Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.163

(11/2005)

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

IPCablecom

Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems

Recommandation UIT-T J.163

Recommandation UIT-T J.163

Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems

Résumé

La présente Recommandation traite des prescriptions pour qu'un dispositif client obtienne l'accès aux ressources d'un réseau. Elle spécifie en particulier un mécanisme global pour qu'un dispositif client demande au réseau DOCSIS une qualité de service spécifique. De nombreux exemples illustrent l'utilisation de la présente Recommandation. Le domaine d'application de la présente Recommandation est la définition de l'architecture de qualité de service pour la portion "accès" du réseau IPCablecom, fournie flux par flux aux applications demandeuses. La portion accès du réseau est définie comme étant située entre l'adaptateur de terminal multimédia (MTA, *multimedia terminal adapter*) et le système de terminaison de câblo-modem (CMTS, *cable modem termination system*), y compris le réseau DOCSIS. La méthode d'allocation de la qualité de service (QS) sur le cœur de réseau n'est pas définie dans la présente Recommandation, laquelle n'aborde pas non plus l'interfaçage avec le cœur de réseau IP géré ni les questions relatives à la multidiffusion IP. La présente Recommandation reconnaît également que des réservations par flux peuvent être requises à l'intérieur des locaux du client, et donc le protocole qui y est développé traite de ce besoin potentiel.

Source

La Recommandation UIT-T J.163 a été approuvée le 29 novembre 2005 par la Commission d'études 9 (2005-2008) 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

Recommandation UIT-T J.163

Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems

1 Domaine d'application

La présente Recommandation traite des prescriptions pour qu'un dispositif client obtienne l'accès aux ressources d'un réseau. Elle spécifie en particulier un mécanisme global pour qu'un dispositif client demande au réseau DOCSIS une qualité de service spécifique. De nombreux exemples illustrent l'utilisation de la présente Recommandation. Le domaine d'application de la présente Recommandation est la définition de l'architecture de qualité de service pour la portion "accès" du réseau IPCablecom, fournie flux par flux aux applications demandeuses. La portion accès du réseau est définie comme étant située entre l'adaptateur de terminal multimédia (MTA) et le système de terminaison de câblo-modem (CMTS), y compris le réseau DOCSIS. La méthode d'allocation de la qualité de service (QS) sur le cœur de réseau n'est pas définie dans la présente Recommandation, laquelle n'aborde pas non plus l'interfaçage avec le cœur de réseau IP géré ni les questions relatives à la multidiffusion IP. La présente Recommandation reconnaît également que des réservations par flux peuvent être requises à l'intérieur des locaux du client, et donc le protocole qui y est développé traite de ce besoin potentiel.

2 Références

2.1 Références normatives

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 figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

- Recommandation UIT-T J.83 (1997), *Systèmes numériques multiprogrammes pour la distribution par câble des services de télévision, son et données*.
- Recommandation UIT-T J.112 (1998), *Systèmes de transmission pour services interactifs de télévision par câble*.
- Recommandation UIT-T J.112 Annexe A (2001), *Diffusion vidéonumérique: canal d'interaction pour les systèmes de télédistribution par câble*.
- Recommandation UIT-T J.112 Annexe B (2004), *Spécifications de l'interface du service de transmission de données par câble: interface radioélectrique*.
- Recommandation UIT-T J.160 (2005), *Cadre architectural pour l'acheminement de services à temps critique sur des réseaux de télévision par câble utilisant des câblo-modems*.
- Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems*.
- IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.

2.2 Références informatives

– Recommandation UIT-T G.114 (2003), *Temps de transmission dans un sens*.

– Recommandation UIT-T G.711 (1988), *Modulation par impulsions et codage (MIC) des fréquences vocales*.

– Recommandation UIT-T G.726 (1990), *Modulation par impulsions et codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s*.

– Recommandation UIT-T G.728 (1992), *Codage de la parole à 16 kbit/s en utilisant la prédiction linéaire à faible délai avec excitation par code*.

– Recommandation UIT-T G.729 Annexe E (1998), *Algorithme de codage vocal CS-ACELP à 11,8 kbit/s*.

– Recommandation UIT-T J.162 (2005), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.164 (2005), *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*.

– Recommandation UIT-T J.170 (2005), *Spécification de la sécurité sur IPCablecom*.

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol specification (Protocole Internet; Programme Internet DARPA; spécification du protocole)*.

– IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal control (Profil du protocole RTP pour audioconférences et visioconférences avec contrôle minimal)*.

– IETF RFC 2327 (1998), *SDP: Session Description Protocol (SDP: Protocole de description de session)*.

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (Définition du champ de services différenciés (Champ DS) dans les en-têtes IPv4 et IPv6)*.

– IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control (Cadre pour un contrôle d'admission fondé sur une politique)*.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 câblo-modem: un dispositif terminal de couche 2 terminant l'extrémité client de la connexion J.112 (ou J.122).

3.2 flux DOCSIS: flux de paquets de données mono ou bidirectionnel, qui est soumis à la signalisation de couche MAC et à une attribution de qualité de service (QS) conformes à la Rec. UIT-T J.112 (ou Rec. UIT-T J.122).

3.3 IPCablecom: projet de l'UIT-T qui inclut une architecture et une série de Recommandations qui permettent la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems.

4 Abréviations et conventions

4.1 Abréviations

La présente Recommandation utilise les abréviations suivantes:

CM câblo-modem (*cable modem*)

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

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

CPE équipement de locaux d'abonné (*customer premises equipment*)

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

DSA ajout de service dynamique (*dynamic service addition*)

DSC changement de service dynamique (*dynamic service change*)

INA adaptateur de réseau interactif (*interactive network adapter*)

IP protocole Internet (*Internet protocol*)

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

NCS signalisation d'appel fondée sur le réseau (*network-based call signalling*)

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

QS qualité de service

RAP protocole d'allocation de ressources (*resource allocation protocol*)

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

RTPC réseau téléphonique public commuté

TLV type-longueur-valeur (*type-length-value*)

VAD détection d'activité vocale (*voice activity detection*)

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 de mettre en œuvre 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 technique

La qualité de service améliorée est requise pour prendre en charge les applications multimédias interactives. Les ressources peuvent être restreintes dans des segments du réseau, nécessitant l'allocation de ressources dans le réseau. Le domaine d'application de la présente Recommandation est la définition de l'architecture de qualité de service pour la portion "accès" du réseau IPCablecom. La portion accès du réseau est définie comme étant située entre l'adaptateur de terminal multimédia (MTA, *multimedia terminal adaptor*) et le système de terminaison de câblo-modem (CMTS, *cable modem termination system*), y compris le réseau DOCSIS. La présente Recommandation reconnaît également que des réservations par flux peuvent être requises à l'intérieur des locaux du client, et donc les protocoles développés dans la présente Recommandation traitent de ce besoin potentiel. Bien que certains segments du cœur de réseau puissent nécessiter la réservation de ressources pour fournir une qualité de service adéquate, on considère que les protocoles relatifs à la gestion des ressources du cœur de réseau sont en dehors du domaine d'application de la présente Recommandation.

Les ressources sont allouées sur le réseau DOCSIS pour les flux individuels associés à chaque session d'une application, par abonné, sur une base autorisée et authentifiée. Une session DQS, ou simplement une session, est définie par la présente Recommandation comme un flux de données bidirectionnel unique entre deux clients. Lorsqu'une application multimédia nécessite plusieurs flux de données bidirectionnels (par exemple, un flux pour la voix et un flux séparé pour la vidéo), des sessions DQS séparées sont établies pour chaque flux. Les applications peuvent utiliser uniquement la moitié du flux de données bidirectionnel de la session, en fournissant ainsi des services en émission seule ou en réception seule. Par exemple, dans une application de communication vocale typique, une simple communication entre deux parties est implémentée par une seule session, alors que les communications complexes, multipartites (par exemple "conférences téléphoniques") sont implémentées par des sessions simultanées multiples.

Le protocole de signalisation d'appel IPCablecom défini utilise la signalisation d'appel fondée sur le réseau (Rec. UIT-T J.162). La présente spécification de QS dynamique est la structure de QS sous-jacente pour ce protocole de signalisation d'appel. La QS est allouée pour les flux associés à une session de concert avec le protocole de signalisation.

La présente Recommandation introduit le concept de structure de QS segment par segment. Elle exploite les informations disponibles dans les protocoles de signalisation pour effectuer l'allocation de QS sur le segment "local" (sur le réseau DOCSIS proche de la partie d'origine) et sur le segment "distant" (le réseau DOCSIS proche de la partie d'arrivée). Ainsi, la présente Recommandation permet à différents fournisseurs d'utiliser les mécanismes les plus appropriés pour le segment qu'ils gèrent. L'utilisation d'un enchaînement des segments avec QS fournit l'assurance d'une QS de bout en bout pour la session.

La spécification d'une QS dynamique incorpore des protocoles permettant aux fournisseurs de communications vocales fondées sur le paquet qui utilisent la structure IPCablecom, d'utiliser différents modèles de facturation, dont la facturation forfaitaire et la facturation en fonction de l'utilisation. La présente Recommandation a pour objet de s'assurer que la QS améliorée est fournie uniquement aux utilisateurs autorisés et authentifiés. Les techniques spécifiques utilisées pour autoriser et authentifier un utilisateur sortent du domaine d'application de la présente Recommandation.

La présente spécification de la QS dynamique reconnaît les exigences d'un service de communications vocales commercialement viable, analogue à celui offert par les moyens du réseau téléphonique public commuté. Il est important de veiller à ce que les ressources soient disponibles avant que les deux parties impliquées dans la session ne soient invitées à communiquer. Ainsi, les ressources sont réservées avant que le destinataire de la communication ne soit averti qu'un correspondant essaie de lancer une communication. S'il n'existe pas de ressources suffisantes pour une session, cette dernière est alors bloquée.

Les protocoles développés dans la présente Recommandation reconnaissent explicitement la nécessité de veiller à éviter toute fraude ou vol de service par des points d'extrémité qui ne souhaitent pas coopérer avec les protocoles de signalisation d'appel et de signalisation de la QS et cherchent ainsi à éviter d'être facturés sur l'utilisation. La présente Recommandation introduit le concept de deux phases pour les réservations de ressources (*reserve* et *commit* c'est-à-dire réservation et engagement). Les deux phases permettent à un fournisseur de n'allouer des ressources que lorsque ces dernières sont nécessaires (lorsque le chemin vocal est coupé) et de pouvoir ainsi les facturer. De plus, étant donné que la seconde phase d'engagement des ressources exige une demande explicite du MTA, elle permet au fournisseur d'empêcher la fraude et le vol de service.

La présente Recommandation est techniquement compatible avec le document correspondant des CableLabs PacketCable: *PacketCable Dynamic Quality-of-Service Specification* PKT-SP-DQOS1.5 I01.

5.1 Exigences relatives à la QS dans une architecture IPCablecom

La liste qui suit présente les exigences de QS pour la prise en charge d'applications multimédias sur des réseaux IPCablecom.

1) *Fournir une comptabilité IPCablecom pour les ressources de QS sur une base session par session*

   Il est prévu, dans une perspective de facturation, que l'une des ressources qu'il sera nécessaire de prendre en compte est l'utilisation de la QS dans le réseau DOCSIS. Il est donc nécessaire d'identifier et de suivre les informations qui permettent de concilier l'utilisation des ressources de QS DOCSIS avec l'activité de la session IPCablecom.

2) *Les deux modèles d'activation de la QS, à deux phases (réservation-engagement) et à phase unique (engagement)*

   Dans le cadre du contrôle des applications, il devrait être possible d'utiliser un modèle d'activation de la QS à deux phases ou à phase unique. Dans le modèle à deux phases, l'application réserve la ressource puis ensuite l'engage. Dans le modèle à phase unique, la réservation et l'engagement se produisent comme une seule opération autonome. Comme dans le modèle DOCSIS, les ressources qui sont réservées mais qui ne sont pas encore engagées sont disponibles pour une allocation temporaire à d'autres flux de service (par exemple, "au mieux"). La présente Recommandation fournit des mécanismes pour l'activation à deux phases et à phase unique pour les MTA intégrés.

3) *Fournir des politiques IPCablecom définies pour contrôler la QS dans le réseau DOCSIS et le cœur de réseau IP*

   Il devrait être possible que différents types de sessions aient différentes caractéristiques de QS. Par exemple, les sessions dans un domaine unique d'un fournisseur exploitant de câble peuvent recevoir une QS différente des sessions en dehors du domaine (par exemple, les sessions internationales incluant des liaisons au RTPC). La présente spécification de QS dynamique peut permettre à un câblo-opérateur de fournir une QS différente pour différents types de clients (par exemple, une QS supérieure pour des abonnés d'un service d'affaires à

certains moments de la journée par rapport à des clients résidentiels) ou différents types d'applications pour un même client.

4) *Empêcher (réduire) l'utilisation abusive de la QS*

Deux types d'utilisation abusive de la QS sont identifiés: celle qui est facturée avec précision mais amène à refuser le service à d'autres et celle qui n'est pas facturée avec précision et amène au vol de service. Les applications d'abonné et les applications IPCablecom (soit intégrées, soit sur PC) peuvent abuser par inadvertance ou intentionnellement de leurs privilèges de QS (par exemple, utilisation par une application FTP d'une QS améliorée, alors que le fournisseur veut la limiter aux applications vocales). Bien que le réseau DOCSIS soit supposé s'appliquer à un accès par abonnement à la QS, des mécanismes élaborés de classification de paquets et de commande de signalisation devraient exister pour empêcher l'abonné (et les appareils de l'abonné) de faire une utilisation frauduleuse de la QS. Il convient que des procédures de contrôle d'admission soient utilisées pour réduire les attaques de refus de service.

5) *Fournir des mécanismes de contrôle d'admission pour le sens amont et aval dans le réseau DOCSIS*

Il convient que la QS amont et aval soit soumise à un contrôle d'admission session par session.

6) *QS DOCSIS*

Il devrait être possible de réguler (par le marquage, l'abandon ou le retard de paquets) tous les aspects de la QS définis au niveau du système CMTS en utilisant les mécanismes de QS DOCSIS. De plus, il devrait être possible de prendre en charge les modèles de mappage de flux multiple – associer une session IPCablecom unique à un flux de service unique et des sessions IPCablecom multiples à un flux de service unique.

7) *La politique est appliquée par le système CMTS*

Le dernier contrôle de politique est confié au système CMTS. Le principe est que tout client puisse effectuer toute demande de QS mais le système CMTS (ou une entité derrière le système CMTS) est la seule entité habilitée à accorder ou à refuser les demandes de QS.

8) *Les entités IPCablecom doivent avoir le moins de connaissances possibles des primitives et des paramètres de QS DOCSIS*

Pour IPCablecom, comme pour toute autre application qui utilise le réseau IP, l'objectif de conception est de réduire la quantité de connaissances spécifiques à la liaison d'accès contenues dans la couche Application. Moins il existera de connaissances sur la liaison d'accès dans la couche Application, plus il existera d'applications disponibles pour le développement et le déploiement et moins les problèmes d'essais et de prise en charge seront nombreux.

9) *Récupération de ressources de QS pour les sessions mortes/anciennes*

Il est nécessaire de récupérer et de réaffecter les précieuses ressources de QS des sessions qui ne sont plus actives mais qui n'ont pas été correctement terminées. Il ne devrait pas y avoir de "fuites" dans la liaison DOCSIS. Par exemple, si un module client IPCablecom ne fonctionne pas correctement au milieu d'une session IPCablecom, toutes les ressources QS DOCSIS utilisées par la session devraient être libérées dans un délai raisonnable.

10) *Changements de politique de QS dynamique*

Il est souhaitable de changer dynamiquement les politiques de QS pour les abonnés. Par exemple, cette exigence concerne la capacité à changer directement le niveau de service d'un client (par exemple, passage d'un service "bronze" à un service "or") sans réinitialiser le câblo-modem.

11) *Temps d'attente minimal absolu d'établissement de session et délai après prise d'appel*

Le réseau IPCablecom devrait permettre l'émulation et l'amélioration de l'expérience que l'utilisateur a du RTPC et présenter la même qualité, voire meilleure, pour les paramètres d'établissement de session et de retard après prise d'appel.

12) *Sessions simultanées multiples*

Il est souhaitable d'allouer des ressources de QS (par exemple, de bande passante) non seulement pour les sessions point à point individuelles mais également pour les sessions point à point multiples (par exemple, conférence téléphonique, appels combinés audio/vidéo).

13) *Réglage dynamique des paramètres de QS au milieu des sessions IPCablecom*

Le service IPCablecom devrait pouvoir changer la QS à mi-session, par exemple, réglage de ressources à l'échelle du réseau ou création de paramètres de codec compatibles (nécessitant des changements de QS) ou caractéristique définie par l'utilisateur pour varier les niveaux de QS ou détection de flux de télécopie ou modem (nécessitant un changement de compression de codec selon la Rec. UIT-T G.711).

14) *Prise en charge de modèles de commande de QS multiples*

Des arguments irréfutables peuvent être avancés aussi bien en faveur de l'initialisation de la signalisation de la QS côté abonné que côté réseau. Dans la signalisation côté abonné, une application peut lancer sa demande de QS immédiatement lorsque l'application pense qu'elle a besoin de la QS. Par ailleurs, la signalisation côté abonné prend en charge des modèles d'application d'homologue à homologue. Dans la signalisation côté réseau, l'implémentation de l'application de point d'extrémité peut ne pas avoir du tout connaissance de la QS (en particulier dans le réseau DOCSIS). La signalisation côté réseau prend en charge des modèles d'application qui sont du type client-serveur (avec serveur de confiance). Il est prévu que les deux modèles coexistent dans les réseaux IPCablecom (et autre application). La présente Recommandation concerne uniquement la signalisation côté abonné.

15) *Prise en charge de la signalisation de la QS aussi bien depuis un MTA intégré que d'un MTA autonome*

Il devrait être possible de signaler la QS depuis un MTA intégré comme d'un MTA autonome. La présente Recommandation ne s'applique qu'au MTA intégré utilisant l'accès direct à la signalisation MAC DOCSIS.

5.2 Eléments de réseau pour l'accès à la QS IP

Les éléments de réseau suivants sont utilisés pour prendre en charge la QS pour les réseaux IPCablecom.

5.2.1 Adaptateur de terminal multimédia (MTA)

Le dispositif client du réseau IPCablecom (c'est-à-dire le MTA) peut être l'un des appareils suivants. Ces dispositifs résident sur le site du client et sont connectés au réseau par l'intermédiaire du canal DOCSIS. Tous les MTA sont supposés implémenter certains protocoles de signalisation

multimédias, tels que J.162. Un MTA peut être soit un dispositif avec un poste téléphonique standard à deux fils dans la configuration MTA-1, soit y ajouter des capacités d'entrée/sortie vidéo dans la configuration MTA-2. Il peut avoir des capacités minimales ou implémenter cette fonctionnalité sur un PC multimédia et avoir toutes les capacités du PC à sa disposition.

Du point de vue de la QS, il existe deux types de MTA.

1) **MTA intégré**: il s'agit d'un terminal multimédia client qui incorpore une interface de couche MAC DOCSIS au réseau DOCSIS.

2) **MTA autonome**: il s'agit d'un terminal client qui implémente la fonctionnalité multimédia sans incorporer une interface de couche MAC DOCSIS. Le MTA autonome utilisera généralement Ethernet, USB, ou IEEE 1394 comme interconnexion physique à un câblo-modem. Le MTA autonome peut être connecté à un réseau client et utiliser des équipements de transport du réseau client (pouvant comprendre des routeurs IP intermédiaires) pour établir des sessions sur le réseau DOCSIS.

5.2.2 Câblo-modem (CM)

Il s'agit d'un élément de réseau IPCablecom défini par la Rec. UIT-T J.112 ou J.122. Le câblo-modem est responsable du classement, de la régulation par une politique et du marquage des paquets une fois que les flux de trafic sont établis par les protocoles de signalisation décrits dans la présente Recommandation.

5.2.3 Système de terminaison de câblo-modem (CMTS)

Le système de terminaison de câblo-modem (CMTS) est responsable de l'allocation et de la programmation d'une bande passante amont et aval conformément aux demandes du MTA et aux autorisations de QS établies par l'administration du réseau. Le système CMTS agit comme un point d'application de la politique (PEP, *policy enforcement point*) conforme au cadre du protocole d'allocation de ressources (RAP, *resource allocation protocol*) de l'IETF (RFC 2753).

Le système CMTS met en œuvre une "porte de QS dynamique IPCablecom" (appelée simplement ci-après "porte") entre le réseau DOCSIS et un cœur de réseau IP. La porte est implémentée en utilisant les fonctions de classification de paquets et de filtrage définies dans la Rec. UIT-T J.112/122.

Le système CMTS peut ou non être également configuré comme une entité "limite IS-DS". Une limite IS-DS (*IS-DS boundary*) établit l'interface avec un interréseau en utilisant le modèle de services intégrés (IntServ*, integrated services*) de contrôle de la QS et d'autres modèles, par exemple, services différenciés (DiffServ*, differentiated services*).

5.2.4 Serveur de gestion des appels (CMS) et contrôleur de porte (GC, *gate controller*)

L'entité serveur de gestion des appels (CMS, *call management server*) d'un réseau IPCablecom exécute des services qui permettent aux MTA d'établir des sessions multimédias (y compris des applications de communications telles que "téléphonie IP" ou "VoIP"). Le terme contrôleur de porte (GC, *gate controller*) est utilisé pour désigner la portion de chaque type de CMS qui exécute les fonctions liées à la qualité de service.

Dans le modèle QS dynamique IPCablecom, le contrôleur de porte commande le fonctionnement des portes implémentées sur un système CMTS. Le GC agit comme point de décision de politique (PDP, *policy decision point*) conforme au cadre du protocole d'allocation de ressources (RAP, *resource allocation protocol*) de l'IETF (RFC 2753).

5.2.5 Serveur d'archivage (RKS)

Le serveur d'archivage (RKS, *record keeping server*) est un élément de réseau IPCablecom qui ne reçoit que les informations des éléments IPCablecom décrits dans la présente Recommandation. Le RKS peut être utilisé comme serveur de facturation, outil de diagnostic, etc.

5.3 Architecture de la QS dynamique IPCablecom

L'architecture de QS dynamique IPCablecom repose sur la Rec. UIT-T J.112, le protocole RSVP de l'IETF et la QS garantie pour les services intégrés de l'IETF.

En particulier, l'architecture de la QS IPCablecom utilise le protocole défini dans la Rec. UIT-T J.112 au sein du réseau de télévision par câble. Ces messages prennent en charge l'installation statique et dynamique de classeurs de paquets (c'est-à-dire les Spéc de filtre *Filter-Specs*) et les mécanismes de programmation de flux (c'est-à-dire les spéc de flux *flowSpecs*) pour fournir une qualité de service améliorée. La QS DOCSIS repose sur les objets que décrivent les spécifications de trafic et de flux, similaires aux objets TSpec et RSpec, tels que définis dans le protocole de réservation de ressources (RSVP) de l'IETF. Cela permet de définir flux par flux les réservations de ressources de QS.

Dans l'architecture de QS DOCSIS, les flux de trafic sont assimilés à une session interactive comprenant deux flux soumis chacun aux opérations indiquées ci-dessous. Pour chaque flux (unidirectionnel):

Lorsque le trafic entre dans le réseau en câble autorisé à la QS IP, le câblo-modem est chargé des fonctions suivantes:

- classification du trafic IP dans les flux QS IP en fonction des spécifications de filtrage définies;
- exécution de la mise en forme et de la régulation du trafic selon la spécification du flux;
- maintien de l'état pour les flux actifs;
- modification du champ Type de service (TOS) dans les en-têtes IP amont en fonction de la politique de l'opérateur du réseau;
- obtention de la QS demandée de la part du système CMTS;
- application correcte des mécanismes de QS DOCSIS.

Le système CMTS est chargé des fonctions suivantes:

- délivrance de la QS requise au câblo-modem en fonction de la configuration de politique;
- allocation de la largeur de bande amont conforme aux demandes du câblo-modem et aux politiques de QS du réseau;
- classement de chaque paquet provenant de l'interface côté réseau et allocation à ce paquet d'un niveau de QS fondé sur les spécifications de filtrage définies;
- régulation du champ Type de service (TOS) à la réception des paquets du réseau en câble pour appliquer les paramètres du champ TOS selon la politique de l'opérateur du réseau;
- modification du champ TOS dans les en-têtes IP aval en fonction de la politique de l'opérateur du réseau;
- exécution de la mise en forme et de la régulation du trafic selon la spécification de flux;
- envoi des paquets aval au réseau DOCSIS en utilisant la QS allouée;
- envoi des paquets amont aux appareils du cœur de réseau en utilisant la QS allouée;
- maintien de l'état pour les flux actifs.

Le cœur de réseau peut utiliser les mécanismes fondés sur les services intégrés de l'IETF ou les mécanismes de services différenciés de l'IETF. Dans un cœur de réseau DiffServ, les routeurs du réseau envoient un paquet en fournissant la QS IP appropriée, en fonction du réglage du champ TOS. Dans un cœur de réseau DiffServ, aucun état par flux n'est nécessaire dans les appareils du réseau central.

5.4 Interfaces de la QS

Les interfaces de signalisation de la qualité de service sont définies entre de nombreux composants du réseau IPCablecom comme l'indique la Figure 1. La signalisation implique la communication des exigences de QS au niveau de la couche Application (par exemple, paramètres SDP), de la couche Réseau (par exemple, RSVP) et de la couche Liaison de données (par exemple, QS DOCSIS). Par ailleurs, l'exigence d'application de la politique et des liaisons de systèmes entre le provisionnement d'abonné OSS, le contrôle d'admission dans le cœur de réseau IP géré et le contrôle d'admission dans le réseau DOCSIS créent un besoin d'interfaces supplémentaires entre les composants du réseau IPCablecom.

La Figure 1 représente pour la QS le cadre de l'architecture IPCablecom, dont une explication détaillée figure dans la Rec. UIT-T J.160.

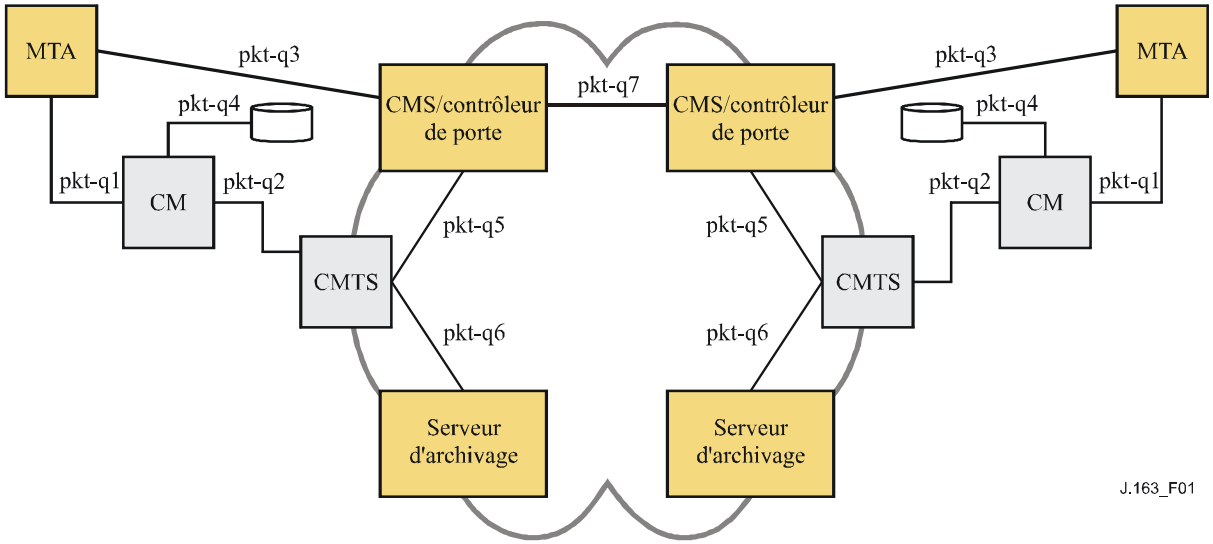


Figure 1/J.163 – Interfaces de signalisation de la QS dans le réseau IPCablecom

Les interfaces pkt-q1 à pkt-q7 sont disponibles pour contrôler et traiter la QS. Toutes les interfaces ne sont pas utilisées dans toutes les variations de configurations et de protocole. Mais toutes les interfaces, sauf pkt-q5, sont utilisées par la QS dynamique. Le Tableau 1 identifie brièvement chaque interface et montre comment chaque interface est utilisée dans cette spécification de QS dynamique (DQS, *dynamic QoS specification*).

Tableau 1/J.163 – Interfaces de la QS dynamique

Interface	Description	QS dynamique de MTA intégré (option)
pkt-q1	MTA-CM	Interface de service de commande MAC d'adaptateur E-MTA
pkt-q2	CM-CMTS	QS DOCSIS, initialisée par le CM
pkt-q3	MTA-GC/CMS	NCS
pkt-q4	Serveur d'appro de CM	N/A
pkt-q5	GC-CMTS	Gestion de porte
pkt-q6	CMTS-RKS	Facturation
pkt-q7	CMS-CMS	Signalisation de CMS à CMS

pkt-q1: interface entre MTA et câblo-modem

Cette interface est uniquement définie pour le MTA intégré. L'interface se décompose en trois sous-interfaces:

- contrôle: utilisé pour gérer les flux de service DOCSIS et leurs paramètres de trafic de QS et règles de classement associées;
- synchronisation: utilisée pour synchroniser la mise en paquets et la programmation pour réduire le retard et la gigue;
- transport: utilisé pour traiter les paquets dans le flux de média et effectuer le traitement approprié de la QS par paquet.

Le concept de cette interface est défini dans la Rec. UIT-T J.112. Pour les MTA autonomes, aucune instance de cette interface n'est définie.

pkt-q2: interface de QS DOCSIS entre câblo-modem et système CMTS

Il s'agit de l'interface de QS DOCSIS (contrôle, programmation et transport). Les fonctions de contrôle peuvent être initialisées depuis le câblo-modem ou le système CMTS. Toutefois, le système CMTS est l'arbitre final de la politique et l'entité finale qui accorde les ressources en effectuant le contrôle d'admission pour le réseau DOCSIS. Cette interface est définie dans la Rec. UIT-T J.112.

pkt-q3: signalisation de la couche Application entre le GC/CMS et le MTA

De nombreux paramètres sont signalés à travers cette interface, tels que le flux de média, les adresses IP, les numéros de port et la sélection des caractéristiques du codec et de la mise en paquets. DCS et NCS sont deux exemples de signalisation de la couche Application.

pkt-q4: signalisation de l'approvisionnement DOCSIS/IPCablecom au câblo-modem

Cette interface n'est pas utilisée pour la signalisation de QS dans la QS dynamique.

pkt-q5: interface entre le GC/CMS et le système CMTS

Cette interface est utilisée pour gérer les portes dynamiques pour les sessions de flux de média. Cette interface permet au réseau IPCablecom de demander et autoriser la QS.

pkt-q6: CMTS vers serveur d'archivage (RKS)

Cette interface est utilisée par le système CMTS pour signaler au RKS toutes les modifications intervenues dans l'autorisation et l'utilisation de la session.

pkt-q7: interface CMS vers CMS

Cette interface est utilisée pour la gestion de session et la coordination des ressources entre une paire de serveurs CMS.

5.5 Cadre pour la QS d'IPCablecom

Afin de justifier son coût pour l'utilisateur final, un service multimédia commercial (par exemple, la capacité de communications vocales) peut nécessiter un niveau élevé de performance de transport et de signalisation, y compris:

- faible délai: le délai de bout en bout du paquet doit être suffisamment faible pour ne pas interférer avec les interactions multimédias normales. Pour le service normal de téléphonie utilisant le RTPC, l'UIT-T recommande un temps de transmission aller-retour inférieur ou égal à 300 ms[1]. Etant donné que le temps de propagation du cœur de réseau peut absorber une quantité significative de ce capital de délai, il est important de contrôler le délai sur le canal d'accès, au moins pour les appels longue distance;
- faible perte de paquet: il est nécessaire que la perte de paquets soit la plus faible possible pour que la qualité de la voix ou les performances des modems des télécopieurs et de bande vocale ne soit pas perturbées de façon perceptible. Alors que des algorithmes de masquage des pertes peuvent être utilisés pour reproduire une parole intelligible même avec des pertes élevées, les performances résultantes ne peuvent pas être considérées comme adaptées pour se substituer au service téléphonique à commutation de circuits existant. Les prescriptions de perte pour une performance de modem à bande vocale acceptable sont mêmes plus strictes que celles relatives à la voix;
- court délai d'attente après la numérotation: il est nécessaire que le délai entre le moment où l'utilisateur signale une demande de connexion et la réception d'une confirmation positive du réseau soit suffisamment court pour que les utilisateurs ne perçoivent pas de différence avec le délai après numérotation auquel ils sont habitués dans le réseau à commutation de circuits. Ce délai doit être de l'ordre d'une seconde;
- court délai après la prise d'appel: il est nécessaire que le délai entre le moment où un utilisateur prend l'appel sur un téléphone qui sonne et celui où le canal vocal se fraie un chemin soit suffisamment court pour que le "Allô" ne soit pas tronqué. Il convient donc que ce délai soit inférieur à quelques millisecondes (de façon idéale moins de 100 ms).

Une contribution fondamentale du cadre de la QS dynamique est la reconnaissance de la nécessité d'une coordination entre la signalisation, qui contrôle l'accès aux services spécifiques de l'application, et la gestion des ressources, qui contrôle l'accès aux ressources de la couche Réseau. Cette coordination fournit un certain nombre de fonctions cruciales. Elle garantit que les utilisateurs sont authentifiés et autorisés avant de recevoir l'accès à la QS améliorée associée au service. Elle garantit que les ressources du réseau sont disponibles de bout en bout avant d'avertir le MTA de destination. Finalement, elle garantit que l'utilisation de ressources est correctement prise en compte, de manière cohérente avec les conventions du service téléphonique de qualité vocale traditionnel (auxquelles certains services IPCablecom sont similaires en se plaçant dans une perspective client) dans lequel la facturation n'intervient que lorsque le correspondant recevant la communication a décroché.

---

[1] La Rec. UIT-T G.114 établit qu'un délai dans un sens de 150 ms est acceptable pour la plupart des applications d'utilisateur. Toutefois, des applications hautement interactives de voix et données peuvent subir une dégradation même lorsque les délais sont au-dessous de 150 ms. Par conséquent, toute augmentation dans le traitement du délai (même sur les connexions avec des temps de transmission bien au-dessous de 150 ms) devrait être découragée à moins qu'il existe des avantages clairs au niveau du service et des applications.

Afin de prendre en charge les exigences ci-dessus, les protocoles de QS assurent que toutes les ressources sont engagées pour tous les segments du transport avant que les protocoles de signalisation n'avertissent la destination. De même, lorsqu'il est mis fin à une session, les protocoles de QS incluent des mesures pour assurer que toutes les ressources dédiées exclusivement à la session sont libérées. Sans cette coordination entre les deux sens des flux de données, il serait possible aux utilisateurs de déjouer les contrôles de QS et d'obtenir un service gratuit. Par exemple, si le client qui paie termine la session, mais non celui qui ne paie pas, une "demi-voie" subsiste, qui peut être utilisée pour transférer frauduleusement des données dans un sens. Les protocoles de QS adoucissent les sémantiques de transaction "tout ou rien" pour la création et la destruction de sessions.

Il est souhaitable que les mécanismes utilisés pour implémenter la session reposent sur les normes et pratiques existantes et aussi que les résultats de ce travail soient utilisables pour prendre en charge d'autres modèles d'appel. Ces souhaits ont conduit à l'utilisation du protocole en temps réel (RTP, *real time protocol*) de l'IETF pour acheminer des données multimédia, transportées sur le protocole datagramme d'utilisateur (UDP, *user datagram protocol*) de l'IETF. La signalisation intrabande pour établir la qualité de service est transportée en utilisant des messages de QS dynamique DOCSIS.

L'architecture de la QS devrait fournir la prise en charge des nouvelles applications émergeantes qui sont dépendantes de la livraison de données multidiffusion. Bien qu'il ne s'agisse pas d'une exigence stricte dans l'architecture de la QS, la prise en charge de la multidiffusion permettra le développement ultérieur d'un ensemble riche d'applications multimédia. La question de savoir si les améliorations apportées à la gestion des ressources présentées ici prendront ou non en charge la multidiffusion de façon transparente n'a pas encore été examinée.

Pour les besoins de gestion de la qualité de service, le canal porteur pour une session est géré comme s'il existait trois segments distincts: le réseau d'accès côté départ de la session, un cœur de réseau et le réseau d'accès côté arrivée de la session. Les ressources de réseau DOCSIS sont gérées, en tant que paire de flux de service dynamique, en utilisant les mécanismes définis dans la Rec. UIT-T J.112. Les ressources du cœur de réseau peuvent être gérées soit au flux soit, plus vraisemblablement, par un mécanisme de qualité de service agrégé. La gestion des ressources du cœur de réseau est en dehors du domaine d'application de la présente Recommandation.

Une structure définie par la QS appelée *porte* fournit un point de contrôle pour la connexion des réseaux d'accès à un service de cœur de réseau de haute qualité. Une porte est implémentée par un système CMTS et se compose d'un classeur de paquets, d'un régulateur de trafic et d'une interface avec une entité qui collecte les données statistiques et les événements (tous ces composants existent dans le réseau DOCSIS). Une porte permet de garantir que seules les sessions qui ont été autorisées par le fournisseur de service reçoivent le service de haute qualité. Les portes sont gérées sélectivement pour un flux. Pour le service de communications vocales fondé sur IPCablecom, elles sont ouvertes pour les appels individuels. L'ouverture d'une porte implique qu'un contrôle d'admission soit effectué lorsqu'une demande de gestion de ressources est reçue du client pour une session individuelle et peut impliquer au besoin la réservation de ressources dans le réseau pour la session. Le filtre de paquets amont dans la porte permet à un flux de paquets de recevoir une QS améliorée pour une session de la part d'une adresse IP de source et d'un numéro de port spécifiques vers une adresse IP de destination et un numéro de port spécifiques. Le filtre de paquets aval sur la porte permet à flux de paquets de recevoir une QS améliorée pour une session de la part d'une adresse IP de source spécifique vers une adresse IP de destination et un numéro de port spécifiques.

Une porte est une entité logique qui réside dans un système CMTS. Un Identifiant de porte (*GateID*) est associé à une session individuelle et est significatif au niveau de la porte; le GateID est un identifiant qui est localement unique au niveau du système CMTS et qui est alloué par ce CMTS. Une porte est par nature unidirectionnelle. Si une porte est "fermée", les données dans le sens amont/aval sur le réseau d'accès DOCSIS peuvent être éliminées ou fournies "au mieux" (*best-effort*

service). Le choix d'éliminer des paquets ou de les desservir "au mieux" est un choix qui relève de la politique du fournisseur.

Le contrôleur de porte est chargé de la décision de politique fixant quand la porte doit ou non être ouverte et si elle doit l'être. Une porte est établie avant une demande de gestion de ressources. Ceci permet à la fonction politique, qui se situe au niveau du contrôleur de porte, d'être "sans état" en ce qu'elle n'a pas besoin de connaître l'état des sessions qui sont déjà en cours.

Alors que la porte contrôle le flux garanti en QS, d'autres flux, tels que les messages du RTCP ou les messages de signalisation, ne sont pas régulés par la porte. La prise en charge de la QS améliorée pour les messages de signalisation peut jouer un rôle très important si le système câblé utilise le trafic de données au mieux. Afin de satisfaire aux objectifs de performance de signalisation donnés au début du présent paragraphe, il peut être crucial d'utiliser un flux de signalisation dédié avec des schémas de QS appropriés. Il convient de plus de noter que la nature exacte de la QS qui devrait être donnée au flux de signalisation dédié dépend du trafic et de la conception du système CMTS et elle reste un point de différentiation entre les fournisseurs.

5.6 Exigences pour la gestion de ressources des réseaux d'accès

La fourniture de service de communications vocales sur des réseaux IP avec le même niveau de qualité que celui disponible sur le RTPC impose des limites sur les paramètres de perte et de retard de transmission pour les paquets vocaux et implique une gestion des ressources active dans les réseaux d'accès et les cœurs de réseau. Il est nécessaire que le fournisseur de services puisse contrôler l'accès aux ressources du réseau, afin d'assurer la disponibilité d'une capacité adéquate de bout en bout, même en cas de surcharge ou de conditions inhabituelles. Le fournisseur de services peut chercher à obtenir des revenus supplémentaires pour la fourniture d'un service de service de communications vocales avec ces caractéristiques de qualité améliorée (c'est-à-dire, qualité dépassant celle obtenue selon le service "au mieux"). Les mécanismes fournis ici pour l'accès géré à une QS améliorée permettent au fournisseur de services de s'assurer que l'accès est fourni uniquement à des utilisateurs autorisés et authentifiés sur une base session par session et qu'il n'y a pas de vol de ce service.

Les clients du service signalent leurs paramètres de trafic et de performances à la "porte" à l'extrémité du réseau, où le réseau effectue une décision de contrôle d'admission fondée sur la disponibilité des ressources et sur les informations de politique associées à la porte.

Dans les réseaux DOCSIS, la capacité des réseaux est limitée et il est nécessaire d'effectuer la gestion des ressources sur une base flux par flux. Dans le cœur de réseau, plusieurs alternatives sont possibles, allant du contrôle d'admission par flux et par saut à la fourniture de ressources en vrac. La présente Recommandation ne traite que de la QS des réseaux d'accès et ignore les schémas de QS des cœurs de réseau.

5.6.1 Empêcher le vol de service

Les ressources réseau dédiées à la session sont protégées contre l'utilisation abusive, notamment:

- autorisation et sécurité: garantissant que les utilisateurs sont authentifiés et autorisés avant de recevoir l'accès à la QS améliorée associée au service de communications vocales. Le CMS/GC impliqué dans la signalisation d'appel est habilité à effectuer ces contrôles et est la seule entité habilitée à créer une nouvelle porte dans un CMTS. Le CMS/GC agit comme point de décision de politique dans la perspective de la gestion de la QS;
- contrôle de ressources: garantissant que l'utilisation de ressources est correctement prise en compte, en cohérence avec les conventions des fournisseurs qui font partie du RTPC dans lequel la facturation n'a lieu que lorsque l'appelé a décroché. Ceci inclut la prévention de l'utilisation de ressources réservées pour des besoins autres que la session à laquelle elles sont allouées. Le contrôle de ressources est obtenu grâce à l'utilisation de portes et à la

coordination entre les portes, qui relient ensemble les mécanismes de filtrage d'adresse avec les réservations de ressources.

Etant donné que ce service peut être facturé sur la base de l'utilisation, il existe un risque important de fraude ou de vol de service. L'architecture permet au fournisseur de facturer la qualité de service. Cette pratique évite ainsi les scénarios de vol de service, dont plusieurs sont décrits à l'Appendice IX.

Les scénarios de vol de service sont traités dans la présente Recommandation et dans d'autres Recommandations. Ils motivent certaines des architectures et des protocoles de QS et de signalisation d'appel.

5.6.2 Engagement de ressources à deux phases

Un protocole à deux phases pour l'engagement de ressources est essentiel pour un service de niveau commercial de communications vocales, pour deux raisons propres aux exigences d'un tel service. Tout d'abord, il garantit que les ressources sont disponibles avant de signaler à la partie située à l'extrémité distante qu'une communication est entrante. Deuxièmement, il garantit que l'enregistrement de l'utilisation et la facturation ne sont pas lancés avant que l'extrémité distante ne décroche, moment également où la voix peut se frayer un chemin. Ces propriétés sont fournies par les protocoles conventionnels de signalisation de téléphonie; la même sémantique sera émulée ici. Par ailleurs, si la largeur de bande est allouée avant que l'extrémité distante ne décroche, un vol de service devient possible. Le fait de demander que les points d'extrémité envoient explicitement un message d'engagement garantit que l'enregistrement de l'utilisation repose sur la connaissance du point d'extrémité et de son action explicite.

Ce cadre prend en charge également les entités telles que les serveurs d'annonce et les passerelles RTPC, qui ont besoin que la voix se fraye le passage après la première phase du protocole de gestion des ressources.

5.6.3 Allocation segmentée des ressources

L'architecture de la QS dynamique sépare la gestion des ressources en segments distincts pour le réseau d'accès et pour le cœur de réseau. L'allocation de ressources segmentée est avantageuse à double titre:

- elle permet différents mécanismes de fourniture de bande passante et de signalisation pour le réseau du demandeur, le réseau de l'extrémité distante et le cœur de réseau;
- elle permet aux segments pauvres en ressources de maintenir des réservations flux par flux et de gérer soigneusement l'utilisation des ressources. En même temps lorsque les segments du cœur de réseau ont suffisamment de ressources pour gérer les ressources plus grossièrement, elle permet au cœur de réseau d'éviter de conserver un état par flux et d'améliorer ainsi l'évolutivité.

Lorsque le cœur de réseau ne requiert pas une signalisation par flux explicite (comme avec un cœur de réseau Diffserv), elle réduit le temps pris pour établir une session (réduction du délai après numérotation) et évite d'affecter le temps de traversée de la voix (réduction du délai après prise d'appel).

Elle réduit potentiellement la valeur de l'état de réservation à stocker si le client distant est une passerelle RTPC.

Après la première phase de la signalisation d'appel, les deux clients ont réalisé la négociation de capacités et savent quelles sont les ressources nécessaires de bout en bout. Les clients envoient des messages de gestion des ressources en utilisant l'interface des services de contrôle MAC. Le système CMTS transpose les messages de gestion des ressources dans le protocole de gestion des ressources utilisé sur le cœur de réseau (par exemple, DiffServ de l'IETF). Il transpose également le

message de gestion des ressources dans le protocole de gestion des ressources utilisé sur la liaison d'accès (c'est-à-dire DOCSIS).

5.6.4 Changements de ressources pendant une session

Il est possible de changer les ressources allouées pour une session pendant la durée de vie de cette session. Cela facilite les changements à mi-session tels que le passage d'un codec vocal bas débit à un codec G.711 lorsque des tonalités de modem sont détectées et l'adjonction de données vidéo à une session qui commence en vocal seul.

5.6.5 Association dynamique de ressources

L'association dynamique de ressources ("re-réservation") est une exigence pour permettre l'utilisation efficace des ressources lorsque des services tels que la mise en instance d'appel sont invoqués. De façon abstraite, la re-réservation prend la bande passante allouée à une session entre un hôte VoIP et un client et réaffecte cette même bande passante à une session avec un client différent.

Il est important de comprendre le danger potentiel d'enlever l'allocation de bande passante de la session, puis d'effectuer une nouvelle demande pour l'allocation de la nouvelle bande passante. Il existe un risque qu'un autre client utilise la dernière bande passante restante entre les deux étapes, laissant la session d'origine sans un chemin de qualité assuré. Le mécanisme de re-réservation en une étape évite cet inconvénient, dans la mesure où la bande passante n'est pas mise à la disposition d'autres clients.

5.6.6 Performances de QS dynamique

La transmission de message de QS a lieu en temps réel alors que les appelants attendent que les services soient activés ou changés. Il faut donc que le protocole soit rapide. Le nombre de messages est réduit, en particulier le nombre de messages qui transitent par le cœur de réseau et le nombre de messages DOCSIS amont.

Les messages de gestion DOCSIS et les messages de signalisation d'appel (désignés collectivement comme messages de signalisation) sont tous transportés "au mieux" sur le réseau DOCSIS. Si le câblo-modem prend également en charge des services de données, le service "au mieux" peut être incapable de fournir le faible temps d'attente nécessaire pour les messages de signalisation. Dans cette situation, le câblo-modem PEUT être approvisionné avec un flux de service séparé, avec une QS améliorée, pour porter du trafic de signalisation. Par exemple, le flux de service de signalisation pourrait utiliser le service d'interrogation en temps réel ou en temps différé. Ce flux de service séparé est provisionné de la même manière que les autres flux de média DOCSIS et PEUT inclure des classeurs tels que sa présence soit transparente au MTA.

5.6.7 Classe de session

Des ressources peuvent être réservées pour différents types of service et chaque service peut à son tour définir différentes classes de service pour ses sessions. Les réservations de QS pour les sessions que le fournisseur de services a conçu comme ayant une priorité supérieure (par exemple appels d'urgence) connaissent une probabilité de blocage inférieure à celle des sessions normales. La détermination de la classe à allouer à une session est effectuée par le fournisseur de services. C'est une politique qui est exercée par le complexe agent d'appel/contrôleur de porte d'origine au moment où la demande de session initiale est effectuée.

5.6.8 Prise en charge du réseau intermédiaire

L'architecture ne devrait pas interdire les réseaux intermédiaires entre le MTA ou l'hôte multimédia et le câblo-modem (par exemple, réseau du client). Bien que le réseau intermédiaire puisse ne pas tomber dans le domaine ou la responsabilité administrative de l'opérateur de câble, l'allocation de bande passante dans le réseau DOCSIS de l'opérateur de câble est possible lorsqu'existe un réseau

intermédiaire. Il est également souhaitable de présenter une solution qui tienne compte de façon transparente de la réservation de ressources sur le réseau intermédiaire.

5.6.9 Prise en charge de la QS sur le cœur de réseau

Il est possible qu'un mécanisme permettant de gérer explicitement les ressources du cœur de réseau soit nécessaire. Le domaine d'application de la présente Recommandation est la QS sur le réseau DOCSIS, mais l'architecture fournit des interfaces ouvertes, suffisamment générales, qui sont compatibles avec de nombreux mécanismes de QS connus sur les cœurs de réseau.

5.6.10 Traitement de codecs multiples

La signalisation NCS utilisée avec IPCablecom permet d'établir des connexions avec des codecs multiples. Dans le cas où une connexion avec plusieurs des codecs de la liste a été négociée avec succès, il est important que les ressources appropriées soient allouées pour faire que les changements de codec en résultant dans la liste négociée s'effectuent comme prévu. Toutefois, il appartient au serveur CMS de déterminer le moment où il autorisera la largeur de bande durant la phase d'établissement de l'appel, et de décider du degré d'efficacité dont il entend faire montre dans son enveloppe autorisée. S'il choisit d'autoriser la largeur de bande avant la commande CRCX (*createconnection*) de signalisation NCS initiale, il devra déterminer l'enveloppe autorisée en fonction des paramètres LCO proposés (ne sachant pas quel sous-ensemble l'adaptateur MTA pourra négocier). Si le serveur CMS reste dans la phase d'établissement d'appel en attendant que les codecs aient été renégociés, il pourrait autoriser un sous-ensemble des paramètres LCO en fonction de la liste négociée actuelle sans que cela n'ait aucune incidence négative (le signal DSA/DSC continuera de transmettre l'autorisation). Les composants de ressources qui doivent être alloués sont donnés ci-dessous:

– largeur de bande autorisée: lorsque le serveur CMS demande à l'adaptateur MTA de réserver ou d'engager des ressources en incluant un Identifiant de porte (*GateID*) dans une commande CRCX (*createconnection*) ou MDCX (*modifyconnection*) de signalisation NCS, le serveur CMS DOIT faire en sorte que la largeur de bande autorisée de la porte traitera toute demande de ressources légale (DSA/DSC) adressée par l'adaptateur MTA au système CMTS et découlant de la procédure de négociation de codecs. En d'autres termes, la largeur de bande autorisée par le CMS/GC DOIT être supérieure ou égale à la limite supérieure minimale de la liste de codecs négociée;

– largeur de bande réservée: le MTA DOIT réserver la limite supérieure minimale de la bande passante des codecs pouvant être utilisés pendant l'appel (les codecs possibles sont déterminés par la procédure de négociation de codecs définie au § 6.7/J.162).

  NOTE – Si la bande réservée est supérieure à la bande engagée, elle doit alors être réajustée par un signal DSC envoyé au CMTS.

– largeur de bande engagée: le MTA ne DOIT engager que le codec actuel utilisé dans la direction amont. Ceci permet d'utiliser le reliquat inutilisé de la largeur de bande (la différence entre la bande réservée et la bande engagée) pour le trafic non garanti. Dans la direction aval, le MTA DOIT engager la limite supérieure minimale de largeur de bande de codec pouvant être utilisée pendant l'appel (les codecs possibles sont déterminés par la procédure de négociation de codecs définie au § 6.7/J.162).

Cette procédure garantit qu'une demande d'un CMS de passer sur un des codecs de la liste négociée réussira. C'est particulièrement important pour la prise en charge de dispositifs tels que fax/modem qui nécessitent de passer sur G.711 pour le succès de la transmission.

Si un fournisseur de système estime que l'allocation de ressources ci-dessus est trop contraignante pour le nombre de canaux vocaux qui peuvent être pris en charge (dans la mesure où la surréservation de ressources peut être fréquente), le serveur CMS a alors seulement besoin de déclarer un seul codec dans le champ LocalConnectionOptions de la demande de connexion. Ceci

garantira que les ressources réservées et engagées sont égales (en utilisant le même mécanisme que défini dans le cas du codec multiple). Ensuite, si le CMS veut commuter les codecs il devra placer le nouveau codec dans le champ LocalConnectionOptions d'un changement de connexion ultérieur. Cependant, cette approche présente certains risques. Par exemple, lorsqu'un appel de modem est détecté et rapporté au serveur CMS, il serait possible que la modification de connexion résultante pour utiliser G.711 échoue du fait de ressources insuffisantes sur le système CMTS. Cela ne sera pas le cas si des codecs multiples étaient définis car les limites inférieure/supérieure auraient d'ores et déjà été réservées et leur accessibilité garanties pour un engagement ultérieur.

5.6.11 Appels de port à port sur un adaptateur MTA

Lorsque des appels vocaux sont établis entre différents ports (points de terminaison) sur le même MTA, les règles de transmission DOCSIS spécifient que le câblo-modem ne doit pas transmettre de paquets sur le réseau DOCSIS. Il en résulte que les actions entreprises par le serveur CMS et l'adaptateur MTA dans ces circonstances particulières sont différentes du flux d'appel classique de MTA à MTA. L'appel de port à port est défini par le fait que les deux points de terminaison utilisent la même adresse IP.

Si un MTA reçoit une demande de connexion sans Identifiant de porte (*GateID*), il NE DOIT PAS initialiser de message DSx vers le système CMTS. Si un adaptateur MTA reçoit pour instruction de faire un appel de port à port, le MTA NE DOIT PAS initialiser de message DSx pour établir un flux de service pour cette connexion et NE DOIT PAS envoyer de paquets vocaux sur le réseau. De plus, si l'adaptateur MTA avait précédemment créé un flux de service pour un appel dont le SDP d'extrémité distante n'était pas disponible (mais qu'un GateID était spécifié dans un CRCX ou MDCX), il DOIT alors interrompre le flux de service si un appel de port à port est ensuite reconnu une fois que le SDP distant est reçu.

Le serveur CMS DEVRAIT reconnaître les appels de port à port, DEVRAIT omettre la commande de porte vers le système CMTS, et DEVRAIT omettre l'Identifiant de porte dans la commande de connexion à l'adaptateur MTA. Comme dans le cas de l'adaptateur MTA ci-dessus, si le serveur CMS a déjà établi une porte pour un appel dont le SDP distant n'est pas disponible, il DEVRAIT s'attendre à un message Porte fermée de la part du système CMTS une fois que l'adaptateur MTA interrompt le flux de service lorsqu'il détecte l'appel de port à port. Le CMS NE DOIT PAS interrompre un appel entre points d'extrémité ayant la même adresse IP à réception d'un message PORTE FERMEE.

5.6.12 Plusieurs allocations par intervalle

Pour utiliser de manière efficace les ressources DOCSIS, l'adaptateur MTA PEUT choisir de mettre plusieurs sous-flux ayant les mêmes ensembles de paramètres de QS sur le même flux de service. Etant donné que le type de programmation de flux de service ServiceFlowScheduling fait partie de l'ensemble de paramètres de QS, il DOIT être commun à tous les sous-flux qui utilisent le même flux de service DOCSIS. Par exemple, si un flux prenant en charge la suppression de silence utilise une programmation de flux de service de type UGS/AD, et que le flux de service existant soit configuré uniquement pour la programmation de type UGS, le nouveau flux DOIT être créé sur un flux de service séparé. Pour faciliter l'implémentation, en cas d'utilisation de plusieurs allocations par intervalle, le type de programmation du flux de service existant ne peut pas être modifié.

La prise en charge de cette fonctionnalité par le MTA est facultative. Le CMTS DOIT prendre en charge un nombre d'allocations par intervalle supérieur à 1. Si un MTA demande plusieurs allocations par intervalle et que le message DSx soit rejeté par le CMTS (le programmateur du CMTS ne pouvant programmer de façon appropriée cette demande sur le flux de service existant, tout en étant éventuellement en mesure de satisfaire à cette demande sur un flux de service séparé), le MTA PEUT essayer une nouvelle fois d'utiliser un flux de service séparé pour la demande (si les ressources le permettent).

Le champ allocations actives par intervalle de l'en-tête MAC étendu est utilisé pour enregistrer les allocations actives sur un flux de service donné qui contient plusieurs sous-flux. Par exemple, si vous avez deux appels actifs et que l'un passe à l'état suppression de silence, le nombre d'allocations actives dans l'en-tête MAC étendu est réduit de 2 à 1. Dans ce scénario, aucun rafraîchissement du signal DSC n'est nécessaire sur le flux, car la détection de l'activité se fait en fonction du flux et non pas de l'allocation. Le nombre d'allocations par intervalle dans le signal DSC reste égale à 2 pour les paramètres Admis et Actif et le rafraîchissement du flux ne sera nécessaire que lorsque le nombre d'allocations actives passera à 0 et que tous les sous-flux passeront à l'état suppression de silence. Le nombre d'allocations actives par intervalle DOIT être inférieur ou égal au nombre de sous-flux.

Les règles de suppression d'en-tête de charge utile (PHS) applicables à tous les sous-flux d'un flux de service DOIVENT être les mêmes.

5.7 Théorie de fonctionnement

5.7.1 Etablissement de la session de base

La réservation de ressources est divisée en deux phases réservation (*Reserve*) et engagement (*Commit*) séparées. (Sur les liaisons DOCSIS, les flux de service dans chaque sens sont admis.) A la fin de la première phase, les ressources sont réservées mais ne sont pas encore disponibles au niveau du MTA. A la fin de la seconde phase, les ressources sont rendues disponibles au niveau du MTA et l'enregistrement de l'utilisation est lancé pour que l'utilisateur puisse être facturé pour l'utilisation. (Sur les liaisons DOCSIS, les flux de service sont actifs.)

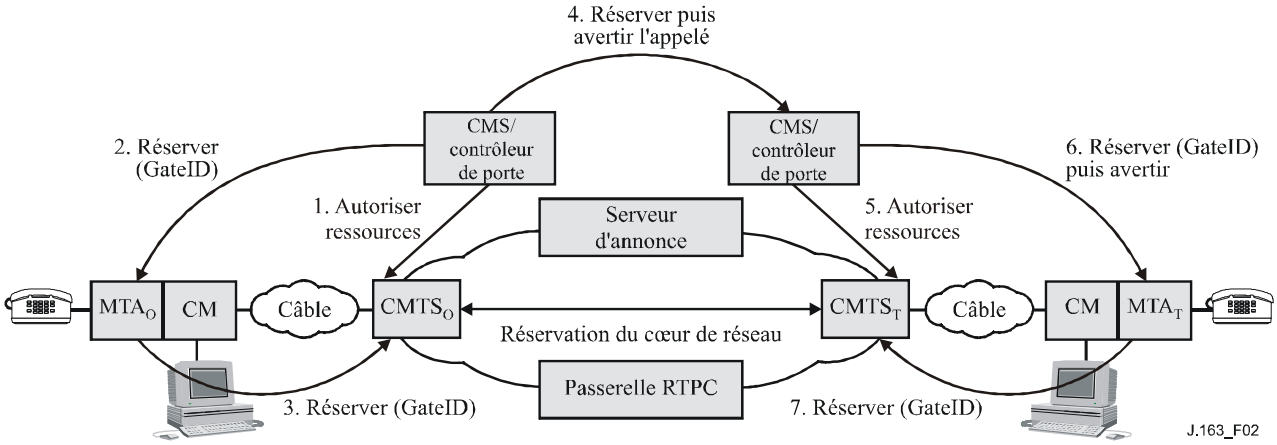


Figure 2/J.163 – Phase 1 de la gestion de ressources

La Figure 2 représente la première phase du protocole de gestion des ressources pour un appel. Dans cette description, les indices "O" et "T" désignent les points d'origine et d'arrivée de l'appel représentés sur la Figure 2; les MTA_O et MTA_T demandent la réservation de ressources. (Signalisation de services dynamiques DOCSIS pour clients intégrés) respectivement au $CMTS_O$ et au $CMTS_T$. Le $CMTS_O$ et le $CMTS_T$ effectuent une vérification de contrôle d'admission pour la disponibilité des ressources (en initialisant au besoin la signalisation pour la réservation de ressources dans le cœur de réseau) et envoient une réponse aux MTA respectifs qui, à leur tour, répondent au serveur CMS.

La Figure 3 représente la seconde phase. Après avoir déterminé la disponibilité des ressources, le CMS envoie un message au MTA_T en lui donnant l'instruction de commencer à faire sonner le téléphone. Lorsque l'appelé décroche son téléphone, le MTA_T envoie un message au CMS, lequel donne instruction au MTA_O et au MTA_T de demander un engagement de ressources. L'arrivée des messages COMMIT au niveau du $CMTS_T$ et du $CMTS_O$ les amène à ouvrir leur porte et démarre également la comptabilité relative à l'utilisation des ressources. Pour empêcher un scénario de vol

de service, les CMTS coordonnent l'ouverture des portes en échangeant des messages GATE-OPEN (*Porte ouverte*).

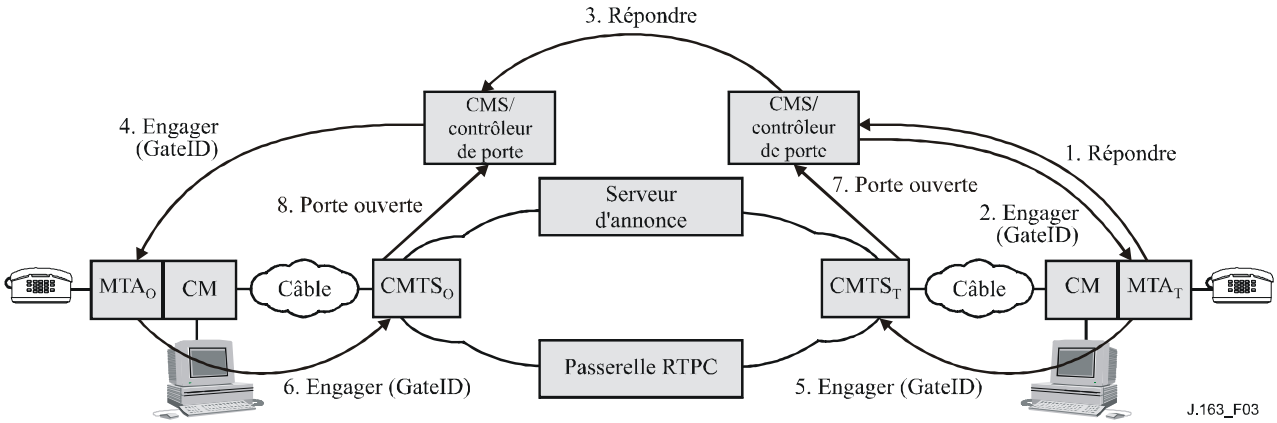


Figure 3/J.163 – Phase 2 de la gestion des ressources

5.7.2 Coordination des portes

La signalisation de la QS amène la création d'une porte au niveau de chaque CMTS associé à un client impliqué dans la session. Chaque porte maintient les données d'utilisation pour la session et contrôle si les paquets générés par le client associé reçoivent l'accès à une QS améliorée. La coordination des portes est nécessaire pour empêcher la fraude et le vol de service dans des situations où un client en dérangement ou modifié n'envoie pas les messages de signalisation attendus. Il est essentiel que les mécanismes du protocole résistent aux abus[2]. Un protocole de coordination de porte garantit les points suivants:

- éviter la possibilité d'établir une session unidirectionnelle sans facturation. Parce que les clients peuvent avoir l'intelligence adéquate et ne sont pas de confiance, il est envisageable que des clients établissent deux sessions unidirectionnelles pour fournir aux utilisateurs un canal de communication vocale interactif adapté. La coordination des portes empêche que de telles sessions soient établies sans que le fournisseur puisse les facturer;
- l'ouverture et la fermeture des portes sont étroitement synchronisées avec les changements d'état correspondants au serveur CMS.

5.7.3 Changement des classeurs de paquets associés à une porte

Une fois qu'une paire de portes est établie, les clients peuvent communiquer sur le réseau avec une QS améliorée. Plusieurs fonctions nécessaires à un service commercial de communications vocales supposent le changement des clients impliqués dans une session, par exemple lorsqu'une session est transférée ou réacheminée ou pendant une conférence à trois. Ceci nécessite que les classeurs de paquets associés à une porte soient modifiés pour refléter l'adresse du nouveau client. De plus, le fait de changer les extrémités impliquées dans une session peut affecter le mode de facturation de la session. Il en résulte que les portes incluent les informations d'adressage pour les points de départ et d'arrivée.

5.7.4 Ressources d'une session

La relation entre les différentes catégories de ressources, autorisées, réservées et engagées, est représentée à la Figure 4. Un ensemble de ressources est représenté par un espace à *n* dimensions (représenté ici comme un espace à deux dimensions) où *n* est le nombre de paramètres (par exemple, bande passante, taille des rafales, gigue, classeurs) nécessaires pour décrire les ressources.

---

2 Plusieurs scénarios de vol de service sont décrits à l'Appendice IX.

Les procédures exactes pour comparer les vecteurs de ressources à *n* dimensions sont données dans la Rec. UIT-T J.112.

Lorsqu'une session est d'abord établie, les protocoles de QS dynamique autorisent l'utilisation d'une certaine quantité maximale de ressources indiquée par la ligne ovale extérieure, spécifiant les ressources autorisées. Lorsqu'un client effectue une réservation pour une session, il réserve une certaine quantité de ressources, qui ne sont pas supérieures à celles pour lesquelles il a été autorisé. Lorsque la session est prête à fonctionner, le client engage une certaine quantité de ressources qui ne sont pas supérieures aux ressources réservées. Dans de nombreux cas communs, les ressources engagées et réservées seront égales. Les ressources engagées représentent les ressources qui sont en cours d'utilisation par la session active, tandis que les ressources réservées représentent celles qui sont immobilisées par le client et qui sont retirées du pool pour les besoins du contrôle d'admission, mais qui ne sont pas nécessairement utilisées par le client.

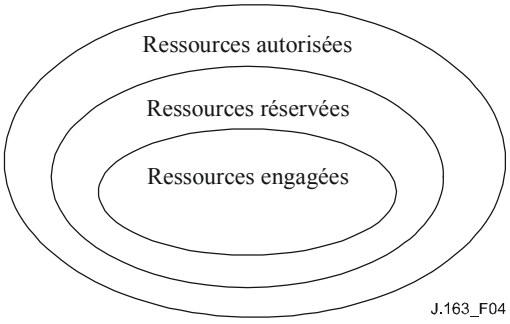


Figure 4/J.163 – Ressources autorisées, réservées et engagées

Les autorisations n'affectent que les demandes futures de réservation de ressources. Les ressources qui ont été réservées avant un changement d'autorisation ne sont pas affectées.

Les ressources qui ont été réservées mais non engagées sont à la disposition du système uniquement pour des utilisations à court terme, telle que le traitement de données "au mieux". Ces ressources ne sont pas disponibles pour d'autres réservations (c'est-à-dire la surréservation n'est pas permise). La portion maximale de ressources disponibles qui peuvent être réservées immédiatement relève d'une décision de politique du système CMTS et sort du domaine d'application de la QS dynamique.

Les ressources excédentaires, réservées au-delà de celles engagées, sont libérées à moins que le client ne demande explicitement qu'elles soient conservées par l'intermédiaire d'opérations périodiques de mise à jour de la réservation. Le maintien de cette condition est déconseillé sur de longues périodes, car elle réduit la capacité globale du système. Il existe toutefois des situations (par exemple, service de mise en instance, où l'appel en attente exige des ressources qui dépassent celles nécessaires pour l'appel actif) dans lesquelles des réservations excédentaires sont nécessaires.

5.7.5 Contrôle d'admission et classes de session

Il est envisagé que la porte au niveau du système CMTS puisse utiliser une ou plusieurs classes de session pour des ressources réservées depuis un MTA. Les classes de session définissent les politiques de contrôle d'admission fournies ou leurs paramètres. Il est prévu que le fournisseur indique les paramètres nécessaires et/ou les politiques de contrôle d'admission alternatives dans le système CMTS et dans le contrôleur de porte. Par exemple, une classe de session pour les communications vocales normales et une classe de session en chevauchement pour les appels d'urgence pourraient être définies pour permettre l'allocation de, respectivement, jusqu'à 50% et 70% des ressources totales à ces classes d'appels et laisser les 30 à 50% restants de la bande passante totale disponibles pour d'autres services, vraisemblablement de priorité inférieure. Les classes de session peuvent de plus permettre l'élimination de ressources déjà réservées, auquel cas la

politique pour cette élimination serait fournie par le fournisseur de services. Lorsque l'enveloppe autorisée est communiquée à la porte au niveau du système CMTS par le contrôleur de porte dans le message Gate-Set (*Porte établie*), le contrôleur de porte inclut les informations adéquates pour indiquer quelle classe de session devrait s'appliquer lorsque la demande DSA/DSC correspondante est traitée.

5.7.6 Renégociations des ressources

Plusieurs des caractéristiques de la session prises en charge nécessitent des renégociations des paramètres de QS associés à une session pendant la durée de vie de la session. Par exemple, des clients pourraient commencer à communiquer en utilisant un codec audio à faible débit binaire. Ils peuvent ensuite passer à un codec à débit binaire plus élevé ou ajouter un flux vidéo, tant que la QS demandée reste dans l'enveloppe autorisée et qu'il existe de la bande passante disponible sur le réseau. L'utilisation d'une enveloppe de QS autorisée, qui est préautorisée par le contrôleur de porte agissant comme point de décision de politique, confère aux clients la souplesse nécessaire pour renégocier la QS avec le réseau sans impliquer ultérieurement le contrôleur de porte. Ceci signifie principalement que l'utilisation de ressources jusqu'aux limites de l'enveloppe est préautorisée mais NON préréservée. Une allocation de ressources réussie dans l'enveloppe autorisée implique une décision de contrôle d'admission et n'est pas garantie. Après le contrôle d'admission, les ressources sont réservées pour le flux, bien que l'utilisation réelle des ressources ne soit permise qu'après l'achèvement de la phase Engagement du protocole de réservation de ressources. Toutefois, aucune décision de contrôle n'est nécessaire au moment de l'engagement des ressources. Chaque changement intervenant dans l'engagement des ressources dans les limites de la décision de contrôle d'admission ne nécessite pas de réservation ultérieure. Toutes les demandes de réservation qui franchissent le contrôle d'admission DOIVENT être conformes à l'enveloppe d'autorisation.

5.7.7 Association dynamique de ressources (*Re-reserve*)

L'architecture de QS dynamique reconnaît qu'il peut être nécessaire de partager des ressources sur plusieurs sessions, spécialement en cas de pénurie de ressources. Notamment, l'utilisation du dispositif de mise en instance dans les applications du type téléphonie peut impliquer le client dans deux sessions simultanées, mais ce dernier ne sera actif que dans une conversation à la fois. Il est faisable dans ce cas de partager les ressources de la couche Réseau (en particulier sur la liaison d'accès) entre les deux conversations. Par conséquent, cette architecture permet à un ensemble de ressources de la couche Réseau (telle qu'une réservation de bande passante) d'être explicitement identifié. Elle permet également à une ou plusieurs portes d'être associées à ces ressources. Les primitives de signalisation permettent aux ressources associées à une porte d'être *partagées* avec une autre porte au niveau du même système CMTS. Ceci améliore l'efficacité avec laquelle sont utilisées les ressources dans le réseau DOCSIS.

En passant d'une session à l'autre dans un scénario de mise en instance d'appel, un client a besoin de conserver suffisamment de ressources réservées pour prendre en charge l'une ou l'autre des sessions qui, en général, peuvent ne pas avoir besoin de la même quantité de ressources. Ainsi l'opération de rengagement peut changer les ressources engagées. Toutefois, les ressources réservées ne changent pas dans ce cas, étant donné que le client ne devrait pas avoir à passer par le contrôle d'admission lorsqu'il revient à l'autre session.

Alors que les ressources engagées sont toujours associées à la session active en cours (et son flux IP correspondant), les ressources réservées peuvent être associées à différents flux et à différentes portes à différents moments. Un outil, appelé Identifiant de ressources (*resource ID*), est utilisé pour identifier un ensemble de ressources réservées pour les besoins de l'association d'un flux à ces ressources.

5.7.8 Prise en charge de la facturation

La signalisation de la QS peut être utilisée pour prendre en charge une gamme étendue de modèles de facturation, reposant uniquement sur un flux d'enregistrements d'événements depuis le système CMTS. Etant donné que la porte se trouve sur le chemin des données et qu'elle participe aux interactions relatives à la gestion des ressources avec un client, la comptabilité de l'utilisation des ressources est effectuée par la porte. La porte dans le système CMTS est l'endroit approprié pour effectuer la comptabilité des ressources, étant donné que le système CMTS est directement impliqué dans la gestion des ressources fournies à un client. Il est également important d'effectuer la comptabilité de l'utilisation dans le système CMTS pour faire face aux défaillances des clients. Si un client qui est impliqué dans une session active tombe en panne, le système CMTS DOIT détecter cette défaillance et arrêter la comptabilité de l'utilisation pour la session. Ceci peut être effectué en surveillant le flux de paquets le long du trajet des données pour les applications à média continu ou par d'autres mécanismes (tels que la maintenance de la station) effectué par le système CMTS. De plus, étant donné que la porte retient l'état pour les flux qui ont été autorisés par un contrôleur de porte spécifique au service, il est utilisé pour conserver des informations spécifiques au service associées à la facturation, telles que le numéro de compte de l'abonné qui paiera pour la session. La fonction de politique dans le contrôleur de porte devient ainsi sans état.

La prise en charge requise dans le système CMTS consiste à générer et à transmettre un message d'événement à un serveur d'archivage pour tout changement à la QS, autorisé et spécifié par une porte. Des données opaques fournies par le contrôleur de porte, qui peuvent être utiles pour le serveur d'archivage, peuvent également être incluses dans le message. Les exigences pour le traitement des enregistrements d'événement sont contenues dans d'autres spécifications de la prise en charge des opérations.

5.7.9 Gestion des ressources du cœur de réseau

Lorsqu'un CMTS reçoit un message de réservation de ressources d'un MTA, il vérifie tout d'abord qu'une bande passante amont et aval adéquate est disponible sur le canal d'accès en utilisant les informations de programmation localement disponibles. Si ce contrôle est réussi, le système CMTS peut soit générer un nouveau message de réservation de ressources sur le cœur de réseau soit envoyer au cœur de réseau une version modifiée du message de réservation de ressources reçu du MTA. Le système CMTS effectue toute transposition spécifique de la technologie du cœur de réseau qui est nécessaire. Ceci permet à l'architecture de prendre en charge différentes technologies de cœur de réseau, au choix du fournisseur de services. Les mécanismes spécifiques de réservation de la QS sur le cœur de réseau sortent du domaine d'application de la présente Recommandation.

Un modèle bidirectionnel est utilisé pour la réservation de ressources dans un réseau DOCSIS où le routage est symétrique. Un modèle unidirectionnel est utilisé pour la réservation de ressources dans le cœur de réseau, ce qui permet des asymétries de routage. Par conséquent, lorsque le MTA_O effectue une réservation avec le système CMTS, il connaît deux choses: qu'il a une bande passante adéquate dans les deux directions sur le réseau DOCSIS et qu'il a une bande passante adéquate sur les cœurs de réseau pour le flux MTA_O vers MTA_T. Par conséquent, l'adaptateur MTA_O sait que les ressources sont disponibles de bout en bout dans les deux sens une fois qu'il a eu une réponse de MTA_T.

5.7.10 Réglage du point de code DiffServ

Cette architecture permet aussi l'utilisation d'un cœur de réseau à services différenciés, lorsqu'il existe une bande passante adéquate pour transporter des conversations vocales, mais l'accès à cette bande passante se fait sur une base contrôlée. L'accès à la bande passante et le traitement différencié sont fournis aux paquets avec le codage approprié des bits dans le champ de l'en-tête IP spécifié pour le service différencié. Ce mécanisme est appelé le point de code DiffServ (DSCP, *DiffServ code point*). Le champ DS assure la compatibilité amont avec les utilisations présentes des bits IP de préséance de l'octet de type de service d'IPv4 [IETF RFC 2474]. Il est souhaitable de pouvoir

régler le point de code DiffServ des paquets qui sont sur le point d'entrer dans le cœur de réseau du fournisseur en provenance du système CMTS. Etant donné que les ressources consommées par ces paquets dans le cœur de réseau peuvent dépendre largement de ce marquage, cette architecture fournit le contrôle du marquage aux entités du réseau. Ceci permet au réseau et au fournisseur de service de contrôler l'utilisation de la QS améliorée plutôt que de faire confiance à l'adaptateur MTA. Le fournisseur peut configurer des politiques dans le système CMTS qui déterminent comment régler le DSCP pour des flux qui transitent par le système CMTS. Ces politiques sont envoyées par le CMS/GC au système CMTS dans le protocole d'établissement de portes.

Pour l'efficacité de l'implémentation, les informations sur le DSCP approprié sont transmises au MTA pour qu'il l'utilise sur une session donnée. Le système CMTS a encore besoin de réguler les paquets reçus pour s'assurer qu'un DSCP correct est utilisé et que le volume de paquets dans une classe donnée se trouve dans les limites autorisées.

5.8 Mappage d'échantillons des descriptions SDP en flowspecs de RSVP

Les messages du protocole de description de session sont utilisés pour décrire les sessions multimédias pour les besoins de l'annonce de session, l'invitation de session, et autres formes d'initialisation de session multimédia conformément au document RFC 2327 de l'IETF. Le présent paragraphe décrit un mécanisme pour le mappage de descriptions du protocole SDP en flowSpecs du protocole RSVP.

Une description du protocole SDP courante contient de nombreux champs qui comportent les informations concernant la description de la session (version du protocole, nom de la session, lignes d'attributs de la session, etc.), la description de l'heure (l'heure à laquelle la session est active, etc.), et la description des média (nom et transport du médium, intitulé du médium, informations sur la connexion, lignes d'attributs du médium, etc.). Les deux composants critiques pour le mappage d'une description de protocole SDP en un message FlowSpec du protocole RSVP sont l'adresse du nom et transport du médium (m) et les lignes d'attribut du médium (a).

L'adresse du nom et transport du médium (m) sont de la forme:

m = <médium> <port> <transport> <liste fmt>

La ou les lignes d'attribut du médium (a) sont de la forme:

a = <jeton>:<valeur>

Une communication vocale sur IP typique serait de la forme:

m = audio 3456 RTP/AVP 0

a = ptime: 10

Sur la ligne d'adresse du transport (m), le premier terme définit le type de médium, qui est audio dans le cas d'une session vocale sur IP. Le second terme définit le port UDP auquel est envoyé le médium (port 3456). Le troisième terme indique que ce flux est un profil audio/vidéo du protocole RTP. Finalement, le dernier terme est le type de charge utile du médium comme défini dans le profil Audio/Vidéo RTP (voir le document RFC 3551 de l'IETF). Dans ce cas, le 0 représente un type de charge utile statique de codage MIC loi μ sur un seul canal audio échantillonné à 8 kHz. Sur la ligne attribut de média (a), le premier terme définit le temps de formation du paquet (10 ms).

Les types de charge utile autres que ceux définis dans le document RFC 3551 de l'IETF sont liés de façon dynamique par l'utilisation d'un type de charge utile dynamique dans la gamme 96 à 127, comme défini dans le document RFC 2327 de l'IETF, et une ligne d'attribut de médium. Par exemple, un message de protocole SDP typique pour G.726 serait composé comme suit:

m = audio 3456 RTP/AVP 96

a = rtpmap:96 G726-32/8000

Le type de charge utile 96 indique qu'il est définit localement pour la durée de cette session, et la ligne suivante indique que le type de charge utile 96 est lié au codage "G726-32" avec un débit d'horloge de 8000 échantillon/s. Pour chaque CODEC défini (qu'il soit représenté en SDP comme un type de charge utile statique ou dynamique), il est nécessaire d'avoir un tableau de mappage du type de charge utile ou de la représentation de chaîne ASCII aux exigences de bande passante pour ce CODEC.

Pour les codecs qui ne sont pas d'un modèle courant, les exigences de bande passante ne peuvent pas être déterminées à partir seulement des lignes adresse du nom et transport du médium (m) et attributs du médium.

a) Dans cette situation, le protocole SDP DOIT utiliser la ligne paramètre de largeur de bande;

b) pour spécifier ses exigences de largeur de bande au codec inconnu. La ligne paramètre de largeur de bande (b) est de la forme:

b = <modifier>: <valeur de largeur de bande>

Par exemple:

b = AS:99

Ce paramètre de largeur de bande DOIT être utilisé conjointement avec les attributs du médium pour transposer le protocole SDP en un FlowSpec, qui sera utilisé dans la décision d'autorisation de politique et dans l'allocation de porte suivante.

NOTE – L'acceptation ou le rejet de la largeur de bande demandée dans le message SDP est une décision de politique du CMS/CMTS.

Le paramètre largeur de bande (b) inclura la redondance de largeur de bande nécessaire pour les en-têtes IP/UDP/RTP. De plus, aucune suppression PHS utilisée dans la liaison DOCSIS ne sera reflétée dans la largeur de bande demandée. Dans le cas spécifique où des codecs multiples sont spécifiés dans le message SDP, le paramètre largeur de bande devrait contenir le maximum des bandes passantes désirées des codecs.

Le mappage de code RTP/AVP en FlowSpec du protocole RSVP se fait conformément au Tableau 2/J.161.

6 MTA incorporés au protocole de QS du câblo-modem (pkt-q1)

Le CMTS DOIT prendre en charge l'interface MAC DOCSIS comme indiqué dans le présent paragraphe. Un MTA intégré DOIT utiliser les mécanismes définis dans le présent paragraphe pour réserver dynamiquement des ressources locales de QS.

En utilisant cette approche, un MTA intégré signale directement pour la QS du réseau d'accès local en utilisant l'interface de service de contrôle MAC définie dans la Recommandation RFI DOCSIS (Recommandations UIT-T J.112 et J.122). Un MTA intégré signale ses exigences de QS de niveau de session dans les protocoles de signalisation DCS et NCS. Une fois que le MTA intégré détermine que les ressources de QS ont besoin d'être réservées ou engagées, le MTA DOIT initialiser la signalisation de flux de service dynamique DOCSIS pour amener la création, le changement et/ou la suppression du ou des flux de service et l'allocation des ressources DOCSIS. Si la session est créée par le MTA intégré ou par un homologue ou un nœud de réseau, le MTA transmet les exigences de QS à la couche MAC DOCSIS via l'interface de service de contrôle MAC. Ceci amène la création ou la modification du ou des flux de service nécessaires pour la session en utilisant les mécanismes d'échange de messages de flux de service dynamique DOCSIS. Les paragraphes qui suivent étudient le mappage par le MTA des exigences de QS de niveau de session en celles de DOCSIS, la

prise en charge de DOCSIS pour la réservation/engagement en deux phases et l'utilisation de l'interface de service de contrôle MAC DOCSIS.

6.1 FlowSpec du protocole RSVP

L'architecture de services intégrés de l'IETF utilise des descriptions à usage général (indépendant de la couche 2) des caractéristiques du trafic et des exigences relatives aux ressources d'un flux. La description du trafic est appelée une TSpec, les exigences relatives aux ressources sont contenues dans une RSpec et la combinaison de ces éléments est appelée une FlowSpec. Afin de réserver des ressources sur un support de couche 2 spécifique tel qu'un réseau DOCSIS, il est nécessaire de définir un mappage entre la FlowSpec indépendante de la couche 2 et les paramètres spécifiques de la couche 2. Des mappages pour un grand nombre d'autres technologies (ATM, LAN 802.3, etc.) ont déjà été définis.

D'autres spécifications (par exemple, la spécification du codec IPCablecom de la Rec. UIT-T J.161) définissent les exigences de mappage entre les descriptions de service de la couche supérieure (par exemple SDP tel qu'utilisé dans les applications VoIP) et les FlowSpec. Le présent paragraphe spécifie comment le système CMTS et l'adaptateur MTA DOIVENT mapper les FlowSpec en paramètres de la couche 2.

Les services intégrés définissent actuellement deux types de service: service à charge contrôlée et service garanti, ce dernier étant le plus adapté pour les applications sensibles au temps d'attente. Lorsqu'elle effectue une réservation pour un service garanti, la FlowSpec contient:

TSpec

profondeur du seau (b) – octets
débit du seau (r) – octets/s
débit de crête (p) – octets/s
unité régulée minimale (m) – octets
taille maximale du datagramme (M) – octets

RSpec

débit réservé (R) – octets/s
terme de surlongueur (S) – microsecondes

Les termes de TSpec sont pour la plupart suffisamment explicites. (r,b) spécifie un "seau de jetons" auquel le trafic se conforme, p est le débit de crête avec lequel la source émettra et M est la taille maximale du paquet (y compris l'en-tête IP et l'en-tête de la couche supérieure) qui sera généré par la source. L'unité régulée minimale m, est habituellement la taille de paquet la plus petite que la source générera; si la source envoie un paquet plus petit, il comptera comme un paquet de taille m pour les besoins de la régulation.

Pour comprendre la RSpec, il est utile de comprendre comment est calculé le délai dans un environnement de services intégrés. Le délai maximal de bout en bout subi par un paquet recevant un service garanti est:

$$\text{Délai} = b / R + C_{tot} / R + D_{tot}$$

où b et R sont tels que définis ci-dessus et C_{tot} et D_{tot} sont des "termes d'erreur" cumulés fournis par les éléments de réseau le long du trajet, qui décrivent leur écart par rapport à un comportement "idéal".

Le débit R fourni dans la RSpec est la quantité de bande passante allouée au flux. Il DOIT être supérieur ou égal au r de la TSpec pour la limite de délai à tenir. Ainsi, une limite de délai de flux est complètement déterminée par le choix de R; l'utilisation d'une valeur de R supérieure à r serait destinée à réduire le délai subi par le flux.

Etant donné qu'il n'est pas admissible de régler R < r, un nœud effectuant une réservation peut effectuer le calcul ci-dessus et déterminer que la limite du délai est plus serrée que nécessaire. Dans ce cas, le nœud peut régler R = r et régler S à une valeur non nulle. La valeur de S serait choisie telle que:

$$\text{Limite de délai souhaitée} = S + b / R + C_{tot} / R + D_{tot}$$

Le service garanti n'essaie pas de borner la gigue plus que ne l'implique la limite du délai. En général, le délai minimal qu'un paquet peut subir est le délai de la vitesse de la lumière et le délai maximal est la limite du délai donnée ci-dessus. La gigue maximale est la différence entre ces deux délais. Ainsi la gigue peut être contrôlée par un choix convenable de R et S.

6.1.1 Descriptions SDP complexes avec des codecs multiples

Il existe différentes situations dans lesquelles une réservation a besoin de couvrir une gamme de flowspecs possibles. Par exemple, pour certaines applications, il est souhaitable de créer une réservation, qui peut gérer le passage d'un codec à un autre à mi-session sans avoir à réussir le contrôle d'admission à chaque temps de commutation.

La TSpec expéditrice DOIT contenir la limite supérieure minimale (LUB, *least upper bound*) des paramètres de flux nécessaires pour le flux composant.

La limite supérieure minimale des flux avec deux types de programmation DOCSIS différents n'est pas autorisée.

La limite supérieure minimale (LUB) de deux flux A et B, LUB(A, B), est la "plus faible" enveloppe qui peut porter les deux flux A, B non simultanément. LUB(A, B) est calculée paramètre par paramètre comme suit:

Définissons les valeurs de TSpec pour un flux α comme au § 6. Définissons aussi la période $P\alpha$ comme $M\alpha/r\alpha$. LUB(A, B) est alors donné par:

LUB(A, B) ≡ { bLUB(A, B) ≡ MAX(bA, bB),
r LUB(A, B) ≡ (M LUB(A, B)/P LUB(A, B)),
p LUB(A, B) ≡ MAX(pA, pB, r LUB(A, B)),
m LUB(A, B) ≡ MAX(mA, mB),
M LUB(A, B) ≡ MAX(MA, MB)
}

où:

p LUB(A, B) ≡ GCF(PA, PB);

la fonction MAX(x, y) signifie "prendre la plus haute de la paire (x, y)";

la fonction MAX(x, y, z) ≡ MAX(MAX(x, y), z);

la fonction GCF(x, y) signifie "prendre le plus grand facteur commun de la paire (x, y)".

La LUB de n flux (n ≠ 2), LUB(n1, n2, ...), est définie récursivement comme:

LUB(n1, n2, ..., N) ≡ LUB(n1, LUB(n2, ..., N))

De plus, le terme de surlongueur dans la RSpec correspondante doit permettre à tout flux composant d'utiliser les ressources. Pour garantir que ce critère est satisfait, la RSpec pour le flux est réglée à la valeur minimale des valeurs de RSpec dans le flux composant. C'est-à-dire:

SLUB(A, B) ≡ MIN(SA, SB)

où la fonction MIN(x, y) signifie "prendre le plus petit de la paire (x, y)".

L'exemple suivant montre comment les paramètres de TSpec sont déterminés en utilisant l'algorithme LUB spécifié ci-dessus:

1) en résultat de la négociation de codec, les codecs suivants sont choisis pour un appel:
   G711(20 ms) et G728(10 ms)
2) la profondeur de seau LUB pour les codecs choisis est:
   G711(20 ms) = (8000/50) + 40 = 200 octets
   G728(10 ms) = (2000/100) + 40 = 60 octets
   b[LUB] = m[LUB] = M[LUB] = MAX(200, 60) = 200 octets
3) le débit du seau LUB pour les codecs choisis est:
   P [LUB] = GCF(10 ms, 20 ms) = 10 ms = 0,01 s
   r[LUB] = M × 1/P = 200 × 1/0.01 = 20,000 octets par seconde
   r[G711(20 ms)] = 200 × 1/0.02 = 10,000 octets par seconde
   r[G728(10 ms)] = 60 × 1/0.01 = 6,000 octets par seconde
   p[LUB] = MAX(10000, 6000, 20000) = 20,000 octets par seconde

6.1.2 Mappage des FlowSpec RSVP en paramètres de QS DOCSIS

Le système CMTS, à réception d'une demande de réservation, doit utiliser les algorithmes suivants pour le mappage des FlowSpec RSVP en paramètres de QS DOCSIS:

Le MTA DOIT utiliser les prescriptions définies dans le paragraphe suivant pour le mappage des prescriptions de QS de niveau session en paramètres de QS de DOCSIS.

En plus de ces prescriptions, les MTA incorporés DOIVENT inclure leurs propres adresse et ports envoyés (c'est-à-dire de source amont) et reçus (c'est-à-dire de destination aval) dans tous les TLV de classement fournis via un échange de messages DSx. Les adresses d'extrémité distante et les ports de réception PEUVENT être génériques si le SDP d'extrémité distante n'a pas été fourni et si les valeurs n'ont pas été fournies via LCO. Si ces valeurs sont fournies dans l'un ou l'autre format, elles DOIVENT être incluses dans les TLV de classement. Les ports de source d'extrémité distante DOIVENT dans tous les cas être génériques dans la mesure où ce paramètre n'est pas communiqué via SDP.

On devrait noter que les exemples fournis dans le présent paragraphe ne comportent pas la redondance associée à l'en-tête étendu BPI+ de DOCSIS, comme recommandé dans la Recommandation sur la sécurité (Rec. UIT-T J.170). Si BPI+ est désactivé (par exemple, pour les besoins des essais) les valeurs données dans ces exemples devraient être mises à jour de façon appropriée en retranchant cinq octets de la redondance de couche Liaison du calcul de la taille d'allocation amont.

6.1.2.1 Codages de qualité de service amont

Les objets amont DOCSIS doivent être réglés comme indiqué ci-dessous. Tous les autres codages de TLV de qualité de service de flux de NE DOIVENT PAS être définis, permettant ainsi aux valeurs par défaut d'être utilisées. Si l'adaptateur MTA fournit un de ces TLV, le système CMTS DOIT rejeter la demande avec un code d'erreur "rejet permanent/rejet administratif".

La valeur du temporisateur *Temporisation DOCSIS active* est utilisée pour détecter l'inactivité et initialiser la récupération de ressources pour les flux de service engagés. La synchronisation MTA/CMTS peut être coordonnée par le système CMTS en fournissant une valeur appropriée dans le message REQ/RSP du DSA/DSC. Ce champ NE DOIT PAS être rempli par le MTA.

La valeur du temporisateur *Temporisation DOCSIS admise* est utilisée pour détecter l'inactivité et initialiser la récupération de ressources pour les flux de service réservés. La synchronisation MTA/CMTS peut être coordonnée par le système CMTS en fournissant une valeur appropriée dans le message REQ/RSP du DSA/DSC. Ce champ NE DOIT PAS être rempli par le MTA.

Le paramètre de taille de paquet à débit réservé *Minimum supposé DOCSIS* NE DOIT PAS être établi pour les flux amont.

Si un dispositif choisit d'invoquer plusieurs allocations par intervalles, le paramètre *Allocations DOCSIS par intervalle* DOIT être mis à une valeur entière supérieure à 1. Si ce dispositif ne prend pas en charge, ou choisit de ne pas utiliser plusieurs allocations par intervalle, le paramètre *Allocations DOCSIS par intervalle* DOIT être mis à 1.

Le paramètre *Intervalle d'allocation nominal DOCSIS* DOIT être réglé à l'intervalle de mise en paquets du codec.

Intervalle d'allocation nominal DOCSIS = 10000 ou 20000 ou 30000

Le paramètre *Gigue d'allocation DOCSIS tolérée* DOIT être réglé à une valeur spécifiée par le serveur CMS et qui est fondée sur les informations de coût de l'acheminement. La gamme admise pour ce paramètre est entre 0 et 2 fois l'intervalle de mise en paquets. Si la valeur n'est pas spécifiée par le serveur CMS, une valeur par défaut de 800 microsecondes DOIT être utilisée.

Le paramètre *Intervalle d'interrogation DOCSIS nominal* NE DOIT PAS être spécifié pour les flux de service UGS, et DEVRAIT être mis à une valeur qui est un multiple entier de l'intervalle de mise en paquets du codec pour les flux de service UGS/AD.

Le paramètre *Gigue d'interrogation DOCSIS tolérée* NE DOIT PAS être spécifié pour les flux de service UGS, et DEVRAIT être mis à une valeur qui est un multiple entier de l'intervalle de mise en paquets du codec pour les flux de service UGS/AD.

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

Le paramètre *Outrepasser le TOS DOCSIS* NE DOIT PAS être utilisé. Même si ce paramètre est défini par DOCSIS, l'utilisation de ce champ est interdite par PacketCable.

Le paramètre *Taille d'allocation non sollicitée DOCSIS* DOIT être calculé à partir du FC d'en-tête MAC DOCSIS jusqu'à la fin du CRC. Cette valeur inclut une 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). Cette valeur incorpore aussi la redondance de couche MAC DOCSIS, y compris l'en-tête de base DOCSIS (6 octets), l'en-tête étendu UGS (3 octets), et l'en-tête étendu BPI+ (5 octets). Si la suppression d'en-tête de charge utile (PHS) est activée, le nombre d'octets supprimés NE DOIT PAS être inclus. Noter que l'en-tête étendu de suppression PHS (2 octets) NE DOIT PAS être inclus pour les flux de service UGS ou UGS/AD, dans la mesure où les informations appropriées sont incorporées dans l'en-tête étendue UGS.

Taille d'allocation non sollicitée DOCSIS^8,9 = M + 32-PHS[3, 4]

Le paramètre *Type de programmation amont DOCSIS* DOIT être mis soit à UGS soit à UGS/AD, selon que la suppression de silence est prise en charge ou non sur l'appel.

Si l'adaptateur MTA effectue une réservation ou un engagement pour un codec qui ne réalise pas de détection d'activité vocale, le MTA DOIT alors utiliser l'UGS comme type de programmation, autrement, il DOIT utiliser l'UGS/AD.

---

[3] Cet exemple suppose que BPI+ est utilisé comme prescrit par la spécification sur la sécurité PacketCable.

[4] La suppression PHS utilisée dans cet exemple est définie dans la spécification RFI de DOCSIS, § B.C.2.2.10.4/J.112.

Si l'adaptateur MTA effectue une réservation pour un flux de service au profit de codecs multiples dont l'un réalise la détection d'activité vocale, le MTA DOIT alors demander à l'UGS/AD la réservation et l'engagement pour les propriétés du seul codec actif, comme décrit ci-dessus.

6.1.2.2 Codages de classification de paquet amont

Demandes de classification de paquets amont DOCSIS

Les objets amont DOCSIS doivent être établis comme indiqué ci-dessous. Aucun autre codage de TLV de classification NE DOIT être défini, permettant ainsi d'utiliser les valeurs par défaut. Si l'adaptateur MTA fournit un des TLV qui doivent être omis, le système CMTS DOIT alors rejeter la demande avec un code d'erreur "rejet permanent/rejet administratif".

S'il est défini par le système CMTS, le paramètre *Identifiant de classement DOCSIS* DOIT être utilisé. Autrement, le paramètre *Référence de classement DOCSIS* DOIT être mis à une valeur unique par message de service dynamique.

Le paramètre *Référence de flux de service DOCSIS* DOIT être mis à une valeur unique d'E-MTA pour les appels existant dans les messages DSA_REQ, et DOIT être omis dans tous les autres messages. On DOIT utiliser à la place le paramètre *Identifiant de flux de service DOCSIS* provenant du système CMTS.

Le paramètre *Priorité de règle DOCSIS* DOIT être mis à 128.

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

L'*Action de changement de service dynamique DOCSIS* PEUT utiliser les opérations de Changement de service dynamique Ajouter Classeur (0), Remplacer Classeur (1) et Supprimer Classeur (2) selon la spécification RFI de DOCSIS.

Le *Type de service IP DOCSIS* et les champs de gabarit PEUVENT être omis, dans la mesure où PacketCable n'incorpore pas les paramètres de type de service dans sa classification. Autrement, si ce paramètre est inclus, il DOIT correspondre à la valeur de type de service spécifiée par le serveur CMS ou à une valeur approvisionnée pour les flux de service vocaux.

Le paramètre *Protocole IP DOCSIS* DOIT être mis à UDP (17).

Le paramètre *Adresse IP de source DOCSIS* DOIT être réglé à la même adresse que celle qui figure dans le Gabarit d'expéditeur, pourvu que la valeur fournie soit différente de zéro. Si l'adresse spécifiée dans l'objet Gabarit d'expéditeur est zéro, ce paramètre DOIT être omis.

Le paramètre *Gabarit de source IP DOCSIS* DOIT être omis.

Les paramètres *Début de port IP de source DOCSIS* et *Fin de port IP de source DOCSIS* DOIVENT être réglés à la même valeur de port de transport que dans le Gabarit d'expéditeur.

Le paramètre *Adresse IP de destination DOCSIS* DOIT être réglé à la même adresse que celle qui figure dans l'objet Session, pourvu que la valeur fournie soit différente de zéro. Si l'adresse spécifiée dans l'objet Session est zéro, ce paramètre DOIT être omis.

Le paramètre *Gabarit de destination IP DOCSIS* DOIT être omis.

Les paramètres *Début de port IP de destination DOCSIS* et *Fin de port IP de destination DOCSIS* DOIVENT être mis au même port de transport que l'objet Session, pourvu que la valeur fournie soit différente de zéro. Si le port IP de destination est spécifié avec une valeur de zéro dans l'objet Session, les TLV de Début et de Fin de port IP de destination DOCSIS DOIVENT être omis.

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

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

Comportement du système CMTS pour les demandes de classification de paquet amont DOCSIS

A réception de la demande Ajout de classeur (par exemple, via la messagerie DOCSIS DSx) le système CMTS DOIT comparer les réglages de porte référencés par l'ID de porte avec les TLV. Si les TLV ne correspondent pas, le système CMTS DOIT retourner le codage Erreur de classeur DOCSIS avec les informations suivantes:

- le paramètre *Code d'erreur* DOIT contenir une valeur "rejet-autorisation-échec";
- le paramètre *Paramètre erroné* DOIT faire référence au premier TLV qui n'a pas été autorisé. Dans la mesure où des implémentations différentes PEUVENT authentifier les TLV dans un ordre différent, le TLV retourné dans ce champ PEUT être différent dans des conditions identiques;
- le paramètre *Message d'erreur* PEUT être rempli.

6.1.2.3 Codages de suppression d'en-tête de charge utile

Demandes de suppression d'en-tête de charge utile DOCSIS

La suppression d'en-tête de charge utile est facultative, cependant, si elle est utilisée, les exigences ci-après doivent être suivies. Ces règles s'appliquent à la PHS sur les flux amont et aval.

Le paramètre *Champ de suppression d'en-tête de charge utile DOCSIS* se réfère aux octets des en-têtes qui DOIVENT être supprimés par l'entité expéditrice, et DOIVENT être restaurés par l'entité de réception.

Le paramètre *Taille de suppression d'en-tête de charge utile DOCSIS* DOIT être égal au nombre total d'octets du champ Suppression d'en-tête de charge utile (PHSF, *payload header suppression field*).

Le paramètre *Gabarit de suppression d'en-tête de charge utile DOCSIS* DOIT indiquer les octets à supprimer.

Le paramètre *Vérification de suppression d'en-tête de charge utile DOCSIS* DEVRAIT être mis à 0 (vérifier).

Le paramètre *Identifiant de classeur DOCSIS* DOIT être utilisé s'il est défini par le système CMTS. Autrement, le paramètre *Référence de classeur DOCSIS* qui était utilisé dans la définition du classeur DOIT être utilisé.

Le paramètre *Référence de classeur DOCSIS* DOIT être utilisé si l'Identifiant de classeur DOCSIS n'est pas défini par le système CMTS. Autrement, le paramètre Identifiant de classeur DOCSIS qui était utilisé dans la définition du classeur DOIT être utilisé.

Le paramètre *Identifiant de flux de service DOCSIS* DOIT être utilisé s'il est défini par le système CMTS. Autrement, le paramètre Référence de flux de service DOCSIS qui était utilisé dans la définition du classeur DOIT être utilisé.

L'action *Changement de service dynamique DOCSIS* PEUT utiliser les opérations Ajout de règle de PHS (0), Etablissement de règle de PHS (1), Suppression de règle de PHS (2), et Suppression de toutes les règles de PHS, conformément à la spécification RFI de DOCSIS.

Comportement du système CMTS pour les demandes de suppression d'en-tête de charge utile DOCSIS

Le traitement des erreurs de PHS décrit ici donne un mécanisme de rétroaction très sophistiqué entre le système CMTS qui rejette une demande initiale de PHS et l'adaptateur MTA demandeur avec l'idée que les informations fournies dans la réponse d'erreur puissent être utilisées pour faciliter le succès d'une approche différente (c'est-à-dire, l'admission réussie du flux UGS sans suppression ou avec une règle de PHS plus simple).

A réception de la demande DSx avec suppression d'en-tête de charge utile DOCSIS, si un système CMTS décide qu'il ne peut pas prendre en charge la suppression demandée (peut-être due à un manque de traitement local ou de ressources mémoire) mais peut prendre en charge le Service d'allocation non sollicitée sans suppression, il DOIT retourner le code de confirmation "rejet-de-suppression-d'en-tête" dans les codages d'erreur de suppression d'en-tête de charge utile DOCSIS avec le Paramètre erroné DOCSIS comme décrit ci-dessus. Le message Erreur DOCSIS PEUT être utilisé.

Si le système CMTS ne peut pas prendre en charge une suppression d'en-tête de charge utile DOCSIS complexe demandée, mais peut en prendre en charge une plus simple, le système CMTS DOIT alors fournir le gabarit de suppression d'en-tête de charge utile DOCSIS dans le champ Paramètre erroné DOCSIS.

Paramètre erroné DOCSIS = gabarit de suppression d'en-tête de charge utile DOCSIS

Si le système CMTS ne peut pas prendre en charge une taille demandée pour la suppression d'en-tête de charge utile DOCSIS mais peut prendre en charge une taille de suppression d'en-tête de charge utile DOCSIS plus petite, le système CMTS DOIT alors fournir la taille de suppression d'en-tête de charge utile DOCSIS dans le champ Paramètre erroné DOCSIS.

Paramètre erroné DOCSIS = taille de suppression d'en-tête de charge utile DOCSIS

Comportement de l'E-MTA pour les demandes de suppression d'en-tête de charge utile DOCSIS

A réception d'un code de confirmation de "rejet-de suppression-d'en-tête" dans lequel le paramètre erroné DOCSIS inclut le Gabarit de suppression d'en-tête de charge utile DOCSIS, l'E-MTA PEUT redemander la bande passante sans suppression d'en-tête de charge utile DOCSIS ou PEUT redéfinir le Gabarit de suppression d'en-tête de charge utile DOCSIS de telle sorte que le gabarit contienne une règle de suppression plus simple (par exemple, indiquant un bloc contigu d'octets supprimés).

A réception d'un code de confirmation de "rejet-de suppression-d'en-tête" dans lequel le paramètre erroné DOCSIS inclut la taille de suppression d'en-tête de charge utile DOCSIS, le E-MTA PEUT redemander la bande passante sans suppression d'en-tête de charge utile DOCSIS.

Utilisation par l'adaptateur E-MTA de l'en-tête étendu UGS DOCSIS

Le paramètre *Indice de suppression d'en-tête de charge utile* DOCSIS DOIT contenir la valeur de l'indice de PHS préétabli ou zéro lorsqu'il n'y a pas de suppression d'en-tête de charge utile définie pour le flux de service.

Le paramètre *Indicateur de file d'attente DOCSIS* DOIT être établi par l'adaptateur E-MTA chaque fois que plus d'un paquet a été mis en file d'attente de transmission. Autrement, cette valeur DEVRAIT être ramenée à zéro.

Le champ *Allocations actives* de l'en-tête MAC étendu DOCSIS DOIT refléter uniquement les sous-flux (sans perdre de vue qu'en mode dégénéré il ne peut y avoir qu'un seul sous-flux) qui ne sont pas dans l'état Suppression de silence, et DOIT être mis à 0 chaque fois que l'E-MTA est en Suppression de silence pour le codec qui est utilisé pour le flux de données associé à ce flux de service.

6.1.2.4 Codages de qualité de service aval

Les codages de TLV de qualité de service de flux de service aval DOCSIS DOIVENT être établis comme indiqué ci-dessous. Aucun autre TLV NE DOIT être défini, pour permettre ainsi d'utiliser les valeurs par défaut. Si l'adaptateur MTA utilise un de ces TLV, le système CMTS DOIT alors rejeter la demande avec un code d'erreur "rejet permanent/rejet administratif".

Les paramètres DOCSIS aval sont calculés à partir de l'octet d'en-tête MAC DOCSIS 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 de la façon suivante:

Taille de paquet au débit réservé minimal supposé DOCSIS = m + 18 – PHS

Le paramètre *Débit maximal de trafic soutenu DOCSIS*[5] est donné en bits par seconde, y compris la redondance de couche MAC d'Ethernet (mais pas DOCSIS). La conversion à partir des paramètres spécifiques du protocole Internet implique d'abord de déterminer la vitesse de mise en paquet en divisant le débit de crête par l'Unité de régulation minimale. Cette valeur est alors multipliée par la taille de paquet, corrigée pour inclure la redondance de couche MAC, puis le produit entier est étalonné des octets au bit. Le Débit maximal de trafic soutenu DOCSIS DOIT être calculé de la façon suivante:

Débit maximal de trafic soutenu DOCSIS = (p/m) × (m + 18 – PHS) × 8 × z

où z est le nombre de sous-flux que comporte le flux de service.

Le paramètre *Débit minimal de trafic réservé DOCSIS*[5] est calculé d'une façon similaire à celle du Débit maximal de trafic soutenu DOCSIS, sauf qu'au lieu d'utiliser le paramètre Débit de crête (p), on utilise le Débit réservé (R).

Débit minimal de trafic réservé DOCSIS = (R/m) × (m + 18 – PHS) × 8 × z

où z est le nombre d'allocations par intervalle utilisées sur le flux de service amont.

Le paramètre *Rafale maximale de trafic DOCSIS* DOIT être mis supérieur à:

1) un multiple entier de Taille de paquet au débit réservé minimal supposé;
2) la valeur minimale spécifiée DOCSIS de 1522.

Rafale maximale de trafic DOCSIS = max((M + 18 – PHS) × 3 × z, 1522)

où z est le nombre d'allocations par intervalle utilisées sur le flux de service amont.

Le paramètre *Priorité de trafic DOCSIS* DOIT être mis à cinq.

Le paramètre *Temps d'attente aval DOCSIS* NE DOIT PAS être utilisé.

La valeur du temporisateur *Temporisation DOCSIS activée* est utilisée pour détecter l'inactivité et initialiser la récupération de ressources pour les flux de service engagés. Comme les flux de service amont et aval ainsi que les portes sont gérés sous un seul ID de porte et sont supprimés par paires, il n'est pas nécessaire dans le modèle PacketCable de surveiller l'activité des deux flux amont et aval. Pour cette raison, seuls les flux de service amont sont surveillés grâce à l'utilisation de la valeur de la Temporisation DOCSIS activée. Ce champ NE DOIT PAS être rempli par le MTA ou le CMTS pour les flux de service aval.

La valeur du temporisateur *Temporisation DOCSIS admise* est utilisée pour détecter l'inactivité et initialiser la récupération de ressources pour les flux de service réservés. Cependant, suivant la même logique que décrit ci-dessus pour le paramètre Temporisation DOCSIS active, la surveillance des flux de service aval par l'utilisation du paramètre Temporisation DOCSIS admise n'est pas définie dans le modèle IPCablecom. Ce champ NE DOIT PAS être rempli par le MTA ou le CMTS pour les flux de service aval.

---

5 On notera que si une valeur est fractionnaire, elle est alors arrondie.

6.1.2.5 Codages de classification de paquet aval

Demandes de classification de paquet aval DOCSIS

Les objets de classification amont DOCSIS DOIVENT être établis comme indiqué ci-dessous. Aucun autre codage de TLV de classification NE DOIT être défini, permettant ainsi d'utiliser les valeurs par défaut. Si l'adaptateur MTA inclut un des TLV qui doivent être omis, le système CMTS DOIT alors rejeter la demande avec un code d'erreur "rejet permanent/rejet administratif".

S'il est défini par le système CMTS, le paramètre *Identifiant de classeur DOCSIS* DOIT être utilisé. Autrement, le paramètre *Référence de classeur DOCSIS* DOIT être mis à une valeur unique par message de service dynamique.

Le paramètre *Référence de flux de service DOCSIS* DOIT être mis à une valeur unique de E-MTA pour les messages DSA_REQ, et DOIT être omis dans tous les autres messages. On DOIT utiliser à la place le paramètre *Identifiant de flux de service DOCSIS*.

Le paramètre *Priorité de règle DOCSIS* DOIT être mis à 128.

Le paramètre *Etat d'activation de classification DOCSIS* DOIT être mis à actif (1) lorsque l'appel utilisant le flux de service est engagé, et pour tous les autres cas, il DOIT être mis à inactif (0).

L'action *Changement de service dynamique DOCSIS* PEUT utiliser les opérations Classeur d'ajout de DSC (0), Classeur de remplacement de DSC (1) et Classeur de suppression de DSC (2) conformément à la spécification RFI de DOCSIS.

Les champs *TOS IP DOCSIS* et gabarit NE DOIVENT PAS être utilisés.

Le paramètre *Protocole IP DOCSIS* DOIT être mis à UDP (17).

Le paramètre *Adresse IP de source DOCSIS* DOIT être mis à la même adresse que celle qui figure dans le Gabarit d'expéditeur inverse, pourvu qu'une valeur différente de zéro soit fournie. Si l'adresse spécifiée dans l'objet Gabarit d'expéditeur inverse est zéro, ce paramètre DOIT être omis.

Le paramètre *Gabarit de source IP DOCSIS* DOIT être omis.

Les paramètres *Début de port IP de source DOCSIS* et *Fin de port IP de source DOCSIS* DOIVENT être mis à la même valeur de port de transport que celle indiquée dans le Gabarit d'expéditeur inverse, pourvu qu'une valeur différente de zéro soit fournie. Si le Port IP de source est spécifié comme une valeur zéro dans le Gabarit d'expéditeur inverse, les TLV de Début et de Fin de port IP de source DOCSIS DOIVENT être omis.

Le paramètre *Adresse IP de destination DOCSIS* DOIT être mis à la même adresse que celle indiquée dans l'objet Session inverse.

Le paramètre *Gabarit de destination IP DOCSIS* DOIT être omis.

Les paramètres *Début de port IP de destination DOCSIS* et *Fin de port IP de destination DOCSIS* DOIVENT être mis à la même valeur de port que celle indiquée dans l'objet Session inverse.

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

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

Comportement du système CMTS pour les demandes de classification de paquet aval DOCSIS

A réception de la demande Ajout de classeur (par exemple, via la messagerie DSx DOCSIS) le CMTS DOIT comparer les réglages de porte référencés par l'ID de porte aux TLV de la demande. Si les TLV ne correspondent pas, le CMTS DOIT retourner un codage Erreur de classement DOCSIS avec les informations suivantes:

- le paramètre *Code d'erreur* DOIT contenir "rejet-autorisation-échec";

- le paramètre *Paramètre erroné* DOIT pointer le premier TLV qui a manqué l'autorisation. Dans la mesure où des implémentations différentes peuvent authentifier les TLV dans un ordre différent, le TLV retourné dans ce champ peut être différent dans des conditions identiques;
- le paramètre *Message d'erreur* PEUT être rempli.

6.1.2.6 Exemple de mappage

Considérons l'exemple suivant. Un codec vocal produit un flux de données CBR en sortie de 64 kbit/s, qui est mis en paquets à des intervalles de 10 ms, produisant ainsi une charge utile de 80 octets toutes les 10 ms. La charge utile est incorporée en utilisant le protocole RTP/UDP/IP, avec 40 octets supplémentaires, ce qui donne un paquet de 120 octets toutes les 10 ms. La TSpec dans ce cas est:

profondeur de seau (b) = 120 octets

débit de seau (r) = 12 000 octets/seconde

débit de crête (p) = 12 000 octets/seconde

unité régulée minimale (m) = 120 octets

taille maximale de datagramme (M) = 120 octets

Supposons qu'un client demande une réservation en utilisant cette TSpec et une RSpec avec R = r. Un CMTS recevant cette demande va établir un flux de service qui utilise le service d'allocation non sollicitée parce que p = r et M = b, indiquant un flux CBR. Il peut utiliser une taille d'allocation de M octets à un intervalle de M/R = 10 ms.

Pour le calcul de la gigue, l'adaptateur MTA ne connaît pas de combien dévie par rapport à l'idéal le système CMTS dans son comportement de programmation. Le client devrait supposer que le système CMTS est idéal, ce qui signifie que le délai qu'il va subir avec la TSpec et son débit réservé R = r est simplement:

$$b/r + \text{temps de propagation}$$

En ignorant le temps de propagation, il en résulte un délai de 10 ms. Supposons que le client tolère un délai de 15 ms pour cette session (seulement sur le trajet client-CMTS), il mettrait alors son terme de surlongueur (S) à 15 – 10 = 5 ms. En recevant la réservation, le système CMTS interprète ceci comme une indication qu'une gigue d'allocation de 5 ms est acceptable pour le client.

Supposons que le client tolère un délai de 25 ms, et règle son terme de surlongueur à 25 – 10 = 15 ms. Le système CMTS peut utiliser cette information pour déterminer qu'il peut utiliser un plus grand intervalle d'allocation, par exemple de 20 ms, dans la mesure où cela peut augmenter le délai jusqu'à 20 ms pour un paquet qui arrive au câblo-modem juste après une allocation. Il reste encore 5 ms de surlongueur, que le CMTS peut utiliser pour établir la gigue d'allocation.

Noter que cette approche laisse une souplesse considérable au système CMTS pour satisfaire aux exigences du client en ce qui concerne le délai selon la manière qui convient le mieux aux capacités du système CMTS.

6.1.3 Autorisation et comportement du système CMTS

A réception de demandes de réservation ou d'engagement de bande passante contenant un ID de porte, le système CMTS doit effectuer un contrôle d'admission sur la demande de bande passante en utilisant les objets de porte associés à l'ID de porte.

Chaque demande DSA ou DSC originaire d'un E-MTA pour la prise en charge d'une session d'appel donnée DOIT contenir un ID de porte dans le bloc d'autorisation, autrement, le système CMTS DOIT rejeter la demande avec le code de confirmation 24 (échec d'autorisation). Si un message de demande DSC est reçu, et qu'il contient un ID de porte différent de celui fourni dans la demande

DSA utilisée pour créer le flux de service, le CMTS DOIT alors effectuer les procédures normales d'autorisation et d'admission en utilisant la porte associée au nouvel ID de porte.

Si un MTA n'utilise pas plusieurs allocations par intervalle sur le flux en cours de modification et que le contrôle d'autorisation et d'admission réussissent, le système CMTS DOIT associer le nouvel ID de porte au flux de service modifié, remplacer les valeurs de Temporisateur de flux admis et de Temporisateur de flux actif DOCSIS du flux de service associé par les temporisateurs T7 et T8 de la nouvelle porte amont, et inclure ces valeurs de temporisateur dans la réponse DSC à l'adaptateur MTA. Dans ce cas, le CMTS DOIT retirer immédiatement la porte d'origine et le notifier au serveur CMS via un message Porte fermée avec pour Raison le sous-code 0 (Normal).

Si un MTA utilise plusieurs allocations par intervalle et que le contrôle d'autorisation et d'admission réussissent, le système CMTS DOIT associer le nouvel ID de porte au nouveau sous-flux, sans modifier en rien le ou les sous-flux existants ni la ou les portes associées à ces sous-flux. Le système CMTS DOIT remplacer les valeurs de Temporisateur de flux admis et de Temporisateur de flux actif DOCSIS associées au flux de service par les temporisateurs T7 et T8 de la nouvelle porte amont, et inclure ces valeurs de temporisateur dans la réponse DSC à l'adaptateur MTA.

Les éléments CMTS et CMS NE DOIVENT PAS réutiliser une porte précédemment associée à un flux de service lors de l'autorisation d'un flux de service distinct. Un système CMTS DOIT rejeter une demande de réservation ou d'engagement pour un nouveau flux de service pour une porte autorisant un flux de service distinct avec le code de confirmation DOCSIS 24 (échec d'autorisation).

Si le module d'autorisation IPCablecom reçoit une demande de réservation de largeur de bande sans bloc d'autorisation, le système CMTS DOIT rejeter la demande avec le code de confirmation "*24, échec d'autorisation*".

Il est à noter que la prescription ci-dessus s'applique aux demandes de bande passante traitées par le module d'autorisation IPCablecom. Elle n'exclut pas la possibilité d'utiliser le module d'autorisation DOCSIS pour traiter d'autres demandes en l'absence d'un bloc d'autorisation. Le module d'autorisation IPCablecom et le module d'autorisation DOCSIS sont des fonctions logiques du système CMTS qui approuvent ou refusent les paramètres et les classeurs de QS. Théoriquement, à l'arrivée d'une demande de QS dans le système CMTS, le module d'autorisation DOCSIS détermine s'il va traiter lui-même cette demande ou s'il va confier cette tâche au module d'autorisation IPCablecom.

Si le système CMTS ne peut pas trouver de porte associée à l'ID de porte, il DOIT renvoyer un code de confirmation "24, échec d'autorisation" indiquant que cette demande a échoué au processus d'autorisation et sera rejetée.

Si le système CMTS trouve une porte associée à l'ID de porte, il doit alors se plier à la procédure d'autorisation suivante. Afin d'effectuer le contrôle d'admission sur les messages DSx DOCSIS et de comparer ces messages en fonction des paramètres avec ceux autorisés via l'objet GateSpec (*spécification de porte, Spec de porte*), le système CMTS doit normaliser les paramètres de QS à la couche deux ou à la couche trois en ajoutant ou en soustrayant la redondance de couche de liaison. Les exemples fournis dans la présente Recommandation supposent que la normalisation donne des paramètres de couche trois en convertissant les paramètres DOCSIS en leurs équivalents RSVP en utilisant les méthodes décrites dans le présent paragraphe.

– La Profondeur de seau de Spec de porte (b), DOIT être supérieure ou égale à la valeur demandée par le MTA.
– Le Débit de seau de Spec de porte (r), DOIT être supérieur ou égal à la valeur demandée par le MTA.

– La Taille maximale de datagramme de Spec de porte (M), DOIT être supérieure ou égale à la valeur demandée par le MTA.
– La taille minimale de datagramme de Spec de porte (m), DOIT être supérieure ou égale à la valeur demandée par le MTA.
– Le Débit de crête de Spec de porte (p), DOIT être supérieur ou égal à la valeur demandée par le MTA.
– Le Débit réservé de Spec de porte (R), DOIT être supérieur ou égal à la valeur demandée par le MTA.
– Le Terme de surlongueur de Spec de porte (s), DOIT être supérieur ou égal à la valeur demandée par le MTA.
– Le Protocole de Spec de porte DOIT être équivalent au protocole demandé par le MTA.
– L'Adresse de destination de Spec de porte DOIT être la même que l'adresse demandée par le MTA, si la Spec de porte contient une valeur différente de zéro. Si la Spec de porte contient une valeur de zéro, cette comparaison DOIT alors être omise.
– Le Port de destination de Spec de porte DOIT être le même que le port demandé par le MTA si la Spec de porte contient une valeur différente de zéro. Si la Spec de porte contient une valeur de zéro, cette comparaison DOIT alors être omise.
– L'Adresse de source de Spec de porte DOIT être la même que l'adresse demandée par le MTA, si la Spec de porte contient une valeur différente de zéro. Si la Spec de porte contient une valeur de zéro, cette comparaison DOIT alors être omise.
– Le Port de source de Spec de porte DOIT être le même que le port demandé par le MTA si la Spec de porte contient une valeur différente de zéro. Si la Spec de porte contient une valeur de zéro, cette comparaison DOIT alors être omise.

Si une des comparaisons d'autorisation ci-dessus échoue pour un message demandant un nouveau flux de service ou modifiant les paramètres de réservation d'un flux existant, le système CMTS NE DOIT PAS alors honorer la demande en créant un nouveau flux de service ou en modifiant les paramètres du flux de service existant. Si l'adaptateur MTA demande une opération d'engagement pour un flux réservé, l'autorisation DOIT alors être effectuée en utilisant les paramètres DOCSIS et la méthode définie dans DOCSIS.

6.2 Prise en charge de DOCSIS pour la réservation de ressources

Dans la Rec. UIT-T J.112, il n'existe aucun mode défini pour transmettre les informations d'autorisation du câblo-modem au *Module d'autorisation* dans le système CMTS. Le module d'autorisation est une fonction logique du système CMTS définie dans la Rec. UIT-T J.112. La présente Recommandation utilise un nouveau TLV de DOCSIS qui transmet un bloc d'autorisation composé d'une chaîne arbitraire de longueur *n* au système CMTS pour être interprétée et traitée uniquement par le module d'autorisation.

Le modèle de QS dynamique est un modèle dans lequel chaque session est autorisée. L'autorisation de chaque session utilise un outil donné à la fois au système CMTS et au MTA, qui est utilisé pour confronter les demandes et les autorisations. Cet outil est l'ID de porte (*GateID*). A réception d'une information de signalisation d'appel, le MTA transmet l'ID de porte au système CMTS en utilisant le TLV AuthBlock contenu dans un message DSA/DSC.

Un système CMTS IPCablecom DOIT disposer de moyens pour activer/désactiver différentes méthodes d'autorisation d'une demande DSx de câblo-modem afin de lancer et/ou de modifier des flux de service. Le système CMTS IPCablecom DOIT implémenter la méthode d'"autorisation d'ID de porte", qui lui permettra de n'autoriser que les demandes contenant un ID de porte dans le bloc d'autorisation IPCablecom. Le système CMTS DEVRAIT implémenter l'autorisation de nom de

classe de service (SCN, *service class name*), qui lui permettra de n'autoriser que les demandes DSx pour un ensemble configuré de noms de classe de service définis par lui.

6.2.1 Réservation/engagement de QS en deux phases

Un flux de service DOCSIS a trois ensembles de paramètres de qualité de service associés, désignés sous la forme d'ensembles de paramètres de QS provisionnés, admis, ou actifs. La relation entre ces ensembles est identique à la description des ressources autorisées, réservées et engagées donnée au § 5.7.4.

Les opérations Réservation et Engagement sont toutes deux exécutées en utilisant des messages de service dynamique DOCSIS, en changeant les valeurs de l'ensemble de paramètres de QS admis et de l'ensemble de paramètres de QS actifs du flux de service. Dans un message Ajout de service dynamique (DSA, *dynamic service addition*) ou changement de service dynamique (DSC, *dynamic service change*), l'opération Réservation est accomplie en incluant, dans les codages de flux de service amont ou les codages de flux de service aval, le TLV de Type d'ensemble de paramètres de QS avec la valeur réglée à Admis (valeur 2). De même, l'opération Engagement est accomplie en réglant le TLV de Type d'ensemble de paramètres de QS à Actif (valeur 4) ou à Admis+Actif (valeur 6).

Les échanges de DSA et DSC entre le câblo-modem et le système CMTS sont des messages de prise de contact à trois voies, se composant d'un message de demande suivi d'une réponse suivie d'un accusé de réception. Ce principe est illustré à la Figure 5.

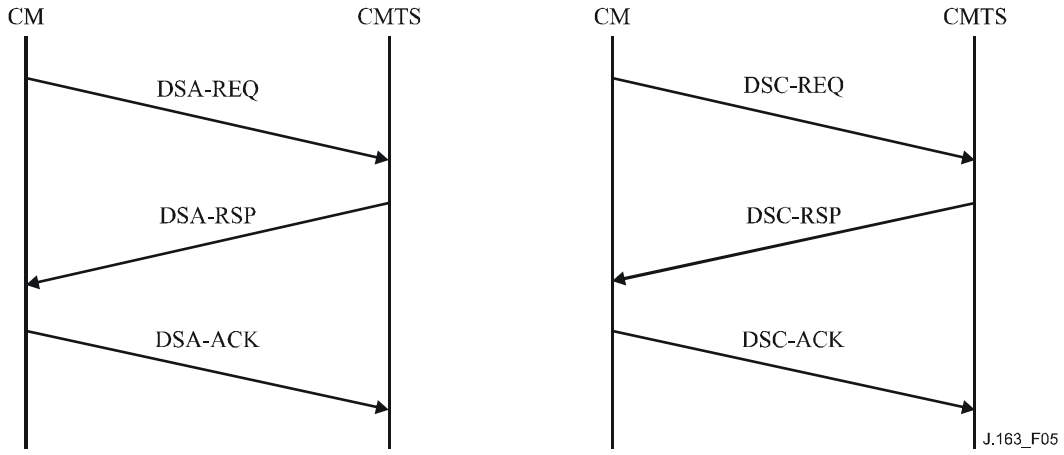


Figure 5/J.163 – Echanges de DSA et DSC entre câblo-modem et CMTS

Par exemple, le message DSA-REQ suivant provoque l'admission des flux de service amont et aval, ce qui signifie que les ressources de QS qui seront utilisées dans le réseau DOCSIS sont réservées.

DSA-REQ (*Demande d'Ajout de service dynamique*)

ID de transaction		1
Flux de service amont	Référence de flux de service	1
	Type d'ensemble de paramètre de QS	Admis (2)
	Programmation de flux de service	UGS (6)
	Intervalle d'allocation nominal	10 ms
	Gigue d'allocation tolérée	2 ms
	Allocations par intervalle	1
	Taille d'allocation non sollicitée	222
Flux de service aval	Référence de flux de service	2
	Type d'ensemble de paramètre de QS	Admis (2)
	Priorité de trafic	3
	Débit soutenu maximal	12000

Autre exemple, le message DSC-REQ suivant provoque l'activation du flux de service, ce qui signifie que les ressources de QS utilisées dans un réseau DOCSIS sont engagées.

DSC-REQ (*Demande de Changement de service dynamique*)

ID de transaction		1
Flux de service amont	ID de flux de service	10288
	Type d'ensemble de paramètre de QS	Admis + Actif (6)
	Programmation de flux de service	UGS (6)
	Intervalle d'allocation nominal	10 ms
	Gigue d'allocation tolérée	2 ms
	Allocations par intervalle	1
	Taille d'allocation non sollicitée	222
Flux de service aval	ID de flux de service	10289
	Type d'ensemble de paramètre de QS	Admis + Actif (6)
	Priorité de trafic	3
	Débit soutenu maximal	12000

La spécification des ensembles de paramètres de QS admis et activés par le MTA passe par les demandes MAC_CREATE_SERVICE_FLOW et MAC_CHANGE_SERVICE_FLOW. Le temps qu'un flux de service soit admis, il a généralement un ou plusieurs classeurs associés.

6.2.2 Maintenance de la réservation

Les paramètres de QS du flux de service DOCSIS "Temporisation pour les paramètres de QS actifs" et "Temporisation pour les paramètres de QS admis" permettent à une session d'être terminée et ses ressources libérées en raison de l'inactivité.

Le paramètre Temporisation pour les paramètres de QS actifs est destiné à récupérer les ressources allouées aux câblo-modems qui tombent en panne, subissent une défaillance ou perdent leur connectivité au réseau câblé. La transmission normale de paquets de données sur le flux de service est suffisante pour éviter cette action de récupération.

Si le temporisateur d'activité DOCSIS arrive à expiration au système CMTS pour un flux de service qui est autorisé via une porte (c'est-à-dire un flux de service PacketCable) le système CMTS doit alors supprimer tous les flux de service associés à la porte en utilisant une demande DSD DOCSIS.

Le système CMTS spécifiera "Temporisateur T8 expiré; inactivité du flux de service dans la direction amont" pour informer le contrôleur de porte de la fermeture de la porte.

Si le MTA effectue la détection d'activité vocale, en utilisant une programmation de flux de service du type UGS/AD et que le système CMTS surveille activement l'activité du flux amont, alors pendant les périodes de silence étendues le MTA DOIT envoyer des paquets de données périodiques sur le flux de service ou rafraîchir le temporisateur actif au moyen d'échange de messages DSC. La Temporisation pour les paramètres de QS admis est destinée à récupérer les ressources qui sont réservées par un câblo-modem mais non engagées. En général, les paramètres engagés seront identiques aux paramètres réservés et cela ne posera pas de problème. Lorsque l'engagement est inférieur à la réservation, il est nécessaire de réinitialiser périodiquement le temporisateur du système CMTS. Cette opération est accomplie en effectuant une opération DSC-REQ qui réserve les mêmes ressources que précédemment.

6.2.3 Prise en charge de l'association dynamique de ressources

Le modèle dynamique de QS demande de pouvoir modifier dynamiquement l'association des ressources aux flux. Par exemple, pour assurer la mise en instance d'un appel, il peut être souhaitable de maintenir en place suffisamment de ressources pour une seule session sur le réseau DOCSIS et de passer l'allocation de ces ressources d'un demandeur à l'autre.

Pour prendre en charge cette fonctionnalité, un objet ID de ressource est ajouté. L'objet ID de ressource est un identifiant opaque généré par le nœud qui a le contrôle des ressources, c'est-à-dire dans ce cas le système CMTS.

Lorsqu'un client envoie une demande de réservation pour un nouveau flux, il indique au système CMTS que cette session souhaite partager les ressources pour cette nouvelle porte (porte 2) avec une porte précédemment créée (porte 1) en incluant l'Identifiant de ressource dans la demande. Tant que la QS demandée pour la nouvelle porte peut être satisfaite avec une allocation de bande passante inférieure ou égale à celle de la porte existante, aucune nouvelle bande passante n'est réservée dans le réseau DOCSIS. Toutefois, il peut être nécessaire de réserver de la bande passante dans le réseau en fonction du trajet de bout en bout emprunté par la nouvelle session. L'accès à la réservation partagée intervient de manière mutuellement exclusive.

L'association dynamique de ressources, requise au § 5.7.7, est accomplie dans la Rec. UIT-T J.112 par l'utilisation du TLV de bloc d'autorisation.

Le système CMTS DOIT inclure l'ID de ressources dans le TLV de bloc d'autorisation pour le message DSA-RSP qu'il envoie au client. Le client PEUT inclure l'ID de ressources dans les messages DOCSIS suivants pour l'application des ressources en question. Plus important, si le client souhaite établir une nouvelle session et réutiliser les ressources d'une session existante, il DOIT d'abord désactiver les flux de service de l'ancienne session au moyen d'une demande DSC-REQ puis inclure l'ID de ressources associé à l'ancienne session dans le message DSA-REQ qu'il envoie au système CMTS.

6.2.4 Mappage de paramètres de la QS pour l'autorisation

La porte identifiée par l'ID de porte est paramétrée au moyen d'un FlowSpec RSVP (qui est constitué d'objets RSVP RSpec et TSpec) pour chaque direction. Le module d'autorisation dans le système CMTS DOIT convertir les paramètres de QS DOCSIS en paramètres RSVP correspondants en utilisant les règles définies ci-dessous:

Les paramètres *Taille du seau de jetons* (b), *Taille maximale de paquet* (M), et *Unité régulée minimale RSVP* (m) DOIVENT être réglés à *Taille d'allocation non sollicitée DOCSIS* moins la

redondance UGS amont DOCSIS[6] pour le sens amont et *Taille de paquet à débit réservé minimal supposé DOCSIS* moins la redondance aval DOCSIS[7] pour le sens aval.

Pour le sens aval, les paramètres *Débit du seau de jetons* (r), et *Débit de crête de données* (p) DOIVENT être calculés en convertissant en termes de couche 3 le *Débit soutenu maximal DOCSIS* en le divisant par la *Taille de paquet au débit réservé minimal supposé DOCSIS* et en multipliant ensuite le résultat par la *Taille maximale de paquet* calculée précédemment. Pour le sens amont, les paramètres *Débit du seau de jetons* (r) et *Débit de crête de données* (p) DOIVENT être mis égaux à *Intervalle d'allocation nominal DOCSIS* multiplié par *Taille d'allocation non sollicitée*.

Pour le sens aval, le paramètre *Débit* (R) DOIT être calculé en convertissant en termes de couche 3 le *Débit de trafic réservé maximal DOCSIS* en le divisant par la *Taille de paquet au débit réservé minimal supposé DOCSIS* et en multipliant ensuite le résultat par l'*Unité régulée minimale* calculée précédemment. Pour le sens amont, le paramètre *Débit* (R) DOIT être mis égal à *Intervalle d'allocation nominal DOCSIS* multiplié par *Taille d'allocation non sollicitée*.

Le *Terme de surlongueur* DOIT être mis à *Gigue d'allocation tolérée DOCSIS* pour le sens amont. Le *Terme de surlongueur* DOIT être mis à zéro pour le flux aval, indiquant que ce paramètre ne sera pas spécifié par l'adaptateur MTA.

Le protocole *Protocol ID* DOIT être mis à *Protocole IP DOCSIS*.

L'*Adresse de destination* DOIT être mise à *Adresse IP de destination DOCSIS*. Si ce paramètre est omis, la valeur DOIT être mise à zéro.

Le *Port de destination* DOIT être mis à *Début de port de destination DOCSIS*. Si ce paramètre est omis, la valeur DOIT être mise à zéro.

L'*Adresse de source* DOIT être mise à *Adresse IP de source DOCSIS*. Si ce paramètre est omis, la valeur DOIT être mise à zéro.

Le *Port de source* DOIT être mis à *Début de port de source DOCSIS*. Si ce paramètre est omis, la valeur DOIT être mise à zéro.

Les objets RSVP convertis qui en résultent doivent alors être vérifiés par rapport à la porte correspondante en utilisant les règles suivantes:

Tous les paramètres nécessaires de *FlowSpec RSVP* et *Terme de surlongueur* DOIVENT être inférieurs ou égaux aux valeurs spécifiées des portes.

Tous les paramètres nécessaires de *TSpec RSVP* DOIVENT être égaux aux valeurs spécifiées de la porte, sauf pour le cas où la porte a une valeur de zéro, auquel cas les paramètres requis correspondants NE DOIVENT PAS être vérifiés.

Si la vérification réussit, le système CMTS DOIT alors continuer de traiter la demande. Si la vérification échoue, le système CMTS DOIT alors faire un rejet permanent de la demande du fait du défaut d'autorisation.

---

6 La redondance devrait inclure 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, qui comprend l'en-tête de base DOCSIS (6 octets), l'en-tête étendu UGS (3 octets), et l'en-tête étendu BPI+ (5 octets). Si la suppression d'en-tête de charge utile (PHS, *payload header suppression*) est activée, le nombre d'octets supprimés doit alors être ajouté à la *Taille d'allocation non sollicitée DOCSIS*.

7 La redondance de couche MAC de DOCSIS 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). Si la PHS est utilisée sur le sens aval, le nombre d'octets supprimés doit être soustrait de la *Taille de paquet au débit réservé minimal supposé DOCSIS*.

Par exemple, en supposant un codec conforme à G.711, un tramage à 20 ms, avec une couche MAC RTP-S de deux octets, et BPI+ activé:

G.711 @ 20 ms

Débit binaire nominal de 64 kbit/s

Débit d'octets nominal de 8 koctet/s

Débit de tramage de 20 ms = 50 paquet/s

8 koctet/s / 50 = 160 octets par paquet de charge utile

42 octets d'en-tête IP/UDP/RTP

160 + 42 = 202 octets par paquet au total

202 × 50 = 10,1 koctet/s de débit d'octet réel

10,1 × 8 = 80,8 kbit/s de débit réel

Les paramètres GateSpec résultants établis par le serveur CMS seraient:

profondeur de seau (b) = taille de datagramme, y compris la redondance d'en-tête IP/UDP/RTP-S = 202 octets

unité régulée minimale (m) = Profondeur de seau (b) = 202 octets

taille de datagramme maximale (M) = Profondeur de seau (b) = 202 octets

débit de seau (r) = débit de données réel, y compris la redondance d'en-tête IP/UDP/RTP-S = 10 100 octet/s

débit de crête (p) = débit de seau (r) = 10 100 octet/s

débit réservé (R) = débit de seau (r) = 10 100 octet/s

Les paramètres DOCSIS incluent la redondance venant de l'octet FC par le CRC.

En-tête de base DOCSIS (de FC à HCS, pas d'en-tête étendu): 6 octets

En-tête étendue UGS: 3 octets

En-tête étendue BPI+: 5 octets

En-tête Ethernet: 14 octets

CRC: 4 octets

Total de redondance de sens amont: 32 octets par paquet

Paramètres de flux de service amont

Type de programmation de sens amont: UGS

Politique de demande/transmission (gabarit binaire): bits 0 à 6 et 8 établis (en binaire: 101111111)

Taille d'allocation: 234 octets

Allocations par intervalle (entier): 1

Intervalle d'allocation: 20 000 µs

Gigue d'allocation tolérée: 800 µs

La procédure de contrôle d'autorisation du système CMTS est conduite comme suit pour les paramètres de sens amont:

Pour se comparer aux paramètres GateSpec, la redondance de couche MAC doit être soustraite des paramètres DOCSIS.

Profondeur de seau GateSpec (b) ≥ Taille d'allocation non sollicitée DOCSIS – 32 octets

202 octets ≥ 234 octets – 32 octets = 202 octets

Débit de seau GateSpec (r) ≥ 1/intervalle d'alloc. DOCSIS × (Taille d'alloc. non sollicitée DOCSIS – 32)

10,1 koctet/s ≥ 1/20 ms × (234 octets – 32 octets) = 50 paquet/s × 202 octets/paquet = 10,1 koctet/s

Les paramètres DOCSIS de sens aval incluent une redondance provenant de l'octet suivant le HCS à travers le CRC.

En-tête Ethernet: 14 octets

CRC: 4 octets

Redondance aval totale: 18 octets par paquet

Paramètres de flux de service aval DOCSIS

Rafale de trafic maximal (valeur minimale de 1522): 1522 octets

Débit soutenu maximal: 88 000 bit/s

Taille de paquet au débit réservé minimal supposé: 220 octets

Débit réservé minimal: 88 000 bit/s

Priorité de trafic: 5

La procédure de contrôle d'autorisation du système CMTS est conduite comme suit pour les paramètres de sens aval:

cette redondance doit encore une fois être soustraite des paramètres DOCSIS afin d'effectuer la comparaison avec GateSpec. La procédure est une simple soustraction du paramètre Taille de paquet au débit réservé minimal supposé DOCSIS. Toutefois, le réglage du paramètre Débit réservé minimal est un peu plus compliqué.

Unité régulée minimale GateSpec (m) ≥ Taille de paquet au débit réservé minimal supposé DOCSIS – (18 × z) octets

Par exemple, si le paramètre *Allocations par intervalle* = z = 1

202 octets ≥ 220 octets – 18 octets = 202 octets

Débit de seau GateSpec (r) ≥ (Débit réservé minimal DOCSIS / (8 × taille de paquet au débit réservé minimal supposé DOCSIS) = (Taille de paquet au débit réservé minimal supposé DOCSIS – 18 × z octets)

Par exemple, si le paramètre *Allocations par intervalle* = z = 1

10,1 koctet/s ≥ (88 kbit/s / (8 × 220 octets)) × (220 octets – 18 octets) = 10,1 koctet/s

6.2.5 Codage de bloc d'autorisation

Le bloc d'autorisation consiste en une chaîne d'octets. Pour donner de la souplesse, le bloc d'autorisation DOIT être codé en utilisant les champs Type-Longueur-Valeur (TLV). Les champs TLV sont non ordonnés, et peuvent être imbriqués. La taille du champ de valeur (en octets) doit être supérieure à zéro; les tailles du champ de type et de longueur sont chacune d'un octet. Noter que la longueur n'inclut que le champ Valeur et non pas la totalité du composé TLV.

Le format du bloc d'autorisation est comme suit:

Codage de bloc d'autorisation IPCablecom

Ce champ définit les paramètres associés au bloc d'autorisation IPCablecom. Noter que ce champ se compose de sous-champs imbriqués.

Type	Longueur	Valeur
1	n	"voir les sous-champs ci-dessous"

Codage de l'ID de porte

La valeur de ce champ spécifie le traitement de l'identifiant de porte utilisé pour l'autorisation.

Type	Longueur	Valeur
[1].1	4	ID de porte

Codage d'ID de ressource

La valeur de ce champ spécifie le traitement de l'identifiant de ressource utilisé pour identifier de façon univoque l'ensemble de ressources associé à un flux de service (service_flow).

Type	Longueur	Valeur
[1].2	4	ID de ressource

Etat de sous-flux

Type	Longueur	Valeur
[1].3	1	état

Cet octet indique l'état du sous-flux parmi 4 états possibles (0-Admis, 1-Actif, 2-Supprimé, 3-Transféré). L'octet d'état est destiné à aider le système CMTS à contrôler l'état des diverses portes qui peuvent être présentes dans un même flux de service. Ce paramètre DOIT être inclus dans toutes les demandes DSx lancées par le câblo-modem dont le paramètre *plusieurs allocations par intervalle* a une valeur supérieure à 1.

Admis (0) – le sous-flux est à l'état admis

Actif (1) – le sous-flux est à l'état actif

Supprimé (2) – la porte doit être supprimée par suite de ce changement de service dynamique (DSC)

Transféré (3) – le sous-flux est en cours de transfert dans un nouveau flux de service.

Pour permettre au système CMTS d'associer de façon appropriée les modifications apportées à un ID de porte donné, l'adaptateur MTA DOIT uniquement inclure une instance du bloc d'autorisation DOCSIS (type 30) dans une demande DSx donnée. Dans le bloc d'autorisation DOCSIS, un codage de bloc d'autorisation IPCablecom (type 30.1) ainsi que le sous-TLV de l'ID de porte requis (type 30.1.1) et éventuellement plusieurs autres sous-TLV DOIVENT être utilisés pour chaque sous-flux du flux. Si une seule allocation par intervalle (et par conséquent un seul ID de porte) est utilisée, le bloc d'autorisation DOIT néanmoins être présent et le champ *état du sous-flux* DOIT être omis.

Pour plus de précisions sur l'autorisation du système CMTS, voir le § 6.1.3.

6.2.6 Traitement de la suppression d'en-tête de charge utile

La spécification RFI DOCSIS définit les règles d'adjonction et de suppression des règles de suppression d'en-tête de charge utile (PHS) (associées à un classeur). Cependant, la procédure de mise à jour d'une règle PHS qui commence à laisser à désirer n'est pas claire. La procédure suivante est REQUISE pour l'adaptateur MTA et le système CMTS si une règle PHS sur un flux vocal doit être modifiée.

Dans le cas où une règle PHS existante commence à laisser à désirer, l'adaptateur MTA DOIT envoyer une seule transaction de changement de service dynamique (DSC) qui:

– ajoute un nouveau classeur avec une nouvelle règle PHS;
– adapte l'enveloppe de QS compte tenu de la nouvelle règle PHS;
– supprime l'ancien classeur et la règle PHS associée.

6.3 Utilisation de l'interface de service de contrôle MAC DOCSIS

Les paramètres de QS DOCSIS pour le flux de service déduit de la description du SDP sont signalés pour établir le ou les flux de service. Le présent paragraphe décrit comment ceci peut être effectué en utilisant les interfaces de service de contrôle MAC DOCSIS (Annexe E de l'Annexe B/J.112).

Au niveau des primitives de l'interface de service de contrôle MAC DOCSIS, le MTA intégré signale pour les ressources de QS comme suit:

1) demande MAC_CREATE_SERVICE_FLOW:

   tel que décrit dans le § B.E.3.2/J.112, le MTA intégré peut demander qu'un flux de service soit ajouté via cette primitive. Cette primitive peut également être utilisée pour définir des classeurs pour le nouveau flux de service, mais également pour fournir les Ensembles de paramètres de QS admis et actif du flux de service. Le succès ou l'échec de la primitive est indiqué via la primitive de réponse MAC_CREATE_SERVICE_FLOW.

2) demande MAC_CHANGE_SERVICE_FLOW:

   le MTA intégré peut initialiser un changement dans les Ensembles de paramètres de QS admis et actif via cette primitive. Un scénario possible est le cas où l'appelé est mis en garde. Le succès ou l'échec de la primitive est indiqué via la primitive de réponse MAC_CHANGE_SERVICE_FLOW.

3) demande MAC_DELETE_SERVICE_FLOW:

   lorsque le MTA intégré n'a plus besoin du flux de service, il envoie une demande MAC_DELETE_SERVICE_FLOW au câblo-modem intégré pour mettre à zéro les ensembles de paramètres de QS actif et admis du flux de service.

Les paramètres de ces primitives correspondent aux paramètres associés aux messages DSA, DSC et DSD tels que donnés à l'Annexe B/J.112.

6.3.1 Etablissement de la réservation

Le MTA initialise la réservation de ressources de QS grâce à l'utilisation de la primitive de demande MAC_CREATE_SERVICE_FLOW. Le MTA DOIT inclure l'ID de porte dans le TLV de bloc d'autorisation. A réception de ce message, la couche MAC du câblo-modem invoque la signalisation DSA en envoyant une DSA_REQ au système CMTS. Le système CMTS DOIT vérifier l'autorisation sur la base de l'ID de porte (contenu dans le TLV de bloc d'autorisation) et rejeter la demande si la porte est non valide ou si les ressources autorisées sont insuffisantes pour la demande. A réception de la DSA_RSP du système CMTS, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_CREATE_SERVICE_FLOW. Ceci est illustré à la Figure 6.

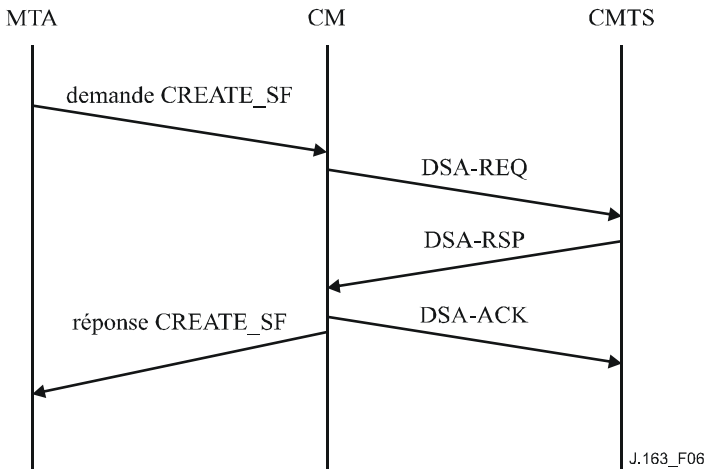


Figure 6/J.163 – Etablissement de réservation

6.3.2 Changement de réservation

Le MTA initialise les changements dans les ressources de QS en utilisant la primitive de demande MAC_CHANGE_SERVICE_FLOW. Ceci est illustré à la Figure 7.

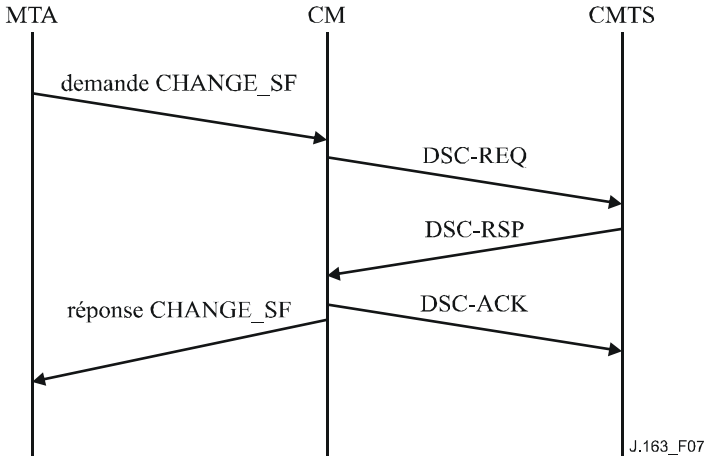


Figure 7/J.163 – Changement de réservation

A réception de ce message, la couche MAC du câblo-modem invoque la signalisation DSC. A réception du DSC_RSP du système CMTS, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_CHANGE_SERVICE_FLOW.

6.3.3 Suppression de réservation

Le MTA initialise la désallocation de réservation de QS en utilisant la primitive de demande MAC_DELETE_SERVICE_FLOW. A réception de ce message, la couche MAC invoque la signalisation DSD. En recevant le DSD_RSP du système CMTS, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_DELETE_SERVICE_FLOW. Ceci est illustré à la Figure 8.

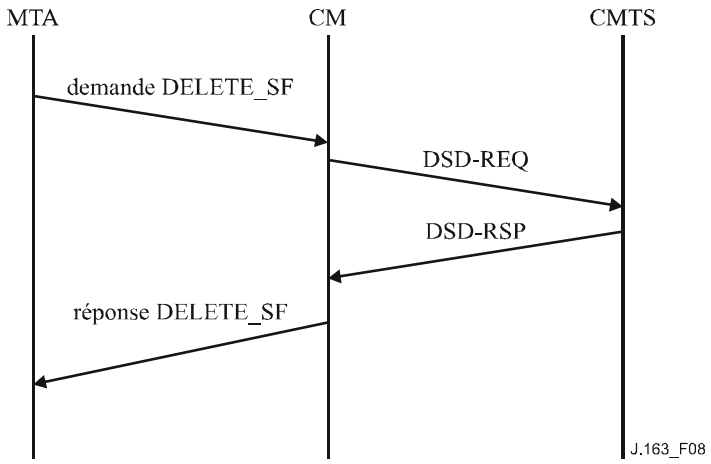


Figure 8/J.163 – Suppression de réservation

6.3.4 Considérations sur la présence de plusieurs allocations par intervalle

6.3.4.1 Adjonction d'une paire de sous-flux

Attendu qu'un seul bloc d'autorisation est autorisé dans un message DSx donné, lorsqu'il ajoute un classeur, le MTA DOIT utiliser le TLV d'Action de changement de service dynamique (en plus du champ *état de sous-flux* du bloc d'autorisation) avec une valeur de 0.

Pour ajouter une paire de sous-flux, le MTA DOIT procéder comme suit:

– envoyer un message DSC avec un bloc d'autorisation contenant les informations relatives à toutes les portes de sous-flux;

– mettre le champ *état de sous-flux* de chaque porte à 0 (réservation) ou à 1 (engagement);

– inclure les classeurs (amont et aval) associés à la porte avec le TLV d'Action de changement de service dynamique mis à 0 – opération DSC Ajouter Classeur. Le MTA DOIT inclure uniquement les classeurs correspondant à la porte utilisée pour l'opération DSC;

– inclure les paramètres de QS amont avec le paramètre Allocations par intervalle incrémenté de 1 pour l'ensemble de paramètres de QS Admis (et éventuellement l'ensemble de paramètres de QS actifs si les ressources sont également engagées);

– actualiser la limite supérieure minimale (LUB) des paramètres de QS aval pour traiter tous les sous-flux aval.

A la réception de ce message DSC, le système CMTS DOIT procéder au contrôle d'admission comme indiqué au § 6.1.3.

6.3.4.2 Modification d'une paire de sous-flux

Lorsqu'une modification de ressources s'impose, le MTA NE DOIT PAS modifier les paramètres de QS du flux de service DOCSIS existants. Au lieu de cela, le MTA DOIT transférer le sous-flux dans un nouveau flux de service, ou dans un nouveau sous-flux d'un flux de service existant. Pour transférer une paire de sous-flux (les sous-flux amont et aval associés à un ID de porte), le MTA DOIT procéder comme suit:

– le MTA envoie un message DSC-REQ pour modifier l'état du sous-flux à "transfert", règle l'état du classeur sur inactif et désengage toutes les ressources actives de la paire de sous-flux;

– le système CMTS envoie un message DSC-RSP et démarre le temporisateur DOCSIS admis qui DOIT être mis à la valeur du temporisateur T7 indiquée dans le message Gate-Set (*Porte établie*) associé et à l'ID de porte indiqué dans le message DSC-REQ;

– à la réception du message DSC-RSP, le MTA envoie un message DSC-ACK et lance le transfert en envoyant un message DSA-REQ (en cas de transfert dans un nouveau flux de service) ou un message DSC-REQ (en cas de transfert dans un flux de service existant) pour réserver/engager la nouvelle paire de flux de service (avec le même ID de porte);
– en cas d'établissement fructueux de la nouvelle paire de flux de service, le MTA DOIT immédiatement envoyer un message DSC-REQ pour supprimer l'ancienne paire de sous-flux;
– si le temporisateur T7 expire pour l'ancien sous-flux avant réception d'un message DSA-REQ ou d'un message DSC-REQ avec le même ID de porte, le système CMTS DOIT supprimer la paire de sous-flux expiré et fermer la porte;
– si le temporisateur T7 expire pour l'ancienne paire de sous-flux, après réception d'un message DSA-REQ ou d'un message DSC-REQ (avec les paramètres de QS admis) avec le même ID de porte mais avant d'avoir reçu le message DSC-REQ qui supprime l'ancienne paire de sous-flux, le système CMTS DOIT supprimer le sous-flux expiré et transférer la porte dans le nouveau flux.

6.3.4.3 Suppression d'une paire de sous-flux

La suppression de paires de sous-flux peut être effectuée par l'adaptateur MTA ou le système CMTS. Les procédures applicables à l'un et à l'autre sont définies ci-dessous:

Suppression à l'initiative de l'adaptateur MTA

Pour supprimer une paire de sous-flux, le MTA DOIT procéder comme suit:

– envoyer un message DSC avec un bloc d'autorisation contenant les informations relatives à toutes les portes de sous-flux;
– mettre le champ *état du sous-flux* à 2 – supprimé pour la paire de sous-flux à supprimer;
– inclure les classeurs (amont et aval) associés à la porte avec le TLV d'Action de changement de service dynamique mis à 2 – opération DSC Supprimer Classeur pour chaque classeur. Le MTA DOIT inclure uniquement les classeurs correspondant à la porte utilisée pour l'opération DSC;
– inclure les paramètres de QS amont avec le paramètre Allocations par Intervalle décrémenté de 1 pour l'ensemble de paramètres de QS admis (et éventuellement l'ensemble de paramètres de QS actifs si les ressources étaient actives);
– recalculer la limite supérieure minimale (LUB) pour le flux aval avec le flux supprimé.

A la réception de ce message DSC, le système CMTS DOIT supprimer les ressources associées à l'ID de porte, supprimer la porte, envoyer un message Gate-Close (*Porte fermée*) au serveur CMS et envoyer un message DSC-RSP.

Suppression à l'initiative du système CMTS

Bien que ce soit là une procédure peu courante, il peut arriver dans certains cas que le système CMTS doive supprimer les ressources amont et aval associées à un ID de porte (après réception d'un message de suppression de porte Gate Delete). Pour pouvoir procéder ainsi pour un sous-flux qui partage un flux avec d'autres sous-flux valides, le système CMTS DOIT:

– envoyer un message DSC qui inclut les classeurs (amont et aval) associés à la porte avec le TLV d'Action de changement de service dynamique mis à 2 – opération DSC Supprimer Classeur pour chaque classeur;
– inclure les paramètres de QS amont avec le paramètre Allocations par Intervalle décrémenté de 1;
– recalculer la limite supérieure minimale (LUB) pour le flux aval avec le flux supprimé;

– à la réception du message DSC, le MTA DOIT supprimer le classeur indiqué et envoyer un message DSC-RSP.

Si le dernier sous-flux est en cours de suppression, un message DSD DOIT être utilisé pour supprimer le flux dans son intégralité.

6.3.4.4 Groupement des flux de service

Des sous-flux peuvent être ajoutés aux flux de service existants au moyen du mécanisme défini au § 6.3.4.1. En outre, des sous-flux peuvent être transférés d'un flux de service existant dans un nouveau flux de service au moyen du mécanisme défini au § 6.3.4.2. Toutefois, pour faciliter l'implémentation, un flux de service existant NE DOIT PAS être transféré dans un autre flux de service existant sous la forme d'un sous-flux.

D'autre part, le MTA NE DOIT PAS tenter de partager des ressources de flux de service sauf sous la direction du serveur CMS moyennant l'inclusion de l'ID de ressource.

7 Description de l'interface d'autorisation (pkt-q6)

Le présent paragraphe décrit les interfaces entre le système CMTS et le contrôleur de porte dans le but d'autoriser l'adaptateur MTA à recevoir une qualité de service élevée. De la signalisation est nécessaire entre le contrôleur de porte et le système CMTS pour prendre en charge la gestion de portes et le service de contrôle d'admission de la QS IPCablecom. De plus, une facturation précise de l'abonné nécessite que le système CMTS indique l'utilisation des ressources effectivement "engagées" sur la base de la session. Le présent paragraphe décrit l'utilisation du protocole COPS pour le transport de messages définis de QS IPCablecom entre le contrôleur de porte et le CMTS.

7.1 Les portes: un cadre pour le contrôle de QS

Une "porte" de QS dynamique IPCablecom est une entité de contrôle de politique implémentée au niveau du système CMTS pour contrôler l'accès à des services de QS améliorés d'un réseau DOCSIS par un seul flux IP. Les portes sont unidirectionnelles, en ce qu'une seule porte contrôle l'accès à un flux soit dans le sens amont soit dans le sens aval. Les portes permettent la création de classeurs de flux de service, qui contrôlent l'acheminement de paquets sur les flux de service.

Alors qu'une porte a également un N-tuple tout comme un classeur, elle n'est pas identique à un classeur. Le système CMTS DOIT établir la porte lorsqu'un flux est autorisé, jusqu'à ce qu'elle soit explicitement désactivée pour terminer l'autorisation pour un flux. Un classeur DOCSIS PEUT être établi et associé à une porte. Une porte PEUT exister avant et après que le classeur qu'elle autorise existe. Une porte PEUT être considérée comme associée à exactement zéro, un ou deux classeurs.

Un système CMTS conforme à la présente Recommandation NE DOIT PAS créer dynamiquement une demande ou réponse d'ajout de service dynamique (DSA) DOCSIS à moins d'y être autorisé par l'existence d'une porte pour ce classeur. Un identifiant, appelé l'ID de porte est associé aux portes. L'ID de porte, administré localement par le système CMTS où la porte existe, PEUT être associé à une ou plusieurs portes unidirectionnelles. Pour une session point à point, généralement deux portes unidirectionnelles existent, associées à un seul ID de porte. De plus, des classeurs DOCSIS existent pour chaque flux unidirectionnel qui est établi.

7.1.1 Classeur

Un classeur est un tuple de 6 données:

- sens (amont/aval);
- protocole;
- source IP;

- destination IP;
- port de destination;
- port de source.

S'il existe un flux amont et un flux aval associé (faisant partie de la même session), il DOIT alors exister des classeurs séparés pour le flux amont et le flux aval. Le classeur est mis à jour par la réservation effectuée pour les flux amont et aval. Le flux de données de la session DOIT correspondre au classeur pour recevoir la qualité de service associée à la réservation.

Le système CMTS DOIT appliquer les filtres de classement de paquets amont pour les flux de service IPCablecom. C'est-à-dire que le système CMTS DOIT éliminer les paquets amont qui ne correspondent pas à l'ensemble des classeurs de paquets amont pour le flux de service.

Le filtrage de classement des paquets amont est une exigence optionnelle du système CMTS dans les réseaux DOCSIS 1.1. La présente Recommandation demande son implémentation pour les flux de service utilisés pour transporter les flux de média IPCablecom. Si un CMTS choisit d'appliquer des filtres de classement amont uniquement sur les flux de service IPCablecom et non sur les autres flux de service, le mode de détermination des flux de service IPCablecom particuliers est une décision spécifique du fabricant du système CMTS. Ce système pourrait, par exemple, se fixer pour politique de n'appliquer le classement des paquets amont qu'aux flux de service amont non primaires.

7.1.2 Porte

Une porte est associée à un flux unidirectionnel et comprend les données suivantes:

- ID de porte (*Gate-ID*).
- Classeur de prototype.
- Différents bits fanions décrits ci-dessous.
- Enveloppe autorisée (Spec de flux).
- Enveloppe réservée (Spec de flux).
- ID de ressource.

L'ID de porte (décrit ci-dessous) est un identifiant de 32 bits qui est alloué à partir de l'espace local au niveau du système CMTS où la porte réside. Jusqu'à deux portes PEUVENT partager le même ID de porte. Généralement, un ID de porte identifiera un seul flux amont et un seul flux aval et correspondra à une seule session multimédia.

Le classeur prototype se compose des six mêmes éléments qu'un classeur, comme décrit ci-dessus. La Source IP est l'adresse IP (telle qu'elle est vue au système CMTS) de l'émetteur du flux. Dans le cas d'une porte amont sur le canal DOCSIS, la Source IP est l'adresse IP de l'adaptateur MTA local. Pour le flux aval, l'adresse de la Source IP est l'adresse IP du MTA distant. Pour les paramètres choisis d'un classeur prototype de porte, un caractère générique est permis. Dans la signalisation d'appel multimédia, le port UDP de source n'est pas signalé, de sorte que sa valeur n'est pas considérée comme faisant partie des informations d'une porte.

Le port de source PEUT avoir recours à un caractère générique, pour prendre en charge les deux protocoles de signalisation d'appel IPCablecom (DCS et la Rec. UIT-T J.162). Si le port de source utilise un caractère générique, sa valeur dans les paramètres de la porte sera zéro.

L'adresse IP de source PEUT utiliser un caractère générique, pour prendre en charge le protocole de signalisation d'appel J.162. Si l'adresse IP de source utilise un caractère générique, sa valeur dans les paramètres de la porte sera zéro.

L'enveloppe autorisée et l'enveloppe réservée sont des portions des spécifications de flux (*FlowSpec*) de RSVP (TSpec et RSpec), telles que décrites dans les paragraphes précédents.

Une demande de réservation de ressources (telle que spécifiée dans un message d'ajout/changement de flux de service dynamique) DOIT être vérifiée par rapport à ce qui a été autorisé pour l'ID de porte associé au sens pour la demande de ressources. Les ressources autorisées sont spécifiées dans l'enveloppe autorisée. Le caractère générique est également vérifié dans la porte pour les entrées particulières.

L'ID de ressources est un identifiant local de 32 bits qui est alloué à partir de l'espace local au niveau du système CMTS où la porte réside. N'importe quel nombre de portes PEUT partager un identifiant de ressources et partager par conséquent un ensemble de ressources communes, à la restriction près que dans chaque sens seule une de ces portes a des ressources engagées.

7.1.3 Identification de porte

Un ID de porte est un identifiant unique qui est localement alloué par le système CMTS où la porte réside. L'ID de porte est un identifiant de 32 bits. Un ID de porte PEUT être associé à une ou plusieurs portes. Dans les protocoles d'appel de signalisation J.162 et DCS, un ID de porte est associé à chaque tronçon de l'appel et se compose d'une seule porte amont et d'une seule porte aval.

Un ID de porte DOIT être associé aux informations suivantes:

- une ou deux portes, qui DOIVENT être l'une des combinaisons suivantes:
  - porte amont seule;
  - porte aval seule;
  - porte amont seule et porte aval seule;
- informations de comptabilité et de facturation:
  - adresse: port du serveur d'archivage primaire qui devrait recevoir les enregistrements d'événements;
  - adresse: port du serveur d'archivage secondaire, à utiliser si le serveur primaire est indisponible;
  - fanion indiquant si les messages d'événement doivent être envoyés au serveur d'archivage en temps réel ou s'ils doivent être regroupés par lot et envoyés à intervalles périodiques;
  - identifiant de corrélation de facturation, qui sera transmis au serveur d'archivage avec chaque enregistrement d'événement;
  - informations de facturation supplémentaires, si elles sont fournies, qui seront utilisées pour générer des messages d'événement Réponse d'appel et Appel déconnecté;
  - l'omission d'informations de génération d'événements (c'est-à-dire de l'objet Information de génération d'événement) implique que la génération de message d'événement NE DOIT PAS être effectuée par une porte.

L'ID de porte DOIT être unique parmi toutes les portes courantes allouées par le système CMTS. La valeur de la quantité de 32 bits NE DOIT PAS être choisie dans un ensemble de petits entiers, étant donné que la possession de la valeur d'ID de porte est un élément clé de l'authentification des messages Engagement en provenance du MTA. Un algorithme qui PEUT être utilisé pour allouer des valeurs d'ID de porte est le suivant: diviser le mot de 32 bits en deux parties, une partie indice et une partie aléatoire. La partie indice identifie la porte en indexant une petite table, tandis que la partie aléatoire fournit un certain niveau d'obscurité à la valeur. Indépendamment de l'algorithme choisi, le système CMTS DEVRAIT essayer de minimiser les possibilités d'ambiguïté de l'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 précédemment, ceci pourrait être fait en incrémentant simplement la partie indice de chaque ID de porte alloué successivement, avec retour à zéro lorsque la valeur d'entier maximale de la partie indice est atteinte.

7.1.4 Schéma de transition des portes

Les portes sont considérées comme ayant les états suivants:

- alloué – l'état initial de la porte créée à la demande du GC;
- autorisé – le GC a autorisé le flux avec des limites de ressources définies;
- réservé – les ressources ont été réservées pour le flux;
- engagé – les ressources sont en cours d'utilisation.

Le système CMTS DOIT prendre en charge les états et les transitions de porte comme indiqué à la Figure 9 et décrit dans le présent paragraphe. Toutes les portes allouées au même ID de porte par le système CMTS DOIVENT transiter ensemble par les états indiqués à la Figure 9. Ceci est vrai même lorsqu'un seul des flux amont/aval est autorisé à acheminer du trafic. Dans un but de simplicité, le diagramme de transition de portes de la Figure 9 ne décrit pas complètement toutes les transitions qui doivent être implémentées, bien que toutes les transitions incluses doivent être implémentées comme indiqué.

Une porte est créée dans le système CMTS par une commande Allocation de porte ou par une commande Porte établie en provenance du GC. Dans les deux cas, le système CMTS alloue un identifiant localement unique appelé ID de porte, qui est renvoyé au GC. Si la porte a été créée par un message Porte établie, le système CMTS DOIT alors marquer la porte à l'état "Autorisé" et DOIT démarrer le temporisateur T1. Si la porte a été créée par un message Allocation de porte, le système CMTS DOIT alors marquer la porte à l'état "Alloué", démarrer le temporisateur T0 et DOIT attendre une commande Porte établie; à ce moment la porte DOIT être marquée à l'état "Autorisé". Si le temporisateur T0 expire avec la porte à l'état "Alloué" ou si le temporisateur T1 expire avec la porte à l'état "Autorisé", le système CMTS DOIT alors supprimer la porte. Le temporisateur T0 limite le temps pendant lequel l'ID de porte restera valide sans aucun paramètre de porte spécifié. Le temporisateur T1 limite le temps de validité de l'autorisation.

Une porte dans l'état "Alloué" DOIT être supprimée à réception d'un message Suppression de porte. Lorsque cela arrive, le système CMTS DOIT répondre par un message Accusé de réception de suppression de porte et DOIT arrêter le temporisateur T0. De même, une porte dans l'état "Autorisé DOIT être supprimée à réception d'un message Suppression de porte. Lorsque cela arrive, le système CMTS DOIT répondre par un message Accusé de réception de suppression de porte et DOIT arrêter le temporisateur T1.

Une porte dans l'état "Autorisé" attend que le client tente de réserver des ressources. Le client effectue cette opération via l'interface de services de contrôle MAC. A réception de cette demande de réservation, le système CMTS DOIT vérifier que la demande se trouve dans les limites établies pour la porte et effectuer les procédures de contrôle d'admission.

Le système CMTS DOIT implémenter au moins deux politiques de contrôle d'admission, une pour les communications vocales normales, une pour les communications d'urgence. Ces deux politiques DOIVENT avoir des paramètres provisionnables qui spécifient, au minimum:

1) une quantité de ressources maximale qui peut être allouée non exclusivement à des sessions de ce type (cette quantité peut être 100% de la capacité);
2) la quantité de ressources qui peut être allouée exclusivement aux sessions de ce type (cette quantité peut être 0% de la capacité);
3) la quantité maximale de ressources qui peut être allouée aux sessions des deux types.

La politique de contrôle d'admission PEUT également spécifier si une nouvelle session de ce type peut "emprunter" aux classes de priorité inférieure ou devrait éliminer une session existante d'un autre type pour satisfaire aux réglages de la politique de contrôle d'admission.

Si la demande de réservation est destinée à ajouter un sous-flux à un flux de service existant, l'ID de classe de session pour la porte DOIT correspondre à l'ID de classe de session de toutes les portes des sous-flux restants qui forment déjà le flux de service recherché. Si la classe de session de toutes

les portes des sous-flux ne correspond pas, le système CMTS DOIT alors rejeter la demande de réservation.

Si les procédures de contrôle admission réussissent, et que seule une réservation de ressources était demandée, la porte DOIT être marquée à l'état "Réservé". Si les procédures de contrôle d'admission réussissent et que la réservation et l'engagement de ressource à étape unique était demandée, la porte DOIT être marquée à l'état "Engagé" et le système CMTS DOIT envoyer un message Porte ouverte au contrôleur de porte et arrêter le temporisateur T1.

Si les procédures de contrôle d'admission ne réussissent pas, la porte DOIT rester dans l'état "Autorisé".

Il est à noter que la réservation effective effectuée par le client peut porter sur un nombre de ressources inférieur autorisé par exemple, réservation pour l'amont uniquement lorsqu'une paire de portes a été établie en autorisant les flux amont et aval.

Dans l'état "Réservé" la porte attend que le client engage les ressources, les activant ainsi. La commande Engagement en provenance du client est une transaction concluante de demande d'activation d'un flux de service via l'interface de services de contrôle MAC. Si la porte est encore à l'état "Réservé" et que le temporisateur T1 arrive à expiration (c'est-à-dire que le client n'émet pas la commande Engagement), le système CMTS DOIT libérer toutes les ressources réservées et supprimer la porte. Si un message Suppression de porte est reçu dans l'état "Réservé", le système CMTS DOIT répondre avec un message Accusé de réception de suppression de porte, DOIT libérer toutes les ressources associées à la porte, et DOIT arrêter le temporisateur T1.

Pour les besoins de ce diagramme de transition d'état, un "Engagement" provenant du client est un message qui engage le flux amont. Si le CMTS reçoit une demande asymétrique telle que le trafic puisse passer sur le flux aval mais pas sur le flux amont, le système CMTS NE DOIT PAS sortir de l'état "Réservé". Si d'un autre côté, le système CMTS reçoit une demande asymétrique telle que le trafic puisse passer sur le flux amont mais pas sur le flux aval, le système CMTS DOIT traiter la demande comme un engagement et doit changer son état conformément à la description ci-dessous.

Pour les besoins de ce diagramme de transition d'état, un message "Suppression" provenant du client est un message qui supprime le flux amont. Si le CMTS reçoit une demande asymétrique telle que le flux aval soit supprimé mais pas le flux amont, le système CMTS NE DOIT PAS sortir de l'état dans lequel il se trouve. Si d'un autre côté, le système CMTS reçoit une demande asymétrique telle que le flux amont soit supprimé mais pas le flux aval, le système CMTS DOIT traiter la demande comme un une suppression et doit changer son état conformément aux règles de transition des portes.

Si le temporisateur T0 arrive à expiration au CMTS avant de recevoir une commande Porte établie du serveur CMS, le CMTS DOIT initialiser un message Porte fermée en utilisant "Expiration du temporisateur T0; pas de Porte établie reçu du CMS" comme code de cause, et détruire la porte associée.

Si le temporisateur T1 arrive à expiration au système CMTS avant de recevoir une commande Engagement de l'adaptateur MTA, le système CMTS DOIT initialiser un message Porte fermée en utilisant "Expiration du temporisateur T1; pas d'Engagement reçu du MTA" comme code de cause, et détruire la ou les portes associées.

Si, dans l'état "Réservé", le système CMTS reçoit une commande Engagement provenant du client, le système CMTS DOIT marquer la porte dans l'état "Engagé", arrêter le temporisateur T1, et lancer un message Porte ouverte.

Si le temporisateur T7 arrive à expiration alors que le MTA utilise le paramètre "Plusieurs allocations par intervalle" et qu'un sous-flux du flux de service correspondant à la ou aux portes référencées via l'ID de porte associé n'a pas été engagé sur le CMTS, celui-ci DOIT lancer un message Porte fermée en utilisant "Expiration du temporisateur T7; fin du temps de réservation de

flux de service" comme code de cause, et détruire la ou les portes associées. Autrement, le système CMTS DOIT établir l'enveloppe réservée égale à l'enveloppe engagée pour les flux correspondants aux portes référencées via l'ID de porte associé.

Si le temporisateur T7 arrive à expiration alors qu'un MTA n'utilise pas le paramètre "Plusieurs allocations par intervalle" et qu'un flux de service correspondant à la ou aux portes référencées via l'ID de porte associé n'a pas été engagé sur le CMTS, celui-ci DOIT lancer un message Porte fermée en utilisant "Expiration du temporisateur T7; fin du temps de réservation de flux de service" comme code de cause, et détruire la ou les portes associées. Autrement, le système CMTS DOIT établir l'enveloppe réservée égale à l'enveloppe engagée pour les flux correspondants aux portes référencées via l'ID de porte associé.

Si le temporisateur T8 arrive à expiration au système CMTS du fait de l'inactivité du flux de service, le système CMTS DOIT lancer un message Porte fermée pour chaque porte associée au flux en utilisant "Expiration du temporisateur T8; inactivité du flux de service dans le sens amont" comme code de cause, et détruire la porte associée.

Une fois dans l'état "Engagé", la porte a atteint une configuration stable. Les ressources ont été activées aux portes locales. Les ressources continueront à être activées jusqu'à ce que le client local indique une commande de libération, le temporisateur actif arrive à expiration ou le serveur CMS envoie une commande Suppression de porte.

Si, dans l'état "Engagé", le système CMTS reçoit une commande Libération en provenance du client, via l'interface de services de contrôle MAC, ou d'une défaillance du client à rafraîchir une réservation, ou encore de mécanismes DOCSIS internes qui détectent une défaillance du client, le système CMTS DOIT désactiver toutes les ressources engagées pour le client, libérer toutes les ressources réservées, envoyer un message Porte fermée à l'entité de coordination de porte et supprimer la porte.

Si, à l'état "Engagé", le système CMTS reçoit un message Suppression de porte, le système CMTS DOIT désactiver toutes les ressources engagées pour le client local, libérer toutes les ressources réservées et supprimer la porte. De plus, le système CMTS doit répondre par un message Accusé de réception de suppression de porte.

Pendant qu'il est dans l'état "Engagé", le système CMTS DOIT permettre au client d'initialiser des changements dans la réservation ou l'activation de ressources, dans les limites du contrôle d'autorisation et d'admission locale.

7.1.5 Coordination de porte

Les messages de coordination de porte à l'interface Contrôle de porte COPS, Porte ouverte et Porte fermée, fournissent un mécanisme de rétro-contrôle non sollicité du système CMTS vers le serveur CMS afin de maintenir la synchronisation d'état entre ces éléments. Ceci est particulièrement utile dans le cas de demande de réservation ou d'engagement prématurée à l'initiative de l'adaptateur MTA qui n'est pas stimulé par le serveur CMS ou dans l'éventualité d'une défaillance du MTA, ce qui provoque la récupération de ressources au niveau du système CMTS. Dans ces deux scénarios possibles, l'état interne maintenu au sein du serveur CMS sera mis à jour pour refléter le changement d'état survenu au système CMTS et le serveur CMS sera à même de prendre l'action appropriée sur la base de ces informations.

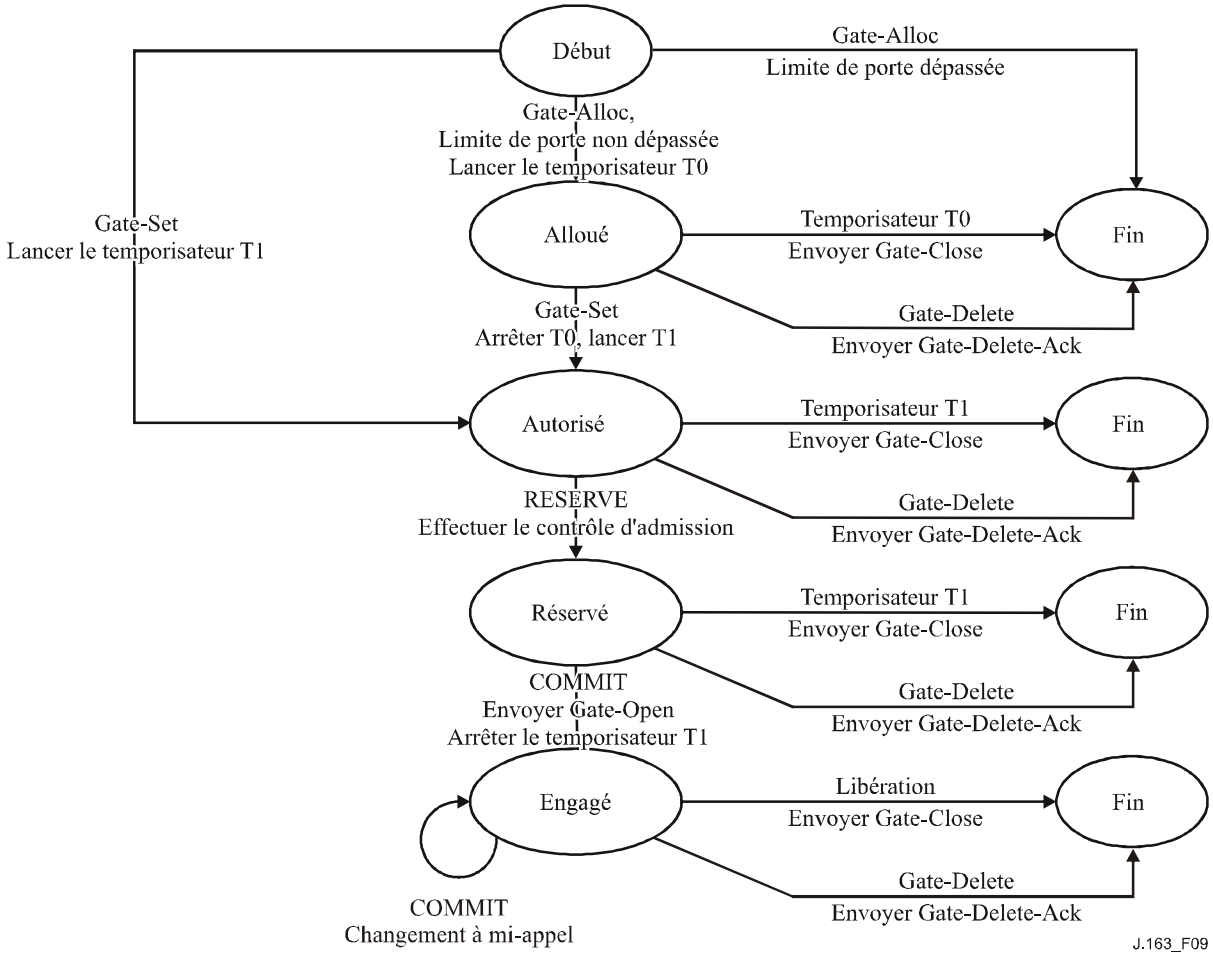


Figure 9/J.163 – Schéma de transition d'états de porte

7.2 Profil COPS pour IPCablecom

Le contrôle d'admission de QS IP est l'acte de gestion de l'allocation de ressources de QS à partir des politiques administratives et des ressources disponibles. Le service de contrôle d'admission de la QS IP utilise une architecture client/serveur. Les modules opérationnels de haut niveau sont décrits à la Figure 10. Les politiques administratives sont stockées dans des bases de données de politique et contrôlées par le serveur COPS. Alors qu'une implémentation IntServ typique du protocole COPS laisse le serveur déterminer les ressources disponibles, une implémentation DiffServ repousse la politique chez le client, de sorte que le client peut prendre les décisions de contrôle d'admission.

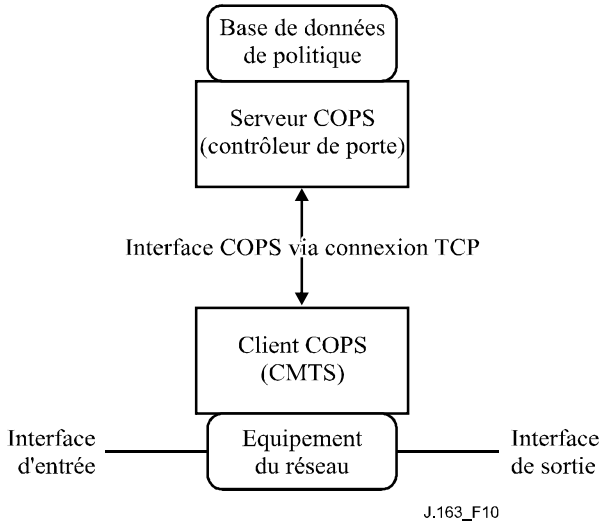


Figure 10/J.163 – Disposition du contrôle d'admission de la QS

Les décisions de contrôle d'admission de la QS prises par le serveur COPS DOIVENT passer au client COPS en utilisant COPS. Le client COPS PEUT faire des demandes de contrôle d'admission de la QS au serveur COPS en se fondant sur les événements du réseau déclenchés soit par le protocole de signalisation de la QS, soit via les mécanismes de détection de flux de données. L'événement de réseau peut également être le besoin de gestion de bande passante de la QS, par exemple une nouvelle interface compatible avec la QS devient opérationnelle.

Les décisions de politique de la QS prises par le serveur COPS PEUVENT être repoussées chez le client COPS en se fondant sur une demande de service de QS externe, hors bande, par exemple, une demande en provenance du système CMTS de terminaison ou d'un contrôleur de porte. Ces décisions de politique PEUVENT être stockées par le client COPS dans un point de décision de politique local et le système CMTS peut accéder à ces informations de décision pour prendre des décisions de contrôle d'admission sur des demandes de session entrantes reçues au système CMTS.

La prise en charge de l'interaction client COPS-serveur COPS pour le contrôle d'admission de la QS est fourni par le protocole COPS de l'IETF. Le protocole COPS inclut les opérations suivantes:

- client ouvert (OPN, *client-open*)/client accepté (CAT, *client-accept*)/client fermé (CC, *client-close*): le client COPS envoie un message OPN pour initialiser une connexion avec le serveur COPS et le serveur répond avec un message CAT pour accepter la connexion. Le serveur envoie un message CC pour terminer la connexion avec le client;
- demande (REQ, *request*): le client COPS envoie un message REQ au serveur pour demander des informations sur la décision de contrôle d'admission ou des informations sur la configuration de dispositifs. Le message REQ contient des informations spécifiques du client que le serveur utilise, avec les données contenues dans la base de données de politique d'admission de la session, pour prendre des décisions fondées sur la politique;
- décision (DEC): le serveur répond aux REQ en renvoyant 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 DEC demandé) ou à tout moment ultérieur pour changer/mettre à jour une décision précédente (c'est-à-dire un DEC non sollicité);
- rapport d'état (RPT, *report state*): le client COPS envoie un message RPT au serveur COPS en indiquant les changements à l'état de la demande dans le client COPS. Le client COPS envoie ce message pour informer le serveur COPS des ressources réelles réservées après que le serveur COPS a accordé l'admission. Le client COPS peut également utiliser Report State pour informer périodiquement le serveur COPS de l'état courant du client COPS;

- supprimer rapport d'état (DEL, *delete request state*): le client COPS envoie un message DEL au serveur COPS pour un nettoyage de l'état de la demande. Ceci peut être le résultat d'une libération de ressources de QS par le client COPS;
- garder en vie (KA, *keep alive*): envoyé par le client COPS et par le serveur COPS pour la détection de défauts de communication;
- demande d'état de synchronisation (SSR, *synchronize state request*)/état de synchronisation terminé (SSC, *synchronize state complete*): SSR est envoyé par le serveur COPS pour demander des informations sur l'état en cours du client COPS. Le client renvoie les interrogations de demande au serveur pour effectuer la synchronisation puis le client envoie un message SSC pour indiquer que la synchronisation est effectuée. Etant donné que le GC est sans état, les opérations SSR/SSC n'ont pas d'importance dans IPCablecom et ne sont pas utilisées par le système CMTS ou le GC.

Dans l'architecture IPCablecom, le contrôleur de porte est une entité de point de décision de politique (PDP) de COPS et le système CMTS est l'entité qui est le point d'application de la politique (PEP, *policy enforcement point*) de COPS.

Les détails du protocole COPS sont fournis dans le projet RFC 2748. Ce projet de RFC 2748 de l'IETF fait la description du protocole COPS de base, indépendant du type de client. Des projets additionnels fournissent des informations pour l'utilisation du protocole COPS pour les services intégrés avec le protocole RSVP et pour les services différenciés (c'est-à-dire approvisionnant les clients). Un aperçu plus détaillé du protocole COPS est fourni à titre informatif à l'Appendice X.

7.3 Formats des messages du protocole de contrôle des portes

Les messages du protocole pour le contrôle des portes sont transportés dans les messages du protocole COPS. Le protocole COPS utilise une connexion TCP établie entre le système CMTS et le contrôleur de porte et utilise les mécanismes spécifiés dans la Rec. UIT-T J.170 pour sécuriser le trajet de communication.

7.3.1 Format du message commun COPS

Chaque message COPS se compose de l'en-tête COPS suivi d'un certain nombre d'objets typés. Le contrôleur de porte et le système CMTS DOIVENT prendre en charge l'échange de messages COPS tel que défini ci-dessous (voir Figure 11):

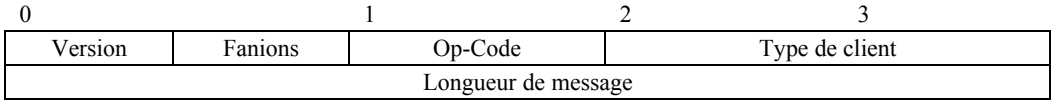


Figure 11/J.163 – En-tête de message COPS commun

Version est un champ de 4 bits donnant le numéro de la version COPS en cours. Il DOIT être mis à 1.

Fanions est un champ de 4 bits. 0x1 est le fanion du message sollicité. Lorsqu'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 les autres cas (par exemple, une décision non sollicitée) le fanion NE DOIT PAS être établi (valeur = 0). Tous les autres fanions DOIVENT être mis à 0.

Op-code est un champ d'un octet qui donne l'opération COPS à exécuter. Les opérations COPS utilisées dans la présente spécification IPCablecom sont les suivantes:

1 = Demande (REQ)

2 = Décision (DEC)

3 = Rapport d'état (RPT)

6 = Client ouvert (OPN)

7 = Client accepté (CAT)

9 = Garder en vie (KA)

Type de client (*C-type*) est un identifiant de 16 bits. Pour l'utilisation d'IPCablecom, le type de client DOIT être réglé à client IPCablecom (0x8008). Pour les messages Garder en vie (Op-code = 9), le type de client DOIT être réglé à zéro, car le KA est utilisé pour la vérification de la connexion plutôt qu'à une vérification de session par client.

Longueur de message est une valeur de 32 bits donnant la taille du message en octets. Les messages DOIVENT être alignés sur les limites de 4 octets, de sorte que la longueur DOIT être un multiple de quatre.

Un nombre variable d'objets suivent l'en-tête commun COPS. Tous les objets adoptent le même format d'objet. Chaque objet se compose d'un ou plusieurs mots de 32 bits avec un en-tête de quatre octets, utilisant le format suivant (voir la Figure 12):

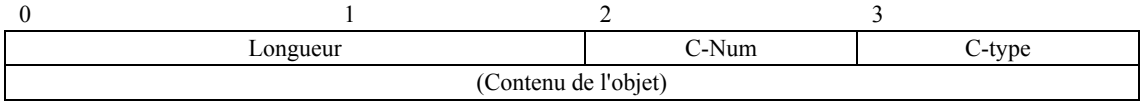


Figure 12/J.163 – Format d'objet COPS commun

La longueur est une valeur de deux octets qui DOIT donner le nombre d'octets (y compris l'en-tête) qui composent l'objet. Si la longueur en octets n'est pas un multiple de quatre, un bourrage DOIT être ajouté à la fin de l'objet de sorte qu'il soit aligné sur la limite suivante de 32 bits. Du côté de la réception, une limite d'objet subséquente DOIT être trouvée en arrondissant la longueur de l'objet précédent défini à la limite suivante de 32 bits.

C-Num identifie la classe d'information contenue dans l'objet et C-Type identifie le sous-type ou la version de l'information contenue dans l'objet. Les objets COPS standards (tels que définis dans le projet RFC 2748 utilisés dans la présente Recommandation et leurs valeurs de C-Num, sont les suivants:

1 = Handle (*Outil*)

6 = Decision (*Décision*)

8 = Error (*Erreur*)

9 = Client Specific Info (*Information spécifique sur le client*)

10 = Keep-Alive-Timer (*Temporisateur de repos*)

11 = PEP Identification (*Identification PEP*)

7.3.2 Objets COPS supplémentaires pour le contrôle de portes

Comme avec les types de client COPS-PR et COPS-RSVP, le type de client IPCablecom définit un certain nombre de formats d'objets. Ces objets DOIVENT être placés à l'intérieur d'un objet Décision, C-Num = 6, C-Type = 4 (Données de décision spécifique du client) lorsqu'ils sont transportés du GC au système CMTS dans un message de décision. Ils DOIVENT également être placés dans un objet ClientSI, C-Num = 9, C-Type = 1 (SI de client signalé) lorsqu'ils sont transportés du système CMTS au GC dans un message Rapport. Ils sont codés de manière similaire aux objets spécifiques du client pour COPS-PR. Les codages détaillés sont indiqués ci-dessous. Comme dans COPS-PR, ces objets sont numérotés en utilisant un espace de nombre spécifique du client, qui est indépendant de l'espace de nombre de l'objet COPS de niveau élevé. Pour cette raison, les numéros et les types d'objet sont donnés respectivement comme S-Num et S-Type.

Les objets COPS supplémentaires définis pour être utilisés par IPCablecom sont les suivants:

7.3.2.1 ID de transaction

L'objet ID de transaction contient un jeton qui est utilisé par le GC pour faire correspondre les réponses en provenance du système CMTS aux demandes précédentes et le type de commande qui identifie l'action à prendre ou la réponse.

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

Identifiant de transaction a une longueur de 16 bits qui PEUT être utilisée par le GC pour faire correspondre les réponses avec les commandes.

Le type de commande de porte DOIT être l'un des suivants:

Gate-Alloc (*allocation de porte*)	1
Gate-Alloc-Ack (*accusé de réception d'allocation de porte*)	2
Gate-Alloc-Err (*erreur d'allocation de porte*)	3
Gate-Set (*porte établie*)	4
Gate-Set-Ack (*accusé de réception de porte établie*)	5
Gate-Set-Err (*erreur de porte établie*)	6
Gate-Info (*informations de porte*)	7
Gate-Info-Ack (*accusé de réception d'informations de porte*)	8
Gate-Info-Err (*erreur d'informations de porte*)	9
Gate-Delete (*suppression de porte*)	10
Gate-Delete-Ack (*accusé de réception de suppression de porte*)	11
Gate-Delete-Err (*erreur de suppression de porte*)	12
Gate-Open (*porte ouverte*)	13
Gate-Close (*porte fermée*)	14

7.3.2.2 Identifiant d'abonné

L'objet ID d'abonné identifie l'abonné pour cette demande de service. Sa principale utilisation est d'empêcher différentes attaques de déni de service.

Longueur = 8	S-Num = 2	S-Type = 1
Adresse IPv4 (32 bits)		

ou:

Longueur = 20	S-Num = 2	S-Type = 2
Adresse IPv6 (128 bits)		

7.3.2.3 ID de porte

Cet objet identifie la porte ou un ensemble de portes référencées dans le message de commande ou allouées par le système CMTS pour un message de réponse.

Longueur = 8	S-Num = 3	S-Type = 1
ID de porte (32 bits)		

7.3.2.4 Compte d'activité

Lorsqu'il est utilisé dans un message Gate-Alloc, cet objet spécifie le nombre maximal de portes qui peuvent être simultanément allouées à l'ID d'abonné indiqué. Cet objet renvoie, dans un message Gate-Set-Ack ou Gate-Alloc-Ack, le nombre de portes allouées à un seul abonné. Il est utile pour empêcher les attaques de déni de service.

Longueur = 8	S-Num = 4	S-Type = 1
Compte (32 bits)		

7.3.2.5 Spécification de porte

Longueur = 60		S-Num = 5	S-Type = 1
Direction	ID de protocole	Fanions	Classe de session
Adresse IP de source (32 bits)			
Adresse IP de destination (32 bits)			
Port de source (16 bits)		Port de destination (16 bits)	
Valeur du temporisateur T1		Réservé	
Valeur du temporisateur T7		Valeur du temporisateur T8	
Débit du seau de jetons [r] (nombre à virgule flottante IEEE de 32 bits)			
Taille du seau de jetons [b] (nombre à virgule flottante IEEE de 32 bits)			
Débit de crête de données (p) (nombre à virgule flottante IEEE de 32 bits)			
Unité régulée minimale [m] (entier de 32 bits)			
Taille maximale de paquet [M] (entier de 32 bits)			
Débit [R] (nombre à virgule flottante IEEE de 32 bits)			
Terme de surlongueur [S] (entier de 32 bits)			

La direction est soit 0 pour une porte aval, soit 1 pour une porte amont.

ID de protocole est la valeur à atteindre dans l'en-tête IP ou zéro en cas de non-correspondance.

Les fanions sont définis comme suit:

0x01 les fonctions Auto-Commit et Commit-Not-Allowed qui étaient précédemment signalées au moyen des champs de fanions ont été désapprouvées. Il en résulte que les bits un et deux sont réservés.

Tous les bits DOIVENT être à zéro.

Classe de session identifie la politique de contrôle d'admission correcte ou les paramètres à appliquer pour cette porte. Les valeurs permises sont les suivantes:

0x00 non spécifié.

0x01 session VoIP à priorité normale.

0x02 session VoIP à priorité élevée (par exemple, E911).

Toutes les autres valeurs sont actuellement réservées.

Adresse IP de source et adresse IP de destination constituent une paire d'adresses IPv4 de 32 bits ou zéro pour la non-correspondance (c'est-à-dire, la spécification d'un caractère générique qui correspondra à toute demande en provenance du MTA).

Port de source et port de destination définissent un couple de valeurs de 16 bits, ou zéro en cas de non-correspondance.

Les valeurs r, b, p, m, M et R, sont décrites au § 6.1. Au lieu du terme de surlongueur défini dans le document RFC du protocole RSVP, la valeur S représenterait, en microsecondes, la gigue d'allocation admise minimale qui peut être admise dans la direction amont, et le délai admis minimal dans la direction aval qui peut être admis.

D'autres paragraphes donnent des prescriptions normatives qui représentent des contraintes sur l'enveloppe d'autorisation qui est définie par ces paramètres. Spécifiquement, la discussion sur le codec multiple du § 5.6.10 définit une limite supérieure sur l'enveloppe d'autorisation, alors que le § 7.5 plus loin dans le présent paragraphe donne un ensemble d'exigences minimales pour ces paramètres. Il est fortement recommandé que les implémentations de serveurs CMS tiennent autant que possible les paramètres d'autorisation car leur tenue est fondamentale pour la définition et l'application des politiques de gestion de la bande passante des fournisseurs de service.

Le champ DS est défini par la structure suivante:

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

Le document RFC 2474 définit le champ *Services différenciés* (DS) comme étant un gabarit binaire en deux parties: un point de code de services différenciés (DSCP) de 6 bits et 2 bits réservés. Le document RFC 3168 définit les 2 bits réservés comme devant être utilisés pour la notification explicite d'encombrement (ECN, *explicit congestion notification*). Ces bits sont utilisés par des routeurs pour la notification d'encombrement et la gestion active de file d'attente. Le serveur CMS DOIT mettre les bits 6 et 7 du champ DS à zéro. Si ces bits ne sont pas mis à zéro, le système CMTS DOIT répondre au message *Porte établie* par un message *Erreur d'informations de porte* avec un code d'erreur de 8 (valeur de champ DS illégale).

Pour la compatibilité amont avec les implémentations de système courantes et l'utilisation de la préséance IP telle que définie dans les documents RFC 2474 et RFC 791 de l'IETF, les bits appropriés de l'octet Type de service (TOS) d'IPv4 représentés ci-dessous PEUVENT être insérés dans le champ DS. Toutefois, la restriction applicable au réglage des bits 6 et 7 reste applicable. Le champ IP TOS (bits 3-6) n'est pas pris en charge dans les réseaux DiffServ.

0	1	2	3	4	5	6	7
Préséance IP			Type de service IP d'IPv4				Non utilisé

Le temporisateur T1 est donné en secondes, et utilisé dans le diagramme de transition de porte décrit au § 7.1.4. Si des objets Gate-Spec apparaissent dans un seul message COPS, les valeurs de T1 DOIVENT être identiques dans toutes les occurrences de Gate-Spec. Si les valeurs de T1 diffèrent entre les objets Gate-Spec de sens amont et de sens aval, le système CMTS DOIT alors utiliser la valeur de T1 spécifiée dans la GateSpec amont pour gérer la paire de portes.

Les temporisateurs T7 et T8 sont des valeurs en secondes et sont utilisés pour commander la temporisation DOCSIS pour respectivement les Paramètres de QS admis et les Paramètres de QS actifs.

7.3.2.6 Info de porte distante

Cet objet n'est plus valide. S-Num 6 est réservé pour empêcher tout malentendu.

Longueur 36	S-Num = 6	S-Type = 1
Adresse IP du CMTS (32 bits)		
Port du CMTS (16 bits)	Fanions, définis ci-dessous	
ID de porte distante		
Algorithme	Réservé	
Clé de sécurité (16 octets)		

7.3.2.7 Info de génération d'événement

Cet objet contient toutes les informations nécessaires pour prendre en charge les messages d'événement tels que spécifiés et requis dans la Rec. UIT-T J.164.

Longueur = 44	S-Num = 7	S-Type = 1
Adresse IP du serveur d'archivage primaire (32 bits)		
Port du serveur d'archivage primaire	Fanions, voir ci-dessous	Réservé
Adresse IP du serveur d'archivage secondaire (32 bits)		
Port du serveur d'archivage secondaire	Réservé	
Identifiant de corrélation de facturation (24 octets)		

L'Adresse IP du serveur d'archivage primaire est l'adresse du serveur d'archivage auquel les enregistrements d'événements sont envoyés.

Le Port du serveur d'archivage primaire est le numéro de port pour les enregistrements d'événements envoyés.

Les valeurs de fanion sont les suivantes:

0x01 indicateur de traitement par lot. S'il est mis, le système CMTS DOIT accumuler les enregistrements d'événements comme partie du fichier de commande par lots et les envoyer au serveur d'archivage à intervalles périodiques. S'il n'est pas mis, le système CMTS DOIT envoyer les enregistrements d'événement au serveur d'archivage en temps réel.

Le reste est réservé et DOIT être à zéro.

L'Adresse IP du serveur d'archivage secondaire est l'adresse du serveur d'archivage secondaire auquel les enregistrements sont envoyés si le serveur d'archivage primaire est indisponible.

Le Port du serveur d'archivage secondaire est le numéro de port pour les enregistrements d'événement envoyés.

L'ID de corrélation de facturation est l'identifiant assigné par le serveur CMS pour tous les enregistrements associés à cette session.

7.3.2.8 Media-Connection-Event-Info

Cet objet n'est plus nécessaire. S-Num 8 est réservé pour prévenir tout malentendu.

7.3.2.9 Cause IPCablecom

Cet objet contient la cause de la suppression de la porte.

Longueur = 8	S-Num = 13	S-Type = 1
Code de cause	Sous-code de cause	

Les valeurs de code de cause définies dans la présente Recommandation sont les suivantes:

0: opération Suppression de porte

1: opération Porte fermée

Les sous-codes de cause sont définis de la façon suivante:

opération Suppression de porte:

0 = fonctionnement normal

1 = coordination locale de porte non achevée

2 = coordination distante de porte non achevée

3 = autorisation révoquée

4 = ouverture de porte inattendue

5 = échec local de fermeture de porte

127 = autre, erreur non spécifiée

Opération Porte fermée:

0 = libération à l'initiative du client (fonctionnement normal)

1 = réallocation de réservation (par exemple, pour une session prioritaire)

2 = défaut de maintenance de réservation (par exemple, rafraîchissement interfaces de services de contrôle MAC)

3 = défaut de réponse de couche MAC DOCSIS (par ex., maintenance de station)

4 = expiration du temporisateur T0; pas de Porte établie reçu du CMS

5 = expiration du temporisateur T1; pas d'Engagement reçu du MTA

6 = expiration du temporisateur T7; fin du délai de réservation de flux de service

7 = expiration du temporisateur T8; inactivité du flux de service en amont

127 = autre, erreur non spécifiée

7.3.2.10 Erreur IPCablecom

Objet d'erreur spécifique du client défini comme suit:

Longueur = 8	S-Num = 9	S-Type = 1
Code d'erreur	Sous-code d'erreur	

Les valeurs de code d'erreur définies dans la présente Recommandation sont les suivantes:

1 = pas de porte actuellement disponible

2 = ID de porte inconnu

3 = valeur de Classe de session illégale

4 = l'abonné a excédé le nombre limite de portes

5 = porte déjà établie

6 = objet requis manquant

7 = objet non valide

8 = valeur de champ DS illégale

127 = autre, erreur non spécifiée

Le champ Sous-code d'erreur est utilisé pour fournir plus d'informations sur l'erreur. Dans le cas des codes d'erreur 6 à 7, ce champ de 16 bits contient sous la forme de deux valeurs de 8 bits le S-Num et le S-Type de l'objet manquant ou erroné. L'ordre des valeurs S-Num et S-Type au sein du sous-code d'erreur DOIT être le même que celui du message d'origine. Dans les cas où existent de multiples alternatives valides pour le S-Type d'un objet manquant, cette portion du sous-code d'erreur devrait être mise à 0.

7.3.2.11 Paramètres de surveillance électronique

L'objet *Paramètres de surveillance électronique* contient toutes les informations nécessaires à la prise en charge de la surveillance électronique. Il PEUT être inclus dans le message *Porte établie* pour permettre la surveillance électronique. Un système CMTS DOIT accepter cet objet dans le message *Porte établie* et mettre en œuvre les mesures appropriées définies ci-dessous.

Longueur = 24	S-Num = 10	S-Type = 1
Adresse IP DF pour CDC (32 bits)		
Port DF pour CDC (16 bits)	Fanions, définis ci-dessous	
Adresse IP DF pour CCC (32 bits)		
Port DF pour CCC (16 bits)	Réservé	
ID de CCC (32 bits)		
Identifiant de corrélation de facturation (24 octets)		

L'Adresse IP DF (*delivery function, fonction de fourniture de surveillance électronique*) pour CDC est l'adresse de la fonction Fourniture de surveillance électronique à laquelle les messages d'événement doublés doivent être envoyés.

Le Port DF pour CDC est le numéro de port pour les messages d'événement doublés.

Les fanions sont définis comme suit:

0x0001 DUP-EVENT (*copie d'événement*). S'il est mis, le système CMTS DOIT envoyer une copie en double de tous les messages d'événement se rapportant à cette porte à l'Adresse IP DF pour CDC.

0x0002 DUP-CONTENT (*copie du contenu*). S'il est mis, le système CMTS DOIT envoyer des copies de tous les paquets correspondant au ou aux classeurs pour cette porte à l'Adresse IP DF pour CCC et au Port DF pour CCC. Le format adapté aux paquets interceptés est décrit ci-après.

Le reste est réservé et DOIT être mis à 0.

L'Adresse IP DF pour CCC est l'adresse de la fonction Fourniture de surveillance électronique à laquelle les messages d'événement dupliqués doivent être envoyés.

Port DF pour CCC est le numéro de port pour le contenu de l'appel dupliqué.

L'ID de CCC est l'identifiant pour les paquets de contenu d'appel dupliqué.

L'ID de corrélation de facturation est l'identifiant assigné par le serveur CMS pour tous les enregistrements associés à cette session. Voir la Rec. UIT-T J.164 pour le format. L'inclusion de l'ID de corrélation de facturation permet la remise de messages d'événement au DF sans qu'il soit nécessaire d'inclure l'objet Info de génération d'événement (voir le § 7.3.2.7). Le serveur CMS DOIT veiller à ce que les ID de corrélation de facturation soient identiques lorsque l'objet Paramètres de surveillance électronique et l'objet Info de génération d'événement sont inclus.

Les paquets copiés DOIVENT être transmis sous la forme d'un flux de datagrammes UDP/IP envoyé à l'adresse IP (adresse IP DF pour CCC) et au numéro de port (port DF pour CCC) indiqués dans l'objet Paramètres de surveillance électronique. La charge utile UDP/IP DOIT respecter le format suivant:

Tableau 2/J.163 – Charge utile des datagrammes de connexion pour le contenu de l'appel

ID de CCC (4 octets)
Informations interceptées (longueur arbitraire)

Les informations RTP interceptées respecteront le format suivant:

Tableau 3/J.163 – Informations interceptées

En-tête IP initial (20 octets)
En-tête UDP initial (8 octets)
En-tête RTP initial (longueur variable, 12-72 octets)
Charge utile initiale (longueur arbitraire)

Il est à noter que les protocoles de type autres que RTP peuvent être interceptés, pour le relais de données de télécopie T.38 (fax relay), par exemple.

7.3.2.12 Paramètre de description de session

Cet objet n'est plus utilisé; S-Num 11 est réservé pour prévenir tout malentendu.

Longueur =	S-Num = 11	S-Type = 1

7.3.3 Définition des messages de contrôle de porte

Les messages qui effectuent le contrôle de porte entre le GC et le système CMTS DOIVENT être définis et formatés comme suit. Noter que les messages du GC au système CMTS sont des messages Décision COPS et que les messages du CMTS au GC sont des messages Rapport COPS.

<Gate-Control-Cmd> := <En-tête commun COPS> <Outil>

<Contexte> <Fanions de décision>

<Données du Client>

<ClientSI-Data> := <Allocation de porte> | <Porte établie> | <Info de porte>> | <Suppression de porte>

<Gate-Control-Response> := <En-tête commun COPS> <Outil>

<Type de Rapport> <Objet du SIClient>

<ClientSI-Object> := <Accusé de réception d'allocation de porte> | <Erreur d'allocation de porte> |

<Accusé de réception d'établissement de porte> | <Erreur d'établissement de porte> |

<Accusé de réception d'informations de porte> | <Erreur d'informations de porte> |

<Accusé de réception de suppression de porte> | <Erreur de suppression de porte>

<Gate-Alloc> := <En-tête de Décision> <ID de Transaction> <ID d'abonné>> [<Compte d'Activité>]

<Gate-Alloc-Ack> := <En-tête de SIClient> <ID de Transaction> <ID d'abonné>

<ID de porte> <Compte d'Activité>

<Gate-Alloc-Err> := <En-tête de SIClient> <ID de Transaction> <ID d'abonné> <Erreur IPCablecom>

<Gate-Set> := <En-tête de Décision> <ID de Transaction> <ID d'abonné> [<Compte d'Activité>] [<ID de porte>]

[<Info de génération d'événement>]

[<Paramètres de surveillance électronique>]

<Spec de porte> [<Spec de porte>]

<Gate-Set-Ack> := <En-tête de SIClient> <ID de Transaction> <ID d'abonné>

<ID de porte> <Compte d'Activité>

<Gate-Set-Err> := <En-tête de SIClient> <ID de Transaction> <ID d'abonné> <Erreur IPCablecom>

<Gate-Info> := <En-tête de Décision> <ID de Transaction> <ID de porte>

<Gate-Info-Ack> := <En-tête de SIClient> <ID de Transaction> <ID d'abonné> <ID de porte>

[<Info de génération d'événement>][<Paramètres de surveillance électronique>]

<Spec de porte> [<Spec de porte>]

<Gate-Info-Err> := <En-tête de SIClient> <ID de Transaction> <ID de porte> <Erreur IPCablecom>

<Gate-Delete> := <En-tête de Décision> <ID de Transaction> <ID de porte> <Cause IPCablecom>

<Gate-Delete-Ack> := <En-tête de SIClient> <ID de Transaction> <ID de porte>

<Gate-Delete-Err> := <En-tête de SIClient> <ID de Transaction> <ID de porte> <Erreur IPCablecom>

<Gate-Open> := <En-tête de SIClient> <ID de Transaction> <ID de porte>

<Gate-Close> := <En-tête de SIClient> <ID de Transaction> <ID de porte> <Cause IPCablecom>

L'objet Contexte (C-NUM = 2, C-TYPE = 1) dans le message Décision COPS a la valeur R-Type (fanion de type de demande) réglée à 0x08 (demande de configuration) et la valeur M-Type réglée à zéro. Le champ Code de commande dans l'objet obligatoire Fanions de décision (C-NUM = 6, C-TYPE = 1) est réglé à 1 (configuration d'installation). D'autres valeurs amèneraient le système CMTS à générer un message Rapport indiquant l'échec. L'objet Type de rapport (C-NUM = 12, C-TYPE = 1) inclus dans le message Rapport COPS a le champ Type de rapport réglé à 1 (succès) ou 2 (échec) en fonction de l'aboutissement de la commande de contrôle de porte. Tous les messages Rapport transportant la réponse du contrôle de porte devraient avoir le bit fanion du message sollicité établi dans l'en-tête COPS. Tous les messages Decision (DEC), sauf le premier, devraient avoir le fanion du message sollicité mis à faux dans l'en-tête COPS. Le premier message de décision envoyés du serveur CMS au système CMTS devrait avoir le fanion (du message) sollicité mis à Vrai. Les valeurs de ce fanion sont établies pour se conformer à la spécification COPS. Elles ne devraient pas affecter le fonctionnement du protocole de commande de porte.

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

7.4 Fonctionnement du protocole de contrôle de portes

7.4.1 Séquence d'initialisation

Au moment où il est amorcé, le système CMTS (c'est-à-dire, COPS PEP) DOIT écouter les connexions COPS sur le port TCP numéro 2126 (assigné par IANA). Tout contrôleur de porte qui a besoin de contacter le système CMTS DOIT établir une connexion TCP avec le système CMTS sur ce port. Il est prévisible que plusieurs contrôleurs de porte établiront des connexions COPS avec un seul CMTS. Lorsque la connexion TCP entre le CMTS et le GC est établie, le CMTS envoie des informations sur lui-même au GC sous la forme d'un message CLIENT-OPEN. Ces informations incluent le CMTS-ID provisionné dans l'objet PEP Identification (PEPID). Le système CMTS DEVRAIT omettre l'objet Dernière adresse PDP (LastPDPAddr) du message CLIENT-OPEN.

En réponse, le contrôleur de porte envoie un message CLIENT-ACCEPT. Ce message inclut l'objet Temporisateur de durée de vie qui indique au système CMTS l'intervalle maximal entre les messages Garder en vie.

Le système CMTS envoie alors un message REQUEST, comprenant les objets Outil et Contexte. L'objet Contexte (C-NUM = 2, C-TYPE = 1) PEUT avoir la valeur R-Type (fanion de type de demande) réglée à 0x08 (demande de Configuration) et M-Type réglée à zéro. L'objet Outil contient un nombre qui est choisi par le système CMTS. La seule exigence imposée sur ce nombre est qu'un CMTS NE DOIT PAS utiliser le même nombre pour deux demandes différentes sur une seule connexion COPS; dans l'environnement IPCablecom, la valeur numérique de Outil n'a pas d'autre signification dans le protocole. Ceci complète la séquence d'initialisation qui est représentée à la Figure 13.

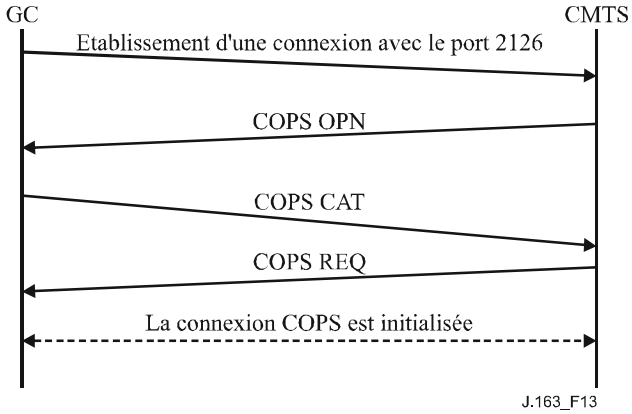


Figure 13/J.163 – Etablissement d'une connexion COPS

Périodiquement le système CMTS DOIT envoyer un message COPS KEEP-ALIVE (KA) (*Garder en vie*) au GC. A réception du message COPS KA, le serveur CMS DOIT renvoyer un message COPS KA au système CMTS. Cette transaction est représentée à la Figure 14 et est complètement documentée dans le document RFC 2748 de l'IETF. Ceci DOIT être effectué au moins aussi souvent que spécifié dans l'objet Keep-Alive-Timer renvoyé dans le message CLIENT-ACCEPT. Le message KEEP-ALIVE est envoyé avec Client-Type réglé à zéro.

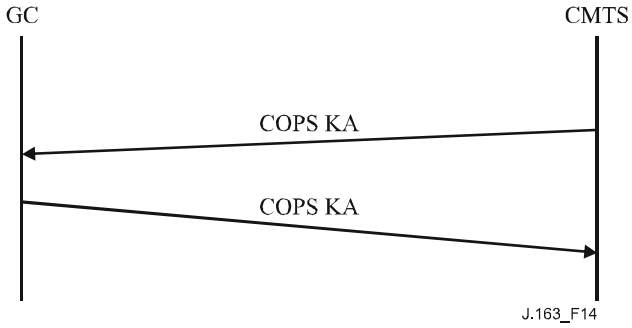


Figure 14/J.163 – Echange de messages COPS keep-alive

7.4.2 Séquence de fonctionnement

Le protocole entre le contrôleur de porte et le système CMTS répond aux besoins de la politique de contrôle des ressources et d'allocation des ressources. Le contrôleur de porte implémente toutes les politiques d'allocation et utilise ces informations pour gérer l'ensemble des portes implémentées dans le système CMTS. Le contrôleur de porte initialise les portes avec les restrictions spécifiques au niveau de la source, la destination et la bande passante. Une fois initialisé, le MTA est capable de demander des allocations de ressources situées dans les limites imposées par le contrôleur de porte.

Les messages initialisés par le contrôleur de porte incluent Gate-Alloc (*Allocation de porte*), Gate-Set (*Porte établie*), Gate-Info (*Informations de porte*) et Gate-Delete (*Suppression de porte*). Les procédures relatives à ces messages sont décrites dans les paragraphes suivants.

Les messages initialisés par le contrôleur de porte sont envoyés en utilisant les objets spécifiques du client dans l'objet Décision des messages COPS DECISION. Les réponses aux messages initialisés par le contrôleur de porte sont envoyées comme un message REPORT-STATE avec des objets spécifiques du client dans l'objet ClientSI par le système CMTS. Pour les messages ACK (*d'accusé de réception*) la valeur du Type de rapport COPS DOIT être 1 et pour les messages ERR (*d'erreur*) le Type de rapport DOIT être 2. Les messages Porte Ouverte et Porte fermée DOIVENT être envoyés comme un message REPORT-STATE non sollicité avec l'ID de transaction à zéro, avec les

objets spécifiques du client dans l'objet ClientSI, en utilisant le Type de rapport 3, au serveur CMS par l'intermédiaire de la connexion TCP qui a servi à construire la porte à l'origine. Si cette connexion TCP n'est plus valide, le système CMTS doit alors abandonner les messages du contrôleur de porte.

Les messages DECISION et les messages REPORT-STATE DOIVENT contenir le même outil que celui utilisé dans la REQUEST initiale envoyée par le système CMTS lorsque la connexion COPS a été initialisée.

Gate-Alloc valide le nombre de sessions simultanées qui peuvent être établies depuis le MTA d'origine et alloue un ID de porte à utiliser pour tous les messages futurs concernant cette porte ou ensemble de portes.

Gate-Set initialise et modifie tous les paramètres de la politique et du trafic pour la porte ou l'ensemble de portes et règle les informations de facturation et de coordination de porte.

Gate-Info est un mécanisme par lequel le contrôleur de porte peut trouver tous les réglages de paramètres et d'état courants d'une porte ou ensemble de portes existant.

Le système CMTS DOIT envoyer périodiquement un message (Garder en vie) Keep-alive (KA) au GC pour faciliter la détection des pannes de connexion du TCP. Le contrôleur de porte garde trace du moment de réception des messages KA. Si le contrôleur de porte n'a pas reçu un KA du système CMTS dans le temps spécifié par le document RFC 2748 de l'IETF ou si le contrôleur de porte a reçu une indication d'erreur de la connexion TCP, alors le contrôleur de porte DOIT mettre fin à la connexion TCP et tenter de rétablir la connexion TCP avant la prochaine demande d'allocation de porte de ce CMTS.

Gate-Delete permet dans certaines circonstances (voir ci-dessous) à un contrôleur de porte de supprimer une porte récemment allouée.

Porte ouverte permet au CMTS d'informer le contrôleur de porte de l'engagement des ressources de porte. Le message Porte ouverte, conjointement avec le message Porte fermée décrit ci-dessous, donne une voie de rétroaction du CMTS au serveur CMS afin de permettre une gestion précise de l'état d'appel à l'élément CMS.

Gate-Close (*Porte fermée*) permet au CMTS d'informer le contrôleur de porte que la porte a été supprimée pour cause d'interaction entre MTA ou d'inactivité.

7.4.3 Procédures pour allouer une nouvelle porte

Un message Gate-Alloc est envoyé par le contrôleur de porte au système CMTS au moment où le message "Call_Set-up" ("Appel_Etabli") est envoyé depuis le MTA d'origine comme l'indique la Figure 14.

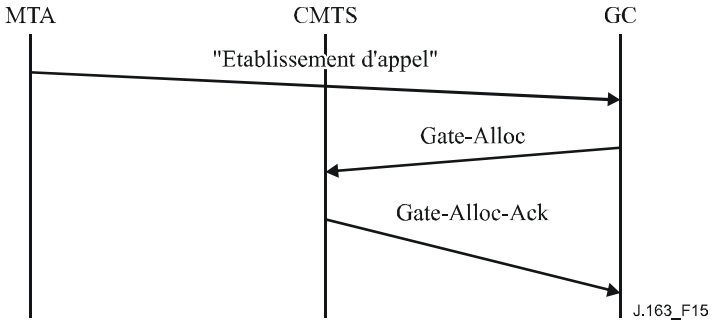
L'utilisation de Gate-Alloc garantit qu'un trop grand nombre de sessions n'est pas simultanément demandé depuis un MTA donné. Ce mécanisme peut être utilisé pour contrôler une attaque de déni de service en provenance du MTA. Le système CMTS, dans sa réponse au message Gate-Alloc, compare le nombre de portes actuellement alloué pour l'ID de l'abonné indiqué avec le champ Compte de l'objet Compte d'activité dans le message Gate-Alloc. Si le nombre de portes en cours est supérieur ou égal au champ Compte dans Gate-Alloc, alors le système CMTS DOIT renvoyer un message Gate-Alloc-Err. Si le nombre de portes en cours est supérieur au champ Compte dans Gate-Alloc, alors il est vraisemblable que l'abonné a été réapprovisionné pour avoir une limite de porte plus faible que précédemment. Dans ce cas, les sessions en cours de l'abonné ne sont pas affectées mais toute nouvelle session de cet abonné sera rejetée par le système CMTS tant que le compte de session de l'abonné ne sera pas descendu en dessous de la valeur spécifiée dans le champ Compte.

La détermination de la valeur réelle que doit contenir le champ Compte est une question de fonctionnement. Il devrait être suffisamment élevé (par MTA) pour qu'aucun scénario d'appel

légitime ne puisse en être affecté, mais suffisamment bas pour empêcher de monter une attaque viable de déni de service.

Si l'objet Compte d'activité n'est pas présent, le système CMTS n'effectue pas le contrôle de limite de porte. Un GC cherchant à réduire le temps d'établissement d'appel PEUT décider d'exécuter le contrôle de limite de porte à la réception du message Gate-Alloc-Ack au lieu que le système CMTS effectue le contrôle pour que le GC puisse faire le Gate-Alloc et les opérations de recherche d'abonnés de la politique en parallèle. Lorsque les résultats des deux opérations sont disponibles, le GC peut effectuer le contrôle de limite de portes. Si le contrôle échoue, le GC DOIT envoyer un message Gate-Delete au système CMTS pour supprimer la porte qui a été incorrectement allouée (voir le § 7.4.8). Le GC PEUT inclure l'objet Compte d'activité dans les messages Gate-Alloc suivants pour cet abonné une fois que la politique a été mise en mémoire.

Le schéma qui suit (voir Figure 15) est un exemple de la signalisation Gate-Alloc:



NOTE – A titre d'exemple, le message "Call Setup" ("Etablissement d'appel") dans ce contexte se réfère à "Invite sans sonnerie" lorsque l'on utilise DCS.

Figure 15/J.163 – Exemple de signalisation de Gate-Alloc

Le système CMTS DOIT répondre à un message Gate-Alloc avec un Gate-Alloc-Ack (indiquant la réussite) ou un Gate-Alloc-Err (indiquant l'échec). L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande.

Les erreurs lors de l'allocation des portes sont rapportées par une réponse Gate-Alloc-Err. L'objet Erreur IPCablecom contient l'un des codes d'erreur suivants:

1 = pas de porte actuellement disponible.

4 = l'abonné a dépassé la limite de portes.

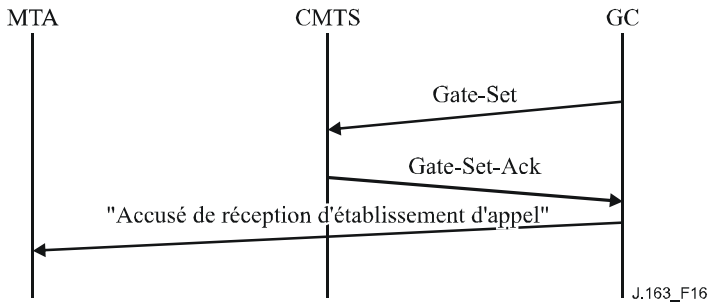
6 = objet requis manquant.

7 = objet non valide.

127 = autre, erreur non spécifiée.

7.4.4 Procédures pour autoriser les ressources à travers une porte

Le message Gate-Set est envoyé par le contrôleur de porte au système CMTS pour initialiser ou modifier les paramètres opérationnels de la ou des portes. La Figure 16 donne un exemple de la signalisation Gate-Set.



NOTE – A titre d'exemple, le message "Call Setup Ack" (Accusé de réception d'établissement d'appel) se rapporte dans ce contexte au message "200 OK" qui est "Invite sans sonnerie" lorsque l'on utilise DCS.

Figure 16/J.163 – Exemple de signalisation de Gate-Set

Si un objet ID de porte est présent dans le message Gate-Set, la demande est alors de modifier une porte existante. Si l'objet ID de porte manque dans le message Gate-Set, il s'agit alors d'une demande d'allocation d'une nouvelle porte et l'objet Compte d'activité PEUT être présent de sorte que le système CMTS puisse déterminer si l'abonné a dépassé le nombre maximal de portes simultanées (voir au § 7.4.3).

Le message Gate-Set DOIT contenir exactement un ou deux objets Gate-Spec, décrivant zéro ou une porte amont et zéro ou une porte aval.

Le système CMTS DOIT répondre à un message Gate-Set avec un Gate-Set-Ack (indiquant la réussite) ou un Gate-Set-Err (indiquant l'échec). L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande.

Les erreurs dans l'allocation ou l'autorisation de portes sont rapportées par une réponse Gate-Set-Err. L'objet Erreur IPCablecom contient un des codes d'erreur suivants:

1 = aucune porte actuellement disponible.

2 = ID de porte inconnu.

3 = valeur de Classe de session illégale.

4 = limite de portes de l'abonné dépassée.

5 = porte déjà établie.

6 = objet requis manquant.

7 = objet non valide.

127 = autre, erreur non spécifiée.

En traitant une demande de réservation d'un MTA, le système CMTS DOIT déterminer la porte correcte en utilisant TLV de bloc d'autorisation. Le système CMTS DOIT vérifier que la demande de réservation se trouve dans les limites autorisées spécifiées pour la porte.

Le système CMTS met alors à jour la demande de réservation à partir des paramètres de la porte. Si l'ensemble de paramètres de QS est admis (2), le système CMTS DOIT alors régler la temporisation pour les paramètres de QS admis sur la valeur du temporisateur T7. Le système CMTS DOIT utiliser la valeur du Point de code DiffServ ou du Type de service pour recouvrir l'octet Type de service IP avant d'envoyer des paquets.

Le système CMTS DOIT exécuter une fonction de contrôle d'admission, fondée sur les paramètres de politique fournis et la valeur Classe de session de la porte.

Noter qu'un message Gate-Set peut être utilisé pour allouer (et établir) une porte au lieu du message Gate-Alloc. Dans ces situations, il est possible que le numéro de port utilisé par la porte distante pour recevoir le message de coordination de porte ne soit pas disponible pour le contrôleur de porte. Si tel est le cas, le port CMTS dans l'objet Informations de porte distante (transporté dans le message Gate-Set) est réglé à zéro. Ceci amène le système CMTS à ignorer le numéro de port de coordination de porte. Toutefois, lorsque le contrôleur de porte (ultérieurement) prend connaissance du numéro de port utilisé par la porte distante, il doit envoyer un autre message Gate-Set (avec le numéro de port dans l'objet Informations de porte distante) pour informer le système CMTS sur ce port.

L'objectif du message Gate-Set est que les valeurs les plus récentes des paramètres soient utilisées pour le contrôle d'admission lorsqu'on fait passer une porte de l'état Autorisé à l'état Réservé. Une fois que les ressources ont été réservées, l'adaptateur MTA a la garantie que toute opération d'engagement au sein de l'enveloppe réservée réussira. Après ce moment (c'est-à-dire, celui où l'état de la porte est Réservé, ou Engagé), la porte DOIT rester dans le même état. Tout message Gate-Set (*Porte établie*) pour une porte à l'état Réservé ou Engagé DOIT être rejeté par le système CMTS. Si, par suite d'événements extérieurs (changement de codec, changement de port RTP ou d'adresse IP, etc.) les paramètres de la porte deviennent insuffisants pour transporter le flux de média à venir, le contrôleur de porte DOIT essayer de créer une nouvelle porte pour traiter le flux de média modifié.

7.4.5 Procédures pour interroger une porte

Lorsqu'un contrôleur de porte souhaite trouver les valeurs des paramètres en cours d'une porte, il envoie au système CMTS un message Gate-Info. Le système CMTS DOIT répondre à un message Gate-Info par un Gate-Info-Ack (indiquant la réussite) ou un Gate-Info-Err (indiquant l'échec). L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande. Le ou les objets GateSpec DOIVENT être inclus dans l'accusé de réception d'information de porte s'ils ont été précédemment fournis au CMTS en association avec une porte.

Les erreurs dans l'interrogation des portes sont rapportées par une réponse Gate-Info-Err. L'objet Erreur contient l'un des codes d'erreur suivants:

2 = ID de porte inconnu.

127 = autre, erreur non spécifiée.

7.4.6 Procédures pour engager une porte

Lorsque le MTA effectue avec succès l'opération initiale d'engagement (comme décrit au § 6.2.1, pour un MTA intégré) pour une porte, le système CMTS DOIT envoyer un message Porte ouverte.

7.4.7 Procédures pour fermer une porte

Le système CMTS DOIT libérer toutes les ressources associées à une porte, supprimer la porte, supprimer le ou les flux de service associés en utilisant un message DSD de DOCSIS, et envoyer un message Porte fermée lorsqu'il reçoit un message explicite de libération de la part du MTA client (comme décrit au § 6.3.3 pour les MTA intégrés), ou lorsqu'il détecte que le client n'est plus actif dans la génération de paquets et ne génère plus de rafraîchissements corrects pour le flux associé à une porte.

7.4.8 Procédures pour supprimer une porte

Dans un flux d'appel normal, une porte est supprimée par le système CMTS lorsqu'elle reçoit un message DSD-REQ. Le système CMTS supprime également une porte à réception d'un message Gate-Close.

Si la porte amont et la porte aval sont l'une et l'autre réservées ou engagées, le système CMTS doit alors respecter les règles suivantes:

– pour un message DSD-REQ lancé par l'adaptateur E-MTA et incluant les identifiants de flux de service amont et aval valides associés à une porte valide, le système CMTS doit supprimer les flux de service amont et aval et libérer toutes les ressources associées à la porte;

– pour un message DSD-REQ lancé par l'adaptateur E-MTA n'incluant qu'un identifiant de flux de service amont valide et n'incluant aucun identifiant de flux de service aval associé à une porte valide, le système CMTS DOIT alors supprimer les flux de service amont et aval. Le système CMTS doit envoyer un message DSD-REQ pour le flux de service aval associé à l'adaptateur E-MTA et libérer toutes les ressources associées à la porte;

– pour un message DSD-REQ lancé par l'adaptateur E-MTA n'incluant qu'un identifiant de flux de service aval valide et n'incluant aucun identifiant de flux de service amont associé à une porte valide, le système CMTS DOIT alors supprimer uniquement le flux de service aval. Le système CMTS doit attendre que le temporisateur T8 amont associé, s'il fonctionne, expire, ou attendre un message DSD-REQ pour le flux de service amont ou encore attendre la libération des ressources associées à la porte.

Un contrôleur de porte, généralement, n'initialise pas une opération de suppression de porte. Un certain nombre de situations anormales peuvent toutefois se produire au cours desquelles un contrôleur de porte serait amené à supprimer une porte sur le système CMTS. Par exemple, si le contrôleur de porte apprend (à réception de la réponse Gate-Alloc-Ack) qu'un abonné a dépassé sa limite de portes, il peut vouloir supprimer la porte récemment allouée au CMTS. Dans des scénarios de ce type, il DEVRAIT envoyer un message Gate-Delete au système CMTS (au lieu de permettre à la porte d'effectuer une temporisation). Il pourrait exister d'autres situations au cours desquelles la fonctionnalité de suppression s'avérerait utile.

Le système CMTS DOIT répondre à un message Gate-Delete par un Gate-Delete-Ack (indiquant la réussite) ou un Gate-Delete-Err (indiquant l'échec). L'ID de transaction dans la réponse DOIT correspondre à l'ID de transaction dans la demande. Les erreurs dans la suppression des portes sont rapportées par une réponse Gate-Delete-Err. L'objet Erreur contient l'un des codes d'erreurs suivants:

2 = ID de porte inconnu.

127 = autre, erreur non spécifiée.

7.4.9 Séquence de terminaison

Lorsque le système CMTS ferme sa connexion TCP vers le GC, il PEUT d'abord envoyer un message DELETE-REQUEST-STATE (*supprimer la demande d'état*) (comprenant l'objet outil utilisé dans le message REQUEST). Le système CMTS PEUT suivre avec un message CLIENT-CLOSE. Ces messages sont optionnels parce que le GC est sans état et que le protocole COPS demande à un serveur COPS de supprimer automatiquement tout état associé au système CMTS lorsque la connexion TCP est terminée.

Lorsque le contrôleur de porte va s'arrêter, il DEVRAIT envoyer un message Client fermé (CC, *client-close*) COPS au système CMTS. Dans le message CC COPS, le contrôleur de porte NE DEVRAIT PAS envoyer l'objet Adresse de redirection PDP <PDPRedirAddr>. Si le système CMTS reçoit un message CC COPS du contrôleur de porte avec un objet <PDPRedirAddr>, le système CMTS DOIT ignorer le <PDPRedirAddr> lorsqu'il traite le message CC COPS.

7.4.10 Scénario d'échec

Lorsqu'un CMTS détecte la perte de la connexion TCP ou COPS au contrôleur de porte, par exemple, si le GC subit une panne catastrophique, le CMTS DOIT conserver toutes les portes

établies en place. Une méthode permettant de maintenir l'état de la connexion TCP ou COPS consiste à utiliser les messages COPS Keep-Alive (*Garder en vie*). Dans ce cas, si le serveur CMS ne lui renvoie pas un message Keep-Alive dans l'intervalle de maintien en l'état de la connexion (Keep-Alive), le système CMTS DOIT considérer la connexion COPS comme étant perdue et se mettre à l'écoute dans l'attente de la réinitialisation du support TCP sur le port 2126.

Les portes qui ont été engagées resteront engagées et les portes dans tous les autres états resteront dans cet état jusqu'à ce que leur état soit changé de façon active ou que les temporisateurs appropriés arrivent à expiration. Le maintien des portes lors de défaillance du GC/CMS permet à tout flux critique (par exemple un appel d'urgence) de rester en place.

7.5 Utilisation du protocole de porte par le CMS

Le CMS DOIT s'assurer que tous les codecs agréés durant la négociation tiennent dans l'enveloppe de ressources demandées au système CMTS utilisant la porte de communication. Le CMS DOIT utiliser l'algorithme LUB donné au § 6.1.1 pour déterminer les valeurs de b, r, p, m, et M.

Le CMS DEVRAIT s'assurer que le message Commande de porte communiqué au système CMTS contient les adresses et ports IP de point de terminaison appropriés de telle sorte que les points de terminaison d'appel soient référencés et qu'un possible vol de service soit empêché.

Le CMS DOIT mettre le terme de surlongueur à une valeur de 800 µs pour le sens amont s'il n'envoie pas de paramètre de gigue d'allocation amont au MTA. Autrement, la valeur qui est utilisée à la porte devrait être inférieure ou égale à la valeur envoyée au MTA pour qu'il l'utilise comme paramètre de gigue tolérée DOCSIS. Pour la direction aval, le CMS DOIT mettre la valeur à zéro.

7.6 Coordination de porte

Le contrôleur de porte conserve l'état de chaque porte. Il crée une porte sur le système CMTS en utilisant le message Gate-Alloc (*Allocation de porte*) ou Gate-Set (*Porte établie*). Le contrôleur de porte peut supprimer une porte au moyen de la commande Gate-Delete (*Suppression de porte*) ou peut interroger le système CMTS sur les informations associées à une porte particulière en utilisant le message Gate-Info (*Informations de porte*). Le système CMTS informe le contrôleur de porte des changements d'état qui surviennent du fait de messages du MTA ou de l'inactivité en utilisant les messages Gate-Open (*Porte ouverte*) et Gate-Close (*Porte fermée*).

Le message Gate-Open est généré par le système CMTS lorsque le MTA engage des ressources de QS, débutant par là l'appel. Le message Gate-Close signale la fermeture de la porte au système CMTS et la libération des ressources de QS associées. Les messages Gate-Open et Gate-Close sont tous deux des messages d'information en ce qui concerne les changements d'état au CMTS par rapport à une porte spécifique, et ne requièrent pas de rétroaction de la part du serveur CMS.

Les événements Gate-Open et Gate-Close des points de terminaison local et distant doivent être synchronisés pour empêcher de possibles scénarios de vol de service. Cette synchronisation est réalisée en utilisant la logique interne du CMS ou, dans le cas de CMS multiples, en utilisant la signalisation de CMS à CMS.

7.6.1 Connexion d'un appel

La réussite de la connexion d'un appel normal exige que trois événements se succèdent rapidement:

- le CMS demande l'engagement de ressources au MTA local;
- le CMTS indique que des ressources ont été engagées par le MTA local;
- l'engagement de ressource local et distant est coordonné sur le plan de la signalisation.

Voir Figure 17.

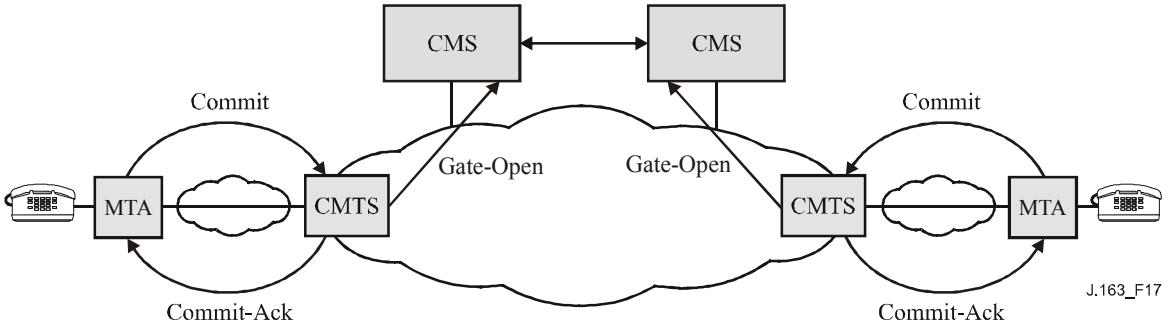


Figure 17/J.163 – Coordination de connexion d'appel

Si un serveur CMS reçoit un message Gate-Open pour une porte qui n'a pas communiqué que des ressources vont être engagées, le CMS DOIT alors supprimer la porte avec la cause "Ouverture de porte inattendue" décrite dans le code de cause.

7.6.2 Fin d'un appel

La fin d'un appel exige, comme dans le cas de la connexion, que trois événements se succèdent dans un court laps de temps:

- le CMS demande la libération des ressources au MTA local;
- le CMTS indique que les ressources ont été libérées par le MTA local;
- la libération de ressource locale et distante est coordonnée sur le plan de la signalisation.

Voir Figure 18.

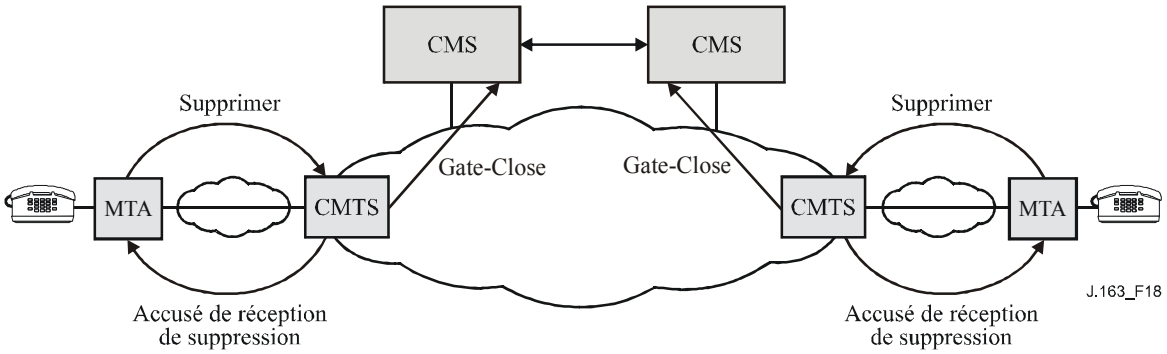


Figure 18/J.163 – Coordination de fin d'appel

Lorsque le CMS envoie à l'adaptateur MTA un message pour supprimer la connexion, le CMS DOIT lancer un temporisateur pour T5 périodes de temps. Si à l'expiration du temporisateur, le CMTS n'a pas indiqué la fermeture de la porte, le serveur CMS DOIT alors produire une commande Suppression de porte pour supprimer la porte au CMTS avec la cause "Défaillance locale de fermeture de porte" décrit dans le code de cause.

Lorsque le serveur CMS reçoit un message Gate-Close, il doit mettre à jour son état interne pour refléter le retrait de la porte au système CMTS.

Annexe A

Définitions et valeurs des temporisateurs

Plusieurs temporisateurs sont mentionnés dans la présente Recommandation. La présente annexe contient la liste de ces temporisateurs et leurs valeurs recommandées.

Temporisateur T0

Ce temporisateur est implémenté dans le système CMTS dans la machine d'état de porte et limite la période pendant laquelle une porte peut être allouée sans que les paramètres de la porte soient réglés. Ceci permet au système CMTS de récupérer les ressources de l'ID de porte (GateID) lorsque le système de gestion d'appel n'arrive pas à exécuter la séquence de signalisation pour une nouvelle session.

Ce temporisateur est lancé lorsqu'une porte est allouée.

Ce temporisateur est remis à zéro lorsque les paramètres de la porte sont réglés.

A l'expiration de ce temporisateur, le système CMTS DOIT considérer que l'ID de porte (Gate ID) alloué est non valide.

La valeur RECOMMANDÉE de ce temporisateur est de 30 secondes.

Temporisateur T1

Ce temporisateur est implémenté au système CMTS dans la machine d'état de porte et limite la période qui peut s'écouler entre l'autorisation et l'exécution d'une opération d'engagement.

Ce temporisateur est lancé chaque fois qu'une porte est établie.

Ce temporisateur est remis à zéro lorsque la porte passe à l'état ENGAGÉ.

A l'expiration de ce temporisateur, le système CMTS DOIT libérer toutes les ressources réservée au CMTS pour cette porte, révoquer toutes les réservations faîtes par le MTA, qui étaient autorisées par cette porte en signalant au câblo-modem via DSC ou DSD de libérer les ressources qu'il avait réservé et lancer un message Gate-Close pour la porte.

Le temporisateur T1 DOIT être réglé à la valeur donnée dans le message Gate-Set. Si la valeur donnée dans le message Gate-Set est zéro, le temporisateur T1 DOIT alors être réglé à une valeur par défaut à fournir. La valeur recommandée de cette valeur par défaut se situe dans la gamme de 200 à 300 secondes.

Si la valeur du temporisateur T1 dans le message Porte établie est 0, le système CMTS DOIT retourner la valeur T1 provisionnée au CMTS ou zéro pour T1 dans l'objet Spec de porte du message Accusé de réception d'information de porte. La valeur provisionnée pour T1 est celle qui est préférée dans ce cas.

Temporisateur T2

Ce temporisateur n'est plus utilisé.

Temporisateur T3

Ce temporisateur n'est plus utilisé.

Temporisateur T4

Ce temporisateur n'est plus utilisé.

Temporisateur T5

Ce temporisateur est implémenté au système CMTS. Il contrôle la synchronisation entre la libération de ressources au MTA local et la vérification au CMTS de la fermeture de la porte locale.

Lorsque le système CMS envoie au MTA un message pour supprimer la connexion, le serveur CMS DOIT s'assurer que la porte est fermée au CMTS dans le délai de T5. Ce temporisateur est remis à zéro lorsque le CMS reçoit une confirmation de la fermeture de la porte locale via le message Gate-Close.

A l'expiration de ce temporisateur, le serveur CMS supprime la porte au CMTS en utilisant le message Gate-Delete avec "Défaillance de fermeture de porte locale" décrit dans le code de cause.

La valeur RECOMMANDÉE de ce temporisateur est de 5 secondes.

Temporisateur T6

Ce temporisateur n'est plus utilisé.

Temporisateur T7

Le système CMTS DOIT régler la temporisation pour les Paramètres de QS admise pour le flux de service à la valeur spécifiée pour ce temporisateur. Dans le cas d'un flux comportant plusieurs sous-flux, la temporisation pour les paramètres de QS admise pour ce flux est mise à la valeur du temporisateur T7 retenue dans le message Gate-Set (*Porte établie*) reçu en date la plus récente pour n'importe quel sous-flux du flux. La temporisation pour les Paramètres de QS admise limite la période pendant laquelle le système CMTS doit garder les ressources pour un Ensemble de paramètres de QS admise d'un flux de service lorsqu'elles sont en excédent de son Ensemble de paramètres de QS active. Voir à l'Annexe C de l'Annexe B/J.112 des détails complémentaires sur l'utilisation de la temporisation pour les paramètres de QS admise.

Pour permettre à l'E-MTA de rafraîchir ce temporisateur, le système CMTS DOIT informer l'E-MTA de la temporisation pour la valeur des Paramètres de QS admise dans la réponse (c'est-à-dire, dans la DSA-RSP) à la demande de réservation de l'EMTA.

La valeur recommandée de ce temporisateur est 200 secondes.

Temporisateur T8

Le système CMTS DOIT régler la temporisation pour les Paramètres de QS active pour le flux de service à la valeur spécifiée pour ce temporisateur. Dans le cas d'un flux comportant plusieurs sous-flux, la temporisation pour les paramètres de QS active pour ce flux est mise à la valeur du temporisateur T8 retenue dans le message Gate-Set (*Porte établie*) reçu en date la plus récente pour n'importe quel sous-flux du flux. La temporisation pour les Paramètres de QS admise limite la période pendant laquelle les ressources restent inutilisées pour un flux de service actif. Voir à l'Appendice C de l'Annexe B/J.112 des détails complémentaires sur l'utilisation de la temporisation pour les paramètres de QS active.

Pour permettre à l'E-MTA de rafraîchir ce temporisateur, le système CMTS DOIT informer l'E-MTA de la temporisation pour la valeur des Paramètres de QS active dans la réponse (c'est-à-dire, dans la DSA-RSP) à la demande de réservation de l'E-MTA.

La valeur par défaut de ce temporisateur est 0, qui indique au système CMTS de ne pas interroger sur l'activité du flux de service.

Appendices I à VIII, et XI

A insérer ultérieurement.

Appendice IX

Scénarios de vol de service

Sont indiquées ici les grandes lignes de plusieurs scénarios possibles de vol de service pour mettre en évidence la nécessité d'une autorisation dynamique, la nécessité du protocole de réservation de ressources en deux phases, la nécessité des portes, et la nécessité de la coordination de porte. La conception du système place une grande partie de l'intelligence de commande de la session au niveau des clients, où elle peut facilement évoluer avec la technologie et fournir des services nouveaux et innovants. Avoir un système à "l'épreuve du futur" est certes un objectif de conception, mais il faut reconnaître que dans ce cas la porte reste ouverte à une gamme importante de fraudes. Le présent appendice étudie certaines de ces possibilités et comment l'architecture de la signalisation de la QS les empêche.

L'hypothèse de départ est que le MTA n'est pas à l'abri de la fraude par l'abonné et que l'inclination importante en faveur d'un service gratuit amènera à des tentatives très sophistiquées pour abuser tout contrôle de réseau placé sur le MTA. Cette fraude par l'abonné inclut, sans s'y limiter, l'ouverture du boîtier et le remplacement des mémoires en lecture seule, le remplacement des circuits intégrés, l'analyse et le démontage du cœur du MTA et même le remplacement total du MTA par une version spéciale issue du marché noir. Alors que des solutions techniques existent pour assurer la sécurité physique du MTA (par exemple piéger le boîtier avec un gaz mortel), elles ne sont pas considérées comme acceptables.

Etant donné que le MTA peut uniquement être distingué par sa communication sur un réseau DOCSIS, il est possible et tout à fait vraisemblable, qu'un logiciel d'ordinateur individuel sera écrit pour émuler le comportement du MTA. Il peut être impossible de distinguer un tel ordinateur d'un MTA réel. Le comportement du logiciel dans ce cas est sous le contrôle total du client.

De plus, il est prévu que des nouveaux services seront implémentés dans le MTA et que le contrôle logiciel de ces nouveaux services sera fourni par des constructeurs très divers. Ce logiciel mis à jour sera chargé dans le MTA, laissant ouverte la possibilité que des clients chargent des versions piratées spéciales qui fournissent un service gratuit. Ne sera pas abordé ici le problème des "chevaux de Troie" dans ces logiciels téléchargés, car ce problème est considéré comme identique à celui des clients qui communiquent leur numéro de carte de crédit et/ou leur numéro d'identification personnel (PIN). Le problème du client qui télécharge intentionnellement un logiciel spécial qui ne fonctionne que dans son intérêt sera également traité.

IX.1 Scénario n° 1: clients établissant eux-mêmes des connexions à QS élevée

Le MTA, avec une intelligence suffisante, peut se rappeler des destinations composées passées et de l'adresse de destination ou utiliser tout autre mécanisme pour déterminer l'adresse IP d'une destination. Il peut ensuite signaler cette destination proprement dite (avec une certaine coopération de l'autre client) et négocier une connexion à QS élevée via l'interface DOCSIS pour un client intégré. Etant donné qu'aucun agent de réseau n'est utilisé pour initialiser la session, aucun enregistrement destiné à la facturation ne sera produit. Ce scénario est évité en demandant une autorisation dynamique au niveau du système CMTS; sans l'autorisation, la tentative d'obtenir la qualité de service élevée échouera.

Le scénario ci-dessus a demandé la coopération de deux MTA modifiés. Un vol de service similaire pourrait être accompli avec la seule modification de l'émetteur. Si le MTA d'origine utilisait l'agent de réseau pour établir la session, en informant de cette façon la destination de la manière standard d'une session entrante, mais encore négociait la qualité de service élevée proprement dite, il n'y aurait aucun enregistrement de facturation généré et l'émetteur obtiendrait une session gratuite. Ici encore, la solution consiste à requérir l'utilisation de portes dans les CMTS.

IX.2 Scénario n° 2: clients utilisant une QS fournie pour des applications non vocales

Une QS fournie de manière statique peut uniquement identifier un abonné comme une personne autorisée à un service de qualité élevée. Il n'y a aucune restriction sur l'utilisation du service. En particulier, un client qui a souscrit un service de communications vocales de classe commerciale et qui est par conséquent autorisé à activer des connexions à temps d'attente faible et à bande passante élevée sur le réseau DOCSIS, peut utiliser cette possibilité pour surfer sur le Web ou pour d'autres applications d'ordinateur. Ce scénario est évité en exigeant une autorisation dynamique au niveau du système CMTS; sans l'autorisation, la tentative d'obtenir une qualité de service élevée échouera.

IX.3 Scénario n° 3: MTA modifiant l'adresse de destination dans les paquets vocaux

Un autre exemple est celui de deux MTA éloignés l'un de l'autre, établissant chacun une session locale. Une fois que la bande passante et la connexion sont établies, les MTA changent alors les adresses IP dans les flux RTP pour se désigner l'un à l'autre. Le système de facturation continue à facturer chacun d'entre eux pour une session locale, tandis que les clients sont en réalité engagés dans une session longue distance. Ceci implique la présence de mécanismes au niveau des CMTS qui fournissent l'accès à une QS plus élevée reposant uniquement sur des filtres de paquets précédemment autorisés. Ainsi, en plus de la gestion des ressources en deux phases, ce scénario motive la nécessité d'implanter des filtres de paquets au niveau des portes.

IX.4 Scénario n° 4: utilisation de demi-connexions

Il s'agit là d'un exemple de vol de service qui pourrait se produire en l'absence de coordination de porte. Supposons qu'un client dans une session engage les ressources de la session et l'autre non. Disons par exemple, que le client d'arrivée engage ses ressources, mais ne réussit pas à envoyer le message de signalisation correct, ainsi le client d'origine engage ses ressources. Dans ce cas, seule une porte est ouverte et les utilisateurs et le réseau sont laissés avec une demi-connexion. Etant donné que l'abonné d'origine n'a pas engagé ses ressources, le réseau ne peut légitimement pas facturer l'utilisateur pour la demi-connexion. Toutefois, il est possible pour deux clients de connivence d'envoyer deux demi-connexions, dont aucune n'est facturable, qui peuvent être combinées pour donner une connexion complète entre les parties. Il en résulte une session gratuite. Une fraude de ce type peut uniquement être empêchée en synchronisant le fonctionnement des deux portes.

IX.5 Scénario n° 5: terminaison rapide laissant une demi-connexion

La coordination de porte est également requise à la fin de la session. Supposons que le MTA_O appelle le MTA_T et paie pour la session. Etant donné que le MTA_O est facturé pour la session, il a clairement une incitation à envoyer un message Release au $CMTS_O$ pour fermer sa porte et arrêter la facturation. Toutefois, si le MTA_T n'envoie pas le message Release pour fermer la porte au niveau du $CMTS_T$, une demi-connexion reste. Dans ce cas le MTA_T peut continuer à envoyer de la voix et/ou des données au MTA_O sans facturation pour la session. Par conséquent, un message GATE-CLOSE doit être envoyé de la porte côté départ au niveau du $CMTS_O$ pour fermer la porte côté arrivée au niveau du $CMTS_T$.

IX.6 Scénario n° 6: messages de coordination de porte falsifiés

Chaque MTA connaît l'identité de son CMTS et connaît le quintuplet que son CMTS utilise pour identifier l'ID de porte. Les MTA peuvent effectuer différents types de négociations de bout en bout avant de demander des ressources; en particulier, ils peuvent facilement échanger les informations sur leur ID de porte. Le MTA peut alors falsifier le message Gate-Open Envoyé à l'extrémité qui ne paie pas et obtenir une connexion à une voie non facturée. Cette opération renouvelée deux fois donne une connexion complète non facturée. L'une des solutions au problème consiste pour le contrôleur de porte de donner au système CMTS une clé à utiliser pour les messages de CMTS à CMTS, sur une base session par session (ou par porte).

IX.7 Scénario n° 7: fraude dirigée contre des demandeurs indésirables

En raison des détails de la séquence d'établissement d'appel, il est possible que l'autorisation de bande passante au niveau de la destination soit plus généreuse qu'à la source. Dès lors, il est possible pour un appelé de réserver et d'allouer une bande passante dépassant de loin la quantité finale négociée, ce qui amène l'appelant a être facturé plus que prévu. Si cette possibilité était disponible, ceci serait probablement utilisé à l'encontre des télévendeurs, en luttant contre les appels indésirables aux heures de repas.

Le fait que le serveur CMS autorise les ressources de la session avant que l'adaptateur MTA ne demande ces ressources garantit que le système CMTS veillera à limiter les demandes de ressources à hauteur du nombre de ressources autorisées.

Appendice X

COPS (service commun de politique ouverte)

X.1 Procédures et principes de COPS

Le présent appendice fournit une description brève des procédures et des principes du protocole COPS et de la façon dont le protocole COPS est associé aux autres protocoles tels que LDAP.

Le protocole du service commun de politique ouverte (COPS, *common open policy service*) est un protocole client/serveur défini pour être utilisé au contrôle d'admission dans les réseaux à QS RSVP/IntServ et DiffServ. Le protocole COPS opère sur TCP/IP, en utilisant un numéro de port bien connu 3288. Les entités COPS résideraient au niveau d'un dispositif en bordure de réseau et d'un serveur de politique. Trois entités fonctionnelles sont définies pour rap:

- point de décision de politique (PDP, *policy decision point*) – L'entité serveur du COPS, qui prend la décision finale d'admission ou de rejet de session, fondée sur les informations de politique auxquelles il a accès. Il est prévu de l'implémenter en tant qu'application sur un dispositif serveur autonome;
- point d'application de la politique (PEP, *policy enforcement point*) – L'entité client de COPS, qui consulte le PDP pour prendre les décisions de politique ou obtenir des informations de politique qu'il peut lui-même utiliser pour prendre des décisions de contrôle d'admission. Le PEP peut recevoir des demandes de service et initialiser une demande au PDP qui résultera en une réponse tout ou rien, ou le PEP peut informer le PDP qu'il souhaite recevoir les décisions et les informations associées à la politique sans demande préalable;
- point de décision locale (LDP, *local decision point*) – Une version locale du PDP qui peut prendre des décisions à partir d'informations locales ou d'informations conservées en mémoire de décisions précédentes. Une décision PDP a toujours priorité sur le LPD.

Une séquence COPS, telle qu'utilisée dans un environnement RSVP/IntServ, est présentée à la Figure X.1.

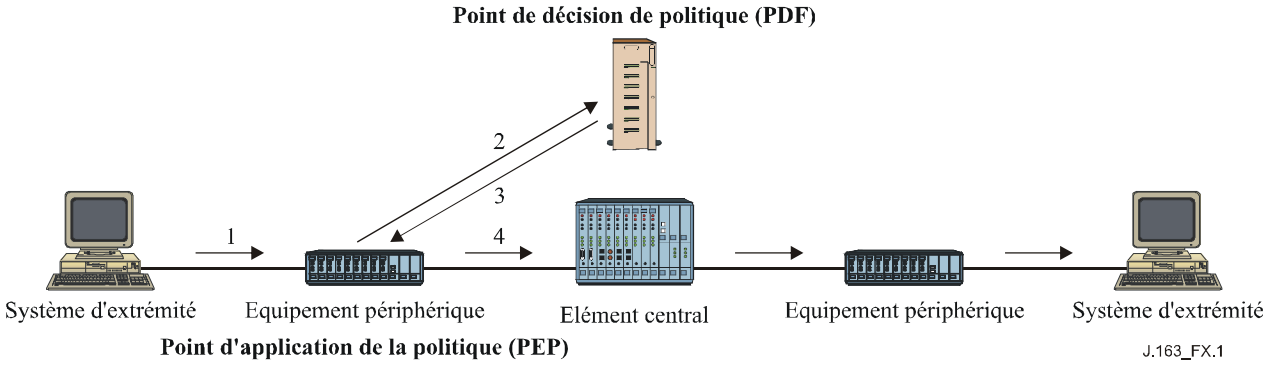


Figure X.1/J.163 – Protocole COPS

Dans la séquence COPS, le client PEP est responsable de l'établissement initial d'une session avec le PDP, en utilisant les informations qui sont configurées dans le PEP ou déterminées par d'autres moyens. Une fois la session établie, si le dispositif de bordure reçoit un message RSVP (1), il génère une demande à traiter au PDP (2) qui décrit le contexte de la demande et transporte les informations sur la demande. Le PDP répond alors (3) avec une décision d'accepter ou rejeter la demande, et si elle est acceptée le dispositif de bordure continue en envoyant le message RSVP dans le réseau (4).

Chaque session est maintenue par un message Keep Alive (Garder en vie) qui vérifie que la session est active dans le cas où aucun message n'a été reçu récemment. Chaque message RSVP ou autre demande est identifié par un Outil, qui peut être utilisé pour associer la réponse, les réponses ultérieures non sollicitées et l'effacement.

Les messages du protocole peuvent être étendus à d'autres tâches. Ils se composent d'un Code Op identifiant si le message est une demande, une réponse, ou d'un autre type, suivi par des objets à auto-identification, chacun contenant une classe d'objet et un identifiant de version. Chaque objet inclut un numéro de classe qui définit ce qu'est l'objet, par exemple, un objet Temporisateur, ou un objet Décision, plus un type de classe qui identifie le sous-type ou la version de la classe utilisée.

D'autres classes d'objets incluent les données d'allocation de bande passante nécessaires pour identifier les ressources demandées par l'utilisateur et les objets Policy qui peuvent être transmis du PDP pour être inclus dans le message RSVP lorsqu'il est envoyé au réseau.

X.2 Comparaison de COPS et de LDAP pour la politique

Les protocoles COPS et LDAP ont été associés à la gestion fondée sur la politique, toutefois, ils devraient fournir des fonctions très différentes.

COPS est conçu pour que le client demande une décision à un Point de décision de politique et pour interagir avec le PDP pour participer activement à la gestion de la politique et aux problèmes associés à la politique. Le PEP qui effectue la demande peut n'avoir aucune connaissance des politiques et repose sur le PDP pour prendre des décisions fondées sur sa connaissance des politiques. Le protocole permet au PEP de transmettre les informations sur la demande au PDP et au PDP de repasser une décision pour permettre ou rejeter la demande.

Le protocole LDAP est conçu pour que le client demande un enregistrement à partir d'un annuaire. La fonction d'utilisation de l'enregistrement dépend du client qui doit être capable de comprendre l'enregistrement extrait et de décider comment utiliser les informations. Le serveur doit être capable

de trouver l'enregistrement correct à partir des informations contenues dans la demande, qui peuvent invoquer une fonction de recherche ou l'extraction de plusieurs enregistrements.

Les deux protocoles COPS et LDAP pourraient être utilisés dans le contexte du contrôle d'admission de RSVP. COPS serait utilisé entre le PEP et le PDP pour envoyer une demande pour une analyse fondée sur la politique. LDAP serait utilisé entre le PDP et un serveur d'annuaire pour extraire les enregistrements de politique associés aux adresses de départ et d'arrivée pour la demande RSVP. Le PDP prendrait alors une décision fondée sur les informations de politique extraites et utiliserait le protocole COPS pour repasser cette décision au PEP. Voir la Figure X.2.

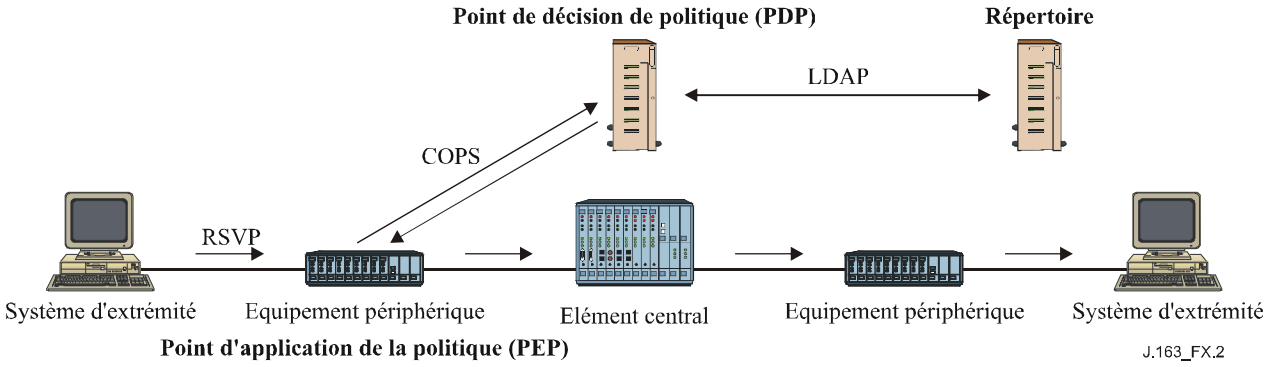


Figure X.2/J.163 – Modèle COPS et LDAP

Appendice XII

Considérations sur le protocole TCP

La présente Recommandation définit une interface entre un contrôleur de porte (GC) et un système de terminaison de câblo-modem (CMTS) à utiliser pour l'autorisation de porte, qui prend fondamentalement en charge un protocole fondé sur les transactions dans lequel chaque transaction est indépendante. Le protocole TCP peut être utilisé comme transport pour cet échange de messages. Toutefois, des questions se sont posées concernant les implications de l'utilisation du TCP sur les performances. Le présent appendice examine quelques-unes de ces questions et propose certaines solutions potentielles qui peuvent fournir un transport acceptable par l'intermédiaire de l'optimisation des implémentations et des mises au point du protocole TCP.

La conception du réseau devrait prenne en charge le degré de fiabilité désiré et les performances en temps réel.

XII.1 Exigences

Il faut considérer d'abord les exigences sur le protocole de transport pour l'interaction entre GC et CMTS:

1) la remise fiable des messages échangés entre contrôleur de porte et CMTS est requise;
2) l'échange de messages devrait avoir un temps d'attente faible (de l'ordre de quelques millisecondes), dans le cas normal (sans perte de paquets). Il est également nécessaire d'avoir un temps d'attente faible raisonnable même en cas de perte de paquets (de l'ordre du dixième de milliseconde);
3) on veut que plusieurs demandes soient en suspens simultanément. Cela parce qu'il est probable que plusieurs établissements d'appel seront en cours concurremment;

4) si un blocage en tête de ligne (HOL, *head-of-the-line*) est probable, il devrait être évité;

5) il est probable qu'il y ait une association longue (au moins de l'ordre de plusieurs minutes) entre le contrôleur de porte et le CMTS. Toutefois, lorsqu'une panne du contrôleur de porte se produit, le procédé d'établissement d'une nouvelle connexion au CMTS ne devrait pas prenne pas un temps excessif. Ceci est particulièrement vrai lorsque l'établissement d'une nouvelle connexion se produit pendant le temps d'établissement d'un appel.

XII.2 Changements recommandés

En résumé, les changements que nous recommandons sur une implémentation ordinaire du TCP sont les suivants:

1) modifier le mécanisme de temporisation pour l'établissement des connexions (le rendre plus agressif);

2) permettre une plus grande fenêtre après l'établissement d'une connexion;

3) avoir plusieurs connexions TCP par paire GC-CMTS pour travailler sur des problèmes potentiels du HOL (par exemple, les utiliser sur une base cyclique);

4) abaisser la granularité de 500 ms de la temporisation;

5) désactiver l'algorithme de Nagle sur l'extrémité de transmission afin de réduire le temps d'attente;

6) avoir une interface non bloquante entre l'application et la pile TCP.

Le reste du présent appendice donne des détails sur la façon dont ces changements peuvent être implémentés.

XII.3 Etablissement d'une connexion TCP affectant le délai après numérotation

L'établissement de la connexion TCP utilise une prise de contact à trois voies définie comme suit (voir Figure XII.1).

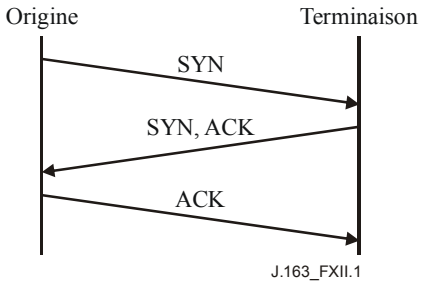


Figure XII.1/J.163 – Etablissement de la connexion TCP

Le TCP retransmet les segments supposés perdus selon une estimation du temps de propagation aller-retour, A, et un écart moyen D, de A. La valeur de la temporisation de retransmission (RTO, *retransmission timeout*) est généralement calculée en utilisant la formule:

$$RTO = A + 4D$$

mais la RTO initiale est calculée en utilisant la formule:

$$RTO = A + 2D$$

où A et D sont initialisés à 0 et 3 secondes respectivement. Lorsqu'une retransmission se produit, une temporisation exponentielle utilisant un multiple de 2 est appliquée à la valeur courante de RTO. Ainsi, pour le premier segment, la RTO est calculée comme suit:

$$RTO = 0 + 2 \times 3 = 6$$

Ainsi, si le segment initial SYN est perdu, une retransmission ne se produira pas jusqu'à 6 secondes plus tard. A ce moment, la RTO sera calculée comme suit:

$$RTO = 0 + 4 \times 3 = 12$$

et une temporisation exponentielle de 2 est appliquée, amenant à une nouvelle valeur de temporisation de la retransmission de 24 secondes. Ainsi, si la retransmission est également perdue, un total de 30 s se sera écoulé avant la troisième retransmission.

L'importance de ce problème dépend entièrement de la fréquence avec laquelle l'établissement de la connexion GC → CMTS tombe pendant la période après numérotation. Dans les scénarios couramment envisagés, il convient que cette occurrence soit plutôt l'exception que la règle. Le temps d'établissement de la connexion affectant le délai après numérotation est une raison importante pour éviter d'avoir l'établissement d'une connexion dans la période du délai après numérotation. Le marquage Diffserv des paquets pour à la fois le temps d'attente et la probabilité de perte, analogue à ce qui est fait avec le trafic aujourd'hui, pourrait être utilisé pour réduire les délais d'établissement de connexion en raison de paquets perdus.

XII.4 Nécessité d'un temps d'attente faible pour les paquets entre GC et CMTS, même en cas de perte

L'exigence (2), qui traite de la récupération de la perte de paquets, a besoin de quelques remèdes disponibles au TCP pour récupérer rapidement une perte. Lorsque seuls quelques paquets sont transmis et que le destinataire est incapable de générer un nombre suffisant de duplications d'accusés de réception, la récupération de la perte de paquets se fait à partir d'une temporisation de retransmission. L'algorithme de retransmission du TCP repose sur un lissage de la moyenne du temps de propagation aller-retour (RTT, *round-trip time*) observé A, et une moyenne pondérée de l'écart moyen dans le RTT. Telle qu'elle est décrite ci-dessus, la valeur de temporisation de retransmission est alors réglée à:

$$RTO = A + 4D$$

et si le temporisateur court, le segment en question est retransmis et la RTO est temporisée exponentiellement en utilisant un multiplicateur[8] de 2 jusqu'à une limite supérieure de 64 secondes pour la RTO. Une fois qu'un segment a été transmis au TCP, le segment est ensuite transmis avec succès jusqu'à sa destination ou la connexion est fermée après une certaine période (généralement une période de temps importante, par exemple 2 à 9 minutes).

Alors que cette stratégie de retransmission ci-dessus est considérée comme désirable, nous pensons qu'elle a deux problèmes (associés) pour l'interface considérée:

1) si le segment n'est pas délivré avec succès dans un délai bref, l'appel qui est en cours d'établissement sera selon toute vraisemblance abandonné et la transaction devrait par conséquent pouvoir être interrompue;
2) le plafond de 64 secondes de la temporisation de retransmission est mal adapté à une communication en temps réel et devrait être réglé plus bas.

Un problème séparé, mais toutefois en rapport, est celui de la granularité de la RTO. Alors que la spécification TCP elle-même ne spécifie pas la granularité de la RTO, il est très commun d'avoir

---

[8] TCP utilise de plus des accusés de réception doubles pour déclencher la retransmission de segments potentiellement perdus, cette particularité sera toutefois ignorée pour cette partie de l'étude.

une granularité de 500 ms dans des systèmes d'exploitation commerciaux. Ainsi, un segment perdu ne sera généralement pas détecté en moins de 500 ms et deux segments perdus ne seront pas détectés en moins de 500 ms + 1000 ms = 1,5 s.

Pour récupérer rapidement la perte de paquets dans une séquence de paquets (sans avoir à dépendre de plusieurs doubles accusés de réception pour déclencher une retransmission rapide ou avoir à attendre tant que le temporisateur RTO court), il peut être souhaitable d'implémenter TCP-SACK, qui aide à la récupération même si le seuil de retransmission rapide n'est pas atteint. Il est également recommandé que l'implémentation du TCP utilise une granularité du temporisateur plus faible (moins de 500 ms si possible).

XII.5 Blocage de tête de ligne

Le blocage de tête de ligne se réfère au fait que le TCP fournit un service de livraison de données dans l'ordre où un segment perdu peut bloquer les segments suivants du bloc les empêchant d'être délivrés à l'application. Ainsi, si les segments 1 et 2 sont envoyés de A à B et que le segment 1 est perdu, le segment 2 ne peut pas être délivré à l'application jusqu'à ce que segment 1 ait été retransmis avec succès.

Pour l'interface considérée, ce blocage tête de ligne peut probablement être surmonté d'une manière relativement satisfaisante en ayant des connexions TCP multiples établies entre le GC et le système CMTS, puis en utilisant l'ensemble des connexions TCP par exemple de façon cyclique pour les transactions. Ainsi, si un segment est perdu sur une connexion, il n'affectera pas les segments, c'est-à-dire les transactions, envoyés sur les autres connexions.

L'inconvénient de cette approche est qu'un segment perdu n'est en principe pas retransmis tant que son temporisateur court (contrairement à un double accusé de réception reçu), étant donné qu'il n'y aurait pas de segments supplémentaires à transmettre jusqu'alors.

XII.6 Démarrage lent de TCP

La capacité de TCP à démarrer la transmission d'un flux de paquets de données est quelquefois limitée par le mécanisme de démarrage lent de TCP, en particulier lorsque le flux est un petit nombre (supérieur à 1) de paquets de données. Il est souhaitable de choisir une fenêtre initiale qui soit plus grande que 1 (tant au début de la durée de vie de la connexion qu'après une récupération d'encombrement suite à la perte d'un seul paquet). Le choix d'une taille de fenêtre initiale de 2 à 4 ms est considéré comme souhaitable. Il est toutefois important de veiller à ce que cette fenêtre initiale ne dépasse pas 4 ms, en raison de la possibilité de provoquer un encombrement.

XII.7 Retard de paquets: algorithme de Nagle

Le protocole TCP/IP a été conçu à l'origine pour prendre en charge plusieurs sessions d'utilisateur sur un réseau lent. Afin d'optimiser l'utilisation du réseau, l'algorithme de Nagle a été introduit pour les utilisateurs effectuant leur entrée au clavier. En résumé, cet algorithme retarde la transmission d'un paquet jusqu'à ce qu'un tampon de transmission suffisamment important soit accumulé ou jusqu'à ce qu'une certaine période de temps (habituellement environ 200 ms) s'écoule.

En raison de la nature en temps réel de ce trafic, il est recommandé de désactiver l'algorithme de Nagle pour la communication GC-CMTS. Sur la plupart des plate-formes Unix, l'algorithme de Nagle peut être désactivé en envoyant l'appel système suivant sur le descripteur de fichier du support:

Exemple 1: réglage de l'option TCP_NODELAY

```
/* set TCP No-delay flag (disable Nagle algorithm) */
int flag = 1;
setsockopt(fd, IPPROTO_TCP, TCP_NODELAY, &flag,
                 sizeof(flag));
```

La plupart des autres langages et plate-formes ont une fonction similaire pour désactiver l'algorithme de Nagle, connue normalement sous le nom option TCP_NODELAY.

XII.8 Interface non bloquante

Par défaut, la plupart des systèmes d'exploitation fournissent une interface bloquante pour les supports TCP/IP. Cela permet un schéma amélioré de récupération d'erreur, mais influe sur les performances du canal de communication.

Essentiellement, un appel système tel que send() avec interface bloquante ne revient jamais tant que le système d'exploitation n'a pas confirmé que le message a été stocké avec succès dans le tampon de transmission.

On peut préférer utiliser une interface non bloquante pour améliorer les performances et prendre en charge des événements asynchrones en utilisant l'appel de fonction select() sur une architecture fondée sur UNIX. Une interface de support non bloquant peut être établie en utilisant l'appel suivant sur le support nouvellement créé.

Exemple 2: réglage de l'option O_NONBLOCK

```
/* set the socket to non blocking */
fcntl( fd, F_SETFL, O_NONBLOCK );
```

La plupart des autres langages et plates-formes ont un dispositif similaire.

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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006