UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.171

(02/2002)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

IPCablecom

Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom

Recommandation UIT-T J.171

RECOMMANDATIONS UIT-T DE LA SÉRIE J

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

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

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

Recommandation UIT-T J.171

Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom

Résumé

La présente Recommandation décrit les profils IPCablecom d'une interface de programmation d'applications (API, *application programming interface*) ainsi que le protocole de commande de passerelle de jonction (TGCP, *trunk gateway control protocol*) destinés à la commande des passerelles médias RTPC voix sur IP (VoIP, *voice-over-IP*) par des éléments extérieurs de commande d'appel.

Source

La Recommandation J.171 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 13 février 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2002

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

Recommandation UIT-T J.171

Protocole de commande de passerelle de jonction (TGCP) du système IPCablecom

1 Domaine d'application

La présente Recommandation décrit les profils IPCablecom d'une interface de programmation d'applications (API, *application programming interface*) ainsi que le protocole de commande de passerelle de jonction (TGCP, *trunk gateway control protocol*) destinés à la commande des passerelles médias RTPC voix sur IP (VoIP, *voice-over-IP*) par des éléments extérieurs de commande d'appel.

La spécification à ces fins des profils est donnée dans les annexes à la présente Recommandation.

2 Références

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

2.1 Références normatives

– Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio pour la fourniture de services téléphoniques dans les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.162 (2001), *Protocole réseau de signalisation d'appel par le réseau pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.170 (2002), *Spécifications de sécurité de IPCablecom*.

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

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

2.2 Références informatives

– IETF Internet Draft (draft-huitema-sgcp-v1-02.txt), *Simple Gateway Control Protocol (SGCP)*.

– IETF Internet Draft (draft-taylor-ipdc-00.txt), *IPDC Base Protocol*.

– IETF RFC 1889 (1996) *RTP: A Transport Protocol for Real-Time Applications*.

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

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

– IETF RFC 2326 (1998) *Real Time Streaming Protocol (RTSP)*.

– Recommandation UIT-T E.180/Q.35 (1998), *Caractéristiques techniques des tonalités du service téléphonique*.

– Recommandation UIT-T Q.761 (1999), *Système de signalisation n° 7 – Description fonctionnelle du sous-système utilisateur du RNIS*.

– Recommandation UIT-T Q.762 (1999), *Système de signalisation n° 7 – Fonctions générales des messages et des signaux du sous-système utilisateur du RNIS*.

– Recommandation UIT-T H.323 (2000), *Systèmes de communication multimédia en mode paquet*.

– Recommandation UIT-T H.225.0 (2000), *Protocoles de signalisation d'appel et mise en paquets des trains multimédias dans les systèmes de communication multimédia en mode paquet*.

– Recommandation UIT-T H.245 (2001), *Protocole de commande pour communications multimédias*.

– IETF RFC 1825 (1996), *Security Architecture for the Internet Protocol*.

– IETF RFC 1826 (1995), *IP Authentication Header*.

– IETF RFC 2705 (1999), *Media Gateway Control Protocol (MGCP) Version 1.0*.

– TCP/IP Illustrated, Volume 1 (2001), *The Protocols,* Addison-Wesley, 1994.

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

3 Termes et définitions, abréviations et conventions

3.1 Définitions

La présente Recommandation définit les termes suivants:

3.1.1 modem-câble; câblo-modem: dispositif conforme aux Recs. UIT-T J.83 et J.112 offrant un accès numérique à grande vitesse aux sites des clients.

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

3.2 Abréviations

La présente Recommandation utilise les abréviations suivantes:

DNS système de dénomination de domaine (*domain name system*)

IP protocole Internet (*Internet protocol*)

IPSec sécurité IP (*Internet protocol security*)

ISUP sous-système utilisateur RNIS (*ISDN user part*)

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

MGCP protocole de contrôle de passerelle média (*media gateway control protocol*)

MIB base d'informations de gestion (*management information base*)

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

MWD temps d'attente maximal (*maximum waiting delay*)

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

NTP protocole relatif au temps dans le réseau (*network time protocol*)

QS qualité de service

RTCP protocole de commande en temps réel (*real-time control protocol*)

RTO temporisation de retransmission (*retransmission timeout*)

RTP protocole en temps réel (*real-time protocol*)

SDP protocole de description de session (*session description protocol*)

SG passerelle de signalisation (*signalling gateway*)

SPI indice des paramètres de sécurité (*security parameters index*)

3.3 Conventions

Si la présente Recommandation est implémentée, les mots clés "DOIT" (MUST ou SHALL, en anglais) et "REQUIS" doivent être interprétés comme indiquant un aspect obligatoire de la présente spécification. Les mots clés indiquant un certain niveau d'importance de telle ou telle prescription utilisée dans la présente Recommandation sont résumés ci-dessous.

"DOIT"	Ce mot ainsi que l'adjectif "REQUIS" indiquent que l'article est une prescription absolue de la présente spécification.
"NE DOIT PAS"	Cette expression indique que l'article est une interdiction absolue de la présente spécification.
"IL CONVIENT DE"	Cette expression ainsi que l'adjectif "RECOMMANDÉ" indiquent qu'il peut, dans des circonstances particulières, exister des raisons valables pour ignorer cet article, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.
"IL NE CONVIENT PAS DE"	Cette expression indique qu'il peut, dans des circonstances particulières, exister des raisons valables pour que le comportement indiqué soit acceptable ou même utile, mais qu'il convient, avant de faire ce choix, de prendre en considération la totalité des incidences et d'étudier soigneusement le cas.
"PEUT"	Ce mot ainsi que l'adjectif "FACULTATIF" indiquent que cet article est effectivement facultatif. Un fournisseur peut choisir d'inclure l'article par exemple parce qu'il est requis sur un marché particulier ou parce qu'il améliore le produit, alors qu'un autre fournisseur peut choisir d'omettre ce même article.

Annexe A

Profil 1 du protocole TGCP

A.1 Domaine d'application

La présente annexe décrit un profil IPCablecom d'une interface de programmation d'applications (API, *application programming interface*) nommée interface de commande de passerelle média (MGCI, *media gateway control interface*) et un protocole associé (MGCP) destinés à la commande des passerelles RTPC voix sur IP (VoIP, *voice-over-IP*) par des éléments extérieurs de commande d'appel. Le protocole MGCP prévoit une architecture de commande d'appel dans laquelle la "programmation" de la commande d'appel, en dehors des passerelles, se fait par des éléments extérieurs de commande d'appel. Le profil IPCablecom qui est décrit dans la présente annexe portera le nom de protocole de commande de passerelle de jonction (TGCP, *trunking gateway control protocol*) IPCablecom.

La présente annexe est fondée sur la Rec. UIT-T J.162 traitant de la signalisation d'appel par le réseau IPCablecom et sur le document IETF RTC 2705, *Media Gateway Control Protocol* (MGCP). La présente annexe, où est défini le protocole TGCP IPCablecom, donne une spécification qui est indépendante du protocole MGCP. Le profil TGCP du protocole MGCP n'est en toute rigueur défini que par la présente annexe.

NOTE – La spécification qui est donnée dans la présente annexe est utilisée en Amérique du Nord.

A.2 Interface de commande de passerelle média (MGCI)

Les fonctions de l'interface MGCI assurent la commande de la connexion, la commande des extrémités, l'audit et l'état d'avancement. Elles emploient toutes le même modèle de système et les mêmes conventions en matière de dénomination.

A.2.1 Modèle et conventions en matière de dénomination

Le protocole MGCP prévoit un modèle de connexion dont les éléments fondamentaux sont les extrémités et les connexions. Les connexions sont regroupées dans les appels. Un appel peut comprendre une ou plusieurs connexions. Les connexions et les appels sont établis à l'initiative d'un ou de plusieurs contrôleurs de passerelle média (MGC, *media gateway controller*). Il convient néanmoins de noter qu'en aucun de ces cas une "connexion" n'est établie dans un réseau IPCablecom, au sens qui est utilisé dans le réseau RTPC à commutation de circuits. Les termes "appel" et "connexion" dans ce contexte (et dans l'ensemble de la présente Recommandation) sont utilisés afin de s'y référer facilement, et non pour indiquer une quelconque similitude technique ou autre entre le réseau IPCablecom et le RTPC.

A.2.1.1 Noms des extrémités

Les noms des extrémités, alias les identificateurs des extrémités, sont composés de deux parties qui sont définies de manière à être insensibles à la casse:

- le nom du domaine de la passerelle commandant l'extrémité;
- un nom d'extrémité local de cette passerelle.

Les noms des extrémités auront la forme suivante:

```
local-endpoint-name@domain-name
```

où le nom domain-name est un nom de domaine absolu tel qu'il est défini dans le document IETF RFC 1034, qui comporte une partie relative à l'hôte et dont un exemple pourrait être le suivant:

```
MyTrunkingGateway.cablelabs.com
```

Le nom `domain-name` peut également être une adresse IPv4 en format décimal à points représentée par une chaîne de texte entourée à gauche et à droite de crochets ("[" et "]") telle que "[128.96.41.1]" – Veuillez consulter le document IETF RFC 821 pour plus de détails. L'utilisation des adresses IP est toutefois généralement déconseillée.

Les passerelles de jonction ont une ou plusieurs extrémités (par exemple, une extrémité par jonction) qui leur sont associées, et chacune de ces extrémités est identifiée par un nom local distinct d'extrémité. Comme dans le cas du nom de domaine, le nom d'extrémité local est insensible à la casse. A ce nom d'extrémité local, on associe un type d'extrémité endpoint-type afin de définir ce type, par exemple DS-0 ou une ligne d'accès analogique. Le type peut être obtenu à partir du nom d'extrémité local. Celui-ci est un nom hiérarchique, dont la composante la moins spécifique correspond au terme qui est situé à l'extrémité gauche, tandis que la composante la plus spécifique correspond à celui qui est situé à l'extrémité droite. Plus formellement, le nom d'extrémité local doit respecter les règles suivantes en matière de dénomination:

- les différents termes du nom d'extrémité local doivent être séparés par une barre oblique unique ("/", ASCII 2F hex).
- les différents termes sont des chaînes de caractères ASCII composées de lettres, de chiffres et d'autres caractères imprimables, à l'exception des caractères qui sont employés pour délimiter les noms d'extrémité endpoint-names ("/", "@"), des caractères génériques de remplacement ("*", "$") et des caractères d'espacement;
- les termes devant être remplacés dans le nom sont indiqués soit par un astérisque ("*") soit par un signe dollar ("$"). Donc, si le nom local entier d'extrémité a la forme suivante:

  `term1/term2/term3`

  et qu'un de ses termes est remplacé, le nom d'extrémité local aura la forme suivante:

  `term1/term2/*` lorsque le `term3` est remplacé.
  `term1/*/*` lorsque le `term2` et `term3` sont remplacés.

  L'astérisque aurait pu être remplacé dans chacun des exemples par un signe dollar;
- le remplacement ne peut se faire qu'à partir de la droite. Donc, lorsqu'un terme est remplacé, tous ceux qui sont à sa droite doivent l'être également;
- lorsque le signe dollar est employé en même temps que l'astérisque, il doit se situer à sa droite. Donc, lorsqu'un terme est remplacé par un signe dollar, tous ceux qui sont à sa droite doivent l'être par lui également;
- on interprétera un terme représenté par un astérisque comme suit: "employer *toutes* les valeurs de ce terme qui s'appliquent à la passerelle de jonction concernée";
- on interprétera un terme représenté par un signe dollar comme suit: "employer *une quelconque* valeur de ce terme qui s'applique à la passerelle de jonction concernée";
- chaque type d'extrémité endpoint-type peut fournir des précisions supplémentaires en ce qui concerne les règles en matière de dénomination pour ce type d'extrémité endpoint-type, ces règles n'allant toutefois pas à l'encontre de celles qui sont susmentionnées.

Il convient de noter que différents types d'extrémité endpoint-types ou même différents sous-termes, par exemple des "lignes", dans le même type d'extrémité endpoint-type donneront deux noms différents d'extrémité. En conséquence, chaque "ligne" sera considérée comme une extrémité distincte.

A.2.1.1.1 Noms des extrémités des passerelles de jonction

Les conventions supplémentaires en matière de dénomination qui sont spécifiées dans le présent paragraphe s'appliqueront aux extrémités des passerelles de jonction.

Les passerelles de jonction prendront en charge les types d'extrémité endpoint-type de base suivants:

- `ds` Un circuit DS-0.

  Il est prévu que le type d'extrémité de base soit configuré au moyen d'informations supplémentaires sur le type de signalisation pris en charge par le circuit de jonction et sur la fonction de système de commutation qu'il assure.

Extrémités des circuits de jonction:

outre les conventions en matière de dénomination spécifiées ci-dessus, les noms locaux des extrémités de passerelles de jonction RTPC du type "`ds`" devront respecter les conventions suivantes:

- les noms locaux des extrémités comporteront une suite de termes séparés par une barre oblique ("/") qui décrivent la hiérarchie physique dans la passerelle:

  `ds/<unit-type1>-<unit #>/<unit-type2>-<unit #>/.../<channel #>`

- le premier terme (`ds`) identifie le système utilisé pour nommer les extrémités et le type d'extrémité de base;
- le dernier terme est un nombre décimal qui indique le numéro[1] de la *voie* au plus bas niveau hiérarchique;
- les termes intermédiaires entre le premier terme (`ds`) et le dernier terme (numéro de voie) indiquent des niveaux hiérarchiques intermédiaires et comportent le type d'unité <unit-type> et le numéro d'unité <unit #> séparés par un tiret ("-") où:
  - le type d'unité <unit-type> identifie le niveau hiérarchique particulier. Les valeurs du type d'unité <unit-type> actuellement définies sont les suivantes: "s", "su", "oc3", "ds3", "e3", "ds2", "e2", "ds1" et "e1" où "s" est un numéro de tiroir et où "su" est une sous-unité dans un tiroir. D'autres valeurs indiquant des niveaux hiérarchiques physiques, dont il n'a pas été tenu compte dans cette liste mais auxquelles s'appliquent les mêmes règles fondamentales en matière de dénomination, seront également admises;
  - le numéro d'unité <unit #> est un nombre décimal qui est utilisé pour renvoyer à une instance particulière d'un type d'unité <unit-type> à ce niveau hiérarchique.
- le nombre de niveaux et la dénomination de ces niveaux sont fondés sur la hiérarchie physique au sein de la passerelle média, comme illustré dans les exemples suivants:
  - passerelle média ayant un certain nombre d'interfaces DS1:

    `ds/ds1-#/#`

  - passerelle média ayant un certain nombre d'interfaces OC3, qui contiennent des hiérarchies DS3 et DS1 de voies:

    `ds/oc3-#/ds3-#/ds1-#/#`

  - passerelle média contenant un certain nombre de tiroirs, chacun d'eux ayant un certain nombre d'interfaces DS3:

    `ds/s-#/ds3-#/ds1-#/#`

---

[1] Veuillez noter l'emploi du mot "voie" par opposition aux mots "intervalle de temps".

- certaines extrémités peuvent ne pas contenir tous les niveaux hiérarchiques possibles, mais tous les niveaux pris en charge par une extrémité donnée sont contenus dans la désignation de cette extrémité. Par exemple, une interface DS3 sans verrouillage de trames DS1 pourrait être nommée comme suit:

  `ds/s-#/ds3-#/#`

  ce système de dénomination ne permet toutefois pas de représenter une interface DS3 *avec* verrouillage de trames DS1;
- la dénomination de remplacement est conforme aux conventions stipulées au A.2.1.1, le caractère astérisque ("*") se rapportant à "tous", tandis que le caractère dollar ("$") se rapporte à "un quelconque". Le remplacement d'une gamme "[N-M]" de voies allant de la voie N à la voie M, inclusivement, est également pris en charge:
  - il convient de noter que le caractère de remplacement "tous" pour le premier terme (`ds`) se rapporte à tous les types d'extrémité endpoint-types de la passerelle média, quel que soit le type. Cette caractéristique est généralement destinée à être employée à des fins administratives, par exemple l'audit ou le redémarrage;
  - un nom d'extrémité local peut être sous-spécifié lorsque le nombre de termes fournis est inférieur au nombre normal à compter de la gauche du nom d'extrémité. Dans ce cas, les termes manquants à la droite du dernier terme spécifié sont supposés être le caractère de remplacement "*", se rapportant à "tous", à moins que les termes spécifiés ne soient le caractère de remplacement "un quelconque", auquel cas les termes manquants à la droite du dernier terme spécifié sont supposés être le caractère de remplacement "un quelconque";
  - lorsque l'emploi du caractère de remplacement "tous" est admis, on peut utiliser au lieu de celui-ci le remplacement d'une gamme de voies "[N-M]" dans le dernier terme (c'est-à-dire le numéro de voie <channel-#>) du nom d'extrémité local. Ce caractère de remplacement "gamme" se rapportera alors à toutes les voies de N à M. Les règles et les restrictions qui s'appliquent à l'emploi du caractère de remplacement "tous" s'appliqueront également à l'emploi du caractère de remplacement "gamme".

Les exemples suivants illustrent l'emploi des caractères de remplacement:

`ds/ds1-3/*`	toutes les voies de l'interface ds1 numéro 3 de la passerelle média concernée;
`ds/ds1-3/$`	une quelconque voie de l'interface ds1 numéro 3 de la passerelle média concernée;
`ds/*`	toutes les extrémités des circuits de jonction de la passerelle média concernée;
`*`	toutes les extrémités (quel que soit le type d'extrémité endpoint-type) de la passerelle média concernée;
`ds/ds1-3/[1-24]`	voies 1 à 24 de l'interface ds1 numéro 3 de la passerelle média concernée.

La forme canonique des noms est définie dans ce qui précède pour les extrémités d'une passerelle de jonction. Il est prévu que les alias pourront être pris en charge dans une version ultérieure de la présente Recommandation, par exemple afin de prendre en charge la liaison entre des circuits DS-0 multiples pour les communications vidéo, par exemple de la forme "`ds/ds1-1/H0-1`".

A.2.1.2 Noms des appels

Les appels sont identifiés par des identificateurs uniques et indépendants des plates-formes ou des agents sous-jacents. Les identificateurs d'appel sont des chaînes hexadécimales qui sont établies par le contrôleur MGC. Leur longueur maximale est de 32 caractères.

Au minimum, les identificateurs d'appel DOIVENT être uniques auprès de l'ensemble des contrôleurs MGC qui commandent les mêmes passerelles. Toutefois, la coordination entre les contrôleurs MGC au sujet de ces identificateurs d'appel sort du cadre de la présente Recommandation. Lorsqu'un contrôleur MGC établit plusieurs connexions qui se rapportent au même appel, sur une même passerelle ou sur des passerelles différentes, ces connexions seront liées au même appel au moyen de l'identificateur d'appel. Cet identificateur peut ensuite être utilisé par les procédures de comptabilité ou celles de gestion, qui sortent du cadre du protocole MGCP.

A.2.1.3 Noms des connexions

Les identificateurs de connexion sont établis par la passerelle lorsqu'il est demandé à celle-ci d'établir une connexion. Ils identifient la connexion dans le cadre d'une extrémité. Les identificateurs de connexion sont traités dans le protocole MGCP comme des chaînes hexadécimales. La passerelle DOIT faire en sorte qu'une période d'attente correcte, d'au moins trois minutes, s'écoule entre la fin d'une connexion qui a employé cet identificateur et l'utilisation de celui-ci dans une nouvelle connexion pour la même extrémité. La longueur maximale du nom d'une connexion est de 32 caractères.

A.2.1.4 Noms des contrôleurs de passerelle média et d'autres entités

Le protocole de commande de passerelle média a été conçu dans le but d'améliorer la fiabilité du réseau afin de permettre l'implémentation de contrôleurs MGC redondants. Cela veut dire qu'il n'y a pas de liaison fixe entre les entités et les plates-formes matérielles ou les interfaces de réseau.

Les noms des contrôleurs MGC sont composés de deux parties, comme les noms des extrémités. La partie locale du nom ne révèle pas la structure interne. Un exemple de nom de contrôleur MGC est donné ci-après:

```
mgc1@mgc.whatever.net
```

Les précautions suivantes permettent d'assurer la fiabilité:

- des entités telles que les passerelles de jonction ou les contrôleurs MGC sont identifiées par leur nom de domaine, et non par leurs adresses dans le réseau. Plusieurs adresses peuvent être associées à un nom de domaine. Si une commande ne peut être transmise à l'une des adresses dans le réseau, les implémentations DOIVENT réessayer la transmission au moyen d'une autre adresse;
- les entités peuvent passer à une autre plate-forme. L'association entre un nom logique (nom de domaine) et la plate-forme effective est conservée dans le service de dénomination de domaine (DNS, *domain name system*). Les contrôleurs MGC et les passerelles DOIVENT garder la trace de la lecture dans le service DNS de la durée de vie de l'enregistrement. Ils DOIVENT interroger le service DNS afin de renouveler les informations si la durée de vie a expiré.

Outre le traitement des données grâce à l'emploi des noms de domaine et du service DNS, la notion "d'entité notifiée" est essentielle pour la fiabilité et le basculement dans le protocole MGCP. "L'entité notifiée" pour une extrémité est le contrôleur MGC commandant effectivement cette extrémité. A tout moment, une extrémité dispose d'une et d'une seule "entité notifiée" qui lui est associée, et lorsqu'elle doit envoyer une commande au contrôleur MGC, elle DOIT envoyer cette commande à "l'entité notifiée" effective en indiquant la ou les extrémités auxquelles cette commande s'applique. Dès le démarrage, on DOIT attribuer une valeur fixée par la configuration à "l'entité notifiée". La plupart des commandes envoyées par le contrôleur MGC sont en mesure d'indiquer explicitement le nom de "l'entité notifiée" en utilisant un paramètre "NotifiedEntity". "L'entité notifiée" restera inchangée jusqu'à la réception d'un nouveau paramètre "NotifiedEntity" ou jusqu'à la réinitialisation

de l'extrémité. S'il n'y a pas "d'entité notifiée" pour une extrémité ou qu'elle n'a pas été explicitement[2] fixée, l'adresse de "l'entité notifiée" sera alors par défaut celle de l'émetteur de la dernière commande de prise en charge de la connexion ou demande de notification reçue pour l'extrémité. L'audit ne modifiera donc pas "l'entité notifiée".

Le paragraphe A.2.4 contient une description plus détaillée de la fiabilité et du basculement.

A.2.1.5 Cartes de chiffres

Dans le protocole MGCP, le contrôleur MGC peut demander que la passerelle recueille les chiffres qui ont été composés par un utilisateur. Cette fonctionnalité est généralement utilisée par des lignes d'accès analogique avec des passerelles résidentielles pour recueillir les numéros que compose un utilisateur, ou elle peut être utilisée pour les interfaces privées de signalisation associée à la voie. Plutôt que d'envoyer chaque chiffre au contrôleur MGC dès sa détection, celui-ci peut fournir une grammaire décrivant combien de chiffres devraient être accumulés avant qu'il n'en soit notifié. Cette grammaire est désignée comme étant une *carte de chiffres*.

Aucun type de circuit pris en charge par la version actuelle de la Recommandation relative au protocole TGCP ne nécessite de carte de chiffres, et celles-ci ne font donc pas partie de la présente Recommandation.

A.2.1.6 Evénements et signaux

La notion d'événements et de signaux est essentielle pour le protocole MGCP. Un contrôleur MGC peut demander à être notifié lorsque certains événements se produisent à une extrémité, par exemple, des décrochages. Il peut également demander que certains signaux soient appliqués à une extrémité, tels que le rappel automatique.

Les événements et les signaux sont regroupés dans des paquetages dans lesquels ils se partagent le même espace de noms, auquel nous nous référerons ci-après au moyen de la désignation noms d'événement. Un paquetage est un ensemble d'événements et de signaux qui sont pris en charge par un type d'extrémité endpoint-type particulier. Par exemple, un paquetage peut prendre en charge un certain groupe d'événements et de signaux pour les circuits ISUP, tandis qu'un autre paquetage peut prendre en charge un autre groupe d'événements et de signaux pour les circuits multifréquences. Il peut exister un ou plusieurs paquetages pour un type d'extrémité endpoint-type donné, et chaque type d'extrémité endpoint-type possède un paquetage par défaut auquel il est associé.

Les noms d'événement sont composés d'un nom de paquetage et d'un code d'événement et, puisque chaque paquetage définit un espace de noms distinct, les mêmes codes d'événement peuvent être utilisés dans différents paquetages. Les noms de paquetage et les codes d'événement sont des chaînes de lettres, de chiffres et de tirets insensibles à la casse, et soumis à la restriction que le tiret ne sera jamais ni le premier ni le dernier caractère d'un nom. Certains codes d'événement doivent parfois être paramétrisés au moyen de données supplémentaires, ce qui peut être fait par l'adjonction de paramètres entre parenthèses. Le nom du paquetage est séparé du code d'événement par une barre oblique ("/"). Il peut ne pas être contenu dans le nom d'événement, auquel cas le nom du paquetage par défaut est attribué au type d'extrémité endpoint-type concerné. Par exemple, pour un circuit de jonction ISUP, le paquetage ISUP (nom du paquetage "IT") étant le paquetage par défaut, les deux noms d'événement suivants sont considérés comme étant équivalents:

`IT/oc` opération achevée dans le paquetage ISUP pour un circuit de jonction ISUP.

`oc` opération achevée dans le paquetage ISUP (par défaut) pour un circuit de jonction ISUP.

---

[2] Ceci pourrait être dû au fait qu'aucune valeur n'ait été attribuée au paramètre NotifiedEntity.

Un ensemble initial de paquetages est défini à l'Annexe A.A. Des noms de paquetage et des codes d'événement supplémentaires peuvent être définis dans l'architecture IPCablecom ou enregistrés à l'aide de celle-ci. Toute modification des paquetages définis dans la présente Recommandation DOIT entraîner un changement de nom du paquetage, ou un changement de numéro de la version du profil du protocole TGCP, ou éventuellement les deux.

Chaque paquetage DOIT être défini, à savoir son nom DOIT être défini et il DOIT contenir la définition de chaque événement qui fait partie de lui. La définition des événements DOIT inclure le nom précis de l'événement, c'est-à-dire le code d'événement, une définition claire de l'événement et, selon le cas, la définition précise des signaux correspondants, par exemple les fréquences exactes des signaux audio tels que les tonalités de rappel automatique ou de télécopie. Les événements doivent en outre spécifier s'ils sont durables (voir A.2.3.1) et s'ils contiennent des états d'événement contrôlables (voir A.2.3.8.1). Les signaux DOIVENT être de type défini (activé/désactivé, avec interruption, ou bref) et la temporisation par défaut DOIT être définie pour les signaux qui sont de type avec interruption – voir A.2.3.1.

Outre les paquetages IPCablecom, les responsables de l'implémentation PEUVENT trouver profitable de définir des paquetages expérimentaux. Le nom de ces paquetages DOIT commencer par les deux caractères "x-" ou "X-"; dans l'architecture IPCablecom, les noms de paquetage qui commencent par ces deux caractères ne DOIVENT PAS être enregistrés. Une passerelle qui reçoit une commande se référant à un paquetage non pris en charge DOIT renvoyer une erreur (code d'erreur 518 – paquetage non pris en charge).

Les noms de paquetage et les codes d'événement prennent chacun en charge une notation de remplacement. Le caractère de remplacement "*" (astérisque) peut être utilisé pour renvoyer à tous les paquetages pris en charge par l'extrémité concernée, tandis que le code d'événement "tous" peut l'être pour renvoyer à tous les événements dans le paquetage concerné. Par exemple:

`IT/all` pour un circuit de jonction ISUP; renvoie à tous les événements dans le paquetage de circuits ISUP.

`*/all` pour un circuit de jonction ISUP; renvoie à tous les paquetages et à tous les événements dans les paquetages qui sont pris en charge par l'extrémité concernée.

En conséquence, le nom de paquetage "*" NE DOIT PAS être attribué à un paquetage, et le code d'événement "tous" NE DOIT PAS être utilisé dans un quelconque paquetage.

Des événements et des signaux sont détectés et produits par défaut aux extrémités. Toutefois, certains événements et signaux peuvent être détectés et produits dans les connexions en plus ou au lieu de ceux qui sont détectés ou produits aux extrémités. Par exemple, il peut être demandé que les extrémités fournissent une tonalité de rappel automatique lors d'une connexion. Afin qu'un événement ou un signal puisse être détecté ou produit dans une connexion, la définition de l'événement ou du signal DOIT explicitement établir que l'événement ou le signal peut être détecté ou produit dans une connexion.

Lorsqu'un signal est appliqué à une connexion, le nom de la connexion est ajouté au nom de l'événement, au moyen du signe "arobase" (@) en tant que signe de délimitation, comme dans l'expression suivante:

```
IT/rt@0A3F58
```

Le caractère de remplacement "*" (astérisque) peut être utilisé pour indiquer "toutes les connexions" à l'extrémité ou aux extrémités concernées. Lorsque cette convention est employée, la passerelle produira ou détectera l'événement dans toutes les connexions avec l'extrémité ou les extrémités. Un exemple de cette convention est donné ci-après:

```
IT/ma@*
```

Le caractère de remplacement "$" (signe dollar) peut être utilisé pour indiquer la "connexion effective". Cette convention NE DOIT PAS être utilisée, à moins que la demande de notification

d'événement ne soit "intégrée"dans une commande CreateConnection ou ModifyConnection. Lorsque la convention est employée, la passerelle produira ou détectera l'événement dans la connexion qui est effectivement en cours d'établissement ou de modification. Un exemple de cette convention est donné ci-après:

```
IT/rt@$
```

L'identificateur de connexion ou un caractère de remplacement peut être utilisé conjointement avec les conventions "tous les paquetages" et "tous les événements". Par exemple, la notation suivante:

```
*/all@*
```

peut être utilisée pour désigner tous les événements dans toutes les connexions à l'extrémité ou aux extrémités concernées.

A.2.2 Utilisation du protocole de description de session (SDP)

Le contrôleur MGC emploie le protocole MGCP pour fournir aux passerelles la description des paramètres de connexion tels que les adresses IP, les ports UDP et les profils de protocole en temps réel (RTP, *real-time protocol*). Sauf mention ou suggestion contraire dans la présente Recommandation, les descriptions du protocole SDP DOIVENT se faire suivant les conventions établies dans le protocole de description de session (SDP) qui est maintenant une norme proposée par l'IETF et est décrite dans le document IETF RFC 2327.

Le protocole SDP permet de décrire les conférences multimédias. Le profil du protocole TGCP ne prendra en charge que l'établissement de connexions audio au moyen du type de média "audio".

A.2.3 Fonctions de commande de passerelle

Le présent paragraphe décrit les commandes du protocole MGCP sous la forme d'un appel de procédure à distance (RPC, *remote procedure call*) telle que l'interface API, que nous désignerons comme étant l'interface de commande de passerelle média (MGCI). Une fonction de l'interface MGCI est définie pour chaque commande du protocole MGCP, cette fonction prenant et renvoyant les mêmes paramètres que la commande correspondante du protocole MGCP. Les fonctions indiquées dans le présent paragraphe fournissent une description de haut niveau de l'exploitation du protocole MGCP et donnent un exemple d'une interface API de type appel RPC qui PEUT être utilisée pour l'implémentation du protocole MGCP. Bien que l'interface API de type MGCI soit simplement un exemple d'interface API, le comportement sémantique défini par l'interface MGCI fait partie intégrante de la Recommandation, et toutes les implémentations DOIVENT être conformes à la sémantique spécifiée pour l'interface MGCI. Les messages du protocole MGCP effectivement échangés, y compris les formats et les codages des messages utilisés sont définis au A.3. Les passerelles de jonction DOIVENT permettre de les implémenter exactement comme spécifié.

Le service de l'interface MGCI consiste en les commandes de prise en charge des connexions et des extrémités. Un aperçu des commandes est donné ci-après:

- le contrôleur MGC peut lancer une commande NotificationRequest à une passerelle, ordonnant à celle-ci de surveiller des événements particuliers tels qu'une tonalité de prise ou de télécopie se produisant à une extrémité spécifiée;
- la passerelle utilisera ensuite la commande Notify pour informer le contrôleur MGC lorsque les événements demandés se produisent à l'extrémité spécifiée;
- le contrôleur MGC peut employer la commande CreateConnection pour établir une connexion qui aboutit à une extrémité à l'intérieur de la passerelle;
- le contrôleur MGC peut utiliser la commande ModifyConnection pour modifier les paramètres associés à une connexion établie précédemment;

- le contrôleur MGC peut employer la commande DeleteConnection pour supprimer une connexion existante. Dans certaines circonstances, la commande DeleteConnection peut aussi être utilisée par une passerelle pour indiquer qu'une connexion ne peut pas être retenue plus longtemps;
- le contrôleur MGC peut employer les commandes AuditEndpoint et AuditConnection pour vérifier l'état d'une "extrémité" et toutes les connexions qui lui sont associées. Une gestion du réseau, plus poussée que celle qui est obtenue au moyen de ces commandes est généralement souhaitable, par exemple en ce qui concerne des informations sur l'état de la passerelle de jonction et de chacun des circuits de jonction. On prévoit que ces capacités seront prises en charge lors de l'utilisation du protocole simple de gestion de réseau (SNMP, *simple network management protocol*) et de la définition d'une base d'informations de gestion (MIB, *management information base*), sujets qui sortent du cadre de la présente Recommandation;
- la passerelle peut employer la commande RestartInProgress pour notifier au contrôleur MGC que l'extrémité ou un groupe d'extrémités gérés par elle sont mis hors service ou ont été remis en service.

Ces services permettent au contrôleur (normalement le contrôleur MGC) de communiquer à une passerelle l'établissement des connexions qui aboutissent à une extrémité reliée à la passerelle, et d'être informé des événements qui se produisent à l'extrémité. Actuellement, une extrémité de passerelle de jonction est limitée à un circuit de jonction particulier dans une passerelle de jonction.

Les connexions sont regroupées en "appels". Plusieurs connexions, qui appartiennent éventuellement au même appel, peuvent aboutir à la même extrémité. Chaque connexion est spécifiée par un paramètre "mode", dont la valeur peut être fixée à "envoi seulement" (sendonly), "réception seulement" (recvonly), "envoi/réception" (sendrecv), "inactif" (inactive), "bouclage" (loopback), "essai de continuité" (conttest), "bouclage en réseau" (netwloop) ou "essai de continuité en réseau" (netwtest). Le paramètre "mode" détermine si les paquets médias peuvent être envoyés ou reçus par l'intermédiaire de la connexion; le RTCP n'est toutefois pas concerné.

Les signaux audio reçus en provenance d'une extrémité seront envoyés dans toute connexion à cette extrémité dont le mode est soit "envoi seulement" soit "envoi/réception".

Le traitement des signaux audio qui sont reçus dans ces connexions est également déterminé par les paramètres mode:

- les signaux audio reçus en paquets de données par l'intermédiaire de connexions en modes "inactif", "bouclage" ou "essai de continuité" sont ignorés;
- les signaux audio reçus en paquets de données par l'intermédiaire de connexions en modes "réception seulement" ou "envoi/réception" sont combinés, puis envoyés à l'extrémité[3];
- les signaux audio en provenance d'une extrémité sont transmis par l'intermédiaire de toutes les connexions en modes "envoi seulement" ou "envoi/réception";
- les signaux audio reçus en paquets de données par l'intermédiaire de connexions en modes "bouclage en réseau" ou "essai de continuité en réseau" seront renvoyés vers les connexions comme décrit ci-après.

Les modes "bouclage" et "essai de continuité" sont utilisés au cours d'opérations de maintenance et d'essai de continuité. Il existe deux variantes d'essai de continuité (COT, *continuity test*), l'une destinée à un usage général et l'autre employée dans le cas de plusieurs réseaux nationaux. Dans le premier cas, l'essai est un essai de bouclage. Le commutateur de départ enverra une tonalité (la tonalité aller) sur le circuit support et attendra que le commutateur d'arrivée effectue une boucle sur

---

[3] Les extrémités conformes au protocole TGCP ne sont actuellement pas exigées pour la prise en charge de la combinaison.

le circuit. Si le commutateur de départ observe que la même tonalité lui est renvoyée (la tonalité retour), l'essai COT a réussi. Dans le cas contraire, il a échoué. Dans le second cas, les tonalités aller et retour sont différentes. Le commutateur de départ envoie une certaine tonalité aller. Le commutateur d'arrivée détecte la tonalité aller, mais impose une tonalité retour différente dans la direction arrière. Lorsque le commutateur de départ détecte la tonalité retour, l'essai COT a réussi. S'il ne la détecte pas dans un certain délai, l'essai COT a échoué.

Lorsque le mode est "bouclage", la passerelle est censée renvoyer le signal entrant provenant d'une extrémité vers cette même extrémité. Ceci est la procédure générale. Si le mode est "essai de continuité", la passerelle est informée que l'autre bout du circuit a entamé une procédure d'essai de continuité conformément aux procédures spécifiées dans le cas de plusieurs réseaux nationaux. La passerelle placera le circuit en mode transpondeur nécessaire aux essais de continuité à deux tonalités.

En outre, lorsqu'une connexion à une extrémité est en mode "bouclage" ou "essai de continuité":

- les signaux audio reçus dans toute connexion à l'extrémité ne seront *pas* envoyés à l'extrémité;
- les signaux audio reçus à l'extrémité ne seront *pas* envoyés vers toute connexion à cette extrémité.

Si le mode est "bouclage en réseau", les signaux audio reçus par l'intermédiaire de la connexion seront répercutés et renvoyés dans cette même connexion. Le mode "bouclage en réseau" DEVRAIT simplement fonctionner comme un réflecteur de paquets conformes au protocole RTP.

Le mode "essai de continuité en réseau" est employé pour vérifier la continuité à travers le réseau IP. Un signal propre au type d'extrémité endpoint-type est envoyé vers les extrémités par l'intermédiaire du réseau IP, et les extrémités sont ensuite censées répercuter le signal dans le réseau IP après l'avoir fait passer par l'équipement interne de la passerelle pour vérifier le fonctionnement correct. Le signal DOIT passer par un décodage et un recodage internes avant d'être renvoyé. Pour les extrémités DS-0, le signal sera un signal audio, et il NE DOIT PAS être envoyé dans un circuit connecté à l'extrémité, quel que soit l'état effectif de prise de ce circuit.

Des connexions existantes et nouvelles à l'extrémité NE DOIVENT PAS être concernées par des connexions placées en modes "bouclage en réseau" ou "essai de continuité en réseau". Toutefois, des contraintes locales relatives aux ressources peuvent limiter le nombre de nouvelles connexions qui peuvent être établies.

Se référer à l'Appendice A.I en ce qui concerne les illustrations d'interactions des modes.

A.2.3.1 Commande NotificationRequest

La commande NotificationRequest est utilisée pour demander que la passerelle envoie une notification lorsque des événements spécifiés se produisent à une extrémité. Par exemple, une notification peut être demandée lorsque des tonalités associées à une communication destinée à la télécopie sont détectées à l'extrémité. L'entité recevant cette notification, habituellement le contrôleur MGC, peut alors décider qu'un type de codage différent devrait être utilisé dans les connexions aboutissant à cette extrémité et en informer la passerelle en conséquence[4].

```
ReturnCode
     ← NotificationRequest(EndpointId
                         [, NotifiedEntity]
                         [, RequestedEvents]
                         , RequestIdentifier
                         [, SignalRequests]
                         [, QuarantineHandling]
                         [, DetectEvents])
```

Le paramètre **EndpointId** est l'identificateur de l'extrémité ou des extrémités de la passerelle où la commande NotificationRequest est exécutée. Il suit les règles applicables aux noms d'extrémité spécifiées au A.2.1.1. Le caractère de remplacement "un quelconque" NE DOIT PAS être employé.

Le paramètre **NotifiedEntity** est un paramètre facultatif qui spécifie une nouvelle "entité notifiée" pour l'extrémité.

Le paramètre **RequestIdentifier** est employé pour relier cette demande avec la notification qu'elle peut déclencher. Il sera répété dans la commande Notify correspondante.

Le paramètre **SignalRequests** est un paramètre qui contient un ensemble de signaux que la passerelle est priée d'appliquer. Sauf mention contraire, les signaux sont appliqués à l'extrémité, mais certains signaux peuvent être appliqués à une connexion. Des exemples de signaux[5] sont donnés ci-après:

- essai de continuité;
- appel multifréquence de démarrage au système d'aide à l'exploitation.

Les signaux sont divisés en différents types en fonction de leur comportement:

- `On/off (OO)` (à désactivation) – Lorsqu'ils sont appliqués, ces signaux fonctionnent jusqu'à ce qu'ils soient arrêtés. Ceci ne peut se produire que lorsqu'un nouveau paramètre SignalRequests est défini, indiquant que le signal est désactivé (voir ci-dessous). Des signaux du type OO sont définis comme étant idempotents, donc plusieurs demandes d'activation (ou de désactivation) d'un signal OO donné sont parfaitement valables et NE DOIVENT PAS entraîner d'erreur. Lorsqu'ils sont activés, ils NE DOIVENT PAS être désactivés avant que le contrôleur MGC ne l'ait explicitement ordonné, ou que l'extrémité soit réinitialisée.
- `Time-out (TO)` (à temporisation) – Lorsqu'ils sont appliqués, ces signaux fonctionnent jusqu'à ce qu'ils soient arrêtés (en raison de la présence d'un événement ou du fait qu'ils n'ont pas été inclus dans une liste suivante [éventuellement vide] de signaux), ou qu'un intervalle de temps propre au signal s'est écoulé. Un signal qui est interrompu produira un événement "opération achevée" (se reporter à l'Annexe A.A.1 pour une définition plus approfondie de cet événement). Un signal TO pourrait consister en un " placement d'appel multifréquence" qui est interrompu après 16 secondes. Si un événement se produit avant la fin des 16

---

[4] La nouvelle instruction consisterait en la commande ModifyConnection.

[5] Veuillez vous reporter à l'Annexe A.A pour une liste exhaustive de signaux.

secondes, le signal sera arrêté[6] par défaut. Si le signal n'est pas arrêté, il sera interrompu, s'arrêtera et produira un événement "opération achevée", dont le contrôleur MGC peut éventuellement avoir demandé à être notifié. S'il a demandé à en être notifié, l'événement "opération achevée" qui lui est envoyé comprendra le ou les noms du ou des signaux qui ont été interrompus[7]. Le ou les signaux produits dans une connexion comporteront le nom de cette connexion. Une temporisation par défaut, qui peut être modifiée par le processus de configuration, est définie pour les signaux TO. La temporisation peut également être fournie comme un paramètre au signal. Une valeur nulle indique que la temporisation est illimitée. Un signal TO qui est défaillant, après avoir été activé, mais avant d'avoir produit un événement "opération achevée", produira un événement "échec de l'opération" qui comportera le ou les noms du ou des signaux qui ont été interrompus[7].

- `Brief (BR)` (bref) – La durée de ces signaux est tellement courte qu'ils s'arrêtent d'eux-mêmes. Si un événement tel que l'arrêt d'un signal se produit, ou qu'un nouveau paramètre SignalRequests est défini, un signal BR activé ne s'arrêtera pas. Toutefois, tout signal BR en attente non encore activé sera annulé.

Les signaux sont appliqués par défaut aux extrémités. Si un signal appliqué à une extrémité entraîne la production d'un flux média (audio, vidéo, etc.), le flux média NE DOIT PAS être transmis dans une connexion reliée à cette extrémité, quel que soit le mode de connexion. Par exemple, lorsqu'une tonalité est appliquée à une extrémité qui est impliquée dans une communication active, seule l'entité utilisant l'extrémité concernée entendra la tonalité. Des signaux différents peuvent toutefois définir un comportement différent.

Lorsqu'un signal est appliqué à une connexion qui a reçu un paramètre RemoteConnectionDescriptor (voir A.2.3.3), le flux média produit par ce signal sera transmis par l'intermédiaire de la connexion *quel que soit* le mode effectif de connexion. Si un paramètre RemoteConnectionDescriptor n'a pas été reçu, la passerelle DOIT renvoyer une erreur (code d'erreur 527 – Paramètre RemoteConnectionDescriptor manquant).

Lorsqu'une liste (éventuellement vide) de signaux est fournie, elle remplace entièrement la liste en cours des signaux TO activés. Les signaux TO effectivement activés qui ne sont pas fournis dans la nouvelle liste DOIVENT être arrêtés et le ou les nouveaux signaux fournis seront maintenant activés. Les signaux TO effectivement activés qui sont fournis dans la nouvelle liste DOIVENT rester activés sans interruption, et le temporisateur pour ces signaux TO ne sera donc pas modifié. Il n'y a en conséquence aucun moyen de relancer le temporisateur pour un signal TO effectivement activé sans désactiver le signal d'abord. Si le signal TO est paramétrisé, l'ensemble initial de paramètres restera valable, quelles que soient les valeurs qui sont fournies par la suite. Un signal donné NE DOIT PAS figurer plus d'une fois dans le paramètre SignalRequests.

On trouvera à l'Annexe A.A les signaux qui sont actuellement définis.

Le paramètre **RequestedEvents** est une liste d'événements que la passerelle est priée de détecter à l'extrémité. Sauf indication contraire, les événements sont détectés à l'extrémité. Toutefois, certains événements peuvent être détectés dans une connexion. Des exemples d'événements sont donnés ci-après:

- prise;
- tonalités relatives à la télécopie;
- opération achevée;
- appel multifréquence entrant.

---

[6] La commande "garder le ou les signaux activés" peut l'emporter sur ce comportement.

[7] Si les paramètres ont été transmis au signal, il n'en sera pas fait état.

On trouvera à l'Annexe A.A les événements qui sont actuellement définis.

A chaque événement sont associées une ou plusieurs **mesures** qui définissent celle que la passerelle doit prendre lorsque l'événement en question se produit. Les mesures possibles sont les suivantes:

- notifier l'événement immédiatement, en même temps que la liste des événements observés jusque-là;
- recueillir l'événement;
- ne pas tenir compte de l'événement;
- garder le ou les signaux activés;
- insérer la demande NotificationRequest;
- insérer la demande ModifyConnection.

Les types d'événements que l'extrémité sera priée de détecter sont au nombre de deux: les événements durables et les événements non durables.

Les événements durables sont toujours détectés à une extrémité. Si un événement durable ne fait pas partie de la liste des événements RequestedEvents, et qu'il se produit, il sera détecté de toute manière, et traité comme tous les autres événements, comme s'il avait été demandé au moyen d'une commande Notify[8]. Donc, sans que ce soit officiel, les événements durables peuvent être considérés comme faisant implicitement toujours partie de la liste des événements RequestedEvents avec effet sur la commande Notify, même si aucune détection manifeste, etc. n'aura lieu[9]. Les événements durables sont identifiés comme tels au moyen de leur définition – voir l'Annexe A.A.

Les événements non durables sont des événements qui doivent explicitement faire partie de la liste des événements RequestedEvents. La liste (éventuellement vide) d'événements demandés remplace entièrement la précédente liste d'événements demandés. L'extrémité détectera, outre les événements durables, seuls les événements qui figurent dans la liste des événements demandés. Si un événement durable fait partie le la liste des événements RequestedEvents, la mesure spécifiée remplacera la mesure par défaut associée à cet événement pendant la durée de vie de la liste, suite à quoi la mesure par défaut sera rétablie. Un événement donné NE DOIT PAS figurer plus d'une fois dans la liste des événements RequestedEvents.

On peut spécifier plus d'une mesure pour un événement, même si une mesure donnée ne peut figurer plus d'une fois pour un événement donné. Le Tableau A.1 spécifie les combinaisons admises de mesures:

---

[8] Le paramètre RequestIdentifier sera donc le paramètre RequestIdentifier de la commande effective NotificationRequest.

[9] Normalement, lorsqu'une demande d'observation de décrochage, par exemple, est faite, elle ne peut aboutir que si le combiné n'est pas encore décroché.

Tableau A.1/J.171 – Combinaisons admises de mesures

	Notifier	**Recueillir**	**Ne pas tenir compte**	**Garder le ou les signaux activés**	**Insérer la demande NotificationRequest**	**Insérer la demande ModifyConnection**
Notifier	–	–	–	√	–	√
Recueillir	–	–	–	√	√	√
Ne pas tenir compte	–	–	–	√	–	√
Garder le ou les signaux activés	√	√	√	–	√	√
Insérer la demande NotificationRequest	–	√	–	√	–	√
Insérer la demande ModifyConnection	√	√	√	√	√	–

Si un client reçoit une demande comportant une mesure non valable ou une combinaison non admise de mesures, il DOIT renvoyer une erreur au contrôleur MGC (code d'erreur 523 – Mesure inconnue ou combinaison non admise de mesures).

Lorsque de nombreuses mesures sont spécifiées, par exemple "garder le ou les signaux activés" et "notifier", les différentes mesures sont supposées être prises simultanément.

Un contrôleur MGC peut envoyer à la passerelle une commande NotificationRequest dont la liste des événements RequestedEvents est vide. Les événements durables seront toutefois encore détectés et notifiés.

Les signaux étant appliqués à la suite de la commande SignalRequests sont synchronisés avec l'ensemble des événements spécifiés dans le paramètre RequestedEvents ou découlant de lui, sauf si la mesure " garder le ou les signaux activés" l'emporte. La définition formelle stipule que la production de tous les signaux TO DOIT s'arrêter dès qu'un des événements demandés est détecté, à moins que la mesure " garder le ou les signaux activés" ne soit associée à l'événement spécifié.

Si l'on souhaite qu'un ou des signaux TO restent activés lorsqu'un événement recherché se produit, la mesure " garder le ou les signaux activés" peut être utilisée. Cette mesure a pour effet de recueillir l'activité de tous les signaux TO effectivement activés, en refusant l'arrêt par défaut des signaux TO lorsqu'un événement se produit.

Si l'on souhaite qu'un ou des signaux débutent lorsqu'un événement recherché se produit, la mesure "insérer la demande NotificationRequest " peut être utilisée. La demande insérée NotificationRequest peut comporter une nouvelle liste d'événements RequestedEvents et une nouvelle commande SignalRequests. Elle ne peut toutefois pas inclure une autre commande "insérer la demande NotificationRequest". Lorsqu'elle est activée, la liste des événements observés et le tampon de quarantaine resteront inchangés (voir A.2.4.3.1).

La mesure relative à la demande insérée NotificationRequest permet au contrôleur MGC d'élaborer un "miniscript" devant être traité par la passerelle immédiatement après la détection de l'événement associé. Toute commande SignalRequests qui est spécifiée dans la demande insérée NotificationRequest sera déclenchée immédiatement. Il importe de veiller à ce que les désaccords entre le contrôleur MGC et la passerelle soient évités. Des désaccords à long terme ne devraient toutefois pas avoir lieu puisque de nouvelles commandes SignalRequests remplacent complètement l'ancienne liste de signaux TO activés, et que les signaux de type BR s'arrêtent toujours d'eux-mêmes. Il est recommandé de limiter le nombre de signaux de type OO. Il est souhaitable que le contrôleur MGC n'active qu'occasionnellement tous les signaux OO qui devraient être activés, et ne désactive qu'occasionnellement aussi tous ceux qui devraient être désactivés.

Si l'on désire changer les modes de connexion lorsqu'un événement recherché se produit, la mesure "insérer la demande ModifyConnection" peut être utilisée. La demande insérée ModifyConnection peut comporter une liste des changements de mode de connexion, chacun de ceux-ci incluant le changement de mode et l'identificateur de la connexion concerné. Le caractère de remplacement "$" peut être utilisé pour indiquer la "connexion effective", mais cette notation NE DOIT PAS être employée en dehors d'une commande de prise en charge de connexion – le caractère de remplacement se rapporte à la connexion concernée pour la commande de prise en charge de connexion.

La mesure relative à la demande insérée ModifyConnection permet au contrôleur MGC d'ordonner à l'extrémité de modifier le mode de connexion de l'une ou de plusieurs connexions immédiatement après la détection de l'événement associé. Chaque changement de mode de connexion fonctionne d'une manière qui est semblable à la commande ModifyConnection correspondante. Lorsqu'une liste des changements de mode de connexion est fournie, les changements de mode de connexion DOIVENT être appliqués l'un après l'autre en allant de gauche à droite. Lorsque tous les changements de mode de connexion ont été effectués, un événement "opération achevée" paramétrisé au moyen du nom de la mesure achevée se produira (voir l'Annexe A.A pour plus de détails). Si l'un des changements de mode de connexion devait échouer, un événement "échec de l'opération" paramétrisé au moyen du nom de la mesure et du changement de mode de connexion qui ont échoué se produira (voir l'Annexe A.A pour plus de détails) – les autres changements de mode de connexion NE DOIVENT PAS être tentés, et les précédents changements réussis de mode de connexion dans la liste NE DOIVENT PAS être modifiés non plus.

Finalement, la mesure ne pas tenir compte peut être employée pour ne pas tenir compte d'un événement, à savoir pour éviter qu'un événement durable soit notifié. Toutefois, la synchronisation entre l'événement et le signal activé se fera encore par défaut.

NOTE – Le paragraphe A.2.4.3.1 contient des détails supplémentaires sur la sémantique de la détection et du rapport des événements. Le lecteur est invité à examiner cette question avec soin.

La définition particulière des mesures qui sont nécessaires pour répondre aux commandes SignalRequests sort du cadre de la présente Recommandation de base relative au protocole TGCP. Cette définition peut varier d'un endroit à l'autre, et donc d'une passerelle à l'autre. En conséquence, les définitions qui sont fournies dans des paquetages d'événements peuvent être données en dehors de la présente Recommandation de base. On trouvera une liste initiale des paquetages d'événements à l'Annexe A.A.

Les commandes RequestedEvents et SignalRequests se réfèrent généralement aux mêmes événements. Dans un cas, la passerelle est priée de détecter les occurrences d'un événement, tandis que dans l'autre cas, elle est priée de le produire. Il n'y a que peu d'exceptions à cette règle, notamment en ce qui concerne les tonalités relatives à la télécopie et au modem, qui peuvent être détectées mais ne peuvent être signalées. Toutefois, nous ne pouvons forcément pas nous attendre que toutes les extrémités détectent tous les événements. Les événements et les signaux particuliers qu'une extrémité donnée peut détecter ou produire sont déterminés en fonction de la liste des paquetages d'événements qui sont pris en charge par cette extrémité. Chaque paquetage spécifie une liste d'événements et de signaux qui peuvent être détectés ou appliqués. Une passerelle qui est priée de détecter ou d'appliquer un événement appartenant à un paquetage qui n'est pas pris en charge par l'extrémité spécifiée DOIT renvoyer une erreur (code d'erreur 512 ou 513 – Non équipé pour la détection d'un événement ou la production d'un signal). Lorsque le nom d'un événement n'est pas spécifié par un nom de paquetage, on suppose que le nom de paquetage pour l'extrémité est le nom par défaut. Si le nom de l'événement n'est pas enregistré dans ce paquetage par défaut, la passerelle DOIT renvoyer une erreur (code d'erreur 522 – Evénement ou signal inexistant).

Le contrôleur MGC peut envoyer une demande NotificationRequest dont la liste des signaux demandés est vide. Ceci a pour effet d'arrêter tous les signaux TO activés. Il peut agir de la sorte, par exemple, lorsque l'émission d'une tonalité, à savoir un rappel automatique, devrait s'arrêter.

Le paramètre **QuarantineHandling** est un paramètre facultatif qui spécifie les options de traitement pour le tampon de quarantaine (voir A.2.4.3.1). Il permet au contrôleur MGC de spécifier si les événements en quarantaine doivent être traités ou rejetés. S'il n'est pas présent, les événements en quarantaine DOIVENT être traités.

Le paramètre **DetectEvents** est un paramètre facultatif qui spécifie une liste minimale d'événements que la passerelle est priée de détecter dans l'état de "notification" et dans l'état "figé". La liste est valable jusqu'à ce qu'une nouvelle valeur soit spécifiée. On trouvera d'autres explications relatives à ce paramètre au A.2.4.3.1.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.2 Notifications

Les notifications sont envoyées par la passerelle à l'aide de la commande Notify lorsqu'un événement observé doit être notifié:

```
ReturnCode
     ← Notify(EndpointId
               [, NotifiedEntity]
               , RequestIdentifier
               , ObservedEvents)
```

Le paramètre **EndpointId** est le nom de l'extrémité de la passerelle, provenant de la commande Notify, comme défini au A.2.1.1. L'identificateur DOIT être un nom d'extrémité complètement spécifié, comprenant le nom de domaine de la passerelle. La partie locale du nom NE DOIT PAS faire appel à la convention concernant les caractères de remplacement.

Le paramètre **NotifiedEntity** est un paramètre facultatif qui identifie l'entité à laquelle la notification est envoyée. Ce paramètre est le même que celui qui figure dans la commande NotificationRequest à l'émetteur de cette notification. Il n'est pas présent lorsqu'un tel paramètre ne figurait pas dans la demande ayant suscité la notification. Quelle que soit la valeur du paramètre NotifiedEntity, la notification DOIT être envoyée à "l'entité notifiée" pour cette extrémité.

Le paramètre **RequestIdentifier** est un paramètre qui est le même que celui qui figure dans la commande NotificationRequest ayant suscité cette notification. Il est employé pour corréler cette notification avec la demande de notification qui en est à l'origine. Le événements durables seront considérés ici comme ayant été inclus dans la dernière commande NotificationRequest. Lorsqu'aucune commande NotificationRequest n'a été reçue, la valeur de l'identificateur RequestIdentifier utilisé sera nulle ("0").

Le paramètre **ObservedEvents** est une liste d'événements que la passerelle a détectés et recueillis, soit par des mesures de "recueil", soit par des mesures de "notification". Une seule notification peut faire état d'une liste d'événements qui seront rapportés dans l'ordre de leur détection. La liste ne peut contenir que des événements durables et des événements qui ont été demandés dans le paramètre RequestedEvents de la commande NotificationRequest ayant suscité la notification. Les événements détectés dans une connexion comprendront le nom de cette connexion. La liste contiendra les événements qui ont été recueillis (mais non notifiés) et l'événement final qui à été à l'origine de la notification.

Le paramètre **ReturnCode** est un paramètre renvoyé par le contrôleur MGC. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.3 Commande CreateConnection

Cette commande est utilisée pour établir une connexion.

```
ReturnCode
, ConnectionId
[, SpecificEndPointId]
, LocalConnectionDescriptor,
          ← CreateConnection(CallId
               , EndpointId
                              [, NotifiedEntity]
                              , LocalConnectionOptions
                              , Mode
                              [, RemoteConnectionDescriptor]
                              [, RequestedEvents]
                              [, RequestIdentifier]
                              [, SignalRequests]
                              [, QuarantineHandling]
                              [, DetectEvents])
```

Cette fonction est utilisée lors de l'établissement d'une connexion entre deux extrémités. Une connexion est définie par ses attributs et les extrémités qu'elle relie. Les paramètres d'entrée dans la commande CreateConnection fournissent les informations nécessaires pour construire l'une des deux "vues" des extrémités d'une connexion.

Le paramètre **CallId** est un paramètre qui identifie l'appel (ou la session) auquel cette connexion appartient. Au minimum, ce paramètre est unique auprès de l'ensemble des contrôleurs MGC qui commandent les mêmes passerelles; les connexions qui font partie du même appel ont le même identificateur d'appel. Celui-ci peut être utilisé pour identifier les appels aux fins de rapport et de comptabilité.

Le paramètre **EndpointId** est l'identificateur de l'extrémité de la passerelle où la commande CreateConnection est exécutée. Cet identificateur peut entièrement être spécifié si le paramètre EndpointId de la fonction d'appel a une valeur qui n'est pas un caractère de remplacement ou il peut être sous-spécifié lorsqu'il est fait appel à la convention concernant le caractère de remplacement "un quelconque". Si l'extrémité est sous-spécifiée, la valeur de son identificateur sera attribuée par la passerelle et elle sera renvoyée dans son entièreté dans le paramètre **SpecificEndPointId** de la réponse. La convention concernant le caractère de remplacement "tous" NE DOIT PAS être employée.

Le paramètre **NotifiedEntity** est un paramètre facultatif qui spécifie une nouvelle "entité notifiée" pour l'extrémité.

Le paramètre **LocalConnectionOptions** est une structure décrivant les caractéristiques de la connexion média du point de vue de la passerelle qui exécute la commande CreateConnection. Il informe l'extrémité sur les caractéristiques relatives à l'envoi et à la réception de la connexion média. Les champs fondamentaux contenus dans le paramètre LocalConnectionOptions sont les suivants:

- **méthode de codage**: une liste des noms littéraux pour l'algorithme de compression (méthode de codage/décodage) employé pour envoyer et recevoir des données médias par l'intermédiaire de la connexion DOIT être spécifiée et comporter au moins une valeur. Les rubriques de cette liste sont classées par ordre de préférence. L'extrémité DOIT choisir un et un seul codec, et ce choix DEVRAIT se faire selon la préférence indiquée. Si l'extrémité reçoit par l'intermédiaire de la connexion des données médias codées à l'aide d'une méthode de codage différente, elle PEUT les ignorer. L'extrémité DOIT en outre indiquer quels autres algorithmes de compression elle est prête à prendre en charge en tant qu'algorithmes de remplacement – voir A.3.4.1 pour plus de détails. Une liste des méthodes de codage admissibles est spécifiée dans un document IPCablecom distinct;

- **période de mise en paquets**: la période de mise en paquets exprimée en millisecondes, telle qu'elle est définie dans la norme relative au protocole SDP (document IETF RFC 2327), DOIT être spécifiée et comporter une et une seule valeur. La valeur ne se rapporte qu'aux données médias envoyées. Une liste des périodes de mise en paquets admissibles est spécifiée dans une Recommandation IPCablecom distinct;
- **suppression d'écho**: ce paramètre indique si la suppression d'écho devrait être employée du côté jonction ou pas[10]. Il peut prendre la valeur "activé" (lorsque la suppression d'écho est demandée) ou "désactivé" (lorsqu'elle est désactivée). Il est facultatif. Lorsqu'il est omis, la passerelle de jonction DOIT employer la suppression d'écho;
- **type de service**: ce paramètre spécifie la classe de service qui sera utilisée pour l'envoi de données médias par l'intermédiaire de la connexion en codant le paramètre de l'en-tête IP à 8 bits correspondant au type de service sous la forme de deux chiffres hexadécimaux. Il est facultatif. Lorsqu'il est omis, une valeur par défaut de $A0_H$ est utilisée, correspondant à l'attribution de la valeur cinq aux bits de priorité IP;
- **suppression des silences**: ce paramètre indique si la suppression des silences devrait être employée ou pas dans le sens de l'envoi. Il peut prendre la valeur "activé" (lorsque les silences doivent être supprimés) ou "désactivé" (lorsque ce n'est pas le cas). Il est facultatif. Lorsqu'il est omis, la valeur par défaut est de ne pas employer la suppression des silences.

En outre, les champs suivants du paramètre LocalConnectionOptions sont utilisés pour la prise en charge des services de sécurité IPCablecom:

- **code secret**: le code secret en option consiste en une valeur de départ qui DOIT être utilisée pour déduire les clés de chiffrement de bout en bout pour les services de sécurité des protocoles RTP et RTCP comme spécifié dans la Rec. UIT-T J.170. Le code secret DEVRAIT être codé sous la forme de texte en clair s'il ne contient que des valeurs dans la gamme des caractères ASCII s'étendant de 21_H à $7E_H$. Sinon, le code secret DOIT être codé à l'aide du codage en base64. Si aucune valeur n'est fournie, ou que ce paramètre est omis et que les services de sécurité doivent être employés, l'extrémité DOIT produire elle-même un code secret[11]. Lorsqu'un code secret est fourni par le contrôleur MGC, ce code DEVRAIT être utilisé;
- **suite de chiffrement pour le protocole RTP**: ce paramètre consiste en une liste de suites de chiffrement pour la sécurité du protocole RTP. Les rubriques de cette liste sont classées par ordre de préférence, la première suite correspondant au choix préféré. L'extrémité DOIT choisir une et une seule suite de chiffrement. Elle DEVRAIT en outre indiquer quelles autres suites de chiffrement elle est prête à prendre en charge en tant que suites de remplacement (voir A.3.4.1 pour plus de détails). Chaque suite de chiffrement est représentée par des chaînes ASCII composées de deux sous-chaînes (éventuellement vides) séparées par une barre oblique ("/"), la première sous-chaîne identifiant l'algorithme d'authentification tandis que la seconde sous-chaîne identifie l'algorithme de chiffrement. Une liste des suites de chiffrement admissibles est spécifiée dans la Rec. UIT-T J.170 relative à la sécurité dans l'architecture IPCablecom;
- **suite de chiffrement pour le protocole RTCP**: ce paramètre consiste en une liste de suites de chiffrement pour la sécurité du protocole RTCP. Les rubriques de cette liste sont classées par ordre de préférence, la première suite correspondant au choix préféré. L'extrémité DOIT choisir une et une seule suite de chiffrement. Elle DEVRAIT en outre indiquer quelles autres suites de chiffrement elle est prête à prendre en charge en tant que suites de remplacement

---

[10] La suppression d'écho du côté paquet n'est pas prise en charge.

[11] Cela comprend aussi bien la production d'un nouveau code secret que l'utilisation d'un code secret fourni dans un paramètre RemoteConnectionDescriptor.

(voir A.3.4.1 pour plus de détails). Chaque suite de chiffrement est représentée par des chaînes ASCII composées de deux sous-chaînes (éventuellement vides) séparées par une barre oblique ("/"), la première sous-chaîne identifiant l'algorithme d'authentification tandis que la seconde sous-chaîne identifie l'algorithme de chiffrement. Une liste des suites de chiffrement admissibles est spécifiée dans la Rec. UIT-T J.170 relative à la sécurité dans l'architecture IPCablecom.

Le protocole TGCP permet en outre de prendre en charge la surveillance électronique IPCablecom (voir le document PKT-SP-ESP-I01-991229). Lorsqu'une connexion est soumise à une surveillance électronique, tous les paquets médias valables reçus par l'intermédiaire de la connexion et tous les paquets médias envoyés par l'intermédiaire de la connexion seront dupliqués et transmis à une fonction chargée d'assurer la surveillance électronique[12], après insertion d'un identificateur de la connexion relatif au contenu de l'appel. Cette duplication se fera suivant le mode de la connexion, sauf pour les données médias produites par des signaux appliqués à la connexion, qui seront dupliquées sans tenir compte du mode de connexion. Par exemple, une connexion en mode "inactif" ne produira pas de données médias qui seront interceptées[13], tandis qu'une connexion en mode "sendonly" ne produira que des données qui seront interceptées dans le sens de l'envoi. Il ne sera pas tenu compte des paquets dupliqués dans les statistiques relatives à la connexion. Les champs suivants du paramètre LocalConnectionOptions sont utilisés pour la prise en charge la surveillance électronique IPCablecom (voir le document PKT-SP-ESP-I01-991229 pour plus de détails):

- **identificateur de la connexion relatif au contenu de l'appel**: l'identificateur de la connexion relatif au contenu de l'appel (CCC, *call content connection*) est une valeur à 32 bits qui spécifie l'identificateur devant être utilisé pour une connexion qui est soumise à la surveillance électronique. Il sera ajouté à l'en-tête des paquets vocaux qui seront interceptés;
- **destination relative au contenu de l'appel**: la destination relative au contenu de l'appel spécifie une adresse Ipv4 suivie d'un point-virgule et d'un numéro de port UDP. Elle spécifie l'adresse IP de destination et le port pour le contenu de l'appel devant être intercepté.

La passerelle de jonction DOIT répondre par un code d'erreur (code d'erreur 524 – Incohérence en ce qui concerne un champ LocalConnectionOptions) lorsqu'une des règles susmentionnées est violée. Toutes les valeurs par défaut susmentionnées peuvent être modifiées au cours du processus de configuration.

Le paramètre **RemoteConnectionDescriptor** est un descripteur de connexion pour le côté à distance d'une connexion, de l'autre côté du réseau IP. Il comporte les mêmes champs que le paramètre LocalConnectionDescriptor (à ne pas confondre avec le paramètre LocalConnectionOptions), à savoir les champs qui décrivent une session conformément à la norme du protocole SDP. Le paragraphe A.3.4 donne des détails sur l'utilisation prise en charge du protocole SDP dans le profil du protocole TGCP. Ce paramètre peut avoir une valeur nulle lorsque l'information pour l'extrémité distante n'est pas connue. Cela peut se produire parce que l'entité qui établit une connexion commence par envoyer une commande CreateConnection à l'une des deux passerelles impliquées. Lorsque la première commande est lancée, aucune information n'est disponible sur l'autre côté de la connexion. Cette information peut être fournie plus tard au moyen d'un appel ModifyConnection.

Dans le profil du protocole TGCP, on suppose actuellement que les paramètres médias qui s'appliquent à une connexion dans le sens de l'envoi sont les mêmes que dans le sens de la réception. Une partie de l'information contenue dans le paramètre RemoteConnectionDescriptor est donc redondante et il peut y avoir des incohérences avec le paramètre LocalConnectionOptions. Le

---

[12] Il convient de noter que la duplication se fait au niveau du réseau – Voir le document PKT-SP-ESP-I01-991229 pour plus de détails.

[13] On suppose qu'aucun signal produisant des données médias n'a été activé dans la connexion.

contrôleur MGC a toutefois seul la responsabilité de faire en sorte qu'il lance des commandes cohérentes à chaque extrémité afin que des paramètres médias cohérents puissent être spécifiés. Si une incohérence est détectée par une passerelle malgré tout, le paramètre LocalConnectionOptions aura simplement la priorité. Lorsque des codecs sont modifiés pendant une communication, il se peut que pendant de courtes périodes les extrémités utilisent des codes différents. Comme mentionné ci-dessus, les passerelles de jonction PEUVENT ignorer toute donnée média reçue qui est codée au moyen d'un codec différent de celui qui est spécifié dans le paramètre LocalConnectionOptions de la connexion.

Le paramètre **Mode** indique le mode de fonctionnement de ce côté de la connexion. Les options sont "envoi seulement", "réception seulement", "envoi/réception", "inactif", "bouclage en réseau" ou "essai de continuité en réseau". Le traitement de ces modes est spécifié au début du A.2.3. Certaines extrémités peuvent ne pas être en mesure de prendre en charge tous les modes – Voir l'Appendice A.V.1. Si la commande spécifie un mode que l'extrémité ne prend pas en charge, une erreur DOIT être renvoyée (code d'erreur 517 – Mode non pris en charge). Par ailleurs, lorsqu'une connexion n'a pas encore reçu le paramètre RemoteConnectionDescriptor, une erreur DOIT être renvoyée dans le cas où il a été tenté de placer la connexion dans l'un des modes "envoi seulement" ou "envoi/réception" (code d'erreur 527 – Paramètre RemoteConnectionDescriptor manquant).

Le paramètre **ConnectionId** est un paramètre renvoyé par la passerelle qui identifie de manière univoque la connexion dans le contexte de l'extrémité considérée.

Le paramètre **LocalConnectionDescriptor** est un paramètre renvoyé par la passerelle, qui fournit une description de session contenant des informations, par exemple, sur des adresses et des ports RTP pour les connexions "IN" telles qu'elles sont définies dans le protocole SDP. Il est semblable au paramètre RemoteConnectionDescriptor, sauf qu'il spécifie ce côté de la connexion. Le paragraphe A.3.4 donne des détails sur l'utilisation prise en charge du protocole SDP dans le profil du protocole TGCP.

Lorsqu'une passerelle reçoit une commande "CreateConnection" qui ne comprend pas de paramètre RemoteConnectionDescriptor, elle est dans une situation ambiguë en ce qui concerne la connexion en question. Comme elle a envoyé un paramètre LocalConnectionDescriptor, elle pourrait recevoir des paquets par l'intermédiaire de cette connexion. Mais comme elle n'a pas encore reçu le paramètre RemoteConnectionDescriptor de l'autre passerelle, elle ne sait pas si les paquets qu'elle reçoit ont été admis par le contrôleur MGC. Elle doit donc naviguer entre deux risques, à savoir la coupe de certaines annonces importantes et l'écoute de données insensées. Le comportement de la passerelle est déterminé par la valeur du paramètre mode (soumis à le sécurité):

- si le mode est "réception seulement", la passerelle DOIT accepter les signaux vocaux reçus par l'intermédiaire de la connexion et les transmettre vers l'extrémité;
- si le mode est "inactif", "bouclage" ou "essai de continuité", la passerelle DOIT (comme toujours) ignorer les signaux vocaux reçus par l'intermédiaire de la connexion;
- si le mode est "bouclage en réseau" ou "essai de continuité en réseau", la passerelle DOIT répercuter ou répondre, comme attendu. Les données médias répercutées ou produites DOIVENT être envoyées à la source dont elles proviennent.

Il convient de noter que lorsque l'extrémité ne dispose pas du paramètre RemoteConnectionDescriptor pour la connexion, celle-ci peut par définition ne pas être dans les modes "envoi seulement" ou "envoi/réception".

Les paramètres **RequestedEvents, RequestIdentifier, SignalRequests, QuarantineHandling** et **DetectEvents** sont tous facultatifs. Ils peuvent être utilisés par le contrôleur MGC pour insérer effectivement une demande de notification qui soit exécutée simultanément avec l'établissement de la connexion. Si un ou plusieurs paramètres sont présents, le paramètre RequestIdentifier DOIT faire partie de ceux-là. L'insertion d'une demande de notification peut donc être confirmée par la présence du paramètre RequestIdentifier. Les autres paramètres peuvent être présents ou pas. Si l'un des

paramètres fait défaut, la demande DOIT être traitée comme si elle était une demande NotificationRequest normale, le paramètre en question ayant été omis. Cela peut avoir pour effet d'annuler des signaux et d'arrêter la recherche des événements.

Considérons, en guise d'exemple d'utilisation, un contrôleur MGC qui souhaiterait placer un appel à destination d'un système de services d'un opérateur par l'intermédiaire d'une passerelle de jonction multifréquence. Ce contrôleur MGC pourrait:

- demander à la passerelle de jonction d'établir une connexion, afin de s'assurer que la passerelle média dispose des ressources nécessaires à l'appel;
- demander à la passerelle de jonction de mettre en état de prise un circuit multifréquence de services d'opérateur et lancer l'appel;
- demander à la passerelle de jonction de notifier le contrôleur MGC lorsque l'appel a été placé.

On peut effectuer toutes les opérations qui sont décrites ci-dessus à l'aide d'une seule commande CreateConnection, en incluant une demande de notification avec le paramètre RequestedEvents pour l'événement réponse et le paramètre SignalRequests pour le signal d'établissement.

Lorsque ces paramètres sont présents, l'établissement de la connexion et la demande de notification DOIVENT être synchronisés, ce qui veut dire qu'ils sont tous deux soit acceptés soit refusés. Dans notre exemple, la commande CreateConnection doit être refusée si la passerelle ne dispose pas de ressources suffisantes ou ne peut obtenir de l'accès au réseau local les ressources appropriées. La demande de notification de lancement d'un appel doit être refusée en situation d'interférence lorsque le circuit est déjà pris. Dans cet exemple, l'appel ne doit pas être placé si la connexion ne peut être établie, et la connexion ne doit pas être établie si le circuit est déjà pris. Au lieu de cela, une erreur devrait être renvoyée (code d'erreur 401 – Circuit déjà pris), qui informerait le contrôleur MGC de la situation d'interférence.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.4 Commande ModifyConnection

Cette commande est utilisée pour modifier les caractéristiques de la "vue" d'une connexion par une passerelle. Cette "vue" de l'appel comprend aussi bien le descripteur de connexion local que le descripteur de connexion distant.

```
ReturnCode
[, LocalConnectionDescriptor]
              ← ModifyConnection(CallId
                                 , EndpointId
                                 , ConnectionId
                                 [, NotifiedEntity]
                                 [, LocalConnectionOptions]
                                 [, Mode]
                                 [, RemoteConnectionDescriptor]
                                 [, RequestedEvents]
                                 [, RequestIdentifier]
                                 [, SignalRequests]
                                 [, QuarantineHandling]
                                 [, DetectEvents])
```

Les paramètres utilisés sont les mêmes que ceux de la commande CreateConnection, avec en outre un paramètre **ConnectionId** qui identifie de manière univoque la connexion dans le contexte de l'extrémité. Ce paramètre est renvoyé par la commande CreateConnection en même temps que le descripteur de connexion local.

La paramètre **EndpointId** DOIT être un nom d'extrémité entièrement spécifié. Le nom local NE DOIT PAS faire appel à la convention concernant le caractère de remplacement.

La commande ModifyConnection peut être employée pour attribuer des paramètres de connexion, soumis aux mêmes règles et contraintes que celles qui ont été spécifiées pour la commande CreateConnection:

- fournir des informations sur l'autre bout de la connexion par l'intermédiaire du paramètre **RemoteConnectionDescriptor**;
- activer ou désactiver la connexion en modifiant la valeur du paramètre **mode**. Cela peut être fait à tout moment pendant de la connexion, les valeurs des paramètres étant arbitraires. La valeur du mode pour une activation peut par exemple être "réception seulement";
- modifier les paramètres de la connexion par l'intermédiaire du paramètre **LocalConnectionOptions**, par exemple, en passant à un système de codage différent, en modifiant la période de mise en paquets ou en changeant le traitement de la suppression d'écho.

La commande ne renverra un paramètre **LocalConnectionDescriptor** que si les paramètres de connexion locaux, tels que les ports RTP, etc., sont modifiés. Donc, si, par exemple, seul le mode de connexion est changé, un paramètre LocalConnectionDescriptor ne sera pas renvoyé. Si un paramètre de connexion est omis, par exemple, le mode ou la suppression des silences, l'ancienne valeur de ce paramètre sera conservée si possible. Si une modification de paramètre nécessite un changement d'un ou de plusieurs paramètres *non spécifiés*, la passerelle est libre de choisir des valeurs adaptées pour les paramètres non spécifiés qui doivent être modifiés[14].

Les informations concernant les adresses RTP fournies dans le paramètre RemoteConnectionDescriptor spécifient l'adresse RTP distante du récepteur de données médias pour la connexion. Ces informations peuvent avoir été modifiées par le contrôleur MGC[15]. Lorsqu'elles sont fournies à une passerelle de jonction pour une connexion, la passerelle ne DEVRAIT accepter que les flux médias (et conformes au protocole RTCP) en provenance des adresses RTP spécifiées également. Tout flux média reçu provenant d'autres adresses DEVRAIT être ignoré. La Rec. UIT-T J.170 relative à la sécurité dans l'architecture IPCablecom devrait être consultée au sujet de normes de sécurité supplémentaires.

Les paramètres **RequestedEvents, RequestIdentifier, SignalRequests, QuarantineHandling** et **DetectEvents** sont facultatifs. Ils peuvent être utilisés par le contrôleur MGC pour insérer une demande de notification qui soit liée à la modification de la connexion et exécutée simultanément avec elle. Si un ou plusieurs paramètres sont fournis, le paramètre RequestIdentifier DOIT faire partie de ceux-là.

Lorsque ces paramètres sont présents, la modification de la connexion et la demande de notification DOIVENT être synchronisées, ce qui veut dire qu'elles sont toutes deux soit acceptées soit refusées.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

---

[14] Ceci peut par exemple se produire lorsqu'une modification de codec est spécifiée, et que l'ancien codec employait la suppression des silences, tandis que le nouveau ne le prend pas en charge. Si, par exemple, la période de mise en paquets n'a en outre pas été spécifiée, et que le nouveau codec prend en charge l'ancienne période de mise en paquets, la valeur de ce paramètre ne changerait pas, puisqu'un changement ne serait pas nécessaire.

[15] Par exemple, lorsque les données médias doivent franchir un coupe-feu.

A.2.3.5 Commande DeleteConnection (par le contrôleur de passerelle média)

Cette commande est utilisée pour mettre fin à une connexion. Une conséquence indirecte de cette commande est la collecte de statistiques relatives à l'exécution de la connexion.

```
ReturnCode
, Connection-parameters
     ← DeleteConnection(CallId
                        , EndpointId
                        , ConnectionId
                        [, NotifiedEntity]
                        [, RequestedEvents]
                        [, RequestIdentifier]
                        [, SignalRequests]
                        [, QuarantineHandling]
                        [, DetectEvents])
```

Dans cette forme de la commande DeleteConnection, l'identificateur de l'extrémité DOIT être entièrement spécifié. La convention concernant les caractères de remplacement NE DOIT PAS être employée.

Dans le cas général où une connexion a deux extrémités, cette commande doit être envoyée aux deux passerelles impliquées dans la connexion. Après la suppression de la connexion, les flux médias du réseau en mode paquet précédemment pris en charge par la connexion ne sont plus disponibles. Tout paquet média reçu pour l'ancienne connexion est simplement ignoré, et aucun nouveau paquet média pour le flux n'est envoyé.

En réponse à la commande DeleteConnection, la passerelle renvoie une liste de paramètres qui décrivent l'état de la connexion[16]. Ces paramètres sont les suivants:

- **nombre de paquets envoyés**: nombre total de paquets de données conformes au protocole RTP transmis par l'envoyeur depuis le début de la transmission par l'intermédiaire de la connexion. Le comptage n'est pas réinitialisé lorsque l'envoyeur modifie son identificateur de source de synchronisation (SSRC, *synchronization source*) telle qu'elle est définie dans le protocole RTP, par exemple, suite à une commande Modify. La valeur est nulle lorsque la connexion a toujours été en mode "réception seulement";
- **nombre d'octets envoyés**: nombre total d'octets de charge utile (à savoir, pas ceux de l'en-tête ou du bourrage) transmis dans les paquets de données conformes au protocole RTP par l'envoyeur depuis le début de la transmission par l'intermédiaire de la connexion. Le comptage n'est pas réinitialisé lorsque l'envoyeur modifie son identificateur SSRC, par exemple, suite à une commande ModifyConnection. La valeur est nulle lorsque la connexion a toujours été en mode "réception seulement";
- **nombre de paquets reçus**: nombre total de paquets de données conformes au protocole RTP reçus par l'envoyeur depuis le début de la réception par l'intermédiaire de la connexion. Le comptage inclut les paquets reçus des différentes sources SSRC si l'envoyeur en a utilisées plusieurs. La valeur est nulle lorsque la connexion a toujours été en mode "envoi seulement";
- **nombre d'octets reçus**: nombre total d'octets de charge utile (à savoir, pas ceux de l'en-tête ou du bourrage) reçus par l'envoyeur depuis le début de la réception par l'intermédiaire de la connexion. Le comptage inclut les paquets reçus des différentes sources SSRC si l'envoyeur en a utilisées plusieurs. La valeur est nulle lorsque la connexion a toujours été en mode "envoi seulement";

[16] Les valeurs calculées ne comprendront pas les paquets qui proviennent de la surveillance électronique.

- **nombre de paquets perdus**: nombre total de paquets de données conformes au protocole RTP qui ont été perdus depuis le début de la réception. Ce nombre est défini comme étant le nombre de paquets attendus moins le nombre de paquets réellement reçus, celui-ci incluant tout paquet tardif ou double. Donc, les paquets qui arrivent en retard ne sont pas considérés comme étant perdus, et la perte peut être négative lorsqu'ils arrivent en double. Le nombre de paquets attendus est défini comme étant le nombre dans la toute dernière séquence reçue moins le nombre dans la séquence initiale reçue. Le comptage inclut les paquets reçus des différentes sources SSRC si l'envoyeur en a utilisées plusieurs. La valeur est nulle lorsque la connexion a toujours été en mode "envoi seulement";
- **gigue entre les arrivées**: évaluation de la variance statistique du temps entre les arrivées des paquets de données conformes au protocole RTP mesuré en millisecondes et exprimé comme un nombre entier sans signe. La gigue entre les arrivées "J" est définie comme étant la déviation moyenne (valeur absolue lissée) de la différence "D" de l'espacement des paquets au niveau du récepteur comparée à celle qui est observée au niveau de l'émetteur pour une paire de paquets. On trouvera des algorithmes de calcul détaillés dans le document IETF RFC 1889. Le comptage inclut les paquets reçus des différentes sources SSRC si l'envoyeur en a utilisées plusieurs. La valeur est nulle lorsque la connexion a toujours été en mode "envoi seulement";
- **délai moyen de transmission**: évaluation du temps d'attente dans le réseau, exprimé en millisecondes. Ceci est une valeur moyenne de la différence entre les horodateurs NTP de ceux qui envoient des messages conformes au protocole RTCP et les horodateurs NTP des récepteurs, mesurée à la réception des messages. La moyenne est obtenue en faisant la somme de toutes les évaluations, et en la divisant ensuite par le nombre de messages reçus conformes au protocole RTCP. Il convient de noter que le calcul correct de ce paramètre suppose des horloges synchronisés. Les dispositifs des passerelles de jonction PEUVENT autrement évaluer le délai moyen de transmission en divisant par deux le temps mesuré d'un aller-retour.

Se reporter au document IETF RFC 1889 pour une définition plus détaillée de ces variables.

Les paramètres **NotifiedEntity, RequestedEvents, RequestIdentifier, SignalRequests, QuarantineHandling** et **DetectEvents** sont facultatifs. Ils peuvent être utilisés par le contrôleur MGC pour transmettre une demande de notification qui soit liée à la suppression de la connexion et exécutée simultanément avec elle. Toutefois, si un ou plusieurs paramètres sont présents, le paramètre RequestIdentifier DOIT faire partie de ceux-là. Par exemple, lorsqu'un circuit est déconnecté, la passerelle pourrait être priée de supprimer la connexion et de commencer à rechercher un événement prise. Ceci peut se faire au moyen d'une seule commande DeleteConnection en transmettant également le paramètre RequestedEvents pour l'événement prise et un paramètre SignalRequests ne contenant pas de valeur.

Lorsque ces paramètres sont présents, la suppression de la connexion et la demande de notification DOIVENT être synchronisées, ce qui veut dire qu'elles sont toutes deux soit acceptées soit refusées.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.6 Commande DeleteConnection (par la passerelle de jonction)

Dans certaines circonstances, une passerelle peut être amenée à libérer une connexion, par exemple, parce qu'elle a perdu les ressources associées à la connexion. Elle peut mettre fin à la connexion en utilisant une variante de la commande DeleteConnection:

```
ReturnCode
     ← DeleteConnection(CallId,
                        EndpointId,
                        ConnectionId,
                        Reason-code,
                        Connection-parameters)
```

Dans cette forme de la commande DeleteConnection, le paramètre **EndpointId** DOIT être entièrement spécifié. La convention concernant les caractères de remplacement NE DOIT PAS être employée.

Le paramètre **Reason-code** est une chaîne de texte commençant par un code de motif suivi en option d'une chaîne de texte descriptif. On trouvera une liste des paramètres reasoncodes au A.2.6.

Outre les paramètres **CallId, EndpointId** et **ConnectionId**, la passerelle de jonction enverra aussi les paramètres de la connexion qui auraient été renvoyés au contrôleur MGC en réponse à une commande DeleteConnection provenant de lui. Le code de motif indique le motif de la commande DeleteConnection.

Le paramètre **ReturnCode** est un paramètre renvoyé par le contrôleur MGC. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.7 Commande DeleteConnection (par le contrôleur de passerelle média, dans le cas de connexions multiples)

Une variante de la fonction DeleteConnection peut être utilisée par le contrôleur MGC pour supprimer plusieurs connexions en même temps. La commande peut être utilisée pour supprimer toutes les connexions qui se rapportent à un appel pour une extrémité:

```
ReturnCode
     ← DeleteConnection(CallId,
                        EndpointId)
```

Dans cette forme de la commande DeleteConnection, le paramètre **EndpointId** NE DOIT PAS utiliser le caractère de remplacement "un quelconque". Toutes les connexions pour l'extrémité ou les extrémités dont le paramètre CallId est spécifié seront supprimées. La commande ne renvoie pas de statistiques individuelles ou de paramètres d'appel.

La commande DeleteConnection peut également être utilisée par le contrôleur MGC pour supprimer toutes les connexions qui aboutissent à une extrémité donnée:

```
ReturnCode
     ← DeleteConnection(EndpointId)
```

Dans cette forme de la commande DeleteConnection, le contrôleur MGC peut profiter de la structure hiérarchique des noms d'extrémité pour supprimer toutes les connexions qui appartiennent à un groupe d'extrémités. Dans ce cas, une partie de la composante "nom d'extrémité local" du paramètre EndpointId peut être spécifiée au moyen de la convention concernant le caractère de remplacement "tous", comme stipulé au A.2.1.1. La convention concernant le caractère de remplacement "un quelconque" NE DOIT PAS être utilisée. La commande ne renvoie pas de statistiques individuelles ou de paramètres d'appel.

Après la suppression de la connexion, les flux médias du réseau en mode paquet précédemment pris en charge par la connexion ne sont plus disponibles. Tout paquet média reçu pour l'ancienne connexion est simplement ignoré, et aucun nouveau paquet média pour le flux n'est envoyé.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

A.2.3.8 Audit

Le protocole MGCP est fondé sur une architecture de commande d'appel centralisée où un contrôleur MGC joue le rôle de contrôleur à distance des dispositifs clients qui fournissent des interfaces de communication vocale aux utilisateurs et aux réseaux. Afin d'arriver à un degré de disponibilité égal ou supérieur à celui du RTPC actuel, certains protocoles font appel aux mécanismes permettant d'envoyer régulièrement aux abonnés des utilitaires "ping" afin de réduire le temps nécessaire à la détection des différentes pannes. A cet égard, il est fourni un mécanisme d'audit propre au protocole MGCP entre les passerelles de jonction et le contrôleur MGC d'un système IPCablecom, afin de permettre à celui-ci de vérifier l'état des extrémités et des connexions et d'extraire d'une extrémité des capacités propres au protocole.

Deux commandes permettant d'assurer l'audit sont définies pour les passerelles de jonction:

AuditEndPoint: utilisée par le contrôleur MGC pour déterminer l'état d'une extrémité.

AuditConnection: utilisée par le contrôleur MGC pour obtenir des informations sur une connexion.

Une gestion du réseau, plus poussée que celle qui est obtenue au moyen de ces commandes est généralement souhaitable, par exemple en ce qui concerne des informations sur l'état de la passerelle de jonction comparé à celui des différentes extrémités. On prévoit que ces capacités seront prises en charge lors de l'utilisation du protocole simple de gestion de réseau (SNMP) et de la définition d'une base MIB pour la passerelle de jonction, sujets qui sortent du cadre de la présente Recommandation.

A.2.3.8.1 Commande AuditEndPoint

La commande AuditEndPoint peut être utilisée par le contrôleur MGC pour déterminer l'état d'une extrémité donnée.

```
{ ReturnCode
     [, EndPointIdList]
     [, NumEndPoints] } |
{ ReturnCode
     [, RequestedEvents]
     [, SignalRequests]
     [, RequestIdentifier]
     [, NotifiedEntity]
     [, ConnectionIdentifiers]
     [, DetectEvents]
     [, ObservedEvents]
     [, EventStates]
     [, Capabilities] }
          ← AuditEndPoint(EndpointId
                       [, RequestedInfo] |
                       { [, SpecificEndpointID]
                            [, MaxEndpointIDs] } )
```

Le paramètre **EndpointId** identifie l'extrémité qui fait l'objet d'un audit. La convention concernant le caractère de remplacement "un quelconque" NE DOIT PAS être employée.

La convention concernant le caractère de remplacement "tous" peut être utilisée pour vérifier un groupe d'extrémités. Si cette convention est employée, la passerelle DOIT renvoyer une liste des identificateurs d'extrémité qui concorde avec celle qui a été obtenue au moyen du caractère de remplacement dans le paramètre **EndPointIdList**, et est simplement la liste des paramètres SpecificEndpointIds – le paramètre RequestedInfo NE DOIT PAS être inclus dans ce cas. Le paramètre **MaxEndPointIDs** consiste en une valeur numérique qui indique le nombre maximal de paramètres EndpointIds à renvoyer. Lorsque des extrémités supplémentaires existent, le paramètre de renvoi **NumEndPoints** DOIT être présent et indiquer le nombre total d'extrémités qui concordent avec le paramètre EndpointID spécifié. Afin d'extraire le bloc suivant de paramètres EndpointIDs, le paramètre **SpecificEndPointID** est fixé à la valeur de la dernière extrémité renvoyée du précédent paramètre EndpointIDList, et la commande est lancée.

Lorsque la convention concernant les caractères de remplacement n'est pas employée, le paramètre **RequestedInfo** (ne contenant éventuellement pas de valeur) décrit les informations qui sont demandées pour le paramètre EndpointId spécifié – les paramètres SpecificEnpointID et MaxEndpointID NE DOIVENT PAS être utilisés dans ce cas. Les informations suivantes propres aux extrémités peuvent alors faire l'objet d'un audit au moyen de cette commande:

RequestedEvents, SignalRequests, RequestIdentifier, NotifiedEntity, ConnectionIdentifiers, DetectEvents, ObservedEvents, EventStates, VersionSupported et Capabilities.

La réponse, pour sa part, comprendra des informations sur chacun des points pour lesquels des informations d'audit ont été demandées:

- **RequestedEvents**: valeur effective du paramètre RequestedEvents que l'extrémité emploie, y compris la mesure associée à chaque événement. Les événements durables sont inclus dans la liste.
- **SignalRequests**: liste de signaux TO qui sont effectivement activés, de signaux OO qui sont effectivement "activés" pour l'extrémité (avec ou sans paramètre) et de signaux brefs en attente[17]. Les signaux TO qui se sont arrêtés et les signaux bref effectivement produits ne sont pas compris. Il est fait état des signaux paramétrisés avec les paramètres qu'ils ont utilisés.
- **RequestIdentifier**: paramètre RequestIdentifier pour le dernier paramètre NotificationRequest reçu par l'extrémité (y compris la demande de notification insérée dans les primitives traitant la connexion). Si aucune demande de notification n'a été reçue, la valeur zéro sera renvoyée.
- **NotifiedEntity**: "entité notifiée" effective pour l'extrémité.
- **ConnectionIdentifiers**: liste des paramètres ConnectionIdentifiers séparés par des points-virgules pour toutes les connexions qui existent effectivement pour l'extrémité spécifiée.
- **DetectEvents**: valeur effective du paramètre DetectEvents que l'extrémité utilise. Les événements durables sont compris dans la liste.
- **ObservedEvents**: liste effective des événements observés pour l'extrémité.
- **EventStates**: pour les événements dont les états peuvent faire l'objet d'un audit, l'événement correspondant à l'état de l'extrémité est, par exemple, une prise, lorsque le circuit multifréquence pour l'extrémité est effectivement pris. La définition des différents événements stipulera si l'événement concerné est dans un état pouvant faire l'objet d'un audit.
- **VersionSupported**: liste des versions de protocole prises en charge par l'extrémité.
- **Capabilities**: capacités de l'extrémité semblables à celles du paramètre LocalConnectionOptions et comprenant des paquetages d'événements et des modes de connexion. S'il est nécessaire de spécifier que certains paramètres, tels que, par exemple, la suppression des silences, ne sont compatibles qu'avec certains codecs, la passerelle renverra plusieurs ensembles de capacités. Si une extrémité est interrogée au sujet d'une capacité qu'elle ne comprend pas, elle NE DOIT PAS produire d'erreur; au lieu de cela, le paramètre DOIT être omis de la réponse:
  - **algorithme de compression** liste des codecs pris en charge. Le reste des paramètres s'appliquera à tous les codecs spécifiés dans cette liste;
  - **période de mise en paquets** spécification d'une valeur unique ou d'une gamme de valeurs;

[17] Généralement, il ne devrait pas y avoir de signaux brefs en attente.

– **largeur de bande** spécification d'une valeur unique ou d'une gamme de valeurs correspondant à la gamme des périodes de mise en paquets (avec l'hypothèse qu'il n'y ait pas de suppression des silences);

– **suppression d'écho** indication de la prise en charge ou pas[18] de la suppression d'écho;

– **suppression des silences** indication de la prise en charge ou pas de la suppression des silences;

– **type de service** indication de la prise en charge ou pas du type de service;

– **paquetages d'événements** liste des paquetages d'événements pris en charge. Le premier paquetage d'événements de la liste sera le paquetage par défaut;

– **modes** liste des modes de connexion pris en charge;

– **sécurité** indication de la prise en charge ou pas des services de sécurité IPCablecom. En cas de prise en charge, les paramètres suivants peuvent également être présents:

- **suite de chiffrement pour le protocole RTP** – Liste d'algorithmes d'authentification et de chiffrement pris en charge pour le protocole RTP;
- **suite de chiffrement pour le protocole RTCP**– Liste d'algorithmes d'authentification et de chiffrement pris en charge pour le protocole RTCP;
- **surveillance électronique** – Indication de la prise en charge ou pas de la surveillance électronique IPCablecom.

Le contrôleur MGC peut alors décider d'utiliser la commande AuditConnection pour obtenir plus d'informations sur les connexions.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

Si aucune information n'a été demandée et que le paramètre EndpointId renvoie à un paramètre EndpointId valable entièrement spécifié, la passerelle renvoie simplement une réponse de réussite (code de renvoi 200 – Transaction exécutée normalement).

Il convient de noter que toutes les informations renvoyées correspondent simplement à un instantané. Les nouvelles commandes reçues, l'activité locale, etc. peuvent influer sur la plupart des informations susmentionnées. Par exemple, l'état de prise peut changer avant que le contrôleur MGC ne reçoive ces informations.

A.2.3.8.2 Commande AuditConnection

L'audit des différentes connexions à une extrémité peut être réalisé au moyen de la commande AuditConnection.

```
ReturnCode
[, CallId]
[, NotifiedEntity]
```

[18] Actuellement toutes les extrémités conformes au protocole TGCP doivent prendre en charge la suppression d'écho.

```
[, LocalConnectionOptions]
[, Mode]
[, RemoteConnectionDescriptor]
[, LocalConnectionDescriptor]
[, ConnectionParameters]
     ← AuditConnection(EndpointId
                       , ConnectionId
                       [, RequestedInfo])
```

Le paramètre **EndpointId** identifie l'extrémité qui fait l'objet d'un audit – Les caractères de remplacement NE DOIVENT PAS être utilisés. Le paramètre **RequestedInfo** (ne contenant éventuellement pas de valeur) décrit les informations qui sont demandées pour le paramètre **ConnectionId** dans le paramètre EndpointId spécifié. Les informations de connexion suivantes peuvent faire l'objet d'un audit au moyen de cette commande:

CallId, NotifiedEntity, LocalConnectionOptions, Mode, ConnectionParameters, RemoteConnectionDescriptor, LocalConnectionDescriptor.

La réponse, pour sa part, comprendra des informations sur chacun des points pour lesquels des informations d'audit ont été demandées:

- **CallId** identificateur de l'appel auquel la connexion appartient;
- **NotifiedEntity** "entité notifiée" pour l'extrémité;
- **LocalConnectionOptions** paramètre fourni pour la connexion;
- **Mode** mode de connexion effectif;
- **ConnectionParameters** paramètres de connexion effectifs pour la connexion;
- **LocalConnectionDescriptor** paramètre que la passerelle a fourni pour la connexion;
- **RemoteConnectionDescriptor** paramètre qui a été fourni à la passerelle pour la connexion.

Le paramètre **ReturnCode** est un paramètre renvoyé par la passerelle. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

Lorsqu'aucune information n'est demandée, et que le paramètre EndpointId renvoie à une extrémité valable, la passerelle vérifie simplement que la connexion spécifiée existe et, si tel est le cas, renvoie une réponse positive (code de renvoi 200 – Transaction exécutée).

A.2.3.9 Redémarrage en cours

La commande RestartInProgress est utilisée par la passerelle pour signaler qu'une extrémité ou un groupe d'extrémités est mis hors service ou est remis en service.

```
ReturnCode
[, NotifiedEntity]
[, VersionSupported]
         ← RestartInProgress(EndpointId
                       , RestartMethod
                       [, RestartDelay])
```

Le paramètre **EndpointId** identifie les extrémités qui sont mises en service ou hors service. La convention concernant le caractère de remplacement "tous" peut être employée pour appliquer la commande à un groupe d'extrémités, par exemple, toutes les extrémités qui sont reliées à une interface spécifiée, ou même toutes les extrémités qui sont reliées à une passerelle donnée. La convention concernant le caractère de remplacement "un quelconque" NE DOIT PAS être utilisée.

Le paramètre RestartMethod spécifie le type de redémarrage:

- la méthode de redémarrage "progressif" spécifie que l'extrémité ou les extrémités spécifiées seront mises hors service après le "délai de redémarrage" spécifié. Les connexions établies ne sont pas encore touchées, mais le contrôleur MGC devrait s'abstenir d'établir de nouvelles

connexions et devrait essayer de réduire progressivement et assez rapidement le nombre de connexions existantes;

- la méthode de redémarrage "progressif annulé" spécifie qu'une passerelle procède à l'annulation de la méthode de redémarrage "progressif" précédemment mise en œuvre aux extrémités considérées. Sitôt cette commande émise, la passerelle autorisera immédiatement l'établissement de nouvelles connexions à ces extrémités;
- la méthode de redémarrage "forcé" spécifie que les extrémités spécifiées sont mises hors services de manière brusque. Les connexions établies, s'il y en a, sont perdues;
- la méthode de "redémarrage" spécifie que le service sera rétabli aux extrémités après le "délai de redémarrage" spécifié. Aucune connexion n'est effectivement établie aux extrémités;
- la méthode de "déconnexion" spécifie que l'extrémité a été déconnectée et tente maintenant d'établir la connexion. Le "délai de redémarrage" spécifie le nombre de secondes pendant lesquelles l'extrémité a été déconnectée. Les connexions établies ne sont pas touchées.

Le paramètre facultatif "délai de redémarrage" s'exprime sous la forme d'un nombre de secondes. Si ce nombre fait défaut, la valeur du délai devrait être considérée comme étant nulle. Dans le cas de la méthode "progressive", un délai nul indique que le contrôleur MGC devrait simplement attendre que les connexions existantes prennent fin naturellement, sans établir de nouvelles connexions. Le délai de redémarrage est toujours considéré comme étant nul dans le cas des méthodes "forcée" et "progressive annulée". Un délai de redémarrage nul pour la méthode de "redémarrage" indique que le service a déjà été rétabli. Cela se produira généralement après le démarrage ou le redémarrage de la passerelle. Afin d'atténuer les effets causés par le changement d'adresse IP d'une passerelle, le contrôleur MGC PEUT vouloir trancher la question du nom de domaine de la passerelle en interrogeant le système DNS sans tenir compte de la durée de vie de l'enregistrement effectif des ressources pour la passerelle redémarrée.

Les passerelles de jonction DEVRAIENT envoyer, par courtoisie envers le contrôleur MGC, un message RestartInProgress "progressif" ou "forcé" lorsqu'elles sont mises hors service, par exemple, lors de leur fermeture ou de leur mise hors service par un système de gestion de réseau, même si le contrôleur MGC ne peut toujours compter recevoir de tels messages. Les passerelles de jonction DOIVENT envoyer à leurs contrôleurs MGC un message RestartInProgress de "redémarrage" avec un délai nul lorsqu'elles sont remises en service, conformément à la procédure de redémarrage spécifiée au A.2.4.3.5 – les contrôleurs MGC peuvent compter recevoir ce message. En outre, les passerelles de jonction DOIVENT envoyer à leurs "entités notifiées" effectives un message RestartInProgress de "déconnexion", conformément à la procédure de "déconnexion" spécifiée au A.2.4.3.6. Le paramètre "délai de redémarrage" NE DOIT PAS être utilisé avec la méthode de redémarrage "forcé".

Le message RestartInProgress sera envoyé à "l'entité notifiée" effective pour le paramètre EndpointId concerné. Il est prévu qu'un contrôleur MGC par défaut, à savoir "l'entité notifiée", ait été configuré pour chacune des extrémités de manière qu'après un redémarrage ce contrôleur MGC par défaut puisse être "l'entité notifiée" pour chacune de ces extrémités. Les passerelles de jonction DOIVENT pleinement mettre à profit les caractères de remplacement de manière à minimiser le nombre de messages RestartInProgress produits lorsque des extrémités multiples d'une passerelle redémarrent et que ces extrémités sont gérées par le même contrôleur MGC.

Le paramètre **ReturnCode** est un paramètre renvoyé par le contrôleur MGC. Il indique le résultat de la commande et comporte un nombre entier (voir A.2.5) suivi en option d'un commentaire.

Un paramètre **NotifiedEntity** peut en outre être renvoyé avec la réponse provenant du contrôleur MGC:

- si la réponse indique la réussite (code de renvoi 200 – Transaction exécutée), la procédure de redémarrage est achevée et le paramètre NotifiedEntity renvoyé est la nouvelle "entité notifiée" pour l'extrémité ou les extrémités;
- si la réponse provenant du contrôleur MGC a signalé une erreur, la procédure de redémarrage n'est pas encore achevée et doit donc être redémarrée. Si un paramètre NotifiedEntity a été renvoyé, il spécifie alors la nouvelle "entité notifiée" pour l'extrémité ou les extrémités, qui doit en conséquence être utilisée lorsque la procédure de redémarrage est réessayée.

Finalement, un paramètre **VersionSupported** comprenant une liste des versions prises en charge peut être renvoyé, si la réponse a indiqué une incompatibilité de version (code d'erreur 528).

A.2.4 Etats, situations de relais en cas de défaillance et situations de course

Afin d'implémenter une signalisation d'appel qui convient, le contrôleur MGC doit suivre l'état de l'extrémité et la passerelle doit s'assurer que les événements sont correctement notifiés au contrôleur MGC. Des situations particulières peuvent exister lorsque la passerelle ou le contrôleur MGC sont redémarrés: la passerelle peut devoir être réorientée vers un nouveau contrôleur MGC au cours des procédures de relais en cas de défaillance; de même, le contrôleur MGC peut devoir prendre des mesures spéciales lorsque la passerelle est mise hors ligne ou est redémarrée.

A.2.4.1 Récapitulatif des points essentiels

Comme il est mentionné au A.2.1.4, les contrôleurs MGC sont identifiés par leur nom de domaine, et chaque extrémité possède à tout moment donné une et une seule "entité notifiée" qui lui est associée. Dans le présent paragraphe, les points essentiels qui sont d'une importance particulière en ce qui concerne la fiabilité et le relais en cas de défaillance dans le cadre du protocole MGCP sont récapitulés:

- un contrôleur MGC est identifié par son nom de domaine, non par ses adresses dans le réseau, et plusieurs adresses dans le réseau peuvent être associées à un nom de domaine;
- une extrémité dispose à tout moment donné d'un et d'un seul contrôleur MGC qui lui est associé. Le contrôleur MGC associé à une extrémité est la valeur effective de "l'entité notifiée";
- la valeur attribuée initialement à "l'entité notifiée" est une valeur qui est fixée par la configuration. Lorsqu'une commande comprenant un paramètre NotifiedEntity est reçue à une extrémité, ainsi que des noms d'extrémité comportant des caractères de remplacement, la valeur attribuée à "l'entité notifiée" est celle qui est spécifiée. Si aucune valeur n'est attribuée à "l'entité notifiée" pour une extrémité ou que cette valeur n'a pas été fixée explicitement[19], l'adresse par défaut de "l'entité notifiée" est l'adresse de l'émetteur de la dernière commande de traitement de la connexion ou demande de notification reçue pour l'extrémité. Dans ce cas, le contrôleur MGC sera donc identifié par son adresse dans le réseau, ce qui ne DEVRAIT se faire qu'exceptionnellement;
- les réponses aux commandes sont toujours envoyées aux adresses de leurs émetteurs, sans qu'il soit tenu compte de "l'entité notifiée" effective. Lorsqu'un message Notify doit accompagner la réponse, le datagramme est encore envoyé à l'adresse de l'émetteur de la nouvelle commande reçue, sans qu'il soit tenu compte du paramètre NotifiedEntity pour les commandes;

[19] Ceci pourrait par exemple se produire lorsqu'aucune valeur n'est spécifiée pour le paramètre NotifiedEntry.

- lorsque "l'entité notifiée" renvoie à un nom de domaine qui se décompose en plusieurs adresses IP, les extrémités sont en mesure de passer d'une adresse à l'autre, sans toutefois pouvoir modifier de leur propre initiative le nom de domaine de "l'entité notifiée". Un contrôleur MGC peut toutefois leur ordonner d'effectuer le changement en leur attribuant une nouvelle "entité notifiée";
- si un contrôleur MGC n'est plus disponible, les extrémités qu'il gère seront éventuellement "déconnectées". La seule façon pour que ces extrémités soient connectées à nouveau est que soit le contrôleur MGC défaillant redevient disponible soit qu'un autre contrôleur MGC (de secours) contacte les extrémités touchées avec une nouvelle "entité notifiée";
- lorsqu'un autre contrôleur MGC (de secours) a repris la commande d'un groupe d'extrémités, on suppose que le contrôleur MGC défaillant communiquera avec le contrôleur MGC de secours et se synchronisera avec lui afin que la commande des extrémités touchées puisse lui être repassée, si cela est souhaité. Autrement, le contrôleur MGC défaillant pourrait maintenant simplement devenir le contrôleur MGC de secours.

Il convient de noter que la résolution des différends en ce qui concerne la passation entre différents contrôleurs MGC n'est pas configurée – ceci étant strictement fondé sur le fait que les contrôleurs MGC savent ce qu'ils font et qu'ils communiquent entre eux (même si le paramètre AuditEndpoint peut être employé pour connaître "l'entité notifiée" effective).

A.2.4.2 Retransmission et détection d'associations perdues

Le protocole MGCP est structuré comme un ensemble de transactions, chacune d'elles étant constituée d'une commande et d'une réponse. Les messages relatifs à ce protocole, transportés à l'aide du protocole UDP, peuvent subir des pertes. En l'absence d'une réponse dans les délais (voir A.3.5), les commandes sont reproduites. Les passerelles DOIVENT garder en mémoire une liste des réponses qu'elles ont envoyées au cours des récentes transactions et une liste des transactions qui sont en cours d'exécution. "Récentes transactions" est défini ici par la valeur Tt_{hist} qui spécifie le nombre de secondes pendant lesquelles les réponses à d'anciennes transactions doivent être conservées. La valeur par défaut de Tt_{hist} est égale à 30 secondes.

Les identificateurs de transaction des commandes entrantes sont d'abord comparés aux identificateurs de transaction des réponses récentes. Lorsqu'une concordance est trouvée, la passerelle n'effectue pas la transaction, mais reproduit simplement l'ancienne réponse. Si aucune concordance avec une transaction à laquelle il a été répondu précédemment n'est trouvée, l'identificateur de transaction de la commande entrante est comparé à la liste des transactions dont l'exécution n'est pas encore terminée. Si une concordance est trouvée, la passerelle n'effectue pas la transaction, dont il n'est simplement pas tenu compte – Une réponse sera fournie lorsque l'exécution de la commande est achevée.

Ce mécanisme de répétition est utilisé pour prévenir quatre types d'erreur:

- erreurs de transmission, lorsque, par exemple, un paquet est perdu en raison du bruit sur la ligne ou de l'encombrement dans une file d'attente;
- défaillance d'un composant, lorsque, par exemple, une interface de contrôleur MGC n'est plus disponible;
- défaillance d'un contrôleur MGC, lorsque, par exemple, toutes ses interfaces ne sont plus disponibles;
- relais en cas de défaillance, lorsqu'un nouveau contrôleur MGC "prend le relais" de manière transparente.

Les éléments devraient être en mesure d'évaluer à partir de l'historique le taux de perte de paquets. Dans un système correctement configuré, ce taux de perte devrait être très faible, généralement moins de 1% en moyenne. Si un contrôleur MGC ou une passerelle doit reproduire un message plus de quelques fois, il est légitime de penser qu'il s'est produit une chose autre qu'une erreur de

transmission. Par exemple, si le taux de perte est uniformément distribué et s'élève à 1%, la probabilité pour que 5 tentatives consécutives de transmission échouent est de 1 sur 100 milliards, événement qui devrait se produire moins d'une fois tous les 10 jours dans le cas d'un contrôleur MGC qui effectue 1 000 transactions par seconde. (En effet, le nombre de répétitions qui est considéré comme étant excessif devrait être fonction du taux habituel de perte de paquets.) Lorsque les erreurs ne sont pas distribuées uniformément, la probabilité d'échecs consécutifs peut être un peu plus grande. Il convient de noter que le "seuil de suspicion", que nous nommerons "Max1", est normalement inférieur au "seuil de déconnexion", que nous nommerons "Max2", et qu'on devrait lui attribuer une valeur plus élevée.

Un algorithme classique de retransmission (voir Figure A.1) consisterait simplement en un comptage du nombre de répétitions successives et en la conclusion que l'association est rompue après que le paquet ait été retransmis un nombre excessif de fois (généralement compris entre 7 et 11 fois). Afin de tenir compte de la possibilité de l'existence d'un "relais en cas de défaillance" non détecté ou en cours, nous modifions comme suit l'algorithme classique:

- la passerelle DOIT toujours relever la présence d'un nouveau contrôleur MGC. Elle peut en être informée:
  - en recevant une commande où le paramètre NotifiedEntity indique un nouveau contrôleur MGC;
  - en recevant une réponse de réorientation vers un nouveau contrôleur MGC;
- lorsqu'un nouveau contrôleur MGC est détecté, la passerelle DOIT orienter les retransmissions des commandes en suspens pour l'extrémité ou les extrémités vers ce nouveau contrôleur MGC. Les réponses aux nouvelles ou anciennes commandes sont toujours transmises vers l'adresse de l'émetteur de la commande;
- avant toute retransmission, on vérifie que le temps qui s'est écoulé depuis l'envoi du datagramme initial n'est pas supérieur à Ts_{max}. Si plus de temps que cette valeur s'est écoulé, l'extrémité se déconnecte;
- si le nombre de retransmissions vers ce contrôleur MGC est égal à "Max1", la passerelle PEUT activement interroger le serveur de noms afin de détecter les éventuels changements d'interfaces des contrôleurs MGC, sans qu'il soit tenu compte de la durée de vie associée à l'enregistrement dans le système DNS;
- la passerelle peut avoir pris connaissance de plusieurs adresses IP pour le contrôleur MGC. Si le nombre de retransmissions pour une adresse IP est supérieur à "Max1" et inférieur à "Max2", et qu'il y a d'autres adresses IP qui n'ont pas été essayées, la passerelle DOIT orienter les retransmissions vers les autres adresses restantes de sa liste locale;
- s'il ne reste plus d'autres interfaces à essayer, et que le nombre de retransmissions est égal à "Max2", la passerelle DEVRAIT contacter le système DNS encore une fois pour voir si d'autres interfaces sont devenues disponibles. Si ce n'est pas le cas, l'extrémité ou les extrémités gérées par ce contrôleur MGC sont maintenant déconnectées. Lorsqu'une extrémité se déconnecte, elle DOIT entamer une procédure de "déconnexion" comme spécifié au A.2.4.3.6.

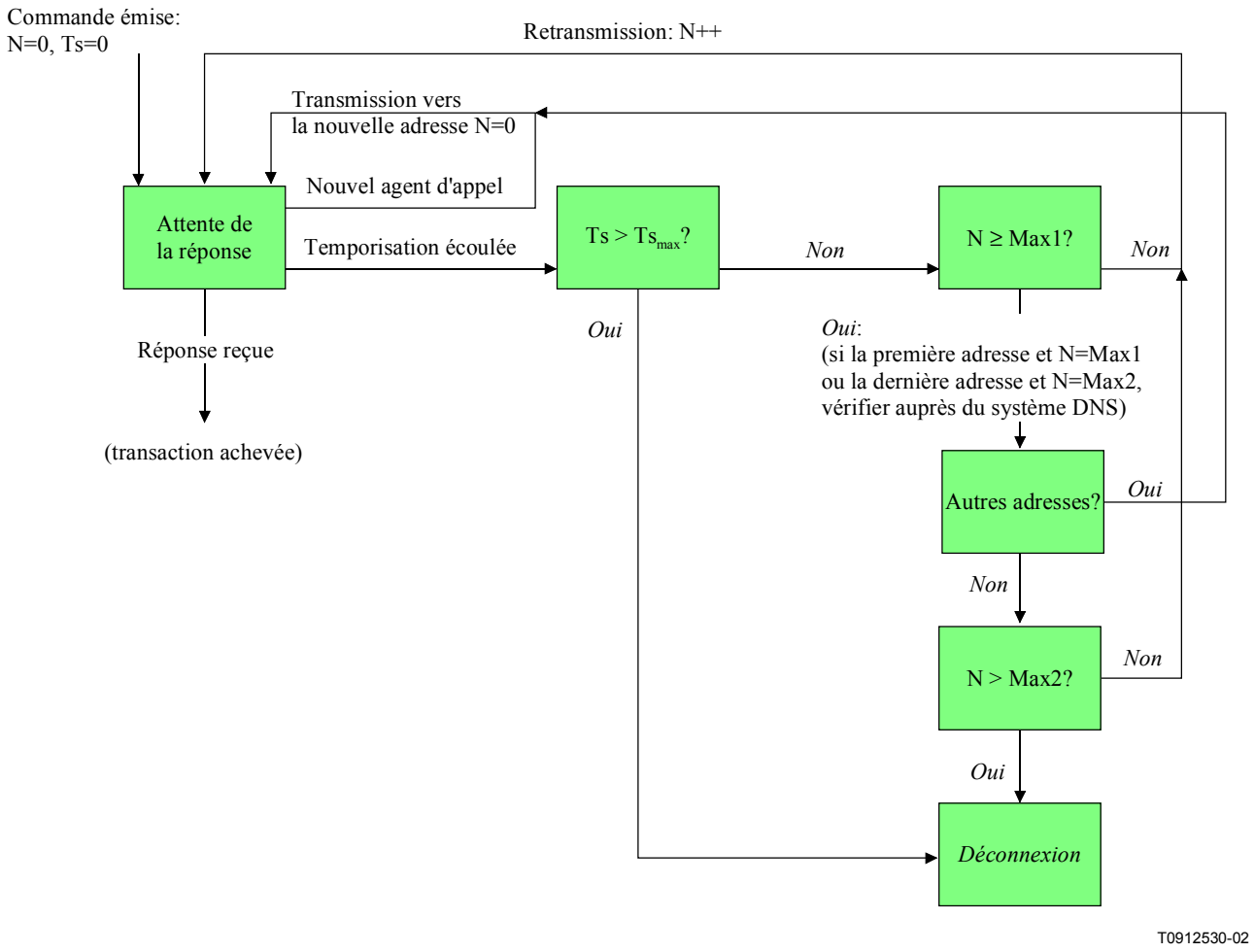

Figure A.1/J.171 – Algorithme de retransmission

Afin que l'adaptation automatique à la charge du réseau puisse se faire, il est spécifié dans le protocole MGCP des temporisations qui augmentent exponentiellement (voir A.3.5.2). Si la temporisation est fixée initialement à 200 millisecondes, la perte d'une cinquième retransmission sera détectée après environ 6 secondes. Ceci constitue sans doute un délai d'attente acceptable pour détecter un relais en cas de défaillance. Les retransmissions devraient être poursuivies après ce délai, non seulement pour surmonter peut-être des problèmes transitoires de connectivité, mais également afin d'accorder un peu plus de temps à la prise du relais – Un délai d'attente total de 30 secondes est sans doute acceptable.

Il convient de noter que la relation entre Ts_{max}, Tt_{hist} et le temps de transit maximal, Tp_{max}, est étroite. En particulier, le relation suivante DOIT être satisfaite pour éviter que des commandes retransmises soient exécutées plus d'une fois:

$$Tt_{hist} \geq Ts_{max} + Tp_{max}$$

La valeur par défaut de Ts_{max} est égale à 20 secondes. Donc, si on suppose que le délai de propagation maximal est de 10 secondes, les réponses aux anciennes transactions doivent être conservées pendant une durée d'au moins 30 secondes. L'importance d'un accord entre l'envoyeur et le récepteur concernant ces valeurs est toujours sous-estimée.

La valeur par défaut pour Max1 est égale à 5 retransmissions tandis que celle pour Max2 s'élève à 7 retransmissions. Ces deux valeurs peuvent être modifiées au cours du processus de configuration.

En outre, le processus de configuration DOIT être en mesure de désactiver une requête ou les deux requêtes Max1 et Max2 auprès du système DNS.

A.2.4.3 Situations de course

Dans le présent paragraphe, les situations de course sont abordées dans le protocole MGCP.

Premièrement, le protocole MGCP aborde les situations de course à travers la notion d'une "liste de quarantaine" où des événements sont mis en quarantaine et à travers la détection explicite de la désynchronisation, par exemple, pour des états de prise non concordants à cause d'une interférence à une extrémité.

Deuxièmement, dans le protocole MGCP on ne suppose pas que le mécanisme de transport conservera l'ordre des commandes et des réponses. Cela peut conduire à des situations de course auxquelles il peut être remédié en adaptant le comportement du contrôleur MGC de manière à ordonner correctement les commandes.

Finalement, dans certains cas, des passerelles en grand nombre peuvent décider de recommencer à fonctionner en même temps. Cela peut se produire, par exemple, lorsque dans une zone le courant est interrompu ou que la transmission ne peut plus se faire pendant un tremblement de terre ou une tempête de neige. Lorsque le courant est rétabli et que la transmission peut à nouveau se faire, des passerelles en grand nombre peuvent décider d'envoyer simultanément des commandes RestartInProgress, ce qui pourrait conduire à un fonctionnement très instable s'il n'est pas bien contrôlé.

A.2.4.3.1 Liste de quarantaine

Les passerelles commandées par le protocole MGCP recevront des demandes de notification leur enjoignant de surveiller un ensemble d'événements. Les éléments du protocole qui déterminent comment ces événements seront traités sont les listes "d'événements demandés" et "d'événements détectés".

Lorsque l'extrémité est initialisée, la liste des événements demandés ne comporte que des événements durables pour cette extrémité. Après la réception d'une commande, la passerelle commence à observer au niveau de cette extrémité les occurrences des événements qui sont mentionnés dans la liste, y compris celles des événements durables.

Les événements sont examinés au fur et à mesure de leur production. La mesure qui en découle est déterminée par le paramètre "mesure" qui est associé à l'événement de la liste des événements demandés. Les événements qui sont définis comme étant "recueillis" sont recueillis dans une liste d'événements observés. Ceci sera poursuivi jusqu'à ce qu'un événement produit déclenche une commande Notify qui sera envoyée à "l'entité notifiée".

A ce moment, la passerelle transmettra la commande Notify et placera l'extrémité dans un "état de notification". Aussi longtemps que cette extrémité est dans cet "état de notification", les événements qui sont détectés à cette extrémité sont entreposés dans un tampon de "quarantaine" pour être traités ultérieurement. Les événements sont, dans un certain sens, mis en "quarantaine". Les événements détectés sont des événements spécifiés par l'union du paramètre RequestedEvents avec le paramètre reçu le plus récemment DetectEvents, ou lorsque celui-ci n'a pas été reçu, par les événements auxquels renvoie le paramètre RequestedEvents. Les événements durables sont également détectés.

L'extrémité quitte "l'état de notification" lors de la réception d'une réponse à la commande Notify[20]. La commande Notify peut être retransmise dans "l'état de notification", comme spécifié au A.2.4.2.

Lorsque l'extrémité quitte "l'état de notification", elle réinitialise à zéro la valeur attribuée à l'ensemble des événements qui ont été observés à son niveau.

---

[20] Il convient de noter que la mesure Notify ne peut être combinée avec une demande NotificationRequest incorporée.

Le profil du protocole TGCP ordonne l'emploi du "mode figé" qui implique que la passerelle DOIT recevoir une nouvelle commande NotificationRequest après qu'elle a envoyé une commande Notify. Jusqu'à ce que cela ait lieu, l'extrémité est dans un "état figé", et les événements qui se produisent et doivent être détectés sont simplement entreposés dans le tampon de quarantaine. Les événements à mettre en quarantaine sont les mêmes que ceux qui sont dans "l'état de notification". Lorsque la nouvelle demande NotificationRequest est reçue et que son exécution a réussi, l'extrémité quitte "l'état figé".

Une passerelle peut à tout moment recevoir une nouvelle commande NotificationRequest pour l'extrémité qui aura aussi pour conséquence de sortir l'extrémité de "l'état de notification", si l'exécution de la demande NotificationRequest a réussi.

Lorsqu'une nouvelle demande NotificationRequest est reçue dans "l'état de notification", la passerelle doit faire en sorte que la commande Notify en suspens soit reçue par le contrôleur MGC avant une réponse de réussite à une demande NotificationRequest. Elle fait cela en utilisant la fonctionnalité "d'accompagnement" du protocole et en classant les messages (commandes et réponses) à envoyer par ordre d'arrivée en commençant par le plus ancien. Les messages seront ensuite envoyés dans un paquet unique à l'émetteur de la commande NotificationRequest, quelles que soient l'émetteur et "l'entité notifiée" pour l'ancienne et la nouvelle commande. Les étapes mises en jeu sont les suivantes:

1) la passerelle élabore un message qui transporte dans un paquet unique une répétition de l'ancienne commande Notify en suspens et la réponse à la nouvelle commande NotificationRequest;

2) l'extrémité est ensuite sortie de "l'état de notification" sans attendre la réponse à la commande Notify;

3) une copie de la commande Notify en suspens est conservée jusqu'à ce qu'une réponse est reçue. Si une temporisation a lieu, la commande Notify sera reproduite, dans un paquet qui transportera également une répétition de la réponse à la commande NotificationRequest:

   - si le paquet transportant la réponse à la commande NotificationRequest était perdu, le contrôleur MGC retransmettra la commande NotificationRequest. La passerelle répondra à cette répétition en retransmettant dans un unique paquet la commande Notify en suspens et la réponse à la commande NotificationRequest – Ce datagramme sera envoyé à l'émetteur de la commande NotificationRequest;
   - si la passerelle devait transmettre une nouvelle commande Notify avant qu'une réponse à la précédente commande Notify ait été reçue, elle construit un paquet qui est accompagné d'une répétition de l'ancienne commande Notify, d'une répétition de la réponse à la dernière commande NotificationRequest, et d'une nouvelle commande Notify – Ce datagramme sera envoyé à "l'entité notifiée" effective.

Après avoir reçu une commande NotificationRequest, la liste des "événements demandés" est remplacée par les paramètres nouvellement reçus, et la valeur attribuée à l'ensemble des "événements observés" est réinitialisée. Le comportement ultérieur est alors conditionné par la valeur du paramètre QuarantineHandling. Ce paramètre peut spécifier que des événements mis en quarantaine doivent être ignorés, auquel cas ceux-ci le seront. Si, au contraire, il stipule que les événements en quarantaine devraient être traités, la passerelle commencera à traiter la liste des événements en quarantaine, en employant la liste nouvellement reçue des "événements demandés". Au cours du traitement de ces événements, la passerelle peut rencontrer un événement qui déclenche l'envoi d'une commande Notify. Si tel est le cas, la passerelle transmettra immédiatement une commande Notify qui signalera tous les événements ayant été recueillis dans la liste des "événements observés" jusqu'à l'événement déclencheur et y compris celui-ci, en reléguant les événements non traités dans le tampon de quarantaine. L'extrémité retourne ensuite dans "l'état de notification".

La procédure décrite ci-dessus s'applique à toutes les formes de demandes de notification, qu'elles fassent partie d'une commande de traitement d'une connexion ou qu'elles soient fournies en tant que commande NotificationRequest. Les commandes de traitement d'une connexion qui ne comportent pas de demande de notification ne sont pas affectées par la procédure susmentionnée et n'affectent pas non plus cette procédure.

La Figure A.2 illustre la procédure spécifiée ci-dessus, toutes les transactions étant supposées être exécutées avec succès:

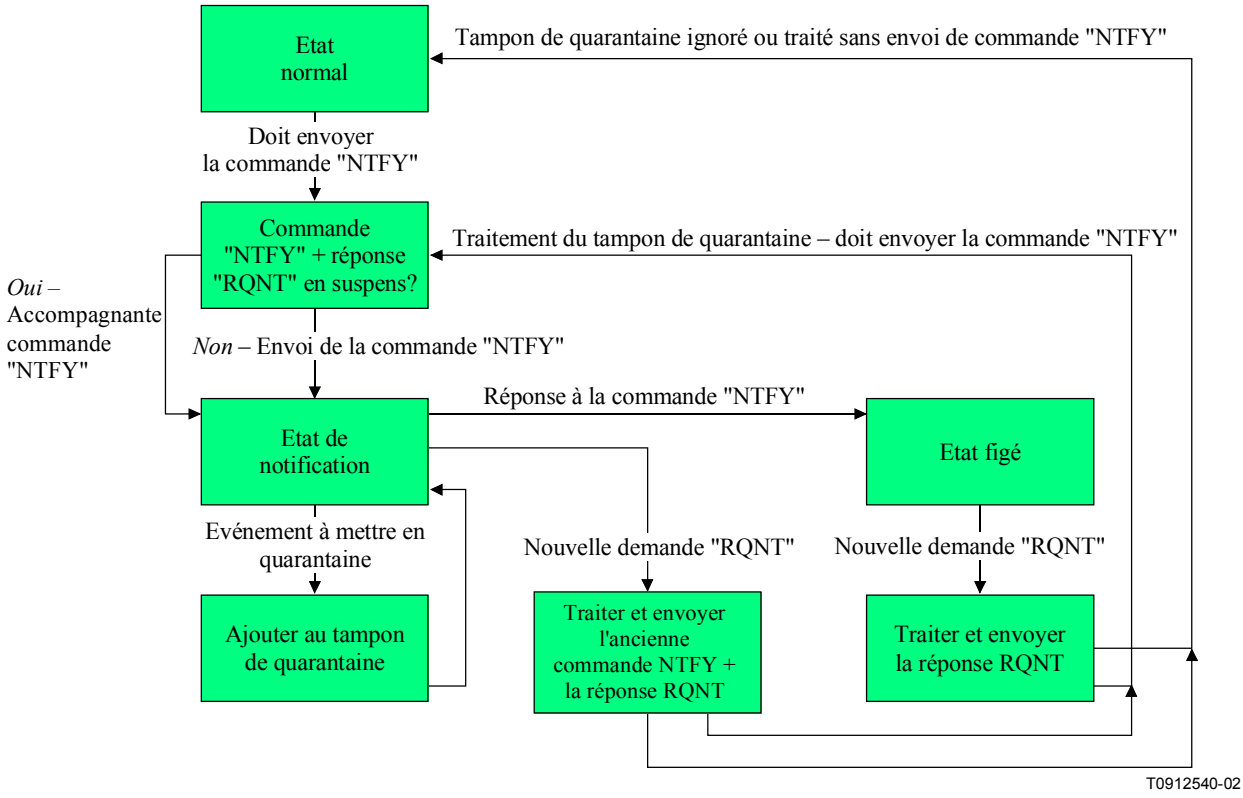

Figure A.2/J.171 – Algorithme de quarantaine

Les contrôleurs MGC DEVRAIENT fournir la réponse à un message Notify de réussite et la nouvelle demande NotificationRequest dans le même datagramme en utilisant le mécanisme d'accompagnement[21].

[21] Les vendeurs qui choisissent de ne pas appliquer la présente Recommandation devraient examiner attentivement les scénarios d'échec pour les contrôleurs de passerelle média.

A.2.4.3.2 Détection explicite

Un élément fondamental pour l'état des différentes extrémités est l'état de prise d'un circuit. Bien que les événements modifiant l'état de prise soient durables dans le protocole TGCP, les situations de course et la non-concordance des états peuvent quand-même exister, par exemple, lorsqu'un circuit est pris tandis que le contrôleur MGC s'emploie à demander à la passerelle de rechercher une prise (la situation "d'interférence" bien connue en téléphonie – Ceci est toutefois une question qui concerne principalement les circuits CAS bidirectionnels n'étant pas pris en charge dans la présente version de la Recommandation).

Afin d'éviter cette situation de course, la passerelle DOIT vérifier la situation au niveau de l'extrémité avant de répondre à une demande NotificationRequest. En particulier, elle DOIT renvoyer une erreur:

1) lorsqu'elle est priée de notifier une transition d'état de "prise"[22] tandis que le circuit est déjà pris (code d'erreur 401 – Circuit pris);

2) lorsqu'elle est priée de notifier une situation de "non prise"[23] tandis que le circuit n'est pas pris (code d'erreur 402 – Circuit non pris).

En outre, des définitions de signaux différentes peuvent spécifier qu'un signal ne fonctionnera que dans certaines conditions, par exemple, un rappel automatique de l'opérateur multifréquence ne peut être possible que si le circuit est déjà pris. Si de telles conditions sont prérequises pour un signal donné, la passerelle DOIT renvoyer l'erreur spécifiée dans la définition du signal lorsque ces conditions ne sont pas remplies.

Il convient de noter que la vérification des conditions est effectuée au moment de la réception de la demande de notification, où l'événement proprement dit qui est responsable de la situation effective peut être soit signalé, soit avoir été omis, soit effectivement mis en quarantaine.

Les autres variables relatives à l'état de la passerelle, telles que la liste des événements demandés ou celle des signaux demandés, sont complètement remplacées après chaque demande NotificationRequest accomplie, ce qui évite les désaccords de longue durée entre le contrôleur MGC et la passerelle.

Lorsqu'une demande NotificationRequest n'aboutit pas, qu'elle fasse partie ou pas d'une commande destinée à prendre en charge les connexions, la passerelle continuera simplement comme si la commande n'avait jamais été reçue, même si une erreur est renvoyée. Comme toutes les autres transactions, la demande NotificationRequest DOIT fonctionner comme une transaction atomique; tout changement entamé suite à la commande DOIT être annulé.

Une autre situation de course peut se produire lorsqu'une commande Notify est émise peu de temps avant la réception par la passerelle d'une demande NotificationRequest. L'identificateur RequestIdentifier est employé pour corréler les commandes Notify avec les commandes NotificationRequest, le contrôleur MGC étant ainsi en mesure de déterminer si la commande Notify a été produite avant ou après que la passerelle a reçu la nouvelle demande NotificationRequest.

A.2.4.3.3 Sémantique transactionnelle

Alors que le temps d'achèvement des transactions éventuelles augmente, par exemple, en raison des réserves de ressources extérieures, il est de plus en plus important de définir précisément la sémantique transactionnelle. En particulier, la question des situations de course, dans la mesure où elle se rapporte à l'état de prise, doit faire l'objet d'une définition précise.

---

[22] Par exemple, en demandant l'événement "sup" dans un circuit BLV/OI multifréquence de terminaison avec un appel en cours.

[23] Par exemple, en demandant l'événement "rel" dans un circuit multifréquence de services d'opérateur sans appel en cours.

Un point important qu'il faut examiner est le fait que l'état de prise peut en fait être modifié entre le moment où la transaction débute et celui où elle s'achève. Plus généralement, il peut être affirmé que la réussite de l'achèvement d'une transaction dépend d'une ou de plusieurs conditions préexistantes, une ou plusieurs d'entre elles pouvant changer dynamiquement au cours de l'exécution de la transaction.

La sémantique la plus simple pour cela consiste à demander simplement que toutes les conditions préexistantes DOIVENT s'appliquer à partir du moment où la transaction débute jusqu'à celui où elle s'achève. Donc, si l'une des conditions préexistantes change au cours de l'exécution de la transaction, celle-ci DOIT échouer. En outre, dès le début de la transaction, tous les nouveaux événements sont mis en quarantaine. Lorsque le résultat de la transaction est connu, tous les événements mis en quarantaine sont traités.

Considérons, à titre d'exemple, une transaction qui comporte une demande relative à un événement "prise". Lorsque la transaction débute, le circuit est en état de "non-prise" et c'est cette condition préexistante qui prévaut. Si cet état de prise est modifié et devient un état de "prise" avant que la transaction ne s'achève, la condition préexistante n'est plus remplie et la transaction échoue rapidement. L'événement "prise" sera maintenant entreposé dans le tampon de "quarantaine" qui sera traité ultérieurement.

A.2.4.3.4 Classement des commandes et traitement du désordre

Dans le cadre du protocole MGCP, il n'est pas demandé que le protocole de transport sous-jacent assure le classement des commandes envoyées à une passerelle ou à une extrémité. Cette propriété vise à actualiser les mesures autant que possible, mais elle a quelques défauts. Par exemple:

- les commandes Notify peuvent être retardées et aboutir au contrôleur MGC après la transmission d'une nouvelle commande NotificationRequest;
- si une nouvelle commande NotificationRequest est transmise avant qu'une réponse à une commande précédente ne soit reçue, rien ne garantit que la commande précédente ne sera pas reçue en deuxième position.

Les contrôleurs MGC et les passerelles qui désirent assurer un fonctionnement cohérent des extrémités peuvent utiliser les règles suivantes:

1) lorsqu'une passerelle prend en charge plusieurs extrémités, les commandes se rapportant aux différentes extrémités peuvent être envoyées en parallèle, par exemple, en suivant un modèle où chaque extrémité est commandée au moyen d'un processus ou d'un chemin qui lui sont propres;
2) lorsque plusieurs connexions sont établies à la même extrémité, les commandes se rapportant aux différentes connexions peuvent être envoyées en parallèle;
3) lors d'une connexion donnée, il ne devrait normalement y avoir qu'une seule commande en suspens (de création ou de modification). Toutefois, une commande DeleteConnection peut être lancée à tout moment. En conséquence, une passerelle peut parfois recevoir une commande ModifyConnection qui s'applique à une connexion précédemment supprimée. On ne DOIT pas tenir compte de telles commandes, et une erreur doit être renvoyée (code d'erreur 515 – Identificateur de connexion incorrect);
4) a une extrémité donnée, il ne devrait normalement y avoir à tout moment qu'une seule commande NotificationRequest en suspens. Le paramètre RequestId est utilisé pour corréler les commandes Notify avec la commande NotificationRequest qui les a déclenchées;
5) dans certains cas, une commande DeleteConnection avec caractère de remplacement implicite ou explicite qui s'applique à un groupe d'extrémités peut précéder une commande CreateConnection en suspens. Le contrôleur MGC devrait supprimer individuellement toutes les connexions dont l'achèvement était en suspens au moment de la commande globale DeleteConnection. Par ailleurs, de nouvelles commandes CreateConnection pour les

extrémités désignées au moyen d'un caractère de remplacement ne devraient pas être envoyées avant la réception d'une commande DeleteConnection avec caractère de remplacement;

6) lorsque des commandes sont incorporées les unes dans les autres, des spécifications de classement pour toutes les commandes DOIVENT être respectées. Par exemple, une commande CreateConnection contenant une demande de notification doit respecter simultanément les spécifications de classement pour la commande CreateConnection et pour la commande NotificationRequest;

7) les commandes AuditEnpoint et AuditConnection ne sont pas soumises à un quelconque classement;

8) la commande RestartInProgress doit toujours être la première commande envoyée par une extrémité, comme spécifié dans la procédure de redémarrage (voir A.2.4.3.5). Toute autre commande ou réponse doit être fournie après cette commande RestartInProgress (accompagnement admis);

9) lorsque plusieurs messages accompagnent un unique paquet, ils sont toujours traités dans l'ordre.

Parmi les règles susmentionnées, celles qui spécifient le comportement des passerelles DOIVENT être respectées par les passerelles de jonction, qui toutefois NE DOIVENT PAS faire d'hypothèse quant à l'application ou non des règles par les contrôleurs MGC. En conséquence, les passerelles DOIVENT toujours répondre aux commandes, qu'elles appliquent les règles susmentionnées ou non.

A.2.4.3.5 Lutte contre l'avalanche de redémarrages

Supposons qu'un grand nombre de passerelles soient activées simultanément. Si elles devaient toutes entamer une transaction RestartInProgress, le contrôleur MGC serait très certainement submergé, et il en résulterait des pertes de messages et un encombrement du réseau pendant la période critique de rétablissement du service. Afin d'éviter ces avalanches, les comportements suivants DOIVENT être adoptés:

1) lorsqu'une passerelle est activée, elle attribue à un temporisateur de redémarrage une valeur aléatoire, distribuée uniformément entre zéro et un temps d'attente maximal configurable (MWD, *maximum waiting delay*), par exemple, 360 secondes (voir ci-dessous). On DOIT prendre soin d'éviter que les nombres aléatoires produits aux différentes passerelles qui utiliseraient le même algorithme soient synchrones;

2) la passerelle attend ensuite la fin de la temporisation, la réception d'une commande provenant du contrôleur MGC ou la détection d'une activité locale du circuit, telle que, par exemple, une transition d'état de prise dans une passerelle de jonction. Une situation de prise préexistante conduit à la production d'un événement prise;

3) lorsque la temporisation de redémarrage est écoulée, à la réception d'une commande, ou à la détection d'une activité ou d'une situation de prise préexistante, la passerelle entame la procédure de redémarrage.

La procédure de redémarrage stipule simplement que l'extrémité DOIT envoyer au contrôleur MGC une commande RestartInProgress l'informant du redémarrage et l'assurant en outre que le premier message (commande ou réponse) qu'il observera en provenance de cette extrémité DOIT être cette commande RestartInProgress. Pour y arriver, l'extrémité DOIT profiter pleinement de l'accompagnement. Par exemple, si une activité de prise de circuit a lieu avant l'expiration de la temporisation de redémarrage, un paquet contenant la commande RestartInProgress accompagné d'une commande Notify pour l'événement prise sera produit. Dans le cas où la temporisation de redémarrage expire sans qu'une autre activité ait eu lieu, la passerelle envoie simplement un message RestartInProgress.

Si la passerelle devait entrer dans un état de "déconnexion" pendant la procédure de redémarrage, la procédure de déconnexion spécifiée au A.2.4.3.6 DOIT être appliquée, sauf qu'un message de "redémarrage" plutôt que de "déconnexion" est envoyé au cours de la procédure.

Il est prévu que chaque extrémité d'une passerelle disposera d'un contrôleur MGC configurable, à savoir une "entité notifiée", vers lequel le message initial de redémarrage est envoyé. Lorsque l'ensemble des extrémités d'une passerelle est géré par plus d'un contrôleur MGC, la procédure ci-dessus doit être effectuée pour chaque ensemble d'extrémités géré par un contrôleur MGC donné. La passerelle DOIT profiter pleinement des caractères de remplacement pour minimiser le nombre de messages RestartInProgress produits lorsque plusieurs extrémités d'une passerelle redémarrent et que ces extrémités sont gérées par le même contrôleur MGC.

La valeur du temps MWD est donnée par un paramètre de configuration qui dépend du type de la passerelle. Le raisonnement suivant peut être utilisé pour déterminer la valeur de ce temps dans une passerelle.

Les contrôleurs MGC sont généralement dimensionnés pour prendre en charge le trafic aux heures de pointe, au cours duquel, en moyenne, 60% des circuits seront occupés à servir des appels dont la durée moyenne est généralement de 3 minutes. Le traitement d'un appel comporte généralement 5 à 6 transactions entre chaque extrémité et le contrôleur MGC. Ce simple calcul montre que le contrôleur MGC devrait traiter 5 à 6 transactions par extrémité, toutes les 5 minutes en moyenne, ou, formulé différemment, environ une transaction par extrémité et par minute. Cela suggère qu'une valeur raisonnable du temps MWD pourrait être de 2 minutes par extrémité. Lorsque la valeur du temps est fixé pour la passerelle, cette valeur devrait être inversement proportionnelle aux nombre d'extrémités qui sont redémarrées. Par exemple, le temps pourrait être fixé à 5 secondes pour une passerelle qui prend en charge une ligne T1, ou à 180 millisecondes pour une passerelle qui prend en charge une ligne T3.

A.2.4.3.6 Extrémités déconnectées

Outre la procédure de redémarrage, les passerelles de jonction disposent également d'une procédure de "déconnexion", qui est entamée lorsqu'une extrémité se "déconnecte", comme décrit au A.2.4.2. Il convient de noter ici, que les extrémités peuvent seulement être déconnectées lorsqu'elles tentent de communiquer avec le contrôleur MGC. Les étapes suivantes sont suivies par une extrémité qui se "déconnecte":

1) un temporisateur de "déconnexion" est initialisé au moyen d'une valeur aléatoire, distribuée uniformément entre zéro et un temps d'attente initial de "déconnexion" configurable (Td_{init}), par exemple, 15 secondes. On DOIT prendre soin d'éviter que les nombres aléatoires produits aux différentes passerelles et extrémités qui utiliseraient le même algorithme soient synchrones;
2) la passerelle attend ensuite la fin de la temporisation, la réception d'une commande provenant du contrôleur MGC ou la détection d'une activité locale du circuit pour l'extrémité, telle que par exemple une transition d'état de prise;
3) lorsque la temporisation de "déconnexion" est écoulée, à la réception d'une commande, ou à la détection d'une activité locale du circuit, la passerelle entame la procédure de "déconnexion" à l'extrémité. Dans le cas d'une activité locale d'un utilisateur, un temps d'attente minimal de "déconnexion" configurable (Td_{min}) doit en outre s'être écoulé après la déconnexion de la passerelle ou après qu'elle a entamé pour la dernière fois la procédure de "déconnexion", afin de limiter le nombre d'applications de cette procédure;
4) si l'extrémité est encore déconnectée après l'application de la procédure de déconnexion, la temporisation de "déconnexion" est alors doublée, sous réserve d'un temps d'attente maximal de "déconnexion" configurable (Td_{max}), par exemple, 600 secondes, et la passerelle reprend à l'étape 2).

La procédure de "déconnexion" est semblable à celle de redémarrage, en raison du fait qu'elle stipule maintenant simplement que l'extrémité DOIT envoyer au contrôleur MGC une commande RestartInProgress l'informant de la déconnexion de l'extrémité et l'assurant en outre que le premier message (commande ou réponse) qu'il observera en provenance de cette extrémité DOIT être cette commande RestartInProgress. Pour y arriver, l'extrémité DOIT profiter pleinement de l'accompagnement. Le contrôleur MGC peut ensuite, par exemple, décider de procéder à l'audit de l'extrémité, ou simplement de supprimer toutes les connexions à cette extrémité.

La présente Recommandation ne spécifie pas, à dessein, d'autres comportements pour les extrémités déconnectées. Les vendeurs PEUVENT par exemple choisir de conserver les silences, de reproduire la tonalité de renumérotation ou même de permettre qu'un fichier téléchargé de type wav puisse être joué aux extrémités concernées.

Les valeurs par défaut sont égales à 15 secondes pour Td_{init}, à 15 secondes pour Td_{min} et à 600 secondes pour Td_{max}.

A.2.5 Codes de renvoi et codes d'erreur

Toutes les commandes dans le cadre du protocole MGCP donnent lieu à une réponse. La réponse contient un code de renvoi qui indique l'état de la commande. Les codes de renvoi sont des nombres entiers qui ont été divisés en cinq gammes:

- la valeur 000 indique un accusé de réception de réponse[24];
- les valeurs comprises entre 100 et 199 indiquent une réponse provisoire;
- les valeurs comprises entre 200 et 299 indiquent un établissement réussi;
- les valeurs comprises entre 400 et 499 indiquent une erreur transitoire;
- les valeurs comprises entre 500 et 599 indiquent une erreur durable.

[24] Un accusé de réception de réponse est employé pour les réponses provisoires (voir A.3.8)

La liste des valeurs qui ont été définies est donnée dans le Tableau A.2:

Table A.2/J.171 – Codes de renvoi

Code	Signification
000	Accusé de réception de réponse.
100	La transaction est en cours d'exécution. Un message d'établissement proprement dit suivra plus tard.
200	La transaction demandée a été exécutée normalement.
250	La ou les connexions ont été supprimées.
400	La transaction n'a pu être exécutée à cause d'une erreur transitoire.
401	Le combiné est déjà décroché ou le circuit est déjà pris.
402	Le combiné est déjà raccroché ou le circuit n'est pas pris.
500	La transaction n'a pu être exécutée parce que l'extrémité est inconnue.
501	La transaction n'a pu être exécutée parce que l'extrémité n'est pas prête.
502	La transaction n'a pu être exécutée parce que l'extrémité ne dispose pas de ressources suffisantes.
510	La transaction n'a pu être exécutée parce qu'une erreur de protocole a été détectée.
511	La transaction n'a pu être exécutée parce que la commande contenait une extension non reconnue.
512	La transaction n'a pu être exécutée parce que la passerelle n'est pas équipée pour détecter l'un des événements demandés.
513	La transaction n'a pu être exécutée parce que la passerelle n'est pas équipée pour produire l'un des signaux demandés.
514	La transaction n'a pu être exécutée parce que la passerelle ne peut envoyer l'annonce spécifiée.
515	La transaction renvoie à une identificateur de connexion erroné (pouvant déjà avoir été supprimé).
516	La transaction renvoie à un identificateur d'appel inconnu.
517	Mode non pris en charge ou non valable.
518	Paquetage non pris en charge ou inconnu.
519	Extrémité n'ayant pas de table numérique de mappages.
520	La transaction n'a pu être exécutée parce que l'extrémité est en cours de "redémarrage".
521	Extrémité réorientée vers un autre contrôleur MGC.
522	Evénement ou signal faisant défaut.
523	Mesure inconnue ou combinaison interdite de mesures.
524	Incohérence interne dans le paramètre LocalConnectionOptions.
525	Extension inconnue dans le paramètre LocalConnectionOptions.
526	Largeur de bande insuffisante.
527	Paramètre RemoteConnectionDescriptor manquant.
528	Version de protocole incompatible.
529	Défaillance matérielle interne.
532	Valeur(s) non prise(s) en charge dans le paramètre LocalConnectionOptions.
533	Réponse trop longue.

A.2.6 Codes de motif

Les codes de motif sont employés par la passerelle lors de la suppression d'une connexion pour informer le contrôleur MGC sur le motif qui a conduit à supprimer cette connexion. Le code de motif est un nombre entier, et les valeurs ont été définies dans le Tableau A.3:

Tableau A.3/J.171 – Codes de motif

Code	Signification
900	Dysfonctionnement de l'extrémité
901	Extrémité mise hors service
902	Perte de la connectivité de couche inférieure (par exemple synchronisation en aval)

A.3 Protocole de commande de passerelle média

Le protocole MGCP met en œuvre l'interface de commande de passerelle média comme un ensemble de transactions. Les transactions sont composées d'une commande et d'une réponse obligatoire. Les types de commande sont au nombre de huit:

- CreateConnection;
- ModifyConnection;
- DeleteConnection;
- NotificationRequest;
- Notify;
- AuditEndpoint;
- AuditConnection;
- RestartInProgress.

Les quatre premières commandes sont envoyées par le contrôleur MGC à une passerelle. La commande Notify est envoyée par la passerelle au contrôleur MGC. La passerelle peut également envoyer une commande DeleteConnection, comme défini au A.2.3.6. Le contrôleur MGC peut envoyer une quelconque commande d'audit à la passerelle et, finalement, la passerelle peut envoyer une commande RestartInProgress au contrôleur MGC.

A.3.1 Description générale

Toutes les commandes sont composées d'un en-tête de commande, qui pour certaines d'entre elles peut être suivi d'une description de session.

Toutes les réponses sont composées d'un en-tête de réponse, qui pour certaines d'entre elles peut être suivi d'une description de session.

Les en-têtes et les descriptions de session sont codés au moyen d'un ensemble de lignes de texte, séparées par un caractère de retour à la ligne et d'avancement (ou, éventuellement de retour à la ligne seulement). Les en-têtes sont séparés des descriptions de session par un interligne.

Le protocole MGCP emploie un identificateur de transaction dont la valeur est comprise entre 1 et 999999999 pour corréler les commandes et les réponses. L'identificateur de la transaction est codé au moyen d'un composant de l'en-tête de commande et répété au moyen d'un composant de l'en-tête de réponse.

A.3.2 En-tête de commande

L'en-tête de commande est composé des éléments suivants:

- une ligne de commande identifiant la mesure ou l'action demandée, l'identificateur de la transaction, l'extrémité pour laquelle la mesure est demandée, et la version du protocole MGCP;
- un ensemble de lignes de paramètres composées d'un nom de paramètre suivi de sa valeur.

Sauf indication ou stipulation contraires par d'autres normes en référence, tous les composants de l'en-tête de commande sont insensibles à la casse. Cela vaut pour les actions ainsi que pour les paramètres et leurs valeurs, et toutes les comparaisons DOIVENT traiter les majuscules et les minuscules ainsi que leur combinaison comme étant semblables.

A.3.2.1 Ligne de commande

Une ligne de commande est composée des éléments suivants:

- le nom de l'action demandée;
- l'identification de la transaction;
- le nom de l'extrémité ou des extrémités qui devraient exécuter la commande (dans les notifications ou les redémarrages, le nom de l'extrémité ou des extrémités qui émettent la commande);
- la version du protocole.

Ces quatre éléments sont codés au moyen de chaînes de caractères d'imprimerie ASCII séparés par des blancs, c'est-à-dire, les caractères blancs ASCII (0x20) ou de tabulation (0x09). Les passerelles de jonction DEVRAIENT employer un seul séparateur d'espace ASCII, mais elles DOIVENT être en mesure d'analyser des messages contenant des blancs supplémentaires.

A.3.2.1.1 Codage de l'action demandée

Les actions demandées sont codées au moyen de codes ASCII à quatre lettres majuscules ou minuscules (les comparaisons DOIVENT être insensibles à la casse), comme défini dans le Tableau A.4:

Tableau A.4/J.171 – Codes de l'action demandée

Action	Code
CreateConnection	CRCX
ModifyConnection	MDCX
DeleteConnection	DLCX
NotificationRequest	RQNT
Notify	NTFY
AuditEndpoint	AUEP
AuditConnection	AUCX
RestartInProgress	RSIP

De nouvelles actions pourront être définies dans des versions ultérieures du protocole. Il pourrait être nécessaire, à des fins expérimentales, d'employer de nouvelles actions avant que celles-ci ne soient confirmées dans une version publiée du présent protocole. Les actions expérimentales devraient être identifiées par un code à quatre lettres commençant par la lettre X (par exemple, XPER).

Une passerelle qui reçoit une commande contenant une action expérimentale qu'elle ne prend pas en charge DOIT renvoyer une erreur (code d'erreur 511 – Extension non reconnue).

A.3.2.1.2 Identificateurs de transaction

Les identificateurs de transaction sont utilisés pour corréler les commandes et les réponses.

Une passerelle de jonction prend en charge les deux espaces distincts suivants de nom d'identificateur de transaction:

- un espace de nom d'identificateur de transaction pour l'envoi de transactions;
- un espace de nom d'identificateur de transaction pour la réception de transactions.

Les identificateurs de transaction pour les commandes qui sont envoyées à une passerelle de jonction donnée DOIVENT au minimum être uniques pendant toute la durée des transactions qui sont effectuées par l'ensemble des contrôleurs MGC commandant cette passerelle de jonction (voir A.3.5). Donc, indépendamment du contrôleur MGC émetteur, les passerelles de jonction peuvent toujours détecter les transactions reproduites en examinant simplement l'identificateur de transaction. La coordination entre les contrôleurs MGC en ce qui concerne ces identificateurs de transaction sort toutefois du cadre de la présente Recommandation.

Les identificateurs de transaction pour toutes les commandes envoyées en provenance d'une passerelle de jonction donnée DOIVENT être uniques pendant toute la durée des transactions (voir A.3.5), indépendamment du contrôleur MGC à qui la commande est envoyée. Donc, un contrôleur MGC peut toujours détecter une transaction reproduite provenant d'une passerelle de jonction à partir de la combinaison du nom de domaine domain-name de l'extrémité et de l'identificateur de transaction. La passerelle, pour sa part, peut toujours détecter un accusé de réception de réponse reproduit en examinant l'identificateur ou les identificateurs de transaction.

L'identificateur de transaction est codé au moyen d'une chaîne à neuf chiffres décimaux au plus. Dans les lignes de commande, il suit immédiatement le code de l'action.

Les valeurs des identificateurs de transaction sont comprises entre 1 et 999999999. Une entité de protocole MGCP NE DOIT PAS réutiliser un identificateur de transaction moins de trois minutes après l'achèvement d'une commande précédente où cet identificateur était employé.

A.3.2.1.3 Codage des extrémités, contrôleurs de passerelle média et noms de l'entité notifiée

Les noms des extrémités et des contrôleurs MGC sont codés au moyen d'adresses de courrier électronique, comme défini dans le document IETF RFC 821. Dans ces adresses, le nom de domaine identifie le système auquel l'extrémité est rattachée, tandis que la partie de gauche identifie une extrémité particulière de ce système. Les deux composantes DOIVENT être insensibles à la casse.

Des exemples de ces noms sont donnés ci-après:

ds/ds1-3/2@TGCP2.whatever.net	Deuxième circuit de la troisième interface DS1 dans la passerelle de jonction TGCP2 du réseau "whatever".
MGC@mgc.whatever.net	Contrôleur de passerelle média du réseau "whatever".

Le nom des entités notifiées s'exprime à l'aide de la même syntaxe, le numéro du port pouvant éventuellement être ajouté, comme dans l'adresse suivante:

```
MGC@mgc.whatever.net:5234
```

Dans le cas où le numéro du port est omis, le port par défaut pour le protocole MGCP (2427) sera utilisé. On trouvera des précisions supplémentaires sur les noms d'extrémité au A.2.1.1.

A.3.2.1.4 Codage de la version du protocole

La version du protocole est codée au moyen du mot-clé "MGCP" suivi d'un blanc et du numéro de la version, qui précède lui-même le nom de profil "TGCP" et un numéro de version de celui-ci. Les numéros de version comportent un numéro de version principal, un point et un numéro de version secondaire. Les numéros principaux et secondaires sont codés au moyen de nombres décimaux. Le numéro de version du profil défini par la présente Recommandation est 1.0.

La version du protocole pour la présente Recommandation DOIT être codée comme suit:

```
MGCP 1.0 TGCP 1.0
```

La partie "TGCP 1.0" indique qu'il s'agit du profil TGCP 1.0 du protocole MGCP 1.0.

Une entité qui reçoit une commande contenant une version de protocole qu'elle ne prend pas en charge DOIT répondre par une erreur (code d'erreur 528 – Version de protocole incompatible).

A.3.2.2 Lignes de paramètre

Les lignes de paramètre sont composées d'un nom de paramètre, qui dans la plupart des cas comporte un seul caractère en majuscule, suivi d'un double point, d'un blanc et d'une valeur pour le paramètre. Les noms et les valeurs de paramètre sont toutefois encore insensibles à la casse. Les paramètres qui peuvent figurer dans les commandes sont définis dans le Tableau A.5:

Tableau A.5/J.171 – Paramètres de commande

Nom du paramètre	Code	Valeur du paramètre
ResponseAck[25]	K	Voir la description.
CallId	C	Chaîne hexadécimale à 32 caractères au plus.
ConnectionId	I	Chaîne hexadécimale à 32 caractères au plus.
NotifiedEntity	N	Un identificateur, de format IETF RFC 821, composé d'une chaîne arbitraire et du nom de domaine de l'entité demandeuse, éventuellement complétés par un numéro de port, comme dans l'adresse suivante: Call-agent@ca.whatever.net:5234
RequestIdentifier	X	Voir la description.
LocalConnectionOptions	L	Voir la description.
Connection Mode	M	Voir la description.
RequestedEvents	R	Voir la description.
SignalRequests	S	Voir la description.
ObservedEvents	O	Voir la description.
ConnectionParameters	P	Voir la description.
ReasonCode	E	Voir la description.
SpecificEndPointId	Z	Un identificateur, de format IETF RFC 821, composé d'une chaîne arbitraire, suivie éventuellement du signe "@", lui-même précédant le nom de domaine de la passerelle de jonction à laquelle cette extrémité est rattachée.
MaxEndPointIds	ZM	Chaîne décimale à 16 caractères au plus.
NumEndPoints	ZN	Chaîne décimale à 16 caractères au plus.
RequestedInfo	F	Voir la description.
QuarantineHandling	Q	Voir la description.
DetectEvents	T	Voir la description.
EventStates	ES	Voir la description.
RestartMethod	RM	Voir la description.
RestartDelay	RD	Un nombre de secondes codées au moyen d'un nombre décimal.
Capabilities	A	Voir la description.
VersionSupported	VS	Voir la description.

[25] Le paramètre ResponseAck ne figure pas au A.2.3 parce que les identificateurs de transaction n'apparaissent pas dans notre exemple d'interface API. Les responsables chargés de l'implémentation peuvent choisir une approche différente.

Les paramètres ne sont pas nécessairement présents dans toutes les commandes. Le Tableau A.6 donne la relation entre les paramètres et les commandes. La lettre M signifie "obligatoire", O "facultatif" et F "interdit":

Tableau A.6/J.171 –

Nom du paramètre	CRCX	MDCX	DLCX	RQNT	NTFY	AUEP	AUCX	RSIP
ResponseAck[25]	O	O	O	O	O	O	O	O
CallId	M	M	O	F	F	F	F	F
ConnectionId	F	M	O	F	F	F	M	F
RequestIdentifier	O	O	O	M	M	F	F	F
LocalConnectionOptions	M	O	F	F	F	F	F	F
ConnectionMode	M	O	F	F	F	F	F	F
RequestedEvents	O[a)]	O[a)]	O[a)]	O[a)]	F	F	F	F
SignalRequests	O[a)]	O[a)]	O[a)]	O[a)]	F	F	F	F
NotifiedEntity	O	O	O	O	O	F	F	F
ReasonCode	F	F	O	F	F	F	F	F
ObservedEvents	F	F	F	F	M	F	F	F
Connection parameters	F	F	O	F	F	F	F	F
SpecificEndpointId	F	F	F	F	F	O	F	F
MaxEndPointIds	F	F	F	F	F	O	F	F
NumEndPoints	F	F	F	F	F	F	F	F
RequestedInfo	F	F	F	F	F	O	O	F
QuarantineHandling	O	O	O	O	F	F	F	F
DetectEvents	O	O	O	O	F	F	F	F
EventStates	F	F	F	F	F	F	F	F
RestartMethod	F	F	F	F	F	F	F	M
RestartDelay	F	F	F	F	F	F	F	O
Capabilities	F	F	F	F	F	F	F	F
VersionSupported	F	F	F	F	F	F	F	F
RemoteConnectionDescriptor	O	O	F	F	F	F	F	F

[a)] Les paramètres RequestedEvents et SignalRequests sont en option dans la demande NotificationRequest. S'ils sont omis, les listes correspondantes seront considérées comme étant vides. Pour les commandes de prise en charge des connexions, cela s'applique aussi lorsqu'un identificateur RequestIdentifier est présent.

Les passerelles de jonction et les contrôleurs MGC DEVRAIENT toujours fournir les paramètres obligatoires avant les paramètres facultatifs; cependant les passerelles de jonction NE DOIVENT PAS échouer lorsque la présente Recommandation n'est pas appliquée.

Si les responsables chargés de l'implémentation doivent expérimenter de nouveaux paramètres, par exemple lors de l'élaboration d'une nouvelle application dans le cadre du protocole MGCP, ils devraient identifier ces paramètres au moyen de noms qui commencent par les chaînes "X-" ou "X+", comme dans l'exemple suivant:

```
X-FlowerOfTheDay: Daisy
```

Les noms de paramètre qui commencent par "X+" sont des extensions de paramètre obligatoires. Une passerelle qui reçoit une extension de paramètre obligatoire qu'elle ne comprend pas DOIT répondre par une erreur (code d'erreur 511 – Extension non reconnue).

Les noms de paramètre qui commencent par "X-" sont des extensions de paramètre non critiques. Une passerelle qui reçoit une extension de paramètre non critique qu'elle ne comprend pas peut en toute sécurité ne pas tenir compte de ce paramètre.

Il convient de noter que les actions expérimentales sont de la forme X*ABC*, tandis que les paramètres expérimentaux sont de la forme X-ABC.

Lorsqu'une ligne de paramètre est reçue avec un paramètre interdit, ou une quelconque erreur de format, l'entité qui la reçoit devrait répondre par le code d'erreur le plus précis possible pour l'erreur en question. Le code d'erreur le moins précis est le code 510 – Erreur de protocole. Un texte de commentaires peut toujours être fourni.

A.3.2.2.1 Accusé de réception de réponse

Le paramètre accusé de réception de réponse est utilisé pour prendre en charge la prise de contact à trois décrite au A.3.7. Il contient une liste de "domaines d'identificateurs de transaction confirmée", séparés par des virgules.

NOTE – Le paramètre ResponseAck ne figure pas au A.2.3 parce que les identificateurs de transaction n'apparaissent pas dans notre exemple d'interface API. Les responsables chargés de l'implémentation peuvent choisir une approche différente.

Chaque "domaine d'identificateurs de transaction confirmée" est composé soit d'un nombre décimal, lorsque le domaine ne comprend qu'une transaction, soit de deux nombres décimaux séparés par un tiret unique, donnant les identificateurs inférieur et supérieur de transaction du domaine.

Un exemple d'accusé de réception de réponse est donné ci-après:

```
K: 6234-6255, 6257, 19030-19044
```

A.3.2.2.2 Identificateur de demande

Le paramètre RequestIdentifier établit une corrélation entre une commande Notify et la demande NotificationRequest qui l'a déclenchée. Il a la forme d'une chaîne hexadécimale à 32 caractères au plus. La chaîne "0" est réservée pour la signalisation d'événements durables lorsque qu'aucune demande NotificationRequest n'a encore été reçue (voir A.2.3.2).

A.3.2.2.3 Options locales de connexion

Les options locales de connexion décrivent les paramètres opérationnels que les contrôleurs MGC ordonnent à la passerelle d'employer pour une connexion. Ces paramètres sont les suivants:

- la période de mise en paquets exprimée en millisecondes, codée au moyen du mot-clé "p" suivi d'un double point et d'un nombre décimal;
- le nom littéral de l'algorithme de compression, codé au moyen du mot-clé "a" suivi d'un double point et d'une chaîne de caractères;
- le paramètre suppression d'écho, codé au moyen du mot-clé "e" suivi d'un double point et de la valeur "on" ou "off";
- le paramètre type de service, codé au moyen du mot-clé "t" suivi d'un double point et de la valeur codée au moyen de deux chiffres hexadécimaux;
- le paramètre suppression des silences, codé au moyen du mot-clé "s" suivi d'un double point et de la valeur "on" ou "off".

Les paramètres LocalConnectionOptions utilisés pour la sécurité sont codés de la manière suivante:

- le code secret est codé au moyen du mot-clé "sc-st" suivi d'un double point, d'une méthode, d'un double point et du code secret en vigueur. La méthode est soit la chaîne "clear" si le code secret est codé au moyen de texte en clair soit la chaîne "base64" si le code secret est codé au moyen de la base64;
- la suite de chiffrement pour le protocole RTP est codée au moyen du mot-clé "sc-rtp" suivi d'un double point et d'une chaîne relative à la suite de chiffrement pour le protocole RTP, comme défini ci-après. Une liste des valeurs peut être spécifiée, auquel cas ces valeurs seront séparées par des points-virgules;
- la suite de chiffrement pour le protocole RTCP est codée au moyen du mot-clé "sc-rtcp" suivi d'un double point et d'une chaîne relative à la suite de chiffrement pour le protocole RTCP, comme défini ci-après. Une liste des valeurs peut être spécifiée, auquel cas ces valeurs seront séparées par des points-virgules.

Les chaînes relatives aux suites de chiffrement pour les protocoles RTP et RTCP obéissent à la syntaxe suivante:

ciphersuite = [AuthenticationAlgorithm] "/" [EncryptionAlgorithm]

AuthenticationAlgorithm = 1*(ALPHA / DIGIT / "-" / "_")

EncryptionAlgorithm = 1*(ALPHA / DIGIT | "-" / "_")

où ALPHA et DIGIT sont définis dans le document IETF RFC 2234. Les blancs ne sont pas admis dans une suite de chiffrement. L'exemple suivant illustre l'emploi d'une suite de chiffrement:

62/51

La liste en vigueur des suites de chiffrement prises en charge dans les réseaux IPCablecom est fournie dans la Rec. UIT-T J.170.

Lorsque plusieurs paramètres sont présents, les valeurs sont séparées par des virgules. L'introduction d'un paramètre sans valeur est considérée comme une erreur (code d'erreur 524 – Incohérence dans le paramètre LocalConnectionOptions).

Des exemples d'options locales de connexion sont donnés ci-après:

```
L: p:10, a:PCMU
L: p:10, a:PCMU, e:off, t:20, s:on
L: p:30, a:G729A, e:on, t:A0, s:off
```

Le type de service à valeur hexadécimale "20" implique une priorité IP égale à 1 tandis qu'un type "A0" implique une priorité IP égale à 5.

Cet ensemble d'attributs peut être élargi au moyen d'attributs d'extension. Ces attributs d'extension sont composés d'un nom d'attribut, suivi d'un double point, et d'une liste de valeurs d'attribut séparées par des points-virgules. Le nom d'attribut DOIT commencer par les deux caractères "x+" pour une extension obligatoire ou "x-" pour une extension non obligatoire. Si une passerelle reçoit un attribut d'extension obligatoire qu'elle ne reconnaît pas, elle DOIT rejeter la commande avec une erreur (code d'erreur 525 – Extension inconnue dans le paramètre LocalConnectionOptions).

Les paramètres LocalConnectionOptions qui sont utilisés pour la surveillance électronique sont les suivants:

- l'identificateur de connexion pour le contenu de l'appel, codé au moyen du mot-clé "es-cci" suivi d'un double point et d'une chaîne à 8 caractères hexadécimaux au plus, correspondant à un identificateur de connexion à 32 bits pour le contenu de l'appel;

- la destination du contenu de l'appel, codée au moyen du mot-clé "es-ccd" suivi d'un double point et d'une adresse IP codée comme une adresse IP pour la partie du nom de domaine d'un nom d'extrémité. L'adresse IP est suivie d'un double point et de 5 caractères décimaux au plus pour un numéro de port UDP à utiliser.

A.3.2.2.4 Capacités

Les capacités informent le contrôleur MGC sur ses capacités lorsqu'il est soumis à un audit. Le codage des capacités est fondé sur le codage des paramètres LocalConnectionOptions pour les paramètres qui sont communs aux deux. En outre, les capacités peuvent aussi contenir une liste des paquetages pris en charge et une liste des modes pris en charge.

Les paramètres utilisés sont les suivants:

- la période de mise en paquets exprimée en millisecondes, codée au moyen du mot-clé "p" suivi d'un double point et d'un nombre décimal. Un domaine peut être spécifié au moyen de deux nombres décimaux séparés par un tiret;
- le nom litéral de l'algorithme de compression, codé au moyen du mot-clé "a" suivi d'un double point et d'une chaîne de caractères. Une liste de valeurs peut être spécifiée, auquel cas les valeurs seront séparées par des points-virgules;
- la largeur de bande en kilobits par seconde (1 000 bits par seconde), codée au moyen du mot-clé "b" suivi d'un double point et d'un nombre décimal. Un domaine peut être spécifié au moyen de deux nombres décimaux séparés par un tiret;
- le paramètre suppression d'écho, codé au moyen du mot-clé "e" suivi d'un double point et de la valeur "on" si la suppression d'écho est effectuée, et "off" dans les autres cas;
- le paramètre type de service, codé au moyen du mot-clé "t" suivi d'un double point et d'une valeur "0" si le type de service n'est pas pris en charge, les autres valeurs indiquant la prise en charge du type de service;
- le paramètre suppression des silences, codé au moyen du mot-clé "s" suivi d'un double point et de la valeur "on" lorsque la suppression des silences est prise en charge, et "off" dans les autres cas;
- les paquetages d'événements pris en charge par cette extrémité, codés au moyen du mot-clé "v" suivi d'un double point et d'une liste des noms de paquetages pris en charge, séparés par des points-virgules. La première valeur spécifiée correspondra au paquetage par défaut pour l'extrémité;
- les modes de connexion pris en charge par cette extrémité, codés au moyen du mot-clé "m" suivi d'un double point et d'une liste des modes de connexion pris en charge, séparés par des points-virgules, comme défini au A.3.2.2.7;
- le mot-clé "sc-st" si la sécurité IPCablecom est prise en charge. Dans ce cas, les mots-clés suivants indiquent les suites de chiffrement qui sont prises en charge:
  - le mot-clé "sc-rtp" suivi d'un double point et d'une liste d'algorithmes d'authentification pour le protocole RTP séparés par des points-virgules, une barre oblique et une liste d'algorithmes de chiffrement pris en charge, séparés par des points-virgules.
  - le mot-clé "sc-rtcp" suivi d'un double point et d'une liste d'algorithmes d'authentification pour le protocole RTCP séparés par des points-virgules, une barre oblique et une liste d'algorithmes de chiffrement pris en charge, séparés par des points-virgules.

Lorsque plusieurs paramètres sont présents, les valeurs sont séparées par des virgules.

Des exemples de capacité sont donnés ci-après:

```
A: a:PCMU;G729A, p:10-100, e:on, s:off, v:IT,
              m:sendonly;recvonly;sendrecv;inactive
A: a:G729A; p:30-90, e:on, s:on, v:MT,
              m:sendonly;recvonly;sendrecv;inactive,
              sc-st, sc-rtp: 00/51;03
```

Il convient de noter que les codecs et les algorithmes de sécurité ne sont donnés qu'à titre d'exemple – des Recommandations IPCablecom distinctes donnent des précisions concernant les codecs et les algorithmes concrètement pris en charge, ainsi que le codage utilisé (voir les Recs. UIT-T J.170, J.162 et J.161).

- Le mot-clé "es-cci" lorsque la surveillance électronique IPCablecom est prise en charge.

A.3.2.2.5 Paramètres de connexion

Les paramètres de connexion sont codés au moyen d'une chaîne de couples, formés du type et de la valeur, où le type est un identificateur de paramètre à deux lettres et la valeur est un nombre entier décimal. Les types sont séparés des valeurs par le signe "=". Les paramètres sont séparés les uns des autres par une virgule.

Les types des paramètres de connexion sont spécifiés dans le Tableau A.7:

Tableau A.7/J.171 – Types de paramètres de connexion

Nom du paramètre de connexion	Code	Valeur du paramètre de connexion
Paquets envoyés	PS	Nombre de paquets qui ont été envoyés par l'intermédiaire de la connexion
Octets envoyés	OS	Nombre d'octets qui ont été envoyés par l'intermédiaire de la connexion
Paquets reçus	PR	Nombre de paquets qui ont été reçus par l'intermédiaire de la connexion
Octets reçus	OR	Nombre d'octets qui ont été reçus par l'intermédiaire de la connexion
Paquets perdus	PL	Nombre de paquets qui n'ont pas été reçus par l'intermédiaire de la connexion, obtenu à partir des numéros manquants parmi les numéros d'ordre
Gigue	JI	Gigue moyenne entre l'arrivée des paquets, exprimée comme un nombre entier de millisecondes
Temps d'attente	LA	Temps d'attente moyen, exprimé comme un nombre entier de millisecondes

Les noms des paramètres d'extension de connexion sont composés de la chaîne "X-" suivie d'un nom de paramètre d'extension à deux lettres. Les contrôleurs MGC qui reçoivent des extensions non reconnues DOIVENT, sans le communiquer expressément, ne pas tenir compte de ces extensions.

Un exemple du codage d'un paramètre de connexion est donné ci-après:

```
P: PS=1245, OS=62345, PR=0, OR=0, PL=0, JI=0, LA=48
```

A.3.2.2.6 Codes de motif

Les codes de motif sont des valeurs numériques à trois chiffres. Il sont suivis en option d'un blanc et de commentaires, par exemple:

```
900 Endpoint malfunctioning
```

On trouvera une liste des codes de motif au A.2.6.

A.3.2.2.7 Mode de connexion

Le mode de connexion décrit le mode de fonctionnement de la connexion. Les valeurs possibles sont indiquées dans le Tableau A.8:

Tableau A.8/J.171 – Valeurs du mode de connexion

Mode	Signification
M: sendonly	La passerelle devrait seulement envoyer des paquets
M: recvonly	La passerelle devrait seulement recevoir des paquets
M: sendrecv	La passerelle devrait envoyer et recevoir des paquets
M: inactive	La passerelle ne devrait ni envoyer ni recevoir des paquets
M: loopback	La passerelle devrait placer l'extrémité en mode bouclage
M: conttest	La passerelle devrait placer l'extrémité en mode essai de continuité
M: netwloop	La passerelle devrait placer l'extrémité en mode bouclage en réseau
M: netwtest	La passerelle devrait placer l'extrémité en mode essai de continuité en réseau

A.3.2.2.8 Codage du nom d'événement ou de signal

Les noms d'événement ou de signal sont composés d'un nom de paquetage en option, séparé par une barre oblique (/) du nom de l'événement effectif. Le nom d'événement peut éventuellement être suivi du signe arobase (@) et de l'identificateur de la connexion où l'événement devrait être observé. Les noms d'événement sont utilisés dans les paramètres RequestedEvents, SignalRequests, DetectEvents, ObservedEvents et EventStates. Chaque événement est identifié par un code d'événement. Ces codages ASCII ne sont pas sensibles à la casse. Des valeurs telles que "co", "Co", "CO" ou "cO" devraient être considérées comme étant égales.

Les noms d'événement suivants constituent des exemples valables:

`IT/co1`	Essai de continuité à l'émission dans le paquetage de circuits de l'ISUP.
`co1`	Essai de continuité à l'émission dans le paquetage de circuits de l'ISUP, en supposant que ce paquetage est le paquetage pas défaut pour l'extrémité.
`IT/rt@0A3F58`	Rappel automatique pour la connexion "0A3F58"

On peut en outre désigner les événements au moyen de caractères de remplacement, au lieu de les nommer individuellement, dans les paramètres RequestedEvents et DetectEvents (mais pas dans les paramètres SignalRequests, ObservedEvents ou EventStates):

`IT/all`	Tous les événements du paquetage de circuits de l'ISUP.

Enfin, le signe astérisque peut être employé pour désigner "toutes les connexions", et le signe dollar pour désigner la "connexion effective". Les notations suivantes constituent des exemples valables:

`IT/ma@*`	L'événement démarrage média pour le protocole RTP dans toutes les connexions à l'extrémité
`IT/rt@$`	Rappel automatique pour la connexion effective

On trouvera un ensemble initial de paquetages d'événements pour les passerelles de jonction à l'Annexe A.A.

A.3.2.2.9 Paramètre RequestedEvents

Le paramètre RequestedEvents fournit la liste d'événements qui ont été demandés. Les codes d'événement actuellement définis sont décrits à l'Annexe A.A. Chaque événement peut être spécifié par une mesure demandée, ou par une liste de mesures. Toutes les mesures ne peuvent pas être combinées – Se reporter au A.2.3.1 pour les combinaisons valables. Ces mesures, lorsqu'elles sont spécifiées, sont codées au moyen d'une liste de mots-clés compris entre des parenthèses et séparés par des virgules. Ces codes, pour les différentes mesures, sont indiquées dans le Tableau A.9:

Tableau A.9/J.171 – Codes de mesures

Mesure	Code
Notifier immédiatement	N
Recueillir	A
Ne pas tenir compte	I
Garder le ou les signaux activés	K
Insérer la demande NotificationRequest	E
Insérer la demande ModifyConnection	C

Lorsque aucune mesure n'est spécifiée, la mesure par défaut est la notification de l'événement. Cela signifie que "ft" et "ft(N)" sont par exemple équivalents. Des événements qui ne font pas partie d'une liste sont ignorés, sauf lorsqu'il s'agit d'événements durables.

La liste des événements demandés est codée sur une seule ligne, les groupes d'événements ou de mesures étant séparés par des virgules. Un exemple de codage du paramètre RequestedEvents est donné ci-après:

`R: oc(N), of(N)` Notifier l'achèvement de l'opération, notifier l'échec de l'opération.

Le format de la demande NotificationRequest insérée est le suivant:

`E ( R( <RequestedEvents>), S( <SignalRequests>) )`

chacune des grandeurs R et S étant en option et éventuellement données dans un ordre différent.

Le format de la mesure insérée ModifyConnection est le suivant:

`C(M(<ConnectionMode`$_1$`>( <ConnectionID`$_1$`> )) , ... ,`
`M(<ConnectionMode`$_n$`>(ConnectionID`$_n$` )))`

L'exemple suivant illustre l'emploi de la demande insérée ModifyConnection:

`R: ma@23B34D(A, C(M(sendrecv($)))), oc(N), of(N)`

Lors du démarrage média pour la connexion "23B34D", changer le mode de connexion et passer de "connection effective" à "envoyer et recevoir". Notifier les événements en ce qui concerne "l'opération achevée" et "l'opération échouée".

A.3.2.2.10 Paramètre SignalRequests

Le paramètre SignalRequests fournit le nom des signaux qui ont été demandés. On trouvera les signaux actuellement définis à l'Annexe A.A. Un signal donné ne peut figurer qu'une fois dans la liste, et tous les signaux seront appliqués, par définition, en même temps.

Certains signaux peuvent être spécifiés par des paramètres de signal. Lorsqu'un signal est spécifié par plusieurs paramètres de signal, ceux-ci sont séparés par des virgules. Tous les paramètres de signal DOIVENT posséder le format spécifié ci-après (des blancs étant admis):

signal-parameter = signal-parameter-value /

signal-parameter-name "="signal-parameter-value /

signal-parameter-name "(" signal-parameter-list ")"

signal-parameter-list = signal-parameter-value 0*("," signal-parameter-value)

où la grandeur signal-parameter-value peut être soit une chaîne soit une chaîne entre guillemets. Une paire de guillemets consécutifs dans une chaîne entre guillemets éliminera ceux-ci. Par exemple, la chaîne "ab" "c" est en fait la chaîne ab"c.

Chaque signal est d'un des types de signal suivants (voir A.2.3.1):

- On/Off (OO) (activé/désactivé)
- Time-out (TO) (avec interruption)
- Brief (BR) (bref)

Les signaux OO peuvent être paramétrisés au moyen d'un signe "+" pour activer le signal, ou d'un signe "-" pour le désactiver. Lorsqu'un signal OO n'est pas paramétrisé, il est activé. Les deux commandes suivantes activeront le signal "mysignal":

```
mysignal(+), mysignal
```

Les signaux TO peuvent être paramétrisés au moyen du paramètre de signal "TO" et d'une temporisation qui l'emporte sur la valeur par défaut. Lorsqu'un signal TO n'est pas paramétrisé au moyen d'une temporisation, la valeur par défaut sera utilisée. Les deux commandes suivantes résulteront en un signal de tonalité de rappel automatique d'une durée de 6 secondes:

```
rt(to=6000)
rt(to(6000))
```

Des signaux différents peuvent conduire à la définition de paramètres de signal supplémentaires.

Les paramètres de signal seront placés entre des parenthèses, comme dans l'exemple hypothétique suivant:

```
S: display(10/14/17/26, "555 1212", CableLabs)
```

Lorsque plusieurs signaux sont demandés, leurs codes sont séparés par des virgules, comme indiqué ci-après:

```
S: signal1, signal2
```

A.3.2.2.11 Paramètre ObservedEvents

Les paramètres ObservedEvents fournissent la liste des événements qui ont été observés. Les codes d'événement sont les mêmes que ceux qui sont utilisés dans la demande NotificationRequest. Lorsqu'un événement est détecté et observé dans une connexion, il permettra d'identifier la connexion dans laquelle il a été détecté au moyen de la syntaxe "@<connection>". Des exemples d'événements observés sont donnés ci-après:

```
O: ma@A43B81
O: ft
O: IT/ft
O: IT/ft, IT/mt
```

A.3.2.2.12 Paramètre RequestedInfo

Le paramètre RequestedInfo contient une liste de codes de paramètre séparés par des virgules, comme défini dans la section sur les lignes de paramètre – Le paragraphe A.2.3.8 donne une liste des paramètres qui peuvent faire l'objet d'un audit. Les valeurs du Tableau A.10 sont également prises en charge:

Tableau A.10/J.171 – Valeurs du paramètre RequestedInfo prises en charge

Paramètre RequestedInfo	Code
LocalConnectionDescriptor	LC
RemoteConnectionDescriptor	RC

Si l'on souhaite, par exemple, soumettre à un audit les valeurs des paramètres NotifiedEntity, RequestIdentifier, RequestedEvents, SignalRequests, DetectEvents, EventStates, LocalConnectionDescriptor et RemoteConnectionDescriptor, les valeurs du paramètre RequestedInfo seront les suivantes:

```
F: N, X, R, S, T, ES, LC, RC
```

La demande de capacités, pour la commande AuditEndpoint, est codée au moyen du code de paramètre "A" comme dans l'expression suivante:

```
F: A
```

A.3.2.2.13 Paramètre QuarantineHandling

Le paramètre QuarantineHandling contient le mot-clé "process" ou "discard" pour indiquer le traitement des événements de quarantaine, à savoir:

```
Q: process
```

A.3.2.2.14 Paramètre DetectEvents

Le paramètre DetectEvents est codé au moyen d'une liste d'événements séparés par des virgules, tels que par exemple:

```
T: ft, mt
```

Il convient de noter qu'aucune mesure ne peut être associée aux événements.

A.3.2.2.15 Paramètre EventStates

Le paramètre EventStates est codé au moyen d'une liste d'événements séparés par des virgules, tels que par exemple:

```
ES: MO/rlc
```

Il convient de noter qu'aucune mesure ne peut être associée aux événements.

A.3.2.2.16 Paramètre RestartMethod

Le paramètre RestartMethod est codé au moyen de l'un des mots-clés "graceful", "forced", "restart" ou "disconnected", tels que par exemple:

```
RM: restart
```

A.3.2.2.17 Paramètre VersionSupported

Le paramètre VersionSupported est codé au moyen d'une liste de versions prises en charge, séparées par des virgules, telles que par exemple:

```
VS: MGCP 1.0, MGCP 1.0 TGCP 1.0
```

A.3.3 Formats d'en-tête de réponse

L'en-tête de réponse est composé d'une ligne de réponse suivie en option d'en-têtes qui codent les paramètres de réponse.

La ligne de réponse commence par un code de réponse qui est une valeur numérique à trois chiffres. Ce code est suivi d'un blanc, d'un identificateur de transaction, et d'un commentaire en option précédé d'un blanc, comme par exemple dans l'expression suivante:

```
200 1201 OK
```

Le Tableau A.11 résume les paramètres de réponse qui doivent obligatoirement ou facultativement figurer dans un en-tête de réponse, en fonction de la commande qui a déclenché la réponse, en supposant que la commande a réussi. Le lecteur est toutefois prié d'examiner mieux les différentes définitions des commandes parce que le présent tableau ne donne qu'un résumé des informations. La lettre M signifie obligatoire, O facultatif et F interdit.

Tableau A.11/J.171 – Association des paramètres avec les réponses de commande

Nom du paramètre	CRCX	MDCX	DLCX	RQNT	NTFY	AUEP	AUCX	RSIP
ResponseAck[26]	O[a)]	O[a)]	O[a)]	O[a)]	O[a)]	O [a)]	O[a)]	O[a)]
CallId	F	F	F	F	F	F	O	F
ConnectionId	M	F	F	F	F	O	F	F
RequestIdentifier	F	F	F	F	F	O	F	F
LocalConnectionOptions	F	F	F	F	F	O	O	F
ConnectionMode	F	F	F	F	F	F	O	F
RequestedEvents	F	F	F	F	F	O	F	F
SignalRequests	F	F	F	F	F	O	F	F
NotifiedEntity	F	F	F	F	F	O	O	O
ReasonCode	F	F	F	F	F	F	F	F
ObservedEvents	F	F	F	F	F	O	F	F
ConnectionParameters	F	F	O	F	F	F	O	F
Specific Endpoint ID	O	F	F	F	F	O	F	F
MaxEndPointIds	F	F	F	F	F	F	F	F
NumEndPoints	F	F	F	F	F	O	F	F
RequestedInfo	F	F	F	F	F	F	F	F
QuarantineHandling	F	F	F	F	F	F	F	F
DetectEvents	F	F	F	F	F	O	F	F
EventStates	F	F	F	F	F	O	F	F
RestartMethod	F	F	F	F	F	F	F	F
RestartDelay	F	F	F	F	F	F	F	F
Capabilities	F	F	F	F	F	O	F	F
VersionSupported	F	F	F	F	F	O	F	O
LocalConnection Descriptor	M	O	F	F	F	F	O	F
RemoteConnection Descriptor	F	F	F	F	F	F	O	F

[a)] Le paramètre ResponseAck NE DOIT PAS être utilisé avec des réponses autres que la réponse finale émise après une réponse provisoire en ce qui concerne la transaction en question. Dans ce cas, la présence du paramètre ResponseAck DOIT déclencher un message d'accusé de réception de réponse – Il ne sera pas tenu compte des valeurs ResponseAck fournies.

Les paramètres de réponse sont décrits pour chaque commande dans les sections suivantes.

[26] Le paramètre responseAck ne figure pas au A.2.3 parce que les identificateurs de transaction n'apparaissent pas dans notre exemple d'interface API. Les responsables chargés de l'implémentation peuvent choisir une approche différente.

A.3.3.1 Commande CreateConnection

Dans le cas d'un message CreateConnection, la ligne de réponse est suivie d'un paramètre identificateur de connexion contenant une réponse de réussite (code 200). Un paramètre LocalConnectionDescriptor est en outre transmis avec une réponse positive. Il est codé au moyen d'une "description de session", telle qu'elle est définie au A.3.4. Il est séparé de l'en-tête de réponse par un interligne, à savoir:

```
200 1204 OK
I: FDE234C8

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 96
a=rtpmap:96 G726-32/8000
```

Lorsqu'une réponse provisoire a été donnée précédemment, la réponse finale peut en outre contenir le paramètre accusé de réception de réponse, comme dans ce qui suit:

```
200 1204 OK
K:
I: FDE234C8

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 96
a=rtpmap:96 G726-32/8000
```

Il est accusé réception de la réponse finale au moyen du paramètre accusé de réception de réponse:

```
000 1204
```

A.3.3.2 Commande ModifyConnection

Dans le cas d'un message ModifyConnection de réussite, la ligne de réponse est suivie d'un paramètre LocalConnectionDescriptor, lorsque la modification a conduit à modifier les paramètres de session (le seul changement du mode de connexion ne modifie pas les paramètres de session, par exemple). Ce paramètre est codé au moyen d'une "description de session", telle qu'elle est définie au A.3.4. Il est séparé de l'en-tête de réponse par un interligne.

```
200 1207 OK

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 0

Lorsqu'une réponse provisoire a été donnée précédemment, la réponse finale peut
en outre contenir le paramètre accusé de réception de réponse, comme dans ce qui
suit:

526 1207 No bandwidth
K:
```

Il est accusé réception de la réponse finale au moyen du paramètre accusé de réception de réponse:

```
000 1207 OK
```

A.3.3.3 Commande DeleteConnection

En fonction de la version du message DeleteConnection, la ligne de réponse peut être suivie par une ligne de paramètre Paramètres de connexion, comme défini au A.3.2.2.5.

```
250 1210 OK
P: PS=1245, OS=62345, PR=780, OR=45123, PL=10, JI=27, LA=48
```

A.3.3.4 Commande NotificationRequest

La réponse à une commande NotificationRequest ne contient aucun paramètre de réponse supplémentaire.

A.3.3.5 Commande Notify

La réponse à une commande Notify ne contient aucun paramètre de réponse supplémentaire.

A.3.3.6 Commande AuditEndpoint

Dans le cas d'une commande AuditEndpoint, la ligne de réponse peut être suivie des informations pour chacun des paramètres demandés – Chaque paramètre figurera sur une ligne distincte. Les paramètres pour lesquels aucune valeur concrète n'existe seront quand-même fournis. Tout nom local d'extrémité "prolongé" par un caractère de remplacement figurera sur une ligne distincte au moyen du code de paramètre "SpecificEndpointId", par exemple:

```
200 1200 OK
Z: ds/ds1-1/1@tgw.whatever.net
Z: ds/ds1-1/2@tgw.whatever.net
ZN: 24
```

ou:

```
200 1200 OK
A: a:PCMU;G728, p:10-100, e:on, s:off, t:1, v:IT,
     m:sendonly;recvonly;sendrecv;inactive
A: a:G729A; p:30-90, e:on, s:on, t:1, v:MT,
     m:sendonly;recvonly;sendrecv;inactive
```

A.3.3.7 Commande AuditConnection

Dans le cas d'une commande AuditConnection, la réponse peut être suivie des informations pour chacun des paramètres demandés. Les paramètres pour lesquels aucune valeur concrète n'existe seront quand-même fournis. Les descripteurs de connexion figureront toujours en dernière position et chacun sera précédé d'un interligne, comme par exemple:

```
200 1203 OK
C: A3C47F21456789F0
N: [128.96.41.12]
L: p:10, a:PCMU;G728
M: sendrecv
P: PS=622, OS=31172, PR=390, OR=22561, PL=5, JI=29, LA=50

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 1296 RTP/AVP 96
a=rtpmap:96 G726-32/8000
```

Si aussi bien un descripteur de connexion local que distant est fourni, le descripteur local sera le premier des deux. Lorsqu'un descripteur de connexion est demandé, mais qu'il n'existe pas pour la connexion faisant l'objet d'un audit, ce descripteur figurera seulement dans le champ destiné à la version du protocole SDP.

A.3.3.8 Commande RestartInProgress

La réponse à une commande RestartInProgress peut comprendre le nom d'un autre contrôleur MGC à contacter, par exemple lorsque le contrôleur MGC réoriente l'extrémité vers un autre contrôleur MGC comme dans ce qui suit:

```
521 1204 Redirect
N: MGC-1@whatever.net
```

A.3.4 Codage de la description de session

La description de session est codée conformément au protocole de description de session (SDP, *session description protocol*); toutefois les passerelles de jonction peuvent faire certaines hypothèses simplificatrices concernant la description de session, comme spécifié dans ce qui suit. Il convient de noter que les descriptions de session sont sensibles à la casse, suivant le document IETF RFC 2327.

L'utilisation du protocole SDP dépend du type de session, tel qu'il est spécifié dans le paramètre "media". Actuellement la Recommandation TGCP ne prend en charge que le média de type "audio".

A.3.4.1 Utilisation du service audio selon le protocole SDP

Dans une passerelle destinée aux communications téléphoniques, ne doivent être décrites que les sessions où est employé un seul média, le média audio. Les paramètres du protocole SDP qui sont à prendre en considération pour les applications audio téléphoniques sont spécifiés ci-après. La passerelle de jonction DOIT prendre en charge les descriptions de session qui sont conformes à ces règles et respectent l'ordre suivant:

1) le profil du protocole SDP présenté ci-après;

2) le document IETF RFC 2327 (SDP, protocole de description de session).

Le profil du protocole SDP qui est donné décrit l'emploi du protocole de description de session dans le cadre du protocole TGCP. On trouvera la description générale et l'explication des différents paramètres dans le document IETF RFC 2327, mais ci-dessous sont détaillées quelles valeurs les extrémités conformes au protocole TGCP doivent fournir pour ces champs (envoi) et ce que ces extrémités doivent faire avec les valeurs fournies ou non fournies pour ces champs (réception).

Tout paramètre non spécifié ci-après NE DEVRAIT PAS être fourni par une extrémité conforme au protocole TGCP, et si un tel paramètre était reçu, il DEVRAIT être laissé à l'écart.

A.3.4.1.1 Paramètre version du protocole (v=)

```
v=<version>
v=0
```

Envoi: ce champ DOIT être fourni conformément au document IETF RFC 2327 (à savoir v=0).

Réception: ce champ DOIT être fourni conformément au document IETF RFC 2327.

A.3.4.1.2 Paramètre origine (o=)

Le champ correspondant à l'origine (o=) est composé de 6 sous-champs dans le document IETF RFC 2327:

```
o=<username> <session-ID> <version> <network-type> <address-type> <address>
o=-          2987933615   2987933615 IN           IP4            A3C47F2146789F0
```

Username (nom d'utilisateur)

Envoi: le tiret DOIT être employé comme nom d'utilisateur lorsque la confidentialité est demandée. Le tiret DEVRAIT être utilisé dans les autres cas.[27]

Réception: ce champ DEVRAIT être laissé à l'écart.

Session-ID (identificateur de session)

Envoi: ce champ DOIT être conforme au document IETF RFC 2327 afin de permettre l'interfonctionnement avec des clients sur réseaux non IPCablecom.

Réception: ce champ DEVRAIT être laissé à l'écart.

Version

Envoi: ce champ est conforme au document IETF RFC 2327.

Réception: ce champ DEVRAIT être laissé à l'écart.

Network Type (type de réseau)

Envoi: le type "IN" DOIT être utilisé.

Réception: ce champ DEVRAIT être laissé à l'écart.

Address Type (type d'adresse)

Envoi: le type "IP4" DOIT être utilisé.

Réception: ce champ DEVRAIT être laissé à l'écart.

Address (adresse)

Envoi: ce champ DOIT être conforme au document IETF RFC 2327 afin de permettre l'interfonctionnement avec des clients sur réseaux non IPCablecom.

Réception: ce champ DOIT être laissé à l'écart.

A.3.4.1.3 Paramètre nom de session (s=)

```
s=<session-name>
s=-
```

Envoi: le tiret DOIT être employé comme nom de session.

Réception: ce champ DOIT être laissé à l'écart.

A.3.4.1.4 Paramètre information relative à la session et au média (i=)

```
i=<session-description>
```

Envoi: pour le protocole TGCP, ce champ NE DOIT PAS être employé.

Réception: ce champ DOIT être laissé à l'écart.

A.3.4.1.5 Paramètre URI (u=)

```
u= <URI>
```

Envoi: pour le protocole TGCP, ce champ NE DOIT PAS être employé.

Réception: ce champ DOIT être laissé à l'écart.

---

[27] Puisque les extrémités conformes au protocole TGCP ne savent pas quand la confidentialité est demandée, elles DEVRAIENT toujours employer un tiret.

A.3.4.1.6 Paramètres adresse du courrier électronique et numéro de téléphone (e=, p=)

```
e=<e-mail-address>
p=<phone-number>
```

Envoi: pour le protocole TGCP, ce champ NE DOIT PAS être employé.

Réception: ce champ DOIT être laissé à l'écart.

A.3.4.1.7 Paramètre données de connexion (c=)

Le paramètre données de connexion est composé de 3 sous-champs:

```
c=<network-type>   <address-type>     <connection-address>
c=IN               IP4                10.10.111.11
```

Network Type (type de réseau)

Envoi: le type "IN" DOIT être employé.

Réception: le type "IN" DOIT être présent.

Address Type (type d'adresse)

Envoi: le type "IP4" DOIT être employé

Réception: le type "IP4" DOIT être présent.

Connection Address (adresse de connexion)

Envoi: ce champ DOIT être rempli au moyen d'une adresse IP destinée à la transmission de point à point où l'application recevra le flux média. En conséquence, la durée de vie NE DOIT PAS être présente et le "nombre d'adresses" NE DOIT PAS être présent non plus. Le champ NE DOIT PAS être rempli au moyen d'un nom de domaine entièrement spécifié au lieu d'une adresse IP. Une adresse non nulle spécifie aussi bien l'adresse de l'envoyeur que celle du receveur pour le ou les flux médias sur lesquels elle porte.

Réception: une adresse IP destinée à la transmission de point à point ou un nom de domaine entièrement spécifié DOIT être présent. Une adresse non nulle spécifie aussi bien l'adresse de l'envoyeur que celle du receveur pour le ou les flux médias sur lesquels elle porte.

A.3.4.1.8 Paramètre largeur de bande (b=)

```
b=<modifier> : <bandwidth-value>
b=AS : 64
```

Envoi: les informations concernant la largeur de bande sont facultatives dans le protocole SDP, mais elles DEVRAIENT toujours être présentes[28]. Lorsqu'un paramètre rtpmap ou qu'un codec mal connu[29] est employé, les informations concernant la largeur de bande DOIVENT être employées.

Réception: les informations concernant la largeur de bande DEVRAIENT être présentes. Si un modificateur de largeur de bande n'est pas présent, le récepteur DOIT attribuer aux codecs bien connus des valeurs de largeur de bande par défaut raisonnables.

Modifier (modificateur)

Envoi: le type "AS" DOIT être employé.

Réception: le type "AS" DOIT être présent.

---

[28] Si ce champ n'est pas employé, le contrôleur de passerelle pourrait interdire la largeur de bande appropriée.

[29] Un codec mal connu est un codec qui n'est pas défini dans la Rec. UIT-T J.161 relative au codec IPCablecom.

Bandwith Value (largeur de bande)

Envoi: le champ DOIT être rempli au moyen de la spécification relative à la largeur de bande maximale du flux média en kilobits par seconde.

Réception: la spécification relative à la largeur de bande maximale du flux média en kilobits par seconde DOIT être présente.

A.3.4.1.9 Paramètres temps, intervalles de répétition et fuseaux horaires (t=, r=, z=)

```
t=<start-time><stop-time>
t=36124033         0
r=<repeat-interval> <active-duration> <list-of-offsets-from-start-time>
z=<adjustment-time> <offset>
```

Envoi: le temps DOIT être présent; le temps de démarrage PEUT être zéro, mais DEVRAIT être le temps effectif, et le temps d'arrêt DEVRAIT être zéro. Les intervalles de répétition et les fuseaux horaires NE DEVRAIENT PAS être employés, et s'ils le sont, il faudrait que cela soit en conformité avec le document IETF RFC 2327.

Réception: si l'un de ces champs était présent, il DEVRAIT être laissé à l'écart.

A.3.4.1.10 Paramètre clés de chiffrement

```
k=<method>
k=<method> : <encryption-keys>
```

Les services de sécurité pour les réseaux IPCablecom sont définis dans la Rec. UIT-T J.170. Ceux qui sont spécifiés pour les protocoles RTP et RTCP ne sont pas conformes à ceux des documents IETF RFC 1889, IETF RFC 1890 et IETF RFC 2327. Dans l'intérêt de l'interfonctionnement avec des dispositifs non IPCablecom, le paramètre "k" ne sera donc pas employé pour acheminer des paramètres de sécurité.

Envoi: ce champ NE DOIT PAS être employé.

Réception: ce champ DEVRAIT être laissé à l'écart.

A.3.4.1.11 Paramètre attributs (a=)

```
a=<attribute> : <value>
a=rtpmap : <payload type> <encoding name>/<clock rate> [/<encoding parameters>]
a=rtpmap : 0                              PCMU / 8000
a=X-pc-codecs: <alternative 1> <alternative 2> ...
a=X-pc-secret: <method>:<encryption key>
a =X-pc-csuites-rtp: <alternative 1> <alternative 2> ...
a =X-pc-csuites-rtcp: <alternative 1> <alternative 2> ...
a =X-pc-spi-rtcp: <value>
a =X-pc-bridge: <number-ports>
a=<attribute>
a=recvonly
a=sendrecv
a=sendonly
a= ptime
```

Envoi: une ou plusieurs lignes d'attribut "a" spécifié ci-après PEUVENT être présentes. Une ligne d'attribut non spécifié ci-après NE DEVRAIT PAS être employée.

Réception: une ou plusieurs lignes d'attribut "a" spécifié ci-après PEUVENT être présentes et DOIVENT dès lors être mises à exécution. Les lignes d'attribut "a" non spécifié ci-après peuvent être présentes mais DOIVENT être laissées à l'écart.

rtpmap

Envoi: lorsqu'il est employé, ce champ DOIT l'être en conformité avec le document IETF RFC 2327. Il PEUT être employé pour des codecs bien connus ainsi que pour des codecs mal connus. Les noms de codage employés sont donnés dans une Recommandation IPCablecom distincte (voir les Recs. UIT-T J.161 et J.170).

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2327.

X-pc-codecs

Envoi: ce champ contient une liste de codecs de remplacement que l'extrémité est en mesure d'employer pour cette connexion. La liste est rangée selon un ordre de préférence décroissant, à savoir le codec de remplacement qui est le préféré figure en tête de liste. Un codec est codé d'une manière qui est semblable au "nom de codage" dans le paramètre rtpmap.

Réception: ce champ achemine une liste de codecs que l'extrémité distante est en mesure d'employer pour cette connexion. Les codecs NE DOIVENT PAS être employés avant d'être signalés au moyen d'une ligne de média (m=).

X-pc-secret

Envoi: ce champ contient un code secret de bout en bout destiné à être employé pour la sécurité dans les protocoles RTP et RTCP. Le code secret est codé d'une manière qui est semblable au paramètre clé de chiffrement (k=) dans le document IETF RFC 2327, avec les contraintes suivantes:

la clé de chiffrement NE DOIT PAS contenir une suite de chiffrement, mais seulement une phrase de passe;

le champ <method> spécifiant le codage de la phrase de passe DOIT être en "clair" ou en "base64", comme défini dans le document IETF RFC 2045, sauf en ce qui concerne la longueur maximale de ligne qui n'est pas spécifiée ici. La méthode en "clair" NE DOIT PAS être employée si le code secret contient des caractères qui sont interdits dans le protocole SDP.

Réception: ce champ achemine le code secret de bout en bout destiné à être employé pour la sécurité dans les protocoles RTP et RTCP.

X-pc-csuites-rtp
X-pc-csuites-rtcp

Envoi: le champ contient une liste de suites de chiffrement que l'extrémité est en mesure d'employer pour cette connexion (respectivement pour les protocoles RTP et RTCP). La suite de chiffrement qui figure en tête de liste est celle que l'extrémité est censée employer concrètement. Les suites de chiffrement restantes dans la liste représentent des suites de remplacement rangées par ordre de préférence décroissant, à savoir la suite de remplacement qui est préférée est en deuxième position dans la liste. Une suite de chiffrement est codée comme il est spécifié ci-après:

ciphersuite = [AuthenticationAlgorithm] "/" [EncryptionAlgorithm]

AuthenticationAlgorithm = 1*(ALPHA / DIGIT / "-" / "_")

EncryptionAlgorithm = 1*(ALPHA / DIGIT / "-" / "_")

où les grandeurs ALPHA et DIGIT sont définies dans le document IETF RFC 2234. Des blancs ne sont pas admis dans une suite de chiffrement. L'exemple suivant illustre l'emploi d'une suite de chiffrement:

```
62/51
```

La liste des suites de chiffrement actuellement définie est donnée dans la Rec. UIT-T J.170.

Réception: ce champ achemine une liste de suites de chiffrement que l'extrémité distante est en mesure d'employer pour cette connexion. Toute suite de chiffrement autre que la première de la liste ne peut être employée avant d'être signalée au moyen d'une nouvelle ligne de suite de chiffrement avec la suite de chiffrement souhaitée en première position.

X-pc-spi-rtcp

Envoi: ce champ contient un indice de paramètre de sécurité (SPI, *security parameter index*) IPSec à utiliser au cours de l'envoi de paquets conformes au protocole RTCP à l'extrémité pour le flux média concerné. L'indice SPI est un identificateur à 32 bits codé au moyen d'une chaîne à 8 caractères hexadécimaux au plus. Ce champ DOIT être fourni lorsque la sécurité relative au protocole RTCP est employée.

Réception: ce champ achemine l'indice SPI IPSec à employer lors de l'envoi de paquets conformes au protocole RTCP utilisant la sécurité IPSec. Ce champ DOIT être présent lorsque la sécurité relative au protocole RTCP est employée.

X-pc-bridge

Envoi: les extrémités conformes au protocole TGCP NE DOIVENT PAS employer cet attribut.

Réception: si les extrémités conformes au protocole TGCP reçoivent cet attribut, elles DOIVENT le laisser à l'écart.

recvonly

Envoi: ce champ DOIT être employé en conformité avec le document IETF RFC 2543.

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2543.

sendrecv

Envoi: ce champ DOIT être employé en conformité avec le document IETF RFC 2543.

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2543.

sendonly

Envoi: ce champ DOIT être employé en conformité avec le document IETF RFC 2543, sauf que la valeur de l'adresse IP et du numéro de port NE DOIT PAS être nulle.

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2543.

ptime

Envoi: ce champ DEVRAIT toujours être fourni, et, lorsqu'il est employé, il DOIT l'être en conformité avec le document IETF RFC 2327. Lorsqu'un paramètre rtpmap ou qu'un codec mal connu est employé, le paramètre ptime DOIT être fourni.

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2327. Lorsque le paramètre "ptime" est présent, l'adaptateur MTA DOIT l'employer dans le calcul des réserves de qualité de service. S'il n'est pas présent, l'adaptateur MTA DOIT attribuer aux codecs bien connus des valeurs par défaut raisonnables.

A.3.4.1.12 Paramètre annonces de média (m=)

Le paramètre annonces de média (m=) est composé de 3 sous-champs:

```
M=<media> <port>   <transport>   <format>
M=audio       3456      RTP/AVP        0
```

Media (média)

Envoi: le type de média "audio" DOIT être employé.

Réception: le type reçu DOIT être le type "audio".

Port

Envoi: ce champ DOIT être rempli conformément au document IETF RFC 2327. Le port spécifié est le port de réception, le flux étant unidirectionnel ou bidirectionnel. Le port d'envoi peut être différent.

Réception: ce champ DOIT être employé en conformité avec le document IETF RFC 2327. Le port spécifié est le port de réception. Le port d'envoi peut être différent.

Transport

Envoi: le protocole de transport "RTP/AVP" DOIT être employé.

Réception: le protocole de transport DOIT être le protocole "RTP/AVP".

Media Formats (formats du média)

Envoi: le type de média approprié tel qu'il est défini dans le document IETF RFC 2327 DOIT être employé.

Réception: ce champ est conforme au document IETF RFC 2327.

A.3.5 Transmission par l'intermédiaire du protocole datagramme d'utilisateur

A.3.5.1 Livraison fiable de messages

Les messages conformes aux protocoles MGCP sont transmis par l'intermédiaire du protocole datagramme d'utilisateur (UDP, *user datagram protocol*). Les commandes sont envoyées à l'une des adresses IP qui sont définies dans le système de dénomination de domaine (DNS, *domain name system*) pour l'extrémité ou le contrôleur MGC spécifié. Les réponses sont renvoyées à l'adresse émettrice de la commande. Toutefois, il convient de noter que la réponse peut en fait provenir d'une adresse IP autre que celle à laquelle la commande a été envoyée.

Lorsque aucun port n'est mis à la disposition de l'extrémité[30], les commandes devraient être envoyées au port MGCP par défaut, 2427.

Les messages MGCP, acheminés par l'intermédiaire du protocole UDP, peuvent subir des pertes. En l'absence d'une réponse en temps utile, les commandes sont reproduites. Les entités du protocole MGCP sont censées garder en mémoire une liste des réponses envoyées aux transactions récentes, c'est-à-dire une liste de toutes les réponses envoyées pendant les dernières secondes Tt_{hist}, ainsi qu'une liste des transactions qui sont réellement exécutées. Les identificateurs de transaction des commandes entrantes sont comparés aux identificateurs de transaction des dernières réponses. Si une concordance est établie, l'entité du protocole MGCP n'exécute pas la transaction, mais reproduit simplement la réponse. Si aucune concordance n'est établie, elle examine la liste des transactions effectivement en cours d'exécution. Si une concordance est établie, elle n'exécutera pas la transaction, mais la laissera simplement à l'écart.

L'entité demandeuse a la charge de fournir des temporisations appropriées pour toutes les commandes en suspens et de réessayer les commandes lorsque les temporisations ont été dépassées. Une stratégie de retransmission est spécifiée au A.3.5.2.

En outre, lorsque des commandes reproduites ne réussissent pas à obtenir de réponse, l'entité de destination est supposée être non disponible. L'entité demandeuse a la charge de rechercher des services excédentaires ou de libérer des connexions existantes ou en suspens, comme spécifié au A.2.4.

---

[30] On peut attribuer à chaque extrémité une adresse et un port de contrôleur MGC distinct.

A.3.5.2 Stratégie de retransmission

La présente Recommandation évite de spécifier de quelconques valeurs permanentes pour les temporisateurs de retransmission, parce que ces valeurs sont généralement fonction du réseau. Normalement, les temporisateurs de retransmission devraient évaluer la temporisation en mesurant le temps qui s'écoule entre l'envoi d'une commande et le renvoi d'une réponse. Au minimum, les passerelles de jonction DOIVENT implémenter une stratégie de retransmission utilisant une temporisation exponentielle avec des valeurs initiale et maximale configurables pour les temporisateurs de retransmission.

Les passerelles de jonction DEVRAIENT employer l'algorithme implémenté dans le protocole TCP-IP, qui utilise deux variables (voir, par exemple, l'article *TCP/IP Illustrated, Volume 1, The Protocols*).

Le délai de réponse moyen (AAD, *average response delay*), évalué à l'aide d'une moyenne lissée exponentiellement des délais observés,

- l'écart moyen (ADEV, *average deviation*), évalué à l'aide d'une moyenne lissée exponentiellement de la valeur absolue de la différence entre les délais observés et la moyenne actuelle.

Le temporisateur de retransmission (RTO) dans le protocole TCP est fixé à la somme du délai moyen et de N fois l'écart moyen, N étant une constante.

Après une retransmission, l'entité du protocole MGCP devrait agir de la manière suivante:

- elle devrait multiplier par deux la valeur évaluée du délai moyen, AAD;
- elle devrait calculer une valeur aléatoire, uniformément distribuée entre les valeurs correspondantes à 0,5 AAD et à AAD;
- elle devrait attribuer au temporisateur de retransmission (RTO) la valeur minimale de:
  - la somme de cette valeur aléatoire et de N fois l'écart moyen,
  - RTO_{max}, dont la valeur par défaut est de 4 secondes.

L'effet de cette procédure est double. Parce qu'elle comporte une composante dont la croissance est exponentielle, elle ralentira automatiquement le flux de messages en cas d'encombrement, en fonction des besoins de la communication en temps réel. Parce ce qu'elle comporte une composante aléatoire, elle rompra la synchronisation possible entre les notifications déclenchées par le même événement extérieur.

La valeur initiale qui est utilisée pour le temporisateur de retransmission est de 200 millisecondes par défaut tandis que la valeur maximale s'élève à 4 secondes par défaut. Ces valeurs par défaut peuvent être modifiées par le processus de configuration.

A.3.6 Accompagnement

Dans certains cas, un contrôleur MGC souhaiterait envoyer plusieurs messages en même temps à une ou plusieurs extrémités d'une passerelle et vice versa. Lorsque plusieurs messages doivent être envoyés dans les mêmes paquets conformes au protocole UDP, ils sont séparés par une ligne de texte qui comporte un unique point, comme dans l'exemple suivant:

```
200 2005 OK
.
DLCX 1244 ds/ds1-2/2@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: FDE234C8
```

Les messages joints DOIVENT être traités comme s'ils avaient été reçus dans des datagrammes différents; mais, si un message (commande ou réponse) doit être retransmis, le datagramme entier DOIT être retransmis, non le message manquant seulement. Les messages individuels du datagramme DOIVENT être traités dans l'ordre, en commençant par le premier message.

Les erreurs qui se produisent dans un message qui accompagne d'autres messages, NE DOIVENT PAS avoir d'effet sur les autres messages qui sont reçus dans ce paquet – Chaque message étant traité isolément.

A.3.7 Identificateurs de transaction et prise de contact à trois

Les identificateurs de transaction sont des nombres entiers compris entre 1 et 999 999 999. Les contrôleurs MGC peuvent décider d'employer un ensemble de nombres propre à chaque passerelle qu'ils administrent, ou d'employer le même ensemble de nombres pour toutes les passerelles qui font partie d'un certain groupe donné. Les contrôleurs MGC peuvent décider de répartir la charge de la gestion d'une grande passerelle en plusieurs processus indépendants. Ces processus se partageront le même ensemble de nombres pour les identificateurs de transaction. Ce partage peut s'effectuer de plusieurs façons, telles que celle qui consiste en l'attribution centralisée d'identificateurs de transaction, ou en la préattribution à différents processus d'ensembles d'identificateurs, ne se chevauchant pas. Les implémentations du partage DOIVENT garantir que des identificateurs de transaction uniques soient attribués à toutes les transactions émanant d'un contrôleur MGC et envoyées pendant une durée de Tt_{hist} secondes à une passerelle donnée. Les passerelles peuvent détecter facilement les transactions doubles au moyen d'un simple examen de l'identificateur de transaction.

Le paramètre accusé de réception de réponse peut se retrouver dans toute commande. Il transporte un ensemble "d'intervalles d'identificateurs de transaction transaction-id confirmés" pour les réponses finales reçues – Les réponses provisoires NE DOIVENT PAS être confirmées.

Les passerelles conformes au protocole MGCP peuvent choisir de supprimer les copies des réponses aux transactions dont l'identificateur figure dans les "intervalles d'identificateurs de transaction transaction-id confirmés" reçus dans un message, mais le fait que la transaction ait été exécutée DOIT encore être conservé pendant Tt_{hist} secondes. Par ailleurs, lorsqu'un message d'accusé de réception de réponse[31] est reçu, la réponse dont il accuse réception peut être supprimée. Les passerelles devraient, sans le communiquer expressément, ignorer d'autres commandes provenant de ce contrôleur MGC lorsque l'identificateur de transaction transaction-id appartient à ces intervalles, et que la réponse a été émise il y a moins de Tt_{hist} secondes.

Soient $term_{new}$ et $term_{old}$, le nom d'extrémité endpoint-name dans une nouvelle commande cmd_{new} et dans une ancienne commande cmd_{old}, respectivement. Les identificateurs de transaction transaction-id à confirmer dans la commande cmd_{new} DEVRAIENT alors être déterminés au moyen des éléments suivants:

1) si le nom d'extrémité $term_{new}$ ne contient aucun caractère de remplacement:

   a) réponses non confirmées aux anciennes commandes où le nom d'extrémité $term_{old}$ est le même que le nom d'extrémité $term_{new}$;

   b) en option, une ou plusieurs réponses non confirmées où le nom d'extrémité $term_{old}$ contient le caractère de remplacement "un quelconque", et le nom d'extrémité endpoint-name renvoyé dans la réponse est le nom d'extrémité $term_{new}$;

[31] A distinguer d'une commande contenant un paramètre accusé de réception de réponse.

c) en option, une ou plusieurs réponses non confirmées où le nom d'extrémité $term_{old}$ contient le caractère de remplacement "tous", et le nom d'extrémité $term_{new}$ est couvert par le caractère de remplacement dans le nom d'extrémité $term_{old}$;

d) en option, une ou plusieurs réponses non confirmées où le nom d'extrémité $term_{old}$ contient le caractère de remplacement "un quelconque", aucun nom d'extrémité endpoint-name n'a été renvoyé, et le nom d'extrémité $term_{new}$ est couvert par le caractère de remplacement dans le nom d'extrémité $term_{old}$.

2) Si le nom d'extrémité $term_{new}$ contient le caractère de remplacement "tous":

a) en option, une ou plusieurs réponses non confirmées où le nom d'extrémité $term_{old}$ contient le caractère de remplacement "tous", et le nom d'extrémité $term_{new}$ est couvert par le caractère de remplacement dans le nom d'extrémité $term_{old}$.

3) Si le nom d'extrémité $term_{new}$ contient le caractère de remplacement "un quelconque":

a) en option, une ou plusieurs réponses non confirmées où le nom d'extrémité $term_{old}$ contient le caractère de remplacement "tous, et le nom d'extrémité $term_{new}$ est couvert par le caractère de remplacement dans le nom d'extrémité $term_{old}$ lorsque le caractère de remplacement "un quelconque" dans le nom d'extrémité $term_{new}$ a été remplacé par le caractère de remplacement "tous".

Une réponse donnée NE DEVRAIT PAS être confirmée dans deux messages distincts.

Les exemples suivants illustrent l'emploi de ces règles:

- si le nom d'extrémité $term_{new}$ est "ds/ds1-2/1" et que le nom d'extrémité $term_{old}$ est "ds/ds1-2/1", l'ancienne réponse peut être confirmée au moyen de la règle 1a;
- si le nom d'extrémité $term_{new}$ est "ds/ds1-1/3" et que le nom d'extrémité $term_{old}$ est "*", l'ancienne réponse peut être confirmée au moyen de la règle 1c;
- si le nom d'extrémité $term_{new}$ est "ds/ds1-2/*" et que le nom d'extrémité $term_{old}$ est "*", l'ancienne réponse peut être confirmée au moyen de la règle 2a;
- si le nom d'extrémité $term_{new}$ est "ds/ds1-2/$" et que le nom d'extrémité $term_{old}$ est "ds/ds1-2/*", l'ancienne réponse peut être confirmée au moyen de la règle 3a.

Les valeurs des "intervalles d'identificateurs de transaction transaction-id confirmés" NE DEVRAIENT PAS être employées si plus de Tt_{hist} secondes se sont écoulées depuis que la passerelle a émis sa dernière réponse à destination de ce contrôleur MGC, ou lorsqu'une passerelle reprend l'exploitation. Dans cette situation, les commandes devraient être acceptées et traitées, sans essai d'identificateur de transaction transaction-identificateur.

En outre, une réponse NE DEVRAIT pas être confirmée lorsqu'elle a été reçue il y a plus de Tt_{hist} secondes.

Les messages qui confirment les réponses peuvent être émis et reçus en désordre. La passerelle gardera l'ensemble des identificateurs de transaction transaction-id reçues dans les commandes récentes.

A.3.8 Réponses provisoires

Dans certains cas, les temps d'achèvement des transactions peuvent être bien plus longs que dans d'autres cas. Le protocole TGCP utilise le protocole UDP comme protocole de transport et la fiabilité est assurée au moyen de retransmissions fondées sur une temporisation sélective, cette temporisation étant basée sur une évaluation de l'addition du temps aller-retour dans le réseau et du temps nécessaire à l'achèvement de la transaction. Des variations significatives des temps d'achèvement des transactions sont en conséquence problématiques lorsque l'on désire que la détection de la perte de messages soit rapide et sans surcharge excessive.

Afin de surmonter ce problème, une réponse provisoire DOIT donc être donnée, à condition que le temps nécessaire à l'achèvement de la transaction dépasse un court laps de temps donné. Cette réponse provisoire accuse réception de la commande, même si le résultat de cette commande n'est éventuellement pas encore connu, par exemple, en raison d'une réserve de ressources en suspens. A titre de recommandation, une transaction qui nécessite l'achèvement d'une communication externe, par exemple, la réserve des ressources de réseau, devrait émettre une réponse provisoire. En outre, si une double commande CreateConnection ou ModifyConnection est reçue, et que l'exécution de la transaction n'est pas encore achevée, une réponse provisoire DOIT être renvoyée.

La sémantique transactionnelle pure impliquerait que des réponses provisoires ne renvoient pas d'information autre que le fait que la transaction est effectivement exécutée, tandis qu'une démarche optimiste permettant le renvoi de certaines informations entraînerait une réduction du délai encouru par le système autrement.

Des réponses provisoires DOIVENT seulement être envoyées en réponse à une commande CreateConnection ou ModifyConnection. Afin de réduire le délai encouru par le système, un identificateur de connexion et une description de session DOIVENT faire partie de la réponse provisoire à la commande CreateConnection. Lorsqu'une description de session est renvoyée par la commande ModifyConnection, la description de session DOIT faire partie de la réponse provisoire dans ce cas également. Si la transaction est achevée avec succès, l'information renvoyée dans la réponse provisoire DOIT être reproduite dans la réponse finale. On considère qu'il s'agit d'une erreur de protocole lorsque cette information n'est pas reprise ou que des informations précédemment fournies sont modifiées dans une réponse de réussite. Si la transaction échoue, un code d'erreur est renvoyé – l'information renvoyée précédemment n'est plus valable.

Une transaction exécutant effectivement une commande CreateConnection ou ModifyConnection DOIT être annulée si une commande DeleteConnection est reçue pour cette extrémité. Dans ce cas, une réponse pour la transaction annulée DEVRAIT encore être renvoyée automatiquement, et une réponse pour la transaction annulée DOIT être renvoyée si une retransmission de la transaction annulée est détectée.

Lorsqu'une réponse provisoire est reçue, la valeur de la temporisation pour la transaction concernée DOIT être beaucoup plus élevée pour cette transaction ($Tt_{longtran}$). Le but de cette temporisation est en premier lieu de détecter une défaillance de l'extrémité. La valeur par défaut de $Tt_{longtran}$ est de 5 secondes, mais le processus de configuration peut modifier cette valeur.

Lorsque l'exécution de la transaction prend fin, la réponse finale est envoyée et la réponse provisoire maintenant obsolète est supprimée. Afin que la perte d'une réponse finale puisse rapidement être détectée, on DOIT accuser réception des réponses finales émises pour une transaction après les réponses provisoires. L'extrémité DOIT donc inclure un paramètre "ResponseAck" sans valeur dans ces réponses finales et, seulement dans ces réponses. La présence de ce paramètre dans la réponse finale déclenchera une réponse "accusé de réception de réponse" qui sera renvoyée à l'extrémité. Cette dernière réponse comportera dans l'en-tête de réponse un identificateur de transaction transaction-id de la réponse dont elle accuse réception. Sa réception est soumise à la même temporisation et aux mêmes stratégies et procédures de retransmission que les réponses aux commandes (voir A.2.4), à savoir, l'envoyeur de la réponse finale la retransmettra si "l'accusé de réception de réponse" n'est pas reçu dans les délais. Il n'est jamais accusé réception de la réponse "accusé de réception de réponse".

A.4 Sécurité

Si des entités non autorisées pouvaient utiliser le protocole MGCP, elles seraient en mesure d'établir des appels non autorisés ou d'interférer avec des appels autorisés. La sécurité ne fait pas partie intégrante du protocole MGCP. Au lieu de cela, le protocole MGCP prévoit l'existence d'une couche inférieure assurant la sécurité proprement dite.

Des spécifications et des solutions concernant la sécurité pour le protocole TGCP sont données dans la Rec. UIT-T J.170 qu'il conviendrait de consulter pour de plus amples informations.

Annexe A.A

Paquetages d'événements

La présente annexe à l'Annexe A définit un ensemble initial de paquetages d'événements pour les divers types d'extrémités actuellement définies par l'architecture IPCablecom pour les passerelles de jonction.

Chaque paquetage définit un nom de paquetage et des codes d'événement, et donne des définitions pour chacun des événements du paquetage. Les tableaux des événements ou des signaux de chaque paquetage comportent les cinq colonnes suivantes:

- **code** le code d'événement unique dans le paquetage employé pour l'événement ou le signal;
- **description** une brève description de l'événement ou du signal;
- **événement** une marque de pointage figure dans cette colonne si l'événement peut être demandé par le contrôleur MGC. Sinon, un ou plusieurs symboles suivants peuvent figurer dans la colonne:
  - **"P"** indiquant que l'événement est durable;
  - **"S"** indiquant que l'événement est un état d'événement event-state qui peut faire l'objet d'un audit;
  - **"C"** indiquant que l'événement ou le signal peut être détecté dans une connexion ou appliqué à celle-ci;
- **signal** si rien ne figure dans cette colonne pour un événement, cet événement ne peut être signalé en réponse à une commande par le contrôleur MGC. Sinon, les symboles suivants identifient le type d'événement:
  - **"OO"** signal activé/désactivé. Le signal est activé jusqu'à la commande par le contrôleur MGC de l'arrêter, et vice versa;
  - **"TO"** signal avec interruption. Le signal est activé pendant un temps donné à moins d'être supplanté par un nouveau signal. Les temporisations par défaut sont fournies. Une valeur nulle indique que la temporisation est illimitée. Le processus de configuration peut modifier ces valeurs par défaut;
  - **"BR"** signal bref. L'événement a une durée connue et courte;
- **informations supplémentaires** elles donnent des informations en supplément pour l'événement ou le signal, par exemple, la durée par défaut des signaux TO.

Sauf mention contraire, tous les événements ou les signaux sont détectés ou appliqués aux extrémités et le flux audio produit par celles-ci n'est pas transmis dans les connexions auxquelles l'extrémité peut être reliée. Le flux audio produit par des événements ou des signaux qui sont détectés dans une connexion ou appliqués à celle-ci sera toutefois transmis dans la connexion associée, quel que soit le mode de connexion.

A.A.1 Paquetage de circuits de l'ISUP

Nom du paquetage: IT

Tableau A.A.1/J.171 – Evénements et signaux du paquetage de circuits de l'ISUP

Code	Description	Evénement	Signal	Informations supplémentaires
co1	Tonalité de continuité 1	√	TO	Temporisation = 3 secondes
co2	Tonalité de continuité 2	√	TO	Temporisation = 3 secondes
ft	Tonalité de télécopie	√	–	
ld	Connexion de longue durée	C	–	
ma	Démarrage média	C	–	
mt	Tonalité de modem	√	–	
oc	Opération achevée	√	–	
of	Echec de l'opération	√	–	
ro	Tonalité de renumérotation	–	TO	Temporisation = 30 secondes
rt	Tonalité de rappel automatique	–	C, TO	Temporisation = 180 secondes
TDD	Tonalités des appareils de télécommunication pour les personnes malentendantes (TDD, *telecommunications devices for the deaf*)	√		

La définition des différents événements et signaux est donnée ci-après:

tonalité de continuité 1 (co1): une tonalité à 2 010 Hz suivant la Rec. UIT-T Q.724. Afin de se conformer aux pratiques actuelles relatives aux essais de continuité, l'événement NE DEVRAIT PAS être produit avant la suppression de la tonalité. La tonalité est de type TO – l'essai de continuité ne sera appliqué qu'au cours de périodes précises. Le processus de configuration peut modifier la valeur par défaut.

tonalité de continuité 2 (co2): une tonalité à 1 780 Hz suivant la Rec. UIT-T Q.724. Afin de se conformer aux pratiques actuelles relatives aux essais de continuité, l'événement NE DEVRAIT PAS être produit avant la suppression de la tonalité. La tonalité est de type TO – l'essai de continuité ne sera appliqué qu'au cours de périodes précises. Le processus de configuration peut modifier la valeur par défaut.

Les tonalités de continuité sont employées lorsque le contrôleur MGC souhaite procéder à un essai de continuité: les types d'essai sont au nombre de deux, à l'aide d'une tonalité simple et d'une tonalité double. L'entité lançant l'essai de continuité signale et détecte les tonalités appropriées pour le circuit concerné. Par exemple, on pourrait utiliser les messages suivants pour un essai de continuité de passage d'un circuit à 4 fils à un circuit à 2 fils:

passerelle de départ

```
RQNT 1234 ds/ds3-1/ds1-6/17@tgw1.example.net
X: AB123FE0
S: co2
R: co1
```

passerelle de terminaison

```
CRCX 1234 ds/ds1-4/7@tgw2.example.net
C: A3C47F21456789F0
L: p:10, a:PCMU
M: conttest
```

La passerelle de départ envoie le signal demandé, et attend le retour de la tonalité appropriée pour le circuit en question. Lorsqu'elle détecte cette tonalité et juge que l'essai de continuité a réussi, elle produit l'événement "co1" qui, dans l'exemple, sera notifié au contrôleur MGC. Si l'essai ne réussit pas avant l'interruption, un événement "opération achevée" sera produit, et envoyé, dans ce cas aussi, au contrôleur MGC. De même, si une erreur se produit avant l'interruption, un événement "échec de l'opération" sera produit. Les événements "oc" et "of" seront paramétrisés au moyen du nom de l'événement ou du signal dont ils font état, à savoir "co1" dans ce cas.

Tonalité de télécopie (ft): l'événement tonalité de télécopie est produit lorsqu'une communication de type télécopie est détectée – Voir, par exemple, les Rec. UIT-T T.30 ou V.21.

Connexion de longue durée (ld): la "connexion de longue durée" est détectée lorsqu'une connexion a été établie depuis plus d'une certain temps. La valeur par défaut est une heure, mais elle peut être modifiée par le processus de configuration.

L'événement peut être détecté dans une connexion. Lorsque aucune connexion n'est spécifiée, l'événement s'applique à toutes les connexions reliées à l'extrémité, quel que soit l'instant où elles ont été établies.

Démarrage média (ma): l'événement démarrage média se produit dans une connexion lorsque le premier paquet média valable[32] conforme au protocole RTP est reçu par l'intermédiaire de la connexion. Cet événement peut être employé pour synchroniser un signal local, par exemple, un rappel automatique, avec l'arrivée d'un flux média provenant d'une autre entité.

L'événement peut être détecté dans une connexion. Lorsque aucune connexion n'est spécifiée, l'événement s'applique à toutes les connexions reliées à l'extrémité, quel que soit l'instant où elles ont été établies.

Tonalités de modem (mt): l'événement tonalité de modem est produit lorsqu'une communication de type modem est détectée – voir, par exemple, la Rec. UIT-T V.8.

Opération achevée (oc): l'événement opération achevée est produit lorsque la passerelle a été priée d'appliquer un ou plusieurs signaux de type TO à l'extrémité, et qu'un ou plusieurs d'entre eux ont pris fin sans avoir été arrêtés par la détection d'un événement demandé tel que "tonalité de continuité 1". Le rapport d'achèvement peut comporter en tant que paramètre le nom du signal dont la durée de vie s'est achevée, comme dans l'expression suivante:

```
O: IT/oc(IT/co1)
```

lorsque le signal rapporté a été appliqué à une connexion, le paramètre fourni comportera également le nom de la connexion, comme dans l'expression suivante:

```
O: IT/oc(IT/rt@0A3F58)
```

lorsque l'événement opération achevée est demandé, il ne peut être paramétrisé au moyen de paramètres d'événement quelconques. Lorsque le nom du paquetage est omis, on suppose qu'il s'agit du nom par défaut.

L'événement opération achevée peut par ailleurs être produit de la manière qui est définie dans le protocole de base, par exemple, lorsqu'une commande insérée ModifyConnection s'achève avec succès, comme dans l'expression suivante[33]:

```
O: IT/oc(B/C)
```

---

[32] Lorsque les services d'authentification et d'intégrité sont employés, un paquet conforme au protocole RTP n'est considéré comme étant valable qu'une fois qu'il a passé les vérifications de sécurité.

[33] Il convient de noter l'emploi ici de "B" en tant que préfixe pour le paramètre signalé.

Echec de l'opération (of): en général, l'événement échec de l'opération peut être produit lorsque l'extrémité a été priée d'appliquer un ou plusieurs signaux du type TO à l'extrémité, et qu'un ou plusieurs d'entre eux ont échoué avant l'interruption. Le rapport d'achèvement peut comporter en tant que paramètre le nom du signal qui a échoué, comme dans l'expression suivante:

```
O: IT/of(IT/co2)
```

lorsque le signal rapporté a été appliqué à une connexion, le paramètre fourni comportera également le nom de la connexion, comme dans l'expression suivante:

```
O: IT/of(IT/rt@0A3F58)
```

lorsque l'événement échec de l'opération est demandé, les paramètres d'événement ne peuvent être spécifiés. Lorsque le nom du paquetage est omis, on suppose qu'il s'agit du nom par défaut.

L'événement échec de l'opération peut par ailleurs être produit de la manière qui est définie dans le protocole de base, par exemple, lorsqu'une commande insérée ModifyConnection échoue, comme dans l'expression suivante[33]:

```
O: IT/of(B/C(M(sendrecv(AB2354))))
```

Tonalité de renumérotation (ro): la tonalité de renumérotation, alias tonalité d'encombrement, est spécifiée dans la Rec. UIT-T E.180/Q.35.

Tonalité de rappel automatique (rt): la tonalité de rappel automatique sonore est spécifiée dans la Rec. UIT-T E.180/Q.35. Sa définition est conforme aux normes nationales relatives à la tonalité de rappel automatique, et elle PEUT être établie lors de la configuration. Le signal de rappel automatique peut être appliqué aussi bien à l'extrémité qu'à la connexion.

Tonalités des appareils de télécommunication pour malentendants (TDD): l'événement TDD est produit lorsqu'une communication de type TDD est détectée – voir la Rec. UIT-T V.18.

Appendice A.I

Combinaison des modes

Une connexion dans le cadre du protocole MGCP peut assurer le passage d'un ou de plusieurs flux médias. Ces flux sont soit entrants (en provenance d'une extrémité distante) soit sortants (produits à l'extrémité du circuit). Le paramètre "mode de connexion" fixe la direction et la production de ces flux. Lorsqu'une connexion seulement est reliée une extrémité, le mappage de ces flux est simple; l'extrémité du circuit fait passer le flux entrant à travers le circuit et produit le flux sortant à partir du signal du circuit, en fonction de paramètre mode.

Toutefois, lorsque plusieurs connexions sont reliées à une extrémité, il peut y avoir de nombreux flux entrants et sortants. Suivant le mode de connexion employé, ces flux peuvent interagir différemment les uns avec les autres et avec les flux allant vers l'extrémité ou en provenance de celle-ci.

Le Tableau A.I.1 décrit comment les différentes connexions devraient être combinées lorsqu'une ou plusieurs connexions sont "actives" en même temps. Une connection active est définie ici comme étant une connexion qui est dans l'un des modes suivants:

- "envoi/réception";
- "envoi seulement";
- "réception seulement".

Tableau A.I.1/J.171 – Regroupement des différentes connexions lorsqu'une ou plusieurs connexions sont simultanément actives

		Mode de connexion A					
		sendonly	**recvonly**	**sendrecv**	**loopback/ conttest**	**inactive**	**netwloop/ netwtest**
Mode de connexion B	**sendonly**	$A_{out}= H_{in}$ $B_{out}= H_{in}$ $H_{out}=NA$	$A_{out}=NA$ $B_{out}=H_{in}$ $H_{out}= A_{in}$	$A_{out}=H_{in}$ $B_{out}=H_{in}$ $H_{out}=A_{in}$	$A_{out}=NA$ $B_{out}=NA$ $H_{out}=cot$	$A_{out}= NA$ $B_{out}= H_{in}$ $H_{out}=NA$	$A_{out}=A_{in}$ $B_{out}= H_{in}$ $H_{out}=NA$
	recvonly		$A_{out}= NA$ $B_{out}= NA$ $H_{out}=A_{in}+B_{in}$	$A_{out}= H_{in}$ $B_{out}= NA$ $H_{out}=A_{in}+B_{in}$	$A_{out}=NA$ $B_{out}=NA$ $H_{out}=cot$	$A_{out}=NA$ $B_{out}=NA$ $H_{out}= B_{in}$	$A_{out}= A_{in}$ $B_{out}= NA$ $H_{out}= B_{in}$
	sendrecv			$A_{out}= H_{in}$ $B_{out}= H_{in}$ $H_{out}=A_{in}+B_{in}$	$A_{out}=NA$ $B_{out}=NA$ $H_{out}=cot$	$A_{out}= NA$ $B_{out}= H_{in}$ $H_{out}= B_{in}$	$A_{out}= A_{in}$ $B_{out}= H_{in}$ $H_{out}= B_{in}$
	loopback/ conttest				$A_{out}=NA$ $B_{out}=NA$ $H_{out}=cot$	$A_{out}= NA$ $B_{out}= NA$ $H_{out}= cot$	$A_{out}= NA$ $B_{out}= NA$ $H_{out}= cot$
	inactive					$A_{out}= NA$ $B_{out}= NA$ $H_{out}= NA$	$A_{out}= A_{in}$ $B_{out}= NA$ $H_{out}=NA$
	netwloop/ netwtest						$A_{out}= A_{in}$ $B_{out}= B_{in}$ $H_{out}=NA$

Les connexions en modes "bouclage en réseau", "essai de continuité en réseau" ou "inactif" ne subissent aucun effet des connexions dans les modes "actif". Les conventions suivantes sont employées dans le Tableau A.I.1:

- A_{in} est le flux média entrant en provenance de la connexion A;
- B_{in} est le flux média entrant en provenance de la connexion B;
- H_{in} est le flux média entrant en provenance de la jonction;
- A_{out} est le flux média sortant vers la connexion A;
- B_{out} est le flux média sortant vers la connexion B;
- H_{out} est le flux média sortant vers l'extrémité, où "cot" indique l'essai de continuité, que le mode soit "essai de continuité" ou "bouclage";
- NA indique l'absence de flux dans tous les cas.

Appendice A.II

Exemples de codage des commandes

Le présent appendice donne des exemples de commandes et de réponses et indique le codage effectivement employé. Toutes les commandes y sont traitées. Les commentaires figurant dans les commandes et les réponses sont facultatifs.

A.II.1 Commande NotificationRequest

Le premier exemple illustre une commande NotificationRequest qui lance un essai de continuité et cherche à le vérifier. "L'entité notifiée" pour l'extrémité est fixée par l'adresse "ca@ca1.whatever.net:5678" et le paramètre RequestIdentifier sera reproduit dans la commande Notify correspondante:

```
RQNT 1201 ds/ds1-1/2@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
N: mgc@mgc1.whatever.net:5678
X: 0123456789AC
R: co1, oc(N), of(N)
S: co1
```

la réponse indique que la transaction a réussi:

```
200 1201 OK
```

A.II.2 Commande Notify

L'exemple ci-après illustre un message Notify qui notifie la réussite d'un essai de continuité comme l'indiquent les événements observés. Puisqu'une "entité notifiée" a été spécifiée dans la commande NotificationRequest qui a déclenché la notification, elle est reproduite ici. En outre, le paramètre RequestIdentifier est également repris, afin d'assurer la corrélation entre cette commande Notify et la commande NotificationRequest qui en est à l'origine:

```
NTFY 2002 ds/ds1-1/2@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
N: mgc@mgc1.whatever.net:5678
X: 0123456789AC
O: co1
```

la réponse à la commande Notify indique que la transaction a réussi:

```
200 2002 OK
```

A.II.3 Commande CreateConnection

Le premier exemple illustre une commande CreateConnection destinée à établir une connexion à l'extrémité spécifiée. La connexion figure dans l'identificateur CallId spécifié. Le paramètre LocalConnectionOptions spécifie que le codec utilisé est donné par la loi μ de la Rec. UIT-T G.711 et que la période de mise en paquets est égale à 10 ms. Le mode de connexion est le mode "réception seulement":

```
CRCX 1204 ds/ds1-1/17@tgw2.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
L: p:10, a:PCMU
M: recvonly
```

la réponse indique que la transaction a réussi, et un identificateur de connexion pour la connexion nouvellement établie est donc inclus. Une description de session pour la nouvelle connexion est également incluse – Il convient de noter qu'elle est précédée d'un interligne.

```
200 1204 OK
I: FDE234C8

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 0
```

Le deuxième exemple illustre une commande CreateConnection contenant une demande de notification et un paramètre RemoteConnectionDescriptor:

```
CRCX 1205 ds/ds1-1/1@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
L: p:10, a:PCMU
M: recvonly
X: 0123456789AD
R: MO/sup(addr(K0, 4,1,1, s2), id(K0,0,0,7,3,2,5,5,5,1,2,3,4,s0))
S: MO/ans

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 0
```

la réponse indique que la transaction a échoué, parce que le circuit était déjà pris. En conséquence, il n'est renvoyé ni un identificateur de connexion connection-id ni une description de session:

```
401 2005 Circuit already seized
```

Notre troisième exemple illustre l'emploi de la réponse provisoire et de la prise de contact à trois:

```
CRCX 1206 ds/ds1-1/1@tgw.whatever.net MGCP 1.0 TGCP 1.0
K: 1205
C: A3C47F21456789F0
L: p:10, a:PCMU
M: inactive

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 0
```

une réponse provisoire est d'abord renvoyée:

```
100 1206 Pending
I: DFE233D1

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 3456 RTP/AVP 0
```

Peu après, la réponse finale est reçue:

```
200 1206 OK
K:
I: DFE233D1

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 3456 RTP/AVP 0
```

le contrôleur MGC accuse réception de la réponse finale, comme il en a été prié:

```
000 1206
```

et la transaction est achevée.

A.II.4 Commande ModifyConnection

Le premier exemple montre une commande ModifyConnection qui attribue simplement au mode de connexion la valeur "envoi/réception" – "L'entité notifiée" est également fixée:

```
MDCX 1209 ds/ds1-1/21@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: FDE234C8
N: mgc@mgc1.whatever.net
M: sendrecv
```

la réponse indique que la transaction a réussi:

```
200 1209 OK
```

dans le deuxième exemple, nous transmettons une description de session et incorporons une demande de notification avec la commande ModifyConnection. L'extrémité commencera à produire des tonalités de rappel automatique à destination du RTPC jusqu'à ce qu'elle détecte un flux audio dans la connexion spécifiée pour le signal de rappel automatique:

```
MDCX 1210 ds/ds1-1/3@abc5.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: FDE234C8
M: recvonly
X: 0123456789AE
R: ma@ FDE234C8
S: rt

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 3456 RTP/AVP 0
```

la réponse indique que la transaction a réussi:

```
200 1206 OK
```

A.II.5 Commande DeleteConnection (par le contrôleur de passerelle média)

Dans cet exemple, le contrôleur MGC ordonne simplement à la passerelle de jonction de supprimer la connexion FDE234C8 à l'extrémité spécifiée:

```
DLCX 1210 ds/ds1-1/1@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: FDE234C8
```

la réponse indique la réussite, et signale que la connexion a été supprimée. Les paramètres de connexion pour cette connexion sont donc inclus aussi:

```
250 1210 OK
P: PS=1245, OS=62345, PR=780, OR=45123, PL=10, JI=27, LA=48
```

A.II.6 Commande DeleteConnection (par la passerelle de jonction)

Dans cet exemple, la passerelle de jonction envoie une commande DeleteConnection au contrôleur MGC pour lui signaler qu'une connexion à l'extrémité spécifiée a été supprimée. Le code de motif ReasonCode spécifie le motif de suppression, et les paramètres de connexion pour cette connexion sont fournis aussi:

```
DLCX 1210 ds/ds1-1/1@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: FDE234C8
E: 900 – Hardware error
P: PS=1245, OS=62345, PR=780, OR=45123, PL=10, JI=27, LA=48
```

le contrôleur MGC envoie à la passerelle une réponse de réussite:

```
200 1210 OK
```

A.II.7 Commande DeleteConnection (par le contrôleur de passerelle média dans le cas de connexions multiples)

Dans le premier exemple, le contrôleur MGC ordonne à la passerelle de jonction de supprimer toutes les connexions liées à l'appel "A3C47F21456789F0" à l'extrémité spécifiée:

```
DLCX 1210 ds/ds1-1/6@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
```

la réponse indique la réussite et signale que la ou les connexions ont été supprimées:

```
250 1210 OK
```

dans le deuxième exemple, le contrôleur MGC ordonne à la passerelle de jonction de supprimer toutes les connexions reliées à toutes les extrémités qui sont spécifiées:

```
DLCX 1210 ds/ds1-1/*@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
```

la réponse indique la réussite:

```
250 1210 OK
```

A.II.8 Commande AuditEndpoint

Dans le premier exemple, le contrôleur MGC veut savoir quelles extrémités existent au niveau de la passerelle de jonction spécifiée. Il emploie donc le caractère de remplacement "tous" pour la partie locale du nom d'extrémité endpoint-name. Le contrôleur MGC ne veut que deux noms d'extrémité:

```
AUEP 1200 *@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
ZM: 2
```

la passerelle de jonction indique la réussite et inclut une liste de deux noms d'extrémité. Le total des noms d'extrémité concordant au nom spécifié avec caractère de remplacement s'élevait à 24:

```
200 1200 OK
Z: ds/ds1-1/1@tgw-2567.whatever.net
Z: ds/ds1-1/2@tgw-2567.whatever.net
ZN: 24
```

dans le deuxième exemple, les capacités de l'une des extrémités est demandée:

```
AUEP 1201 ds/ds1-1/1@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
F: A
```

la réponse indique la réussite et donne aussi les capacités. Deux codecs sont pris en charge, de capacités différentes toutefois. En conséquence, deux ensembles de capacités sont renvoyés:

```
200 1201 OK
A: a:PCMU, p:10-100, e:on, s:off, v:IT, m:sendonly;recvonly;sendrecv;
                    inactive;loopback;conttest;netwloop;netwtest
A: a:G728, p:30-90, e:on, s:on, v:IT, m: sendonly;recvonly;sendrecv;
                         inactive;loopback;conttest;netwloop
```

dans le troisième exemple, le contrôleur MGC procède à un audit de toutes les informations possibles concernant l'extrémité:

```
AUEP 2002 ds/ds1-1/1@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
F: R, S,X,N,I,T,O,ES
```

la réponse indique la réussite:

```
200 2002 OK
R: IT/ft,mt(N)
S:
X: 0123456789B1
N: [128.96.41.12]
I: 32F345E2
T: ft
O:
ES:
```

la liste des événements demandés contient deux événements. Lorsque aucun nom de paquetage n'est spécifié, on suppose qu'il s'agit du nom par défaut. La même chose vaut pour les mesures, et il faut supposer pour l'événement "IT/ft" que la mesure est donc la mesure par défaut – Notify. L'omission d'une valeur pour le paramètre "SignalRequests" signifie qu'aucun signal n'est effectivement activé. "L'entité notifiée" effective renvoie à une adresse IP et une connexion seulement existe à l'extrémité. La valeur réelle du paramètre DetectEvents est "ft" et la liste pour le paramètre ObservedEvents est vide tout comme est vide le paramètre EventStates.

A.II.9 Commande AuditConnection

Le premier exemple montre une commande AuditConnection où il est procédé à l'audit des paramètres CallId, NotifiedEntity, LocalConnectionOptions, ConnectionMode, LocalConnectionDescriptor et des paramètres de connexion:

```
AUCX 2003 ds/ds1-1/18@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
I: 32F345E2
F: C,N,L,M,LC,P
```

la réponse indique la réussite et donne des informations pour le paramètre RequestedInfo:

```
200 2003 OK
C: A3C47F21456789F0
N: mgc@mgc1.whatever.net
L: p:10, a:PCMU
M: sendrecv
P: PS=395, OS=22850, PR=615, OR=30937, PL=7, JI=26, LA=47

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 1296 RTP/AVP 0
```

dans le deuxième exemple, il est demandé de procéder à l'audit des paramètres RemoteConnectionDescriptor et LocalConnectionDescriptor:

```
AUCX 1203 ds/ds1-1/2@tgw.whatever.net MGCP 1.0 TGCP 1.0
I: FDE234C8
F: RC,LC
```

la réponse indique la réussite et donne des informations pour le paramètre RequestedInfo. Dans ce cas, il n'existe pas de paramètre RemoteConnectionDescriptor; donc, en ce qui concerne celui-ci, seul le champ de la version de protocole est inclus:

```
200 1203 OK

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 1296 RTP/AVP 0

v=0
```

A.II.10 Commande RestartInProgress

Le premier exemple illustre un message RestartInProgress envoyé par une passerelle de jonction pour informer le contrôleur MGC que l'extrémité spécifiée sera mise hors service dans 300 secondes:

```
RSIP 1200 ds/ds1-1/1@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
RM: graceful
RD: 300
```

la réponse du contrôleur MGC indique que la transaction a réussi:

```
200 1200 OK
```

dans le deuxième exemple, le message RestartInProgress message envoyé par la passerelle de jonction informe le contrôleur MGC que toutes les extrémités de cette passerelle seront remises en service dans 0 seconde, c'est-à-dire qu'elles sont de nouveau en service. Le délai aurait aussi bien pu être omis:

```
RSIP 1204 *@tgw-2567.whatever.net MGCP 1.0 TGCP 1.0
RM: restart
RD: 0
```

la réponse du contrôleur MGC indique la réussite et signale en outre aux extrémités concernées la nouvelle "entité notifiée":

```
200 1204 OK
N: MGC-1@whatever.net
```

il se peut aussi que la commande échoue, la nouvelle "entité notifiée" étant indiquée comme dans l'expression suivante:

```
521 1204 OK
N: MGC-1@whatever.net
```

dans ce cas, la commande devrait ensuite être réessayée afin de respecter la "procédure de redémarrage" (voir A.2.4.3.5), cette fois allant vers le contrôleur MGC `"MGC-1@whatever.net"`.

Appendice A.III

Exemple de flux d'appel

Dans le présent appendice, un exemple de flux d'appel est donné entre un utilisateur faisant partie d'un réseau employant un adaptateur MTA et un protocole de signalisation[34] non spécifiés, et un utilisateur en dehors du réseau, joignable par l'intermédiaire d'une passerelle de jonction utilisant le protocole TGCP et d'une passerelle de signalisation prenant en charge la signalisation de l'ISUP du système de signalisation n° 7 (SS7). Il convient de noter que ce flux d'appel, bien qu'étant un flux valable, n'est donné qu'à titre d'exemple qui peut ou ne peut pas être employé dans la pratique.

Dans le flux d'appel ci-après dans la Figure A.III.1, le sigle CMS renvoie au serveur de gestion d'appels (*call management server*), MGC au contrôleur de passerelle média, TGW à la passerelle de jonction (*trunking gateway*) et SG à la passerelle de signalisation.

[34] Cette signalisation peut être de type NCS ou DCS.

MTA	CMS	MGC	TGW	SG
Placement d'appel (E.164)	→			
	Etablissement d'appel	→		
		Create Connection(SDP1) + Notification Request	→	
		←	**Ack(SDP2)**	
		IAM	———	→
		←	**Notify**	
		Ack + Modify Connection + Notification Request	→	
		COT	———	→
		←	———	**ACM**
	←	***Alerte***		
←	***Alerte***	←	———	**ANM**
		ModifyConnection	->	
		←	**Ack**	
	←	***Réponse***		
←	***Réponse***			
		(Communication établie)		
Raccrochage	→			
	Libération	→		
		REL	———	→
		Delete Connection	→	
		←	Ack(Perf data)	
		←	———	**RLC**
		(Fin de communication)		

Figure A.III.1/J.171 – Exemple de flux d'appel

Au cours de ces échanges, le profil TGCP du protocole MGCP est employé par le contrôleur MGC pour commander la passerelle de jonction. On suppose qu'un protocole non spécifié existe entre l'adaptateur MTA, le serveur CMS et le contrôleur MGC.

Nous supposons que l'adaptateur MTA indique (directement ou indirectement) au contrôleur MGC qu'il souhaite établir une communication vocale avec un numéro de téléphone conforme à la Rec. UIT-T E.164 et qu'il joint à sa demande une description de session. Le serveur CMS recherche le numéro demandé, conclut qu'il doit placer un appel en dehors du réseau et contacte donc le contrôleur MGC approprié. Celui-ci décide qu'il doit placer l'appel par l'intermédiaire de la passerelle de jonction `tgw.whatever.net.` En outre, il décide qu'un essai de continuité devrait être effectué pour cet appel.

La première commande est une combinaison des commandes CreateConnection et NotificationRequest qui est envoyée à la passerelle de jonction:

```
CRCX 2001 ds/ds1-1/6@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
L: p:10, a:PCMU
M: inactive
X: 0123456789B0
R: co2, oc, of
S: co1

v=0
o=- 25678 753849 IN IP4 128.96.41.1
s=-
c=IN IP4 128.96.41.1
t=0 0
m=audio 3456 RTP/AVP 0
```

à ce stade, la passerelle de jonction reçoit l'ordre d'entamer l'essai de continuité, d'attendre son résultat et de signaler celui-ci. La production du signal de l'essai de continuité et la détection de sa réussite (ou de son échec) au moyen du mécanisme des événements sont synchronisées, de manière que lorsque l'événement "co2" se produit, l'essai "co1" s'arrête. La partie de la commande se rapportant à l'établissement de la connexion ordonne d'établir une connexion inactive à l'extrémité spécifiée conformément à la Rec. UIT-T G.711 avec une période de mise en paquets de 10 ms. La commande incorpore également la description de session reçue de l'adaptateur MTA de départ.

La passerelle de jonction de sortie accusera réception de la commande en envoyant dans la description de session ses propres paramètres tels que l'adresse, les ports et le profil du protocole RTP ainsi que l'identificateur de la nouvelle connexion:

```
200 2001 OK
I: 32F345E2

v=0
o=- 4723891 7428910 IN IP4 128.96.63.25
s=-
c=IN IP4 128.96.63.25
t=0 0
m=audio 1297 RTP/AVP 0
```

le contrôleur MGC envoie au commutateur relié au circuit où l'appel est placé, par l'intermédiaire de la passerelle de signalisation, un message initial d'adresse conforme au système SS7. Ce message comporte une indication précisant que l'essai de continuité doit être effectué.

Par la suite, nous supposons que l'essai de continuité a réussi. En conséquence, l'événement "co2" est produit et notifié au contrôleur MGC:

```
NTFY 3001 ds/ds1-1/6@tgw.whatever.net MGCP 1.0 TGCP 1.0
X: 0123456789B0
O: co2
```

le contrôleur MGC envoie au commutateur distant un essai COT conforme au système SS7 indiquant "essai de continuité réussi" et accuse réception de la commande Notify reçue. Il joint également la combinaison des commandes ModifyConnection et NotificationRequest ordonnant à la passerelle de placer la connexion en mode "réception seulement" et de commencer à attendre les tonalités de télécopie et de modem:

```
200 3001 OK
.
MDCX 2006 ds/ds1-1/6@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: 32F345E2
M: recvonly
X: 0123456789B0
R: ft,mt
```

à ce stade, le contrôleur MGC a établi un chemin de transmission en semi-duplex. Le téléphone relié à l'adaptateur MTA d'entrée sera en mesure de recevoir des signaux, tels que des tonalités ou des annonces qui peuvent être produites en cas d'erreurs, ainsi le début de la parole qui très probablement sera produite lorsque l'utilisateur à l'arrivée répond au téléphone.

Le contrôleur MGC reçoit ensuite un message d'adresse complète conforme au système SS7 indiquant que l'entité appelée est dûment appelée, et par la suite un message de réponse conforme au système SS7 indiquant que l'entité appelée a répondu. Le contrôleur MGC place la connexion en mode duplex complet en envoyant à la passerelle de jonction la commande ModifyConnection suivante:

```
MDCX 2007 ds/ds1-1/6@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: 32F345E2
M: sendrecv
```

la passerelle de jonction répond immédiatement à cette commande:

```
200 2007 OK
```

parallèlement à cela, le contrôleur MGC informe l'adaptateur MTA de départ de l'existence de l'événement réponse à l'appel et enregistre à quel moment la réponse à l'appel a eu lieu.

A ce stade, la communication est entièrement établie.

Un peu plus tard, le téléphone relié à l'adaptateur MTA de départ, dans notre scénario, est raccroché et un événement raccrochage est transmis au contrôleur MGC (soit directement soit indirectement par l'intermédiaire du serveur CMS comme dans le cas exposé ici) lui enjoignant que la communication devrait se terminer.

Le contrôleur MGC vérifie qu'il y aurait lieu d'effectuer la déconnexion, par exemple lorsqu'il n'existe pas de maintien pour complément de service, et il envoie donc un message de libération conforme au système SS7 au commutateur distant, ainsi qu'une commande DeleteConnection à la passerelle de jonction:

```
DLCX 2009 ds/ds1-1/6@tgw.whatever.net MGCP 1.0 TGCP 1.0
C: A3C47F21456789F0
I: 32F345E2
```

les passerelles de jonction répondront par un accusé de réception qui contient les paramètres de la connexion:

```
250 2009 OK
P: PS=1245, OS=62345, PR=780, OR=45123, PL=10, JI=27, LA=48
```

une confirmation de la terminaison de la communication sous la forme d'un message de fin de libération conforme au système SS7 est également reçue par le contrôleur MGC qui finalement enregistre la fin de la communication.

Appendice A.IV

Spécifications relatives aux extrémités

Le présent appendice définit un ensemble de spécifications propres aux extrémités dans le cadre du protocole TGCP.

A.IV.1 Modes de connexion pris en charge

Les modes de connexion qu'une extrémité donnée DOIT prendre en charge dans le cadre du protocole TGCP sont énumérés dans le Tableau A.IV.1:

Tableau A.IV.1/J.171 – Listes des modes de connexion qui doivent être prises en charge par un point de terminaison TGCP

Type d'extrémité	Information supplémentaire relative à l'extrémité	sendonly	recvonly	sendrecv	inactive	loopback	conttest	netwloop	netwtest
DS-0	Jonction ISUP	√	√	√	√	√	√	√	√
DS-0	Jonction MF	√	√	√	√	–	–	√	√

Appendice A.V

Informations relatives à la compatibilité

Le présent appendice donne des informations sur la compatibilité du protocole TGCP.

A.V.1 Compatibilité avec la signalisation NCS

La présente version du protocole TGCP est fondée, dans la mesure du possible, sur la Rec. UIT-T J.162 et alignée sur celle-ci. Puisque le protocole TGCP et la signalisation NCS portent sur des types de passerelles différents, il existe plusieurs différences. Ces différences sont résumées ci-après:

- **modes de connexion**: la signalisation NCS et le protocole TGCP ont en commun un ensemble de modes de connexion, mais chacun a aussi des modes que l'autre ne prend pas en charge:
  - la signalisation NCS prend en charge les modes de connexion "conférence" et "duplication", contrairement au protocole TGCP;
  - le protocole TGCP prend en charge les modes de connexion "essai de continuité" et "bouclage", contrairement à la signalisation NCS;
- **cartes de chiffres**: le protocole TGCP ne prend pas en charge les cartes de chiffres, contrairement à la signalisation NCS. Cela a les conséquences suivantes:
  - il n'existe aucune commande dans le protocole TGCP qui peut accepter une carte de chiffres en tant que paramètre;
  - la mesure "recueillir conformément à la carte de chiffres" n'est pas prise en charge dans le protocole TGCP;

– la "carte de chiffres" ne peut pas être soumise à un audit;

- **qualité de service dynamique**: la signalisation NCS prend en charge la dynamique IPCablecom de signalisation de la qualité de service, contrairement au protocole TGCP.

Outre ce qui précède, les différences suivantes, non reliées au protocole, existent entre la signalisation NCS et le protocole TGCP:

- **paquetages d'événements**: les paquetages initiaux d'événements dans le protocole TGCP et dans la signalisation NCS sont différents;
- **schéma de dénomination des extrémités**: les schémas de dénomination des extrémités dans le protocole TGCP et dans la signalisation NCS diffèrent un peu.

A.V.2 Compatibilité avec le protocole MGCP

Le protocole TGCP (tout comme la signalisation NCS) est en outre un profil du protocole MGCP 1.0 conforme au document IETF RFC 2705, mais il contient également quelques éléments supplémentaires. Ci-après est donnée une liste des éléments ajoutés au protocole TGCP qui ne figurent pas dans le protocole MGCP:

- **schéma de dénomination des extrémités**: un schéma de dénomination des extrémités spécifique a été introduit pour les extrémités DS-0. Les règles relatives au remplacement de caractères, plus restrictives que dans le protocole MGCP, introduisent aussi la notion "d'intervalle" pour les extrémités DS-0;
- **commande incorporée ModifyConnection**: une nouvelle mesure relative à la commande incorporée ModifyConnection a été introduite;
- **sécurité**: les services de sécurité IPCablecom sont pris en charge dans le protocole TGCP. Cela influe sur le paramètre LocalConnectionOptions, sur les capacités et sur le protocole SDP.
- **extraction des noms d'extrémité**: la commande AuditEndpoint a été renforcée de manière à permettre le renvoi du nombre d'extrémités qui concordent avec un nom comportant un caractère de remplacement, ainsi que l'emploi d'un mécanisme d'extraction par bloc de ces noms d'extrémité. Cela implique, outre le renforcement de la commande AuditEndpoint, l'introduction de deux nouveaux noms de paramètre, à savoir MaxEndPointIds et NumEndPoints;
- **versions prises en charge**: la réponse RestartInProgress et la commande AuditEndpoint ont été renforcées par l'adjonction d'un paramètre VersionSupported destiné à permettre aux contrôleurs MGC et aux passerelles de déterminer quelles versions de protocole chacun prend en charge.
- **codes d'erreur**: deux nouveaux codes d'erreur ont été introduits, à savoir les codes 532 et 533;
- **utilisation du protocole SDP**: un nouveau profil d'utilisation du protocole SDP a été introduit dans le protocole TGCP. Ce profil et tous les exemples d'utilisation en particulier nécessitent une stricte conformité avec le protocole SDP, quelle que soit l'utilité des champs inclus. Des extensions propres à l'environnement IPCablecom ont également été ajoutées au protocole SDP;
- **réponse provisoire**: des précisions supplémentaires et la recommandation du mécanisme de réponse provisoire ont été incorporées dans le protocole TGCP. Une réponse d'accusé de réception d'une réponse (000) a été introduite, tandis qu'un paramètre ResponseAck sans valeur attribuée a été admis dans les réponses finales qui suivent les réponses provisoires, et qu'une procédure pour le mécanisme a été spécifiée;

- **paramètres de signal**: la syntaxe des paramètres de signal a été étendue de manière à permettre l'utilisation dans les paramètres de signal de parenthèses s'équilibrant. La temporisation de tous les signaux TO peut être modifiée par un paramètre de signal;
- **paquetages d'événements**: le protocole TGCP introduit un ensemble de nouveaux paquetages d'événements.

Finalement, il convient de noter que le protocole TGCP fournit des interprétations et, dans certains cas, une recommandation ou une clarification supplémentaire du comportement de base du protocole MGCP qui n'est pas toujours en mesure de rendre compte du comportement voulu du protocole MGCP.

Appendice A.VI

Exemple de paquetages d'événements

A.VI.1 Paquetage de services d'opérateur multifréquences du groupe de fonctions D

Nom du paquetage: MO

Les codes dans le Tableau A.VI.1 sont employés pour identifier des événements ou des signaux dans le cadre du paquetage "MO", qui sont destinés à la "signalisation des services d'opérateur" dans les circuits sortants unidirectionnels multifréquences. La signalisation des services d'opérateur multifréquences du groupe de fonctions C est également prise en charge. Ce paquetage sera utilisé pour des circuits de services généraux d'opérateur ainsi que pour des circuits réservés aux services d'urgence:

Tableau A.VI.1/J.171 – Codes utilisés pour identifier les événements et signaux du paquetage MO

Code	Description	Evénement	Signal	Informations supplémentaires
ans	Réponse à un appel	P	–	
ft	Tonalité de télécopie	√	–	
ld	Connexion de longue durée	C	–	
mt	Tonalité de modem	√	–	
orbk	Rappel automatique de l'opérateur	√	–	
rbz	Renvoi de mise en occupation	P	–	
rcl	Rappel de l'opérateur	–	BR	
rel	Libération d'appel	P	BR	
res	Reprise d'appel	–	BR	
rlc	Libération achevée	P, S	BR	
sup(<addr>, <id>)	Etablissement d'un appel	–	TO	Temporisation variable
sus	Suspension d'appel	–	BR	
swk	Démarrage sur signalisation de décrochage	√	–	
TDD	Tonalités des appareils de télécommunication pour les personnes malentendantes (TDD)	√		
oc	Opération achevée	√		
of	Echec de l'opération	√		

La définition des différents événements et signaux est donnée ci-après:

réponse à un appel (ans): une réponse à un appel est produite lorsque l'enregistrement automatique des numéros est demandé par le système OSS, ce qui veut dire que l'appel ne doit pas nécessairement avoir transité par un opérateur. Après qu'une réponse à un appel est donnée, le complément de services sera maintenu, à savoir seul le système OSS peut maintenant libérer le circuit.

tonalité de télécopie (ft): l'événement tonalité de télécopie est produit lorsqu'une communication de type télécopie est détectée – Voir, par exemple, les Recs. UIT-T T.30 ou V.21.

connexion de longue durée (ld): la "connexion de longue durée" est détectée lorsqu'une connexion a été établie depuis plus d'un certain temps. La valeur par défaut est une heure, mais elle peut être modifiée par le processus de configuration.

L'événement peut être détecté dans une connexion. Lorsque aucune connexion n'est spécifiée, l'événement s'applique à toutes les connexions reliées à l'extrémité, quel que soit l'instant où elles ont été établies.

tonalités de modem (mt): l'événement tonalité de modem est produit lorsqu'une communication de type modem est détectée – Voir, par exemple, la Rec. UIT-T V.8.

rappel automatique de l'opérateur (orbk): cet événement se produira lorsque le système OSS demande que l'entité appelante sera appelée[35].

renvoi de mise en occupation (rbz): cet événement a lieu lorsque le système OSS marque le circuit. Un événement libération sera produit lorsque le circuit n'est plus occupé.

rappel de l'opérateur (rcl): ce signal peut être employé pour demander le rappel de l'opérateur, par exemple suite à un appel par signal du crochet commutateur du client destiné à faire revenir l'opérateur.

libération d'appel (rel): la libération d'appel peut être signalée à la passerelle média, mais lorsque le complément de services est maintenu, il ne peut y avoir déconnexion de la communication avant que le système OSS libère celle-ci. La passerelle média produit un événement "libération d'appel" lorsqu'elle considère que le système OSS a libéré le circuit. Dans ce cas, l'événement peut être paramétrisé au moyen de l'un des codes du Tableau A.VI.2, qui indiquent le motif de la libération:

Tableau A.VI.2/J.171 – Codes des motifs de libération d'appel

Code du motif	Motif
0	Libération normale
3	Pas de chemin vers la destination
8	Préemption
19	Pas de réponse
21	Appel rejeté
27	Destination hors service
28	Format de numéro non valable (par exemple, adresse incomplète)
38	Réseau hors service
111	Erreur de protocole ou de signalisation non spécifiée (par exemple, temporisation)

Reprise d'appel (res): ce signal indique que l'autre entité a repris l'appel, à savoir qu'elle a décroché.

Libération achevée (rlc): l'extrémité et le contrôleur MGC emploient l'événement ou le signal de libération achevée pour confirmer que la communication a été libérée et que le circuit est disponible pour d'autres appels.

Etablissement d'un appel (sup(<addr>, <id>)): établissement d'un appel au système des services d'opérateur au moyen d'informations fournies relatives à l'adresse et à l'identification. L'information relative à l'adresse sera de la forme suivante:

$addr(MF_1, MF_2, \ldots, MF_n)$

tandis que celle qui se rapporte à l'identification sera de la forme suivante:

$id(MF_1, MF_2, \ldots, MF_n)$

chaque chiffre MF_i correspondant à l'un des symboles numériques suivants/MF dans le Tableau A.VI.3:

[35] Si l'entité appelante a raccroché, la sonnerie sera généralement employée, tandis qu'une tonalité de renumérotation sera en général utilisée dans le cas où l'entité appelante a décroché.

Tableau A.VI.3/J.171 – Symboles numériques MF

Symbole	Chiffre MF_i	Symbole	Chiffre MF_i
0	MF 0	K0	MF K0 or KP
1	MF 1	K1	MF K1
2	MF 2	K2	MF K2
3	MF 3	S0	MF S0 or ST
4	MF 4	S1	MF S1
5	MF 5	S2	MF S2
6	MF 6	S3	MF S3
7	MF 7	K0	MF K0 or KP
8	MF 8		
9	MF 9		

Donc, un signal d'établissement d'un appel pourrait par exemple être de la forme suivante:

```
sup(addr(K0, 5,5,5,1,2,1,2, S0), id(K0, 5,5,5,1,2,3,4, S0))
```

Suspension d'appel (sus): ce signal indique que l'autre entité a mis l'appel en suspens, à savoir qu'elle a raccroché.

Démarrage sur signalisation de décrochage (swk): un contrôleur de passerelle média peut demander que la passerelle média lui notifie à quel moment le signal de démarrage sur signalisation de décrochage est produit.

Tonalités des appareils de télécommunication pour les personnes malentendantes (TDD): l'événement TDD est produit lorsqu'une communication de type TDD est détectée – Voir la Rec. UIT-T V.18.

Opération achevée (oc): l'événement opération achevée est produit lorsque la passerelle a été priée d'appliquer un ou plusieurs signaux de type TO à l'extrémité, et qu'un ou plusieurs d'entre eux ont pris fin sans avoir été arrêtés par la détection d'un événement demandé tel que "passage à l'état décroché ou chiffre composé" (off-hook transition or dialed digit). Le rapport d'achèvement peut comporter en tant que paramètre le nom du signal dont la durée de vie s'est achevée, comme dans l'expression suivante:

```
O: MO/oc(MO/sup)
```

lorsque l'événement opération achevée est demandé, il ne peut être paramétrisé au moyen de paramètres d'événement quelconques. Lorsque le nom du paquetage est omis, on suppose qu'il s'agit du nom par défaut.

Echec de l'opération (of): en général, l'événement échec de l'opération peut être produit lorsque l'extrémité a été priée d'appliquer un ou plusieurs signaux du type TO à l'extrémité, et qu'un ou plusieurs d'entre eux ont échoué avant l'interruption. Le rapport d'achèvement peut comporter en tant que paramètre le nom du signal qui a échoué, comme dans l'expression suivante:

```
O: MO/of(MO/sup)
```

Lorsque l'événement échec de l'opération est demandé, les paramètres d'événement ne peuvent être spécifiés. Lorsque le nom du paquetage est omis, on suppose qu'il s'agit du nom par défaut.

A.VI.2 Paquetage de protocoles de terminaison multifréquence

Nom du paquetage: MT

Dans la présente version de la Recommandation relative au protocole TGCP, le paquetage ne peut être employé que pour la vérification de l'occupation des lignes (BLV, *busy-line verification*) et pour l'interruption par l'opérateur (OI, *operator interrupt*) dans des circuits entrants unidirectionnels multifréquences de terminaison dédiés à ces tâches[36].

Les codes dans le Tableau A.VI.4 sont employés pour identifier les événements et les signaux dans le cas du paquetage "MT" pour les "circuits de jonction multifréquences de terminaison" entrants unidirectionnels employés pour les services BLV et OI:

Tableau A.VI.4/J.171 – Codes employés pour identifier les événements et signaux du paquetage MT

Code	Description	Evénement	Signal	Informations supplémentaires
ans	Réponse à un appel	–	BR	
bz	Tonalité d'occupation	–	TO	Temporisation = 30 secondes
hf	Signalisation de décrochage	–	BR	
inf	Chiffres pour information	√		
oc	Opération achevée	√	–	
of	Echec de l'opération	√	–	
oi	Interruption par l'opérateur	√	–	
pst	Tonalité de signal continu	–	TO	Temporisation = illimitée
rel	Libération d'appel	P	BR	
res	Reprise d'appel	–	BR	
rlc	Libération achevée	P, S	BR	
ro	Tonalité de renumérotation	–	TO	Temporisation = 30 secondes
sup	Etablissement d'un appel	P	–	
sus	Suspension d'appel	–	BR	

La définition des différents événements et signaux est donnée ci-après:

NOTE – Voir la Rec. UIT-T E.180/Q.35 pour les détails techniques particuliers des tonalités.

Réponse à un appel (ans): le signal de réponse à un appel informe l'extrémité que l'entité ayant fait l'objet d'une vérification a répondu. Cela comprend le cas où cette entité avait déjà décroché. L'extrémité est censée transmettre la supervision de la réponse au système OSS.

Tonalité d'occupation (bz): poste occupé

Signalisation de décrochage (hf): ce signal indique que l'entité ayant fait l'objet d'une vérification a signalé un décrochage.

---

[36] Veuillez noter que lorsque les services d'opérateur sont fournis par un fournisseur extérieur au réseau, le système OSS peut ne pas avoir accès aux bases de données des abonnés pour déterminer si les services BLV et OI devraient être autorisés ou pas.

Chiffres pour information (inf (<inf-digits>): ce signal est employé dans un circuit entrant multifréquence pour indiquer les chiffres reçus. Les valeurs du paramètre <inf-digits> sont tous les chiffres qui ont été recueillis jusqu'au délimiteur et y compris celui-ci, à savoir ST, ST', ST" ou ST'".

Les valeurs du paramètre <inf-digits> sont données dans une liste de chiffres MF_i séparés par des virgules:

$MF_1, MF_2, \ldots, MF_n$

chaque chiffre MF_i correspondant à l'un des symboles numériques suivants dans le Tableau A.VI.5:

Tableau A.VI.5/J.171 – Symboles numériques MF

Symbole	Chiffre MF_i	Symbole	Chiffre MF_i
0	MF 0	K0	MF K0 or KP
1	MF 1	K1	MF K1
2	MF 2	K2	MF K2
3	MF 3	S0	MF S0 or ST
4	MF 4	S1	MF S1
5	MF 5	S2	MF S2
6	MF 6	S3	MF S3
7	MF 7	K0	MF K0 or KP
8	MF 8		
9	MF 9		

Donc un signal ou un événement pourrait par exemple être de la forme suivante:

```
inf(k0, 5,5,5,1,2,3,4, s0)
```

un exemple dans lequel la temporisation entre les chiffres expire après les chiffres 5,5,5 est le suivant:

```
inf(k0, 5,5,5)
```

Opération achevée (oc): voir la définition correspondante dans le paquetage de circuits de l'ISUP.

Echec de l'opération (of): voir la définition correspondante dans le paquetage de circuits de l'ISUP.

Interruption par l'opérateur (oi): l'événement interruption par l'opérateur se produit lorsque l'opérateur tente d'interrompre l'appel et produit une tonalité "interruption par l'opérateur". Puisque aucune tonalité normalisée n'est définie à ces fins, l'événement est défini de manière à se produire lorsqu'un certain niveau énergétique est détecté dans le circuit correspondant à une transition du bruit de ligne à la voix ou aux tonalités. Il convient de noter qu'il n'est pas possible de détecter une transition inverse de la voix ou des tonalités au bruit de ligne.

Tonalité de signal continu (pst): **libération d'appel (rel)**: le contrôleur MGC peut utiliser le signal de libération pour libérer la communication[37]. Dans ce cas, le signal de libération peut ne pas être paramétré.

L'extrémité peut en revanche employer l'événement pour informer le contrôleur MGC qu'elle a libéré la communication – dans ce cas, l'événement peut être paramétré au moyen de l'un des codes dans le Tableau A.VI.6, qui indiquent le motif de la libération:

Tableau A.VI.6/J.171 – Codes de motifs de libération de l'appel

Code du motif	Motif
0	Libération normale
3	Pas de route vers la destination
8	Préemption
19	Pas de réponse
21	Appel rejeté
27	Destination hors service
28	Format de numéro non valable (par exemple, adresse incomplète)
38	Réseau hors service
111	Erreur de protocole ou de signalisation non spécifiée (par exemple, temporisation)

Reprise d'appel (res): ce signal indique que l'entité qui a fait l'objet d'une vérification a repris l'appel, à savoir qu'elle a décroché.

Libération achevée (rlc): l'extrémité et le contrôleur MGC emploient l'événement ou le signal de libération achevée pour confirmer que la communication a été libérée et que le circuit est disponible pour d'autres appels.

Etablissement d'appel (sup): un événement "sup" est utilisé pour indiquer l'arrivée d'un appel entrant (correspondant à l'événement de décrochage entrant). L'événement est fourni sans paramètre.

Suspension d'appel (sus): ce signal indique que l'entité qui a fait l'objet d'une vérification a mis l'appel en suspens, à savoir qu'elle a raccroché.

[37] Veuillez noter que l'opérateur qui effectue la vérification commande normalement la libération de connexions achevées sans essai et que le signal de suspension devrait dont généralement être employé.

Appendice A.VII

Bibliographie

– *Bellcore Notes on the Networks*, Bellcore, SR-2275.

– *Compatibility Information for Feature Group D Switched Access Service,* Bellcore, TR-NPL-000258, Issue 1, octobre 1985.

– *Interoffice LATA Switching Systems Generic Requirements (LSSGR): Verification Connections (25-05-0903)*, Bellcore, TR-TSY-000531, Issue 2, juillet 1987.

– *Signalling for Analog Interfaces*, Bellcore, LSSGR GR-506-CORE, Issue 1, juin 1996.

– *Switching System Generic Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)*, Bellcore, LSSGR GR-317-CORE, Issue 2, décembrer 1997.

– *Custom Call Handling Features (FSD 80 Series)*, Bellcore, OSSGR GR-1176-CORE, Issue 1, mars 1999.

– IETF RFC 1827 (1995), *IP Encapsulating Security Payload (ESP)*.

– IETF RFC 2974 (Experimental), *Session Announcement Protocol*.

– *RTP Parameters*, http://www.iana.org/assignments/rtp-parameters.

Annexe A.B

Profil 2 du protocole TGCP

Doit encore faire l'objet d'un complément d'étude sur la base de la Rec. UIT-T H.248.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Genève, 2002