
Evaluation de la différenciation de services dans l'Internet

Emmanuel Lochin*, **Pascal Anelli***, **Serge Fdida***, **Fabien Garcia****,
Guillaume Auriol**, **Christophe Chassot****, **André Lozes****

* LIP6 – Université Pierre et Marie Curie
4, place Jussieu, 75252 Paris Cedex 05 - France
{emmanuel.lochin, pascal.anelli, serge.fdida}@lip6.fr

** LAAS/CNRS
7 avenue du Colonel Roche, 31077 Toulouse Cedex 04 - France
{fgarcia, gauriol, chassot, alozes}@laas.fr

RÉSUMÉ. Cet article traite de la mise en oeuvre d'une architecture de qualité de service (QoS : Quality of Service) et de l'évaluation de ses services au moyen d'une plate-forme d'expérimentation. Cette plate-forme utilise un environnement de communication en IPv6. Elle a été développée dans le cadre du projet RNRT @irs. Son but est de déployer et valider un ensemble de services s'appuyant sur les principes d'une architecture Diff-Serv. La sémantique des services courants pour les applications est définie. La qualité de service est évaluée de bout en bout sur la base d'un flot applicatif et effectuée par des mesures expérimentales. L'isolation des flots aux conditions de trafic est étudiée. Les résultats de ces expérimentations montrent qu'un niveau de différenciation de services peut être rendu indépendamment des conditions de trafic. Cependant, le marquage de flots TCP pose des problèmes pour atteindre les objectifs de QoS. Les améliorations de l'architecture en vue de renforcer la QoS et de faciliter l'utilisation des services sont introduites en perspective de ces travaux.

ABSTRACT. Research reported in this paper deals with a communication architecture with guaranteed end-to-end Quality of Service (QoS) in an IPv6 environment providing differentiated services within a single Diff-Serv domain. The paper successively presents the design principles and services of the proposed architecture, their implementation and finally experimental measurements evaluating the QoS available the user level. In order to ease the application programmer task, principles of an architecture optimization are introduced in the future work part of the paper.

MOTS-CLÉS : Qualité de service, Mesure de services, Différenciation de Services, Agrégation de flots, plate-forme d'expérimentation IPv6.

KEYWORDS: QoS, Service évaluation, Diff-Serv, Behavior aggregate, IPv6 testbed

1. Introduction

En quittant le monde académique et militaire pour se développer dans la société, les contraintes posées sur le service de transfert offert par l'Internet ont changé. En effet, l'Internet commercial s'accommode mal du service "au mieux" qui a prévalu depuis ses débuts. Les progrès des technologies numériques ont fait émerger des applications qui posent de nouvelles contraintes au service de communication. Les fournisseurs d'accès Internet souhaitent allouer efficacement les ressources afin d'accroître leur activité au prix d'un investissement minimum. La Qualité de Service (*QoS*) est au cœur de ces nouvelles demandes. La QoS (sous l'angle quantitatif) se conjugue selon deux aspects : temporel et sémantique. Elle s'exprime principalement au travers des paramètres de bande passante, de latence, de variation de la latence également appelée gigue et de taux de perte. Ce dernier représente le degré de transparence sémantique de l'infrastructure de communication. Au niveau de la couche d'interconnexion IP, la QoS désigne les traitements appliqués aux flots de paquets afin qu'ils obtiennent un niveau de service en adéquation avec la demande applicative. Les fonctions localisées à ce niveau et sur le chemin de données applicatives sont désignées par certains sous le terme de plan utilisateur. Le choix d'un service de communication pertinent pour l'application pose le problème de la sémantique des services offerts par un réseau au sens large. Ceux-ci doivent être en nombre limité et doivent servir pour un large éventail d'applications actuelles ou futures. La multiplicité des services est un élément de complexité dans la réalisation, la gestion et la lisibilité des services.

Cette réflexion sur le nombre de services et leurs caractéristiques a été menée, il y a déjà quelques années, par le groupe de travail Integrated Services (Int-Serv). La solution retenue [BRA 94] s'appuie sur trois services que l'on peut schématiser de la manière suivante :

- le service de l'Internet classique de communication dit "au mieux",
- un service d'un Internet sans congestion, c'est-à-dire peu de pertes de paquets (dues aux erreurs d'intégrité uniquement) et une latence proche d'un réseau peu chargé. La définition du service reste relativement peu précise,
- un service pour des utilisateurs exigeants sur les délais.

L'architecture proposée dans [NIC 99] s'appuie aussi sur un découpage des services en trois catégories assez similaires à celui proposé par Int-Serv. Ce découpage en trois classes de services (par défaut, intermédiaire et absolu) reste encore pertinent de nos jours. Il repose sur le constat que les applications se divisent en fonction de leurs exigences de QoS schématiquement en deux catégories [ROB 98] :

- Les applications **interactives**, comme par exemple les applications de type "Contrôle/Commande" qui effectuent un contrôle distant de systèmes mécaniques, les applications distribuées (comme l'application DIS : *Distributed Interactive Simulation*), les applications de téléphonie ou de vidéoconférence. Et, plus généralement, toutes les applications qui en plus du débit posent des contraintes sur les délais de transit de chaque paquet et la variabilité de ces délais.

– Les applications dites **élastiques**, qui consistent typiquement en un transfert d'un ou plusieurs documents de grande taille, sont sensibles uniquement au temps de transfert total du ou des documents. La QoS requise porte sur le débit moyen reçu au cours du transfert, et non sur le délai de transit de chaque paquet.

Cette division des applications en deux catégories identifie les garanties de QoS exigées d'un réseau en termes de **délai de transit** pour un débit intrinsèque donné, ou en termes de **débit utile** (*goodput*) indépendamment du délai de transit des paquets ou du débit instantané.

La sémantique des services développés pour la plate-forme d'expérimentation @IRS s'appuie sur cette analyse des besoins applicatifs. Les services proposés sont de trois catégories :

– un service "au mieux" (*Best Effort* : *BE*) traditionnel qui a l'avantage d'être simple de mise en œuvre et économique,

– un service à débit assuré (*Assured Service* : *AS*) qui améliore la qualité du service BE et destiné à mieux traiter une large gamme d'applications. Le service AS est conçu pour les flots élastiques issus des applications adaptatives. Les flots de ces applications ont un débit qui augmente tant qu'il y a des ressources disponibles et diminue quand une congestion apparaît. Le débit de ces flots se décompose en un débit minimum et en un débit opportuniste. Le premier correspond à un débit minimum assuré et invariant. En cas de congestion conjoncturelle dans le réseau, les paquets de cette partie étant marqués comme inadéquates pour la perte, ils ne doivent pas souffrir de la congestion. Le second correspond à un débit de paquets opportunistes et constitue la partie variable du débit dite "élastique". Aucune garantie n'est apportée à ces paquets. Ceux-ci sont acheminés par le réseau sur le principe du "au mieux". En cas de congestion, ce sont ces paquets qui seront éliminés en premier. Le débit opportuniste doit varier en fonction de l'état des ressources utilisées, d'où son caractère élastique. Il demande à l'utilisateur du service réseau d'adapter son débit opportuniste à la capacité du moment du réseau. En tout état de cause, le débit offert par ce service doit être meilleur que le service BE.

– un service à garanties fermes (*Guaranteed Service* : *GS*) pour des applications rares qui posent des contraintes de QoS fortes et qui, de plus, ne supportent pas des variations de la QoS. Ce service est destiné aux flots déterministes. Le service est conçu pour des flots continus ou réguliers. Ce service est souvent assimilé à une émulation de ligne louée.

La faisabilité de ces services et plus généralement les problèmes de la QoS sont étudiés dans de nombreux projets ; citons en particulier l'activité TF-TANT [TFT] du projet européen GEANT [GEA], le projet QBone [TEI 99] et les projets européens TEQUILA [TEQ], CADENUS [CAD], AQUILA [AQU], contribuant tous à la proposition d'architectures orientées Diff-Serv, dont le cadre général est défini dans [BLA 98].

Réalisés dans le cadre du projet @IRS¹, les travaux présentés dans cet article s'inscrivent dans ce contexte et portent sur la conception, l'implémentation et la mesure des performances d'une architecture de communication garantissant une QoS de bout en bout, dans un environnement IPv6 constituant un unique domaine Diff-Serv. Ils visent à démontrer les services différenciés qu'il est possible d'offrir au travers d'une architecture Diff-Serv. Les objectifs du projet consistaient à développer et analyser de nouveaux mécanismes et protocoles pour l'Internet (QoS et multicast) dans un environnement de réseaux hétérogènes (réseaux locaux, réseaux filaires et sans fil) en vue de supporter des services de communication pour un large spectre d'applications. Les acteurs de ce projet sont issus à la fois du monde académique et industriel. La description exhaustive du projet est disponible en ligne à l'URL : <http://www.lip6.fr/airs>. Les contributions de ce projet dans le domaine de la QoS sur réseau filaire sont : (1) étude et mise en oeuvre des éléments fonctionnels pour la gestion de la QoS sur le chemin de données dans un routeur en vue de fournir trois services clairement identifiés ; (2) mesure et analyse de la QoS offerte au niveau d'un flot individuel par un système de communication qui traite des agrégations de flots ; (3) identification des problèmes de l'utilisation par TCP d'un service réseau supportant la QoS.

Cet article vise à présenter ce qu'il a été possible de faire au travers d'une architecture Diff-Serv conçue pour la gestion des deux types de trafic de l'Internet (élastique et "temps-réel"). Les résultats sur les délais obtenus par cette plate-forme sont présentés dans [GAR 02]. Cet article se propose de compléter les mesures effectués en présentant une synthèse exhaustive des services Diff-Serv. Une étude sur le débit des flots TCP dans la classe assurée sera présentée afin d'obtenir l'évaluation de l'ensemble des services offerts selon un paramètre de QoS pertinent pour chaque service. L'article est structuré de la façon suivante : la partie 2 présente les principes de l'architecture ainsi que la mise en oeuvre des éléments fonctionnels nécessaires aux trois services. Les objectifs de l'étude sont définis dans la partie 3. La partie 4 décrit les scénarios d'expérimentation pour l'étude de la QoS de bout en bout. Les résultats des mesures sont présentés et analysés. Ces résultats sont rapprochés à ceux déjà existants dans la littérature. Les conclusions et perspectives de ces travaux sont enfin tirées en partie 5.

2. Architecture : principes et mise en oeuvre

L'architecture générale d'un réseau IP pour le support de la QoS repose sur le principe de l'agrégation de flots de paquets en classes de services et de la gestion des ressources par classe plutôt que par flot individuel [BLA 98]. Un flot individuel consiste en une séquence de paquets issus d'un utilisateur. Celui-ci peut être tout aussi bien un site ou une application. Ces flots sont regroupés en fonction du service requis pour former des agrégats de flots. Le nombre d'agrégats de flots dépend des classes de services offertes. L'agrégat de flots forme un macro-flot. Par opposition, les flots in-

1. @IRS (Architecture Intégrée de Réseaux et Services - Décembre 1998 - Avril 2001) est un projet français financé par le Réseau National de la Recherche en Télécommunications (RNRT).

dividuels sont appelés des micro-flots. L'architecture Diff-Serv distingue la frontière de l'intérieur d'un domaine d'administration. Un domaine se définit comme une portion contiguë de l'Internet contrôlée par une même autorité administrative. La frontière d'un domaine d'administration est marquée par un routeur de bordure. Ce routeur joue un rôle supplémentaire de celui situé au cœur du domaine. Cette architecture s'inscrit dans le même paradigme que l'Internet qui est : "de reléguer la complexité dans les extrémités du réseau et de laisser le cœur du réseau aussi simple que possible". Cette architecture conduit à procéder à un simple ordonnancement des agrégats de flots au cœur du réseau et au contrôle de flots individuels en bordure.

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 servent à limiter la quantité de trafic injecté par chaque utilisateur dans sa classe de service. Elles sont essentielles et limitent l'apparition de la congestion dans la classe de service. Les contrôles sur le trafic entrant s'appliquent au niveau du flot utilisateur. La granularité du flot utilisateur et les paramètres du conditionnement de trafic sont décrits dans un profil (TCA : *Traffic Conditioning Agreement*). Le résultat du conditionnement se traduit concrètement par un marquage des paquets admis dans le domaine, par la suppression des paquets excédentaires, ou par la remise en forme du flot (assurer un espacement temporel entre les paquets). Le traitement des paquets par les routeurs du domaine est défini par le comportement de relayage (PHB : *Per-Hop Behavior*). La sélection du PHB est en fonction de la marque contenue dans l'en-tête du paquet. En plus du comportement standard actuel dit DE (*Default*) utilisé par le service BE, deux PHB sont disponibles EF (*Expedited Forwarding*) [DAV 02] et AF (*Assured Forwarding*) [HEI 99]. Le PHB EF permet de réaliser un service de transfert à forte contrainte temporelle tandis que le PHB AF assure à certains paquets une protection contre la perte en cas de congestion.

2.1. Structure d'un routeur

La structure fonctionnelle d'un routeur IP peut se représenter selon la figure 1.

Les fonctions de QoS de niveau IP résident dans les interfaces d'entrée et de sortie du routeur. Les fonctions mises en oeuvre dépendent du rôle du routeur dans l'architecture (c.a.d. de bordure ou de cœur). Un routeur de cœur comportera uniquement les fonctions liées au relayage, localisées dans l'interface de sortie. Ces fonctions visent à allouer efficacement les ressources que sont la bande passante et la mémoire de la file d'attente en fonction du comportement de relayage propre à chaque classe de paquets. Un routeur bien dimensionné suppose que la capacité de commutation de la matrice est supérieure à la somme des débits entrants. Dans ces conditions, la file d'attente des interfaces d'entrée ne peut être saturée. La congestion se manifeste donc uniquement sur la file d'attente de l'interface de sortie. Il est donc de la responsabilité des fonctions de relayage de protéger les flots à QoS de la congestion afin de maintenir un niveau de service stable. En plus des fonctions de relayage qui sont identiques aux fonctions d'un routeur de cœur, le routeur de bordure conditionne le trafic entrant dans

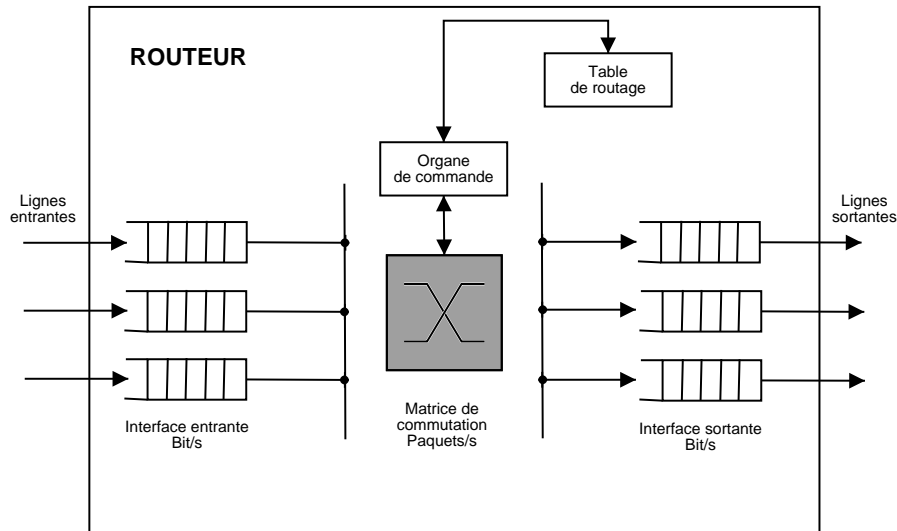


Figure 1. Structure fonctionnelle d'un routeur

le domaine. Ces dernières fonctions sont placées dans l'interface d'entrée. L'interface d'entrée en question est celle qui reçoit le trafic de l'extérieur du domaine. Cette interface peut être qualifiée d'interface amont.

La démarche prise dans la définition de l'architecture de la plate-forme d'expérimentation va consister à identifier un jeu de mécanismes cohérents afin de fournir simplement des services conformes à la spécification. Les paragraphes suivants décrivent les mécanismes de gestion de la QoS pour spécialiser le rôle des routeurs selon leur place dans le domaine.

2.1.1. Interface amont

L'interface réseau amont se trouve exclusivement dans le routeur de bordure en entrée du domaine. Elle a en charge le filtrage du trafic entrant. Les éléments fonctionnels de l'interface amont sont représentés par la figure 3. Les règles et les paramètres du conditionnement du trafic d'un utilisateur sont décrits dans le TCA. On y trouvera les règles de filtrage pour l'identification de l'utilisateur du service, le profil du trafic et les actions pour le trafic soumis en excès. La classification multicritère (*Multi-field : MF*) repose sur les règles de filtrage. Dans le cas d'IPv6, ce travail d'identification est grandement facilité par le champ *flow label* présent dans l'en-tête des datagrammes. En effet un flot applicatif est identifié de manière unique par la paire (adresse source, *flow label*).

Concernant les flots GS, le profil de trafic est constitué uniquement d'un débit crête. La vérification du respect du TCA consiste alors simplement en un mètre-espaceur, qui n'est autre qu'une file d'attente de taille finie, dont la vitesse du serveur

correspond à ce débit crête. Les paquets acceptés dans la file sont marqués EF, les paquets non conformes sont rejetés. La file d'attente permet d'absorber des rafales de paquets en retardant ces paquets afin de respecter le débit crête ; il faut cependant que la taille de cette file d'attente ne soit pas trop grande pour que le délai d'attente maximal dans cette file soit acceptable.

Concernant les flots AS, le profil d'un flot est défini par un débit moyen et par une sporadicité. Sachant que le débit moyen correspond à l'assurance soit au débit minimum, le contrôle de conformité du flot par rapport au profil se fait par un *leaky bucket* caractérisé par deux paramètres (r, b) , à savoir le taux de fuite et la taille du seau. Un *leaky bucket* analyse les données d'un flot par une sporadicité et un débit moyen. Chaque unité de données émise ajoute un jeton dans le seau. Le seau a une capacité de b jetons et fuit à un taux de r jetons par seconde. Quand une unité de données fait déborder le seau, elle est déclarée non conforme. Les paquets sont marqués AF et une priorité spatiale leur est également attribuée en fonction de leur conformité au profil. Les paquets détectés conformes reçoivent une priorité à la perte faible (marque *IN*) et les paquets non conformes ont une indication de forte priorité à la perte (marque *OUT*). Ces derniers deviennent des paquets opportunistes. La priorité à la perte est utilisée quand le paquet passe par des routeurs saturés. En l'absence de congestion, cette priorité ne sert pas.

Concernant les flots BE, aucun contrôle particulier n'est effectué : tous les paquets sont marqués DE. Le métreur n'a qu'un rôle d'information pour l'administration de réseau.

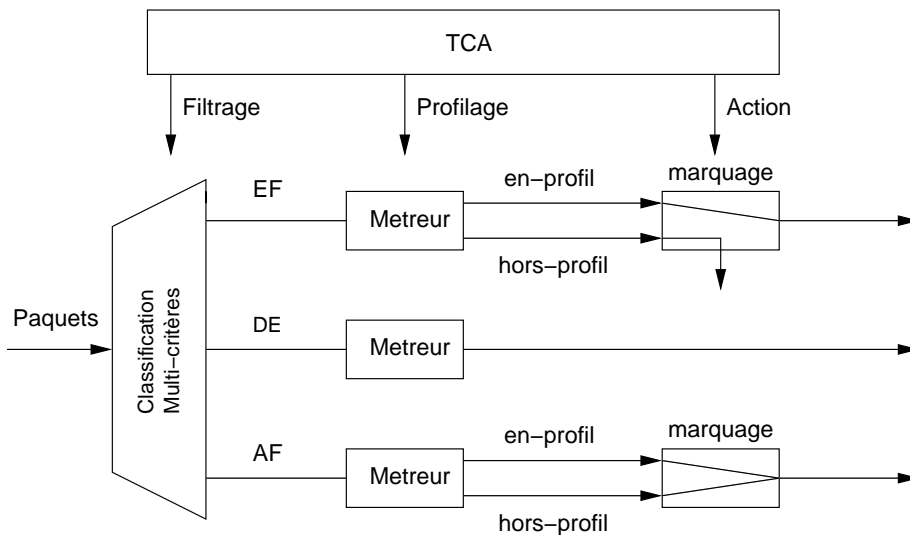


Figure 2. Éléments fonctionnels d'une interface d'entrée d'un routeur de bordure

2.1.2. Interface de sortie

L'interface de sortie d'un routeur @IRS comprend l'ensemble des mécanismes de relayage. Ces mécanismes ont en charge l'ordonnement des paquets et la gestion des pertes en cas de congestion. La figure 3 décrit la solution retenue et développée. A l'entrée de l'interface, les paquets sont classés dans l'une des trois files d'attente. Cette classification est effectuée en fonction de la marque attribuée par le conditionnement lors de leur entrée dans le domaine. Une telle classification est dite BA (*Behavior Aggregate*), ou autrement dit selon la classe de service. La notion de flot individuel n'existe plus.

La politique d'ordonnement s'appuie sur 2 ordonnanceurs mis en étage afin de pouvoir gérer les trois PHB de l'architecture. Le PHB EF de la classe GS est obtenu par une priorité stricte (non préemptive) notée PQ (*Priority Queuing*), ce mécanisme assure un traitement rapide des paquets marqués EF. Le délai de paquets (retard induit par le fonctionnement en paquet par rapport à un modèle fluide) est de L_{max}/C où L_{max} est la taille maximum d'un paquet EF. Un ordonnancement unique de type WFQ (*Weighted Fair Queuing*) introduirait un délai de paquets de L_{max}/R où R est la bande passante allouée au PHB EF (avec $R < C$). La motivation de PQ se trouve dans la faiblesse du délai de paquets ajoutée par rapport à WFQ. Le PHB EF est destiné à un service exigeant sur les délais. Le mécanisme retenu donne le relayage le plus rapide [FER 00]. Il protège le trafic de la classe GS du trafic des classes AS et DE, à l'exception du cas où un paquet de la classe GS doit attendre la fin de transmission d'un éventuel paquet de la classe AS ou BE en cours de transmission avant d'être servi. Ce délai dû à la non préemption des paquets en cours de transmission est connu sous le nom de délai de sérialisation. L'utilisation d'un PQ doit se compléter d'un contrôle d'admission afin d'éviter que le service GS entraîne une famine sur les autres services et plus généralement pour éviter que la charge dans le service GS soit importante et qu'il se transforme en fin de compte en un service BE bis. La fonction de contrôle d'admission est localisée dans le plan de contrôle qui n'était pas dans les objectifs du projet. Le reste de la bande passante non utilisée par GS est partagée équitablement entre les services AS et DE. Ce partage est effectué par un WFQ selon l'algorithme WF2Q [BEN 96].

Le taux de service μ de la discipline de service PQ représenté sur la figure 3 sert à régler le débit d'émission. Le débit d'émission de l'interface est ainsi configurable et indépendant du débit du support. Cette fonction trouve son utilité dans les expérimentations pour faire apparaître un goulot d'étranglement par rapport à la charge de trafic offerte. L'autre utilité consiste, dans le cas de support ATM, à adapter le débit d'émission au débit du lien logique qui est soit un VC (*Virtual Channel*), soit un VP (*Virtual Path*). Le taux de service μ est celui du lien logique.

Des pertes de paquets apparaissent lorsque la file d'attente arrive à saturation. La politique de perte par défaut notée DT (*DropTail*) consiste à éliminer le paquet trouvant une file pleine à son arrivée. Cette politique est appliquée aux PHB DE et EF bien que dans le cas EF cette situation ne doit pas exister. Concernant le PHB AF, une différenciation est faite entre paquets conformes et paquets non conformes. La dis-

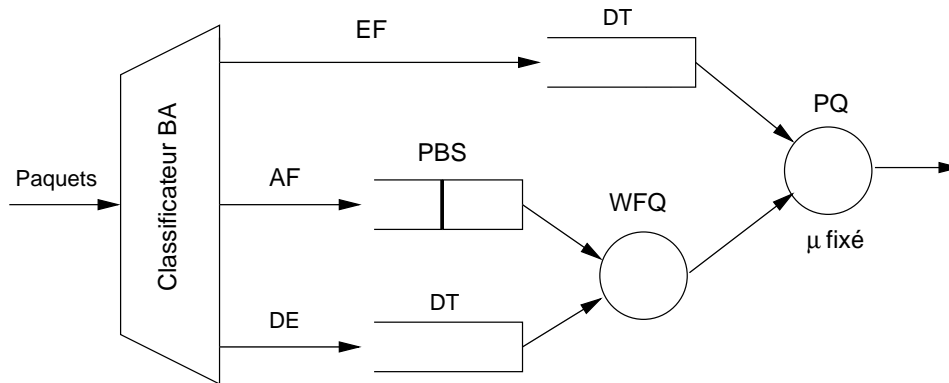


Figure 3. Éléments fonctionnels d'une interface de sortie

crimination de la perte selon une politique probabiliste tel que RED (*Random Early Discard*) est difficile à mettre en oeuvre principalement à cause du grand nombre de paramètres à régler. De plus des études ont montré que la politique de gestion de l'attente RED introduit de l'instabilité et des oscillations [BON 00] [ZIE 99]. Pour ces raisons, son utilisation dans les routeurs reste problématique [MAY 99]. Notre solution repose sur une politique déterministe mise en oeuvre par un mécanisme à simple seuil de type PBS (*Partial Buffer Sharing*). Les paquets opportunistes sont systématiquement rejetés dès que le nombre total de paquets en attente dans la file excède un certain seuil.

3. Méthode d'évaluation des services

3.1. Conditions d'études

Les premières mesures effectuées avec la plate-forme ont eu pour but de valider les classes de services les unes par rapport aux autres. Pour ce faire, le pire des cas est retenu. Un flot UDP occupant 100% des ressources disponibles de la classe de service AS (resp. GS) est émis parallèlement à un flot BE dont la charge va en s'accroissant jusqu'à saturation complète de l'ensemble des ressources du réseau. Un flot dans cette étude représente un agrégat de flot à savoir la charge totale dans la classe de service. Les résultats de ces mesures ont permis de conclure que les QoS AS et GS étaient conformes à celles attendues, à savoir une influence nulle du trafic BE sur la QoS GS (délai minimum, moyen, maximum, fiabilité et débit moyen inchangés), et "acceptable" sur la QoS AS (délai minimum et moyen, fiabilité et débit moyen inchangés, le délai maximum étant variable) [GAR 01].

Cette première étape d'évaluation n'est cependant pas suffisante. Cependant, elle est intéressante pour un opérateur désireux de montrer qu'il est capable d'offrir trois comportements de relayage différents. Pour un utilisateur, la perception d'un service

de communication avec une qualité de service se fait au niveau de son flot de paquets. L'évaluation présentée dans la suite de cet article va consister à étudier la QoS pour un micro-flot. Une certaine indépendance doit exister entre les micro-flots d'un même agrégat. De même, la qualité de service doit être insensible à la charge ou à la composition de la classe de service (ou agrégat). L'étude présentée par la suite vise à vérifier ce postulat pour les deux types de trafic de l'Internet et vise à démontrer qu'une qualité de service peut être fournie au niveau d'un micro flot sans avoir recours à une gestion par micro-flot comme dans l'architecture Int-Serv. Dans l'architecture proposée, le traitement au niveau d'un micro flot s'effectue uniquement à l'entrée du réseau dans le routeur de bordure. Les expérimentations portent sur l'étude de : (1) l'influence de la composition de l'agrégat exprimée en nombre de flot sur la QoS d'un flot individuel, (2) la QoS reçue par un flot élastique lorsqu'il utilise le service à débit assuré.

Ces évaluations sont faites dans le pire des cas. Le réseau est à chaque fois saturé par du trafic BE (le réseau est donc en état de congestion). La mesure de l'influence dans le premier cas d'étude se fera par le délai de transit de bout en bout et le taux de perte. Plus précisément, les valeurs minimales, moyennes et maximales du délai de transit sont déterminées pour des sessions expérimentales d'environ 300 secondes chacune. La fonction de répartition du délai de transit des paquets est également calculée. Le taux de perte correspond au rapport du nombre de paquets non reçus sur le nombre de paquets émis pour une session complète. La dernière évaluation utilisera des sources de trafic TCP et retiendra le débit utile comme paramètre de QoS.

3.2. La plate-forme de tests

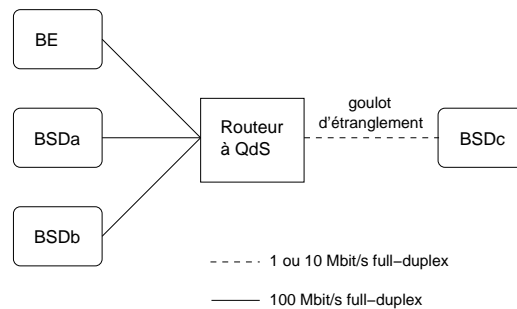


Figure 4. Représentation fonctionnelle de la plate-forme de tests

Comme le montre la figure 4, la plate-forme de tests est composée de cinq nœuds. Le routeur utilise un noyau Unix FreeBSD et comporte les mécanismes d'ordonnement décrits dans la première partie. Les deux hôtes FreeBSD (BSD_A et BSD_B) sont aussi des machines Unix qui émettent un trafic marqué, correspondant aux services GS ou AS. Elles effectuent également les fonctions de conditionnement. Le rôle du puit de trafic qui a en charge certaines mesures est joué par l'hôte (BSD_C). L'hôte noté

BE génère le trafic du service "au mieux". Afin de saturer le réseau, l'hôte *BE* émet à un débit équivalent au débit de l'interface de sortie du routeur.

Les tests ont nécessité deux générateurs de trafic. Pour les flots non élastiques, les flots sont générés au moyen d'un logiciel de génération de trafic développé en interne, nommé DEBIT6², permettant d'envoyer un trafic UDP dont le profil est déterminé par un *leaky bucket*. Pour les flots élastiques, le générateur de trafic retenu est BENCH [ROC] que nous avons porté en IPv6 afin d'effectuer les mesures et modifié pour qu'il puisse marquer le *flow label* de chaque paquet. BENCH offre la possibilité de générer plusieurs connexions simultanées depuis un même émetteur. Cette capacité a été utilisée par la machine *BSD_B*.

Le choix de cette plate-forme peut paraître simple au premier abord, mais elle caractérise en fait n'importe quel routeur dans un domaine. Que ce soit un routeur de bordure ou un routeur de cœur, au niveau microscopique, le comportement de relayage de chacun est identique. Au niveau macroscopique, la QoS résultante dépendra du routeur qui accusera les conditions de trafic les plus mauvaises en entrée par rapport à la capacité d'écoulement de son support en sortie. Pour le service AS, les routeurs en aval recevront donc un flot déjà lissé. Construire une plate-forme de tests à un seul routeur repose sur l'hypothèse que le flot subira les perturbations les plus significatives au niveau de ce routeur. Une telle configuration peut être désignée par le terme de goulot d'étranglement. Formellement, un lien est défini comme goulot d'étranglement pour un flot si le flot possède le débit plus important par rapport aux autres flots de ce lien et que le lien est saturé. L'objectif de cette plateforme consiste à mesurer les écarts de QoS les plus significatifs. Par exemple, la perte de temps au niveau d'un paquet ou la perte d'un paquet ne se corrige pas sur la suite de la route. Les détériorations d'un flot de paquets ne peuvent qu'empirer ou au mieux rester identiques. Donc une plate-forme de tests composée d'un seul routeur pour former un goulot d'étranglement est suffisante pour effectuer l'évaluation des services proposés.

Les hypothèses de configuration de la plate-forme sont :

- Le débit maximal R_{GS} de trafic GS admis est fixé à 20% de la capacité du goulot d'étranglement. Il reste donc au minimum 80 % de la capacité de la bande passante du goulot d'étranglement pour les autres services,
- la classe AS est dimensionnée pour avoir une garantie de 50 % de la bande passante non utilisée par le service GS. La pondération du WFQ utilisée pour AS est équivalente à celle de BE à savoir 0.5. Le service AS a donc une garantie de 40 % de la bande passante du goulot d'étranglement. Notons R_{AS} , cette garantie de débit.
- aucun biais n'est introduit entre les services par la taille des paquets. Tous les paquets ont une taille de 1024 octets,
- Les délais de propagation entre émetteurs et récepteur sont équivalents,
- les hôtes sont synchronisés par NTP (*Network Time Protocol*), limitant l'incertitude sur les mesures du délai à +/- 5 ms.

2. DEBIT6 est disponible sur <http://rp.lip6.fr/airs>

– la valeur du seuil de PBS est fixé à 32ko. Cette valeur représente la moitié de la fenêtre d’anticipation utilisée par défaut par TCP.

En ce qui concerne le débit du goulot d’étranglement, il est intéressant d’utiliser un faible débit lorsque des délais sont mesurés. Le temps de paquets et de sérialisation des paquets dépendent du débit du goulot d’étranglement, les écarts de délai seront plus importants avec un faible débit. De plus les imprécisions dans les mesures (à cause de NTP) deviennent négligeables. Et les temps de traitement du routeur dépendant du matériel sont minorés par rapport aux termes de délai liés à la communication. En revanche, pour la mesure du débit et pour augmenter la taille de l’agrégat, le débit a été décuplé par rapport au cas précédent.

4. Mesures et analyses des services

L’évaluation de la QoS au niveau du flot individuel se fera par la mise en oeuvre de trois scénarios d’études. Les deux premiers se placeront dans la perspective de l’utilisation des services par des flots issus des applications interactifs. Le dernier concernera les flots issus des applications élastiques.

4.1. Etude en isolation des services

Ce scénario a pour but d’évaluer l’influence du nombre de flots AS (resp. GS) sur la QoS AS (resp. GS) quand le réseau est saturé par du trafic BE. Aucun flot GS (resp. AS) n’est généré dans le réseau. Cette évaluation est faite à charge constante. L’étude du service s’effectue selon trois cas de figure comme indiqués par le tableau 1 :

- 1 flot à QoS est généré par l’hôte BSD_A avec un débit moyen équivalent à 50% de la capacité du service,
- 2 flots à QoS sont générés par les hôtes BSD_A et BSD_B avec un débit moyen équivalent à 23 et 27% de la capacité du service,
- 4 flots à QoS sont générés par les hôtes BSD_A et BSD_B avec un débit moyen équivalent à 11, 12, 13 et 14% de la capacité du service,

Parallèlement à ces flots, un flot BE (pour le premier cas) et deux flots BE (pour les deux autres) sont générés par la machine BE. La somme de leur débit est toujours équivalente à la capacité du goulot d’étranglement. Le débit du goulot d’étranglement est fixé à 1 Mbits/s.

4.1.1. service GS

La figure 5 montre l’évolution du délai de transit en fonction du nombre de flots de l’agrégat. D’après le tableau 2, la progression est de 8 ms en valeur moyenne et qui est également la valeur de variation pour 100% des paquets (figure 5). Cette valeur reste inférieure à l’écart maximum dans le cas d’un flot GS unique (14 ms) qui permet d’indiquer que le nombre de flots dans l’agrégat a une influence relativement faible.

Service AS	R_{AS}	Service GS	R_{GS}
AS (BSD _A)	50	GS (BSD _A)	50
AS _A (BSD _A)	23	GS _A (BSD _A)	23
AS _B (BSD _B)	27	GS _B (BSD _B)	27
AS _{A1} (BSD _A)	11	GS _{A1} (BSD _A)	11
AS _{A2} (BSD _A)	14	GS _{A2} (BSD _A)	14
AS _{B1} (BSD _B)	13	GS _{B1} (BSD _B)	13
AS _{B2} (BSD _B)	12	GS _{B2} (BSD _B)	12

Tableau 1. Différents cas de la génération de trafic pour chaque service

Avec un délai de sérialisation de 10 ms (la capacité du support au niveau paquet vaut 100Koctets/s et tous les paquets ont une taille de 1 Koctets), l'interprétation de l'écart maximal devient simple. L'écart de 20 ms (cas du flot GS_{B2}) signifie qu'il existe au pire une sporadicité de 2 paquets dans l'agrégat. L'étude de la relation entre la sporadicité de l'agrégat et la charge est développée dans [FER 00]. Celle-ci indique que la charge est le terme prédominant dans la QoS de GS. Une méthode de calcul de la borne maximale du délai est développée dans [BEN 01]. Le délai dépend du nombre de noeuds, de la charge et de la sporadicité de l'agrégat.

Délai(ms)	GS	GS _A	GS _B	GS _{A1}	GS _{A2}	GS _{B1}	GS _{B2}
min	19	16	16	18	18	18	18
moyen	25	26	26	32	31	33	31
max	33	33	35	33	34	37	38
% de perte	0	0	0	0	0	0	0

Tableau 2. Évaluation du service GS en fonction de sa composition

4.1.2. service AS

L'influence du nombre de flots sur un flot est faible. En effet, le tableau 3 indique une variation inférieure à 5 ms sur la valeur moyenne du délai de transit et un taux de perte constant à la valeur nulle.

Délai(ms)	AS	AS _A	AS _B	AS _{A1}	AS _{A2}	AS _{B1}	AS _{B2}
min	25	18	18	20	18	18	20
moyen	38	38	37	42	42	40	41
max	49	59	63	86	75	65	77
% de perte	0	0	0	0	0	0	0

Tableau 3. Évaluation du service AS en fonction de sa composition

Ce résultat est conforté par la figure 6 qui met en évidence que le délai de transit est quasi inchangé pour 90% des paquets. La courbe du flot de référence de la figure 6

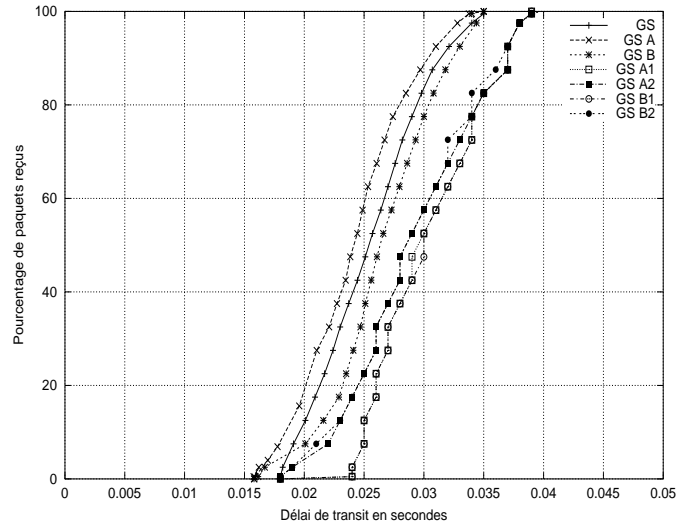


Figure 5. Répartition du délai de transit du service GS

représente le service AS dans le meilleur des cas, quand le réseau ne comporte aucun autre trafic. On peut cependant remarquer que 10% des paquets (pour les flots AS_A , AS_{B2} , AS_{A1} , AS_{A2} , AS_{B1} , AS_{B2}) ont un délai de transit nettement plus important que celui observé pour le flot AS seul. Ceci est intrinsèque au fonctionnement paquet et à l'asynchronisme. Lorsqu'il n'y a qu'une source, les paquets vont être générés en séquence. Dès qu'il y a plusieurs sources, des contentions sur l'interface de sortie du routeur peuvent se produire. Plus la charge sera importante et plus la probabilité de contention sera forte. Ce phénomène est amplifié par WFQ qui fait une remise en forme quand le débit instantané de l'agrégat est supérieur à son débit alloué. Une remise en forme ajoute un délai d'attente pour les paquets concernés. Cette dispersion n'apparaît pas dans les mesures du service GS, justement car la charge est plus faible et que PQ n'effectue aucun contrôle de débit.

Au terme de cette étude, il faut remarquer que le service AS souffre d'un délai de transit supérieur à celui du service GS dans les mêmes conditions de trafic. Ceci valide les choix de mise en oeuvre des services dans l'interface de sortie.

4.2. Étude des services en présence mutuelle

Cette étude a pour but d'évaluer l'influence sur leur QoS du nombre de flot AS et GS générés conjointement quand le réseau est saturé par du trafic BE. Pour ces mesures (voir le tableau 4), les flots AS et GS sont émis depuis les hôtes BSD_A et BSD_B à destination de l'hôte BSD_C . Deux cas de figure sont considérés :

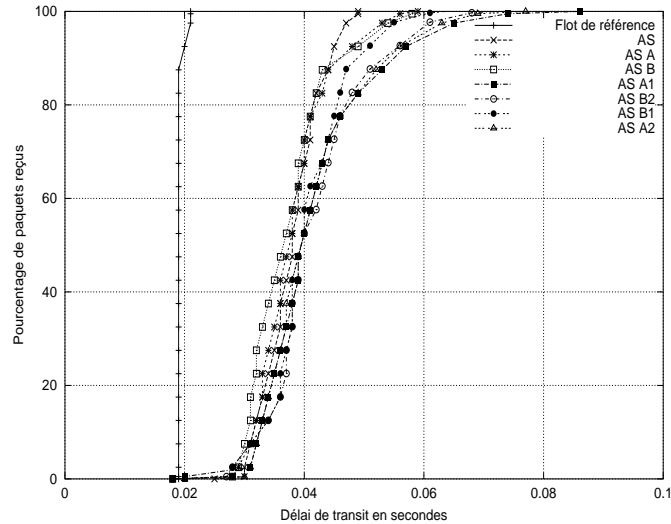


Figure 6. Répartition du délai de transit du service AS

– 1 flot AS est généré par l'hôte BSD_A avec un débit correspondant à 100% de R_{AS} ; parallèlement, 1 flot GS est généré par l'hôte BSD_B avec un débit moyen équivalent à R_{GS} ;

– 2 flots AS sont générés par les hôtes BSD_A et BSD_B avec un débit moyen correspondant chacun à 50% de R_{AS} ; parallèlement, 2 flots GS sont générés par les hôtes BSD_A et BSD_B ayant chacun un débit équivalent à 50% de R_{GS} .

Un flot BE est toujours généré à un débit équivalent à celui de la capacité du goulot d'étranglement soit de 1 Mbits/s.

	R_{GS} ou R_{AS}
AS (BSD_A)	100
GS (BSD_B)	100
AS _A (BSD_A)	50
AS _B (BSD_B)	50
GS _A (BSD_A)	50
GS _B (BSD_B)	50

Tableau 4. Les 2 cas étudiés de la génération de trafic

L'influence du nombre de flots GS (resp. AS) sur la QoS AS (resp. GS) est presque nul. En effet, le tableau 5 indique une variation inférieure à 6 ms pour AS et 2 ms pour GS sur la valeur moyenne du délai de transit. Ce résultat est illustré par la figure 7. Là encore, le taux de perte est inchangé (nul). Notons que les délais de transit sont quasiment les mêmes que ceux observés dans l'étude des services en isolation. Enfin la figure 7 montre bien des délais plus faibles pour le service GS par rapport à celui de

AS. La différence provient du terme de paquets comme expliqué dans la partie 2.1.2. La différence entre les ordonnanceurs WFQ et PQ s'atténue quand la taille des paquets diminue [FER 00]. L'étude des services en présence mutuelle valide donc le choix des mécanismes mis en oeuvre dans l'interface de sortie.

Délai(ms)	AS	GS	AS _A	AS _B	GS _A	GS _B
min	19	18	17	17	17	18
moyen	42	26	47	48	27	28
max	61	42	78	88	41	40
% de perte	0	0	0	0	0	0

Tableau 5. Répartition du délai de transit

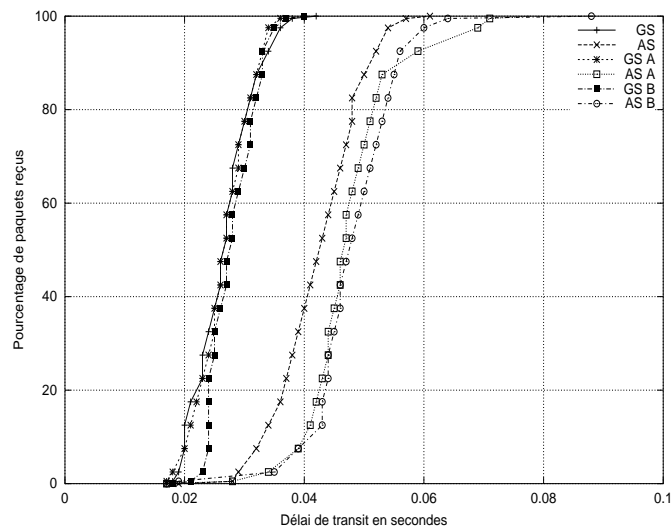


Figure 7. Évaluation des services en présence mutuelle

4.3. Étude du service AS pour les flots élastiques

Le service AS vise à donner une garantie de QoS à un flot en terme de débit et cela quelque soit la composition de l'agrégat. L'objectif de cette étude consiste à évaluer l'adéquation du service AS pour les flots élastiques. Dorénavant, la source de trafic doit pouvoir changer son débit en fonction de l'état de charge de la route. Des paquets avec des priorités spatiales différentes vont constituer le flot applicatif. A la différence des études précédentes, c'est le marquage de la priorité spatiale qui est contrôlé et non plus le débit de génération des paquets. Les mesures sont effectuées en utilisant TCP. Les flots de données reposant sur le protocole de transport TCP présente un caractère élastique de par le mécanisme de contrôle de congestion de TCP. Le débit

est défini pour TCP comme la quantité de bits reçus par le récepteur (à l'exclusion des retransmissions) pendant la durée d'un transfert. Dans le cas présent, ceci correspond au débit utile (*goodput*).

La méthode retenue s'appuie sur un flot AS nommé "flot de référence" généré depuis BSD_A . Son comportement est mesuré selon le nombre de flots supplémentaires générés par la machine BSD_B composant l'agrégat. Les tests se déroulent de la façon suivante :

- un flot BE en UDP est émis en permanence depuis la machine BE (voir figure 4) à un débit équivalent au goulot d'étranglement afin de maintenir l'interface de sortie du routeur dans un état de congestion,
- Chaque flot AS est émis en TCP et l'ensemble des flots de l'agrégat commence tous en même temps pour une durée de 120 secondes. Un flot représente le transfert d'un fichier (*bulk transfer*).
- chaque seconde, le générateur de trafic donne une évaluation du débit utile du flot de référence. En fin de test, celui-ci fait la moyenne des résultats obtenus et retourne en plus la valeur minimale et maximale. Cette mesure est faite par la machine source BSD_A ,

Le débit du goulot d'étranglement est fixé à 10 Mbits/s. La taille de la file d'attente PBS (voir paragraphe 2.1.2) est fixée à $64Ko$ correspondant à la taille maximum par défaut de la fenêtre TCP et pour seuil, la moitié : $32Ko$ [ZIE 01].

Lorsque des évaluations sont faites avec TCP, il faut prendre garde à ce que la voie de retour des acquittements ne soit pas saturée [PAP 01]. Les mesures faites ici ne concernent que l'augmentation du nombre de flot dans un agrégat composé uniquement de segment de données. La voie retour prise par les acquittements est isolé de la voie aller de par la configuration des expérimentations et de l'utilisation de liens *full-duplex* de la plate-forme de tests.

Le dimensionnement du service AS (noté R_{AS}) par rapport au trafic AS offert joue un grand rôle dans l'assurance de débit offert à TCP. De manière évidente, l'assurance de débit du service AS n'est valable que si le service est convenablement dimensionné. A savoir, tant que la condition suivante est vraie :

$$\sum_{i=0}^n r_i \leq R_{AS} \quad (1)$$

avec n le nombre de flots de l'agrégat dans le service au niveau du goulot d'étranglement, r_i le débit assuré du flot i (le débit des paquets IN), R_{AS} le débit garanti au service AS. Lorsque le service comporte de la bande passante en excès (par rapport à la demande), une assurance de débit peut être donnée indépendamment des cinq paramètres qui peuvent affecter le débit de TCP (RTT(*Round Trip Time*), nombre de flots, débit voulu, taille des paquets, flots non-réactifs) [SED 99] [GOY 00] [REZ 99]. Bien que la distribution de la bande passante en excès dépend de ces cinq paramètres. Dans la présente étude, le service est dimensionné convenablement mais sans bande passante en excès.

Dans le cas le plus favorable, un flot de référence en-profil est agrégé avec plusieurs flots hors-profil. Dans ces conditions, les paquets du flot de référence sont tous marqués IN et ne sont concurrencés que par des paquets marqués OUT. Le résultat est illustré par le tableau 6 et par la figure 8. Le tableau 6 indique qu'à partir de dix flots hors-profil, la file PBS est pleine et accuse quelques pertes de paquets opportunistes. Le flot de référence reste quant à lui constant au niveau du délai et de son débit utile quelque soit le nombre de flots hors-profil arrivant au routeur. Ce test démontre qu'un contrôle de la bande passante peut être obtenu par une priorité spatiale [CLA 98]. Ce test définit la borne supérieure de la QoS AS.

Nb. de flots hors-profil	0	1	2	3	5
Débit utile Mbits/s	4.930	4.824	4.823	4.728	4.718
RTT en ms	1.662	1.698	1.699	1.733	1.736
Perte de paquets IN	0	0	0	0	0
Perte de paquets OUT	0	0	0	0	0

	10	20	30	50	100
Débit utile Mbits/s	4.697	4.703	4.650	4.598	4.583
RTT en ms	1.744	1.742	1.762	1.782	1.787
Perte de paquets IN	0	0	0	0	0
Perte de paquets OUT	0.27%	2.36%	4.27%	7.58%	13.4%

Tableau 6. Débit utile du flot de référence en-profil en fonction du nombre de flots hors-profil

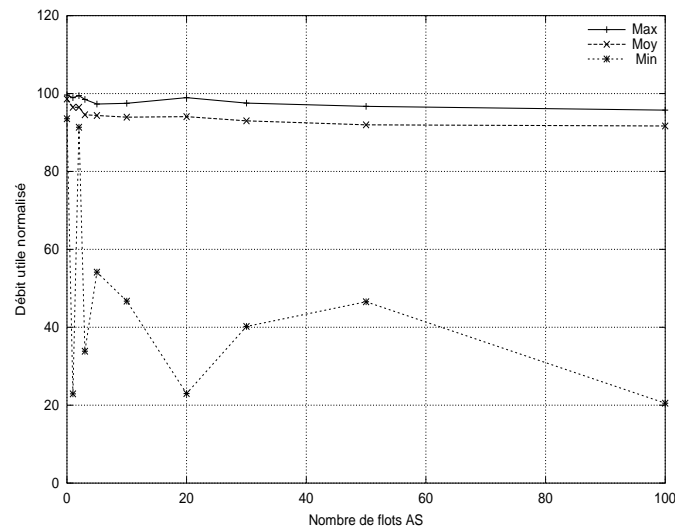


Figure 8. Débit utile normalisé du flot de référence en fonction du nombre de flots hors-profil

Dans le cas normal, le flot de référence est conditionné selon un profil défini par les paramètres (r, b) d'un *leaky bucket*. Dans [REZ 99], il est noté que la taille du seau a une influence sur l'assurance de débit pour les flots qui ont une assurance de débit importante dans le cas d'un service sur-dimensionné. Le sur-dimensionnement est défini comme :

$$\sum_{i=0}^n r_i \leq 0.4 * R_{AS} \quad (2)$$

Cependant, l'augmentation de la taille du seau combinée avec la sporadicité inhérente de TCP accroît les rafales de paquets IN. Dans le cas du dimensionnement utilisé dans la plate-forme de test, des congestions conjoncturelles peuvent se produire pouvant conduire à des pertes de paquet IN. Pour éviter ce genre de situation, la taille du seau b est invariable et est équivalente à la taille d'un paquet, soit 1024 octets. L'assurance de débit du flot de référence sera indiquée par le paramètre r . Quatre cas de figure sont retenus pour $R_{AS} = 5 \text{ Mbits/s}$; le débit assuré du flot de référence r_{ref} varie de 1 à 4 Mbits/s avec un pas de 1 Mbits/s. Le débit assuré d'un flot i de l'agrégat vaut selon l'équation (1) :

$$r_i = \frac{R_{AS} - r_{ref}}{n - 1} \quad (3)$$

La figure 9 représente l'évolution du débit utile normalisé par rapport à R_{AS} du flot de référence en fonction du nombre de flots AS supplémentaires. Cette figure montre une forte variation du débit du flot de référence lorsque que le nombre de flots AS augmente. Le flot de référence n'est pas isolé des conditions de trafic. De plus, le taux de perte des paquets hors-profil du flot de référence augmente quand le nombre de flots AS augmente. Enfin, l'augmentation du taux r du *leaky bucket* du flot de référence ne se traduit pas par une augmentation significative du débit utile pour ce dernier. Quand n tend vers l'infini, le débit du flot de référence converge quelque soit son profil. Enfin, très logiquement, un flot avec un débit minimum faible atteint plus facilement son objectif qu'un flot avec une forte assurance de débit. L'explication provient de TCP qui réagit par un facteur multiplicatif à la perte et par un facteur additif aux transmissions réussies. Il en résulte un temps différent pour retrouver la taille de la fenêtre de contrôle de congestion permettant d'émettre au débit minimum [YEO 99]. Ce test montre également que le *leaky bucket* est un très mauvais marqueur pour les flots TCP car il ne prend pas en compte la sporadicité de TCP [LIN 99]. Des rafales de paquets hors-profil sont émis et peuvent entraîner des pertes en séquence. Il est connu que TCP a des problèmes de performance lorsque la connexion souffre de pertes en rafale [FAL 95].

A noter que ses résultats sont indépendants de la gestion de la file d'attente du routeur. En effet, il a été observé par des simulations étendues sur les agrégats de flots TCP que la gestion de la file d'attente du routeur a une faible influence sur le débit utile et le taux de pertes [QIU 01]. Cependant, une gestion probabiliste de la file d'attente tend à rendre le partage de la bande passante plus équitable. Il y a tout de même une diminution linéaire du débit utile de TCP au fur et à mesure que le nombre de connexions augmente.

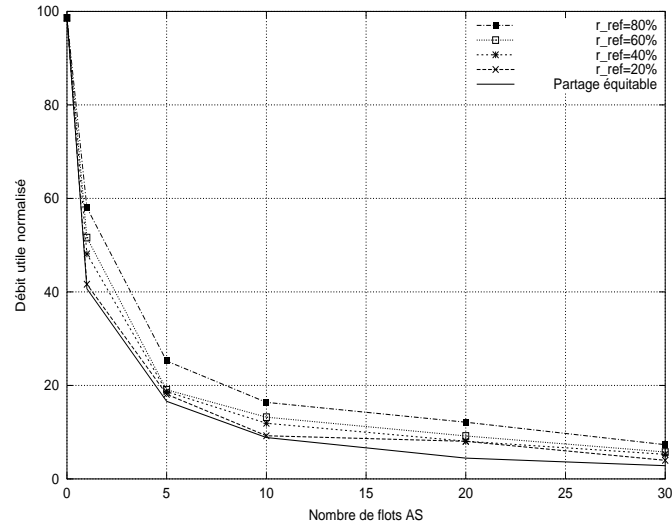


Figure 9. Débit utile normalisé du flot de référence en fonction du nombre de flots AS

Les principales conclusions de cette expérience sont qu'il n'est pas possible d'effectuer une différenciation de service entre les flots TCP par un marquage selon un simple *leaky bucket*. Cette analyse rejoint celle faite par plusieurs études dont celle de [SAH 00]. Enfin, la perte d'un paquet pour TCP, qu'il soit dans le profil ou hors profil, est préjudiciable au débit utile du flot. TCP réagit à la perte sans distinction de la priorité associée au paquet. Dans [FEN 97], il est proposé un contrôle de congestion à deux fenêtres : une pour chaque partie du service AS.

Quelles solutions ?

La figure 10 reprend l'expérience précédente mais une remise en forme du flot de référence est effectuée selon son profil (tous les paquets sont dans le profil). Le flot de référence obtient un débit constant quelque soit le nombre de flots dans l'agrégat. Ceci démontre bien que la perte d'un paquet hors-profil est préjudiciable au débit assuré et que la politique de marquage a donc un rôle prédominant dans la différenciation de services. Cependant, le lissage du trafic ne peut être une solution pour obtenir une différenciation de services car en émettant aucun paquet hors-profil, le débit de la source est limité à son débit minimum (indiqué par le profil). Elle ne peut donc concourir à obtenir la bande passante en excès si elle existe. Dans ce cas, le service AS peut devenir un service moins performant que BE.

Les propositions de marquage pour TCP se divisent en deux familles : celles qui traitent du marquage d'un flot TCP avec un profil sur un agrégat, et celles qui traitent du marquage du flot TCP par rapport à un profil individuel. La première vise la propriété d'équité en plus de l'assurance de débit recherchée par la seconde. Par exemple dans [YEO 01], il est décrit un marquage équitable de flot TCP dans un agrégat en uti-

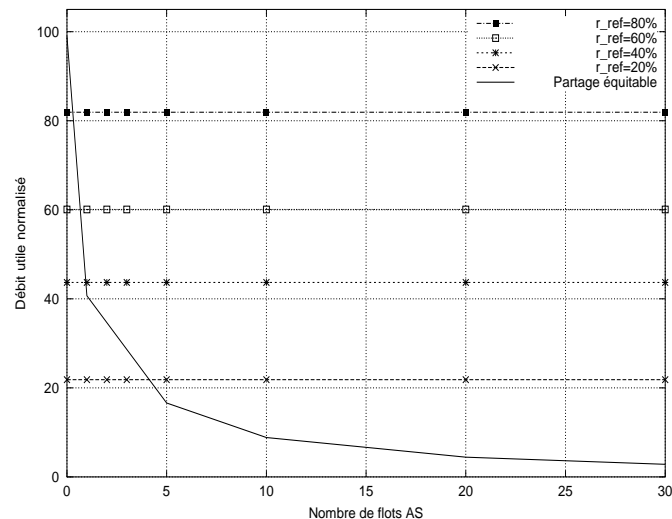


Figure 10. Débit utile normalisé du flot de référence lissé en fonction du nombre de flots AS

lisant un modèle de TCP qui repose sur le RTT et la taille du paquet. Plus récemment, un *leaky bucket* à configuration dynamique a été proposé [CHA 02] pour le marquage d'un flot TCP selon un profil par flot.

Les enseignements tirés au terme de l'évaluation du service AS pour les flots élastiques amènent à penser qu'il est possible d'effectuer une différenciation entre les flots par une priorité spatiale mais que cette différenciation dépend en grande partie du conditionnement.

5. Conclusions et travaux futurs

Les travaux présentés dans cet article posent le problème de la QoS dans l'Internet et portent sur la conception, l'implémentation et la mesure des performances d'une architecture de communication à QoS garantie, supportant des services différenciés au niveau IP et une QoS par flot de bout en bout. Les principes de conception de l'architecture ainsi que sa mise en oeuvre ont été exposés dans la partie 2. Les évaluations de la QoS offerte au niveau utilisateur ont été exposées et analysées dans la partie 4.

Plusieurs conclusions peuvent être tirées ; elles étendent celles données dans [GAR 01], qui étaient les suivantes : (1) une architecture à services différenciés au niveau IP peut être facilement déployée dans un environnement de type VPN (*Virtual Private Network*) tel que celui de @IRS ; (2) une différenciation de services existe entre les services GS et AS selon le paramètre du délai. Cette conclusion est appuyée par l'étude de faisabilité du déploiement des mécanismes de QoS dans un routeur [GUE 99]. Cette

étude montre que la QoS peut être déployée avec un coût minimal sur les performances des routeurs.

Les mesures présentées dans cet article permettent d'apporter les conclusions supplémentaires suivantes. Pour des flots (AS ou GS) respectant leur profil de trafic : (1) l'influence du nombre de flot GS sur la QoS GS est faible ; (2) les services sont isolés les uns des autres ; et (3) un flot élastique utilisant le service AS n'a pas d'assurance de débit. La cause principale en revient au marquage et que le marquage selon un *leaky bucket* est inadapté à la caractérisation d'un flot TCP.

Les perspectives de ces travaux actuellement en cours de développement sont multiples. La première consiste à évaluer (au moyen du simulateur *ns*) l'influence des paramètres de niveau IP (taille des files des routeurs, poids des WFQ, etc.) sur la QoS ; en effet, la valeur exacte des paramètres mesurés en dépend en grande partie. La seconde perspective est de formaliser les sémantiques de garantie associées aux paramètres de QoS, de façon à établir un lien entre la relative imprécision du service AS et la marge d'erreur qu'une application peut tolérer pour certains de ses flots. La troisième est le développement d'un mécanisme de marquage adapté à TCP afin de contrôler la différenciation de débit entre les flots quelque soit la composition de l'agrégat. Enfin, la quatrième perspective est de développer un mécanisme (activé par l'API) permettant au programmeur d'une application de faire abstraction du choix des services de niveaux IP et Transport lors de l'accès au système de communication. La motivation sous-jacente à cette proposition est que le système de communication actuel nous semble difficile à utiliser pour un programmeur n'ayant pas de solides compétences en réseau. Ce mécanisme de sélection est basé sur une caractérisation *a priori* des services GS et AS (fonction de répartition du délai de transit et pourcentage de perte), dont nous faisons l'hypothèse qu'elle est envisageable entre deux sites, moyennant un routage faiblement dynamique. Cette hypothèse, que nous souhaitons soutenir de façon exhaustive en simulation, est confortée par le résultat des mesures effectuées sur la plate-forme @IRS. Plus prospective, la dernière perspective est d'étendre ces travaux à un contexte multidomaine.

6. Bibliographie

- [AQU] « Adaptive Resource Control for QoS Using an IP-based Layered Architecture », <http://www-st.inf.tu-dresden.de/aquila/>.
- [BEN 96] BENNETT J. C. R., ZHANG H., « WF2Q : Worst-Case Fair Weighted Fair Queueing », *Proc. of IEEE INFOCOM*, vol. 1, 1996, p. 120-128.
- [BEN 01] BENNETT J. C. R., BENSON K., CHARNY A., COURTNEY W. F., BOUDEC J.-Y. L., « Delay Jitter Bounds and Packet Scale Rate Guarantee for Expedited Forwarding », *Proc. of IEEE INFOCOM*, 2001, p. 1502-1509.
- [BLA 98] BLAKE S. et al., « An Architecture for Differentiated Services », RFC n° 2475, décembre 1998, IETF.
- [BON 00] BONALD T., MAY M., BOLOT J.-C., « Analytic Evaluation of RED Performance », *Proc. of IEEE INFOCOM*, vol. 3, Tel-Aviv - Israël, mars 2000, p. 1415-1424.

- [BRA 94] BRADEN R., CLARK D. D., SHENKER S., « Integrated Services in the Internet Architecture : an Overview », RFC n° 1633, juin 1994, IETF.
- [CAD] « Creation and Deployment of End-User Services in Premium IP Networks », <http://www.cadenus.org/>.
- [CHA 02] CHAIT Y., HOLLOT C., MISRA V., TOWSLEY D., ZHANG H., « Providing Throughput Differentiation for TCP Flows using Adaptive Two Color Marking and Multi-level AQM », *Proc. of IEEE INFOCOM*, New York, juin 2002.
- [CLA 98] CLARK D., FANG W., « Explicit Allocation of Best Effort Packet Delivery Service », *IEEE/ACM Transactions on Networking*, vol. 6, n° 4, 1998, p. 362-373.
- [DAV 02] DAVIE B., CHARNY A., BENNETT J., BENSON K., AL., « An Expedited Forwarding PHB (Per-Hop Behavior) », RFC n° 3246, mars 2002, IETF.
- [FAL 95] FALL K., FLOYD S., « Comparison of Tahoe, Reno and SACK TCP », *ACM Computer Communication Review*, vol. 26, n° 3, 1995.
- [FEN 97] FENG W., KANDLUR D., SAHA D., SHIN K. S., « Adaptive Packet Marking for Providing Differentiated Services in the Internet », rapport n° CSE-TR-347-97, octobre 1997, IBM.
- [FER 00] FERRARI T., « End-to-End Performance Analysis with Traffic Aggregation », *Computer Networks*, vol. 34, n° 6, 2000, p. 905-914.
- [GAR 01] GARCIA F., CHASSOT C., LOZES A., DIAZ M., ANELLI P., LOCHIN E., « Conception, Implementation and Evaluation of a QoS - Based Architecture for an IP Environment Supporting Differential Services », *IDMS*, septembre 2001, p. 86-98.
- [GAR 02] GARCIA F., AURIOL G., CHASSOT C., LOZES A., LOCHIN E., ANELLI P., « Conception, Implémentation et Mesure des Performances d'une Architecture de Communication à QoS Garantie dans un Domaine IPv6 à Services Différenciés », *9ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'2002)*, Montréal (Canada), 2002, p. 381-394.
- [GEA] « GÉANT : The pan-European Gigabit Research Network », <http://www.dante.net/geant/>.
- [GOY 00] GOYAL M., DURRESI A., JAIN R., LIU C., « Performance Analysis of Assured Forwarding », draft, février 2000, IETF, Internet Draft, draft-goyal-diffserv-afstdy-00.txt.
- [GUE 99] GUERIN R., LI L., NADAS S. J., PAN P., G. V., PERIS J., « The Cost of QoS Support in Edge Devices : An Experimental Study », *Proc. of IEEE INFOCOM*, vol. 2, juillet 1999, p. 873-882.
- [HEI 99] HEINANEN J., BAKER F., WEISS W., WROCLAWSKI J., « Assured Forwarding PHB Group », RFC n° 2597, juin 1999, IETF.
- [LIN 99] LIN W., ZHENG R., HOU J. C., « How to Make Assured Service More Assured », *Proc. of the IEEE International Conference on Network Protocols - ICNP*, Toronto, Canada, novembre 1999, p. 182+.
- [MAY 99] MAY M., BOLOT J., DIOT C., LYLES B., « Reasons Not to Deploy RED », *Proc. of 7th. International Workshop on Quality of Service (IWQoS'99)*, London, June 1999, p. 260-262.
- [NIC 99] NICHOLS K., JACOBSON V., ZHANG L., « A Two-bit Differentiated Services Architecture for the Internet », RFC n° 2638, juillet 1999, IETF.

- [PAP 01] PAPAGIANNAKI K., THIRAN P., CROWCROFT J., DIOT C., « Preferential Treatment of Acknowledgment Packets in a Differentiated Services Network », *Proc. of IEEE/IFIP International Workshop on Quality of Service - IWQoS*, 2001, p. 187-201.
- [QIU 01] QIU L., ZHANG Y., KESHAV S., « Understanding the Performance of Many TCP Flows », *Computer Networks*, vol. 37, n° 3-4, 2001, p. 277-306.
- [REZ 99] DE REZENDE J. F., « Assured Service Evaluation », *Proc. of IEEE GLOBECOM*, Rio de Janeiro, Brasil, décembre 1999, p. 100-104.
- [ROB 98] ROBERTS J., « Quality of Service Guarantees and Charging in Multi-service Networks », *IEICE Transactions on Communications*, n° E81-B(5), 1998.
- [ROC] ROCA V., « BENCH : a Network Performance Evaluation Environment », <http://www.inrialpes.fr/planete/people/roca/bench/bench.html>.
- [SAH 00] SAHU S., NAIN P., DIOT C., FIROIU V., TOWSLEY D. F., « On Achievable Service Differentiation with Token Bucket Marking for TCP », *Measurement and Modeling of Computer Systems*, 2000, p. 23-33.
- [SED 99] SEDDIGH N., NANDY B., PIEDA P., « Bandwidth Assurance Issues for TCP Flows in a Differentiated Services Network », *Proc. of IEEE GLOBECOM*, Rio De Janeiro, Brazil, décembre 1999, page 6.
- [TEI 99] TEITELBAUM B., HARES S., DUNN L., NEILSON R., NARAYAN R., REICHMEYER F., « Internet2 qbone : Building a Testbed for Differentiated Services », *IEEE Network*, vol. 13, n° 5, 1999.
- [TEQ] « Traffic Engineering for Quality of Service in the Internet, at Large Scale », <http://www.ist-tequila.org/>.
- [TFT] « TF-TANT : Differentiated Services Testing », <http://www.dante.net/quantum/qtp/>.
- [YEO 99] YEOM I., REDDY N., « Realizing Throughput Guarantees in a Differentiated Services Network », *Proc. of IEEE International Conference on Multimedia Computing and Systems- ICMCS*, vol. 2, Florence, Italy, juin 1999, p. 372-376.
- [YEO 01] YEOM I., REDDY N., « Adaptive marking for aggregated flows », *Proc. of IEEE GLOBECOM*, San Antonio, Texas, USA, novembre 2001.
- [ZIE 99] ZIEGLER T., FDIDA S., HOFMANN U., « RED+ Gateways for Identification and Discrimination of Unfriendly Best-Effort Flows in the Internet », *IFIP Broadband Communications*, 1999, p. 27-38.
- [ZIE 01] ZIEGLER T., FDIDA S., BRANDAUER C., « Stability Criteria of RED with TCP Traffic », *IFIP ATM&IP Working Conference*, Budapest, juin 2001.