UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.174

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(02/2002)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

IPCablecom

Qualité de service interdomaniale IPCablecom

Recommandation UIT-T J.174

RECOMMANDATIONS UIT-T DE LA SÉRIE J

RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Recommandations générales	J.1–J.9
Spécifications générales des transmissions radiophoniques analogiques	J.10–J.19
Caractéristiques de fonctionnement des circuits radiophoniques analogiques	J.20–J.29
Equipements et lignes utilisés pour les circuits radiophoniques analogiques	J.30–J.39
Codeurs numériques pour les signaux radiophoniques analogiques	J.40–J.49
Transmission numérique de signaux radiophoniques	J.50–J.59
Circuits de transmission télévisuelle analogique	J.60–J.69
Transmission télévisuelle analogique sur lignes métalliques et interconnexion avec les faisceaux hertziens	J.70–J.79
Transmission numérique des signaux de télévision	J.80–J.89
Services numériques auxiliaires propres aux transmissions télévisuelles	J.90–J.99
Prescriptions et méthodes opérationnelles de transmission télévisuelle	J.100–J.109
Services interactifs pour la distribution de télévision numérique	J.110–J.129
Transport des signaux MPEG-2 sur les réseaux par paquets	J.130–J.139
Mesure de la qualité de service	J.140–J.149
Distribution de la télévision numérique sur les réseaux locaux d'abonnés	J.150–J.159
IPCablecom	**J.160–J.179**
Divers	J.180–J.199
Application à la télévision numérique interactive	J.200–J.209

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T J.174

Qualité de service interdomaniale IPCablecom

Résumé

La présente Recommandation décrit un ensemble de mécanismes propres à garantir une certaine qualité de service (QS) de bout en bout, applicables aux configurations interdomaniales et intradomaniales IPCablecom.

Source

La Recommandation J.174 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 13 février 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T J.174

Qualité de service interdomaniale IPCablecom

1 Domaine d'application

La présente Recommandation décrit un ensemble de mécanismes propres à garantir une certaine qualité de service, mécanismes appelés par la suite du texte mécanismes QS, pour le projet IPCablecom. L'objectif de la présente Recommandation est de définir un modèle architectural de qualité de service de bout en bout applicable aux configurations interdomaniales et intradomaniales IPCablecom. La présente Recommandation décrit des mécanismes permettant d'intégrer dans les modèles de QS des réseaux centraux IP, les protocoles de signalisation de qualité de service dynamique (DQoS) IPCablecom. Les réseaux qui ne sont pas dotés d'une gestion de la qualité de service n'entrent pas dans le domaine d'application de la présente Recommandation. On suppose également que le lecteur est familier avec l'architecture IPCablecom, en particulier avec la DQoS et la signalisation d'appel.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

2.1 Références normatives

[1] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service*.

[2] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

[3] IETF RFC 2475 (1998), *An Architecture for Differentiated Service*.

[4] IETF RFC 2998 (2000), *A Framework for Integrated Services Operation over Diffserv Networks*.

[5] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations*.

[6] IETF RFC 3181 (2001), *Signalled Preemption Priority Policy Element*.

[7] Recommandation UIT-T J.163 (2001), *Qualité de service dynamique pour la fourniture de services en temps réel sur l*es *réseaux de télévision par câble utilisant des câblo-modems*.

2.2 Références informatives

[8] IETF RFC 2638 (1999), *A Two-bit Differentiated Services Architecture for the Internet*.

[9] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

[10] IETF RFC 2598 (1999), *An Expedited Forwarding PHB*.

[11] IETF RFC 2702 (1999), *Requirements for Traffic Engineering Over MPLS*.

[12] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[13] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)*.

[14] Recommandation UIT-T J.171 (2002), *Protocole de commande de passerelle pour jonctions (TGCP) IPCablecom*.

[15] MAKAM [S.] et al.: Framework for MPLS-based Recovery, *draft-ietf-mpls-recovery-frmwrk-03.txt*, juillet 2001.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 nœud d'accès: dans le présent document, un nœud d'accès est un dispositif de terminaison de couche 2 qui aboutit à l'extrémité de réseaux d'une connexion J.112. Il dépend de la technologie utilisée. Dans l'Annexe A/J.112, ce dispositif est appelé INA et dans les Annexes B et C, CMTS.

3.2 point d'extrémité: désigne un terminal, une passerelle ou une unité MCU.

3.3 flux [flux IP]: séquence unidirectionnelle de paquets identifiés par l'information d'en-tête ISO de couche 3 et de couche 4. Cette information inclut les adresses IP d'origine/de destination, les numéros de port d'origine/de destination, l'identificateur de protocole. Plusieurs flux multimédias peuvent être acheminés dans un même flux IP.

3.4 flux [flux J.112]: flux unidirectionnel ou bidirectionnel de paquets de données qui utilise la signalisation de couche MAC et l'assignation de QS conforme à la Rec. UIT-T J.112. Plusieurs flux multimédias peuvent être acheminés dans un même flux J.112.

3.5 passerelle: dispositif assurant la liaison entre le monde des communications vocales IPCablecom et le RTPC. On peut citer par exemple la passerelle média qui assure l'interface de circuit support avec le RTPC et effectue le transcodage du flux média et la passerelle de signalisation qui envoie et reçoit la signalisation de réseau à commutation de circuits vers le bord du réseau IPCablecom.

3.6 temps d'attente: désigne le temps, exprimé en quantité de symboles, pris par un élément de signal pour traverser un dispositif.

3.7 mandat: fonction qui assure de manière indirecte un certain service ou agit en qualité de représentant pour la fourniture de l'information ce qui dispense les serveurs de la prise en charge du service.

3.8 jonction: désigne une connexion analogique ou numérique depuis un commutateur de circuits qui achemine le contenu média de l'utilisateur et peut acheminer la signalisation vocale (MF, R2, etc.).

4 Abréviations, acronymes et conventions

4.1 Abréviations et Acronymes

La présente Recommandation utilise les abréviations suivantes:

AF réacheminement assuré (*assured forwarding*)

AN nœud d'accès (*access node*)

ATM mode de transfert asynchrone (*asynchronous transfer mode*)

CMS serveur de gestion d'appels (*call management server*)

COPS protocole de service commun de politique ouverte (*common open policy service protocol*)

DCS signalisation d'appel décentralisé (*distributed call signalling*)

DQoS qualité de service dynamique (*dynamic quality of service*)

DSCP point de code Diffserv (*differentiated services codepoint*)

EF retransmission accélérée (*expedited forwarding*)

ER routeur de bord (*edge router*)

IETF Groupe de travail d'ingénierie Internet (*Internet Engineering Task Force*)

IntServ services intégrés (*integrated services*)

IP protocole Internet (*Internet protocol*)

MPLS commutation multiprocolaire par étiquetage (*multiprotocol label switching*)

MTA adaptateur de terminal de média (*media terminal adapter*)

PHB comportement par saut (*per-hop behaviour*)

PHS suppression d'en-têtes de charge utile (*payload header suppression*)

QS qualité de service

RSVP protocole de réservation de ressources (*resource reservation protocol*)

RTPC réseau téléphonique public commuté

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

VoIP téléphonie IP ou phonie IP (*voice over Internet protocol*)

4.2 Conventions

Si la présente Recommandation est implémentée, les mots clés "DOIT" (MUST ou SHALL, en anglais) et "REQUIS" doivent être interprétés comme indiquant un aspect obligatoire de la présente spécification.

Les mots clés indiquant un certain niveau d'importance de telle ou telle prescription utilisée dans la présente Recommandation sont résumés ci-dessous.

"DOIT" Ce mot ainsi que l'adjectif "REQUIS" indiquent que l'article est une prescription absolue de la présente Recommandation.

"NE DOIT PAS" Cette expression indique que l'article est une interdiction absolue de la présente Recommandation.

"DEVRAIT" Cette expression ainsi que l'adjectif "RECOMMANDE" indiquent qu'il peut, dans des circonstances particulières, exister des raisons valables pour ignorer cet article, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.

"NE DEVRAIT PAS " Cette expression indique qu'il peut, dans des circonstances particulières, exister des raisons valables pour que le comportement indiqué soit acceptable ou même utile, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.

"PEUT" Ce mot ainsi que l'adjectif "FACULTATIF" indiquent que cet article est effectivement facultatif. Un fournisseur peut choisir d'inclure l'article par exemple parce qu'il est requis sur un marché particulier ou parce qu'il améliore le produit, alors qu'un autre fournisseur peut choisir d'omettre ce même article.

5 Introduction

5.1 Exigences en matière de solutions

Il y a trois exigences de base en ce qui concerne la fourniture d'une QS de bout en bout pour les sessions IPCablecom, à savoir:

1) offrir des temps d'établissement d'appel acceptables, comparables à ceux offerts par le RTPC;
2) offrir une qualité vocale acceptable en offrant des mécanismes garantissant des délais, gigue et perte de paquets suffisamment faibles;
3) offrir une qualité de service élevée pendant toute la durée de la session (bloquer par exemple toutes les nouvelles tentatives d'appel lorsque leur aboutissement compromet la qualité des appels existants).

Dans un réseau de type paquet, la deuxième exigence se traduit comme suit: offrir des mécanismes permettant de reconnaître le trafic IP Cablecom et de gérer la programmation ainsi que l'attribution des tampons dans chaque commutateur et routeur afin de limiter les délais et la perte de paquet.

La troisième exigence reflète la nécessité d'un contrôle d'admission. Selon les mécanismes de qualité de service retenus, il s'agit de définir une méthode satisfaisante permettant de bloquer ou d'admettre des appels ou des sessions sur la base de la disponibilité des ressources dans le système dorsal.

Les critères généraux qui permettent d'évaluer des solutions de QS de bout en bout pour l'IPCablecom sont les suivants:

- la solution doit répondre aux trois exigences précitées;
- la solution est gérable et implémentable;
- la solution est évolutive. Les mécanismes QS pour les services de communication vocale doivent pouvoir s'adapter à la prise en charge un grand nombre de sessions IPCablecom parallèles sans engendrer des coûts d'implémentation exagérés ou une complexité superflue;
- la solution doit permettre un rétablissement progressif lorsque des pannes de réseau se produisent. Par exemple, il n'est probablement pas possible d'éviter la perte de certains appels en cas de panne dans le réseau, mais cet événement ne devra pas compromettre les autres appels dans le réseau.

Ces exigences, en particulier l'évolutivité, conduisent à une architecture dorsale basée sur l'approche [2], [3] des services différenciés de l'IETF (Diffserv, *differentiated services*). Cette approche a spécialement été conçue comme approche évolutive pour délivrer une QS dans les grands systèmes dorsaux. Son application dans le contexte IPCablecom est décrite dans les paragraphes qui suivent.

5.2 Phasage des exigences

La présente Recommandation définit plusieurs approches permettant d'assurer la QS à travers un réseau dorsal géré IPCablecom. Plusieurs de ces approches sont complémentaires et sont fondées sur les besoins en gestion des ressources de l'opérateur de réseau, ces approches peuvent être combinées pour obtenir le contrôle et la gestion souhaités des ressources et des sessions IPCablecom.

Le tableau ci-dessous illustre les combinaisons pratiquement possibles d'approches décrites dans les paragraphes 7 à 10.

Approche	Paragraphes
Diffserv	Paragraphe 7 (Diffserv)
RSVP par flux	Paragraphes 7, 8.1
RSVP agrégé	Paragraphes 7, 8.1, 8.2
Courtier de BW	Paragraphes 7, 8.3

Tous les réseaux dorsaux IPCablecom DOIVENT prendre en charge les services Diffserv. Les dispositifs IPCablecom DOIVENT être compatibles au minimum avec conditions applicables aux services DiffServ et définies au § 7.

Les conditions relatives au protocole RSVP par flux définies dans les paragraphes 8 et 8.1 sont FACULTATIVES. Toutefois, si le protocole RSVP par flux est pris en charge, le respect des conditions définies dans les paragraphes 8 et 8.1 est REQUIS.

Le paragraphe 8.2 décrit l'approche utilisée pour l'agrégation des protocoles RSVP. Si cette agrégation est prise en charge, toutes conditions définies dans le paragraphe 8.2 DOIVENT être respectées. De même, toutes les conditions relatives au protocole RSVP par flux définies dans les paragraphes 8 et 8.1, DOIVENT être respectées.

Les optimisations de la commutation MPLS, telles que décrites dans le paragraphe 9, sont FACULTATIVES et peuvent être utilisées avec toutes approches décrites.

5.3 Objectifs généraux

La présente Recommandation a les objectifs généraux suivants:

- définir des mécanismes de signalisation permettant la mise en place de ressources QS entre des nœuds AN séparés par un réseau dorsal IP géré;
- définir des mécanismes de signalisation permettant la mise en place de ressources QS entre des nœuds AN et d'autres éléments IPCablecom dans le trajet média, comme par exemple des routeurs de bord, des routeurs de limite, des passerelles média et des serveurs média;
- prendre en charge des sessions à QS dynamique de bout en bout à travers les réseaux dorsaux IP gérés;
- définir les interfaces pour la gestion et la fourniture de QS entre les domaines IPCablecom;
- permettre la prise en charge des modèles de signalisation d'appel sur réseau (NCS, *network-based call signalling*) et de signalisation d'appel décentralisée (DCS, *distributed call signalling*);
- permettre la prise en charge à la fois de la signalisation QS de couche 2 (J.112) et de la signalisation QS de couche 3 (RSVP) sur le réseau d'accès;
- permettre la prise en charge de plusieurs réseaux dorsaux avec des implémentations de QS normalisées pour pouvoir assurer la gestion de la programmation et de l'attribution des tampons dans les commutateurs et les routeurs (par exemple, MPLS, DiffServ, ATM, RSVP, etc.).

6 Modèle de réseau

L'architecture générale de réseau IPCablecom est décrite à la Figure 1. Un réseau dorsal IPCablecom se compose d'un réseau IP géré de topologie générale pouvant comporter plusieurs domaines administratifs.

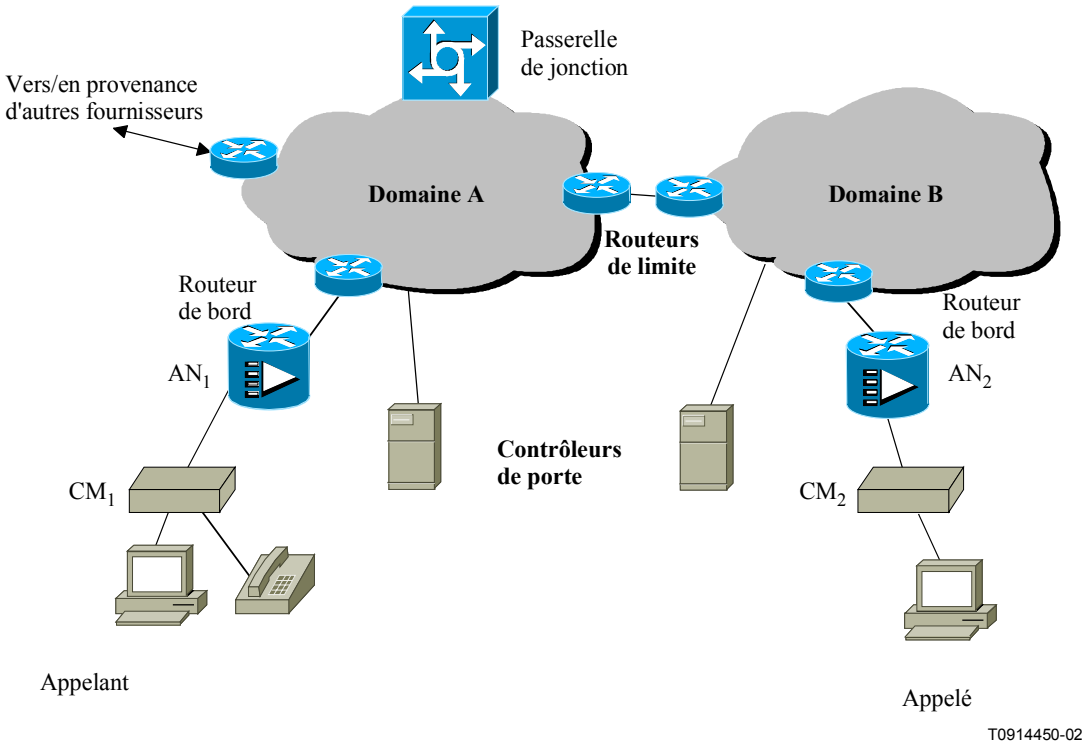


Figure 1/J.174 – Architecture de QS interdomaniale

Dans cette architecture, on suppose qu'il existe un accord de service entre les différents fournisseurs de services, accord qui définit le niveau de confiance entre domaines IPCablecom ainsi que les exigences en matière de QS, de signalisation d'appel, de transport, d'interconnexion et autres détails analogues.

Cette architecture intègre également le transport des médias et de la signalisation interdomaniale et peut inclure un ou plusieurs réseaux IP intermédiaires ou de transit. Pour l'IPCablecom, on suppose que les opérateurs disposent d'accords de transport relatifs à tous les réseaux de transit avec lesquels ils sont directement connectés.

Dans cette architecture, on suppose que la signalisation DQoS est utilisée dans le réseau d'accès. La partie accès du réseau est définie comme étant située entre l'adaptateur de terminal de média (MTA, *media terminal adapter*) et le nœud d'accès (AN, *access node*) et inclut le réseau hybride fibre/câble coaxial (HFC) J.112.

Les réseaux IP dorsaux et de transit sont supposés être au moins conformes à l'architecture Diffserv. La partie dorsale du réseau est définie comme étant l'ensemble de tous les éléments de réseau IP situés entre deux nœuds AN. Elle inclut tous les routeurs de bord, de limite et tous les routeurs centraux. Pour toutes les sessions qui aboutissent sur le RTPC, le réseau dorsal peut être ensuite défini comme incluant toutes les ressources entre le nœud AN et la passerelle média.

Les paragraphes qui suivent décrivent un certain nombre d'approches possibles présentant différents degrés d'assurance et de complexité.

A noter que le nœud AN peut être situé ou non au bord du réseau dorsal Diffserv, cela dépend de différents facteurs présentés ci-dessous. A noter également qu'il peut exister des dispositifs intermédiaires (non représentés dans la Figure 1) entre le nœud AN et le bord du réseau dorsal Diffserv.

Les routeurs de limite sont ceux qui se trouvent aux frontières séparant les fournisseurs. Ils ont des rôles spécifiques dans un environnement Diffserv (politique et remarquage cumulatif par exemple). Ils sont étudiés dans le détail dans les paragraphes qui suivent.

7 Utilisation du service Diffserv dans la partie dorsale

Dans le présent paragraphe, on suppose la présence d'une simple partie dorsale Diffserv [2], [3] sans signalisation des besoins en ressources au-delà de ceux spécifiés dans la DQoS. Dans ce cas, le nœud AN fonctionne comme dispositif de bord de Diffserv. Dans les paragraphes ultérieurs, on part d'une infrastructure dorsale Diffserv à laquelle on ajoute des capacités de signalisation permettant de contrôler l'accès aux ressources dans la partie dorsale. On suppose ici la présence d'une partie dorsale commune pour les données et la voix; parmi les autres possibilités, on peut utiliser un réseau physiquement ou logiquement distinct pour la voix.

7.1 Trafic média

Le trafic média IPCablecom est défini comme étant constitué de paquets qui ont pour origine ou pour terminaison un point d'extrémité IPCablecom pour lequel une QS a été demandée en utilisant la DQoS. (A noter qu'explicitement sont exclus les paquets de signalisation d'appels et de QS tels les messages de coordination de porte DQoS, les messages d'invitation DCS/SIP, etc., qui sont étudiés au § 7.2.) Dans la partie dorsale, au moins un comportement par saut (PHB, *per-hop behaviour*) DEVRAIT être réservé au trafic média IPCablecom. Ce comportement par saut PEUT être la retransmission accélérée EF [10], un des comportements PHB à retransmission assurée AF [9], un des comportements PHB sélecteurs de classe (CS, *class selector*) ou un comportement PHB "privé". Les seules restrictions sont les suivantes:

- Il NE DOIT PAS s'agir d'un comportement PHB par défaut (de meilleur effort).
- Les seuls paquets qui sont assignés à ce comportement PHB DEVRAIENT être ceux pour lesquels la QS a été demandée au moyen de la DQoS.
- Si un comportement PHB de retransmission AF est utilisé, il DEVRAIT s'agir de l'Afx1, c'est-à-dire celui qui offre la plus faible probabilité de perte.

Il n'est pas nécessaire pour tous les domaines d'utiliser le même comportement PHB pour les paquets média IPCablecom. Il est également possible à l'intérieur d'un même domaine d'utiliser plusieurs comportements PHB pour les paquets média IPCablecom, auquel cas il est nécessaire de définir une certaine politique au niveau du nœud AN pour déterminer les comportements PHB qui peuvent être utilisés pour un paquet donné. Ce point sera étudié plus loin.

7.2 Trafic de signalisation

Le trafic de signalisation est défini de manière à inclure les messages de signalisation d'appel entre les éléments de commande d'appel IPCablecom (messages DCS ou NCS, messages de coordination de porte DQoS, messages RSVP, etc.). Afin de contrôler le temps d'attente et l'affaiblissement subi par un trafic de signalisation, un ou plusieurs comportements PHB PEUVENT être affectés au trafic de signalisation IPCablecom. Par exemple, l'ensemble CS6 PHB a habituellement été utilisé pour acheminer le trafic. Si un comportement PHB est affecté aux messages de signalisation, il convient de se conformer aux directives suivantes:

- le comportement PHB pour les messages de signalisation DEVRAIT être distinct du comportement PHB de meilleur effort par défaut;
- seuls les paquets qui sont assignés à ce PHB DEVRAIENT être des messages de signalisation;
- le comportement PHB pour les messages de signalisation DOIT être distinct du comportement PHB utilisé pour les messages d'acheminement;
- le comportement PHB pour les messages de signalisation DEVRAIT être distinct du comportement PHB utilisé pour les messages de média;
- le volume de trafic généré par le comportement PHB DEVRAIT être limité.

Cette dernière directive peut parfois être difficile à appliquer. Une approche possible consiste à limiter le volume de trafic qu'un utilisateur peut générer et qui est marqué avec le point de code DSCP pour ce comportement PHB à une valeur configurée. Il faut seulement que cette valeur soit suffisamment grande pour traiter la charge de signalisation attendue de la part de l'utilisateur. Cette limite peut être transgressée par des paquets de politique de régulation supportant: le point de code DSCP désigné au niveau d'un nœud AN, les paquets excédentaires étant réétiquetés "de meilleur effort". Les paquets excédentaires NE DEVRAIENT PAS être éliminés. En réétiquetant les paquets excédentaires, on empêche les utilisateurs d'envoyer des volumes importants de trafic de données avec le point de code DSCP réservé à la signalisation. Parallèlement, si la charge offerte du trafic de signalisation excède temporairement le niveau attendu, l'excédent est toujours transmis dans le réseau avec une probabilité raisonnable de remise dans les délais, évitant ainsi une dégradation sérieuse des performances de signalisation.

A noter que l'utilisation de comportements PHB différents pour le trafic média et le trafic de signalisation ne doit pas impliquer une priorité relative du trafic de média sur le trafic de signalisation et inversement. Il s'agit simplement de permettre l'allocation des ressources au trafic média et à la signalisation de manière indépendante pour remplir les objectifs de perte et de temps d'attente pour chaque type de trafic.

7.3 Choix du comportement PHB et fixation du point de code DSCP

Un nœud AN est nécessaire pour fixer ou policer le point de code DSCP pour les paquets média et des paquets de signalisation IPCablecom. La Recommandation sur la qualité dynamique de service DQoS IPCablecom [7] définit un moyen par lequel un contrôleur de porte peut indiquer à un nœud AN quel point de code DSCP utiliser appel par appel, via le message GATE-SET. Le nœud AN DOIT s'assurer que le point de code DSCP pour tous les paquets média associés à un appel donné est fixé à la valeur contenue dans le GATE-SPEC pour cet appel. Un nœud AN DOIT s'assurer que le volume du trafic média généré pour un appel donné marqué avec le point code DSCP désiré ne dépasse pas la recommandation "*token bucket*" donnée par la signalisation DQoS.

Chaque domaine PEUT utiliser ses propres points de code DSCP pour tous les comportements PHB qu'il utilise indépendamment des autres domaines, aussi longtemps que le choix est cohérent à l'intérieur d'un même domaine. Si un comportement PHB standard est utilisé, le point de code recommandé par l'IETF DEVRAIT être utilisé tel que défini dans [9] et [10]. Si différents codes de point DSCP sont utilisés pour les paquets média et de signalisation IPCablecom dans des domaines voisins, le réétiquetage du point de code DSCP DOIT être effectué par un routeur de limite sur les paquets qui quittent un domaine et pénètrent dans un autre. Les capacités requises pour les routeurs de limite sont décrites ci-dessous.

Les routeurs au niveau des limites de domaine DOIVENT également pouvoir fixer ou policer le point de code DSCP pour les paquets qui sont destinés à un point d'extrémité IPCablecom et pour lequel une QS a été demandée en utilisant la DQoS. En l'absence de signalisation explicite aux limites de domaine, il n'est pas possible d'identifier convenablement les paquets média IPCablecom arrivant à un routeur de limite flux par flux. Ainsi, les routeurs de limite doivent s'appuyer sur le point de code DSCP pour identifier ces paquets. C'est pour cette raison que le routeur de limite DEVRAIT offrir les capacités suivantes:

- il DEVRAIT être possible de configurer le routeur de limite pour imposer une limite sur le volume total de trafic pénétrant dans le domaine et qui est marqué avec un certain point de code DSCP;
- il DEVRAIT être possible de configurer le routeur de limite pour modifier le point de code DSCP du trafic pénétrant dans le domaine. Cette capacité est utilisée si l'on sait qu'un point de code DSCP différent est en cours d'utilisation pour des paquets média IPCablecom dans un domaine depuis lequel les paquets sont reçus. C'est-à-dire, qu'un routeur peut être configuré pour reconnaître les paquets qui arrivent sur une interface avec un DSCP = x

comme paquets média IPCablecom et puis les transmettre sur une autre interface avec un DSCP = y (où x != y). Ce mappage d'un DSCP à un autre DEVRAIT être négocié entre les opérateurs des réseaux homologues.

Des passerelles de jonction DEVRAIENT également fixer le code de point DSCP approprié sur les paquets qu'elles produisent et qui sont destinés à un point d'extrémité DQoS. Par exemple, cela peut être réalisé en indiquant le point de code DSCP souhaité dans le TGCP [14] (à noter que le terme obsolète Type de service est utilisé dans la recommandation relative au TGCP). Il peut être également acceptable pour une passerelle de fixer la même valeur de DSCP sur tous les paquets qu'elle produit. Si la passerelle de jonction ne peut pas correctement marquer les paquets qu'elle génère, un autre dispositif situé entre la passerelle et le système dorsal (par exemple un routeur) DEVRAIT être configuré pour fixer le code de point DSCP pour les paquets de média IPCablecom arrivant au système dorsal en provenance de la passerelle.

Les autres éléments IPCablecom dans le trajet de média (par exemple serveurs audio/d'annonce, anonymiseurs, ponts de conférence, etc.) DEVRAIENT pouvoir de marquer les paquets qu'ils produisent et qui sont destinés à des points d'extrémité QS.

Dans un même domaine, tous les dispositifs qui fixent ou policent les points de code DSCP pour les paquets média IPCablecom, ou assurent une QS aux paquets en examinant leurs points de code DSCP DEVRAIENT avoir une configuration homogène. Cette configuration homogène peut être réalisée en utilisant le service de politique commune ouverte (COPS, *common open policy service*) fournissant [13] ou par d'autres moyens.

Il est possible d'utiliser plusieurs comportements PHB pour différents types de service. Par exemple, il peut être intéressant d'utiliser un comportement PHB différent pour la vidéo et pour la voix, ou il peut être souhaitable d'utiliser différents comportements PHB pour les appels pour lesquels il y a des exigences plus strictes en matière de délai en raison de la distance entre les points d'extrémité ou pour d'autres raisons. Les mécanismes permettant d'indiquer le choix approprié d'un comportement PHB dans ce cas sont décrits ci-dessus.

7.4 Prise en charge d'un comportement PHB par un nœud AN

Sur la base des critères examinés précédemment, on choisit un ou plusieurs comportement PHB à utiliser dans le système dorsal. Le nœud AN DEVRAIT implémenter tous ces comportements PHB sur ses liaisons amont (c'est-à-dire les liaisons le reliant au système dorsal) afin de délivrer la QS appropriée aux paquets qui pénètrent dans le système dorsal. De même, il doit être possible de surprovisionner des liaisons amont sur le nœud AN au lieu de reposer sur la prise en charge du service Diffserv sur ces liaisons. Il est important de noter que les solutions de surprovisionnement, tout en étant des approches viables à la QS, ne sont pas toujours la solution la plus économique ou la plus efficace en termes de ressources.

7.5 Attribution des ressources

Il est nécessaire de faire en sorte qu'un nombre suffisant de ressources soient attribuées aux comportements PHB choisis au niveau de tous les éléments de réseau dans le système dorsal. En l'absence de signalisation dans le système dorsal, c'est essentiellement un problème de mise à disposition. La mise à disposition [13] du service COPS ou d'autres moyens peuvent être utilisés pour distribuer l'information de mise à disposition aux éléments de réseau.

7.6 Contrôle d'admission

Même dans un système dorsal avec service Diffserv mis à disposition de manière statistique, il est possible d'exécuter un contrôle d'admission en certains points du réseau. Une des possibilités consiste à effectuer le contrôle d'admission au niveau du nœud AN, une autre est d'exécuter ce contrôle d'admission au niveau du serveur CMS. Une de ces possibilités, les deux ou aucune peuvent convenir. Par exemple si la largeur de bande amont entre le nœud AN et le système dorsal

est importante relativement à la capacité des liaisons J.112 qu'elle dessert, il est possible qu'il ne soit pas nécessaire d'exécuter un contrôle d'admission sur les liaisons amont du nœud AN.

Si le contrôle d'admission doit être exécuté au niveau d'un nœud AN, chaque nœud AN DOIT être configuré avec une largeur de bande maximale pour chaque comportement PHB qui doit être utilisé pour le trafic média IPCablecom sur chacune de ces interfaces amont (non-J.112). Chaque nœud AN DOIT également conserver trace de la largeur de bande qui a été offerte à chaque comportement PHB sur chaque interface. Lorsqu'un nœud AN reçoit une demande de service DQoS pour admettre un appel, il détermine le comportement PHB que l'appel utilisera en consultant le mappage DSCP-PHB avec lequel il est configuré, et en utilisant le code de point DSCP fourni dans le message GATE-SET. Il DOIT procéder à une vérification pour voir si la largeur de bande disponible dans le comportement PHB considéré sur l'interface sortante que cet appel utilisera est suffisante pour prendre en charge les ressources nécessaires à cet appel. Ainsi, le volume total de trafic pour un comportement PHB donné, qui sera injecté dans le réseau par un nœud AN quelconque, est limité.

Dans certaines circonstances, il peut également être possible d'effectuer le contrôle d'admission basé sur le serveur CMS. Si un serveur CMS peut disposer d'une connaissance suffisante des ressources et de la topologie de réseau, il peut être en mesure d'effectuer le contrôle d'admission sur la base de la destination des appels. Par exemple, un serveur CMS X peut savoir que les appels qui sont acheminés vers des destinations gérées par le serveur CMS Y doivent passer par une liaison de capacité connue et peut ainsi refuser des appels à cette destination une fois que la capacité de la liaison a été épuisée.

Les approches de contrôle d'admission décrites dans le présent paragraphe peuvent avoir certaines limitations. En particulier, elles peuvent ne pas tenir compte du trajet total via le système dorsal que les paquets d'un appel donné emprunteront. Elles peuvent aussi ne pas nécessairement tenir compte de l'éventualité d'une panne de liaison affectant la capacité disponible. Ainsi, il existe un risque de voir certaines liaisons devenir "surabonnées". Les méthodes permettant de traiter ces points sont examinées dans les paragraphes ci-après.

8 Contrôle d'admission pour un seul domaine

8.1 Plan contrôle RSVP par flux

Il est possible d'utiliser le protocole RSVP par flux comme protocole de commande d'admission pour une nébuleuse Diffserv. Une description générale de cette approche est donnée dans [4]. Le présent paragraphe décrit l'application de la signalisation RSVP par flux à un système dorsal Diffserv dans l'environnement IPCablecom. L'approche décrite ici est plus adaptable que le protocole RSVP par flux traditionnel car toute la classification et le séquencement (c'est-à-dire toutes les opérations effectuées dans le plan retransmission) sont effectués sur des agrégations de comportement Diffserv.

Afin de prendre en charge les capacités décrites dans cette section, la fonctionnalité de base Diffserv décrite dans le § 7 DOIT être fournie dans le nœud AN et le réseau dorsal. D'autres exigences sont exposées dans les paragraphes qui suivent.

Pour prendre en charge un plan de contrôle RSVP par flux, un nœud AN participant à une signalisation DQoS DOIT prendre en charge les deux modes de fonctionnement suivants:

- Mode RSVP de bout en bout: dans ce mode, l'adaptateur MTA effectue la signalisation au moyen de messages RSVP tels que décrits au § 6/J.163 [7] que le nœud AN DOIT retransmettre vers l'adaptateur MTA situé à l'extrémité distante de l'appel.
- Mode de signalisation intégré: dans ce mode, l'adaptateur MTA intégré utilise la signalisation J.112, et le nœud AN DOIT produire des messages RSVP en direction de l'adaptateur MTA de l'extrémité distante.

Dans chacun de ces modes, le protocole RSVP par flux est utilisé entre les deux nœuds AN qui interviennent dans un appel. Il peut s'agir d'un protocole vrai de bout en bout (MTA-MTA) ou d'un protocole situé seulement entre deux nœuds AN agissant comme entités disposant de mandats pour les adaptateurs MTA; ceci n'a aucun effet sur les mécanismes de QS dans le système dorsal.

Grâce au protocole RSVP par flux fonctionnant entre deux nœuds AN, un opérateur de réseau dispose d'une souplesse considérable pour ce qui est de classer le bord de la région Diffserv. Comme le montre la Figure 1, le bord du réseau Diffserv ne doit pas nécessairement être le nœud AN, bien qu'il puisse l'être. C'est-à-dire qu'il est possible d'utiliser le protocole RSVP par flux avec la classification et le séquencement par flux entre le nœud AN et le bord de la région Diffserv; de même, le nœud AN peut constituer le bord de la région Diffserv, auquel cas le séquencement et la classification composite sont utilisés sur tout le trafic qui se trouve en amont du nœud AN.

Dans un souci de généralisation, on utilise le concept de routeur de bord (ER, *edge router*) défini dans [4]. Ce dispositif est capable d'exécuter le protocole RSVP par flux et d'effectuer le contrôle d'admission sur le trafic qui pénètre dans le réseau Diffserv. Le nœud AN PEUT exécuter la fonction de routeur de bord (ER) ou la fonction peut être assignée à un routeur se trouvant en amont du nœud AN, à savoir un routeur proche du système dorsal.

Les paragraphes qui suivent décrivent le comportement des nœuds AN, des routeurs de bord et des routeurs principaux (les routeurs Diffserv dans le système dorsal qui ne sont pas des routeurs de bord).

8.1.1 Comportement du nœud AN

Un nœud AN peut fonctionner en un des deux modes suivants, selon que l'adaptateur MTA qu'il dessert utilise la signalisation intégrée ou la signalisation RSVP. Les deux modes DOIVENT être pris en charge. Nous allons traiter de chacun des modes successivement ci-après. Dans chaque cas, le nœud AN exécute le protocole RSVP sur ses interfaces amont (non-J.112), et utilise les procédures normalisées RSVP/Intserv pour effectuer le contrôle d'admission, la classification et le séquencement des paquets envoyés à ces interfaces.

A noter qu'indépendamment du mode avec lequel il fonctionne, un nœud AN est responsable de la retransmission (ou de la production) des messages PATH et RESV vers l'extrémité distante. Une réservation bidirectionnelle est établie entre deux nœuds AN lorsque deux messages RESV ont été changés entre eux.

8.1.1.1 Signalisation intégrée

Lorsqu'il utilise la signalisation intégrée définie dans les Annexes A et B de la Rec. UIT-T J.163 [7], un nœud AN détecte le besoin de procéder à une réservation dans le système dorsal lorsqu'un message de signalisation de couche MAC indiquant la demande d'établissement d'un nouveau flux J.112 parvient et lorsqu'une porte a été établie pour l'appel correspondant. Dans ce cas, le nœud AN DOIT envoyer un message PATH à l'adaptateur situé à l'extrémité distante, en utilisant les paramètres extraits du message MAC pour créer le message PATH tel que décrit ci-dessous. Il attend ensuite un message RESV en provenance du nœud AN ou de l'adaptateur MTA distant. Lorsqu'il a reçu un message RESV provenant de l'extrémité distante, il sait que la réservation a pu avoir lieu et DOIT répondre à l'adaptateur MTA avec un message de signalisation de couche MAC indiquant la réussite de l'opération.

Lorsqu'un nœud AN reçoit un message PATH d'un nœud AN ou d'un adaptateur MTA distant, et que ce message est destiné à un adaptateur MTA qui ne prend pas en charge le protocole RSVP, le nœud AN DOIT d'abord vérifier qu'il dispose d'une porte qui a été établie pour l'appel correspondant. Si tel est le cas, il DOIT répondre par un message RESV qu'il renvoie vers le bond précédent (PHOP, *previous hop*) contenu dans ce message PATH. Les paramètres contenus dans le message RESV sont déterminés à partir du message PATH reçu.

Le type et le format des messages de signalisation de couche MAC à utiliser pour établir les flux J.112 dépendent du protocole de couche 2 implémenté dans le réseau de télévision par câble. On trouvera de plus amples détails sur la signalisation MAC dans les Annexes A, B ou C de la Rec. UIT-T J.112.

8.1.1.1.1 Détermination des paramètres du message RSVP PATH

Afin de produire un message RSVP PATH (à la réception du message de couche MAC indiquant la nécessité de faire une réservation au niveau du système dorsal), le nœud AN doit construire un objet session, un objet modèle d'expéditeur et un objet Tspec d'expéditeur. L'objet session se compose du protocole, de l'adresse de destination et du numéro du port de destination. Le modèle d'expéditeur se compose de l'adresse d'expéditeur et du numéro de port d'expéditeur. Le mappage des paramètres RSVP avec les paramètres contenus dans le message MAC est représenté dans le tableau ci-dessous.

Paramètre RSVP	Paramètre RESC-REQ Annexe A/J.112	Paramètre DSA-REQ Annexes B et C/J.112
Objet session		
Identificateur de protocole	Session_Binding_US. Upstream_internet_protocol	Classificateur de paquets amont. Protocole IP
Adresse de destination	Session_Binding_US. NIU_client_destination_IP_add	Classificateur de paquets amont. Adresse de destination IP
Port de destination	Session_Binding_US. NIU_client_destination_port	Classificateur de paquets amont. Début de port de destination TCP/UDP
Objet modèle d'expéditeur		
Adresse source	Session_Binding_US. NIU_client_source_IP_add	Classificateur de paquets amont. Adresse source IP
Port source	Session_Binding_US. NIU_client_source_port	Classificateur de paquets amont. Début de port source TCP/UDP

Les paramètres d'expéditeur Tspec sont dérivés des codes de paramètre QS amont J.112 contenus dans le message de signalisation de couche MAC demandant l'établissement du nouveau flux. Un exemple de mappage des paramètres de QS MAC en un objet Tspec pour construire le message PATH RSVP est donné ci-dessous. Pour de plus amples détails, on se reportera aux Annexes A, B ou C de la Rec. UIT-T J.112.

Le message PATH doit également acheminer l'objet Adspec actualisé, qui achemine le délai supplémentaire introduit par le nœud AN vers les routeurs RSVP aval. En raison des limites strictes en matière de temps d'attente, les serveurs générant le trafic VoIP devraient indiquer leurs besoins en ressources au moyen des paramètres de QS de service garantis tels que définis dans l'architecture IntServ. Ainsi, le bloc service garanti de l'objet Adspec devrait contenir les termes C (composante dépendant du débit) et D (composante indépendant du débit) appropriés. La valeur de D doit tenir compte du délai fixe (par exemple le délai de traitement de message, le délai dû au codec, etc.).

8.1.1.1.1.1 Elaboration de l'objet Tspec à partir des paramètres QS définis dans l'Annexe A de la Rec. UIT-T J.112

Pour la prise en charge des caractéristiques de débit CBR généralement associées aux sources vocales, on peut utiliser un mode d'accès à débit fixe ou à réservation.

Les détails appellent un complément d'étude.

8.1.1.1.1.2 Elaboration de l'objet Tspec à partir de des paramètres QS définis dans les Annexes B et C de la Rec. UIT-T J.112

Etant donné que les sources vocales en général présentent des caractéristiques de débit constant (CBR), les adaptateurs MTA demanderont un service d'octroi non sollicité (UGS, *unsolicited grant service*) sur la liaison J.112. Si le "type de programmation de flux de service" dans le message DSA-REQ est mis à UGS, l'objet Tspec de l'expéditeur est déterminé comme suit:

G = taille octroyée (octets);

I = intervalle octroyé (secondes).

Pour les flux VoIP, le paramètre "octroi par intervalle" serait en général mis à 1 (s'il est supérieur à 1, G doit être calculé en conséquence). Les paramètres IntServ pour "conteneur de jeton" (*token bucket*) sont les suivants:

M (taille datagramme maximale) = G – préfixe Ethernet – préfixe ES 201 488;

r (débit du conteneur) = M/I.

Le préfixe d'en-tête Ethernet occupe 18 octets et le préfixe d'en-tête défini dans les Annexes B et C/J.112 treize octets au maximum. Comme les sources VoIP présentent des caractéristiques de débit CBR, on a:

p (débit de crête) = r;

b (profondeur de conteneur) = M;

m = M.

Le préfixe défini dans les Annexes B et C/J.112 inclut seulement le préfixe de couche MAC (en-tête MAC standard, en-tête étendu BPI, etc.). Il n'inclut pas de préfixe de couche Physique.

Si la suppression d'en-tête de charge utile est utilisée dans le sens amont, M (calculé précédemment) DOIT être modifié afin de refléter les octets supprimés. Le paramètre "taille de PHS" du message DSA-REQ DOIT être utilisé pour modifier M comme suit:

M' = M – 2 + taille PHS,

où deux octets constituent l'en-tête étendue de type défini dans les Annexes B et C/J.112, contenant la valeur de l'indice PHS. Etant donné que la taille d'octroi inclut également le préfixe, elle DOIT être soustraite pour calculer M'.

Les autres paramètres Tspec sont modifiés en conséquence:

r = M'/I;

p = r;

b = M';

m = M'.

En ce qui concerne l'objet Adspec actualisé, la valeur annoncée de C pour un service UGS serait M (ou M').

8.1.1.1.2 Détermination des paramètres RSPV RESV

Lorsqu'un nœud AN reçoit un message PATH en provenance d'un nœud AN distant, il DOIT envoyer un message RESV pour réserver les ressources appropriées dans le système dorsal. Le message RESV DOIT inclure l'objet session, flowspec et le filterspec. L'objet session et filterspec sont déduits du message PATH. Le trafic VoIP doit utiliser les spécifications de flux de service garanti, qui se composent d'un Tspec et d'un Rspec. Les paramètres Tspec sont déduits de l'objet Tspec contenu dans le message PATH, les paramètres Rspec sont déduits des paramètres de QS avals J.112. Dans un environnement défini dans les Annexes B et C/J.112, les paramètres Rspec sont calculés comme suit:

R = "Débit maximal soutenable de trafic aval";

S = 0.

La valeur zéro pour le paramètre S (ralentissement) est la valeur recommandée à partir de [1] lorsque aucun ralentissement n'est spécifié.

8.1.1.2 Signalisation RSVP

Lorsque l'adaptateur MTA utilise la signalisation RSVP définie au § 6/J.163 [7], et que la signalisation RSVP par flux doit être prise en charge dans le système dorsal, le nœud AN DOIT pouvoir retransmettre les messages RSVP vers le système dorsal plutôt que de simplement les intercepter lorsqu'il les reçoit de l'adaptateur MTA. Le nœud AN DOIT prendre en charge un paramètre configurable sur chacune de ses interfaces de réseau non J.112 qui indiquent si les retransmissions de messages RSVP sont activées pour l'interface considérée. Lorsque ce paramètre a la valeur "activée" sur une interface donnée et si le nœud AN reçoit un message PATH en provenance d'un adaptateur MTA qui DEVRAIT être envoyé à travers cette interface conformément au tableau de retransmission du nœud AN, le nœud AN DOIT retransmettre le message PATH à travers cette interface. Lorsqu'il retransmet un tel message PATH qui a été reçu en provenance de l'adaptateur MTA, le nœud AN DOIT supprimer tous les objets spécifiques au DQoS (par exemple Tspec inverse, etc.) avant de retransmettre vers sa destination. Dans cette configuration, le nœud AN NE DEVRAIT PAS retourner les messages RESV avec mandat vers l'adaptateur MTA, mais DEVRAIT attendre un message RESV provenant du système dorsal et ensuite le traiter et le retransmettre conformément aux règles de traitement normalisées du protocole RSVP. De même, il ne DEVRAIT pas mandater les messages PATH vers l'adaptateur MTA, mais DEVRAIT plutôt attendre un message PATH provenant de l'extrémité distante qu'il DOIT traiter conformément aux règles normalisées du protocole RSVP.

A noter que la décision de retransmettre les messages vers le système dorsal, et non pas d'agir comme mandataire tel que décrit au § 6/J.163 [7], est basée sur une configuration interface par interface. Ainsi tous les flux de paquets média IPCablecom traversant l'interface qui est configurée tel que décrit ci-dessus feront l'objet d'un contrôle d'admission. Ce comportement est souhaitable dans la mesure où il garantit que tous les flux qui pénètrent dans le réseau par une interface donnée seront soumis à un contrôle d'admission, ce qui permettra de prendre des décisions intelligentes de contrôle d'admission.[1]

8.1.2 Position du bord Diffserv

Lorsqu'un plan de commande RSVP par flux est utilisé à travers le système dorsal, il n'est pas nécessaire pour le nœud AN de constituer le bord du nuage Diffserv. En effet, la fonction bord Diffserv peut se trouver dans un routeur de bord situé en amont du nœud AN. Dans ce cas, il peut exister un réseau entre le nœud AN et le routeur de bord, qui peut être aussi simple qu'une liaison point à point (comme c'est le cas dans la Figure 1) ou être un réseau IP de topologie générale. La QS requise peut être assurée entre le nœud AN et le routeur de bord par l'utilisation de services intégrés ou en prévoyant une largeur de bande excédentaire, le choix entre ces possibilités pouvant être effectué pour chaque liaison.

---

[1] Une autre approche consisterait à décider flux par flux s'il faut retransmettre les messages PATH pour chaque flux. Le problème qui se poserait alors serait de savoir comment une telle décision pourrait être prise, et de plus, ce qui est plus important, cela présenterait le risque de voir certains sous-ensembles de flux injecter du trafic dans le système dorsal sans être soumis à un contrôle d'admission, ce qui compromettrait la précision globale du contrôle d'admission.

8.1.3 Comportement du routeur de bord

Que le routeur de bord soit le nœud AN ou un routeur quelconque situé en amont d'un nœud AN, il DOIT participer au protocole RSVP par flux. En outre, un routeur de bord (ER) dispose d'un certain ensemble d'interfaces qui sont "internes" à la nébuleuse Diffserv et un autre ensemble d'interfaces qui sont "externes". Le routeur ER est responsable du marquage des paquets qui passent d'une interface externe à une interface interne avec un point de code DSCP convenablement choisi, à moins qu'il ait de bonnes raisons de croire que ce point de code DSCP a été fixé correctement au niveau du nœud AN. Le routeur ER DOIT effectuer le contrôle d'admission sur toutes ses interfaces pour pouvoir procéder ainsi sur ses interfaces internes, chaque interface interne doit être configurée avec un ensemble de ressources disponibles pour chaque comportement PHB qui est utilisé pour le trafic de média IPCablecom. Le routeur ER effectue le contrôle d'admission sur cet ensemble de ressources pour chaque demande RSVP qui lui parvient. Le routeur ER doit pouvoir déterminer quel comportement PHB et quel point de code DSCP il doit utiliser pour une demande RSVP donnée. Cette détermination peut être effectuée par configuration locale ou faire partie d'une politique fournie à partir d'une ressource externe, par exemple un serveur de politique.

Un routeur ER PEUT effectuer une classification, une régulation par une politique et un séquencement des microflux sur ses interfaces extérieures mais DOIT effectuer une classification agrégée, une régulation par une politique et une programmation sur ces interfaces internes. Si le routeur ER n'effectue pas cette classification et la régulation par politique des microflux sur des flux qui transitent par lui vers le système dorsal, ces fonctions DOIVENT être exécutées par les nœuds AN qui envoient le trafic au routeur ER. La régulation des microflux par une politique au niveau d'un nœud AN peut offrir une meilleure évolutivité que d'effectuer la même chose au niveau du routeur ER, étant donné que le nombre de flux devrait être plus important au niveau du routeur ER.

8.1.4 Autres dispositifs de terminaison (passerelles média, anonymiseurs, serveurs d'annonces, ponts conférences)

Pour que la signalisation RSVP par flux fonctionne effectivement à travers le système dorsal, tous les dispositifs sur lesquels peut aboutir un flux média DOIVENT pouvoir prendre en charge la signalisation RSVP par flux. Parmi ces dispositifs, citons les passerelles média, les anonymiseurs, les serveurs d'annonces, les ponts conférences. Tout dispositif sur lequel aboutit un flux média IPCablecom DOIT:

- envoyer des messages PATH vers l'extrémité ou les extrémités distantes de l'appel;
- recevoir des messages PATH et RESV en provenance de ou des extrémités distantes de l'appel;
- envoyer des messages RESV vers l'extrémité ou les extrémités distantes de l'appel en réponse aux messages PATH reçus.

Ces dispositifs extraient le contenu des messages PATH de la signalisation d'appel de la même manière qu'un adaptateur MTA le fait en fonctionnement DQoS normal. Le contenu des messages RESV peut être déduit des messages PATH de la même manière que décrite au § 8.1.1.

A noter que, tout comme un nœud AN, les dispositifs cités dans le présent paragraphe peuvent ou non fonctionner en qualité de routeur de bord, en ceci qu'ils peuvent se trouver sur le bord de la nébuleuse Diffserv ou non.

8.1.5 Comportement des routeurs principaux

Un routeur se comporte comme un routeur principal lorsqu'il reçoit des paquets sur une interface interne et les retransmet sur une interface interne. A noter qu'un simple routeur peut se comporter comme un routeur ER pour certains flux et comme un routeur principal pour d'autres flux.

Un routeur principal n'exécute pas de remarquage du point de code DSCP dans les paquets qu'il retransmet. Il effectue le contrôle d'admission sur les ressources allouées au comportement PHB approprié pour chaque réservation. Il effectue une classification, une régulation par politique et une programmation agrégées. Ainsi, le comportement de retransmission d'un routeur principal ressemble à celui d'un routeur Diffserv quelconque, même s'il utilise le protocole RSVP pour le contrôle d'admission.

8.1.6 Temps d'attente de signalisation

L'approche concernant la réservation de largeur de bande décrite dans le présent paragraphe fait appel à des messages RSVP de bout en bout pour traverser le système dorsal. Ainsi, cela peut avoir un impact sur le temps d'attente de signalisation et donc sur le délai après numérotation. Pour remplir les objectifs fixés par le fournisseur en matière de délai après numérotation, on peut utiliser les techniques suivantes:

– diminution du rafraîchissement RSVP et amélioration de la fiabilité;

– choix d'un comportement PHB à faible temps d'attente et d'un point de code DSCP pour les messages de commande RSVP.

La même situation s'applique à l'approche définie dans le paragraphe ci-dessous.

8.1.7 Préemption

Le présent paragraphe décrit les mécanismes qui peuvent être utilisés pour prendre en charge la préemption en matière de réservations (par exemple mettre à la disposition des appels d'urgence des ressources de manière préférentielle par rapport aux appels précédemment admis).

L'élément de priorité de préemption défini pour être utilisé dans les protocoles RSVP et COPS [6] PEUT être utilisé dans le système dorsal. Cet objet ne devrait pas être fourni par l'adaptateur MTA, car on ne peut pas en général confier aux utilisateurs finaux le soin de déterminer leur propre priorité de préemption. Toutefois, le contrôleur de porte fournit une classe de session au nœud AN qui PEUT être utilisée par le nœud AN pour générer un élément de priorité de préemption valide. Dans ce cas, le nœud AN DEVRAIT utiliser le mappage suivant des valeurs de classe de session en valeurs de priorité de préemption:

Type de session	Valeur de classe de session	Valeur de priorité de préemption
Normal	0x01	32767
A haute priorité (urgence)	0x02	64911

Ce mappage DEVRAIT être configurable. L'élément priorité de préemption contient à la fois un champ priorité défendante et un champ priorité de préemption. Ces champs DEVRAIENT être mis à la même valeur.

Il est aussi possible que les routeurs compatibles RSVP dans le système dorsal utilisent le protocole COPS pour importer des décisions de politique. Dans ce cas, l'élément de priorité de préemption PEUT être transporté dans une décision COPS et son interprétation au niveau des routeurs DOIT être telle que définie dans [6].

8.2 Protocole RSVP agrégé

Le protocole RSVP agrégé [5] est une extension logique du protocole RSVP par flux à travers un système dorsal Diffserv. Pour prendre en charge cette fonctionnalité, les fonctions du nœud AN, du routeur de bord et du routeur principal, décrites au § 8.1, DOIVENT être assurées. Une fonctionnalité additionnelle peut être assurée en agrégeant et en désagrégeant des routeurs tels que définis ci-dessous. La signalisation RSVP est effectuée entre les points d'extrémité d'appel (soit les

adaptateurs MTA ou le nœud AN agissant au nom des adaptateurs MTA) comme au paragraphe précédent. Outre la fonctionnalité du § 8.1, le protocole RSVP agrégé définit la manière avec laquelle un grand nombre de réservations RSVP par flux peuvent être combinées pour former une seule réservation agrégée. Plusieurs réservations RSVP par flux peuvent être agrégées lorsque leur trajet passe à travers une paire commune de routeurs. Nous parlons de routeurs qui sont capables d'agréger ou de désagréger des réservations comme des routeurs d'agrégation. Le comportement des routeurs d'agrégation et de désagrégation est défini de façon plus formelle dans le commentaire IETF RFC 3175 [5].

Les routeurs d'agrégation ont la responsabilité de créer des réservations agrégées à travers une région d'agrégation qui peut être la totalité de la nébuleuse Diffserv ou une région d'agrégation définie dans la nébuleuse. Chaque réservation agrégée représente un flux agrégé de trafic provenant d'un routeur d'entrée (ou agrégateur) vers un routeur de sortie (désagrégateur). Les réservations agrégées peuvent être configurées statistiquement sur la base de la charge attendue provenant d'un routeur d'entrée et destinées à un routeur de sortie, ou peuvent être automatiquement redimensionnées tel que décrit dans [5]. Chaque réservation agrégée achemine le trafic à partir d'un certain nombre de réservations RSVP "de bout en bout" qui partagent une paire commune de routeurs d'entrée/sortie. Une réservation de bout en bout représente un simple microflux, et la signalisation associée à une telle réservation est effectuée en utilisant le protocole RSVP standard. Les messages RSVP "de bout en bout" peuvent être produits par l'adaptateur MTA ou par le nœud AN au nom de l'adaptateur MTA dans le cas d'une signalisation intégrée, tel que décrit ci-dessus. Ces messages RSVP E2E sont "tunnelés" à travers la région d'agrégation en donnant au numéro de protocole IP contenu dans le message PATH la valeur "RSVP-E2E-IGNORE".

A noter que l'agrégateur et le désagrégateur peuvent aussi être des routeurs de bord tels que définis ci-dessus. La relation entre ces dispositifs est définie au § 8.2.4.

8.2.1 Réservations agrégées fournies

Il est possible de fournir une réservation agrégée à partir d'un routeur d'entrée (agrégateur) vers un routeur de sortie (désagrégateur). Cela nécessite une connaissance préalable de la charge attendue entre les routeurs afin de déterminer la taille de la réservation. Dans ce cas, le routeur d'entrée envoie un message PATH agrégé vers le routeur de sortie, et le routeur de sortie répond par un message RESV agrégé qu'il renvoie au routeur d'entrée. Cela établit une réservation agrégée pour le trafic circulant du routeur d'entrée vers le routeur de sortie et qui est marqué avec le code point DSCP approprié tel qu'identifié dans le message RSVP d'agrégation.

Après avoir été établie entre une paire de routeurs, la réservation d'agrégation peut être traitée comme liaison logique pour les besoins du contrôle d'admission. Le contrôle d'admission pour un appel individuel est effectué lorsque le message RESV de bout en bout parvient au routeur de sortie. Avant que cela se produise, un message PATH E2E DOIT être envoyé du routeur d'entrée vers le routeur de sortie. Le routeur d'entrée positionne l'identificateur de protocole à RSVP-E2E-IGNORE, ce qui signifie que le trajet est ignoré par tous les routeurs entre l'entrée et la sortie. Lorsque la sortie reçoit le message PATH E2E, le saut précédent (PHOP, *previous hop*) identifie le routeur d'entrée. Le routeur de sortie stocke cette information et retransmet le trajet vers sa destination.

Lorsqu'un RESV E2E parvient au routeur de sortie, il détermine à quelle réservation agrégée cette réservation E2E appartient en examinant l'information PHOP se trouvant dans l'état PATH qui correspond au RESV. Le trajet PHOP est le routeur d'entrée de la réservation agrégée appropriée. Le routeur de sortie DOIT suivre les ressources attribuées à une réservation agrégée particulière étant donné qu'elles sont consommées par les réservations E2E admises et DOIT rejeter une réservation E2E qui ne peut pas être prise en charge dans la réservation agrégée appropriée.

8.2.2 Réservations agrégées dynamiques

L'inconvénient le plus évident de la fourniture statistique de réservations agrégées est qu'elles doivent être dimensionnées de manière appropriée et que le surdimensionnement provoque un gâchis de ressources alors que le sous-dimensionnement mènera à un blocage d'appel excessif. Ces inconvénients sont évités par la création et le redimensionnement dynamique des réservations agrégées en réaction à l'arrivée et au départ de réservations E2E. Les détails concernant la création, le redimensionnement et la suppression automatique de réservations agrégées sont donnés dans [5].

Une considération importante concernant le redimensionnement dynamique des réservations est le volume de préfixe de signalisation qu'elle peut introduire. Si la réservation agrégée est ajustée en taille à chaque arrivée ou départ de réservation E2E, le préfixe de signalisation reste égal à ce qu'il serait sans agrégation RSVP, bien que l'état de réservation stocké se trouve néanmoins réduit. Si la présence de préfixe de signalisation excessif peut poser un problème, il est préférable d'utiliser l'heuristique pour dimensionner la réservation agrégée, par exemple en arrondissant les largeurs de bande agrégées réservées à une valeur un peu supérieure à la somme des réservations E2E courantes.

8.2.3 Agrégation hiérarchique

Comme indiqué dans [5], les réservations agrégées peuvent être à leur tour agrégées. Cela permet une réduction plus poussée du nombre total de réservations qui doivent être effectuées à travers le système dorsal du réseau, bien que la réduction réelle dépende clairement de la topologie.

8.2.4 Localisation des points d'intégration et du bord DiffServ

Tout comme au § 8.1.2, le bord Diffserv peut se trouver au niveau du nœud AN ou plus loin en amont dans le système dorsal, et les mêmes options s'appliquent ici pour la fourniture de QS entre le nœud AN et le bord Diffserv. Les fournisseurs disposent d'une souplesse considérable pour ce qui est de l'implantation des points d'agrégation (routeur d'agrégation et routeur de désagrégation). Un point d'agrégation peut coïncider avec le bord Diffserv (c'est-à-dire un routeur de bord PEUT effectuer l'agrégation) ou peut être placé à l'intérieur de la nébuleuse Diffserv. Les points d'intégration ne DOIVENT PAS être placés en dehors de la nébuleuse Diffserv.

Une solution extrême consiste à faire en sorte que le nœud AN soit à la fois le routeur de bord Diffserv et le point d'agrégation. Dans ce cas, le nœud AN assume les fonctions de routeur de bord et également celles d'agrégation et de désagrégation. Bien qu'il puisse être théoriquement possible de se dispenser de signalisation RSVP de bout en bout pour les flux individuels dans cette configuration, une signalisation RSVP de bout en bout offre deux avantages, à savoir:

– Elle permet, de manière simple, de découvrir quelle réservation agrégée parmi les nombreuses réservations en concurrence et celle à laquelle un flux donné appartient.

– Elle offre un mécanisme par lequel les points d'extrémité peuvent reconnaître la nécessité de créer dynamiquement une réservation agrégée ou d'augmenter ou de diminuer la taille d'une réservation agrégée.

Le deuxième avantage ne s'applique pas aux réservations agrégées fournies statistiquement et il y a, dans certains cas, d'autres façons de déterminer la réservation agrégée à laquelle un simple flux appartient. Par exemple, si les nœuds agrégeants et désagrégeants se trouvent dans la même zone d'un réseau utilisant le routage par état de liaison, la base de données état de liaison peut être utilisée pour trouver le désagrégateur compte tenu de l'adresse de l'adaptateur MTA d'extrémité distante.

L'agrégation au niveau du nœud AN conduit à un grand nombre potentiel de réservations agrégées dans le système dorsal, nombre qui est de l'ordre du carré du nombre de nœuds AN. Si le nombre d'appels en cours entre une paire de nœuds AN est souvent faible, il est plus utile de l'agréger encore plus dans le système dorsal.

Un point d'agrégation donné peut décider d'agréger le trafic vers certaines destinations et pas d'autres sur la base d'une politique locale (par exemple, procéder à une agrégation seulement lorsque le nombre d'appels vers cette destination dépasse un seul configuré).

Tout comme au § 8.1.3, une régulation par politique des microflux DOIT être effectuée avant que les paquets d'un flux ne pénètrent la nébuleuse DiffServ. Cette fonction peut être exécutée par le nœud AN ou par le routeur de bord.

8.3 Courtier en largeur de bande

La notion de courtier en largeur de bande (voir Figure 2) est introduite dans [8] et a fait l'objet de très importantes recherches. Un courtier en largeur de bande est un agent de contrôle d'admission centralisé à partir duquel les demandes en largeur de bande peuvent être formulées. Ces demandes peuvent être formulées par des serveurs, par d'autres courtiers situés dans des domaines voisins ou par des routeurs de bord. Dans l'environnement IPCablecom, il serait possible pour chaque nœud AN ou serveur CMS de formuler des demandes de largeur de bande à partir d'un courtier de largeur de bande qui est responsable de la gestion de l'accès à la largeur de bande pour un domaine particulier. Ces demandes spécifieraient également le comportement PHB pour lequel la demande est formulée. Le courtier en largeur de bande pour chaque domaine est alors responsable de la formulation des demandes de largeur de bande provenant des domaines voisins.

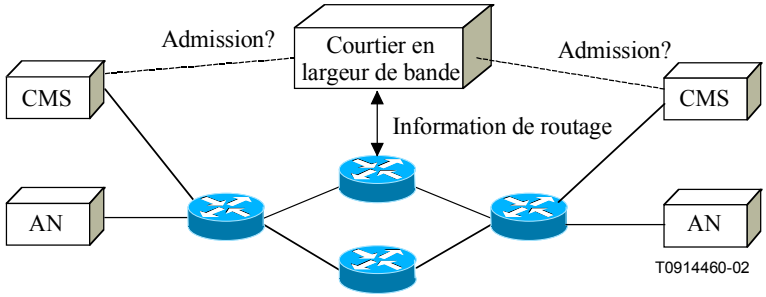


Figure 2/J.174 – Exemple de courtier en largeur de bande

Il existe une très grande souplesse en matière d'algorithme et de mécanismes de commande d'admission que le courtier en largeur de bande peut utiliser. Chaque courtier doit rejeter toute demande de largeur de bande pour un comportement donné qui se traduirait par une suraffectation des ressources et une dégradation de la qualité des appels déjà en cours. Afin d'effectuer cette fonction de contrôle d'admission, un courtier en largeur de bande peut simplement limiter le volume total de trafic qui est autorisé à pénétrer dans le domaine indépendamment des trajets que les appels emprunteront. Dans ce cas, l'opérateur de réseau peut faire certaines hypothèses statistiques concernant la distribution des appels (par exemple, il est très improbable que tous les appels convergeront vers une seule liaison) afin de déterminer la quantité de largeur de bande qu'il peut en toute sécurité octroyer. Une approche plus prudente serait de prendre pour hypothèse le cas le plus défavorable, cas dans lequel tous les appels convergent vers la liaison la plus limitée en ressources, et d'utiliser la capacité de cette liaison pour le comportement PHB demandeur comme limite pour les demandes en largeur de bande admises.

Une approche plus élaborée du contrôle d'admission consisterait à ce qu'elle repose sur le courtier en largeur de bande ayant une certaine compréhension de la topologie du réseau et de la route à emprunter par un appel. Un courtier en largeur de bande pourrait être configuré avec la connaissance de la topologie du réseau (éventuellement limitée à la localisation des liaisons les plus limitées en ressource) ou pourrait apprendre dynamiquement la topologie, par exemple en écoutant les annonces de routage d'état de liaison, améliorées par des informations relatives aux ressources. Les demandes en largeur de bande formulées au courtier dans ce cas doivent comprendre un nombre suffisant d'informations au sujet de la destination de l'appel pour permettre au courtier de

déterminer quelles liaisons limitées en ressources seront empruntées par l'appel et ainsi si l'appel peut être admis en toute sécurité.

Tout comme avec le protocole RSVP agrégé, il n'est pas strictement nécessaire d'avoir une signalisation par appel – il peut être possible pour un nœud AN d'agréger les demandes pour des appels ayant des destinations similaires. A noter toutefois que cela nécessiterait une certaine connaissance de la topologie dans le nœud AN.

Il n'existe pas actuellement un protocole normalisé pour la communication avec ou entre des courtiers en largeur de bande.

9 Contrôle d'admission sur plusieurs domaines

En principe, chaque réseau à domaine IPCablecom devrait avoir leur propre politique et leur propre procédure opérationnelle. En principe également, les opérateurs de réseau IPCablecom devraient peut-être utiliser plusieurs fournisseurs de transport IP pour acheminer leur trafic IPCablecom, chacun pouvant utiliser différentes topologies de réseau. Il est donc difficile de supposer que des mécanismes de QoS homogènes seront disponibles de bout en bout pour des appels franchissant des systèmes dorsaux de plusieurs fournisseurs. Comme décrit dans [4], il est possible d'utiliser le protocole RSVP de bout en bout sans exiger que tous les domaines intervenant aient connaissance du protocole RSVP. Par exemple, un domaine peut utiliser un modèle pur Diffserv préinstallé, un autre l'agrégation RSVP et enfin un autre le protocole RSVP par flux. On peut observer qu'il n'y a pas de raisons pour lesquelles les réservations par flux ou RSVP agrégées ne puissent traverser les limites de domaine si deux domaines adjacents décident d'honorer chaque autre demande RSVP. Dans un tel environnement, on peut atteindre une plus forte assurance que celle obtenue si certains domaines ne prennent pas en charge le protocole RSVP. En outre, l'effet de l'agrégation sur l'évolutivité peut être amélioré si les réservations agrégées peuvent franchir les limites des domaines, étant donné que cela ne rend pas nécessaire la désagrégation des demandes RSVP au niveau du routeur de limite.

Il est également possible pour différents fournisseurs de choisir des approches technologiques très variables pour fournir la QS dans leurs systèmes dorsaux. Par exemple, un fournisseur peut choisir de mettre en œuvre son système dorsal en utilisant l'ATM, et des réservations RSVP (individuelles ou agrégées) peuvent être satisfaites en établissant des circuits virtuels ATM avec les caractéristiques de QS appropriées. D'autres fournisseurs peuvent utiliser des liaisons à hiérarchie numériques synchrones pour connecter directement des routeurs. Les fournisseurs disposent d'une souplesse analogue pour ce qui est de la décision d'utiliser ou de ne pas utiliser la commutation MPLS examinée plus haut.

10 Utilisation de la commutation MPLS

NOTE – Le texte présenté dans le présent paragraphe a un caractère uniquement informationnel.

La commutation MPLS [12] (commutation multiprotocolaire par étiquetage) PEUT être utilisée dans le système dorsal, les trajets avec commutation d'étiquette (LSP, *label switched path*) étant utilisés pour représenter les réservations agrégées ou les flux de trafic agrégés. Cette façon de procéder présente les avantages potentiels suivants:

1) possibilité d'effectuer une ingénierie du trafic de façon plus précise en l'absence de commutation MPLS;
2) présence de mécanismes de rétablissement en cas de pannes de liaison ou de nœud;
3) acheminement fondé sur des contraintes des réservations agrégées;
4) acheminement homogène des messages et des données de contrôle d'agrégation.

Le premier avantage s'applique à toutes les approches décrites dans les paragraphes précédents. Par ingénierie du trafic, on entend la capacité à gérer les trajets pris par les flux agrégés de trafic, avec le but général d'éviter la sur ou sous-utilisation des liaisons. L'ingénierie du trafic MPLS et les avantages qu'elle procure sont décrits en [11].

Comme décrit dans [15], la commutation MPLS offre les moyens de protection contre les pannes de liaison ou de nœud dans un réseau. Par exemple, des trajets de secours peuvent être préétablis pour contourner les circuits défectueux, et ainsi protéger une liaison ou un nœud contre les pannes. En acheminant des paquets sur un trajet de secours LSP depuis un nœud situé en amont d'un point où il y a eu une panne, il est possible d'éviter le délai associé à l'attente de routage IP pour reconverger après une panne. Ainsi, la période de temps pendant laquelle la retransmission des paquets est interrompue en raison d'une panne de liaison, d'une panne de nœud ou d'une perte de paquet résultant d'un routage non homogène, peut être fortement réduite.

L'acheminement fondé sur des contraintes des réservations agrégées permet de choisir les trajets sur la base de leur capacité à satisfaire aux contraintes, en particulier la disponibilité d'une largeur de bande suffisante pour prendre en charge une demande de réservation particulière, telle que décrite en [11]. Cela permettra en général d'établir un plus grand nombre de réservations que cela ne serait possible si toutes les demandes de réservation suivaient le trajet le plus court comme déterminé par le routage IP conventionnel.

Le quatrième avantage, décrit dans [5], s'applique tout d'abord au cas où le trafic est scindé entre des trajets de coût égal, introduisant le risque qu'un message PATH agrégé n'emprunterait qu'un seul trajet tandis que les données nécessitant une réservation en emprunterait un autre. Ce problème serait évité si les données sont "tunnelées" depuis l'entrée jusqu'à la sortie, et la commutation MPLS offre une technologie de tunnelage appropriée.

Un autre avantage de la commutation MPLS est qu'elle peut être mise en œuvre par étape, nœud par nœud, via des mises à jour logicielles. Cela est avantageux dans le sens où le routage existant et les mécanismes de QS peuvent être préservés et pris en charge pendant une mise en place progressive de la commutation MPLS.

Le choix d'appliquer la commutation MPLS dans un domaine quelconque peut être effectué indépendamment des autres domaines et dépend de la façon dont le fournisseur a besoin ou souhaite traiter des trois points précités.

A noter que la commutation MPLS peut être utilisée avec toutes les approches décrites aux paragraphes 7 et 8. Dans un système dorsal Diffserv pur (sans signalisation), les principaux avantages seraient dans le domaine de l'ingénierie du trafic et dans le reroutage rapide. Le routage de réservation fondé sur des contraintes est utile pour les approches exposées aux § 8.1 et 8.2, tandis que le routage homogène des messages de contrôle et de données n'a de sens que pour le protocole RSVP avec agrégation (voir § 8.2).

11 Mise en file d'attente et filtrage

11.1 Mise en file d'attente

La qualité vocale sur les réseaux IPCablecom peut être dégradée non uniquement par des restrictions de largeur de bande. Le temps d'attente, la gigue et la perte de paquet sont également des paramètres de transmission qu'il faut observer. La diminution du délai et de la gigue est principalement obtenue par une gestion appropriée des files d'attente dans les routeurs. En tant que tel, le choix des technologies de file d'attente peut s'avérer aussi important que le choix des mécanismes de QS tel Diffserv, le protocole RSVP par flux et l'agrégation RSVP sont utilisés. Des méthodes de mise en file d'attente soigneusement choisies et convenablement configurées peuvent se traduire par une faible gigue et un faible temps d'attente pour le trafic spécifié.

La mise en file d'attente avec priorité (PQ, *priority queuing*) par exemple, peut donner une priorité plus élevée au trafic média IPCablecom par rapport aux autres types de trafic. Le classement par ordre de priorité permet aux autres paquets, outre le trafic média IPCablecom, d'utiliser la file d'attente aussi longtemps que la QS pour le trafic IPCablecom est maintenue. Toutefois, dans le cas de la mise en file d'attente avec priorité, le traitement équitable du trafic de faible priorité doit être garanti.

La mise en file d'attente équitable pondérée (WFQ, *weighted fair queuing*) peut répartir la largeur de bande disponible équitablement entre les flux de trafic. Même dans des situations d'encombrement, un débit constant est maintenu. Toutefois, étant donné que cette méthode ne peut pas donner de priorité absolue au trafic média IPCablecom, on peut s'attendre à une dégradation de la qualité dans les routeurs encombrés.

Plusieurs autres méthodes qui produisent des files d'attente de manière dynamique ou utilisent une multitude de files d'attente peuvent également être mises en œuvre. L'applicabilité de ces méthodes à IPCablecom nécessite une évaluation relativement à leur capacité à maintenir la QS spécifiée pour le trafic média. Une configuration soigneuse de la méthode de mise en file d'attente sera souvent nécessaire.

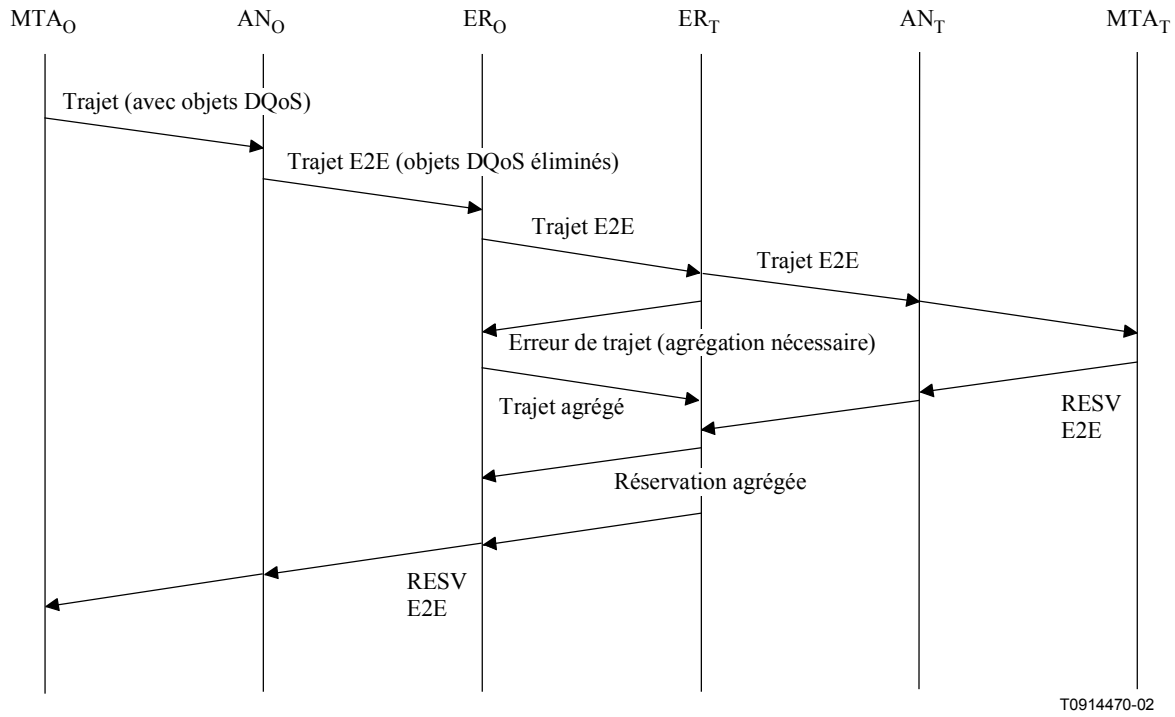
11.2 Filtrage

Certains routeurs utilisent des fonctions de filtrage pour limiter le trafic pour des raisons de sécurité de réseau. Les fonctions de filtrage peuvent mobiliser des ressources telles que de la puissance d'unité centrale et de la mémoire qui peut dégrader les performances du routeur et, de ce fait, provoquer une dégradation des paramètres de QS tels des pertes de paquets, de la gigue et des délais d'attente. Les routeurs qui utilisent le filtrage des paquets devraient disposer de ressources suffisantes pour traiter tout le trafic soumis.

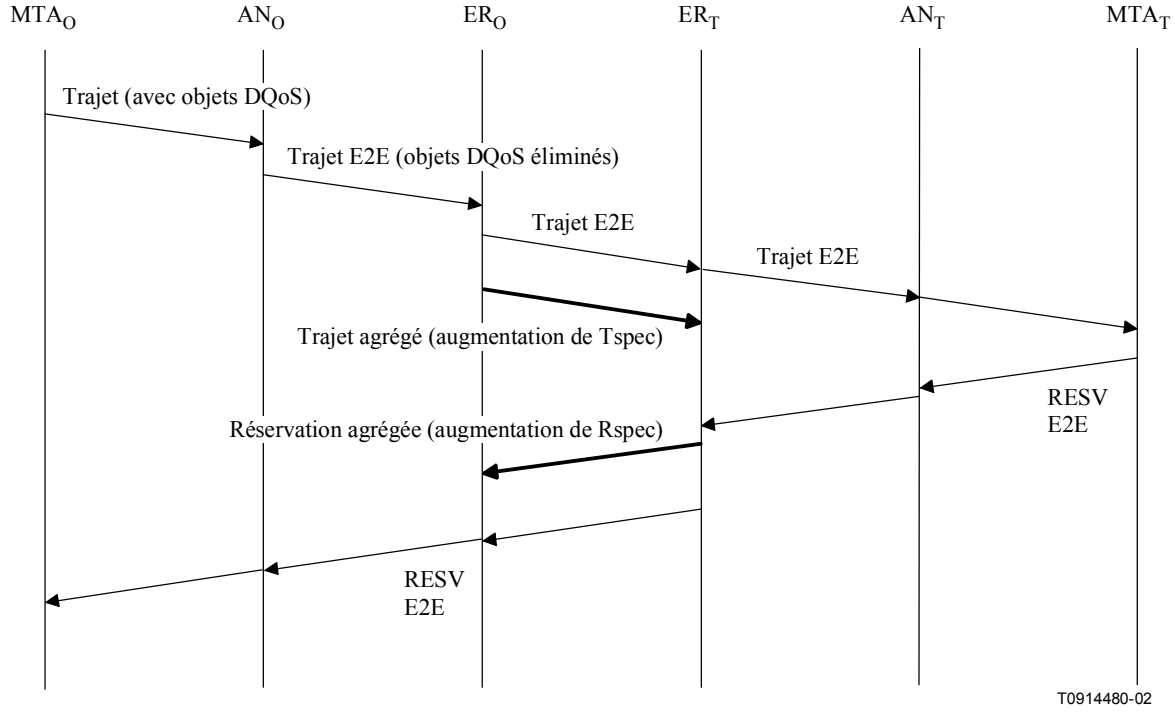
Appendice I

Exemples de flux d'appel

Dans les exemples, les deux adaptateurs MTA utilisent la signalisation RSVP DQoS et l'agrégation RSVP effectuée par les routeurs de bord; dans un souci de clarté, seul l'échange des messages unidirectionnel est représenté.



L'exemple suivant montre l'augmentation de taille d'une réservation agrégée existante en réponse à une nouvelle réservation E2E.



Appendice II

Bibliographie

[1] Recommandation UIT-T Y.1541 (2002), *Objectifs de qualité de fonctionnement du réseau pour services en mode IP*.

[2] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[3] IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services*.

[4] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service*.

[5] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*.

[6] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[7] IETF RFC 2747 (2000), *RSVP Cryptographic Authentication*.

[8] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.

[9] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.

[10] AWDUCHE [D.] et al.: Extensions to RSVP for LSP Tunnels, *draft-ietf-mpls-rsvp-lsp-tunnel-09.txt*, août 2001.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2002