Yann Garbé

TP n°2 Réseaux

CAPTURE DE TRAMES

1) Que fait cette commande (utilisez le man) ?
> La commande "$ ifconfig -a" affiche des informations sur toutes les interfaces actives ou non.

2) Quelles interfaces réseaux sont actuellement actives (running) ?
> Il y a actuellement 2 interfaces réseaux qui sont actives :
- L'interface eth0
- L'interface lo

3) Parmi ces interfaces, quelle est celle qui vous permet de communiquer avec d'autres machines ?
> Parmis ces deux interfaces, seule l'interface eth0 permet de communiquer avec d'autres machine.
(eth0 est en MULTICAST et utilise Ethernet, tandis que lo est locale).

4) Quelles sont les adresses MAC et IPv4 de cette interface ?
Pour eth0 :
- adresse MAC 98:90:96:bb:8c:ea
- adresse IPv4 192.168.5.70

5) Utilisez la commande ping pour tester la connectivité de votre machine vers la machine du voisin.
{
$ping 192.168.5.69
PING 192.168.5.69 (192.168.5.69) 56(84) bytes of data.
64 bytes from 192.168.5.69: icmp_seq=1 ttl=64 time=1.39 ms
64 bytes from 192.168.5.69: icmp_seq=2 ttl=64 time=0.721 ms
64 bytes from 192.168.5.69: icmp_seq=3 ttl=64 time=0.619 ms
64 bytes from 192.168.5.69: icmp_seq=4 ttl=64 time=0.704 ms
}

6) Que représente la valeur « Time » retournée par la commande ping ?
> La valeur "time" représente le temps qu'a mis le paquet pour atteindre la machine du voisin et revenir vers notre machine

7) . Selon vous, de manière générale, pourquoi utilise-t-on l'adresse IP et non directement l'adresse MAC pour
les communications réseaux ?
> L'adresse MAC d'une machine est propre à sa carte réseau et non à la machine.

Wireshark
8) Lancez la commande ping vers votre voisin. D'après les informations capturées et décodées par
wireshark, quels sont les paquets envoyés et reçus suite à l'exécution du ping ? Quels protocoles sont utilisés ?

>Voici les deux paquets correspondant à un ping :
182 81.448044408 192.168.5.70 192.168.5.69 ICMP 98 Echo (ping) request id=0x66ef, seq=6/1536, ttl=64 (reply in 183)
183 81.448622352 192.168.5.69 192.168.5.70 ICMP 98 Echo (ping) reply id=0x66ef, seq=6/1536, ttl=64 (request in 182)

> Le protocole utilisé pour les deux paquets est ICMP

9) A quelles couches appartiennent les protocoles cités précédemment ?

>Le protocole ICMP appartient à la couche Réseau.

10) . le filtre à l'affichage : après avoir effectué la capture précédente, dans le menu « analyse display filters », faites en sorte que s'affiche uniquement le dialogue entre votre machine et celle du voisin.

> Il suffit d'ajouter dans l'onglet de filtrage "ip.addr == 192.168.5.69"

11) le filtre de capture : dans le menu « capture > options », faites en sorte que soit capturé uniquement ledialogue entre votre machine et celle du voisin.

> Dans l'onglet capture > option, on sélection eth0, puis on utilise le filtre IPv4.
"host 192.168.5.69"

ETHERNET

1) Sélectionnez un paquet ICMP. Situez, dans la fenêtre du bas, le champ de l'en-tête ethernet qui assure la fonction de multiplexage, c'est-à-dire qui indique le protocole de couche supérieur encapsulé dans la
trame. Quel est le code du protocole de couche supérieur ?

> Le code du protocole de couche supérieur est eth.addr

2) Quel est le rôle des 2 premiers champs de l'en-tête de la trame ?
- Le premier champ {98 90 96 bb 8c 81} indique l'adresse de destination (celle de la machine du voisin)
- Le deuxième champ {98 90 96 bb 8c ea} indique l'adresse source (celle de notre machine)

3) Utilisez les commandes mii-tool et ethtool pour connaître le mode de duplex et la vitesse de l'interface. Quelle est l'utilité de ces commandes et à quel niveau du modèle OSI interviennent-elles principalement ?

> La commande $sudo mii-tool eth0 indique une erreur :
> SIOCGMIIREG on eth0 failed: Input/output error

Avec l'aide de $sudo ethtool eth0
Speed: 100Mb/s
Duplex: Full

4) Déconnectez le câble de la prise « EXT » qui connecte votre machine au réseau EXTérieur. Lancez de nouveau les commandes mii-tool et ifconfig -a. Que constatez-vous ?

(Remarque : c'est le cable blanc)

> En utilisant $ifconfig -a, on remarque que l'interface réseau eth0 n'est plus active (le mot RUNNING n'est plus présent).

> De plus, en utilisant $sudo ethtool eth0, on remarque que le duplex ainsi que la vitesse sont inconnues :
Speed: Unknown!
Duplex: Unknown! (255)

5) Connectez-vous maintenant à un voisin en point-à-point, sans passer par un actif réseau (hub, switch,
routeur), en réalisant le brassage au niveau de la baie (attention au type de câble).
Puis tester la connectivité de votre machine vers la machine du voisin.

Instruction : - Brancher le cable eth0 qui était branché dans EXT, dans v4/3
- Le voisin fait de même avec v6/2 (192.168.5.72)
- Utiliser un câble blanc de même numéro (19 par exemple), puis le connecter dans v4/3 et v6/2
- Nous pouvons désormais effectuer un ping vers 192.168.5.72 et 192.168.5.70

Client
[3] local 192.168.5.72 port 50938 connected with 192.168.5.71 port 5001
[ID] Interval Transfer Bandwidth
[3] 0.0-10.4 sec 6.12 MBytes 4.95 Mbits/sec

Serveur

Collisions avant : 0
Collisions après : 238

CONCENTRATEUR

Deux voisins : 192.168.5.71 et 192.168.5.72

1) Lancez une capture de trames sur un poste, et transmettez un ping entre les deux autres postes. Que
constatez-vous ? Déduisez-en la manière dont fonctionne cet équipement. Les données émises par un
poste sont-elles reçues par ce même poste ?

> Les ping fonctionnent sur les deux adresses voisines. De plus, le HUB transfère le ping à tout le monde, même quand ce n'est pas le destinataire.
> Le HUB semble utiliser une structure en étoile.

2) Recommencez la manipulation en désactivant le mode promiscuous de wireshark. A quoi sert-il ?
> Le ping se comporte normalement(un ping, un destinataire, une source). On suppose que le mode promiscuous permet de recevoir des packets qui ne nous sont pas destinés.

3) Quel est le mode de duplex des interfaces connectées au hub ? Quelle en est la signification ?
> Le mode est en Half-duplex : on ne peut pas recevoir et envoyer en même temps.

4) Quelles sont les topologies physique et logique du réseau constitué par le concentrateur et les postes qui y sont connectés ?²
> La topologie physique du réseau avec concentrateur est une topologie d'étoile.
> La topologie logique du réseau avec concentrateur est une topologie de bus.

5) Utilisez « iperf -s » sur un poste et « iperf -c ip_du_serveur » sur un autre poste pour lancer un test de bande passante. Notez le débit atteint et les valeurs du compteur de collisions (ifconfig) avant et après la manipulation.
Connectez un poste supplémentaire sur le hub (soit au minimum 4 postes) et réalisez de nouveau la manip en parallèle sur les deux paires de postes.
Notez le débit atteint et les nouvelles valeurs des compteurs de collisions. Déduisez-en la manière dont fonctionne un hub.

[# Client
[3] local 192.168.5.72 port 50938 connected with 192.168.5.71 port 5001
[ID] Interval Transfer Bandwidth
[3] 0.0-10.4 sec 6.12 MBytes 4.95 Mbits/sec

Serveur

Collisions avant : 0
Collisions après : 238

Avec un deuxième couple serveur/client en parallèle :

Client
[3] local 192.168.5.72 port 50946 connected with 192.168.5.71 port 5001
[ID] Interval   Transfer   Bandwidth
[3] 0.0-10.3 sec 5.62 MBytes 4.60 Mbits/sec

On suppose donc que le hub envoie et renvoie les trames à toutes les machines, sans analyser leur entêtes.

COMMUTATEUR

1) Réactivez le mode promiscuous. Recommencez les manipulations précédentes et répondez aux questions
1 à 5 de la partie « concentrateur » en remplaçant le concentrateur par un commutateur (switch).

1-1) Lancez une capture de trames sur un poste, et transmettez un ping entre les deux autres postes. Que
constatez-vous ? Déduisez-en la manière dont fonctionne cet équipement. Les données émises par un
poste sont-elles reçues par ce même poste ?
> Les pings utilisés a travers un commutateur se dirigent vers le bon poste et uniquement le bon poste.

1-2) Recommencez la manipulation en désactivant le mode promiscuous de wireshark. A quoi sert-il?> Le ping se comporte normalement(un ping, un destinataire, une source). On suppose que le mode promiscuous permet de recevoir des packets qui ne nous sont pas destinés.
> Rien n'a changé

1-3) Quel est le mode de duplex des interfaces connectées au hub ? Quelle en est la signification ?
> Le mode est en Full-duplex : on peut recevoir et envoyer des paquets en même temps

1-4) Quelles sont les topologies physique et logique du réseau constitué par le commutateur et les postes qui y sont connectés ?
> La topologie physique du réseau avec commutateur est une topologie d'étoile.
> La topologie logique du réseau avec commmutateur est une topologie de bus.

1-5) Notez le débit atteint et les nouvelles valeurs des compteurs de collisions. Déduisez-en la manière dont fonctionne un hub.

Client
[3] local 192.168.5.72 port 50948 connected with 192.168.5.71 port 5001
[ID] Interval   Transfer   Bandwidth
[3] 0.0-10.0 sec   113 MBytes 94.6 Mbits/sec

Serveur

Pas de collision avec le commutateur.

2) Comparez les adresses MAC listée avec celles de vos postes et les ports du switch sur lesquels ils sont
connectés. Comment le switch a-t-il obtenu ces adresses ? Quel est le rôle de la table de commutation
(appelée aussi table d'adresses MAC) ?
{

```
Address       Type        Ports
----    -----------       --------    -----
 All    000d.2860.9b00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    9890.96bb.78d4    DYNAMIC     Fa0/4
   1    9890.96bb.8cea    DYNAMIC     Fa0/12
   1    9890.96bb.8f55    DYNAMIC     Fa0/11
Total Mac Addresses for this criterion: 7
```

3) Pour fonctionner, le switch a-t-il besoin de connaître les adresses mac des trames ? les adresses IP des paquets ? Déduisez-en à quels niveaux du modèle OSI interviennent un switch et un hub et quelles sont les unités de données sur lesquelles ils agissent.
> Les adresses mac sont affichées, on peut supposer qu'un switch a besoin de les connaître.
> Les adresses IP ne sont pas nécessaires, il s'agit d'un réseau local.
> Les switch et les hubs interviennent au niveau de la couche liaison.

4) Concluez sur les avantages du switch par rapport au hub.
> La communication en full duplex utilisé par le commutateur permet un meilleur débit au niveau de l'envoi de données. De plus, nous évitons les problèmes de collision.

5) Lancez maintenant une capture de trames sur plusieurs postes connectés au switch et transmettez un ping
vers l'adresse IP 192.168.5.255. Que constatez-vous ? Comment s'appelle ce type de transfert ? Quelle est l'adresse ethernet de destination des trames reçues ?
> On remarque l'apparition du ping chez les autres postes.
> Type de transfert : Broadcast
> Les adresses ethernet correspondent aux autres postes connecté au switch.

ROUTEUR

{Composition
Deux postes branchés sur le switch. Le poste destiné au routeur est branché à la console du routeur.
La machine destinée au poste 3 est branché au routeur (0/1). Le routeur est branché au switch}

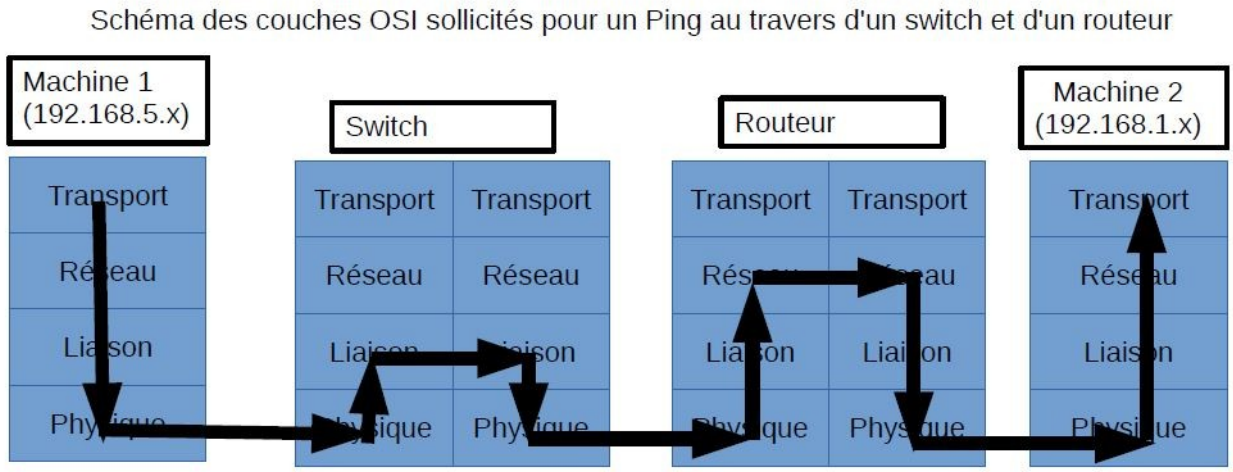
6)Après avoir lancé une capture de trames sur les postes 2 et 3, lancez un ping depuis le poste 1 vers le poste 2, puis vers le poste 3 (voir schéma). Il s'agit d'un transfert unicast. Comparez les valeurs du champ TTL de l'entête IP des paquets reçus sur les postes 2 et 3. Pourquoi sont-elles différentes ?
Quelle est l'utilité de ce champ ?
> Les ping envoyés ont un TTL de 64 avec comme destination le poste 2.
> Avec l'accès au routeur, le TTL est décrémenté de 1, donc les ping avec comme destination le poste 3 ont un TTL de 63.
> Ce champs permet d'éviter les problème de boucle de routage.

7) Quelle devrait être la valeur du TTL pour que le poste 1 puisse communiquer avec le poste 2, mais pas avec le poste 3 ? Testez la validité de votre réponse en envoyant, depuis le poste 1, un ping avec ce TTL vers les postes 2 et 3 (voir « man ping »).
Lancez une capture sur le poste 1 et envoyez un ping du poste 1 vers le poste 3 en conservant le TTL que vous avez choisi. Que se passe-t-il ?
>Il faut que le TTL du paquet envoyé par le poste 1 soit de 1, car avec l'accès au routeur, le TTL passera à 0, en supprimant le paquet.
> Le paquet du ping ne peut pas acceder au poste 3.

8) Lancez de nouveau un ping depuis le poste 1 vers le poste 3. Quelles sont l'adresse MAC source de la trame reçue (sur le poste 3) et l'adresse MAC de destination de la trame envoyée (à partir du poste 1) ?
Selon vous, à quelles interfaces ethernet correspondent ces adresses ? Pour vous aider, lancez la commande « show interface fastethernet » sur le routeur.
> Poste 1 :
Adresse MAC reçue = adresse du routeur
Poste 3 :
Adresse MAC reçue : adresse du routeur
Interfaces ethernet GigabitEthernet 0/1

9)Comment le poste 1 a-t-il su que la trame ethernet contenant le paquet IP à destination du poste 3 devait être envoyée au routeur ?
> C'est grâce à la table de routage que le poste 1 a su que la trame devait être envoyée au routeur

10).Dessinez un schéma des couches OSI utilisées dans chaque équipement mis en jeu dans le transfert unicast (2 postes, 1 switch et 1 routeur), et tracez une ligne représentant le flux de données passant d'un équipement à l'autre (communication horizontale) en traversant les couches (communication verticale).



11.Lancez une capture de trames sur plusieurs postes des deux réseaux et lancez un ping depuis un poste du réseau 192.168.5.0 vers l'adresse 255.255.255.255. Il s'agit d'un transfert en diffusion limitée. Que constatez-vous ?
> Le ping ne passe pas par le routeur, donc la machine se trouvant dessus ne le détecte pas. Cependant, le ping est détecté par les autres machines.

12. Lancez une capture de trames sur plusieurs postes des deux réseaux et lancez un ping depuis le réseau 192.168.1.0 vers l'adresse 192.168.5.255. Que constatez-vous ?
> En toute logique, le ping n'est perçu par aucun des postes. Par contre, on constate que le routeur a envoyé une réponse suite au ping.

13. Recommencez la manipulation précédente. Il s'agit d'un transfert en diffusion dirigée. Que constatez-vous? Quelle est l'adresse IP des paquets reçus? Selon vous, pourquoi ce mode de transfert est-il désactivé par défaut ?
> Le ping est transmis aux autres postes du réseau.
> On reçoit l'adresse IP de la machine, ainsi que l'adresse MAC du routeur.
> Ce mode de transfert est désactivé par défaut par sécurité mais également afin d'empêcher une éventuelle surcharge réseau.

14. Quelle est la différence entre diffusion limitée, diffusion dirigée et unicast ?
> Diffusion limitée : Il s’agit d’un paquet broadcast seulement sur le réseau de la machine actuelle.
> Diffusion dirigée : Il s’agit d’un paquet broadcast qui utilisera le routeur pour être transmis dans d’autres réseaux
> Unicast : Un paquet qui va être dirigé depuis une source vers une destination, une machine vers une autre.

15. Comment un routeur réagit à ces différents types de paquets? Concluez sur la différence entre un routeur et un switch vis-à-vis de la diffusion IP.
> Diffusion limitée : Pas de redirection, le routeur pas l’ignorer.
> Diffusion dirigée : Redirection vers les machines correspondantes. Attention cependant, cette diffusion est souvent désactivé.
> Unicast : Redirection vers la destination.

ARP

1. Utilisez la commande «arp» pour consulter le cache ARP de votre poste et y ajouter une entrée statique faisant correspondre l'adresse MAC du voisin 1 avec l'adresse IP du voisin 2.

2. Lancez une capture de trames sur voisin 1 et voisin 2 et lancez, depuis votre poste, un ping sur voisin 2. Que constatez-vous? Déduisez-en le rôle du cache ARP.
> L’autre machine ne reçoit pas le paquet car il ne lui est pas destiné. Le cache ARP permet donc de connaître l’adresse MAC correspondant à l’adresse IP demandée.

3. Lancez une capture de trames et exécutez un ping vers votre voisin. Consultez la table ARP et la capture de trames. Que constatez-vous? Comment votre machine a-t-elle eu connaissance de l'adresse MAC de votre voisin?
> L’adresse MAC de la machine voisine a été ajoutée. La machine a eu connaissance de l’adresse MAC en diffusant en broadcast une demande de correspondance avec l’adresse IP voulue. La machine du voisin a répondu.

4.Analysez l'en-tête ethernet pour identifier le code associé au protocole ARP.
>Le code associé au protocole ARP est 0x0806

5. Dans la requête ARP, que contient le champ constitué des 6 octets commençant à l'octet n°0x20. Quel est son rôle?
> C’est le champ de l’adresse MAC de destination (celle que l’on ne connaît pas). C’est pour cela que le champ est défini à 0 dans la requête.

6. Dans la réponse ARP, situez l'adresse MAC objet de la requête précédente.
> Il s’agit de la deuxième addresse MAC dans le paquet (les 7 à 12 permiers octets pour être plus précis).

7. Pourquoi la fin des paquets ARP est-elle constituée de 0 ou de motifs répétitifs?
> La trame Ethernet doit avoir une taille minimum (afin d’assurer que la station va emettre assez longtemps pour détecter des éventuelles collisions) et il est donc nécessaire de remplir le reste. La fin des paquets ARP sert juste donc « à remplir le quota » de taille.

8. Faites un schéma représentant les différents champs de la requête et de la réponse ARP, ainsi que leur longueur.s