# Support de QoS pour les Applications Multimédias sur LAN Partagé par Différenciation de Services[1]

B. Nassereddine* P. Anelli**. E. Horlait** A .Benkiran*

*Laboratoire des Réseaux Informatiques et Multimédias (RIM) Ecole Mohammadia d'Ingénieurs, Rabat Maroc

** Laboratoire d'Informatique de Paris 6 (LIP6), Université Pierre et Marie Curie Paris 6, Paris France

## Abstract

In order to meet the needs of applications QoS, Differentiated Services architecture is proposed. A service is the combination of condition policy and a per hop behaviour. The whole being localised in the router. This architecture assumes that between the host (the final user) and the router, the links are well-provisioned and that they are able to cover the different streams without congestion. This can be done easily in the case of point to point links. In the case of multiple access and broadcast network like IEEE 802.x LAN, this assumption is no longer true.

This document proposes a bandwidth manager able to share out fairly and efficiently the bandwidth between the different streams in order to support a QoS manager using differentiated services. The proposed manager is based on a distributed algorithm using a token technique to carry out the bandwidth access control and a sequencing techniques to manage differents streams inside the same node . This algorithm is based also on a state exchange protocol.

## Résumé

Dans l'objectif de répondre aux besoins des applications multimédias en QoS, l'architecture de différenciation de services (Diff-Serv) a été proposée. Elle définit une solution simple fournissant une différenciation de services entre les flots. Un service est la combinaison d'une politique de condition et d'un comportement de relayage. L'ensemble est localisé dans le routeur. Cette architecture suppose que, entre l'hôte (l'utilisateur final) et le routeur, les liens sont suffisamment provisionnés et capables d'acheminer sans perturbation les différents flots. Ceci peut être aisément réalisé dans le cas des liaisons point à point entre le hôte et le routeur. Dans le cas des liaisons multipoints à bande passante partagée, comme les LAN de style IEEE 802.x, cette hypothèse n'est plus vraie.

Dans cet article, nous proposons un gestionnaire de bande passante distribué qui répartit équitablement et efficacement la bande passante entre les différents flots. Ainsi il est l'élément pour un support à une gestion de QoS par différenciation de services. Le gestionnaire proposé s'appuie sur un algorithme distribué. Il utilise une technique de jetons pour effectuer le contrôle d'accès à la bande passante et une technique d'ordonnancement pour gérer les flots concurrents au sein d'un même nœud. Cet algorithme utilise également un protocole d'échange d'état.

**Mots Clés :** Diff-Serv, Int-Serv, QoS, Bandwidth management, LAN, PHB, EF, Access control.

## 1. Introduction et problématique.

La différenciation de services est la dernière méthode proposée permettant à Internet de fournir d'autres services de transfert que le traditionnel "service au mieux" (*BE : Best Effort*). Cette demande d'enrichissement de la gamme des services de l'Internet va en s'accroissant. En effet, il est utilisé de plus en plus comme un outil commercial et de moins en moins comme un outil de recherche. Les protocoles de l'Internet subissent de fortes pressions pour offrir des garanties de Qualité de Service (QoS). Ces demandes de garanties proviennent des applications multimédias réparties qui ne se contentent plus du service "au mieux" de l'Internet. Ces applications vont du simple transfert de données à celles plus complexes telles que la téléphonie, la vidéo à la demande ou la conférence multimédia. L'introduction de QoS dans le réseau répond également à des soucis financiers des prestataires de service Internet. Offrir différents niveaux de services QoS est un moyen d'augmenter leur revenu. La QoS au niveau d'un réseau se décline en 4 paramètres : **débit**, **latence**, la **gigue** et la **perte**.

Le débit communément appelé "bande passante" représente la ressource de transmission qu'occupe ou reçoit un flot. La gestion de la bande passante est un élément important pour la garantie de QoS. La latence est définie par le délai de transfert de bout-en-bout d'un paquet d'un flot. Les applications interactives comme la téléphonie ont une latence maximum

[1] Publié à ISIVC'2000, International Symposium on Image/Video Communications over Fixed and Mobile Networks, (http://www.fsr.ac.ma/ISIVC), Rabat, Maroc, 17-20 Avril 2000.

tolérable. Si un paquet subit un retard important, au delà de la valeur tolérable, les données qu'il contient deviennent inutiles pour l'application. Le retard est équivalent pour ces applications à une perte de données. La gigue correspond aux variations de latence des paquets. La cause principale de l'apparition de la gigue dans les flots provient des changements d'intensité de trafic sur les liens de sorties des commutateurs. La perte signifie la perte de paquets. Elle se produit lorsqu'il y a des erreurs d'intégrité sur les données. Dans les réseaux actuels où la qualité des transmissions est très bonne, cette cause est marginale. La perte de paquet se produit principalement lorsque l'intensité du trafic sur les liens de sorties devient supérieure à leur capacité d'écoulement. Elle est une indication de congestion.

Ces quatre paramètres, à priori indépendants, sont en vérité tous concernés par la congestion. En l'absence de congestion, chaque flot peut utiliser le niveau de bande passante qu'il souhaite, aucun paquet n'est perdu, la latence est minimale et la gigue est quasiment nulle. Ces paramètres se dégradent quand la contention sur les ressources augmente. La congestion est si répandue dans l'Internet d'aujourd'hui, qu'aucun des 4 paramètres ne peut être garanti. C'est la raison pour laquelle on qualifie le service rendu de BE : il traite tous les paquets de la même manière quel que soit le service qu'il souhaiterait recevoir. La solution tient donc à la capacité du réseau à isoler les flots pour leur fournir la QoS requise. L'isolation des flots consiste à fournir aux flots demandant une QoS particulière une protection contre les flots perturbateurs et autres trafics BE. Le passé récent a montré qu'il était difficile de déployer une QoS par flot. Le déploiement avec succès du service BE suggère également que la distance pour offrir d'autres services soit faible. Aussi l'IETF a constitué le groupe de travail Diff-Serv en charge de proposer un cadre intermédiaire de QoS qui soit facile à déployer comme du BE tout en offrant une QoS avec une garantie relative. L'architecture pour la différenciation de services (*Diff-Serv*) est définie en détail dans [1] et [2].

## 2. Architecture Diff-Serv

Une des idées de Diff-Serv est d'agréger les flots d'applications dit micro-flot en fonction de leurs contraintes de QoS. Par opposition au micro-flot, l'agrégation se nomme macro-flot et représente une classe de QoS. Les routeurs effectuent les traitements non plus sur des micro-flots (trop nombreux dans l'Internet) mais sur des macro-flots dont le nombre est limité et fixé par l'administrateur du domaine. Un domaine représente une portion contiguë de l'Internet contrôlée par une même autorité administrative.

L'autre idée de Diff-Serv concerne l'architecture et consiste à distinguer la frontière de l'intérieur d'un domaine d'administration. Celle-ci est matérialisée par un routeur de bordure. Ce routeur joue un rôle diffèrent de celui situé au cœur du domaine. La figure 1 montre le placement des différents routeurs dans le domaine d'administration. L'architecture Diff-Serv s'inscrit dans le même paradigme que l'Internet qui est : "reléguer la complexité dans les extrémités du réseau et laisser le cœur du réseau aussi simple que possible". Cette architecture consiste à procéder à un simple ordonnancement des flots au sein du réseau et au contrôle du trafic en bordure.

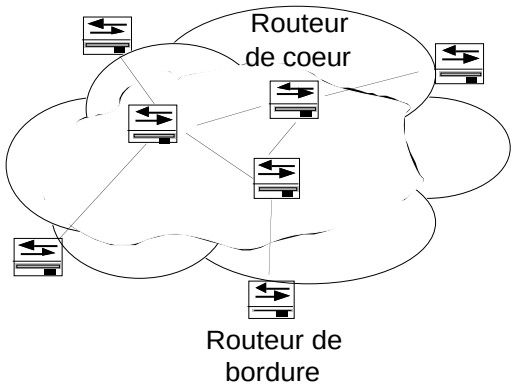



**Figure 1 : Architecture d'un domaine d'administration Diff-Serv.**

Le routeur de bordure a en charge la surveillance et le conditionnement du trafic entrant. Ces tâches sont complexes et mettent en jeu une grande variété de contextes. Elles sont essentielles et servent à renforcer la garantie de service de l'agrégation en limitant la quantité de trafic injectée par chaque utilisateur. Les contrôles sur le trafic entrant s'appliquent au niveau du flot utilisateur. Le flot utilisateur peut être soit le trafic issu d'un site, soit celui généré par une application. La granularité du flot utilisateur dépend directement de celui du service souscrit (*SLA : Service Level Agreement*). Le SLA est le résultat d'un accord entre un utilisateur et un prestataire de service. Un SLA est défini selon une échelle de temps différente de la session applicative. Les paramètres de description du service nécessaires au conditionnement de trafic sont décrits dans un profil (*TCA : Traffic Conditioning Agreement*). Le TCA est un sous-ensemble du SLA. Les conditionneurs de trafic et leur configuration sont décrits en détail dans [3]. Le résultat du conditionnement se traduit concrètement par un marquage des paquets admis dans un réseau IP, par la suppression des paquets excédentaires ou par la remise en forme du flot (assurer un espacement temporel entre les paquets).

Les routeurs de cœur déchargés des contrôles policiers se consacrent exclusivement au relayage des paquets. Ils ne voient plus des flots utilisateurs mais des classes. Une classe représente une agrégation de flots utilisateurs comme définie préalablement. Selon la terminologie [1], la classe constitue une agrégation de comportement (*BA* : *Behavior Aggregate*) qui demande aux routeurs un même comportement de relayage des paquets (*PHB : Per Hop Behaviour*). L'identification d'un paquet à un BA se fait par un motif particulier dans l'en-tête du paquet. Dans le cas d'IPv6, ce motif est en lieu et place du champ classe [4]. Le motif, appelé également le champ DS (*Differentiated Service Field*), est présent dans chaque paquet et sert à leur marquage. Les routeurs appliquent un traitement aux paquets en fonction de leur champ DS. Spécifiquement, le champ DS décrit un PHB se définissant par exemple comme :

- le niveau de priorité du paquet si le routeur gère les paquets suivant un mécanisme par priorité (avec une file d'attente par niveau de priorité) ;
- la portion minimale de la capacité du routeur associée à chaque classe de paquets si la file est gérée suivant une discipline WFQ (*Weighted Fair Queuing*) ;
- la probabilité de rejet du paquet en fonction de sa classe (et du niveau d'occupation de la file) si le routeur gère le trafic suivant une politique RED (*Random Early Discard*).

Selon l'architecture Diff-Serv, les fonctions de relayage sont clairement séparées de celles du contrôle que l'on nomme dans la terminologie conditionnement. La gestion de la QoS est ainsi répartie entre les éléments de bordure du réseau et les nœuds internes. Dans ces conditions, le service réseau offert est la combinaison d'une politique de conditionnement du trafic et d'un comportement de relayage dans les routeurs. Une grande variété de services peut être ainsi définie avec un jeu très limité de PHB. Les travaux du groupe Diff-Serv de l'IETF ont dégagé deux nouveaux PHB :

- EF (*Expedited Forwarding*) permettant de réaliser le transfert de flux à forte contrainte temps réel (équivalent à la classe de trafic CBR d'un réseau ATM) [5],
- AF (*Assured Forwarding*) permettant de garantir à certains paquets d'un flux de ne pas être supprimés en cas de congestion [6]. Le service de transfert doit être amélioré par rapport à celui du BE.

Le modèle d'architecture Diff-Serv repose sur un contrôle de traitement centralisé du relayage des paquets. Cela veut dire concrètement que la totalité de la bande passante du lien est dédiée à une interface de sortie. Celle-ci contient les mécanismes pour le relayage des paquets conformément au PHB sollicité. Tous les nœuds de l'Internet possède au moins une interface de sortie. Elle représente pour IP une abstraction de la technologie réseau sous-jacente. Le modèle Diff-Serv s'applique donc aisément aux topologies des réseaux commutés. Cette topologie se caractérise par liens point à point interconnectés par des routeurs. La topologie du réseau commuté est principalement appliquée aux WAN comme ceux ayant un rôle de réseaux de transit ou d'accès dans l'Internet. La tendance actuelle est d'introduire les topologies commutées dans les LAN (réseaux d'entreprises) au détriment des topologies à diffusion. Les topologies à diffusion (réseau de type 802.x ) se caractérisent par un support unique et partagé par l'ensemble des nœuds connectés au réseau. Comme son nom l'indique, la diffusion est une propriété naturelle de ce type de réseau : une trame émise sur le support est reçue par tous les nœuds. Les LAN commutés mettent en jeu des commutateurs et des liens point à point dédiés pour relier les différents nœuds du LAN au commutateur. Les commutateurs de la dernière génération effectuent une gestion de la priorité suivant le standard lEEE 802.1p [7]. Ce standard définit un moyen de différencier plusieurs valeurs de "priorité utilisateur" contenues dans les trames. Or tous les LAN n'ont pas un contrôle de trafic ou un mécanisme de priorité de niveau liaison indispensable pour différencier les différents types de flots. C'est notamment le cas pour les LAN partagés comme par exemple, le réseau Ethernet/IEEE 802.3 qui ne contient aucune notion de classes de trafic. Initialement Ethernet fonctionnait selon une topologie à diffusion : il était constitué d'un lien multipoints non fermé (un bus). L'ensemble des nœuds connectés au segment partageait la bande passante et se répartissait l'accès au lien. La technologie de réseau Ethernet a évolué et fonctionne maintenant aussi bien en LAN partagé qu'en LAN commuté. En 1996, on estimait à 120 millions de machines connectées à l'Internet via un réseau Ethernet. Les réseaux à diffusion connaissent un regain d'intérêt ces dernières années avec le déploiement des réseaux locaux sans fil. Vis à vis de la gestion de la QoS, les réseaux à diffusion posent quelques problèmes :

- tous les émetteurs partagent les même ressources. Comme le contrôle d'accès est réparti et qu'il n'y a aucun contrôle de trafic, aucune isolation des flots n'existe pour protéger les flots à QoS des flots BE. Il n’est possible dans ces conditions de garantir la moindre QoS à des flots spécifiques.
- la multiplicité des accès au support empêche d'effectuer un ordonnancement de l'ensemble des paquets émis comme c'est le cas lorsqu'il y a un accès unique.
- la bande passante du support est instable, elle peut dépendre de l'environnement d'exploitation mais également de la charge offerte. Cette remarque est surtout vraie dans le cas des réseaux Ethernet/IEEE 802.3 puisque après avoir atteint un maximum, les performances se dégradent d’une façon presque inversement proportionnelle à la charge dans les conditions de pointe.

La conclusion de ces remarques est qu'aucun émetteur sur un réseau à diffusion ne peut avoir une garantie de QoS pour ses propres besoins. Il n'en est pas moins que la QoS est un concept de bout en bout. Cela signifie que de l'émetteur au récepteur, tous les réseaux sollicités pour l'acheminement des données doivent être en mesure de fournir une QoS conforme

à la demande. La QoS vue par le récepteur correspondra à la QoS rendue par le réseau le moins performant. Le maillon faible dans cette chaîne est le réseau local lorsqu'il fonctionne selon une topologie à distribution.

## 3. Architecture Int-Serv

La solution de l'IETF pour garantir une QoS de bout en bout s'appuie essentiellement sur l'architecture intégration de services (Int-Serv) [8] et de son protocole de signalisation RSVP [9]. Les réseaux de périphérie de l'Internet, communément appelés les Intranet, fonctionnent suivant l'architecture Int-Serv. Un Intranet est un réseau IP d'entreprise qui joue un rôle de distribution dans l'Internet. Ils sont principalement construits sur la base des technologies LAN. [10] définit pour les technologies LAN un contrôle d'admission. La projection de la QoS dans Int-Serv sur les niveaux de priorité utilisés par les commutateurs de LAN du style IEEE 802.x est présentée dans [11]. Les réseaux commutés de grandes tailles (WAN) que l'on trouve au cœur de l'Internet adoptent une architecture de gestion de QoS Diff-Serv. Le document [12] présente comment utiliser ces réseaux dans une optique Int-Serv et suggère de considérer un réseau avec une architecture Diff-Serv comme une des technologies de réseaux sous-jacent à IP. Cet ensemble de documents décrit une architecture de gestion de QoS de bout en bout et les moyens à mettre en œuvre pour son utilisation au dessus des différentes technologies réseau.

L'inconvénient de Int-Serv est qu'il introduit un contrôle d'admission et change le modèle de fonctionnement de l'Internet classique. De plus, il oblige les applications à signaler "à l'appel" leur besoin de QoS par un protocole dédié. Ceci complique le développement des applications. Cette architecture s'inspire fortement du modèle connecté qui n'est pas du niveau IP. L'architecture Diff-Serv apporte un cadre de gestion de la QoS qui est plus conforme au mode de fonctionnement de l'Internet (non connecté). A la vue de ces remarques, la question que l'on se pose est : que faut-il faire pour avoir une QoS de bout en bout au moyen d'une architecture Diff-Serv ? Comme, nous l'avons précédemment cité, la gestion de QoS sur les LAN partagés est difficile à cause du manque d'isolation des flots et de la sensibilité de la bande passante à la charge. Pour avoir une QoS de bout en bout dans les cas d'utilisation des réseaux Diff-Serv, il devient indispensable que les LAN puissent offrir des services de communications différents.

Une partie de la solution du problème est présentée par [13]. La solution proposée permet d'effectuer des réservations de bande passante pour un flot d'un émetteur sur un LAN partagé. Le principe de la gestion de QoS décrit repose sur un contrôle de la charge offerte et se caractérise par :

- un contrôle d'accès pour l'ensemble des flots,
- une isolation des flots avec une réservation,
- une répartition équitable de la bande passante disponible entre les flots BE des différents nœuds,

Cette proposition appelée CLEP est différente de celle soutenue par l'IETF [10]. Elle s'inscrit dans le contexte Int-Serv. La réservation est faite dynamiquement pour un micro flot après avoir passé un contrôle d'admission. Si le mécanisme proposé fonctionne bien, il est à noter cependant qu'il n'y a aucune recherche de gains statistiques. Une fois la bande passante réservée, elle ne peut plus être utilisée par des trafics sans réservation même s'il n'y a aucune émission dans la portion de la bande passante réservée.

Dans ce qui suit, nous décrivons un mécanisme de contrôle de la bande passante pour le support du PHB EF sur les LAN partagés du style IEEE 802.x. Ce mécanisme inspiré des travaux sur CLEP [13, 14] en diffère par la gestion des flots dans un nœud et la suppression des mécanismes de réservations dynamiques. La similitude porte sur la stabilisation de la bande passante du lien. L'objectif principal de notre proposition est de garantir la QoS à certains flux lorsqu'ils sont gérés au niveau du réseau sous-jacent sous forme d'une agrégation des flots. Le contrôle de trafic quant à lui reste au niveau des nœuds. Le second objectif est d'obtenir des gains statistiques malgré l'isolation des classes de trafics et sans entraîner des dégradations sur les garanties de QoS. Ainsi nous transformons un réseau à service unique BE en un réseau compatible à une architecture Diff-Serv à 2 PHB : EF et DE. Le PHB EF sert à fournir un service de transfert expéditif. Le PHB DE (*Default*) est utilisé par le service BE.

## 4. Contrôle de charge pour services différenciés sur média partagé

L'architecture proposée se situe dans le contexte d'un réseau local de type IEEE 802.x constitué par un lien partagé. Le TCA indique les règles d'identification des flots bénéficiant d'un service de transfert expéditif et leur débit maximum autorisé.

Pour faire un contrôle de charge, notre architecture s'appuie d'une part sur un protocole de signalisation appelé DS-CLEP (Differentiated Services Controlled load Ethernet Protocol) qui doit être exécuté par chaque machine connectée au réseau et d'autre part sur un conditionnement des flots et un contrôle d'accès au lien. Actuellement, deux classes de trafics sont prises en compte : i) la classe de transfert expéditif caractérisée par une sensibilité à la latence qui doit être la plus faible possible, par une gigue quasi-constante et des débits constants quelles que soient les conditions des trafics dans l'autre classe, ii) la classe BE. La suite du document présente le modèle de réseau Diff-Serv sur média partagé.

### 4.1. Modèle du réseau Diff-Serv sur média partagé

La figure 2 représente les éléments fonctionnels d'un réseau Diff-Serv sur média partagé. Le réseau physique correspond aux éléments qui sont sous la couche IP dans le modèle architecturale TCP/IP. Chaque nœud connecté au réseau doit effectuer un contrôle d'accès au lien. Un nœud non-DS (Differentiated Services) est un nœud n'émettant que du trafic BE. Il n'a pas besoin de faire de conditionnement de trafic. Par contre, un nœud DS doit intégrer un conditionnement pour les flots utilisateurs du service de transfert expéditif. L'opération de conditionnement de trafic expéditif consiste à limiter le débit en fonction du profil indiqué par le TCA et à marquer les flots avec le PHB EF. La figure 3 montre les différents éléments fonctionnels pour le conditionnement. La classification des flots se fait selon les règles de filtrage contenu dans le TCA. En l'absence d'identification, les flots sont supposés utiliser le service BE et sont marqués avec le PHB DE.

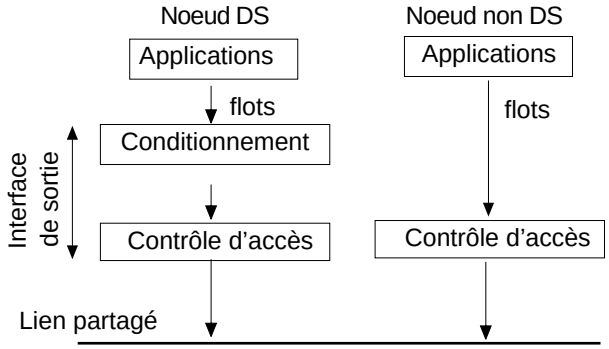



**Figure 2 : Eléments fonctionnels d'un réseau Diff-Serv sur lien partagé.**

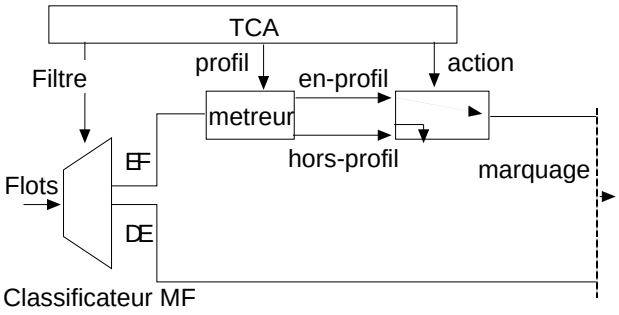



**Figure 3 : Eléments fonctionnels pour le conditionnement.**

La figure 4 montre les éléments fonctionnels du contrôle d'accès. Le composant de REFA (Remise En Forme Adaptative) régule le débit d'émission des flots DE et adapte le débit à la bande passante laissée libre par les autres classes de trafic. La variation du débit DE transmis se fait à partir d'une signalisation échangée entre les contrôleurs d'accès des noeuds. Le paragraphe suivant explique le fonctionnement du composant REFA au sein de DS-CLEP.

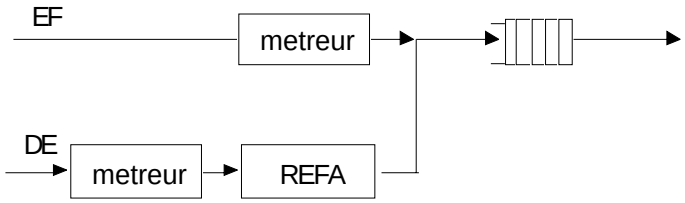



**Figure 4 : Eléments fonctionnels pour le contrôle d'accès**

### 4.2. Fonctionnement de DS-CLEP

Soit un LAN avec une bande passante totale $r_{max}$ qui est partagée par des flux expéditifs et des flux DE. La gestion du partage de la bande passante de ce LAN conduit à traiter deux paramètres: la bande passante allouée aux flux DE et la bande passante occupée par les flux EF. Cette gestion repose sur le principe d'une connaissance par chaque noeud des conditions de trafic locales et celles des autres noeuds connectés au LAN. Nous notons $r_{de}$ la bande passante allouée et effectivement utilisée par les flux DE et $r_{fe}$ la bande passante utilisée par les flux EF d'un noeud. La bande passante utilisée par un noeud correspond à son débit d'émission. On note REF la bande passante maximum du service expéditif d'un LAN. Cette valeur est déterminée par l'administrateur du réseau. Le débit maximum alloué au trafic EF d'un noeud est indiqué par son TCA et est noté $r_{ef\_max}$. La somme des allocations de débits du trafic EF ne doit pas dépasser la bande passante maximum du service expéditif, soit :

$$\sum_{i=1}^{n} r_{ef\_\max_i} \leq REF$$ avec n le nombre de noeuds du LAN.

Chaque noeud diffuse périodiquement sur le réseau l'état de son trafic. Il précise son $r_{de}$, $r_{ef}$ et $r_{min}$ qui est la valeur minimale que peut prendre $r_{de}$. Il précise éventuellement qu'il veut plus de bande passante pour son trafic DE. Les états du trafic diffusés servent à chaque noeud à construire localement une représentation globale de l'état d'utilisation de la bande passante du LAN. A partir de cette représentation, le contrôle d'accès de chaque noeud calcule $r_{free}$, sa bande passante disponible :

$$r_{free} = \frac{r_{\max} - \sum_{i=1}^{n} (r_{de_i} + r_{ef_i})}{n_{wm}} \quad (1)$$

où $n_{wm}$ représente le nombre de noeud demandant plus de bande passante. Le contrôle d'accès de chaque noeud détermine l'ajustement de $r_{de}$ par le calcul du paramètre $r_{free\_de}$ afin d'obtenir un partage égalitaire de la bande passante. L'algorithme de $r_{free\_de}$ est le suivant :

$$r_{free\_de} = r_{free} \text{ si } r_{de} < \frac{\sum_{i=1}^{n} (r_{de_i})}{n} \quad (2)$$

$$r_{free\_de} = r_{free} - r_{max}/100 \quad \text{sinon} \quad (3)$$

Si $r_{free\_de}$ est négatif, $r_{de}$ doit être diminué de :

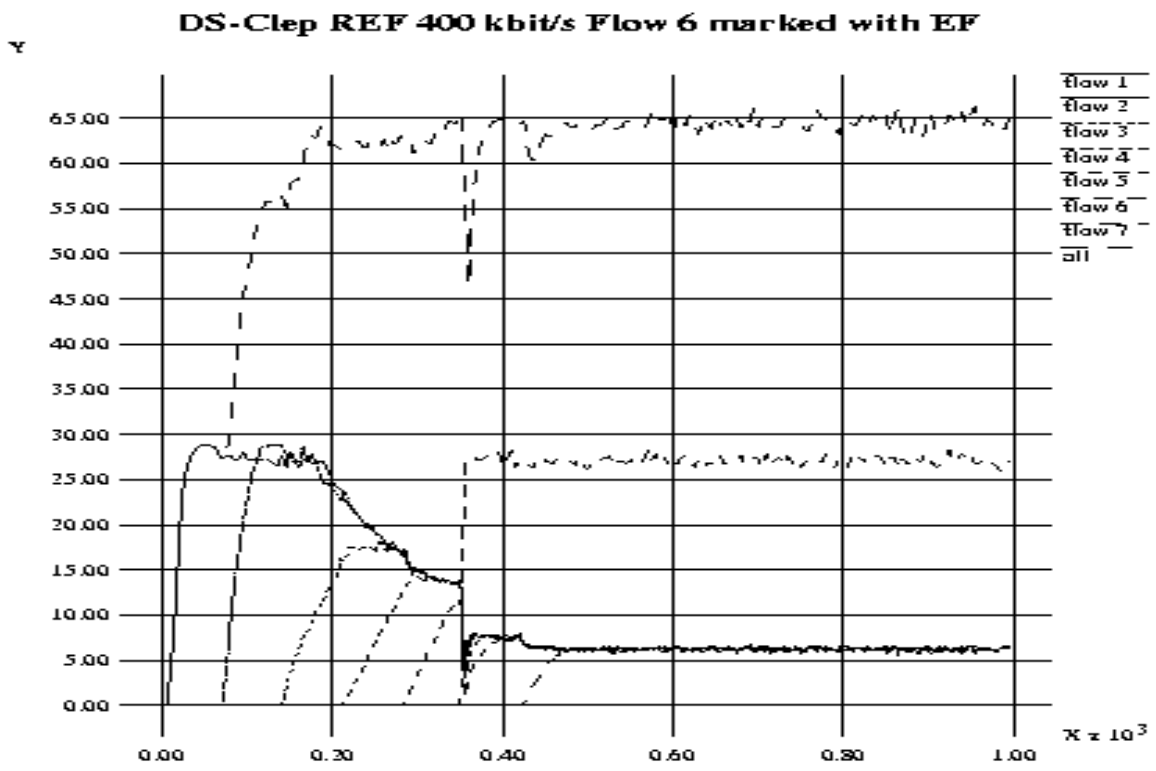
$$\frac{r_{de} - r_{\min}}{\sum_{i=1}^{n} (r_{de_i} - r_{\min_i})} * \left(-r_{free\_de} + 0.5\right) \quad (4)$$

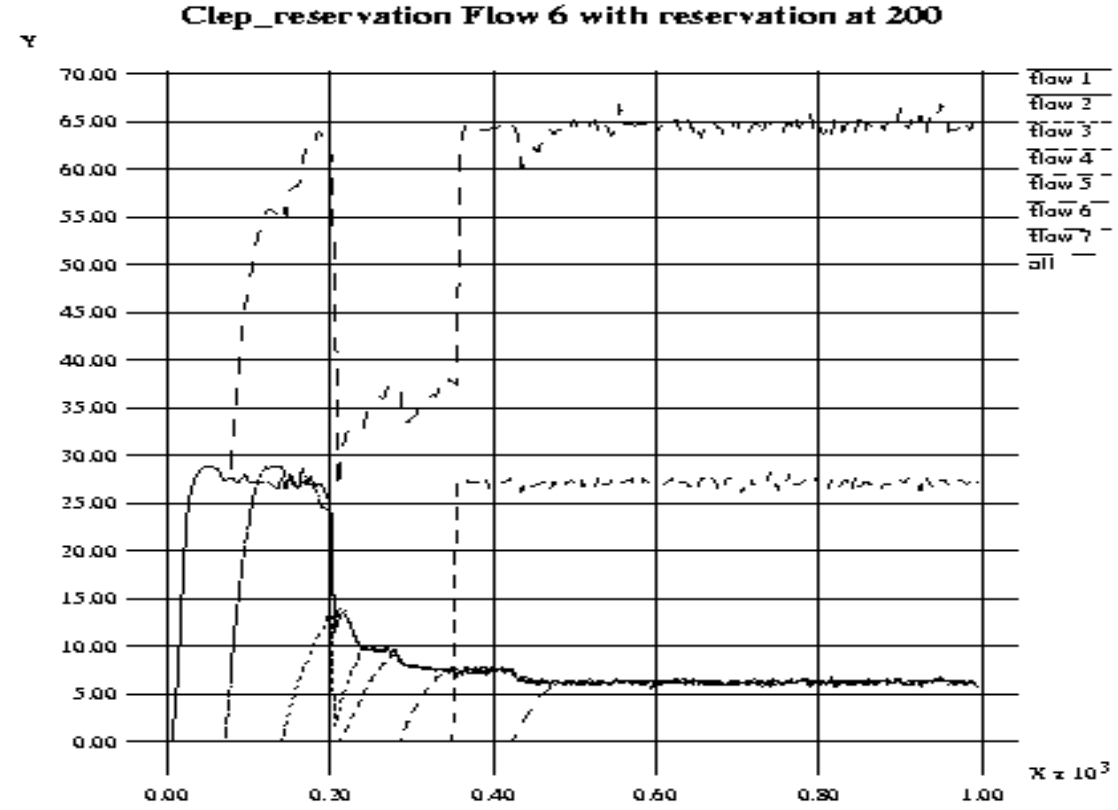
Par la formule (3), seuls les gros consommateurs de bande passante devront diminuer leur débit en trafic DE. Il donne une tolérance qui assure une stabilité au mécanisme de convergence. Enfin il est à noter que si $r_{de} < r_{min}$ , $r_{de} = r_{min}$. Aprés chaque modification du paramétre $r_{de}$, un état est diffusé aux autres noeuds du LAN. Enfin le composant REFA utilise le paramètre $r_{de}$ pour effectuer le lissage du trafic DE.

## 5. Evaluations et conclusions

L'évaluation de DS-CLEP a été faite avec l'outil de simulation NS [15]. Le modèle de simulation se compose de 7 noeuds émetteurs dont 6 émettent des flux DE et 1 émet un flux EF. Les figures 5 et 6 représentent l'évolution du début en fonction du temps. La figure 5 montre qu'en l'absence de flux EF jusqu'à t= 380 (date de l'activation du flux EF) les flux DE se répartissent la totalité de la bande passante. Après une courte période d'ajustement, nous remarquons que le débit du flux EF est garanti et que la bande passante totale reste proche de la valeur $r_{max}$. L'ajout du flot EF n'entraîne pas un chute du trafic écoulé mais à imposer aux trafics DE une diminution de leur débit d'émission. Il est à noter également la convergence des débits des flux DE. La figure 6 montre le gain statistique en bande passante par rapport à une solution utilisant une réservation comme c'est le cas pour CLEP [14]. Une réservation est faite à t=200 pour un flux d'un service prioritaire. La bande passante disponible pour le trafic Best Effort est donc $r_{max}$ moins la bande passante réservée. Nous voyons que le trafic écoulé a baissé entre l'instant de la réservation et le début de la transmission du flux prioritaire à t=380. Cette baisse n'existe pas dans la figure 5 alors que dans les deux cas nous avons la garantie en débit pour le flux prioritaire.

En conclusion, ces premiers résultats montrent qu'une gestion de la QoS reste possible sur LAN partagé selon un modèle d'architecture Diff-Serv. L'extension de cette architecture à d'autres classes de services est à l'étude. Le contrôle de la latence réseau et de la gigue pour les flux à QoS contraints font parties de nos futures thèmes d'études.


DS-Clep REF 400 kbit/s Flow 6 marked with EF
Y
65.00
60.00
55.00
50.00
45.00
40.00
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
0.00
0.20
0.40
0.60
0.80
1.00
X x 10^3
flow 1
flow 2
flow 3
flow 4
flow 5
flow 6
flow 7
all


Clep_reservation Flow 6 with reservation at 200
Y
70.00
65.00
60.00
55.00
50.00
45.00
40.00
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0.00
0.00
0.20
0.40
0.60
0.80
1.00
X x 10^3
flow 1
flow 2
flow 3
flow 4
flow 5
flow 6
flow 7
all

## Bibliographie


[1] **Blake, S.; Black, D. and Carlson, M.** (1998). RFC: 2475. December 1998.
*An Architecture for Differentiated Services.*

[2] **Bernet, Y.; Binder, J.; Blake, S. and Carlson, M.** (1999). draft-ietf-diffserv-framework-06.txt. February 1998.
*A Framework for Differentiated Services.*

[3] **Bernet, Y.; Smith, A. and Blake, S.** (1999). draft-ietf-diffserv-model-01.txt. October 1999.
*A Conceptual Model for Diffserv Routers.*

[4] **Nichols, K.; Blake, S.; Baker, F. and Black, D.** (1998). RFC: 2474. Décember 1998.
*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.*

[5] **Jacobson, V.; Nichols, K. and Poduri, K.** (1999). RFC: 2598. June 1999.
*An Expedited Forwarding PHB.*

[6] **Heinanen, J.; Baker, F.; Weiss, W. and Wroclawski, J.** (1999). RFC: 2597. June 1999.
*Assured Forwarding PHB Group.*

[7] **IEEE 802.1p** (1997). ISO/IEC Final CD 15802-3 IEEE P802.1D/D15.
Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision (Incorporating IEEE P802.1p: Traffic Class Expediting and Dynamic Multicast Filtering).

[8] **Braden, R.; Clark, D. and Shenker, S.** (1994). RFC: 1633. June 1994.
*Integrated Services in the Internet Architecture: An Overview.*

[9] **Braden, R.; Zhang, L.; Berson, S.; Herzog, S. and Jamin, S.** (1997). RFC: 2205. September 1997.
*Resource Reservation Protocol (RSVP) version 1 Functionnal Specification.*

[10] **Yavatkar, R.; Hoffman, D.; Bernet, Y.; Baker, F. and Speer, M.** (1999). draft-ietf-issll-is802-sbm-09.txt. October 1999.
*SBM (Subnet Bandwidth Manager): A Protocol for RSVP-based Admission Control over IEEE 802-style networks.*

[11] **Seaman, M.; Smith, A.; Crawley, E.; Networks, A. and Wroclawski, J.** (1999). draft-ietf-issll-is802-svc-mapping-04.txt. June 1999.
*Integrated Service Mappings on IEEE 802 Networks.*

[12] **Bernet, Y.; Yavatkar, R.; Ford, P.; Baker, F.; Speer, M.; Braden, R.; Davie, B.; Wroclawski, J. and Felstaine, E.** (1999). draft-ietf-issll-diffserv-rsp-03.txt. September 1999.
*A Framework for Integrated Servies Operation over Diffserv Networks.*

[13] **Horlait, E. and Bouyer, M.** (1999). draft-horlait-clep-00.txt. July 1999.
*CLEP (Controlled Load Ethernet Protocol): Bandwidth Management and Reservation Protocol for Shared Media.*

[14] **Bouyer, M. and Horlait, E.** (1997). SFBSID'97, Fortaleza, Brésil, November 1997.
*Bandwidth Management and Reservation over Shared Media.*

[15] **MacCanne, S and Floyd, S** (1997). http://www-mash.CS.Berkeley.EDU/ns/
*NS Network Simulator.*