Couche Réseau (Internet)

Laurent Signac – CC-BY-SA – 17-11-22 1332 c90de59ff7f1fc8c658e

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 est le **routeur**. Il optimise les parcours en se basant sur l'adresse IP (l'adressage est hiérarchique), opère au niveau de la couche réseau (contrairement à un commutateur par exemple), et ne laisse pas circuler les trames broadcast (limite le domaine de diffusion).

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 Détail d'un datagramme IPv4

Références : IPv4, Rfc 791[1] et IPv6, Rfc 2460[2]

Un datagramme IPv4 est représenté figure suivante.

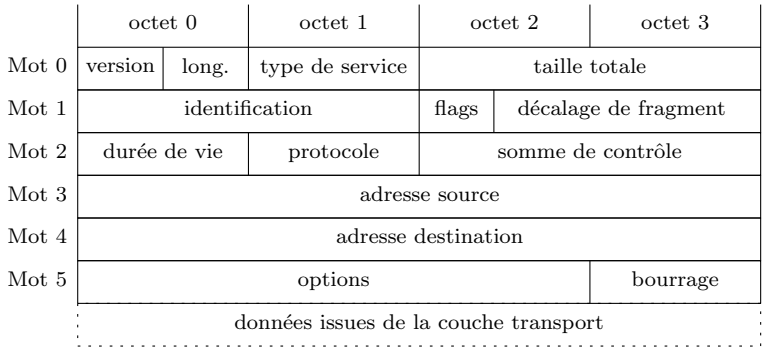


Figure 1: Datagramme IPv4

L'en-tête IP; constitué d'au moins cinq mots de quatre octets contient les champs suivants :

Version : Numéro de version d'IP (4 pour IPv4).

Long. : Longueur de l'en-tête exprimé en nombre de mots de quatre octets. La valeur courante est 5, lorsqu'il n'y a pas d'option.

Type de service : Cette valeur décrit «l'importance» du datagramme, et donc s'il doit être traité prioritairement. Les bits 0 à 2 codent la priorité (000 pour un paquet ordinaire et 111 pour un paquet utile au bon fonctionnement du réseau, en passant par toutes les valeurs intermédiaires), les bits 3, 4 et 5 permettent d'exprimer une demande de retard faible, de débit élevé, ou bien de taux d'erreur faible. Enfin, les bits 6 et 7 ne sont pas utilisés.

Taille totale : Indique la taille totale en octets du datagramme, en-tête compris (le total est donc limité à $2^{16} - 1 = 65\,535$ octets).

Identification : Chaque fragment d'un datagramme fragmenté doit avoir le même numéro d'identification qui permettra de les apparier. L'ordre d'appariement est obtenu grâce au décalage.

[1] https://tools.ietf.org/html/rfc791
[2] https://tools.ietf.org/html/rfc2460

Flags : Le premier bit n'est pas utilisé, le second, s'il est à 1 signifie qu'il ne faut pas fragmenter ce datagramme, et le troisième, s'il est à 1 signifie que le datagramme est issu d'une fragmentation et n'est pas la dernière partie.

Décalage du fragment : Indique la position relative du fragment en blocs de 8 octets dans le datagramme complet. Pour le datagramme initial, le décalage est de 0.

Durée de vie : Cette valeur est diminuée de 1 à chaque seconde ou à chaque routeur. Si elle prend la valeur 0, le datagramme est effacé. Cela évite que des paquets perdus ne *tournent* indéfiniment.

Protocole : Indique de quel protocole, au niveau de la couche transport, le datagramme est issu. Ceci permet, lors de la «remontée» des paquets de transmettre les données au bon protocole de la couche transport. Les valeurs usuelles sont 1 (Icmp), 2 (Igmp), 6 (Tcp), 17 (Udp).

Somme de contrôle : Permet de vérifier l'intégrité de l'en-tête. La somme est le complément à 1 sur 16 bits de la somme des compléments à 1 sur 16 bits de chaque mot de deux octets de l'en-tête (pendant le calcul, le champs somme de contrôle est pris égal à 0).

Adresse source : Contient l'adresse Ip de l'expéditeur du datagramme.

Adresse destination : Contient l'adresse Ip du destinataire du datagramme.

Options : Un en-tête Ip peut contenir plusieurs options, si bien que sa taille peut finalement dépasser les cinq mots de quatre octets. Nous ne détaillerons pas ici les options (voir la Rfc).

Bourrage : Ce champs de taille variable ne contient que des 0, et permet d'assurer que l'en-tête Ip a une longueur en octets multiple de quatre.

```
0x0000:  .... .... .... .... .... .... .... 4500  ..............E.
0x0010:  0054 0000 4000 4001 7216 0a10 5a46 0a10  .T..@.@.r...ZF..
0x0020:  5a2d .... .... .... .... .... .... ....  Z-..............
```

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.

3 Internet Control Message Protocol

Icmp (Rfc 792[3]) est un autre protocole de la couche Internet. Placé au dessus d'Ip (en ce sens qu'il l'utilise) il est en particulier utilisé pour les tests de connectivité proposés par le programme `ping`.

Les paquets Icmp sont de taille variable.

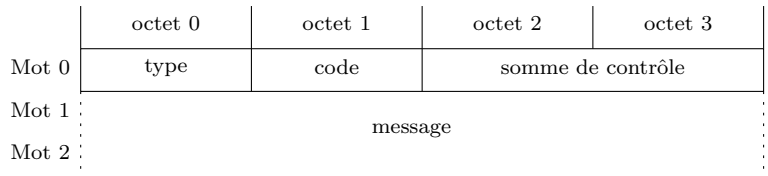


Figure 2: Paquet Icmp

Selon les valeurs des champs `type` et `code`, le contenu de la partie `message` varie. La somme de contrôle est le complément à 1 de la somme des compléments à 1 des mots de 16 bits du message Icmp. Le tableau suivant résume les messages qui sont émis en réponse à des datagrammes Ip (pour signaler un problème par exemple). La dernière colonne du tableau indique le contenu du mot 1 du paquet Icmp. Dans tous les cas, le mot 2 et les suivants contiendront le début du datagramme Ip qui a provoqué l'émission du message Icmp.

[3] https://tools.ietf.org/html/rfc792

Type	Code	Signification	Contenu du message
3	0	Réseau inaccessible	Vide
3	1	Hôte inaccessible	id.
3	2	Protocole non disponible	id.
3	3	Port non accessible	id.
3	4	Fragmentation nécessaire mais interdit	id.
3	5	Échec d'acheminement source	id.
11	0	Durée de vie écoulée avant arrivée à destination	id.
11	1	Temps limite de réassemblage du fragment dépassé	id.
4	0	Contrôle de flux (manque de mémoire par ex.)	id.
12	0	Erreur dans l'en-tête	8 premiers bits de mot 1 : numéro de l'octet ayant provoqué l'erreur.
5	0	Redirection sur base réseau	Adresse du nouveau routeur
5	1	Redirection sur base hôte	Adresse du nouveau routeur
5	2	Redirection sur base réseau et type de service	Adresse du nouveau routeur
5	3	Redirection sur base hôte et type de service	Adresse du nouveau routeur

Le tableau suivant résume les types et codes ICMP qui ne sont pas émis suite à la réception d'un datagramme. La partie message est détaillée dans la colonne de droite.

Type	Code	Signification	Contenu du message
8	0	Demande d'echo (ping)	Deux mots de 16 bits permettant d'identifier la réponse à l'echo
0	0	Réponse à une demande d'echo	Deux mots de 16 bits permettant d'identifier la réponse à l'echo
13	0	Marqueur temporel	id. + trois mots de 32 bits contenant les marqueurs temporels
14	0	Réponse à un marqueur temporel	id.
15	0	Demande d'information	Deux mots de 16 bits permettant d'identifier la réponse à la demande d'information
16	0	Réponse à une demande d'information	id.

```
0x0020:  .... 0800 ac07 731d 0002 27f1 0541 bba3  ......s...'..A..
0x0030:  0500 0809 0a0b 0c0d 0e0f 1011 1213 1415  ................
0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425  ...........!"#..
0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
0x0060:  3637                                     67
```

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 prévues pour 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.

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.

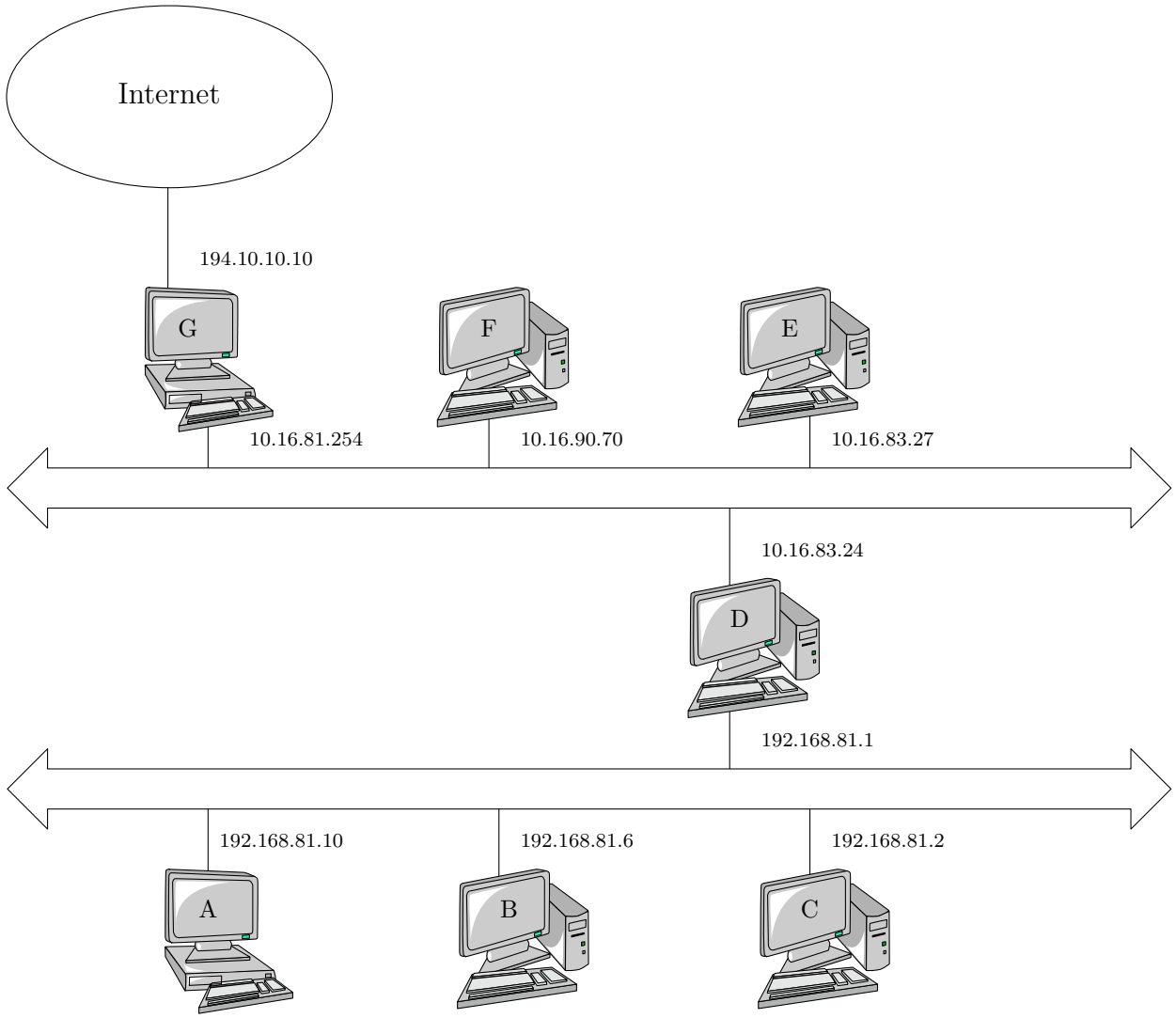


Figure 3: Trois réseaux interconnectés

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 les systèmes. Celle 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 4, 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-réseau. 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.

Reprenons l'exemple de la figure 3 (supposons que les adresses de l'exemple ne sont pas des adresses privées, que le réseau du bas a pour masque 24 et celui du haut pour masque 20) : Si C souhaite communiquer avec A, puisque les deux machines font partie du même réseau, il n'y a pas besoin de routeur, les datagrammes sont directement envoyés de A à C. La table de routage de A indiquera ceci :

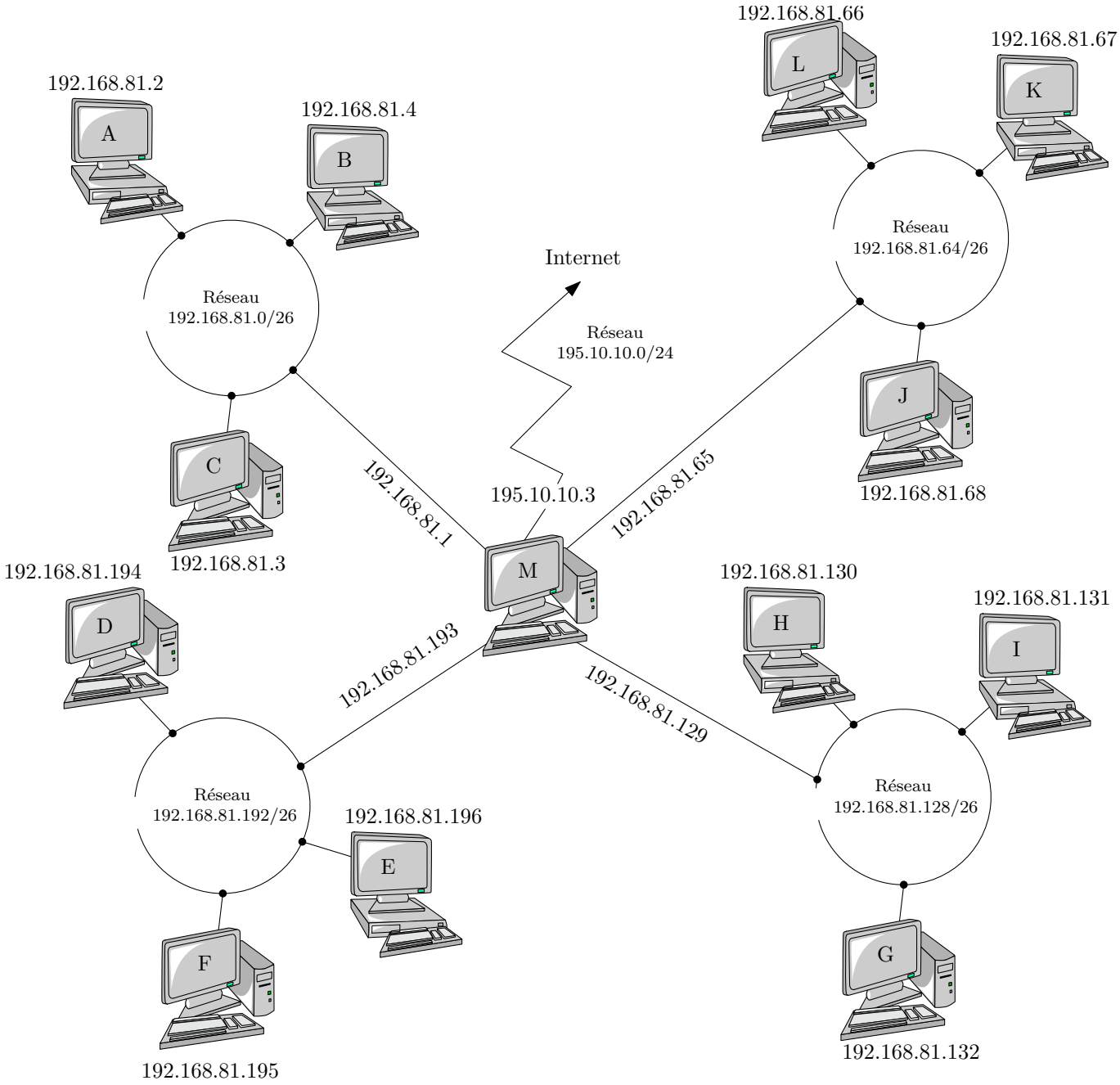


Figure 4: Découpage d'un réseau en sous-réseaux

Destination	Masque	Routeur
192.168.81.0	255.255.255.0	0.0.0.0

Cette information signifie : Pour joindre une machine du réseau 192.168.81.0/255.255.255.0, il n'y a pas besoin de routeur (0.0.0.0). De même si F souhaite communiquer avec E, elle devra avoir dans sa table de routage :

Destination	Masque	Routeur
10.16.80.0	255.255.240.0	0.0.0.0

Maintenant, que se passe-t-il si A souhaite communiquer avec F ? La machine A doit transmettre son datagramme à D, qui pourra communiquer avec F. La machine A aura donc pour table de routage :

Destination	Masque	Routeur
192.168.81.0	255.255.255.0	0.0.0.0
10.16.80.0	255.255.240.0	192.168.81.1

La nouvelle ligne signifie que pour atteindre une machine du réseau 10.16.80.0/255.255.240.0, les datagrammes doivent être transmis à 192.168.81.1 (et ce sera à sa charge de continuer le routage).

Naturellement, s'il fallait ainsi préciser une nouvelle route pour chaque réseau, A ne serait pas prête de communiquer avec tout internet. Il existe donc une notion de route par défaut, qui indique quel est le routeur à utiliser au cas où le destinataire ne soit pas dans un des réseaux listés de la table de routage. La table de routage de A sera donc finalement :

Destination	Masque	Routeur
192.168.81.0	255.255.255.0	0.0.0.0
10.16.80.0	255.255.240.0	192.168.81.1
0.0.0.0	0.0.0.0	192.168.81.1

Ainsi, tous les datagrammes à destination d'autres réseaux que 192.168.81.0 ou 10.16.80.0 seront dirigés vers D. La seconde ligne de la table de routage n'est donc plus utile.

Toutes les machines pourront communiquer si leurs tables de routage sont correctes :

- Table de routage de A, B et C :

Destination	Masque	Routeur
192.168.81.0	255.255.255.0	0.0.0.0
0.0.0.0	0.0.0.0	192.168.81.1

- Table de routage de F et E :

Destination	Masque	Routeur
10.16.80.0	255.255.240.0	0.0.0.0
192.168.81.0	255.255.255.0	10.16.83.24
0.0.0.0	0.0.0.0	10.16.81.254

- Table de routage de D (dans le cas où une machine possède plusieurs interfaces, il est utile de faire figurer l'interface concernée par chaque route) :

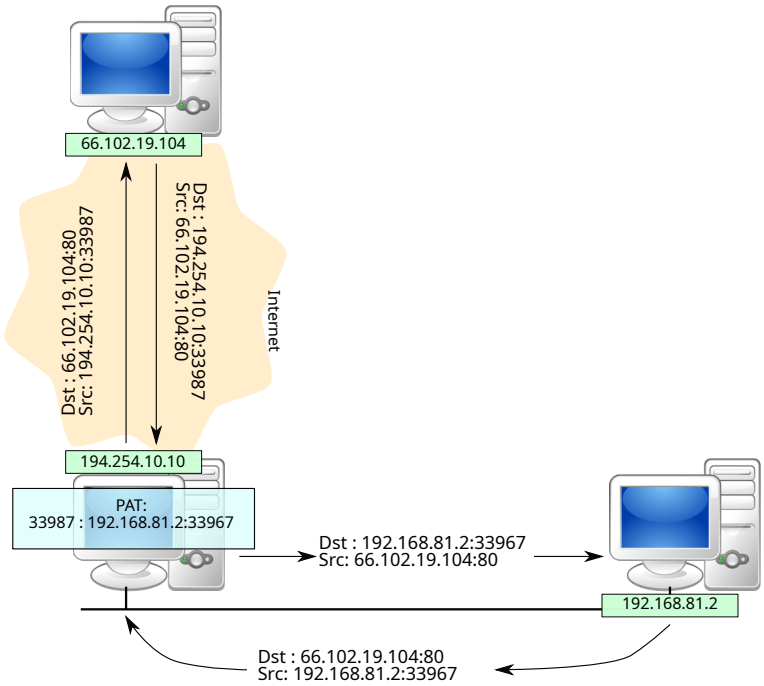
Destination	Masque	Routeur	Iface
10.16.80.0	255.255.240.0	0.0.0.0	i0
192.168.81.0	255.255.255.0	0.0.0.0	i1
0.0.0.0	0.0.0.0	10.16.81.254	i0

- Table de routage de G (si nous supposons que G fait partie d'un réseau de masque 24 et que le routeur de niveau supérieur est 194.10.10.254) :

Destination	Masque	Routeur	Iface
10.16.80.0	255.255.240.0	0.0.0.0	i0
192.168.81.0	255.255.255.0	10.16.83.24	i0
194.10.10.0	255.255.255.0	0.0.0.0	i1
0.0.0.0	0.0.0.0	194.10.10.254	i1

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 l'arrivée 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 adresse 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 adresses routables. 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.



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 statique ou 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 dynamique ou 1-to-n. C'est dans ce dernier cas que la table PAT est utilisée.