UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.179

(04/2004)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

IPCablecom

Prise en charge du multimédia par IPCablecom

Recommandation UIT-T J.179

Recommandation UIT-T J.179

Prise en charge du multimédia par IPCablecom

Résumé

La présente Recommandation prend en charge la mise en place de services multimédia généraux en fournissant une définition technique de plusieurs interfaces de signalisation fondées sur le protocole IP qui démultiplient les capacités en matière de qualité de service et de gestion de politique à partir des câblo-modems.

Source

La Recommandation UIT-T J.179 a été approuvée le 22 avril 2004 par la Commission d'études 9 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

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

Introduction

Depuis le début, l'initiative IPCablecom s'est présentée comme une infrastructure de mise en place de services multimédia fondés sur IP, exploitant et améliorant les capacités sous-jacentes de qualité de service du réseau d'accès par câblo-modem. Sur la base de la demande du marché et des avancées de la technologie, la téléphonie vocale a été choisie comme premier service fondé sur le protocole IP pour démultiplier ces capacités uniques de réseau d'accès haut débit, puisque la série de Recommandations IPCablecom-T définit simultanément à la fois un cadre général de livraison de services fondés sur la qualité de service et un certain nombre d'éléments fonctionnels et de mécanismes spécifiques de la téléphonie. Dans la mesure où les intentions de la présente Recommandation sont d'extraire le centre fonctionnel de cette architecture pour servir à l'amélioration et au développement d'autres services multimédia, la prise en charge de ces caractéristiques spécifiques de la téléphonie n'est pas exigée, alors que sont développés et généralisés les mécanismes d'échange de messages d'événement et de sécurité ainsi que la qualité de service centrale. Il en résulte un cadre qui fournit les mécanismes de qualité de service du réseau d'accès par câblo-modem en accès fondé sur le protocole IP complétés par des mécanismes solides et sécurisés d'autorisation et d'audit.

Recommandation UIT-T J.179

Prise en charge du multimédia par IPCablecom

1 Domaine d'application

La présente Recommandation prend en charge le développement de services multimédia généraux en fournissant une définition technique de plusieurs interfaces de signalisation fondées sur IP qui mettent à niveau les capacités centrales de gestion de politique inhérentes aux câblo-modems. Les services multimédia sont définis comme services fondés sur IP (par exemple, jeux en ligne, visioconférence, transferts de média, etc.) nécessitant des ressources de réseau fondées sur la qualité de service (par opposition à des services comme la consultation sur le Web, la messagerie électronique, la messagerie instantanée et le partage de fichiers qui sont habituellement fournis en utilisant des flux au mieux). Alors que la téléphonie ou les services fondés sur la voix ne sont pas spécifiquement exclus de cette définition, l'ensemble des Recommandations IPCablecom-T fournit une couverture spécifique pour ce type de prestation de service, et donc, ces Recommandations devraient être consultées en tant que de besoin.

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. La référence à un document au sein de la présente Recommandation ne lui donne pas, en tant que document autonome, le statut d'une Recommandation.

2.1 Références normatives

[1] Recommandation UIT-T J.112 Annexe B (2004), *Spécifications de l'interface du service de transmission de données par câble: interface radioélectrique*.

[2] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis* (Spécification du protocole temporel de réseau (version 3), mise en œuvre et analyse).

[3] IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services* (Utilisation du protocole RSVP avec des services intégrés de l'IETF).

[4] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service* (Spécification de l'élément de service de réseau à charge contrôlée).

[5] IETF RFC 2212 (1997), *Specification of Guaranteed Quality of Service* (Spécification de la qualité de service garantie).

[6] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* (Définition du champ de services différentiés dans les en-têtes Ipv4 et Ipv6).

[7] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* (Le protocole COPS (Service commun de politique ouverte)).

[8] IETF RFC 2866 (2000), *RADIUS Accounting* (Comptabilité RADIUS).

[9] Recommandation UIT-T J.163 (2004), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[10] Recommandation UIT-T J.164 (2001), *Prescriptions relatives aux messages d'événement pour la prise en charge des services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[11] Recommandation UIT-T J.170 (2002), *Spécification de la Sécurité IPCablecom*.

[12] Recommandation UIT-T J.125 (2004), *Confidentialité des liaisons pour les implémentations de câblo-modem*.

2.2 Références informatives

[13] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview* (Services intégrés dans l'architecture Internet: vue d'ensemble).

[14] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification* (Protocole de réservation de ressources (RSVP) – Version 1 de la spécification fonctionnelle).

[15] IETF RFC 2216 (1997), *Network Element Service Specification Template* (Canevas de spécification de service d'élément de réseau).

[16] IETF RFC 2475 (1998), *An Architecture for Differentiated Services* (Architecture de services différentiés).

[17] IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces* (Base d'informations de gestion d'interface radio fréquence pour interfaces RF conformes à MCNS/DOCSIS).

[18] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* (Cadre général pour le contrôle d'admission fondé sur la politique).

[19] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* (Utilisation de COPS pour l'approvisionnement en politique (COPS-PR)).

[20] IETF RFC 3175 (2001), *Aggregation of RSVP for IPv4 and IPv6 Reservations* (Agrégation de RSVP pour les réservations Ipv4 et Ipv6).

[21] CableLabs (http://www.cablemodem.com/specifications/).

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 client de type 1: le client de type 1 représente les points d'extrémité ordinaires existants (par exemple, des applications pour micro-ordinateur, des consoles de jeu) qui ne possèdent pas de capacités de qualité de service spécifiques ou de capacités de signalisation. Ce client ne sait rien des câblo-modems, d'IPCable2Home, ou de l'échange de messages IPCablecom, et par conséquent, on ne peut rien exiger de sa part pour ce qui les concerne. De tels clients vont des simples appareils de présentation analogiques audio et vidéo à des périphériques complexes en réseau avec de l'électronique grand public, tels que "set-top boxes" ou consoles de jeu. Ce client communique avec un gestionnaire d'application pour ses demandes de service, et n'a pas besoin de demander des ressources de qualité de service directement à l'opérateur du réseau d'accès. La présente Recommandation ne prend en charge que le client de type 1.

3.2 client de type 2: le client de type 2 est semblable à un adaptateur MTA de téléphonie d'IPCablecom-T en ce qu'il prend en charge la signalisation de qualité de service fondée sur la qualité de service dynamique d'IPCablecom. Ce client est averti de la qualité de service multimédia d'IPCablecom et communique avec un gestionnaire d'application pour demander le service et

obtenir un jeton pour les ressources du réseau d'accès. Ce client présente alors ce jeton lorsqu'il demande des ressources de qualité de service du réseau d'accès (pkt-mm-1, pkt-mm-6). La prise en charge du client de type 2 par la présente Recommandation fera l'objet d'un complément d'étude.

3.3 client de type 3: le client de type 3 demande de la qualité de service fondée sur le protocole RSVP sans interaction avec un gestionnaire d'application. Ce client est averti du protocole RSVP fondé sur les normes de l'IETF et utilise ce protocole pour demander des ressources de qualité de service du réseau d'accès directement au système CMTS. La prise en charge du client de type 3 par la présente Recommandation fera l'objet d'un complément d'étude.

3.4 DOCSIS: décrit une technologie spécifique des câblo-modems qui est développée par les Laboratoires de Télévision par câble, Inc. ("CableLabs") qu'on trouve à: http://www.cablemodem.com/specifications/. La version internationale est définie à l'Annexe B de la Rec. UIT-T J.112.

3.5 IPCablecom-T: série des Recommandations UIT-T sur IPCablecom qui prend en charge le service téléphonique.

4 Abréviations, acronymes et conventions

4.1 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

AM gestionnaire d'application (*application manager*). Système qui sert d'interface au ou aux serveurs de politique pour demander un service fondé sur la qualité de service au nom de l'utilisateur final ou du système de gestion de réseau.

BCID identifiant de corrélation de facturation (*billing correlation ID*). Défini dans la Recommandation sur l'échange de messages d'événement d'IPCablecom.

CM câblo-modem (*cable modem*)

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

CMTS système de terminaison de câblo-modem (*cable modem termination system*)

COPS service commun de politique ouverte (*common open policy service*). Défini dans RFC 2748.

DSx (échange de messages) Mécanisme de signalisation de la qualité de service de la Rec. J.112 Annexe B qui fournit la sémantique de l'Ajout, du Changement et de la Suppression de service dynamique.

FQDN nom de domaine complet (*fully qualified domain name*)

HFC hybride optique coaxial (*hybrid fibre/coax*)

IETF Groupe de travail d'ingénierie Internet (*Internet engineering task force*)

IP protocole Internet (*Internet protocol*)

KDC centre de distribution de clé (*key distribution center*)

MG passerelle média (*media gateway*)

MGC contrôleur de passerelle média (*media gateway controller*)

MTA adaptateur de terminal multimédia (*multimedia terminal adapter*)

NAT traduction d'adresse de réseau (*network address translation*)

PDP point de décision de politique (*policy decision point*). Défini dans RFC 2753.

PEP point d'application de politique (*policy enforcement point*). Défini dans RFC 2753.

PS serveur de politique (*policy server*)

QS qualité de service

RADIUS service d'authentification à distance des utilisateurs entrants (*remote authentication dial-in user service*). Défini dans RFC 2138 et RFC 2139.

RAP groupe de travail Protocole d'allocation de ressources de l'IETF (*resource allocation protocol*). Responsable de la définition et de la maintenance du protocole COPS.

RCD domaine de contrôle des ressources (*resource control domain*)

RFC demande de commentaires (*request for comments*). Documents de politique technique adoptés par l'IETF et disponibles à http://www.ietf.org/rfc.html.

RFI spécification d'interface Radio Fréquence (*radio frequency interface*), qui définit les interfaces des couches MAC et Physique entre les éléments de réseau CMTS et câblo-modem

RKS serveur d'archivage (*record keeping server*)

RSVP protocole de réservation de ressources (*resource reservation protocol*). Défini dans RFC 2205.

RSVP+ profil et extension IPCablecom de RSVP, défini dans la Recommandation sur la DQoS IPCablecom.

RTPC réseau téléphonique public commuté

SCD domaine de commande de session (*session control domain*)

S-MTA MTA autonome. Nœud unique qui contient un adaptateur MTA et un code MAC non-DOCSIS (par exemple, Ethernet).

TCP protocole de commande de transmission (*transmission control protocol*)

TLV type-longueur-valeur. Technique utilisée pour le formatage d'éléments de protocole

UDP protocole datagramme d'utilisateur (*user datagram protocol*). Protocole sans connexion construit sur le protocole Internet (IP).

UGS attribution non sollicitée (*unsolicited grant service*). Type de programmation de la qualité de service de l'Annexe B de la Rec. UIT-T J.112, utilisé pour les services à débit binaire constant (par exemple, les codecs vocaux).

UGS/AD attribution non sollicitée avec détection d'activité vocale (*unsolicited grant service with activity detection*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

VPN réseau privé virtuel (*virtual private network*)

4.2 Conventions

Dans l'ensemble de la présente Recommandation, les termes employés pour définir l'importance d'une prescription particulière sont en majuscules. Ce sont les suivants:

"DOIT" ce mot ou l'adjectif "REQUIS" signifie que l'élément est une exigence absolue de la présente Recommandation.

"NE DOIT PAS" cette phrase signifie que l'élément est une exigence absolue de la présente Recommandation.

"DEVRAIT"	ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il existe des raisons valables dans des circonstances particulières pour ignorer cet élément, mais il faut en comprendre toutes les implications et peser attentivement les choses avant de choisir une voie différente.
"NE DEVRAIT PAS"	cette phrase signifie qu'il peut exister des raisons valables dans des circonstances particulières, lorsque le comportement indiqué est acceptable ou même utile, mais il faut en comprendre toutes les implications et peser attentivement les choses avant d'implémenter tout comportement décrit avec cette mention.
"PEUT"	ce mot ou l'adjectif "OPTIONNEL" signifie que cet élément est véritablement optionnel. Un vendeur peut choisir d'inclure l'élément, par exemple parce qu'un marché particulier le requiert ou parce qu'il améliore le produit ; un autre vendeur peut omettre le même élément.

5 Aperçu général technique

Le présent paragraphe contient les matériaux de base que certains lecteurs pourront trouver utiles pour replacer dans leur contexte les recommandations détaillées sur le protocole d'interface qui suit. L'objet du présent paragraphe est de fournir un aperçu général de haut niveau de l'architecture multimédia d'IPCablecom et des techniques fondamentales qui la fondent. Pour des détails complémentaires sur l'architecture multimédia, se reporter à l'Appendice I.

5.1 Bases de la qualité de service

Ainsi qu'il est noté tout au long de la présente Recommandation, une des caractéristiques de base du cadre du service multimédia d'IPCablecom tient au fait qu'elle fournit un accès de couche IP aux capacités sophistiquées de qualité de service définies dans l'Annexe B à la Rec. UIT-T J.112 et dans IPCablecom-T. Le présent paragraphe donne un bref aperçu général de ces capacités comme approche préliminaire de l'examen détaillé de la politique de qualité de service et de la gestion des ressources qui suit.

5.1.1 Résumé de la qualité de service de l'Annexe B de J.112

La Recommandation sur l'interface RFI de l'Annexe B de J.112 [1] définit un ensemble de facilités de qualité de service fondées sur un organe fondamental de gestion des ressources réseau connu sous le nom de Flux de service. Un flux de service se définit comme un "service de transport de couche MAC qui:

1) fournit du transport unidirectionnel de paquets de l'entité de service de couche supérieure à l'interface radio fréquence;
2) met en forme, régule, et donne des priorités au trafic conformément aux paramètres de qualité de service du trafic définis pour le flux."

En plus de cette idée de base abstraite de faciliter la réservation et la programmation des ressources partagées du réseau d'accès flux par flux, un certain nombres d'organe concrets de prise en charge sont définis et utilisés pour la gestion de ces ressources. Deux d'entre eux sont:

– les codages de flux de service: les paramètres codés de type-longueur-valeur (TLV) utilisés pour définir les paramètres de qualité de service associés à un flux de service;
– le classeur: les paramètres codés de type-longueur-valeur (TLV) du protocole IP, d'Ethernet et de IEEE802.1p/q utilisés pour définir et limiter le domaine d'application d'un flux en termes de points d'extrémité d'origine et de terminaison.

Alors que l'Annexe B de la Rec. UIT-T J.112 accepte les modèles de qualité de service approvisionnés (c'est-à-dire, des flux de service statiques, à longue durée de vie qui sont établis pendant le processus d'enregistrement du câblo-modem) et dynamiques (c'est-à-dire, des flux de service transitoires qui sont ajoutés, modifiés et supprimés en tant que de besoin), le cadre multimédia d'IPCablecom est principalement concerné par le modèle dynamique car il permet une gestion optimale des ressources réseau par un multiplexage statistique conforme à la demande des prescriptions de service.

La gestion de flux de service est effectuée au moyen de l'échange de messages Ajout/Changement/Suppression (DSA/DSC/DSD) de service dynamique DOCSIS de couche MAC, qui peut être lancé soit par le câblo-modem, soit par le système CMTS. Les transactions DSA et DSC prennent la forme d'un échange à trois dans lequel une demande (REQ) est suivie d'une réponse (RSP) qui reçoit un accusé de réception (ACK). Les messages DSD sont de simples échanges à deux. Un attribut spécifique appelé Code de confirmation est fourni dans chaque message de réponse DSx et indique le succès ou l'échec d'une transaction.

Un point important à noter lorsque qu'on passe en revue les capacités de qualité de service fournies par l'Annexe B de la Rec. UIT-T J.112 est que les flux de service amont et aval reçoivent un traitement fondamentalement différent au système CMTS. C'est le résultat du fait que les canaux RF amont sont des média conflictuels, en accès partagé, qui prennent la forme topologique d'une relation multi-univoque entre des câblo-modems multiples et un système CMTS unique. A l'inverse, le canal RF aval se comporte beaucoup plus comme un routeur IP traditionnel dans lequel arrivent des paquets (du réseau d'accès ou des circuits du cœur de réseau) qui sont mis en file d'attente et puis sont transmis à une où plusieurs destinations. Par conséquent, des mécanismes de qualité de service distincts sont appliqués selon qu'un flux de service unidirectionnel particulier est orienté dans le sens aval ou dans le sens amont.

Les flux de service amont peuvent être définis par un des cinq types de programmation de flux de service suivants:

– au mieux: c'est une stratégie standard de gestion de ressources fondée sur la concurrence, dans laquelle les opportunités de transmission sont allouées sur la base du premier entré, premier servi, quoique sous la coordination du programmeur du système CMTS. Ce type de programmation peut être complété par des caractéristiques de qualité de service dans lesquelles, par exemple, des limites de débit maximal sont appliquées à un flux de service particulier;
– interrogation en temps différé: c'est une stratégie de gestion de ressources fondée sur la réservation dans laquelle un câblo-modem particulier est interrogé à intervalle fixe pour déterminer si des données ont été mises en file d'attente pour être transmises sur un flux de service particulier, et si c'est le cas, le programmeur va allouer une opportunité de transmission pour ce flux de service;
– interrogation en temps réel: elle est analogue au type de programmation par interrogation en temps différé, excepté que l'intervalle fixe d'interrogation est normalement très court (<500 ms). Les types de programmation d'interrogation conviennent parfaitement pour le trafic à débit binaire variable qui a des exigences de débit et de latence inflexibles;
– allocation non sollicitée: c'est une stratégie de gestion de ressources fondée sur la réservation dans laquelle une allocation de taille fixe est fournie à un flux de service particulier à intervalles fixes (ou presque) sans interrogation ou interaction supplémentaire. Ce type de programmation convient parfaitement pour le trafic à débit constant et élimine la plus grande partie des redondances de protocole associées aux types d'interrogations;
– allocation non sollicitée avec détection d'activité vocale: c'est une stratégie de gestion de ressources fondée sur la réservation qui représente un hybride entre les types de programmation par interrogation et l'allocation non sollicitée, dans laquelle des allocations fixes sont fournies à des intervalles (presque) fixes tant que des données sont dans la file

d'attente pour être transmises. Durant les périodes d'inactivité, ce type de programmation revient au mode par interrogation de façon à préserver la bande passante non utilisée.

Ces types de programmation ayant chacun une nature unique et des caractéristiques spécialisées, des paramètres spécifiques de qualité de service leur sont associés individuellement. Ces paramètres sont précisés de façon détaillée dans le paragraphe qui suit.

Les flux de service aval sont définis en utilisant le même ensemble de paramètres de qualité de service qui sont associés au type de programmation au mieux pour le sens amont.

Indépendamment de l'orientation du flux ou du type particulier de programmation demandé, tous les flux de service dynamiques passent par trois états logiques, résumés ci-dessous. Alors que certains scénarios de signalisation optimisés permettent ce qu'on appelle une opération d'engagement "en une seule phase", la demande passe toujours par les trois phases logiques lorsqu'elle est traitée par le système CMTS.

– Autorisée: les demandes sont authentifiées et les règles de politique du réseau sont appliquées, ce qui donne une enveloppe d'autorisation qui forme la frontière avec les demandes de réservation suivantes.
– Admise (ou Réservée): un flux de service inactif est construit et des ressources sont réservées par le programmeur de sorte que les demandes d'activation subséquentes sont assurées du succès ; les ressources réservées peuvent être utilisées par du trafic au mieux (provenant du même câblo-modem ou de câblo-modems différents) jusqu'à l'engagement des ressources.
– Actif (ou Engagé): le flux de service est activé, ainsi que les classeurs correspondants ; les paquets de qualité de service améliorée sont maintenant en mesure de traverser le flux.

NOTE – Au sens propre, DOCSIS ne définit pas des "états", mais plutôt des, "attributs" de flux de service qui sont complètement remplacés dans chaque transaction DSC. Les états décrits ici sont une construction logique utilisée dans un modèle conceptuel qui décrit le processus de gestion de ressources effectué au CMTS. La Recommandation sur l'interface RFI DOCSIS normalise les termes "admis" et "actif" en définissant les attributs d'un flux de service, alors qu'IPCablecom a adopté les termes équivalents de "réservé" et "engagé" dans la caractérisation des états des portes.

Alors que DOCSIS ne définit pas une procédure d'autorisation spécifique à appliquer aux messages DSx, il fournit un protocole de prise en charge au moyen d'une facilité appelée Bloc d'autorisation pour les schémas d'autorisation spécifiques des services. Toute accréditation ou jeton d'autorisation qui est présenté via le Bloc d'autorisation est transmis à un module d'autorisation approprié avant le traitement de la demande DSx dans le système CMTS. IPCablecom fait un très large usage du mécanisme d'autorisation décrit ci-dessous.

5.1.2 Résumé de la qualité de service IPCablecom-T

Alors que la Recommandation RFI de l'Annexe B de la Rec. UIT-T J.112 définit les mécanismes fondamentaux qui forment le cœur du modèle de DQOS d'IPCablecom, la Recommandation IPCablecom sur la DQoS [9] augmente ces capacités avec un cadre de gestion de politique fondé sur COPS. Tout comme le flux de service représente le concept fondamental dans le modèle de qualité de service de l'Annexe B de la Recommandation UIT-T J.112, la porte joue un rôle tout à fait aussi significatif dans le schéma de DQoS d'IPCablecom. Une porte définit une enveloppe d'autorisation de ressources consistant en paramètres de qualité de service de niveau IP ainsi que de classeurs qui définissent le domaine d'application des flux de service qui peuvent être établis à l'égard de la porte. Conformément aux mécanismes d'autorisation de l'Annexe B de la Rec. UIT-T J.112 décrits ci-dessus, seules les demandes DSx qui sont conformes, paramètre par paramètre, à la relation générale suivante seront accordées:

$$\text{Enveloppe autorisée} \geq \text{Enveloppe réservée} \geq \text{Enveloppe engagée}$$

Sur la base de son modèle de gestion de politique, IPCablecom-T définit un schéma de préautorisation dans lequel les ressources réseau sont autorisées à l'avance de l'échange de messages DSx qui demande l'établissement d'un flux de service correspondant. Par conséquent, l'interface COPS utilisé pour installer et gérer les portes correspond plus étroitement au modèle COPS-PR définit dans le document RFC 3084 [19] qu'au schéma standard COPS spécifié dans le document RFC 2748 [7]. Aussi, dans le but d'installer et gérer ces portes, la Recommandation sur la DQoS d'IPCablecom définit un ensemble d'objets COPS spécifiques du client qui constituent les primitives de l'interface de signalisation de la commande de porte entre le serveur CMS et le système CMTS.

Spécifiquement, le serveur CMS peut être décomposé logiquement en un agent d'appel, responsable de la maintenance de l'état d'appel de téléphonie, et un contrôleur de porte, qui reçoit les demandes d'autorisation de l'agent d'appel (via une interface interne) et installe les décisions de politique sous la forme de portes sur le système CMTS. Dans le modèle multimédia d'IPCablecom, cette décomposition est formalisée au moyen de deux éléments de réseau séparés, le Serveur de politique (analogue au contrôleur de porte d'IPCablecom-T) et le Gestionnaire d'application (qui définit les fonctionnalités spécifiques du service comme le fait l'agent d'appel dans le modèle IPCablecom-T).

A titre d'illustration de ce modèle d'autorisation et de l'utilisation de l'interface de contrôleur de porte au système CMTS, un flux d'appel IPCablecom-T normal sur réseau à zone unique (c'est-à-dire, utilisant un seul serveur CMS) se déroule comme suit (certaines de ces étapes se dérouleraient normalement en parallèle):

- l'E-MTA$_o$ s'amorce, s'approvisionne et s'enregistre avec le serveur CMS;
- le serveur CMS envoie les demandes à l'E-MTA$_o$ pour notifier l'événement de décrochage et les numéros composés;
- l'E-MTA$_t$ s'amorce, s'approvisionne et s'enregistre avec le serveur CMS;
- le serveur CMS envoie les demandes à l'E-MTA$_t$ pour notifier l'événement de décrochage et les numéros composés;
- l'E-MTA$_o$ décroche, le notifie au serveur CMS et fournit les numéros composés;
- le serveur CMS envoie une demande à l'E-MTA$_o$ pour créer une nouvelle connexion logique et extraire le SDP$_{o;}$
- le serveur CMS envoie une demande à l'E-MTA$_t$ pour créer une nouvelle connexion logique et extraire le SDP$_{t;}$
- le serveur CMS installe une porte au CMTS$_o$ et extrait le jeton d'ID de porte$_o$ correspondant;
- le serveur CMS installe une porte au CMTS$_t$ et extrait le jeton d'ID de porte$_t$ correspondant;
- le serveur CMS envoie une demande (avec l'ID de porte$_o$) à l'E-MTA$_o$ pour réserver des ressources et joue la tonalité de retour d'appel;
- l'E-MTA$_o$ envoie une DSA-REQ au CMTS$_o$ pour établir les flux de service et réserver les ressources;
- le serveur CMS envoie une demande (avec l'ID de porte$_t$) à l'E-MTA$_t$ pour réserver des ressources et joue une tonalité d'alarme;
- l'E-MTA$_t$ envoie une DSA-REQ au CMTS$_t$ pour établir les flux de service et réserver les ressources;
- l'E-MTA$_t$ décroche et le notifie au serveur CMS;
- le serveur CMS envoie une demande à l'E-MTA$_o$ pour arrêter la tonalité de retour d'appel, engager les ressources et passe par le conduit de média;
- l'E-MTA$_o$ envoie une demande DSC-REQ au CMTS$_o$ pour engager les ressources;

- le serveur CMS envoie une demande à l'E-MTA$_t$ pour engager les ressources et passe par le conduit de média;
- l'E-MTA$_t$ envoie une demande DSC-REQ au CMTS$_t$ pour engager les ressources;
- l'appel suit son cours.

A la différence du modèle IPCablecom dans lequel l'appareil client (c'est-à-dire, l'E-MTA) lance la réservation de ressource et les procédures d'activation, le modèle de gestion de ressources d'IPCablecom multimédia permet la délégation de ces étapes au nom du point d'extrémité au moyen d'une interface de commande de porte améliorée.

Ceci conclut ce bref résumé des fondements de l'Annexe B de la Rec. UIT-T J.112 et de la qualité de service IPCablecom. Pour des précisions sur ces sujets complexes, se reporter aux textes de base respectifs des références [1] et [9]. Le paragraphe 5.2 donne un aperçu général résumé de l'architecture d'IPCablecom multimédia comprenant chacun des éléments primaires de réseau et les interfaces qui leur sont associées pour préparer l'examen de la Recommandation de protocole technique qui suit.

5.2 Architecture

L'Appendice I décrit le cadre architectural et le modèle de référence pour IPCablecom multimédia. La présente Recommandation applique le modèle contenu dans le cadre architectural et y ajoute des prescriptions normatives pour fournir une solution mesurable et interopérable qui convienne pour le développement des service d'IPCablecom multimédia.

5.2.1 Types de Client

Le rapport technique d'IPCablecom multimédia définit trois sortes de type de client:

- le client de type 1 représente les points d'extrémité ordinaires existants (par exemple, des applications pour micro-ordinateur, des consoles de jeu) qui ne possèdent pas de capacités de qualité de service spécifiques ou de capacités de signalisation. Ce client ne sait rien des câblo-modems, d'IPCable2Home, ou de l'échange de messages IPCablecom, et par conséquent, on ne peut rien exiger de sa part pour ce qui les concerne. Le client de type 1 communique avec un gestionnaire d'application pour ses demandes de service, et ne demande pas directement (il ne peut pas) de ressources de qualité de service à l'opérateur du réseau d'accès par câble;
- le client de type 2 est semblable à un adaptateur MTA de téléphonie d'IPCablecom-T en ce qu'il prend en charge la signalisation de qualité de service fondée sur la Recommandation sur la qualité de service dynamique d'IPCablecom;
- le client de type 3 demande directement le traitement de qualité de service au réseau d'accès, sans interaction avec un gestionnaire d'application. Ce client connaît le protocole RSVP fondé sur les normes de l'IETF et utilise ce protocole pour demander directement au système CMTS les ressources de qualité de service du réseau d'accès.

Dans la version actuelle de la présente Recommandation, la prise en charge est limitée au client de type 1. Par conséquent, la version actuelle de la présente Recommandation ne prend en charge que le scénario 1, le scénario "Qualité de service mandatée poussée par la politique", décrit à l'Appendice I. D'après ce scénario, le gestionnaire d'application est responsable de la demande de ressources de qualité de service au nom du client, et un serveur de politique fait avancer la demande jusqu'au système CMTS, qui est le dispositif réellement responsable de l'établissement et de la gestion des flux de service DOCSIS réclamés par l'application.

5.2.2 Dispositifs d'IPCablecom multimédia

En plus du client (qui est normalement situé dans les locaux de l'abonné), IPCablecom multimédia requiert que plusieurs éléments de réseau résident dans le réseau du câblo-opérateur ou soient

accessibles et accrédités par son intermédiaire. Tout au long de la présente Recommandation, nous faisons de larges emprunts à la terminologie et aux concepts standard de l'IETF pour décrire ces éléments de réseau. Se reporter à l'Appendice I pour une description plus précise de l'architecture d'ensemble d'IPCablecom Multimédia qui comporte aussi un développement sur les exigences et les objectifs qui la sous-tendent.

Comme COPS [7] et COPS-PR [19] utilisent chacun les termes Point d'application de politique (PEP, *policy enforcement point*) et Point de décision de politique (PDP, *policy decision point*) dans des scénarios d'interaction substantiellement différents et comme IPCablecom Multimédia ajoute de nouvelles nuances à ces concepts (en particulier dans la définition du Serveur de politique), penser uniquement en termes de PEP et PDP peut occasionnellement créer une confusion lorsqu'il s'agit de comprendre les responsabilités respectives des différents composants de l'architecture d'IPCablecom Multimédia. Pour essayer de dissiper cette confusion, certaines parties de la présente Recommandation emploient les notions de Domaine de commande de service et de Domaine de commande de ressource pour faire la distinction entre les types de politique qui sont définis et appliqués.

Domaine de commande de ressource (RCD, *resource control domain*) peut se définir comme un regroupement logique d'éléments qui procurent la connectivité et la gestion de politique au niveau des ressources réseau tout au long des conduits de transmission des paquets de et vers l'hôte d'extrémité. Le domaine RCD consiste en entités de système CMTS et de Serveur de politique dont les responsabilités incluent la gestion des ressources tout au long des conduits de transmission des paquets.

Le Domaine de commande de service (SCD, *service control domain*) se définit comme un regroupement logique d'éléments qui offrent des applications et du contenu aux abonnés au service. Le gestionnaire d'application réside dans le domaine SCD. Noter qu'il peut y avoir un ou plusieurs domaines SCD qui se rapportent à un seul domaine RCD. Réciproquement, chaque domaine RCD peut interagir avec un ou plusieurs SCD.

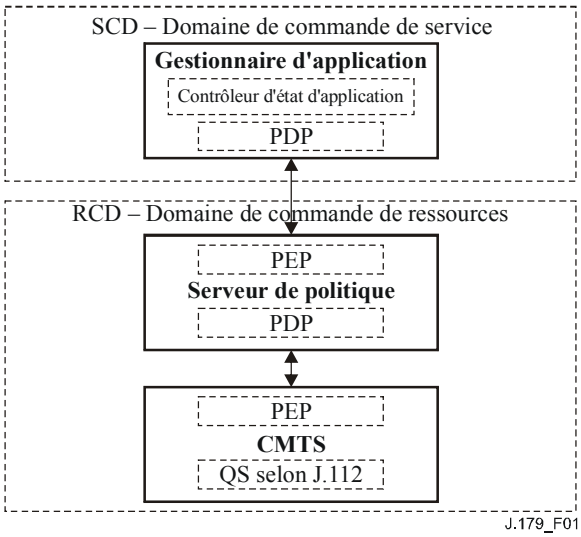

Figure 1/J.179 – Domaines de commande de session et ressource

Dans l'architecture d'IPCablecom multimédia le rôle fondamental du gestionnaire d'application est de maintenir un état de niveau de session de l'application et d'appliquer les politiques du Domaine de commande de service (SCD) aux demandes de session commandées par le client. Si les demandes de session du client satisfont aux vérifications de politique de domaine SCD du gestionnaire d'application, celui-ci convertit la demande de session en demande de ressource et la passe au Serveur de politique pour les vérifications de politique du Domaine de commande de

ressource (RCD). Si la demande de ressource échoue à la vérification de politique du domaine RCD, le Serveur de politique rejette la demande de ressource et par conséquent le gestionnaire d'application rejette la demande de session du client. Si, cependant, la demande de ressource passe les vérifications du domaine RCD du Serveur de politique, celui-ci transmet la demande au système CMTS pour les contrôles d'admission de niveau réseau.

Les rôles fondamentaux des divers composants d'IPCablecom multimédia sont:

- le Gestionnaire d'application est responsable de l'état du niveau d'application ou de session et de l'application de la politique du domaine SCD;
- le Serveur de politique est responsable de l'application de la politique du domaine RCD et de la gestion des relations entre les gestionnaires d'application et les systèmes CMTS;
- le système CMTS est chargé d'effectuer les contrôles d'admission et de gérer les ressources réseau à travers les flux de service DOCSIS.

Il peut être utile ici de clarifier notre utilisation des termes "contrôle d'admission" et "autorisation de politique." Pour les besoins de la présente Recommandation, contrôle d'admission se comprend généralement comme le processus de gestion d'un ensemble fini de ressources de niveau réseau (par exemple, la bande passante du réseau d'accès, les mini-intervalles de programmation DOCSIS, ou les ressources du système CMTS pour prendre en charge les portes et les temporisateurs, etc.) et d'admission des demandes concernant cet ensemble. Pour des raisons de performances le contrôle d'admission est habituellement effectué directement sur les éléments de réseau qui gèrent le conduit de transmission de paquets (comme le système CMTS), bien que certaines implémentations sophistiquées de Serveur de politique puissent choisir de faire la maintenance des états associés aux ressources du réseau, et donc complètent le processus de contrôle d'admission et y participent.

A l'inverse, l'autorisation de politique est utilisée pour décrire des politiques d'utilisation agrégée de plus haut niveau (par exemple, le nombre d'autorisations concurrentes pour un abonné ou service particulier) qui constituent la stratégie de gestion de réseau d'un câblo-opérateur. L'autorisation de politique est presque toujours définie et appliquée au Serveur de politique.

Le reste du présent paragraphe décrit plus en détail chacun de ces composants architecturaux et leurs interfaces associées.

5.2.2.1 Gestionnaire d'application (AM)

Ainsi qu'il est noté dans le résumé ci-dessus, le gestionnaire d'application (AM, *application manager*) est une entité du réseau qui définit les politiques du domaine SCD, coordonne les demandes lancées par l'abonné pour des sessions d'applications avec accès aux ressources nécessaires pour satisfaire ces demandes, et maintient l'état du niveau d'application.

Le gestionnaire d'application peut résider sur le réseau du câblo-opérateur ou bien il peut résider en dehors de ce domaine et interagir avec le réseau du câblo-opérateur via une relation de confiance particulière (normalement définie et appliquée sur la base d'un accord de niveau de service). De même, le gestionnaire d'application peut être sous le contrôle direct de l'opérateur, ou bien il peut être contrôlé par une tierce partie. Tout gestionnaire d'application donné peut communiquer avec un ou plusieurs Serveurs de politique sur le réseau de l'opérateur ; un ou plusieurs gestionnaires d'application peuvent aussi communiquer avec tout Serveur de politique donné sur le réseau de l'opérateur (dans la mesure où existe une relation de confiance appropriée).

Dans les scénarios de développement de service les plus futuristes, le gestionnaire d'application communiquera avec un client via un protocole de signalisation qui est en dehors du domaine d'application de la présente Recommandation. Utilisant ce protocole non spécifié, le gestionnaire d'application authentifie et autorise les demandes de client sur la base des politiques du Domaine de commande de service. Pour les demandes de client qui réussissent aux examens, le gestionnaire d'application détermine les paramètres de qualité de service particuliers qui sont nécessaires pour fournir le service au client, sur la base de sa connaissance du service demandé. Il envoie alors une

demande pour ces ressources au Serveur de politique approprié, qui peut refuser la demande sur la base de la politique du réseau ou du domaine RCD ou peut passer la demande au système CMTS pour le contrôle d'admission et l'application.

5.2.2.2 Serveur de politique (PS)

Ainsi qu'exposé dans le document RFC 2753 [18], le cadre de gestion de la politique qui sous-tend d'IPCablecom multimédia est fondé sur les travaux du groupe de travail Protocole d'allocation de ressources (RAP, *Resource Allocation Protocol*) de l'IETF. Comme le Serveur de politique est situé entre le gestionnaire d'application et le système CMTS, il joue simultanément le double rôle de "mandataire" pour les demandes de session lancées par le gestionnaire d'application et de "sentinelle" pour la définition et la mise en application de la politique du Domaine de commande de ressources.

Ainsi qu'il est décrit dans [18] et en s'en tenant au modèle de qualité de service dynamique d'IPCablecom-T, le Serveur de politique sert de Point de décision de politique (PDP) en relation avec le système CMTS en ce que le Serveur de politique met en œuvre les procédures d'autorisation et de gestion de ressources définies par le câblo-opérateur. Réciproquement, le Serveur de politique assume le rôle de Point d'application de politique (PEP) en relation avec le gestionnaire d'application qui sert de mandataire pour les messages de commande de porte de et vers l'élément CMTS.

Pour modifier le scénario d'interaction, le gestionnaire d'application envoie des demandes de politique au Serveur de politique. Le Serveur de politique agit comme "sentinelle" pour ces demandes, et applique un ensemble de règles de politique qui ont été préapprovisionnées par le câblo-opérateur. Lors du passage des examens, le Serveur de politique agit alors comme "mandataire" par rapport au gestionnaire d'application et au système CMTS, transmettant la demande de politique et renvoyant toute réponse qui lui serait associée. Chaque transaction de demande de politique doit être traitée individuellement.

Les décisions de politique peuvent se fonder sur un certain nombre de facteurs, tels que:

- des paramètres associés à la demande et à l'état des ressources disponibles;
- l'identité du client particulier et les informations de profil qui y sont associées;
- des paramètres d'application;
- des considérations de sécurité;
- l'heure du jour.

Les fonctions de base du Serveur de politique comprennent:

- un mécanisme de demande de décision de politique, invoqué par les gestionnaires d'application;
- un mécanisme de "régulation" de demande de décision de politique, appliquant les règles de politique installées;
- un mécanisme de fourniture de décision de politique, utilisé pour installer les décisions de politique au système CMTS;
- un mécanisme permettant de mandater le système CMTS pour les messages de gestion de qualité de service pour le compte du gestionnaire d'application;
- une interface d'enregistrement des événements avec un Serveur d'archivage qui est utilisé pour conserver les demandes de politique, qui peuvent alors être corrélées avec les enregistrements d'utilisation des ressources réseau.

Comme le Serveur de politique fonctionne comme mandataire entre les éléments gestionnaire d'application et système CMTS (avec des interfaces client et serveur complémentaires) certains câblo-opérateurs peuvent choisir de développer plusieurs couches de Serveurs de politique et de

déléguer certaines décisions de politique parmi ces serveurs afin de satisfaire aux exigences associées à l'échelonnement et à la tolérance aux fautes.

5.2.2.2.1 Serveurs de politique à états et sans état

Il y a deux classe de base de serveurs de politique – à état et sans état. Un Serveur de politique sans état est un peu un abus de langage dans la mesure où il conserve assez d'état pour translater les demandes du gestionnaire d'application au système CMTS approprié et pour maintenir l'état de session COPS, alors qu'un vrai Serveur de politique sans état ne maintient aucun état sur une quelconque de session de média. Les Serveurs de politique à états sont de plusieurs sortes, certains participent au contrôle d'admission et donc surveillent les attributs de qualité de service des sessions de média actives, certains laissent le contrôle de qualité de service et d'admission au système CMTS mais surveillent les demandes de service fondées sur le temps ou le volume qui viennent du gestionnaire d'application, et certains Serveurs de politique se situent entre ces deux extrêmes.

La raison pour laquelle il y a différents types de Serveurs de politique est dans la diversité des environnements que les opérateurs essayent de prendre en charge. Par exemple, certains opérateurs peuvent souhaiter prendre en charge IPCablecom multimédia sur les mêmes systèmes CMTS qu'ils utilisent pour la téléphonie IPCablecom, et ils peuvent vouloir un serveur CMS/serveur de politique unique qui ait une vue plus globale des ressources réseau utilisées. D'un autre côté, certains opérateurs peuvent souhaiter travailler dans un environnement IPCablecom Multimédia uniquement, ou bien ils peuvent utiliser des mécanismes plus simples dirigés par le système CMTS pour séparer les ressources d'IPCablecom multimédia et de la téléphonie. Ces configurations plus simples ont des exigences plus modestes quant à la quantité d'états qu'un serveur de politique doit maintenir.

Les exigences d'état du Serveur de politique peuvent aussi être menées par le niveau de confiance entre le Serveur de politique et le gestionnaire d'application ; un Serveur de politique à états peut mieux réguler le comportement de contrôle de session du gestionnaire d'application que ne le peut un Serveur de politique sans état. Ainsi un Serveur de politique à états peut être mieux approprié pour les opérateurs qui acceptent les gestionnaires d'application tiers. Les autres opérateurs peuvent s'appuyer sur des considérations économiques pour mettre en application leurs relations de confiance avec les gestionnaires d'application, ou bien ils peuvent contrôler eux-même les gestionnaires d'application. Dans ces cas, un Serveur de politique sans état peut être plus approprié.

Comme il est impossible de classifier tous les multiples composants de session de média et d'état de qualité de service réseau qu'entretient un Serveur de politique, le protocole est conçu de façon à être indépendant de cette complexité. Un Serveur de politique à états glane des informations de session de média IPCablecom multimédia auprès des demandes du gestionnaire d'application dont il est le mandataire ; toutes les autres informations dont il a besoin sont rassemblées via des mécanismes qui sont en dehors du domaine d'application de la présente Recommandation. Le système CMTS et le gestionnaire d'application ne font pas de distinction quant au type de Serveur de politique auquel ils sont connectés, et le protocole est conçu d'une manière telle que le type de Serveur de politique soit transparent pour le point d'extrémité. Le type de Serveur de politique n'a d'importance que pour l'opérateur.

Dans la mesure où certains types de Serveurs de politique essayent d'aider au contrôle d'admission et peuvent avoir une vue plus large du réseau et de ses ressources, des questions supplémentaires de synchronisation d'état peuvent surgir dans la conception d'un réseau qui contient plus d'un de ces types de Serveur de politique. Il appartient à l'opérateur de s'assurer que les efforts de ces Serveurs de politique ne sont pas sapés par un réseau qui comporterait d'autres Serveurs de politique autonomes.

5.2.2.3 Système de terminaison de câblo-modem (CMTS)

Lorsqu'on décrit le rôle de l'élément de réseau CMTS, il est important de prendre en compte la relation entre les fonctionnalités de câblo-modem, d'IPCablecom-T et d'IPCablecom multimédia.

Alors que chaque ensemble de Recommandations vise un ensemble spécifique d'exigences fonctionnelles, chacune a aussi été définie de telle sorte que les implémentations correspondantes puissent être construites de façon modulaire ; le contrôle de porte d'IPCablecom-T ou d'IPCablecom multimédia peut être mis en couches sur la base du système CMTS de l'Annexe B de la Rec. UIT-T J.112, avec la faculté d'ajouter des fonctionnalités supplémentaires ou complémentaires en tant que de besoin. De plus, on doit souligner un acquis important de l'architecture IPCablecom, qui est qu'aussi bien la variante de téléphonie que le multimédia présentent des similarités considérables, amenant à des réutilisations potentielles dans les modèles de gestion de porte sous-jacents.

Le système CMTS d'IPCablecom multimédia est une version généralisée du système CMTS d'IPCablecom-T qui a été défini pour fournir des services de téléphonie dans les réseaux IPCablecom-T. Le système CMTS est chargé de satisfaire les demandes de qualité de service qui sont reçues d'un ou plusieurs Serveurs de politique. Il exécute cette fonction en installant des portes, qui sont semblables aux portes définies dans [9] ; les portes permettent au câblo-modem de l'abonné de demander des ressources réseau au CMTS par la création de flux de qualité de service dynamique DOCSIS avec des niveaux garantis de qualitéde service. Le CMTS envoie aussi des messages d'événement détaillant l'utilisation réelle des ressources de qualité de service au Serveur d'archivage.

5.2.2.4 Serveur d'archivage (RKS)

Le Serveur d'archivage (RKS, *record keeping server*) d'IPCablecom multimédia accomplit un rôle semblable à celui du RKS dans IPCablecom-T [10]. Il reçoit du système CMTS des messages d'événement relevant des décisions de politique du Serveur de politique et des messages d'événement relevant de l'utilisation des ressources de qualité de service.

Dans l'architecture IPCablecom multimédia, le Serveur d'archivage ne reçoit pas directement de messages du gestionnaire d'application. Cependant, le gestionnaire d'application peut incorporer des données opaques dans les messages qu'il envoie au Serveur de politique, et ces données peuvent alors être incluses dans les messages d'événement qui sont ensuite envoyés au Serveur d'archivage.

5.2.3 Interfaces d'IPCablecom multimédia

IPCablecom Multimédia est construit à partir de l'ensemble des Recommandations pour IPCablecom-T. Lorsqu'une interface d'IPCablecom multimédia a un équivalent dans IPCablecom-T, IPCablecom multimédia utilise le même protocole, ou une extension du même protocole.

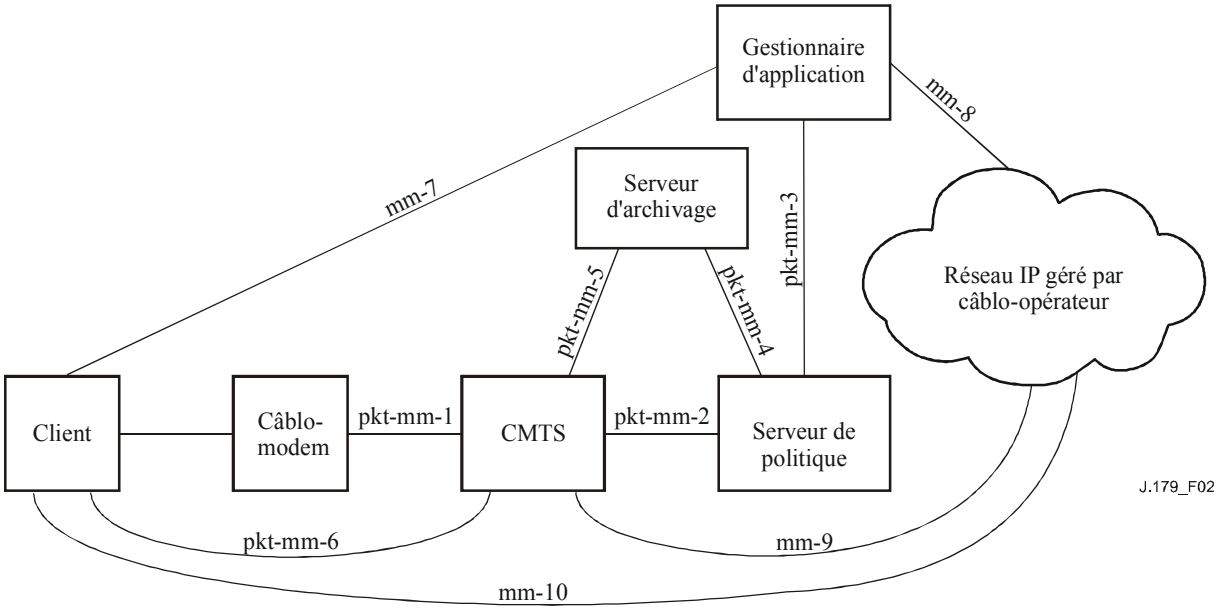

Figure 2/J.179 – Cadre architectural d'IPCablecom multimédia

Tableau 1/J.179 – Interfaces d'IPCablecom multimédia

Interface	Description	Notes
pkt-mm-1	CMTS – CM	Le câblo-modem (CM) peut demander de la QS au CMTS via la signalisation DSx de l'Annexe B de la Rec. UIT-T J.112. Autrement, le CMTS peut ordonner au CM d'établir, supprimer ou changer un flux de service DOCSIS pour satisfaire une demande de QS, toujours via la signalisation DSx.
pkt-mm-2	PS – CMTS	Cette interface est fondamentale pour le cadre de gestion de politique. Elle contrôle les décisions de politique, qui peuvent être: a) poussées par le Serveur de politique (PS) vers le CMTS; b) tirées du PS par le CMTS. L'interface permet aussi des demandes de QS mandatées au nom d'un client. Dans certains scénarios, cette interface peut aussi être utilisée pour informer le PS lorsque des ressources de QS deviennent inactives.
pkt-mm-3	AM – PS	Le gestionnaire d'application (AM) peut demander que le PS installe une décision de politique sur le CMTS au nom du client. Cette interface peut aussi être utilisée pour informer l'AM de changements dans l'état des ressources de QS.
pkt-mm-4	PS – RKS	Le PS envoie des messages d'événement au Serveur d'archivage (RKS) pour garder trace des décisions de politique qui se rapportent à la qualité de service.
pkt-mm-5	CMTS – RKS	Le CMTS envoie au RKS les messages d'événement pour garder trace des demandes de QS et d'utilisation de QS (par exemple, ajouts, changements et suppressions de flux de service, et mesures de volume).
pkt-mm-6	Client – CMTS	Le client peut utiliser cette interface pour demander et gérer directement les ressources de QS du réseau. S'il y est autorisé, ces ressources sont fournies par le CMTS.
mm-7	Client – AM	Cette interface peut être utilisée par le client pour interagir avec l'AM et pour demander et gérer indirectement les ressources de QS. Cette interface est en dehors du domaine d'application de la présente Recommandation.
mm-8	AM – homologue	L'AM peut utiliser cette interface pour interagir avec quelque autre entité faisant partie de l'application en question. Cette interface est en dehors du domaine d'application de la présente Recommandation.
mm-9	CMTS – réseau IP géré par le câblo-opérateur	Cette interface sur le CMTS peut être utilisée pour prendre en charge les demandes de QS de bout en bout au delà du réseau d'accès. Cette interface est en dehors du domaine d'application de la présente Recommandation.
mm-10	Client – homologue	Le Client peut utiliser cette interface pour interagir avec quelque autre entité qui appartient à l'application en question. Cette interface est en dehors du domaine d'application de la présente Recommandation.

5.2.3.1 Interface entre Client et Gestionnaire d'application (mm-7)

L'interface entre le client et le gestionnaire d'application est en dehors du domaine d'application de la présente Recommandation. Normalement, le gestionnaire d'application va, à l'aide de moyens qui sortent du domaine d'application de la présente Recommandation, authentifier le client et s'assurer que le client a bien droit au service multimédia. Par exemple, le client peut se connecter à une page Web et demander le service en fournissant un nom d'utilisateur et un mot de passe. Quelle que soit la façon dont ceci est accompli, le gestionnaire d'application doit être capable d'identifier de façon non ambiguë le ou les câblo-modems auxquels le service doit être fourni, dans la mesure où ces informations doivent être disponibles pour l'opérateur du réseau avant que la qualité de service ne puisse être fournie.

5.2.3.2 Interface entre gestionnaire d'application et Serveur de politique (pkt-mm-3)

Cette interface correspond à l'interface d'IPCablecom-T entre un Agent d'appel et un contrôleur de porte. Dans IPCablecom-T, c'est une interface cachée, non testable, et il n'y a donc pas d'exigences de protocole a priori sur cette interface.

IPCablecom multimédia requiert l'utilisation de COPS [7] à cette interface. Afin de simplifier l'architecture et pour permettre plusieurs niveaux d'éléments de Serveur de politique entre le gestionnaire d'application et le système CMTS, cette interface reflète autant que possible l'interface entre le Serveur de politique et le CMTS. Bien que le gestionnaire d'application soit celui qui demande l'autorisation des ressources au Serveur de politique, il génère réellement cette demande dans un message de Décision COPS, au lieu d'un message de Demande COPS. Ceci permet à l'interface entre le gestionnaire d'application et le Serveur de politique d'apparaître identique à l'interface entre le Serveur de politique et le système CMTS. Le gestionnaire d'application est le point PDP qui se rapporte au Serveur de politique, et le Serveur de politique est le point PEP qui se rapporte au gestionnaire d'application.

Lorsqu'un gestionnaire d'application accepte de fournir le service à un client, il envoie une Décision COPS qui contient (au moins) les informations suivantes sous forme d'objets COPS:

- identité du gestionnaire d'application qui fait la demande;
- identité du ou des clients à qui le service doit être fourni;
- le ou les Spec de flux RSVP spécifiant la ou les enveloppes de trafic pour la session.

Dans la réponse du Serveur de politique, le serveur inclut un jeton d'autorisation, l'ID de porte, qui lui est fourni par le système CMTS.

5.2.3.3 Interface entre le Serveur de politique et le système CMTS (pkt-mm-2)

Cette interface est essentiellement identique à l'interface équivalente (entre CMTS et contrôleur de porte) d'IPCablecom-T. Comme dans IPCablecom-T, COPS est utilisé pour transférer les informations de politique entre le Serveur de politique et le CMTS. Le système CMTS agit comme un point PEP de COPS et le Serveur de politique agit comme un point PDP de COPS. Suivant le modèle IPCablecom-T, le Serveur de politique lance la communication pour une session multimédia en envoyant un message de DQoS Porte établie (qui est un message DECISION COPS non sollicité) au CMTS.

Ce message contient (au moins):

- l'Identifiant du gestionnaire d'application;
- l'Identifiant d'abonné;
- la Spec de porte;
- le ou les Spec de flux;
- le classeur.

Le système CMTS répond, comme en DQos avec Acc de porte établie ou avec Erreur de porte établie (qui sont tous deux des messages REPORT COPS).

Si le CMTS répond favorablement (c'est-à-dire, avec un Acc de porte établie), il inclut un ID de porte. Comme dans IPCablecom-T, l'ID de porte agit comme un jeton d'autorisation. A la différence d'IPCablecom-T, le jeton n'est pas ensuite passé au client (dans la mesure où les points d'extrémité de Client de Type 1 n'ont pas de connaissance d'IPCablecom) ; au lieu de cela, il est détenu par le Serveur de politique (s'il est à états) et par le gestionnaire d'application, permettant ainsi de produire des commandes se rapportant à la session au CMTS, soit directement dans le cas du Serveur de politique, soit indirectement via le Serveur de politique dans le cas du gestionnaire d'application.

5.2.3.4 Interface Serveur d'archivage et Serveur de politique (pkt-mm-4) et Serveur d'archivage et CMTS (pkt-mm-5)

Les interfaces au Serveur d'archivage avec le Serveur de politique et le CMTS sont identiques aux interfaces équivalentes (respectivement avec le serveur CMS et le CMTS) dans IPCablecom-T (voir [10]). Ces interfaces sont utilisées pour transporter les messages d'événement IPCablecom, qui utilisent le formatage RADIUS. Dans IPCablecom multimédia, les messages d'événement portent des informations détaillées se rapportant au service fourni, y compris l'heure exacte de création et de suppression des flux de service et (facultativement) la quantité de trafic qui est passée sur le flux de service durant son existence.

5.2.4 Informations d'état

Le présent paragraphe donne un aperçu général de la localisation d'état dans le système d'IPCablecom multimédia. En plus de la maintenance d'informations d'état détaillées, les appareils envoient des informations sur les transitions d'état au Serveur d'archivage pour les besoins de la facturation, de la détection des erreurs, de la reconstruction de session, etc.

5.2.4.1 Etat d'application

Le gestionnaire d'application est responsable à tout moment de la maintenance d'une information détaillée de l'état de la session de média d'application. Le détail de la façon dont il opère est en dehors du domaine d'application de la présente Recommandation, mais il est important de reconnaître qu'aucun dispositif autre que le gestionnaire d'application n'est nécessaire pour maintenir la connaissance de l'état d'application.

Le gestionnaire d'application peut cependant rapporter l'état de session en mandatant de telles information au Serveur d'archivage, via le Serveur de politique. De plus, certaines informations d'état brutes (telles que le fait que des ressources aient été demandées) sont automatiquement envoyées du Serveur de politique au Serveur d'archivage.

5.2.4.2 Etat des ressources de QS

Le système CMTS est naturellement au courant de l'état détaillé des flux qu'il gère. Le Serveur de politique (si c'est un Serveur de politique à états) peut aussi conserver une notion de l'état des ressources de qualité de service sur un CMTS unique ; il peut aussi collecter les informations d'état auprès de plusieurs CMTS de sorte qu'il (et lui seul) connaît l'état de la qualité de service sur le système tout entier. Cela peut être important, par exemple, si un opérateur a institué une politique selon laquelle il n'est pas permis à une application particulière de consommer plus qu'un pourcentage donné des ressources totales du système. Dans un réseau avec peu de Serveurs de politique sans état, les systèmes CMTS sont les seuls appareils à conserver les informations d'état de la qualité de service. Comme les Serveurs de politique sans état ne conservent pas les ID de porte, ils ne peuvent même pas interroger un CMTS pour obtenir des informations sur une session multimédia particulière.

Chaque fois qu'une ressource de qualité de service passe d'un état à un autre, et chaque fois qu'une ressource de qualité de service est supprimée, un message d'événement correspondant est envoyé du système CMTS au Serveur d'archivage.

6 Description de l'interface d'Autorisation

Le présent paragraphe décrit l'interface entre le gestionnaire d'application et le Serveur de politique, et l'interface entre le ou les Serveurs de politique et le système CMTS.

L'interface entre le gestionnaire d'application et le Serveur de politique est du point de vue des transactions le symétrique des interfaces entre le Serveur de politique et le système CMTS. Les interfaces sont utilisées pour passer les informations d'autorisation, de réservation et d'activation au système CMTS, pour fournir des informations d'état du système CMTS au Serveur de politique, et du Serveur de politique au gestionnaire d'application.

Le gestionnaire d'application est le point PDP pour le Domaine de contrôle de service. Le Serveur de politique est le point PEP par rapport au gestionnaire d'application et applique les politiques du Domaine de contrôle de ressource. Le serveur de politique est un point PDP par rapport au système CMTS, et le CMTS est le point PEP par rapport au serveur de politique et se tient dans le conduit de transmission de paquet réel.

Le présent paragraphe décrit l'utilisation du protocole COPS pour le transport des messages de qualité de service IPCablecom entre le gestionnaire d'application et le Serveur de politique, et entre le Serveur de politique et le CMTS.

6.1 Portes: cadre du contrôle de qualité de service

Une porte multimédia d'IPCablecom est une représentation logique d'une décision de politique qui a été installée sur le système CMTS. Une porte est utilisée pour contrôler l'accès à un seul flux IP pour les services de QS améliorée fournis par un réseau câblé de l'Annexe B de la Rec. UIT-T J.112. Les portes sont unidirectionnelles ; une seule porte contrôle l'accès à un flux dans le sens amont ou dans le sens aval, mais pas les deux. Pour une session IP bidirectionnelle, deux portes sont nécessaires, une pour l'amont et une pour l'aval, chacune d'elles étant identifiée par un ID de porte unique. Il est important de reconnaître que ceci est une différence fondamentale avec IPCablecom-T, dans lequel un seul ID de porte peut faire référence à la fois à une porte amont et à une porte aval.

Dans IPCablecom multimédia, chaque porte a un ID de porte distinct. La porte définit les enveloppes d'autorisation, de réservation et d'engagement que le système CMTS doit utiliser pour effectuer les opérations d'autorisation, de réservation et d'engagement.

Dans tous les scénarios, le système CMTS DOIT effectuer les vérifications du contrôle d'admission des enveloppes pour s'assurer que les enveloppes d'engagement sont inférieures ou égales à l'enveloppe réservée, et que les enveloppes réservées sont inférieures ou égales à l'enveloppe autorisée. (Voir au [1] les exigences de contrôle d'admission spécifiques de DOCSIS.)

Dans le modèle "QS mandatée poussée par la politique" (scénario 1), les informations qui sont dans une porte sont utilisées par le système CMTS pour créer directement le flux de service de l'Annexe B de la Rec. UIT-T J.112, après que le CMTS ait effectué les vérifications nécessaires de contrôle d'admission des enveloppes. Dans les deux autres modèles exposés dans l'Appendice I, "QS poussée par la politique demandée par le client" 'scénario 2), et "QS tirée par la politique demandée par le client" 'scénario 3), le système CMTS utilise les informations de porte pour effectuer le contrôle d'admission des ressources demandées par le client ; le système CMTS ne prend pas l'initiative de la création des flux. Le gestionnaire d'application est responsable de l'envoi des messages de porte au Serveur de politique et le Serveur de politique est responsable de l'application des règles de politique, et ensuite de l'envoi des messages de commande de porte au système CMTS.

Une porte comporte les éléments suivants, qui sont décrits plus loin dans le présent paragraphe:

- ID de porte;
- ID de gestionnaire d'application;
- ID d'abonné;
- Spec de porte;
- Classeur;
- Profil du trafic;
- Informations de génération d'événement (facultatif);
- Limite de temps d'utilisation (facultatif);
- Limite d'utilisation en volume (facultatif);
- Données opaques (facultatif).

L'ID de porte est l'outil pour la porte. L'ID de porte est alloué par le système CMTS et est utilisé par le gestionnaire d'application, le Serveur de politique et le client pour désigner la porte.

L'ID de gestionnaire d'application est l'outil qui identifie le gestionnaire d'application.

L'ID d'abonné identifie de façon unique le client pour lequel la politique est établie.

La Spec de porte décrit les paramètres d'autorisation spécifiques qui définissent une porte (c'est-à-dire, les limites de qualité de service, les temporisateurs, etc.)

Le classeur décrit le ou les flux IP qui seront transposés dans le flux de service DOCSIS.

Le Profil de trafic décrit les attributs de qualité de service du flux de service utilisés pour prendre en charge le flux IP.

Les Informations de génération d'événement contiennent les informations utilisées par le système CMTS pour les rapports de comptabilité et d'utilisation.

La Limite d'utilisation en volume définit une enveloppe de volume pour le trafic traversant le flux associé à la porte.

La Limite de temps d'utilisation définit une enveloppe de temps limitant la durée du flux associé à la porte.

Les Données opaques représentent un objet d'utilisation générale qui reste opaque pour les éléments CMTS et PS, mais qui peut contenir des données significatives pour le gestionnaire d'application. Cet objet facultatif, s'il est fourni par le gestionnaire d'application, est conservé au système CMTS et est retourné dans toutes les réponses associées (voir au § 6.4.2.11).

Ces éléments sont communiqués au Serveur de politique et au système CMTS via les objets COPS et sont décrits plus en détail plus loin dans le présent paragraphe. Durant l'installation de la porte, les informations ci-dessus sont communiquées au système CMTS. Après l'achèvement de l'installation, un flux de service DOCSIS peut être créé. Après la création du flux de service DOCSIS, la porte y aura associé un élément supplémentaire, le flux de service DOCSIS. Il y a un mappage univoque strict entre un flux de service DOCSIS et une porte.

Une porte passe par de multiples états. Dans les scénarios 2 et 3, où l'entité client est responsable de la réservation puis de l'activation des flux de service DOCSIS, une porte multimédia se comporte de façon très similaire à une porte de DQoS d'IPCablecom-T. Lorsque le Serveur de politique installe la porte sur le système CMTS, la porte est réputée être dans un état "autorisé". Elle reste dans cet état jusqu'à ce qu'il soit explicitement supprimé par le Serveur de politique (ou, moins vraisemblablement, il est supprimé pour une raison quelconque par le CMTS lui-même), ou jusqu'à ce qu'arrive une demande de flux dynamique du client.

Lorsque le client demande l'ajout d'un flux de service dynamique, il présente l'ID de porte comme un jeton d'autorisation. Le système CMTS utilise l'ID de porte pour effectuer le contrôle d'admission sur le flux dynamique DOCSIS à l'égard de l'enveloppe d'autorisation définie par la porte. Dans le scénario 1, le Serveur de politique ordonne au système CMTS de faire la transition d'état au nom du gestionnaire d'application, et le système CMTS est l'entité responsable de l'initialisation et de la suppression des flux de service DOCSIS. Dans la présente Recommandation, le paragraphe Transition d'état décrit ce comportement. Lorsque le système CMTS reçoit pour instruction de supprimer un flux de service DOCSIS, sa porte associée demeure jusqu'à ce qu'elle soit explicitement supprimée par le Serveur de politique/gestionnaire d'application, ou jusqu'à ce qu'elle arrive en fin de temporisation et que ses ressources soient réclamées par le système CMTS (voir au § 6.5.8). Au contraire, lorsque le Serveur de politique/gestionnaire d'application supprime une porte, le système CMTS supprimera les flux de service DOCSIS associés.

6.1.1 Identification de porte (ID de porte)

Un ID de porte est un identifiant qui est alloué localement par le système CMTS où réside la porte. Un ID de porte DOIT être associé à une seule porte. Alors que le modèle de commande de porte de DQoS d'IPCablecom-T suppose généralement une paire de portes unidirectionnelles (une amont et une aval) par ID de porte pour la prise en charge d'une session vocale deux voies normale, ici, la relation entre porte et ID de porte est explicitement univoque, de sorte qu'il est plus facile de prendre en charge une large gamme de services multimédia.

Lorsque le gestionnaire d'application envoie une demande d'établissement de porte, cela déclenche chez le Serveur de politique l'envoi d'un message Etablir porte au CMTS. Lorsque le CMTS répond par un accusé de réception contenant l'ID de porte, le Serveur de politique transmet cette réponse qui comprend l'ID de porte en retour au gestionnaire d'application. Cet identifiant DOIT être unique dans le cadre de la session COPS d'IPCablecom multimédia. Noter que comme il peut y avoir des relations multivoques entre un Serveur de politique et un CMTS, l'ID de porte alloué par un CMTS ne peut être à coup sûr unique sur l'ensemble du réseau, et les Serveurs de politique peuvent utiliser l'ID de gestionnaire d'application à côté de l'ID de porte afin d'identifier la porte de façon univoque.

Ci-après figure un algorithme qui peut être utilisé pour allouer des valeurs de l'ID de porte. On partage le mot de 32 bits en deux parties, une partie indice, et une partie aléatoire. La partie indice identifie la porte en l'indexant dans un petit tableau, alors que la partie aléatoire donne un peu d'obscurité à la valeur. Indépendamment de l'algorithme choisi, le système CMTS DEVRAIT essayer de minimiser la possibilité d'ambiguïtés d'ID de porte en s'assurant qu'aucun ID de porte n'est réutilisé dans les trois minutes de sa fermeture ou suppression. Pour l'algorithme suggéré, cela pourrait être effectué en incrémentant simplement la partie indice à chaque allocation consécutive d'ID de porte, en revenant à zéro lorsque la valeur d'entier maximale de la partie indice est atteinte.

6.1.2 Identification de gestionnaire d'application (AMID)

Chaque gestionnaire d'application est préapprovisionné avec un AMID qui est unique dans l'univers d'un seul fournisseur de service. Le gestionnaire d'application inclut cet identifiant dans tous les messages qu'il envoie au Serveur de politique. Le Serveur de politique passe de façon transparente ces informations au système CMTS via les messages de commande de porte. Le CMTS DOIT retourner l'AMID associé à la porte au Serveur de politique. Le Serveur de politique utilise ces informations pour associer les messages de porte à un gestionnaire d'application particulier.

L'AMID DOIT être une valeur mondialement unique allouée au gestionnaire d'application par le fournisseur de service. Le gestionnaire d'application DOIT utiliser l'AMID alloué dans toutes ses transactions avec les Serveurs de politique. Noter que comme le gestionnaire d'application peut être manipulé par une tierce partie, et qu'un unique gestionnaire d'application pourrait interagir avec plusieurs opérateurs fournisseurs de service, un seul gestionnaire d'application physique peut être approvisionné avec plusieurs AMID.

6.1.3 Identification de l'abonné (ID d'abonné)

L'ID d'abonné, consistant en l'adresse IP de l'appareil CPE du client ou du câblo-modem, identifie l'utilisateur qui demande le service. Dans les environnements de réseau complexes, cette adresse peut être utilisée pour acheminer les messages de commande de porte entre un certain nombre de Serveurs de politique et pour déterminer quel CMTS fournit le service à un point d'extrémité donné. En plus de l'adresse IP, un abonné peut aussi être identifié via un FQDN ou des données opaques (objet défini ci-dessous) pertinentes pour le service en question.

6.1.4 Spécification de porte (Spec de porte)

La Spec de porte décrit des attributs de haut niveau de la porte, et contient des informations qui concernent le traitement d'autres objets spécifiés dans le message de porte. Les informations contenues dans une Spec de porte sont précisées ci-dessous:

- ID de porte;
- ID de classe de session;
- Direction;
- Temporisateur d'autorisation;
- Temporisateur de réservation;
- Temporisateur d'engagement;
- Outre passement de DSCP/Type de service.

L'ID de porte identifie de façon univoque la porte pour laquelle l'opération devrait être effectuée.

L'ID de classe de session fournit au gestionnaire d'application et au Serveur de politique le moyen de grouper des portes en différentes classes avec différentes caractéristiques d'autorisation. Par exemple, on pourrait utiliser l'ID de classe de session pour représenter un schéma de priorité ou de préemption qui permettrait au Serveur de politique ou au système CMTS de préempter une porte préautorisée pour permettre l'autorisation d'une nouvelle porte possédant une priorité supérieure.

Direction indique si la porte est pour un flux amont ou aval. En fonction de cette direction, le système CMTS DOIT réserver et activer en conséquence les flux DOCSIS.

Temporisateur d'autorisation limite la quantité de temps pendant laquelle l'autorisation doit rester valide avant qu'elle soit réservée (voir au § 6.2).

Temporisateur de réservation limite la quantité de temps pendant laquelle la réservation doit rester valide avant que les ressources ne soient engagées (voir au § 6.2).

Temporisateur d'engagement limite la quantité de temps pendant lequel un flux de service peut rester inactif.

Le champ Outre passement de DSCP/Type de service peut être utilisé pour outrepasser le champ DSCP/Type de service de paquets associé au flux de service DOCSIS qui correspond à la porte. Ce champ PEUT être non spécifié, auquel cas le champ DSCP/Type de service de paquet n'est pas outrepassé par le CMTS. Ce champ PEUT être utilisé aussi bien dans la direction amont qu'aval.

6.1.5 Classeur

Un classeur DOIT être défini pour une porte. Des classeurs supplémentaires peuvent être inclus dans le message Etablir porte d'origine. Les classeurs peuvent être ajoutés ou supprimés dans un Etablir porte ultérieur. Les implémentations conformes DOIVENT être capables de prendre en charge un minimum de quatre classeurs lors du traitement d'un message Etablir porte. Le classeur identifie le flux IP qui sera transposé en flux de service DOCSIS pour la porte. Dans le scénario 1, lorsque le système CMTS crée le flux dynamique, il DOIT utiliser le classeur de porte comme classeur pour le flux de service DOCSIS.

Un classeur est un septuplé:

- protocole;
- source IP;
- port de source;
- destination IP;
- port de destination;
- priorité;
- DSCP/Type de service.

Le champ Protocole identifie le type de protocole (par exemple, IP, ICMP, etc).

Source IP est l'adresse IP (comme elle est vue du CMTS) de l'origine du flux IP, alors que Destination IP est le point de terminaison pour le flux IP.

Port de source et Port de destination spécifient les ports UDP ou TCP pour le flux IP.

Priorité peut être utilisé pour distinguer entre plusieurs classeurs qui correspondent à un paquet donné. Elle est normalement réglée à une valeur par défaut dans la mesure où les classeurs sont généralement destinés à être uniques.

Le champ DSCP/Type de service identifie le champ DSCP/Type de service qui doit être vérifié pour les paquets à classer sur le flux IP. Pour donner le maximum de souplesse dans la définition de la stratégie de gestion d'un réseau, un gabarit d'accompagnement est défini qui détermine quels bits de l'octet DSCP/Type de service doivent être utilisés comme filtre dans la classification des paquets. Ceci permet aussi bien les stratégies DiffServ que TOS (*type of service*) (qui définissent et utilisent des bits différents au sein de cet octet).

Un classeur PEUT avoir des champs contenant des caractères génériques de remplacement (indiqués par des champs à zéro), mais il faut faire attention à ce que plusieurs flux IP ne correspondent pas, par inadvertance, au même classeur, ce qui pourrait conduire à des résultats inattendus.

6.1.6 Profil de trafic

Pour une porte, il y a trois façons de base pour exprimer le profil de trafic:

1) spec de flux;
2) nom de classe de service DOCSIS;
3) paramétrisation spécifique de DOCSIS.

Le Serveur de politique ou le gestionnaire d'application DOIVENT définir le Profil de trafic pour une porte en utilisant un des éléments qui suivent:

1) la Spec de flux;
2) les Noms de classe de service DOCSIS;
3) les paramètres spécifiques de DOCSIS.

Si le Serveur de politique ou le gestionnaire d'application utilisent les Spec de flux pour définir l'enveloppe autorisée, les enveloppes réservée et engagée DOIVENT alors être elles aussi définies en utilisant les Spec de flux. Autrement, si le Serveur de politique ou le gestionnaire d'application utilisent les noms de classe de service DOCSIS pour définir l'enveloppe autorisée, les enveloppes réservée et engagée DOIVENT alors être elles aussi définies en utilisant les noms de classe de service DOCSIS.

Il DOIT y avoir au moins un ensemble de paramètres de Profil de trafic spécifié lorsque la porte est installée pour la première fois. Le Serveur de politique et le gestionnaire d'application PEUVENT

spécifier un second ensemble pour représenter l'enveloppe réservée, et un troisième ensemble pour représenter l'enveloppe engagée. Si le système CMTS a reçu l'ordre de créer immédiatement un flux de service à réception d'un message Etablir porte (via la présence des enveloppes réservée ou engagée), le système CMTS DOIT utiliser les paramètres de Profil de trafic des enveloppes réservée et engagée pour effectuer l'échange de messages de l'Annexe B de la Rec. UIT-T J.112 afin de créer le flux, dans le sens spécifié par le champ Direction dans la Spec de porte (pourvu que la demande soit autorisée et que des ressources suffisantes existent pour satisfaire la demande). Lorsqu'il reçoit l'ordre de passer à l'état d'engagement, le système CMTS DOIT utiliser le Profil de trafic pour activer le flux de service DOCSIS. Pour optimiser l'action, le Serveur de politique PEUT ordonner au système CMTS d'effectuer les trois actions (autorisation, réservation et engagement) au nom du gestionnaire d'application via un seul message de commande de porte. Autrement, le Serveur d'application/gestionnaire d'application PEUT envoyer des messages Etablir porte séparés pour dire au système CMTS d'autoriser et réserver puis ensuite d'engager via un message Etablir porte ultérieur.

6.1.6.1 Spec de flux

L'objet Spec de flux contient des Spec de flux RSVP qui sont utilisés pour décrire le Profil de trafic du flux IP. L'objet Spec de flux peut contenir plusieurs Spec de flux RSVP:

- Spec de flux qui définit l'enveloppe d'autorisation de ressources au sein de laquelle peuvent être faites les futures réservations;
- Spec de flux qui définit l'enveloppe réservée au sein de laquelle peuvent être faites les futures demandes d'engagement;
- Spec de flux qui définit les ressources à engager.

Les Spec de flux RSVP prennent en charge deux types de services: charge contrôlée [4] et qualité de service garantie [5]. La principale différence entre les deux types de service est exposée dans le § 8. Les deux types de service se distinguent par le numéro de service de Spec de flux, qui est spécifié dans la Spec de flux RSVP. Le numéro de service 5 est pour la charge contrôlée, et le numéro de service 2 est pour la qualité de service garantie. Un service de charge contrôlée NE DOIT contenir que les paramètres du seau de jetons de Tspec, et pas ceux de RSpec. Un service garanti DOIT contenir à la fois les paramètres de TSpec et de RSpec.

Se reporter au § 8 pour des informations sur la façon de transposer explicitement les paramètres RSVP en paramètres DOCSIS. Lorsqu'on déduit les paramètres DOCSIS en utilisant les paramètres de Spec de flux RSVP, il y a quelques paramètres DOCSIS qui sont très approximés. Si les approximations ne donnent pas au Serveur de politique ou au gestionnaire d'application le contrôle qu'il souhaite, le Serveur de politique /gestionnaire d'application PEUT utiliser les autres méthodes de définition du Profil de trafic, qui incluent la capacité de définir certains paramètres spécifiques de DOCSIS. Ces paramètres permettent au Serveur de politique ou au gestionnaire d'application de raffiner le réglage de la transposition standard entre Spec de flux et paramètres DOCSIS.

6.1.6.2 Nom de classe de service DOCSIS

Le Nom de classe de service DOCSIS indique la classe de service DOCSIS à utiliser pour décrire les attributs de qualité de service. Le système CMTS DOIT prendre en charge les Noms de classe de service DOCSIS.

Le Nom de classe de service DOCSIS permet d'utiliser les paramètres de qualité de service DOCSIS pré-approvisionnés au CMTS. On peut configurer au CMTS des Classes de service nommées DOCSIS avec différents profils de qualité de service DOCSIS, puis référencer le Nom de classe de service DOCSIS dans la porte pour associer indirectement un profil de qualité de service à une porte particulière. DOCSIS permet aussi de modifier les paramètres en utilisant les TLV. Dans IPCablecom multimédia, les paramètres de qualité de service du Nom de classe de service DOCSIS NE DOIVENT PAS être modifiés à l'aide de TLV. Un système CMTS DOIT retourner l'erreur

"Nom de classe de service indéfini" si des modifications des paramètres de qualité de service du Nom de classe de service sont demandés (voir au § 8.4.2.1.4).

Pour plus d'informations sur les classes de service DOCSIS, se reporter au § B.10.1.3 de la Rec. UIT-T J.112, Annexe B sur l'interface RFI [1].

6.1.6.3 Paramétrisation spécifique de DOCSIS

La troisième façon de définir le Profil de trafic consiste à utiliser le Profil de trafic spécifique de DOCSIS, ce qui permet au gestionnaire d'application de spécifier explicitement les paramètres DOCSIS du flux DOCSIS. Si le gestionnaire d'application souhaite utiliser cette troisième voie de définition du Profil de trafic, il DOIT inclure un objet contenant les paramètres spécifiques DOCSIS.

Tous les types de programmation de flux de service DOCSIS sont pris en charge via plusieurs S-Types de Profil de trafic différents. Chaque S-Type a un codage différent des paramètres spécifiques de DOCSIS pertinents pour ce type de programmation de flux de service. Pour des précisions concernant la mise en paramètres spécifique de DOCSIS, se reporter au § 6.4.2.7.

6.1.7 Info de génération d'événement

Cet objet contient des informations se rapportant au CMTS pour servir aux fonctions de comptabilité et facturation. Ses attributs incluent:

- adresse primaire: port du Serveur d'archivage primaire auquel le système CMTS DOIT envoyer les enregistrements d'événement;
- adresse secondaire: port du Serveur d'archivage secondaire que le CMTS DOIT utiliser comme spécifié en [10] si le primaire est indisponible;
- fanion indiquant si le CMTS DOIT envoyer des messages d'événement au Serveur d'archivage en temps réel, ou si le CMTS DOIT faire des lots des messages d'événement et les envoyer à intervalles périodiques;
- ID de Corrélation de facturation, que le CMTS DOIT passer au Serveur d'archivage avec chaque enregistrement d'événement.

L'omission de l'objet Info de génération d'événement indique que le CMTS NE DOIT PAS générer de message d'événement pour une porte donnée.

6.1.8 Limite de temps d'utilisation

Cet objet spécifie la quantité de temps pendant laquelle une porte peut rester engagée avant d'atteindre le seuil de limite de temps pour cette porte. Cet objet est opaque pour le CMTS. Le CMTS n'est pas responsable de l'application des limites de temps, mais il DOIT mémoriser cet objet et le retourner sur demande.

6.1.9 Limite de volume d'utilisation

Le gestionnaire d'application utilise la Limite de volume d'utilisation pour signaler au CMTS de générer un message de commande de porte lorsque la quantité de données spécifiée a traversé la porte. Le système CMTS n'est pas responsable de l'application des limites de volume, mais il DOIT signaler au Serveur de politique/gestionnaire d'application qu'une limite de volume a été atteinte.

6.1.10 Données opaques

Les Données opaques consistent en informations générales qu'un Serveur de politique ou un gestionnaire d'application peut mémoriser sur un CMTS. Ces données restent opaques pour le CMTS, mais contiennent des informations utiles pour le Serveur de politique ou le gestionnaire d'application. Si ceux-ci les fournissent, le CMTS retournera cet objet dans toutes les réponses (voir § 6.4.2.11).

6.1.11 Info d'heure de porte

Info d'heure de porte contient un horodatage qui représente le temps pendant lequel la porte a été engagée. Ceci peut être consulté et utilisé par un Serveur de politique ou gestionnaire d'application pour l'application d'une politique réseau sur le temps.

6.1.12 Info d'utilisation de porte

Info d'utilisation de porte consiste en un compteur d'octets indiquant le nombre d'octets de données qui ont été transmis par cette porte (voir § 6.4.2.13). Semblable à l'objet Info d'heure de porte, ces informations peuvent être utilisées par un Serveur de politique ou gestionnaire d'application pour appliquer une politique réseau sur le volume.

6.2 Transitions de porte

Ainsi qu'il a été brièvement exposé plus haut, une porte peut se trouver dans les états logiques suivants:

- autorisé – un Serveur de politique a autorisé le flux avec des limites de ressources définies;
- réservé – des ressources ont été réservées pour le flux;
- engagé – des ressources sont actives et sont en cours d'utilisation.

Pour l'automate à états décrit à la Figure 3, le CMTS DOIT terminer l'événement de déclenchement avec un résultat réussi avant de faire passer une porte d'un état à un autre. Pour les événements de commande de porte, le CMTS NE DOIT PAS changer d'état jusqu'à ce que la demande ait été entièrement traitée (y compris toute transition de flux résultante) et que le système CMTS ait déterminé qu'un accusé de réception de réussite va être transmis.

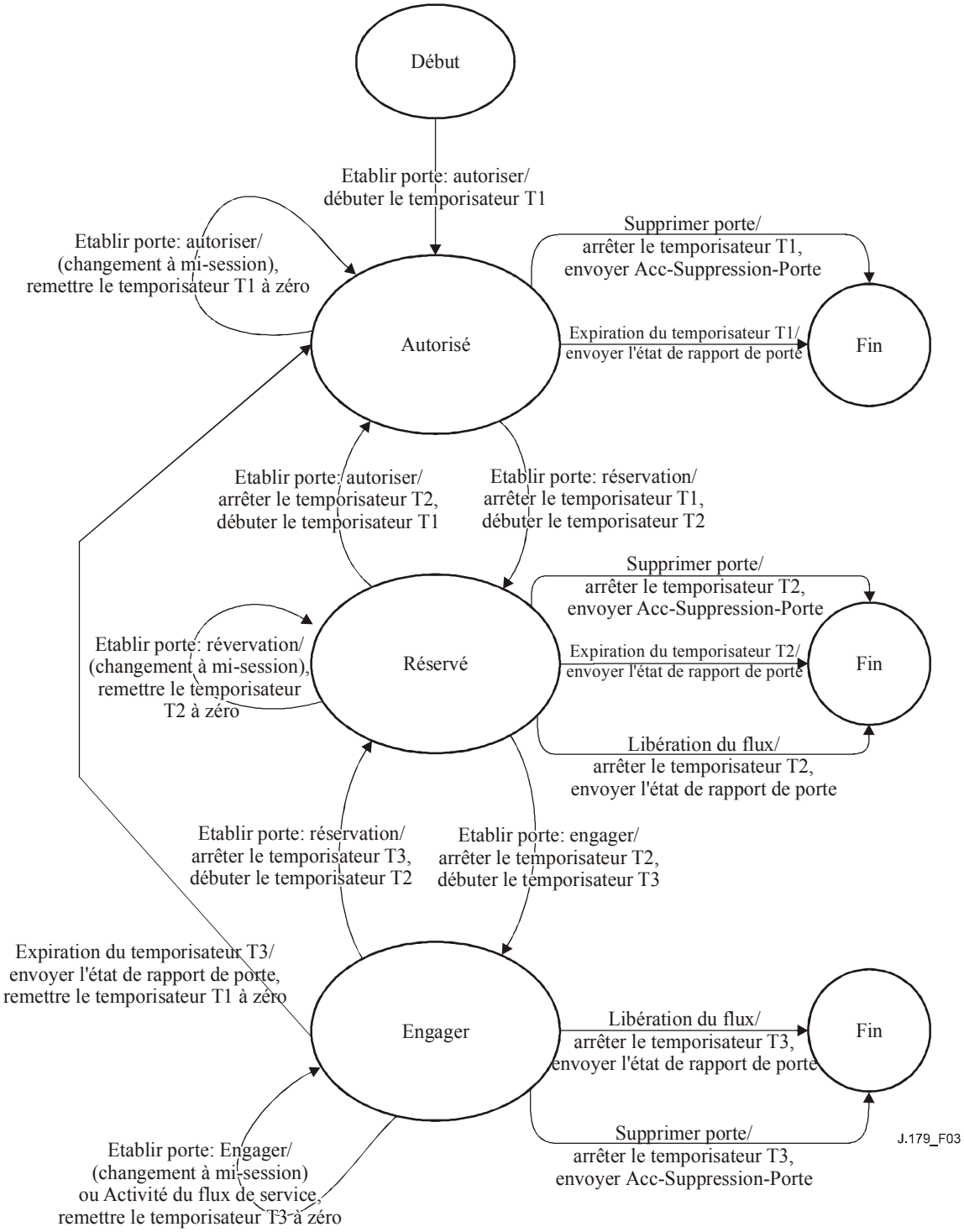

Figure 3/J.179 – Transitions d'état de porte

Le CMTS DOIT prendre en charge les états et les transitions de porte comme indiqué à la Figure 3 et décrit dans le présent paragraphe. Le CMTS DOIT aussi implémenter les transitions pour le traitement des erreurs de protocole.

Dans le présent paragraphe sont décrites les transitions d'état de la porte dans le CMTS qui résultent d'événements externes (messages de commande de porte venant du Serveur de politique), ainsi que les transitions qui résultent d'événements internes (par exemple, expiration de temporisateur). Noter que le Serveur de politique n'est pas la source des événements extérieurs ; au lieu de cela, le Serveur

de politique agit simplement comme mandataire du gestionnaire d'application qui est le déclencheur des événements.

6.2.1 Autorisé

Une porte est créée dans le CMTS par une commande Etablir porte du Serveur de politique. Le système CMTS alloue un identifiant unique appelé ID de porte. La porte est maintenant réputée être dans l'état autorisé et le CMTS DOIT lancer le temporisateur T1. Le temporisateur T1 limite la durée de validité de l'autorisation.

Une porte dans l'état autorisé DOIT être supprimée à réception d'un message Suppression de porte. Lorsque cela arrive, le CMTS DOIT répondre par un message Acc de suppression de porte et DOIT arrêter le temporisateur T1.

Le CMTS DOIT prendre en charge les transitions d'état suivantes lorsqu'une porte est dans l'état autorisé:

Transitions dans l'état autorisé:

- de bouclage autorisé à autorisé: Modifie l'enveloppe autorisée;
- d'autorisé à réservé (définit le passage d'enveloppe réservée ≤ enveloppe autorisée);
- d'autorisé à fin (supprime l'enveloppe autorisée).

Le CMTS NE DOIT PAS prendre en charge d'autres transitions d'état pour une porte dans l'état autorisé, mais plusieurs stimuli séparés peuvent déboucher sur les transitions décrites.

Lorsque la porte est installée, elle est réputée être dans l'état Autorisé. Lorsqu'elle est dans cet état, le Serveur de politique PEUT modifier tout paramètre associé à une porte (par exemple, Profil de trafic, Classeur, etc). Si un message Etablir porte est reçu dans l'état Autorisé et qu'il ne fait pas passer la porte dans les états Réservé ou Engagé, le système CMTS DOIT alors relancer le temporisateur T1.

Lorsqu'elle est dans l'état Autorisé, le système CMTS DOIT faire passer la porte dans l'état Réservation sur demande réussie du Serveur de politique. Le système CMTS DOIT faire passer la porte dans l'état Fin à réception d'un message Suppression de porte venant du Serveur de politique ou à l'expiration du temporisateur T1.

6.2.2 Réservé

Une porte dans l'état Autorisé s'attend à ce que le client essaye de réserver des ressources. Dans le scénario 1, le Serveur de politique réserve les ressources au nom du client. Pour réserver des ressources, le Serveur de politique DOIT produire un message Etablir porte ultérieur avec un Profil de trafic qui inclut l'enveloppe réservée. A réception de cette demande de réservation, le CMTS DOIT vérifier que la demande est dans les limites de l'autorisation établie pour la porte et effectuer les procédures de contrôle d'admission.

Si la demande de réservation n'arrive pas avant l'expiration du temporisateur T1, le CMTS DOIT supprimer la porte, arrêter le temporisateur T1, et notifier au Serveur de politique le changement d'état. Si le contrôle d'admission réussit et que seule la réservation de ressources était demandée, le CMTS DOIT mettre la porte dans l'état Réservé. Simultanément, le CMTS DOIT aussi arrêter le temporisateur T1 et lancer le temporisateur T2 (Temporisateur de réservation). Si les procédures de contrôle d'admission ne réussissent pas, le CMTS DOIT maintenir la porte dans l'état Autorisé et fournir une réponse Erreur-d'établissement-de-porte au Serveur de politique.

Le CMTS DOIT prendre en charge les transitions d'état suivantes lorsqu'une porte est dans l'état Réservé:

Transitions d'état Réservé:

- de Bouclage réservé à Réservé: modifie Enveloppe autorisée (≥ Enveloppe réservée);
- de Bouclage réservé à Réservé: modifie Enveloppe réservée (≤ Enveloppe autorisée);
- de Réservé à Engagé (définit Enveloppe engagée ≤ Enveloppe réservée);
- de Réservé à Fin (supprime Enveloppes réservée et autorisée).

Le CMTS NE DOIT PAS accepter d'autres transitions d'état pour une porte dans l'état Réservé, mais plusieurs stimuli distincts peuvent avoir pour résultat les transitions décrites.

A partir de l'état Autorisé, le CMTS DOIT faire passer la porte dans l'état Réservé, s'il est demandé par le Serveur de politique. Tant que l'enveloppe réservée est inférieure ou égale à l'enveloppe autorisée, la demande réussit le contrôle d'admission et la réservation du flux est réussie. Une fois qu'elle est dans l'état Réservé, l'enveloppe autorisée de la porte PEUT être modifiée via un message Etablir porte. L'enveloppe réservée de la porte peut aussi être modifiée dans l'état Réservé (voir § 6.5.6). Si dans un état Réservé un message Etablir porte est reçu et qu'il ne fait pas passer la porte à l'état Autorisé ou Engagé, le système CMTS DOIT alors relancer le temporisateur T2.

L'enveloppe réservée DOIT toujours être inférieure ou égale à l'enveloppe autorisée. Dans l'état Réservé, pour qu'un CMTS fasse passer une porte à l'état Engagé, l'enveloppe engagée DOIT être inférieure ou égale à l'enveloppe réservée (voir § 6.5.3).

Dans l'état Réservé, le Serveur de politique peut modifier l'enveloppe autorisée en spécifiant un nouveau Profil de trafic dans un message Etablir porte. Le nouveau Profil de trafic définira une enveloppe autorisée modifiée et la même enveloppe réservée qui était utilisée précédemment pour faire passer la porte dans l'état Réservé. Cependant, toutes les demandes pour modifier les enveloppes Autorisée, Réservée ou Engagée DOIVENT être conformes à la règle générale:

Enveloppe autorisée ≥ Enveloppe réservée ≥ Enveloppe engagée

Le Serveur de politique PEUT supprimer une porte dans l'état Réservé en produisant un message Suppression de porte.

6.2.3 Engagé

Dans l'état Réservé, la porte s'attend à ce que le client engage des ressources, et donc à les activer. Dans le scénario 1, le Serveur de politique engage les ressources au nom du client. Pour engager des ressources, le Serveur de politique DOIT produire une commande Etablir porte avec un Profil de trafic qui inclut l'enveloppe engagée. Le CMTS DOIT à nouveau autoriser la qualité de service demandée à l'égard de l'enveloppe réservée. Si l'autorisation réussit, le CMTS DOIT arrêter le temporisateur T2 et lancer le temporisateur T3. Si l'autorisation échoue, le CMTS DOIT relancer le temporisateur T2.

Si la demande d'engagement ne survient pas avant l'expiration du temporisateur T2, le CMTS DOIT supprimer la porte, arrêter le temporisateur T2 et notifier au Serveur de politique le changement d'état.

Noter qu'une fois que le flux de service DOCSIS a été activé, le CMTS DOIT rafraîchir le temporisateur T3 lorsque les données sont transférées sur le flux. S'il n'y a pas d'activité sur le flux pour une durée égale à T3, le CMTS DOIT supprimer le flux de service ainsi que la porte correspondante, et le Serveur de politique DOIT recevoir notification du changement d'état. De même, le Serveur de politique DOIT notifier le changement d'état au gestionnaire d'application.

Dans l'état Engagé, le gestionnaire d'application PEUT supprimer la porte en produisant un message Supprimer porte auprès du Serveur de politique, qui à son tour DOIT relayer le message jusqu'au

CMTS. Si le Serveur de politique envoie un message Supprimer porte au CMTS avant l'expiration du temporisateur T2, le CMTS DOIT supprimer la porte et le flux de service correspondant et arrêter le temporisateur T2.

Le CMTS DOIT prendre en charge les transitions d'état suivantes lorsque la porte est dans l'état Engagé:

Transitions de l'état Engagé:

- de Bouclage engagé à Engagé: modifie l'enveloppe autorisée (≥ Enveloppe réservée);
- de Bouclage engagé à Engagé: modifie l'enveloppe réservée (≥ Enveloppe engagée);
- de Bouclage engagé à Engagé: modifie l'enveloppe engagée (≤ Enveloppe réservée);
- de Engagé à Réservé (supprime l'enveloppe engagée);
- de Engagé à Fin (supprime les enveloppes engagée, réservée et autorisée).

Le CMTS NE DOIT PAS accepter d'autres états de transitions pour une porte dans l'état Engagé, mais un certain nombre de stimuli distincts peuvent avoir pour résultat les transitions décrites.

Lorsqu'il est dans l'état Réservé, le CMTS DOIT faire passer une porte à l'état Engagé, si c'est demandé par le Serveur de politique tant que l'enveloppe engagée est inférieure ou égale à l'enveloppe réservée (voir § 6.5.3). Alors que dans l'état Engagé, le Serveur de politique PEUT modifier l'enveloppe autorisée de la porte via un message Etablir porte, tant que l'enveloppe autorisée est supérieure ou égale à l'enveloppe réservée. Dans cet état, le Serveur de politique PEUT aussi modifier l'enveloppe réservée, tant que l'enveloppe réservée est supérieure ou égale à l'enveloppe engagée. Dans cet état, le Serveur de politique PEUT même modifier l'enveloppe engagée, tant que la nouvelle enveloppe est inférieure ou égale à l'enveloppe réservée. Alors que dans l'état Engagé, le CMTS DOIT faire revenir une porte à l'état Réservé si c'est demandé. Dans le scénario 1, le Serveur de politique PEUT demander cette action en produisant un message Etablir porte avec un Profil de trafic qui inclut les enveloppes autorisée et réservée, mais n'inclut pas d'enveloppe engagée.

Alors qu'il est dans l'état Engagé, le CMTS DOIT faire passer une porte à l'état Fin à réception d'un message Supprimer porte du Serveur de politique. Lorsqu'il est dans l'état Engagé, le Serveur de politique PEUT modifier l'enveloppe autorisée ou réservée en spécifiant simplement le nouveau Profil de trafic ; le nouveau Profil de trafic DOIT contenir les enveloppes autorisée ou réservée modifiées, et la même enveloppe engagée qui était utilisée avant la transition de porte dans l'état Engagé.

Pour l'optimisation du scénario 1, le Serveur de politique PEUT autoriser, réserver et engager au même moment en produisant un message Etablir porte avec le Profil de trafic incluant l'ensemble des trois enveloppes de sorte que le CMTS reçoive pour instruction d'exécuter les trois actions à la suite sans autre délai, c'est-à-dire qu'ils DOIVENT réussir tous trois (s'il en est ainsi, le CMTS DOIT l'indiquer par un Acc d'Etablissement de porte) ou échouer tous trois (s'il en est ainsi, le CMTS DOIT l'indiquer par un Erreur d'Etablissement de porte).

A partir de l'état Engagé, la porte peut retourner à l'état Autorisé du fait de l'expiration du temporisateur T3. Si le CMTS détecte qu'il n'y a pas eu d'activité sur le flux associé pendant une durée de T3, il DOIT générer un message Rapport d'état de porte au Serveur de politique indiquant que le flux a été inactif pendant une durée définie par T3. Le Serveur de politique DOIT relayer le message au gestionnaire d'application. Le gestionnaire d'application DOIT réactiver le flux et relancer le temporisateur en produisant un autre message Etablir porte, ou retirer la porte en produisant un message Supprimer porte.

6.3 Profil COPS pour IPCablecom multimédia

Comme défini plus haut, le contrôle d'admission implique le processus de gestion des demandes de ressources de qualité de service sur la base des politiques administratives et des ressources disponibles. Des modules opératoires de haut niveau associés à ce processus sont décrits dans l'Appendice I. D'après ce modèle, les politiques administratives sont mémorisées dans une base de données de politique et contrôlées par le Serveur de politique.

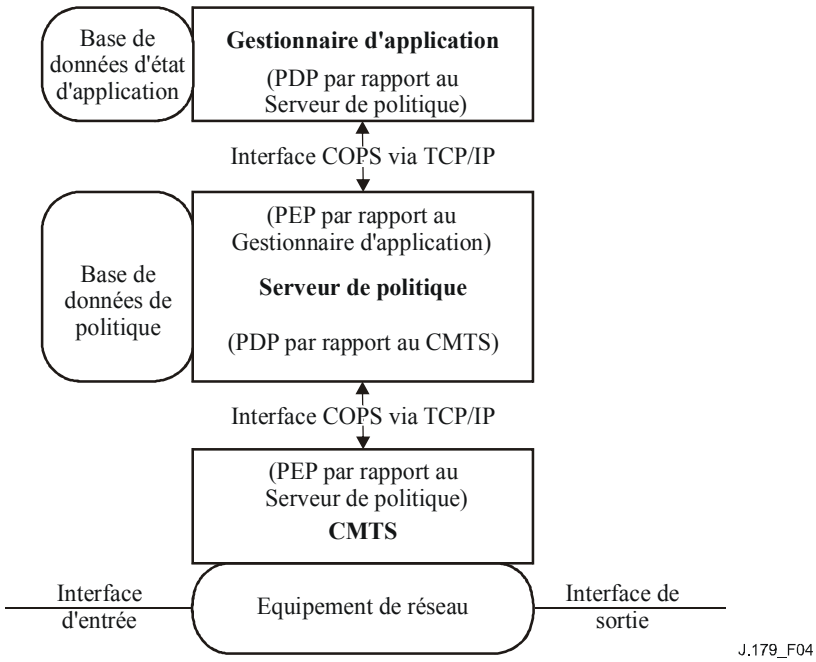

Figure 4/J.179 – Agencement du contrôle d'admission de qualité de service

Les décisions de contrôle d'admission faites par le Serveur de politique DOIVENT être communiquées au système CMTS ou au gestionnaire d'application en utilisant COPS. Le CMTS PEUT faire les demandes de contrôle d'admission de qualité de service au serveur COPS sur la base des événements de réseau déclenchés soit par le protocole de signalisation de qualité de service, soit via des mécanismes de détection de flux de données. L'événement réseau peut aussi avoir besoin de gestion de bande passante de qualité de service, par exemple, si une nouvelle interface capable de qualité de service devient opérationnelle.

Les décisions de politique de qualité de service faites par le Serveur de politique PEUVENT être poussées au système CMTS sur la base d'une demande du gestionnaire d'application. Le CMTS PEUT accéder à ces informations de décision pour faire des décisions d'application de politique sur les demandes de session entrantes reçues au CMTS. Le CMTS NE DOIT PAS accepter de messages DSx provenant de modems-câble dans IPCablecom multimédia. Le CMTS DOIT traiter un message DSx provenant d'un modem-câble comme une demande avec un ID de porte non valide.

Une configuration client/serveur COPS acceptant le contrôle d'admission COPS est spécifiée dans le protocole COPS de l'IETF [7]. Ce protocole comporte les opérations suivantes:

- Client Ouvert (OPN, *client-open*)/Client Accepté (CAT, *client-accept*)/Client Fermé (CC, *client-close*): le client COPS (PEP) envoie un message OPN pour initialiser une connexion avec le serveur COPS (PDP), et le serveur répond avec un message CAT pour accepter la connexion. Le serveur ou le client envoie un message CC pour terminer la connexion.
- Demande (REQ, *request*): le client envoie un message REQ au serveur pour demander les informations de décision de contrôle d'admission ou les informations de configuration de

l'appareil. Le message REQ peut contenir des informations spécifiques du client qu'utilise le serveur, ainsi que des données dans la base de données de politique d'admission de session, pour prendre des décisions de politique.

- Décision (DEC): le serveur répond aux messages REQ en envoyant en retour un message DEC au client qui a initialisé la demande d'origine. Les messages DEC peuvent être envoyés immédiatement en réponse à un message REQ (c'est-à-dire, un message DEC sollicité) ou à tout moment après, pour changer ou mettre à jour une décision précédente (c'est-à-dire, un message DEC non sollicité).
- Rapport-d'état (RPT): le client envoie un message RPT au serveur indiquant des changements à l'état de demande chez le client. Le client envoie cela pour informer le serveur des ressources réservées réelles après que le serveur ait accordé l'admission. Le client peut aussi utiliser Rapport-d'état pour informer périodiquement le serveur de l'état en cours du client.
- Supprimer-l'état-de-demande (DRQ, *delete-request-state*): le client envoie un message DEL au serveur pour demander le nettoyage d'état. Ceci peut être le résultat d'une libération de ressources de qualité de service par le client.
- Garder-en-vie (KA, *keep-alive*): envoyé à la fois par le client et le serveur pour une détection d'échec de communication.
- Demande d'état de synchronisation (SSQ, *synchronize-state-request*)/Fin d'état de synchronisation (SSC, *synchronize-state-complete*): le serveur envoie le message SSQ au client qui demande des informations sur l'état en cours. Le client envoie à nouveau des interrogations de demande au serveur pour effectuer la synchronisation, puis envoie un message SSC pour indiquer l'achèvement de l'événement de synchronisation. Un Serveur de politique PEUT prendre en charge les fonctions de synchronisation SSQ/SSC s'il est nécessaire au Serveur de politique d'acquérir ou de reconstruire l'état à partir du CMTS. Le CMTS DOIT prendre en charge les fonctions de synchronisation SSQ/SSC.

Au sein de l'architecture IPCablecom multimédia, les relations de points PDP-PEP sont les suivantes:

- le gestionnaire d'application est un Point de décision de politique (PDP, *policy decision point*) COPS par rapport au Serveur de politique;
- le Serveur de politique est un PEP par rapport au gestionnaire d'application;
- le Serveur de politique est un PDP par rapport au CMTS;
- le CMTS est un PEP par rapport au Serveur de politique.

Bien que les échanges de messages COPS nécessaires pour IPCablecom multimédia soient cohérents avec le protocole COPS, il y a une petite différence dans la façon dont débute la session COPS. Le document RFC 2748 [7] déclare:

"le protocole COPS utilise une seule connexion TCP permanente entre le PEP et un PDP distant. Un seul PDP par serveur DOIT être branché sur un numéro de port bien connu (COPS = 3288 [IANA]). Le PEP est responsable de l'initialisation de la connexion TCP à un PDP."

La dernière ligne de la déclaration dit que le PEP est responsable de l'initialisation de la connexion TCP. A l'inverse, dans le modèle IPCablecom, le CMTS (PEP) est celui qui se branche sur un port 3918 alloué, et c'est le Serveur de politique qui DOIT initialiser la connexion TCP au CMTS. C'est le contraire du modèle décrit dans le document RFC. Cependant, une fois que la connexion TCP est en place, le CMTS se comporte de façon cohérente avec le client, ou PEP, dans le protocole COPS. De même, le Serveur de politique (PEP) se branche sur le port 3918 alloué et c'est le gestionnaire d'application qui DOIT initialiser la connexion TCP au Serveur de politique.

Noter que la qualité de service dynamique d'IPCablecom multimédia et d'IPCablecom-T se branchent sur des ports différents, de sorte que le CMTS peut initialiser la session COPS avec le Type de client approprié.

Les détails du protocole COPS figurent dans [7]. Ce document RFC de l'IETF donne la description du protocole COPS de base, indépendant du Type de client. L'architecture IPCablecom est aussi alignée avec le document RFC 3084 [19] de l'IETF. COPS-PR déclare:

"dans COPS-PR, les demandes de politique décrivent le PEP et ses paramètres configurables (plutôt qu'un événement opérationnel). Si un changement survient dans ces paramètres de base, une demande de mise à jour est envoyée. Donc, les demandes ne sont pas produites très fréquemment. Les décisions ne sont pas nécessairement transposées directement en demandes, et elles sont produites le plus souvent lorsque le PDP répond aux événements extérieurs ou aux événements de PDP (mises à jour de politique)."

Lorsque ce concept est mappé dans l'architecture IPCablecom multimédia, le PEP produit une Demande au PDP, spécifiant un Outil Client. Cet Outil-client est ensuite utilisé dans les messages Décision futurs du PDP au PEP. Ces messages Décision portent les messages de commande de porte (c'est-à-dire, Etablir porte, Info de porte et Supprimer porte) définis pour les types de client de DQoS et du multimédia. L'Outil client est uniquement utilisé pour identifier l'association PDP-PEP.

Dans l'architecture IPCablecom multimédia, il peut y avoir de multiples gestionnaires d'application qui interagissent avec un ou plusieurs Serveurs de politique. Il y a une seule instance de session COPS IPCablecom multimédia par connexion TCP; et une session COPS IPCablecom multimédia se réfère aux messages de porte entre le PDP et le PEP associé à un seul Outil-client. Ceci signifie qu'il y a une seule connexion COPS-TCP entre un gestionnaire d'application et un Serveur de politique. De même, il peut y avoir un ou plusieurs Serveurs de politique qui parlent à un ou plusieurs CMTS. Lorsqu'il est connecté à plusieurs PDP, le PEP DOIT s'assurer que l'Outil-Client utilisé est unique pour chaque association.

6.4 Formats de message du protocole de commande de porte

Les messages du protocole de commande de porte DOIVENT être transportés dans les messages du protocole COPS. Le PDP et le PEP DOIVENT établir et utiliser une connexion TCP pour la communication, et utiliser les mécanismes spécifiés dans [11] pour sécuriser le conduit de communication.

6.4.1 Format de message commun COPS

Chaque message COPS comporte un en-tête COPS suivi d'un certain nombre d'objets typés. Le gestionnaire d'application, le Serveur de politique et le système CMTS DOIVENT utiliser le format de message commun COPS défini ci-dessous comme format de message pour tous les échanges de message. Dans les spécifications d'objet qui suivent, chaque rangée représente un mot de quatre octets car tous les objets s'alignent sur une limite de mot de quatre octets.

0		1	2	3
Version	Fanions	Op-Code	Type-de-Client	
Longueur du message				

Version est un champ de quatre bits qui donne le numéro de la version COPS en cours. Ce champ DOIT être mis à 1.

Fanions est un champ de quatre bits. Le bit de plus faible poids est le fanion de message sollicité. lorsque un message COPS est envoyé en réponse à un autre message (par exemple, une décision sollicitée envoyée en réponse à une demande) ce fanion DOIT être mis à 1. Dans d'autres cas (par exemple, une décision non sollicitée) le fanion NE DOIT PAS être établi (valeur = 0). En restant

dans le modèle DQoS, le premier message Décision envoyé en réponse à un message Demande est une réponse sollicitée et son fanion de message sollicité DOIT être établi. Tous les autres messages Décision sont non sollicités et le fanion de message sollicité DOIT être retiré. Tous les autres fanions DOIVENT être mis à zéro.

Op-code est un champ d'entier arithmétique de quatre bits qui donne l'opération COPS à effectuer. Les opérations COPS utilisées dans la présente Recommandation IPCablecom sont:

1 = demande (REQ, *request*)

2 = décision (DEC)

3 = rapport d'état (RPT, *report-state*)

4 = supprimer rapport d'état (DRQ, *delete request state*)

5 = demande d'état de synchronisation (SSQ, *synchronize state request)*

6 = client ouvert (OPN, *client-open)*

7 = client accepté (CAT, *client-accept*)

9 = garder en vie (KA, *keep-alive*)

10 = synchronisation terminée (SSC, *synchronize state complete*)

Type-de-client est un identifiant de deux octets représenté par un entier arithmétique. Pour l'usage d'IPCablecom multimédia, le Type de client DOIT être mis à client IPCablecom multimédia (0x800a). Pour les messages Garder en vie (Op-code = 9), le Type-de-client DOIT être mis à zéro, car le KA est utilisé pour la vérification de la connexion plutôt que pour la vérification de session selon le client.

Longueur de message est une valeur d'entier arithmétique de quatre octets qui donne la taille de la totalité du message en octets. Les messages DOIVENT être alignés sur des limites de quatre octets, de sorte que la longueur DOIT être un multiple de quatre.

Un ou plusieurs objets se trouvent à la suite de l'en-tête commun COPS. Tous les objets DOIVENT être conformes au même format d'objet dans lequel chaque objet comporte un ou plusieurs mots de quatre octets avec un en-tête de quatre octets, utilisant le format suivant.

0	1	2	3
Longueur		C-Num	C-Type
Contenu de l'objet			

Longueur est une valeur d'entier arithmétique de deux octets qui DOIT donner le nombre d'octets (y compris l'en-tête) qui compose l'objet. Si la longueur d'origine en octets n'est pas un multiple de quatre, un bourrage DOIT être ajouté à la fin de l'objet de façon qu'il soit aligné sur la prochaine limite de quatre octets.

C-Num identifie la classe d'information contenue dans l'objet, et le C-Type identifie le sous-type ou version des informations contenues dans l'objet. Les objets COPS standard (comme définis en [7]) utilisés dans la présente Recommandation, et leur valeurs de C-Num sont:

1 = outil (*handle*)

6 = décision

8 = erreur

9 = info spécifique du client (*client specific info*)

10 = temporisateur de maintien en vie (*keep-alive-timer*)

11 = identification de PEP (*PEP identification*)

Chacun de ces objets DOIT se conformer au format et aux règles relatives à l'objet individuel comme défini en [7].

6.4.2 Objets COPS supplémentaires pour la commande de porte

Comme avec les profils COPS-PR et COPS-RSVP, le Type de client IPCablecom définit un certain nombre de formats d'objet supplémentaires. Ces objets DOIVENT être placés à l'intérieur d'un objet Décision, C-Num = 6, C-Type = 4 (Données de décision spécifiques du client) lorsqu'ils sont transportés du PDP au PEP dans un message Décision. Ils DOIVENT aussi être placés dans un objet ClientSI, C-Num = 9, C-Type = 1 (ClientSI signalé) lorsqu'ils sont transportés du PEP au PDP dans un message Rapport.

Ces objets sont codés de la même façon que les objets spécifiques du client pour COPS-PR, et comme dans COPS-PR, ces objets sont numérotés en utilisant un espace de numéro spécifique du client, qui est indépendant de l'espace de numéro d'objet COPS de haut niveau. Pour cette raison, les numéros et types d'objet sont donnés respectivement comme S-Num et S-Type. S-Num et S-Type DOIVENT être d'un octet. Le champ Longueur de COPS DOIT être de deux octets. Les objets COPS supplémentaires sont définis dans les paragraphes suivants pour être utilisés dans IPCablecom multimédia.

6.4.2.1 ID de transaction

ID de transaction contient un jeton qui est utilisé par le gestionnaire d'application pour examiner les réponses du Serveur de politique et par le Serveur de politique pour examiner les réponses du système CMTS aux précédentes demandes. L'ID de transaction DOIT aussi contenir le type de commande qui identifie l'action à entreprendre ou la réponse. L'objet ID de transaction DOIT être conforme au format suivant.

Longueur = 8	S-Num = 1	S-Type = 1
Identifiant de transaction	Type de commande de porte	

L'Identifiant de transaction est une quantité d'entier arithmétique de deux octets qui DOIT être utilisé par le Serveur de politique et le gestionnaire d'application pour examiner la correspondance des réponses aux commandes. L'identifiant de transaction DOIT être mis à 0 lorsqu'il est inclus dans un message Rapport-d'état-de-porte.

Type de commande de porte est une valeur d'entier arithmétique de deux octets qui identifie le type de message de commande de porte et DOIT être un des suivants:

<Réservé>	1-3
Etablir porte	4
Acc-d'établir-porte	5
Erreur-établir-porte	6
Info-de-porte	7
Acc-d'info-de-porte	8
Erreur-d'info-de-porte	9
Supprimer-porte	10
Acc-supprimer-pporte	11
Erreur-supprimer-porte	12
Porte-ouverte	13
Porte-fermée	14
Etat-de-rapport-de-porte	15

6.4.2.2 AMID

AMID, l'identifiant du gestionnaire d'application, est une valeur d'entier arithmétique de quatre octets qui identifie le gestionnaire d'application responsable du traitement de la session. Le gestionnaire d'application DOIT inclure cet objet dans tous les messages qu'il envoie au Serveur de politique. Le Serveur de politique DOIT inclure l'AMID reçu dans tous les messages qu'il renvoie au système CMTS en réponse aux messages qu'il reçoit du gestionnaire d'application. Le CMTS DOIT inclure l'objet AMID reçu dans tous les messages qu'il envoie au Serveur de politique. Le Serveur de politique peut utiliser l'AMID dans les messages provenant du CMTS pour déterminer le gestionnaire d'application auquel il pourrait avoir besoin d'envoyer un message. L'objet AMID DOIT se conformer au format suivant.

Longueur = 8	S-Num = 2	S-Type = 1
AMID		

6.4.2.3 ID d'abonné

ID d'abonné est une valeur de quatre octets qui donne l'adresse IPv4 (représentée comme quatre valeurs d'octet enchaînées) de l'abonné pour cette demande de service. Cette adresse peut être l'adresse IP réelle de l'appareil CPE de l'abonné qui demande le service (si cette adresse est acheminable et visible depuis l'extrémité de tête) ou alors cette adresse peut être l'adresse IP du câblo-modem desservant cet abonné (si NAT est effectué derrière le câblo-modem). Cet objet est utilisé pour acheminer les messages de commande de porte au sein d'un réseau complexe d'éléments de serveurs de politique et de CMTS. Il peut aussi être utilisé pour la définition et la mise en application de règles de politique selon l'abonné. L'objet ID d'abonné DOIT se conformer au format suivant.

Longueur = 8	S-Num = 3	S-Type = 1
ID d'abonné (Adresse IPv4 de 4 octets)		

6.4.2.4 ID de porte

ID de porte est une valeur d'entier arithmétique de quatre octets qui identifie la porte référencée dans le message de commande, ou référencé par le CMTS pour un message de réponse. Le CMTS DOIT s'assurer que l'ID de porte est unique. Si le CMTS accepte aussi IPCablecom-T, l'ID de porte NE DOIT PAS dupliquer un ID de porte IPCablecom-T actuellement utilisé. L'objet ID de porte DOIT se conformer au format suivant.

Longueur = 8	S-Num = 4	S-Type = 1
ID de porte		

6.4.2.5 Spec de porte

Spec de porte définit un ensemble spécifique d'attributs associé à une porte. L'objet Spec de porte DOIT être conforme au format suivant.

Longueur = 16		S-Num = 5	S-Type = 1
Fanions	Champ DSCP/TOS	Gabarit DSCP/TOS	ID de classe de session
Temporisateur T1		Temporisateur T2	
Temporisateur T3		Réservé	

Fanions est une valeur de champ binaire d'un octet définie comme suit:

Bit 0: bit de direction, DOIT être soit zéro pour une porte aval, soit un pour une porte amont.

Bit 1: bit d'activation DSCP/TOS, DOIT être soit zéro pour désactiver Outrepasser DSCP, ou un pour activer.

Bits 2-7: réservé, DOIT être zéro.

ID de classe de session est une valeur d'entier arithmétique d'un octet qui identifie la politique de contrôle d'admission ou les paramètres appropriés qui doivent être appliqués à cette porte. La signification et l'interprétation de ce champ relève des politiques de l'administrateur. Le Serveur de politique et le CMTS PEUVENT accepter des politiques configurables fondées sur l'ID de classe de session. De telles politiques peuvent être utilisées pour limiter la bande passante en fonction des différent types de services ou sessions administrés.

Le champ DSCP/TOS est un champ binaire d'un octet [6] défini par les structures alternatives suivantes, dépendant de la stratégie de gestion de réseau. Ce champ, combiné au Gabarit DSCP/TOS d'un octet est utilisé pour identifier des bits particuliers au sein de l'octet IPv4 DSCP/TOS.

0	1	2	3	4	5	6	7
Point de code de services différenciés (DSCP, *differentiated services code point*)						Non utilisé	Non utilisé

0	1	2	3	4	5	6	7
Préséance IP			Type de service IP				Non utilisé

Si le bit 'activer' dans le champ des fanions de Spec de porte est établi, le CMTS DOIT alors marquer la valeur DSCP/TOS des paquets traversant le CMTS. Si le bit 'activer' est à zéro, le CMTS NE DOIT alors effectuer aucun marquage.

Les temporisateurs T1, T2 et T3 sont des entiers arithmétiques de deux octets spécifiés en secondes, et DOIVENT être utilisés comme indiqué dans le diagramme de transition de porte décrit au § 6.2. Une valeur de zéro pour T1 indique que la valeur provisionnée au CMTS pour le temporisateur DOIT être utilisée. T2 correspond au temporisateur DOCSIS Admis et T3 correspond au temporisateur DOCSIS Actif. Toutes les exigences correspondantes de DOCSIS s'appliquent à ces temporisateurs. Spécifiquement, une valeur de zéro pour l'un ou l'autre de ces temporisateurs indique que le temporisateur correspondant DOIT être désactivé.

6.4.2.6 Classeur

L'objet Classeur spécifie les règles de correspondance de paquet associées à une porte. Comme défini aux § 6.4.3.1 et 6.4.3.2, plusieurs objets Classeur peuvent être inclus dans Etablir porte pour permettre des règles complexes de classeur. L'objet Classeur DOIT se conformer au format suivant.

Longueur = 24		S-Num = 6	S-Type = 1
Réservé	ID de protocole	Champ DSCP/TOS	Gabarit DSCP/TOS
Adresse IP de source (4 octets)			
Adresse IP de destination (4 octets)			
Port de source		Port de destination	
Priorité	Réservé		

Adresse IP de source et Adresse IP de destination DOIT être une paire d'adresses IPv4 de quatre octets, ou zéro pour une non-correspondance (c'est-à-dire, une spécification de caractère générique qui ne correspond à aucune demande de l'adaptateur MTA).

Port de source et Port de destination DOIT être une paire de valeurs d'entiers arithmétiques de deux octets, ou zéro pour une non-correspondance.

Le champ DSCP/TOS est un champ d'un octet qui DOIT se conformer aux structures alternatives suivantes:

0	1	2	3	4	5	6	7
Point de code de services différenciés (DSCP)						Non utilisé	Activé

0	1	2	3	4	5	6	7
Préséance IP			IP TOS				Activé

Gabarit DSCP/TOS est un champ binaire d'un octet qui fournit un gabarit binaire qui sert à choisir les bits pertinents dans la valeur du champ DSCP/TOS d'accompagnement.

Si le bit 'Activé' est établi, le CMTS DOIT alors utiliser ces valeurs pour construire le champ Gabarit et Gamme de Type de service IP spécifié dans son échange de messages DSx. Si le bit 'Activé' est à zéro, le CMTS DOIT alors omettre les valeurs Gabarit et Gamme de type de service IP dans son échange de messages DSx et exclure l'octet TOS IP du processus de classement de paquet.

Priorité est un champ d'un octet qui permet une différentiation entre les classeurs qui pourraient se chevaucher. Une valeur par défaut de 64 DEVRAIT être utilisée si une valeur de priorité spécifique n'est pas nécessaire. Pour un examen plus approfondi du champ Priorité, se reporter au § B.C.2.1.3.5 de [1].

6.4.2.7 Profils de trafic

Il y a trois façons différentes d'exprimer un Profil de trafic. Le Profil de trafic peut être exprimé via une Spec de flux, via un Nom de classe de service DOCSIS, ou via des paramètres spécifiques DOCSIS. Les trois méthodes sont distinguées via une valeur de S-Type différente dans l'objet Profil de trafic (S-Num = 7). Un S-Type de 1 indique que l'objet contient un Profil de trafic spécifié dans le format de Spec de flux RSVP. Un S-Type de 2 indique que l'objet contient un Profil de trafic spécifié dans le format de Nom de classe de service DOCSIS. Un S-Type de 3 indique que l'objet contient un Profil de trafic qui est spécifié via une combinaison de Spec de flux RSVP et de paramètres spécifiques de DOCSIS.

Tous les Profils de trafic utilisent la sémantique "remplacer", qui signifie que les enveloppes présentes dans ce Profil de trafic remplacent toutes les enveloppes existantes associées à la porte et au flux de service correspondant. Ainsi, tous les paramètres de trafic associés à une porte donnée DOIVENT être inclus dans chaque message qui inclut un Profil de trafic.

Tous les Profils de trafic partagent un champ commun appelé Champ d'enveloppe. Ce champ est un champ binaire qui signale les types d'enveloppe (c'est-à-dire, Autorisé, Réservé, et Engagé) qui sont présents dans l'objet. Une valeur de 1 dans un champ binaire donné indique que le type d'enveloppe est présent dans le Profil de trafic.

- bit 0: enveloppe autorisée;
- bit 1: enveloppe réservée;
- bit 2: enveloppe engagée.

Ainsi un schéma binaire de 001 (ou 0x01) indique la présence de la seule Enveloppe autorisée, alors qu'une valeur de 111 (ou 0x7) indique la présence des trois enveloppes. Seules les valeurs suivantes sont légales: 001, 011 et 111; le champ Enveloppe DOIT être réglé à une de ces trois valeurs légales. D'autres limitations sur la valeur du champ Enveloppe peuvent résulter de l'état en cours de la porte. Pour plus d'informations, se reporter au § 6.2

Alors que tous les Profils de trafic se terminent en fournissant la qualité de service sur le réseau d'accès, il est important de noter plusieurs différences subtiles entre les mécanismes de signalisation. Comme noté précédemment, la conversion d'une Spec de flux (S-Type 1) en paramètres DOCSIS par le CMTS est généralement moins efficace que la spécification des paramètres DOCSIS eux-même. Cela dit, la spécification explicite des paramètres DOCSIS

(S-Types 3-7) n'est pas non plus une panacée, la base MIB de qualité de service ne mémorise que les informations sur les flux de service nommés dans ses Tableaux d'enregistrement de flux de service. Et donc, seuls les flux crées via S-Type 2 auront des informations de qualité de service enregistrées sur ce tableau. Pour certains, ce peut être un gros problème, pour l'élimination des erreurs et pour le simple suivi opérationnel général, cette finesse devrait être prise en compte par les opérateurs et vendeurs de gestionnaires d'application en évaluant les alternatives de signalisation du Profil de trafic fournies dans la présente Recommandation.

6.4.2.7.1 Spec de flux

L'objet Spec de flux définit le Profil de trafic associé à une porte selon un schéma de paramètrisation du type RSVP. La transposition de ces paramètres en paramètres DOCSIS est spécifiée au § 8. L'objet Spec de flux DOIT se conformer à la spécification suivante:

Longueur = 36 ou 64 ou 92		S-Num = 7	S-Type = 1
Enveloppe	Numéro de service	Réservé	Réservé
Enveloppe autorisée			
Débit de seau de jeton [r] (nombre IEEE à virgule flottante)			
Taille de seau de jeton [b] (nombre IEEE à virgule flottante)			
Débit de crête de données (p) (nombre IEEE à virgule flottante)			
Unité régulée minimale [m] (entier)			
Taille maximale de paquet [M] (entier)			
Rate [R] (nombre IEEE à virgule flottante)			
Terme de surlongueur [S] (entier)			
Enveloppe réservée (facultatif)			
Débit de seau de jeton [r] (nombre IEEE à virgule flottante)			
Taille de seau de jeton [b] (nombre IEEE à virgule flottante)			
Débit de crête de données (p) (nombre IEEE à virgule flottante)			
Unité régulée minimale [m] (entier)			
Taille maximale de paquet [M] (entier)			
Débit [R] (nombre IEEE à virgule flottante)			
Terme de surlongueur [S] (entier)			
Enveloppe engagée (facultatif)			
Débit de seau de jeton [r] (nombre IEEE à virgule flottante)			
Taille de seau de jeton [b] (nombre IEEE à virgule flottante)			
Débit de crête de données (p) (nombre IEEE à virgule flottante)			
Unité régulée minimale [m] (entier)			
Taille maximale de paquet [M] (entier)			
Débit [R] (nombre IEEE à virgule flottante)			
Terme de surlongueur [S] (entier)			

Le champ Numéro de service correspond au numéro de service de Spec de flux RSVP tel que défini en [3]. Si Numéro de service est réglé à cinq, cela indique le service à charge contrôlée et le système CMTS DOIT utiliser seulement les valeurs de la TSpec (c'est-à-dire, les paramètres du seau de jetons) pour effectuer les opérations d'autorisation, de réservation et d'engagement nécessaires. Pour le service à charge contrôlée, le système CMTS DOIT ignorer les champs RSpec R et S.

Si Numéro de service est réglé à deux, cela signale le service Garanti et le CMTS DOIT utiliser les deux valeurs TSpec et RSpec pour effectuer les opérations d'autorisation, de réservation et d'engagement nécessaires.

Les valeurs r, b, p, m, M, R, et S sont définies et décrites au § 9.

6.4.2.7.2 Nom de classe de service DOCSIS

L'objet Nom de classe de service DOCSIS définit le Nom de classe de service préconfiguré associé à une porte. L'objet Nom de classe de service DOCSIS DOIT se conformer à la spécification suivante:

Longueur = 12 ou 16 ou 20 ou 24		S-Num = 7	S-Type = 2
Enveloppe	Réservé	Réservé	Réservé
Nom de classe de service			

Le Nom de classe de service DOIT être une chaîne ASCII de 2 à 16 octets terminés par des zéros. (Se reporter au § B.C.2.2.3.4 de [1]). Ce nom DOIT être bourré avec des octets à zéro pour s'aligner sur la limite des quatre octets.

Noter qu'à la différence d'une Spec de flux, Profil de trafic va permettre à des paramètres différents d'être associés à chaque enveloppe, le Profil de trafic de nom de classe de service DOCSIS accepte différents états de porte comme spécifié par le champ Enveloppe, mais chaque enveloppe est définie par le même nom de classe de service DOCSIS associé. Cela permet d'avoir des opérations d'engagement en deux phases utilisant les Noms de classe de service DOCSIS, mais chaque enveloppe DOIT être identique. Noter aussi qu'il est possible de changer le Nom de classe de service DOCSIS associé à une porte, mais qu'un tel changement s'applique à toutes les enveloppes associées à une porte donnée.

6.4.2.7.3 Service au mieux

L'objet Au mieux définit le Profil de trafic associé à une porte par un schéma de paramétrisation amont spécifique de DOCSIS. L'objet Au mieux DOIT se conformer à la spécification suivante:

Longueur = 32, 56 ou 80		S-Num = 7	S-Type = 3
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Priorité de trafic	Réservé		
Politique de transmission de demande			
Débit de trafic soutenu maximal			
Rafale de trafic maximal			
Débit de trafic réservé maximal			
Taille supposée de paquet au débit de trafic réservé minimal		Réservé	
Enveloppe réservée (facultatif)			
Priorité de trafic	Réservé		
Politique de transmission de demande			
Débit de trafic soutenu maximal			
Rafale de trafic maximal			

Débit de trafic réservé minimal	
Taille supposée de paquet au débit de trafic réservé minimal	Réservé
Enveloppe engagée (facultatif)	
Priorité de trafic	Réservé
Politique de transmission de demande	
Débit au trafic réservé maximal	
Rafale de trafic maximal	
Débit de trafic réservé minimal	
Taille supposée de paquet au débit de trafic réservé minimal	Réservé

Priorité de trafic est un champ d'un octet d'entier arithmétique spécifiant la priorité relative allouée au flux de service par rapport aux autres flux. Ce champ est complètement défini au § B.C.2.2.5.1 de [1]. Une Priorité de trafic par défaut de 0 DEVRAIT être utilisée si une valeur de Priorité de trafic spécifique n'est pas exigée.

Politique de demande/transmission est un champ binaire de quatre octets comme défini au § B.C.2.2.6.3 de [1]. Une politique de demande/transmission par défaut de 0 DEVRAIT être utilisée si une valeur de Politique de demande/transmission spécifique n'est pas exigée.

Débit au trafic soutenu maximal est un champ d'entier arithmétique de quatre octets spécifiant le paramètre débit, en bit/s, pour une limite de débit en seau de jetons pour ce Flux de service. Ce champ est complètement défini au § B.C.2.2.5.2 de [1]. Une valeur de 0 indique qu'il n'est pas demandé de mise en application explicite de débit soutenu maximal. Un Débit au trafic soutenu maximal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic soutenu maximal spécifique n'est pas exigé.

Rafale de trafic maximal est un champ d'entier arithmétique de quatre octets spécifiant la taille du seau de jetons, en octets, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.3 de [1]. Une Rafale de trafic maximal par défaut de 3044 octets DEVRAIT être utilisée si une Rafale de trafic maximal spécifique n'est pas exigée. La valeur de ce paramètre n'a pas d'effet sauf lorsqu'une valeur différente de zéro est fournie pour le paramètre Débit au trafic soutenu maximal.

Débit de trafic réservé minimal est un champ d'entier arithmétique de quatre octets spécifiant le débit minimal, en bit/s, réservé pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.4 de [1]. Un débit de trafic réservé minimal par défaut de 0 DEVRAIT être utilisé si un Débit de trafic réservé minimal spécifique n'est pas exigé.

Taille supposée de paquet au débit de trafic réservé minimal est un champ d'entier arithmétique de deux octets spécifiant une taille de paquet minimal supposée, en octets, pour laquelle le Débit au trafic réservé minimal sera fourni pour ce flux. ce champ est complètement défini au § B.C.2.2.5.5 de [1]. Une Taille supposée de paquet au débit de trafic réservé minimal par défaut de 0 DEVRAIT être utilisée si une Taille supposée de paquet au débit de trafic réservé minimal spécifique n'est pas exigée. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non des octets à zéro.

6.4.2.7.4 Service d'interrogation en temps différé

L'objet Interrogation en temps différé définit le Profil de trafic associé à une porte amont par un schéma de paramétrisation spécifique de DOCSIS. L'objet Interrogation en temps différé DOIT se conformer à la spécification suivante:

Longueur = 36, 64 ou 92		S-Num = 7	S-Type = 4
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Priorité de trafic	Réservé		
Politique de transmission de demande			
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit de trafic réservé minimal supposé		Réservé	
Intervalle d'interrogation nominal			
Enveloppe réservée (facultatif)			
Priorité de trafic	Réservé		
Politique de transmission de demande			
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit de trafic réservé minimal supposé		Réservé	
Intervalle d'interrogation nominal			
Enveloppe engagée (facultatif)			
Priorité de trafic	Réservé		
Politique de transmission de demande			
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit de trafic réservé minimal supposé		Réservé	
Intervalle d'interrogation nominal			

Priorité de trafic est un champ d'entier arithmétique d'un octet spécifiant la priorité relative allouée au flux de service par rapport aux autres flux. Ce champ est complètement défini au § B.C.2.2.5.1 de [1]. Une Priorité de trafic par défaut de 0 DEVRAIT être utilisée si une valeur de Priorité de trafic spécifique n'est pas exigée. Politique de demande/transmission est un champ binaire de quatre octets comme défini au § B.C.2.2.6.3 de [1].

NOTE – Pour ce type de programmation de flux de service, il n'y a pas de valeur par défaut pour Politique de demande/transmission et toutes les valeurs (y compris 0) ont une signification dans DOCSIS.

Débit au trafic soutenu maximal est un champ d'entier arithmétique de quatre octets spécifiant le paramètre débit, en bit/s, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.2 de [1]. Une valeur de 0 indique qu'aucune mise en application explicite de Débit soutenu maximal n'est demandée. Un Débit au trafic soutenu maximal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic soutenu maximal spécifique n'est pas exigé.

Rafale de trafic maximal est un champ d'entier arithmétique de quatre octets spécifiant la taille du seau de jetons, en octets, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.3 de [1]. Une Rafale de trafic maximal par défaut de 3044 octets DEVRAIT être utilisée si une Rafale de trafic maximal spécifique n'est pas exigée. La

valeur de ce paramètre n'a pas d'effet sauf lorsqu'une valeur différente de zéro a été fournie pour le paramètre Débit au trafic soutenu maximal.

Débit au trafic réservé minimal est un champ d'entier arithmétique de quatre octets spécifiant le débit minimal, en bit/s, réservé pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.4 de [1]. Un Débit au trafic réservé minimal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic réservé minimal spécifique n'est pas exigé.

Taille de paquet au débit de trafic réservé minimal supposé est un champ d'entier arithmétique de deux octets spécifiant une taille minimale de paquet supposée, en octets, pour laquelle le Débit au trafic réservé minimal sera fourni pour ce flux. Ce champ est complètement défini au § B.C.2.2.5.5 de [1]. Une Taille de paquet au débit au trafic réservé minimal supposé par défaut de 0 DEVRAIT être utilisée si une taille de paquet au débit de trafic réservé minimal supposé spécifique n'est pas exigée. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non des octets à zéro.

Intervalle d'interrogation nominal est un champ d'entier arithmétique de quatre octets spécifiant l'intervalle nominal (en unités de micro-secondes) entre les opportunités de demande en monodiffusion successives pour ce flux de service sur le canal amont. Ce champ est complètement défini au § B.C.2.2.6.4 de [1]. Un Intervalle d'interrogation nominal par défaut de 0 DEVRAIT être utilisé si un Intervalle d'interrogation nominal spécifique n'est pas exigé. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non 0 microseconde.

6.4.2.7.5 Service d'interrogation en temps réel

L'objet Interrogation en temps réel définit le Profil de trafic associé à une porte amont au moyen d'un schéma de paramétrisation spécifique de DOCSIS. L'objet Interrogation en temps réel DOIT suivre la spécification ci-après:

Longueur = 36, 64 ou 92		S-Num = 7	S-Type = 4
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Politique de transmission de demande			
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit au trafic réservé minimal supposé		Réservé	
Intervalle d'interrogation nominal			
Gigue d'interrogation tolérée			
Enveloppe réservée (facultatif)			
Politique de transmission de demande			
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit au trafic réservé minimal supposé		Réservé	
Intervalle d'interrogation nominal			
Gigue d'interrogation tolérée			
Enveloppe engagée (facultatif)			
Politique de transmission de demande			

Débit au trafic soutenu maximal	
Rafale de trafic maximal	
Débit au trafic réservé minimal	
Taille de paquet au débit au trafic réservé minimal supposé	Réservé
Intervalle d'interrogation nominal	
Gigue d'interrogation tolérée	

Politique de demande/transmission est un champ binaire de quatre octets comme défini au § B.C.2.2.6.3 de [1].

NOTE – Pour ce Type de programmation de flux de service il n'y a pas de valeur par défaut pour Politique de demande/transmission et toutes les valeurs (y compris 0) ont une signification dans DOCSIS.

Débit au trafic soutenu maximal est un champ d'entier arithmétique de quatre octets spécifiant le paramètre débit, en bit/s, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.2 de [1]. Une valeur de 0 indique qu'aucune mise en application explicite de Débit soutenu maximal n'est demandée. Un Débit au trafic soutenu maximal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic soutenu maximal spécifique n'est pas exigé.

Rafale de trafic maximal est un champ d'entier arithmétique de quatre octets spécifiant la taille du seau de jetons, en octets, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.3 de [1]. Une Rafale de trafic maximal par défaut de 3044 octets DEVRAIT être utilisée si une Rafale de trafic maximal spécifique n'est pas demandée. La valeur de ce paramètre n'a pas d'effet sauf lorsqu'une valeur différente de zéro a été fournie pour le paramètre Débit au trafic soutenu maximal.

Débit au trafic réservé minimal est un champ d'entier arithmétique de quatre octets spécifiant le débit minimal, en bit/s, réservé pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.4 de [1]. Un Débit au trafic réservé minimal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic réservé minimal spécifique n'est pas exigé.

Taille de paquet au débit de trafic réservé minimal supposé est un champ d'entier arithmétique de deux octets spécifiant une taille de paquet minimale supposée, en octets, pour laquelle le Débit au trafic réservé minimal sera fourni pour ce flux. Ce champ est complètement défini au § B.C.2.2.5.5 de [1]. Une Taille de paquet au débit au trafic réservé minimal supposé par défaut de 0 DEVRAIT être utilisée si une Taille de paquet au débit au trafic réservé minimal supposé spécifique n'est pas exigée. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non des octets à zéro.

Intervalle d'interrogation nominal est un champ d'entier arithmétique de quatre octets spécifiant l'intervalle nominal (en unités de micro-secondes) entre les opportunités de demande en monodiffusion successives pour ce flux de service sur le canal amont. Ce champ est complètement défini au § B.C.2.2.6.4 de [1]. Pour ce Type de programmation de flux de service il n'y a pas de valeur par défaut pour Intervalle d'interrogation nominal.

Gigue d'interrogation tolérée est un champ d'entier arithmétique de quatre octets spécifiant la quantité de temps maximal pendant lequel l'intervalle de demande en monodiffusion peut être retardé par rapport à la programmation périodique nominale (mesurée en micro-secondes). Ce champ est complètement défini au § B.C.2.2.6.5 de [1]. Une Gigue d'interrogation tolérée par défaut de 0 DEVRAIT être utilisée si une Gigue d'interrogation tolérée spécifique n'est pas exigée. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre – et non 0 micro-seconde.

6.4.2.7.6 Service d'allocation non sollicitée

L'objet Allocation non sollicitée définit le Profil de trafic associé à une porte amont au moyen d'un schéma de paramétrisation spécifique de DOCSIS. L'objet Allocation non sollicitée DOIT se conformer à la spécification suivante:

Longueur = 36, 64 ou 92		S-Num = 7	S-Type = 6
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			
Enveloppe réservée (facultatif)			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			
Enveloppe engagée (facultatif)			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			

Politique de demande/transmission est un champ binaire de quatre octets comme défini au § B.C.2.2.6.3 de [1].

NOTE – Pour ce Type de programmation de flux de service il n'y a pas de valeur par défaut pour Politique de demande/transmission et toutes les valeurs (y compris 0) ont une signification dans DOCSIS.

Taille d'allocation non sollicitée est un champ d'entier arithmétique de deux octets spécifiant la taille d'allocation (en octets) comme défini au § B.C.2.2.6.6 de [1]. Il n'y a pas de valeur par défaut de Taille d'allocation non sollicitée.

Allocations par intervalle est un champ d'entier arithmétique d'un octet spécifiant le nombre d'allocations par intervalle d'allocation nominal comme défini au § B.C.2.2.6.9 de [1]. Il n'y a pas de valeur par défaut de Allocations par intervalle, mais une valeur de 1 est recommandée.

Intervalle d'allocation nominal est un champ d'entier arithmétique de quatre octets spécifiant le temps nominal entre des opportunités d'allocation de données successives pour ce flux de service (en micro-secondes) comme défini au § B.C.2.2.6.7 de [1]. Il n'y a pas de valeur par défaut de Intervalle d'allocation nominal.

Gigue d'allocation tolérée est un champ d'entier arithmétique de quatre octets spécifiant la quantité de temps maximale dont peuvent être retardées les opportunités de transmission par rapport à la programmation périodique nominale (en micro-secondes) comme défini au § B.C.2.2.6.8 de [1]. Il n'y a pas de valeur par défaut de Gigue d'allocation tolérée.

6.4.2.7.7 Service d'allocation non sollicitée avec Détection d'activité

L'objet allocation non sollicitée avec détection d'activité définit le Profil de trafic associé à une porte amont au moyen d'un schéma de paramétrisation spécifique de DOCSIS. L'objet allocation non sollicitée avec détection d'activité DOIT se conformer à la spécification suivante:

Longueur = 36, 64 ou 92		S-Num = 7	S-Type = 7
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			
Intervalle d'interrogation nominal			
Gigue d'interrogation tolérée			
Enveloppe réservée (facultatif)			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			
Intervalle d'interrogation nominal			
Gigue d'interrogation tolérée			
Enveloppe engagée (facultatif)			
Politique de transmission de demande			
Taille d'allocation non sollicitée		Allocations/ Intervalle	Réservé
Intervalle d'allocation nominal			
Gigue d'allocation tolérée			
Intervalle d'interrogation nominal			
Gigue d'interrogation tolérée			

Politique de demande/transmission est un champ binaire de quatre octets comme défini au § B.C.2.2.6.3 de [1].

NOTE – Pour ce Type de programmation de flux de service il n'y a pas de valeur par défaut pour Politique de demande/transmission et toutes les valeurs (y compris 0) ont une signification dans DOCSIS.

Taille d'allocation non sollicitée est un champ d'entier arithmétique de deux octets spécifiant la taille d'allocation (en octets) comme défini au § B.C.2.2.6.6 de [1]. Il n'y a pas de valeur par défaut pour Taille d'allocation non sollicitée.

Allocations par intervalle est un champ d'entier arithmétique d'un octet spécifiant le nombre d'allocations par Intervalle d'allocation nominal comme défini au § B.C.2.2.6.9 de [1]. Il n'y a pas de valeur par défaut pour Allocations par intervalle, mais une valeur de 1 est recommandée.

Intervalle d'allocation nominal est un champ d'entier arithmétique de quatre octets spécifiant la durée nominale entre des opportunités d'allocation de données successives pour ce flux de service

(en micro-secondes) comme défini au § B.C.2.2.6.7 de [1]. Il n'y a pas de valeur par défaut pour Intervalle d'allocation nominal.

Gigue d'allocation tolérée est un champ d'entier arithmétique de quatre octets spécifiant la durée maximale du retard des opportunités de transmission par rapport à la programmation périodique nominale (en micro-secondes) comme défini au § B.C.2.2.6.8 de [1]. Il n'y a pas de valeur par défaut pour Gigue d'allocation tolérée.

Intervalle d'interrogation nominal est un champ d'entier arithmétique de quatre octets spécifiant l'intervalle nominal (en micro-secondes) entre des opportunités de demande de monodiffusion successives pour ce flux de service sur le canal amont. Ce champ est complètement défini au § B.C.2.2.6.4 de [1]. Il n'y a pas de valeur par défaut pour Intervalle d'interrogation nominal.

Gigue d'interrogation tolérée est un champ d'entier arithmétique de quatre octets spécifiant la durée maximale du retard que peut subir l'intervalle de demande en monodiffusion par rapport à la programmation périodique nominale (mesurée en micro-secondes). Ce champ est complètement défini au § B.C.2.2.6.5 de [1]. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non 0 micro-seconde.

6.4.2.7.8 Service aval

L'objet Aval définit le Profil de trafic associé à une porte au moyen d'un schéma de paramétrisation spécifique de DOCSIS pour l'aval. L'objet Aval DOIT se conformer à la spécification suivante:

Longueur = 32, 56 ou 80		S-Num = 7	S-Type = 8
Enveloppe	Réservé	Réservé	Réservé
Enveloppe autorisée			
Priorité de trafic	Réservé		
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit au trafic réservé minimal supposé		Réservé	
Temps de latence aval maximal			
Enveloppe réservée (facultatif)			
Priorité de trafic	Réservé		
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit au trafic réservé minimal supposé		Réservé	
Temps de latence aval maximal			
Enveloppe engagée (facultatif)			
Priorité de trafic	Réservé		
Débit au trafic soutenu maximal			
Rafale de trafic maximal			
Débit au trafic réservé minimal			
Taille de paquet au débit au trafic réservé minimal supposé		Réservé	
Temps de latence aval maximal			

Priorité de trafic est un champ d'entier arithmétique d'un octet spécifiant la priorité relative allouée au flux de service par rapport aux autres flux. Ce champ est complètement défini au § B.C.2.2.5.1 de [1]. Une Priorité de trafic par défaut de 0 DEVRAIT être utilisée si une valeur de Priorité de trafic spécifique n'est pas exigée.

Débit au trafic soutenu maximal est un champ d'entier arithmétique de quatre octets spécifiant le paramètre débit, en bit/s, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.2 de [1]. Une valeur de 0 indique qu'aucune mise en application explicite de Débit soutenu maximal n'est demandée. Un Débit au trafic soutenu maximal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic soutenu maximal spécifique n'est pas exigée.

Rafale de trafic maximal est un champ d'entier arithmétique de quatre octets spécifiant la taille du seau de jetons, en octets, pour une limite de débit en seau de jetons pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.3 de [1]. Une Rafale de trafic maximal par défaut de 3044 octets DEVRAIT être utilisée si une Rafale de trafic maximal spécifique n'est pas exigée. La valeur de ce paramètre n'a pas d'effet sauf lorsqu'une valeur différente de zéro a été fournie pour le paramètre Débit au trafic soutenu maximal.

Débit au trafic réservé minimal est un champ d'entier arithmétique de quatre octets spécifiant le débit minimal, en bit/s, réservé pour ce flux de service. Ce champ est complètement défini au § B.C.2.2.5.4 de [1]. Un Débit au trafic réservé minimal par défaut de 0 DEVRAIT être utilisé si un Débit au trafic réservé minimal spécifique n'est pas exigé.

Taille de paquet au débit de trafic réservé minimal supposé est un champ d'entier arithmétique de deux octets spécifiant une taille de paquet minimale supposée, en octets, pour laquelle le Débit au trafic réservé minimal sera fourni pour ce flux. Ce champ est complètement défini au § B.C.2.2.5.5 de [1]. Une Taille de paquet au débit au trafic réservé minimal supposé par défaut de 0 DEVRAIT être utilisée si une Taille de paquet au débit de trafic réservé minimal supposé n'est pas exigée. A réception d'une valeur de 0 le CMTS DOIT utiliser sa taille par défaut spécifique de l'implémentation pour ce paramètre, et non des octets à zéro.

Temps de latence aval maximal est un champ d'entier arithmétique de quatre octets spécifiant le délai maximal entre la réception d'un paquet sur l'interface NSI du CMTS et la transmission du paquet à son interface RF, comme défini au § B.C.2.2.7.1 de [1]. Un Temps de latence aval maximal par défaut de 0 DEVRAIT être utilisé si un Temps de latence aval maximal spécifique n'est pas exigé. A réception d'une valeur de 0, le CMTS NE DOIT PAS inclure ce paramètre dans sa signalisation DOCSIS pour ce flux de service.

6.4.2.8 Info de génération d'événement

L'objet Info de génération d'événement contient toutes les informations nécessaires pour prendre en charge les messages d'événement comme spécifié et prescrit dans la Rec. UIT-T J.164. L'objet Info de génération d'événement DOIT se conformer à la spécification suivante:

Longueur = 44	S-Num = 8	S-Type = 1
Adresse IP de serveur d'archivage primaire (4 octets)		
Port de serveur d'archivage primaire	Réservé	
Adresse IP de serveur d'archivage secondaire (4-octets)		
Port de serveur d'archivage secondaire	Réservé	
ID de corrélation de facturation (24 octets)		

Adresse IP de serveur d'archivage primaire est un champ de quatre octets qui DOIT contenir l'adresse IPv4 du RKS primaire à qui doivent être envoyés les enregistrements d'événement.

Le champ Port de serveur d'archivage primaire est un entier arithmétique de deux octets qui DOIT contenir le numéro de port sur le RKS primaire où doivent être envoyés les enregistrements d'événements.

Adresse IP de serveur d'archivage secondaire est un champ de quatre octets qui DOIT contenir l'adresse IPv4 du RKS secondaire à qui les enregistrements doivent être envoyés si le RKS primaire est indisponible.

Port de serveur d'archivage secondaire est un entier arithmétique de deux octets qui DOIT contenir le numéro de port sur le RKS secondaire où doivent être envoyés les enregistrements d'événements.

ID de corrélation de facturation est un champ de 24 octets qui DOIT contenir l'identifiant alloué par le gestionnaire d'application ou le Serveur de politique pour tous les enregistrements qui se rapportent à cette session. Voir en [10] la définition et le format de cet attribut.

6.4.2.9 Limite d'utilisation en volume

L'objet Limite d'utilisation en volume spécifie la quantité de données qui peut être transmise sur cette porte avant de toucher le seuil de volume. Cet objet est FACULTATIF dans un message Etablir porte et Acc d'info de porte. Il NE DOIT PAS être utilisé dans tout autre message. L'objet Limite d'utilisation en volume DOIT se conformer à la spécification suivante:

Longueur = 12	S-Num = 9	S-Type = 1
Limite d'utilisation		

Limite d'utilisation est un entier arithmétique de huit octets défini en kilo octets. Une valeur de zéro indique qu'aucune limite de volume n'est imposée. Les octets comptés jusqu'à la limite sont depuis l'octet après le HCS d'en-tête MAC de DOCSIS jusqu'à la fin du CRC pour tout paquet transmis sur le flux de service associé à cette porte.

6.4.2.10 Limite de temps d'utilisation

L'objet Limite de temps d'utilisation spécifie la quantité de temps pendant laquelle une porte peut rester engagée avant de toucher le seuil de la limite de temps. L'objet Limite de temps d'utilisation DOIT suivre la spécification ci-après:

Longueur = 8	S-Num = 10	S-Type = 1
Limite de temps		

Limite de temps est un entier arithmétique de quatre octets défini en secondes. C'est une limite sur la quantité de temps pendant lequel une porte peut être dans l'état Engagé. Cet objet est FACULTATIF dans un message Etablir porte. S'il est inclus dans un Etablir porte, cet objet DOIT être mémorisé par le CMTS et fourni en réponse à toute interrogation de porte subséquente. Alors que le gestionnaire d'application est REQUIS de supprimer les portes associées à une session de média qui a dépassé sa Limite de temps d'utilisation, le CMTS ou Serveur de politique PEUT utiliser cet objet pour réguler la mise en application par le gestionnaire d'application des Limites de temps d'utilisation. Le gestionnaire d'application ou Serveur de politique PEUT aussi demander cet objet dans le cadre d'une reprise sur erreur ou autre mécanisme.

Une valeur de zéro indique qu'il n'y a pas de limite de temps pour la porte associée.

6.4.2.11 Données Opaques

L'objet Données opaques contient des informations qu'un Serveur de politique ou gestionnaire d'application PEUT mémoriser sur un système CMTS et qui restent opaques pour le CMTS. L'objet Données opaques est FACULTATIF dans un message Etablir porte. Il NE DOIT PAS être utilisé dans tout autre message produit par le PDP au PEP. Si l'objet est présent, le CMTS DOIT mémoriser localement les Données opaques, et les inclure dans tous les messages qu'il génère vers le Serveur de politique associé à la porte.

Si l'objet Données opaques est inclus dans un message Etablir porte du gestionnaire d'application à un Serveur de politique, le Serveur de politique DOIT faire suivre cet objet au CMTS. La longueur des Données opaques est fixée à 8 octets.

Longueur = 12	S-Num = 11	S-Type = 1
Données opaques		

6.4.2.12 Info d'heure de porte

L'objet Info d'heure de porte contient un horodatage qui représente l'heure à laquelle la porte est entrée dans l'état Engagé pour la dernière fois. L'objet Info d'heure de porte DOIT se conformer à la spécification suivante:

Longueur = 8	S-Num = 12	S-Type = 1
Temps engagé		

Temps engagé est un entier arithmétique de quatre octets indiquant le nombre de secondes pendant lesquelles cette porte a été dans l'état Engagé.

NOTE – Ceci est destiné à être identique au docsQosServiceFlowTimeActive tiré de la base MIB de qualité de service de [17].

6.4.2.13 Info d'utilisation de porte

L'objet Info d'utilisation de porte contient un compteur qui indique le nombre de kilo octets transmis sur cette porte. L'objet Info d'utilisation de porte DOIT se conformer à la spécification suivante:

Longueur = 8	S-Num = 13	S-Type = 1
Compteur d'octet		

Compteur d'octet est un entier arithmétique de quatre octets qui représente le nombre d'octets (compté depuis le HCS d'en-tête MAC de DOCSIS jusqu'à la fin du CRC) qui ont traversé le flux de service associé à la porte en unités de 1024 octets.

6.4.2.14 Erreur IPCablecom

L'objet Erreur IPCablecom contient des informations sur le type d'erreur survenue. L'erreur est générée en réponse à une commande Commande de porte et est contenue dans les messages Err Etablir porte, Err d'Info de porte et Err Supprimer porte. L'objet Erreur IPCablecom DOIT se conformer à la spécification suivante:

Longueur = 8	S-Num = 14	S-Type = 1
Code d'erreur	Sous-code d'erreur	

Code d'erreur est un entier arithmétique de deux octets représentant une erreur spécifique et DOIT être un des suivants:

1 = ressources insuffisantes

2 = ID de porte inconnu

6 = objet demandé manquant

7 = objet non valide

8 = limite d'utilisation en volume dépassée

9 = limite de temps d'utilisation dépassée

10 = limite de classe de session dépassée

11 = nom de classe de service indéfinie

12 = enveloppe incompatible

13 = ID d'abonné non valide

14 = AMID non autorisé

15 = nombre de Classeurs non accepté

127 = autre erreur, non spécifiée

Sous-code d'erreur est un champ d'entier arithmétique de deux octets utilisé pour donner des informations complémentaires sur l'erreur. Dans le cas des codes d'erreur 6 et 7, ce champ DOIT contenir le S-Num et S-Type de l'objet qui manque ou est erroné. L'ordre des valeurs de S-Num et S-Type au sein du Sous-code d'erreur DOIT être le même que dans le message d'origine. Dans les cas où existent plusieurs alternatives valides pour le S-Type d'un objet manquant, cette portion du Sous-code d'erreur DOIT être mise à zéro. Dans le cas du code d'erreur 15, le champ sous-code d'erreur DOIT contenir le nombre de Classeurs acceptés par porte.

Les codes d'erreur 8, 9 et 10 sont générés par suite de l'échec d'une Demande de politique à satisfaire les prescriptions d'une autorisation d'un Serveur de politique. Lorsque le gestionnaire d'application produit un message Etablir porte avec une limite de volume ou de temps pour le Serveur de politique, celui-ci PEUT rejeter la demande sur la base des règles de politique installées sur le Serveur de politique. Par exemple, une telle règle de politique pourrait dire que si une demande de limite de volume dépasse une valeur maximale, le Serveur de politique DOIT rejeter la demande.

6.4.2.15 Etat de la porte

Les informations dans l'objet Etat de la porte reflètent l'état en cours de la porte. Le CMTS DOIT inclure l'objet Etat de la porte dans tout message non sollicité qu'il envoie au Serveur de politique. Le Serveur de politique peut utiliser ces informations pour faire rapport de l'état au gestionnaire d'application, ou pour mettre en application des règles complexes qui pourraient nécessiter de connaître l'état de la porte.

Normalement, le Serveur de politique est au courant des transitions d'état puisqu'il fournit habituellement le stimulus pour ces transitions au CMTS, mais dans certains cas la porte peut faire

transition localement sur le CMTS sans que le Serveur de politique soit impliqué. Dans ces cas, le CMTS DOIT rapporter la transition d'état au Serveur de politique via des messages Rapport d'état de porte non sollicités. Lors de la production de messages Rapport d'état de porte, le PEP DOIT s'assurer que le fanion Sollicité dans l'en-tête de message COPS est effacé, et que le Type de rapport dans l'en-tête est réglé à Comptabilité. L'objet Etat de la porte DOIT se conformer à la spécification suivante:

Longueur = 8	S-Num = 15	S-Type = 1
Etat	Cause	

Etat est un champ d'entier arithmétique de deux octets qui DOIT indiquer un des états suivants:

1 = repos/fermé

2 = autorisé

3 = réservé

4 = engagé

Cause est un champ d'entier arithmétique de deux octets qui DOIT indiquer une des causes suivantes pour cette mise à jour:

1 = fermeture à l'initiative du CMTS du fait d'une réallocation de réservation

2 = fermeture à l'initiative du CMTS due à l'absence de réponse DOCSIS de couche MAC

3 = fermeture à l'initiative du CMTS due à l'expiration du temporisateur T1

4 = fermeture à l'initiative du CMTS due à l'expiration du temporisateur T2

5 = expiration du temporisateur d'inactivité due à l'inactivité du flux de service (expiration du temporisateur T3)

6 = fermeture à l'initiative du CMTS due au manque de maintenance de réservation

7 = état de porte inchangé, mais limite de volume atteinte

65535 = autre

6.4.3 Messages de commande de porte

Il y a deux profils séparés pour les messages Commande de porte, un pour les échanges de messages entre gestionnaire d'application et Serveur de politique, et un pour les messages entre Serveur de politique et CMTS. Bien que similaires, ces deux profils présentent quelques différences.

6.4.3.1 Profil pour l'interface Gestionnaire d'application à Serveur de politique

Les messages qui effectuent la commande de porte entre le gestionnaire d'application et le Serveur de politique sont définis et DOIVENT être formatés comme suit.

Noter que les messages du gestionnaire d'application au Serveur de politique DOIVENT être formatés comme des messages Décision de COPS, et les messages du Serveur de politique au gestionnaire d'application DOIVENT être formatés comme des messages Rapport d'état COPS.

<Commande de porte> = <En-tête commun COPS> <Outil Client> <Contexte>

<Fanions Décision> <Données du ClientSI>

<Données du ClientSI> = <Etablir porte> | <Info de porte> | <Supprimer porte>

<Réponse de commande de porte> = <En-tête commun COPS> <Outil Client> <Type de rapport>

<Objet ClientSI>

<Objet ClientSI> = <Acc Etablir porte> | <Erreur Etablir porte> | <Acc info de porte> | <Erreur d'info de porte> |

<Acc Supprimer porte> | <Erreur Supprimer porte> <Rapport d'état de porte>

<Etablir porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> [<ID de porte>]

<Spec de porte> <Profil de trafic> <Classeur> [<Classeur>]

[<Limite d'utilisation en volume>] [<Limite de temps d'utilisation>] [<Données opaques>]

<Acc Etablir porte> = <En-tête de ClientSI> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

[<Données opaques>]

<Erreur Etablir porte> = <En-tête de ClientSI> <ID de transaction> <AMID> <ID d'abonné>

<Erreur IPCablecom> [<Données opaques>]

<Info de porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

<Acc d'Info de porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

<Spec de porte> <Etat de porte> <Classeur> <Profil de trafic> <Info de temps de porte>

<Info d'utilisation de porte> [<Limite d'utilisation en volume>]

[<Limite de temps d'utilisation>] [<Données opaques>]

<Erreur Info de porte> = <En-tête de ClientSI> <ID de transaction> <AMID> <ID de porte> <Erreur IPCom>

[<Données opaques>]

<Supprimer porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

<Acc Supprimer porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID de porte> [<Données opaques>]

<Err Supprimer porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID de porte>

<Erreur IPCablecom> [<Données opaques>]

<Rapport d'état de porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID d'abonné> <ID de porte> <Etat de porte> <Info de temps de porte> <Info utilisation de porte> [<Données opaques>]

6.4.3.2 Profil pour l'interface Serveur de politique à CMTS

Les messages qui effectuent la commande de porte entre le Serveur de politique et le CMTS sont définis et DOIVENT être formatés comme suit.

Noter que les messages du Serveur de politique au CMTS DOIVENT être formatés comme des messages Décision de COPS, et que les messages du CMTS au Serveur de politique DOIVENT être formatés comme des messages COPS de Rapport d'état.

<Commande de porte> = <En-tête commun COPS> <Outil Client> <Contexte>

<Fanions Décision> <Données ClientSI>

<Données ClientSI> = <Etablir porte> | <Info de porte> | <Supprimer porte>

<Réponse de commande de porte> = <En-tête commun COPS> <Outil Client> <Type de rapport>

<Objet ClientSI>

<Objet ClientSI> = <Acc Etablir porte> | <Erreur Etablir porte> | <Acc Info de porte> | <Erreur Info de porte> |

<Acc Supprimer porte> | <Erreur Supprimer porte> | <Rapport d'état de porte>

<Etablir porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> [<ID de porte>]

<Spec de porte> <Profil de trafic> <Classeur> [<Classeur>] [<Info de génération d'événement>]

[<Limite d'utilisation en volume>] [<Limite de temps d'utilisation>] [<Données opaques>]

<Acc Etablir porte> = <En-tête ClientSI> <ID de Transaction> <AMID> <ID d'abonné> <ID de porte>

[<Données opaques>]

<Erreur Etablir porter> = <En-tête ClientSI> <ID de Transaction> <AMID> <ID d'abonné>

<Erreur IPCablecom> [<Données opaques>]

<Info de porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

<Acc Info de porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

[<Info de génération d'événement>] <Spec de porte> <Classeur> <Profil de trafic>

<Info de temps de porte> <Info d'utilisation de porte> [<Limite d'utilisation en volume>]

[<Limite de temps d'utilisation>] [<Données opaques>]

<Erreur d'Info de porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID de porte> <Erreur IPCcom>

[<Données opaques>]

<Supprimer porte> = <En-tête Décision> <ID de transaction> <AMID> <ID d'abonné> <ID de porte>

<Acc Supprimer porte> = <En-tête ClientSI> <ID transaction> <AMID> <ID de porte> [<Données opaques>]

<Erreur de Supprimer porte> = <En-tête de ClientSI> <ID de transaction> <AMID> <ID de porte>

<Erreur IPCablecom> [<Données opaques>]

<Rapport d'état de porte> = <En-tête ClientSI> <ID de transaction> <AMID> <ID d'abonné> <ID de porte> <Etat de porte>

<Info de temps de porte> <Info d'utilisation de porte> [<Données opaques>]

Il y a trois messages de base de commande de porte: Etablir porte, Info de porte, et Supprimer porte. Ces messages sont incorporés dans les Données de décision spécifiques du client dans un message

Décision de COPS. Pour les messages de commande de porte, l'objet Contexte (C-Num = 2, C-Type = 1)dans le message Décision de COPS DOIT avoir la valeur du R-Type (Fanion Type de demande) mise à 0x08 (Demande de configuration) et celle de M-Type mise à zéro. Le champ Code de commande dans l'objet obligatoire Fanions de décision (C-Num = 6, C-Type = 1) DOIT être mis à 1 (Configuration d'installation). Les autres valeurs DOIVENT amener le CMTS à générer un message Rapport d'état indiquant l'échec. Le champ Type de commande de porte dans l'objet ID de transaction distingue le type de commande produite.

Il y a sept messages de réponse de commande de porte: Acc Etablir porte, Erreur Etablir porte, Acc d'Info de porte, Erreur d'Info de porte, Acc Supprimer porte, Erreur Supprimer porte, et Rapport d'état de porte. Les six premiers messages de réponse de commande de porte sont des réponses sollicitées aux messages de commande de porte. Le septième, Rapport d'état de porte, est une réponse non sollicitée du CMTS au Serveur de politique pour informer d'un changement d'état.

Ces messages sont incorporés dans l'objet Informations spécifiques du client dans les messages de rapport d'état COPS. L'objet Type de rapport (C-Num = 12, C-Type = 1) inclus dans le message COPS Rapport d'état pour les réponses de commande de porte DOIVENT avoir le champ Type de rapport mis à 1 (réussite) ou 2 (échec) selon le résultat de la commande de porte. Les messages Rapport d'état en réponse à une commande de porte DOIVENT avoir le fanion de message sollicité établi dans l'en-tête COPS. Le champ Type de commande dans l'ID de transaction distingue le type de réponse produite.

Le CMTS génère le message Rapport d'état de porte lorsqu'il y a une transition d'état sur la porte qui n'est pas due à un message Décision, ou lorsqu'une limite de politique a été atteinte. Pour le message Rapport d'état de porte, le champ Type de rapport DOIT être mis à 3 (Comptabilité), et le champ fanion sollicité DOIT être supprimé dans l'en-tête commun.

Si un objet reçu dans un message de commande de porte contient un S-Num ou S-Type qui n'est pas reconnu, cet objet DOIT être ignoré. La présence d'un tel objet au sein d'un message de commande de porte NE DOIT PAS être traité comme une erreur pourvu qu'après l'abandon d'un tel paramètre, tous les objets nécessaires soient présents dans le message.

6.5 Fonctionnement du protocole de commande de porte

6.5.1 Séquence d'initialisation

Lorsqu'un PEP (Serveur de politique ou CMTS) s'initialise, il DOIT écouter les connexions COPS entrantes sur le numéro de port TCP n° 3918 alloué par l'IANA. Tout gestionnaire d'application ou Serveur de politique (PDP) ayant besoin de contacter un PEP DOIT initialiser une connexion TCP avec le PEP sur ce port. On s'attend à ce que plusieurs gestionnaires d'application établissent des connexions COPS avec plusieurs Serveurs de politique, et que plusieurs Serveurs de politique établissent des connexions COPS avec plusieurs CMTS. Lorsque la connexion TCP entre le PEP et le PDP est établie, le PEP DOIT envoyer des informations sur lui-même au PDP sous la forme d'un message Client ouvert.

A réception d'un message Client ouvert réussi, le PDP DOIT envoyer un message Client accepté. Ce message DOIT inclure l'objet Temporisateur de durée de vie, qui indique au PEP l'intervalle maximal entre les messages Garder en vie.

A réception du message Client accepté réussi, le PEP DOIT envoyer un message de demande, incluant les objets Outil Client et Contexte. L'objet Contexte (C-Num = 2, C-Type = 1) DOIT avoir la valeur du R-Type (Fanion Type de demande) mise à 0x08 (Demande de configuration) et du M-Type mise à zéro. L'objet Outil Client contient un numéro qui DOIT être choisi par le PEP. La seule exigence imposée sur ce numéro est qu'un PEP NE DOIT PAS utiliser le même numéro pour deux demandes différentes sur une même connexion TCP. Ceci termine la séquence d'initialisation, qui est décrite visuellement ci-dessous.

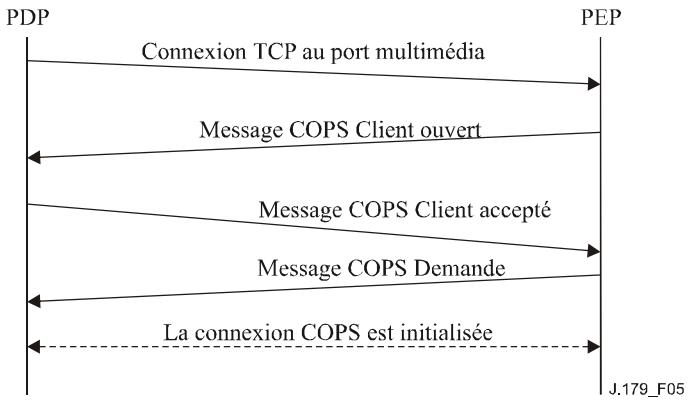

Figure 5/J.179 – Etablissement d'une connexion COPS

Périodiquement, le PEP DOIT envoyer un message COPS Garder en vie (KA, *keep alive*) au PDP. A réception du message COPS KA, le PDP DOIT répondre par un message COPS KA en retour au PDP. Cette transaction est montrée dans la Figure 6 et complètement décrite dans [7]. Le PEP DOIT envoyer un message Garder en vie au moins aussi souvent que spécifié dans l'objet Temporisateur de durée de vie retourné dans le message Client accepté. Le message Garder en vie DOIT être envoyé avec le Type de client mis à zéro et le fanion sollicité supprimé.

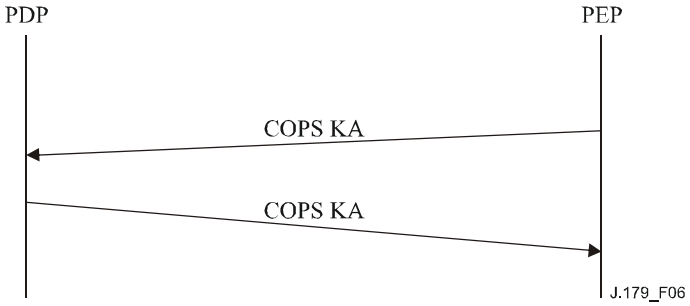

Figure 6/J.179 – Echange Garder en vie COPS

6.5.2 Séquence de fonctionnement

Le protocole entre le PDP et le PEP est utilisé pour les besoins du contrôle de ressource et la politique d'allocation de ressources. Le gestionnaire d'application demande des décisions de politique au Serveur de politique, et le Serveur de politique autorise les demandes et les installe sur le système CMTS pour mise en application par l'utilisation des portes.

Les messages qui PEUVENT être initialisés par le gestionnaire d'application et le Serveur de politique incluent Etablir porte, Info de porte et Supprimer porte. Le CMTS PEUT initialiser les messages Rapport d'état de porte. La procédure pour ces messages est décrite dans les paragraphes qui suivent. Tous les messages du PDP au PEP DOIVENT être envoyés en utilisant les objets spécifiques du Client au sein de l'objet Décision d'un message COPS Décision. Les réponses sollicitées du PEP DOIVENT être envoyées comme un message Rapport d'état avec des objets spécifiques du Client dans l'objet ClientSI, et le fanion sollicité DOIT être mis. Les messages Rapport d'état de porte du CMTS DOIVENT être envoyés comme des messages Rapport d'état non sollicité via des objets spécifiques du Client dans l'objet ClientSI.

Les messages Décision et les messages Rapport d'état DOIVENT contenir le même Outil Client que celui fourni dans la Demande initiale envoyée par le CMTS lors de l'initialisation de la connexion COPS.

Etablir porte initialise et modifie tous les paramètres de politique et de trafic pour la porte et établit les informations de facturation. Etablir porte peut aussi être utilisé pour contrôler et mettre à jour l'état d'une porte au CMTS.

Info de porte est un mécanisme par lequel le Serveur de politique peut interroger tous les états et réglages de paramètres en cours d'une porte existante.

Supprimer porte permet à un Serveur de politique de supprimer une porte spécifique et tout flux de service associé.

Rapport d'état de porte permet au CMTS d'informer le Serveur de politique du passage de la porte dans un nouvel état. Les messages Rapport d'état de porte DOIVENT être générés lorsque la transition d'état survient de façon asynchrone (c'est-à-dire, pas en réponse au message Etablir porte). Les messages Rapport d'état de porte NE DOIVENT PAS être générés lorsque la transition d'état survient de façon synchrone.

Le PEP DOIT périodiquement envoyer un message Garder en vie (KA) au PDP pour faciliter la détection d'échecs de connexion TCP. Le PDP DOIT garder trace du moment où les messages KA sont reçus. Si le PDP n'a pas reçu un message KA du PDP dans l'intervalle de temps spécifié en [7] ou si le PDP n'a pas reçu une indication d'erreur de la connexion TCP, le PDP DOIT alors supprimer la tentative de connexion TCP et tenter de rétablir la connexion TCP.

On utilise les règles suivantes pour acheminer les messages de commande de porte à travers l'architecture IPCablecom Multimédia. En particulier, des dispositions sont fournies pour transmettre les messages de commande de porte aller (c'est-à-dire, gestionnaire d'application – Serveur de politique – système CMTS) et retour (c'est-à-dire, CMTS – Serveur de politique – gestionnaire d'application) à travers en réseau en couches complexe avec de multiples instances de chaque élément interagissant avec des éléments dans la ou les couches adjacentes.

Comme décrit au § 6.4.3.1, chaque Demande de commande de porte qui est initialisée par un gestionnaire d'application (c'est-à-dire, Etablir porte, Info de porte, et Supprimer porte) DOIT inclure (en plus des autres objets obligatoires) les objets AMID et ID d'abonné.

A réception d'un message Commande de porte d'un gestionnaire d'application, un Serveur de politique va appliquer toutes les règles de politiques provisionnées et déterminer s'il faut admettre ou rejeter la demande. Si la demande est admise, le Serveur de politique DOIT acheminer le message au CMTS approprié sur la base de l'ID d'abonné inclus dans le message. Ce mappage d'ID d'abonné à CMTS PEUT être effectué de façon dynamique sur la base d'une interrogation à l'infrastructure OSS ou PEUT refléter les informations préapprovisionnées qui se rapportent à la ou les gammes de sous-réseaux IP qui sont associés à chaque CMTS.

Si une demande de commande de porte est rejetée par le Serveur de politique, une réponse d'erreur DOIT être retournée au gestionnaire d'application qui l'a produite sur la connexion sur laquelle la demande d'origine a été reçue. Si un échec est détecté sur cette connexion entre le moment de réception de la demande et la délivrance de la réponse, le Serveur de politique DOIT écarter la réponse.

A réception d'un message Commande de porte d'un Serveur de politique, un CMTS exécutera l'opération demandée. Si cette opération est réussie en impliquant une opération Etablir porte ou Info de porte, le CMTS DOIT enregistrer l'AMID et l'ID d'abonné inclus dans le message et maintenir une association avec la porte référencée. Cette information DOIT être utilisée pour s'assurer que seul le gestionnaire d'application qui a créé la porte à l'origine est autorisé à l'interroger ou la modifier. Tout message de commande de porte qui fait référence à une porte mais qui contient un AMID autre que celui associé à la porte DOIT être rejeté par le CMTS avec l'erreur "AMID non autorisé". Finalement, les messages Rapport d'état de porte DOIVENT être délivrés à l'élément Serveur de politique, identifié par son adresse IP, qui a créé la porte à l'origine. Si aucune

connexion à ce Serveur de politique n'est disponible, le CMST DOIT alors supprimer les messages Rapport d'état de porte.

Lorsqu'un Serveur de politique reçoit un message Rapport d'état de porte d'un système CMTS, le Serveur de politique DOIT transmettre ce message au gestionnaire d'application associé à l'AMID inclus dans le message. Afin de maintenir un certain niveau d'abstraction entre couches non adjacentes et de cacher à la couche du gestionnaire d'application les informations qui se rapportent à la topologie du réseau, le Serveur de politique NE DOIT PAS inclure d'informations identifiant directement un CMTS particulier pour la couche du gestionnaire d'application.

6.5.3 Procédures de validation des enveloppes de ressource

L'ensemble des caractéristiques des flux de service de données qui est important pour la fourniture de la qualité de service améliorée est connu sous le nom d'enveloppe. Une porte d'IPCablecom multimédia contient jusqu'à trois enveloppes: une qui indique les ressources autorisées, une qui indique les ressources réservées, et une qui indique les ressources engagées pour le flux de service correspondant à la porte. A tout moment, l'enveloppe engagée DOIT tenir dans l'enveloppe réservée qui DOIT tenir dans l'enveloppe autorisée.

Lorsqu'un CMTS reçoit un message Etablir porte, il DOIT valider la relation entre les enveloppes engagée, réservée, et autorisée de la porte. Si la relation entre les enveloppes n'est pas valide, le CMTS DOIT répondre avec un message Erreur d'Etablir porte avec un code d'erreur IPCablecom "Enveloppe incompatible".

Le CMTS DOIT aussi effectuer le contrôle d'admission chaque fois qu'un changement (y compris un ajout) de l'enveloppe réservée est demandé. Le contrôle d'admission est le processus d'allocation de ressources pour le flux correspondant à la porte. Si les ressources ne peuvent pas être allouées, le CMTS DOIT répondre par un message Erreur d'établir porte avec un code d'erreur IPCablecom "Ressources insuffisantes".

6.5.3.1 Spec de flux

Dans le Tableau 2, la seconde colonne indique l'opération qui devrait être utilisée pour comparer un paramètre de l'enveloppe de A à un paramètre correspondant dans l'enveloppe de B. En d'autres termes, l'enveloppe A tient dans l'enveloppe B si chacun des paramètres de A satisfait aux critères spécifié dans le Tableau.

Tableau 2/J.179 – Règles de comparaison d'enveloppe

Paramètre	A {OP} B
Débit de seau de jeton [r]	≤
Taille de seau de jeton [b]	≤
Débit de crête de données [p]	≤
Unité régulée minimale [m]	≥
Taille maximale de paquet [M]	≤
Débit [R]	≤
Terme de surlongueur [S]	≥

6.5.3.2 Nom de classe de service DOCSIS

Pour les Profils de trafics en forme de Nom de classe de service, la chaîne Nom de classe de service DOIT correspondre exactement au Nom de classe de service préexistant au système CMTS. Aucune comparaison d'enveloppe n'est nécessaire car les trois enveloppes DOIVENT toutes partager les même paramètres d'enveloppe.

6.5.3.3 Paramètres de flux de service DOCSIS

6.5.3.3.1 Codages amont

Au Tableau 3, la seconde colonne indique les opérations qui devraient être utilisées pour comparer un paramètre de l'enveloppe de A à un paramètre correspondant dans l'enveloppe de B. En d'autres termes, l'enveloppe A tient dans l'enveloppe de B si chacun des paramètres de A satisfait aux critères spécifiés dans le Tableau.

Tableau 3/J.179 – Comparaison d'enveloppe amont

Paramètre	A {OP} B
Priorité de trafic (Au mieux & NRTPS)	≤
Politique de transmission de demande (toutes)	==
Débit au trafic soutenu maximal (Au mieux, NRTPS, RTPS)	≤
Rafale de trafic maximal (Au mieux, NRTPS, RTPS)	≤
Débit au trafic réservé minimal (Au mieux, NRTPS, RTPS)	≤
Taille de paquet au débit au trafic réservé minimal supposé (Au mieux, NRTPS, RTPS)	≥
Intervalle d'interrogation nominal (NRTPS, RTPS, UGS/AD)	Voir la description d'intervalle ci-dessous
Gigue d'interrogation tolérée (RTPS, UGS/AD)	≥
Taille d'allocation non sollicitée (UGS & UGS/AD)	≤
Allocations par intervalle (UGS & UGS/AD)	≤
Intervalle d'allocation nominal (UGS & UGS/AD)	Voir la description d'intervalle ci-dessous
Gigue d'allocation tolérée (UGS & UGS/AD)	≥

Intervalles – A est un sous-ensemble de B si le paramètre dans A est un multiple entier des mêmes paramètres dans B.

6.5.3.3.2 Codages aval

Au Tableau 4, la seconde colonne indique l'opération qui devrait être utilisée pour comparer un paramètre de l'enveloppe de A avec un paramètre correspondant dans l'enveloppe de B En d'autres termes, l'enveloppe A tient dans l'enveloppe B si chacun des paramètres de A satisfait aux critères spécifiés dans le Tableau.

Tableau 4/J.179 – Comparaison d'enveloppe aval

Paramètre	A {OP} B
Priorité de trafic	≤
Débit au trafic soutenu maximal	≤
Rafale de trafic maximal	≤
Débit au trafic réservé minimal	≤
Taille de paquet au débit au trafic réservé minimal supposé	≥
Temps de latence aval maximal	≥

6.5.4 Procédures d'autorisation de ressources à travers une porte

Le message Etablir porte PEUT être envoyé par le PDP au PEP pour initialiser ou modifier les paramètres de fonctionnement d'une porte. La Figure 7 ci-dessous donne un exemple de la signalisation Etablir porte.

NOTE – A titre d'exemple, le message "Débuter Session " peut être utilisé pour indiquer au Client que les ressources ont été autorisées.

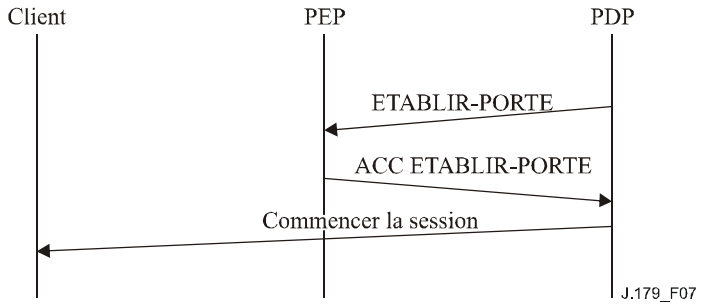

Figure 7/J.179 – Exemple de signalisation de Etablir porte

Si un objet ID de porte est présent dans le message Etablir porte, la demande est alors de modifier une porte existante. Si l'objet ID de porte manque dans le message Etablir porte, c'est alors une demande d'allocation d'une nouvelle porte. Le message Etablir porte DOIT contenir exactement un objet Spec de porte décrivant une porte aval ou amont.

Le message Etablir porte contient aussi l'ID d'abonné. Le CMTS DOIT utiliser cette adresse IP (c'est-à-dire, l'ID d'abonné) pour déterminer le câblo-modem de service et DOIT utiliser l'adresse MAC du câblo-modem pour les échanges de messages de couche MAC suivants.

Le PEP DOIT répondre à un message Etablir porte par un Acc Etablir porte, indiquant le succès, ou par Erreur Etablir porte, indiquant l'échec. L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction de la demande. Les erreurs dans l'allocation ou l'autorisation des portes DOIVENT être rapportées par une réponse Erreur-Etablir-porte. Se reporter au § 6.4.2.14.

Dans le scénario 1, le Serveur de politique PEUT spécifier les enveloppes Autorisée, Réservée et Engagée via un Profil de trafic envoyé dans le message Etablir porte. Il PEUT simultanément ordonner au CMTS d'autoriser, réserver et engager les ressources.

A réception d'un Etablir porte, le CMTS DOIT d'abord satisfaire aux exigences spécifiées au § 6.5.3 puis alors effectuer les actions demandées. A l'achèvement réussi des actions demandées dans Etablir porte (par exemple, création d'un flux de service DOCSIS) le CMTS DOIT répondre par Acc Etablir porte. Le CMTS NE DOIT PAS répondre par un Acc Etablir porte tant qu'il n'a pas réalisé d'étapes suffisantes pour garantir que toute demande subséquente d'admettre ou engager la porte n'échouera pas faute de ressources.

Un CMTS PEUT effectuer une autorisation complexe fondée non seulement sur la qualité de service demandée et la Spec de flux autorisée de la porte, mais aussi fondée sur l'ID de classe de session spécifié dans la Spec de porte. Le CMTS PEUT avoir provisionné des politiques qui définissent la quantité de ressources allouées exclusivement à la Classe de session particulière, aussi bien que des règles "emprunter" et préempter" qui s'appliquent à l'utilisation des ressources. Les particularités de ces types de politiques et règles au niveau du CMTS sont en dehors du domaine d'application de la présente Recommandation.

A réception de Acc Etablir porte ou Erreur Etablir porte venant d'un CMTS, le Serveur de politique DOIT faire suivre le message au gestionnaire d'application correspondant à l'AMID dans l'Acc Etablir porte. Le Serveur de politique Ne DOIT PAS transmettre un Acc Etablir porte à un

gestionnaire d'application avant d'avoir reçu un Acc Etablir porte du CMTS. Si le gestionnaire d'application demande un service qui ne passe pas la vérification de politique du Serveur de politique, le Serveur de politique NE DOIT PAS cependant envoyer Etablir porte au CMTS et DOIT envoyer Erreur Etablir porte au gestionnaire d'application avec l'ensemble d'erreurs approprié.

6.5.5 Procédures d'interrogation de porte

Lorsqu'un Serveur de politique ou gestionnaire d'application souhaite interroger les réglages des paramètres en cours d'une porte, il envoie au CMTS un message Info de porte. Le CMTS DOIT répondre à un message Info de porte par un Acc d'Info de porte, indiquant le succès, ou une Erreur d'Info de porte, indiquant l'échec. Acc d'Info de porte DOIT contenir des informations sur la porte associées à l'ID de porte dans le message Info de porte. Si la porte interrogée a une Limite de volume et/ou Limite de temps d'utilisation existante, le CMTS DOIT alors inclure ces objets dans Acc d'Info de porte. Un Serveur de politique ou gestionnaire d'application peut utiliser ces informations pour récupérer des informations d'état de la porte auprès du CMTS pour des besoins de régulation, de récupération d'erreur ou tout autre objet. L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande.

Les erreurs d'interrogation des portes DOIVENT être rapportées par une réponse Erreur d'Info de porte. L'objet Erreur dans un message Erreur d'Info de porte DOIT contenir un des Codes d'erreur suivants:

2 = ID de porte inconnu

127 = autre, Erreur non spécifiée

6.5.6 Procédures de modification de porte

Pour modifier le Profil de trafic associé à une porte existante, un gestionnaire d'application PEUT envoyer un message Etablir porte avec l'ID de porte de la porte à modifier et le nouveau Profil de trafic. Si Etablir porte échoue à la vérification du Serveur de politique, le Serveur de politique DOIT envoyer Erreur d'Etablir porte au gestionnaire d'application et NE DOIT Pas envoyer Etablir porte au CMTS. Cependant, si Etablir porte passe les vérifications du Serveur de politique, le Serveur de politique DOIT envoyer Etablir porte au CMTS sans modification. L'ID de transaction dans Etablir porte du Serveur de politique DOIT correspondre à l'ID de transaction dans Etablir porte du gestionnaire d'application.

A réception d'Etablir porte, le CMTS DOIT d'abord satisfaire aux exigences spécifiées au § 6.5.3 puis effectuer les actions demandées. Comme pour la création d'une nouvelle porte, après le succès de l'achèvement des actions demandées dans Etablir porte (par exemple, modification d'un flux de service DOCSIS) le CMTS DOIT répondre par un Acc Etablir porte. Le CMTS NE DOIT PAS répondre par un Acc Etablir porte tant qu'il n'a pas achevé un nombre suffisant d'étapes pour garantir que toute demande ultérieure pour admettre ou engager la porte n'échouera pas à cause d'un manque de ressources.

A réception de Acc Etablir porte ou Erreur d'Etablir porte provenant du CMTS, le Serveur de politique DOIT transmettre la réponse non modifiée au gestionnaire d'application.

Pour modifier les Limites d'utilisation associées à une porte existante, un gestionnaire d'application PEUT envoyer un message Etablir porte avec l'ID de porte de la porte à modifier. Si le Profil de trafic dans Etablir porte est différent du Profil de trafic actuellement associé à la porte, les règles précédentes s'appliquent alors. Dans tous les cas, si les Limite de temps d'utilisation ou Limite d'utilisation en volume du flux sont présentes, les limites existantes associées à ce ou ces paramètres DOIVENT alors être remplacées par le ou les nouveaux paramètres et tout compteur ou temporisateur existant DOIT être remis à zéro. Cependant, l'absence de ces paramètres dans un message Etablir porte indique que même si le Profil de trafic pour la porte est en train d'être modifié, les Limites de temps d'utilisation ou Limite d'utilisation en volume existantes de la porte

s'appliquent toujours. Si ces paramètres ne sont pas présents dans un message Etablir porte, les limites existantes DOIVENT être maintenues et leurs compteurs/temporisateurs associés DOIVENT continuer à partir de leur valeur en cours sans être remis à zéro.

6.5.7 Procédures de prise en charge des limites d'utilisation

Les gestionnaire d'application, Serveur de politique et CMTS ont tous un rôle dans la mise en application des limites d'utilisation. Il y a des différences subtiles entre les limites de temps d'utilisation et les limites d'utilisation en volume et chacune est donc décrite séparément.

6.5.7.1 Procédures en atteignant une Limite d'utilisation en volume

Comme le CMTS est le seul appareil de confiance d'IPCablecom multimédia sur le conduit de paquet, il est le seul appareil capable de retracer de façon appropriée l'utilisation des portes individuelles. Et donc, le CMTS DOIT retracer l'utilisation de toutes les portes sans considérer si elles ont ou non une Limite d'utilisation en volume associée. Le CMTS DOIT rapporter la quantité de données transférées via une porte dans tous les messages Acc d'Info de porte et Rapport d'état de porte.

Si la porte a une Limite d'utilisation en volume associée lorsque la quantité de données qui ont traversé la porte égale la Limite d'utilisation en volume, le CMTS DOIT envoyer un message Rapport d'état de porte avec le bit Sollicité mis à 0. Le message Rapport d'état de porte DOIT inclure un objet Etat de porte avec la cause mise à 7 (Etat de porte inchangé, mais limite de volume atteinte). A réception d'un message Rapport d'état de porte, le Serveur de politique DOIT transmettre le message Rapport d'état de porte au gestionnaire d'application sans modification. A réception d'un message Rapport d'état de porte avec la cause mise à 7, le gestionnaire d'application DOIT répondre en effectuant une des actions suivantes:

- envoyer un message Etablir porte avec un nouvel objet Limite d'utilisation en volume, que le CMTS DOIT utiliser pour 'redémarrer' le comptage pour cette porte;
- envoyer un message Etablir porte avec Limite d'utilisation en volume mis à 0 pour désactiver le dispositif et permettre au CMTS de continuer à servir la session;
- fermer la porte en produisant une commande Supprimer porte.

6.5.7.2 Procédures en atteignant une Limite de temps d'utilisation

Bien que ce soit un objectif de conception souhaitable de garder les procédures de Limite d'utilisation en volume et de Limite de temps d'utilisation aussi similaires que possible, le nombre de coupures de CMTS nécessaires pour prendre en charge la mise en application de Limite de temps d'utilisation par le CMTS rend cette approche impossible. Et donc, le gestionnaire d'application DOIT mettre en application la Limite de temps d'utilisation de la porte. A réception de l'Acc d'Etablir porte pour une porte avec une Limite de temps d'utilisation, le gestionnaire d'application DOIT lancer un temporisateur d'application. Lorsque le temporisateur d'application est égal à la Limite de temps d'utilisation, le gestionnaire d'application DOIT répondre en effectuant une des actions suivantes:

- envoyer un message Etablir porte avec un nouvel objet Limite de temps d'utilisation et remettre à zéro son temporisateur d'application;
- envoyer un message Etablir porte avec une Limite de temps d'utilisation à 0 pour désactiver le dispositif;
- fermer la porte en produisant une commande Supprimer porte.

NOTE – D'une certaine façon il est plus raisonnable pour le gestionnaire d'application de mettre en application les limites d'utilisation, dans la mesure où Limite de temps d'utilisation et Limite d'utilisation en volume sont un reflet du service qui est offert et sont de la responsabilité du Domaine de commande de service. C'est la procédure de Limite d'utilisation en volume qui est inhabituelle, mais le CMTS est le seul appareil qui puisse valablement appliquer cette limite.

6.5.7.3 Récupération de ressource et d'erreur

Alors qu'il est exigé que le gestionnaire d'application effectue une des diverses actions prévues lorsqu'une limite d'utilisation de porte a été atteinte, il y a toujours la possibilité que le gestionnaire d'application ne réponde pas correctement. Dans ce cas, le Serveur d'archivage mémorisera toujours l'utilisation de cette porte de sorte que son activité soit toujours facturable, mais dans certains cas, il peut être utile de récupérer les ressources qui sont utilisées "illégalement" par le gestionnaire d'application. Un Serveur de politique PEUT découvrir le fait que la Limite d'utilisation en volume ou la Limite de temps d'utilisation d'une porte a été dépassée sur la base des messages dont il est mandataire entre le gestionnaire d'application et le CMTS. Utiliser la technique du "glanage" implique que le Serveur de politique soit à états, mais un Serveur de politique qui n'est pas "à états" peut toujours récupérer les ressources via une seconde technique décrite ci-dessous.

Autrement, un Serveur de politique PEUT interroger occasionnellement le CMTS avec un message Info de porte. La réponse contiendra toute Limite d'utilisation en volume et Info d'utilisation de porte (ou Limite de temps d'utilisation et Info d'heure de porte) associée. Le Serveur de politique peut alors comparer ces valeurs. Indépendamment de la façon dont un Serveur de politique apprend qu'une porte a dépassé une limite, il PEUT produire un Supprimer porte pour les portes hors limites. A réception de l'Acc d'Etablir port (ou Erreur d'Etablir porte) venant du CMTS, le Serveur de politique DOIT envoyer le message au gestionnaire d'application sans modification excepté pour l'ID de transaction.

De même, bien qu'on ne lui demande pas de récupérer les ressources des portes hors limites, un serveur CMTS PEUT effectuer les mêmes comparaisons lui-même et PEUT supprimer les portes hors limites. Des prescriptions complémentaires pour ce scénario figurent au § 6.5.8.

6.5.7.4 Traçage de Limite de temps d'utilisation et de Limite d'utilisation en volume

Les portes IPCablecom multimédia peuvent entrer et quitter l'état Engagé à de nombreuses reprises (pour prendre en charge, par exemple, une fonction "pause" sur un média de jeu ou de streaming). Comme un abonné ne peut pas émettre/recevoir de données pendant que la porte n'est pas dans l'état Engagé, ces périodes ne devraient pas être comptées à ce titre. Pour les Limites en volume, cette prescription est sans effet car il n'y a pas de paquet qui puisse être compté à tort dans la mesure où aucun paquet ne peut être envoyé si une porte n'est pas Engagée. Cependant, pour les Limites de temps d'utilisation, le CMTS DOIT arrêter son temporisateur d'Info d'heure de porte lorsque la porte n'est pas dans l'état engagé. Si la porte est ré-engagée sans changement de la limite de temps, le temporisateur d'Info d'heure de porte DOIT être relancé depuis le moment où il a arrêté le compte. Si des changements sont apportés à la Limite de temps, le temporisateur d'Info d'heure de porte DOIT être remis à 0 et relancé lorsque la porte est ré-engagée.

NOTE – Le gestionnaire d'application doit maintenir un temporisateur indépendant du temporisateur du CMTS pour mettre en application la Limite de temps d'utilisation. Comme ce temporisateur est séparé du système CMTS lui-même, les retards d'échange de messagerie pourraient causer des différences entres ces deux temporisateurs. Pour les applications qui ont besoin d'une haute précision d'horloge, le gestionnaire d'application PEUT interroger le CMTS sur son objet Info d'heure de porte après qu'il ait passé une porte dans ou hors de l'état Engagé.

6.5.8 Procédures de suppression d'une porte

Normalement, lorsqu'une session multimédia s'achève, le gestionnaire d'application indique au Serveur de politique que la session est terminée, et le Serveur de politique ordonne à son tour au CMTS de retirer la porte via un message Supprimer porte. Le CMTS DOIT répondre au message Supprimer porte par un Acc Supprimer porte, indiquant le succès, ou un Erreur de Supprimer porte, indiquant l'échec. L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande.

Les erreurs de suppression des portes DOIVENT être rapportées par une réponse Erreur de Supprimer porte. L'objet Erreur DOIT contenir un des Codes d'erreur suivants:

2 = ID de porte inconnu

127 = autre, Erreur non spécifiée

Au CMTS, si le temporisateur T1 ou T2 arrive à expiration, la porte DOIT être supprimée. Lorsqu'un CMTS supprime une porte sans être sollicité par le Serveur de politique, le CMTS DOIT envoyer un message Rapport d'état de porte (avec le bit Sollicité mis à 0) au Serveur de politique indiquant que la porte a été supprimée. Si le temporisateur T2 arrive à expiration, le CMTS DOIT supprimer le flux DOCSIS au moyen des mécanismes DOCSIS (c'est-à-dire, un message DSD), puis le CMTS DOIT remettre la porte à l'état Autorisé, redémarrer le temporisateur T1, et produire un message Rapport d'état de porte (avec le bit Sollicité mis à 0) au Serveur de politique l'informant de cette transition d'état. A réception d'un message Rapport d'état de porte, le Serveur de politique DOIT le transmettre sans modification au gestionnaire d'application.

6.5.9 Procédure pour engager une porte

Dans le scénario 1, le Serveur de politique est responsable de l'engagement d'une porte au moyen d'un Profil de trafic contenant une Enveloppe engagée. Le CMTS engage la porte et active le flux de service DOCSIS en utilisant les paramètres que lui a passé le Serveur de politique.

6.5.10 Séquence de terminaison

Lorsque le PEP ferme sa connexion TCP au PDP, il PEUT d'abord envoyer un message Etat demande de suppression (y compris l'objet Outil utilisé dans le message Demande initial). Le PEP PEUT faire suite à cela avec un message Client-fermé. Le PDP en réponse DOIT automatiquement supprimer tout état associé au PEP lorsque la connexion TCP est terminée. Lorsque le PDP est sur le point de fermer, il DEVRAIT envoyer un message COPS Client-fermé au PEP. Dans le message COPS Client-fermé, le PDP NE DEVRAIT PAS envoyer l'objet adresse de redirection du PDP PDPRedirAddr. Si le PEP reçoit un message COPS Client-fermé du PDP avec un objet PDPRedirAddr, le PDP DOIT ignorer le PDPRedirAddr alors qu'il traite le message COPS Client-fermé.

Le Serveur de protocole et le CMTS NE DOIVENT PAS supprimer les portes par suite d'un échec de connexion COPS.

6.5.11 Procédures de synchronisation d'état

Lorsqu'un Serveur de politique veut synchroniser son état avec celui d'un CMTS il PEUT envoyer un message Demande-de-synchronisation-d'état (SSQ). Cette SSQ PEUT contenir l'Outil-client du Serveur de politique. Si l'Outil-client facultatif est présent, seul l'état associé à cet outil est synchronisé. Si le CMTS ne reconnaît pas l'outil demandé, il DOIT immédiatement envoyer un message DRQ au Serveur de politique pour l'outil qui était spécifié dans le message SSQ. Si aucun Outil-client n'est spécifié dans le message SSQ, tout état actif pour les clients ayant le Type de client IPCablecom multimédia DOIT être synchronisé avec le PDP.

Le CMTS effectue la synchronisation d'état en produisant des messages Demande pour les portes associées à l'Outil-client (s'il est inclus dans le SSQ) ou pour toutes les portes connues (si aucun Outil-client n'est fourni). Lorsque la synchronisation est terminée, le CMTS DOIT produire un message Etat-de-synchronisation-terminé (SSC) au PDP. Si le SSQ initial contenait un Outil-client, le SSC correspondant DOIT alors contenir aussi l'Outil-client.

7 Description de l'interface d'echange de message d'evenements

7.1 Introduction

Comme dans l'architecture d'IPCablecom-T, les messages d'événement d'IPCablecom multimédia fournissent des informations détaillées sur l'utilisation des ressources de qualité de service, comme la réservation, l'activation, et la libération. Le besoin de garder trace de l'état des décisions de politique (demandes, mises à jour, suppression) est nouveau dans le cadre d'IPCablecom multimédia. Aussi, comme l'utilisation des ressources réseau sort du profil d'IPCablecom-T (utilisation constante dans le temps), il est nécessaire de faire rapport des informations d'utilisation en volume et en temps.

Les messages d'événement, tels que définis dans ce cadre, sont générés par des éléments de réseau et mémorisés dans le Serveur d'archivage (RKS). Ces messages d'événement sont ensuite corrélés par le RKS ou d'autres systèmes de l'arrière pour enregistrer une seule instance d'un service. Ces enregistrements peuvent être utilisés pour en déduire des informations de service, des schémas d'utilisation des ressources réseau, la planification des capacités, etc. Les messages d'événement ne sont pas cependant, destinés à la surveillance des défaillances.

Actuellement, seuls le CMTS et le Serveur de politique, qui font partie du réseau du câblo-opérateur et sont considérés comme des entités de confiance, génèrent des messages d'événement dans le cadre multimédia. Les autres éléments du réseau, comme les divers types de client, sont considérés comme n'étant pas de confiance. Dans le cas du gestionnaire d'application, cet élément peut faire ou non partie du réseau du câblo-opérateur, et donc ne fournit pas directement de messages d'événement au RKS. Le gestionnaire d'application fournit toutefois des informations supplémentaires au sein des champs de données opaques au Serveur de politique qui seront ensuite incluses dans les messages d'événement générés par le Serveur de politique.

Les messages d'événement IPCablecom pour le multimédia représentent une simplification et une modification des messages d'événement d'IPCablecom-T. Les événements spécifiques de la téléphonie, comme Réponse d'appel et Appel déconnecté sont considérés comme facultatifs, car ce sont des messages d'événement spécifiques du service téléphonique (par exemple, instance de service y). L'objectif est d'alléger les implémentations de messages d'événement existantes autant que possible tout en fournissant des mécanismes d'abstraction suffisants pour prendre en charge les services multimédia généraux.

Spécifiquement, parmi les quatorze types de message définis pour la prise en charge des services vocaux d'IPCablecom-T, quatre vont être nécessaires pour IPCablecom multimédia, qui sont Réservation_QS, Engagement_QS, Libération_QS, et Changement_d'heure. Trois nouveaux types de message d'événement se rapportant aux décisions de politique sont définis: Demande de politique, Suppression de politique, et Mise à jour de politique. Le Tableau 5 ci-dessous fait un résumé des types de message d'événement d'IPCablecom multimédia.

Tableau 5/J.179 – Types de message d'événement d'IPCablecom Multimédia

ID de message d'événement	Message d'événement	Elément d'origine	Description
7	Réservation_QS	CMTS	Indique le moment auquel le CMTS réserve la bande passante sur le réseau d'accès IPCablecom. Le CMTS DOIT aussi générer cet événement si la bande passante réservée change.
8	Libération_QS	CMTS	Indique le moment auquel le CMTS libère son engagement de bande passante sur le réseau d'accès IPCablecom
17	Changement_ d'heure	PS, CMTS	Capture une instance de changement d'heure. Chaque fois que l'horloge (IPCablecom) d'un élément de confiance du réseau (PS, et CMTS) est changé de plus de 200 ms, l'élément de réseau DOIT générer un message Changement d'heure.
19	Engagement_QS	CMTS	Indique le moment auquel le CMTS engage la bande passante sur le réseau d'accès IPCablecom. Le CMTS DOIT aussi générer cet événement si la bande passante engagée change.
31	Demande de_ politique	PS	Indique le moment auquel le Serveur de politique reçoit une nouvelle demande de politique du gestionnaire d'application
32	Supprimer_ politique	PS	Indique le moment auquel le Serveur de politique supprime une politique
33	Mise à jour de_ politique	PS	Indique le moment auquel le Serveur de politique reçoit une demande de mise à jour de politique

Bien que les messages d'événement d'IPCablecom Multimédia se fondent sur IPCablecom-T, les événements spécifiques de la téléphonie sont facultatifs pour IPCablecom Multimédia et la liste en figure ci-dessous. Pour de détail complémentaires sur ces événements et attributs associés, se reporter à la Recommandation sur les messages d'événement IPCablecom-T [10].

Tableau 6/J.179 – Types de message d'événement de téléphonie IPCablecom-T

ID de message d'événement	Message d'événement	Description
1	Début_Signalisation	Indique le moment auquel débute la signalisation
2	Arrêt_Signalisation	Indique le moment auquel se termine la signalisation
3	Interrogation_Base_ de_données	Indique le moment auquel une transaction de demande/réponse unique ou recherche dans une base de données est menée à bien par un périphérique intelligent (par exemple, base de donnée des n° 800, base de données LNP).
6	Instance_de_Service	Indique le moment auquel le serveur CMS fournit une instance de service de commande d'appel/dispositif (par exemple, mise en garde, appel en instance).
9	Activation_de_ Service	Indique le moment auquel le CMS enregistre une tentative d'activer un service (par exemple, renvoi d'appel, appel en instance).

Tableau 6/J.179 – Types de message d'événement de téléphonie IPCablecom-T

ID de message d'événement	Message d'événement	Description
10	Désactivation_de_ Service	Indique le moment auquel le CMS enregistre une tentative de désactiver un service (par exemple, renvoi d'appel, appel en instance).
13	Début_Interconnexion	Indique le moment auquel survient le début de la signalisation d'interconnexion de réseau
14	Arrêt_Interconnexion	Indique la fin de l'attribution de bande passante entre le réseau IPCablecom et le RTPC
15	Réponse_Appel	Indique que la connexion de média est ouverte parce qu'un événement de réponse est survenu
16	Déconnexion_Appel	Indique le moment auquel la connexion de média est fermée suite au raccroché du demandeur qui a mis fin à l'appel, ou au raccroché du destinataire et à l'expiration du temporisateur de continuation d'appel de l'appelé.
20	Média_Actif	Indique que le service est actif par suite de la continuation de l'existence d'une connexion support. Ce message peut être généré par tout élément de confiance du réseau IPCablecom (CMS, MGC, et CMTS) à la convenance du fabricant.

7.2 Exigences du Serveur d'archivage

Le serveur d'archivage (RKS) est une fonction d'élément de réseau de confiance. Le RKS est généralement décrit dans la présente Recommandation comme un élément autonome distinct, mais rien n'empêche quelque autre application d'effectuer les fonctions d'un serveur d'archivage, pourvu que l'application se conforme aux exigences présentes.

Le RKS est la couche de médiation entre le réseau IPCablecom multimédia et les applications de l'arrière. Le RKS est censé traiter les données reçues du réseau IPCablecom multimédia et les présenter aux applications de l'arrière dans le format et sous les contraintes de temps jugées nécessaires par le câblo-opérateur. Le RKS agit donc comme un point de démarcation entre le réseau IPCablecom et les applications de l'arrière.

Le RKS DOIT être capable de recevoir et traiter les messages d'événement formatés conformément à la présente Recommandation.

Les messages RADIUS à l'intérieur desquels sont incorporés les messages d'événement sont transportés sous le protocole UDP, qui ne garantit pas une livraison fiable des messages, d'où la nature demande/réponse du protocole défini ici. Lorsque un RKS reçoit et réussit à enregistrer tous les messages d'événement IPCablecom contenus dans un message Demande-comptabilité RADIUS, il DOIT transmettre un message Réponse-comptabilité au client. Le RKS NE DOIT PAS transmettre de Réponse-comptabilité s'il échoue à enregistrer tous les messages d'événement dans un message Demande-comptabilité RADIUS.

Le RKS DEVRAIT ignorer les messages d'événement dans lesquels le "type de message d'événement" IPCablecom n'est pas reconnu. Le RKS DEVRAIT aussi ignorer les attributs d'événement IPCablecom où l'ID d'attribut d'événement n'est pas reconnu.

7.3 Exigences générales pour l'élément de réseau IPCablecom multimédia

Le présent paragraphe fait la liste des exigences formulées pour les éléments de réseau IPCablecom multimédia.

7.3.1 ID d'élément

Chaque élément de réseau IPCablecom qui génère un message d'événement DOIT s'identifier par un ID d'élément unique et statique. L'ID d'élément est un numéro d'élément configuré de façon statique, unique au sein d'un domaine IPCablecom, qui DOIT être dans la gamme 0 à 99 999.

7.3.2 Synchronisation

Il est important pour les éléments qui génèrent des messages d'événement de rester en étroite synchronisation les uns avec les autres et avec une horloge standard. Les exigences du présent paragraphe s'assurent que de tels éléments maintiennent cette synchronisation et rapportent des événements avec un horodatage à la fois précis et adapté.

Les éléments qui génèrent des messages d'événement DOIT utiliser le Protocole de synchronisation de réseau (NTP, *network time protocol*) défini en [2]. Les éléments DOIVENT fonctionner en mode 3 (mode Client). La valeur de NTP.MAXPOLL NE DOIT PAS excéder onze, ce qui correspond à 2048 secondes.

Les messages d'événement DOIVENT inclure les horodatages avec une précision d'une milliseconde.

7.3.3 Considérations sur le RKS primaire et secondaire

IPCablecom multimédia prend en charge une architecture qui se compose de RKS primaires et secondaires. Le RKS secondaire est utilisé comme RKS de secours lorsqu'un élément de réseau (PS, CMTS) n'est pas en mesure de réussir à envoyer un message au RKS primaire. Les éléments de réseau IPCablecom multimédia DOIVENT prendre en charge le transport des messages d'événement vers un RKS primaire et un échappatoire vers un RKS secondaire lorsque les communications avec le RKS primaire échouent. Une fois que l'élément de réseau se rabat sur le RKS secondaire, le secondaire devient le primaire pour la durée de la session ou de la porte. Le Serveur de politique est approvisionné des RKS primaires et secondaires qui lui sont nécessaires pour les applications qu'il prend en charge. Le Serveur de politique DOIT fournir l'adresse IP et le port du RKS primaire, et facultativement du RKS secondaire, au CMTS dans les messages de décision de politique (Etablir porte). Le Serveur de politique DOIT prendre en charge plusieurs ensembles de RKS primaires et secondaires.

Pour garantir un transfert fiable des données, les éléments de réseau devraient implémenter un intervalle de temps de réessai configurable par l'utilisateur et le nombre de fois que le client doit retransmettre l'événement. L'intervalle de temps devrait être configurable (suggestion: 10 ms à 10 s), le nombre de réessais devrai être configurable (suggestion: 0 à 9). Le nombre de réessais devrai être tenté à la fois sur le RKS primaire et le RKS secondaire. Après épuisement du nombre de réessais, le message d'événement devrait être inscrit dans un fichier d'erreur, et le message d'événement peut alors être supprimé de l'élément de réseau.

Si l'élément de réseau IPCablecom ne reçoit pas de Réponse de comptabilité dans l'intervalle de réessai configuré, il DOIT continuer d'envoyer la Demande de comptabilité jusqu'à ce qu'il reçoive une Réponse de comptabilité d'un RKS ou que le nombre maximal de réessais soit atteint. L'élément de réseau IPCablecom DOIT renvoyer la même Demande de comptabilité au RKS primaire et si la limite de réessai est atteinte, renvoyer la même Demande de comptabilité au RKS secondaire.

Tous les éléments de réseau DOIVENT emmagasiner les messages d'événement jusqu'à ce qu'ils aient reçu un accusé de réception (Réponse de comptabilité) de la part d'un RKS confirmant la bonne réception des données et leur emmagasinage, ou jusqu'à ce que le nombre maximal de

réessais ait été atteint. C'est seulement lorsque un accusé de réception est reçu ou que le maximal de réessai est atteint que les éléments de réseau sont autorisés à détruire ces messages d'événement.

Une fois qu'un élément de réseau a réussi à envoyer des messages d'événement au RKS secondaire devrait survenir une reprise du RKS secondaire. Il s'agit d'une reprise non réversible, ce qui signifie que le RKS secondaire devient actif, et qu'il est le nouveau RKS primaire. Tous les messages d'événement ultérieurs pour la session devraient être envoyés au RKS secondaire maintenant actif. Pour toute nouvelle session, le Serveur de politique devrait ordonner au CMTS d'utiliser le RKS nouvellement actif comme primaire (c'est-à-dire, l'ancien RKS secondaire devient le nouveau RKS primaire pour la session suivante). Noter qu'il est possible dans certaines circonstances qu'un élément, PS ou CMTS, puisse être capable de communiquer avec le RKS primaire alors que l'autre élément ne le puisse pas pour la même session. Dans de tels cas, on attend du serveur RKS qu'il soit capable de coordonner les messages d'événement entre les RKS primaire et secondaire.

7.4 Messages d'événement pour IPCablecom multimédia

Le présent paragraphe donne une description et définition détaillée de chacun des messages d'événement définis pour IPCablecom multimédia.

7.4.1 Evénements de politique

Les messages d'événement de politique sont nouveaux pour IPCablecom multimédia. Ils indiquent le moment auquel le Serveur de politique reçoit une demande d'action de politique et servent à associer les ensembles de messages d'événement suivants pour toute utilisation de ressource associée aux différentes instances d'un service. Les messages d'événement de politique sont utilisés pour indiquer la demande de politique initiale, et mettre à jour selon la politique, et pour la suppression d'une politique.

Le Serveur de politique DOIT horodater les messages d'événement de politique à réception d'un message de demande de politique provenant du gestionnaire d'application. Dès réception d'une demande de politique initiale, le Serveur de politique DOIT créer un ID de corrélation de facturation (BCID, *billing correlation ID*). Chaque BCID généré DOIT être conforme aux prescriptions de format de structure d'attribut d'identifiant de corrélation de facturation (BCID) du Tableau 17.

Le Serveur de politique DOIT inclure le BCID dans l'en-tête de message d'événement pour tous les messages d'événement de politique associés générés par cette demande. Si la demande est approuvée, le Serveur de politique DOIT inclure le BCID dans le message Acc d'Etablir porte envoyé au gestionnaire d'application (pour accuser réception de la demande). Le Serveur de politique DOIT aussi inclure le BCID dans le message Etablir porte envoyé au CMTS.

Le Serveur de politique DOIT générer des messages d'événement de politique immédiatement après avoir déterminé le résultat de la demande de politique. Le résultat peut être fondé sur les mécanismes internes d'autorisation et de contrôle d'admission du Serveur de politique, ou, à réception d'une réponse à ses messages Etablir porte et Supprimer porte venant du système CMTS. Le Serveur de politique crée un horodatage pour un message d'événement lorsqu'il reçoit une demande du gestionnaire d'application mais il ne génère pas l'événement tant qu'il ne connaît pas le résultat de la demande.

7.4.1.1 Demande_de_politique

Le Serveur de politique DOIT envoyer un message d'événement Demande_de_Politique au serveur RKS si une demande de création d'une nouvelle politique est reçu. Le serveur de politique DOIT mettre l'Etat_de_Décision_de_Politique à Approuvé (1) ou Refusé (2), sur la base du résultat de l'autorisation et du contrôle d'admission.

NOTE – Comme le Serveur de politique n'envoie pas le message d'événement Demande_de_Politique jusqu'à ce que le CMTS ait répondu au message Etablir-porte, il est possible que les messages d'événement de qualité de service provenant du système CMTS arrivent au serveur RKS avant un message d'événement Demande_de_Politique.

Tableau 7/J.179 – Message d'événement Demande_de_Politique

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_Message_Evénement	O	Voir le Tableau 16
ID_Gestionnaire_Application	O	Contient l'identifiant unique pour l'ensemble du réseau du gestionnaire d'application
ID_Abonné	O	Adresse IPv4 de l'abonné
Etat_Décision_Politique	O	1 – Politique acceptée 2 – Politique refusée
Cause_Refus_Politique	F	Nécessaire lorsque Etat_Décision_Politique = 2 (Politique refusée) 1 – Echec de contrôle d'admission au Serveur de politique 2 – Ressources insuffisantes 3 – Abonné inconnu 127 – Autre
FEID	O	ID d'entité financière. Identifie l'entité qui paye. Fourni par le PS.
Données_Opaques_AM	F	Si le gestionnaire d'application inclut cet objet (ClientSI: données opaques) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement de politique.
Limite_Volume_d'Utilisation	F	Si le gestionnaire d'application inclut cet objet (ClientSI: limite d'utilisation en volume) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement de politique.
Limite_Temps_d'Utilisation	F	Si le gestionnaire d'application inclut cet objet (ClientSI: limite de temps d'utilisation) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement de politique.

7.4.1.2 Supprimer_Politique

Le Serveur de politique DOIT envoyer un message d'événement Supprimer_Politique au serveur RKS lorsqu'il reçoit un Supprimer porte du gestionnaire d'application indiquant que les ressources ne sont plus nécessaires pour une session, un Acc-Supprimer-porte du serveur CMTS en réponse à un Supprimer porte généré par un Serveur de politique, ou un Rapport d'état de porte provenant du serveur CMTS indiquant que les ressources ne sont plus disponibles pour une session. Le Serveur de politique DOIT toujours générer un message d'événement Supprimer-Politique pour fermer une session s'il avait préalablement généré un message d'événement Demande de politique pour ouvrir la session.

Tableau 8/J.179 – Message d'événement Supprimer_Politique

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_Message_d'Evénement	O	Voir le Tableau 16
ID_Gestionnaire d'Application	O	Contient l'identifiant unique pour tout le réseau du gestionnaire d'application
ID_d'Abonné	O	Adresse IPv4 de l'abonné
Cause_Suppression_Politique	O	1 – Demande du gestionnaire d'application 2 – Décision du CMTS 127 – Autre
FEID	O	ID de l'entité financière. Identifie l'entité qui paye. Fourni par le Serveur de politique.
Données_Opaques_d'AM	F	Si le gestionnaire d'application inclut cet objet (ClientSI: données opaques) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement Demande de politique.

7.4.1.3 Mise à jour_Politique

Le Serveur de politique DOIT envoyer un message d'événement Mise à jour de politique au serveur RKS si une demande de changement du Profil de trafic, de classeur, de limite de volume, de limite de temps, ou de données opaques d'une porte est reçue du gestionnaire d'application.

Tableau 9/J.179 – Message d'événement Mise à jour_de_Politique

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_de_message_ d'Evénement	O	Voir le Tableau 16
ID_de_gestionnaire_ d'Application	O	Contient l'identifiant unique pour l'ensemble du réseau du gestionnaire d'application
ID d'abonné	O	ID d'abonné
Etat_Décision_de_Politique	O	1 – Politique approuvée 2 – Politique refusée
Cause_Refus_Politique	F	Obligatoire lorsque Etat_Décision_Politique = 2 (Politique refusée) 1 – Echec de contrôle d'admission du Serveur de politique 2 – Ressources insuffisantes 3 – Abonné inconnu 4 – AMID non autorisé 5 – Nom de classe de service non défini 6 – Enveloppe incompatible 127 – Autre

Tableau 9/J.179 – Message d'événement Mise à jour_de_Politique

Nom d'attribut	Obligatoire ou facultatif	Commentaire
Cause_Mise à jour_Politique	O	1 – Profil de trafic 2 – Classeur 3 – Limite de volume 4 – Limite de temps 5 – Données opaques 6 – Mise à jour multiple (combinaison de 1 à 5) 127 – Autre
FEID	O	ID d'entité financière. Identifie l'entité qui paye. Fourni par le PS.
Données_Opaques_d'AM	F	Si le gestionnaire d'application inclut cet objet (ClientSI: données opaques) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement Evénement de politique.
Limite_Utilisation_Volume	F	Si le gestionnaire d'application inclut cet objet (ClientSI: limite d'utilisation en volume) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement Evénement de politique.
Limite_Temps_Utilisation	F	Si le gestionnaire d'application inclut cet objet (ClientSI: limite de temps d'utilisation) dans la "Demande de politique" (COPS DEC), le Serveur de politique DOIT alors l'inclure dans le message d'événement Evénement de politique.

7.4.2 Réservation de QS

Ce message d'événement indique le moment auquel le CMTS réserve la bande passante sur le réseau d'accès IPCablecom. Le CMTS DOIT aussi générer cet événement si la bande passante Réservée change.

Le CMTS DOIT horodater ce message immédiatement après transmission d'un DSA-ACK ou DSC-ACK accusant réception d'un DSA-RSP ou DSC-RSP réussi au câblo-modem qui termine une transaction de réservation de ressources.

Si le code de conformation de DSA-RSP ou DSC-RSP provenant du câblo-modem est un échec, le système CMTS NE DOIT PAS générer ce message.

Tableau 10/J.179 – Message d'événement Réservation_de_QS

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_de_message_d'événement	O	Voir le Tableau 16
Descripteur_de_QS	O	Aucun
ID_Flux_de_service	O	Aucun
Direction_Flux	O	Aucun
Elément_Demandant_QS	O	0 = client 1 = serveur de politique 2 = client incorporé

7.4.3 Engagement_QS

Le message d'événement Engagement_QS indique le moment auquel le CMTS engage la bande passante sur le réseau d'accès IPCablecom. Le CMTS DOIT aussi générer cet événement si la bande passante engagée change.

Le CMTS DOIT horodater ce message immédiatement après transmission au câblo-modem d'un DSA-ACK ou DSC-ACK accusant réception d'une DSA-RSP ou DSC-RSP réussie qui termine une transaction engageant des ressources.

Si le code de conformation de DSA-RSP ou DSC-RSP provenant du câblo-modem n'est pas réussi, le système CMTS NE DOIT PAS générer ce message.

Tableau 11/J.179 – Message d'événement Engagement_de_QS

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_de_message_d'événement	O	Voir le Tableau 16
Descripteur_de_QS	O	Aucun
ID_de_SF	O	Aucun
Direction_du_flux	O	Aucun

7.4.4 Libération_de_QS

Le message d'événement Libération_de_QS indique le moment auquel le CMTS libère sa réservation et/ou son engagement de bande passante sur le réseau d'accès IPCablecom.

Le CMTS DOIT horodater ce message immédiatement après transmission d'une DSD-REQ qui indique la demande de suppression de la bande passante.

Tableau 12/J.179 – Message d'événement Libération de QS

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_de_message_ d'événement	O	Voir le Tableau 16
SF_ID	O	Aucun
Direction_du_flux	O	Aucun
Cause_Libération_QS	O	1 – Porte fermée par le PS 2 – Expiration du temporisateur d'inactivité 3 – Défaillance de câblo-modem 4 – Préemption 5 – Demande de suppression de conduit RSVP 6 – Demande du câblo-modem 7 – Expiration du temporisateur admis (T2) 127 – Autre
Info_Usage_Porte	O	Aucun
Info_Temps_Porte	O	Aucun

7.4.5 Changement_d'heure

Cet événement retrace une instance de changement d'heure. Chaque fois que l'horloge (IPCablecom) de l'élément de réseau (PS ou CMTS) est changée de plus de 200 millisecondes, l'élément de réseau DOIT générer un message Changement d'heure. Ceci inclut les événements de changement d'horaire (passage à l'heure d'été), les ajustements par étape pour se synchroniser avec l'horloge de référence NTP et les changements manuels de réglage de l'heure. L'attribut Evénement_de_Temps dans l'en-tête de message d'événement DOIT refléter la nouvelle notion (ajustée) d'heure. Noter que le message Changement_d'heure n'est pas exigé pour les ajustements radicaux effectués par NTP.

Les élément de réseau (PS et CMTS) DOIVENT envoyer le message d'événement Changement_d'heure au RKS actif (le primaire en cours). Le message d'événement Changement_d'heure DOIT être généré lorsqu'une ou des portes sont actuellement présentes dans le CMTS. Le message d'événement Changement_d'heure n'a pas besoin d'être généré lorsqu'il n'y a pas de porte dans le CMTS. Un seul message d'événement Changement_d'heure est envoyé à chaque RKS primaire indépendamment du nombre de portes qui peut exister sur le CMTS. En d'autres termes, si le CMTS a plusieurs portes qui pointent toutes sur le même RKS, un seul message d'événement Changement_d'heure devrait alors être envoyé à ce RKS.

Dans l'en-tête de message d'événement du message d'événement Changement_d'heure, le BCID DOIT être généré localement au moment de l'événement. Le BCID n'est associé à aucune session se rapportant au BCID, c'est un BCID unique pour cet événement.

Tableau 13/J.179 – Message d'événement Changement_d'heure

Nom d'attribut	Obligatoire ou facultatif	Commentaire
En-tête_de_message_d'événement	O	Voir le Tableau 16
Réglage_d'heure	O	Aucun

7.5 Attributs d'échange de messages d'événement pour IPCablecom multimédia

Le présent paragraphe décrit et définit les attributs IPCablecom inclus dans les messages d'événement IPCablecom.

Elle fournit le mappage de chacun des messages d'événement IPCablecom et ses attributs associés. Le Tableau 14 donne une description détaillée de chacun de ces attributs.

Tableau 14/J.179 – Attributs IPCablecom mappés en messages d'événement IPCablecom MM

ID d'attribut d'EM	Nom d'attribut d'EM	7 – Réservation_de_QS	8 – Libération_de_QS	17 – Changement_d'heure	19 – Engagement_QS	31 – Demande_de_Politique	32 – Suppression_Politique	33 – Mise à jour_Politique
1	En-tête_message_d'événement	X	X	X	X	X	X	X
30	SF_ID	X	X		X			
32	Descripteur_de_QS	X			X			
38	Réglage_Horaire			X				
49	FEID					X	X	X
50	Direction_du_flux	X	X		X			
51	Données_Opaques_d'AM					X	X	X
52	ID_d'abonné					X	X	X
53	Limite_Usage_Volume					X		X
54	Info_Usage_Porte		X					
55	Elément_Demandant_Qs	X						
56	Cause_Libération_QS		X					
57	Raison_Refus_Politique					X		X
58	Raison_Suppression_Politique						X	
59	Raison_Mise-à-jour_Politique							X
60	Etat_Décision_Politique					X		X
61	ID_Gestionnaire_Application					X	X	X
62	Limite_Temps_Utilisation					X		X
63	Info_Heure_Porte		X					

Le Tableau 15 donne une définition détaillée de chacun des attributs de message d'événement IPCablecom. Une valeur de données d'un attribut peut être représentée par un format de données simple (un champ de données) ou par une structure de données plus complexe.

Tableau 15/J.179 – Attributs de message d'événement IPCablecom MM

ID d'attribut d'EM	Longueur d'attribut d'EM	Nom d'attribut d'EM	Type de valeur d'attribut d'EM	Description des données d'attribut
1	76 octets	En-tête_EM	Structure de données Voir le Tableau 16	Données communes nécessaires sur chaque message d'événement IPCablecom
30	4 octets	SF_ID	Entier arithmétique	ID de flux de service, un entier de 32 bits alloué par le CMTS à chaque flux de service DOCSIS défini au sein d'un domaine MAC DOCSIS RF. Les SFID sont considérés comme étant de sens amont (USFID) ou de sens aval (DSFID). Les USFID et DSFID sont alloués à partir du même espace de numéro de SFID.
32	Variable; mini 8 octets	Descripteur_QS	Structure de données Voir le Tableau 19	Données de paramètres de QS
38	8 octets	Réglage_Heure	Entier arithmétique	Réglage de l'heure de l'horloge d'un élément (PS, CMTS). Cette heure est en ms, elle précise la quantité de changement d'heure
49	Longueur variable, maximum de 247 octets	FEID	Chaîne de caractères ASCII	ID d'entité financière. Les 8 premiers octets sont des données définies par le câblo-opérateur. Par défaut, ces 8 premiers octets sont remplis de 0. A partir du 9^{e} octet, le champ contient le nom de domaine du câblo-opérateur qui l'identifie de façon univoque pour les besoins de la taxation et de la facturation. Le nom de domaine du câblo-opérateur est limité à 239 octets.
50	2 octets	Sens du Flux	Entier arithmétique	Sens du Flux: 0 = réservé 1 = amont 2 = aval
51	8 octets	Données_ Opaques_d'AM	Entier arithmétique	Données opaques provenant du gestionnaire d'application
52	4 octets	ID_d'abonné	Entier arithmétique	quatre valeurs d'octet enchaînées représentant une adresse IPv4
53	8 octets	Limite_Usage_ Volume	Entier arithmétique	Limite de volume en octets réglée par l'AM
54	8 octets	Info_Usage_ Porte	Entier arithmétique	Le nombre d'octets transmis sur le réseau DOCSIS RFdepuis l'octet après le HCS d'en-tête MAC jusqu'à la fin du CRC
55	2 octets	Elément_ Demandant_QS	Entier arithmétique	0 = client 1 = serveur de politique 2 = client intégré

Tableau 15/J.179 – Attributs de message d'événement IPCablecom MM

ID d'attribut d'EM	Longueur d'attribut d'EM	Nom d'attribut d'EM	Type de valeur d'attribut d'EM	Description des données d'attribut
56	2 octets	Cause_ Libération_QS	Entier arithmétique	1 – Porte fermée par le PS 2 – Temporisateur d'inactivité expiré 3 – Défaillance de CM 4 – Préempté 5 – Demande de suppression de conduit RSVP 6 – Demande de CM 7 – Expiration du temporisateur Admis (T2) 127 – Autre
57	2 octets	Raison_Refus_ Politique	Entier arithmétique	1 –Echec du contrôle d'admission du Serveur de politique 2 – Ressources insuffisantes 3 – Abonné inconnu 4 – AMID non autorisé 5 – Nom de classe de service non défini 6 – Enveloppe incompatible 127 – Autre
58	2 octets	Raison_ Supression_ Politique	Entier arithmétique	1 – Demande de gestionnaire d'application 2 – Décision du CMTS 127 – Autre
59	2 octets	Raison_Mise-à-jour_Politique	Entier arithmétique	1 – Profil de trafic 2 – Classeur 3 – Limite de volume 4 – Limite de temps 5 – Données opaques 6 – Mises à jour multiples (combinaison de 1 à 5) 127 – Autre
60	2 octets	Etat_Décision_ Politique	Entier arithmétique	1 – Politique approuvée 2 – Politique refusée
61	4 octets	ID_Gestionnaire _Application	Entier arithmétique	Identifiant unique pour tout le réseau alloué au gestionnaire d'application
62	4 octets	Limite_Temps_ Utilisation	Entier arithmétique	Limite de temps en secondes fixée par l'AM
63	4 octets	Info_Temps_de-porte	Entier arithmétique	Nombre de secondes pendant lesquelles une porte a été dans l'état Engagé

7.5.1 Structure d'attribut En-tête de message d'événement

Le Tableau 16 contient une description détaillée des champs dans la structure de l'attribut En-tête EM (de message d'événement). Cet attribut d'en-tête de message d'événement DOIT être le premier attribut de chaque message d'événement IPCablecom.

Tableau 16/J.179 – Structure d'attribut d'en-tête_de_message_d'événement

Nom de champ	Sémantique	Type de valeur	Longueur
ID de version	Identifie la version de cette structure d'en-tête d'EM. 1 = IPCablecom 1.0 2 = IPCablecom 1.1 3 = IPCablecom Multimédia	Entier arithmétique	2 octets
BCID	Identifiant unique pour une transaction au sein d'un réseau.	Structure de données Voir le Tableau 17	24 octets
Type d'EM	Identifie le type de message d'événement.	Entier arithmétique	2 octets
Type d'élément	Identifie le type de l'élément d'origine: 0 = réservé 1 = réservé 2 = CMTS 3 = réservé 4 = serveur de politique	Entier arithmétique	2 octets
ID d'élément	Identifiant unique au niveau du réseau Cinq chiffres (numéro d'élément configuré de façon statique, unique au sein d'un domaine IPCablecom, dans la gamme 0 à 99,999)	Justifié à droite, chaîne de caractères ASCII à bourrage d'espaces	8 octets
Zone horaire	Identifie l'heure d'été et les décalages par rapport au temps universel (UTC). Heure d'été: 0 = heure standard 1 = heure d'été Décalage à l'UTC + HHMMSS Le décalage est rapporté du point de vue de l'élément de réseau (PS, CMTS), et non du point de vue de l'abonné.	Chaîne de caractères ASCII	 1 octet 7 octets
Numéro de séquence	Chaque élément de réseau DOIT allouer un entier arithmétique unique à croissance monotone pour chaque message d'événement envoyé à un RKS donné. Pour les besoins de la présente Recommandation, croissance monotone doit être interprété comme croissance par pas de 1. Ceci est utilisé par le RKS pour déterminer si un message d'événement manque dans un élément de réseau donné.	Entier arithmétique	4 octets
Heure_d'événement	Date et heure générale d'un événement. Granularité d'une ms. Format: aaaammjjhhmmss.mmm	Chaîne de caractères ASCII	18 octets
Etat	Indicateurs d'état	Voir le Tableau 18	4 octets
Priorité	Indique l'importance à accorder par rapport aux autres messages d'événement. 255 = priorité supérieure 0 = priorité inférieure 128 = par défaut.	Entier arithmétique	1 octet

Tableau 16/J.179 – Structure d'attribut d'en-tête_de_message_d'événement

Nom de champ	Sémantique	Type de valeur	Longueur
Compte d'attribut	Indique le nombre d'attributs qui suivent (ou sont accolés à) cet en-tête dans le message d'événement en cours	Entier arithmétique	2 octets
Objet événement	Ceci est un "bouche-trou" pour de futures versions d'IPCablecom pour permettre un groupage de services. Ce pourra être IPCablecom Voix, IPCablecom Vidéo, etc. ou ce pourrait être IPCablecom, DOCSIS, etc. Il DOIT avoir une valeur de zéro pour IPCablecom version 1.0 et IPCablecom multimédia.	Entier arithmétique	1 octet

7.5.2 Structure de l'attribut ID de corrélation de facturation (BCID)

Le Tableau 17 décrit l'ID de corrélation de facturation (BCID, *billing correlation ID*). Le RKS, ou quelque autre application de l'arrière, utilise le BCID pour corréler les messages d'événement qui sont générés pour une seule transaction. C'est un des champs de l'en-tête de message d'événement. Le BCID est unique pour chaque transaction au niveau du réseau. Tous les messages d'événement provenant du même élément de réseau ayant le même BCID DOIVENT être envoyés au même RKS primaire sauf dans le cas de reprise sur défaillance auquel cas les messages d'événement DOIVENT être envoyés au RKS secondaire.

Tableau 17/J.179 – Description du BCID

Nom du champ	Sémantique	Type de valeur	Longueur
Horodatage	32 bits d'ordre supérieur de la référence horaire du NTP	Entier arithmétique	4 octets
ID_d'élément	Identifiant unique au niveau du réseau Cinq chiffres (numéro d'élément configuré de façon statique, unique au sein d'un domaine IPCablecom, dans la gamme 0 à 99 999).	Justifié à droite, chaîne de caractères ASCII à bourrage d'espaces	8 octets
Zone horaire	Identifie l'heure d'été et les décalages par rapport au temps universel (UTC). Heure d'été: 0 = heure standard 1 = heure d'été Décalage à l'UTC + HHMMSS Le décalage est rapporté du point de vue de l'élément de réseau (PS, CMTS), et non du point de vue de l'abonné.	Chaîne de caractères ASCII	 1 octet 7 octets
Compteur d'événement	Accroissement monotone pour chaque transaction	Entier arithmétique	4 octets

7.5.3 Structure de l'attribut Champ d'état

Le champ Etat de l'en-tête de message d'événement est un gabarit de 32 bits. Le bit 0 est le bit de plus faible poids; le champ est traité comme un entier arithmétique de quatre octets. Le Tableau 18 donne la description du champ Etat.

Tableau 18/J.179 – Description du champ Etat

Bit de début	Sémantique	Compte de bits
0	Indicateur d'erreurs: 0 = pas d'erreur 1 = erreur possible 2 = erreur reconnue 3 = réservé	2
2	Origine d'événement: 0 = élément de confiance 1 = élément incertain	1
3	Message d'événement mandaté: 0 = non mandaté, toutes les données sont connues par l'élément expéditeur 1 = mandaté, données envoyées par un élément de confiance au nom d'un élément incertain	1
4	Réservé. La valeur d'IPCablecom 1.0 DOIT être 0.	28

7.5.4 Structure de l'attribut Descripteur de QS

Le Tableau 19 décrit la structure des données du Descripteur de QS.

Tableau 19/J.179 – Structure des données de Descripteur de qualité de service

Nom de champ	Sémantique	Type de valeur	Longueur
Gabrit_binaire_ d'état	Gabarit binaire décrivant le contenu de la structure. (Voir le Tableau 20.)	Au bit près	4 octets
Nom_de_Classe_ de_service	Nom de profil de service	Chaîne de caractères ASCII à bourrage d'espaces, justifiée à droite	16 octets
Suite_de_ paramètres_de_QS	Paramètres de QS. Le contenu est déterminé par le Gabarit binaire d'état.	Entier arithmétique	Suite de longueur variable d'entiers arithmétiques de 32 bits

Le Tableau 20 décrit le champ Gabarit binaire d'état de QS de l'attribut Descripteur de QS. Les bits 2 à 17 décrivent le contenu de Suite_Paramètres_de-QS. Chacun de ces bits indique la présence (bit = 1) ou l'absence (bit = 0) du paramètre de QS nommé dans la suite. La localisation d'un paramètre de QS particulier dans la suite correspond à l'ordre dans lequel ce bit de paramètre est placé dans le gabarit binaire, en commençant par le bit de plus faible poids.

Chaque paramètre de qualité de service présent dans la Suite_Paramètres_de-QS doit occuper quatre octets. La définition et les codages des paramètres de qualité de service se trouvent à l'Appendice C de la Recommandation RFI de DOCSIS [1]; les paramètres de qualité de service dont la définition spécifie moins de quatre octets doivent être justifiés à droite (les quatre octets sont alors traités comme un entier arithmétique) dans les quatre octets alloués pour l'élément de suite.

Tableau 20/J.179 – Gabarit binaire d'Etat de QS

Bit de début	Sémantique	Compte de bits
0	Indication d'état: 0 = valeur illégale 1 = ressource Réservée mais pas Activée 2 = valeur illégale 3 = ressource Réservée et Activée	2
2	Type de programmation de flux de service	1
3	Intervalle d'allocation nominal	1
4	Gigue d'allocation tolérée	1
5	Allocations par intervalle	1
6	Taille d'allocation non sollicitée	1
7	Priorité de trafic	1
8	Débit soutenu maximal	1
9	Rafale de trafic maximal	1
10	Débit au trafic réservé minimal	1
11	Taille de paquet minimal	1
12	Rafale enchaînée maximale	1
13	Politique de demande/transmission	1
14	Intervalle d'interrogation nominal	1
15	Gigue d'interrogation tolérée	1
16	Outre passement de type de service IP	1
17	Retard aval maximal	1

7.6 Protocole RADIUS de comptabilité

Le présent paragraphe spécifie le protocole utilisé entre les éléments de réseau IPCablecom qui génèrent des messages d'événement (PS, CMTS) et le Serveur d'archivage (RKS). Ces éléments de réseau DOIVENT prendre en charge la comptabilité RADIUS (RFC 2866) [8] avec les extensions IPCablecom comme défini dans la présente Recommandation.

Le protocole de comptabilité RADIUS est un protocole client/serveur qui consiste en deux types de message: Demande de comptabilité et Réponse de comptabilité. Les éléments de réseau IPCablecom qui génèrent des messages d'événement sont des clients RADIUS qui envoient des messages Demande de comptabilité au RKS. Le RKS est un serveur RADIUS qui renvoie les messages Réponse de comptabilité aux éléments de réseau IPCablecom en indiquant qu'il a bien reçu et mémorisé le message d'événement.

Les messages d'événement sont formatés comme des paquets RADIUS Demande de comptabilité et Réponse de comptabilité comme spécifié en [8].

7.6.1 Authentification et confidentialité

Se reporter au § 8 pour les précisions concernant l'utilisation de IPsec pour la fourniture de l'authentification et de la confidentialité des messages RADIUS, et des précisions sur l'utilisation correcte du secret partagé RADIUS.

7.6.2 Attributs RADIUS standard

Chaque message RADIUS commence par l'en-tête standard RADIUS indiqué dans le Tableau 21.

Tableau 21/J.179 – En-tête de message RADIUS

Nom de champ	Sémantique	Longueur de champ
Code	Demande de comptabilité = 4 Réponse de comptabilité = 5	1 octet
Identifiant	Utilisé pour faire correspondre la demande de comptabilité et les messages de réponse de comptabilité.	1 octet
Longueur	Longueur totale du message RADIUS valeur minimale = 20 valeur maximale = 4096	2 octets
Authentifiant	Calculé selon la spécification RADIUS	16 octets

Deux attributs standard RADIUS DOIVENT suivre l'en-tête de message RADIUS: NAS-IP-Adresse et Acct_Status_Type. Ces deux champs sont inclus pour améliorer l'interopérabilité avec les implémentations existantes de serveur RADIUS car il y a des attributs obligatoires dans un paquet Demande de comptabilité RADIUS.

L'Adresse NAS-IP indique l'origine du message Demande de comptabilité et DOIT contenir l'adresse IP de l'élément de réseau IPCablecom d'origine.

L'attribut Acc-Type-Etat indique normalement si la Demande de comptabilité marque le début du service d'usager (Start) ou sa fin (Stop). Un message Demande de comptabilité IPCablecom peut contenir le début, la fin ou une mise à jour du service d'usager. Pour cette raison, une valeur d'Acct-Status-Type de Mise_à_jour_provisoire est utilisée pour représenter les messages d'événement IPCablecom.

Tableau 22/J.179 – Attributs RADIUS obligatoires

Nom	Type	Longueur	Valeur
Adresse-IP-NAS	4	6	Adresse IP de l'élément de réseau IPCablecom d'origine
Type-Etat-Acct	40	6	Mise à jour intérimaire = 3

Tableau 23/J.179 – Acct_Status_Type RADIUS

Type	Longueur	Valeur
40	6 octets	Mise à jour intérimaire = 3

Les attributs IPCablecom sont codés dans la structure Attributs spécifiques du vendeur (VSA, *vendor specific attributes*) de RADIUS comme décrit dans le présent paragraphe. Des attributs IPCablecom ou des attributs spécifiques du vendeur supplémentaires peuvent être ajoutés à des messages d'événement existants en ajoutant des VSA RADIUS supplémentaires au message.

L'attribut spécifique du vendeur inclut un champ pour identifier le vendeur, et l'Autorité chargée de l'assignation des numéros Internet (IANA, *Internet assigned numbers authority*) a alloué à IPCablecom un numéro d'entreprise privée de gestion de réseau SMI de 4491 pour le codage de ces attributs.

Tableau 24/J.179 – Structure Radius de VSA pour les attributs IPCablecom

Nom de champ	Sémantique	Longueur de champ
Type	Spécifique du vendeur = 26	1 octet
Longueur	Longueur totale d'attribut NOTE – La valeur est la Longueur du vendeur + 8	1 octet
ID de vendeur	CableLabs = 4491	4 octets
Type d'attribut de vendeur	Type d'attribut IPCablecom	1 octet (voir le Tableau 15)
Longueur d'attribut de vendeur	Longueur d'attribut IPCablecom	1 octet (voir le Tableau 15) NOTE – La valeur est la Longueur du vendeur + 2
Valeur d'attribut de vendeur	Valeur d'attribut IPCablecom	Octets de la longueur du vendeur

7.6.3 Syntaxe du paquet Demande de comptabilité RADIUS dans IPCablecom

```
<<RADIUS Demande de comptabilité>::==
 <En-tête de message RADIUS>
 <Attribut RADIUS NAS-IP-Adresse>
 <Attribut RADIUS Acct-Status-Type>
 <Message d'événement Paquet Câble>

<Message d'événement Paquet Câble>::==
 <RADIUS VSA pour Attribut d'en-tête d'EM IPCablecom>
 <Liste des attributs d'EM IPCablecom>

<Liste des attributs d'EM IPCablecom>::==
 <RADIUS VSA pour Attribut d'en-tête d'EM IPCablecom> |
 <Liste des attributs d'EM IPCablecom>
 <RADIUS VSA pour Attribut d'en-tête d'EM IPCablecom>>
```

L'en-tête de message d'événement est le premier attribut au sein d'un message d'événement donné. L'ordre des attributs de message d'événement qui suivent l'en-tête de message d'événement est arbitraire.

IPCablecom étend la comptabilité RADIUS en introduisant de nouveaux attributs et de nouvelles valeurs pour les attributs existants. Comme le protocole RADIUS est extensible de cette façon, on s'attend à ce que les implémentations de serveur RADIUS existantes aient besoin de modifications minimes pour prendre en charge l'ensemble des messages d'événement IPCablecom.

8 Exigences de sécurité

La sécurité pour les interfaces IPCablecom multimédia utilise les mécanismes de sécurité définis en [11] ainsi que en [1]. Le Tableau 25 résume les mécanismes de sécurité pour chacune des interfaces IPCablecom multimédia.

Tableau 25/J.179 – Interfaces de sécurité Multimédia

Interface	Description	Mécanismes de sécurité
pkt-mm-1	**CMTS – CM**	Authentification fondée sur HMAC définie par la Rec. UIT-T J.112, Annexe B sur l'interface RFI.
pkt-mm-2	PS – CMTS	IPsec ESP utilisant la gestion de clé fondée sur IKE ou Kerberos.
pkt-mm-3	AM – PS	IPsec ESP utilisant la gestion de clé fondée sur IKE ou Kerberos.
pkt-mm-4	PS – RKS	IPsec ESP utilisant la gestion de clé fondée sur IKE ou Kerberos.
pkt-mm-5	CMTS – RKS	IPsec ESP utilisant la gestion de clé fondée sur IKE ou Kerberos.
pkt-mm-6	Client – CMTS	Hors du domaine d'application de cette version de la présente Recommandation.
pkt-mm-7	Client – AM	Hors du domaine d'application de cette version de la présente Recommandation.
pkt-mm-8	AM – Homologue	Hors du domaine d'application de cette version de la présente Recommandation.
pkt-mm-9	CMTS – Réseau IP de câblo-opérateur	Hors du domaine d'application de cette version de la présente Recommandation.
pkt-mm-10	Client – Homologue	Hors du domaine d'application de cette version de la présente Recommandation.

Les paragraphes qui suivent décrivent la sécurité appliquée à chaque interface IPCablecom multimédia et spécifient des exigences ou extensions supplémentaires partout où c'est nécessaire.

8.1 Interface de QS CMTS – CM (pkt-mm-1)

Les messages de qualité de service de l'Annexe B à la Rec. UIT-T J.112 sont authentifiés en utilisant un code d'authentification de message par hachage (HMAC, *hash message authentication code*), qui est un hachage chiffré à clés. Le calcul de l'attribut HMAC qui DOIT être inclus dans les messages de qualité de service de l'Annexe B à la Rec. UIT-T J.112 est spécifié au § B.C.1.4.1 de [1].

8.2 Interface COPS Serveur de politique – CMTS (pkt-mm-2)

L'interface COPS Serveur de politique – CMTS DOIT être sécurisée en utilisant le protocole IPsec ESP, comme spécifié au § 7.2.1.3.2 de [11]. Les exigences de gestion de clés pour cette interface DOIVENT être conformes au § 7.2.1.4.1 de [11]. Pour cette interface, le Serveur de politique DOIT se conformer à toutes les exigences du contrôleur de porte dont la liste figure dans les § 7.2.1.3.2 et 7.2.1.4.1 de [11]. L'implémentation de IKE avec des clés prépartagées est exigée.

8.3 Interface COPS gestionnaire d'application – Serveur de politique (pkt-mm-3)

L'interface COPS gestionnaire d'application – Serveur de politique DOIT être sécurisée en utilisant le protocole IPsec ESP, comme spécifié au § 7.2.1.3.2 de [11]. Les exigences de gestion de clés pour cette interface DOIVENT être conformes au § 7.2.1.4.1 de [11]. Pour cette interface, le gestionnaire d'application DOIT se conformer à toutes les exigences du Contrôleur de porte des § 7.2.1.3.2 et 7.2.1.4.1 de [11]. L'implémentation de IKE avec clés prépartagées est nécessaire.

8.4 Interface de message d'événement Serveur de politique – RKS (pkt-mm-4)

L'interface de message d'événement Serveur de politique – RKS DOIT être sécurisée en utilisant le protocole IPsec ESP, comme spécifié au § 7.3.2 de [11]. La gestion de clés pour cette interface DOIT être identique à celle spécifiée pour l'interface CMTS-RKS au § 7.3.3.2 de [11]. L'implémentation d'IKE avec clés prépartagées est obligatoire.

8.5 Interface de message d'événement CMTS – RKS (pkt-mm-5)

L'interface de message d'événement CMTS – RKS DOIT être sécurisée en utilisant le protocole IPsec ESP, comme spécifié au § 7.3.2 de [11]. La gestion de clés pour cette interface est spécifiée au § 7.3.3.2 de [11]. L'implémentation d'IKE avec clés prépartagées est obligatoire, alors que l'implémentation d'IKE avec certificats et d'IPsec Kerbérisé est facultative.

9 Mappage d'un Profil de trafic spec de flux en DOCSIS

Un Profil de trafic définit les attributs de qualité de service du flux IP ou du flux de service de l'Annexe B à la Rec. UIT-T J.112 pour être utilisé en effectuant les opérations d'autorisation, réservation et engagement. Un Profil de trafic peut être défini via une des méthodes suivantes:

- Spec de flux;
- Nom de classe de service DOCSIS;
- Paramétrisation spécifique DOCSIS.

Le présent paragraphe décrit les procédures de mappage pour calculer les paramètres de qualité de service spécifiques de DOCSIS à partir des diverses représentations de Profil de trafic. Un Profil de trafic peut inclure les enveloppes d'autorisation, réservation ou engagement. Comme défini en [3], une Spec de flux consiste en une TSpec et une RSpec facultative.

9.1 Mappage de Spec de flux en type de programmation DOCSIS

Les Spec de flux prennent en charge deux types de services: Charge contrôlée et Garantie. Les services Charge contrôlée fournissent une garantie de bande passante minimale, mais pas de garantie de latence/délai. Les services Garantie fournissent à la fois des garanties de bande passante et de latence/délai. Le service Garantie peut être approximé au moyen de l'interrogation en temps réel DOCSIS et des types de programmation UGS. Les services Charge contrôlée peuvent être approximés au moyen du type de programmation au mieux de DOCSIS. Le numéro de service de Spec de flux dans la définition de Spec de flux distingue entre les services Charge contrôlée et Garantie. Le numéro de service 5 indique que la définition est pour le service Charge contrôlée, et le numéro de service 2 indique que la définition est pour le service Garantie. De plus, le service Charge contrôlée ne contient que les paramètres de seau de jetons de TSpec, et pas de RSpec. Le service Garantie DOIT contenir à la fois ceux de TSpec et de RSpec.

Pour les applications sensibles au retard et à la gigue comme la voix, la vidéo MPEG ou les jeux, on peut demander le service Garantie. Le CMTS peut alors utiliser les paramètres de Profil de trafic spécifiés dans la Spec de flux pour sélectionner un des deux types de programmation DOCSIS qui pourraient fournir le service Garantie: rtPS et UGS. Pour d'autres applications qui ne sont pas sensibles au retard, on peut demander le service Charge contrôlée, qui peut être utilisé pour fournir des garanties de bande passante minimale. Le Tableau 26 ci-dessous résume les choix.

Tableau 26/J.179 – Mappage des types de Spec de flux

Type de programmation DOCSIS	Numéro de service de Spec de flux	Exemple d'application
Service d'allocation non sollicitée (UGS)	2 (Garantie)	Voix sur IP
Service d'Interrogation en temps réel (rtPS)	2 (Garantie)	VPN
Au mieux (BE)	5 (Charge contrôlée)	Données Internet Au mieux

La procédure générale de transposition de Spec de flux à DOCSIS pour les flux de service amont est comme suit:

- à réception d'un message Etablir porte avec une Spec de flux le CMTS DOIT analyser l'en-tête de service TSpec pour déterminer si le service Charge contrôlée ou Garantie est demandé;
- si c'est le service Charge contrôlée, le CMTS DOIT alors utiliser seulement les paramètres TSpec pour résoudre les paramètres de programmation DOCSIS pour définir les paramètres de trafic DOCSIS pour un type de programmation DOCSIS au mieux;.
- si c'est le service Garantie, le CMTS DOIT examiner les valeurs des paramètres Tspec pour Débit Réservé (R) et Débit de seau (r). Si les deux valeurs sont égales, le CMTS DOIT alors utiliser la TSpec et la RSpec pour définir les paramètres de trafic DOCSIS pour un type de programmation UGS de DOCSIS;
- si le Débit Réservé (R) et le Débit de seau (r) ne sont pas égaux, le CMTS DOIT alors utiliser la TSpec et la RSpec pour définir les paramètres de trafic DOCSIS pour un type de programmation Interrogation en temps réel de DOCSIS.

Noter que deux autres types de programmation DOCSIS ne sont pas mentionnés ci-dessus. Ce sont:

- le Service d'allocation non sollicitée avec détection d'activité;
- le service d'interrogation en temps différé.

Si le gestionnaire d'application souhaite demander un de ces services, il ne peut le faire qu'en utilisant le Nom de classe de service ou la méthode de paramétrisation spécifique de DOCSIS pour la définition du Profil de trafic.

9.2 Mappage des Spec de flux en Paramètres de trafic DOCSIS

La Spec de flux est composée de deux parties, la TSpec et la RSpec. La TSpec décrit le trafic pour le flux, et la RSpec décrit le service désiré ; noter que pour un service Charge contrôlée, la RSpec n'est pas utilisée. Les paramètres de RSpec DOIVENT être spécifiés pour un service Garantie. Le CMTS DOIT ignorer les paramètres de RSpec pour un service Charge contrôlée. La RSpec est utilisée pour fournir des garanties de temps de latence pour les services garantis. Se reporter aux documents RFC 2210 [3], 1305 [2], 2211 [4], et 2212 [5] pour des informations complémentaires sur la façon dont ces paramètres devraient être utilisés par les gestionnaires d'application pour spécifier le Profil de trafic. Noter que l'interprétation des Flowspec d'IPCablecom multimédia diffère de celle des RFC sur les points suivants:

- le service Garantie, comme définit en [5] contrôle le délai de mise en file d'attente de couche 3 (c'est-à-dire, le délai associé à la programmation des paquets), alors que dans IPCablecom multimédia nous sommes concernés au premier chef par le contrôle du délai d'accès à la couche MAC DOCSIS. Par conséquent, on réserve les ressources de bande passante conformément au paramètre r de la Tspec plutôt qu'au R de la Rspec;
- comme défini dans [4], le service Charge contrôlée ne définit qu'un débit minimal garanti pour un flux. Le service Charge contrôlée d'IPCablecom multimédia facilite la définition du débit maximal pour un flux, ainsi que la définition des flux sans débit minimal garanti;
- le paramètre Terme de surlongueur du service Garantie n'est pas nécessaire dans IPCablecom multimédia, de telle sorte que le champ est redéfini pour permettre le contrôle de la gigue d'interrogation DOCSIS.

Paramètres TSpec:

- profondeur de seau (b), en octet;
- débit de seau (r), en octet/seconde;
- taille maximale de datagramme (M), en octet;

- unité régulée minimale (m), en octet;
- débit de crête (p), en octet/seconde.

Paramètres RSpec:

- débit Réservé (R), en octet/seconde;
- terme de surlongueur (S), en microseconde.

Le mappage de paramètre, approximé grossièrement, implique les associations suivantes pour les flux de service DOCSIS amont au mieux (BE, *best-effort*) et à Charge contrôlée aval. La procédure de transposition réelle devrait impliquer la normalisation de ces paramètres pour prendre en compte les besoins d'en-tête de couche 2 et 3.

- profondeur de seau TSpec (b) ~= Rafale de trafic maximal DOCSIS;
- taille maximale de datagramme TSpec (M) ~= <non demandé pour DOCSIS >;
- unité régulée minimale TSpec (m) ~= Taille de paquet au débit minimal réservé supposé DOCSIS;
- débit de seau TSpec (r) ~= Débit minimal réservé DOCSIS;
- débit de crête TSpec (p) ~= Débit soutenu maximal pour le service Charge contrôlée DOCSIS.

Pour les flux de service Garantie aval, les paramètres RSpec sont ajoutés pour fournir les garanties de temps de latence et de réservation.

- profondeur de seau TSpec (b) ~= Rafale de trafic maximal DOCSIS;
- taille maximale de datagramme TSpec (M) ~= <non demandé pour DOCSIS>;
- unité régulée minimale TSpec (m) ~= Taille de paquet au débit minimal réservé supposé DOCSIS;
- débit de seau TSpec (r) ~= Débit minimal réservé DOCSIS;
- débit réservé RSpec (R) ~= Débit soutenu maximal pour le service Charge contrôlée DOCSIS;
- terme de surlongueur RSpec ~= Temps de latence aval DOCSIS.

Le mappage de paramètres, approximé grossièrement, implique les associations suivantes pour les flux de service UGS de DOCSIS.

- profondeur de seau TSpec (b) = Taille maximale de datagramme TSpec (M) = Unité régulée minimale TSpec (m) ~= Taille d'allocation non sollicitée DOCSIS;
- débit de seau TSpec (r) ~= Débit de crête TSpec (p) = Débit réservé RSpec (R) ~= <non demandé pour DOCSIS>;
- terme de surlongueur RSpec ~= Gigue d'allocation tolérée DOCSIS.

De même, les associations suivantes s'appliquent pour les flux de services Interrogation en temps réel DOCSIS.

- profondeur de seau TSpec (b) ~= Rafale de trafic maximum DOCSIS;
- taille maximale de datagramme TSpec (M) ~= <non demandé pour DOCSIS>;
- débit de seau TSpec (r) ~= Débit soutenu maximale pour le service Garantie DOCSIS;
- débit réservé RSpec (R) ~= utilisé pour calculer l'intervalle d'interrogation;
- terme de surlongueur RSpec ~= Gigue d'interrogation tolérée.

Ce modèle d'abstraction permet des implémentations RSVP standard (comme prévu dans les scénarios 2 et 3) pour demander et recevoir le service à charge contrôlée ou à garantie du réseau sans avoir nécessairement besoin d'informations spécifiques DOCSIS.

Dans certaines situations où le gestionnaire d'application et le Serveur de politique sont effectivement au courant de DOCSIS, ils PEUVENT spécifier le Profil de trafic pour la porte qui utilise le Nom de classe de service DOCSIS ou le format de paramétrisation spécifique de DOCSIS.

Noter qu'il y a plusieurs paramètres de flux de service DOCSIS qui ne peuvent pas être directement solutionnés à partir des Spec de flux ; dans ces cas, la Recommandation IPCablecom multimédia définit des valeurs par défaut pour ces paramètres de flux de service. Si le gestionnaire d'application/Serveur de politique souhaite régler ces paramètres de flux de service à autre chose que les valeurs par défaut spécifiées par la présente Recommandation, le gestionnaire d'application/Serveur de politique DOIT utiliser les Noms de classe de service ou les formats de paramétrisation spécifique de DOCSIS pour définir le Profil de trafic.

Pour le service Garantie, le Débit minimal réservé et les Débits soutenus maximum sont réglés à la même valeur, et ils se fondent sur le Débit de seau, 'r'. Cela parce que le service Garantie fournit des garanties de temps de latence, ce qui signifie qu'un flux ne peut pas être soutenu à un débit supérieur à celui auquel la source a accepté de générer le trafic (lorsque la réservation a été faite à l'origine). Une réservation faite avec un Profil de trafic spécifiant un Débit de seau 'r' signifie que la source ne soutiendra pas un flux de trafic supérieur à 'r'. Et donc, il serait incorrect d'utiliser le Débit Réservé 'R' pour représenter un débit soutenu DOCSIS quelconque (minimal ou maximal), dans le cas du service Garantie.

Pour la programmation d'interrogation en temps réel, le CMTS utilise cependant le Débit Réservé R pour calculer l'intervalle d'interrogation, de sorte que les sources de trafic peuvent envoyer des rafales au débit R sans accroître le retard subi par les paquets qui attendent une opportunité de transmission amont DOCSIS. Bien que la source de trafic puisse générer du trafic au débit 'R' dans ce cas, le CMTS s'assurera que le débit soutenu ne viole pas 'r' à la longue.

Pour le service Charge contrôlée, comme il n'y a pas de garantie du temps de latence, et comme on veut permettre d'utiliser les concepts spécifiques de DOCSIS de garantie minimale aussi bien que de débit soutenu maximal, le débit de seau TSpec 'r' est mappé en débit minimal DOCSIS, et le Débit de crête TSpec 'p' est transposé en Débit soutenu maximal DOCSIS. Si une valeur zéro ou infinie est indiquée pour 'r', le paramètre Débit réservé minimal DOCSIS DOIT être omis. Si une valeur zéro ou infinie est indiquée pour 'p', le paramètre Débit soutenu maximal DOCSIS DOIT être omis.

9.3 Paramètres amont DOCSIS

La formule suivante doit être utilisée pour tous les calculs de taille de paquet amont: la taille DOCSIS DOIT être calculée à partir du FC de l'en-tête MAC de DOCSIS jusqu'à la fin du CRC. Cette valeur inclut la redondance d'en-tête Ethernet de 18 octets (6 octets pour l'adresse de source, 6 octets pour l'adresse de destination, 2 octets pour la longueur, et 4 octets pour le CRC). La valeur comprend aussi la redondance de couche MAC de DOCSIS, y compris l'en-tête de base DOCSIS (6 octets), l'en-tête étendu d'UGS (3 octets), et l'en-tête étendu BPI+ (5 octets).

$$\text{Taille d'allocation non sollicitée DOCSIS} = M + 32$$

L'exemple ci-dessus suppose que BPI+ [12] est activé.

9.3.1 Programmation d'allocation non sollicitée (UGS et UGS/AD)

La programmation d'allocation non sollicitée DOIT être utilisée lorsque le Numéro de service est 2 (Garantie), le Débit de crête, le Débit de seau, et le Débit Réservé sont tous égaux, et la Taille maximale de datagramme est égale à la Taille minimale de datagramme.

Les objets amont DOCSIS DOIVENT être réglés comme indiqué ci-dessus. Tous les codages de TLV de qualité de service des flux de service qui ne sont pas définis ici DOIVENT recevoir leurs valeurs par défaut indiquées par DOCSIS.

Les paramètres Débit au trafic soutenu maximal DOCSIS et Taille de paquet au débit réservé minimal supposé DOCSIS NE DOIVENT PAS être utilisés pour les flux amont.

Le paramètre Allocations par intervalle DOCSIS DOIT être mis à 1.

Le paramètre Intervalle d'allocation nominal DOCSIS DOIT être mis à Taille maximale de datagramme divisée par le Débit Réservé.

$$\text{Intervalle d'allocation nominal DOCSIS} = M/R$$

Le paramètre Gigue d'allocation tolérée DOCSIS DOIT être mis à Terme de surlongueur. Si la valeur est inférieure à la durée d'un mini-intervalle DOCSIS, la durée de mini-intervalle DOIT être utilisée à sa place. Si une valeur de zéro est spécifiée, la valeur par défaut de 800 µs DOIT être utilisée.

Le paramètre Intervalle d'interrogation nominal DOCSIS NE DOIT PAS être spécifié dans le Profil de trafic pour les flux de service UGS. Pour les flux de service UGS/AD, l'Intervalle d'interrogation nominal DOCSIS DOIT être explicitement spécifié dans le paramètre spécifique DOCSIS. Le CMTS DOIT utiliser le paramètre fourni dans le Profil de trafic pour le traitement des flux UGS/AD.

Le paramètre Gigue d'interrogation tolérée DOCSIS NE DOIT PAS être spécifié dans le Profil de trafic pour les flux UGS. Pour les flux de service UGS/AD, la Gigue d'interrogation tolérée DOCSIS DOIT être explicitement spécifiée dans le paramètre spécifique DOCSIS. Le CMTS DOIT utiliser le paramètre fourni dans le Profil de trafic pour le traitement des flux UGS/AD.

Le paramètre Politique de demande/transmission DOCSIS est un gabarit binaire, les bits 0 à 6 et 8 DOIVENT être établis pour les flux de service UGS et UGS/AD.

Le paramètre Taille d'allocation non sollicitée DOCSIS DOIT être calculé à partir de Taille maximale de datagramme en ajoutant la redondance DOCSIS de couche 2.

9.3.2 Programmation d'Interrogation en temps réel

La programmation d'Interrogation en temps réel DOIT être utilisée lorsque le Numéro de service est 2 (Service Garantie) et que Débit de crête n'est pas égal à Débit de seau ou que Taille maximale de datagramme n'est pas égal à Taille minimale de datagramme.

Les objets amont DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de qualité de service de flux de service qui ne sont pas définis ici DOIVENT recevoir leurs valeurs par défaut, comme indiqué par DOCSIS.

Le paramètre Débit au trafic soutenu maximal DOCSIS est donné en bits par seconde, et il inclut la redondance de couche MAC. La conversion à partir des paramètres spécifiques IP implique d'abord de déterminer la vitesse de mise en paquet en divisant le Débit de seau par la Taille minimale de datagramme. Cette valeur est alors multipliée par la taille de paquet, Taille minimale de datagramme, y compris la redondance de couche MAC, et le produit complet est échelonné d'octets en bits.

$$\text{Débit au trafic soutenu maximal DOCSIS} = r/m \times (m + 29) \times 8$$

Le paramètre DOCSIS Rafale de trafic maximal DOIT être réglé au plus grand de:

1) profondeur de seau y compris la redondance DOCSIS calculée en utilisant la Taille minimale de datagramme;

2) la valeur minimale spécifiée par DOCSIS de 1522.

$$\text{Rafale de trafic maximal DOCSIS} = \max ((\text{Profondeur de seau}/ m) \times (m + 29) , 1522)$$

Le paramètre Débit au trafic réservé minimum DOCSIS est le même que le Débit au trafic soutenu maximal DOCSIS.

Débit au trafic réservé minimal DOCSIS = r/m × (m + 29) × 8

Le paramètre Politique de demande/transmission DOCSIS est un gabarit binaire, tous les bits devraient être mis à 0.

Le paramètre Intervalle d'interrogation nominal DOCSIS DOIT être réglé à Débit Réservé divisé par la Taille minimale de datagramme.

Intervalle d'interrogation nominal DOCSIS = R/m

Le paramètre Gigue d'interrogation tolérée DOCSIS DOIT être réglé à Terme de surlongueur. Si la valeur est différente de zéro mais moins que la durée d'un mini-intervalle, il DOIT alors être réglé à la durée d'un mini-intervalle. Si une valeur de zéro est spécifiée, la Gigue d'interrogation tolérée DOCSIS DOIT être par défaut une valeur de 800 µs.

Gigue d'interrogation nominale DOCSIS = S

9.3.3 Programmation Au mieux

La programmation Au mieux DOIT être utilisée lorsque le Numéro de service est 5 (Charge contrôlée).

Les objets amont DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de qualité de service de flux de service qui ne sont pas définis ici DOIVENT recevoir leurs valeurs par défaut comme indiqué par DOCSIS.

La Priorité de trafic DOCSIS DOIT être mise à 5.

Le paramètre Débit au trafic soutenu maximal DOCSIS est donné en bits par seconde, y compris la redondance de couche MAC. La conversion à partir des paramètres spécifiques du protocole IP implique d'abord de déterminer la vitesse de mise en paquet en divisant le Débit de crête par la Taille minimale de datagramme. Cette valeur est alors multipliée par la taille de paquet, Taille minimale de datagramme, amendée pour inclure la redondance de couche MAC, et le produit complet est échelonné des octets aux bits. Le Débit au trafic soutenu maximal DOCSIS DOIT être converti de la Taille minimale de datagramme tant qu'une valeur différente de zéro est fournie. Si l'objet Taille minimale de datagramme est zéro, ce paramètre DOIT être omis.

Débit au trafic soutenu maximal DOCSIS = p/m × (m + 29) × 8

Le paramètre Rafale de trafic maximal DOCSIS DOIT être réglé au plus grand de:

1) profondeur de seau y compris la redondance DOCSIS calculée en utilisant la Taille minimale de datagramme;

2) la valeur minimale spécifiée par DOCSIS de 1522.

Rafale de trafic maximal DOCSIS = max (Profondeur de seau / m) × (m + 29), 1522)

Le paramètre Débit au trafic réservé minimal DOCSIS est calculé de manière similaire au Débit au trafic soutenu maximal DOCSIS, excepté qu'au lieu d'utiliser le paramètre Débit de crête, on utilise le Débit de seau.

Débit au trafic réservé minimal DOCSIS = r/m × (m + 29) × 8

9.3.4 Codages de classification de paquets amont

9.3.4.1 Demandes de classification de paquet amont DOCSIS

Les objets amont DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de classification qui ne sont pas définis ici DOIVENT être donnés par leurs valeurs par défaut, comme indiqué par DOCSIS.

S'il est défini par le CMTS, le paramètre Identifiant de classeur DOCSIS DOIT être utilisé.

Le paramètre Priorité de règle DOCSIS DOIT être réglé à la valeur Priorité dans l'objet Classeur.

Le paramètre Etat d'activation de classification DOCSIS DOIT être réglé à actif (1) lorsque la porte utilisant le flux de service est engagée, et pour tous les autres cas, il DOIT être réglé à inactif (0).

L'action Changement de service dynamique DOCSIS PEUT utiliser les opérations DSC Ajout de classeur (0), Remplacer Classeur (1) et Supprimer Classeur (2) selon la Recommandation RFI DOCSIS.

Le paramètre Protocole IP DOCSIS DOIT être réglé à la même signification que Protocole.

Le paramètre Adresse IP de source DOCSIS DOIT être réglé à la même adresse que celle qui se trouve dans l'objet Classeur, tant qu'une valeur différente de zéro est fournie. Si l'adresse spécifiée dans l'objet Classeur est zéro, ce paramètre DOIT être omis.

Le paramètre Gabarit de source IP DOCSIS DOIT être omis.

Les paramètres Début de Port de source IP et Fin de Port de source IP DOCSIS DOIVENT être réglés à la même valeur de port de transport que dans l'objet Classeur.

Le paramètre Adresse IP de destination DOCSIS DOIT être réglé à la même adresse que dans l'objet Classeur, tant qu'est fournie une valeur différente de zéro. Si l'adresse spécifiée dans l'objet Classeur est zéro, ce paramètre DOIT être omis.

Le paramètre Gabarit de destination IP DOCSIS DOIT être omis.

Les paramètres Début de port de destination IP DOCSIS et Fin de port de destination IP DOCSIS DOIVENT être réglés au même port de transport que l'objet Classeur, tant qu'est fournie une valeur différente de zéro. Si le Port IP de destination est spécifié comme une valeur de zéro dans l'objet Classeur, le TLV de Fin de port IP de destination DOCSIS DOIT être omis.

Les paramètres Codages de classification de paquet LLC Ethernet de DOCSIS DOIVENT être omis.

Les paramètres Codages de classification de paquet DOCSIS 802.1P/Q DOIVENT être omis.

9.4 Paramètres DOCSIS aval

9.4.1 Codages de qualité de service aval pour le service Garantie

Les codages de TLV de qualité de service de flux de service aval DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de qualité de service de flux de service qui ne sont pas définis ici DOIVENT être donnés pour leurs valeurs par défaut, comme indiqué par DOCSIS.

Les paramètres aval DOCSIS sont calculés en utilisant l'en-tête MAC de DOCSIS à partir de l'octet suivant le HCS jusqu'à la fin du CRC. La redondance de couche MAC (c'est-à-dire, Ethernet) est de 18 octets (6 octets pour l'adresse de source, 6 octets pour l'adresse de destination, 2 octets pour la longueur, et 4 octets pour le CRC).

Sur la base de cette redondance, le paramètre Taille de paquet au débit réservé minimal supposé DOCSIS DOIT être calculé comme:

$$\text{Taille de paquet au débit réservé minimal supposé DOCSIS} = m + 18$$

Le paramètre Débit au trafic soutenu maximal DOCSIS est donné en bits par seconde, y compris la redondance de couche MAC. La conversion à partir des paramètres spécifiques d'IP implique d'abord de déterminer la vitesse de mise en paquet en divisant le Débit de seau par la Taille minimale de datagramme. Cette valeur est ensuite multipliée par la taille de paquet, Taille minimale de datagramme, corrigée pour inclure la redondance de couche MAC, et le produit complet est échelonné des octets aux bits. Le Débit au trafic soutenu maximal DOCSIS DOIT être calculé comme:

Débit au trafic soutenu maximal DOCSIS = r/m × (m + 18) × 8

Le Débit au trafic réservé minimal DOCSIS est égal au Débit au trafic soutenu maximal DOCSIS.

Noter qu'il y a une légère différence entre les modes de calcul du Débit au trafic soutenu maximal DOCSIS et du Débit au trafic réservé minimal DOCSIS dans IPCablecom multimédia et IPCablecom DQoS. IPCablecom multimédia se fonde sur r et IPCablecom DQoS se fonde sur p. Ceci est dû au fait que dans DQoS, r = p, alors qu'en multimédia ces valeurs diffèrent (auquel cas r est la bonne valeur de débit à utiliser).

Le paramètre Rafale de trafic maximal DOCSIS DOIT être réglé au plus grand de:

1) profondeur de seau incluant la redondance DOCSIS calculée en utilisant la Taille minimale de datagramme;
2) la valeur minimale spécifiée par DOCSIS de 1522.

Rafale de trafic maximal DOCSIS = max ((Profondeur de seau / m) × (m + 18), 1522)

Le paramètre Priorité de trafic DOCSIS DOIT être réglé à 5.

Le paramètre Temps de latence aval DOCSIS DOIT être réglé à Terme de surlongueur, si Terme de surlongueur est différent de zéro. Si Terme de surlongueur est zéro, ce paramètre NE DOIT PAS être rempli.

9.4.2 Codages de qualité de service aval pour le service Charge contrôlée

Les codages de TLV de qualité de service de flux de service aval DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de qualité de service de flux de service qui ne sont pas définis ici DOIVENT être donnés pour leurs valeurs par défaut, comme indiqué par DOCSIS.

Les paramètres aval DOCSIS sont calculés en utilisant l'en-tête MAC de DOCSIS à partir de l'octet qui suit le HCS jusqu'à la fin du CRC. La redondance de couche MAC (c'est-à-dire, Ethernet) est de 18 octets (6 octets pour l'adresse de source, 6 octets pour l'adresse de destination, 2 octets pour la longueur, et 4 octets pour le CRC).

Sur la base de cette redondance, le paramètre Taille de paquet au débit réservé minimal supposé DOCSIS DOIT être calculé comme:

Taille de paquet au débit réservé minimal supposé DOCSIS = m + 18

Le paramètre Débit au trafic soutenu maximal DOCSIS est donné en bits par seconde, y compris la redondance de couche MAC. La conversion à partir des paramètres spécifiques d'IP implique d'abord de déterminer la vitesse de mise en paquet en divisant le Débit de seau par la Taille minimale de datagramme. Cette valeur est ensuite multipliée par la taille de paquet, Taille minimale de datagramme, corrigée pour inclure la redondance de couche MAC, et le produit complet est échelonné des octets aux bits. Le Débit au trafic soutenu maximal DOCSIS DOIT être calculé comme:

Débit au trafic soutenu maximal DOCSIS = p/m × (m + 18) × 8

Le paramètre Débit au trafic réservé minimal DOCSIS est calculé de manière similaire à celle du Débit au trafic soutenu maximal DOCSIS, excepté qu'on utilise Débit de seau au lieu de Débit de crête.

Débit au trafic réservé minimal DOCSIS = r/m × (m + 18) × 8

Le paramètre Rafale de trafic maximal DOCSIS DOIT être réglé au plus grand de:

1) profondeur de seau incluant la redondance DOCSIS calculée en utilisant la Taille maximale de datagramme;
2) la valeur minimale spécifiée de DOCSIS de 1522.

Rafale de trafic maximal DOCSIS = max ((Profondeur de seau / M) × (M + 18), 1522)

Le paramètre Priorité de trafic DOCSIS DOIT être réglé à 5.

Le paramètre Temps de latence aval DOCSIS NE DOIT PAS être rempli.

9.4.3 Codages de classification de paquets aval

9.4.3.1 Demandes de classification de paquets aval DOCSIS

Les objets de classification aval DOCSIS DOIVENT être réglés comme indiqué ci-dessous. Tous les codages de TLV de classification DOIVENT être donnés pour leurs valeurs par défaut, comme indiqué par DOCSIS.

S'il est défini par le CMTS, le paramètre Identifiant de classeur DOCSIS DOIT être utilisé.

S'il est défini par le CMTS, le paramètre Identifiant de flux de service DOCSIS DOIT être utilisé.

Le paramètre Priorité de règle DOCSIS DOIT être réglé à la valeur Priorité spécifiée dans l'objet Classeur.

Le paramètre Etat d'activation de Classification DOCSIS DOIT être mis à actif (1) lorsque la porte utilisant le flux de service est engagée, et pour tous les autres cas, il DOIT être mis à inactif (0).

L'action Changement de service dynamique DOCSIS PEUT utiliser les opérations DSC Ajout de classeur (0), Changer de classeur (1) et Supprimer casseur (2) selon la Recommandation RFI de DOCSIS.

Les champs Type de service IP et Gabarit IP NE DOIVENT PAS être utilisés.

Le paramètre Protocole IP DOCSIS DOIT être réglé à la valeur d'ID de protocole spécifiée dans l'objet Classeur.

Le paramètre Adresse IP de source DOIT être réglé à l'adresse de source fournie dans l'objet Classeur, tant qu'est fournie une valeur différente de zéro. Si l'adresse spécifiée dans l'objet Classeur est zéro, ce paramètre DOIT être omis.

Le paramètre Gabarit de source IP DOCSIS DOIT être omis.

Les paramètres Début de Port de source IP DOCSIS et Fin de Port de source IP DOCSIS DOIVENT être réglés à la même valeur de port de transport que celle indiquée dans le Classeur, tant qu'est fournie une valeur différente de zéro. Si le Port IP de source est spécifié comme une valeur de zéro dans le Classeur, le TLV de Fin de port IP de source DOCSIS DOIT être omis.

Le paramètre Adresse IP de destination DOCSIS DOIT être réglé à la même adresse qu'indiquée dans l'objet Classeur.

Le paramètre Gabarit de destination IP DOCSIS DOIT être omis.

Les paramètres Début de port de destination IP DOCSIS et Fin de port de destination IP DOCSIS DOIVENT être réglés au même port qu'indiqué dans l'objet Classeur.

Les codages de classification de paquet LLC Ethernet DOCSIS DOIVENT être omis.

Les codages de classification de paquet DOCSIS 802.1P/Q DOIVENT être omis.

10 Flux de messages

Le présent paragraphe donne deux scénarios d'interaction entre les divers éléments de réseau précédemment introduits dans la présente Recommandation. La première interaction souligne à relativement haut niveau les échanges de messages de base qui ont lieu sans le cadre d'IPCablecom multimédia pour autoriser, réserver et engager les ressources de réseau d'accès du scénario 1. La seconde interaction donne une description détaillée de chaque message et attribut impliqué dans les interfaces de qualité de service et de message d'événement IPCablecom multimédia.

10.1 Séquence de message de base

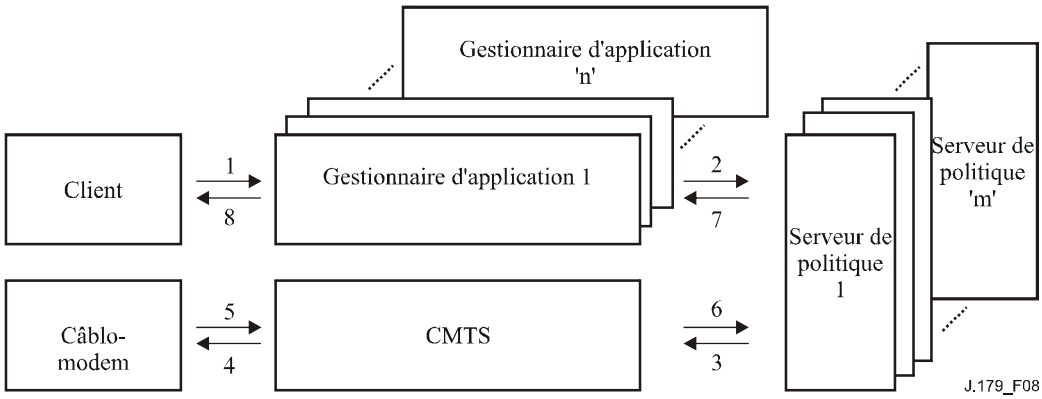

Figure 8/J.179 – Séquence de message de base

1) Le client produit une demande d'établissement de session au gestionnaire d'application via la signalisation de couche d'application. Le client peut s'authentifier auprès du gestionnaire d'application durant cette étape.

2) Avant que le gestionnaire d'application n'active la session, le gestionnaire d'application produit un Etablir porte (dans un message DECISION COPS) et l'envoie au Serveur de politique afin de déterminer si la demande d'établissement de session peut être autorisée. Le message comporte:
   a) l'AMID;
   b) l'ID d'abonné;
   c) l'ID de transaction;
   d) le Classeur;
   e) le Profil de trafic pour le flux.

3) A réception de la demande, le Serveur de politique vérifie la demande par rapport aux règles de politique, et si la demande est approuvée, envoie un message Etablir porte au CMTS. Le message comporte:
   a) l'AMID;
   b) l'ID d'abonné;
   c) l'ID de transaction;
   d) le Classeur;
   e) le Profil de trafic pour le Flux (Autorisé, Réservé et Engagé).

4) Le CMTS utilise les informations de Classeur et Profil de trafic pour déclencher l'activation du flux en produisant les messages DSx DOCSIS appropriés.

5) Le câblo-modem accuse réception de l'échange de messages DSx approprié.

6) Le CMTS produit un Acc Etablir porte au Serveur de politique en réponse au message Etablir porte reçu à l'étape 3. Le message comporte:
   a) l'AMID;
   b) l'ID de transaction;
   c) l'ID de porte.

7) En réponse le Serveur de politique va générer un Acc Etablir porte au gestionnaire d'application ; cela indique au gestionnaire d'application que la Demande de politique a été

admise et que la demande du client peut continuer, et que les ressources dans le réseau sous-jacent ont été réservées. Le message comporte:

a) l'AMID;

b) l'ID de transaction;

c) l'ID de porte.

8) Le gestionnaire d'application, à réception de l'Acc Etablir porte va informer le client de la possibilité de poursuivre l'établissement de la session.

10.2 Séquence de message détaillée

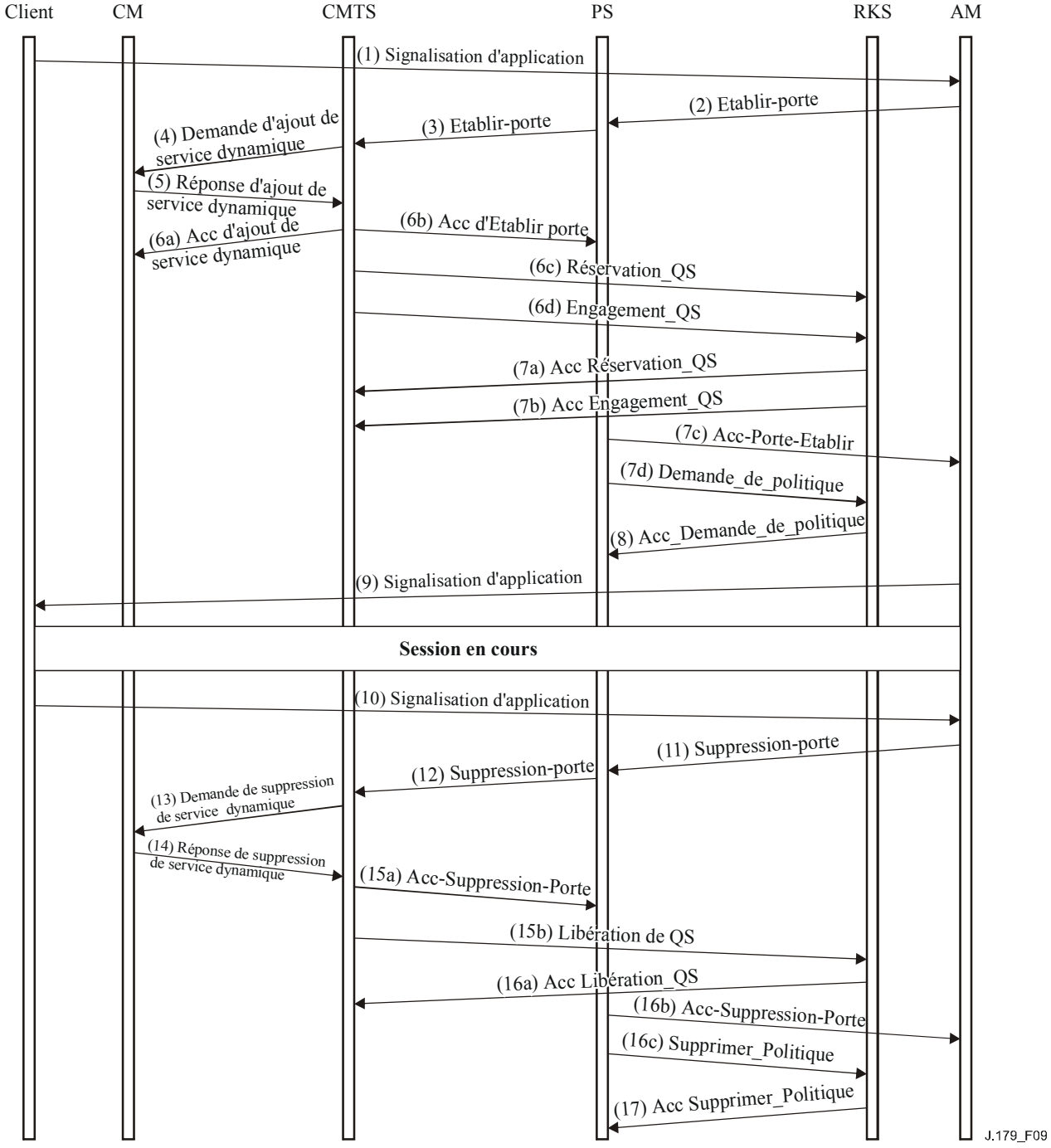

Figure 9/J.179 – Séquence de message détaillée

Les pages qui suivent décrivent en détail les messages échangés dans un exemple de session IPCablecom multimédia. Les numéros de bande passante sont de simples exemples, et ne se rapportent à aucun service particulier. Seules les ressources de réseau d'accès amont sont réservées et engagées, dans un souci de clarté. Les TLV se rapportant au BPI ont elles aussi été laissées de côté dans le même souci.

1) Le client initialise la session en interrogeant un gestionnaire d'application sur les ressources nécessaires pour les besoins de l'application. Cela pourrait être par exemple, un jeu vidéo fondé sur un logiciel, qui demande des ressources pour jouer en ligne. Cette signalisation est hors du domaine d'application de la présente Recommandation.

2) Après réception de la signalisation d'application du client, le gestionnaire d'application envoie un message Etablir porte au Serveur de politique, demandant les ressources nécessaires pour cette session.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x0	Op-Code 0x02	Type de Client 0X800A	
Longueur de message 0x000000C0				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00001234				
Objet de contexte COPS				
Longueur 0x0008			C-Num 0x02	C-Type 0x01
Type de demande (R-Type) 0x0008 (Demande de configuration)			Type de message (M-Type) 0x0000	
Objet Décision COPS				
Longueur 0x0008			C-Num 0x06	C-Type 0x01
Code de commande 0x0001 (Configuration d'installation)			Fanions 0x0000	
En-tête d'objet SI client COPS				
Longueur 0x00A0			C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x9999			Commande de porte 0x0004 (Etablir porte)	

Objet AMID multimédia			
Longueur 0x0008		S-Num 0x02	S-Type 0x01
AMID 0x00005678			
Objet ID d'abonné multimédia			
Longueur 0x0008		S-Num 0x03	S-Type 0x01
ID d'abonné 0x01010101			
Objet Spec de porte multimédia			
Longueur 0x0010		S-Num 0x05	S-Type 0x01
Fanions 0x01	Champ DSCP/TOS 0x00	Gabarit DSCP/TOS 0x00	ID de classe de session 0x00
Temporisateur T1 0x00C8 (200 s)		Temporisateur T2 0x012C (300 s)	
Temporisateur T3 0x003C (60 s)		Réservé	
Objet Spec de flux multimédia			
Longueur 0x005C		S-Num 0x07	S-Type 0x01
Enveloppe 0x07	Numéro de service 0x02	Réservé	Réservé
Enveloppe autorisée			
Débit de seau de jeton [r] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Taille de seau de jeton [b] (codé en virgule flottante IEEE) 0x43480000 (200 octets)			
Débit de pointe de données [p] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Unité régulée minimale [m] 0x000000C8 (200 octets)			
Taille maximale de paquet [M] 0x000000C8 (200 octets)			
Débit [R] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Terme de surlongueur [S] 0x00000320 (800 µs)			

Enveloppe réservée			
Débit de seau de jeton [r] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Taille de seau de jeton [b] (codé en virgule flottante IEEE) 0x43480000 (200 octets)			
Débit de crête de données [p] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Unité régulée minimale [m] 0x000000C8 (200 octets)			
Taille maximale de paquet [M] 0x000000C8 (200 octets)			
Débit [R] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Terme de surlongueur [S] 0x00000320 (800 µs)			
Enveloppe engagée			
Débit de seau de jeton [r] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Taille de seau de jeton [b] (codé en virgule flottante IEEE) 0x43480000 (200 octets)			
Débit de crête de données [p] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Unité régulée minimale [m] 0x000000C8 (200 octets)			
Taille maximale de paquet [M] 0x000000C8 (200 octets)			
Débit [R] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Terme de surlongueur [S] 0x00000320 (800 µs)			
Objet Classeur Multimédia			
Longueur 0x0018		S-Num 0x06	S-Type 0x01
Réservé	ID de protocole 0x11 (17 UDP)	Champ DSCP/TOS 0x00	Gabarit DSCP/TOS 0x00
Adresse IP de source 0x01010101			
Adresse IP de destination 0x02020202			
Port de source 0x1234		Port de destination 0x9876	

Priorité 0x0040 (64)	Réservé

3) Après que le Serveur de politique ait reçu le message Etablir porte du gestionnaire d'application, il vérifie pour voir si la demande est autorisée, et si elle l'est, envoie un Etablir porte au CMTS.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x0	Op-Code 0x02	Type de client 0X800A	
Longueur de message 0x000000EC				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00005678				
Objet Contexte COPS				
Longueur 0x0008			C-Num 0x02	C-Type 0x01
Type de demande (R-Type) 0x0008 (Demande de configuration)			Type de message (M-Type) 0x0000	
Objet Décision COPS				
Longueur 0x0008			C-Num 0x06	C-Type 0x01
Code de commande 0x0001 (Configuration d'installation)			Fanions 0x0000	
En-tête d'objet SI client COPS				
Longueur 0x00CC			C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x0001			Commande de porte 0x0004 (Etablir porte)	
Objet AMID multimédia				
Longueur 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objet ID d'abonné multimédia				
Longueur 0x0008			S-Num 0x03	S-Type 0x01

<table>
<tr><td colspan="4">ID d'abonné
0x01010101</td></tr>
<tr><td colspan="4">Objet Spec de porte multimédia</td></tr>
<tr><td colspan="2">Longueur
0x0010</td><td>S-Num
0x05</td><td>S-Type
0x01</td></tr>
<tr><td>Direction
0x01</td><td>Champ DSCP/TOS
0x00</td><td>Gabarit DSCP/TOS
0x00</td><td>ID de classe de session
0x00</td></tr>
<tr><td colspan="2">Temporisateur T1
0x00C8 (200 s)</td><td colspan="2">Temporisateur T2
0x012C (300s)</td></tr>
<tr><td colspan="2">Temporisateur T3
0x003C (60 s)</td><td colspan="2">Réservé</td></tr>
<tr><td colspan="4">Objet Spec de flux multimédia</td></tr>
<tr><td colspan="2">Longueur
0x005C</td><td>S-Num
0x07</td><td>S-Type
0x01</td></tr>
<tr><td>Enveloppe
0x07</td><td>Numéro de service
0x02</td><td>Réservé</td><td>Réservé</td></tr>
<tr><td colspan="4">Enveloppe autorisée</td></tr>
<tr><td colspan="4">Débit de seau de jeton [r] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
<tr><td colspan="4">Taille de seau de jeton [b] (codé en virgule flottante IEEE)
0x43480000 (200 octets)</td></tr>
<tr><td colspan="4">Débit de pointe de données [p] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
<tr><td colspan="4">Unité régulée minimale [m]
0x000000C8 (200 octets)</td></tr>
<tr><td colspan="4">Taille maximale de paquet [M]
0x000000C8 (200 octets)</td></tr>
<tr><td colspan="4">Débit [R] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
<tr><td colspan="4">Terme de surlongueur [S]
0x00000320 (800 μs)</td></tr>
<tr><td colspan="4">Enveloppe réservée</td></tr>
<tr><td colspan="4">Débit de seau de jeton [r] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
<tr><td colspan="4">Taille de seau de jeton [b] (codé en virgule flottante IEEE)
0x43480000 (200 octets)</td></tr>
<tr><td colspan="4">Débit de pointe de données [p] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
<tr><td colspan="4">Unité régulée minimale [m]
0x000000C8 (200 octets)</td></tr>
<tr><td colspan="4">Taille maximale de paquet [M]
0x000000C8 (200 octets)</td></tr>
<tr><td colspan="4">Débit [R] (codé en virgule flottante IEEE)
0x461C4000 (10 000 bit/s)</td></tr>
</table>

Terme de surlongueur [S] 0x00000320 (800 µs)			
Enveloppe engagée			
Débit de seau de jeton [r] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Taille de seau de jeton [b] (codé en virgule flottante IEEE) 0x43480000 (200 octets)			
Débit de pointe de données [p] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Unité régulée minimale [m] 0x000000C8 (200 octets)			
Taille maximale de paquet [M] 0x000000C8 (200 octets)			
Débit [R] (codé en virgule flottante IEEE) 0x461C4000 (10 000 bit/s)			
Terme de surlongueur [S] 0x00000320 (800 µs)			
Objet Classeur multimédia			
Longueur 0x0018		S-Num 0x06	S-Type 0x01
Réservé	ID de protocole 0x11	Champ DSCP/TOS 0x00	Gabarit DSCP/TOS 0x00
Adresse IP de source 0x01010101			
Adresse IP de destination 0x02020202			
Port de source 0x1234		Port de destination 0x9876	
Priorité 0x0040 (64)		Réservé	
Objet Info de génération d'événement Multimédia			
Longueur 0x002C		S-Num 0x08	S-Type 0x01
Adresse de Serveur d'archivage primaire 0x03030303			
Port de RKS primaire 0x1111		Réservé	
Adresse de Serveur d'archivage secondaire 0x04040404			
Port de RKS secondaire 0x1111		Réservé	

BCID 0x3E4812082020202020313436302D3035303030300003DB77

4) Si le contrôle d'admission du CMTS réussit, le CMTS va lancer la réservation et l'engagement des ressources du réseau d'accès en envoyant un message DSA au câblo-modem.

0	1	2	3
En-tête de gestion MAC			
ID de transaction 0x0007		Flux de service US 0x18	Longueur 0x29
ID flux de service 0x02	Longueur 0x04	Valeur 0x0000	
Valeur (suite) 0001		ID de service 0x03	Longueur 0x02
Valeur 0x0001		Ensemble param. de QS 0x06	Longueur 0x01
Valeur 0x06 (Ad.+Act.)	Type de program. 0x0F	Longueur 0x01	Valeur 0x06
Taille UGS 0x13	Longueur 0x02	Valeur 0x00E8 (232 octets)	
Intervalle nominal d'alloc. 0x14	Longueur 0x04	Valeur 0x0000	
Valeur (suite) 4E20 (20,000 µs)		Alloc par intervalle 0x16	Longueur 0x01
Valeur 0x01	Politique RX/TX 0x10	Longueur 0x04	Valeur 0x00
Valeur (suite) 00017F			Gigue d'allocation tolérée 0x15
Longueur 0x04	Valeur 0x000003		
Valeur (suite) 20 (800 µs)	Classeur paquet US 0x16	Longueur 0x13	ID de classeur 0x02

Longueur 0x02	Valeur 0x0001		ID de flux de service 0x04
Longueur 0x04	Valeur 0x000000		
Valeur (suite) 01	Priorité de règle 0x05	Longueur 0x01	Valeur 0x40
Etat Act. classeur 0x06	Longueur 0x01	Valeur 0x01 (Actif)	Action Changement 0x07 (Ajout)
Longueur 0x01	Valeur 0x00	Classeur paquet IP 0x09	Longueur 0x001A
Protocole IP 0x02	Longueur 0x02	Valeur 0x0011 (17 UDP)	
Adresse IP Src. 0x03	Longueur 0x04	Valeur 0x0101	
Valeur (suite) 0101		Début port IP Src 0x07	Longueur 0x02
Valeur 0x1234		Fin port IP Src 0x08	Longueur 0x02
Valeur 0x1234		Début port IP dest 0x09	Longueur 0x02
Valeur 0x9876		Fin port IP dest 0x0A	Longueur 0x02
Valeur 0x9876			

5) Le câblo-modem répond au système CMTS avec un message DSA-RSP (*réponse d'ajout de service dynamique*).

0	1	2	3
En-tête de gestion MAC			
ID de transaction 0x0007		Code de confirm. 0x00	

6a) Le CMTS termine la transaction avec un DSA-ACK (*accusé de réception de DSA*)

0	1	2	3
En-tête de gestion MAC			
ID de transaction 0x0007		Code de confirm. 0x00	

6b) Une fois que la DSA-RSP est reçue du câblo-modem par le CMTS, confirmant la réussite de la transaction, le CMTS va envoyer un Acc Etablir porte au Serveur de politique.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x1	Op-Code 0x03	Type de client 0X800A	
Longueur de message 0x0000003C				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00005678				
Objet Type de rapport COPS				
Longueur 0x0008			C-Num 0x12	C-Type 0x01
Type de rapport (R-Type) 0x0001 (Succès)			Réservé	
En-tête d'objet SI client COPS				
Longueur 0x0024			C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x0001			Commande de porte 0x0005 (Acc Etablir porte)	
Objet AMID multimédia				
Longueur 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objet ID d'abonné multimédia				
Longueur 0x0008			S-Num 0x03	S-Type 0x01
ID d'abonné 0x01010101				
Objet ID de porte multimédia				
Longueur 0x0008			S-Num 0x04	S-Type 0x01
ID de porte 0x12345678				

6c) Le CMTS va aussi envoyer un message d'événement Réservation_de_QS pour signaler au serveur d'archivage que les ressources de réseau d'accès ont été réservées.

0	1	2	3
En-tête Radius de Demande de comptabilité			
Spec. Radius de vendeur 0x1A	Longueur 0x54	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type (En-tête d'EM) 0x01	Longueur 0x4E
Version 0x0003		BCID 0x3D48	
BCID (suite) 1208202020202031343630 2D3035303030300003DB77			
		Type de message d'événement 0x0007 (Réserveur de QS)	
Type d'élément 0x0002 (CMTS)		ID d'élément 0x2020202031323334	
		Zone horaire 0x302D303530303030	
		Numéro de séquence 0x0000	
Numéro de séquence (suite) 0001		Heure d'événement 0x3230	
Heure d'événement (suite) 303331323036303030303030 2E303030			
Etat 0x00000000			
Priorité 0x80 (128)	Compte d'attribut 0x0004		Objet Evénement 0x00
Spec. Radius de vendeur 0x1A	Longueur 0x5C	Id de vendeur 0x0000	

ID de vendeur (suite) 118B		Type 0x20	Longueur 0x56
Descripteur_de_QS 0x0003FFFD0000000000000000000000000000000000000600004E2000000320000000001000000E8			
0000000000000000000000BE40000004000000000000005F20000017F000186A0000007D000FF0000			
00000000			
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x1E	Longueur 0x06
SF_ID 0x00000001			
Spec. Radius de vendeur 0x1A	Longueur 0x0A	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x32	Longueur 0x04
Direction du flux 0x0001 (amont)		Spec. Radius de vendeur 0x1A	Longueur 0x0A
ID de vendeur 0x0000118B			
Type 0x37	Longueur 0x04	Elément_Demandant_QS 0x0001 (Serveur de politique)	

6d) Immédiatement après l'envoi du message d'événement Réservation_de_QS au RKS, le CMTS va envoyer le message d'événement Engagement_de_QS au RKS. Ceci est dû au fait que les ressources de réseau d'accès sont réservées et engagées en une seule étape.

0	1	2	3
En-tête Radius de Demande de comptabilité			
Spec. Radius de vendeur 0x1A	Longueur 0x54	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type (En-tête d'EM) 0x01	Longueur 0x4E
Version 0x0003		BCID 0x3E48	
BCID (suite) 120820202020203134363 02D3035303030300003DB77			
		Type de message d'événement 0x0013 (Engagement de QS)	
Type d'élément 0x0002 (CMTS)		ID d'élément 0x2020202031323334	
		Zone horaire 0x302d303530303030	
		Numéro de séquence 0x0000	
Numéro de séquence (suite) 0002		Heure d'événement 0x3230	
Heure d'événement (suite) 30333132303630303030302E303030			
Etat 0x00000000			
Priorité 0x80 (128)	Compte d'attribut 0x0003		Objet Evénement 0x00
Spec. Radius de vendeur 0x1A	Longueur 0x5C	ID de vendeur 0x0000	

ID de vendeur (suite) 118B		Type 0x20	Longueur 0x56
Descripteur de QS 0x0003FFFD0000000000000000000000000000000000000000600004E200000320000000001000000E8			
0000000000000000000000BE400000040000000000000005F20000017F000186A0000007D000FF0000			
00000000			
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x1E	Longueur 0x06
ID_de_Flux de service 0x00000001			
Spec. Radius de vendeur 0x1A	Longueur 0x0A	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x32	Longueur 0x04
Direction du flux 0x0001 (amont)			

7a) Après réception et enregistrement du message d'événement Réservation_QS, le RKS accuse réception du message.

0	1	2	3
En-tête Radius de Réponse de comptabilité			

7b) Après réception et enregistrement du message d'événement Engagement_QS, le RKS accuse réception du message.

0	1	2	3
En-tête Radius de Réponse de comptabilité			

7c) Suite à la réception de Acc-Etablir-porte du CMTS, le Serveur de politique va envoyer un Acc-Etablir-porte au gestionnaire d'application pour terminer la transaction.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x1	Op-Code 0x03	Type de client 0X800A	
Longueur de message 0x0000003C				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00001234				
Objet Type de rapport COPS				
Longueur 0x0008			C-Num 0x12	C-Type 0x01
Type de rapport (R-Type) 0x0001 (Succès)			Réservé	
En-tête d'objet Si de client COPS				
Longueur 0x0024			C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x9999			Commande de porte 0x0005	

Objet AMID multimédia		
Longueur 0x0008	S-Num 0x02	S-Type 0x01
AMID 0x00005678		
Objet ID d'abonné multimédia		
Longueur 0x0008	S-Num 0x03	S-Type 0x01
ID d'abonné 0x01010101		
Objet ID de porte multimédia		
Longueur 0x0008	S-Num 0x04	S-Type 0x01
ID de porte 0x12345678		

7d) Le Serveur de politique va aussi envoyer un message d'événement Demande de politique au RKS pour suivre la Demande de politique et le résultat associé.

0	1	2	3
En-tête Radius de Demande de comptabilité			
Spec. Radius de vendeur 0x1A	Longueur 0x54	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type (En-tête d'EM) 0x01	Longueur 0x4E
Version 0x0001		BCID 0x3E48	
BCID (suite) 12082020202020313436302D3035303030300003DB77			
		Type de message d'événement 0x0015 (Demande de politique)	
Type d'élément 0x0004 (Serveur de politique)		ID d'élément 0x2020202035363738	
		Zone horaire 0x302E303530303030	
		Numéro de séquence 0x0000	

Numéro de séquence (suite) 0001		Heure d'événement 0x3230	
Heure d'événement (suite) 3033313230363030303030302E323130			
Etat 0x00000000			
Priorité 0x80 (128)	Compte d'attribut 0x0004		Objet Evénement 0x00
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x3D	Longueur 0x06
ID_Gestionnaire_d'Application 0x00005678			
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x34	Longueur 0x06
ID_d'abonné 0x01010101			
Spec. Radius de vendeur 0x1A	Longueur 0x0A	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x3C	Longueur 0x04
Etat_Décision_Politique 0x0001 (Politique approuvée)		Spec. Radius de vendeur 0x1A	Longueur 0x1C
ID de vendeur 0x0000118B			
Type 0x31	Longueur 0x16	FEID 0x0000	
FEID (suite) 00000000000000005061636B65744361626C65			

8) Après réception et enregistrement du message d'événement Demande_de_politique, le RKS accuse réception du message.

0	1	2	3
En-tête Radius de Réponse de comptabilité			

9) Le Gestionnaire d'application va répondre au client pour l'informer qu'il peut maintenant commencer à jouer. Cette signalisation est en dehors du domaine d'application de la présente Recommandation.

10) Lorsque le client en a fini avec l'application, il va le notifier au gestionnaire d'application. Cette signalisation est en dehors du domaine d'application de la présente Recommandation.

11) Le gestionnaire d'application va terminer la session en envoyant un message Supprimer-porte au Serveur de politique.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x0	Op-Code 0x02	Type de client 0x800A	
Longueur de message 0x00000044				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00001234				
Objet Contexte COPS				
Longueur 0x0008			C-Num 0x02	C-Type 0x01
Type de demande (R-Type) 0x0008 (Demande de Configuration)			Type de message (M-Type) 0x0000	
Objet Décision COPS				
Longueur 0x0008			C-Num 0x06	C-Type 0x01
Code de commande 0x0001 (Configuration d'installation)			Fanions 0x0000	
En-tête d'objet COPS SI du client				
Longueur 0x0014			C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x9998			Commande de porte 0x000A (Supprimer porte)	

Objet AMID multimédia		
Longueur 0x0008	S-Num 0x02	S-Type 0x01
AMID 0x00005678		
Objet ID d'abonné multimédia		
Longueur 0x0008	S-Num 0x03	S-Type 0x01
ID d'abonné 0x01010101		
Objet ID de porte multimédia		
Longueur 0x0008	S-Num 0x04	S-Type 0x01
ID de porte 0x12345678		

12) Le Serveur de politique va ordonner au CMTS de supprimer la session en envoyant Supprimer porte

0	1	2	3
En-tête COPS			
Version 0x1	Fanions 0x0	Op-Code 0x02	Type de client 0x800A
Longueur de message 0x00000044			
Objet Outil COPS			
Longueur 0x0008		C-Num 0x01	C-Type 0x01
Outil 0x00005678			
Objet Contexte COPS			
Longueur 0x0008		C-Num 0x02	C-Type 0x01
Type de demande (R-Type) 0x0008 (Demande de Configuration)		Type de message (M-Type) 0x0000	
Objet Décision COPS			
Longueur 0x0008		C-Num 0x06	C-Type 0x01
Code de commande 0x0001 (Configuration d'installation)		Fanions 0x0000	
En-tête d'objet COPS SI de client			
Longueur 0x0014		C-Num 0x09	C-Type 0x01
Objet ID de transaction multimédia			
Longueur 0x0008		S-Num 0x01	S-Type 0x01

ID de transaction 0x0002	Commande de porte 0x000A (Supprimer porte)	
Objet ID de transaction multimédia		
Longueur 0x0008	S-Num 0x02	S-Type 0x01
AMID 0x00005678		
Objet ID d'abonné multimédia		
Longueur 0x0008	S-Num 0x03	S-Type 0x01
ID d'abonné 0x01010101		
Objet ID de porte multimédia		
Longueur 0x0008	S-Num 0x04	S-Type 0x01
ID de porte 0x12345678		

13) Le CMTS va supprimer les ressources de réseau d'accès en envoyant une DSD-REQ (*demande de suppression de service dynamique*) au câblo-modem.

0	1	2	3
En-tête de gestion MAC			
ID de transaction 0x0008		Réservé	
ID de flux de service 0x00000001			

14) Le câblo-modem va accuser réception de la suppression de session avec une DSD-RSP (*réponse DSD*).

0	1	2	3
En-tête de gestion MAC			
ID de transaction 0x0008		Code de confirmation 0x00	Réservé

15a) Le CMTS va terminer la transaction de commande de porte par un Acc-Supprimer-porte.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x1	Op-Code 0x03	Type de client 0X800A	
Longueur de message 0x00000034				
Objet Outil COPS				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00005678				
Objet Type de rapport COPS				
Longueur 0x0008			C-Num 0x12	C-Type 0x01
Type de rapport (R-Type) 0x0001			Réservé	
En-tête d'objet SI client COPS				
Longueur 0x001C			C-Num 0x09	C-Type 0x01
Objet multimédia ID de transaction				
Longueur 0x0008			S-Num 0x01	S-Type 0x01
ID de transaction 0x0002			Commande de porte 0x000B (Acc-Supprimer-porte)	
Objet multimédia AMID				
Longueur 0x0008			S-Num 0x02	S-Type 0x01
AMID 0x00005678				
Objet multimédia ID de porte				
Longueur 0x0008			S-Num 0x04	S-Type 0x01
ID de porte 0x12345678				

15b) Aussi à réception de la réponse DSD-RSP, le CMTS va informer le serveur RKS que les ressources de réseau d'accès ont été libérées en envoyant un message Libération_de_QS.

0	1	2	3
En-tête Radius de Demande de comptabilité			
Spec. Radius de vendeur 0x1A	Longueur 0x54	ID de vendeur 0x0000	

ID de vendeur (suite) 118B		Type (En-tête d'EM) 0x01	Longueur 0x4E
Version 0x0001		BCID 0x3E48	
BCID (suite) 120820202020203134363 02D3035303030300003DB77			
		Type de message d'événement 0x0008 (Libération de QS)	
Type d'élément 0x0002 (CMTS)		ID d'élément 0x2020202031323334	
		Zone horaire 0x302D303530303030	
		Numéro de séquence 0x0000	
Numéro de séquence (suite) 0003		Heure d'événement 0x3230	
Heure d'événement (suite) 30323132303630303030302E333030			
Etat 0x00000000			
Priorité 0x80 (128)	Compte d'attribut 0x0005		Objet Evénement 0x00
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x1E	Longueur 0x06
ID_de_Flux_de_service 0x00000001			
Spec. Radius de vendeur 0x1A	Longueur 0x0A	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x32	Longueur 0x04
Direction du flux 0x0001 (Amont)		Spec. Radius de vendeur 0x1A	Longueur 0x0A
ID de vendeur 0x0000118B			

Type 0x38	Longueur 0x04	Cause de libération de QS 0x0001 (Porte fermée par PS)	
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x36	Longueur 0x06
Info_d'utilisation_de_QS 0x77777777 (octets)			
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x3F	Longueur 0x06
Info_d'heure_de_QS 0x77777777 (secondes)			

16a) Après réception et enregistrement du message d'événement Libération_de_QS, le RKS accuse réception du message.

0	1	2	3
En-tête Radius de Réponse de comptabilité			

16b) Après réception de l'Acc-Supprimer-porte du CMTS, le Serveur de politique va envoyer un Acc-Supprimer-porte pour terminer la transaction de commande de porte.

0		1	2	3
En-tête COPS				
Version 0x1	Fanions 0x1	Op-Code 0x03	Client-Type 0X800A	
Longueur de message 0x00000034				
Objet COPS Outil				
Longueur 0x0008			C-Num 0x01	C-Type 0x01
Outil 0x00001234				
Objet COPS Type de rapport				
Longueur 0x0008			C-Num 0x12	C-Type 0x01
Type de rapport (R-Type) 0x0001 (Succès)			Réservé	
En-tête d'objet COPS SI de client				
Longueur 0x001C			C-Num 0x09	C-Type 0x01

Objet multimédia ID de transaction		
Longueur 0x0008	S-Num 0x01	S-Type 0x01
ID de transaction 0x9998	Commande de porte 0x000B (Acc-Supprimer-porte)	
Objet multimédia AMID		
Longueur 0x0008	S-Num 0x02	S-Type 0x01
AMID 0x00005678		
Objet multimédia ID de porte		
Longueur 0x0008	S-Num 0x04	S-Type 0x01
ID de porte 0x12345678		

16c) Le Serveur de politique envoie un message d'événement Supprimer-politique au RKS pour terminer l'ensemble du processus.

0	1	2	3
En-tête Radius de Demande de comptabilité			
Spec. Radius de vendeur 0x1A	Longueur 0x54	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type (En-tête d'EM) 0x01	Longueur 0x4E
Version 0x0001		BCID 0x3E48	
BCID (suite) 1208202020202031343630 2D3035303030300003DB77			
		Type de message d'événement 0x0016 (Supprimer_Politique)	
Type d'élément 0x0004 (Serveur de politique)		ID d'élément 0x2020202035363738	
		Zone horaire 0x302D303530303030	
		Numéro de séquence 0x0000	

Numéro de séquence (suite) 0002		Heure d'événement 0x3230	
Heure d'événement (suite) 3032313230363030303030302E343030			
Etat 0x00000000			
Priorité 0x80	Compte d'attribut 0x0004		Objet Evénement 0x00
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x3D	Longueur 0x06
ID_Gestionnaire_d'application 0x00005678			
Spec. Radius de vendeur 0x1A	Longueur 0x0C	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x34	Longueur 0x06
ID_d'abonné 0x01010101			
Spec. Radius vendeur 0x1A	Longueur 0x0A	ID de vendeur 0x0000	
ID de vendeur (suite) 118B		Type 0x3A	Longueur 0x04
Cause_de_Suppression_de_Politique 0x0001 (Demande du gestionnaire d'application)		Spec. Radius vendeur 0x1A	Longueur 0x1C
ID de vendeur 0x0000118B			
Type 0x31	Longueur 0x16	FEID 0x0000	
FEID (suite) 00000000000000005061636B65744361626C65			

17) Après réception et enregistrement du message d'événement Supprimer_Politique, le RKS accuse réception du message.

0	1	2	3
En-tête Radius de Réponse de comptabilité			

11 Questions encore à l'étude

Les questions suivantes ont été identifiées comme sujets d'études pour l'avenir.

- Prescriptions pour le traitement des erreurs (c'est-à-dire, définir des codes d'erreur spécifiques pour des conditions spécifiques).
- Acheminement des messages de commande de porte dans le cadre Multimédia.
- Prescriptions pour la synchronisation d'état (c'est-à-dire, granularité, portée, fréquence, etc.) et le mécanisme du protocole.
- Prise en charge par le protocole des stratégies de reprise sur erreur et de redondance. Egalement, comment devraient être traitées les portes dans le cas d'un échec de la connexion COPS.
- Mécanisme de formatage et d'approvisionnement de règle de Serveur de politique: approvisionnement du CMS avec XML DTD spécifique du Multimédia.
- Prise en charge de la Suppression d'en-tête de charge utile (PHS, *payload header suppression*).
- Délivrance du message de commande de porte pour les connexions défaillantes (actuellement ces messages sont supprimés).

Appendice I

Informations de base

I.1 Introduction

Le présent appendice décrit une architecture fournissant une plate-forme fondée sur IP pour prendre en charge des applications et services multimédia variés qui nécessitent un traitement de la qualité de service sur les réseaux d'accès par câblo-modem. Cette architecture définit des composants fonctionnels et des interfaces de protocole qui permettront à chaque câblo-opérateur de livrer des services multimédia à qualité de service améliorée satisfaisant leurs propres exigences professionnelles.

Comme l'architecture ignore tout de la couche d'application, les détails des offres multimédia particulières, de l'approvisionnement spécifique, et des fonctions du système de prise en charge de la signalisation et du fonctionnement (OSS, *operation support system*) nécessaires pour la fourniture d'un service particulier sont en dehors du domaine d'application du présent document. IPCablecom multimédia se concentre plutôt sur la fourniture d'une qualité de service fiable sur le réseau d'accès, en s'intéressant spécifiquement aux questions techniques de l'autorisation de politique, de la signalisation de qualité de service, de la comptabilité des ressources, et de la sécurité.

I.1.1 Aperçu général d'IPCablecom

Le projet IPCablecom vise à définir des spécifications d'interfaces utilisées par la communauté des fabricants pour développer des équipements interopérables capables de fournir la voix fondée sur IP, la vidéo et d'autres services multimédia à grande vitesse sur des systèmes par câble hybride optique coaxial (HFC) conformes aux Recommandations sur les réseaux d'accès à haut débit par câblo-modem.

La téléphonie utilisant le protocole Internet (VoIP, *voice over Internet protocol*) a été le premier service de ce type identifié pour la fourniture sur la plate-forme IPCablecom. Le jeu actuel de Recommandations IPCablecom, sous le nom d'IPCablecom-T, définit une architecture IPCablecom optimisée pour la fourniture de services VoIP résidentiels. Voir la Rec. UIT-T J.160.

I.1.2 Motivations d'IPCablecom multimédia

Comme VoIP, les applications multimédia les plus populaires (par exemple, jeux en ligne, média en continu, communications vidéo en temps réel) sont sensibles au délai de transmission au sein du réseau. De plus, comme de nouvelles applications émergent qui sont conçues pour tirer parti des réseaux haut débit, elles aussi présentent des exigences particulières de bande passante et de temps de latence.

Actuellement, les utilisateurs haut débit reçoivent les services multimédia par la fourniture de données au mieux. Il en résulte une fourniture en ligne incohérente, de qualité variable selon la disponibilité de la bande passante, et l'encombrement du réseau. Un réseau capable de réserver des ressources et de fournir la bande passante à la demande selon les exigences de service permettrait de fournir une large gamme de nouveaux services à ses utilisateurs.

Pour répondre à ces besoins pour les services VoIP, IPCablecom définit actuellement les mécanismes de signalisation de la Qualité de service dynamique (DQoS) qui permettent aux applications vocales de demander et obtenir de la bande passante à partir de la couche de liaison des données de câblo-modem. Le cadre actuel de la DQoS prend aussi en charge l'établissement de session sécurisé au moyen de l'authentification et l'autorisation de point d'extrémité et un modèle de traçage de l'utilisation fondée sur la qualité de service. Fondée sur ces capacités de base, l'architecture IPCablecom est bien positionnée pour prendre en charge les applications et services existants et futurs de qualité de service améliorée au-delà de la téléphonie.

Le principal objectif d'IPCablecom multimédia est de définir le cadre architectural central nécessaire pour prendre en charge les applications multimédia fondées sur la qualité de service. Au cœur de ce cadre sont les mécanismes de qualité de service définis dans les spécifications de DQoS de câblo-modem et d'IPCablecom. Le bon achèvement de cette initiative fournira un fort fondement technique pour la prise en charge à l'avenir d'offres de services multimédia spécifiques.

I.2 Objectifs et domaine d'application d'IPCablecom multimédia

Le principal objectif d'IPCablecom multimédia est de développer une architecture généraliste qui:

- prenne en charge une large gamme de services capables de fournir la qualité de service, au-delà de la voix;
- se fonde sur les mécanismes existants définis dans les Recommandations IPCablecom-T et câblo-modem;
- requière un ensemble minimal d'extensions en plus d'IPCablecom-T;
- réduise la complexité de développement en éliminant les exigences spécifiques de la téléphonie lorsqu'elles ne sont pas applicables (par exemple, interconnexion au RTPC, surveillance électronique, modèles de facturation de la téléphonie, etc.);

- coexiste avec l'architecture IPCablecom-T de telle façon que:
  - les exigences d'IPCablecom multimédia soient suffisantes pour prendre en charge une plate-forme de fourniture de services multimédia fondée sur la qualité de service;
  - les exigences d'IPCablecom multimédia puissent être ajoutées aux composants fonctionnels IPCablecom-T existants pertinents;
  - les exigences d'IPCablecom-T puissent être ajoutées aux composants fonctionnels IPCablecom multimédia existants pertinents;
- accepte les adaptateurs MTA d'IPCablecom-T comme appareils "Client de type 2" (définis) dans l'architecture IPCablecom multimédia;
- interopère avec les architectures IPCable2Home (Rec. UIT-T J.191) et Câblo-modem (Recommandations UIT-T J.112 et J.122)

Le présent paragraphe décrit les exigences qui ont été identifiées afin de satisfaire aux objectifs ci-dessus et dessine les contours de la portée du travail qui sera effectué par l'architecture.

I.2.1 Exigences

Cette architecture dessine les contours des interactions de divers éléments de réseau, y compris les appareils Client, les gestionnaires d'application, les Serveurs de politique, les CMTS et les câblo-modems. Ces éléments de réseau sont formellement définis dans la section Cadre multimédia de la présente Recommandation. Cependant, des hypothèses spécifiques concernant l'autorité de gestion et les relations de confiance ont été faites sur certains de ces éléments de réseau, et ces hypothèses sont reprises ci-dessous comme exigences d'IPCablecom multimédia. Des exigences de haut niveau au sujet de la signalisation de qualité de service, de gestion de ressources, d'échange de messages d'événement et de sécurité sont également traitées dans le présent paragraphe.

IPCablecom multimédia est indifférent au protocole de signalisation d'application en ce qui concerne l'interaction entre l'appareil Client et le gestionnaire d'application. On doit comprendre que l'appareil Client et le gestionnaire d'application peuvent prendre en charge diverses applications et protocoles de signalisation (par exemple, HTTP, SIP, H.323, DCS, NCS, etc.).

Dans l'architecture IPCablecom multimédia, les appareils Client:

1) résident directement sur le réseau d'accès de l'opérateur, ou dans le domicile;
2) peuvent être des appareils autonomes ou peuvent contenir un câblo-modem incorporé;
3) sont considérés comme des éléments de réseau qui ne sont pas de confiance et, comme tels, l'opérateur du réseau peut en exiger certaines formes d'authentification de l'usager, de l'application, ou de l'échange de messages d'application.

Les gestionnaires d'application dans l'architecture IPCablecom multimédia:

1) résident sur le réseau géré par l'opérateur;
2) sont gérés par l'opérateur;
3) sont responsables de la vérification de l'habilitation des clients qui demandent un service au réseau de l'opérateur à recevoir ce service.

Les Serveurs de politique dans l'architecture IPCablecom multimédia:

1) résident dans le réseau géré par l'opérateur;
2) sont gérés par l'opérateur;
3) sont responsables de la prise des décisions de politique se rapportant à la qualité de service sur la base des règles de politique définies par l'opérateur.

Les systèmes CMTS sont responsables dans l'architecture IPCablecom multimédia de la mise en application des décisions de politique se rapportant à la qualité de service.

Exigences de signalisation de qualité de service et de gestion de ressources

- Les mécanismes de demande de ressource dynamique DOIVENT être définis, y compris:
  - l'accès à tous les modèles de programmation de qualité de service de câblo-modem;
  - les demandes de ressources à temps limité;
  - les demandes de ressources à volume limité.
- Les modèles de réservation de ressources à une seule phase et à deux phases DOIVENT être pris en charge.
- Les réservations unidirectionnelles DOIVENT être acceptées; la prise en charge des réservations bidirectionnelles devrait être permise.
- Les gestionnaires d'application peuvent initialiser les demandes de réservation de qualité de service au nom des appareils Client.
- L'architecture DOIT fournir le moyen de détecter les défaillances du client et/ou du serveur et réclamer les ressources associées.

Exigences de collecte des informations de message d'événement

- Un ensemble complet de messages d'événement DOIT être défini pour retracer l'utilisation des ressources flux par flux, y compris:
  - les événements de politique retraçant une demande de ressources du réseau d'accès, soumise aux règles de politique définies par l'opérateur;
  - les événements de politique retraçant la libération des ressources du réseau d'accès;
  - les événements de qualité de service retraçant la réservation, l'engagement et la libération des ressources de qualité de service;
  - les événements supplémentaires prenant en charge l'utilisation de ressources flux par flux fondée sur le volume (comptage métrique des paquets).
- Les informations suivantes devraient être contenues dans les messages:
  - source de la demande (par exemple, abonné ou fournisseur de service);
  - caractéristiques des ressources demandées;
  - décision d'autorisation de politique.

Exigences de sécurité

- La sécurité est exigée et DOIT être définie pour les interfaces pertinentes.
- Les clients qui initialisent la signalisation de qualité de service peuvent demander certaines formes d'authentification des utilisateurs ou de l'application.

I.2.2 Domaine d'application

Les éléments suivants dessinent les contours du domaine d'application de la phase initiale actuelle de l'initiative IPCablecom multimédia:

- l'architecture s'intéressera aux éléments de réseau qui résident:
  1) sur le réseau d'accès;
  2) au sein du réseau IP géré par un seul opérateur.
- L'architecture définira les protocoles et interfaces nécessaires pour prendre en charge l'autorisation de politique, le contrôle d'admission de qualité de service, la comptabilité des ressources, et les mécanismes de sécurité.
- L'architecture ne s'intéressera pas aux questions spécifiques des applications (par exemple, approvisionnement de service, signalisation, facturation, etc).

- L'architecture ne s'intéressera pas aux exigences d'approvisionnement et d'OSS pour les éléments de réseau IPCablecom multimédia.
- L'architecture se concentrera sur la gestion de la qualité de service entre le système CMTS et le câblo-modem.
- L'architecture n'empêchera pas la fourniture de services en multidiffusion, même si elle ne s'intéresse pas explicitement aux considérations sur la multidiffusion.
- L'architecture ne s'intéressera pas aux exigences de transposition et d'interopérabilité de traduction d'adresse de réseau (NAT, *network address translation*) pour l'instant.
- L'architecture ne définira pas d'exigences de qualité de service de bout en bout dans la phase actuelle.
- L'architecture fournira la prise en charge du "Client de type 1" et du "Scénario 1" (comme défini plus haut) dans la présente phase. Dans un but d'exhaustivité et par anticipation de son élaboration prochaine, le présent appendice décrit les trois types de client et les trois scénarios de service.
- L'architecture ne fournira pas de découverte topologique dynamique (c'est-à-dire, les relations entre les gestionnaires d'application, les Serveurs de politique, les CMTS, les RKS, etc.) dans la présente phase.
- L'architecture ne s'intéressera pas à l'authentification de client par le gestionnaire d'application.
- L'architecture ne s'intéressera pas aux mécanismes spécifiques par lesquels le Serveur de politique obtient et gère les règles de politique.
- L'architecture ne prendra pas en charge la collecte des événements spécifiques d'application ou de service pour leur incorporation dans le système d'audit de l'utilisation des ressources.

I.3 Cadre IPCablecom multimédia

Pour faciliter la fourniture d'applications multimédia large bande de qualité exigeant des garanties de qualité de service, le cadre multimédia offre des fonctionnalités généralistes de qualité de service fondées sur des mécanismes définis dans les spécifications IPCablecom-T de base. Pour le soutien de cet objectif, plusieurs éléments clé de réseau ont té identifiés et profilés. La Figure I.1 présente les composants IPCablecom Multimédia qui résident dans le réseau IP géré par l'opérateur.

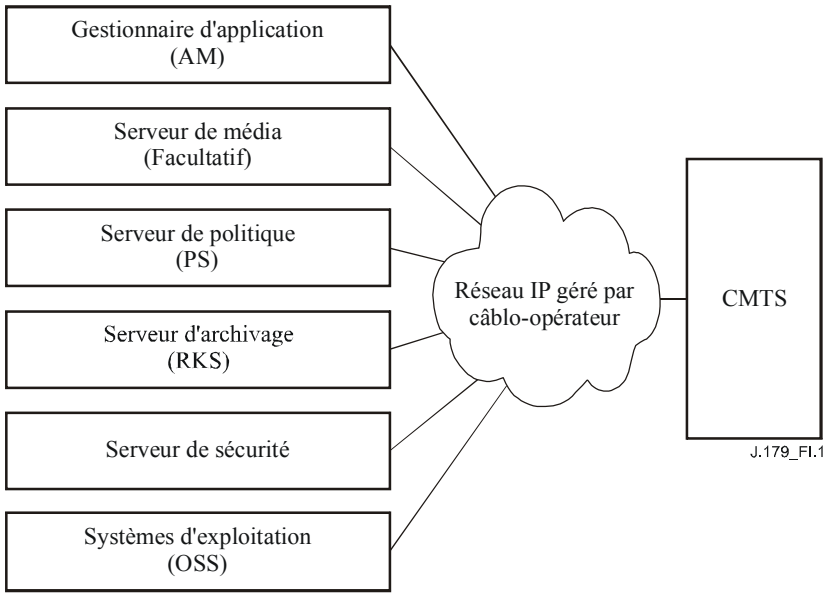

Figure I.1/J.179 – Eléments de réseau multimédia de l'opérateur

En plus des capacités d'aide au système CMTS pour la qualité de service fondées sur des paramètres, l'architecture du réseau multimédia de l'opérateur consiste en un distributeur de serveurs qui peut être re-divisé selon les zones suivantes:

- un gestionnaire d'application et un Serveur de média (facultatif) hébergeant une application capable de gérer la qualité de service;
- un cadre d'administration de politique qui fournit l'autorisation et le contrôle d'admission de qualité de service en soutient de la gestion des ressources réseau;
- un sous-système d'échange de messages d'événements utilisé pour surveiller et enregistrer les informations d'utilisation des ressources.

Des systèmes d'exploitation pour effectuer les fonctions d'approvisionnement, de gestion de réseau, et de surveillance peuvent aussi être inclus dans la configuration du réseau multimédia de l'opérateur, bien que ces éléments sortent du domaine d'application de l'architecture actuelle.

I.3.1 Modèle de référence de l'architecture IPCablecom multimédia

En plus des éléments qui résident au sein de la tête d'extrémité du réseau de l'opérateur, un certain nombre d'appareils clients situés dans les locaux de l'abonné ont également été définis afin de compléter le modèle. La Figure I.2 montre le cadre architectural d'IPCablecom multimédia et identifie les interfaces clés entre les composants. Ces interfaces ont été étiquetés par des identifiants auxquels il sera fait référence dans la discussion qui suit.

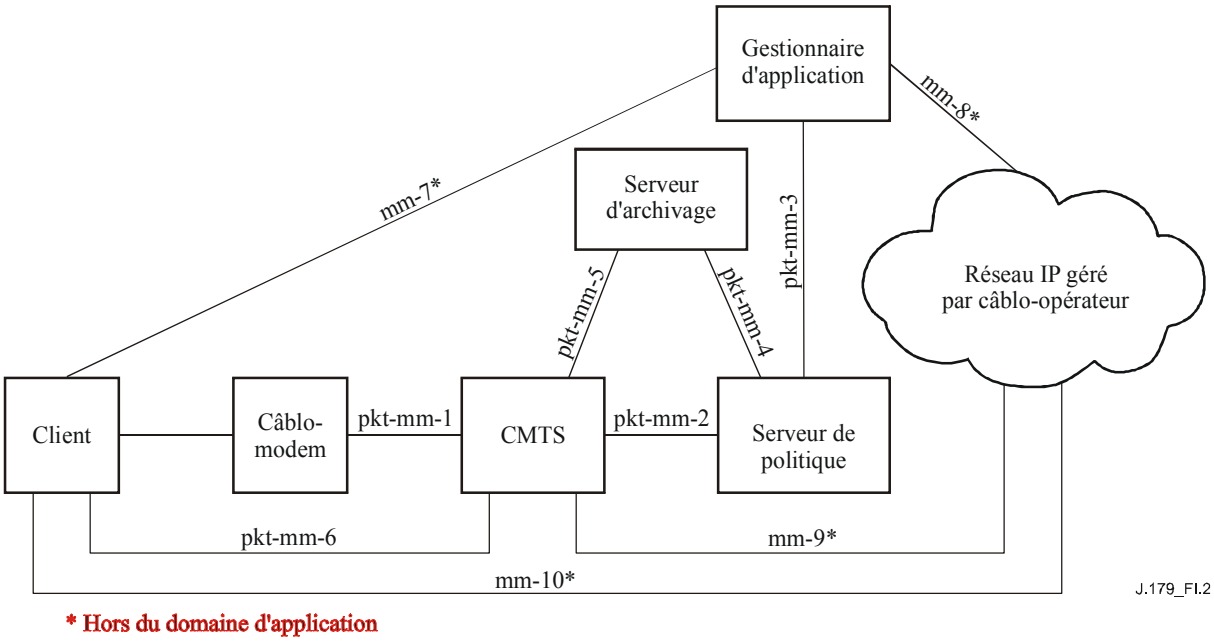

Figure I.2/J.179 – Cadre architectural d'IPCablecom multimédia

Dans cette architecture, les clients peuvent prendre en charge ou non le cadre IPCablecom multimédia. Les clients qui prennent en charge le cadre et ses mécanismes de signalisation produisent de façon explicite des demandes en leur nom propre, qui sont autorisées à l'extrémité de tête par le Serveur de politique. Les clients qui ne prennent pas en charge les mécanismes de signalisation de qualité de service voient leurs demandes de ressources réseau portées par un gestionnaire d'application qui agit en leur nom comme mandataire, et avec lequel ils interagissent.

Indépendamment de la méthode de signalisation de la qualité de service, les demandes de ressources de réseau d'accès sont toujours soumises à un contrôle de politique, qui est mis en application au système de terminaison de câblo-modem (CMTS) qui sert de Point de mise en

application de politique (PEP, *policy enforcement point*) et défini au Serveur de politique (PS), qui sert de point de décision de politique (PDP, *policy decision point*).

- Les décisions de politique peuvent être tirées du Serveur de politique par le CMTS. Dans ce cas, le CMTS produit normalement une demande de politique en résultat d'une demande de ressources de qualité de service déjà conforme mais pas encore autorisée. Sur la base de la décision qui en résulte, la demande de qualité de service d'origine est servie ou rejetée.
- Autrement, les décisions de politiques peuvent être poussées dans le système CMTS par le Serveur de politique. Dans ce cas, le Serveur de politique doit installer une décision de politique avant une demande de ressources de qualité de service fondée sur une demande de politique provenant d'un gestionnaire d'application. Un gestionnaire d'application génère une telle demande, fondée sur l'interaction avec le client (au moyen de mécanismes de signalisation non spécifiés).

Le Serveur de politique et le CMTS génèrent des messages d'événement pour suivre la trace des demandes et des utilisations de qualité de service. Ces messages d'événement sont envoyés à un Serveur d'archivage (RKS, *record keeping server*) où ils peuvent être utilisés pour les besoins de la facturation et la comptabilité.

Le Tableau I.1 résume les interfaces présentées à la Figure I.2. Les interfaces qui sont définies dans la présente Recommandation sont marquées "pkt-mm-x", tandis que les autres interfaces, qui figurent dans un souci d'exhaustivité, sont marquées "mm-x".

Tableau I.1/J.179 – Interfaces IPCablecom multimédia

Interface	Description	Notes
pkt-mm-1	CMTS – CM	Le câblo-modem peut demander la qualité de service au CMTS via la signalisation DSx de câblo-modem. Autrement, le CMTS peut ordonner au câblo-modem (CM) d'établir, supprimer ou changer un flux de service de câblo-modem pour satisfaire une demande de QS, toujours via la signalisation DSx.
pkt-mm-2	PS – CMTS	Cette interface est fondamentale pour le cadre de gestion de politique. Elle contrôle les décisions de politique qui peuvent être: a) poussées par le Serveur de politique (PS) jusqu'au CMTS; b) tirées du PS par le CMTS. L'interface permet aussi des demandes de QS mandatées au nom d'un client. Dans certains scénarios, cette interface peut aussi être utilisée pour informer le PS lorsque des ressources de QS sont devenues inactives.
pkt-mm-3	AM – PS	Le gestionnaire d'application (AM) peut demander que le PS installe une décision de politique au CMTS. De plus, l'AM peut aussi demander que le PS soit mandataire des demandes de QS au CMTS au nom du client. Cette interface peut aussi être utilisée pour informer l'AM des changements d'état des ressources de qualité de service.
pkt-mm-4	PS – RKS	Le PS envoie des messages d'événement au RKS pour garder trace de décisions de politique qui se rapportent à la qualité de service.
pkt-mm-5	CMTS – RKS	Le CMTS envoie au RKS les messages d'événement pour garder la trace des demandes de QS et de leur utilisation (par exemple, ajouts, changements, suppressions de flux de service et mesures de volume).
pkt-mm-6	Client – CMTS	Le client peut utiliser cette interface pour demander et gérer directement les ressources réseau de QS. Si elles sont autorisées, ces ressources sont fournies par le CMTS. Cette interface est hors du champ de la présente Recommandation.

Tableau I.1/J.179 – Interfaces IPCablecom multimédia

Interface	Description	Notes
mm-7	Client – AM	Cette interface peut être utilisée par le client pour interagir avec l'AM et pour demander et gérer indirectement des ressources de QS. Cette interface est hors du champ de la présente Recommandation.
mm-8	AM – Homologue	L'AM peut utiliser cette interface pour interagir avec une autre entité faisant partie de l'application en question. Cette interface est hors du champ de la présente Recommandation.
mm-9	CMTS – Réseau IP géré par l'opérateur	Cette interface sur le CMTS peut être utilisée pour la prise en charge de demandes de QS de bout en bout au delà du réseau d'accès. Cette interface est hors du champ de la présente Recommandation.
mm-10	Client – Homologue	Le Client peut utiliser cette interface pour interagir avec d'autres entités qui font partie de l'application en question. Cette interface est hors du champ de la présente Recommandation.

I.3.2 Composants multimédia

Le présent paragraphe développe la discussion précédente au sujet du cadre architectural en fournissant des précisions supplémentaires sur chacun des éléments de réseau.

I.3.2.1 Client

Un client multimédia est une entité logique qui peut envoyer ou recevoir des données. IPCablecom multimédia définit trois différents types de client, qui diffèrent dans la façon de signaler la qualité de service et la façon d'installer les décisions de politique associées à la qualité de service dans le CMTS.

Le Client de type 1 représente les points d'extrémité ordinaires existants (par exemple, applications de micro-ordinateur, consoles de jeu) qui n'ont pas de prédispositions pour la QS ou de capacités de signalisation. Ce client ignore tout des câblo-modems, d'IPCable2Home, ou des échanges de message IPCablecom, et donc aucune exigence s'y rapportant ne peut en être attendue. De tels clients peuvent aller du simple appareil de présentation audiovisuel analogique à des périphériques en réseau et dispositifs électroniques complexes comme des décodeurs ou des consoles de jeu. Le client communique avec un gestionnaire d'application pour demander le service, et il ne demande pas directement les ressources de qualité de service à l'opérateur du réseau d'accès.

Le Client de type 2 est similaire à un adaptateur MTA de téléphonie d'IPCablecom-T en ce qu'il prend en charge la signalisation de qualité de service sur la base de la DQOS d'IPCablecom. Ce client est averti de la QS d'IPCablecom multimédia, et il communique avec un gestionnaire d'application pour demander le service et obtenir un jeton pour les ressources de réseau d'accès. Le client présente alors ce jeton lorsqu'il demande des ressources de qualité de service au réseau d'accès (pkt-mm-1, pkt-mm-6).

Le Client de type 3 demande de la QS sur la base de RSVP sans interaction avec un gestionnaire d'application. Ce client est averti du protocole RSVP fondé sur les normes de l'IETF et utilise ce protocole pour demander des ressources de qualité de service du réseau d'accès directement au CMTS.

I.3.2.2 Serveur de politique

Le cadre de la gestion de politique pour l'initiative IPCablecom multimédia se fonde sur les travaux du groupe de travail Protocole d'allocation de ressources (RAP, *resource allocation protocole*) de l'IETF. Comme défini et décrit dans le document RFC 2753, l'élément de réseau Serveur de politique (PS) implémente les procédures d'autorisation et de gestion de ressources définies par

l'opérateur. En plus des paramètres de ressource demandés et de l'état des ressources disponibles, les décisions de politique peuvent impliquer les informations d'identité du client et le profil associé, les paramètres d'application, des considérations de sécurité, la date et l'heure, etc. Aussi, certains opérateurs peuvent choisir d'installer plusieurs Serveurs de politique et de déléguer certaines décisions de politique parmi ces serveurs afin de satisfaire aux exigences d'échelonnement et de tolérance aux fautes.

Les principales fonctions du Serveur de politique comportent:

- un mécanisme de demande de décision de politique, invoqué par les gestionnaires d'application (pkt-mm-3, modèle poussé) ou les CMTS (pkt-mm-2, modèle tiré);
- un mécanisme de fourniture de décision de politique, utilisé pour installer les décisions de politique sur le CMTS (pkt-mm-2);
- un mécanisme permettant de mandater le CMTS pour émettre les messages de gestion de la qualité de service au nom du gestionnaire d'application (pour les clients qui n'ont pas de capacités de signalisation de QS par eux-même);
- une interface d'enregistrement des événements sur un serveur d'archivage (pkt-mm-4) utilisé pour enregistrer les demandes de politique, qui peut aussi être corrélée avec les enregistrements d'utilisation des ressources réseau.

Le Serveur de politique peut prendre en charge deux modèles différents d'installation des décisions de politique sur le CMTS:

- le Serveur de politique peut installer (pousser) une décision de politique sur le CMTS avant que n'arrive une demande de réservation de QS au CMTS;
- le CMTS peut demander (tirer) une décision de politique du Serveur de politique lorqu'une demande de réservation de QS arrive au CMTS.

Les règles de politique peuvent contenir les informations suivantes:

- Règles définissant les ressources autorisées par le Serveur de politique:
  - par service;
  - par abonné;
  - bande passante (spécifiée en utilisant le paramètre de seau de jeton);
  - garanties de temps de latence;
  - politique d'expiration des délais;
  - politique de limites de volume.
- Règles définissant la rareté/valeur de la bande passante selon l'heure de la journée.
- Règles de préemption.

Au minimum, dans le scénario "poussé", le Serveur de politique DOIT effectuer les fonctions suivantes:

- authentifier et vérifier les messages de politique provenant des gestionnaires d'application;
- traiter les messages de politique sur la base des règles définies par l'opérateur;
- traduire l'identité correcte du CMTS auquel la politique doit être fournie;
- communiquer les décisions de politique et autres messages en toute sécurité avec le CMTS;
- envoyer les messages d'événement retraçant ces demandes au serveur d'archivage.

Au minimum, dans le scénario "poussé" le Serveur de politique DOIT effectuer les fonctions suivantes:

- si un Gestionnaire d'application est impliqué dans le service, authentifier et vérifier les messages de politique provenant du gestionnaire d'application;

- communiquer les décisions de politique et autres messages en toute sécurité avec le CMTS;
- traiter les messages de politique sur la base des règles définies par l'opérateur;
- envoyer les messages d'événement retraçant ces demandes au serveur d'archivage.

Le Serveur de politique peut effectuer les fonctions supplémentaires suivantes:

- retracer l'utilisation des ressources sur la base des informations d'état entretenues en interne (par exemple, temporisateurs);
- retracer les ressources autorisées sur la base de l'utilisateur, du service ou une agrégation des deux.

I.3.2.3 Système de terminaison de câblo-modem

IPCablecom multimédia fournit l'accès à l'ensemble des algorithmes de programmation amont du CMTS comme défini dans les Recommandations des câblo-modems. Plus précisément, l'architecture définit un "Profil de trafic" IPCablecom multimédia qui donne une couche d'abstraction à partir des types de programmation associés des câblo-modems (UGS, UGS/AD, etc.). De plus, les dispositifs spécifiques de la téléphonie et les hypothèses qu'on trouve dans les spécifications IPCablecom-T ont été généralisées pour fournir une infrastructure de qualité de service qui peut être utilisée par de multiples types de clients et d'applications.

Le CMTS prend en charge les deux modèles de réservation en une et deux phases pour la gestion des ressources de réseau d'accès. Dans le modèle à deux phases, les ressources du réseau d'accès sont réservées au départ, puis engagées pour être utilisées ultérieurement en tant que de besoin. Le CMTS prend aussi en charge un modèle de réservation en une seule phase dans lequel les ressources du réseau d'accès sont simultanément réservées et engagées pour une utilisation immédiate.

Le CMTS établit le ou les flux de service pertinents sur le réseau d'accès par câblo-modem via l'interface pkt-mm-1. Le CMTS envoie des messages d'événement pour les réservations de ressources de qualité de service et leur utilisation à un Serveur d'archivage via un identifiant d'interface pkt-mm-5. Finalement, le CMTS surveille les flux de service fondés sur la qualité de service et les comptabilise comme défini dans le sous-système (facultatif) de Gestion de comptabilité dans les Recommandations des câblo-modems.

I.3.2.4 Gestionnaire d'application

Le gestionnaire d'application joue un rôle de coordination impliquant la signalisation et la sémantique d'application ainsi que l'interaction avec le cadre de politique d'IPCablecom, comme évoqué dans l'exposé précédant sur l'élément Serveur de politique. Noter qu'un gestionnaire d'application peut être co-hébergé avec un Serveur de média ou bien, dans un modèle divisé, que les deux éléments peuvent exister séparément.

Le gestionnaire d'application s'interface avec un client via mm-7. Sur la base de sa connaissance des offres de service particulières, le gestionnaire d'application DOIT déduire ou définir les paramètres particuliers de qualité de service nécessaires pour la fourniture du service au client de type 1. Une fois que ces informations ont été confirmées, le gestionnaire d'application envoie une demande de politique au Serveur de politique via l'interface pkt-mm-3. Si nécessaire, le gestionnaire d'application peut utiliser l'interface mm-8 pour se synchroniser avec un Serveur de média.

Le Client de type 2 interagit aussi avec le gestionnaire d'application et communique les informations de demande de service via l'interface mm-7. A nouveau, le gestionnaire d'application DOIT déduire les paramètres de qualité de service nécessaires à la fourniture du service au Client de type 2. Le gestionnaire d'application envoie une demande de politique au Serveur de politique via l'interface pkt-mm-3. Lorsque l'autorisation a été accordée, le gestionnaire d'application reçoit un jeton du Serveur de politique et envoie le jeton au Client via l'interface mm-7. Si nécessaire, le

gestionnaire d'application peut utiliser l'interface mm-8 pour se synchroniser avec un Serveur de média.

Le Client de type 3 n'a pas besoin d'un gestionnaire d'application, bien que la présence d'un Serveur d'application dans les scénarios de fourniture de service sophistiqués soit assez vraisemblable.

I.3.2.5 Serveur d'archivage

Le Serveur d'archivage (RKS) reçoit des messages d'événement indiquant l'utilisation des ressources de qualité de service du réseau d'accès. Le RKS s'interface avec le Serveur de politique (pkt-mm-4) et le CMTS (pkt-mm-5). Le RKS ne reçoit pas directement les informations spécifiques de l'application du gestionnaire d'application. Au lieu de cela, les informations spécifiques de l'application peuvent être incluses dans un message d'événement comme données opaques envoyées du gestionnaire d'application au Serveur de politique et incorporées dans le message d'événement de demande de politique envoyé au Serveur d'archivage.

I.4 Qualité de service mandatée avec politique poussée (Scénario 1)

Comme on l'a noté auparavant, trois scénarios architecturaux ont été identifiés pour la prise en charge des trois types de client. Le modèle d'autorisation "QS mandatée avec politique poussée" (Scénario 1) prend en charge le Client de type 1, qui ne prend pas en charge lui-même les mécanismes de signalisation de qualité de service. La Figure I.3 donne un aperçu général de haut niveau de l'interaction des éléments impliqués dans ce scénario.

Le Client demande un service spécifique de l'application en envoyant une "Demande de service" au gestionnaire d'application. A réception de cette demande, le gestionnaire d'application détermine les besoins de qualité de service du service demandé et envoie une "Demande de politique" au Serveur de politique. A son tour, le Serveur de politique valide la "Demande de politique" à l'égard des règles de politique définies par l'opérateur, et si la décision est affirmative, envoie un message "Etablir politique" au CMTS. Le CMTS effectue le contrôle d'admission sur l'enveloppe de qualité de service demandée (en vérifiant que les ressources adéquates sont disponibles pour satisfaire cette demande), installe la décision de politique, et (finalement) établit le ou les flux de service avec les niveaux de qualité de service demandés.

Il devrait être noté que la gestion réelle du ou des flux de service (c'est-à-dire, les demandes d'ajout, de changement, et de suppression) peuvent être étroitement contrôlées et surveillées par le gestionnaire d'application au moyen d'extensions aux mécanismes de signalisation de base retracés ici pour l'installation de la décision de politique. Dans le scénario 1, il n'y a pas de communication directe entre le client et le CMTS.

Noter que l'interface entre le client et le gestionnaire d'application, y compris les détails de la "Demande de service," est en dehors du domaine de la présente Recommandation. Il est possible que le client ignore tout de la qualité de service et demande simplement un service (par exemple, l'utilisateur veut jouer un jeu à plusieurs joueurs avec un ami) du gestionnaire d'application dans le message "Demande de service". Il est aussi possible que le client soit pleinement informé de ses exigences de qualité de service (par exemple, l'utilisateur demande un service à 128 kbit/s garantis pour son VPN professionnel, sécurisé par IPSec) et communique ces informations supplémentaires dans la "Demande de service". Le mécanisme par lequel le gestionnaire d'application détermine les exigences de qualité de service pour le service demandé sont en dehors du domaine d'application de cette architecture.

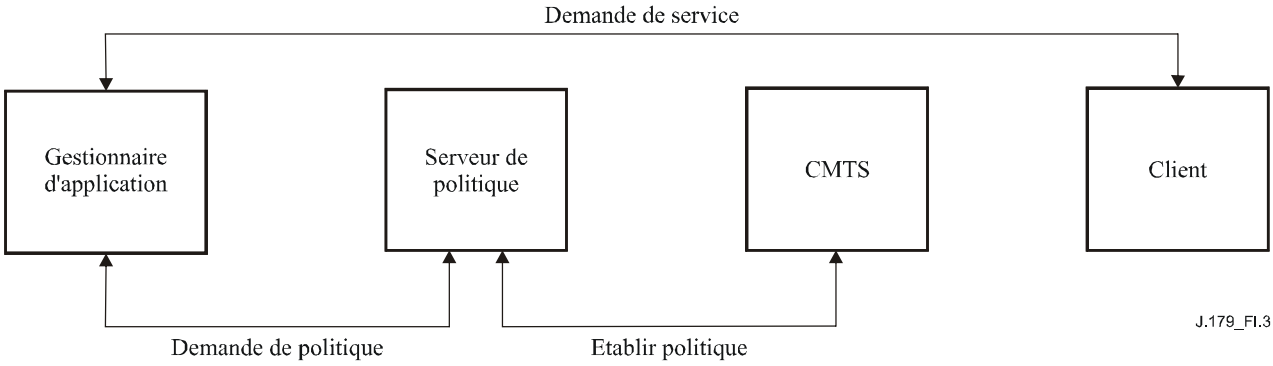

Figure I.3/J.179 – Cadre d'autorisation pour le scénario 1

Dans le scénario 1, le CMTS prend en charge un modèle de réservation de ressources en un seule phase, comme indiqué ci-dessous à la Figure I.4, pour permettre une activation et une utilisation immédiate des ressources du réseau d'accès par le client. (Un modèle de réservation en deux phases est aussi pris en charge dans ce scénario comme indiqué plus loin dans le présent paragraphe.)

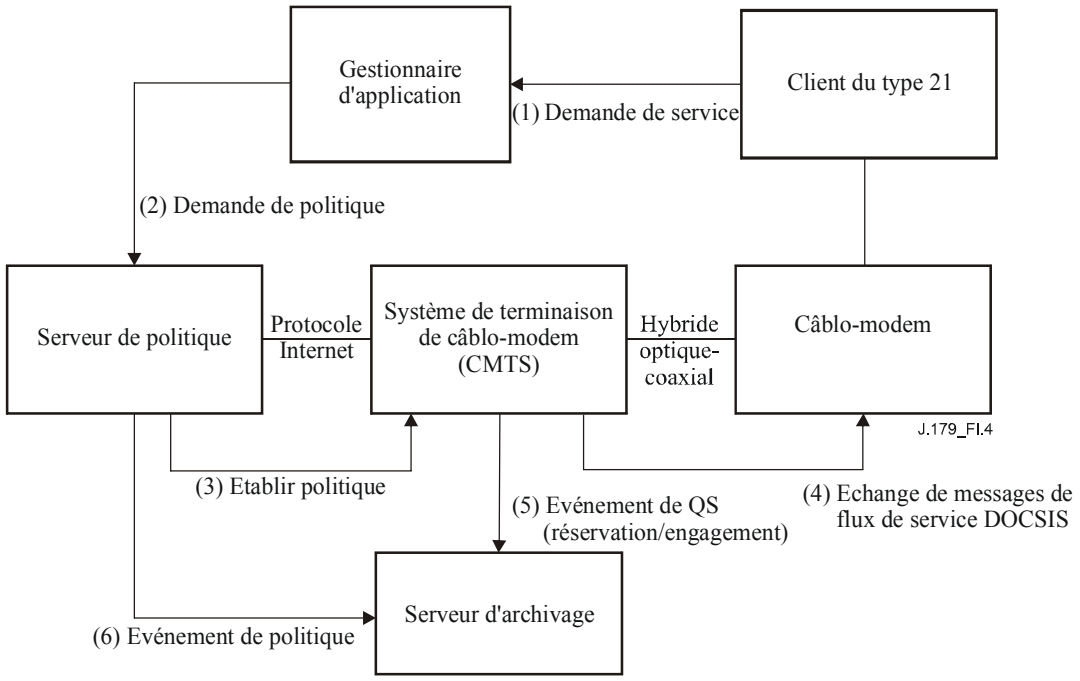

Figure I.4/J.179 – Modèle de réservation de ressources en un seule phase pour le scénario 1

Sur la base de cette séquence d'échange de message en une seule phase, le Tableau I.2 résume à haut niveau chacun de ces messages. Les détails spécifiques des messages et objets du protocole ont été renvoyés aux spécifications respectives d'IPCablecom multimédia.

Tableau I.2/J.179 – Détails des messages de réservation de ressources en une seule phase pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(1) Demande de service	Le client demande le service au gestionnaire d'application	<aucun>	Hors du domaine d'IPCablecom multimédia	Ce protocole devrait prendre en charge l'authentification du client et du gestionnaire d'application. Le protocole devrait aussi fournir des informations suffisantes pour que le gestionnaire d'application transmette les besoins de QS du service demandé.
(2) Demande de politique	L'AM demande l'établissement de la QS au nom de son client	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque.	Commande de porte (COPS)	Le Serveur de politique utilise les règles de politique gérées par l'opérateur pour permettre ou refuser la demande
(3) Etablir politique	Le Serveur de politique envoie un message au CMTS, installe sa décision de politique et demande l'établissement du flux de service.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS).	Commande de porte (COPS)	Dans le modèle à phase unique, cette demande est pour l'autorisation, la réservation et l'engagement des ressources de qualité de service.
(4) Echange de messages de câblo-modem	Le CMTS établit les flux de service de QS améliorée	Paramètres Type de programmation de câblo-modem, Bande passante et Temps de latence, Classeur de trafic.	Echange de messages DSx de câblo-modem	Les fonctions de QS sont fondées ici sur les mécanismes définis dans la spécification de l'interface RFI de câblo-modem
(5) Evénement de QS	Le CMTS génère le message d'événement approprié, indiquant l'utilisation de QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation de service, Heure du jour.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation

Tableau I.2/J.179 – Détails des messages de réservation de ressources en une seule phase pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(6) Evénement de politique	Le Serveur de politique génère le message d'événement approprié, indiquant la Demande de politique et l'action effectuée	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation

Les informations résumées dans la colonne Champs du Tableau I.2 sont destinées à donner un exemple du type d'informations portées par chaque message. Pour les détails de chaque message du protocole, se reporter aux documents de spécification appropriés.

Le scénario 1 prend aussi en charge un modèle de réservation de ressources à deux phases, comme indiqué ci-dessous à la Figure I.5. Ici, le gestionnaire d'application demande d'abord que les ressources de QS de réseau d'accès soient autorisées et réservées. Une fois que ces ressources ont été réservées, le gestionnaire d'application peut continuer son dialogue avec le client au sujet du service. En tant que de besoin, le gestionnaire d'application demande l'engagement des ressources de qualité de service. Ce modèle de réservation/engagement en deux phases garantit que les ressources de réseau d'accès sont disponibles avant d'offrir le service au client.

Noter que les accusés de réception de chacun des messages indiqués ne sont pas explicitement inclus, mais sont implicites. Chaque message d'accusé de réception ne peut être envoyé qu'une fois que le résultat final de la demande correspondante est connu. Ceci est particulièrement important dans le séquencement des accusés de réception des messages 4 (Réservation DOCSIS), 3 (Politique établie), et 2 (Demande de politique) dans la mesure où le gestionnaire d'application va vraisemblablement attendre la confirmation du succès de la phase de réservation avant de continuer son dialogue avec le client et d'engager finalement les ressources.

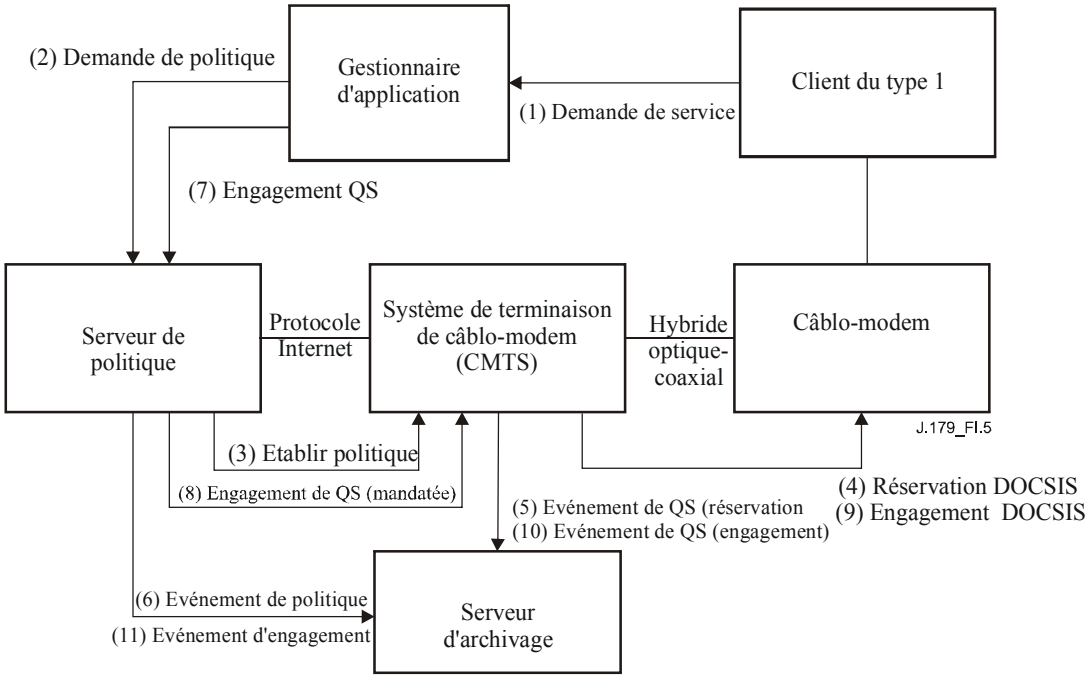

Figure I.5/J.179 – Modèle de réservation de ressources en deux phases pour le scénario 1

Le Tableau I.3 ci-dessous donne un résumé des messages de la Figure I.5. Noter que les messages (7 à 10) ont été ajoutés pour prendre en charge la phase de signalisation de l'engagement.

Tableau I.3/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(1) Demande de service	Le client demande le service au gestionnaire d'application	<aucun>	Hors du domaine d'IPCablecom multimédia	Ces protocole devrait prendre en charge l'authentification du client et du gestionnaire d'application. Le protocole devrait aussi fournir des informations suffisantes pour que le gestionnaire d'application transmette les besoins de QS pour le service demandé.
(2) Demande de politique	Le gestionnaire d'application demande l'établissement de la QS au nom du client	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque.	Commande de porte (COPS)	Le Serveur de politique utilise les règles de politique gérées par l'opérateur pour accorder ou refuser la demande

Tableau I.3/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(3) Politique établie	Le Serveur de politique envoie un message au CMTS, installe sa décision de politique et demande la réservation du flux de service.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS).	Commande de porte (COPS)	Dans le modèle à deux phases, cette demande est pour l'autorisation et la réservation des ressources de QS.
(4) Réservation DOCSIS	Le CMTS établit les flux de service de QS améliorée et les place dans l'état "admis".	Paramètres Type de programmation câblo-modem, Bande passante et Temps de latence, Classeur de trafic.	Echange de messages DSx de câblo-modem	Ici, les fonctions de QS se fondent sur les mécanismes définis dans la spécification RFI de câblo-modem. Les ressources réservées restent inactives et peuvent être utilisées par du trafic au mieux sur d'autres flux jusqu'à leur engagement.
(5) Evénement de QS	Le CMTS génère le message d'événement approprié, indiquant la réservation de QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation de service, Heure du jour.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation

Tableau I.3/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(6) Evénement de politique	Le CMTS génère le message d'événement approprié, indiquant la Demande de politique et l'action effectuée.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation
(7) Engagement de QS	L'AM signale d'engager les ressources de QS	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Identifiant de politique.	Commande de porte (COPS)	L'engagement de l'AM peut dépendre des échanges de messages ultérieurs avec le client
(8) Engagement de QS (mandatée)	Le Serveur de politique reçoit la demande de l'AM et la mandate au CMTS	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Identifiant de politique.	Commande de porte (COPS)	Même si le PS peut appliquer les règles de politique durant la phase d'engagement, on suppose généralement que la bande passante réservée peut être engagée à tout moment par l'AM.
(9) Engagement DOCSIS	Le CMTS met le flux de service dans l'état "actif"	Paramètres Type de programmation de câblo-modem, Bande passante et Temps de latence, Classeur de trafic, ID de flux de service.	Echange de messages DSx de câblo-modem	Les fonctions de QS sont ici fondées sur les mécanismes définis dans la spécification RFI de câblo-modem

Tableau I.3/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 1

Message	Fonction	Champs	Protocole candidat	Commentaires
(10) Evénement de QS (Engagement)	Le CMTS génère le message d'événement approprié, indiquant l'utilisation de la QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation de service, Heure du jour.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation
(11) Evénement d'engagement	Le CMTS génère le message d'événement approprié, indiquant l'engagement de la QS et l'action effectuée	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Identifiant de politique.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir une matière suffisante pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou de la réconciliation

Une fois que les ressources de qualité de service ont été autorisées, réservées et engagées avec succès sur le réseau d'accès, l'activité de ces ressources est surveillée au CMTS. En général, un modèle à états souples est utilisé, dans lequel des messages de rafraîchissement périodiques sont nécessaires durant les périodes d'inactivité sur les flux de service réservés et engagés. Si les temporisateurs d'activité arrivent à expiration sans un rafraîchissement, les ressources associées peuvent être récupérées par le CMTS. Ceci améliore la faculté de résistance du réseau en cas de défaillance d'un point d'extrémité.

Une séquence de récupération de ressources plus normale est également fournie dans ce scénario, dans laquelle le gestionnaire d'application signale au Serveur de politique le moment où se termine la session de service. Le Serveur de politique répond en générant un message d'événement, qui est envoyé au serveur RKS, et en ordonnant au CMTS de détruire le ou les flux de service associés et de récupérer les ressources associées. Sans considérer si l'arrivée à expiration du flux de service est due à l'inactivité ou s'il est explicitement supprimé, un chemin d'audit solide est entretenu, qui garde la trace de l'utilisation réelle des ressources via les messages d'événement produit au CMTS et envoyés au RKS.

I.4.1 Exemple: bande passante à la demande fondée sur le Web

Un exemple de la façon dont les mécanismes du scénario 1 peuvent être appliqués dans un contexte de livraison de service est le cas d'un site Web sécurisé hébergé par un opérateur, ce qui devrait permettre aux abonnés de demander des réservations de bande passante à la demande.

Supposons par exemple, que le service normal d'un abonné soit limité en débit à 128 kbit/s en aval et 128 kbit/s en amont. Alors que ce niveau de service peut être adéquat pour la plupart des utilisations, il peut y avoir des cas où l'application de cet abonné réclame plus de bande passante ou a des besoins de qualité de service différents. Si l'utilisateur décide d'utiliser le service de bande passante à la demande pour effectuer des modifications temporaires à son niveau de service normal, il aura simplement à se connecter au site Web de l'opérateur (le gestionnaire d'application) pour demander un relèvement temporaire de son niveau de service.

Une motivation possible d'une telle demande pourrait être le désir de charger des fichiers de média à haut débit d'un fournisseur de contenu. Dans ce cas, l'abonné peut demander explicitement un service à débit réservé minimal de 512 kbit/s dans le sens aval pour les trois heures à venir. Autrement, le besoin exact de qualité de service de l'application peut être opaque pour l'abonné, qui pourrait simplement demander un clip vidéo donné de trois heures (qui, à l'insu de l'abonné, se trouve être codé à 512 kbit/s). Dans l'un ou l'autre cas, cet échange représente la "Demande de service" de l'abonné au gestionnaire d'application.

Dans l'un ou l'autre cas, le gestionnaire d'application présentera une "Demande de politique" pour un service au débit réservé de 512 kbit/s minimal pour trois heures au Serveur de politique au nom de l'abonné. Le Serveur de politique appliquera alors ses propres critères d'autorisation, et, si la demande est approuvée, demandera au CMTS (au moyen d'une commande "Etablir politique") de fournir la bande passante à l'abonné. A son tour, le CMTS effectuera le contrôle d'admission interne et établira la qualité de service en utilisant l'échange de messages de câblo-modem, gardant la trace de ce processus au moyen d'un message d'événement de QS.

I.4.2 Exemple: jeu en ligne via des consoles en réseau

Autrement, considérons le cas où deux consoles de jeu souhaitent s'engager ensemble via un réseau tunnel. Dans cet exemple, deux utilisateurs ne peuvent normalement mettre leurs consoles en réseau que s'ils sont co-localisés. Cependant un logiciel spécial installé sur le micro-ordinateur de chaque utilisateur, co-localisé sur un réseau local et servant de mandataire pour la console distante, permet la constitution en réseau de telle sorte que deux consoles de jeu n'ont plus besoin d'être co-localisées. Le seul problème avec cette nouvelle approche est que le tunnel résultant requiert une qualité de service suffisante pour que les consoles de jeu puissent être utilisées comme si elles étaient co-localisées sur un même réseau à haut débit.

Dans ce scénario, le ou les utilisateurs se connecteraient au gestionnaire d'application via le ou les micro-ordinateurs qui tunnellent leurs paquets. Au moyen d'un échange de messages spécifique de l'application, ils s'authentifient eux-même et indiquent leur demande de jouer l'un avec l'autre. Le gestionnaire d'application accepte la demande, et génère la ou les "Demandes de politique" au nom du ou des utilisateurs. Le Serveur de politique prend sa décision et relaie le message comme commande "Etablir politique" au CMTS. Le CMTS effectue le contrôle d'admission et active la qualité de service de réseau d'accès entre les micro-ordinateurs pour le tunnel de jeu utilisant l'échange de messages de câblo-modem. A partir de ce point, les consoles de jeu peuvent échanger des paquets sans savoir qu'elles ne sont pas co-localisées. Noter que l'échange de messages d'événement a été omis dans cet exemple, par souci de simplicité.

Dans cet exemple hypothétique, si les utilisateurs résident sur des nœuds HFC séparés, il est de la responsabilité de l'opérateur de s'assurer que la qualité de service de cœur de réseau vers et à partir du CMTS est traitée correctement et au niveau requis par sa politique et les accords de service. La Figure I.6 donne une illustration graphique de cet exemple pour le cas simplifié dans lequel les deux utilisateurs sont desservis par un seul CMTS.

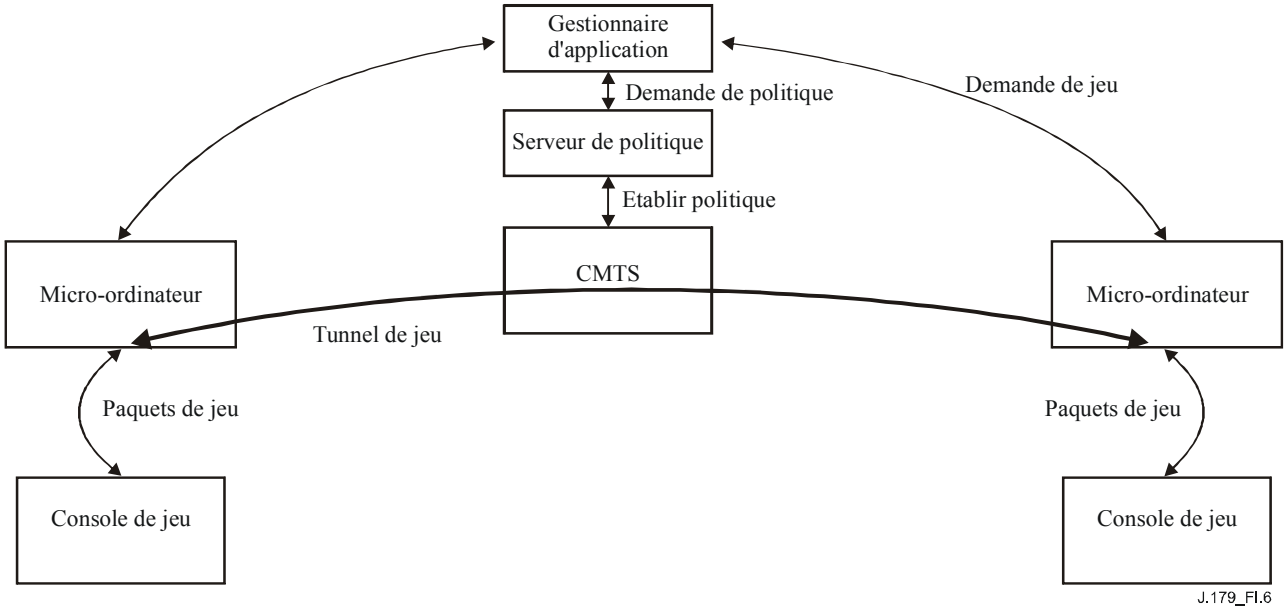

Figure I.6/J.179 – Consoles de jeu en réseau via un tunnel IP à QS améliorée

I.5 QS demandée par le client avec politique poussée (scénario 2)

Le modèle du scénario 2 "QS demandée par le client avec politique poussée" prend en charge le Client de type 2, qui est capable de signaler et gérer ses propres ressources de QS mais a besoin d'une autorisation préalable de ces demandes via un gestionnaire d'application. Dans ce scénario, le modèle d'autorisation de politique et de réservation de qualité de service ressemble étroitement au modèle de la téléphonie IPCablecom-T défini dans la spécification de la qualité de service dynamique. Le Serveur de politique pousse la politique au CMTS d'une manière similaire à celle dont le Contrôleur de porte envoie la politique au CMTS via COPS. Le Client de type 2 utilise l'échange de messagerie DSx de câblo-modem ou RSVP+ similaire au dispositif d'adaptateur MTA dans IPCablecom-T.

La Figure I.7 donne un aperçu général de haut niveau du scénario 2. Noter les ressemblances avec le cadre d'autorisation indiqué pour le scénario 1. Ici encore, le client demande un service spécifique de l'application en envoyant une "Demande de service" au gestionnaire d'application. Le gestionnaire d'application détermine alors les besoins de qualité de service du service demandé et envoie une "Demande de politique" au Serveur de politique. La "Demande de politique" contient

"l'enveloppe autorisée" ou QS maximale permise pour le client. Le Serveur de politique valide à son tour la "Demande de politique" à l'égard des règles de politique définies par l 'opérateur et, si la décision est affirmative, envoie un "Etablir politique" au CMTS. Le CMTS effectue le contrôle d'admission de la QS demandée et installe l'autorisation de politique. Comme dans le scénario 1, les messages d'événement sont générés par le Serveur de politique et le CMTS et envoyés au RKS. Le Serveur de politique enregistre un événement chaque fois qu'il prend une décision ou met à jour son état, et le CMTS garde trace de la maintenance et de l'utilisation des ressources de QS.

Dans le scénario 2 et à la différence du scénario 1, il y a une communication directe entre le Client et le CMTS pour ajouter, modifier et supprimer les réservations de ressources. Après que le CMTS ait reçu le message "Etablir politique" du Serveur de politique, le client peut demander directement la qualité de service au CMTS en utilisant les mécanismes de signalisation de QS précédemment notés. Le client peut aussi changer dynamiquement la QS tant que la QS demandée est comprise dans "l'enveloppe autorisée" approuvée par le Serveur de politique. L'avantage de cette méthode est que le gestionnaire d'application n'a pas à négocier l'utilisation de la bande passante du client, ce qui est un facteur très utile lorsqu'il y a un changement dynamique des besoins de QS du client.

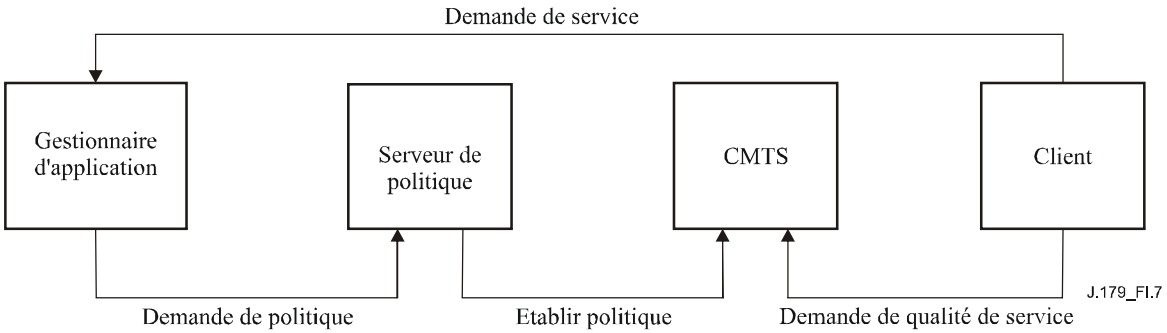

Figure I.7/J.179 – Cadre d'autorisation pour le scénario 2

Comme dans le scénario précédent, le scénario 2 (comme indiqué à la Figure I.8) prend en charge un modèle de réservation de ressources en une seule phase pour permettre l'activation et l'utilisation immédiate des ressources du réseau d'accès par le client.

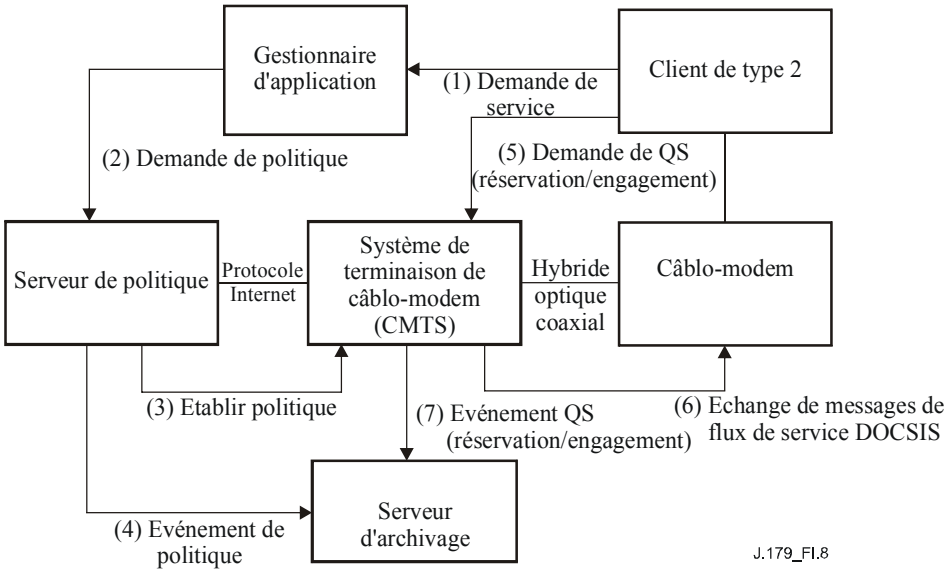

Figure I.8/J.179 – Modèle de réservation de ressources en une seule phase pour le scénario 2

Sur la base de cette séquence d'échange de messages en une seule phase, le Tableau I.4 donne un résumé de haut niveau de chacun de ces messages.

Tableau I.4/J.179 – Détails des messages de réservation de ressources en une seule phase pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(1) Demande de service	Le client demande le service au gestionnaire d'application	<aucun>	Hors du domaine d'IPCablecom multimédia	Ce protocole devrait prendre en charge l'authentification du client et du gestionnaire d'application. Le protocole devrait aussi fournir des informations suffisantes pour que le gestionnaire d'application convoie les besoins de QS du service demandé.
(2) Demande de politique	Le gestionnaire d'application demande l'autorisation de QS au nom du client.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque.	Commande de porte (COPS)	Le Serveur de politique utilise les règles de politique gérées par l'opérateur pour accorder ou refuser la demande
(3) Etablir politique	Le Serveur de politique envoie un message au CMTS, installant sa décision de politique	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS).	Commande de porte (COPS)	Dans ce scénario, cette demande est seulement pour autorisation.

Tableau I.4/J.179 – Détails des messages de réservation de ressources en une seule phase pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(4) Evénement de politique	Le Serveur de politique génère le message d'événement approprié, indiquant la Demande de politique et l'action effectuée.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir suffisamment de matière pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou la réconciliation
(5) Demande de QS (Réservation/ Engagement)	Le client demande que les ressources de QS soient réservées et immédiatement engagées pour utilisation	Paramètres de bande passante et Temps de latence, Classeur de trafic.	DSx câblo-modem ou RSVP+	Le client peut établir directement les flux de service de câblo-modem via l'échange de messages DSx ou peut produire des messages RSVP+ pour établir ces flux
(6) Echange de message DOCSIS	Le CMTS établit les flux de service de QS améliorée et les place dans l'état "actif"	Paramètres Type de programmation de câblo-modem et Temps de latence, Classeur de trafic.	Echange de messages DSx câblo-modem	Cette étape n'est nécessaire que si la signalisation RSVP+ a été fournie au CMTS dans le message précédent, autrement, les flux de service ont déjà été établis et activés via l'échange de messages DSx de câblo-modem. Les fonctions de QS sont ici fondées sur les mécanismes définis dans les Recommandations de câblo-modem.

Tableau I.4/J.179 – Détails des messages de réservation de ressources en une seule phase pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(7) Evénement de QS	Le CMTS génère le message d'événement approprié, indiquant l'utilisation de la QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation du service, Heure du jour.	Echange de message d'événement (RADIUS)	Ce message devrait contenir suffisamment de matière pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou la réconciliation

Le CMTS prend aussi en charge un modèle de réservation de ressources en deux phases, comme indiqué à la Figure I.9. Dans ce modèle, le client demande d'abord la réservation de ressources de qualité de service du réseau d'accès. Une fois que ces ressources ont été réservées, le client signale alors que des ressources de QS devrait être engagées. Le modèle réservation /engagement en deux phases garantit que ces ressources de réseau d'accès sont disponibles avant d'offrir les services au client.

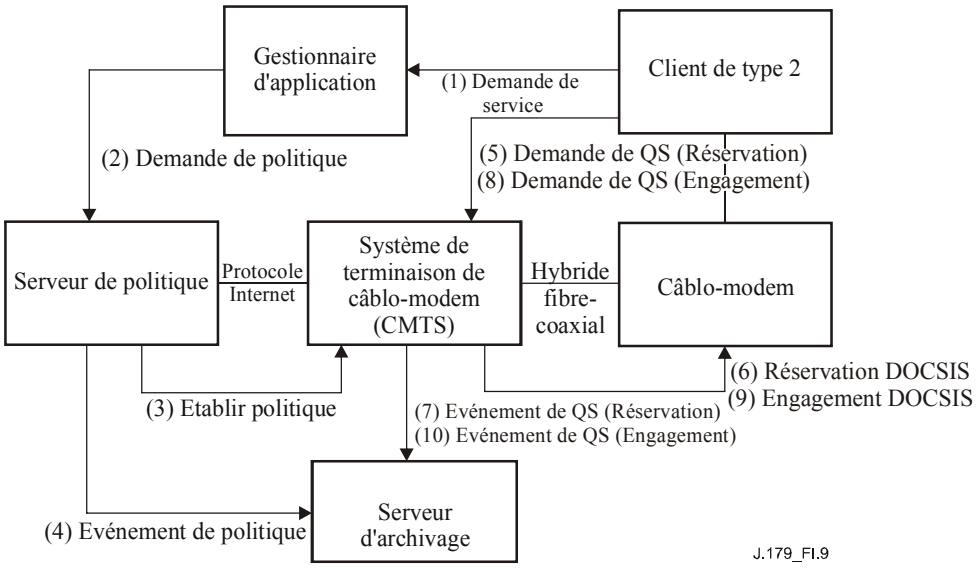

Figure I.9/J.179 – Modèle de réservation de ressources en deux phases pour le scénario 2

Tableau I.5/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(1) Demande de service	Le client demande le service au gestionnaire d'application.	<aucun>	Hors du domaine d'IPCablecom multimédia	Ce protocole devrait prendre en charge l'authentification du client et du gestionnaire d'application. Le protocole devrait aussi fournir des informations suffisantes pour que le gestionnaire d'application convoie les besoins de QS du service demandé.
(2) Demande de politique	Le gestionnaire d'application demande l'autorisation de QS au nom du client.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque.	Commande de porte (COPS)	Le Serveur de politique utilise les règles de politique gérées par l'opérateur pour accorder ou refuser la demande
(3) Etablir politique	Le Serveur de politique envoie un message au CMTS, installant sa décision de politique.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS).	Commande de porte (COPS)	Dans ce scénario, cette demande est seulement pour autorisation
(4) Evénement de politique	Le Serveur de politique génère le message d'événement approprié, indiquant la Demande de politique et l'action effectuée.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir suffisamment de matière pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou la réconciliation.

Tableau I.5/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(5) Demande de QS (Réservation)	Le client demande que les ressources de QS soient réservées	Paramètres de Bande passante et Temps de latence, Classeur de trafic.	DSx de câblo-modem ou RSVP+	Le client peut établir directement les flux de service de câblo-modem via l'échange de message DSx ou peut produire des messages RSVP+ pour établir ces flux.
(6) Réservation DOCSIS	Le CMTS établit les flux de service de QS améliorée et les place dans un état "admis".	Paramètres Type de programmation de câblo-modem, Bande passante et Temps de latence, Classeur de trafic.	Echange de messages DSx de câblo-modem	Cette étape n'est nécessaire que si la signalisation RSVP+ a été fournie au CMTS dans le message précédent, autrement, les flux de service ont déjà été établis et activés via l'échange de messages DSx de câblo-modem. Les fonctions de QS sont fondées ici sur les mécanismes définis dans les Recommandations de câblo-modem.
(7) Evénement de QS	Le CMTS génère le message d'événement approprié, indiquant l'utilisation de la QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation de service, Heure du jour.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir suffisamment de matière pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou la réconciliation.
(8) Demande de QS (Engagement)	Le client demande que les ressources de QS soient engagées	Paramètres de Bande passante et Temps de latence, Classeur de trafic.	DSx de câblo-modem ou RSVP+	Le client peut établir directement les flux de service de câblo-modem via l'échange de message DSx ou peut produire des messages RSVP+ pour établir ces flux.

Tableau I.5/J.179 – Détails des messages de réservation de ressources en deux phases pour le scénario 2

Message	Fonction	Champs	Protocole candidat	Commentaires
(9) Engagement DOCSIS	Le CMTS place les flux de service dans l'état "actif".	Paramètres Type de programmation de câblo-modem, Bande passante et Temps de latence, Classeur de trafic, ID de flux de service.	Echange de messages DSx de câblo-modem	Cette étape n'est nécessaire que si la signalisation RSVP+ a été fournie au CMTS dans le message précédent, autrement, les flux de service ont déjà été établis et activés via l'échange de messages DSx de câblo-modem. Les fonctions de QS sont fondées ici sur les mécanismes définis dans les Recommandations de câblo-modem.
(10) Evénement de QS	Le CMTS génère le message d'événement approprié, indiquant l'utilisation de la QS et les autres paramètres de facturation.	Paramètres Type de QS IPCablecom MM, Classe de session IPCablecom MM, Bande passante et Temps de latence, Classeur de trafic, Conseil de facturation opaque (pour l'AM et le PS), Décision de politique, Données d'utilisation de service, Heure du jour.	Echange de messages d'événement (RADIUS)	Ce message devrait contenir suffisamment de matière pour permettre une reconstruction du ou des événements et de la ou des décisions prises par rapport à un service particulier pour les besoins de la prise en charge et/ou la réconciliation

Comme dans le scénario précédent, il existe une alternative à l'égard de la suppression et la récupération des ressources de qualité de service. Les ressources peuvent arriver au terme du délai qui leur est accordé (ce qui est détecté au CMTS) pour cause d'inactivité sans un rafraîchissement de temporisateur signalé, ou bien elles peuvent être explicitement supprimées par le client à la conclusion d'une session de service. Le mécanisme fourni pour signaler explicitement la suppression d'un flux de service est un composant du protocole de la qualité de service défini pour le Client de type 2. La seule variante entre la séquence de récupération définie pour le scénario 1 et celle du scénario 2 est que la suppression du flux de service est signalée directement via le client au lieu d'être mandatée au moyen du gestionnaire d'application dans le second scénario.

I.5.1 Exemple: jeu en ligne via des consoles en réseau

L'exemple de la console de jeu en réseau pour le scénario 1 au § I.4.2 peut facilement être modifié pour se conformer au modèle de gestion de ressources de QS présenté dans le scénario 2. Dans ce cas, les consoles se coordonneraient encore avec un gestionnaire d'application afin de se localiser l'une l'autre et établir la signalisation spécifique de l'application. De plus, le gestionnaire d'application devrait soumettre une Demande de ressources au Serveur de politique pour demander

l'autorisation des ressources de QS nécessaires. Cependant, lors de l'installation réussie de cette décision d'autorisation au CMTS, le gestionnaire d'application devrait simplement retourner un accusé de réception affirmatif contenant un jeton d'autorisation à chaque mandataire de micro-ordinateur. Ce jeton pourrait alors être utilisé par les micro-ordinateurs dans leur signalisation de QS aux CMTS afin de réserver, engager et supprimer les flux de service nécessités par le tunnel de jeu.

I.6 Qualité de service demandée par le client avec politique poussée (Scénario 3)

Le troisième scénario, avec son modèle d'autorisation de "QS demandée par le client avec politique poussée", prend en charge le Client de type 3. Le scénario 3 définit un modèle dans lequel les décisions d'autorisation de politique ne sont pas préétablies et sont poussées au CMTS via les mécanismes de gestionnaire d'application et de Serveur de politique décrits dans les scénarios précédents, mais sont appelées à la demande par le CMTS auprès du Serveur de politique selon les demandes de réservation entrantes. Ceci permet un modèle de réservations de ressources très souple, stimulé par le client, tout en maintenant un contrôle sur les autorisations par l'opérateur à l'extrémité de tête pour toutes les demandes de ressource.

Dans ce scénario, le CMTS reçoit une demande de qualité de service du client avant qu'une décision de politique ne soit installée par le Serveur de politique. Les habilitations qui permettent au client d'être authentifié sont incluses avec cette demande de qualité de service. Le CMTS construit une demande de politique qu'il envoie au Serveur de politique. Au Serveur de politique, la demande est authentifiée et une décision d'autorisation est prise sur la base des critères spécifiés par l'opérateur (par exemple, disponibilité des ressources, profil de l'utilisateur, taux de crédit, classe de service, interaction avec d'autres éléments de réseau, etc.). Si l'autorisation de politique réussit, la réservation de ressources est autorisée à continuer sur le CMTS et les flux de service de câblo-modem appropriés sont établis sur la base de la qualité de service demandée. Les interfaces IPCablecom multimédia (définis au § I.3.1) impliqués dans cette interaction comprennent pkt-mm1, pkt-mm-2, pkt-mm-4, pkt-mm-5, pkt-mm-6, et mm-9. L'interface pkt-mm-3 peut aussi être utilisée selon les exigences de signalisation spécifiques de l'application mais elle n'est pas supposée être utilisée.

La Figure I.10 illustre le flux d'informations entre les éléments de réseau d'accès principaux pour le scénario 3. Le Tableau I.6 qui suit la Figure I.10 donne une description de chaque message. Dans l'exemple qui figure ci-dessous, la qualité de service n'est établie que dans le sens amont entre le câblo-modem et le système CMTS. Un flux similaire serait nécessaire pour établir la qualité de service aval symétrique.

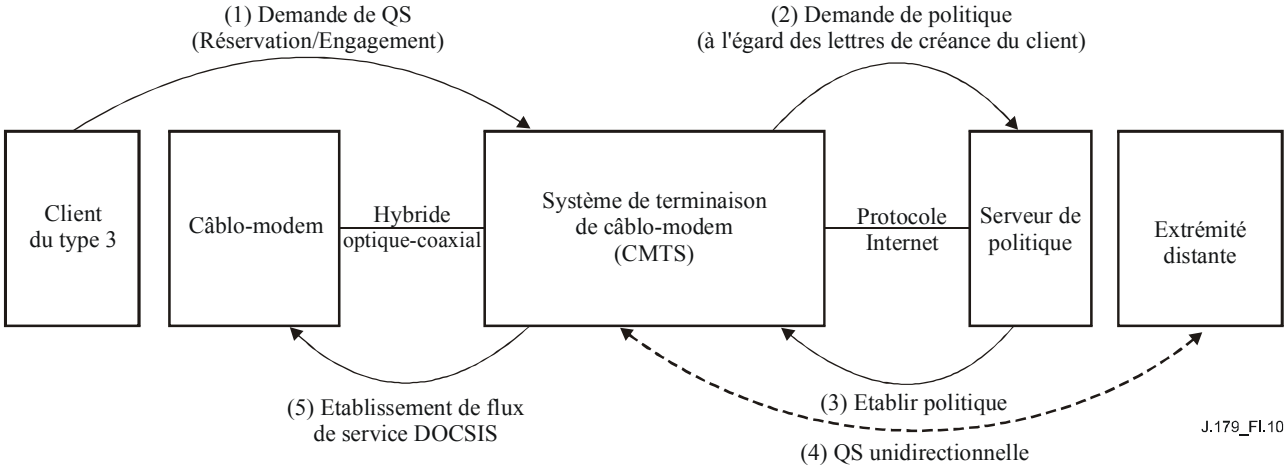

Figure I.10/J.179 – Cadre d'autorisation pour le scénario 3

Tableau I.6/J.179 – Détails des messages pour le scénario 3

Message	Fonction	Champs	Protocole candidat	Commentaires
(1) Demande de QS (Réservation/Engagement)	Le client demande une réservation de ressources au CMTS	Paramètres Bande passante et Temps de latence, Classeur de trafic, Créances d'authentification.	RSVP	Ce scénario suppose que les capacités de RFC 2205 existent chez le client.
(2) Demande de politique	Le CMTS sollicite une décision d'autorisation de politique du Serveur de politique	Paramètres Bande passante et Temps de latence, Classeur de trafic, Créances d'authentification.	COPS	RFC 2748
(3) Etablir politique	Le Serveur de politique installe l'autorisation au CMTS	Paramètres Bande passante et Temps de latence, Classeur de trafic.	COPS	RFC 2748
(4) QS unidirectionnelle	Le CMTS fait suivre la signalisation RSVP d'extrémité distante	Paramètres Bande passante et Temps de latence, Classeur de trafic, Créances d'authentification.	RSVP	RFC 2205
(5) Etablissement de flux de service de câblo-modem	Le CMTS négocie avec le câblo-modem l'établissement du flux de service programmé de câblo-modem	Paramètres Type de programmation de câblo-modem, Bande passante et Temps de latence, Classeur de trafic, ID de flux de service.	Echange de messages DSx de câblo-modem	Les fonctions de qualité de service sont ici fondées sur les mécanismes définis dans les Recommandations des câblo-modems.

Une des principales caractéristiques distinctives de ce scénario est de prendre en charge le protocole RSVP, mécanisme de signalisation de la qualité de service fondé sur les normes. Alors que le scénario 1 vise les clients qui n'ont pas de capacités propres de signalisation de la qualité de service, et que le scénario 2 définit un mécanisme de signalisation de la qualité de service spécifique d'IPCablecom (fondé sur le protocole RSVP, mais incluant des extensions non normalisées), ce scénario se fonde sur une norme de l'IETF. Ceci permettra l'interopérabilité avec les clients qui s'appuient sur les normes et souscrivent aux services de QS de l'opérateur, qui auront ainsi un moyen de s'authentifier en toute sécurité sur le réseau d'accès. Il n'exige pas non plus d'application qui pousse les décisions de politique à l'avance, et n'impose donc pas de contrainte d'architecture sur la signalisation d'application.

Le scénario 3 suppose que l'échange de message RSVP est effectué entre le client et l'extrémité distante. Noter cependant que cela n'exige pas que tous les éléments de réseau entre le client et l'extrémité distante aient besoin de prendre en charge RSVP, pas plus que cela n'implique l'utilisation d'une stratégie de qualité de service de bout en bout de services intégrés (IntServ [18]). Par exemple, des services différenciés (DiffServ 19) ou un autre schéma de QS peut être utilisé au delà du CMTS. De plus, les routeurs intermédiaires qui ne souhaitent pas prendre en charge RSVP peuvent simplement passer les messages RSVP sans les traiter. Autrement, si les garanties de qualité de service peuvent être obtenues par d'autres moyens, de tels routeurs peuvent être définis

comme des régions d'agrégation et donc passer les messages RSVP de façon transparente, comme défini dans le document RFC 3175 [20].

NOTE – RFC 3175 exige une implémentation de cette fonction d'agrégation sur les deux routeurs périphériques, proche et distant.

De plus, il convient de noter que l'utilisation de RSVP dans ce scénario se conforme étroitement au fonctionnement RSVP standard (c'est-à-dire, RFC 2205 [14]), et donc, les réservations de ressources sur le réseau d'accès sont unidirectionnelles. Ainsi, le client réserves des ressources amont, et l'extrémité distante est responsable de la réservation des ressources aval.

Les réservations de ressources réussies sont maintenues de la même façon que les réservations des autres scénarios, au moyen de rafraîchissements d'états souples. Le client RSVP DOIVENT envoyer périodiquement des messages pour maintenir leurs réservations, faute de quoi elles arriveront à expiration et seront réclamées au CMTS.

Finalement, des mécanismes spécifiques sont inclus dans le protocole RSVP pour permettre au point de terminaison émetteur ou récepteur de signaler l'achèvement et la suppression d'un flux de service. Sur la base de la nature unidirectionnelle des réservations RSV, un point d'extrémité maintenant plusieurs flux de service est responsable de la suppression explicite de ces flux à la conclusion d'une session de service.

Etant donné ce modèle, une considération toute particulière doit être apportée à l'authentification de la demande de l'extrémité distante pour permettre la réservation de ressources aval. Une solution est d'exiger que le Serveur de politique puisse authentifier les deux clients d'extrémité proche et d'extrémité distante. D'autres solutions sont aussi possibles, mais les implications en matière de sécurité, et en particulier le vol de service potentiel, DOIVENT être considérées avec attention.

I.6.1 Exemple: jeu en ligne avec signalisation de QS native

Un service potentiel qui peut tirer profit du scénario 3 est le jeu en ligne. Dans cet exemple, tout ce qui serait nécessaire est la prise en charge par le client du protocole RSVP intégré normalisé. Ce qui veut dire que le jeu en ligne devrait être conçu pour fonctionner avec ou sans Serveur d'application.

Lorsqu'un client souhaite se joindre à une partie, il doit simplement envoyer un message spécifique de l'application à l'extrémité distante, puis continuer en demandant la qualité de service du réseau par l'envoi d'un message RSVP, lui aussi adressé au point de terminaison distant. Lorsque le CMTS reçoit ce message, il devrait envoyer une demande au Serveur de politique afin d'authentifier le client et décider si la qualité de service devrait être accordée ou non. Le succès de l'autorisation devrait déboucher sur une réservation unidirectionnelle.

De même, l'extrémité distante devrait envoyer un message RSVP adressé au client. A nouveau, à réception au CMTS, ce message devrait être envoyé au Serveur de politique pour déterminer si la qualité de service sera accordée. L'autorisation et le service étant accordés, le client aurait alors la qualité de service dans les deux directions et pourrait engager la partie.

I.7 Comparaison d'IPCablecom-T et d'IPCablecom multimédia

Le présent paragraphe décrit, à haut niveau, les principales différences entre les architectures IPCablecom-T et IPCablecom multimédia. Considérons que la plupart des caractéristiques spécifiques du protocole et les détails fonctionnels d'IPCablecom multimédia ne sont pas encore définis à ce moment. Voir au Tableau I.7 le résumé des différences connues pour servir de référence.

Tableau I.7/J.179 – Différences entre IPCablecom-T et IPCablecom multimédia

	IPCablecom-T	IPCablecom multimédia
Services pris en charge	Téléphonie résidentielle: • caractéristiques téléphoniques résidentielles de base; • caractéristiques téléphoniques étendues.	Services multimédia: • fondés sur le client (d'homologue à homologue); • fondés sur le serveur.
Echange de messages d'événement	Chemin d'audit solide pour tous les événements de politique et qualité de service Prise en charge du modèle de facturation du RTPC	Chemin d'audit solide pour tous les événements de politique et de qualité de service Prise en charge de la comptabilité fondée sur la QS Prise en charge de la comptabilité fondée sur la durée et le volume
Capacités de qualité de service	Algorithmes de programmation de QS de câblo-modem: • service d'allocation non sollicitée; • service d'allocation non sollicitée avec détection d'activité. Caractéristiques de bande passante: • débit binaire constant; • débit binaire variable. Niveau de QS garantie: de client-à-client (c'est-à-dire, de bout en bout au moyen du modèle segmenté)	Algorithmes de programmation de QS de câblo-modem: • service d'allocation non sollicitée; • service d'allocation non sollicitée avec détection d'activité; • interrogation en temps réel; • interrogation en temps différé; • au mieux avec ou sans Priorité; Caractéristiques de bande passante: • débit binaire constant; • débit binaire variable; • symétrie amont/aval; • asymétrie amont/ava;l Niveau de QS garantie: de CMTS à CM (c-à-d, sur le réseau d'accès)
Sécurité	Signalisation et média sécurisés Approvisionnement d'appareil et gestion de configuration sécurisés	COPS et RADIUS sécurisés via IPsec; gestion de clés via IKE avec des clés d'authentification prépartagées (IKE avec certificats ou gestion de clés Kerbérisées sont facultatifs). La signalisation client est hors du domaine d'application de la présente Recommandation, et donc il n'y a pas de sécurité définie pour l'interface de signalisation client.

I.7.1 DQoS

IPCablecom-T est principalement orienté vers les services de téléphonie résidentielle. La spécification de la Qualité de service dynamique (DQoS) a été développée à ce titre, pour définir les mécanismes nécessaires à la fourniture de qualité de service sur la partie accès fondée sur le câblo-modem du réseau IP. Cela étant, IPCablecom-T adopte une approche segmentée (qui sépare le média de bout en bout et le canal sémaphore en réseaux d'accès proche et distant joints par un cœur de réseau) dans laquelle la DQoS s'intéresse spécifiquement aux réservations de ressources sur le segment d'accès, et non au cœur de réseau ou à la qualité de service de bout en bout.

La cible d'IPCablecom multimédia est plus centrée sur des applications multimédia générales, qui vont au delà de la prise en charge de la voix. Cependant, il est bâtit sur certains des mécanismes fondamentaux de la DQoS d'IPCablecom-T pour fournir des services de QS améliorée à ces applications.

I.7.1.1 Eléments de réseau d'accès

IPCablecom-T prend en charge les éléments de réseau suivants: adaptateur MTA, câblo-modem, système CMTS, serveur CMS (logiquement composé d'un Agent d'appel et d'un Contrôleur de porte) et d'un serveur d'archivage. Dans l'architecture IPCablecom multimédia, l'Agent d'appel peut être transposé fonctionnellement en un gestionnaire d'application, et le Contrôleur de porte peut être transposé fonctionnellement en Serveur de politique. Dans l'architecture IPCablecom multimédia, des éléments de réseau additionnels peuvent être introduits, y compris, par exemple, un Serveur de média. Le gestionnaire d'application et le Serveur de média peuvent résider physiquement dans le même équipement, ou bien peuvent être séparés.

I.7.1.2 Architecture de DQoS

L'architecture IPCablecom DQoS [14] se fonde sur les politiques de câblo-modem, RSVP+, et de qualité de service installées au CMTS par le serveur CMS (Contrôleur de porte).

Comme décrit tout au long de ce rapport, l'architecture IPCablecom multimédia se fonde aussi sur ces technologies. En plus, l'effort multimédia a pour objectif de prendre en charge un modèle de signalisation RSVP plus normalisé (scénario 3) avec l'idée que cette capacité rendra les services de qualité de service améliorée disponibles pour une base plus large de consommateurs.

Dans l'architecture de DQoS d'IPCablecom-T, le système CMTS sert de point de mise en application des politiques de qualité de service. Le CMTS va effectuer une fonction similaire dans l'architecture IPCablecom multimédia. En plus de la satisfaction des demandes de qualité de service provenant des clients, le CMTS peut aussi recevoir des demandes de qualité de service mandatées provenant du Serveur de politique (scénario 1). Ceci diffère de l'architecture de DQoS d'IPCablecom-T, où seuls les adaptateurs MTA autonomes ou les MTA intégrés peut lancer l'activation de la qualité de service.

I.7.1.3 Interfaces de qualité de service

Dans l'architecture IPCablecom-T, les interfaces de signalisation ont été définies entre tous les éléments de réseau, aussi bien qu'entre les CMTS pour les appels de réseau à réseau acceptant la coordination de porte. En résumé, le principal protocole de signalisation entre l'adaptateur MTA et l'Agent d'appel est la signalisation NCS, entre le MTA intégré et le CMTS, c'est le câblo-modem, et entre un MTA intégré et le CMTS, c'est RSVP+. La signalisation venant du Contrôleur de porte vers le CMTS est l'échange de messages de commande de porte fondé sur COPS.

IPCablecom multimédia se bâtit sur ces interfaces de signalisation et de plus prend en charge les interfaces de signalisation entre le gestionnaire d'application et le Serveur de politique. On rappelle que toute signalisation spécifique de l'application survenant entre le gestionnaire d'application et ses clients est en dehors du domaine d'application de cette architecture.

I.7.1.4 Cadres de la qualité de service IPCablecom

Dans l'architecture IPCablecom-T, "une construction définie de qualité de service appelée une porte fournit le point de contrôle pour la connexion des réseaux d'accès au service de cœur de réseau de haute qualité." (Voir la spécification DQoS [14].) La porte représente une autorisation de qualité de service qui est installée au CMTS pour les besoins de la mise en application de la politique. IPCablecom multimédia définit une construction de politique de qualité de service similaire, et on pense que la construction de la porte de DQoS d'IPCablecom-T sera au niveau pour fournir la fonction de politique dans IPCablecom multimédia. Des modifications aux mécanismes existants de

la commande de porte d'IPCablecom-T pourront être nécessaires pour fournir une commande de qualité de service atténuée (par exemple, pour la prise en charge du scénario 1).

I.7.1.5 Exigences pour la gestion de ressources de réseau d'accès

L'architecture IPCablecom-T "vise à fournir un haut degré de généralité avec l'intention de rendre possibles de nouveaux services et une évolution future des architectures de réseau". Cet objectif conduit à plusieurs exigences pour une architecture de qualité de service viable dans les domaines suivants (noter que chacune de ces capacités se rapportant à la qualité de service est clairement définie et discutée dans la spécification IPCablecom DQoS):

- changements de ressources durant une session;
- liaison dynamique des ressources;
- classe de session (désignation de la priorité);
- engagement de ressources en deux phases;
- allocation de ressources segmentée;
- prise en charge de la qualité de service de cœur de réseau;
- prévention du vol de service.

L'architecture IPCablecom multimédia va aussi prendre en charge un modèle de réservation de ressources en une seule phase. Au départ, l'architecture multimédia ne s'intéresse pas à la prise en charge de la qualité de service de cœur de réseau, bien que cette fonctionnalité puisse être formellement considérée si les besoins de l'opérateur l'exigent. Pour plus d'informations sur les exigences de qualité de service existantes d'IPCablecom-T, se référer à la spécification de la DQoS d'IPCablecom-T [14].

I.7.1.6 Théorie de fonctionnement

La DQoS IPCablecom-T implique des phases distinctes de réservation et d'engagement pour l'obtention des ressources de réseau d'accès. A la fin de la phase de réservation, les ressources sont mises de côté mais pas encore actives ou disponibles pour l'adaptateur MTA. A la fin de la seconde phase, les ressources sont engagées et rendues disponibles pour utilisation. Dans le modèle traditionnel de la téléphonie, la facturation commence à la phase d'engagement.

Dans le modèle avec adaptateur MTA intégré, RSVP+ n'est pas nécessaire entre l'adaptateur MTA et le système CMTS. A la place, l'E-MTA peut signaler la réservation et l'engagement des ressources via l'échange de messages de câblo-modem. Dans le modèle d'adaptateur MTA autonome, l'échange de messages RSVP+ est utilisé pour effectuer ces étapes. Le câblo-modem et le système CMTS se coordonnent alors via l'échange de messages DSx de câblo-modem pour programmer les flux de service nécessaires sur le réseau d'accès.

Comme évoqué dans le présent appendice, IPCablecom multimédia prend en charge un modèle similaire à celui d'IPCablecom-T, et de plus prend en charge une utilisation plus normalisée de RSVP. Il fournit aussi un modèle de demande de qualité de service mandaté, dans lequel le gestionnaire d'application gère la qualité de service au nom du client. Ces modèles sont décrits en détails dans la section consacrée aux scénarios du présent appendice. Le modèle existant d'IPCablecom-T correspond au scénario 2. Les deux autres modèles sont pris en charge dans l'architecture IPCablecom multimédia pour donner plus de souplesse à la façon dont les services multimédia peuvent être déployés dans le réseau de l'opérateur.

I.7.2 Messages d'événement pour la facturation

Les messages d'événement IPCablecom sont conçus pour être flexibles et extensibles afin de transporter les informations sur l'utilisation du réseau pour une grande diversité de services fournis sur l'architecture IPCablecom. La spécification de message d'événement d'IPCablecom-T définit l'architecture générale de message d'événement aussi bien que les exigences spécifiques pour

prendre en charge le service vocal d'IPCablecom-T. La spécification de message d'événement IPCablecom [15] précise les détails du format de TLV de message d'événement indépendant du protocole de transport, un format de fichier de message d'événement, et des protocoles de transport obligatoires et facultatifs.

Ces messages contiennent des informations suffisantes sur la base de la session pour prendre en charge la facturation de l'utilisateur du service. Les informations contenues dans les messages d'événement prennent en charge une grande variété de modèles de facturation et de règlements. IPCablecom ne rend pas obligatoires les modèles spécifiques de facturation ou de règlement car ces modèles sont définis et fondés sur les exigences commerciales spécifiques des câblo-opérateurs particuliers. IPCablecom ne rend pas obligatoire ni n'interdit l'utilisation d'une chambre de compensation pour les règlements.

Les messages d'événement IPCablecom se fondent sur un modèle dans lequel la session ou le service est divisé en une moitié d'origine et une moitié de terminaison. Le serveur CMS d'origine ou MGC DOIT générer un ID de corrélation de facturation unique (BCID) pour identifier tous les messages d'événement associés à la moitié d'origine de la session. Le CMS de terminaison ou MGC DOIT générer un BCID unique pour identifier tous les messages d'événement associés à la moitié de terminaison de la session. Pour chaque moitié de la session ou service, l'ensemble des éléments de réseau IPCablecom qui génèrent des messages d'événement (CMS, MGC, CMTS) DOIVENT fournir toutes les informations nécessaires requises pour la facturation et/ou les règlements de façon appropriée selon le service. Les informations générées par la moitié d'origine DOIVENT être envoyées au RKS qui prend en charge la moitié d'origine. Les informations générées par la moitié de terminaison DOIVENT être envoyées au RKS qui prend en charge la moitié de terminaison.

Un ensemble limité de messages d'événement est nécessaire pour les services IPCablecom multimédia. Ces messages comportent:

- Début _de_Signal pour "Service de QS améliorée" généré par le Serveur de politique qui indique le moment auquel le Serveur de politique reçoit une demande de qualité de service de réseau d'accès;
- Fin_de_Signal pour "Service de QS améliorée" généré par le Serveur de politique qui indique le moment auquel le Serveur de politique reçoit une notification de la fin de l'utilisation de la qualité de service par le réseau;
- Réservation_de_QS, Engagement_de_QS, Fin_de_QS, généré par le CMTS. Ces messages indiquent le moment auquel le CMTS réserve, engage ou libère la qualité de service de réseau d'accès.

I.7.3 Sécurité

L'architecture de sécurité IPCablecom-T définit les mécanismes, algorithmes et protocoles qui satisfont les exigences du service de sécurité. Les interfaces IPCablecom multimédia sont sécurisées en utilisant des mécanismes identiques pour les interfaces correspondantes.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005