UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.163

(03/2001)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE J: 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

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE J

TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

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

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

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

De nombreux opérateurs de télévision par câble améliorent leurs installations pour fournir une capacité à deux voies et utiliser cette capacité pour fournir des services de données IP haute vitesse conformes aux UIT-T J.83 et J.112. Ces opérateurs souhaitent maintenant étendre la capacité de cette plate-forme de fourniture pour y inclure la téléphonie. La présente Recommandation appartient à une série de Recommandations destinées à atteindre cet objectif. Elle fournit les exigences nécessaires pour la qualité de service dynamique dans de nombreuses applications en temps réel.

Source

La Recommandation J.163 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 9 mars 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T J.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 établit les prescriptions pour qu'un dispositif client obtienne l'accès aux ressources d'un réseau. Il spécifie en particulier un mécanisme global pour qu'un dispositif client demande une qualité de service spécifique à un réseau J.112. De nombreux exemples illustrent l'utilisation de la présente spécification. Le domaine d'application de la présente Recommandation consiste à définir l'architecture de la qualité de service pour la portion "accès" du réseau IPCablecom, fournie aux applications effectuant une demande sur une base flux par flux.

2 Références

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

NOTE – La référence à un document dans la présente Recommandation ne lui confère pas, en tant que document autonome, le statut de Recommandation.

Références normatives

- UIT-T J.83 (1997), *Systèmes numériques multiprogrammes pour la distribution par câble des services de télévision, son et données*.
- UIT-T J.112 (1998), *Systèmes de transmission pour services interactifs de télévision par câble*.
- UIT-T J.112 Annexe A (2001), *Diffusion vidéonumérique: canal d'interaction pour les systèmes de télédistribution par câble*.
- UIT-T J.112 Annexe B (2001), *Interface radioélectrique pour la transmission de données par câble*.
- UIT-T J.160 (2001), *Fonctionnalités opérationnelles pour la fourniture de services numériques multiprogammes de télévision, son et données par des systèmes de distribution multicanaux multipoints*.
- UIT-T J.161 (2001), *Caractéristiques des codecs audio pour la fourniture de services audio bidirectionnels sur des réseaux de télévision par câble au moyen de câblo-modems*.
- IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.
- IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. (Updated by RFC 2750.)
- IETF RFC 2210 (1997), *The Use of RSVP with IETF Integrated Services*.
- IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol*.
- IETF RFC 2865 (2000), *Remote Authentication Dial in User Service (RADIUS)*.

Références informatives

– UIT-T G.114 (2000), *Temps de transmission dans un sens*.

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

– UIT-T G.726 (1999), *Modulation par impulsion et codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s*.

– 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*.

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

– UIT-T J.162 (2001), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur des réseaux de télévision par câble au moyen de modem-câbles*.

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

– UIT-T J.170 (2001), *Spécification de la sécurité IPCablecom*.

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program – Protocol specification*.

– IETF RFC 1890 (1996), *RTP Profile for Audio and Video Conferences with Minimal control*.

– IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

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

– IETF RFC 2543 (1999), *Session Initiation Protocol (SIP)*.

– IETF RFC 2749 (2000), *COPS usage for RSVP*.

– IETF RFC 2750 (2000), *RSVP Extensions for Policy Control*.

– IETF RFC 2753 (2000), *A Framework for Policy Based Admission Control*.

– IETF RFC 2866 (2000), *RADIUS Accounting*.

– Draft-bernet-dclass-01, *Use and Format of the DCLASS Object with RSVP Signalling*, octobre 1999.

– Draft-ietf-rsvp.refresh-reduct-02, *RSVP Refresh Overhead Reduction Extensions*, janvier 2000.

– Draft-davie-intserv-compress-02, *Integrated Services in the Presence of Compressible Flows*, février 2000.

– Draft-ietf-mpls-rsvp-lsp-tunnel-06, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, mai 2000.

– Draft-ietf-rap-pr-02, *COPS Usage for Policy Provisioning* (2000).

– *PacketCable Distributed Call Signalling Specification*, PKT-SP-DCS-D03-000428, 28 avril 2000.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

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

3.2 nœud d'accès: dans le cadre de la présente Recommandation, un nœud d'accès est un dispositif terminal de couche 2 formant l'extrémité réseau de la connexion J.112. Il est spécifique à la technique employée. Il est appelé équipement multimédia d'abonné (INA, *interactive network adapter*) dans l'Annexe A/J.112 et nœud d'accès (AN, *access node*) dans l'Annexe B.

3.3 flux J.112: flux de paquets de données mono ou bidirectionnel, qui est soumis à la signalisation de couche MAC et à l'attribution de la qualité de service (QS) conformément à UIT-T J.112.

3.4 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.

3.5 DOIT: les termes DOIT et NE DOIT PAS sont utilisés par convention dans la présente Recommandation pour dénoter un aspect absolument obligatoire de la spécification.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AN	nœud d'accès (*access node)*
CM	câblo-modem (*cable modem)*
COPS	service commun de politique ouverte (*common open policy service*)
CPE	équipement de local d'abonné (*customer premises equipment*)
DCS	signalisation d'appel répartie (*distributed call signalling*)
INA	adaptateur de réseau interactif (*interactive network adapter*)
IP	protocole Internet (*Internet protocol*)
MTA	adaptateur de terminal multimédia (*media terminal adaptor*)
NCS	signalisation d'appel par le réseau (*network-based call signalling*)
PHS	suppression d'en-tête de charge utile (*payload header suppression*)
RTPC	réseau téléphonique public commuté
QS	qualité de service
RAP	protocole d'allocation de ressources (*resource allocation protocol*)
RSVP	protocole de réservation de ressources (*resource reservation protocol*)
TLV	type-longueur-valeur (*type-length-value*)
VAD	détection d'activité vocale (*voice activity detection*)

5 Aperçu technique

La qualité de service améliorée est requise pour prendre en charge les applications multimédias interactives. Les ressources peuvent être contraintes dans des segments du réseau, nécessitant l'allocation de ressources dans le réseau. Le domaine d'application de la présente Recommandation consiste à définir l'architecture de la QS pour la portion "accès" du réseau IPCablecom. La portion

accès du réseau est définie comme étant située entre l'adaptateur de terminal multimédia (MTA) et le nœud d'accès (AN), y compris le réseau J.112. La présente Recommandation reconnaît également que des réservations par flux peuvent être requises à l'intérieur des locaux du client, les protocoles développés dans la présente Recommandation traitent par conséquent de ce besoin potentiel. Bien que certains segments du réseau de base puissent nécessiter la réservation de ressources pour fournir une qualité de service adéquate, nous considérons que les protocoles relatifs à la gestion des ressources du réseau de base sortent du domaine d'application de la présente Recommandation.

Les ressources sont attribuées sur le réseau J.112 pour les flux individuels associés à chaque session d'une application, par abonné, sur une base autorisée et authentifiée. Une session QS dynamique, ou simplement une session, est définie par la présente Recommandation comme étant 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 QS dynamiques 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.

Deux protocoles de signalisation d'appel IPCablecom sont définis – signalisation d'appel basée réseau (UIT-T J.162) et signalisation d'appel répartie (IETF RFC 2543 SIP). La présente spécification de QS dynamique est la structure de QS sous-jacente pour ces deux protocoles de signalisation d'appel. La QS est attribuée pour les flux associés à une session de concert avec le protocole de signalisation.

La présente Recommandation introduit le concept d'une structure de QS segment par segment. Elle exploite les informations disponibles dans les protocoles de signalisation pour pouvoir attribuer la QS sur le segment "local" (sur le réseau J.112 proche de la partie de départ) et le segment "distant" (le réseau J.112 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'une concaténation 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 pour permettre aux fournisseurs de communications vocales reposant sur des paquets, utilisant la structure IPCablecom, d'utiliser différents modèles de facturation, dont la facturation fixe et la facturation établie sur 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 dépassent le domaine d'application de la présente Recommandation.

La présente spécification de 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 soient invitées à communiquer. Ainsi, les ressources sont réservées avant que le destinataire de la communication soit averti qu'un correspondant essaie de lancer une communication. S'il existe des 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 d'une activation en 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 voix est coupé) et de pouvoir ainsi les

facturer. De plus, étant donné que la seconde phase d'engagement des ressources implique une demande explicite du MTA, elle permet au fournisseur d'empêcher la fraude et le vol de service.

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 J.112. Il est donc nécessaire d'identifier et de suivre les informations qui permettent la conciliation de l'utilisation des ressources de QS J.112 avec l'activité de la session IPCablecom.

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

   Dans le cadre du contrôle des applications, il convient de pouvoir 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 l'engage dans un deuxième temps. Dans le modèle à phase unique, la réservation et l'engagement se produisent comme une seule opération autonome. Comme dans le modèle J.112, les ressources qui sont réservées mais qui ne sont pas encore engagées sont disponibles pour une assignation temporaire à d'autres flux J.112 (par exemple, "au mieux"). La présente Recommandation fournit des mécanismes pour l'activation à deux phases et à phase unique pour les MTA intégrés et pour l'activation en deux phases pour les MTA autonomes. L'activation à phase unique pour les MTA autonomes sera traitée dans des versions ultérieures de la présente Recommandation.

3) *Fournir des politiques IPCablecom définies pour contrôler la QS dans le réseau J.112 et le réseau de base IP*

   Il convient que différents types de sessions puissent avoir 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 exploitant de câble de fournir une QS différente pour différents types de clients (par exemple QS supérieure pour des abonnés d'un service commercial 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 d'une QS améliorée, que le fournisseur veut limiter aux applications vocales, par une application FTP). Même s'il est prévisible que le réseau J.112 applique un accès de l'abonné à la QS, il convient que des mécanismes riches de classification de paquets et de commande de signalisation existent pour préserver l'abonné (et les dispositifs de l'abonné) d'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 J.112*

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

6) *Utilisation d'un mécanisme QS de la couche MAC J.112*

Il convient de pouvoir réguler par une politique (politique définie comme le marquage, l'abandon ou le retard de paquets) tous les aspects de la QS définis au niveau de l'AN en utilisant les mécanismes de QS J.112. Il convient de plus de pouvoir prendre en charge les modèles de mappage de flux multiple – associer une session IPCablecom unique à un flux J.112 unique et des sessions IPCablecom multiples à un flux J.112 unique.

7) *La politique est appliquée par l'AN*

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

8) *Les entités IPC doivent avoir le moins de connaissances possibles des primitives et des paramètres de QS J.112 spécifiques*

Pour IPCablecom, comme pour toute autre application qui utilise le réseau IP, l'objectif de la 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 QS pour les sessions mortes/anciennes*

Il est nécessaire de récupérer et de réaffecter les précieuses ressources de QS précédentes pour les sessions qui ne sont plus actives mais qui n'ont pas été correctement terminées. Il convient qu'il n'y ait pas de "fuites" dans la liaison J.112. Par exemple, si un module client IPCablecom ne fonctionne pas correctement au milieu d'une session IPCablecom, il convient que toutes les ressources QS J.112 utilisées par la session soient libérées dans un délai raisonnable.

10) *Changements de politique de la 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 (exemple, passage d'un service "bronze" à un service "or") sans réinitialiser le CM.

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

Il convient que le réseau IPCablecom permette l'émulation et l'amélioration de l'expérience que l'utilisateur a du RTPC et qu'il présente la même qualité, voire une meilleure qualité, 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 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*

Il convient que le service IPCablecom puisse changer la QS à mi-session, par exemple réglage de ressources à l'échelle du réseau ou création de paramètres CODEC compatibles (nécessitant des changements de QS) ou fonction définie par l'utilisateur pour varier les niveaux de QS ou détection de flux de télécopie ou modem (nécessitant un changement de CODEC de compression à G.711).

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

Des arguments irréfutables peuvent être avancés sur le fait que la signalisation de la QS soit initiée côté abonné et 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 qui sont d'homologue à homologue. Dans la signalisation côté réseau, l'implémentation de l'application de l'extrémité peut ne pas avoir connaissance de la QS (en particulier dans le réseau J.112). La signalisation côté réseau prend en charge des modèles d'application qui sont du type client-serveur (avec serveur validé). 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 depuis un MTA intégré et un MTA autonome*

Il convient de pouvoir signaler la QS depuis un MTA intégré et un MTA autonome. Dans un MTA autonome, le seul chemin de signalisation pris en charge est celui spécifié dans la présente Recommandation en utilisant le protocole RSVP. Dans un MTA intégré, l'accès RSVP et direct à la signalisation MAC J.112 est possible.

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 périphériques suivants. Ces dispositifs résident au niveau du site client et sont connectés par l'intermédiaire du canal J.112 au réseau. 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 ajouter des capacités d'entrée/sortie vidéo dans la configuration MTA-2 existante. 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 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 J.112 au réseau J.112;

2) **MTA autonome**: il s'agit d'un terminal multimédia client qui implémente la fonctionnalité multimédia sans incorporer une interface de couche MAC J.112. Le MTA autonome utilisera généralement Ethernet, USB, ou IEEE 1394 comme interconnexion physique à un CM. Le MTA autonome peut être connecté à un réseau client et utiliser des équipements de transport du réseau client (comprenant généralement des routeurs IP intermédiaires) pour établir des sessions sur le réseau J.112.

5.2.2 Câblo-modem (CM)

Il s'agit d'un élément de réseau IPCablecom défini par UIT-T J.112. Le CM est responsable de classer, réguler par une politique et marquer les paquets une fois que les flux de trafic sont établis par les protocoles de signalisation décrits dans la présente Recommandation.

5.2.3 Nœud d'accès (AN)

Le nœud d'accès (AN) est l'élément du réseau IPCablecom qui contient les fonctions centralisées responsables du traitement des flux d'information. L'AN agit comme un point d'application de la politique (PEP, *policy enforcement point*) conforme au cadre protocole d'allocation de ressources (RAP, *resource allocation protocol*) de l'IETF.

L'AN implémente une "porte de QS dynamique IPCablecom" (appelée simplement ci-après "porte") entre le réseau J.112 et un réseau de base IP. La porte est implémentée en utilisant les fonctions de classification de paquets et de filtrage définies dans UIT-T J.112.

L'AN 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 différentiés (*Diffserv, differentiated services*).

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

L'entité serveur de gestion des appels 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"). Un CMS utilisant le modèle de signalisation d'appel contrôlé par le réseau implémente un agent d'appel qui contrôle directement la session et maintient l'état appel par appel. Un CMS utilisant le modèle de signalisation d'appel distribué peut servir de "DCS mandataire" (DCS *Proxy*) et n'exécute les services que pendant l'établissement initial de la session. 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 contrôle le fonctionnement des portes implémentées sur un AN. Le GC agit comme point de décision de politique (PDP) conforme au cadre du protocole d'allocation de ressources (RAP, *resource allocation protocol*) de l'IETF.

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 la QS dynamique IPCablecom repose sur UIT-T J.112, le protocole RSVP de l'IETF et la QS services intégrés garantis (*integrated services guaranteed*) de l'IETF.

En particulier, l'architecture de la QS IPCablecom utilise le protocole tel que défini dans UIT-T J.112 au sein du réseau de télévision par câble. Ces messages prennent en charge l'installation statique et dynamique de classificateurs de paquets (par exemple Filter-Specs) et les mécanismes de programmation de flux (par exemple flow specs) pour délivrer une qualité de service améliorée. La QS J.112 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 RSVP (*Resource Reservation Protocol*) de l'IETF. Il est ainsi possible de définir les réservations de ressources de la QS sur une base flux par flux.

Dans l'architecture de la QS J.112, les flux J.112 sont considérés comme étant unidirectionnels ou bidirectionnels. Dans chaque sens, les flux J.112 sont soumis aux opérations indiquées ci-dessous.

Le CM, lorsque le trafic entre dans le réseau J.112 autorisé à la QS, se charge des fonctions suivantes:

- classification d'un trafic IP dans les flux J.112 basée sur les spécifications de filtrage définies;
- exécution du "shaping" et du "policing" de trafic tels que requis par la spécification de flux;
- maintien de l'état pour les flux actifs;
- modification du champ TOS dans les en-tête IP amont en fonction de la politique de l'opérateur du réseau;
- obtention de l'AN de la QS J.112 requise;
- application correcte des mécanismes de QS J.112.

L'AN est chargé des fonctions suivantes:

- délivrance au CM de la QS requise reposant sur la configuration de la politique;
- allocation de la bande passante amont conforme aux demandes du CM et aux politiques de QS du réseau;
- classification de chaque paquet provenant de l'interface côté réseau et assignation de ce paquet à un niveau de QS basé sur les spécifications de filtrage définies;
- politique du champ TOS dans la réception des paquets du réseau J.112 pour appliquer les réglages du champ TOS conformes à 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 du "shaping" et du "policing" de trafic tels que requis par la spécification de flux;
- envoi des paquets aval au réseau J.112 en utilisant la QS assignée;
- envoi des paquets amont au dispositif du réseau de base en utilisant la QS assignée;
- maintien de l'état pour les flux actifs.

Le réseau de base peut utiliser des mécanismes basés sur les services intégrés de l'IETF ou utiliser des mécanismes de services différentiés de l'IETF. Dans un réseau de base du type Diffserv, les routeurs du réseau envoient un paquet en fournissant la QS appropriée de l'IETF, en fonction du réglage du champ TOS. Dans un réseau de base du type Diffserv, aucun état par flux est requis dans les dispositifs du réseau central.

5.4 Interfaces de la QS

Les interfaces de signalisation de la qualité de service sont définis entre de nombreux composants du réseau IPCablecom comme l'indique la Figure 1. La signalisation implique la communication des exigences relatives à la 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 J.112). Par ailleurs, l'exigence d'application de la politique et de liaison de systèmes entre la fourniture à l'abonné OSS, le contrôle d'admission dans le réseau de base IP géré et le contrôle d'admission dans le réseau J.112 impliquent des interfaces supplémentaires entre les composants du réseau IPCablecom.

Le cadre de l'architecture IPCablecom, UIT-T J.160, représenté à la Figure 1, contient une explication étendue du cadre de l'architecture de la QS.

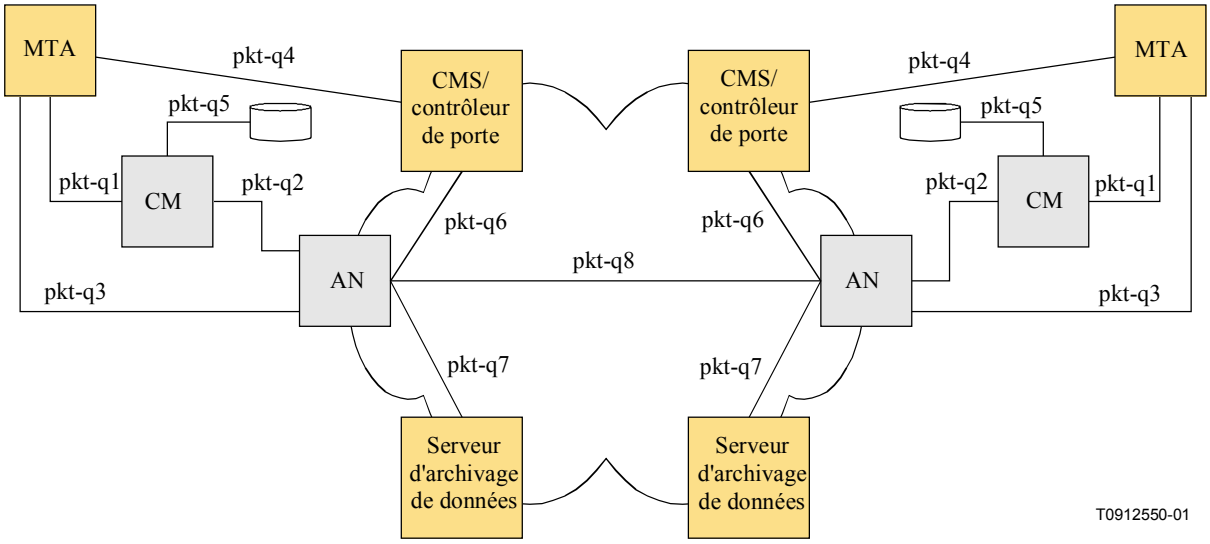


Figure 1/J.163 – Interfaces de signalisation de la QS dans le réseau IPCablecom

Les interfaces pkt-q1 à pkt-q8 sont disponibles pour contrôler et traiter la QS. Toutes les interfaces ne sont pas utilisées dans toutes les configurations et variations de protocole. 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. Deux alternatives apparaissent pour cette spécification. Tout d'abord, une interface générale, qui soit applicable à un MTA intégré ou autonome, deuxièmement une interface en option qui soit uniquement à la disposition des MTA intégrés.

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

Interface	Description	QS dynamique MTA intégré/autonome	QS dynamique MTA intégré (option)
pkt-q1	MTA-CM	N/A	Interface de couche MAC J.112
pkt-q2	CM-AN	QS J.112, initié par l'AN	QS J.112, initié par le CM
pkt-q3	MTA-AN	RSVP+	N/A
pkt-q4	MTA-GC/CMS	NCS/DCS	NCS/DCS
pkt-q5	Serveur fournissant le CM	N/A	N/A
pkt-q6	GC-AN	Gestion de porte	Gestion de porte
pkt-q7	AN-RKS	Facturation	Facturation
pkt-q8	AN-AN	Gestion de porte	Gestion de porte

pkt-q1: interface entre le MTA et le CM

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

- contrôle: utilisé pour gérer les flux J.112 et leurs paramètres de trafic de QS et règles de classification associées;
- synchronisation: utilisée pour synchroniser la paquétisation et la programmation pour réduire le retard et la gigue;

- transport: utilisé pour traiter les paquets dans le flux de média et exécuter le traitement approprié de la QS par paquet.

La conception de cette interface est définie dans UIT-T J.112. Pour les MTA autonomes, aucune instance de cette interface n'est définie.

pkt-q2: interface de QS J.112 entre CM et AN

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

pkt-q3: interface de couche Réseau entre le MTA et l'AN

L'interface est utilisée pour demander la bande passante et la QS en termes de délai en utilisant le RSVP standard et les extensions spécifiées dans la présente Recommandation. En résultat des échanges de messages entre le MTA et l'AN, les flux J.112 sont activés en utilisant une signalisation au départ de l'AN sur l'interface pkt-q2.

pkt-q4: 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 paquétisation. DCS et NCS sont deux exemples de signalisation de la couche Application.

pkt-q5: signalisation depuis la fourniture J.112/IPCablecom au CM

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

pkt-q6: interface entre le GC/CMS et l'AN

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 d'autoriser la QS. Concernant l'admission et l'autorisation dans le contexte de IPCablecom, une relation d'approbation doit exister entre le GC/CMS et l'AN.

pkt-q7: AN vers serveur d'archivage (RKS)

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

pkt-q8: AN vers interface AN

Cette interface est utilisée pour la coordination des ressources (portes) entre l'AN du MTA local et l'AN du MTA distant. L'AN est chargé de l'allocation et la politique des ressources de la QS dans le réseau J.112 qu'il gère.

5.5 Cadre pour la QS IPCablecom

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

- retard faible: le retard de paquet de bout en bout 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 réseau de base peut absorber une quantité importante de ce budget de retard, il est important de contrôler le retard sur le canal d'accès, au moins pour les appels longue distance;

- perte de paquet faible: il est nécessaire que la perte de paquets soit le plus faible possible pour que la qualité de la voix ou les performances des modems 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 au remplacement du service téléphonique à commutation de circuits existant. Les exigences de perte pour une performance de modem à bande vocale acceptable sont mêmes plus strictes que celles relatives à la voix;
- délai d'attente court après numérotation: il est nécessaire que le délai entre l'utilisation signalant 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;
- délai court après prise d'appel: il est nécessaire que le délai entre le moment où un utilisateur prend l'appel sur un téléphone qui sonne et la traversée du chemin de la voix 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 assure que l'utilisation de ressources est correctement prise en compte, de manière cohérente avec les conventions du service de liaisons téléphoniques 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.

Afin de prendre en charge les exigences présentées ci-dessus, les protocoles de QS assurent que toutes les ressources sont engagées pour tous les segments de transport avant que les protocoles de signalisation 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 pour les utilisateurs de déjouer les contrôles de la 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" utilisable pour transférer frauduleusement des données dans un sens reste en service. 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 repose sur des normes et des pratiques existantes et que les résultats de ce travail soient utilisables pour prendre en charge des modèles d'appel alternatifs. Ces souhaits ont conduit à l'utilisation du protocole en temps réel

---

[1] L'UIT-T G.114 établit qu'un délai dans un sens de 150 ms est acceptable pour la plupart des utilisations de l'utilisateur. Toutefois, des applications voix et données hautement interactives 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.

(RTP, *real time protocol*) de l'IETF pour acheminer des données multimédias, 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 un surensemble du protocole de réservation de ressources (RSVP) de l'IETF.

Il convient que l'architecture de la QS fournisse 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 multimédias. Nous n'avons pas encore examiné si les améliorations apportées à la gestion des ressources présentées ici prendront en charge la multidiffusion de façon transparente.

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 réseau de base et le réseau d'accès côté arrivée de la session. Les ressources de réseau J.112 sont gérées sur la base de flux J.112, en utilisant les mécanismes définis dans UIT-T J.112. Les ressources du réseau de base peuvent être gérées soit au flux ou, de façon plus vraisemblable, par un mécanisme de qualité de service agrégé. La gestion des ressources du réseau de base sort du domaine d'application de la présente Recommandation.

La Figure 2, cadre de la session, représente graphiquement ce modèle. Cette Recommandation prend en charge un environnement client où un MTA autonome peut être connecté au CM via un réseau de liaisons et de routeurs standards compatibles au protocole RSVP.

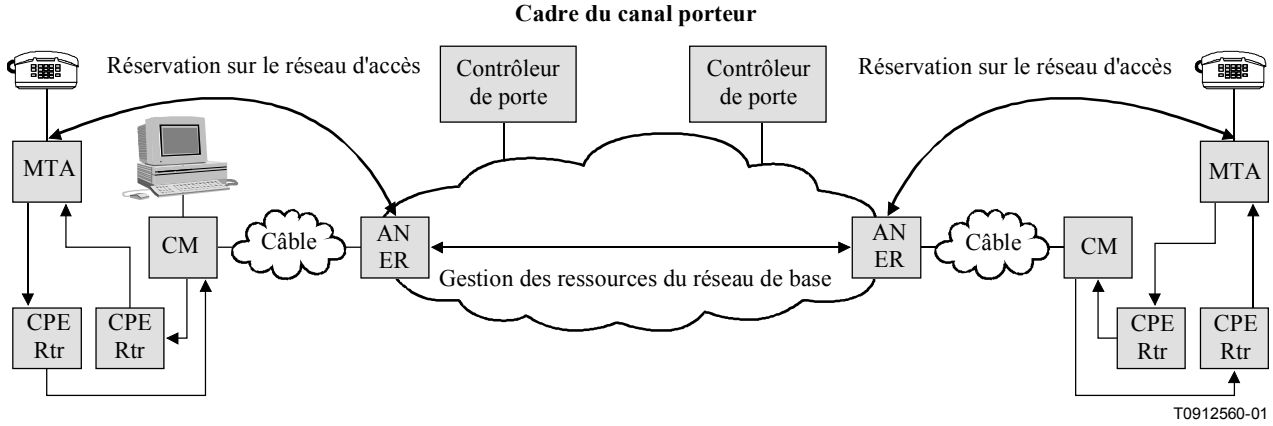


Figure 2/J.163 – Cadre de la session

Une structure définie par la QS appelée *porte* fournit un point de contrôle pour la connexion des réseaux d'accès à un service de réseau de base de grande qualité. Une porte est implémentée par un AN et se compose d'un classificateur de paquets, d'un régulateur de trafic et d'une interface avec une entité qui collecte les données statistiques et les événements (tous ces composantes existent dans le réseau J.112). 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 basé 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 d'une adresse IP source et d'un numéro de port spécifiques à 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 d'une adresse source IP spécifique à une adresse IP de destination et un numéro de port spécifiques.

Une porte est une entité logique qui réside dans un AN. Une identification de porte (*GateID*) est associée à une session individuelle et est significative au niveau de la porte; GateID est un identificateur qui est logiquement unique au niveau de l'AN et qui assigné par cet AN. Une porte est par nature unidirectionnelle. Si une porte est "fermée", les données dans le sens amont/aval sur le réseau d'accès J.112 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 à l'avance d'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. Ces derniers flux peuvent être transportés sur différents flux J.112 dans le réseau J.112, tels qu'une liaison de signalisation dédiée.

5.6 Exigences relatives à 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 voix et implique une gestion des ressources active dans les réseaux d'accès et de base. 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 sur une base de bout en bout, même en cas de surcharge ou de conditions inhabituelles. Le fournisseur de services peut chercher à obtenir des revenus supplémentaires en fournissant 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 garantir l'accès uniquement à des utilisateurs autorisés et authentifiés sur une base session par session et qu'il n'y ait 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 basée sur la disponibilité des ressources et sur les informations de politique associées à la porte.

Dans les réseaux J.112, la capacité des réseaux est limitée et il est nécessaire d'effectuer la gestion des ressources sur une base flux par flux. Dans le réseau de base, plusieurs alternatives sont possibles, allant du contrôle d'admission flux par flux saut par saut à la fourniture de ressources "grossières". La présente Recommandation ne traite que de la QS des réseaux d'accès et ignore les schémas de QS des réseaux de base.

Cette architecture vise à fournir un degré élevé de généralités afin de susciter l'émergence de nouveaux services et une évolution future des architectures de réseau. Cet objectif implique plusieurs exigences pour une architecture de QS viable décrite dans les paragraphes suivants.

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 une QS améliorée associée au service de communications vocales. Le CMS/contrôleur de porte 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 AN. 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, de manière cohérente 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 assignées. 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 une base liée à 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 en deux phases

Un protocole en deux phases pour l'engagement de ressources est essentiel pour un service de niveau commercial de communications vocales, pour deux raisons liées aux exigences propres 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 traverser. Ces propriétés sont fournies par les protocoles conventionnels de signalisation de téléphonie; nous souhaitons simplement émuler la même sémantique ici. Par ailleurs, si la bande passante est allouée avant que l'extrémité distante 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 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 traverse après la première phase du protocole de gestion des ressources.

5.6.3 Assignation segmentée des ressources

L'architecture de la QS dynamique sépare la gestion des ressources en segment distincts du réseau d'accès et du réseau de base. L'assignation de ressources segmentée est avantageuse à double titre:

- elle tient compte des différents mécanismes de fourniture et de signalisation pour le réseau du demandeur, le réseau de l'extrémité distante et le réseau de base;
- 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 réseau de base ont suffisamment de ressources pour gérer les ressources plus grossièrement, elle permet au réseau de base d'éviter de conserver un état par flux et d'améliorer ainsi l'évolutivité.

Lorsque le réseau de base ne requiert pas une signalisation par flux (comme pour un réseau de base 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 qui est stockée 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 le protocole RSVP qui peut être interprété saut par

saut sur le réseau local (c'est-à-dire de l'utilisateur) et le réseau d'accès (ou en option pour les clients intégrés, l'interface de la couche MAC J.112). L'AN mappe les messages de gestion des ressources avec le protocole de gestion des ressources utilisé sur le réseau de base (par exemple, diffserv de l'IETF). Il mappe également le message de gestion des ressources avec le protocole de gestion des ressources utilisé sur la liaison d'accès (c'est-à-dire UIT-T J.112).

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 la session. Ceci facilite les changements à mi-session tels qu'une commutation depuis un codec voix à débit lent et G.711 lorsque des tonalités de modem sont détectées et l'adjonction de données vidéo à une session qui commence comme une session de voix seule.

5.6.5 Association dynamique de ressources

L'association dynamique de ressources ("re-réservation") est une exigence nécessaire pour permettre l'utilisation efficace des ressources lorsque des services tels que la mise en instance d'appel (CW, *call waiting*) sont invoqués. De façon abstraite, la re-réservation prend la bande passante allouée pour 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 la 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 Performance 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 réseau de base et le nombre de messages J.112 amont. Sur un réseau J.112, sur lequel il n'est pas possible que des chemins vers l'avant ou vers l'arrière soient différents, ce protocole ajoute plusieurs nouveaux objets au protocole RSVP, ce qui permet à l'AN de réduire le temps d'attente en agissant comme mandataire pour le client de l'extrémité distante.

Les messages RSVP, les messages de gestion J.112 et les messages de signalisation d'appel (désignés collectivement par l'expression messages de signalisation) sont tous transportés "au mieux" (principe du "*best effort basis*" = au mieux) sur le réseau J.112. Si le CM prend également en charge des services de données, le service "au mieux" peut être incapable de fournir le temps d'attente bas nécessaire pour les messages de signalisation. Dans cette situation, un flux J.112 séparé, avec une QS améliorée, pour transporter le trafic de signalisation PEUT être fourni au CM. Ce flux J.112 séparé est délivré de la même manière que les autres flux de média J.112 et PEUT inclure des classificateurs tels que leur 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 la QS pour les sessions désignées par le fournisseur de services pour avoir une priorité supérieure (par exemple appels d'urgence) connaissent une probabilité de blocage inférieure à des sessions normales. La détermination de la classe à assigner 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 (par exemple, première étape INVITE dans le cas de SIP IETF RFC 2543) est effectuée.

5.6.8 Prise en charge du réseau intermédiaire

Il convient que l'architecture n'interdise pas les réseaux intermédiaires entre le MTA ou l'hôte multimédia et le CM (par exemple, réseau du client). Bien que le réseau intermédiaire ne puisse pas tomber dans le domaine ou la responsabilité administrative de l'opérateur de câble, l'allocation de bande passante dans le réseau J.112 de l'opérateur de câble est possible lorsqu'un réseau intermédiaire existe. 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 réseau de base

Il est possible qu'un mécanisme permettant de gérer explicitement les ressources du réseau de base soit nécessaire. Le domaine d'application de la présente Recommandation est la QS sur un réseau J.112, mais l'architecture fournit des interfaces ouvertes, suffisamment générales qui sont compatibles avec de nombreux mécanismes de QS connus sur les réseaux de base.

5.7 Théorie de fonctionnement

5.7.1 Etablissement de la session de base

La réservation de ressources est divisée en deux phases séparées, une phase de réservation (*Reserve*) et une phase d'engagement (*Commit*). 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 démarré pour que l'utilisateur puisse être facturé pour l'utilisation.

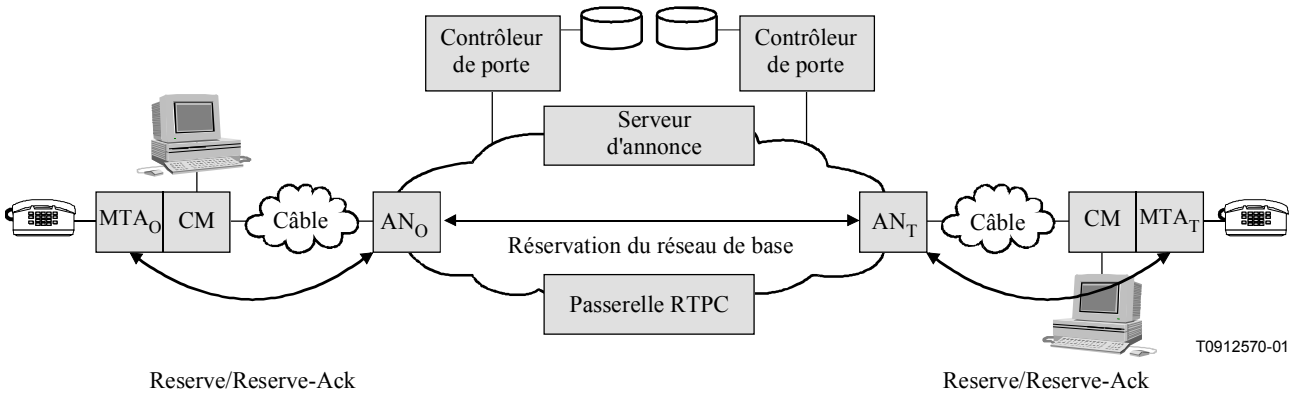


Figure 3/J.163 – Gestion des ressources phase 1

La Figure 3 représente la première phase du protocole de gestion des ressources pour une application multimédia. Dans cette description, les indices "O" et "T" désignent les points d'origine et d'arrivée de l'appel. Le MTA peut être soit un hôte VoIP autonome soit un MTA intégré; ce dernier est indiqué dans la Figure 3. MTA_O et MTA_T demandent la réservation de ressources (message PATH dans le protocole RSVP ou message J.112 dans l'interface optionnelle pour clients intégrés) respectivement à AN_O et AN_T. AN_O et AN_T effectuent une vérification de contrôle d'admission pour la disponibilité des ressources (en initiant au besoin la signalisation pour la réservation de ressources dans le réseau de base) et envoient une réponse aux MTA respectifs. Dans le cadre de RSVP, le message RESV provenant de l'AN (où la porte réside) est l'accusé de réception au MTA.

La Figure 4 représente la seconde phase. Après avoir déterminé la disponibilité des ressources, MTA_O envoie un message RING à MTA_T en lui donnant l'instruction de commencer à faire sonner le téléphone. MTA_T envoie une indication RINGING à MTA_O en indiquant que les ressources sont disponibles et que le message RING a été reçu. Lorsque l'appelé décroche son téléphone, MTA_T envoie un message ANSWERED à MTA_O et un message COMMIT à AN_T. Lorsque MTA_O reçoit le message ANSWERED, MTA_O envoie un message COMMIT à AN_O. Les messages COMMIT provoquent l'allocation des ressources pour l'appel dans les réseaux J.112. L'arrivée des messages COMMIT au niveau de AN_T et AN_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 AN coordonnent l'ouverture des portes en échangeant des messages GATE-OPEN.

Les messages RING, RINGING et ANSWERED représentés dans la Figure 4 et dans la description ci-dessus sont des équivalents logiques des messages de signalisation d'appel échangés par J.162 et SIP IETF RFC 2543.

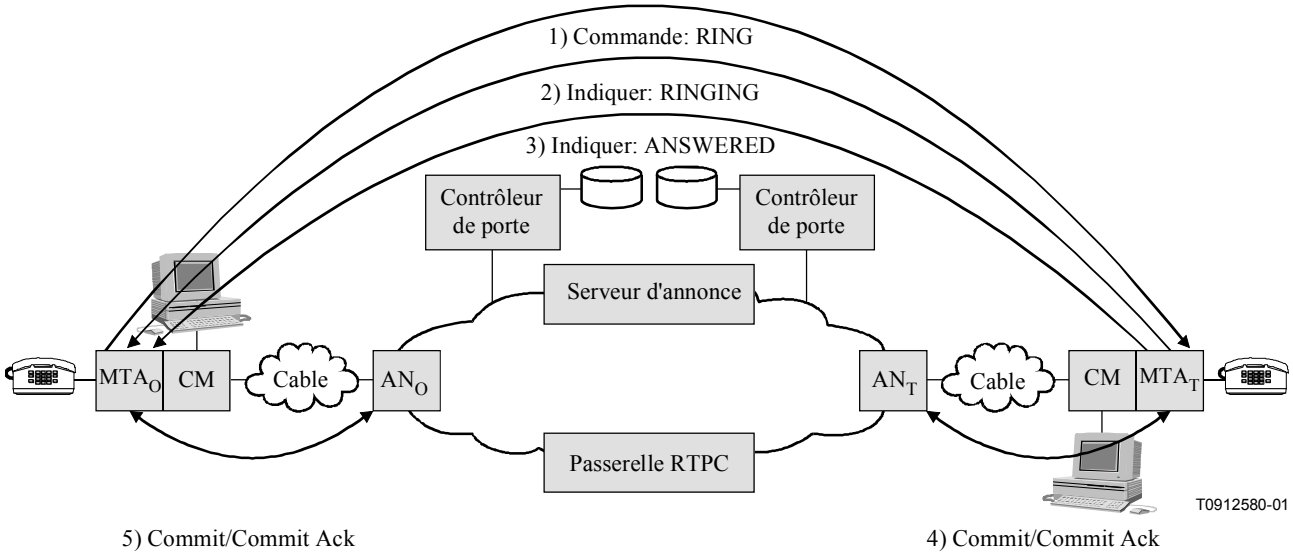


Figure 4/J.163 – Gestion des ressources phase 2

5.7.2 Coordination des portes

La signalisation de la QS amène la création d'une porte au niveau de chaque AN 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 de protocole résistent aux abus[2]. Un protocole de coordination de portes garantit les points suivants:

- éviter la possibilité d'établir une session sans facturation. Parce que les clients peuvent avoir l'intelligence adéquate et ne sont pas sécurisés, il est envisageable que des clients établissent deux sessions à une voie pour fournir aux utilisateurs un canal de communication vocale interactif adapté. La coordination des portes empêche l'établissement de telles sessions sans que le fournisseur puisse facturer ces sessions;

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

- les ressources réservées et engagées par les deux clients sont cohérentes avec les résultats de la négociation de capacités. Si un seul client paie pour une session, il est important que les ressources qui sont réservées et utilisées soient cohérentes avec les attentes du payeur. La coordination des portes empêche à un destinataire malveillant de définir des caractéristiques d'une session qui résulteraient en une charge anormalement élevée pour l'émetteur;
- les portes s'ouvrent et se ferment pratiquement simultanément (c'est-à-dire avec un écart de l'ordre de quelques centaines de millisecondes). La coordination des portes garantit que les données de facturation aux deux extrémités de la session sont cohérentes, de sorte que le coût de la session ne dépend pas de quelle extrémité paie pour cette session.

5.7.3 Changement des classificateurs 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 demandent de changer les clients impliqués dans une session, par exemple lorsqu'une session est transférée ou réacheminée ou pendant une conférence à trois. Ceci nécessite que les classificateurs 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 5, Ressources autorisées, réservées et engagées. Un ensemble de ressources est représenté par un espace à *n* dimensions (représenté ici comme un espace à 2 dimensions) où *n* est le nombre de paramètres (par exemple, bande passante, taille des rafales, gigue, classificateurs) nécessaires pour décrire les ressources. Les procédures exactes pour comparer les vecteurs de ressources à *n* dimensions sont données dans UIT-T J.112.

Lorsqu'une session est établie, les protocoles QS dynamique autorisent l'utilisation d'une certaine quantité de ressources maximale 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 continuer, 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.

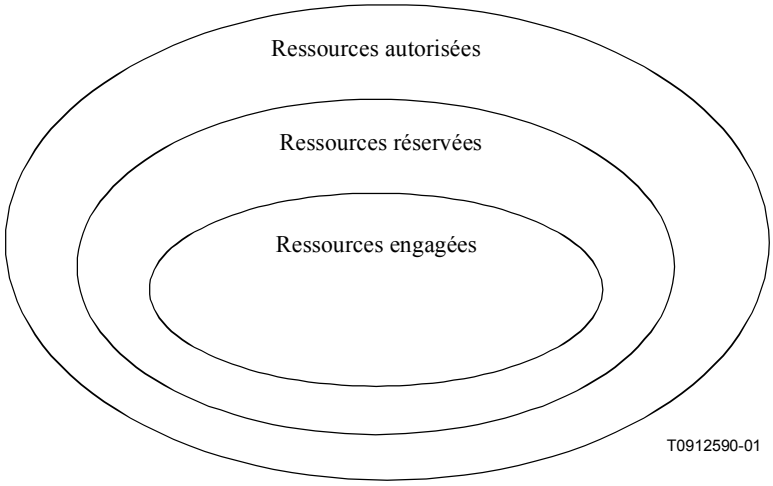


Figure 5/J.163 – Ressources autorisées, réservées et engagées

Les autorisations affectent uniquement 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 la manipulation 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 par l'AN et sort du domaine d'application de QS dynamique.

Les ressources excédentaires, réservées au-dessus de celles engagées, sont libérées à moins que le client demande explicitement qu'elles soient conservées par l'intermédiaire d'opérations périodiques de rafraîchissement de la réservation. Cette condition est déconseillée 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 de l'AN puisse utiliser une ou plusieurs classes de session pour des ressources réservées depuis un MTA. Les classes de session définissent des politiques de contrôle d'admission à fournir ou leurs paramètres. Il est prévu que le fournisseur indique les paramètres nécessaires et/ou les politiques de contrôle d'admission alternatives dans l'AN 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 de l'AN par le contrôleur de porte dans le message Gate-Set, le contrôleur de porte inclut des informations adéquates pour indiquer quelle classe de session devrait s'appliquer lorsque la demande RESERVE correspondante est traitée.

5.7.6 Renégociation des ressources

Plusieurs des fonctions de la session prises en charge nécessitent plusieurs renégociations des paramètres de QS associées 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 débit binaire faible. 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 généralement 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 Commit 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 du 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 de fonction 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 identifiés. 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 AN. Ceci améliore l'efficacité avec laquelle les ressources dans un réseau J.112 sont utilisées.

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 session qui, en général peuvent ne pas avoir besoin de la même quantité de ressources. Ainsi l'opération *re-commit* 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 identificateur, appelé Identification 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 l'AN. 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 l'AN est l'endroit approprié pour effectuer la comptabilité des ressources, étant donné que l'AN est directement impliqué dans la gestion des ressources fournies à un client. Il est également important d'effectuer la comptabilité de l'utilisation dans l'AN pour faire face aux défaillances des clients. Si un client qui est impliqué dans une session active tombe en panne, l'AN DOIT détecter cette défaillance et arrêter la comptabilité de l'utilisation pour la session. Ceci peut être effectué en utilisant un état souple (*soft state*) par l'intermédiaire d'un message de rafraîchissement des ressources (par la transmission périodique de messages RSVP-PATH pour une

session active), 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 l'AN. 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 l'AN 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. Les données opaques fournies par le contrôleur de porte qui peuvent être appropriées pour le serveur d'archivage peuvent également être incluses dans le message. Les exigences pour traiter les enregistrements d'événement sont contenues dans d'autres spécifications de la prise en charge des opérations.

5.7.9 Gestion des ressources du réseau de base

Lorsqu'un AN 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, l'AN peut soit générer un nouveau message de réservation de ressources sur le réseau de base soit envoyer au réseau de base une version modifiée du message de réservation de ressources reçu du MTA. L'AN effectue tout mappage spécifique à la technologie du réseau de base qui est nécessaire. Ceci permet à l'architecture de prendre en charge différentes technologies de réseau de base, au choix du fournisseur de services. Les mécanismes spécifiques de réservation de la QS sur le réseau de base sortent du domaine d'application de la présente Recommandation.

Un modèle bidirectionnel est utilisé pour la réservation de ressources dans un réseau J.112 où le routage est symétrique. Un modèle unidirectionnel est utilisé pour la réservation de ressources dans le réseau de base, ce qui permet des asymétries de routage. Par conséquent, lorsque MTA_O effectue une réservation avec l'AN, il connaît deux choses: qu'il a une bande passante adéquate dans les deux directions sur le réseau J.112 et qu'il a une bande passante adéquate sur les réseaux de base pour le flux MTA_O vers MTA_T. Par conséquent, MTA_O sait que les ressources sont disponibles de bout en bout dans les deux sens une fois qu'il reçoit une réponse de MTA_T.

5.7.10 Réglage du point de code DiffServ

Cette architecture tient compte de l'utilisation d'un réseau de base à services différentiés, où 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 différentié sont fournis aux paquets avec le codage approprié de bits dans le champ de l'en-tête IP spécifié pour le service différentié. 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 Precedence de l'octet IPv4 TOS [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 réseau de base du fournisseur en provenance de l'AN. Etant donné que les ressources consommées par ces paquets dans le réseau de base 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 d'une QS améliorée plutôt que de sécuriser le MTA. Le fournisseur peut configurer des politiques dans l'AN qui déterminent comment régler le DSCP pour des flux qui transitent par l'AN. Ces politiques sont envoyées à l'AN dans le protocole d'établissement de portes par le CMS/GC.

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. Ceci est effectué avec l'objet DCLASS dans le protocole RSVP, proposé par l'IETF. L'AN a encore besoin de réguler par une politique 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.

6 Protocole de qualité de service MTA vers AN (pkt-q3)

Pour répondre aux exigences décrites précédemment, le protocole RSVP et l'architecture de services intégrés de l'IETF, IETF RFC 2210 sont utilisés pour servir de base au mécanisme de signalisation afin de fournir la QS locale. Le protocole RSVP, tel qu'il est actuellement spécifié, a besoin de quelques améliorations pour répondre aux exigences de l'architecture de QS dynamique.

Le protocole RSVP et l'architecture de services intégrés spécifient les paramètres de QS en termes génériques indépendamment de la technologie de la couche 2 sous-jacente. Il est nécessaire de spécifier un moyen de mappage entre ces spécifications générales de trafic et les spécifications de flux J.112 spécifiques. Ces mappages existent pour les autres protocoles de la couche 2 (par exemple, ATM, LAN IEEE 802.XX). Le présent paragraphe décrit les mappages pour les réseaux J.112.

L'architecture de QS dynamique utilise un surensemble de RSVP avec les différences suivantes:

- étant donné que les réservations de ressources sont initiées indépendamment pour chaque réseau J.112 (modèle d'allocation de ressources segmentée), la présente Recommandation ne dépend pas des messages de gestion des ressources qui se propagent de bout en bout;
- l'échange de gestion des ressources entre le MTA et l'AN réserve des ressources dans les *deux* sens sur la zone locale (c'est-à-dire, exploitée par le client) et les réseaux J.112. Ceci permet à l'AN d'agir comme mandataire pour l'extrémité distante, en présentant l'avantage de réduire le nombre de messages requis pour la gestion des ressources dans les réseaux J.112 contraints par la bande passante et de réduire le délai après numérotation et le délai après prise d'appel;
- dans la portion de la zone locale (c'est-à-dire, exploitée par le client) du réseau, les routeurs compatibles avec le protocole RSVP peuvent être présents. Dans cet environnement, des réservations unidirectionnelles sont requises. Pour activer ces deux fonctions (réservations bidirectionnelles sur le réseau J.112 et réservations unidirectionnelles à l'intérieur du site du client), un message PATH amélioré est envoyé par le MTA à la porte;
- la capacité à lier un seul ensemble de ressources à un groupe de réservations multiples, à partir d'informations du MTA indiquant que seule une réservation dans le groupe sera active à un moment donné;
- prise en charge de la facilité d'activation de ressources en deux phases disponible dans le protocole J.112, en garantissant que les ressources sont disponibles avant de faire sonner le téléphone de l'extrémité distante. L'échange du protocole RSVP avec l'AN effectue la première phase, le contrôle d'admission et le MTA envoie un message séparé à l'AN pour effectuer l'activation.

L'opération qualité de service dynamique (*Dynamic Quality of Service*) ne concerne pas le protocole RSVP standard qui peut ou non être pris en charge. Indépendamment, les messages RSVP standards ne déclencheront pas les opérations QS dynamique spécifiées dans la présente Recommandation.

6.1 Aperçu des extensions de RSVP

6.1.1 Exploitation segmentée

Tel que défini dans IETF RFC 2205, le protocole RSVP est prévu pour opérer entre deux hôtes. Toutefois, le modèle de QS IPCablecom nécessite que la signalisation soit effectuée de manière segmentée, lorsqu'un segment se trouve entre un MTA et un AN. Le présent paragraphe illustre comment le protocole RSVP peut prendre en charge un modèle segmenté.

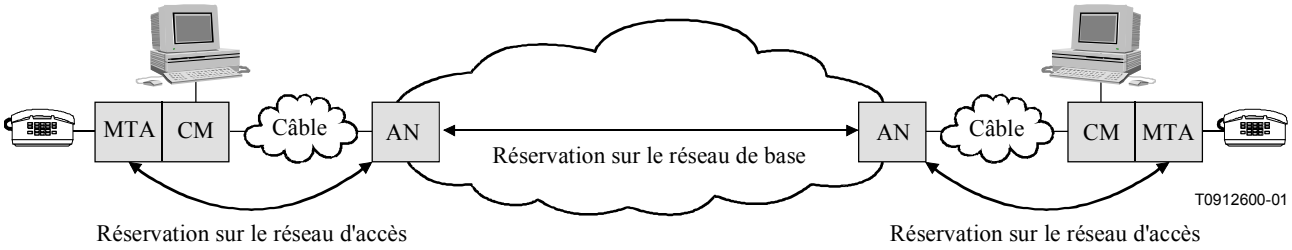


Figure 6/J.163 – Modèle de signalisation segmenté

Dans le modèle segmenté, un MTA communique avec l'AN. En plus du scénario simple représenté à la Figure 6, la présente Recommandation permet des scénarios plus complexes, par exemple lorsqu'il existe un réseau privé entre le client et le CM, qui peut comprendre une grande diversité d'éléments de réseau, y compris des commutateurs ou des routeurs compatibles avec le protocole RSVP. La présence d'un réseau privé signifie que la solution fonctionne même si le client et l'AN ne sont pas immédiatement adjacents à la couche IP. Le réseau privé peut fournir des trajets multiples entre le client et le CM, offrant la possibilité de chemins asymétriques dans ce réseau.

L'AN intercepte les messages RSVP envoyés depuis le MTA de départ au MTA situé côté arrivée de la session pour implémenter le modèle segmenté. Ceci réduit les changements apportés au RSVP, en conservant l'adresse de destination des messages PATH identique à l'adresse de destination des données.

6.1.2 Réservations bidirectionnelles

Le protocole RSVP traditionnel procède à des réservations unidirectionnelles. Le flux de messages PATH dans le même sens que les données et le flux de messages RESV dans le sens opposé. Pour effectuer une réservation bidirectionnelle, il est nécessaire d'ajouter de nouveaux objets RSVP pour définir les deux sens. L'AN répond à la demande en établissant des réservations dans les deux sens de la liaison J.112. S'il existe des routeurs compatibles avec le protocole RSVP entre le MTA de départ et le CM, alors l'AN envoie un message PATH qui apparaît provenir du client distant.

6.1.3 Compression, suppression d'en-tête et VAD

Si l'AN et CM sont configurés pour effectuer la compression ou la suppression d'en-tête, alors la bande passante qui est nécessaire pour un flux J.112 peut être réduite. Il est nécessaire pour le client d'informer l'AN que cette compression ou suppression peut être appliquée avant l'installation d'une réservation pour garantir que la bande passante appropriée est réservée. La solution générale de ce problème est décrite dans *Integrated Services in the Presence of Compressible Flows* (services intégrés en présence de flux compressibles) [draft-davie-intserv-compress-02].

Le MTA ajoute un paramètre (Compression_Hint) décrit dans [draft-davie-intserv-compress-02] au Sender-Tspec (Tspec de l'émetteur) qui identifie le ou les types de compression ou suppression d'en-tête qui pourraient être appliqués aux données. Le paramètre Compression_Hint contient un champ Hint qui donne des informations sur le ou les types de compression ou suppression possibles, et indique si l'expéditeur utilise ou non les totaux de contrôle IP et/ou IP-Ident; si ces derniers ne sont pas utilisés, ces champs peuvent également être comprimés ou supprimés. Si un champ dans l'en-tête IP n'est pas comprimé ou supprimé, alors le total de contrôle IP NE DOIT PAS être comprimé ou supprimé.

Pour signaler la suppression de l'en-tête au réseau J.112, l'AN utilise les données fournies par le champ Hint du paramètre Compression_Hint pour indiquer le schéma de la suppression d'en-tête qui sera effectué sur ce flux J.112. Ces informations sont utilisées pour réduire le débit et la profondeur

efficaces du "token bucket" fourni par le MTA. Si la suppression de l'en-tête n'est pas prise en charge sur une liaison, le paramètre Compression_Hint est ignoré et le Tspec complet est utilisé.

En effectuant la suppression d'en-tête sur une liaison J.112, il est également nécessaire de communiquer le contenu de l'en-tête qui sera supprimé à l'AN avant la transmission du premier paquet de données pour que le contexte de la suppression puisse être établi au niveau du CM et l'AN. Ces informations peuvent être délivrées par le message RSVP qui est utilisé pour établir la réservation ou par l'intermédiaire des messages de la couche MAC envoyés en avant du premier paquet de données. Etant donné que les messages PATH sont traités par des sauts intermédiaires entre le client et l'AN, un message PATH entrant contiendra la même valeur TTL que les paquets de données, sous réserve que les messages PATH et les paquets de données aient le même TTL initial lorsqu'ils sont envoyés par le MTA. L'AN peut ainsi utiliser le contenu du PATH pour apprendre les valeurs des champs qui seront supprimées. L'AN utilise les messages MAC J.112 pour porter à la connaissance du CM le fait que la suppression devrait être utilisée pour un flux particulier et lui indiquer de supprimer des champs appropriés étant donné la présence ou l'absence de totaux de contrôle UDP.

L'AN peut également indiquer au CM de supprimer le champ IP Identification. Ce champ est utilisé uniquement lorsque la fragmentation se produit. Etant donné que ce champ change avec chaque paquet, sa valeur ne peut pas être acheminée ni en utilisant les messages RSVP ni les messages MAC. La question de le supprimer ou non dépend de la possibilité ou non de fragmenter le paquet ultérieurement. Il n'est pas nécessaire pour le MTA d'acheminer des informations à l'AN sur la possibilité de supprimer ce champ; l'AN peut décider de le supprimer ou non en fonction d'une politique locale.

La même approche de base permet de prendre en charge la détection de l'activité vocale (VAD, *voice activity detection*). Un AN peut utiliser différents algorithmes de programmation pour les flux qui utilisent la VAD et a donc besoin de savoir quels flux peuvent être traités avec la VAD. L'objet de compressibilité transporté dans Tspec DOIT contenir une valeur qui indique que le flux de données pour lequel cette réservation est demandée peut être traité avec VAD (c'est-à-dire qu'il n'a pas subi de détection de silence au niveau du MTA et qu'il s'agit de voix et non de télécopie ou de données).

6.1.4 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 J.112 et de commuter l'allocation de ces ressources d'un demandeur à l'autre. Alors que cette capacité a été suggérée pour le protocole RSVP dans le passé, elle n'était pas incluse dans RSVP version 1.

Dans le protocole RSVP, le "traitement" sur un ensemble de ressources réservées est l'objet Session. Etant donné que la session contient l'adresse de destination du flux, la réallocation de ressources à un flux avec une adresse de destination différente nécessiterait un changement dans l'objet session. Le changement de l'adresse source du flux pourrait être accompli en utilisant un nouveau Filterspec dans le message RESV.

Pour prendre en charge cette fonctionnalité, un objet Resource-ID est ajouté aux messages RSVP. Les routeurs, qui comprennent cet objet, essaieront d'utiliser les ressources associées à cette ID. L'objet Resource-ID est un identificateur opaque généré par le nœud qui a le contrôle des ressources, c'est-à-dire l'AN dans ce cas.

Ce principe est illustré à la Figure 7. Lorsqu'un MTA envoie une demande de réservation pour un nouveau flux, il indique à l'AN que cette session souhaite partager les ressources pour cette nouvelle porte (porte 2) avec une porte précédemment créée (porte 1) en incluant l'identification ResourceID 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 J.112. Toutefois, il peut être nécessaire de réserver 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: un MTA doit envoyer un message Commit pour indiquer à l'AN quel flux est actuellement actif et ce message Commit supprime explicitement les ressources engagées pour l'autre session. Dans l'exemple de l'appel en instance, le client envoie un message Commit à l'AN pour identifier le flux actuellement actif lorsque l'utilisateur commute entre les sessions.

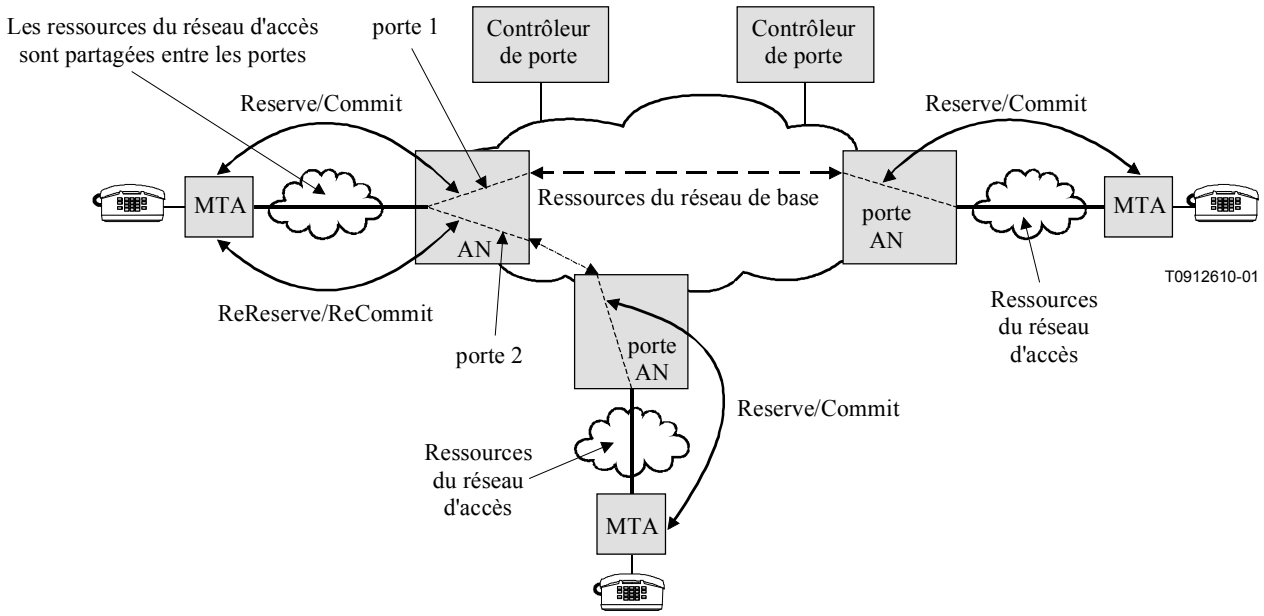


Figure 7/J.163 – Partage des réservations de ressources à travers les portes

Dans le modèle segmenté, l'AN inclut la Resource-ID dans le premier message RESV qu'il envoie au MTA. Le MTA peut inclure la Resource-ID dans les messages suivants qui s'appliquent aux ressources en question. De façon plus importante, si le MTA souhaite établir une nouvelle session et réutiliser les ressources d'une session existante, il inclut la Resource-ID associée à l'ancienne session dans le message PATH qu'il envoie à l'AN. Un message PATH qui contient la Resource-ID d'un ensemble de ressources actuellement allouées ajoute une nouvelle association entre un flux (tel qu'il est identifié dans les objets Session et Sender-Template) et ces ressources. Il peut, le cas échéant, changer la quantité de ressources allouées par l'inclusion de Tspec et Rspec qui diffèrent de ceux précédemment reçus par l'AN pour cet ensemble de ressources. Ceci peut inclure l'adjonction d'un nouvel ensemble de Tspec et Rspec pour prendre en charge les codecs multiples comme il est décrit au § 6.2.

Le protocole RSVP permet aux réservations de varier en taille dans le temps. Une réservation qui n'est pas supérieure à celle actuellement installée (c'est-à-dire, qui ne nécessite pas une augmentation du niveau de ressources dans une dimension pour l'un au l'autre sens de la session) NE DOIT PAS manquer le contrôle d'admission. La même règle s'applique pour l'utilisation de l'objet Resource-ID. Si la quantité de ressources demandées dans la nouvelle réservation n'est pas supérieure à celle précédemment installée, la réservation NE DOIT PAS manquer le contrôle d'admission.

Un routeur qui ne comprend pas ce nouvel objet (par exemple, dans le réseau privé) essaiera simplement d'installer ce qui apparaît comme une nouvelle réservation sans réutiliser des ressources précédemment allouées. Dans la mesure où il est peu probable qu'il y ait moins de bande passante dans le réseau de rattachement que sur le réseau J.112, ceci ne posera normalement pas de problème. L'ancienne réservation sera libérée sur temporisation si elle n'est pas rafraîchie. Dans le cas où la rareté des ressources poserait problème dans le réseau privé, il serait nécessaire d'améliorer les

routeurs dans le réseau de rattachement pour supporter ce nouvel objet. Il est à noter que le fait d'essayer d'installer des réservations sur le réseau privé est intéressant, même si bande passante est relativement abondante, dans la mesure où une réservation fournit des dispositifs dans le réseau privé avec les informations nécessaires pour isoler les flux spécifiques d'un délai et d'une gigue excessifs qu'ils subiraient s'ils étaient simplement mélangés au trafic "au mieux" (ou flux réservé de caractéristiques de trafic largement différentes) dans une file d'attente commune.

6.1.5 Processus Reserve/Commit en deux étapes

Un aspect significatif du modèle de QS dynamique IPCablecom tient au fait que cette réservation est un processus en deux phases, avec une phase Commit (engagement) qui suit la phase Reserve (réservation). Le protocole RSVP est utilisé pour couvrir la phase Reserve, ainsi l'AN ne fournit pas réellement les ressources avant la deuxième étape du processus.

Etant donné que la phase Commit implique uniquement un MTA et une porte locale, il s'agit d'un message à monodiffusion envoyé par le MTA à l'AN. Le MTA prend connaissance de l'ID de porte à partir du protocole de signalisation d'appel.

6.1.6 Authentification

Le fournisseur est en mesure d'assurer que les parties ne réservent pas de ressources réseau non autorisées. Le protocole RSVP fournit un certain nombre de mécanismes à cet effet, tels que des objets d'intégrité du RSVP et des données de politique contenues dans d'autres messages RSVP. La spécification de QS dynamique inclut une GateID comme donnée de politique qui DOIT être incluse dans les messages RSVP-PATH.

6.2 RSVP Flowspec

L'architecture de services intégrés 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 connue comme un Tspec, les exigences relatives aux ressources sont contenues dans Rspec et la combinaison de ces éléments est connue comme un Flowspec. Afin de réserver des ressources sur un support de couche 2 spécifique tel qu'un réseau J.112, il est nécessaire de définir un mappage entre le Flowspec indépendant 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 J.167 CODEC IPCablecom) 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. Les Annexes A et B spécifient comment l'AN et le MTA DOIVENT mapper les Flowspec avec les paramètres de la couche 2 J.112.

Les services intégrés (*Integrated Services*) définissent actuellement deux types de service, service à charge contrôlée (*controlled load*) et service garanti (*guaranteed*), le dernier service étant le plus adapté pour les applications sensibles au temps d'attente. Lorsqu'il effectue une réservation pour un service garanti, le Flowspec contient:

Tspec

profondeur du bucket (b) – octets
débit du bucket (r) – octets/s
débit pic (p) – octets/s
unité régulée min (m) – octets
taille maximale du datagramme (M) – octets

Rspec

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

Les termes de TSpec sont pour la plupart suffisamment explicites. (r,b) spécifie un "token bucket" auquel le trafic se conforme, p est le débit pic 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 minimale régulée avec une politique, 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 pour les besoins de la politique.

Pour comprendre le RSpec, il est utile de comprendre comment le délai est calculé 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 une conduite "idéale".

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

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 un commutateur d'un codec à une autre à mi-session sans avoir à passer le contrôle d'admission à chaque temps de commutation.

Dans des cas tels que celui-ci, le MTA DOIT générer plusieurs Tspec. Le deuxième et le dernier Tspec DOIVENT être marqués comme Component Tspec (voir § 6.3.6) et contiennent les paramètres Flowspec pour un codec individuel. Le premier Tspec DOIT être formé, pour chaque composante de la description du flux, en prenant l'utilisation de ressources maximales de l'un quelconque des Component Tspec suivants. Ceci est désigné comme étant la borne supérieure (LUB, *least-upper-bound*). Avec le LUB placé dans un RSVP Tspec standard, tout routeur non familier avec ces extensions allouera suffisamment de ressources (et probablement plus que nécessaire) pour transporter l'une des alternatives.

Le fait de prendre simplement la borne supérieure de deux flowspec provoque une certaine perte d'informations. Par exemple, supposons que codec A soit du type G.726-24 avec des paquets toutes les 20 ms, ce qui nécessite un Tspec de:

profondeur du bucket (b) = 100 octets
débit du bucket (r) = 5000 octets/s
débit pic (p) = 5000 octets/s
unité régulée min (m) = 100 octets
taille maximale du datagramme (M) = 100 octets

tandis que le codec B est G.726-40 avec des paquets toutes les 10 ms, ce qui nécessite un Tspec de:

profondeur du bucket (b) = 90 octets
débit du bucket (r) = 9000 octets/s
débit pic (p) = 9000 octets/s
unité régulée min (m) = 90 octets
taille maximale du datagramme (M) = 90 octets

L'examen initial de codec A, permet de conclure qu'il a besoin d'une allocation pour transporter des paquets IP de taille 100 octets toutes les 20 ms (M/r = 0,02 s), tandis que codec B nécessite une allocation pour délivrer des paquets de 90 octets toutes les 10 ms. Toutefois, la borne supérieure des deux Tspec est:

profondeur du bucket (b) = 100 octets
débit du bucket (r) = 9000 octets/s
débit pic (p) = 9000 octets/s
unité régulée min (m) = 100 octets
taille maximale du datagramme (M) = 100 octets

qui amène à accorder 100 octets toutes les 11,1 ms (M/r = 100/9), ce qui n'est pas approprié pour l'une ou l'autre session. Pour cette raison, lorsqu'on effectue une réservation qui aura besoin de couvrir deux flowspec différents ou plus, chaque composante flowspec DOIT être incluse dans les messages RSVP appropriés.

6.3 Définition d'objets RSVP supplémentaires

Plusieurs nouveaux objets RSVP DOIVENT être ajoutés au message PATH d'origine envoyé par le MTA. Tous les nouveaux objets ont un numéro de classe avec les deux bits les plus significatifs mis à 1, ce qui signifie qu'il est recommandé que les nœuds RSVP qui ne reconnaissent pas ces objets les envoient sans modification. Le présent paragraphe définit les formats des différents nouveaux objets qui doivent être transportés dans les messages RSVP. Tous les objets utilisent le schéma de codage TLV de RSVP IETF RFC 2205.

6.3.1 Reverse-Rspec

Objet Reverse-Rspec: Class = 226, C-type = 1.

130 (h)	0 (i)	2 (j)
Débit [R] (nombre à virgule flottante IEEE 32 bits)		
Slack term (terme de latitude) [S] (entier 32 bits)		

(h) – ID paramètre, paramètre 130 (Rspec service garanti).

(i) – Drapeaux du paramètre 130 (aucun réglé).

(j) – Longueur du paramètre 130, 2 mots en-tête de paramètre non compris.

Voir IETF RFC 2210 pour l'explication des champs.

Reverse-Rspec s'applique aux données envoyées par le MTA, c'est-à-dire en amont du réseau J.112. Il est inclus dans le message PATH envoyé par le MTA et est transformé en objet Forward-Rspec dans le message RESV généré par l'AN dans son rôle de mandataire pour le point d'extrémité distant.

6.3.2 Reverse-Session

Objet IPv4 Reverse Session: Class = 226, C-Type = 2.

Adresse de destination IPv4 (4 octets)		
ID de protocole	Drapeaux	Port de destination

L'objet Reverse-Session décrit les informations de destination des flux de données à recevoir par le MTA, c'est-à-dire en aval du réseau J.112. Il devient l'objet Session dans le Message PATH généré par l'AN dans son rôle de mandataire pour le point d'extrémité distant.

6.3.3 Reverse-Sender-Template

Objet IPv4 Reverse-Sender-Template: Class = 226, C-Type = 3.

Adresse source IPv4 (4 octets)		
Réservé	Réservé	Port source

L'objet Reverse-Sender-Template décrit les informations source du flux de données à recevoir par le MTA, c'est-à-dire en aval du réseau J.112. Il devient l'objet Sender-Template dans le message PATH généré par l'AN dans son rôle de mandataire pour le point d'extrémité distant.

6.3.4 Reverse-Sender-Tspec

Objet Reverse-Sender-Tspec: Class = 226, C-Type = 4. Mêmes champs que Sender-Tspec décrit dans les services intégrés en présence de flux compressibles [draft-davie-intserv-compress-02].

0 (a) Réservé		10 (b)
1 (c)	0 Réservé	9 (d)
127 (e)	0 (f)	5 (g)
Débit du token bucket [r] (nombre à virgule flottante IEEE 32 bits)		
Taille du token bucket [b] (nombre à virgule flottante IEEE 32 bits)		
Taux de transfert pic des données [p] (nombre à virgule flottante IEEE 32 bits)		
Unité minimale régulée avec une politique [m] (entier 32 bits)		
Taille maximale de paquet [M] (entier 32 bits)		
126(h)	Drapeaux (i)	2 (j)
Hint (nombre assigné) (k)		
Facteur de compression (entier 32 bits) (l)		

(a) – Numéro de version de format de message (0).

(b) – Longueur générale (10 mots en-tête non compris).

(c) – En-tête de service, nombre de service 1 (informations par défaut/globales).

(d) – Données de longueur de service 1, 9 mots en-tête non compris.

(e) – ID paramètre, paramètre 127 (Token_Bucket_Tspec).

(f) – Drapeaux du paramètre 127 (aucun réglé).

(g) – Longueur du paramètre 127, 5 mots en-tête non compris.

(h) – ID paramètre, paramètre 126 (Compression_Hint).

(i) – Drapeaux paramètre 126 (aucun réglé).

(j) – Longueur paramètre 126, 2 mots en-tête non compris.

(k) – Valeur suggérée définie pour la suppression de l'en-tête J.112 (à déterminer).

0x????0001 Ne pas supprimer le champ UDP checksum (total de contrôle UDP) ET ne pas supprimer le champ IP-Ident ni le champ IP-Checksum.

0x????0002 Ne pas supprimer le champ UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

0x????0003 Supprimer le champ UDP checksum ET ne pas supprimer IP-Ident ni le champ IP-Checksum.

0x????0004 Supprimer le champ UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

NOTE – ???? – Affectation du nombre à déterminer (to be determined) IANA pour IPCablecom

(l) – Valeur de facteur de compression – le pourcentage de réduction de la taille du paquet résultant de l'utilisation de la suppression de l'en-tête J.112. Il est à noter que cette valeur varie en fonction du CODEC utilisé. Voir IETF RFC 2210 pour l'explication des champs.

Reverse-Sender-Tspec décrit le flux de données à envoyer au MTA, c'est-à-dire en amont dans le réseau J.112. Il devient l'objet Sender-Tspec dans le message PATH généré par l'AN dans son rôle de mandataire pour le point d'extrémité distant.

6.3.5 Forward-Rspec

Objet Forward-Rspec, Class = 226, C-type = 5. Mêmes champs que Reverse-Rspec.

130 (h)	0 (i)	2 (j)
Rate [R] (débit [R] (nombre à virgule flottante IEEE 32 bits)		
Slack term (terme de latitude) [S] (entier 32 bits)		

Forward-Rspec s'applique à l'envoi de flux de données vers le MTA, c'est-à-dire en aval du réseau J.112. Cet objet apparaît dans un message PATH envoyé par le MTA et le contenu est incorporé dans l'objet Flowspec dans le message RESV renvoyé.

6.3.6 Component-Tspec

Objet Component-Tspec: Class = 226, C-type = 6. Mêmes champs que Sender-Tspec définis dans les services intégrés en présence de flux compressibles [draft-davie-intserv-compress-02].

0 (a) Réservé		10 (b)
1 (c)	0 Réservé	9 (d)
127 (e)	0 (f)	5 (g)
Débit du token bucket [r] (nombre à virgule flottante IEEE 32 bits)		
Taille du token bucket [b] (nombre à virgule flottante IEEE 32 bits)		
Taux de transfert pic des données (p) (nombre à virgule flottante IEEE 32 bits)		
Unité minimale régulée avec une politique [m] (entier 32 bits)		
Taille maximale de paquet [M] (entier 32 bits)		
126 (h)	Drapeaux (i)	2 (j)
Hint (nombre assigné) (k)		
Facteur de compression (entier 32 bits) (l)		

(a) – Numéro de version de format de message (0).

(b) – longueur générale (10 mots en-tête non compris).

(c) – En-tête de service, nombre de service 1 (informations par défaut/globales).

(d) – Données de longueur de service 1, 9 mots en-tête non compris.

(e) – ID paramètre, paramètre 127 (Token_Bucket_TSpec).

(f) – Drapeaux du paramètre 127 Drapeaux (aucun réglé).

(g) – Longueur du paramètre 127, 5 mots en-tête non compris.

(h) – ID paramètre, paramètre 126 (Compression_Hint).

(i) – Drapeaux du paramètre 126 (aucun réglé).

(j) – Longueur du paramètre 126, 2 mots en-tête non compris.

(k) – Valeur suggérée définie pour la suppression d'en-tête J.112 (à déterminer).

0x????0001 Ne pas supprimer le champ UDP checksum ET ne pas supprimer le champ IP-Ident ni le champ IP-Checksum.

0x????0002 Ne pas supprimer le champ UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

0x????0003 Supprimer le champ UDP checksum ET ne pas supprimer le champ IP-Ident ni le champ IP-Checksum.

0x????0004 Supprimer le champ UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

NOTE – ???? – affectation du nombre à déterminer IANA pour IPCablecom

(l) – Valeur de facteur de compression – le pourcentage de réduction de la taille du paquet résultant de l'utilisation de la suppression de l'en-tête J.112. Il est à noter que cette valeur varie en fonction du CODEC utilisé.

6.3.7 Resource-ID

Objet Resource-ID: Class = 226, C-type = 7.

Resource ID (entier 32 bits)

L'objet Resource-ID est renvoyé dans un message RESV au MTA et contient l'identifiant utilisé pour les futurs changements de ressources. Il est également inclus dans les messages PATH envoyés par le MTA dans les demandes de partager les ressources dans les sessions multiples.

6.3.8 Gate-ID

Objet Gate-ID: Class = 226, C-type = 8.

ID de porte (entier 32 bits)

L'objet Gate-ID est inclus dans les messages PATH en provenance du MTA pour identifier l'autorisation de ressource correcte au niveau de l'AN.

6.3.9 Commit-Entity

Objet Commit-Entity d'IPv4: Class = 226, C-type = 9.

Adresse de destination IPv4 (4 octets)	
Réservé	Port de destination

L'objet Commit-Entity est renvoyé dans un message RESV depuis l'AN et indique l'adresse de destination et le numéro de port auquel le MTA doit envoyer le message COMMIT.

6.3.10 DClass

Objet DClass: Class = 225, C-Type = 1

Inutilisé	Inutilisé	Inutilisé	DSCP

L'objet DClass est renvoyé dans un message RESV depuis l'AN et indique le DSCP qu'il CONVIENT que le MTA utilise lorsqu'il envoie des paquets de données sur cette réservation à l'AN. L'utilisation de l'objet DClass est décrite dans utilisation et format de l'objet DCLASS avec signalisation RSVP [draft-bernet-dclass-01].

6.4 Définition des messages RSVP

Le présent paragraphe définit les messages RSVP amélioré qui DOIVENT être générés par le MTA et DOIVENT être supportés par l'AN.

Messages RSVP DOIVENT être envoyés comme des datagrammes "bruts" avec le numéro de protocole 46. Le message RSVP-PATH DOIT être envoyé avec l'option RouterAlert IETF RFC 2113 dans l'en-tête IP. Chaque message RSVP DOIT occuper exactement un datagramme IP.

Tous les messages RSVP DOIVENT comporter un en-tête commun, suivi d'un nombre variable d'objets de longueur variable. L'en-tête commun DOIT être le suivant:

Version	Drapeaux	Type de Message	RSVP Total de contrôle
Sent-TTL		(Réservé)	RSVP Longueur de message

Les valeurs de chaque champ DOIVENT être telles que spécifiées dans IETF RFC 2205.

Chaque objet doit se composer d'un ou plusieurs mots de 32 bits avec un en-tête d'un mot du format suivant:

Longueur en octets	Numéro de classe	Type C
Contenu de l'objet ...		

Les valeurs de chaque champ DOIVENT être telles que spécifiées dans IETF RFC 2205.

Le format du message RSVP-PATH et du message RSVP-RESV conforme à la présente Recommandation DOIT contenir les objets suivants (les éléments en italique sont définis dans la présente Recommandation, tous les autres dans IETF RFC 2205 et/ou IETF RFC 2210). Pour les objets non définis dans la présente Recommandation, les règles d'ordonnancement d'objets DOIVENT être suivies conformément à IETF RFC 2205. Aucune exigence d'ordonnancement ne

s'applique pour les objets <Resource-ID>, <Gate-ID> et <Commit-Entity>. <Reverse-Rspec> et <Downstream-Flowspec> DOIVENT suivre l'objet <Sender-Tspec>. Si <Component-Item> est inclus dans le message, <Component-Item> DOIT apparaître dans le message PATH après le triplé <Sender-Tspec><Reverse-Rspec><Downstream-Flowspec>. Les objets définis dans <Downstream-Flowspec> et <Component-Item> DOIVENT suivre l'ordre indiqué dans leur BNF ci-dessous:

<PATH-Message> ::=Common-Header> [<Integrity-Object>]
<Session-Object> <RSVP-Hop> <Time-Values>
<Policy-Data> …] <Sender-Template>
Sender-Tspec> <*Reverse-Rspec*>
Downstream-Flowspec> [<*Resource-ID*>]
Gate-ID> [<*Component-Item*> …]

<*Downstream-Flowspec*> *::=* <*Reverse-Session*> <*Reverse-Sender-Template*>
<*Reverse-Sender-Tspec*><*Forward-Rspec*>

<*Component-Item*> *::=* <*Component-Tspec*> <*Reverse-Rspec*>
<*Downstream-Flowspec*>

<RESV-Message> ::= <Common-Header> [<Integrity-Object>]
<Session-Object> <RSVP-Hop> [<DClass>]
Time-Values> [<RESV-Confirm>] [<Scope>]
<Policy-Data> …] <*Resource-ID*>
Commit-Entity> <Style> <Flowspec>
Filter-Spec>

Les différentes composantes de ces messages sont décrites dans les paragraphes suivants.

6.4.1 Objets Message pour réservation amont

Un message RSVP-PATH standard contient au minimum les objets suivants:

<Session> <RSVP-Hop> <Time-Values> <Sender-Template> <Sender-Tspec>

Toutefois dans le modèle segmenté, il est nécessaire de fournir toutes les informations à l'AN qui lui permettrait d'effectuer une réservation bidirectionnelle sur la liaison J.112. Il est également nécessaire de lui permettre d'envoyer un RSVP-RESV au MTA. Un message RSVP-RESV standard contient au minimum les objets suivants:

<Session> <RSVP-Hop> <Time-Values> <Style> <Flowspec> <Filter-Spec>

L'AN DOIT envoyer un tel message au MTA après avoir reçu un message RSVP-PATH du MTA. Le seul objet ici qui ne puisse être dérivé du RSVP-PATH ou d'informations locales est le Flowspec. Le Filter-Spec, qui se compose de l'adresse IP et du port source à utiliser par le MTA, est dérivé du Sender-Template dans le PATH. La quasi-totalité de Flowspec peut être dérivée de Sender-Tspec dans le message PATH. Les exceptions à cette règle sont les valeurs de R (débit réservé) et S (terme de latitude) qui constituent ensemble Rspec. Ainsi, le MTA fournit un Rspec adapté, contenant R et S pour le service garanti qui est codé tel que spécifié dans IETF RFC 2210. Celui-ci est enfermé/inclus dans un objet Reverse-Rspec, qui est décrit au § 6.3.2.

6.4.2 Objets Message pour réservation aval

Le MTA DOIT fournir suffisamment d'informations pour permettre à l'AN de construire un message RSVP-PATH pour le flux de données aval qui vient de recevoir un message RSVP-PATH pour le flux de données amont. Ceci signifie que le MTA doit fournir les objets suivants qui se rapportent au flux de données aval (AN → MTA).

<Session> <Sender-Template> <Sender-Tspec>

Ces objets ont leurs définitions RSVP normales et s'appliquent au flux de données unidirectionnel qui sera acheminé depuis l'extrémité distante du MTA. Dans le message RSVP-PATH envoyé par le MTA, ils reçoivent de nouveaux codes d'objet (notés ci-dessous) et de nouveaux noms (Reverse-session, Reverse-sender-template, Reverse-Sender-Tspec). Le Reverse-Session-Object DOIT contenir l'adresse IP du MTA, le type de protocole et le port (le cas échéant) sur lequel il recevra les données pour ce flux. Reverse-Sender-Template DOIT contenir l'adresse IP de l'extrémité distante ou des zéros si la source est spécifiée comme un joker. Le Reverse-Sender-Template DOIT contenir le numéro du port, le cas échéant et s'il est connu, sinon zéro. Reverse-Sender-Tspec DOIT contenir les informations Tspec qui décrivent le flux de données depuis l'extrémité distante. L'AN DOIT utiliser sa propre adresse comme le RSVP-Hop et choisir une valeur pour Time-Values qui indique avec quelle fréquence il rafraîchira le message RSVP-PATH. Même si l'AN n'a pas besoin de générer le message RSVP-PATH pour l'envoyer au MTA, cette information est nécessaire pour lui permettre d'établir une réservation et créer des classificateurs de paquets dans le sens aval.

Etant donné les informations décrites ci-dessous, la seule information supplémentaire dont l'AN a besoin pour effectuer une réservation dans le sens aval est un Rspec. De nouveau, il reçoit un nouveau numéro et nom d'objet, Forward-Rspec. Il contient les mêmes éléments d'informations et est codé de la même façon qu'un Rspec conventionnel.

Il est à noter qu'un Forward-Rspec s'applique aux données qui sont acheminées vers le MTA, ce qui signifie qu'il est envoyé par le MTA dans le même sens que le RSVP-RESV qui transporterait normalement ces informations. Il est fourni dans le message RSVP-PATH simplement comme une optimalisation pour réduire l'attente d'établissement. Un Reverse-Rspec est envoyé par le MTA dans le sens opposé au RSVP-RESV qui transporterait normalement ces informations.

6.4.3 Objets Message pour la prise en charge de Flowspec multiples

Pour prendre en charge la situation d'un codec multiple décrite au § 6.2, un message PATH peut avoir besoin de transporter des Tspec et Rspec multiples. En même temps, des dispositifs compatibles avec le protocole RSVP entre le MTA et l'AN ont besoin de recevoir le Tspec et le Rspec de la borne supérieure. Ainsi, dans le cas où les ressources sont réservées avec l'objectif de prendre en charge des codecs multiples, il convient qu'un objet Tspec ou Rspec standard transporté dans un message RSVP contienne la borne supérieure des ressources requises. Des Tspec et Rspec supplémentaires peuvent être inclus dans le message PATH, en utilisant de nouveaux types d'objet qui seront ignorés par des dispositifs RSVP standards. Etant donné que tous les objets décrivant le Downstream-Flowspec (Flowspec aval) et le Reverse-Rspec (Rspec inverse) seront ignorés par le RSVP standard, le seul nouvel objet nécessaire est un objet Component-Tspec qui PEUT être transporté dans le message RSVP-PATH. Il peut exister deux objets ou plus de ce type dans un message RSVP-PATH, en plus du Tspec standard qui est requis pour transporter la borne supérieure de toutes les composantes et qui sera utilisé par des dispositifs dans le réseau privé. L'interprétation de chaque objet Component-Tspec est que les ressources réservées sur la liaison J.112 sont adaptées pour prendre en charge tout flux correspondant à l'un des Tspec.

De manière similaire, il PEUT exister des objets Reverse-Rspec, Reverse-Session, Reverse-Sender-Template, Reverse-Sender-Tspec et Forward-Rspec multiples. Etant donné qu'il est nécessaire de pouvoir identifier correctement quelle combinaison de paramètres avant et arrière a besoin d'être pris en charge à la fois, l'ordre de ces objets dans le message RSVP-PATH est important. L'ordre donné ci-dessus, au § 6.4, est requis.

6.5 Opération réservation

Le présent paragraphe décrit le comportement requis du MTA et de l'AN pour qu'ils effectuent en collaboration les réservations de ressources.

Pour les besoins de l'étude, l'extrémité qui est en communication directe avec l'AN est désignée comme le client et l'autre extrémité de la session est désignée comme l'extrémité distante. Aucune

hypothèse n'est formulée sur les types de dispositifs qui pourraient exister (passerelles, PC, clients intégrés). Il est supposé que le client utilise le protocole RSVP pour communiquer les demandes de QS à l'AN et aucune hypothèse n'est formulée sur les capacités de l'extrémité distante. Le flux de données du client à l'AN est désigné comme étant le flux amont et le flux de l'AN au client comme le flux aval.

6.5.1 Etablissement de réservations

L'exploitation du RSVP avec le modèle segmenté est le suivant:

le client DOIT envoyer un message RSVP-PATH à l'extrémité distante de la session, qui DOIT être intercepté par l'AN. Ceci initie le processus de réservation de la bande passante amont et aval. Le RSVP-PATH DOIT transporter des informations sur les exigences de ressources amont (c'est-à-dire Reverse-Rspec) et aval (c'est-à-dire Reverse-Sender-Tspec, Forward-Rspec) dans le cas où les réservations sont requises dans les deux directions.

L'AN DOIT vérifier que la quantité de ressources requise se trouve dans les limites de la quantité autorisée pour cette session et qu'il existe suffisamment de ressources locales pour prendre en charge la réservation. Il réserve ensuite les ressources amont et aval et DOIT effectuer l'échange de messages de niveau MAC J.112 pour allouer les ressources appropriées sur la liaison J.112.

L'AN DOIT établir des classificateurs pour les flux amont et aval. Le classificateur amont DOIT contenir l'adresse IP source du client et le numéro de port provenant de l'objet Sender Template. Le classificateur amont DOIT contenir le type de protocole, l'adresse IP de destination et le numéro de port de l'objet Session. Si l'objet Reverse-Sender-Template est présent et contient une adresse autre que 0.0.0.0, alors le classificateur aval DOIT contenir cette adresse comme adresse IP source. Si l'objet Reverse-Sender-Template est présent et contient un numéro de port autre que 0, alors le classificateur aval DOIT contenir cette valeur comme port source. Le classificateur aval DOIT contenir le type de protocole, l'adresse IP de destination et le numéro de port provenant de l'objet Reverse Session.

L'AN DOIT effectuer toute réservation de ressources nécessaire sur le réseau de base, en utilisant l'algorithme fourni défini pour la configuration particulière du réseau de base.

Si les réservations sur le réseau d'accès et le réseau de base réussissent, l'AN DOIT envoyer un RSVP-RESV au client. Le contenu du RSVP-RESV DOIT être dérivé du RSVP-PATH: Session-Object est copié du RSVP-PATH, le style est réglé à Fixed-Filter, Flowspec est formé à partir du Sender-Tspec et Forward-Rspec, Filter-Spec est réglé à partir du Sender-Template et Resource-ID est générée, contenant l'identification des ressources assignées aux ressources allouées. L'objet Commit-Entity DOIT être inclus et contenir l'adresse de l'AN et le numéro de port sur lequel l'AN acceptera le message Commit (tel que décrit au § 6.6). Il convient que l'objet DCLASS soit inclus et que la valeur soit réglée en se basant sur le champ Diffserv Code Point de la porte.

Si l'adresse du saut précédent diffère de l'adresse source (*Source Address*) du message RSVP-PATH, alors l'AN DOIT générer un RSVP-PATH pour les réservations amont. Le contenu du RSVP-PATH DOIT être dérivé du RSVP-PATH reçu du client. Session-Object DOIT être obtenu à partir de Reverse-Session-Object dans le message RSVP-PATH. Si l'adresse contenue dans le Reverse-Sender-Template est 0.0.0.0, ou le numéro de port est 0, alors le Sender-Tspec et le Sender-Template ne sont pas envoyés dans le RSVP-PATH. Sinon, le Sender-Tspec est obtenu de Reverse-Sender-Tspec, le Forward-Rspec est obtenu du Reverse-Rspec et le Sender-Template est obtenu du Reverse-Sender-Template. L'objet Resource-ID est généré et contient l'identification de ressources (*Resource-ID*) assignée aux ressources allouées. Le MTA PEUT utiliser le Reverse-Sender-Tspec qu'il a envoyé dans le message RSVP-PATH en calculant the Filter-Spec retourné dans sa réponse RSVP-RESV ou PEUT générer une réponse Wildcard-Filter (Caractère joker-Filtre). A la réception du message RSVP-RESV, le client sait que les ressources nécessaires ont été réservées. A ce moment, dans le cas d'une réservation réussie, le client sait qu'il a une réservation dans les deux sens et peut poursuivre la signalisation de l'appel en faisant sonner le téléphone à l'extrémité distante.

Si la réservation échoue, l'AN DOIT envoyer un message RSVP-PATH-ERR au client, en indiquant pourquoi la réservation a échoué (par exemple, absence d'autorisation, ressources insuffisantes, etc.). Si la réservation a échoué pour des raisons de politique, le message RSVP-PATH-ERR DOIT contenir un objet RSVP-ERREUR-SPEC avec les codes d'erreur (*Error Code*) et les valeurs d'erreur suivantes:

- Error Code = 2 (*Policy Control Failure*, échec de contrôle de politique), Error Value = 3 (*Generic Policy Rejection*, rejet de politique générique) est renvoyé si le RSVP-PATH ne contenait pas un objet Gate-ID ou si l'objet Gate-ID ne correspondait à aucune porte connue au niveau de l'AN.
- Error Code = 1 (*Admission Control Failure*, échec de contrôle d'admission), Error Value = 2 (bande passante demandée indisponible). Ce code est renvoyé si le RSVP-PATH a été rejeté parce qu'il n'y avait plus de ressources disponibles pour le niveau de priorité de la porte. Dans ce cas, le MTA PEUT entreprendre une action spéciale indiquant l'erreur spécifique à l'utilisateur. Si le RSVP-PATH a échoué pour des raisons autres que la politique, il DOIT contenir un objet RSVP-ERREUR-SPEC avec un code d'erreur et une valeur d'erreur, tel que défini à l'Annexe B de IETF RFC 2205.

L'émetteur d'un RSVP-PATH (MTA ou AN) est responsable de l'installation fiable de la réservation. Lorsque l'émetteur transmet un RSVP-PATH, il DOIT recevoir un message RSVP-RESV ou RSVP-PATH-ERR dans les limites de l'intervalle de temporisation configuré du temporisateur T3 (voir Annexe C).

Chaque fois qu'un MTA ou un AN transmet un message RSVP qui nécessite un accusé de réception, l'émetteur DOIT inclure un objet RSVP-MESSAGE-ID dans ce message et le drapeau ACK_Desired de l'objet RSVP-MESSAGE-ID DOIT être réglé. Le MTA et l'AN DOIVENT régler le drapeau Refresh-Reduction-Capable dans l'en-tête commun de chaque message RSVP. Lorsque le MTA ou l'AN reçoit un message RSVP avec un objet RSVP-MESSAGE-ID, il DOIT répondre avec un message RSVP qui contient un objet RSVP-MESSAGE-ACK ou RSVP-MESSAGE-NACK. L'objet RSVP-MESSAGE-(N)ACK PEUT être superposé sur les messages standards RSVP, mais il PEUT être transmis dans un message RSVP-ACK si le destinataire de l'objet RSVP-MESSAGE-ID n'a pas d'autre message RSVP à envoyer à ce moment. Par exemple, il convient que l'AN ne retarde pas le traitement d'un message RSVP-PATH reçu, mais s'il choisit de retarder ce traitement, il DOIT répondre immédiatement avec un message RSVP-ACK, qui sera suivi ultérieurement pas un message RSVP-RESV.

Les messages RSVP-ACK transportent un ou plusieurs objets RSVP-MESSAGE-(N)ACK. Ils ne DOIVENT PAS contenir d'autres objets RSVP sauf un objet optionnel RSVP-INTEGRITY. Lorsqu'il est inclus, un objet RSVP-MESSAGE-(N)ACK DOIT être le premier objet du message, à moins qu'un objet RSVP-INTEGRITY soit présent (auquel cas, l'objet RSVP-MESSAGE-(N)ACK DOIT immédiatement suivre l'objet RSVP-INTEGRITY). Le MTA ou l'AN PEUT utiliser les objets RSVP-INTEGRITY.

Les objets RSVP-MESSAGE-ID et RSVP-MESSAGE-(N)ACK peuvent être utilisés pour assurer une remise fiable des messages RSVP en cas de perte du réseau. Etant donné que le MTA ou l'AN règle le drapeau ACK_Desired, il DOIT retransmettre les messages qui n'ont pas fait l'objet d'un accusé de réception à un intervalle plus rapide que l'intervalle de rafraîchissement standard de RSVP jusqu'à ce que le message ait fait l'objet d'un accusé de réception ou jusqu'à ce qu'un intervalle de temps du temporisateur T3 (voir Annexe C) expire. Un débit rapide de retransmission basé sur des fonctions d'attente exponentielles bien connues DOIT être utilisé. Une temporisation de retransmission initiale du temporisateur T6 (voir Annexe C) DOIT être utilisée, avec une attente puissance 2. Le processus de retransmission rapide se termine lorsqu'un objet RSVP-MESSAGE-(N)ACK est reçu ou un temporisateur T3 expire. Si l'expéditeur RSVP-PATH ne reçoit pas un RSVP-RESV, RSVP-PATH-ERROR, ou RSVP-MESSAGE-(N)ACK avant la retransmission suivante, il DOIT considérer que son RSVP-PATH original ou la réponse de l'autre

extrémité a été perdue et renvoie le RSVP-PATH. Etant donné que tous les messages RSVP sont idempotents, aucune duplication des réservations ne se produira.

Dans IPCablecom, seul les messages RSVP-PATH DOIVENT inclure des objets RSVP-MESSAGE-ID avec le drapeau ACK_Desired réglé. Les objets RSVP-MESSAGE-ID PEUVENT être utilisés dans d'autres messages RSVP.

Les RSVP-MESSAGE-ID sont utilisés sur une base saut par saut RSVP. Chaque saut compatible avec le protocole dans le trajet qui prend en charge la réduction du rafraîchissement effectue sa propre retransmission rapide jusqu'à ce qu'il voit un accusé de réception provenant du nœud amont suivant. Aussi, si un MTA autonome derrière un CM compatible avec le protocole RSVP reçoit un objet RSVP-MESSAGE-ACK du CM pour un RSVP-PATH et que le CM attend un RSVP-MESSAGE-ACK depuis l'AN pour le RSVP-PATH, le CM effectuera la retransmission rapide tandis que le MTA autonome attend que son temporisateur de rafraîchissement normal de RSVP-PATH expire (30 s). (Le MTA n'effectue plus une retransmission rapide parce qu'il a eu un accusé de réception.) Si un CM compatible avec le protocole RSVP abandonne sa retransmission rapide, il renverra un RSVP-PATH-ERROR au MTA autonome. De cette manière, les retransmissions n'affectent pas le chemin complet, juste les sauts faisant l'objet d'une perte.

La remise de messages fiable pour les messages RSVP est définie dans RSVP Refresh Overhead Reduction Extensions [Draft-ietf-rsvp-refresh-reduct-02].

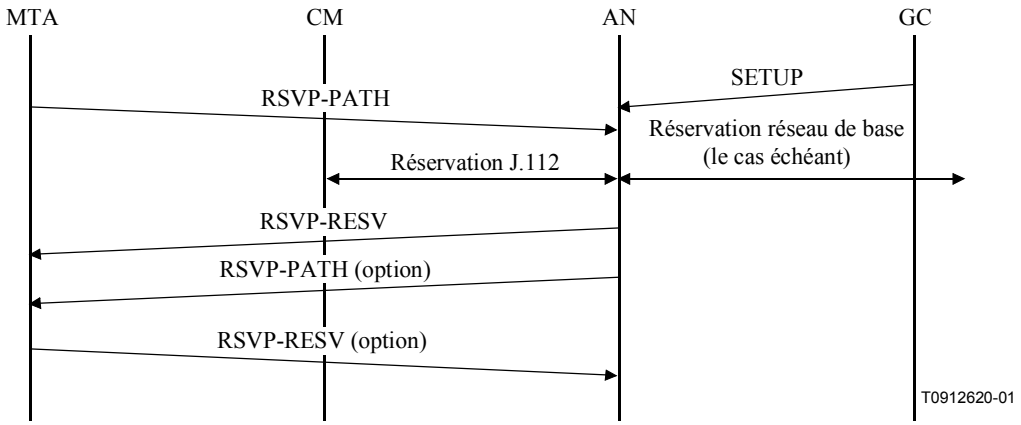


Figure 8/J.163 – Etablissement d'une réservation

L'AN DOIT appliquer les filtres de classification de paquets amont pour les flux J.112. C'est-à-dire que l'AN DOIT éliminer les paquets amont, qui ne correspondent pas à l'ensemble des classificateurs de paquets amont pour le flux J.112. Le filtrage de classification des paquets amont est une exigence optionnelle de l'AN dans les réseaux J.112. La présente Recommandation nécessite son implémentation pour les flux J.112 utilisés pour transporter les flux de média IPCablecom. Si un AN choisit d'appliquer des filtres de classification amont uniquement sur les flux J.112 et non sur les autres flux, la décision relative au mode de détermination des flux J.112 particuliers est une décision spécifique au vendeur.

6.5.2 Changement de réservation

En plus d'établir une réservation pour une certaine quantité de ressources, il peut être nécessaire de changer les ressources allouées. L'utilisation des ressources peut avoir besoin d'être augmentée ou diminuée. Le protocole RSVP gère les changements dans l'utilisation des ressources par des changements dans l'objet FLOWSPEC d'un message RSVP-RESV et/ou un changement dans le Sender-Tspec dans un message RSVP-PATH. Un changement de réservation DOIT suivre les mêmes séries d'étapes que l'établissement d'une nouvelle réservation. Il convient que le contrôle

d'admission réussisse toujours pour une session, qui change ses exigences de ressources d'une façon qui ne provoque pas d'augmentation de toute dimension relative aux ressources précédemment réservées. Etant donné que les ressources sont décrites par vecteurs multidimensionnels, un changement de réservation qui a augmenté les ressources dans un sens et les a fait baisser dans l'autre DOIT passer par le contrôle d'admission. Il est à noter qu'afin de réussir le contrôle d'admission, les ressources DOIVENT être situées dans les limites des ressources autorisées pour la session et également dans les limites de la quantité de ressources dont l'AN dispose.

Si une réservation existante est éliminée parce qu'une session avec une porte de priorité plus élevée doit être établie en présence d'une bande passante insuffisante, alors l'AN DOIT envoyer un message RSVP-PATH-ERR et/ou un message PATH-RESV-ERR pour la session qui est éliminée. Il convient que ce message soit envoyé dès que possible. En réponse, il convient que le MTA mette fin à une réservation et puisse notifier à l'utilisateur l'élimination (par exemple faire entendre une tonalité spéciale à l'utilisateur du téléphone). Le message RSVP-PATH-ERR (ou RSVP-RESV-ERR) dans ce cas DOIT contenir un objet RSVP-ERREUR-SPEC avec un code d'erreur de 2 (*Policy Control Failure*, échec de contrôle de la politique) et une valeur d'erreur de 5 (le flux a été éliminé).

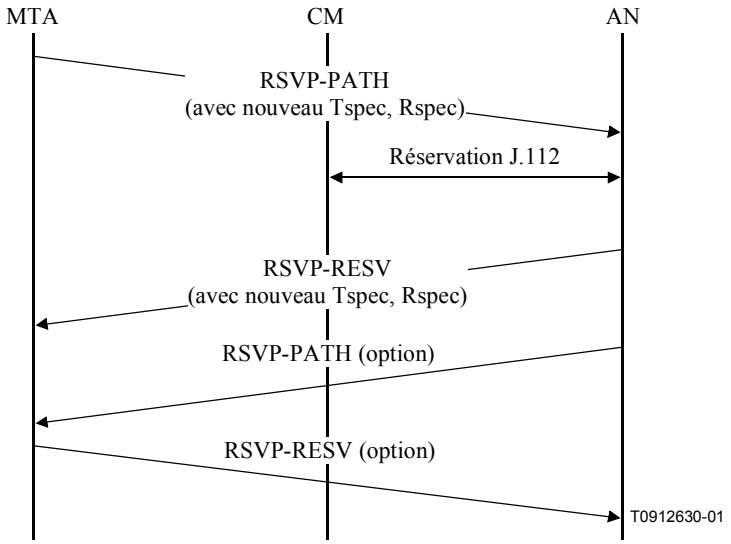


Figure 9/J.163 – Changement de réservation

6.5.3 Suppression d'une réservation

Le protocole RSVP fournit deux messages pour la suppression explicite de l'état de Path et de Reservation, les messages RSVP-PATH-TEAR et RSVP-RESV-TEAR. Pour supprimer une réservation au niveau de l'AN, il convient que le MTA envoie un message RSVP-PATH-TEAR. Pour supprimer une réservation provenant de dispositifs compatibles avec le protocole RSVP entre le MTA et l'AN, le MTA PEUT envoyer un message RSVP-RESV-TEAR. Le format de ces messages DOIT être conforme avec IETF RFC 2205 et DOIT inclure le Session-Object et le Sender-Template pour permettre à l'AN d'identifier la porte correcte.

Si l'état de Path et l'état de Reservation ne sont pas rafraîchis périodiquement, ils DOIVENT expirer. Ceci s'applique, par exemple, en cas de blocage du MTA. Le § 6.5.4 fournit des détails supplémentaires sur les mécanismes de rafraîchissement.

L'AN DOIT répondre à un RSVP-PATH-TEAR reçu en envoyant un RSVP-RESV-TEAR au MTA. Le format de ces messages DOIT être tel que donné dans IETF RFC 2205.

RSVP version 1 ne fournit aucun moyen d'assurer la remise fiable des messages RSVP-PATH-TEAR et RSVP-RESV-TEAR, dans la mesure où l'état qu'ils visent à supprimer finira de toute façon par expirer. Toutefois, pour éviter tout retard dans la terminaison (qui provoque un gaspillage des ressources à court terme et peut provoquer une surfacturation), l'extension de fiabilité du message au RSVP décrit dans [Draft-ietf-mpls-lsp-tunnel-00] peut être utilisée.

6.5.4 Mise à jour de la réservation

RSVP possède un modèle à état souple, en ce que l'état de réservation est libéré sur temporisation si elle n'est pas périodiquement rafraîchie. Cette caractéristique est conservée dans le modèle segmenté décrit ici. Etant donné que le processus entier de réservation dans ce modèle est initié par le MTA, le MTA DOIT périodiquement rafraîchir toutes les informations d'état RSVP. Le MTA DOIT envoyer des messages RSVP-PATH, tel que décrit au § 6.5.1 dans les limites de l'intervalle de temps donné par l'AN dans l'objet de valeurs de temps RSVP-RESV. L'AN DOIT générer des messages RSVP-RESV à destination du MTA à la réception du RSVP-PATH (et un message RSVP-PATH également si des nœuds compatibles avec le protocole RSVP ont été détectés, tel que décrit au § 6.5.1). Ceci préserve la nature d'état souple du RSVP, qui garde sa souplesse face à des changements de routage et des défaillances de nœud.

Le MTA (ou l'AN) PEUT également implémenter le rafraîchissement sommaire RSVP (RSVP *Summary Refresh*) comme un autre moyen de conserver la bande passante amont lorsqu'il rafraîchit l'état de la réservation. Ceci permet aux nœuds compatibles avec le protocole RSVP de "comprimer" leurs états Path (ou Resv) pour des réservations multiples dans un seul message. *RSVP Refresh Overhead Reduction Extensions* (Extensions de la réduction du préfixe du rafraîchissement RSVP) [Draft-ietf-rsvp-refresh-reduct-02] décrit le rafraîchissement sommaire comme suit:

"L'extension de rafraîchissement sommaire permet le rafraîchissement de l'état RSVP sans la transmission de messages Path ou Resv. L'avantage de l'extension décrite est une réduction de la quantité d'informations qui doivent être transmises et traitées afin de maintenir la synchronisation d'état RSVP. L'extension décrite préserve vraiment la capacité du RSVP à gérer les sauts suivants autres que RSVP et à ajuster les changements dans le routage. Cette extension ne peut pas être utilisée avec des messages Path ou Resv qui contiennent tout changement provenant de messages précédemment transmis, c'est-à-dire qui sont des messages de déclenchement.

L'extension de rafraîchissement sommaire se fonde sur l'extension MESSAGE_ID précédemment définie. Seul l'état qui était précédemment annoncé dans les messages Path et Resv contenant des objets MESSAGE_ID peut être rafraîchi via l'extension de rafraîchissement sommaire.

L'extension de rafraîchissement sommaire utilise les objets et le message ACK précédemment défini comme partie de l'extension le MESSAGE_ID et un nouveau message Srefresh. Le nouveau message transporte une liste de champs Message _identifier correspondant aux messages de déclenchement Path et Resv qui ont établi l'état. Les champs Message _identifier sont transportés dans un des trois objets associés Srefresh. Les trois objets sont l'objet MESSAGE_ID LIST, l'objet MESSAGE_ID SRC_LIST et l'objet MESSAGE_ID MCAST_LIST.

L'objet MESSAGE_ID LIST est utilisé pour rafraîchir l'état Resv et l'état Path de sessions à monodiffusion. Il est constitué d'une liste de champs Message_Identifier qui ont été à l'origine annoncés dans les objets MESSAGE_ID. Les deux autres objets sont utilisés pour rafraîchir l'état Path de sessions à multidiffusion. Un nœud recevant un rafraîchissement sommaire pour un état de chemin multidiffusion nécessitera par moment des informations sur la source et le groupe. Ces deux objets fournissent ces informations. Ces objets diffèrent dans les informations qu'ils contiennent et sur leur mode d'envoi. Ils transportent tous les deux les champs Message_Identifier et les adresses IP source correspondantes. Le MESSAGE_ID SRC_LIST est envoyé dans les messages adressés à l'adresse IP multidiffusion de la session. L'objet MESSAGE_ID MCAST_LIST ajoute l'adresse de groupe et est envoyé dans les messages adressés au saut suivant du RSVP.

Le MESSAGE_ID MCAST_LIST est normalement utilisé sur les liaisons point à point.

Un nœud RSVP recevant un message Srefresh, fait correspondre chaque champ Message_Identifier listé avec l'état Path ou Resv installé. Tout état correspondant est mis à jour comme si un message de rafraîchissement RSVP normal a été reçu. Si un état correspondant ne peut pas être trouvé, alors l'émetteur du message Srefresh est notifié via un refresh NACK.

Un refresh NACK est envoyé via un objet MESSAGE_ID_NACK. Telles que décrites au paragraphe précédent, les règles d'envoi d'un objet MESSAGE_ID_NACK sont les mêmes que pour envoyer un objet MESSAGE_ID_ACK. Ceci inclut l'envoi d'un objet MESSAGE_ID_NACK superposé dans des messages distincts RSVP ou dans des messages RSVP ACK."

Pour des détails complets sur le fonctionnement du rafraîchissement sommaire, se reporter à l'article 5 de RSVP Refresh Overhead Reduction Extensions [Draft-ietf-rsvp-refresh-reduct-02].

6.6 Définition des messages Commit

Le présent paragraphe définit les messages Commit qui DOIVENT être générés par le MTA et DOIVENT être pris en charge par l'AN.

Les messages Commit DOIVENT être envoyés comme datagrammes UDP/IP avec le numéro de protocole 17 (UDP). Chaque message Commit DOIT occuper exactement un datagramme UDP/IP. L'adresse IP de destination et le numéro de port de l'en-tête UDP DOIVENT être tels que spécifiés à partir de l'objet Commit-Entity renvoyé dans le message RSVP-RESV. Le numéro de port source DOIT être le port sur lequel le MTA acceptera le message d'accusé de réception.

Les messages Commit DOIVENT se composer d'un en-tête commun, suivi par un nombre variable d'objets de longueur variable. L'en-tête commun DOIT être le suivant:

Version	Drapeaux	Type de Message	Total de contrôle du message
Sent-TTL		(Réservé)	Longueur de message

Les valeurs de chaque champ DOIVENT être telles que spécifiées dans IETF RFC 2205. Les types de messages DOIVENT être les suivants:

COMMIT	240
COMMIT-ACK	241
COMMIT-ERR	242

Chaque objet DOIT se composer de un ou plusieurs mots de 32 bits, avec un en-tête de un mot au format suivant:

Longueur en octets	Class-Number (numéro de classe)	C-Type (type-C)
Contenu de l'objet …		

Les valeurs de chaque champ DOIVENT être telles que spécifiées dans IETF RFC 2205.

Le format du message COMMIT et du message COMMIT-ACK conforme à la présente Recommandation DOIT être le suivant (les éléments en italiques sont définis dans la présente Recommandation au § 6.3, tous les autres dans IETF RFC 2205 et/ou IETF RFC 2210):

<COMMIT-Message> ::= <Common-Header> <Session>
Sender-Template> <*Gate-ID*>
<Flowspec>] [<*Downstream_Flowspec*>]
<COMMIT-ACK-Message> ::= <Common-Header> <Session>
Sender-Template><*Gate-ID*>
<COMMIT-ERR-Message> ::= <Common-Header> <Session>
<Sender-Template><*Gate-ID*><Error-Spec>

Les objets Session et Sender-Template identifient l'émetteur. Les adresses IP et les ports de destination DOIVENT être présents. Les ressources engagées PEUVENT être inférieures aux ressources réservées (notamment dans un scénario de mise en instance d'appel ou de changement de codec), de sorte qu'un message Commit PEUT également contenir un objet <Flowspec> pour chaque sens de la session. Ceci fournit un mécanisme par lequel la taille des ressources engagées peut être modifiée vers le haut ou vers le bas tant que la quantité de ressources engagées ne dépasse pas les ressources réservées. Il est à noter qu'un ensemble de ressources PEUT être mis en attente (gelé) en abaissant les ressources engagées à zéro tout en laissant les ressources réservées en place. Si l'un ou l'autre flowspec est omis, l'AN DOIT régler la quantité de ressources engagées dans ce sens pour qu'elles soient égales à la quantité de ressources réservées.

6.7 Opérations Commit

Un aspect significatif du modèle de la QS dynamique tient au fait que la réservation est un processus en deux phases, avec une phase Commit qui suit la phase Reserve. Le § 6.5 ci-dessus décrit la phase Reserve, alors que le présent paragraphe décrit la phase Commit et sa relation avec la phase Reserve.

Un AN compatible DOIT exécuter toutes les fonctions de contrôle d'admission et d'allocation de ressources à la réception du message RSVP-PATH d'origine, mais NE DOIT PAS permettre d'accéder à ces ressources par le MTA tant qu'un message COMMIT n'a pas été reçu, sauf indications contraires dans les paramètres GATE-SET.

Pour effectuer une opération COMMIT le MTA DOIT envoyer un message à monodiffusion à l'AN. Ce message est souhaitable car la phase Commit implique uniquement un MTA et une porte. Le MTA apprend l'adresse et le numéro de port de l'AN de l'objet Commit-Entity dans le message RSVP-RESV.

Il est à noter qu'un message COMMIT diffère de façon importante d'un message RSVP standard. Il est envoyé directement du MTA à l'AN plutôt que saut par saut, comme le ferait un message RSVP. Toutefois, il contient des objets qui sont syntactiquement les mêmes que les objets RSVP.

L'AN DOIT vérifier la valeur de Gate-ID et vérifier que le contenu des objets Session et Sender-Template correspondent à la réservation précédente avec la même valeur de Gate-ID et que Reverse-Session et Reverse-Sender-Template, s'ils sont présents, correspondent à la réservation précédente avec la même valeur de Gate-ID. L'AN DOIT accuser réception d'un message COMMIT avec un message COMMIT-ACK ou un message COMMIT-ERR.

Lorsqu'un MTA ne reçoit pas l'accusé de réception dans un intervalle de temporisation du temporisateur T4 (voir Annexe C), le MTA DOIT renvoyer le COMMIT, jusqu'à 7 tentatives.

Si le MTA désire changer la quantité de ressources engagées dans les limites de l'enveloppe réservée, une autre séquence COMMIT/COMMIT-ACK est requise.

Si le MTA désire changer la quantité de ressources réservées, alors l'échange RSVP-PATH/RSVP-RESV DOIT être répété.

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

Le présent paragraphe décrit les interfaces entre l'AN et le contrôleur de porte pour les besoins d'autoriser le MTA à recevoir une qualité de service élevée. La signalisation est requise entre le contrôleur de porte et l'AN 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 l'AN indique l'utilisation des ressources effectivement "engagées" sur une base session par session. Le présente paragraphe décrit l'utilisation du protocole COPS pour transporter des messages définis de QS IPCablecom entre le contrôleur de porte et l'AN.

7.1 Portes: le cadre pour le contrôle de la QS

Une "porte" (*Gate*) de la QS dynamique IPCablecom est une entité de contrôle de la politique implémentée au niveau de l'AN pour contrôler l'accès à des services de QS améliorés d'un réseau J.112 par un seul flux IP. Les portes sont unidirectionnelles, en ce qu'une seule porte contrôle l'accès à un flux dans le sens amont ou aval. Les portes permettent la création de classificateur de flux classificateur J.112, qui à leur tout contrôle l'acheminement de paquets aux flux J.112.

Alors qu'une porte a également un tuple-N tout comme un classificateur, elle n'est pas identique à un classificateur. L'AN 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 classificateur J.112 PEUT être établi et associé à une porte. Une porte PEUT exister avant et après que le classificateur qu'elle autorise existe. Une porte PEUT être considérée associée à exactement zéro, un ou deux classificateurs.

Un AN conforme à la présente Recommandation NE DOIT PAS créer dynamiquement de classificateur avec un échange de messages MAC J.112 à moins d'y avoir été autorisé par l'existence d'une porte pour ce classificateur. Un identificateur, appelé GateID (identificateur de porte) est associé aux portes. L'identification de porte, administrée localement par l'AN où la porte existe, PEUT être associée à une ou plusieurs portes unidirectionnelles. Pour une session point à point, généralement deux portes unidirectionnelles existent, associées à une seule GateID. De plus, des classificateurs J.112 existent pour chaque flux unidirectionnel qui est établi.

7.1.1 Classificateur

Un classificateur est un tuple de 6 données:

- sens (amont/aval);
- protocole;
- IP source;
- IP de destination;
- port de destination;
- port source.

S'il existe un flux amont et un flux aval associé (partie de la même session), il DOIT alors exister des classificateurs séparés pour le flux amont et le flux aval. Le classificateur est mis à jour par le message RSVP pour la réservation effectuée pour les flux amont et aval. Le flux de session de données DOIT correspondre au classificateur pour recevoir la qualité de service associée à la réservation RSVP. Des réservations futures peuvent changer le classificateur.

7.1.2 Porte

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

- ID de porte (Gate-ID);
- classificateur prototype;

- différents bits indicateurs décrits ci-dessous;
- enveloppe autorisée (Flow Spec);
- enveloppe réservée (Flow Spec);
- Resource-ID.

L'ID de porte (décrite ci-dessous) est un identificateur de 32 bits qui est alloué à partir de l'espace local au niveau de l'AN où la porte réside. Jusqu'à deux portes PEUVENT partager la même ID de porte. Généralement, une ID de porte identifiera un seul flux amont et un seul flux aval et correspondra à une seule session multimédia. [Ceci n'empêche toutefois pas la possibilité d'implémentations bidirectionnelles.]

Le classificateur prototype se compose des six mêmes éléments qu'un classificateur, comme la description ci-dessus. L'IP Source est l'adresse IP (telle qu'elle est vue au niveau de l'AN) de l'émetteur du flux. Dans le cas d'une porte amont sur le canal J.112, la source IP est l'adresse IP du MTA. Pour le flux aval, l'adresse de la source IP est l'adresse IP du MTA distant. Pour les paramètres sélectionnés d'un classificateur prototype de porte, un caractère joker est permis. Dans la signalisation d'appel multimédia, le port UDP source n'est pas signalé, de sorte que sa valeur n'est pas considérée comme faisant partie des informations d'une porte.

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

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

Le drapeau Auto-Commit, lorsqu'il est réglé, provoque l'engagement immédiat des ressources sur réservation. Pour une application en téléphonie, ce drapeau sera généralement utilisé pour la porte aval au niveau de l'émetteur d'un appel lorsque la destination est une passerelle RTPC. Lorsque le MTA de départ réserve les ressources, le flux aval est activé de sorte que le signal de retour d'appel, les tonalités de progression d'appel et les annonces peuvent être entendues par le demandeur. Voir § 7.1.4 pour une description complémentaire.

Le drapeau Commit-Not-Allowed, lorsqu'il est réglé, amène l'AN à ignorer tout message COMMIT pour cette porte. Cette fonction peut être utilisée par un contrôleur de porte lorsque l'adresse de l'extrémité distante n'est pas encore connue et par conséquent spécifiée comme caractère joker dans le classificateur prototype. Dans une telle application, le contrôleur de porte met généralement à jour le classificateur prototype de la porte avant que le MTA envoie le message COMMIT. L'utilisation de ce drapeau évite les scénarios de vol de service.

L'enveloppe autorisée (*Authorized Envelope*) et l'enveloppe réservée (*Reserved Envelope*) sont des Flow Spec de RSVP (T-Spec et R-Spec), tels que décrits dans les paragraphes précédents.

Une demande de réservation pour les ressources (telle que spécifiée dans le message PATH ou message MAC J.112 équivalent) DOIT être vérifiée par rapport à ce qui a été autorisé pour l'ID de porte associée au sens pour la demande de ressources. Les ressources autorisées sont spécifiées dans l'enveloppe autorisée. Le caractère joker est également vérifié dans la porte pour les entrées particulières.

L'identification de ressources (Resource-ID) est un identificateur local de 32 bits qui est alloué au niveau de l'AN où la porte réside. N'importe quel nombre de portes PEUT partager une identification de ressource et partager par conséquent un ensemble de ressources communes, à la restriction près que seule une de ces portes dans chaque sens a des ressources engagées.

7.1.3 Identification de porte

Une identification de porte (GateID) est un identificateur unique qui est localement alloué par l'AN où la porte réside. L'ID de porte est un identificateur de 32 bits. Une ID de porte PEUT être associée à une ou plusieurs portes. Dans les protocoles d'appel de signalisation J.162 et DCS, une Gate-ID est associée à chaque tronçon de l'appel et se compose d'une porte amont et d'une seule porte aval.

Une ID de porte DOIT être associée 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 une porte aval seule [il s'agira généralement d'une implémentation bidirectionnelle];
- information de coordination de porte;
- adresse: port de l'AN distant (ou autre entité) avec lequel coordonner l'allocation de ressources pour cet ensemble de portes;
- ID de porte assignée au niveau de l'AN distant (ou autre entité) pour l'ensemble de portes distant;
- clé de sécurité pour la communication avec l'AN distant (ou autre entité);
- drapeau No-Gate-Coordination qui, lorsqu'il est réglé, amène l'AN à sauter la coordination des portes, c'est-à-dire ne pas nécessiter la réception d'un message Gate-Open de l'AN distant (ou autre entité);
- drapeau No-Gate-Open, qui lorsqu'il est réglé, amène l'AN à ne pas envoyer un message Gate-Open à l'AN distant (ou autre entité);
- informations sur la comptabilité et la facturation;
- adresse: port du serveur d'archivage primaire qui devrait recevoir les enregistrements d'événement;
- adresse: port du serveur d'archivage secondaire, à utiliser si le primaire est indisponible;
- drapeau 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;
- ID Corrélation-Facturation, qui sera transmise au serveur d'archivage avec chaque enregistrement d'événement QoS-Start/QoS-Stop;
- informations de facturation supplémentaires, si elles sont fournies, qui seront utilisées pour générer des messages d'événement Call-Answer et Call-Disconnect.

L'ID de porte DOIT être unique parmi toutes les portes courantes allouées par l'AN. Il convient que la valeur de la quantité de 32 bits ne soit pas choisie dans un ensemble de petits entiers, étant donné que la possession de la valeur GateID est un élément clé de l'authentification des messages COMMIT en provenance du MTA. Un algorithme qui PEUT être utilisé pour assigner des valeurs d'identifications 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.

Le drapeau No-Gate-Open et le drapeau No-Gate-Coordination, s'associent pour offrir au contrôleur de porte la souplesse nécessaire pour les connexions à des systèmes autres que AN, à des AN non conformes ou à des systèmes autres que des systèmes IPCablecom. L'agent d'appel NCS fournira généralement sa propre adresse comme adresse d'AN distant et réglera le drapeau No-Gate-Open. A la fin de l'appel, l'agent d'appel générera un message Gate-Open et l'enverra à l'AN; ceci démarre le temporisateur T2 (voir § 7.1.4) et force le MTA à engager les ressources. A la fin de l'appel, en raison d'erreurs diverses (lorsque le MTA n'est pas en mesure d'indiquer cet événement), l'agent

d'appel reçoit la notification de raccrochage via le message Gate-Close. L'utilisation du drapeau No-Gate-Open réduit la charge de traitement sur l'agent d'appel de la NCS sans perte de fonctionnalité.

Le drapeau No-Gate-Coordination est généralement utilisé lorsque l'extrémité distante n'est pas un système compatible IPCablecom et n'est pas capable d'effectuer les procédures de coordination de portes. Ce drapeau, lorsqu'il est associé au drapeau No-Gate-Open, fait fonctionner la porte indépendamment de l'autre extrémité. Voir § 7.1.4 pour plus de détails sur l'effet de ces deux bits indicateurs sur le schéma de transition des états.

7.1.4 Schéma de transition des portes

Les portes sont considérées comme ayant les états suivants:

- Allocated (alloué) – l'état initial de la porte créée à la demande du GC;
- Authorized (autorisé) – le GC a autorisé le flux avec des limites de ressources définies;
- Reserved (réservé) – les ressources ont été réservées pour le flux;
- Committed (engagé) – les ressources sont utilisées;
- Remote-Committed (engagé-distant) et Local-Committed (engagé-local) – états transitoires qui existent lorsqu'une porte exécute le protocole de coordination de portes avec la porte distante.

L'AN DOIT prendre en charge les états et les transitions de porte comme indiqué et décrit dans le présent paragraphe. Toutes les portes assignées à la même ID de porte par l'AN DOIVENT transiter ensemble par les états indiqués à la Figure 10, schéma de transition d'états de porte.

Une porte est créée dans l'AN par une commande Gate-Alloc ou par une commande Gate-Set en provenance du GC. Dans les deux cas, l'AN alloue un identificateur localement uniquement appelé Gate-ID (ID de porte), qui est renvoyé au GC. Si la porte a été créée par un message Gate-Set, alors l'AN DOIT marquer la porte à l'état "Authorized" et DOIT démarrer le temporisateur T1. Si la porte a été créée par un message Gate-Alloc, alors l'AN DOIT marquer la porte à l'état "Allocated", démarrer le temporisateur T0 et DOIT attendre une commande Gate-Set, à ce moment la porte DOIT être marquée à l'état "Authorized". Si le temporisateur T0 expire avec la porte à l'état "Allocated" ou si le temporisateur T1 expire avec la porte à l'état "Authorized" alors l'AN DOIT 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 pendant lequel l'autorisation restera valide.

Une porte dans l'état "Authorized" attend que le MTA tente de réserver des ressources. Le MTA effectue cette opération avec un message RSVP-PATH ou via l'interface de la couche MAC. A la réception de cette demande de réservation, l'AN DOIT vérifier que la demande se trouve dans les limites établies pour la porte et effectue les procédures de contrôle d'admission.

L'AN 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 à renseigner qui spécifient, au minimum:

1) une quantité de ressources maximale qui peuvent être allouées 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 à des 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 les procédures de contrôle admission aboutissent avec succès, la porte DOIT être marquée à l'état "Reserved". Sinon, la porte reste dans l'état "Authorized". Il est à noter que la réservation effective par le MTA peut être pour moins qu'autorisée, par exemple réservation pour l'amont uniquement lorsqu'une paire de portes a été établie en autorisant les flux amont et aval. Si la porte individuelle a été marquée avec le drapeau "Auto-Commit" flag, alors les ressources réservées sont immédiatement engagées, mais l'état de la porte est inchangée.

Dans l'état "Reserved" la porte attend que le MTA engage les ressources. La commande Commit en provenance du MTA est un message UDP à monodiffusion ou une demande équivalente via l'interface de la couche MAC. La commande Commit est normalement synchronisée avec la porte distante, via le message de coordination de portes; à moins que les deux clients aux extrémités envoient les commandes Commit presque simultanément, l'autorisation sera retirée. Si la porte est encore à l'état "Reserved" et que le temporisateur T1 expire (c'est-à-dire que le MTA n'émet pas la commande Commit), l'AN DOIT libérer toutes les ressources réservées et supprimer la porte. Si le drapeau Commit-Not-Allowed est réglé lorsque la commande Commit est reçue, l'AN DOIT répondre avec un Commit-Err et NE DOIT PAS changer l'état de la porte.

Si, dans l'état "Reserved", l'AN reçoit une commande Commit en provenance du MTA et que le drapeau No-Gate-Coordination est réglé, alors l'AN DOIT marquer la porte à l'état "Committed" et arrêter le temporisateur T1. A moins que le drapeau No-Gate-Open soit réglé, l'AN DOIT envoyer un message Gate-Open à l'entité de coordination de portes.

Si, dans l'état "Reserved", l'AN reçoit une commande Commit en provenance du MTA et que le drapeau No-Gate-Coordination n'est pas réglé, alors l'AN DOIT marquer la porte à l'état "Local-Committed" et démarrer le temporisateur T2. A moins que le drapeau No-Gate-Open soit réglé, l'AN DOIT envoyer un message Gate-Open à l'entité de coordination de portes. Le temporisateur T2 limite le temps pendant lequel une porte peut avoir des ressources engagées à une extrémité et non à l'autre.

Dans l'état "Local-Committed" la porte a engagé les ressources locales mais attend que le client de l'extrémité distante engage les ressources à cette extrémité. Si le temporisateur T1 ou T2 expire dans cet état, l'AN DOIT désactiver toutes les ressources engagées avec cette porte, libérer toutes les ressources réservées avec cette porte, envoyer un message Gate-Close (uniquement si la porte a été ouverte) avec l'entité de coordination de portes et supprimer la porte.

Si, dans l'état "Local Committed", l'AN reçoit un message Gate-Open de l'entité de coordination de portes, l'AN DOIT arrêter les temporisateurs T1 et T2 et DOIT marquer la porte à l'état "Committed".

Si, dans l'état "Reserved", l'AN reçoit un message Gate-Open de l'entité de coordination de portes, l'AN DOIT marquer la porte dans l'état "Remote-Committed" et démarrer le temporisateur T2.

Dans l'état "Remote-Committed" la porte a été notifiée que le MTA de l'extrémité distante a activé les ressources, mais non le MTA local. Si le temporisateur T1 ou T2 expire dans cet état, l'AN DOIT libérer toutes les ressources réservées avec cette porte, envoyer un message Gate-Close avec l'entité de coordination de portes et supprimer la porte. Si le drapeau Commit-Not-Allowed est réglé lorsque la commande Commit est reçue, l'AN DOIT répondre avec Commit-Err et NE DOIT PAS changer l'état de la porte.

Si, dans l'état "Remote-Committed", l'AN reçoit une commande Commit en provenance du MTA, alors l'AN DOIT arrêter les temporisateurs T1 et T2 et DOIT marquer la porte à l'état "Committed". A moins que le drapeau No-Gate-Open soit réglé, l'AN DOIT envoyer un message Gate-Open à l'entité de coordination de portes.

Une fois dans l'état "Committed", la porte a atteint une configuration stable et n'a pas de temporisateurs en suspens ni d'actions de temporisation à effectuer. Les ressources ont été engagées à cette porte et à la porte correspondante au niveau de l'entité distante. Les ressources continueront à

être engagées jusqu'à ce que le MTA local envoie une commande Release ou que la porte distante signale son intention de terminer les ressources.

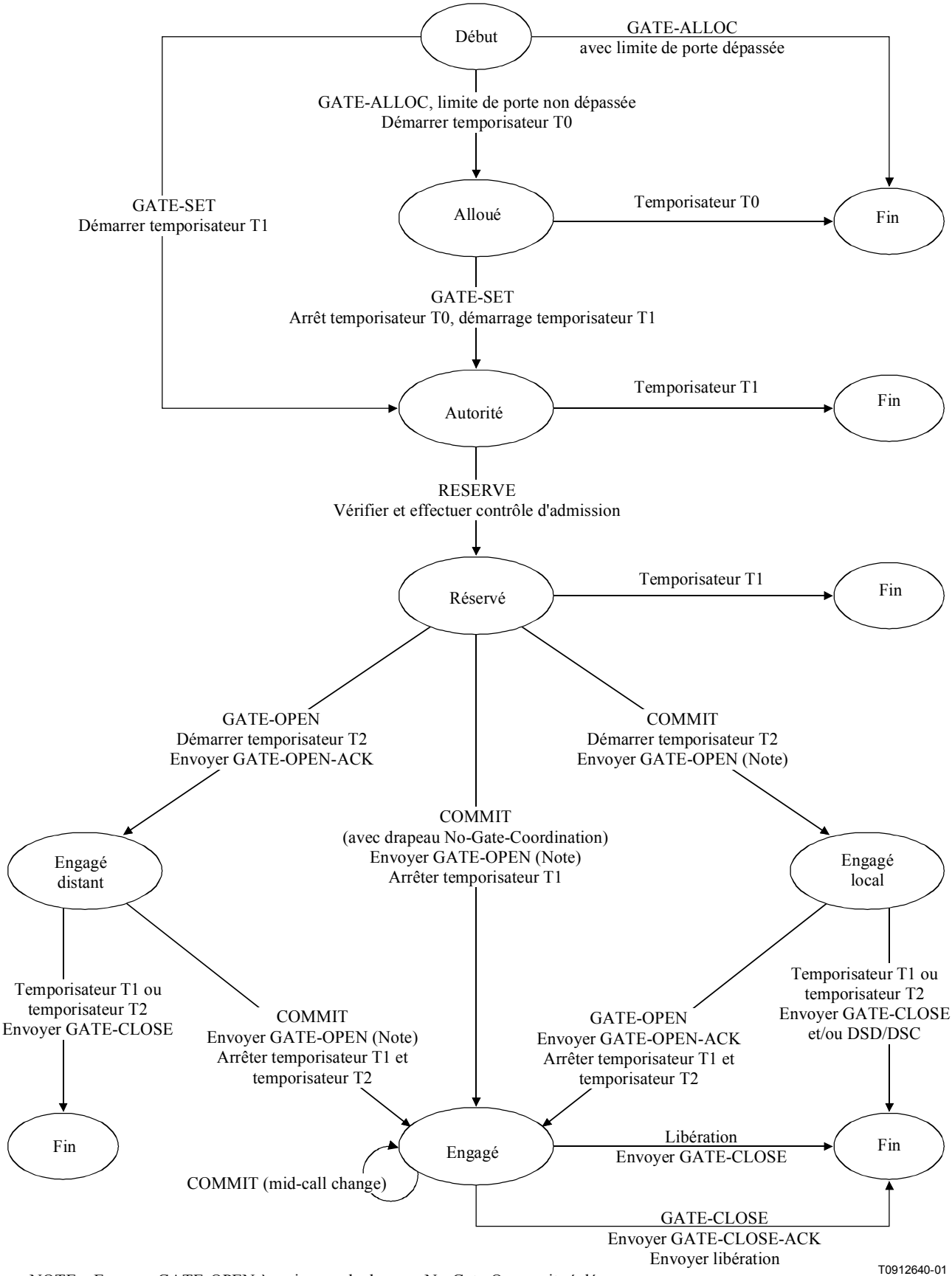
Si, à l'état "Committed", l'AN reçoit un message Gate-Close de l'entité de coordination de portes, l'AN DOIT désactiver toutes les ressources engagées pour le MTA local, libérer toutes les ressources réservées et supprimer la porte.

Si, dans l'état "Committed", l'AN reçoit une commande Release en provenance du MTA, soit sous la forme d'un message RSVP-PATH-TEAR, soit via l'interface de couche MAC, ou d'une défaillance du client à rafraîchir une réservation, ou encore de mécanismes J.112 internes qui détectent une défaillance du client, l'AN DOIT désactiver toutes les ressources engagées pour le MTA, libérer toutes les ressources réservées, envoyer un message Gate-Close à l'entité de coordination de portes et supprimer la porte.

Pendant qu'il est dans l'état "Committed", l'AN DOIT permettre au MTA d'initier des changements dans la réservation ou l'engagement de ressources, dans les limites du contrôle d'autorisation et d'admission locale.

7.1.5 Coordination de portes

En plus de contrôler la fonction de classification locale de flux J.112 classification, les portes DOIVENT communiquer avec leurs contreparties distantes pour le même flux afin de confirmer que l'extrémité distante s'est également engagée pour la facturation pour la session. Ceci est nécessaire pour éviter plusieurs scénarios de vol de service, tel que décrit à l'Appendice IX. Le protocole pour cette communication est donnée au § 8.



NOTE – Envoyer GATE-OPEN à moins que le drapeau No-Gate-Open soit réglé.

Figure 10/J.163 – Schéma de transition d'états de porte

7.2 Profil COPS pour IPCablecom

Le contrôle d'admission de QS IPCablecom est l'acte de gérer l'allocation de ressources QS à partir des politiques administratives et des ressources disponibles. Le service de contrôle d'admission de la QS IPCablecom utilise une architecture client/serveur. Les modules opérationnels de haut niveau sont décrits à la Figure 11. 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 pousse la politique chez le client, de sorte que le client peut prendre les décisions de contrôle d'admission.

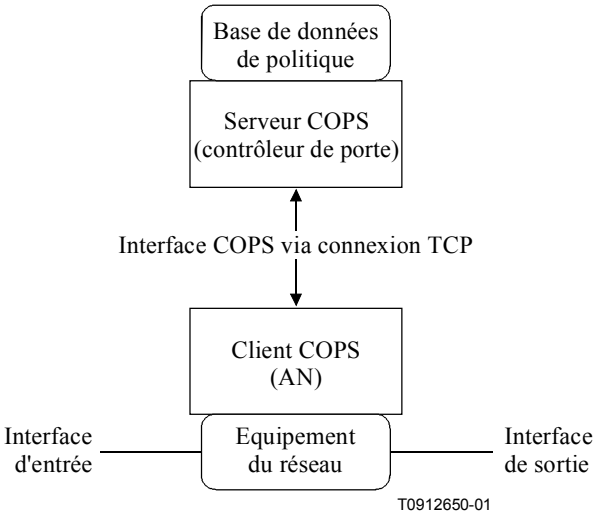


Figure 11/J.163 – Disposition du contrôle d'admission de la QS

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 basant 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 poussées chez le client COPS en se basant sur une demande de service de QS externe, hors bande, par exemple, une demande en provenance de l'AN d'arrivée 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 l'AN peut accéder à ces décisions d'informations pour prendre des décisions de contrôle d'admission sur des demandes de session entrantes reçues au niveau de l'AN.

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-Open (OPN)/Client-Accept(CAT)/Client-Close(CC): le client COPS envoie un message OPN pour initier 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;
- Request (REQ): 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 au client que le

serveur utilise, avec les données dans la base de données de politique d'admission de la session, pour prendre des décisions basées sur la politique;

- Decision (DEC): le serveur répond aux REQ en renvoyant un message DEC au client qui a initié 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 ensuite pour changer/mettre à jour une décision précédente (c'est-à-dire un DEC non demandé);
- Report State (RPT): le client COPS envoie un message RPT message 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 actuelles réservées après que le serveur COPS a accordé l'admission. Le client COPS peut également utiliser un rapport pour informer périodiquement le serveur COPS de l'état courant du client COPS;
- Delete Request State (DEL): 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;
- Keep Alive (KA): envoyé par le client COPS et le serveur COPS pour la détection des défauts de communication;
- Synchronize State Request (SSR)/Synchronize State Complete (SSC): SSR est envoyé par le serveur COPS en demandant des informations d'état du client COPS courant. 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 l'AN ou le GC.

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

Les détails du protocole COPS sont fournis dans le projet IETF RAP-COPS-07. Ce RFC d'IETF fournit une description du protocole COPS de base, indépendant du type de client. Des projets supplémentaires fournissent des informations pour utiliser le protocole COPS pour les services intégrés avec le protocole RSVP et pour les services différentiés (c'est-à-dire approvisionner 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 pour le 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 l'AN et le contrôleur de porte et utilisera les mécanismes spécifiés dans les normes en cours de développement pour protéger la voie de communication.

7.3.1 Format du message commun COPS

Chaque message COPS se compose de l'en-tête COPS suivi par un certain nombre d'objets typés. Le GC et l'AN DOIVENT prendre en charge l'échange de messages COPS tel que défini ci-dessous.

<table>
<tr><td colspan="2">0</td><td>1</td><td>2</td><td>3</td></tr>
<tr><td>Version</td><td>Flags (drapeau)</td><td>Op-Code</td><td colspan="2">Client-type</td></tr>
<tr><td colspan="5">Longueur de message</td></tr>
</table>

Figure 12/J.163 – En-tête de message COPS commun

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

Flags (drapeaux) est un champ de 4 bits. 0x1 est le drapeau de 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 drapeau DOIT être réglé à 1. Dans les autres cas (par exemple une décision non sollicitée) le drapeau NE DOIT PAS être réglé (valeur = 0). Tous les autres drapeaux DOIVENT être réglés à 0.

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

1 = Request (REQ)

2 = Decision (DEC)

3 = Report-State (RPT)

6 = Client-Open (OPN)

7 = Client-Accept (CAT)

9 = Keep-Alive (KA)

Client type est un identificateur de 16 bits. Pour l'utilisation d'IPCablecom, Client type DOIT être réglé à client IPCablecom (0x8005). pour les messages Keep-Alive (Op-code = 9), Client-type DOIT être réglé à zéro, comme le KA est utilisé pour la vérification de la connexion plutôt qu'une vérification de session par client.

Message length (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 Figure 13):

0	1	2	3
Length (longueur)		C-Num	C-type
(Contenu de l'objet)			

Figure 13/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 selon la limite de 32 bits suivante. 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 IETF RAP-COPS-07) utilisés dans la présente Recommandation et leurs valeurs de C-Num, sont les suivants:

1 = Handle (Identificateur)

6 = Decision (Décision)

8 = Error (Erreur)

9 = Client Specific Information (Informations 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 Decision, C-Num = 6, C-Type = 4 (Données de décision spécifique au client) lorsqu'ils sont transportés du GC à l'AN dans un message de décision. Ils DOIVENT également être placés dans un objet ClientSI, C-Num = 9, C-Type = 1 (Signalled Client SI) lorsqu'ils sont transportés de l'AN au GC dans un message Report. Ils sont codés de manière similaire aux objets spécifiques au 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 au 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 Transaction-ID

L'objet Transaction-ID contient un jeton qui est utilisé par le GC pour faire correspondre les réponses en provenance de l'AN 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
Transaction Identifier (identificateur de la transaction)	Gate Command Type (type de commande de porte)	

Transaction ID a une longueur de 16 bits qui PEUT être utilisée par le GC pour faire correspondre les réponses aux commandes.

Gate Command Type DOIT être l'un des suivants:

GATE-ALLOC	1
GATE-ALLOC-ACK	2
GATE-ALLOC-ERR	3
GATE-SET	4
GATE-SET-ACK	5
GATE-SET-ERR	6
GATE-INFO	7
GATE-INFO-ACK	8
GATE-INFO-ERR	9
GATE-DELETE	10
GATE-DELETE-ACK	11
GATE-DELETE-ERR	12

7.3.2.2 Subscriber-ID

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

Longueur = 8	S-Num = 2	S-Type = 1
Adresse IP v4 (32 bits)		

ou:

Longueur = 20	S-Num = 2	S-Type = 2
Adresse IP v6 (128 bits)		

7.3.2.3 Gate-ID

Cet objet identifie la porte ou un ensemble de portes référencées dans le message de commande ou assignées par l'AN pour un message de réponse.

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

7.3.2.4 Activity-Count

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 indiquée. Cet objet renvoie, dans un message GATE-SET-ACK ou GATE-ALLOC-ACK, le nombre de portes assignées à un seul abonné. Il est utile pour empêcher les attaques de refus de service.

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

7.3.2.5 Gate-spec

Longueur = 60 ou 88 ou 116, etc.		S-Num = 5	S-Type = 1
Direction	Protocol ID	Drapeaux, définis ci-dessous	Session Class
Source IP Address (32 bits)			
Destination IP Address (32 bits)			
Source Port (16 bits)		Destination Port (16 bits)	
DS Field	Réservé	Réservé	Réservé
Valeur de Timer T1 (temporisateur T1)			
Valeur de Timer T2 (temporisateur T2)			
Débit du token bucket [r] (nombre à virgule flottante IEEE 32 bits)			
Taille du token bucket [b] (nombre à virgule flottante IEEE 32 bits)			
Taux de transfert pic des données (p) (nombre à virgule flottante IEEE 32 bits)			
Unité minimale régulée avec une politique [m] (entier 32 bits)			

Flow spec alt #1

Taille maximale de paquet [M] (entier 32 bits)	
Débit [R] (nombre à virgule flottante IEEE 32 bits)	
Terme de latitude (Slack Term) [S] (entier 32 bits)	
Réglages supplémentaires des valeurs de r, b, p, m, M, R et S, selon les besoins pour décrire l'autorisation	Flow spec alt #2, etc.

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

Protocol-ID est la valeur à faire correspondre dans l'en-tête IP ou zéro en cas d'absence de correspondance.

Les drapeaux sont définis comme suit:

0x01 Auto-Commit, s'il est réglé, provoque l'engagement des ressources immédiatement au moment de leur réservation.

0x02 Commit-Not-Allowed, s'il est réglé, amène l'AN à ignorer tous les messages COMMIT pour cette porte.

Le reste est réservé et DOIT être nul.

Session class 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.

Source IP Address et Destination IP Address constituent une paire d'adresses IPv4 de 32 bits ou zéro pour l'absence de correspondance (c'est-à-dire, la spécification d'un caractère joker qui correspondra à toute demande en provenance du MTA).

Source Port et Destination Port constituent un couple de valeurs de 16 bits, ou zéro en cas d'absence de correspondance.

Les valeurs de r, b, p, m, M, R et S, sont décrites au § 6.2. Le Gate-Spec PEUT contenir des plusieurs ensembles de ces valeurs pour spécifier des autorisations complexes (tel que décrit au § 6.2).

Le champ DS est défini par la structure suivante:

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

Pour la compatibilité amont avec les implémentations de systèmes courants et l'utilisation de IP Precedence tel que défini dans IETF RFC 2474 et IETF RFC 791, les bits appropriés de l'octet IPv4 TOS représentés ci-dessous PEUVENT être insérés dans le champ DS. 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
IP Precedence			IPv4 IP TOS				Non utilisé

Timer T1 et Timer T2 sont des valeurs en millisecondes et sont utilisées dans le schéma de transition de portes décrit au § 8.1.4. Si plusieurs objets Gate-Spec apparaissent dans un seul message COPS, les valeurs de T1 et T2 DOIVENT être identiques dans toutes les occurrences Gate-Spec.

7.3.2.6 Remote-Gate-Info

Length	S-Num = 6	S-Type = 1
AN IP Address (32 bits)		
AN Port (16 bits)	Drapeaux, définis ci-dessous	
Remote Gate-ID		
Algorithm (algorithme)	Security Key (Clé de sécurité)	

AN-IP-Address est l'adresse de l'AN distant avec laquelle la coordination des portes est effectuée.

AN-Port est le numéro de port pour les messages envoyés pour la coordination des portes. Si le numéro de port n'est pas disponible pour le contrôleur de porte, il est réglé à zéro. Une valeur de zéro amène l'AN à ignorer ce champ.

Les drapeaux sont définis comme suit:

0x0001 No-Gate-Coordination, s'il est réglé, saute la coordination des portes. L'AN ne nécessitera pas la réception d'un Gate-Open de l'entité distante.

0x0002 No-Gate-Open, s'il est réglé, amène l'AN à sauter l'envoi du message Gate-Open lorsque un Commit est traité.

Le reste est réservé et DOIT être nul.

Remote-Gate-ID est l'ID de porte assignée par l'AN distant pour la porte ou l'ensemble de portes.

L'algorithme est un champ de 1 octet qui peut être couramment réglé selon les valeurs décimales suivantes:

100 = MAC basé MD5, tel que spécifié par Radius dans IETF RFC 2865.

Des choix supplémentaires pour un algorithme d'authentification peuvent être ajoutés dans des versions futures de la présente Recommandation.

Security key (clé de sécurité) est une clé de longueur variable utilisée pour le contrôle d'authentification dans les messages de coordination de portes. La longueur de la clé est 17 [octets] de moins que la longueur de l'objet.

7.3.2.7 Event-Generation-Info

Cet objet contient toutes les informations nécessaires pour prendre en charge les messages d'événement QoS-Start et QoS-Stop tel que spécifié et requis dans UIT-T J.164.

Longueur = 36	S-Num = 7	S-Type = 1
Primary-Record-Keeping-Server-IP-Address (adresse IP du serveur d'archivage primaire) (32 bits)		
Primary-Record-Keeping-Server-Port (port du serveur d'archivage primaire)	Drapeaux, voir ci-dessous	Réservé
Secondary-Record-Keeping-Server-IP-Address (adresse IP du serveur d'archivage secondaire) (32 bits)		
Secondary-Record-Keeping-Server-Port (port du serveur d'archivage secondaire)	Réservé	
Billing-Correlation-ID (ID corrélation facturation) (16 octets)		

Primary-Record-Keeping-Server-IP-Address est l'adresse du serveur d'archivage auquel les enregistrements d'événements doivent être envoyés.

Primary-Record-Keeping-Server-Port est le numéro de port pour les enregistrements d'événements envoyés.

Les valeurs de drapeaux sont les suivantes:

0x01 Indicateur de traitement par lot. S'il est réglé, l'AN DOIT accumuler les enregistrements d'événements comme une partie du fichier de commande par lots et envoyer au serveur d'archivage à intervalles périodiques. S'il n'est pas réglé, l'AN DOIT envoyer les enregistrements d'événement au serveur d'archivage en temps réel.

Le reste est réservé et DOIT être nul.

Secondary-Record-Keeping-Server-IP-Address est l'adresse du serveur d'archivage secondaire auquel les enregistrements sont envoyés si le serveur d'archivage primaire est indisponible.

Secondary-Record-Keeping-Server-Port est le numéro de port pour les enregistrements d'événement envoyés.

Billing-Correlation-ID est l'identificateur assigné par le CMS pour tous les enregistrements associés à cette session.

7.3.2.8 Media-Connection-Event-Info

Cet objet contient toutes les informations nécessaires pour prendre en charge les messages d'événement Call-Answer et Call-Disconnect. Si cet objet est présent dans la commande GATE-SET, alors l'AN DOIT générer les messages d'événement Call-Answer et Call-Disconnect.

Longueur = 84	S-Num = 8	S-Type = 1
Called-Party-Number (numéro de l'appelé)		
		Réservé
Routing-Number (numéro de routage)		
		Réservé
Charged-Number (numéro facturé)		
		Réservé
Location-Routing-Number (numéro de routage d'emplacement)		
		Réservé

7.3.2.9 IPCablecom-Error

Objet d'erreur spécifique au client défini comme suit:

Longueur = 8	S-Num = 9	S-Type = 1
Error-code (code d'erreur)	Error Sub-code (sous-code d'erreur)	

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

1 = No gates currently available (pas de portes actuellement disponibles).

2 = Illegal Gate-ID (ID de porte illégale).

3 = Illegal Session Class value (valeur de classe de session illégale).

4 = Subscriber exceeded gate limit (limite de porte dépassée par l'abonné).

127 = Other, unspecified error (autre, erreur non spécifiée).

Le sous-code d'erreur est réservé pour une usage ultérieur.

7.3.2.10 Electronic-Surveillance-Parameters

Longueur = 20	S-Num = 10	S-Type = 1
DF-IP-Address-for-CDC (32 bits)		
DF-Port-for-CDC (16 bits)	Drapeaux, définis ci-dessous	
DF-IP-Address-for-CCC (32 bits)		
DF-Port-for-CCC (16 bits)	Réservé	

DF-IP-Address-for-CDC est l'adresse de la fonction Electronic Surveillance Delivery (fourniture de la surveillance électronique) à laquelle les messages d'événement doublés doivent être envoyés.

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

Les drapeaux sont définis comme suit:

0x0001 DUP-EVENT. S'il est réglé, l'AN DOIT envoyer une copie en double de tous les messages d'événement associés à cette porte (par exemple QoS-Start, QoS-Stop et vraisemblablement Call-Answer et Call-Disconnect) à l'adresse DF-IP-Address-for-CDC.

0x0002 DUP-CONTENT. S'il est réglé, l'AN DOIT envoyer une copie en double de tous les paquets correspondant au(x) classificateur(s) pour cette porte à l'adresse DF-IP-Address-for-CCC.

Le reste est réservé et DOIT être nul.

DF-IP-Address-for-CCC est l'adresse de la fonction Electronic Surveillance Delivery à laquelle les messages d'événement doublés doivent être envoyés.

DF-Port-for-CCC est le numéro de port pour le contenu de l'appel doublé.

7.3.2.11 Session-Description-Parameters

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

SDP-strings est la description de la session (SDP, *session description*) du flux de paquets amont, suivie par un octet NUL, suivie par la description de la session (SDP) du flux de paquets aval. Un bourrage suffisant d'octets NUL est ajouté pour faire de la longueur totale un multiple de quatre octets.

Si cet objet est présent dans le message Gate-Set, alors l'AN DOIT inclure ces informations dans le message d'événement QoS-Start.

7.3.2.12 Port de coordination de porte

Cet objet contient le numéro de port UDP, qui est utilisé par un AN pour guetter le message de coordination de portes.

Longueur = 8	S-Num = 12	S-Type = 1
AN port (16 bits)	Réservé	

Cet objet serait normalement inclus dans le message GATE-ALLOC-ACK, envoyé par un AN en réponse à un GATE-ALLOC. Toutefois, si un message GATE-SET est utilisé pour allouer une porte au lieu de GATE-ALLOC, cet objet doit être dans le message GATE-SET-ACK.

7.3.3 Définition des messages de contrôle de porte

Les messages qui effectuent le contrôle de porte entre le GC et AN DOIVENT être définis et formatés comme suit. Il est à noter que les messages du GC à l'AN sont des messages COPS Decision et que les messages de l'AN au GC sont des messages COPS Report.

```
<Gate-Control-Cmd>      := <COPS-Common-Header> <Handle>
                           <Context> <Decision Flags>
                           <ClientSI-Data>
<ClientSI-Data          := <Gate-Alloc> | <Gate-Set> | <Gate-Info>> |
                           <Gate-Delete>
<Gate-Control-Response> := <COPS-Common-Header> <Handle>
                           <Report-Type> <ClientSI-Object>
<ClientSI-Object>       := <Gate-Alloc-Ack> | <Gate-Alloc-Err> |
                           <Gate-Set-Ack> | <Gate-Set-Err> |
                           <Gate-Info-Ack> | <Gate-Info-Err> |
                           <Gate-Delete-Ack> | <Gate-Delete-Err>
<Gate-Alloc>            := <Decision-Header> <Transaction-ID> <Subscriber-ID>>>
                                                  [<Activity-Count>]
<Gate-Alloc-Ack>        := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                           <Gate-ID> <Activity-Count>>
                           <Gate-Coordination-Port>
<Gate-Alloc-Err>        := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <IPCablecom-Error>
<Gate-Set>              := <Decision-Header> <Transaction-ID> <Subscriber-ID>
                           [<Activity-Count>] [<Gate-ID>]
                           [<Remote-Gate-Info>]
                           [<Event-Generation-Info>]
                           [<Media-Connection-Event-Info>]
                           [<Electronic-Surveillance-Parameters>]
                           [<Session-Description-Parameters>]
                           <Gate-Spec> [<Gate-Spec>]
<Gate-Set-Ack>          := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                           <Gate-ID> <Activity-Count>
                           [<Gate-Coordination-Port>]
<Gate-Set-Err>          := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <IPCablecom-Error>
<Gate-Info>             := <Decision-Header> <Transaction-ID> <Gate-ID>
<Gate-Info-Ack>         := <ClientSI-Header> <Transaction-ID> <Subscriber-ID>
                                <Gate-ID> [<Remote-Gate-Info>]
                           [<Event-Generation-Info>]
                           [<Media-Connection-Event-Info>]
                           <Gate-Spec> [<Gate-Spec>]
<Gate-Info-Err>         := <ClientSI-Header> <Transaction-ID> <Gate-ID>
                                <IPCablecom-Err>
<Gate-Delete>           := <Decision-Header> <Transaction-ID> <Gate-ID>
<Gate-Delete-Ack>       := <ClientSI-Header> <Transaction-ID> <Gate-ID>
<Gate-Delete-Err>       := <ClientSI-Header> <Transaction-ID> <Gate-ID>
                                <IPCablecom-Err>
```

L'objet Context (C-NUM = 2, C-TYPE = 1) dans le message COPS Decision a la valeur R-Type (*request type flag*) réglée à 0x08 (*Configuration Request*) et la valeur M-Type réglée à zéro. Le champ Command-Code dans l'objet obligatoire Decision-Flags (C-NUM = 6, C-TYPE = 1) est réglé à 1 (*Install Configuration*). D'autres valeurs amèneraient l'AN à générer un message Report indiquant l'échec. L'objet Report-Type (C-NUM = 12, C-TYPE = 1) inclus dans le message COPS Report a le champ Report-Type réglé à 1 (succès) ou 2 (échec) en fonction de l'aboutissement de la commande de contrôle de porte. Il convient que tous les messages Report transportant la réponse du contrôle de porte aient le bit indicateur mis à 1 dans l'en-tête COPS.

7.4 Fonctionnement du protocole de contrôle de portes

7.4.1 Séquence d'initialisation

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

En réponse, le contrôleur de porte envoie un message CLIENT-ACCEPT. Ce message inclut l'objet Keep-Alive-Timer qui indique à l'AN l'intervalle maximal entre les messages Keep-Alive.

L'AN envoie alors un message REQUEST, comprenant les objets Handle et Context. L'objet Context (C-NUM = 2, C-TYPE = 1) PEUT avoir la valeur R-Type (*Request Type Flag*) réglée à 0x08 (*Configuration Request*) et M-Type réglée à zéro. L'objet Handle contient un nombre qui est choisi par l'AN. La seule exigence imposée sur ce nombre est qu'un AN NE DOIT PAS utiliser le même nombre pour deux DEMANDES différentes sur une seule connexion COPS; dans l'environnement IPCablecom, la valeur numérique Handle n'a pas d'autre signification dans le protocole. Ceci complète la séquence d'initialisation qui est représentée à la Figure 14.

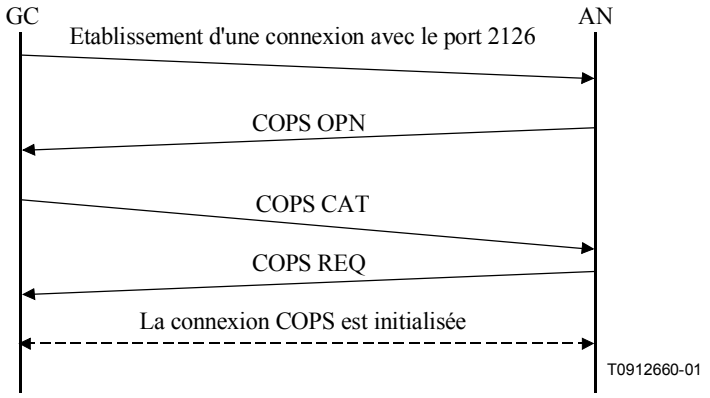


Figure 14/J.163 – Etablissement d'une connexion COPS

Périodiquement l'AN DOIT envoyer un message COPS KEEP-ALIVE (KA) au GC. A la réception du message COPS KA, le GC DOIT renvoyer un message COPS KA à l'AN. Cette transaction est représentée à la Figure 15 et est complètement documentée dans IETF RFC 2748. 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.

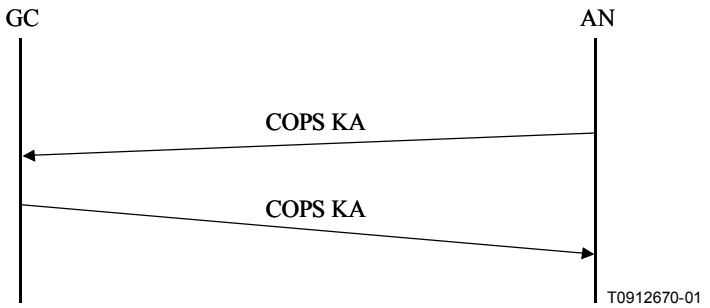


Figure 15/J.163 – Echange de messages Keep-Alive COPS

7.4.2 Séquence d'opérations

Le protocole entre le contrôleur de porte et l'AN 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 l'AN. 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 initiés par le contrôleur de porte incluent GATE-ALLOC, GATE-SET, GATE-INFO et GATE-DELETE. Les procédures relatives à ces messages sont décrites dans les paragraphes suivants. Tous ces messages sont envoyés en utilisant les objets spécifiques au client dans l'objet décision des messages COPS DECISION. Les réponses depuis l'AN sont envoyées comme un message REPORT-STATE avec les objets spécifiques au client dans l'objet ClientSI.

Les messages DECISION et les messages REPORT-STATE DOIVENT contenir le même identificateur que celui utilisé dans la DEMANDE initiale envoyée par l'AN lorsque la connexion COPS a été initiée.

GATE-ALLOC valide le nombre de sessions simultanées qui peuvent être établies depuis le MTA de départ 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 portes.

GATE-INFO est un mécanisme par lequel le contrôleur de porte peut trouver toutes les fixations de paramètres et d'états courants d'une porte ou d'un ensemble de portes existant.

L'AN DOIT envoyer périodiquement un message Keep Alive (KA) au GC pour faciliter la détection des pannes de connexion du TCP. Le contrôleur de porte effectue le suivi de la réception des messages KA. Si le contrôleur de porte n'a pas reçu un KA de l'AN dans le temps spécifié par IETF RFC 2748 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 fois où cet AN lui demande d'allouer une porte.

GATE-DELETE permet à un contrôleur de porte de supprimer une porte récemment allouée dans certains cas (voir ci-dessous).

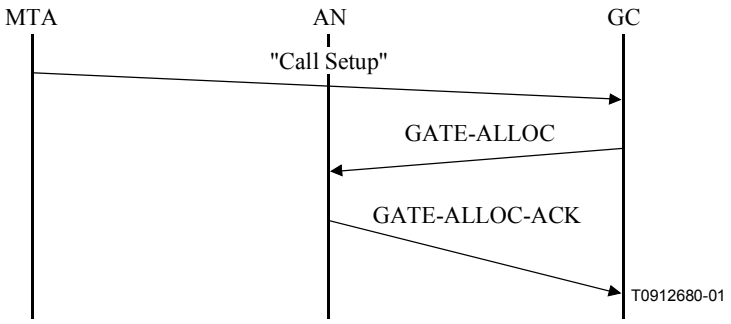
7.4.3 Procédures pour allouer une nouvelle porte

Un message GATE-ALLOC est envoyé par le contrôleur de porte à l'AN au moment où le message "Call_Set-up" est envoyé depuis le MTA de départ (par exemple, message "Invite(stage1)" lorsque le DCS est utilisé), comme l'indique la Figure 16.

L'utilisation de GATE-ALLOC garantit qu'un trop grand nombre de sessions ne soit pas simultanément demandé depuis un MTA donné. Ce mécanisme peut être utilisé pour contrôler une attaque de refus de service en provenance du MTA. L'AN, dans sa réponse au message GATE-ALLOC, compare le nombre de portes actuellement alloué pour l'ID de l'abonné indiqué avec le champ Count de l'objet Activity-Count dans le message GATE-ALLOC. Si le nombre de portes en cours est supérieur ou égal au champ Count dans GATE-ALLOC, alors l'AN DOIT renvoyer un message GATE-ALLOC-ERR. Si le nombre de portes en cours est supérieur au champ Count dans GATE-ALLOC, alors il est vraisemblable que l'abonné a été réapprovisionné pour avoir une limite de porte inférieure à 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 l'AN tant que le compte de session de l'abonné n'est pas descendu en dessous de la valeur spécifiée dans le champ Count.

Si l'objet Activity-Count n'est pas présent, l'AN 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 l'AN 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 à l'AN pour supprimer la porte qui a été incorrectement allouée (voir § 7.4.6). Le GC PEUT inclure l'objet Activity-Count dans les messages GATE-ALLOC suivants pour cet abonné une fois que la politique a été mise en antémémoire.

Le schéma qui suit (voir Figure 16) illustre un exemple de la signalisation GATE-ALLOC:



NOTE – A titre d'exemple, le message "Call Setup" dans ce contexte se réfère à "Invite without ring" lorsque l'on utilise DCS.

Figure 16/J.163 – Exemple de signalisation de GATE-ALLOC

L'AN DOIT répondre à un message GATE-ALLOC avec un GATE-ALLOC-ACK (indiquant la réussite) ou un GATE-ALLOC-ERR (indiquant l'échec). L'identification de la réponse (Transaction-ID) dans la réponse DOIT correspondre à l'identification de la transaction dans la demande.

Les erreurs lors de l'allocation de portes sont rapportées par une réponse GATE-ALLOC-ERR. L'objet IPCablecomError contient l'un des codes d'erreur suivants:

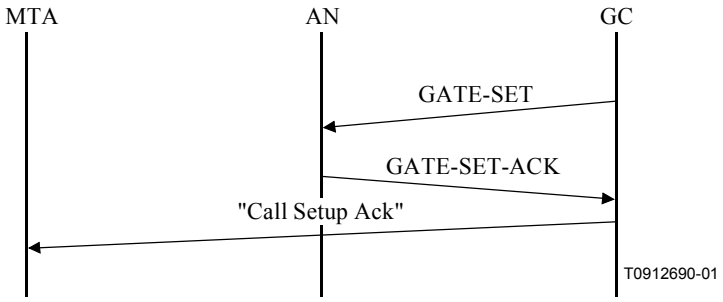
1 = Pas de portes actuellement disponibles

4 = L'abonné a dépassé la limite de porte

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 à l'AN pour initialiser ou modifier les paramètres opérationnels de la ou des portes. La Figure 17 donne un exemple de la signalisation GATE-SET.



NOTE – A titre d'exemple, le message "Call Setup Ack" se rapporte dans ce contexte au message "200 OK" qui est "Invite without ring" lorsque l'on utilise DCS.

Figure 17/J.163 – Exemple de signalisation de GATE-SET

Si un objet Gate-ID est présent dans le message GATE-SET, alors la demande est de modifier une porte existante. Si l'objet Gate-ID manque dans le message GATE-SET, alors il s'agit d'une demande d'allocation d'une nouvelle porte et l'objet Activity-Count PEUT être présent de sorte que l'AN peut déterminer si l'abonné a dépassé le nombre maximal de portes simultanées.

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.

L'AN 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 transaction dans la réponse DOIT correspondre à l'ID transaction dans la demande.

Les erreurs dans l'allocation ou l'autorisation de portes sont rapportées par une réponse GATE-SET-ERR. L'objet IPCablecom-Error contient un des codes d'erreur suivants:

1 = Aucune porte actuellement disponible

2 = ID porte illégale

3 = Valeur de classe de session illégale

4 = Limite de porte dépassée de l'abonné

127 = Autre, erreur non spécifiée

En traitant une demande de réservation d'un MTA, l'AN DOIT déterminer la porte correcte en utilisant l'objet RSVP Gate-ID ou en utilisant le bloc d'autorisation TLV. L'AN DOIT vérifier que la demande de réservation se trouve dans les limites autorisées spécifiées pour la porte.

L'AN met alors à jour la demande de réservation à partir des paramètres de la porte. Si le drapeau auto-commit est réglé, l'AN DOIT alors prendre l'action appropriée sur la couche MAC J.112 pour engager immédiatement les ressources. L'AN DOIT régler l'IP-Type-Of-Service-Overwrite (TOS) par le paramètre Diffserv Code Point (DSCP).

L'AN DOIT exécuter une fonction de contrôle d'admission, basée sur les paramètres de politiques fournis et la valeur Session Class de la porte.

Noter qu'un message GATE-SET peut être utilisé pour allouer (et régler) 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 portes ne soit pas disponible pour le contrôleur de porte. Si tel est le cas, le port AN dans l'objet Remote-Gate-Info (transporté dans le message GATE-SET) est réglé à zéro. Ceci amène l'AN 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 Remote-Gate-Info) pour informer l'AN sur ce port.

7.4.5 Procédures pour interroger une porte

Lorsqu'un contrôleur de porte souhaite trouver les fixations de paramètres en cours d'une porte, il envoie à l'AN un message GATE-INFO. L'AN DOIT répondre à un message GATE-INFO avec 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.

Les erreurs dans l'interrogation de portes sont rapportées par une réponse GATE-INFO-ERR. L'objet Erreur contient l'un des codes d'erreur suivants:

2 = ID de porte illégale

127 = Autre, erreur non spécifiée

7.4.6 Procédures pour supprimer une porte

Dans un flux d'appel normal, une porte est supprimée par l'AN lorsqu'elle reçoit un message RSVP-PATH-TEAR ou la demande de libérer le flux J.112 via l'interface de couche MAC J.112 (depuis un MTA intégré qui ne prend pas en charge RSVP). L'AN supprime également une porte à la réception d'un message GATE-CLOSE d'un AN distant (modèle DCS) ou un CMS (modèle NCS).

Un contrôleur de porte, généralement, n'initie 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 une porte sur l'AN. Par exemple, si le contrôleur de porte apprend (au moment de la réception de la réponse GATE-ALLOC-ACK) qu'un abonné a dépassé sa limite de porte, il peut vouloir supprimer la porte récemment allouée au niveau de l'AN. Dans des scénarios de ce type, il PEUT envoyer un message GATE-DELETE à l'AN (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.

L'AN DOIT répondre à un message GATE-DELETE avec 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 Error contient l'un des codes d'erreurs suivants:

2 = ID de porte illégale

127 = Autre, erreur non spécifiée

7.4.7 Séquence de terminaison

Lorsque l'AN ferme sa connexion TCP vers le GC, il PEUT d'abord envoyer un message DELETE-REQUEST-STATE (comprenant l'objet identificateur utilisé dans le message REQUEST). L'AN 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 à l'AN lorsque la connexion TCP est terminée.

Lorsque le contrôleur de porte va s'arrêter, il CONVIENT qu'il envoie un message COPS Client-Close (CC) à l'AN. Dans le message COPS CC, il convient que le contrôleur de porte n'envoie pas l'objet PDP redirect address object <PDPRedirAddr>. Si l'AN reçoit un message COPS CC du contrôleur de porte avec un objet <PDPRedirAddr> object, l'AN DOIT ignorer le <PDPRedirAddr> lorsqu'il traite le message COPS CC.

8 Interface de coordination de porte à porte (pkt-q8)

Des messages sont échangés entre les portes pour synchroniser leur utilisation. Il s'agit de messages qui incluent GATE-OPEN, GATE-CLOSE et leur accusé de réception correspondant. Les messages GATE-OPEN sont échangés lorsque la porte a engagé des ressources activées ou changées en résultat d'une commande provenant du MTA (voir Figure 18). Les messages GATE-CLOSE sont échangés lorsque ces ressources sont libérées. Les temporisateurs à l'intérieur de l'implémentation de porte imposent un contrôle strict sur la durée que ces échanges peuvent occuper.

Les messages de synchronisation de portes peuvent être échangés directement entre les AN ou peuvent être échangés par l'intermédiaire de mandataires (généralement le système de traitement des appels IPCablecom (CMS, *call management system*), qui désire une notification des différents cas d'erreur qui provoquent une fermeture prématurée des portes). La Figure 18 montre la coordination directe de porte à porte et la Figure 19 montre la coordination des portes par l'intermédiaire de mandataires CMS aux deux extrémités. Des configurations non représentées sont également possibles avec un mandataire à une extrémité simplement.

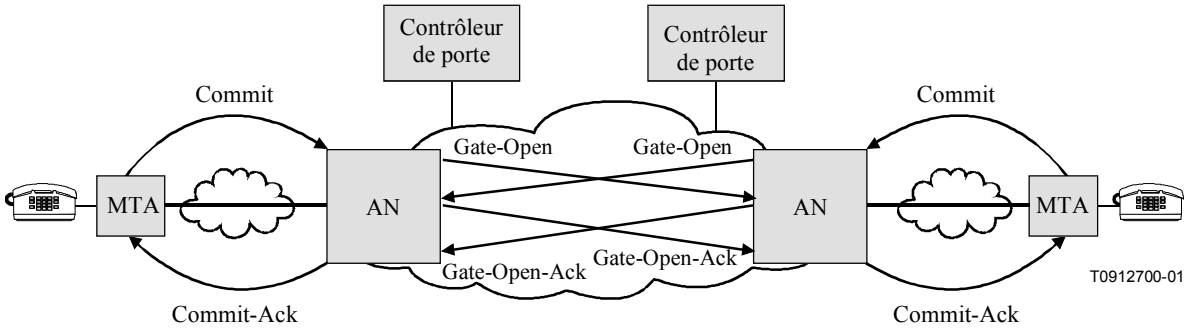


Figure 18/J.163 – Coordination de portes de bout en bout

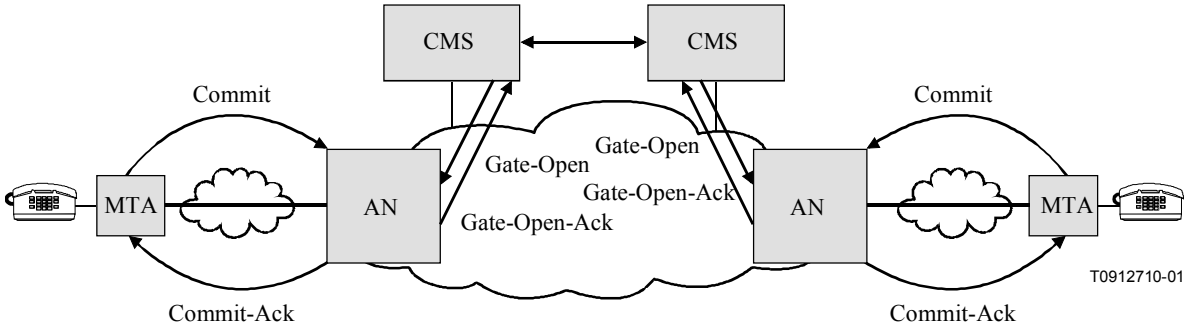


Figure 19/J.163 – Coordination de portes par des mandataires CMS

Une porte est initialement créée par une commande GATE-SET du contrôleur de porte. La commande GATE-SET contiendra des informations telles que les classificateurs de prototype (par exemple, tuple 6) et Flowspecs pour les portes locales et distantes. Elle contient également l'adresse IP et le numéro de port de l'AN distant de sorte qu'ils puissent implémenter la coordination de porte à porte.

8.1 Messages du protocole de porte à porte

Les messages du protocole de porte à porte (*Gate-to-Gate Protocol*) sont envoyés sous la forme de paquets UDP/IP, où le port de destination EDP est donné par la commande GATE-SET. Le port source UDP DOIT être le port au niveau duquel l'émetteur guette l'accusé de réception. Exactement, un message DOIT être encapsulé dans le champ UDP Data. Le format de l'en-tête commun à tous les messages est représenté ci-dessous et est identique à la spécification de RADIUS dont il est copié.

Message type (Type de Message)	Transaction ID (ID de la transaction)	Message length (Longueur de message)
Authentificateur de message (16 octets)		
Paramètres ….		

Le champ Message type occupe un octet et identifie le type de paquet. Les codes de type sont assignés comme suit:

GATE-OPEN	48
GATE-OPEN-ACK	49
GATE-OPEN-ERR	50
GATE-CLOSE	51
GATE-CLOSE-ACK	52
GATE-CLOSE-ERR	53

Le champ Transaction ID occupe un octet et facilite la correspondance entre les demandes et les réponses.

Message Length occupe deux octets et indique la longueur du message, y compris l'en-tête et tous les paramètres.

L'authentificateur de message (*Message Authenticator*) est un total de contrôle MD5 de 16 octets. Cette valeur est utilisée pour authentifier la demande et la réponse et repose sur un secret partagé entre les deux AN. L'authentificateur de message dans les messages GATE-OPEN et GATE-CLOSE contient un total factice MD5 IETF RFC 1321 à une voie calculé sur un flux d'octets composé de Message-Type + Transaction-ID + Message-Length + 16 zéro octets + Paramètres + secret partagé. L'authentificateur de message dans les messages GATE-OPEN-ACK, GATE-OPEN-ERR et GATE-CLOSE-ACK contient un total factice MD5 à une voie calculé sur un flux d'octets composé de Message-Type, Transaction-ID + Message-Length + Message Authenticator de la demande de message + paramètres de la réponse (le cas échéant) + secret partagé secret. La valeur du total factice résultant MD5 de 16 octets est stockée dans le champ Message Authenticator du paquet. Cet algorithme pour le calcul de l'authentificateur de message est identique à celui décrit dans IETF RFC 2865.

Les paramètres sont tous codés dans le style Type-Length-Value (Type-Longueur-Valeur) de RADIUS IETF RFC 2138. Les paramètres transportent la demande spécifique et les informations d'indication nécessaires pour parvenir à la coordination des portes. Le format de paramètre DOIT être le suivant:

Type	Length (Longueur)	Réservé, DOIT être nul
Valeur ….		

Le champ Type occupe un octet et contient les valeurs suivantes:

Gate-ID	224
Tspec	225
Reverse-Tspec	226
Error-code	227

Le champ Length occupe un octet et contient la longueur en octets du paramètre. Toutes les valeurs de longueur dans cette Recommandation sont des multiples de 4.

Le paramètre Gate-ID, lorsqu'il est présent dans un message, possède le format suivant:

224	8	0
Valeur Gate-ID (entier 32 bits)		

Le paramètre Tspec, lorsqu'il est présent dans un message, possède le format suivant (voir § 6.3.1 pour l'explication des champs):

225	36	0
0 (a) Réservé		7 (b)
1 (c)	0 Réservé	6 (d)
127 (e)	0 (f)	5 (g)
Débit du token bucket [r] (nombre à virgule flottante IEEE 32 bits)		
Taille du token bucket [b] (nombre à virgule flottante IEEE 32 bits)		
Taux de transfert pic des données [p] (nombre à virgule flottante IEEE 32 bits)		
Unité minimale régulée avec une politique [m] (entier 32 bits)		
Taille maximale de paquet [M] (entier 32 bits)		

Le paramètre Reverse-Tspec, lorsqu'il est présent dans un message, possède le format suivant (voir § 6.3.5 pour l'explication des champs):

226	36	0
0 (a) Réservé		7 (b)
1 (c)	0 Réservé	6 (d)
127 (e)	0 (f)	5 (g)
Débit du token bucket [r] (nombre à virgule flottante IEEE 32 bits)		
Taille du token bucket [b] (nombre à virgule flottante IEEE 32 bits)		
Taux de transfert pic des données [p] (nombre à virgule flottante IEEE 32 bits)		
Unité minimale régulée avec une politique [m] (entier 32 bits)		
Taille maximale de paquet [M] (entier 32 bits)		

Le paramètre Error-code, lorsqu'il est présent dans un message, possède le format suivant:

227	4	Erreur Code	Réservé

Les valeurs de code d'erreur sont comme suit:

0 Libération normale, initiée par MTA

1 Fermeture initiée par l'AN en raison de l'absence de mise à jour de la réservation (Reservation Maintenance) (par exemple rafraîchissements RSVP)

2 Fermeture initiée par l'AN en raison du manque de réponses de la couche MAC J.112 (par exemple mise à jour de station)

3 Expiration du temporisateur T1; pas de message COMMIT reçu du MTA

4 Expiration du temporisateur T2; échec de coordination des portes

5 Fermeture initiée par l'AN due à la nouvelle assignation de la réservation (par exemple pour une session priorité)

6 Fermeture initiée par l'AN due à une incompatibilité de réservation

129 ID de porte illégale

130 Authentificateur de message incorrect

255 Autre, erreur non spécifiée

8.1.1 GATE-OPEN

Le format d'un message GATE-OPEN DOIT être le suivant:

<GATE-OPEN> ::= <RADIUS-Common-Header> <Gate-ID>
[<Tspec> <Reverse-Tspec>]

La valeur de Gate-ID est copiée de la valeur Remote-Gate-ID contenue dans l'objet Remote-Gate-Info du message Gate-Set.

Lorsqu'un message GATE-OPEN est généré, les objets Tspec et Reverse-Tspec DOIVENT être présents.

Les valeurs dans le paramètre Tspec sont copiées de l'objet Flowspec du message COMMIT, s'il existe, et s'il n'existe pas, de l'objet Sender-Tspec du message RSVP-PATH qui a initié la réservation, ou elles sont générées des messages de la couche MAC J.112 qui ont initié l'opération Commit. Dans tous les cas, il indique les ressources engagées dans le sens amont (avant).

Les valeurs dans le paramètre Reverse-Tspec sont copiées de l'objet Reverse-Sender-Tspec du message COMMIT, s'il existe, et s'il n'existe pas de l'objet Reverse-Sender-Tspec du message RSVP-PATH qui a initié la réservation, ou généré des messages de la couche MAC J.112 qui ont initié l'opération Commit. Dans tous les cas, il indique les ressources engagées dans le sens aval (contraire).

8.1.2 GATE-OPEN-ACK

Le format d'un message GATE-OPEN-ACK DOIT être le suivant:

<GATE-OPEN-ACK> ::= <RADIUS-Common-Header>

Il n'y a pas de paramètres dans ce message d'accusé de réception. L'ID de transaction de l'en-tête commun sert à identifier auprès du destinataire quel message GATE-OPEN fait l'objet d'un accusé de réception.

8.1.3 GATE-OPEN-ERR

Le format d'un message GATE-OPEN-ERR DOIT être le suivant:

<GATE-OPEN-ERR> ::= <RADIUS-Common-Header> <Error-code>

Le Transaction-ID dans l'en-tête commun sert à identifier auprès du destinataire quel message GATE-OPEN fait l'objet d'un accusé de réception.

Le paramètre Error-code contient un code de raison indiquant la cause de l'erreur.

Si l'erreur est telle que l'ID de porte n'est pas reconnue et que par conséquent la clé correcte d'authentification n'est pas connue ou si l'Authentificateur de message du message GATE-OPEN est incorrect, l'authentificateur de message du message GATE-OPEN-ERR DOIT être une copie exacte de l'authentificateur du message GATE-OPEN.

8.1.4 GATE-CLOSE

Le format d'un message GATE-CLOSE DOIT être le suivant:

<GATE-CLOSE> ::= <RADIUS-Common-Header> <Gate-ID> [<Error-Code>]

Le message GATE-CLOSE est généré pour une raison autre qu'une demande normale de libération en provenance du MTA, alors le code d'erreur DOIT être présent en indiquant la raison.

GATE-CLOSE ne DOIT PAS être utilisé lorsque aucune porte n'est ouverte. Lorsque aucune porte n'est ouverte ou lorsque le CMS (lorsqu'il ne sert pas de mandataire pour l'AN distant) demande de fermer une porte, le message GATE-DELETE est utilisé.

8.1.5 GATE-CLOSE-ACK

Le format d'un message GATE-CLOSE-ACK DOIT être le suivant:

<GATE-CLOSE-ACK> ::= <RADIUS-Common-Header>

L'ID de transaction dans l'en-tête commun sert à identifier auprès du destinataire quel message GATE-CLOSE fait l'objet d'un accusé de réception.

8.1.6 GATE-CLOSE-ERR

Le format d'un GATE-CLOSE-ERR message DOIT être le suivant:

<GATE-CLOSE-ERR> ::= <RADIUS-Common-Header> <Error-String>

L'ID de transaction dans l'en-tête commun sert à identifier auprès du destinataire quel message GATE-CLOSE fait l'objet d'un accusé de réception. L'authentificateur de message est une copie exacte de l'authentificateur de message du message GATE-CLOSE.

8.2 Procédure de coordination de portes

Lorsque le MTA effectue une opération Commit (comme décrit au § 6.7 pour tout MTA, ou dans l'Annexe A ou l'Annexe B pour les MTA intégrés), l'AN DOIT envoyer un message GATE-OPEN. Le message GATE-OPEN DOIT contenir les Flowspec (c'est-à-dire les flux directionnels). L'AN DOIT retransmettre le message GATE-OPEN, basé sur le temporisateur T5, jusqu'à la réception d'une réponse GATE-OPEN-ACK. Après un nombre fixe de tentatives de retransmission, l'AN déclare la perte de paquet inacceptable et ferme la porte.

A la réception d'un message GATE-OPEN, l'AN DOIT en accuser réception avec un message GATE-OPEN-ACK.

Si l'AN reçoit un message GATE-OPEN, mais n'a pas d'enregistrement de l'ID de porte et par conséquent ne connaît pas la clé de sécurité correcte, il DOIT envoyer le GATE-OPEN-ERR avec un authentificateur de message correspondant à l'authentificateur de message du message GATE-OPEN.

L'AN DOIT ignorer un authentificateur de message incorrect lorsque le type de message est GATE-OPEN-ERR, l'ID de transaction correspond à un message GATE-OPEN exceptionnel envoyé et l'authentificateur de message correspond à l'authentificateur de message du message GATE-OPEN.

Sur une demande Commit ou à la réception du message GATE-OPEN, selon que l'un ou l'autre intervient en premier, l'AN DOIT démarrer le temporisateur T2.

Sur une demande Commit à la réception du message GATE-OPEN, selon que l'un ou l'autre intervient en second, l'AN DOIT annuler le temporisateur T2. Si le flowspec ne correspond pas, l'AN DOIT fermer la porte, initier la libération du flux J.112 et envoyer un message GATE-CLOSE.

Si le temporisateur T2 expire après réception d'une demande Commit, mais sans réception d'un message GATE-OPEN, l'AN DOIT fermer la porter, initier la libération du flux J.112 et envoyer un message GATE-CLOSE.

L'AN DOIT envoyer un message GATE-CLOSE lorsqu'il reçoit un message explicite de libération en provenance du MTA client (comme indiqué au § 6.5.3 pour tout MTA, ou dans l'Annexe A ou l'Annexe B pour les MTA intégrés), ou lorsqu'il détecte que le client ne génère plus activement de paquets et ne génère pas de rafraîchissement adapté pour le flux associé à une porte. L'AN DOIT également fermer une porte lorsqu'il reçoit un message GATE-CLOSE. Ceci garantit que les portes associées à une session sont fermées presque simultanément.

A la réception d'un message GATE-CLOSE correctement authentifié, l'AN DOIT toujours répondre avec un GATE-CLOSE-ACK, envoyé à l'adresse donnée comme adresse source de la commande. Après avoir envoyé le GATE-CLOSE-ACK, l'AN DOIT conserver l'ID de porte et la clé d'authentification disponibles pendant une période d'au moins 30 secondes pour permettre les retransmissions possibles du message GATE-CLOSE.

Si l'AN n'a pas d'enregistrement de l'ID de porte et par conséquent ne connaît pas la clé de sécurité correcte, il DOIT envoyer le GATE-CLOSE-ERR avec un authentificateur de message correspondant à l'authentificateur de message du message GATE-CLOSE.

L'AN DOIT ignorer un authentificateur de message incorrect lorsque le type de message est GATE-CLOSE-ERR, l'ID de la transaction correspond à un message GATE-CLOSE exceptionnel envoyé et l'authentificateur de message correspond à l'authentificateur de message du message GATE-CLOSE.

8.2.1 Exemple de procédures pour la coordination des portes de bout en bout

Pour effectuer la synchronisation de portes de bout en bout, le contrôleur de porte établit chaque porte avec l'adresse et l'ID de porte de l'autre AN distant; chaque AN envoie et reçoit les messages GATE-OPEN/GATE-CLOSE de l'autre.

Une fois que les MTA ont effectué la signalisation de leur session, ils commenceront la session avec une opération Commit (comme indiqué au § 6.7 pour tout MTA, ou à l'Annexe A ou l'Annexe B pour les MTA intégrés) à l'AN. Ceci amène l'AN à ouvrir la porte. L'AN informe maintenant l'AN distant que la porte est ouverte. L'AN local envoie un message GATE-OPEN à l'AN distant et démarre le temporisateur T2, décrit à l'Annexe C. Le message GATE-OPEN contient les deux Flowspec (c'est-à-dire les flux bidirectionnels). L'AN distant accuse réception du message GATE-OPEN avec un message GATE-OPEN-ACK.

De plus, l'AN s'attend à recevoir un message GATE-OPEN de l'AN distant après que le MTA distant a envoyé son message COMMIT. Ce message GATE-OPEN distant, de l'AN distant contient de façon similaire les deux Flowspec. Ces paramètres flowspec sont comparés à ceux de l'AN local. Si les Flowspec correspondent, la porte est autorisée à rester ouverte.

Pour désactiver le temporisateur T2, un GATE-OPEN-ACK et un message GATE-OPEN sont reçus de l'AN distant. Si le GATE-OPEN-ACK n'est pas reçu de l'AN distant avant l'expiration du temporisateur T5 (décrit à l'Annexe C, la valeur est de l'ordre d'un trajet aller-retour), l'AN retransmet le message GATE-OPEN local pour récupérer la perte. Cette méthode de reprise par niveau d'application est tentée sur un nombre fixe de tentatives de retransmission au-delà duquel l'AN déclare la perte de paquet inacceptable et ferme la porte. Il convient que la valeur du temporisateur T2 soit suffisamment grande pour tenir de compte de la récupération de messages perdus. Voir Figure 20.

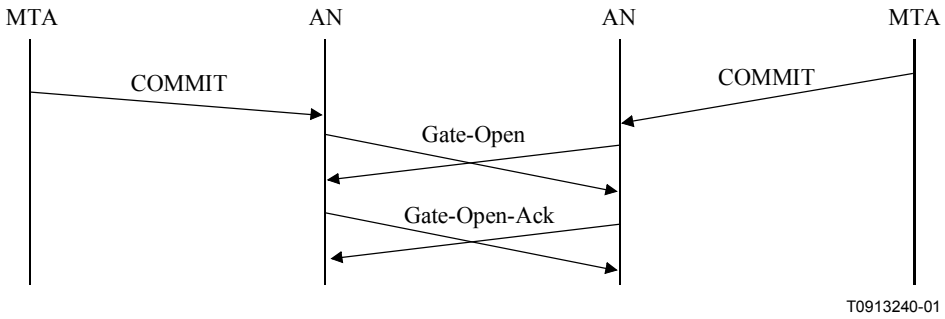


Figure 20/J.163 – Coordination de portes au moment de COMMIT

La coordination des portes est également effectuée au moment où une porte est fermée. Chaque AN envoie un message GATE-CLOSE à son AN homologue lorsqu'il reçoit un message de libération explicite en provenance du MTA (tel que décrit au § 6.5.3 pour tout MTA, ou à l'Annexe A ou l'Annexe B pour les MTA intégrés), ou lorsqu'il détecte que le client ne génère plus activement des paquets et ne génère plus de rafraîchissements adaptés pour le flux associé à une porte. Un AN ferme également une porte lorsqu'il reçoit un message GATE-CLOSE de l'AN distant. Ceci garantit que les portes associées à une session soient fermées presque simultanément. Voir Figure 21.

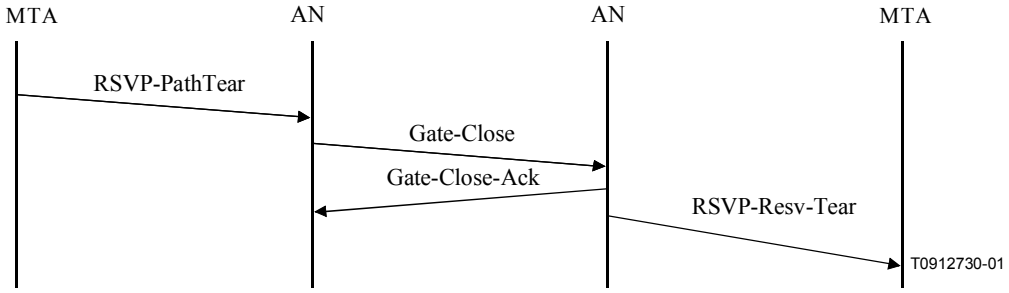


Figure 21/J.163 – Coordination de portes sur libération

A la réception d'un message GATE-CLOSE correctement authentifié, l'AN répond avec un GATE-CLOSE-ACK, envoyé à l'adresse donnée comme adresse source de la commande. Après avoir envoyé le GATE-CLOSE-ACK, l'AN conserve l'ID de porte et la clé d'authentification disponibles pendant une période de 30 secondes pour permettre les retransmissions possibles du message GATE-CLOSE.

8.2.2 Exemple de procédure pour coordination de portes mandatée

Cet exemple montre comment un système de gestion d'appels (CMS, *call management system*) peut utiliser une coordination de portes mandatée. Le contrôleur de porte initialise chaque porte avec l'adresse du CMS comme entité de coordination distante et un identificateur choisi par le CMS comme ID de porte. L'AN exécute les procédures de coordination de portes en envoyant les messages GATE-OPEN/GATE-CLOSE au CMS, qui les transmet à la porte distante.

Lorsque le CMS détermine que les ressources sont disponibles au niveau de l'extrémité (distante) d'arrivée il donne l'ordre au MTA d'engager les ressources. Il enverra également un message GATE-OPEN à l'AN et démarrera le temporisateur T5. L'AN accuse réception du message GATE-OPEN avec un message GATE_OPEN_ACK qui désactive le temporisateur T5 dans le CMS. Si le message GATE_OPEN_ACK n'est pas reçu depuis l'AN avant l'expiration du temporisateur T5, le CMS retransmet le message GATE-OPEN pour récupérer la perte. Cette méthode de récupération du message au niveau de l'application est tentée un nombre fixe de tentatives de retransmission, au-delà

duquel le CMS déclare la perte du paquet inacceptable et ferme la porte. A la réception du message GATE-OPEN du CMS ou du message COMMIT du MTA, l'AN démarre le temporisateur T2.

Pour désactiver le temporisateur T2, l'AN doit recevoir avec succès un message COMMIT en provenance du MTA et un message GATE-OPEN du CMS. Si le temporisateur T2 expire, l'AN initie un message GATE-CLOSE ou un message de couche MAC J.112 (selon le cas) afin de fermer la porte et libérer toutes les ressources associées à la porte. Voir Figure 22.

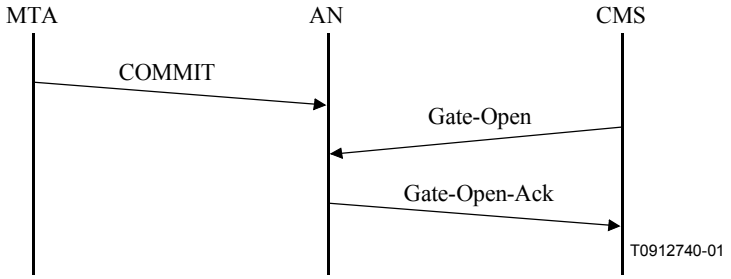


Figure 22/J.163 – Coordination de portes au moment de COMMIT

La coordination des portes est également effectuée au moment où une porte est fermée. L'AN envoie un message GATE-CLOSE à son CMS lorsqu'il reçoit un message explicite de libération en provenance du MTA (tel que décrit au § 6.5.3 pour tout MTA ou à l'Annexe A ou l'Annexe B pour les MTA intégrés), ou lorsqu'il détecte que le client ne génère plus activement de paquets et ne génère pas de rafraîchissement adapté pour le flux associé à une porte. Un AN ferme également une porte lorsqu'il reçoit un message GATE-CLOSE ou GATE-DELETE du CMS. Ceci garantit que les portes associées à des MTA non réceptifs sont fermées presque simultanément.

A la réception d'un message GATE-CLOSE correctement authentifié, le CMS répond avec un GATE-CLOSE-ACK, envoyé à l'adresse donnée comme adresse source de la commande. Après avoir envoyé le message GATE-CLOSE-ACK, le CMS conserve l'ID de porte et la clé d'authentification disponibles pendant une période d'au moins 30 secondes pour tenir compte des retransmissions possibles du message GATE-CLOSE. Voir Figure 23.

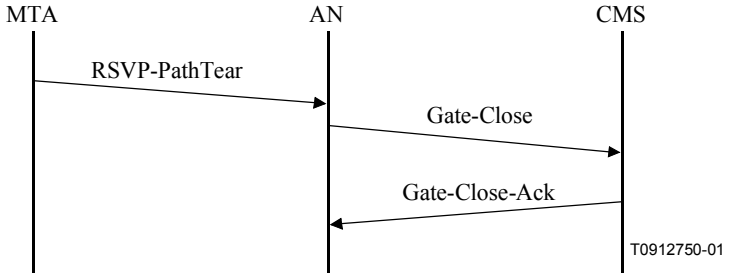


Figure 23/J.163 – Coordination de portes sur libération

ANNEXE A

Exigences supplémentaires relatives aux implémentations de l'Annexe A/J.112

Au lieu d'utiliser l'interface pkt-q3 (RSVP+) pour demander la QS dans le réseau J.112 tel que décrit au § 6, un MTA intégré PEUT réserver dynamiquement des ressources QS locales en utilisant les mécanismes définis dans UIT-T J.112. Avec cette autre approche, un MTA intégré signale directement son besoin de QS dans le réseau d'accès local J.112 en utilisant les primitives MAC définies dans l'Annexe A/J.112. Comparé au § 6, la signalisation de la QS utilisant le protocole MAC J.112 (pkt-q2) est initiée par le CM au lieu de l'AN sur demande du MTA. Dans le mécanisme décrit à l'article 6, la demande de QS est reçue par l'AN via une interface de couche 4 (pkt-q3) tandis que le mécanisme décrit dans la présente annexe utilise une interface de couche MAC (primitives MAC) mettant en interface le MTA avec le CM (pkt-q1). Toutes les autres interfaces et signaux restent inchangés. Des exemples illustrant cette approche sont donnés aux Appendices VII et VIII.

Un MTA intégré reçoit au niveau de son interface avec la couche Application les exigences de QS basées sur la session dans les protocoles de signalisation (IETF RFC 2543 et UIT-T J.162). Une fois que le MTA intégré détermine que les ressources de QS ont besoin d'être réservées ou engagées, le MTA DOIT initier la signalisation J.112 pour provoquer la traduction des exigences de QS de l'application basées sur la session en une allocation de ressources basée sur des flux J.112 dans le réseau J.112 et la création, le changement, et/ou la suppression des flux appropriés résultants. Selon que la session a ou non son origine dans le MTA intégré ou par un homologue ou encore par un nœud de réseau du CPE, le MTA transmet les exigences de QS au protocole MAC J.112 via les primitives MAC. Ceci déclenche des actions appropriées sur la couche MAC pour créer ou modifier J.112 en utilisant des mécanismes d'envoi de messages pour l'établissement de connexions et/ou la gestion de liaisons du protocole MAC J.112.

Les paragraphes qui suivent étudient le mappage par le MTA des exigences de la QS de l'application basée sur la session avec les ressources requises dans un réseau J.112, l'utilisation des primitives MAC et le support de l'allocation de ressources en deux phases réservation/engagement (reserve/commit) dans un réseau J.112.

A.1 Terminologie

Dans un réseau conforme à l'Annexe A/J.112, le terminal côté client peut être formé soit par un CM soit un boîtier décodeur (STB, *set-top box*). Les deux dispositifs incorporent une unité d'interface réseau (NIU, *network interface unit*) qui fournit l'interface physique et logique entre le réseau J.112 et le CPE. Le nœud d'accès (AN) est, dans ce cas, implémenté comme un adaptateur de réseau interactif (INA, *interactive network adapter*) fournissant l'interface au réseau de base et aux éléments de l'architecture IPCablecom qui sont établis en dehors du réseau J.112, tels que CMS et RKS. Les flux J.112 sont considérés comme des connexions bidirectionnelles.

Dans la mesure où la présente annexe se réfère uniquement aux réseaux J.112 conforme à l'Annexe A, les termes nœud d'accès (AN, *access node*) et adaptateur de réseau interactif (INA) sont utilisés de façon interchangeable.

A.2 Mappage des Flowspec avec les paramètres J.112 de QS

Un MTA intégré reçoit les exigences de QS d'une application sur une base par session et doit les transmettre au protocole MAC J.112 en utilisant les primitives MAC. Les exigences de QS sont reçues au format des descriptions de service de la couche supérieure (par exemple SDP tel que utilisé dans les applications VoIP) si la session est initiée par le MTA lui-même ou au format des flowspec RSVP si la session est initiée par un homologue ou un nœud de réseau. D'autres spécifications (par exemple la spécification CODEC IPCablecom J.161) définissent le mappage des descriptions de service de la couche supérieure en flowspec. Le présent paragraphe spécifie comment le MTA DOIT

mapper les exigences de QS avec les paramètres de la couche MAC J.112. Dans le présent paragraphe il est supposé que le protocole de transport utilisé soit UDP. Si un protocole de transport différent était utilisé, des changements appropriés seraient applicables aux paramètres spécifiés dans la présente Recommandation et pour la suppression d'en-tête.

Dans un réseau J.112, les ressources sont allouées sur une base connexion par connexion. Une connexion est un flux de données bidirectionnel simple entre le CM et l'INA. A ce titre, la connexion comprend un flux aval et un flux amont. Les ressources sont réservées pour les sens amont et aval. Ils sont décrits avec un ensemble de paramètres, qui pourraient en général différer pour les sens amont et aval. Le protocole MAC J.112 définit plusieurs paramètres de QS qui sont applicables pour différents modes d'accès de l'Annexe A/J.112. Ainsi, le MTA spécifie dans sa demande les paramètres de QS à associer à la connexion correspondante dans le sens amont et aval.

Pour demander un mode d'accès spécifique le MTA PEUT utiliser des informations de politique données par l'opérateur de réseau J.112 et les caractéristiques de la source telles que décrites dans les exigences de QS pour la session. Toutefois, la décision finale concernant quelles ressources sont allouées à une connexion particulière est confiée à l'INA et DOIT également reposer sur la quantité totale de ressources disponibles.

A titre d'exemple de mappage d'une description de session avec les paramètres de QS J.112, considérons une application VoIP qui utilise le codec audio G.729 Annexe E et la description de SDP suivante:

- c = IN IP4 192.168.73.10
- m = audio 3456 RTP/AVP 96
- a = rtpmap: 96 G729E/8000
- a = ptime: 10

où "c" contient les informations sur la connexion, "m" est la description du média à transporter dans cette session et "a" décrit les attributs de la session. Dans cette session particulière, un "rtpmap" est inclus spécifiant les paramètres code. L'attribut "ptime" définit qu'un paquet représente 10 ms de signal audio. La description de la session peut être mappée avec les paramètres MAC J.112 dans le sens amont tel que:

- accès à débit fixe;
- bande passante demandée de 240 cellules ATM par 1200 ms (équivalent à 75 kbit/s);
- assignation cyclique de deux intervalles tous les 60 intervalles.

Dans l'exemple ci-dessus il est supposé que DirectIP est utilisé comme méthode d'encapsulage amont et que la vitesse de transmission des données amont est de 3,088 Mbit/s. En calculant la bande passante demandée, le préfixe de la méthode d'encapsulage et tout préfixe de protocole MAC J.112 DOIVENT être pris en compte. En utilisant la suppression d'en-tête, la taille PDU dans le sens amont peut potentiellement être réduite de manière significative, en fonction des champs des en-têtes qui peuvent être supprimés.

Un classificateur est utilisé pour assigner les paquets arrivant soit au niveau du CM ou de l'INA à la connexion appropriée, afin de garantir qu'ils reçoivent la QS appropriée. Pour pouvoir établir un classificateur aux deux extrémités du réseau J.112 le MTA intégré peut inclure des paramètres d'association de session dans sa demande. Toutefois, l'INA peut également recevoir ces paramètres de la porte via l'interface couche MAC J.112. Les paramètres d'association de session amont sont les suivants:

- Source Address (adresse source): l'adresse IP du MTA.
- Source Port (port source): le numéro de port sur lequel le MTA enverra le flux de média.
- Destination Address (adresse de destination): l'adresse IP de l'extrémité distante de la connexion telle qu'elle est donnée dans le paramètre "c" de la description SDP.

- Destination Port (port de destination): le numéro de port sur lequel l'extrémité distante recevra le flux de média tel qu'il est donné dans le paramètre "m" de la description SDP.
- Protocol (protocole): le protocole de transport à utiliser (UDP dans l'exemple ci-dessus).

Les paramètres d'association de session aval incluent:

- Source Address (adresse source): l'adresse IP de l'extrémité distante de la connexion telle qu'elle est donnée dans le paramètre "c" de la description SDP.
- Source Port (port source): le numéro de port sur lequel l'extrémité distante enverra le flux de média, ce paramètre n'est pas disponible au niveau du MTA et il convient qu'il ne soit pas spécifié comme partie du classificateur.
- Destination Address (adresse de destination): l'adresse IP du MTA.
- Destination Port (port de destination): le numéro de port sur lequel le MTA recevra le flux de média.
- Protocole: le protocole de transport à utiliser (UDP dans l'exemple ci-dessus).

A.3 Utilisation de primitives MAC J.112

Une fois que le MTA intégré a déterminé que les ressources de QS ont besoin d'être réservées ou engagées, il initie la signalisation J.112 appropriée en utilisant les primitives MAC. Les primitives MAC sont définies dans l'Annexe A/J.112. Le présent paragraphe décrit l'usage des primitives MAC.

La primitive MAC MAC_RESOURCE_REQ DOIT être utilisée par le MTA intégré pour signaler une demande pour créer, changer et/ou supprimer une connexion. Le type de la ressource qui est demandée (y compris la demande de libérer des ressources réservées) est indiqué par le paramètre Resource_Type.

A.3.1 Réservation de ressources

Le MTA initie la réservation de ressources de la QS en utilisant la primitive MAC_RESOURCE_REQ avec le paramètre Resource_Type réglé à 1, 2 ou 4. Le MTA doit inclure l'identification de la porte comme identification de la connexion. Pour une description plus détaillée des paramètres de la primitive MAC_RESOURCE_REQ se reporter à l'Annexe A/J. 112. Si le CM reçoit ce message, il invoque la signalisation MAC amenant à l'établissement d'une nouvelle connexion. Il confirme la réception de la primitive en répondant avec une primitive MAC_RESOURCE_CNF. L'autorisation du MTA de demander les ressources et la disponibilité des ressources est vérifiée par l'INA. Si l'INA détecte une ID de connexion qui est déjà utilisée comme ID de porte avec une connexion correspondante qui n'existe pas, c'est une indication que les ressources sont réservées mais pas encore engagées. La décision finale est prise en fonction du bit Admit_Bit dans le message de <MAC> Resource Request. Si Admit_Bit est mis à 1, l'INA ne DOIT PAS encore engager les ressources. S'il est remis à zéro, l'INA DOIT engager les ressources à la connexion si le contrôle d'admission a été réussi. Si les ressources demandées ne sont pas disponibles la demande est refusée. Le CM avertit le MTA du résultat de la demande de ressources avec la primitive MAC_CONNECT_IND ou une primitive MAC_RESOURCE_DENIED_IND. Le procédé de réservation de ressources est illustré dans la Figure A.1.

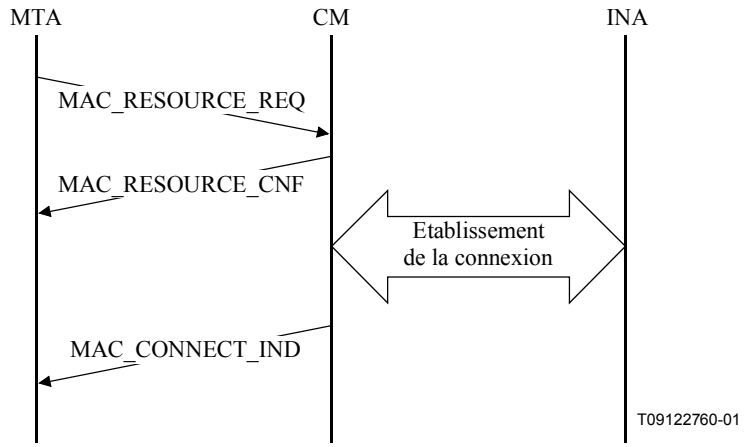


Figure A.1/J.163 – Réservation de ressources en utilisant les primitives MAC

A.3.2 Engagement de ressources

Le MTA initie l'engagement des ressources de QS en utilisant la primitive MAC_RESOURCE_REQ avec le paramètre Resource_Type réglé à 1 ou 8. Le MTA doit inclure l'ID de porte comme ID de connexion. Pour une description plus détaillée des paramètres de la primitive MAC_RESOURCE_REQ, se reporter à l'Annexe A/J.112. Les ressources demandées dans ce message NE DOIVENT PAS être supérieures aux ressources réservées dans une demande précédente. Si le CM reçoit ce message il invoque la signalisation MAC aboutissant au réapprovisionnement de la connexion existante. Il confirme la réception de la primitive en répondant avec une primitive MAC_RESOURCE_CNF. Si l'INA détecte une identification de connexion qui est déjà utilisée comme identification de porte avec une connexion correspondante existante et le bit Admit_Bit dans le message <MAC> Resource Request reçu via le CM est remis à zéro, les ressources sont engagées. Il convient que l'INA ne refuse pas les ressources demandées si ces dernières sont dans l'enveloppe réservée. Le CM avertit le MTA du résultat de la demande de ressources avec la primitive MAC_CONNECT_IND ou une primitive MAC_RSV_ID_IND. Le processus d'engagement de ressources est illustré à la Figure A.2:

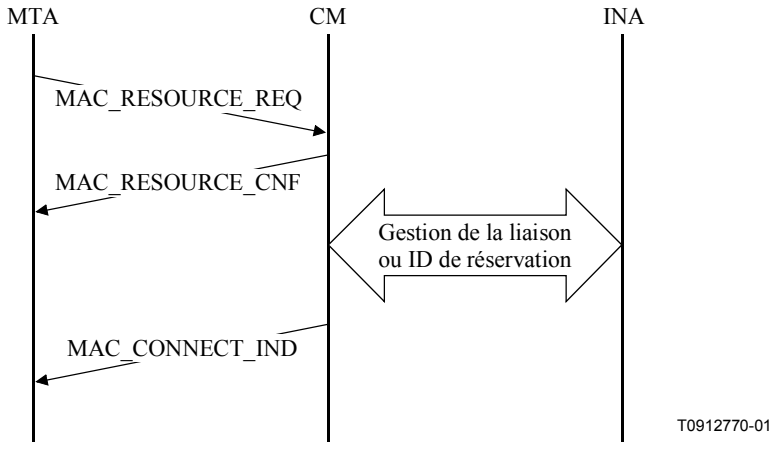


Figure A.2/J.163 – Engagement de ressources en utilisant les primitives MAC

A.3.3 Libération de ressources

Le MTA initie la libération de ressources de QS en utilisant la primitive MAC_RESOURCE_REQ avec le paramètre Resource_Type réglé à 16. Le MTA doit inclure l'ID de porte comme ID de connexion. Pour une description plus détaillée des paramètres de la primitive MAC_RESOURCE_REQ se reporter à l'Annexe A/J.112. Si le CM reçoit ce message il invoque la signalisation MAC amenant à la suppression de la connexion et ainsi à la libération des ressources allouées à cette connexion. Il confirme la réception de la primitive en répondant avec une primitive MAC_RESOURCE_CNF. Le CM avertit le MTA du résultat de la demande de ressources avec la primitive MAC_RELEASE_IND. Le processus de libération de ressources est illustré dans la Figure A.3:

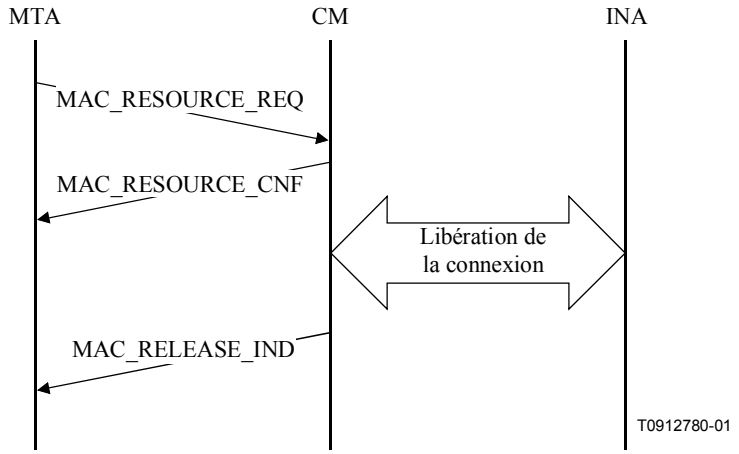


Figure A.3/J.163 – Libération de ressources utilisant les primitives MAC

A.4 Prise en charge de l'allocation de ressources en deux phases

Pour un service de communications vocales voué à un déploiement commercial, il est essentiel de pouvoir distinguer entre les ressources qui sont réservées pour une session et les ressources qui sont engagées pour cette session. La raison en est, d'une part, de garantir que toutes les ressources sont disponibles avant que les parties de la communication soient averties qu'ils peuvent commencer leur conversation. D'autre part, une allocation de ressources en deux phases garantit que l'enregistrement et la facturation ne seront pas commencés tant que le média (c'est-à-dire la voix) n'a pas traversé. Le présent paragraphe décrit le support de réseau J.112 pour ce mécanisme d'allocation de ressources.

Un flux J.112 possède trois ensemble de paramètres de QS associés. Les paramètres autorisés réglés sont définis par la politique du réseau et/ou le fournisseur de services et donnent la quantité de ressources maximales qu'il est possible d'accorder à une session particulière. Sur demande, des ressources sont réservées. Pour engager ces ressources, une seconde demande explicite doit être soumise par les deux parties.

Les deux types de demande, l'opération Reserve et l'opération Commit, sont effectuées par l'utilisation de messages MAC J.112 envoyés par le CM. L'opération Reserve est exécutée en établissant une nouvelle connexion. L'allocation et la réservation des ressources ont lieu dans l'INA. L'opération Commit utilise le mécanisme de demande de ressources pour une connexion existante établie dans le protocole MAC J.112. Les échanges de messages comprenant les opérations Reserve et Commit sont illustrés dans la Figure A.4:

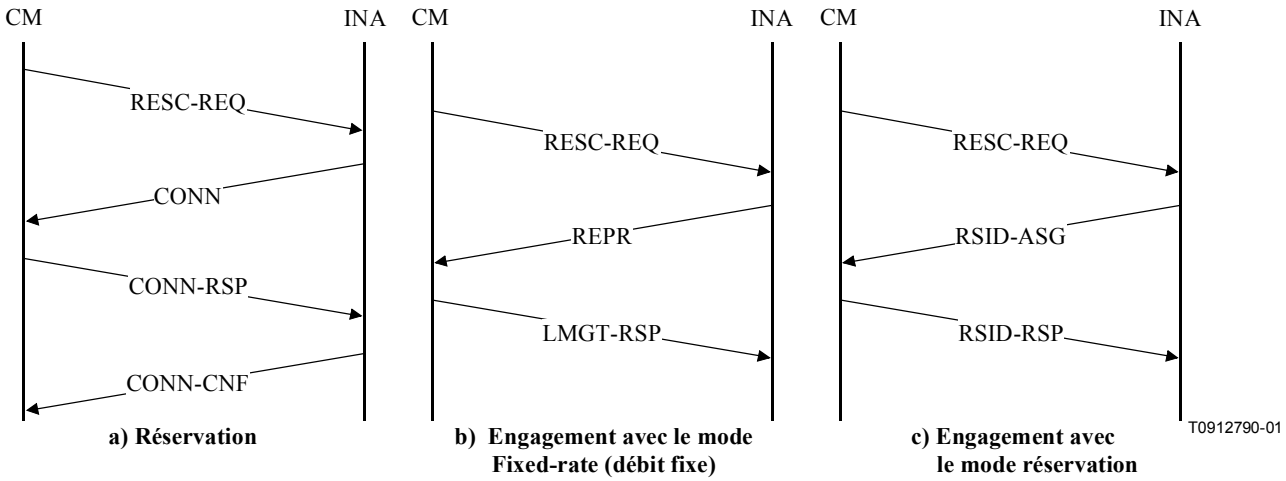


Figure A.4/J.163 – Opération Reserve et Commit utilisant les échanges de messages MC de l'Annexe A/J.112

A titre d'exemple, le message RESC-REQ suivant amène l'INA à établir une connexion et à réserver des ressources en amont en aval du réseau J.112. Sa réponse est le message CONN indiqué ci-dessous:

RESC-REQ (message de demande de ressources)	
Resource Request ID (ID de demande de ressources)	**0x01**
Connection ID (ID de connexion)	**Gate ID (ID de porte)**
Field (Champ)	
Aux_control_field_included	1
Admit_flag	1
Priority_included	0
Max_packet_size_included	1
Session_binding_US_included	0
Release_requested	0
Reservation_ID_requested	0
Cyclic_assignment_needed	1
Requested_bandwidth	240
Maximum_distance_between_slots	60
Encapsulation	DirectIP (1)
Aux_control_field	
IPv6_add	0
Flowspec_DS_included	1
Session_binding_DS_included	0
Frame_length	2
Flowspec_DS	
Max_packet_size	55
Average_bitrate	5632
Jitter	0

RESC-REQ (message de demande de ressources)	
CONN (Message de connexion)	
Connection ID (ID de connexion)	**ID de porte**
Session_number	**ne pas tenir compte**
Connection_Control_Field_Aux	
Connection_control_field2_included	1
IPv6_add	0
Priority_included	0
Flowspec_DS_included	0
Session_binding_US_included	0
Session_binding_DS_included	0
Encapsulation_included	1
DS_multiprotocol_CBD_included	0
Resource_number	**0x01**
Connection_Control_Field	
DS_ATM_CBD_included	0
DS_MPEG_CBD_included	1
US_ATM_CBD_included	1
Upstream_Channel_Number	0x1
Slot_list_included	0
Cyclic_assignment	0
Frame_Length	**0**
Maximum_Contention_Access_Message_Length	**1**
Maximum_Reservation_Access_Message_Length	**50**
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000
Program_Number	0xA437

Upstream_ATM_CBD	
Upstream_Frequency	20 000 000
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Connection_control_field2	
Upstream_modulation_included	1
Upstream_Modulation	QPSK (1)

En supposant que la source de média affiche un comportement de type CBR, le MTA demandera selon toute vraisemblance une connexion en mode d'accès à débit fixe avec l'INA en ayant précédemment réservé les ressources appropriées. Dans ce cas, l'échange suivant d'un message RESC-REQ et REPR se produira entre le CM et l'INA pour engager les ressources.

RESC-REQ (message de demande de ressources)	
Resource Request ID (ID de demande de ressources)	**0x02**
Connection ID (ID de connexion)	**Gate ID (ID de porte)**
Field (Champ)	
Aux_control_field_included	1
Admit_flag	0
Priority_included	0
Max_packet_size_included	1
Session_binding_US_included	0
Release_requested	0
Reservation_ID_requested	0
Cyclic_assignment_needed	1
Requested_bandwidth	240
Maximum_distance_between_slots	60
Encapsulation	DirectIP (1)
Aux_control_field	
IPv6_add	0
Flowspec_DS_included	1
Session_binding_DS_included	0
Frame_length	2
Flowspec_DS	
Max_packet_size	55
Average_bitrate	5632
Jitter	0

REPR (Message de réapprovisionnement)	
Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0
Delete_Reservation_Ids	0
New_Downstream_IB_Frequency_included	0
New_Downstream_OOB_Frequency_included	0
New_Upstream_Frequency_included	0
New_Frame_Length_included	1
New_Cyclical_Assignment_included	1
New_Slot_List_included	0

New_Frame_Length	**2**
Number_of_Connections	**1**
Connection_ID	**Gate ID (ID de porte)**
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_End	0xFFFF

A.5 Mise à jour de la réservation

Fait l'objet d'un complément d'étude.

ANNEXE B

Exigences supplémentaires pour les implémentations de l'Annexe B et de l'Annexe C

Plutôt qu'utiliser l'interface pkt-q3 comme indiqué à l'article 6, un MTA intégré PEUT réserver dynamiquement des ressources locales de QS en utilisant uniquement les mécanismes définis dans UIT-T J.112. En utilisant cette autre approche, un MTA intégré signale directement pour la QS du réseau d'accès local en utilisant l'interface de service de contrôle MAC définie à l'Annexe E de l'Annexe B/J.112. Contrairement au § 6, la signalisation de la QS à travers l'interface J.112 (interface pkt-q2) est initiée par le CM au lieu de l'AN. Toutes les autres interfaces restent inchangées. Les Appendices VII et VIII fournissent un exemple illustrant cette approche.

Un MTA intégré signale ses exigences de QS de niveau de session dans les protocoles de signalisation (SIP IETF RFC 2543 et UIT-T J.162). Une fois que le MTA intégré détermine que les ressources de QS ont besoin d'être réservées ou engagées, le MTA DOIT initier la signalisation de flux de service dynamique J.112 pour amener la création, le changement et/ou la suppression du ou des flux de service et l'allocation des ressources J.112. 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 au MAC J.112 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 de J.112. Les paragraphes qui suivent étudient le mappage par MTA des exigences de QS de niveau de session avec celles de J.112, la prise en charge de J.112 pour la réservation/l'engagement en deux phases et l'utilisation de l'interface de service de contrôle MAC J.112.

B.1 Mappage des Flowspec avec les paramètres de QS de J.112

D'autres spécifications (par exemple la spécification de CODEC IPCablecom J.161) contiennent les exigences de mappage des descriptions de service de la couche supérieure (par exemple SDP tel qu'il est utilisé dans les applications VoIp) en Flowspec. Le présent paragraphe spécifie comment le MTA DOIT mapper les Flowspec avec les paramètres de la couche 2 J.112. La présente Recommandation suppose que le protocole de transport utilisé est UDP. Si un protocole de transport différent est utilisé, les changements appropriés seraient applicables aux classificateurs et pour l'en-tête de suppression du payload.

L'UIT-T J.112 définit un ensemble de paramètres de QS riche, qui en général peut être appliqué au flux de service amont et aval. Un codage de flux de service définit le contenu de l'ensemble de paramètres de la QS Provisioned (fourni), Admitted (admis) ou Active (actif) pour un flux de service. Chaque ensemble se compose de plusieurs paramètres de QS qui définissent les attributs individuels du flux de service.

Le MTA DOIT spécifier:

- quel service J.112 utiliser (par exemple, attribution non demandée, interrogation en temps réel, etc.);
- quels paramètres de QS associer au flux de service correspondant.

Le choix de la classe de service affectera le temps d'attente et l'efficacité. Un service d'attribution non sollicitée introduira un temps d'attente qui ne sera pas supérieur au temps entre les attributions. Un service d'interrogation a la possibilité d'introduire un temps d'attente plus grand puisque le CM attend qu'un cycle d'interrogation puis qu'une attribution soient effectués.

Pour décider d'utiliser le mécanisme d'attribution non sollicitée ou le mécanisme d'interrogation en temps réel, le MTA DOIT utiliser les informations de politique et les caractéristiques de la source telles qu'elles sont indiquées dans les exigences de QS pour la session. En général, il est logique

d'utiliser les attributions non sollicitées uniquement si la source montre des caractéristiques de type CBR avec une taille de paquet fixe tous les intervalles de temps fixes.

Pour UGS, l'intervalle d'attribution peut être réglé selon le temps de formation du paquet, bien que des valeurs différentes puissent être utilisées en fonction de l'exigence de temps d'attente et de gigue.

Par exemple, considérons une application VoIP qui utilise G.729 Annexe E et le SDP suivant:

c = IN IP4 10.1.1.10

m = audio 3456 RTP/AVP 96

a = rtpmap: 96 G729E/8000

a = ptime: 10

où le rtpmap spécifie les paramètres du codec et ptime spécifie le temps de formation de paquet de 10 ms. Ces valeurs peuvent être mappées avec les paramètres du flux de service amont de la QS (QoS Upstream Service Flow) tels que:

– service d'attribution non sollicitée;
– taille de l'attribution de 86 octets (55 octets pour le paquet IP, donné par le Flowspec et 31 octets du préfixe de la couche MAC J.112);
– intervalle d'attribution de 10 ms.

La taille du PDU amont DOIT prendre en compte le préfixe Ethernet (18 octets) ainsi que tout préfixe J.112 (généralement 6-13 octets). L'en-tête de suppression de la charge utile a la possibilité de réduire la taille de PDU d'un maximum de 42 octets, en fonction de l'utilisation du total de contrôle UDP et du champ IP Ident auquel sont ajoutés deux octets d'en-tête étendu J.112 donnant la valeur de l'indice PHS.

Si le total de contrôle UDP (*UDP checksum*) n'est pas utilisé et que le champ IP Ident doit être supprimé – 40 octets sont soustraits de la taille de PDU.

Si UDP checksum est utilisé et le champ IP Ident doit être supprimé – 38 octets sont soustraits de la taille de PDU.

Si UDP checksum n'est pas utilisé et le champ IP Ident ne peut pas être supprimé – 36 octets sont soustraits de la taille de PDU.

Si UDP checksum est utilisé et le champ IP Ident ne peut pas être supprimé – 34 octets sont soustraits de la taille de PDU.

Le classificateur amont DOIT être réglé comme suit. L'adresse source (*Source Address*) est l'adresse IP MTA IP. Le port source (*Source Port*) est le numéro de port sur lequel le MTA enverra le débit voix. L'adresse de destination est l'adresse IP de destination obtenue de c = ligne de la description de l'extrémité distante. Le port de destination est le numéro de port obtenu de m = ligne de la description de l'extrémité SDP distante. Le type de protocole est UDP.

Le classificateur aval DOIT être réglé comme suit. L'adresse source est l'adresse IP du MT distant, obtenu de c = ligne de la description de l'extrémité SDP distante. Le port source n'est pas disponible dans la description de SDP et il convient qu'il ne soit pas spécifié comme partie du classificateur. L'adresse de destination est l'adresse IP du MTA. Le port de destination est le port local sur lequel le MTA a indiqué qu'il recevra les paquets de données voix. Le type de protocole est UDP.

Le masque PHS amont (*Upstream PHS Mask*) DOIT être réglé comme une chaîne de bits, un bit par octet par le paquet, avec le premier bit correspondant au premier octet de l'en-tête Ethernet. Il convient que tous les bits soient mis à 1, à l'exception des bits correspondant aux champs IP Ident, IP checksum et UDP checksum, si ces champs ne peuvent pas être supprimés.

Le champ Upstream PHS DOIT être réglé selon la chaîne d'octets que l'AN va restaurer au début de chaque paquet, se composant de la valeur de l'en-tête Ethernet, l'en-tête IP et l'en-tête UDP. Les

octets de IP Ident, IP checksum et UDP checksum DOIVENT être sautés dans le champ PHS Field s'ils ne sont pas en cours de suppression.

Il convient que Downstream PHS Size soit réglé à 32 octets. Cette valeur inclut le SA et le type de l'en-tête Ethernet (8 octets), l'en-tête IP complète (20 octets) et la longueur de paquet UDP et le port de destination (4 octets). Le port source UDP, le total de contrôle et l'adresse de destination de l'en-tête Ethernet ne sont pas supprimés.

Il convient que le champ Downstream PHS Mask soit réglé à 0xFFFFFFFF, indiquant que tous les octets énumérés ci-dessus, démarrant après le Ethernet DA, sont supprimés.

Le champ Downstream PHS DOIT être réglé selon la chaîne d'octets que le CM va restaurer au début de chaque paquet, se composant de la valeur de l'adresse source de l'Ethernet (PEUT être réglé à l'adresse de l'AN ou peut être réglé à toute autre valeur convenant au MTA), l'en-tête IP, la longueur du paquet UDP et la valeur du port de destination.

B.2 Prise en charge de J.112 pour la réservation de ressources

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

Le modèle QS dynamique est un modèle dans lequel chaque session est autorisée. L'autorisation de chaque session utilise un identificateur donné à l'AN et au MTA, qui est utilisé pour mettre en correspondance les demandes et les autorisations. Cet identificateur est l'identification de port (Gate-ID). A la réception d'une information d'appel de signalisation, le MTA transmet l'ID de porte à l'AN en utilisant le AuthBlock TLV contenu dans un message DSA/DSC.

L'Appendice VII donne un exemple de l'utilisation du bloc d'autorisation en tant que partie des messages DSA-REQ.

B.2.1 Réservation/engagement en deux phases

Un flux de service a trois ensembles de paramètres de qualité de service associés, désignés sous la forme d'ensembles de paramètres de QS fournis (*Provisioned*), admis (*Admitted*), actifs (*Active*). La relation entre ces ensembles est identique à la description des ressources autorisées (*Authorized*), réservées (*Reserved*) et engagées (*Committed*) donnée au § 5.7.4. De plus, la possibilité de prendre en charge des Admitted QoSParameterSet multiples pour un flux de service unique est une option spécifique au constructeur dans UIT-T J.112.

Les opérations Reserve et Commit sont toutes deux exécutées en utilisant des messages Dynamic Service J.112, en changeant les valeurs du AdmittedQoSParameterSet et du ActiveQoSParameterSet du flux de service. Dans un message addition de service dynamique (DSA, *dynamic service addition*) ou change de service dynamique (DSC, *dynamic service change*), l'opération Reserve est accomplie en incluant, dans les codages de flux de service amont ou les codages de flux de service aval, le QoSParameterSetType TLV avec la value réglée à Admitted (valeur 2). De façon similaire, l'opération Commit est accomplie en réglant le QoSParameterSetType TLV à Active (valeur 4) ou à Admitted+Active (valeur 6).

Les échanges de DSA et DSC entre le CM et AN sont des messages d'établissement de liaison à 3 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 B.1.

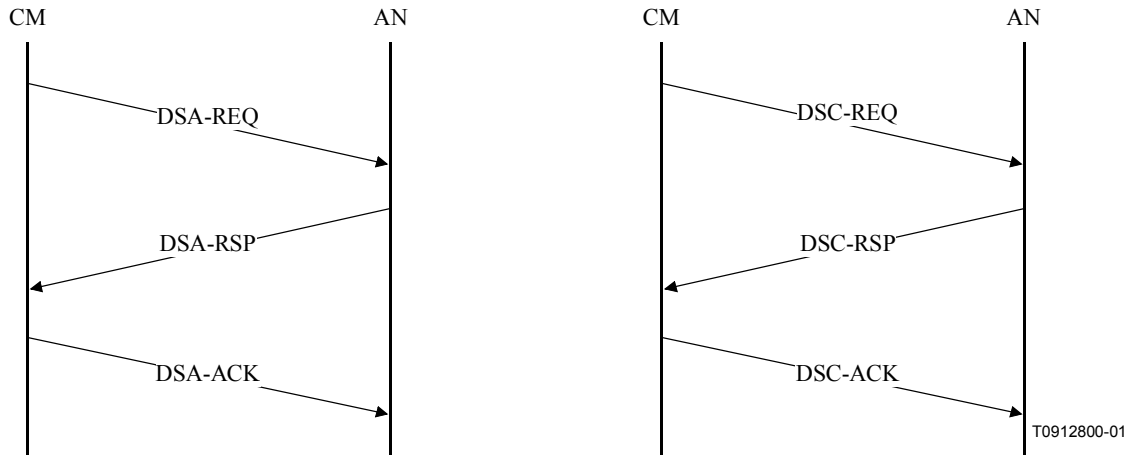


Figure B.1/J.163 – Echanges de DSA et DSC entre CM et AN

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 J.112 sont réservées.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Admitted (2) (admis)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	222
DownstreamServiceFlow	ServiceFlowReference	2
	QoSParameterSetType	Admitted (2) (admis)
	TrafficPriority	3
	MaximumSustainedRate	12 000

A titre d'exemple supplémentaire, le message DSC-REQ suivant provoque l'activation du flux de service, ce qui signifie que les ressources de QS utilisées dans un réseau J.112 sont engagées.

DSC-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowID	10 288
	QoSParameterSetType	Admis + Actif (6)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	222

DSC-REQ

DownstreamServiceFlow	ServiceFlowID	10 289
	QoSParameterSetType	Admis + Actif (6)
	TrafficPriority	3
	MaximumSustainedRate	12 000

Des paramètres tels que ToleratedGrantJitter et TrafficPriority PEUVENT être fournis par l'approvisionnement ou PEUVENT être déterminés par l'implémentation du MTA. Il est prévu que les valeurs proposées par le MTA soient remplacées par les valeurs de la politique dans l'AN.

La spécification des 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 classificateurs associés. Voir l'Appendice VII pour des exemples supplémentaires.

B.2.2 Réservation avec spécifications de flux de service multiples

Il existe diverses situations dans lesquelles une réservation a besoin de couvrir une plage d'applications possibles. Par exemple, certaines applications désirent créer une réservation qui peut traiter la commutation entre une spécification de flux et une autre à mi-session sans avoir à passer par le contrôle d'admission à chaque temps de commutation. Afin que le ActiveQoSParameterSet d'un flux de service varie pendant une session, un AuthorizedQoSParameterSet a besoin d'être spécifié par des politiques au niveau du contrôleur de porte.

Conformément à UIT-T J.112, il est éventuellement possible (option du constructeur) d'avoir plus qu'un seul ensemble de paramètres de QS Admis (Admitted set of QoSParameters). Par exemple:

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Admitted (2) (admis)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	111
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Admitted (2) (admis)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	20 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	444

Ceci amène l'AN à réserver des ressources telles que l'un ou l'autre des flux décrits puisse être ensuite activé et que l'AN ne puisse pas renvoyer une erreur pour "ressources insuffisantes" à la tentative d'activation. Toutefois, l'AN peut rejeter une telle demande de réservation avec un 2-reject-unrecognized-configuration-setting. Dans ce cas, le MTA DOIT utiliser une approche de borne supérieure pour la réservation de ressources.

La borne supérieure de deux ensembles de paramètres est formée en prenant, pour chaque dimension de la réservation de ressources, la ressource maximale requise par toute spécification de flux individuelle. Ceci produit habituellement une surestimation des ressources qui seront requises par le MTA, mais constitue la meilleure solution qui puisse être effectuée dans les installations disponibles.

En utilisant les deux spécifications de service de l'exemple ci-dessus, un message DSC-REQ indiquant que les ressources sont réservées pour les deux flux mais qu'elles sont engagées uniquement pour le premier serait:

DSC-REQ

TransactionID		1
Upstream Service Flow	ServiceFlowID	10 288
	QoSParameterSetType	Admitted (2) (admis)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	444
UpstreamServiceFlow	ServiceFlowID	10288
	QoSParameterSetType	Active (4) (actif)
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	UnsolicitedGrantSize	111

Dans la première spécification UpstreamServiceFlow, le NominalGrantInterval a été donné égal à 10 ms, le plus grand commun diviseur des deux spécifications de ressources séparées et UnsolicitedGrantSize a été donné comme étant égal à 444 octets, le maximum des deux spécifications.

B.2.3 Mise à jour de la réservation

Alors que le protocole RSVP a un modèle d'état souple tel que décrit au § 6.5.4, UIT-T J.112 fournit uniquement un mécanisme de temporisation à travers l'interface J.112. Les paramètres du flux de service de QS "Timeout for Active QoS Parameters" et "Timeout for Admitted QoS Parameters" permettent à une session d'être terminée et ses ressources libérées en raison de l'inactivité.

Les paramètres TimeoutForActiveQoSParameters sont conçus pour récupérer les ressources allouées aux CM qui subissent une défaillance ou qui sinon 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 MTA effectue une détection d'activité vocale (VDA, *voice activity detection*), en utilisant un type de programmation de flux de service de UGS/AD, alors pendant les périodes de silence étendues le MTA DOIT effectuer une opération DSC-REQ pour réinitialiser le temporisateur ou DOIT envoyer des paquets de données périodiques sur le flux de service. Comme alternative, le MTA PEUT régler ce temporisateur à une valeur zéro (c'est-à-dire pas de vérification) s'il utilise la VAD.

Lorsqu'une session est terminée, l'AN envoie un message Gate-Close, avec le code d'erreur approprié, tel que décrit au § 8.2.

Le TimeoutForAdmittedQoSParameters est conçu pour récupérer les ressources qui sont réservées par un CM mais non engagées. Dans des cas typiques, les paramètres engagés seront identiques aux paramètres réservés et cela ne posera pas de problème. Lorsque la réservation inclut des spécifications de flux de service multiple, tel que décrit en B.2.2, ou lorsque l'engagement est inférieur à la réservation, il est nécessaire de réinitialiser périodiquement le temporisateur de l'AN. Cette opération est accomplie en effectuant une opération DSC-REQ qui réserve les mêmes ressources que les précédentes.

B.2.4 Prise en charge de l'association dynamique de ressources

L'association dynamique de ressources, requise au § 5.7.7 et décrite au § 6.1.4, est accomplie dans UIT-T J.112 par l'utilisation de messages Dynamic-Service-Change sur un flux de service établi, changeant les classificateurs associés au flux de service.

B.2.5 Mappage de paramètres de la QS pour l'autorisation

La porte identifiée par la GateID est paramétrée par des objets RSVP (FlowSpec). Le module d'autorisation dans l'AN DOIT convertir le paramètre Gate en paramètres de QS J.112 en utilisant les règles définies aux § B.3.4 et 7.1. Les objets de QS convertis résultants DOIVENT être ensuite vérifiés par rapport aux enveloppes de QS correspondantes de flux de service.

Par exemple, si l'autorisation amont est donnée sous la forme:

Profondeur du bucket (b) = 120 octets

Débit du bucket (r) = 12 000 octets/s

Débit pic (p) = 12 000 octets/s

Unité régulée min (m) = 120 octets

Taille maximale du datagramme (M) = 120 octets

L'autorisation sera convertie en paramètres de QS J.112:

Scheduling: UGS

Nominal Grant Interval (intervalle d'attribution nominal): 10 ms

Tolerated Grant Jitter (gigue d'attribution tolérée): 5 ms

Unsolicited Grant Size (taille de l'attribution non sollicitée): 151 Octets

Ces objets J.112 convertis seront vérifiés par rapport à l'enveloppe de ressources du flux de service correspondant.

B.2.6 Ressources engagées automatiquement

Si la porte individuelle a été marquée avec le drapeau "auto-commit" (voir § 7.3.2.5) alors les ressources réservées sont immédiatement activées, mais l'état de la porte est inchangé.

Dans le cas d'un MTA intégré non RSVP, où la réservation de ressources est initiée par le MTA avec un DSA-REQ J.112, l'AN DOIT initier un échange de DSC-REQ J.112 avec le MTA à la fin de l'établissement des réservations, avec un QoSParameterSetType de Admitted+Active (valeur 6) pour le flux de service engagé. Voir l'Appendice VIII pour obtenir un exemple.

B.3 Utilisation de l'interface de service de contrôle MAC J.112

Les paramètres de QS J.112 pour le flux de service dérivé 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 J.112 (Annexe E de l'Annexe B/J.112).

Au niveau des primitives de l'interface de service de contrôle MAC J.112, le MTA intégré signale pour les ressources de QS comme suit:

1) demande MAC_CREATE_SERVICE_FLOW:

   tel que décrit dans 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 classificateurs pour le nouveau flux de service, mais également pour fournir les Admitted et Active QoS Parameter Sets (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 initier 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 placé en instance. 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 CM 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 tel que donné dans l'Appendice B.II/J.112.

B.3.1 Etablissement de la réservation

Le MTA initie 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 bloc d'autorisation TLV. A la réception de ce message, la couche MAC du CM invoque la signalisation DSA en envoyant un DSA_REQ à l'AN. L'AN DOIT vérifier l'autorisation basée sur l'ID de porte (contenue dans le bloc d'autorisation TLV) et rejeter la demande si la porte est non valide ou si les ressources autorisées sont insuffisantes pour la demande. A la réception du DSA_RSP de l'AN, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_CREATE_SERVICE_FLOW. Ceci est illustré dans la Figure B.1.

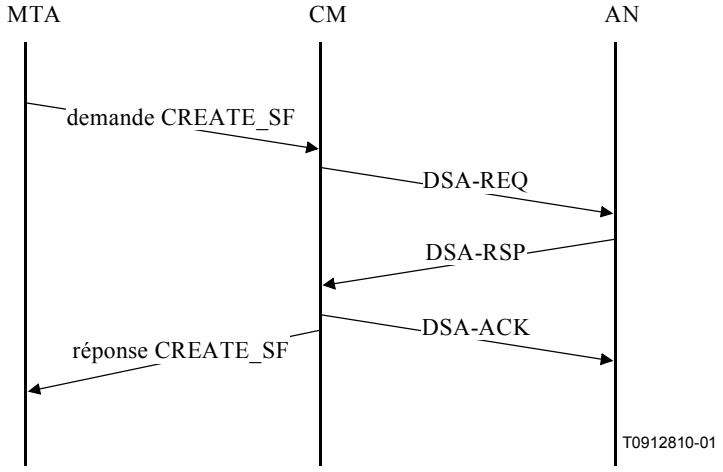


Figure B.1/J.163 – Etablissement de la réservation

B.3.2 Changement de réservation

Le MTA initie les changements dans les ressources de QS en utilisant la primitive de demande MAC_CHANGE_SERVICE_FLOW. Ceci est illustré dans la Figure B.2

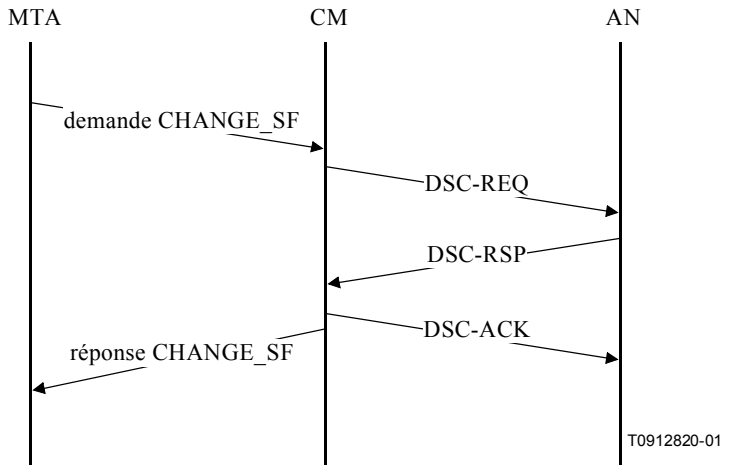


Figure B.2/J.163 – Changement de réservation

A la réception de ce message, la couche MAC du CM invoque la signalisation DSC. A la réception du DSC_RSP depuis l'AN, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_CHANGE_SERVICE_FLOW.

B.3.3 Suppression de la réservation

Le MTA initie la suppression de l'allocation de la réservation de la QS en utilisant la primitive de demande MAC_DELETE_SERVICE_FLOW. A la réception de ce message, la couche MAC invoque la signalisation DSD. En recevant le DSD_RSP de l'AN, le service MAC notifie la couche supérieure en utilisant le message de réponse MAC_DELETE_SERVICE_FLOW. Ceci est illustré dans la Figure B.3.

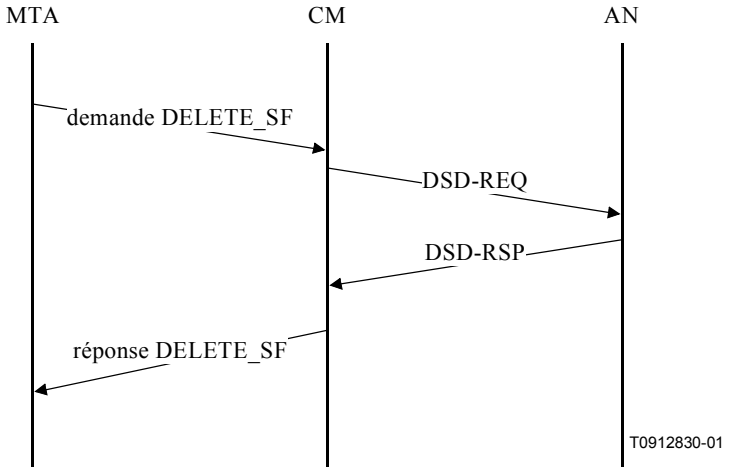


Figure B.3/J.163 – Suppression de la réservation

B.3.4 Mappage des Flowspecs du protocole RSVP avec les paramètres de QS J.112

L'AN, à la réception d'une demande de réservation, décide des points suivants:

- quel type de service J.112 utiliser (par exemple, attribution non sollicitée (*unsolicited grant*), interrogation en temps réel (*real-time polled*), etc.);
- quels paramètres de QS associer au flux de service correspondant.

Le choix de la classe de service affectera le temps d'attente et l'efficacité. Une attribution de service non demandée introduira un temps d'attente supplémentaire non supérieur au temps entre les attributions. Un service interrogé a la possibilité d'introduire un temps d'attente plus grand, étant donné que le CM attend un cycle d'interrogation puis qu'une attribution soit effectuée.

Pour décider d'utiliser le mécanisme d'attribution non sollicitée ou le mécanisme d'interrogation en temps réel, l'AN PEUT utiliser les informations de politique et les caractéristiques de la source telles que décrites dans le Tspec. En général, il est logique d'utiliser les attributions non sollicitées uniquement si la source montre des caractéristiques de type CBR avec une taille de paquet fixe tous les intervalles de temps fixes. Une telle source CBR source pourrait être identifiée en ayant un débit pic (p) quasiment égal au débit moyen (r) dans le Sender-Tspec et une taille de rafale (b) égale à la taille maximale de paquet (M). Les informations de politique pourraient être utilisées pour déterminer de combien p est proche de r et b de M, avant qu'un mode d'attribution non sollicité soit utilisé.

Pour les sources du type VBR par rafale, les nombreuses rafales de la source amèneraient un débit pic (p) "average rate (r) and b" M dans le Tspec et il convient alors qu'un mode d'interrogation en temps réel soit utilisé.

Pour les sources VoIP sources décrites dans la présente Recommandation, avec p = r et M = b, il convient qu'un service d'attribution non sollicitée soit utilisé.

Une fois que l'AN a recueilli un mécanisme de programmation, il PEUT fournir des informations à son voisin RSVP sous la forme d'un AdSpec. Le AdSpec permet à l'AN de faire connaître à quel point son comportement dévie de l'"idéal", c'est-à-dire, la valeur du délai supplémentaire qu'il peut introduire. Ce délai comporte deux parties:

- une composante fixe, par exemple, délai qui pourrait être introduit pendant le traitement de la mise à jour d'un routage, temps de propagation, etc. (représentés par D dans la formule de délai ci-dessus);
- une composante dépendant du débit, par exemple, en raison de l'intervalle entre les attributions, qui diminue lorsque le débit de la réservation augmente (représentée par C dans la formule ci-dessus).

L'AN PEUT déterminer les deux composantes de délai selon qu'il a choisi un service d'attribution interrogée ou non sollicitée donné dans le Sender-Tspec. Dans le cas d'une composante dépendant du débit, l'AN utilise la taille maximale du datagramme (M) et le débit réservé (r) pour déterminer C. Par exemple, si un AN installe une réservation de débit R octets/s, il pourrait effectuer une attribution non sollicitée de taille M octets toutes les M/R secondes. Ainsi, la valeur communiquée de C serait M. En utilisant un service interrogé en temps réel, l'AN DOIT déterminer combien de temps pourrait prendre un paquet mis en file d'attente au niveau du CM pour recevoir une attribution étant donné l'intervalle d'interrogation qui sera utilisé, les temps de transmission sur la liaison, etc. Ces facteurs peuvent avoir des composantes fixes et dépendant du débit, qu'il convient que l'AN fasse connaître en conséquence.

Pour régler l'intervalle d'attribution nominale, l'AN DOIT utiliser le paramètre débit du Rspec (R) et la taille maximale du datagramme M. Tel que noté ci-dessus, un intervalle d'attribution de M/R fournira le débit de réservation appropriée. Toutefois, si le terme de latitude (*slack term*) permet d'introduire un délai supplémentaire, l'AN PEUT offrir des attributions plus importantes moins fréquemment, par exemple, une attribution de 2 Mo toutes les 2M/R secondes.

Pour le service d'attribution non sollicitée, l'AN DOIT utiliser la "taille maximale du datagramme (M)" du Tspec en octets pour calculer la taille de l'attribution non sollicitée (*unsolicited grant size*) en mini-intervalles (après avoir calculé le préfixe au niveau de la liaison) pour le canal amont sur lequel le client demandeur se trouve.

L'autre paramètre clé qu'il est nécessaire pour un flux de service UGS de connaître est la gigue d'attribution tolérée (*tolerated grant jitter*). Un client qui a besoin d'une gigue moins stricte PEUT prendre une valeur non nulle pour le terme de latitude S, ce qui donne à l'AN toute latitude pour augmenter au besoin la gigue. Un exemple de calcul de gigue est donné au § B.3.4.1.

Pour le service interrogé en temps réel, l'intervalle d'interrogation PEUT être une fonction du débit, ou PEUT être fixe. Par exemple, un intervalle d'interrogation de M/R permettrait au CM d'envoyer un paquet de taille maximale à chaque intervalle d'interrogation pour soutenir son débit moyen. Des intervalles d'interrogation plus longs ou plus courts PEUVENT être utilisés mais affecteront le délai total.

L'AdSpec PEUT être utilisé pour transporter des informations sur le délai de codage introduit par le codec de l'émetteur. Ceci serait inclus dans le terme D et l'AN DOIT ajouter ses propres composantes de délai à l'AdSpec en calculant la tolérance pour la gigue augmentée.

L'AN utilise l'objet Session et Sender Template pour générer le classificateur amont et utilise l'objet Reverse Session et Reverse Sender Template pour générer le classificateur aval.

B.3.4.1 Exemple de mappage

Considérons l'exemple suivant. Un codec voix produit un flux de données de sortie de 64 kbit/s qui est paquétisé à intervalle de 10 ms, produisant ainsi une charge utile de 80 octets toutes les 10 ms. La charge utile est encapsulée en utilisant RTP/UDP/IP, 40 octets supplémentaires, produisant un paquet de 120 octets toutes les 10 ms. Le Tspec dans ce cas est:

profondeur du bucket (b) = 120 octets

débit du bucket (r) = 12 000 octets/s

débit pic (p) = 12 000 octets/s

unité régulée min (m) = 120 octets

taille maximale du datagramme (M) = 120 octets

Supposons qu'un client demande une réservation en utilisant ce Tspec et un Rspec avec R = r. Un AN recevant cette demande établira un flux de service qui utilise un service d'attribution non sollicitée parce que p = r et M = b, indiquant un flux CBR. Il peut utiliser une taille de l'attribution de M octets selon un intervalle de M/R = 10 ms.

Pour le calcul de la gigue, le MTA ne sait pas de combien l'AN dévie de l'idéal dans son comportement de programmation. Le client devrait supposer que le niveau de l'AN est idéal, ce qui signifie que le délai qu'il subira avec Tspec ci-dessus et son débit R = r réservé est simplement:

b/r + temps de transmission

En ignorant ce temps de transmission, un délai de 10 ms est obtenu. Supposons que le client souhaite tolérer un délai de 15 ms pour cette session (sur le chemin AN du client-AN uniquement). Il réglerait alors son terme de latitude (S) à 15−10 = 5 ms. A la réception de la réservation, l'AN interprète cela comme une indication qu'une gigue d'attribution de 5 ms est acceptable pour le client.

Supposons que le client souhaite tolérer un délai de 25 ms et règle son terme de latitude à 25 − 10 = 15 ms. L'AN peut utiliser cette information pour déterminer qu'il peut utiliser un intervalle d'attribution plus long, par exemple, 20 ms, étant donné que cela augmente potentiellement le délai jusqu'à 20 ms pour un paquet qui arrive au CM juste après une attribution. Il existe encore une marge de 5 ms de libre que l'AN peut utiliser pour régler la gigue de l'attribution.

Il est à noter que cette approche laisse une souplesse considérable dans l'AN pour répondre aux exigences du client concernant le délai d'une façon qui réponde le mieux aux capacités de l'AN.

B.3.4.2 En-tête de suppression de payload et VAD

Si l'AN et le CM effectuent la suppression d'en-tête, alors la bande passante qui est nécessaire sur un flux de service peut être réduite. Le client DOIT transmettre à l'AN le fait que la suppression puisse être appliquée avant l'installation d'une réservation pour garantir que la bande passante appropriée est réservée. La solution générale de ce problème est décrite dans draft-davie-intserv-compress-00. L'émetteur (client) ajoute un paramètre (Compression_Hint), décrit dans *Integrated Services in the Presence of Compressible Flows* (services intégrés en présence de flux compressibles), au Sender-Tspec qui identifie le type de compression ou de suppression d'en-tête qui pourrait être appliqué au données. Le paramètre Compression_Hint contient un champ Hint qui indique le ou les types de compressions possibles.

Un MTA qui désire que le CM effectue la suppression d'en-tête DOIT inclure le paramètre Compression_Hint, *Integrated Services in the Presence of Compressible Flows,* dans le Tspec. Le champ Compression Factor (facteur de compression), un pourcentage sur la plage 1 à 100 inclus, DOIT être réglé à une valeur qui produise des économies de bande passante lorsque PHS (42 octets) est utilisé. La valeur pour le facteur de compression varie relativement au profil de trafic du CODEC. Le Hint DOIT être réglé à l'une des valeurs suivantes en fonction du ou des types de compression/suppression que le MTA désire:

0x????0001 Ne pas supprimer UDP checksum (total de contrôle UDP) ET ne pas supprimer le champ IP-Ident ni le champ IP-Checksum.

0x????0002 Ne pas supprimer UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

0x????0003 Supprimer UDP checksum ET ne pas supprimer le champ IP-Ident ni le champ IP-Checksum.

0x????0004 Supprimer UDP checksum ET supprimer le champ IP-Ident et le champ IP-Checksum.

NOTE – ???? = Nombre à déterminer IANA pour IPCablecom.

Il est à noter que la suppression du champ IP Ident créera des problèmes si le paquet est ensuite fragmenté dans le réseau IP. Pour des paquets inférieurs à 576 octets en longueur (valeur par défaut Internet de MAX-MTU), il est raisonnable de supposer qu'aucune fragmentation ne se produira. Il convient que le MTA ne demande pas la suppression du champ IP-Ident s'il doit envoyer des paquets plus longs que 576 octets.

Un AN connecté à un CM qui est capable d'effectuer la suppression d'en-tête utilise le paramètre Compression_Hint [*Integrated Services in the Presence of Compressible Flows*] pour réduire le débit et la profondeur effectifs du "token bucket" fourni par l'émetteur. Si la suppression d'en-tête n'est pas prise en charge sur une liaison, le paramètre Compression_Hint est ignoré et le Tspec complet est utilisé.

En effectuant la suppression d'en-tête sur une liaison J.112, il est également nécessaire de communiquer le contenu de l'en-tête qui sera supprimé à l'AN avant la transmission du premier paquet de données de sorte que le contexte de la suppression peut être établi au niveau du CM et de l'AN. Toutes ces informations sont présentes dans le message RSVP qui est utilisé pour établir la réservation, y compris les adresses et les ports IP source et de destination. Etant donné que les messages PATH sont traités par tout saut intermédiaire entre le client et l'AN, un message PATH contiendra la même valeur TTL que les paquets de données, sous réserve que les messages PATH et les paquets de données aient le même TTL initial lorsqu'ils sont envoyés par le client. L'AN DOIT utiliser le contenu du PATH pour connaître les valeurs des champs qui seront supprimés. L'AN DOIT utiliser un échange de messages MAC J.112 pour informer le CM que cette suppression devrait être utilisée pour un flux particulier et lui indiquer de supprimer des champs appropriés étant donné la présence ou l'absence des UDP checksums (totaux de contrôle UDP) et des nombres IP Sequence.

Si le MTA initie un message PATH spécifiant un émetteur avec un caractère joker, alors aucun contenu du champ PHS peut être déterminé avec précision. L'AN DOIT spécifier la taille du PHS (PHS Size) de sorte que le CM puisse évaluer avec précision les besoins de ressource du flux de service.

La même approche de base permet la prise en charge de la détection d'activité vocale (VAD). Un AN PEUT utiliser différents algorithmes de programmation pour des flux qui utilisent la VAD et a ainsi besoin de connaître quels flux peuvent être traités avec la VAD. Le paramètre Compression_Hint transporté dans le Tspec DOIT contenir le bit indicateur pour indiquer que le flux de données pour lequel cette réservation est demandée PEUT être traité avec la VAD.

ANNEXE C

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 l'AN 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 à l'AN de récupérer les ressources de l'ID de porte lorsque le système de signalisation 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, l'AN DOIT considérer non valide l'ID de porte assignée.

La valeur recommandée de ce temporisateur est de 30 secondes.

Temporisateur T1

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

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

Ce temporisateur est remis à zéro chaque fois qu'une opération Commit est effectuée sur les ressources autorisées par la porte.

A l'expiration de ce temporisateur, l'AN DOIT révoquer toute réservation effectuée par le MTA qui a été autorisée par cette porte, libérer toutes les ressources réservées dans l'AN, envoyer un message GATE-CLOSE pour toute porte ouverte et signaler au CM via les messages MAC J.112 de libérer les ressources qu'il avait réservées.

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 réglée à zéro, alors le temporisateur T1 DOIT être réglé à une valeur par défaut à fournir. La valeur recommandée de cette valeur par défaut se situe sur la plage 200-300 secondes.

Temporisateur T2

Ce temporisateur est implémenté dans l'AN dans la machine d'état de porte et limite le temps dans les états transitoires de la coordination des portes. Ce temporisateur est suffisamment long pour prendre en charge la perte et la retransmission des messages de coordination de portes, mais est suffisamment court pour ne pas permettre un vol de service important.

Ce temporisateur est lancé lorsque l'AN reçoit un message COMMIT, ou lorsque l'AN reçoit un message GATE-OPEN.

Ce temporisateur est remis à zéro lorsque l'AN a reçu un message COMMIT et un message GATE-OPEN pour la porte.

A l'expiration de ce temporisateur, l'AN DOIT révoquer toute réservation effectuée par le MTA qui a été autorisée par cette porte, libérer toutes les ressources réservées dans l'AN, libérer toutes les ressources activées par l'AN et signaler le CM via les mécanismes de signalisation spécifique à la couche MAC J.112 pour libérer les ressources qu'il avait réservées ou activées, et utiliser GATE-CLOSE pour fermer toute porte ouverte.

Le temporisateur T2 DOIT être réglé à la valeur donnée dans le message GATE-SET. Si la valeur donnée dans le message GATE-SET est zéro, alors le temporisateur T2 DOIT être réglé à une valeur par défaut à fournir. La valeur recommandée de cette valeur par défaut est 2 secondes.

Temporisateur T3

Ce temporisateur est implémenté dans le MTA ou l'AN dans le traitement de réservations RSVP. Il contrôle le temps total qui peut s'écouler avant que le processus de retransmission RSVP abandonne sans avoir reçu un accusé de réception en présence de pertes de réseau. Il est suffisamment court pour récupérer rapidement en cas de messages perdus et ne pas avoir d'impact important sur le délai après numérotation, mais suffisamment long pour permettre à l'AN d'accuser réception de la demande et tous les routeurs intermédiaires dans le réseau privé.

Ce temporisateur est lancé lorsque le MTA ou l'AN envoie un message RSVP qui nécessite un accusé de réception (tel que RSVP-PATH). Ce temporisateur est remis à zéro lorsque l'expéditeur du message qui doit faire l'objet d'un accusé de réception reçoit une réponse à ce message. Dans le cas d'un message RSVP-PATH, cette réponse PEUT être RSVP-RESV, RSVP-PATH-ERROR ou RSVP-MESSAGE-ACK, ou encore RSVP-MESSAGE-NACK.

A l'expiration de ce temporisateur, la procédure de retransmission RSVP se termine.

La valeur recommandée de ce temporisateur est 4 secondes (4 000 ms).

Temporisateur T4

Ce temporisateur est implémenté dans le MTA dans le traitement de messages COMMIT. Il contrôle la retransmission de messages COMMIT qui peuvent avoir été perdus par le réseau. Il est suffisamment court pour récupérer rapidement en cas de demandes d'opération commit perdues et ne pas avoir un impact important sur le délai après prise d'appel, mais est suffisamment long pour permettre le traitement de la demande COMMIT au niveau de l'AN.

Ce temporisateur est lancé lorsque le MTA envoie un message COMMIT.

Ce temporisateur est remis à zéro lorsque le MTA reçoit un message COMMIT-ACK ou COMMIT-ERR qui est reconnu comme une réponse au message COMMIT.

A l'expiration de ce temporisateur, le MTA renvoie le message COMMIT.

La valeur recommandée de ce temporisateur est 500 ms.

Temporisateur T5

Ce temporisateur est implémenté dans l'AN (et AN-mandataire) dans le traitement du message de coordination de portes. Il contrôle la retransmission des messages GATE-OPEN et GATE-CLOSE qui peuvent avoir été perdus par le réseau. Il est suffisamment court pour récupérer rapidement en cas de perte de messages de coordination de portes, suffisamment long pour permettre le traitement du message de coordination de portes au niveau de l'AN ou l'AN-mandataire. Ce temporisateur interagit dans le cas de GATE-OPEN avec le temporisateur T2. Il convient qu'il soit de façon significative plus petit que le temporisateur T2.

Ce temporisateur est lancé lorsque l'AN (ou l'AN-mandataire) envoie un message GATE-OPEN/GATE-CLOSE.

Ce temporisateur est remis à zéro lorsque l'AN (ou l'AN-mandataire) reçoit un message GATE-OPEN-ACK/GATE-CLOSE-ACK qui est reconnu comme réponse à GATE-OPEN/GATE-CLOSE.

A l'expiration de ce temporisateur, l'AN (ou l'AN-mandataire) renvoie le message GATE-OPEN/GATE-CLOSE.

La retransmission du message GATE-OPEN/GATE-CLOSE est répétée pour un nombre de répétitions fixe.

La valeur recommandée de ce temporisateur est de 500 ms.

Temporisateur T6

Ce temporisateur est implémenté dans le MTA ou l'AN dans le traitement de réservations RSVP. Il contrôle le délai initial utilisé par la procédure de retransmission RSVP.

La valeur recommandée de ce temporisateur est 500 ms.

APPENDICE I

Exemple de mappage de descriptions SDP avec des messages flowspec RSVP

Les messages de protocole de descripteurs de session sont utilisés pour décrire les sessions multimédias pour les besoins de l'annonce de session, l'invitation de session et les autres formes d'ouverture de session multimédia conforme à IETF RFC 2327. Le présent appendice décrit un mécanisme pour le mappage des descriptions SDP avec les flowspec RSVP.

Une description SDP typique contient plusieurs champs qui contiennent des informations concernant la description de la session (version de protocole, nom de session, lignes d'attribut de session, etc.), la description du temps (le temps pendant lequel la session est active, etc.) et la description du média (nom du média et transport, titre du support, information sur la connexion, lignes d'attribut du support, etc.). Les deux composantes cruciales pour mapper une description SDP avec un message RSVP sont le nom du support et l'adresse de transport (m) et les lignes d'attribut du média (a).

Le nom du média et l'adresse de transport (m) sont de la forme:

m=<media> <port> <transport> <fmt list>

La ou les lignes d'attribution de support (a) sont de la forme:

a=<token>: <value>

Une communication vocale IP typique serait de la forme:

m = audio 3456 RTP/AVP 0

a = ptime: 10

Sur la ligne de l'adresse de transport (m), le premier terme définit le type de média, qui dans le cas d'une session voix IP est audio. Le deuxième terme définit le port UDP auquel le média est envoyé (port 3456). Le troisième terme indique que ce flux est un profil audio/vidéo RTP. Enfin, le dernier terme et le type de charge utile du média tel que défini dans le profil audio/vidéo RTP (référence IETF RFC 1890). Dans ce cas, le 0 représente un type de charge utile statique de canal audio simple codé MIC selon une loi μ échantillonné à 8 kHz. Sur la ligne d'attribution du média (a), le premier terme définit le temps de formation de paquet (10 ms).

Les types de payload autres que ceux définis dans IETF RFC 1890 sont associés dynamiquement en utilisant un type de charge utile dynamique de la plage 96-127, tel que défini dans IETF RFC 2327 et une ligne d'attribution de média. Par exemple, un message SDP typique pour G.726 serait composé comme suit:

m = audio 3456 RTP/AVP 96

a = rtpmap: 96 G726-32/8000

Le type de payload 96 indique que le type de payload est défini localement pour la durée de la session et la ligne suivante indique que le type de payload 96 est associé au codage "G726-32" avec une fréquence de l'horloge de 8 000 échantillons/s. Pour chaque CODEC défini (s'il est représenté en SDP comme type de charge utile statique ou dynamique) il est nécessaire d'avoir un mappage de table entre soit le type de charge utile, soit la représentation de chaîne ASCII et les exigences de bande passante pour ce CODEC.

Le mappage du code RTP/AVP avec le message RSVP Flowspec est conforme au Tableau I.1, comme le stipule la spécification J.161 de CODEC IPCablecom:

Tableau I.1/J.163 – Mappage des paramètres de description de session avec Flowspec RSVP

Paramètres de description de session			**Paramètres Flowspec**		**Commentaires**
Code RTP/AVP	Rtpmap	Ptime	Valeurs b,m,M	Valeurs r,p	
0	<none> (néant)	10	120 octets	12 000 octets/s	G.711 utilisant le type de charge utile défini par l'IETF
0	<none>	20	200 octets	10 000 octets/s	
0	<none>	30	280 octets	9 333 octets/s	
96-127	PCMU/8000	10	120 octets	12 000 octets/s	MIC G.711, 64 kbit/s, CODEC par défaut
96-127	PCMU/8000	20	200 octets	10 000 octets/s	
96-127	PCMU/8000	30	280 octets	9 333 octets/s	
96-127	G726-16/8000	10	60 octets	6 000 octets/s	
96-127	G726-16/8000	20	80 octets	4 000 octets/s	
96-127	G726-16/8000	30	100 octets	3 333 octets/s	
96-127	G726-24/8000	10	70 octets	7 000 octets/s	
96-127	G726-24/8000	20	100 octets	5 000 octets/s	
96-127	G726-24/8000	30	130 octets	4 333 octets/s	
2	<none>	10	80 octets	8 000 octets/s	G.726-32, identique à G.721, qui est la charge utile type 2 assignée par IETF
2	<none>	20	120 octets	6 000 octets/s	
2	<none>	30	160 octets	5 333 octets/s	
96-127	G726-32/8000	10	80 octets	8 000 octets/s	
96-127	G726-32/8000	20	120 octets	6 000 octets/s	
96-127	G726-32/8000	30	160 octets	5 333 octets/s	
96-127	G726-40/8000	10	90 octets	9 000 octets/s	
96-127	G726-40/8000	20	140 octets	7 000 octets/s	
96-127	G726-40/8000	30	190 octets	6 333 octets/s	
15	<none>	10	60 octets	6 000 octets/s	G.728, charge utile assignée type 15 par IETF
15	<none>	20	80 octets	4 000 octets/s	
15	<none>	30	100 octets	3 333 octets/s	

Tableau I.1/J.163 – Mappage des paramètres de description de session avec Flowspec RSVP *(fin)*

Paramètres de description de session			Paramètres Flowspec		Commentaires
96-127	G728/8000	10	60 octets	6 000 octets/s	G.728, LD-CELP, 16 kbit/s
96-127	G728/8000	20	80 octets	4 000 octets/s	
96-127	G728/8000	30	100 octets	3 333 octets/s	
18	<none>	10	50 octets	5 000 octets/s	G.729 Annexe A, identique à G.729, charge utile assignée type 18 par IETF
18	<none>	20	60 octets	3 000 octets/s	
18	<none>	30	70 octets	2 333 octets/s	
96-127	G729A/8000	10	50 octets	5 000 octets/s	G.729 Annexe A, CS-ACEL, 8 kbit/s, taille de trame 10 ms avec 5 ms de préanalyse
96-127	G729A/8000	20	60 octets	3 000 octets/s	
96-127	G729A/8000	30	70 octets	2 333 octets/s	
96-127	G729E/8000	10	55 octets	5 500 octets/s	G.729 Annexe E, CS-ACELP, 11,8 kbit/s, taille de trame 10 ms avec 5 ms de préanalyse
96-127	G729E/8000	20	70 octets	3 500 octets/s	
96-127	G729E/8000	30	85 octets	2 833 octets/s	

APPENDICE II

Exemple d'échange de messages, de protocole pour un appel de base de réseau privé à réseau privé avec DCS pour MTA autonome

Le présent appendice constitue une description informative, informelle de la relation entre le protocole DCS (DCS, *distributed call signalling*) et les méthodes de QS dynamique qui peuvent être invoquées à différents points du flux d'appel. Cette description ne se veut pas exhaustive. En dépit de la précision recherchée dans cet exemple, la spécification de la description d'appel DCS remplace cette description pour la spécification des flux de signalisation d'appel.

Lorsqu'un message INVITE est envoyé depuis le MTA_O de départ et arrive au GC_O, le GC_O envoie une demande GATE-ALLOC à l'AN_O le plus près du MTA_O de départ. Il s'agit là d'une demande pour l'allocation d'une ID de porte de 32 bits qui est unique dans cet AN_O. Cette ID de porte est communiquée à l'AN_T distant dans le message INVITE qui est suivi par le GC_O. De plus, l'AN_O de départ communique le nombre de connexions actives (portes) qui sont utilisées par le MTA_O pour permettre au GC_O ou au DP de rapporter le niveau d'activité courant pour l'abonné.

Le GC_T d'arrivée connaît tous les codecs possibles qui peuvent être utilisés pour l'appel, tel qu'ils sont proposés par MTA_O et peut calculer une "enveloppe autorisée" à partir de ces éléments et envoyer une commande GATE-SET à l'AN_T. Comme alternative, le GC_T peut envoyer uniquement une commande GATE-ALLOC à ce moment, attendre le résultat des procédures de négociation de codecs effectuée par MTA_T, calculer une "enveloppe d'autorisation" plus précise après avoir reçu le 200-OK de MTA_T puis envoyer la commande GATE-SET. Cette dernière est indiquée dans les diagrammes suivants de flux d'appel. Dans tous les cas, la GateID est allouée et donnée à MTA_T dans le message INVITE et MTA_T attend le message de signalisation ACK pour déterminer les valeurs finales des codecs négociés.

L'ID de porte (GateID) à l'extrémité distante est incluse dans le message 200-OK du GC_T au GC_O. Elle est fournie à l'AN_O dans l'échange GATE-SET correspondant avec l'"enveloppe autorisée" des paramètres Flowspec.

Une fois que le 200-OK a été renvoyé au MTA_O, ce dernier connaît l'adresse du MTA_T de destination et les paramètres associés à l'appel (codecs utilisés), et les traduit aux paramètres Flowspec pour les deux sens. Le MTA_O de départ envoie un ACK pour le 200-OK et effectue maintenant une réservation de ressources. Lorsque l'ACK arrive au MTA_T d'arrivée, il a toutes les informations nécessaires et effectue une réservation de ressources.

La réservation implique l'envoi d'un message RSVP-PATH avec les paramètres Flowspec dans les deux sens. L'AN effectue le contrôle d'admission, après avoir confronté les paramètres à l'enveloppe autorisée ainsi que la disponibilité des ressources et accuse réception de la réservation réussie avec un message RSVP-RESV. Entre-temps, l'échange de messages MAC J.112 pour l'allocation de ressources de la couche 2 est effectué par l'AN et le CM. Les ressources requises pour l'appel sont maintenant prêtes à être engagées. Toutefois, elles attendent une phase supplémentaire du protocole de signalisation d'appel et que les utilisateurs aux deux extrémités de l'appel décrochent leur "téléphone" pour communiquer.

Le second message 200-OK du MTA_T au MTA_O de départ est une indication que les deux utilisateurs (dans ce simple appel de base à deux correspondants) sont prêts à communiquer. Le MTA_T d'arrivée envoie un message COMMIT immédiatement après avoir envoyé le 200-OK. Le MTA_O de départ à la réception du 200-OK accuse réception de ce message et envoie également un message COMMIT. Le message COMMIT part de chaque MTA à son AN local et provoque un échange de messages MAC J.112 pour engager les ressources au flux. Une fois que le message COMMIT a fait l'objet d'un accusé de réception par les AN, les deux extrémités peuvent commencer à communiquer tout en recevant une QS améliorée. Lorsque le message COMMIT est reçu par l'un ou l'autre deux AN, il démarre le temporisateur T2 qui attend la réception du message Gate-Open de l'AN distant avec son ID de porte. A la réception du message COMMIT les AN enregistrent également l'événement QoS-Start et l'événement Call-Answer.

Les messages de coordination de portes entre les deux AN indiquant l'un à l'autre que la porte a été ouverte et que la description (FlowSpec) du flux attendu de l'autre extrémité a été échangée sont également indiqués. La réception du message Gate-Open indique que le temporisateur au niveau des AN serait désactivé.

A la fin de l'appel, les MTA envoient un message RSVP-PATH-TEAR pour mettre fin aux réservations. A ce moment, les AN envoient également un message de coordination Gate-Close à l'AN distant ainsi qu'un message d'événement QoS-Stop et un message d'événement Call-Disconnect au serveur d'archivage.

II.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Voir Figure II.1.

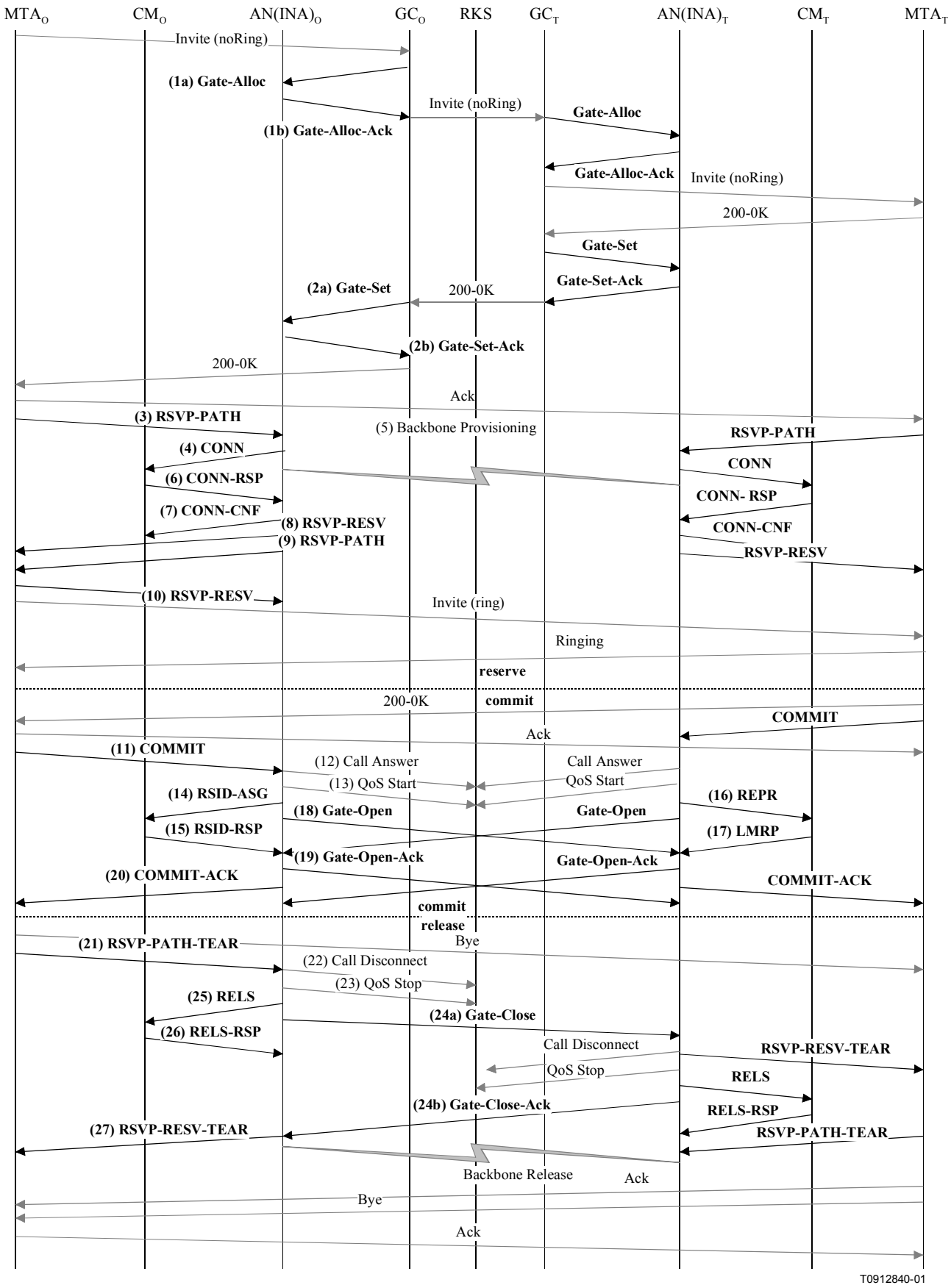


Figure II.1/J.163 – Flux d'appel de base avec les messages J.112 de l'Annexe A – DCS

1) GCo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo (1a).

GATE-ALLOC

TransactionID (ID de la transaction)		3176	
Subscriber (abonné)		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count (compte d'activité)		4	Nombre de portes maximales permises pour cet abonné.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de portes allouées (1b).

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Répond à la demande de ressources totales utilisées par ce point d'extrémité.
Gate-ID (ID de porte)		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de portes établies pour cet abonné.
Gate Coordination Port (coordination de portes port)		4104	Port UDP au niveau duquel l'AN écoutera les messages de coordination de portes.

2) GCo, après des échanges supplémentaires de signalisation, donne à ANo l'autorisation d'initier la phase de réservation du procédé d'allocation de ressources pour le nouveau flux J.112 (2a).

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info (information sur porte distante)	Address (adresse)	ANt	Information nécessaire pour coordonner les portes.
	Port	2052	
	Remote Gate-ID (identification de porte distante)	1273	
	Security Key (clé de sécurité)	<clé>	

GATE-SET

Event-Generation-Info (information sur la génération d'événement)	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID (ID de corrélation avec la facturation)	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.
Media-Connection-Info (information sur la connexion du média)	Called Number (numéro appelé)	0531-3915-2478	Champs nécessaires pour la génération du message d'événement Call Answer.
	Routing Number (numéro de routage)	0531-3915-2478	
	Charged Number (numéro facturé)	0531-3915-2480	
	Location Routing Number (numéro de routage de l'emplacement)	0531-3915-2478	
Gate-Spec	Direction (sens)	amont	
	Protocol (protocole)	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address (adresse source)	MTAo	
	Destination Address (adresse de destination)	MTAt	
	Source Port (port source)	0	
	Destination Port (port de destination)	7000	
	DSCP	6	Valeur Packet Type (type de paquet) pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.

GATE-SET

Gate-Spec	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction (sens)	aval	
	Protocol (protocole)	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address (adresse source)	MTAt	
	Destination Address (adresse de destination)	MTAo	
	Source Port (port source)	0	
	Destination Port (port de destination)	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond to la commande Gate-Set avec un accusé de réception (2b).

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Réponse à demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de portes établies pour cet abonné.

3) MTAo, à la réception d'une information d'appel de signalisation, envoie un message RSVP-PATH, adressé au MTAt, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le réseau CPE interceptent, traitent et envoient ce message comme un RSVP-PATH normal.

RSVP-PATH

Session-Object	Protocol	UDP	Ces paramètres identifient la session RSVP, font correspondre l'autorisation précédemment demandée par le GateController et sont également utilisés pour les classificateurs QS.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Sender-Tspec	b	120	Paramètres de trafic négociés actuellement demandés pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le trajet entre le MTA et l'AN. NOTE – Le paramètre HdrSuppression est uniquement utilisé pour identifier les flux sur lesquels la suppression d'en-tête sera effectuée. Le contexte de suppression d'en-tête est établi en utilisant les messages MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7120	
Reverse-Sender Templ	Source Address	MTAt	
	Source Port	0	
Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés effectivement demandés pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires. NOTE – Le paramètre HdrSuppression est uniquement utilisé pour identifier les flux sur lesquels la suppression d'en-tête sera effectuée. Le contexte de suppression d'en-tête est établi en utilisant les messages MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
Gate-ID		37 125	

4) ANo utilise le message RSVP-PATH et calcule les paramètres de QS pour la liaison J.112. ANo envoie le message Connect suivant à CMo. Ce message est utilisé pour établir les paramètres amont et aval. En supposant qu'un débit amont de 3,088 Mbit/s soit utilisé et que les paquets IP soient encapsulés en utilisant DirectIP, les ressources amont sont calculées comme suit. Un paquet IP d'une taille de 120 octets (du Tspec), y compris l'en-queue de 5 octets AAL 5, occupe trois cellules ATM. Ainsi, en utilisant le mode Reservation Access ANo doit accorder 3 intervalles toutes les 10 ms. En mode d'accès à débit fixe, une affectation cyclique de 3 intervalles à la fois est nécessaire avec une distance maximale de 60 intervalles. La bande passante demandée est de 360 intervalles par 1200 ms. Toutefois, aucune ressource n'est allouée dans le message Connect. Cela indique au CMo que les ressources pour ce flux J.112 sont réservées mais ne sont pas encore engagées.

CONN

Connection_ID	37 125 <ID de porte>
Session_number	<non utilisé>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <oui>
IPv6_add	0 <non>
Priority_included	0 <non>
Flowspec_DS_included	0 <non>
Session_binding_US_included	1 <oui>
Session_binding_DS_included	1 <oui>
Encapsulation_included	1 <oui>
DS_multiprotocol_CBD_included	0 <non>
Resource_number	0x00
Connection_Control_Field	
DS_ATM_CBD_included	0 <non>
DS_MPEG_CBD_included	1 <oui>
US_ATM_CBD_included	1 <oui>
Upstream_Channel_Number	0x1
Slot_list_included	0 <non>
Cyclic_assignment	0 <non>
Frame_Length	0 <non>
Maximum_Contention_Access_Message_Length	1 <intervalles>
Maximum_Reservation_Access_Message_Length	50 <intervalles>
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20 000 000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)

CONN

Session_binding_US	
US_session_binding_control	0x1F
NIU_client_source_IP_add	MTAo
NIU_client_destination_IP_add	MTAt
NIU_client_source_port	0
NIU_client_destination_port	7000
Upstream_transport_protocol	UDP
Session_binding_DS	
DS_session_binding_control	0x1F
INA_client_source_IP_add	MTAt
INA_client_destination_IP_add	MTAo
INA_client_source_port	0
INA_client_destination_port	7120
Downstream_transport_protocol	UDP
Connection_control_field2	
Upstream_modulation_included	1 <oui>
Upstream_Modulation	QPSK (1)

5) Simultanément avec le message 4, ANo initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à ANo toute notification nécessaire indiquant que la réservation a abouti.

6) CMo vérifie les ressources qu'il lui est demandé d'allouer (par exemple, contexte de suppression d'en-tête, ID de connexion, contexte de classificateur) et installe les classificateurs. Si l'opération aboutit, il retourne le message Connect Response indiquant la réussite de cette opération.

CONN-RSP

Connection_ID	37 125 <ID de porte>

7) A la réception du Message Connect Response, ANo accuse réception avec un message Connect Confirm.

CONN-CNF

Connection_ID	37 125 <ID de porte>

8) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, ANo répond au message RSVP-PATH en envoyant un message RSVP-RESV. Le message inclut la Resource ID qui est assignée par ANo à ce flux IP. Le message RSVP-RESV est envoyé avec l'adresse source de MTAt et l'adresse de destination de MTAo. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lesquels la réservation est établie.
	Destination Address	MTAt	
	Destination Port	7000	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

9) Si l'adresse du saut précédent dans le message RSVP-PATH diffère de l'adresse source (*Source Address*), il est alors demandé à l'AN de générer un message RSVP-PATH pour réserver les ressources aval au niveau de tous les routeurs intermédiaires. Cette condition serait uniquement satisfaite si le MTA n'était pas immédiatement adjacent au CM.

Pour cet exemple, supposons qu'un routeur intermédiaire existe entre MTAo et CMo, mais non entre MTAt et CMt.

ANo construit un message RSVP-PATH en utilisant l'information Reverse Path et envoie le message au MTAo de départ. Ce message inclut l'objet ResourceID.

RSVP-PATH

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont simulés comme si le message RSVP venait de l'extrémité distante.
	Destination Address	MTAo	
	Destination Port	7120	
Sender-Tspec	b	120	Sender-Tspec venait de Reverse-Sender-Tspec dans le message RSVP-PATH en provenance du MTAo. Ceci identifie les ressources qui seront nécessaires dans le sens aval (de MTAt à MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

10) MTAo, en réponse au RSVP-PATH, envoie RSVP-RESV à MTAt. Ce message est envoyé avec "Router-Alert" réglé et tous les routeurs intermédiaires interceptent, traitent et envoient ce message jusqu'à ce qu'il atteigne ANo.

RSVP-RESV

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont copiés du message RSVP-PATH reçu.
	Destination Address	MTAo	
	Destination Port	7120	
Flowspec	b	120	Ces valeurs sont également copiées du message RSVP-PATH et spécifient la quantité de ressources réservée pour le flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
	R	12 000	
	S	0	
ResourceID		1	Resource ID, copié de RSVP-PATH.

11) En réponse aux messages de signalisation qui indiquent que l'appel a été établi (c'est-à-dire que l'autre partie a décroché), MTAo envoie le message COMMIT à ANo. Ce message est envoyé à ANo à un port UDP déterminé par la signalisation d'appel. Session-Object et Sender Template donnent à ANo suffisamment d'informations pour identifier la "porte" et pour identifier quelles sont les ressources réservées qui sont engagées.

COMMIT

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port doivent correspondre à ces paramètres pour l'ID de porte.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

12) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant que la connexion de média a commencé. Le format de ce message est décrit dans UIT-T J.164.

13) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant qu'une qualité de service améliorée a été accordée à cet appel. Le format de ce message est décrit dans UIT-T J.164.

14) L'AN peut engager les ressources réservées en utilisant le mode Fixed-rate Acces (accès à débit réduit) ou le mode Reservation Access (accès de réservation). A la réception du message COMMIT, il a besoin d'envoyer les messages de couche MAC appropriés pour établir un flux J.112.

Pour cet exemple, il est supposé que ANo décide d'utiliser le mode Reservation Access tandis que ANt engage les ressources en mode d'accès à débit fixe.

Une superposition continue est utilisée pour prendre en charge le CBR comme caractéristique de ce trafic. Pour commencer la transmission ANo envoie un message Reservation ID Assignment.

RSID-ASG

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <intervalles>
GFC_10_Slots	3 < intervalles >
GFC_01_Slots	1 < intervalles >

15) CMo envoie un message Reservation ID Response montrant que l'opération a réussi.

RSID-RSP

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

16) L'ANt côté arrivée de l'appel a décidé de fournir les ressources demandées en utilisant le mode accès à débit fixe. Pour engager les ressources et pour commencer la transmission ANt envoie un message Reprovision à CMt.

REPR

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <non>
Delete_Reservation_IDs	0 <non>
New_Downstream_IB_Frequency_included	0 <non>
New_Downstream_OOB_Frequency_included	0 <non>
New_Upstream_Frequency_included	0 <non>
New_Frame_Length_included	1 <oui>
New_Cyclical_Assignment_included	1 <oui>
New_Slot_List_included	0 <non>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	1273 <ID de porte>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

17) CMt envoie un message Link Management Response montrant que l'opération a réussi.

LMRP

Link_Management_Msg_Number	<Reprovision Message Type Value>

18) ANo envoie le message de coordination de portes à l'ANt distant pour l'informer que les ressources au niveau de l'extrémité locale ont été engagées.

GATE-OPEN

TransactionID		72	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	Gate-ID au niveau de l'AN recevant ce message.
Tspec	b	120	Paramètres de trafic utilisés réellement pour les ressources engagées pour le flux dans le sens MTAo vers MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Reverse Tspec	b	120	Paramètres de trafic prévus d'être utilisés pour le flux dans le sens MTAt vers MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Total de contrôle de sécurité pour ce message.

19) A la réception du message GATE-OPEN de l'ANt distant, ANo répond avec un GATE-OPEN-ACK.

GATE-OPEN-ACK

TransactionID		8096	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

20) ANo accuse réception du message COMMIT avec un message COMMIT-ACK.

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

21) Lorsque l'appel est fini MTAo envoie un message RSVP-PATH-TEAR à l'AN. Pour chaque réservation RSVP, MTAo envoie un message RSVP-PATH-TEAR séparé.

RSVP-PATH-TEAR

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port identifient le flux RSVP.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

22) ANo envoie la notification au serveur d'archivage (RKS) indiquant que la connexion du média est terminée. Le format de ce message d'événement est décrit dans UIT-T J.164.

23) ANo envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé. Le format de ce message d'événement est décrit dans UIT-T J.164.

24) ANo, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de portes à l'adresse donnée précédemment dans la commande GATE-SET, qui dans le cas de DCS est ANt desservant MTAt (24b).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	Gate-ID au niveau de l'élément de réseau recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

ANt répond avec un message GATE-CLOSE-ACK (24b).

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

25) ANo, à la réception de RSVP-PATH-TEAR, envoie un message Release à CMo indiquant le flux J.112 qui doit être supprimé.

RELS

Number_of_Connections	1
Connection_ID	37 125 <ID de porte>

26) CMt génère le flux J.112 et envoie le Release Response à ANo.

RELS-RSP

Connection_ID	37 125 <ID de porte>

27) ANo envoie le RSVP-RESV-TEAR au MTAo.

RSVP-RESV-TEAR

Session-Object	Protocol	UDP	Ces paramètres identifient le flux IP qui est en train de se terminer.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

II.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure II.2

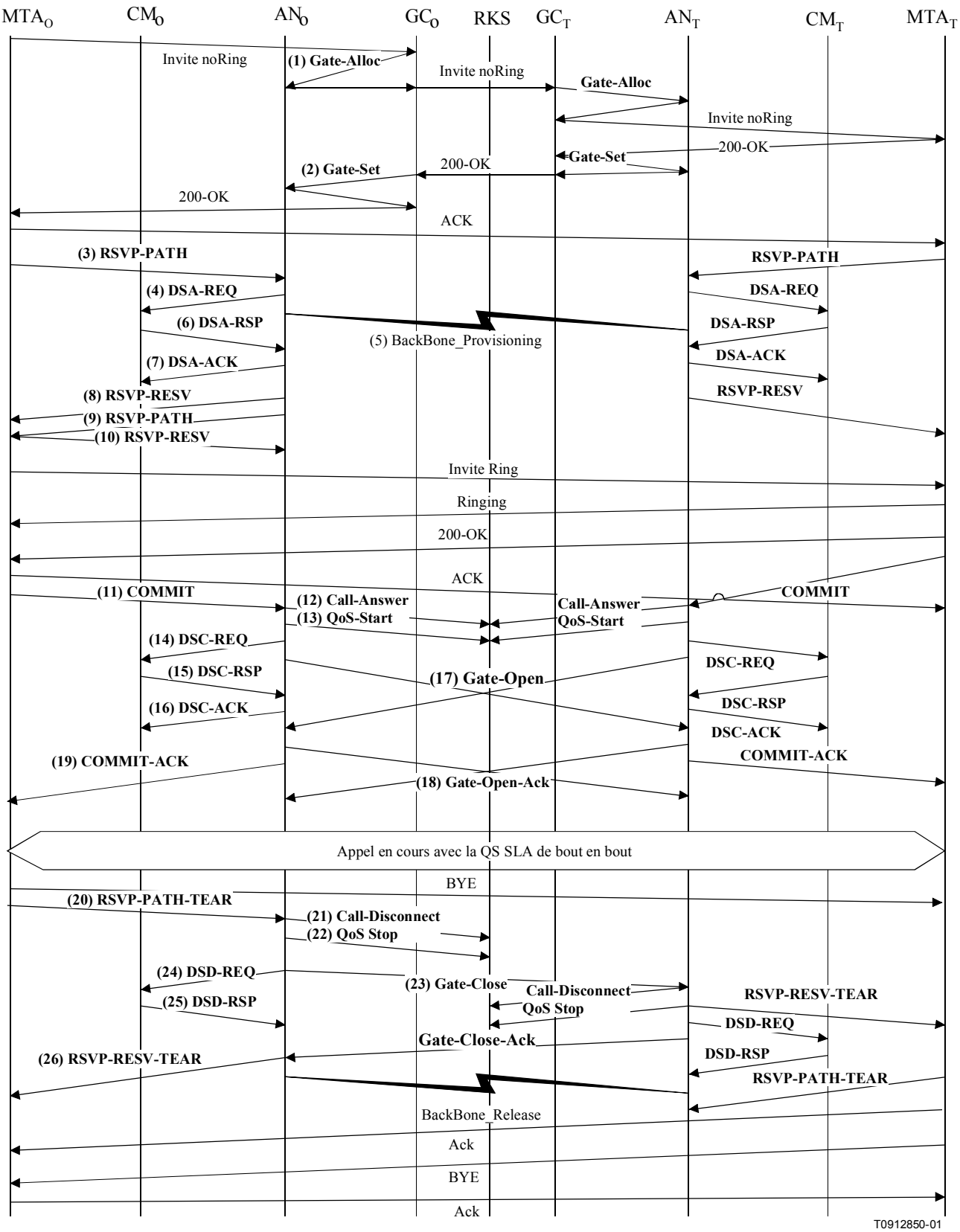


Figure II.2/J.163 – Flux d'appel de base – Signalisation DCS

1) GCo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo.

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count		4	Nombre maximal de connexions permises par le client.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de connexions actives.

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de connexions établies par ce client.
Gate Coordination Port		4104	Port UDP au niveau duquel l'AN écoutera les messages de coordination de portes.

2) GCo, après des échanges supplémentaires de signalisation, donne à l'ANo l'autorisation d'admettre la nouvelle connexion.

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	AN Address	ANt	Information nécessaire pour coordonner les portes.
	AN Port	2052	
	Remote Gate-ID	1273	
	Security Key	<clé>	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Media-Connection-Info	Called-Number	212-555-2222	Champs nécessaires pour la génération du message Call-Answer.
	Routing Number	212-555-2222	
	Charged Number	212-555-1111	
	Location Routing Number	212-555-2222	
Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source Port	0	
	Destination Port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre réserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source Port	0	
	Destination Port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre réserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.

GATE-SET

Gate-Spec	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la commande Gate Setup avec un accusé de réception.

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de connexions établies par ce client.

3) MTAo, à la réception d'une information d'appel de signalisation, envoie un message RSVP-PATH, adressé au MTAt, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le LAN de rattachement interceptent, traitent et envoient ce message comme un RSVP-PATH normal.

RSVP-PATH

Session-Object	Protocol	UDP	Ces paramètres identifient la session RSVP, font correspondre l'autorisation précédemment demandée par le GateController et sont également utilisés pour les classificateurs QS.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Sender-Tspec	b	120	Paramètres de trafic négociés actuellement demandés pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le chemin entre le MTA et l'AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination Port	7120	

RSVP-PATH

Reverse-Sender Templ	Source Address	MTAt	
	Source Port	0	
Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés effectivement demandés pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	0	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
Gate-ID		37 125	

4) L'AN utilise le message RSVP-PATH et calcule les paramètres de QS pour la liaison J.112. L'AN envoie le DSA-REQ suivant au CM. Ce message est utilisé pour établir les paramètres amont et aval. La Upstream Unsolicited Grant Size (taille d'attribution non sollicitée amont) a été calculée égale à 120 (du Tspec) plus 18 (préfixe Ethernet) moins 40 (valeur de suppression d'en-tête) plus 13 (préfixe J.112). La suppression d'en-tête, spécifiée comme une longueur de 40 dans le RSVP-PATH, indique les 42 octets de l'en-tête Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est pris dans le paquet RSVP.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/Transmission Policy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)

DSA-REQ

UpstreamPacketClassification	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactif (0)
	IPSourceAddress	MTAt
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)
PayloadHeaderSuppression	ClassifierIdentifier	3001
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42octets>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Verifier (0)
HMAC		

5) Simultanément avec le message n° 2, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

6) Le CM vérifie les ressources qu'il lui est demandé d'allouer (par exemple, espace de table de suppression d'en-tête, identifications de flux de service, espace de table de classificateurs, bande passante de réseau local) et installe les classificateurs. Si l'opération aboutit, il renvoie le message DSA-RSP indiquant le succès de l'opération.

DSA-RSP

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

7) A la réception du DSA-RSP, l'AN accuse réception avec un message DSA-ACK.

DSA-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

8) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, l'AN répond au message RSVP-PATH en envoyant un message RSVP-RESV. Le message inclut le ResourceID qui est assigné par l'AN à cette connexion. Le message

RSVP-RESV est envoyé avec l'adresse source de MTA_T et l'adresse de destination de MTA_O. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lesquels la réservation est établie.
	Destination Address	MTAt	
	Destination Port	7000	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

9) Si l'adresse du saut précédent diffère de l'adresse source (*Source Address*), il est alors demandé à l'AN de générer un message RSVP-PATH pour réserver les ressources aval au niveau de tous les routeurs intermédiaires. Cette condition ne serait remplie que si le MTA n'était pas immédiatement adjacent au CM.

Pour cet exemple, supposons qu'un routeur intermédiaire existe entre MTAo et son CM, mais non entre MTAt et son CM.

L'AN construit le message RSVP-PATH en utilisant l'information Reverse Path qu'il a reçu du message RSVP-PATH et envoie le message au MTA de départ. Ce message inclut l'objet ResourceID.

RSVP-PATH

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont simulés comme si le message RSVP venait de l'extrémité distante.
	Destination Address	MTAo	
	Destination Port	7120	
Sender-Tspec	b	120	Sender-Tspec venait de Reverse-Sender-Tspec dans le message RSVP-PATH en provenance du MTAo. Ceci identifie les ressources qui seront nécessaires dans le sens aval (de MTAt à MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

10) MTAo, en réponse au RSVP-PATH(7), envoie RSVP-RESV à MTAt. Ce message est envoyé avec "router alert" réglé et tous les routeurs intermédiaires interceptent, traitent et envoient ce message jusqu'à ce qu'il atteigne l'AN.

RSVP-RESV

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont copiés du message RSVP-PATH reçu.
	Destination Address	MTAo	
	Destination Port	7120	
Filter-Spec	Source Address	MTAt	
	Source Port	7000	
Flowspec	b	120	Ces données sont également copiées depuis le message RSVP-PATH et spécifient la quantité de ressources réservée pour le flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
	R	12 000	
	S	0	
ResourceID		1	Resource ID, copié de RSP-PATH.

11) En réponse aux messages de signalisation qui indiquent que l'appel a été effectué (c'est-à-dire que l'autre partie a décroché), MTAo envoie le message COMMIT à l'AN. Ce message est envoyé à l'AN à un port UDP déterminé via la signalisation d'appel.

Session-Object et Sender Template donnent à l'AN suffisamment d'informations pour identifier la "porte" et pour identifier quelles sont les ressources réservées qui sont engagées.

COMMIT

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination doivent correspondre à ces paramètres pour l'ID de porte.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

12) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant que la connexion de média a commencé.

Call-Answer

Header	Time Stamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	ID de corrélation de facturation donnée dans Gate-Set.

Call-Answer

Called Party	Called Party Number	212-555-2222	Eléments fournis par CMS dans Gate-Set.
Routing Number	Routing Number	212-555-2222	
Charged Number	Charged Number	212-555-1111	
Location Routing Number	Location Routing Number	212-555-2222	

13) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) indiquant qu'une connexion avec une qualité de service améliorée a été accordée à cet appel.

QoS-START

Header (en-tête)	Horodateur	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	ID de corrélation donnée dans Gate-Set.
QoS Descriptor	Type	UGS	Description de la QS fournie pour cette connexion.
	Grant interval	10 ms	
	Grant Jitter	2 ms	
	Grant/Interval	1	
	Grant Size	111	
MTA Port	Port	7120	

14) L'AN décide quelle réservation doit être activée et envoie un DSC-REQ au CM pour activer le flux.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000

DSC-REQ

UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

15) Le CM envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

16) L'AN envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

17) L'AN envoie le message de coordination de portes à l'AN distant pour l'informer que les ressources à cette extrémité ont été engagées.

GATE-OPEN

Transaction ID		72	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	ID de porte (Gate-ID) au niveau de l'AN distant.

GATE-OPEN

Tspec	b	120	Paramètres de trafic engagés effectivement utilisés dans le sens MTAo vers MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Reverse-Tspec	b	120	Paramètres de trafic prévus utilisés dans le sens MTAt vers MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Total de contrôle de sécurité pour ce message.

18) L'AN distant répond à GATE-OPEN par:

GATE-OPEN-ACK

TransactionID		72	Identifiant pour faire correspondre ce message à sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

19) L'AN accuse réception du message COMMIT avec:

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37125	

20) Lorsque l'appel est fini le MTA envoie un message RSVP-PATH-TEAR à l'AN. Pour chaque réservation RSVP, le MTA envoie un message RSVP-PATH-TEAR séparé.

RSVP-PATH-TEAR

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port identifient le flux RSVP.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

21) L'AN envoie la notification au serveur d'archivage (RKS) indiquant que la connexion du média est terminée.

Call-Disconnect

Header	Timestamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	ID de corrélation de facturation fournie dans Gate-Set.
Termination Cause	Cause	1100C	Code Cause tel que défini par les messages Event.

22) L'AN envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un message QoS-Stop.

QoS-Stop

TimeStamp		<heure>	Heure de l'événement enregistré.
Header	Time Stamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	ID de corrélation du message Gate-Set.
SF-ID	SF-ID	1001	Identifiant de flux de service.

23) L'AN, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de porte à son AN correspondant desservant MTAt.

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	Identifie la GateID au niveau de l'AN distant.
HMAC			Total de contrôle de sécurité pour ce message.

L'AN distant répond par:

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse
HMAC			Total de contrôle de sécurité pour ce message

24) L'AN, à la réception de RSVP-PATH-TEAR, envoie un DSD-REQ au CM indiquant l'identification de flux de service qui doit être supprimée.

DSD-REQ

TransactionID		3
ServiceFlowID		1001
HMAC		

DSD-REQ

TransactionID		4
ServiceFlowID		2001
HMAC		

25) Le CM supprime le Service Flow ID et envoie la réponse à l'AN.

DSD-RSP

TransactionID		3
ServiceFlowID		1001
ConfirmationCode		Succès (0)
HMAC		

DSD-RSP

TransactionID		3
ServiceFlowID		2001
ConfirmationCode		Succès (0)
HMAC		

26) L'AN envoie le RSVP-RESV-TEAR au MTA.

RSVP-RESV-TEAR

Session-Object	Protocol	UDP	Ces paramètres identifient le flux IP qui est en train de se terminer.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

APPENDICE III

Exemple d'échange de messages de protocole pour un appel de base de réseau privé à réseau privé avec NCS pour MTA autonome

Le présent appendice fournit une description informationnelle d'une relation possible entre le protocole de signalisation d'appel (UIT-T J.162) et les méthodes de QS dynamique qui peuvent être invoquées à différents points dans le flux d'appel.

Lorsque le MTA_O de départ effectue la numérotation, c'est-à-dire, la carte de chiffres indique qu'un numéro de téléphone complet a été entré, les chiffres sont envoyés au CMS_O via un message Notify. Le CMS_O, dans sa première phase de lancement d'un nouvel appel, demande au MTA_O de créer une nouvelle connexion inactive. Le MTA_O alloue un port de réception pour le flux de média et répond avec un message ACK qui inclut la description de la session donnant la liste de tous les flux de média que le MTA_O souhaite recevoir. Le CMS_O effectue un échange GATE-ALLOC avec l'AN_O pour allouer une Gate-ID et transmet cette information au CMS_T d'arrivée avec le profil du SDP de départ.

Le CMS_T d'arrivée configure la porte au niveau de l'AN_T d'arrivée (en utilisant une commande GATE-SET), permettant à tous les flux de média qui sont acceptables pour l'initiateur dans l'"enveloppe autorisée" et permettant un port de destination avec un caractère joker sur le MTA_T. L'AN_T assigne également une Gate-ID et la renvoie au CMS_T. Le CMS_T transmet la Gate-ID locale au MTA_T d'arrivée dans une commande Create Connection, avec le profil SDP proposé. MTA_T, dans

sa réponse, indique l'ensemble de flux de média qu'il trouve acceptable et le port alloué pour la réception de ces flux.

A ce moment, MTA_T connaît le codec émetteur, le codec récepteur, l'adresse et le port de destination pour les paquets voix qu'il envoie et le port local pour la réception des paquets voix. Il commence alors la séquence de réservation en envoyant un RSVP-PATH à AN_T.

Lorsque CMS_O reçoit le profil SDP de MTA_T, il a suffisamment d'informations pour établir la porte au niveau de AN_O. Il effectue par conséquent l'opération GATE-SET, y compris la Gate-ID distante et l'adresse de AN_T. CMS_O envoie alors une commande Modify Connection à MTA_O, en lui indiquant l'adresse de destination, le port et le codec à utiliser. MTA_O a maintenant suffisamment d'informations pour effectuer une réservation de ressources. Lorsqu'une réservation est effectuée, il envoie un accusé de réception de succès à CMS_O. CMS_T indique maintenant à MTA_T d'avertir l'utilisateur d'un appel entrant. MTA_T vérifie d'abord que la réservation de ressources qu'il a lancée précédemment a abouti et si tel est le cas, continue en faisant sonner le téléphone.

Lorsque l'appelé répond, MTA_T informe CMS_T avec un message Notify, indiquant Offhook (décroché). CMS_T envoie alors une commande Modify Connection à MTA_T en établissant le mode de connexion émission+réception; MTA_T effectue l'échange COMMIT avec AN_T puis envoie l'accusé de réception. CMS_O envoie également une commande Modify Connection à MTA_O en effectuant son mode de connexion envoi+réception, amenant MTA_O à effectuer également l'échange COMMIT avec AN_O. L'appel est maintenant établi.

Chaque partie peut lancer une terminaison d'appel en envoyant un message Notify à son CMS en indiquant Onhook (raccroché). Le schéma montre MTA_O en train de réaliser cette opération. CMS_O répond à la notification Onhook en envoyant une commande Delete Connection, qui déclenche la séquence RSVP-PATH-TEAR pour libérer les ressources. MTA_T est informé du raccroché par la signalisation d'appel (une commande Delete Connection, non représentée) ou par le message de QS dynamique RSVP-RESV-TEAR. Lorsque MTA_T décroche ensuite, il produit le même message Notify que celui envoyé précédemment par MTA_O et termine la séquence.

III.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Voir Figure III.1

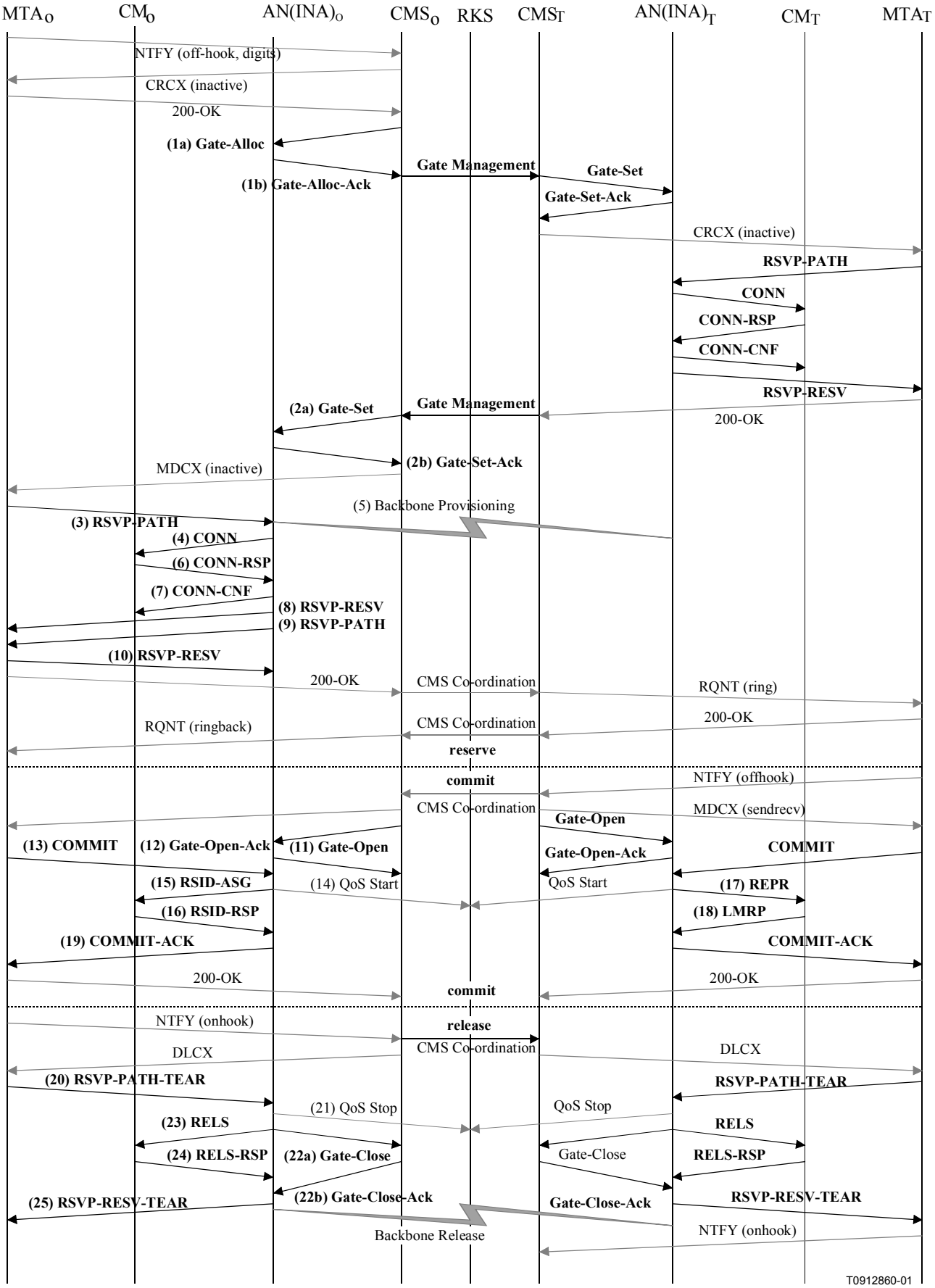


Figure III.1/J.163 – Flux d'appel de base avec les messages J.112 de l'Annexe A – NCS

1) GCo/CMSo, à la réception des informations de signalisation de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo (1a).

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count		4	Nombre de portes maximales permises pour cet abonné.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de portes allouées (1b).

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de portes établies pour cet abonné.

2) GCo/CMSo, après des échanges supplémentaires de signalisation, donne à ANo l'autorisation d'initier la phase de réservation du procédé d'allocation de ressources pour le nouveau flux J.112 (2a).

GATE-SET

Transaction ID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	Address	CMSo	Information nécessaire pour coordonner les portes. Il est à noter que CMSo s'est donné comme l'entité pour échanger les messages de coordination de portes. La valeur du drapeau indique qu'il convient que l'AN n'envoie pas de message Gate-Open lorsqu'il reçoit un COMMIT en provenance du MTA, mais attend encore pour recevoir un message Gate-Open de CMSo.
	Port	2052	
	Remote Gate-ID	8095	
	Security Key	<clé>	
	Flag	No-gate-open	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la commande Gate Setup avec un accusé de réception (2b).

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de portes établies pour cet abonné.

MTAo, à la réception d'une commande Modify-Connection, envoie un message RSVP-PATH, adressé au MTAt, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le LAN de rattachement interceptent, traitent et envoient ce message comme un RSVP-PATH normal.

RSVP-PATH

Session-Object	Protocol	UDP	Ces paramètres identifient la session RSVP, font correspondre l'autorisation précédemment demandée par le GateController et sont également utilisés pour les classificateurs QS.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Sender-Tspec	b	120	Paramètres de trafic négociés actuellement demandés pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le trajet entre le MTA et l'AN. NOTE – Le paramètre HdrSuppression est uniquement utilisé pour identifier les flux sur lesquels la suppression d'en-tête sera effectuée. Le contexte de suppression d'en-tête est établi en utilisant les messages MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7120	
Reverse-Sender Templ	Source Address	MTAt	
	Source Port	0	

RSVP-PATH

Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés effectivement demandés pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires. NOTE – Le paramètre HdrSuppression est uniquement utilisé pour identifier les flux sur lesquels la suppression d'en-tête sera effectuée. Le contexte de suppression d'en-tête est établi en utilisant les messages MAC.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
Gate-ID		37 125	

4) L'AN utilise le message RSVP-PATH et calcule les paramètres de QS pour la liaison J.112. L'AN envoie le message Connect suivant au CM. Ce message est utilisé pour établir les paramètres amont et aval. En supposant qu'un débit amont de 3,088 Mbit/s soit utilisé et que les paquets IP soient encapsulés en utilisant DirectIP, les ressources amont sont calculées comme suit. Un paquet IP d'une taille de 120 octets (du Tspec) y compris l'en-queue de 5 octets AAL 5 occupe trois cellules ATM. Ainsi, en utilisant le mode Reservation Access, l'AN doit accorder 3 intervalles toutes les 10 ms. En mode d'accès à débit fixe, une affectation cyclique de 3 intervalles à la fois est nécessaire avec une distance maximale de 60 intervalles. La bande passante demandée est de 360 intervalles par 1200 ms. Toutefois, aucune ressource n'est allouée dans le message Connect. Cela indique au CM que les ressources pour ce flux J.112 sont réservées mais ne sont pas encore engagées.

CONN

Connection_ID	37 125 <ID de porte>
Session_number	<non utilisé>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <oui>
IPv6_add	0 <non>
Priority_included	0 <non>
Flowspec_DS_included	0 <non>
Session_binding_US_included	1 <oui>
Session_binding_DS_included	1 <oui>
Encapsulation_included	1 <oui>
DS_multiprotocol_CBD_included	0 <non>
Resource_number	0x00
Connection_Control_Field	
DS_ATM_CBD_included	0 <non>
DS_MPEG_CBD_included	1 <oui>
US_ATM_CBD_included	1 <oui>
Upstream_Channel_Number	0x1
Slot_list_included	0 <non>
Cyclic_assignment	0 <non>
Frame_Length	0 <non>

CONN

Maximum_Contention_Access_Message_Length	1 <intervalles>
Maximum_Reservation_Access_Message_Length	50 <intervalles>
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20 000 000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Session_binding_US	
US_session_binding_control	0x1F
NIU_client_source_IP_add	MTAo
NIU_client_destination_IP_add	MTAt
NIU_client_source_port	0
NIU_client_destination_port	7000
Upstream_transport_protocol	UDP
Session_binding_DS	
DS_session_binding_control	0x1F
INA_client_source_IP_add	MTAt
INA_client_destination_IP_add	MTAo
INA_client_source_port	0
INA_client_destination_port	7120
Downstream_transport_protocol	UDP
Connection_control_field2	
Upstream_modulation_included	1 <oui>
Upstream_Modulation	QPSK (1)

5) Simultanément avec le message 4, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

6) Le CM vérifie les ressources qu'il lui est demandé d'allouer (par exemple, contexte de suppression d'en-tête, ID de connexion, contexte de classificateur) et installe les classificateurs. Si l'opération aboutit, il renvoie le message Connect Response indiquant la réussite de cette opération.

CONN-RSP

Connection_ID	37 125 <ID de porte>

7) A la réception du message Connect Response, l'AN accuse réception avec un message Connect Confirm.

CONN-CNF

Connection_ID	37125 <ID de porte>

8) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, l'AN répond au message RSVP-PATH en envoyant un message RSVP-RESV. Ce message inclut la RessourceID qui est assignée par l'AN à ce flux IP. Le message RSVP-RESV est envoyé avec l'adresse source de MTAt et l'adresse de destination de MTAo. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lequel la réservation est établie.
	Destination Address	MTAt	
	Destination port	7000	
Filter-Spec	Source Address	MTAo	
	Source Port	7120	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

9) Si l'adresse du saut précédent dans le message RSVP-PATH diffère de l'adresse source (*Source Address*), il est alors demandé à l'AN de générer un message RSVP-PATH pour réserver les ressources aval au niveau de tous les routeurs intermédiaires. Cette condition ne serait satisfaite que si le MTAo n'était pas immédiatement adjacent au CM.

Pour cet exemple, supposons qu'un routeur intermédiaire existe entre MTAo et son CM, mais non entre MTAt et son CM.

L'AN construit un message RSVP-PATH en utilisant l'information Reverse Path et envoie le message au MTAo de départ. Ce message inclut l'objet ResourceID.

RSVP-PATH

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont simulés comme si le message RSVP venait de l'extrémité distante.
	Destination Address	MTAo	
	Destination port	7120	

RSVP-PATH

Sender-Tspec	b	120	Sender-Tspec venait de Reverse-Sender-Tspec dans le message RSVP-PATH en provenance du MTAo. Ceci identifie les ressources qui seront nécessaires dans le sens aval (de MTAt à MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	non	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

10) MTAo, en réponse au RSVP-PATH, envoie RSVP-RESV à MTAt. Ce message est envoyé avec "Router-Alert" réglé et tous les routeurs intermédiaires interceptent, traitent et envoient ce message jusqu'à ce qu'il atteigne l'AN.

RSVP-RESV

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont copiés du message RSVP-PATH reçu.
	Destination Address	MTAo	
	Destination port	7120	
Flowspec	b	120	Ces données sont également copiées depuis le message RSVP-PATH et spécifient la quantité de ressources réservée pour le flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	Non	
	VAD	off	
	R	12 000	
	S	0	
ResourceID		1	Resource ID, copiée de RSVP-PATH.

11) Le CMS envoie le message de coordination de portes à l'AN pour l'informer que les ressources devraient être engagées. Si l'AN ne reçoit pas un message Commit en provenance du MTA avant l'expiration du temporisateur T2, il abandonne l'appel.

GATE-OPEN

TransactionID		8096	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		37 125	Gate-ID au niveau de l'AN recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

12) L'AN répond à GATE-OPEN par un GATE-OPEN-ACK.

GATE-OPEN-ACK

TransactionID		8096	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

13) En réponse à une commande Modify-Connection, que l'appel a été établi (c'est-à-dire que l'autre partie a décroché), MTAo envoie le message COMMIT à l'AN. Ce message est envoyé à l'AN à un port UDP donné dans l'objet RSVP-RESV Commit-Entity. Session-Object et Sender Template donnent à l'AN suffisamment d'informations pour identifier la 'porte' et pour identifier quelles sont les ressources réservées qui sont engagées.

COMMIT

Session-Object	Protocol	UDP	Les informations Protocol, Destination Address, Source Address et Destination doivent correspondre à ces paramètres pour l'ID de porte.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

14) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant qu'une qualité de service améliorée a été accordée à cet appel. Le format de ce message est décrit dans UIT-T J.164.

15) L'AN peut engager les ressources réservées en utilisant le mode Fixed-rate Access (accès à débit réduit) ou le mode Reservation Access (accès de réservation). A la réception du message COMMIT, il a besoin d'envoyer les messages de couche MAC appropriés pour établir un flux J.112.

Pour cet exemple, il est supposé que l'AN de MTAo décide d'utiliser le mode Reservation Access tandis que l'AN de MTAt engage les ressources en mode d'accès à débit fixe.

Une superposition continue est utilisée pour prendre en charge le CBR comme caractéristique de ce trafic. Pour commencer la transmission l'AN envoie un message Reservation ID Assignment.

RSID-ASG

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <intervalles>
GFC_10_Slots	3 <intervalles>
GFC_01_Slots	1 <intervalles>

16) Le CM envoie un message Reservation ID Response montrant que l'opération a réussi.

RSID-RSP

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

17) L'AN côté arrivée de l'appel a décidé de fournir les ressources demandées en utilisant le mode accès à débit fixe. Pour engager les ressources et pour commencer la transmission l'AN envoie un message Reprovision au CM.

REPR

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <non>
Delete_Reservation_IDs	0 <non>
New_Downstream_IB_Frequency_included	0 <non>
New_Downstream_OOB_Frequency_included	0 <non>
New_Upstream_Frequency_included	0 <non>
New_Frame_Length_included	1 <oui>
New_Cyclical_Assignment_included	1 <oui>
New_Slot_List_included	0 <non>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	37 125 <ID de porte>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

18) Le CM envoie un message Link Management Response montrant que l'opération a réussi.

LMRP

Link_Management_Msg_Number	<Reprovision Message Type Value>

19) L'AN accuse réception du message COMMIT avec un message COMMIT-ACK.

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source port	7120	
Gate-ID		37 125	

20) Lorsque l'appel est fini, en réponse à une commande Delete-Connection, le MTA envoie un message RSVP-PATH-TEAR à l'AN. Pour chaque réservation RSVP, le MTA envoie un message RSVP-PATH-TEAR séparé.

RSVP-PATH-TEAR

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port identifient le flux RSVP.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source port	7120	

21) L'AN envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé. Le format de ce message d'événement est décrit dans UIT-T J.164.

22) L'AN, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de portes à l'adresse donnée précédemment dans la commande GATE-SET, qui dans le cas du NCS est l'agent d'appel (Call Agent) (21b).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		8095	GateID au niveau de l'élément de réseau (ici: CMS) recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

Le CMS répond avec un message GATE-CLOSE-ACK (22b).

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

23) L'AN, à la réception de RSVP-PATH-TEAR, envoie un message Release au CM indiquant le flux J.112 qui doit être supprimé.

RELS

Number_of_Connections	1
Connection_ID	37 125 <ID de porte>

24) Le CM libère le flux J.112 et envoie le Release Response à l'AN.

RELS-RSP

Connection_ID	37 125 <ID de porte>

25) L'AN envoie le RSVP-RESV-TEAR au MTA.

RSVP-RESV-TEAR

Session-Object	Protocol	UDP	Ces paramètres identifient le flux IP qui est en train de se terminer.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

III.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure III.2

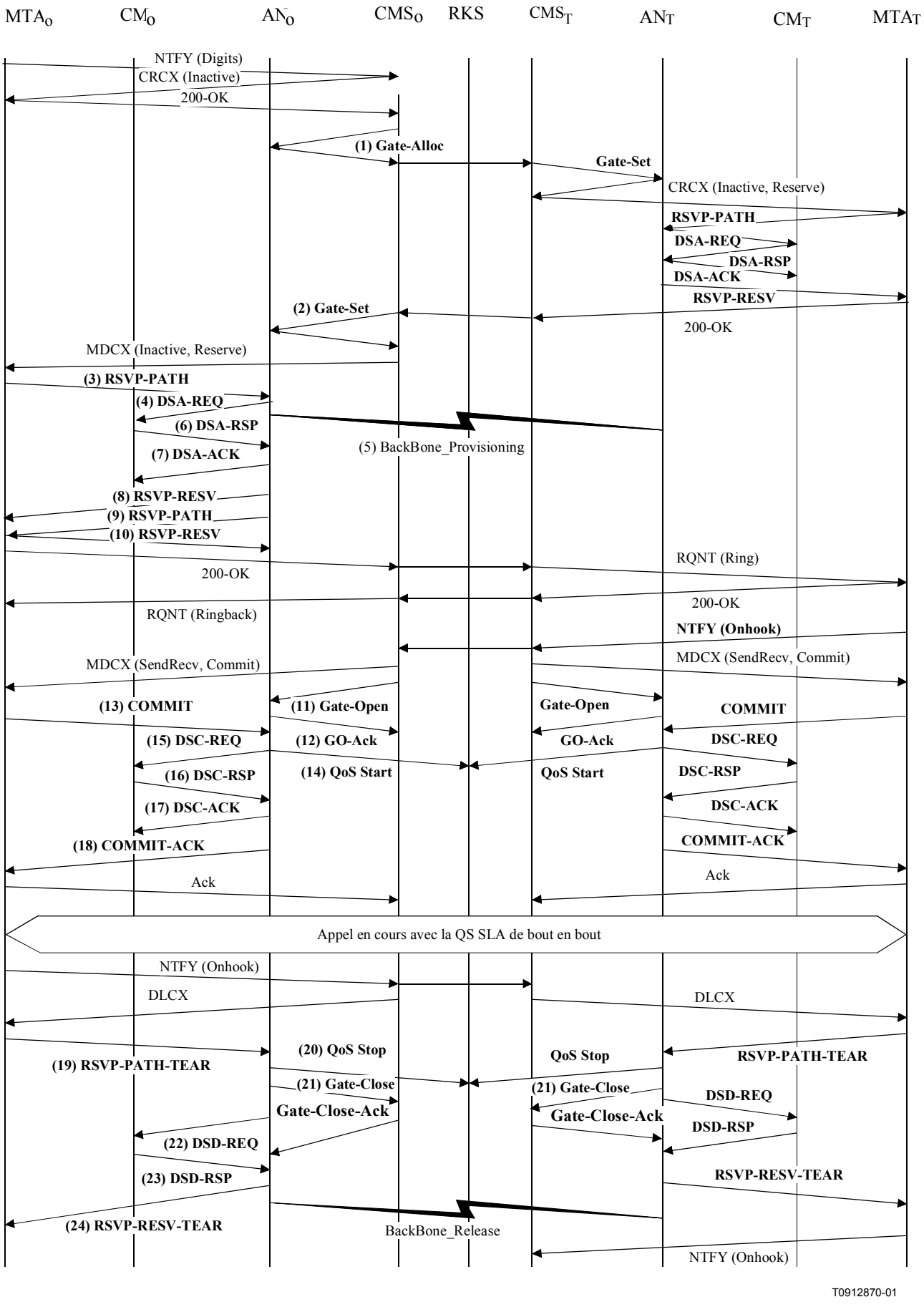


Figure III.2/J.163 – Flux d'appel de base – NCS

1) GCo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo.

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count		4	Nombre maximal de connexions permises par le client.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de connexions actives.

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de connexions établies par ce client.

2) GCo, après des échanges supplémentaires de signalisation, donne à l'ANo l'autorisation d'admettre la nouvelle connexion.

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Information	Address	CMSo	Information nécessaire pour coordonner les portes. Il est à noter que CMSo s'est donné comme l'entité pour échanger les messages de coordination de portes. La valeur du drapeau indique qu'il convient que l'AN n'envoie pas de message Gate-Open lorsqu'il reçoit un COMMIT en provenance du MTA, mais attend encore pour recevoir un message Gate-Open de CMSo.
	Port	2052	
	Remote Gate-ID	8095	
	Security Key	<clé>	
	Flag	No-gate-open	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la commande Gate Setup avec un accusé de réception.

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de connexions établies par ce client.

3) MTAo, à la réception d'une commande Modify-Connection, envoie un message RSVP-PATH, adressé au MTAt, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le LAN de rattachement interceptent, traitent et envoient ce message comme un RSVP-PATH normal.

RSVP-PATH

Session-Object	Protocol	UDP	Ces paramètres identifient la session RSVP, font correspondre l'autorisation précédemment demandée par le GateController et sont également utilisés pour les classificateurs QS.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Sender-Tspec	b	120	Paramètres de trafic négociés actuellement demandés pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le trajet entre le MTA et l'AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7120	
Reverse-Sender Templ	Source Address	MTAt	
	Source Port	0	

RSVP-PATH

Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés effectivement demandés pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	0	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
Gate-ID		37 125	

4) L'AN utilise le message RSVP-PATH et calcule les paramètres de QS pour la liaison J.112. L'AN envoie le DSA-REQ suivant au CM. Ce message est utilisé pour établir les paramètres amont et aval. La Upstream Unsolicited Grant Size (taille d'attribution non sollicitée amont) a été calculée égale à 120 (du Tspec) plus 18 (préfixe Ethernet) moins 40 (valeur de suppression d'en-tête) plus 13 (préfixe J.112). La suppression d'en-tête, spécifiée comme une longueur de 40 dans le RSVP-PATH, indique les 42 octets de l'en-tête Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est pris dans le paquet RSVP.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000

DSA-REQ

UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactive(0) (inactif)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)
PayloadHeaderSuppression	ClassifierIdentifier	3001
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42octets>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	vérifier (0)
HMAC		

5) Simultanément avec le message n° 2, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sort du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

6) Le CM vérifie les ressources qu'il lui est demandé d'allouer (par exemple, espace de table de suppression d'en-tête, identifications de flux de service, espace de table de classificateurs, bande passante de réseau local) et installe les classificateurs. Si l'opération aboutit, il renvoie le message DSA-RSP indiquant le succès de l'opération.

DSA-RSP

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

7) A la réception du DSA-RSP, l'AN accuse réception avec un message DSA-ACK.

DSA-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

8) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, l'AN répond au message RSVP-PATH en envoyant un message RSVP-RESV. Le message inclut le ResourceID qui est assigné par l'AN à cette connexion. Le message RSVP-RESV est envoyé avec l'adresse source de MTAt et l'adresse de destination de MTAo. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lequel la réservation est établie.
	Destination Address	MTAt	
	Destination Port	7000	
Filter-Spec	Source Address	MTAo	
	Source Port	7120	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

9) Si l'adresse du saut précédent diffère de l'adresse source (*Source Address*), il est alors demandé à l'AN de générer un message RSVP-PATH pour réserver les ressources aval au niveau de tous les routeurs intermédiaires. Cette condition ne serait remplie que si le MTA n'était pas immédiatement adjacent au CM.

Pour cet exemple, supposons qu'un routeur intermédiaire existe entre MTAo et son CM, mais non entre MTAt et son CM.

L'AN construit le message RSVP-PATH en utilisant l'information Reverse Path qu'il a reçue du message RSVP-PATH et envoie le message au MTA de départ. Ce message inclut l'objet ResourceID.

RSVP-PATH

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont simulés comme si le message RSVP venait de l'extrémité distante.
	Destination Address	MTAo	
	Destination Port	7120	
Sender-Tspec	b	120	Sender-Tspec venait de Reverse-Sender-Tspec dans le message RSVP-PATH en provenance du MTAo. Ceci identifie les ressources qui seront nécessaires dans le sens aval (de MTAt à MTAo).
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
ResourceID		1	ID des nouvelles ressources créée pour cette réservation.

10) MTAo, en réponse au RSVP-PATH (7), envoie RSVP-RESV à MTAt. Ce message est envoyé avec "Router-Alert" réglé et tous les routeurs intermédiaires interceptent, traitent et envoient ce message jusqu'à ce qu'il atteigne l'AN.

RSVP-RESV

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont copiés du message RSVP-PATH reçu.
	Destination Address	MTAo	
	Destination port	7120	
Flowspec	b	120	Ces données sont également copiées depuis le message RSVP-PATH et spécifient la quantité de ressources réservée pour le flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
	R	12 000	
	S	0	
ResourceID		1	Resource ID, copiée de RSP-PATH.

11) Le CMS envoie le message de coordination de portes à l'AN pour l'informer que les ressources devraient être engagées. Si l'AN ne reçoit pas un message COMMIT en provenance du MTA avant l'expiration du temporisateur T2, il abandonne la connexion.

GATE-OPEN

TransactionID		8096	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		37 125	Gate-ID au niveau de l'AN distant.
HMAC			Total de contrôle de sécurité pour ce message.

12) L'AN répond à GATE-OPEN par:

GATE-OPEN-ACK

TransactionID		8096	Identifiant pour faire correspondre ce message à sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

13) En réponse à la commande Modify-Connection, qui indique que l'appel a abouti (c'est-à-dire que l'autre partie a décroché), MTAo envoie le message COMMIT à l'AN. Ce message est envoyé à l'AN à un port UDP donné dans l'objet RSVP-RESV Commit-Entity. Session-Object et Sender Template donnent à l'AN suffisamment d'informations pour identifier la "porte" et pour identifier quelles sont les ressources réservées qui sont engagées.

COMMIT

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination doivent correspondre à ces paramètres pour l'ID de porte.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

14) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) indiquant qu'une connexion avec une qualité de service améliorée a été accordée à cet appel.

QoS-START

Header	Timestamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID donnée dans Gate-Set.
QoS Descriptor	Type	UGS	Description de la QS fournie pour cette connexion.
	Grant interval	10 ms	
	Grant Jitter	2 ms	
	Grant/Interval	1	
	Grant Size	111	
MTA Port	Port	7120	

15) L'AN décide quelle réservation doit être activée et envoie un DSC-REQ au CM pour activer le flux.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Actif (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111

DSC-REQ

DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Actif (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Active(1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

16) Le CM envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

17) L'AN envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

18) L'AN accuse réception du message COMMIT avec:

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

19) Lorsque l'appel est fini, en réponse à une commande Delete-Connection, le MTA envoie un message RSVP-PATH-TEAR à l'AN. Pour chaque réservation RSVP, le MTA envoie un message RSVP-PATH-TEAR séparé.

RSVP-PATH-TEAR

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port identifient le flux RSVP.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

20) L'AN envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé.

QoS-Stop

TimeStamp		<heure>	Heure de l'événement enregistré.
Header	Time Stamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID du message Gate-Set.
SF-ID	SF-ID	1001	Identifiant de flux de service.

21) L'AN, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de portes à l'adresse donnée précédemment dans la commande GATE-SET, qui dans le cas du NCS est l'agent d'appel (*Call Agent*).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		8095	Identifie la GateID au niveau de l'AN distant.
HMAC			Total de contrôle de sécurité pour ce message.

Le CMS répond par:

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message à sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

22) L'AN, à la réception de RSVP-PATH-TEAR, envoie un DSD-REQ au CM indiquant l'identification de flux de service qui doit être supprimée.

DSD-REQ

TransactionID		3
ServiceFlowID		1001
HMAC		

DSD-REQ

TransactionID		4
ServiceFlowID		2001
HMAC		

23) Le CM supprime le Service Flow ID et envoie la réponse à l'AN.

DSD-RSP

TransactionID		3
ServiceFlowID		1001
ConfirmationCode		Succès (0)
HMAC		

DSD-RSP

TransactionID		4
ServiceFlowID		2001
ConfirmationCode		Succès (0)
HMAC		

24) L'AN envoie le RSVP-RESV-TEAR au MTA.

RSVP-RESV-TEAR

Session-Object	Protocol	UDP	Ces paramètres identifient le flux IP qui est en train de se terminer.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	

APPENDICE IV

Exemple d'échange de messages de protocole pour changement de code à mi-appel

Le changement de codec est exécuté par les MTA transmettant un nouveau message RSVP-PATH après échange de signalisation d'appel entre eux pour déterminer quel nouveau codec est utilisé. Le nouveau FlowSpec pour l'appel est décrit dans le RSVP-PATH et doit s'insérer dans l'enveloppe autorisée spécifiée dans le message Gate-Set qui a été précédemment échangé entre les GC et les AN pour cette porte. Le RSVP-PATH inclut la même GateID qui a été précédemment utilisée pour cet appel. Il est à noter que l'INVITE initial pour établir l'appel aurait inclus les codecs dans le SDP pour s'assurer que l'enveloppe autorisée est suffisamment grande pour prendre en charge le changement de codec. Le message RSVP-PATH inclut le FlowSpec pour les deux codecs conformément à l'explication donnée ci-dessous.

IV.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Fait l'objet d'un complément d'étude.

IV.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure IV.1.

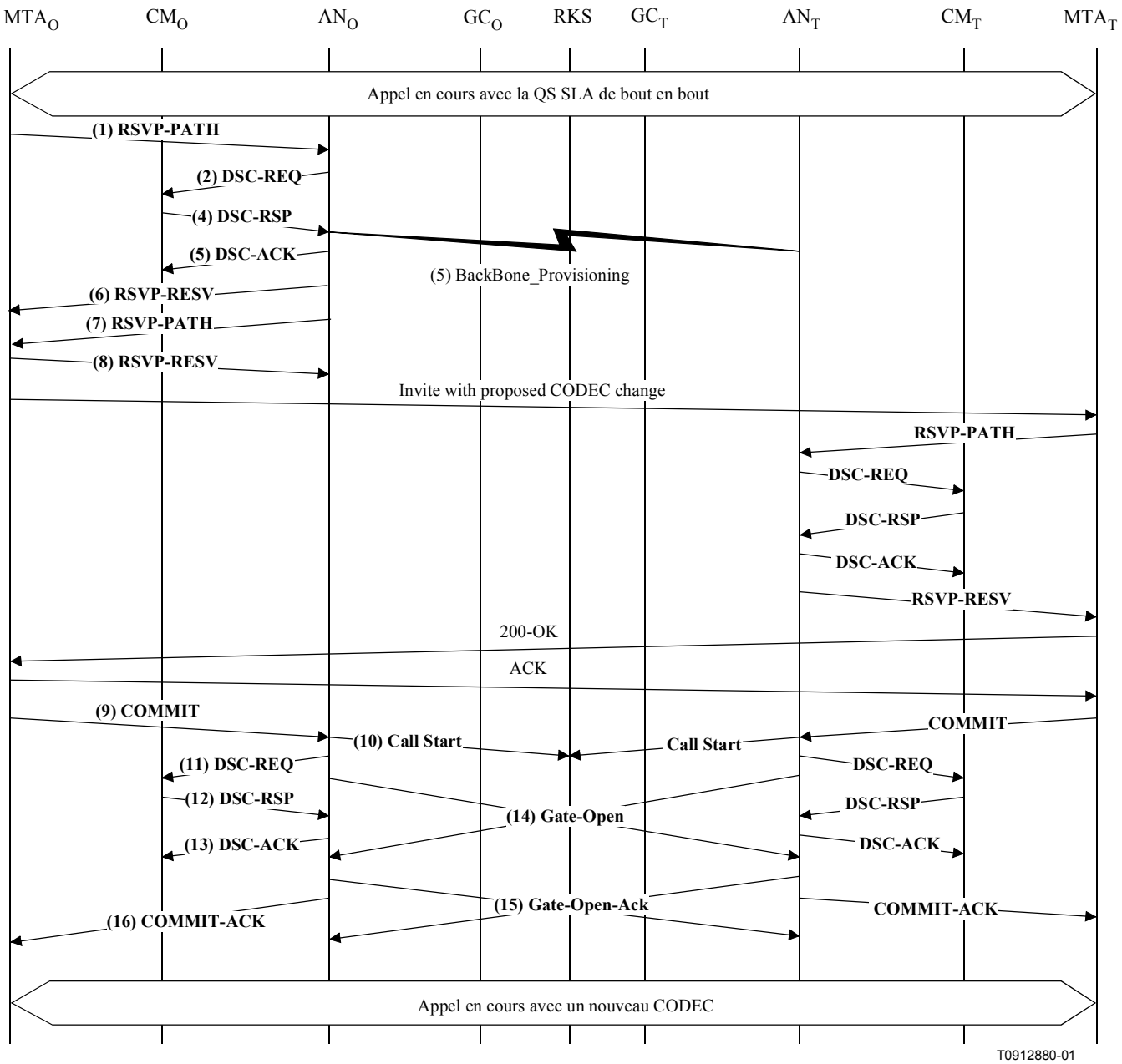


Figure IV.1/J.163 – Signalisation de la QS pour changement de codec

1) MTAo et MTAt sont supposés avoir un appel actif G.728 (paquets 20 ms, tous les 80 octets) lorsque MTAo décide, quelle que soit la raison, qu'un changement de CODEC est nécessaire pour G.711 (10 ms paquets, tous les 120 octets). Après un échange de signalisation initial qui détermine MTAt est capable de gérer le nouveau codec désiré, MTAo envoie un message RSVP-PATH adressé au MTAt, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le LAN de rattachement interceptent, traitent et envoient ce message comme un RSVP-PATH normal, comprenant uniquement la seule série de paramètres de trafic de la borne supérieure donnée dans le Sender-Tspec.

RSVP-PATH

Session-Object	Protocol	UDP	Ces paramètres identifient la session RSVP, font correspondre l'autorisation précédemment demandée par le GateController et sont également utilisés pour les classificateurs QS.
	Destination Address	MTAt	
	Destination Port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Sender-Tspec	b	120	Donnent la borne supérieure pour tous les paramètres de trafic individuels pour les deux flux séparés possibles. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le trajet entre le MTA et l'AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Gate-ID		37 125	Identité de porte qui autorise cette demande.
Component Tspec	b	120	Paramètres de trafic négociés pour le nouveau CODEC demandé pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	Rspec qui correspond au Component Tspec immédiatement précédent.
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7120	
Reverse-Sender Templ	Source Address	MTAt	
	Source Port	7000	

RSVP-PATH

Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés pour le nouveau CODEC demandé pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	0	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
Component Tspec	b	80	Paramètres de trafic négociés pour l'ancien CODEC actuellement utilisé pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec.
	r	4000	
	p	4000	
	m	80	
	M	80	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	4000	Rspec qui correspond au Component Tspec immédiatement précédent.
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7120	
Reverse-Sender Templ	Source Address	MTAt	
	Source Port	7000	
Reverse-Sender-Tspec	b	80	Paramètres de trafic négociés pour l'ancien CODEC actuellement utilisé pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires.
	r	4000	
	p	4000	
	m	80	
	M	80	
	Hdr Suppression	0	
	VAD	off	
Reverse-Rspec	R	4000	
	S	0	

2) L'AN utilise le message RSVP-PATH et calcule les nouveaux paramètres de QS pour la liaison J.112. Etant donné que le flux G.728 s'insère complètement dans une allocation pour G.711, un flux de service séparé n'est pas nécessaire; par conséquent les flux de service existants sont modifiés pour augmenter la bande passante admise. L'AN envoie le DSC-REQ suivant au CM. Ce message est utilisé pour établir les paramètres amont et aval. La Upstream Unsolicited Grant Size (taille d'attribution non sollicitée amont) a été calculée

égale à 120 (du Tspec) plus 18 (préfixe Ethernet) moins 40 (valeur de suppression d'en-tête) plus 13 (préfixe J.112). La suppression d'en-tête, spécifiée comme une longueur de 40 dans le RSVP-PATH, indique 42 octets d'Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est pris dans le paquet RSVP.

DSC-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Active (4) (actif)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	20 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	71
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Active(4) (actif)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	4 000
HMAC		

3) Simultanément avec le message n° 2, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sort du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

4) Le CM vérifie les ressources supplémentaires qu'il lui est demandé d'allouer (par exemple, bande passante de réseau local). Si l'opération aboutit, il renvoie le message DCS-RSP indiquant le succès de l'opération.

DSC-RSP

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

5) A la réception du DSC-RSP, l'AN accuse réception avec un message DSA-ACK.

DSC-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

6) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, l'AN répond au message RSVP-PATH en envoyant un message RSVP-RESV. Le message inclut la borne supérieure des deux Sender-Tspec, amenant les routeurs intermédiaires à allouer des ressources suffisantes pour couvrir l'un ou l'autre flux. Le message RSVP-RESV est envoyé avec l'adresse source de MTAt et l'adresse de destination de MTAo. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lequel la réservation est établie.
	Destination Address	MTAt	
	Destination port	7000	
Filter-Spec	Source Address	MTAo	
	Source Port	7120	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux. Ces valeurs constituent la borne supérieure des deux Tspec donnés dans le RSVP-PATH.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		1	Resource ID précédemment créée pour cette réservation.

7) Si l'adresse du saut précédent diffère de l'adresse source (*Source Address*), il est alors demandé à l'AN de générer un message RSVP-PATH pour réserver les ressources aval au niveau de tous les routeurs intermédiaires. Ce drapeau ne serait réglé que si le MTA n'était pas immédiatement adjacent au CM.

L'AN construit le message RSVP-PATH en utilisant l'information Reverse Path qu'il a reçue du message RSVP-PATH et envoie le message au MTA de départ. Ce message inclut l'objet ResourceID.

RSVP-PATH

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont simulés comme si le message RSVP venait de l'extrémité distante.
	Destination Address	MTAo	
	Destination port	7120	
Sender Templ	Source Address	MTAt	
	Source Port	7000	

RSVP-PATH

Sender-Tspec	b	120	Sender-Tspec venait de Reverse-Sender-Tspec dans le message RSVP-PATH en provenance du MTAo. Ceci identifie les ressources qui seront nécessaires dans le sens aval (de MTAt à MTAo). Ce Tspec est la borne supérieure des deux Tspec individuels envoyés à l'AN, amenant tous les routeurs intermédiaires à allouer suffisamment de ressources pour l'un ou l'autre flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
ResourceID		1	Resource ID précédemment créée pour cette réservation.

8) MTAo, en réponse au RSVP-PATH (7), envoie RSVP-RESV à MTAt. Ce message est envoyé avec "Router-Alert" réglé et tous les routeurs intermédiaires interceptent, traitent et envoient ce message jusqu'à ce qu'il atteigne l'AN.

RSVP-RESV

Session-Object	Protocol	UDP	Session-Object et Sender-Template sont copiés du message RSVP-PATH reçu.
	Destination Address	MTAo	
	Destination port	7120	
Filter-Spec	Source Address	MTAt	
	Source Port	7000	
Flowspec	b	120	Ces données sont également copiées depuis le message RSVP-PATH et spécifient la quantité de ressources réservée pour le flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
	R	12 000	
	S	0	
ResourceID		1	Resource ID, copiée de RSP-PATH.

9) En réponse aux messages de signalisation de bout en bout qui indiquent que la réservation de ressources a réussi aux deux extrémités, MTAo envoie le message Commit à l'AN. Ce message est envoyé à l'AN à un port UDP déterminé via la signalisation d'appel.

Session-Object et Sender Template donnent à l'AN l'information pour vérifier l'ID de porte et pour identifier quelles sont les ressources réservées qui sont engagées.

COMMIT

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination doivent correspondre à ces paramètres pour l'ID de porte.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

10) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) indiquant qu'un Commit a été reçu sur cet appel. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un QoS-Start message.

QoS-START

Header	Timestamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID donnée dans Gate-Set.
QoS Descriptor	Type	UGS	Description de la QS fournie pour cette connexion.
	Grant interval	10 ms	
	Grant Jitter	2 ms	
	Grant/Interval	1	
	Grant Size	111	
MTA Port	Port	7120	

11) L'AN décide quelle réservation doit être activée et envoie un DSC-REQ au CM pour activer le flux.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
HMAC		

12) Le CM envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

13) L'AN envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

14) L'AN envoie le message de coordination de portes à l'AN distant pour l'informer que les ressources à cette extrémité ont été engagées.

GATE-OPEN

TransactionID		74	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	ID de porte (Gate-ID) au niveau de l'AN distant.
Tspec	b	120	Paramètres de trafic engagés effectivement utilisés dans le sens MTAo vers MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Reverse-Tspec	b	120	Paramètres de trafic prévus utilisés dans le sens MTAt vers MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Total de contrôle de sécurité pour ce message.

15) L'AN distant répond à GATE-OPEN par:

GATE-OPEN-ACK

Transaction ID		74	Identifiant pour faire correspondre ce message à sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

16) L'AN accuse réception du message COMMIT avec:

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

APPENDICE V

Exemple d'échange de messages de protocole pour mise en garde d'appel

La mise en garde d'un appel au niveau d'un MTA se fait en envoyant un INVITE au MTA avec les paramètres SDP à 0. Le MTA envoie alors un message COMMIT avec un Flow Spec de 0. Resource ID est également inclus. Ceci permet à l'AN de mettre l'appel en garde selon les ressources admises mais engagera maintenant des ressources zéro pour l'appel. Ceci est effectué avec un échange de messages MAC au niveau de MAC J.112.

V.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Voir Figure V.1.

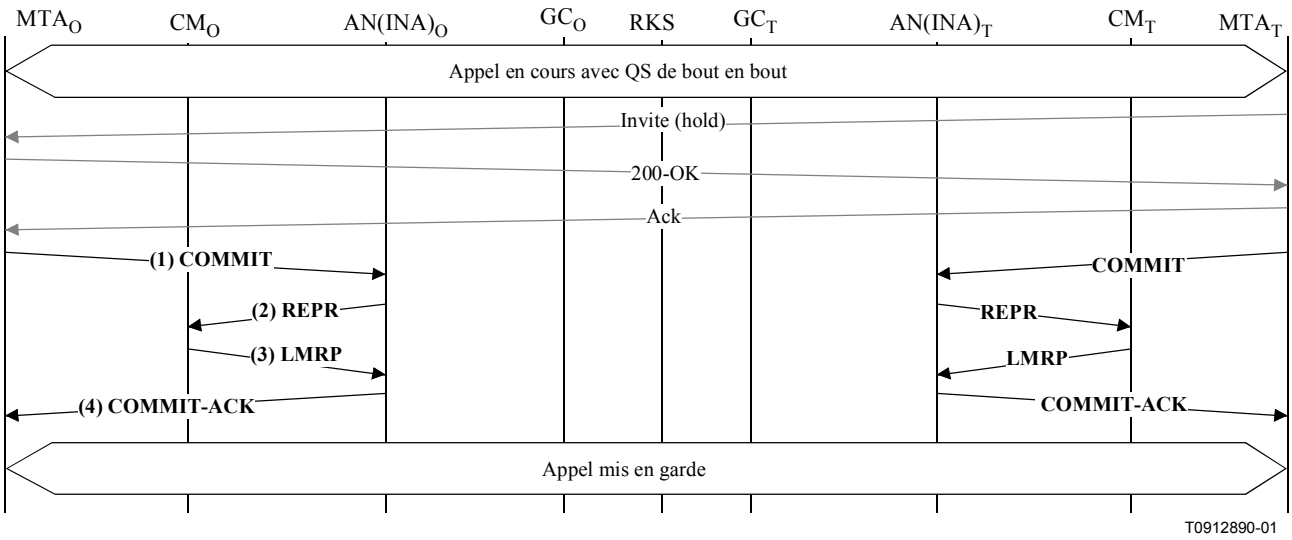


Figure V.1/J.163 – Signalisation de la QS pour mise en garde d'appel

1) Lorsque MTAt décide que l'appel courant doit être mis en garde, il envoie un message INVITE au MTAo. Après un autre échange de signalisation, MTAo envoie un message COMMIT avec un Flowspec vide.

COMMIT

Session-Object	Protocol	UDP	Session-Object et Sender Template vérifient l'identité de la porte.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	
Flowspec	b	0	Un Flowspec est un objet optionnel pour un message COMMIT et indique que les ressources engagées diffèrent d'une certaine quantité des ressources réservées; pour la mise en garde d'appel (*Call Hold*) les ressources amont engagées sont changées en 0.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

COMMIT

Reverse-Flowspec	b	0	Un Flowspec est un objet optionnel pour un message COMMIT et indique que les ressources engagées diffèrent d'une certaine quantité des ressources réservées; pour la mise en garde d'appel (*Call Hold*) les ressources aval engagées sont changées en 0.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

2) ANo envoie un message Reprovision à CMt.

REPR

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <non>
Delete_Reservation_Ids	1 <oui>
New_Downstream_IB_Frequency_included	0 <non>
New_Downstream_OOB_Frequency_included	0 <non>
New_Upstream_Frequency_included	0 <non>
New_Frame_Length_included	1 <oui>
New_Cyclical_Assignment_included	1 <oui>
New_Slot_List_included	0 <non>
New_Frame_Length	0
Number_of_Connections	1
Connection_ID	37 125 <ID de porte>
Cyclic_Assignment	
Fixedrate_Start	0xFFFF
Fixedrate_Dist	0
Fixedrate_Stop	0xFFFF

3) CMt envoie un message Link Management Response montrant que l'opération a réussi.

LMRP

Link_Management_Msg_Number	<Reprovision Message Type Value>

4) ANo accuse réception du message COMMIT avec un message COMMIT-ACK.

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port peuvent aider à faire correspondre l'accusé de réception avec le message COMMIT.
	Destination Address	MTAt	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7120	
Gate-ID		37 125	

V.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure V.2.

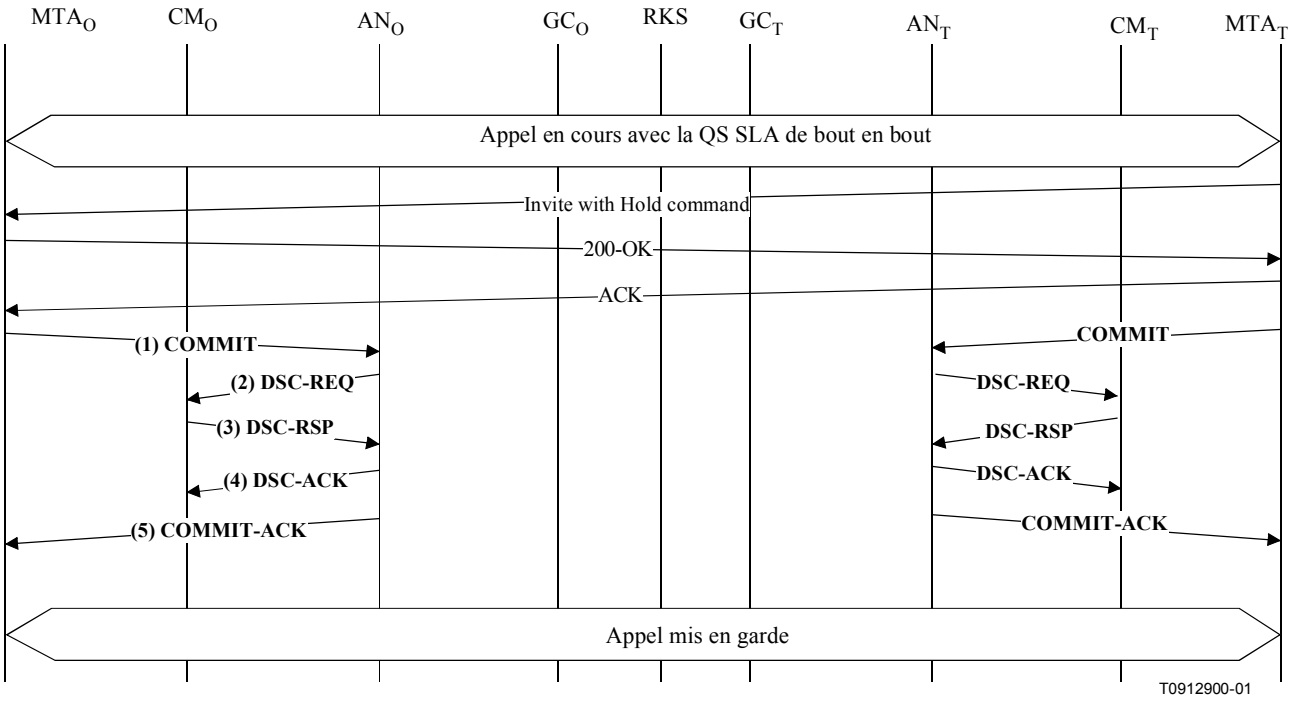


Figure V.2/J.163 – Signalisation de la QS pour mise en garde d'appel

1) Lorsque MTA décide que l'appel en cours doit être mis en garde, il envoie un message COMMIT message avec une bande passante de zéro. Le MTA ne peut pas changer l'ID de session active pendant un message Call Hold Commit.

COMMIT

Session-Object	Protocol	UDP	Session-Object et Sender-Template vérifient l'identité de la porte.
	Destination Address	MTAo	
	Destination port	7120	
Sender Templ	Source Address	MTAt	
	Source Port	7000	
Gate-ID		37 125	
Flowspec	b	0	Ils sont optionnels dans un message COMMIT et indiquent que l'activation diffère d'une certaine valeur de la réservation; dans ce cas l'activation amont désirée est nulle.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

COMMIT

Reverse-Flowspec	b	0	Ils sont optionnels dans un message COMMIT et indiquent que l'activation diffère d'une certaine valeur de la réservation; dans ce cas l'activation aval désirée est nulle.
	r	0	
	p	0	
	m	0	
	M	0	
	R	0	
	S	0	

2) L'AN envoie au CM un message DSC pour désactiver le flux de service et pour désactiver les classificateurs.

DSC-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSC-REQ

DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

3) Le CM envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

4) L'AN envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

5) L'AN envoie un message COMMIT-ACK.

COMMIT-ACK

Session-Object	Protocol	UDP	Session-Object et Sender-Template vérifient l'identité de la porte.
	Destination Address	MTAo	
	Destination port	7120	
Sender Templ	Source Address	MTAt	
	Source Port	7000	
Gate-ID		37 125	

APPENDICE VI

Exemple d'échange de messages de protocole pour mise en instance d'appel

VI.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Fait l'objet d'un complément d'étude.

VI.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure VI.1.

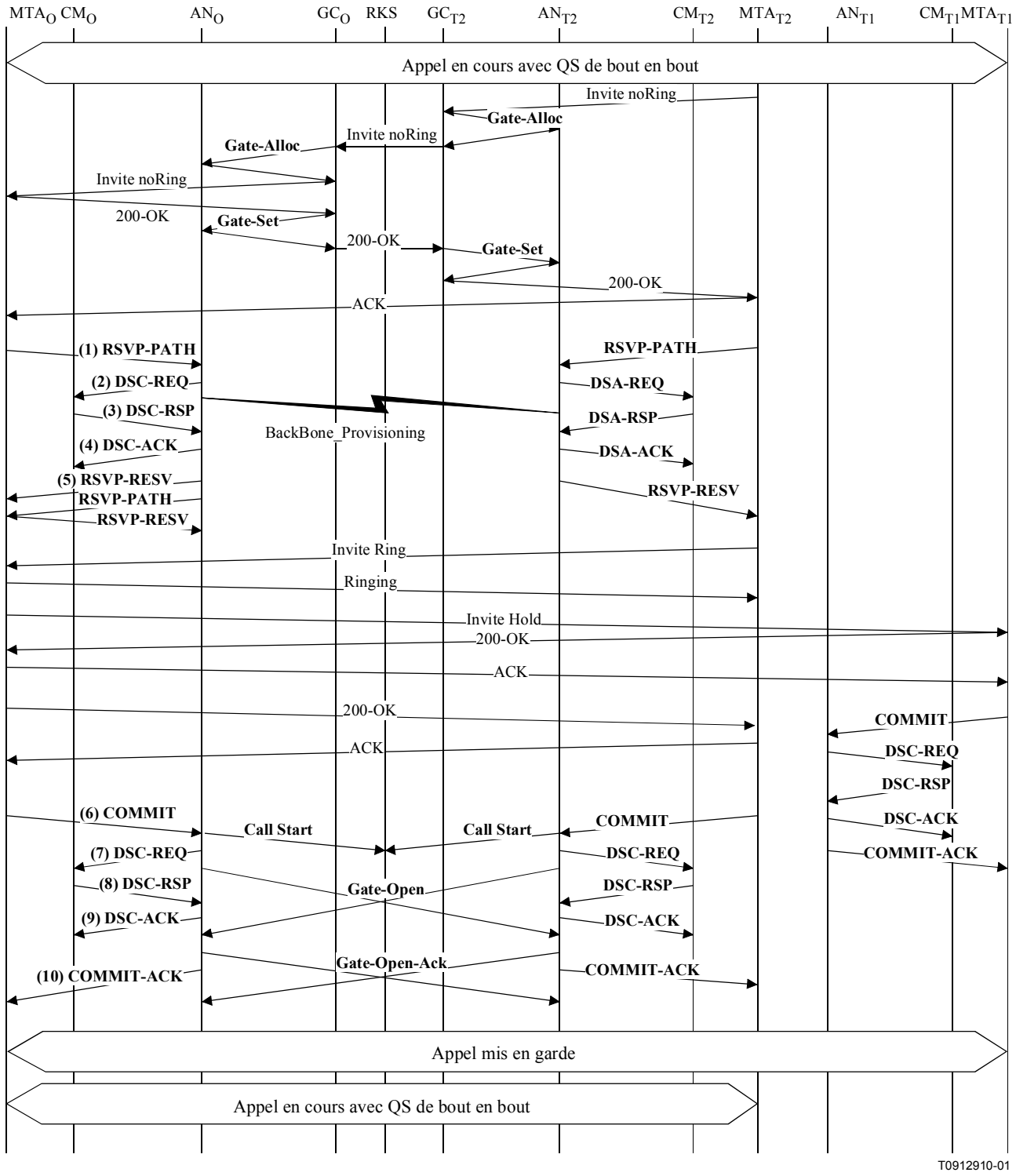


Figure VI.1/J.163 – Signalisation de la QS pour appel en instance

1) MTAo est connecté à MTAt1 et reçoit un appel entrant de MTAt2. Pour cet exemple, supposons que l'appel de MTAt1 a utilisé le port UDP 7120 et une ResourceID 472 assignée. A la réception des informations de signalisation de l'appel, MTAo envoie un message RSVP-PATH, adressé au MTAt2, mais avec le bit Router-Alert mis à 1 dans l'en-tête IP. Les routeurs intermédiaires dans le LAN de rattachement interceptent, traitent et envoient ce

message comme un RSVP-PATH normal, pensant qu'il s'agit d'un flux séparé et allouant des ressources séparées à son intention.

RSVP-PATH

Session-Object	Protocol	UDP	Les paramètres forment le classificateur, correspondant à l'autorisation précédemment envoyée par le contrôleur de porte (*GateController*).
	Destination Address	MTAt2	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source port	7122	
Sender-Tspec	b	120	Paramètres de trafic négociés actuellement demandés pour cet appel. L'AN calcule les paramètres de QS amont réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un objet RSVP standard qui sera interprété par tous les routeurs intermédiaires sur le trajet entre le MTA et l'AN.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	40	
	VAD	off	
Forward Rspec	R	12 000	
	S	0	
Reverse-Session	Protocol	UDP	Nouveaux objets RSVP qui fournissent à l'AN suffisamment d'informations pour calculer les paramètres de trafic aval et pour générer un message RSVP-PATH pour le flux aval.
	Destination Addr	MTAo	
	Destination port	7122	
Reverse-Sender Templ	Source Address	MTAt	
	Source port	0	
Reverse-Sender-Tspec	b	120	Paramètres de trafic négociés effectivement demandés pour cet appel. L'AN calcule les paramètres de QS aval réels en utilisant ces paramètres Tspec et Rspec. Il s'agit d'un nouvel objet RSVP qui sera ignoré par les routeurs intermédiaires.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	Hdr Suppression	0	
	VAD	off	
Reverse-Rspec	R	12 000	
	S	0	
ResourceID		472	Resource ID assignée pour appel existant.
Gate-ID		37 126	Gate-ID pour ce nouvel appel, prendre les ressources à partir des anciennes.

2) L'AN utilise le message RSVP-PATH et calcule les paramètres de QS pour la liaison J.112. Pour cet exemple, supposons que l'appel précédent était conforme à G.711, et par conséquent que les exigences de bande passante sont identiques. Ainsi, le ServiceFlow existant peut être utilisé pour le flux de paquet. L'AN envoie le DSC-REQ suivant au CM, qui établit les nouveaux classificateurs. La suppression d'en-tête, spécifiée comme une longueur de 40 dans le RSVP-PATH, indique les 42 octets de l'en-tête Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est pris dans le paquet RSVP.

DSC-REQ

TransactionID		1
UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3003
	ClassifierChangeAction	Add (0)
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7122
	IPDestinationAddress	MTAt2
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3004
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAt2
	IPDestinationAddress	MTAo
	IPDestinationPort	7122
	IPProtocol	UDP (17)
PayloadHeaderSuppression	ClassifierIdentifier	3003
	ServiceFlowIdentifier	1001
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42octets>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Vérifier (0)
HMAC		

3) Le CM vérifie les ressources qu'il lui est demandé d'allouer (par exemple, espace de table de suppression d'en-tête, identifications de flux de service, espace de table de classificateurs, bande passante de réseau local) et installe les classificateurs. Si l'opération aboutit, il renvoie le message DSC-RSP indiquant le succès de l'opération.

DSC-RSP

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

4) A la réception du DSC-RSP, l'AN accuse réception avec un message DSC-ACK.

DSC-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

5) Une fois que la réservation J.112 est terminée et que la réservation du réseau de base a abouti, l'AN répond au message RSVP-PATH en envoyant un message RSVP-RESV. Le message inclut la ResourceID qui est assignée par l'AN à cette connexion. Le message RSVP-RESV est envoyé avec l'adresse source de MTAt et l'adresse de destination de MTAo. Tous les routeurs intermédiaires intercepteront, traiteront et enverront ce message comme un message RSVP-RESV standard.

RSVP-RESV

Session-Object	Protocol	UDP	Ces champs identifient le flux IP pour lequel la réservation est établie.
	Destination Address	MTAt2	
	Destination port	7000	
Filter-Spec	Source Address	MTAo	
	Source Port	7122	
Flowspec	b	120	Ces champs identifient les ressources réservées pour ce flux.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
ResourceID		472	Resource ID pour cette réservation.

6) En réponse à un crochet commutateur et après avoir effectué la suite de la signalisation avec la partie précédente et la nouvelle partie, MTAo envoie le message COMMIT à l'AN. Ce message est envoyé à l'AN à un port UDP déterminé via la signalisation d'appel.

7) La Session-Object et Sender-Template donnent à l'AN suffisamment d'informations pour identifier la "porte" et pour identifier quelles sont les ressources réservées qui sont engagées. Etant donné qu'aucun Tspec n'est donné dans ce message, toutes les ressources réservées seront activées. Tous les autres flux assignés à la même ResourceID seront désactivés.

COMMIT

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port doivent correspondre à ceux de l'ID de port.
	Destination Address	MTAt2	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7122	
Gate-ID		37 126	

8) L'AN décide quelle réservation doit être activée et envoie un DSC-REQ au CM pour activer le flux.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
Upstream Classifier	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Downstream Classifier	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7120
	IPProtocol	UDP (17)

DSC-REQ

UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3003
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAo
	IPSourcePort	7122
	IPDestinationAddress	MTAt2
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3004
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAt2
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7122
	IPProtocol	UDP (17)
HMAC		

9) Le CM envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

10) L'AN envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

11) L'AN accuse réception du message COMMIT avec:

COMMIT-ACK

Session-Object	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination correspondent à l'ID de porte.
	Destination Address	MTAt2	
	Destination port	7000	
Sender Templ	Source Address	MTAo	
	Source Port	7122	
Gate-ID		37 126	

APPENDICE VII

Exemple d'échange de messages de protocole pour un appel de base DCS de réseau privé à réseau privé d'un MTA intégré

VII.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Voir Figure VII.1.

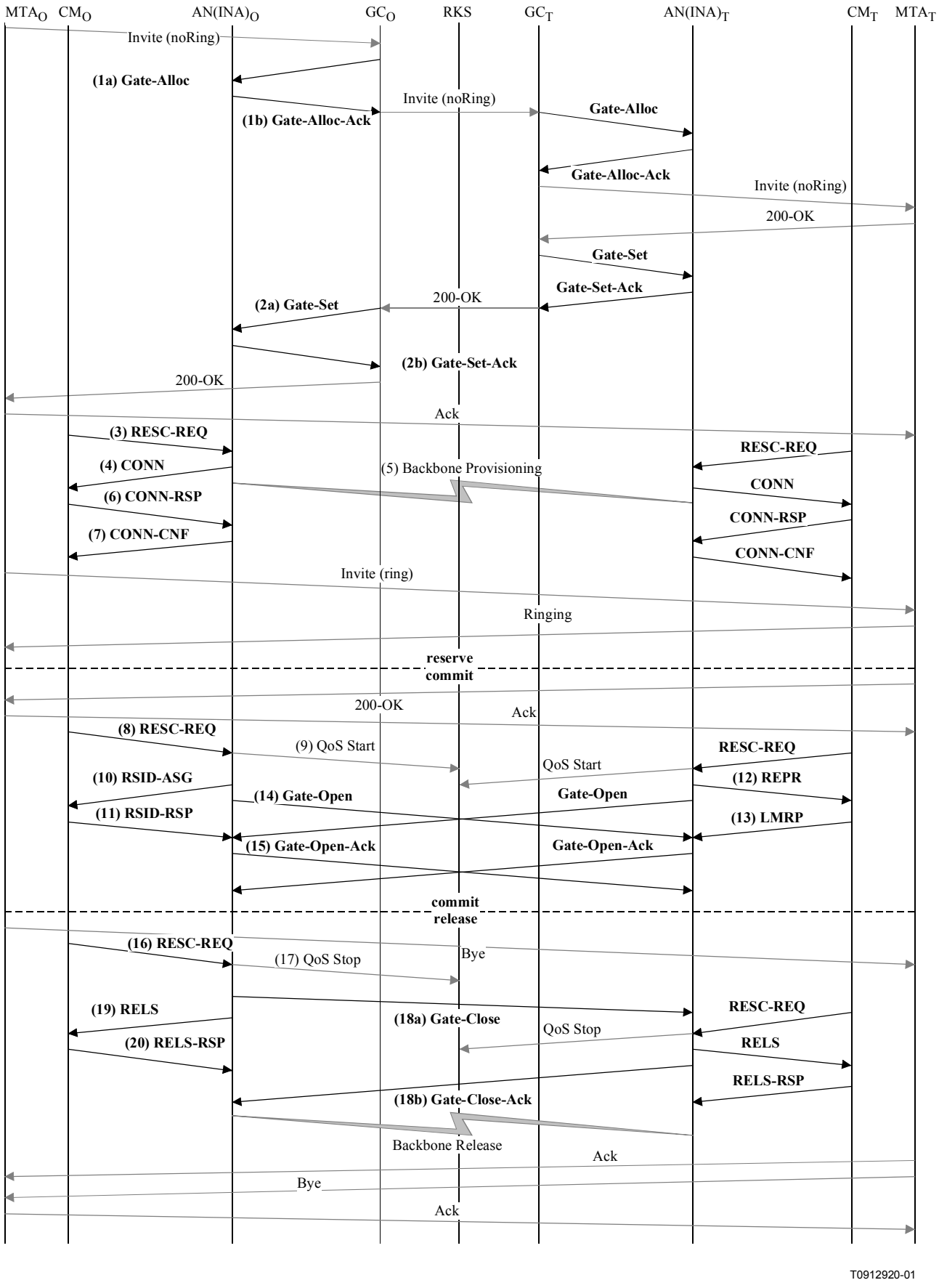


Figure VII.1/J.163 – Flux d'appel de base avec les messages J.112 de l'Annexe A – DCS sur MTA intégrés

1) GCo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo (1a).

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count		4	Nombre de portes maximales permises pour cet abonné.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de portes allouées (1b).

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Répond à la demande de ressources totales utilisées par ce point d'extrémité.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de portes établies pour cet abonné.
Gate Coordination Port		4104	Port UDP au niveau duquel l'AN écoutera les messages de coordination de portes.

2) GCo, après des échanges supplémentaires de signalisation, donne à ANo l'autorisation d'initier la phase de réservation du procédé d'allocation de ressources pour le nouveau flux J.112 (2a).

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	Address	ANt	Information nécessaire pour coordonner les portes.
	Port	2052	
	Remote Gate-ID	1273	
	Security Key	<clé>	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la Commande Gate-Set avec un accusé de réception (2b).

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Réponse à demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de portes établies pour cet abonné.

3) MTAo, à la réception d'une information d'appel de signalisation, calcule les paramètres de QS pour la liaison J.112. Il utilise l'interface de la couche MAC pour donner l'ordre à CMo d'envoyer un message Resource Request à ANo. En supposant qu'un débit amont de 3,088 Mbit/s soit utilisé et que les paquets IP soient encapsulés en utilisant DirectIP, les ressources amont sont calculées comme suit. Un paquet IP d'une taille de 120 octets (du Tspec) y compris l'en-queue de 5 octets AAL 5 occupe trois cellules ATM. Ainsi, en utilisant le mode Reservation Access ANo doit accorder 3 intervalles toutes les 10 ms. En mode d'accès à débit fixe, une affectation cyclique de 3 intervalles à la fois est nécessaire avec une distance maximale de 60 intervalles. La bande passante demandée est de 360 intervalles par 1200 ms.

RESC-REQ

Resource_Request_ID	0x01
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	1 <oui>
Admit_Flag	1 <réservation demandée>
Flowspec_DS_included	1 <oui>
Priority_included	0 <non>
Max_packet_size_included	1 <oui>
Session_binding_US_included	0 <non>
Release_requested	0 <non>
Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	1 <oui>
Requested_Bandwidth	360 <intervalles par 1200 ms>
Maximum_Distance_Between_Slots	60 <intervalles>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <non>
Flowspec_DS_included	1 <oui>
Session_binding_DS_included	0 <non>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

4) ANo détecte la demande de ressources et ne peut faire correspondre l'ID de connexion incluse avec un flux J.112 existant. Il vérifie alors l'autorisation en cherchant une ID de porte qui corresponde à l'ID de connexion. Si la porte est déjà réglée, ANo est capable de vérifier que les ressources demandées se trouvent dans les limites de l'enveloppe autorisée. Si tel est le cas, ANo envoie le message Connect suivant à CMo. Ce message est utilisé pour établir les paramètres amont et aval. Toutefois, aucune ressource n'est allouée dans le message Connect. Cela indique au CMo que les ressources pour ce flux J.112 sont réservées mais ne sont pas encore engagées.

CONN

Connection_ID	37 125 <Gate ID>
Session_number	<non utilisé>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <oui>
IPv6_add	0 <non>
Priority_included	0 <non>
Flowspec_DS_included	0 <non>
Session_binding_US_included	0 <non>
Session_binding_DS_included	0 <non>
Encapsulation_included	1 <oui>
DS_multiprotocol_CBD_included	0 <non>
Resource_number	0x01
Connection_Control_Field	
DS_ATM_CBD_included	0 <non>
DS_MPEG_CBD_included	1 <oui>
US_ATM_CBD_included	1 <oui>
Upstream_Channel_Number	0x1
Slot_list_included	0 <non>
Cyclic_assignment	0 <non>
Frame_Length	0 <non>
Maximum_Contention_Access_Message_Length	1 <intervalles>
Maximum_Reservation_Access_Message_Length	50 <intervalles>
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20 000 000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Connection_control_field2	
Upstream_modulation_included	1 <oui>
Upstream_Modulation	QPSK (1)

5) Simultanément avec le message n° 4, ANo initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à ANo toute notification nécessaire indiquant que la réservation a abouti.

6) CMo vérifie les ressources qu'il lui est demandé d'allouer (par exemple, contexte de suppression d'en-tête, ID de connexion, contexte de classificateur) et installe les classificateurs. Si l'opération aboutit, il retourne le message Connect Response indiquant la réussite de cette opération.

CONN-RSP

Connection_ID	37 125 <ID de porte>

7) A la réception du message Connect Response, ANo accuse réception avec un message Connect Confirm.

CONN-CNF

Connection_ID	37 125 <ID de porte>

8) En réponse aux messages de signalisation qui indiquent que l'appel a été établi (c'est-à-dire que l'autre partie a décroché), MTAo utilise l'interface de la couche MAC J.112 pour initier l'engagement des ressources réservées. Cela se fait via l'envoi par CMo d'un message Resource Request.

RESC-REQ

Resource_Request_ID	0x02
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	1 <oui>
Admit_Flag	0 <engagement demandé>
Flowspec_DS_included	1 <oui>
Priority_included	0 <non>
Max_packet_size_included	1 <oui>
Session_binding_US_included	0 <non>
Release_requested	0 <non>
Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	1 <oui>
Requested_Bandwidth	360 <intervalles par 1200 ms>
Maximum_Distance_Between_Slots	60 <intervalles>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <non>
Flowspec_DS_included	1 <oui>
Session_binding_DS_included	0 <non>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

9) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant qu'une qualité de service améliorée a été accordée à cet appel. Le format de ce message est décrit dans UIT-T J.164.

10) L'AN peut engager les ressources réservées en utilisant le mode Fixed-rate Acces (accès à débit réduit) ou le mode Reservation Access (accès de réservation). A la réception du message Resource Request, il a besoin d'envoyer les messages de couche MAC appropriés pour établir un flux J.112.

Pour cet exemple, il est supposé que ANo décide d'utiliser le mode Reservation Access tandis que ANt engage les ressources en mode d'accès à débit fixe.

Une superposition continue est utilisée pour prendre en charge le CBR comme caractéristique de ce trafic. Pour commencer la transmission ANo envoie un message Reservation ID Assignment.

RSID-ASG

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <intervalles>
GFC_10_Slots	3 <intervalles>
GFC_01_Slots	1 <intervalles>

11) CMo envoie un message Reservation ID Response montrant que l'opération a réussi.

RSID-RSP

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

12) ANt côté arrivée de l'appel a décidé de fournir les ressources demandées en utilisant le mode accès à débit fixe. Pour engager les ressources et pour commencer la transmission ANt envoie un message Reprovision à CMt.

REPR

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <non>
Delete_Reservation_IDs	0 <non>
New_Downstream_IB_Frequency_included	0 <non>
New_Downstream_OOB_Frequency_included	0 <non>
New_Upstream_Frequency_included	0 <non>
New_Frame_Length_included	1 <oui>
New_Cyclical_Assignment_included	1 <oui>
New_Slot_List_included	0 <non>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	1273 <ID de porte>

REPR

Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

13) CMt envoie un message Link Management Response montrant que l'opération a réussi.

LMRP

Link_Management_Msg_Number	<Reprovision Message Type Value>

14) ANo envoie le message de coordination de portes à l'ANt distant pour l'informer que les ressources au niveau de l'extrémité locale ont été engagées.

GATE-OPEN

TransactionID		72	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	Gate-ID au niveau de l'AN recevant ce message.
Tspec	b	120	Paramètres de trafic utilisés réellement pour les ressources engagées pour le flux dans le sens MTAo vers MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Reverse Tspec	b	120	Paramètres de trafic prévus d'être utilisés pour le flux dans le sens MTAt vers MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Total de contrôle de sécurité pour ce message.

15) A la réception du message GATE-OPEN de l'ANt distant, ANo répond avec un GATE-OPEN-ACK.

GATE-OPEN-ACK

TransactionID		8096	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

16) Lorsque l'appel est fini MTAo utilise l'interface de la couche MAC J.112 pour libérer les ressources réservées. Cela se fait via l'envoi d'un message Resource Request par CMo.

RESC-REQ

Resource_Request_ID	0x04
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	0 <non>
Admit_Flag	0

RESC-REQ

Flowspec_DS_included	0 <non>
Priority_included	0 <non>
Max_packet_size_included	0 <non>
Session_binding_US_included	0 <non>
Release_requested	1 <oui>
Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	0 <non>
Requested_Bandwidth	0
Maximum_Distance_Between_Slots	0
Encapsulation	DirectIP (1)

17) ANo envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé. Le format de ce message d'événement est décrit dans UIT-T J.164.

18) ANo, à la réception de demande de libération de ressources, envoie le message de coordination de portes à l'adresse donnée précédemment dans la commande GATE-SET, qui dans le cas de DCS est ANt desservant MTAt (18a).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
Gate-ID		1273	GateID au niveau de l'élément de réseau recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

ANt répond avec un message GATE-CLOSE-ACK (18b).

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

19) ANo répond au message Resource Request en envoyant un message Release au CMo indiquant le flux J.112 qui doit être supprimé.

RELS

Number_of_Connections	1
Connection_ID	37 125 <ID de porte>

20) CMo génère le flux J.112 et envoie Release Response à ANo.

RELS-RSP

Connection_ID	37 125 <ID de porte>

VII.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figure VII.2.

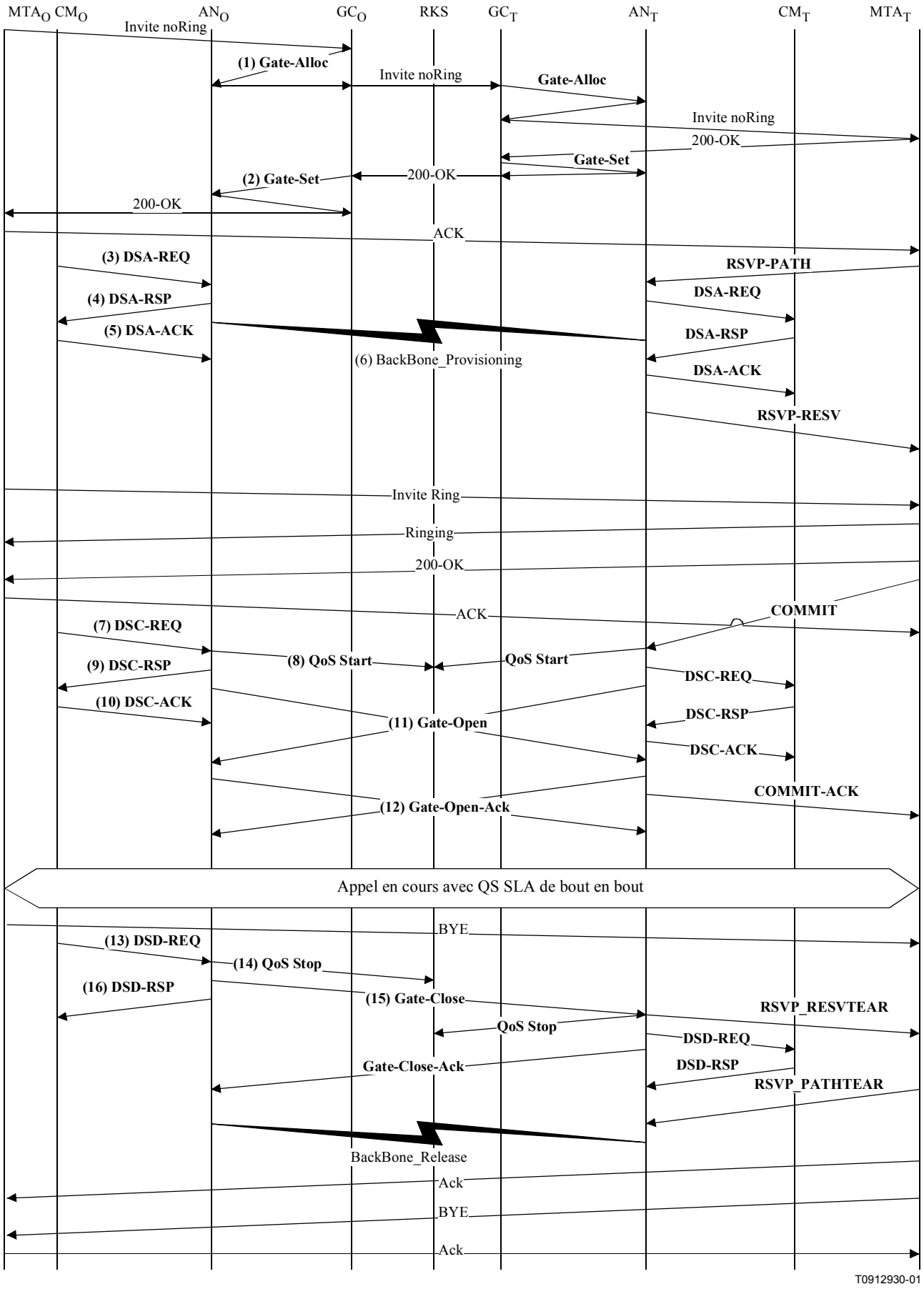


Figure VII.2/J.163 – Flux d'appel de base – MTA intégré

1) GCo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo.

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Activity-Count		4	Nombre maximal de connexions permises par le client.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de connexions actives.

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de connexions établies par ce client.

2) GCo, après des échanges supplémentaires de signalisation, donne à l'ANo l'autorisation d'admettre la nouvelle connexion.

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	AN Address	ANt	Information nécessaire pour coordonner les portes.
	AN Port	2052	
	Remote Gate-ID	1273	
	Security Key	<clé>	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

3) ANo répond à la commande Gate Set-up avec un accusé de réception

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de connexions établies par ce client.

4) MTAo, à la réception d'une information d'appel de signalisation, calcule les paramètres de QS pour la liaison J.112. Il utilise l'interface de l'Annexe E de l'Annexe B/J.112 avec le CM pour envoyer le DSA-REQ suivant à l'AN. Ce message est utilisé pour établir les paramètres amont et aval. La Upstream Unsolicited Grant Size (taille d'attribution non sollicitée amont) a été calculée égale à 120 (du SDP) plus 18 (préfixe Ethernet) moins 40 (valeur de suppression d'en-tête) plus 13 (préfixe J.112). Suppression d'en-tête indique les 42 octets de l'en-tête Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est inclus dans le DSA-REQ.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37 125
DownstreamServiceFlow	ServiceFlowReference	2
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37 125
UpstreamPacketClassification	ServiceFlowReference	1
	PacketClassifierReference	1
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSA-REQ

DownstreamPacketClassification	ServiceFlowReference	2
	PacketClassifierReference	2
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
PayloadHeaderSuppression	ClassifierReference	1
	ServiceFlowReference	1
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42octets>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Vérifier (0)
AuthorizationBlock		37 125
HMAC		

5) L'AN vérifie l'autorisation, en cherchant une porte avec l'ID de porte correspondant à la valeur dans AuthBlock et vérifie les ressources qu'il lui est demandé d'allouer (par exemple, espace de table de suppression d'en-tête, identifications de flux de service, espace de table de classificateurs) et installe les classificateurs. Si l'opération aboutit, il renvoie le message DSA-RSP indiquant le succès de l'opération.

DSA-RSP

TransactionID		1
ConfirmationCode		Succès (0)
UpstreamServiceFlow	ServiceFlowReference	1
	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37 125

DSA-RSP

DownstreamServiceFlow	ServiceFlowReference	2
	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37 125
UpstreamPacketClassification	ServiceFlowReference	1
	PacketClassifierReference	1
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowReference	2
	PacketClassifierReference	2
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

6) A la réception du DSA-RSP, le CM accuse réception avec un message DSA-ACK.

DSA-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

7) Simultanément avec le message n° 4, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

8) En réponse aux messages de signalisation qui indiquent que l'appel a été effectué (c'est-à-dire que l'autre partie a décroché), MTAo utilise l'interface de l'Annexe E de l'Annexe B/J.112 pour activer les ressources admises. Cela se fait par l'intermédiaire d'une commande DSC-REQ à l'AN.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	Request/TransmissionPolicy	0x00000017
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MTAt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAt
	IPSourcePort	7000
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

9) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) indiquant qu'un Commit a été reçu sur cet appel. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un message QoS-Start:

QoS-START

Header	Timestamp	< heure >	Heure de l'événement enregistré.
	Billing Correlation ID	< chaîne >	Correlation ID donnée dans Gate-Set.
QoS Descriptor	Type	UGS	Description de la QS fournie pour cette connexion.
	Grant interval	10 ms	
	Grant Jitter	2 ms	
	Grant/Interval	1	
	Grant Size	111	
MTA Port	Port	7120	

10) L'AN envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

11) Le CM envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

12) L'AN envoie le message de coordination de portes à l'AN distant pour l'informer que les ressources à cette extrémité ont été engagées.

GATE-OPEN

TransactionID		72	Identifiant pour faire correspondre ce message à sa réponse.
Gate-ID		1273	Gate-ID au niveau de l'AN distant.
Tspec	b	120	Paramètres de trafic engagés effectivement utilisés dans le sens MTAo vers MTAt.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
Reverse-Tspec	b	120	Paramètres de trafic prévus utilisés dans le sens MTAt vers MTAo.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
HMAC			Total de contrôle de sécurité pour ce message.

13) L'AN distant répond à GATE-OPEN par:

GATE-OPEN-ACK

TransactionID		72	Identifiant pour faire correspondre ce message avec sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

14) Lorsque l'appel est fini le MTA utilise l'interface de l'Annexe E de l'Annexe B/J.112 pour supprimer les flux de service, en envoyant un message DSD-REQ à l'AN.

DSD-REQ

TransactionID		3
ServiceFlowID		1001
HMAC		

DSD-REQ

TransactionID		4
ServiceFlowID		2001
HMAC		

15) L'AN envoie la notification au serveur d'archivage pour indiquer que l'appel est terminé. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un message QoS-Stop; se reporter à UIT-T J.164.

QoS-Stop

TimeStamp		<heure>	Heure de l'événement enregistré.
Header	Time Stamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID du message Gate-Set.
SF-ID	SF-ID	1001	Identifiant de flux de service.

16) L'AN, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de portes à son AN correspondant desservant MTAt.

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
Gate-ID		1273	Identifie la Gate-ID au niveau de l'AN distant.
HMAC			Total de contrôle de sécurité pour ce message.

L'AN distant répond par:

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

17) L'AN supprime les identifications de flux de service et envoie la réponse au CM.

DSD-RSP

TransactionID		3
ServiceFlowID		1001
ConfirmationCode		Succès (0)
HMAC		

DSD-RSP

TransactionID		4
ServiceFlowID		2001
ConfirmationCode		Succès (0)
HMAC		

APPENDICE VIII

Exemple d'échange de messages de protocole pour appel de base NCS pour MTA intégré

VIII.1 Exemple de flux d'appel avec les messages J.112 de l'Annexe A

Voir Figure VIII.1.

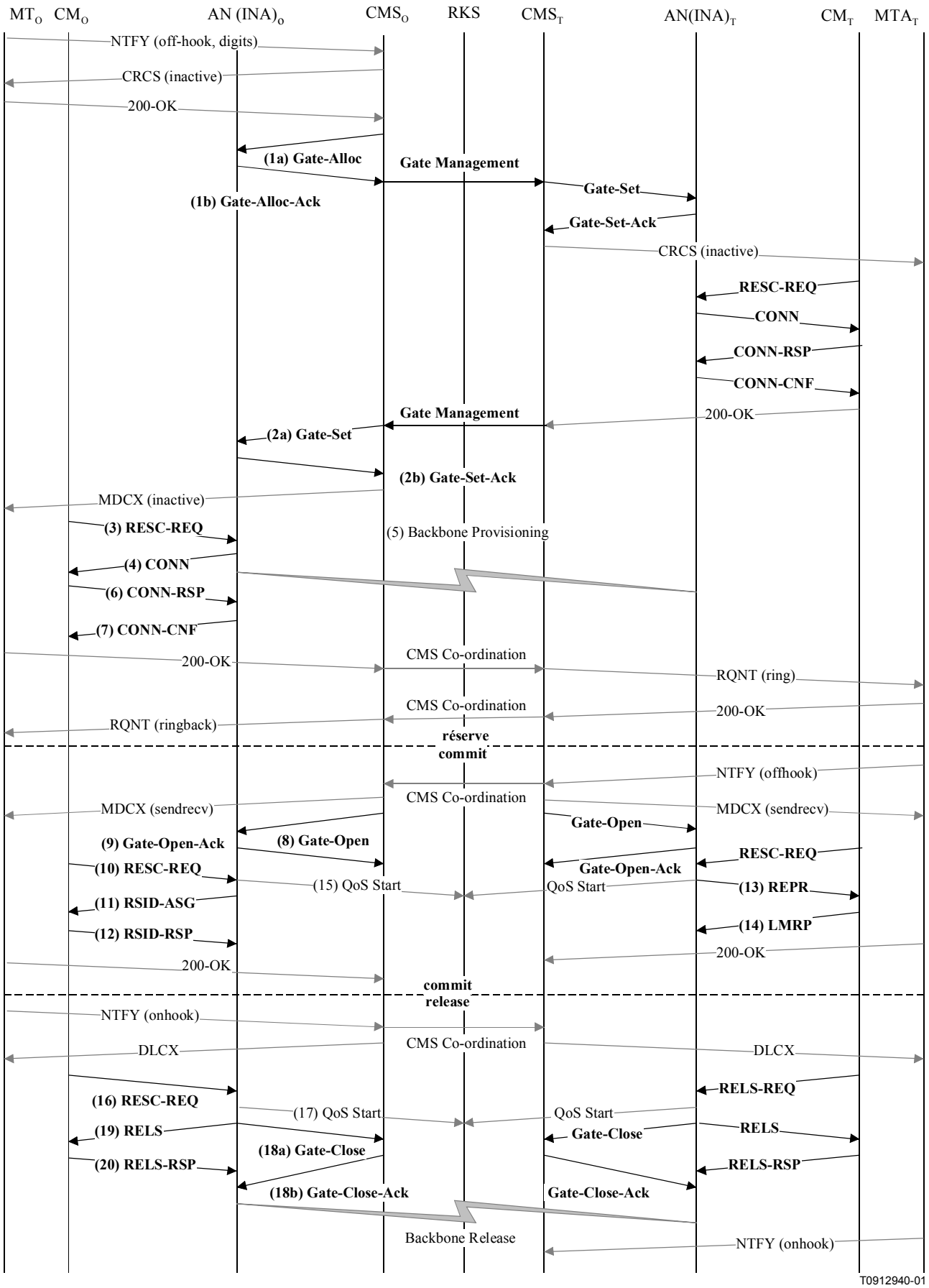


Figure VIII.1/J.163 – Flux d'appel de base avec les messages J.112 de l'Annexe A – NCS sur MTA intégrés

1) GCo/CMSo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo (1a).

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce point d'extrémité.
Activity-Count		4	Nombre de portes maximales permises pour cet abonné.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de portes allouées (1b).

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Répond à la demande de ressources totales utilisées par ce point d'extrémité.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de portes établies pour cet abonné.

2) GCo/CMSo, après des échanges supplémentaires de signalisation, donne à ANo l'autorisation d'initier la phase de réservation du procédé d'allocation de ressources pour le nouveau flux J.112 (2a).

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	Address	CMSo	Information nécessaire pour coordonner les portes. Il est à noter que CMSo s'est donné comme l'entité pour échanger les messages de coordination de portes. La valeur du drapeau indique qu'il convient que l'AN n'envoie pas de message Gate-Open lorsqu'il reçoit un COMMIT en provenance du MTA, mais attend encore pour recevoir un message Gate-Open de CMSo.
	Port	2052	
	Remote Gate-ID	8095	
	Security Key	<clé>	
	Flag	No-gate-open	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la commande Gate Set-up avec un accusé de réception (2b).

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande de spécification de la porte précédemment allouée.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de portes établies pour cet abonné.

3) MTAo, à la réception d'une commande Modify-Connection, calcule les paramètres de QS pour la liaison J.112. Il utilise l'interface de la couche MAC pour donner l'ordre à CMo d'envoyer un message Resource Request à ANo. En supposant qu'un débit amont de 3,088 Mbit/s soit utilisé et que les paquets IP soient encapsulés en utilisant DirectIP, les ressources amont sont calculées comme suit. Un paquet IP d'une taille de 120 octets (du Tspec) y compris l'en-queue de 5 octets AAL 5 occupe trois cellules ATM. Ainsi, en utilisant le mode Reservation Access, l'AN doit accorder 3 intervalles toutes les 10 ms. En mode d'accès à débit fixe, une affectation cyclique de 3 intervalles à la fois est nécessaire avec une distance maximale de 60 intervalles. La bande passante demandée est de 360 intervalles par 1200 ms.

RESC-REQ

Resource_Request_ID	0x01
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	1 <oui>
Admit_Flag	1 <réservation demandée>
Flowspec_DS_included	1 <oui>
Priority_included	0 <non>
Max_packet_size_included	1 <oui>
Session_binding_US_included	0 <non>
Release_requested	0 <non>
Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	1 <oui>
Requested_Bandwidth	360 <intervalles par 1200 ms>
Maximum_Distance_Between_Slots	60 <intervalles>
Encapsulation	DirectIP (1)
Aux_Control_Field	
Pv6_Add	0 <non>
Flowspec_DS_included	1 <oui>
Session_binding_DS_included	0 <non>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

4) ANo détecte le Resource Request et ne peut pas faire correspondre l'ID de connexion incluse avec un flux J.112 existant. Ainsi, il vérifie l'autorisation en cherchant une ID de porte qui corresponde à l'ID de connexion. Si la porte est déjà réglée, ANo est capable de vérifier que les ressources demandées se trouvent dans les limites de l'enveloppe autorisée. Si tel est le cas, ANo envoie le message Connect suivant à CMo. Ce message est utilisé pour établir les paramètres amont et aval. Toutefois, aucune ressource n'est allouée dans le message Connect. Cela indique au CMo que les ressources pour ce flux J.112 sont réservées mais ne sont pas encore engagées.

CONN

Connection_ID	37 125 <ID de porte>
Session_number	<non utilisé>
Connection_Control_Field_Aux	
Connection_control_field2_included	1 <oui>
IPv6_add	0 <non>
Priority_included	0 <non>
Flowspec_DS_included	0 <non>
Session_binding_US_included	0 <non>
Session_binding_DS_included	0 <non>
Encapsulation_included	1 <oui>
DS_multiprotocol_CBD_included	0 <non>
Resource_number	0x01
Connection_Control_Field	
DS_ATM_CBD_included	0 <non>
DS_MPEG_CBD_included	1 <oui>
US_ATM_CBD_included	1 <oui>
Upstream_Channel_Number	0x1
Slot_list_included	0 <non>
Cyclic_assignment	0 <non>
Frame_Length	0 <non>
Maximum_Contention_Access_Message_Length	1 <intervalles>
Maximum_Reservation_Access_Message_Length	50 <intervalles>
Downstream_MPEG_CBD	
Downstream_Frequency	472 000 000 <Hz>
Program_Number	0xA437
Upstream_ATM_CBD	
Upstream_Frequency	20 000 000 <Hz>
Upstream_VPI	0x01
Upstream_VCI	0x54AC
MAC_Flag_Set	0x01
Upstream_Rate	Upstream_3.088M
Encapsulation	DirectIP (1)
Connection_control_field2	
Upstream_modulation_included	1 <oui>
Upstream_Modulation	QPSK (1)

5) Simultanément avec le message n° 4, ANo initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à ANo toute notification nécessaire indiquant que la réservation a abouti.

6) CMo vérifie les ressources qu'il lui est demandé d'allouer (par exemple, contexte de suppression d'en-tête, ID de connexion, contexte de classificateur) et installe les classificateurs. Si l'opération aboutit, il retourne le message Connect Response indiquant la réussite de cette opération.

CONN-RSP

Connection_ID	37 125 <ID de porte>

7) A la réception du message Connect Response, ANo accuse réception avec un message Connect Confirm.

CONN-CNF

Connection_ID	37 125 <ID de porte>

8) CMSo envoie le message de coordination de portes à ANo pour l'informer que les ressources devraient être engagées. Si ANo ne reçoit pas de message Resource Request de CMo dans un temps raisonnable, il révoque l'autorisation de porte.

GATE-OPEN

TransactionID		8096	Identifiant pour faire correspondre ce message avec sa réponse.
Gate ID		37 125	Gate-ID au niveau de l'AN recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

9) ANo répond à GATE-OPEN par a GATE-OPEN-ACK

GATE-OPEN-ACK

TransactionID		8096	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

10) En réponse à une commande Modify-Connection, que l'appel a été établi (c'est-à-dire que l'autre partie a décroché), MTAo utilise l'interface de la couche MAC J.112 pour initier l'engagement des ressources réservées. Cela se fait via l'envoi d'un message Resource Request par le CMo.

RESC-REQ

Resource_Request_ID	0x02
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	1 <oui>
Admit_Flag	0 <engagement demandé>
Flowspec_DS_included	1 <oui>
Priority_included	0 <non>
Max_packet_size_included	1 <oui>
Session_binding_US_included	0 <non>
Release_requested	0 <non>

RESC-REQ

Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	1 <oui>
Requested_Bandwidth	360 <intervalles par 1200 ms>
Maximum_Distance_Between_Slots	60 <intervalles>
Encapsulation	DirectIP (1)
Aux_Control_Field	
IPv6_Add	0 <non>
Flowspec_DS_included	1 <oui>
Session_binding_DS_included	0 <non>
Frame_Length	3
Flowspec_DS	
Max_Packet_Size	120
Average_Bitrate	12 000
Jitter	0 <ms>

11) L'AN peut engager les ressources réservées en utilisant le mode Fixed-rate Acces (accès à débit réduit) ou le mode Reservation Access (accès de réservation). A la réception du message COMMIT, il a besoin d'envoyer les messages de couche MAC appropriés pour établir un flux J.112.

Pour cet exemple, il est supposé que ANo décide d'utiliser le mode Reservation Access tandis que ANt engage les ressources en mode d'accès à débit fixe.

Une superposition continue est utilisée pour prendre en charge le CBR comme caractéristique de ce trafic. Pour commencer la transmission ANo envoie un message Reservation ID Assignment.

RSID-ASG

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>
Piggy_Back_Request_Values	
Continuous_Piggy_Back_Timeout	4 <36 ms>
GFC_11_Slots	9 <intervalles>
GFC_10_Slots	3 <intervalles>
GFC_01_Slots	1 <intervalles>

12) CMo envoie un message Reservation ID Response montrant que l'opération a réussi.

RSID-RSP

Connection_ID	37 125 <ID de porte>
Reservation_ID	0x1234
Grant_Protocol_Timeout	15 <ms>

13) ANt côté arrivée de l'appel a décidé de fournir les ressources demandées en utilisant le mode accès à débit fixe. Pour engager les ressources et pour commencer la transmission ANt envoie un message Reprovision à CMt.

REPR

Reprovision_Control_Field	
Reprovision_Control_Aux_Field_included	0 <non>
Delete_Reservation_IDs	0 <non>
New_Downstream_IB_Frequency_included	0 <non>
New_Downstream_OOB_Frequency_included	0 <non>
New_Upstream_Frequency_included	0 <non>
New_Frame_Length_included	1 <oui>
New_Cyclical_Assignment_included	1 <oui>
New_Slot_List_included	0 <non>
New_Frame_Length	3
Number_of_Connections	1
Connection_ID	8095 <ID de porte>
Cyclic_Assignment	
Fixedrate_Start	0x0000
Fixedrate_Dist	60
Fixedrate_Stop	0xFFFF

14) CMt envoie un message Link Management Response montrant que l'opération a réussi.

LMRP

Link_Management_Msg_Number	<Reprovision Message Type Value>

15) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) en indiquant qu'une qualité de service améliorée a été accordée à cet appel. Le format de ce message est décrit dans UIT-T J.164.

16) Lorsque l'appel est fini, en réponse à une commande Delete-Connection, MTAo utilise l'interface de la couche MAC J.112 pour libérer les ressources réservées. Cela se fait via l'envoi d'un message Resource Request par le CMo.

RESC-REQ

Resource_Request_ID	0x04
Connection_ID	37 125 <ID de porte>
Field	
Aux_Control_Field_included	0 <non>
Admit_Flag	0
Flowspec_DS_included	0 <non>
Priority_included	0 <non>
Max_packet_size_included	0 <non>
Session_binding_US_included	0 <non>
Release_requested	1 <oui>
Reservation_ID_requested	0 <non>
Cyclic_Assignment_needed	0 <non>
Requested_Bandwidth	0
Maximum_Distance_Between_Slots	0
Encapsulation	DirectIP (1)

17) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) que l'appel est terminé. Le format de ce message est décrit dans UIT-T J.164.

18) ANo, a la réception du message Resource Request, envoie le message de coordination de portes à l'adresse donnée précédemment dans la commande GATE-SET, qui dans le cas du NCS est l'agent d'appel (*Call Agent*) (18a).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
Gate-ID		8095	Gate-ID au niveau de l'élément de réseau (ici: CMS) recevant ce message.
HMAC			Total de contrôle de sécurité pour ce message.

CMSo répond avec un message GATE-CLOSE-ACK (18b).

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa demande.
HMAC			Total de contrôle de sécurité pour ce message.

19) ANo répond au message Resource Request en envoyant un message Release à CMo indiquant le flux J.112 qui doit être supprimé.

RELS

Number_of_Connections	1
Connection_ID	37 125 <ID de porte>

20) CMo génère le flux J.112 et envoie le Release Response à ANo.

RELS-RSP

Connection_ID	37 125 <ID de porte>

VIII.2 Exemple de flux d'appel avec messages J.112 de l'Annexe B/Annexe C

Voir Figures VIII.2 et VIII.3.

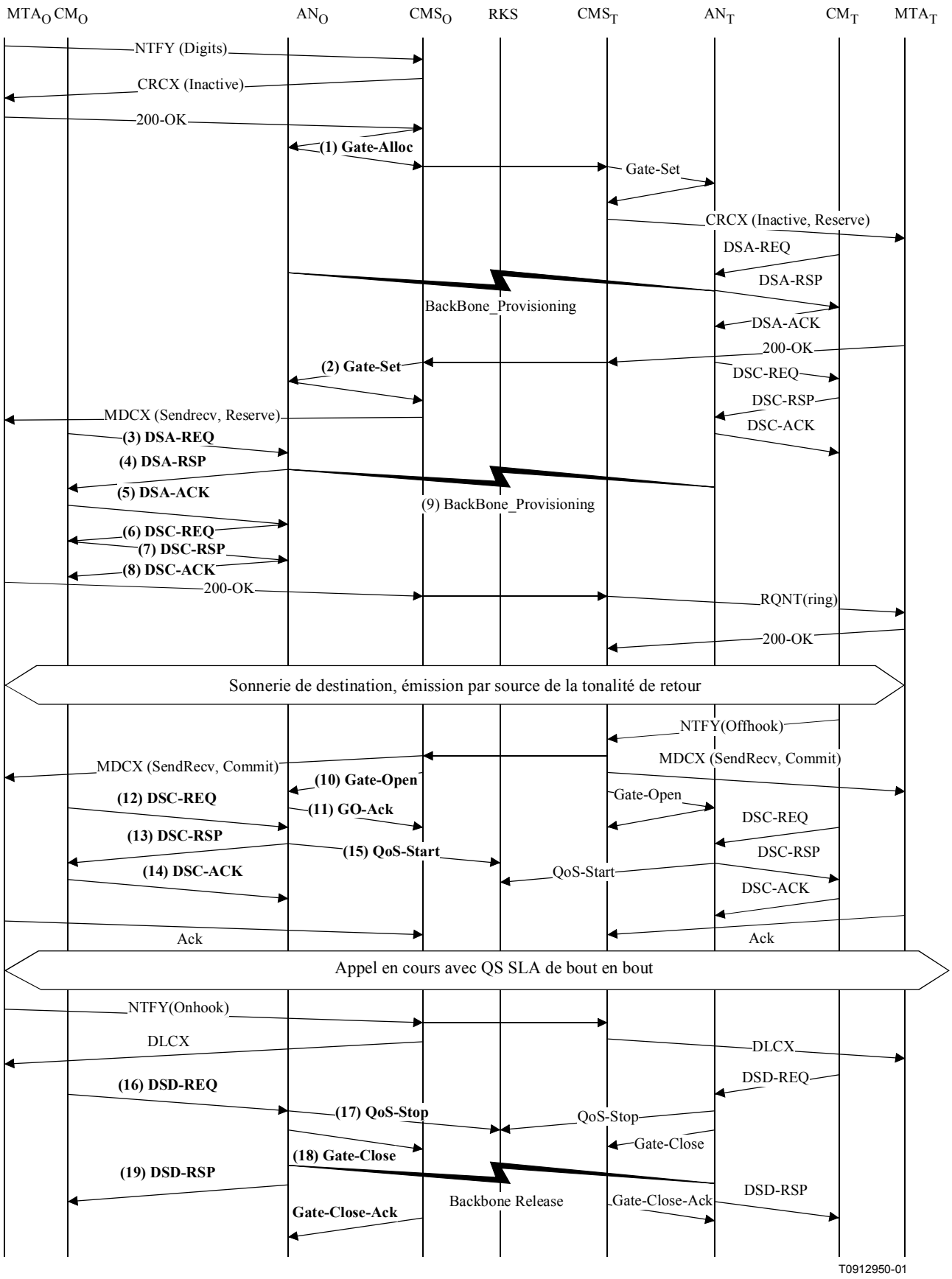


Figure VIII.2/J.163 – Appel NCS intégré de réseau privé à réseau privé

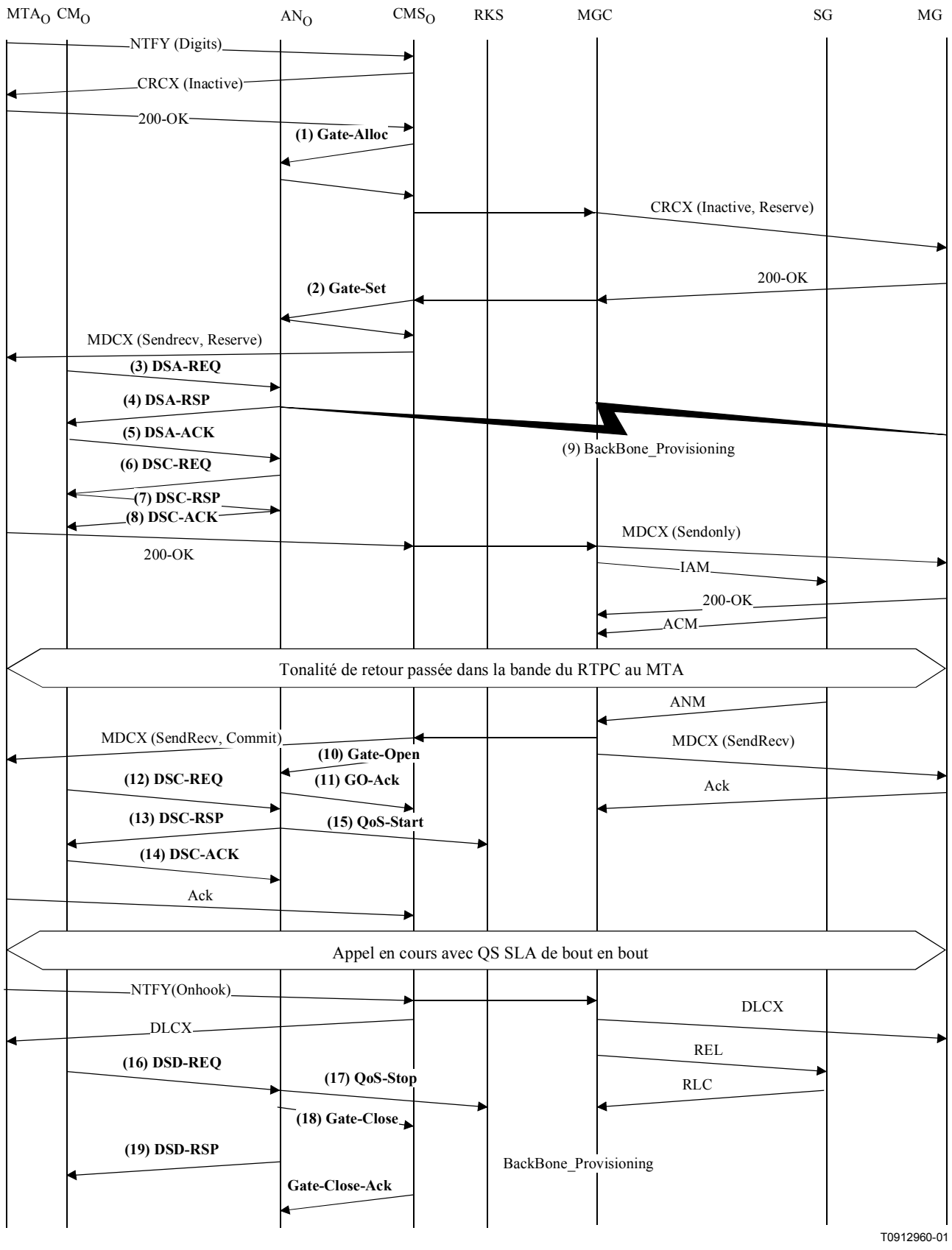


Figure VIII.3/J.163 – NCS intégré de réseau privé à réseau public

1) CMSo, à la réception des informations de signalisation provenant de MTAo, vérifie la consommation de ressources en cours de MTAo en consultant ANo.

GATE-ALLOC

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Activity-Count		4	Nombre maximal de connexions permises par le client.

ANo vérifie l'utilisation des ressources en cours par MTAo et répond en indiquant le nombre de connexions actives.

GATE-ALLOC-ACK

TransactionID		3176	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		3	Nombre total de connexions établies par ce client.

2) CMSo, après des échanges supplémentaires de signalisation, donne à l'ANo l'autorisation d'admettre la nouvelle connexion.

GATE-SET

TransactionID		3177	Transaction ID unique pour cet échange de messages.
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Remote-Gate-Info	AN Address	CMSo	Information nécessaire pour coordonner les portes. Il est à noter que le CMS s'est donné lui-même comme l'entité pour échanger les messages de coordination de portes.
	AN Port	2052	
	Remote Gate-ID	8095	
	Security Key	<clé>	
	Flag	No-gate-open	
Event-Generation-Info	RKS-Addr	RKS	Adresse du serveur d'archivage (RKS).
	RKS-Port	3288	Port sur le serveur d'archivage (RKS).
	Billing Correlation ID	<id>	Données opaques qui sont transmises au RKS lorsque les ressources sont engagées.

GATE-SET

Gate-Spec	Direction	amont	
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAo	
	Destination Address	MTAt	
	Source Port	0	
	Destination port	7000	
	DSCP	6	Valeur Packet Type pour les paquets amont.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	
Gate-Spec	Direction	aval	
	Flag	Auto-commit	Drapeau pour activer les ressources sur l'opération Reserve.
	Protocol	UDP	Les quatre informations Protocol, Destination Address, Source Address et Destination Port sont utilisées pour les classificateurs de QS.
	Source Address	MTAt	
	Destination Address	MTAo	
	Source Port	0	
	Destination port	7120	
	DSCP	9	Valeur Packet Type pour les paquets aval.
	T1	180 000	Temps maximal entre reserve et commit.
	T2	2000	Temps maximal pour que la coordination des portes ait lieu.
	b	120	Paramètres de bande passante maximale que MTAo est autorisé à demander pour cette conversation.
	r	12 000	
	p	12 000	
	m	120	
	M	120	
	R	12 000	
	S	0	

ANo répond à la commande Gate Set-up avec un accusé de réception.

GATE-SET-ACK

TransactionID		3177	
Subscriber		MTAo	Demande des ressources totales utilisées par ce client.
Gate-ID		37 125	Identifiant pour porte allouée.
Activity Count		4	Nombre total de connexions établies par ce client.

3) MTAo, à la réception d'une information d'appel de signalisation, calcule les paramètres de QS pour la liaison J.112. Il utilise l'interface de l'Annexe E de l'Annexe B/J.112 avec le CM pour envoyer le DSA-REQ suivant à l'AN. Ce message est utilisé pour établir les paramètres amont et aval. La Upstream Unsolicited Grant Size (taille d'attribution non sollicitée amont) a été calculée égale à 120 (du SDP) plus 18 (préfixe Ethernet) moins 40 (valeur de suppression d'en-tête) plus 13 (préfixe J.112). Suppression d'en-tête indique les 42 octets de l'en-tête Ethernet/IP/UDP. Le contenu de l'en-tête supprimé est inclus dans le DSA-REQ.

DSA-REQ

TransactionID		1
UpstreamServiceFlow	ServiceFlowReference	1
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37 125
DownstreamServiceFlow	ServiceFlowReference	2
	QoSParameterSetType	Admis (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37 125
UpstreamPacketClassification	ServiceFlowReference	1
	PacketClassifierReference	1
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)

DSA-REQ

DownstreamPacketClassification	ServiceFlowReference	2
	PacketClassifierReference	2
	ClassifierPriority	150
	ClassifierActivationState	Inactif (0)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
PayloadHeaderSuppression	ClassifierReference	1
	ServiceFlowReference	1
	HeaderSuppressionIndex	1
	HeaderSuppressionField	<42octets>
	HeaderSuppressionMask	<42bits>
	HeaderSuppressionSize	42
	HeaderSuppressionVerify	Vérifier (0)
AuthorizationBlock		37 125
HMAC		

4) L'AN vérifie l'autorisation, en cherchant une porte avec l'ID de porte correspondant à la valeur dans AuthBlock et vérifie les ressources qu'il lui est demandé d'allouer (par exemple, espace de table de suppression d'en-tête, identifications de flux de service, espace de table de classificateurs) et installe les classificateurs. Si l'opération aboutit, il renvoie le message DSA-RSP indiquant le succès de l'opération.

DSA-RSP

TransactionID		1
ConfirmationCode		Succès (0)
UpstreamServiceFlow	ServiceFlowReference	1
	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
	AuthBlock	37 125

DSA-RSP

DownstreamServiceFlow	ServiceFlowReference	2
	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis (2)
	TimeOutAdmitted	200
	TrafficPriority	5
	MaximumSustainedRate	12 000
	AuthBlock	37 125
UpstreamPacketClassification	ServiceFlowReference	1
	PacketClassifierReference	1
	PacketClassifierIdentifier	3001
	ClassifierPriority	150
	ClassifierActivationState	Inactive (0) (inactif)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowReference	2
	PacketClassifierReference	2
	PacketClassifierIdentifier	3002
	ClassifierPriority	150
	ClassifierActivationState	Active (1) (actif)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

5) A la réception du DSA-RSP, le CM accuse réception avec un message DSA-ACK.

DSA-ACK

TransactionID		1
ConfirmationCode		Succès (0)
HMAC		

6) A la réception du DSA-ACK du CM, l'AN envoie un DSC-REQ message au CM pour activer les ressources pour le service de flux aval. L'AN fait cela parce que le drapeau Auto-commit est activé dans le GATE-SET du CMS pour la porte aval.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admitted (2) (admis)
	TimeOutAdmitted	200
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000
Upstream Classifier	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Inactif (0)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
Downstream Classifier	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

7) A la réception du DSC-REQ depuis l'AN, le CM envoie un DSC-RSP à l'AN.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

8) A la réception du DSC-RSP du CM, l'AN envoie un DSC-ACK au CM.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

9) Simultanément avec le message n° 4, l'AN initie toute réservation de réseau de base requise pour la qualité de service demandée. Le contenu de ce message dépend d'algorithmes de réseau de base particuliers et sortent du domaine d'application de la présente Recommandation. Le routeur du réseau de base envoie à l'AN toute notification nécessaire indiquant que la réservation a abouti.

10) Le CMS envoie la porte open message à l'AN pour l'informer que les ressources devraient être engagées. Si l'AN ne reçoit pas le DSC-REQ provenant de MTAo dans un certain délai, il convient qu'il révoque l'autorisation de porte.

GATE-OPEN

TransactionID		72	Identifiant pour faire correspondre ce message avec sa réponse.
Gate ID		37 125	Gate-ID à AN.
HMAC			Total de contrôle de sécurité pour ce message.

11) L'AN répond à GATE-OPEN par:

GATE-OPEN-ACK

TransactionID		72	Identifiant pour faire correspondre ce message avec sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

12) En réponse aux messages de signalisation qui indiquent que l'appel a été effectué (c'est-à-dire que l'autre partie a décroché), MTAo utilise l'interface de l'Annexe E de l'Annexe B/J.112 pour activer les ressources admises. Cette opération se fait par l'intermédiaire d'une commande DSC-REQ à l'AN.

DSC-REQ

TransactionID		2
UpstreamServiceFlow	ServiceFlowIdentifier	1001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	ServiceFlowScheduling	UGS (6)
	NominalGrantInterval	10 ms
	ToleratedGrantJitter	2 ms
	GrantsPerInterval	1
	UnsolicitedGrantSize	111
DownstreamServiceFlow	ServiceFlowIdentifier	2001
	QoSParameterSetType	Admis + Activé (6)
	TimeOutActive	10
	TrafficPriority	5
	MaximumSustainedRate	12 000

DSC-REQ

UpstreamPacketClassification	ServiceFlowIdentifier	1001
	PacketClassifierIdentifier	3001
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MTAo
	IPSourcePort	7120
	IPDestinationAddress	MGt
	IPDestinationPort	7000
	IPProtocol	UDP (17)
DownstreamPacketClassification	ServiceFlowIdentifier	2001
	PacketClassifierIdentifier	3002
	ClassifierChangeAction	Remplace (1)
	ClassifierPriority	150
	ClassifierActivationState	Actif (1)
	IPSourceAddress	MGt
	IPDestinationAddress	MTAo
	IPDestinationPort	7124
	IPProtocol	UDP (17)
HMAC		

13) L'AN envoie un message DSC-RSP montrant que l'opération a réussi.

DSC-RSP

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

14) Le CM envoie un message DSC-ACK pour indiquer que le DSC-RSP a été reçu et adopté.

DSC-ACK

TransactionID		2
ConfirmationCode		Succès (0)
HMAC		

15) ANo envoie l'enregistrement de l'événement au serveur d'archivage (RKS) indiquant qu'un Commit a été reçu sur cet appel. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un QoS-Start message.

QoS-START

Header	Timestamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID donnée dans Gate-Set.
QoS Descriptor	Type	UGS	Description de la QS fournie pour cette connexion.
	Grant interval	10 ms	
	Grant Jitter	2 ms	
	Grant/Interval	1	
	Grant Size	111	
MTA Port	Port	7120	

16) Lorsque l'appel est fini le MTA utilise l'interface de l'Annexe E de l'Annexe B/J.112 pour supprimer les flux de service, envoyant un message DSD-REQ à l'AN.

DSD-REQ

TransactionID		3
ServiceFlowID		1001
HMAC		

DSD-REQ

TransactionID		4
ServiceFlowID		2001
HMAC		

17) L'AN envoie la notification au serveur d'archivage (RKS) pour indiquer que l'appel est terminé. Ce message est uniquement un exemple de ce qui pourrait être inclus dans un message QoS-Stop.

QoS-Stop

TimeStamp		<heure>	Heure de l'événement enregistré.
Header	Time Stamp	<heure>	Heure de l'événement enregistré.
	Billing Correlation ID	<chaîne>	Correlation ID du message Gate-Set.
SF-ID	SF-ID	1001	Identifiant de flux de service.

18) L'AN, à la réception de RSVP-PATH-TEAR, envoie le message de coordination de portes au CMS (identifié dans le message Gate-Set).

GATE-CLOSE

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
Gate-ID		8095	Identifie la Gate-ID au CMS.
HMAC			Total de contrôle de sécurité pour ce message.

Le CMS répond par :

GATE-CLOSE-ACK

TransactionID		73	Identifiant pour faire correspondre ce message avec sa réponse.
HMAC			Total de contrôle de sécurité pour ce message.

19 L'AN supprime les identifications de flux de service et envoie la réponse au CM.

DSD-RSP

TransactionID		3
ServiceFlowID		1001
ConfirmationCode		Succès (0)
HMAC		

DSD-RSP

TransactionID		4
ServiceFlowID		2001
ConfirmationCode		Succès (0)
HMAC		

APPENDICE IX

Scénarios de vol de service

Nous indiquons ici les grandes lignes de plusieurs scénarios possibles de vol de service pour mettre en évidence la nécessité d'une autorisation dynamique, la nécessité pour le protocole d'une réservation de ressources en deux phases, la nécessité de la coordination des portes. 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'abri du vieillissement" est certes un objectif de la 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 la signalisation de l'architecture 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'incitation importante pour 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 ROM, le remplacement des puces et l'ingénierie inverse de la conception 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 J.112, il est possible et tout à fait vraisemblable, que le logiciel du PC sera écrit pour émuler le comportement du MTA. Il peut être impossible de distinguer un tel PC d'un MTA réel. Le comportement du logiciel dans ce cas est sous le contrôle total du client.

De plus, il est prévu que les nouveaux services seront implémentés dans le MTA et que le contrôle logiciel de ces nouveaux services sera fourni par un grand nombre de constructeurs. 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. Nous n'abordons pas ici le problème des "chevaux de Troie" dans ces logiciels téléchargés, car ce problème est considéré comme identique à celui des clients qui perdent leur numéro de carte de crédit ou leur numéro d'identification personnel (PIN). Nous traitons le problème du client qui télécharge intentionnellement un logiciel spécial qui ne fonctionne que dans son intérêt.

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 passées composées 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 du client) et négocier une connexion à QS élevée via le mécanisme RSVP ou via l'interface de l'Annexe E de l'Annexe B/J.112 interface pour un client intégré. Etant donné qu'aucun agent de réseau n'est utilisé pour initier la session, aucun enregistrement destiné à la facturation ne sera produit. Ce scénario est évité en demandant une autorisation dynamique au niveau de l'AN; 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 uniquement l'émetteur modifié. Si le MTA de départ 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 AN.

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

Une QS fournie de manière statistique 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 J.112, peut utiliser cette possibilité pour surfer sur le web ou pour d'autres applications PC. Ce scénario est évité en demandant une autorisation dynamique au niveau de l'AN; sans l'autorisation la tentative d'obtenir une qualité de service élevée échouera.

IX.3 Scénario n° 3: absence de coopération du MTA pour la facturation

Il est facilement possible d'imaginer ce qui se passerait face à un message du MTA à l'établissement de la session indiquant, "OK, l'appelé a répondu, commencer maintenant à me facturer" ou un message au moment du raccroché disant "session terminée, arrêter la facturation maintenant". Toutefois, il existe des façons plus subtiles pour un utilisateur d'obtenir le même effet qu'en trafiquant ce type de messages s'ils existaient.

Il est essentiel de fournir un service de communications vocales de classe commerciale en utilisant IPCablecom pour garantir que la capacité du réseau existe avant de signaler le CPE au niveau de l'emplacement de l'appelé. Cette fonction est effectuée avec les messages RESERVE. Si le message RESERVE n'était que pour allouer effectivement la bande passante (c'est-à-dire, en combinant les mécanismes RESERVE et COMMIT), il n'y aurait dans ce cas aucune incitation à envoyer le COMMIT. Le MTA pourrait simplement démarrer la transmission de paquets voix immédiatement et la destination pourrait transmettre des paquets voix dès que le téléphone a répondu. Le message COMMIT devient, en effet, le message de début de facturation ci-dessus. Il est par conséquent essentiel que le mécanisme RESERVE n'alloue pas de façon effective la bande passante, mais vérifie plutôt toutes les allocations en cours et les réservations en suspens pour s'assurer que de la bande passante sera disponible au moment d'un message COMMIT.

IX.4 Scénario n° 4: MTA modifiant l'adresse de destination dans les paquets voix

Un autre exemple est celui de deux MTA éloignés 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 vers l'autre. Le système de facturation continue à facturer chacun d'entre eux pour une session locale, tandis que les clients sont effectivement engagés dans une session longue distance. Ceci implique la présence de mécanismes au niveau des AN 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.5 Scénario n° 5: 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 portes. Supposons qu'un client dans une session envoie un message COMMIT et l'autre non. Disons par exemple, que le client d'arrivée envoie un COMMIT, mais ne réussit pas à envoyer le message de signalisation correct, alors l'émetteur n'envoie jamais un COMMIT. 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 de départ n'a pas envoyé de message COMMIT, 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 combinée 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.6 Scénario n° 6: terminaison rapide laissant une demi-connexion

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

IX.7 Scénario n° 7: message de coordination de portes falsifié

Chaque MTA connaît l'identité de son AN et connaît le tuple-5 que son AN utilise pour identifier la GateID. 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 GateID. 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 à l'AN une clé à utiliser pour les messages AN-AN, sur une base session par session (ou par porte).

IX.8 Scénario n° 8: 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.

La coordination des portes, qui était utilisée précédemment pour protéger contre les demi-connexions, protège également contre ce type de fraude. Le message GATE-OPEN indique à la bande passante qu'elle a été allouée en résultat du COMMIT et le COMMIT-ACK envoyé à l'émetteur dit exactement quelle bande passante sera facturée pour la session. Si l'émetteur détecte une anomalie quelconque, il peut immédiatement terminer la session.

APPENDICE X

COPS (service commun de politique ouverte)

X.1 Procédures et principes du COPS

Le présent appendice fournit une description brève des procédures et des principes du protocole COPS et comment le protocole COPS est associé aux autres protocoles tels que LDAP. Le protocole COPS est actuellement défini dans un draft-IETF-RAP-COPS-07 Internet.

Le protocole service commun de politique ouverte (COPS, *common open policy service*) est un protocole client/serveur défini dans le groupe de travail sur la politique d'admission du RSVP de l'IETF (rap) pour être utilisé dans le contrôle d'admission dans les réseaux de QS RSVP/IntServ et DiffServ QS. 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 au bord du réseau et d'un serveur de politique. Trois entités fonctionnelles sont définies pour le cadre du rap:

- point de décision de politique (PDP) – L'entité serveur du COPS, qui prend la décision finale d'admission ou de rejet de session, basée 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 du 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 initier une demande au PDP qui résultera dans 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'elle est utilisée dans un environnement RSVP/IntServ, est représentée à la Figure X.1.

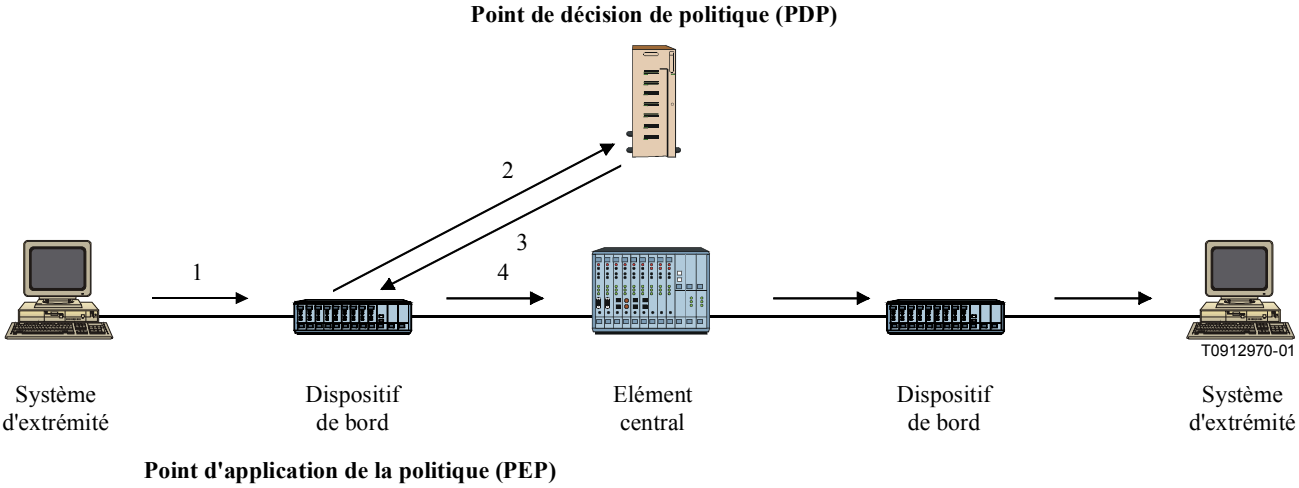


Figure X.1/J.163 – Protocole COPS

Dans la séquence COPS, le client PEP est responsable d'établir initialement une session avec le PDP, en utilisant les informations qui sont soit configurées dans le PEP soit déterminée par d'autres moyens. Une fois que la session est établie, si le dispositif de bord 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 de rejeter la demande et si elle est acceptée, le dispositif de bord continue à envoyer le message RSVP dans le réseau (4).

Chaque session est maintenue par un message Keep Alive 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 identifiée par un Handle (identificateur), qui peut être utilisée pour associer la réponse, les réponses ultérieures non demandées 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 (*request*), une réponse (*response*), ou d'un autre type, suivi par des objets à auto-identification, chacun contenant une classe d'objet et un identificateur de version. Chaque objet inclut un numéro de classe (*class number*) qui définit ce qu'est l'objet, par exemple, un objet Timer, ou un objet Decision, plus un type de classe (*class type*) qui identifie le sous-type ou la version de la classe qui est utilisée.

D'autres classes d'objet incluent les données d'allocation de la bande 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 du COPS et du LDAP pour la politique

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

COPS est conçu pour que le client demande une décision d'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 basées sur sa connaissance des politiques. Le protocole permet au PEP de transmettre ces informations sur la demande au PDP et le PDP de repasser une décision pour permettre ou rejeter la demande.

Le protocole LDAP est conçu pour que le client demande un enregistrement d'annuaire provenant d'un annuaire. La fonction pour l'utilisation de l'enregistrement dépend du client qui doit être capable de comprendre l'enregistrement extrait et 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 du RSVP. COPS serait utilisé entre le PEP et le PDP pour envoyer une demande pour une analyse basée 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 basée sur les informations de politique extraites et utiliserait le protocole COPS pour repasser cette décision au PEP. Voir Figure X.2.

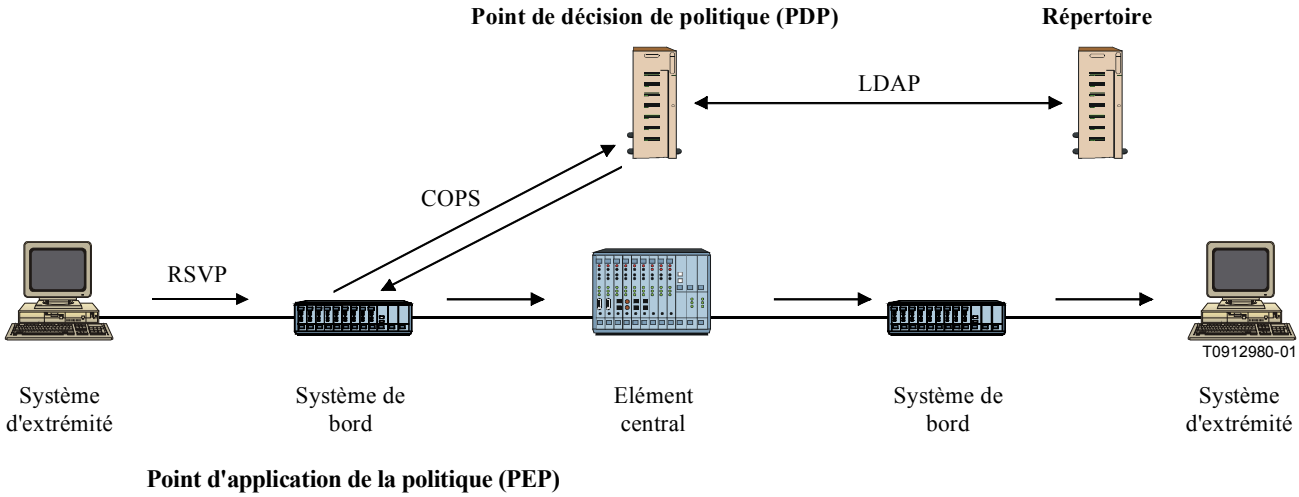


Figure X.2/J.163 – Modèle COPS et LDAP

APPENDICE XI

RSVP (Resource Reservation Protocol)

XI.1 RSVP Procédures et principes

Le présent appendice fournit une description brève de procédures et de principes du protocole RSVP. Le protocole RSVP est actuellement défini dans IETF RFC 2205.

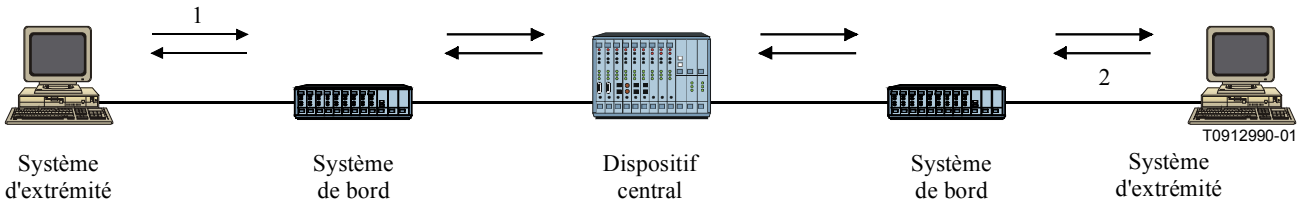


Figure XI.1/J.163 – RSVP

Le protocole RSVP a été développé dans l'IETF pour la réservation de ressources pour prendre en charge des flux d'information sur Internet. Certaines des caractéristiques principales du RSVP sont les suivantes :

- réservation de ressources saut par saut pour prendre en charge les flux d'information de bout en bout;
- informations sur les états conservées au niveau de chaque routeur participant;
- les routeurs non-participants traitent les messages RSVP comme des paquets IP normaux;
- état souple – la réservation doit être rafraîchie périodiquement ou elle s'annule automatiquement;
- demande pilotée – un message PATH initial établit l'état dans le routeur. Un message RESV du destinataire aboutit effectivement à la réservation des ressources.

Dans le protocole RSVP, la source initie une session en envoyant un message PATH (1). Ce message est acheminé sur le réseau selon son adresse de destination (qui peut être une adresse multidiffusion) et crée un état de flux au niveau de chaque routeur prenant en charge le protocole RSVP qu'il traverse. Le message PATH est acheminé en utilisant les mêmes procédures que les autres paquets IP avec cette adresse de destination, de sorte qu'il reproduit le trajet à suivre par le paquets de données. Au cours de sa progression, il enregistre l'adresse du dernier routeur compatible avec le protocole RSVP et cette adresse est ajoutée aux informations d'état au niveau du routeur suivant.

A l'extrémité d'arrivée, le destinataire rejoint la session en envoyant un message RESV (2) qui identifie un flux ou des flux que ce récepteur souhaite recevoir des différents flux pris en charge dans la session. Le message RESV retrace la séquence suivie par le message PATH, en utilisant les enregistrements du dernier routeur compatible avec le protocole RSVP et entraîne la réservation des ressources à chaque saut. Si plusieurs messages RESV sont reçus au niveau du même routeur, ils peuvent être fondus en un seul message RESV avec la demande combinée de réservation de ressources.

Le processus requiert l'établissement d'état au niveau de plusieurs nœuds internes et la réservation de ressources au niveau de ces mêmes nœuds. Il établit un chemin fixe pour le flux d'information. Il garantit toutefois que les ressources ont été allouées au niveau de tous les points prenant en charge le protocole RSVP sur le chemin.

XI.2 Flowspec du RSVP

Une demande RSVP élémentaire se compose d'un "flowspec" et d'un "Filter-Spec"; ce couple est appelé "descripteur de flux". Le flowspec spécifie une QS désirée. Le filterspec, avec une spécification de session, définit l'ensemble de paquets de données – le "flux" – pour recevoir la QS définie par le flowspec. Le flowspec est utilisé pour régler les paramètres dans le programmateur de paquets du nœud ou tout autre mécanisme de la couche de liaison, tandis que le Filter-Spec est utilisé pour régler les paramètres dans le classificateur de paquets. Les paquets de données qui sont adressées à une session particulière mais qui ne correspondent à aucun des Filter-Spec pour cette session sont gérés comme trafic "au mieux".

Le flowspec dans une demande de réservation inclura généralement une classe de service et deux ensembles de paramètres numériques:

1) un "Rspec" (R pour "reserve") qui définit la QS désirée;
2) un "Tspec" (T pour "traffic") qui décrit le flux de données.

Il est important de noter que les formats et le contenu des Tspec et Rspec sont déterminés par les modèles de service intégrés RFC 2210 de l'IETF définis dans le groupe de travail intserv de l'IETF et sont généralement opaques au protocole RSVP lui-même. Le RSVP définit le mécanisme de signalisation et non le modèle de trafic.

APPENDICE XII

Considérations sur le TCP

La présente Recommandation définit une interface entre un contrôleur de porte (GC) et un nœud d'accès (AN) à utiliser pour l'autorisation de portes, qui prend fondamentalement en charge un protocole basé sur les transactions dans lequel chaque transaction est indépendante. Le TCP peut être utilisé comme transport pour cet échange de message. Toutefois, des problèmes se sont posés concernant les implications sur les performances d'utilisation du TCP. Le présent appendice examine quelques-uns de ces problèmes et propose certaines solutions potentielles qui peuvent fournir un

transport acceptable par l'intermédiaire de l'optimalisation des implémentations et la mise au point de l'implémentation du TCP.

Il convient que la conception du réseau prenne en charge le degré désiré de fiabilité et les performances en temps réel.

XII.1 Exigences

Considérons tout d'abord les exigences sur le protocole de transport pour l'interaction entre le GC et l'AN:

1) la remise fiable des messages échangés entre le GC et l'AN est requise;
2) il convient que l'échange de message ait 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 de dixième de millisecondes);
3) il est souhaitable que plusieurs demandes soient en suspens simultanément. Cela parce qu'il est probable que plusieurs établissements d'appel seront en cours simultanément;
4) si un blocage en tête de ligne (HOL, *head-of-the-line*) est probable, il convient que cela soit évité;
5) il est probable qu'il y ait une association longue (au moins de l'ordre de plusieurs minutes) entre le GC et l'AN. Toutefois, lorsqu'une panne du GC se produit, il convient que le procédé d'établissement d'une nouvelle connexion à l'AN ne 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) prendre en compte une plus grande fenêtre après l'établissement d'une connexion;
3) avoir plusieurs connexions TCP par paire GC-AN 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 trois voies définie comme suit (voir Figure XII.1):

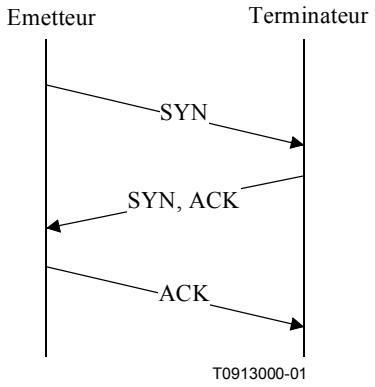


Figure XII.1/J.163 – Etablissement de la connexion TCP

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 la retransmission (RTO, *retransmission timeout value*) est généralement calculée en utilisant la formule:

$$RTO = A + 4D$$

mais le RTO initial est calculé 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 attente exponentielle utilisant un multiple de 2 est appliquée à la valeur courante de RTO. Ainsi, pour le premier segment, le RTO est calculé 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, RTO sera calculé comme suit:

$$RTO = 0 + 4 \times 3 = 12$$

et une attente 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 secondes se sera écoulé avant que la troisième retransAmission se produise.

L'importance de ce problème dépend entièrement de la fréquence avec laquelle l'établissement de la connexion GC $\rightarrow$ AN 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 bas pour les paquets entre le GC et l'AN, même en cas de perte

Les exigences (2), qui traitent de la récupération de la perte de paquets, ont besoin de quelques recours disponibles pour le TCP pour récupérer rapidement une perte. Lorsque seuls quelques paquets sont transmis et que le destinataire est incapable de générer un nombre suffisant de doubles ACK, la récupération de la perte de paquets se fait à partir d'une temporisation de la retransmission time-out. L'algorithme de retransmission du TCP repose sur une moyenne pondérée 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 la retransmission est alors réglée à:

$$RTO = A + 4D$$

et si le temporisateur déclenche, le segment en question est retransmis et le RTO est temporisé exponentiellement en utilisant un multiplicateur de 2[3] jusqu'à une limite supérieure de 64 secondes pour le 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 une petite période de temps, 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 RTO. Alors que la spécification TCP elle-même ne spécifie pas la granularité de RTO, il est très commun d'avoir 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 seconde.

Pour récupérer rapidement la perte de paquets dans une séquence de paquets (sans avoir à dépendre de plusieurs doubles ACK pour déclencher une retransmission rapide ou avoir à attendre que le temporisateur RTO déclenche), il peut être souhaitable d'implémenter un TCP-SACK, qui facilite 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 (vraisemblablement moins de 500 millisecondes).

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 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 multiple établies entre le GC et l'AN, puis utiliser 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 envoyées sur les autres connexions.

L'inconvénient de cette approche est qu'un segment perdu n'est en principe pas retransmis tant que son temporisateur se déclenche (contrairement à un double ACK reçu), étant donné qu'il n'y aurait pas de segments supplémentaires à transmettre jusqu'alors.

---

[3] TCP utilise de plus des ACK doubles pour déclencher la retransmission de segments potentiellement perdus, cette particularité sera toutefois ignorée pour cette partie de l'étude.

XII.6 Démarrage lent de TCP

La capacité du TCP à démarrer la transmission d'un flux de paquets de données est quelquefois limitée par le mécanisme de démarrage lent du 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 la récupération de l'encombrement résultant de la perte d'un seul paquet). Le choix d'une taille de fenêtre initiale de 2 à 4 MSS est considéré comme souhaitable. Il est toutefois important de veiller à ce que cette fenêtre initiale ne dépasse pas 4 MSS, 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'optimaliser l'utilisation du réseau, l'algorithme de Nagle a été introduit pour les utilisateurs effectuant leur entrée au clavier. De manière essentielle, 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 millisecondes) 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-AN. 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 socket :

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 sockets TCP/IP. Bien qu'elle puisse permettre un schéma amélioré de récupération d'erreur, elle a un impact 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.

Il peut être recommandé d'utiliser une interface non bloquante pour améliorer les performances et prendre en charge des événements asynchrones en utilisant l'appel de fonction () sur architecture basée sur UNIX. Une interface de socket non bloquant peut être établie en utilisant l'appel suivant sur le socket 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 plate-formes ont une fonction similaire.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Genève, 2001