UNIVERSITEDEBATNA 2

DEPARTMENTD'INFORMATIQUE

Master

Réseaux et systèmes distribués

Semestre : S2

Support de Cours

Routage et Interconnexion

Dr. Hamouma Moumen

hamouma.moumen@univ-batna2.dz

2022

Table des matières

Chapitre I : Concepts généraux

1. Introduction :

Le routage est devenu un mécanisme indispensable pour interconnecter un réseau au reste de l'Internet, pour construire un grand réseau ou gérer des flux à l'intérieur du réseau. Grace à la fonction de routage qui utilise les routeurs comme équipements d'interconnexion, nous pouvons concevoir des réseaux sans limitation de taille et de nombre d'équipements.

Ce chapitre présente les différents concepts de base liés au routage. Après quelques définitions de base, le lecteur trouvera les règles d'attribution d'adresses mises en œuvre dans les réseaux Internet, ainsi que leurs évolutions au cours du temps, notamment la technique d'allocation hiérarchique CIDR et l'adressage privé.

2. Définitions :

- **Le terme routage :** est souvent confondu avec le terme de relayage (forwarding) qui fait référence à la fonction principale d'un routeur. Cette fonction consiste à recopier le plus vite possible un paquet sur l'interface de sortie. Initialement les équipements d'interconnexion mémorisaient entièrement l'information avant de la retransmettre (stockage et retransmission), mais pour optimiser les performances, certains équipements prennent la décision dès que l'en-tête est reçue. Cette technologie est appelée **commutation** (switching) ;

- **La fonction de routage** construit les bases de données (appelées tables de routage) indiquant l'interface de sortie pour une destination. Cette information servira pour le relayage.

3. Fonctionnement d'un routeur :

Un routeur exécute en parallèle trois tâches différentes :

• la commutation de paquets

• le routage

• la gestion

La commutation de paquets représente la finalité du routeur. Ces paquets sont reçus sur un port d'entrée I, forwardés vers un port de sortie J et enfin émis sur ce port J. Le forwarding nécessite la consultation d'une table de routage qui indique le port de sortie correspondant à l'adresse de destination du paquet.

4. Adressage :

4.1 Adresses physiques (MAC) :

Au niveau de la couche liaison, les nœuds utilisent une adresse dite « physique » pour communiquer. L'adresse correspond à l'adresse de la carte réseau. On parle **d'adresse physique, d'adresse MAC** (Medium Access Control) ou d'adresse de couche 2 (référence au modèle OSI).

Cette adresse est identique pour les réseaux Ethernet, Token Ring et FDDI. **Sa longueur est de 48 bits soi**t six octets (par exemple : 08-00-14-57-69-69) définie par le constructeur de la carte. Une adresse universelle sur 3 octets est attribuée par l'IEEE à chaque constructeur de matériel réseau. Sur les réseaux CCITT X.25, c'est la norme X.121 qui est utilisée pour les adresses physiques, qui consistent en un nombre de 14 chiffres.

L'adresse MAC identifie de manière unique un nœud dans le monde. Elle est physiquement liée au matériel (écrite sur la PROM), c'est à dire à la carte réseau.

4.2 Adresses Internet (IP) :

Pour le but de fournir un service de communication universel permettant à toute machine de communiquer avec toute autre machine de l'interconnexion, une machine doit être accessible

aussi bien par des humains que par d'autres machines **.** Pour cela, elle doit pouvoir être identifiée par :

- un nom (mnémotechnique pour les utilisateurs),
- une adresse qui doit être un identificateur universel de la machine,
- une route précisant comment la machine peut être atteinte.

Comme solution l'adressage IP est Utilisé.

4.2.1 Classes d'adresses IP : Une adresse = 32 bits dite "Internet address" ou "IP address" constituée d'une paire (NET-ID, HOST-ID) où NET-ID identifie un réseau et HOST-ID identifie une machine sur ce réseau. Cette paire est structurée de manière à définir cinq classes d'adresse.

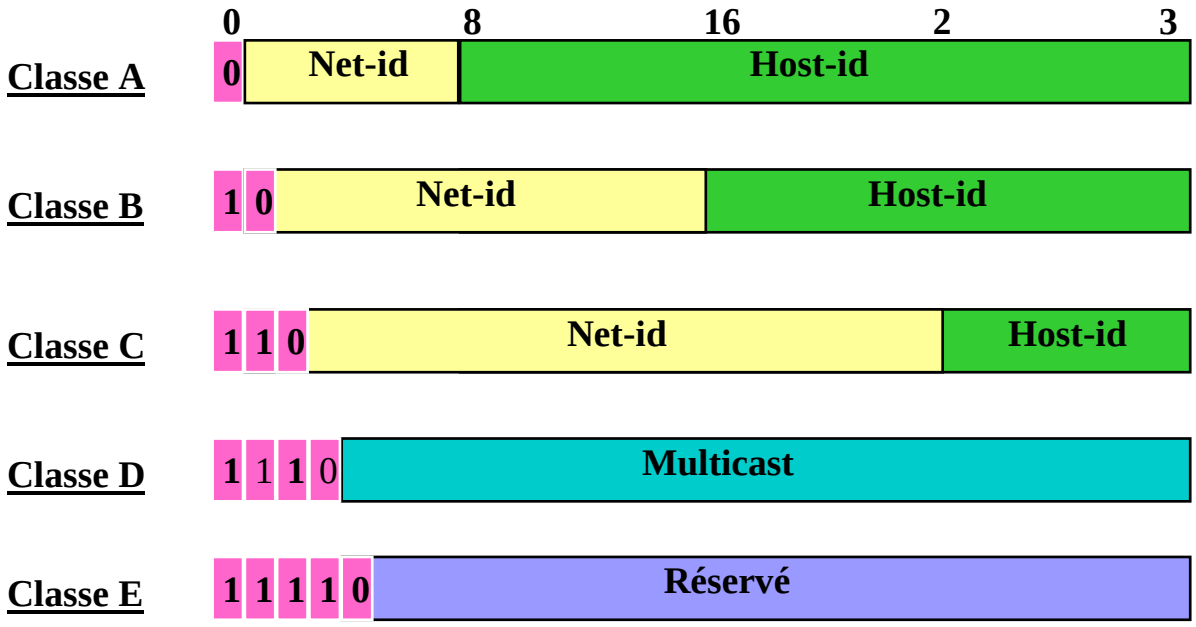


Figure 1. Classes d'adresses

Notation décimale : l'interface utilisateur concernant les adresses IP consiste en la notation de quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP : 10000000 00001010 00000010 00011110 est écrit : 128.10.2.30

4.2.2 Adresses particulières :

- ***Adresses réseau*** **:** adresse IP dont la partie hostid ne comprend que des zéros; => la valeur zéro ne peut être attribuée à une machine réelle : 192.20.0.0 désigne le réseau de classe B 192.20;
- ***Adresse machine locale*** : adresse IP dont le champ réseau (netid) ne contient que des zéros;
- ***Adresses de diffusion*** **:** la partie hostid ne contient que des 1;
- ***Adresse de diffusion limitée*** : netid ne contient que des 1 : l'adresse constituée concerne uniquement le réseau physique associé;
- ***L'adresse de diffusion dirigée*** **:** netid est une adresse réseau spécifique => la diffusion concerne toutes les machines situées sur le réseau spécifié : 192.20.255.255 désigne toutes les machines du réseau 192.20.
- ***Adresse de boucle locale*** : l'adresse réseau 127.0.0.0 est réservée pour la désignation de la machine locale, c'est à dire la communication intra-machine. Une adresse réseau 127 ne doit, en conséquence, jamais être véhiculée sur un réseau et un routeur ne doit jamais router un datagramme pour le réseau 127**.**

4.2.3 Adresses et connexions

Une adresse IP => une interface physique => une connexion réseau. S'applique particulièrement aux routeurs qui possèdent par définition plusieurs connexions à des réseaux différents. A une machine, est associé un certain nombre N d'adresses IP. Si N > 0 la machine (ou passerelle) est multi-domiciliée

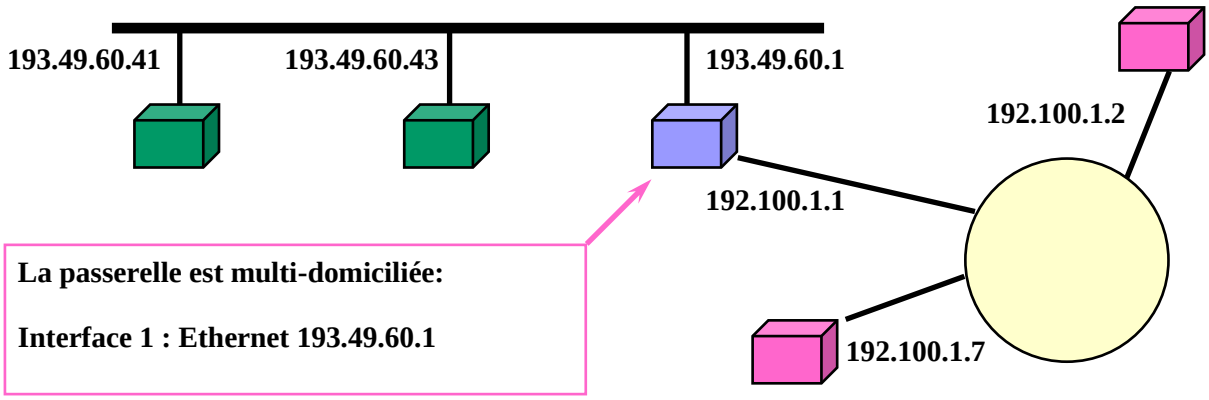


Figure 2. Adresses et connexions

4.3 Réseaux et sous-réseaux :

Un réseau peut être divisé en sous-réseaux afin de pouvoir :

- éviter le gaspillage des adresses nœuds d'un réseau

- utiliser des supports physiques différents.

- réduire le trafic sur le réseau.

- isoler une partie du réseau en cas de défaillance d'un composant du réseau.

- augmenter la sécurité.

Chaque sous-réseau est relié à un autre par un routeur.

Exemple :

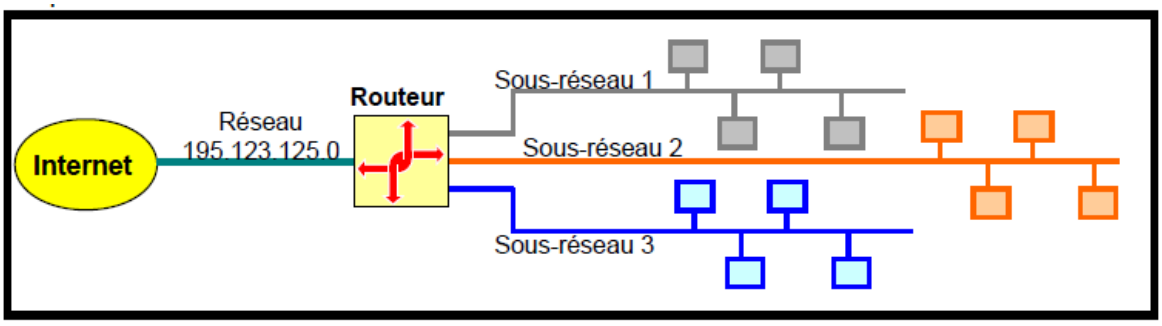


Figure 3: Sous-réseaux.

Dans la figure ci-dessus, le routeur est connecté à Internet par un réseau de classe C 195.123.125.0. Il est donc possible d'utiliser 256 (- 2) adresses pour les nœuds. Cependant si tous les nœuds sont sur le même réseau, celui-ci risque d'être chargé. On répartit les nœuds sur 3 réseaux que l'on connecte à un routeur. Chacun de ces réseaux devant avoir une adresse distincte, on crée des adresses de sous-réseaux pour chacun d'eux

5. Masques de sous-réseaux :

La notion de sous-réseaux était inexistante au début de IP. L'adressage de sous-réseaux va se faire avec des bits normalement réservés à l'adressage des nœuds.

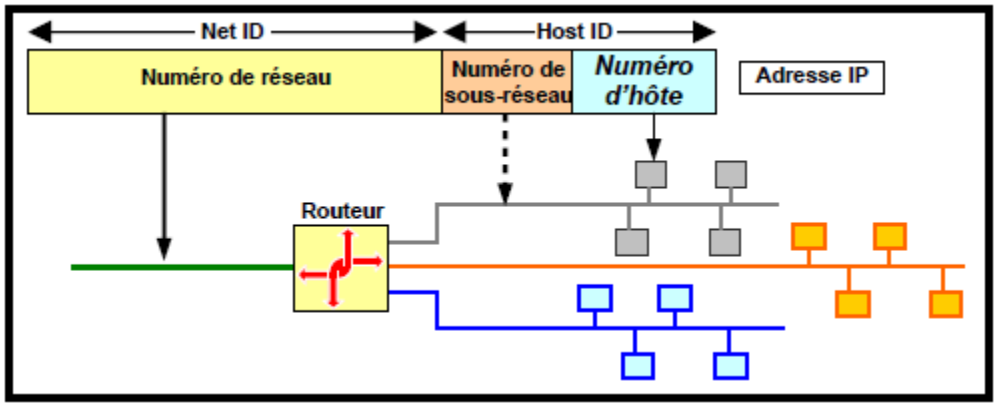


Figure 4 : Numérotation des sous-réseaux.

Pour indiquer le nombre de bits pris sur la partie HostID comme numéro de sous-réseau, on va utiliser un masque de sous-réseaux. Ce masque indique par des bits à 1 le nombre de bits de l'adresse IP qui correspondent à l'adresse réseau et à l'adresse sous-réseaux. Les bits à 0 du masque indiquent les bits de l'adresse IP qui correspondent à l'HostID

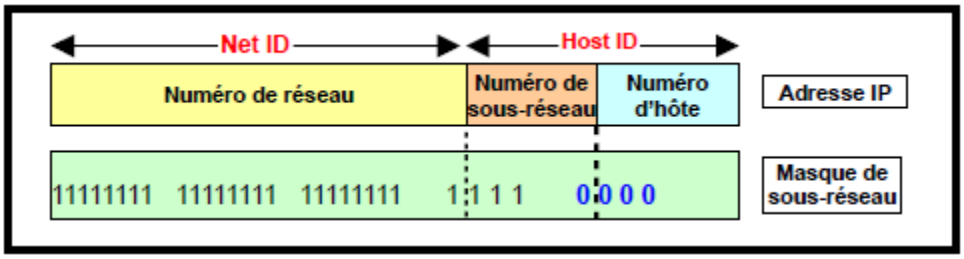


Figure 5: Masque de sous-réseau.

Dans l'exemple ci-dessus, l'adresse IP est une adresse de classe C. On désire créer 16 sous-réseaux. Il est donc nécessaire d'utiliser 4 bits de la partie HostID pour indiquer le numéro de sous-réseau. Le masque comporte 28 bits à 1 , c'est à dire :

- 24 bits correspondant à la partie NetID de l'adresse et 4 bits pour indiquer les bits de l'adresse IP qui doivent être interprétés comme étant l'adresse de sous-réseaux.
- 4bits à 0, indiquent les bits de l'adresse IP qui doivent être interprétés comme des adresses de nœuds.

Remarque : la RFC 1860 (remplacée par la RFC 1878) stipulait qu'un numéro de sous réseau ne peut être composé de bits tous positionnés à zéro ou tous positionnés à un.

Autrement dit, dans notre exemple, on ne pouvait pas utiliser le sous-réseau 0 et le sous-réseau 240. Le premier nous donnant une adresse de sous-réseau équivalente à l'adresse du réseau. Le deuxième nous donnant une adresse de sous-réseau dont l'adresse de diffusion se confondrait avec l'adresse de diffusion du réseau. Le nombre de sous-réseaux aurait alors été de seulement *: 2^4-2 =14.*

Il est donc important de savoir quelle RFC est utilisée par votre matériel pour savoir si les adresses de sous-réseau composées de bits tous positionnés à zéro ou tous positionnés à un sont prises en compte ou non.

6. Notation CIDR:

Le schéma d'adressage sans classes est appelée **CIDR (Classless Inter-Domain Routing)** permet de réduire les huit entrées utilisées dans l'exemple précédent à une seule entrée correspondant à tous les identificateurs de réseau de classe C utilisés par cette entreprise. Le nom est infortuné puisque CIDR spécifie uniquement l'adressage et le relayage. Quand le schéma d'adressage CIDR a été créé, les concepteurs voulaient faciliter à un utilisateur de spécifier un masque. Pour comprendre la difficulté, considérons l'exemple figure 6, où le masque est 255.255.255.192.

Pour faciliter aux être humains de spécifier et d'interpréter les valeurs d'un masque, la notation décimale séparée par des points est étendue. Dans cette version étendue, Connue par CIDR, une adresse et un masque peut être spécifié par une adresse IP en décimal suivi par un slash et un nombre en décimal qui désigne le nombre bits contigus les plus à gauche utilisés par la masque. La forme générale d'une notation CIDR est **ddd.ddd.ddd.ddd /m**.

La figure 7 présente une liste de masques d'adresse IP en notation CIDR et leurs équivalences en notation décimal.

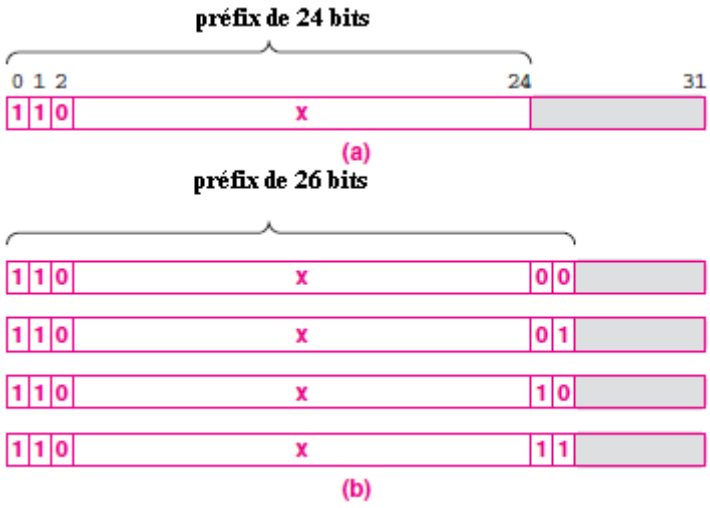


Figure 7 : (a) un préfix de classe C (b) le même préfix devisé en 4 Classeless préfixes

CIDR	Address Mask
/0	0 . 0 . 0 . 0
/1	128 . 0 . 0 . 0
/2	192 . 0 . 0 . 0
/3	224 . 0 . 0 . 0
/4	240 . 0 . 0 . 0
/5	248 . 0 . 0 . 0
/6	252 . 0 . 0 . 0
/7	254 . 0 . 0 . 0
/8	255 . 0 . 0 . 0
/9	255 . 128 . 0 . 0
/10	255 . 192 . 0 . 0
/11	255 . 224 . 0 . 0
/12	255 . 240 . 0 . 0
/13	255 . 248 . 0 . 0
/14	255 . 252 . 0 . 0
/15	255 . 254 . 0 . 0
/16	255 . 255 . 0 . 0
/17	255 . 255 . 128 . 0
/18	255 . 255 . 192 . 0
/19	255 . 255 . 224 . 0
/20	255 . 255 . 240 . 0
/21	255 . 255 . 248 . 0
/22	255 . 255 . 252 . 0
/23	255 . 255 . 254 . 0
/24	255 . 255 . 255 . 0
/25	255 . 255 . 255 . 128
/26	255 . 255 . 255 . 192
/27	255 . 255 . 255 . 224
/28	255 . 255 . 255 . 240
/29	255 . 255 . 255 . 248
/30	255 . 255 . 255 . 252
/31	255 . 255 . 255 . 254
/32	255 . 255 . 255 . 255

Figure 8 : une liste de masques d'adresse IP en notation CIDR et leurs équivalences en notation décimal

7. Le routage statique et le routage dynamique :

Le routage statique permet l'élimination du processus de routage ce qui libère certaines ressources mémoire et CPU. Cependant, toute modification de la topologie du réseau (ajout, suppression ou panne d'équipements du réseau) doit être immédiatement prise en compte par l'ingénieur réseau; celui-ci doit alors modifier la table de routage en conséquence sous peine de dysfonctionnements plus ou moins graves (trous noirs).

Le routage dynamique détecte toute modification de la topologie du réseau et la répercute en recalculant la table de routage. La détection de la modification de la topologie de réseau et le recalcule de la table de routage qui en découle sont d'autant plus rapides que le protocole de routage est efficace.

7.1 Le Routage statique :

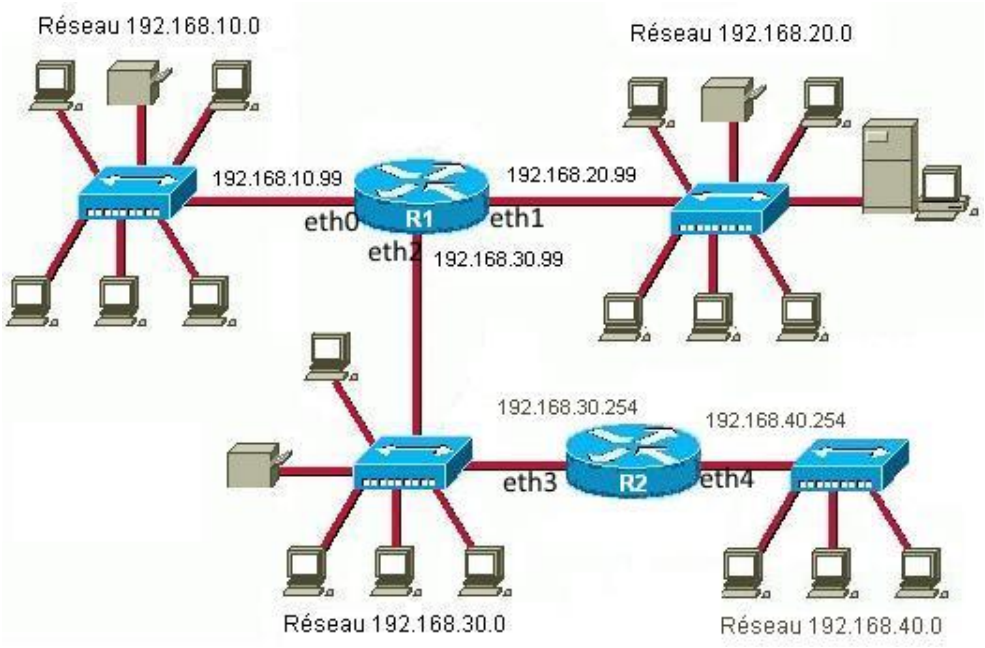
Le Routage statique est le routage le plus simple à mettre en œuvre. D'autant plus encore, il offre des avantages en termes de sécurité et ne consomme que peu de bande passante par rapport aux protocoles de Routages Dynamique.

Malgré ces avantages nets, il présente quand même un inconvénient à souligner: sa maintenance devient plus lourde que les protocoles de routages dynamiques une fois que le nombre de nœuds (Routeurs) augmentent dans le réseau (Au delà de 4 Routeurs).Néanmoins pour un Réseau informatique de 3 Routeurs, le routage statique s'avère avantageux à mettre en œuvre.

Dans une configuration de **routage statique**, une table de correspondance entre adresses de destination et adresses de routeurs intermédiaires est complétée « à la main » par l'administrateur, on parle de **table de routage**.

La table de routage d'un routeur comporte les adresses des réseaux de destination, le masque, les adresses des passerelles (routeurs intermédiaires) permettant de les atteindre, l'adresse de la carte réseau (interface) par laquelle le paquet doit sortir du routeur.

Considérons le schéma de réseau suivant :



La table de routage du routeur R1 sera :

Destination	*Masque de Sous réseau*	*Passerelle*	*Interface*
192.168.10.0	255.255.255.0	Remise Directe	
192.168.20.0	255.255.255.0	Remise Directe	
192.168.30.0	255.255.255.0	Remise Directe	
192.168.40.0	255.255.255.0	192.168.30.254	eth3

La table de routage du routeur R2 sera :

Destination	*Masque de Sous réseau*	*Passerelle*	*Interface*
192.168.10.0	255.255.255.0	192.168.40.254	eth4
192.168.20.0	255.255.255.0	192.168.40.254	eth4
192.168.30.0	255.255.255.0	192.168.40.254	eth4
192.168.40.0	255.255.255.0	Remise Directe	

8. La Fragmentation IP :

L'objectif principal de la couche IP est de trouver un chemin pour envoyer des datagrammes.

Pour atteindre leur destination finale, ces datagrammes vont passer par plusieurs passerelles.

Ces passerelles sont connectées grâces à des supports physique qui peuvent avoir des capacités maximales de transfert différentes, appelées MTU (Maximum Transfert Unit).

Comme, la taille d'un datagramme maximale est de 65536 octets, cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer des paquets de telle taille. Donc, il est nécessaire de fragmenter les datagrammes si ceux-ci ont une taille plus importante que le MTU du réseau.

Type de réseau	MTU (en octets)
Arpanet	1000
Ethernet	1500
FDDI	4470

La fragmentation d'un datagramme se fait au niveau des routeurs, c'est-à-dire lors de la transition d'un réseau dont le MTU est important à un réseau dont le MTU est plus faible. Si le datagramme est trop grand pour passer sur le réseau, le routeur va le fragmenter, c'est-à-dire le découper en fragments de tailles inférieures au MTU du réseau et de telle façon que la taille du fragment soit un multiple de 8 octets.

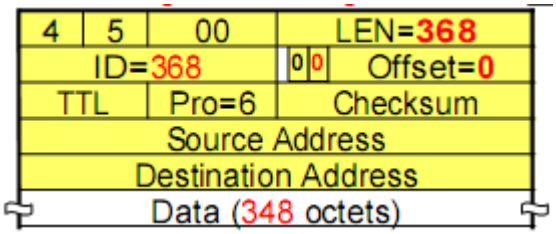
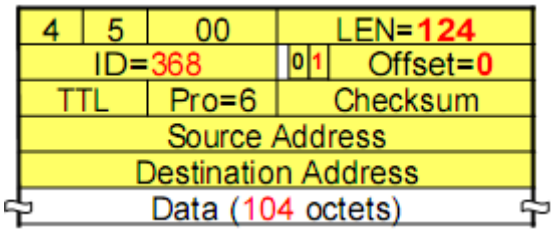
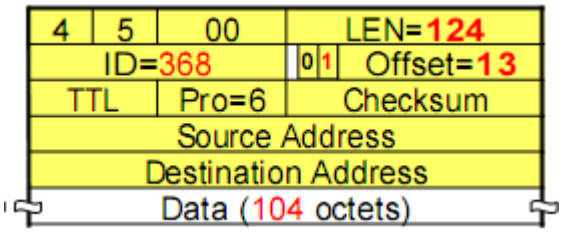
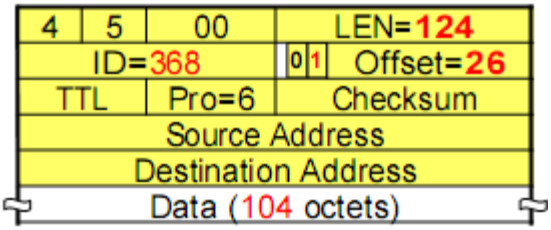
Le routeur va ensuite envoyer ces fragments de manière indépendante et les réencapsuler (ajouter un en-tête à chaque fragment) de telle façon à tenir compte de la nouvelle taille du fragment. De plus, le routeur ajoute des informations afin que la machine de

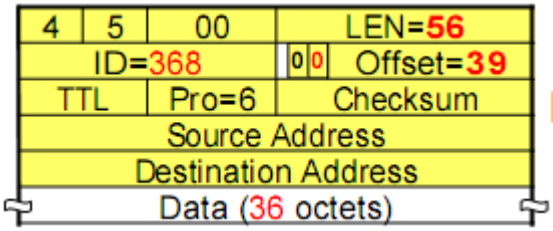
destination puisse réassembler les fragments dans le bon ordre. Pour tenir compte de la fragmentation, chaque datagramme possède plusieurs champs permettant leur réassemblage :

- ***champ déplacement de fragment (13 bits)*** ou **fragment offset** : champ permettant de connaître la position du début du fragment dans le datagramme initial. L'unité de mesure de ce champ est le multiple de 8 octets le plus proche de la MTU sauf pour le dernier fragment. Le premier fragment ayant une valeur de zéro.
- ***champ identification (16 bits)*** : numéro attribué à chaque fragment afin de permettre leur réassemblage.
- ***champ longueur totale (16 bits) :*** il est recalculé pour chaque fragment.
- ***champ drapeau (3 bits) :*** il est composé de trois bits :
    - Le premier n'est pas utilisé.
    - Le second (appelé DF : Don't Fragment) indique si le datagramme peut être fragmenté ou non. Si ce bit est positionné à 1 et que le routeur ne peut pas l'acheminer sans le fragmenter, alors le datagramme est rejeté avec un message d'erreur.
    - Le dernier (appelé MF : More Fragments) indique si le datagramme est un fragment de donnée (1). Si ce bit est positionné à 0, cela indique que le fragment est le dernier (donc que le routeur devrait être en possession de tous les fragments précédents) ou bien que le datagramme n'a pas fait l'objet d'une fragmentation.

Exemple de fragmentation :

Exemple (valeurs en décimal) : MTU de 128 octets. La charge utile est donc de 128 – 20 octets d'en-tête IP) soit 108 octets de données par fragment. L'offset devant être un multiple de 8 octets la taille sera ramenée à 104 octets (13*8=104 octets).

	Contenu des différents champs	Commentaire
Datagramme d'origine		ID=368 DF=0 (paquet fragmentable) MF=0
Fragment 1		ID=368 (appartenance au paquet d'origine) DF=0 MF=1 (il y'a un autre fragment)
Fragment 2		ID=368 (appartenance au paquet d'origine) DF=0 MF=1 (il y'a un autre fragment)
Fragment 3		ID=368 (appartenance au paquet d'origine) DF=0 MF=1(il y'a un autre fragment)

Fragment 4		ID=368 (appartenance au paquet d'origine) DF=0 MF=0 (il n'y a pas d'autre fragment)

Chapitre II
Le protocole RIP

Chapitre II : Le protocole RIP

1- Les protocoles de routage dynamiques

Plusieurs classes de protocoles existent :

a- Distance vecteur : la distance est le nombre de routeurs pour joindre une destination, chaque routeur ne connaît que son voisinage et propage les routes qu'il connaît à ses voisins (ex. RIP).

b- Etats des liens : chaque routeur connaît la topologie et l'état de l'ensemble des liens du réseau, puis en déduit les chemins optimaux. À chaque interaction les routeurs s'envoient toute leur table de routage (ex. OSPF).

Le protocole BGP peut être considéré comme à mi-chemin entre les deux types de protocoles précédents. En effet, l'échange de chemins d'AS permet à chaque routeur de reconstruire une grande partie de la topologie du réseau, ce qui est caractéristique des protocoles de type «état des liens», mais deux routeurs voisins n'échangent que les routes qu'ils connaissent, ce qui est caractéristique d'un protocole de type «distance-vecteur».

2- Le Protocole RIP (Routing Information Protocol) :

RIP est un protocole qui se base sur l'algorithme de **[Bellman & Ford].** Il a été implémenté pour la première fois sur le réseau XNS de Xérox.

2.1- Principe du protocole :

Chaque routeur maintient localement une liste (BdD) des meilleures routes

=> table de routage <@ de destination, distance, @ du prochain routeur>

Chaque routeur actif diffuse un **extrait** de sa table de routage (message de routage) :

- Périodiquement (30s)
- A tous leurs voisins immédiats

- Une liste de couple <@ de destination, distance>

Tous les routeurs mettent à jour leurs tables de routage en conséquence. L'adresse du prochain routeur est implicitement celui de l'émetteur du message de routage.

Etat des stations :

- Actif (les routeurs) diffusent leurs routes,
- Passif (les stations d'extrémité) écoutent.

2.2 Algorithmes de mise à jour :

Chaque couple de la liste est comparé aux entrées de la table de routage :

1. l'entrée n'existe pas dans la table et la métrique reçue n'est pas infinie :
    - une nouvelle entrée est crée : prochain routeur = routeur d'où provient la liste; distance = distance reçue + 1.
2. l'entrée existe et sa métrique est supérieure à celle reçue :
    - on met à jour l'entrée : prochain routeur = routeur d'où provient la liste; distance = distance reçue + 1.
3. l'entrée existe et son prochain routeur est celui d'où provient la liste :
    - distance = distance reçue + 1 (augmentation ou diminution de la distance).
4. sinon rien.

Etat initial :

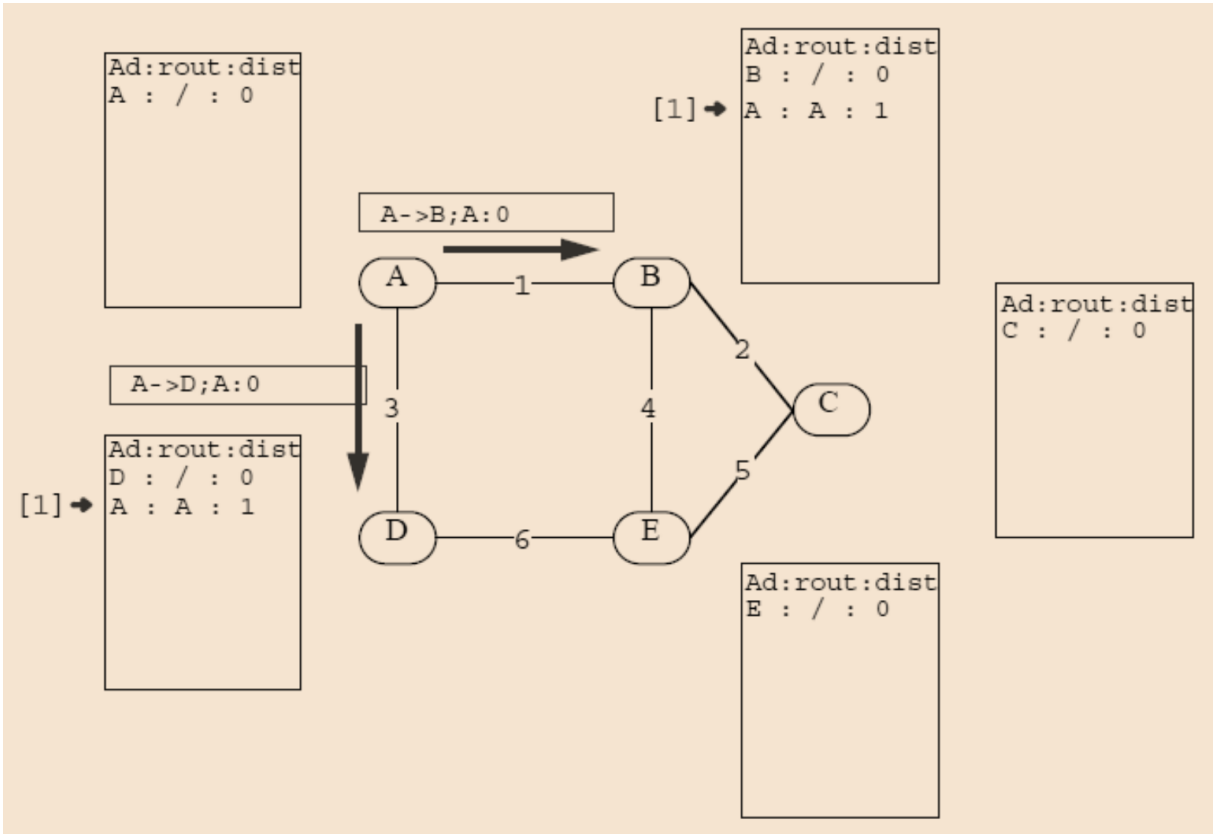
Chaque routeur connaît son environnement immédiat :

- son adresse, ses interfaces,
- ses (sous-)réseaux directs : distance = 0.

2.3 Illustration des différentes phases de l'algorithme :

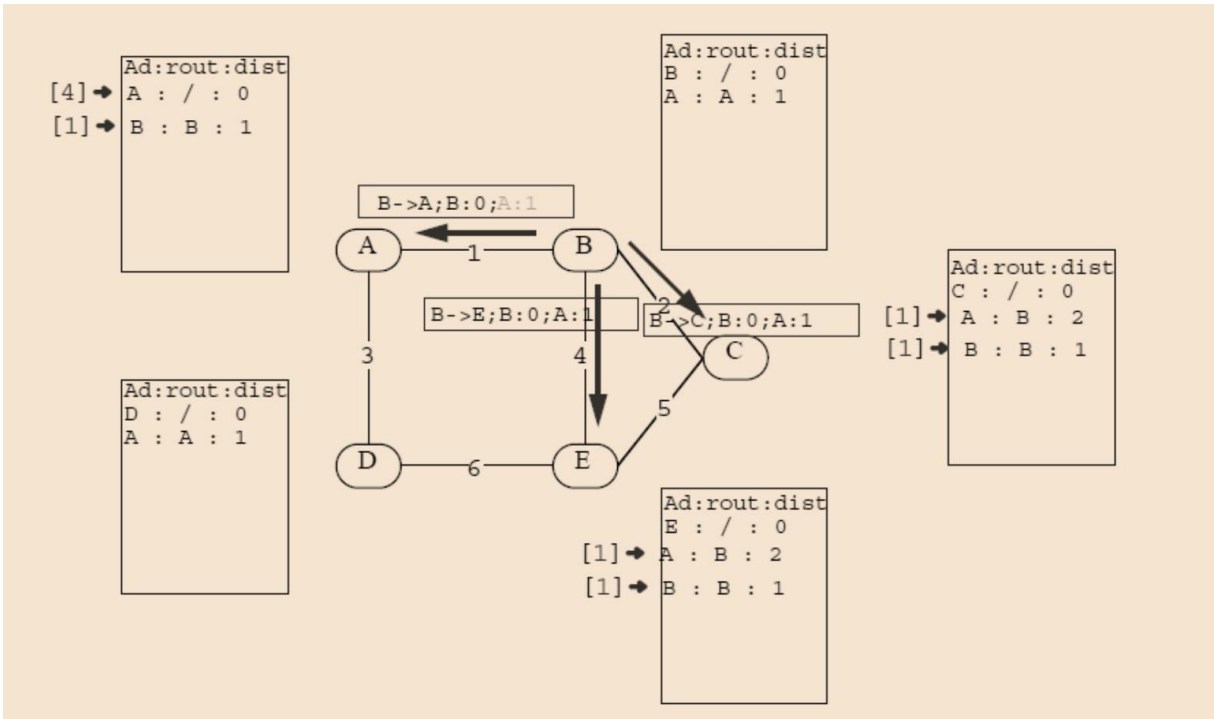
a) La première phase :

Lors de son démarrage, une station diffuse un premier message de routage



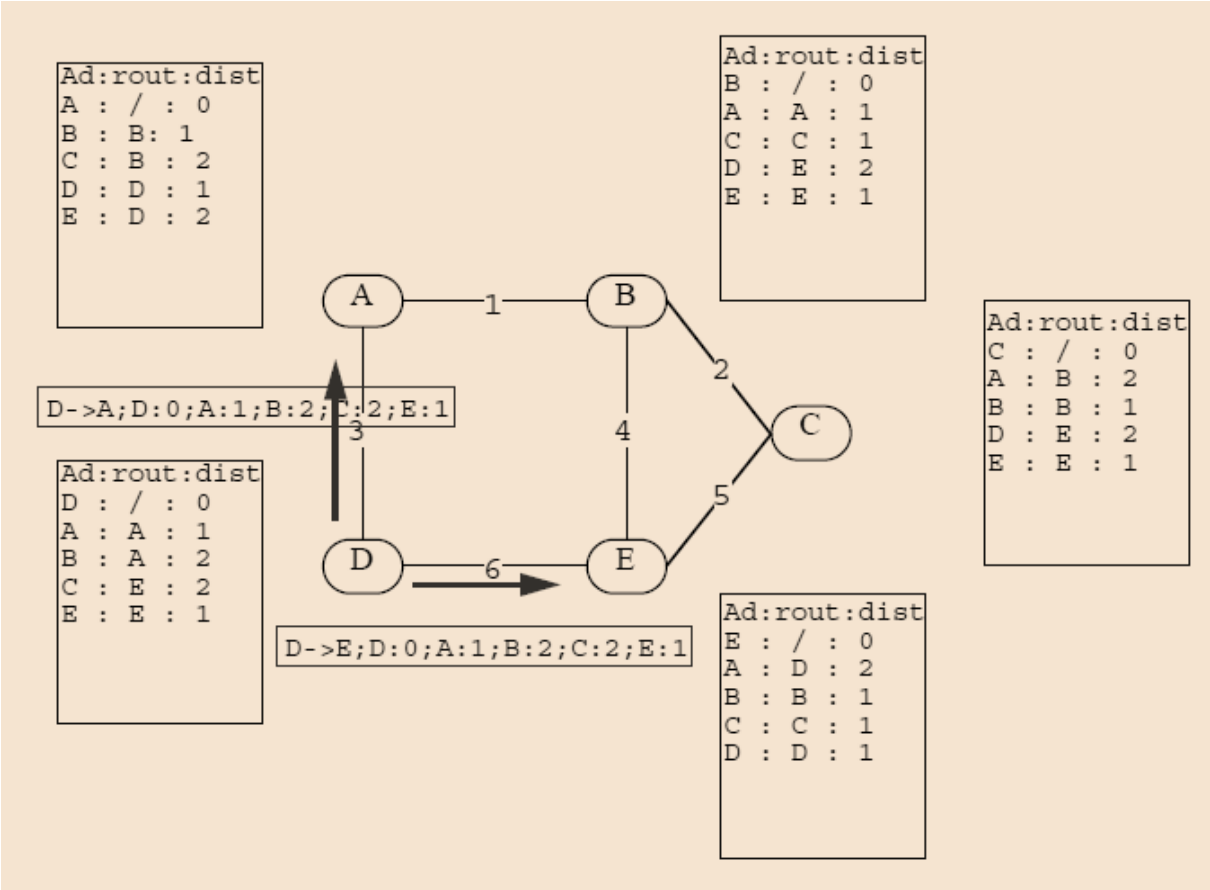
b) Les phases suivantes :

Toute modification de la table locale entraîne, la diffusion d'un nouveau message de routage



c) L'état stable de surveillance

La diffusion des messages de routage est effectuée périodiquement (30s) (surveillance, perte)



3. Contraintes et avalanches :

Contraintes :

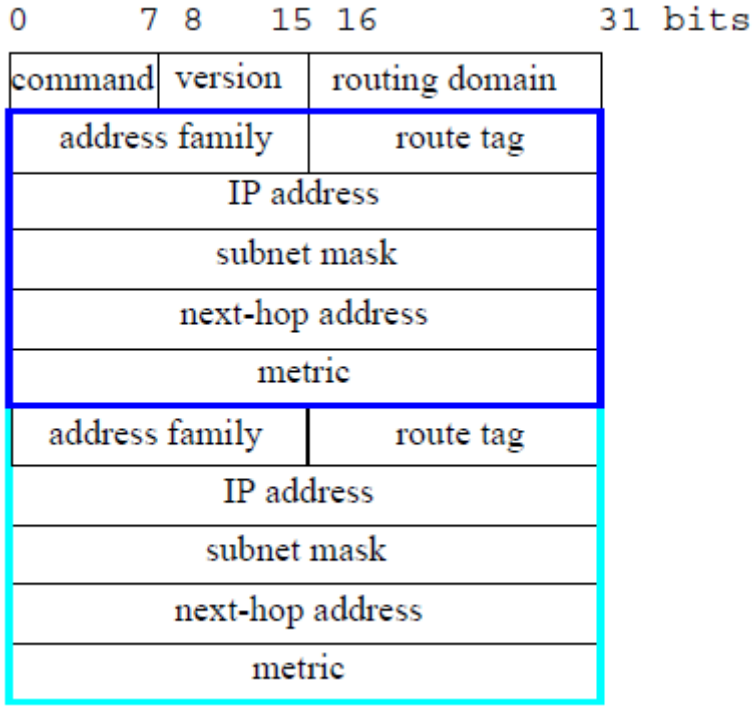
- Les messages de routage ont une longueur limitée : 512 octets
- si les informations à transmettre sont plus longues, on diffuse plusieurs messages de routage.
- le protocole RIP est sans mémoire ("memoryless"), ces messages ne sont pas liés (par ex. pas de n°).

Avantages:

Pour limiter les risques de congestion (avalanche/synchronisation) les diffusions sont retardées aléatoirement [RFC 1056] :

- diffusion immédiate [0-5s]
- diffusion périodique [15-45s]

4. Le format général des messages RIP :



Un message RIP a les ctatrerstiques suivantes :

- en mots de 32 bits
- longueur < 512 octets
- une entête d'un mot
- autant de blocs de 5 mots que d'entrées à transmettre
    - en nombre quelconque : [1-25]

- Le champ "**command** "(8 bits) : code le type du message :

.1 = demande d'information

- ✓ demande partielle pour certaines destinations (dont les entrées figurent dans la demande)
- ✓ demande totale (s'il y a une seule entrée associée à la demande tel que "address family"=0 et "metric"=16)

.2 = réponse

- ✓ l'extrait des meilleures routes du routeur
- ✓ suit à une demande, envoi périodique, envoi spontané

- Le champ "**version**"(8 bits) :

. 1 = RIP-1 (Þ les champs "routing domain", "route tag", "Subnet address", "next-hop address" sont inutilisés = 0)

. 2 = RIP-2

- Le champ "**routing domain**"(16 bits) :

. RIP est générique :

- ✓ plusieurs domaines peuvent être gérés simultanément par le même routeur.

. 0 par défaut et obligatoire pour RIP-1

- Le champ "**address family** "(16 bits) : code le format d'adressage :

. Les adresses peuvent être de longueur quelconque

. 2 = IP => (32 bits)

- Le champ "**route tag**"(16 bits) :

. Transmet des informations utilisées par le routage interdomaine (EGP)

. 0 pour RIP-1

- Le champ "**IP address**"(32 bits) : l'adresse de destination

. L’adresse d'un réseau IP (=> netid)

. L’adresse d'un sous-réseau IP (=> subnet mask : subnetid)

. L’adresse d'une station (=>@IP)

. L’adresse par défaut (=>n’importe quelle destination : 0.0.0.0)

- Le champ “**subnet mask**“(32 bits) :

. 0 pour RIP-1

. Spécifie la taille du champ “subnetID” dans le champ “hostID” de l'adresse IP.

- Le champ “**next-hop address**” (32 bits) :

. Contient explicitement l'adresse du prochain routeur qui est associé à l'entrée (ce n'est plus implicitement l'émetteur du message de routage. Cela permet à un routeur d'informer sur les meilleurs chemins d'un autre routeur).

. 0 = RIP-1

- Le champ “**metric**“(32 bits) :

. Distance en nombre de “hops” entre la destination spécifiée par “IP address” et le prochain routeur spécifié, soit par “next-hop address” (RIP-2), soit par l'adresse de l'émetteur du message (RIP-1).

. [1-15] : distance normale

. 16 = distance infinie (destination inaccessible

Chapitre III
QoS dans l'internet

Chapitre III : QoS dans l'internet

1. Introduction :

L'Internet est un réseau à commutation de paquets qui ne fournit qu'un service ``au mieux" (*best-effort*), c'est à dire qu'aucune garantie d'aucune sorte n'est faite sur le service offert, autre que l'engagement du réseau à faire ``du mieux qu'il peut" pour amener les paquets à destination.

Ce service s'avère suffisant pour les applications ``élastiques" de transfert de données telles que le courrier électronique, groupes de discussion, transfert de fichiers etc. qui n'ont pas de contraintes temporelles et peuvent donc accepter de grandes variations de délai et compenser les pertes éventuelles par des retransmissions. Ainsi le réseau ne fournit qu'un service minimal et toutes les applications initialement développées sur l'Internet se satisfont d'un tel service.

Cependant, le développement de l'Internet a suscité la création de nouveaux types d'applications, multimédias, et des applications en temps réel comme la téléphonie ou la vidéo qui sont très contraignantes

Ces applications ne peuvent pas se satisfaire d'un tel service minimal, elles ont besoin de garanties de délai et/ou de débit pour les flots de données qu'elles génèrent. Pouvoir satisfaire les besoins de ces applications, c'est leur fournir une qualité de service adaptée. Depuis quelques années la communauté Internet est mobilisée pour essayer d'introduire la notion de qualité de service (QoS) pour pallier aux lacunes de service « best effort » actuel.

Des travaux importants sont menés dans ce domaine,et cela a engendré de nombreux développements théoriques et pratiques en particulier, des techniques d'ordonnancement de paquets (comme par exemple le weighted fair queuing) permettent de garantir un débit et sous certaines conditions un délai à un flot de données. Dans le cadre de l'Internet, une architecture pour fournir la qualité de service a été développée par l'IETF. Basée sur l'intégration de

services, l'architecture IntServ/RSVP utilise le protocole RSVP pour gérer des réservations de ressources pour chaque flot de données. Plus récemment, une approche différente a été proposée par l'IETF : la différenciation de services, DiffServ, repose sur une gestion de trafic par classe et des méthodes de conditionnement du trafic à l'entrée dans le réseau. Cette approche résout certains des problèmes qui se posent à IntServ mais apporte ses propres difficultés.

2. Généralités

2.1 Définitions de Qualité de service :

La qualité de service (Quality of Service) d'un réseau désigne sa capacité à transporter dans de bonnes conditions les flux de données issus de différentes applications (informatique, voix, image). Les flux engendrés par les applications étant très divers, ils donneront lieu à des mises en oeuvre variés selon le niveau de QOS exigé par les applications. EN résumé, la QOS sur le réseau consiste un paradoxe : la simplicité de construction des réseau informatique (IP), qui a permis de se concentrer sur les applications est à la base du succès de l'Internet. [21]

2.2 Paramètres de QoS :

Les différents paramètres ou critères qui caractérisent la qualité de service sont :

- Disponibilité du service rendu
- La bande passante
- Délai de traversée du réseau (latence)
- La variation de délai (gigue)
- Le taux de perte de paquets

Chapitre III : QoS dans l'internet

1-Disponibilité

La disponibilité du réseau se définit comme le rapport entre le temps de bon fonctionnement du service et le temps total d'ouverture du service. En d'autres termes c'est la durée qui s'écoule entre le moment où une demande de connexion est émise et le moment où la confirmation de cet établissement est reçue et plus ce délai est court meilleure est la qualité de service.

2-Bande passante (Debit)

Mesure le nombre d'octets utiles qui peuvent être transférés en une seconde, ce débit est évalué séparément dans les deux sens. La bande passante disponible sur un chemin entre une source et une destination correspond à la plus petite capacité disponible sur ces liens.

3-Latence (Délai)

Temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Ce temps est évalué séparément dans les deux sens. La latence dépend des facteurs suivants :

1. du type de média de transmission (temps de propagation)
2. du nombre d'équipements réseau traversés (temps de traitement)
3. La taille des paquets (temps d'émission) : Correspond au temps nécessaire pour écouler les paquets sur le lien réseau bit par bit jusqu'au dernier bit.

Ce paramètre est particulièrement important dans les applications temps réel telles que le VoIP (Voice over IP).

4- Gigue

Se définit comme la variation de délais d'acheminement (latence) des paquets sur le réseau. Ce paramètre aussi, est particulièrement sensible pour les applications multimédia temps réel qui requièrent un délai interpaquet relativement stable. Pour maintenir une stabilité minimale et éviter les ruptures de débit, il convient par exemple de placer une mémoire tampon ou cache en réception ;Son rôle est d'assurer une indépendance minimale du débit de sortie par rapport au débit d'entrée.

5- Taux de perte

C'est le rapport du nombre de paquets émis et le nombre de paquets reçus. il s'agit de mesure de la capacité utile de transmission. Les pertes peuvent se produirent quand des nœuds du réseau, lors d'une congestion, abandonnent des paquets. Le protocole TCP implémentant un système de protection contre les pertes, les paquets perdus sont retransmis. Si la congestion est importante, les performances du réseau baissent dramatiquement, car toute la bande passante est occupée par les retransmissions.

Exemples d'applications [3]

Le tableau suivant présente l'importance des paramètres définis ci-dessus sur des types de trafic usuels. Sans QoS, tous ces trafics se partageraient les mêmes paramètres de liaison.

Applications	**Bande passante(débit)**	***Sensibilité pour***		
		latence	**gigue**	**perte**
Voip	faible	haute	Haute	Moyenne
Video conference	haute	haute	Haute	Moyenne
Streaming video	Haute	Moyenne	Moyenne	Moyenne
Streaming audio	Faible	Moyenne	Moyenne	Moyenne
E_mail	Faible	faible	faible	Haute
Transfert de fichiers	moyenne	faible	faible	haute

Remarque : plusieurs facteurs peuvent avoir un impact sur ces critères,on peux citer par exemple :

- ***L'instabilité dans les protocoles de routage*** influence la gigue ou variation du délai de bout en bout de manière significative, en forçant les routeurs à modifier le choix du chemin, lors de changement de topologies ou situation de congestion

- ***Les routeurs*** peuvent aussi avoir un impact significatif sur le délai, la gigue et la disponibilité. En effet, les fonctions d'un routeur consistent à contrôler l'intégrité du paquet reçu sur l'interface d'entrée, déterminer l'interface de sortie en fonction de la destination souhaitée, puis stocker ce paquet dans la file d'attente associée à celle-ci. Lorsque le fonctionnement se dégrade (trop de trafic compte tenu des capacités du routeur) les files d'attente se remplissent, introduisant un délai supplémentaire dans la transmission des paquets, puis le routeur est forcé de jeter des paquets. Ces différentes actions ont un impact sur le délai, la gigue et en augmentant la probabilité de paquets transmis dans le désordre influent également sur la disponibilité.

- ***Les liaisons*** qui possèdent des caractéristiques de délai, débit maximum et disponibilité,

Dans ce contexte, offrir un service de bonne qualité consiste à fournir un service avec un délai et une gigue minimum ainsi qu'une disponibilité et un débit maximum, assurant un service "best-effort" convenable pour tous les types de trafic

3. Implémentation de la Qualité de Service dans l'Internet (classes de service différenciées) :

La Qualité de Service est généralement assimilée à la discrimination des services, autrement dit à la définition de **classes différenciées de services.** Mais cela signifie aussi **garantir** un service et pour cela réserver des ressources.[3]

Pour implémenter ces classes ou garantir des ressources, il faut définir une ou plusieurs **politiques** sur les nœuds du réseau permettant d'implémenter la Qualité de Service demandée, en utilisant divers mécanismes (trafic shaping, admission control, gestion de la congestion etc...).

3.1 Où implémenter ces politiques ?

Implémenter une politique dans un grand réseau est compliqué : le choix des systèmes sur lesquels mettre en oeuvre les mécanismes a un impact direct sur les performances globales du réseau.

L'architecture générique de l'Internet fait la distinction entre le système global à haut débit qui constitue le coeur du réseau (core ou backbone), et les systèmes réalisant l'accès aux réseaux terminaux (access).

Les fonctions principales des routeurs constituant le core, consistent à acheminer les paquets aussi vite que possible, ainsi que construire et échanger les informations de routage avec ses voisins. Les routeurs d'accès se chargent des fonctions de contrôle d'intégrité et d'admission des paquets dans le réseau.

Implémenter une politique de différenciation de trafic doit se faire sur les routeurs d'accès (filtrage de routes et de trafic, contrôle de la bande passante, politique de routage,

gestion de la congestion...) afin de ne pas affecter les performances globales et maintenir la stabilité dans le coeur du réseau. Les méthodes mises en oeuvre pour implémenter ces classes de services doivent tenir compte de ces considérations.

3.2 Comment implémenter des services différenciés?[5].[6]

Pour implémenter la Qos divers mécanismes peuvent être utilisés à savoir

- Gestion des files d'attente
- Contrôle du trafic « trafic shaping »
- Prévention de la congestion

1-Gestion des files d'attente :

La file d'attente est un composant central dans l'architecture des routeurs. Un routeur permet de :

- Assembler les paquets reçus (file d'attente en entrée),
- Contrôler l'intégrité du paquet (calcul du checksum),
- Déterminer l'interface de destination,
- Transmettre les paquets (files d'attente en sortie).

La stratégie de gestion des diverses files d'attente sur un routeur joue un rôle essentiel dans la différenciation des services, à travers le choix de l'algorithme qui place les paquets dans la queue de sortie, et le choix de la taille maximale de la queue. Plusieurs algorithmes ont été développés:

- **FIFO (First In First Out):** dans cette méthode les paquets sont places dans la file de sortie dans l'ordre dans lesquels ils sont reçus.

- **Priority Queuing (FQ)** dans cette méthode un trafic particulier peut être identifié et réordonné dans la file de sortie suivant un critère fourni par l'utilisateur dans la file de sortie.
- **Class_Based Queuing** (**CBQ**) Ce mécanisme, utilisé pour éviter qu'une seule classe de trafic ne monopolise les ressources, définit plusieurs files de sortie avec une priorité et un total de trafic autorisé. Le trafic est extrait de chaque queue suivant une rotation
- **Weighted Fair Queuing (WFC)** Cet algorithme donne un traitement prioritaire aux flux de faible volume et permet aux flux de volume important d'utiliser la place qui reste. Pour cela, il trie et regroupe les paquets par flux, puis met ceux-ci en file d'attente suivant le volume de trafic dans chaque flux.

2-Trafic shaping (Lissage du trafic) :

Permet de contrôler le volume de trafic entrant dans le réseau ainsi que le débit avec lequel il est transmis. Les deux techniques principales de Trafic Shaping sont:

- ***Leaky Bucket :***Le trafic arrivant dans la file d'attente est régulé pour sortir en flux fixes sur le réseau. La taille de la file d'attente et le taux de transmission sont configurables par l'utilisateur.

  Ce mécanisme est bien adapté pour envoyer des débits fixes sur le réseau mais, en contrepartie, ne permet pas d'utiliser plus de ressources lorsque le réseau est peu chargé.

- ***Token-Bucket :*** Le trafic ne traverse pas effectivement le seau, mais est transmis sur la base de jetons (octets) présents dans le seau.

Ce mécanisme permet à un trafic en rafale d'être transmis tant qu'il y a des jetons dans la file d'attente (ceux-ci ayant pu être accumulés en situation de réseau peu chargé).

3- Prévention de la congestion :

La gestion des phénomènes de congestion est un point fondamental pour garantir la QoS des flux. En effet, les mécanismes de gestion des QoS n'auront un impact effectif que lorsque le réseau sera chargé. pour prévenir la congestion on peut utiliser les deux techniques suivantes :

- ***Random Early Detection (RED):***

  Cette technique consiste à jeter des paquets de manière aléatoire, en prévention. Le seuil à partir duquel RED commence à jeter les paquets est configurable par l'administrateur ainsi que le taux de remplissage de la file.

- ***Weighted Random Early Detection (WRED)***

  Cette technique est semblable à la précédente, mais permet de déterminer quel trafic est jeté. Elle s'appuie sur les techniques de IP Precedence mises en oeuvre sur les routeurs d'accès.

4. Modèles de QoS et protocoles :

Tous les mécanismes cités précédemment fournissent des niveaux variés de services et constitue une méthode simple d'implémentation de classes de services différenciées.

Mais cela ne suffit pas à garantir le service. Pour cela, il faut s'appuyer sur des modèles développés par l'IETF (Internet Engineering Task Force)

- **INTSERV** (Integrated Service),
- **DIFFSERV** (Differentiated Services)
- **MPLS** (MultiProtocol Label Switching).

4.1 le modèle INTSERV/RSVP (RFC 1633)[16].[17] :

Ce modèle repose sur un mécanisme de réservation des ressources dans le réseau par flux pour donner à chaque application les garanties dont elle a besoin. Ce modèle utilise le protocole RSVP pour la réservation de ressources entre l'émetteur et le récepteur.

4.1.1 Définition d'un flux Intserv :

Dans Intserv un flux de données (ou flot) correspond à une suite de paquets possédant les mêmes sources, destinations (une ou plusieurs)et qui ont besoin de la même qualité de service. Un flux est défini par :

- Adresse IP source
- Adresse IP destination
- Numéro de port source
- Numéro de port destination

4.1.2 Modele de service :

En plus du service best effort,le modèle INTSERV propose deux classes de services :

- **Le service garanti** (Guaranteed Service : GS) : garantie de bande passante et un délai d'acheminement limité Elle s'adresse aux applications temps réel non adaptatives
- **La charge contrôlée** (Controlled Load ;CL) : Ce service propose aux applications une connexion de bout en bout de type best effort mais dans des conditions de charge normale. Il est donc plus élaboré que le best effort mais sans garantie. Cette classe est destinée tout particulièrement aux applications multimédia adaptatives dont l'usage s'est développé ces dernières années. Il a en effet été constaté que ces applications se comportent remarquablement bien avec un service *best-effort*, s'adaptant aux variations et aléas du service

tant que le réseau n'est pas dans une situation de congestion critique, auquel cas leur comportement se dégrade très rapidement.

4.1.3 Architecture de base d'un routeur Intserv [18].[21] :

Pour mettre en place ces services, il faut intervenir sur la structure des routeurs d'un réseau IP en y incluant des mécanismes complémentaires de contrôles. La Figure 2 montre les composants fonctionnels d'un tel nœud. On y voit en particulier apparaître des mécanismes de contrôle absents d'un nœud classique.

Un routeur prenant en charge les services Intserv doit mettre en œuvre les fonctions suivantes:

- Le classificateur de paquets (*Packet Classifier*)
- L'ordonnancement des paquets *(Packet scheduler)*
- Le contrôle d'admission *(Admission control)*
- Le protocole de réservation de ressources RSVP

1- Le Classificateur de paquets

Le classificateur de paquet détermine à quel flot appartient un paquet. Principalement, il s'agit de déterminer si le paquet arrivant dans un nœud appartient à un flux best effort ou s'il doit bénéficier d'une réservation. Cette classification réalisée sur chaque routeur du réseau se fonde sur les informations contenues dans le paquet lui-même (champ TOS ou DSCP).

2- L'Ordonnanceur de paquets

L'Ordonnanceur de paquets détermine l'ordre de traitement des paquets classifiés et gère la retransmission des différents paquets en utilisant un ensemble de files d'attente, chaque file correspondant à une classe de service gérée par différents algorithmes du style Simple Priorité (FIFO), gestion par classe (custom queuing), partage équitable (weighted fair queuing), etc…

3- *Le contrôle d'admission :*

Détermine si la Qos demandée par un flux peut lui être attribuée sans affecter les flux existants, il sert aussi à déterminer si le flux entrant est conforme au profil de trafic prévu et à marquer le trafic non conforme. Pour déterminer si un trafic correspond ou non à un

profil on peux utiliser le mécanisme du seau à jetons « token bucket » qui indique à quel moment le trafic peut être émis,en fonction des jetons présents dans le seau.

4- ***Le protocole de réservation RSVP :***

Le protocole de réservation (RSVP: Ressource ReSerVation Protocol) sert à créer et à mettre à jour l'état relatif à une réservation dans les routeurs situés sur le chemin que le flux emprunte ainsi que dans les machines d'extrémité. Ce protocole est en charge de la signalisation associée au mécanisme de réservation.

La concaténation de ces éléments assurant le service le long du chemin de Bout en bout fournit une vue globale de la Qualité de Service.

4.1.4 Le protocole RSVP :

Définition : RSVP est un protocole de signalisation qui fournit l'initialisation et le contrôle de réservations nécessaires aux services intégrés (Intserv)

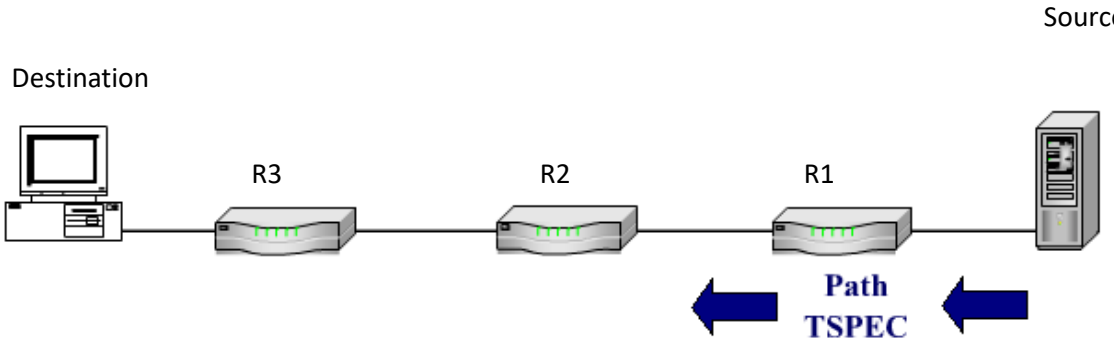
Caractéristiques

- RSVP rend obligatoire la demande de QoS par le récepteur plutôt que par l'émetteur, ce qui permet d'éviter que certaines applications émettrices monopolisent des ressources inutilement, au détriment de la performance globale du réseau
- RSVP travaille au dessus de IP (IPv4 ou IPv6) et occupe la place d'un protocole de transport dans la pile des protocoles mais ne transporte pas de données utilisateurs comme ICMP ou IGMP
- RSVP n'est pas un protocole de routage. Il est sensé travailler avec les protocoles de routage unicast et multicast comme RIP, OSPF, RPM,...
- RSVP fait des réservations de ressources pour les applications unicast et multicast et s'adapte dynamiquement aux évolutions (comme les changements de routes par exemple ou introduction de nouveaux membres dans un groupe multicast)

- Il demande des ressources dans une seule direction et traite l'émetteur et le récepteur de manière différente
- RSVP établit et maintient un état logiciel entre les noeuds constituant le chemin réservé. cet état logiciel est caractérisé par des messages périodiques de rafraîchissement envoyés le long du chemin pour maintenir l'état

4.1.5 Fonctionnement de RSVP

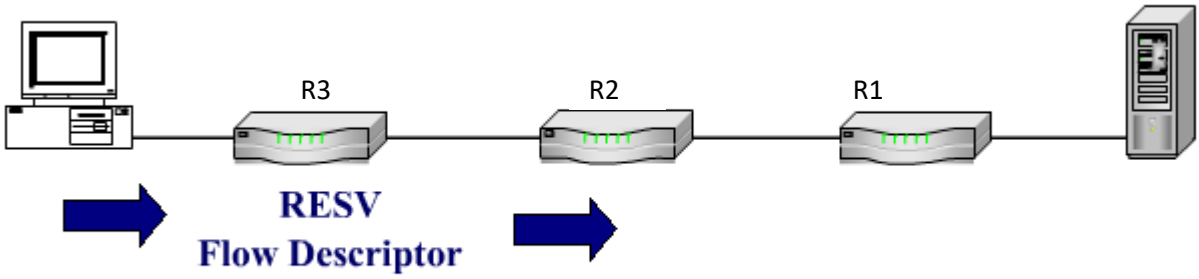
- L'émetteur spécifie le trafic en terme de bande passante maximale et minimale,délai d'acheminement et gigue dans un descripteur de trafic TSPEC .il envoie un message PATH contenant TSPEC à l'adresse de destination avec une spécification additionnelle ADSPEC
- Path est acheminé vers le destinataire à l'aide du protocole de routage unicast ou multicast



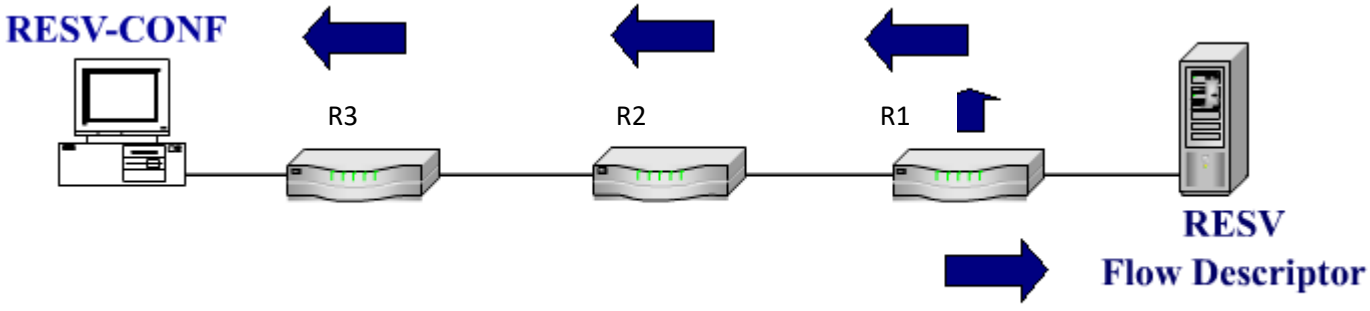
- Chaque routeur rencontré sur la route empruntée mémorise des informations relatives au chemin constitué « PATH STATE » qui incluent l'adresse d'origine du message PATH puis transfère PATH au routeur suivant.PATH STATE permet le retour du message RESV
- Grâce à TSPEC (décrites par l'émetteur) et ADSPEC (modifiées par le réseau pour rendre compte des ses possibilités réelles),le récepteur détermine les paramètres à utiliser en retour. il envoie un message RESV incluant une spécification de demande

RSPEC (indique le type de service) et une spécification de filtre FILTER SPEC qui caractérisent les paquets

- Le message RESV revient en amont en utilisant la route indiquée dans PATH



- Quand chaque routeur reçoit RESV,il utilise son processus de contrôle d'admission pour authentifier la demande et procéder à l'allocation de ressources .si la requête ne peux être satisfaite (faute de ressource ou échec d'authentification)le routeur retourne un message d'erreur au récepteur .si la requête peut être satisfaite le routeur configure le classificateur de paquets pour qu'il sélectionne les paquets définis dans Filter Spec et demande au lien réseau d'obtenir la QoS définie dans Flow Spec .il envoie alors un RESV au routeur suivant.
- Quand le dernier routeur reçoit RESV et l'accepte, il envoie un message de confirmation en retour au récepteur



Cas Multicast

Dans ce cas le message PATH sera acheminé vers les destinataires à l'aide d'un protocole Multicast.chaque destinataire enverra vers l'émetteur un message RESV.l'ensemble de ces messages RESV seront fusionnés au niveau des points de réplication. Le FlowSpec le plus important est utilisé. Deux demandes de 25 Mbps et de 10 Mbps donne une demande de 25 Mbps

Les limitations du modèle INTSERV/RSVP

- IntServ pose le problème de scalabilité qui désigne la possibilité de continuer à bien se comporter lorsque le nombre de flots devient très grand. En effet, le contrôle IntServ se faisant sur la base de flots individuels, les routeurs du réseau doivent garder en mémoire les caractéristiques de chaque flot. Les traitements de nombreux flots de classes et de paramètres distincts constituent également une autre lourdeur de taille. Cette approche de la QoS est complexe à mettre en œuvre. Elle convient plutôt aux réseaux de petites tailles, mais n'est pas vraiment adapté à Internet dans son ensemble. De ce fait, il a été peu déployé. De plus il suffit qu'un seul routeur sur le chemin de Transmission n'offre pas le service d'IntServ pour que le service IntServ soit mis à mal
- La réservation de ressources est limitée dans le temps, elle doit etre donc périodiquement rafraîchie car RSVP est indépendant du routage, donc il faut vérifier périodiquement si le routage n'a pas été modifié (changement de topologie par panne d'un routeur par exemple). Si le routage est modifié, il serait vain de continuer à réserver des ressources dans des équipements qui ne se trouvent pas sur la nouvelle route empruntée.

4.2 Le Modèle DIFFSERV :[21].[19].[13].[14].[20]

4.2.1 Présentation des services différenciés

4.2.1.1 Pourquoi DiffServ ?

Les algorithmes des services intégrés sont capables de fournir une bonne qualité de service à un ou plusieurs flux car ils réservent les ressources requises le long des itinéraires. Ils présentent toutefois l'inconvénient de nécessiter une configuration avancée pour établir chaque flux, une caractéristique qui les empêche de bien s'adapter lorsqu'il faut établir des milliers ou des millions de flux.

De plus, ils maintiennent en interne sur les routeurs l'état de chaque flux, ce qui les rend fragiles lorsqu'un routeur tombe en panne. Pour ces raison, l'IETF a également imaginé une approche plus simple de la qualité de service, qui peut être implémentée pour une grande part localement sur chaque routeur sans nécessiter de configuration avancée ni la participation de l'ensemble des acteurs sur le parcours : il s'agit de la qualité de service par classe (par opposition à celle par flux). L'IETF a normalisé une architecture pour sa mise en œuvre, appelée les services différenciés, qui est décrite dans les RFC 2474 et 2475

4.2.1.2 Définition du modèle DiffServ :

La différenciation de services consiste dans une situation de congestion à respecter les pertes de paquets sur certaines classes de trafic, pour en protéger d'autres. Les services différenciés peuvent être offerts par un ensemble de routeurs formant un domaine administratif (par exemple : un opérateur de téléphonie).

Le domaine définit un ensemble de classes de services avec leurs règles de transmission correspondantes. Le modèle DiffServ permet d'assurer une qualité de service sans avoir besoin de signalisation. Il repose sur un contrat négocié entre le client et son fournisseur (SLA : Service Level Agreement).

Le principe de DiffServ consiste à introduire plusieurs classes de services offrant chacune une qualité de service différente. Chaque flux de trafic se voit attribuer une classe de service appropriée. Cette classification de trafic est effectuée en périphérie de réseau, directement à la source ou sur un routeur d'accès, selon des critères pré-configurés.

Cette stratégie ne requiert aucune configuration avancée, aucune réservation de ressources et aucune négociation pour chaque flux, comme c'est le cas pour les services intégrés. L'avantage de DiffServ est qu'il n'y a plus nécessité de maintenir un état des sources et des destinations dans les routeurs de cœur du réseau, d'où une meilleure *scalability*.

4.2.1.3 Fonctions de DiffServ

Les fonctions de DiffServ sont :

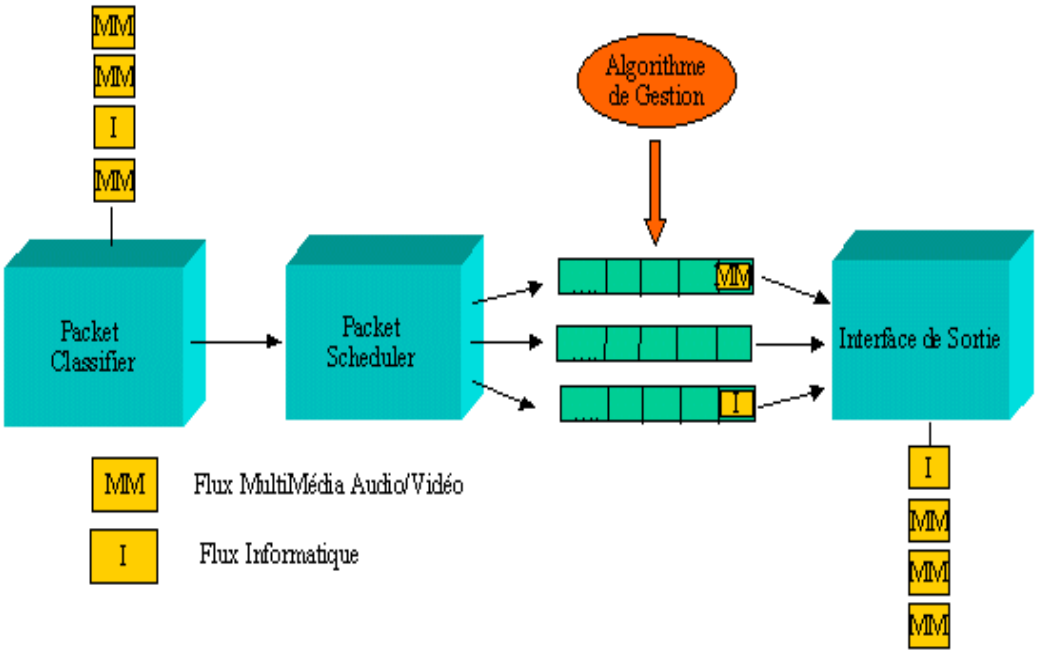
1-La classification du trafic par application/réseau.

2-Le marquage des paquets.

3-La régulation du trafic en utilisant les techniques de lissage et de policing,

4-Les gestions des files d'attente par classe et par flux.

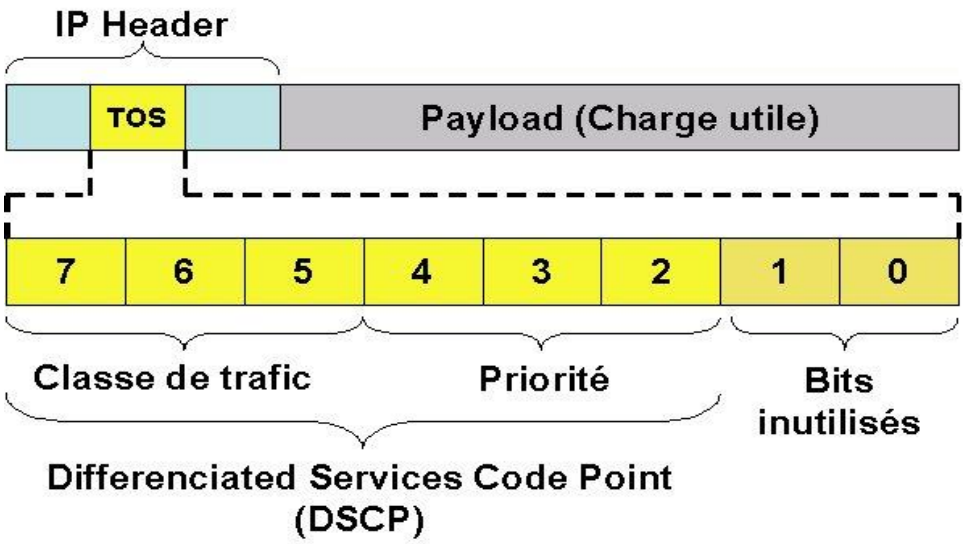
Le lissage permet de retarder les paquets pour respecter le débit. Le policing effectue le rejet de paquets.



4.2.1.4 Fonctionnement de DiffServ

Identification de la classe d'un paquet et principe du DSCP :

Chaque classe est identifiée par une valeur codée dans l'en-tête IP dans Champ Type Of Service (TOS) pour Ipv4.Ce champ a été redéfini en champ DS par l'IETF et porte l'indice de la Classe de Service : DSCP (Differentiated Service Code Point).DSCP est le champ qui identifie le traitement que le paquet doit recevoir. Ce champ est codé sur 6 bits et fait parti des 8 bits codant le champ TOS d'IPv4,



Entête d'un datagramme IPv4

Les classes de service de DiffServ :

Les routeurs DiffServ traitent les paquets en fonction de la classe codée dans l'en-tête IP (champ DS) selon un comportement spécifique : le PHB (Per Hop Behaviour).

Le PHB est donc le paramètre qui définit le comportement des routeurs du cœur du réseau. Il influence la façon dont les files d'attentes du routeur et le lien, sont partagés parmi les différentes classes de trafic

Une chose importante dans l'architecture DS est que les PHB routeurs se basent uniquement sur le marquage de paquet, c'est à dire la classe de trafic auquel le paquet appartient ; en aucun cas ils ne traiteront différemment des paquets de sources différentes.

Les PHB sont mis en oeuvre par les constructeurs dans les routeurs en utilisant des mécanismes de gestion de files d'attente (Custom Queuing, Weighted Fair Queuing,..et de régulation de flux.

En aucun cas, les routeurs ne traiteront différemment des paquets de même PHB de sources différentes.

DiffServ définit 4 PHB ou classes de services :

- Best Effort (priorité basse) : PHB par défaut avec un DSCP 000 000.

- Expedited Forwarding (EF) ou transmission accélérée, DSCP 101 110.

- Assured Forwarding :(AF) ou transmission garantie.

- Default Forwarding (DF).

Chapitre III : QoS dans l'internet

1- Best Effort

Le principe du Best Effort se traduit par une simplification à l'extrême des équipements d'interconnexion. Quand la mémoire d'un routeur est saturée, les paquets sont rejetés

2 -Expedited Forwarding(traitement accéléré)

Expedited Forwarding ou Premium service correspond à la priorité maximale. Son objectif est de fournir un service de transfert équivalent à une ligne dédiée, avec très peu de pertes et la gigue et le délai réduits au minimum. Il existe deux classes de services : service ordinaire et service accéléré.

La plus grande majorité du trafic est traitée avec un service ordinaire, mais une petite fraction doit être traitée avec le service accéléré.

Il ne s'agit que d'une seule ligne physique. Une façon d'implémenter cette stratégie est de programmer les routeurs pour qu'il y ait deux files d'attente par ligne de sortie : une pour les paquets ordinaires et une autre pour les paquets accélérés.

On peut réaliser ce type d'allocation en transmettant un paquet urgent tous les quatre paquets ordinaires, en supposant une répartition égale pour les deux classes de trafic. Le contrat porte sur un débit constant. Les paquets excédentaires sont lissés ou rejetés à l'entrée pour toujours rester conforme au contrat. L'opérateur s'engage à traiter ce trafic prioritairement.

Pour atteindre ces performances, les paquets d'un service EF ne devraient pas subir de files d'attente ou passer par des files de très petites tailles et strictement prioritaires. EF est un comportement coûteux, en particulier à cause des garanties de délai qu'il peut offrir.

3- Assured Forwarding

Il existe une catégorie de classes de services plus élaborée : la transmission garantie AF regroupe plusieurs PHB garantissant un acheminement de paquets IP avec une haute probabilité, sans tenir compte des délais.

Pour l'AF, il est défini 4 classes de service et 3 priorités de rejets (appelées niveau de post précédence) suivant que l'utilisateur respecte son contrat, le dépasse légèrement ou est largement en dehors. Les classes sont donc choisies par l'utilisateur et restent les même tout au long du trajet dans le réseau.

Chaque classe peut être vue comme une file d'attente séparée en utilisant une certaine proportion des ressources du réseau. A l'intérieur de chaque classe, un algorithme de rejet sélectif différencie les 3 niveaux de priorités.

En cas de congestion dans une classe AF, les paquets de basse priorité sont rejetés en premier (la priorité peut être modifiée dans le réseau par les utilisateurs en fonction du respect ou non du contrat.).Les étapes du traitement du paquet dans le cas de la transmission garantie :

- La première étape consiste à classer les paquets en fonction des 4 classes de priorités. Elle peut être réalisée sur l'hôte émetteur, ou sur le premier routeur d'accès. (L'avantage d'effectuer la classification sur l'hôte émetteur est qu'il est possible de savoir à quel flux appartient le paquet.)

- La deuxième étape consiste à marquer les paquets en fonction de la priorité définie. Pour cela, on utilise le champ codé dans l'en-tête du paquet IP

- La troisième étape consiste à faire passer les paquets à travers un filtre de canalisation/suppression qui peut retarder ou éliminer certains paquets pour donner aux 4 flux un comportement acceptable, par exemple, en utilisant des techniques de seau percé. S'il y a trop de paquets, certains pourront être supprimés à ce stade en fonction de leur catégorie.

Les objectifs de la différenciation par l'Assured Forwarding sont l'attribution différenciée des ressources et la protection des flux TCP des flux UDP.

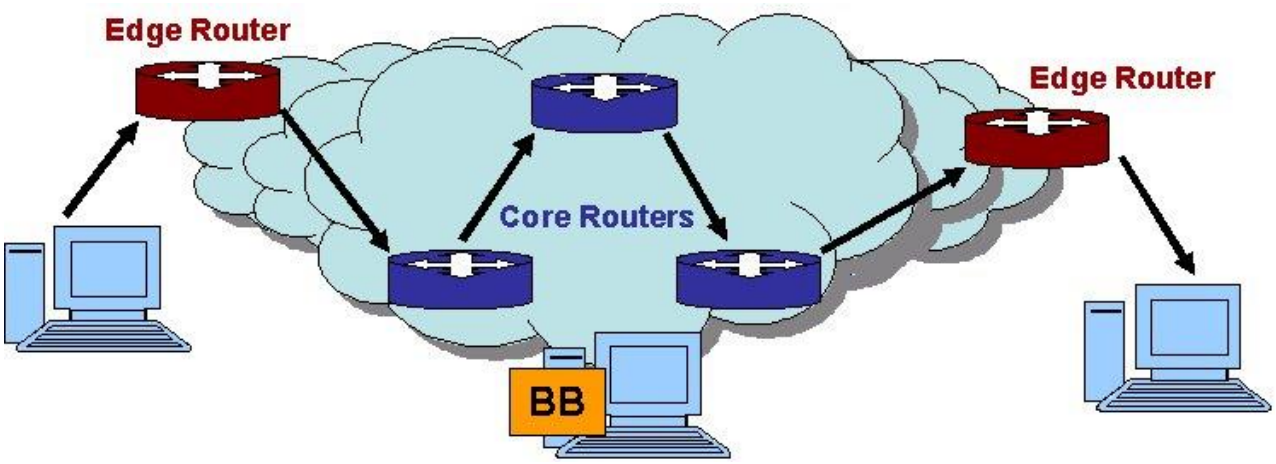
4 - Default Forwarding (DF) :

DF est utilisé uniquement pour les flux Internet qui ne nécessitent pas un trafic en temps réel.

L'architecture du modèle DiffServ :[2].[5].[19]

L'idée consiste à diviser le réseau en domaines qui désignent un ensemble de nœuds (routeurs) contigus ayant un service commun de règles et de groupes de PHB; Chaque DS domain comprend deux types de noeuds: les routeurs intérieur (Core router) et les routeurs d'accès et de bordure (Edge router). Les routeurs d'accès sont connectés aux clients, tandis qu'un routeur de bordure est connecté à un autre routeur de bordure appartenant à un domaine différent et joue un rôle différent.

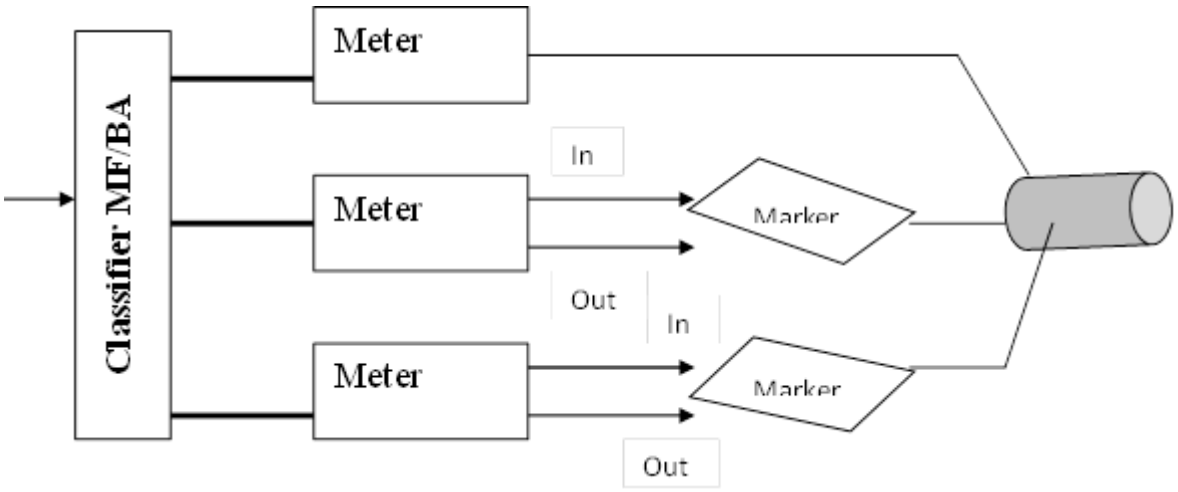
.



Architecture du modèle DiffServ

a- Les routeurs de bordure (edge routers)

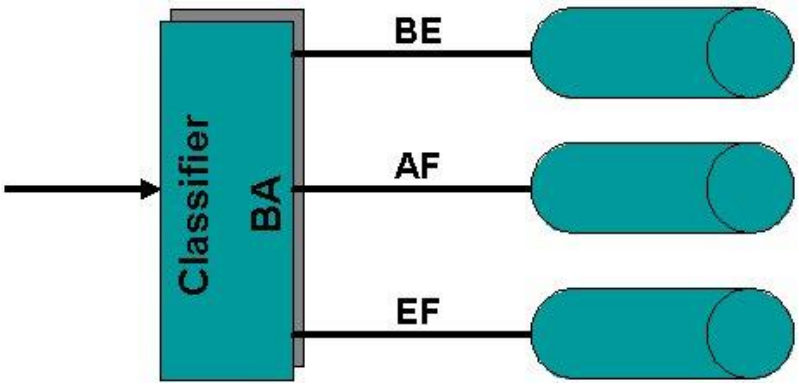
Ils sont responsables de la classification des paquets et du conditionnement du trafic. En bordure du réseau, c'est-à-dire à l'arrivée du premier élément actif capable de traiter le champ DS (DS-capable), les paquets arrivant ont dans leur champ TOS une certaine valeur DS. La marque qu'un paquet identifie la classe du trafic auquel il appartient. Après son marquage, le paquet est envoyé dans le réseau ou jeté.



Traitement d'un paquet par un Edge Router

b- Les routeurs du cœur du réseau (core routers)

Ils sont responsables de l'envoi uniquement. Quand un paquet, marqué de son champ DS, arrive sur un routeur DS-capable, celui-ci est envoyé au prochain nœud selon ce que l'on appelle son Per Hop Behaviour (PHB) associé à la classe du paquet. Le PHB influence la façon dont les buffers du routeur et le lien ; sont partagés parmi les différentes classes de trafic.



Traitement d'un paquet par un Core Router

Le traitement différencié des paquets :

Dans l'architecture DiffServ, le traitement différencié des paquets s'appuie sur plusieurs opérations fondamentales :

- Classification des flux en classes de services.
- Conditionnement du trafic.
- Gestion de la congestion : introduction des priorités au sein des classes (scheduling) et gestion du trafic dans une classe donnée (queue management).

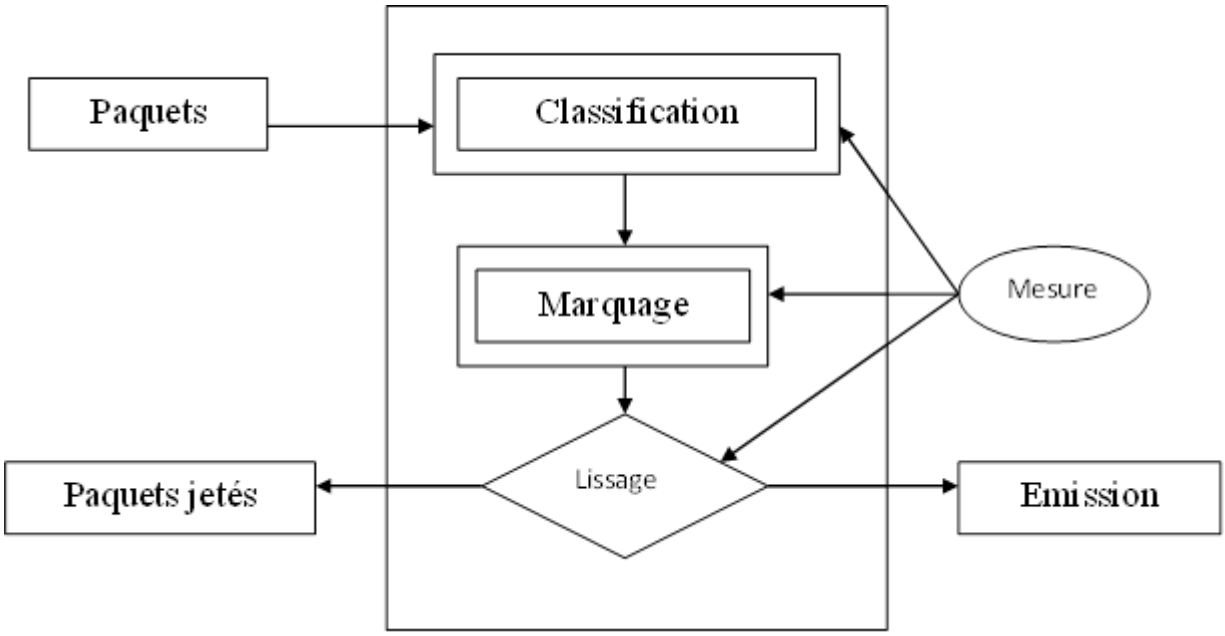
1-Classification et conditionnement du trafic

La classification s'effectue suivant une ou plusieurs valeurs contenues dans l'en-tête IP . On en distingue 2 types :

- BA (Behaviour Aggregate): classification établie uniquement en fonction de la valeur du champ DS.
- MF (Multi Field): classification établie selon la valeur d'un ou de plusieurs champs de l'en-tête du paquet (champ DS, @ source, @ destination, port...)

Celle-ci faite, elle dirige le paquet vers la fonction de marquage appropriée .Une fois les paquets marqués, ils sont envoyés à leur destination puis à chaque routeur DS-capable, ils reçoivent le service associé à leur classe. En plus de cette classification/marquage, un mécanisme de profilage du trafic est mis en place. Il a pour objet la prise en compte du taux d'arrivée des paquets, afin de ne pas dépasser le seuil maximum de paquets pouvant être envoyés sur le réseau. Ainsi, un mécanisme de mesure du trafic permet de savoir si le flot de paquets entrant correspond au profil de trafic négocié. Si ce flot dépasse un certain seuil, certains paquets seront marqués comme moins prioritaires et seront

automatiquement jetés en cas de congestion dans le réseau comme le montre la figure ci-dessous :



Classification, marquage et conditionnement du trafic au niveau du edge router

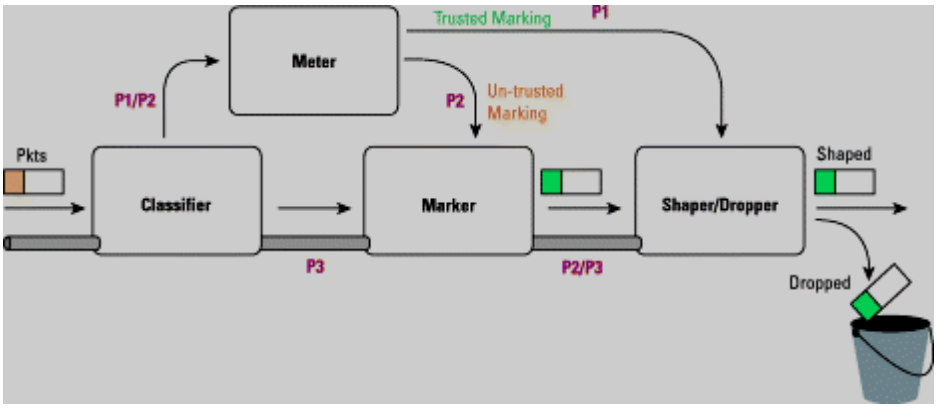
Le Conditionnement du trafic met donc en oeuvre 4 composants:

1-Meter : mesure du trafic pour vérifier s'il est compatible avec le contrat et fourniture des infos aux autres composants.

2-Marker: affectation d'un DS qui peut être différent de celui qui est reçu.

3-Shaper: lissage du trafic en retardant certains paquets de telle sorte qui'il respecte le débit contractuel.

4-Dropper: suppression de paquets dépassant le trafic contractuel.



Conditionnement du trafic

Limitations du modèle Diffserv

- Diffserv nécessite d'établir préalablement un contrat dans tous les équipements de son domaine. Ceci implique une connaissance approfondie des applicatifs pouvant transiter sur le réseau et peut se révéler parfois difficile à appliquer.
- Le fonctionnement basé sur l'agrégation de flux implique aussi une perte de granularité des applications transitant sur le réseau. Cela peut se révéler dans certains cas inadapté.

4.3 Multi-Protocol Label Switching (MPLS):[21].[3]

4.3.1 Définition et caractéristiques :

L'objectif de Diffserv est de fournir une solution de qualité de service qui résiste au facteur d'échelle. Le protocole MPLS, a été conçu pour répondre aux mêmes besoins.

MPLS est un nouveau standard de l'IETF visant à homogénéiser les différentes approches de commutation multi niveau. Les techniques commutations multi niveau ont pour objectifs d'associer efficacement les avantages de routage niveau 3 et ceux de la commutation niveau 2.

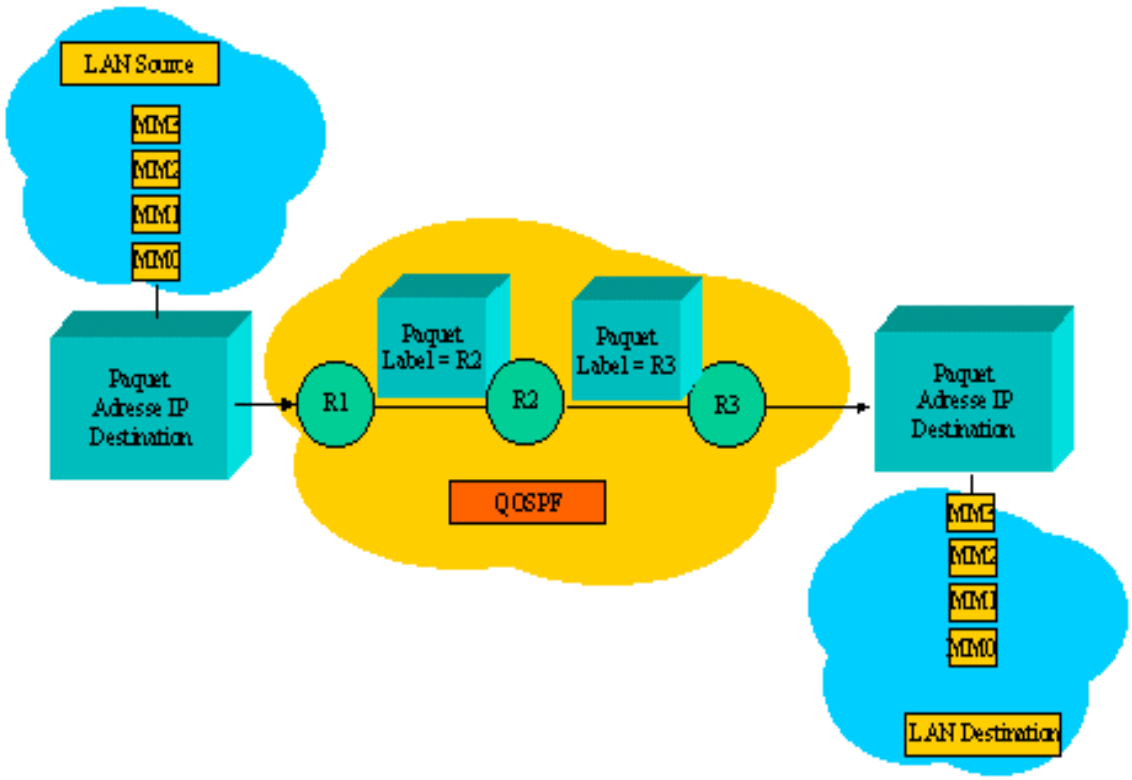
En bref, MPLS traduit la volonté de l'IETF d'améliorer les débits grâce à l'optimisation de la complexité du traitement des paquets IP dans le réseau .MPLS se fonde sur le concept de commutation multiniveau proposé par Cisco : le tag switching.

Ainsi l'architecture MPLS est composée d'un certain nombre de protocoles définis ou en cours de définition. Selon le domaine d'application de MPLS. Les protocoles mis en œuvre sur le mécanisme de base seront différents.

MPLS n'est pas proprement parler une technique de QoS, mais on peut mettre en œuvre les mécanismes de QoS à l'intérieur de l'architecture MPLS.

MPLS se caractérise comme suit :

- Il définit les mécanises de gestion de flux selon différents niveaux de précision ;
- Il est indépendant des protocoles de niveau 2 et 3 qu'il supporte ;
- Il permet d'assigner des profils de trafic (Forwardinge Equivalence Class) à des labels (ou étiquettes), qui serons utilisés par différents technologies de commutation, pour acheminer l'information au sein de réseau MPLS.



Fonctionnement de MPLS

La notion de FEC :

La mise en oeuvre de MPLS repose sur la détermination de caractéristiques communes à un ensemble de paquets et dont dépendra l'acheminement de ces derniers, cette notion de caractéristique commune est appelée FEC, elle est fondamentale pour comprendre la puissance et la souplesse des réseau MPLS. En réalité c'est une notion utilisée depuis longtemps de manière implicite en routage traditionnel, la décision d'acheminement est prise indépendamment par chaque routeur que le paquet traverse pour rejoindre sa destination, En effet, chaque routeur analyse l'en-tête du paquet et la meilleure route déterminée par l'algorithme de routage ; en d'autres termes, il choisit indépendamment le prochain saut, en se fondant sur l'analyse de l'en-tête de paquet et la meilleure route déterminée par l'algorithme de routage. On peut résumer le comportement d'un routeur aux deux fonctions distinctes :

- Regroupement de l'ensemble de paquets vers une même destination (c à d, possédants le même préfixe dans une FEC).
- Assignation à chaque FEC d'un routeur suivant (interface de sortie).

Définition d'une FEC : Une FEC est la représentation d'un ensemble de paquets qui partagent les mêmes caractéristiques pour leur transport. Contrairement au routage traditionnel qui suppose que cette caractéristique est liée aux adresses des réseaux de destination (et donc au préfixe d'adresse

MPLS permet de constituer des FECs selon de nombreux critères : même préfixe de destination, paquets issus d'un même préfixe d'adresses sources, paquets d'une même application, qualité de service demandée, etc. à la différence du routage traditionnel, l'assignation des paquets à une FEC a lieu juste une fois à l'entrée du réseau.

4.3.2 Principe général de MPLS :

Il correspond aux étapes suivantes :

1. dés son entrée sur le réseau MPLS, un paquet est affecté à une FEC selon différents critères.
2. La FEC à laquelle est assigné le paquet est encodée par chaque routeur en une valeur courte de longueur fixe, appelée LABEL et qui est incluse dans le paquet.

3. Dans les sauts suivants (routeurs suivant), il n'y a plus d'analyser sur l'en-tête du paquet IP, mais l'acheminement réaliser grâce au label.
4. le label est associé localement (sur chaque nœud du réseau) à une FEC déterminer.

4.3.3 Fonctionnement de MPLS : La prise en compte d'un paquet au travers d'un domaine MPLS indique les étapes suivantes :

1- Création des labels et distribution ;

2- Création des tables de Forwarding de labels sur les routeurs ;

3- Acheminement de paquets.

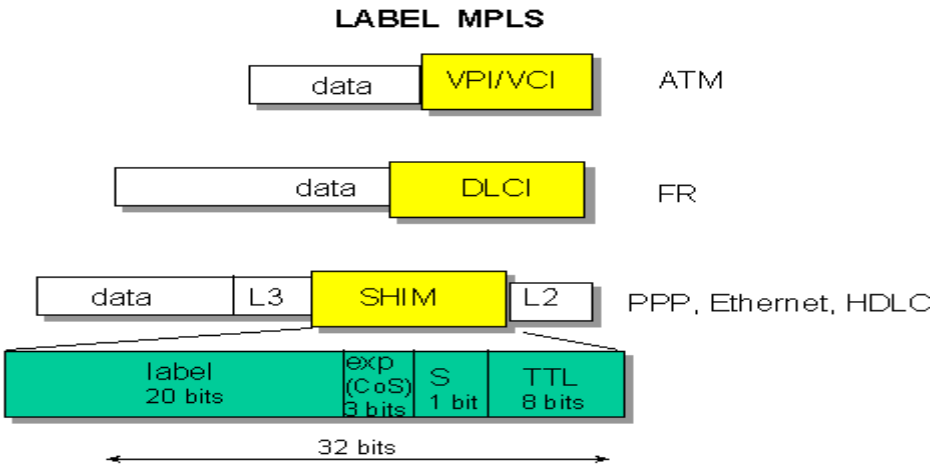
4.3.4 Composants de MPLS :

1- Label switch router (LSR) : C'est un équipement de type routeur ou commutateur, capable de commuter des paquets ou des cellules en fonction des labels qu'il contient. Dans le cœur de réseau les LSR lisent uniquement les labels et non les adresses des protocoles de niveau supérieur (adresse IP).

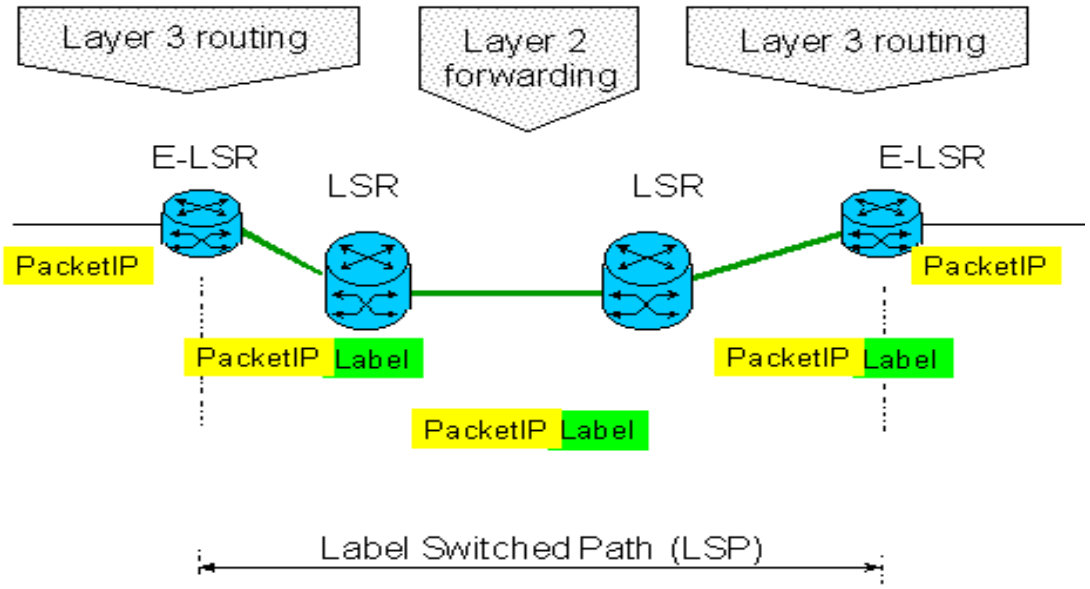
2- Label edge router (LER) : c'est un routeur situé à la frontière des réseaux MPLS, également appelé routeur d'extrémités. les (LER) jouent un rôle important des assignations et la suppression des labels au moment où les paquets entrent sur le réseau ou en sortant.

3- Label : Un label a une signification locale entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et la LSR aval. A chaque bond le long du LSP, un label est utilisé pour chercher les informations de routage (next hop, lien de sortie, encapsulation, queueing et scheduling) et les actions à réaliser sur le label : insérer, changer ou retirer. La figure ci dessous, décrit la mise en œuvre des labels dans les différentes technologies ATM, Frame Relay, PPP, Ethernet et HDLC. Pour les réseaux Ethernet, un champ appelé shim a été introduit entre la couche 2 et la couche 3. Sur 32

bits, il a une signification d'identificateur local d'une FEC. 20 bits contiennent le label, un champ de 3 bits appelé Classe of Service (CoS) sert actuellement pour la QoS, un bit S pour indiquer s'il y a empilement de labels et un dernier champ, le TTL sur 8 bits (même signification que pour IP). L'empilement des labels permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversé du réseau MPLS.



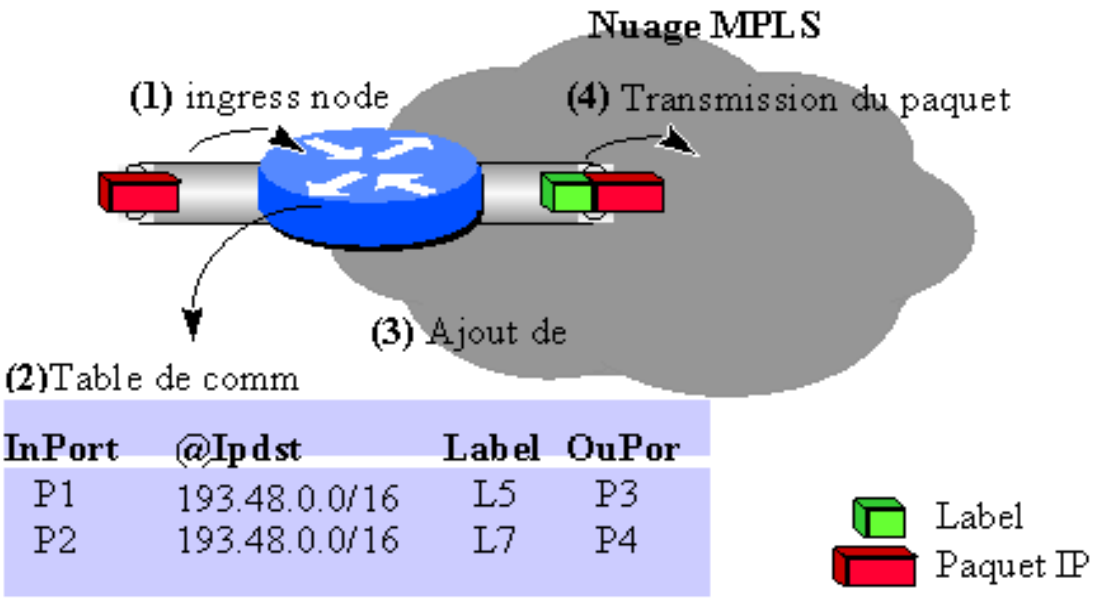
4- Label Switching Path (LSP) : c'est le chemin défini entre le LSR d'entrée sur le réseau MPLS (Ingress switch) et le LSR de sortie du réseau (Egress switch). Un LSP est constitué par la succession de labels assignés entres extrémités. Un LSP soit dynamique soit statique, les LSPs dynamiques sont réservé automatiquement en utilisant des informations de routage. Les LSPs statiques sont positionnées de manière explicite.



5- Label Distribution Protocol (LDP) : Ce protocole distribue les labels et leur signification entre LSRs. Il assigne les labels dans les équipements situés à la périphérie ou dans le cœur de réseau MPLS. A cet effet il tient compte des protocoles de routage de niveau supérieur.

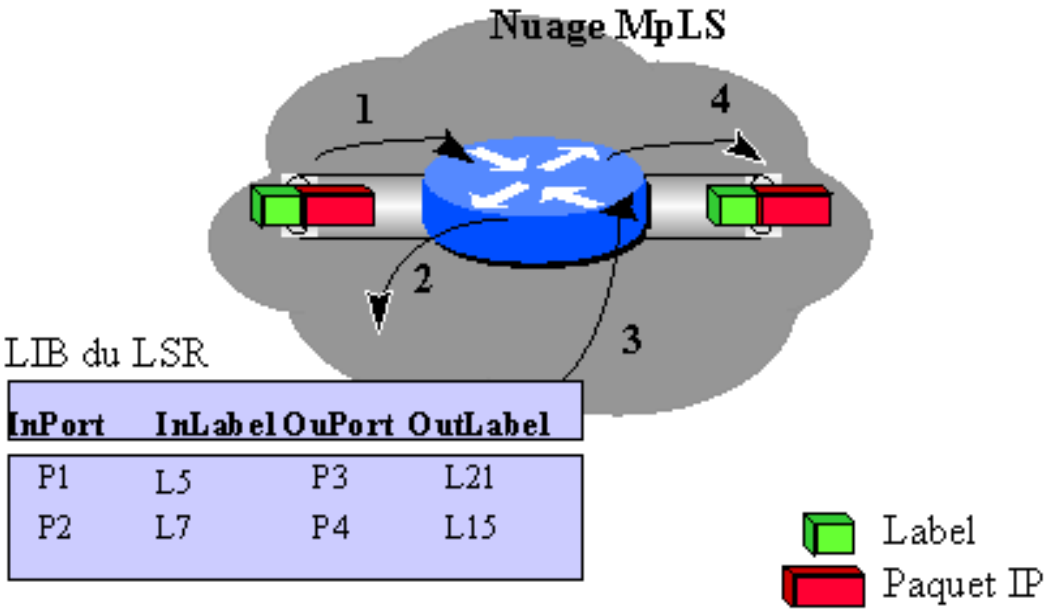
4.3.5 Commutation de labels :

Lorsqu'un paquet arrive dans un réseau MPLS **(1).** En fonction de la FEC auquelle appartient le paquet, l'ingress *node* consulte sa table de commutation **(2)** et affecte un label au paquet **(3)**, et le transmet au LSR suivant **(4)**.



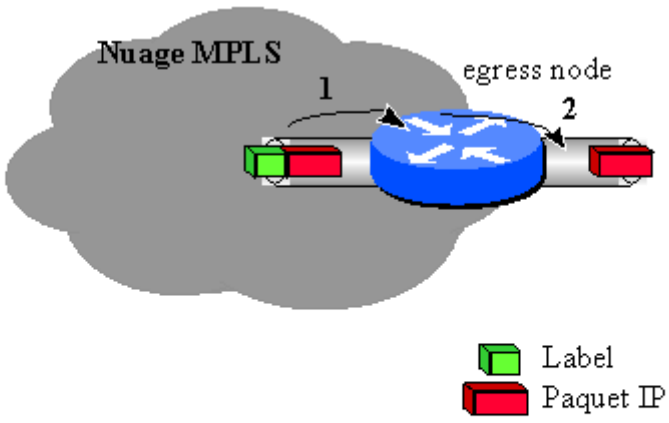
1 - Le paquet IP arrive sur l' ingress node
2 - Le protocole de routage IP détermine, à partir de l'adresse IP de l'eggress node, la FEC, le label et le port de sortie.
3 - Ajout de l'en-tête
4 - Paquet IP + Label envoyé vers le noeud suivant

Lorsque le paquet MPLS arrive sur un *LSR* **[1]** interne du nuage MPLS, le protocole de routage fonctionnant sur cet équipement détermine dans la base de données des labels LIB (Label Base Information), le prochain label à appliquer à ce paquet pour qu'il parvienne jusqu'à sa destination **[2]**. L'équipement procède ensuite à une mise à jour de l'en-tête MPLS (swapping du label et mise à jour du champ TTL, du bit S) **[3]**, avant de l'envoyer au noeud suivant (*LSR* ou *l'egress node)* **[4]**. Il faut bien noter que sur un *LSR interne*, le protocole de routage de la couche réseau n'est jamais sollicité.



1 - Paquet IP + Label arrive sur le LSR
2 - Protocole de routage détermine, à partir de la LIB le next hop LSR ou E-LSR
3 - Mise à jour du label MPLS
4 - Paquet IP + Label envoyé vers le noeud suivant

Enfin, une fois que le paquet MPLS arrive à l'*egress node* **[1]**, l'équipement lui retire toute trace MPLS **[2]** et le transmet à la couche réseau.



1 - Paquet IP + label arrive sur l'egress node
2 - Retrait du label et transmission du paquet IP à la couche réseau

4.3.6 Modes de création des labels :

Plusieurs méthodes sont utilisées pour la création des labels, en fonction des objectifs recherchés, par exemples :

a-Fondée sur la topologie (topology-based) : cette méthode engendre la création des labels à l'issue de l'exécution normale de processus de routage.

b-Fondée sur les requêtes (request-based) : cette méthode de création des labels est déclenchée lors de l'exécution d'une requête de signalisation (trafic de contrôle), comme RSVP.

c-Fondée sur le trafic (trafic-based) : cette méthode de création de labels attend la réception d'un paquet de données pour déclencher l'assignation et la distribution des labels.

4.3.7 Les protocoles de distribution des labels :

MPLS permet de mettre en œuvre plusieurs protocoles de distribution des labels, en fonction des objectifs visés.

Voici les protocoles de distribution des labels envisagés :

1- LDP : Protocole crée spécifiquement.

2- BGP : Amélioration de BGP pour la distribution des labels.

3- PIM : Amélioration de PIM pour la distribution des labels.

4- RSVP : Amélioration de PIM pour la distribution des labels.

5- CR-LDP : Protocole spécifique.

LES trois premiers approches à assigner les labels selon le travail d'un protocole de routage fondée sur la topologie et qui :

- Développe un protocole de distribution de labels spécifique (LDP) ;
- Améliore un protocole de routage unicast existant pour assurer la distribution de labels (BGP) ;
- Améliore un protocole de routage multicast pour assurer la distribution de labels (PIM) pour des connexions multicast.

Les deux dernières solutions consistent à assigner des labels non plus se référant au protocole de routage, mais en désignant explicitement une route (routage à la source) , c'est une approche fondée sur les requêtes et qui

- Améliore un protocole qui existe (RSVP) qui n'est pas un protocole de routage, mais un protocole de signalisation ;
- Développe un nouveau protocole (CR-LDP).

4.3.8 Le protocole LDP :

4.3.8.1 Caractéristiques générales du protocole :

Le protocole LDP fonctionne entre homologues (peers), par le biais de l'échange de messages, préalablement à l'échange de messages, il est nécessaire de découvrir les homologues et d'établir une session avec ses voisins, LDP est indépendant de tout protocole de routage, car il exploite directement la table de routage que génère ce dernier. Comme tout protocole de distribution de labels, LDP pour assigner des labels à des FECs et les destiner.

Dans le cas de LDP, une FEC est définie comme une information de la couche réseau IP, ce qui signifie q'une FEC équivaut à un numéro de réseau IP.

4.3.8.2 Messages LDP :

- **messages de découverte :** ils servent à découvrir de nouveau homologues et les maintenir, à cet effet. Des paquets **HellO** sont émis vers l'ensemble des routeurs MPLS sur une adresse multicast, à l'aide du protocole UDP.
- **Messages de session :** dés q'un voisin est découvert, une session LDP est ouverte sur TCP, les messages de session servent à établir, maintenir, et clôturer les sessions LDP.
- **Messages d'avertissement** : ces sont ces messages qui servent à créer, modifier, et supprimer les assignations de labels.
- **Messages de notification** : Ces messages servent à signaler les éventuelles erreurs.

4.3.8.3 Espace de labels :

Les labels utilisés par un LSR pour l'assignation de labels à une FEC sont définis de deux façons :

- **Par plate-forme :** dans ce cas, les valeurs de labels sont uniques dans tout l'équipement LSR LES labels sont alloués depuis un ensemble commun de labels.
- **Par interface :** les domaines de valeurs des labels sont associés à une interface. Plusieurs peuvent être définis. Dans ce cas les valeurs de labels fournies sur des interfaces différentes peuvent être identiques.

Un LSR peut utiliser une assignation de label par interface, à la condition expresse qu'il soit en mesure de distinguer l'interface depuis laquelle arrive le paquet.

4.3.8.4 Contrôle du mode de distribution des labels :

LDP définit deux modes de contrôle de distribution des labels aux LSR voisins :

-Indépendant : dans ce mode, un LSR peut diffuser un label à n'importe quel moment. Ainsi, un LSR peut diffuser un label à une FEC, quand bien même il n'est pas prêt à commuter sur ce label. Dans ce mode, une FEC est reconnue et prise en compte chaque fois que le routeur avise de nouvelles routes.

- Ordonné : Dans ce mode, un LSR associe un label à une FEC particulière, s'il s'agit du routeur de sortie de réseau (Egress router) ou si l'assignation a été reçue du LSR au saut suivant.

4.3.8.5 Conservation des labels :

LDP définit la façon dont les LSR conservent les labels reçus. Deux options sont possibles :

- **Modèle de conservation libéral :** dans ce mode les LSR conservent les labels reçus de tous leurs voisins. Il permet une convergence plus rapide face aux modifications

topologiques du réseau et la commutation de trafics vers d'autre LSP en cas de changement ;

- **Mode de conservation conservateur :** ici, les LSR retiennent uniquement les labels des voisins situés sur le saut suivant et ignorent tous les autres.

4.3.8.6 Fusion des labels (ou agrégation) : LDP est capable d'agréger des trafics. Ainsi, des trafics issus d'interfaces différents d'un SLR peuvent être fusionné en tout point du réseau et être acheminés grâce au même label, s'ils traversent le réseau vers un même destination.

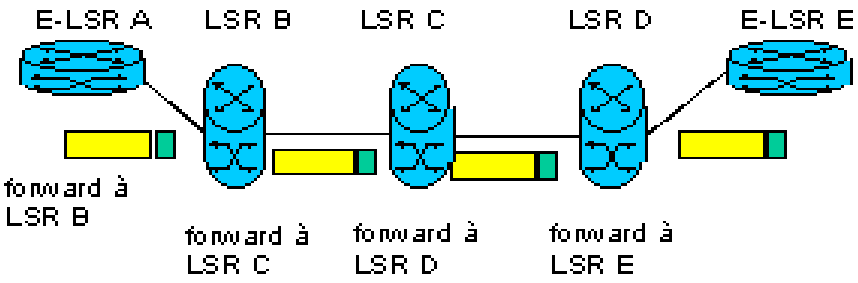
4.3.8.7 Détection et prévention des boucles :

Sur le réseau IP, le champ TTL de l'en-tête IP évite au paquet IP de voyager indéfiniment sur le réseau. Ainsi, la valeur du champ TTL est décrémentée à chaque saut de routeur, et lorsque cette valeur est égale à 0, le paquet est ignoré. MPLS peut utiliser ce mécanisme, mais pas sur tous les réseaux sur lesquels il peut être déployé. Lors de la mise en œuvre de MPLS sur des liens PPP ou LAN, le champ TTL du label est utilisé de la même manière que le champ TTL du paquet IP. Mieux à l'entrée du domaine MPLS, le champ TTL de la trame IP sera généralement recopié dans le champ TTL du label par le LSR d'entrée, et le LSR de sortie recopiera de la méme façon la copie du champ TTL du label du paquet IP. Au sien du réseau MPLS, la valeur du champ TTL du label sera décrémentée à chaque saut de LSR.

4.3.9 Routage implicite dans un réseau MPLS :

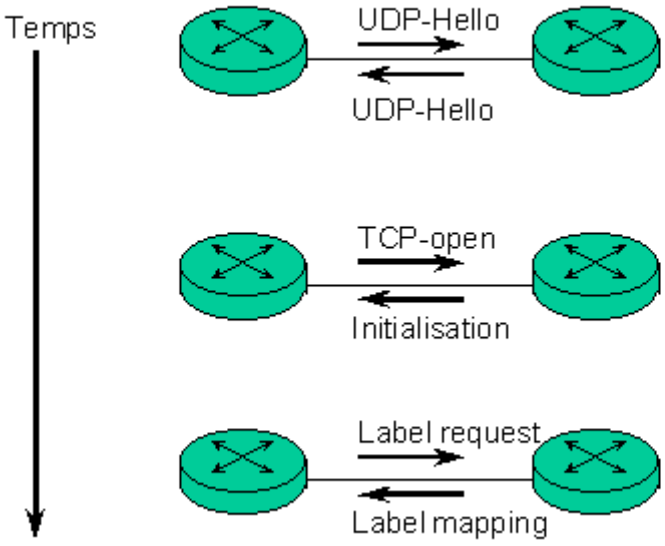
La distribution implicite de labels aux LSR est réalisée grâce au protocole LDP (Label Distribution Protocol). LDP définit une suite de procédures et de messages utilisés par les LSR pour s'informer mutuellement du mapping entre les labels et le flux. Les labels sont spécifiés selon le chemin " Hop By Hop " dans le réseau. Chaque noeud doit donc mettre en œuvre un protocole de routage de niveau 3, et les décisions de routage sont prises indépendamment les unes des autres.

IMPLICIT ROUTING: LSP HOP BY HOP



LDP est bidirectionnel et permet la découverte dynamique des noeuds adjacents grâce à des messages Hello échangés par UDP. Une fois que les 2 noeuds se sont découverts, ils établissent une session TCP qui agit comme un mécanisme de transport fiable des messages d'établissement de session TCP, des messages d'annonce de labels et des messages de notification.

ETABLISSEMENT D'UNE CONNEXION LDP



LDP supporte les spécifications suivantes :

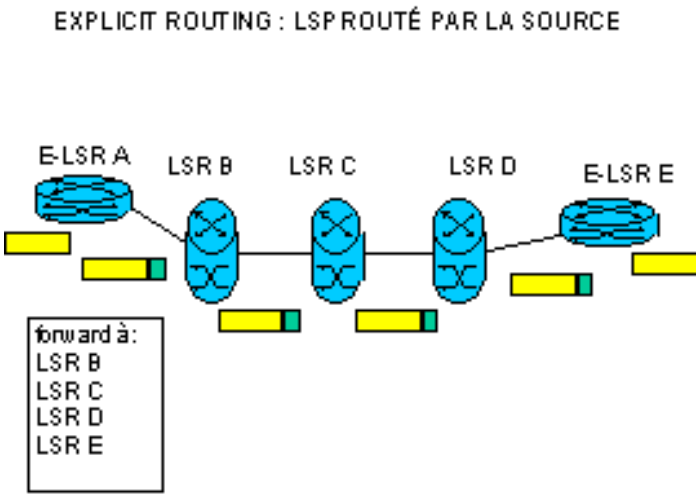
- Les labels sont assignés à un noeud amont à partir des informations contenues dans la table de routage:

- 3 FEC (Forwarding Equivalent Classes) sont définies : il est possible de mapper un label soit à un flux de trafic, à un préfixe d'adresse IP ou à un router-ID. Le flux de trafic reçoit le même traitement de forwarding selon le label qui lui est associé.
- Une connexion LDP peut être établie entre 2 LSR directement ou indirectement connectés
- Il existe 2 modes de rétention de label : soit " conservatif " soit " libéral ". Pour le mode de rétention " conservatif », seul le label correspondant au meilleur bond est retenu. Par contre, pour le mode de rétention " libéral ", tous les labels transmis par les LSR adjacents pour un flux donné sont retenus. Ce mode permet un reroutage rapide en cas de problème car des labels alternatifs sont disponibles instantanément.

4.3.10 Routage explicite dans un réseau MPLS :

Le routage explicite est la solution MPLS pour faire du Traffic Engineering dont l'objectif est le suivant :

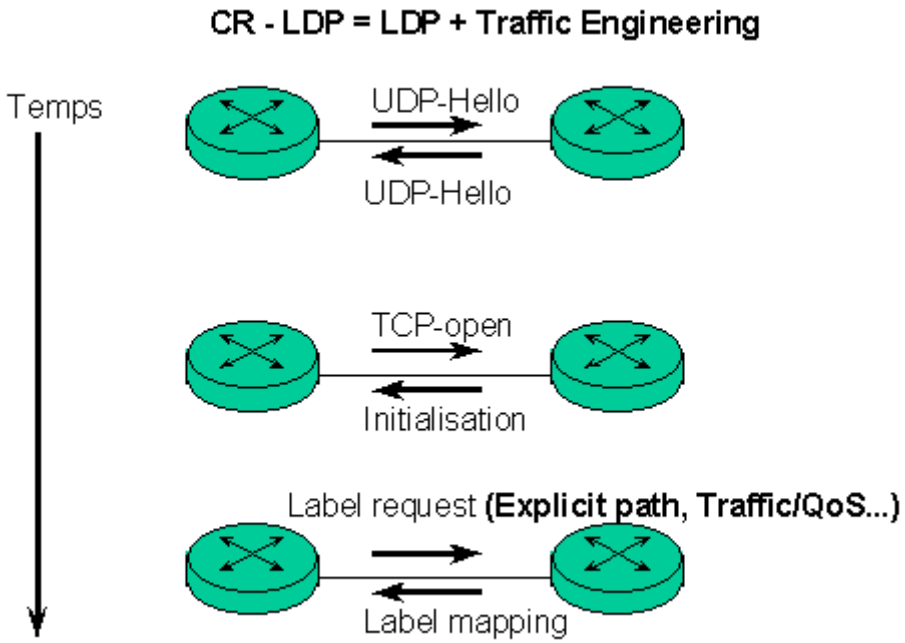
- Utiliser efficacement des ressources du réseau
- Eviter les points de forte congestion en répartissant le trafic sur l'ensemble du réseau.



Le routage explicite permet à un opérateur de faire du *Traffic Engineering* en imposant au réseau des contraintes sur les flux, du point source jusqu'au point destination. Ainsi, des routes autres

que le plus court chemin peuvent être utilisées. Le réseau détermine lui-même le chemin en suivant les étapes ci-dessous :

- Connaissance de l'état du réseau : topologie, bande passante réelle d'un lien, bande passante utilisée, bande passante restante
- Calcul d'un chemin répondant aux contraintes spécifiées.
- Etablissement du ER-LSP (*Explicitly Routed Path*). La source connaît le chemin complet de l'ingress node à l'egress node et c'est elle qui spécifie les LSR à l'intérieur du LSP. Deux options de signalisation spécifiées pour l'établissement du LSP : RSVP ou CR-LDP (*Constraint-Based Routing LDP*) :
- CR-LDP est l'alternative à RSVP; il est jugé plus fiable dans la mesure où il met en oeuvre TCP (orienté connexion). De plus, CR-LDP peut interfonctionner avec LDP et utilise les messages LDP pour signaler les différentes contraintes. Les fonctions de CR-LDP sont réalisées par des instructions matérielles (asics) ne nécessitant pas de fréquents rafraîchissements, contrairement à RSVP dont les fonctions sont réalisées par le logiciel nécessitant de fréquents messages de rafraîchissement.
- envoi du trafic sur le chemin trouvé
- supervision de l'état des LSP et le transmet à l'IGP
- ré-optimisation des LSP quand nécessaire



Les fonctions supportées par ER-LDP sont :

- ER-LSP de bout en bout.
- *strict/loose explicit routing* : dans un LSP routé de manière " stricte ", chaque bond est spécifié. Une section du LSP peut être routée de manière " imprécise " lorsque sont introduits 2 LSR non directement connectés.
- spécification d'une classe de service.
- réservation de bande passante.
- *route pinning* : dans une section de ER-LSP routée de manière " imprécise ", les bonds sont sélectionnés selon une transmission bond par bond.
- *ER-LSP preemption* : établissement/maintien de priorité.

4.3.11 Applications de MPLS [21]

Les applications les plus courantes du MPLS sont les suivantes :

1- L'ingénierie de trafic est activée par des mécanismes MPLS permettant de diriger le trafic via un chemin spécifique, qui n'est pas nécessairement le chemin le moins coûteux. Les

administrateurs de réseau peuvent mettre en oeuvre des politiques visant à assurer une distribution optimale du trafic et à améliorer l'utilisation globale du réseau.

2- La bande passante garantie constitue une amélioration à forte valeur ajoutée par rapport aux mécanismes d'ingénierie de trafic traditionnels. MPLS permet aux fournisseurs de services d'allouer des largeurs de bande passante et des canaux garantis. La bande passante garantie permet également la comptabilité des ressources QoS (qualité de service) de manière à organiser le trafic 'prioritaire' et 'au mieux', tels que la voix et les données.

3- Le reroutage rapide permet une reprise très rapide après la défaillance d'une liaison ou d'un noeud. Une telle rapidité de reprise empêche l'interruption des applications utilisateur ainsi que toute perte de données.

4- Les réseaux privés virtuels MPLS simplifient considérablement le déploiement des services par rapport aux VPN IP traditionnels. Lorsque le nombre de routes et de clients augmente, les VPN MPLS peuvent facilement monter en charge, tout en offrant le même niveau de confidentialité que les technologies de niveau 2. Ils peuvent également transporter des adresses IP non-uniques à travers un domaine public.

5- La fonction Classe de service (CoS) MPLS assure que le trafic important est traité avec la priorité adéquate sur le réseau et que les exigences de latence sont respectées. Les mécanismes de qualité de service IP peuvent être mis en oeuvre de façon transparente dans un environnement MPLS.

5. Interopérabilité des modèles IntServ, DiffServ et MPLS :[21]

Dans les sections précédentes nous avons présenté séparément les différents modèles de QoS. Maintenant en va voir les interactions entre ces différents modèles de QoS. NOUS

allons nous intéresser aux cas les plus fréquemment rencontrés, qui, s'ils ne correspondent pas forcément tous un standard de l'IETF (c'est-à-dire une RFC), en sont au minimum à l'état de spécification provisoire (draft). Nous allons successivement aborder les cas suivants :

- Adaptation d'IntServ sur DiffServ.
- MPLS pour RSVP.
- MPLS pour DiffServ.

5.1 IntServ sur DiffServ : cette adaptation est née du constat que le modèle IntServ ne peut se déployer à grande échelle. En effet. Le protocole RSVP requiert un traitement par paquet, au niveau de l'ensemble des routeurs du réseaux DiffServ, et le maintien d'informations d'état pour chaque session RSVP, sur tous les routeur. Le traitement par paquet repose principalement sur la classification multichamp, qui nécessite une capacité de traitement importante de la part de routeurs. Le maintien d'information d'état est caractérisé par la prise en compte des nombreux messages PATH et RSVP, qui doit être rafraîchit périodiquement, et par la mémorisation dans les routeurs.

La principale piste utilisée consiste à agréger les sessions RSVP qui partagent des sections communes du réseau, afin de réduire la charge de classification et de signalisation.

C'est également dans ce sens que l'adaptation IntServ sur DiffServ a été réalisée. L'idée de cette approche consiste à prendre en compte un cœur de réseau fondé sur DiffServ, ce dernier offrant des caractéristiques de QoS limitées à une périphérie de réseau en IntServ. Cela revient à considérer, dans l'architecture IntServ, le réseau DiffServ comme un élément réseau (NE) de type lien, qui offre des caractéristique particulières de QoS.

5.2 MPLS pour RSVP (IntServ) : Il est tout à fois possible d'imaginer un fonctionnement où l'assignation de labels serait réalisée d'après l'objet Flow-Spec, précisant la QoS attendue.

Toutefois, chaque flux RSVP ne sera pas attribué à un label spécifique. Un ensemble de flux RSVP possédant des caractéristiques voisines se verront assigner un même label. On dit alors que la QoS est agrégée. L'utilisation de MPLS permet une simplification par rapport à RSVP. En effet dans le modèle IntServ/DiffServ. Chaque routeur doit procéder à une classification complexe (multichamp) des paquets, pour les assigner à un flux permettant alors d'appliquer une QoS particulière.

Dans le pratique, le label assigné pourra être la résultante d'une même destination et d'un ensemble possédant des caractéristiques de QoS voisins.

5.3 MPLS pour DiffServ : DiffServ, tout comme MPLS, procède à une agrégation des demandes de QoS en fournissant des valeurs discrètes de DSCP pour des flux possédant des caractéristiques de QoS voisins.

La mise en correspondance des services DiffServ et de MPLS consiste à associer à chaque classe DiffServ un LSP-MPLS distinct, doté de caractéristiques de QoS équivalentes.

La correspondance MPLS/DiffServ ne pose pas de problèmes techniques particuliers. En revanche, il est nécessaire de savoir ce qui a réellement été mis en œuvre dans le cas d'un opérateur particulier. Il faut notamment déterminer si l'opérateur fait confiance à la valeur du DSCP par le client pour obtenir un LSP particulier.

6. Gestion et administration de la QoS :[21][11].[7]

L'administration de la **QoS** exige des modèles complexes de gestion de politiques. Les **actions** sont toujours prises comme conséquence d'une **condition** présente dans le réseau. Ces conditions peuvent être reliées à des phénomènes variés : un changement des conditions de charge des liens, une tombée des liens, un nouveau service configuré qu'il faut implémenter

dans le réseau, etc. L'ensemble des conditions et ses actions associées sont les politiques. Par exemple, une politique peut être exprimé comme suit :*" Tous les jours, de 3 : 00 heure à 5 : 00 heure, le département de marketing aura un service additionnel d'accès à la base de donnés externe, en utilisant 30 connections maximum de 250 Kbps chacune "* Cet ensemble de conditions et actions est simple à énoncer, mais complexe à mettre en œuvre dans le réseau. Il est en effet nécessaire de considérer des configurations d'authentification, comptabilité, et ingénierie de trafic en même temps. Ceci est encore plus complexe si les conditions et les actions changent avec une échelle de temps plus courte, comme par exemple des changements topologiques qui peuvent empêcher le respect des **accords de services** (SLAs).

6.1 Les règles de QoS (QoS policies) :

La qualité de service au sein d'un réseau revient à regrouper les paquets d'un flux d'application dans une certaine classe de trafic Cette classification a pour objet d'accorder à ces paquets un traitement plus ou moins prioritaire par rapport à d'autres paquets. Ainsi certains utilisateurs recevront un meilleur service que d'autres. il est alors inévitable que les utilisateurs cherchent à obtenir le meilleur service sans en payer le prix ou sans y être autorisé. On conçoit donc qu'il est nécessaire de disposer de certains mécanismes sur le réseau afin de mettre en œuvre des règles de gestion des trafics, faisant appel à une architecture, un certain nombre de protocoles et modèles de représentation de données

6.2 Définition d'une politique de QoS :

Une politique de QoS est un ensemble de règles associées à certains services. Les règles définissent les critères à satisfaire pour obtenir ces services, elles sont définies en fonction de conditions et d'actions.

Exemple : les flux de trafic issus d'une application X doivent être prioritaires par rapport à d'autres flux .Dans ce cas la condition est : « si les flux de trafic sont des flux X » et l'action est « assignation de la haute priorité à ces flux ».

6.3 Structure et architecture d'une politique de QoS

Le groupe de travail RAP (RSVP Admision Policy) de l'IETF a défini un modèle pour gérer le contrôle des règles de QoS associées à RSVP et le modèle INTSERV qu'il représente, ce modèle décrit dans RFC 2753 a été repris pour s'appliquer à l'ensemble des technologies de QoS.

Ce modèle identifie deux composants principaux :

PEP (Policy Enforcement Point) :C'est le point d'application de la politique .il joue le rôle du policier

PDP (Policy Decision Point) :il constitue l'organe de décisions d'applications des règles .Il joue le rôle du juge.

Le PEP reçoit un message de demande de ressources qui nécessite une décision d'application d'une politique. PEP l'envoie au PDP. Le PDP retourne sa décision et le PEP l'applique en acceptant ou en refusant la demande d'allocation de ressources du message RSVP.

Cette architecture recourt principalement au protocole COPS (Common Open Policy service) qui permet l'échange d'informations entre le PDP et les PEP ,il est décrit dans la RFC 2748

COPS se caractérise par les éléments suivants :

- Il est de type client/serveur entre le serveur PDP et les clients PEP
- Il fournit une sécurisation des messages
- Il est fondé sur le protocole TCP
- Il prend en charge plusieurs types de clients

7. Outils de mesure de QoS [21].[14]

Mesurer la Qualité de Service revient à mesurer les performances du réseau. Les critères généralement utilisés tels que la disponibilité, le délai, la gigue, et le taux de pertes de paquets sont difficiles à mesurer, du fait du caractère aléatoire des pertes de paquets et du temps indéterminé passé dans les files d'attente sur tous les routeurs qui constituent le chemin entre une source et une destination. Pour établir une vérification de la QoS ou pouvoir comparer les QoS fournies par différents réseaux, il faut pouvoir comparer ces observations.

Dans cette optique, le groupe de travail IPPM de l'IETF a défini préalablement une structure formelle de méthodologie des mesures (RFC2330). Pour mesurer les performances, deux types de méthode existent:

1. la méthode active qui consiste à injecter du trafic dans le réseau de manière contrôlée et à analyser les paquets retournés

   Outils : PING, TRACEROUTE

   L'inconvénient de ces outils est de fausser les résultats, en introduisant du trafic supplémentaire pouvant influencer les métriques de la Qualité de service qu'on souhaite précisément mesurer.

2. la méthode passive qui consiste à observer et analyser les paquets reçus sur un système terminal

   Outil : NetraMet, outil développé par le groupe de travail RTFM de l'IETF et distribué comme logiciel du domaine public, permet d'analyser le trafic de manière passive.

8. Les champs d'application de QoS :

Le champ d'application de technologies de QoS est toutefois encore limité dans les entreprises et chez les opérateurs, certes, certains font exception, mais il serait erroné de croire que toutes les technologies présentées dans cet exposé sont largement utilisées à ce jour.

Les applications qui utilisent la QoS disponible sur les réseaux sont les deux cas suivants :

- application ne sachant pas signaler ses besoins de QoS au réseau : les plus parts des applications actuelles correspondent à ce cas. Il est nécessaire qu'un élément du réseau effectue la classification des applications ;
- application sachant signaler ses besoins de QoS au réseau : les nouvelles applications multimédias ont été développées pour tirer parti des nouvelles interfaces de développement (Winsock 2 notamment). Ces interfaces sont en mesure de signaler au réseau les demandes de QoS de l'application.

Parmi les applications, en peux généralement distinguer plusieurs niveaux de besoins :

1- les applications temps réel, qui vont nécessiter une QoS rigoureuse.
2- Les applications critiques de l'entreprise : applications de types ERP qui requièrent un traitement préférentiel.
3- Les autres applications, qui vont se satisfaire d'un niveau de service standard, encore appelé service en best effort.

Généralement, seules les applications du cas N°1 ont été développées avec le souci de signalisation des besoins de QoS. Les applications des cas N°2 et N°3 ne sont en principe pas en mesure de signaler leurs besoins.

9. Conclusion :

Comme nous venons de le voir, la Qualité de Service dans l'Internet est encore un vaste chantier, à tel point qu'il est difficile d'en faire la synthèse!

L'aspect best effort de l'Internet, a montré ses limites face aux nouveaux besoins (voix, vidéo, etc..) c'est pour ça il y a Aujourd'hui de multiples groupes de travail de l'IETF qui travaillent dans des domaines touchant la Qualité de Service et des nombreux travaux de normalisation sont encore en cours. Certains tiennent compte de nouveaux développements dans les réseaux tels que les modèles IntServ, DiffServ et MPLS, tandis que d'autres se focalisent sur les politiques de contrôle dans les réseaux ou la définition de nouveaux protocoles de routage. Tous ces travaux sont néanmoins étroitement imbriqués et permettent de construire progressivement les morceaux du puzzle QoS adapté à l'Internet.

Plusieurs alternatives existent aujourd'hui. Cependant, parallèlement au modèle de réservation de ressources et de services intégrés posant des problèmes de déploiement à large échelle, il semble que les efforts s'orientent maintenant vers l'allocation prioritaire de ressources permettant de créer des distinctions de classes au sein du service "best-effort". Ce type de modèle étudié actuellement au sein du groupe diffserv ("Differentiated Services") repose essentiellement sur un champ dans l'en-tête du paquet IP, de telle sorte que les mécanismes de mise en file d'attente et de rejet des paquets puissent être mis en oeuvre sur chaque noeud intermédiaire.

L'implémentation de tels algorithmes ajoutée au déploiement d'architectures adéquates (offrant un service prévisible, stable et cohérent) pourront offrir à terme des niveaux de services différenciés tout en offrant une bonne stabilité.

Il est évident que les technologies de QoS se développeront encore plus rapidement sur les réseaux, s'il existe davantage d'applications pour en tirer parti. De même, de nouvelles applications ne serons développées qu(à condition que les mécanismes de QoS soit Disponibles.

Service QoS = Mécanismes de QoS + Processus de gestion

10. BIBLIOGRAPHIE :

[1]- Eric Gressier-Soudan « Introduction à la problématique des Réseaux avec QoS » Janvier 2002

[2]- Timur FRIEDMAN « La Qualité de Service dans la conception des réseaux » février 2003

[3]- Laurent Toutain, Jean Marie Bonnin, Octavio Medina « La qualité de service dans l'Internet »

[4]- Weibin Zhao, David Olshefski and Henning Schulzrinne “Internet Quality of Service:: an Overview” Columbia University

[5]- Sylvain FRANCOIS Anne-Lise RENARD Jérémy ROVARIS « Etude du service DiffServ »

[6]- Koubâa Anis « Qualité de Service Dans l ’Internet »

[7]- JEAN-YVES LE BOUDEC “Quality of Service in the Internet”

October 23, 2003

[8]- Eric Horlait Nicolas Rouhana « Qualité de service dans l’architecture TCP/IP »

[9]- Lila boukhatem « La qualité de service et IP » Septembre 2003

[10]- « QoS sur IP et protocole diffserv »

[11]- « RSVP: The ReSerVation Protoco” March 19, 1998 Gordon Chaffee Berkeley Multimedia Research Center University of California, Berkeley

[12]- “Providing quality of service in the internet” By Xipeng Xiao

[13]- « La gestion de la qualité de service dans les réseaux d'entreprise » juin 2003

[14]- Claudine Chassagne « Qualité de Service dans l'Internet » CNRS-UREC Août 1998

[15]- Laurent Toutain, Octavio Medina, Jean Marie Bonnin « La qualité de service dans l'Internet »

[16]- Benoît Christophe Nuno Morgado Gonçalves Jérôme Rauch « Intégration de la qualité de services, à travers un réseau »
[17]-« Quality of Service:for Multimedia Internet Broadcasting Applications"

[18]- « IntServ, DiffServ et les flux Multimédia »Octavio Medina février 2000

[19]- *Geoff Huston* « Quality of Service in the Internet:"
[20]- Algorithmes d'attribution de priorités dans un Internet à Différentiation de Services Octavio Medina mars 2001

[21]- J.L Melin Qualité de service sur IP ,Ed.Eyrolles,2001