Chapitre 4

Couche Réseau

1. Introduction

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 réseau. Ces moyens sont situés, selon le modèle OSI, au niveau de la couche 3 : la couche réseau.

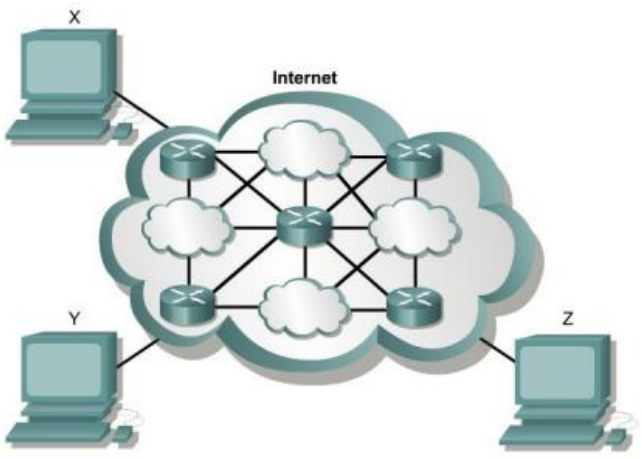
La couche réseau est appelée, donc, à fournir les procédures et les moyens fonctionnels nécessaires à l'échange des informations données par la couche transport. C'est un service de bout en bout qui est responsable de l'acheminement des paquets de données qui peuvent traverser plusieurs nœuds intermédiaires.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

Les caractéristiques de cette couche ont été déterminées par la réalisation effective de réseaux d'ordinateurs généraux (Internet). La couche réseau du modèle OSI correspond à la couche Internet du modèle TCP/IP.

2. TCP/IP et l'Internet

Le réseau « Internet » a été créé dans le but de fournir un réseau de communication capable de fonctionner en cas de guerre.

Internet fait appel au principe d'interconnexion de la couche réseau. Ce qui nous amène au concept d'interréseaux. Un interréseau est un réseau qui comprend plusieurs réseaux.



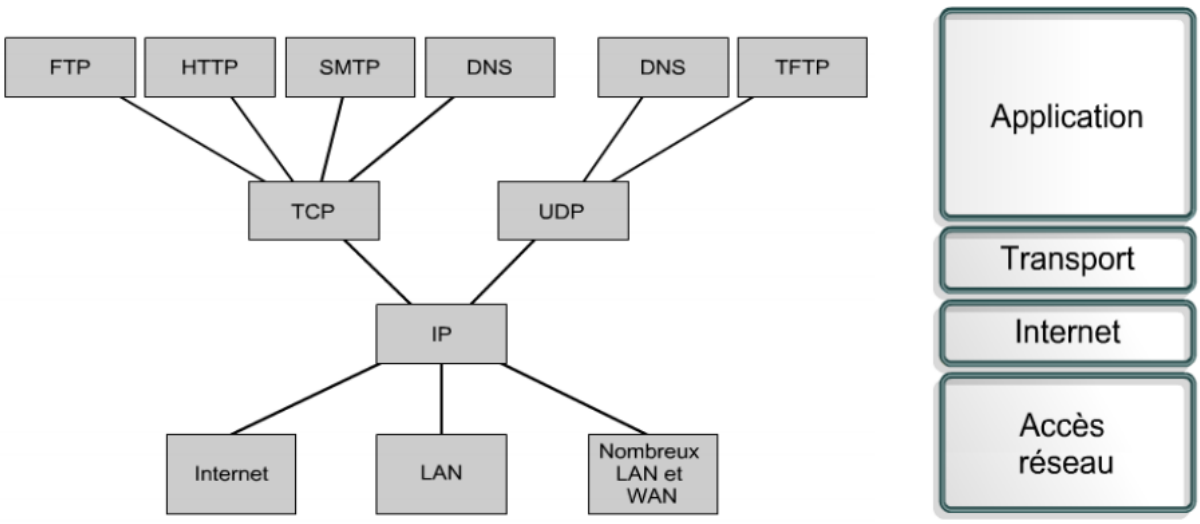
Le réseau Internet repose sur le modèle TCP/IP qui a été développé en vue d'avoir un réseau pouvant résister à toutes les situations (les données doivent être transmises quel que soit l'état d'un nœud/réseau). Depuis son développement, le modèle TCP/IP s'est imposé comme la norme Internet.

2.1. Historique : Quelques dates importantes

- 1969 : aux Etats Unis, l'agence gouvernementale DARPA (Defense Advanced Research Projects Agency) lance un projet de réseau expérimental, nommé ARPANET, basé sur la commutation de paquets.
- 1975 : le réseau passe officiellement du stade expérimental au stade opérationnel.
- 1978 : Jon Postel2 définit IPv4.
- 1981 : IP est standardisé dans la RFC7 91[*J.P ostel*1981].
- 1983 : les protocoles TCP/IP sont adoptés comme un standard militaire et toutes les machines sur le réseau commencent à l'utiliser.
- 1990 : fin d'ARPANET. Internet demeure, il désigne maintenant un espace de communication qui englobe la planète toute entière.

2.2. Le modèle TCP/IP

Le modèle TCP/IP est constitué de quatre couches : Application, Transport, Internet et Accès réseau :



2.3. Couche Internet

Couche d'interconnexion de réseaux. De nombreux services sont fournis par cette couche :

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

Le principal protocole de cette couche est le protocole **IP**. Les protocoles ci-dessous s'exécutent au niveau la couche Internet :

- **Le protocole IP (Internet Protocol)**
  - Assure l'acheminement au mieux des paquets, non orienté connexion.
- **Le protocole ICMP (Internet Control Message Protocol)**
  - Offre des fonctions de messagerie et de contrôle.
  - Signalisation de problèmes entre routeurs.
- **Le protocole ARP (Address Resolution Protocol)**
  - Détermine une adresse MAC (physique) pour une adresse IP connue (IP → MAC).
- **Le protocole RARP (Reverse Address Resolution Protocol)**
  - Détermine l'adresse IP pour une adresse MAC connue (MAC → IP).

3. L'adressage IP

Tout équipement sur à un réseau TCP/IP doit disposer d'une adresse IP unique. Cette adresse permet à un ordinateur de localiser un autre ordinateur sur le réseau.

3.1. L'adresse IP

Une adresse IP est une séquence de 32 bits composée de 1 et de 0.

Exemple :

Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous forme de quatre nombres décimaux séparés par des points.

Exemple :

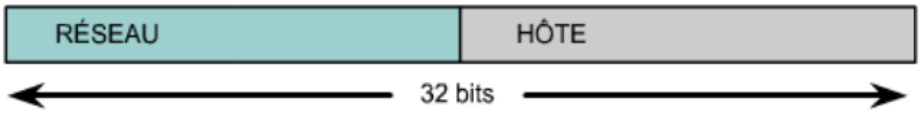
L'adresse IP d'un ordinateur : 192.168.1.8 correspond à la valeur :

11000000.10101000.00000001.00001000 en notation binaire.

Remarque : Chaque élément d'une adresse est un octet, donc, il représente une valeur comprise entre 0 et 255.

Chaque adresse IP comporte également deux parties :

- La première partie **« partie réseau »** identifie le réseau auquel la machine est connectée.
- La seconde partie **« partie hôte »** identifie la machine.



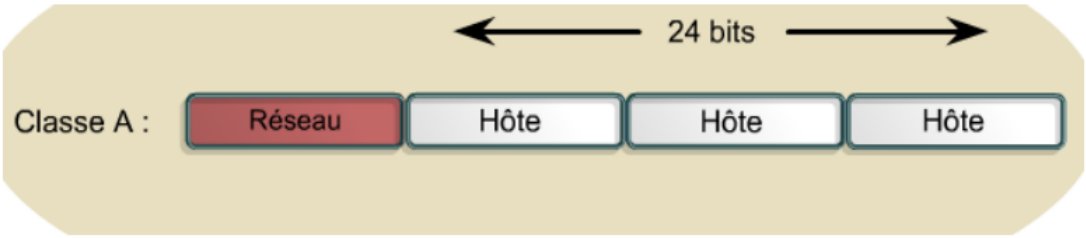
3.2. Les classes des adresses IP

Les adresses IP sont réparties en classes afin de permettre l'adaptation à des réseaux de différentes tailles (grande, moyenne et petite taille) et de faciliter leur classification.

Un bit, ou une séquence de bits, situé en début d'adresse détermine la classe de l'adresse. Il existe cinq classes d'adresses IP :

3.2.1. Les adresses de classe A

- Elles utilisent le **premier octet** pour indiquer l'adresse réseau. Les **trois octets** suivants sont utilisés pour définir les adresses hôte.



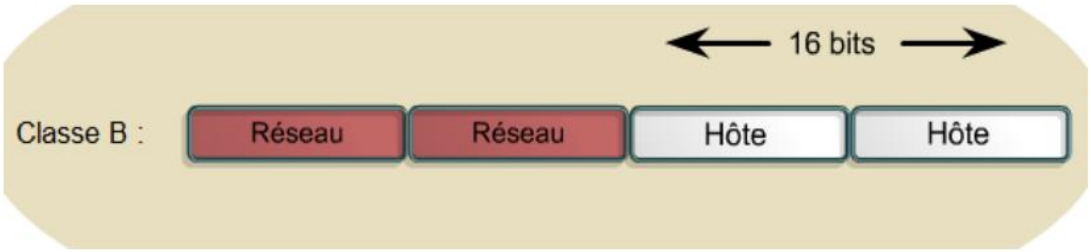
- Le **premier bit** d'une adresse de classe A est toujours **0** → Les adresses sont entre : **0**0000000 (0 en décimal) et **0**1111111 (127 en décimal).
- Les valeurs **0** et **127** sont réservées et ne peuvent pas être utilisées comme adresses réseau. Ainsi, toute adresse commençant par une valeur comprise entre 1 et 126 dans le premier octet est une adresse de classe A.

Remarques :

- Les adresses de la classe A sont réservées aux réseaux de très grande taille, avec plus de 16 millions d'adresses hôte disponibles.
- La plage d'adresses 127.x.x.x est réservée et utilisée pour les tests et diagnostiques.

3.2.2. Les adresses de classe B

- Elles utilisent les **deux premiers octets** pour indiquer l'adresse réseau. Les **deux autres octets** sont utilisés pour les adresses hôte.

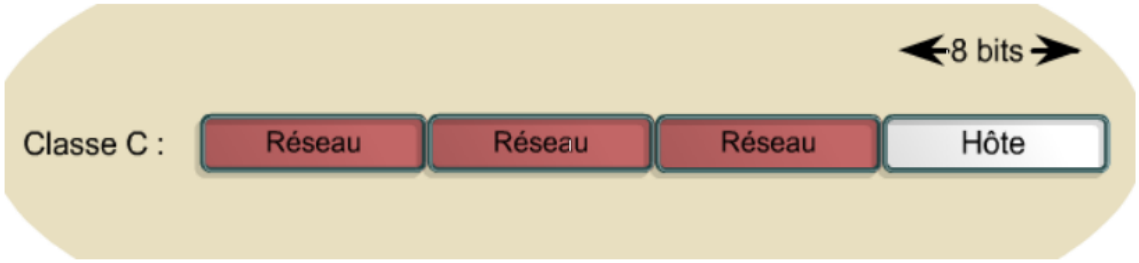


- Les **deux premiers bits** du premier octet d'une adresse de classe B sont toujours **10** → L'adresse la plus faible est **10**000000 (128 en décimal) et la plus élevée est **10**111111 (191 en décimal).
- Toute adresse commençant par une valeur comprise entre **128** et **191** dans le premier octet est une adresse de classe B.

Remarque : Les adresses de la classe B sont réservées aux réseaux de taille moyenne ou grande.

3.2.3. Les adresses de classe C

- Elles constituent l'espace le plus utilisé des classes d'adresses.

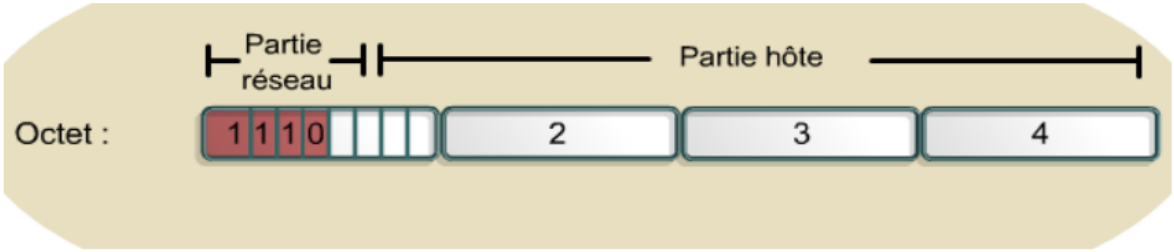


- Elles utilisent **trois octets** pour représenter l'adresse réseau et **un octet** pour définir l'adresse hôte.
- Une adresse de classe C commence par la valeur binaire **110** → L'adresse la plus faible est **110**00000 (192 en décimal) et la plus élevée est **110**11111 (223 en décimal).
- Toute adresse contenant un nombre compris entre **192** et **223** dans le premier octet est une adresse de classe C.

Remarque : les adresses de classe C sont réservées aux réseaux de petite taille (254 hôtes maximum).

3.2.4. Les adresses de classe D

- Réservées à la diffusion multicast d'une adresse IP.

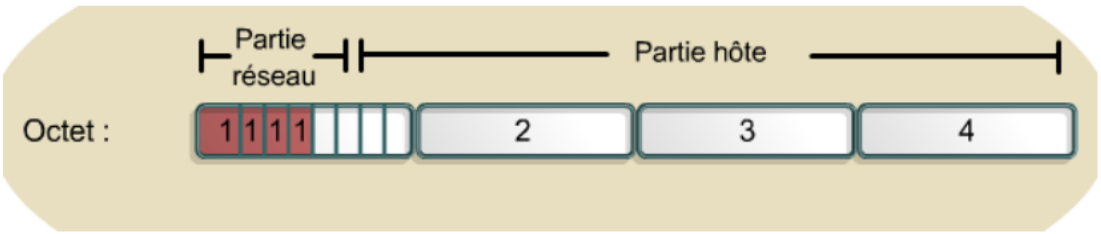


- Les **quatre premiers bits** doivent correspondre à **1110**. Par conséquent, le premier octet d'une adresse de classe D est compris entre **1110**0000 et **1110**1111 (soit 224 et 239 en décimal).
- Toute adresse IP commençant par une valeur comprise entre **224** et **239** dans le premier octet est une adresse de classe D.

Remarque : Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP.

3.2.5. Les adresses de classe E

- Utilisées à des fins expérimentales.



- Les **quatre premiers bits** d'une adresse de classe E sont toujours des 1. Par conséquent, le **premier octet** d'une adresse de classe E est compris entre **1111**0000 et 11111111 (soit 240 et 255 en décimal).
- Aucune adresse de classe E n'est disponible sur Internet.

3.3. Les adresses IP réservées, privées et publiques

3.3.1. Les adresses réservées

Certaines adresses hôte sont réservées et ne peuvent pas être affectées aux équipements du réseau. Ces adresses sont:

- **L'adresse réseau**

L'adresse réseau est celle dont tous les bits hôte sont à **0**. Elle est utilisée pour identifier le réseau lui-même.

- **L'adresse de broadcast**

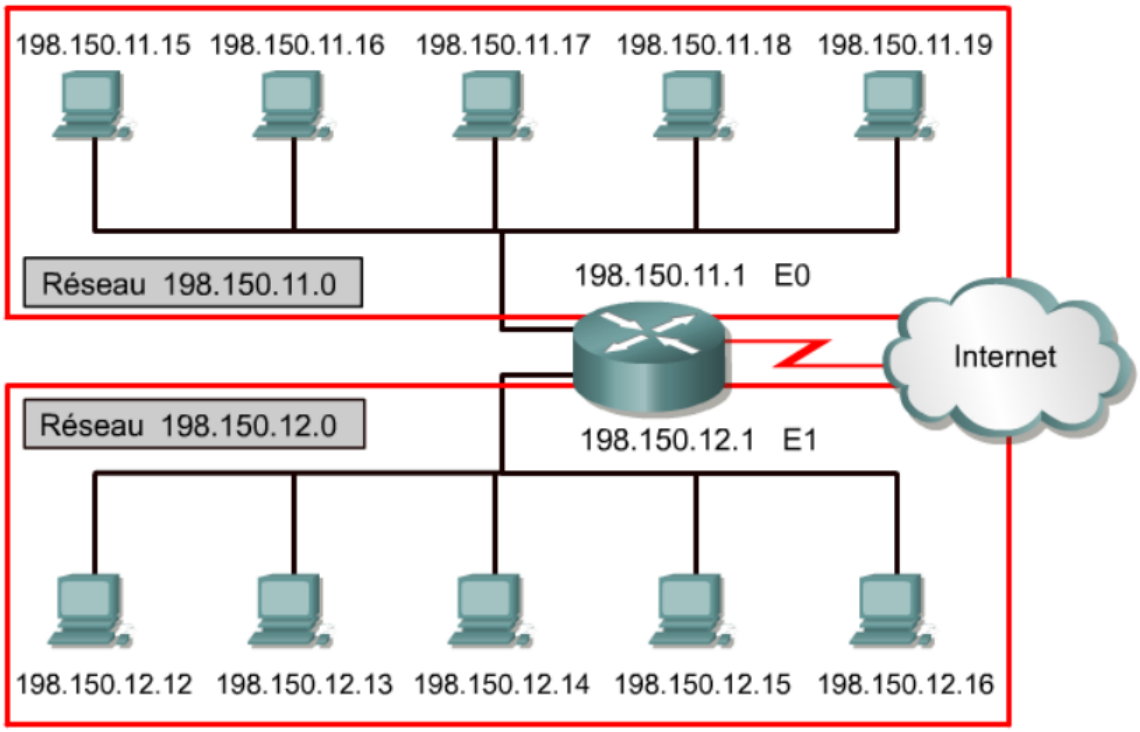
Est une adresse IP dont tous les bits hôte sont à **1**. Elle est utilisée pour diffuser des paquets vers tous les équipements d'un réseau.

Exemple 1:

Dans un réseau de classe B, les 16 derniers bits forment la partie hôte, ainsi :

- L'adresse 176.10.0.0 est une adresse réseau.
- L'adresse de broadcast est 176.10.255.255 (255 correspond à la valeur décimale d'un octet contenant 11111111).

Exemple 2 :



On a deux réseaux locaux (LAN) reliés par un routeur : le premier est celui dont l'adresse est 198.150.11.0 (la partie hôte vaut 0), le deuxième a l'adresse 198.150.12.0.

- Les données envoyées aux hôtes : 198.150.11.1, …. , 198.150.11.254, seront visibles en dehors du réseau local sous la forme 198.150.11.0 → Les numéros d'hôte ne sont pris en compte que localement.
- L'adresse de broadcast du premier réseau est 198.150.11.255 (les bits de la partie hôte sont à 1). Les données envoyées à cette adresse seront lues par tous les hôtes du réseau, de 198.150.11.1 à 198.150.11.254.

3.3.2. Les adresses privées

Les adresses privées sont des adresses IP réservées pour une utilisation privée et interne (intranet non public ou un réseau domestique).

Trois blocs d'adresses privées existent :

- Une plage d'adresses de classe A : 10.0.0.0 – 10.255.255.255
- Une de classe B : 172.16.0.0 – 172.31.255.255
- Une autre de classe C : 192.168.0.0 – 192.168.255.255

Les adresses contenues dans ces plages ne sont pas acheminées sur les routeurs du backbone d'Internet (Les routeurs Internet les rejettent immédiatement).

Remarque : Les adresses IP privées constituent une solution au problème de pénurie des adresses IP publiques. Les hôtes d'un réseau public doivent disposer d'une adresse IP unique. Néanmoins, les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse hôte, pourvu qu'elle soit unique.

3.3.3. Les adresses IP publiques

- Les hôtes d'un réseau public doivent disposer d'une adresse IP unique.
- Les réseaux privés qui ne sont pas connectés à Internet peuvent utiliser n'importe quelle adresse, pourvu qu'elle soit unique.

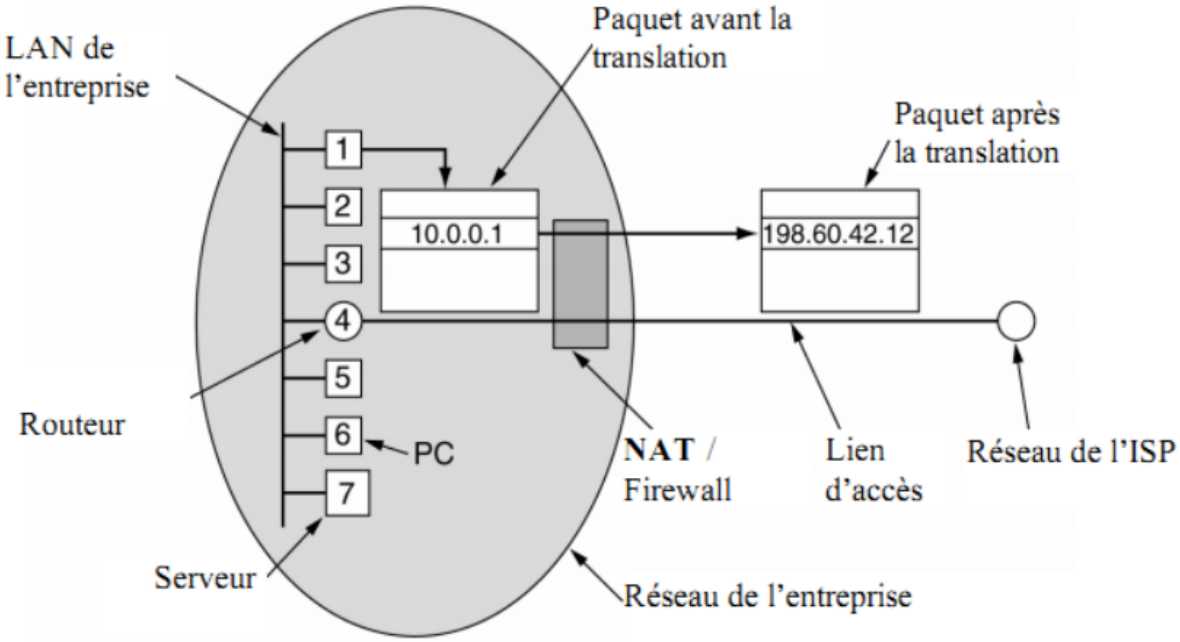
3.4. Traduction d'adresse réseau : NAT (Network Address Translation)

La traduction d'adresse réseau (NAT) permet de faire correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Elle permet de :

- Faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un privé.
- Diminuer significativement le nombre d'adresses IP uniques utilisées.
- Pallier l'épuisement des adresses IPv4.

Remarque : La NAT permet de rendre les adresses privées invisibles depuis Internet.

Exemple :



3.5. Attribution d'adresses IP

Dans Internet l'adresse IP publique d'un équipement est unique. Afin de garantir qu'une même adresse IP publique n'est pas utilisée deux fois, un organisme IANA (Internet Assigned Numbers Authority) gère scrupuleusement les adresses IP disponibles.

Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI).

Il existe plusieurs façons d'attribuer une adresse IP à un équipement :

- **Statique :** L'équipement possède toujours la même adresse.
- **Dynamique :** L'équipement se voit attribuer une adresse différente à chaque connexion au réseau.

Remarque : Un ordinateur peut être connecté à plusieurs réseaux. Ainsi, il reçoit plusieurs adresses. Chaque point de connexion, ou interface, dispose d'une adresse.

3.6. IP version 4 et 6

La version du protocole IP actuellement utilisée sur Internet est IPv4. Avec la croissance rapide d'Internet, le problème de pénurie d'adresses IP publiques est apparu (le nombre d'adresses IP ne suffit plus). Pour résoudre ce problème, un nouveau système d'adressage a été développé : la norme IPv6.

Le protocole IPv6 apporte des améliorations à la version IPv4 et fournit un espace d'adressage beaucoup plus important. Il encode les adresses sur 128 bits au lieu de 32 (en utilisant des nombres hexadécimaux). Un exemple d'une adresse IPv6 est :
A524 :72D3 :2C80 :DD02 :0029 :EC7A :002B :EA73

3.7. Le masque de réseau

Une adresse IP comporte une partie réseau et une partie hôte. Afin de différencier ces deux numéros, un masque de réseau est nécessaire.

Le masque de réseau est une adresse IP dont les bits de la partie réseau sont à **1** et ceux de la partie hôte à **0**. Ce masque permet d'obtenir l'adresse réseau en effectuant une opération **AND logique** sur l'adresse et le masque de réseau.

Exemple : dans une adresse IP de classe B, la partie réseau comporte les deux premiers octets, et les deux derniers sont ceux de la partie machine → le masque de réseau d'une adresse de classes B est :
11111111.11111111.00000000.00000000 → 255.255.0.0
Soit l'adresse IP : 176.11.16.1 d'une machine, pour avoir l'adresse réseau, on fait :
(176.11.16.1) AND (255.255.0.0) = 176.11.0.0
Remarque : le masque est très important dans le cas d'un découpage en sous réseaux.

3.8. Les sous réseaux

Le découpage d'un réseau en sous-réseaux permet de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces.

Dans la conception d'un réseau, il est essentiel de définir le nombre de sous-réseaux requis, ainsi que le nombre d'hôtes requis par sous réseau.

- **Avantages**
  - Faciliter la gestion du réseau.
  - Confiner le broadcast.
  - Garantir une certaine sécurité sur le réseau LAN (autoriser ou refuser l'accès à un sous-réseau en fonction de plusieurs critères).

- **Comment faire le découpage ?**

Pour créer une adresse de sous-réseau, il faut emprunter des bits au champ d'hôte et les désigner comme champ de sous-réseau.

Le nombre de bits à sélectionner dans le processus de découpage en sous-réseaux dépend du nombre maximal d'hôtes requis par sous-réseau.

Pour savoir combien de bits doivent être empruntés, il faut :

- Calculer le nombre de sous-réseaux requis ainsi que le nombre d'hôtes nécessaires au sous-réseau le plus vaste.
- Il faut savoir l'emprunt de N bits donne combien de sous-réseaux utilisables, et combien de hôtes utilisables pour chaque sous-réseau. Il y a une différence entre les hôtes utilisables et le nombre total d'hôtes (y compris les deux adresses réservées : l'adresse du réseau et celle de broadcast). Pour ce faire, la méthode se base sur les formules suivantes :

$$\textbf{Nbr sous-réseaux utilisables} = (2^{\textbf{nombre de bits empruntés}})$$

$$\textbf{Nbr hôtes utilisables} = (2^{\textbf{nombre de bits hôtes restants}}) - 2$$

Remarque : pour le nombre d'hôtes, **– 2** correspond aux adresses du sous-réseau et de broadcast du sous-réseau).

Exemple : Supposons que nous devons faire la conception d'un réseau qui requiert six sous-réseaux de 25 hôtes chacun. On essaye jusqu'à arriver au bon choix :

- L'emprunt d'1 bit donne 2 sous-réseaux => Non.
- L'emprunt de 2 bits donne 4 sous-réseaux => Non.
- L'emprunt de 3 bits donne :

  $2^3 = 8$, huit sous-réseaux utilisables (> 6).

  $(2^5) - 2 = 30$, trente (> 25) hôtes utilisables pour chaque sous-réseau.

Donc, ceci répond tout à fait à nos besoins.

Remarque : Il est possible d'itérer ce découpage plusieurs fois (on aura des sous sous-réseaux, etc.) => d'où la notion d'adressage hiérarchique.

- **Le masque de sous réseau**

Le masque de sous-réseau apporte au routeur l'information dont il a besoin pour déterminer le réseau et le sous-réseau auxquels un hôte donné appartient.

Le masque de sous-réseau est créé en mettant **1** dans les positions des bits du réseau ainsi que ceux empruntés pour créer les sous réseaux.

Exemple :

Le masque de réseau d'une adresse de classe C est :

11111111.11111111.11111111.00000000 → 255.255.255.0.

Si trois bits sont empruntés pour créer des sous réseaux, le masque de sous réseau est :

11111111.11111111.11111111.**111**00000 → 255.255.255.224

Remarque : Une forme plus courte est connue sous le nom de **« notation CIDR »** (Classless Inter-Domain Routing). Elle donne le numéro du réseau suivi par une barre oblique (ou slash, « / ») et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau.

Exemple : Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par **/19** (19 bits à la valeur 1, suivis de 13 bits 0). La notation 91.198.174.2/19 désigne donc l'adresse IP 91.198.174.2 avec le masque 255.255.224.0, et signifie que les 19 premiers bits de l'adresse sont dédiés à l'adresse du sous-réseau, et le reste à l'adresse de l'ordinateur hôte à l'intérieur du sous-réseau.

- **Utilisation du masque de sous réseau**

Afin de savoir l'adresse de sous réseau, on effectue une opération **AND logique** entre l'adresse IP et le masque de sous réseau. Il est par conséquent nécessaire d'afficher l'adresse IP et le masque au format binaire.

Exemple :
Adresse du paquet : 201.10.11.65 et Masque : 255.255.255.224
(11001001.00001010.00001011.01000001) AND (11111111.11111111.11111111.11100000)
→ 11001001.00001010.00001011.01000000
L'adresse du sous réseau est : 201.10.11.64

Remarque : Cette opération est effectuée par le routeur pour déterminer le sous-réseau de chacun des nœuds.

4. Le routage

Le routage est l'acheminement des données de la source vers la destination tout en cherchant le chemin le plus efficace. L'équipement utilisé est le routeur.

Les protocoles de routage utilisent diverses combinaisons des métriques pour établir la meilleure route possible des données (délai, bande passante, coût, charge, fiabilité, etc.). Les routes d'acheminement sont stockées dans des Tables de routage.

4.1. Table de routage (TR)

Les tables de routage contiennent les informations d'acheminement nécessaires à la transmission des paquets de données sur le réseau. En utilisant ces tables, le processus de sélection du chemin est facilité.

Les routeurs emploient des protocoles de routage pour construire et gérer les tables de routage. Les informations d'acheminement contenues dans les tables de routage varient selon le protocole de routage utilisé. Les plus importantes sont :

- **Type de protocole:** identifie le type de protocole de routage utilisé.
- **Associations du saut suivant:** indique au routeur que la destination lui est directement connectée, ou qu'elle peut être atteinte par le biais d'un autre routeur appelé le « saut suivant » vers la destination finale.
- **Métrique de routage:** permet de déterminer les avantages d'une route sur une autre (exemple : le nombre de sauts).
- **Interfaces de sortie:** Désigne l'interface à partir de laquelle les données doivent être envoyées pour atteindre leur destination finale.

4.2. Utilisation des TR pour déterminer le chemin

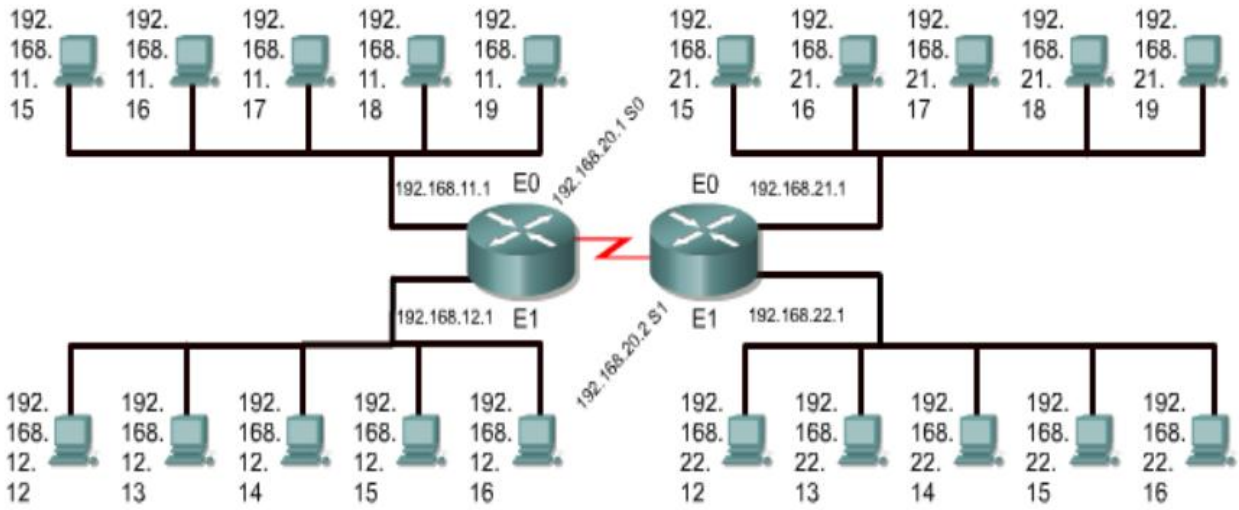
- Dès la réception d'un paquet, le routeur vérifie l'adresse de destination et tente de trouver une correspondance dans sa table de routage pour déterminer le chemin à suivre.
- La détermination du chemin permet au routeur de choisir le port à partir duquel envoyer le paquet pour qu'il arrive à destination.
- Chaque routeur rencontré sur le chemin du paquet est appelé un saut.
- Le nombre de sauts constitue la distance parcourue.

La détermination du chemin par le routeur peut être comparée à la situation d'une personne conduisant sa voiture d'un endroit de la ville à un autre :

- Le conducteur consulte une carte qui lui indique les rues à prendre pour arriver à sa destination.
- Le routeur de même consulte sa table de routage.
- Il passe par la voiture d'un carrefour à un autre.
- De même, un paquet circule d'un routeur à un autre lors de chaque saut.
- À chaque carrefour, le conducteur peut choisir de prendre à gauche, à droite ou de continuer tout droit.
- Le routeur, aussi, choisit le port de sortie à partir duquel le paquet sera envoyé.
- Le conducteur prend ses décisions en fonction de certains facteurs (l'état du trafic, le nombre de voies, si une route est fréquemment fermée ou pas).
- Le routeur prend sa décision en fonction de la charge, de la bande passante, du délai, du coût et de la fiabilité d'une liaison de réseau.

→ Ce processus est appelé : Routage d'un paquet.

Exemple : Soit le réseau suivant :



Les tables de routage deux routeurs sont :

Table de routage (routeur gauche)		
Adresse réseau	Saut	Interface
192.168.11.0	0	E0
192.168.12.0	0	E1
192.168.20.0	0	S0
192.168.21.0	1	S0
192.168.22.0	1	S0

Table de routage (routeur droit)		
Adresse réseau	Saut	Interface
192.168.21.0	0	E0
192.168.22.0	0	E1
192.168.20.0	0	S1
192.168.11.0	1	S1
192.168.12.0	1	S1

4.3. La mise à jour des tables de routage

Les routeurs s'envoient des messages afin de mettre à jour leurs tables de routage. Les méthodes de mises à jour diffèrent selon le protocole de routage utilisé :

- Périodique ou lorsque des changements sont intervenus dans la topologie du réseau.
- Transmission de l'intégralité de la table ou seulement les modifications.

4.4. Protocole de routage

Le protocole de routage permet de créer des tables de routage et partager d'autres informations d'acheminement. Les fonctions du protocole de routage sont :

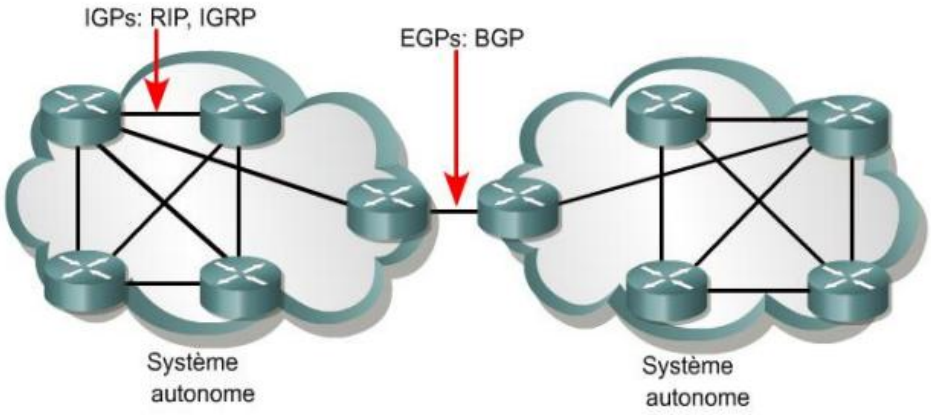
- Fournir les processus utilisés pour partager les informations d'acheminement.
- Permettre aux routeurs de communiquer entre eux afin de mettre à jour et de gérer les tables de routage.

Les protocoles de routage prenant en charge le protocole IP sont par exemple les protocoles : RIP, IGRP, OSPF, BGP et EIGRP.

4.4.1. Type de protocole de routage

Il existe deux familles de protocoles de routage :

- Les protocoles IGP (Interior Gateway Protocol) : Ils acheminent les données au sein d'un système autonome.
- Les protocoles EGP (Exterior Gateway Protocol) : Ils acheminent les données entre les systèmes autonomes.



Nous allons étudier seulement les protocoles IGP. Ces protocoles peuvent être subdivisés en:

- Protocoles à vecteur de distance : ex. le protocole RIP (Routing Information Protocol).
- Protocoles à état de liens : ex. le protocole OSPF (Open Shortest Path First).

a) Les protocoles à vecteur de distance

- Déterminent la direction et la distance vers n'importe quelle liaison de l'interréseau.
- La distance est représentée par le nombre de sauts vers la destination.
- Ces algorithmes envoient périodiquement l'intégralité ou une partie des entrées de leur table de routage aux routeurs adjacents (que des modifications aient été ou non apportées au réseau).
- Lorsqu'un routeur reçoit une mise à jour de routage, il vérifie tous les chemins connus et modifie le cas échéant sa propre table de routage.

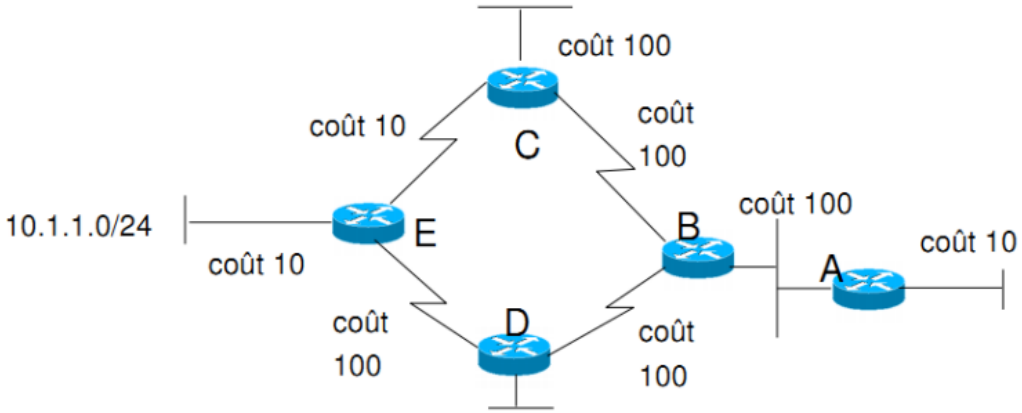
Les protocoles RIP (Routing Information Protocol), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced IGRP) sont des exemples de protocoles à vecteur de distance.

b) Les protocoles à état de liens

- Ils ont été conçus pour pallier les limitations des protocoles de routage à vecteur de distance.
- Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue.

- Ils envoient des mises à jour périodiques (actualisations à état de liens), à des intervalles moins fréquents (ex. toutes les 30 minutes).
- Dès qu'une unité a détecté la modification d'une liaison (route), elle crée une MAJ de routage à état de liens concernant cette liaison.
- Cette mise à jour est ensuite transmise à tous les équipements voisins. Chacun d'eux en prend une copie et met à jour sa base de données à état de liens.
- La diffusion de mises à jour permet aux équipements de routage de créer une vue locale transcrivant la topologie du réseau.
- Chaque routeur possède :
  - Une table de ses voisins, appelé Neighbour table.
  - Une base de données de la topologie du réseau, appelée Topology database.
  - Une table de routage, appelée Routing table.
- Les protocoles OSPF (Open Shortest Path First) et IS-IS (Intermediate System-to-Intermediate System) sont des exemples de protocoles à état de liens.

Exemple :



- Dans les protocoles à état de lien, B ne va pas donner à A le coût de la liaison mais la carte qu'il connaît du réseau.
- Ainsi, A va pouvoir calculer les meilleurs routes vers tous les sous-réseaux en se basant sur les informations topologiques transmises par B.
- Comparativement aux protocoles à vecteur distance, les protocoles à états de liens doivent calculer les coûts vers tous les sous-réseaux.
- Avec les vecteurs distances, B dit à A : sous-réseau 10.1.1.0, métrique 3.
- Avec les états de liens : A va apprendre puis calculer :
  - A vers 10.1.1.0/24 : par C, coût 220.
  - A vers 10.1.1.0/24 : par D, coût 310.
  - Résultat : A mettra dans sa table de routage la route vers 10.1.1.0/24 par C.

4.5. Protocole routé et protocole de routage

Les routeurs se servent des protocoles de routage pour créer les tables de routage. Les protocoles de routage permettent aux routeurs de déterminer le meilleur chemin possible pour acheminer les données de la source vers leur destination. Une fois le chemin est défini, le protocole routé transporte les données sur le réseau (IP).

Remarque : Les chemins configurés manuellement par l'administrateur réseau sont appelés « routes statiques ». Ceux que le routeur a acquis d'autres routeurs à l'aide d'un protocole de routage sont dits « routes dynamiques ».

- **Protocole routé**

  Les fonctions d'un protocole routé sont :

  - Il inclut toute suite de protocoles réseau capable de fournir des informations pour permettre au routeur d'effectuer le transfert vers l'unité suivante, jusqu'à la destination finale.
  - Il définit le format et l'usage des champs dans un paquet.

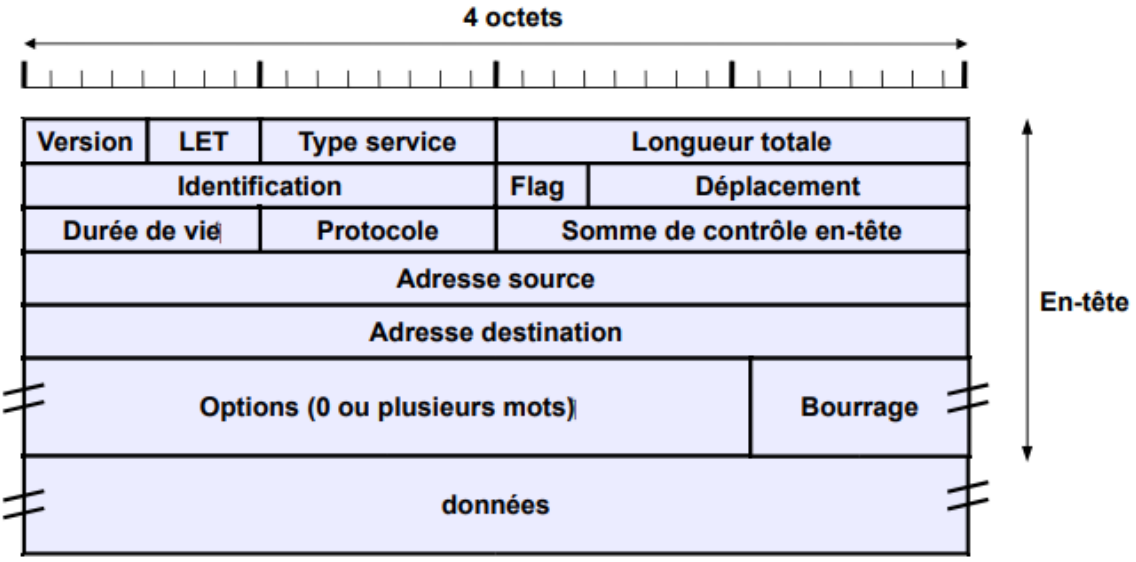
  Le protocole IP (Internet Protocol) est un exemple de protocoles routés.

4.6. Le protocole IP

- IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé.
- C'est un protocole non orienté connexion (aucune connexion à un circuit dédié n'est établie avant la transmission).
- Peu fiable (il ne s'assure pas de la bonne livraison des données envoyées sur le réseau, ceci est effectuée par les protocoles de couche supérieure).
- Axé sur l'acheminement au mieux (best-effort Delivery). Le protocole IP détermine le meilleur chemin pour les données en fonction du protocole de routage.

- **Le paquet IP (datagramme IP)**

  Un datagramme IP, aussi appelé paquet IP, a le format suivant :



- **Version (4 bits) :** indique le format de l'en-tête du paquet IP (IPv4 ou IPv6).
- **LET : Longueur d'en-tête IP (4 bits) :** indique la longueur de l'en-tête du datagramme en nombre de mots de 32 bits.
- **Type de service (8 bits) :** indique des informations au protocole de couche supérieure.
- **Longueur totale (16 bits) :** spécifie la taille totale du paquet en octets, données et en-tête inclus.
- **Identification (16 bits) :** identifie le datagramme actuel (le numéro de séquence).
- **Flags : Drapeaux (3 bits) :** les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment.
- **Déplacement (13 bits) :** Position du fragment par rapport au paquet de départ, en nombre de mots de 8 octets.
- **Durée de vie : TTL (Time To Live) (8 bits) :** indiquant le nombre de sauts par lesquels un paquet peut passer. Lorsque le compteur atteint zéro, le paquet est éliminé.
- **Protocole (8 bits) :** indique le protocole de couche supérieure qui reçoit les paquets.
- **Somme de contrôle de l'en-tête : Header Checksum (16 bits) :** aide à garantir l'intégrité de l'en-tête IP.
- **Adresse source (32 bits) :** l'adresse IP du nœud émetteur du paquet.
- **Adresse de destination (32 bits) :** l'adresse IP du nœud destinataire.
- **Options :** prendre en charge diverses options (la sécurité, etc.).

- **Remplissage (bourrage) :** des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.
- **Données :** ce champ contient les informations de couche supérieure.

Remarque : La Taille maximale d'un datagramme IP est : $2^{16} - 1 = 65535$ octets.

- **La fragmentation IP**

En fait, il existe d'autres limites à la taille d'un datagramme que celle fixée par la valeur maximale de 65535 octets. Notamment, pour optimiser le débit il est préférable qu'un datagramme IP soit encapsulé dans une seule trame de niveau 2 (Ethernet par exemple).

Mais,comme un datagramme IP peut transiter à travers Internet sur un ensemble de réseaux aux technologies différentes il est impossible de définir, a priori, une taille maximale (1500 octets pour Ethernet et 4470 pour FDDI par exemple) des datagrammes IP qui permette de les encapsuler dans une seule trame quelque soit le réseau traversé.

On appelle la taille maximale d'une trame d'un réseau le **MTU** (Maximum Transfert Unit) et elle va servir à fragmenter les datagrammes trop grands pour le réseau qu'ils traversent. Mais, si le MTU d'un réseau traversé est suffisamment grand pour accepter un datagramme, évidemment il sera encapsulé tel quel dans la trame du réseau concerné.

La taille d'un fragment est choisie la plus grande possible tout en étant un multiple de 8 octets. Un datagramme fragmenté n'est réassemblé que lorsqu'il arrive à destination finale. Même s'ils arrivent sur des réseaux avec un plus grand MTU les routeurs ne réassemblent pas les petits fragments.

De plus chaque fragment est routé de manière totalement indépendante des autres fragments du datagramme d'où il provient.

Le destinataire final qui reçoit un premier fragment d'un datagramme arme un temporisateur de réassemblage, c'est-à-dire un délai maximal d'attente de tous les fragments.

Si, passé ce délai, tous les fragments ne sont pas arrivés il détruit les fragments reçus et ne traite pas le datagramme. Plus précisément, l'ordinateur destinataire décrémente, à intervalles réguliers, de une unité le champ TTL de chaque fragment en attente de réassemblage. Cette technique permet également de ne pas faire coexister au même instant deux datagrammes avec le même identifiant.

Les paquets d'information fractionnés s'éparpillent dans le réseau et peuvent arriver dans le désordre, il est donc nécessaire d'indiquer sur chaque datagramme de quel "morceau" il s'agit. Ces indications sont portées par l'entête IP. Elles se composent des bits **O** - **DF** - **MF** et du mot de 13 bits OFFSET DU FRAGMENT.

Champ	Information
O	Toujours zéro
DF	**D**ont' **F**ragment : Ne pas fragmenter ce paquet
MF	**M**ore **F**ragments : ce datagramme n'est pas le dernier fragment du datagramme initial.
OFFSET DU FRAGMENT	Voir explication ci-dessous

Le champ OFFSET FRAGMENT contient, pour chaque fragment, le décalage entre le premier octet de données du datagramme non fragmenté et le premier octet de données fragmentées qu'il transporte.

Ce décalage est zéro pour le premier fragment puisqu'il contient le début de l'ensemble des données à transmettre.

Cependant, la longueur de ce champ est de 13 bits, il ne permet d'écrire que les nombres entiers de 0 à 8192.

Or, la longueur maximale d'un datagramme s'écrit sur 16 bits et peut donc atteindre 65535 octets.

On est donc convenu que le nombre écrit dans le champ " décalage de fragment " indiquerait non pas un nombre d'octets mais un nombre de mots de 8 octets.

Ainsi si ce champ contient le nombre 100, le décalage indiqué est de 800 octets. Lors de la fragmentation, il faudra donc faire en sorte que la longueur des données du datagramme fragment soit un multiple de 8 octets.

Exemple :

Un datagramme est envoyé d'un réseau Token Ring à un hôte du réseau IEEE 802.4 à travers les routeurs A et B.

La taille des datagrammes envoyés par les hôtes du réseau A est généralement égale à la MTU du réseau de départ, soit 4440 pour A.

Supposons donc qu'un datagramme de 4440 octets soit envoyé par un hôte du réseau Token Ring avec un champ d'identification égal à 500 par exemple.

Le routeur A fractionnera cette datagramme en fragments de dimension égale ou inférieure à la MTU du réseau ETHERNET soit 1500 octets ou moins.

Nous allons examiner les caractéristiques des fragments qui en résultent.

Si on ne se sert pas des options, l'entête IP compte 20 octets.

La quantité de données à transmettre est donc de 4440 - 20 = 4420 octets.

La quantité maximale d'octets que peut transmettre, en un seul datagramme, le réseau Ethernet est 1500 - 20 = 1480 octets.

Mais, pour tous les datagrammes sauf le dernier, la quantité d'octets envoyés doit être un multiple de 8.

Ceci afin de pouvoir remplir le champ "décalage" comme vu plus haut.

Il se trouve que 1480 est un multiple de 8 : 1480 = 185 * 8.

Dans le cas contraire, nous aurions retenu le multiple de 8 immédiatement inférieur.

Divisons 4420 par 1480, résultat :

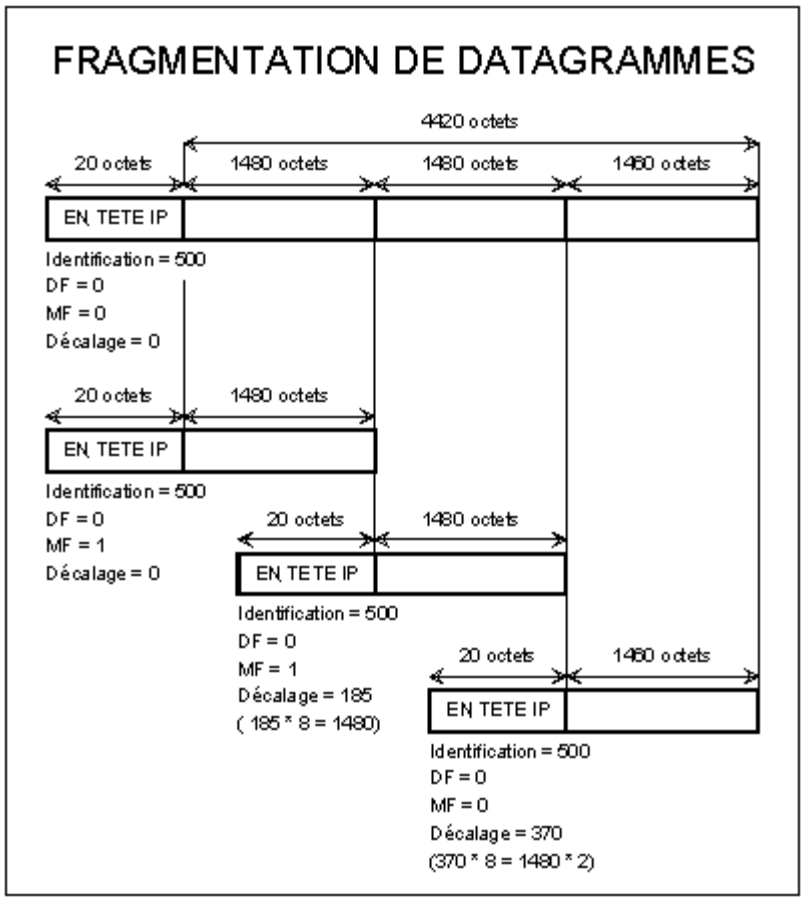
4420 = 2 * 1480 +1460

Nous utiliserons donc deux datagrammes transportant 1480 octets puis un dernier transportant 1460 octets.

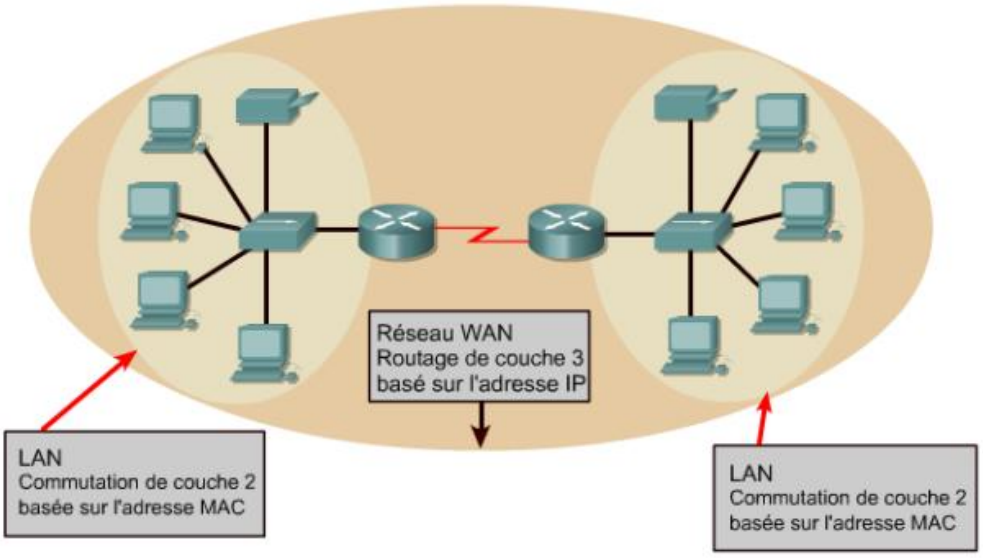
Les fragments obtenus ne sont pas assemblés avant de traverser le réseau terminal IEEE 802.4 bien que sa MTU soit nettement plus élevée.

Leur assemblage interviendra à leur arrivée dans la couche IP de l'hôte de destination.

Il a tous les éléments en main pour le faire : le champ identification pour repérer les fragments d'un même datagramme, les décalages pour les assembler dans l'ordre, le champ MF pour reconnaître le dernier fragment.



5. Routage et commutation



La commutation est une fonctionnalité de la couche 2 du modèle OSI et le routage de la couche 3. Un commutateur ne travaille qu'en couche 2 par contre un routeur en couche 2 et 3, donc, un routeur route et commute.

La commutation consiste à faire passer une trame d'une interface à une autre, tandis que le routage consiste à déterminer le chemin le plus efficace (grâce aux algorithmes de routage il choisit la meilleure route à l'aide des tables de routages) pour atteindre une destination (qui sera finalement traduite à son tour par une commutation).

Le commutateur n'effectue pas cette décision de routage, il ne travaille qu'en couche 2 OSI, il étudie la trame qui arrive et regarde l'adresse MAC de destination pour savoir quel port de sortie permet de joindre cette MAC : le fait qu'une trame passe d'un port à un autre c'est de la commutation.

Autrement dit, après avoir choisi la route en question (choix du "nexthop") → routage ; Il faut chercher quelle interface physique correspond à ce next-hop → commutation.

Remarques :

- Le routage : méthode d'acheminement d'informations à la bonne destination à travers un réseau.
- La commutation: établissement d'une connexion entre deux points d'un réseau.

Plus concrètement : Un concentrateur reçoit une trame sur un port, il lit dans la trame une adresse de couche 2 (@MAC), ce qui lui permettra de décider où acheminer la trame (sur quel port de sortie). Le routeur est capable de s'appuyer sur l'@ IP (de couche 3), il tient une table de routage, qui est mise en place par l'administrateur, et qui lui permet de décider vers quel sous réseau il faut envoyer le paquet reçu.