Chapitre 2

Routage intra et inter-domaines

Pour pouvoir échanger des informations entre les utilisateurs de plusieurs réseaux locaux, les entités intermédiaires jouent un rôle capital. Elles doivent contenir les moyens nécessaires à l'acheminement des informations entre deux stations quelconques dans le réseaux. Ces moyens sont situés, selon le modèle OSI, au niveau de la couche 3 : la couche réseaux.

La couche réseaux est appelée, donc, à fournir les procédures et les moyens fonctionnels nécessaires à l'échange des informations données par la couche transport. C'est un service de bout en bout qui est responsable de l'acheminement des paquets de données qui peuvent traverser plusieurs nœuds intermédiaires. Le paquet est l'unité de transport de données dans la couche réseaux.

Cette couche est surtout nécessaire dans les réseaux maillés où les paquets doivent traverser plusieurs nœuds avant d'arriver à, leurs destinations ; elle n'est pas prise en compte dans les réseaux constitués par une seule liaison. Les caractéristiques de cette couche ont été déterminées par la réalisation effective de réseaux d'ordinateurs généraux (Internet).

Le rôle de la couche réseau est de transporter d'une extrémité à l'autre du réseau des blocs de données provenant d'une fragmentation des messages du niveau supérieur, le niveau transport.

Pour pouvoir échanger des informations entre deux entités communicantes quelconques à travers un ou plusieurs réseaux, de nombreux services sont fournis par la couche réseau :

1. **Commutation :** pour mettre en relation les deux correspondants.
2. **Adressage et nommage :** pour identifier et localiser chaque correspondant de manière unique sur le réseau.
3. **Routage :** pour acheminer les blocs d'information vers le destinataire.

4. **Segmentation :** pour adapter la taille des unités de données transférées aux capacités du réseau.
5. **Contrôle de congestion :** pour contrôler le trafic admis dans le réseau pour empêcher son effondrement.

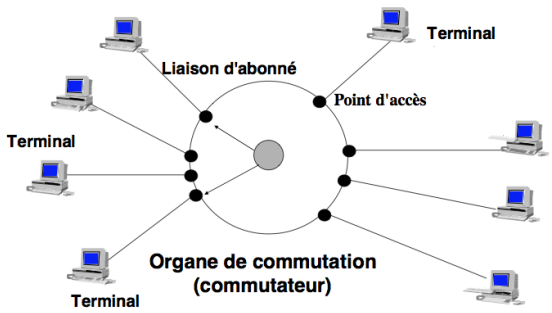
En plus de ces grands services, la couche réseau assure l'intégrité du transport des paquets. Pour ce faire, il est nécessaire de définir un format de paquet et de se donner des moyens pour détecter les erreurs.

Des services facultatifs peuvent être rendus par la couche réseau. Par exemple, la livraison en séquence des paquets reçus par la couche transport, le transfert accéléré de paquets de supervision, le multiplexage de connexions réseau... etc.

La commutation (vue dans le chapitre précédent) est une tâche de base de la couche réseaux, elle peut être de circuit de message ou de paquet. Dans le dernier cas, souvent utilisé, les paquets peuvent être transférés en mode connecté ou non connecté

2.1 Commutation

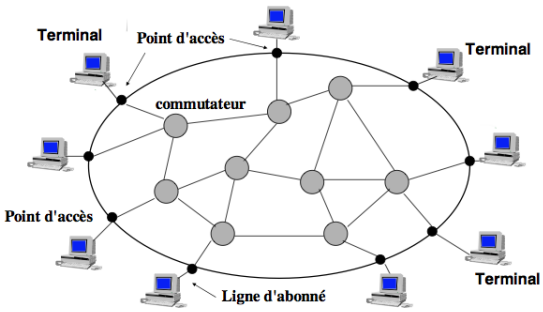
La commutation consiste à mettre en relation de façon temporaire 2 points de connexion, créant ainsi une liaison temporaire entre les 2 terminaux connectés. L'organe de commutation s'appelle un commutateur. Cette solution résout le problème du nombre de lignes d'abonnés (une ligne par abonné). Par contre, si le commutateur est unique, les lignes d'abonnés doivent être très longues, et de plus, à un instant, seuls 2 abonnés peuvent être connectés.



Pour résoudre ce problème, il faut rapprocher les points de connexion des abonnés, offrir la possibilité de construire des chemins multiples entre les points de connexion : il faut créer un maillage entre des commutateurs, c'est à dire un réseau de commutation.

2.1.1 Réseaux de commutation

Les terminaux sont reliés au réseau de commutation par une ligne d'abonné locale (courte). Plusieurs liaisons peuvent être établies simultanément. Plusieurs terminaux peuvent accéder au réseau de commutation par le même point d'accès (non représenté sur le schéma). Les commutateurs réalisent une fonction d'aiguillage et participent au routage des données, pour constituer des connexions entre les terminaux.



Dans ce contexte où la ressource est rare vis-à-vis de la demande potentielle (si simultanément tous les abonnés du réseau désiraient joindre un autre abonné...), il est indispensable de rechercher des techniques particulières pour optimiser le partage des ressources, c'est l'objectif des techniques de commutation.

2.1.2 Techniques de commutation

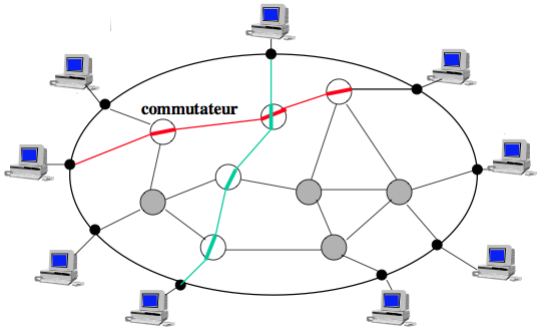
Selon la technique employée pour relier deux utilisateurs, on distingue la commutation de circuits, de messages ou de paquets.

2.1.2.1 La commutation de circuits

Elle est issue des techniques utilisées dans les réseaux téléphoniques (RTC). Elle se déroule en 3 phases :

1. **La connexion :** un chemin est établi entre l'appelant et l'appelé, par commutations successives. Les commutateurs ne remplissent qu'une fonction d'aiguillage. Tout se passe comme s'il n'y avait qu'une seule liaison entre les extrémités.
2. **Le transfert :** Les données (ou la voix) sont transmises de bout en bout sur le "circuit de données". Les ressources (lignes) sont attribuées en permanence, et en volume constant, pendant toute la durée de la communication (les "silences" sont pénalisés).

3. **La libération :** après le transfert, les ressources sont restituées au réseau de commutation, et sont disponibles pour d'autres communications.

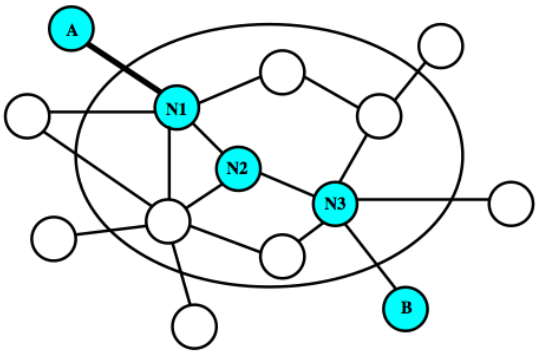


Cette technique soufre de trois inconvénients :

- Chevelure analogique (débit limité)
- Délais de connexion importants
- Signalisation indistincte des données, et mal adaptée

2.1.2.2 La commutation de message

Le principe est très différent de la commutation de circuits. Les données sont structurées en messages. Un message est une suite logique de données qui forment un tout (fichier, enregistrement ...).



Un message est acheminé vers sa destination au fur et à mesure des commutations :

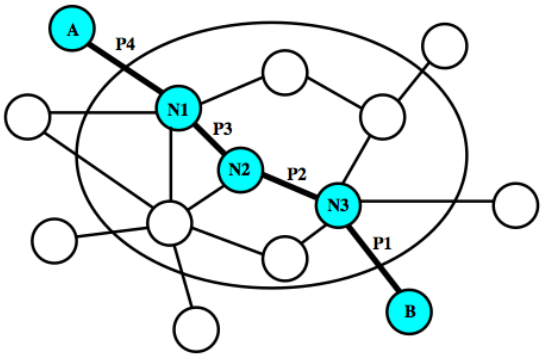
- Le message délivré par A est envoyé vers N1, où il est stocké et vérifié,
- La liaison A-N1 est libérée
- Il est transmis à N2, où il est stocké et vérifié,
- La liaison N1-N2 est libérée,
- Le processus est itératif jusqu'à la livraison du message à B

– Ainsi, les commutateurs (ou nœuds de commutation) sont dotés de mémoire et de capacité de traitement de données (leur fonction va au-delà d'un simple aiguillage).
– Quand un message est enregistré dans un nœud de commutation, la liaison par laquelle il est arrivé est libérée, et ses ressources sont disponibles pour le réseau de commutation.

L'avantage de cette technique est que sur le chemin AB, on n'utilise qu'une seule liaison de données à la fois, les autres étant disponibles pendant ce temps pour d'autres communications. Cependant, si la taille des messages est trop importante, il y a des risques de débordement des tampons de stockage puisqu'un nœud de commutation peut recevoir des messages depuis plusieurs stations). En plus, le délai d'acheminement de bout en bout est excessif (il faut attendre qu'un message soit entièrement stocké dans un nœud avant de le retransmettre vers le nœud suivant),

2.1.2.3 Commutation de paquets

Pour palier aux inconvénients engendrés par les messages de taille trop importante, on fragmente les messages en paquets de taille moyenne. Les paquets sont acheminés de nœud en nœud : après avoir été vérifiés, ils sont réexpédiés, sans attendre la totalité du message.



Cette fragmentation élimine les inconvénients engendrés par la commutation de messages trop longs :

– A débit constant, le délai d'acheminement de bout en bout est plus court,
– La capacité de stockage des nœuds de commutation est moindre,
– A taux d'erreur constant, la probabilité d'erreur sur un paquet (un bit erroné) est plus faible, et en cas d'erreur, seul le paquet erroné doit être retransmis.
– De plus, les paquets peuvent plus facilement être multiplexés sur des liaisons à haut débit.

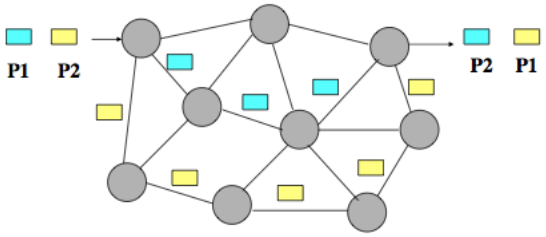
La taille des paquets est fixée par un compromis entre 2 contraintes :

– Il faut réduire leur taille pour profiter au maximum des avantages de la fragmentation,
– Il ne faut pas trop la réduire, à cause de l'encapsulation des données (pour ne pas réduire le débit utile, il faut que la taille des données utiles soit très supérieure à celle de la signalisation et des informations protocolaires).

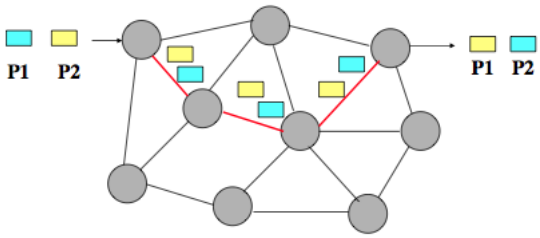
En pratique, elle est fixée par les protocoles de transfert de paquets : Elle est généralement de l'ordre de grandeur du koctet (sauf pour les réseaux à commutations rapides, pour lesquels les messages sont fragmentés en cellules de quelques dizaines d'octets).

La commutation de paquets peut se faire en deux modes :

– Mode non connecté : les paquets (appelés datagrammes) sont transmis de nœud en nœud, au fur et à mesure que la connexion est établie, sans s'assurer que les ressources soient disponibles de bout en bout. Les paquets d'un même message, sont indépendants. Ils peuvent suivre des chemins différents, car les algorithmes de routage sont adaptatifs (chaque paquet subit un routage, et son parcours dépend du trafic). Ils sont livrés dans le désordre.



– En mode connecté, un circuit est établi de bout en bout, avant de transférer le message, comme pour la commutation de circuits. Mais il s'agit bien de la commutation de paquets (le circuit est virtuel). Avant de transférer les paquets de données, un paquet (appelé paquet d'appel) subit un routage adaptatif, pour parcourir un chemin optimal. Au fur et à mesure de son parcours, les ressources sont réservées, et les tables de routage des nœuds traversés sont fixées. Ainsi, tous les paquets suivants d'un même message suivront le même chemin (appelé circuit virtuel commuté ou CVC), et sont livrés dans l'ordre d'émission. Après le transfert des données, un paquet (de libération) parcourt le CVC, et le ferme en restituant ses ressources.



Le transfert des paquets de données est plus rapide, car ils ne sont pas retardés par l'exécution d'un algorithme de routage.

Le contrôle d'erreur dans les réseaux à commutation de paquets peu se faire en deux manières :

1. Un contrôle d'erreur par liaison de données : Le paquet, encapsulé dans une trame, est contrôlé dans chaque nœud de commutation. Cette méthode augmente la fiabilité, mais aussi le délai de transit.
2. Un contrôle d'erreur de bout en bout : Il n'y a pas de contrôle d'erreur dans les nœuds de commutation. Le contrôle est effectué aux extrémités par les usagers du réseau de commutation. Le transfert est moins fiable, mais plus rapide.

2.2 Adressage et nommage

Le but de l'adressage est de fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine. Les machines doivent être accessibles aussi bien par des humains que par d'autres machines. Une machine doit pouvoir donc être identifiée par :

- une adresse qui doit être un identificateur universel de la machine,
- un nom (mnémotechnique pour les utilisateurs),
- une route précisant comment la machine peut être atteinte.

Les noms sont plus faciles à utiliser par les utilisateurs, mais ne permettent pas l'identification des machines et nécessitent un moyens de faire la correspondance avec les adresses.

Les adresses forment le moyen d'identifier de manière unique chacun de ses utilisateurs.

On utilise dans les réseaux, selon la cas, deux types d'adressage :

- Adressage hiérarchique : l'adresse est décomposée en différentes parties qui permettent d'identifier :
  - le réseau auquel l'utilisateur est rattaché
  - le point d'accès par lequel il est raccordé au réseau

– l'utilisateur dans l'installation locale Le champ adresse diminue au fur et à mesure de la progression des blocs dans le réseau. L'exemple courant de ce type est la numérotation téléphonique

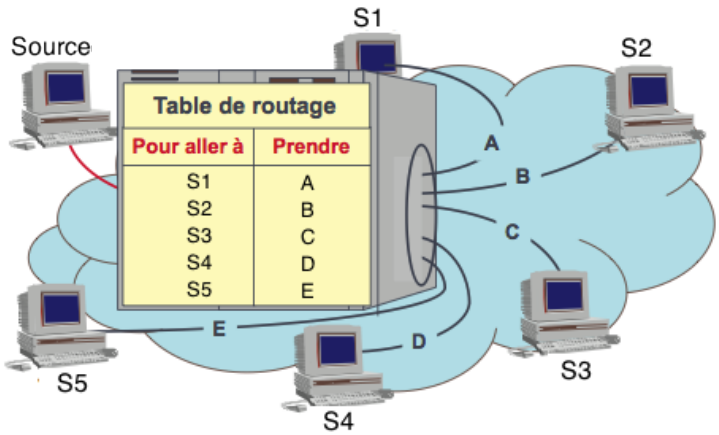
– Adressage à plat : le format de l'adresse n'a aucune signification particulière quant à la localisation de l'entité communicante. L'exemple est l'adresse MAC.

2.3 Principe du routage

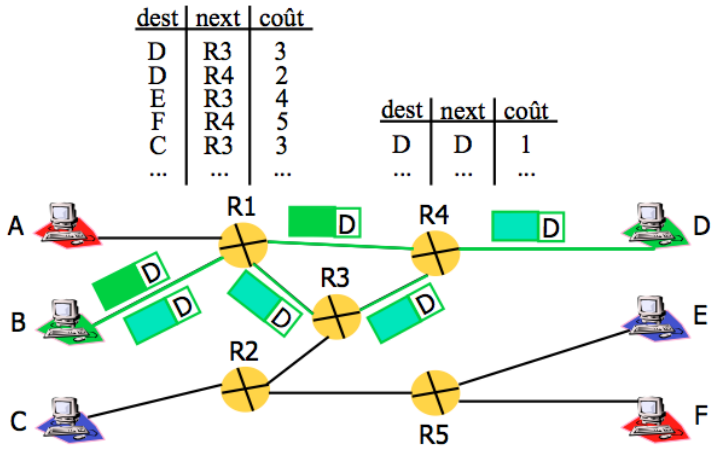
Le but du routage est la détermination d'un chemin à travers le réseau entre une machine émettrice et une machine réceptrice, toutes deux identifiées par leur adresse. Les protocoles de routage établissent des règles d'échange entre routeurs pour mettre à jour leurs tables d'informations selon des critères de coût comme, par exemple, la distance, l'état de la liaison, le débit. Ils améliorent ainsi l'efficacité du routage.

Il y a de très nombreux problèmes à résoudre. L'un des problèmes fondamentaux à éviter réside dans les boucles de routage (le message peut "tourner en rond" dans le réseau et ne jamais atteindre son destinataire). L'autre apparait lorsqu'il y a une panne dans le réseau et qu'il faut optimiser le calcul des nouvelles routes : une fois la panne détectée, il faut transmettre l'information sur l'évènement le plus rapidement possible pour que les différents routeurs recalculent par où faire passer leurs messages en contournant la liaison en panne.

Chaque nœud du réseau comporte des tables, dites tables d'acheminement couramment appelées tables de routage, qui indiquent la route à suivre pour atteindre le destinataire. En principe, une table de routage est un triplet <Adresse destination>/<Route à prendre>/<Coût>.



Chaque paquet doit contenir une information qui permet d'identifier le destinataire pour que chaque routeur puisse prendre une décision (@destination). Le "coût" permet de choisir la route appropriée si plusieurs routes sont possibles (coût pour atteindre la destination). Par exemple dans la figure suivante, le coût et représenté par le nombre de sauts (de routeurs) pour atteindre la destination.



Un protocole de routage commence par la construction des tables de routage au niveau de chaque nœud, ensuite utilise ces tables pour l'acheminement des paquets entre les stations. À priori, aucun routeur n'a une vision globale de la route que prendront les paquets : les paquets sont relayés de proche en proche jusqu'au destinataire. L'émetteur du paquet doit connaître le premier routeur relais, ensuite, chaque routeur est chargé d'acheminer le paquet vers le routeur suivant jusqu'à la destination finale.

Un protocole de routage efficace doit assurer :

- une taille minimale pour les tables de routage,
- Une consultation rapide des tables,
- Une consommation acceptable de mémoire
- Le moins possible d'informations à échanger
- minimiser la fréquence des messages de contrôle générés par l'échange des informations de routage
- être robuste en évitant les boucles,la surcharge de certains routeurs...
- trouver une route optimale

2.4 Types d'algorithmes de routage

En général des types de routage existent :

2.4.1 Routage statique

Dans le routage statique (ou non adaptatif), la décision de routage ne dépend pas de l'état du réseau ; le choix de la route est défini par l'administrateur une fois pour toute lors de l'initialisation et elles sont mises à jour uniquement quand la topologie du réseau change (cas de panne).

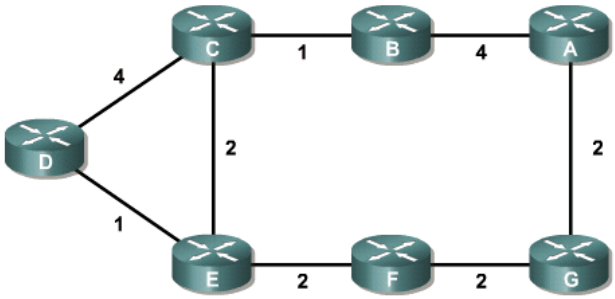
Le routage statique est simple mais ne recherche pas la route optimale et n'est pas adapté à la défaillance d'un lien. Il est généralement adapté aux petits réseaux et aux réseaux dans lesquels le choix de la route est limité (routes rentrées manuellement). Cependant, il assure le séquencement des paquets même en mode non connecté car tous les paquets prennent la même route.

Deux variantes de routage statique sont utilisées :

2.4.1.1 Plus court chemin

Dans ce type de routage, l'administrateur calcule les chemins minimums entre chaque deux stations (réseaux) puis introduits les tables correspondant à ces chemins dans chaque routeur. Le réseaux tout entier est représenté par un graphe pondéré. Le coût (métrique) de chaque arrête peut être calculé selon :

- le nombre de saut (nombre de routeurs traversés)
- la distance réelle (en km) entre deux routeurs
- le délai de transmission (temps de latence)
- le nombre de paquets moyen dans les files d'attente
- le taux d'erreurs moyen
- le trafic moyen observé, ...



Le calcul des chemins est effectué en utilisant des algorithmes connus en théorie des graphes tel que Dijkstra.

2.4.1.2 Inondation

Dans le routage par inondation, chaque nœud envoie le message sur toutes ses lignes de sortie, sauf celle d'où provient le message. Pour éviter une surcharge du réseau, chaque message comporte un compteur de sauts. Le compteur est initialisé à l'émission (nombre de sauts autorisés) et décrémenté par chaque nœud. Le message est détruit quand le compteur de sauts est à zéro. Pour éviter les bouclages, les messages sont numérotés, chaque nœud mémorise cet identifiant et détruit les messages déjà vus.

Ce système est très robuste, il résiste à la destruction de plusieurs lignes et garantit de trouver toujours le plus court chemin ; il est utilisé dans certaines communications militaires et par certains protocoles de routage pour diffuser les informations d'états du réseau. Il est utilisé, également pour découvrir le chemin optimal et en déduire une route statique.

2.4.2 Routage dynamique

Dans le Routage dynamique, les tables de routage sont construites automatiquement sans l'intervention de l'administrateur. Les routeurs échangent régulièrement leurs états et mettent à jour leurs tables de routage. Ce routage est plus complexe que le routage statique et surcharge le réseau par l'échange d'informations de routage et ne garantit pas le séquencement en mode non connecté. Cependant, il permet de choisir la route optimale.

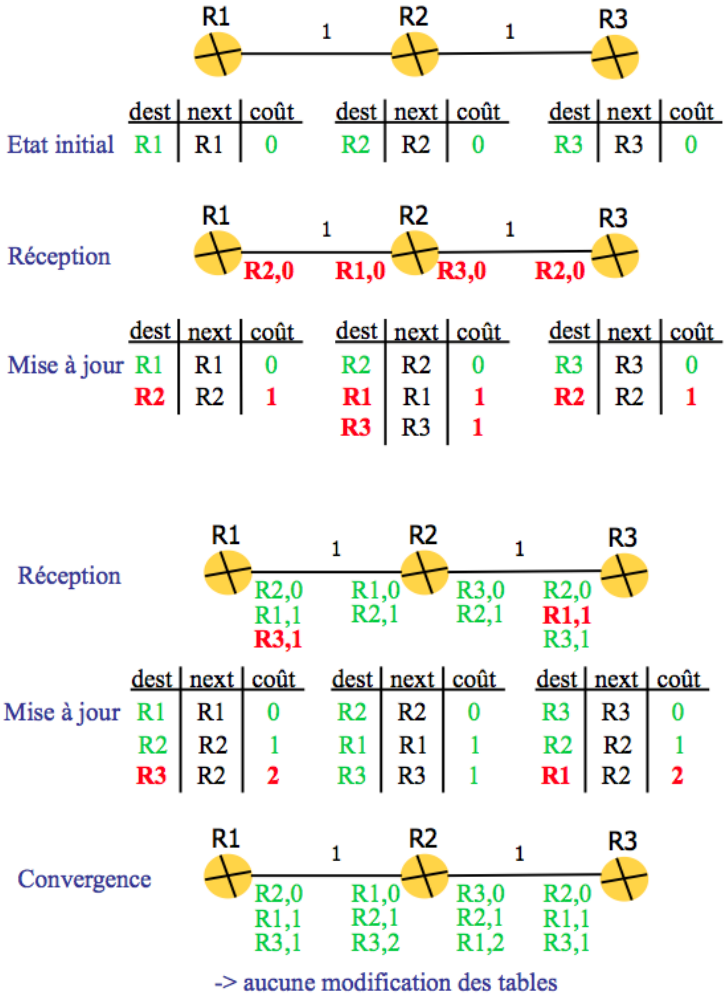
Il existe trois algorithmes de routage dynamique :

2.4.2.1 Routage à Vecteur de distance

Dans le routage à vecteur de distance ou routage de Bellman-Ford (distance vector routing), chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins. Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre. À réception, le nœud compare les informations reçues à sa propre base de connaissance :

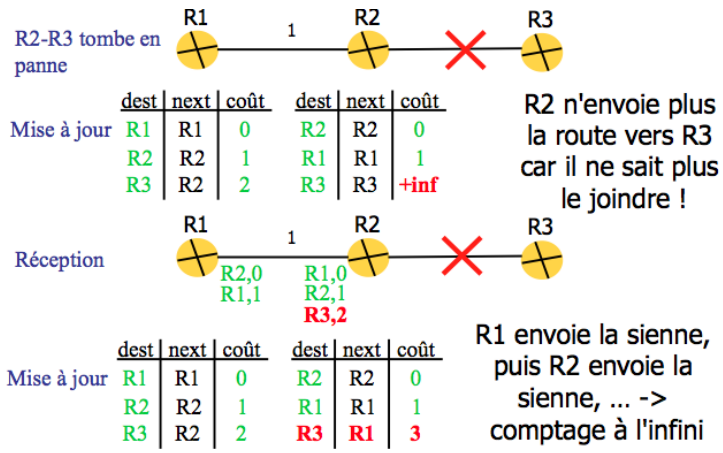
- La table reçue contient une entrée qui n'est pas déjà dans sa propre table, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette entrée dans sa table. Il a ainsi appris une nouvelle destination.
- La table contient une entrée qu'il connaît déjà. Si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il l'ignore sinon il met sa table à jour de cette nouvelle entrée.

De proche en proche chaque nœud apprend la configuration du réseau et le coût des différents chemins. La convergence des différentes tables peut être assez longue. Les deux figures suivantes en représentent un exemple.



Deux problèmes majeurs peuvent survenir dans cet algorithme en cas de panne d'un lien entre deux routeurs :

1. Les boucles de routage : la panne d'un lien peut conduire à une bouclage infini des paquets dans le réseau. La figure suivante illustre ce phénomène :tous les paquets à destination de R3 oscillent entre R1 et R2



2. l'algorithme ne converge plus : à l'échange suivant, R1 apprend de R2 que désormais le coût pour joindre R3 en passant par R2 est de 3 -> il met sa table à jour (R3, R2, 4) ; de même, R2 va apprendre de R1 que désormais le coût pour joindre R3 est de 4...

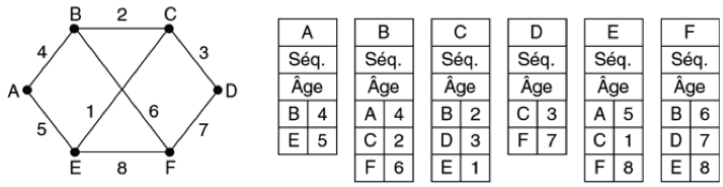
Les solutions utilisées consistent à :

- interdire à un nœd de signaler une destination qu'il connaît au routeur par lequel il l'a apprise (split horizon)
- limiter la valeur infinie du coût à une petite valeur (16 dans RIP) -> convergence dés que l'infini est atteint

2.4.2.2 Routage à état des liens

Le principal défaut du routage vecteur distance provient du fait que les routeurs n'ont la connaissance d'un changement d'état du réseau que lorsque leur voisin le leur communique, ce qui peut être long. Pour pallier ce défaut, le routage à état des liens (link state routing) procède différemment :

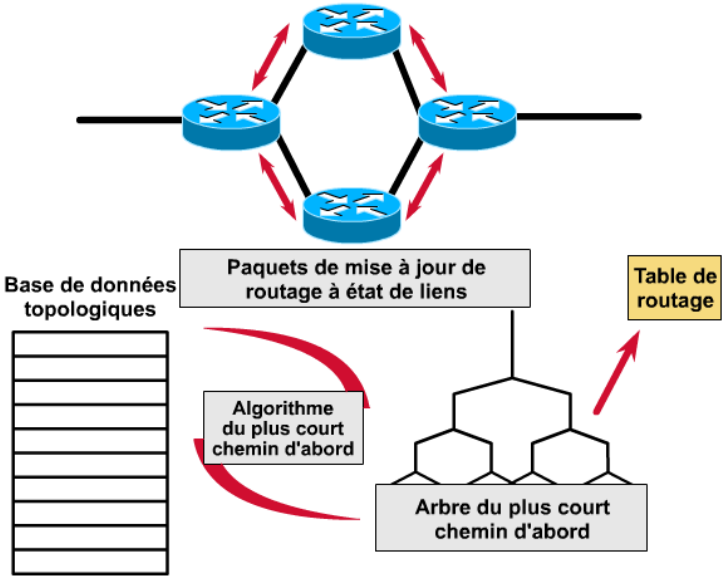
- Chaque routeur apprend ses propres réseaux directement connectés
- Les routeurs découvrent les routeurs directement connectés
- Chaque routeur A construit son propre LSP (Link State Packet) sous la forme (A, B, c), le lien du nœud A vers le nœud B a un coût de c ;



- Dés que le LSP est crée, le routeur le diffuse vers tous ses voisins qui stockent l'information et ensuite l'achemine jusqu'à ce que tous les routeurs aient la même information (par inondation).
- Une fois que tous les routeurs ont reçu tous les LSP, chaque nœud construit une table où figure pour chaque lien son coût (matrice de coûts).

	A	B	C	D	E	F
A	0	4	∞	∞	5	∞
B	4	0	2	∞	∞	6
C	∞	2	0	3	1	∞
D	∞	∞	3	0	∞	7
E	5	∞	1	∞	0	8
F	∞	6	∞	7	8	0

- À partir de cette table, il calcule la table de routage.



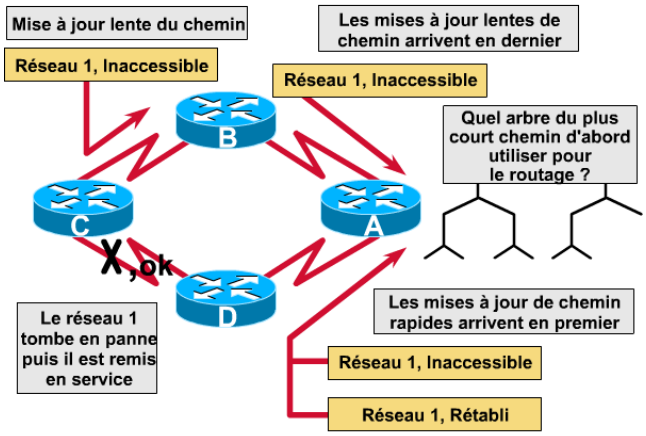
En pratique on utilisent les solutions suivantes

- découverte des voisins : envoi d'un paquet spécial, HELLO, auquel les voisins répondent par leur identité
- mesure du coût de la ligne : envoi d'un paquet spécial, ECHO, qui est aussitôt renvoyé par les voisins ; un timer mesure le temps d'aller retour en tenant compte ou non de la charge du lien (temps dans les files d'attente)
- élaboration des paquets d'état de lien quand un évènement important se produit
- distribution des paquets : par inondation avec numérotation des paquets et âge du paquet
- calcul de la nouvelle table par l'algorithme de Dijkstra (en se plaçant à la racine)

Dans le cas d'une modification de la topologie du réseau tel qu'une panne d'une liaison ou l'ajout d'une nouvelle, le premier routeur informé de cette modification transmet l'information aux autres routeurs ou à un routeur désigné auquel tous les autres routeurs se réfèrent pour obtenir des mises à jour. Ainsi, les informations de routage communes sont envoyées à tous les routeurs de l'interréseau. Chaque routeur recevant cette information modifie sa base topologique et recalcule sa table de routage.

L'un des défit les plus importants du routage à états de liens et de garantir la cohérence des informations des routeurs. Si la distribution des paquets de mise à jour de routage à état de liens à tous les routeurs ne s'effectue pas correctement, le routage à état de liens peut comporter des routes non valides. Par exemple, si une liaison tombe en panne, le routeur directement lié envoie l'information dans un paquet. Si après une petite période

la liaison est rétablie et le routeur envoie la nouvelle information qui arrive à un routeur avant la première, ce dernier ne saura pas quoi faire.



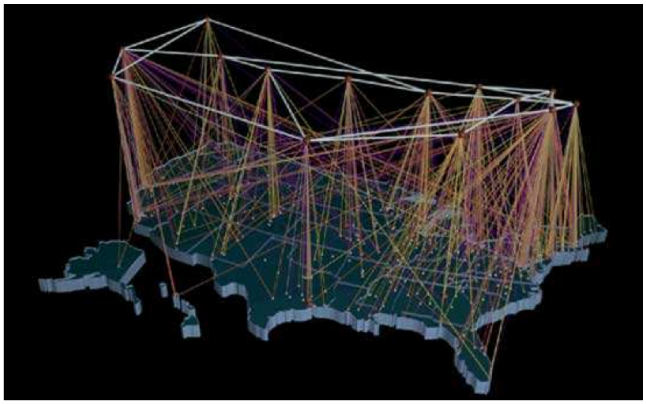
Le tableau suivant représente une comparaison entre les deux techniques de routage : à vecteurs de distance et à état de lien :

Vecteur de distance	**État des liens**
Vue de la topologie du réseau dans la perspective du voisin	Vue commune de toute la topologie du réseau
Additionne les vecteurs de distance d'un routeur à l'autre	Calcule le chemin le plus court au autres routeurs
Mises à jour périodiques fréquentes : convergence lente	Mise à jour déclenchée par évènement : convergence plus rapide
Copie des tables de routage passées aux routeurs voisins	Les mises à jour de routage à état de liaison sont passées aux autres routeurs

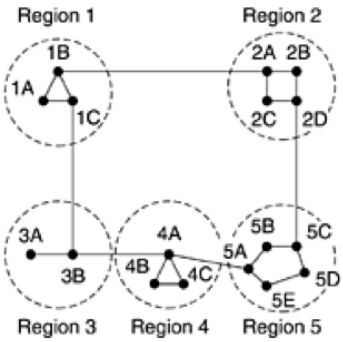
2.4.2.3 Routage hiérarchique

Le routage au moindre coût nécessite la diffusion, à travers le réseau, d'information concernant soit les tables de routage (vector distance), soit l'état des liens (link status). Ce trafic consomme de la bande passante au détriment des données à écouler. Plus le réseau est grand, plus le trafic de mise à jour est conséquent, plus les tables de routage sont importantes et plus le calcul des routes consomme du temps CPU. Dans ce cas, le routage doit être fait hiérarchiquement tel que dans les réseaux téléphoniques. Les routeurs sont subdivisés en régions où chaque routeur connait tous les détails de routage sur sa région et ne connait rien à propos des autres. Si les réseaux sont plus grands la subdivision peut être

plus profonde : le réseau en groupes, le groupe en zones, les zones en cluster, les clusters en régions etc. La figure suivante présente l'exemple de la subdivision des routeurs au états unis :



Le routage hiérarchique permet de réduire les tables de routage et leur gestion. Le figure suivante en illuste un exemple :



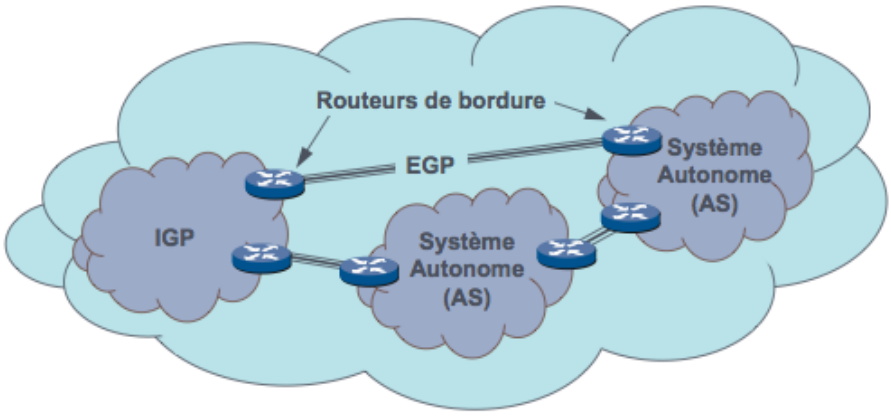
Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

En routage hiérarchique sur internet, le réseau est découpé en domaines appelés systèmes autonomes (AS, Autonomus System). Chaque domaine est identifié, les messages n'appartenant pas au domaine sont éliminés.



Ce mode de découpage des réseaux conduit à définir deux familles de protocoles de routage, notamment utilisés dans Internet :

- Les protocoles internes au domaine (IGP, Interior Gateway Protocol), qui assurent le routage dans le domaine, mais ignorent les nœuds des autres domaines. Il concentre sur la performance de routage.
- Les protocoles externes au domaine (EGP, External Gateway Protocol), qui gèrent l'échange d'information entre domaines afin de découvrir la connectivité de chaque domaine. Il concentre sur la politique de routage et l'efficacité passe après.

Dans un système autonome, il y a un ou plusieurs routeurs de bordure qui dialoguent avec le ou les routeurs de bordure des SA voisins. Lorsqu'il n'y a qu'un seul routeur de bordure, le SA est vu comme un cul-de-sac ; il ne peut pas être un SA de transit pour des messages sur l'interconnexion. Quand il y en a plusieurs, le SA est un SA de transit : des messages sur l'interconnexion peuvent y entrer par l'un des routeurs de bordure et ressortir par l'autre. Il faut toutefois ajouter que certains SA interdisent le transit interne (pour des raisons politiques ou commerciales, par exemple). Ils sont ignorés par les protocoles EGP. Chaque domaine est autonome et peut mettre en œuvre un protocole de routage interne différent vecteurs de distance ou état des liens.

2.5 Routage dans les réseaux ad-hoc

2.5.1 Environnements mobiles

Les environnements mobiles offrent aujourd'hui une grande flexibilité d'emploi. En particulier, ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible. Plusieurs systèmes utilisent déjà le modèle cellulaire de réseaux sans fil, et connaissent une très forte expansion à l'heure

actuelle tel que l'exemple des réseaux GSM.

Les applications des réseaux ad-hoc sont nombreuses, on cite l'exemple classique de leur application dans le domaine militaire et les autres applications de tactique comme les opérations de secours et les missions d'exploration.

Les entités mobiles quelque soit leur type et leur puissance sont caractérisés par :

- une petite taille,
- une durée de vie des batteries limitée,
- risque de perte, vol, accident,...

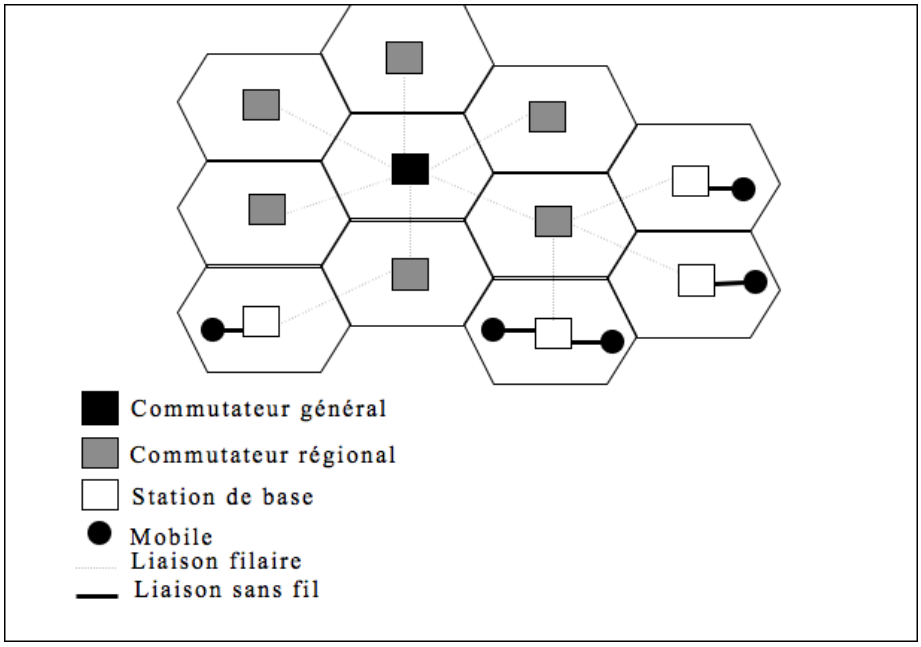
Le médium sans fil, aussi, est caractérisé par :

- une faible largeur de bande passante,
- des déconnexions fréquentes mais prévisibles,
- une diffusion naturelle dans chaque cellule.

En pratique, il existe aujourd'hui deux grands types e réseaux supportant la mobilité : les réseaux à base d'infrastructure tel que les réseaux cellulaires et les réseaux sans infrastructure appelés aussi réseaux mobiles ad-hoc.

2.5.1.1 Réseaux cellulaires

La surface couverte par un tel réseau est divisée en sous-surfaces, disposant chacune d'une station fixe MSS (Mobile Service Station) gérant les communications sans fil à l'intérieur de cette zone. Ces sous-surfaces de forme circonférencielle (360°), et de superficie limitée par la portée d'émission et de réception des MSSs et des téléphones, sont appelées cellules. La gestion des déplacements des téléphones entre les cellules est sous la responsabilité du réseau, elle est assurée par des commutateurs généraux et régionaux.



Divers problèmes sont apparus lors de l'implémentation de ce schéma, entre autres l'allocation des canaux de communication aux mobiles, le basculement des mobiles entre les cellules de communications (Hand-off), la localisation des mobiles,... etc.

2.5.1.2 Réseaux mobiles ad-hoc

Un réseau mobile ad-hoc, appelé généralement MANET (Mobile Ad-hoc NETwork), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque et dont le seul moyen de communication est l'utilisation des interfaces sans fil, sans l'aide d'une infrastructure préexistante ou administration centralisée.

Le concept des réseaux mobiles ad-hoc essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication cellulaire :

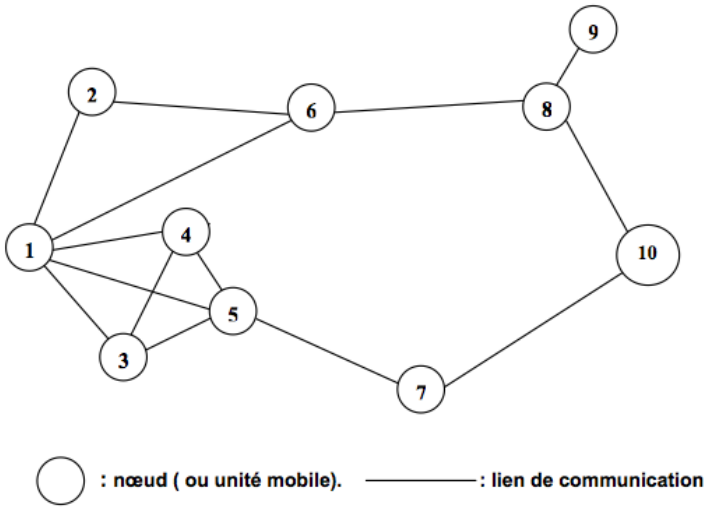
- Aucune administration centralisée n'est disponible. Ce sont les hôtes mobiles eux-mêmes qui forment, d'une manière ad-hoc, une infrastructure du réseau.
- Aucune supposition ou limitation n'est faite sur la taille du réseau ad-hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles.

Les réseaux ad-hoc sont idéals pour les applications caractérisées par une absence (ou la non-fiabilité) d'une infrastructure préexistante, tel que les applications militaires et les autres applications de tactique comme les opérations de secours (incendies, tremblement

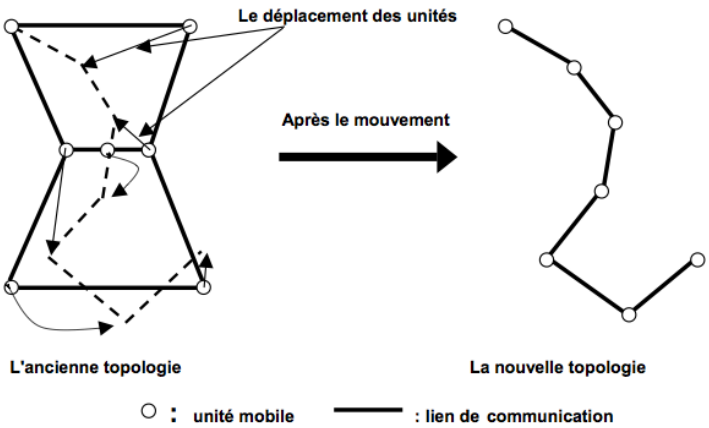
de terre..) et les missions d'exploration.

Un réseau ad-hoc peut être modélisé par un graphe $G_t = (V_t, E_t)$. Où : V_t représente l'ensemble des nœuds (i.e. les unités ou les ho ?tes mobiles) du réseau et E_t modélise l'ensemble les connections qui existent entre ces nœuds.

Si $e = (u, v) \in E_t$, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t. La figure suivante représente un réseau ad-hoc de 10 unités mobiles sous forme d'un graphe :



La topologie du réseau peut changer à tout moment, elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente.



2.5.2 Routage dans les réseaux cellulaires

Le problème de routage dans ce type de réseaux passe premièrement par la localisation des mobiles. Pour qu'un mobile puisse envoyer un message à un autre mobile, il doit

l'envoyer à la MSS (M) de la cellule où il se trouve, via la liaison sans fil. Cette MSS lance une recherche, dans le réseau, de la MSS (M') gérant la cellule où le mobile récepteur évolue actuellement. Une fois M' trouvée le message lui est transmis via le réseau statique, pour qu'elle le transmette au mobile récepteur via la liaison sans fil. L'envoie du message entre les deux MSS se fait par un protocole de routage classique, mais doit qui prendre en compte les hand-offs pour la mise à jour des tables de routage.

Pour pouvoir, donc, acheminer un message à un site mobile, il est indispensable de connaître sa position, c-à-d le localiser. En réalité, il existe plusieurs méthodes de localisation des mobiles , présentant chacune ses avantages et ses inconvénients.

2.5.2.1 La méthode Search

Elle consiste à chercher le mobile dans le réseau entier, c-à-d envoyer une demande de localisation à toutes les MSS, et celle gérant la cellule où le mobile se trouve répond. le coût engendré par cette méthode dépend seulement du nombre des stations de base dans le réseau mobile.

2.5.2.2 Méthode Inform

Elle fait passer le message au mobile à travers son serveur habituel, qui est informé de façon permanente de ses mouvements. Le coût dans cette méthode dépend du nombre des mouvements intercellulaires faits par le mobile.

2.5.2.3 Méthode combinée

Les deux méthodes Search et Inform peuvent être combiné de façon à ce que le mobile informe son serveur de sa position à chaque intervalle de temps, ou après un certain nombre de mouvements, et est ensuite recherché dans le voisinage de sa dernière position connue. Évidement, le mobile n'est recherché que s'il n'est pas trouvé dans sa dernière position connue

2.5.2.4 Autres méthodes

Dans le cas de concentration d'un grand nombre de mobiles dans un petit area, les serveurs de localité dans cet area peuvent être surchargés voir engorgés par les messages de localisation. Pour palier à ce problème, une méthode dynamique de localisation est proposée, dans laquelle, l'information sur la localité d'un mobile est dupliquée dans un ensemble

de serveurs (MSS), qui varient en fonctions de la localité du mobile, pour distribuer la charge de localisation sur tous le réseau. Évidement, dans toutes ces méthodes le mobile n'est recherché que s'il n'était pas trouvé dans sa dernière position connue. Le choix entre ces méthodes nécessite une étude du comportement général des mobiles, par exemples, la méthode search est moins coûteuse que la méthode Inform pour les mobiles qui se déplacent beaucoup, et vice versa. La méthode dynamique est efficace pour les cas de concentration des mobiles dans des zones spécifiques.

2.5.3 Routage ad-hoc

Suivant la manière de création et de maintenance des routes lors de l'acheminement des données, les protocoles de routage peuvent être séparés en deux catégories, les protocoles pro-actifs et les protocoles réactifs. Les protocoles pro-actifs établissent les routes à l'avance en se basant sur l'échange périodique des tables de routage, alors que les protocoles réactifs cherchent les routes à la demande.

2.5.3.1 Protocoles pro-actifs

Les protocoles de routage pro-actifs pour les réseaux mobiles ad-hoc, sont basé sur la même philosophie des protocoles de routage utilisés dans les réseaux filaires conventionnels. Les deux principales méthodes utilisées sont :

- La méthode Etat de Lien ("Link State") et
- La méthode du Vecteur de Distance ("Distance Vector").

Les deux méthodes exigent une mise à jour périodique des données de routage qui doit être diffusée par les différents nœuds de routage du réseau. Parmi les principaux protocoles de cette classe on trouve :

2.5.3.1.1 Protocole DSDV Le protocole DSDV (Destination-Sequenced Distance Vector routing) est caractérisé par :

- Basé sur l'algorithme Bellman-Ford en rajoutant quelques améliorations.
- Chaque station mobile maintient une table de routage qui contient :
  - Toutes les destinations possibles.
  - Le nombre de nœud (ou de sauts) nécessaire pour atteindre la destination.
  - Le numéro de séquences (SN :sequence number) qui correspond à un nœud destination.

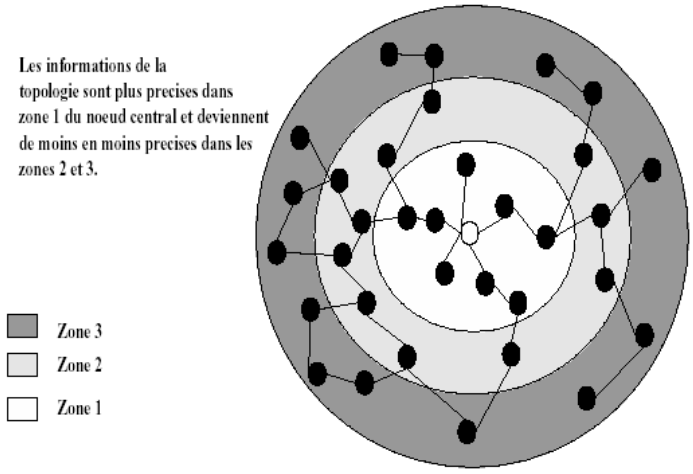
- Le NS est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage.
- La mise à jour dépend donc de deux paramètres : Le temps, c'est à dire la période de transmission, et Les événements
- Un paquet de mise à jour contient :
    1. Le nouveau numéro de séquence incrémenté, du nœud émetteur. Et pour chaque nouvelle route :
    2. L'adresse de la destination.
    3. Le nombre de nœuds (ou de sauts) séparant le nœud de la destination.
    4. Le numéro de séquence (des données reçues de la destination) tel qu'il a été estampillé par la destination.

Le DSDV élimine les deux problèmes de boucle de routage "routing loop", et celui du "counting to infinity". Cependant, une unité mobile doit attendre jusqu'à ce qu'elle reçoive la prochaine mise à jour initiée par la destination, afin de mettre à jour l'entrée associée à cette destination, dans la table de distance. Ce qui fait que le DSDV est lent.

Le DSDV utilise une mise à jour périodique et basée sur les événements, ce qui cause un contro ?le excessif dans la communication.

2.5.3.1.2 Protocole FSR Le protocole FSR (Fisheye State Routing) est basé sur l'utilisation de la technique "œil de poisson" (fisheye), proposée par Kleinrock et Stevens, qui l'ont utilisé dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques.

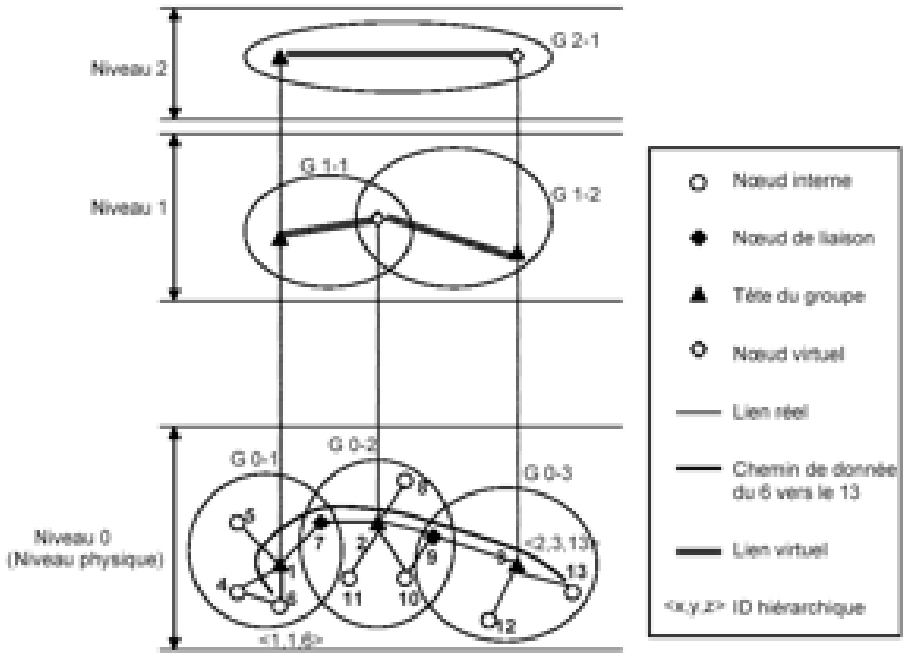
Dans la pratique, l'œil d'un poisson capture avec précision, les points proches du point focal. La précision diminue quand la distance, séparant le point vu et le point focal, augmente. La figure suivante illustre la technique FE utilisée par le protocole :



Dans le contexte du routage, l'approche du "fisheye" matérialise, pour un nœud, le maintien des données concernant la précision de la distance et la qualité du chemin d'un voisin direct, avec une diminution progressive, du détail et de précision, quand la distance augmente. La diminution de fréquence est assurée en changeant les fréquences de mise à jour, et cela en utilisant des périodes d'échanges différentes pour les différentes entrées de la table de routage. Les entrées qui correspondent aux nœuds les plus proches, sont envoyés aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite).

2.5.3.1.3 Protocole HSR Le protocle HSR ((Hierarchical State Routing)) combine les notions de groupes dynamiques, niveaux hiérarchiques avec une gestion efficace de localisation.

Dans le HSR, l'image de la topologie du réseau, est sauvegardée sous forme hiérarchique. Le réseau est partitioné en un ensemble de groupes. Dans un groupe, un nœud doit être élu pour représenter le reste des membres. Les représentants des groupes dans un niveau l, deviennent des membres dans le niveau l+1. Ces nouveaux membres, s'organisent en un ensemble de groupes de la même manière du niveau bas, et ainsi de suite pour le reste des niveaux. La figure suivante illustre l'application du mécanisme de partitionnement hiérarchique :



L'adresse hiérarchique, suffit pour délivrer les paquets de données à une destination, indépendamment de la localisation de la source, et cela en utilisant la table HSR. Exemple : <1,1,7> est une adresse du nœud de liaison d'ID 7.

Exemple : l'acheminement des données entre le nœud 6 et le nœud 3 (figure précédente).

Prenons comme exemple le nœud 6 (figure 3.4) comme source, et le nœud 13 comme destination. Les adresses de ces nœuds sont respectivement : HID(6) = <1,1,6> et HID(13) = <2,3,13>. Pour acheminer une information du nœud 6 vers le nœud 13, le nœud 6 envoie l'information au nœud supérieur, qui le suit hiérarchiquement, i.e. le nœud d'ID 1. Le nœud 1 délivre l'information au nœud 3 qui suit le nœud destination dans l'ordre hiérarchique. Un "lien virtuel" existe entre les nœuds 1 et 3, matérialisé par le chemin (1,7,2,9,3). Par conséquent, l'information suivra ce chemin pour atteindre la destination. Dans la dernière étape, le nœud 3 délivre l'information au nœud 13 en suivant le chemin hiérarchique qui le relie à la destination (dans notre cas, ce chemin se réduit en un seul saut).

2.5.3.2 Protocoles réactifs

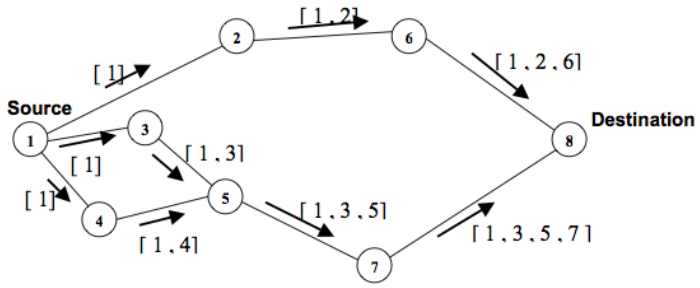
Les protocoles de routage appartenant à cette catégorie, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information spécifiée, inconnue au préalable.

La majorité des algorithmes utilisés sont basé sur le mécanisme d'apprentissage en

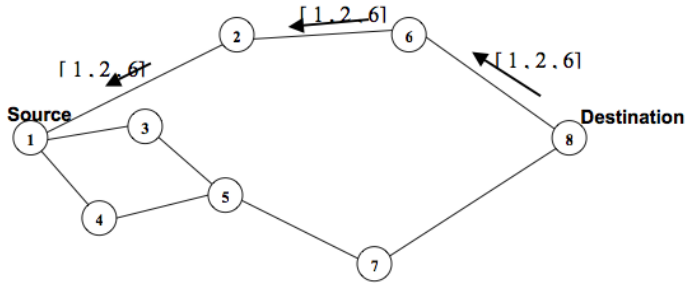
arrière (backward learning). On trouve pr exemple dans cette classe :

2.5.3.2.1 Protocole DSR Le protocole "Routage à Source Dynamique" (DSR), est basé sur l'utilisation de la technique "routage source". Dans cette technique : la source des données détermine la séquence complète des nœuds à travers lesquelles, les paquets de données seront envoyés.

Un site initiateur de l'opération de « découverte de routes », diffuse un paquet requête de route. Si l'opération de découverte est réussite, l'initiateur reçoit un paquet réponse de route qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. Le paquet requête de route contient donc un champ enregistrement de route, dans lequel sera accumulée la séquence des nœuds visités durant la propagation de la requête dans le réseau, comme le montre la figure suivante :



(a) Construction de l'*enregistrement de route.*



(b) Le renvoi du chemin.

Afin d'assurer la validité des chemins utilisés, le DSR exécute une procédure de maintenance de routes :

- Quand un nœud détecte un problème fatal de transmission, à l'aide de sa couche de liaison, un message erreur de route (route error) est envoyé à l'émetteur original du paquet. Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin.
- Lors de la réception du paquet erreur de route par l'hôte source, le nœud concerné par

l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont tronqués à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.

– L'utilisation de la technique "routage source", fait que les nœuds de transit n'aient pas besoin de maintenir les informations de mise à jour pour envoyer les paquets de données, puisque ces derniers contiennent toutes les décisions de routage.

Dans ce protocole, il y a une absence totale de boucle de routage, car le chemin source-destination fait partie des paquets de données envoyés.

2.5.3.2.2 Protocole TORA Le protocole TORA (Temporally-Ordered Routing Algorithm) a été conçu principalement pour minimiser l'effet des changements de la topologie qui sont fréquents dans les réseaux ad hoc.

Afin de s'adapter à la mobilité des réseaux ad hoc, le protocole stocke plusieurs chemins vers une même destination, ce qui fait que beaucoup de changements de topologie n'auront pas d'effets sur le routage des données, à moins que tous les chemins qui mènent vers la destination seront perdus (rompus).

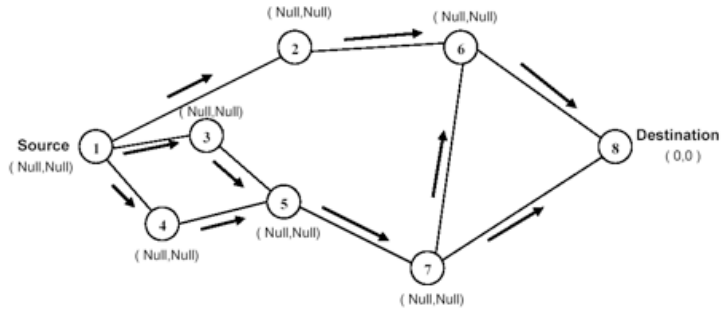
TORA est caractérisé essentiellement par le fait que les messages de contrôle sont limités à l'ensemble des nœuds proches du lieu de l'occurrence du changement de la topologie.

Dans ce protocole, l'utilisation des meilleurs chemins a une importance secondaire, les longs chemins peuvent être utilisés afin d'éviter le contrôle induit par le processus de découverte de nouveaux chemins.

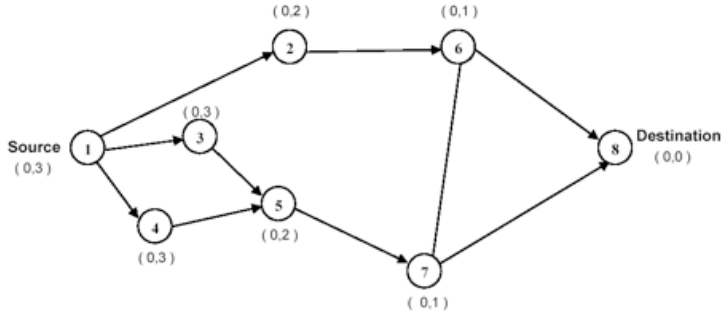
TORA est basé sur l'utilisation de la propriété appelée "orientation destination" des graphes acycliques orientés. Un graphe acyclique orienté (DAG) est orienté destination s'il y a toujours un chemin possible vers une destination spécifiée. Le graphe devient non orienté destination, si un lien (ou plus) devient défaillant. Dans ce cas, les algorithmes utilisent le concept d'inversement de liens. Ce concept assure la transformation du graphe précédent, en un graphe orienté destination durant un temps fini.

Afin de maintenir le DAG orienté destination, l'algorithme TORA utilise la notion de taille de nœud. Chaque nœud possède une taille qui l'échange avec l'ensemble de ses voisins directs. Un lien est toujours orienté du nœud qui a la plus grande taille, vers le nœud qui la plus petite taille.

La figure suivante montre la création du DAG dans le protocole TORA :

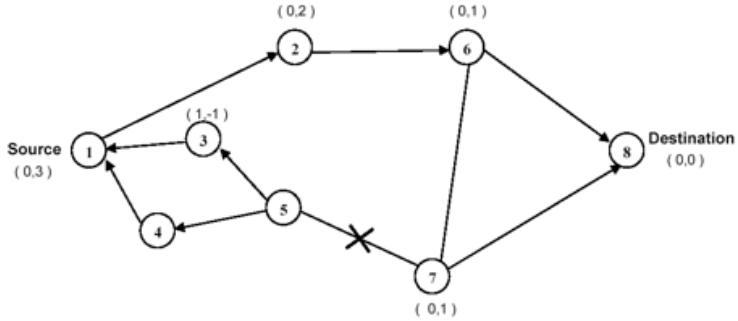


(a) La propagation du paquet QRY



(b) Les tailles des nœuds après la réception du paquet UPD

Quand un nœud i détecte une défaillance, i.e. invalidité d'un lien (sachant qu'il ne possède pas de suivants valides vers la destination), il lance un nouveau niveau de référence. L'objectif du nouveau niveau de référence est d'indiquer à la source l'invalidité des chemins rompus. La figure suivante donne un exemple de ce processus :



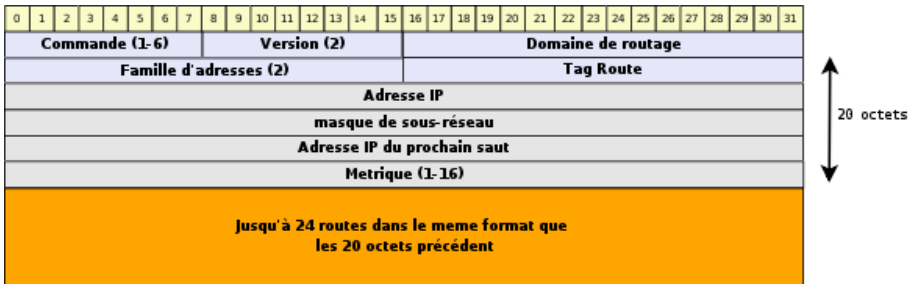
2.6 Protocoles de routage

Les principaux protocoles de routage utilisés sont :

2.6.1 RIP(Routing Information Protocol)

De type vecteur distance, RIP est le premier protocole interne. Utilisé dans la communauté Internet, il est aujourd'hui remplacé par OSPF. Malgré une convergence lente et un

trafic de gestion important, RIP reste le protocole de routage le plus employé. Il existe en deux version RIPv1 et RIPv2. Les messages RIP sont portés par des datagrammes UDP. La figure suivante montre la structuration d'un tel message.



- Commande : requête/repose ou diffusion
- La version pour RIPv2 est 2 !
- Domaine (RIPv2) Pour pouvoir faire tourner simultanément sur une même machine plusieurs instances du logiciel de routage
- Famille d'adresse : IPv4 ou IPv6. Ce champ peut également contenir la valeur hexadécimale 0xffff pour indiquer qu'il s'agit un bloc d'authentification. Dans ce cas l'identifiant de route contient la valeur 2 et les 16 octets qui suivent un mot de passe en clair, aligné à gauche et complété par des zéros.
- Le tag de routage existe pour prendre en compte les protocoles de type Exterior Gateway, c'est un numéro d'AS pour BGP et EGP.
- Adresse IP : Il s'agit de la destination à atteindre par le routeur qui émet cette annonce
- Le masque de sous-réseau de chaque entrée est lié aux adresses IP correspondantes.
- L'adresse IP du prochain saut correspondant à l'adresse où sont envoyés les paquets.

Les apports de RIPv2 sont les suivants :

- Transmission d'un masque de sous-réseau avec chaque route. Ce point est majeur parce qu'il permet d'utiliser RIP avec des réseaux comportant des sous-réseaux ;
- Authentification (très insuffisante puisque le mot de passe circule en clair). Le constructeur Cisco a ajouté des extensions permettant l'usage de MD5, c'est mieux ;
- Indication d'un prochain routeur qui n'est pas celui qui annonce la route ;
- Indication de routes de provenances externes, ou route tag ;
- Usage de l'adresse multicast 244.0.0.9 pour propager des routes (plutôt qu'un limited broadcast IP, plus perturbateur parce que lu par tous les hôtes).

2.6.2 OSPF (Open Short Path First)

C'est un protocole interne à état des liens utilisés dans Internet. Pour éviter l'inondation, les informations d'état sont diffusées sur une adresse de multicast réservée à OSPF.

2.6.3 IS-IS (Intermediate System to Intermediate System)

C'est le protocole de routage interne de l'ISO . C'est un protocole à état des liens.

2.6.4 IGRP (Interior Gateway Routing Protocol)

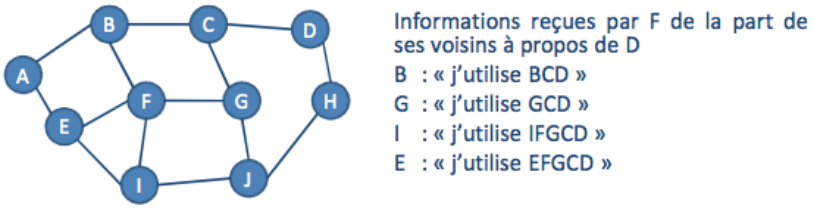
C'est un protocole propriétaire de la société Cisco de type vecteur-distance. Cependant, IGRP utilise une métrique construite qui prend en compte le délai d'acheminement, le débit, la fiabilité, la charge du réseau et le MTU (Maximum Transfer Unit).

2.6.5 EGP (Exterior Gateway Protocol)

EGP est le premier algorithme de routage à avoir été mis au point, au début des années 1980, pour router un paquet d'un système autonome vers un autre. Ses faiblesses sont apparues avec le développement exponentiel d'Internet et le besoin d'éviter certaines zones politiquement sensibles. Il a été remplacé par le protocole BGP

2.6.6 BGP (Border Gateway Protocol)

Pour répondre aux faiblesses d'EGP, un nouvel algorithme a été mis en chantier par l'IETF(Internet Engineering Task Force) sous le nom de BGP. Une première version, BGP-1, a été implémentée en 1990, suivie de près par BGP-2 puis BGP-3. Au bout de quelques années a été déployé BGP-4, qui permet de gérer beaucoup plus efficacement les tables de routage de grande dimension en rassemblant en une seule ligne plusieurs sous-réseaux. Les routeurs de bordure des SA sont appelés routeurs BGP. Ils calculent des routes avec un algorithme à vecteurs de distance. À la différence de RIP, ils mémorisent la totalité du chemin et non seulement le premier routeur du chemin. Ils échangent donc des informations complètes, ce qui est possible car le graphe BGP est de petite taille. La figure suivante en illustre un exemple :



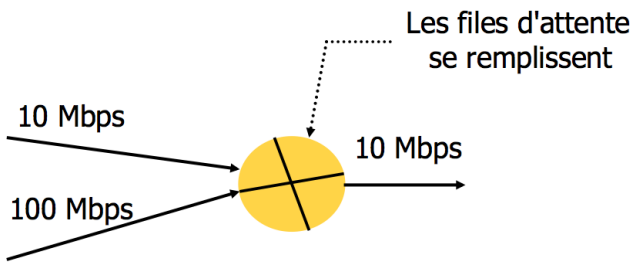
- Initialement F utilise le chemin FGCD pour aller en D
- Après réception de ces informations :
  - F élimine les chemins passant par lui même
  - F choisit le chemin minimum entre FBCD et FGCD
- Imaginons que G plante ou FG=infini
  - F reçoit les routes BCD, IFGCD, et EFGCD
  - Il choisit BCD directement

Une anecdote très connue sur BGP et qu'en Février 2008, YouTube est devenu inaccessible pendant environ 2 heures. Le responsable était l'opérateur pakistanais Pakistan Telecom qui a utilisé une technique très connue, le "détournement d'adresse IP". Il a annoncé à tous les routeurs BGP qu'il était la meilleure route à qui envoyer tout le trafic Youtube. On travail actuellement sur des solutions techniques futures : Secure BGP, soBGP,...

2.7 Contrôle de congestion

Les routeurs dans un réseau possèdent des files d'attente finies, si le trafic augmente, ces files d'attente se remplissent et le temps d'attente avant traitement augmente et le débit global du réseau diminue. Et si les paquets retardés ne sont pas acquittés à temps, ils sont retransmis par leur émetteurs et qui augmente le trafic d'autant plus, les files d'attente débordent et le réseaux finit par s'effondre.

Ce phénomène est appelé la congestion, il est du généralement à une sur-injection de paquets dans le réseaux, à la différence des capacités de traitement des routeurs, ou à l'émission des paquets en rafales.



La solution de ce problème peut être préventive ou réactive.

2.7.1 Solution préventive

Dans cette solution, on essaye d'empêcher le problème de se produire. La congestion résulte d'un trafic à écouler supérieur aux capacités du réseau, la solution la plus simple consiste à ne pas admettre, dans le réseau, plus de trafic que celui-ci est capable d'assimiler. Plusieurs solutions sont envisageables :

2.7.1.1 Contrôle de flux

Il s'agit d'asservir le débit des sources sur les capacités de traitement de chacun des nœuds. En limitant la longueur des files d'attente dans les nœuds intermédiaires, le contrôle de flux participe à la prévention de la congestion.

2.7.1.2 Contrôle d'admission

Le contrôle d'admission est assurée par le nœud d'entrée au réseau. L'émetteur spécifie, à la connexion, la nature du trafic qu'il va acheminer dans le réseaux, trois zones peuvent être définies :

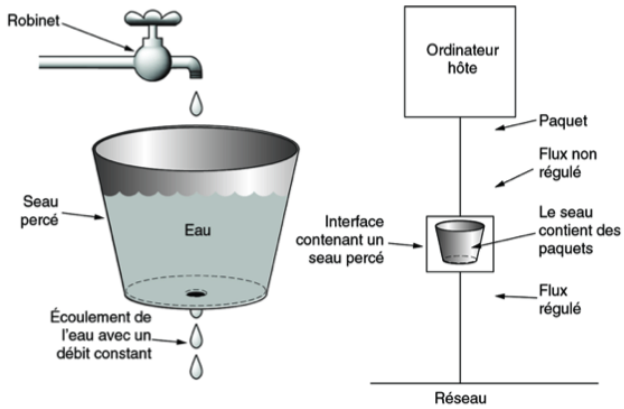
1. Zone garantie : correspond au trafic toujours acheminé
2. Zone de tolérance : correspond au trafic acheminé mais marqué, en cas de congestion, il est éliminé
3. Zone hors contrat : correspond au trafic excédentaire, éliminé et jamais acheminé par le réseau.

On interdit alors le trafic supérieur à la capacité de transit du réseaux.

2.7.1.3 Lissage du trafic

Même si chaque source respecte son contrat de service, la congestion peut résulter d'une simultanéité de soumission de rafales par les différentes sources. Pour éviter ce phénomène,

on effectue, à l'entrée du réseau, un lissage du trafic (technique du seau percé, leaky bucket algorithm). Dans ce système, les données sont mises en file d'attente et délivrées régulièrement.



2.7.2 Solution réactive

Quels que soient les mécanismes de prévention utilisés, rien ne permet de garantir qu'un état de congestion ne peut apparaître. Plusieurs politiques peuvent être mises en œuvre pour réduire la congestion : ils visent tous à éliminer le trafic en excès. Ces solutions dérivent des principes suivants :

- mettre en attente le trafic excédentaire dans une file d'attente de moindre priorité ;
- identifier le trafic excédentaire (Cell Tagging) et l'éliminer en cas de congestion ;
- éliminer tout le trafic ;
- envoyer à la source ou aux sources responsables une demande de ralentissement.

2.8 Protocole IP

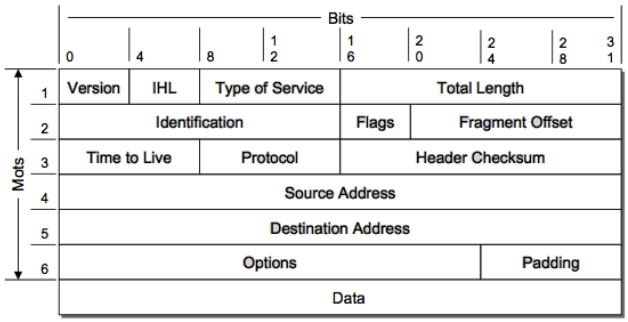
Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP. C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (paquets), sans toutefois en assurer la livraison. En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire d'un paquets grâce à trois informations disponible au niveau de chaque machine : l'adresse IP, le masque de sous-réseau, l'adresse de la passerelle par défaut. Les tables de routages établies au niveaux des routeurs permettent de déterminer les routes à suivre par les paquets. Le protocole RIP (routing information

protocol) utilisant un algorithme de type vecteur à distance permet de construire et mettre à jour les tables de routage.

2.8.1 Structure d'un paquet IP

Le datagramme IP contient un en-tête IP suivi des données IP provenant des protocoles des couches supérieures.



- Par défaut, la longueur de l'en-tête est de 5 mots de 32 bits (soit 20 octets) ; le sixième mot est facultatif. Puisque la longueur de l'en-tête est variable, elle inclut un champ appelé Internet Header Lenght (IHL - longueur de l'en-tête Internet) en mots.
- Le champ Version fait quatre bits et indique le format de l'en-tête IP (IPv4 ou IPv6).
- Le champ Type of Service (TOS) informe les réseaux de la qualité de service désirée, spécifiant ainsi les délais, le débit et la fiabilité. Les implémentations actuelles ignorent ce champ.
- Le champ Total length (longueur totale) contient la longueur de l'en-tête et des données IP, en octets.
- La durée de vie (Time To Live) représente la durée maximale de vie d'un datagramme sur le réseau. Cette valeur est décrémentée à chaque routeur. Lorsque le champ TTL tombe à 0, datagramme IP est écarté par le routeur.

Plusieurs autres protocoles sont utilisés avec le protocole IP dans la couche réseaux notamment :

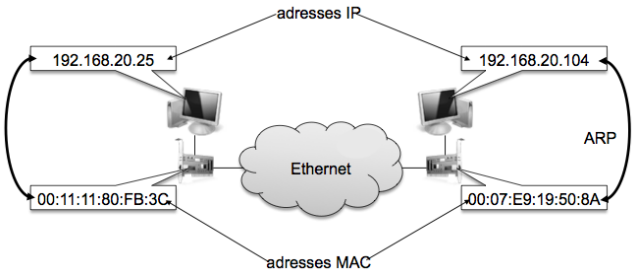
2.8.2 RIP

RIP (Routing Information Protocol) est un protocole de routage IP de type vecteur distance basé sur l'algorithme de routage décentralisé Bellman-Ford. Il utilise le nombre de sauts (hops) comme métrique de distance entre les machines. Chaque routeur diffuse sa table de routage à ses voisins toutes les 30 secondes. En recevant une table de routage d'un

voisin, un routeur met à jour la sienne. Le TTL max étant fixé à 16. Un routeur supprime une information de sa table si elles n'est pas confirmée pour 180 secondes. Il existe deux versions de RIP, la deuxième étant une amélioration de la première : RIPv1 et RIPv2.

2.8.3 ARP

En TCP/IP les interfaces du réseau sont modélisées par un unique identificateur à 32 bits, l'adresse IP. Or la transmission des datagrammes IP sur le réseau physique nécessite que ces datagrammes soient encapsulés dans des trames de couche de liaison de données (couche 2), telles que Ethernet ou Token-Ring, qui elles contiennent des adresses "physiques" (adresses MAC).



Un mécanisme souple, implémenté sous forme d'un protocole distinct et appelé ARP (Address Resolution Protocol) permet de déterminer dynamiquement l'adresse MAC à partir de l'adresse IP d'un hôte.

Pour déterminer l'adresse matérielle de l'hôte B avant de lui envoyer son message, la station A envoie sur le réseau une trame MAC de diffusion, appelée trame ARP de requête. Celle-ci contient les adresses IP et MAC de l'hôte A émetteur, ainsi que l'adresse IP de la destination B. La trame inclut un champ destiné à contenir l'adresse MAC de B. Tous les nœuds du réseau physique reçoivent la trame ARP. Seul l'hôte dont l'adresse IP correspond à l'adresse requise dans la trame de requête ARP répond en encodant sa propre adresse matérielle dans une trame de réponse ARP. L'hôte A initialise alors sa table cache ARP (conservée en mémoire) en utilisant la réponse fournie. Les entrées dans cette table expirent après une temporisation donnée qui peut être configurée dans certaines implémentations de TCP/IP (généralement 15 mn). Le cache ARP est consulté par un hôte juste avant l'envoi d'une requête ARP ; si la réponse se trouve dans le cache, la requête n'est pas effectuée.

2.8.4 RARP

RARP (Reverse ARP) est un mécanisme utilisé par les stations sans disques (terminaux) pour obtenir leur adresse IP auprès d'un serveur distant. Le nœud qui veut connaître sa propre adresse envoie en diffusion une requête RARP. S'il existe plusieurs serveurs RARP, chacun d'eux tente de traiter la requête RARP. Généralement, le client RARP accepte la première réponse reçue et ignore silencieusement les suivantes.

2.8.5 ICMP

Le protocole ICMP (Internet Control Message Protocol) envoie des messages qui réalisent des fonctions de contrôle, de détection des erreurs, et de transmission d'informations pour TCP/IP. Il existe 18 types de messages ICMP.

La commande *traceroute*, par exemple, utilise également des messages ICMP ; elle permet de connaître la route exacte empruntée par les datagrammes. traceroute envoie 3 paquets UDP avec un TTL égal à 1 puis recommence en augmentant le TTL de 1 à chaque envoi. A chaque fois que le TTL arrive à 0, le routeur renvoie un message ICMP d'erreur.

2.8.6 IGMP

IGMP (Internet Group Management Protocol) permet aux machines de déclarer leur appartenance à un ou plusieurs groupes auprès du routeur multipoint dont elles dépendent soit spontanément soit après interrogation du routeur. Celui-ci diffusera alors les datagrammes destinés à ce ou ces groupes. IGMP comprend essentiellement deux types de messages : un message d'interrogation (Host Membership Query), utilisé par les routeurs, pour découvrir et/ou suivre l'existence de membres d'un groupe et un message de réponse (Host Membership Report), délivré en réponse au premier, par au moins un membre du groupe concerné.