# Routage IP et sous-réseaux

P. Sicard

10 novembre 2021

## 1 Rappels

L'ensemble des protocoles de la couche 3 du modèle OSI (appelée ***couche réseau***) permet la communication entre les différents type de réseaux de niveau 2 ( ***couche liaison de donnée***). Plusieurs problèmes doivent être résolus, avec principalement :

- Hétérogénéité des réseaux,
- Reconnaissance générale des machines (adressage universel),
- Acheminement des paquets (routage)

Dans Internet, des réseaux indépendants sont interconnectés et le protocole de la couche réseau IP fournit un service de communication universel. Ce service doit être indépendant de la structure et de la technologie utilisées localement sur chacun des réseaux.

Physiquement, deux réseaux (ou plus) sont interconnectés par l'intermédiaire d'une machine qui possède un point d'attache sur chacun des réseaux.

Cette machine qui joue un rôle particulier sur les réseaux s'appelle un *routeur* (ou passerelle ou en anglais *gateway*). Par opposition, les machines utilisateurs sont appelées *hôte*. Un routeur possède donc plusieurs interfaces réseaux et donc plusieurs adresses Internet.

Le mécanisme permettant l'acheminement des paquets à bon port à travers un ensemble de réseau est appelé *routage*.

L'adresse Internet (que ce soit IPV4 ou IPV6) est partagée en deux parties :

- l'adresse du réseau sur lequel la machine est située ;
- l'adresse de cette machine sur ce réseau.

Le routage se fait à l'aide des adresses des « réseaux ». C'est sur la première partie de l'adresse que se basent les routeurs pour faire parvenir les messages au réseau destination. Une fois les messages arrivés sur le réseau destination, c'est le protocole ARP qui permet d'acheminer les messages du dernier routeur vers les hôtes.

Pour décider de la route à suivre, les routeurs gèrent une table appelée ***table de routage*** qui leur permet de répondre à la question : « d'après l'adresse destination du paquet, quel est le prochain routeur à qui envoyer le paquet pour qu'il arrive à destination ? ». Ce

routeur est forcément un « voisin » connecté à un de ses réseaux. Une table de routage contient donc une liste (Adresse de réseau, Netmask associé, Adresse de routeur voisin). Le chemin complet n'est noté nulle part. Le Netmask permet de décider quels bits sont comparé entre l'adresse de la machine destination et du réseau donné dans la table.

Si l'on prend l'analogie avec une voiture circulant sur un réseau routier. A chaque carrefour, le conducteur demande quelle est la route à prendre pour arriver au prochain carrefour sans jamais connaître le chemin complet jusqu'à la destination.

Les machines hôtes doivent également gérer une telle table de routage pour savoir à quel routeur il faut s'adresser sur son réseau local pour atteindre le réseau destination.

On peut distinguer deux fonctionnalités indépendantes dans le routage :
- la prise de décision sur la route à prendre au vue de la table de routage et de l'adresse destination contenu dans le paquet (entête IP), c'est l'aiguillage des paquets ;
- la mise à jour des tables de routage, elle peut être faite manuellement ou réalisée automatiquement à l'aide d'applications basées sur des échanges d'information entre les routeurs et les hôtes.

# 2 Manipulation des tables de routage

Nous avons vu que toutes les machines, qu'elles soient hosts ou routeurs gèrent une table de routage. Nous avons la possibilité par l'intermédiaire de certains outils standards de manipuler cette table, comme par exemple afficher les entrées, ajouter ou supprimer une entrée...(voir la documentation sur les commandes systèmes).

- Pour afficher la table de routage sous FreeBSD :
  `netstat -rn -f inet`

- Pour mettre à jour la table :
  `route  add|delete destination gateway`
  Exemple : `route add 172.16.0.0/20 192.168.2.4`

- Pour rendre une machine routeur :
  `sysctl net.inet.ip.forwarding=1`

- Pour accéder au réseau du batiment F, le plus simple est d'appeler le script :
  `/var/backups/BackToNormal` qui affecte la l'adresse officielle du PC à l'interface `em0` et remet le routage par défaut vers le bon routeur.

- Pour configurer les routeurs Cisco, voir la documentation abrégée fournie (sur le moodle)

# 3 Déroulement du TP

**Conseils avant d'attaquer bille en tête** :

- Utilisez les fichiers `hosts` permettant de manipuler des noms symboliques.
- Il est **IMPERATIF**, avant tout câblage, de faire un plan d'adressage précisant les noms des machines, leurs adresses et les noms des interfaces réseaux. Sans quoi vous allez passer 3 heures à débuguer votre montage.

## 3.1 Manipulation des tables de routage

Le but de cette manipulation est de vous remettre en mémoire les concepts de base liés au routage vus en première année. Nous utiliserons des routeurs (Cisco) possédant leur langage de configuration de commandes propre. Ces routeurs sont simplement des ordinateurs spécialisés.

On va configurer le réseau de la figure 1.

- les routeurs B et C et l'hôte D composent l'Intranet que vous devez administrer.
- La machine hôte A représente l'extérieur de l'Intranet (Internet)

Supposons que l'on vous ait octroyé la plage d'adresse (appelé préfixe) 192.168.1.64/26 pour votre Intranet. Votre Intranet est composé de 3 réseaux. Il vous faut donc à partir de cette plage d'adresse "fabriquer" trois adresses de réseaux IP différentes.

De plus, vous voulez relier votre Intranet à l'ensemble d'Internet, pour cela vous louez une ligne spécialisée permettant de vous relier à Internet. L'adresse réseau de cette ligne vous est fournie : 20 .0.0.0/28, le routeur B (côté extérieur) aura l'adresse 20 .0.0.1/28. On vous fournit aussi l'adresse du routeur extérieur –la machine A en fait ici– par lequel vous devriez passer pour accéder à Internet : 20.0.0.2/28

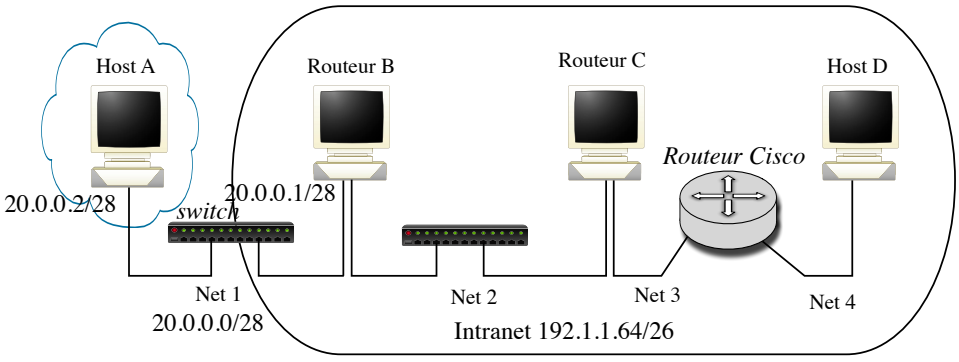


FIGURE 1 – Le réseau

1. Reliez les quatre machines de la plate-forme comme en figure 1 : on pourra utiliser des câbles croisés pour économiser l'installation de switch.

2. Indiquez précisément sur le plan du réseau les adresses et les noms des interfaces réseaux.

3. Configurez les interfaces des machines et du routeur.

4. Faites les configurations nécessaires (routage statique) de manière à ce que les quatre machines et le routeur puissent communiquer.

   **Rappel :** pour ajouter une ligne à la table de routage :
   `route add -net 192.1.1.96 192.168.0.66`). Par défaut le *netmask* est celui associés aux classes (A, B, C).
   On peut le préciser à l'aide de l'option `-netmask` suivi du *netmask* en décimal ou spécifier le nombre de bits de la partie réseau.
   Exemple :`route add -net 192.1.1.64 192.168.0.66 -netmask 255.255.255.192` ou bien `route add -net 192.1.1.64/26 192.168.0.66`

5. Vérifiez que toutes les machines communiquent.
   Pour débuguer quand ça ne marche pas, quelques conseils :
   - Essayez tout d'abord des pings entre des machines se trouvant sur un même réseau. On peut vérifier l'état des connexions en regardant le *status* de l'interface dans la commande `ifconfig`.
     Vérifiez les adresses utilisées. Attention aux adresses appartenant à un même réseau pour les deux interfaces d'un routeur (possible sous bsd).
   - Puis essayez ensuite des pings entre machines éloignées. Faire des captures de paquets pour comprendre où "ça coince".

6. Énumérez sur un chronogramme la liste des paquets échangés lors d'un `ping` de A vers D.
   On supposera les tables ARP vides sur chaque machine. On donnera les adresses Ethernet et Internet apparaissant dans les entêtes respectives des paquets sur chaque réseau.

7. En utilisant la commande `traceroute` mesurez les délais de transfert entre A et B, entre A et C, entre C et D et entre A et D.
   Capturez les paquets émis par cet utilitaire. Regardez en particulier le champ TTL de l'entête IP, avant et après la traversée d'un routeur.
   Expliquez le principe de cet outil de mesure en vous appuyant sur une capture de paquets sur les réseaux traversés lors d'un `traceroute` ?

## 3.2 Fonctionnement du protocole RIP

Le but de cette manipulation est de rappeler le principe de fonctionnement d'un des protocoles permettant le remplissage automatique des tables de routage dans Internet : le protocole RIP (Routing Information Protocol).

1. Supprimer toutes les entrées statiques des tables de routages sur l'ensemble des machines (`route flush` ou `route delete adresse`). Sur le routeur toute commande

peut être annulée en retapant (ou rappelant la commande à l'aide de la flèche montante) la commande précédée de `no`.

2. Lancez les démons `routed` sur les machines et configurez le routeur pour qu'il utilise RIP.
   On lancera ces démons sur B et C avec l'option `-s` (`routed -s -P no_rdisc -P ripv2` ) et sur A et D avec l'option `-q` (`routed -q -P no_rdisc -P ripv2`). L'option `-s` (*supply*) spécifie au démon de publier ses routes à ses voisins (pour les routeurs). L'option `-q` (*quiet*) démarre un démon silencieux, mais pas sourd (pour les machines hôtes).
   L'option `-P ripv2` permet de lancer la deuxième version de RIP qui transmet les netmasks des adresses. Dans la première version de RIP les netmasks étaient déduits de la classe des adresses.

   Cette version de RIP utilise le *multicast* (adresse IP de groupe) au lieu du *broadcast* pour diffuser ses paquets. C'est le protocole IGMP qui gère le multicast local.

   **Remarque :** Pour que des paquets mulitcast puissent être émis sur les machines, il est nécessaire de rajouter une route par défaut dans la table de routage (particularité de BSD).

3. Sur le routeur Cisco lancez le démon RIP sur les deux interfaces (`router RIP` puis `network AdresseReseau`). Ne pas oubliez `version 2`.

4. Donnez les tables de routages de A et du routeur Cisco.

5. Capturez des paquets sur le réseau entre B et C.

6. Enumérez la liste des paquets RIP échangés et détaillez les informations contenues dans ces paquets.

7. Expliquez comment cette version de RIP implémente la méthode appelée *split horizon* (*horizon coupé*) ?
   Une métrique de 16 signifie pour RIP qu'une adresse est inaccessible.

8. Introduisez l'adresse du routeur B par défaut dans la table de C. Introduisez une adresse inconnue via le routeur B dans la table de C.

9. Capturez des paquets RIP émis par C. Conclusion sur RIP et les routes statiques et par défaut ?

10. Lancez l'utilitaire `check-route` sur D. Lancez une capture de paquets sur *net3* et *net4*. Tuez le demon `routed` sur C (`killall routed`). Puis relancez le.

Que s'est-il passé ? Expliquez.

11. Faites cette fois un `killall -9 router` sur C, et attendez qu'un changement se produise sur D. Expliquez. (l'option -9 supprime immédiatement le processus.)

12. Rajoutez un réseau entre A et D. Transformez A et D en routeurs à l'aide du `sysctl net.inet.ip.forwarding=1`. Lancez RIP en mode *supply* sur A et D. Capturez les paquets RIP échangés sur ce réseau.

13. Donnez le contenu de la nouvelle table de routage du routeur D. Quelle sont les changements par rapport au montage précédent. Expliquez en rappelant l'algorithme des démons de routages RIP ce qu'il s'est passé.

14. Est ce que cette version de RIP implémente la méthode appelée *Route poisoning* (*Empoisonnement de route*) ?
    Cette technique consiste à envoyer, au moment de la suppression d'une ligne par timer, un paquet RIP avec l'adresse supprimée associée à une métrique de 16. Elle limite les cas de comptage à l'infini en cas de panne du réseau (voir le cours de première année).
    Imaginez (et testez) une expérience vous permettant de le savoir.
    Quel interêt apporte cette méthode ?

15. Est ce que cette version de RIP implémente la méthode appelée *Triggered updates* (*Mise à jour déclenchée*) ?
    Cette technique consiste au moment de l'ajout d'une nouvelle adresse à la table de routage (suite à la réception d'un paquet RIP), à émettre tout de suite un (ou des) paquets RIP portant cette modification (au lieu d'attendre le timer de re-émission de 30 secondes). Elle permet ainsi une propagation très rapide de la nouvelle information.
    Imaginez (et testez) une expérience vous permettant de le savoir.
    Quel interêt apporte cette méthode ?

## 3.3 `Traceroute` en vrai

Sur une machine reliée au réseau de l'UFR, lancez un `traceroute` [1] à destination d'une machine distante (en dehors de l'université).

Capturez les paquets correspondant et commentez le résultat : en particulier les délais affichés peuvent souvent être assez parlant.

1. utilisez l'option -n de façon à éviter un important trafic de résolution de nom.