Chapitre 6

Couche Réseaux

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.

6.1 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.

6.1.1 Adressage

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

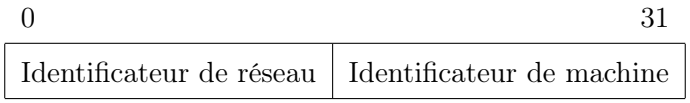
– l'utilisateur dans l'installation locale Le champ adresse diminue au fur et à mesure de la progression des blocs dans le réseau. L'exemple courant de ce type est la numérotation téléphonique

– 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.

6.1.1.1 Principe de l'adressage IP

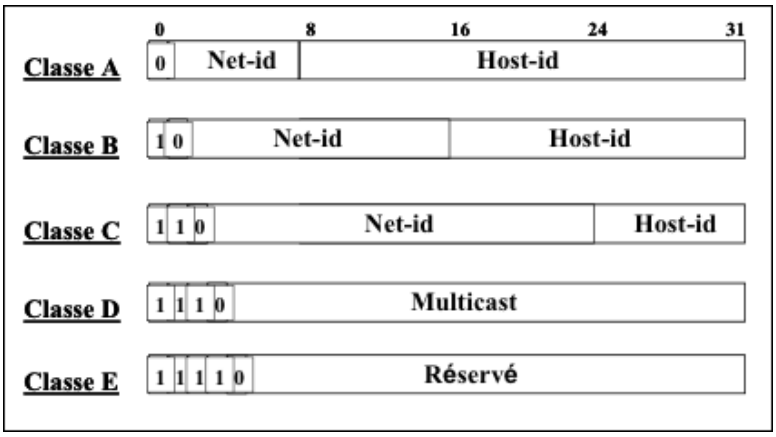
Les adresses IP permettent d'identifier à la fois les réseaux et les machines. Une adresse IP est constitué de 32 bits structuré en deux parties : identificateur de réseau et identificateur de machine.

Une adresse IP version 4 est constituée de 32 bits structurés en deux parties : identificateur de réseau et identificateur de machine.



Les identificateurs des réseaux sont contrôlés par le NIC (Network Information Center) en Californie mais les identificateurs des machines sont contrôlés localement.

Les adresses IP sont organisées en cinq classes :



– La classe A est la classe des très gros réseaux tel que ARPANET et MILNET, elle comporte 126 réseaux de 17 millions de machines chacun.

– La classe B est la classe des réseaux moyens, elle comporte 16384 réseaux de 65000 machines.

– La classe C est la classe des réseaux locaux, c'est la classe la plus utilisé dans l'Internet, elle comporte deux millions de réseaux de 254 machine chacun.

– La classe D est la classe de diffusion multiple (Multicast).
– La classe E est une classe expérimentale, réservée à des usages d'essai ou des usages futurs.

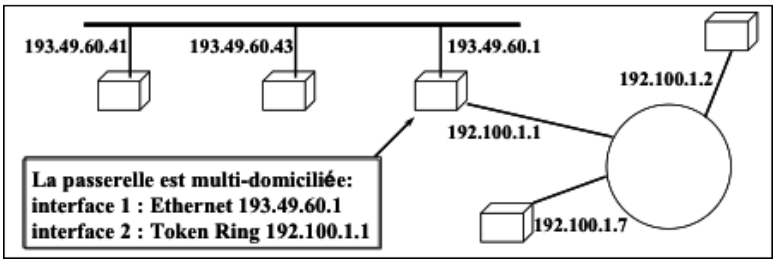
6.1.1.2 Notation décimale

Les adresses IP binaires sont difficiles à manipuler, on utilise alors la notation décimale qui représente l'adresse IP sous la forme de quatre valeurs décimale comprises entre 0 et 255 représentant les valeurs des quatre octets de l'adresse binaire.

10000000		00001010		00000010		00011110
128	.	10	.	2	.	30

On écrit : 128.10.2.30

Exemple



6.1.1.3 Adresses particulières

Dans chaque classe, il existe des adresses réservés pour une utilisation particulière et qui ne peuvent être attribuées à aucune machine et qui ont une signification particulière. En général :

– Un champ d'adresse (Netid ou Hostid) tout à 1 signifie tous les objets (réseaux ou machines) (utilisé pour la diffusion)
– Un champ d'adresse (Netid ou Hostid) tout à 0 signifie cet objet (réseau ou machine) (utilisé en cas d'ignorance des identificateurs)

Exemples

– L'adresse du réseau a une valeur d'indentificateur de machine où tous les bits sont nuls (0)
– Une adresse contenant les bits de réseau à 0 signifie ce réseau
– Une adresse de diffusion dans le réseau d'attachement (local) comporte les 32 bits IP à 1 (plein 1 ou all 1s) (Utilisée lors du démarrage lorsqu'on ignore son adresse IP).

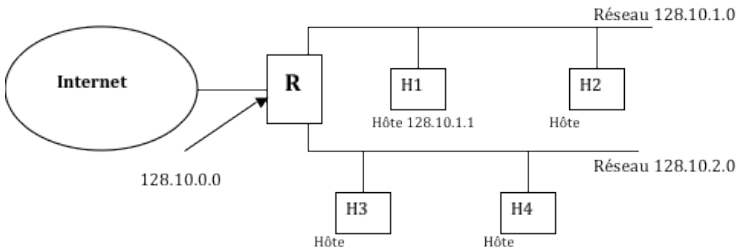
– Une adresse tout à 0 veut dire cet ordinateur n'est autorisé que lors du processus de démarrage.
– Une adresse qui à le premier octet égale à 01111111 (127) est dite adresse de Rebouclage, elle est utilisé pour les communications intra-machine pour des besoins de tests ou pour la communication entre les applications dans la même machine. Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés autrement appelés intranet 1.
– Les adresses de classe A de 10.0.0.0 à 10.255.255.255, de classe B de 172.16.0.0 à 172.31.255.255 et de classe C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés autrement appelés intranet

6.1.1.4 Sous adressage

Les concepteurs de l'adressage IP, travaillant dans un monde de gros systèmes coûteux, ont pensé à un Internet de quelques dizaines de réseaux et de quelques centaines de machines. Ils n'ont pas prévu l'explosion du nombre de petits réseaux individuels, la croissance était exponentielle et on a vu un doublement de taille tous les neuf mois. Le grand nombre de réseaux élémentaires a fini par poser des problèmes :

– La tâche de gestion des adresses IP est énorme
– Les tables de routage deviennent gigantesques voire saturés.
– La classe C (2 millions de réseaux) est devenue rapidement insuffisante.
– L'utilisation de la classe B engendre aussi des problèmes : le nombre de réseaux est insuffisant et la gestion de 65000 machines au sein de chaque réseau est très difficile.

D'où la nécessité de subdiviser. Le sous adressage (subnet adressing ou subnetting) est une technique standardisée dans l'adressage IP, elle permet d'utiliser une seule adresse réseau avec plusieurs réseaux (sous-réseaux) en découpant la partie réservée à l'adresse des machines sur un réseau en deux parties dont la première sera un identificateur de sous-réseau. Ainsi un seul réseau de classe B, sur lequel on pourrait nommer 65536 machines pourra être décomposé en 254 sous-réseaux de 254 machines.



Pour l'Internet, il n'existe q'un seul réseau 128.10.0.0 et tous les routeurs traitent les datagrammes à destination de ce réseau de la même façon. Par contre, le routeur R se sert du troisième octet (égal à 1 ou 2) de l'adresse contenue dans les datagrammes qui lui proviennent pour les diriger vers le sous-réseau auquel ils sont destinés assurant ainsi un routage hiérarchique.

0 31

NetID	HostID		Ancienne adresse IP
Partie Internet	Partie locale		
Partie Internet	Sous réseau	Machine	Nouvelle adresse IP

Le choix du nombre de bits représentant l'identificateur de sous réseaux est laissé à l'administrateur local. Si ce nombre est fixe pour tous les sous-réseaux, on parle alors de sous adressage fixe, sinon on parle de sous adressage variable. Le sous adressage variable est utilisé dans le cas ou une entreprise par exemple compte à la fois de petits réseaux et de grands réseaux. Dans l'adressage fixe (utilisé souvent), on doit faire un compromis entre le nombre de réseaux et le nombre de machines.

Nombre de bits de sous réseau	Nombre de sous réseau	Nombre d'hôtes
2	2	16382
3	6	8190
4	14	4094
.	.	.
.	.	.
.	.	.

- Les masques de sous réseaux

Le standard TCP/IP indique q'un site qui utilise le subnetting doit choisir un masque (subnet mask) pour chaque sous réseau qui sera enregistré sur chaque machine. Le masque

permet à une machine de connaître le nombre de bits attribués à l'identificateur du sous-réseau et à celui de la machine.Un masque de sous réseau est un mot de 32 bits contenant des bits à 1 au lieu de l'identificateur de réseau et de sous-réseau et des bits à 0 au lieu de l'identificateur de machines.

Exemples de masques

11111111	11111111	11111111	00000000
Réseau			Hôte
255	255	255	0

11111111	11111111	11110000	00000000
Réseau			Hôte
255	255	240	0

11111111	11111111	11111111	11110000
Réseau			Hôte
255	255	255	240

- Appartenance d'une machine à un sous réseau

Donc, à partir de l'adresse d'un datagramme et de son masque de sous-réseau une machine peut déterminer si le datagramme est destiné à une machine sur son propre sous-réseau, à une machine sur un autre sous-réseau de son réseau ou à une machine extérieure à son sous-réseau.

Pour vérifier que la machine d'adresse IPDest appartient au sous-réseau d'adresse IPRes ayant le masque N, on calcule

$$V = IPdest \wedge N$$

Si $V = IPres$ alors la machine se trouve dans le même sous réseau et les messages lui sont envoyés, sinon les messages sont envoyés à une passerelle (routeur) qui les transmet au reste du réseau qui se charge de les acheminer vers leur destination.

Par exemple, dans le cadre du réseau présenté au debut de cette section où le masque de sous-réseau est 255.255.255.0 supposons que notre machine soit celle identifiée par l'adresse IP 128.10.1.2 (H2).

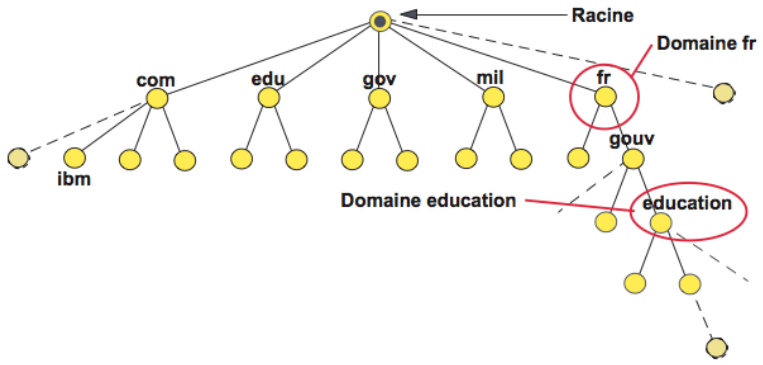
– Si l'adresse de destination est 128.10.1.1, un "et" entre la représentation binaire de cette adresse est de celle du masque de sous-réseau donne 128.10.1.0 à savoir l'adresse du sous-réseau de notre machine, donc le datagramme est destiné à une machine de ce même sous-réseau.

– Si l'adresse de destination est 128.10.2.1, un calcul du même genre donne 128.10.2.0 c'est-à-dire l'adresse d'un autre sous-réseau du même réseau.
– Si l'adresse de destination est S.T.U.V (avec (S,T) $\neq$ (128,10)) le résultat sera l'adresse d'un réseau différent de celui auquel appartient notre machine.

6.1.2 Nommage

La notion de nommage est complémentaire de celle d'adressage, l'un désigne l'objet, l'autre précise sa localisation. Indépendamment qu'il est plus aisé de manipuler des noms que des adresses, l'avantage du nommage est essentiellement de dissocier l'objet de sa localisation géographique. Le déplacement de l'objet nommé est transparent à l'utilisateur. De manière similaire à l'adressage, le nommage utilise deux modes de représentation :

– Le nommage à plat ou horizontal, ce type de nommage impose une démarche rigoureuse pour garantir l'unicité d'un nom sur l'ensemble du réseau. NetBios, protocole allégé mis en œuvre dans les réseaux locaux, utilise un nommage à plat.
– Le nommage hiérarchique ou arborescent, plus souple, organise le nommage en domaines. Cette technique autorise une représentation des objets calquée sur l'organisation de l'entreprise. Chaque nœud peut être un domaine dont la gestion peut être confiée à une autorité particulière. Ce mode de représentation et d'administration convient parfaitement à la gestion d'un annuaire très important comme celui d'Internet.



DNS (Domain Name System) est un système d'annuaire permettant de faire la correspondance entre le nom symbolique et l'adresse IP. Les serveurs de noms, ou serveurs DNS, sont des machines qui assurent la traduction des noms en adresses IP et réciproquement. On parle de résolution d'un nom ou d'une adresse. Pour cela, ils possèdent des informations sur l'architecture de l'arbre et sur les données associées.

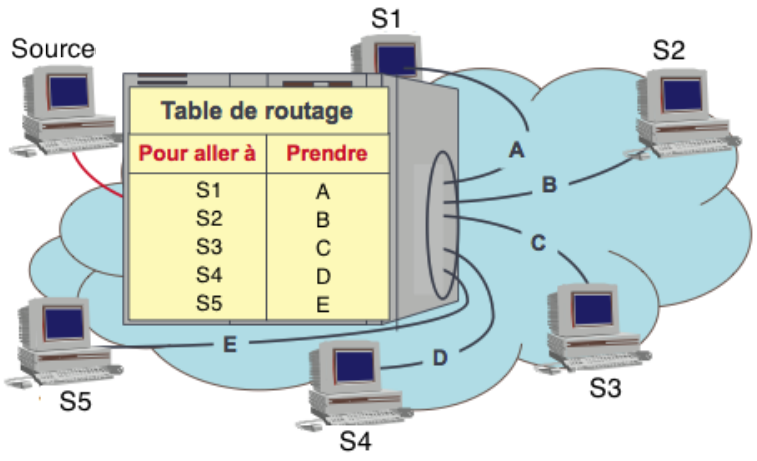
6.2 Routage

6.2.1 Principe

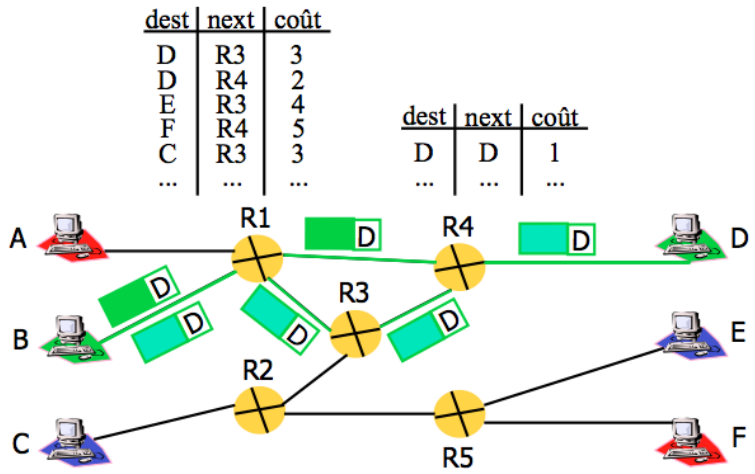
Le but du routage est la détermination d'un chemin à travers le réseau entre une machine émettrice et une machine réceptrice, toutes deux identifiées par leur adresse. Les protocoles de routage établissent des règles d'échange entre routeurs pour mettre à jour leurs tables d'informations selon des critères 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

En général des types de routage existent :

6.2.2 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

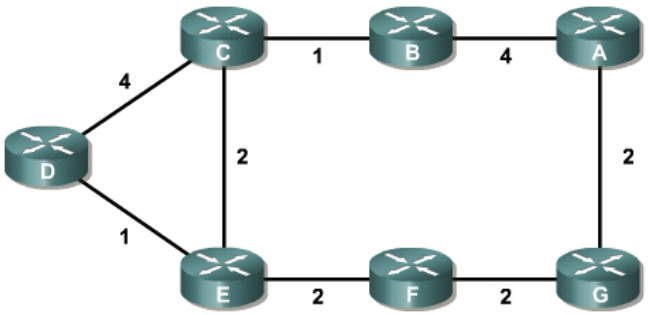
réseaux dans lesquels le choix de la route est limité (routes rentrées manuellement). Cependant, il assure le séquencement des paquets même en mode non connecté car tous les paquets prennent la même route.

Deux variantes de routage statique sont utilisées :

6.2.2.1 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.

6.2.2.2 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.

6.2.3 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.

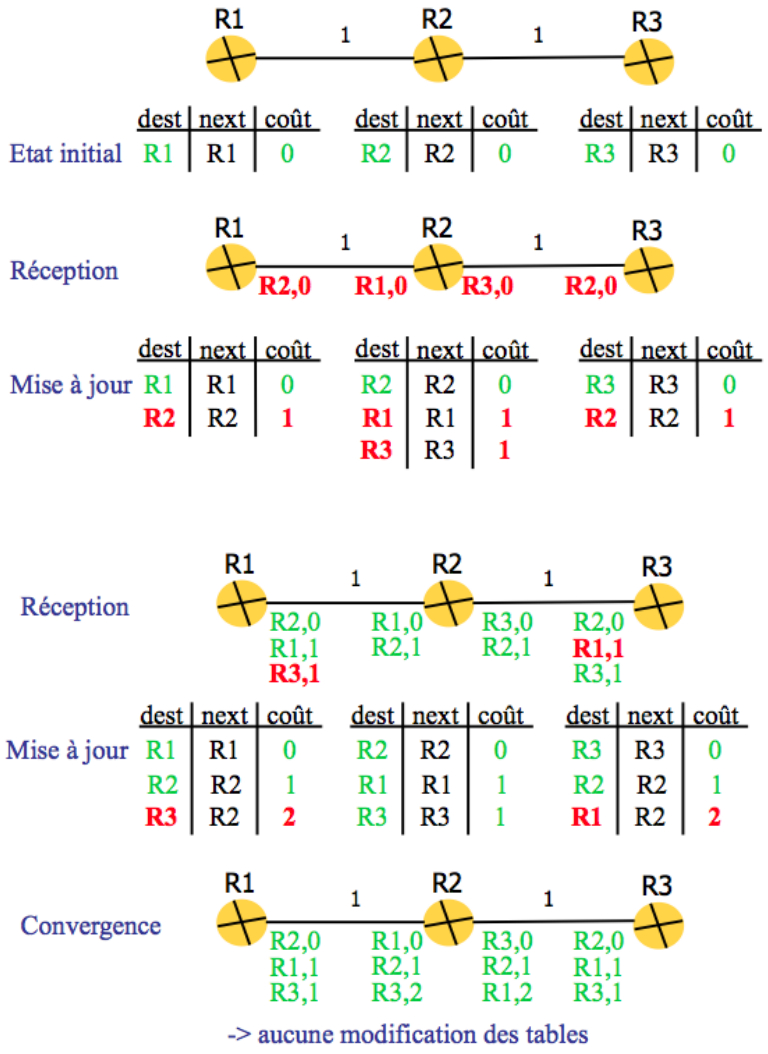
Il existe trois algorithmes de routage dynamique :

6.2.3.1 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 :

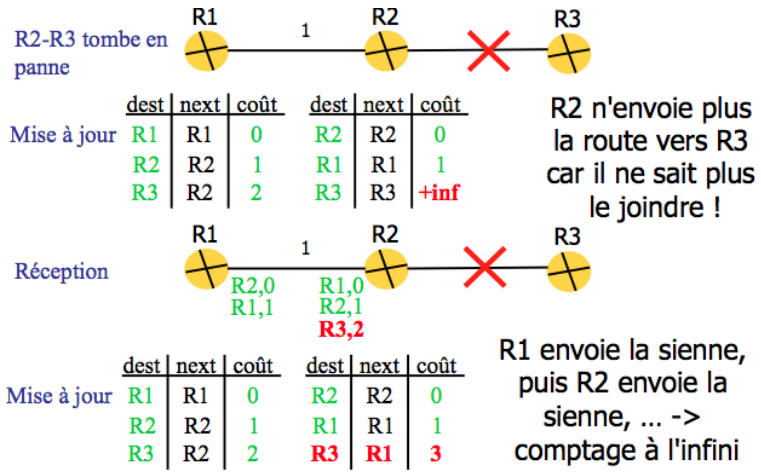
- La table reçue contient une entrée qui n'est pas déjà dans sa propre table, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette entrée dans sa table. Il a ainsi appris une nouvelle destination.
- La table contient une entrée qu'il connaît 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

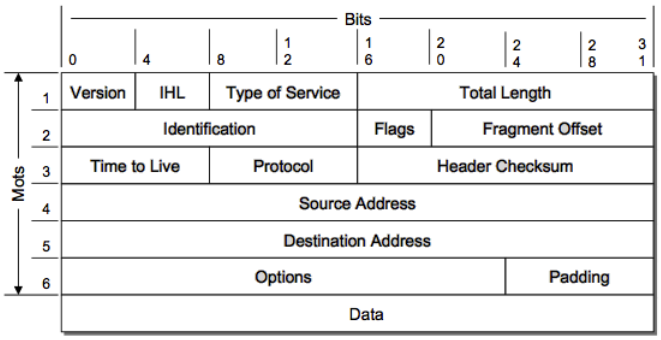
6.3 Protocole IP

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.

6.3.1 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.

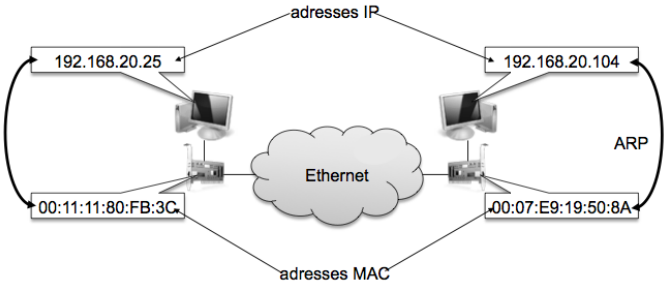
Plusieurs autres protocoles sont utilisés avec le protocole IP dans la couche réseaux notamment :

6.3.2 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.

6.3.3 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.

6.3.4 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.

6.3.5 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.

6.3.6 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.

6.4 Exercices

Exercice 1 Adresses IP

1. Déterminer les classes des adresses IP suivantes. En déduire les identifiants de réseau et de machine correspondants.

   192.18.97.39 (www.javasoft.com), 138.96.64.15 (www.inria.fr), 18.181.0.31 (www.mit.edu), 226.192.60.40, 91.216.107.152

2. Dites si les adresses IP suivantes sont correctes ou fausses. Justifier votre réponse.

   192.168.262.10, 200.30.1.5.2, 1.12.200.13, 55.255.255.255, 153.12.6, 172.24.15.7, 0.0.0.0

3. Dites si les adresses IP suivantes sont utilisables pour adresser des machines sur Internet. Justifier votre réponse.

   205.0.0.1, 192.168.104.0, 127.17.128.2, 172.125.38.224, 172.217.23.196, 10.148.255.255, 195.14.172.255, 128.0.143.2