Adressage IP

Hassine Moungla

Adressage IP

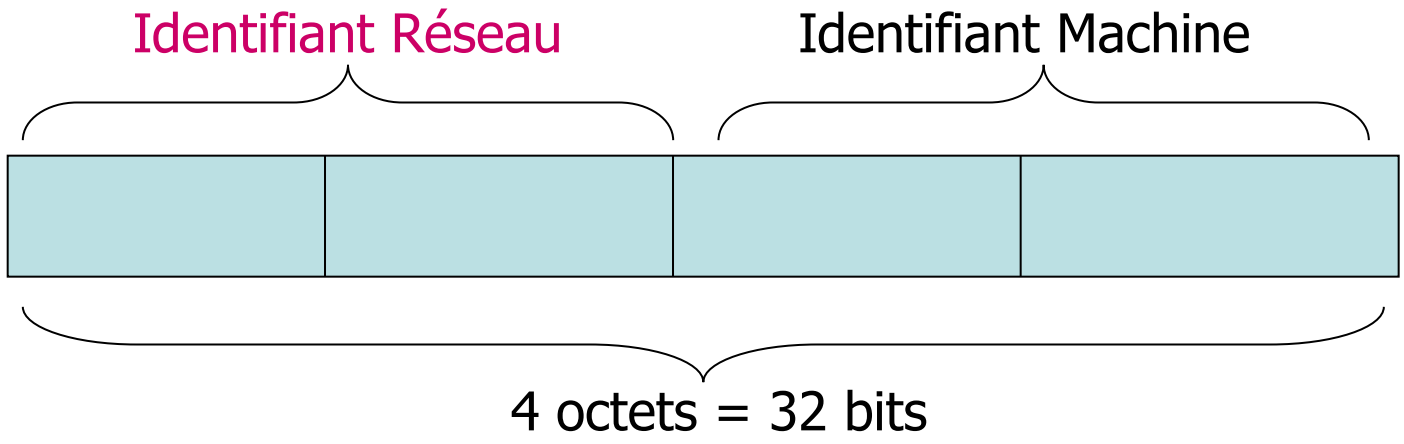
Adresse IP : introduction

- Adresse IP :
  - identificateur sur 32 bits
  - identifie pour chaque interface hôte et routeur
- Interface : connexion entre un hôte ou routeur et la couche physique
  - Les routeurs ont typiquement plusieurs interfaces
  - Les hôtes peuvent avoir plusieurs interfaces
  - Les adresses IP sont associées à une interface

Adressage IP

- L'adresse IP et le masque sont composés de 32 bits chacun, répartis en 4 octets séparés par des points

- L'adresse IP est elle même divisée en deux parties, la partie Net-ID et la partie Host-ID

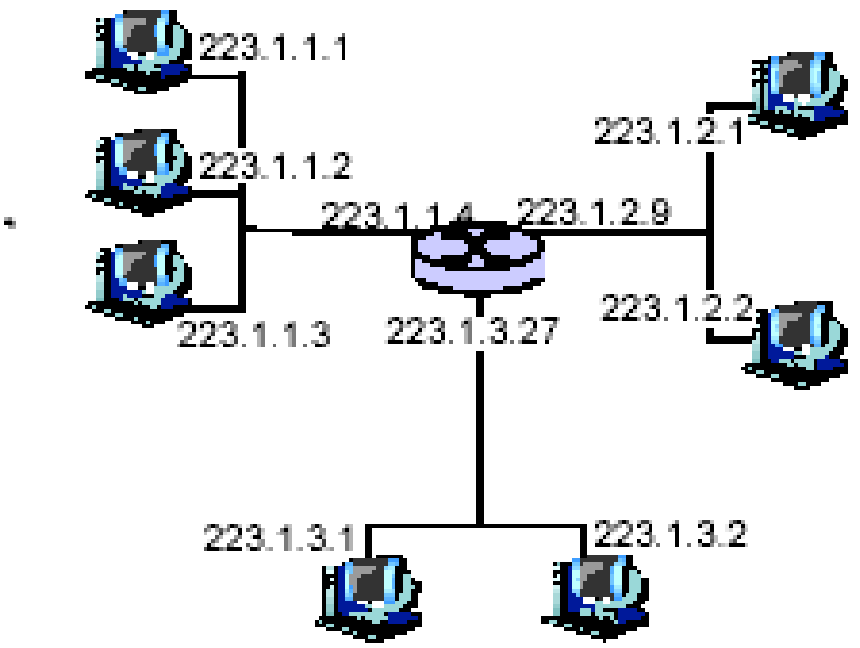


Adressage IP

- La partie Net-ID représente la partie réseau, partie qui sera commune à toutes les adresses IP d'un même réseau.
- La partie Host-ID représente la partie hôte, c'est-à-dire la machine et sera unique sur un réseau.
- Le masque est nécessaire au calcul de réseau, car sans masque il est très difficile de savoir à quel réseau appartient une adresse.

Adressage IP

- Adresse IP
  - Partie réseau (bits de poids forts)
  - Partie hôte (bits de poids faible)

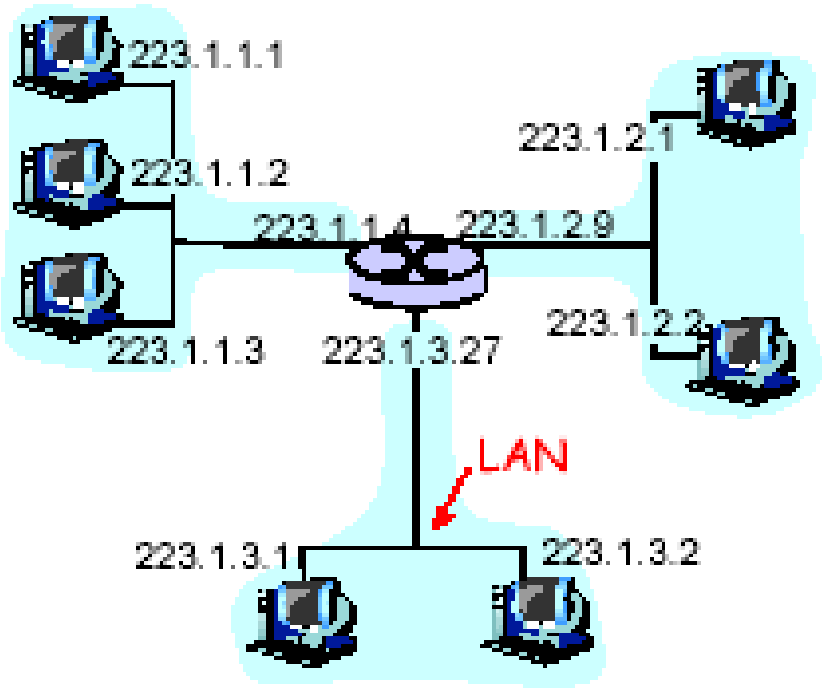


223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Adressage IP

- Réseau ? (du point de vue IP)
  - Les interfaces avec la même partie réseau de l'adresse IP
  - Et qui peuvent communiquer sans avoir besoin d'un routeur de passerelle



Le réseau est constitué de 3 réseaux IP (Les 24 premiers bits sont l'adresse réseau)

3.2 Pourquoi un subnet ?

- Dans un réseau local Ethernet TCP/IP il peut y avoir des problèmes de charge de réseau qui apparaissent pour plusieurs raisons :
  - diffusion trop importante (broadcast)
  - trop grande quantité de machines sur un seul réseau logique d'ou un trafic trop important.

Pourquoi un subnet ?

- Dans un réseau local, par sécurité, on peut vouloir isoler certains utilisateurs de certaines ressources.
- Dans un réseau MAN ou WAN, les phénomènes de diffusion sont à éviter pour des problèmes de coût. Pour des questions de sécurité, il est préférable d'isoler certaines portions de réseau.
- Dans tout ces cas de figure, tout en gardant les mêmes adresses TCP/IP, le découpage en sous-réseaux (subnetting) associé à l'utilisation de routeurs peut être une solution.

Pourquoi un subnet ?

- L'utilisation de TCP/IP oblige traditionnellement à choisir une classe d'adresse

- Chaque classe proposée offre un compromis entre le nombre maximum de réseaux et le nombre de machines

3.3 Quelles adresses TCP/IP utiliser

- Classes d’adresses
- Adresses réservés
- Le masque de réseaux

Les classes d'adresses

- Il existe à ce jour 5 classes d'adresses possibles :

Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

Les classes d’adresses

- Les adresses de la classe D sont réservées au muticasting
- Les adresses de la classe E sont réservées à un usage futur (...)
- Les seules classes vraiment utiles sont les classes A, B et C

- On le voit, plus le nombre de réseaux par classe est important, moins le nombre possible de machines est important

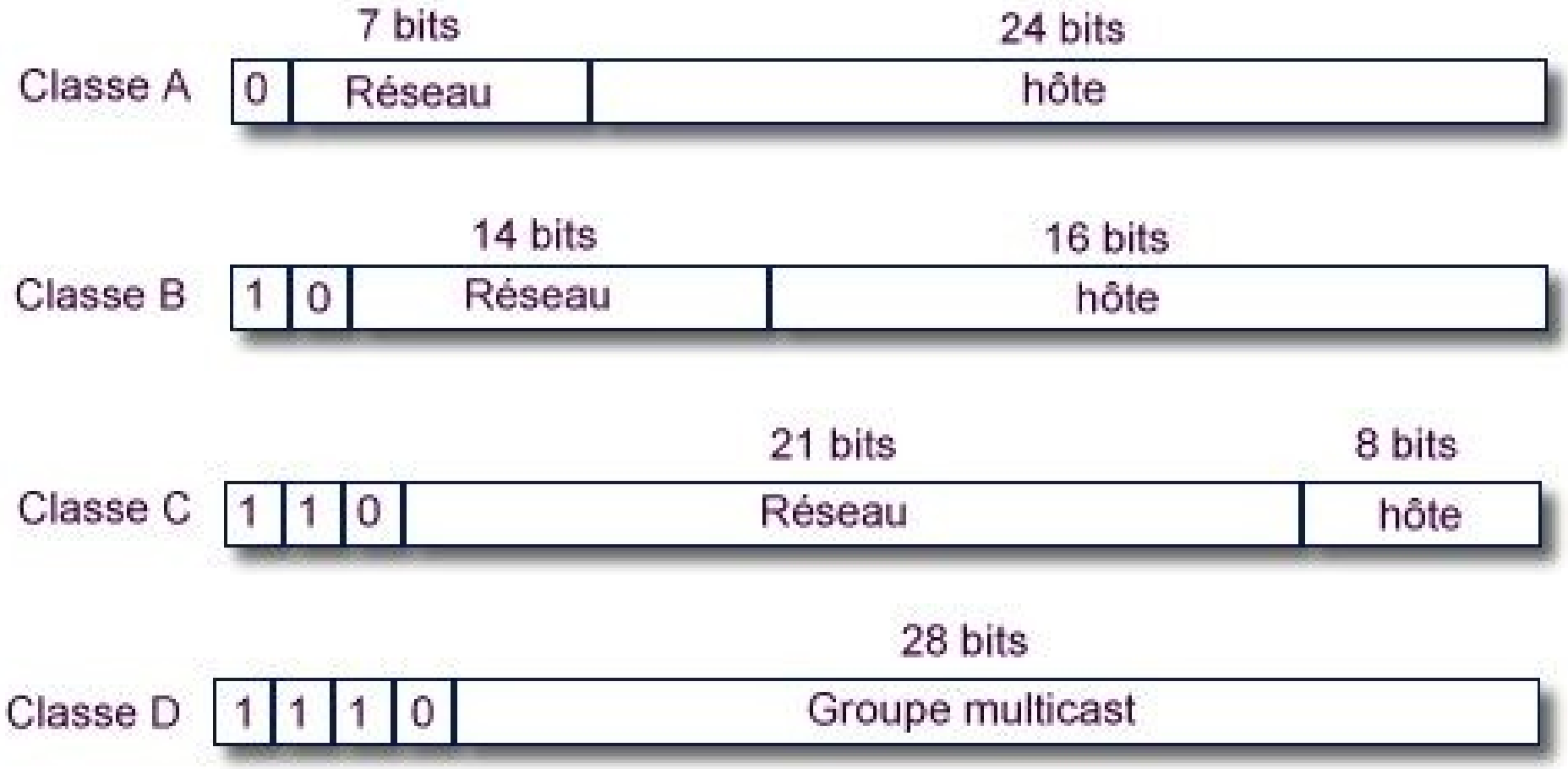
Les classes d’adresses

- Dans la classe A, le réseau 127 tient une place à part. Conventionnellement, il désigne l'adresse de la machine (moi même) dans le contexte TCP/IP.
  - La table /etc/host de toute machine UNIX comporte par exemple la mention "127.0.0.1 localhost".
- Tout autre numéro de ce réseau peut être utilisé pour cet usage.

Les classes d’adresses

- On peut alors choisir, à partir du nombre de machines que l'on compte mettre en oeuvre, le type de classe le plus approprié.
- Pour trouver à quelle classe appartient une machine donnée, il suffit de repérer la valeur du premier octet de l'adresse TCP/IP.
  - L'adresse 174.23.2.45 est par exemple une adresse de classe B, car le premier octet, 174, est compris entre 128 et 191.
  - L'adresse 5.6.7.8 est une adresse de classe A

Les classes d'adresses



Les adresses IP réservées

- Il existe aussi, à l'intérieur de chaque classe, un sous-ensemble d'adresses qui sont destinées à un usage privé
  - Ce qui signifie que tout routeur du marché ne routera pas, par défaut, ces adresses sur Internet
- Plusieurs réseaux locaux utilisent donc ces adresses pour leur usage interne
  - Il n'y a pas de conflit, puisque ce sont des réseaux privés dont les adresses ne sont pas accessibles depuis Internet

Les adresses IP réservées

- Les adresses sont réservées pour satisfaire certaines contraintes :
  - Toutes les adresses de bouclage commencent par 127 (par exemple, 127.0.0.1 est la boucle locale)
  - Toutes les dernières adresses d'un réseau sont des adresses de broadcast.
  - En général, elles se terminent par 255, mais pas obligatoirement si le masque n'est pas courant (par exemple : 192.168.0.255 ou 80.34.255.255).

Les adresses IP réservées

- Toutes les adresses finissant par 0 sont des adresses représentant le réseau
  - par exemple : 192.168.0.0 ou 12.54.255.0
- Toutes les adresses commençants par 169.254.0.0/16 sont des adresses APIPA (Automatic Private IP Addressing) réservées au DHCP (Dynamic Host Configuration Protocol)
  - **Voir RFC 2131, 2132**

Les adresses IP réservées

- Ces adresses sont définies dans la **RFC1918** :

1. pour la classe A les adresses 10.x.x.x
2. pour la classe B les adresses 172.16.x.x à 172.31.x.x
3. pour la classe B les adresses 192.168.x.x

Le masque de réseau

- Un masque réseau TCP/IP est un ensemble de 4 octets qui permet de distinguer, dans une adresse TCP/IP, la partie réseau de la partie machine.

- Exemple : l'adresse de la machine est 184.23.3.67, avec un masque de 255.255.0.0
- Cette machine appartient au réseau 184.23.0.0.

Le masque de réseau

- Codés sur 4 octets (32 bits)
- Ils permettent de faire la séparation entre la partie réseau et la partie machine de l'adresse IP
- La partie réseau est représentée par des bits à 1, et la partie machine par des bits à 0,
- Le masque ne représente rien sans l'adresse IP à laquelle il est associé.

Le masque de réseau

- le masque est codé sur 32 bits,
- voici un exemple possible de masque :

Réseau Machine

11111111.11111111.11111111.00000000

Ce qui s'écrit en décimal 255.255.255.0

Le masque de réseau

- Quelles adresses pour les masques ?
- Etant donné que l'on conserve la contiguïté des bits, on va toujours rencontrer les mêmes nombres pour les octets du masque. Ce sont les suivants:
  - 11111111
  - 11111110
  - 11111100
  - ...
  - 10000000
  - 00000000

- Soit en décimal : 255, 254, 252, 248, 240, 224, 192, 128, et 0.

Le masque de réseau

- Vous pouvez aller voir tous les masques possibles dans la RFC suivante :

- http://www.faqs.org/rfcs/rfc1878.html

Le masque de réseau

Quelle est cette notation avec un /, comme /24 ?

- Une autre notation est souvent utilisée pour représenter les masques
  - plus rapide à écrire
- Dans celle-ci, on note directement le nombre de bits significatifs en décimal, en considérant que la contiguïté est respectée.
  - Par exemple 192.168.25.0/255.255.255.0, on peut aussi écrire 192.168.25.0/24, car 24 bits sont significatifs de la partie réseau de l'adresse.
- De même, les écritures suivantes sont équivalentes:
  10.0.0.0/255.0.0.0 = 10.0.0.0/8
  192.168.25.32/255.255.255.248 = 192.168.25.32/29

Le masque de réseau

Rappel de fonctionnement :

- Quand un ordinateur cherche a communiquer avec un autre ordinateur ou avec un périphérique réseau quelconque en utilisant le protocole TCP/IP, la procédure suivante se déroule :
  1. Le nom de la machine est transformé en une adresse TCP/IP. Ceci est effectué par le resolver qui utilise un service de nommage (table hosts, DNS)..
  2. Les routines des couches TCP/IP associent ce numéro et le masque de réseau pour déterminer si la machine à atteindre fait ou non partie de même réseau.

Le masque de réseau

2.1 Si oui, l’adresse TCP/IP est résolue en une adresse Ethernet; une trame est alors formée avec cette dernière et est envoyée sur le réseau.

2.2 Sinon, et si il existe une table de routage, l'adresse Ethernet du routeur est utilisée pour former une trame qui est envoyée sur le réseau (donc vers le routeur approprié).

3. Sinon, un message d'erreur est renvoyé vers le programme utilisateur (celui qui cherchait à envoyer des données). Ce message indique que l'adresse de la machine destinataire est impossible à joindre.

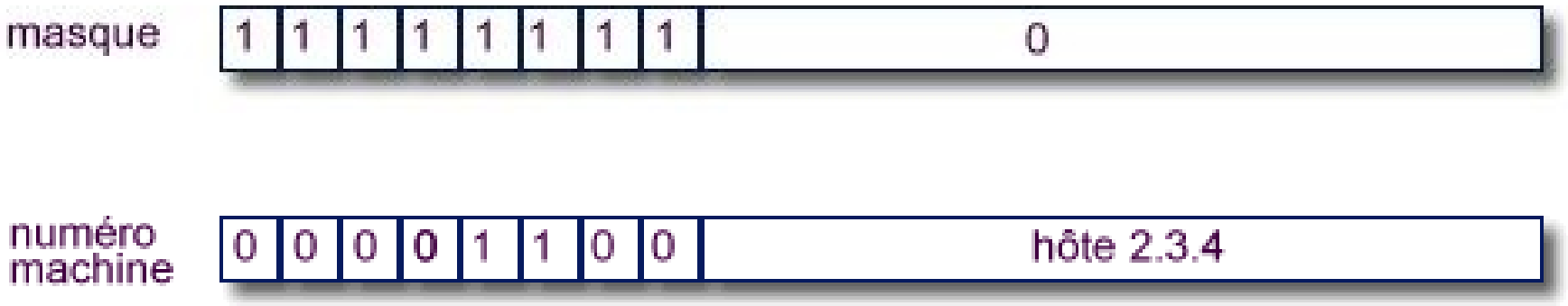
Le masque de réseau

Pour réaliser le masquage, on utilise l'opération AND binaire

- Masque sous-réseau = masque par défaut de la classe + bits utilisés pour le sous-réseau à 1
- Sous-réseau = adresse IP AND binaire masque de la classe (ou la masque du sous-réseau)
- Adresse de diffusion = Adresse du réseau + partie hôte avec tous les bits à 1
- Adresse machine = adresse IP AND binaire ~masque

Le masque de réseau

- Dans le cas d'une machine dont le numéro TCP/IP est 12.2.3.4 et le masque de 255.0.0.0, on a alors les valeurs de masque et d'adresse hôte ci-dessous :



Le masque de réseau

- Si on compare bit à bit ces deux valeurs (opération *AND binaire*), on obtient l'adresse du réseau qui est indispensable pour savoir comment expédier le paquet TCP/IP, c'est à dire : 12.0.0.0
- Autre exemple, si on a un réseau de classe B (sans sous-réseau), le masque par défaut est de 255.255.0.0
  - La machine dont l'adresse TCP/IP est 171.21.36.12 appartient au réseau 171.21.0.0 (*AND binaire* entre 171.21.36.12 et 255.255.0.0)

3.4 La création d'un sous-réseau

- Intérêt de diviser de grands réseaux en sous-réseaux
  - plus faciles à gérer
- l'espace d'adressage alloué doit être re-découpé
- Le (ou les) dernier(s) octet(s) va donc être utilisé pour "coder" un sous-réseau et une adresse de machine.
- Une contrainte va apparaître : chacun des sous-réseaux formé devra avoir une adresse de réseau et une adresse de diffusion (broadcast). Ces deux adresses ne pourront pas être allouées à des machines.

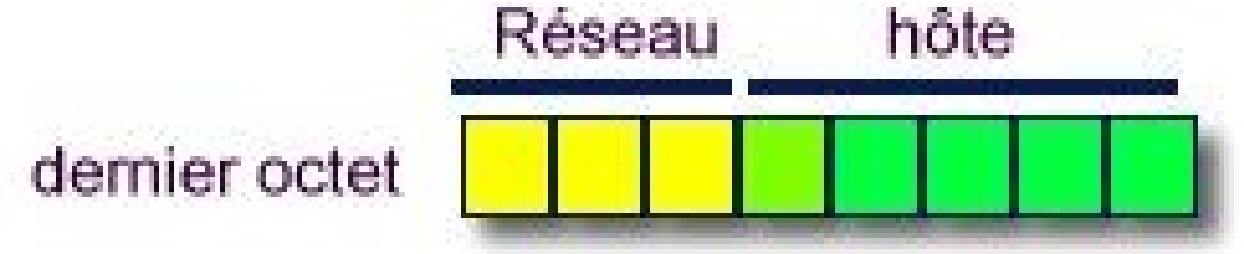
La création d'un sous-réseau

Exemple

- L'espace d'adressage 204.34.57.0 de classe C nous a été allouée avec un masque de 255.255.255.0
- Si on ne découpe pas en sous-réseaux, la totalité du dernier octet sert à numéroter les machines.
- Mais on désire créer des sous-réseaux :
  - on va donc re-découper l'espace fourni par les 8 bits du dernier octet.

La création d'un sous-réseau

- On peut par exemple allouer les bits de la façon suivante :



Les 3 bits de poids 32, 64 et 128 (jaunes) seront utilisés pour déterminer le sous-réseau et les 5 bits de poids 1, 2, 4, 8 et 16 (verts) pour définir les adresses des hôtes au sein des sous-réseaux.

La création d'un sous-réseau

- En groupant les bits de sous-réseau avec les bits de réseau, on va définir les sous réseaux suivants :
  - 204.34.57.0 (bits de sous-réseau = 000)
  - 204.34.57.32 (bits de sous réseau = 001)
  - 204.34.57.64 (bits de sous-réseau = 010)
  - 204.34.57.96 (bits de sous-réseau = 011)
  - 204.34.57.128 (bits de sous-réseau = 100)
  - 204.34.57.160 (bits de sous-réseau = 101)
  - 204.34.57.192 (bits de sous-réseau = 110)
  - 204.34.57.224 (bits de sous-réseau = 111)

La création d'un sous-réseau

- Pour notre exemple, on obtient donc 8 sous-réseaux possibles.

- Les bits de poids faibles (les bits verts) vont indiquer, pour chacun de ces sous-réseaux, les adresses à allouer aux machines.

La création d'un sous-réseau

- Remarquez bien que l'on utilise les combinaisons 000 et 111 pour ces sous-réseaux.
  - La RFC950 qui stipulait que la première et la dernière adresse d'un réseau ne devaient pas être utilisées, est maintenant obsolète.

- En effet, la plupart des routeurs modernes savent très bien gérer des adresses réseau dont tous les bits de sous-réseau sont à 1 ou à 0.
- Pour plus de précision ➔ reportez-vous à la RFC1878 qui propose un découpage en sous-réseaux indépendant des classes (voir l'adressage CIDR - ip classless)

La création d'un sous-réseau

- Par exemple, dans le réseau 204.34.57.32, la première machine portera l'adresse 1.
- Le dernier octet aura alors la valeur de 33.

La création d'un sous-réseau

- L'adresse TCP/IP complète sera donc 204.34.57.33
- Ainsi de suite jusqu'à 204.34.57.62

- On ne peut utiliser l'adresse 204.34.57.63 pour une machine, car elle correspond a l'adresse de broadcast du sous-réseau 204.34.57.32

- Ensuite, dans le réseau 204.34.57.64, la première machine aura pour adresse 204.34.57.65 et ainsi de suite.

La création d'un sous-réseau

- En procédant ainsi, on a découpé un espace, où l'on pouvait initialement allouer 254 machines, en 8 sous-réseaux dans lesquels on ne peut allouer au total que 8 fois 30 machines.

La création d'un sous-réseau

- Le tableau ci-dessous montre, en fonction des bits alloués soit au réseau soit aux hôtes, les différentes possibilités envisageables en classe C

bits réseau/ bits hôte	nb de sous - réseaux	nb d'hôtes	masque
1 / 7	2	126	255.255.255.128
2 / 6	4	62	255.255.255.192
3 / 5	8	30	255.255.255.224
4 / 4	16	14	255.255.255.240
5 / 3	32	6	255.255.255.248
6 / 2	64	2	255.255.255.252
7 / 1	128	0	255.255.255.254

Le masque du sous-réseau

- Avec ces nouveaux sous-réseaux, on doit également modifier le masque de réseau
- Pour notre exemple, le masque initial fourni pour la classe C était de 255.255.255.0
  - Mais on a utilisé les trois bits de poids fort du dernier octet pour coder les sous-réseaux
  - Il faut donc rajouter au masque initial le masque de sous-réseau. Ce dernier vaut 32+64+128, soit 224
- Le nouveau masque réseau est donc 255.255.255.0 + 224 = 255.255.255.224

Le masque du sous-réseau

- Pour résumer, le masque ne dépend que du nombre de bits affectés au réseau et au sous-réseau :
  - il suffit de positionner ces bits à 1 et de faire une somme binaire (un *OU binaire*) pour obtenir le masque
- Ce masque de réseau est important, car il va déterminer l'adresse de diffusion (broadcast) et, limiter les diffusions aux seules machines faisant partie d'un sous-réseau déterminé

Les adresses de diffusion

- Chaque sous-réseau ainsi constitué doit avoir une adresse réseau, un masque de réseau et une adresse de diffusion (broadcast)
- L'adresse de diffusion est simple à calculer : elle correspond à l'adresse du réseau ou du sous-réseau plus l'adresse de l'hôte dont tous les bits sont à 1
  - Chaque sous-réseau possède une adresse de diffusion propre
  - Dans le cas du sous-réseau 204.34.57.32 (exemple traité), le numéro d'hôte dont tous les bits (les bits verts de la figure) sont à 1 est 31
  - Si on ajoute ce nombre à l'adresse du réseau, on obtient 204.34.57.32 + 31 = 204.34.57.63

Exemple 2 : sous-réseau classe B

bits réseau/ bits hôte	nb de sous - réseaux	nb d'hôtes	masque
1 / 15	2	32766	255.255.128.0
2 / 1 4	4	16382	255.255.192.0
3 / 13	8	8190	255.255.224.0
4 / 12	16	4094	255.255.240.0
5 / 11	32	2046	255.255.248.0
6 / 10	64	1022	255.255.252.0
7 / 9	128	510	255.255.254.0
8 / 8	255	254	255.255.255.0

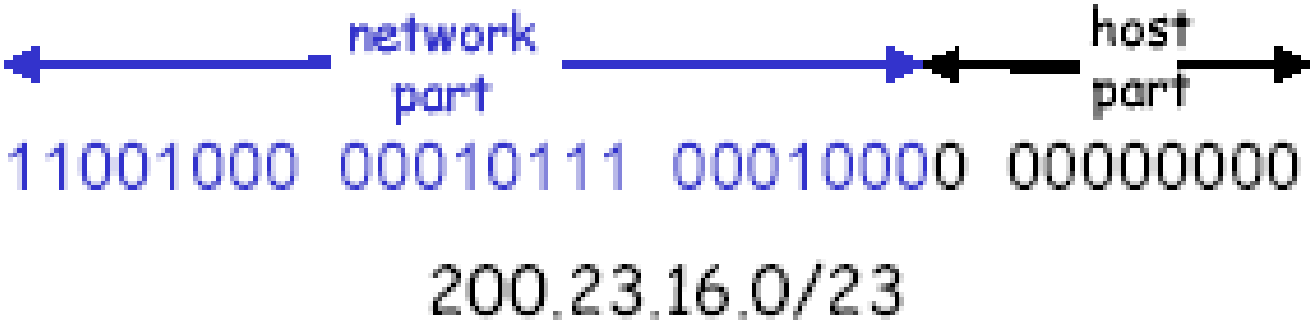
3.5 Adressage IP : CIRD

- **Adressage par classe** :
  - utilisation inefficace de l'espace d'adressage
  - Exemple : une adresse de classe B a assez de place pour pour 65K hôtes, même si il n'y a que 2K hôtes dans ce réseau

Adressage IP : CIRD

CIDR : Classless InterDomain Routing

- La taille de la partie réseau est arbitraire
- Format de l'adresse : a.b.c.d/x, où x est le nombre de bits dans la partie réseau de l'adresse



Adressage IP : CIRD

- En 1992, l'Internet est confronté à plusieurs problèmes cruciaux :
  - Les Classes B sont presque épuisées
  - La croissance des tables de routage sur l'Internet global est très rapide
  - L'espace d'adressage IPv4 s'épuise de manière générale.

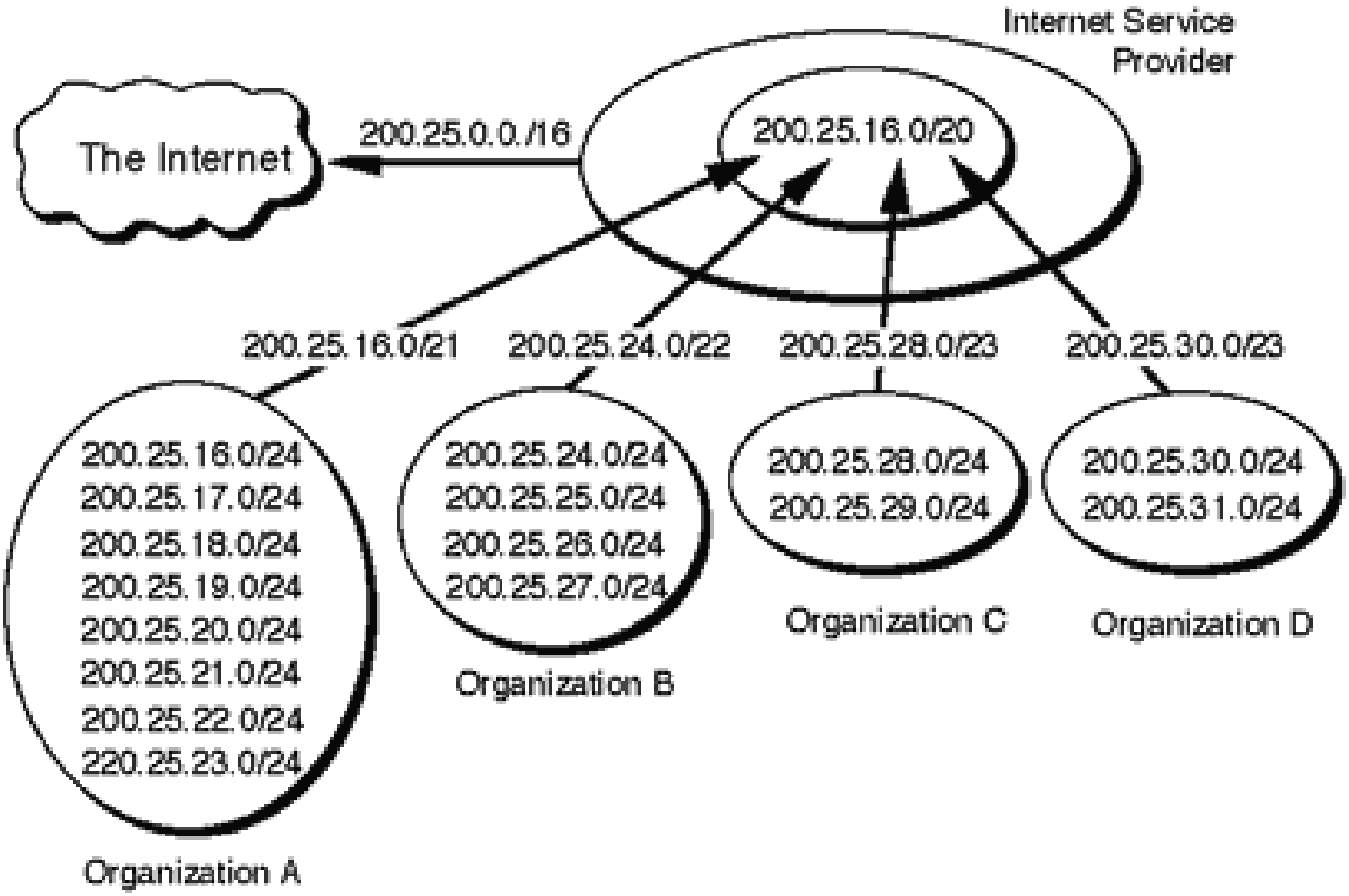
Adressage IP : CIRD

CIDR améliore l'allocation des adresses IPv4

- CIDR supprime l'usage des classes A, B et C pour généraliser celui du préfixe réseau étendu. Les classes A, B ou C n'existent plus; toutes les adresses de réseaux sont annoncées avec leur préfixe qui peut être de taille arbitraire : /9, /10, /11, /12 ...

- Les routeurs ne se basent plus sur les 3 premiers bits de chaque adresse pour déterminer la classe du réseau : seul le préfixe fait loi. Les adresses annoncées de cette manière peuvent être d'anciennes adresses de classe A, B ou C

Adressage IP : CIRD



Adressage IP : CIRD

- Dans l'exemple, un ISP dispose du bloc d'adresse 200.25.0.0/16
  - Cet ISP a alloué 8 blocs /24 à l'organisation A , 4 à l'organisation B, 2 à C et D
  - L'organisation A agrége ses 8 réseaux /24 dans une seule annonce (200.25.16.0/21), B agrége ses 4 /24 dans la seule annonce 200.25.24.0/22, C agrège ses 2 /24 avec l'annonce 200.25.28.0/23 et D fait de même avec l'annonce 200.25.30.0/23
  - Enfin, l'ISP agrège les 254 blocs /24 de ses clients par une seule annonce : 200.25.0.0/16

Adressage IP : CIRD

- l'utilisation d'hôtes classfull en CIDR reste possible dans certains cas :
  - le cas où une adresse comme 192.136.53.0/20 sera allouée sous la forme de 16 réseaux /24, /24 étant correctement interprété comme une adresse de classe C par les hôtes

Adressage IP : CIRD

Classless Inter-Domain Routing)

- Cet adressage ne tient pas compte des classes globales et autorise l'utilisation de sous-réseaux au sein de toutes les classes d'adresses.

- Cette agrégation se fait par région géographique et fournisseurs d'accès.
- Ce système de sur-réseau permet ainsi de faire apparaître dans les tables de routage plusieurs réseaux sous le même identifiant.

Adressage IP : CIRD

- Les réseaux aggrégés doivent avoir des adresses contiguës de manière à avoir des préfixes identiques.
  - Par exemple, 193.127.32.0 et 193.127.33.0 peuvent être agrégés sous la notation 193.127.32.0 / 23.
  - Le nombre 23 est le masque signifiant que les 23 bits de poids fort représentent l'adresse du sous-réseau comme illustré dans le tableau ci-dessous.

Adressage IP : CIRD

193.127.32.0	11000001.01111111.00100000.00000000
193.127.33.0	11000001.01111111.00100001.00000000
193.127.32.0 / 23	11000001.01111111.00100000.00000000

- On peut donc voir le réseau 193.127.32.0 / 23 comme un réseau de 512 machines, ou comme 2 réseaux de 256 machines chacun, car le 24ème bit permet de coder l'un ou l'autre des 2 réseaux.

Adressage IP : CIRD

- Selon les RFC les masques ont de 13 à 27 bits, ce qui donne les possibilités suivantes pour les tailles de réseau.

masque	équivalent en classe C	nombre d'adresses
/27	1/8	32
/26	1/4	64
	...	
/14	1 024	262 144
/13	2 048	524 288

Adressage IP : CIRD

- De cette manière si une société a besoin de 100 000 adresses on lui fournira une part de réseau de classe A en l'associant à un masque de 15 bits.
  - Ainsi, il disposera de $2^{(32-15)}$=131 072 (la plus petite puissance de 2 supérieure à 100 000) adresses.
- Dans l'ancien système, un réseau de classe B n'aurait pas été suffisant et un réseau de classe A, avec ses 16 millions d'adresses, aurait été largement surdimensionné

Adressage IP : CIRD

- Plus d'information dans :
- http://www.faqs.org/rfcs/rfcNUM.html
- http://www.rfc-editor.org/
  - DHCP (Dynamic Host Configuration Protocol) : RFC 2131, 2132
  - Les masques possibles : RFC 1878
  - La conception et le déploiement de CIDR : rfc1517, rfc1518, rfc1519, rfc 1520

4. Fragmentation

- Chaque réseau impose ses contraintes en terme de taille maximum de paquets :
  - Ces limitations sont liées :
    - au matériel ou l'OS
    - au protocole (champs longueur du paquet)
    - réduction des erreurs, de la congestion (retransmission) et de l'occupation du canal

Fragmentation

- Dans le cas d'IP :
  - la taille d'un datagramme maximale est de 65535 octets.
  - Toutefois cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets.
- De plus, les réseaux sur Internet utilisent différentes technologies :
  - taille maximale d'un datagramme varie suivant le type de réseau.

Fragmentation

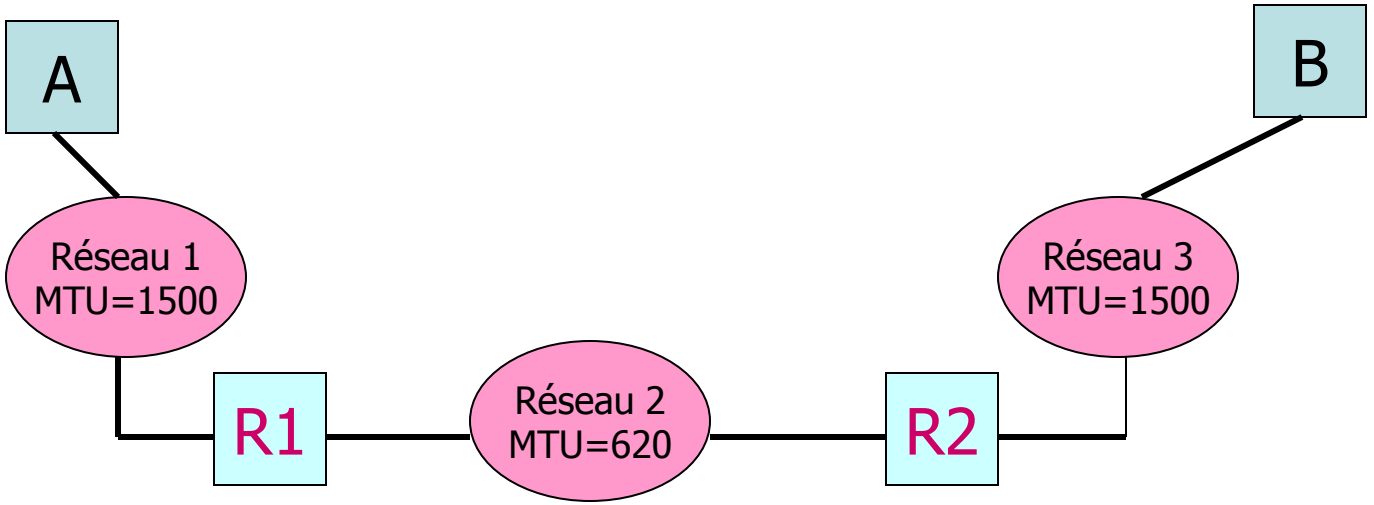
- La taille maximale d'une trame est appelée MTU (Maximum Transfer Unit)
- Elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau
  - 1500 octets pour Ethernet
  - 4470 pour FDDI

Fragmentation

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

Fragmentation

- la fragmentation se situe au niveau d'un routeur qui reçoit des datagrammes issus d'un réseau à grand MTU et qui doit les réexpédier vers un réseau à plus petit MTU.



Fragmentation

- Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter,
  - c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets.

Fragmentation

- Le routeur va ensuite envoyer ces fragments de manière indépendante et les réencapsuler (il ajoute un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment

- et en ajoutant des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre (rien ne dit que les fragments vont arriver dans le bon ordre étant donné qu'ils sont acheminés indépendamment les uns des autres...)

Fragmentation

- Un datagramme fragmenté n'est réassemblé que lorsqu'il arrive à destination finale, même s'ils traversent des réseaux avec un plus grand MTU les routeurs ne réassemblent pas les petits fragments

- De plus chaque fragment est routé de manière totalement indépendante des autres fragments du datagramme d'où il provient

Fragmentation

- Le destinataire final qui reçoit un premier fragment d'un datagramme arme un temporisateur de réassemblage, c'est-à-dire un délai maximal d'attente de tous les fragments.
  - Si, passé ce délai, tous les fragments ne sont pas arrivés il détruit les fragments reçus et ne traite pas le datagramme.
  - Plus précisément, l'ordinateur destinataire décrémente, à intervalles réguliers, de une unité le champ TTL de chaque fragment en attente de réassemblage.

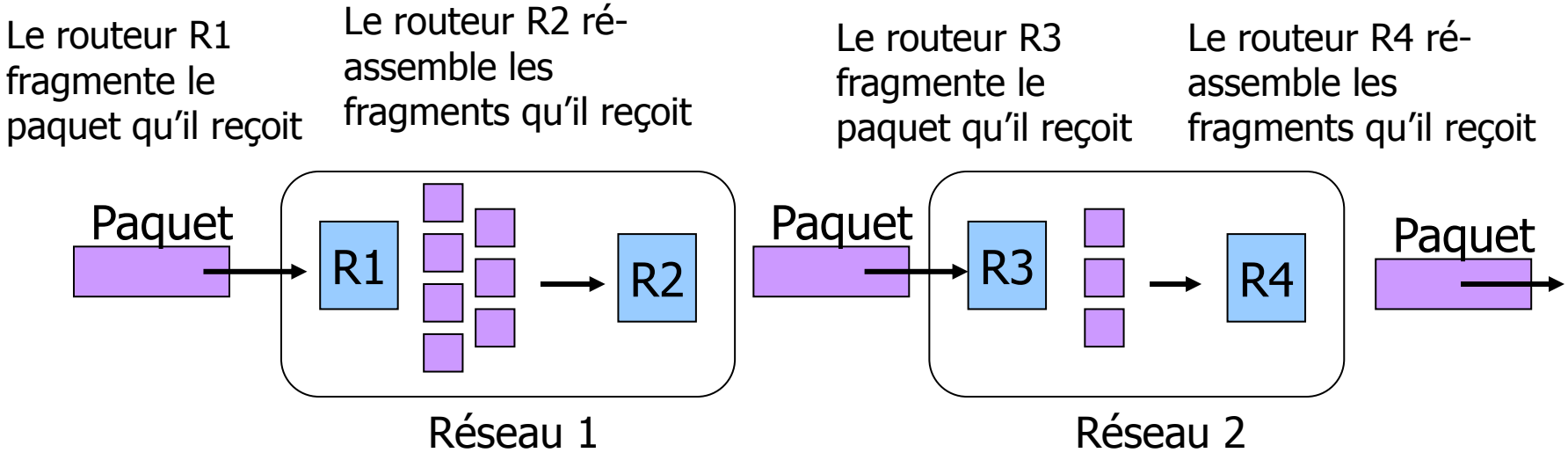
Fragmentation

- Type de Fragmentation
  - Deux stratégies opposées pour réassembler le paquet d'origine à partir des fragments
  - Fragmentation transparente ou
  - Fragmentation non transparent

Fragmentation

Fragmentation transparent

– La fragmentation due à un « réseau à petit paquets » soit transparente à tous les réseaux au travers desquels le paquet doit transiter par la suite vers sa destination finale



Fragmentation

Fragmentation transparent

- Lors qu'un paquet arrive à un routeur, celui-ci le divise en fragments.
  - Chaque fragment est adressé au même routeur de sortie, où ils sont recombinés
  - Les réseaux suivants ne sont même pas au courant qu'il y a eu fragmentation

Fragmentation

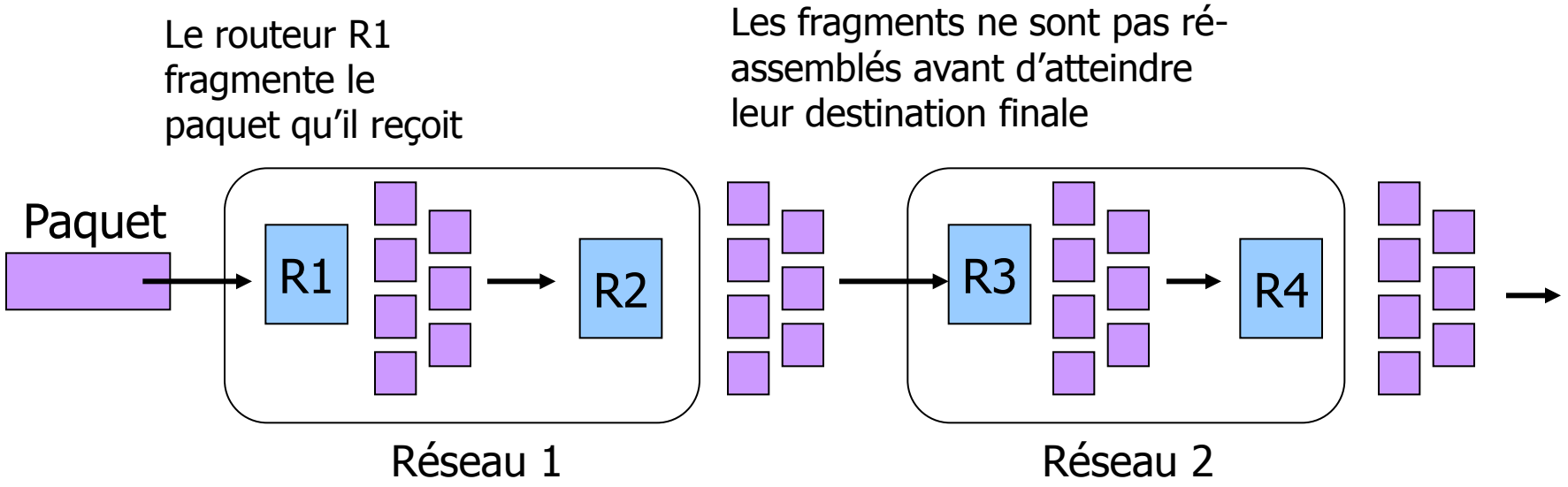
Fragmentation transparent

- Quelques problèmes :
  - Le routeur de sortie doit savoir s'il a bien reçu tous les fragments ou non
    - Champ de numérotation, ou un bit de « fin de paquet » doit être inclus dans chaque paquet
  - Tous les paquets doivent sortir par le même routeur
  - Possibilité de blocage du réassemblage au niveau du routeur de sortie
  - Surcharge (overhead)
    - causée par les fragmentations et réassemblages répétés de paquets volumineux passant au travers toute série de réseaux à petit paquets

Fragmentation

Fragmentation non transparent

– Ne pas faire de réassemblage au niveau des routeurs intermédiaires



Fragmentation

Fragmentation non transparent

- Une fois le paquet fragmenté, chaque fragment est traité comme un autre paquet
- Tous les fragments traversent le (ou les) routeur(s) de sortie
- Le réassemblage des fragments n'intervient qu'au niveau du destinataire

Fragmentation

Fragmentation non transparent

- Quelques problèmes :
  - Nécessite que tout ordinateur destinataire soit capable d'effectuer le réassemblage
  - L'accroissement de la charge globale lorsqu'un gros paquet est fragmenté
    - La surcharge demeure tout au long du trajet
  - Avantage
    - Plusieurs routeurs de sortie peuvent être utilisés
      - mais pas d'avantage si l'inter-réseau est conçu sur le modèle circuit virtuel

Fragmentation

Numérotation des Fragments

- Lorsqu'un paquet est fragmenté, les fragments doivent être numérotés de manière à ce que le flot d'origine puisse être reconstitué

- Différents façon de numéroter les fragments :
  - Utilisation d'un arbre
  - Utilisation de la taille de fragment

Fragmentation

Numérotation des Fragments

- **Utiliser un arbre**
  - Si un paquet 0 doit être subdivisé, les fragments sont appelés 0.0, 0.1, 0.2, etc.
  - Si ces paquets doivent être eux-mêmes subdivisés au routeur suivant les éléments résultants seront numérotés : 0.0.0, 0.0.1, 0.0.2, …0.1.0, 0.1.1, 0.1.2, etc.

- **Problèmes :**
  - Dans le cas où il y a des retransmissions du au fait que le réseau a perdu ou abandonné des paquets

Fragmentation

Numérotation des Fragments

- Supposons qu'un paquet de 1024 bits soit initialement fragmenté en 4 fragments : 0.0, 0.1, 0.2 et 0.3 de tailles égales
  - Le fragment 0.1 est perdu, mais les autres arrivent à destination
- Eventuellement, la temporisation de ré-émission de la source peut passer à zéro, ce qui entraîne la ré-émission du paquet d'origine
  - Supposons cette fois que la route emprunte un réseau ayant une taille de paquet maximale de 512 bits, cela entraîne la génération de deux fragments
  - Lorsque le fragment 0.1 arrive à destination le récepteur pense que les 4 morceaux sont bien là, et reconstruit incorrectement le paquet

Fragmentation

- **Par la taille de fragment élémentaire**
  - Le protocole d'interconnexion définit une taille de fragment élémentaire, suffisamment faible pour qu'il puisse traverser n'importe quel réseau
  - Lorsqu'un un paquet est fragmenté, tous ses fragment ont la taille du fragment élémentaire, excepté le dernier qui peut être plus court
  - Sur inter-réseau, un paquet peut éventuellement contenir, pour des raisons d'efficacité, plusieurs fragments

Fragmentation

Numérotation des Fragments (taille)

- L'en-tête du paquet fournit :
  - Le numéro d'origine du paquet et le numéro du premier fragment élémentaire contenu dans le paquet
  - Il doit y avoir aussi un bit indiquant que le dernier fragment contenu dans le paquet en transit dans l'inter-réseau est le dernier du paquet d'origine

Fragmentation

Numérotation des Fragments (taille)

- Cette approche nécessite deux champs de séquencement dans l'en-tête du paquet en transit dans l'inter-réseau :
  - Le numéro du paquet d'origine
  - Et le numéro de fragment
- Un compromis doit être fait entre la taille du fragment élémentaire et le nombre de bits utilisés pour le numéro du fragment
  - L'ultime limite pour un fragment élémentaire est le bit ou l'octet, avec comme numéro de fragment une indication de décalage d'un octet (ou d'un nombre de bits) à l'intérieur du paquet d'origine

Fragmentation

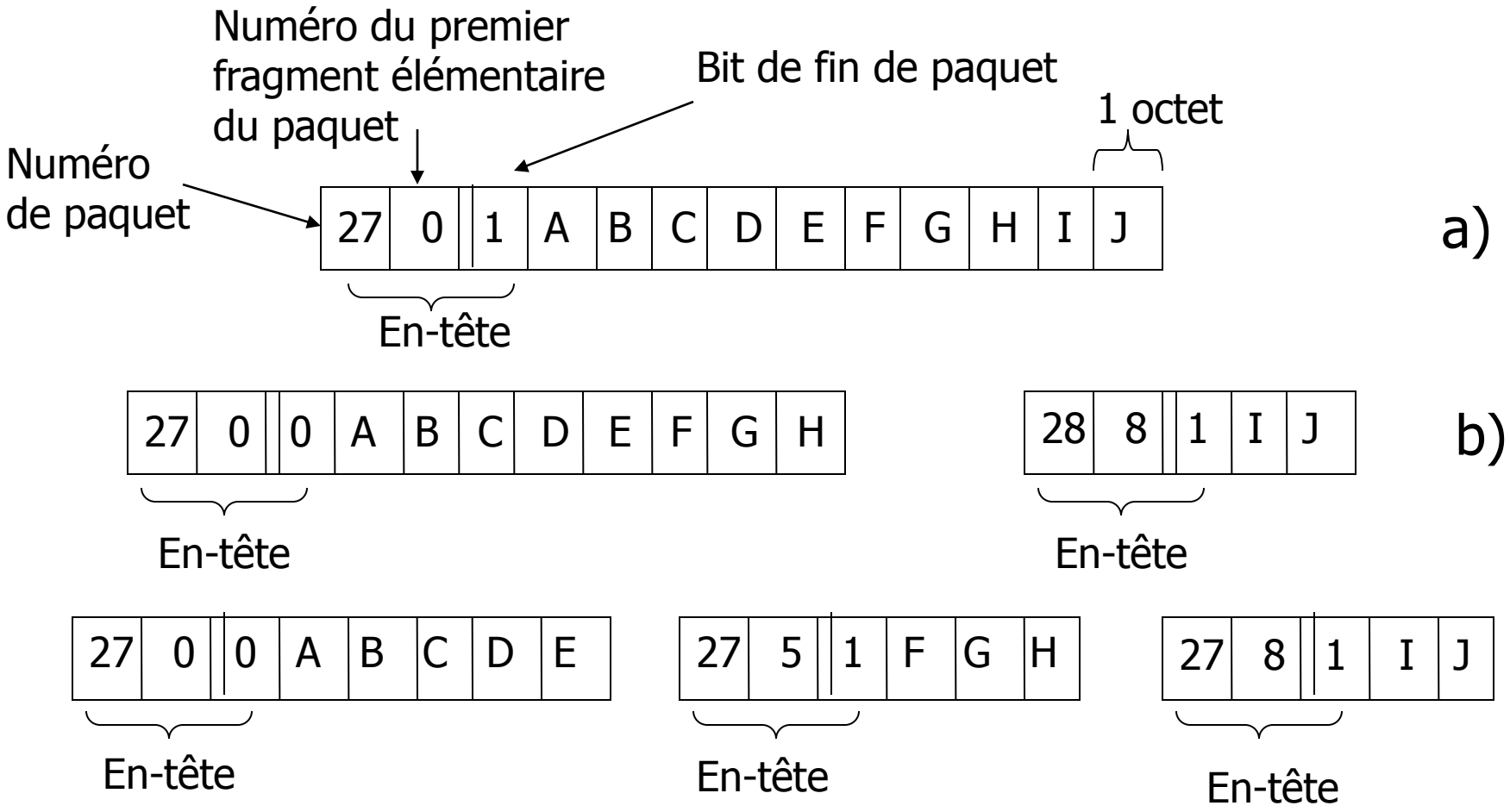
Numérotation des Fragments (taille)

Exemple

- Fragmentation : l'unité de données élémentaire est l'octet
  - A) paquet original de 10 octets
  - B) fragments obtenus dans un réseau où la taille maximale du paquet est de 8 octets
  - C) fragments suivants après passage des paquets de (b) dans un réseau de taille de paquets à 5 octets

Fragmentation

Numérotation des Fragments (taille)



Fragmentation

- Pour tenir compte de la fragmentation, chaque datagramme possède plusieurs champs permettant leur réassemblage :
  - **champ déplacement de fragment** (13 bits) :
    - champ permettant de connaître la position du début du fragment dans le datagramme initial.
    - L'unité de mesure de ce champ est de 8 octets (64 bits)
      - Seul un datagramme complet ou le premier fragment ayant une valeur de zéro

Fragmentation

- **champ identification** (16 bits) : numéro attribué à chaque fragment afin de permettre leur réassemblage dans le bon ordre
- **champ longueur totale** (16 bits) : il est recalculé pour chaque fragment
- **champ drapeau** (3 bits) : il est composé de trois bits :

DF 0 = May Fragment
1 = Don't Fragment

MF 0 = Last Fragment
1 = More Fragments

Fragmentation

- Le premier n'est pas utilisé
- Le second (appelé **DF** : *Don't Fragment*) indique si le datagramme peut être fragmenté ou non.
  - Si jamais un datagramme a ce bit positionné à un et que le routeur ne peut pas l'acheminer sans le fragmenter, alors le datagramme est rejeté avec un message d'erreur

Fragmentation

- Le dernier (appelé **MF** : *More Fragments*, en français *Fragments à suivre*) indique si le datagramme est un fragment de donnée
  - Si l'indicateur est à zéro, cela indique que le fragment est le dernier (donc que le routeur devrait être en possession de tous les fragments précédents) ou bien que le datagramme n'a pas fait l'objet d'une fragmentation