TCP/IP

1 Introduction à Tcp/Ip

1.1 Introduction

Les réseaux d'ordinateurs ont pris peu à peu une importance considérable dans la vie de tous les jours. La plupart des informations peuvent prendre un format électronique, ce qui permet de les échanger facilement avec d'autres utilisateurs. Afin de pouvoir échanger ces informations, il est nécessaire de connecter les ordinateurs entre eux. Une fois reliés, il forment un réseau ou Lan (Local Area Network).

Si on relie plusieurs Lan entre eux, on obtient l'Internet un Wan (Wide Area Netwok). L'Internet (INTERconnexion NETwork) est le plus grand Wan conçu par l'homme. Les particuliers ont accès à ce réseau par l'intermédiaire d'un FAI (Fournisseur d'Accès Internet).

Nous allons étudier les réseaux utilisant la technologie TCP/IP. D'autres protocoles ont étés créés (IPX/SPX, AX25, DEC), mais TCP/IP est actuellement le plus utilisé pour plusieurs raisons :

- Le protocole est libre.
- Interopérabilité.
- Snmp.

1.2 Vue d'ensemble

Parler de TCP/IP, c'est parler de différents concepts. On pourrait grossièrement traduire TCP/IP par : « Protocole de communication pour la transmission de données ».

TCP : Transmission Control Protocol.
IP : Internet Protocol.

Un protocole de communication est un ensemble de règles permettant à plusieurs ordinateurs de dialoguer entre eux. A la manière des humains, les ordinateurs doivent parler le même langage afin de se comprendre. Tcp/Ip recouvre toute une famille de protocoles :

- UDP : User Datagram Protocol
- FTP : File Transfert Protocol
- TELNET : Terminal Emulation Protocol
- HTTP : Hyper Text Transfert Protocol
- ...

1.3 Historique

Dans les années 70, la DARPA (Defense Advanced Research Project Agency) possédait plusieurs réseaux d'ordinateurs de marques différentes, qui ne pouvaient dialoguer qu'avec d'autres ordinateurs de même marque.

Pour résoudre ces problèmes, le ministère de la Défense demanda à la DARPA de définir une famille de protocoles pour :

- Simplifier les communications : grâce à un jeu de protocoles, tous les appareils pourraient communiquer entre eux.
- Développer la compétition entre les différentes sociétés informatiques.
- Efficacité et productivité : Le fabricants consacrent du temps à l'implémentation des protocoles et non à leur développement.

En 1969, une première expérimentation permit de relier les 4 sites suivants :
Université de Californie de L.A., Santa Barbara, Utah, et le SRI Internationnal. Cette expérience vu le début du projet ARPANET (Advanced Research Project Agency Network). L'expérience fut un succès, et d'autres sites se sont intégrés à ce réseau.

En 1972, Une démonstration reliait 50 noeuds et 20 hôtes

Noeud : Nom générique donné à tout périphérique relié à un réseau.
Hôte : Ordinateur « puissant » sur lequel viennent se connecter des stations.

Serveur : Machine sur laquelle tourne un logiciel serveur offrant des services à un logiciel utilisateur nommé Client.

Arpanet continua de se développer et en 86, il englobait la plupart des grandes universités nord-américaines, le réseau militaire MILNET et d'autres centres de recherche internationaux. Peu à peu, le réseau ARPANET fut remplacé par l'Internet. Celui-ci dépassa le domaine exclusif des universités et passa très vite dans le domaine commercial. Actuellement, la communauté Internet regroupe à la fois des organisations commerciales et de simples utilisateurs. On y trouve les universités, les organismes de recherche, les fournisseurs d'accès, les institutions et les utilisateurs.

Initialement TCP/IP a été implémenté sous Unix BSD 4.2. Ce système a constitué une version de base d'unix, ce qui explique sa popularité.

1.4 Vue d'ensemble des applications Tcp/Ip

Tcp/Ip est non seulement une pile de protocoles permettant la remise de paquets et la gestion de la connexion, mais aussi un ensemble d'applications réseau.

- Telnet : Terminal Emulation Protocol
- Ftp : File Transfert Protocol
- Smtp : Simple Mail Transfert Protocol
- Snmp : Simple Network Management Protocol
- Nfs : Network File System
- Http : Hyper Text Transfert Protocol
- Dns : Domain Name System

1.5 Rfc

Afin de faire circuler les nouvelles idées sur les protocoles, la recherche et les standards, on commença d'abord à utiliser les Rfc (Request For Comments). Quand un chercheur définit un nouveau protocole, il propose ses recherches dans une Rfc. Ainsi, les Rfc consistent en définitions des standards de l'Internet, propositions pour de nouveaux protocoles, stratégies d'implémentation, etc.

Les protocoles qui peuvent devenir un standard de l'Internet passent par une série d'états qui décrivent leur niveau de maturité. Ces niveaux sont la proposition, le brouillon et le standard. Quand un protocole passe les 3 niveaux, un n° Std lui est attribué.

2 Un réseau en couches

2.1 Introduction

Les applications Tcp/Ip utilisées par les intranets et l'Internet dépendent de plusieurs couches de protocoles. Le terme couche de protocole suggère qu'il y a interaction entre les différents protocoles. Chaque couche de protocoles interagit avec la couche suivante grâce à une interface spécifique.

Construire des systèmes, comme des protocoles, en les disposant en couches présente plusieurs avantages. Chaque couche peut-être définie précisément pour effectuer une fonction bien particulière. La couche représente en quelque sorte une boite noire à qui l'on fournit des données, qui les traite et les propose à la couche suivante. Ainsi, grâce à ses traitements, on peut présenter les données dans un format particulier, acheminer ces données de façon fiable à travers le réseau, choisir une route optimale pour ces données, etc.

En séparant les fonctions des couches de l'implémentation, on peut modifier certaines caractéristiques d'une couche sans toucher aux autres.

2.2Principe des couches de protocoles

2.2.1 Le modèle OSI Open System Interconnexion

Développé en 1978 par l'ISO (Internationnal Organization of Standards) afin que soit défini un standard utilisé dans le développement de systèmes ouverts.

Chaque couche, excepté la 1^{ere} et la dernière, utilise les services de la couche inférieure et propose des services à la couche supérieure.

Il est composé de 7 couches :

1 Couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

2 Couche liaison de données

Son rôle est un rôle de "liant". Elle va transformer la couche physique en une liaison à priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. Rappelons que pour la couche

physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.
La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.
L'unité d'information de la couche liaison de données est la trame qui est composées de quelques centaines à quelques milliers d'octets maximum.

3 Couche réseau

C'est la couche qui permet de gérer le sous-réseau, le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).
La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat.
L'unité d'information de la couche réseau est le paquet.

4 Couche transport

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le ré-assemblage du message à la réception des morceaux.
Cette couche est responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois...
Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau.
Un des tous derniers rôles à évoquer est le contrôle de flux.
C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.
L'unité d'information de la couche réseau est le message.

5 Couche session

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

6 Couche présentation

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.
Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

7 Couche application

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

2.2.2 Le modèle DoD Department of Defence

Tcp/Ip a été historiquement créé à la demande du ministère de la Défense des États-Unis, c'est pourquoi le modèle garde ce nom.

1 Couche accès réseau

La couche la plus basse représente la connexion physique avec les câbles, les circuits d'interface électrique, les cartes réseau, les protocoles d'accès au réseau (Carrier Sense Multiple Access / Collision Detection pour les réseaux éthernet et le jeton pour les réseaux Token Ring). La couche accès réseau est utilisée par la couche Internet.

2 Couche Internet

La couche Internet doit fournir une adresse logique pour l'interface physique. C'est la couche Ip qui assure ce travail. Elle fournit un mappage entre l'adresse logique et l'adresse physique fournit par la couche accès réseau grâce aux protocoles Arp (Address Resolution Protocol) et Rarp. Les incidents et les diagnostics associées au protocole Ip relèvent du protocole Icmp (Internet Control Message Protocol), qui opère aussi au niveau de la couche internet.

Elle est aussi responsable du routage des paquets entre les hôtes. (Routing Information Protocol et Open Shortest Path First).

3 Couche Transport de hôte à hôte

La couche hôte à hôte définit les connexions entre 2 hôtes sur le réseau. Le modèle DoD comprend 2 protocoles TCP, Transmission Control Protocol et UDP, User Datagram Protocol. Le protocole Tcp est responsable du service de transmission fiable de données avec détection et correction d'erreurs. Il permet des connexion full-duplex dans une seule connexion. Udp est employé quand le volume de données est très faible. En cas de non réponse, on ré-émet tout simplement le paquet.

4 Couche Application

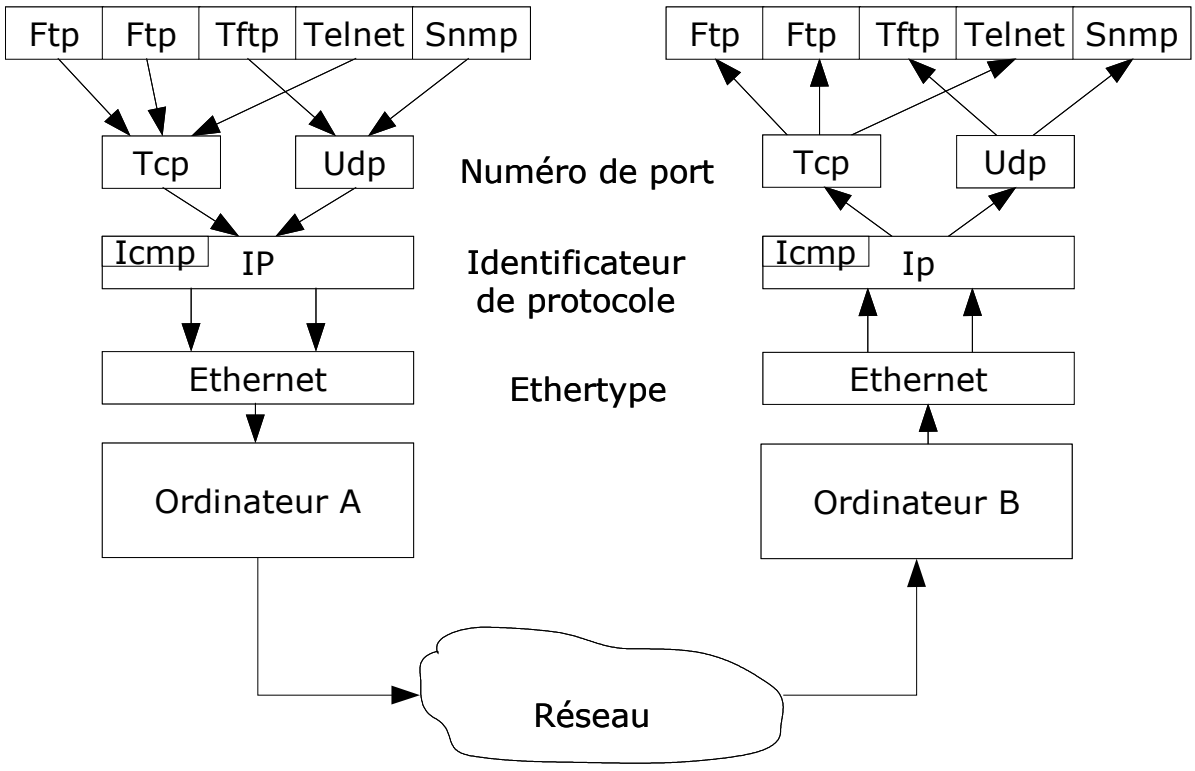
Elle permet aux applications d'utiliser les protocoles de la couche transport. On trouve les mêmes application que dans le modèle Osi.

Osi		Dod		Unités	Équipement
Application	7	4	Application	Message	Passerelle
Présentation	6				
Session	5				
Transport	4	3	Transport de hôte à hôte	Segment	
Réseau	3	2	Internet	Datagramme	Routeur
Liaison de données	2	1	Accès réseau	Trame	Pont
Physique	1			Bits	Répéteur

2.3 Hiérarchie de l'implémentation de Tcp/Ip

La suite de protocoles Tcp/Ip comprend un ensemble performant de services qui peuvent utiliser un grande variété de technologies réseau comme les réseaux étendus, les réseaux locaux, les ondes radio, les satellites ou les lignes numéris. Les modules du protocole Tcp/Ip et les relations entre ces modules forment la hiérarchie de l'implémentation Tcp/Ip.

2.4 Multiplexage et démultiplexage de protocoles



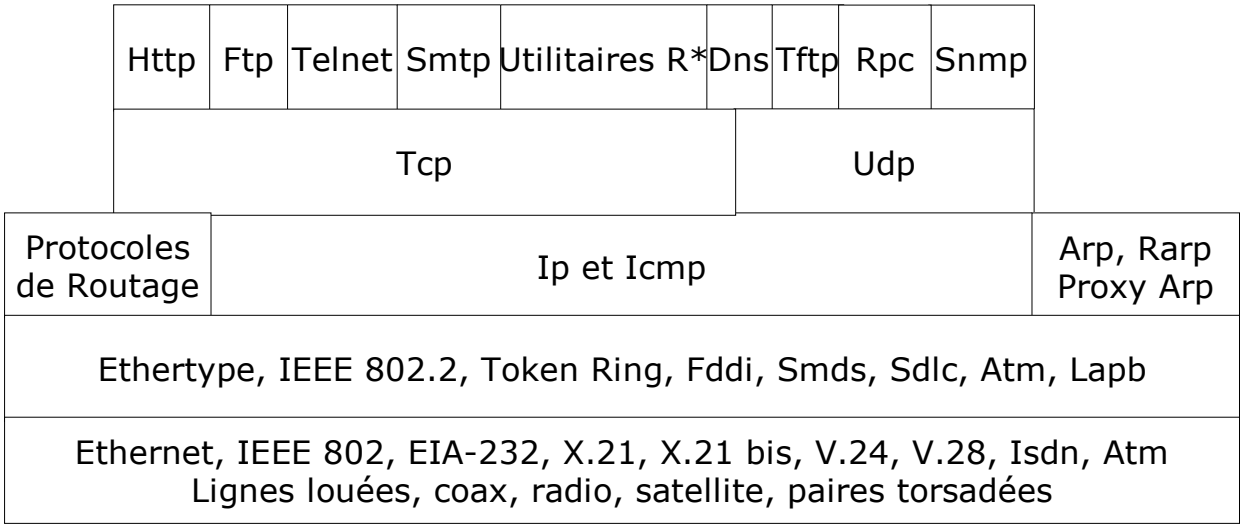
Plusieurs sessions existent entre les hôtes A et B. Comment les logiciels sur chaque hôtes arrivent-ils à différencier les divers protocoles ou applications au niveau d'une couche donnée?

Le réseau ci-dessus montre un environnement supportant Ip et Icmp. Comment savoir si un paquet sortant du réseau est destiné à Ip ou Icmp ? Pour résoudre ce problème, la trame éthernet contient un champ de 2 octets : Ethertype utilisé par les protocoles de la couche réseau.

Le champ Ethertype de la couche liaison de données autorise le multiplexage de plusieurs protocoles réseau au niveau de la source, et le démultiplexage au niveau de la destination.

Quand la couche Ip reçoit un paquet éthernet, elle doit distinguer les paquets pour Tcp ou Udp grâce à un champ d'identification du protocole de 8 bits situé dans le paquet. Plusieurs implémentations de Tcp/Ip stockent ces valeurs dans un fichier : /etc/protocols.

De la même manière, quand un module Tcp ou Udp reçoit un paquet de la couche Ip, il doit distinguer l'application qui traitera ce paquet. Chaque paquet contient un champ de 16 bits indiquant le numéro du port correspondant à l'application.
Fichier : /etc/services.



2.6 Tcp/Ip et système d'exploitation

Les performances de Tcp/Ip, sa configuration et sa facilité de maintenance dépendent du système d'exploitation sur lequel il est implémenté. En théorie, le système n'est pas nécessaire pour faire tourner Tcp/Ip : il peut être implémenté en Rom. Toutefois, la plupart des implémentations commerciales de Tcp/Ip interagissent avec le système.

Ces interactions entre Tcp/Ip et système peuvent être classés de la façon suivante :

- comme faisant partie du noyau (kernel)
- comme un pilote de périphérique
- comme un processus d'application

Dans un système comme Unix ou Netware, Tcp/Ip est implémenté dans le kernel du système. Cette implémentation permet d'obtenir des fonctions de communication très rapides.

Les systèmes dont l'implémentation de Tcp/Ip est faite sous forme de pilote de périphérique comprennent Windows Nt et Windows 3.11, 95, 98, et Me, Vms, Os/2 et Ms-Dos.

Les systèmes qui implémentent Tcp/Ip sous forme de processus comprennent les systèmes des mainframes Ibm, Mvs.

3 Vue d'ensemble des applications TCP/IP

3.1 Modèle client / serveur

La plupart des applications TCP/IP fonctionnent sur le modèle client / serveur. Un serveur est une machine TCP/IP sur laquelle tourne un logiciel serveur qui a pour rôle principal d'attendre un message de la part d'un client. Il analyse la requête du client, formate sa réponse et la renvoie au client. L'exemple typique est le navigateur web, qui demande au serveur de lui envoyer une page. La demande se fait sous la forme d'une chaîne de caractères : « http://www.google.fr/index.html ». Le serveur (en l'occurrence la machine qui a pour nom « www » dans le domaine « google.fr ») renvoie le contenu de la page « index.html » (<html><body> ... </html></body>), et le logiciel client l'interprète et l'affiche en retour.

3.2 Telnet (Terminal Emulation Protocol)

Telnet permet à un utilisateur de se connecter à distance sur un hôte. L'utilisateur travaille sur l'hôte distant comme s'il était directement connecté dessus. Les séquences de touche tapées sur l'ordinateur sont envoyées à l'hôte qui les interprète et renvoie les réponses à l'ordinateur appelant.

3.3 Ftp (File Transfert Protocol)

Ftp permet de transférer des fichiers entre deux machines sur un réseau TCP/IP. Le client se connecte au serveur distant et établi une session interactive. Il peut alors visualiser les fichiers et les répertoires distants et lancer des commandes de transfert.

3.4 Smtp (Simple Mail Transfert Protocol)

Smtp permet à un utilisateur d'envoyer un message à un destinataire connecté à un réseau TCP/IP. Le message est composé sous forme de texte, et l'utilisateur tape l'adresse électronique du destinataire, l'objet du message et le texte lui-même. Smtp utilise TCP/IP pour envoyer ce message à un serveur de messagerie. Les serveurs de messagerie agissent comme des relais et délivrent leurs messages au destinataire.

3.5 Snmp (Simple Network Management Protocol)

Snmp permet la gestion à distance de périphériques tels que les ponts, routeurs ou switchs. Un agent snmp doit tourner sur ces périphériques. Une station Snmp envoie des requêtes pour lire ou modifier les paramètres d'un périphérique. Il utilise UDP et IP.

3.6 Dns (Domain Name System)

Dns constitue un annuaire électronique permettant de nommer les différentes ressources d'un réseau. Dns associe les noms des périphériques à leur adresse IP. Par exemple l'hôte www.google.com à pour adresse IP : 216.239.51.101. Les noms Dns jouent un rôle prépondérant dans tous les protocoles TCP/IP, car ils permettent de travailler avec des mots plutôt que des chiffres.

3.7 Http (Hyper Text Transfert Protocol)

Http est un protocole permettant d'envoyer des pages web à un ordinateur équipé d'un navigateur. Ce navigateur peut lire des documents textes, graphiques, audio ou vidéo.

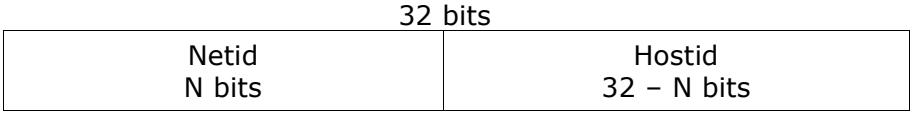
4 L'adressage IP

Une des tâches fondamentale lors de la mise en place d'un réseau TCP/IP consiste à affecter des adresses Internet aux noeuds du réseau. Ce sont les adresses IP. Si l'affectation des adresses IP peut sembler facile à première vue, il est nécessaire de prendre en considération un certain nombre de points. Pour que l 'ensemble soit cohérent et puisse fonctionner, tous les périphériques doivent avoir une adresse unique. De plus, afin de pouvoir communiquer avec les autres noeuds, il est indispensable que ces adresses soient cohérentes entre elles.

La base de l'adressage dans un réseau TCP/IP est l'adresse de la carte réseau (adresse MAC). Elle est inscrite en dur dans le programme implémenté. Pour de nombreuses raisons (changement de carte réseau, facilité de groupage de mêmes types d'adresses), la décision fut prise de mettre en place un système d'adressage logique indépendant au dessus des adresses physiques.

4.1 Structure de l'adresse IP

La vision logique de l'Internet créé un réseau virtuel. Chaque connexion de réseau à ce réseau virtuel est identifié de manière distincte au moyen d'une adresse IP. Les concepteurs de TCP/IP ont choisi un adressage sur 32 bits. Le nombre maximal de connexions est donc de 2^32, soit 4 296 967 296. Comme nous le verrons, le nombre maximal effectif de connexions est moindre car certaines adresses ont des significations réservées et ne peuvent être attribuées à des hôtes. Le réseau virtuel est constitué de réseaux reliés entre eux par le biais de périphériques tels que routeurs ou passerelles. Afin d'aiguiller les datagrammes IP, les routeurs doivent être en mesure de distinguer différent réseaux logiques. On a donc décidé de structurer l'adresse IP de façon à ce qu'elle puisse refléter la distinction entre les différents réseaux logiques. Un certain nombre de bits dans l'adresse IP sont utilisés pour identifier le réseau individuel dans le réseau virtuel, et les bits suivants permettent d'identifier l'hôte au sein du réseau.



La méthode consistant à partager l'adresse IP entre un numéro de réseau et un numéro d'hôte constitue un plan d'adressage hiérarchique, ce qui permet de rendre le routage beaucoup plus efficace. La fonction première d'un routeur est d'envoyer un datagramme IP dans au réseau idoine. A cet effet, les routeurs doivent stocker les informations concernant les Netids et non les Hostids. Le nombre de Netids est forcément inférieur aux Hostids, ce qui maintient à un nombre raisonnable la quantité d'informations qu'un routeur doit connaître. Si l'on n'avait pas établit cette distinction entre Netid et Hostid (en choisissant un système d'adressage plat, plutôt qu'un plan d'adressage hiérarchique), les routeurs auraient dû stocker les quatres milliards d'adresses IP.

A partir du nombre de 32 bits utilisé pour l'adresse IP, les concepteurs ont décidé que l'on utiliserait le premier, les 2 premiers ou les 3 premiers octets comme Netid.

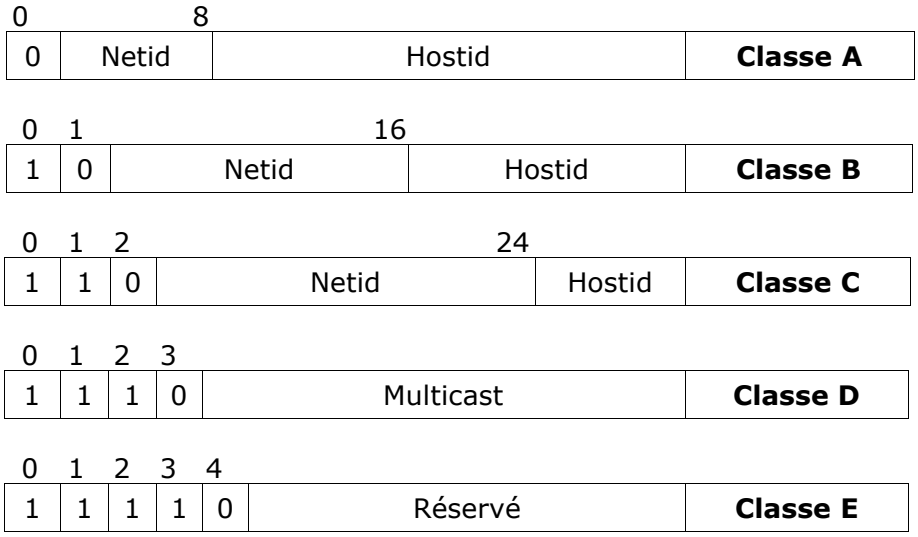
Rappel : 1 octet est constitué de 8 bits. Attention à la confusion avec l'anglais.
bit en français = **bit** en anglais alors que
octet en français = **byte** en anglais

Netid	Hostid	Classe
1 octet	3 octets	A
2 octets	2 octets	B
3 octets	1 octet	C

L'adresse IP est partitionnée en une paire Netid/Hostid alignée à l'octet. On obtient ainsi 3 classes d'adresses. Cette alignement à l'octet vient d'une volonté de simplicité, mais on aurait très bien pu partitionner l'IP en s'alignant au bit.

Comment distinguer les différents formats d'adresses ? Les bits les plus significatifs permettent de déterminer le format de l'adresse IP, c'est à dire le nombre de bits utilisés pour le Netid et le Hostid.

En plus des 3 classes A, B et C, deux autres classes sont définies. On peut affecter des adresses de classe A, B ou C, tandis que la classe D est réservée à la multidiffusion (multicast), technique utilisée par des protocoles spéciaux pour transmettre simultanément des messages à un groupe donné de noeuds différents. La classe E est réservée à un usage ultérieur.



Pourquoi utiliser des classes d'adresses spécifiques ?

Les différents types de classes d'adresses IP sont définis pour répondre aux besoins des réseaux de différentes tailles. Sur demande, l'autorité d'enregistrement du réseau affecte un numéro de réseau (Netid) à une organisation. Une fois ce numéro alloué à une organisation, il incombe à cette dernière d'affecter les numéros d'hôte (Hostid).

Classe	Nombre de réseaux	Nombre de noeuds
A	127	16777214
B	16383	65534
C	2097151	254

Notation décimale à points pour les adresses IP

Pour simplifier les choses, on représente le nombre à 32 bits sous forme de 4 nombres décimaux correspondants à la valeur décimale des 4 octets qui composent l'adresse. Les nombres sont séparés par des points.

Adresse IP : 10010000 00010011 01001010 11001001
144 . 19 . 74 . 201

Calcul d'une classe d'adresse

Ce tableau donne la classe d'une adresse en fonction de son 1er octet (décimal).

Classe	Minimum	Maximum
A	0	126
B	127	191
C	192	223
D	224	239
E	240	247

Adresse réservées

Pour chaque classe, 2 adresses sont réservées et ne peuvent être utilisées. Ce sont l'adresse du réseau lui-même et l'adresse de diffusion dirigée (broadcast).

Classe	Netid	Réseau	Diffusion
A	X.Y.Z	0	255
B	X.Y	0.0	255.255
C	X	0.0.0	255.255.255

255.255.255.255 : diffusion limitée : tous les ordinateurs de ce réseau.

0.0.0.0 : correspond à Netid 0 : le réseau d'ici
Hostid 0 : le noeud d'ici

Cette adresse (0.0.0.0) est généralement utilisée par un hôte qui essaye de déterminer sa propre adresse, par l'intermédiaire du protocole Bootp ou Dhcp.

On utilise aussi cette adresse dans les tables de routage pour indiquer l'adresse d'entrée du routeur (passerelle par défaut).

127.X.Y.Z : Bouclage logiciel (loopback)

Tout paquet envoyé par une application TCP/IP vers une adresse de type 127.X.Y.Z à pour conséquence le renvoi de ce paquet à l'application sans que le paquet n'atteigne le support du réseau. Le paquet est copié du buffer de transmission sur le buffer de réception de la machine elle-même. L'adresse de bouclage permet de vérifier rapidement que la pile TCP/IP est correctement configurée. Elle est aussi utile lorsqu'un

logiciel client et un logiciel serveur s'exécute sur la même machine. On peut accéder au serveur en utilisant cette adresse. Ex : telnet 127.0.0.1

Lorsque qu'un paquet est envoyé à une adresse IP individuelle, on dit qu'il s'agit d'un paquet UNICAST.

Lorsque qu'un paquet est envoyé à tous les noeuds d'un réseau spécifique, on dit qu'il s'agit d'un paquet de diffusion (BROADCAST).

Enfin, lorsque qu'un paquet est envoyé à une adresse de classe D, on parle de MULTICAST. Tous les hôtes ayant cette adresse, en supplément de leur adresse IP classique, reçoivent ce paquet. Le protocole qui utilise cette technique est appelé IGMP (Internet Group Management Protocol).

Réseaux privés

Pour réduire le besoin en nouvelles adresses, un groupe d'adresse par classe à été réservé. Ce sont les adresses privées.

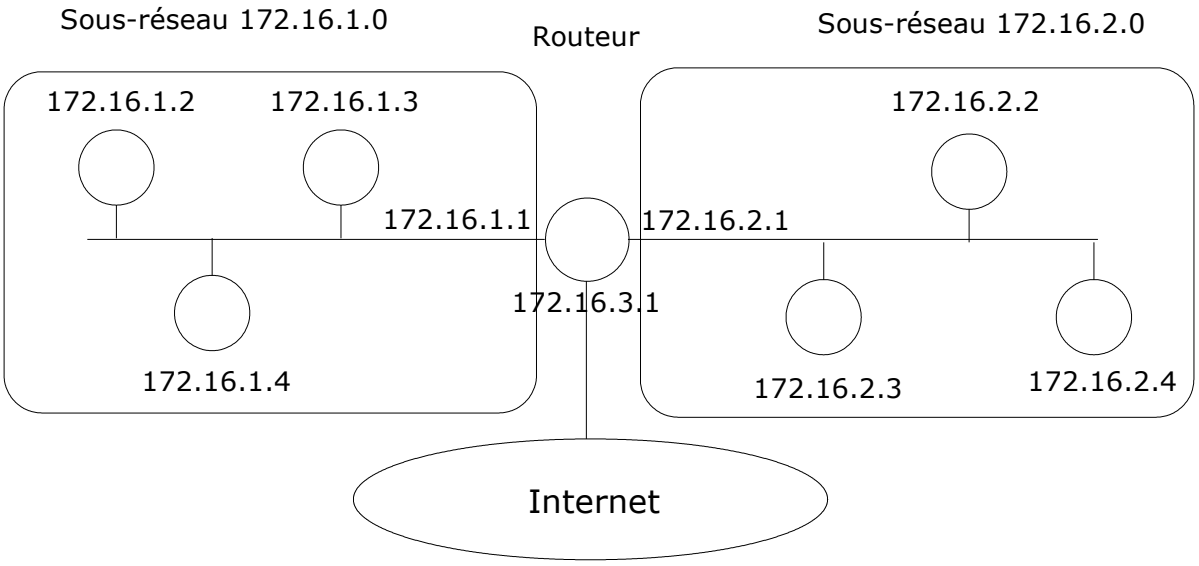
10.0.0.0	10.255.255.255	1 réseau de classe A
172.16.0.0	172.31.255.255	16 réseaux de classe B
192.168.0.0	192.168.255.255	256 réseaux de classe C

Elle ne sont pas routées sur l'internet. Afin de pouvoir sortir du réseau, on doit employer un proxy, passerelle NAT (Network Address Translation) ou tout autre équipement permettant l'utilisation de l'adresse publique de cet équipement.

5 Sous-réseaux

Les formats d'adresse Ipv4 ont étés conçus pour s'adapter à des réseaux de différentes tailles. Ces format convenaient bien dans les premiers temps de l'internet. La principale faiblesse du format Ipv4 réside dans le gâchis d'espace d'adressage consécutif à la conception d'un interréseau.
Pour pallier à ce défaut, la RFC 950 a défini et normalisé le concept de sous-réseau en 1985. Les sous-réseaux permettent d'utiliser un numéro de réseau unique pour construire plusieurs réseaux interconnectés. Le préfixe de numéro de réseau est partagé entre plusieurs réseaux appelés sous-réseaux. Cette mise en sous-réseaux est généralement utilisée lorsque le même numéro de réseau est utilisé pour plusieurs réseaux interconnectés.
De la même manière, la mise en surréseau consiste à combiner plusieurs numéros de réseaux en un seul numéro de réseau logique qui peut être utilisé pour construire un réseau de plus grande taille. La mise en surréseau est utilisée le plus souvent pour combiner plusieurs adresses de classes C en une classe logique plus grande qu'une classe C mais plus petite qu'une classe B.

5.1 Sous-réseaux



Netid	Sous-réseau	Hostid
172.16	1	1
172.16	1	2
172.16	1	3
172.16	1	4
172.16	2	1
172.16	2	2
172.16	2	3
172.16	2	4

A partir d'un réseau de classe B (172.16.0.0), on décide de créer des sous-réseaux de plus petites tailles. Pour ce faire, il est nécessaire de partager le hostid. Une partie servira à identifier le sous-réseau, la deuxième à identifier l'hôte. Afin de pouvoir faire la différence entre ces 2 nouveaux champs, un nouveau concept à été inventé : le masque de sous-réseau. Il s'agit d'un nombre de 32 bits (comparable à l'adresse IP) ne contenant que des 1 ou des 0. Un bit à 1 indique que le bit correspondant dans l'adresse IP fait partie du Netid, un bit à 0 du Hostid.

172	16	1	1
10101100	00010000	00000001	00000001
11111111	11111111	11111111	00000000
255	255	255	0
Netid		Sous-réseau	Hostid

On obtient ainsi 254 sous-réseaux de 254 machines (256 – 2 adresses réservées).

Le masque de sous-réseau se note indifféremment : 255.255.255.0 ou /24 (Nombre de bits à 1).

Exemple :

Adresse IP : 128.12.34.71
Masque : 255.255.255.0

C'est une adresse de classe B car 128 est compris entre 128 et 191. Les 2 premiers 255 du masque correspondent aux 16 bits du champs Netid pour une classe B. Le 255 suivant doit donc correspondre au numéro de sous-réseau. En conséquence, le numéro de sous-réseau est 34, le numéro d'hôte 71 et l'adresse de broadcast 128.12.34.255.

5.2 Masque de sous-réseau non aligné à l'octet

Dans l'exemple précédent, le masque de sous-réseau était : 255.255.255.0. Ce qui assignait un octet au numéro de sous-réseau. Il est possible d'aligner le masque au bit, ce qui permet un découpage plus fin des sous-réseaux.

Exemple : Découper une classe C 192.168.1.0 en 4 sous-réseaux.

Combien de bits avons-nous besoin de réserver pour compter jusqu'à 4 ? 2 bits

Décimal	**Binaire**
0	0
1	1
2	10
3	11

Le masque aura donc la forme

255	255	255	192
11111111	11111111	11111111	11000000

Il nous reste 6 bits pour coder le hostid, c'est à dire : 2^6 soit 64 – 2 hôtes = 62.

Nous disposerons donc des sous-réseaux suivants :

Adresses utilisables	Dernier octet	Réseau	Broadcast
192.168.1.1 -> 192.168.1.62	00000001 -> 00111110	192.168.1.0	192.168.1.63
192.168.1.65 -> 192.168.1.126	01000001 -> 01111110	192.168.1.64	192.168.1.127
192.168.1.129 -> 192.168.1.190	10000001 -> 10111110	192.168.1.128	192.168.1.191
192.168.1.193 -> 192.168.1.254	11000001 -> 11111110	192.168.1.192	192.168.1.255

En alignant le masque de sous-réseau au bit, nous pouvons obtenir :

Masque	Dernier octet	Nombre de sous-réseaux	Nombre d'hôtes
255.255.255.128	10000000	2	128 – 2 = 126
255.255.255.192	11000000	4	64 – 2 = 62
255.255.255.224	11100000	8	32 – 2 = 30
255.255.255.240	11110000	16	16 – 2 = 14
255.255.255.248	11111000	32	8 – 2 = 6
255.255.255.252	11111100	64	4 – 2 = 2

6 Protocole de résolution d'adresse

Le plan d'adressage IP est un plan d'adressage logique conçu pour créer l'apparence d'un réseau virtuel. Toutes les interfaces du réseau sont modélisées par un unique identificateur à 32 bits, l'adresse IP. Toutefois, la transmission des datagrammes IP sur le réseau physique nécessite que ces datagrammes soient encapsulés dans des trames de la couche liaison de donnée (couche 2). Les trames de la couche liaison de donnée, telles que les trames éthernet ou d'anneaux à jeton, doivent connaître les adresses matérielles ou adresse MAC (Medium Access Control). Ces adresses sont codées en dur dans la carte réseau. Un pool d'adresses MAC est attribué à chaque fabriquant qui à la charge de les attribuer à ses carte réseau. Ainsi, il est théoriquement impossible que 2 cartes réseau aient la même adresse. Il est néanmoins possible de changer cette adresse grâce à un logiciel spécifique. Ce n'est naturellement pas conseillé.

Address Resolution Protocol (ARP)

Quand un hôte A veut envoyer un message à un hôte B, celui-ci ne connaît que son adresse IP. L'hôte A envoie sur le réseau une trame MAC de diffusion appelée trame ARP de requête. La trame contient les adresse IP et MAC de l'hôte A émetteur, ainsi que l'adresse IP de l'hôte B. Tous les noeuds du réseau physique reçoivent la trame de requête ARP de diffusion. Ces noeuds comparent leur adresse IP à l'adresse IP contenue dans la requête ARP. Seul l'hôte dont l'adresse IP correspond à l'adresse requise dans la trame de requête ARP répond.

Si l'hôte B existe sur le réseau, il répond en encodant sa propre adresse matérielle dans une trame de réponse ARP. L'hôte A initialise alors sa table de cache ARP (en mémoire) en utilisant la réponse fournie par la réponse ARP. Les entrées du cache ARP expirent après une temporisation donnée qui peut être configurée dans certaines implémentations de Tcp/Ip. Généralement, la temporisation du cache ARP est de 15 minutes. Une fois qu'une entrée de cache ARP pour un hôte donné a expiré, une nouvelle trame de requête ARP est envoyée pour découvrir l'adresse matérielle de l'hôte. Le cache ARP pour un hôte juste avant l'envoi d'une requête ARP. Si la réponse se trouve dans le cache, l'hôte peut ainsi se passer d'envoyer la requête.

La requête ARP est envoyée avec une adresse matérielle de diffusion car l'adresse matérielle n'est pas connue. La réponse ARP n'est pas une trame de diffusion. En effet, le noeud cible prend connaissance de l'adresse matérielle de l'émetteur en examinant le paquet ARP. La réponse ARP est par conséquent directement envoyée au noeud qui a émis la requête ARP.

La trame de requête ARP n'est pas routée.

7 Notion de port

Nous avons vu comment, grâce à Tcp/Ip et ARP, la pile de protocoles gérait les flux de communication entre différents hôtes sur un réseau. Mais Tcp peut servir simultanément à plusieurs processus de la même machine. Ces processus communiquent par la même interface réseau et partagent donc la même adresse IP que l'interface réseau, et l'adresse IP ne permet pas d'identifier un processus.

Tcp associe en fait un numéro de port à chaque application qui utilise ses services. Une telle association permet de distinguer les connexions Tcp entre les différents processus d'application se trouvant sur des machines distantes. A chaque connexion correspondra une paire de numéro de ports (client + serveur).

Le numéros de ports sont codés sur 16 bits, ce qui constitue un stock de 65536 ports. Les ports de 0 à 1024 sont appelés ports privilégiés car ils sont traditionnellement réservés à l'utilisateur root. Ils sont attribués en fait aux services serveurs d'une machine.

Concrètement, dans le cas d'une connexion entre un client http (navigateur) et un serveur web, le client établi cette connexion avec 4 informations primordiales :

Le client envoie une requête. La connexion s'établit entre d'une part :

- L'ip du client et un port x local supérieur à 1024 (en fait le premier port disponible sur le client) et d'autre part

- L'ip du serveur sur le port 80 (http)

Le serveur prépare sa réponse et la renvoie au client sur le port x.

Ces informations (adresse IP + numéro de port) constituent une socket, qui assure que chaque paquet circulant sur le réseau est unique et identifiable.

On a associé un port à chaque application. Cette liste est disponible sur la plupart des implémentation de Tcp/IP, dans le fichier /etc/services.

8 Routage

Le routage est la tâche consistant à trouver un chemin d'un émetteur à une destination souhaitée. Il se réduit essentiellement à trouver des routeurs entre des réseaux. Aussi longtemps qu'un message reste sur un réseau ou sous-réseau unique, tout problème de routage est résolu par une technologie qui est spécifique au réseau. Par exemple, Ethernet définit un moyen par lequel tout émetteur peut parler à toute destination spécifiée à l'intérieur de ce propre réseau. Le routage IP entre en jeu essentiellement quand les messages doivent aller d'un émetteur sur un tel réseau vers une destination située sur un autre réseau. Dans ce cas, le message doit traverser des routeurs connectant les réseaux. Si les réseaux ne sont pas adjacents, le message peut traverser plusieurs réseaux intermédiaires, et les routeurs les connectant. Une fois que le message arrive sur un routeur situé sur le même réseau que la destination, la technologie propre de ce réseau est utilisée pour atteindre la destination.

8.1 Les routeurs

Les routeurs sont les dispositifs permettant de "choisir" le chemin que les datagrammes vont emprunter pour arriver à destination.
Il s'agit de machines ayant plusieurs cartes réseau dont chacune est reliée à un réseau différent. Ainsi, dans la configuration la plus simple, le routeur n'a qu'à "regarder" sur quel réseau se trouve un ordinateur pour lui faire parvenir les datagrammes en provenance de l'expéditeur.

Toutefois, sur Internet le schéma est beaucoup plus compliqué pour les raisons suivantes:

- Le nombre de réseau auquel un routeur est connecté est généralement important.
- Les réseaux auquel le routeur est relié peuvent être reliés à d'autres réseaux que le routeur ne connaît pas directement.

Ainsi, les routeurs fonctionnent grâce à des tables de routage et des protocoles de routage, selon le modèle suivant:

- Le routeur reçoit des datagrammes provenant d'une machine connectée à un des réseau auquel il est rattaché.
- Les datagrammes sont transmis à la couche Internet.
- Le routeur regarde l'en-tête du datagramme.
- Si l'adresse IP fait partie du réseau duquel le datagramme provient, le routeur n'a aucune action à accomplir car la machine visée aura reçu ce même datagramme.
- Si l'adresse IP fait partie d'un réseau différent, le routeur consulte sa table de routage, une table qui définit le chemin à emprunter pour une adresse donnée.
- Le routeur envoie le datagramme grâce à la carte réseau reliée au réseau sur lequel le routeur décide d'envoyer le paquet.

Ainsi, il y a deux scénarios, soit l'émetteur et le destinataire appartiennent au même réseau auquel cas on parle de **remise directe**, soit il y a au moins un routeur entre l'expéditeur et le destinataire, auquel cas on parle de **remise indirecte**.

Dans le cas de la remise indirecte, le rôle du routeur et surtout de la table de routage est très important. Ainsi le fonctionnement d'un routeur est déterminé par la façon selon laquelle cette table de routage est créée.

- Si la table routage est entrée manuellement par l'administrateur, on parle de **routage statique** (viable pour de petits réseaux).
- Si le routeur construit lui-même la table de routage en fonctions des informations qu'il reçoit (par l'intermédiaire de protocoles de routage), on parle de **routage dynamique.**

8.2 La table de routage

La table de routage est une table de correspondance entre l'adresse de la machine visée et le noeud suivant auquel le routeur doit délivrer le message. En réalité il suffit que le message soit délivré sur le réseau qui contient la machine, il n'est donc pas nécessaire de stocker l'adresse IP complète de la machine : seul l'identificateur du réseau de l'adresse IP (c'est-à-dire le Netid a besoin d'être stocké.

La table de routage est donc un tableau contenant des paires d'adresses :

Adresse de destination	Adresse du prochain routeur directement accessible	Interface

Ainsi grâce à cette table, le routeur, connaissant l'adresse du destinataire encapsulé dans le message, va être capable de savoir sur quelle interface envoyer le message (cela revient à savoir quelle carte réseau utiliser), et à quel routeur, directement accessible sur le réseau auquel cette carte est connectée, remettre le datagramme.
Ce mécanisme consistant à ne connaître que l'adresse du prochain maillon menant à la destination est appelé routage par sauts successifs (en anglais next-hop routing).

Cependant, il se peut que le destinataire appartienne à un réseau non référencé dans la table de routage. Dans ce cas, le routeur utilise un **routeur par défaut** (appelé aussi passerelle par défaut).

Exemple de table de routage :

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
255.255.255.255	*	255.255.255.255	UH	0	0	0	eth0
193.253.160.3	*	255.255.255.255	UH	0	0	0	ppp0
192.168.0.0	*	255.255.255.0	U	0	0	0	eth0
10.0.0.0	*	255.0.0.0	U	0	0	0	eth1
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	193.253.160.3	0.0.0.0	UG	0	0	0	PPP0

Le message est ainsi remis de routeur en routeur par sauts successifs, jusqu'à ce que le destinataire appartienne à un réseau directement connecté à un routeur. Celui-ci remet alors directement le message à la machine visée.

Dans le cas du routage statique, c'est l'administrateur qui met à jour la table de routage.
Dans le cas du routage dynamique, par contre, un protocole appelé **protocole de routage** permet la mise à jour automatique de la table afin qu'elle contienne à tout moment la route optimale.

8.3 Les protocoles de routage

Internet est un ensemble de réseaux interconnectés. Par conséquent tous les routeurs ne font pas le même travail selon le type de réseau sur lequel ils se trouvent.

En effet, il y a différents niveaux de routeurs, ceux-ci fonctionnent donc avec des protocoles différents:

- Les **routeurs noyaux** sont les routeurs principaux car ce sont eux qui relient les différents réseaux
- Les **routeurs externes** permettent une liaison des réseaux autonomes entre eux. Ils fonctionnent avec un protocole appelé EGP (Exterior Gateway Protocol) qui évolue petit à petit en gardant la même appellation
- Les **routeurs internes** permettent le routage des informations à l'intérieur d'un réseau autonome. Ils s'échangent des informations grâce à des protocoles appelés IGP (Interior Gateway Protocol), tels que RIP et OSPF

8.4 Le protocole RIP

RIP signifie Routing Information Protocol (protocole d'information de routage). Il s'agit d'un protocole de type Vecteur Distance, c'est-à-dire que chaque routeur communique aux autres routeurs la distance qui les sépare (le nombre de saut qui les sépare). Ainsi, lorsqu'un routeur reçoit un de ces messages il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles. Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de saut pour atteindre un réseau soit minimal. Toutefois ce protocole ne prend en compte que la distance entre deux machines en termes de saut, mais il ne considère pas l'état de la liaison afin de choisir la meilleure bande passante possible.

8.5 Le protocole OSPF

OSPF (*Open Shortest Path First*) est plus performant que RIP et commence donc à le remplacer petit à petit. Il s'agit d'un protocole de type protocole route-link (que l'on pourrait traduire par Protocole d'état des liens), cela signifie que, contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné.

De plus, ce routeur évite aux routeurs intermédiaires d'avoir à incrémenter le nombre de sauts, ce qui se traduit par une information beaucoup moins abondante, ce qui permet d'avoir une meilleure bande passante utile qu'avec RIP.