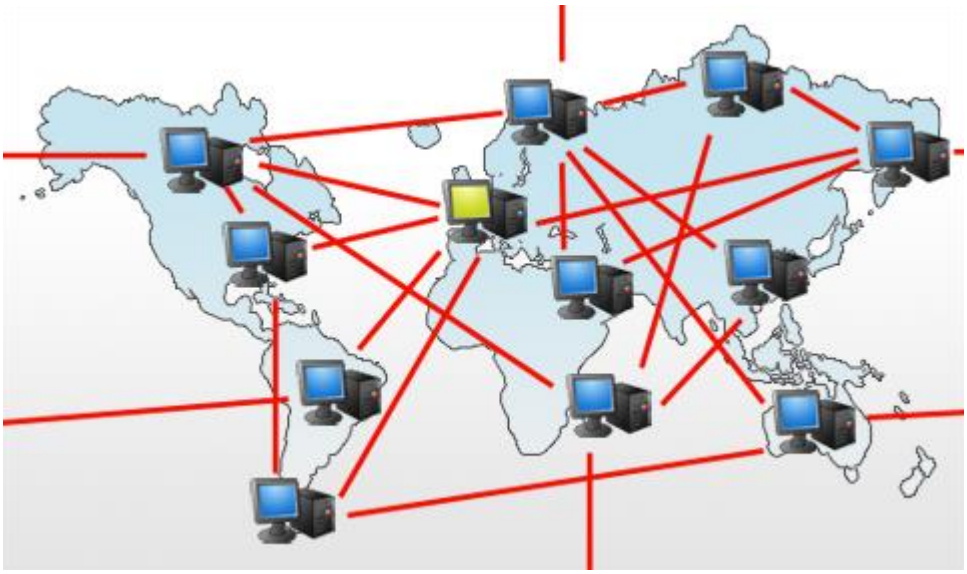
2ème L. Informatique

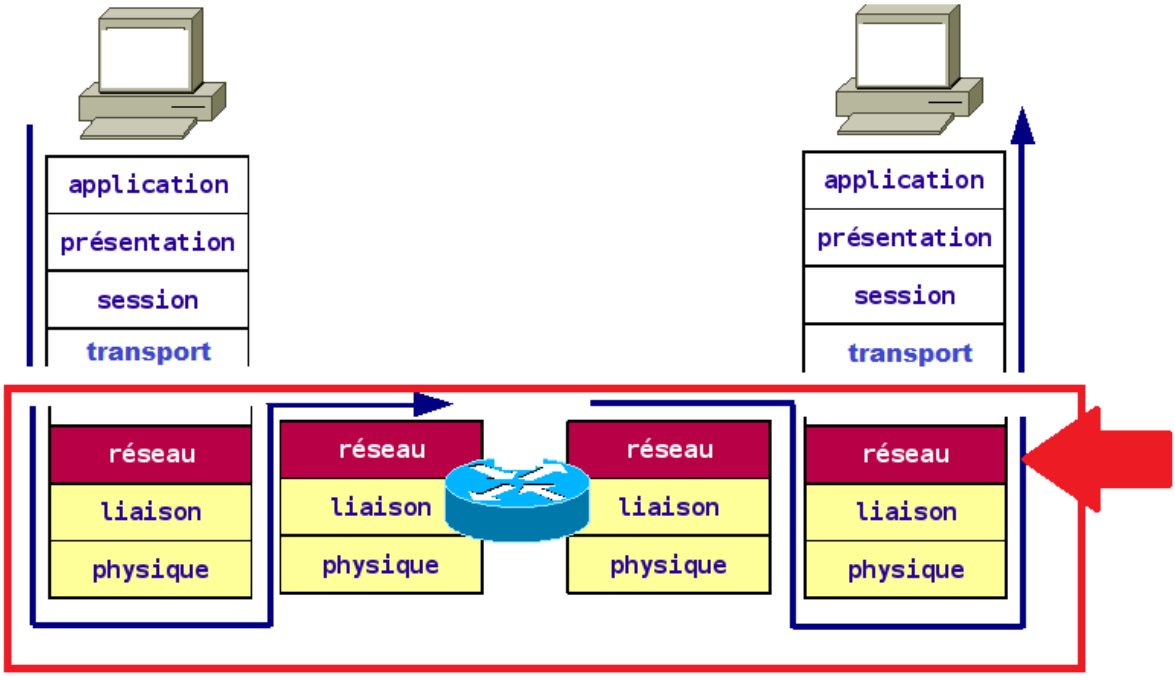
Module : Réseaux

Partie N°05:

Réseaux grande distance :

techniques de commutation, adressage, routage, contrôle de congestion, illustration avec des réseaux d'opérateurs (X.25, Relais de Trames ou Frame Relay, ATM)

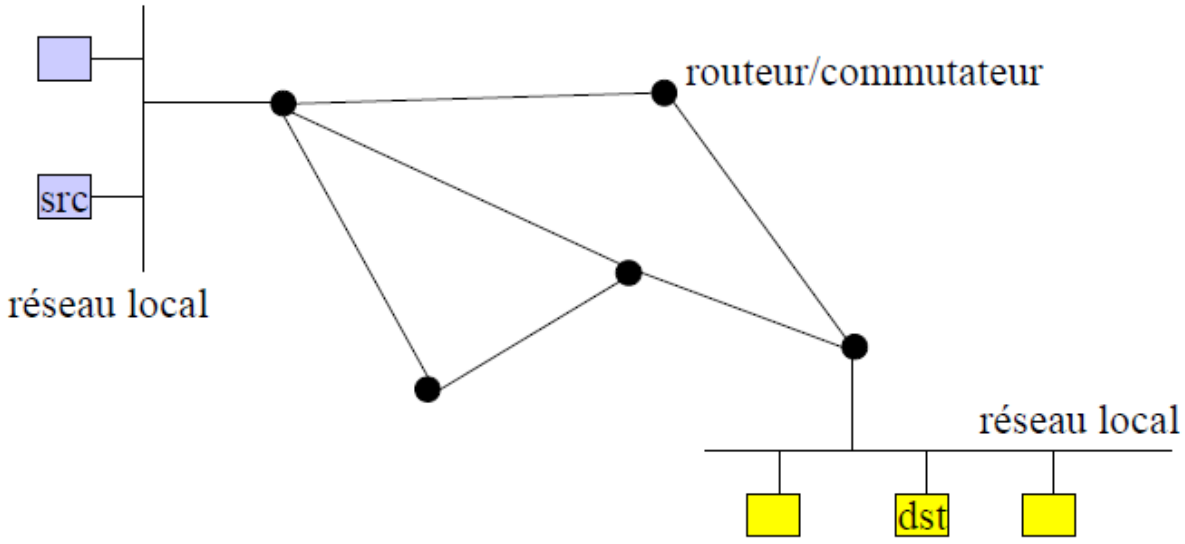




La couche réseau :

La couche de réseau est la troisième couche du modèle OSI.

- Cette couche doit permettre une transmission entre **2 machines**.
- Celles-ci **ne sont pas nécessairement directement connectées**.
- Les données sont fractionnées **en paquets.**



La couche réseau construit une **voie de communication de bout à bout à partir de voies de communication avec ses voisins directs**. Ses fonctions principaux sont donc:

- 1 Adressage :

Il est nécessaire de pouvoir désigner toute machine quelconque accessible directement ou indirectement. ***Il faut donc introduire un mécanisme d'adressage universel***

- **2 Le routage :**

Détermination d'un chemin permettant de relier les 2 machines distantes;

- **3 Le contrôle des flux et contrôle de congestion.**

Cette couche est donc la seule à être directement concernée par la topologie du réseau. C'est aussi la dernière couche supportée par toutes les machines du réseau pour le transport des données utilisateur : les couches supérieures sont réalisées uniquement dans les machines d'extrémité.

Le PDU de cette couche est souvent appelé « **paquet** ».

1- Types de Commutation

Selon **la manière de faire passer l'information de l'émetteur au Récepteur** : on peut classifier les réseaux en deux catégories : **Les réseaux à commutation de circuit** et **les réseaux à commutation de données :**

1-1 Commutation de circuit :

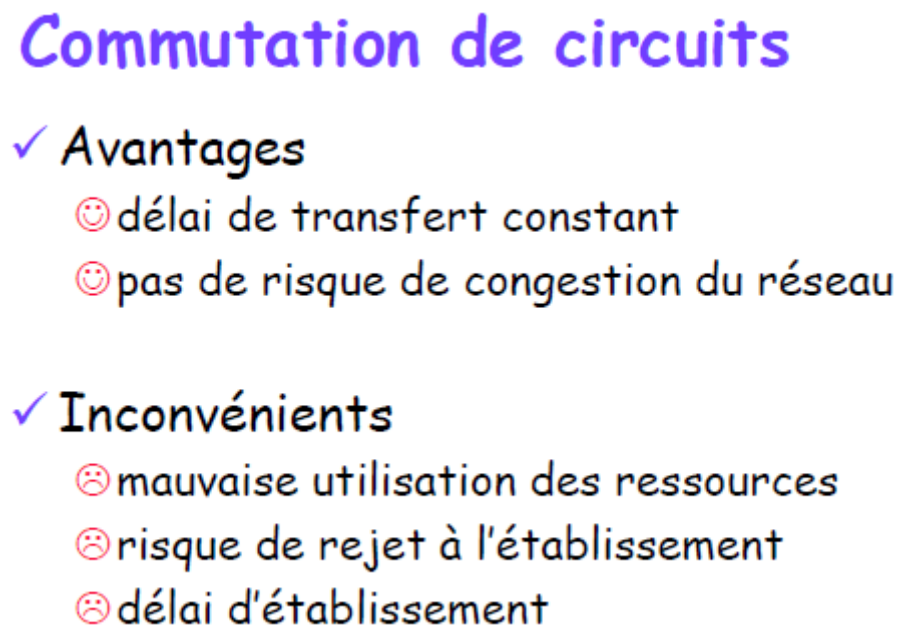
Principe : Un chemin physique est construit de bout en bout (phase de connexion) avant tout échange de données. Le circuit est bloqué **(phase de transfert)** tant que les deux abonnées ne le restituent pas explicitement **(phase de libération).**

Caractéristiques : La commutation de circuit garantit **le bon ordonnancement des données**. **Il n'ya pas de stockage intermédiaire des données**. **Les abonnés monopolisent la ressource durant la connexion. Il ya facturation à la minute.**

Inconvénients : S'il n'ya plus de ressources disponible de bout en bout, **la connexion est refusée.** En plus, il y a une mauvaise utilisation des ressources. : **Le circuit est occupé pendant la communication, qu'il soit utilisé ou non**

Remarque :
Création d'un circuit physique reliant les deux extrémités lors de l'établissement de la connexion Elle est adaptée au transport de la voix

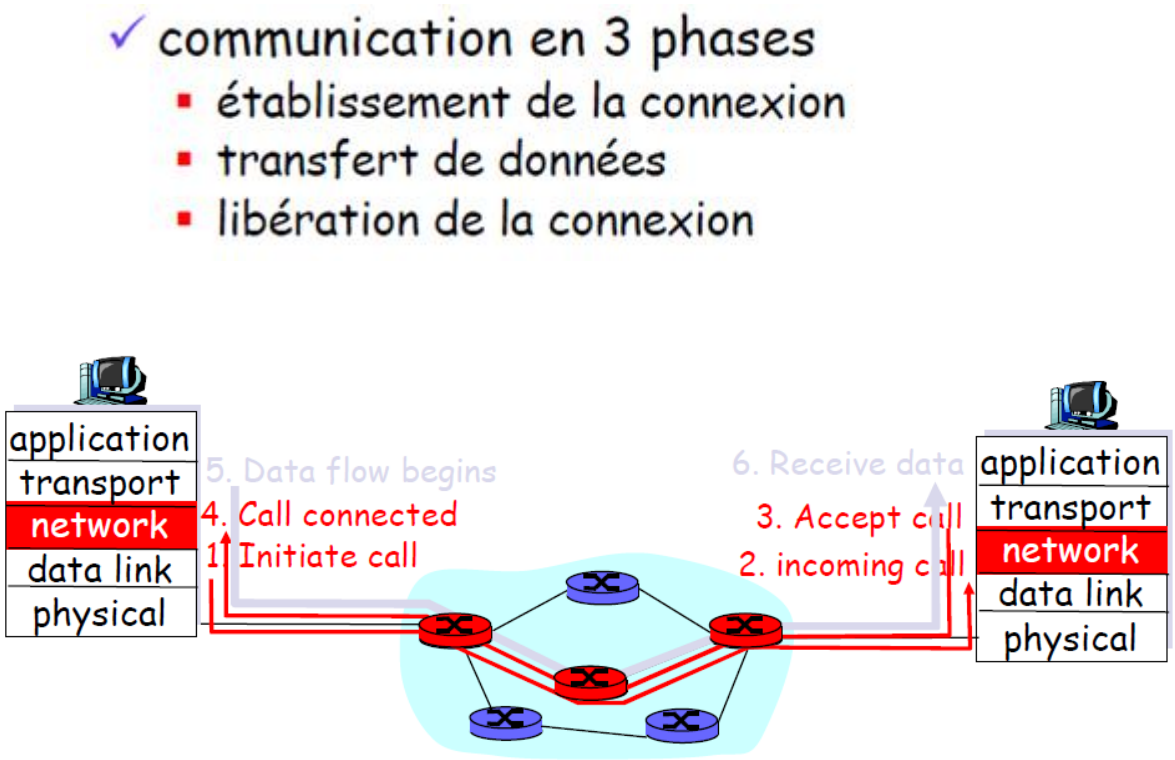
Utilisée sur le réseau téléphonique, RNIS, GSM



Service en mode connecté :

- Est appelée circuit virtuel (VC)
- Chaque paquet comprend le numéro du circuit virtuel. (et non pas l'adresse de la destination)

- Une route est calculée à chaque connexion
- Chaque commutateur maintient un « état » pour chaque connexion qui le traverse
- Des ressources du lien (bande passante) ou du routeur (mémoire) peuvent être allouées au VC



1-2 Commutation de données

Les réseaux à commutation de donnée sont classés selon trois catégories :

1-2-1 La commutation de messages :

Principe : elle consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation en nœud de commutation. **Chaque nœud attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant. Cette technique nécessite de prévoir de grandes zones tampon dans chaque nœud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du réseau. Dans cette approche il devient très difficile de transmettre de longs messages.**

Avantages : Meilleure utilisation des ressources. En cas de fort trafic, il n'ya pas de blocage lié au réseau empêchant l'émission : le message est simplement ralenti. Il ya possibilité de diffusion.

Inconvénients : Nécessite une mémoire de masse importante dans les commutateurs. Le temps d'acheminement non maitrisé, pas adapté aux applications temps réel. Si un message est corrompu, il devra être retransmis intégralement.

1-2-2 La commutation de paquets :

Principe : Elle est apparue au début des années 70 pour résoudre les problèmes d'erreur de la commutation de messages. **Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les unes derrière les autres des paquets appartenant à différents messages. Chaque nœud redirige chaque paquet vers la bonne liaison grâce à une table de routage. La reprise sur erreur est donc ici plus simple que dans la commutation de messages, par contre le récepteur final doit être capable de reconstituer le message émis en réassemblant les paquets. Ceci nécessitera un protocole particulier car les paquets peuvent ne pas arriver dans l'ordre initial, soit parce qu'ils ont emprunté des routes différentes, soit parce que l'un d'eux a du être réémis suite à une erreur de transmission.**

Avantages :

- **Optimisation de l'utilisation des ressources.**
- **Transmission plus rapide que la commutation de messages.**
- **Retransmission uniquement du paquet erroné en d'erreurs.**

Inconvénients :

- **Il peut être nécessaire de réordonner les paquets à l'arrivée.**
- **Chaque paquet doit contenir les informations nécessaires à son acheminement**.

La commutation de paquets est utilisée sur les réseaux locaux, Internet, Frame Relay, GPRS Elle est adaptée au transport des données.

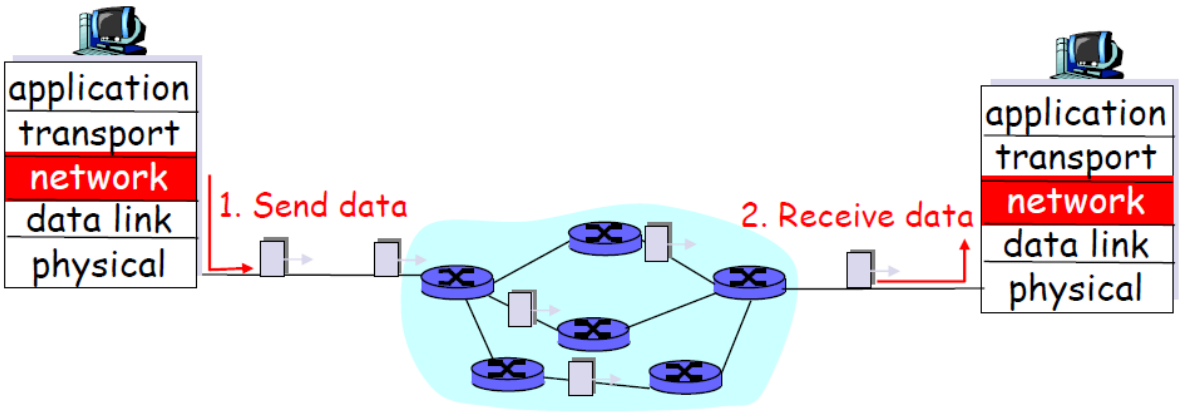
Service en mode non connecté

- Chaque paquet est transporté de façon indépendante.
- comprend l'adresse de destination
- est appelé datagramme (par analogie avec le télégramme)
- Une route est calculée pour chaque paquet

Routage

Le routage est utilisé en mode non connecté. Il consiste à :

- calculer une route pour transférer chaque paquet
- aucun état mémorisé au sujet des connexions
- Des paquets avec la même source et destination peuvent suivre des trajets différents



1-2-3 La commutation de cellules :

Principe : une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets (5 octets d'en-tête et 48 octets de données). C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en **mode connecté** où avant toute émission de cellules, **un chemin virtuel est établi par lequel passeront toutes les cellules**. **Cette technique mixe donc la commutation de circuits et la commutation de paquets de taille fixe** permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.

2- Adressage

Introduction

À la différence des adresses physiques, les adresses réseaux ou adresse IP ont attribuées par les administrateurs réseau et sont configurées logiquement.

Cette adresse IP a un format de 4 octets (32 bits), que l'on a l'habitude de représenter :

- En binaire, si l'on veut identifier plus facilement les deux parties de l'adresse IP, l'adresse réseau et l'adresse hôte :

XXXX XXXX . XXXX XXXX . XXXX XXXX . XXXX XXXX

(**XXXX XXXX** allant de **0000 0000** à **1111 1111**)

- En décimal, si l'on veut condenser l'écriture :

xxx.xxx.xxx.xxx

(xxx allant de **0** à **255**)

Exemple : 193.49.144.1 est une adresse IP

L'adresse IP comporte deux parties principales :

- **Une ID de réseau (netID)** : qui est l'adresse réseau logique du sous réseau auquel l'ordinateur se rattache,
- **Une ID d'hôte (hostID)** : qui est l'adresse logique du périphérique logique identifiant chaque ordinateur sur un sous réseau.

Les classes d'adressage

Les 5 classes d'adresse IP

Au début du développement des protocoles, les réseaux étaient supposés entrer dans l'une des catégories suivantes :

- Un petit nombre de réseaux dotés de nombreux hôtes,
- Quelques réseaux dotés d'un nombre intermédiaire d'hôtes,
- Un grand nombre de réseaux dotés de peu d'hôtes.

1.Définition

Les deux champs de l'adresse IP (**netID** et **hostID**) vont varier suivant ce qu'on appelle la classe d'adresse IP. Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

classe	adresses
A	0.0.0.1 à 126.255.255.254
B	128.0.0.1 à 191.255.255.254
C	192.0.0.1 à 223.255.255.254
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Détermination de la classe

Comment fait-on pour savoir à quelle classe appartient une adresse ?

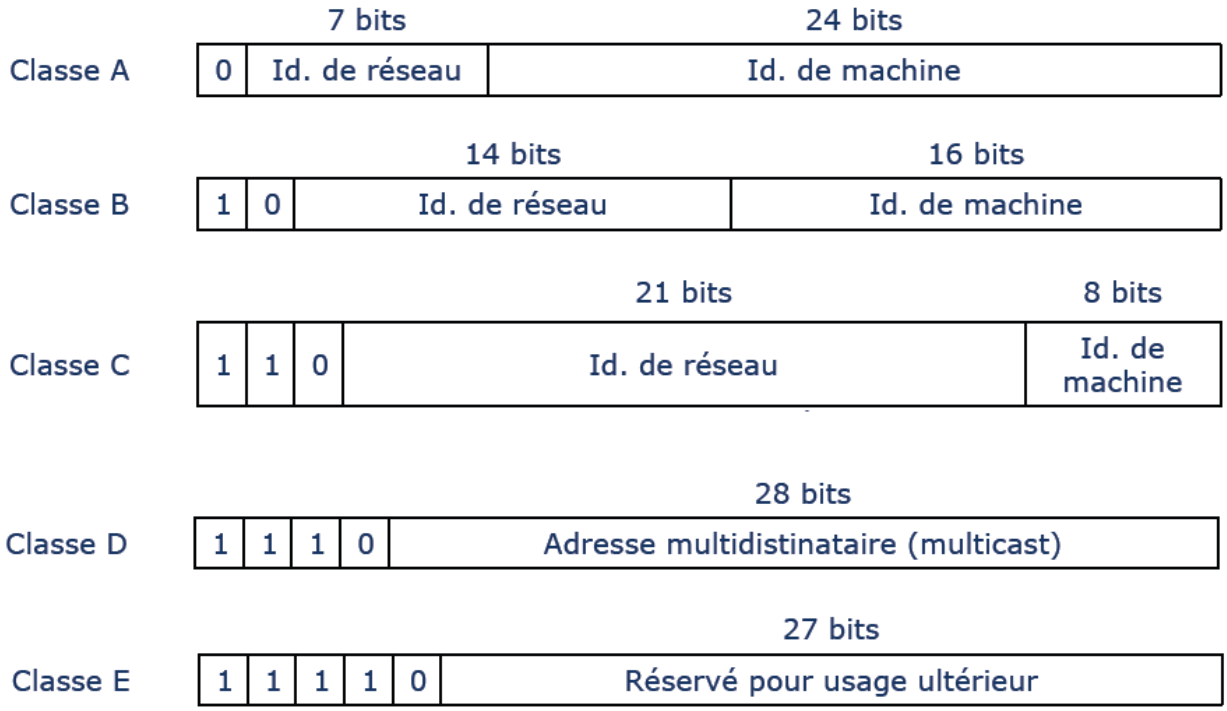
Il y a deux méthodes pour le savoir :

- La triviale, qui consiste à apprendre par cœur le tableau,
- La subtile, qui consiste à retenir la règle, qui est logique :

Voici la règle :

- La classe est définie par les bits les plus lourds (les plus à gauche) de l'adresse,
- Le bit le moins signifiant pour la classe est toujours un 0,
- Les autres sont tous à 1,
- La classe A est signalée par 1 bit, donc **0**,
- La classe B est signalée par 2 bits, donc **1 0**,
- La classe C est signalée par 3 bits, donc **1 1 0**,
- La classe D est signalée par 4 bits, donc **1 1 1 0**,
- La classe E est signalée par 5 bits, donc **1 1 1 1 0**,

Représentation des classes d'adresse IP



Les adresses de classe A

- Le 1er octets est utilisé pour l'adresse réseau (NetID), il varie de 1 à126. Les 2ème ,3ème , et 4ème octets sont utilisés pour les adresses machines (HostID).
- L'adresse IP de classe A autorise 2^7-2 = 126 réseaux (0 et 127 étant réservés), ayant : 2^{24}-2=16777214 machines. Elles sont utilisées pour **les très grands réseaux**.

- **Le masque par défaut** d'une adresse de **classe A** est **255.0.0.0**.

Les adresses de classe B

- Les 1er et le 2ème octets sont utilisés pour l'adresse réseau (NetID), ils varient de 128.0 à191.255. Le 3ème , et 4ème octets sont utilisés pour les adresses machines (HostID).
- L'adresse IP de classe B autorise 2^{14}=16384 réseaux, ayant 2^{16}-2 = 65534 machines.
- **Le masque par défaut** d'une adresse de **classe B** est **255.255.0.0**.

Les adresses de classe C

- Les 1^{er} , le $2^{ème}$, et le $3^{ème}$ octets sont utilisés pour l'adresse réseau (NetID), ils varient de 192.0.0 à 223.255.255. Le $4^{ème}$ octets est utilisé pour les adresses machines (HostID).
- L'adresse IP de classe C autorise 2^{21}= 2097152 réseaux, ayant 2^{8}-2 = 254 machines.
- **Le masque par défaut** d'une adresse de **classe C** est **255.255.255.0**.

Les adresses de classe D

- La classe D est ce qu'on appelle "Multicast", c'est-à-dire qu'elle est destinée à faire de la diffusion d'information sur plusieurs hôtes simultanément. Elle n'a donc pas de netID ni de hostID.

Les adresses de classe E

- La classe E n'est pas utilisée et est destinée à un usage ultérieur.

Remarques

L'obtention d'une adresse IP pour créer un nouveau réseau est gérée par l'INTERNIC de manière décentralisée, à savoir qu'un organisme national gère les demandes pour chaque pays.

Les adresses IP spécifiques

1. 0.X.Y.Z

Elle est utilisée par une machine pour connaître sa propre adresse IP lors d'un processus d'amorçage par exemple,

2. <netID=0>.<hostID>

Elle est également utilisée pour désigner une machine sur son réseau lors d'un boot également,

3. <netID>.<hostIDa tous ses bits à0>

Elle n'est jamais affectée à une machine car elle permet de désigner le réseau lui-même (ex : 145.32.0.0),

4. <netID>.<hostIDa tous ses bits à1>

C'est une adresse de diffusion ou de broadcasting, c'est-à-dire qu'elle désigne toutes les machines du réseau concerné. Un datagramme adressé à cette adresse sera ainsi envoyé à toutes les machines du réseau (ex : un message envoyéà165.10.255.255 est diffusé à tous les hôtes du netID: 165.10),

5. 255.255.255.255

C'est une adresse de diffusion locale car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. L'avantage par rapport à l'adresse précédente est que l'émetteur n'est pas obligé de connaître l'adresse du réseau auquel il appartient,

6. 127.X.Y.Z

C'est une adresse de rebouclage (loopbackou encore localhost). **Le message est envoyé à cet adresse ne sera pas envoyé au réseau, il sera retourné à l'application par le logiciel de pilote de la carte.** L'adresse IP 127.0.0.1 est utilisée pour la machine locale et pour tester si la carte de réseau est bien installée.

Délivrance des adresses IPv4 :

On distingue deux types d'adresses IP :

Les adresses privées :

Il arrive fréquemment dans une entreprise ou une organisation qu'un seul ordinateur soit relié à internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à internet (on parle généralement de proxy ou de passerelle).

Dans ce cas de figure, seul l'ordinateur relié à internet a besoin de réserver une adresse IP auprès de l'ICANN. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble en interne.

Ainsi, l'ICANN a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux. Il s'agit des adresses suivantes :

- **Adresses IP privées de classe A : 10.0.0.1 à 10.255.255.254**, permettant la création de vastes réseaux privés comprenant des milliers d'ordinateurs.
- **Adresses IP privées de classe B : 172.16.0.1 à 172.31.255.254**, permettant de créer des réseaux privés de taille moyenne.
- **Adresses IP privées de classe C : 192.168.0.1 à 192.168.255.254**, pour la mise en place de petits réseaux privés.

Les adresses publiques :

Délivrées par une structure mondiale qui en assure l'unicité. Ce dernier point est capital pour assurer l'efficience du routage.

Notion de sous-réseaux et de masque :

La hiérarchie à deux niveaux (réseau et machine) de l'adressage IP s'est rapidement révélée **insuffisante à cause de la diversité des architectures des réseaux** d'organisation connectés. La notion de sous-réseau fut introduite en 1984 et a conservé le format de l'adresse IP sur 32 bits. **Dans un réseau subdivisé en plusieurs sous-réseaux**, **on exploite autrement le champ identifiant de machine de l'adresse IP. Celui-ci se décompose désormais en un identifiant de sous-réseau et un identifiant de machine.** Remarquons que ce découpage n'est connu qu'à l'intérieur du réseau lui-même. En d'autres termes, une adresse IP, vue de l'extérieur, reste une adresse sur 32 bits. On ne peut donc pas savoir si le réseau d'organisation est constitué d'un seul réseau ou subdivisé en plusieurs sous-réseaux.

Le masque de sous-réseau (netmask) est alors utilisé pour différencier les bits réservés à l'adressage des sous-réseaux de ceux qui correspondent à la machine. Il contient des 1 sur toute la partie identifiant le réseau et les bits de sous-réseau et des 0 sur la partie réservée au numéro de machine dans le sous-réseau.

Le masque comme l'adresse IP est une suite de 4 octets, soit 32 bits. **Chacun des ces bits peut prendre la valeur 1 ou 0. Et bien il nous suffit de dire que les bits à 1 représenteront la partie réseau de l'adresse, et les bits à 0 la partie machine**.

Il y a plusieurs aspects importants des masques :

- Codés sur 4 octets, soit 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.

Comment le masque et l'adresse IP sont-ils associés ?

Prenons par exemple une machine qui a pour adresse IP 192.168.25.147. Il nous faut lui associer un masque pour savoir quelle partie de cette adresse représente le réseau. Associons-lui le masque suivant : 255.255.255.0. On remarque que les bits des trois premiers octets sont à 1, ils représentent donc la partie réseau de l'adresse, soit 192.168.25, le 147 permettant d'identifier la machine au sein de ce réseau. Dans cet exemple, on remarque qu'un octet a été réservé pour l'adresse machine, ce qui nous donne $2^8 = 256$ adresses disponibles pour les machines sur le réseau 192.168.25. Les adresses disponibles pour les machines seront donc:

192.168.25.0 (réservée pour le réseau,)
192.168.25.1
...
192.168.25.254
192.168.25.255 (réservée pour le broadcast,)

On observe donc que c'est le masque qui détermine le nombre de machines d'un 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.

Ainsi, on peut tout de suite dire si un masque semble valide au premier coup d'œil. Un masque en 255.255.224.0 sera correct alors qu'un masque en 255.255.232.0 ne le sera pas (à moins de ne pas vouloir respecter la contiguïté des bits) .

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

Une autre notation est souvent utilisée pour représenter les masques. On la rencontre souvent car elle est plus rapide à écrire. Dans celle-ci, on note directement le nombre de bits significatifs en décimal, en considérant que la contiguïté est respectée. Ainsi, pour notre 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

Comment déterminer qu'une machine appartient à mon réseau ?

C'est très simple. Pour cela, il va falloir déterminer si l'adresse de la machine appartient à la plage d'adresses définie par mon adresse et mon masque. **Pour cela, je fais un ET logique entre mon adresse et mon masque réseau**, j'en déduis donc l'adresse de mon réseau.

Je fais pareil avec l'adresse de l'autre machine et MON masque réseau, et j'obtiens une adresse de réseau. Si les deux adresses de réseau sont les mêmes, ça veut dire que la machine appartient bien au même réseau.

Disons par exemple que ma machine ait pour adresse 192.168.0.140/255.255.255.128 et je veux savoir si les machines A et B ayant pour adresses 192.168.0.20(A) et 192.168.0.185(B) sont sur le même réseau ? Je fais

```
      192.168.   0. 140
ET  255.255.255.128
    ------------------
=     192.168. 0.  128
```

de même avec les deux autres adresses :

Pour A

```
      192.168.  0.   20
ET   255.255.255.128
    ------------------
=     192.168.0.0
```

et pour B

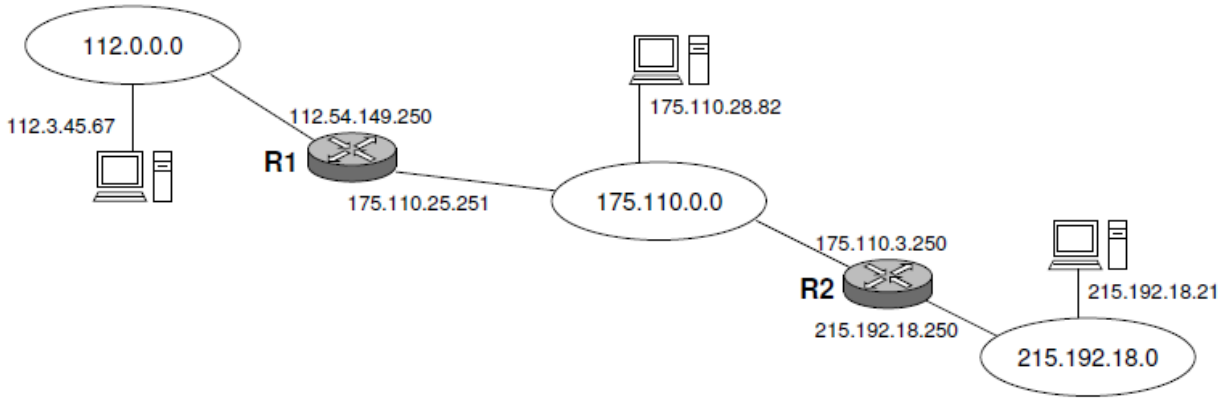
```
      192.168.0.185
ET   255.255.255.128
    ------------------
=     192.168.0.128
```

On voit ainsi que les nombres obtenus sont les mêmes pour ma machine et B. On en déduit donc que B est sur le même réseau, et que A est sur un réseau différent.

Décision de routage dans IP

Le réseau local auquel est relié la machine est calculé en effectuant un et logique entre l'adresse IP de la machine et son masque de réseau. Pour savoir si une machine destination est dans le même réseau il faut faire la même opération avec l'adresse que l'on souhaite joindre et son propre masque de réseau. Si le résultat est le même alors les deux machines sont dans le même réseau local et la communication peut s'effectuer via le réseau local. Dans le cas contraire la machine source doit envoyer le datagramme au routeur de sortie (dont elle connaît l'adresse IP par configuration et qu'elle peut joindre en utilisant le LAN). Le routeur se chargera de trouver le prochain saut et ainsi d'acheminer le datagramme un peu plus loin dans le réseau jusqu'à destination.

Exemple :



La table de routage de la station `112.3.45.67` peut être la suivante :

Destination	Routeur
112.0.0.0	0.0.0.0
175.110.0.0	112.54.149.250
215.192.18.0	112.54.149.250

Celle du routeur R1 peut être :

Destination	Routeur
112.0.0.0	0.0.0.0
175.110.0.0	0.0.0.0
215.192.18.0	175.110.3.250

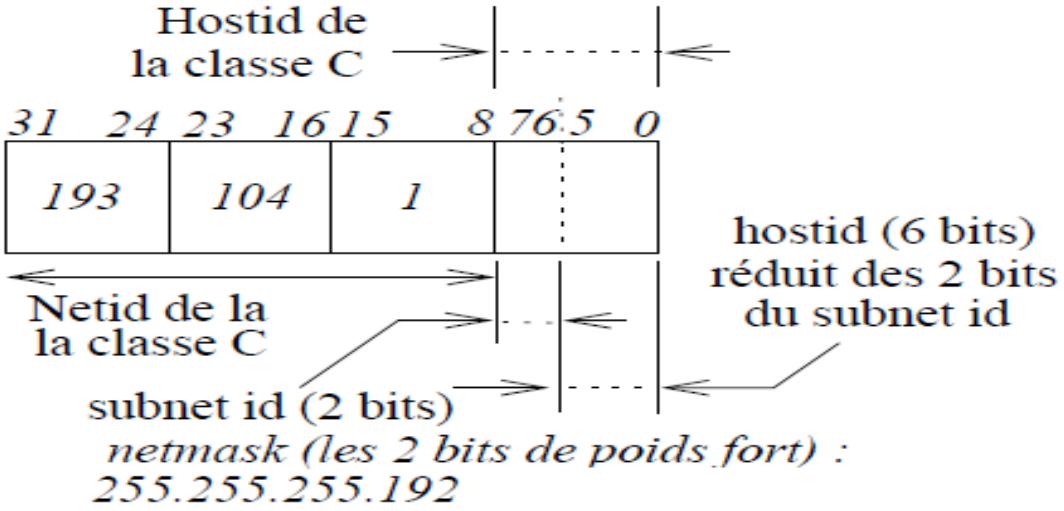
Si la station 112.3.45.67 émet un datagramme à destination de 215.192.18.21, alors elle enverra une trame à R1 (112.54.149.250). Celui-ci enverra une autre trame à R2 (175.110.3.250) qui, à son tour, émettra une trame à destination de 215.192.18.21 (remise directe).

Sous-réseaux

Le " subnet " ou sous-réseau est mis en place pour permettre aux administrateurs de gérer plus finement de grands réseaux.
Le " subnet " utilise les bits de poids fort de la partie hôte de l'adresse IP, pour désigner un réseau. Le nombre de bits employés est laissé à l'initiative de l'administrateur.

Exemple :

Dans l'exemple suivant, les bits 6 et 7 de la partie " host " sont utilisés pour caractériser un sous réseau.



Nous avons d'une part $2^7 + 2^6 = 192$, et d'autre part $2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 63$. Ce qui permet de caractériser 4 sous-réseaux de 61 machines (63 moins l'adresse de broascast, et le " 0 " n'´etant pas compté). Le calcul des masques et des adresses de diffusion est expliqué dans le tableau suivant :

Numéro du réseau	" Netmask "	" Broadcast "	Adressage hôte
193.104.1.00	255.255.255.192	00 + 63 = 63	.1 à .62
193.104.1.64	255.255.255.192	64 + 63 = 127	.65 à .126
193.104.1.128	255.255.255.192	128 + 63 = 191	.129 à .190
193.104.1.192	255.255.255.192	192 + 63 = 255	.193 à .254

Soit un total de 61 × 4 = 244 hôtes possibles pour cette classe C avec un masque de sous-réseau , au lieu des 253 hôtes sans.

Comment découper une plage d'adresses en plusieurs sous-réseaux ?

1 - Détermination des masques pour chacun des réseaux

Ainsi nous allons encore partir du nombre de machines dans chacun des réseaux. Prenons l'exemple suivant du réseau 193.225.34.0/255.255.255.0. On désire faire un sous-réseau de 44 machines et un sous réseau de 20 machines. De la même façon que nous l'avons vu précédemment, pour 44 machines, il faudra réserver 64 adresses, soit un masque 255.255.255.192. Pour 20 machines, il faudra réserver 32 adresses, soit un masque 255.255.255.224.

2 - Détermination des plages réseau

Nous allons donc devoir placer trois plages de 128, 64 et 32 adresses dans une plage de 256 adresses, cela ne devrait pas poser de problème.

On commence par la plage la plus grande de 128 adresses. Si on commençait par la plus petite et qu'on la plaçait n'importe où, cela pourrait poser problème. Imaginons que l'on place la plage de 32 adresses de 0 à 31, et celle de 64 adresses de 128 à 192, il ne nous resterai plus de place pour la plage de 128 adresses !!! On a donc deux choix pour cette plage de 128 adresses, soit les adresses de 0 à 127, soit de 128 à 255. A priori, les deux choix sont possibles et non déterminants. On choisit de 0 à 127. Ainsi, notre sous-réseau sera caractérisé par 193.225.34.0/255.255.255.128.

Pour la seconde plage de 64 adresses, il nous reste deux plages d'adresses possibles, de 128 à 191, et de 192 à 255. Là encore le choix n'est pas déterminant. On choisit de 128 à 191. Ainsi, notre sous-réseau sera caractérisé par 193.225.34.128/255.255.255.192

(ici, la première adresse de notre plage (l'adresse du réseau)est celle en 128 et le dernier octet du masque en 192 nous indique que ce sous-réseau contient 64 adresses)

Enfin, pour la dernière plage de 32 adresses, il nous reste encore deux possibilités de 192 à 223 ou de 224 à 255. On choisit de 192 à 223. Ainsi, notre sous-réseau sera caractérisé par 193.225.34.192/255.255.255.224

Le résultat

Nous avons donc découpé notre réseau d'origine 193.225.34.0/255.255.255.0 en trois sous-réseaux

193.225.34.0/255.255.255.128
193.225.34.128/255.255.255.192
193.225.34.192/255.255.255.224

Il nous reste même une plage de 32 adresses non utilisées de 224 à 255.

3- Routage

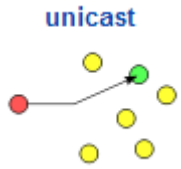
Présentation du routage :

Le routage est le processus qu'un routeur utilise pour transmettre des paquets vers un réseau de destination.

Types de cardinalité de la communication

En fonction du nombre de destinataires et de la manière de délivrer le message, on distingue :

- **unicast**, qui consiste à acheminer les données vers une seule destination déterminée,



- **broadcast** qui consiste à diffuser les données à toutes les machines,

- **multicast** qui consiste à délivrer le message à un ensemble de machines manifestant un intérêt pour un groupe,

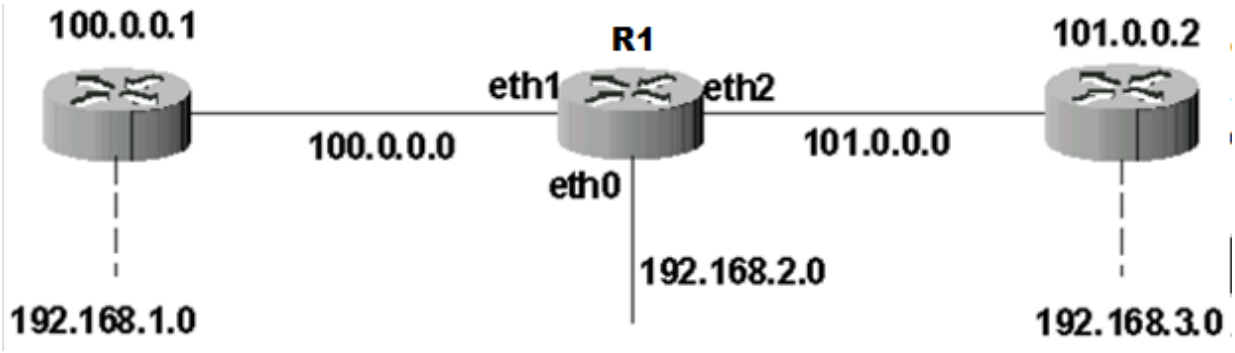
Remarque :

Routeur :

- Un routeur est un dispositif relié à au moins deux réseaux, dont le travail est de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé. Pour ce faire un routeur utilise une « table de routage ».

Table de routage :

- Une table de routage est une liste contenant essentiellement trois types d'informations : **des adresses réseau avec le masque réseau associé et le moyen de les atteindre**. Soit le réseau est **directement connecté** à l'appareil, dans ce cas le moyen de l'atteindre est **le nom de l'interface**, soit, il s'agit de l'adresse du **prochain routeur** situé sur la route vers ce réseau. **Dans le cas où plusieurs chemins sont possibles**, on fait appel à des **algorithmes** spéciaux. Par exemple, considérons **le routeur R1**, sa table de routage :



Réseau	Masque	Moyen de l'atteindre
192.168.2.0	255.255.255.0	eth0
100.0.0.0	255.0.0.0	eth1
101.0.0.0	255.0.0.0	eth2
192.168.1.0	255.255.255.0	100.0.0.1
192.168.3.0	255.255.255.0	101.0.0.2

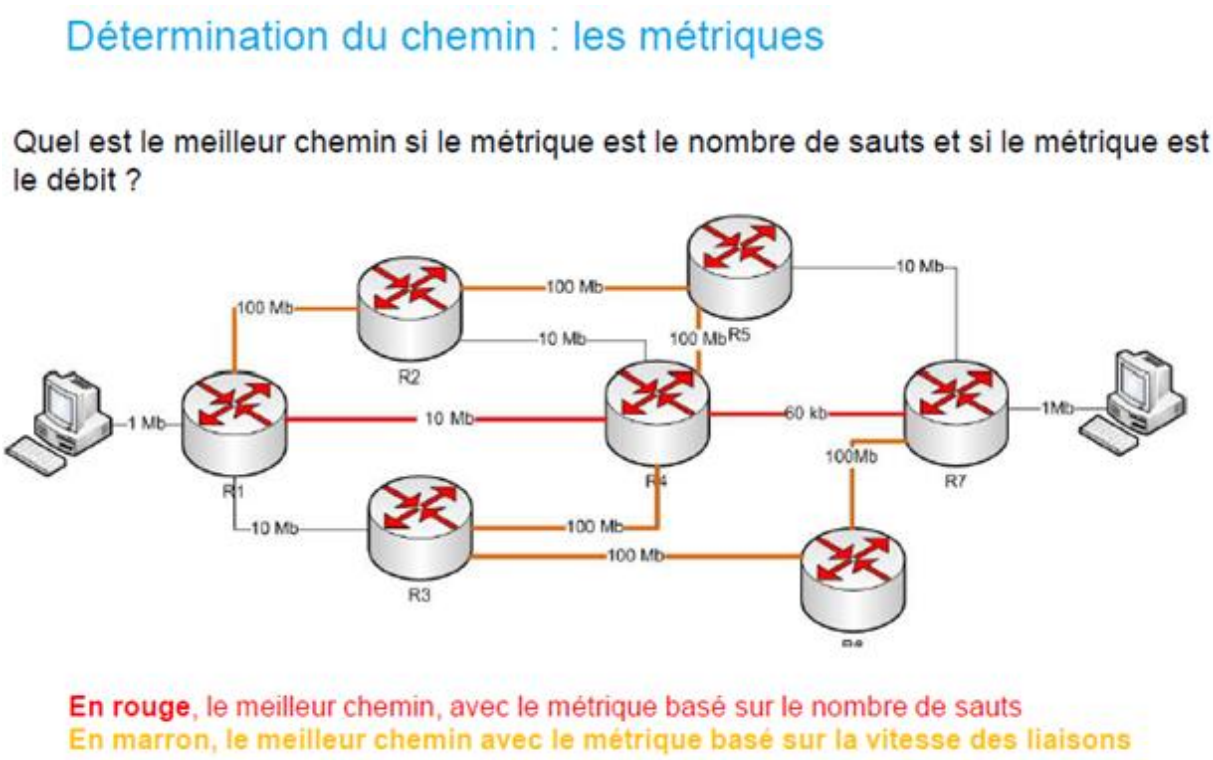
Un routeur prend des décisions en fonction de l'adresse IP de destination d'un paquet.

Lorsque les routeurs utilisent ***le routage dynamique***, ces informations sont fournies **par les autres routeurs**. Lorsque **le *routage statique*** est utilisé, **un administrateur** réseau configure manuellement les informations sur les réseaux distants.

Les service de routage utilisent les informations de topologie du réseau pour évaluer les chemins (distance) ; cette distance est un coût estimé par chaque routeur à partir de messages envoyés par les routeurs voisins. Elle impose de fixer **une métrique** commune à chaque routeur, basée par exemple sur :

- **Le nombre de saut**, c'est à dire le nombre de réseaux intermédiaires que le paquet devra traverser avant d'atteindre sa destination finale. Dans ce cas, la distance entre routeurs voisins est une constante fixée à 1.
- **Vitesse de liaisons (débit)**.

- **Le nombre de paquets dans la file d'attente de l'interface choisie**, ce qui permet d'avoir une idée de l'état de congestion d'un lien particulier.
- **Le temps mis pour atteindre le prochain routeur**. Ce délai est estimé grâce à l'émission de paquets comparables à des Ping ICMP.
- **Le coût financier du lien**.



Utilisation de la route statique

Puisqu'une route statique est configurée manuellement, l'administrateur doit la configurer sur le routeur à l'aide de la commande ip route

Router(config)#ip route **{réseau destination} {masque} {passerelle} {distance administrative}**

La passerelle : 1- Soit l'interface de sortie du routeur local
2- Soit l'adresse IP de l'interface du saut suivant

Exemple : 1- Router(config)#ip route 10.0.0.0 255.0.0.0 S1

La distance administrative est un paramètre optionnel qui donne une mesure de la fiabilité de la route. *Plus la valeur de la distance administrative est faible et plus la route est fiable*.
La distance administrative par défaut est **1** quand on utilise une route statique (Entre 0 et 255).

Introduction aux protocoles de routage

Un protocole de routage est le *système de communication* utilisé *entre les routeurs*, il permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît (mises à jour des tables de routage).

Un protocole routé (IP, IPX, DECnet,AppleTalk,…) sert à diriger le trafic utilisateur. Il fournit suffisamment d'informations dans son adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre en fonction de la méthode d'adressage.

Fonctionnement du routage dynamique :

Le protocole de routage prend connaissance de toutes les routes disponibles. Il insère les meilleures routes dans la table de routage et supprime celles qui ne sont plus valides. Chaque fois que la topologie du réseau est modifiée (la croissance, reconfiguration ou une panne), la base de connaissances du réseau doit également être modifiée.
Lorsque tous les routeurs d'un interréseau reposent sur les mêmes connaissances, on dit de l'interréseau qu'il a **convergé**.
Une convergence rapide est préférable, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces.

Identification des classes des protocoles de routage

Il existe 2 grandes catégories :

- vecteur de distance :

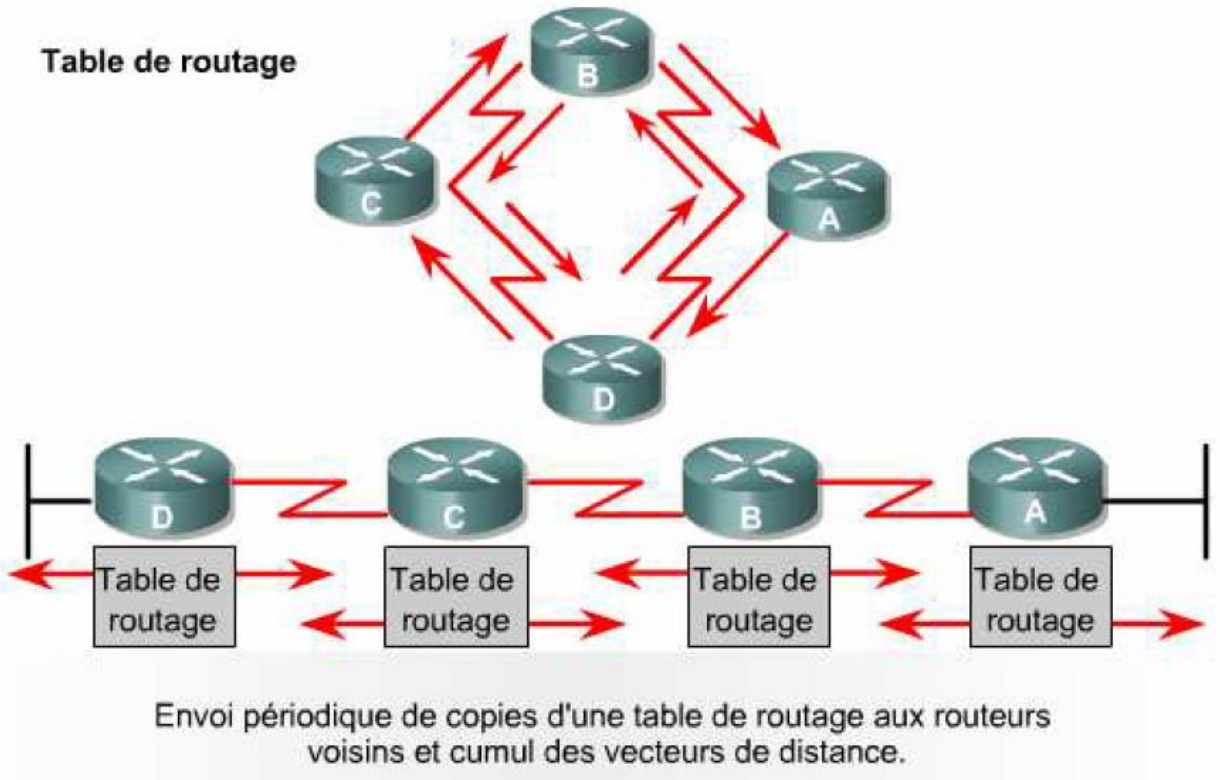
Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'interréseau.

- état de liens :

L'approche à état de liens, également appelée routage par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau.

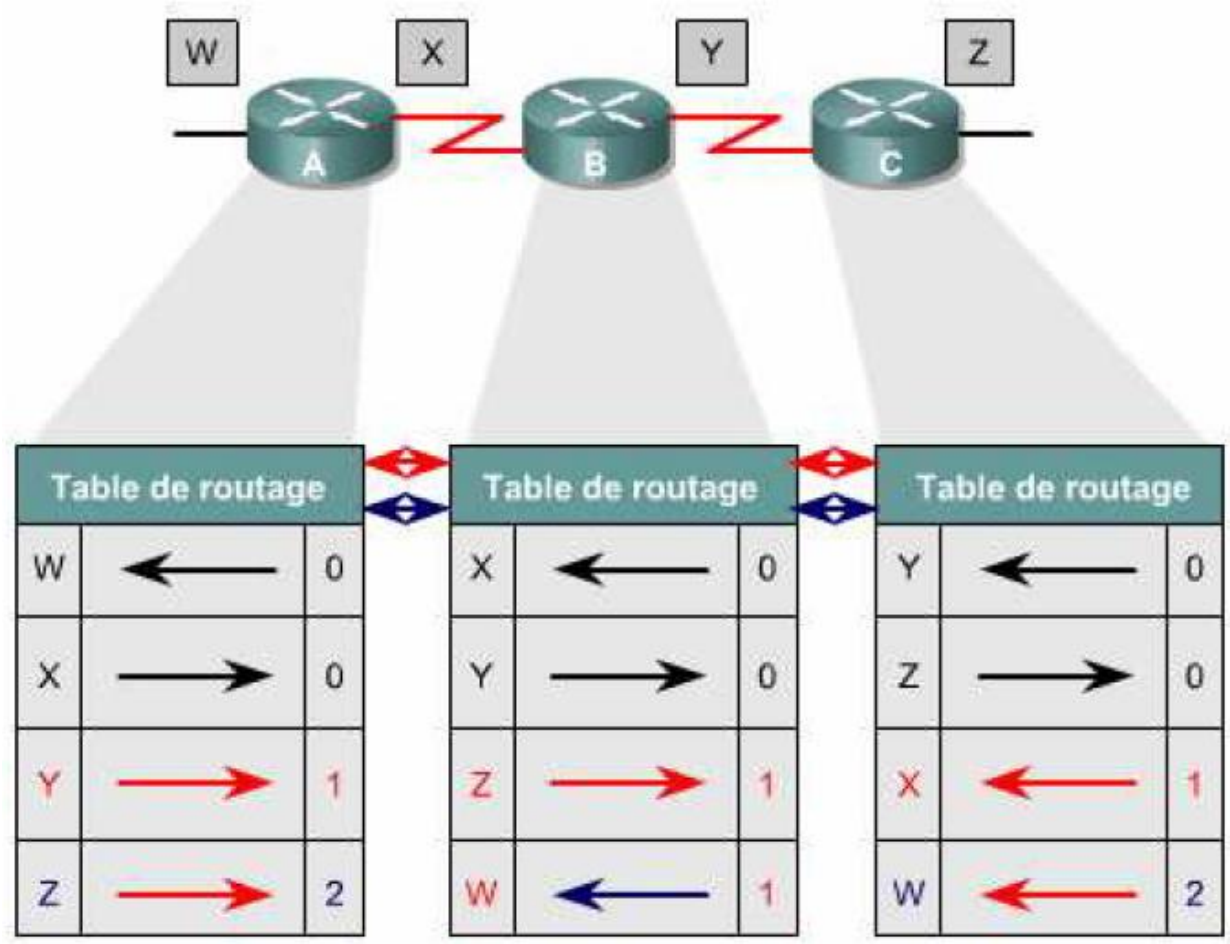
Fonctions du protocole de routage à vecteur de distance

Les algorithmes de routage à vecteur de distance (algorithmes Bellman-Ford) transmettent régulièrement des copies de table de routage d'un routeur à l'autre.
Chaque routeur reçoit l'intégralité des tables de routage des routeurs voisins auxquels il est directement connecté.



Envoi périodique de copies d'une table de routage aux routeurs voisins et cumul des vecteurs de distance.

L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau.
Chaque routeur voit uniquement ses voisins (ne connait pas la topologie exacte).
La distance entre l'interface et chaque réseau directement connecté est égale à **0**.



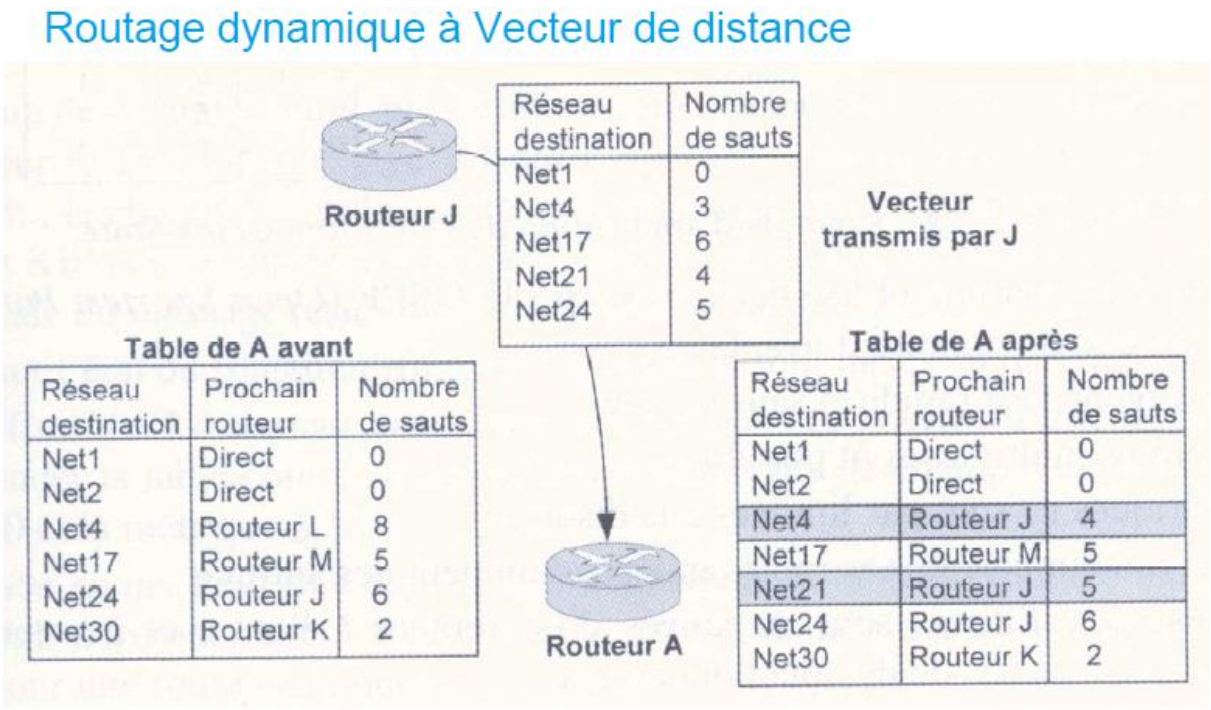
Cet algorithme se base sur le principe que chaque routeur dispose d'une table de routage indiquant, pour chaque réseau de destination, l'interface locale permettant de l'atteindre et la meilleure distance qui lui est associée.

Le coût total d'un chemin est alors calculé en sommant les coûts des sauts qui le composent, et ces coûts estimés sont régulièrement envoyés aux routeurs voisins afin qu'à leur tour ils mettent à jour leur table.
A l'initialisation, un routeur n'a qu'une connaissance très limitée du réseau : sa table de routage de contient que les réseaux auxquels il est directement connecté.
Il va ensuite envoyer le contenu de sa table de routage à ses voisins, qui pourront mettre à jour leur propre table en se basant sur les coûts indiqués par l'émetteur.
Pour avoir leur propre estimation du coût, il leur suffit de sommer le coût estimé par le routeur émetteur avec le coût pour atteindre ce dernier. La mise à jour effectuée, ils émettent à leur tour leur table, à destination de leurs autres voisins, …
Au fur et à mesure de la progression dans le réseau, chaque routeur finit par connaître l'existence des réseaux auxquels il n'est pas connecté, mais que ses voisins sont capables d'atteindre, en se basant eux mêmes sur d'autres routeurs, ...

Par exemple, supposons qu'un **routeur K** possède dans **sa table de routage la destination X** avec **une distance d1**. Il envoie cette information à **son voisin J**, qui possèdent dans sa table

une entrée pour **K** avec **une distance d2**. **En sommant ces distances**, **J sait maintenant qu'il peut atteindre X en passant par K avec un coût de d1 + d2**. **Si J possède une autre entrée indiquant qu'il peut atteindre X par un autre voisin (L), mais avec un coût supérieur (d3), il en déduit qu'il a trouvé un chemin plus court le menant à X, et par conséquent il met à jour sa table en remplaçant le triplet (X, L, d3) par (X, K, d1 + d2).** En envoyant régulièrement le contenu de la table de routage, **et en effectuant une mise à jour des entrées uniquement lorsqu'un nouveau coût est inférieur à l'ancien, cet algorithme permet de découvrir la distance la plus courte pour atteindre un réseau.**

Cependant certains défauts doivent être mis en évidence, et notamment le manque de réactivité lors du changement de topologie du réseau (panne d'un routeur par exemple).



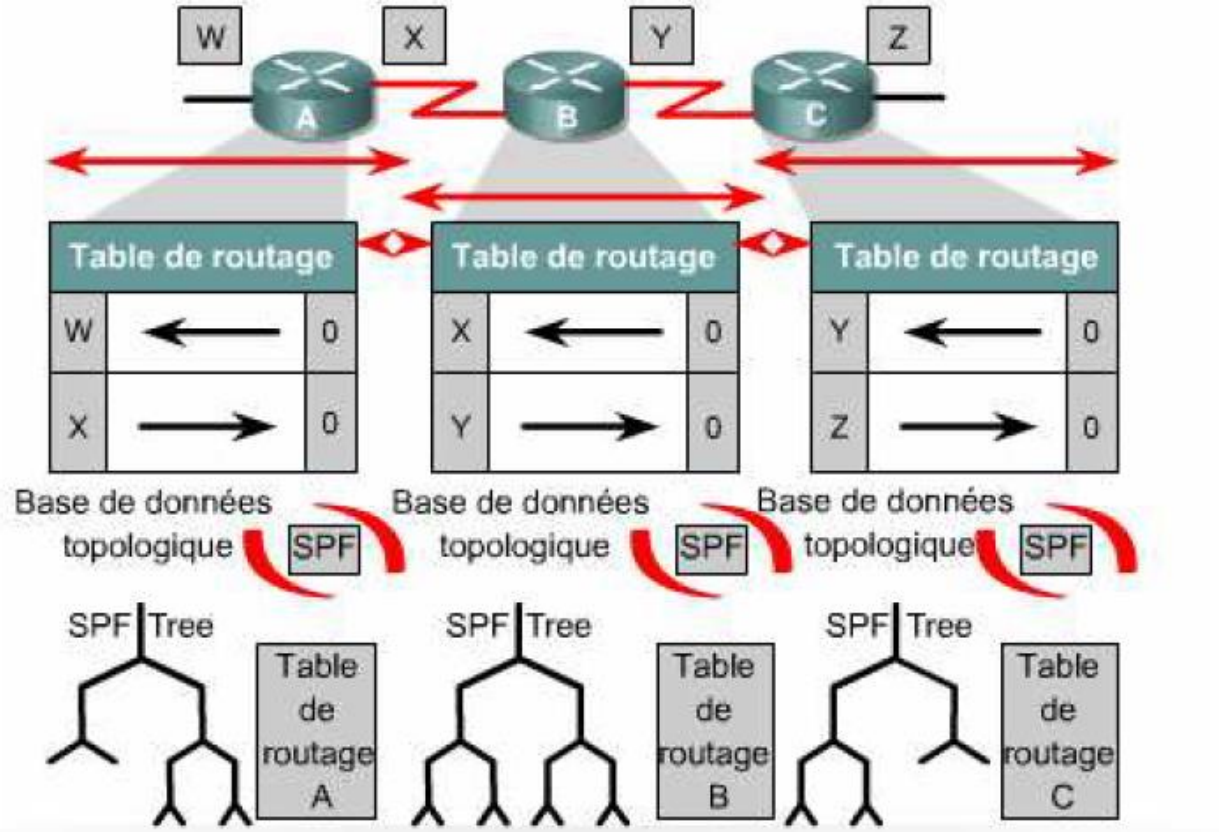
L'entrée pour atteindre le réseau 4 est modifiée car le routeur J connaît une route plus courte. Le nombre de saut transmis est de 3, le routeur A ajoute 1 saut pour aller jusqu'à J.

Fonctions du protocole de routage à état de liens

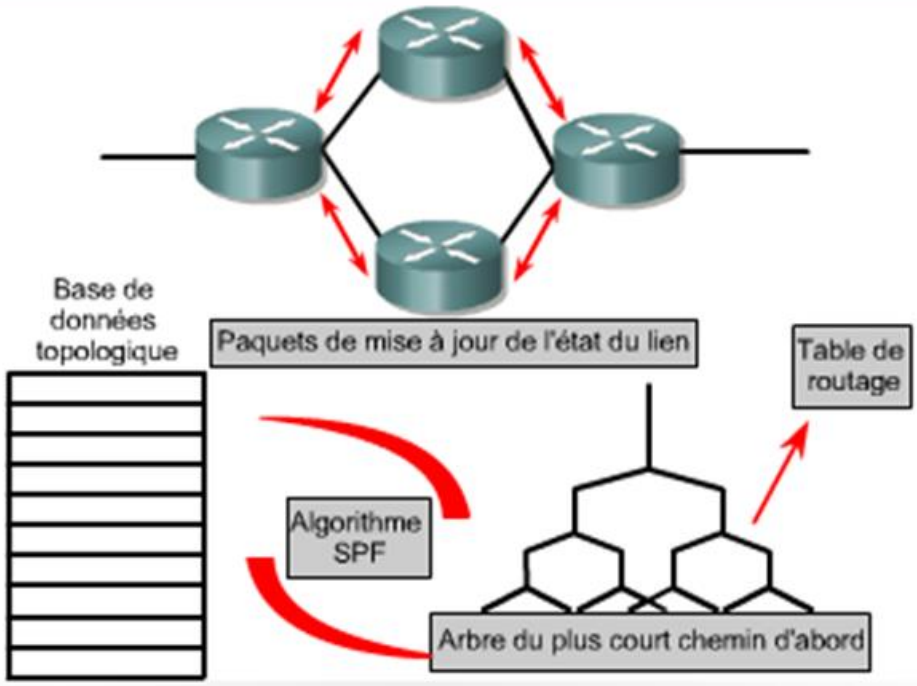
Les algorithmes à état de liens (algorithme de Dijkstra ou algorithme SPF) gèrent une base de données complexe d'informations topologiques (complète sur les routeurs distants et leurs interconnexions).

Le routage à état de liens utilise les éléments suivants :

- ***Mises à jour de routage à état de liens (LSA)*** **–** un petit paquet d'informations de routage qui est transmis entre les routeurs.
- ***Base de données topologique*** **–** un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liens.
- ***Algorithme SPF*** **–** L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.
- ***Tables de routage*** **–** Une liste des chemins et des interfaces connus.



Chaque routeur dispose de sa propre base de données topologique sur laquelle l'algorithme SPF est exécuté.



Les routeurs envoient des LSA à leurs voisins. Les LSA sont utilisées pour créer une base de données topologique. L'algorithme SPF est utilisé pour calculer l'arbre du plus court chemin d'abord dans lequel la racine est le routeur lui même. Une table de routage est ensuite créée.

Protocole de routage par État des liens

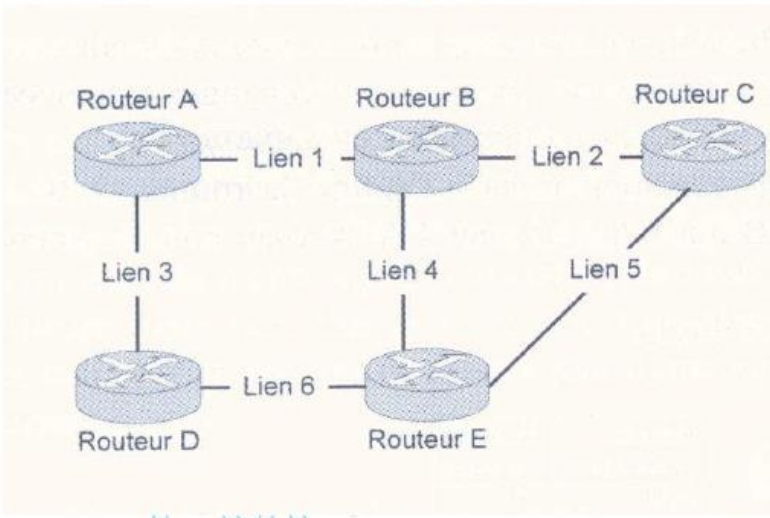


Table des liens

De	à	Lien	Distance
A	B	1	1
A	D	3	1
B	A	1	1
B	C	2	1
B	E	4	1
C	B	2	1
C	E	1	1
D	A	3	1
D	E	6	1
E	B	4	1
E	C	5	1
E	D	6	1

Tous les routeurs possèdent à un instant donné, la même table des liens. Si le routeur A veut envoyer un paquet vers le routeur C, il calcule le plus court chemin vers C et sélectionne le routeur B pour lui envoyer le paquet. B trouve à son tour le plus court chemin vers C qui est direct.

Dans ce type d'algorithme, chaque routeur tient à jour une base de données décrivant la topologie entière du réseau, c'est à dire l'ensemble des routeurs, et leur interconnexion. Pour calculer la distance qui le sépare d'une destination, chaque routeur construit un arbre dont il est la racine, et suit au fur et à mesure toutes les ramifications du réseau tant qu'il n'a pas atteint la destination finale.
Le calcul de cet arbre permet de connaître le chemin complet (c'est à dire tous les routeurs que le paquet devra traverser), **cependant seule l'adresse du prochain saut est conservée par le routeur puisque de son point de vue, c'est la seule information utile. Lorsqu'un lien change d'état, le routeur qui le détecte transmet cette information à tous ses voisins par un mécanisme d'inondation**. Chaque routeur recevant cette information met à jour sa base de donnée, et s'il s'agit d'une information nouvelle (en d'autres termes, s'il n'a pas déjà reçu cette information), il réémet le message d'information à tous ses voisins. Ce mécanisme permet à tous les routeurs d'être informé rapidement de toute modification, tout en assurant que le message soit détruit dès que tous l'ont reçu.

Le principal problème de cet algorithme est le coût, en termes de capacité de calcul et de mémoire, demandé par l'élaboration de l'arbre. En effet, à chaque changement de topologie, chaque routeur doit à nouveau dérouler le même algorithme, et calculer le plus court chemin pour atteindre chaque destination présente dans sa base de données.

Considérations relatives au routage à état de liens:

- Surcharge du système (Processeurs)
- Mémoire requise.
- Consommation de bande passante

Vue d'ensemble des protocoles de routage :

Les protocoles suivants sont des exemples de protocoles de routage IP :

1- **Le protocole RIP** (Routing Internet Protocol) :

- un protocole de routage à **vecteur de distance.**
- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

Pour accélérer la convergence de l'algorithme, si un routeur modifie sa table de routage, il n'attend pas l'expiration de son temporisateur pour envoyer le contenu de sa table : il l'émet immédiatement à tous ses voisins.

La simplicité et **les performances** de RIP font qu'il est encore largement utilisé aujourd'hui.

2- **Le protocole OSPF** (Open Shortest Path First)

- un protocole de routage à **état de liens**.
- Il utilise l'algorithme SPF ou l'algorithme de Dijkstra pour calculer le coût le plus bas vers une destination.
- Les mises à jour du routage sont diffusées à mesure des modifications de topologie.

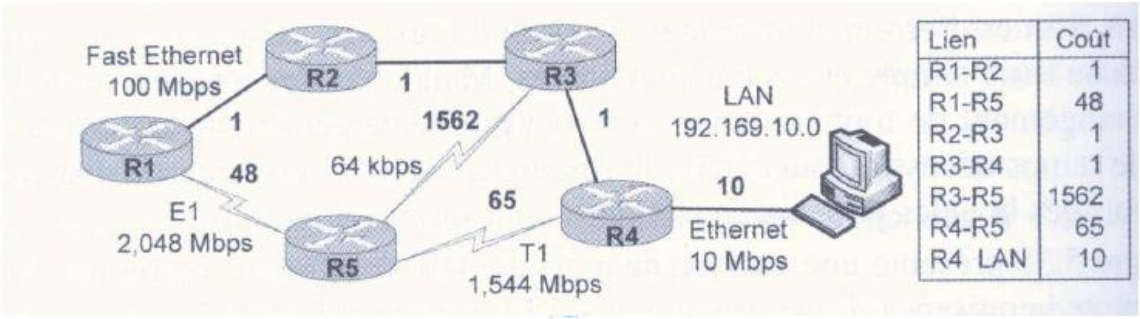
Le protocole Hello permet à chaque routeur d'échanger des informations concernant l'état de leurs liens, et de vérifier que les liaisons sont opérationnelles.

Deux mécanismes sont utilisés pour détecter les changements d'état de lien :

- Les changements d'état d'interface. Ces changements sont détectés localement par le système d'exploitation du routeur.
- L'expiration du temporisateur pour un paquet Hello, indiquant qu'un voisin est inactif.

La détection d'un changement de topologie est suivie par l'inondation, sur toutes les interfaces, d'un paquet indiquant cette information. Chaque routeur met à jour sa base de donnée et recalcule le plus court chemin pour chaque destination.

Présentation du protocole OSPF à État des liens

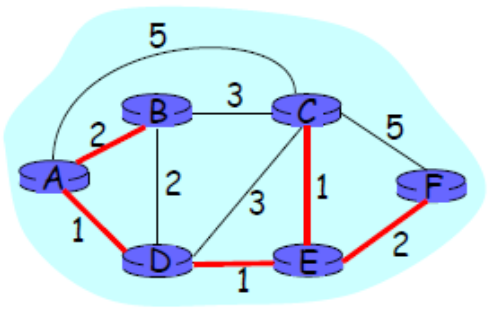


Lien	Coût
R1-R2	1
R1-R5	48
R2-R3	1
R3-R4	1
R3-R5	1562
R4-R5	65
R4 LAN	10

Exemple de coût dans OSPF – Le métrique choisit est le débit.
Suivant la table des liens et les coûts associés, la route OSPF passera par R2, R3, et R4 avec un coût total de 13.

Algorithme de Dijkstra : exemple

étapes	start N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
→ 0	A	2,A	5,A	1,A	inf	inf
→ 1	AD	2,A	4,D		2,D	inf
→ 2	ADE	2,A	3,E			4,E
→ 3	ADEB		3,E			4,E
→ 4	ADEBC					4,E
5	ADEBCF					



Notation :

- c(i,j) : coût du lien de i à j. Est infini si *i* et *j* ne sont pas voisins
- D(v) : Valeur courante du coût du chemin de la source à la destination V
- p(v) : noeud précédant v dans le chemin de la source à v
- N : Ensemble des nœuds dont on connaît le coût minimal

3- Le protocole IGRP (Interior Gateway Routing Protocol)

- un protocole propriétaire développée par Cisco.
- un protocole de routage à vecteur de distance.
- La bande passante, la charge, le délai et la fiabilité (une métrique composite).
- Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes.

4- Le protocole EIGRP (Enhanced IGRP)

- un protocole de routage à vecteur de distance amélioré (Cisco).

5- **Le protocole BGP** (Border Gateway Protocol)

Résumé - Protocoles de routage

Protocole	Algorithme	Métrique	Mise à jour
RIP v1	Vecteur de distance	Nombre de sauts	30 sec
RIP v2	Vecteur de distance	Nombre de sauts	30 sec
IGRP	Vecteur de distance	Délais Bande passante Fiabilité	90 sec
OSPF	État de lien	Le coût de la route	changement topologique
IS - IS	État de lien	Poids du lien	changement topologique
EIGRP	Hybride	Délais Bande passante Fiabilité	Changement topologique
BGP	Vecteurs de chemins	Politique réseau Attribut de chemin	

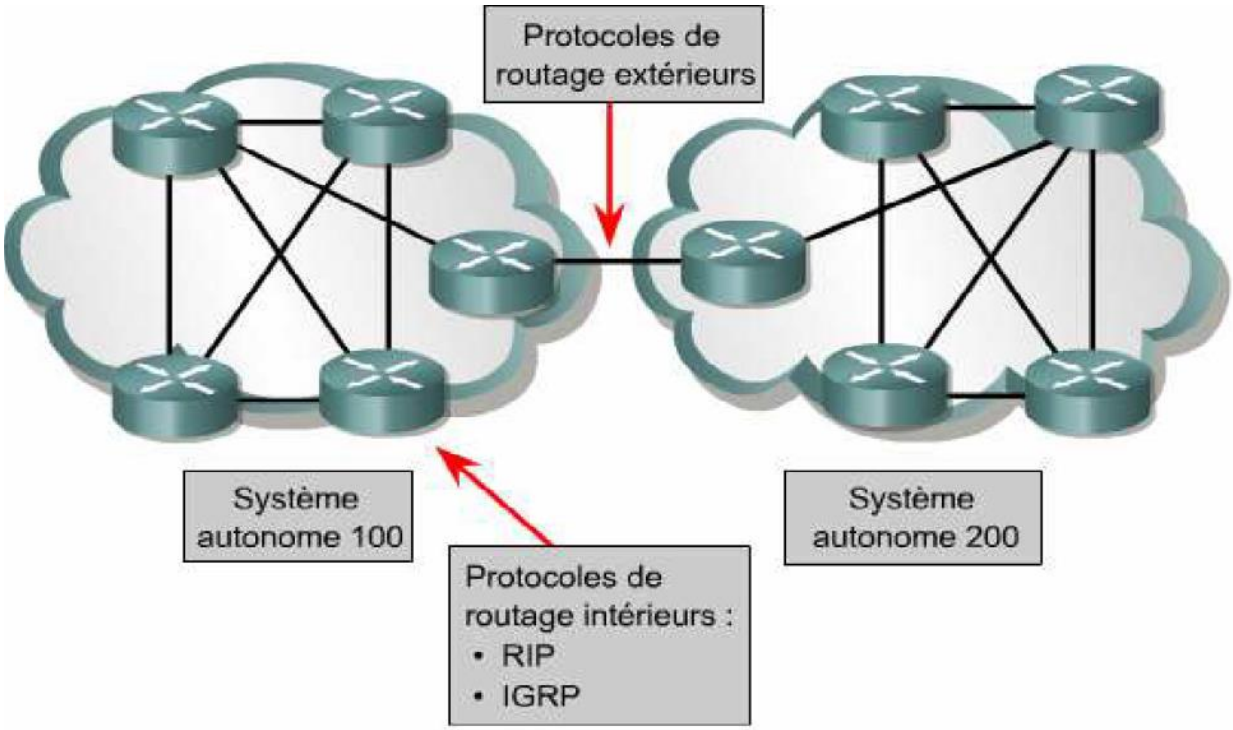
Protocole IGP & EGP :

IGP : Protocoles utilisés à l'intérieur d'un Système autonome.
EGP : Protocoles utilisés entre les Systèmes autonomes.

Systèmes autonomes :

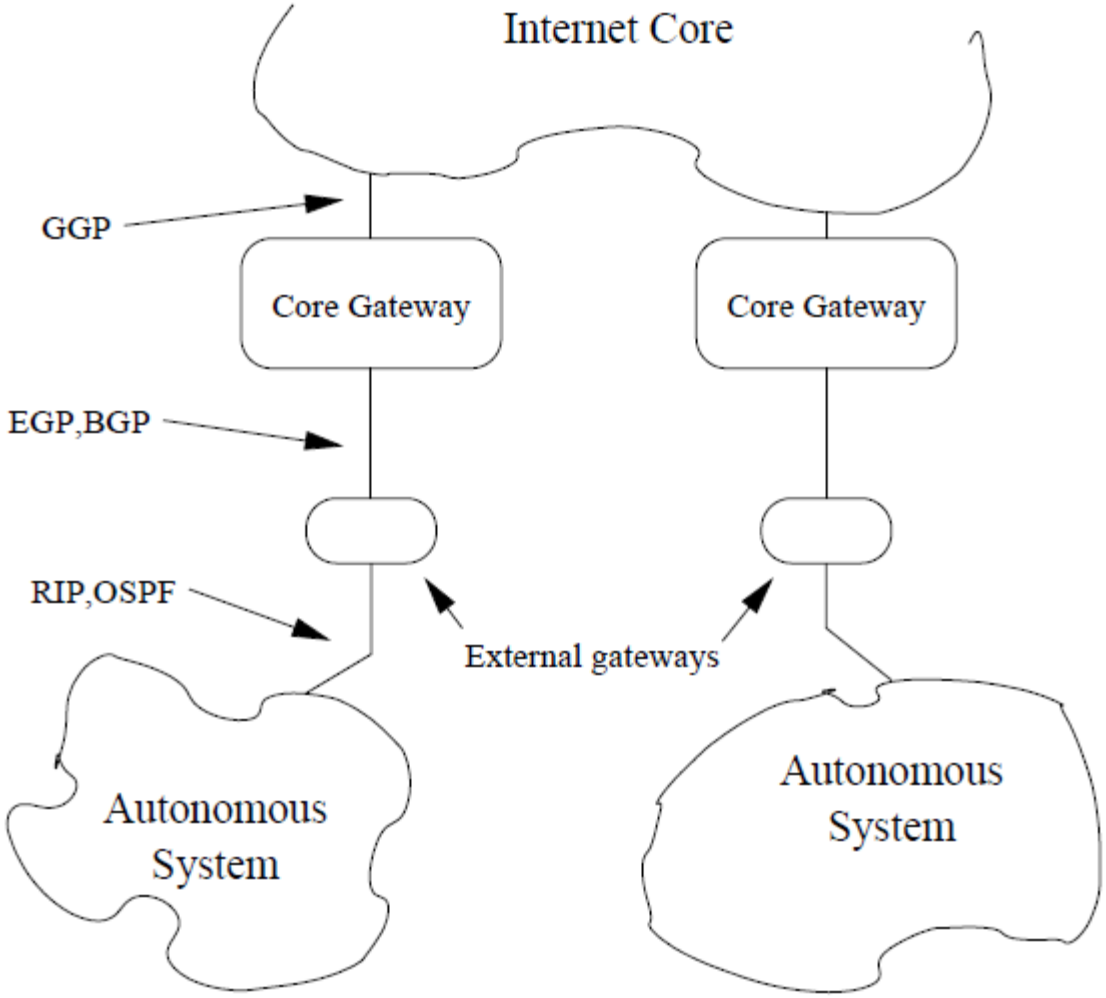
<u>Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune.</u>

Les systèmes autonomes (AS) assurent la division de l'interréseau global en réseaux plus petits et plus faciles à gérer L'InterNIC (Internet Network Information Center), un fournisseur de services ou encore un administrateur attribue un numéro d'identification à chaque système autonome. Ce numéro est un nombre à 16 bits (vitale pour la configuration d'IGRP).



Schématiquement on peut imaginer l'Internet comme une hiérarchie de routeurs. Les routeurs principaux (" core gateways ") de cette architecture utilisent entres-eux des protocoles comme **GGP** (" Gateway to Gateway Protocol "), l'ensemble de ces routeurs forment ce que l'on nomme l'" Internet Core ".

En bordure de ces routeurs principaux se situent les routeurs qui marquent la frontière avec ce que l'on nomme les " Autonomous systems ", c'est à dire des systèmes de routeurs et de réseaux qui possèdent leurs mécanismes propres de propagation des routes. Le protocole utilisé par ces routeurs limitrophes est souvent **EGP** (" Exterior Gateway Protocol ") ou **BGP** (" Border Gateway Protocol ").



Au sein d'un système autonome on utilise un IGP (" Interior Gateway Protocol ") c'est à dire un " protocole de gateways intérieurs ". Les protocoles les plus couramment employés sont **RIP** (" Routing Information Protocol ") qui est simple `a comprendre et `a utiliser, ou encore **OSPF** (" Open Shortest Path First ") plus récent, plus capable mais aussi beaucoup plus complexe à comprendre dans son mode de fonctionnement.

Configuration de routage dynamique :

Router **{protocole} {option} :** pour lancer le processus de routage (mode config globale)

Network **{adresse réseau directement connectée} :** permet de déterminer les interfaces qui participeront à l'envoi et à la réception des mises à jour du routage.

Exemple :

```
Router(config)#router rip
Roouter(config-router)#network 172.16.0.0
```

Contrôle de congestion

Dégradation des performances du réseau si le nombre de paquets circulant atteint la capacité limite admissible.

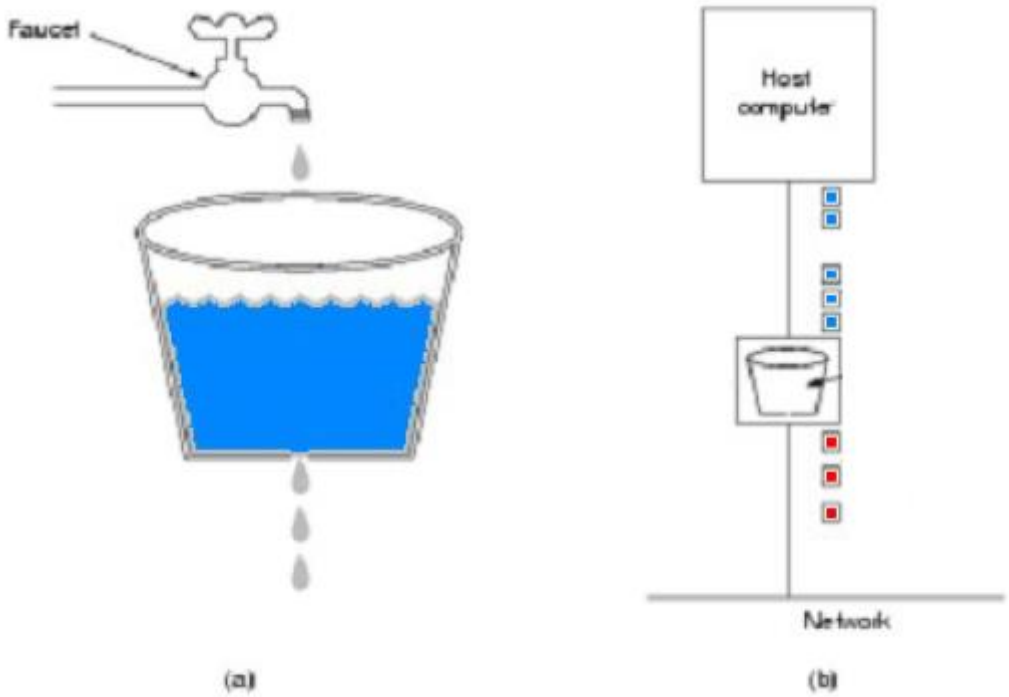
Solutions

– ***Préventives*** :
• Contrôler le nombre de paquets entrant par unité de temps dans le réseau.
– ***Correctives*** :
• Ralentir les émissions en avertissant les stations émettrices.

Congestion : Algorithme du seau percé :

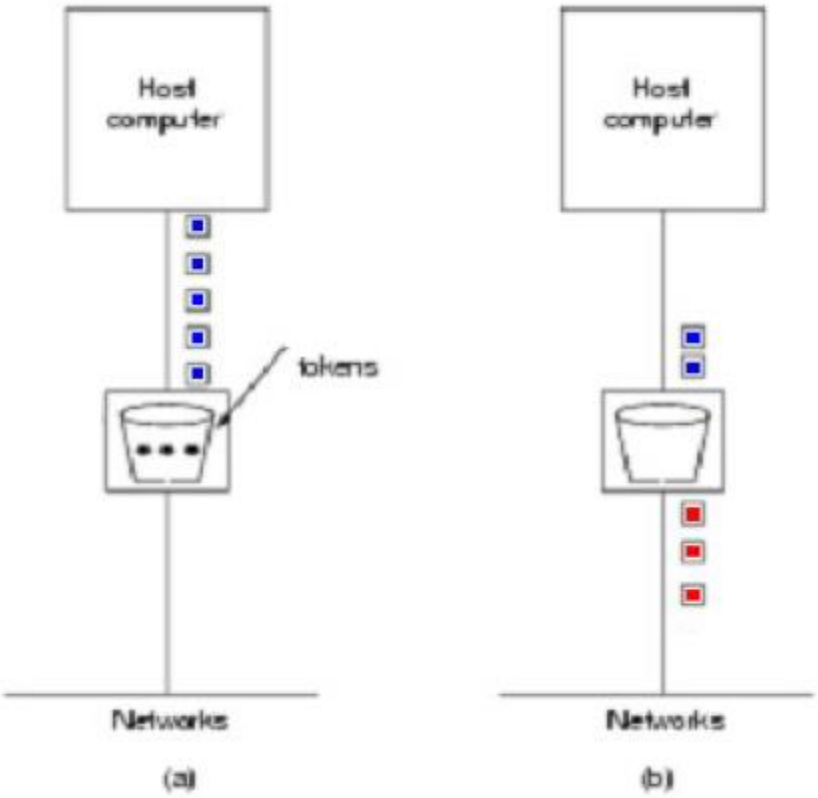
- Éviter les surprises: **réguler** le trafic **entrant** dans le réseau
- Serveur avec **un temps** de service constant
- La file d'attente du serveur est de taille limitée

Possibilité de perdre des paquets



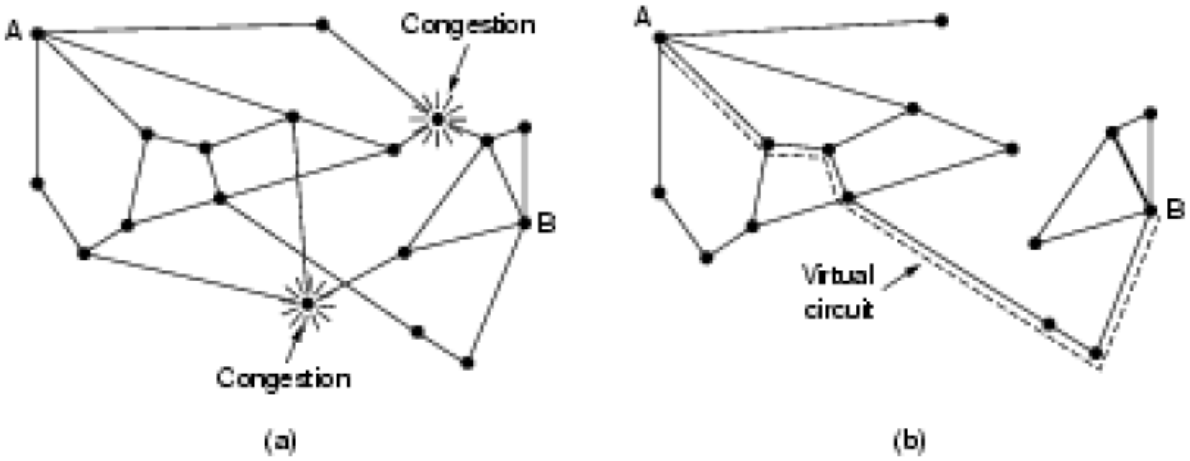
Congestion : Algorithme du seau percé à jetons

- Introduire plus de flexibilité par rapport à l'algorithme précédent
- Périodiquement, un nouveau **jeton** est généré
- **k** paquets arrivent et disposent de **i** jetons
  *Si k < ou = i, transmettre k paquets
  *Sinon transmettre i paquets (k-i restent dans le file d'attente).



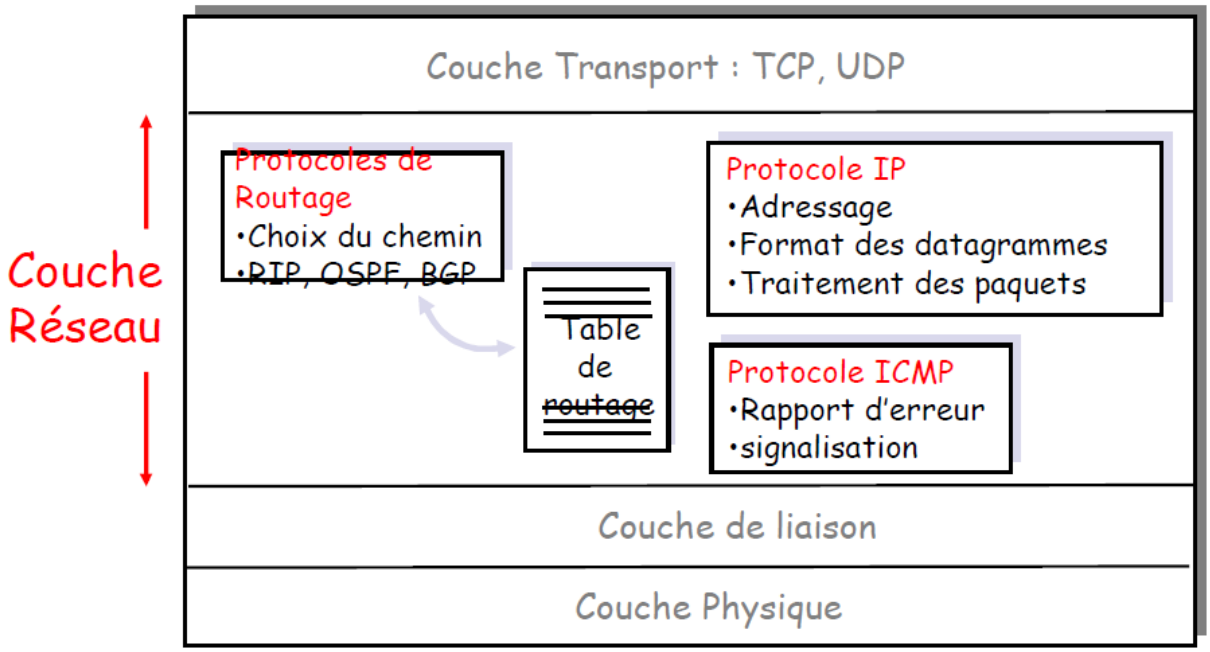
Congestion : Circuit virtuel

- Avant d'établir un circuit, s'assurer qu'il n'y aura pas de congestion
- Choisir des routes non congestionnées.
- Refuser l'établissement de circuit, si cela n'est pas possible



Congestion : Technique des paquets d'engorgement

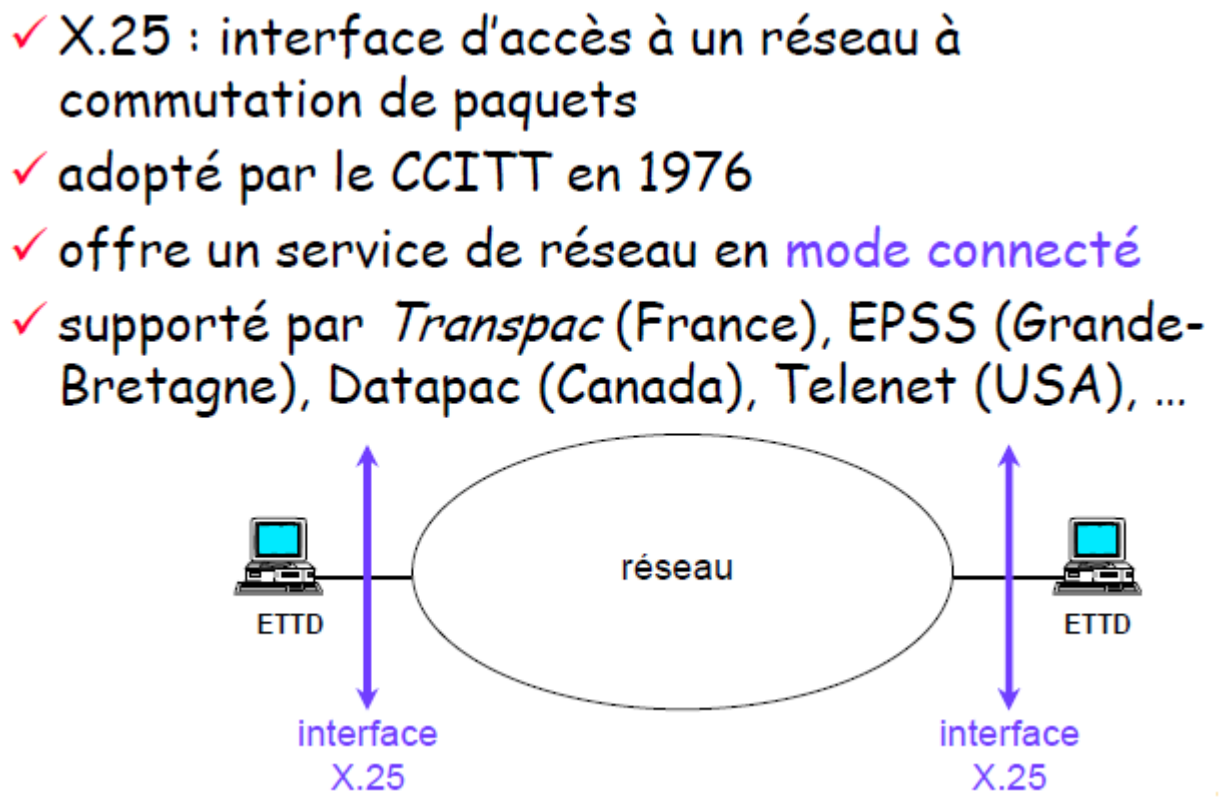
- Envoyer des paquets d'engorgement aux émetteurs quand les performances du réseau commencent à se dégrader.
- Si les files d'attentes de sorties du routeur commencent à saturer, celui-ci envoie des paquets d'engorgement aux émetteurs.
- Les émetteurs sont supposés être coopératifs



Présentation de X.25

X.25 est un protocole de communication normalisé par commutation de paquets en mode point à point offrant de nombreux services[1]. Son abandon par Transpac est prévu pour le 30 septembre 2011[2]. Finalement la date officielle de son arrêt par Orange France Telecom a été repoussée du 30 septembre 2011 au 30 juin 2012.

X.25 définit l'interface entre un ETTD (Équipement terminal de traitement de données) et un ETCD (Équipement terminal de circuit de données) pour la transmission de paquets. Elle fixe donc les règles de fonctionnement entre un usager du réseau et le réseau lui-même.

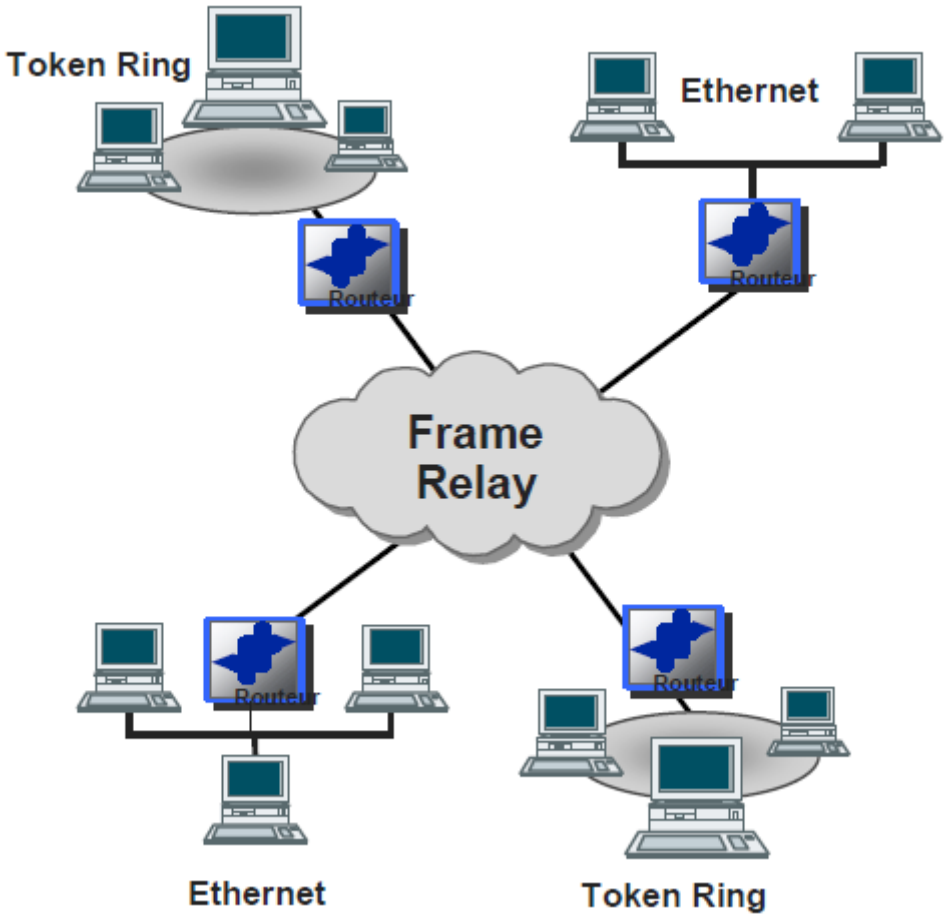


X.25 est une technologie vieillissante qui tend à disparaître. Le protocole X.25 est encore utilisé dans des réseaux tels que le réseau de la navigation aérienne, dans le protocole radio AX.25 (utilisé par les radioamateurs, et notamment pour l'APRS), ainsi que dans beaucoup d'établissements bancaires (protocole ETEBAC) notamment pour les échanges bancaires avec leurs clients et pour gérer les guichets automatiques bancaires. Cette norme a l'avantage d'être sûre à 100% (il n'y a aucune perte de données grâce aux nombreux contrôles et aux éventuelles retransmissions d'éléments perdus).

Relais de Trames ou Frame Relay :

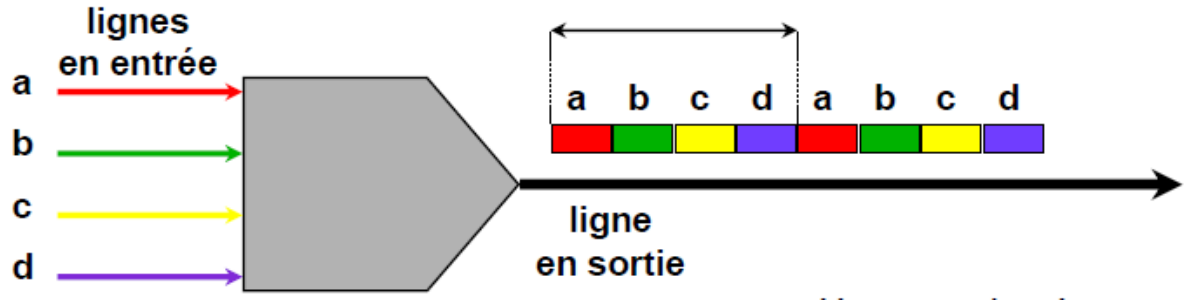
Le relayage de trames (ou FR, pour l'anglais Frame Relay) est un protocole à commutation de paquets situé au niveau de la couche de liaison(niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN) il a été inventé par Eric Scace, ingénieur chez Sprint International.

Le FR sert surtout à router des protocoles des réseaux LAN ("Local Area Network" - des réseaux à petite superficie comme Ethernet, Token-Ring) sur des plus grandes surfaces. Par exemple, il pourra servir à connecter deux réseaux IPX qui sont distants géographiquement. À l'interne des réseaux, le protocole utilisé sera donc IPX mais FR servira pour véhiculer les données entre les réseaux.



ATM

Asynchronous Transfer Mode ou **ATM** (traduit en français par « Mode de transfert asynchrone ») est un protocole réseau de niveau 2 à commutation de cellules, qui a pour objectif de multiplexer différents flots de données sur un même lien utilisant une technique de type TDM ou MRT (multiplexage à répartition dans le temps).



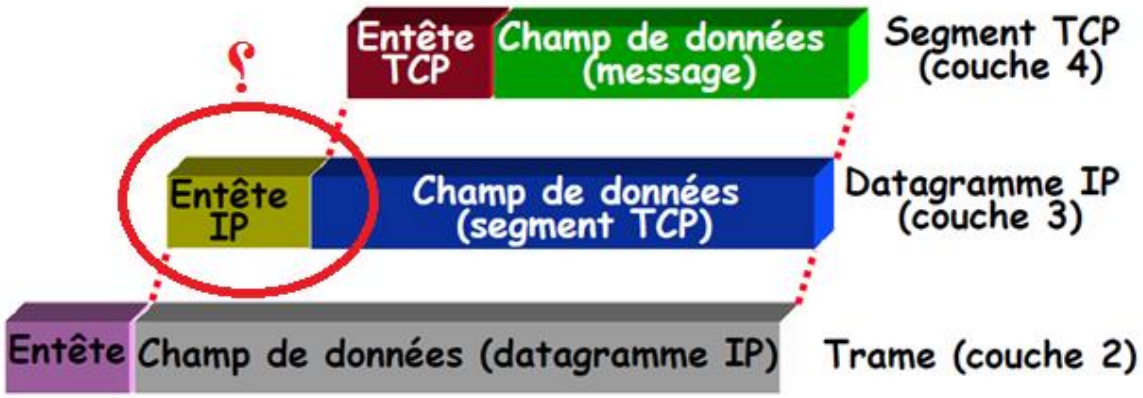
Les cellules ATM sont des segments de données de taille fixe de 53 octets (48 octets de charge utile et 5 octets d'en-tête), à la différence de paquets de longueur variable, utilisés dans des protocoles du type IP ou Ethernet.

La commutation des cellules allie la simplicité de la commutation de circuits et la flexibilité de la commutation de paquets. Un circuit virtuel est établi soit par configuration des équipements, soit par signalisation, et l'ensemble des cellules seront commutées sur ce même circuit virtuel par commutation de labels. En particulier, le chemin utilisé dans le réseau ne varie pas au cours du temps puisqu'il est déterminé lors de l'établissement du circuit virtuel.

Les labels permettant la commutation des cellules sont portés dans l'en-tête de chaque cellule.

Internet Protocol (abrégé en IP) est une famille de protocoles de communication de réseau informatique conçus pour être utilisés par Internet. Les protocoles IP sont au niveau 3 dans le modèle OSI. Les protocoles IP permettent un service d'adressage unique pour l'ensemble des terminaux connectés.

Lors d'une communication entre deux postes, le flux de données provenant de la couche transport — niveau 4 du modèle OSI — (par exemple des segments TCP) est encapsulé dans des paquets par le protocole IP lors de leur passage au niveau de la couche réseau. Ces paquets sont ensuite transmis à la couche de liaison de données — niveau 2 du modèle OSI — afin d'y être encapsulés dans des trames (par exempleEthernet).



Les protocoles IP assurent l'acheminement au mieux (best-effort delivery) des paquets. Ils ne se préoccupent pas du contenu des paquets, mais fournissent une méthode pour les mener à destination.

Fiabilité :

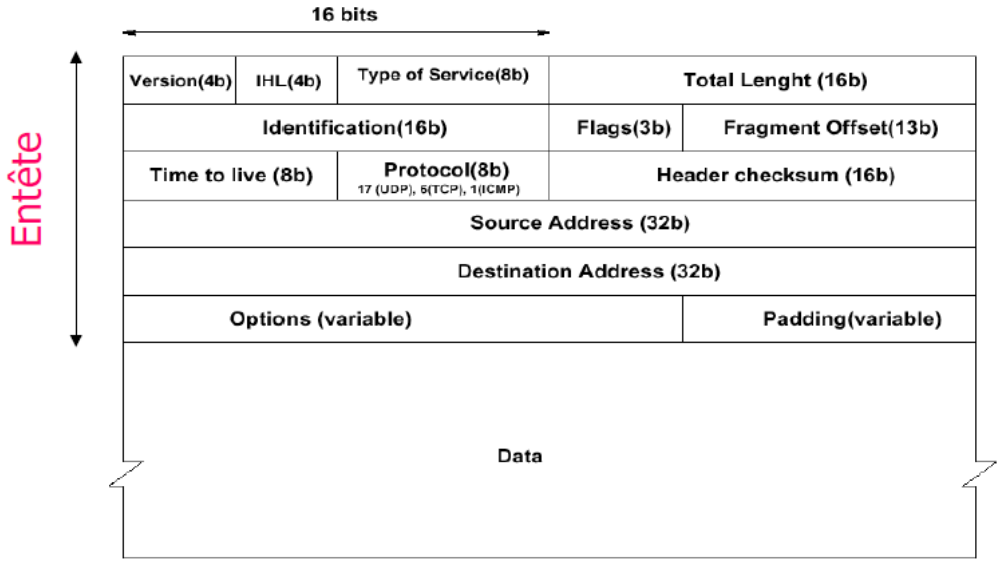
Les protocoles IP sont considérés comme « non fiables ». Cela ne signifie pas qu'ils n'envoient pas correctement les données sur le réseau, mais qu'ils n'offrent aucune garantie pour les paquets envoyés sur les points suivants :

- corruption de données ;
- ordre d'arrivée des paquets (un paquet A peut être envoyé avant un paquet B, mais le paquet B peut arriver avant le paquet A) ;
- perte ou destruction de paquet ;
- duplication des paquets.

Les garanties qu'un protocole IP n'offre pas sont déléguées aux protocoles de niveau supérieur. **La raison principale de cette absence de gestion de la fiabilité est la volonté de réduire le niveau de complexité des routeurs et ainsi de leur permettre de disposer d'une plus grande rapidité.** L'intelligence est alors déportée vers les points d'extrémité du réseau.

Protocole IP V4 Datagramme

Datagramme: Unité de données échangée par des entités IP



Description

Version :
Indique la version IP (IPv4, IPv6) du datagramme

Internet Header Lenght (IHL) :
Longueur de l'entête multiple de mots de 32 bits (au moins 5 mots)

Type of Service (TOS) : Type de service souhaité

0 1 2	3	4	5	6	7
priorité	D	T	R	C	inutilisé

Priorité: de 0 à 7
0: priorité normale (valeur par défaut)
7: priorité maximale (pour la supervision du réseau)

- D=1 : minimiser le délai d'acheminement
- T=1 : maximiser le débit de transmission
- R=1 : assurer une plus grande fiabilité
- C=1 : minimiser les coûts de transmission

Total length : Longueur (en octets) du fragment IP incluant l'entête
Espace réservé pour ce champ : 2 octets; longueur ≤ 65535

IDENTIFICATION, FLAGS et FRAGMENT OFFSET Ces mots sont prévus pour contrôler la fragmentation des datagrammes. Les données sont fragmentées car les datagrammes peuvent avoir à traverser des réseaux avec des MTU plus petits que celui du premier support physique employé.

Checksum : Code détecteur d'erreur (ne s'applique qu'à l'entête)

Time to live : Durée de vie restante (nombre de routeurs à traverser)
Initialisée à N par la station émettrice, décrémenté d 'une unité par le routeur récepteur.

➢ **Comment éviter qu 'un datagramme ne séjourne indéfiniment dans un internet ?**
Un routeur qui reçoit un datagramme de TTL nul, détruit ce dernier et avertit l'expéditeur à l 'aide d 'un message ICMP.

Protocol :
Identification du protocole client (IP →4, 17→ UDP, 6 → TCP, 1 → ICMP):
Permet de remettre (démultiplixer) les données au protocole adéquat.

Options :
Sécurité, enregistrement de route, horaire, routage strict, ...

Padding :
Bourrage pour compléter l 'en-tête. (permet à l'entête d 'occuper un nombre entier de mots de 32 bits).

En conclusion partielle que peut-on dire du travail de la couche IP ?

1. Il consiste à router les datagrammes en les acheminant " au mieux ", C'est son travail principal.
2. Il peut avoir à fragmenter les données de taille supérieure au MTU du support physique à employer.

Fragmentation IP – MTU

La couche de liaison (Couche 2 " Link ") impose une taille limite, le " **M**aximum **T**ransfer **U**nit ". Par exemple cette valeur est de 1500 pour une trame Ethernet…
Dans ces conditions, si la couche IP doit transmettre un bloc de données de taille supérieure au MTU à employer, il y a fragmentation !