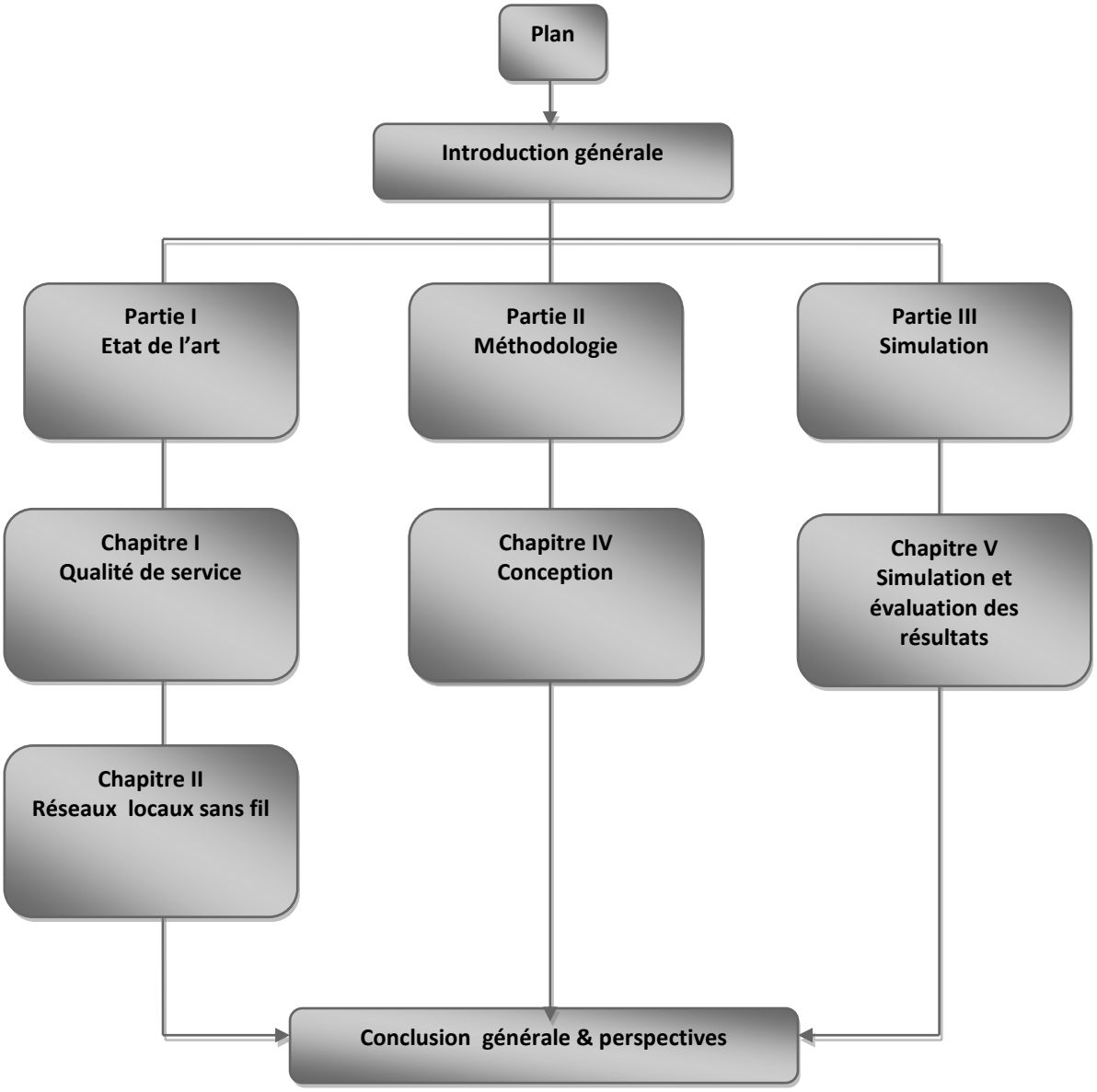
Table des matières

Table des figures

Liste des Tableaux

Plan détaillé

Comme l'illustre la figure si dessous, ce mémoire est décomposé essentiellement en trois parties :



Plan général du mémoire

Résumé

Les réseaux locaux sans fils IEEE 802.11 sont de plus en plus utilisés. Les débits atteints aujourd'hui par ces réseaux permettent d'exécuter des applications complexes nécessitant des garanties sur le débit, le délai ou encore la gigue des communications. Plusieurs travaux de recherches ont été proposés pour apporter un support de qualité de service aux réseaux locaux sans fil dotés de la norme IEEE 802.11. Ces travaux, dont l'IEEE 802.11e, sont pour la plupart basés sur une différentiation de services. Dans ce travail nous proposons une gestion de qualité de service appliquée aux environnements Diffserv et au standard IEEE 802.11e. Cette gestion se base sur le couplage dynamique entre les composants Diffserv et les classes de service EDCA. Pour compléter cette gestion, nous proposons une architecture qui permet d'intégrer les fonctionnalités du conditionneur de trafics afin de limiter le volume du trafic admis dans le réseau pour maintenir la stabilité des files d'attente des classes prioritaires.

Abstract

Wireless local area networks IEEE 802.11 are increasingly used. The flow rates achieved by these networks today run complex applications that require guarantees on throughput, delay or jitter for communications. Several research works have been proposed to provide a quality support service for wireless local networks equipped with IEEE 802.11. These works are mostly based on service differentiation. In this work we propose a QoS management applied to DiffServ environments and IEEE 802.11e. This management is based on the dynamic coupling between Diffserv components and service classes EDCA. To complete this management, we propose an architecture that integrates the functionality of the traffic conditioner to limit the amount of traffic admitted to the networkin order to maintain the stability of queues of priority classes.

clicours.com

Introduction générale

Les réseaux locaux sans fils (ou *Wireless Local Area Network*, WLANs) sont apparus au cours de l'explosion des technologies de communication numérique des années 90 qui suivait elle-même de près celle des supports numériques de la décennie précédente

Les réseaux locaux sans fil WLAN sont en passe de devenir l'une de principales solutions de connexion pour de nombreuses entreprises. Le marché du sans fil se développe rapidement dès l'ors que les entreprises constatent les gains de productivité qui découlent de la disparition des câbles.

Les WLAN ont essentiellement étaient implémentés dans les usines, entrepôts et magasins de détails. Actuellement nombre de domaines profitent déjà de la technologie sans fil, parmi ces domaines : les activités de santé, les institutions éducatives et les bureaux des grandes entreprises.

Les WLANs utilisent des antennes omnidirectionnelles –sauf application spécifique– si bien que toute émission est en fait une diffusion à tous les voisins qui filtrent généralement le trafic pour ne garder que ce qui leur est destiné.

Il y a quelques années chaque type de trafic - voix, données, etc. - avait son propre réseau, dédié et taillé sur mesure. Aujourd'hui les différents flux sont regroupés sur un seul et même support que constituent les réseaux IP. En effet IP est en passe de véhiculer la voix, mais aussi la vidéo. Un bon nombre d'applications fonctionnent dans ce contexte, comme par exemple NetMeeting, NetToPhone, Voix sur IP (VoIP).

Les débits ne cessent donc de grimper et les réseaux sont désormais multiservices. Cette centralisation simplifie grandement les taches des administrateurs et utilisateurs car il n'y a plus qu'une seule infrastructure à gérer.

Cependant, sans régulation du trafic, les réseaux IP se retrouvent vite saturés. La multiplication des flux provoque l'engorgement des liaisons, il faut donc faire la police pour fluidifier la circulation. Afin de pouvoir assurer un niveau de service satisfaisant pour les utilisateurs et améliorer les performances d'un réseau, il convient d'envisager une notion nouvelle : la Qualité de Service (QOS). La généralisation des infrastructures IP dans les entreprises s'accompagne du développement de techniques d'amélioration ou de garantie de la qualité des services proposés.

Fournir une qualité de service (QoS) au sein d'un réseau sans fil est l'une des problématiques de recherche essentielles. Les avancées récentes dans le domaine ont permis la standardisation en 2005 de l'IEEE 802.11e [3] contenant l'ensemble des modifications à apporter au standard IEEE 802.11 afin de fournir une bonne qualité de service. IEEE 802.11e

a introduit, entre autres, une nouvelle fonction d'accès : EDCA (*Enhanced Distributed Channel Access*) qui est basée sur le schéma CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). EDCA introduit à l'ancienne version la possibilité de différencier le trafic à l'accès au médium. Il a aussi été introduit, par le standard 802.11e, la possibilité d'appliquer un contrôle d'admission au flux souhaitant accéder au réseau ; cependant, aucun algorithme de contrôle d'admission n'a été spécifié par le standard.

Dans le cadre de nos travaux, nous nous sommes intéressés à la gestion de quelité de services en se basant sur la différentiation de services et cela en appliquant l'architecture Diffserv (Differentiated Services) [1] qui offre une différenciation par priorité basée sur une classification des paquets à l'entrée du réseau et un traitement différencié à l'intérieur. Une gestion soutenue de la qualité de service par l'architecture DiffServ impose un dimensionnement adéquat du réseau et une configuration optimale des paramètres qui interviennent dans la garantie de la QoS. La gestion de bout en bout de la qualité de service implique la présence de mécanismes spécifiques de gestion de qualité de service à chaque niveau (réseau backbone et réseaux d'accès). Le goulot d'étranglement se situe bien souvent au niveau des réseaux d'accès. L'introduction de la QoS dans ces réseaux devient donc une nécessité, typiquement dans un environnement sans fil. Cependant, elle doit être faite dans deux cas : pour le trafic entrant dans le réseau d'accès et pour le trafic sortant.

Dans le premier chapitre nous commençons par présenter une étude sur la qualité de services dans l'internet en mettant l'accès sur l'architecture de différentiation de services Diffserv. Un état de l'art sur les réseaux sans fils sera exposé dans le chapitre 2. Dans le chapitre 3 nous donnerons une description générale de la qualité de service dans les réseaux locaux sans fil. Le chapitre 4 portera sur la présentation de notre solution proposée ainsi que les résultats des simulations réalisées pour valider notre contribution. Nous terminons par une conclusion générale et des perspectives.

Clicours.COM

Chapitre 1 : Qualité de service

Ce chapitre présente une définition de la qualité de services ainsi que Diffserv qui est une Méthode de différentiation de services pour la gestion de la Qos.

Sommaire

1. Introduction

À ses débuts, Internet avait pour seul objectif de transmettre les paquets à leur destination. Conçu pour le transport asynchrone des données, IP (*Internet Protocol*) n'a pas été prévu pour les applications en temps réel comme la téléphonie ou la vidéo, très contraignantes. Le besoin en équipements de plus en plus fiables, d'un bout à l'autre du réseau, est donc devenu incontournable.

Cependant, les défauts rencontrés sur les réseaux (perte de paquets, congestion) ne peuvent pas être surmontés sans une rénovation profonde de l'architecture.

La qualité de service est la méthode permettant de garantir à un trafic de données, quelle que soit sa nature, les meilleures conditions d'acheminement répondant à des exigences prédéfinies. Elles fixent notamment des règles de priorité entre les différents flux.

La maîtrise de la qualité de service est un enjeu essentiel. La qualité de service doit être visualisée et mesurée de bout en bout.

L'architecture à Différenciation de Services (DiffServ) résulte des efforts menés pour résoudre les problèmes de complexité et de passage à l'échelle posés par IntServ. Le passage à l'échelle devient possible en offrant des services à des agrégats plutôt qu'à chaque flot et en repoussant le traitement par flot aux extrémités du réseau. L'objectif est de laisser le cœur du réseau aussi simple que possible.

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*

2. Définition de la Qualité de service

Selon la recommandation E.800 du CCITT, la qualité de service (QoS pour Quality of Service) correspond à « l'effet général de la performance d'un service qui détermine le degré de satisfaction d'un utilisateur du service ». Cette définition n'est que subjective et reflète la perception de la qualité de service observée par un utilisateur.

Plus techniquement, nous proposons une seconde définition de la qualité de service : la qualité de service constitue, pour un élément du réseau (une application, un hôte ou même un routeur), la capacité d'obtenir un certain niveau d'assurance de telle sorte que la fluidité du trafic et/ou les services requis soient au mieux satisfaits.

Enfin, une troisième définition consisterait à dire que la qualité de service correspond à tous les mécanismes d'un réseau qui permettent de partager équitablement et selon les besoins requis des applications, toutes les ressources offertes, de manière à offrir, autant que possible, à chaque utilisateur la qualité dont il a besoin. Généralement, cette qualité est axée sur le débit, le délai et la perte des paquets : la téléphonie par Internet a pour but de pouvoir converser en temps réel (facteur du délai) sans entre-coupures engendrées par des délais supplémentaires; télécharger une application volumineuse ne demande pas plus que de disposer d'une assez large bande passante pour récupérer le fichier le plus vite possible (facteur du débit) ; les deux applications sont

demandeuses (fermement ou plus souplement) en matière de réception de l'intégralité des paquets (facteur de pertes).

Pour un maximum de fiabilité, la qualité de service requiert la coopération de toutes les couches actives du réseau ainsi que celle de chaque élément du réseau, de bout en bout (figure 1). Des politiques de gestion différentes sont adoptées pour garantir de la qualité de service, selon que l'on se place au niveau des couches du modèle OSI, ou au niveau matériel du réseau (QoS gérée entre les hôtes et les routeurs ou entre les routeurs eux-mêmes).

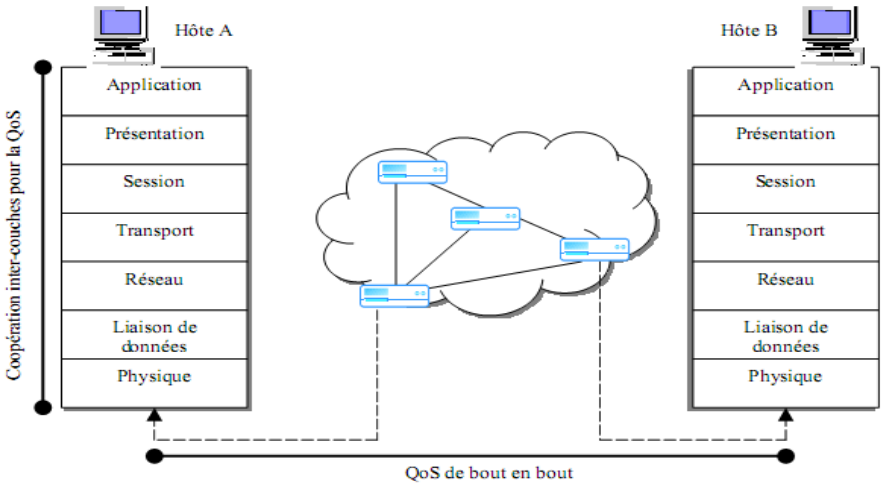


Figure 1 : Perception de la QoS dans les réseaux

Nous pouvons considérer la qualité de service comme un aspect tridimensionnel basé sur trois composantes : une composante « étendue », un modèle de contrôle et une garantie de transmission

Par la composante « étendue » nous définissons les limites de services de qualité de service : par exemple, nous pouvons citer la réservation de ressources d'un flot par le protocole RSVP (Resource Reservation Protocol). La réservation s'effectuera entre les hôtes pour délivrer un niveau spécifié de qualité de service.

Le modèle de contrôle décrit la granularité, la durée et l'emplacement du contrôle des requêtes de qualité de service. Il est alors nécessaire de disposer d'un ensemble flexible de politiques, de pouvoir éviter ou empêcher des failles de qualité de service, etc. Nous pouvons citer à titre d'exemple la technique du contrôle d'admission des flots à l'intérieur d'un réseau, les mécanismes de gestion de files d'attente, etc. [36]

La garantie de transmission est accentuée par la 'mesurabilité' qui consiste à pouvoir disposer de moyens permettant le contrôle des performances du réseau. La performance d'un réseau est évaluée selon le débit et délai de transmission, la largeur et la disponibilité de la bande passante offerte, le taux de pertes des paquets, etc.…

3. Paramètres de garantie de la qualité de service

La notion de qualité de service est, comme nous l'avons précédemment explicité, un aspect multidimensionnel basé sur des critères plus ou moins complexes à pouvoir garantir. Les principaux aspects connus de la qualité de service sont le délai, la gigue, le débit, la bande passante et la disponibilité (souvent exprimée en termes de taux d'erreurs).

3.1. Garanties de délai

L'information qui circule à l'intérieur d'un réseau est hétérogène, tant sur l'aspect de son flux, de sa nature ou de sa fréquence. En effet, les utilisateurs du réseau manipulent aussi bien des applications de transfert de fichiers que des applications multimédia. Contrairement à une opération simple du type de transfert de fichier, le domaine du multimédia requiert beaucoup plus de garanties en matière de qualité de service temporelle. Plus particulièrement, ces dernières applications sont sensibles au délai et à la gigue (variation du délai), mais aussi aux pertes d'information. Ainsi, la téléphonie par Internet, la vidéo-conférence, le multimédia interactif, etc… requièrent de strictes garanties en délai, en gigue et en taux de pertes. Citons à titre d'exemple le cas des jeux interactifs multimédia : les paquets de ces applications, qui subiront un délai de transit significatif ne seront plus correctement utilisés et détérioreront l'efficacité et la synchronisation de l'application. La perte des paquets aura un impact plus accentué sur la qualité du jeu puisque le son et la vidéo seront particulièrement dégradés.

Le terme « délai » englobe en réalité trois aspects temporels différents :

Le délai de propagation, déterminé par la distance physique qui sépare la source de la destination ;

Le délai de transmission dépendant de la taille des flots. Ce paramètre est aussi étroitement lié à l'utilisation du réseau et au partage de la bande passante disponible ;

Enfin, le délai d'attente et de traitement des paquets à l'intérieur des files d'attente, déterminé par la charge du réseau, ainsi que les politiques de traitement de l'information dans les routeurs pour obtenir une fluidité maximale de l'écoulement de l'information.

Garantir le délai implique la nécessité de mettre en œuvre des mécanismes permettant de gérer au mieux l'acheminement de l'information vers la destination en un temps minimal, tenant compte des trois natures de délais précédemment cités. Ainsi, pour minimiser le délai d'écoulement des flots de données, il est nécessaire que ces derniers qui transitent sur le réseau passent un temps négligeable, voire nul, au sein des routeurs. La configuration de ces derniers requiert donc une mise en œuvre de disciplines de services efficaces et adaptées aux besoins des applications pour leur assurer les garanties nécessaires en délais mais aussi en débit.

La gigue, résultant du paramètre « délai », correspond à la variation du délai d'acheminement de bout en bout. Des délais relativement importants éventuellement substitués par les traitements lents des routeurs nuisent automatiquement à la qualité de service par ce paramètre : des variations de délais apparaîtront et affecteront la qualité demandée. Le taux moyen d'erreurs sur une liaison définit la disponibilité d'un réseau. L'efficacité d'un réseau dépend donc des erreurs qui surgissent sur les liaisons. Des taux d'erreurs minimes, voire nuls caractérisent un certain rendement et

paramètrent une bonne qualité de service en matière de disponibilité du réseau. On associe souvent le taux d'erreurs au paramètre temporel, les erreurs affectant directement le transfert des flots, et retardant/bloquant ainsi leur arrivée à destination.

Les délais et les pertes sont les deux facteurs les plus connus qui nuisent aux garanties temporelles et qui engendrent l'amoindrissement des possibilités d'une application, voire rendent celle-ci totalement inefficace et inopérante.

3.2. Garanties de débit

Comme nous l'avons indiqué précédemment, les applications actuelles consomment de plus en plus de bande passante (figure 3), ce qui ralentit ou bloque le déroulement d'autres applications. De même, une utilisation massive du réseau (plusieurs flots provenant de plusieurs utilisateurs traversant le réseau au même instant) entraîne des conséquences de ralentissement de traversée des flots. La notion de bande passante d'un réseau intervient à ce niveau : un minimum de bande passante est requis pour assurer des garanties de qualité de service point à point, demandées à intervalles différents [37]. La capacité d'un réseau doit être suffisamment importante pour pouvoir laisser passer de l'information sans pour autant qu'il y ait de retard d'acheminement, ni de distorsion des flux d'origine en matière de pertes de paquets. C'est pourquoi nous portons davantage notre attention sur le débit de transfert sur le réseau. Ceci nous conduit à traiter les flots à l'intérieur d'un réseau en fonction du débit que chaque application cliente envisage de consommer. Pour cela, des mécanismes sont implémentés dans les routeurs pour contrôler le trafic et le lisser. Les techniques utilisées pour pratiquer le contrôle et le lissage du trafic seront mentionnées dans ce chapitre, et développées dans un prochain chapitre.

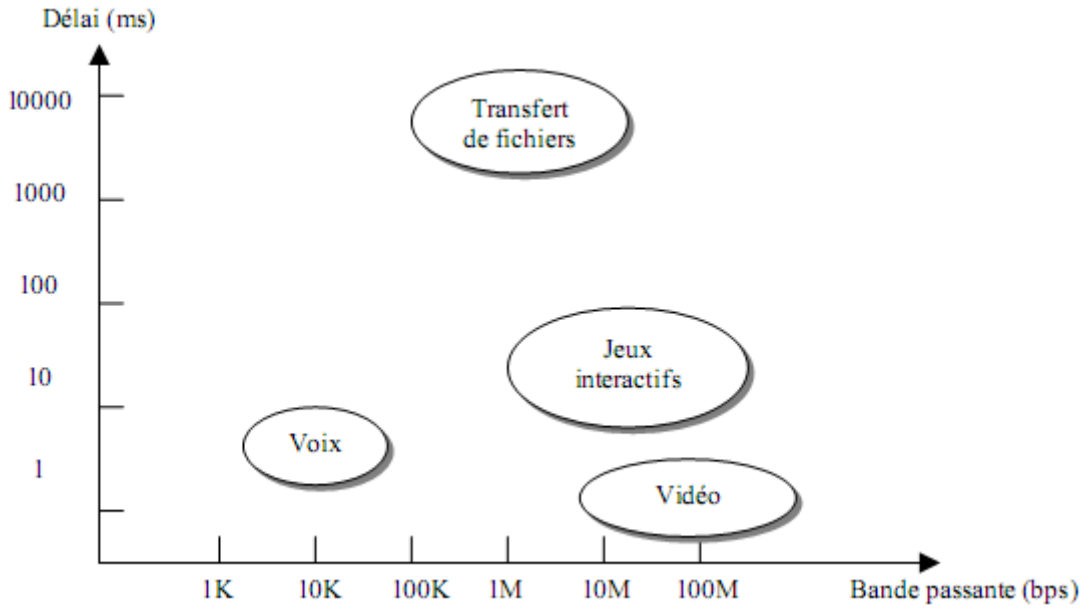


Figure 2 : Besoins en délai et bande passante des applications

4. Le modèle à intégration de services : IntServ

4.1. Définition

Le groupe de travail « Integrated Services » a été développé en 1994 lorsque le multimédia est apparu et est devenu un domaine à part entière de l'Internet. Conçu à la même époque qu'ATM, le système avait pour objectif d'offrir un service semblable sur la couche réseau d'Internet. Le but était donc de pouvoir « améliorer » le réseau Internet et d'en faire un réseau à intégration de services. Il a fallu en effet pouvoir différencier l'utilisation de la bande-passante disponible entre les flots multimédia et les flots de données [42]. Les besoins requis par chacun de ces types de flots n'étant pas les mêmes, le groupe de l'IntServ a défini un ensemble de classes de services qui, implémentées au sein des routeurs, devraient allouer aux flots une certaine qualité de service, à chaque traversée des routeurs, pour les acheminer jusqu'à destination avec cette QoS [43].

Le principe du modèle IntServ repose sur deux fondements [44] :

Tout d'abord, le réseau doit être contrôlé et soumis aux mécanismes de contrôle d'admission des flux ;

La nécessité de disposer de mécanismes de réservation de ressources pour obtenir différents services. Pour cela, l'émetteur envoie une requête de réservation de bande passante qui doit être acceptée par l'ensemble des équipements qui seront traversés par les flux. Le protocole utilisé est le RSVP (Ressource reSerVation Protocol) [45, 46, 47, 48, 49,50].

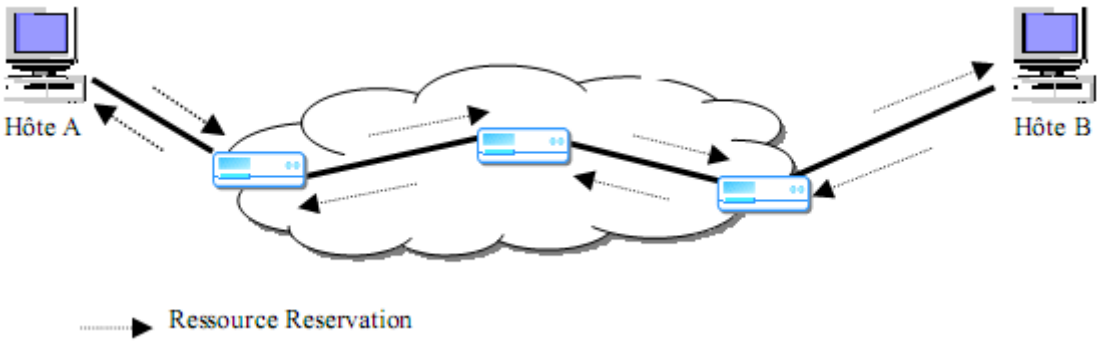


Figure 3 : Principe général du modèle à intégration de service

Les réseaux à intégration de services sont donc constitués de routeurs qui assurent les fonctionnalités de contrôle d'admission de flux et de réservation de ressources. Leur architecture est présentée dans la figure 1.8 :

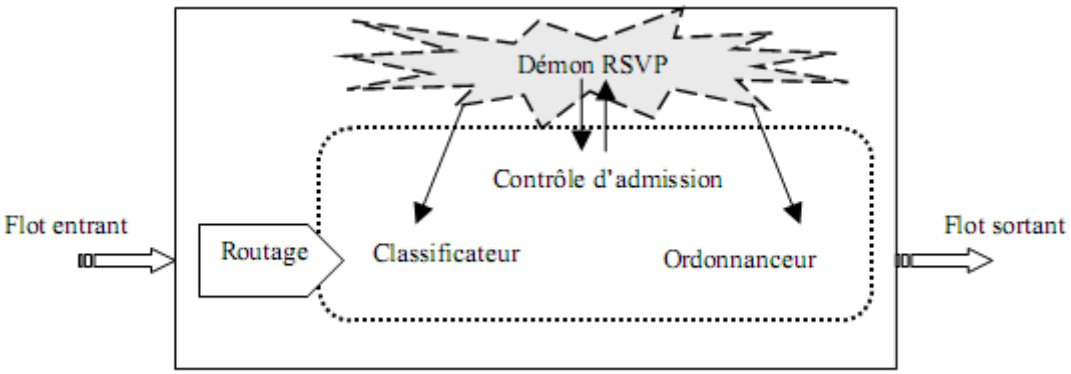


Figure 4 : Modules internes d'un routeur IntServ

Chaque routeur IntServ est ainsi constitué des éléments suivants :

Le classificateur (classifier) accueille les paquets en provenance du module de routage et détermine leur appartenance ainsi que leur type. Par exemple, le classificateur va devoir détecter si les paquets ont besoin ou non d'une réservation, s'ils sont ou non porteurs d'une réservation, etc…

L'ordonnanceur (scheduler) reçoit les paquets du module précédent et gère leur retransmission en utilisant des files d'attente. Tous les paquets qui seront classés par le classificateur et appartenant à une même classe seront traités de la même manière par l'ordonnanceur. Chaque file d'attente implémente des algorithmes de gestion des paquets pour permettre un partage des ressources en fonction des besoins demandés par les utilisateurs. Les algorithmes peuvent par exemple utiliser le principe de partage équitable, le principe de gestion par classe, le principe de priorité, etc… Nous développerons les techniques utilisées par ces algorithmes dans le prochain chapitre ;

Le contrôleur d'admission (admission controller) vérifie s'il est capable de garantir la qualité de service requise par un flot et s'il y a suffisamment de ressources disponibles au moment de l'établissement d'une réservation ;

Un démon du protocole RSVP est en permanence en communication avec les différents composants du routeur. A partir de la requête formulée par une application, il fournit les informations au contrôle de trafic de chacun des routeurs qui appartiennent au flot et récupère la réponse du module de contrôle d'admission.

4.2. Caractérisation des flots

La spécification des flots permet d'expliciter la qualité de service requise par chacun des flots ainsi que les caractéristiques du trafic généré par ceux-ci.

Les besoins de qualité de service spécifiés par une application sont définis selon les paramètres suivants :

La priorité : priorité qui sera attribuée au flot ;

Le débit : débit requis par l'application ;

Le délai : besoin en délai de bout en bout ;

La perte : taux de perte autorisé par l'application.

Pour pouvoir utiliser les services définis pour les réseaux à intégration de services, le groupe IntServ a dû définir et déterminer une propriété pour caractériser les trafics d'un tel réseau. [51] décrit des paramètres de spécification de trafic contenus dans une variable de spécification TSpec (Traffic Specification). La caractérisation s'effectue selon le modèle représenté par la figure ci-dessous : le token bucket (« seau à jetons »).

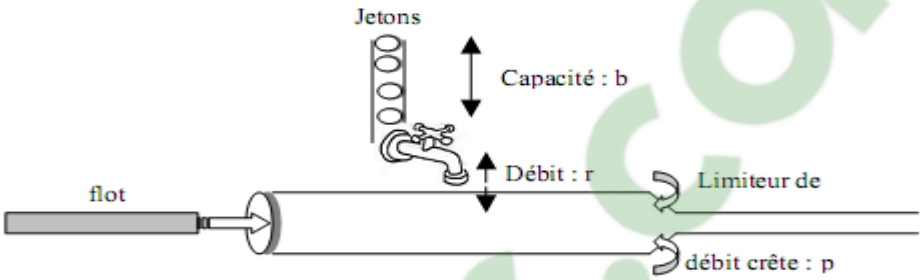


Figure 5 : Principe du Token Bucket

Le token bucket regroupe trois paramètres parmi cinq du TSpec. Tout d'abord, par sa capacité (paramètre b) et par le débit autorisé (paramètre r), il permet de contrôler le débit moyen du flot. Le paramètre p est utilisé pour limiter le débit crête. Les deux autres paramètres de

TSpec qui interviennent dans la spécification des flots sont « la taille maximale » du paquet contenu dans le flot (notée M), et « la plus petite unité de traitement» (notée m). Ces deux paramètres ne caractérisent les flots que par rapport à l'implémentation des mécanismes de qualité de service. Ainsi, on ne pourra garantir une certaine qualité de service qu'aux paquets du flot n'excédant pas la taille maximale définie dans TSpec. Le paramètre « m » indique que tous les paquets dont la taille lui sera inférieure, seront tout de même traités comme un paquet ayant cette taille « m ».

Paramètre	Description
b	Capacité du « seau »
r	Débit moyen délivré par le « seau »
p	Débit crête
M	Taille maximale du paquet
m	Taille minimale de « traitement »

Tableau 1 : Paramètres de spécification d'un flot

4.3. Classes de service

Le groupe de travail IntServ a rendu l'Internet un réseau à intégration de services en distinguant deux classes de services supplémentaires par rapport au service traditionnel du « best-

effort ». Ces nouveaux services sont la classe à charge contrôlée, mieux connue sous le nom « controlled load service », où les performances reçues sont celles d'un réseau peu chargé ; et la classe de service garanti, ou encore « guaranteed service », où l'application qui demande le service possède l'assurance que les performances du réseau vont rester celles dont elle a besoin.

4.3.1. Le service best-effort

Le service dit « au-mieux » (Best-Effort, ou BE) ne garantit aucun critère de qualité de service : ni le délai de transmission, ni l'absence de pertes de paquets, ni l'absence de gigue ne sont considérés pour acheminer les flots de diverses natures. Ce service n'est évidemment pas approprié pour les flux multimédia qui transportent des informations à délivrer en temps réel. Il peut toutefois servir pour le transport de données. La messagerie électronique serait l'application la moins sensible à tous ces critères et supporterait donc sans trop de contraintes, le service du best-effort.

4.3.2. Le service « controlled-load »

Le service de charge contrôlée (Controlled-Load, ou CL) effectue une différenciation entre les trafics et leur attribue des codes de priorité en fonction de la sensibilité des applications [52]

Bien évidemment, ce service est plus adéquat que le best-effort pour les applications multimédia plutôt adaptatives (décrites dans le chapitre 3) très sensibles à la congestion dans le réseau. Il offre un service proche de celui présenté par le best-effort lorsque celui-ci se trouve particulièrement dans des conditions de réseaux non congestionnés. La garantie est donc fournie pour le débit. Mais contrairement au best-effort, le service de charge contrôlée ne détériore pas la qualité du flot lorsque le réseau est surchargé. En effet, les applications qui demandent ce type de service doivent tenir informé le réseau du trafic qui va le traverser, de manière à obtenir une meilleure exploitation du service et du réseau lui-même. Néanmoins, le réseau ne promet pas de garanties temporelles.

La variable de spécification de trafic (TSpec) est nécessaire pour identifier la conformité des paquets par rapport au service. La formule suivante nous montre les besoins auxquels doivent se plier les flots pour bénéficier du service « controlled load ».

$$\text{Durée\_burst} \leq r.M + b$$

La durée d'un burst correspond à la durée nécessaire pour transmettre la taille maximale d'un burst au débit demandé. Si sa durée vérifie l'équation ci-dessus, alors le flot est pris en charge par le service à charge contrôlée ; sinon, le trafic est traité comme du best-effort, ou peut être éliminé.

4.3.3. Le service garanti

Dans [47], les auteurs définissent le service garanti (Guaranteed Service, ou GS) comme étant « un service qui doit assurer de fermes garanties, de telle sorte que le délai de bout en bout mesuré sur les paquets d'un flot n'excède pas une certaine limite ». La classe de service garanti permet de même une garantie de bande-passante. Le service garanti livre les données (applications) en fonction des paramètres négociés et de la classe de service demandée. Le service est défini selon deux paramètres :

TSpec qui caractérise le trafic pour lequel nous demandons le service garanti ; nous avons précédemment défini les paramètres de TSpec ;

RSpec qui permet de spécifier les ressources à réserver. RSpec est défini au moyen de deux éléments :

R (Requested Rate), qui spécifie un taux de service désiré (exprimé en octets/s) pour lequel le trafic sera envoyé. Dans [53] l'auteur démontre que pour réduire le temps d'attente au niveau de la file, on doit avoir R > r (r étant le paramètre de TSpec identifiant le débit moyen du token bucket)

S (Slack term) qui définit la différence entre le délai attendu et le délai obtenu. Cette valeur, exprimée en micro-secondes, permet au réseau d'ajuster le taux alloué pour obtenir les délais requis. Elle peut être utilisée par une entité du réseau pour réduire la réservation locale de ressources d'un flot. Dans certains cas, la présence d'une valeur dans ce champ peut augmenter la probabilité d'effectuer avec succès une réservation de bout en bout. [54]

La classe de service garanti permet ainsi d'apporter aux applications un contrôle considérable du point de vue délai. Le délai d'une application se subdivisant en plusieurs sous-délais, seul le délai d'attente est déterminé par le service garanti , grâce au paramètre R de RSpec (les autres délais sont plutôt liés aux propriétés physiques du réseau). De ce fait, une application peut précisément estimer à l'avance quel délai de mise en attente le service garanti peut offrir. Par conséquent, si le délai d'une application est supérieur à celui attendu, celle-ci peut modifier le token-bucket du trafic ainsi que le taux de données pour obtenir un plus faible délai.

5. Le modèle à différenciation de services : DiffServ

5.1. Principe du service différencié

Le modèle DiffServ [28] a été conçu pour répondre aux limites d'IntServ. L'idée de base est de fournir une qualité de service non par flux, mais par classe de paquets IP tout en repoussant (le plus possible) la complexité du traitement en bordure du réseau afin de ne pas en surcharger le cœur.

L'intérêt d'un tel modèle est de pouvoir s'occuper du problème d'approvisionnement en qualité de service à travers une allocation de services basée sur un contrat établi entre un fournisseur de services et un client.

Pour le groupe de travail DiffServ, un micro-flux de paquet IP perd son identité propre et circule sur Internet en tant que membre d'une classe de flux. L'approche de DiffServ permet donc à des fournisseurs d'offrir différents niveaux de services à certaines classes de flots de trafic rassemblés.

Ainsi, il devient question de supporter un schéma de classification en attribuant des priorités à des agrégats de trafic [60]. De ce fait, les paquets sont classés grâce à un mécanisme de marquage d'octets dans l'en-tête des paquets IP, et les services qui sont octroyés par les routeurs à ces paquets dépendent des classes alors définies [61]. Ce marquage est effectué au niveau de l'étiquette de l'en-

Clicours.com

tête du paquet : le DSCP (DiffServ Code Point) [62] qui se situe dans le champ DS de l'en-tête IP réservé à DiffServ.

Grâce à ce marquage, et à l'approche différente de DiffServ par rapport à IntServ, les routeurs DiffServ gardent une certaine souplesse d'utilisation du point de vue acheminement par rapport à ceux utilisés dans l'IntServ.

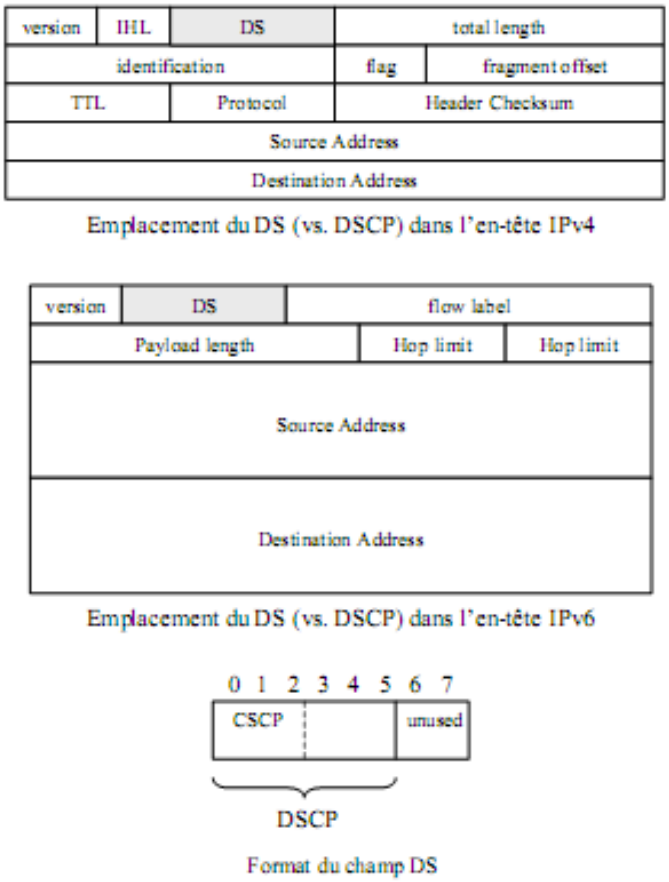


Figure 6 : Positionnement du champ DSCP dans les paquets IP

5.2. Notion de domaine Diffserv

Par définition, l'Internet est constitué d'une interconnexion de réseaux. Cependant, plusieurs de ces réseaux sont souvent rassemblés sous une même autorité administrative (par exemple dans les grandes entreprises, les centres de recherches, les universités, ...) et constituent un domaine. [29] désigne par domaine, un ensemble de nœuds (hôtes et routeurs) administrés de façon homogène.

Dans un domaine, on distingue les nœuds internes et les nœuds frontières : les premiers ne sont entourés que de nœuds appartenant au domaine alors que les seconds sont connectés à des nœuds frontières d'autres domaines (Figure 4). Si on considère le sens de communication de la source vers la destination, les nœuds de frontières peuvent être d'entrée (ingress) dans le domaine ou de sortie (egress).

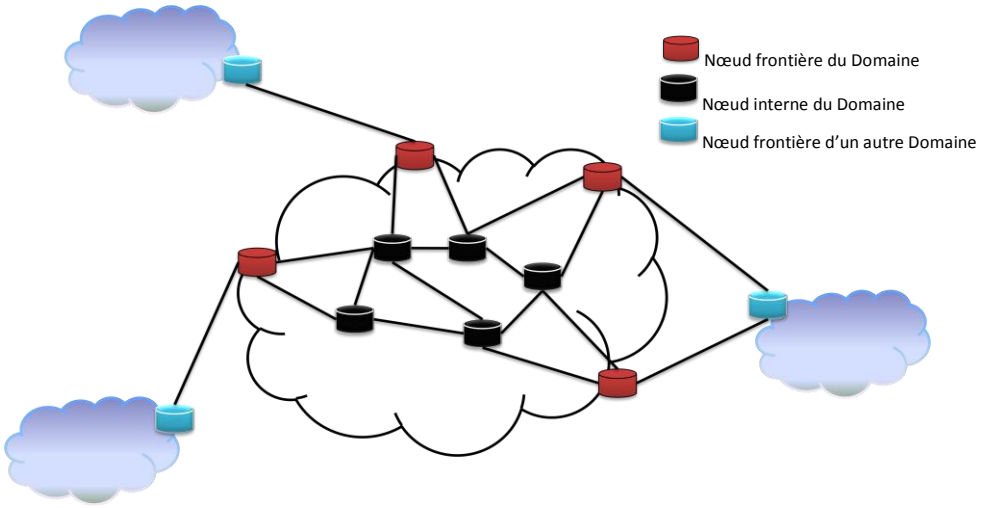


Figure 7 : Distinction des nœuds d'un domaine Diffserv

5.3. La notion de SLA (Service Level Agreement)

L'utilisation des services DiffServ implique pour le client la souscription d'un contrat avec le fournisseur des services : Service Level Agreement (SLA). Ce contrat est signé avant toute connexion au réseau, et non à l'établissement d'une session. Les spécifications techniques du SLA sont contenues dans le SLS (Service Level Specification). Le SLA contient les informations suivantes :

Le trafic que l'utilisateur peut injecter dans le réseau fournisseur (en termes de volume de données, de débit moyen, d'hôtes source ou destination, …) ;

Les actions entreprises par le réseau en cas de dépassement de trafic (rejet, surtaxe, remise en forme du trafic) ;

La QoS que le fournisseur s'engage à offrir au trafic généré ou reçu par l'utilisateur (ou les deux). Celle-ci peut s'exprimer notamment en termes de délai, de bande passante, de fiabilité ou de sécurité.

Pour le moment, seuls des contrats statiques, c'est-à-dire peu susceptibles de changer dans le temps, sont établis, la gestion des contrats dynamiques dont les caractéristiques varient rapidement étant plus complexe.

5.4. La notion de comportement (PHB : Per Hop Behavior)

Au sein d'un domaine DiffServ, tous les nœuds (hôtes et routeurs) implémentent les mêmes classes de service et les mêmes comportements ou Per Hop Behavior: PHB vis-à-vis des paquets des différentes classes. Un comportement inclut le routage, les politiques de service des paquets (notamment la priorité de passage ou de rejet en cas de congestion) et éventuellement la mise en forme du trafic entrant dans le domaine. Les nœuds internes ne doivent pas conserver d'états en mémoire (contrairement à la proposition IntServ) ; ils ne font que transmettre les paquets selon le comportement défini pour leur classe. Les nœuds frontières se chargent de marquer les paquets selon le code réservé à chaque classe.

La RFC 2475 [28] définit le PHB comme le comportement d'acheminement observable de l'extérieur qui s'applique aux données dans un nœud DiffServ. Le système marque les paquets conformément aux codes DSCP et tous les paquets ayant le même code seront agrégés et soumis au même traitement particulier.

Plusieurs PHB standard ont été définis :

- Le PHB par default (default PHB, défini en [29])
- Assured Forwarding (AF) PHB (défini en [30])
- Expedited Forwarding (EF) PHB (défini en [31])

Ces trois classes de services seront décris en détail dans les paragraphes suivants.

5.5. Classes de services de DiffServ

Dans cette approche, on dispose de trois niveaux de priorité : le service « Best-Effort », le service « Assured Forwarding », et le service « Expedited Forwarding ».

5.5.1. Le service « 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. Le principe de bout en bout de l'Internet est aussi adopté pour le contrôle de flux grâce à différents algorithmes comme le *Congestion Avoidance* introduit dans TCP.

Les principaux inconvénients de cette politique de contrôle de flux sont un trafic en dents de scie composé de phases où le débit augmente puis est réduit brutalement et une absence de garantie à long terme.

La valeur DSCP recommandé pour le PHB par défaut est « 000000 ». Un paquet marqué pour le traitement par défaut peut être remarqué en sortie d'un domaine en fonction des contrats SLA convenus entre deux domaines (opérateurs), ainsi un paquet non prioritaire dans un domaine peut se retrouver prioritaire dans un autre domaine.

5.5.2. Le service « Assured Forwarding »

Le comportement Assured Forwarding (AF) est le fruit de plusieurs propositions [63,64,61] qui centraient la différenciation des paquets sur des algorithmes de discrimination des paquets à l'intérieur d'une même file d'attente.

L'AF définit 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.

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 ;

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.

PHB $_{ij}$	Classe 1	Classe 2	Classe 3	Classe 4
Précédence 1	001 010	010 010	011 010	100 010
Précédence 2	001 100	010 100	011 100	100 100
Précédence 3	001 110	010 110	011 110	100 110

Tableau 2 : Codage des DSCP correspondants à AF

[65] impose la contrainte suivante : au sein d'une même classe, les paquets qui appartiennent à la précédence « x » sont prioritaires devant ceux ayant une précédence « y », et ce, pour $x < y$. Ainsi, pour la classe 1, les paquets de précédence 2 seront prioritaires par rapport aux paquets de précédence 3.

Avantages de l'*Assured Forwarding* :

- Peut offrir une meilleure différenciation (classe et priorité).
- Le marquage à l'entrée du réseau est une opération moins coûteuse que le *shaping.*
- Ne ne demande pas une coordination entre domaines.
- Une facturation simple peut être utilisée.

Inconvénients de l'*Assured Forwarding* :

La qualité offerte dépend énormément du niveau d'agrégation et de la présence de flux concurrents

- Il n'existe aucune assurance de délai.
- Il y a beaucoup de paramètres à régler.
- 3 niveaux de priorité ne suffissent pas pour assurer une bonne différentiation sur des liens non-chargés.
- Un mauvais dimensionnement rend inutile la présence de priorités sur des liens en congestion.
- Le marquage ne suffit pas pour protéger TCP de UDP.

5.5.3. Le service « Expedited Forwarding »

Le service Expedited Forwarding (EF) [66] est un dérivé du service « premium » [61] conçu pour servir des applications demandant de faibles pertes, un délai et une gigue très faibles et une garantie de bande-passante.

EF est défini comme un traitement d'acheminement appliqué à un agrégat DiffServ où son débit en sortie dans un nœud quelconque doit être supérieur ou égal à une valeur configurable.

Il correspond à un service critique similaire à un lien dédié ou VLL (Virtuel Leasing Line) dans lequel un débit instantané et un délai instantané sont garantis. EF possède une forte priorité dans les nœuds et doit cependant être contrôlé pour que la somme des capacités provenant des différentes sources et passant par un même nœud ne dépasse pas la capacité de la liaison de sortie. Le trafic en excès est rejeté.

L'EF PHB peut être utilisé pour simuler un lien dédié caractérisé par :

- un faible taux de perte.
- un temps de traversée faible.
- Une gigue minimum.
- un débit garanti.
- Un service de bout en bout au travers d'un domaine DS.

Cependant, la création d'un tel service implique deux pré-requis :

Premièrement, Il faut configurer les nœuds de façon que l'agrégat considéré ait un débit maximum de départ indépendant de l'état dynamique du nœud. L'état des files et des ressources mémoires influent sur l'état de charge du trafic, et par conséquent, la mise en mémoire tampon doit être minimale.

Deuxièmement, Via les fonctions adéquates du Dropping : Rejeter les paquets en excès, et du shaping : retardement des paquets, l'agrégat est conditionné de façon que son débit d'arrivée dans un nœud soit toujours inférieur au débit maximum de départ.

Le trafic EF doit être soumis à un débit de façon indépendante de l'intensité de tout autre trafic traversant le nœud.

Les débits minimum et maximum peuvent être les mêmes et être configurables via un seul paramètre. Ils doivent être configurés par l'administrateur du réseau.

Afin que le trafic EF ne monopolise pas les ressources d'un nœud, l'implémentation doit prévoir des moyens de ne pas nuire aux autres trafics. Le trafic en excès doit être systématiquement détruit.

Dans [66], les auteurs proposent, suite à une étude comparative de technique d'implémentation du PHB, l'utilisation d'une file prioritaire pour les flux typés EF. Le délai observé pour les flux à l'intérieur des files est fortement réduit, mais un problème de famine des autres classes pourrait se manifester si une mauvaise gestion est opérée dans le système. C'est

pourquoi il est nécessaire d'intégrer des méthodes permettant de lisser le trafic EF. Le service EF est un service à forte priorité, délivrant des garanties en matière de bande passante, et permettant des taux de perte, de délai et de gigue faibles [67]. On peut apparenter ce service à celui du service garanti du groupe IntServ.

101 110

Format du DSCP attribué à EF

Nous résumons dans le tableau ci-dessous les différents services selon leur priorité, puis dans la figure 13, nous donnons des exemples d'applications courantes en leur associant les classes de services de l'architecture DiffServ :

Service	Priorité
Best Effort	Faible
Assured Forwarding	Moyenne
Expedited Forwarding	Forte

Tableau 3 : Récapitulatif des priorités de services DiffServ

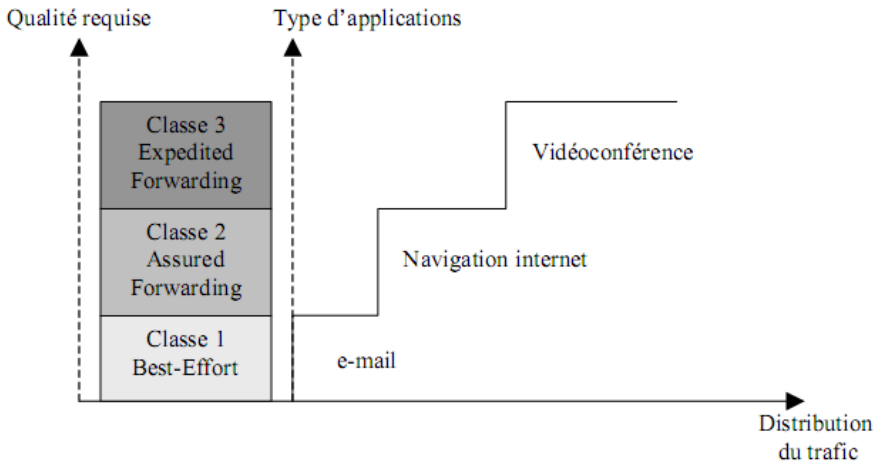


Figure 8 : Qualités requises pour des applications sous DiffServ

5.6. Architecture Diffserv

Le groupe Diffserv propose donc d'abandonner le traitement du trafic sous forme de flots pour le caractériser sous forme de classes. Le [32] préfère d'ailleurs le terme de *behaviour aggregate* (BA) plutôt que de classe de trafic.

Le service différencié de l'architecture Diffserv permet de diminuer les informations d'état que chaque nœud du réseau doit mémoriser. Il n'est plus nécessaire de maintenir des états dans les routeurs pour chacun des flux. Ceci permet son utilisation à grande échelle.

L'idée consiste à diviser le réseau en domaines. On distingue ainsi les routeurs à l'intérieur d'un domaine (*Core router*) des 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. Les routeurs de bordure jouent un rôle différent de ceux qui sont au cœur du domaine. Ils sont chargés de conditionner le trafic entrant en indiquant explicitement sur le paquet le service qu'il doit subir. Ainsi, la complexité des routeurs ne dépend plus du nombre de flux qui passent mais du nombre de classes de service. Chaque classe est identifiée par une valeur codée dans l'en-tête IP.

Le trafic conditionné est identifié par un champ DS ou un marquage du champ *Type of Service* (ToS) de l'en-tête de paquet IPv4 ou l'octet *Class Of Service* (COS) d'IPv6. Ce champ d'entête IP porte l'indice de la Classe de Service DSCP (Differentiated service Code Point). Sachant que ce travail de marquage est assez complexe et coûteux en temps de calcul, il vaut mieux limiter au maximum les répétitions.

Les opérations de classification, contrôle et marquage sont effectuées par les routeurs périphériques (*Edge Router*) tandis que les routeurs centraux (*Core Router*) traitent les paquets en fonction de la classe codée dans l'en-tête d'IP (champ DS) selon un comportement spécifique : le PHB (*Per Hop Behavior*) codé par le DSCP.

Rappel sur le principe du DSCP : *c'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 ou le champ classe de trafic d'IPv6.*

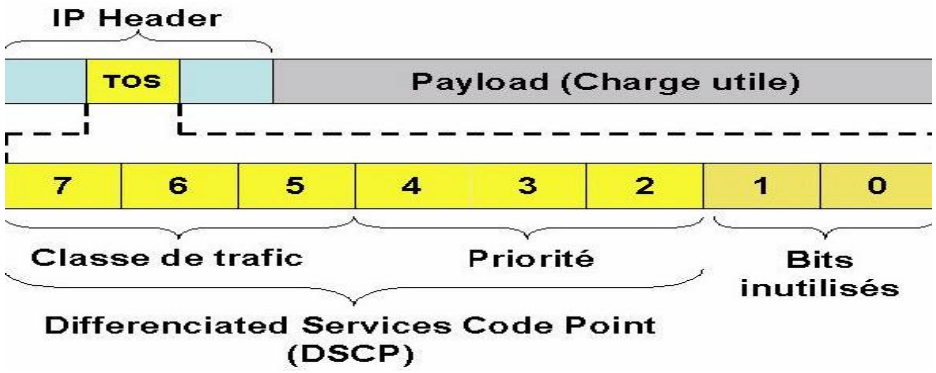


Figure 9 : Entête d'un datagramme IPV4

5.6.1. Architecture des routeurs DiffServ

On peut distinguer les routeurs situés dans le cœur de réseau « Core routers » de ceux situés à sa frontière « Edge routers ». Les routeurs du cœur de réseau du domaine DiffServ réalisent des opérations simples de bufferisation et d'avancement des paquets de chaque flot en se basant uniquement sur le marquage fait par les routeurs situés à la frontière du domaine DiffServ. Les «

Core routers » possèdent les deux mécanismes cruciaux du modèle DiffServ, le Scheduling et le Buffer Management. C'est à ce niveau que la différenciation de service est faite.

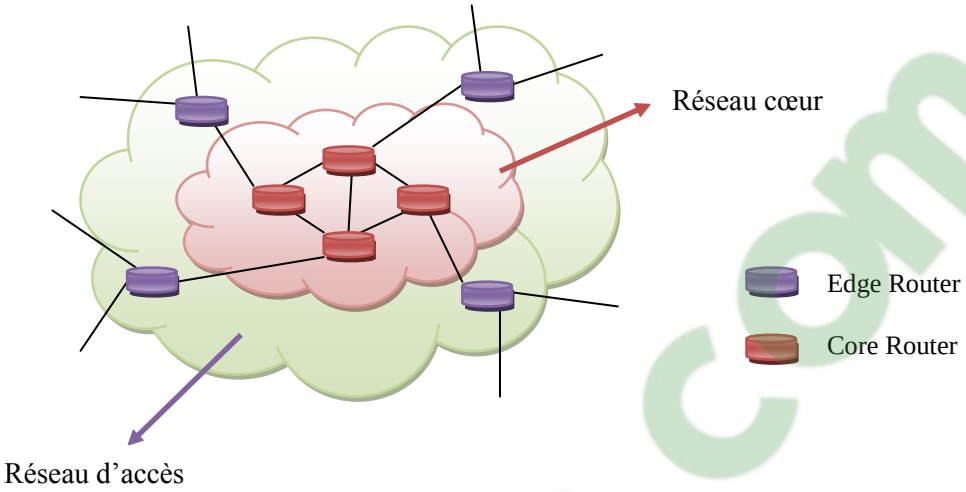


Figure 10 : Aspect général d'un réseau DiffServ

5.6.1.1. Les routeurs de bordure : les « edge routers »

Les routeurs « edge » sont responsables de la classification des paquets et du conditionnement du trafic. L'opération de classification est opérée à l'entrée du réseau, zone où la différenciation de service est mise en œuvre, le domaine DS, pour assurer le traitement ciblé : celui de pouvoir différencier les différents flots qui arrivent dans le réseau.

Ces routeurs sont caractérisés par leur gestion des états par flots. Après classification, les paquets subissent une opération de vérification (module « meter ») qui consiste à déterminer le niveau de conformité pour chacun des paquets d'un même flot. Ces niveaux de conformité varient en fonction du conditionnement requis par le service. On peut définir par exemple deux niveaux « in » et « out » spécifiant si les paquets sont conformes ou non conformes avec le contrat établi.

Cette dernière différenciation est néanmoins utilisée dans l'algorithme d'ordonnancement [68]. L'étape qui suit la vérification du niveau de conformité est de deux types : si les paquets sont conformes, alors ils sont envoyés pour être étiquetés (nous présenterons cette technique ultérieurement). Dans le cas contraire, alors il y a trois manières de traiter les paquets non conformes : mise en forme (shape), marquage (mark) ou élimination (drop) :

- L'opération de mise en forme (shape) a pour but de rendre conforme les paquets qui ne le sont pas, et ce, par simple retardement de son acheminement. Après un certain temps de retardement, les paquets deviendront conformes et seront injectés vers le module d'étiquetage. Cette opération régule les flots suivant les caractéristiques de leur classe. Le plus souvent cela est fait par la technique du token bucket; des utilitaires de fragmentation et de compression peuvent y être associés (LFI et RTP de CISCO).

- Le processus d'élimination (drop) est nécessaire pour assurer un fonctionnement fiable du routeur : tous les paquets qui ne sont pas conformes seront forcés à être éliminés. Les flots pour

lesquels il serait préférable d'utiliser cette méthode sont les flots interactifs. En effet, si on choisit d'appliquer la mise en forme pour ce type de flots, les paquets subiront un retard significatif et rendront l'interactivité de l'application impossible. C'est pourquoi il leur est préférable d'être éliminés.

- Enfin, le mécanisme de marquage (mark) a pour effet d'attribuer une priorité aux paquets en fonction du résultat fourni par l'opération de vérification. C'est à ce niveau qu'est réalisée l'agrégation des flots en classes. Le Marker détermine le PHB (Per Hop Behavior) du paquet, et en accord avec les informations transmises par le Meter, positionne le champ DSCP (marquage de la classe). Il est important de noter que cela n'est pas fait par le classifier, car un même flot suivant les conditions de trafic peut être marqué différemment.

Avant d'être envoyés vers l'intérieur du réseau, les paquets subissent une dernière opération : l'étiquetage effectif du champ DSCP. La valeur attribuée au champ correspond au résultat de toutes les opérations précédentes. Celle-ci peut être modifiée au sein d'autres routeurs de bordure, selon le nouveau conditionnement qui va être appliqué au flot après sa traversée dans les équipements. La marque qu'un paquet reçoit identifie la classe de trafic à laquelle il appartient. Les paquets ainsi marqués sont alors envoyés dans le réseau avec cette mise en forme.

En bref la fonctionnalité du routeur de bordure est le conditionnement du trafic. Ce dernier peut donc contenir un ensemble d'éléments tels que le vérificateur, le marqueur, le « shaper » et le « dropper ». En effet, une fois un flot de trafic est choisi par un classificateur, il le dirige vers un module de conditionnement spécifié pour continuer le processus de traitement. Un conditionneur de trafic peut ne pas contenir nécessairement chacun des quatre éléments tels que le cas où aucun profil de traitement n'est présent (les paquets peuvent seulement passer par un classificateur et un marqueur).

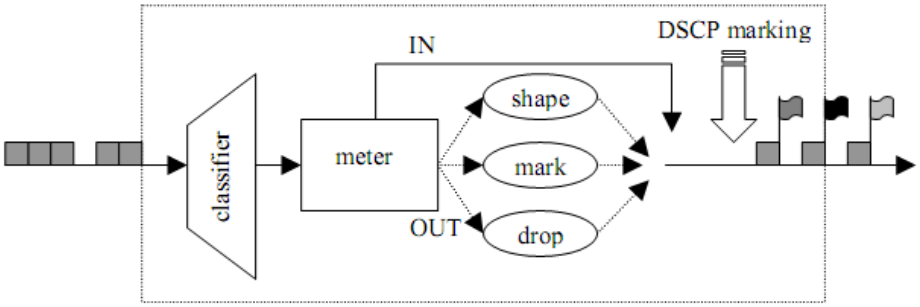


Figure 11 : Principe de fonctionnement d'un routeur « edge »

5.6.1.2. Les routeurs de cœur : les « 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. 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. [32]

Dans un routeur DiffServ du cœur de réseau, chaque sortie possède un nombre fixe de files d'attente logiques où le routeur dépose les paquets arrivants sur la base de leur PHB. Les files d'attente sont servies en accord avec l'algorithme d'ordonnancement.

Le « core router » est constitué de trois éléments principaux. Le routage proprement dit qui consiste à la détermination du PHB, le scheduling et la gestion de buffer (cf. figure ci-dessous)

• **Routage :** Cette opération consiste à aiguiller le paquet vers un port de sortie et à déterminer son nouveau PHB.

• **Scheduling :** Plusieurs politiques d'ordonnancement peuvent être utilisées : WFQ, WRR ou priorités fixes. A l'heure actuelle, il semblerait que les opérateurs s'orientent vers une combinaison de ces politiques avec une priorité fixe pour le trafic temps réel et un ordonnancement WFQ pour les autres classes. C'est le champ DSCP des paquets qui permet d'affecter les paquets à une file d'ordonnancement particulière.

WFQ (Weighted Fair Queuing) :

Chaque file d'attente comporte un poids, par exemple 70 pour la file EF, 20 pour la file AF Gold et 10 pour l'autre file AF. L'ordonnanceur laisse passer pendant 70% du temps les clients EF. Si ces clients dépassent l'utilisation de 70%, l'ordonnanceur accepte de laisser passer des clients AF Gold pendant 20% du temps restant et pendant 10% des clients AF Silver ou Bronze. [35]

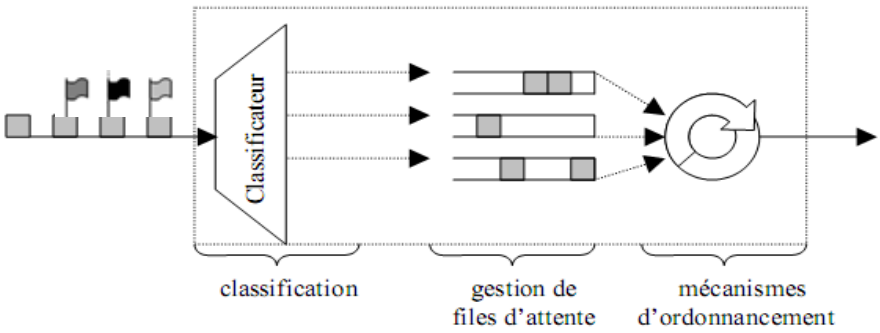


Figure 12 : Architecture d'un routeur interne

Comme le montre la figure 17, le classificateur envoie les paquets vers différentes files d'attente, selon l'identificateur placé dans le champ DS, préalablement marqué par les routeurs d'entrée du réseau (les routeurs « edge »). Seule une partie du champ permet d'indiquer la file d'attente appropriée : il s'agit du champ CSCP (Class Selector Code Points)

Clicours.COM

Un troisième type de routeur est mis en jeu dans des réseaux utilisant DiffServ. Il s'agit des routeurs de bordure (border router) placés en sortie des domaines DS pour relier deux réseaux DS.

Leur fonction consiste à remarquer les paquets et de les remettre en forme pour les acheminer vers le sous-réseau suivant DS à travers les routeurs de bordure.

La figure 18 présente l'architecture d'un réseau à différenciation de services, et montre les différents types de routeurs utilisés pour bénéficier de ce type de services. Nous distinguons deux sous-réseaux DS utilisant chacun les principes de DiffServ. Ces deux sous-réseaux sont reliés entre eux par des routeurs de bordure ; les routeurs de cœur peuvent être reliés entre eux, ou à des routeurs de bordure ou encore à des routeurs « edge ». Enfin, les hôtes sont directement rattachés aux routeurs « edge ». Entre ces derniers et les domaines DS, des contrats de service appelé SLA (Service-Level Agreement) sont mis en œuvre pour spécifier les classes de service supportées et la quantité de trafic autorisée pour chaque classe [69]. Ces informations sont nécessaires à connaître si un client désire obtenir des services différenciés.

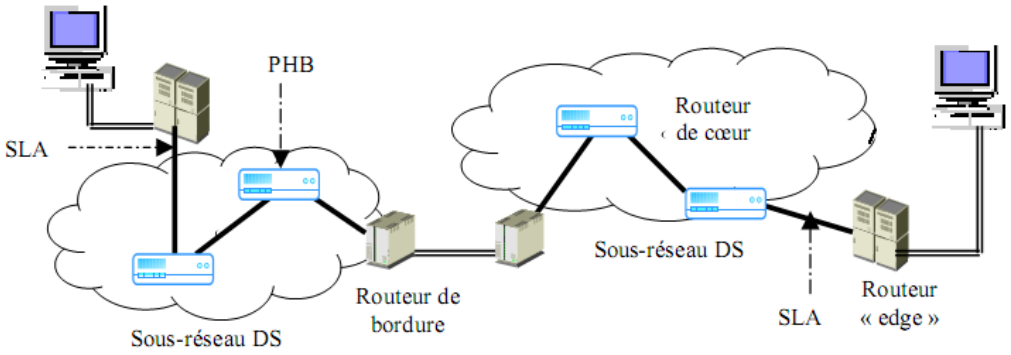


Figure 13 : Eléments constitutifs d'un réseau DiffServ

6. Ordonnancement des trafics (Traffic Scheduling)

C'est l'un des composants les plus critiques dans l'architecture d'un réseau à QoS. En effet, même en l'absence de congestion, les paquets des différents flux subissent des délais d'attente plus ou moins importants. Ces délais d'attente dans les tampons sont néfastes pour les applications sensibles aux délais et surtout pour les applications sensibles à la gigue. L'idée du traffic scheduling est d'adapter la politique de transmission des paquets en attente dans un tampon, en fonction des besoins en QoS des flux. Le choix de la politique d'ordonnancement a un impact important non seulement sur le délai et la gigue mais aussi sur la taille des tampons. Suivant la politique, la garantie de QoS sera déterministe ou statistique.

Les principales qualités attendues d'un ordonnanceur sont une bonne isolation des flots (traitement séparé des flots, ou découplage des différents flots en classe de trafic), une implémentation aisée et scalable, un temps de traitement faible et la qualité des garanties de QoS apportées.

Plusieurs algorithmes qui ont étaient présentés dans [72], chacun de ces derniers peut être vu de deux manières différentes : La vision IntServ, qui consiste à traiter chaque flux indépendamment, et la vision DiffServ, qui consiste à regrouper tous les flux par classe de service, et à traiter chaque classe de service comme s'il s'agissait d'un seul flux. Les flux d'une même classe sont alors traités selon la discipline FIFO à l'intérieur de cette classe. Un problème se pose cependant dans la vision

DiffServ : Si un flux est prépondérant par rapport aux autres au sein d'une même classe de service, alors aucun mécanisme DiffServ ne pourra empêcher la gêne occasionné aux autres flux de la même classe.

Principalement trois types d'ordonnancement ont été envisagés : l'ordonnancement à priorité fixe, l'ordonnancement basé sur le paradigme GPS (Generalized Processor Sharing : Temps partagé généralisé) et celui basé sur la notion de trame temporelle.

Ordonnanceurs à Priorité Fixe :

Les ordonnanceurs de type priorité fixe transmettent les paquets dans l'ordre de leurs priorités. Un paquet ne peut être transmis s'il y a un paquet de priorité supérieure en attente. Ces ordonnanceurs garantissent les délais les plus faibles possibles pour les paquets de priorité haute (temps réel). Toutefois, un des inconvénients majeurs de ce type de politique est que les sessions de priorités inférieures ne sont absolument pas isolées (elles sont défavorisées). Cet algorithme est néanmoins utilisé car très simple à implémenter et donc rapide.

7. Conclusion

La gestion de la qualité de service par IntServ et DiffServ présente tout de même quelques limites. Tout d'abord, IntServ emploi un mécanisme de réservation de ressources, qui doit être implémentée au niveau de chaque routeur, ce qui conduit à une lourdeur de traitement. D'autre part, IntServ applique ses algorithmes à une échelle macroscopique des données : la gestion de QoS est par conséquent appliquée par flot. De ces limites découlent des critiques en raison de son incapacité à gérer la QoS pour des réseaux largement déployés : le problème de passage à l'échelle est un aspect important puisque l'envergure des réseaux ne cesse d'accroître, et le trafic qui les traverse est en perpétuelle augmentation. L'approche DiffServ consiste, quant à elle, à remédier aux problèmes de passage à l'échelle et de complexité de gestion. Néanmoins, cette politique présente l'inconvénient de garantir une différenciation absolue, c'est-à-dire que plus une classe est grande, plus elle sera privilégiée pour le partage des ressources par rapport aux autres classes concurrentes. Ces mécanismes engendrent une discrimination de répartition et par conséquent peut provoquer le phénomène de famine entre les classes.

Chapitre 2 : Réseaux locaux sans fil

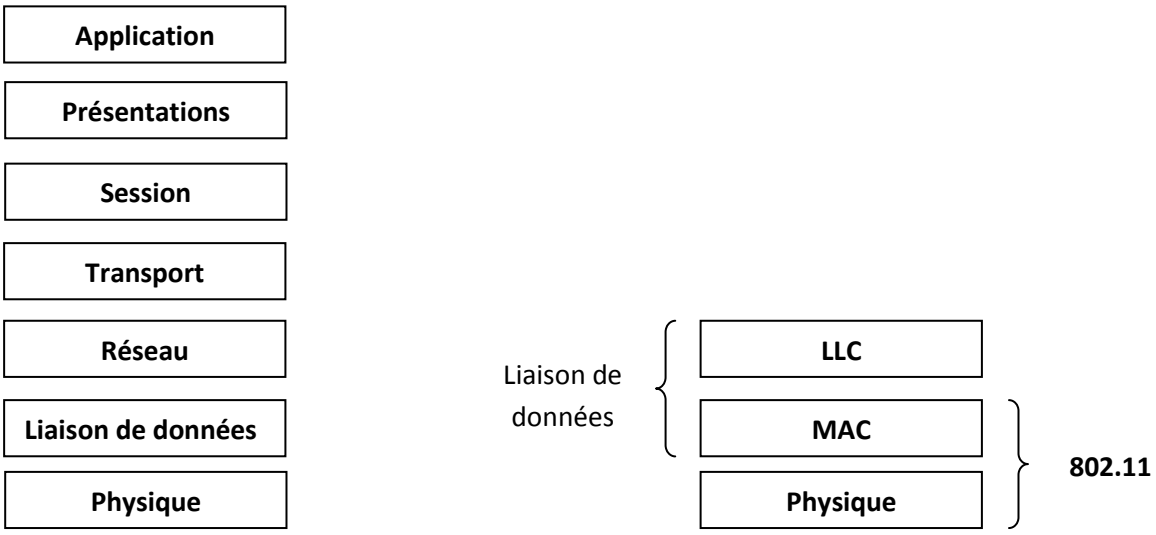
Ce chapitre présente l'évolution des réseaux locaux sans fil.

Sommaire

1. Introduction

Au début du 21ème siècle, les réseaux locaux informatiques connaissent deux évolutions importantes. D'une part, l'utilisation courante du réseau local chez les particuliers, due en grande partie à Internet et, d'autre part, l'arrivée en masse des micros ordinateurs et autres matériels mobiles. Pour cela il faillait trouver une technologie permettant de préserver les mobilités des produits portables. D'où la notion du sans fil.

Le premier standard international de réseaux locaux sans fils IEEE 802.11 a été écrit par l'IEEE (Institute of Electrical and Electronics Engineers) en 1997. Ce standard couvre la couche physique (PHY) et la sous couche de contrôle d'accès au medium (MAC) du modèle de référence OSI. Il devient facile d'interconnecter un réseau local sans fils IEEE 802.11 aux différents standards de réseaux locaux filaires.



Le modèle de référence OSI Standard 802.11

Figure 14 : Couches protocolaires modèle de référence OSI/Standard 802.11

Dans ce chapitre nous présenterons en détail le standard le plus utilisé dans les réseaux locaux sans fil à savoir IEEE 802.11.

2. Généralités

Le standard IEEE 802.11-2007 [01] définit les spécifications d'un contrôle d'accès au médium et de plusieurs couches physiques pour la connectivité sans fil de stations fixes ou mobiles dans une "zone locale" (local area dans le standard). Il est le résultat de l'intégration au premier standard IEEE 802.11-1997 [02] (communément appelé 802.11-legacy ; publié en 1999 et confirmé en 2003) des différentes modifications qui sont apparues au fil des années jusqu'à la date de publication de la nouvelle révision. 802.11-legacy, rendu obsolète par les modifications apportées, permettait un fonctionnement à des débits physiques de 1 Mbit/s ou 2 Mbit/s utilisant 3 technologies au niveau physique au choix : l'infrarouge ; les radiofréquences avec étalement de

spectre par saut de fréquence (FHSS Frequency-Hopping Spread Spectrum) ou avec étalement de spectre à séquence directe (DSSS Direct-Sequence Spread Spectrum).

Les technologies à radio-fréquences fonctionnent dans la bande ISM Industrial Scientific Medical) autour de 2,4 GHz et la bande U-NII (Unlicensed National Information Infrastructure) autour de 5 GHz. Les modifications qu'intègre cette nouvelle révision sont les suivantes :

IEEE 802.11a-1999 permettant un fonctionnement dans la bande de fréquence 5 Ghz à un débit physique allant jusqu'à 54 Mbit/s grâce à l'utilisation d'une technique de codage OFDM (Orthogonal Frequency-Division Multiplexing) ;

IEEE 802.11b-1999 ainsi que la correction **IEEE 802.11b-1999 Corrigendum 1-2001** permettant d'augmenter le débit physique dans la bande de 2,4 GHz jusqu'à 11 Mbit/s ;

IEEE 802.11d-2001 ajoutant des mécanismes permettant aux stations de respecter les réglementations locales en termes de puissances de transmission et de plages de fréquences autorisées ;

IEEE 802.11g-2003 introduit la technique de codage OFDM dans la bande de fréquence 2,4 GHz permettant ainsi des débit allant jusqu'à 54 Mbit/s ;

IEEE 802.11h-2003 harmonisant la modification 802.11a avec les contraintes réglementaires de la communauté européenne ;

IEEE 802.11i-2004 spécifiant des mécanismes de sécurité ;

IEEE 802.11j-2004 établissant la conformité de l'utilisation de la bande 4,9-5 GHz avec les règles japonaises ;

IEEE 802.11e-2005 spécifiant des mécanismes de Qualité de Service sur lesquelles porte une partie de notre travail ; les modifications apportées par le groupe de travail 802.11e sont détaillées dans le document [03].

D'autres groupes de travail et groupes d'études ont été mis en place par le comité de travail 802.11 afin de mettre en place des modifications à apporter au standard 802.11, parmi ceux-là :

IEEE 802.11k-2008 fournit aux couches de plus haut niveau des interfaces d'accès à des mesures radio, cette modification a été publiée en 2008 [4] ;

IEEE 802.11n étudie la possibilité de fournir des débits utiles allant au delà des 100 Mbit/s. Le groupe de travail 802.11n est toujours actif avec un projet de modification proposant l'utilisation de la technologie MIMO (Multiple-Input Multiple-Output). La standardisation de 802.11n est prévue pour Novembre 2009 ;

IEEE 802.11p étudie la possibilité de modifier le standard afin de fournir la possibilité de communiquer entre un véhicule et une entité de bord de route ou entre deux véhicules circulant à une vitesse allant jusqu'à 200 Km/h avec une portée allant jusqu'à 1000 m, le travail de ce groupe se pose dans le cadre d'un système de transport intelligent, le groupe de travail est actif ;

IEEE 802.11r-2008 permet une connectivité continue des entités mobiles en utilisant des mécanismes de transition rapides, transparents et sécurisés : Fast Basic Service Set Transition, cette modification a été publiée en 2008 [5] ;

IEEE 802.11aa ou VTS (Video Transport System) a pour but de spécifier des mécanismes permettant le transport robuste des flux audio et vidéo sur 802.11, le travail de ce groupe a débuté en 2007 et est toujours actif.

3. La famille IEEE 802

La 802.11 est issu de la famille 802, qui est une série de spécifications pour les réseaux locaux ou Local Area Network (LAN). La figure 20 montre la relation entre les différents composants de la famille 802 et leurs emplacements dans le modèle OSI.

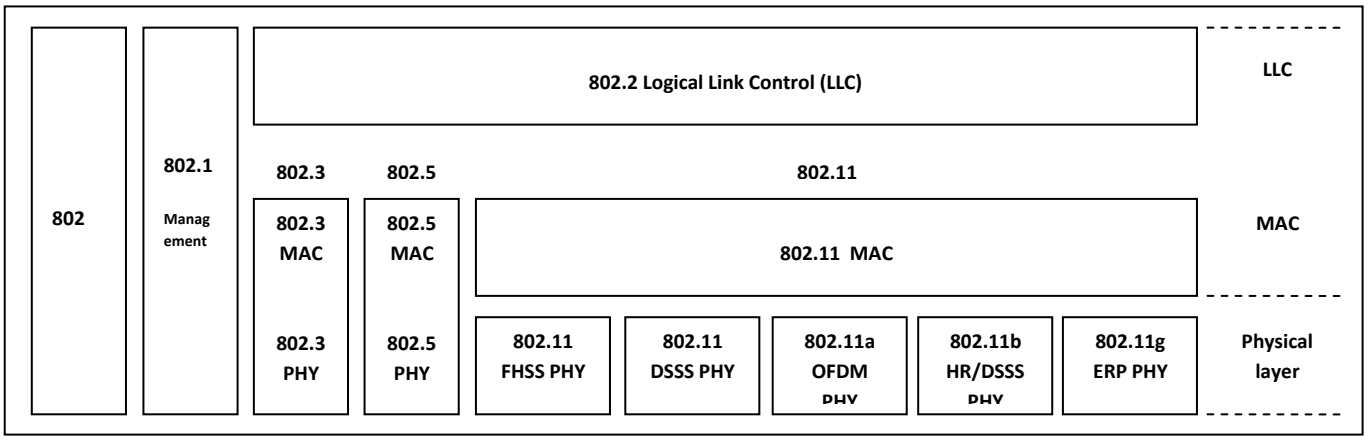


Figure 15 : La famille IEEE 802

Comme les spécifications 802, le standard IEEE 802.11 couvre les deux couches inférieures du modèle OSI : la couche liaison et la couche physique. La couche MAC définit un ensemble de règles permettant d'accéder au médium et d'envoyer des données, les détails de la réception et de la transmission sont traités au niveau de la couche physique.

Chaque série de spécification 802 est identifiée par un second nombre. Par exemple :

- Les procédures de management des réseaux 802 sont spécifiées dans 802.1.
- 802.2 définit la sous couche Logical Link Control (LLC).
- 802.3 définit le mécanisme d'accès CSMA/CD utilisé dans les réseaux Ethernet.
- 802.5 est la spécification pour les réseaux Token Ring.
- 802.11 est couche de lien qui utilise l'encapsulation 202.2/LLC.

3.1. Classification des réseaux IEEE 802.11

Les réseaux sans fil peuvent être classé soit :

Selon la zone de couverture (portée de transmission) : périmètre géographique offrant une connectivité.

Selon le mode de fonctionnement (avec infrastructure ou sans infrastructure Ad Hoc)

3.1.1. Classification selon la zone de couverture

- Les réseaux sans fil personnel (WPAN : Wireless Personal Area Networks) : ils concernent l'entourage immédiat d'une personne (quelque mètres). Exemples : Blue touth 802.15.1, Zigbee 802.15.4.
- Les réseaux sans fil locaux (WLAN : Wireless Local Area Networks) : ils concernent un environnement de vie plus étendu comme une maison, une entreprise (à partir de quelques dizaines de mètres jusqu'à 100 mètres). Exemple : Norme 802.11 WIFI
- Les réseaux sans fil métropolitains (WMAN : Wireless Metropolitan Area Networks) : ils visent à couvrir une région étendue comme une ville (plusieurs Km).
- Les réseaux étendus (WWAN : Wireless Wide Area Networks) : ils visent à couvrir une zone très vaste comme une région du globe ou toute une planète.

3.1.2. Classification selon le mode de fonctionnement

Deux modes de fonctionnement peuvent être utilisés pour la mise en place d'un réseau IEEE 802.11.

- Réseaux sans fil avec infrastructure :

Dans le mode avec infrastructure, toutes les communications, entre les stations mobiles ou entre les stations et le réseau extérieur, passent a travers un point d'accès (AP ou Access Point) qui prend alors le rôle de relais. L'ensemble AP et tous les terminaux mobiles se trouvant sur ça zone de couverture est appelé un BSS ou Basic Service Set (ensemble de service de base). Les APs peuvent être reliés ensemble par un système de distribution (DS). Le standard ne donne pas des spécifications particulières sur la nature de cette interconnexion mais il s'agit en général d'un réseau filaire (de type Ethernet). La figure 21 illustre l'architecture d'un ESS (Extended Service Set) constitue par un ensemble de BSS relies par un réseau filaire.

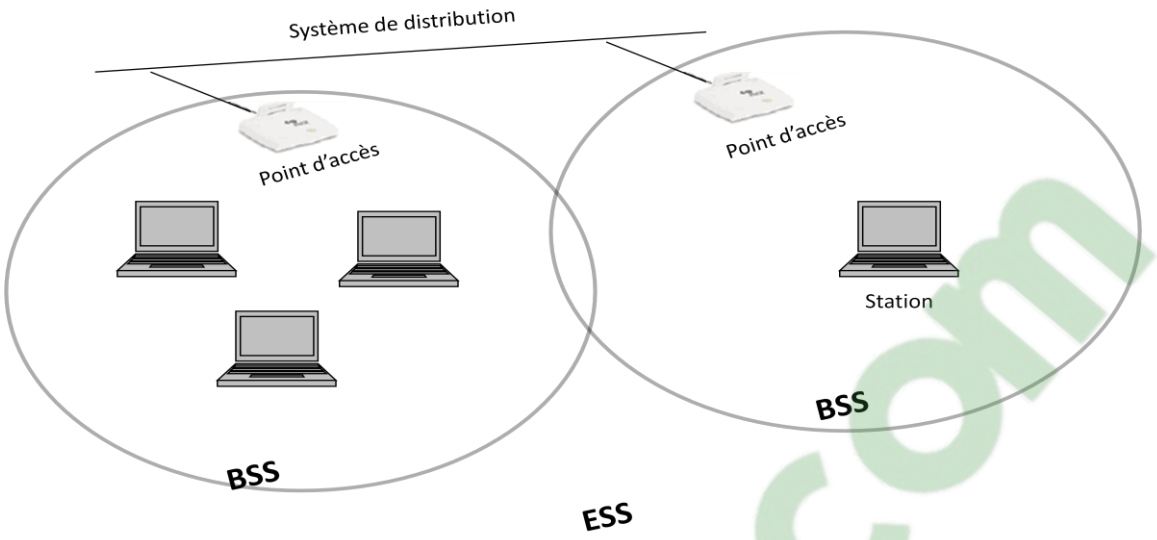


Figure 16 : Architecture generale d'un reseau IEEE 802.11 en mode infrastructure

SB : station de base

UM : unité mobile

Dans ce mode de fonctionnement le réseau est obligatoirement composé d'un point d'accès appelé Station de Base SB munie d'une interface de communication sans fil pour la communication directe avec les unités mobiles UM, une station de base couvre une zone géographique limitée, la SB représente un pont réseau filaire et réseau sans fil permettant de relier une UM à une autre UM connectée à un site fixe. La station de base est aussi le point de passage de la transmission d'une UM à une autre UM.

- Réseaux sans fil sans infrastructure :

Généralement appelés réseaux mobile Ad Hoc (MANET : Mobil Ad Hoc Networks)

Dans le mode sans infrastructure ou ad hoc, les utilisateurs communiquent directement entre eux sans aucun intermédiaire. Les stations mobiles se trouvant à la portée les unes des autres forment alors un IBSS ou Independent Basic Service Set.

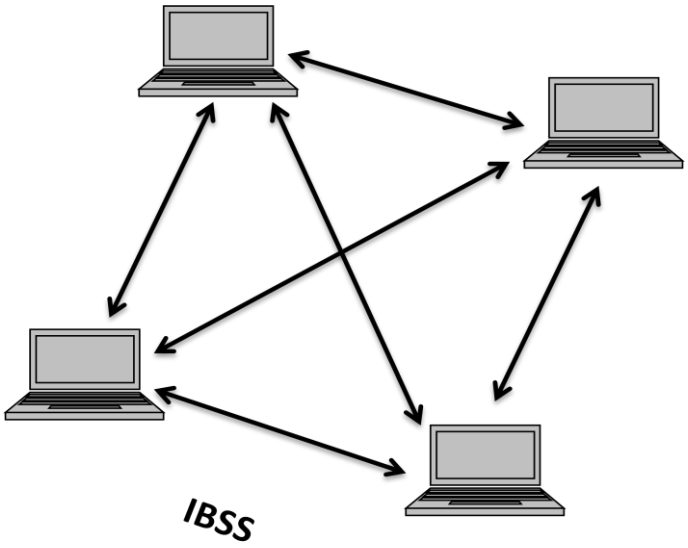


Figure 17 : Mode Ad hoc

4. La couche MAC

Les spécificités du médium radio rendent l'utilisation d'un protocole d'accès au médium efficace primordial. Le rôle du protocole d'accès au médium est multiple. Il est en charge d'éviter les collisions, d'assurer le partage de la bande passante, de résoudre certains problèmes spécifiques aux transmissions hertziennes (stations cachées ou exposées), et d'assurer une bonne qualité de services pour les clients.

La sous couche MAC IEEE 802.11 définit deux fonctions d'accès au medium sans fils dites fonctions de coordination. Une fonction de coordination distribuée DCF (Distributed Coordination Function) et une fonction de coordination centralisée PCF (Point Coordination Function). DCF est une méthode d'accès asynchrone dont l'implémentation est obligatoire pour tous les équipements IEEE 802.11 fonctionnant en mode avec ou sans infrastructures. PCF, utilisée uniquement en mode avec infrastructure, offre un service synchrone facultatif. L'utilisation de ce service nécessite l'implémentation du mode DCF. PCF est un mode sans contention pour lequel l'accès au medium des différentes stations est coordonne par le point d'accès.

4.1. La fonction de coordination distribuée DCF

Le mode DCF est base sur le protocole CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance). En effet l'utilisation de la méthode CSMA/CD de l'Ethernet est impossible sur un canal radio : une station ne peut pas transmettre et écouter simultanément sur le canal vu les différences significatives des puissances de transmission et d'émission, c'est une méthode coûteuse car elle nécessite l'utilisation d'un circuit full duplex pour la détection de collision. Pour la signalisation de la bonne réception d'une trame, un mécanisme d'acquittement positif est utilisé dans la méthode CSMA/CA. Chaque fois qu'une trame est correctement reçue, un paquet d'acquittement doit être renvoyé à la source. L'absence de cet acquittement indique un problème dans la transmission de la trame. La trame doit être retransmise. La méthode CSMA/CA abandonne la détection de collisions tout en renforçant les mécanismes pour les éviter.

Protocole CSMA/CA

- Quand une station désire envoyer une trame, elle écoute d'abord le canal pour savoir s'il y a quelqu'un qui transmet.
- Si le canal est libre alors la station transmet.
- Si le canal est occupé, elle attend que l'émetteur termine et reçoit l'ACK, en suite elle attend un temps aléatoire et transmet. Ce temps d'attente (Backoff Time) est compris entre 0 et la taille de la fenêtre de contention.
- La station attend que le récepteur lui envoie l'ACK. Si ceci ne se produit pas dans un délai seuil, elle considère qu'il c'est produit une collision, dans un tel cas elle répète le processus depuis le début.

Dans le mode DCF, chaque station doit écouter le canal avant de commencer la transmission d'un paquet. La sensation physique de la porteuse du canal radio permet d'analyser toute activité sur le canal et de détecter s'il est ou non occupe par d'autres stations. Un temps d'inactivité est obligatoire entre deux trames qui circulent sur le canal radio. Une station qui a écouté le canal et qui a trouvé le canal libre doit attendre un temps inter trame IFS (Inter Frame Space) avant d'émettre. Si le canal est toujours libre la station peut alors transmettre son paquet.

- Dans le mode DCF, ce temps inter trame correspond a un DIFS (DCF IFS) si la station commence une nouvelle transmission,
- PIFS (PCF IFS) s'il s'agit d'un AP voulant initialiser une période sans contention PCF,
- et SIFS (Short IFS) si la trame fait partie d'une communication déjà établie.

Le risque de collision, avec la méthode DCF n'est jamais nul. Un mécanisme de backoff est utilisé pour réduire la probabilité d'une collision. Les stations en contention pour l'accès au canal doivent choisir un nombre aléatoire de backoff dans une fenêtre de contention (0, CW).
CW (Contention Window) est définit entre CWmin et CWmax. Multiplié par le time slot, ce nombre définit le temps de backoff (backoff_timer), intervalle de temps aléatoire pour chacune des stations. CWmin, CWmax et le time slot dépendent de la couche physique utilisée. Les stations décrémentent leurs temps de Backoff chaque fois que le canal est libre.

Ce temps est maintenu quand le canal radio devient occupe. Chaque fois que le canal devient libre, chaque station attend un temps DIFS et continue à décrémenter son temps de Backoff. Quand il atteint zéro, la station est autorisée à transmettre. Pour réduire la probabilité de collision, suite à chaque tentative de transmission échouée, la fenêtre de contention CW est doublée dans la limite de la valeur maximale CWmax. Quand la tentative est réussie, la valeur de la fenêtre est réduite à CWmin.

Clicours.COM

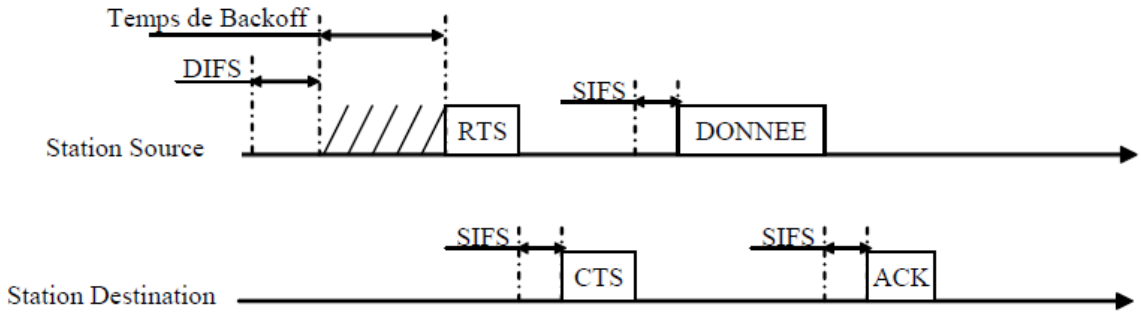


Figure 18 : Méthode d'accès DCF

4.2. La fonction de coordination centralisée PCF

La deuxième méthode d'accès PCF utilisée pour le contrôle d'accès au medium sans fils est facultative et nécessite la présence d'un coordinateur, généralement le point d'accès. Cette méthode n'est donc valable que dans les réseaux 802.11 avec infrastructure.

Les communications directes entre les stations sans fils ne sont plus possibles, elles doivent toutes passer par le point d'accès. De ce fait, la moitie de la bande passante est gaspillée.

Cette méthode à été lancée par le standard pour répondre aux besoins des utilisateurs ayant des trafics temps réel. Elle est basée sur la définition d'une période sans contention (Contention Free Period) qui se déroulera en alternance avec la période avec contention (Contention Period) gérée par le mode DCF.

Au sein d'un même BSS, le temps d'accès au canal sera alors partagé en deux intervalles (CFP + CP) nommes Beacon Interval.

Durant la période sans contention, le point d'accès, coordinateur de ce mode PCF, maintient une liste des stations voulant transmettre des données. A tour de rôle le point d'accès consulte les stations pour commencer la transmission de leurs paquets. La durée maximale, CFP_max_duration, de la période sans contention est définie par le point d'accès. Les stations ne sont pas autorisées à envoyer des trames au dessus d'une taille maximale. Une trame de gestion Beacon est envoyée au début de la période CFP à un temps nomme Target Beacon Transmission Time (TBTT). A chaque TBTT, le temps inter trames PIFS alloué aux points d'accès permet à chacun de ces derniers d'accéder au canal, de lancer à chaque fois le mode PCF et d'interdire l'accès en mode DCF des autres stations du BSS. Chaque trame Beacon, diffusée pour l'ensemble des stations du BSS, contient le TBTT de la prochaine période CFP. A la réception de cette trame, les stations n'ayant pas des trafics à envoyer mettent à jour leurs temporisateurs NAV de la durée de la période CFP.

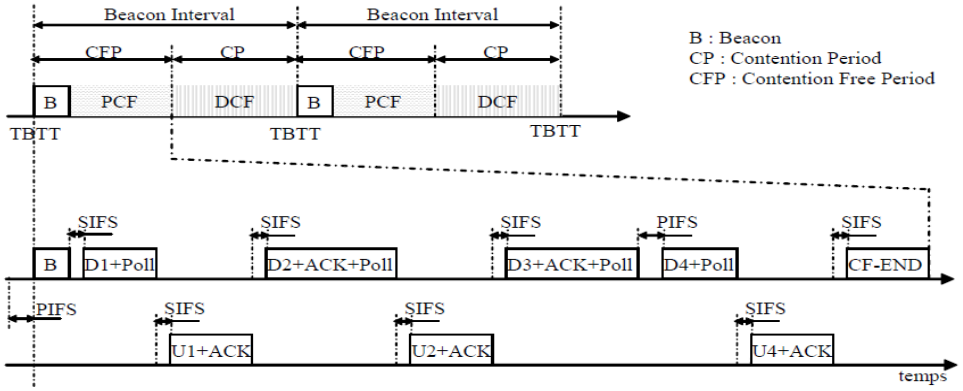


Figure 19 : Une séquence d'accès au medium sans fils en mode PCF.

La trame Beacon est utilisée avec et sans le mode PCF. Quand le mode PCF n'est pas utilisé, cette trame permet de gérer le mode économie d'énergie des stations défini par le standard. [6]

4.3. Les trames MAC :

Le standard 802.11 définit trois types de trames :

- Les trames de données, utilisée pour la transmission de données.
- Les trames de contrôle, par exemple RTS, CTS et ACK.
- Les trames de gestion, pour l'échange d'information de gestion au niveau MAC.

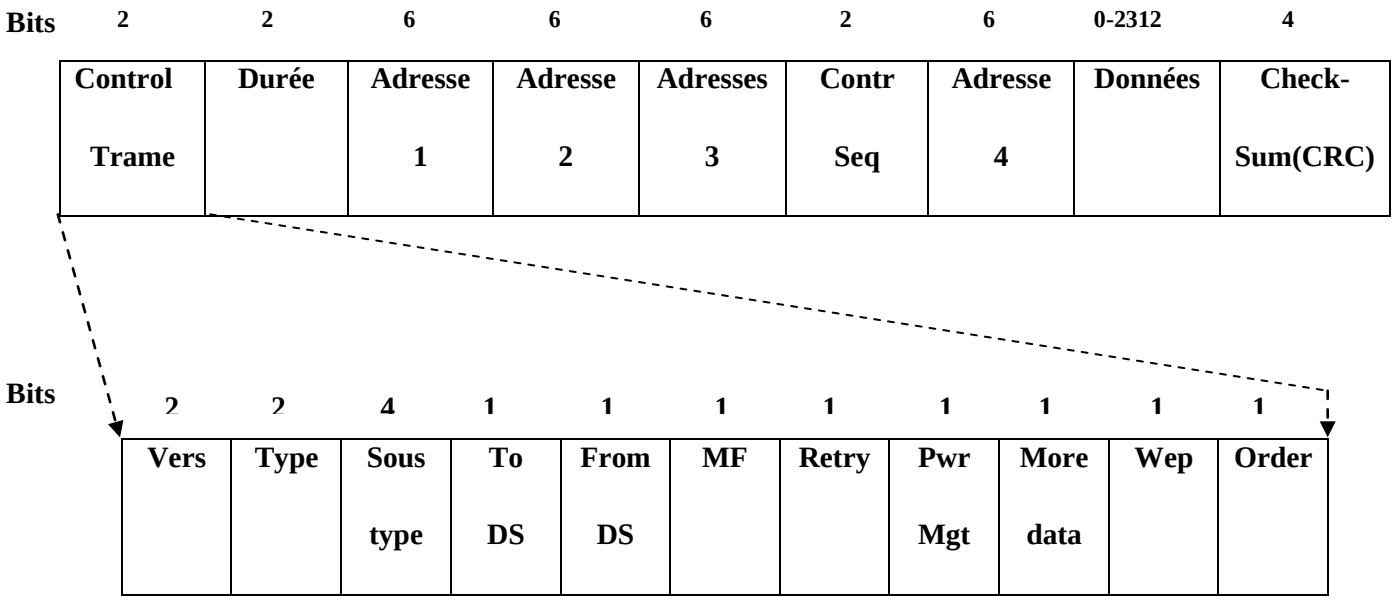


Figure 20 : Format de la trame 802.11

5. Conclusion

Le 802.11 est la technologie la plus déployée dans les entreprises. Elle est soutenue par la majorité des opérateurs Télécom, qui ont crée un consensus autour des normes IEEE 802.11b (WiFi) et IEEE 802.11a (WiFi 5). Cependant, le manque de garantie de QoS limite le déploiement de plusieurs applications temps réel et multimédia sur les réseaux WiFi. En effet, le mécanisme DCF ne supporte que les services de type best-effort, qui ne requiert aucune garantie de QoS, car DCF offre à toutes les stations et à tous les flux de la même station les mêmes priorités d'accès aux ressources et au canal. De plus, PCF introduit plusieurs problèmes.

Dans ce qui suit, un état de l'art de la qualité de service dans les réseaux sans fil sera présenter ainsi que les limites DCF et PCF en terme de QoS.

Chapitre 3 : Conception

Ce chapitre présente un état de l'art de la qualité de service dans les réseaux sans fil.

Sommaire

Section 1 : Qualité de services dans les réseaux locaux sans fil.

1. Introduction

Les réseaux locaux basés sur la technologie IEEE 802.11 ont pris une ampleur telle qu'ils sont déployés un peut partout dans notre entourage quotidien. Ce déploiement est favorisé par la maturité atteinte par le standard grâce aux travaux des groupes 802.11 chargés de rendre le standard plus compétitif (QoS, sécurité, haut débit). Le groupe de travail 802.11e répond aux challenges de garantie de QoS aux applications temps réel en définissant de nouveaux mécanismes d'accès au médium. Le draft résultant des travaux du groupe 802.11e propose deux nouveaux mécanismes : Enhanced Distributed Channel Access (EDCA) et le Hybrid coordination function Controled Channel Access (HCCA).

Dans ce chapitre, nous nous intéresserons plus particulièrement à la gestion de la qualité de service et ses contraintes dans les réseaux IEEE 802.11.Dans un premier temps un aperçu sur la QoS sera établi. Dans un deuxième temps nous allons énumérer les limités en QoS dans le 802.11 ; nous nous attarderons sur les limites des deux mécanismes DCF et PCF. Troisièmement nous présenterons quelques approches d'amélioration de qualité de service notant le 802.11e, la différentiation de service et le contrôle d'admission.

2. Généralités sur la qualité de service

L'explosion de l'Internet et la multitude de ses usages ont rapidement fait évoluer les besoins des utilisateurs des réseaux. Si on se place dans les réseaux IP, de nouvelles applications très sensibles aux performances des réseaux ont émergées :

- la téléphonie sur IP : selon les statistiques de l'observatoire des marches de l'ARCEP (http://www.art-telecom.fr/) au premier trimestre de l'année 2007, Le nombre d'abonnements a un service téléphonique progresse de 4,0% sur un an grâce a l'essor des offres de téléphonie sur IP. Elles représentent 20% des 38,7 millions d'abonnements, soit 7,8 millions ; cette proportion n'était que de 11% au premier trimestre de l'année 2006.
- La diffusion de contenus multimédia : visioconférences, vidéo à la demande, radio en ligne…
- Les jeux en réseaux : ils ont existe des la naissance des réseaux, mais la puissance de calcul disponible actuellement sur les ordinateurs permet de concevoir des jeux toujours plus gourmands en ressources.

D'autres applications plus anciennes ont été également transférées sur les réseaux IP telles que les fonctions d'administration (contrôle à distance), les applications bancaires ou de bourse, les applications médicales et les applications industrielles.

Avec cette diversité d'applications, il n'est pas facile de donner une définition globale de la qualité de service. Un utilisateur par exemple voudra tout simplement que le service fonctionne correctement alors qu'un autre exigera des performances minimales.

Par exemple, pour le transfert de fichier, le critère principal de jugement sera la vitesse et la fiabilité. Par contre, pour une visioconférence, il faudra des délais de transmission bornes tout en

tolérant un faible taux de perte. Pour la visualisation d'un film, il faudra une bonne définition d'image et une bonne vitesse de rafraichissement. Dans le cas ou l'on souhaiterait effectuer des virements bancaires, on s'intéressera surtout a la fiabilité et la sécurité de la transaction. Pour les jeux en réseaux, une bonne synchronisation entre les machines des différents joueurs est nécessaire. Pour des applications médicales ou industrielles, on s'intéresse plutôt aux délais maximaux (délais de bout en bout bornes) et a la fiabilité des échanges. On pourrait probablement trouver encore de nombreux critères en énumérant plus d'applications.

Pour cette raison, il n'y a pas une définition exacte de la qualité de service dans la terminologie réseau et nous présenterons ici quelques définitions issues de la littérature.

- La définition de base de la qualité de service a été donnée dans [16] comme étant l'effet collectif de la performance des services, qui détermine le degré de satisfaction d'un utilisateur pour un service.
- Pour Vogel et Al. [17], la qualité de service représente l'ensemble des caractéristiques quantitatives et qualitatives d'un système multimédia distribué nécessaire pour assurer les fonctionnalistes requises d'une application.
- Dans [18] la qualité de service est l'ensemble des qualités reliées au comportement d'un ou plusieurs objets.
- Pour l'IETF, la qualité de service est un ensemble d'exigences de service devant êtres remplies par le réseau lors du transport d'un flux.
- Pour Malamos et Al. [19], la qualité de service est la mesure de base qui détermine si oui ou non le fonctionnement d'un système répond aux besoins des utilisateurs.
- Pour Chalmers et Sloman [20] : alors que les systèmes sont souvent définis en fonction de leurs fonctionnalités, la qualité de service définit les caractéristiques non fonctionnelles d'un système qui affectent la qualité du résultat perçu par les utilisateurs (qualité de la vidéo pour un spectateur par exemple).

Les besoins en qualité de service de l'utilisateur sont transformés en paramètres technologiques de qualité de service par des outils de gestion de qualité de service. Celle-ci est définie comme étant un ensemble de fonctions et de mécanismes de supervision et de contrôle pour assurer que le niveau de qualité de service recherché est bien mis en place et surtout maintenu [20]. Deux types de fonctions de gestion de qualité de service sont identifies : statique et dynamique. Les fonctions de gestion de QoS statiques sont appliquées à l'initialisation du système, alors que les fonctions dynamiques sont appliquées autant que nécessaire durant l'exploitation du système [20]. Les fonctions statiques et dynamiques de la gestion de QoS sont résumées dans les tableaux suivants.

Tableau 4 : Fonctions statiques de gestion de QoS [20]

Fonction	**Définition**	**Exemple de techniques**
Spécification	Définition des besoins et des capacités de QoS	Besoins à différents niveaux, utilisateur, environnement, technologies, application, etc.
Négociation	Processus pour atteindre une spécification acceptée par tous les partis	Modification des paramètres après une panne, ces modifications doivent considérer les relations établies entre les paramètres et les préférences de l'utilisateur
Contrôle d'admission	Comparaison des besoins en QoS et la capacité d'atteindre ces besoins	Les ressources disponibles peuvent êtres estimées avec l'aide des informations de réservation et des modèles de performance
Réservation de Ressources	Allocation de ressources a des connexions	Les techniques de réservation de ressources en réseau (ex : RSVP)

Tableau 5 : Fonctions dynamiques de gestion de QoS [20]

Fonction	**Définition**	**Exemple de techniques**
Supervision	Mesure de la QoS réellement Fournie	Surveillance du paramètre en relation avec la spécification
Contrôle	Assurer que tous les partis adhérent au contrat de QoS	Contrôle des paramètres qui sont en relation avec le contrat
Maintenance	Modification des paramètres par le système pour maintenir	Utilisation de filtre, file d'attente pour maintenir le

	la QoS	paramètre de délai ou de Débit
Renégociation	Renégociation du contrat	Nécessaire lorsque les fonctions de maintenance de la QoS ne peuvent plus assurer le contrat
Adaptation	L'application s'adapte aux changements en QoS du système, probablement après une renégociation	Techniques d'adaptation au niveau applicatif telle que la diminution du débit de sortie des données si la bande passante diminue
Synchronisation	Combinaison de plusieurs flots multimédia avec des contraintes temporelles de QoS qui nécessite une synchronisation	Il est nécessaire de relier l'information temporelle des deux flots multimédia que l'on veut synchroniser

Si les critères de la qualité de service sont bien définis, il reste à trouver les moyens de les garantir. Une des difficultés principales de la mise en place de la qualité de service est de réussir une intégration selon deux axes : verticale et horizontal.

- L'intégration verticale consiste à descendre des besoins des utilisateurs vers les ressources physiques. La qualité de service n'est pas reliée à une couche spécifique du modèle OSI : elle nécessite une coordination de l'ensemble des couches du modèle. Il faut effectuer la traduction des besoins, et s'assurer de l'interopérabilité des mécanismes

- L'intégration horizontale concerne les équipements traversés entre les deux extrémités qui communiquent. On peut ici avoir l'intervention de plusieurs operateurs, ce qui pose éventuellement des problèmes de négociation, et l'on a probablement une diversité des technologies de QoS mises en œuvre. La traversée du réseau nécessite donc une interopérabilité de celles-ci.

Les paramètres classiquement associes a la qualité de service dans les réseaux sont : la disponibilité, la bande passante, la latence, la gigue et le taux de perte.

- la disponibilité décrit la fiabilité du réseau et peut êtres définie comme un rapport entre le temps où la connexion au réseau est disponible et le temps total d'ouverture théorique du service. En particulier, la disponibilité concerne plus que la simple accessibilité au service. Elle concerne plutôt un niveau de service exploitable par l'utilisateur.

- La bande passante est définie comme étant le débit ou la vitesse de transmission des données ou encore le nombre de bits transmis par unité de temps. Elle dépend des supports physiques utilisés et de la capacité de traitement des équipements du réseau traversé.

- Le délai est définit comme étant le temps mis par un paquet (ou une information) pour parcourir le chemin entre une source et une destination. Ce paramètre dépend du support physique utilisé, du nombre d'équipements traversés sur le chemin entre la source et la destination, de la taille des paquets des protocoles MAC utilisés et du niveau de partage du réseau (congestion,…).

- La gigue est définie comme étant la variation des délais entre les différents paquets d'un même flux. Ce paramètre est assez important dans les applications multimédia et temps réel nécessitant une forte synchronisation entre source et destination.

- Le taux de perte est défini comme le rapport entre le nombre d'octets émis et le nombre d'octets effectivement reçus. Ce paramètre permet d'avoir une idée sur la capacité de la transmission du réseau.

3. Etat de l'art

Le manque de mécanismes efficaces de support des services temps réel dans la version originale du standard 802.11 a donné lieu à beaucoup de travaux menés conjointement par l'industrie et les universitaires, la modification de cette version est devenue nécessaire pour fournir des garanties de qualité de service pour les applications qui y sont sensibles [7, 8, 9, 10]. Ces travaux concernent plus particulièrement les mécanismes d'accès au canal (MAC).

a. Avant le draft 802.11e

Les auteurs de [15] démontrent qu'il est possible de différencier les flux dans le réseau IEEE 802.11 par le biais de plusieurs paramètres MAC :

- Différents facteurs d'incrémentation du backoff timer pour différentes priorités.
- Différentes tailles minimales de la fenêtre de contention, CWmin : en attribuant de courtes fenêtres de contention aux flux de haute priorité, cela garantit que ces flux ont plus de chance de pouvoir accéder au canal que ceux de moindre priorité.
- Différents espacements inter-paquets DIFS : en associant différents DIFS à différents flux, il est possible d'établir une stricte différentiation entre ces flux dans l'accès au medium. En effet, plus la valeur du DIFS est petite, plus le flux à une chance d'accéder au canal, et vice versa.
- Différentes longueurs maximales de paquets : en donnant la possibilité d'envoyer des paquets de tailles différentes, le débit utile obtenu par une priorité est proportionnel à la taille des paquets utilisés.

b. Le draft 802.11e

Afin de pallier aux limitations des mécanismes DCF et PCF à garantir de la QoS, le groupe 802.11e a défini un seul mécanisme d'accès au médium HCF qui combine les deux nouveaux mécanismes EDCA et HCCA. HCF est basé sur l'utilisation d'une supertrame contenant deux phases d'opération, Contention Period (CP) et Contention Free Period (CFP). EDCA est utilisé seulement dans la phase d'opération CP, alors que HCCA peut être associé aux deux phases. La norme 802.11e sera présentée en détail dans la section 5.

c. Après le draft 802.11e

Sachant la difficulté de déploiement des mécanismes centralisés et de leurs gestions très délicates, la majorité des travaux post draft 802.11e se sont intéressés à l'amélioration du mécanisme EDCA plutôt que HCCA. Cependant, la nature du protocole CSMA/CA rend difficile la garantie de QoS dans EDCA. En effet, dès que le réseau devient congestionné, EDCA exhibe une grande dégradation de la QoS. Dans ce contexte, il est nécessaire de prendre plus en compte l'état du réseau afin de définir des paramètres dynamiques qui permettent de garantir une bonne QoS pour les ACs de haute priorité.

d. Limites du standard 802.11 en termes de qualité de services

Limites de DCF (Distributed Coordination Function)

L'inconvénient de la technique DCF est qu'elle ne fournie pas de garantie de qualité de service. Les différentes stations du BSS et les différentes classes de trafic ont la même probabilité d'accès au support. Cette technique ne comporte donc aucun mécanisme de différentiation qui garanti le débit et le délai pour les trafics de hautes priorités puisque CW_{MIN} et CW_{MAX} par exemple dépendent des caractéristiques de la couche physique. Finalement, il est important de signaler que cette technique supporte uniquement les services de type Best-effort

Limites de PCF (Point Coordination Function)

Le mode PCF a été conçu par IEEE pour supporter principalement des applications multimédia temps réel. Ceci étant, trois facteurs réduisent ces performances en termes de QoS : La complexité du plan de polling a pour conséquence de détériorer les performances en terme de qualité de service pour les trafics de haute priorité.

- L'alternance entre les périodes CP et CFP ne se déroule pas toujours sans problèmes : les transmissions en mode DCF peuvent mettre du temps à se terminer ce qui peut retarder l'envoie de la trame Beacon pour passer en mode PCF. Ce retard provoque des délais supplémentaires sur les différentes transmissions en mode PCF, et détériore la qualité de service.

Clicours.COM

- Le PC n'est pas en mesure d'estimer avec exactitude la durée des transmissions des stations «élues» ; cette durée dépend en effet des différentes méthodes de codage de la couche physique. La fragmentation des trames influe également sur cette durée.

4. La norme 802.11e

Pour supporter la qualité de service, le groupe de travail "e" du standard 802.11 définit des améliorations de la couche MAC de 802.11 [12] en introduisant une fonction de coordination hybride (HCF : Hybrid Coordination Function). HCF définit deux mécanismes d'accès au canal (synonyme d'accès au médium dans 802.11) : accès avec contention et accès contrôlé. La méthode d'accès avec contention est nommée EDCA (Enhanced Distributed Channel Access). La deuxième méthode, offrant un accès contrôlé, est nommée HCCA (HCF Controled Channel Access).

Les stations sans fils opérant sous 802.11e [13] sont appelées stations améliorées (enhanced stations). La station améliorée qui joue le rôle de contrôleur central au sein de la même cellule QBSS (QoS BSS, réseau WLAN supportant la QoS) est appelée le point de coordination hybride (HC : Hybrid Coordinator). Le point de coordination hybride est typiquement combiné au point d'accès. Un QBSS est un BSS qui inclut un HC et des stations améliorées.

Les paramètres QoS sont ajustés au cours du temps par le coordinateur hybride et sont annoncés périodiquement à travers les trames balises. Plusieurs entités de Backoff (Backoff Entity) fonctionnent en parallèle dans une station améliorée. Une entité de backoff est une file de transmission pour une classe de trafic bien déterminée avec des paramètres d'accès au canal spécifiques. Une station 802.11e ou plus précisément une entité de backoff ne peut utiliser le canal que pour une durée limitée. L'intervalle de temps durant lequel la station a le droit d'émettre est appelé l'opportunité de transmission TXOP (Transmission Opportunity). TXOP est dé_ni par un instant de début et une durée. Un intervalle TXOP obtenu suite à une contention au canal est appelé EDCA-TXOP. Quand cet intervalle est obtenu dans la période contrôlée par le HC, il est appelé HCCA-TXOP. La durée d'une EDCA-TXOP est limitée par la valeur du paramètre QBSS-limit-TXOP régulièrement distribuée par le point d'accès à travers les trames balises (beacon). Ce paramètre permet donc de contrôler la durée maximale d'une transmission en cours ce qui est important pour les délais d'accès et de transmission de l'ensemble des stations. L'utilisation de ce paramètre permet aussi d'assurer à un instant précis et sans retard, le démarrage de chaque période d'accès contrôlée par le HC. Une entité ne sera autorisée à transmettre sur le support que si sa transmission arrive à terme avant le prochain TBTT (Target Beacon Transmission Time).

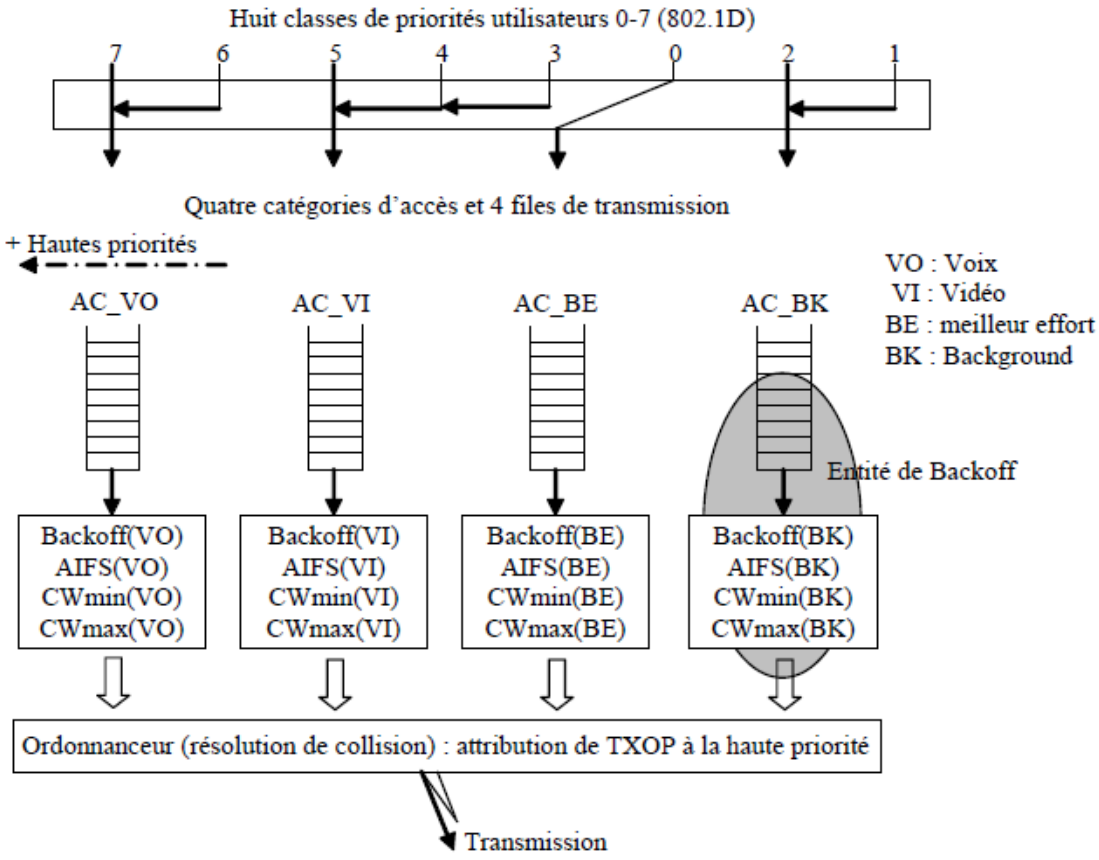
Une autre amélioration est apportée par le nouveau standard : les stations améliorées sont maintenant autorisées à transmettre directement des trames à une autre entité du QBSS sans être obligées de passer par le point d'accès. Ce fait permet d'optimiser l'utilisation de la bande passante partagée entre les utilisateurs. Dans le standard 802.11, toutes les communications passaient obligatoirement par le point d'accès. [14]

Enhanced Distributed Channel Access EDCA

Dans le mode d'accès EDCA, le support de la qualité de service est assuré par l'introduction de plusieurs catégories d'accès (AC : Access Categories). On peut avoir au total huit classes de trafics différentes pour huit priorités utilisateurs définies dans IEEE 802.1D [21].

A chaque catégorie d'accès est associée une entité de backoff ou file d'attente indépendante. En utilisant des paramètres de contention spécifiques, des priorités différentes sont attribuées à l'ensemble des AC. Dans le modèle simplifie du 802.11e, 4 catégories sont implémentées figure si dessous. Ce modèle a été adopte en observant que les huit classes d'application utilisateurs définies précédemment ne se déroulent jamais simultanément [22].

L'utilisation d'un nombre réduit de files d'attentes par rapport au nombre de priorités utilisateurs permet de limiter les risques de saturation de la sous couche MAC. Les huit priorités utilisateurs sont alors mappées dans 4 files d'attentes. Des applications spécifiques [23] sont généralement associées à chacune des files (Video, Voix, Best Effort, Background).



La contention au canal est effectuée par chacune des entités de backoff d'une façon indépendante des autres [24]. Les paramètres utilisés pour l'accès au canal permettent d'affecter des priorités différentes pour chaque catégorie d'accès. Ces paramètres qui seront identiques pour la même catégorie d'accès dans toutes les stations du QBSS, peuvent être modifies par le HC au cours du temps. Ces paramètres sont :

Le temps inter trames AIFS [AC] : au lieu du temps DIFS d'une station 802.11, avant d'accéder au canal une entité de backoff doit attendre un temps AIFS [AC] (Arbitration IFS). Les valeurs les plus faibles sont affectées aux priorités les plus hautes. Ce temps est calcule par :

AIFS [AC] = SIFS + AIFSN [AC]*SlotTime, AIFSN[AC] ≥ 2

AIFSN (Arbitration IFS Number) est le nombre arbitraire de temps inter trames. Un nombre arbitraire sera alors affecte a chaque catégorie d'accès (contrairement a la norme de base, ou une seule valeur est affectée a toutes les stations mobiles). La valeur la plus faible de AIFSN sera égale a 2 ce qui donne une valeur de AIFS minimale égale a DIFS (si AIFSN = 1, le temps inter trames serait égal a PIFS, valeur toujours affectée a un AP).

La valeur minimale de la fenêtre de contention CWmin[AC] : quand une collision se produit, les entités de backoff entrant en collision doivent choisir aléatoirement un temps d'attente de backoff. Ce temps est choisi dans l'intervalle [CWmin[AC], CWmax[AC]]. Pour chaque entité de backoff, si elle voit que le canal est libre pendant une durée égale à AIFS [AC], elle commence le décompte du temps de backoff qu'elle a choisi. L'entité commence à transmettre un slot time après le décompte total du temporisateur de backoff. Pour les catégories d'accès a hautes priorités des valeurs plus faibles du seuil minimal de la fenêtre de contention CWmin[AC] sont utilisées. Les entités de backoff correspondantes ont alors plus de chances d'accéder au canal. Cependant, le choix de valeurs faibles augmente la probabilité de collision si plusieurs entités de backoff de la même catégorie se trouvent dans le même QBSS.

La valeur maximale de la fenêtre de contention CWmax[AC] : quand une collision se produit, une deuxième valeur du compteur de backoff, supérieure a la première doit être choisie. Cette valeur reste toujours inferieure a une valeur maximale CWmax[AC] correspondant a chaque catégorie d'accès. Les valeurs les plus faibles de CWmax[AC] permettent une probabilité d'accès plus rapide et sont donc attribuées aux priorités hautes.

Un facteur de persistance PF[AC] : ce paramètre est utilise pour réduire la probabilité de collision entre plusieurs catégories d'accès. Dans le standard 802.11, la taille de la fenêtre de contention est doublée après un échec d'accès au canal (facteur de persistance égal à 2). EDCA utilise le paramètre PF pour incrémenter la taille de la fenêtre CW différemment pour chaque classe de trafic ou catégorie d'accès.

TXOPlimit[AC] : en plus des paramètres de backoff, l'opportunité de transmission peut être affectée différemment pour les catégories d'accès. La définition d'une durée de transmission maximale plus large pour une catégorie d'accès permet à l'application correspondante de bénéficier d'une bande passante plus importante, le standard 802.11e autorise la transmission de plusieurs MSDU[1]au sein d'une seule TXOP.

[1] MSDU : MAC Service Data Unit, contient les données des couches supérieures. Elle peut être fragmentée en plusieurs MPDU (MAC Protocol Data Unit).

L'EDCA introduit quatre catégories d'accès (AC) relatives aux applications traitées dans les couches supérieures. Elles sont notées respectivement :

AC_V O : pour les applications temps réels tel que la voix

AC_V I : pour les applications vidéo

AC_BE : pour le tra_c " Best E_ort "

AC_BK : pour le tra_c Background

Le tableau suivant présente les valeurs des paramètres de la méthode d'accès EDCA utilisés dans le standard [25].

AC	CW_{min}	CW_{max}	AIFSN
AC_VO	3	7	2
AC_VI	7	15	2
AC_BE	15	1023	3
AC_BK	15	1023	7

Tableau 6 : Affectation du AIFSN, *CWmin* et *CWmax* pour les différentes ACs.

La différenciation de service proprement dite se fait par une affectation d'espace inter trames AIFS et de valeurs de *CWmin* et *CWmax* non identiques pour les catégories de d'accès citées. En effet, on affecte à chaque AC un triplet (Tableau 6). Chaque AC détient son propre compteur de Back-off qui est désormais compris entre 1 et 1+*CW*[*AC*].

Quand deux ACs finissent en même temps leur durée de backoff, alors c'est le paquet de plus haute priorité qui sera transmis. Les autres entités doivent augmenter leurs fenêtres de backoff.

Lorsqu' une trame arrive dans une file AC vide et le canal reste libre pendant *AIFS*[*AC*]+ *SlotTime*, elle est transmise immédiatement. Dans le cas contraire (c-à-d canal occupé), chaque trame qui arrive dans une des files *AC* doit attendre la libération du canal puis elle diffère sa transmission pendant *AIFS* + *SlotTime*.

D'une façon similaire au standard 802.11, des compteurs de retransmission sont aussi définis pour 802.11e. Le 802.11e introduit en plus une durée de vie maximale des MSDU dans chaque file d'attente. Dépassant cette durée dans la sous couche MAC la trame est éliminée.

Cette approche est efficace pour des applications temps réel pour lesquelles des trames transmises en retard n'ont plus d'intérêt.

Durant la contention au canal, quand les compteurs de backoff de deux ou plusieurs entités de backoff d'une station donnée atteignent la valeur zéro au même instant, une collision virtuelle a lieu. Mises à part les autres stations essayant d'accéder au canal, pour cette station, l'entité de backoff avec la plus haute priorité va transmettre sur le canal. Les autres entités réagissent comme si une vraie collision avait lieu sur le canal.

La figure suivante représente la contention des quatre classes de trafic pour l'accès au canal en utilisant l'ensemble des paramètres.

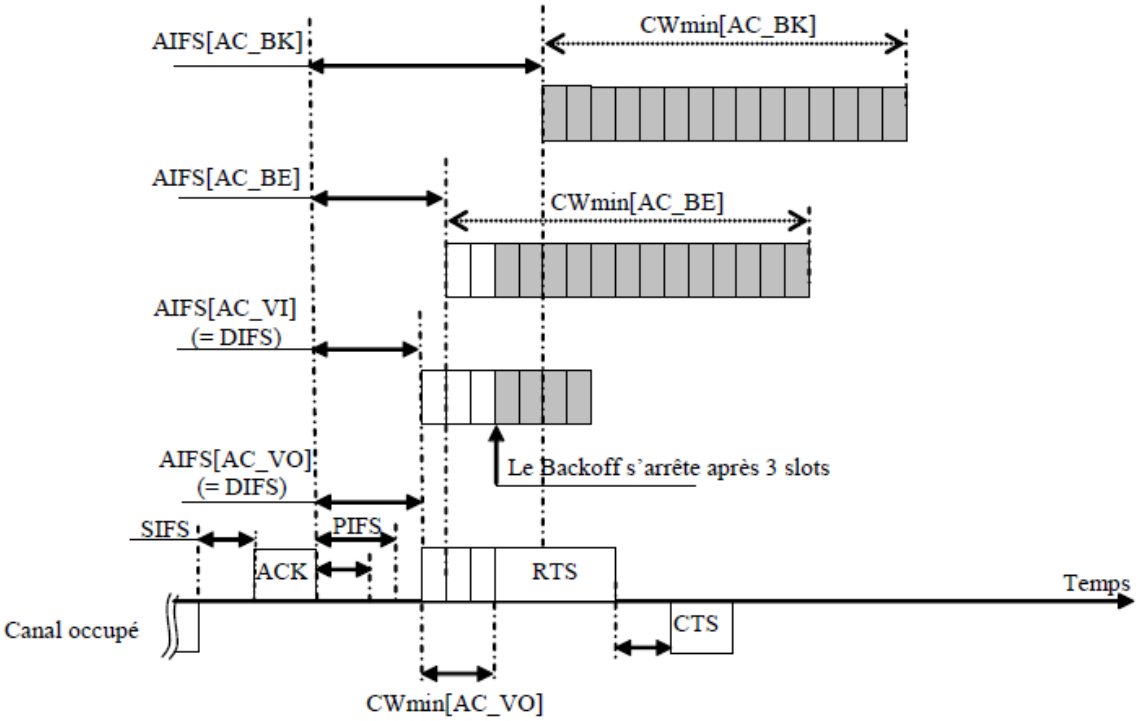


Figure 21 : La contention au canal pendant une période EDCA [26]

HCF Controlled Channel Access HCCA

Le mode d'accès contrôlé de la méthode HCF, nommé HCCA, est un mode d'accès sans contention au canal. Les entités de backoff d'une station donnée seront explicitement sollicitées par le HC pour une possibilité de transmission sur le canal. Pour lancer ce mode, le HC doit tout d'abord accéder au canal au cours du mode EDCA : le HC possède la plus haute priorité par rapport à l'ensemble des catégories d'accès. En effet, le HC est autorisé à transmettre si le canal est libre pendant une durée PIFS (sans backoff). Le point coordinateur ou HC commence par transmettre une trame de contrôle QoS CF-Poll.

Cette trame est utilisée pour scruter les stations voulant émettre par la suite en mode sans contention. Elle définit aussi les débuts et les durées maximales des transmissions HCCA-TXOP. Durant une période HCCA-TXOP, une station peut transmettre plusieurs trames selon un algorithme d'ordonnancement dans la limite du temps maximal alloué (TXOPlimit). Un temps SIFS

sépare deux trames consécutives d'un même émetteur. Le mode HCCA est beaucoup plus flexible que le mode PCF du standard 802.11. En effet, en plus de la période sans contention, un QAP11 peut initier une période HCCA-TXOP à tout moment pendant la période avec contention. Cependant, pour garantir des périodes de temps suffisantes pour le mode EDCA, une durée maximale du mode HCCA est définie par la variable TCAPLimit [27]. La Figure 4.4 illustre un exemple de supertrame 802.11e.

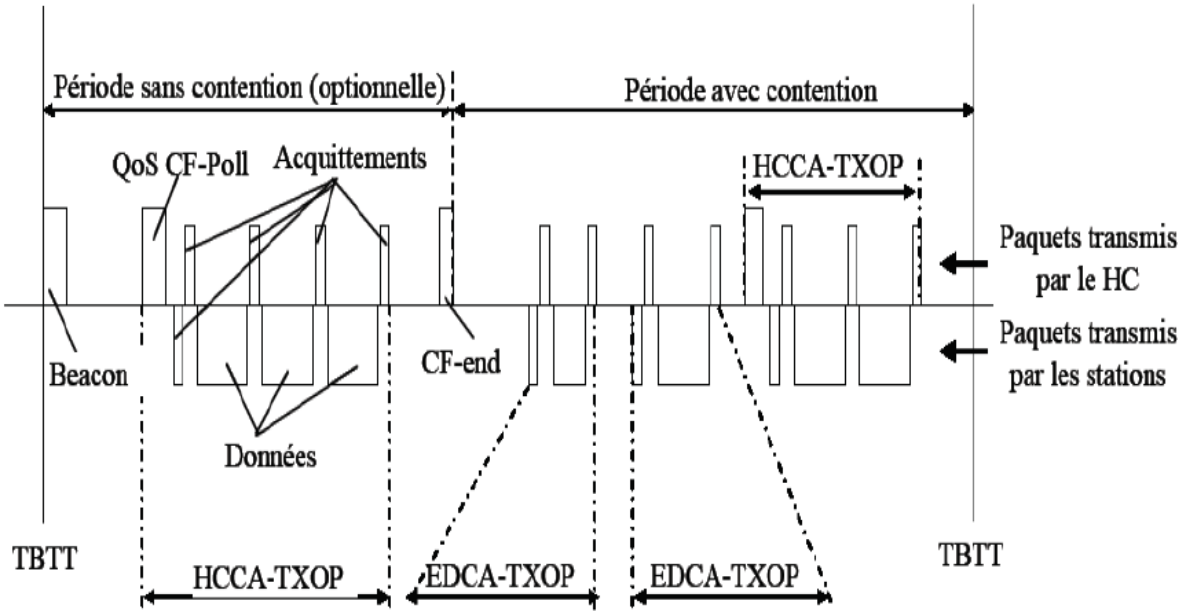


Figure 22 : Procédure HCF [27]

Section 2 : Présentation et conception de l'approche proposée.

1. La position du problème

Le problème de la QoS sur IP a fait l'objet d'un grand intérêt. Mais le support de la QoS sur des liens sans-fil et l'intégration de mécanismes de QoS avec la mobilité reste une question ouverte,

- le premier problème, concerne le provisionnement, est relatif au dimensionnement des ressources de chaque domaine, qu'il s'agit d'adapter aux besoins des clients potentiels.
- le second problème est relatif à la disponibilité des ressources sur le chemin de donnée ; sa solution nécessite qu'un conditionneur de trafic soi mis en place au niveau de chaque station QSTA

2. Approche proposée

Nous proposons une solution pour la mise en œuvre de la QoS dans les réseaux sans fil, basée sur le modèle DiffServ. Il s'agit d'introduire DiffServ pour un partage et une utilisation efficace du support sans fil par les applications les plus exigeantes. La première partie de la solution consiste à

établir un couplage dynamique entre les classes Diffserv et les ACs 802.11e, la deuxième partie c'est d'introduire un conditionneur de trafic afin de limiter le volume du trafic admis dans le réseau.

a. Architecture de cette approche

Le réseau global est constitué de deux réseaux d'accès sans fil et d'un domaine DiffServ filaire. Le domaine Diffserv est constitué d'un nœud Core router et deux nœuds Edge router.

L'un des réseaux d'accès représente le 802.11e en ajoutant le mapping (EDCA-Diffserv) au niveau du QAP et l'autre réseau sera un réseau sans fil ordinaire 802.11e.

3. Simulation sans le mapping

Pour faire la simulation du réseau présenté sur la figure il a fallu suivre les étapes si dessous :

1ère étape :

Pour notre application, la version choisie du NS est 2.29 [voir Annexe], n'intègre que la méthode d'accès DCF relative à la norme IEEE 802.11. Alors il a fallu intégrer la norme 802.11e afin de pouvoir tester la méthode d'accès EDCF pour faire la comparaison avec notre solution de couplage.

Son implémentation exige :

- des modifications de certains fichiers NS tels que :
  - /ns-2.29/Makefile.in.
  - /ns-2.29/tcl/lib/ns-lib.tcl.
  - /ns-2.29/tcl/lib/ns-default.tcl .
  - /ns-2.29/tcl/lan/ns-mac.tcl
- Suppression de certains fichiers tels que :
  - tcl/lib/ns-mobilenode.tcl .
- Intégration des fichiers décrivant le code de la norme 802.11 e.

L'EDCF définit les paramètres suivants [15] :

· Quatre queues à priorité sont uniquement définies au lieu de 8.

· Le facteur de persistance PF est neutralisé à 2.

· La valeur minimale des AIFS est passée de SIFS à DIFS.

· Les paramètres relatifs aux queues (AIFS, CWMIN, CWMAX, TXOP-limit) ont acquis de nouvelles valeurs.

Les files d'attentes EDCF se caractérisent par des priorités. Ces priorités sont associées à l'une des quatre files d'attente des catégories d'accès EDCF par une instance définie au dessus de ces files. La priorité '0' est définie comme la plus haute priorité.

Nous allons commencer par simuler un réseau sans le mapping, nous avons proposé de simuler l'architecture si dessous qui se constitue d'un réseau diffserv et de deux réseaux d'extrémité 802.11e.

Dans nos simulations, nous allons considérer trois types de trafic : voix, vidéo et données.

La différentiation de services est assurée en associant chacun des services à une catégorie d'accès relative à l'IEEE 802.11e. Selon la définition des catégories d'accès et les caractéristiques des services, l'association se fait de la manière suivante

Services	Catégorie d'accès	Priorité
Voice	AC_VO	0
Vidéo	AC_VI	1
Data	AC_BK	2

Tableau 7 : Association trafic/AC

2ème étape :

La deuxième étape est la configuration du domaine Diffserv qui lie les deux réseaux d'accès 802.11e.

La configuration du modèle DiffServ dans un réseau dans NS2 passe par les étapes suivantes:

- Etablir la nature des routeurs du réseau : routeur de bordure (edge) ou routeur (core)

Exemple de code: $ns simplex-link $edge $core 1Mb 1ms dsRED/edge

$ns simplex- link $core $edge1Mb 1ms dsRED/core

- Configurer les files d'attentes suivant le modèle DiffServ au niveau des liens entre les différents routeurs.
  Exemple de code : set qEC [[$ns link $edge $core] queue]
- Ajouter les DiffServ Policy. Ces derniers permettent de spécifier pour chaque trafic le niveau de service permis dans le réseau.

clicours.com

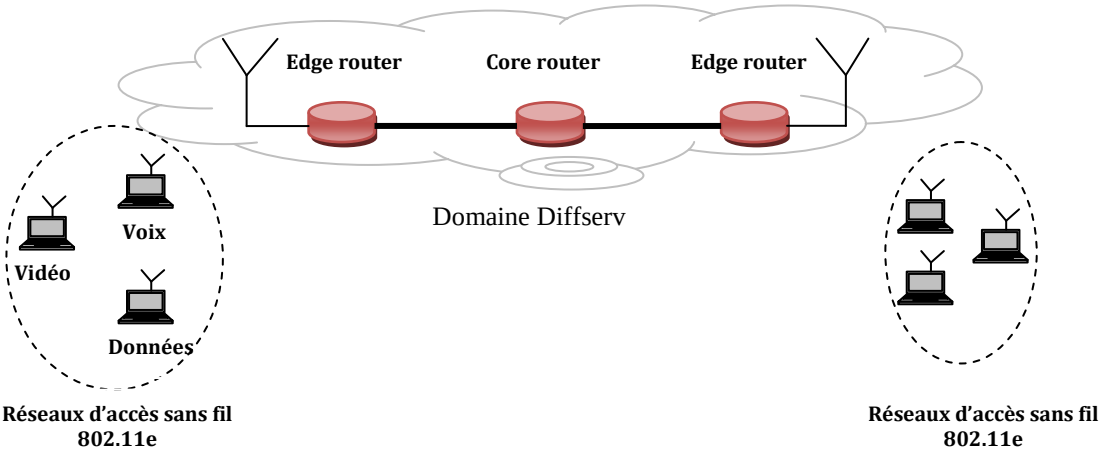


Figure 23 : Architecture globale du réseau à simuler

4. Simulation avec mapping « 802.11e et Diffserv »

Cette partie de notre travail consiste en la présentation de notre solution pour contribuer à la gestion de qualité de service de bout en bout. Pour ce faire il fallait suivre les étapes suivantes :

a) Configurer le mapping Diffserv 802.11e :

Nous proposons de réaliser une architecture de gestion de qualité de services en se basant sur la mise en place du couplage entre les PHBs Diffserv et les catégories d'accès 802.11e dans un module distinct et indépendant. Ce module est appelé QMM "Sos Mapping module».

Le QMM s'assurera du couplage entre les PHBs DiffServ et les catégories d'accès 802.11e en attribuant le bon PHB à sa catégorie correspondante. Le mapping est mis en place à l'intérieur du module QMM, aucun besoin de communication entre le nœud Diffserv et le QAP. Une transparence est donc réalisée tout au long de l'architecture.

Le QMM est très simple dans son fonctionnement, car il ne fait que consultation de table, ainsi que la lecture et écriture des en-têtes MAC et IP d'un paquet. Le QMM peut être placé à l'intérieur du QAP, comme le montre la figure 29.

Le QMM est ajouté en tant que module dans le QAP, ce dernier doit lire / écrire l'en-tête IP dans les paquets pour pouvoir lire et écrire les le champ DSCP. Lorsqu'un paquet arrive dans un nœud de bordure Diffserv, le module QMM l'intercepte et lui donne une priorité 802.11e correspondante à la valeur de son champ DSCP Diffserv. Quand le paquet arrive au nœud de cœur « QSTA » ramène la valeur du DSCP Diffserv.

L'architecture proposé dans le document c'est l'implémentation du module QMM entre deux interface différente : Filaire 802.3 Ethernet et sans fil 802.11e WLAN.

Dans cette implémentation, aucune des modifications du nœud de bordure Diffserv ni la couche MAC WLAN n'ai nécessaire. Le QMM doit être ajouté au niveau du QAP « nœud de bordure ».

Le mapping proposé n'utilise que trois des quatre catégories d'accès :

- EF « expedited forwarding » → AC_VO
- AF « assured forwarding » → AC_VI
- BE « best effort » → AC_BE

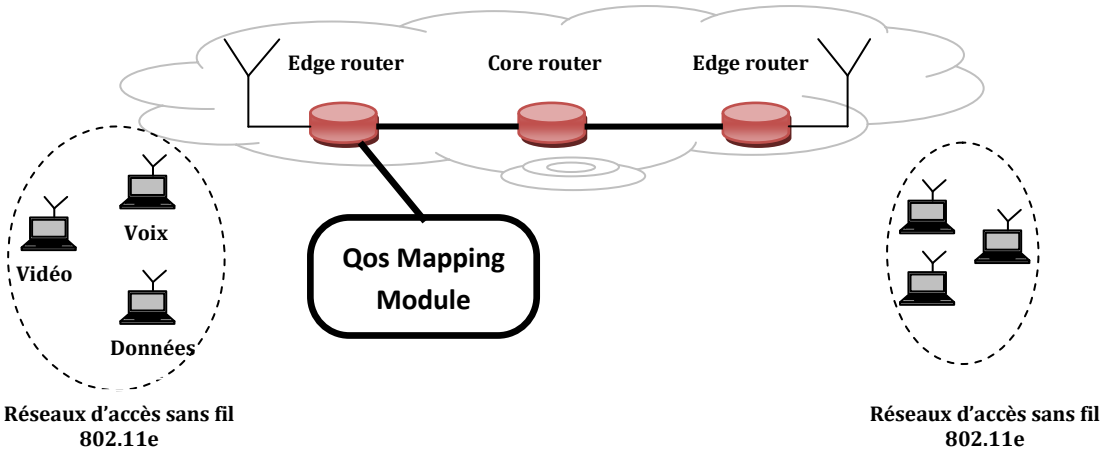


Figure 24 : Architecture proposée

b) Implémentation du conditionneur de trafic :

Afin de gérer la disponibilité des ressources sur le chemin de donnée ; la solution nécessite qu'un conditionneur de trafic soi mis en place au niveau de chaque station QSTA

Le conditionneur de trafic peut contenir plusieurs éléments :

Le METER : permet de savoir si le flot de paquets entrant correspond au profil de trafic négocié

Il est paramétré par un profil temporel et des niveaux de conformité « chaque niveau est associé à une sortie.

Un trafic jugé non conforme par le METER est dirigé vers le DROPPER « effaceur » les flux AF et EF conforme sont dirigés vers le MARKER

Le MARKER : permet la mise à jour du champ DS par le placement d'un code point particulier de comportement DS d'où le DSCP.

Le SHAPER : « lissage » peut s'effectuer lorsque les flux d'une classe dépassent le contrat SLA prédéfini

Donc les paquets seront mis en fil d'attente afin d'être transmis un peut plus tard

Clicours.COM

En résumé le SHAPER à deux fonctionnalités :

- Mise en forme du trafic
- Surveillance du trafic « retarder le paquet ou l'éliminer »

Dans le cas d'un réseau Diffserv le conditionneur de trafic se situe au niveau des nœuds de bordure (edge router), Mais dans notre solution nous avons mis en place un conditionneur de trafic au niveau de chaque station QSTA car parmi les fonctions de gestion de qualité de service au niveau des QSTA est la réaction à la congestion (filtre et élimination des paquets).

Pour réaliser la réaction à la congestion nous avons mis en place deux des éléments que peut contenir un conditionneur de trafic : la surveillance du trafic (POLICING) et le lissage (SHAPING). L'algorithme Shaper implémenté est illustré sur la figure 30.

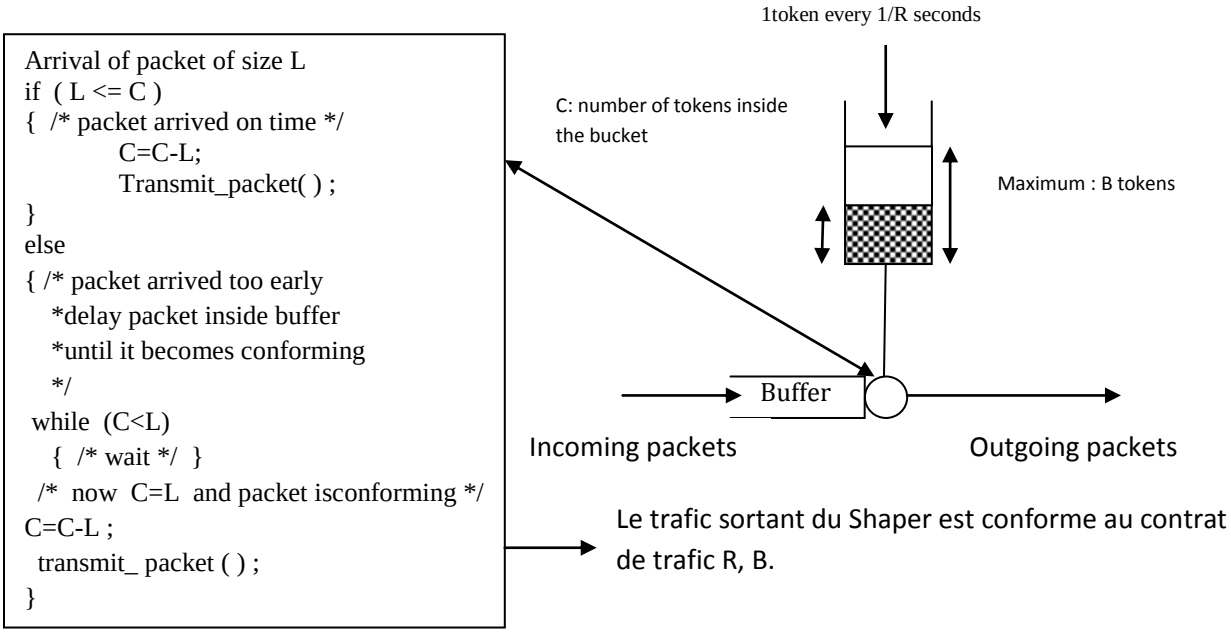


Figure 25 : Token Bucket (Shaping Mode)

5. Simulation d'un réseau congestionné

La troisième simulation est de tester notre solution cas d'un réseau congestionné.

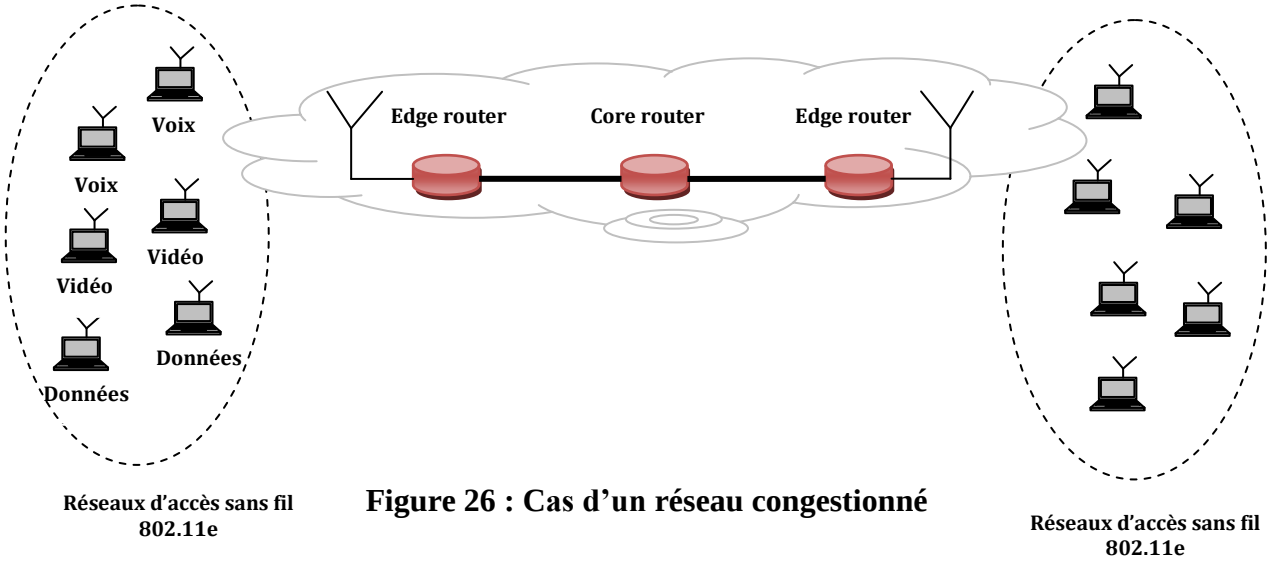


Figure 26 : Cas d'un réseau congestionné

5. Conclusion

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau utilisées d'une façon optimale.

Chapitre 5 : Simulations

Ce chapitre présente : La simulation sur NS 2 et l'évaluation des résultats de notre approche.

Sommaire

1. Introduction

Ce chapitre présente les travaux de simulation, et d'évaluation, liés à nos contributions à la gestion de qualité de services dans les réseaux sans fils. Ces travaux portent sur :

L'implémentation de la norme 802.11e au niveau du simulateur NS afin de contribuer à la gestion de qualité de service en réalisant le couplage entre les catégories d'accès ACs de l'IEEE 802.11e 802.11e et les PHBs Diffserv. Pour ce faire nous somme passer par plusieurs étapes qui seront détaillées dans les sections qui suivent.

2. Simulation avec NS (Network Simulator)

Nous avons implémenté la solution de couplage dans NS. Des tests ont été effectués afin de montrer l'utilité d'avoir la QoS de bout en bout. Pour cela, nous avons simulé la configuration définie dans la figure 28. Le réseau global est constitué de deux réseaux d'accès sans fils et d'un domaine DiffServ. Notre modèle de simulation est composé de trois stations mobiles qui émettent des flux cbr0, cbr1 et cbr2 modélisant respectivement l'audio, la vidéo et des données classiques. Les sources transmettent au même instant t0 à 2 Mbit/s.

Le modèle de simulation utilise une extension du logiciel NS qui intègre des fonctionnalités de l'architecture DiffServ. Trois files d'attente sont gérées représentant chacune les trois types de trafic (audio, vidéo, données). Nous avons effectué des simulations pour deux scenarios : 802.11e et 802.11e avec le mapping et le conditionneur de trafics.

2.1. Le simulateur NS2

2.1.1. Introduction

Le simulateur NS est un outil logiciel de simulation de réseaux informatiques, développé dans le cadre du projet VINT, ce dernier est un projet en cours de développement avec la collaboration de plusieurs acteurs (USC/ISI, Xerox parc, LBNL et UCB) dans l'objectif principal de construire un simulateur multiprotocole pour faciliter l'étude de l'interaction entre les protocoles et le comportement d'un réseau à différentes échelles.

Le projet contient des bibliothèques pour la génération de topologies réseau, des trafics ainsi que des outils de visualisation tels que l'animateur réseau NAM (network animator).

2.1.2. Présentation du simulateur NS2

NS est un outil logiciel de simulation de réseaux informatiques. Il est essentiellement élaboré avec les idées de la conception par objets, de la réutilisation du code et de modularité. Il est aujourd'hui un standard de référence en ce domaine, plusieurs laboratoires de recherche recommandent son utilisation pour tester les nouveaux protocoles.

Le simulateur NS actuel est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de grande taille (le test du passage à l'échelle). Il contient les fonctionnalités nécessaires à l'étude des algorithmes de routage unicast ou multicast, des protocoles de transport, de session, de réservation, des services intégrés, des protocoles d'application comme FTP. A titre d'exemple la liste des principaux composants actuellement disponibles dans NS par catégorie est :

• application : Web, ftp, telnet, générateur de trafic (CBR...) ;
• transport : TCP, UDP, RTP, SRM ;
• routage unicast : Statique, dynamique (vecteur distance) ;
• routage multicast : DVMRP, PIM ;
• gestion de file d'attente : RED, DropTail, Token bucket.

2.1.3. L'outil de visualisation NAM

NS-2 ne permet pas de visualiser le résultat des expérimentations. Il permet uniquement de stocker une trace de la simulation, de sorte qu'elle puisse être exploitée par un autre logiciel, comme NAM.

NAM est un outil de visualisation qui présente deux intérêts principaux : représenter la topologie d'un réseau décrit avec NS-2, et afficher temporellement les résultats d'une trace d'exécution NS-2. Par exemple, il est capable de représenter des paquets TCP ou UDP, la rupture d'un lien entre nœuds, ou encore de représenter les paquets rejetés d'une file d'attente pleine. Ce logiciel est souvent appelé directement depuis les scripts TCL pour NS-2, pour visualiser directement le résultat de la simulation.

2.1.4. Installation du simulateur NS2

Maintenant que nous avons vu quelques-unes des notions de base sur le simulateur NS-2, regardons comment cela se passe dans le monde réel.
Notez bien que l'installation et la simulation vont être faites sur une distribution GNU Linux Ubuntu.

Prérequis

Pour l'installation du ns2, on doit tout d'abord installer les paquets suivants :

• build-essential ;
• autoconf ;
• Automak ;
• libxmu-dev.

Cela par la commande suivante (sous Fedora pour Ubuntu vous allez utiliser apt-get au lieu de yum):

```
su -
yum install build-essential autoconf automake libxmu-dev
```

téléchargement et installation

Le téléchargement du NS2 se fait par la commande suivante (il faut remplacer le X par la version du NS2 que vous voulez installer, personnellement je travaille avec la version 2.31) :

```
wget http://nchc.dl.sourceforge.net/sourceforge/nsnam/ns-allinone-vX.tar.gz
```

Après la décompression de l'archive avec la commande tar -xzvf ns-allinone-X.tar.g, vous tapez la commande d'installation suivante après l'accès au dossier ns-allinone-X :

```
./install
```

L'étape la plus importante est la gestion des variables d'environnement qui s'affichent après la fin d'installation. La déclaration de ces variables se fait dans le fichier .bashrc comme suivant (il faut changer les X, Y, Z, T par les versions que vous avez) :

```
# LD_LIBRARY_PATH
OTCL_LIB=/home/<votre dossier personnel>/el>/ns-allinone-X/otcl-Y
NS2_LIB=/home/<votre dossier perso>/ns-allinone-2.31/lib
X11_LIB=/usr/X11R6/lib
USR_LOCAL_LIB=/usr/local/lib
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_
LIB:$USR_LOCAL_LIB

# TCL_LIBRARY
TCL_LIB=/home/<votre dossier personnel>/ns-allinone-2.31/tclZ/library
USR_LIB=/usr/lib
export TCL_LIBRARY=$TCL_LIB:$USR_LIB

# PATH
XGRAPH=/home/<votre dossier perso>/ns-allinone-2.31/bin:/home/<votre dossier perso>/
ns-allinone-X/tclZ/unix:/home/<votre dossier perso>/ns-allinone-2.31/tk8.4.14/unix
NS=/home/<votre dossier perso>/ns-allinone-X/ns-X/
NAM=/home/<votre dossier perso/-allinone-X/nam-T/
PATH=$PATH:$XGRAPH:$NS:$NAM
```

Après chaque changement au niveau du fichier .bashrc, on doit le recharger sinon on est obligé de redémarrer le terminal avec la commande :

```
$ source ~/.bashrc
```

Pour tester l'installation il suffit de lancer la commande ns qui affichera un % indiquant le bon fonctionnement de notre simulateur NS2. Une étape optionnelle de validation qui va tester des exemples de simulation déjà implémentés (cette étape prend plus ou moins de temps selon la puissance de la machine) :

```
cd ns-X
./validate
```

2.2. Paramètres de Simulation

2.2.1. Débit utile (throughput)

Le débit utile (ou throughput) est le débit total en réception. Il est calculé pour un intervalle de temps, en divisant la quantité totale d'information reçue pendant cet intervalle, par la durée de l'intervalle en question.

La formule générale pour le calcul du débit utile est ainsi :

$$throughput = \frac{nombre\ des\ paquets\ reçus\ pendant\ \Delta t * taille\ d'un\ paquet}{\Delta t}$$

Avec :

Δt : durée de l'intervalle considéré.

t : limite supérieure de l'intervalle Δt.

2.2.2. Le taux de pertes

Nous avons modélisé ce taux de pertes par le nombre de bits perdus en fonction du temps. Pour cela, nous avons utilisé l'agent Loss Monitor qui enregistre le nombre de paquets perdus dans sa variable associés n_lost.

2.2.3. Le délai

Le délai est le temps entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Nous le calculons pour un paquet donné de la manière suivante :

Délai = tr - ts avec tr : instant de réception du paquet et ts : instant de son émission.

Ainsi, toutes les courbes de délai qui suivent représentent le délai en fonction du temps d'émission.

2.3. Évaluation des résultats

2.3.1. Simulation 802.11e sans le mapping

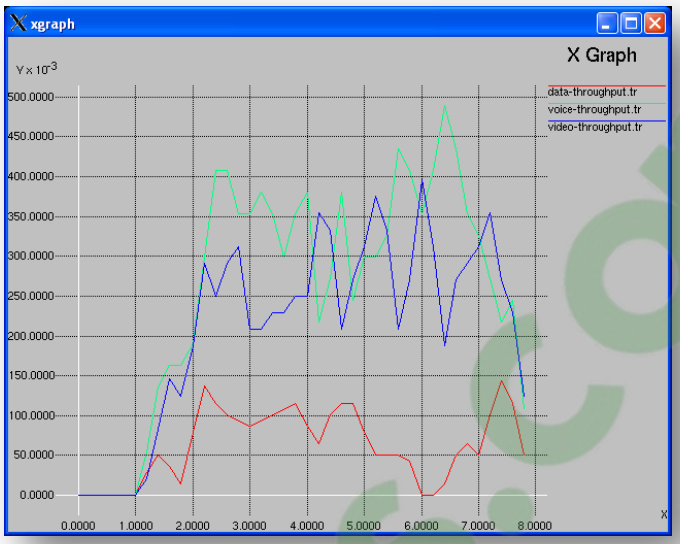


Figure 27 : Débit utile en Mo par rapport au temps

L'analyse de la courbe précédente montre bien que le 802.11e permet de favoriser les trafics les plus prioritaires. Plus le trafic est prioritaire, plus il est servi.

A t=0s, les trois stations commencent à émettre avec un débit très faible, à t=2s tous les débits sont augmentés mais le plus visible est pour la station voix car c'est la plus prioritaire.

Tout au long de la simulation la station voix est la mieux servi.

Ainsi, les pertes générées au niveau de la station donnée diminuent est la plus élevée car c'est la moins prioritaire.

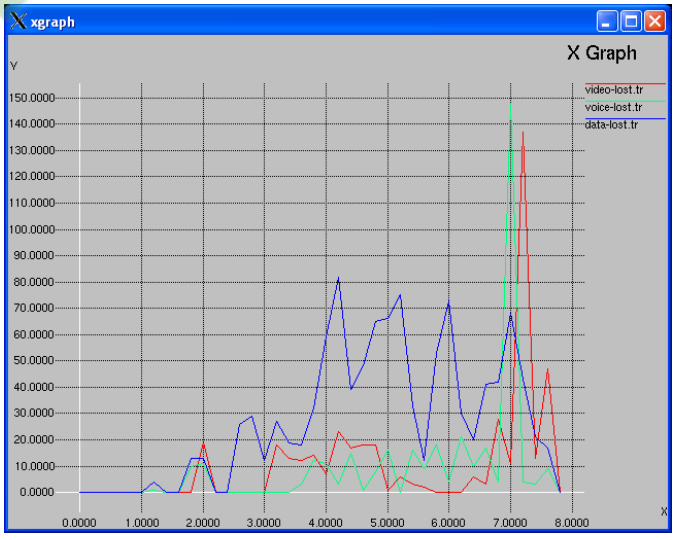


Figure 28 : Nombre de paquet perdus par rapport au temps

2.3.2. Simulation avec Mapping et mise en place du conditionneur

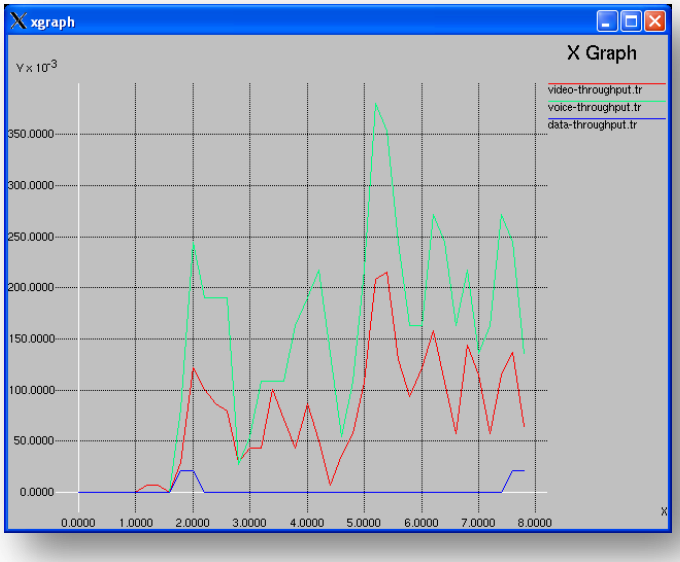


Figure 29 : Débit utile en Mo par rapport au temps

L'architecture proposée gère très bien la gestion de la qualité de service de bout en bout. Les résultats montrent une nette amélioration des performances du trafic donnée (trafic le moins prioritaire) par rapport aux autres trafics, à savoir voix et vidéo.

L'analyse de la courbe Figure 34 présentant le débit utile de chaque type de trafic en fonction du temps, montre bien l'amélioration de la gestion ddu débit pour les trois type de trafic en gardant le principe du plus prioritaire est le mieux servis.

En conclusion on peut dire que la combinaison de la différentiation de service et le conditionnement du trafic fournit un meilleur traitement que le 802.11e pour les paquets de faible priorité dans les files d'attente, et accroît sa probabilité d'accès au canal.

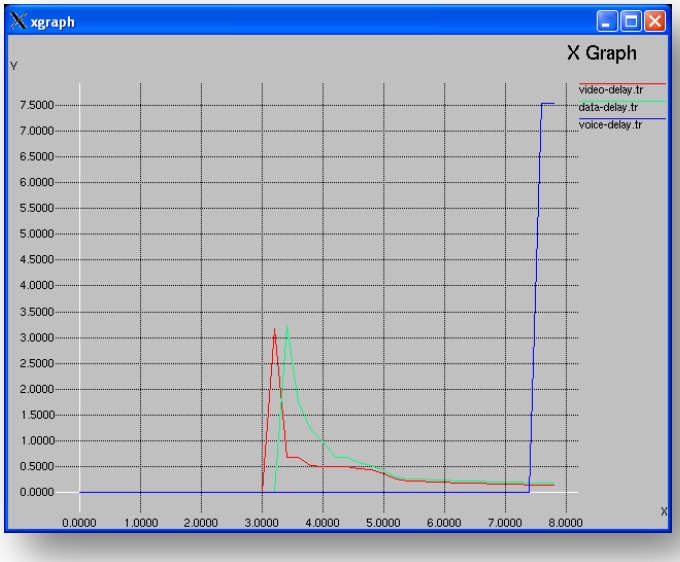


Figure 30 : Délai avec qualité de service de bout en bout

La figure 35 illustre le délai de bout en bout des flux voix et vidéo et Donnée. On observe un délai nul pour le trafic Voice c'est-à-dire que la réception des paquets est immédiate, ce délai augmente pour les autre type de trafic à l'instant t=3s mais ça diminuent j'usqu'a atteindre un délai très faible à la fin de simulation.

Nous avons finalement évalué les pertes au niveau de chaque type de trafics, présentée dans la figure 36 on observe une nette amélioration en cas d'introduction de la gestion de qualité de service de bout en bout.

En conclusion, le couplage défini permet d'harmoniser la qualité de service dans les réseaux d'accès et dans le backbone. En effet, il permet à une classe de service d'observer le même comportement dans les deux niveaux de réseaux ceci afin d'améliorer la gestion de bout en bout de la qualité de service des classes de trafics.

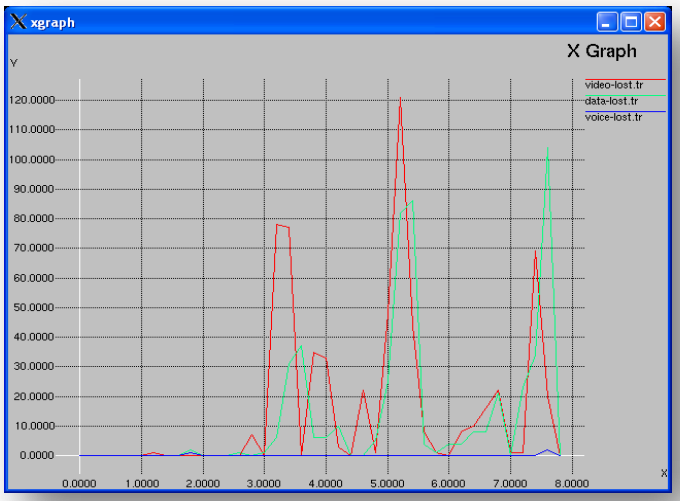
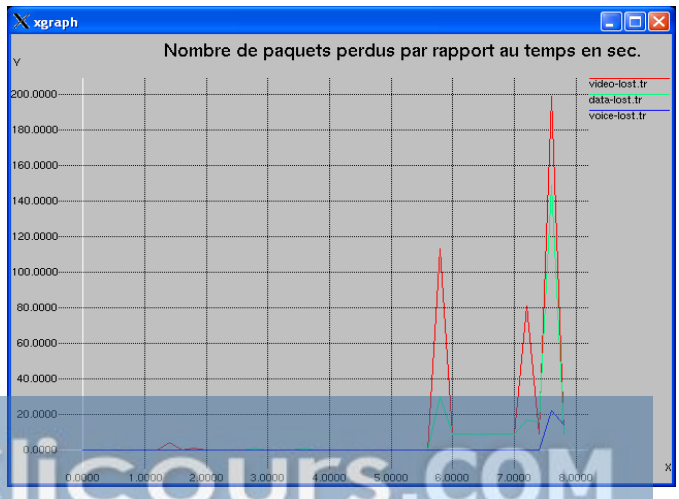


Figure 31 : Nombre de paquets perdus par rapport au temps

2.3.3. Cas d'un réseau Congestionné



Clicours.COM

Figure 32 : Nombre de paquet perdus par rapport au temps

Nous avons simulé la contribution de la gestion de qualité de service sur un réseau congestionnée illustré dans la figure 37, 38, cette étude nous a permis d'évaluer les performances de notre solution sur un réseau congestionné.

Les résultats de la simulation sont presque identique que la simulation d'un réseau simple ce qui signifie que notre solution de gestion de qualité de service est performante au niveau d'un réseau simple et un réseau congestionné.

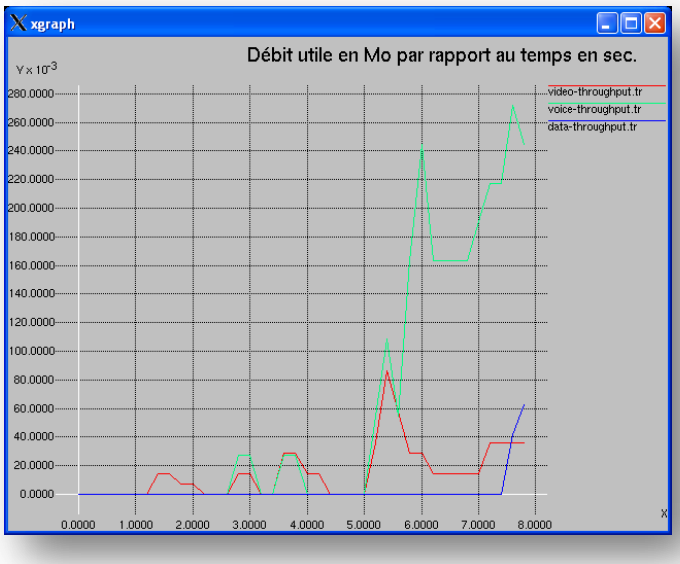


Figure 33 : Débit utile en Mo par rapport au temps

2.3.4. Evaluation des performances de l'approche simulée

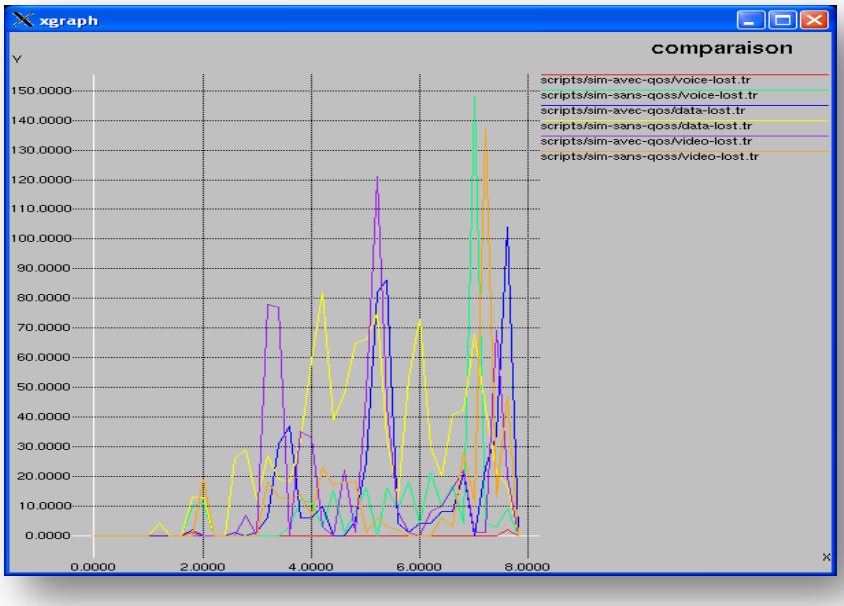


Figure 34 : Perte de paquets avec/sans mapping

L'analyse de la figure 39 montre très bien que les pertes des trafics diminuent progressivement avec mapping. D'après tous ces résultats, il est clair que réaliser une différentiation de service IP dans les réseaux filaires ou mobiles fournit une meilleure qualité de service surtout pour les trafics les moins prioritaires. Les paquets prioritaires peuvent être retardés par des paquets moins prioritaires. Dans ce cas, les paquets les moins prioritaires peuvent aussi attendre plus de temps pour accéder au médium. Par conséquent, les paquets prioritaires sont encore plus pénalisés dans leur accès au lien.

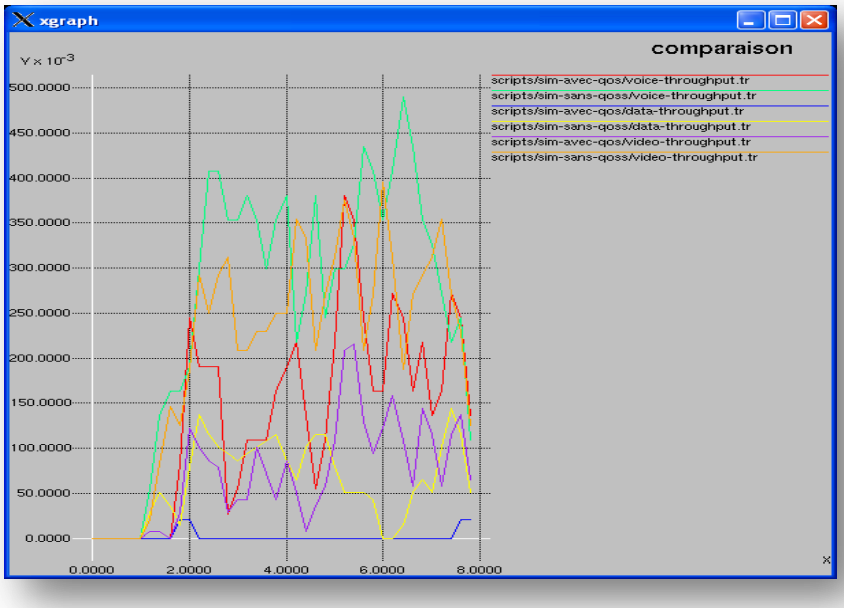


Figure 35 : Débit utile avec sans maping

Cette figure montre une amélioration des débits. En utilisant le «mapping»

3. Conclusion

Le but de notre travail était d'aboutir à la gestion de bout en bout en assurant la qualité de service. Nous avons contribué à cette gestion dans le réseau backbone et proposé une solution pour l'introduire dans les réseaux d'accès sans fil. Notre dernière contribution a été donc une étude du couplage (mapping) entre DiffServ et les schémas de qualité de service dans le réseau d'accès 802.11e en première partie, la deuxième partie de notre travail était de mêttre en œuvre un conditionneur de trafic au niveau de chaque station QSTA.

Conclusion générale & Perspectives

L'objectif principal de la mise en application d'une stratégie de QoS dans un réseau informatique est de fournir le meilleur service possible en se basant sur des règles et politiques de priorités qui expédient les données de façon personnalisée pour les différents clients - le terme client pouvant s'appliquer a des personnes physiques mais aussi à des applications ou plus simplement des flux réseaux -.

Pour les réseaux rapides et de tailles importantes, il est préférable d'implémenter l'architecture des services différenciés dans la mise en place de QoS. Ce modèle est nous l'avons vu le plus approprié pour les grandes structures car il fonctionne sur un principe de classification et de priorités.

Dans un réseau il est recommandé d'appliquer QoS au niveau des goulots d'étranglement.

Avec une stratégie de QoS judicieuse il est possible d'améliorer considérablement les performances d'un réseau sans avoir à faire de gros changements architecturaux ou devoir augmenter la largeur de bande disponible.

Les architectures basées sur le modèle de services différenciés telle que DiffServ s'appuient sur des mécanismes d'ordonnancement, de prévention et de gestion de congestion pour offrir des services flexibles. Une gestion soutenue de la qualité de service par l'architecture DiffServ impose un dimensionnement adéquat du réseau et une configuration optimale des paramètres qui interviennent dans la garantie de la QoS.Il reste que la QoS dépend des services fournis par les réseaux d'accès où le sans fil occupe une place prépondérante. Nous avons analysé la solution de différentiation de services pour introduire la QoS dans les réseaux d'accès sans fil afin d'améliorer les performances des flux prioritaires qui entrent dans un réseau sans fil.

Notre but ultime était d'aboutir à la gestion de bout en bout de la QoS. Nous avons contribué à cette gestion et proposé des solutions pour l'introduire dans les réseaux d'accès sans fil. Notre dernière contribution a été donc une étude de l'interopérabilité entre DiffServ et les schémas de QoS dans le réseau d'accès 802.11e. Nous avons mis en correspondance les services de DiffServ et ceux issus des schémas de QoS dans 802.11e, vue : les flux voix, vidéo et données.

Perspectives

Le sujet abordé dans ce mémoire peut être encore étendu et amélioré, en élargissant nos travaux et contribuer à la gestion de qualité de services dans les réseaux locaux sans fil sans infrastructure c'est-à-dire réseaux adhoc.

Bibliographies

[01] 80211. IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks- Specific requirements - Part *11* : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), 2007.

[02] 80211. IEEE Std *802.11-1997* Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part *11* : Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications. IEEE Std 802.11-1997, 1997.

[03] 802.11e. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part *11* : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment *8* : Medium Access Control (MAC) Quality of Service Enhancements. IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)), 2005.

[04] 802.11k. IEEE Standard for information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part *11* : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment *1* : Radio Resource Measurement of Wireless LANs. IEEE Std 802.11k-2008 (Amendment to IEEE Std 802.11-2007), 2008.

[05] 802.11r. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements part *11* : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment *2* : fast Basic Service Set (BSS). IEEE Std 802.11r-2008 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008), 2008.

[6] Thèse Présentée pour l'obtention du titre de : Docteur de l'Université Henri Poincaré, Nancy I « Spécialité Automatique, Traitement du Signal et Génie Informatique » Et : Docteur de l'Ecole Nationale d'Ingénieurs de Sfax « Spécialité Ingénierie des Systèmes Informatiques » Par Issam JABRI. « Gestion dynamique des topologies sans fils », 2007.

[7] A. Balachandran, G.M. Voelker, P. Bahl, et P.V. Rangan, "Characterizing user behavior and network performance in a public wireless LAN", June 15-19 2002, ACM SIGMETRICS international conference on measurement and modelling of computer systems (Marina Del Rey, California).

[8] A. Balachandran, G.M. Voelker, P. Bahl, "Hot spot congestion relief in public-area wireless networks", June 20-21 2002, 4th workshop on mobile computing systems and applications (Callicoon, NY, USA) pp 70-80.

[9] D. Kotz et K. Essien, "Characterizing usage of a campuswide wireless network", September 23-28 2002, 8th annual ACM international conference on mobile computing and networking (Westin Peachtree Plaza,

Atlanta, Georgia, USA), pp 107-118.

[10] D. Tang et M. baker, "Analysis of a metropolitain area wireless network", March-May 2002, Wireless Networks (Kluwer Academic Publishers), Vol. 8 (2-3), pp 107-120.

[11] IEEE 802.11 WG, 2003. Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer(PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/Draft 4.2.

[12] S. Mangold, S. Choi, G. R. Hiertz, O. Klein et B. Walke, " Analysis of IEEE 802.11e for QoS support in wireless LANs", IEEE Wireless Communications, Vol. 10, 2003.

[13] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Speci_c requirements Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) speci_cations : Amendment 8 : Medium Access Control (MAC) Quality of Service Enhancements.

[14] Thèse présentée pour obtenir le diplôme de Docteur de l'École Supérieure des Communications de Tunis; Spécialité : Technologie de l'Information et de la Communication. Présentée par : Olfa Bouatay. Titre de la thèse : Gestion de la consommation d'énergie dans les réseaux ad hoc via la différenciation de service

[15] I.Aad and C. Castellucia, « differentiation mechanisms for IEEE 802.11 », in Proc. Of IEEE INFOCOM'01, Anchodage, Alaska, USA, April 2001.

[16]. ITU-T Recommendation X 739 (1993) ISO/IEC 10164-12, Information Technology-Open System Interconnection-Structure of Management Information: Metric Objects and Attributes.

[17]. Vogel, A., Kerherv_e, B., von Bochman, G., Gecsei, J., 1995. Distributed multimedia and QOS: A survey. IEEE Multimedia Magazine 3, 10-19.

[18]. ISO/IEC, "The ODP Trading Function", ISO/IEC JTC1/SC21 1995.

[19]. Malamos, A. G., Varvarigou, T. A., and Malamas, E. N., (1999) Quality Of Service Admission Control For Multimedia End-Systems, *Proc. IMACS/IEEE CSCC'99*, Greece.

[20]. D. Chalmers and M. Sloman, A Survey of Quality of Services in Mobile Computing Environments, *IEEE Communications Survey*, pp. 2-10, Second Quarter 1999.

[21]. 802.1D-1998, Part 3 : Media Access Control (MAC) Bridges, ANSI/IEEE Std. 802.1D.

[22]. Q. Ni, L. Romdhani and T. Turletti, " A survey of QoS enhancements for IEEE 802.11 wireless LAN", Journal of wireless communications and mobile computing, Vol. 4, No. 5, pp. 547-566, 2004.

[23]. S. Mangold, S. Choi, G. R. Hiertz, O. Klein et B. Walke, " Analysis of IEEE 802.11e for QoS support in wireless LANs", IEEE Wireless Communications, Vol. 10, 2003.

[24]. Y. L Kuo, C. H. Lu, E. H. K.Wu, G. H. Chen and Y. H. Tseng, " Performance analysis of the enhanced distributed coordination function in the IEEE 802.11e", IEEE 58th Vehicular Technology Conference, VTC 2003-Fall, Vol. 5, Pages : 3488_3492, 2003.

[25]. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Speci_c requirements Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) speci_cations : Amendment 8 : Medium Access Control (MAC) Quality of Service Enhancements.

[26]. M. Gast, "802.11 Wireless networks : the de_nitive guide", O'reilly, 2002.

[27]. Q. Ni, " Performance analysis and enhancements for IEEE802.11e wireless networks", IEEE Network, 2005.

[28]. Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., & Weiss, W. (1998). An Architecture for Differentiated Services. IETF RFC 2475.

[29]. Nichols, K., Blake, S., Baker, F., and Black, D. (1998). Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 headers. IETF RFC 2474.

[30]. Heinanen, J., Baker, F., Weiss, W., & Wroclawski, J. (1999). Assured Forwarding PHB Group. IETF RFC 2597.

[31]. Jacobson, V. (1999). An Expedited forwarding PHB. IETF RFC 2598.

[32]. [RFC2475] : RFC Diffserv http://www.ietf.org/rfc/rfc2475.txt

[33]. Introduction à la problématique des Réseaux avec QoS –Eléments d'Architecture de l'Internet à QoS. Eric Gressier-Soudan. http://arcad.essi.fr/cours/reseau2/02-IREQoS2002-b.pdf. Janvier 2002.

[34]. QoS IP : modèles IntServ / DiffServ. Jean Sébastien NATCHIA KOUAO et Abdelkader BENLAHCEN.http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesr o2002t tnfa03/NatchiaKouao-Benlahcen/index.htm. 2003.

[35]. Les réseaux 6 ème édition. Guy Pujolle. Eyrolles. 2008.

[36] J. W. Roberts, " Qualité de service, tarification et contrôle d'admission dans l'Internet », CENT/DAC, RHDM, Brest, France, Septembre 1999

[37] T. Bonald and J. W. Roberts, "Performance of bandwith Sharing Mechanisms for Service Differenciation in the Internet", ITC Specialist Seminar, Monterey, CA, USA, 18-20 September, 2000

[38] S. Shenker, "Fundamental Design Issues for the Future Internet", IEEE Journal of Selected Areas in Communication, vol. 13, no. 7, September 1995, pp. 1176-1188

[39] J. W. Roberts, "Engineering for Quality of Sevice", France Télécom – CNET, Issy les moulineaux, France, July 1998

[40] H. J. Einsiedler and al., "Differentiated Services – Network Configuration and Management, Service Models and Architectures", EURESCOM Technical Information, pp.1-28, January 2001

[41] J. Postel, "Transmission Control Protocol", RFC 793, September 1981

[42] R. Guérin and V. Persi, "Quality-of-Service in Packet Networks: Basic Mechanisms and Directions", Computer Networks, Vol. 31, N. 3, pp. 169-189, February 1999

[43] P. White and J. Crowcroft. "Integrated services in the Internet : the next stage in Internet : state of the art", Proceedings of the IEE, Vol.85, no.12, pp.1934-1946, December 1997

[44] R.Braden, D.Clark, S.Shenker, "Integrated Services in the Internet Architecture: an Overview" , RFC 1633, June 1994

[45] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997

[46] F. Baker, J. Krawczyk, A. Sastry, "RSVP Management Information Base using SMIv2", RFC 2206, September 1997

[47] L. Berger, T. O'Malley, "RSVP Extensions for IPSEC Data Flows" , RFC 2207 , September 1997

[48] A. Mankin, and all, "Resource ReSerVation Protocol (RSVP) -- Version 1 Applicability Statement -- Some Guidelines on Deployment", RFC 2208, September 1997

[49] R. Braden, L. Zhang, "Resource ReSerVation Protocol (RSVP) -- Version 1 Message Processing Rules", RFC 2209, September 1997

[50] P. White and J. Crowcroft. "Integrated services in the Internet : the next stage in Internet : state of the art", Proceedings of the IEE, Vol.85, no.12, pp.1934-1946, December 1997

[51] S. Shenker, J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements", RFC 2215, September 1997

[52] J. Wroclawski, "Specification of the Controlled-Load Network Element Service", RFC 2211, September 1997

[53] S. Shenker, C. Partridge, R. Guerin, "Specification of Guaranteed Quality of Service", RFC 2212, September 1997

[54] J. Crowcroft, M.Handley, I.Wakeman, "Internetworking Multimedia", 290 pages, 1st edition, November 1999

[55] L.Zhang, and all, "RSVP : A New Resource reservation Protocol", IEEE Network Magazine, pp. 8-18, September 1993

[56] S.Gai, D.Dutt, N.Elfassy, Y.Bernet, "RSVP+ : An Extension to RSVP", Internet Draft , June 1999. draft-sgai-rsvp-plus-00.txt

[57] C.Deleuze, "Qualité de Service dans l'Internet : Problèmes liés au haut débit et au facteur d'échelle", Thèse de Doctorat, Université Paris VI, Janvier 2000

[58] P. Pan, H. Schulzrinne, "YESSIR : A Simple Reservation Mechanism for the Internet", Computer Communication Review ACM SIGCOMM , Vol.29, no2, April 1999

[59] H. Schulzrinne, "Resource Control and Reservation", Advanced Internet Services Course, October 2001 Available at : http://www.cs.columbia.edu/~hgs/teaching/ais/slides/rsvp.pdf

[60] F. Li, N. Seddigh, B. Nandy, and D. Matute. "An Empirical Study of Today's Internet Traffic for Differentiated Services IP QoS", The Fifth IEEE Symposium on Computers and Communication (ISCC 2000), Antibes, France, July 2000

[61] K. Nichols, V. Jacobson, L. Zhang, "RFC 2638 - A Two-bit Differentiated Services Architecture for the Internet" , July 1999

[62] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998

[63] K. Kilkki, J.Ruutu, "Simple Integrated Media Access – an Internet Service Based on Priorities", Proceedings of the 6th International Conference on Telecommunication Systems Modeling and Analysis - TN, USA- March 5-8, 1998

[64] D.Clark, W.Fang, "Explicit Allocation of Best Effort Packet Delivery Service", ACM Transactions on Networking, August 1998

[65] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "RFC 2597 - Assured Forwarding PHB Group" , June 1999

[66] V. Jacobson, K. Nichols, K. Poduri, "RFC 2598 - An Expedited Forwarding PHB" , June 1999

[67] Anurag, "Study of Expedited Forwarding in Differentiated Service and its Performance Characteristics using CBQ Implementation"

[68] D. Clark, S. Shenker, L.Zhang, "Supporting Real-Time Applications in an Integrated Services Packet Network : Architecture and Mechanisms", ACM SIGCOMM'92, pp 14-26, August 1992

[69] X. Xiao and L.Ni, "Internet QoS : The Big Picture", IEEE Network, vol.13, no.2, pp.1-13

[70] O. N. Medina Carvajal, " Etude des Algorithmes d'Attribution de Priorités dans un Internet à Différenciation de Services », Thèse de Doctorat – Université de Rennes 1, Mars 2001

[71] O. N. Medina, J-M. Bonnin, L. Toutain, " Service DiffServ pour les flux audio et vidéo", Colloque Francophone pour l'Ingénierie des Protocoles (CFIP'2000), Toulouse, France, 17-20 Octobre 2000

[72] GAUCHARD David, laboratoire d'analyse et d'architecture des systèmes (LAAS-CNRS) Simulation Hybride des Réseaux IP-DiffServ-MPLS Multi-services sur Environnement d'Exécution Distribuée, Avril 2003 : LAAS CNRS à Toulouse.

[73] Seyong Park, Kyungtae Kim, Doug C. Kim, Sunghyun Choi, Sangjin Hong "Collaborative QoS Architecture between DiffServ and 802.11e Wireless

clicours.com

Résumé

Les réseaux locaux sans fils IEEE 802.11 sont de plus en plus utilisés. Les débits atteints aujourd'hui par ces réseaux permettent d'exécuter des applications complexes nécessitant des garanties sur le débit, le délai ou encore la gigue des communications. Plusieurs travaux de recherches ont été proposés pour apporter un support de qualité de service aux réseaux locaux sans fil dotés de la norme IEEE 802.11. Ces travaux, dont l'IEEE 802.11e, sont pour la plupart basés sur une différentiation de services. Dans ce travail nous proposons une gestion de qualité de service appliquée aux environnements Diffserv et au standard IEEE 802.11e. Cette gestion se base sur le couplage dynamique entre les composants Diffserv et les classes de service EDCA. Pour compléter cette gestion, nous proposons une architecture qui permet d'intégrer les fonctionnalités du conditionneur de trafics afin de limiter le volume du trafic admis dans le réseau pour maintenir la stabilité des files d'attente des classes prioritaires.

Mots clefs :

Réseaux locaux sans fils; Files d'attente 802.11; Qualité de services; Diffserv; Intserv; Couplage; Conditionneur de trafics; 802.11e; EDCA.

Clicours.COM