Groupe de travail Réseau
Request for Comments : 2998
Catégorie : Information
Novembre 2000

Y. Bernet & P. Ford, Microsoft
R. Yavatkar, Intel
F. Baker, Cisco
L. Zhang, UCLA
M. Speer, Sun Microsystems
R. Braden, ISI
B. Davie, Cisco
J. Wroclawski, MIT LCS
E. Felstaine, SANRAD

Traduction Claude Brière de L'Isle

Cadre pour le fonctionnement de services intégrés (Intserv) sur les réseaux Diffserv

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
L'architecture des services intégrés (Intserv, *Integrated Services*) donne le moyen de livrer de la qualité de service (QS) de bout en bout aux applications sur des réseaux hétérogènes. Pour prendre en charge le modèle de bout en bout, l'architecture Intserv doit être acceptée sur une grande variété de types d'éléments de réseau différents. Dans ce contexte, un réseau qui prend en charge les services différenciés (Diffserv, *Differentiated Services*) peut être vu comme un élément de réseau sur le chemin de bout en bout total. Le présent document décrit un cadre dans lequel les services intégrés peuvent être pris en charge sur les réseaux Diffserv.

Table des matières

1. Introduction

Le travail sur les réseaux IP à capacité de qualité de service (QS) a conduit à deux approches distinctes : l'architecture des services intégrés (Intserv) [RFC1633] et le protocole de signalisation qui l'accompagne, RSVP [RFC2205], et l'architecture des services différenciés (Diffserv) [RFC2475]. Le présent document décrit la façon dont un réseau Diffserv peut être utilisé dans le contexte de l'architecture Intserv pour prendre en charge la fourniture de la QS de bout en bout.

1.1 Architecture des services intégrés

L'architecture de services intégrés définit un ensemble d'extensions au modèle traditionnel au mieux de l'Internet dans le but de permettre de fournir aux applications la qualité de service de bout en bout. Un des composants clés de l'architecture est un ensemble de définitions de service ; l'ensemble actuel des services consiste en la charge contrôlée et en services garantis. L'architecture suppose l'utilisation d'un mécanisme explicite d'établissement pour porter les information aux routeurs de sorte qu'ils puissent fournir les services demandés aux flux qui les exigent. Alors que RSVP est l'exemple le plus largement connu d'un tel mécanisme d'établissement, l'architecture Intserv est conçue pour s'accommoder d'autres mécanismes.

Les services Intserv sont mis en œuvre par des "éléments de réseau". Bien qu'il soit courant pour les éléments de réseau d'être des nœuds individuels comme les routeurs ou les liaisons, des entités plus complexes, comme les "nuages" ATM ou les réseaux 802.3 peuvent aussi fonctionner comme éléments de réseau. Comme on l'expose plus en détails dans la suite de ce document, un réseau Diffserv (ou "nuage") peut être vu comme un élément de réseau au sein d'un réseau Intserv plus large.

1.2 RSVP

RSVP est un protocole de signalisation que peuvent utiliser les applications pour demander des ressources au réseau. Le réseau répond en admettant ou rejetant explicitement les demandes RSVP. Certaines applications qui ont des exigences de ressource quantifiables expriment ces exigences en utilisant les paramètres Intserv comme défini dans les spécifications de service Intserv appropriées. Comme noté ci-dessus, RSVP et Intserv sont séparables. RSVP est un protocole de signalisation qui peut porter des informations Intserv. Intserv définit les modèles pour exprimer les types de service, quantifier les exigences de ressource et déterminer la disponibilité des ressources demandées aux éléments de réseau pertinents (contrôle d'admission).

Le modèle d'utilisation de RSVP qui prévaut actuellement se fonde sur une architecture RSVP/Inserv combinée. Dans ce modèle, RSVP signale des exigences de ressource par flux aux éléments de réseau, en utilisant les paramètres Intserv. Ces éléments de réseau appliquent le contrôle d'admission Intserv aux demandes signalées. De plus, les mécanismes de contrôle de trafic sur l'élément de réseau sont configurés de façon à assurer que chaque flux admis reçoit le service demandé en strict isolement de tout autre trafic. À cette fin, la signalisation RSVP configure des classeurs de paquet de microflux (MF) [RFC2475] dans les routeurs à capacité Intserv le long du chemin du flux de trafic. Ces classeurs permettent un classement par flux des paquets sur la base des adresses IP et des numéros d'accès.

Les facteurs suivants ont gêné le déploiement de RSVP (et de l'architecture Intserv) dans l'ensemble de l'Internet :

1. L'utilisation d'états et de traitements par flux soulève des problèmes d'échelle pour les grands réseaux.
2. Seul un petit nombre d'hôtes génèrent actuellement la signalisation RSVP. Bien qu'on s'attende à ce que ce nombre croisse considérablement, de nombreuses applications peuvent ne jamais générer de signalisation RSVP.
3. Les mécanismes nécessaires de contrôle de politique – contrôle d'accès, authentification, et comptabilité – ne sont devenus disponibles que récemment [RFC2749].

1.3 Diffserv

À la différence de l'orientation par flux de RSVP, les réseaux Diffserv classent les paquets en un flux agrégé parmi un petit nombre de "classes", fondées sur le codet Diffserv (DSCP) dans l'en-tête IP du paquet. C'est ce qu'on appelle la classification des agrégats de comportement (BA, *behavior aggregate*) [RFC2475]. À chaque routeur Diffserv, les paquets

sont soumis à un comportement "par bond" (PHB, *per-hop behavior*) qui est invoqué par le DSCP. Le principal avantage de Diffserv est son adaptabilité. Diffserv élimine le besoin d'un état et d'un traitement par flux et s'adapte donc bien aux grands réseaux.

1.4 Rôles de Intserv, RSVP et Diffserv

On voit Intserv, RSVP et Diffserv comme des technologies complémentaires pour la recherche de la qualité de service de bout en bout. Ensemble, ces mécanismes peuvent faciliter le déploiement d'applications telles que la téléphonie IP, la vidéo à la demande, et diverses applications non multi supports à la mission critique. Intserv permet aux hôtes de demander par flux des ressources quantifiables le long de chemins de données de bout en bout et d'obtenir un retour en ce qui concerne l'admissibilité de ces demandes. Diffserv permet l'adaptabilité à travers les grands réseaux.

1.5 Composants de Intserv, RSVP et Diffserv

Avant d'aller plus loin, il est utile d'identifier les composants suivants des technologie de qualité de service décrites :

Signalisation RSVP - Ce terme se réfère au protocole de signalisation de la norme RSVP. La signalisation RSVP est utilisée par les hôtes pour signaler au réseau les exigences en ressources des applications (ainsi qu'à chacun d'entre eux). Les éléments de réseau utilisent la signalisation RSVP pour retourner les décisions de contrôle d'admission aux hôtes. La signalisation RSVP peut porter ou non des paramètres Intserv.

Le contrôle d'admission à un élément de réseau peut se fonder ou non sur le modèle Intserv.

Contrôle du trafic MF - Ce terme se réfère au contrôle de trafic qui est appliqué indépendamment à chaque flux de trafic individuel et exige donc de reconnaître les flux de trafic individuels via le classement MF.

Contrôle de trafic agrégé - Ce terme se réfère au contrôle de trafic qui est appliqué collectivement à des ensembles de flux de trafic. Ces ensembles de flux de trafic sont reconnus sur la base du classement par DSCP des agrégats de comportement (BA, *Behaviour Aggregate*). Dans le présent document, on utilise indifféremment les termes de "contrôle de trafic agrégé" et de "Diffserv".

RSVP agrégé – Bien que la définition existante de RSVP ne prenne en charge que les réservations par flux, des extensions en cours de développement à RSVP prévoient de permettre que des réservations RSVP soient faites pour du trafic agrégé, c'est à dire, des ensembles de flux qui puissent être reconnus par le classement par BA. Cette utilisation de RSVP peut être utile pour le contrôle des allocations de bande passante dans les réseaux Diffserv.

RSVP par flux – C'est l'utilisation conventionnelle de RSVP pour effectuer des réservations de ressource pour des microflux individuels.

RSVP/Intserv - Ce terme est utilisé pour se référer au modèle prédominant d'utilisation de RSVP qui inclut la signalisation RSVP avec des paramètres Intserv, les contrôles d'admission Intserv et le contrôle du trafic par flux aux éléments de réseau.

Région Diffserv – C'est un ensemble de routeurs contigus qui prennent en charge la classification par BA et le contrôle de trafic. Bien que de telles régions puissent aussi prendre en charge le classement MF, l'objectif du présent document est de décrire comment une telle région peut être utilisée pour la livraison de la qualité de service de bout en bout lorsque seul le classement par BA est effectué à l'intérieur de la région Diffserv.

Région non Diffserv – Ce sont les portions du réseau qui se trouvent en dehors de la région Diffserv. Une telle région peut aussi offrir une variété de types différents de classement et de contrôle de trafic.

Noter que pour les besoins du présent document, les caractéristiques qui définissent une région Diffserv sont le type de classement et le contrôle de trafic qui sont utilisés pour la livraison de la qualité de service de bout en bout pour une application particulière. Donc, bien qu'il puisse n'être pas possible d'identifier une certaine région comme "purement Diffserv" par rapport à tout le trafic qui s'écoule à travers la région, il est possible de la définir de cette façon du point de vue du traitement du trafic provenant d'une seule application.

1.6 Cadre

Dans le cadre présenté, la qualité de service quantitative de bout en bout est fournie en appliquant le modèle Intserv de bout en bout à travers un réseau contenant une ou plusieurs régions Diffserv. Les régions Diffserv peuvent, mais n'y sont pas obligées, participer à la signalisation RSVP de bout en bout pour les besoins de l'optimisation de l'allocation des ressource et la prise en charge du contrôle d'admission.

Du point de vue de Intserv, les régions Diffserv du réseau sont traitées comme des liaisons virtuelles qui connectent des routeurs ou hôtes à capacité Intserv (tout à fait comme une région de réseau 802.1p est traitée comme une liaison virtuelle dans [RFC2815]). Au sein des régions Diffserv du réseau, les routeurs mettent en œuvre des PHB spécifiques (contrôle de trafic agrégé). La quantité totale de trafic qui est admis dans la région Diffserv qui va recevoir un certain PHB peut être limitée par la régulation à la frontière. Il en résulte qu'on s'attend à ce que les régions Diffserv du réseau soient capables de prendre en charge le service de style Intserv demandé depuis la périphérie. Dans notre cadre, on traite de la prise en charge des services intégrés de bout en bout sur les régions Diffserv du réseau. Le but est de mettre en place une inter-opération sans solution de continuité. Par suite, l'administrateur de réseau est libre de choisir quelles régions du réseau agissent comme régions Diffserv. À une extrémité, la région Diffserv est poussée tout au long vers la périphérie, les seuls hôtes ayant la pleine capacité Intserv. À l'autre extrémité, Intserv est poussé tout le long du chemin vers le cœur, sans aucune région Diffserv.

1.7 Contenu

La section 3 expose les avantages qui peuvent être retirés de l'utilisation du contrôle de trafic agrégé fourni pas les régions de réseau Diffserv dans le contexte plus large de l'architecture Intserv. La section 4 présente le cadre et le réseau de référence. La section 5 détaille deux réalisations possibles du cadre. La section 6 expose les implications du cadre pour Diffserv. La section 7 présente des questions spécifiques des flux en diffusion groupée.

2. Avantages de l'utilisation de Intserv avec Diffserv

Le principal avantage du contrôle de trafic agrégé Diffserv est son adaptabilité. Dans la présente section, on expose les avantages que peut apporter l'interopération avec Intserv à une région de réseau Diffserv. Noter que cette discussion est dans le contexte de la desserte spécifique d'applications de qualité de service quantitative. On entend par là les applications qui sont capables de quantifier leur trafic et leurs exigences de qualité de service.

2.1 Contrôle d'admission fondé sur la ressource

Dans les réseaux Intserv, les applications de qualité de service quantitatives utilisent un mécanisme d'établissement explicite (par exemple, RSVP) pour demander des ressources du réseau. Le réseau peut en réponse accepter ou rejeter ces demandes. C'est le "contrôle d'admission explicite". Le contrôle d'admission explicite et dynamique permet de s'assurer que l'utilisation des ressources est optimale. Pour mieux comprendre cette question, considérons une région de réseau Diffserv qui ne fournit que du contrôle de trafic agrégé sans signalisation. Dans la région de réseau Diffserv, le contrôle d'admission est appliqué d'une façon relativement statique en provisionnant des paramètres de politique aux éléments de réseau. Par exemple, un élément de réseau à l'entrée d'une région de réseau Diffserv pourrait être provisionnée pour n'accepter que 50 kbit/s de trafic pour le DSCP EF.

Bien que de telles formes statiques de contrôle d'admission donnent un certain degré de protection au réseau, elles peuvent être assez inefficaces. Par exemple, considérons qu'il peut y avoir 10 sessions de téléphonie IP générées en dehors de la région de réseau Diffserv, chacune exigeant 10 kbit/s de service EF de la région de réseau Diffserv. Comme l'élément de réseau qui protège la région de réseau Diffserv est provisionné pour n'accepter que 50 kbit/s de trafic pour le DSCP EF, il va éliminer la moitié du trafic offert. Ce trafic sera éliminé de l'agrégation du trafic marqué EF, sans considération du microflux d'où il est originaire. Le résultat est qu'il est vraisemblable que sur les dix sessions de téléphonie IP, aucune n'obtiendra un service satisfaisant alors qu'en fait, il y a des ressources disponibles suffisantes dans la région de réseau Diffserv pour satisfaire cinq sessions.

Dans le cas d'un contrôle d'admission dynamique explicitement signalé, le réseau va signaler le rejet en réponse aux demandes de ressources qui iraient au delà de la limite des 50 kbit/s. Il en résulte que les éléments de réseau et applications en amont (y compris les hôtes d'origine) vont avoir les informations dont ils ont besoin pour prendre des actions correctives. L'application peut répondre en s'abstenant de transmettre, ou en demandant l'admission pour un moindre profil de trafic. Le système d'exploitation de l'hôte peut répondre en marquant le trafic de l'application avec le DSCP qui correspond au service au mieux. Les éléments de réseau en amont peuvent répondre en marquant à nouveau les paquets sur le flux rejeté à un niveau de service inférieur. Dans certains cas, il est possible de réacheminer le trafic sur des chemins de remplacement ou même des réseaux de remplacement (par exemple, le RTPC pour les appels vocaux). Dans tous les cas, l'intégrité de ces flux qui ont été admis sera préservée, aux dépens des flux qui n'ont pas été admis. Donc, en appointant un agent de contrôle d'admission dialoguant avec Intserv pour la région Diffserv du réseau, il est possible d'améliorer le service que peut fournir le réseau aux applications de qualité de service quantitative.

2.2 Contrôle d'admission fondé sur la politique

Dans les régions de réseau où RSVP est utilisé, les demandes de ressource peuvent être interceptées par les éléments de réseau à capacité RSVP et peuvent être revues en fonction des politiques mémorisées dans les bases de données de politiques. Ces demandes de ressource identifient en toute sécurité l'usager et l'application pour lesquels les ressources sont demandées. Par conséquent, l'élément de réseau est capable de considérer une politique par usager et/ou par application lorsque il décide d'admettre ou non une demande de ressource. Ainsi, en plus d'optimiser l'utilisation des ressources dans une région de réseau Diffserv (comme exposé au paragraphe 3.1) les agents de contrôle d'admission qui conversent avec RSVP peuvent être utilisés pour appliquer des politiques spécifiques du consommateur pour déterminer les flux de trafic spécifiques du consommateur qui ont le droit d'utiliser les ressources de la région de réseau Diffserv. Les politiques des consommateurs peuvent être utilisées pour allouer des ressources à des utilisateurs et/ou applications spécifiques.

Par comparaison, dans les régions de réseau Diffserv sans signalisation RSVP, les politiques sont normalement appliquées sur la base du réseau du consommateur Diffserv d'où est originaire le trafic, et non de l'utilisateur ou application d'origine au sein du réseau consommateur.

2.3 Assistance à l'identification/classification du trafic

Au sein des régions de réseau Diffserv, le trafic est desservi sur la base du DSCP marqué dans chaque en-tête IP de paquet. Donc, pour obtenir un niveau particulier de service au sein de la région de réseau Diffserv, il est nécessaire d'effectuer le marquage du DSCP correct dans les en-tête de paquet. Il y a deux mécanismes pour faire cela : le marquage de l'hôte et le marquage du routeur. Dans le cas du marquage de l'hôte, le système d'exploitation de l'hôte marque le DSCP dans les paquets transmis. Dans le cas de marquage du routeur, les routeurs dans le réseau sont configurés pour identifier un trafic spécifique (normalement sur la base de la classe MF) et pour marquer le DSCP lorsque les paquets transitent par le routeur. Chaque schéma présente ses avantages et ses inconvénients. Sans considération du schéma utilisé, la signalisation explicite offre des avantages significatifs.

2.3.1 Marquage d'hôte

Dans le cas du marquage par l'hôte, le système d'exploitation de l'hôte marque le DSCP dans les paquets émis. Cette approche présente l'avantage de déplacer le classement et le marquage par flux à la source du trafic, où ils s'adaptent le mieux. Il permet aussi à l'hôte de prendre des décisions concernant le marquage approprié pour chaque paquet émis et donc sur l'importance relative attachée à chaque paquet. L'hôte est généralement mieux équipé pour prendre ces décisions que le réseau. De plus, si le chiffrement IPSEC est utilisé, l'hôte peut être le seul appareil dans le réseau qui soit capable de faire une détermination significative du marquage approprié pour le marquage de chaque paquet, car divers champs comme les numéros d'accès seront indisponibles aux routeurs pour le classement MF.

Le marquage par l'hôte exige que celui-ci soit conscient de l'interprétation des DSCP par le réseau. Ces informations peuvent être configurées dans chaque hôte. Cependant, une telle configuration impose une charge de gestion. Autrement, les hôtes peuvent utiliser un protocole de signalisation explicite tel que RSVP pour interroger le réseau afin d'obtenir un DSCP ou un ensemble de DSCP convenables à appliquer aux paquets pour lesquels un certain service Intserv a été demandé. Un exemple de la façon dont ceci peut être réalisé est décrit dans [RFC2996].

2.3.2 Marquage de routeur

Dans le cas du marquage par le routeur, les critères de classement MF peuvent être configurés d'une certaine façon dans le routeur. Cela peut être fait de façon dynamique (par exemple, en utilisant le provisionnement COPS) par demande du système d'exploitation de l'hôte, ou de façon statique via configuration manuelle ou via des scripts automatisés.

Il y a des difficultés significatives à le faire de façon statique. Dans de nombreux cas, il est souhaitable d'allouer le service au trafic sur la base de l'application et/ou de l'usager qui génère le trafic. Certaines fois, il est possible d'identifier les paquets associés à une application spécifique par le numéro d'accès IP dans les en-têtes. Il est aussi parfois possible d'identifier les paquets originaires d'un utilisateur spécifique par l'adresse IP de source. Cependant, de tels critères de classement peuvent changer fréquemment. Les usagers peuvent se voir allouer des adresses IP différentes par DHCP. Les applications peuvent utiliser des accès provisoires. Pour compliquer encore plus les choses, plusieurs utilisateurs peuvent partager une adresse IP. Ces facteurs rendent très difficile la gestion d'une configuration statique des informations de classement requises pour marquer le trafic dans les routeurs.

Une solution de remplacement séduisante à la configuration statique est de permette au système d'exploitation de l'hôte de signaler les critères de classement au routeur au nom des utilisateurs et des applications. Comme on le montrera plus loin dans ce document, la signalisation RSVP convient idéalement à cette tâche. En plus de permettre la mise à jour dynamique et précise des critères de classement MF, la signalisation RSVP permet le classement des paquets IPSEC [RFC2401] (en utilisant le SPI) qui seraient autrement non reconnaissables.

2.4 Conditionnement du trafic

Les éléments de réseau à capacité Intserv sont capables de conditionner le trafic à la granularité du flux, par une combinaison de formatage et/ou de régulation. Le pré-conditionnement du trafic de cette manière avant sa soumission à la région Diffserv du réseau est bénéfique. En particulier, il améliore la capacité de la région Diffserv du réseau à fournir des services quantitatifs en utilisant le contrôle de trafic agrégé.

3. Le cadre

Dans le cadre général on envisage un Internet dans lequel l'architecture de services intégrés est utilisée pour livrer la qualité de service de bout en bout aux applications. Le réseau comporte des combinaisons de nœuds à capacité Intserv (dans lesquels est appliqué le classement MF et le contrôle de trafic par flux) et de régions Diffserv (dans lesquelles est appliqué le contrôle de trafic agrégé). Les routeurs individuels peuvent participer ou non à la signalisation RSVP sans considération de l'endroit où ils résident dans le réseau.

Nous allons considérer deux réalisations spécifiques du cadre. Dans la première, les ressources au sein des régions Diffserv du réseau sont provisionnées de façon statique et ces régions ne comportent pas d'appareil à capacité RSVP. Dans le second, les ressources au sein de la région Diffserv du réseau sont provisionnées de façon dynamique et choisissent les appareils qui participent à la signalisation RSVP au sein des régions Diffserv du réseau.

3.1 Réseau de référence

Les deux réalisations du cadre vont être exposées dans le contexte du réseau de référence suivant :

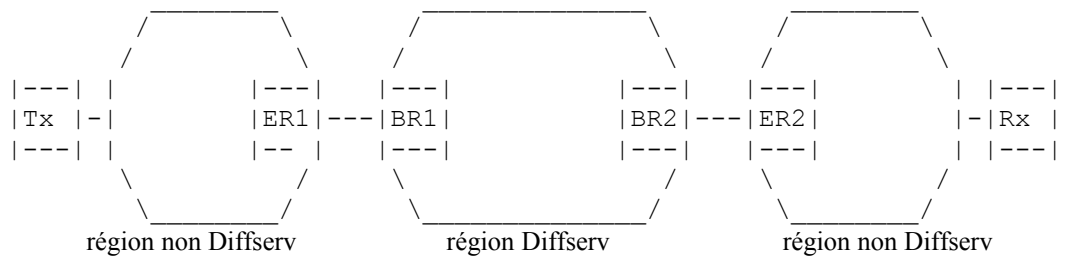

Figure 1 : Exemple de configuration de réseau

Le réseau de référence comporte une région Diffserv au milieu d'un plus grand réseau qui prend en charge Intserv de bout en bout. La région Diffserv contient un maillage de routeurs, dont au moins quelques uns fournissent le contrôle de trafic agrégé. Les régions en dehors de la région Diffserv (des régions non Diffserv) contiennent des maillages de routeurs et d'hôtes rattachés, dont au moins quelques uns prennent en charge l'architecture de services intégrés.

Pour simplifier, on considère un seul envoyeur de QS, Tx, qui communique à travers ce réseau avec un seul receveur de QS, Rx. Les routeurs bordures (ER1, ER2) qui sont adjacents à la région Diffserv font l'interface des routeurs frontières (BR1, BR2) au sein de la région Diffserv.

D'un point de vue économique, on peut considérer que la région Diffserv vend du service au réseau en dehors de la région Diffserv, qui à son tour fournit du service aux hôtes. Donc, on peut penser les régions non Diffserv comme des clients ou des consommateurs de la région Diffserv. Dans la suite de ce document, on utilise le terme "consommateur" pour les régions non Diffserv. Noter que les frontières des régions peuvent s'aligner ou non sur les frontières de domaines administratifs, et qu'une seule région peut contenir plusieurs domaines administratifs.

On définit maintenant les composants majeurs du réseau de référence.

3.1.1 Hôtes

On suppose que les hôtes aussi bien envoyeurs que receveurs utilisent RSVP pour communiquer les exigences quantitatives de qualité de service des applications à capacité de qualité de service qui fonctionnent sur l'hôte. En principe, d'autres mécanismes peuvent être utilisés pour établir des réservations de ressources dans les nœuds à capacité Intserv, mais RSVP est évidemment le mécanisme prépondérant dans ce domaine.

Normalement, un processus de qualité de service au sein du système d'exploitation de l'hôte génère de la signalisation RSVP au nom des applications. Ce processus peut aussi invoquer le contrôle de trafic local.

Comme on l'a exposé précédemment, le contrôle de trafic chez l'hôte peut marquer le DSCP dans les paquets transmis, et formater le trafic émis selon les exigences du service Intserv utilisé. Autrement, le premier routeur à capacité Intserv vers l'aval de l'hôte peut fournir ces fonctions de contrôle de trafic.

3.1.2 Signalisation RSVP de bout en bout

On suppose que les messages de signalisation RSVP voyagent de bout en bout entre les hôtes Tx et Rx pour prendre en charge les réservations RSVP/Intserv en dehors de la région de réseau Diffserv. On exige que ces messages RSVP de bout en bout soient au moins transportés à travers la région Diffserv. Selon les spécificités de la réalisation du cadre, ces messages peuvent être traités par aucun, quelques uns, ou tous les routeurs dans la région Diffserv.

3.1.3 Routeurs de bordure

ER1 et ER2 sont des routeurs de bordure, qui sont adjacents aux régions de réseau Diffserv. Les fonctionnalités des routeurs bordures varient selon les spécificités de la réalisation du cadre. Dans le cas où la région de réseau Diffserv n'a pas de capacité RSVP, les routeurs bordures agissent comme agents de contrôle d'admission pour le réseau Diffserv. Ils traitent les messages de signalisation provenant de Tx comme de Rx, et appliquent le contrôle d'admission sur la base de la disponibilité des ressources au sein de la région de réseau Diffserv et de la politique définie par le consommateur. Dans le cas où la région de réseau Diffserv est à capacité RSVP, les routeurs bordures appliquent le contrôle d'admission sur la base de la disponibilité des ressources locales et sur la politique définie par le consommateur. Dans ce cas, les routeurs bordures agissent comme agent de contrôle d'admission pour la région de réseau Diffserv.

Nous décrirons plus loin et plus à fond les fonctionnalités des routeurs bordures pour chacune des deux réalisations du cadre.

3.1.4 Routeurs frontières

BR1 et BR2 sont des routeurs frontières, qui résident dans la région de réseau Diffserv. Les fonctions des routeurs frontières varient selon les spécificités de la réalisation du cadre. Dans le cas où la région de réseau Diffserv n'est pas à capacité RSVP, ces routeurs agissent comme de purs routeurs Diffserv. À ce titre, leur seule responsabilité est de réguler le trafic soumis sur la base du niveau de service spécifié dans le DSCP et de l'accord négocié avec le consommateur (contrôle de trafic agrégé). Dans le cas où la région de réseau Diffserv est à capacité RSVP, les routeurs frontières participent à la signalisation RSVP et agissent comme des agents de contrôle d'admission pour la région de réseau Diffserv.

Nous décrirons plus en détails plus loin les fonctionnalités du routeur frontière dans chacune des deux réalisations du cadre.

3.1.5 Région de réseau Diffserv

La région de réseau Diffserv prend en charge le contrôle de trafic agrégé et est supposée n'être pas capable de faire le classement MF. Selon les spécificités de la réalisation du cadre, un certain nombre de routeurs au sein de la région Diffserv peuvent être à capacité RSVP et donc capables de signalisation et de contrôle d'admission par flux. Si les appareils dans la région Diffserv n'ont pas la capacité RSVP, il vont passer les messages RSVP de façon transparente avec un impact négligeable sur les performances (voir [ASQR]).

La région de réseau Diffserv fournit au moins deux niveaux de service sur la base du DSCP dans l'en-tête de paquet. Elle peut être un seul domaine administratif ou s'étendre sur plusieurs domaines.

3.1.6 Régions de réseau non Diffserv

Le réseau en dehors de la région Diffserv consiste en hôtes à capacité Intserv et en autres éléments de réseau. Les autres éléments peuvent inclure des routeurs et peut-être divers types de réseaux (par exemple, 802, ATM, etc.). Ces éléments de réseau peuvent raisonnablement être supposés prendre en charge Intserv, bien que ce ne soit pas obligé dans le cas de sur provisionnement. Même si ces éléments ne sont pas à capacité Intserv, on supposera qu'il vont passer les messages RSVP dont ils ont hérité. Les routeurs en dehors de la région de réseau Diffserv ne sont pas empêchés de fournir le contrôle de trafic agrégé à un sous ensemble du trafic qui passe à travers eux.

3.2 Transposition de service

Les demandes de service Intserv spécifient un type de service Intserv et un ensemble de paramètres quantitatifs connus sous

le nom de "flowspec". À chaque bond dans un réseau Intserv, les demandes du service Intserv sont interprétées sous une forme significative pour le support de couche liaison. Par exemple à un bond 802.1, les paramètres Intserv sont transposés en un niveau de priorité 802.1p approprié [RFC2815].

Dans notre cadre, les régions Diffserv du réseau sont analogues au segment commuté à capacité 802.1p décrit dans la [RFC2815]. Les demandes de services Intserv doivent être transposées en capacités sous-jacentes de la région de réseau Diffserv. Les aspects de la transposition incluent :

- le choix d'un PHB ou ensemble de PHB approprié pour le service demandé ;
- d'effectuer la régulation appropriée (y compris, peut-être du formatage ou remarquage) aux bordures de la région Diffserv;
- d'exporter les paramètres Intserv provenant de la région Diffserv (par exemple, pour mettre à jour les Adspec) ;
- d'effectuer le contrôle d'admission sur les demandes Intserv qui prennent en compte la disponibilité des ressources dans la région Diffserv.

La façon exacte dont s'effectuent ces fonctions va dépendre de la façon dont est gérée la bande passante à l'intérieur de la région de réseau Diffserv, ce qui fait le sujet du paragraphe 4.3.

Lorsque le PHB (ou l'ensemble de PHB) a été choisi pour un flux Intserv particulier, il peut être nécessaire de communiquer le choix du DSCP pour le flux aux autres éléments de réseau. Deux schémas peuvent être utilisés à cette fin, comme on l'expose plus loin.

3.2.1 Transposition par défaut

Dans ce schéma, il y a une transposition standard bien connue du type de service Intserv en DSCP qui va invoquer le comportement approprié dans le réseau Diffserv.

3.2.2 Transposition conduite par le réseau

Dans ce schéma, les routeurs qui parlent RSVP dans la région de réseau Diffserv (peut-être sur ses bordures) peuvent outrepasser la transposition bien connue décrite au paragraphe 4.2.1. Dans le cas où les DSCP sont marqués à l'entrée de la région Diffserv, les DSCP peuvent simplement être marqués à nouveau aux routeurs frontières. Cependant, dans le cas où le marquage de DSCP survient en amont de la région Diffserv, dans un hôte ou dans un routeur, le marquage approprié doit alors être communiqué en amont, à l'appareil marqueur. Cela peut être accompli en utilisant RSVP, comme décrit dans la [RFC2996].

La décision sur où marquer le DSCP et si il faut outrepasser la transposition de service bien connue est une affaire de politique décidée par l'administrateur de la région de réseau Diffserv en coopération avec l'administrateur du réseau adjacent à la région Diffserv.

3.2.3 Séparation de microflux

Les routeurs frontières qui résident à la périphérie de la région Diffserv vont normalement réguler le trafic soumis de l'extérieur de la région Diffserv afin de protéger les ressources au sein de la région Diffserv. Cette régulation sera appliquée sur la base de l'agrégat, sans considération des microflux individuels qui constituent chaque agrégat. Il en résulte qu'il est possible à un microflux qui se conduit mal de réclamer plus que sa part équitable des ressources au sein de l'agrégat, dégradant par là le service fourni aux autres microflux. Ce problème peut être réglé par :

1. Fournir une régulation par microflux chez les routeurs bordures – c'est généralement la localisation la plus appropriée pour la régulation des microflux, car cela pousse le travail par flux sur les bordures du réseau, où il s'adapte mieux. De plus, comme les routeurs à capacité Intserv qui sont en dehors de la région Diffserv sont chargés de fournir le service des microflux à leurs consommateurs et que la région Diffserv est chargée de fournir le service agrégé aux consommateurs, cette distribution des fonctionnalités reflète la distribution des responsabilités.

2. Fournir une régulation par microflux chez les routeurs frontières – cette approche a tendance à être moins adaptable que l'approche précédente. Elle impose aussi une charge de gestion à la région Diffserv du réseau. Cependant, elle peut être appropriée dans certains cas, pour que les routeurs frontières Diffserv offrent en prime à leurs consommateurs Intserv une régulation par microflux.

3. S'appuyer sur le formatage et la régulation en amont – dans certains cas, le consommateur peut faire suffisamment confiance au formatage de certains groupes d'hôtes pour ne pas exiger le reformatage ou la régulation à la frontière de la région Diffserv. Noter que même si les hôtes formatent correctement les microflux, ces flux formatés peuvent être distordus lors du transit à travers la région non Diffserv du réseau. Selon le degré de distorsion, il peut être nécessaire de

sur provisionner un peu les capacités agrégées dans la région Diffserv, ou de re-réguler en utilisant le 1 ou le 2 ci-dessus. Le choix d'un mécanisme ou de l'autre est une affaire de politique à décider chez l'administrateur du réseau en dehors de la région Diffserv.

3.3 Gestion de ressource dans les régions Diffserv

Il existe diverses options pour la gestion des ressources (par exemple, de bande passante) dans les régions de réseau Diffserv pour satisfaire aux besoins de bout en bout des flux Intserv. Ces options incluent :

- des ressources à provisionnement statique ;
- des ressources provisionnées de façon dynamique par RSVP ;
- des ressources à provisionnement dynamique par d'autres moyens (par exemple, une forme de courtier en bande passante).

La section suivante donne des détails sur l'utilisation de chacune de ces différentes approches.

4. Exemples détaillés du fonctionnement de Intserv sur des régions Diffserv

La présente section fournit des exemples détaillés de notre cadre en action. On expose deux exemples ; dans l'un, la région de réseau Diffserv n'a pas la capacité RSVP ; dans l'autre la région de réseau Diffserv a la capacité RSVP.

4.1 Région de réseau Diffserv à approvisionnement statique

Dans cet exemple, aucun appareil de la région de réseau Diffserv n'a la capacité RSVP. La région de réseau Diffserv est provisionnée de façon statique. Le ou les consommateurs des régions de réseau Diffserv et le propriétaire de la région de réseau Diffserv ont négocié un contrat statique (une spécification de niveau de service, ou SLS) pour la capacité de transmission à fournir au consommateur à chacun d'un certain nombre de niveaux de service Diffserv standard. La "capacité de transmission" peut être simplement une quantité de bande passante ou ce pourrait être un "profil" plus complexe impliquant un certain nombre de facteurs tels que la taille de salve, le débit de crête, l'heure, etc..

Il est utile de considérer chaque routeur dans le réseau consommateur comme consistant en deux moitiés, une moitié Intserv standard, qui fait l'interface avec les régions du réseau du consommateur et une moitié Diffserv qui fait l'interface avec la région de réseau Diffserv. La moitié Intserv est capable d'identifier et traiter le trafic avec une granularité par flux.

La moitié Diffserv du routeur peut être considérée comme consistant en un certain nombre d'interfaces de transmission virtuelles, une pour chaque niveau de service Diffserv négocié dans le SLS. Le routeur contient un tableau qui indique la capacité de transmission provisionnée, selon la SLS, à chaque niveau de service Diffserv. Ce tableau, conjointement avec la transposition par défaut décrite au paragraphe 4.2.1, est utilisé pour prendre les décisions de contrôle d'admission sur les flux Intserv qui traversent la région de réseau Diffserv.

4.1.1 Séquence d'événements de l'obtention de la QS de bout en bout

La séquence suivante illustre le processus par lequel une application obtient la qualité de service de bout en bout lorsque RSVP est utilisé par les hôtes.

1. Le processus de QS sur l'hôte envoyeur Tx génère un message PATH RSVP qui décrit le trafic offert par l'application d'envoi.

2. Le message PATH est porté vers l'hôte receveur, Rx. Dans la région de réseau à laquelle l'envoyeur est rattaché, le traitement standard RSVP/Intserv est appliqué aux éléments de réseau capables.

3. Au routeur bordure ER1, le message PATH est soumis au traitement standard RSVP et l'état PATH est installé dans le routeur. Le message PATH est envoyé plus loin à la région de réseau Diffserv.

4. Le message PATH est ignoré par les routeurs dans la région de réseau Diffserv puis traité en ER2 conformément aux règles de traitement RSVP standard.

5. Lorsque le message PATH atteint l'hôte receveur, le système d'exploitation génère un message RSVP RESV qui indique l'intérêt pour le trafic offert d'un certain type de service Intserv.

6. Le message RESV est ramené vers la région de réseau Diffserv et l'hôte envoyeur. Conformément au traitement

RSVP/Intserv standard, il peut être rejeté à tout nœud à capacité RSVP dans le chemin si les ressources sont réputées insuffisantes pour porter le trafic demandé.

7. À ER2, le message RESV est soumis au traitement RSVP/Intserv standard. Il peut être rejeté si les ressources sur l'interface aval de ER2 sont réputées insuffisantes pour porter les ressources demandées. Si il n'est pas rejeté, il va être transporté de façon transparente à travers la région de réseau Diffserv, pour arriver à ER1.

8. Dans ER1, le message RESV déclanche le traitement de contrôle d'admission. ER1 compare les ressources demandées dans la demande RSVP/Intserv aux ressources disponibles dans la région de réseau Diffserv au niveau de service Diffserv correspondant. Le niveau de service correspondant est déterminé par la transposition d'Intserv en Diffserv exposée précédemment. La disponibilité des ressources est déterminée par la capacité provisionnée dans la SLS. ER1 peut aussi applique une décision de politique telle que la demande de ressource puisse être rejetée sur la base de critères de politique spécifiques du consommateur, même si les ressources agrégées sont déterminées comme disponibles selon la SLS.

9. Si ER1 approuve la demande, le message RESV est admis et il lui est permis de continuer en amont vers l'envoyeur. Si il rejette la demande, le RESV n'est pas transmis et les messages d'erreur RSVP appropriés sont envoyés. Si la demande est approuvée, ER1 met à jour ses tableaux internes pour indiquer la réduction de capacité disponible au niveau de service admis sur son interface d'émission.

10. Le message RESV continue à travers la région de réseau à laquelle est rattaché l'envoyeur. Tout nœud RSVP dans cette région peut rejeter la demande de réservation à cause de ressources ou de politique inadéquates. Si la demande n'est pas rejetée, le message RESV va arriver chez l'hôte envoyeur, Tx.

11. À Tx, le processus de qualité de service reçoit le message RESV. Il interprète la réception du message comme l'indication que le flux de trafic spécifié a été admis pour le type de service Intserv spécifié (dans les nœuds à capacité). Il peut aussi apprendre le marquage de DSCP approprié à appliquer aux paquets pour ce flux à partir des informations fournies par le RESV.

12. Tx peut marquer le DSCP dans les en-têtes des paquets qui sont transmis sur le flux de trafic admis. Le DSCP peut être la valeur par défaut qui se transpose en le type de service Intserv spécifié dans le message RESV admis, ou il peut être une valeur fournie explicitement dans le RESV.

De cette manière, on obtient la qualité de service de bout en bout à travers une combinaison de réseaux qui prennent en charge RSVP/Intserv et de réseaux qui prennent en charge Diffserv.

4.2 Région de réseau Diffserv à capacité RSVP

Dans cet exemple, les routeurs de bordure du consommateur sont des routeurs RSVP standard. Le routeur frontière BR1 est à capacité RSVP. De plus, il peut y avoir d'autres routeurs au sein de la région de réseau Diffserv qui sont à capacité RSVP. Noter que bien que ces routeurs soient capables de participer à certaines formes de signalisation RSVP, ils classent et programment le trafic en agrégats, sur la base du DSCP, et non selon les critères de classement par flux utilisés par les routeurs RSVP/Intserv standard. On peut dire que leur plan de contrôle est RSVP alors que leur plan de données est Diffserv. Cette approche exploite les avantages de la signalisation RSVP tout en conservant beaucoup de l'adaptabilité associée à Diffserv.

Dans l'exemple précédant, il n'y a pas de signalisation entre la région de réseau Diffserv et les éléments de réseau qui lui sont extérieurs. La négociation d'une SLS est le seul échange explicite d'informations sur la disponibilité des ressources entre les deux régions de réseau. ER1 est configuré avec les informations représentées par la SLS et comme tel est capable d'agir comme agent de contrôle d'admission pour la région de réseau Diffserv. Une telle configuration ne prend pas directement en charge les changements dynamiques de SLS, car ER1 exige une reconfiguration chaque fois que la SLS change. Il est aussi difficile de faire une utilisation efficace des ressources dans la région de réseau Diffserv, parce que le contrôle d'admission ne considère pas la disponibilité des ressources dans la région de réseau Diffserv le long des chemins qui seraient spécifiquement impactés.

À l'opposé, lorsque la région de réseau Diffserv est à capacité RSVP, l'agent de contrôle d'admission fait partie du réseau Diffserv. Il en résulte que les changements de la capacité disponible dans la région de réseau Diffserv peuvent être indiqués aux nœuds à capacité Intserv en dehors de la région Diffserv via RSVP. En incluant les routeurs intérieurs à la région de réseau Diffserv dans la signalisation RSVP, il est possible d'améliorer simultanément l'efficacité de l'utilisation des ressources au sein de la région Diffserv et le niveau de confiance que les ressources demandées au contrôle d'admission sont bien disponibles à ce moment particulier. Cela parce que le contrôle d'admission peut être relié à la disponibilité des ressources le long du chemin spécifique qui serait impacté. On appelle cet avantage de la signalisation RSVP un " contrôle

d'admission à capacité topologique". Un autre avantage de la prise en charge de la signalisation RSVP au sein de la région de réseau Diffserv est qu'il est possible d'effectuer des changements dans le provisionnement de la région de réseau Diffserv (par exemple, en allouant plus ou moins de bande passante à la file d'attente EF dans un routeur) en réponse à des demandes de ressources provenant de l'extérieur de la région Diffserv.

Divers mécanismes peuvent être utilisés au sein de la région de réseau Diffserv pour prendre en charge le provisionnement dynamique et le contrôle d'admission à capacité topologique. Cela inclut le RSVP agrégé, le RSVP par flux et les courtiers en bande passante, comme décrit dans les paragraphes suivants.

4.2.1 RSVP agrégé ou tunnelé

Un certain nombre de documents [AIISS], [ASQR], [RFC2746], [RFC3175] proposent des mécanismes pour étendre RSVP à la réservation de ressources pour un flux agrégé entre les bordures d'un réseau. Les routeurs de bordure peuvent interagir avec les routeurs du centre et les autres routeurs de bordure en utilisant RSVP agrégé pour réserver des ressources entre les bords de la région de réseau Diffserv. Les niveaux de réservation initiaux pour chaque niveau de service peuvent être établis entre les routeurs bordures majeurs, sur la base de schéma de trafic prévus à l'avance. Les routeurs bordures pourraient déclancher des changements des niveaux de réservation par suite des demandes RSVP accumulées par flux à partir des régions non Diffserv qui atteignent des niveaux de marquage élevés ou faibles.

Dans cette approche, l'admission de demandes RSVP par flux à partir des nœuds qui sont en dehors de la région Diffserv serait confrontée aux réservations agrégées appropriées pour le niveau de service correspondant. La taille des réservations agrégées peut ou non ajustée de façon dynamique pour faire face aux changements dans les réservations par flux.

L'avantage de cette approche est qu'elle offre un contrôle d'admission dynamique à capacité topologique à la région de réseau Diffserv sans exiger le niveau de traitement de la signalisation RSVP qui serait requis pour prendre en charge RSVP par flux.

On note que la gestion de ressource d'une région Diffserv utilisant RSVP agrégé ne sera vraisemblablement faisable que dans un seul domaine administratif, car chaque domaine va probablement choisir son propre mécanisme pour gérer ses ressources.

4.2.3 RSVP par flux

Dans cette approche, décrite dans [AIISS], les routeurs dans la région de réseau Diffserv répondent à la signalisation RSVP standard par flux générée par les nœuds à capacité Intserv en dehors de la région Diffserv. Cette approche présente l'avantage de l'approche précédente (contrôle d'admission dynamique à capacité topologique) sans exiger la prise en charge de RSVP agrégé. Les ressources sont aussi utilisées plus efficacement par suite du contrôle d'admission par flux. Cependant, les demandes sur les ressources de signalisation RSVP au sein de la région de réseau Diffserv peuvent être significativement plus élevées que dans une approche de RSVP agrégé.

Noter que RSVP par flux et RSVP agrégé ne s'excluent pas mutuellement dans une seule région Diffserv. Il est possible d'utiliser RSVP par flux aux bordures de la région Diffserv et l'agrégation seulement dans certaines régions "cœur" au sein de la région Diffserv.

4.2.4 Granularité du déploiement de routeurs à capacité RSVP

Dans les paragraphes 4.2.2 et 4.2.3, un certain sous ensemble des routeurs au sein du réseau Diffserv a la capacité de signalisation RSVP (bien que le contrôle du trafic soit agrégé et non par flux). Le nombre relatif de routeurs dans le cœur qui participent à la signalisation RSVP est une décision d'approvisionnement qui doit être prise par l'administrateur du réseau.

Dans un cas extrême, seuls les routeurs frontières participent à la signalisation RSVP. Dans ce cas, soit la région de réseau Diffserv doit être extrêmement sur-provisionnée et donc, utilisée sans efficacité, soit autrement elle doit être prudente et être provisionnée de façon statique pour des schémas de trafic limités. Les routeurs frontières doivent mettre en application ces schémas.

Dans l'autre cas extrême, chaque routeur dans la région de réseau Diffserv peut participer à la signalisation RSVP. Dans ce cas, les ressources peuvent être utilisées avec une efficacité optimale, mais les exigences de traitement de la signalisation et la redondance associée augmentent. Comme on l'a noté ci-dessus, l'agrégation RSVP est unidirectionnelle pour limiter la redondance de signalisation au prix de la perte de l'optimisation de l'utilisation des ressources.

Il est vraisemblable que certains administrateurs de réseau vont faire un compromis en activant la signalisation RSVP sur

certains sous ensembles de routeurs dans la région de réseau Diffserv. Ces routeurs vont vraisemblablement représenter des point de commutation de trafic majeurs avec des régions sur-provisionnées ou provisionnées de façon statique de routeurs sans capacité RSVP entre eux.

4.3 Régions Diffserv sans capacité RSVP à approvisionnement dynamique

Des routeurs frontières pourraient n'utiliser aucune forme de signalisation RSVP au sein de la région de réseau Diffserv mais pourraient utiliser plutôt des protocoles personnalisés pour interagir avec un "oracle". L'oracle est un agent qui a une connaissance suffisante de la disponibilité des ressources et de la topologie du réseau pour prendre des décisions de contrôle d'admission. L'ensemble des routeurs à capacité RSVP dans les deux exemples précédents peut être considéré collectivement comme une forme d'oracle réparti. Dans diverses définitions du "courtier de bande passante" [RFC2638], il est capable d'agir comme un oracle centralisé.

5. Implications du cadre pour les régions de réseau Diffserv

Nous avons décrit un cadre dans lequel la qualité de service de style RSVP/Intserv peut être fournie à travers des chemins de bout en bout qui incluent les régions de réseau Diffserv. La présente section expose certaines des implications de ce cadre pour la région de réseau Diffserv.

5.1 Exigences des régions de réseau Diffserv

Une région de réseau Diffserv doit satisfaire aux exigences suivantes afin de prendre en charge le cadre décrit dans le présent document.

1. Une région de réseau Diffserv doit être capable de fournir la prise en charge du service de qualité de service Intserv standard entre ses routeurs frontières. Il doit être possible d'invoquer ces services en utilisant les PHB standard au sein de la région Diffserv et le comportement approprié à la bordure de la région Diffserv.

2. Les régions de réseau Diffserv doivent fournir les informations de contrôle d'admission à leurs régions de réseau "consommateur" (non Diffserv). Ces informations peuvent être fournies par un protocole dynamique ou à travers des accords de niveau de service statiques mis en application aux bordures de la région Diffserv.

3. Les régions de réseau Diffserv doivent être capables de passer les messages RSVP, d'une manière telle qu'ils puissent être récupérés à la sortie de la région de réseau Diffserv. La région de réseau Diffserv peut, mais n'y est pas obligée, traiter ces messages. Les mécanismes pour porter les messages RSVP en toute transparence à travers un réseau de transit sont décrites dans [AIISS], [ASQR], [RFC3175], [RFC2746].

Pour satisfaire à ces exigences, du travail supplémentaire devra être effectué dans les domaines de :

1. Transposer les spécifications de service de style Intserv en services qui puissent être fournis par les régions de réseau Diffserv.

2. Définir les fonctionnalités exigées dans les éléments de réseau pour prendre en charge la signalisation RSVP avec le contrôle de trafic agrégé (pour les éléments de réseau qui résident dans la région de réseau Diffserv).

3. Définir les mécanismes pour provisionner efficacement et de façon dynamique les ressources dans une région de réseau Diffserv (par exemple, RSVP agrégé, tunnelage, MPLS, etc.). Cela peut inclure des protocoles par lesquels un "oracle" transporte des informations sur la disponibilité des ressources du sein d'une région Diffserv aux routeurs de bordure. Un exemple d'un tel mécanisme est ce qu'on appelle le "courtier en bande passante" proposé dans [Diff-SA], [RFC2638], [FIBB].

5.2 Protection du trafic Intserv contre les autres trafics

Les administrateurs de réseau doivent être capables de partager les ressources dans la région de réseau Diffserv entre trois types de trafic :

a. Trafic Intserv de bout en bout. C'est normalement le trafic associé aux applications quantitatives de qualité de service. Il exige une quantité de ressources spécifique avec un degré d'assurance élevé.

b. Trafic non Intserv. La région Diffserv peut allouer des ressources au trafic qui n'utilise pas les techniques de Intserv

pour quantifier ses exigences, par exemple, par l'utilisation d'un approvisionnement statique et des SLS mis en application aux bordures de la région. Un tel trafic peut être associé aux applications dont les exigences de QS ne sont pas directement quantifiables mais exigent un niveau de service "meilleur que au mieux".

c. Tout trafic autre (au mieux). Ces trois classes de trafic doivent être isolées les unes des autres par la configuration appropriée de régulateurs et de classeurs aux points d'entrée de la région de réseau Diffserv, et par un provisionnement approprié au sein de la région de réseau Diffserv. Pour protéger le trafic Intserv dans les régions Diffserv du réseau, on suggère que les DSCP alloués à un tel trafic ne se recouvrent pas avec les DSCP alloués à d'autres trafics.

6. Diffusion groupée

L'utilisation de services intégrés sur les réseaux Diffserv est significativement plus complexe pour les sessions en diffusion groupée que pour les sessions en envoi individuel. Pour ce qui concerne une connexion de diffusion groupée, chaque région participante a un seul routeur d'entrée et zéro, un ou plusieurs routeurs de sortie. Les difficultés de la diffusion groupée sont associées aux régions Diffserv qui contiennent plusieurs routeurs de sortie. (La prise en charge de la fonction de diffusion groupée en dehors de la région Diffserv est assez directe car chaque routeur à capacité Intserv le long de l'arborescence de diffusion groupée mémorise l'état pour chaque flux.)

Considérons le réseau de référence suivant :

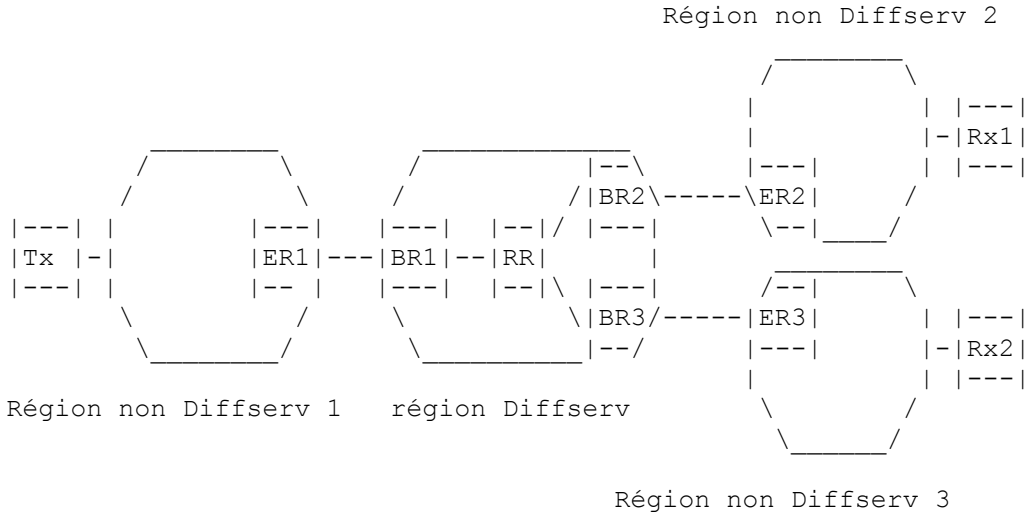

Figure 2 : Exemple de configuration de réseau de diffusion groupée

Le réseau de référence est similaire à celui de la Figure 1. Cependant, dans la Figure 2, des copies des paquets envoyés par Tx sont livrées à plusieurs receveurs en dehors de la région Diffserv, à savoir Rx1 et Rx2. De plus, les paquets sont copiés au sein de la région Diffserv dans un routeur RR " point d'embranchement". Dans le réseau de référence, BR1 est le routeur d'entrée de la région Diffserv tandis que BR2 et BR3 sont les routeurs de sortie.

Dans le plus simple cas de receveurs, Rx1 et Rx2 dans le réseau de référence, exigent des réservations identiques. Le cadre Diffserv [Bernet] prend en charge les spécifications de niveau de service (SLS) provenant d'un routeur d'entrée vers un, quelques uns ou tous les routeurs de sortie. Cela appelle à une SLS de "un à beaucoup" au sein de la région Diffserv, de BR1 à BR2 et BR3. Sachant que la SLS est accordée par la région Diffserv, le routeur d'entrée BR1, ou peut-être un nœud en amont tel que ER1, marque les paquets qui entrent dans la région Diffserv avec le DSCP approprié. Les paquets sont acheminés aux sorties du domaine Diffserv en utilisant l'adresse de diffusion groupée originale.

Les deux problèmes majeurs, expliqués dans ce qui suit, sont associés à des arborescences de diffusion groupée hétérogènes qui contiennent des points d'embranchement au sein de la région Diffserv, c'est-à-dire, des arborescences de diffusion groupée ou le niveau des exigences de ressources n'est pas uniforme entre les receveurs. Un exemple d'un tel scénario dans le réseau de la Figure 2 est le cas où Rx1 et Rx2 ont tous deux besoin de recevoir des données en diffusion groupée de Tx1 mais un seul des receveurs a demandé un niveau de service supérieur à au mieux. On considère de tels scénarios dans les paragraphes suivants.

6.1 Remarquage des paquets dans les routeurs de point d'embranchement

Dans le scénario ci-dessus, les paquets qui arrivent à BR1 sont marqués avec un DSCP approprié pour le service Intserv requis et sont envoyés à RR. Les paquets qui arrivent au point d'embranchement doivent être envoyés vers BR2 avec le même DSCP autrement le service pour Rx1 sera dégradé. Cependant, les paquets qui vont de RR à BR3 n'ont pas besoin de maintenir plus longtemps l'assurance d'un haut niveau de service. Ils peuvent être rétrogradés en service au mieux afin que la QS fournie aux autres paquets le long de cette branche de l'arborescence ne soit pas interrompue. Ce scénario permet d'observer plusieurs problèmes :

- Dans la région Diffserv, le marquage des DSCP est fait aux routeurs bordures (à l'entrée) tandis qu'un routeur point d'embranchement peut être un routeur du cœur qui ne marque pas les paquets.

- Comme RR est un routeur Diffserv du cœur, il fait son classement sur la base des flux de trafic agrégés (BA) et non sur celle du classement par flux (MF). Donc, il n'a pas nécessairement la capacité de distinguer ces paquets qui appartiennent à une arborescence de diffusion groupée spécifique et exigent la rétrogradation des autres paquets dans le comportement agrégé, qui portent le même DSCP.

- Comme RR peut être sans capacité RSVP, il peut ne pas participer au processus de contrôle d'admission, et ne mémoriser donc aucun état par flux sur les réservations pour l'arborescence de diffusion groupée. Donc, même si RR était capable d'effectuer le classement MF et le re-marquage des DSCP, il n'en saurait pas assez sur les réservations vers l'aval pour faire un nouveau marquage intelligent des DSCP.

Ces problèmes pourraient être réglés par divers a mécanismes. Certains sont énumérés dans ce qui suit, tout en notant qu'aucun n'est idéal dans tous les cas et que d'autres mécanismes pourraient être développés à l'avenir :

1. Si des routeurs à capacité Intserv sont placés au sein de la région Diffserv, il serait possible d'administrer la topologie du réseau et les paramètres d'acheminement de telle sorte qu'on s'assure que les points d'embranchement ne surviennent qu'au sein de tels routeurs. Ces routeurs prendraient en charge le classement MF et le re-marquage et tiendraient l'état par flux pour les réservations hétérogènes pour lesquelles ils sont le point d'embranchement. Noter que dans ce cas, les routeurs points d'embranchement auraient essentiellement la même fonction que les routeurs d'entrée d'un domaine Diffserv à capacité RSVP.

2. Les paquets envoyés sur la branche "non réservée" (de RR vers BR3) sont marqués avec le "mauvais" DSCP ; c'est-à-dire qu'ils ne sont pas rétrogradés au service au mieux mais conservent leur DSCP. Cela exige donc une sur réservation de ressources le long de cette liaison ou de courir le risque de dégrader le service pour des paquets qui portent légitimement le même DSCP le long de ce chemin. Cependant, cela permet aux routeurs Diffserv de s'affranchir de l'état par flux.

3. Une combinaison des mécanismes 1 et 2 peut être un compromis efficace. Dans ce cas, il y a des routeurs à capacité Intserv dans le cœur du réseau, mais le réseau ne peut pas être administré d'une façon telle que TOUS les points d'embranchement tombent sur de tels routeurs.

4. Les administrateurs des régions Diffserv peuvent décider de ne pas activer de sous arborescences hétérogènes dans leurs domaines. Dans le cas de réservations différentes vers l'aval, un message ResvErr serait envoyé conformément aux règles de RSVP. Ceci est similaire à l'approche retenue pour Intserv sur des réseaux IEEE 802 [RFC2814], [RFC2815].

5. Dans [AIISS], un schéma a été introduit selon lequel les routeurs points d'embranchement à l'intérieur de la région d'agrégation (c'est-à-dire la région Diffserv) conservent des informations d'état réduites en ce qui concerne les réservations en utilisant un contrôle d'admission fondé sur des mesures. Dans ce schéma, les paquets sont étiquetés par les routeurs bordures Interserv les plus savants avec des informations de programmation qui sont utilisées à la place de l'état Intserv détaillé. Si la région Diffserv et les routeurs point d'embranchement sont conçus en suivant le présent cadre, la dégradation des paquets devient possible.

6.2 SLS de diffusion groupée et arborescences hétérogènes

Les flux en diffusion groupée avec des réservations hétérogènes présentent un certain défi dans le domaine des SLS. Par exemple, un cas courant de SLS est celui où une certaine quantité de trafic est permise à l'entrée d'une région Diffserv marquée avec un certain DSCP, et ce trafic peut être destiné à n'importe quel routeur de sortie de cette région. On appelle une telle SLS une SLS homogène, ou uniforme. Cependant, dans un environnement de diffusion groupée, un seul paquet qui est admis dans la région Diffserv peut consommer des ressources le long de nombreux chemins dans la région car il est dupliqué et transmis vers de nombreux routeurs de sortie ; autrement, il peut s'écouler le long d'un seul chemin. Cette situation est en plus compliquée par la possibilité décrite ci-dessus et schématisée à la Figure 2, dans laquelle un paquet en diffusion groupée peut être traité comme au mieux le long de certaines branches tout en recevant un traitement de QS plus

élevé le long de certaines autres. On note simplement ici que la spécification de SLS significatives qui satisfassent les besoins des flux hétérogènes et qui puissent être satisfaites par les fournisseurs est vraisemblablement un défi.

Des SLS dynamiques peuvent aider à régler ces questions. Par exemple, en utilisant RSVP pour signaler les ressources qui sont requises le long des différentes branches d'une arborescence de diffusion groupée, il serait possible d'approcher de plus près l'objectif d'une allocation appropriée de ressources aux seuls endroits où elles sont nécessaires plutôt que de sur provisionner ou sous provisionner le long de certaines branches d'une arborescence. C'est essentiellement l'approche décrite dans la [RFC3175].

7. Considérations pour la sécurité

7.1 Sécurité RSVP générale

On propose que la signalisation RSVP soit utilisée pour obtenir des ressources dans les régions Diffserv aussi bien que non Diffserv d'un réseau. Donc, toutes les considérations de sécurité de RSVP s'appliquent [RFC2747]. De plus, les administrateurs de réseau sont supposés protéger les ressources du réseau en configurant des régulateurs sûrs aux interfaces avec des consommateurs qui ne sont pas de confiance.

7.2 Marquage des hôtes

Bien qu'elle ne rende pas obligatoire le marquage des DSCP par les hôtes, notre proposition le permet bien. Permettre aux hôtes d'établir le DSCP directement peut alarmer les administrateurs de réseau. Le souci évident est que les hôtes peuvent tenter de "voler" des ressources. En fait, les hôtes peuvent tenter d'excéder la capacité négociée dans les régions de réseau Diffserv à un niveau de service particulier sans considération du fait qu'ils invoquent ce niveau de service directement (en établissant le DSCP) ou indirectement (en soumettant du trafic qui se classe dans un routeur de marquage intermédiaire à un DSCP particulier).

Dans l'un et l'autre cas, il va généralement être nécessaire pour chaque région de réseau Diffserv de protéger ses ressources par la régulation pour s'assurer que les consommateurs n'utilisent pas plus de ressources que ce à quoi ils ont droit, à chaque niveau de service (DSCP). L'exception à cette règle est lorsque l'hôte est connu pour être de confiance, par exemple, un serveur qui est sous le contrôle des administrateurs de réseau. Si un hôte envoyeur qui n'est pas de confiance n'effectue pas le marquage DSCP, le routeur frontière (ou des routeurs intermédiaires de confiance) doit fournir le classement MF, le marquage et la régulation. Si un hôte envoyeur qui n'est pas de confiance effectue le marquage, le routeur frontière a seulement besoin de fournir le classement BA et de réguler pour s'assurer que le consommateur n'excède pas la capacité agrégé négociée pour le niveau de service.

En résumé, il n'y a pas de souci de sécurité supplémentaire soulevé par le marquage du DSCP à la bordure du réseau car les fournisseurs de Diffserv auront de toutes façons à réguler à leurs frontières. De plus, cette approche réduit la granularité à laquelle les routeurs frontières doivent réguler, poussant par là à une responsabilité de formatage et de régulation d'une granularité plus fine sur les bordures du réseau, où elle s'adapte mieux et apporte d'autres avantages décrits au paragraphe 3.3.1. Les plus grandes régions de réseau Diffserv concentrent donc la tâche de protéger leurs réseaux tandis que les nœuds à capacité Intserv se concentrent sur la tâche de formater et réguler leur propre trafic pour qu'il soit en conformité avec leurs paramètres Intserv négociés.

8. Remerciements

Les auteurs remercient les personnes suivantes de leurs commentaires qui ont conduit à l'amélioration des versions précédentes de ce document : David Oran, Andy Veitch, Curtis Villamizer, Walter Weiss, Francois le Faucheur et Russell White.

Beaucoup des idées de ce document ont été précédemment discutées dans le document original de l'architecture Intserv [RFC1633].

9. Références

[AIISS] Berson, S. and R. Vincent, "Aggregation of Internet Integrated Services State", non publié.

[ASQR] Guerin, R., Blake, S. and Herzog, S., "Aggregating RSVP based QoS Requests", non publié.

[Bernet] Y. Bernet, "A Framework for Differentiated Services", non publié.

[Diff-SA] Van Jacobson, "Differentiated Services Architecture", discussion à la réunion de Munich du groupe de travail Int-Serv de l'IETF, août 1997.

[FIBB] First Internet2 bandwidth broker operability event, à http://www.merit.edu/internet/working.groups/i2-qbone-bb/ inter-op/index.htm

[RFC1633] R. Braden, D. Clark et S. Shenker, "Intégration de services dans l'architecture de l'Internet : généralités", , juin 1994. *(Info.)*

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", , septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[RFC2381] M. Garrett, M. Borden, "Interopération du service à charge contrôlée et du service garanti avec ATM", , août 1998. *(P.S.)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", , novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS Field) dans les en-têtes IPv4 et IPv6", , décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", , décembre 1998. *(MàJ par* RFC3260*)*

[RFC2638] K. Nichols, V. Jacobson, L. Zhang, "Architecture de services différenciés à deux bits pour l'Internet", , juillet 1999. *(Info.)*

[RFC2746] A. Terzis, J. Krawczyk, J. Wroclawski, L. Zhang, "Fonctionnement de RSVP sur tunnels IP", , janvier 2000. *(P.S.)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", , janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

[RFC2749] S. Herzog, et autres, "Utilisation de COPS avec RSVP", , janvier 2000. *(P.S.)*

[RFC2814] R. Yavatkar et autres, "SBM (Gestionnaire de bande passante de sous-réseau) : protocole pour le contrôle d'admission fondé sur RSVP sur les réseaux de style IEEE 802", , mai 2000. *(P.S.)*

[RFC2815] M. Seaman et autres, "Transpositions de services intégrés sur réseaux IEEE 802", , mai 2000. *(P.S.)*

[RFC2996] Y. Bernet, "Format de l'objet DCLASS RSVP", , novembre 2000. *(P.S.)*

[RFC3175] T. Baker, C. Iturralde, F. le Faucheur et B.Davie, "Agrégation de RSVP pour réservations IPv4 et IPv6", , septembre 2001. (*MàJ par* RFC5350) *(P.S.)*

[WEISS] Weiss, Walter, communication privée, novembre 1998.

10. Adresse des auteurs

Yoram Bernet
Microsoft
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425-936-9568
mél : yoramb@microsoft.com

Raj Yavatkar
Intel Corporation
JF3-206 2111 NE 25th. Avenue
Hillsboro, OR 97124
téléphone : +1 503-264-9077
mél : raj.yavatkar@intel.com

Peter Ford
Microsoft
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425-703-2032
mél : peterf@microsoft.com

Lixia Zhang
UCLA
4531G Boelter Hall
Los Angeles, CA 90095
téléphone : +1 310-825-2695
mél : lixia@cs.ucla.edu

Michael Speer
Sun Microsystems
901 San Antonio Road, UMPK15-215
Palo Alto, CA 94303
téléphone : +1 650-786-6368
mél : speer@Eng.Sun.COM

Bob Braden
USC/Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292-6695
téléphone +1 310-822-1511
mél : braden@isi.edu

Bruce Davie
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
téléphone : +1 978-244-8000
mél : bsd@cisco.com

Eyal Felstaine
SANRAD Inc.
24 Raul Wallenberg st
Tel Aviv, Israel
téléphone : +972-50-747672
mél : eyal@sanrad.com

John Wroclawski
MIT Laboratory for Computer Science
545 Technology Sq.
Cambridge, MA 02139
téléphone : +1 617-253-7885
mél : jtw@lcs.mit.edu

11. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.