Chapitre 05 : La couche réseau

1. Introduction

La couche liaison de données assure la transmission de données entre deux équipements adjacents. Cette couche est composée de deux sous-couches dont l'une entre eux (la sous-couche MAC) assure la communication de données dans un réseau local. La couche réseau situé au-dessus de la couche liaison de données permet la communication des machines via un système intermédiaire. En effet, cette couche assure la communication de bout-en-bout.

2. Services de la couche réseau

La couche réseau est chargée de l'acheminement des données de la source vers le destinataire en gérant le trafic à travers les nœuds intermédiaires. L'unité de données échangée à ce niveau est appelé *Paquet*. Afin d'effectuer sa tâche, la couche réseau doit avoir une bonne connaissance de la topologie du sous-réseau de communication. En fait, la connaissance de cette topologie permet à la couche réseau de choisir le chemin adéquat pour acheminer les paquets au destinataire. On appelle cette fonction le routage.

Le choix d'un chemin doit prendre en considération le trafic existant déjà sur les lignes. Il ne faut pas surcharger certaines lignes de communication alors qu'il existe d'autres voies libres. Cette fonction est appelée le contrôle de la gestion.

Afin d'acheminer les paquets, chaque retour doit localiser le destinataire. En d'autre terme chaque machine de réseau doit être repérée de manière unique en utilisant des adresses. En fait, les adresses physiques ne permettent pas la localisation géographique des machines. Ce type d'adressage n'est pas adéquat au niveau de la couche réseau. La couche réseau offre un autre type d'adressage appelé l'adressage logique.

Comme les autres couches, la couche réseau offre des services à la couche immédiatement au-dessus (la couche transport). En fait deux types de services sont offerts : le service avec connexion et le service sans connexion.

Dans un service sans connexion, les paquets (appelés Datagrammes) sont injectés dans le sous réseaux et routés de façon indépendante. Chaque retour du sous réseau maintient une table qui associe pour chaque destination, la ligne de sortie correspondante. Comme il est présenté dans la figure 01, chaque paquet peut prendre un chemin différent des autres paquets. En conséquence, chaque paquet doit avoir l'adresse de destinataire. Le service sans connexion offre la flexibilité de routage en fonction de l'état de sous réseau mais les paquets peuvent arriver en désordre. Cette technique est utilisée dans le protocole IP.

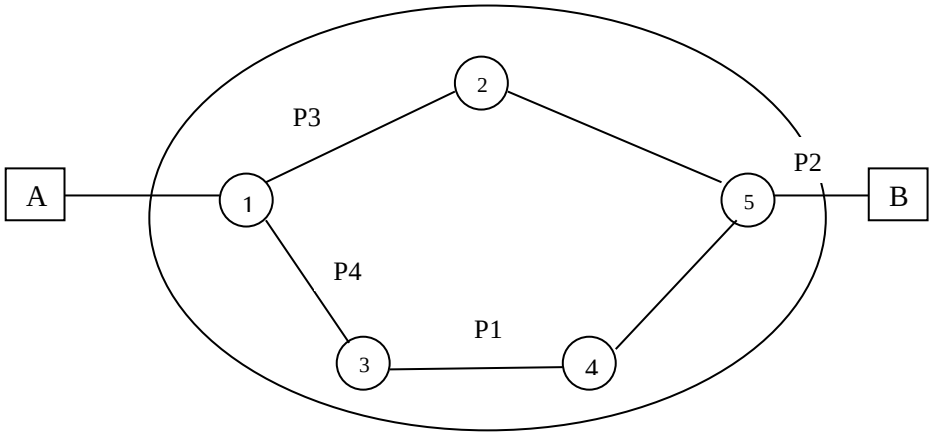

Figure 01 : Le service sans connexion

Le service avec connexion assure le transfert de tous les paquets sur le même chemin, appelé circuit virtuel. Le circuit est décrit par virtuel pour le distinguer de circuit physique. Un circuit physique peut supporter plusieurs circuits virtuels. Il faut donc établir un circuit virtuel avant la transmission des paquets afin d'éviter le choix de chemin dans chaque routeur. Le service avec connexion passe par trois étapes : l'établissement d'une connexion, la transmission des paquets et la libération de la connexion. Lors l'établissement de la connexion, l'émetteur envoie un paquet (appelé paquet d'appel). Ce paquet trace le circuit virtuel qui va être emprunté par tous les autres paquets. Ainsi, les paquets portent le numéro de circuit virtuel et non l'adresse de destinataire. Cette technique est utilisée dans les réseaux x25.

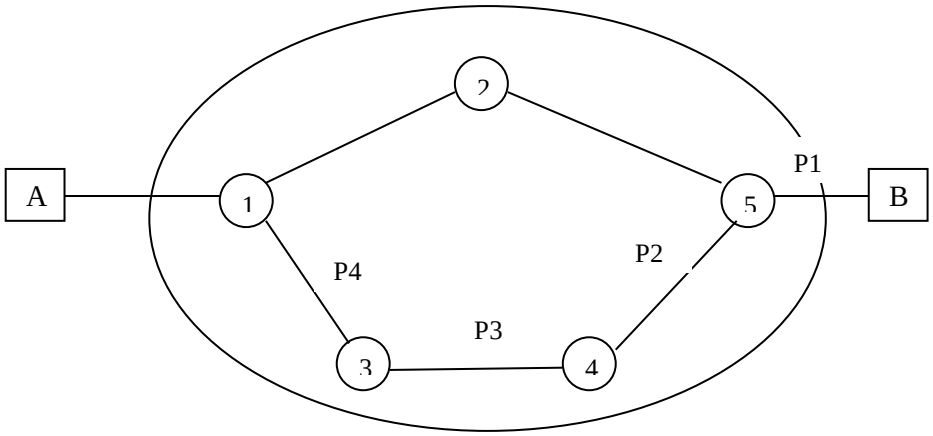

Figure 02 : Le service avec connexion

Le tableau 01 présente une comparaison entre les deux services.

Tableau 01 : Comparaison entre service avec connexion et sans connexion

Critère	**Service sans connexion**	**Service avec connexion**
Adressage	Chaque paquet doit contenir l'adresse complète de source et de destination	Chaque paquet contient un numéro de circuit virtuel (CV)
Informations d'état	Les routeurs ne sauvegardent pas d'informations sur les connexions	Chaque CV nécessite une entrée dans la table de routage
Routage	Chaque paquet routé indépendamment des autres	Tous les paquets empruntent le même chemin.
Effets de panne d'un routeur	Rien sauf les paquets contenus dans le routeur défectueux	Tous les CVs qui le traversent sont terminés
Qualité de service	Difficile	Simple si les ressources nécessaires sont allouées à l'établissement du CV
Contrôle de congestion	Difficile	Simple si les ressources nécessaires sont allouées à l'établissement du CV

3. Les algorithmes de routage

Le routage consiste à associer une ligne de sortie à une ligne d'entrée. Ces informations sont sauvegardées dans des structures de données appelées ***les tables de routage.*** En conséquence, le mécanisme de routage consiste à mettre à jour ces tables afin de trouver un ***chemin optimal*** selon une métrique (comme : coût, distance, nombre de nœuds traversés, temps de transit…etc). Il est important de distinguer le mécanisme de routage de mécanisme d'***acheminement*** qui consiste à la réception des paquets en entrée, de les traiter (contrôle d'erreur) puis les transmettre vers la ligne de sortie correspondante selon la table de routage.

Plusieurs algorithmes ont été proposés pour offrir un mécanisme de routage optimal. On peut classifier ces algorithmes, principalement selon deux critères : l'adaptation et la distribution.

Selon le critère d'adaptation, on distingue les algorithmes statiques (non adaptatifs) et les algorithmes adaptatifs. Les algorithmes statiques chargent au démarrage une table de routage calculée à l'avance et qui sera ainsi fixe, la mise à jour de la table de routage nécessite généralement l'intervention d'administrateurs réseaux. Par contre, les algorithmes de routage adaptatifs consistent à mettre à jour les tables de routage, de façon régulière, pour répondre aux changements de topologie ou de trafic.

Selon le critère de distribution, un algorithme de routage peut être centralisé c'est-à-dire les chemins sont définis par un nœud particulier. C'est un nœud particulier qui possède toutes les informations sur l'état du réseau. Ce nœud est donc en mesure de calculer à chaque instant le chemin optimal entre deux nœuds. Ainsi tout nœud source désirant établir une connexion doit s'adresser au nœud "principal", ce qui augmente le temps pour calculer une route. De plus, il existe un problème de fiabilité important. En effet, si ce nœud de routage venait à être hors service, ou si un des liens le reliant au reste du réseau était coupé, il y aurait alors un impact sur le bon fonctionnement du réseau. Par contre, les algorithmes de routage le choix de chemin est établi par chaque nœud. Ces algorithmes sont favorables du point de vue de la fiabilité, mais ils sont compliqués et l'optimisation de l'acheminement des paquets est difficile. Un routeur collecte les informations sur le trafic et le réseau à partir d'échange de messages avec ses voisins.

3.1. Routage du plus court chemin

Un réseau peut être représenté par un graphe dont les nœuds représentent les routeurs et les arcs représentent les liaisons entres les routeurs. Chaque arc est étiqueté par une distance. En fait, la distance peut représente le nombre de nœuds intermédiaires entre deux machines ou la distance géographique entre des routeurs. Cependant, d'autres métriques spécifiques aux réseaux peuvent être établies comme le débit. En réalité, les métriques représentent le compromis de plusieurs facteurs.

Cette technique de routage consiste à établir le plus court chemin entre deux nœuds à l'aide de l'algorithme de Dijkstra.

3.2. Routage par inondation

C'est un algorithme statique. Son principe est simple, chaque paquet reçu sur une ligne est diffusé sur toutes les autres lignes à l'exception de la voie d'arrivée. Cela peut provoquer la présence de plusieurs duplicata d'un même paquet et l'émission d'un paquet sera un processus éternel. Pour remédier à cet inconvénient, un paquet peut contenir un champ qui marque le nombre de nœuds traversés et sera éliminé s'il atteint une certaine valeur max. mais un paquet peut transiter un nœud plusieurs fois ; si chaque nœud garde une copie des paquets reçus il saura identifier ce phénomène et éliminer ce genre de paquets.

3.3. Routage aléatoire

La technique de l'acheminement aléatoire (***Random Routing, Stochastic Routing***) partage avec la méthode de l'inondation la caractéristique de ne pas nécessiter que les nœuds connaissent la structure du réseau ou l'état du trafic pour prendre la décision du routage à leur niveau. Toutefois, les nœuds évitent ici d'envoyer systématiquement sur toutes les voies de sortie des répliques des paquets qu'ils reçoivent, afin de ne pas produire un trafic fantôme trop important. La méthode de routage aléatoire consiste à émettre une ou plusieurs répliques du paquet reçu sur des voies de sortie qui sont choisies soit au hasard, soit en fonction d'une information sur la direction générale suivie par le paquet. Dans ce dernier cas, la méthode de routage est appelé inondation sélective (*Selective Flooding*). Avec la méthode d'acheminement aléatoire la plus simple, chaque nœud retransmet le paquet reçu sur l'une des voies de sortie choisie au hasard. Avec un réseau

convenablement maillé, le paquet finit toujours par arriver au destinataire, même si le chemin qu'il doit suivre est compliqué. On voit que cette technique conduit à une réalisation très simple au niveau des nœuds, et qu'elle évite la saturation causée par la duplication des paquets. En contrepartie de ces avantages, le délai d'acheminement est en moyenne plus long qu'avec des techniques déterministes classiques, puisque les paquets suivent en général des routes tortueuses au lieu de prendre le chemin le plus direct vers la destination.

3.4. Routage à vecteur de distance

Les algorithmes modernes sont dynamiques, plutôt que statiques comme ceux déjà présentés. Cet algorithme (parmi les plus ancien) est basé sur une métrique prédéfinie (par exemple le temps d'acheminement ou longueur des files d'attente) parfois appelé routage *Bellman-Ford* ou routage *Ford-Fulkerson*, utilisé par les protocoles *DECnet-IPX*, RIP (***Route Information Protocol***), BGP (***Border Gateway Protocol***), EGP (***Exterior Gateway Protocol***). IGRP et EIGRP.

Prenant l'exemple de réseau présenté dans la figure 03. Chaque routeur possède un vecteur qui contenant une référence à chacun des autres routeurs du sous réseau, le temps estimé (TE) pour l'atteindre et la ligne de sortie préférentielle. Périodiquement, chaque retour examine la distance qui le sépare de ses voisins et échange ces informations avec ceux-ci, en même temps il reçoit celles en provenance de ses voisins et il peut ainsi mettre à jour sa table sur la lumière de ces données. Par exemple, le routeur J reçoit les tableaux de routeurs A, I, H et K (présentés dans le tableau 02) dans des délais de (JA=8), (JI=10), (JH=12) et (JK=6). Le routeur J utilise ces information pour obtenir sa nouvelle table de routage de routeur J est représenté dans le tableau 03.

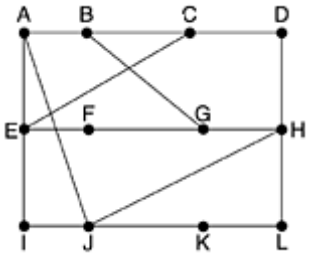

Figure 03 : La topologie d'un réseau

Tableau 02 : Les vecteurs A, I, H et K reçu par le routeur J.

Vecteur ***A***		Vecteur ***I***		Vecteur ***H***		Vecteur ***K***	
À	TE	À	TE	À	TE	À	TE
A	0	A	24	A	20	A	21
B	12	B	36	B	31	B	28
C	25	C	18	C	19	C	36
D	40	D	27	D	8	D	24
E	14	E	7	E	30	E	22
F	23	F	20	F	19	F	40
J	18	J	31	J	6	J	31
H	17	H	20	H	0	H	19
I	21	I	0	I	14	I	22
J	9	J	11	J	7	J	10
K	24	K	22	K	22	K	0
L	29	L	33	L	9	L	9

Tableau 03 : La nouvelle table de routage de routeur ***J.***

Destination	Temps Estimé	La ligne de sortie
A	8	A
B	20	A
C	28	I
D	20	H
E	17	I
F	30	I
J	18	H
H	12	H
I	10	I
J	0	/
K	6	K
L	15	K

3.5. Routage par informations à état de lien

L'échange de tables de routage dans des réseaux avec des tailles importantes va diminuer les performances de ces réseaux. En conséquence, un autre algorithme a remplacé l'algorithme de vecteur de distance. Cet algorithme est basé sur les poids des liens et une idée simple où chaque routeur doit :

- Découvrir ses voisins et apprendre leurs adresses réseau : à son démarrage, chaque retour doit découvrir ses voisins. En effet, le retour envoie a tous ses voisins un paquet ***HELLO.*** Les retours qui reçoivent ce paquet doivent répondre en se présentant.
- Mesurer le temps d'acheminement vers chacun des voisins : l'idée de cet algorithme est basée sur la capacité de chaque retour de savoir le temps d'acheminement vers ses voisins. Afin d'élaborer une estimation de cet temps, un retour doit envoyer des paquets ***ECHO*** à ses voisins. Le retour qui reçoit ce paquet, il doit répondre immédiatement. Ainsi, le temps d'acheminement est ce temps divisé par deux.
- Envoyer un paquet contenant ces informations à ses voisins : après la collecte des informations de voisins, chaque retour construit des paquets spéciaux et les distribue vers tous les retours. Chaque paquet débute par l'identité de son émetteur, suivie par le numéro de séquence de paquet (pour le distinguer d'autres paquets), l'âge de paquet (pour éviter les boucles infinies d'un paquet) et la liste de ses voisins accompagnés aux délais pour l'atteindre.
- Calculer le plus court chemin vers tous les routeurs : en recevant les paquets de différents retours, chaque retour peut prendre une idée de topologie d'un réseau et de trouver le plus court chemin en appliquant l'algorithme de *Dijkstra*.

3.6. Routage hiérarchique

Les sous réseaux grandissent vite, les tables de routage font ainsi. L'espace de stockage des tables, la puissance de traitement et la bande passante pour échanger les états doit augmenter proportionnellement. A un certain point, cela ne peut être faisable.

Le routage hiérarchique permet d'améliorer la situation en divisant le sous réseau en régions. Le routeur d'une région possède toutes les informations nécessaires sur sa région mais n'a aucune connaissance sur les autres régions.

4. Les algorithmes de contrôle de congestion

Le contrôle de flux et un mécanisme point à point qui concerne l'émetteur et le destinataire de paquets, tandis que celui de la congestion concerne le sous réseau entier. Le phénomène de congestion est provoqué par l'arrivée brusque de flux de paquets des lignes d'entrée qui doivent être routés sur la même ligne de sortie, la file d'attente pour accueillir ces paquets peut atteindre rapidement sa capacité maximale et les paquets suivants seront perdus. Le temps de traversée du nœud augmente et le time out provoque la retransmission des paquets perdus et en attente ce qui aggrave la situation avec le temps. Un nœud congestionné affecte ses voisins et si aucun mécanisme de lutte contre ce phénomène n'est prévu, tout le sous réseau sera congestionné après une certaine durée.

Les algorithmes de contrôle de congestion se divisent en deux grandes familles, celle de la ***boucle ouverte*** ayant comme but de prévenir ce phénomène en agissant toujours à priori sans tenir en compte l'état actuel du sous réseau. Ceux de la ***boucle fermée*** préfèrent laisser aller et agir au moment où celle-ci se produit.

Afin d'éviter une situation de congestion, plusieurs mécanismes peuvent être appliqués à divers niveaux. :

- A la couche liaison de données, un bon ajustement de temps d'attente avant de retransmission peut influencer directement sur la congestion. En effet, si ce temps est court la source retransmet les paquets avant qu'ils soient reçus par le destinataire en croyant qu'ils sont perdus ou reçu avec des erreurs. Donc, on peut trouver plusieurs copies d'un même paquet sur les liaisons. En plus, la stratégie d'acquittement peut réduire la congestion. L'application de la technique de superposition (envoie d'un acquittement au sein d'une trame d'information) peut réduire significativement le trafic sur le réseau.
- Au niveau de la couche réseau, le choix d'une bonne stratégie de routage qui répartisse le trafic sur toutes les voies influence positivement

sur la congestion. En effet, des mécanismes simples peuvent influencer positivement ou négativement sur la congestion comme le choix de nombre de files d'attente par ligne d'entrée et ligne de sortie. En plus, la stratégie appliquée pour le traitement de paquets peut diminuer ou aggraver la congestion.

- Au niveau de la couche de transport, la mise en cache des paquets déclassés est une bonne stratégie pour diminuer la congestion.

Le contrôle de la congestion est plus simple dans un service avec connexion (le cas d'un circuit virtuel). En effet, dés qu'une situation de congestion est signalée un routeur peut refuser l'établissement d'autres connexions. On appelle cette technique ***le contrôle d'admission***. Par contre, dans un sous réseau de datagrammes les paquets sont envoyés sans l'attente de permission de nœuds intermédiaires. La solution consiste donc à demander à la source de diminuer son débit d'envoie des paquets dès qu'une situation de congestion soit détectée. La détection de la situation de congestion est basée le contrôle de files d'attente d'un routeur. Si ce dernier détecte que la taille de ses files d'attente a dépassée certaine seuil, il signale une situation de congestion. Dans ce cas le routeur doit informer la source par plusieurs techniques. La première technique consiste à signaler cette situation dans un bit spécifique de l'acquittement (mécanisme de ***bit d'alerte***). Une autre technique consiste à envoyer un paquet spécial à la source (appelé ***paquet de rétention)***. Ce paquet peut avoir un effet seulement sur la source (donc ***paquet de rétention avec effet sur la source***) ou un effet sur la source et tous les routeurs intermédiaires (***paquet de rétention avec effet par paliers***).

Si aucune des techniques précédentes ne permet le contrôle de congestion, les routeurs peuvent appliquer une technique brutale qui consiste à supprimer les paquets qu'ils ne sont plus en mesure de traiter. Cette technique est appelée le ***délestage de charge***. Bien entendu, le choix des paquets à supprimer influence sur les performances de cette technique. Ce choix des paquets à supprimer est fortement dépend de l'application.

5. L'adressage au niveau réseau

La couche MAC offre un type d'adressage dite absolue. Il n'y a donc pas de relation entre des adresses situées sur des sites proches l'un de l'autre. Dans ce type d'adresse la situation géographique de l'abonné est impossible à connaître. En conséquence, le routage est délicat à mettre en œuvre. Si ce type d'adressage est convient aux réseaux locaux où la technique de transmission consiste en diffusion, il semble limite dans les grands réseaux WAN. En effet, il est important d'utiliser des adresses hiérarchiques logiques. Le contenu de ce type d'adresse est significatif parce qu'il permet d'identifier la machine et le réseau dans laquelle la machine est connectée. Un bon exemple de ce type d'adressage est l'adresse IP.

Chaque machine susceptible d'être connectée à l'extérieur de son réseau local possède une adresse IP en principe unique. L'unicité des adresses IP est garantie par l'ICANN (Internet Corporation for Assigned Names and Numbers) qui est chargé au niveau mondial de la gestion de l'espace d'adressage IP. Il définit les procédures d'attribution et de résolution de conflits dans l'attribution des adresses, mais délègue le détail de la gestion de ces ressources `a des instances régionales puis locales, dans chaque pays, appelées « Regional Internet Registries » ou RIR.

Les adresses IP sont codées sur 32 bits comportent deux parties : le numéro de réseau (Net_id) et le numéro de la machine sur le réseau (Host_id). Ces adresses sur 32 bits sont exprimées par octet (soit quatre nombres compris entre 0 et 255) notées en décimal_et séparés par des points (***x.y.z.w***). Suivant l'importance du réseau, plusieurs classes d'adressage sont possibles. Les différentes classes d'adresse correspondent donc à des nombres appartenant aux plages suivantes :

- **Classe A :** représente donc les réseaux de grande envergure. La plage des adresses de 1.0.0.0 à 126.0.0.0, soit 126 réseaux (2^{8-1}-2) et 16 777 214 machines (2^{24}-2) par réseau.
- **Classe B :** désigne les réseaux moyens. Elle englobe les adresses de 128.0.0.0 à 191.255.0.0, soit 16 382 réseaux (2^{16-2}-2) et 65 534 machines (2^{16}-2) par réseau.
- **Classe C :** représente les petits réseaux régionaux. Elle est constitué des adresses de 192.0.0.0 à 223.255.255.0, soit 2 097 150 réseaux (2^{24-3}-2) et 254 machines (2^{8}-2) par réseau.

- **Classe D :** ne désigne pas une machine particulière sur le réseau mais un groupe. Elle est donc utilisée pour diffusion. Ces adresses entre 224.0.0.0 et 239.255.255.255, soit 268 435 454 adresses de groupes (2^{32-4}-2).
- **Classe E :** sont réservées pour une utilisation future. de 240.0.0.0 à 255.255.255.254.

La figure 03 montre ces classes d'adresses IP.

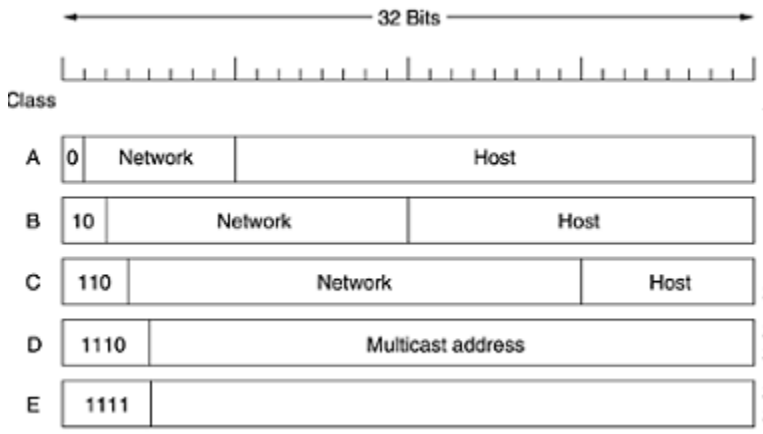

Figure 03 : Les classes d'adresses IP

5.1. Adresses particulières

L'adressage IP offre plusieurs adresses particulières ou réservées.

- L'adresse 0.0.0.0 représente une adresse non reconnue. Elle est utilisée par les machines ne connaissant pas leur adresse IP au démarrage ;
- L'adresse 255.255.255.255 représente une adresse de diffusion générale (broadcasting) sur toutes les stations de réseau de l'émetteur. On note qu'un paquet avec une telle adresse ne transmet ne traverse jamais un routeur (non routable).
- Lorsque l'on annule la partie Host_id, c'est-à-dire lorsque l'on remplace les bits réservés aux machines du réseau par des zéros (par exemple *194.28.12.0*), on obtient ce que l'on appelle l'***adresse réseau***. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.
- Lorsque la partie Net_id est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'adresse machine. Cette

adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.

- Lorsque tous les bits de la partie host-id sont à 1, l'adresse obtenue est appelée l'**adresse de diffusion**.Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le Net_id.
- L'adresse réseau 127.0.0.0 : est une adresse de bouclage ***(localhost, loopback)*** et permet l'utilisation interne de TCP/IP sans aucune interface matérielle ; les paquets portant une telle adresse de destination n'atteignent plus la couche physique.
- Certains réseaux sont reliés à l'Internet via une seule machine. En conséquence, seulement cette machine a besoin d'une adresse IP ***publique*** (attribué par ICANN). Cependant, les autres machines ont besoin des adresses IP pour pouvoir communiquer ensemble en interne. Ainsi, l'ICANN a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux. Il s'agit des adresses suivantes :
  - Classe A : 10.0.0.0 à 10.255.255.255, donc 10.x.y.z
  - Classe B : 172.16.0.0 à 172.31.255.255
  - Classe C : 192.168.0.0 à 192.168.255.255. Donc 192.168.x.y

5.2. Sous-réseau

L'objectif initial de l'adressage IP était l'identification exacte du réseau physique. Imaginons maintenant un grand campus qui dispose de plusieurs réseaux internes et qui veut se connecter à Internet. Chacun des réseaux internes peut nécessiter une adresse de classe C par exemple. Pire encore, si un réseau interne comporte (ou comportera dans le futur) un peu plus de 255 machines, ça va demander une adresse de classe B.

Devant cette situation de gaspillage d'adresses réseaux IP (qui sont limitées). Le découpage en sous réseaux fournit un moyen simple et élégant de réduire le nombre total d'adresses réseau assignées. En 1984 un troisième niveau de hiérarchie est mis en place : le « subnet » ou sous-réseau. L'idée est de prendre un seul numéro de réseau IP et de l'attribuer à plusieurs réseaux physiques d'un

campus qui seront référencés comme étant des sous réseaux. Ces sous réseaux doivent être proche de façon à ce qu'un routeur choisit une seule route pour atteindre l'un de ceux-ci.

Chaque machine d'un sous réseau doit donc posséder un masque de sous réseau. Ainsi, toutes les machines du campus auront le même numéro de réseau. La partie Numéro de machine (Host ID ou Host portion) sera subdivisée en deux parties. La première partie va constituer un numéro de sous-réseau et l'autre un numéro de la machine proprement dit. Les machines d'un réseau physique interne au campus partagent le même numéro de sous réseau (en plus du numéro de réseau).

Un masque réseau se présente sous la forme de 4 octets séparés par des points (comme une adresse IP), il comprend (dans sa notation binaire) des zéros au niveau des bits de l'adresse IP que l'on veut annuler (et des 1 au niveau de ceux que l'on désire conserver). La partie de l'adresse Internet administrée localement *(*Host_id*)* peut être découpée en deux parties : une adresse de sous-réseau et un numéro de machine.

Comme le cas d'un masque réseau, le masque sous réseau permet l'identification d'un sous réseau. Ainsi, les bits à 1 désignent la partie sous réseau de l'adresse et les bits à 0 la partie numérotation des machines sur le sous-réseau. **Il n'y a aucune raison pour que les bits à 1 soient contigus, mais le non respect de cette règle entraînerait des difficultés de gestion inutiles**.

Finalement on note qu'une autre version de protocole IP (appelée IPv6) a remplaçé lancienne version IPv4 dont l'une de ces innovation est l'utilisation des adresse IP sur 128 bits

6. Qualité de service (QoS)

Les besoins de chaque flux de paquets peuvent être caractérisés par 04 paramètres intéressants : Fiabilité, Délai, Gigue et Bande passante. Ces paramètres définissent ce qu'on appelle Qualité de Service requise : QoS (Quality of Service). La qualité de service est fortement dépendante de l'application. Par exemple, le transfert de fichier

exige une fiabilité extrême mais n'est pas exigeant concernant gigue. Par contre, les applications multimédias sont très exigeantes concernant gigue.

7. L'interconnexion des réseaux

Dans la pratique, on a besoin d'interconnecter différents types de réseaux qui diffèrent non seulement par leurs couches réseau mais aussi celle physique et liaison. Le système complet s'appelle internetwork ou internet (avec i minuscule).

L'interconnexion de réseau se fait grâce aux équipements spécifiques qui agissent à différents niveaux. Les répéteurs et les Hubs permettent de ce faire pour la couche physique. Les commutateurs (Switchs) et les ponts opèrent au niveau de la couche liaison. Pour la couche réseau, ce sont les routeurs qui prennent le relai. Si les réseaux utilisent des protocoles différents, on parle de routeurs multi-protocoles. Au niveau de la couche transport, on utilise les passerelles (gateway).