TP n°2 : Liaison de données

Ce TP a pour objectif que vous maîtrisiez certains concepts et outils de base des réseaux informatiques.

Les concepts :
- modèle en couches
- encapsulation / multiplexage
- adressage (MAC / IP) et résolution d'adresses
- commutation / routage
- diffusion

Les outils :
- analyse de paquets
- configuration des interfaces
- configuration d'équipements réseaux

CAPTURE DE TRAMES

Après avoir ouvert une session graphique sur votre poste, ouvrez un terminal fenêtré et lancez la commande ifconfig -a

1. Que fait cette commande (utilisez le man) ?
2. Quelles interfaces réseaux sont actuellement actives (running) ?
3. Parmi ces interfaces, quelle est celle qui vous permet de communiquer avec d'autres machines ?
4. Quelles sont les adresses MAC et IPv4 de cette interface ?
5. Utilisez la commande ping pour tester la connectivité de votre machine vers la machine du voisin.
6. Que représente la valeur « Time » retournée par la commande ping ?
7. Selon vous, de manière générale, pourquoi utilise-t-on l'adresse IP et non directement l'adresse MAC pour les communications réseaux ?

Pour mieux comprendre comment les données sont échangées sur le réseau, vous allez utiliser un logiciel appelé « analyseur de paquets » :
- lancez le logiciel *wireshark*
- tapez Ctrl+I et sélectionnez l'interface connectée sur le réseau de la salle

Appropriez-vous l'application en consultant les info-bulles et l'aide, le cas échéant.
La fenêtre est divisée en 3 parties :
- en haut, la liste des paquets reçus ou envoyés par l'interface
- en bas, le contenu du paquet sélectionné, au format hexadécimal
- au milieu, *wireshark* traduit les données brutes du paquet dans un format compréhensible

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 ?

Le panneau du milieu de Wireshark est basé sur le modèle OSI inversé : en haut, les couches basses (physique, liaison de données, etc.), en bas, les couches hautes (transport, application).

9. A quelles couches appartiennent les protocoles cités précédemment ?

Vous pouvez constater que vous capturez des paquets émis par d'autres machines du réseau. Pour éviter que vos captures ne soient polluées, vous pouvez utiliser des filtres.
Wireshark propose deux types de filtres :

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

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 ?
2. Quel est le rôle des 2 premiers champs de l'en-tête de la trame ?
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 ?
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 ?

Supprimez la route vers le réseau extérieur en lançant la commande :
route del -net default

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.

CONCENTRATEUR

Connectez votre poste de travail sur le concentrateur (hub) situé dans la baie de brassage.
Assurez-vous que deux de vos voisins y sont connectés également.
Supprimez les filtres de capture et d'affichage préalablement configurés.

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 ?
2. Recommencez la manipulation en désactivant le mode *promiscuous* de wireshark. A quoi sert-il ?
3. Quel est le mode de duplex des interfaces connectées au hub ? Quelle en est la signification ?
4. Quelles sont les topologies physique et logique du réseau constitué par le concentrateur et les postes qui y sont connectés ?
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.

Les postes connectés entre eux via des concentrateurs forment un **domaine de collision**.

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).

Pour paramétrer les équipements réseau et obtenir des informations sur leur configuration, il faut établir une liaison série entre votre poste de travail et le port console de l'équipement en question.
Cette liaison permet d'établir une connexion dite « hors bande », c'est-à-dire hors de la bande passante du réseau ethernet.
Connectez-vous sur le port console d'un switch, noté Sx-C (avec x=R,J,B ou V selon votre baie de brassage). Utilisez pour cela un câble série DB9-RJ45 (câble bleu et plat) et lancez le programme « minicom ».

Une fois connecté, si la question « voulez-vous lancer le setup du switch ? » vous est posée, répondez « non ».
Vous êtes actuellement en mode USER EXEC (prompt >), qui ne permet de lancer qu'un nombre réduit de commandes, que vous pouvez lister en tapant « ? ». Passez en mode privilégié (prompt #) en tapant « enable ». Puis lancez la commande « show mac-address-table » ou « show mac address-table ».

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) ?
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.
4. Concluez sur les avantages du switch par rapport au hub.
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 ?

Un commutateur permet de segmenter les domaines de collisions.
Les postes connectés par l'intermédiaire de commutateurs constituent un **domaine de broadcast**.

ROUTEUR

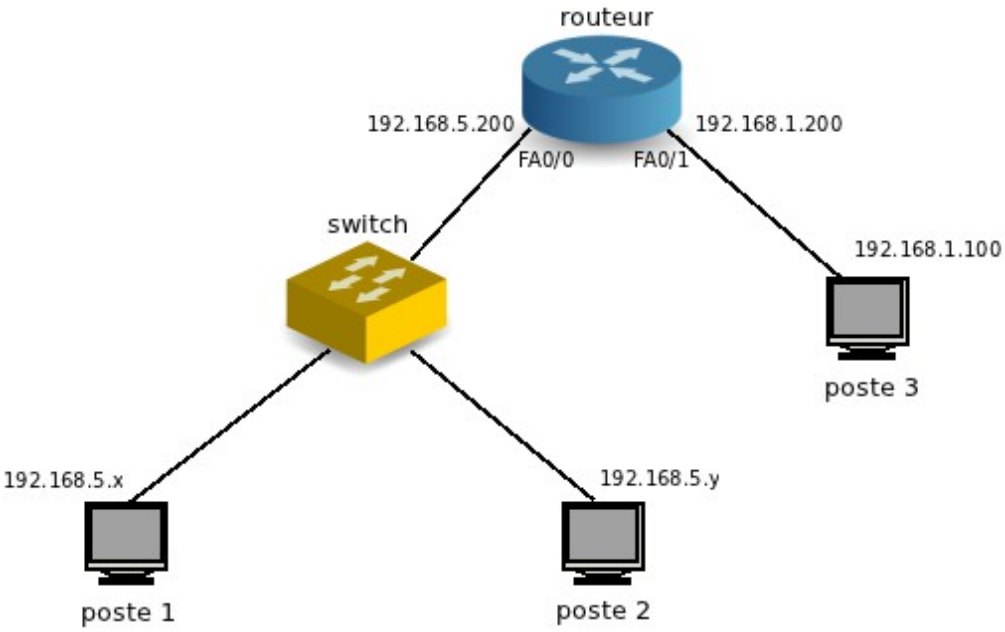
Connectez-vous sur le port console d'un routeur, noté Rx-C (avec x=R,B,V ou J selon votre baie de brassage).

Tapez les commandes suivantes :

```
Router>enable   // pour passer en mode privilégié
Router#configure terminal   // pour passer dans le mode de configuration globale
--- Configuration des interfaces ---
Router(config)#interface fastEthernet 0/0   // ou « interface ethernet 0 » sur les routeurs 25xx
                                            // ou « interface gigabitEthernet 0/0 » sur les 29xx
Router(config-if)#ip address 192.168.5.200 255.255.255.0
Router(config-if)#no shutdown   // allumer cette interface
Router(config-if)#exit

Router(config)#interface fastEthernet 0/1   // ou « interface ethernet 1 » sur les routeurs 25xx
                                            // ou « interface gigabitEthernet 0/1 » sur les 29xx
Router(config-if)#ip address 192.168.1.200 255.255.255.0
Router(config-if)#no shutdown   // allumer cette interface
Router(config-if)#exit
--- Activation du routage ---
Router(config)#ip routing
```

Utilisez la commande *ifconfig* et son manuel pour affecter l'adresse 192.168.1.100 et le masque 255.255.255.0 à l'un de vos postes, et connectez-le à l'interface fastethernet0/1 du routeur (attention au type de câble).
Connectez le switch sur l'interface fastethernet0/0.
Sur chaque poste lancez la commande suivante pour qu'il sache vers quelle adresse transmettre les paquets destinés aux autres réseaux :
sudo route add default gw 192.168.x.200 (avec *x=1* ou *x=5* suivant le réseau du poste)



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.
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 ?
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` » / « `show interface ethernet` » sur le routeur.
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 ?
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 ?
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 ?

Exécutez les commandes suivantes sur le routeur :

```
Router(config)#interface fastEthernet 0/0    // ou « interface ethernet 0 » sur les routeurs 25xx
                                             // ou « interface gigabitEthernet 0/1 » sur les 29xx
Router(config-if)#ip directed-broadcast
```

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 ?
14. Quelle est la différence entre diffusion limitée, diffusion dirigée et unicast.
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.

ARP

Connectez de nouveau au moins 3 postes sur un switch.
Le cas échéant, reconfigurez les paramètres IP initiaux de chacun des postes.

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.

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).
Supprimez du cache ARP les entrées statiques et toute entrée éventuelle concernant votre voisin.

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 ?
4. Analysez l'en-tête ethernet pour identifier le code associé au protocole ARP.
5. Dans la requête ARP, que contient le champ constitué des 6 octets commençant à l'octet n° 0x20. Quel est son rôle ?
6. Dans la réponse ARP, situez l'adresse MAC objet de la requête précédente.
7. Pourquoi la fin des paquets ARP est-elle constituée de 0 ou de motifs répétitifs ?
8. Faites un schéma représentant les différents champs de la requête et de la réponse ARP, ainsi que leur longueur.

Veillez à bien faire la différence entre table ARP et table d'adresses MAC.