à tous les sous-réseaux même si ils ne sont pas concernés.

Q11 :

Une diffusion limitée permet d'envoyer un message en broadcast à toutes les machines du sous-réseau. Le routeur n'est pas utile puisqu'il s'agit d'un message envoyé sur le réseau local. Une diffusion dirigée permet d'envoyer un message en broadcast à toutes les machines du réseau même si elles n'appartiennent pas au même sous-réseau.

Un transfert unicast permet d'envoyer un message d'une machine à une autre , peu importe si elle est sur le même sous-réseau ou non. Si elles ne sont pas sur le même réseau, le routeur servira de passerelle et fera la liaison entre les deux réseaux.

Q12:

Un routeur, contrairement à un switch, identifie l'adresse réseau auquel le paquet est destiné, puis le redirige sur la bonne interface.

ARP :

Q2 :

On constate que voisin 1 reçoit les paquets mais voisin 2 (dont on a donné l'adresse IP) ne reçoit rien.

Le rôle du cache ARP permet de voir la correspondance entre les adresses IP et les adresses MAC.

Q3 :

On constate que l'adresse MAC de notre voisin est associée à son adresse IP. Notre machine a eu connaissance de cette adresse grâce à l'entête de la trame.

Q4 :

Le code associé au protocole ARP est 0806.

Q5:

Le champ constitué des 6 octets correspond à l'adresse MAC cible de la destination. Il s'agit d'un champ "vide" permettant par la suite de compléter les informations sur l'adresse MAC de la destination une fois que celle-ci sera identifiée

Q6:

L'adresse MAC se situe au même endroit c'est à dire sur les six premiers octets de l'octet 0x20.

Q7 :

La fin des paquets est bourrée afin d'allonger le paquet qui sans cela serait trop court

bits	0-7	8-15	16-23	24-31	32 - 39	40-47	48-55	56-63
	adresse MAC du broadcast						adresse MAC de la source ...	
	... adresse MAC de la source				0806 : code protocole ARP		type de matériel	
	type de protocole		taille de l'adresse	taille de l'adresse du protocole	type du message (request/reply ici )		adresse MAC de la source ...	
	Text ... adresse MAC de la source				adresse IP de la source			
	adresse MAC à déterminer						adresse IP de la destination ...	
	... adresse IP de la destination		bourrage					
	bourrage							
	bourrage							

# Requête ARP

bits	0-7	8-15	16-23	24-31	32 - 39	40-47	48-55	56-63
	adresse MAC de la destination (anciennement source)						adresse MAC de la source ...	
	... adresse MAC de la source (anciennement destination à déterminer)				0806 : code protocole ARP		type de matériel	
	type de protocole		taille de l'adresse	taille de l'adresse du protocole	type du message (reply ici )		adresse MAC de la source ...	
	Text ... adresse MAC de la source (anciennement destination à déterminer)				adresse IP de la source (anciennement destination)			
	adresse MAC de la destination (anciennement source )						adresse IP de la destination ...	
	... adresse IP de la destination (anciennement source)							

# Réponse ARP

## Mise en place de l'exercice 2 du TD "Réseaux IP"

### Mise en place des connexions physiques :

- la machine A : machine avec l'IP original 192.168.5.65 est connectée par le port R1/1 au Routeur 2 de la baie rouge sur l'interface fastEthernet 0/0
- la machine B : machine avec l'IP originale 192.168.5.64 est connectée par le port V1/1 au Routeur 2 de la baie verte par l'interface Ethernet 0/1
- le routeur 2 de la baie rouge est connecté au routeur 1 par l'interface fastEthernet 0/1 sur l'interface GigabitEthernet 0/1
- le routeur 2 de la baie verte est connecté au routeur 1 par le biais des ports V01 (respectivement R01) par l'interface ethernet 0/0 sur l'interface GigabitEthernet 0/0

### Configuration des interfaces :

#### Routeurs :

Sur minicom

pour le routeur 1 :

```
> enable
>configure terminal
>interface GigabitEthernet 0/0
>ip address 192.168.5.129 255.255.255.192
>no shutdown
> exit
>interface GigabitEthernet 0/1
>ip address 192.168.5.1 255.255.255.192
>...
>ip routing
```

pour le routeur 2 :

```
>...
>interface fastEthernet 0/0
>ip address 192.168.5.65 255.255.255.192
>...
>interface fastEthernet 0/1
>ip address 192.168.5.2 255.255.255.192
>...
```

pour le routeur 3 (routeur 2 de la baie verte) :

```
>...
>interface ethernet 0/0
>ip address 192.168.5.130 255.255.255.192
>...
>interface ethernet 0/1
>ip address 192.168.5.193 255.255.255.192
>...
```



## Machines :

machine A :

```
>ifconfig eth0 192.168.5.66 netmask 255.255.255.192
>route add -net 192.168.5.0 gw 192.168.5.65 net mask 255.255.255.192
>route add -net 192.168.5.128 gw 192.168.5.65 net mask 255.255.255.192
>route add -net 192.168.5.192 gw 192.168.5.65 net mask 255.255.255.192
```

machine B :

```
>ifconfig eth0 192.168.5.194 netmask 255.255.255.192
>route add -net 192.168.5.0 gw 192.168.5.193 net mask 255.255.255.192
>route add -net 192.168.5.128 gw 192.168.5.193 net mask 255.255.255.192
>route add -net 192.168.5.64 gw 192.168.5.193 net mask 255.255.255.192
```

Lorsque de la machine A on tente “ ping 192.168.5.193” on obtient :

Reply from 192.168.5.65 [...] Host Unreachable