Couche Réseau (Internet)

Laurent Signac – CC-BY-SA – 02-03-20 0944 6642efbca8a2aea0cc80

Le protocole le plus important de le couche réseau est IP. Il existe en deux versions : IPv4, qui est utilisé actuellement, et IPv6, qui remplace peu à peu IPv4. Le protocole IP prend en charge l'adressage sur internet (on parle d'adresse IP), le routage des datagrammes et l'éventuelle fragmentation des datagrammes en datagrammes plus petits.

1 Interconnexion de réseaux IP

Le matériel qui permet d'interconnecter des réseaux IP est le **routeur**. Il optimise les parcours en se basant sur l'adresse IP (l'adressage est hiérarchique) et opère au niveau de la couche réseau (contrairement à un commutateur par exemple).

Lorsque le routeur opère en plus dans les couches supérieures (transport, application), il permet aussi de réaliser du filtrage sur les contenus. Dans ces conditions le routeur est aussi, par exemple, un **pare-feu**.

2 Contenu d'un datagramme IPv4

Les datagrammes IPv4 contiennent des informations comme les adresse IP de l'expéditeur et du destinataire, la durée de vie du datagramme, un champ qui indique quel type de données (de la couche supérieure) ont été encapsulées. La longueur typique d'un entête IPv4 est 20 octets et un datagramme a une taille maximum de 64 Kio.

Le détail du contenu des trames peut être trouvé sur la page Wikipedia IPv4[1] ou dans la RFC 791[2]).

Chaque routeur (voir plus loin les détails de routage) connaît la taille maximale d'un datagramme pouvant être transporté sur le réseau physique auquel il est connecté (valeur MTU : Maximal Transmission Unit). Il se peut donc qu'il reçoive des datagrammes par un réseau physique qui supporte des tailles de paquets plus élevées que le réseau physique vers lequel il doit les envoyer. Dans ce cas, le datagramme est découpé en plusieurs datagrammes avant d'être retransmis : c'est la *fragmentation* de datagrammes. Pour Ethernet, le MTU vaut généralement 1500 octets.

3 Internet Control Message Protocol

ICMP (RFC 792[3]) est un autre protocole de la couche Internet. Placé au dessus d'IP (ICMP est encapsulé dans IP) il est en particulier utilisé pour les tests de connectivité proposés par le programme `ping`.

Les paquets ICMP sont de taille variable. Les deux premiers octets, nommés *type* et *code* permettent d'identifier la nature du message. Des valeurs courantes (utilisées par le programme `ping`) sont `type,code = 8,0` pour une demande d'echo (*Echo Request*) et `type,code = 0,0` pour une réponse à une demande d'echo (*Echo Reply*).

Les messages ICMP sont aussi utilisés pour communiquer sur des événements : réseau inaccessible, hôte inaccessible, durée de vie écoulée avant l'arrivée à destination etc.

4 Adressage et routage

L'adressage utilisé sur internet est l'adressage IP. Il dépend de la couche internet. Nous allons ici détailler l'adressage IPv4 et nous signalerons à la fin quelques améliorations présentes dans IPv6.

L'objectif de l'adressage IP est de pouvoir désigner un matériel réseau connecté à Internet. Une fois le matériel désigné, l'objectif du routage est de trouver un chemin vers la cible.

[1] https://fr.wikipedia.org/wiki/IPv4
[2] https://tools.ietf.org/html/rfc791
[3] https://tools.ietf.org/html/rfc792

4.1 Adressage

Une adresse IPv4 est un nombre de 32 bits, souvent représenté en notation décimale pointée par une série de 4 nombres (de 0 à 255) : 10.16.83.27. Précisons tout de suite qu'une adresse IP n'est pas l'adresse d'une machine sur le réseau, mais l'adresse d'une *interface réseau* (une machine peut avoir plusieurs adresses IP si elle a plusieurs interfaces). Sur le schéma de la figure suivante, par exemple, les machines D et G ont deux adresses IP car elles sont reliées à deux réseaux. Ainsi, la machine D est vue par B avec l'adresse 192.168.81.1, alors qu'elle est vue par E avec l'adresse 10.16.83.24.

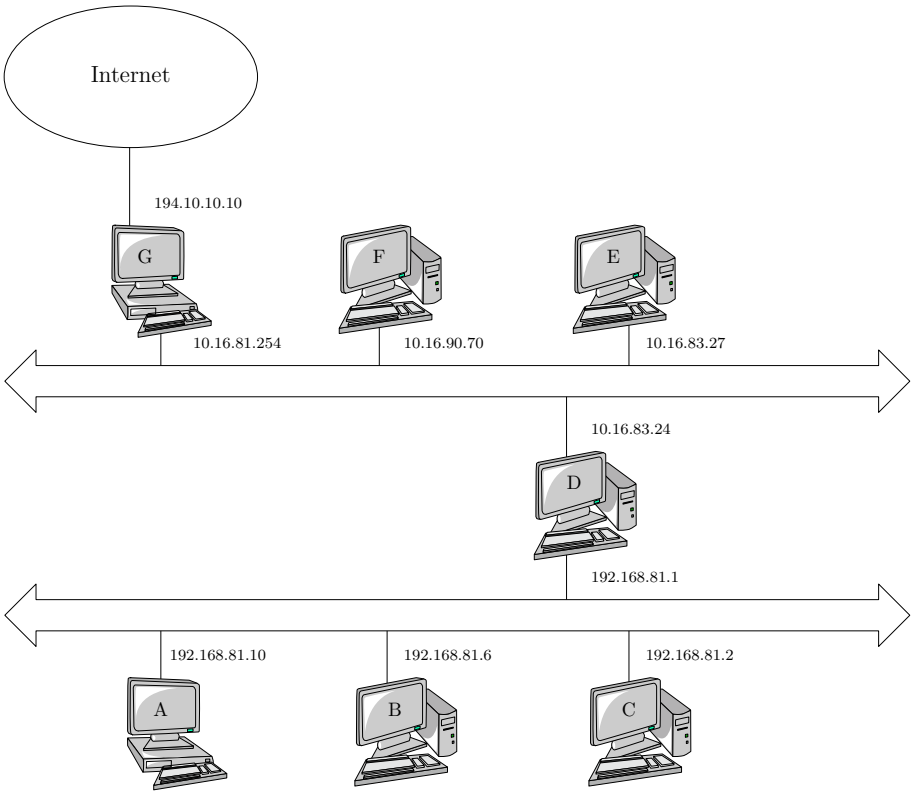

Figure 1: Trois réseaux interconnectés

4.1.1 Composition d'une adresse

Une adresse IP comporte deux parties : l'adresse du réseau et l'adresse de l'hôte dans le réseau. Les k premiers bits constituent l'adresse du réseau et les $32 - k$ derniers celle de l'hôte dans le réseau. La valeur de k étant variable pour chaque réseau, elle accompagne généralement les adresses et se nomme *masque*. Le masque peut être indiqué de deux façons différentes :

- soit en donnant la valeur de k : 192.168.81.1/24 signifie que les 24 premiers bits de l'adresse (192.168.81) désignent le réseau et que les autres (1) désignent l'hôte ;
- soit en donnant le masque en notation décimale pointée (en mettant à 1 les bits qui correspondent au réseau et à 0 ceux qui correspondent à l'hôte : 192.168.81.1/255.255.255.0

4.1.2 Adresses spéciales

Il y a plusieurs façon d'adresser un nœud du réseau. Celles dont nous venons de parler concerne les adresses unipoint (ou unicast). Un réseau entier peut être adressé à l'aide d'adresses de diffusion (ou adresses broadcast). Pour cela, il suffit de mettre à 1 tous les bits de la partie hôte de l'adresse. Sur la figure précédente, les machines A, B, C et D (en supposant que le masque de réseau est 24) peuvent être adressés par : 192.168.81.255/24. Enfin, il existe aussi les adresses multipoint (ou multicast), qui désignent des groupes de machines (nous n'en parlerons pas ici).

En raison de ces différentes méthodes d'adressage, tous les numéros d'hôtes ne sont pas permis. En particulier, le réseau 192.168.81.0/24 ne peut pas avoir d'hôte 255 (c'est l'adresse de diffusion). De même, le

réseau lui même (sans parler des hôtes) peut être désigné par une adresse IP avec tous les bits hôte à 0 : 192.168.81.0/24. En conséquence l'hôte 0 ne peut pas exister non plus.

Enfin :

- les adresses IP dont le premier octet commence par 1110 (premier octet compris entre 224 et 239) sont réservées pour le multipoint ;
- les adresses IP dont le premier octet commence par 1111 (premier octet supérieur ou égal à 240) sont réservées ;
- les adresse IP dont le premier octet vaut 127 sont réservées pour l'adresse de rebouclage (ou adresse loopback).
- les adresses IP suivantes sont réservées pour un usage privé et ne sont donc pas routées :
  - 10.0.0.0 à 10.255.255.255
  - 172.16.0.0 à 172.31.255.255
  - 192.168.0.0 à 192.168.255.255

4.1.3 Sous réseaux

Un réseau particulier peut être divisé en sous-réseaux. Par exemple afin que sa topologie reflète une structure particulière. Sur la figure 2, le réseau 192.168.81.0/24 a été divisé en quatre sous-réseaux :

- 192.168.81.0/26
- 192.168.81.64/26
- 192.168.81.128/26
- 192.168.81.192/26

Notez la façon de diviser le réseau. Alors que le réseau global peut comporter 254 hôtes, chacun des quatre sous-réseaux ne peut en comporter que 62.

Une seule machine (M) est reliée à internet, par le bais du réseau 195.10.10.0/24. La machine M fait office de routeur pour chacun des sous-réseaux. Vu de l'extérieur (de 195.10.10.0/24), il existe un seul réseau 192.168.81.0/24, sur lequel on entre par la machine 195.10.10.3. C'est uniquement en interne que la création des sous-réseaux est visible.

4.1.4 Internet Protocol version 6

Nous avons dit qu'IPv6 était le successeur d' IPv4. Les améliorations principales sont :

- une sécurité accrue au niveau de la couche IP ;
- des en-têtes simplifiés, qui pourront être traités plus rapidement par les routeurs ;
- des adresses sur 128 bits au lieu de 32, qui permettront d'adresser (beaucoup) plus de machines.

4.2 Routage

Le routage est la capacité des datagrammes IP à parvenir à leur destination, même si la destination n'est pas directement connectée à la source. Pour router les datagrammes, les différents hôtes disposent d'une table de routage (statique, mais les gros routeurs construisent des tables dynamiques grâce au protocole BGP). Cette table indique pour chaque type d'adresse, vers quel destinataire (directement joignable) le datagramme doit être envoyé.

La table de routage d'un nœud du réseau (ici un simple poste de travail) ressemble à ceci :

```
Destination     Gateway         Genmask
0.0.0.0         192.168.1.1     0.0.0.0
192.168.1.0     0.0.0.0         255.255.255.0
192.168.2.0     192.168.1.254   255.255.255.0
```

Les colonnes `Destination` et `Genmask` désignent un réseau (adresse et masque). La colonne `Gateway` indique quel est le routeur à contacter pour joindre ce réseau. La table de routage précédente nous indique trois choses:

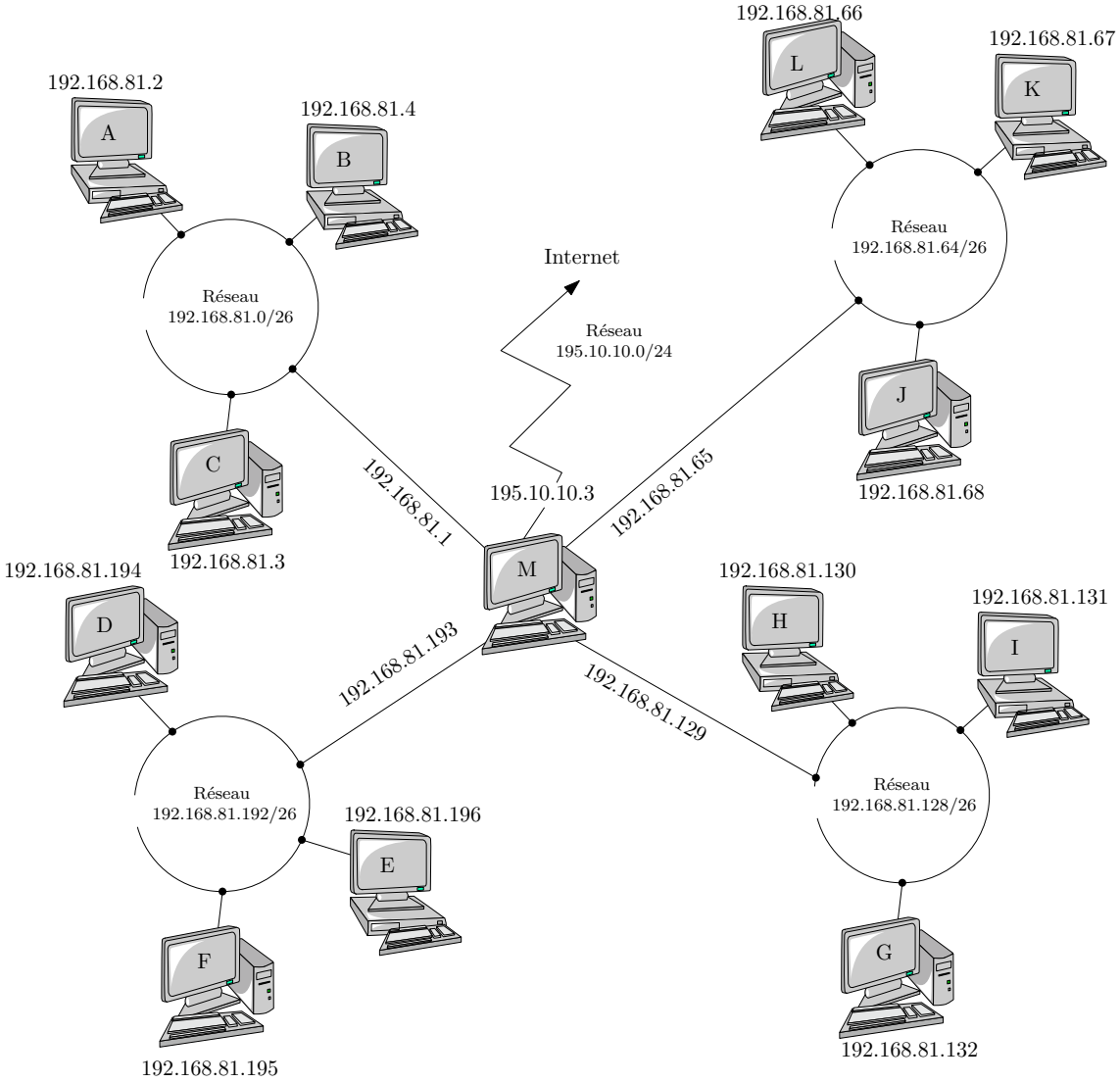

Figure 2: Découpage d'un réseau en sous-réseaux

- le poste de travail fait partie du réseau 192.168.1.0/24 (puisqu'il n'y a pas de routeur indiqué pour joindre ce réseau)
- pour joindre le réseau 192.168.2.0/24, le routeur à contacter est 192.168.1.254 (qui est bien dans le réseau IP local)
- pour joindre le reste du monde (réseau 0.0.0.0/0), le routeur par défaut est 192.168.1.1.

4.3 Réseaux privés et translation d'adresses

Avec la pénurie d'adresses IP qui a suivie l'explosion du nombre de terminaux connectées à internet, et en attendant la généralisation d'IPv6, la technique de la translation d'adresses a été utilisée. Nous avons vu que certaines plages d'adresses IP pouvaient être utilisés dans des réseaux privés. Une conséquence de cela est qu'elles ne sont pas uniques dans le monde puisqu'il y a de nombreux réseaux privés. Ces adresses ne sont pas routables, dans le sens où une machine connectée à internet ne pourra pas joindre une machine ayant une adresse IP privée par le biais de cette adresse. Il existe néanmoins un moyen de relier de tels réseaux privés à internet. L'implantation se fait au niveau de la passerelle, qui *traduit* les adresses non routables en adresse(s) routable(s). La technique est appelée translation d'adresse ou NAT pour Network Address Translation. Lors de la réponse de la machine extérieure, le port utilisé par la passerelle permettra de retrouver la machine du réseau privé à qui le paquet est destiné et de lui faire parvenir. Ce principe est illustré sur la figure suivante.

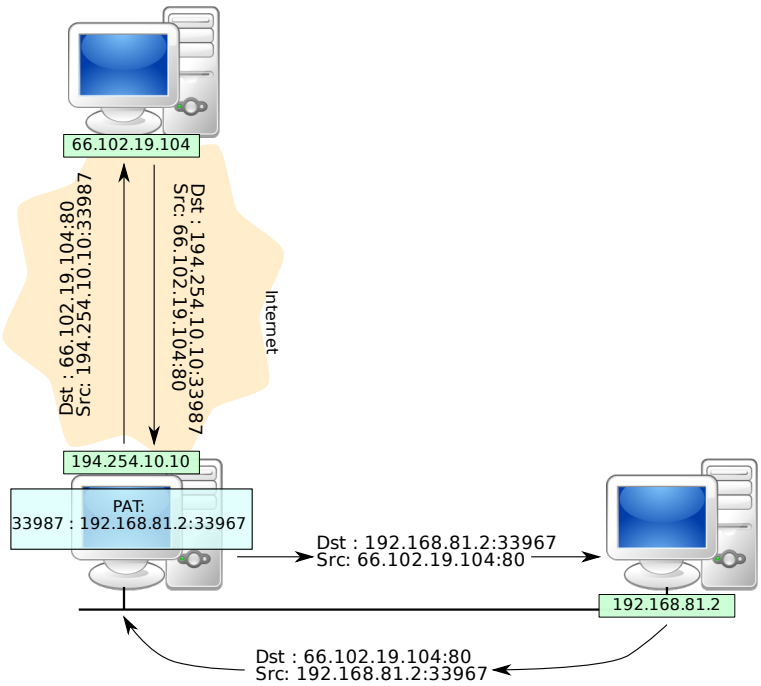

Figure 3: Communications entre un réseau privé et internet en utilisant la translation d'adresse

Une entrée est rajoutée dans la table de translation des ports (PAT pour *Port Addresss Translation*) lorsque le paquet sort. Au retour, la passerelle lit le port destination et l'utilise pour retrouver la machine à qui envoyer le paquet.

Il est possible de faire correspondre une adresse IP routable à chaque adresse IP privée auquel cas on pratique de la translation 1-to-1. On perd alors le bénéfice de l'économie d'adresses IP. Si chaque adresse IP est traduite en la même adresse routable, on pratique de la translation 1-to-n. C'est dans ce dernier cas que la table PAT est utilisée.