TPR-2 de Réseaux en L3 : Sous-réseaux, Routage statique et Analyse de trames (4h30)

Auteur : Olivier GLÜCK, Université Lyon 1

Objectifs

- découpage d'un réseau en sous-réseaux
- configuration d'un routeur et des tables de routage de manière statique
- manipulation des tables ARP
- analyse de trames Ethernet avec `wireshark` ou `tcpdump`
- observation des protocoles Ethernet, IP, ARP, ICMP

Pré-requis

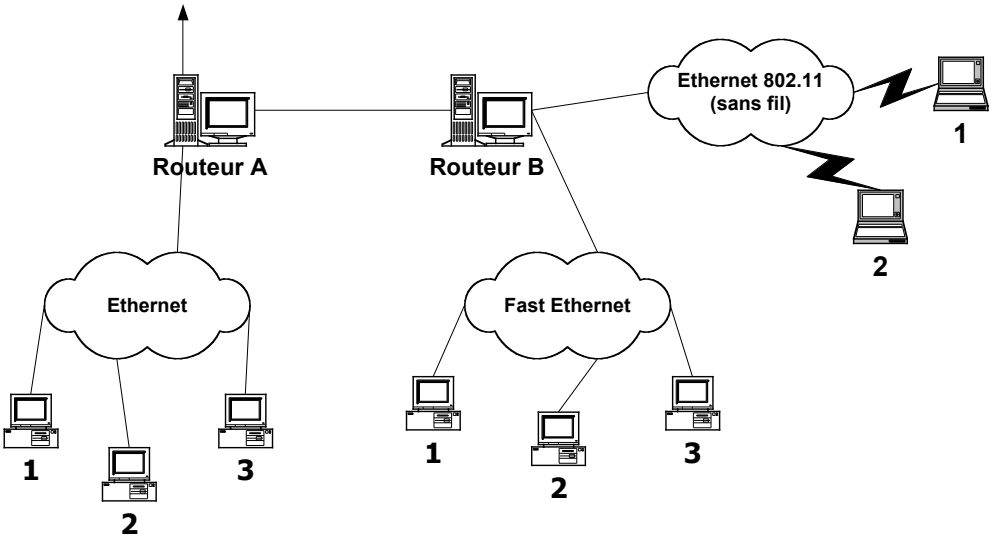
Configuration d'un réseau local avec des adresses IPv4.

1. Introduction (pour vous aider !)

1.1. Notion de routage et sous-réseaux

Routage

Internet est un réseau de réseaux : plusieurs sous-réseaux physiques sont raccordés entre eux pour former un unique réseau global, le réseau mondial. L'interconnexion des différents sous-réseaux est assurée par l'intermédiaire de la couche IP et l'utilisation de nœuds particuliers, connus sous le nom de routeurs. Ces machines particulières permettent de faire le lien (on parle aussi de passerelle) entre les différents sous-réseaux qui peuvent utiliser ou non la même technologie. Elles possèdent généralement autant d'interfaces réseau que le nombre de sous-réseaux auxquels elles sont raccordées. Dans l'exemple ci-dessous, les routeurs A et B permettent l'interconnexion de trois sous-réseaux ; le routeur A peut également faire office de passerelle vers « l'extérieur ».



Les routeurs redirigent les paquets IP provenant d'un sous-réseau vers un autre jusqu'à acheminer les paquets vers le sous-réseau du destinataire final. Pour ce faire, le routeur doit disposer localement de certaines informations contenues dans des tables de routage (topologie du réseau…). Par exemple, le routeur B doit savoir que pour atteindre une machine du sous-réseau « Ethernet », il doit envoyer les paquets vers le routeur A. Une table de routage comporte au moins deux colonnes : la première pour la destination (ou le réseau de destination), et la seconde pour l'adresse de l'élément du réseau correspondant au saut suivant (« *next hop* ») pour atteindre cette destination.

On parle de routage statique lorsque la façon d'atteindre un sous-réseau (information contenue dans la table de routage) est fixée une fois pour toute à l'initialisation du réseau. A l'opposé, on parle de routage dynamique quand les tables de routage sont mises à jour périodiquement par l'échange d'information entre les routeurs.

Adressage de sous-réseaux

Une adresse IP est découpée en un identifiant réseau et un identifiant machine (cf. TPR-1). Pour plus de souplesse et une meilleure utilisation de l'espace d'adressage, tous les bits de l'identifiant machine ne sont pas utilisés pour numéroter les machines. Certains bits sont utilisés pour identifier le sous-réseau. L'adresse IP est alors composée d'un identifiant de réseau, un de sous-réseau et un de machine. La taille de l'identifiant de sous-réseau dépend du nombre de sous-réseaux à distinguer.

En principe, l'acheminement est réalisé à partir de l'identifiant réseau dont la taille, dépendant de la classe d'adressage, est connue de chaque routeur. L'utilisation d'un identifiant supplémentaire (sous-réseau) de taille variable nécessite d'indiquer à chaque machine du réseau quels sont les bits de l'adresse IP à prendre en compte pour définir l'acheminement dans le réseau. Cette information est fournie par le masque de sous-réseau.

Pour réaliser l'acheminement d'un paquet vers un destinataire, la couche IP locale vérifie à l'aide du masque de sous-réseau si le destinataire appartient au même sous-réseau qu'une destination présente dans la table de routage de la machine. Pour cela, elle effectue un & logique entre le masque associé à une destination et l'adresse IP destination. En dernier recours, c'est la route par défaut qui est retenue si elle est présente dans la table de routage.

1.2. Outils de capture de paquets

Pour communiquer, les machines échangent des informations sous forme de paquets qui sont l'unité de données échangées sur le réseau. Il est possible « d'écouter » le câble Ethernet et de regarder ce qui se passe quand vous lancez des commandes comme `ping`, `rlogin`, …

Un premier outil permettant d'observer le réseau s'appelle `tcpdump`. Pour écouter le trafic sur l'interface `eth0`, il faut taper la commande `tcpdump -i eth0`. Par défaut, `tcpdump` écoute en « *promiscuous mode* », c'est à dire qu'il capture et analyse toutes les trames circulant sur le réseau même celles qui ne concernent pas la machine sur laquelle il tourne.

Un deuxième outil, un peu plus convivial que `tcpdump` car utilisable en mode graphique avec un affichage plus lisible, est l'utilitaire `wireshark`. N'oubliez pas de cocher « `Update list of packets in real time` ».

Ces deux outils permettent d'établir des filtres de capture de paquets de manière assez fine. La syntaxe des filtres utilisés est la même pour `wireshark` que pour `tcpdump`. Par exemple, la commande `tcpdump -i eth0 tcp dst port 53` permet de ne capturer sur l'interface `eth0` que les segments TCP dont le port de destination est 53. Pour plus d'informations, consultez la page manuelle de `tcpdump`.

1.3. Commandes et fichiers à utiliser

PENSER A UTILISER LES PAGES MAN DE LINUX :
`man <nom de la commande>`

- `ip a show dev [interface], ip a add [ip_addr/mask] dev [interface], ip link set dev [interface] up/down`
- `ping, ethtool, dmesg`
- `/etc/network/interfaces`
- `/etc/hosts` – permet de nommer symboliquement les machines
- `/etc/networks` – permet de nommer symboliquement les réseaux

- `ss` – permet d'afficher des informations réseaux (équivalent de `netstat`)
- `ip route` – permet de visualiser ou configurer la table de routage d'une machine
- `ip n (ip neighbor)` – permet de visualiser la table ARP d'une machine (équivalent de `arp`)
- `traceroute` – permet de visualiser les routeurs rencontrés pour atteindre l'adresse indiquée
- `zenmap` – permet de visualiser la topologie du réseau
- `tcpdump` et `wireshark` pour capturer des paquets sur le réseau
- `apt-get` pour installer un package

2. Routage et sous-réseaux

Lors du TPR-1, vous avez configuré un réseau « global » à l'aide de switchs et hubs. Ce réseau était constitué d'un seul segment Ethernet ; chaque machine utilisait une seule interface réseau pour se raccorder à l'ensemble du réseau. Vous allez maintenant créer différents sous-réseaux.

ATTENTION : Lors de cette séance, il vous est demandé de noter sur une feuille le schéma du réseau ainsi que les commandes tapées durant ce TP pour faire fonctionner le réseau.

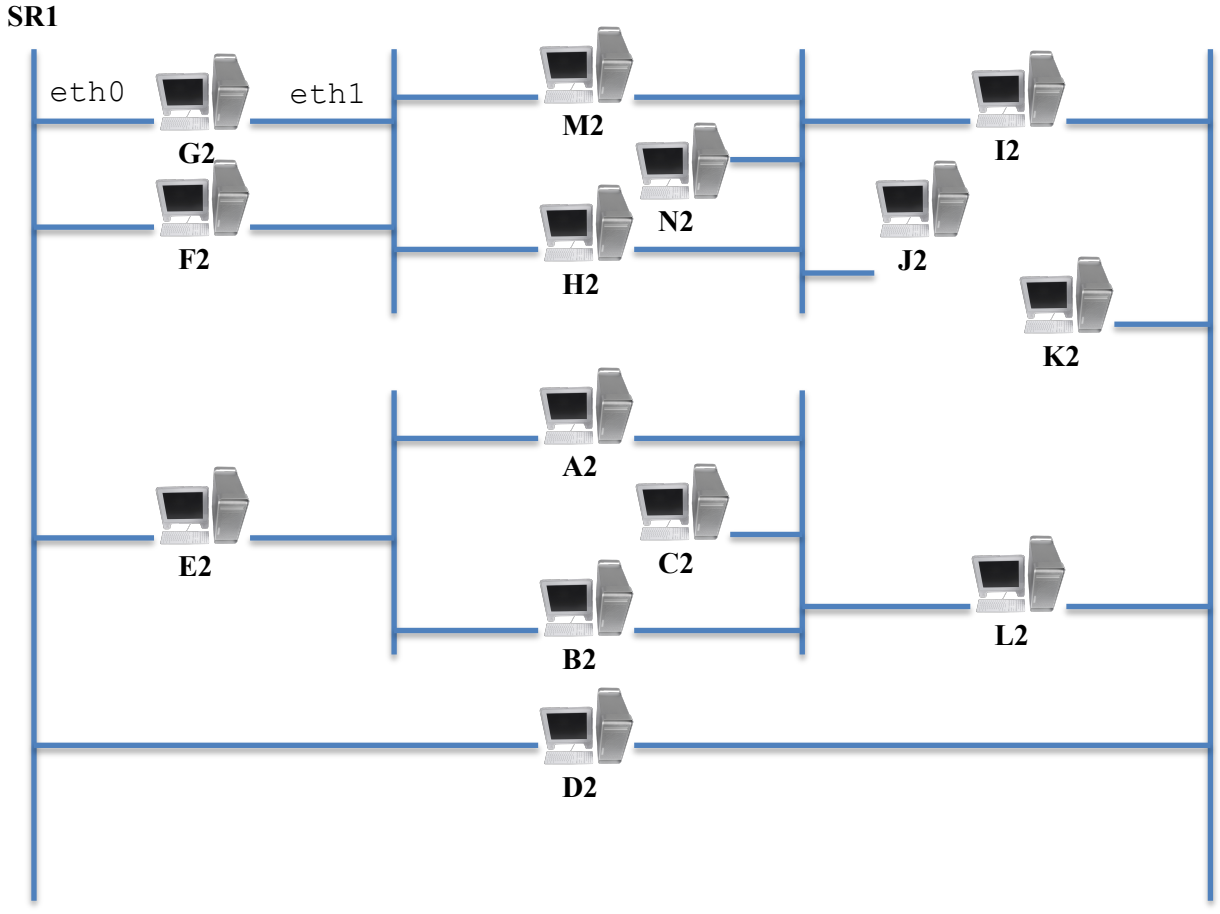
2.1. Raccordement matériel

Manipulation

Dans votre salle de TP, réalisez le câblage de la figure ci-dessous. Notez sur le schéma ci-dessous, les interfaces réseau utilisées pour chaque machine. Pour réaliser le réseau global, au moins un des équipements doit être à 10Mbit/s.

Question

De quel matériel avez-vous besoin (notez-le sur le schéma) ? Combien de sous-réseaux sont définis ? Donnez un nom (SR1, SR2, ...) aux différents sous-réseaux sur le schéma et listez pour chaque sous-réseau les machines qu'il comporte. ***Il vous est conseillé de mettre une étiquette sur chaque équipement pour signaler à quel sous-réseau il correspond.***



2.2. Choix des adresses INTERNET des machines et des sous-réseaux

Un organisme vous attribue l'adresse de réseau suivante : 132.227.0.0

Question

Quelle est la classe de l'adresse qui vous a été attribuée ? On souhaite pouvoir adresser 16 sous-réseaux dans le réseau 132.227.0.0 et 4094 machines par sous-réseau. On rappelle que les valeurs du champ « machine » pour lesquelles tous les bits sont à 0 ou à 1 sont réservées aux adresses de réseaux et de broadcast. Quel est le masque de sous-réseau utilisé ?

Manipulation

Choisissez (le plus simplement possible) les adresses de sous-réseaux ainsi que celles des machines. Prenez garde à prendre des sous-réseaux distincts pour chacun des segments Ethernet. Complétez le schéma précédant en écrivant à côté du nom de l'interface réseau, l'adresse IP associée. Indiquez également sur le schéma les adresses de broadcast et de sous-réseaux.

2.3. Configuration des adresses IP des machines et tests

Manipulation

Utilisez les commandes `ip link set` *et* `ip a add` *pour configurer les interfaces Ethernet de votre machine. Si votre machine utilise deux cartes réseaux, vous placerez* `eth0` *à gauche et* `eth1` *à droite comme indiqué sur le schéma. Arrivez-vous à joindre toutes les machines de votre réseau local ? Indiquez sur le schéma la nature des équipements auxquels vous êtes directement connectés.*

Manipulation

Vérifier votre configuration et essayez de communiquer avec chacune des autres machines connectées au réseau. Que constatez-vous ? Expliquez…

2.4. Tables de routage

Les entrées dans les tables de routage sont de deux types :

- Les routes directes permettant d'atteindre les destinations qui sont sur un réseau directement connecté et qui ne nécessitent pas le passage par un routeur intermédiaire.
- Les entrées de type « *gateway* » permettant de joindre des destinations n'étant pas dans un sous-réseau auquel la machine est directement connectée ; il est alors nécessaire d'indiquer l'adresse du routeur qui va prendre en charge l'acheminement des paquets à destination de ces sous-réseaux distants.

Manipulation

Visualisez les tables de routage à l'aide de la commande `ip route`*. Essayez les commandes suivantes et commentez précisément pour chacune d'entre-elles les affichages produits en vous aidant de la page* `man` *:*

```
ip -s link, ss -s, ss -a, ss -e, ss -t, ss -u,
ip route show all, ip route show dev eth0
```

Question

Que concluez-vous sur les tables de routage actuelles ? En regardant la configuration physique de votre réseau définie à la section 2.1, déterminez pour chaque couple source/destination si plusieurs routes sont possibles. En déduire les routes manquantes permettant d'atteindre l'ensemble des machines distantes.

Manipulation

Mettez à jour les tables de routage de votre machine afin de pouvoir atteindre n'importe quelle autre machine du réseau. Vous utiliserez pour cela la commande `ip route` *en ajoutant une ligne dans la table de routage*

pour chaque sous-réseau inconnu dans votre table. On veillera à positionner correctement le netmask pour chaque destination ajoutée. Exemple : `ip route add|del 132.227.0.0/20 via 132.227.0.4`

Manipulation

Testez avec `ping` *si toutes les machines sont joignables. Si par exemple, vous n'arrivez pas à joindre la machine M2 à partir de la machine A2, vous pouvez utiliser l'utilitaire* `tcpdump` *ou* `wireshark` *sur la machine M2 pour visualiser si la station reçoit la requête du* `ping`*. Pour les machines que vous n'arrivez pas à joindre, déterminez où se trouve le point de blocage en utilisant la commande* `traceroute` *et/ou en essayant d'atteindre une machine plus proche se trouvant sur la même route.*

Manipulation

Activez sur les machines routeur le « forwarding » : par défaut, les machines ne permettent pas le passage des paquets d'une interface réseau vers une autre, ce qui devrait être le cas sur les routeurs. Exécutez pour cela les commandes suivantes :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables --policy FORWARD ACCEPT
```

Testez de nouveau avec la commande `ping`*. Cette fois-ci, vous devriez pouvoir atteindre chaque machine du réseau ! Testez également les adresses de broadcast.*

2.5. Validation et mesure de performances

Manipulation

Que fait la commande `ping -R` *? Testez cette commande. Vérifiez avec la commande* `traceroute` *le chemin parcouru pour atteindre chaque machine du réseau. Utilisez l'utilitaire* `zenmap` *pour visualiser la topologie du réseau. Remplissez un tableau à deux dimensions (vous pouvez utiliser TOMUSS* http://demo710.univ-lyon1.fr/MOTUS/*) qui indique pour chaque couple source/destination le nombre de routeurs traversés. Visualisez la table de routage d'une machine passerelle distante en utilisant la commande* `ip route`*.*

Question

Quelles sont les performances de chaque sous-réseau ? Qu'induit la traversée d'un routeur en termes de performances ? ***Faites un tableau récapitulatif à deux dimensions*** *(vous pouvez utiliser TOMUSS)* ***indiquant les temps de latence mesurés à l'aide d'un*** `ping` ***entre chaque machine du réseau. Vous ferez ces mesures d'abord avec des*** `ping` ***de taille maximale.***

2.6. Modification des tables de routage

Question et manipulation

Au lieu du nombre de sauts, le critère pour un routage optimal devient : « Eviter de traverser un équipement à 10Mbit/s. ». Modifiez votre table de routage en conséquence, vérifiez que vous pouvez joindre toutes les machines et refaites les mesures de performance. Que constatez-vous par rapport à ces mesures ?

Question et manipulation

En utilisant l'agrégation de routes et/ou la route par défaut, optimisez votre table de routage pour qu'elle contienne le moins de lignes possible. La route par défaut englobe toutes les adresses IP d'Internet et correspond à la destination 0.0.0.0 avec un netmask 0.0.0.0.

2.7. Simulation de pannes et dépannage

Dans cette partie, vous allez simuler des pannes sur votre machine et vous irez réparer une autre machine. Les pannes dans un réseau peuvent être matérielles (câble défectueux, mauvais contact, branchement sur un mauvais port, équipement défectueux…) ou bien logicielles (interface non active ou mal configurée, table de routage erronée, `ip_forward` non activé…).

Question et manipulation

Simulez des pannes sur votre machine et pensez à effacer les traces (`history -c`, fermez les terminaux). *Réparez le réseau* ***en vous installant sur une autre machine*** *que celle que vous aviez configurée jusqu'à présent.*

2.8. Visualisation des tables ARP

Pour communiquer sur Ethernet, les paquets IP sont encapsulés dans des trames Ethernet. Avant d'envoyer un paquet IP sur le réseau, une machine doit donc connaître l'adresse Ethernet (adresse physique) de la machine destination. Pour traduire l'adresse IP en adresse Ethernet, la machine locale utilise le protocole ARP en faisant un *broadcast* Ethernet à toutes les machines du sous-réseau, la machine concernée renvoie alors son adresse Ethernet (on parle aussi d'adresse MAC).

Question

En utilisant la commande `ip n`*, visualisez votre table ARP locale. Quelle ligne de commande utilisez-vous ? Quelle est la taille d'une adresse Ethernet ? Quelle est l'adresse MAC de votre machine ?*

Manipulation

Effacez le contenu de votre cache ARP à l'aide de la commande `ip n`*. Quelle ligne de commande utilisez-vous ? Regardez l'évolution de votre table ARP au cours du temps avant/après avoir fait des* `ping` *vers des machines que vous avez déjà contactées ou non.*

3. Utilisation de `tcpdump` et `wireshark`

Pour cette partie, travaillez avec votre voisin.e (deux machines reliées en réseau sont nécessaires).

3.1. Analyse de protocoles (ICMP et ARP)

Manipulation

Effacez toutes les entrées présentes dans la table ARP à l'aide de la commande `ip n`*. Lancez* `wireshark` *sur la machine exploratrice et faites un* `ping` *entre la machine source et la machine destination. La commande* `ping` *utilise le protocole ICMP pour contacter la machine distante et le protocole ARP pour obtenir l'adresse Ethernet de la machine distante. Décrivez à l'aide d'un chronogramme et expliquez l'enchaînement dans le temps des paquets échangés. Retrouvez dans le format hexadécimal, les valeurs des différents champs (en-tête Ethernet, données ARP, ...).*

Manipulation

Videz les tables ARP de la machine source (A) et de la machine destination (B). Faire un `ping` *de A vers B. Consultez les tables ARP. La table de B contient-elle l'adresse de A ?*

Question

Qu'est-ce qui permet d'identifier les paquets comme étant de type ARP ou ICMP ? Les paquets ARP ou ICMP sont-ils encapsulés dans des paquets IP ? Quel est le rôle des différents champs ARP ? Quel est le format d'une trame Ethernet ? Comment le niveau Ethernet détermine-t-il la fin du paquet ? Faites un schéma comportant les différents protocoles examinés et montrant les différents niveaux d'encapsulation des protocoles les un dans les autres. Faites également un schéma correspondant au format des paquets ARP observés.

Manipulation

Utilisez les options `-s` *puis* `-p` *de* `ping` *et analysez le comportement au niveau du contenu des paquets échangés. A partir de quelle taille de* `ping` *constatez-vous de la fragmentation IP ? Observez à l'aide de* `wireshark` *comment est faite la fragmentation.*

3.2. Découverte d'un mot de passe

Manipulation

Créez un compte utilisateur sur une machine avec la commande `adduser`*. Entrez un mot de passe que vous allez ensuite essayer de capturer. Sur cette même machine, installez le serveur telnet et lancez-le :*

```
apt-get update
apt-get install telnetd
systemctl start inetd
```

Démarrez le serveur ssh :

```
systemctl start ssh
```

Lancez `tcpdump` *et/ou* `wireshark` *sur une deuxième machine qui sera traversée quand la troisième machine ci-après va se connecter à la première machine. A partir d'une troisième machine, ouvrez avec* `telnet` *une connexion distante vers la machine sur laquelle vous venez de créer le compte, en tant que l'utilisateur nouvellement créé. Analysez les trames capturées et essayez de retrouver le mot de passe de l'utilisateur. Essayez maintenant la même manipulation en utilisant* `ssh` *pour réaliser la connexion à distance. Quel est l'intérêt de* `ssh` *? A la fin de la manipulation, effacez le compte utilisateur avec* `deluser`*.*