

INTRODUCTION A INTERNET - LE PROTOCOLE IP

1. PRESENTATION D'INTERNET

Internet peut être considéré comme un réseau de réseaux, c'est à dire une interconnexion de différents réseaux dans le monde.

Internet apporte à un utilisateur les principaux services suivants :

- Le transfert de fichiers à l'aide de FTP (File Transfer Protocol). L'utilisateur peut télécharger des fichiers à partir d'un site distant.
- La connexion sur un système distant à l'aide de Telnet (Terminal net protocol). L'ordinateur se comporte comme un simple terminal connecté au système distant.
- L'accès au WWW (World Wide Web ou Web ou W3). L'utilisateur grâce à un navigateur peut notamment visualiser des documents situés sur un site éloigné, et passer d'un document à l'autre même s'ils sont situés en des endroits différents, cette navigation repose du point de vue technique sur le protocole HTTP (Hyper Text Transfer Protocol).
- La messagerie électronique (E Mail) qui repose sur les protocoles POP3 (Post Office Protocol version 3) et SMTP (Simple Mail Transfer Protocol).
- Les forums de discussions appelés NEWS, ces forums sous forme de questions réponses sont fédérés par thème appelés *newsgroup*, un utilisateur peut s'abonner à un ou plusieurs newsgroups. Le service des NEWS repose sur le protocole NNTP (Network News Transfer Protocol).
- La communication entre plusieurs personnes en instantané grâce au protocole IRC (Internet Relay Chat). Ce protocole prévu au départ pour communiquer à l'aide du clavier se perfectionne sans cesse pour aboutir maintenant à la téléphonie (appelée téléphonie comprimée) ainsi qu'à la vidéo-conférence.
- La recherche d'informations sur le réseau à l'aide de GOPHER, la recherche de fichiers avec ARCHIE ou bien encore la recherche de documents à l'aide de WAIS (Wide Area Information Servers) (mais on peut aussi se connecter à l'aide d'un navigateur sur des sites particuliers du Web qui offrent l'utilisation d'un service de recherches appelé moteur de recherches (Altavista, Lycos, Yahoo, ...).

Les applications apportées par le réseau Internet reposent essentiellement sur le principe Client / Serveur.

- Un serveur est un logiciel spécifique qui offre un service bien défini. Ce serveur s'exécute sur une machine multitâche (Unix, WindowsNT, ...). En général, plusieurs programmes serveurs s'exécutent simultanément sur la même machine et, par extension, cette machine est aussi appelée serveur.
- Un client est un programme qui s'exécute sur une machine et qui adresse au serveur des demandes spécifiques, la demande du client est appelée requête de service. Par exemple, le serveur est un serveur de fichier, le client demande à transférer un fichier du serveur sur sa machine, la réponse positive du serveur est l'envoi du fichier.

Cette communication s'effectue à travers le réseau Internet. Le réseau Internet repose techniquement sur l'ensemble des protocoles TCP/IP : Transport Control Protocol / Internet Protocol.

Les protocoles TCP sont des protocoles de la couche Transport (couche 4), les protocoles IP sont des protocoles de la couche Réseau (couche 3), la couche Physique et la couche Liaison qui relie les diverses

machines ne sont pas spécifiées, c'est à dire que diverses voies physiques de communication peuvent être utilisées pour acheminer les informations.

Sans faire un historique complet d'Internet, il est intéressant de savoir que les protocoles TCP/IP résultent des travaux de recherche de la DARPA (Defense Advanced Research Projects Agency), organisme de recherche du ministère américain de la défense. Leur but était de créer un réseau capable de fonctionner en temps de guerre, même malgré la destruction d'une partie de ce réseau. Le projet ARPA a donné naissance au réseau ARPANET qui connectait une quarantaine de sites au début des années 70. Due à son extension, ARPANET a évolué vers Internet. Internet a continué d'évoluer et a pris son essor à la fin des années 80. Puis le CERN a développé en 93 le WWW et depuis le nombre d'internautes (utilisateurs d'Internet) ne cesse de croître.

L'association ISOC (Internet Society) a pour but de promouvoir l'Internet et de favoriser son développement. L'IAB (Internet Architecture Board) est chargée par l'ISOC de contribuer au développement technique du réseau.

L'IAB assure la mise à jour des informations concernant Internet sous la forme de RFC (Request For Comments). La plupart des rfc constituent les normes du réseau Internet.

Chaque machine vue de l'utilisateur semble raccordée à un seul et unique réseau (planétaire), la complexité des interconnexions entre les divers réseaux physiques lui est ainsi complètement masquée.

2. L'IDENTIFICATION DES MACHINES SUR INTERNET

2.1 Les adresses Internet ou adresses IP

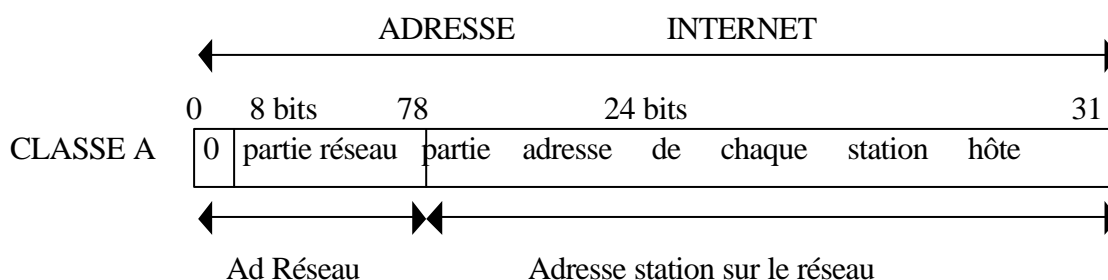
Il est nécessaire de pouvoir identifier de manière unique chaque machine connectée à l'Internet, c'est le rôle des adresses Internet appelées aussi adresses IP.

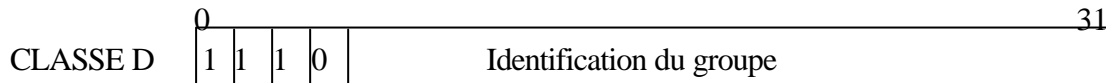
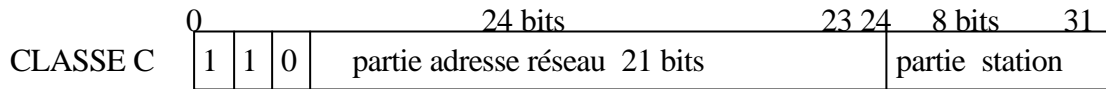
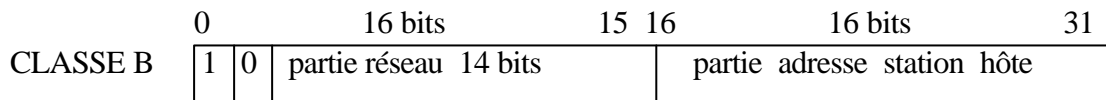
Chaque machine dispose d'une adresse IP codée sur 32 bits qui permet ainsi de l'identifier à chacune de ses communications.

Une adresse INTERNET est constituée d'une partie ADRESSE RESEAU et d'une partie ADRESSE STATION.

Chaque réseau est différent et peut donc comporter un nombre de machines qui varie en fonction de son importance. La « norme Internet » prévoit ce problème et spécifie diverses classes de réseaux suivant leur taille.

L'adresse Internet est sur 32 bits et a la structure suivante :





Les adresses sont des nombres sur 4 octets, on les exprime habituellement sous forme de 4 nombres décimaux séparés les uns des autres par un point, chaque nombre correspondant à un octet.

Les adresses en classe A vont de 0.0.0.0 à 127.255.255.255.

Les adresses en classe B vont de 128.0.0.0 à 191.255.255.255.

Les adresses en classe C vont de 192.0.0.0 à 223.255.255.255.

Prenons comme exemple un réseau de classe C dont la partie réseau de l'adresse Internet est 198.200.10. Les machines connectées sur ce réseau auront une adresse de la forme 198.200.10.N. Par exemple : 198.200.10.1, 198.200.10.2, ...

L'IANA (Internet Assigned Numbers Authority) est chargée au niveau mondial de distribuer les adresses réseaux et les noms des domaines, elle délègue ses pouvoirs en Europe au RIPE (Réseaux IP Européens) qui délègue à son tour à des organismes, quelquefois appelés NIC (Network Information Center), qui gèrent une partie des adresses. On peut citer en France l'INRIA, Renater, France Télécom.

Quelques adresses destinations particulières

0.0.0.0 : Cette adresse a un rôle essentiel dans les tables de routage car elle y signifie la route par défaut; de même, toujours dans les tables de routage, l'adresse <ad_réseau>.0 désigne le réseau d'adresse ad_réseau (de plus, l'utilisation de l'adresse <ad_réseau>.0 n'est pas recommandée pour une machine car elle correspond à la diffusion pour les anciens systèmes Unix BSD).

255.255.255.255 : Un datagramme avec cette adresse sera envoyé à toutes les machines du réseau.

<Ad_réseau>.255 : Diffusion vers toutes les machines du réseau d'adresse Ad_réseau.

127.0.0.1 : Boucle locale interne, une trame qui contient cette adresse destination n'est pas émise vers le réseau mais revient vers l'expéditeur.

Un réseau en classe C peut contenir 254 machines ayant chacune sa propre adresse IP.

En conclusion, une machine qui peut se connecter sur Internet dispose de sa propre adresse IP, mais il ne faut pas oublier que cette adresse Internet caractérise de manière unique à la fois cette machine et le réseau éventuel sur lequel cette machine est connectée.

Adresses fixes ou temporaires

Une entreprise qui veut connecter son réseau local à Internet se voit attribuer une adresse réseau, l'administrateur du réseau à la responsabilité de choisir ensuite les affectations de la partie machine des adresses Internet. Les serveurs de son réseau local doivent alors impérativement disposer d'une adresse Internet fixe si on veut y accéder de l'extérieur.

Un utilisateur qui souhaite se connecter de manière temporaire (Dial-Up) n'a pas besoin d'une adresse permanente. Il accède au réseau par l'intermédiaire d'un fournisseur d'accès (Provider) qui lui allouera pendant la durée de sa connexion une adresse Internet, cette adresse est attribuée de manière dynamique et peut donc être différente à chacune de ses connexions.

2.2 Les noms Internet

Il est plus facile pour les humains de se rappeler d'un nom, il est ainsi possible de « nommer » les machines connectées sur un réseau Internet et ainsi de les désigner par leur nom à la place de leur adresse Internet.

Prenons le cas d'un réseau local avec un serveur UNIX, le fichier `/etc/hosts` sur ce serveur contient la table de correspondance entre l'adresse Internet de chacune des machines connectée au réseau local et leur nom.

Le fichier `/etc/hosts` contient des lignes qui ont la forme suivante :

```
198.9.100.1  SERVEUR_INFO
198.9.100.2  PC1
198.9.100.3  PC2
198.9.100.4  PC3
198.9.100.5  PC4
198.9.100.10 X1
198.9.100.11 X2
```

Une commande sur ce serveur UNIX du type `ping pc1` envoie bien un message à la machine d'adresse 198.9.100.2. Le programme `ping` fait appel à une fonction `resolveur` qui lit le fichier `/etc/hosts` afin de déterminer l'adresse Internet de la machine PC1.

2.3 Le système de noms de domaines

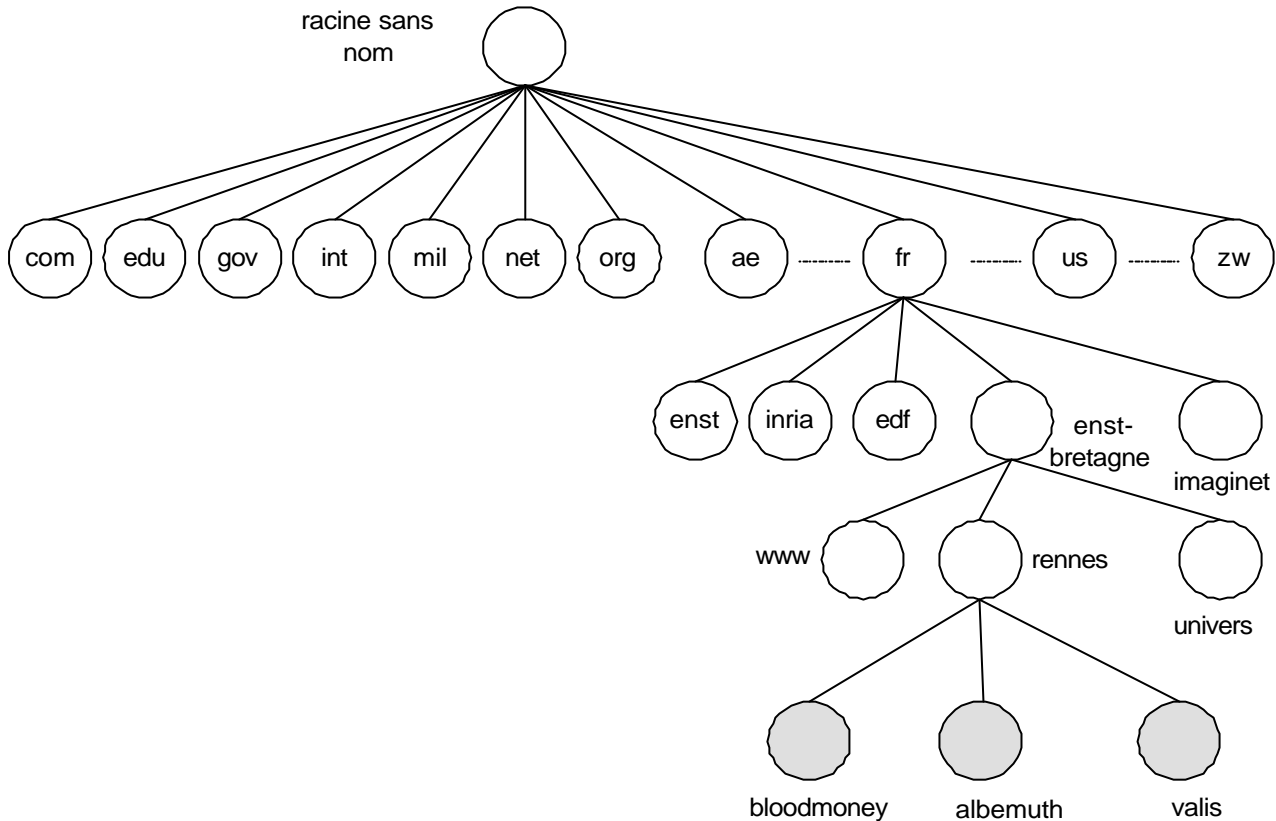
Le réseau Internet est planétaire, ainsi pour pouvoir donner un nom sans ambiguïté il a été décidé d'organiser les noms des machines dans une structure hiérarchique découpée en domaines, eux-mêmes pouvant être subdivisés en sous domaines et ainsi de suite.

Un domaine a donc un nom, on distingue les domaines génériques des domaines géographiques.

Les domaines géographiques sont basés sur les pays, on a le domaine `fr` pour la France, le domaine `uk` pour le Royaume Uni, le domaine `ie` pour l'Irlande, ... Ces domaines ont un nom sur 2 lettres.

Les 7 domaines génériques sont basés sur le type de l'activité des organisations connectées, on a le domaine *edu* pour les universités, le domaine *com* pour les activités commerciales, *mil* pour les militaires, ... Ces domaines ont un nom sur 3 lettres.

On peut encore subdiviser chacun de ces domaines en petits domaines.



Les domaines *gov* et *mil* sont réservés aux américains.

Pour la France, on distingue sur cette figure les domaines *enst.fr*, *inria.fr*, ...

La machine *bloodmoney* est totalement qualifiée par *bloodmoney.rennes.enst-bretagne.fr*. On parle alors d'un nom FQDN (Fully Qualified Domain Name).

La séparation entre les noms est assurée par un « point », la règle fait que le domaine situé à droite du point englobe celui situé à gauche du même point.

Une zone est une branche de l'arbre qui est administrée séparément. Une zone commune est aussi considéré comme un domaine de 2nd niveau.

Les extrémités des branches de l'arbre sont les noms des machines connectées au réseau, cercles grisés sur le dessin.

D'une manière générale, supposons une machine de nom "*mon_nom*" placée dans la zone "*site*" qui est située dans le domaine "*dom*", lui-même placé dans le domaine "*fr*". On qualifiera convenablement cette machine par le nom (lettres majuscules ou minuscules indifféremment) :

`mon_nom.site.dom.fr`

Si les utilisateurs Mr Machin et Mr Truc sont des utilisateurs déclarés sur Mon_nom, leur adresse électronique est :

Machin@ mon_nom.site.dom.fr	pour Mr Machin
Truc@ mon_nom.site.dom.fr	pour Mr Truc

La structure hiérarchique dessinée sur la figure précédente représente le DNS (Domain Name System). Le DNS est une base de données distribuée sur l'ensemble du réseau Internet pour établir la correspondance entre les noms des machines et les adresses IP. Le DNS est donc un système d'annuaire réparti sur des machines appelées serveurs de noms.

L'accès au DNS s'effectue par une machine qui tente de communiquer avec une autre machine par l'intermédiaire de son nom mais sans connaître son adresse Internet.

Au niveau programme client, l'accès au DNS s'effectue à l'aide du résolveur. Sur un système Unix, le résolveur est sollicité par l'intermédiaire de la fonction *gethostbyname()* qui permet d'obtenir l'adresse IP d'une machine à partir de son nom. Le résolveur contacte alors un serveur de noms qui retourne l'adresse IP s'il la connaît ou transmet la demande à un autre serveur de noms dans le cas contraire.

Le fichier */etc/resolv.conf* sur un client Unix donne les informations au résolveur, son contenu a l'allure suivante :

```
nameserver 193.9.56.1
domain mon_site.fr
```

La ligne *nameserver* précise l'adresse IP du serveur de noms à contacter, il peut y avoir jusqu'à 3 lignes débutant par *nameserver* pour procurer des serveurs de remplacement dans le cas d'une défaillance éventuelle du précédent.

La ligne *domain* sert à compléter le nom donné lorsque le résolveur détecte que ce nom est incomplet. Par exemple si le nom de la machine à trouver est *whist*, le résolveur fournira *whist.mon_site.fr*.

En conclusion, la tentative de connexion d'une machine à une autre machine en donnant le nom de celle-ci fait appel au résolveur. Ce résolveur doit alors trouver l'adresse Internet de la machine distante, il analyse le fichier */etc/hosts* puis, s'il n'y trouve pas le nom de la machine, interroge le serveur de noms dont l'adresse Internet est donnée dans le fichier */etc/resolv.conf*.

3 PLACE DU PROTOCOLE IP (INTERNET PROTOCOL)

3.1 La pile de protocoles dans un réseau Ethernet

La figure suivante présente les divers protocoles et quelques applications installés sur une machine connectée sur un réseau Ethernet.

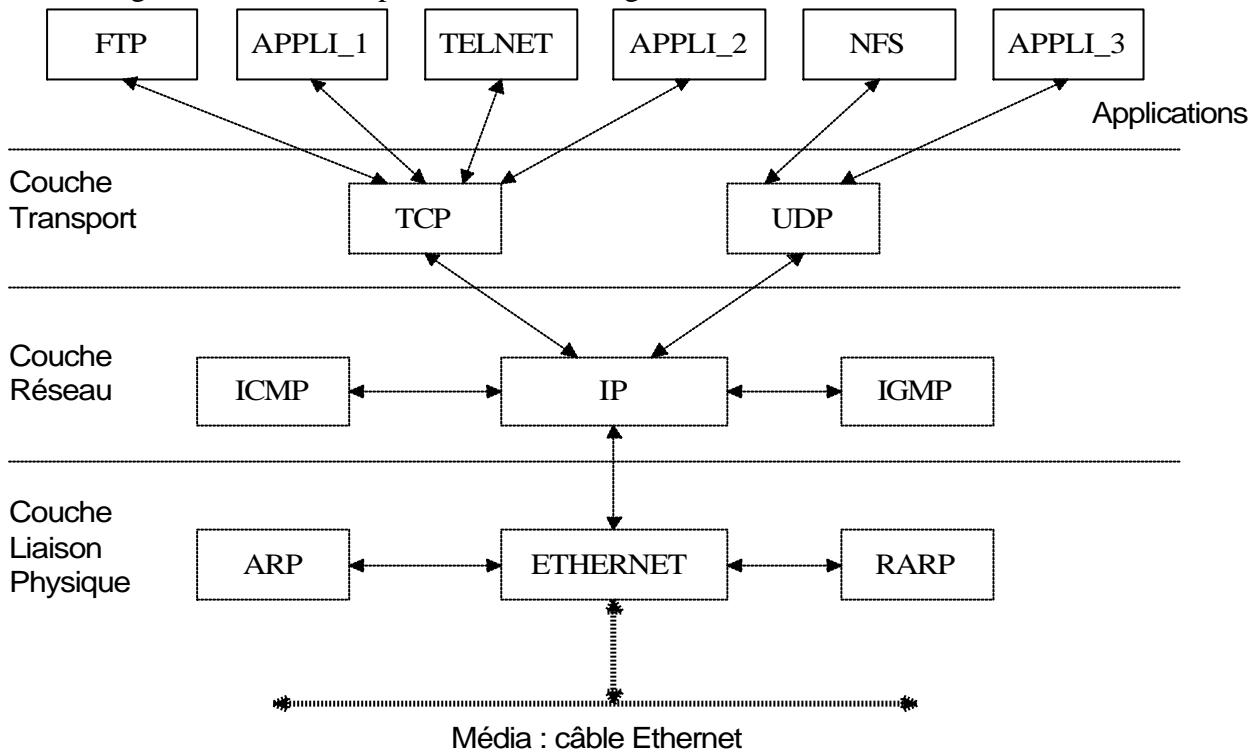
Les applications FTP, APPI_1, TELNET et APPLI_2 utilisent le protocole TCP, NFS et APPLI_3 utilisent UDP.

TCP et UDP sont intégrés dans les protocoles TCP, ils sont étudiés dans le prochain cours.

ICMP, IP et IGMP font partis des protocoles IP.

ICMP et IP sont étudiés dans ce cours.

IGMP (Internet Group Management Protocol) : Une machine peut appartenir à un groupe de diffusion (adresse IP classe D) qui permet d'envoyer un datagramme vers un groupe de machines et, réciproquement, de recevoir un datagramme à destination de son groupe. Le protocole IGMP permet à une machine de signifier aux diverses machines du réseau et aux routeurs son appartenance à ce groupe. Les messages IGMP sont encapsulés dans des datagrammes IP.



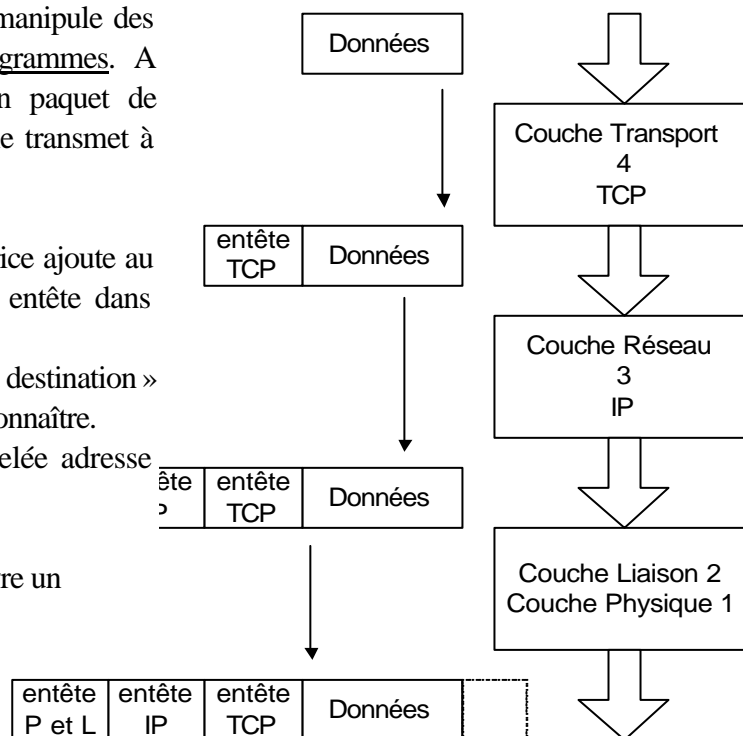
3.2 Emission des datagrammes IP

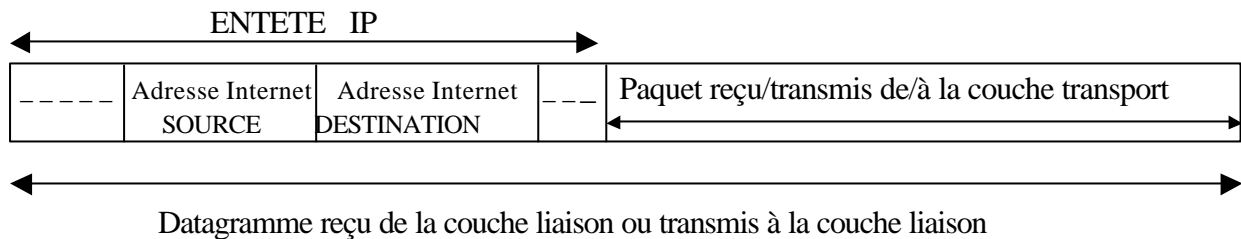
La couche IP (couche Réseau : 3) manipule des paquets de données appelés datagrammes. A l'émission, la couche IP reçoit un paquet de données de la couche Transport, elle transmet à la couche Liaison un datagramme.

Le protocole IP de la station émettrice ajoute au paquet reçu de la couche TCP un entête dans lequel on trouve notamment :

- L'adresse Internet de la station « destination » afin bien sûr qu'elle sache se reconnaître.
- Sa propre adresse Internet appelée adresse de la station « source ».

A la réception, la couche liaison délivre un datagramme à la couche IP.

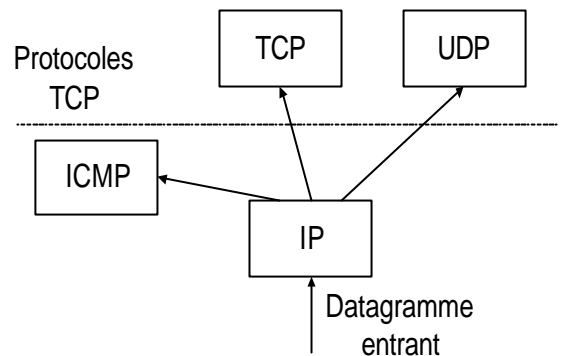




Les autres données de l'entête IP sont étudiées dans le chapitre 4.

3.3 Demultiplexage des datagrammes entrants

La couche IP d'une machine analyse l'adresse Internet destination des datagrammes qui lui sont transmis par la couche liaison. Elle accepte le paquet si l'adresse destination correspond à son adresse IP ou à l'adresse de diffusion. La couche transport est constituée des protocoles TCP, IP doit diriger le datagramme vers le protocole TCP concerné.



Cette figure montre le démultiplexage réalisé par IP pour un datagramme reçu, ce datagramme est envoyé soit vers le protocole TCP, soit vers le protocole UDP, soit vers le protocole ICMP qui est en réalité intégré à la famille IP.

4. L'ENTETE IP

0	4	8	15	16	31
Version	Longueur entête	Type de service (TOS)	Longueur totale du datagramme (en octets)		
Identification			Drapeau (3bits)	Offset du fragment	
Durée de vie (TTL)		Protocole destinataire	Checksum sur l'entête		
Adresse Internet de la source					
Adresse Internet de la destination					
Options facultatives					
DONNEES					

Version : Le champ version vaut actuellement 4, c'est la version IPv4, la version future est IPv6.

Longueur entête : Nombre de mots de 32 bits qui composent l'entête.

Type de service : Informe le routeur pour l'aider à choisir le chemin du datagramme en fonction du double critère « délai - débit ».

Quelques valeurs en fonction des applications :

Telnet		0x10	Minimise le délai
Ftp	Commande	0x10	Minimise le délai
Ftp	Données	0x08	Favorise le débit

Longueur totale : Ce champ donne en octets la longueur totale du datagramme y compris l'entête.

Identification : Chaque datagramme porte un numéro unique qui est placé par l'émetteur. Il est possible que la taille d'un paquet à transmettre soit trop grand pour la couche liaison, IP fragmente alors ce paquet en plusieurs datagramme, chaque datagramme porte alors le même numéro et contient un fragment du paquet initial.

Drapeau : Le 1^{er} bit est toujours nul, le 2^{ème} bit DF (Don't Fragment) indique s'il est à 1 que la fragmentation est interdite, le 3^{ème} bit MF (More Fragment) indique s'il est à 1 qu'il y a d'autres fragments à émettre ou que c'est le dernier fragment s'il vaut 0.

Offset du fragment : Valable uniquement dans le cas d'une fragmentation, représente le rang du 1er octet de ce fragment par-rapport au début du datagramme complet.

Durée de vie (TTL time to live): Ce champ indique le nombre maximal de routeurs que le datagramme peut traverser avant d'être détruit, il est alors décrémenté de 1 à chaque routeur traversé.

Protocole destinataire : Ce champ est fondamental pour les datagrammes reçus du réseau par la couche IP, il permet d'identifier quel est le protocole supérieur auquel est destiné ce datagramme. Les valeurs les plus courantes sont : 6 pour le protocole TCP, 17 pour UDP et 1 pour ICMP. TCP et UDP font partis de la couche transport (famille des protocoles TCP). La couche IP transmet donc le paquet reçu au bon protocole destinataire grâce à cet octet.

Checksum : Mot de 16 bits égal au complément à 1 de la somme de tous les mots de 16 bits de l'entête.

Adresse Internet : Ces 2 champs contiennent les adresses Internet de la source et de la destination.

Options : Les options sont rarement utilisées et ce champ est alors mis à 0, sinon ce champ est utile pour les routeurs (sécurité, marque la route avec les adresses des routeurs, marque le temps).

Données : Représente le paquet reçu de la couche transport TCP.

5. LE PROTOCOLE ARP (Address Resolution Protocol)

Le protocole ARP ne fait pas parti des protocoles IP mais il joue un rôle essentiel dans le cas des réseaux locaux de type Ethernet. Chaque machine a une adresse physique propre appelée adresse Ethernet.

La couche physique Ethernet accepte une trame à la condition que le champs <adresse destination> de la trame contienne soit sa propre adresse, soit l'adresse de diffusion restreinte de groupe, soit l'adresse de diffusion généralisée FF:FF:FF:FF:FF:FF (broadcast).

A l'émission le datagramme Internet est encapsulé dans la trame Ethernet, il faut donc que la couche Ethernet de la machine Emettrice connaisse l'adresse Ethernet de la machine Destinataire.

Avant d'émettre la "trame utile", le pilote Ethernet de la machine Emettrice fait appel au protocole ARP afin d'obtenir l'adresse Ethernet de la machine Destinataire. Le protocole ARP permet d'associer l'adresse Internet d'une machine à son adresse Ethernet.

Ce protocole consiste à émettre une trame Ethernet de diffusion généralisée qui contient l'adresse Internet de la machine recherchée, toutes les machines lisent cette trame, celle qui reconnaît son adresse Internet retourne une trame de réponse dans laquelle elle place sa propre adresse Ethernet.

Description du paquet ARP : Le chiffre sous chaque champ indique sa taille en octets.

Type du matériel	Type du protocole	Longueur Ad physique	Longueur Ad physique	Op	Adresse Ethernet l'émetteur	Adresse IP de l'émetteur	Adresse Ethernet cible	Adresse Internet cible
2	2	1	1	2	6	4	6	4

Type du matériel : La valeur est toujours 1.

Type du protocole : Il s'agit du protocole IP, ici 0x0800.

Longueur Adresse physique : Ce champ a comme valeur 6.

Longueur Ad physique : Longueur de l'adresse IP, donc valeur égale à 4.

Op (opération) : Indique le rôle de ce paquet

- 1 pour une requête ARP (demande d'adresse).
- 2 pour la réponse ARP.

Adresse Ethernet l'émetteur : Contient l'adresse Ethernet de l'émetteur du paquet.

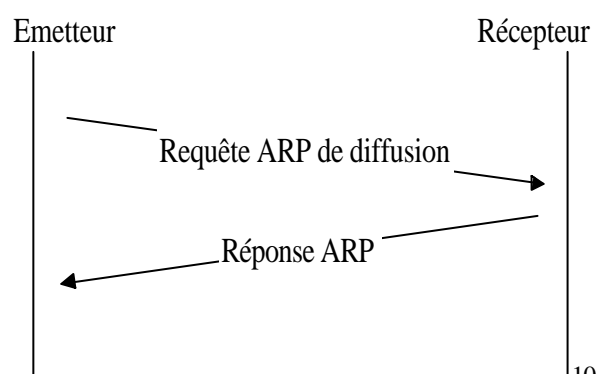
Adresse IP de l'émetteur : Contient l'adresse Internet de l'émetteur du paquet.

Adresse Ethernet cible : Contient l'adresse Ethernet du destinataire du paquet, ce champ est vide dans le cas d'une demande.

Adresse Internet cible : Contient l'adresse Internet du destinataire du paquet.

Il ne faut pas oublier que le paquet ARP est encapsulé dans une trame Ethernet dont le champ "type de protocole" vaut 0x0806.

L'utilisation systématique du protocole ARP serait couteuse en trafic sur le réseau et en utilisation des machines, aussi l'émetteur conserve la correspondance Adresse Internet



- Adresse Ethernet dans une table en mémoire pendant quelques minutes (en général 20mn pour un système Unix).

6. LE PROTOCOLE ICMP (Internet Control Message Protocol)

ICMP permet de délivrer des messages d'erreur ainsi que quelques informations très ciblées, on ne détaille ici que quelques messages particuliers. Pour éviter les boucles à l'infini, un message ICMP ne peut pas provoquer l'émission d'un autre message ICMP, il en est de même si l'adresse IP est une adresse de diffusion.

Les paquets ICMP sont encapsulés dans des datagrammes Ip dont le champ protocole a comme valeur 1, le format d'un paquet ICMP est le suivant :

0	7 8	15 16	23	31
Type	Code	Checksum		
Données complémentaires : dépend du type de du code				

L'émetteur d'un paquet ICMP peut être aussi bien une station qu'un routeur. Le checksum se calcule en effectuant la somme sur 16 bits de tous les mots du paquet ICMP puis en prenant le complément à 1 de ce résultat.

On peut classer les messages d'erreur ICMP en fonction de la raison de leur émission.

- La commande Ping (Packet Internet Groper) : Elle permet de tester l'accessibilité d'une station. Cette commande émet un paquet ICMP de demande d'écho (type 8, code 0) vers une machine donnée; elle reçoit, si la machine distante est active, un paquet réponse d'écho (type 0, code 0). Le champ Identificateur permet d'identifier le processus émetteur de la requête d'écho, le champ N° de séquence est initialisé à 0 au départ puis est incrémenté à chaque nouvelle requête d'écho émise. Les données qui suivent doivent être retournées comme avec un écho.

0	7 8	15 16	23	31
Type = 8 ou 0	Code : 0	Checksum		
Identificateur		Numéro de séquence		
Type = 8 : Données qui doivent être retournées par la machine destinataire Type = 0 : Données retournées par la machine destinataire				

Le paquet ICMP issu de la commande Ping a une taille de 64 octets sur la plupart des machines, il en résulte que le champs Données contient 56 octets. L'exécution de la commande Ping sur un système Unix entraîne l'envoi périodiquement d'un paquet Requête d'Echo (par exemple chaque seconde), le champ N° de séquence est incrémenté à chaque paquet émis, la valeur de ce champ dans la réponse retournée permet d'identifier le paquet.

- Un datagramme IP ne peut atteindre sa destination : Ce type de message peut aussi bien être émis par une station que par un routeur.

0	7 8	15 16	23	31
---	-----	-------	----	----

Type = 3	Code : de 0 à 15	Checksum	
00	00	00	00
Entête Internet et les 64 premiers bits du datagramme qui a déclenché l'émission du paquet ICMP			

Les divers codes possibles :

Code	Description	Code	Description
0	Réseau inaccessible	1	Machine inaccessible
2	Protocole incorrect (champ de l'entête IP)	3	Fragmentation nécessaire mais DF=1
4	Port inaccessible	5	Echec de la route donnée en option
6	Réseau inconnu du routeur	7	Destinataire inconnu du routeur
8	Station émettrice isolée (obsolète)	9	Communication interdite avec le réseau
10	Communication avec la machine interdite	11	Réseau inaccessible avec le TOS donné
12	Machine inaccessible avec le TOS donné		

- Fin de la durée de vie d'un datagramme

Le champ durée de vie (TTL) est décrémenté à chaque routeur traversé. Un routeur qui reçoit un datagramme IP dont le champ TTL est à 1 doit éliminer ce datagramme et émettre vers la machine d'origine un message ICMP avec le champ type à 11. Le champ code à 0 précise que le routeur a éliminé un datagramme isolé, le champ code à 1 indique que cela s'est passé pendant le réassemblage d'un datagramme.

0	7 8	15 16	23	31
Type = 11	Code : 0 ou 1	Checksum		
00	00	00	00	
Entête Internet et les 64 premiers bits du datagramme qui a déclenché l'émission du paquet ICMP				

7. INTRODUCTION AU ROUTAGE

7.1 Présentation

La fonction de routage consiste à choisir un chemin sur lequel un datagramme doit être acheminé.


L'interconnexion des réseaux est assurée par des routeurs dont la fonction essentielle est le routage, un paquet peut avoir à traverser plusieurs routeurs pour arriver à destination.

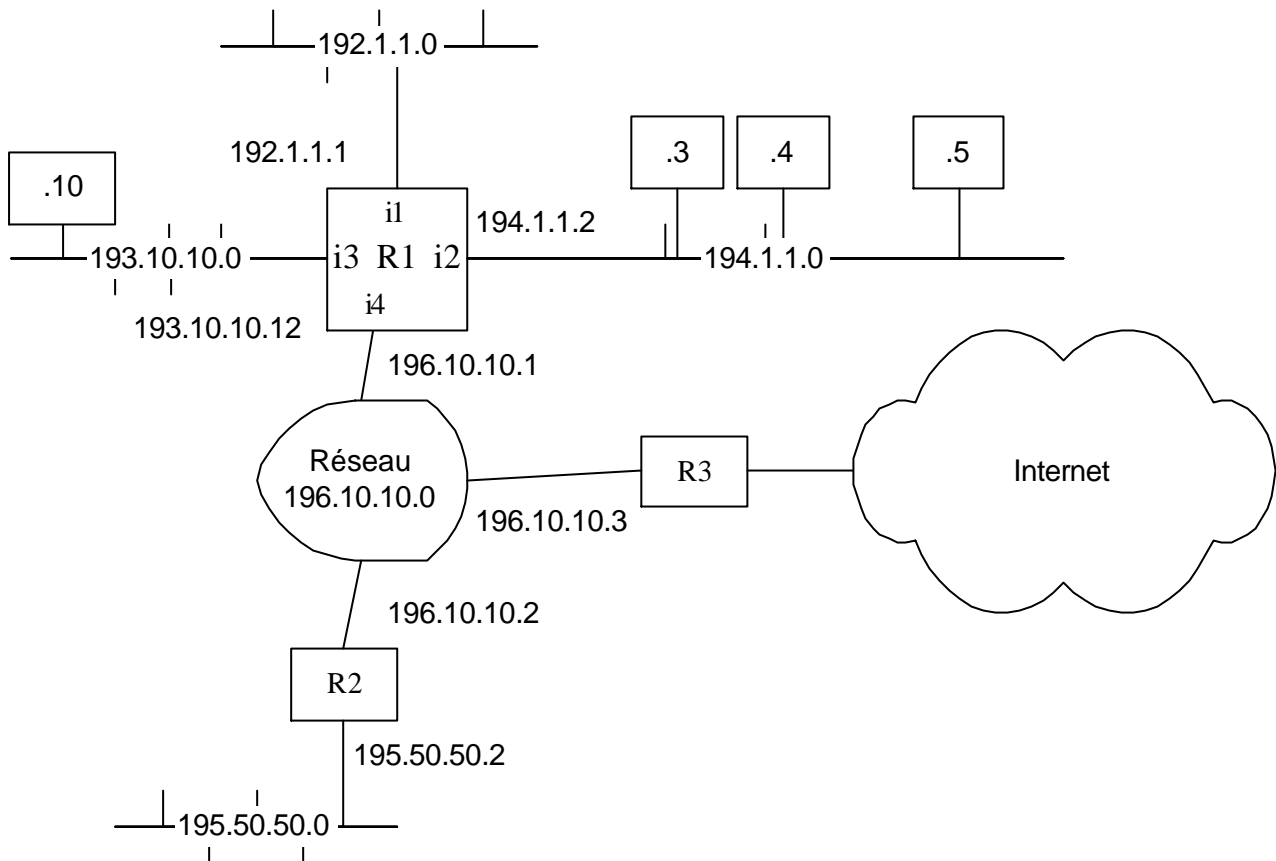
La figure suivante présente un exemple d'interconnexion de réseaux.

Le routeur R1 est relié aux 4 réseaux de classe C d'adresses réseaux 190.10.10, 191.1.1, 192.1.1 et 193.10.10.

Les adresses réseaux se terminent sur la figure par le dernier octet à 0. Le routeur R1 dispose de 4 adresses IP, une par réseau auquel il est connecté.

Machines du réseau 191.1.1





La figure précédente décrit un site utilisateur fictif, par exemple un vaste campus d'université, dont la connexion à l'Internet est assurée par le routeur R3, par exemple une connexion au réseau régional correspondant, lui-même connecté au réseau Renater.

7.2 Routage direct et indirect

Deux situations sont possibles lorsqu'une machine émet un datagramme :

- La machine destinataire est sur le même réseau physique que l'émettrice, on parle de routage direct.
- La machine est située sur un autre réseau et le datagramme doit passer par un routeur au moins, on qualifie cela de routage indirect.

Concrètement, gestion des deux situations précédentes par la machine 194.1.1.3 :

- Le routage direct : Un datagramme dont l'adresse réseau destination est 194.1.1 (même réseau physique Ethernet) doit être transmis tel quel à la couche Ethernet qui utilisera si nécessaire le protocole ARP pour récupérer l'adresse Ethernet du destinataire. Dans la trame émise, l'adresse Ethernet et l'adresse IP sont celles de la même machine.
- Le routage indirect : Un datagramme dont l'adresse réseau destination est autre doit être transmis au routeur R1 dont l'adresse Internet est 194.1.1.2. Il faut que le datagramme soit encapsulé dans une trame Ethernet dont l'adresse destination est celle du routeur d'adresse IP 194.1.1.2 alors que l'adresse IP destination contenue dans le datagramme est celle de la machine destinataire. Donc, dans la trame émise, l'adresse Ethernet et l'adresse IP sont celles de 2 machines différentes, adresse Ethernet du routeur, adresse IP du destinataire.

7.3 Table de routage

Une machine connectée sur un réseau local sur lequel il y a un routeur doit disposer d'une table de routage qui est lue à l'émission de chaque datagramme, cette table doit contenir deux entrées : une pour le réseau local auquel la machine appartient, une pour le routeur. En prenant le cas de la machine 194.1.1.3 :

<u>Destination</u>	<u>Routeur</u>
194.1.1.0	Remise directe
défaut	194.1.1.2

Le terme *défaut* désigne la route par défaut, tous les datagrammes dont l'adresse réseau est différente de 194.1.1 sont envoyés vers le routeur d'adresse IP 194.1.1.2. L'adresse route par défaut peut être donnée en notation pointée 0.0.0.0.

Si la machine 194.1.1.3 est un système Unix, la commande `netstat -rn` affiche la table de routage, le résultat a l'allure suivante :

Destination	Gateway	Flag	---	Interface
194.1.1.0	194.1.1.3	U	---	le0
Default	194.1.1.2	UG	---	le0
127.0.0.1	127.0.0.1	UH	---	lo0

L'interface lo0 est l'interface de loopback (rebouclage interne).

L'interface le0 est lié à la carte Ethernet contenue dans la machine.

Le flag U signifie que la route est en service (Up).

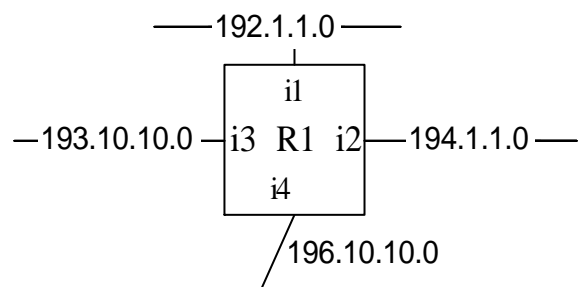
Le flag G signifie que la route passe par un routeur (Gateway).

Le flag H signifie que destination concerne une machine (Host) et non un réseau.

On prend le cas du routeur R1, le but de sa table de routage est d'associer l'adresse IP du datagramme reçu (en réalité son adresse réseau) avec l'interface sur laquelle il doit réémettre le datagramme. Les interfaces sont désignés par i1, i2, i3 et i4.

La table de R1 peut avoir l'allure suivante :

Destination	Routeur	Interface
192.1.1.0	Direct	i1
194.1.1.0	Direct	i2
193.10.10.0	Direct	i3
196.10.10.0	Direct	i4
195.50.50.0	196.10.10.2	i4
défaut	196.10.10.3	i4



L'avant dernière ligne précise qu'il faut envoyer le datagramme au routeur d'adresse 196.10.10.2 quand l'adresse réseau du destinataire est 195.50.50.

La dernière ligne signifie que tous les datagrammes qui ont une autre adresse réseau IP que les 5 mentionnées précédemment doivent être envoyés vers le routeur d'adresse IP 196.10.10.3.

7.4 Introduction au routage dynamique, algorithme du Distant Vector

Le routeur R1 des chapitres précédents connaît sa table de routage, mais que se passe-t-il si de nouveaux réseaux et routeurs sont ajoutés ?

- Soit l'administrateur modifie manuellement les tables de routage, on parle de routage statique.
- Soit les routeurs peuvent apprendre automatiquement la nouvelle topologie du réseau en échangeant les tables de routage, on qualifie ce type de routage de dynamique. L'échange des tables de routage s'effectue à l'aide d'un protocole d'échange de tables. Cette solution est la plus favorable si plusieurs routes deviennent possibles pour communiquer avec une machine.

De nombreux protocoles d'échange de tables existent, aussi Internet a choisi de structurer les divers ensembles connectés au réseau en systèmes autonomes SA (autonomous system). Chaque système autonome peut choisir son protocole d'échange des tables. Typiquement, un SA peut être un campus, une entreprise.

On distingue maintenant deux familles de protocole d'échange de tables :

- Internes au SA, appelés IGP (Interior Gateway Protocol).
- Externes pour l'échange de données entre routeurs de SA différents, appelés EGP (Exterior Gateway Protocol).

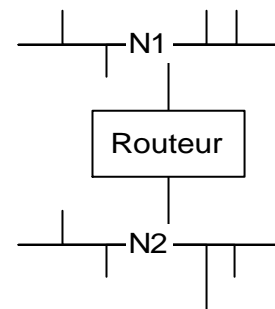
Le RIP (Routing Information Protocol) est le protocole IGP le plus largement utilisé.

Le RIP met en œuvre l'algorithme du Distant Vector qui est basé sur l'échange des tables de routage entre des routeurs adjacents, c'est à dire sur un même réseau physique.

On suppose que chaque routeur connaît initialement les routes qui correspondent aux réseaux auxquels il est rattaché.

Les adresses des réseaux sont désignées par N1, N2, ...

Destination	Routeur	Distance
N1	Direct	1
N2	Direct	1

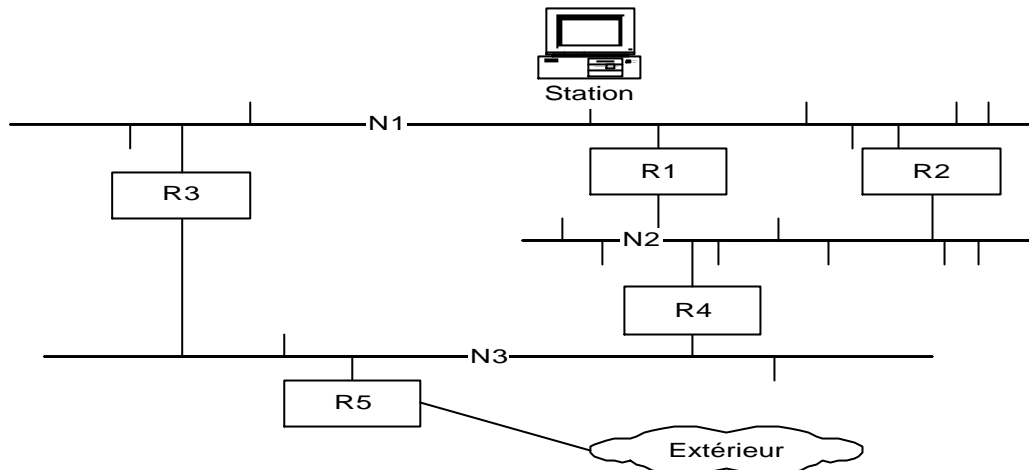


La distance est le nombre de routeur+1 que le datagramme doit physiquement traverser pour atteindre le réseau concerné.

Chaque routeur diffuse périodiquement (en général toutes les 30s) une copie de sa table aux routeurs adjacents. Quand un routeur reçoit une nouvelle table il exécute le traitement suivant (algorithme de Ford Fulkerson, Bellman-Ford) :

- S'il ne possède pas l'entrée d'une nouvelle table, il la rajoute.

- Si la distance d'une nouvelle route proposée est meilleure que celle de sa table, il modifie sa table en conséquence.



La station fait une écoute silencieuse des tables de routage diffusées sur le réseau pour mettre à jour sa propre table de routage.

De : Destination ; Ro : Routeur; Di : Distance ; Dir : Direct; * : Route par défaut.

Au départ

Station			Routeur R1			Routeur R2			Routeur R3			Routeur R4			Routeur R5														
De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di												
N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1	N2	Dir	1	N3	Dir	1	N2	Dir	1	N3	Dir	1	N3	Dir	1	*	Dir	1
N2			N2	Dir	1	N2	Dir	1	N2			N3	Dir	1	N3	Dir	1												

La 1^{ère} diffusion donne le résultat suivant :

Station			Routeur R1			Routeur R2			Routeur R3			Routeur R4			Routeur R5																							
De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di																					
N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	R1	2	N1	R3	2	N1	R1	2	N1	R3	2	N1	R1	2	N1	R3	2									
N2	R1	2	N2	Dir	1	N2	Dir	1	N2	Dir	1	N2	R1	2	N2	R4	2	N2	R1	2	N2	R4	2	N2	R1	2	N2	R4	2	N2	R1	2	N2	R4	2			
N3	R3	2	N3	Dir	1	N3	Dir	1	N3	R4	2	N3	Dir	1	N3	R4	2	N3	R5	2	N3	R4	2	N3	R5	2	N3	R3	2	N3	R4	2	N3	R5	2	N3	R3	2

Les routeurs R1 et R2 reçoivent de R3 et R4 une route pour aller au réseau N3 en passant par un routeur, dans l'exemple le routeur R4 est choisi.

La 2^{ème} diffusion donne le résultat suivant :

Station			Routeur R1			Routeur R2			Routeur R3					
De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di			
N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1
N2	R1	2	N2	Dir	1	N2	Dir	1	N2	Dir	1	N2	Dir	1
			N3	R3	2	N3	Dir	1	N3	R4	2	N3	R4	2
			*	R5	3	N3	Dir	1	*	R4	3	*	R4	3

N3	Dir	1		N2	Dir	1	*	R5	2	De	Ro	Di	N1	R3	2		
N2	R1	2	Routeur R4			N3	Dir	1		N3	Dir	1	N2	R4	2		
*	R5	2	De	Ro	Di	N1	R1	2	Routeur R5			*	Dir	1			

La distance est appelée *métrique*.

Imaginons le routeur R4 qui tombe en panne : Les routeurs R1, R2 et R5 ne reçoivent plus de paquet de R4, ils mettent leur métrique à l'infini.

Station			Routeur R1			Routeur R2			Routeur R3			Routeur R4			Routeur R5		
De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di
N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1	N2	Dir	1	N3	Dir	1
N2	R1	2	N2	Dir	1	N2	Dir	1	N3	Dir	1	N3	Dir	1	*	Dir	1
N3	R3	2	N3	-	α	N3	-	α	N2	R1	2	N1	R1	2	N1	R3	2
*	R3	3	*	-	α	*	-	α	*	R5	2	*	R5	2	N2	-	α

Diffusion suivante : Les routeurs R1 et R2 prennent la route au réseau N3 fournie par R3, le routeur R5 prend la route fournie par R3 pour atteindre N2.

Station			Routeur R1			Routeur R2			Routeur R3			Routeur R4			Routeur R5		
De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di	De	Ro	Di
N1	Dir	1	N1	Dir	1	N1	Dir	1	N1	Dir	1	N2	Dir	1	N3	Dir	1
N2	R1	2	N2	Dir	1	N2	Dir	1	N3	Dir	1	N3	Dir	1	*	Dir	1
N3	R3	2	N3	R3	2	N3	R3	2	N2	R1	2	N1	R1	2	N1	R3	2
*	R3	3	*	R3	3	*	R3	3	*	R5	2	*	R5	2	N2	R3	3

7.5 Le protocole RIP

RIP différencie les machines passives écoutent silencieusement les tables, les stations, des machines actives, les routeurs, qui émettent périodiquement les tables.

Les messages RIP sont encapsulés dans des datagrammes UDP (utilise le port 520), eux-mêmes encapsulés dans des datagrammes IP.

Le format d'un message RIP est donné figure suivante.

La valeur du champ commande indique le type du message :

- 1 Le message est une requête de demande de table. Cette requête est utilisée quand une machine démarre pour obtenir les tables sans attendre leur prochaine diffusion.
- 2 Le message est une réponse, il s'agit d'un message qui contient une table de routage. Il est émis soit en réponse à une requête, soit périodiquement comme le prévoit l'algorithme, soit à la suite d'une reconfiguration du réseau.

Le champs version est toujours à 1.

Il faut un groupe de 10 mots (20 octets) pour identifier une entrée dans la table de routage; on peut transmettre jusqu'à 25 entrées, c'est à dire 25 fois 20 octets.

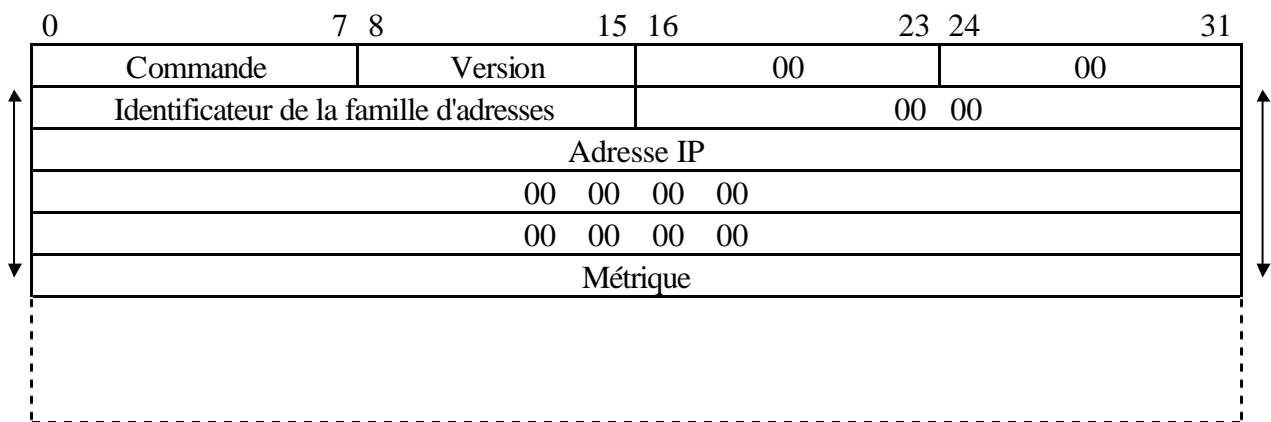
Chaque groupe de 10 mots contient :

Le champ identificateur de la famille de protocole qui vaut toujours 2 (adresses Internet).

Une adresse IP qui peut être :

- ✓ Soit l'adresse d'un réseau (par exemple 140.10.0.0, en classe B).
- ✓ Soit l'adresse d'un sous-réseau.
- ✓ Soit l'adresse d'une station (par exemple 195.25.50.11, la station est directement connectée sur une interface d'un routeur).
- ✓ Soit la route par défaut 0.0.0.0.

Le champ métrique contient le nombre de routeurs à traverser, sa valeur maximale est 15. La valeur de 16 représente une métrique infinie.



Sur un "routeur Unix", le démon de routage *routed* utilise le protocole RIP.

7.6 Autres protocoles

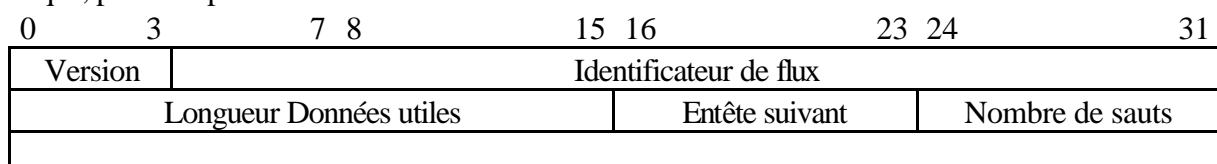
- IGP (Internes au SA) : RIP-2, IGRP, OSPF (algorithme du Link State).
- EGP (pour l'échange de tables entre routeurs de SA différents) : BGP, EGP.

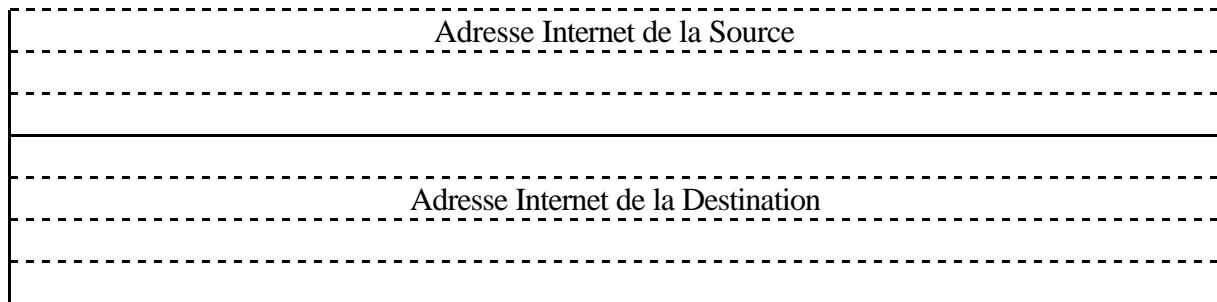
8. LE PROTOCOLE IPv6

Les adresses Internet sont sur 128 bits. La taille de l'entête est fixe, il n'y a plus d'options ni de checksum. Les adresses s'expriment sur des mots de 16 bits en hexadécimal séparés par des "deux points". Par exemple :

ABCD:1234:9876:A45C:0AFE:5ABC:725A:40B2

Les classes de réseaux ont été abandonnées au profit de familles d'adresses qui ont en commun un préfixe identique, par exemple le même 1^{er} octet.





Explications sur les divers champs

- Version : Toujours à 6
- Identificateur de flux : Ce champ contient une priorité pour les routeurs, le but est de faciliter le travail des routeurs et d'offrir une certaine qualité de service.
- Longueur des données utiles : Taille en octets du champs Données.
- Entête suivant : Indique le protocole de niveau supérieur auquel est destiné le datagramme, identique au champ Protocole dans IPv4.
- Nombre de sauts : Ce nombre est décrémenté à chaque routeur, identique au champ Durée de vie (TTL) dans Ipv4.