Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.323

(06/2006)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Infrastructure des services audiovisuels – Systèmes et équipements terminaux pour les services audiovisuels

Systèmes de communication multimédia en mode paquet

Recommandation UIT-T H.323

RECOMMANDATIONS UIT-T DE LA SÉRIE H

SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

CARACTÉRISTIQUES DES SYSTÈMES VISIOPHONIQUES	H.100–H.199
INFRASTRUCTURE DES SERVICES AUDIOVISUELS	
Généralités	H.200–H.219
Multiplexage et synchronisation en transmission	H.220–H.229
Aspects système	H.230–H.239
Procédures de communication	H.240–H.259
Codage des images vidéo animées	H.260–H.279
Aspects liés aux systèmes	H.280–H.299
Systèmes et équipements terminaux pour les services audiovisuels	**H.300–H.349**
Architecture des services d'annuaire pour les services audiovisuels et multimédias	H.350–H.359
Architecture de la qualité de service pour les services audiovisuels et multimédias	H.360–H.369
Services complémentaires en multimédia	H.450–H.499
PROCÉDURES DE MOBILITÉ ET DE COLLABORATION	
Aperçu général de la mobilité et de la collaboration, définitions, protocoles et procédures	H.500–H.509
Mobilité pour les systèmes et services multimédias de la série H	H.510–H.519
Applications et services de collaboration multimédia mobile	H.520–H.529
Sécurité pour les systèmes et services multimédias mobiles	H.530–H.539
Sécurité pour les applications et services de collaboration multimédia mobile	H.540–H.549
Procédures d'interfonctionnement de la mobilité	H.550–H.559
Procédures d'interfonctionnement de collaboration multimédia mobile	H.560–H.569
SERVICES À LARGE BANDE ET MULTIMÉDIAS TRI-SERVICES	
Services multimédias à large bande sur VDSL	H.610–H.619

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

Recommandation UIT-T H.323

Systèmes de communication multimédia en mode paquet

Résumé

La présente Recommandation décrit les terminaux et autres entités qui assurent des services pour communications multimédias sur des réseaux en mode paquet n'offrant pas nécessairement une qualité de service garantie. Les entités H.323 peuvent assurer en temps réel des communications audio, vidéo et de données. Seul le mode audio est obligatoire, les modes données et vidéo étant facultatifs; en cas de prise en charge de ces deux modes facultatifs, on doit pouvoir utiliser un mode de fonctionnement commun spécifié permettant l'interfonctionnement de tous les terminaux acceptant ce type de médias.

Le réseau à commutation de paquets sur lequel communiquent les entités H.323 peut être constitué d'une connexion point à point, d'un seul segment ou d'un interréseau de plusieurs segments aux topologies complexes.

Les entités H.323 peuvent être utilisées dans des configurations point à point, multipoint ou de diffusion (décrites dans la Rec. UIT-T H.332). Elles peuvent fonctionner avec des terminaux H.310 sur le RNIS-LB, des terminaux H.320 sur le RNIS-BE, des terminaux H.321 sur le RNIS-LB, des terminaux H.322 sur des réseaux LAN offrant une qualité de service garantie, des terminaux H.324 sur le RTGC et des réseaux sans fil ainsi que sur des terminaux V.70 sur le RTGC et des terminaux vocaux sur le RTGC ou le RNIS, par l'intermédiaire de passerelles.

Les entités H.323 peuvent être intégrées dans des ordinateurs personnels ou implémentées dans des dispositifs autonomes tels que des visiophones.

Il convient de noter que le titre de la Rec. UIT-T H.323 (1996) était "*Systèmes et équipements visiophoniques pour réseaux locaux offrant une qualité de service non garantie*" et qu'il a été modifié dans la version 2 pour mieux refléter l'extension du domaine d'application de la présente Recommandation.

Les produits revendiquant la conformité à la version 1 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la Recommandation H.323 (1996), qui fait référence aux Recommandations UIT-T H.225.0 (1996) et H.245 (1997). Les produits de la version 1 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 1} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) 2}.

Les produits revendiquant la conformité à la version 2 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la présente Recommandation H.323 (1998), qui fait référence aux Recommandations UIT-T H.225.0 (1998) et H.245 (1998 ou plus récente). Les produits de la version 2 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 2} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x} où "x" est égal ou supérieur à 3.

Les produits revendiquant la conformité à la version 3 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la présente Recommandation H.323 (1999), qui fait référence aux Recommandations UIT-T H.225.0 (1999) et H.245 (1999 ou plus récente). Les produits de la version 3 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 3} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x} où "x" est égal ou supérieur à 5.

Les produits revendiquant la conformité à la version 4 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la présente Recommandation H.323 (2000), qui fait référence aux Recommandations H.225.0 (2000) et H.245 (2000 ou plus récente). Les produits de la version 4 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 4} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x} où "x" est égal ou supérieur à 7.

Les produits revendiquant la conformité à la version 5 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la présente Recommandation H.323 (2003), qui fait référence aux Recommandations UIT-T H.225.0 (2003) et H.245 (02/2003 ou plus récente). Les produits de la version 5 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 5} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x} où "x" est égal ou supérieur à 9.

Les produits revendiquant la conformité à la version 6 de la Rec. UIT-T H.323 doivent satisfaire à toutes les prescriptions obligatoires de la présente Recommandation H.323 (2006), qui fait référence aux Recommandations UIT-T H.225.0 (2006) et H.245 (05/2006 ou plus récente). Les produits de la version 6 doivent être identifiés par des messages H.225.0 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 2250 version (0) 6} et par des messages H.245 contenant un identificateur **protocolIdentifier** = {itu-t (0) recommendation (0) h (8) 245 version (0) x} où "x" est égal ou supérieur à 13.

La présente version de la Rec. UIT-T H.323 intègre les modifications approuvées dans l'Amendement 1 (01/2005) intitulé "*Annexe D révisée*" et dans l'Amendement 2 (01/2005) intitulé "*Nouvelle Annexe M4*".

Source

La Recommandation UIT-T H.323 a été approuvée le 13 juin 2006 par la Commission d'études 16 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT avait 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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références normatives	2
3	Définitions	5
4	Symboles et abréviations	11
5	Conventions	14
6	Description du système	15
6.1	Flux d'information	15
6.2	Caractéristiques des terminaux	16
6.3	Caractéristiques des passerelles	31
6.4	Caractéristiques du portier	48
6.5	Caractéristiques du contrôleur multipoint	50
6.6	Caractéristiques du processeur multipoint	51
6.7	Caractéristiques du pont de conférence	52
6.8	Capacité multipoint	52
6.9	Modèles de services complémentaires	55
7	Signalisation d'appel	57
7.1	Adresses	57
7.2	Voie d'enregistrement, d'admission et de statut (RAS)	59
7.3	Voie de signalisation d'appel	75
7.4	Valeur de référence d'appel	79
7.5	Identificateur d'appel	79
7.6	Identificateur ID de conférence et paramètre conferenceGoal	79
7.7	Capacité d'appel d'extrémité	80
7.8	Services d'identification de l'appelant	81
7.9	Cadre générique d'extensibilité	87
8	Procédures de signalisation d'appel	90
8.1	Phase A – Etablissement de la communication	90
8.2	Phase B – Communication initiale et échange des capacités	114
8.3	Phase C – Etablissement d'une communication audiovisuelle	119
8.4	Phase D – Services de communication	122
8.5	Phase E – Fin de la communication	139
8.6	Gestion des défaillances du protocole	142
9	Interfonctionnement avec d'autres types de terminaux	143
9.1	Terminaux fonctionnant uniquement en mode téléphonique	143
9.2	Terminaux de visiophonie sur le RNIS (Rec. UIT-T H.320)	143
9.3	Terminaux de visiophonie sur le RTGC (Rec. UIT-T H.324)	144
9.4	Terminaux de visiophonie sur le réseau mobile (Annexe C/H.324, aussi appelée "H.324/M")	144

Page

9.5 Terminaux de visiophonie sur des réseaux ATM (terminaux RAST H.321 et H.310) 144
9.6 Terminaux de visiophonie sur des réseaux locaux à qualité de service garantie (Rec. UIT-T H.322) 145
9.7 Terminaux fonctionnant en mode téléphonie et données simultanées sur le RTGC (Rec. UIT-T V.70) 145
9.8 Terminaux T.120 sur le réseau en mode paquet 145
9.9 Passerelle pour l'acheminement de flux H.323 sur réseaux ATM 145
10 Améliorations facultatives 146
10.1 Chiffrement 146
10.2 Exploitation multipoint 146
10.3 Assemblage d'appels dans des messages H.323 146
10.4 Tunnellisation de messages de signalisation non H.323 150
10.5 Utilisation de la charge utile RTP pour les chiffres DTMF, les tonalités et les signaux téléphoniques 152
11 Maintenance 153
11.1 Fonctions de bouclage aux fins de la maintenance 153
11.2 Méthodes de surveillance 155
Annexe A – Messages H.245 utilisés par les extrémités H.323 155
Annexe B – Procédures pour codecs vidéo stratifiés 162
B.1 Domaine d'application 162
B.2 Introduction 162
B.3 Méthodes d'échelonnabilité 162
B.4 Etablissement de l'appel 163
B.5 Utilisation de sessions et de couches de codec en protocole RTP 163
B.6 Modèles de stratification possibles 165
B.7 Incidence sur les conférences multipoints 166
B.8 Utilisation de la qualité de service du réseau pour les flux vidéo stratifiés 168
Annexe C – Flux H.323 en mode ATM 169
C.1 Introduction 169
C.2 Domaine d'application 169
C.3 Architecture 170
C.4 Article relatif au protocole 175
Annexe D – Télécopie en temps réel sur systèmes H.323 179
D.1 Introduction 179
D.2 Domaine d'application 180
D.3 Procédures applicables à l'ouverture de voies pour l'envoi de paquets T.38 180
D.4 Procédures autres que "FastConnect" 183
D.5 Remplacement d'un flux audio existant par un flux fax T.38 185

Page

D.6 Utilisation de maxBitRate dans les messages 189
D.7 Interactions avec les passerelles et avec les dispositifs de type Annexe B/T.38 189
Annexe E – Cadre général et protocole d'échange pour le transport multiplexé de la signalisation d'appel 190
E.1 Domaine d'application 190
E.2 Signalisation d'appel H.225.0 selon la présente annexe 203
Annexe F – Dispositifs d'extrémité simples 208
F.1 Introduction 208
F.2 Conventions de spécification 208
F.3 Domaine d'application 209
F.4 Références normatives 210
F.5 Abréviations 210
F.6 Aperçu général de la fonctionnalité système des types d'extrémité simples audiophoniques 210
F.7 Procédures pour dispositifs d'extrémité simples 211
F.8 Extensions de sécurité 218
F.9 Considérations relatives à l'interopérabilité 219
F.10 Notes d'implémentation (informatives) 219
Annexe G – Conversation en mode texte et type d'extrémité textophonique simple 223
G.1 Introduction 223
G.2 Domaine d'application 223
G.3 Références normatives 224
G.4 Définitions 224
G.5 Indication des capacités pour les communications en mode texte dans le cadre de la Rec. H.323 224
G.6 Procédures d'ouverture des voies pour la conversation en mode texte T.140 227
G.7 Mise en trame et mise en tampon des données T.140 228
G.8 Interaction avec des fonctionnalités de conversation en mode texte dans d'autres dispositifs 228
G.9 Configurations multipoint 229
G.10 Text SET: type d'extrémité textophonique simple 231
Annexe J – Sécurisation des dispositifs de l'Annexe F 233
J.1 Introduction 233
J.2 Conventions 233
J.3 Domaine d'application 233
J.4 Abréviations 234
J.5 Références normatives 234
J.6 Type audio d'extrémité simple sécurisé (SASET) 234

Page

Annexe K – Voie de transport par protocole HTTP des signaux de commande de services dans les réseaux H.323 236
K.1 Introduction 236
K.2 Commande de services dans les réseaux H.323 238
K.3 Utilisation du protocole HTTP 240
K.4 Exemples de scénario 242
K.5 Références 246
Annexe L – Protocole de commande de stimulus 247
L.1 Domaine d'application 247
L.2 Introduction 249
L.3 Modèle schématique des stimulus 250
L.4 Références normatives 253
Annexe M1 – Canalisation de la signalisation à l'interface Q (QSIG) dans les réseaux H.323 253
M1.1 Domaine d'application 253
M1.2 Références normatives 253
M1.3 Procédures aux dispositifs d'extrémité 254
M1.4 Canalisation de connexion QSIG orientée signalisation indépendante de l'appel 255
M1.5 Procédures avec portier 255
Annexe M2 – Tunnellisation du protocole de signalisation (ISUP) dans les réseaux H.323 256
M2.1 Domaine d'application 256
M2.2 Références normatives 256
M2.3 Procédures aux extrémités 256
M2.4 Procédures au portier 258
Annexe M3 – Tunnellisation de la signalisation DSS1 à travers les réseaux H.323 258
M3.1 Domaine d'application 258
M3.2 Références normatives 258
M3.3 Procédures appliquées aux points d'extrémité 259
M3.4 Tunnellisation de signalisation DSS1 indépendante du support 261
M3.5 Procédures relatives au portier 262
Annexe M4 – Tunnellisation de la syntaxe de signalisation en bande étroite (NSS) à travers les réseaux H.323 262
M4.1 Domaine d'application 262
M4.2 Références normatives 263
M4.3 Procédures appliquées aux points d'extrémité H.225.0 263
M4.4 Procédures applicables au portier 264
M4.5 Procédures de signalisation RAS applicables aux appels à routage direct 264

Page

Annexe O – Utilisation des localisateurs uniformes de ressources et du système de noms de domaine 266
O.1 Domaine d'application 266
O.2 Références normatives 266
O.3 Références informatives 266
O.4 Localisateur URL H.323 267
O.5 Codage du localisateur URL H.323 dans des messages H.323 267
O.6 Localisateurs URL et identificateurs URI non H.323 dans le contexte de la Rec. UIT-T H.323 267
O.7 Paramètres du localisateur URL H.323 268
O.8 Utilisation du localisateur URL H.323 269
O.9 Recours au système DNS pour traduire un localisateur URL H.323 à envoyer à l'adresse IP 270
O.10 Utilisation d'enregistrements de ressources SRV du système DNS 271
Annexe P – Transfert des signaux de modems sur les systèmes H.323 274
P.1 Domaine d'application 274
P.2 Références normatives 274
P.3 Définitions 274
P.4 Abréviations 275
P.5 Introduction 275
P.6 Indication des capacités 276
P.7 Etablissement d'appel 276
P.8 Signalisation du canal logique 276
Annexe Q – Télécommande de la caméra distante au moyen des protocoles H.281/H.224 280
Q.1 Domaine d'application 280
Q.2 Références normatives 280
Q.3 Introduction 280
Q.4 Protocole de télécommande de caméra 280
Q.5 Information d'en-tête RTP 282
Annexe R – Méthodes d'amélioration de la robustesse pour les entités H.323 282
R.1 Introduction et domaine d'application 282
R.2 Références normatives 283
R.3 Définitions 283
R.4 Abréviations 284
R.5 Aperçu général des deux méthodes 284
R.6 Mécanismes communs 286
R.7 Méthode A: rétablissement d'état à partir d'entités voisines 289
R.8 Méthode B: rétablissement d'état à partir d'un répertoire partagé 293
R.9 Interfonctionnement des méthodes d'amélioration de la robustesse 296
R.10 Procédures de rétablissement 296

Page

R.11 Utilisation du champ GenericData 299
R.12 Note informative 1: généralités concernant les méthodes d'amélioration de la robustesse 301
R.13 Note informative 2: partage d'état d'appel entre une entité et son entité homologue de secours 304
Appendice I – Commande du mode de communication de contrôleur multipoint échantillon à terminal 310
I.1 Scénario A d'une conférence échantillon 310
I.2 Table des modes de communication envoyée à toutes les extrémités 310
I.3 Scénario B d'une conférence échantillon 311
I.4 Table des modes de communication envoyée à toutes les extrémités 311
Appendice II – Procédures de réservation de ressources dans la couche Transport 312
II.1 Introduction 312
II.2 Prise en charge de la QS pour la H.323 313
II.3 Rappel des bases du protocole RSVP 314
II.4 La phase d'échange de capacités H.245 316
II.5 Ouvertures de voies logiques et établissement de réservations 316
II.6 Clôture de voie logique et libération des réservations 318
II.7 Réservation de ressources pour voies logiques H.323 multidiffusées 318
II.8 Protocole RSVP synchronisé 319
Appendice III – Localisation d'utilisateur par portier 324
III.1 Introduction 324
III.2 Signalisation 324
Appendice IV – Voies logiques de remplacement avec ordre de priorité de signalisation sur une connexion H.245 326
IV.1 Introduction 326
IV.2 Signalisation 326
Appendice V – Utilisation des plans de numérotage E.164 et ISO/CEI 11571 327
V.1 Plan de numérotage E.164 327
V.2 Numéro de réseau privé 329
V.3 Usage des versions 1, 2 et 3 de la Rec. UIT-T H.323 330
Appendice VI – Description d'un système H.323 type sur IP 331

Recommandation UIT-T H.323

Systèmes de communication multimédia en mode paquet

1 Domaine d'application

La présente Recommandation traite des prescriptions techniques pour systèmes de communication multimédia lorsque le transport sous-jacent est un réseau en mode paquet n'offrant pas nécessairement une qualité de service (QS) garantie. Ces réseaux en mode paquet peuvent être des réseaux locaux, des réseaux locaux d'entreprise, des réseaux de zone métropolitaine, des réseaux internes et des interréseaux (y compris l'Internet). Il peut également s'agir de connexions commutées ou point à point sur RTGC ou RNIS, qui font appel à une couche de transport sous-jacente telle que le protocole point à point (PPP). Ces réseaux peuvent être constitués d'un seul segment de réseau ou avoir des topologies complexes, comportant de nombreux segments de réseau interconnectés par d'autres voies de communication.

La présente Recommandation décrit les éléments constituants d'un système H.323. Il s'agit des terminaux, des passerelles, des portiers, des contrôleurs multipoints, des processeurs multipoints et des ponts de conférence. Les messages et procédures de commande définissent, dans le cadre de la présente Recommandation, la façon dont ces éléments communiquent. Une description détaillée de ces éléments est contenue au § 6.

Les terminaux H.323 offrent, dans les conférences point à point ou multipoints, la capacité de communications audio et, facultativement, vidéo et télématiques (données). L'interfonctionnement avec d'autres terminaux conformes à la série H, avec des terminaux de téléphonie sur RTGC ou RNIS, ou avec des terminaux de transmission de données sur RTGC ou RNIS est réalisé au moyen de passerelles. Voir Figure 1. Les portiers fournissent les services de contrôle d'admission et de traduction d'adresse. Les contrôleurs multipoints, les processeurs multipoints et les ponts de conférence fournissent les capacités nécessaires aux conférences multipoints.

Le domaine d'application de la Rec. UIT-T H.323 ne comprend pas l'interface avec le réseau, la couche Physique du réseau ou le protocole de transport utilisé sur le réseau. Exemples (non limitatifs) de ces réseaux:

- Ethernet (IEEE 802.3);
- Fast Ethernet (IEEE 802.3u);
- Interface de données avec distribution par fibre (FDDI);
- Token Ring (IEEE 802.5);
- Mode ATM.

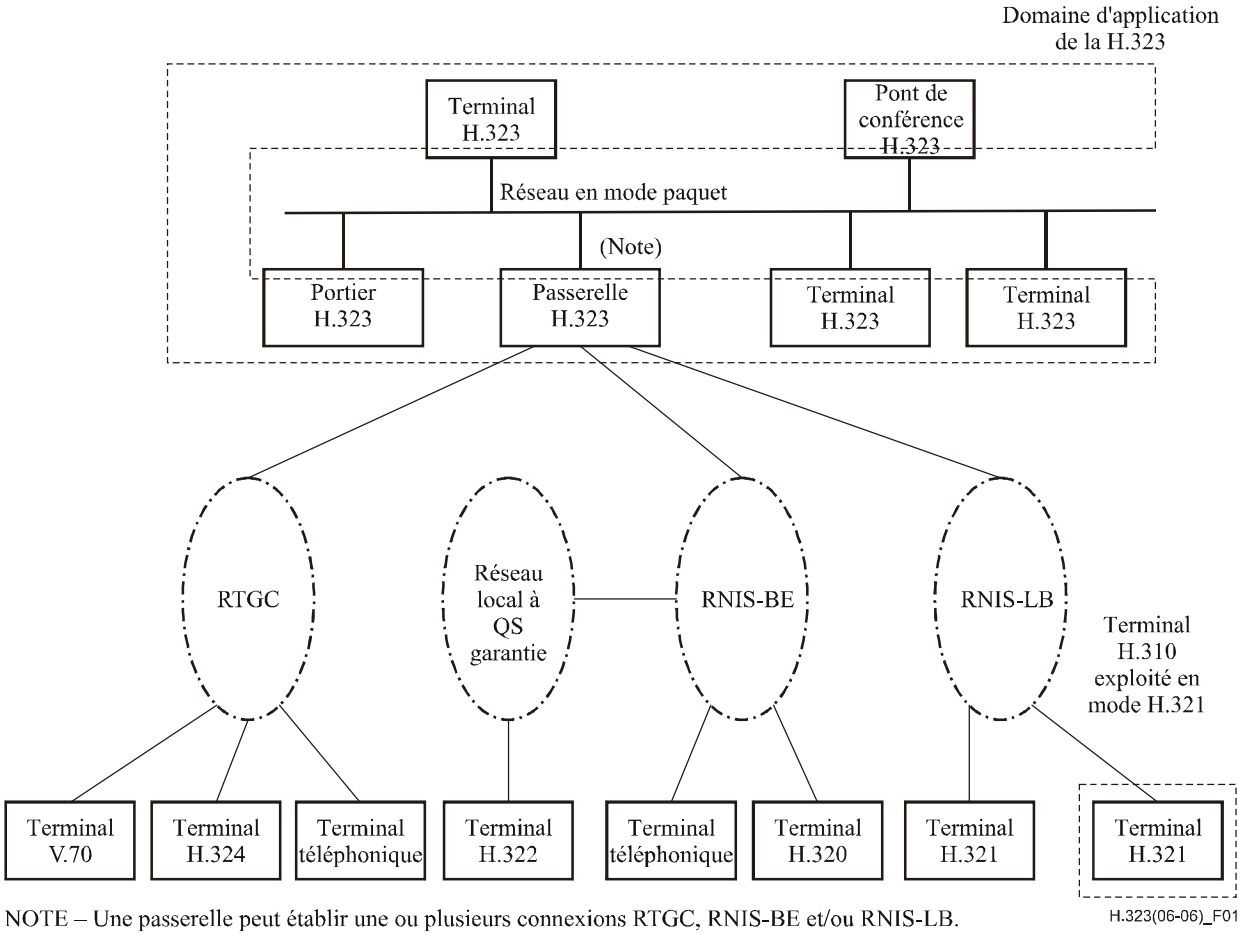


Figure 1/H.323 – Interopérabilité des terminaux H.323

2 Références normatives

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

[1] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

[2] Recommandation UIT-T H.245 (2006), *Protocole de commande pour communications multimédias*.

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

[4] Recommandation UIT-T G.722 (1988), *Codage audiofréquence à 7 kHz à un débit inférieur ou égal à 64 kbit/s*.

[5] Recommandation UIT-T G.723.1 (2006), *Codeur vocal à double débit pour communications multimédias acheminées à 5,3 kbit/s et à 6,3 kbit/s*.

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

[7] Recommandation UIT-T G.729 (1996), *Codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée*.

[8] Recommandation UIT-T H.261 (1993), *Codec vidéo pour services audiovisuels à p ×64 kbit/s*.

[9] Recommandation UIT-T H.263 (2005), *Codage vidéo pour communications à faible débit*.

[10] Recommandation UIT-T T.120 (1996), *Protocoles de données pour conférence multimédia*.

[11] Recommandation UIT-T H.320 (2004), *Systèmes et équipements terminaux visiophoniques à bande étroite*.

[12] Recommandation UIT-T H.321 (1998), *Adaptation des terminaux visiophoniques H.320 aux environnements RNIS à large bande*.

[13] Recommandation UIT-T H.322 (1996), *Systèmes et équipements terminaux visiophoniques pour réseaux locaux offrant une qualité de service garantie*.

[14] Recommandation UIT-T H.324 (2005), *Terminal pour communications multimédias à faible débit*.

[15] Recommandation UIT-T H.310 (1998), *Systèmes et terminaux de communication audiovisuels à large bande*.

[16] Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

[17] Recommandation UIT-T Q.932 (1998), *Système de signalisation d'abonné numérique n° 1 – Procédures génériques pour la commande des services complémentaires RNIS*.

[18] Recommandation UIT-T Q.950 (2000), *Protocoles pour services complémentaires, structure et principes généraux*.

[19] ISO/CEI 10646:2003, *Technologies de l'information – Jeu universel de caractères codés sur plusieurs octets (JVC)*.

[20] Recommandation UIT-T E.164 (2005), *Plan de numérotage des télécommunications publiques internationales*.

[21] Recommandation UIT-T H.246 (2006), *Interfonctionnement des terminaux multimédias de la série H avec d'autres terminaux multimédias de la série H et des terminaux vocaux ou en bande vocale sur le RTGC et le RNIS et le RMTP*.

[22] Recommandation UIT-T H.235.0 (2005), *Cadre de sécurité H.323: cadre de sécurité pour les systèmes multimédias de la série H (systèmes H.323 et autres systèmes de type H.245)*.

[23] Recommandation UIT-T H.332 (1998), *Extension du protocole H.323 aux conférences à faible couplage*.

[24] Recommandation UIT-T H.450.1 (1998), *Protocole générique fonctionnel pour le support des services complémentaires dans les systèmes H.323*.

[25] Recommandation UIT-T I.363.5 (1996), *Spécification de la couche d'adaptation ATM du RNIS-LB – AAL de type 5*.

[26] Recommandation UIT-T Q.2931 (1995), *Système de signalisation d'abonné numérique n° 2 – Spécification de la couche 3 de l'interface utilisateur-réseau pour la commande de connexion/appel de base*.

[27] Recommandation UIT-T I.356 (2000), *Caractéristiques du transfert de cellules de la couche ATM du RNIS-LB*.

[28] Recommandation UIT-T I.371 (2004), *Gestion du trafic et des encombrements dans le RNIS-LB*.

[29] Recommandation UIT-T Q.2961.2 (1997), *Système de signalisation d'abonné numérique n° 2 – Paramètres de trafic supplémentaires: prise en charge de la capacité de transfert ATM dans l'élément d'information de capacité de support à large bande*.

[30] Recommandation UIT-T H.282 (1999), *Protocole de commande d'équipement distant pour les applications multimédias*.

[31] Recommandation UIT-T H.283 (1999), *Transport par canal logique de la commande d'équipement distant*.

[32] ATM Forum, AF-SAA-0124.000 (1999), *H.323 Media Transport Over ATM* (Transport des médias H.323 en mode ATM).

[33] Recommandation UIT-T Q.2941.2 (1999), *Système de signalisation d'abonné numérique n° 2 – Extensions relatives au transport des identificateurs génériques*.

[34] Recommandation UIT-T H.450.2 (1998), *Service complémentaire de transfert de communication dans les systèmes H.323*.

[35] Recommandation UIT-T H.450.4 (1999), *Service complémentaire de mise en attente dans les systèmes H.323*.

[36] Recommandation UIT-T H.248.1 (2005), *Protocole de commande de passerelle: version 3.*

[37] ISO/CEI 11571:1998, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux privés à intégration de services – Adressage*.

[38] Recommandations UIT-T de la série Q.951.x, *Description d'étape 3 des services complémentaires d'identification de numéro utilisant le système de signalisation d'abonné numérique n° 1*.

[39] Recommandation UIT-T H.450.3 (1998), *Service complémentaire de déviation d'appel dans les systèmes H.323*.

[40] Recommandation UIT-T H.450.5 (1999), *Services complémentaires de mise en garde et d'interception d'appel dans les systèmes H.323*.

[41] Recommandation UIT-T H.450.6 (1999), *Service complémentaire d'appel en attente dans les systèmes H.323*.

[42] Recommandation UIT-T H.450.7 (1999), *Service complémentaire d'indication de message en attente dans les systèmes H.323*.

[43] Recommandation UIT-T H.450.8 (2000), *Service complémentaire d'identification de nom dans les systèmes H.323*.

[44] ISO/CEI 11572:2000, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé à intégration de services – Services porteurs en mode circuit – Procédures et protocole de signalisation d'interéchange*.

[45] Recommandation UIT-T H.222.0 (2006), *Technologies de l'information – Codage générique des images animées et du son associé: systèmes*.

[46] Recommandation UIT-T H.223 (2001), *Protocole de multiplexage pour communications multimédias à faible débit*.

[47] IETF RFC 2068 (1997), *Hypertext Transfer Protocol – HTTP/1.1*. (Protocole de transfert en hypertexte).

[48] IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*. (Extensions de courrier Internet à fonctions multiples – Partie 1: Format des corps de message Internet).

[49] Recommandation UIT-T Z.100 (2002), *SDL: langage de description et de spécification*.

[50] IETF RFC 1738 (1994), *Uniform Resource Locators (URL)*. (Localisateurs uniformes de ressource) (URL).

[51] IETF RFC 2234 (1997), *Augmented BNF for Syntax Specifications: ABNF*. (Formalisme BNF augmenté pour spécifications syntaxiques).

[52] ISO 4217:2001, *Codes pour la représentation des monnaies et types de fonds*.

[53] Recommandation UIT-T V.21 (1988), *Modem à 300 bit/s duplex normalisé pour usage sur le réseau téléphonique général avec commutation*.

[54] Recommandation UIT-T T.30 (2005), *Procédures pour la transmission de documents par télécopie sur le réseau téléphonique général commuté*.

[55] Recommandation UIT-T T.38 (2005), *Procédures de communication de télécopie du Groupe 3 en temps réel sur les réseaux à protocole Internet*.

[56] IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. (Charge utile RTP pour chiffres DTMF, tonalités et signaux téléphoniques).

[57] Recommandation UIT-T H.264 (2005), *Codage vidéo évolué pour les services audiovisuels génériques.*

[58] Recommandation UIT-T H.241 (2006), *Procédures vidéo et signaux de commande élargis pour les terminaux de la série H.300.*

3 Définitions

Pour les besoins de la présente Recommandation, les définitions indiquées dans le § 3/H.225.0 [1] et le § 3/H.245 [2] s'appliquent en plus de celles du présent paragraphe. Ces définitions ne s'appliquent que du côté réseau. D'autres termes pourront s'appliquer pour désigner le côté réseau à commutation de circuits (RCC). On trouvera au § 5, Conventions, d'autres informations sur l'usage des termes dans la présente Recommandation.

3.1 passerelle d'accès: passerelle qui connecte un réseau à un autre réseau (comme un réseau SS7 à un réseau QSIG) et qui remplit une certaine fonction d'interfonctionnement entre les différents réseaux.

3.2 contrôleur multipoint actif: contrôleur multipoint ayant mené à bien la procédure de choix du mode maître ou esclave et assurant la fonction de commande multipoint pour la conférence.

3.3 conférence multipoint ad hoc: conférence point à point qui est devenue, par extension à un moment donné au cours de la communication, une conférence multipoint. Cette extension peut être effectuée si un ou plusieurs des terminaux de la conférence point à point initiale incorporent un contrôleur multipoint, si la communication est établie par un portier intégrant une fonctionnalité de contrôleur multipoint ou si la communication initiale est établie par l'intermédiaire d'un pont de conférence sous forme d'une communication multipoint entre deux terminaux seulement.

3.4 adressable: qualité d'une entité H.323 du réseau en mode paquet ayant une adresse de transport. Adressable ne veut pas dire appelable. Un terminal ou un pont de conférence est adressable et appelable. Un portier est adressable mais n'est pas appelable. Un contrôleur multipoint ou un processeur multipoint n'est ni appelable ni adressable mais est intégré dans une extrémité ou dans un portier appelable ou adressable. Dans une passerelle composite, aussi bien la commande MGC que la passerelle média (MG) sont adressables mais seule la commande MGC est appelable.

3.5 silence: suppression du signal audio d'une source ou de toutes les sources. Un silence à l'émission signifie que l'émetteur d'un flux de signaux audio coupe son microphone ou cesse d'émettre tout signal audio. Un silence à la réception signifie que le terminal de réception ne tient pas compte des flux de signaux audio entrants ou coupe son haut-parleur.

3.6 conférence en mode diffusion; conférence diffusée: conférence à laquelle participe un seul émetteur de flux de médias et plusieurs récepteurs. Les flux de commandes ou de médias sont unidirectionnels. Pour l'implémentation de telles conférences, il convient d'utiliser les facilités de transport en multidiffusion du réseau, lorsque de tels services sont offerts. Voir également Rec. UIT-T H.332 [23].

3.7 conférence débat en mode diffusion; conférence débat diffusée: conférence alliant les caractéristiques d'une conférence multipoint et d'une conférence en mode diffusion. Dans une telle conférence, plusieurs terminaux participent à une conférence multipoint cependant que plusieurs autres terminaux se contentent de recevoir les flux de médias. La transmission s'effectue dans les deux sens entre les terminaux sur la portion multipoint de la conférence, mais dans un seul sens entre ces terminaux et les terminaux d'écoute. Voir également Rec. UIT-T H.332.

3.8 appel: communication multimédia point à point entre deux extrémités H.323. L'appel commence par la procédure d'établissement d'appel et finit par la procédure de terminaison d'appel. Il est formé d'un ensemble des voies fiables ou non fiables entre les extrémités. Un appel peut être établi directement entre deux extrémités ou peut comporter d'autres entités H.323 comme un portier ou un contrôleur multipoint. En cas d'interfonctionnement avec certaines extrémités du réseau à commutation de circuits par l'intermédiaire d'une passerelle, toutes les voies aboutissent à la passerelle où elles sont converties dans la représentation appropriée pour le système d'extrémité du RCC. Normalement, un appel est établi entre deux utilisateurs voulant communiquer; mais il peut s'agir d'un échange de trames de signalisation seulement. Une extrémité peut avoir la capacité de prendre en charge plusieurs appels simultanés.

3.9 voie de signalisation d'appel: voie fiable utilisée pour acheminer les messages d'établissement et de libération de la communication (selon la Rec. UIT-T H.225.0) entre deux entités H.323.

3.10 appelable: qualité d'une entité qui peut être appelée, comme indiqué au § 8 ou dans les Recommandations UIT-T relatives aux services complémentaires (H.450.x). En d'autres termes, une entité H.323 est généralement considérée comme étant appelable si un utilisateur la spécifie comme destination. Les terminaux, les ponts de conférence, les passerelles et les contrôleurs MGC sont appelables, mais les portiers, les contrôleurs multipoint et les passerelles médias ne le sont pas.

3.11 conférence multipoint centralisée: conférence dans laquelle tous les terminaux participants communiquent en mode point à point avec un pont de conférence. Les terminaux transmettent leurs flux de signaux de commande, de signaux audio, vidéo ou de données au pont de conférence. Le contrôleur multipoint intégré au pont de conférence assure la gestion centralisée de la conférence. Le processeur multipoint intégré au pont de conférence traite les flux de signaux audio, de signaux vidéo ou de données et les renvoie après traitement à chaque terminal.

3.12 passerelle composite: passerelle qui ne sépare pas les fonctions de contrôleur de passerelle média et de passerelle média.

3.13 commande et indication: signalisation de bout en bout entre terminaux, consistant en une commande qui déclenche un changement d'état du récepteur et en une indication qui fournit des informations sur l'état ou sur le fonctionnement du système (voir aussi Rec. UIT-T H.245 [2] pour un complément d'information et les abréviations).

3.14 données: flux d'informations autres que les signaux audio, vidéo et de commande, acheminé dans le canal de données logique (voir Rec. UIT-T H.225.0 [1]).

3.15 conférence multipoint décentralisée: conférence dans laquelle tous les terminaux participants se communiquent mutuellement leurs signaux audio et vidéo en mode multidiffusion sans utiliser de pont de conférence. Les terminaux ont pour tâche:

a) de mixer les flux de signaux audio reçus;

b) de sélectionner le ou les flux de signaux vidéo reçus à afficher.

Il n'est pas nécessaire dans ce cas d'utiliser un processeur multipoint pour le traitement des signaux audio ou vidéo. Les terminaux communiquent sur leurs voies de commande H.245, le contrôleur multipoint assurant la gestion de la conférence. En outre, le pont de conférence du service de communication multipoint (MCS), parfois intégré dans le processeur multipoint, assure le traitement centralisé du flux de données.

3.16 passerelle décomposée: passerelle qui est fonctionnellement séparée en un contrôleur de passerelle média et une ou plusieurs passerelles médias.

3.17 extrémité: terminal, passerelle ou pont de conférence H.323. Une extrémité peut appeler et être appelée. Elle émet ou reçoit des flux d'information.

3.18 portier (GK, *gatekeeper*): entité H.323 du réseau qui convertit les adresses et contrôle l'accès à ce réseau pour les terminaux, les passerelles et les ponts de conférence. Le portier peut aussi offrir d'autres services aux terminaux, passerelles et ponts de conférence, comme des services de gestion de largeur de bande et de localisation de passerelles.

3.19 passerelle (GW, *gateway*): extrémité du réseau qui assure en temps réel des communications bidirectionnelles entre des terminaux H.323 sur le réseau en mode paquet et d'autres terminaux UIT sur un réseau à commutation de circuits, ou à destination d'une autre passerelle H.323. Les autres terminaux UIT recouvrent les terminaux conformes aux Recommandations UIT-T H.310 (H.320 sur le RNIS-LB), H.320 (RNIS), H.321 (ATM), H.322 (GQOS-LAN, réseau en mode paquet à qualité de service garantie), H.324 (RTGC), H.324M (Mobile) et V.70 (DSVD).

3.20 entité H.323: tout élément H.323: terminaux, passerelles, portiers, contrôleurs multipoint, processeurs multipoints et ponts de conférence.

3.21 voie de commande H.245: voie fiable utilisée pour acheminer les messages d'information de commande H.245 (selon la Rec. UIT-T H.245) entre deux extrémités H.323.

3.22 session H.245: partie de la communication commençant à l'établissement d'une voie de commande H.245 et prenant fin à la réception du message de commande de fin de session **EndSessionCommand** ou par suite d'un dérangement. A ne pas confondre avec une communication, dont le début et la fin correspondent respectivement aux messages d'établissement et de Release Complete H.225.0.

3.23 conférence hybride multipoint audio centralisée: conférence durant laquelle les terminaux transmettent en mode multidiffusion leurs signaux vidéo aux autres terminaux participants, et en mode monodiffusion leurs signaux audio au processeur multipoint pour mélange. Celui-ci renvoie un flux de signaux audio mélangés à chaque terminal.

3.24 conférence hybride multipoint vidéo centralisée: conférence durant laquelle les terminaux transmettent en mode multidiffusion leurs signaux audio aux autres terminaux participants, et en mode monodiffusion leurs signaux vidéo au processeur multipoint pour commutation ou mélange. Celui-ci renvoie un flux de signaux vidéo à chaque terminal.

3.25 flux d'information: flux informationnel d'un type de média donné (par exemple audio) entre une source unique et une ou plusieurs destinations.

3.26 synchronisation labiale: opération destinée à donner l'impression que les mouvements des lèvres du locuteur apparaissant sur l'écran sont synchronisés avec ses paroles.

3.27 réseau local (LAN, *local area network*): réseau de communication d'homologue à homologue, sur média partagé ou commuté, diffusant des informations à destination de tous les postes situés dans un périmètre restreint, par exemple un bâtiment de bureau ou un campus. Ce réseau appartient en général à une organisation, qui l'utilise et l'exploite. Dans le contexte de la présente Recommandation, les réseaux locaux comprennent également des "interréseaux" composés de plusieurs réseaux locaux interconnectés par des ponts ou des routeurs.

3.28 voie logique: voie utilisée pour acheminer les flux d'information entre deux extrémités H.323. Ces voies sont établies selon les procédures d'ouverture de voie logique **OpenLogicalChannel** H.245. Un canal non fiable est utilisé pour acheminer les flux d'informations audio, commande audio, vidéo et commande vidéo. Une voie fiable est utilisée pour acheminer les flux de données et les flux d'informations de commande H.245. Il n'existe aucune relation entre une voie logique et une voie physique.

3.29 passerelle média: passerelle qui convertit les médias fournis en un type de réseau selon le format requis dans un autre type de réseau. Par exemple, une passerelle média peut recevoir des canaux supports provenant d'un réseau à commutation de circuits (c'est-à-dire des signaux DS0) et des flux médias provenant d'un réseau en mode paquet (p. ex. des flux de protocole RTP dans un réseau IP). Cette passerelle possède la capacité de traiter des signaux audio, vidéo et T.120 isolés ou combinés de façon quelconque ainsi que la capacité de conversion de média en exploitation duplex. La passerelle média peut également restituer des messages audio/vidéo et remplir d'autres fonctions de réponse IVR ou de conférence média.

3.30 contrôleur de passerelle média (MGC, *media gateway controller*): dispositif commandant les parties de l'état d'appel qui se rapportent à la commande de connexion pour des voies médias dans une passerelle média.

3.31 conférence multipoint mixte: conférence à laquelle certains terminaux (D, E et F) (voir Figure 2) participent en mode centralisé, cependant que d'autres terminaux (A, B et C) y participent en mode décentralisé. Chaque terminal ignore le caractère mixte de la conférence, n'étant informé que du type de conférence à laquelle il participe. L'unité de commande multipoint (MCU) fait office de pont entre les deux types de conférences.

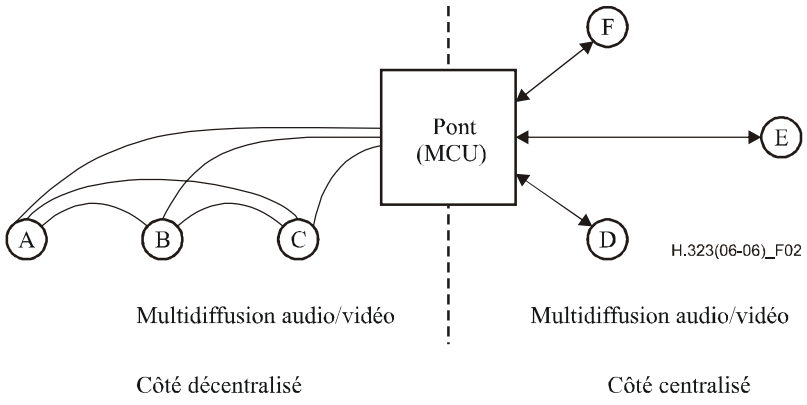


Figure 2/H.323 – Conférence multipoint mixte

3.32 multidiffusion: procédé de transmission d'unités PDU d'une source à de nombreuses destinations. Le mécanisme effectif (multidiffusion IP, multimonodiffusion, etc.) sous-jacent à ce procédé peut différer selon les technologies utilisées par les réseaux.

3.33 conférence multipoint: conférence entre trois terminaux ou plus. Ces terminaux peuvent faire partie du réseau ou du réseau à commutation de circuits. Une conférence multipoint doit toujours être gérée par un contrôleur multipoint. Pour chacun des divers types de conférence multipoint définis dans le présent paragraphe, un contrôleur multipoint par conférence est

nécessaire ainsi que, dans certains cas, un ou plusieurs ponts de conférence H.231 sur le RCC. Un terminal du réseau peut aussi participer à une conférence multipoint sur le RCC par l'intermédiaire d'une passerelle le raccordant à un pont de conférence du RCC. Il n'est pas nécessaire à cette fin d'utiliser un contrôleur multipoint.

3.34 pont de conférence; unité de commande multipoint (MCU, *multipoint control unit*): extrémité d'un réseau permettant à trois terminaux ou plus, et leurs passerelles, de participer à une conférence multipoint. Peuvent aussi être raccordés deux terminaux participant à une conférence point à point susceptible de devenir ultérieurement une conférence multipoint. Le pont de conférence fonctionne généralement à la manière d'un pont de conférence H.231, mais un processeur audio n'est pas obligatoire. Le pont de conférence se compose de deux parties: un contrôleur multipoint obligatoire et des processeurs multipoint facultatifs. Dans le cas le plus simple, un pont de conférence peut être constitué uniquement d'un contrôleur multipoint, sans processeurs multipoints. Un pont de conférence peut également être inséré dans une conférence par le portier sans avoir été explicitement appelé par une des extrémités.

3.35 contrôleur multipoint (MC, *multipoint controller*): entité H.323 du réseau qui assure la gestion d'au moins trois terminaux participant à une conférence multipoint. Peuvent aussi être raccordés deux terminaux participant à une conférence point à point susceptible de devenir ultérieurement une conférence multipoint. Le contrôleur multipoint permet de négocier avec tous les terminaux les moyens à mettre en œuvre pour parvenir à établir des communications de même niveau. Il peut également exercer un contrôle au niveau des ressources de la conférence pour déterminer par exemple l'entité qui transmet en mode multidiffusion les signaux vidéo. Le contrôleur multipoint n'assure pas le mélange ou la commutation des signaux audio, vidéo et de données.

3.36 processeur multipoint (MP, *multipoint processor*): entité H.323 du réseau qui assure le traitement centralisé des flux de signaux audio, vidéo et/ou de données dans une conférence multipoint. Le processeur multipoint assure le mélange, la commutation ou d'autres opérations de traitement des flux de médias sous la supervision du contrôleur multipoint. Celui-ci peut traiter un ou plusieurs flux de médias selon le type de conférence pris en charge.

3.37 multimonodiffusion: processus de transfert d'unités PDU dans lequel une extrémité envoie plusieurs copies d'un flux de médias, mais à différentes extrémités. Ce processus peut être nécessaire dans les réseaux qui ne prennent pas en charge la multidiffusion.

3.38 adresse réseau: adresse de couche Réseau d'une entité H.323 définie par le protocole de couche (inter)réseaux en usage [par exemple une adresse de protocole Internet (IP)]. Cette adresse est mappée à l'adresse de couche 1 du système considéré, par l'un des moyens définis dans le protocole de connexion (d'interconnexion) de réseaux.

3.39 réseau (en mode paquet): tout support partagé, commuté ou point à point qui assure des communications d'homologue à homologue entre au moins deux extrémités au moyen d'un protocole de transport en mode paquet.

3.40 conférence point à point: conférence entre deux terminaux, établie directement entre deux terminaux H.323 ou entre un terminal H.323 et un terminal du RCC par l'intermédiaire d'une passerelle. Communication entre deux terminaux (voir appel).

3.41 voie RAS: voie non fiable utilisée pour acheminer les messages d'enregistrement, d'admission, de changement de largeur de bande et d'indication d'état (selon la Rec. UIT-T H.225.0) entre deux entités H.323.

3.42 voie fiable: connexion de transport utilisée pour transmettre de manière fiable un flux d'information depuis sa source jusqu'à une ou plusieurs destinations.

3.43 transmission fiable: transmission de messages d'un émetteur à un récepteur par transmission de données en mode connexion. Le service de transmission garantit que les messages

seront transmis au récepteur en séquence, sans erreur et avec contrôle du flux de transmission, pendant la durée de la connexion de transport.

3.44 session (de protocole) RTP: session définie, pour chaque participant, par une paire donnée d'adresses de transport de destination (une adresse de réseau plus une paire d'identificateurs de points TSAP pour le protocole RTP et pour le protocole RTCP). La paire d'adresses de transport de destination peut être commune à tous les participants, comme dans le cas de la multidiffusion en protocole IP, ou être différente pour chacun d'entre eux, comme dans le cas d'adresses de réseau monodiffusion individuelles. Dans une session multimédia, les médias audio et vidéo sont acheminés au cours de sessions de protocole RTP distinctes, avec leurs propres paquets de protocole RTCP. Les sessions de protocole RTP multiples sont distinguées par des adresses de transport différentes.

3.45 réseau à commutation de circuits (RCC): réseau public ou privé de télécommunication avec commutation – RTGC, RNIS-BE ou RNIS-LB, par exemple.

NOTE – Bien que le RNIS-LB ne soit pas, au sens strict, un réseau à commutation de circuits, il offre certaines des caractéristiques d'un RCC parce qu'il utilise des circuits virtuels commutés.

3.46 terminal: un terminal H.323 est une extrémité du réseau assurant en temps réel des communications bidirectionnelles avec un autre terminal, une autre passerelle ou un autre pont de conférence H.323. Ces communications permettent l'échange de commandes, d'indications, de signaux audio, d'images animées vidéo en couleur et/ou de données entre les deux terminaux. Un terminal peut transmettre la parole uniquement, la parole et les données, la parole et la vidéo ou la parole, les données et la vidéo.

3.47 adresse de transport: adresse de couche Transport d'une entité H.323 adressable, telle que définie par l'ensemble de protocoles (inter)réseaux en usage. L'adresse de transport d'une entité H.323 se compose de l'adresse du réseau, assortie de l'identificateur du protocole TSAP de l'entité H.323 adressable.

3.48 connexion de transport: association établie par une couche de transport entre deux entités H.323 aux fins du transfert de données. Dans le contexte de la présente Recommandation, une connexion de transport assure la transmission fiable de l'information.

3.49 passerelle de jonction: passerelle qui connecte deux réseaux de même type (p. ex. deux réseaux SS7 ou deux réseaux QSIG), dans laquelle la tunnellisation sert à obtenir une transparence complète et une véritable fonction de cascade.

3.50 identificateur de point TSAP: élément d'information utilisé pour multiplexer plusieurs connexions de transport du même type sur une même entité H.323, toutes les connexions de transport partageant la même adresse de réseau (par exemple, le numéro d'accès dans un environnement TCP/UDP/IP). Les identificateurs de point TSAP peuvent être (pré)assignés statistiquement par une autorité internationale ou peuvent être attribués dynamiquement pendant l'établissement d'une communication. Les identificateurs de point TSAP assignés dynamiquement ont un caractère transitoire, c'est-à-dire que leurs valeurs ne sont valides que pendant la durée d'une seule communication.

3.51 monodiffusion: processus de transmission de messages d'une source à une destination.

3.52 voie non fiable: voie de communication logique utilisée pour la transmission non fiable d'un flux d'information de la source de celui-ci à une ou plusieurs destinations.

3.53 transmission non fiable: transmission de messages d'un émetteur à un ou plusieurs récepteurs, par transmission de données en mode sans connexion. Le service de transmission assurera *au mieux de ses capacités* la remise de l'unité PDU, ce qui veut dire que les messages transmis par l'émetteur pourront être perdus, dupliqués ou reçus dans n'importe quel ordre par les récepteurs (ou l'un quelconque d'entre eux).

3.54 identificateur de point TSAP communément admis: identificateur de point TSAP qui a été attribué par une autorité (internationale) chargée de l'assignation des identificateurs de point TSAP pour un protocole donné de connexion (d'interconnexion) de réseaux et les protocoles de transport correspondants (par exemple, l'autorité IANA pour les numéros d'accès des protocoles TCP et UDP). Le caractère unique de cet identificateur est garanti dans le contexte du protocole considéré.

3.55 zone: ensemble des terminaux (Tx), passerelles (GW) et ponts de conférence (MCU) gérés par un même portier (GK) (voir Figure 3). Une zone n'a qu'un seul portier. La zone peut être indépendante de la topologie du réseau et peut être constituée de plusieurs segments de réseau connectés à l'aide de routeurs (R) ou d'autres dispositifs.

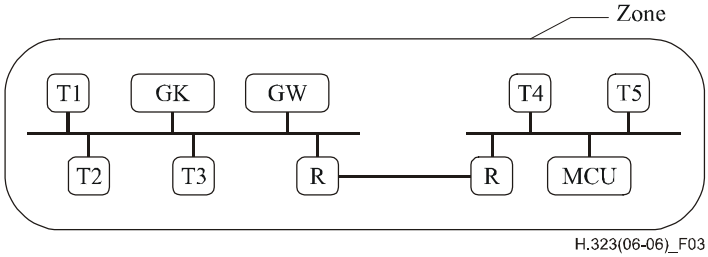


Figure 3/H.323 – Zone

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

4CIF 4 fois le format CIF (format intermédiaire commun)

16CIF 16 fois le format CIF

ABNF formalisme BNF étendu (*augmented Backus-Naur Form*)

ABR débit disponible (*available bit rate*)

ABT/DT transfert de bloc ATM/transmission différée (*ATM block transfer/delayed transmission*)

ABT/IT transfert de bloc ATM/transmission immédiate (*ATM block transfer/immediate transmission*)

ACF confirmation d'admission (*admission confirmation*)

AGW passerelle d'accès (*access gateway*)

APE entité de protocole d'application (*application protocol entity*)

ARJ refus d'admission (*admission reject*)

ARQ demande d'admission (*admission request*)

ATC capacité de transfert ATM (*ATM transfer capability*)

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

BAS signal d'allocation de débit (*bit rate allocation signal*)

BCF confirmation de changement de largeur de bande (*bandwidth change confirmation*)

BCH Bose, Chaudhuri et Hocquengham

B-HLI information de couche supérieure large bande (*broadband high layer information*)

BRJ refus de largeur de bande (*bandwidth change reject*)

BRQ demande de largeur de bande (*bandwidth change request*)

BTC capacité de transfert large bande (*broadband transfer capability*)

CAS signalisation voie par voie (*channel associated signalling*)

CDV variation du délai cellulaire (*cell delay variation*)

CED tonalité d'identification du terminal appelé (*called terminal identification tone*)

CER taux d'erreur de cellules (*cell error ratio*)

CID identificateur de conférence (*conference identifier*)

CIF format intermédiaire commun (*common intermediate format*)

CLR taux de perte de cellules (*cell loss ratio*)

CMR débit de cellules insérées à tort (dystaxiques) (*cell misinsertion rate*)

CNG tonalité appellante (*calling tone*)

CTD temps de transfert de cellules (*cell transfer delay*)

DBR débit déterministe (*deterministic bit rate*)

DCF confirmation de désengagement (*disengage confirmation*)

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

DRQ demande de désengagement (*disengage request*)

DSVD voix et données numériques simultanées (*digital simultaneous voice and data*)

DTMF multifréquence à deux tonalités (*dual-tone multifrequency*)

FAS signalisation en mode service par service (*facility associated signalling*)

FIR demande interne (*full intra request*)

GCC commande de conférence générique (*generic conference control*)

GCF confirmation de portier (*gatekeeper confirmation*)

GID identificateur d'appel mondial (*global call identifier*)

GIT transport d'identificateur générique (*generic identifier transport*)

GK portier (*gatekeeper*)

GQS qualité de service garantie (*guaranteed quality of service*)

GRJ refus de portier (*gatekeeper reject*)

GRQ demande de portier (*gatekeeper request*)

GW passerelle (*gateway*)

HDLC commande de liaison de données à haut niveau (*high level data link control*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IACK accusé de réception d'information (*information acknowledgment*)

IANA Autorité chargée de l'assignation des numéros Internet (*Internet assigned numbers authority*)

ID identificateur

IE élément d'information (*information element*)

IMT jonction entre machines (*inter-machine trunk*)

INAK accusé de réception d'information négatif (*information negative acknowledgment*)

IP protocole Internet (*Internet protocol*)

IPX échange de protocoles interréseaux (*internetwork protocol exchange*)

IRQ demande d'information (*information request*)

IRR réponse à demande d'information (*information request response*)

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

LAN réseau local (*local area network*)

LCF confirmation d'emplacement (*location confirmation*)

LRJ refus d'emplacement (*location reject*)

LRQ demande d'emplacement (*location request*)

MC contrôleur multipoint (*multipoint controller*)

MCS système de communication multipoint (*multipoint communications system*)

MCU pont de conférence; unité de commande multipoint (*multipoint control unit*)

MG passerelle média (*media gateway*)

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

MIME extensions de courrier Internet à fonctions multiples (*multipurpose Internet mail extensions*)

MP processeur multipoint (*multipoint processor*)

MTU unité de transmission maximale (*maximum transmission unit*)

NACK accusé de réception négatif (*negative acknowledge*)

NFAS signalisation autre qu'en mode service par service (*non-facility associated signalling*)

NNI interface réseau-réseau (*network-to-network interface*)

NSAP point d'accès au service de réseau (*network service access point*)

OLC message **openLogicalChannel** H.245

PDU unité de données en mode paquet (*packet data unit*)

PPP protocole point à point

PRI interface à débit primaire (*primary rate interface*)

QCIF quart de format intermédiaire commun (*quarter common intermediate format*)

QS qualité de service

QSIG signalisation entre points de référence Q définis dans [44]

RAS enregistrement, admission et statut (*registration, admission and status*)

RAST terminal d'émission-réception (*receive and send terminal*)

RCC réseau à commutation de circuits

RCF confirmation d'enregistrement (*registration confirmation*)

RCP réseau à commutation de paquets

RIP demande en cours (*request in progress*)

RNIS réseau numérique à intégration de services

RNIS-BE RNIS à bande étroite

RNIS-LB RNIS à large bande

RRJ refus d'enregistrement (*registration reject*)

RRQ demande d'enregistrement (*registration request*)

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

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

RTPC réseau téléphonique public commuté

SBE extension à un octet (*single byte extension*)

SBR1 configuration 1 de débit statistique (*statistical bit rate configuration 1*)

SBR2 configuration 2 de débit statistique (*statistical bit rate configuration 2*)

SBR3 configuration 3 de débit statistique (*statistical bit rate configuration 3*)

SCI indication de commande de service (*service control indication*)

SCM mode de communication sélectionné (*selected communications mode*)

SCR réponse de commande de service (*service control response*)

SDL langage de description et de spécification (*specification and description language*)

SECBR taux de blocs de cellules sévèrement erroné (*severely errored cell block ratio*)

SPX échange protocolaire séquentiel (*sequential protocol exchange*)

SQCIF sous-quart de format intermédiaire commun (*sub QCIF*)

SS7 système de signalisation n° 7

SSRC identificateur de source de synchronisation (*synchronization source identifier*)

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

TGW passerelle de jonction (*trunking gateway*)

TSAP point d'accès à un service de transport (*transport layer service access point*)

UCF confirmation de non-enregistrement (*unregister confirmation*)

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

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

UNI interface utilisateur-réseau (*user-to-network interface*)

URJ refus d'annulation d'enregistrement (*unregister reject*)

URQ demande d'annulation d'enregistrement (*unregister request*)

VC voie virtuelle (*virtual channel*)

5 Conventions

Les conventions utilisées dans la présente Recommandation sont les suivantes:

La forme "doit" indique une exigence obligatoire.

La forme "devrait" (ou "il convient") indique un comportement suggéré mais facultatif.

La forme "peut" indique un comportement facultatif plutôt qu'une Recommandation stricte.

Les références aux paragraphes, aux annexes et aux appendices renvoient aux points correspondants de la présente Recommandation, sauf si une autre spécification est expressément mentionnée. Par exemple, la mention "1.4" renvoie au § 1.4 de la présente Recommandation; la mention "6.4/H.245" renvoie au § 6.4 de la Rec. UIT-T H.245.

Dans toute la présente Recommandation, le terme "réseau" désigne tout réseau en mode paquet quelle que soit sa couche Physique sous-jacente ou son domaine géographique. Un réseau peut être un réseau local, un interréseau ou un autre réseau en mode paquet. Le terme "réseau à commutation de circuit" ou "RCC" est utilisé explicitement pour désigner des réseaux à commutation de circuit tels que le RTGC et le RNIS.

Dans le cas d'équipements qui existent à la fois sur le réseau en mode paquet et sur le réseau à commutation de circuits (RCC), la formulation adoptée permet de distinguer clairement les équipements du RCC. Ainsi, l'expression "pont de conférence" désigne toujours un pont de conférence H.323 du réseau en mode paquet. Un équipement du réseau à commutation de circuits est toujours désigné par l'expression "pont de conférence du RCC".

La présente Recommandation décrit l'utilisation de trois types différents de messages: H.245, RAS et signalisation d'appel H.225.0. Pour distinguer ces différents types de messages, on applique la convention suivante: les noms de messages et de paramètres sont des groupes de mots concaténés en caractères gras (**maximumDelayJitter**). Les noms de message RAS sont représentés par des abréviations de trois lettres (ARQ). Les noms de message de signalisation d'appel H.225.0 sont constitués de 1 ou de deux mots commençant par une majuscule (*Call Proceeding* – appel en cours).

6 Description du système

La présente Recommandation décrit les éléments des systèmes H.323. Il s'agit de terminaux, de passerelles, de portiers, de contrôleurs multipoint et de ponts de conférence. Ces éléments communiquent entre eux par la transmission de flux d'information. Les caractéristiques de ces éléments sont décrites dans le présent paragraphe.

6.1 Flux d'information

Les éléments de visiophonie communiquent par la transmission de flux d'information qui sont classés selon les différents signaux (vidéo, audio, de données, de commande de communication et de commande d'appel) repris en détail ci-dessous.

Les signaux audio contiennent la parole numérisée et codée. Afin de réduire le débit moyen des signaux audio, la fonction d'activation par la voix peut être offerte. Le signal audio est accompagné d'un signal de commande audio.

Les signaux vidéo contiennent les images animées, numérisées et codées. Ces images sont transmises à un débit inférieur ou égal à celui qui a été choisi compte tenu de l'échange de capacités. Le signal vidéo est accompagné d'un signal de commande vidéo.

Les signaux de données comprennent les images fixes, la télécopie, les documents, les fichiers informatiques et les autres flux de données.

Les signaux de commande de communication transmettent des données de commande entre éléments fonctionnels distants et assimilés et sont utilisés pour diverses fonctions (échange de capacités, ouverture et fermeture de voies logiques, commande de mode ou autres) intégrées à la commande de communication.

Les signaux de commande d'appel sont utilisés pour l'établissement et la libération des communications ainsi que pour d'autres fonctions de commande d'appel.

Les flux d'information décrits ci-dessus sont formatés et envoyés à l'interface réseau comme indiqué dans la Rec. UIT-T H.225.0.

6.2 Caractéristiques des terminaux

Un terminal H.323 type est représenté à la Figure 4. Le schéma de principe montre les interfaces de l'équipement d'usager, le codec vidéo, le codec audio, l'équipement télématique, la couche H.225.0, les fonctions de commande du système et l'interface avec le réseau en mode paquet. Tous les terminaux H.323 doivent comprendre un module de commande du système, une couche H.225.0, une interface réseau et un codec audio. Le codec vidéo et les applications de données d'usager sont facultatifs.

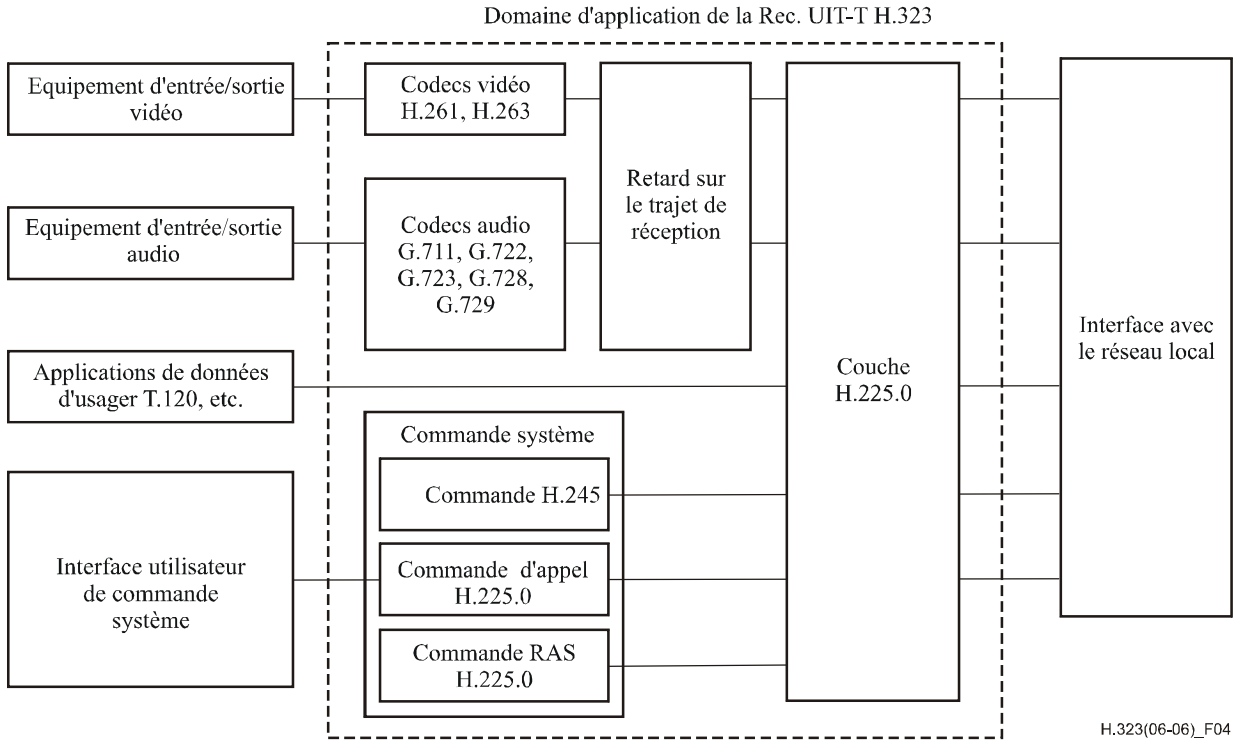


Figure 4/H.323 – Terminal H.323

6.2.1 Eléments de terminal ne relevant pas du domaine d'application de la présente Recommandation

Les éléments suivants ne relèvent pas du domaine d'application de la présente Recommandation et n'y sont donc pas définis:

- dispositifs audio annexes permettant de détecter la parole d'activation, microphone et haut-parleur, appareils téléphoniques ou équivalents, mélangeurs pour microphones multiples et dispositifs d'annulation de l'écho acoustique;
- équipements vidéo annexes pour caméras et écrans de contrôle assurant les fonctions de commande et de sélection correspondantes, le traitement des signaux vidéo propre à améliorer la compression ou des fonctions de subdivision de l'écran;
- interfaces avec les applications de données et interfaces annexes avec les utilisateurs, utilisant les services de données T.120 ou d'autres services analogues sur le canal de données;
- interface annexe avec le réseau en mode paquet, prenant en charge la signalisation et les niveaux de tension appropriés, conformément aux normes nationales et internationales;
- module de commande du système par l'utilisateur, interface avec l'utilisateur et exploitation.

6.2.2 Eléments de terminal relevant du domaine d'application de la présente Recommandation

Les éléments suivants relèvent du domaine d'application de la présente Recommandation: ils sont donc soumis à normalisation et définis dans la présente Recommandation:

- le codec vidéo (H.261, etc.) code le signal vidéo provenant de la source vidéo (c'est-à-dire la caméra) pour transmission et décode le code vidéo reçu qui est restitué sur un écran vidéo;
- le codec audio (G.711, etc.) code le signal audio provenant du microphone pour transmission, et décode le code audio reçu qui est restitué par le haut-parleur;
- le canal de données assure diverses applications de télématique: tableaux électroniques, transfert d'images fixes, échange de fichiers, accès à des bases de données, conférences audiographiques, etc. L'application de données normalisée pour la conférence audiographique en temps réel est celle de la Rec. UIT-T T.120. D'autres applications et protocoles peuvent aussi être utilisés par voie de négociation dans le cadre de la Rec. UIT-T H.245, comme indiqué au § 6.2.7;
- le module de commande du système (H.245, H.225.0) assure la signalisation nécessaire au bon fonctionnement du terminal H.323. Il assure la commande d'appel, l'échange des capacités, la signalisation des commandes et des indications et fournit des messages d'ouverture des voies logiques ou décrivant en détail le contenu de celles-ci;
- la couche H.225.0 (H.225.0) assure le formatage des flux de signaux vidéo, audio, de données et de commande à transmettre à l'interface réseau, et extrait les flux des signaux vidéo, audio, de données et de commande reçus des messages entrants provenant de l'interface réseau. En outre, elle assure le tramage logique, la numérotation séquentielle, la détection et la correction des erreurs, selon les besoins, pour chaque type de média.

6.2.3 Interface avec le réseau en mode paquet

L'interface avec le réseau en mode paquet étant propre à l'implémentation, elle ne relève pas du domaine d'application de la présente Recommandation. Elle doit toutefois fournir les services décrits dans la Rec. UIT-T H.225.0. Cela oblige à assurer un service fiable (TCP, SPX, par exemple) de bout en bout pour la voie de commande, les canaux de données et la voie de signalisation d'appel H.245. Un service de bout en bout non fiable (UDP, IPX, par exemple) est obligatoire pour les voies audio, les voies vidéo et la voie RAS. Ces services peuvent être assurés en mode duplex ou simplex, en monodiffusion ou multidiffusion selon l'application, les capacités des terminaux et la configuration du réseau.

6.2.4 Codec vidéo

Le codec vidéo est facultatif. Si la capacité vidéo est fournie, elle doit l'être conformément aux prescriptions de la présente Recommandation. Tous les terminaux H.323 qui assurent des communications vidéo doivent pouvoir coder et décoder les signaux vidéo selon le format QCIF H.261. A titre facultatif, un terminal peut aussi être à même de coder et de décoder des signaux vidéo selon les autres modes H.261 ou H.263. Un terminal conforme à la Rec. UIT-T H.263 et acceptant le format CIF ou une résolution plus élevée doit aussi pouvoir accepter le format CIF H.261. Tous les terminaux conformes à la Rec. UIT-T H.263 doivent pouvoir accepter le format QCIF H.263. Sur le réseau, les codecs H.261 et H.263 doivent être utilisés avec correction d'erreurs BCH et sans tramage de correction d'erreurs.

Un terminal peut aussi avoir la capacité de coder et décoder les signaux vidéo selon le format de la Rec. UIT-T H.264. La Rec. UIT-T H.241 définit la négociation des modes vidéo H.264.

On peut aussi négocier, dans le cadre H.245, l'utilisation d'autres codecs vidéo et d'autres formats d'image de manière à permettre l'établissement de plusieurs voies vidéo d'émission et/ou de

réception par l'intermédiaire de la voie de commande H.245. Le terminal H.323 peut éventuellement émettre sur plusieurs voies vidéo à la fois, par exemple pour acheminer la voix du locuteur et les signaux vidéo d'une deuxième source. Le terminal H.323 peut éventuellement disposer de plusieurs voies vidéo de réception à la fois, par exemple pour présenter plusieurs participants à l'écran dans une conférence multipoint répartie.

Le débit des signaux vidéo, le format d'image et les différents algorithmes que peut accepter le décodeur sont définis durant l'échange des capacités selon H.245. Le codeur a toute liberté de transmettre l'une quelconque des capacités de l'ensemble de celles du décodeur. Le décodeur devrait avoir la possibilité d'émettre des demandes par les moyens définis dans H.245 pour demander un mode particulier, mais le codeur est autorisé à ignorer purement et simplement ces demandes si les modes demandés ne sont pas obligatoires. Les décodeurs qui indiquent pouvoir accepter une option algorithmique donnée doivent aussi pouvoir accepter des flux de bits vidéo qui n'utilisent pas cette option.

Les terminaux H.323 doivent pouvoir fonctionner de manière asymétrique tant pour ce qui est des débits vidéo, que pour les fréquences d'image, ainsi que pour les résolutions d'image si plusieurs résolutions sont acceptées. Un terminal pouvant transmettre le format CIF pourra ainsi transmettre le format QCIF tout en recevant des images au format CIF.

A l'ouverture de chaque voie logique vidéo, le mode de fonctionnement choisi à utiliser sur cette voie est indiqué au récepteur dans le message d'ouverture de voie logique **openLogicalChannel** H.245. L'en-tête figurant à l'intérieur de la voie logique vidéo indique le mode effectivement utilisé pour chaque image, dans les limites de la capacité spécifiée pour le décodeur.

Le flux de signaux vidéo est formaté comme indiqué dans la Rec. UIT-T H.225.0.

6.2.4.1 Présence continue à l'aide d'un terminal

Les terminaux H.323 peuvent recevoir plusieurs voies vidéo, en particulier pour des conférences multipoint. En pareil cas, le terminal H.323 peut avoir à assurer une fonction de mélange ou de commutation vidéo afin de présenter le signal vidéo à l'usager. Cette fonction peut exiger la présentation à l'usager de signaux vidéo provenant de plusieurs terminaux. Le terminal H.323 doit utiliser les capacités simultanées H.245 pour indiquer le nombre de flux de signaux vidéo simultanés qu'il peut décoder. La capacité simultanée d'un terminal ne doit pas limiter le nombre de flux de signaux vidéo multidiffusés pendant une conférence (ce choix est laissé au contrôleur multipoint).

6.2.5 Codec audio

Tous les terminaux H.323 doivent être munis d'un codec audio et pouvoir coder et décoder la parole conformément à la Rec. UIT-T G.711. Ils doivent tous pouvoir émettre et recevoir en loi A et en loi μ. Un terminal peut facultativement être à même de coder et de décoder la parole au moyen d'autres codecs audio qui peuvent être signalés via négociation H.245. L'algorithme audio utilisé par le codeur doit être calculé pendant l'échange des capacités selon la Rec. UIT-T H.245. Le terminal H.323 devrait pouvoir fonctionner en mode asymétrique pour toutes les capacités audio qu'il a déclarées pour l'ensemble de capacités considéré; ainsi, il devrait pouvoir émettre en mode G.711 et recevoir en mode G.728, s'il est capable de l'un comme de l'autre.

Si le flux audio G.723.1 est fourni, le codec audio doit être capable de coder et de décoder en mode 5,3 kbit/s comme en mode 6,3 kbit/s.

Le flux de signaux audio est formaté comme indiqué dans la Rec. UIT-T H.225.0.

Le terminal H.323 peut éventuellement envoyer plusieurs voies audio à la fois, par exemple pour permettre la transmission de deux langues.

Les paquets de signaux audio devraient être remis périodiquement à la couche de transport, à des intervalles déterminés par la Recommandation en vigueur sur les codecs audio (intervalle de trame audio). Chaque paquet de signaux audio doit être remis 5 ms au plus tard après un multiple entier de l'intervalle de trame audio, à compter de la remise de la première trame audio (gigue de temps de propagation des signaux audio). Les codeurs audio capables de limiter encore la gigue de temps de propagation de leurs signaux audio peuvent le signaler à l'aide du paramètre **maximumDelayJitter** H.245 de la structure **h2250Capability** contenue dans un message d'ensemble de capacités de terminal, de manière que les récepteurs puissent éventuellement réduire leurs mémoires tampons de temps de propagation de gigue. Le temps de propagation de gigue diffère du champ de gigue de réception intermédiaire du protocole RTCP.

NOTE – Le point de mesure de la gigue de temps de propagation maximal est situé à l'entrée de la couche Transport du réseau. L'empilage du réseau, le réseau, le programme pilote et la gigue de carte d'interface ne sont pas traités ici.

6.2.5.1 Mélange audio

Les terminaux H.323 peuvent recevoir plusieurs voies audio, en particulier pour des conférences multipoint. En pareil cas, le terminal H.323 peut devoir assurer une fonction de mélange des signaux audio afin de présenter à l'usager un signal audio composite. Le terminal H.323 doit utiliser les capacités simultanées H.245 pour indiquer le nombre de flux de signaux audio simultanés qu'il peut décoder. La capacité simultanée d'un terminal ne doit pas limiter le nombre de flux de signaux audio multidiffusés au cours d'une conférence.

6.2.5.2 Décalage temporel maximal entre les signaux audio/vidéo à l'émission

Pour pouvoir déterminer de manière appropriée la taille de leurs mémoires tampons de réception, les terminaux H.323 doivent émettre le message d'indication de décalage temporel maximal **h2250MaximumSkewIndication** pour indiquer le décalage temporel maximal entre les signaux audio et vidéo tels qu'ils sont remis à la couche de transport du réseau. Le message **h2250MaximumSkewIndication** devra être envoyé pour chaque pays de voies logiques audio et vidéo associées. Cela n'est pas nécessaire pour les conférences hybrides et pour les conférences ne faisant intervenir que des signaux audio. La synchronisation labiale, si elle est souhaitée, doit être assurée au moyen d'horodateurs.

6.2.5.3 Exploitation à bas débit

Le flux audio G.711 ne peut pas être utilisé dans une conférence H.323 acheminée par des liens ou segments à bas débit (< 56 kbit/s). Une extrémité utilisée pour des communications multimédias au moyen de tels liens ou segments à bas débit devrait avoir un codec audio capable de coder et de décoder la parole conformément à la Rec. UIT-T G.723.1. Une extrémité utilisée pour des communications audio seulement au moyen de tels liens ou segments à bas débit devrait avoir un codec audio capable de coder et de décoder la parole conformément à la Rec. UIT-T G.729. Une extrémité peut prendre en charge plusieurs codecs audio afin d'assurer la plus large interopérabilité possible avec les extrémités qui ne prennent en charge qu'un seul codec audio à bas débit. Cette extrémité doit indiquer, dans les procédures H.245 d'échange de capacités en début de communication, la capacité de réception des signaux audio conformément aux Recommandations applicables en la matière, qui peut être prise en charge dans le cadre des limitations de débit connues pour la connexion. Une extrémité qui ne possède pas cette capacité de réception de signaux audio à bas débit peut ne pas être en mesure de fonctionner lorsque la connexion de bout en bout contient un ou plusieurs segments à bas débit.

L'extrémité doit également satisfaire à la prescription du § 6.2.5 afin d'être capable de coder et de décoder la parole conformément à la Rec. UIT-T G.711. Cependant, l'extrémité n'a pas besoin d'indiquer cette capacité s'il est certain qu'il va communiquer au moyen d'un segment à bas débit. Si une extrémité n'est pas informée de la présence, dans la connexion de bout en bout, de liens ou segments de capacité insuffisante pour prendre en charge les signaux audio G.711 (ainsi que

d'autres flux médias éventuellement prévus), cette extrémité doit déclarer sa capacité de réception audio conformément à la Rec. UIT-T G.711.

6.2.6 Temps de propagation sur la voie de réception

Le temps de propagation sur la voie de réception comprend le temps ajouté au flux de médias afin de maintenir la synchronisation et de tenir compte de la gigue de réception des paquets sur le réseau. On peut éventuellement retarder les flux de médias sur la voie de traitement des signaux dans le récepteur afin de maintenir la synchronisation avec les autres flux de médias. Par ailleurs, on peut éventuellement retarder un flux de média afin d'autoriser des temps de propagation sur le réseau propres à engendrer la gigue de réception des paquets. Un terminal H.323 ne doit pas ajouter de retard à cette fin dans sa voie de médias d'émission.

Les points de traitement intermédiaires comme les ponts de conférence ou les passerelles peuvent modifier les informations des étiquettes temporelles vidéo et audio. Ces points doivent transmettre des étiquettes temporelles et des numéros de séquence audio et vidéo dûment modifiés, reflétant les signaux qu'ils ont transmis. Les extrémités de réception peuvent ajouter un retard approprié dans la voie audio afin d'assurer la synchronisation labiale.

6.2.7 Canal de données

On peut utiliser un ou plusieurs canaux de données. Le canal de données peut être unidirectionnel ou bidirectionnel selon les caractéristiques de l'application de données.

La Rec. UIT-T T.120 régit par défaut l'interopérabilité des données entre un terminal H.323 et les terminaux H.323, H.324, H.320 ou H.310. Pour toute application de données facultative implémentée selon une ou plusieurs des Recommandations de l'UIT-T négociables dans le cadre de la Rec. UIT-T H.245, l'application T.120 équivalente, s'il en existe, doit être une de celles qui sont assurées.

Il est à noter que les applications de données non normalisées (**dataApplicationCapability.application = non-standard** application) et les données d'usager transparentes (**dataApplicationCapability.application = userData** application, **dataProtocolCapability = transparent**) peuvent être utilisées, que l'application T.120 équivalente soit ou non assurée.

La capacité T.120 doit être indiquée comme suit: **dataApplicationCapability.application = t120** application, **dataProtocolCapability = separateLANStack**.

Dans le cadre de la capacité **MediaDistributionCapability**, la structure **distributedData** doit être utilisée si la multidiffusion T.120 est disponible et la structure **centralizedData** si la monodiffusion T.120 est disponible. Tout nœud qui prend en charge la capacité de données T.120 doit prendre en charge la pile de monodiffusion normalisée T.123.

Dans le message **openLogicalChannel**, le choix **distribution** de la structure **NetworkAccessParameters** est mis à la valeur **unicast** si la capacité T.123 doit être utilisée ou à la valeur **multicast** si la capacité de l'Annexe A/T.125 doit être utilisée. Le choix **networkAddress** est mis à la valeur **localAreaAddress**, qui doit toujours faire partie d'une structure **unicastAddress**. Dans la séquence **iPAddress**, le champ **network** est mis à l'adresse IP binaire et l'identificateur **tsapIdentifier** est mis à la valeur désignant l'accès dynamique sur lequel la pile T.120 va émettre ou recevoir.

Le canal de données est formatée comme indiqué dans la Rec. UIT-T H.225.0.

6.2.7.1 Canaux de données T.120

La connexion T.120 est établie pendant un appel H.323 faisant partie intégrante de la communication. Les procédures d'établissement de la connexion T.120 avant la connexion H.323 feront l'objet d'un complément d'étude.

Les procédures normales d'établissement des communications décrites au § 8.1 sont appliquées. Une fois que l'on a procédé à l'échange des capacités, un canal logique bidirectionnel doit être ouvert pour la connexion T.120, conformément aux procédures H.245 normales indiquant qu'une nouvelle connexion doit être créée (voir la description ci-après).

Une des deux entités peut lancer l'ouverture d'un canal logique bidirectionnel pour une connexion T.120 en envoyant le message d'ouverture de voie logique **openLogicalChannel** et en appliquant ensuite les procédures de la Rec. UIT-T H.245 relatives aux canaux logiques bidirectionnels.

Pour que l'ouverture de la voie logique soit effective, l'entité effectuant le lancement doit envoyer un message **openLogicalChannel** où les paramètres **forwardLogicalChannelParameters** et **reverseLogicalChannelParameters** indiquent qu'un canal de données T.120 doit être ouvert. Cette entité doit inclure une adresse de transport dans le message **openLogicalChannel**. L'extrémité homologue peut choisir d'ignorer cette adresse de transport. Une extrémité peut utiliser un numéro d'accès dynamique pour l'adresse de transport T.120 au lieu d'utiliser l'accès 1503 comme spécifié dans la Rec. UIT-T T.123. Si l'entité homologue (celle qui répond) accepte cette voie logique, elle doit confirmer l'ouverture de la voie logique en utilisant le message d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck**. Dans ce message, l'entité qui répond doit inclure une adresse de transport même s'il attend de l'initiateur qu'il lance l'appel T.120. Dans tous les cas, l'adresse de transport pour la connexion T.120 doit figurer dans le paramètre **separateStack** et doit rester valide pendant la durée de la voie logique.

Dans le message **openLogicalChannel**, l'option **t120SetupProcedure** de la structure **NetworkAccessParameters** doit être mise à une valeur indiquant au répondeur la façon dont l'initiateur voudrait établir l'appel T.120. Le répondeur a la possibilité de passer outre à cette préférence. Le message **originateCall** indique que l'initiateur voudrait que le répondeur lance l'appel. Le message **waitForCall** indique que l'initiateur voudrait que le répondeur reçoive l'appel. Le message **issueQuery** n'est pas utilisé lors de l'indication d'une préférence.

Dans le message **openLogicalChannelAck**, l'option **t120SetupProcedure** de la structure **NetworkAccessParameters** doit être mise à une valeur indiquant à l'initiateur la façon dont l'appel T.120 sera établi. Si aucune des deux extrémités n'a de préférence, l'appel T.120 doit être établi dans le même sens que l'appel H.323. Le message **originateCall** indique à l'initiateur qu'il peut lancer un appel. Le message **waitForCall** indique à l'initiateur qu'il va recevoir l'appel. L'émetteur de l'appel, quel qu'il soit, enverra soit une demande de jonction soit une demande d'invitation, selon l'extrémité qui a été déterminée comme étant maître ou esclave (le maître est toujours hiérarchiquement supérieur dans la conférence T.120). Le message **issueQuery** peut être utilisé par une passerelle pour indiquer à l'initiateur qu'il doit lancer l'appel et envoyer une demande d'interrogation à l'extrémité distante. Il doit ensuite établir la conférence T.120 conformément au contenu de la réponse à l'interrogation (comme décrit dans la Rec. UIT-T T.124).

Si possible, l'appel T.120 doit être établi dans le même sens que l'appel H.323. L'initiateur du message d'ouverture OLC ne doit pas indiquer de préférence, à moins qu'il ne soit nécessaire de modifier ce comportement par défaut. Lorsque l'initiateur indique une préférence, le répondeur ne doit pas y passer outre, sauf si cela est nécessaire. Si aucune préférence n'est indiquée, le répondeur doit spécifier la valeur par défaut, à moins qu'il ne soit nécessaire d'opérer autrement.

Dans les messages **openLogicalChannel** et **openLogicalChannelAck**, le paramètre **associateConference** doit être mis à "FALSE".

Pour la connexion T.120, il faut suivre les procédures du protocole T.123 pour la pile de protocoles indiquée dans la capacité **dataProtocolCapability** sauf que les adresses de transport – comme cela est décrit ci-dessus – doivent servir pour l'établissement de la connexion.

Si une extrémité est le contrôleur MC actif ou le maître dans une conférence qui comporte le protocole T.120, il y a lieu que cette extrémité puisse également commander le nœud fournisseur supérieur T.120.

Si une extrémité a l'intention de créer une conférence qui inclut des données audio et/ou vidéo plus T.120, la voie de commande H.245 doit être établie avant la connexion T.120. Cela s'applique aux opérations de création, de jonction et d'invitation pour une conférence, ainsi qu'aux actions d'un contrôleur MC. Les procédures d'établissement d'appel H.323 doivent être utilisées pour établir le contrôleur MC (éventuel) avant qu'une connexion T.120 soit créée.

Pour établir une connexion T.120 au moyen d'une demande GCC-Join, les extrémités doivent connaître le nom de la conférence T.120. Si un nom alias (pseudonyme) existe pour représenter le nom d'une conférence H.323 (**conferenceAlias**), le texte qui a été utilisé pour l'alias de conférence doit normalement être utilisé comme portion textuelle du nom de conférence T.120. De même, l'identificateur CID H.323 devrait être utilisé comme nom numérique de conférence T.120, comme suit. Chaque octet de l'identificateur CID H.323 est converti en une série de trois caractères ASCII qui représentent la valeur décimale de l'octet en cours de conversion. On notera que cela implique que la valeur de certains octets d'identificateur CID soit convertie de façon que des caractères "0" soient utilisés pour le bourrage, le résultat devant être une chaîne de 48 caractères ASCII.

Un processeur multipoint T.120 peut être interrogé pour obtenir une liste des conférences existantes. L'identificateur CID H.323 peut être reconstruit par reconversion du nom numérique de conférence T.120 en chaîne de 16 octets. De même, le nom textuel de conférence peut être utilisé comme alias de conférence H.323. On notera qu'une interrogation de conférence T.124 peut être émise hors bande dans un message H.323, avant l'établissement d'une communication H.323 par une extrémité.

La terminaison de la conférence T.120 associée n'implique pas la terminaison de la communication H.323. En d'autres termes, le fait de fermer le canal T.120 ne doit affecter que le flux de données d'une communication H.323 et seulement ce flux. En revanche, lorsqu'une communication ou une conférence H.323 est terminée, la conférence T.120 associée doit également être terminée.

NOTE – L'exploitation de la connexion T.120 après la fin de l'établissement de la connexion est hors du domaine d'application de la présente Recommandation.

6.2.7.2 Commande d'équipement distant

Les extrémités H.323 peuvent prendre en charge la commande d'équipement distant via le protocole H.282. Celui-ci sera pris en charge dans un canal logique H.245 conformément à la Rec. UIT-T H.283, qui décrit l'acheminement par voie logique pour le protocole H.282 dans une conférence H.323.

Le protocole de la Rec. UIT-T H.282 peut aussi être utilisé par des systèmes T.120 et acheminé dans une entité APE T.120. Des systèmes H.323 peuvent aussi prendre en charge la commande d'équipement distant au moyen du protocole H.282 sur système T.120, mais il s'agit d'une option et les systèmes H.323 qui prennent en charge le protocole H.282 le feront conformément à la Rec. UIT-T H.283.

Si le protocole H.282 avec transport H.283 et le protocole H.282 avec transport T.120 sont possibles, deux protocoles peuvent être utilisés. La coordination des deux protocoles de couche inférieure dans le contexte du protocole H.282 est une question à traiter sur le plan local. Toutefois, le transport H.283 sera toujours actif afin de tenir compte de l'éventualité de l'entrée ultérieure de nœuds qui accepteraient le protocole H.282 avec transport H.283 mais pas avec transport T.120.

6.2.8 Fonction de commande H.245

La fonction de commande H.245 utilise la voie de commande H.245 pour acheminer les messages de commande de bout en bout qui régissent le fonctionnement d'une entité H.323, y compris l'échange des capacités, l'ouverture et la fermeture des voies logiques, les demandes de préférence de mode, les messages de contrôle de flux et les commandes et indications générales.

La signalisation H.245 est établie entre deux extrémités, une extrémité et un contrôleur multipoint, ou une extrémité et un portier. L'extrémité doit établir exactement une voie de commande H.245, pour chaque communication à laquelle elle participe. Cette voie doit utiliser les messages et les procédures de la Rec. UIT-T H.245. Il est à noter qu'un terminal, un pont de conférence, une passerelle ou un portier peut prendre en charge de nombreuses communications, et donc de nombreuses voies de commande H.245. La voie de commande H.245 doit être établie sur la voie logique 0. Celle-ci doit être considérée comme étant ouverte en permanence depuis l'établissement de la voie de commande H.245 jusqu'à la libération de cette voie. Les procédures normales d'ouverture et de fermeture des voies logiques ne doivent pas s'appliquer à la voie de commande H.245.

La Rec. UIT-T H.245 spécifie un certain nombre d'entités de protocole indépendantes qui assurent la signalisation d'extrémité à extrémité. Une entité de protocole est spécifiée par sa syntaxe (messages), sa sémantique et un ensemble de procédures qui spécifient l'échange de messages et l'interaction avec l'usager. Les extrémités H.323 doivent accepter la syntaxe, la sémantique et les procédures des entités de protocole suivantes:

- choix du mode maître ou esclave;
- échange des capacités;
- signalisation de voie logique;
- signalisation de canal logique bidirectionnel;
- signalisation d'ouverture de voie logique;
- demande de mode;
- détermination du temps de propagation aller et retour;
- signalisation de boucle de maintenance.

Les commandes et indications générales doivent être choisies parmi l'ensemble de messages figurant dans la Rec. UIT-T H.245. En outre, il est possible d'envoyer d'autres signaux de commande et d'indication, expressément définis comme étant destinés à être transférés dans la bande dans les flux de signaux vidéo, audio ou de données (voir la Recommandation appropriée pour déterminer si de tels signaux ont été définis).

On distingue quatre catégories de messages H.245: les messages de demande, de réponse, de commande et d'indication. Les messages de demande et de réponse sont utilisés par les entités de protocole. Les messages de demande appellent une action précise par le récepteur, y compris une réponse immédiate. Les messages de réponse répondent à une demande correspondante. Les messages de commande appellent une action précise, mais n'exigent pas de réponse. Les messages d'indication sont à caractère purement informatif et n'appellent aucune action ni réponse. Les terminaux H.323 doivent répondre à toutes les commandes et demandes H.245, comme indiqué dans l'Annexe A, et doivent transmettre des indications reflétant l'état du terminal.

Les terminaux H.323 doivent pouvoir analyser tous les messages H.245 **multimediaSystemControlMessage** (message de commande de système multimédia) et doivent envoyer et recevoir tous les messages nécessaires pour implémenter les fonctions obligatoires ainsi que les fonctions facultatives qu'accepte le terminal. On trouvera dans l'Annexe A un tableau répertoriant les messages H.245 obligatoires, facultatifs ou interdits pour les terminaux H.323. Les

terminaux H.323 doivent envoyer le message **functionNotSupported** (fonction non assurée) en réponse aux messages de demande, de réponse ou de commande non reconnus qu'ils reçoivent.

Une indication H.245 **userInputIndication** (indication de données d'usager) est disponible pour le transport de caractères alphanumériques de données d'usager à partir d'un bloc de touches ou clavier, équivalant aux signaux à tonalités multifréquences (DTMF, *dual-tone multifrequency*) utilisés en téléphonie analogique, ou de messages de numéros SBE de la Rec. UIT-T H.230. Cette indication peut être utilisée pour actionner manuellement des équipements éloignés, tels que des systèmes de messagerie vocale ou vidéo, des systèmes d'information pilotés par menu, etc. Les terminaux H.323 doivent assurer la transmission des caractères de données d'usager 0-9, "*" et "#". La transmission d'autres caractères est facultative.

Trois messages de demande H.245 sont incompatibles avec les paquets de commande du protocole RTCP. Les demandes de mise à jour rapide de l'image vidéo **videoFastUpdatePicture** et de mise à jour rapide de macroblocs de l'image vidéo **videoFastUpdateMB** de mise à jour rapide de groupes de blocs de l'image vidéo **videoFastUpdateGOB** de la Rec. UIT-T H.245 doivent être utilisées à la place des paquets de commande du protocole RTCP de demande interne (FIR, *full intra request*) et d'accusé de réception négatif (NACK, *negative acknowledgement*). La capacité à accepter les paquets FIR et NACK est signalée pendant l'échange de capacités H.245.

6.2.8.1 Echange des capacités

L'échange des capacités doit être effectué suivant les procédures de la Rec. UIT-T H.245, laquelle prévoit des capacités de réception et d'émission séparées, ainsi qu'une méthode permettant au terminal de décrire sa capacité à fonctionner simultanément dans différentes combinaisons de modes.

Les capacités de réception décrivent la capacité du terminal à recevoir et à traiter les flux d'information entrants. Les émetteurs doivent limiter les informations qu'ils transmettent à celles que le récepteur a indiqué pouvoir recevoir. L'absence d'indication de capacité de réception signifie que le terminal n'est pas équipé pour la réception (n'étant qu'un simple émetteur).

Les capacités d'émission décrivent la capacité du terminal à transmettre des flux d'information. Les capacités d'émission permettent d'offrir aux récepteurs un choix de modes de fonctionnement possibles, de manière que le récepteur puisse demander le mode de réception qu'il préfère. L'absence d'indication de capacité d'émission signifie que le terminal n'offre pas un choix de modes préférés au récepteur (sa capacité d'émission étant toutefois égale à la capacité du récepteur).

Les capacités de réception-émission décrivent l'aptitude d'un terminal à recevoir et à émettre des flux d'information lorsque ces capacités ne sont pas indépendantes et qu'il est exigé que ces capacités soient les mêmes dans les deux sens. Par exemple, une extrémité peut ne prendre en charge qu'un mode de fonctionnement symétrique de codec pour ses codecs (G.711 ou bien G.729 dans les deux sens et non G.711 dans un sens et G.729 dans l'autre). Une entité esclave doit aligner son ordre de préférence en matière de codec sur celui de l'entité maître; ainsi, si l'ordre de préférence de l'entité esclave est {G.729, G.711} et celui de l'entité maître {G.711, G.729}, l'entité esclave devra modifier son ordre de préférence pour qu'il devienne {G.711, G.729}. Même si l'ensemble des capacités du terminal avait déjà été fixé, il devra être remanié pour procéder à l'ouverture des canaux logiques.

Le terminal d'émission assigne à chaque mode individuel dans lequel le terminal peut fonctionner un numéro dans un tableau de capacités **capabilityTable**. Ainsi, des numéros séparés seront assignés à chacun des signaux audio G.723.1, audio G.728 et vidéo H.263 de format CIF.

Ces numéros de capacités sont groupés en structures **alternativeCapabilitySet** (ensemble de capacités de repli). Chaque **alternativeCapabilitySet** indique que le terminal peut fonctionner dans exactement un des modes listés dans l'ensemble. Par exemple, un listage **alternativeCapabilitySet**,

{G.711, G.723.1, G.728}, signifie que le terminal peut fonctionner dans l'un quelconque de ces modes audio, mais pas dans plusieurs d'entre eux.

Ces structures **alternativeCapabilitySet** sont groupées en structures **simultaneousCapabilities** (capacités simultanées). Chaque structure **simultaneousCapabilities** indique un ensemble de modes que le terminal peut utiliser simultanément. Ainsi, une structure **simultaneousCapabilities** contenant les deux structures **alternativeCapabilitySet** {H.261, H.263} et {G.711, G.723.1, G.728} signifie que le terminal peut utiliser l'un ou l'autre des codecs vidéo simultanément avec l'un quelconque des codecs audio. L'ensemble **simultaneousCapabilities** { {H.261}, {H.261, H.263}, {G.711, G.723.1, G.728} } signifie que le terminal peut utiliser deux voies vidéo et une voie audio simultanément: une voie vidéo de type H.261, une autre voie vidéo de type H.261 ou H.263 et une voie audio de type G.711, G.723.1 ou G.728.

Lorsqu'on utilise un codec en mode de fonctionnement symétrique (c'est-à-dire lorsque les capacités **receiveAndTransmitVideoCapability** ou **receiveAndTransmitAudioCapability** sont utilisées), l'entité maître peut rejeter une demande **openLogicalChannel** émanant de l'entité esclave, si l'entité maître exige l'utilisation de codecs symétriques alors que le canal proposé n'est pas symétrique. Les procédures de résolution des conflits sont décrites au § C.4.1.3/H.245. Le champ motif de **openLogicalChannelReject** doit être égal à **masterSlaveConflict**.

NOTE 1 – L'entité maître peut envoyer un élément **requestMode** à l'esclave avec le codec approprié avant d'envoyer un élément **openLogicalChannelReject** pour réclamer explicitement un codec particulier.

NOTE 2 – Les capacités effectives consignées dans le tableau de capacités **capabilityTable** sont souvent plus complexes qu'elles ne se présentent ici. Ainsi, chaque capacité H.263 indique un certain nombre de précisions, dont la capacité à accepter divers formats d'image à des intervalles d'image minimaux donnés, ainsi que la capacité à utiliser des modes de codage facultatifs. Pour une description complète, voir la Rec. UIT-T H.245.

Les capacités totales du terminal sont décrites par un ensemble de structures **capabilityDescriptor** (descripteur de capacités), dont chacune est constituée d'une structure unique **simultaneousCapabilities** et d'un numéro **capabilityDescriptorNumber**. En envoyant plus d'un descripteur **capabilityDescriptor**, le terminal peut indiquer des dépendances entre les modes de fonctionnement en décrivant les différents ensembles de modes qu'il peut utiliser simultanément. Ainsi, l'émission par un terminal de deux structures **capabilityDescriptor** – l'une { {H.261, H.263}, {G.711, G.723.1, G.728} } comme dans l'exemple précédent, et l'autre { {H.262, { G.711} } – signifie que le terminal peut aussi utiliser le codec vidéo H.262, mais seulement avec le codec audio G.711 à niveau de complexité réduit.

Les terminaux peuvent dynamiquement ajouter des capacités pendant une session de communication, en émettant des structures **capabilityDescriptor** additionnelles, ou supprimer des capacités en envoyant des structures **capabilityDescriptor** révisées. Tous les terminaux H.323 doivent transmettre au moins une structure **capabilityDescriptor**.

Des capacités et des messages de commande non normalisés peuvent être émis à l'aide de la structure **nonStandardParameter** (paramètre non normalisé) définie dans la Rec. UIT-T H.245. Il est à noter que si la signification des messages non normalisés est définie par les différentes organisations, l'équipement construit par un constructeur peut signaler un message non normalisé quelconque, si la signification en est connue.

Les terminaux peuvent réémettre des ensembles de capacités à tout moment, conformément aux procédures de la Rec. UIT-T H.245.

6.2.8.2 Signalisation de voie logique

Chaque voie logique achemine les informations d'un émetteur à un ou plusieurs récepteurs; elle est identifiée par un numéro de voie logique unique pour chaque sens de transmission.

Les voies logiques sont ouvertes et fermées à l'aide des messages et des procédures d'ouverture et de fermeture de voies logiques **openLogicalChannel** et **closeLogicalChannel** définis dans la Rec. UIT-T H.245. A l'ouverture d'une voie logique, le message **openLogicalChannel** décrit l'intégralité du contenu de la voie logique, y compris le type de média, l'algorithme utilisé, les options éventuelles et toutes les autres informations dont le récepteur a besoin pour interpréter le contenu de la voie logique. Les voies logiques peuvent être fermées lorsqu'elles ne sont plus nécessaires. Des voies logiques ouvertes peuvent rester inactives, si la source d'émission n'a pas d'information à envoyer.

Etant unidirectionnelles, la plupart des voies logiques de la présente Recommandation autorisent l'exploitation en mode asymétrique, dans lequel le nombre et le type des flux d'information diffèrent dans chaque sens de transmission. Toutefois, s'il n'admet que certains modes de fonctionnement symétrique, un récepteur peut envoyer un ensemble de capacités de réception qui reflètent ses limitations, sauf dispositions contraires spécifiées dans la présente Recommandation. Les terminaux peuvent aussi être capables d'utiliser un mode de fonctionnement donné dans un seul sens de transmission. Certains types de média, dont les protocoles de données de type T.120 par exemple, ont par définition besoin d'un canal bidirectionnel pour fonctionner. En pareil cas, une seule voie logique unidirectionnelle peut être ouverte selon les procédures d'ouverture de canal bidirectionnel de la Rec. UIT-T H.245.

Les voies logiques doivent être ouvertes selon la procédure suivante:

le terminal effectuant le lancement doit envoyer un message **openLogicalChannel** comme cela est décrit dans la Rec. UIT-T H.245. Si la voie logique doit transporter un type de média utilisant le protocole RTP (audio ou vidéo), le message **openLogicalChannel** doit comporter le paramètre **mediaControlChannel** dans lequel figure l'adresse de transport de la voie RTCP inverse.

Le terminal destinataire doit répondre par un message **openLogicalChannelAck** comme cela est décrit dans la Rec. UIT-T H.245. Si la voie logique doit transporter un type de média utilisant le protocole RTP, le message **openLogicalChannelAck** doit comporter le paramètre **mediaChannel** dans lequel figure l'adresse de transport RTP de la voie de média ainsi que le paramètre **mediaControlChannel** dans lequel figure l'adresse de transport de la voie RTCP directe.

Pour les types de média (données T.120 par exemple) qui n'utilisent pas les protocoles RTP/RTCP, les paramètres **mediaControlChannel** ne doivent pas être présents.

Si une voie inverse correspondante est ouverte pour une session RTP existante donnée (dont l'identificateur est **sessionID**), les adresses de transport figurant dans le paramètre **mediaControlChannel** et échangées par le processus **openLogicalChannel** doivent être identiques à celles qui sont utilisées pour la voie directe. Les valeurs **sessionID** 1, 2 et 3 sont préattribuées respectivement aux sessions primaires audio, vidéo et de données. Même l'extrémité esclave peut ouvrir des voies logiques pour ces sessions primaires sans négocier la valeur **sessionID** avec l'extrémité maître. Cette dernière peut ouvrir une autre session avec une valeur **sessionID** donnée supérieure à 3. L'extrémité esclave peut ouvrir une session correspondante avec la valeur **sessionID** donnée. A défaut, l'extrémité esclave peut ouvrir d'autres sessions avec la **sessionID**=0 dans le message **openLogicalChannel**, mais elle doit acquérir la valeur **sessionID** effective figurant dans le message **openLogicalChannelAck** de l'extrémité maître. En cas de collision dans laquelle les deux extrémités tentent d'établir des sessions RTP conflictuelles au même moment, l'extrémité maître doit rejeter la tentative conflictuelle comme cela est décrit dans la Rec. UIT-T H.245. La tentative **openLogicalChannel** rejetée peut être refaite ultérieurement.

Sauf spécification contraire pour un type de données particulier, les canaux de données fiables sont bidirectionnels et, en tant que tels, doivent contenir les deux éléments **forwardLogicalChannelParameters** et **reverseLogicalChannelParameters** sans les éléments **mediaChannel**. L'extrémité qui accepte la voie doit renvoyer l'élément **mediaChannel** dans

l'élément **reverseLogicalChannelParameters** et doit être en mesure d'accepter la connexion fiable issue du point d'extrémité demandeur, avant d'envoyer le message **openLogicalChannelAck**.

Une extrémité qui accepte une voie bidirectionnelle fiable doit être en mesure d'accepter une connexion fiable issue du point d'extrémité demandeur, avant de renvoyer le message **openLogicalChannelAck**.

6.2.8.3 Modes préférés

Les récepteurs peuvent demander aux émetteurs d'indiquer un mode de fonctionnement donné en envoyant le message de demande de mode **requestMode** H.245, qui décrit le mode souhaité. Les émetteurs devraient, si possible, s'exécuter.

Une extrémité qui reçoit la commande de mode multipoint **multipointModeCommand** en provenance du contrôleur multipoint doit exécuter toutes les commandes de demande de mode **requestMode**, si celles-ci font partie de son ensemble de capacités. A noter que dans une conférence décentralisée, de même que dans une conférence centralisée, toutes les commandes de demande de mode **requestMode** du terminal sont adressées au contrôleur multipoint. Celui-ci peut accéder ou non à la demande; les motifs qui présideront à cette décision sont laissés à l'appréciation du constructeur.

6.2.8.4 Choix du mode maître ou esclave

Les procédures de choix du mode maître ou esclave H.245 sont utilisées pour résoudre des conflits entre deux extrémités pouvant toutes deux constituer le contrôleur multipoint pour une conférence, ou entre deux extrémités qui tentent d'ouvrir un canal bidirectionnel. Dans cette procédure, deux extrémités échangent des numéros aléatoires dans le message de choix du mode maître ou esclave **masterSlaveDetermination** H.245, pour déterminer les extrémités maître et esclave. Les extrémités H.323 doivent pouvoir fonctionner à la fois dans les modes maître et esclave. Les extrémités doivent mettre **terminalType** à la valeur spécifiée dans le Tableau 1 ci-dessous et le numéro **statusDeterminationNumber** à une valeur numérique aléatoire de 0 à 2^{24}–1. Un seul numéro aléatoire doit être choisi par l'extrémité pour chaque appel, sauf dans le cas de numéros aléatoires identiques, comme indiqué dans la Rec. UIT-T H.245.

Tableau 1/H.323 – Types de terminaux H.323 pour le choix du mode maître ou esclave H.245

Tableau des valeurs TerminalType	**Entité H.323**			
Ensemble de caractéristiques	**Terminal**	**Passerelle**	**Portier**	**Pont de conférence**
Entité sans contrôleur multipoint	50	60	Sans objet	Sans objet
Entité incorporant un contrôleur multipoint mais n'incorporant pas de processeur multipoint	70	80	120	160
Entité incorporant un contrôleur multipoint avec processeur multipoint de données	Sans objet	90	130	170
Entité incorporant un contrôleur multipoint avec processeur multipoint de données et audio	Sans objet	100	140	180
Entité incorporant un contrôleur multipoint avec processeur multipoint de données, audio et vidéo	Sans objet	110	150	190

Le contrôleur multipoint activé, dans une conférence, doit utiliser une valeur de 240.

Si une entité H.323 unique peut participer à plusieurs appels ou communications, la valeur utilisée pour le type **terminalType** dans le processus de choix du mode maître ou esclave doit être basée sur les caractéristiques que l'entité H.323 a assignées ou assignera à l'appel dans lequel elle est signalée.

Un contrôleur multipoint qui agit déjà en tant que tel doit toujours rester le contrôleur multipoint activé. Par conséquent, une fois qu'un contrôleur multipoint a été sélectionné en tant que contrôleur multipoint activé dans une conférence, il doit utiliser la valeur contrôleur multipoint activé pour toutes les connexions ultérieures de raccordement à la conférence.

Si aucun contrôleur multipoint n'est activé et si les entités sont du même type, l'entité H.323 dont l'ensemble de caractéristiques est le plus grand (comme indiqué dans le Tableau 1) doit mener à bien la procédure de choix du mode maître ou esclave. Si aucun contrôleur multipoint n'est activé et si les entités sont de types différents, un contrôleur multipoint situé dans un pont de conférence doit avoir la priorité sur un contrôleur multipoint situé dans un portier, lequel doit avoir la priorité sur un contrôleur multipoint situé dans une passerelle, lequel à son tour doit avoir la priorité sur un contrôleur multipoint situé dans un terminal.

Si elle peut être associée à au moins deux des classifications indiquées dans le Tableau 1, une entité H.323 devrait utiliser la valeur la plus élevée pour laquelle elle présente les qualités requises.

6.2.8.5 Valeurs des temporisateurs et des compteurs

Tous les temporisateurs définis dans la Rec. UIT-T H.245 devraient rester activés pendant des durées au moins égales au temps maximal de remise des données autorisé par la couche Liaison de données écoulant le trafic sur la voie de commande H.245, y compris les retransmissions éventuelles.

Le compteur de nouvelles tentatives N100 H.245 devrait totaliser au moins trois nouvelles tentatives.

Les procédures relatives au traitement des erreurs de protocole H.245 font l'objet du § 8.6.

6.2.8.6 Transmission d'un flux multiplexé dans une seule voie logique

Plusieurs flux médias peuvent être multiplexés dans une seule voie logique. Un flux multiplexé contient plusieurs flux médias utilisant le protocole de multiplexage H.222.0 [45] ou H.223 [46] et transmis sous la forme d'une série de paquets RTP. Grâce à ces protocoles de multiplexage, une extrémité H.323 peut profiter de certains avantages comme une utilisation plus efficace de la largeur de bande, une synchronisation précise des médias et un faible retard de transmission multimédia.

Il existe deux modes de commande de la configuration d'un flux multiplexé. Le premier consiste à transmettre des messages H.245 à l'intérieur des paquets RTP des flux multiplexés. Dans ce cas, les extrémités H.323 ouvrent d'abord, par la procédure H.245 de signalisation de voie logique, un canal logique bidirectionnel pour la transmission du flux multiplexé en tant que flux média RTP normal. Puis la commande de flux multiplexé est assurée au moyen de messages H.245 contenus dans des paquets RTP du flux multiplexé visé. La commande du flux multiplexé inclut l'échange de capacités concernant les codecs médias disponibles pour ce flux multiplexé, l'échange de tables de multiplexage et l'ouverture/la fermeture de voies logiques. Les numéros de voie logique dans un flux multiplexé sont indépendants de ceux des autres flux multiplexés ou de ceux des voies logiques H.245.

L'autre façon de commander la configuration d'un flux multiplexé consiste à contrôler les voies logiques du flux multiplexé comme s'il s'agissait de voies logiques non multiplexées, c'est-à-dire que les messages H.245 pour le flux multiplexé sont transmis comme les autres messages H.245. Dans ce cas, une extrémité H.323 ouvre, au moyen de la procédure de signalisation de voie logique H.245, une voie logique unidirectionnelle ou un canal logique bidirectionnel pour la

transmission du flux multiplexé comme un flux média RTP normal. L'on ouvre ensuite les voies logiques dans le flux multiplexé au moyen de la signalisation de voie logique avec les paramètres de la configuration du protocole de multiplexage et avec le numéro de voie logique du flux multiplexé dans lequel la nouvelle voie logique doit être ouverte.

6.2.8.6.1 Echange de capacités relatif au flux multiplexé

Les terminaux H.323 prenant en charge les flux multiplexés indiquent cette capacité en insérant un élément **MultiplexedStreamCapability** dans le cadre de la capacité du terminal. Le paramètre **controlOnMuxStream** contenu dans l'élément **MultiplexedStreamCapability** indique si le terminal prend en charge la commande du flux multiplexé au moyen de messages H.245 ou au moyen des paquets RTP du flux multiplexé proprement dit. Si la valeur du paramètre **controlOnMuxStream** est "TRUE", la capacité des codecs en terme de flux multiplexé peut être mise à la valeur du paramètre **capabilityOnMuxStream**. Si le paramètre **capabilityOnMuxStream** n'existe pas, le terminal doit appliquer la procédure d'échange de capacités en envoyant les messages H.245 dans les paquets RTP du flux multiplexé, après l'ouverture de la voie logique pour ce flux. Si la valeur du paramètre **controlOnMuxStream** est "FALSE", la capacité des codecs du flux multiplexé doit être mise à la valeur du paramètre **capabilityOnMuxStream**.

6.2.8.6.2 Signalisation par voies logiques pour transporter un flux multiplexé

La voie logique pour le flux multiplexé est ouverte par l'envoi d'un message **openLogicalChannel** contenant le type **dataType** d'un élément **MultiplexedStreamCapability** ainsi que les paramètres **multiplexParameters** contenus dans le paramètre **h2250LogicalChannelParameters**. Si la valeur du paramètre **controlOnMuxStream** contenu dans **MultiplexedStreamCapability** est "TRUE", la voie logique doit être ouverte sous la forme d'un canal logique bidirectionnel, c'est-à-dire que le paramètre **reverseLogicalChannelParameters** doit être activé. Sinon, la voie logique peut être ouverte en tant que voie logique unidirectionnelle. Noter que si la voie logique est ouverte dans un seul sens, une partie de la fonction de protocole multiplex ne pourra pas être utilisée, p. ex. la fonction AL3 de la Rec. UIT-T H.223 ne peut pas être utilisée dans les voies logiques unidirectionnelles.

Un terminal ne peut pas ouvrir plus d'une seule voie logique si la valeur du paramètre **multiplexFormat** contenu dans **h223Capability** et **controlOnMuxStream** est "FALSE".

6.2.8.6.3 Signalisation par voies logiques pour transporter un flux média dans un flux multiplexé

La voie logique contenue dans un flux multiplexé est ouverte par l'envoi d'un message **openLogicalChannel** avec le type **dataType** approprié au média à acheminer et avec le paramètre **multiplexParameters** du protocole multiplex approprié qui est utilisé (c'est-à-dire avec le paramètre **h223logicalChannelParameters**). En cas de messages H.223, la procédure de signalisation de la table de multiplexage doit également être appliquée avant ou après cette signalisation de voie logique, comme décrit au § 6.4.2/H.324.

Si la valeur du paramètre **controlOnMuxStream** est "TRUE", ces messages H.245 sont acheminés à l'intérieur des paquets RTP pour le flux multiplexé dans lequel la nouvelle voie logique est ouverte. En cas de messages H.223, les messages H.245 **MultimediaSystemControlMessage** sont protégés par le protocole de retransmission simple (SRP, *simple retransmission protocol*) et acheminés dans la voie logique n° 0 du flux multiplexé, comme décrit au § 6.5.4/H.324.

Si la valeur du paramètre **controlOnMuxStream** est "FALSE", ces messages H.245 sont acheminés dans une voie de commande H.245 comme cela est d'usage. En cas de messages H.222.0, les identificateurs **resourceID** du paramètre **h2220LogicalChannelParameters** sont mis au numéro de voie logique du flux multiplexé dans lequel la nouvelle voie logique doit être ouverte.

Noter qu'en cas de messages H.223, cette signalisation n'est pas requise car il n'existe pas plus d'une seule voie logique.

Les voies logiques contenues dans le flux multiplexé sont fermées par l'envoi de messages **closeLogicalChannel**, qui sont transmis de la même façon que les messages **openLogicalChannel** pour les mêmes voies.

6.2.8.6.4 Signalisation par voie logique pour fermer un flux multiplexé

La voie logique pour le flux multiplexé qui est ouverte avec le paramètre **controlOnMuxStream** mis à la valeur "TRUE" peut être fermée à tout moment au moyen d'un message **closeLogicalChannel**. La voie logique pour le flux multiplexé qui est ouverte avec le paramètre **controlOnMuxStream** mis à la valeur "FALSE" ne peut être fermée qu'après la fermeture de toutes les voies logiques de ce flux multiplexé.

6.2.9 Fonction de signalisation RAS

La fonction de signalisation RAS utilise des messages H.225.0 pour mener à bien différentes procédures – enregistrement, admissions, modification de largeur de bande, indication d'état et libération – entre extrémités et portiers. La voie de signalisation RAS est indépendante de la voie de signalisation d'appel et de la voie de commande H.245. Les procédures d'ouverture de voie logique H.245 ne sont pas utilisées pour établir la voie de signalisation RAS. Dans des environnements de réseaux sans portier, la voie de signalisation RAS n'est pas utilisée. Dans des environnements de réseaux avec portier (zone), la voie de signalisation RAS est ouverte entre l'extrémité et le portier. La voie de signalisation RAS est ouverte avant l'établissement d'autres voies entre extrémités H.323. Cette voie est décrite en détail au § 7.

6.2.10 Fonction de signalisation d'appel

La fonction de signalisation d'appel utilise la signalisation d'appel H.225.0 pour établir une connexion entre deux extrémités H.323. La voie de signalisation d'appel est indépendante de la voie RAS et de la voie de commande H.245. Les procédures d'ouverture de voie logique H.245 ne sont pas utilisées pour établir la voie de signalisation d'appel. Celle-ci est ouverte avant l'établissement de la voie H.245 et des autres voies logiques entre extrémités H.323. Dans des systèmes sans portier, la voie de signalisation d'appel est ouverte entre les deux extrémités participant à l'appel.

Dans des systèmes avec portier, la voie de signalisation d'appel est ouverte entre l'extrémité et le portier, ou entre les extrémités elles-mêmes telles qu'elles ont été choisies par le portier. Cette voie est décrite en détail au § 7.

6.2.11 Couche H.225.0

Les voies logiques des informations vidéo, audio, de données ou de commande sont établies conformément aux procédures de la Rec. UIT-T H.245. Les voies logiques sont unidirectionnelles et indépendantes dans chaque sens de transmission. Certaines voies logiques, telles que les voies pour données, peuvent être bidirectionnelles, étant associées entre elles par la procédure d'ouverture de canal logique bidirectionnel de la Rec. UIT-T H.245. Les voies logiques de transmission de chaque type de média peuvent être établies en n'importe quel nombre, sauf la voie de commande H.245 qui ne doit être établie qu'à raison d'une seule voie par appel. Les extrémités H.323 utilisent, outre les voies logiques, deux voies de signalisation pour la commande d'appel et les fonctions relatives au portier. Le formatage utilisé pour ces voies doit être conforme à la Rec. UIT-T H.225.0.

6.2.11.1 Numéros de voie logique

Chaque voie logique est identifiée par un numéro de voie logique (LCN, *logical channel number*), de 0 à 65535, qui sert uniquement à associer les voies logiques à la connexion de transport. Les numéros de voies logiques sont sélectionnés arbitrairement par l'émetteur, à l'exception de la voie logique 0 qui doit être assignée en permanence à la voie de commande H.245. L'adresse de

transport effective à destination de laquelle l'émetteur doit émettre doit être renvoyée par le récepteur dans le message d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck**.

6.2.11.2 Limites de débit de voie logique

La largeur de bande d'une voie logique doit avoir une limite supérieure spécifiée par la capacité d'émission minimale de l'extrémité (lorsque cette capacité est spécifiée) et la capacité de réception de l'extrémité de destination. Compte tenu de cette limite, une extrémité doit ouvrir une voie logique à un débit égal ou inférieur à cette limite supérieure. Un émetteur doit transmettre un flux d'information dans la voie logique à un débit égal ou inférieur au débit d'ouverture de la voie logique. Cette limite s'applique aux flux d'information contenus dans la ou les voies logiques, non compris les en-têtes RTP, les en-têtes de charge utile RTP, les en-têtes de réseau et autres préfixes.

Les extrémités H.323 doivent satisfaire au message **flowControlCommand** H.245, qui impose une limite au débit d'une voie logique ou au débit composite de toutes les voies logiques. Les extrémités H.323 qui souhaitent limiter le débit d'une voie logique, ou le débit composite de toutes les voies logiques devraient envoyer le message de commande **flowControlCommand** à l'extrémité émettrice.

Lorsqu'il n'a pas d'informations à envoyer dans une voie donnée, le terminal doit s'abstenir d'en envoyer. Des données de remplissage ne doivent pas être envoyées sur le réseau afin de maintenir un débit de données spécifique.

6.3 Caractéristiques des passerelles

La passerelle doit assurer la conversion voulue entre les formats de transmission (par exemple, du format H.225.0 au format H.221 ou vice versa) ainsi qu'entre les procédures de communication (par exemple de la procédure H.245 à la procédure H.242 ou vice versa). Cette conversion est spécifiée dans la Rec. UIT-T H.246. La passerelle doit aussi assurer l'établissement et la libération des communications tant du côté réseau que du côté réseau à commutation de circuits (RCC). La conversion entre les formats vidéo, audio et de données peut aussi être assurée dans la passerelle. En général, la passerelle (lorsqu'elle ne fait pas office de pont de conférence) a pour rôle d'informer une extrémité du RCC des caractéristiques d'une extrémité du réseau, et vice versa, de façon transparente.

Une extrémité H.323 peut communiquer avec une autre extrémité H.323 directement sur le même réseau, sans l'intermédiaire d'une passerelle. Celle-ci peut être omise s'il n'est pas nécessaire d'établir des communications avec les terminaux du réseau à commutation de circuits (par opposition aux terminaux du réseau). Un terminal situé sur un segment du réseau peut aussi avoir la possibilité d'appeler un numéro extérieur par l'intermédiaire d'une passerelle et de revenir sur le réseau par l'intermédiaire d'une autre passerelle afin de contourner un routeur ou une liaison à faible largeur de bande.

La passerelle présente les caractéristiques d'un terminal ou d'un pont de conférence H.323 sur le réseau et les caractéristiques d'un terminal ou d'un pont de conférence du réseau à commutation de circuits sur ce même réseau. Le choix du terminal ou du pont de conférence est laissé à l'appréciation du constructeur. La passerelle assure la conversion nécessaire entre les différents types de terminaux. Il est à noter que celle-ci peut initialement faire fonction de terminal, puis, en utilisant la signalisation H.245, commencer à jouer le rôle d'un pont de conférence pour la même communication établie initialement point à point. Les portiers savent quels sont les terminaux qui font office de passerelle, cette indication leur étant fournie au moment où chaque terminal/passerelle se fait enregistrer auprès de son portier.

Une passerelle qui transmet des données T.120 entre le réseau à commutation de circuits et le réseau peut comporter un fournisseur de système MCS T.120 qui connecte les fournisseurs de

services MCS T.120 du réseau aux fournisseurs de services MCS T.120 du réseau à commutation de circuits.

La Figure 5 montre quatre exemples de configurations de passerelle H.323. Les schémas de configuration montrent les fonctions de terminal ou de pont de conférence H.323, les fonctions de terminal ou de pont de conférence du réseau à commutation de circuits (RCC) et la fonction de conversion. La fonction de terminal H.323 présente les caractéristiques décrites au § 6.2. La fonction de pont de conférence H.323 présente les caractéristiques décrites au § 6.5. La passerelle se présente pour les autres terminaux H.323 du réseau sous la forme d'un ou de plusieurs terminaux H.323 ou d'un pont de conférence H.323. Elle communique avec les autres terminaux H.323 selon les procédures spécifiées dans la présente Recommandation.

La fonction de terminal ou de pont de conférence du RCC présente les caractéristiques décrites dans la Recommandation pertinente (H.310, H.320, H.321, H.322, H.324, V.70 – terminaux ne fonctionnant qu'en mode téléphonique sur le RTGC ou le RNIS). La passerelle se présente pour les terminaux du RCC sous la forme d'un ou de plusieurs terminaux ou ponts de conférence de même type. Elle communique avec un autre terminal du RCC par les procédures décrites dans la Recommandation relative à ce terminal. Les procédures de signalisation du RCC ne relèvent pas du domaine d'application de la présente Recommandation, incluant des questions comme celle de savoir si la passerelle H.323 se présente pour le RCC sous la forme d'un terminal ou d'un réseau. Il est à noter qu'une passerelle peut convertir le mode H.323 directement au mode H.324 ou H.310 sans passer par le mode H.320.

Les passerelles assurant l'interfonctionnement avec des terminaux fonctionnant uniquement en mode téléphonique sur le RTGC ou le RNIS devraient générer et détecter des signaux à tonalités multifréquences (DTMF) correspondant aux indications de données d'usager **userInputIndications** H.245 pour les caractères 0-9,* et #. En outre, il se peut que les passerelles puissent générer et détecter des signaux DTMF, des tonalités téléphoniques et des signaux téléphoniques correspondant à ces événements transportés avec un type spécial de charge utile RTP, tel que décrit au § 10.5.

La fonction de conversion assure la conversion nécessaire du format de transmission des flux de signaux de commande, audio, vidéo et de données entre les différentes Recommandations relatives aux terminaux. Au minimum, la passerelle doit assurer une fonction de conversion du format de transmission, des signaux et des procédures d'établissement des communications ainsi que des signaux et des procédures de commande des communications. En cas de nécessité, la passerelle doit assurer la conversion H.242 à H.245. La passerelle assure la conversion voulue entre la signalisation d'appel H.225.0 et le système de signalisation du RCC (Q.931, Q.2931, etc.). La conversion entre les messages de signalisation d'appel H.225.0 sur le réseau et les messages Q.931 sur le réseau à commutation de circuits est décrite dans la Rec. UIT-T H.246.

Toute la signalisation d'appel reçue par la passerelle en provenance d'une extrémité du RCC et non applicable à la passerelle doit passer par l'intermédiaire de l'extrémité du réseau, et vice versa. Cette signalisation comprend, sans y être limitée, les messages de la Rec. UIT-T Q.932 et des séries des Recommandations UIT-T Q.950 et H.450. Les extrémités H.323 pourront ainsi implémenter les services complémentaires définis dans ces Recommandations. Le traitement des autres systèmes de signalisation d'appel du réseau à commutation de circuits est à étudier.

La présente Recommandation décrit la connexion d'un terminal H.323 du réseau à un terminal externe du réseau à commutation de circuits, par l'intermédiaire de la passerelle. Le nombre effectif de terminaux H.323 pouvant communiquer par l'intermédiaire de la passerelle n'est pas soumis à normalisation. De même, le nombre de connexions du réseau à commutation de circuits, le nombre de conférences indépendantes simultanées, les fonctions de conversion audio/vidéo/données ainsi que l'inclusion de fonctions multipoint, sont laissés à l'appréciation du constructeur. Si la passerelle intègre une fonction de pont de conférence côté réseau, cette fonction doit être un pont de conférence H.323 du côté du réseau. Si la passerelle intègre une fonction de pont de conférence côté

réseau à commutation de circuits, celle-ci peut se présenter sous la forme d'un pont de conférence H.231/H.243 ou d'un pont de conférence pour systèmes H.310 ou H.324 (ces ponts de conférence sont indiqués comme devant faire l'objet d'un complément d'étude dans les Recommandations concernées) du côté du réseau à commutation de circuits.

Une passerelle peut être connectée par l'intermédiaire du RCC à d'autres passerelles pour mettre en communication des terminaux H.323 n'appartenant pas au même réseau.

Les équipements qui assurent l'interconnexion transparente de réseaux sans utiliser de protocoles de la série H (routeurs et postes à sélection automatique à l'arrivée, par exemple) ne sont pas des passerelles au sens de la présente Recommandation.

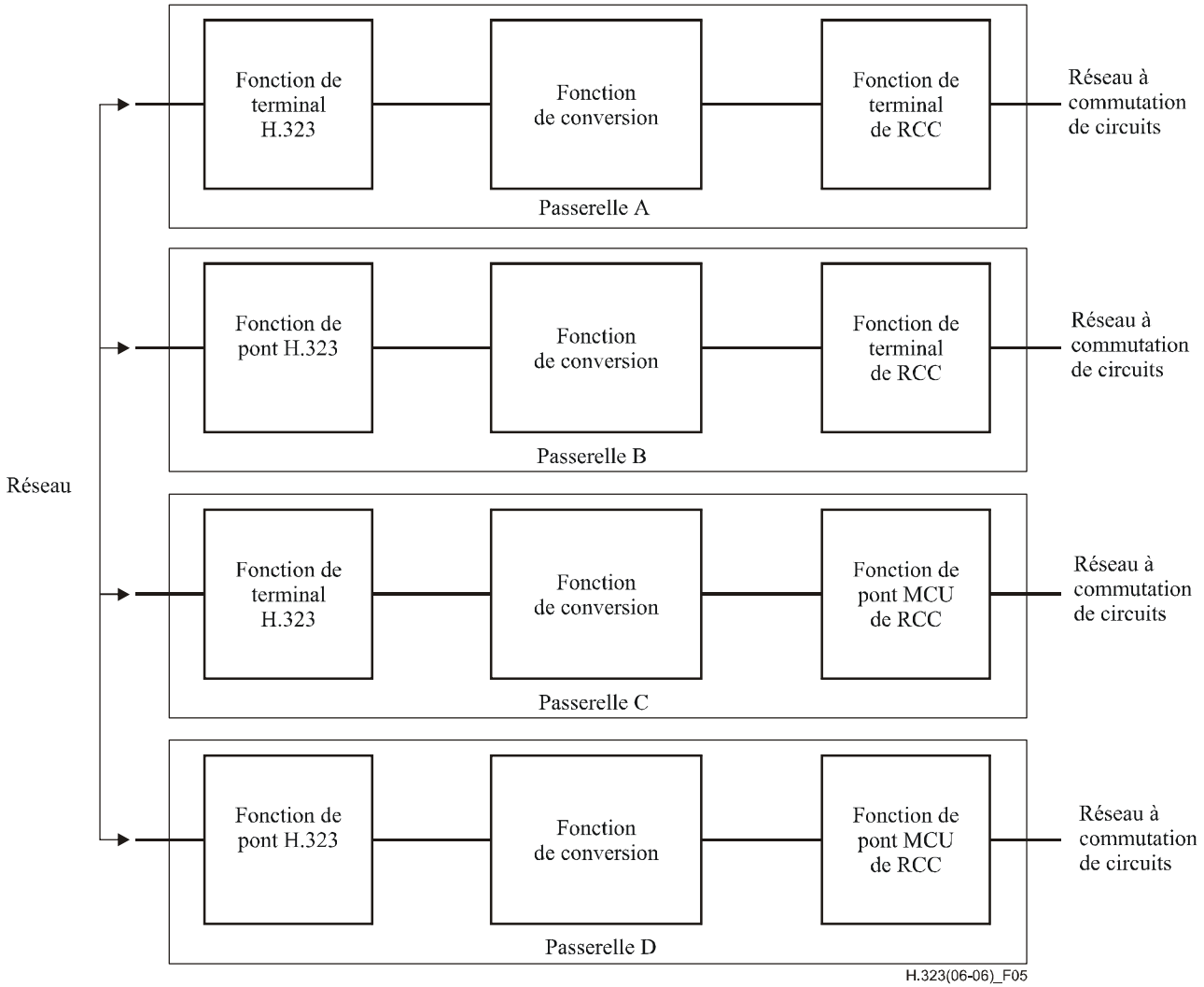


Figure 5/H.323 – Configuration des passerelles H.323

6.3.1 Décomposition de passerelle

Le présent paragraphe définit un groupe d'interfaces et de fonctions à utiliser pour décomposer des passerelles H.323. Il vise chaque interface et son protocole résultant, mais certaines implémentations de passerelle peuvent choisir de grouper deux ou plus de deux composants fonctionnels pour former un seul dispositif physique. C'est pourquoi des interfaces peuvent offrir la capacité de transport en retour transparent d'autres protocoles.

Dans la Figure 6, le composant média à commutation de paquets/circuits reçoit une voie média RCC et convertit ces flux en média en mode paquet à l'interface avec le réseau en mode paquet. L'interface A représente le protocole de commande de dispositif défini dans la Rec. UIT-T H.248.1:

ce protocole sert à créer, à modifier et à supprimer des connexions médias de passerelle. Le composant de logique de commande assurera l'interfonctionnement de signalisation entre le RCC et les fonctions H.323 de la passerelle.

L'interface B représente les composants de protocole H.225.0 et H.245 qui constituent les interfaces de signalisation du côté paquet de la passerelle.

L'interface C décrira la fonction de commande d'appel de type RNIS entre les services RCC de signalisation FAS et la logique de commande de passerelle. L'interface D est un protocole qui achemine la signalisation RCC autre que FAS jusqu'au contrôleur. Cette décomposition offre la flexibilité nécessaire pour conserver les séquences codées SS7. Elle permet également au commutateur SS7 de desservir plusieurs contrôleurs de passerelle décomposée.

Les éléments de commande de ressource établissent une distinction entre les ressources à interprétation de haut niveau dans le contrôleur de passerelle et les ressources à interprétation de niveau inférieur dans un dispositif de passerelle.

Les interfaces RCC sont décrites comme étant une interface de bas niveau qui transporte la signalisation et une terminaison de signalisation RCC de haut niveau qui interfonctionne avec le contrôleur de la passerelle considérée. Cette signalisation peut être de type FAS, comme dans le cas d'une interface PRI du RNIS, ou de type NFAS, comme dans le cas du SS7.

La Figure 6 ne représente pas une décomposition physique à ce point. Le défi posé aux vendeurs de passerelles consiste à regrouper ces composants dans des dispositifs physiques et à réaliser les interfaces associées de façon à produire des passerelles H.323 à modularité élevée et compatibles entre de nombreux vendeurs. L'interface X est l'interface H.323 externe. L'interface Y est l'interface externe avec les médias en mode paquet (c'est-à-dire avec le protocole RTP) et l'interface Z est l'interface externe avec le RCC.

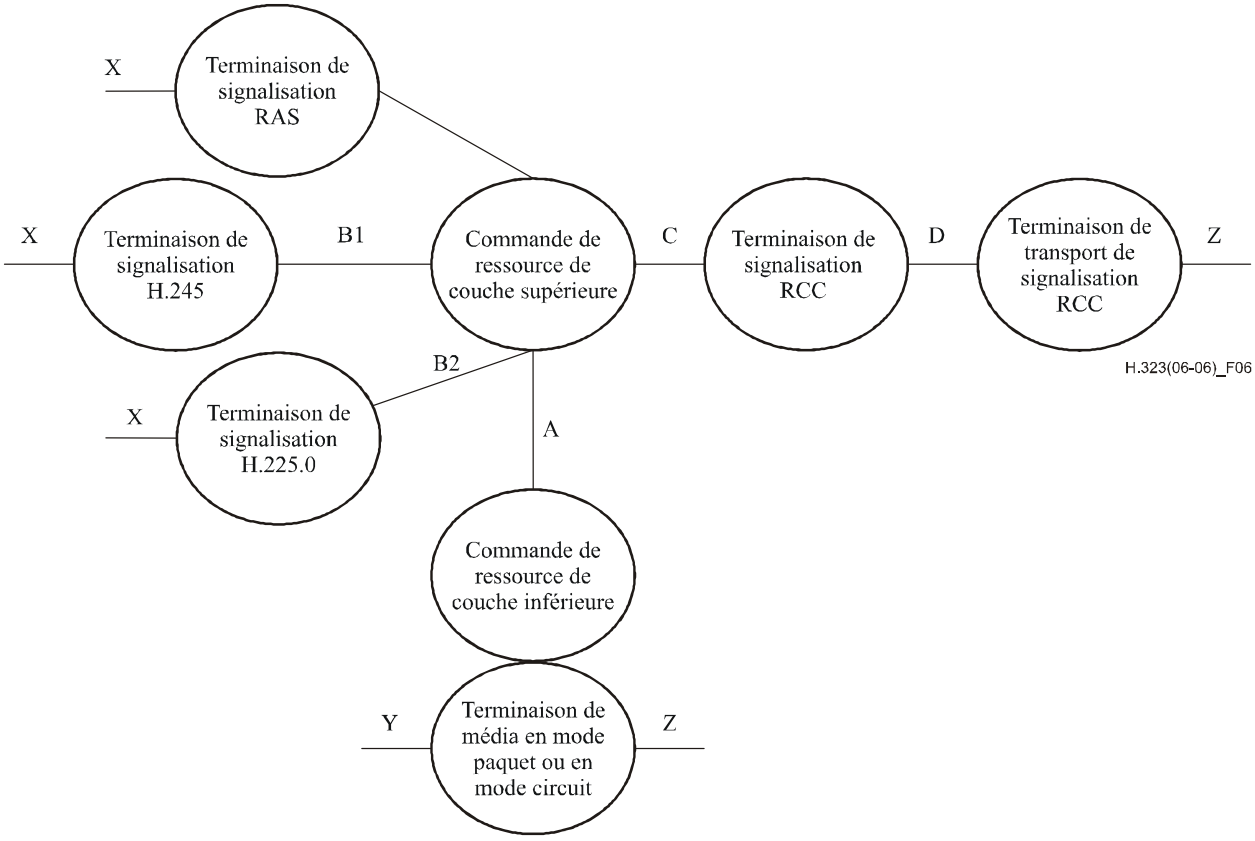


Figure 6/H.323 – Architecture fonctionnelle de la passerelle décomposée

6.3.1.1 Décompositions physiques

Le présent paragraphe décrit des exemples de décomposition possible de passerelle avec les interfaces nécessaires. Les interfaces externes, telles que H.323 et RCC, restent de toute façon inchangées. La partie contrôleur de la passerelle physique est appelée contrôleur de passerelle média (MGC, *media gateway controller*). Les fonctions du contrôleur MGC sont les suivantes:

- traiter les messages de signalisation RAS H.225.0 avec un portier externe;
- traiter facultativement l'interface de signalisation SS7;
- traiter facultativement l'interface de signalisation H.323.

Le composant de passerelle média (MG, *media gateway*):

- reçoit l'interface avec le réseau IP;
- reçoit l'arc RCC;
- peut traiter la signalisation H.323 dans certaines décompositions physiques;
- peut traiter la signalisation FAS du RCC dans certaines décompositions physiques.

Les passerelles décomposées n'ont pas besoin de prendre en charge toutes les interfaces mais l'interface A, qui met en évidence la distinction MGC/MG, est un élément obligatoire de toutes les décompositions, ce qui permet à un contrôleur MGC de commander différents types de passerelle média pouvant être optimisés pour certaines applications (p. ex. les passerelles voix H.320/multimédia H.323). La décomposition des interfaces B et C dans une passerelle média, qui peut nécessiter un protocole pour renvoyer la signalisation de la passerelle média au contrôleur MGC, fera l'objet d'une étude complémentaire.

La passerelle média reçoit les médias en mode IP ou ATM du côté RCP et les canaux supports du côté des interfaces avec le RCC. Le côté RCP peut être en mode IP ou ATM ou en interface avec un réseau ATM dans lequel des paquets audio et vidéo traversent des connexions ATM originales conformément à l'Annexe C.

Le contrôleur MGC et la passerelle média établissent une distinction entre les éléments de gestion de ressource de haut niveau et de bas niveau. Le contrôleur MGC est chargé de la gestion de ressource de haut niveau, par laquelle il interprète la disponibilité de ressources telles que des annuleurs d'écho mais n'assigne pas de ressources spécifiques à des sessions particulières de passerelle. La passerelle média est chargée de l'affectation et de la gestion des ressources de bas niveau, ainsi que des manipulations de matériel requises pour commuter et traiter des flux médias à l'intérieur de la passerelle média.

6.3.1.1.1 Passerelles SS7 distinctes

La Figure 7 représente une décomposition possible de passerelle ISUP-vers-H.323, dans laquelle les fonctions de passerelle SS7, de contrôleur MGC et de passerelle média sont décomposées en dispositifs physiques distincts. Cet arrangement met en évidence une interface D de transport de signalisation ISUP et l'interface A de commande de dispositif.

Pour faciliter l'interopérabilité, les configurations de passerelle décomposée doivent prendre en charge l'interface A et contenir les signalisations H.323 et RCC dans le contrôleur MGC.

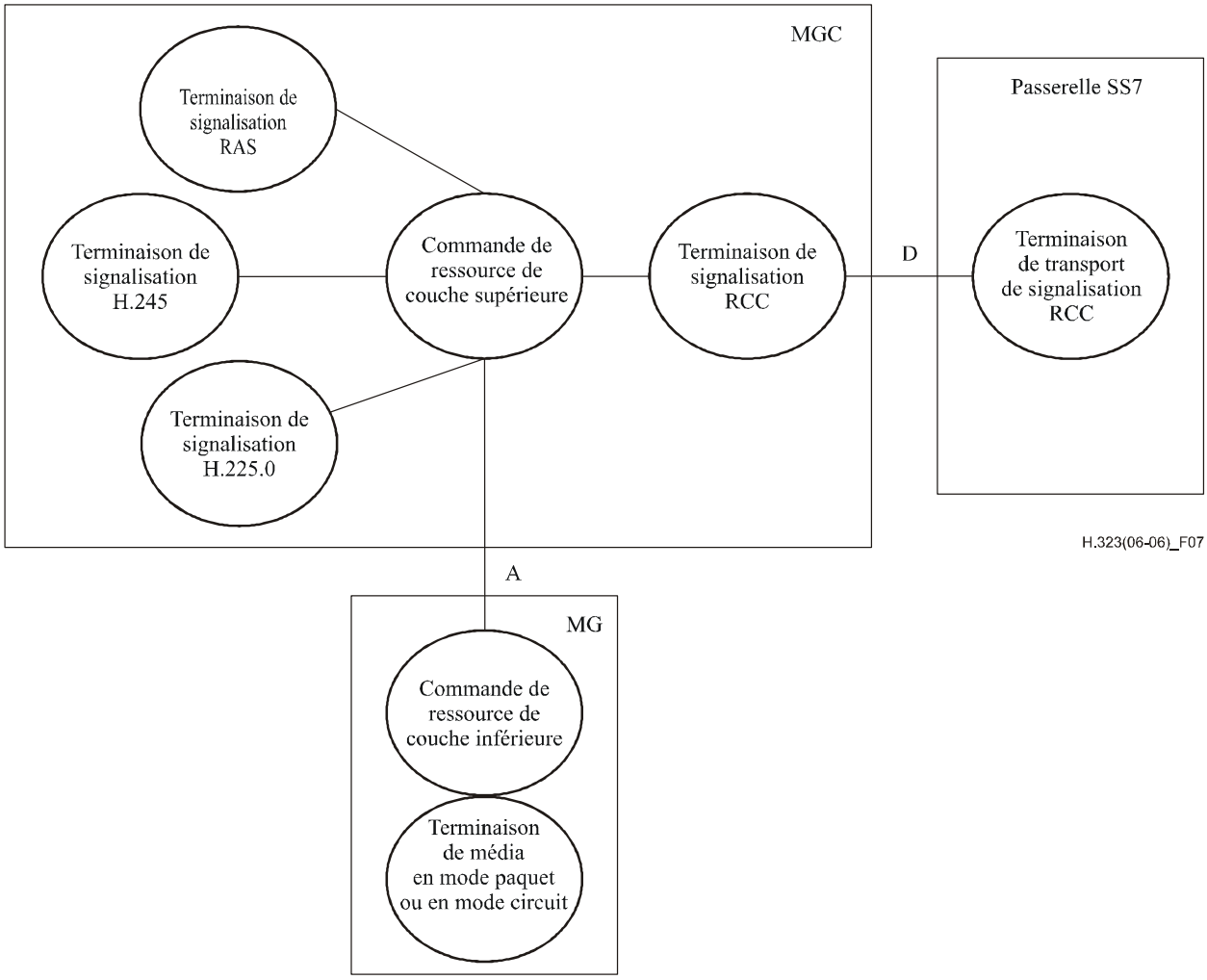


Figure 7/H.323 – Décomposition de passerelle SS7

6.3.1.1.2 Décomposition de passerelle FAS

La décomposition de passerelle représentée sur la Figure 8 isole les services RCC de signalisation FAS tels que l'interface PRI du RNIS dans la passerelle média et conserve la signalisation H.323 dans le contrôleur MGC, ce qui met en évidence les interfaces C et A entre la passerelle média et le contrôleur MGC.

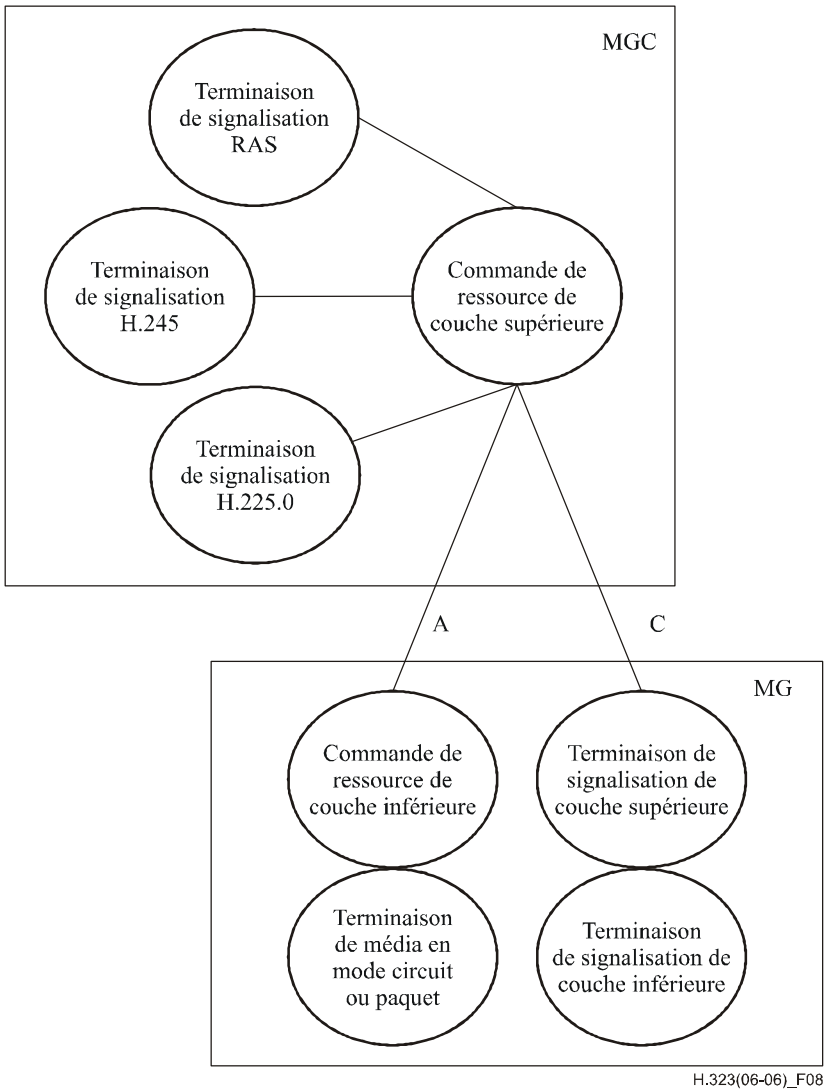


Figure 8/H.323 – Passerelle FAS avec signalisation H.323 dans la passerelle média

6.3.1.1.3 Passerelle SS7 avec signalisation H.323 dans la passerelle média

La décomposition représentée sur la Figure 9 met en évidence l'interface SS7 du contrôleur MGC et déploie la signalisation H.323 aux interfaces D, A et B avec passerelle média.

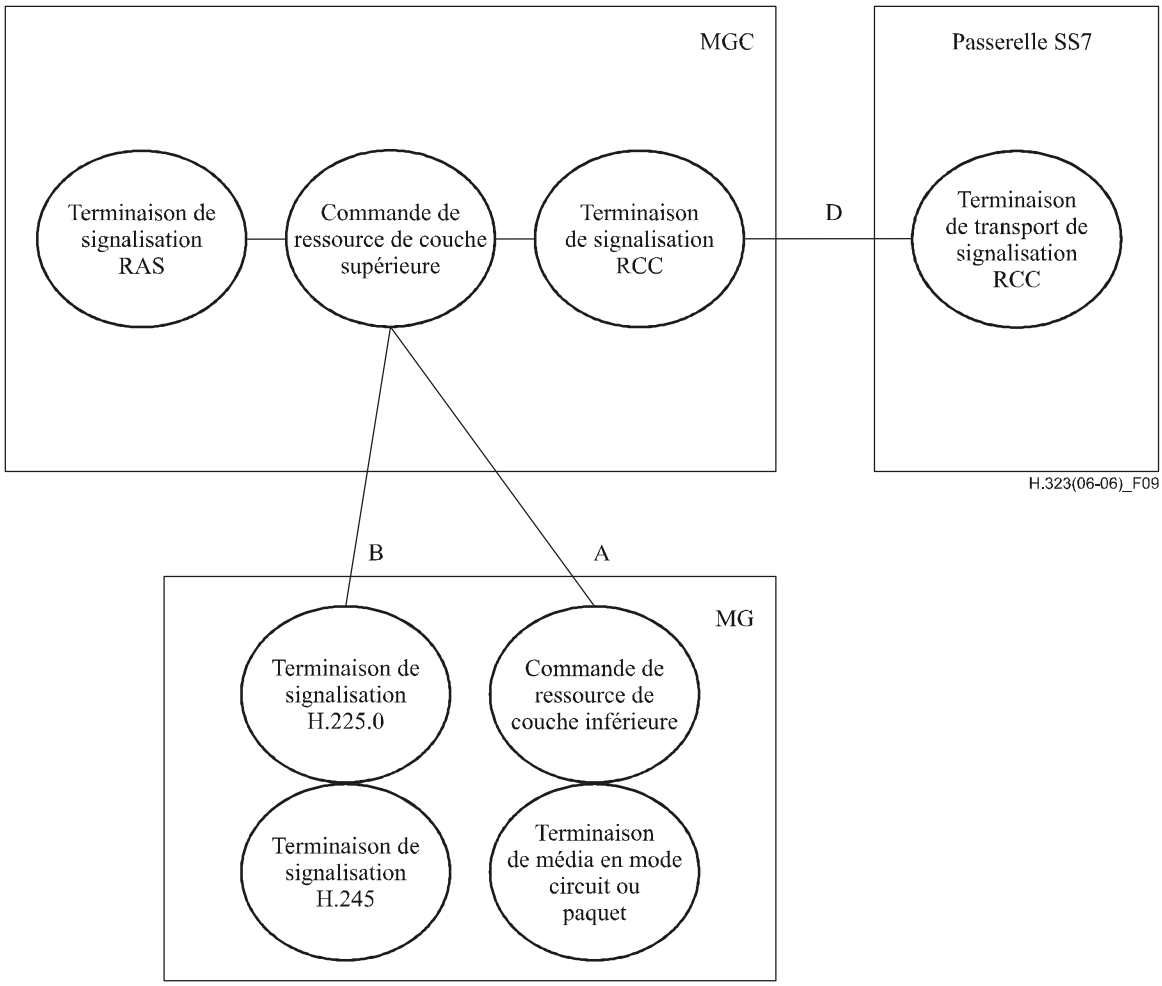


Figure 9/H.323 – Signalisation SS7 reçue dans la passerelle média

6.3.1.1.4 Signalisations FAS et H.323 dans la passerelle média

Il existe des prescriptions pour passerelles H.320 décomposées, telles que les signalisations H.323 et RCC soient toutes deux présentes dans la passerelle média, en plus des terminaisons des réseaux en mode circuit et en mode paquet. Dans cette décomposition, la signalisation est traitée localement par la passerelle média et les notifications d'événement sont signalées au contrôleur MGC (voir Figure 10).

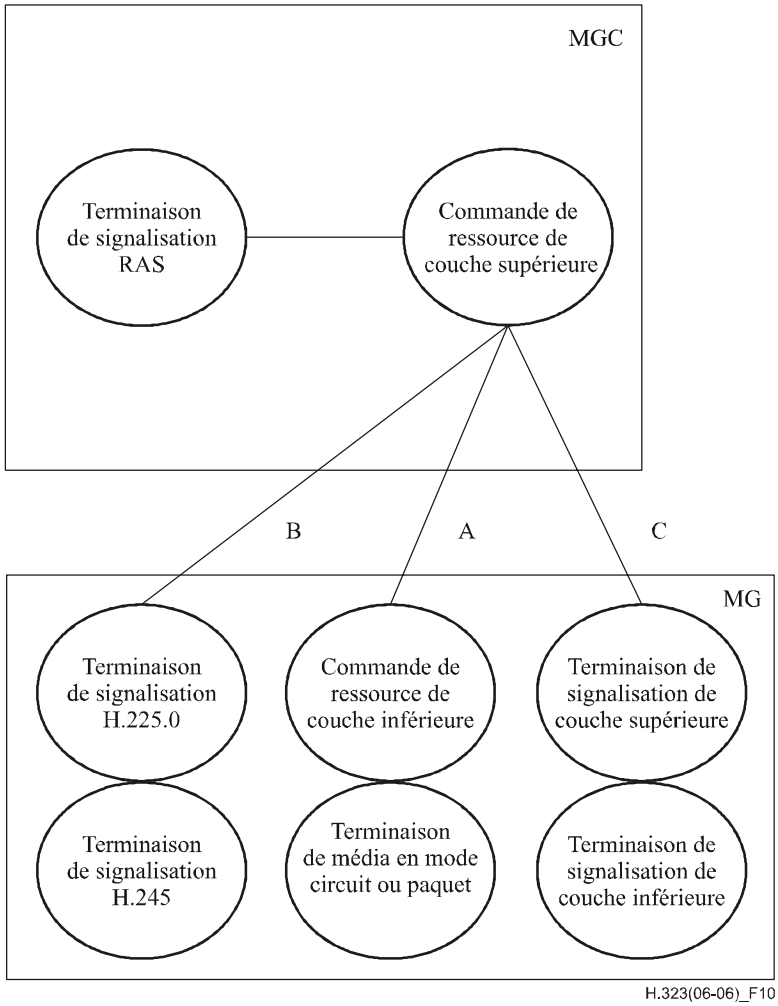


Figure 10/H.323 – Signalisations FAS et H.323 dans la passerelle média

6.3.1.1.5 Signalisation SS7 dans la passerelle média

La décomposition décrite dans la Figure 11 fait aboutir le réseau SS7 dans la passerelle média et met en évidence l'interface D entre le contrôleur MGC et la passerelle média.

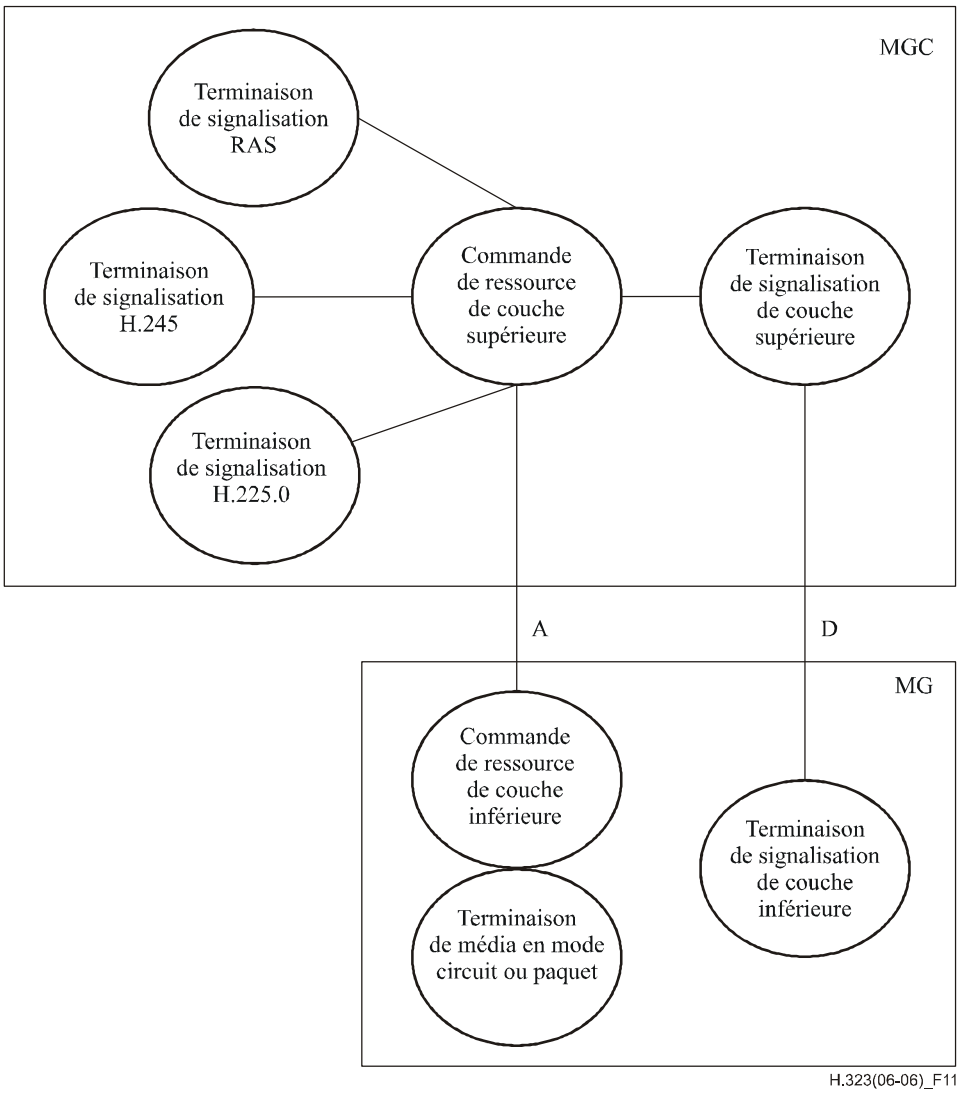


Figure 11/H.323 – Signalisation SS7 aboutissant dans la passerelle média

6.3.2 Applications de passerelle

Il existe de nombreuses applications pour passerelles décomposées et composites. Les vendeurs et/ou les exploitants peuvent décider d'utiliser une passerelle composite ou décomposée selon les exigences applicatives. Les passerelles décomposées sont appelées par la Rec. UIT-T H.248 à interfonctionner avec les passerelles composites.

Le présent paragraphe analyse quelques termes partagés entre équipements H.323, RCC et H.248. Il donne également des exemples de passerelles applicatives. Il ne vise pas à donner une liste complète de toutes les applications ni à illustrer la seule façon dont de telles applications peuvent être prises en charge. Dans ce paragraphe, les termes passerelle média, contrôleur MGC et passerelle représentent des réalisations physiques de ces dispositifs.

6.3.2.1 Aperçu général des passerelles de jonction et d'accès

Les termes passerelle de jonction et passerelle d'accès sont utilisés dans les deux Rec. UIT-T H.323 et H.248. Ils font également partie de la terminologie de la commutation de circuits, où ils

s'appliquent aux commutateurs de transit et d'accès. Comme les mêmes mots servent à désigner différents éléments dans le contexte de trois architectures différentes, le présent paragraphe tente de préciser les nuances terminologiques.

6.3.2.1.1 Terminologie RCC

Dans le RCC, un commutateur "de transit" ou "de jonction" raccorde des réseaux utilisant un protocole d'interface NNI comme SS7/ISUP ou CAS/NNI. Un commutateur "d'accès" possède des connexions d'usager utilisant une interface BRI/PRI avec également une connexion à un plus grand réseau au moyen de protocoles d'interface NNI. Un commutateur "mixte" peut avoir les deux fonctions.

6.3.2.1.2 Terminologie H.323

Dans les réseaux H.323, une passerelle "de jonction" remplit une véritable fonction de tandem qui est transparente aux réseaux rattachés. Ces derniers peuvent être de type SS7, QSIG ou autre. Dans tous les cas cependant, la tunnellisation est utilisée afin de créer une transparence complète et une véritable fonction tandem. L'interfonctionnement entre versions de l'ISUP est considéré comme intervenant à l'extérieur du réseau H.323. La tunnellisation est fondée sur la négociation de protocole H.225.0 et sur l'Annexe M.

Une passerelle "d'accès" H.323 fournit une fonction d'interfonctionnement avec un autre réseau, une autre entreprise ou une autre extrémité dont la transparence n'est pas totale. Les protocoles mis en interfonctionnement sont par exemple les suivants:

- SS7/ISUP, conformément à l'Annexe C/H.246;
- QSIG, conformément à la Rec. UIT-T H.450;
- H.320, conformément à l'Annexe A/H.246.

Il convient de noter que la passerelle "de jonction" H.323 et le commutateur "de transit" RCC remplissent la même fonction, tandis que la "passerelle d'accès" H.323 et le "commutateur d'accès" RCC jouent des rôles très différents. Un point de confusion particulier est que le protocole H.225.0 assure la signalisation des deux interfaces UNI et NNI dans le réseau H.323 et qu'il joue dans le RCC les deux rôles de l'ISUP et des interfaces BRI/PRI du RNIS. Le protocole H.323 n'opère pas les distinctions de signalisation UNI/NNI qui sont effectuées dans le RCC et la signalisation d'appel est la même entre extrémités directement gérées ou passant par l'intermédiaire d'élément de réseau comme un portier H.323 ou un élément périphérique (BE, *border element*).

La Figure 12 résume les points ci-dessus. Elle montre également la relation entre domaines H.323, qui possèdent certaines caractéristiques de type RCC. Il importe toutefois de ne pas perdre de vue le fait que le protocole H.225.0 est aussi utilisé pour toutes les signalisations d'appel, que ce soit entre terminaux, entre zones ou entre domaines. Par ailleurs, les zones et les domaines sont essentiellement virtuels plutôt que physiques et les commutateurs (par exemple, des brasseurs ATM utilisés pour le routage de paquets IP), bien qu'éventuellement présents, ne sont pas visibles d'un point situé au-dessus de la couche IP du réseau en mode paquet.

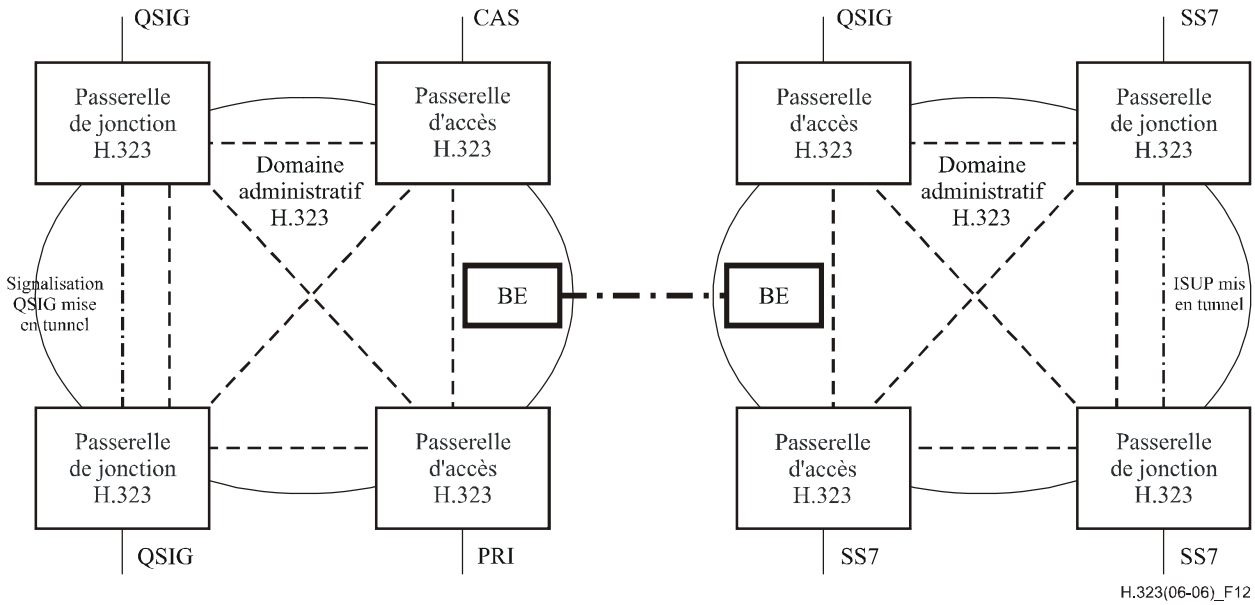


Figure 12/H.323 – Relation entre passerelles H.323, RCC et H.248

6.3.2.1.3 Terminologie H.248

La Rec. UIT-T H.248.1 fait également usage des termes "passerelle de jonction" et "passerelle d'accès". Compte tenu du fait que les dispositifs H.248 peuvent être considérés comme étant de simples décompositions de passerelles composites H.323 en contrôleurs MGC et en passerelles médias, l'on part du principe que les contrôleurs MGC prennent en charge le protocole H.323 et interfonctionnent au moyen du protocole H.225.0, exactement comme toute autre passerelle H.323, y compris la tunnellisation de la signalisation ISUP, etc. Considérés du point de vue d'une décomposition, ces termes prennent cependant des significations qui varient légèrement. Une "passerelle de jonction" est telle que la signalisation est connectée directement au contrôleur MGC, c'est-à-dire à l'ISUP, alors qu'une "passerelle d'accès" est telle que la signalisation arrive directement dans le contrôleur MGC (c'est-à-dire dans l'ISUP) alors qu'une "passerelle d'accès" est telle que la signalisation arrive à la passerelle média puis est transmise au contrôleur MGC par protocole H.248. Il importe de noter qu'une "passerelle d'accès", bien qu'elle puisse prendre en charge un protocole d'interface UNI, peut aussi prendre en charge des protocoles de signalisation CAS d'interface NNI, de sorte que la définition d'une "passerelle d'accès" H.248 comme une passerelle prenant en charge une interface UNI n'est pas exacte.

La Figure 13 décrit l'architecture du protocole H.248.1. Il y a lieu de noter que des passerelles H.323 composites sont souvent utilisées comme "passerelles d'accès" dans les systèmes H.248 tels qu'illustrés. Le schéma montre un contrôleur MGC H.248 et un portier H.323 copositionnés.

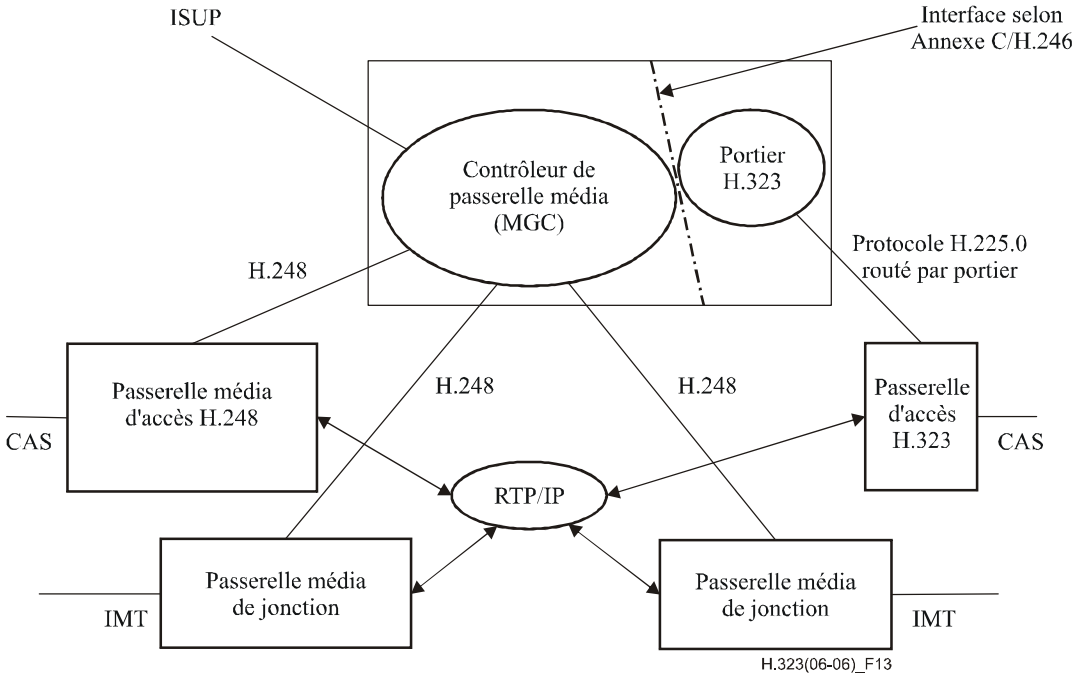


Figure 13/H.323 – Relation entre protocoles H.323 et H.248

6.3.2.2 Passerelles de jonction de fournisseur de services

La Figure 14 montre un exemple d'appel routé dans un réseau à commutation de paquets entre deux passerelles de jonction de fournisseur de services. Dans cette application, le réseau à commutation de paquets joue le rôle d'un réseau vocal en cascade pour le fournisseur de service. Pour cette application, l'interface A sert à commander les passerelles médias. Le réseau en mode paquet se raccorde au réseau à commutation de circuits par canaux sémaphores SS7 et par jonctions entre machines (IMT, *inter-machine trunk*). La Figure 14 décrit le cas de l'utilisation de canaux sémaphores par l'interface A du SS7 pour le raccordement au réseau SS7. Dans ce cas, le contrôleur MGC reçoit directement les canaux sémaphores et non par l'intermédiaire d'une passerelle de signalisation. Les contrôleurs MGC se transmettent les uns aux autres les informations sémaphores au moyen de l'interface X (par exemple par tunnellisation des signaux ISUP dans une connexion H.225.0). Le trafic vocal s'écoule entre les deux passerelles.

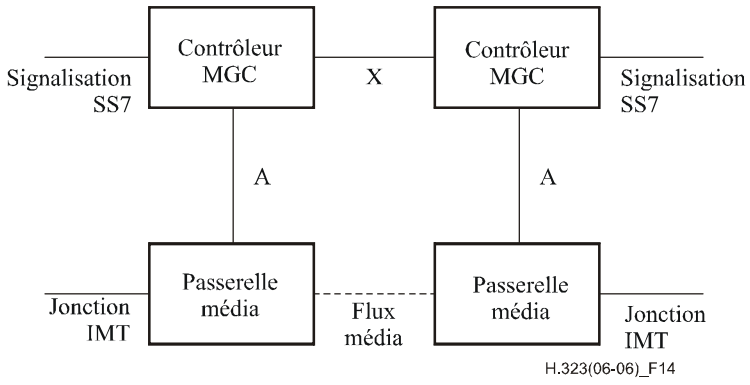


Figure 14/H.323 – Décomposition de deux passerelles de jonction de fournisseur de service

6.3.2.3 Passerelles d'accès de fournisseur de services

La Figure 15 montre un exemple d'appel routé dans un réseau à commutation de paquets entre une passerelle d'accès composite H.323 de fournisseur de services et une passerelle de jonction décomposée de fournisseur de services. Dans cette application, le fournisseur de services offre une interface de signalisation voie par voie (CAS, *channel associated signalling*) à un système autocommutateur d'entreprise pour transporter des communications vocales dans le réseau de ce fournisseur. La signalisation d'appel H.225.0 est utilisée entre la passerelle composite et la passerelle décomposée. Le contrôleur MGC assure la signalisation SS7 appropriée pour communiquer avec le réseau SS7 du fournisseur de services et avec le RCC. Dans cet exemple, la liaison X est en protocole H.225.0 et le contrôleur MGC implémente une fonction d'interfonctionnement conforme à l'Annexe E/H.246.

Bien qu'il existe des Recommandations qui décrivent l'interfonctionnement entre divers protocoles tels qu'ISUP et H.323, il convient que les fournisseurs de services et les constructeurs calculent précisément le moment où il convient d'effectuer un tel interfonctionnement ainsi que le nombre de tels points d'interfonctionnement. Celui-ci peut ne pas assurer une conversion parfaite entre deux protocoles et des conversions multiples peuvent se traduire par une assez grande perte de transparence.

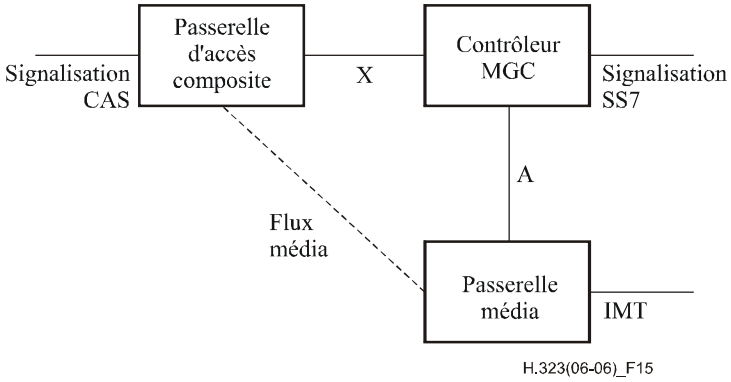


Figure 15/H.323 – Passerelle d'accès composite et passerelle de jonction décomposée

La Figure 16 décrit la même application, dans laquelle la passerelle d'accès de fournisseur de services est également décomposée. Dans ce cas, l'interface A sert à commander la signalisation CAS. Les contrôleurs MGC communiquent les uns avec les autres au moyen de l'interface X. Dans ce cas particulier, s'il n'y a pas de retour de signalisation entre la passerelle média et le contrôleur MGC, la quantité d'informations d'appel mises à la disposition du contrôleur MGC sera limitée à ce qui est défini par la Rec. UIT-T H.248.1. Dans cet exemple, la liaison X est en protocole H.225.0 et le contrôleur MGC de droite effectue un interfonctionnement avec l'ISUP selon l'Annexe E/H.246.

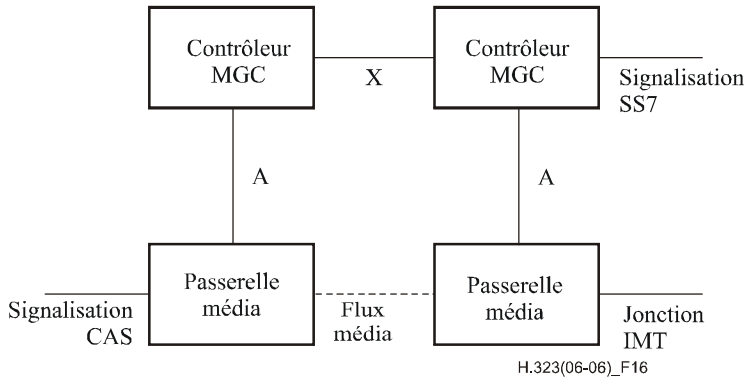


Figure 16/H.323 – Décomposition de passerelles d'accès et de jonction de fournisseur de services

Lors de la recherche de la meilleure approche pour une application particulière, il y a lieu de tenir compte des facteurs suivants:

- nombre de lignes à raccorder;
- coût des jonctions;
- impératifs d'homologation;
- capacité du contrôleur MGC;
- proportion de passerelles d'accès par rapport aux passerelles de jonction;
- types de protocole de signalisation CAS à prendre en charge;
- architecture de traitement d'appel du fournisseur de services;
- conception du réseau.

Pour les passerelles d'accès, l'environnement applicatif déterminera la meilleure solution: passerelle décomposée et terminal H.323 utilisant la signalisation H.450.x, terminal à stimulus de l'Annexe L, ou passerelle composite.

6.3.2.4 Passerelles de jonction d'entreprise

La Figure 17 décrit une passerelle d'entreprise qui est utilisée entre autocommutateurs d'un réseau téléphonique privé. Le réseau en mode paquet est utilisé au lieu de lignes louées afin de connecter les autocommutateurs. Dans ce cas, le protocole QSIG est utilisé pour la signalisation entre les autocommutateurs. Comme le protocole QSIG est une signalisation en mode service par service (FAS, *facility associated signalling*), cette signalisation peut être renvoyée par la passerelle média au contrôleur MGC par l'intermédiaire de l'interface C. L'interface A est utilisée pour la commande entre contrôleur MGC et passerelle média. Les contrôleurs MGC communiquent les uns avec les autres par l'interface X, qui peut utiliser le protocole QSIG tunnellisé H.225.0 conformément à l'Annexe M1.

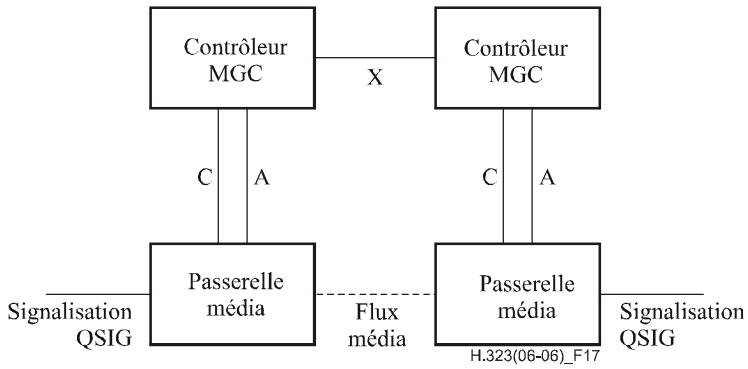


Figure 17/H.323 – Décomposition de passerelles de jonction d'entreprise

La Figure 18 décrit des passerelles qui sont utilisées entre autocommutateurs d'un réseau téléphonique privé. Le réseau en mode paquet est utilisé au lieu de lignes louées afin de connecter les autocommutateurs. Dans ce cas, le protocole QSIG est également utilisé pour la signalisation entre les autocommutateurs. Mais la tunnellisation du protocole QSIG à l'interface X est utilisée pour transporter la signalisation QSIG entre une passerelle composite et une passerelle décomposée. D'autres combinaisons, comme composite-composite ou décomposée-décomposée, peuvent également être utilisées.

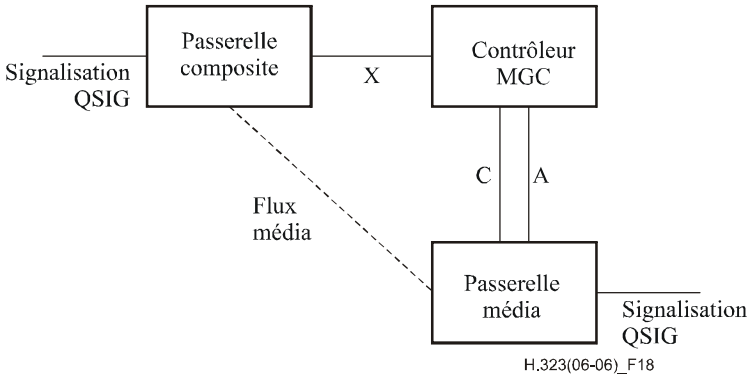


Figure 18/H.323 – Exemple de tunnellisation du protocole QSIG

6.3.2.5 Passerelles d'accès d'entreprise à fournisseur de services

Dans certains cas, un réseau H.323 d'entreprise communique avec le RTGC au moyen d'une passerelle décomposée, ce qui est illustré par la Figure 19. Dans ce cas, la passerelle décomposée communique avec les extrémités H.323 par signalisation H.323 (H.225, H.245, etc.). La passerelle décomposée se raccorde au RTGC au moyen d'une interface PRI du RNIS. La signalisation par le canal D peut être renvoyée par l'interface C.

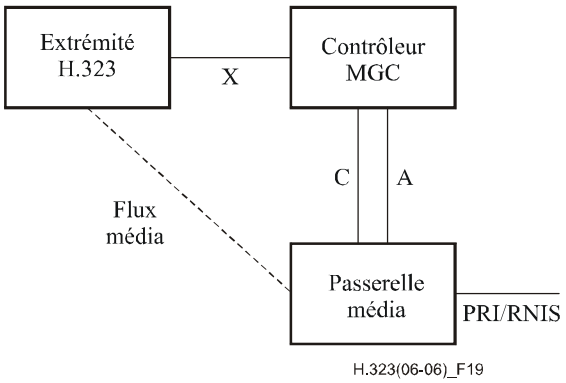


Figure 19/H.323 – Passerelle décomposée et extrémité H.323

Une autre application d'accès d'entreprise utilise le protocole H.248 pour gérer des terminaux mais elle apparaît comme une liaison entre passerelles composites dans d'autres locaux, comme indiqué dans la Figure 20. Dans cet exemple, la signalisation H.450.x est utilisée pour assurer l'interfonctionnement de services complémentaires.

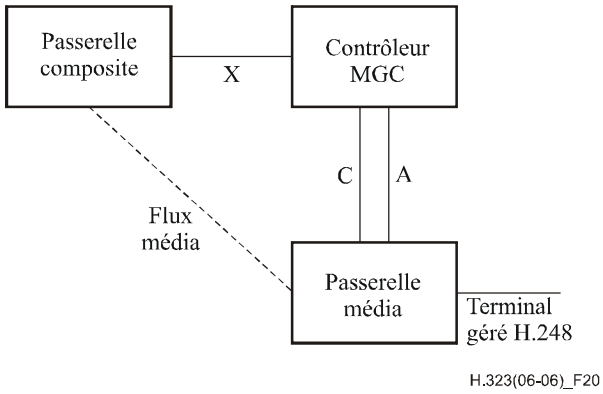


Figure 20/H.323 – Passerelle composite et terminal géré H.248

Une autre application d'accès d'entreprise utilise l'Annexe L pour gérer des terminaux mais elle apparaît comme une liaison entre passerelles composites dans d'autres locaux, comme indiqué dans la Figure 21. Dans cet exemple, la signalisation H.450.x peut être utilisée pour assurer l'interfonctionnement de services complémentaires et la liaison X1 est en protocole H.225.0 avec signalisation H.450, tandis que la liaison X2 utilise le protocole H.225.0 avec la signalisation par stimulus de l'Annexe L.

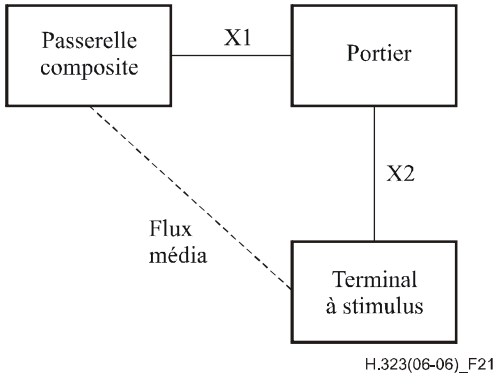


Figure 21/H.323 – Passerelle composite et terminal de l'Annexe L

Il convient de noter que, sur la Figure 21, les terminaux de l'Annexe L peuvent interfonctionner avec les terminaux gérés H.248 de la Figure 20 au moyen de la signalisation H.450.x. Ces configurations permettent d'importantes innovations internes dans l'entreprise tout en assurant l'interopérabilité entre entreprises par signalisation H.450.x. Noter que la signalisation d'appel routée par portier est utilisée à la Figure 21 du portier d'entreprise gérant les terminaux de l'Annexe L, bien que les autres passerelles d'entreprise puissent utiliser le modèle d'appel direct et avoir un portier différent.

6.4 Caractéristiques du portier

Le portier, facultatif dans un système H.323, assure des services de commande d'appel aux extrémités H.323. Plusieurs portiers peuvent coexister et communiquer entre eux dans un mode non précisé. Le portier est en principe séparé des extrémités; il peut toutefois être couplé à un terminal, un pont de conférence, une passerelle, un contrôleur multipoint ou un autre dispositif de réseau non H.323.

A un moment donné, il n'existe qu'un seul portier dans une zone, bien que plusieurs dispositifs distincts puissent remplir la fonction de portier dans une zone. Les multiples dispositifs qui remplissent la fonction de signalisation RAS pour le portier sont dénommés portiers de remplacement. Chaque portier de remplacement peut être vu par des extrémités comme un portier distinct. La communication entre portiers de remplacement et autres dispositifs remplissant la fonction de portier pour la zone est hors du domaine d'application de la présente Recommandation.

Lorsqu'il est intégré dans un système, le portier doit assurer les services suivants:

- Conversion d'adresse – Le portier doit convertir l'adresse de pseudonyme en adresse de transport. Il utilisera à cet effet une table de conversion qu'il mettra à jour à l'aide des messages d'enregistrement décrits au § 7. D'autres méthodes de mise à jour de la table de conversion sont également autorisées.
- Contrôle des admissions – Le portier doit autoriser l'accès au réseau au moyen des messages ARQ/ACF/ARJ (demande/confirmation/refus d'admission) H.225.0. L'autorisation d'accès peut être fondée sur l'autorisation d'appel, la largeur de bande ou d'autres critères laissés à l'appréciation du constructeur. Elle peut aussi consister en une fonction nulle admettant toutes les demandes.
- Régulation de la largeur de bande – Le portier doit prendre en charge les messages BRQ/BRJ/BCF (demande/refus/confirmation de modification de largeur de bande). La prise en charge de ces messages peut être fondée sur la gestion de la largeur de bande. Elle peut aussi consister en une fonction nulle acceptant toutes les demandes de modification de la largeur de bande.

- Gestion de zone – Le portier doit assurer les fonctions mentionnées ci-dessus pour les terminaux, les ponts de conférence et les passerelles qui se sont fait enregistrer auprès de lui comme indiqué au § 7.2.

Le portier peut aussi assurer d'autres fonctions facultatives, dont les suivantes:

- signalisation de commande d'appel – Le portier peut choisir de procéder à la signalisation d'appel avec les extrémités et peut traiter la signalisation d'appel proprement dite. Il peut aussi donner pour instruction aux extrémités de connecter la voie de signalisation d'appel directement entre eux. Il évitera ainsi d'avoir à traiter les signaux de commande d'appel H.225.0. Le portier peut avoir à faire fonction de réseau, comme indiqué dans la Rec. UIT-T Q.931 afin d'assurer des services complémentaires. Ce mode de fonctionnement appelle un complément d'étude.
- Autorisation d'appel – L'utilisation de la signalisation H.225.0 permet au portier de refuser des appels en provenance d'un terminal au motif qu'il n'y est pas autorisé. Les motifs d'un tel refus peuvent être, parmi d'autres, l'accès restreint à certains terminaux ou passerelles ou au départ de ceux-ci et l'accès restreint à certaines heures. Les critères d'octroi ou de refus d'une autorisation d'appel ne relèvent pas de la présente Recommandation.
- Gestion de largeur de bande – Régulation du nombre de terminaux H.323 autorisés à accéder simultanément au réseau. L'utilisation de la signalisation H.225.0 permet au portier de refuser des appels en provenance d'un terminal au motif que la largeur de bande est limitée. Tel peut être le cas si le portier constate que la largeur de bande disponible sur le réseau est insuffisante pour accepter l'appel. Les critères permettant de déterminer si la largeur de bande disponible est suffisante ne relèvent pas de la présente Recommandation. Il est à noter qu'on peut utiliser à cet effet une fonction nulle, c'est-à-dire que tous les terminaux obtiennent une autorisation d'accès. Cette fonction s'applique également pendant un appel activé, lorsqu'un terminal demande une largeur de bande supplémentaire.
- Gestion des appels – Le portier peut, par exemple, tenir à jour une liste des appels H.323 en cours. Une telle liste peut être nécessaire pour indiquer qu'un terminal appelé est occupé et pour fournir des informations à la fonction de gestion de la largeur de bande.
- Modification d'adresse de pseudonyme – Le portier peut renvoyer une adresse de pseudonyme modifiée. S'il renvoie une adresse de pseudonyme dans un message ACF, l'extrémité doit utiliser cette adresse lors de l'établissement de la connexion.
- Conversion des chiffres composés – Le portier peut convertir des chiffres composés en un numéro E.164 ou en un numéro de réseau privé.
- Structure des données d'information de gestion du portier – Cette structure appelle un complément d'étude.
- Réservation d'une largeur de bande pour terminaux ne pouvant pas assurer cette fonction – Ce type de réservation appelle un complément d'étude.
- Services d'annuaire – Ces services appellent un complément d'étude.

Pour pouvoir assurer des conférences multipoint ad hoc, le portier peut choisir de recevoir les voies de commande H.245 provenant des deux terminaux participant à une conférence point à point. Au moment où la conférence devient une conférence multipoint, le portier peut rediriger la voie de commande H.245 vers un contrôleur multipoint. Le portier n'a pas à traiter la signalisation H.245, mais seulement à en assurer l'acheminement entre les terminaux ou entre les terminaux et le contrôleur multipoint.

Les réseaux qui comportent des passerelles devraient aussi comporter un portier qui puisse convertir en adresses de transport les adresses entrantes de type **dialledDigits** ou **partyNumber** (y compris **e164Number** et **privateNumber**).

Les entités H.323 qui comportent un portier doivent incorporer un mécanisme de désactivation du portier interne de manière que dans le cas où plusieurs entités H.323 comportant un portier coexistent sur un réseau, celles-ci puissent être configurées dans la même zone.

6.5 Caractéristiques du contrôleur multipoint

Le contrôleur multipoint assure des fonctions de commande aux fins de la mise en œuvre de conférences entre au moins trois extrémités dans une conférence multipoint. Il procède à l'échange des capacités entre les différentes extrémités participant à la conférence multipoint. Il envoie un ensemble de capacités à ces extrémités, indiquant les modes de fonctionnement dans lesquels ceux-ci peuvent émettre. Le contrôleur multipoint peut modifier l'ensemble de capacités qu'il envoie aux terminaux, par suite de l'introduction ou du retrait de terminaux participant à la conférence, ou pour d'autres raisons.

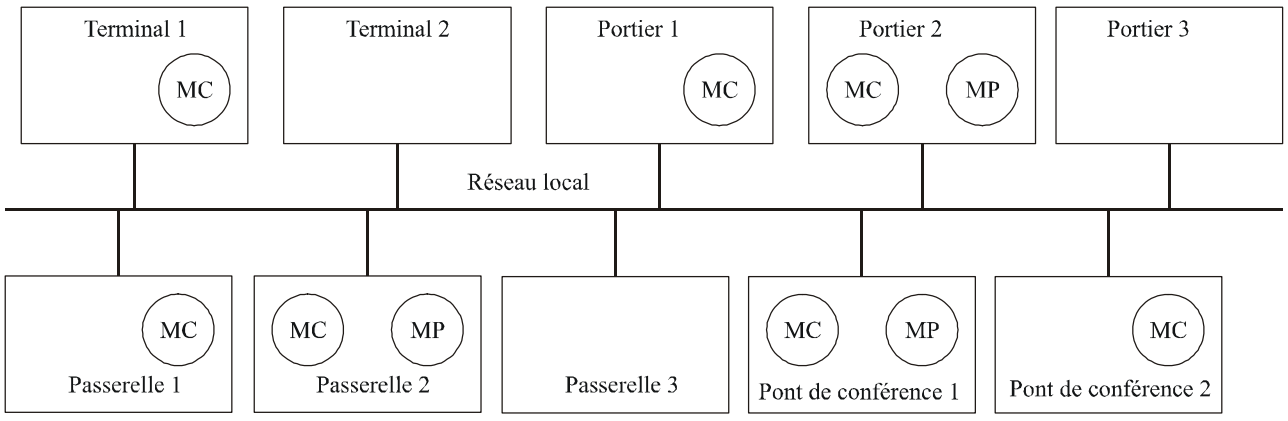
Le contrôleur multipoint détermine ainsi le mode de communication sélectionné (SCM, *selected communications mode*) pour la conférence. Le mode SCM peut être commun à toutes les extrémités participant à la conférence. Certains de ces points peuvent aussi ne pas utiliser le même mode SCM que les autres extrémités participant à la conférence. La manière dont le contrôleur multipoint choisit le mode SCM ne relève pas de la présente Recommandation.

Dans le cadre de l'établissement d'une conférence multipoint, une extrémité se trouvera connectée à un contrôleur multipoint sur sa voie de commande H.245. Cette connexion peut être établie:

– par une connexion explicite avec un pont de conférence;
– par une connexion implicite au contrôleur multipoint à l'intérieur d'un portier;
– par une connexion implicite au contrôleur multipoint à l'intérieur d'un autre terminal ou d'une autre passerelle participant à la conférence multipoint;
– par une connexion implicite, par l'intermédiaire d'un portier, à un pont de conférence.

Le choix du mode de conférence (décentralisé ou centralisé, par exemple) intervient après connexion au contrôleur multipoint en signalisation H.245. Le choix du mode de conférence peut être limité par la capacité des extrémités ou du contrôleur multipoint.

Le contrôleur multipoint peut être intégré dans un portier, une passerelle, un terminal ou un pont de conférence. Voir Figure 22.



NOTE – La passerelle, le portier et le pont de conférence peuvent être regroupés dans le même dispositif.

H.323(06-06)_F22

Figure 22/H.323 – Emplacements possibles des contrôleurs (MC) et des processeurs multipoint (MP) dans un système H.323

Un contrôleur multipoint intégré dans un terminal n'est pas appelable. Il peut intervenir dans l'appel aux fins du traitement de la signalisation H.245 destinée à assurer des conférences multipoint ad hoc. Dans ce cas, il peut n'y avoir aucune distinction entre le contrôleur multipoint et la fonction de commande H.245 (voir § 6.2.8) du terminal. L'établissement de communications entre ces entités ne relève pas de la présente Recommandation.

Un contrôleur multipoint situé au même emplacement que le portier n'est pas appelable, contrairement à un pont de conférence situé au même emplacement qu'un portier, qui peut être appelable. Un pont de conférence situé au même emplacement qu'un portier peut fonctionner comme un pont de conférence indépendant. Un contrôleur multipoint situé au même emplacement qu'un portier peut être utilisé pour assurer des conférences multipoint ad hoc lorsque le portier reçoit les voies de commande H.245 en provenance des extrémités. Le portier peut ainsi aiguiller les voies de commande H.245 vers le contrôleur multipoint au début de la communication ou au moment où la conférence devient une conférence multipoint.

La passerelle peut faire fonction de terminal ou de pont de conférence. Lorsqu'elle fait fonction de terminal, la passerelle peut intégrer un contrôleur multipoint présentant les mêmes caractéristiques qu'un contrôleur multipoint intégré dans un terminal (voir ci-dessus).

Un pont de conférence comporte toujours un contrôleur multipoint. Le pont de conférence est appelable et le contrôleur multipoint traite la voie de commande H.245 au départ de toutes les extrémités.

Quand il existe au moins deux extrémités, dans une conférence ces extrémités doivent utiliser la procédure de choix du mode maître ou esclave de la Rec. UIT-T H.245 pour déterminer le contrôleur multipoint qui dirigera la conférence.

Après l'échange des capacités et le choix du mode maître ou esclave, le contrôleur multipoint peut d'abord assigner un numéro de terminal à une nouvelle extrémité à l'aide du message **terminalNumberAssign**. Le contrôleur multipoint doit ensuite informer les autres extrémités de la nouvelle extrémité participant à la conférence à l'aide du message **terminalJoinedConference**. La nouvelle extrémité peut demander la liste des autres extrémités de la conférence à l'aide du message **terminalListRequest**.

6.6 Caractéristiques du processeur multipoint

Le processeur multipoint reçoit les flux de signaux audio, vidéo et/ou de données en provenance des extrémités participant à une conférence multipoint centralisée ou hybride. Il traite ces flux de média et les renvoie aux extrémités.

Les communications entre le contrôleur multipoint et le processeur multipoint ne sont pas soumises à normalisation.

Le processeur multipoint peut traiter un ou plusieurs types de flux de média. Lorsqu'il traite des flux de signaux vidéo, il doit traiter les algorithmes vidéo et les formats correspondants comme indiqué au § 6.2.4. Lorsqu'il traite des flux de signaux audio, il doit traiter les algorithmes audio comme indiqué au § 6.2.5. Lorsqu'il traite des flux de signaux de données, il doit procéder comme indiqué au § 6.2.7.

Un processeur multipoint assurant le traitement vidéo doit assurer la commutation vidéo ou le mélange vidéo. La commutation vidéo est le processus de sélection de l'image que le processeur multipoint transmet aux terminaux d'une source à une autre. Les critères utilisés pour procéder à la commutation peuvent être déterminés par la détection d'un changement d'orateur (détecté par le niveau audio associé) ou par la commande H.245. Le mélange vidéo consiste à formater plusieurs sources vidéo dans le flux de signaux vidéo que le processeur multipoint envoie aux terminaux. Un exemple de mélange vidéo consiste à combiner quatre images sources dans une matrice de deux sur deux de l'image de sortie vidéo. Il incombe au contrôleur multipoint de déterminer les critères à

retenir pour le choix des sources à mélanger et le nombre de ces sources, en attendant que d'autres commandes soient définies. L'application des dispositions des Recommandations UIT-T de la série T.120 pour ces fonctions de commande appelle un complément d'étude.

Un processeur multipoint qui assure le traitement audio doit préparer N sorties audio à partir de M entrées audio par commutation ou mélange ou par une combinaison de ces deux procédés. Le mélange des signaux audio oblige à décoder les signaux audio d'entrée en signaux linéaires (MIC ou analogiques), à combiner linéairement les signaux et à recoder le résultat dans le format audio approprié. Le processeur multipoint peut éliminer ou atténuer certains des signaux d'entrée afin de réduire le bruit et d'autres signaux brouilleurs. Chaque sortie audio peut avoir un mélange différent de signaux d'entrée pour les besoins de conversations privées. Les terminaux doivent supposer que leurs signaux audio ne sont pas présents dans le flux de signaux audio qui leur est renvoyé. La suppression par le terminal de ses propres signaux audio de la sortie audio du processeur multipoint appelle un complément d'étude.

Un processeur multipoint qui assure le traitement des données T.120 doit pouvoir jouer le rôle du fournisseur d'un système MCS non situé en bout de ramification et devrait pouvoir jouer le rôle du fournisseur du système MCS situé au sommet de la hiérarchie. Un processeur multipoint peut aussi traiter des données non normalisées, des données d'usager transparentes ou d'autres types de données.

Le processeur multipoint peut assurer la conversion d'algorithmes et de formats, ce qui permet aux terminaux de participer à une conférence en différents modes SCM.

Le processeur multipoint n'est pas appelable mais le pont de conférence dont il fait partie est appelable. Le processeur multipoint ferme et ouvre les voies de médias.

6.7 Caractéristiques du pont de conférence

Le pont de conférence est une extrémité qui permet la mise en œuvre de conférences multipoint. Il doit être constitué d'un contrôleur multipoint et éventuellement d'un ou de plusieurs processeurs multipoint. Le pont de conférence utilise les messages et les procédures H.245 pour implémenter des caractéristiques analogues à celles qui sont décrites dans la Rec. UIT-T H.243.

Un pont de conférence type qui assure des conférences multipoint centralisées est constitué d'un contrôleur multipoint ainsi que d'un processeur multipoint de signaux audio, vidéo et de données. Un pont de conférence type qui assure des conférences multipoint décentralisées est constitué d'un contrôleur multipoint et d'un processeur multipoint de données conformes à la Rec. UIT-T T.120. Il a recours au traitement décentralisé des signaux audio et vidéo.

Le côté réseau d'une passerelle peut être un pont de conférence. Un portier peut aussi intégrer un pont de conférence. Il s'agit dans les deux cas d'équipements qui pour être situés au même emplacement n'en remplissent pas moins des fonctions indépendantes.

Le pont de conférence doit être appelable par d'autres extrémités selon les procédures du § 8.

6.8 Capacité multipoint

6.8.1 Capacité multipoint centralisée

Toutes les extrémités doivent avoir une capacité multipoint centralisée. Dans ce mode de fonctionnement, ces équipements communiquent avec le contrôleur multipoint du pont de conférence en mode point à point sur la voie de commande et avec le processeur multipoint sur les voies audio, vidéo et de données. Dans ce mode, le contrôleur multipoint assure des fonctions de commande multipoint H.245, le processeur multipoint assurant quant à lui la commutation ou le mélange des signaux vidéo, le mélange des signaux audio et la distribution des données multipoint T.120. Le processeur multipoint renvoie les flux de signaux vidéo, audio et de données ainsi obtenus aux extrémités. Le processeur multipoint peut avoir la capacité de convertir les différents

formats et débits de signaux audio, vidéo et de données, permettant ainsi aux extrémités de participer à la conférence en différents modes de communication.

Le pont de conférence peut utiliser la multidiffusion pour distribuer les flux médias traités si les extrémités participant à la conférence peuvent recevoir des émissions en multidiffusion. La distribution en multidiffusion de données appelle un complément d'étude.

Ce mode est indiqué par les capacités H.245 suivantes: **centralizedControl**, **centralizedAudio**, **centralizedVideo** et **centralizedData**. A titre facultatif, les capacités **distributedAudio** et **distributedVideo** peuvent être utilisées pour indiquer une distribution en multidiffusion de flux médias.

6.8.2 Capacité multipoint décentralisée

Les extrémités dotées d'une capacité multipoint décentralisée communiquent avec le contrôleur multipoint d'un pont de conférence, la passerelle, le portier ou l'extrémité en mode point à point sur la voie de commande H.245 et, à titre facultatif, avec un processeur multipoint sur des canaux de données. Les extrémités doivent avoir la capacité de multidiffuser leurs voies audio et vidéo à destination de toutes les autres extrémités participant à la conférence. Le contrôleur multipoint peut contrôler la ou les extrémités qui multidiffusent activement les signaux audio et/ou vidéo (en utilisant) par exemple la commande de contrôle de flux **flowControlCommand** sur l'une ou l'autre voie).

Les extrémités reçoivent les voies vidéo à multidiffusion et choisissent une ou plusieurs des voies disponibles pour présentation à l'usager. Les extrémités reçoivent les voies audio à multidiffusion et procèdent au mélange des signaux audio pour présenter un signal audio composite à l'usager.

Le contrôleur multipoint peut assurer des fonctions de commande de la conférence telles que les suivantes: présidence, diffusion des signaux vidéo et sélection du mode vidéo. Ces fonctions doivent être assurées par la commande de réception H.245 en provenance d'une extrémité, puis par l'envoi de la commande appropriée aux autres extrémités pour activer ou désactiver leur mode multidiffusion vidéo. Les commandes T.120 peuvent éventuellement assurer les mêmes fonctions.

Ce mode est indiqué par les capacités H.245 suivantes: **centralizedControl**, **distributedAudio**, **distributedVideo** et **centralizedData**.

6.8.3 Capacité audio hybride multipoint/centralisée

S'ils sont dotés d'une capacité audio hybride multipoint/centralisée, les extrémités et le pont de conférence peuvent utiliser la fonction multipoint répartie pour les signaux vidéo et la fonction multipoint centralisée pour les signaux audio. Dans ce mode, les extrémités communiquent avec le contrôleur multipoint en mode point à point sur la voie de commande H.245 et, à titre facultatif, avec un processeur multipoint sur des canaux de données.

Les extrémités doivent avoir la capacité de multidiffuser leurs voies vidéo à destination de toutes les autres extrémités participant à la conférence. Le contrôleur multipoint peut contrôler la ou les extrémités qui utilisent activement le mode multidiffusion vidéo. Les extrémités reçoivent les voies vidéo à multidiffusion et sélectionnent une ou plusieurs des voies disponibles pour présentation à l'usager.

Toutes les extrémités participant à la conférence transmettent leurs voies audio au processeur multipoint. Celui-ci assure la fonction de mélange des signaux audio et retransmet les flux de signaux audio ainsi obtenus aux extrémités. Le processeur multipoint peut totaliser exclusivement les signaux audio pour chaque extrémité participant à la conférence. La distribution en multidiffusion des signaux audio traités appelle un complément d'étude.

Ce mode est indiqué par les capacités H.245 suivantes: **centralizedControl**, **centralizedAudio**, **distributedVideo** et **centralizedData**.

6.8.4 Capacité vidéo hybride multipoint/centralisée

S'ils sont dotés d'une capacité vidéo hybride multipoint/centralisée, les extrémités et le pont de conférence peuvent utiliser la fonction multipoint répartie pour les signaux audio et la fonction multipoint centralisée pour les signaux vidéo. Dans ce mode, les extrémités communiquent avec le contrôleur multipoint en mode point à point sur la voie de commande H.245 et, à titre facultatif, avec un processeur multipoint sur des canaux de données.

Les extrémités doivent avoir la capacité de multidiffuser leurs voies audio à destination de toutes les autres extrémités participant à la conférence. Le contrôleur multipoint peut contrôler la ou les extrémités qui utilisent activement le mode multidiffusion audio. Les extrémités reçoivent les voies audio à multidiffusion et procèdent au mélange des signaux audio afin de présenter un signal audio composite à l'usager.

Toutes les extrémités participant à la conférence transmettent leurs voies vidéo au processeur multipoint. Celui-ci assure les fonctions de commutation, de mélange ou de conversion de format vidéo et retransmet les flux de signaux vidéo ainsi obtenus aux extrémités. Le processeur multipoint peut produire un flux de signaux vidéo exclusif pour chaque extrémité participant à la conférence, ou multidiffuser un flux de signaux vidéo à destination de toutes les extrémités participantes, afin de réduire au minimum la largeur de bande utilisée sur le réseau.

Ce mode est indiqué par les capacités H.245 suivantes: **centralizedControl**, **distributedAudio**, **centralizedVideo** et **centralizedData**.

6.8.5 Etablissement du mode commun

Le contrôleur multipoint doit coordonner un mode de communication commun entre les extrémités participant à la conférence multipoint. Il peut imposer aux extrémités un mode de transmission commun donné (admis par leurs ensembles de capacités) en envoyant à l'extrémité un ensemble de capacités de réception n'indiquant que le mode de transmission souhaité ou recourir à la commande de mode multipoint **multipointModeCommand** et aux commandes de préférence de mode pour imposer la symétrie de mode. Cette dernière manière de procéder devrait être utilisée car elle permet aux extrémités de connaître la gamme complète des capacités de conférence disponibles qui peuvent être demandées.

Si le pont de conférence a la capacité de convertir les formats audio et/ou vidéo, il peut ne pas être nécessaire d'imposer à toutes les extrémités le même mode de communication.

6.8.6 Adaptation du débit multipoint

Les extrémités pouvant tenter, sur chaque liaison d'une configuration multipoint, de fonctionner à des débits différents, le contrôleur multipoint doit envoyer des messages de commande de contrôle de flux **flowControlCommand** H.245 pour limiter les débits transmis à ceux qui peuvent être envoyés aux récepteurs.

6.8.7 Synchronisation labiale dans une conférence multipoint

Un processeur multipoint qui assure le mélange des signaux audio dans des conférences multipoint centralisées ou hybrides doit modifier les étiquettes temporelles des flux de signaux audio et vidéo, compte tenu de sa propre base de temps, afin de maintenir la synchronisation des signaux audio et vidéo. En outre, lorsqu'il traite les signaux audio et/ou vidéo pour émettre un nouveau flux émanant de lui, le processeur multipoint doit émettre ses propres numéros de séquence dans les paquets de signaux audio et vidéo.

Lorsqu'il mélange les signaux audio, le processeur multipoint doit synchroniser chacun des flux de signaux audio entrants sur son propre rythme, mélanger ces flux de signaux audio puis émettre un nouveau flux de signaux audio compte tenu de son propre rythme avec ses propres numéros de séquence. Si le processeur multipoint assure aussi la commutation vidéo, le flux commuté doit avoir son indication d'horodatage remplacée par la base de temps du processeur multipoint aux fins de

synchronisation avec le flux de signaux audio mélangés et doit avoir un nouveau numéro de séquence représentant le flux provenant du processeur multipoint.

Dans le cas de conférences multipoint réparties, l'extrémité réceptrice peut être en mesure de maintenir la synchronisation du mouvement des lèvres en alignant le flux de signaux vidéo choisi et le flux de signaux audio correspondant à l'aide d'étiquettes temporelles du protocole RTP. L'alignement des autres flux de signaux audio peut ne pas être nécessaire. En cas d'affichage de flux de signaux vidéo multiples, les flux de signaux audio associés devraient être alignés.

Il peut ne pas être possible de garantir la synchronisation labiale dans des conférences multipoint hybrides.

6.8.8 Chiffrement multipoint

Dans une configuration multipoint centralisée, le processeur multipoint est considéré comme étant une entité de confiance. Chaque accès du processeur multipoint déchiffre les flux d'information en provenance de chacune des extrémités H.323 et chiffre les flux d'information à destination de chaque extrémité, comme indiqué au § 10.1. L'exploitation d'un pont de conférence qui ne soit pas de confiance appelle un complément d'étude.

6.8.9 Ponts de conférence en cascade

La fonction de commande multipoint peut être répartie entre plusieurs ponts de conférence. Cette opération, appelée mise en cascade, permet à au moins deux contrôleurs multipoint de communiquer les uns avec les autres afin de gérer une conférence multipoint. La mise en cascade de contrôleurs multipoint consiste à établir une voie de commande H.245 entre eux. L'un des contrôleurs est défini comme jouant le rôle de maître, les autres jouant celui d'esclaves.

Les procédures de mise en cascade sont définies au § 8.4.5.

6.9 Modèles de services complémentaires

La capacité de prendre en charge une grande variété de services et d'éléments de service complémentaires est une exigence pour de nombreuses solutions téléphoniques, quelles qu'en soient les techniques sous-jacentes.

Pour un grand nombre de ces services, l'exigence précédente s'associe à celle de l'existence d'un haut niveau d'interopérabilité entre équipements issus de différents vendeurs, ce qui conduit à des solutions fondées sur des normes.

En même temps, les équipementiers exigent la capacité de fourniture de services mettant en évidence leurs propres produits. Cet objectif peut être atteint par des moyens propres au fournisseur, mais au prix de l'interopérabilité. Il peut arriver qu'une telle pénalité soit acceptable ou souhaitable, mais ce n'est pas souvent le cas.

L'objectif est donc de définir une norme suffisamment flexible pour pouvoir prendre en charge tous les services qu'un vendeur peut avoir à fournir (ou leur plus grand nombre).

Dans l'environnement H.323, il existe plusieurs méthodes permettant de fournir des services: les Recommandations UIT-T de la série H.450.x, la Rec. UIT-T H.248 en association avec ses blocs, l'Annexe L et l'Annexe K. Bien que toutes ces solutions présentent une similitude quant à certains objectifs de conception, leurs particularités varient et chacune convient mieux à certaines situations. Ces solutions représentent une palette d'options pour l'implémentation des systèmes et des éléments de service, allant d'une commande (fonctionnelle) d'homologue à homologue exclusivement à une commande (stimulée) de maître à esclave exclusivement, au moyen d'ordres de poste unique ou de poste tiers. Plutôt que concurrentes, elles sont complémentaires et laissent au développeur de système la liberté de choix.

Les Recommandations UIT-T de la série H.450.x s'appliquent à l'interopérabilité de services à un niveau fonctionnel. Leur évolution à partir de la signalisation QSIG assure l'interfonctionnement avec de nombreux systèmes privés de mise en réseau. Les services sont définis pour des relations d'homologue à homologue, la capacité d'autonomie étant normalement implantée dans l'extrémité. Un service de niveau H.450 doit normalement être explicitement pris en charge par chacune des extrémités concernées dans le système. Cette répartition de la commande des services permet aux extrémités d'être plus indépendantes et plus autonomes. Elle est théoriquement prise en charge par les extrémités évoluées.

Les autres protocoles permettent une commande au niveau du stimulus, dans laquelle une totale compréhension d'un service n'est normalement requise que par une seule entité, normalement dans une relation maître-esclave. De telles méthodes de type stimulus font appel à un ensemble de fonctions atomiques bien définies qui, en diverses combinaisons, fournissent un nombre quelconque de services.

Les protocoles de stimulus simplifient l'introduction de nouveaux services. Différentes implémentations du même service peuvent cependant différer suffisamment pour compliquer l'interopérabilité, même à l'intérieur du même type de réseau.

L'Annexe L, comme la Rec. UIT-T H.450, s'appuie sur la Rec. UIT-T H.323 et toutes les extrémités conformes à l'Annexe L sont par définition conformes à la Rec. UIT-T H.323. Elle autorise l'utilisation des procédures H.323 normalisées pour la signalisation d'appel et la commande de média. Outre la commande d'appel de base, des fonctions spéciales intelligentes sont implémentées dans un serveur à fonctions spéciales (associé à un portier ou à une extrémité H.323). Le protocole utilise la fourniture de services par un ou plusieurs serveurs à fonctions spéciales. L'Annexe L propose donc un modèle mixte conjuguant les modèles de commande homologue et de commande maître/esclave, dans lequel les fonctions intelligentes sont réparties entre l'extrémité et le serveur à fonctions spéciales.

L'Annexe K permet la commande par poste tiers d'un appel H.323 sur la base d'un canal de commande distincts (faisant appel au protocole HTTP [47]) pour l'interaction avec l'usager. Il n'y a pas d'ensemble de capacités fixe pour l'interface avec l'usager car divers types de format de texte, d'image et de son peuvent être utilisés dynamiquement en tant que types MIME [48] enregistrés. Le fournisseur de services (serveur HTTP) est chargé du mappage entre les événements HTTP et les actions de commande d'appel (messages H.450 ou autres) pour des services complémentaires, de sorte que l'extrémité H.323 n'est pas informée de l'application HTTP. Le fournisseur de services peut être associé au portier local, à l'extrémité distante ou au portier distant dans le cadre d'une communication.

Le protocole H.248 est un protocole générique "de commande de dispositif" de type passerelle qui est entièrement fondé sur un modèle de commande maître/esclave (à stimulus) dans lequel toute l'autonomie de commande est maintenue dans une entité centrale (le contrôleur de passerelle média ou MGC) et dans lequel l'extrémité (la passerelle média ou MG) est l'esclave. Le protocole H.248 est conçu de façon à être indépendant du protocole de commande d'appel: il n'exige donc pas que les extrémités soient conformes à la Rec. UIT-T H.323. Le protocole H.248 a été élaboré pour la commande de passerelles médias. Il implique une relation étroite entre le contrôleur MGC et la passerelle média, dans laquelle un usager ne peut souscrire aux éléments de service que d'un seul contrôleur MGC à la fois. Le protocole H.248 est conçu de façon à être facilement extensible au moyen de blocs de propriétés permettant de définir un support spécifique, de façon que les services pouvant être pris en charge par un système en mode H.248 ne soient limités que par les blocs acceptés par le contrôleur MGC et par la passerelle média.

7 Signalisation d'appel

On entend par signalisation d'appel les messages et les procédures utilisés pour établir une communication, demander des modifications de la largeur de bande de la communication, obtenir le statut des messages pour les extrémités participant à la communication et déconnecter la communication. La signalisation d'appel utilise les messages définis dans la Rec. UIT-T H.225.0 et les procédures décrites au § 8. Le présent paragraphe décrit un certain nombre de principes de signalisation d'appel.

7.1 Adresses

7.1.1 Adresse de réseau

Chaque entité H.323 doit avoir au moins une adresse de réseau. Cette adresse identifie spécifiquement l'entité H.323 du réseau. Certaines entités peuvent partager une adresse de réseau (par exemple, un terminal et un contrôleur multipoint situés au même emplacement). Cette adresse est propre à l'environnement de réseau dans lequel l'extrémité est située. Des environnements de réseaux différents peuvent avoir des formats d'adresse de réseaux différents.

Une extrémité peut utiliser différentes adresses de réseau pour les différentes voies participant à la même communication.

7.1.2 Identificateur de point TSAP

Pour chaque adresse de réseau, chaque entité H.323 peut avoir plusieurs identificateurs de point TSAP. Ces identificateurs de point TSAP permettent de multiplexer plusieurs voies partageant la même adresse de réseau.

Pour les extrémités, un identificateur de point TSAP communément admis est défini: l'identificateur de point TSAP de la voie de signalisation d'appel. Pour les portiers, un identificateur de point TSAP communément admis est défini: l'identificateur de point TSAP de la voie RAS et une adresse de multidiffusion communément admise est définie: adresse de multidiffusion de recherche: ces identificateurs et adresse sont définis dans l'Appendice IV/H.225.0.

Les extrémités et les entités H.323 devraient utiliser des identificateurs de point TSAP dynamiques pour la voie de commande, les voies audio, les voies vidéo et les canaux de données H.245. Le portier devrait utiliser un identificateur de point TSAP dynamique pour les voies de signalisation d'appel. Les voies RAS et les voies de signalisation peuvent être redirigées vers les identificateurs de point TSAP dynamiques au cours de la procédure d'enregistrement.

7.1.3 Adresse de pseudonyme

Une extrémité peut aussi avoir une ou plusieurs adresses de pseudonymes qui lui sont associées. Ces adresses peuvent désigner l'extrémité ou des conférences hébergées par l'extrémité. Les adresses de pseudonymes constituent une autre méthode d'adressage de l'extrémité. Ces adresses sont de type **dialledDigits** ou **partyNumber** (y compris les numéros de téléphone privés et les numéros E.164 publics), les identificateurs H.323 (chaînes alphanumériques représentant des noms, des adresses de type messagerie électronique, etc.) et toutes les autres adresses définies dans la Rec. UIT-T H.225.0. Les adresses de pseudonymes doivent être uniques à l'intérieur d'une zone. Les portiers, les contrôleurs multipoint et les processeurs multipoint ne doivent pas avoir d'adresses de pseudonymes.

NOTE – Les versions 1, 2 et 3 des Recommandations UIT-T H.323 et H.225.0 considéraient de façon générale les chiffres composés comme étant des adresses E.164 (et le paramètre **dialledDigits** avait la valeur **e164**) alors que ce n'était pas le cas. De même, ces versions des Recommandations UIT-T H.323 et H.225.0 considéraient les adresses E.164 comme des numéros publics d'abonné (le paramètre **e164number** avait la valeur **publicPartyNumber**) alors qu'il n'était précisé nulle part que les numéros publics d'abonné étaient des numéros E.164. Cette modification terminologique n'a aucune incidence que ce soit sur la compatibilité amont. On trouvera à l'Appendice V une analyse détaillée de l'utilisation des numéros E.164.

Lorsque le système ne comporte pas de portier, l'extrémité appelante doit joindre l'extrémité appelée directement à l'adresse de transport de la voie de signalisation d'appel de l'extrémité appelée. Dans le cas d'un système avec portier, l'extrémité appelante peut joindre l'extrémité appelée à son adresse de transport par la voie de signalisation d'appel ou à son adresse de pseudonyme. Le portier doit convertir cette adresse de pseudonyme en une adresse de transport sur la voie de signalisation d'appel.

L'adresse de type **dialledDigits** de l'extrémité appelée peut consister en un code d'accès facultatif suivi du numéro de téléphone propre au plan de numérotage du fournisseur de services. Le code d'accès est constitué de n chiffres de 0 à 9, *, et #. Le nombre de chiffres et leur signification sont laissés à l'appréciation du constructeur. Un tel code d'accès pourrait notamment servir à demander à accéder à une passerelle. Le portier peut modifier cette adresse avant de l'envoyer vers sa destination. Il peut également fournir un numéro d'abonné **partyNumber** à utiliser à la place des chiffres composés **dialledDigits**.

L'identificateur H.323 consiste en caractères ISO/CEI 10646 comme cela est défini dans la Rec. UIT-T H.225.0. Il peut s'agir d'un nom d'usager, d'un nom de conférence, d'un nom de messagerie électronique ou un autre identificateur.

Une extrémité peut avoir plusieurs adresses de pseudonymes (dont plusieurs du même type) converties dans la même adresse de transport.

7.1.4 Système H.323 de localisateur URL

L'un des types de pseudonyme définis par la présente Recommandation est l'identificateur **url-ID**, qui est destiné à contenir des séquences URL normalisées, qui pourront être utilisées pour atteindre des ressources. Une entité H.323 peut accepter tout localisateur URL valide qu'elle peut interpréter mais elle doit prendre en charge le localisateur URL H.323 tel qu'il est défini dans le présent paragraphe.

Le localisateur URL H.323 vise à aider une entité à résoudre l'adresse d'une autre entité H.323. Il se compose de deux parties: *l'usager* et *l'accès serveur*. L'*usager* spécifie un pseudonyme pour l'entité, tel qu'un usager ou un service, sans acheminer d'informations sur l'emplacement de cette entité. L'*accès serveur* est le nom de domaine du portier de l'extrémité ou de l'élément Border.

Le localisateur URL H.323 est défini en formalisme ABNF comme indiqué ci-après. Noter l'utilisation des règles fondamentales spécifiées au § 6.1 de [51].

```
H323-URL            =    "h323:" address [ url-parameters ]
address             =    user / "@" hostport / user "@" hostport
user                =    1*(%x21-24 / %x26-3F / %x41-7F / escaped)
                         ; Les symboles "%", "@", et les symboles ayant
                         ; une valeur de caractère inférieure à 0x21
                         ; peuvent être représentés sous forme de
                         ; séquences d'échappement.
hostport            =    host [ ":" port]
host                =    hostname / IPv4address / IPv6reference
hostname            =    *( domainlabel "." ) toplabel [ "." ]
domainlabel         =    alphanum / alphanum *( alphanum / "-" ) alphanum
toplabel            =    ALPHA / ALPHA *( alphanum / "-" ) alphanum
IPv4address         =    1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
IPv6reference       =    "[" IPv6address "]"
IPV6address         =    hexpart [ ":" IPv4address ]
hexpart             =    hexseq / hexseq "::" [ hexseq ] / "::" [ hexseq ]
hexseq              =    hex4 *( ":" hex4 )
hex4                =    1*4HEXDIG
port                =    1*DIGIT
url-parameters      =    *( ";" url-parameter )
url-parameter       =    1*(%x21-24 / %x26-3A / %x3C-7F / escaped)
                         ; Les définitions de paramètres spécifiques
```

```
                              ; appellent un complément d'étude.
                              ; Les symboles "%", ";", et les symboles
                              ; ayant une valeur de caractère inférieure à 0x21
                              ; peuvent être représentés sous forme de séquences
                              ; d'échappement.
     alphanum           =     ALPHA / DIGIT
     escaped            =     "%" HEXDIG HEXDIG
```

Le *serveur* n'est pas dépendant maj/min.

L'information *user* est une chaîne Unicode [19] qui doit être codée en UTF-8 et faire l'objet, au besoin, d'un échappement. A l'exception des caractères dont la valeur numérique est inférieure à 0x80, *user* dépend maj/min. Les caractères dont la valeur numérique est inférieure à 0x80 ne sont pas dépendant maj/min.

Le jeu de caractères et la dépendance maj/min de *url-parameter* sont spécifiés dans la définition de chaque paramètre.

Si une extrémité s'enregistre auprès d'un portier sans fournir de chaîne *hostport*, ce portier peut annexer une chaîne *hostport* au localisateur URL lorsqu'il renvoie les pseudonymes de l'extrémité dans un message de confirmation RCF. L'extrémité doit accepter le pseudonyme modifié et l'utiliser lors de l'envoi au portier de demandes ultérieures, y compris les messages URQ pour désenregistrer le pseudonyme.

7.2 Voie d'enregistrement, d'admission et de statut (RAS)

La voie (RAS, *registration, admission and status*) doit être utilisée pour acheminer les messages utilisés dans les processus de recherche du portier et d'enregistrement de l'extrémité qui associent l'adresse de pseudonyme d'une extrémité à son adresse de transport de la voie de signalisation d'appel. La voie RAS doit être une voie non fiable.

Etant donné que les messages RAS sont transmis sur une voie non fiable, la Rec. UIT-T H.225.0 recommande des temporisations et des comptages de répétition de tentative pour divers messages. Une extrémité ou un portier qui ne peut pas répondre à une demande au cours du délai spécifié pour la temporisation peut utiliser le message demande en cours (RIP, *request in progress*) pour indiquer qu'il est encore en phase de traitement de la demande. Une extrémité ou un portier recevant le message RIP doit réinitialiser son temporisateur et son compteur de répétitions de tentative.

7.2.1 Recherche du portier

On entend par recherche du portier le processus utilisé par une extrémité pour déterminer le portier auprès duquel elle souhaite se faire enregistrer. Ce processus peut être manuel ou automatique. La recherche manuelle fait appel à des méthodes ne relevant pas de la présente Recommandation pour déterminer le portier auquel une extrémité est associée. L'extrémité est configurée avec l'adresse de transport du portier associé. Par exemple, cette adresse peut être introduite dans la configuration de l'extrémité ou dans un fichier d'initialisation. Cela permet à l'extrémité de savoir préalablement à quel portier elle est associée. L'extrémité peut dès lors se faire enregistrer auprès de ce portier.

La méthode automatique permet de modifier dans le temps l'association extrémité-portier. L'extrémité peut ne pas savoir qui est son portier ou avoir besoin d'identifier un autre portier par suite d'un dérangement. Il peut utiliser à cet effet la recherche automatique. Celle-ci permet non seulement de réduire les frais administratifs de configuration de chacune des extrémités mais aussi de remplacer un portier existant sans avoir à reconfigurer manuellement toutes les extrémités affectées. Il convient de noter qu'il est également possible d'appliquer les procédures de portier attribué, exposées au § 7.2.6.1, pour automatiser l'attribution des extrémités à leur portier associé.

Pour recourir à cette méthode automatique, l'extrémité peut multidiffuser (ou recourir aux autres méthodes indiquées dans l'Appendice IV/H.225.0) un message de demande de portier (GRQ, *gatekeeper request*) demandant "Qui est mon portier?". Ce message est envoyé à l'adresse de

multidiffusion de recherche communément admise. Un ou plusieurs portiers peuvent répondre par le message de confirmation de portier (GCF, *gatekeeper confirmation*) indiquant "Je peux être votre portier." et contenant l'adresse de transport de la voie RAS du portier. Si un portier ne veut pas que l'extrémité se fasse enregistrer auprès de lui, il doit renvoyer le message de refus du portier (GRJ, *gatekeeper reject*). Voir Figure 23. Si plusieurs portiers lui répondent, l'extrémité peut choisir le portier qu'elle souhaite utiliser. A ce stade, l'extrémité sait auprès de quel portier se faire enregistrer. L'extrémité peut dès lors se faire enregistrer auprès de ce portier.

Si l'extrémité connaît déjà l'emplacement du portier, cette extrémité peut encore choisir de monodiffuser la demande GRQ jusqu'au portier afin d'effectuer un échange de données cryptographiques de type H.225.0.

'

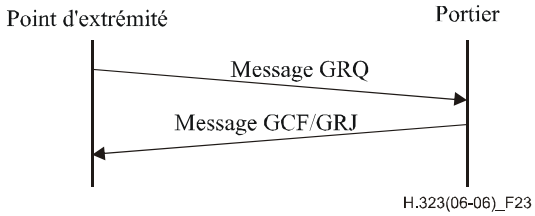


Figure 23/H.323 – Recherche automatique

Afin d'assurer la redondance dans les systèmes faisant appel à un portier, celui-ci peut indiquer des entités homologues à lui-même qui peuvent être utilisées en cas de défaillance d'un portier primaire. Cette liste de portiers secondaires est fournie dans le champ **alternateGatekeeper** des messages GCF/GRJ et RCF/RRJ. L'extrémité peut également appliquer les procédures de portier attribué pour s'enregistrer de nouveau auprès de son portier primaire, lorsque celui-ci redevient disponible. Le portier peut fournir à l'extrémité l'adresse du portier qui lui est attribué dans le champ **assignedGatekeeper** des messages GCF/GRJ et RCF/RRJ.

Si aucun portier ne répond dans un certain délai, l'extrémité peut réémettre le message GRQ. Une extrémité ne doit pas envoyer de message GRQ dans les 5 secondes qui suivent l'envoi d'un précédent message GRQ. Si aucune réponse n'est reçue, l'extrémité peut utiliser la méthode de recherche manuelle.

Si à un moment quelconque une extrémité constate qu'elle n'est pas validement enregistrée auprès de son portier, elle doit relancer la procédure de recherche de son portier. L'extrémité peut supposer qu'un enregistrement est non valide si un message RRJ est renvoyé par un portier en réponse à un message RRQ ou si aucune réponse à une demande RRQ n'est reçue dans un certain délai.

Le message GRQ peut être répété périodiquement (c'est-à-dire à la mise sous tension de l'extrémité), de manière que le portier puisse traiter plusieurs demandes émanant de la même extrémité.

7.2.2 Enregistrement d'une extrémité

On entend par *enregistrement* le processus par lequel une extrémité intègre une zone et informe le portier de ses adresses de transport et de ses adresses de pseudonymes. Dans le cadre de leurs processus de configuration, toutes les extrémités doivent se faire enregistrer auprès du portier identifié par la procédure de recherche. L'enregistrement doit être effectué avant toute tentative d'appel et peut être renouvelé périodiquement en cas de besoin (par exemple, à la mise sous tension de l'extrémité).

Une passerelle ou un pont de conférence peut enregistrer une unique adresse de transport ou plusieurs adresses de transport comme son adresse de signalisation d'appel et peut enregistrer une unique adresse de transport ou plusieurs adresses de transport comme son adresse RAS. L'utilisation

d'adresses de transport multiples comporte obligatoirement l'indication d'une liste hiérarchisée d'adresses à essayer pour communiquer avec une extrémité donnée, soit par sa voie RAS, soit par sa voie de signalisation d'appel.

Une extrémité doit envoyer un message de demande d'enregistrement (RRQ, *registration request*) à un portier. Ce message est envoyé à l'adresse de transport de la voie RAS du portier. L'extrémité connaît l'adresse du réseau du portier à l'issue de la procédure de recherche de celui-ci et utilise l'identificateur de point TSAP de la voie RAS généralement admis. Le portier doit répondre par un message de confirmation d'enregistrement (RCF, *registration confirmation*) ou de refus d'enregistrement (RRJ, *registration reject*). Voir Figure 24. Une extrémité ne doit se faire enregistrer qu'auprès d'un seul portier.

Le message RRQ peut être répété périodiquement (par exemple, à la mise sous tension du terminal), afin que le portier puisse traiter plusieurs demandes émanant de la même extrémité. Si un portier reçoit un message RRQ ayant la même adresse de pseudonyme (ou liste d'adresses de pseudonymes) et les mêmes adresses de transport qu'un précédent message RRQ, il doit répondre par un message RCF. Si un portier reçoit un message RRQ ayant la même adresse de pseudonyme (ou la même liste d'adresses de pseudonymes) que le précédent message RRQ et des adresses de transport différentes, il peut confirmer la demande si celle-ci est conforme à la politique d'enregistrement du portier. Si ce n'est pas le cas, il devrait refuser la demande d'enregistrement au motif que l'enregistrement ferait double emploi ou ne serait pas valide. Si le portier reçoit un message RRQ ayant les mêmes adresses de transport qu'un précédent message RRQ et une adresse de pseudonyme différente (ou une liste d'adresses de pseudonymes différente) et si le message RRQ n'est pas spécifié en tant que message RRQ additif, il devrait remplacer les inscriptions figurant dans la table de conversion. Le portier peut recourir à une méthode d'authentification de ces modifications.

Une extrémité peut indiquer des adresses de repli, redondantes ou substitutives en utilisant la structure **alternateEndpoint** dans les messages RAS. Cela permet à l'extrémité de se replier sur une interface secondaire avec le réseau ou sur une extrémité H.323 secondaire. Le portier doit refuser les enregistrements ambigus. Il peut refuser l'enregistrement pour d'autres raisons (modification de la procédure de recherche ou problèmes de sécurité, par exemple).

Si l'extrémité n'introduit pas d'adresse de pseudonyme dans le message RRQ, le portier peut en attribuer une. Le portier doit renvoyer au terminal l'adresse de pseudonyme ainsi attribuée dans le message RCF.

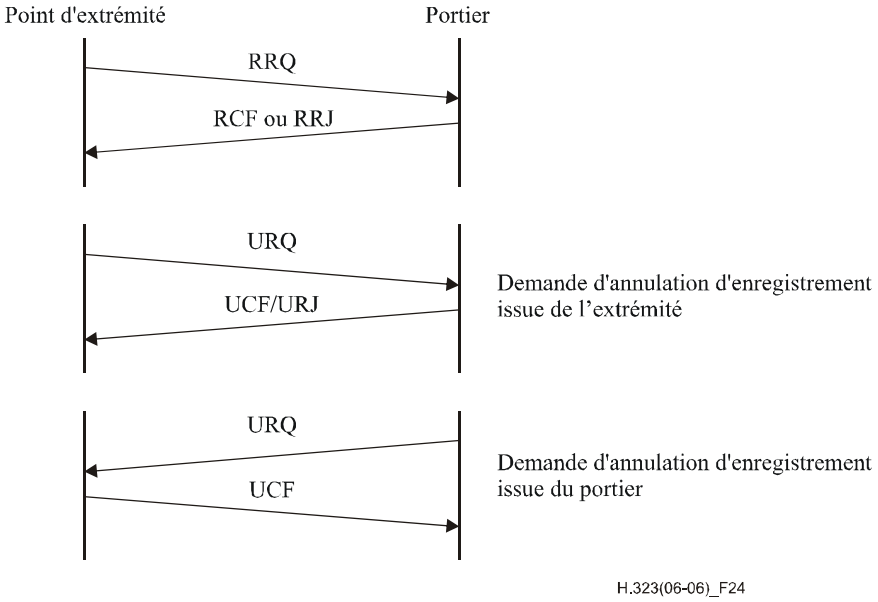


Figure 24/H.323 – Enregistrement

Une extrémité peut annuler son enregistrement en envoyant un message de demande d'annulation d'enregistrement (URQ, *unregister request*) au portier, ce qui permet à une extrémité de modifier l'adresse de pseudonyme associée à son adresse de transport ou vice versa. Le portier doit répondre, selon sa politique, par un message de confirmation d'annulation d'enregistrement (UCF, *unregister confirmation*) ou par un message de rejet d'annulation d'enregistrement (URJ, *unregister reject*).

Si l'extrémité envoie un message URQ contenant une liste d'adresses de pseudonymes, le portier doit seulement annuler l'enregistrement des pseudonymes énumérés, s'il choisit d'accepter la demande. Si l'extrémité envoie un message URQ ne contenant aucune adresse de pseudonyme, le portier doit annuler l'enregistrement de tous les pseudonymes de cette extrémité, s'ils existent et s'il choisit d'accepter la demande.

Un portier peut annuler l'enregistrement d'une extrémité en envoyant un message de demande d'annulation d'enregistrement (URQ) à l'extrémité. Celle-ci doit répondre par un message de confirmation d'annulation d'enregistrement (UCF). L'extrémité doit essayer de se faire réenregistrer auprès d'un portier avant de lancer toute nouvelle tentative d'appel. Cela peut exiger que l'extrémité se fasse enregistrer auprès d'un nouveau portier.

Si le portier envoie un message URQ contenant une liste d'adresses de pseudonymes, l'extrémité doit supposer que l'enregistrement de ces seules adresses de pseudonymes sera annulé. Un message URQ qui ne contient aucune adresse de pseudonyme indiquera une demande d'annulation d'enregistrement de l'extrémité.

Une extrémité qui n'est pas enregistrée auprès d'un portier est appelée *extrémité non enregistrée*. N'ayant pas à demander une autorisation d'admission à un portier, une extrémité de ce type ne peut pas participer aux fonctions de contrôle des admissions, de régulation de largeur de bande, de conversion d'adresses ou autres, exécutées par le portier.

7.2.2.1 Utilisation du message RRQ "allégé"

L'enregistrement d'une extrémité auprès d'un portier peut avoir une durée de vie finie. Une extrémité peut demander une durée **timeToLive** dans le message RRQ adressé au portier. Celui-ci peut répondre par un message RCF contenant la même durée **timeToLive**, une durée supérieure ou une durée inférieure. Si elle ne peut pas prendre en charge la durée **timeToLive** supérieure proposée par le portier, l'extrémité doit utiliser la durée **timeToLive** la plus longue qu'elle puisse admettre et

qui soit inférieure à la durée **timeToLive** proposée par le portier. A l'expiration de cette durée l'enregistrement doit se terminer. La durée **timeToLive** est exprimée en secondes. Avant l'expiration de la durée, l'extrémité peut envoyer un message RRQ dont le bit **keepAlive** est activé. Un tel message peut comporter une quantité minimale d'informations, comme indiqué dans la Rec. UIT-T H.225.0. Ce message RRQ de "maintien d'enregistrement" doit réinitialiser le temporisateur de durée de vie au niveau du portier afin de permettre l'allongement de la durée de l'enregistrement. Au moment de l'expiration, l'extrémité doit se réenregistrer auprès d'un portier au moyen d'un message RRQ complet.

Si le portier n'introduit pas de valeur **timeToLive** dans le message RCF, l'extrémité enregistrée considérera que le portier ne prend pas en charge le mécanisme de maintien d'enregistrement. Les extrémités ne doivent pas envoyer de message RRQ dont le champ **keepAlive** est réglé sur des portiers qui ont indiqué qu'ils ne prennent pas en charge le mécanisme de maintien d'enregistrement. Un portier ne devrait pas supposer qu'une extrémité prend en charge le mécanisme de maintien d'enregistrement si l'extrémité n'indique aucune valeur **timeToLive** dans le message RRQ.

Les portiers ne doivent pas considérer comme un enregistrement complet un message RRQ dont le champ **keepAlive** est activé (c'est-à-dire pour la mise à jour ou l'initialisation de ses tables de conversion).

Les extrémités doivent tenir compte du temps nécessaire à la messagerie et au traitement lorsqu'ils déterminent à quel moment leur enregistrement chez le portier prendra fin (c'est-à-dire la durée de leur propre temporisateur de durée de vie).

L'expiration du temporisateur de durée de vie chez le portier se traduit par l'expiration de l'enregistrement de l'extrémité. Un portier peut envoyer une demande URQ à l'extrémité à titre de notification d'une telle expiration. Cela tient compte de la perte de synchronisation entre les temporisateurs de durée de vie du portier et l'extrémité, et indique aussi la nécessité de se réenregistrer aux extrémités qui ne prennent pas en charge le mécanisme de maintien d'enregistrement.

Une extrémité qui envoie un message RRQ "allégé" à son portier après l'expiration du temporisateur de durée de vie chez le portier recevra une réponse RRJ avec le motif **rejectReason** de **fullRegistrationRequired** ou de **discoveryRequired**, selon les exigences du portier.

Une extrémité qui envoie une demande ARQ à son portier après l'expiration du temporisateur de vie chez le portier recevra un refus d'admission avec le motif **rejectReason** de **callerNotRegistered** ou de **calledPartyNotRegistered**. Une extrémité qui lance un nouvel appel via son portier après l'expiration du temporisateur de durée de vie auprès du portier recevra un message Release Complete accompagné du motif de **callerNotRegistered** ou de **calledPartyNotRegistered**.

L'élimination des appels subsistants à l'expiration du temporisateur de durée de vie est fonction de l'implémentation.

7.2.2.2 Utilisation d'enregistrements additifs

La prise en charge d'enregistrements additifs est facultative aussi bien dans le portier que dans l'extrémité. Un portier qui prend en charge les enregistrements additifs doit l'indiquer en incluant le champ **supportsAdditiveRegistration** dans le message RCF et doit suivre les procédures exposées dans le présent paragraphe. Par ailleurs, une extrémité ne doit pas utiliser la procédure d'enregistrement additif qui est décrite dans le présent paragraphe si le champ **supportsAdditiveRegistration** du message RCF est absent.

Si le portier reçoit un message RRQ avec le champ **additiveRegistration** inclus, il doit traiter ce message comme une information complémentaire à un enregistrement existant pour l'extrémité spécifiée dans le champ **endpointIdentifier**. S'il reçoit un message RRQ de type additif, le portier doit ajouter le pseudonyme (ou la liste de pseudonymes) aux entrées existantes de la table de conversion pour l'extrémité, à partir des champs **terminalAlias** et **terminalAliasPattern**. De

même, le portier doit ajouter aux entrées existantes de la table de conversion pour l'extrémité le champ **supportedPrefixes** du paramètre **terminalType**. Les éventuelles adresses de pseudonymes ou les éventuels préfixes pris en charge, déjà enregistrés pour l'extrémité, doivent rester enregistrés. Le portier doit remplacer les adresses de signalisation d'appel et les adresses de signalisation RAS de l'extrémité par les valeurs spécifiées dans les champs **callSignalAddress** et **rasAddress**, s'ils sont présents. Il doit remplacer également les extrémités de remplacement par les valeurs spécifiées dans le champ **alternateEndpoints**, s'il est présent. Le champ **keepAlive** doit avoir la valeur FALSE si le champ **additiveRegistration** est inclus dans le message RRQ. La réception d'un message RRQ additif doit cependant provoquer le redémarrage, par le portier, du compteur de durée de vie d'extrémité, si un tel compteur est déjà armé.

Une extrémité non enregistrée qui envoie un message RRQ additif à son portier reçoit une réponse RRJ avec la cause de rejet **rejectReason** à la valeur **fullRegistrationRequired** ou **discoveryRequired**, selon les exigences du portier.

NOTE – Comme un message RRQ additif n'est pas un enregistrement complet, le portier peut négliger les champs de ce message non spécifiquement mentionnés ci-dessus.

7.2.3 Localisation d'extrémités

Une extrémité ou un portier qui a une adresse de pseudonyme pour une extrémité et qui souhaiterait en déterminer l'information de contact peut émettre un message de demande de localisation (LRQ, *location request*). Ce message peut être envoyé à un identificateur spécifique de point TSAP d'accès au portier par voie RAS, ou être multidiffusé, comme le message GRQ, à l'adresse de multidiffusion de recherche communément admise du portier. Le portier auprès duquel l'extrémité demandée est enregistrée doit répondre par le message de confirmation de localisation (LCF, *location confirmation*) contenant l'information de contact du portier du ou des points d'extrémité. Ces informations de contact doivent comporter les adresses de la voie de signalisation d'appel et de la voie RAS à utiliser pour atteindre l'extrémité, ainsi que les informations facultatives sur la destination qui peuvent préciser le numéro et le prolongement de la ligne de l'extrémité recherchée.

Tous les portiers qui reçoivent le message LRQ sur la voie RAS et auprès desquels l'extrémité demandée n'est pas enregistrée doivent renvoyer le message de refus de localisation (LRJ, *location reject*). Tout portier qui reçoit le message LRQ sur l'adresse de multidiffusion de recherche et auprès duquel l'extrémité demandée n'est pas enregistrée ne doit pas répondre à ce message LRQ.

Une extrémité ou un portier peut inclure un ou plusieurs prolongements de type **dialledDigits** ou **partyNumber** auxquels il souhaite se connecter, en les insérant dans le champ **destinationInfo** du message LRQ pour tenter de localiser une passerelle disponible à l'extérieur de sa propre zone. Un portier qui reçoit un message LRQ demandant une passerelle disponible n'est pas obligé de mettre ses propres passerelles à la disposition d'une telle demande.

Un portier peut être informé de l'adresse de pseudonyme et des informations de connexion des extrémités sur le RCC. Ce portier peut répondre à un message LRQ demandant des informations sur l'extrémité RCC en envoyant les informations de connexion nécessaires pour atteindre cette extrémité. Il s'agira des informations nécessaires pour s'adresser à la passerelle ainsi qu'à l'extrémité RCC. Noter que l'extrémité RCC n'est pas enregistrée auprès du portier en ce sens qu'elle échange avec lui des messages RRQ/RCF. La méthode permettant à un portier de prendre connaissance des informations sur l'extrémité RCC est hors du domaine d'application de la présente Recommandation.

7.2.4 Admissions, modification de largeur de bande, indication d'état et libération

La voie RAS est également utilisée pour la transmission des messages d'admission, de modification de largeur de bande, d'indication d'état et de libération. Ces messages, échangés entre une extrémité et un portier, sont utilisés pour assurer des fonctions de contrôle des admissions et de gestion de la largeur de bande. Les modalités d'utilisation de ces messages sont exposées au § 8.

Le message de demande d'admission (ARQ, *admission request*) indique la largeur de bande d'appel demandée. Cette largeur de bande détermine la limite supérieure du débit composite de toutes les voies audio et vidéo d'émission et de réception non compris les en-têtes RTP, les en-têtes de charge utile RTP, les en-têtes de réseau et autres préfixes. Les canaux de données et de commande ne sont pas compris dans cette limite. Le portier peut réduire la largeur de bande d'appel demandée dans le message de confirmation d'admission (ACF, *admission confirm*). Une extrémité doit veiller à ce que la moyenne sur une seconde du débit composite de toutes les voies audio et vidéo d'émission et de réception soit égal ou inférieur à la largeur de bande d'appel. Une extrémité ou le portier peut tenter de modifier la largeur de bande d'appel au cours d'une communication en utilisant le message de demande de modification de largeur de bande (BRQ, *bandwidth change request*).

Le message de séquence de confirmation d'admission permet au portier de fournir une seule réponse à un message ARQ contenant l'information de routage par voie détournée, diverses informations de base, divers jetons, etc. Lorsqu'elle reçoit un message de séquence de confirmation d'admission contenant plusieurs messages ACF, une extrémité doit traiter le premier message ACF de la séquence en tentant d'établir la communication comme indiqué dans la présente Recommandation. Dans le cas où elle n'est pas en mesure d'établir la communication en raison d'un dérangement inopiné, l'extrémité peut sélectionner le prochain message ACF de la séquence et procéder à une nouvelle tentative d'établissement de la communication sans consulter préalablement le portier. On entend par "dérangements inopinés" des phénomènes tels que les suivants: circuits occupés, problèmes de routage de transport ("pas de route à destination du serveur", par exemple), ou saturation des ressources du portier, entre autres. En cas d'échec de routage, il appartient à l'extrémité concernée de décider si elle souhaite procéder à de nouvelles tentatives d'établissement de la communication par voie détournée.

Les extrémités qui choisissent de prendre en charge le message de séquence de confirmation d'admission doivent indiquer cette capacité en mettant le champ **acfSequences** du message RRQ à la valeur "TRUE". Le portier doit considérer l'absence de ce champ comme correspondant à une valeur "FALSE". Aucun portier ne doit envoyer le message de séquence de confirmation d'admission à une extrémité qui n'a pas indiqué dans le message RRQ son intention de prendre en charge ce message. Une extrémité peut modifier la valeur du champ **acfSequences** dans des messages RRQ ultérieurs. Dans le cas où elle modifie de "TRUE" à "FALSE" la valeur de ce champ, l'extrémité doit être prête à recevoir, le cas échéant, des messages de séquence de confirmation d'admission en transit, pour avoir précédemment annoncé son intention de prendre en charge de tels messages.

Etant donné que la séquence de confirmation d'admission n'est qu'un moyen de fournir l'information de routage par voie détournée – laquelle information ne pourrait pas être fournie dans un message de confirmation d'admission – aucune distinction supplémentaire n'est établie en d'autres parties de la présente Recommandation quant à la différence sémantique entre les termes "message de confirmation d'admission" et "message de séquence de confirmation d'admission". D'un bout à l'autre de la présente Recommandation, le terme "confirmation d'admission" ou "ACF" désigne indifféremment un simple message de confirmation d'admission ou un message de séquence de confirmation d'admission.

7.2.5 Jetons d'accès

Un jeton d'accès est une chaîne transmise dans certains messages RAS et dans le message Setup. Les jetons d'accès ont deux fonctions. Tout d'abord, ils peuvent assurer le secret des communications en faisant écran entre un appelant et l'adresse de transport et l'information d'adresse de pseudonyme d'une extrémité. Un utilisateur peut ne donner à un appelant que le jeton d'accès lui permettant d'atteindre l'extrémité. Le portier connaîtra l'extrémité associée au jeton d'accès d'après le processus d'enregistrement, de façon que les appels utilisant le jeton d'accès puissent être acheminés par le portier jusqu'à l'extrémité appelée. L'utilisation du jeton d'accès ne

s'applique qu'au modèle d'appels acheminés par le portier lors d'un essai de suppression de visibilité, par l'extrémité, de l'adresse de transport.

La deuxième fonction du jeton d'accès est de faire en sorte que les communications soient acheminées correctement à travers des entités H.323. Un jeton d'accès renvoyé par un portier doit être utilisé dans tous les messages d'établissement envoyés ultérieurement par l'extrémité. Ce jeton d'accès peut être utilisé par une passerelle pour vérifier que l'extrémité est habilitée à utiliser les ressources de passerelle. Il peut également être utilisé par une extrémité appelée pour vérifier que l'extrémité appelante peut lui envoyer directement ses trames de signalisation.

Le jeton d'accès peut également être réparti par des méthodes hors bande afin d'assurer un accès approprié aux passerelles et aux extrémités dans les systèmes qui ne possèdent pas de portiers.

7.2.6 Procédures de portier de remplacement

Afin d'assurer la disponibilité, la redondance et la modularité du système, le portier peut offrir une fonction de signalisation RAS en utilisant plusieurs dispositifs physiques ou logiques, dénommés *portiers de remplacement.* Si l'extrémité prend en charge les procédures de portier de remplacement définies dans le présent paragraphe, elle doit inclure le champ **supportsAltGK** dans les messages GRQ et RRQ.

Lorsqu'une extrémité établit une communication avec le portier, elle peut être munie, par le message GCF, d'une liste des portiers de remplacement. Si le portier ne répond pas au message RRQ subséquent, l'extrémité doit tenter de s'enregistrer auprès de ce portier au moyen de la liste de portiers de remplacement qui lui a été fournie par le message GCF. Si aucun portier de remplacement ne répond, l'extrémité doit réinitialiser le processus de recherche du portier.

Si l'extrémité reçoit un message GRJ contenant des informations de portier de remplacement mais qu'elle ne reçoive pas de message GCF, elle doit envoyer des messages GRQ à un ou plusieurs portiers figurant dans la liste de portiers de remplacement reçue dans le message GRJ. Si plusieurs messages GRJ sont reçus, l'extrémité peut en choisir un, dont elle extraira les informations sur les portiers de remplacement. Si aucun portier de remplacement n'envoie de message GCF, l'extrémité peut tenter d'utiliser l'une quelconque des nouvelles listes de portiers de remplacement reçues pour la recherche du portier, ou peut réinitialiser le processus de recherche du portier.

Si l'extrémité n'est pas encore enregistrée auprès du portier ou a réinitialisé le processus de recherche du portier, elle doit négliger le champ **needToRegister** dans la liste de portiers de remplacement et partir du principe que la valeur de ce champ est "TRUE".

Si l'extrémité est enregistrée auprès du portier et que celui-ci devienne inerte, l'extrémité doit tenter de communiquer avec un portier de remplacement. Elle peut ensuite appliquer les procédures de portier attribué, exposées au § 7.2.6.1, pour s'enregistrer de nouveau auprès de son portier primaire automatiquement, lorsque celui-ci redevient disponible.

Le portier peut renvoyer explicitement une extrémité vers un portier de remplacement en retournant un message de rejet de signalisation RAS contenant une liste de portiers de remplacement. Si le champ **altGkisPermanent** est mis à la valeur "FALSE" lors d'un tel renvoi, celui-ci est considéré comme temporaire car il ne s'applique qu'à un seul message de signalisation RAS.

Un portier peut envoyer une demande URQ à une extrémité avec une liste de portiers de remplacement, auquel cas l'extrémité doit répondre par un message UCF et tenter de communiquer avec un portier de remplacement. Une extrémité ne doit pas inclure de liste de portiers de remplacement dans un quelconque message URQ qu'elle envoie.

Une extrémité ne doit conserver qu'une seule liste de portiers de remplacement. Cette liste doit être extraite de la liste de portiers de remplacement qui a été reçue le plus récemment dans un message RAS quelconque, avec la seule exception que si l'extrémité est temporairement renvoyée vers un portier de remplacement et celui-ci renvoie un message de rejet avec une liste de portiers de

remplacement (même si cette liste est vide), l'extrémité doit interpréter ce rejet comme un renvoi. Elle peut négliger la liste de portiers de remplacement fournie lors d'un tel renvoi et continuer à utiliser la liste de portiers de remplacement qui a été envoyée dans le message de rejet initial.

Si le portier souhaite supprimer la liste des portiers de remplacement de l'extrémité, de sorte que lorsque le portier est reconfiguré pour ne pas utiliser des portiers de remplacement, il doit renvoyer une liste vide de portiers de remplacement (c'est-à-dire une liste ne contenant aucun élément) à l'extrémité en question dans le message RCF. Le fait d'omettre le paramètre facultatif **alternateGatekeeper** dans le message RCF indique à l'extrémité qu'elle doit conserver la liste existante de portiers de remplacement.

L'extrémité doit utiliser le champ **priority** pour indiquer l'ordre de communication avec les portiers de remplacement. Si plusieurs de ces derniers sont spécifiés avec la même valeur du champ **priority**, l'extrémité peut, éventuellement, mettre en séquence les portiers de remplacement ayant la même valeur du champ **priority**.

Lorsqu'une extrémité est renvoyée vers un portier de remplacement temporaire, elle doit négliger le champ **needToRegister** et considérer que sa valeur est "FALSE" puis ne réémettre le message de signalisation RAS renvoyé que vers un portier de remplacement temporaire. Tous les autres messages de signalisation RAS doivent continuer à être envoyés au portier principal comme d'habitude. Noter que cela n'empêche pas le portier de renvoyer temporairement une extrémité vers un portier de remplacement en renvoyant un message RRJ en réponse à un message RRQ normal ou allégé.

Si des demandes de signalisation RAS distinctes sont renvoyées vers des portiers de remplacement temporaires, chaque message distinct ne doit être envoyé qu'à un seul portier de remplacement temporaire à la fois, bien que différents messages de signalisation RAS puissent être envoyés simultanément à différents portiers de remplacement temporaires. Si l'extrémité détermine qu'un portier de remplacement temporaire est inerte, elle doit tenter de réémettre la demande de signalisation RAS vers un autre portier de remplacement. Si tous les portiers de remplacement sont insensibles à une demande de signalisation RAS, l'extrémité doit partir du principe que cette demande est rejetée. Si la demande était du type RRQ, l'extrémité doit réinitialiser le processus de recherche de portier.

Si le portier devient inerte ou renvoie l'extrémité en retournant une liste de portiers de remplacement avec le champ **altGKisPermanent** mis à la valeur "TRUE", l'extrémité doit tenter de communiquer avec un et un seul portier de remplacement. Ce n'est que lorsqu'elle a déterminé qu'un portier de remplacement est inerte qu'elle doit tenter de communiquer avec le portier de remplacement suivant. Si tous les portiers de remplacement sont inertes, l'extrémité doit réinitialiser le processus de recherche de portier. Si un enregistrement est requis auprès d'un portier de remplacement, l'extrémité doit d'abord tenter d'envoyer une demande RRQ à ce portier de remplacement, plutôt qu'une demande GRQ. Ce n'est que si le portier renvoie un message RRJ avec la cause **discoveryRequired** que l'extrémité doit envoyer une demande GRQ au portier de remplacement. Lors d'une transition permanente vers un portier de remplacement, l'extrémité doit envoyer tous les autres messages RAS à ce portier de remplacement, y compris les demandes RAS en instance qui arrivent à expiration. L'extrémité doit normalement réinitialiser les compteurs de tentatives d'envoi d'éventuels messages RAS en instance, avant de les envoyer au portier de remplacement pour la première fois. Elle peut ensuite appliquer les procédures de portier attribué, exposées au § 7.2.6.1, pour s'enregistrer de nouveau auprès de son portier primaire automatiquement, lorsque celui-ci redevient disponible.

Si un portier de remplacement, vers lequel une extrémité est renvoyée, retourne un message de rejet sans liste de portiers de remplacement, l'extrémité doit accepter ce message en tant que rejet de la demande initiale. Si le rejet visait une demande RRQ, l'extrémité doit réinitialiser le processus de recherche de portier. Si le portier de remplacement renvoie l'extrémité en retournant un message de rejet avec une liste de portiers de remplacement, cette extrémité doit tenter d'envoyer la demande à

un autre portier (de remplacement). Si tous les portiers de remplacement renvoient l'extrémité, celle-ci doit finalement considérer que la demande est rejetée.

Une extrémité ne doit pas envoyer de message URQ lorsqu'elle effectue une transition entre portiers de remplacement, même si le champ **needToRegister** a la valeur "TRUE", sauf si le portier envoie un message URQ avec une liste de portiers de remplacement.

Si une extrémité est renvoyée à un portier de remplacement qui est spécifié comme étant permanent (c'est-à-dire que le champ **altGKisPermanent** a la valeur "TRUE") ou si cette extrémité a été forcée de commencer à communiquer avec un portier de remplacement après avoir constaté l'inertie de son portier principal, cette extrémité doit partir du principe que le portier de remplacement est disposé à accepter des demandes relatives à des communications en cours. Elle doit envoyer à ce portier de remplacement tous les messages BRQ, DRQ et IRR subséquents, concernant des communications en cours. De même, le portier de remplacement doit être disposé à traiter de tels messages. Elle peut ensuite appliquer les procédures de portier attribué, exposées au § 7.2.6.1, pour s'enregistrer de nouveau auprès de son portier primaire automatiquement, lorsque celui-ci redevient disponible.

Si une extrémité commence à communiquer avec un portier de remplacement auprès duquel l'enregistrement n'a pas été exigé, y compris les portiers de remplacement temporaires, le champ **gatekeeperIdentifier** des messages URQ, ARQ, BRQ, LRQ et DRQ doivent contenir l'identificateur **gatekeeperIdentifier** du portier de remplacement extrait de la liste des portiers de remplacement. Ce champ ne peut pas être présent lorsque l'enregistrement est requis.

7.2.6.1 Procédures de portier attribué

La procédure de portier attribué est une procédure facultative découlant des procédures de portier de remplacement exposées ci-dessus. La combinaison de ces deux procédures donne lieu à un système avec redondance plus robuste qui permet à l'extrémité de "basculer" vers l'un de ses portiers de remplacement, lorsque son portier attribué devient inactif et de "retourner" ensuite à son portier attribué, lorsque celui-ci redevient actif.

Il convient d'insérer le champ **assignedGatekeeper** uniquement dans des messages provenant du portier, si le champ **alternateGatekeeper** est également présent, même dans le cas où la liste contenue dans le champ **alternateGatekeeper** est vide. Si elle prend en charge les procédures de portier attribué exposées dans le présent paragraphe, l'extrémité doit inclure le champ **supportsAssignedGK** dans ses messages GRQ et RRQ.

Un seul portier peut être désigné comme étant le portier attribué à l'extrémité à un moment donné. L'adresse du portier attribué est communiquée à l'extrémité dans le champ **assignedGatekeeper** des messages GCF, RCF/RRJ, ACF/ARJ, UCF, DCF et IRQ. Dans le cas où l'extrémité utilise le mécanisme de multidiffusion GRQ pour rechercher de façon dynamique un portier disponible et où plusieurs portiers lui répondent, le portier attribué doit être celui qui est indiqué dans le message GCF sélectionné par l'extrémité conformément au § 7.2.1.

L'adresse communiquée dans le champ **assignedGatekeeper** peut changer au fil du temps. Dès lors qu'elle reçoit une adresse contenue dans un champ **assignedGatekeeper** qui est différente de l'adresse existante figurant dans le champ **assignedGatekeeper**, l'extrémité doit accepter cette adresse comme étant l'adresse de son nouveau portier attribué et commencer immédiatement à appliquer les procédures de retour, exposées dans le présent paragraphe, pour s'enregistrer auprès de ce portier. Cela permet à l'administrateur de disposer d'une méthode automatisée de modification du portier attribué aux extrémités sans avoir à reconfigurer ces dernières. La méthode utilisée par le portier pour stocker les données relatives à cette association extrémité-portier ne relève pas de la présente Recommandation, mais l'on part du principe que le portier tient à jour une base de données, sous une forme ou une autre, de façon à stocker ces informations et à fournir d'une certaine manière une interface à l'administrateur qui lui permette de procéder à ces associations.

La procédure de retour au portier primaire peut être assurée soit par le portier soit par l'extrémité, comme indiqué ci-dessous. L'extrémité doit utiliser le modèle spécifié par le portier auprès duquel elle est actuellement enregistrée. Dans le cas où aucun modèle n'est spécifié par le portier, le modèle par défaut doit être le modèle **endpointBased**.

1) **Retour assuré par le portier**

Lorsqu'elle s'enregistre auprès du portier de remplacement, l'extrémité doit indiquer le portier qui lui est actuellement attribué dans le message RRQ. Une fois l'extrémité enregistrée, le portier de remplacement peut utiliser le mécanisme GRQ, décrit ci-dessous, pour déterminer si le portier attribué à l'extrémité est actif. Il peut aussi choisir d'utiliser un mécanisme propriétaire pour déterminer l'état du portier attribué à l'extrémité ainsi que le moment auquel demander à l'extrémité de s'enregistrer auprès du portier qui lui est attribué.

Un portier de remplacement qui utilise le mécanisme GRQ pour déterminer si le portier attribué à l'extrémité est actif doit envoyer périodiquement des messages GRQ au portier attribué à l'extrémité pour déterminer si celui-ci est actif. Les messages GRQ devraient avoir au moins 60 secondes d'intervalle. A la réception d'un message GCF de la part du portier attribué, le portier de remplacement devrait envoyer un message URQ dans lequel les informations relatives au champ du portier attribué seraient indiquées dans le champ alternateGK, et le champ reason du message URQ devrait avoir la valeur **registerWithAssignedGK**. Il peut également envoyer un message RRJ avec le champ RegistrationRejectReason ayant la valeur **registerWithAssignedGK** ou encore un message ARJ avec le champ AdmissionRejectReason ayant la valeur **registerWithAssignedGK** pour demander à l'extrémité de retourner à son portier attribué. Grâce à ce modèle, l'extrémité n'interroge pas son portier attribué en lui envoyant ses propres messages GRQ périodiques.

Le champ **endpointType** contenu dans les messages GRQ adressés par le portier de remplacement au portier attribué doit comporter le champ **gatekeeper**.

Un portier attribué qui reçoit un message GRQ du portier de remplacement devrait répondre par un message GCF seulement s'il est actif et à même de traiter de nouveaux enregistrements. Il ne devrait pas envoyer un tel message si le fait de recevoir un petit nombre d'enregistrements supplémentaires aboutirait à une surcharge qui risquerait de faire aller et venir les extrémités entre les deux portiers. La détermination du point de surcharge ne relève pas de la présente Recommandation.

2) **Retour assuré par l'extrémité**

Lorsque le portier attribué à une extrémité devient inactif, l'extrémité doit enclencher un mécanisme d'interrogation en adressant des messages GRQ périodiques à son portier attribué en vue d'y retourner dès que possible. Une fois que le portier attribué commence à répondre de nouveau (autrement dit, une fois que l'extrémité reçoit un message GCF à l'un de ses messages GRQ), l'extrémité doit tenter de retourner à son portier attribué en lui envoyant un message RRQ. Si elle est enregistrée auprès d'un autre portier lorsqu'elle tente de lancer cette procédure de retour, l'extrémité n'a pas besoin d'envoyer un message URQ à son portier actuel.

Le modèle de retour "assuré par le portier" présente l'avantage de réduire le trafic des messages GRQ par rapport au trafic généré dans le cadre du modèle de retour "assuré par l'extrémité". Si l'extrémité et le portier prennent tous deux en charge cette fonctionnalité de retour, le portier doit préciser dans les champs **rehomingModel** des messages GCF et RCF lequel des deux modèles doit être utilisé.

Les messages GRQ devraient être envoyés au portier attribué à au moins 60 secondes d'intervalle. Cela s'applique aussi bien au modèle de retour assuré par le portier qu'à celui assuré par l'extrémité.

Le champ **assignedGatekeeper** contenu dans des messages envoyés par l'extrémité au portier indique le portier actuellement attribué à celle-ci. Le champ **assignedGatekeeper** contenu dans des messages envoyés par le portier à l'extrémité sert à indiquer le portier attribué à l'extrémité.

A son retour, l'extrémité suppose que le portier attribué est à même d'accepter des demandes relatives aux appels en cours et que le nouveau portier attribué est à même de traiter de tels messages. Cela permet aux appels en cours et aux messages en instance entre l'extrémité et son portier actuel de ne pas être interrompus pendant la procédure de retour. Si elle reçoit une réponse à une demande en instance provenant d'un portier après qu'elle est retournée à son portier attribué, l'extrémité doit accepter cette réponse et poursuivre normalement. Toutefois, après le retour de l'extrémité au portier attribué, tous les messages ultérieurs, retransmis ou nouvellement créés, relatifs à cet appel ou à des appels en cours doivent être adressés au portier attribué auprès duquel elle est désormais enregistrée. Pendant cette transition, il se peut qu'il s'écoule un bref laps de temps durant lequel les portiers ne se sont pas encore synchronisés sur l'état de l'enregistrement des extrémités et que les deux portiers envoient des messages IRQ à l'extrémité pour déterminer l'état de l'appel. L'extrémité doit répondre uniquement aux messages IRQ du portier attribué auprès duquel elle est désormais enregistrée.

Dans le cas où elle reçoit un message de refus de la part de son portier, par exemple un message GRJ, RRJ ou ARJ (ou qu'elle reçoit un message URQ de son portier) contenant une liste de portiers de remplacement et où le champ **altGKisPermanent** a la valeur TRUE, l'extrémité doit suivre les procédures de portier de remplacement, exposées au § 7.2.6, en partant de l'hypothèse que le champ **needToRegister** a la valeur TRUE et en adressant un message RRQ à l'un de ses portiers de remplacement. Toutefois, dans le cas du modèle de retour assuré par l'extrémité, l'extrémité devrait en outre immédiatement déclencher le mécanisme d'interrogation décrit ci-dessus en vue de retourner à son portier attribué dès que possible. S'il souhaite réorienter définitivement l'extrémité vers un portier de remplacement et ne souhaite donc pas que celle-ci retourne vers lui, le portier devrait communiquer à l'extrémité une nouvelle adresse **assignedGatekeeper** ou supprimer la valeur Assigned Gatekeeper en envoyant un champ **assignedGatekeeper** vide.

Dès lors qu'elle reçoit une nouvelle adresse **assignedGatekeeper**, l'extrémité devrait ignorer le champ **needToRegister** et partir de l'hypothèse que la valeur est TRUE. Si le champ **altGKisPermanent** a la valeur FALSE, et si l'adresse du champ assignedGatekeeper diffère de la valeur du portier actuellement attribué à l'extrémité, celle-ci doit ignorer le fait que le champ **altGKisPermanent** a la valeur FALSE et retransmettre ce message à son nouveau portier attribué. C'est seulement dans le cas où le portier ne répondrait pas que l'extrémité doit commencer à appliquer les procédures de portier de remplacement exposées au § 7.2.6 en retransmettant le message à sa liste de portiers de remplacement. Dans le cas d'un modèle de retour assuré par l'extrémité, celle-ci devrait immédiatement déclencher le mécanisme d'interrogation décrit dans le présent paragraphe en vue de retourner à son nouveau portier attribué. Elle peut effectuer ces deux interventions en parallèle.

Le portier peut inclure le champ **assignedGatekeeper** dans tout message GCF, RCF/RRJ, ACF/ARJ, UCF, DCF ou IRQ. Si l'adresse communiquée diffère de la valeur du portier actuellement attribué à l'extrémité et, dans le cas du modèle de retour assuré par l'extrémité, celle-ci doit immédiatement déclencher le mécanisme d'interrogation décrit ci-dessus en vue de retourner à son nouveau portier attribué.

Le portier a la possibilité d'indiquer la valeur **gatekeeperIdentifier** dans le champ **assignedGatekeeper**. Cela est utile lorsque le portier attribué gère plusieurs zones et dispose donc de plusieurs **gatekeeper identifiers** configurés. Si la valeur **gatekeeperIdentifier** envoyée par l'extrémité ne correspond à aucun des identificateurs

configurés du portier, celui-ci doit répondre par un message de refus qui peut contenir la valeur **gatekeeperIdentifier** correcte dans le champ **assignedGatekeeper**. Dans ce cas, l'extrémité devrait envoyer de nouveau la demande en indiquant la valeur **gatekeeperIdentifier** correcte. Sinon, le portier peut ne communiquer aucune valeur **gatekeeperIdentifier** dans le champ **assignedGatekeeper**, auquel cas l'extrémité devrait de nouveau envoyer la demande sans aucune valeur **gatekeeperIdentifier**.

7.2.7 Signalisation des informations de taux d'utilisation

Une extrémité peut avoir la capacité de collecter et de signaler des informations de taux d'utilisation téléphonique, qui peuvent être utiles à des fins de taxation ou de facturation. Un portier peut demander qu'une extrémité signale ces informations. Cet élément de service est destiné à interfonctionner avec les éléments de service de signalisation d'informations de taux d'utilisation offerts par les systèmes qui implémentent l'Annexe G/H.225.0.

A noter que cet élément de service est destiné aux scénarios dans lesquels l'on considère comme fiable l'extrémité à laquelle les informations de taux d'utilisation sont demandées, par exemple lorsqu'une passerelle et un portier sont administrés par le même fournisseur de services. En d'autres termes, l'on part du principe que l'extrémité signalera avec précision ses informations de taux d'utilisation.

7.2.7.1 Annonce des capacités de signalisation des informations de taux d'utilisation

Une extrémité peut annoncer à un portier ses capacités de collecte et de signalisation des informations de taux d'utilisation. Elle spécifie ces capacités dans le champ **usageReportingCapability** du message RRQ. Si l'extrémité a signalé ses capacités et si celles-ci changent par la suite, l'extrémité doit envoyer un autre message RRQ spécifiant ses capacités. L'absence du champ **usageReportingCapability** dans un message RRQ indique que l'extrémité ne peut pas signaler les informations de taux d'utilisation.

7.2.7.2 Demande de signalisation des informations de taux d'utilisation

Un portier peut demander à une extrémité de lui signaler les informations de taux d'utilisation au moyen des messages RCF, ACF et IRQ. Un portier doit partir du principe qu'une extrémité qui n'a pas annoncé sa capacité de signaler un type particulier d'informations de taux d'utilisation ne signalera pas ces informations et ce portier ne doit pas demander ces informations à cette extrémité.

Un portier peut demander des informations de taux d'utilisation au moyen du champ **usageSpec** du message RCF. Cette demande est désignée par le terme *spécification par défaut du taux d'utilisation*. L'inclusion de ce champ par le portier indique que celui-ci demande à l'extrémité de collecter et de signaler les informations de taux d'utilisation spécifiées pour toutes les nouvelles communications. Cette demande ne s'applique pas aux communications qui sont déjà en cours.

Une fois qu'un portier a déposé une spécification par défaut du taux d'utilisation **usageSpec** au moyen du message RCF, il part du principe que cette demande restera applicable jusqu'à ce qu'il dépose une autre spécification par défaut du taux d'utilisation **usageSpec**. Si le portier ne souhaite pas modifier une spécification par défaut du taux d'utilisation déjà déposée, il peut l'indiquer en omettant l'inclusion du champ **usageSpec** dans l'envoi d'un message RCF. Afin de modifier une demande par défaut d'informations de taux d'utilisation déjà acheminée, un portier doit envoyer un nouveau champ **usageSpec** dans son prochain message RCF. Pour demander à une extrémité de mettre fin à la signalisation d'informations de taux d'utilisation, un portier doit lui envoyer un champ **usageSpec** sans sélection d'options dans le champ **when** ou **required**.

Au moyen du champ **usageSpec** du message ACF relatif à une communication, un portier peut demander des informations de taux d'utilisation relatives à cette communication. Cette demande est désignée par le terme *spécification par communication du taux d'utilisation*. Si cette demande est

émise, elle a priorité, pour la communication considérée, sur toute spécification par défaut du taux d'utilisation que le portier peut avoir émise dans un message RCF.

Un portier peut également demander des informations de taux d'utilisation pour une communication particulière au moyen du champ **usageInfoRequested** d'un message IRQ. La réponse à cette demande doit suivre immédiatement, dans un message IRR. Cette demande n'a pas d'incidence sur la spécification par défaut du taux d'utilisation, envoyée au moyen du message RCF ni sur la spécification par communication du taux d'utilisation, envoyée au moyen du message ACF.

Un portier qui souhaite qu'une extrémité signale périodiquement des informations de taux d'utilisation dans des messages IRR spontanés doit indiquer cette demande en choisissant l'option **inIrr** du champ **when** du paramètre **usageSpec**. Il doit également spécifier soit l'option **irrFrequencyInCall** dans le champ **preGrantedARQ** du message RCF, soit l'option **irrFrequency** dans le message ACF, selon ce qui convient pour une communication particulière.

Un portier qui demande que les informations de taux d'utilisation soient signalées au début d'une communication ou dans des messages IRR spontanés (c'est-à-dire qui choisit l'option **start** ou **inIrr** dans le champ **when** du paramètre **usageSpec**) doit acquitter les messages IRR afin de s'assurer que les informations de taux d'utilisation demandées sont acheminées de façon fiable. Pour indiquer qu'il acquittera les messages IRR, le portier donne la valeur "TRUE" au champ **willRespondToIRR** du message RCF ou ACF.

7.2.7.3 Envoi des comptes rendus d'informations de taux d'utilisation

Une extrémité peut signaler les informations de taux d'utilisation à un portier au moyen des messages BRQ, IRR, DRQ et DCF. Une extrémité peut envoyer des informations de taux d'utilisation à un portier qui n'a pas demandé ces informations. Si une extrémité annonce sa capacité de collecter et de signaler un type particulier d'informations de taux d'utilisation et si un portier demande ces informations, cette extrémité doit signaler les informations demandées. Une extrémité ne doit pas tenir compte des demandes d'informations de taux d'utilisation qui sont erronées (comme une demande de présentation de l'heure de fin de communication au début de celle-ci). Une extrémité peut ne pas tenir compte d'une demande d'informations de taux d'utilisation qui n'entre pas dans les capacités de signalisation annoncées par cette extrémité.

Si un portier envoie à une extrémité une spécification par défaut de taux d'utilisation **usageSpec** dans un message RCF, cette extrémité doit régler les paramètres de signalisation des informations de taux d'utilisation pour toutes les nouvelles communications fondées sur ce gabarit, à moins que le portier ne fournisse, dans un message ACF, une spécification par communication de taux d'utilisation **usageSpec** pour une communication particulière. Si elle est fournie, la spécification par communication du taux d'utilisation a priorité sur la spécification par défaut du taux d'utilisation **usageSpec** pour cette communication. Une extrémité peut appliquer une spécification par défaut du taux d'utilisation **usageSpec** à des communications en cours pour lesquelles aucune spécification par communication du taux d'utilisation n'a été fournie.

Une spécification d'utilisation **usageSpec** sans options choisies dans le champ **when** ou **required** doit être interprétée par une extrémité comme étant une demande de non-signalisation des informations de taux d'utilisation.

Lorsqu'une extrémité signale des informations de taux d'utilisation au moyen d'un message IRR et que le portier a indiqué, par le champ **willRespondToIRR** du message RCF ou ACF, qu'il acquittera les messages IRR, cette extrémité doit mettre le champ **needResponse** à la valeur "TRUE" et doit réémettre au besoin ces informations (si un acquittement n'a pas été reçu). Cette règle s'applique quelle que soit la nature des messages IRR, spontanés ou non spontanés.

Si le portier a demandé que les informations de taux d'utilisation soient signalées au début de la communication (c'est-à-dire s'il a sélectionné l'option **start** dans le champ **when** du paramètre **usageSpec**) et si les informations demandées entrent dans les capacités de signalisation annoncées

par l'extrémité, celle-ci doit signaler les informations demandées immédiatement après le début de la communication. Si l'extrémité envoie un message BRQ à cet instant, elle peut inclure les informations d'utilisation demandées dans le champ **usageInformation** du message BRQ. Sinon, l'extrémité doit envoyer un message IRR spontané avec les informations d'utilisation demandées dans le champ de spécification par communication de **usageInformation**.

Si le portier a demandé que les informations de taux d'utilisation soient signalées à la fin de la communication (c'est-à-dire s'il a sélectionné l'option **end** dans le champ **when** du paramètre **usageSpec**) et si les informations demandées entrent dans les capacités de signalisation annoncées par l'extrémité, celle-ci doit signaler les informations demandées immédiatement après la fin de la communication, dans le message DRQ (ou DCF si la communication est interrompue par le portier).

Si le portier a demandé que les informations de taux d'utilisation soient signalées dans des messages IRR (c'est-à-dire s'il a sélectionné l'option **inIrr** dans le champ **when** du paramètre **usageSpec**) et si les informations demandées entrent dans les capacités de signalisation annoncées, l'extrémité doit signaler les informations demandées dans chaque message IRR qu'elle envoie spontanément.

L'extrémité ne doit appliquer ni la spécification par défaut ni la spécification par communication des informations de taux d'utilisation **usageSpec** lors de l'envoi de messages IRR non spontanés (c'est-à-dire des réponses aux messages IRQ). Si le portier demande les informations d'utilisation par l'intermédiaire du champ **usageInfoRequested** du message IRQ et si les capacités de signalisation de ces informations ont été annoncées par l'extrémité, celle-ci doit signaler les informations demandées dans le champ **usageInformation** du message IRR. Si le portier ne demande pas les informations d'utilisation dans le message IRR, l'extrémité ne doit pas inclure de champ **usageInformation** dans sa réponse.

7.2.8 Capacités associées au crédit d'appel

En utilisant les capacités facultatives associées au crédit d'appel, une extrémité peut recevoir des informations de crédit ou de débit d'usager en provenance du portier avant et après l'établissement d'une communication par cet usager. De son côté, l'extrémité peut renvoyer ces informations à l'usager final au moyen d'une annonce. L'extrémité a également la possibilité de limiter la durée de la communication de l'usager à une durée spécifiée par le portier. Par exemple, l'extrémité peut libérer la communication lorsque le compte de l'usager (temps ou argent) est épuisé.

Par ailleurs, le portier peut envoyer à l'extrémité des annonces associées au solde et peut lui indiquer une limite de durée de communication.

7.2.8.1 Annonce par l'extrémité des capacités associées au crédit

L'extrémité indique sa prise en charge des fonctions de crédit d'appel au moyen du message RRQ. La capacité de restituer ou d'afficher des annonces concernant le solde d'un appelant peut être annoncée au moyen d'un nouveau champ **supportedH248Packages** qui se compose d'une liste facultative de descripteurs **H248PackagesDescriptors** en format binaire.

Pour envoyer une annonce sous forme de texte, l'extrémité et le portier peuvent utiliser le bloc "affichage" (**PackageID** dis, 0x0014) défini dans la Rec. UIT-T H.248.3. La Rec. UIT-T H.248.3 traite des dispositifs permettant de choisir l'emplacement du texte sur un terminal d'affichage et d'autres fonctions.

Pour envoyer l'index d'une annonce vocale fixe ou paramétrée, qui est mémorisée localement dans l'extrémité, celle-ci et le portier peuvent utiliser le bloc "annonce générique" (**PackageID** an, 0x001D) qui est défini dans la Rec. UIT-T H.248.7.

En variante à l'utilisation des blocs H.248, l'extrémité peut indiquer par signalisation d'appel H.225.0 qu'elle possède la capacité d'inclure le solde d'usager dans une annonce

alphanumérique qu'elle construit elle-même. Cette capacité peut être indiquée au moyen du fanion **canDisplayAmountString**.

L'extrémité peut indiquer, au moyen du fanion **canEnforceDurationLimit**, si elle peut effectuer son propre chronométrage des communications.

7.2.8.2 Informations de solde envoyées à l'extrémité par le portier

Le portier peut envoyer des annonces (soit sous forme vocale soit sous forme de texte) à l'extrémité au moyen d'un "signal" H.248 contenu dans la structure **ServiceControlDescriptor** des messages ACF, SCI et/ou DRQ. En variante, le portier peut envoyer une chaîne alphanumérique à l'extrémité dans le champ **amountString** qui indique le solde du compte, par exemple "$10.50", dans la monnaie appropriée. Dans ce cas, l'extrémité est responsable de l'encapsulation de la chaîne de montant dans une annonce (par exemple la chaîne "solde actuel de la carte de crédit: $10.50") qui convient à cette extrémité particulière. Noter que l'ISO 4217 définit les abréviations normalisées des différentes monnaies, par exemple "USD" pour le dollar des Etats-Unis d'Amérique. Le champ **amountString** doit être codé en format Unicode.

Un champ **billingMode** est également ajouté afin que le portier puisse indiquer le mode de facturation pour la communication. La valeur **debit** de ce champ indique que la communication sera taxée en fonction du montant financier disponible dans un compte d'usager. La valeur **credit** de ce champ indique que la communication sera taxée ultérieurement à l'usager. Une extrémité peut utiliser cette information pour, par exemple, déterminer le type d'annonce à restituer ou à afficher.

Le champ **callDurationLimit** de la structure **CallCreditServiceControl** indique la durée qui reste disponible pour une communication donnée. Le fanion **enforceCallDurationLimit** indique si l'application de la limite de temps disponible doit être effectuée par l'extrémité. Le champ **callStartingPoint** indique à quel instant de la communication l'application de la limite de temps disponible doit commencer si cette fonction est assurée par l'extrémité.

Si l'extrémité a annoncé sa capacité d'appliquer la limite de temps disponible et si le portier a demandé que cette fonction soit appliquée par l'extrémité, celle-ci doit libérer la communication à l'expiration du temps disponible. Le chronométrage de la durée de communication doit commencer dès l'émission ou la réception du message Connect (Connect) ou d'alerte (Alerting) selon ce qui est indiqué par le champ **callStartingPoint**.

7.2.9 Autres adresses de transport

Une extrémité peut indiquer la prise en charge d'autres protocoles de transport en insérant le champ **alternateTransportAddresses** dans le message RRQ. Le portier peut indiquer à l'extrémité le protocole de transport de signalisation à utiliser pour établir des communications, par l'inclusion du champ **useSpecifiedTransport** dans le message RCF ou ACF. Le portier ne doit inclure dans le champ **useSpecifiedTransport** que les protocoles dont l'extrémité a annoncé la prise en charge. Dès réception du champ **useSpecifiedTransport**, l'extrémité doit utiliser le protocole de transport spécifié pour établir la communication.

Le portier peut offrir à l'extrémité un choix entre plusieurs protocoles de transport à utiliser pour la signalisation d'appel, en insérant le champ **alternateTransportAddresses** dans le message RCF ou ACF sans inclure le champ **useSpecifiedTransport**. Dans ce cas, l'extrémité doit utiliser soit le protocole spécifié dans le champ **destCallSignalAddress** soit sélectionner un des protocoles de transport indiqués dans le champ **alternateTransportAddresses**.

Le portier peut également fournir à une entité H.323, dans un message LCF, **alternateTransportAddresses** d'une extrémité enregistrée chez lui.

7.3 Voie de signalisation d'appel

La voie de signalisation d'appel doit être utilisée pour acheminer des messages de commande d'appel H.225.0. La voie de signalisation d'appel doit être une voie fiable.

Dans les réseaux sans portier, les messages de signalisation d'appel sont transmis directement entre les extrémités appelantes et appelées au moyen des adresses de transport pour voie de signalisation d'appel. Dans ces réseaux, on part du principe que l'extrémité appelante connaît l'adresse de transport contenue dans la voie de signalisation d'appel de l'extrémité appelée et qu'elle peut donc communiquer directement avec celle-ci.

Dans des réseaux avec portier, l'échange initial des messages d'admission a lieu entre l'extrémité appelante et le portier au moyen de l'adresse de transport de la voie RAS du portier. Dans le cadre de cet échange initial des messages d'admission, le portier indique dans le message de confirmation d'admission ACF si la signalisation d'appel doit être envoyée directement à l'autre extrémité ou acheminée par l'intermédiaire du portier. Les messages de signalisation d'appel sont envoyés à l'adresse de transport contenue dans la voie de signalisation d'appel de l'extrémité ou du portier.

La voie de signalisation d'appel peut acheminer la signalisation relative à plusieurs appels simultanés au moyen de la valeur de la référence d'appel pour associer le message à l'appel. Une entité indique sa capacité de traiter plusieurs appels simultanés sur la même connexion sémaphore d'appel par la mise de son drapeau **multipleCalls** à la valeur "TRUE" dans les messages qu'elle envoie sur la voie de signalisation d'appel. Une entité peut fixer dynamiquement la valeur du champ **multipleCalls** afin d'indiquer sa capacité actuelle à prendre en charge des connexions multiples sur la voie de signalisation d'appel. Si une extrémité souhaite modifier la valeur du champ **multipleCalls** à un moment où aucun autre message H.225.0 n'est échangé sur la voie de signalisation, il doit transmettre le champ **multipleCalls** dans un message facilité (Facility) avec la valeur CRV mise à la référence d'appel global comme indiqué dans la Figure 4-5/Q.931 et le descripteur **guid** dans le champ **callIdentifier** ne comportant que des zéros.

Une entité qui est capable de traiter plusieurs appels simultanés sur voie de signalisation d'appel peut indiquer qu'elle ne prendra pas d'autres appels en charge sur la voie de signalisation par l'envoi du message Release Complete ayant la valeur **newConnectionNeeded** dans la cause **reason**. Une entité qui reçoit un message Release Complete avec le motif **newConnectionNeeded** peut tenter de se connecter sur une nouvelle voie de signalisation d'appel.

Une entité peut transmettre un message Status Inquiry ne se rapportant pas à une communication donnée. En pareil cas, elle doit mettre tous les bits du champ **callIdentifier** à zéro. Une entité doit omettre le champ **Status-UUIE** dans le message Status ou le champ **StatusInquiry-UUIE** dans le message Status Inquiry lorsqu'elle transmet ces messages, mais les entités doivent être prêtes à recevoir des messages ne contenant pas ces éléments de message afin de préserver la compatibilité vers l'amont.

La voie de signalisation d'appel peut être établie avant qu'il soit réellement nécessaire de signaler un appel et la voie peut rester connectée entre deux appels. Une entité peut indiquer cette capacité en mettant son drapeau **maintainConnection** à la valeur "TRUE" dans les messages qu'elle envoie sur la voie de signalisation d'appel. De plus, une extrémité qui a cette capacité peut en faire mention quand elle s'enregistre auprès d'un portier. Cela permet à un portier utilisant le routage de portier de se connecter à l'extrémité à n'importe quel instant après l'enregistrement. Si la connexion se termine alors qu'aucune communication ou signalisation n'est active, aucune des extrémités ne tentera d'ouvrir la connexion tant que la signalisation n'est pas nécessaire.

La valeur du fanion **maintainConnection** envoyé par une entité sur une voie de signalisation d'appel donnée doit être la même pour chaque message contenant ce champ pendant la durée de la voie de signalisation d'appel. Cela n'empêche pas une entité de mettre cette valeur à "TRUE" pour une voie de signalisation d'appel et à "FALSE" pour une autre voie de signalisation d'appel.

La Rec. UIT-T H.225.0 spécifie les messages Q.931 obligatoires qui sont utilisés pour la signalisation d'appel dans la présente Recommandation. Le paragraphe 8 spécifie les procédures d'utilisation de ces messages.

7.3.1 Acheminement sur la voie de signalisation d'appel

On distingue deux méthodes d'acheminement des messages de signalisation d'appel. La première méthode est la signalisation d'appel indirecte par l'intermédiaire du portier (voir Figure 25). Dans cette méthode, les messages de signalisation d'appel sont acheminés par l'intermédiaire du portier entre les extrémités. La seconde méthode est la signalisation d'appel directe entre extrémités (voir Figure 26). Dans cette méthode, les messages de signalisation d'appel sont transmis directement entre les extrémités. Le choix de la méthode à utiliser incombe au portier.

Les deux méthodes utilisent les mêmes types de connexions aux mêmes fins, et les mêmes messages. Il est procédé à l'échange des messages d'admission sur les voies RAS avec le portier, puis à l'échange des messages de signalisation d'appel sur une voie de signalisation d'appel. La voie de commande H.245 est ensuite établie. Les actions du portier en réponse aux messages d'admission déterminent le modèle d'appel utilisé; sans supervision aucune de l'extrémité, bien que celle-ci puisse spécifier une préférence.

La méthode de signalisation symétrique de l'Annexe D/Q.931 doit être utilisée pour toutes les procédures de signalisation d'appel obligatoires. Il n'est pas traité ici du rôle qu'une passerelle peut jouer du côté d'un réseau à commutation de circuits utilisant les protocoles de signalisation d'appel de la Rec. UIT-T Q.931 ou d'autres protocoles de signalisation d'appel.

L'entité portier représentée sur les Figures 25 à 28 contient un ou plusieurs portiers pouvant ou non communiquer entre eux. Les extrémités peuvent être connectées au même portier ou à des portiers différents.

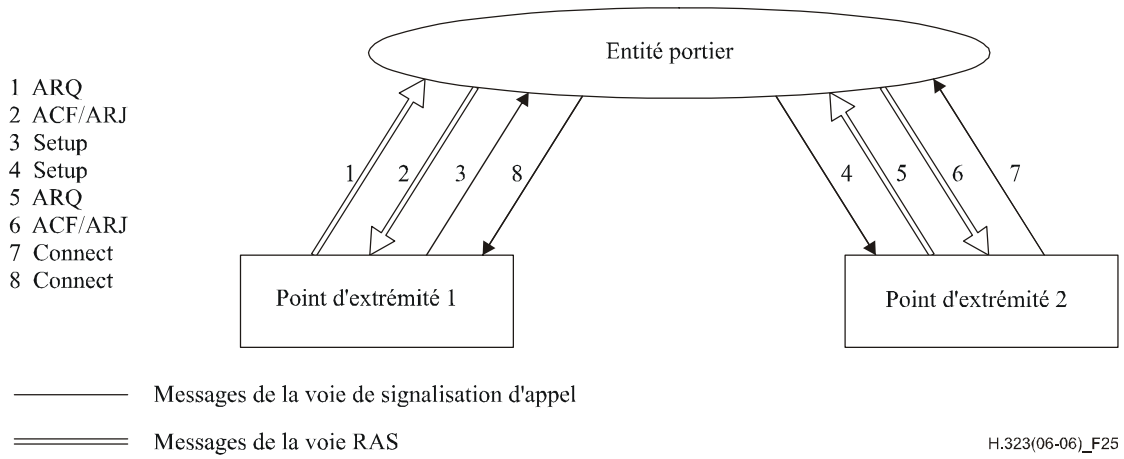


Figure 25/H.323 – Signalisation d'appel acheminée par le portier

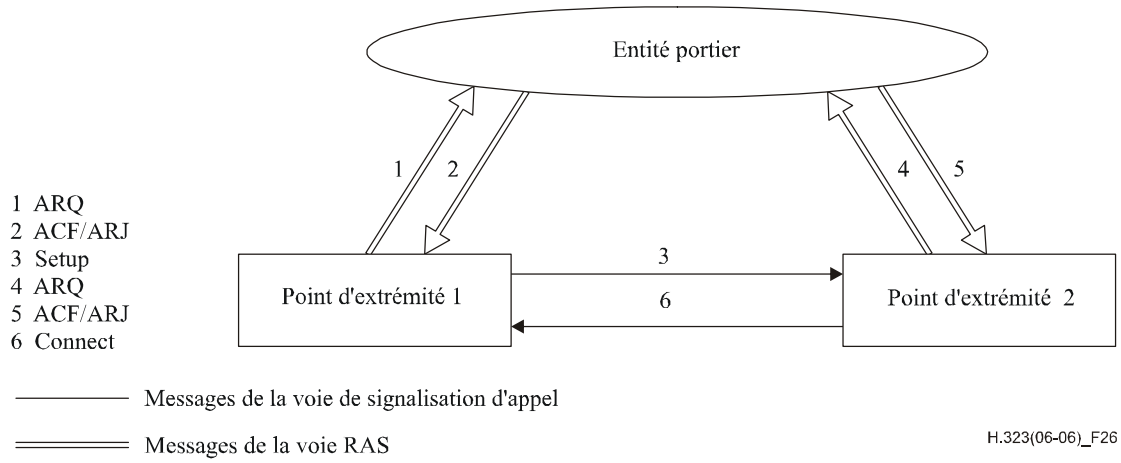


Figure 26/H.323 – Signalisation d'appel directe entre extrémités

7.3.2 Routage de la voie de commande

En cas d'utilisation de la signalisation d'appel indirecte par l'intermédiaire du portier, il y a deux méthodes pour établir la voie de commande H.245. Dans la première méthode, la voie de commande H.245 est établie directement entre les extrémités. Voir Figure 27. Cette méthode appelle un complément d'étude. Dans la seconde méthode, la voie de commande H.245 est établie entre les extrémités par l'intermédiaire du portier. Voir Figure 28. Cette méthode permet au portier de rediriger la voie de commande H.245 vers un contrôleur multipoint au moment où une conférence multipoint ad hoc cesse d'être une conférence point à point pour devenir une conférence multipoint. C'est le portier qui effectue ce choix. En cas d'utilisation de la signalisation d'appel directe entre extrémités, la voie de commande H.245 ne peut être établie que par connexion directe entre les extrémités.

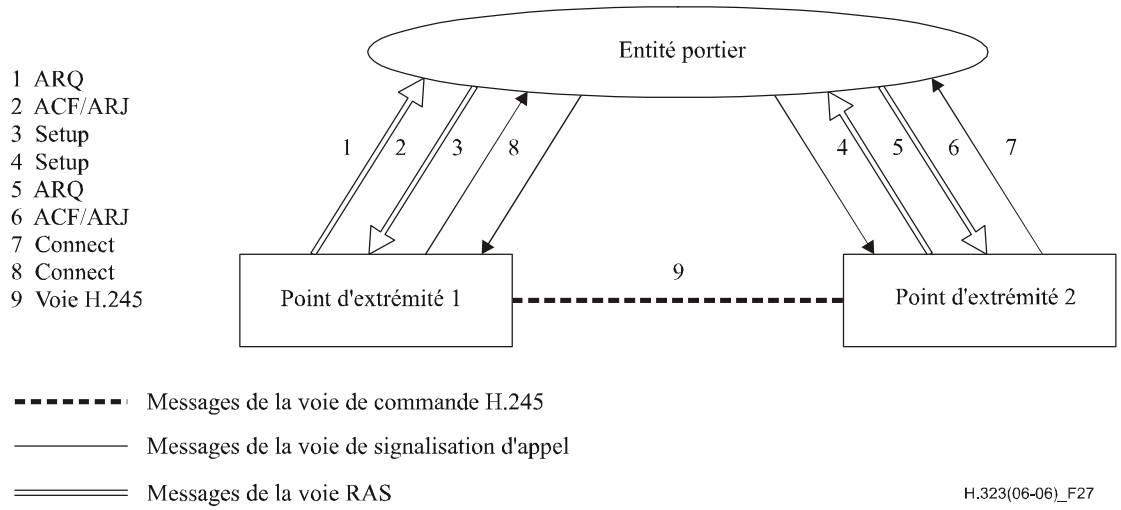


Figure 27/H.323 – Connexion directe de la voie de commande H.245 entre extrémités

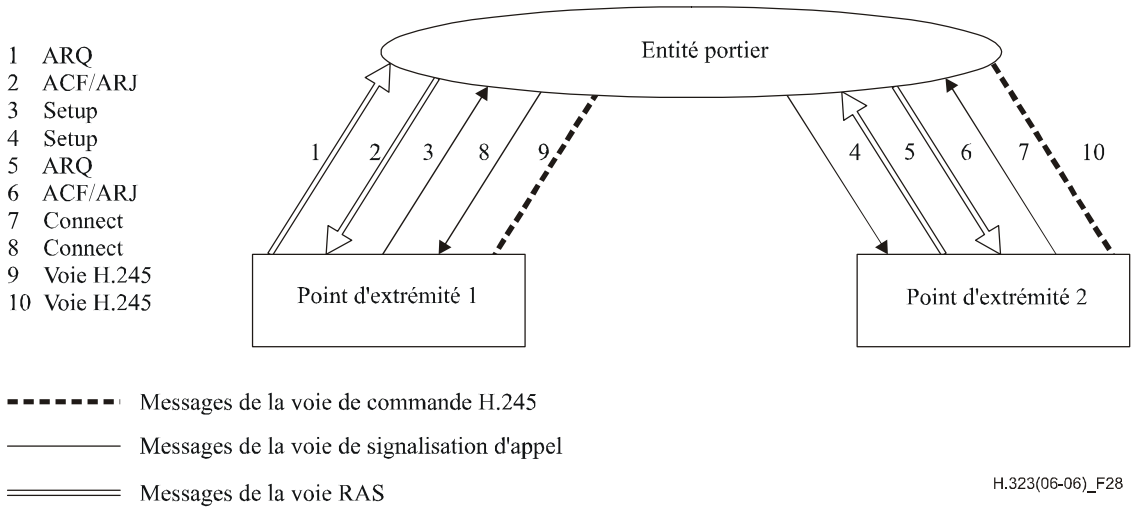


Figure 28/H.323 – Voie de commande H.245 établie par l'intermédiaire du portier

7.3.3 Révisions du protocole de signalisation et de commande d'appel

Lorsqu'un appel est acheminé par l'intermédiaire d'un portier, les portiers doivent suivre les règles suivantes pour déterminer le numéro de la version H.225.0 ou H.245 qu'il y a lieu d'indiquer dans les messages émis par une extrémité et acheminés ou retransmis par le portier:

a) si le numéro de version H.225.0 ou H.245 de l'extrémité émettrice est inférieur ou égal au numéro de version du portier et que ce dernier décide de représenter les fonctions d'un numéro de version identique ou plus récent au nom du point d'origine, les messages acheminés présenteront le numéro de version du portier. Sinon, il présenteront celui de l'extrémité;

b) si le numéro de version de l'extrémité d'origine est plus grand que celui du portier, les messages acheminés présenteront le numéro de version du portier.

Quel que soit le cas, le portier peut utiliser un simple codage ASN.1 spécifié par la version H.225.0 ou H.245 la plus récente compréhensible par le portier en vertu de ces règles.

Etant donné que d'une part, dans la H.323, pour certaines fonctionnalités, tels la pause et reroutage à l'initiative d'une tierce partie, il est exigé que les entités de signalisation connaissent exactement laquelle des versions du protocole est utilisée par les autres entités intervenant dans l'appel et que d'autre part, le paramètre **protocolIdentifier** peut être modifié après la réception du premier message de signalisation de l'appel ou à d'autres moments pendant l'appel, lorsque par exemple un appel est rerouté vers une entité différente, les entités qui reposent sur des fonctionnalités spécifiques à une version doivent déterminer la version utilisée par les autres entités dans un appel en examinant le paramètre **protocolIdentifier** dans le message Setup and Connect au moins. En pareil cas, les entités disposant de fonctionnalités spécifiques à une version doivent à nouveau déterminer la version utilisée par l'entité sur laquelle l'appel peut avoir été commuté. Si la signalisation H.245 est canalisée, l'extrémité peut utiliser le message de signalisation d'appel contenant le message d'ensemble de capacités non vide canalisé afin de déterminer la version associée à l'extrémité distante. Si un canal H.245 distinct est utilisé, une entité peut envoyer un message d'interrogation d'état (Status Inquiry) et déterminer la version du protocole en examinant le **protocolIdentifier** dans le message d'état (Status) résultant. Dans ces deux cas, la version de la H.245 utilisée par l'autre entité est signalée dans le message d'ensemble de capacités non vide.

Il convient de noter qu'il est possible que les entités H.323 antérieures à la version 4 n'insèrent pas d'identificateur **protocolIdentifier** dans le message d'état (Status), de sorte que les entités H.323 doivent supposer que l'absence d'identificateur **protocolIdentifier** indique seulement que l'entité est antérieure à la version 4.

NOTE – Un portier peut indiquer sa version de protocole propre dans sa réponse à un message Status (par exemple pour envoyer un message Call Proceeding avant d'établir la communication avec l'appelé) ou lors du déclenchement d'une connexion sortante indépendante d'un appel existant. Par conséquent, il est important qu'une extrémité n'utilise pas le ou les messages initiaux pour déterminer la révision du protocole associé au point d'extrémité.

7.4 Valeur de référence d'appel

Tous les messages de signalisation d'appel et RAS contiennent une valeur de référence d'appel (CRV, *call reference value*) (voir Rec. UIT-T H.225.0). Il existe une seule valeur CRV pour la voie de signalisation d'appel et une valeur CRV indépendante pour la voie RAS. Une seule valeur CRV est utilisée dans tous les messages de signalisation d'appel entre deux entités (d'extrémité à portier, d'extrémité à extrémité, etc.) concernant le même appel. Une deuxième valeur CRV est utilisée pour associer les messages RAS. Cette valeur CRV doit être utilisée dans tous les messages RAS entre deux entités concernant le même appel. De nouvelles valeurs CRV doivent être utilisées pour les nouveaux appels. Un second appel, issu d'une extrémité pour inviter une autre extrémité à participer à la même conférence, doit utiliser une nouvelle valeur CRV. Celle-ci ne doit pas être confondue avec l'identificateur d'appel ou avec l'identificateur de conférence (CID, *conference ID*). La valeur CRV associe tous les messages échangés entre toutes les entités au cours de la même communication, tandis que l'identificateur CID associe tous les messages échangés entre toutes les entités au cours de toutes les communications d'une même conférence.

La référence d'appel globale, représentée sur la Figure 4-5/Q.931 et ayant la valeur numérique 0, est utilisée pour renvoyer à tous les appels de la voie de signalisation d'appel ou de la voie RAS. Lors de l'établissement ou de l'acceptation d'appels, les entités H.323 doivent sélectionner une valeur CRV autre que la valeur de référence d'appel globale, qui est réservée aux messages ne se rapportant pas à une communication particulière.

Lors de l'établissement d'un nouvel appel, l'extrémité appelante doit choisir une nouvelle valeur CRV pour cet appel et l'utiliser aussi bien sur la voie RAS que sur la voie de signalisation d'appel H.225.0. L'extrémité appelée ne doit cependant pas utiliser la valeur CRV reçue dans le message Setup lorsqu'elle communique sur sa voie RAS, mais plutôt sélectionner une nouvelle valeur CRV à utiliser sur la voie RAS, unique sur cette voie quelle que soit la valeur CRV reçue dans le message Setup, bien qu'il soit évidemment possible que ces valeurs soient numériquement équivalentes.

7.5 Identificateur d'appel

L'identificateur d'appel est une valeur non nulle, mondialement unique, qui est créée par l'extrémité appelante et transmise dans divers messages H.225.0. L'identificateur d'appel désigne l'appel auquel le message est associé. Il sert à associer tous les messages d'enregistrement RAS et de signalisation d'appel concernant la même communication. A la différence de la valeur CRV, l'identificateur d'appel ne change pas en cours de communication. Tous les messages allant de l'extrémité appelante à son portier, de l'extrémité appelante à l'extrémité appelée, et de celle-ci à son portier, associés au même appel, doivent contenir le même identificateur d'appel. Celui-ci est codé comme décrit dans la Rec. UIT-T H.225.0. Dans les références aux Figures 29 à 39 du § 8, tous les messages d'une même figure doivent avoir le même identificateur d'appel.

Lorsqu'une extrémité selon la version 1 appelle une extrémité selon la version 2, il appartient au point d'extrémité selon la version 2 de produire un identificateur d'appel avant d'envoyer la demande ARQ à son portier.

7.6 Identificateur ID de conférence et paramètre conferenceGoal

L'identificateur de conférence (CID, *conference ID*) est une valeur non nulle et unique qui est créée par l'extrémité appelante et transmise dans divers messages H.225.0. L'identificateur CID désigne la conférence à laquelle le message est associé. Les messages issus de toutes les extrémités au cours

d'une même conférence auront donc le même identificateur CID. Celui-ci est codé comme spécifié dans la Rec. UIT-T H.225.0.

Le paramètre **conferenceGoal** indique l'objet de la communication. Les options sont les suivantes: **create** (d'une nouvelle conférence); **join** (à une conférence existante); **invite** (d'une nouvelle extrémité à une conférence existante); **capability-negotiation** (en vue d'une conférence H.332 ultérieure); et **callIndependentSupplementaryService** (pour le transport d'unités APDU de services complémentaires).

7.7 Capacité d'appel d'extrémité

La capacité d'appel indique la possibilité, pour une extrémité, d'accepter chacun des types d'appel qu'elle prend en charge (par exemple voix, données T.120, H.320, etc.). Bien qu'une extrémité de type quelconque puisse signaler sa capacité d'appel au moyen de divers messages H.225.0 afin d'aider un portier à acheminer des appels, les informations de capacité d'appel doivent normalement être signalées par des passerelles afin d'aider le portier à équilibrer les charges entre les passerelles et de contribuer à réduire le nombre de tentatives d'appel infructueuses.

La capacité d'appel maximale et actuelle d'une extrémité peut être indiquée lors de l'enregistrement. Par ailleurs, la capacité d'appel actuelle peut également être indiquée appel par appel. La représentation de cette capacité dynamique nécessite l'examen des modèles d'appel suivants:

- modèle d'appel direct avec admission appel par appel – Dans ce cas, l'extrémité peut indiquer la capacité d'appel restante dans les messages ARQ, DRQ ou BRQ;
- modèle d'appel direct avec admission préattribuée – Dans ce cas, l'extrémité peut indiquer la capacité d'appel dans des messages RRQ ou RAI (si l'extrémité est une passerelle);
- modèle d'appel routé par portier avec admission appel par appel – L'extrémité peut fournir des informations de capacité d'appel dans un message ARQ, DRQ ou BRQ;
- modèle d'appel routé par portier avec admission préattribuée – L'extrémité peut insérer des informations de capacité d'appel dans les messages de signalisation d'appel, tels que établissement (Setup) ou libération terminale (Release Complete). Dans ce cas, l'extrémité d'origine peut insérer ses informations de capacité d'appel dans un message d'alerte (Alerting) ou de connexion (Connect). Chaque extrémité peut fournir des informations de capacité d'appel mises à jour au moyen du message Release Complete.

De toute façon, un portier peut utiliser l'échange de messages IRQ/IRR pour contrôler la capacité d'appel d'une extrémité. Il convient de noter qu'il est préférable d'insérer les informations de capacité d'appel dans des messages déjà appelés à être envoyés à un portier, comme une demande ARQ si l'on n'utilise pas l'admission préattribuée ou un message Setup dans un appel routé par portier, plutôt que d'envoyer des messages additionnels à cette fin. Si cependant une passerelle reçoit un message Release Complete et fonctionne en mode d'admission préattribuée, elle doit envoyer un message IRR au portier pour lui permettre de conserver des informations de capacité d'appel plus exactes.

Si une extrémité fournit des informations de capacité d'appel, elle doit les insérer dans un message RRQ et indiquer sa capacité d'appel dans ce message. Un portier peut demander, au moyen des messages RCF et IRQ, qu'une extrémité fournisse des informations de capacité d'appel. Une extrémité qui a indiqué sa capacité de signalisation de la capacité d'appel doit la signaler comme demandé par le portier. Une extrémité ne doit pas signaler sa capacité d'appel maximale dans un message autre que la demande RRQ initiale, à moins que son portier ne demande les informations de capacité d'appel dans un message IRQ. Une extrémité peut utiliser les informations de capacité d'appel dans un message BRQ, IRR ou RAI afin d'informer le portier de modifications soudaines, comme celles qui provoquent une panne matérielle.

Une extrémité peut signaler qu'elle possède des capacités d'appel différentes pour différents protocoles pris en charge (c'est-à-dire T.120, H.320, H.321, voix, etc.). Comme cependant les

équipementiers peuvent utiliser les mêmes ressources pour plusieurs protocoles, le portier ne doit pas préjuger la façon dont la capacité d'appel de l'extrémité peut changer dans un des protocoles pris en charge lorsque cette extrémité établit un appel utilisant un autre protocole.

Une passerelle peut signaler la capacité d'appel au moyen du paramètre **group** qui peut représenter un faisceau de circuits associés à une interface ou à un exploitant particulier, par exemple. Cette caractéristique permet au portier de suivre la capacité d'appel séparément pour chaque groupe. Le paramètre **group** peut être identique à celui qui est signalé dans l'identificateur **circuitID** d'un appel particulier.

NOTE – Les informations de capacité d'appel signalées dans un message quelconque sont de nature consultative et peuvent ne pas être absolument exactes en raison de conditions critiques, de modifications soudaines dans l'extrémité, ou d'attribution locale de ressources.

7.8 Services d'identification de l'appelant

7.8.1 Description des services

Le présent paragraphe décrit les services d'identification de l'appelant, qui sont les suivants:

- présentation et restriction du numéro de l'appelant;
- présentation et restriction du numéro connecté;
- présentation et restriction du numéro de l'appelé (émettant l'alerte);
- présentation et restriction du numéro de correspondant occupé.

7.8.1.1 Présentation de l'adresse de l'appelant

La présentation de l'adresse de l'appelant est une fonction qui fournit au correspondant appelé l'adresse de pseudonyme de l'appelant. Cette adresse peut être fournie par l'extrémité appelante ou par le portier dans le cas d'appels routés par portier à partir du réseau en mode paquet. Lorsque l'appel est routé par le portier auprès duquel l'extrémité appelante est enregistrée, ce portier peut offrir un service de filtrage garantissant que l'adresse présentée est vraiment celle de l'appelant. Le portier peut également fournir l'adresse du correspondant appelant lorsque aucune adresse n'est fournie par celui-ci ou lorsque l'appelant donne une adresse autre que celle sous laquelle il est enregistré.

Si un appel provient du réseau à commutation de circuits et entre dans le réseau en mode paquet par une passerelle, celle-ci doit transmettre au réseau en mode paquet les informations de numéro d'appelant provenant du réseau à commutation de circuits.

7.8.1.2 Restriction de l'adresse de l'appelant

La restriction de l'adresse de l'appelant est une fonction qui permet à l'extrémité appelante (ou à son portier) de restreindre la présentation à l'appelé de l'adresse de pseudonyme de l'appelant. Cette fonction peut résider dans l'extrémité ou dans le portier pour les appels routés par portier.

Lorsque la restriction de l'adresse de l'appelant a été indiquée, il peut arriver que la restriction soit neutralisée (par exemple si l'appelé doit fournir un certain service d'urgence).

7.8.1.3 Présentation de l'adresse du correspondant connecté

La présentation de l'adresse du correspondant connecté est une fonction qui fournit l'adresse de pseudonyme du correspondant connecté ou répondant à l'appelant. L'adresse du connecté peut être fournie par l'extrémité connectée ou par le portier dans le cas d'appels routés par portier. Lorsque l'appel est routé par le portier auprès duquel l'extrémité connectée est enregistrée, ce portier peut fournir un service de filtrage garantissant que l'adresse fournie est vraiment celle du connecté. Le portier peut également fournir l'adresse du connecté lorsque aucune adresse n'est fournie par celui-ci ou lorsque le connecté donne une adresse autre que celle sous laquelle il s'est enregistré.

Une passerelle doit transmettre les informations du connecté du réseau à commutation de circuits au réseau en mode paquet.

7.8.1.4 Restriction de l'adresse du correspondant connecté

La restriction de l'adresse du correspondant connecté est une fonction qui permet à l'extrémité connectée, ou à son portier, de restreindre la présentation à l'appelant de l'adresse de pseudonyme du connecté. Cette fonction peut résider dans l'extrémité ou dans le portier pour les appels routés par portier.

Lorsque la restriction de l'adresse de l'appelant a été indiquée, il peut arriver que la restriction soit neutralisée (par exemple si l'appelant doit fournir un certain service d'urgence).

7.8.1.5 Présentation de l'adresse du correspondant appelé (émettant l'alerte)

La présentation de l'adresse de l'émetteur de l'alerte est une fonction qui fournit au correspondant appelant l'adresse de pseudonyme de l'émetteur de l'alerte. Cette adresse peut être fournie par l'extrémité émettrice de l'alerte ou par le portier dans le cas d'appels routés par portier. Lorsque l'appel est routé par le portier auprès duquel l'extrémité émettrice de l'alerte est enregistrée, ce portier peut offrir un service de filtrage garantissant que l'adresse présentée est vraiment celle de l'extrémité émettrice de l'alerte. Le portier peut également fournir l'adresse du correspondant émetteur de l'alerte lorsque aucune adresse n'est fournie par celui-ci ou lorsqu'il donne une adresse autre que celle sous laquelle il est enregistré.

7.8.1.6 Restriction de l'adresse du correspondant appelé (émettant l'alerte)

La restriction de l'adresse de l'émetteur de l'alerte est une fonction qui permet à l'extrémité émettrice de l'alerte, ou à son portier, de restreindre la présentation à l'appelant de l'adresse de pseudonyme de l'émetteur de l'alerte. Cette fonction peut résider dans l'extrémité ou dans le portier pour les appels routés par portier.

7.8.1.7 Présentation et restriction de l'adresse du correspondant occupé

La présentation de l'adresse du correspondant occupé est une fonction qui fournit à l'appelant l'adresse de pseudonyme du correspondant occupé. Cette adresse peut être fournie par l'extrémité occupée ou par le portier pour les appels routés par portier. Lorsque l'appel est routé par le portier auprès duquel l'extrémité occupée est enregistrée, ce portier peut offrir un service de filtrage garantissant que l'adresse présentée est vraiment celle du correspondant occupé. Le portier peut également fournir l'adresse du correspondant occupé lorsque aucune adresse n'est fournie par celui-ci ou lorsqu'il donne une adresse autre que celle sous laquelle il est enregistré.

7.8.1.8 Restriction de l'adresse du correspondant occupé

La restriction de l'adresse du correspondant occupé est une fonction qui permet à l'extrémité occupée, ou à son portier, de restreindre la présentation à l'appelant de l'adresse du correspondant occupé. Cette fonction peut résider dans l'extrémité ou dans le portier pour les appels routés par portier.

7.8.2 Messages et éléments d'information

Le présent paragraphe décrit les divers messages et éléments d'information qui permettent aux dispositifs H.323 de fournir des services de présentation et de restriction d'adresse.

7.8.2.1 Informations d'adresse d'appelant

Les informations d'adresse d'appelant apparaissent dans le message Setup (Setup).

Lorsque les informations d'adresse représentent un numéro de téléphone, les informations correspondantes peuvent apparaître dans l'élément d'information numéro de l'appelant. Cet élément d'information contient le numéro de l'appelant, des informations sur ce numéro et les indicateurs de

présentation et de filtrage insérés dans l'octet 3a. C'est le mode de fonctionnement recommandé pour le cas où une passerelle du RTPC envoie un message Setup dans le réseau en mode paquet.

En variante, des informations sur l'appelant peuvent apparaître dans les champs **sourceAddress, presentationIndicator** et **screeningIndicator** du message Setup. Ce mode de fonctionnement est requis lorsque l'adresse **sourceAddress** n'a aucune forme de numéro téléphonique (c'est-à-dire que l'adresse de source n'est ni du type **dialledDigits** ni du type **partyNumber**). Conformément au § 7.2.2.6/H.225.0, ce mode de fonctionnement est également requis lorsque l'information d'adresse se présente sous la forme d'un numéro de téléphone faisant partie d'un plan de numérotage privé.

Le champ **presentationIndicator** contenu dans le message Setup achemine des informations identiques à l'indicateur de présentation contenu dans l'élément d'information numéro de l'appelant. La signification et l'utilisation de l'indicateur de présentation sont définies dans la Rec. UIT-T Q.951.

Le champ **screeningIndicator** contenu dans le message Setup achemine des informations identiques à l'indicateur de filtrage contenu dans l'élément d'information numéro de l'appelant. La signification et l'utilisation de l'indicateur de filtrage sont définies dans la Rec. UIT-T Q.951.

7.8.2.2 Informations d'adresse du correspondant connecté

Les informations d'adresse du correspondant connecté apparaissent dans le message Connect.

Lorsque les informations d'adresse représentent un numéro de téléphone, les informations correspondantes peuvent apparaître dans l'élément d'information numéro connecté, y compris l'indicateur de présentation et l'indicateur de filtrage. C'est le mode de fonctionnement recommandé pour le cas où une passerelle du RTPC envoie un message Connect dans le réseau en mode paquet.

En variante, des informations sur le correspondant connecté peuvent apparaître dans les champs **connectedAddress**, **presentationIndicator** et **screeningIndicator** du message Connect. Ce mode de fonctionnement est requis lorsque l'adresse **connectedAddress** n'a aucune forme de numéro téléphonique (c'est-à-dire que l'adresse **connectedAddress** n'est ni du type **dialledDigits** ni du type **partyNumber**).

Le champ **presentationIndicator** contenu dans le message Connect achemine des informations identiques à l'indicateur de présentation contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de présentation sont définies dans la Rec. UIT-T Q.951.

Le champ **screeningIndicator** contenu dans le message Connect achemine des informations identiques à l'indicateur de filtrage contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de filtrage sont définies dans la Rec. UIT-T Q.951.

7.8.2.3 Informations d'adresse du correspondant appelé (émettant l'alerte)

Les informations d'adresse de l'émetteur de l'alerte apparaissent dans le message Alerting.

Les informations d'adresse de l'émetteur de l'alerte peuvent apparaître dans les champs **alertingAddress**, **presentationIndicator** et **screeningIndicator** du message Alerting.

Le champ **presentationIndicator** contenu dans le message Alerting achemine des informations identiques à l'indicateur de présentation contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de présentation sont définies dans la Rec. UIT-T Q.951.

Le champ **screeningIndicator** contenu dans le message Alerting achemine des informations identiques à l'indicateur de filtrage contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de filtrage sont définies dans la Rec. UIT-T Q.951.

7.8.2.4 Informations d'adresse du correspondant occupé

Les informations d'adresse du correspondant occupé apparaissent dans le message Release Complete.

Les informations d'adresse du correspondant occupé peuvent apparaître dans les champs **busyAddress**, **presentationIndicator** et **screeningIndicator** du message Release Complete.

Le champ **presentationIndicator** contenu dans le message Release Complete achemine des informations identiques à l'indicateur de présentation contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de présentation sont définies dans la Rec. UIT-T Q.951.

Le champ **screeningIndicator** contenu dans le message Release Complete achemine des informations identiques à l'indicateur de filtrage contenu dans l'élément d'information numéro connecté. La signification et l'utilisation de l'indicateur de filtrage sont définies dans la Rec. UIT-T Q.951.

7.8.3 Actions à l'extrémité d'origine

Le présent paragraphe décrit les aspects de procédure nécessaires pour fournir à l'extrémité d'origine des services d'identification d'appelant.

7.8.3.1 Passerelle en tant qu'extrémité d'origine

Dans le cas d'un message Setup reçu du RNIS par une passerelle, le numéro de l'appelant et les informations de présentation résident dans l'élément d'information numéro de l'appelant. La passerelle doit envoyer un message Setup au réseau en mode paquet avec l'élément d'information numéro de l'appelant contenant les mêmes informations que dans le message Setup provenant du RCC, sauf dans le cas suivant. Si le champ identification du plan de numérotage contient la valeur plan de numérotage privé (PNP, *private numbering plan*), les chiffres doivent être omis de l'élément d'information numéro de l'appelant, conformément au § 7.2.2.6/H.225.0. Dans ce cas qui fait exception à la règle, le portier doit mettre l'information d'identification de l'appelant reçue dans les champs **sourceAddress**, **presentationIndicator** et **screeningIndicator** du message Setup. Si le portier envoie délibérément un numéro PNP et un numéro E.164, l'élément d'information numéro de l'appelant doit comporter le numéro E.164 (et non pas le numéro PNP "vide").

Une passerelle recevant du réseau en mode paquet un message Connect contenant l'élément d'information numéro connecté doit copier celui-ci dans le message Connect à envoyer au RNIS. Si l'élément d'information numéro connecté n'est pas contenu dans le message Connect et si le champ **connectedAddress** représente une forme de numéro téléphonique, la passerelle doit convertir les champs **connectedAddress**, **presentationIndicator** et **screeningIndicator** en un élément d'information numéro connecté. Si le champ **connectedAddress** ne représente pas une forme de numéro téléphonique ou si l'élément d'information numéro connecté n'est pas contenu dans le message Connect, la passerelle doit omettre cet élément d'information du message Connect envoyé au RNIS.

Une passerelle recevant un message Alerting contenant les informations d'adresse du correspondant émetteur de l'alerte ou recevant un message Release Complete contenant les informations d'adresse du correspondant occupé doit convertir ces informations en format de signalisation du côté circuit de la passerelle si ce format prend en charge ces informations.

7.8.3.2 Terminal ou pont MCU en tant qu'extrémité d'origine

Pour les appels issus du réseau en mode paquet, le terminal ou pont MCU d'origine peut envoyer un message Setup contenant soit l'élément d'information numéro de l'appelant avec les indicateurs de présentation et de filtrage, soit les champs **sourceAddress**, **presentationIndicator** et **screeningIndicator**. Dans un cas comme dans l'autre, l'indicateur de filtrage doit préciser "informations fournies par l'usager non filtrées". Par exemple, si l'appelant souhaite bloquer son identification auprès de l'appelé, l'indicateur de présentation sera mis à la valeur "restriction" mais le numéro de l'appelant restera contenu dans l'élément d'information numéro de l'appelant. En cas d'appels routés par le portier, celui de l'appelant pourra ajouter cette information si elle fait défaut

ou est incorrecte; de son côté, le portier de l'appelé pourra supprimer, le cas échéant, les informations d'identification de l'appelant. Le portier de l'appelant ou celui de l'appelé peut également ajouter ou retrancher des informations d'adresse sur la base d'une politique locale.

Un terminal ou pont MCU doit, à la réception d'un message Connect, Alerting ou Release Complete, respecter l'indicateur de présentation lors de la communication des informations d'adresse à l'usager.

7.8.4 Actions à l'extrémité de destination

Le présent paragraphe décrit les aspects de procédure nécessaires pour fournir à l'extrémité de destination des services d'identification d'appelant.

7.8.4.1 Passerelle en tant qu'extrémité de destination

Une passerelle du RTPC recevant du réseau en mode paquet un message Setup doit copier les informations contenues dans l'élément d'information numéro de l'appelant de ce message et les convertir dans le format de signalisation pris en charge dans le RTPC. Par exemple, ces informations seront copiées dans l'élément d'information numéro de l'appelant du message Setup Q.931 pour le RNIS. Si l'élément d'information numéro de l'appelant n'est pas contenu dans le message Setup, ou si le champ identification du plan de numérotage contient la valeur plan de numérotage privé, la passerelle doit former un tel élément au moyen des champs **sourceAddress** (en supposant que cette adresse est un des types pseudonymes du numéro téléphonique), **presentationIndicator** et **screeningIndicator** contenus dans le message Setup.

La passerelle doit envoyer au réseau en mode paquet un message Connect avec l'élément d'information numéro connecté contenant les mêmes informations que dans le format de signalisation pris en charge dans le réseau téléphonique. Dans le cas de la réception par une passerelle d'un message Connect Q.931 issu du RNIS, les informations sur le correspondant connecté résident dans l'élément d'information numéro connecté.

7.8.4.2 Terminal ou pont MCU en tant qu'extrémité de destination

Un terminal ou pont MCU recevant le message Setup doit respecter l'indicateur de présentation lors de la communication à l'usager des informations sur l'appelant.

Pour les appels connectés dans le réseau en mode paquet, le terminal ou pont MCU répondeur peut inclure dans le message Connect soit l'élément d'information numéro connecté soit les champs **connectedAddress**, **presentationIndicator** et **screeningIndicator**. Dans un cas comme dans l'autre, le terminal ou pont MCU doit régler l'indicateur de filtrage de façon à préciser "informations fournies par l'usager non filtrées". En cas d'appels routés par le portier, celui du correspondant répondeur pourra ajouter cette information si elle fait défaut ou est incorrecte; de son côté, le portier de l'appelant pourra supprimer, le cas échéant, les informations d'adresse du correspondant répondeur.

Un terminal ou pont MCU peut insérer des informations d'adresse dans le message Alerting, au moyen des champs **alertingAddress**, **presentationIndicator** et **screeningIndicator** contenus dans ce message. Si l'adresse est fournie, le terminal ou pont MCU doit régler l'indicateur de filtrage de façon à préciser "informations fournies par l'usager non filtrées". En cas d'appels routés par le portier, celui du correspondant répondeur pourra ajouter cette information si elle fait défaut ou est incorrecte; de son côté, le portier de l'appelant pourra supprimer, le cas échéant, les informations d'adresse du correspondant répondeur. Le portier du correspondant répondeur ou celui de l'appelant peut également ajouter ou retrancher des informations d'adresse sur la base d'une politique locale.

Un terminal ou pont MCU occupé peut fournir des informations d'adresse dans le message Release Complete au moyen des champs **busyAddress**, **presentationIndicator** et **screeningIndicator** contenus dans ce message. Si l'adresse est fournie, le terminal ou pont MCU doit régler l'indicateur de filtrage de façon à préciser "informations fournies par l'usager non filtrées". En cas d'appels

routés par le portier, celui du correspondant répondeur pourra ajouter cette information si elle fait défaut ou est incorrecte; de son côté, le portier de l'appelant pourra supprimer, le cas échéant, les informations d'adresse du correspondant répondeur.

7.8.5 Actions dans un portier

Dans les scénarios de routage par le portier, celui-ci peut fournir des informations d'identification ou fournir un service de filtrage. Les services qui peuvent être fournis par un portier dépendent du type d'extrémité desservie. Ce paragraphe décrit les aspects de procédure nécessaires pour fournir des services d'identification d'appelant lorsque le portier effectue le routage de la signalisation d'appel.

7.8.5.1 Passerelle en tant qu'extrémité d'origine

Dans les cas de routage par le portier, celui-ci ne doit pas modifier les informations trouvées dans le message Setup issu d'une passerelle. Cette règle implique que le réseau téléphonique ait fourni des informations correctes.

7.8.5.2 Terminal ou pont MCU en tant qu'extrémité d'origine

Dans les cas de routage par le portier, celui-ci peut fournir des informations relatives à l'appelant lorsque celui-ci n'est pas une passerelle. Le portier peut fournir une adresse d'appelant si celui-ci n'en fournit pas une ou si le portier détermine que l'adresse n'est pas correcte. Si le portier fournit une adresse autre que celle qui a été envoyée dans le message Setup, le portier doit régler l'indicateur de filtrage de façon à indiquer "information fournie par le réseau". Si le portier vérifie les informations d'adresse envoyées dans le message Setup mais qu'il ne les modifie pas, il doit régler l'indicateur de filtrage de façon à indiquer "information fournie par l'usager, vérifiée et transmise". Si le portier détermine que les informations d'adresse envoyées dans le message Setup sont incorrectes mais qu'il ne les modifie pas, il doit régler l'indicateur de filtrage de façon à indiquer "information fournie par l'usager, vérifiée et non transmise". Le portier peut régler l'indicateur de présentation de façon à fournir un service à l'extrémité. Le portier peut permettre à l'extrémité d'annuler son service en spécifiant une présentation différente (par exemple la restriction de l'appel en cours alors que le service de l'extrémité est d'autoriser la présentation des appels).

7.8.5.3 Passerelle en tant qu'extrémité de destination

Dans les cas de routage par le portier, celui-ci ne doit pas modifier les informations trouvées dans le message Connect issu d'une passerelle. Cette règle implique que le réseau téléphonique ait fourni des informations correctes.

7.8.5.4 Terminal ou pont MCU en tant qu'extrémité d'origine

Dans les cas de routage par le portier, celui-ci peut fournir des informations relatives au correspondant connecté, ou émetteur de l'alerte ou occupé lorsque celui-ci n'est pas issu d'une passerelle. Le portier peut fournir une adresse de correspondant connecté (ou émetteur de l'alerte ou occupé) si celui-ci n'en fournit pas une ou si le portier détermine que l'adresse n'est pas correcte. Si le portier fournit une adresse autre que celle qui a été envoyée dans le message Connect, Alerting ou Release Complete, le portier doit régler l'indicateur de filtrage de façon à indiquer "information fournie par le réseau". Si le portier vérifie les informations d'adresse envoyées dans le message Connect, Alerting ou Release Complete mais qu'il ne les modifie pas, il doit régler l'indicateur de filtrage de façon à indiquer "information fournie par l'usager, vérifiée et transmise". Si le portier détermine que les informations d'adresse envoyées dans le message Connect, Alerting ou Release Complete sont incorrectes mais qu'il ne les modifie pas, il doit régler l'indicateur de filtrage de façon à indiquer "information fournie par l'usager, vérifiée et non transmise". Le portier peut régler l'indicateur de présentation de façon à fournir un service à l'extrémité. Le portier peut permettre à l'extrémité d'annuler son service en spécifiant une présentation différente (par exemple la restriction de l'appel en cours alors que le service de l'extrémité est d'autoriser la présentation des appels).

7.9 Cadre générique d'extensibilité

Le cadre générique d'extensibilité permet d'ajouter directement de nouvelles fonctions au protocole sans affecter la spécification principale H.225.0 sous-jacente. Le cadre d'extensibilité se compose de deux parties:

- transport de données opaques insérées dans des messages H.225.0;
- négociation des fonctions prises en charge.

La prise en charge du **cadre générique d'extensibilité** est facultative.

7.9.1 Format d'une structure GenericData

Les données opaques peuvent être transportées dans un sous-ensemble de messages RAS ou dans le champ **genericData** des messages de signalisation d'appel H.225.0.

La structure **GenericData** se compose principalement d'un identificateur et de zéro, d'un ou de plusieurs paramètres, ce qui permet une définition flexible des données opaques et des fonctions. La structure **GenericData** se compose d'un champ **id** permettant d'identifier les données génériques, et d'un champ **parameters** permettant de transporter les paramètres proprement dits.

Chaque paramètre contient également un champ **id** d'identification et un champ **content** qui permet d'insérer un certain nombre de types de données différents comme **raw**, **text**, **unicode**, **bool**, **number8**, **number16**, **number32**, **id**, **compound** et **nested**. Cela permet une définition flexible des données génériques et facilite l'implémentation. L'on prévoit cependant que, pour les données génériques qui contiennent un grand nombre de paramètres, la valeur **raw** du champ **content**, qui contiendra les données en notation ASN.1, devra être utilisée.

7.9.2 Négociation au moyen du cadre d'extensibilité – Généralités

Le cadre d'extensibilité offre une méthode commune de négociation des fonctions qui s'applique dans de multiples domaines et qui peut être gérée ou configurée par différentes entités opérationnelles. Les entités n'ont donc pas besoin de connaître au préalable les ensembles fonctionnels des autres entités pour fonctionner correctement.

Le mécanisme utilisé pour négocier les fonctions en signalisation RAS comme en signalisation d'appel utilise la structure **FeatureDescriptor** qui est un pseudonyme de la structure **GenericData** décrite ci-dessus. Ce mécanisme permet d'identifier une fonction et de lui associer des paramètres.

Les entités intermédiaires de signalisation peuvent – sous réserve des impératifs de sécurité – ajouter leurs fonctions requises, recherchées et assurées à des messages les traversant. Les entités intermédiaires peuvent supprimer des fonctions recherchées et assurées qui sont spécifiées dans des messages avant de faire suivre ceux-ci. Les entités intermédiaires ne doivent pas supprimer de champs de fonctions requises à moins qu'elles n'aient la capacité d'assurer les fonctions qu'elles suppriment. Si l'entité intermédiaire ne souhaite pas autoriser une fonction requise, elle doit rejeter la transaction.

Si une entité intermédiaire choisit de prendre en charge une fonction requise qui est signalée dans un message, elle doit supprimer la demande de fonction du message avant de faire suivre celui-ci. Par un moyen ou un autre, l'entité intermédiaire doit renvoyer à l'entité émettrice de la demande l'information de prise en charge de la fonction. A cette fin, l'entité peut modifier la réponse provenant de l'entité distante ou peut produire son propre message.

7.9.3 Négociation au moyen du cadre d'extensibilité – Signal RAS

La négociation des fonctions de signalisation RAS s'applique à la phase découverte, enregistrement et établissement d'appel et en particulier à l'échange de messages de découverte (GRQ, GCF, GRJ), de messages d'enregistrement (RRQ, RCF, RRJ) de messages de demande d'admission (ARQ, ACF, ARJ), de messages de demande d'emplacement (LRQ, LCF, LRJ), de messages de commande de service (SCI/SCR) et du message NonStandardMessage.

Au cours de la négociation, les entités peuvent spécifier l'ensemble des fonctions dont elles ont besoin pour qu'une transaction soit réalisée, l'ensemble des fonctions qu'elles recherchent et l'ensemble des fonctions qu'elles prennent en charge.

7.9.3.1 Traitement par l'entité émettrice de la demande

Une entité émettrice d'une demande (habituellement une extrémité) utilise les éléments contenus dans la structure **FeatureSet** pour spécifier les divers types de fonctions dont elle a besoin. Elle spécifie l'ensemble des fonctions dont elle a besoin au moyen du champ **neededFeatures**, l'ensemble des fonctions qu'elle recherche au moyen du champ **desiredFeatures** et l'ensemble des fonctions qu'elle prend en charge au moyen du champ **supportedFeatures**. Ces trois champs font partie de la structure **FeatureSet**.

En réponse à la demande qu'elle a émise, une entité doit recevoir un message de confirmation ou de rejet.

Si la demande est rejetée, l'entité émettrice de la réponse peut avoir inclus un ensemble de fonctions dont elle a besoin, que l'entité émettrice de la demande doit pouvoir prendre en charge afin que sa demande soit satisfaite. Si tel est le cas et que l'entité émettrice de la demande prenne en charge les fonctions requises, cette entité peut réémettre une demande spécifiant la prise en charge des fonctions dont l'entité émettrice de la réponse a besoin.

Si la demande est acceptée, des procédures spéciales doivent être appliquées pour garantir que la négociation fonctionne de manière compatible avec l'amont. A cette fin, l'entité émettrice de la demande vérifie que les fonctions qu'elle a spécifiées comme étant requises sont énumérées dans la réponse en tant que fonctions prises en charge. Si une entité émettrice de demande ne trouve pas les fonctions dont elle a besoin dans le champ **supportedFeatures** du message de réponse, elle doit partir du principe que l'entité émettrice de la réponse ne prend pas en charge les fonctions dont elle a besoin. Si l'entité émettrice de la demande détermine qu'elle ne peut pas continuer dans ces conditions, elle doit annuler l'opération qu'elle tente d'effectuer (c'est-à-dire envoyer un message DRQ si elle a initialement émis une demande ARQ, et ainsi de suite), de façon que l'état de l'entité émettrice de la réponse soit "invalidé".

7.9.3.2 Traitement par l'entité émettrice de la réponse

L'entité émettrice de la réponse (normalement un portier) examine les fonctions spécifiées dans le champ **neededFeatures** de la demande afin de déterminer si elle peut accepter celle-ci. Elle examine également les champs **neededFeatures**, **desiredFeatures** et **supportedFeatures** afin de déterminer si les fonctions dont elle a besoin sont prises en charge par l'entité émettrice de la demande.

Si l'entité émettrice de la réponse est un portier qui émet une demande LRQ en réponse à une demande ARQ, celui-ci doit copier dans le message LRQ toutes les fonctions qu'il ne fournit pas. En essayant de déterminer si l'ensemble de fonctions nécessaires est pris en charge, le portier doit examiner les fonctions que l'extrémité prend en charge, où la demande ARQ peut être satisfaite soit localement soit en réponse à une confirmation LCF, ainsi que les fonctions qu'il prend lui-même en charge.

Si l'entité émettrice de la réponse détermine que les ensembles nécessaires de fonctions sont pris en charge par les deux entités, elle peut acquitter la demande. L'entité émettrice de la réponse énumère l'ensemble des fonctions qu'elle choisit de prendre en charge dans le champ **supportedFeatures** de sa réponse. Si la demande est acceptée, toutes les fonctions inscrites dans le champ **neededFeatures** de la demande doivent être incluses dans le champ **supportedFeatures** de la réponse. L'entité émettrice de la réponse peut également inclure des fonctions dans le champ **desiredFeatures**.

Si l'entité émettrice de la demande a besoin que des fonctions additionnelles soient prises en charge par l'entité émettrice de la demande, elle doit rejeter cette demande. Si elle cherche à déclarer les fonctions qui doivent être prises en charge pour que la demande soit satisfaite, cette intention doit

être spécifiée dans le champ **neededFeatures** du message de rejet. L'entité qui répond peut également inclure d'autres fonctions dans les champs **desiredFeatures** et **supportedFeatures** du message de rejet.

7.9.4 Négociation au moyen du cadre d'extensibilité – Signalisation d'appel

Les paragraphes suivants décrivent le processus de négociation pour la voie de signalisation d'appel.

7.9.4.1 Traitement par l'extrémité initiatrice

Une extrémité initiatrice peut spécifier les fonctions dont elle a besoin pour un appel, les fonctions qu'elle recherche et celles qu'elle prend en charge. Elle spécifie les fonctions dont elle a besoin au moyen du champ **neededFeatures** du message Setup. Elle spécifie également l'ensemble des fonctions qu'elle recherche au moyen du champ **desiredFeatures** et l'ensemble des fonctions qu'elle prend en charge au moyen du champ **supportedFeatures**.

Si l'appel est rejeté, une ou plusieurs entités émettrices de réponse peuvent avoir inclus un ensemble de fonctions dans le champ **neededFeatures** que l'extrémité initiatrice doit prendre en charge afin que l'appel soit établi. Si tel est le cas et si l'extrémité initiatrice prend en charge les fonctions requises, cette extrémité peut réinitialiser un appel en spécifiant la prise en charge des fonctions requises par les diverses entités situées sur le trajet de signalisation de l'appel.

Si l'appel est accepté, l'extrémité initiatrice doit vérifier que les fonctions qu'elle a spécifiées comme étant requises sont énumérées dans le champ **supportedFeatures** du message Alerting ou Connect. Si une extrémité initiatrice ne trouve pas les fonctions dont elle a besoin dans le champ **supportedFeatures** du message, elle doit en déduire que les entités situées sur le trajet de signalisation d'appel ne prennent pas en charge les fonctions dont elle a besoin. Si l'entité initiatrice détermine qu'elle ne peut pas continuer dans ces conditions, elle doit libérer l'appel au moyen du message Release Complete.

Lorsqu'une extrémité initiatrice reçoit un ensemble de capacités vide à la suite d'une pause de troisième correspondant suivie d'un reroutage, cette extrémité doit supprimer toutes les données qu'elle possède au sujet d'éventuelles capacités d'entités distantes. Lorsque l'extrémité reçoit un ensemble de capacités non vide, elle doit envoyer son ensemble de fonctions au moyen du champ **featureSet** dans un message Facility dont le champ **reason** est mis à la valeur **featureSetUpdate**. Dans ce message, le champ **replacementFeatureSet** doit être mis à la valeur "TRUE". Lorsque l'ensemble de fonctions est reçu de l'extrémité distante dans un message Facility, son contenu peut être interprété de la même façon que ci-dessus.

7.9.4.2 Traitement par des entités intermédiaires

Les entités intermédiaires situées sur le trajet de signalisation d'appel, comme les portiers et les éléments périphériques, peuvent également entrer en interaction avec le processus de négociation.

Les entités intermédiaires situées sur le trajet de signalisation peuvent – sous réserve des impératifs de sécurité – ajouter leurs fonctions requises, recherchées et assurées à des messages les traversant. Les entités intermédiaires peuvent supprimer des fonctions recherchées et assurées qui sont spécifiées dans des messages (tels que Setup, Alerting et Connect) avant de faire suivre ceux-ci. Les entités intermédiaires ne doivent pas supprimer de champs de fonctions requises dans un message Setup ou Facility à moins qu'elles n'aient la capacité d'assurer les fonctions qu'elles suppriment. Si l'entité intermédiaire ne souhaite pas autoriser une fonction requise, elle doit rejeter la transaction.

Si une entité intermédiaire choisit de prendre en charge une fonction requise qui est signalée dans un message Setup, elle doit supprimer la demande de fonction de ce message avant de faire suivre celui-ci. L'entité intermédiaire doit signaler les fonctions assurées qu'elle prend en charge dans le message Alerting (s'il est envoyé) ou Connect avec l'ensemble de fonctions prises en charge par la destination.

Lorsqu'une entité intermédiaire reçoit un paramètre **featureSet** dans un message Facility dont le champ **replacementFeatureSet** est mis à la valeur "TRUE", elle doit modifier les fonctions indiquées conformément à ses besoins de la même façon qu'elle modifie les fonctions signalées dans les messages Setup, Alerting ou Connect. Elle doit ensuite faire suivre le message vers sa prochaine destination.

7.9.4.3 Traitement par l'extrémité appelée

L'extrémité appelée examine les fonctions spécifiées dans le champ **neededFeatures** du message Setup afin de déterminer si elle peut accepter l'appel. Elle examine également les champs **neededFeatures**, **desiredFeatures** et **supportedFeatures** afin de déterminer si les fonctions dont elle a besoin sont prises en charge par les diverses entités situées sur le trajet de signalisation de l'appel.

Si l'extrémité appelée détermine que les ensembles de fonctions nécessaires sont pris en charge par les entités appropriées, l'extrémité appelée peut accepter l'appel. Elle énumère l'ensemble de fonctions qu'elle choisit de prendre en charge dans le champ **supportedFeatures** du message Alerting (s'il est envoyé) et du message Connect. Si l'appel est accepté, toutes les fonctions indiquées dans le champ **neededFeatures** du message Setup doivent être déclarées dans le champ **supportedFeatures** du message de signalisation d'appel Alerting (s'il est envoyé) ou Connect. L'extrémité appelée peut également inclure le champ **desiredFeatures** dans le message.

Si l'extrémité appelée a besoin que des fonctions additionnelles soient prises en charge par les diverses entités se trouvant sur le trajet de signalisation de l'appel, elle doit rejeter l'appel par l'envoi d'un message Release Complete. Si elle cherche à déclarer les fonctions qui doivent être prises en charge pour que l'appel soit établi, cette intention doit être spécifiée dans le champ **neededFeatures** du message Release Complete. L'extrémité appelée peut également inclure d'autres fonctions dans les champs **desiredFeatures** et **supportedFeatures** du message Release Complete.

Lorsqu'une extrémité appelée reçoit un ensemble de capacités vide à la suite d'une pause de troisième correspondant suivie d'un reroutage, cette extrémité doit agir comme si elle avait lancé l'appel, c'est-à-dire qu'elle doit supprimer toutes les données qu'elle possède au sujet d'éventuelles capacités d'entités distantes. Lorsque l'extrémité reçoit ultérieurement un ensemble de capacités non vide, elle doit envoyer son ensemble de fonctions au moyen du champ **featureSet** dans un message Facility dont le champ **reason** est mis à la valeur **featureSetUpdate**. Dans ce message, le champ **replacementFeatureSet** doit être mis à la valeur "TRUE". Lorsque l'ensemble de fonctions est reçu de l'extrémité distante dans un message Facility, son contenu peut être interprété de la même façon que ci-dessus.

8 Procédures de signalisation d'appel

La communication est mise en œuvre selon les étapes suivantes:

– Phase A: établissement de la communication (voir § 8.1).
– Phase B: communication initiale et échange des capacités (voir § 8.2).
– Phase C: établissement de la communication audiovisuelle (voir § 8.3).
– Phase D: services de communication (voir § 8.4).
– Phase E: fin de la communication (voir § 8.5).

8.1 Phase A – Etablissement de la communication

L'établissement de la communication est assuré à l'aide des messages de commande d'appel définis dans la Rec. UIT-T H.225.0 conformément aux procédures de commande d'appel définies ci-dessous. Les demandes de réservation de largeur de bande devraient intervenir dans la première phase possible.

Si l'adresse de pseudonyme et l'adresse de transport sont spécifiées toutes les deux, la préférence doit être accordée à l'adresse de pseudonyme.

Il n'y a pas de synchronisation ni de verrouillage explicite entre deux extrémités au cours de la procédure d'établissement de la communication. Cela implique que l'extrémité A peut envoyer un message Setup à l'extrémité B exactement en même temps que l'extrémité B envoie un message Setup à l'extrémité A. Il appartient à l'application de déterminer si une seule communication est souhaitée et de prendre les mesures appropriées. Celles-ci peuvent consister, pour une extrémité, à indiquer qu'elle est occupée chaque fois qu'elle a un message Setup en cours. Si une extrémité peut prendre en charge plusieurs communications simultanées, elle devrait indiquer qu'elle est occupée chaque fois qu'elle reçoit un message Setup issu de l'extrémité pour laquelle elle a un message Setup en cours.

Une extrémité doit être capable d'envoyer le message d'alerte. Celui-ci implique que l'(utilisateur) appelé a été alerté d'un appel entrant. Le message d'alerte ne peut être émis que par l'extrémité finalement appelée et cela seulement lorsque son utilisateur a été alerté. En cas d'interfonctionnement par l'intermédiaire d'une passerelle, celle-ci doit envoyer le message d'alerte dès qu'elle reçoit du RCC une indication de sonnerie. Si une extrémité peut répondre à un message Setup par un message Connect, de communication en cours ou de Release Complete dans les 4 secondes, cette extrémité n'a pas besoin d'envoyer le message d'alerte. Une extrémité qui émet le message Setup peut s'attendre à recevoir un message d'alerte, de connexion, de communication en cours ou de Release Complete dans les 4 secondes après avoir envoyé ce signal.

Le message Connect ne devrait être émis que s'il est certain que l'échange de capacités H.245 sera effectué correctement et qu'un niveau minimal de communication pourra avoir lieu, cela afin de conserver la cohérence de la signification du message Connect entre réseaux en mode paquet et réseaux à commutation de circuits.

8.1.1 Etablissement de la communication de base – Ni l'une ni l'autre des deux extrémités n'est enregistrée

Dans le scénario représenté à la Figure 29, ni l'une ni l'autre des deux extrémités n'est enregistrée auprès d'un portier. Les deux extrémités communiquent directement entre elles. L'extrémité 1 (extrémité appelante) envoie le message Setup (1) à l'identificateur du point TSAP communément admis de la voie de signalisation d'appel de l'extrémité 2. L'extrémité 2 répond par le message Connect (4) qui contient une adresse de transport par la voie de commande H.245 à utiliser en signalisation H.245.

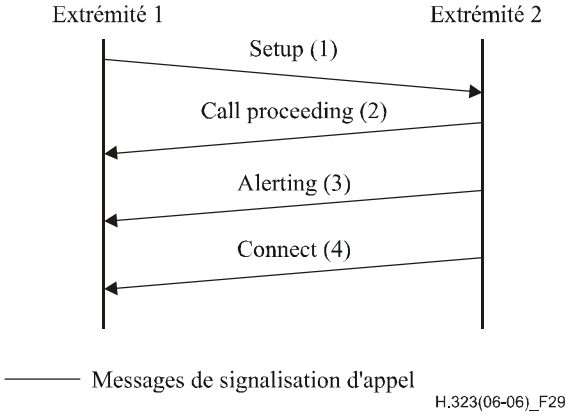


Figure 29/H.323 – Etablissement de la communication de base, sans portiers

8.1.2 Enregistrement des deux extrémités auprès du même portier

Dans le scénario représenté à la Figure 30, les deux extrémités sont enregistrées auprès du même portier, celui-ci ayant choisi la signalisation d'appel directe. L'extrémité 1 (extrémité appelante) lance avec ce portier l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier doit renvoyer l'adresse de transport de la voie de signalisation d'appel de l'extrémité 2 (extrémité appelée) dans le message de confirmation ACF. L'extrémité 1 envoie ensuite à l'extrémité 2 le message Setup (3) à cette adresse de transport. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier un échange de messages de demande ARQ (5)/de confirmation ACF (6). Il est possible qu'un message de refus ARJ (6) soit reçu par l'extrémité 2, auquel cas celle-ci envoie le message Release Complete à l'extrémité 1. L'extrémité 2 répond par un message Connect (8) qui contient une adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245.

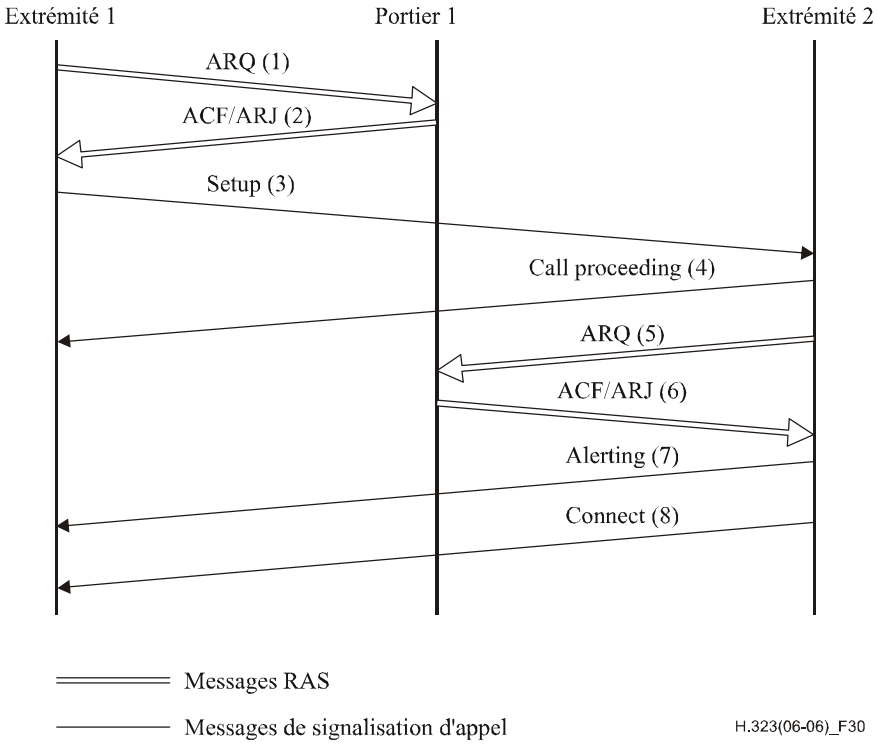


Figure 30/H.323 – Enregistrement des deux extrémités auprès du même portier – Signalisation d'appel directe

Dans le scénario représenté à la Figure 31, les deux extrémités sont enregistrées auprès du même portier, celui-ci ayant choisi d'acheminer la signalisation d'appel. L'extrémité 1 (extrémité appelante) lance avec ce portier l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier doit renvoyer une adresse de transport de la voie de signalisation d'appel de lui-même dans le message de confirmation ACF. L'extrémité 1 envoie alors le message Setup (3) à cette adresse de transport. Le portier envoie ensuite le message Setup (4) à l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier l'échange des messages de demande ARQ (6)/de confirmation ACF (7). Il est possible qu'un message de refus ARJ (7) soit reçu par l'extrémité 2, auquel cas celle-ci envoie un message Release Complete au portier. L'extrémité 2 répond par le message Connect (9) qui contient une adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245. Le portier envoie à l'extrémité 1 le message Connect (10) pouvant inclure l'adresse de transport de la voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de la voie de commande H.245 d'un portier, selon que le portier choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

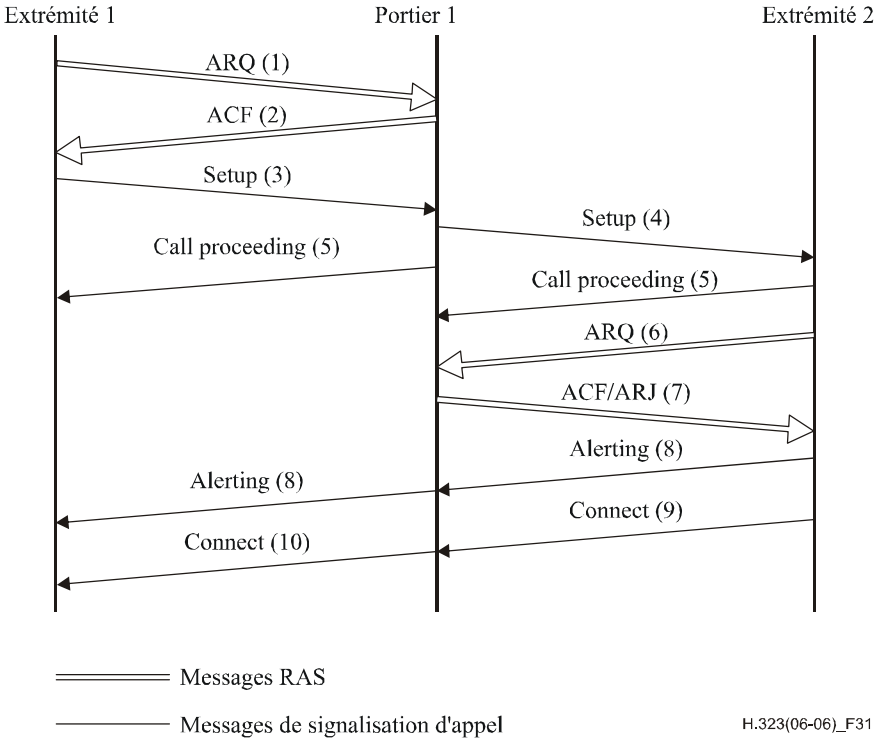


Figure 31/H.323 – Enregistrement des deux extrémités auprès du même portier – Signalisation d'appel indirecte par l'intermédiaire du portier

8.1.3 Enregistrement de la seule extrémité appelante auprès d'un portier

Dans le scénario représenté à la Figure 32, l'extrémité 1 (extrémité appelante) est enregistrée auprès d'un portier, l'extrémité 2 (extrémité appelé) n'est pas enregistrée auprès d'un portier, celui-ci ayant choisi la signalisation d'appel directe. L'extrémité 1 lance avec le portier l'échange des messages de demande ARQ (1)/de confirmation ACF (2). L'extrémité 1 envoie ensuite à l'extrémité 2 le message Setup (3) à l'adresse de transport communément admise de la voie de signalisation d'appel. Si elle souhaite accepter l'appel, l'extrémité 2 répond par le message Connect (6) qui contient l'adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245.

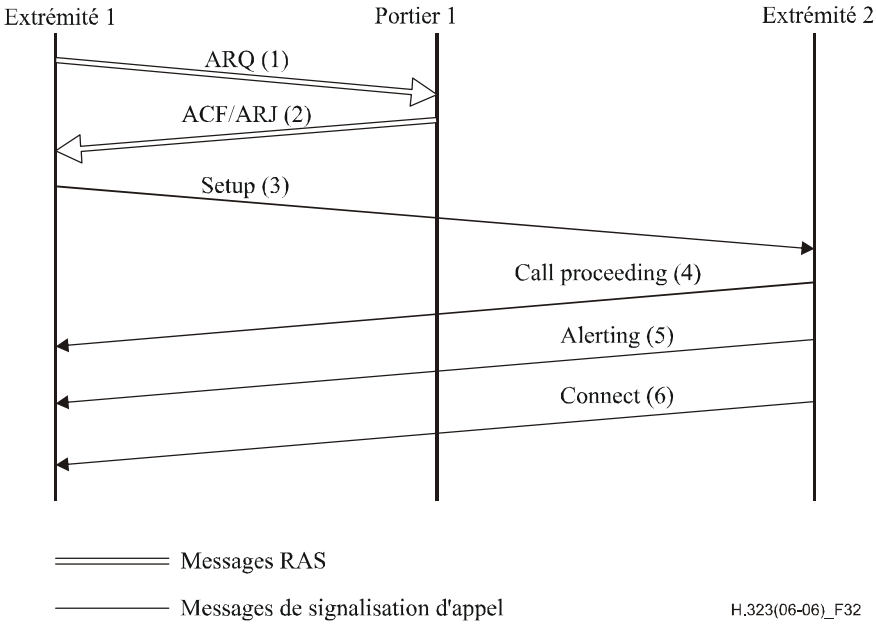


Figure 32/H.323 – Enregistrement de la seule extrémité appelante – Signalisation d'appel directe

Dans le scénario représenté à la Figure 33, l'extrémité 1 (extrémité appelante) est enregistrée auprès d'un portier, l'extrémité 2 (extrémité appelé) n'est pas enregistrée auprès d'un portier, le portier ayant choisi d'acheminer la signalisation d'appel. L'extrémité 1 (extrémité appelante) lance avec ce portier l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier doit renvoyer une adresse de transport de la voie de signalisation d'appel de lui-même dans le message de confirmation ACF (2). L'extrémité 1 envoie alors le message Setup (3) à cette adresse de transport. Le portier envoie ensuite le message Setup (4) à l'adresse de transport communément admise de la voie de signalisation d'appel de l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 répond par le message Connect (7) qui contient une adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245. Le portier envoie à l'extrémité 1 le message Connect (8) qui peut contenir l'adresse de transport de la voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de la voie de commande H.245 d'un portier, selon que le portier choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

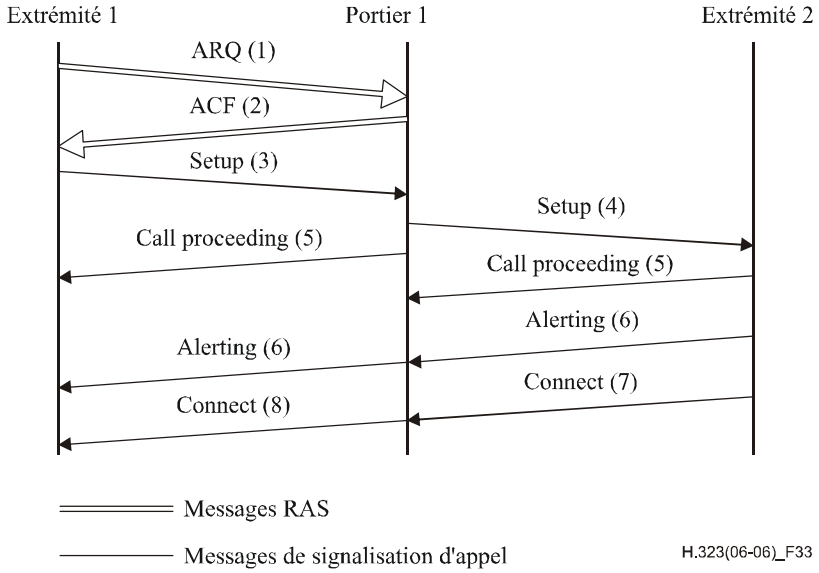


Figure 33/H.323 – Enregistrement de la seule extrémité appelante – Signalisation d'appel indirecte par l'intermédiaire du portier

8.1.4 Enregistrement de la seule extrémité appelée auprès d'un portier

Dans le scénario représenté à la Figure 34, l'extrémité 1 (extrémité appelante) n'est pas enregistrée auprès d'un portier, l'extrémité 2 (extrémité appelée) est enregistrée auprès d'un portier, et le portier a choisi la signalisation d'appel directe. L'extrémité 1 envoie à l'extrémité 2 le message Setup (1) à l'adresse de transport communément admise de la voie de signalisation d'appel. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier l'échange des messages de demande ARQ (3)/de confirmation ACF (4). Il est possible qu'un message de refus ARJ (4) soit reçu par l'extrémité 2, auquel cas celle-ci envoie un message Release Complete à l'extrémité 1. L'extrémité 2 répond par un message Connect (6) qui contient une adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245.

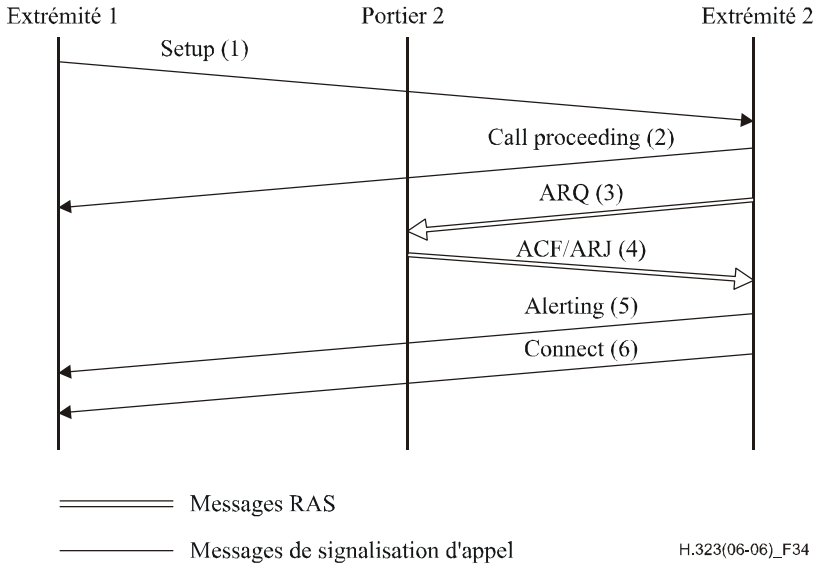


Figure 34/H.323 – Enregistrement de la seule extrémité appelée – Signalisation d'appel directe

Dans le scénario représenté à la Figure 35, l'extrémité 1 (extrémité appelante) n'est pas enregistrée auprès d'un portier, l'extrémité 2 (extrémité appelée) est enregistrée auprès d'un portier, et le portier a choisi d'acheminer la signalisation d'appel. L'extrémité 1 (extrémité appelante) envoie un message Setup (1) à l'adresse de transport de la voie de signalisation d'appel de l'extrémité 2 communément admise. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier l'échange des messages de demande ARQ (3)/de confirmation ACF (4). Si c'est acceptable, le portier doit renvoyer une adresse de transport de la voie de signalisation d'appel de lui-même dans le message de refus ARJ (4) avec un code de cause correspondant à **routeCallToGatekeeper** (acheminement de l'appel au portier). L'extrémité 2 répond à l'extrémité 1 par un message Facility (5) contenant l'adresse de transport pour voie de signalisation d'appel de son portier. L'extrémité 1 envoie alors le message Release Complete (6) à l'extrémité 2. L'extrémité 1 envoie un message Setup (7) à l'adresse de transport de voie de signalisation d'appel du portier. Le portier envoie le message Setup (8) à l'extrémité 2. L'extrémité 2 lance avec ce portier l'échange des messages ARQ(9)/ACF(10). L'extrémité 2 répond ensuite par un message Connect (12) qui contient son adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245. Le portier envoie à l'extrémité 1 le message Connect (13) qui peut contenir l'adresse de transport de la voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de la voie de commande H.245 d'un portier, selon que le portier choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

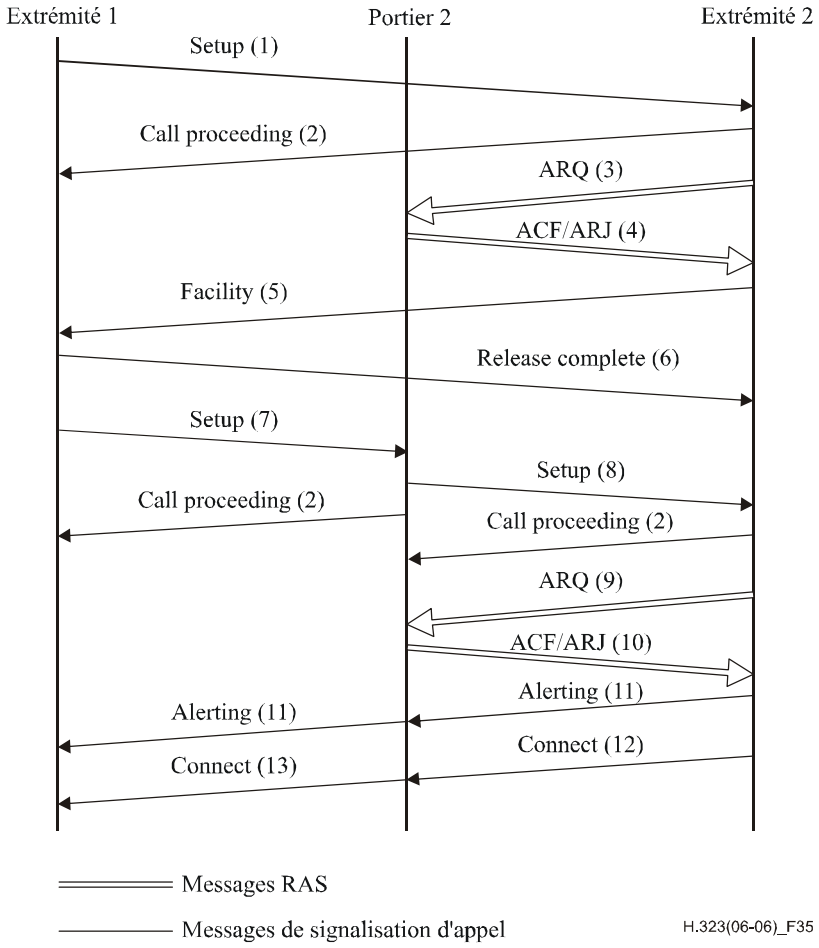


Figure 35/H.323 – Enregistrement de la seule extrémité appelée – Signalisation d'appel indirecte par l'intermédiaire du portier

8.1.5 Enregistrement des deux extrémités auprès de portiers différents

Dans le scénario représenté à la Figure 36, les deux extrémités sont enregistrées auprès de deux portiers différents ayant l'un et l'autre choisi la signalisation d'appel directe. L'extrémité 1 (extrémité appelante) lance avec le portier 1 l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier 1 peut renvoyer l'adresse de transport de la voie de signalisation d'appel de l'extrémité 2 (extrémité appelée) dans le message de confirmation ACF si le portier 1 est en mesure de communiquer avec le portier 2. L'extrémité 1 envoie alors le message Setup (3) à l'adresse de transport renvoyée par le portier (le cas échéant) ou à l'adresse de transport de voie de signalisation d'appel communément admise de l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier 2 l'échange des messages de demande ARQ (5)/de confirmation ACF (6). Il est possible qu'un message de refus ARJ (6) soit reçu par l'extrémité 2, auquel cas celle-ci envoie le message Release Complete à l'extrémité 1. L'extrémité 2 répond par un message Connect (8) qui contient une adresse de transport de la voie de commande H.245 à utiliser en signalisation H.245.

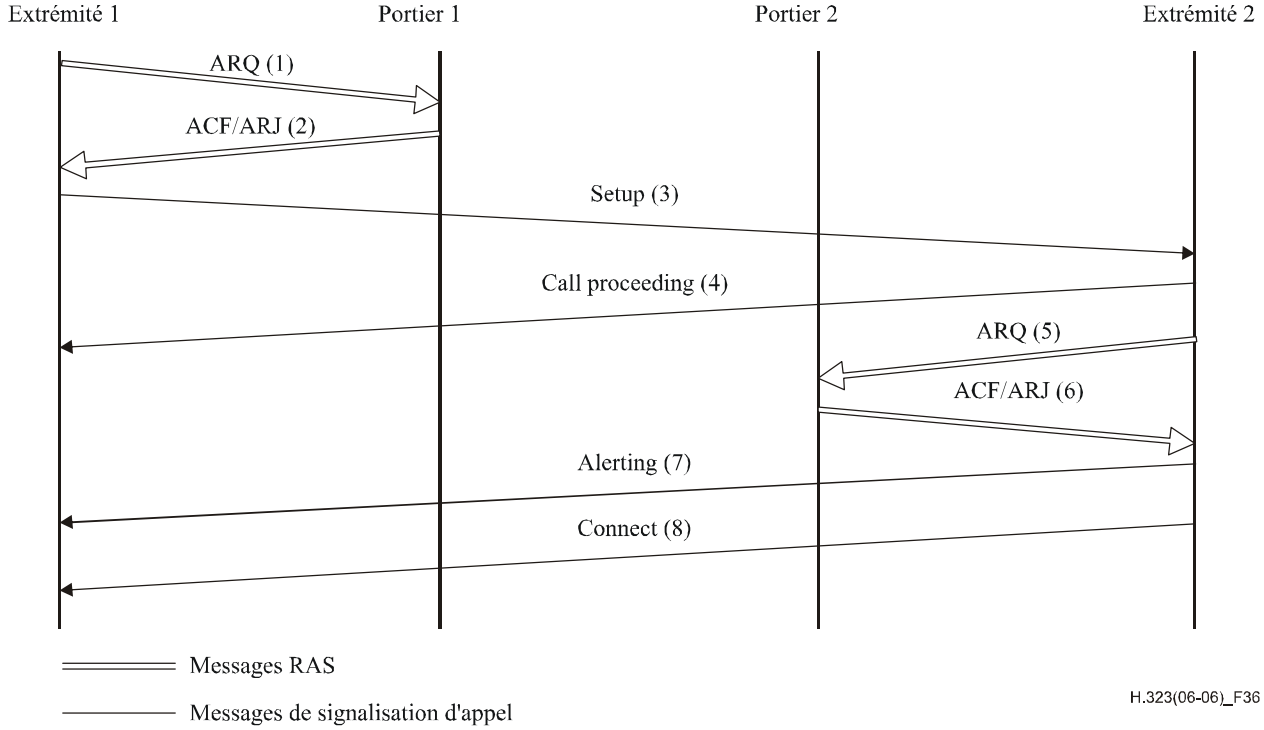


Figure 36/H.323 – Enregistrement des deux extrémités – Signalisation d'appel directe entre les deux portiers

Dans le scénario représenté à la Figure 37, les deux extrémités sont enregistrées auprès de portiers différents, le portier de l'extrémité appelante choisissant la signalisation d'appel directe et le portier de l'extrémité appelée choisissant la signalisation d'appel indirecte. L'extrémité 1 (extrémité appelante) lance avec le portier 1 l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier 1 peut renvoyer l'adresse de transport de la voie de signalisation d'appel de l'extrémité 2 (extrémité appelée) dans le message de confirmation ACF (2) si le portier 1 est en mesure de communiquer avec le portier 2. L'extrémité 1 envoie alors le message Setup (3) à l'adresse de transport renvoyée par le portier (le cas échéant) ou à l'adresse de transport de voie de signalisation d'appel communément admise de l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier 2 l'échange des messages de demande ARQ (5)/de confirmation ACF (6). Si c'est acceptable, le portier 2 doit renvoyer une adresse de transport de la voie de signalisation d'appel de lui-même dans le message de refus ARJ (6) avec un code de cause correspondant à **routeCallToGatekeeper**. L'extrémité 2 répond à l'extrémité 1 par un message

Facility (7) contenant l'adresse de transport pour voie de signalisation d'appel du portier 2. L'extrémité 1 envoie alors le message Release Complete (8) à l'extrémité 2. L'extrémité 1 doit envoyer un message de demande DRQ (9) au portier 1 qui répond par un message de confirmation DCF (10). L'extrémité 1 lance alors un nouvel échange de messages ARQ (11)/ACF (12) avec le portier 1. L'extrémité 1 envoie un message Setup (13) à l'adresse de transport de voie de signalisation d'appel du portier. Le portier 2 envoie le message Setup (14) à l'extrémité 2. Celle-ci lance l'échange de messages ARQ (15)/ACF (16) avec le portier 2. L'extrémité 2 répond alors par un message Connect (18) qui contient son adresse de transport de voie de commande H.245 à utiliser en signalisation H.245. Le portier 2 envoie à l'extrémité 1 le message Connect (19) qui peut contenir l'adresse de transport de voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de voie de commande H.245 d'un portier 2, selon que le portier choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

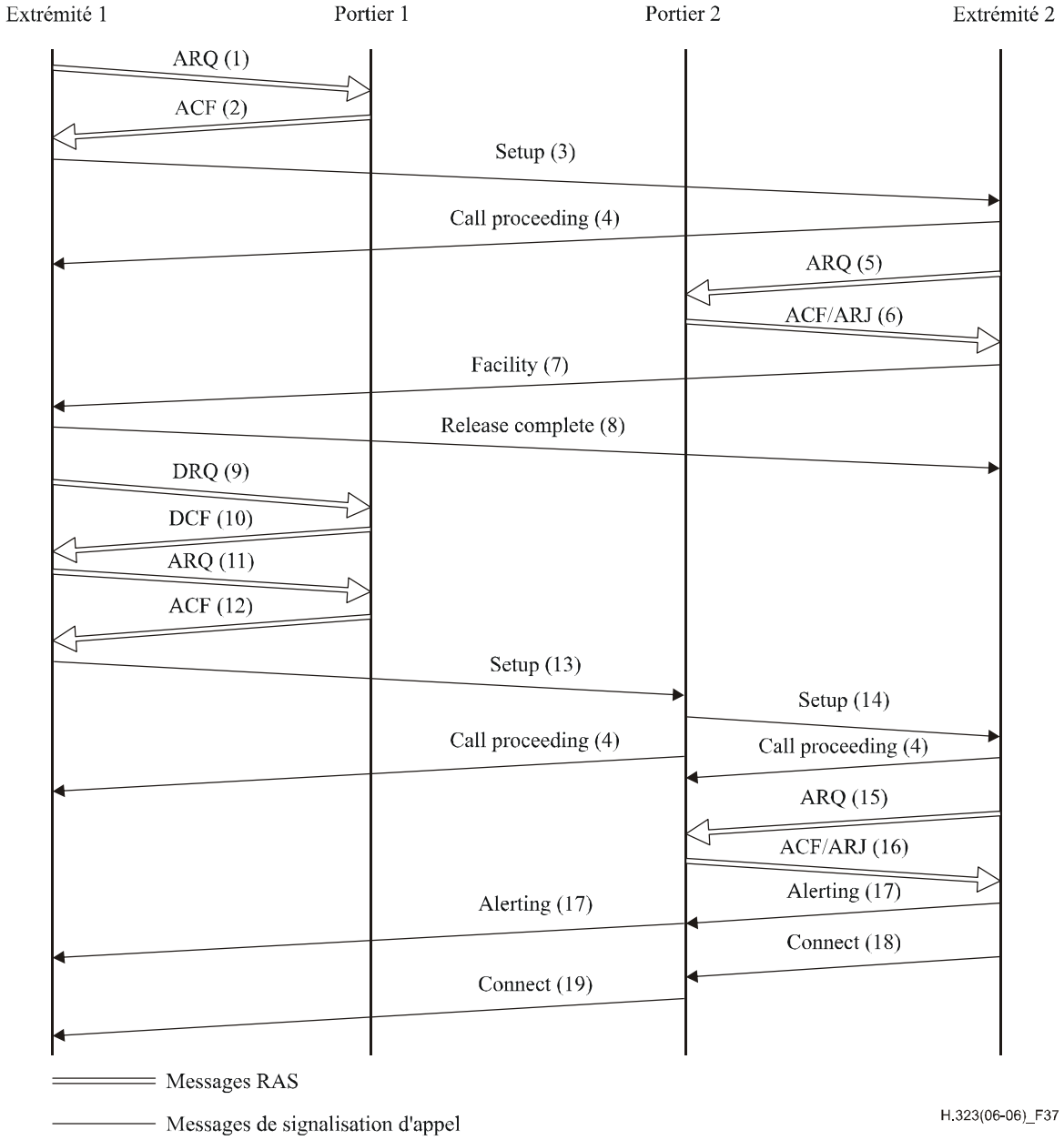


Figure 37/H.323 – Enregistrement des deux extrémités – Signalisation d'appel directe/indirecte

Dans le scénario représenté à la Figure 38, les deux extrémités sont enregistrées auprès de portiers différents, le portier de l'extrémité appelante choisissant la signalisation d'appel indirecte et le portier de l'extrémité appelée choisissant la signalisation d'appel directe. L'extrémité 1 (extrémité appelante) lance avec le portier 1 l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier 1 doit renvoyer une adresse de transport de voie de signalisation d'appel de lui-même dans le message de confirmation ACF (2). L'extrémité 1 envoie alors le message Setup (3) à cette adresse de transport. Le portier 1 envoie ensuite le message Setup (4) contenant son adresse de transport de voie de signalisation d'appel à l'adresse de transport de voie de signalisation d'appel communément admise de l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier 2 l'échange des messages de demande ARQ (6)/de confirmation ACF (7). Il est possible qu'un message de refus ARJ (7) soit reçu par l'extrémité 2, auquel cas celle-ci envoie le message Release Complete à l'extrémité 1. L'extrémité 2 répond au portier 1 par le message Connect (9) qui contient son adresse de transport de voie de commande H.245 à utiliser en signalisation H.245. Le portier 1 envoie à l'extrémité 1 le message Connect (10) qui peut contenir l'adresse de transport de voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de voie de commande H.245 d'un portier 1, selon que le portier choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

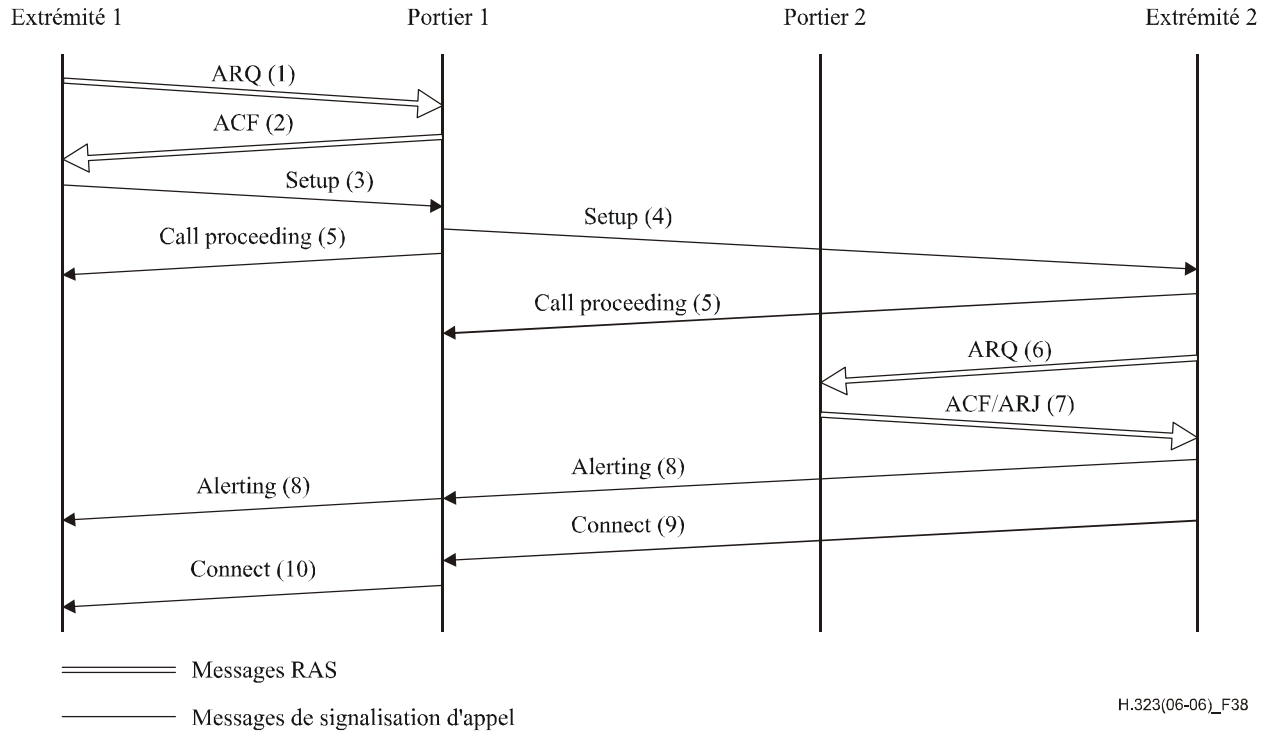


Figure 38/H.323 – Enregistrement des deux extrémités – Signalisation d'appel indirecte/directe

Dans le scénario représenté à la Figure 39, les deux extrémités sont enregistrées auprès de deux portiers différents choisissant l'un et l'autre la signalisation d'appel indirecte. L'extrémité 1 (extrémité appelante) lance avec le portier 1 l'échange des messages de demande ARQ (1)/de confirmation ACF (2). Le portier 1 doit renvoyer une adresse de transport de voie de signalisation d'appel de lui-même dans le message de confirmation ACF (2). L'extrémité 1 envoie alors le message Setup (3) à cette adresse de transport. Le portier 1 envoie ensuite le message Setup (4) à l'adresse de transport de voie de signalisation d'appel communément admise de l'extrémité 2. Si elle souhaite accepter l'appel, l'extrémité 2 lance avec le portier 2 l'échange des messages de demande ARQ (6)/de confirmation ACF (7). Si c'est acceptable, le portier 2 doit renvoyer une adresse de transport de voie de signalisation d'appel de lui-même dans le message de refus ARJ (7) avec un

code de cause correspondant à **routeCallToGatekeeper**. L'extrémité 2 répond au portier 1 par un message Facility (8) contenant l'adresse de transport pour voie de signalisation d'appel du portier 2. Le portier 1 envoie le message Release Complete (9) à l'extrémité 2. Le portier 1 envoie un message Setup (10) à l'adresse de transport de voie de signalisation d'appel du portier 2. Le portier 2 envoie le message Setup (11) à l'extrémité 2. Celle-ci lance l'échange de messages ARQ (12)/ACF (13) avec le portier 2. L'extrémité 2 répond alors au portier 2 par le message Connect (15) qui contient son adresse de transport de voie de commande H.245 à utiliser en signalisation H.245. Le portier 2 envoie au portier 1 le message Connect (16) qui peut contenir l'adresse de transport de voie de commande H.245 de l'extrémité 2 ou l'adresse de transport de voie de commande H.245 du portier 2, selon que le portier 2 choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement. Le portier 1 envoie à l'extrémité 1 le message Connect (17) qui peut contenir l'adresse de transport de voie de commande H.245 envoyée par le portier 2 ou l'adresse de transport de voie de commande H.245 du portier 1, selon que le portier 1 choisit d'utiliser ou non la voie de commande H.245 pour l'acheminement.

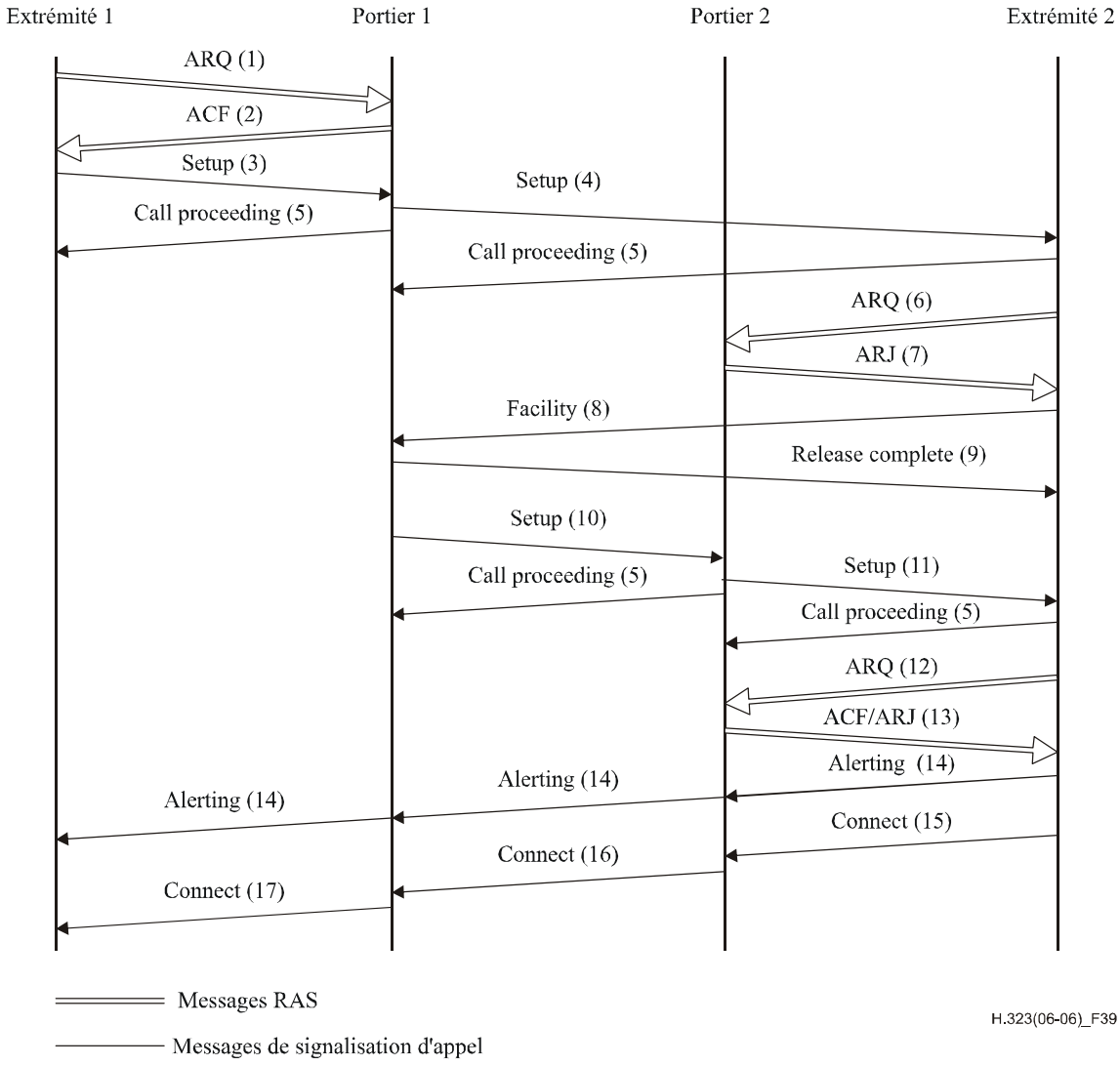


Figure 39/H.323 – Enregistrement des deux extrémités – Utilisation de la signalisation d'appel indirecte par les deux portiers

8.1.6 Signalisation facultative par l'extrémité appelée

Les procédures définies aux § 8.1.4 et 8.1.5 montrent que, lorsqu'une extrémité appelée est enregistrée auprès d'un portier, un message Setup est initialement envoyé à cette extrémité appelée par le point appelant ou par le portier de ce dernier. Si le portier de l'extrémité appelée souhaite utiliser le modèle d'appel acheminé par portier, il renvoie, dans le message ARJ, sa propre adresse de transport pour voie de signalisation d'appel. Le point appelé utilise ensuite le message Facility pour renvoyer l'appel vers l'adresse de transport pour voie de signalisation d'appel du portier de l'extrémité appelée. Ces procédures partent du principe que le point appelant (ou son portier) ne connaît que l'adresse de transport pour voie de signalisation d'appel de l'extrémité appelée. Cette adresse peut avoir été reçue dans un message LCF envoyé en réponse à un message LRQ demandant l'adresse de l'extrémité appelée. Elle peut également être connue par des méthodes hors bande.

Si le portier de l'extrémité appelée souhaite utiliser le modèle d'appel acheminé par portier, il peut renvoyer, dans le message LCF, sa propre adresse de transport pour voie de signalisation d'appel. Cette adresse permettra à l'extrémité appelante (ou à son portier), d'envoyer directement le message Setup au portier de l'extrémité appelée, supprimant ainsi le processus de réacheminement.

La Figure 40 donne un exemple de ce scénario, où les deux extrémités sont enregistrées auprès de portiers différents qui choisissent d'acheminer la signalisation d'appel (comme dans le cas de la Figure 39). L'extrémité 1 (extrémité appelante) envoie une demande ARQ (1) au portier 1. Celui-ci multidiffuse une demande LRQ (2) pour localiser le point appelé 2. Le portier 2 renvoie un message LCF (3) contenant sa propre adresse de transport pour voie de signalisation d'appel. Le portier 1 enverra donc un message Setup (6) à l'adresse de transport pour voie de signalisation d'appel du portier 2 et celui-ci enverra à l'extrémité 2 un message Setup (8). L'extrémité 2 engage le dialogue ARQ (9)/ACF (10) avec le portier 2 puis répond à celui-ci par le message Connect (12) contenant son adresse de transport pour voie de commande H.245, pour utilisation en signalisation H.245. Le portier 2 envoie au portier 1 le message Connect (13), qui peut contenir l'adresse de transport pour voie de commande H.245 de l'extrémité 2 ou une adresse de transport par la voie de commande H.245 du portier 2, selon que celui-ci choisit d'acheminer la voie de commande H.245 ou non. Le portier 1 envoie à l'extrémité 1 le message Connect (14) qui peut contenir l'adresse de transport par voie de commande H.245 envoyée par le portier 2 ou une adresse de transport par la voie de commande H.245 du portier 1, selon que celui-ci choisit d'acheminer la voie de commande H.245 ou non.

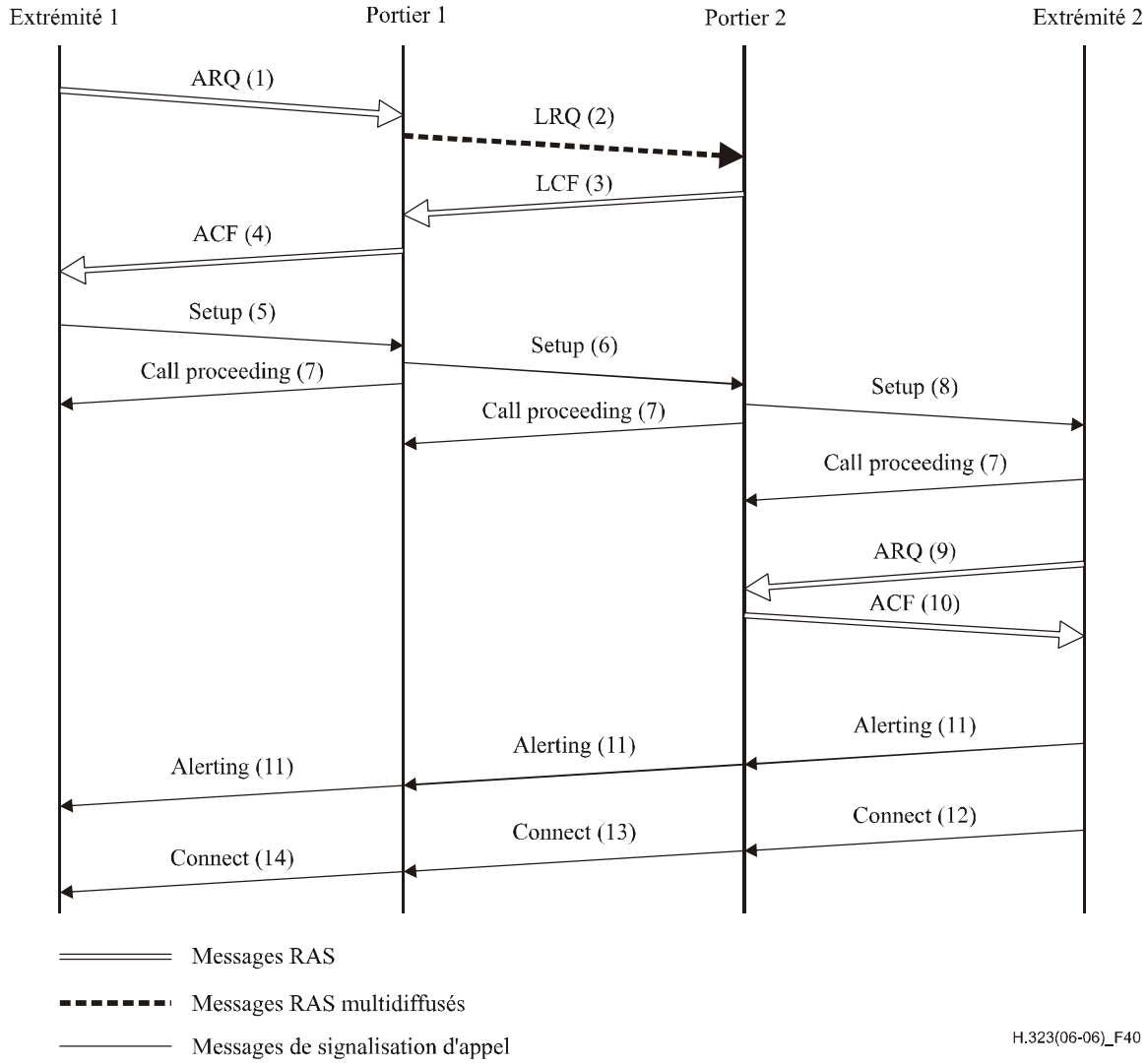


Figure 40/H.323 – Signalisation facultative de l'extrémité appelée

8.1.7 Procédure de connexion rapide

Les extrémités H.323 peuvent établir des voies multimédias dans une chaîne de communication utilisant soit les procédures définies dans la Rec. UIT-T H.245 soit la procédure de connexion rapide décrite dans le présent paragraphe. Cette procédure permet aux extrémités d'établir une communication point à point de base avec un seul aller et retour d'échange de messages, permettant une remise immédiate du flux multimédia dès la connexion de l'appel.

L'extrémité appelante lance la procédure de connexion rapide en envoyant à l'extrémité appelée un message Setup contenant l'élément **fastStart**. Cet élément se compose d'une séquence de structures **OpenLogicalChannel** décrivant des voies multimédias que l'extrémité appelante propose d'émettre et de recevoir, y compris tous les paramètres nécessaires à une ouverture immédiate et à un transfert immédiat des données multimédias sur les voies ainsi ouvertes. Le contenu et l'usage de l'élément **fastStart** sont examinés ci-dessous.

L'extrémité appelée peut refuser d'utiliser la procédure de connexion rapide, soit parce qu'elle ne l'implémente pas soit parce qu'elle a l'intention d'invoquer des capacités qui nécessitent l'application des procédures définies dans la Rec. UIT-T H.245. Le refus de la procédure de connexion rapide s'effectue soit par le non-renvoi de l'élément **fastStart** soit par l'insertion de l'élément **fastConnectRefused** dans un quelconque message de signalisation d'appel H.225.0, jusqu'au message Connect inclus. On constate qu'une extrémité ne peut pas omettre l'élément **fastStart** dans

un message avant le message Connect, mais plus tard, acceptant ainsi la procédure de connexion rapide. Le refus de la procédure de connexion rapide (ou son non-lancement) nécessite l'application des procédures H.245 pour l'échange de capacités et pour l'ouverture des voies multimédias.

Lorsque l'extrémité appelée souhaite appliquer la procédure de connexion rapide, elle envoie un message de signalisation d'appel H.225.0 Call Proceeding, Progress, Alerting, ou Connect contenant un élément **fastStart** opérant une sélection parmi les propositions **OpenLogicalChannel** offertes par l'extrémité appelante. L'extrémité appelante doit traiter chacun de ces messages jusqu'à ce qu'elle détermine que la connexion rapide est acceptée ou refusée. Bien que l'extrémité appelante puisse recevoir l'élément **fastSart** dans le message Facility envoyé par un portier, l'extrémité appelée ne doit pas utiliser le message Facility pour envoyer l'élément **fastStart**. Les voies ainsi acceptées sont considérées comme ouvertes même si la procédure H.245 habituelle **openLogicalChannel** et **openLogicalChannelAck** a été suivie. L'extrémité appelée ne doit pas insérer d'élément **fastStart** dans un quelconque message de signalisation d'appel H.225.0 envoyé après le message Connect. Elle ne doit pas non plus inclure d'élément **fastStart** dans un quelconque message de signalisation d'appel H.225.0, à moins que le message Setup ne contienne déjà cet élément.

L'extrémité appelée peut commencer à émettre des données multimédias (en fonction des voies ouvertes) immédiatement après avoir envoyé un message de signalisation d'appel H.225.0 contenant l'élément **fastStart**. L'extrémité appelante doit donc être disposée à recevoir des données multimédias sur *l'une quelconque* des voies de réception qu'elle a proposées dans le message Setup, car il est possible que les données multimédias soient reçues avant le message de signalisation d'appel H.225.0 indiquant précisément quelles voies seront utilisées. Une fois qu'un message de signalisation d'appel H.225.0 contenant l'élément **fastStart** a été reçu par l'extrémité appelante, celle-ci peut arrêter ses tentatives de réception de données multimédias sur les voies pour lesquelles l'extrémité appelée n'a pas accepté de propositions. Noter que des prescriptions nationales peuvent interdire aux extrémités appelées d'émettre des données multimédias ou limiter la nature des données contenues dans le flux média, avant transmission d'un message Connect. Il appartient à l'extrémité de satisfaire aux prescriptions applicables. Si l'extrémité appelante met l'élément **mediaWaitForConnect** à la valeur "TRUE" dans le message Setup, l'extrémité appelée ne doit pas envoyer de données multimédias avant que le message Connect ait été envoyé.

L'extrémité appelante peut commencer à envoyer les flux média (en fonction des voies ouvertes) dès qu'elle reçoit un message de signalisation d'appel H.225.0 contenant l'élément **fastStart**. L'extrémité appelée doit donc être prête à recevoir immédiatement des données multimédias sur les voies qu'elle a acceptées dans le message de signalisation d'appel H.225.0 contenant l'élément **fastStart**. Noter que des prescriptions nationales peuvent interdire aux extrémités appelantes d'émettre des données multimédias ou limiter la nature des données contenues dans le flux média, avant réception d'un message Connect. Il appartient à l'extrémité de satisfaire aux prescriptions applicables.

NOTE 1 – Une entité ne doit pas envoyer d'élément **fastStart** vide dans un message quelconque (c'est-à-dire qu'un élément **fastStart** doit contenir au moins une proposition **OpenLogicalChannel**). Si une extrémité reçoit effectivement un élément **fastStart** ne contenant pas de proposition **OpenLogicalChannel**, cette extrémité ne doit pas tenir compte de l'élément **fastStart**.

NOTE 2 – Lorsqu'une extrémité ou un portier intervenant dans la signalisation d'appel reçoit un élément **fastStart** dans un message Call Proceeding, cette entité ne sera pas en mesure de faire suivre ce message si celui-ci a déjà été envoyé vers le côté origine. Dans ce cas, l'élément **fastStart** contenu dans le message Call Proceeding doit être appliqué sur un élément **fastStart** d'un message Facility.

8.1.7.1 Proposition, sélection et ouverture de voies médias

L'extrémité appelante peut proposer de multiples voies médias ou de multiples ensembles de caractéristiques en variante pour chaque voie média, par codage de multiples structures **OpenLogicalChannel** dans l'élément **fastStart** du message Setup. Chaque structure

OpenLogicalChannel contenue dans l'élément de **fastStart** décrit exactement une seule voie média unidirectionnelle ou une seule voie média bidirectionnelle.

Dans le message Setup, chaque message **OpenLogicalChannel** est une proposition visant à établir une voie média. Les propositions **OpenLogicalChannel** sont incluses dans l'élément **fastStart** selon l'ordre des préférences, la variante préférée en premier étant citée d'abord dans la séquence **fastStart**. Les propositions d'ouverture de voies audio doivent être citées avant les ouvertures de voies médias d'autres types. Dans le message de signalisation d'appel H.225.0 contenant l'élément **fastStart** envoyé en réponse au message Setup, chaque message **OpenLogicalChannel** signifie l'acceptation d'une voie média proposée, avec l'indication des voies établies qui peuvent être utilisées immédiatement pour la transmission de données multimédias.

Si un élément **dataType** spécifie le cryptage via le choix **h235Media**, l'élément **encryptionAuthenticationAndIntegrity** inclus peut incorporer un élément **encryptionCapability** contenant de multiples algorithmes de cryptage (dont l'algorithme NULL). Cette structure doit être adoptée pour permettre de choisir l'un quelconque des algorithmes de cryptage spécifiés pour la capacité média associée.

Dans un message **OpenLogicalChannel** proposant une voie pour la transmission en provenance de l'extrémité appelante à destination de l'extrémité appelée, l'élément **forwardLogicalChannelParameters** doit contenir des paramètres spécifiant les caractéristiques de la voie proposée, tandis que l'élément **reverseLogicalChannelParameters** doit être omis. Chaque structure **OpenLogicalChannel** de ce type doit comporter une unique valeur de l'élément **forwardLogicalChannelNumber**. Les propositions en variante concernant la même voie d'émission doivent contenir la même valeur **sessionID** dans l'élément **H2250LogicalChannelParameters**. L'élément **mediaChannel** doit être omis de la proposition; il sera fourni par l'extrémité appelée si la proposition est acceptée. Les éléments **H2250LogicalChannelParameters** et **dataType** de ces autres propositions doivent être construits de façon à décrire correctement les capacités d'émission de l'extrémité appelante associées à la voie ainsi proposée. L'extrémité appelante peut choisir de ne pas proposer de voies pour la transmission de données de l'extrémité appelante à l'extrémité appelée, par exemple si elle souhaite utiliser ultérieurement les procédures H.245 pour établir de telles voies.

Dans le message Setup, chaque message **OpenLogicalChannel** qui propose une voie unidirectionnelle pour la transmission dans le sens de l'extrémité appelante vers l'extrémité appelée et qui achemine le média au moyen du protocole RTP doit contenir l'élément **mediaControlChannel** (indiquant la voie RTCP inverse) dans l'élément **H2250LogicalChannelParameters** de la structure **forwardLogicalChannelParameters**.

Dans un message **OpenLogicalChannel** proposant une voie pour la transmission en provenance de l'extrémité appelée à destination de l'extrémité appelante, l'élément **reverseLogicalChannelParameters** doit être inclus et doit contenir des paramètres spécifiant les caractéristiques de la voie proposée. L'élément **forwardLogicalChannelParameters** doit également être inclus (car il n'est pas facultatif) avec l'élément **dataType** mis à la valeur **nullData**, l'élément **multiplexParameters** mis à la valeur **none** et tous les éléments facultatifs omis. Les propositions en variante pour la même voie de réception doivent contenir la même valeur **sessionID** dans l'élément **H2250LogicalChannelParameters**. Toutes les autres structures **OpenLogicalChannel** possibles, qui proposent une voie pour la transmission depuis l'extrémité appelée à l'extrémité appelante, doivent contenir la même valeur **sessionID** et la même valeur **mediaChannel**. Les éléments **H2250LogicalChannelParameters** et **dataType** contenus dans l'élément **reverseLogicalChannelParameters** de ces autres propositions doivent être construits de façon à décrire correctement les capacités de réception de l'extrémité appelante associées à la voie ainsi proposée. L'extrémité appelante peut choisir de ne pas proposer de voies pour la transmission de données de l'extrémité appelée à l'extrémité appelante, par exemple si elle souhaite utiliser ultérieurement les procédures H.245 pour établir de telles voies.

Dans le message Setup, chaque structure **OpenLogicalChannel** qui propose une voie pour la transmission depuis l'extrémité appelée à l'extrémité appelante et qui transportera un média utilisant le protocole RTP doit contenir l'élément **mediaControlChannel** (désignant la voie RTCP allant dans le même sens) dans l'élément **H2250LogicalChannelParameters** de la structure **reverseLogicalChannelParameters**.

Dans une structure **OpenLogicalChannel** proposant une voie bidirectionnelle entre l'extrémité appelante et l'extrémité appelée, les éléments **forwardLogicalChannelParameters** et **reverseLogicalChannelParameters** doivent contenir des paramètres spécifiant les caractéristiques de la voie proposée. Chacune de ces structures **OpenLogicalChannel** doit avoir une valeur unique de l'élément **forwardLogicalChannelNumber**. Les propositions en variante pour la même voie bidirectionnelle doivent contenir la même valeur d'identification **sessionID** dans l'élément **H2250LogicalChannelParameters**. L'élément **mediaChannel** doit être omis de la proposition; il sera fourni dans l'élément **reverseLogicalChannelParameters** par l'extrémité appelée si la proposition est acceptée. Les autres éléments **H2250LogicalChannelParameters** et **dataType** doivent être mis à une valeur permettant de décrire correctement les capacités de transmission de l'extrémité appelante qui est associée à cette voie proposée.

Tous les éléments **mediaControlChannel** introduits par l'extrémité appelante pour la même valeur **sessionID** dans les deux sens doivent avoir la même valeur.

Dès réception d'un message Setup contenant l'élément **fastStart** et indiquant que l'extrémité appelée est disposée à appliquer la procédure de connexion rapide et dès que cette extrémité est arrivée au point de la connexion où elle est prête à commencer l'émission de données médias, cette extrémité doit choisir une des structures **OpenLogicalChannel** proposées, contenant pour chaque type de média qu'elle souhaite émettre un élément **reverseLogicalChannelParameters**, une des structures **OpenLogicalChannel** proposées**,** spécifiant pour chaque type de média qu'elle souhaite recevoir un élément **forwardLogicalChannelParameters** (en omettant l'élément **reverseLogicalChannelParameters**), une des structures **OpenLogicalChannel** proposées, contenant les deux éléments **forwardLogicalChannelParameters** et **reverseLogicalChannelParameters** pour chaque voie bidirectionnelle qu'elle souhaite émettre ou recevoir. Si des propositions en variante sont présentées, une seule structure **OpenLogicalChannel** doit être sélectionnée dans chaque ensemble de variantes; les variantes contenues dans un même ensemble possèdent le même identificateur de session (**sessionID**). Si plusieurs algorithmes de cryptage sont proposés pour une même voie, l'extrémité appelée doit en choisir un et modifier la structure **OpenLogicalChannel** pour supprimer les autres. L'extrémité appelée accepte une voie proposée en renvoyant la structure **OpenLogicalChannel** correspondante dans un quelconque message de signalisation d'appel H.225.0 envoyé en réponse au message Setup, jusqu'au message Connect inclus. L'extrémité appelée peut choisir de répéter l'élément **fastStart** dans tous les messages subséquents jusqu'à et y compris le message Connect: le contenu de l'élément **fastStart** doit être le même. Les extrémités appelantes doivent réagir au premier élément **fastStart** reçu dans un message de réponse au message Setup et ignorer les éléments **fastStart** suivants. L'extrémité appelée peut choisir de ne pas ouvrir de flux média dans un sens particulier ou d'un type média particulier: à cette fin, elle n'insérera pas de structure **OpenLogicalChannel** correspondante dans l'élément **fastStart** de la réponse de signalisation d'appel H.225.0.

Lorsqu'elle accepte une voie proposée pour l'émission de l'extrémité appelée à l'extrémité appelante, l'extrémité appelée doit renvoyer à l'extrémité appelante la structure **OpenLogicalChannel** correspondante, après avoir inséré dans la structure **OpenLogicalChannel** un numéro **forwardLogicalChannelNumber** unique et, pour les voies qui achemineront un média utilisant le protocole RTP, avoir inséré dans l'élément **H2250LogicalChannelParameters** de la structure **reverseLogicalChannelParameters** un élément **mediaControlChannel** valide (désignant la voie RTCP inverse). L'extrémité appelée peut commencer à émettre des données médias sur la voie acceptée, conformément aux paramètres spécifiés dans l'élément **reverseLogicalChannelParameters**, immédiatement après avoir envoyé la réponse de

signalisation d'appel H.225.0 contenant l'élément **fastStart**, à moins que le champ **mediaWaitForConnect** ait été validé à "TRUE", auquel cas l'extrémité doit attendre d'avoir envoyé le message Connect.

Lorsqu'elle accepte une voie proposée pour l'émission de l'extrémité appelante à l'extrémité appelée, celle-ci doit renvoyer à l'extrémité appelante la structure **OpenLogicalChannel** correspondante. L'extrémité appelée doit introduire dans l'élément **h2250LogicalChannelParameters** de la structure **forwardLogicalChannelParameters** un champ **mediaChannel** valide et, pour les voies qui achemineront un type de média utilisant le protocole RTP, un champ **mediaControlChannel** valide (désignant la voie RTCP allant dans le même sens). Tous les éléments **mediaControlChannel** insérés par l'extrémité appelée pour le même identificateur **sessionID** dans les deux sens doivent avoir la même valeur. L'extrémité appelée doit ensuite se préparer à recevoir immédiatement un flux média conforme aux paramètres spécifiés dans l'élément **forwardLogicalChannelParameters**. L'extrémité appelante peut commencer à émettre des données médias sur les voies acceptées et ouvertes, dès réception de la réponse de signalisation d'appel H.225.0 contenant l'élément **fastStart**; elle peut également libérer toutes les ressources éventuellement attribuées à la réception de voies proposées mais non acceptées.

Lorsqu'elle accepte une voie bidirectionnelle proposée pour l'émission de l'extrémité appelante à l'extrémité appelée, celle-ci doit renvoyer à l'extrémité appelante la structure **OpenLogicalChannel** correspondante. Les extrémités appelée et appelante doivent utiliser la valeur contenue dans l'élément **forwardLogicalChannelNumber** en tant que numéro de voie logique des voies de transmission avant et arrière de la voie bidirectionnelle. L'extrémité appelée doit introduire dans l'élément **h2250LogicalChannelParameters** de la structure **reverseLogicalChannelParameters** un champ **mediaChannel**. Les extrémités appelée et appelante doivent respectivement recevoir le flux média conformément aux paramètres spécifiés dans l'élément **forwardLogicalChannelParameters** et la structure **reverseLogicalChannelParameters**. L'extrémité appelée doit être prête à accepter une connexion pour la voie bidirectionnelle avant de renvoyer l'élément **fastStart**. L'extrémité appelante peut commencer à émettre les médias dans les voies acceptées dès qu'elle reçoit la réponse de signalisation d'appel H.225.0 contenant l'élément **fastStart**. Elle peut ensuite libérer d'éventuelles ressources attribuées à des voies proposées mais non acceptées.

NOTE – L'extrémité appelée n'est autorisée à modifier les champs d'une structure **OpenLogicalChannel** proposée que selon les spécifications du présent paragraphe. Une extrémité n'est pas autorisée, par exemple, à modifier le nombre de trames par paquet ni d'autres caractéristiques de la voie proposée, non spécifiquement indiquées dans le présent paragraphe. Si l'extrémité appelante souhaite augmenter la probabilité que la procédure de connexion rapide puisse être acceptée, elle doit inclure de multiples propositions contenant différents paramètres en option. Cette règle n'interdit pas à une extrémité d'inclure le champ **encryptionSync** dans la structure **OpenLogicalChannel** renvoyée.

8.1.7.2 Commutation vers les procédures H.245

Après l'établissement d'un appel au moyen de la procédure de connexion rapide, l'extrémité peut déterminer qu'il est nécessaire d'invoquer pour cet appel des éléments de service qui nécessitent l'application de procédures H.245. L'extrémité peut lancer l'application des procédures H.245 à tout moment de la communication, au moyen du procédé de tunnellisation décrit au § 8.2.1 (si l'élément **h245Tunnelling** reste activé). Une entité H.323 version 4 ou supérieure, qui utilise la procédure de connexion rapide dans un appel doit utiliser la tunnellisation H.245 lorsqu'une voie de commande H.245 est requise: dans ce cas, elle doit mettre le champ **h245Tunnelling** à la valeur "TRUE". Le processus de commutation vers une connexion H.245 distincte est décrit au § 8.2.3 et peut être utilisé par des entités en version 3 ou antérieure ou par des entités H.323 plus récentes lors de la communication avec des entités en version 3 ou antérieure afin de conserver la compatibilité amont.

Lorsqu'un appel est établi au moyen de la procédure de connexion rapide, les deux extrémités doivent garder ouvert le canal de signalisation d'appel H.225.0 jusqu'à ce que la communication soit

terminée ou, afin d'assurer la compatibilité avec des extrémités plus anciennes, jusqu'à ce qu'une connexion H.245 distincte ait été établie.

Lorsque les procédures H.245 sont activées, toutes les procédures obligatoires de la Rec. UIT-T H.245, qui s'appliquent normalement dès l'ouverture d'une connexion H.245, doivent être terminées avant le lancement de toutes éventuelles procédures H.245 additionnelles. Les voies médias qui ont été établies par la procédure de connexion rapide sont "héritées" comme si elles avaient été ouvertes par les procédures H.245 normales **openLogicalChannel** et **openLogicalChannelAck**.

Si l'extrémité appelante utilise la procédure de connexion rapide pour lancer un appel, il ne doit pas ouvrir le canal de commande H.245 en utilisant la mise en tunnel H.245 normale ou une connexion H.245 directe jusqu'à ce que l'extrémité appelée ait renvoyé l'élément **fastStart**, **fastConnectRefused**, **h245Address** ou le message Connect. Il convient de noter que les anciennes extrémités H.323 peuvent ouvrir le canal de commande H.245 même avant d'avoir reçu un de ces éléments ou ce message, malgré le fait qu'elle a initié un appel avec connexion rapide. Alors que ce comportement est fortement découragé dans les publications antérieures et est maintenant interdit, les extrémités ont besoin d'être informées de ce comportement. Si une extrémité ouvre un canal de commande H.245 avant de recevoir les éléments ou le message précités, l'extrémité doit supposer que la connexion rapide a pris fin et ne doit pas envoyer d'élément **fastStart**.

Toutefois, une extrémité peut échanger le message **terminalCapabilitySet** et le message **masterSlaveDetermination** dans le message Setup tel que décrit au § 8.2.4. Cet échange constitue l'ouverture du canal de commande H.245, mais n'interdit pas à l'une des extrémités de continuer en connexion rapide.

L'extrémité appelée doit déclencher la procédure H.245 avant de renvoyer l'élément **fastConnectRefused**, **fastStart** ou le message Connect. Une extrémité appelée qui renvoie l'élément **h245Address** dans tout message jusques et y compris le message Connect, et qui n'a pas déjà explicitement accepté ou refusé la connexion rapide, doit également renvoyer l'élément **fastStart** ou **fastConnectRefused** dans le même message. Il convient de noter qu'il est possible que les extrémités plus anciennes ne renvoient pas les éléments **fastStart** ou **fastConnectRefused**. Pour des raisons de compatibilité avec les extrémités antérieures, les extrémités H.323 supposeront que la connexion rapide est refusée lorsque l'extrémité appelée envoie l'élément **h245Address** ou ouvre le canal de commande H.245 sans avoir envoyé ou sans envoyer simultanément l'élément **fastStart** ou **fastConnectRefused**.

Il convient de noter que lorsqu'une connexion H.245 distincte est ouverte depuis l'extrémité appelée jusqu'à l'extrémité appelante qui a fourni son adresse **h245Address** dans son message Setup (établissement), une condition de concurrence apparaît: l'extrémité appelante peut détecter l'ouverture d'un canal de commande H.245 depuis l'extrémité appelée avant de recevoir l'élément **fastStart**. C'est pourquoi il est recommandé que si une extrémité accepte une connexion rapide et initie une connexion distincte pour la H.245, elle doit introduire un délai entre l'envoi du message H.225.0 contenant l'élément **fastStart** et l'initiation de la connexion H.245 distincte. Au cas où l'extrémité appelée n'introduirait pas de délai, l'extrémité appelante devra toujours être préparée à une éventuelle arrivée tardive de l'élément **fastStart** dans ce scénario. Il est possible que les extrémités plus anciennes considèrent que la connexion rapide est refusée si le canal de commande H.245 est ouvert avant la réception de l'élément **fastStart**.

8.1.7.3 Terminaison d'un appel

Si un appel connecté au moyen de la procédure de connexion rapide continue jusqu'à son terme sans lancement de procédures H.245, cet appel peut être terminé par l'une ou l'autre extrémité au moyen d'un message de signalisation d'appel H.225.0 Release Complete. Si des procédures H.245 sont lancées au cours de l'appel, celui-ci est terminé comme décrit au § 8.5.

Si une connexion H.245 distincte n'a pas été établie et que le canal de signalisation d'appel H.225.0 soit libéré, l'appel doit également être libéré.

8.1.7.4 Tonalités et annonces dans la bande et hors de la bande

Les tonalités et les annonces peuvent être produites localement ou transmises dans la bande à partir de l'extrémité de destination.

Lors de l'exécution de l'établissement d'appel, l'extrémité située du côté de la destination doit déterminer si elle fournira des tonalités dans la bande ou utilisera des tonalités produites localement du côté origine. Noter qu'un autre type d'indication peut, dans certains systèmes, remplacer des tonalités et annonces produites localement (par exemple des indications visuelles sur écran). Dans le cadre du présent paragraphe, ces indications seront désignées par l'expression *tonalités et annonces produites localement*. Par défaut, les tonalités sont produites localement et fournies du côté origine. Le côté destination peut chercher à émettre des tonalités et annonces produites dans la bande, par exemple lorsque l'extrémité de destination est une passerelle vers un réseau analogique. Afin de demander au côté origine de ne pas produire localement de tonalités telles que le retour d'appel ou l'occupation, le côté destination doit ouvrir la voie média en répondant à la demande de connexion rapide et en envoyant un élément d'information *Indicateur de progression* contenant le descripteur d'avancement n° 1, *Appel non RNIS de bout en bout; d'autres informations de progression d'appel peuvent être disponibles dans la bande* ou n° 8, *Informations dans la bande ou structure appropriée maintenant disponible*, inséré dans un message Call Proceeding, Progress ou Alerting ou dans un message Connect si un message Alerting n'a pas été envoyé. La réponse au message Connect rapide doit être émise avant ou dès l'envoi de l'indicateur de progression (c'est-à-dire jusques et y compris l'envoi du même message d'indicateur de progression). Le côté destination peut fournir des tonalités ou annonces dans la bande (telles que les signaux de retour d'appel et d'occupation) dès que le descripteur de progression a été envoyé et que la voie média a été ouverte. Noter que l'indicateur de progression ne doit figurer dans un message Alerting que si l'extrémité doit recevoir une alerte. Si une autre tonalité (comme un signal d'occupation ou de recomposition) est fournie dans la bande, l'indicateur de progression ne doit pas être contenu dans un message Alerting. Si aucun message approprié d'établissement d'appel n'est disponible, un message Progress peut être utilisé pour transporter l'indicateur de progression.

NOTE – Lorsqu'une extrémité ou un portier intervenant dans la signalisation d'un appel reçoit un élément d'information *Indicateur de progression* contenu dans un message Call Proceeding, cette extrémité ou ce portier ne sera pas en mesure de retransmettre ce message si celui-ci a déjà été envoyé au côté origine. Dans ce cas, l'élément d'information *Indicateur de progression* contenu dans le message Call Proceeding doit être appliqué sur l'élément d'information *Indicateur de progression* d'un message Progress.

Si le côté destination ne souhaite pas à fournir de tonalités et annonces distantes, il ne doit pas envoyer l'élément d'information *Indicateur de progression* contenant le descripteur de progression n° 1 ou n° 8. Le message Alerting doit être envoyé pour indiquer au côté origine que l'alerte produite localement doit être appliquée.

Dès réception d'un message Alerting, le côté origine doit fournir des tonalités et annonces produites localement à moins que les conditions suivantes ne soient vérifiées:

1) une voie média est disponible pour "l'écoute". L'élément **fastStart** peut avoir été reçu dans tous message jusques et y compris le message Alerting;

2) un élément d'information *Indicateur de progression* contenant le descripteur de progression n° 1, *Appel non RNIS de bout en bout; d'autres informations de progression d'appel peuvent être disponibles dans la bande* ou n° 8, *Informations dans la bande ou structure appropriée maintenant disponible*, a été reçu dans un message quelconque jusques et y compris le message Alerting.

Dès réception d'un message Release Complete y compris un élément d'information Cause, le côté origine doit produire une tonalité ou fournir une indication appropriée à la valeur de cause reçue.

Par exemple, si la valeur de cause n° 17, *Usager occupé*, est reçue, le côté origine doit produire la tonalité d'occupation ou fournir une indication d'usager occupé.

Lorsque des tonalités et annonces produites localement sont utilisées, l'élément d'information Signal peut facultativement être également présent afin de donner plus d'informations sur le type de signal à fournir.

8.1.8 Etablissement de communications par l'intermédiaire de passerelles

8.1.8.1 Etablissement d'une communication arrivant dans la passerelle

Lorsqu'un terminal extérieur appelle une extrémité de réseau par l'intermédiaire de la passerelle, la procédure d'établissement de la communication entre la passerelle et l'extrémité du réseau est identique à la procédure d'établissement d'une communication entre deux extrémités. La passerelle peut devoir émettre un message Call Proceeding à destination du terminal extérieur tout en établissant la communication sur le réseau.

Une passerelle qui ne peut pas acheminer directement un appel du RCC entrant à destination d'une extrémité H.323 doit pouvoir accepter la numérotation en deux étapes. Pour les passerelles conformes aux réseaux H.320 (ainsi que H.321, H.322 et H.310 en mode H.321), la passerelle doit accepter les numéros d'extension SBE provenant du terminal H.320. Facultativement, les passerelles allant aux réseaux H.320 peuvent prendre en charge les codes TCS-4 et IIS BAS pour récupérer l'information de numérotation H.323 après l'établissement de l'appel H.320. Lorsqu'elle est conforme au mode naturel H.310 et aux réseaux H.324, la passerelle doit accepter les messages d'indication de données d'usager **userInputIndication** de la Rec. UIT-T H.245 provenant du terminal H.324. Dans ces deux cas, la prise en charge des multifréquences bitonalités (DTMF, *dual-tone multifrequency*) est facultative. Lorsqu'elle est conforme aux extrémités ne fonctionnant qu'en mode téléphonique, la passerelle doit accepter les numéros DTMF provenant du terminal ne fonctionnant qu'en mode téléphonique. Ces numéros indiqueront le numéro à composer dans une seconde étape pour accéder à l'extrémité considéré du réseau.

8.1.8.2 Etablissement d'une communication sortant de la passerelle

Lorsqu'une extrémité de réseau appelle un terminal extérieur par l'intermédiaire de la passerelle, la procédure d'établissement de la communication entre l'extrémité du réseau et la passerelle est identique à la procédure d'établissement d'une communication entre extrémités. La passerelle recevra le champ **dialledDigits** ou **partyNumber** de destination (**e164Number** ou **privateNumber**) dans le message Setup. Elle utilisera alors cette adresse pour faire un appel vers l'extérieur. La passerelle peut émettre des messages d'appel en cours à destination de l'extrémité du réseau tout en établissant la communication avec l'extérieur.

Il y a lieu qu'une passerelle envoie un message Call Proceeding dès qu'elle reçoit le message Setup (ou le message ACF) si elle prévoit une durée supérieure à 4 secondes avant de pouvoir répondre par un message Alerting, Connect ou Release Complete.

L'élément d'information Indicateur de progression indique qu'il y a interconnexion de réseaux. La passerelle doit émettre un élément d'information Indicateur de progression dans les messages Alerting, Call Proceeding ou Connect. Cette information peut aussi être envoyée dans un message Progress.

L'extrémité d'un réseau doit envoyer toutes les adresses de type **dialledDigits** ou **partyNumber** qu'il appelle dans le message Setup. Par exemple, un appel à six correspondants sur le canal B du RNIS nécessitera six adresses de type **dialledDigits** ou **partyNumber** dans le message Setup. La passerelle doit répondre au message Setup par un message Connect ou Release Complete ainsi que par des messages Alerting, Call Proceeding ou Progress. L'échec de l'appel sur le RCC doit être signalé à l'extrémité du réseau dans le message Release Complete. L'utilisation de plusieurs valeurs

CRV et de plusieurs messages Setup appelle un complément d'étude. L'adjonction de voies sur le RCC au cours d'un appel appelle un complément d'étude.

Une extrémité de réseau qui est enregistrée auprès d'un portier devrait demander, dans le message de demande ARQ, une largeur de bande d'appel suffisante pour l'ensemble de tous les appels sur le RCC. Si une largeur de bande d'appel suffisante n'a pas été demandée dans le message de demande ARQ, des procédures de modification de largeur de bande décrites au § 8.4.1 doivent être appliquées afin d'obtenir une largeur de bande d'appel supplémentaire.

La passerelle peut passer à la phase B après avoir effectué son premier appel sur le RCC. D'autres appels correspondant aux autres numéros de type **dialledDigits** ou **partyNumber** du RCC peuvent être effectués après l'échange des capacités avec la passerelle et l'établissement de communications audio avec l'extrémité du RCC.

8.1.9 Etablissement de la communication avec un pont de conférence

Dans le cas de conférences multipoint centralisées, toutes les extrémités échangent la signalisation d'appel avec le pont de conférence. La procédure d'établissement de la communication entre une extrémité et le pont de conférence est identique à la procédure d'établissement d'une communication entre deux extrémités mise en œuvre dans les scénarios décrits aux § 8.1.1 à 8.1.5. Le pont de conférence peut être l'extrémité appelée ou l'extrémité appelante.

Dans une conférence multipoint centralisée, la voie de commande H.245 est ouverte entre les extrémités et le contrôleur multipoint incorporé dans le pont de conférence. Les voies audio, vidéo et de données sont ouvertes entre les extrémités et le processeur multipoint incorporé dans le pont de conférence. Dans une conférence multipoint décentralisée, la voie de commande H.245 est ouverte entre l'extrémité et le contrôleur multipoint (il peut y avoir de nombreuses voies de commande H.245, une pour chaque appel). Les voies audio et vidéo doivent être multidiffusées à destination de toutes les extrémités participant à la conférence. Le canal de données doit être ouvert avec le processeur multipoint de données.

Dans une conférence multipoint ad hoc dont les extrémités ne contiennent pas de contrôleur multipoint et dont le portier souhaite fournir aux extrémités un service multipoint ad hoc, la voie de commande H.245 peut être acheminée par ce portier. Dans un premier temps, la voie de commande H.245 établie entre les extrémités passera par le portier. Au moment où la conférence passe au mode multipoint, le portier peut connecter les extrémités à un contrôleur multipoint qui lui est associé.

Dans une conférence multipoint ad hoc où l'une des extrémités, ou les deux, incorporent un contrôleur multipoint, les procédures normales d'établissement de la communication définies aux § 8.1.1 à 8.1.5 sont utilisées. Ces procédures peuvent s'appliquer même si une extrémité qui contient un contrôleur multipoint est en fait un pont de conférence. La procédure de choix du mode maître ou esclave est utilisée pour déterminer quel sera le contrôleur multipoint activé pour la conférence.

8.1.10 Renvoi d'appel

Une extrémité qui souhaite transférer ou renvoyer un appel à une autre extrémité peut émettre un message Facility indiquant l'adresse de la nouvelle extrémité. L'extrémité qui reçoit cette indication de fonctionnalité devrait envoyer un message Release Complete et réengager les procédures de la phase A avec la nouvelle extrémité.

8.1.11 Etablissement d'une communication en diffusion

L'établissement d'une communication pour des conférences (débat) en mode diffusion doit suivre les procédures définies dans la Rec. UIT-T H.332.

8.1.12 Numérotation en chevauchement

Les entités H.323 peuvent, facultativement, prendre en charge la numérotation avec chevauchement. Si un portier est présent lors de l'utilisation de la numérotation avec chevauchement, il y a lieu que les extrémités envoient un message ARQ à ce portier chaque fois qu'une nouvelle information d'adressage est introduite. L'extrémité doit insérer toutes les informations d'adressage cumulatif dans le champ **destinationInfo**, à chaque envoi d'un message de demande ARQ. Si celui-ci ne contient pas suffisamment d'informations d'adressage, il convient que le portier répondre par un rejet ARJ avec **reason** mis à **incompleteAddress**. Cela indiquera que l'extrémité devra envoyer une autre demande ARQ lorsqu'il disposera de plus amples informations d'adressage. Si un portier dispose d'informations d'adressage suffisantes pour attribuer une adresse **destCallSignalAddress** appropriée, il doit renvoyer une confirmation ACF. Noter que cela n'implique pas forcément que l'information d'adressage soit complète. Si le portier envoie un rejet ARJ avec la raison **AdmissionRejectReason** à une valeur autre que **incompleteAddress**, le processus d'établissement d'appel doit être abandonné.

Lorsqu'une extrémité possède une adresse **destCallSignalAddress** appropriée, elle doit envoyer un message Setup dont le champ **canOverlapSend** est validé de façon à indiquer s'il possède la capacité de prendre en charge les procédures de numérotation avec chevauchement. Si une entité distante reçoit un message Setup avec une adresse incomplète et que le champ **canOverlapSend** soit mis à la valeur "TRUE", il convient que cette entité engage les procédures de numérotation par chevauchement en renvoyant le message Setup Acknowledge. Les informations d'adressage additionnel devront être insérées dans des messages de type Information. Si une entité distante reçoit un message Setup avec une adresse incomplète et que le champ **canOverlapSend** soit mis à la valeur "FALSE", il convient que cette entité envoie le message Release Complete. Noter que les passerelles ne devraient pas transférer les messages Setup Acknowledge du RCC vers des extrémités H.323 n'ayant pas signalé leur capacité de prise en charge des procédures de numérotation par chevauchement car le résultat souhaité pourrait ne pas être obtenu.

8.1.13 Etablissement d'un appel vers des conférences pseudonymes

Les adresses de pseudonymes (voir § 7.1.3) peuvent être utilisées pour représenter une conférence à un contrôleur multipoint. Les procédures des paragraphes précédents sont applicables, à l'exception de ce qui est noté ci-après.

8.1.13.1 Entrée dans une conférence de pseudonymes, sans portier

L'extrémité 1 (appelante) envoie le message Setup (1) (voir Figure 29) à l'identificateur notoire de point TSAP d'accès à la voie de signalisation d'appel de l'extrémité 2 (le contrôleur multipoint). Ce message Setup comporte les champs suivants:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = adresse de transport du MC(U)
conferenceID                = 0 (car le CID est inconnu)
conferenceGoal              = entrée (jonction)
```

L'extrémité 2 répond par le message Connect (4) qui contient les champs:

```
h245Address                 = adresse de transport pour signalisation H.245
conferenceID                = CID pour la conférence
```

8.1.13.2 Entrée dans une conférence de pseudonymes, avec portier

L'extrémité 1 (appelante) engage le dialogue ARQ (1)/ACF (2) (voir Figure 30) avec le portier. La demande ARQ contient les champs suivants:

```
destinationInfo             = conferenceAlias
callIdentifier              = valeur N quelconque
conferenceID                = 0 (car le CID est inconnu)
```

Le portier doit renvoyer, dans la confirmation ACF, l'adresse de transport pour la voie de signalisation d'appel de l'extrémité 2 (appelée et contenant le contrôleur multipoint). L'extrémité 1 envoie ensuite à l'extrémité 2 le message Setup (3) en utilisant l'adresse de transport et les champs suivants:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = adresse fournie par le message ACF
conferenceID                = 0
conferenceGoal              = entrée
```

Finalement, l'extrémité 2 renvoie un message Connect avec les champs suivants:

```
h245Address                 = adresse de transport pour signalisation H.245
conferenceID                = CID pour la conférence
```

L'extrémité 1 complète l'appel en indiquant à son portier l'identificateur CID correct. L'extrémité 1 envoie une demande IRR au portier avec les champs suivants:

```
callIdentifier              = même valeur N que dans la première ARQ
conferenceID                = CID original issu de l'extrémité 1
substituteConferenceIDs     = CID issu de l'extrémité 2
```

8.1.13.3 Création ou invitation avec pseudonyme de conférence

L'extrémité 1 (appelante) peut envoyer à l'extrémité 2 un message Setup contenant les champs suivants:

```
destinationAddress          = conferenceAlias
destCallSignalAddress       = adresse de transport du MC(U)
conferenceID                = CID de la conférence
conferenceGoal              = création ou invitation
```

L'extrémité 2 répond par le message Connect, qui contient:

```
h245Address                 = adresse du transport pour signalisation H.245
conferenceID                = CID pour la conférence
```

8.1.13.4 Dispositions pour les extrémités selon la version 1

Lorsqu'une entité H.323 (extrémité ou pont de conférence) reçoit un message Setup issu d'une entité selon la version 1 et que **destinationAddress** correspond à un de ses pseudonymes de conférence, cette entité ne doit pas tenir compte de **conferenceGoal** et traiter la demande d'établissement comme une demande d'entrée par jonction.

Lorsqu'un portier reçoit une demande ARQ issue d'une entité selon la version 1 et que **destinationInfo** correspond à l'un de ses pseudonymes de conférence, ce portier ne doit pas tenir compte du champ **conferenceID**. De même, lorsqu'une entité H.323 reçoit un message Setup issu

d'une entité selon la version 1 et que **destinationAddress** correspond à l'un de ses pseudonymes de conférence, cette entité ne doit pas tenir compte du champ **conferenceID**.

Ces dispositions permettent à une extrémité selon la version 1 d'appeler un pseudonyme de conférence.

8.1.14 Modification par portier d'adresses de destination

Une extrémité doit mettre le champ **canMapAlias** à la valeur "TRUE" pour indiquer sa capacité d'accepter des informations de destination modifiées en provenance d'un portier. L'extrémité doit utiliser les informations de destination renvoyées dans un message ACF ou LCF au lieu des informations de destination transmises dans le message ARQ ou LRQ. Pour une passerelle d'entrée, les informations de destination qui apparaissent dans le message ACF seront utilisées dans le message Setup qui est envoyé dans le réseau en mode paquet. Pour une passerelle de sortie, les informations de destination qui apparaissent dans le message ACF seront utilisées pour atteindre une destination située dans le RTPC (insérées par exemple dans le message Setup envoyé au RNIS).

En cas de routage par le portier, celui-ci peut modifier les adresses de destination dans le message Setup qu'il reçoit avant d'émettre un message Setup correspondant.

NOTE – Les systèmes H.323 antérieurs à la version 4 n'étaient pas requis de mettre le champ **canMapAlias** à la valeur "TRUE".

8.1.15 Indications des protocoles souhaités

Lorsqu'une extrémité établit un appel, elle peut indiquer, dans le champ **desiredProtocols** de divers messages H.225.0, les protocoles qu'elle souhaite utiliser au cours d'une communication, comme télécopie, H.320, T.120, etc. Si l'extrémité fournit à son portier une liste de protocoles souhaités ou si une entité envoie un message LRQ à un portier avec une liste de protocoles souhaités, le portier doit tenter de localiser une extrémité pouvant offrir la prise en charge des protocoles souhaités. Si le portier ne trouve aucune extrémité prenant en charge les protocoles souhaités, il doit tout de même résoudre l'adresse de façon que l'appel puisse progresser.

L'extrémité appelante peut examiner le champ **EndpointType** de l'extrémité de destination afin de déterminer exactement les protocoles conservés par l'extrémité distante.

8.1.16 Tonalités et annonces demandées par le portier

Un portier peut demander à une passerelle de restituer une tonalité ou une annonce pour divers événements d'appel qui peuvent être des "événements de précommunication" (se produisant avant que la passerelle terminale soit signalée, comme l'invitation faite à l'appelant à insérer un numéro de destination ou un code comptable), des "événements de mi-communication" (se produisant au milieu d'une communication comme l'envoi d'une annonce avertissant les correspondants d'une communication que celle-ci va se terminer dans quelques minutes), ou des "événements de fin de communication" (se produisant à la fin de la communication, comme un message de clôture de communication). De toute façon, le portier peut utiliser un champ **H248SignalsDescriptor** afin de décrire l'invitation que la passerelle doit utiliser.

Les événements de précommunication suivants sont pris en charge:

- invitation à insérer une destination – Au cours de la phase qui est souvent appelée *numérotation en deux temps*, l'appelant compose un certain numéro pour atteindre la passerelle puis est invité à composer le véritable numéro de destination. Bien qu'une passerelle puisse avoir comme politique générale de toujours fournir l'invitation, il peut être logique, dans certaines circonstances, de permettre à la passerelle de consulter le portier. Cette opération de "consultation" est constituée simplement par une demande ARQ contenant le numéro appelé dans le champ **destinationInfo**. Si le portier décide qu'un vrai numéro de destination est requis, il peut demander à la passerelle d'inviter l'appelant à l'introduire, de recueillir les chiffres additionnels et de le consulter avec le champ de

destination. Le portier utilise le message ARJ avec un élément **serviceControl** et une valeur **collectDestination** du champ **AdmissionRejectReason**. L'élément **serviceControl** possède un descripteur **ServiceControlDescriptor** de type **signal** (qui contient le descripteur **H248SignalsDescriptor**) et une valeur **open** du champ **reason**. La valeur **collectDestination** du champ **AdmissionRejectReason** demande à la passerelle de placer la vraie destination recueillie dans le champ **destinationInfo** d'une nouvelle demande ARQ.

- Invitation à insérer un code d'autorisation, un code comptable ou un code personnel d'identification – Dans ce cas, le portier répond à la demande ARQ par un rejet ARJ contenant un élément **serviceControl** et une valeur **collectPIN** du champ **AdmissionRejectReason**. L'élément **serviceControl** possède un descripteur **ServiceControlDescriptor** de type **signal** (qui contient le descripteur **H248SignalsDescriptor**) et une valeur **open** du champ **reason**. La valeur **collectPIN** du champ **AdmissionRejectReason** demande à la passerelle de placer le code personnel d'identification (ou le code d'autorisation ou le code comptable) recueilli dans un jeton ou dans le champ **cryptoToken** d'une nouvelle demande ARQ.
- Invitation à insérer à la fois une destination et un code personnel d'identification – Il s'agit d'un simple opération de mise en série des deux cas précédents.
- Rejet d'un appel – Un portier peut choisir le rejet d'un appel mais doit fournir à l'usager une certaine information en retour (par exemple en fournissant une tonalité ou annonce d'occupation du réseau s'il n'y a pas de ressources disponibles pour une destination). Dans ce cas, la demande ARJ contiendra un champ **AdmissionRejectReason** reflétant la situation mais sans valeur **collectPIN** ou **collectDestination**.

Un portier peut lancer un signal de mi-communication au moyen du message d'indication SCI. L'élément **serviceControl** a un descripteur **ServiceControlDescriptor** de type **signal** (qui contient le descripteur **H248SignalsDescriptor**) et une valeur **open** du champ **reason**. Le signal peut être interrompu par l'envoi du message **ServiceControlIndication** mais avec un descripteur **ServiceControlDescriptor** contenant la valeur **close** du champ **reason**. Une passerelle doit normalement répondre au message d'indication SCI par une réponse SCR contenant un champ **result** approprié.

Un portier peut lancer un signal de fin de communication dans une demande DRQ (pour le cas d'un routage direct d'extrémité) ou dans un message Release Complete (pour le cas d'un routage par portier) contenant un élément **serviceControl** ayant un descripteur **ServiceControlDescriptor** de type **signal** (qui contient le descripteur **H248SignalsDescriptor**) et une valeur **open** du champ **reason**. Le signal peut être interrompu par l'envoi du message **ServiceControlIndication** mais avec un descripteur **ServiceControlDescriptor** contenant la valeur **close** du champ **reason**.

8.2 Phase B – Communication initiale et échange des capacités

Une fois que les deux extrémités ont échangé les messages d'établissement de la communication à l'issue de la phase A, ils doivent, s'ils envisagent de recourir aux procédures H.245, établir la voie de commande H.245. Les procédures de la Rec. UIT-T H.245 sont utilisées sur la voie de commande H.245 pour l'échange des capacités et l'ouverture des voies de médias.

NOTE – A titre facultatif, la voie de commande H.245 peut être établie par l'extrémité appelée après réception du message Setup et par l'extrémité appelante après réception des messages Alerting ou Call Proceeding. Si le message Connect n'arrive pas ou si une extrémité envoie un message Release Complete, il faut fermer la voie de commande H.245.

Les extrémités prendront en charge la procédure d'échange des capacités de la Rec. UIT-T H.245 conformément aux indications données au § 6.2.8.1.

L'échange des capacités du système entre les extrémités est effectué par la transmission du message **terminalCapabilitySet** (ensemble de capacités du terminal) H.245. Ce message de capacités doit

être le premier message H.245 envoyé à moins que l'extrémité n'indique qu'elle comprend le champ **parallelH245Control** (voir le § 8.2.4). Si une autre procédure échoue (refusée, non comprise, pas prise en charge) avant l'échange réussi des capacités de terminal, l'extrémité initiatrice doit lancer et terminer complètement cet échange avant de tenter une autre procédure. Une extrémité qui reçoit un message **terminalCapabilitySet** d'une homologue avant le lancement de l'échange de capacités doit répondre conformément aux prescriptions données au § 6.2.8.1; elle doit lancer l'échange en question et l'effectuer complètement avec son homologue avant de lancer une autre opération.

Les extrémités doivent prendre en charge la procédure de choix du mode maître ou esclave de la Rec. UIT-T H.245, comme indiqué au § 6.2.8.4. Si les deux extrémités d'une communication font office de contrôleur multipoint, la procédure de choix du mode maître ou esclave est utilisée pour déterminer quel sera le contrôleur multipoint activé pour la conférence. Le contrôleur multipoint activé peut alors envoyer le message **mcLocationIndication** (indication de localisation du contrôleur multipoint). Cette procédure permet également de choisir le mode maître ou esclave pour l'ouverture de canaux de transmission de données bidirectionnels.

Le choix du mode maître-esclave doit être soumis (par l'envoi du message **MasterSlaveDetermination** ou **MasterSlaveDeterminationAck**, selon le cas) dans le premier message H.245 suivant le lancement de l'échange des capacités de terminal.

Si elles échouent, les procédures initiales d'échange des capacités et de choix du mode maître ou esclave devraient être renouvelées au moins à deux autres reprises avant que l'extrémité abandonne la tentative de connexion et qu'elle passe à la phase E.

Après l'aboutissement des prescriptions de la phase B, les extrémités doivent passer directement au mode de fonctionnement souhaité, c'est-à-dire en principe à la phase C.

8.2.1 Encapsulation de messages H.245 dans des messages de signalisation d'appel H.225.0

De façon à conserver les ressources, à synchroniser la commande et la signalisation d'appel et à réduire le temps d'établissement d'appel, il est parfois préférable d'acheminer des messages H.245 à l'intérieur du canal de signalisation d'appel H.225.0 plutôt que d'établir une voie H.245 distincte. Ce procédé, appelé "encapsulation" ou "tunnellisation" de messages H.245, est réalisé par utilisation de l'élément **h245Control** de l'unité **h323-uu-pdu** pour copier dans le canal de signalisation d'appel un message H.245 codé en chaîne d'octets.

Lorsque la fonction de tunnellisation est active, un ou plusieurs messages H.245 peuvent être encapsulés dans tout message de signalisation d'appel H.225.0. Si la tunnellisation est utilisée et qu'il n'y ait pas besoin d'envoyer un message de signalisation d'appel H.225.0 au moment où un message H.245 doit être émis, un message Facility doit être envoyé avec la **reason** mise à **transportedInformation** (à noter que les systèmes H.323 antérieurs à la version 4 utilisaient un message Facility avec le champ **h323-message-body** mis à la valeur **empty**).

Une entité appelante qui est capable et désireuse d'utiliser l'encapsulation H.245 doit mettre l'élément **h245Tunnelling** à la valeur "TRUE" dans le message Setup et dans tout message de signalisation d'appel H.225.0 qu'elle envoie par la suite, tant qu'elle souhaite que la tunnellisation reste active. Une entité appelée qui est capable et désireuse d'utiliser l'encapsulation H.245 doit mettre l'élément **h245Tunnelling** à la valeur "TRUE" dans le premier message de signalisation d'appel H.225.0 envoyé en réponse au message Setup et dans tout message de signalisation d'appel H.225.0 qu'elle envoie par la suite, tant qu'elle souhaite que la tunnellisation reste active. L'entité appelée ne doit pas mettre l'élément **h245Tunnelling** à la valeur "TRUE" dans toute réponse de signalisation d'appel H.225.0 (et la fonction de tunnellisation doit rester inactivée) si cette valeur n'est pas "TRUE" dans le message Setup auquel elle répond. Si l'entité appelée ne sait pas encore si la tunnellisation H.245 pourra être prise en charge, elle doit inclure le fanion **provisionalRespToH245Tunnelling**. Cela peut arriver, par exemple, lorsqu'un portier répond à une entité appelante par un message tel que Call Proceeding avant que l'extrémité appelée réponde au fanion **h245Tunnelling**. Le fanion **provisionalRespToH245Tunnelling** élimine en fait la

signification du fanion **h245Tunnelling** dans un message, de sorte que ce fanion peut être négligé par l'extrémité réceptrice.

Si l'élément **h245Tunnelling** n'est pas mis à la valeur "TRUE" dans un quelconque message de signalisation d'appel H.225.0 qui ne contient pas le fanion **provisionalRespToH245Tunnelling**, la fonction de tunnellisation est désactivée à partir de ce moment pendant la durée de la communication et une connexion H.245 distincte doit être établie si les procédures H.245 sont invoquées.

L'entité appelante peut insérer dans le message Setup des messages H.245 canalisés; elle doit également mettre l'élément **h245Tunnelling** à "TRUE". Si l'entité appelée ne met pas **h245Tunnelling** à "TRUE" et si le fanion **provisionalRespToH245Tunnelling** est absent dans le premier message de signalisation d'appel H.225.0 envoyé en réponse à Setup, l'entité appelante doit en déduire que les messages H.245 qu'elle avait encapsulés dans le message Setup ont été ignorés par l'entité appelée; elle doit alors les répéter, au besoin, une fois que la voie H.245 distincte a été établie. Si elle met l'élément **h245Tunnelling** à "TRUE", l'entité appelée peut également insérer des messages H.245 encapsulés dans le premier message de signalisation d'appel H.225.0 et dans les suivants.

L'extrémité appelante ne doit pas inclure à la fois dans le même message Setup un élément **fastStart** et des messages H.245 encapsulés dans l'élément **h245Control** car la présence des messages H.245 encapsulés outrepassera la procédure de connexion rapide. Une extrémité appelante peut cependant inclure à la fois dans le même message Setup un élément **fastStart** et une valeur "TRUE" de l'élément **h245Tunnelling**; de même, une extrémité appelée peut inclure dans la même réponse de signalisation d'appel H.225.0 un élément **fastStart** et une valeur "TRUE" de l'élément **h245Tunnelling**. Dans ce cas, les procédures de connexion rapide seront suivies et la connexion H.245 restera "non établie" jusqu'à la transmission effective du premier message H.245 canalisé ou jusqu'à l'ouverture de la connexion H.245 distincte.

Lorsque l'encapsulation H.245 est utilisée, les deux extrémités doivent garder ouvert le canal de signalisation d'appel H.225.0, jusqu'à ce que soit la communication soit terminée ou qu'une connexion H.245 distincte soit établie.

Lorsqu'une extrémité reçoit un élément de commande **h245control** dans lequel sont encapsulées plusieurs unités PDU H.245, celles-ci doivent être traitées (c'est-à-dire livrées aux couches supérieures) séquentiellement, par ordre d'écart croissant par rapport au début du message H.225.0.

Les entités conformes à la version 4 et aux versions ultérieures doivent indiquer la prise en charge de la mise en tunnel H.245 tel que décrit dans le présent paragraphe en positionnant le champ **h245Tunnelling** à "TRUE" dans tous les messages contenant ce champ.

8.2.2 Tunnellisation au moyen d'entités sémaphores intermédiaires

Les entités situées dans le trajet de signalisation (comme les portiers) peuvent exécuter des fonctions telles que le transfert sur non-réponse ou d'autres commandes d'appel évoluées dont le résultat consiste à présenter à une extrémité un état d'appel qui est différent de l'état d'appel réel à l'autre extrémité. De telles entités intermédiaires doivent veiller à ce que les messages H.245 encapsulés dans des messages de signalisation d'appel H.225.0 soient renvoyés à l'autre extrémité même si le message de signalisation d'appel H.225.0, qui encapsule le message H.245, doit être consommé sans être renvoyé à l'autre extrémité. A cette fin, le message H.245 encapsulé est transféré dans un message Facility avec **reason** mis à **transportedInformation**. (A noter que les systèmes antérieurs à la version 4 utilisaient ce message Facility avec le champ **h323-message-body** mis à la valeur **empty**.) Par exemple, si un portier a déjà envoyé un message Connect à une extrémité appelante et qu'il reçoive ensuite un message Connect issu d'une extrémité appelée et contenant un message H.245 encapsulé, ce portier doit renvoyer le message H.245 au moyen d'un message Facility.

Les entités se trouvant sur le trajet de signalisation doivent également utiliser le message Facility ou Progress afin que d'éventuelles informations nouvelles (telles que des éléments d'information Q.931, des champs de l'élément d'information CallProceeding-UUIE, des protocoles non H.323 mis en tunnel et des messages H.245 encapsulés) reçues dans un message Call Proceeding puissent être acheminées vers l'autre extrémité si l'entité a déjà envoyé un message Call Proceeding. Cela permettra à cette entité, par exemple, d'émettre l'élément **fastStart** afin de faciliter un établissement correct d'une communication en connexion rapide et/ou afin qu'un indicateur de progression indique la présence de tonalités et annonces dans la bande. Lors de l'utilisation du message Facility afin d'acheminer de telles informations extraites du message Call Proceeding, le champ **reason** du message Facility doit être mis à la valeur **forwardedElements**.

8.2.3 Commutation vers une connexion H.245 distincte

Lorsqu'on utilise la procédure d'encapsulation H.245 ou la procédure de connexion rapide, l'une ou l'autre des extrémités peut choisir de commuter à tout instant vers la connexion H.245 distincte. De façon à faciliter l'ouverture de la connexion H.245 distincte par l'une ou l'autre des extrémités, chacune de celles-ci peut insérer l'adresse H.245 (**h245Address**) dans tout message de signalisation d'appel H.225.0 qu'elle envoie au cours de la communication. Si une extrémité constate, au moment où elle juge nécessaire d'ouvrir la connexion H.245 distincte, qu'elle n'a pas encore reçu l'adresse H.245 de l'autre extrémité, elle doit émettre un message Facility avec une cause **FacilityReason** de commande **startH245** et avec son adresse H.245 fournie dans l'élément **h245Address**. Une extrémité recevant un message Facility avec une cause **facilityReason** de commande **startH245** doit ouvrir la voie H.245 au moyen de l'adresse **h245Address** spécifiée. L'utilisation de la connexion H.245 distincte est lancée par l'ouverture de la connexion du protocole de transport H.245 (TCP) et est acceptée par l'acquittement de cette connexion.

Si la fonction de tunnellisation doit être utilisée, l'extrémité qui ouvre la connexion H.245 distincte ne doit pas envoyer d'autres messages H.245 canalisés dans le canal de signalisation d'appel ni de messages H.245 dans la connexion H.245 distincte avant que l'établissement de la connexion du protocole TCP ait été acquitté. L'extrémité qui acquitte l'ouverture de la connexion H.245 distincte ne doit pas envoyer d'autres messages H.245 canalisés dans le canal de signalisation d'appel après avoir acquitté l'ouverture de la connexion H.245 distincte. Etant donné que des messages H.245 peuvent avoir déjà été envoyés et peuvent être en transit lors de l'ouverture de la voie H.245 distincte, les extrémités doivent continuer à recevoir et à traiter correctement les messages H.245 canalisés, jusqu'à ce qu'elles reçoivent un message de signalisation d'appel H.225.0 dont le fanion **h245Tunnelling** est mis à "FALSE"; les réponses à de tels messages H.245 canalisés "tardivement" (ou les acquittements de tels messages) doivent être expédiés dans la connexion H.245 distincte après son établissement. Une fois qu'une connexion H.245 distincte a été établie, il n'est plus possible de revenir à la fonction de canalisation en tunnel.

Si les deux extrémités ouvrent simultanément la connexion H.245 distincte, l'extrémité dont **h245Address** est numériquement la plus petite doit fermer la connexion de protocole TCP qu'elle avait ouverte et doit utiliser la connexion ouverte par l'autre extrémité. Afin de comparer les valeurs numériques des adresses H.245, chaque octet de l'adresse doit être comparé individuellement au premier octet de la chaîne d'octets, de gauche à droite de cette chaîne jusqu'à ce qu'une inégalité de valeur numérique d'octet soit constatée. La comparaison doit être appliquée d'abord aux éléments d'adresse de couche Réseau du champ **h245Address** puis, si ces éléments sont trouvés égaux, aux éléments d'adresse de couche Transport (port).

8.2.4 Déclenchement d'une tunnellisation H.245 en parallèle à une connexion rapide H.245

Comme expliqué au § 8.2, les deux premiers messages H.245 envoyés par une extrémité dans la voie de commande H.245 sont le message **terminalCapabilitySet** et le message **masterSlaveDetermination**. Même lorsque la procédure de connexion rapide est utilisée, il est avantageux d'échanger ces messages aussi rapidement que possible. En particulier, une entité peut

avoir besoin de savoir dès que possible si le codage DTMF est pris en charge par l'autre entité dans le message **UserInputIndication** ou des types de charge utile RTP (tel que décrit au § 10.5). Par ailleurs, si la procédure de connexion rapide est refusée, il y a des avantages évidents à avoir déjà transmis ces messages car il restera beaucoup moins de messages à échanger pour ouvrir des voies logiques.

Afin d'exécuter l'échange de capacités et l'établissement d'appel global, une entité peut inclure le message H.245 **terminalCapabilitySet** et le message **masterSlaveDetermination** dans le champ **parallelH245Control** du message Setup. Contrairement au champ **h245Control**, l'entité appelante peut envoyer ces messages dans le message Setup en même temps que l'élément **fastStart**. L'entité appelante doit mettre le champ **h245Tunnelling** à la valeur "TRUE" lors de l'insertion du champ **parallelH245Control**.

NOTE – Une entité appelante ne doit pas inclure le champ **parallelH245Control** sans inclure aussi le champ **fastStart** car la tunnellisation H.245 doit, dans le cadre d'une communication qui n'utilise pas les procédures de connexion rapide, être traitée conformément au § 8.2.1.

Pour indiquer que l'entité appelée interprète correctement le champ **parallelH245Control**, le premier message H.245 que l'entité appelée envoie doit être le message **terminalCapabilitySetAck** mis en tunnel dans la voie de signalisation d'appel H.225.0. Il y a lieu que ce message de réponse soit envoyé par l'entité appelée en même temps que l'élément **fastConnectRefused** ou **fastStart** est envoyé à l'entité appelante. A noter que si une extrémité n'indique pas qu'elle comprend le champ **parallelH245Control**, elle doit se conformer au § 8.2 et envoyer l'élément **terminalCapabilitySet** et non pas l'élément **terminalCapabilitySetAck** comme premier message H.245. L'entité appelée doit mettre le champ **h245Tunnelling** à la valeur "TRUE" s'il interprète correctement le champ **parallelH245Control**. La Figure 41 montre les échanges de messages d'une communication à connexion rapide entre deux extrémités qui interprètent correctement le champ **parallelH245Control**.

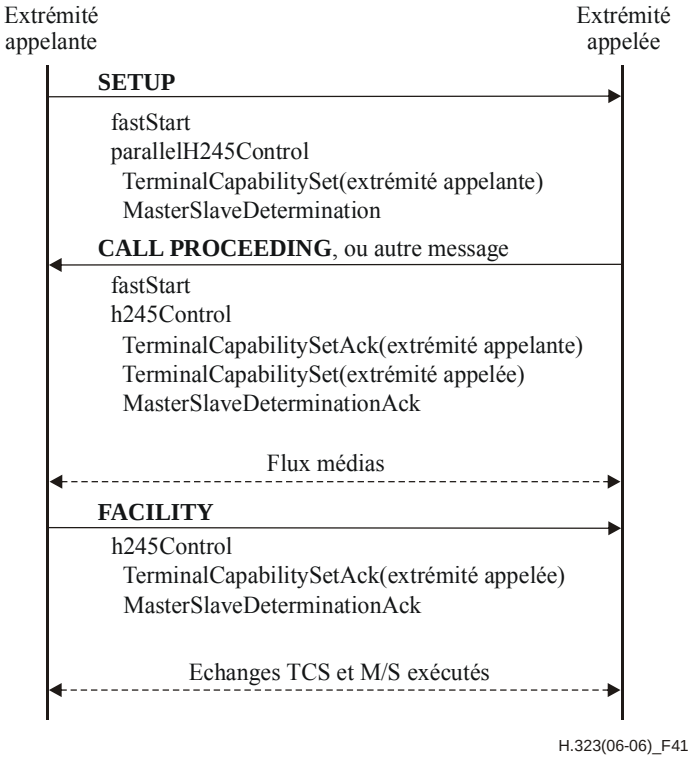


Figure 41/H.323 – Initiation d'une mise en tunnel H.245 en parallèle – Sans échec

L'entité appelante doit reconnaître que le champ **parallelH245Control** n'a pas été compris lorsque soit elle reçoit un message Connect et n'a pas encore reçu de réponse au message **terminalCapabilitySet** initial, soit le premier message H.245 reçu de l'entité appelée n'est pas un message **terminalCapabilitySetAck** mis en tunnel, ou l'élément **fastStart** ou **fastConnectRefused** est reçu et aucune réponse n'a été reçue pour le message **terminalCapabilitySet**. La Figure 42 montre un échange de messages entre une extrémité qui envoie le champ **parallelH245Control** et une extrémité appelée qui n'interprète pas ce champ.

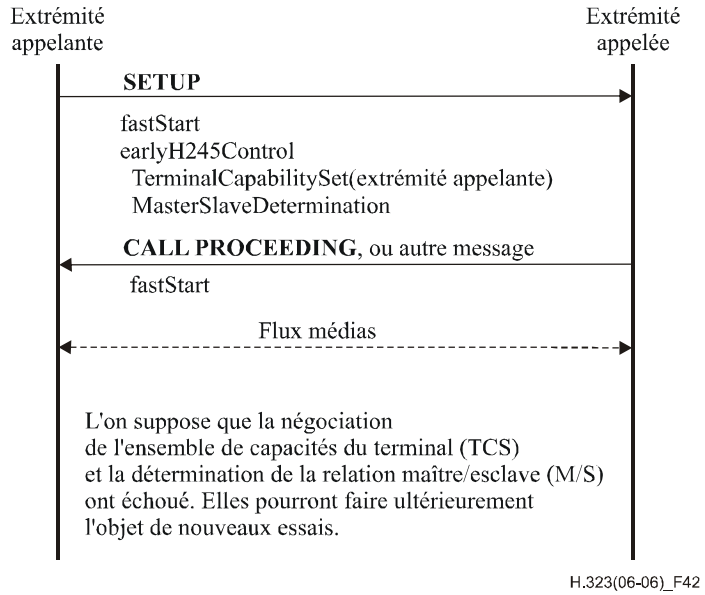


Figure 42/H.323 – Initiation d'une mise en tunnel H.245 en parallèle – Avec échec

8.3 Phase C – Etablissement d'une communication audiovisuelle

Après l'échange des capacités et le choix du mode maître ou esclave, les procédures de la Rec. UIT-T H.245 doivent être utilisées pour ouvrir des voies logiques pour les divers flux d'information. Les flux de signaux audio et vidéo, qui sont transmis dans la configuration de voies logiques présentée dans la Rec. UIT-T H.245, sont transportés sur les identificateurs de point TSAP dynamiques au moyen d'un protocole non fiable (voir Rec. UIT-T H.225.0). Les communications de données qui sont transmises dans la configuration de voies logiques présentée dans la Rec. UIT-T H.245, sont transportées au moyen d'un protocole fiable (voir Rec. UIT-T H.225.0).

Le message d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck** renvoie, ou les paramètres **reverseLogicalChannelParameters** de la demande **openLogicalChannel** contiennent, l'adresse de transport que l'extrémité réceptrice a assigné à cette voie logique. La voie d'émission doit alors envoyer le flux d'information associé à cette voie logique à cette adresse de transport.

Après l'ouverture de voies logiques pour les signaux audio et vidéo, l'émetteur doit envoyer un message d'indication de décalage temporel maximal H.225.0 **h2250MaximumSkewIndication** pour chaque paire audio et vidéo associée.

8.3.1 Changement de mode

Durant une session, les procédures de changement de la structure, de la capacité, du mode de réception, etc. des voies doivent être implémentées comme indiqué dans la Rec. UIT-T H.245, dont l'Appendice V/H.245 contient une procédure de modification des modes sur voie logique qui peut minimiser l'interruption des données audio.

8.3.2 Echange des signaux vidéo par accord mutuel

L'indication **videoIndicateReadyToActivate** (indication vidéo prête à être activée) est définie dans la Rec. UIT-T H.245. Son utilisation est facultative, mais lorsqu'elle est utilisée, la procédure appliquée doit être la suivante.

L'extrémité 1 a été réglée de manière que la vidéo ne soit pas transmise sauf si l'extrémité 2 a également indiqué qu'il était prêt à transmettre la vidéo ou jusqu'à ce qu'il donne cette indication. L'extrémité 1 doit envoyer l'indication **videoIndicateReadyToActivate** à l'issue de l'échange initial des capacités, mais ne doit transmettre aucun signal vidéo avant d'avoir reçu l'indication **videoIndicateReadyToActivate** ou un signal vidéo entrant en provenance de l'extrémité 2.

Une extrémité qui n'a pas été réglée de cette manière facultative n'est pas obligé d'attendre d'avoir reçu l'indication **videoIndicateReadyToActivate** ou un signal vidéo avant de lancer sa transmission vidéo.

8.3.3 Transmission des adresses pour les flux de médias

En monodiffusion, l'extrémité doit ouvrir des voies logiques vers le pont de conférence ou vers une autre extrémité. Les adresses sont transmises dans les messages d'ouverture de voie logique **openLogicalChannel** et d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck**.

En multidiffusion, les adresses de multidiffusion sont assignées par le contrôleur multipoint et transmises aux extrémités dans le message de commande de mode de communication **communicationModeCommand**. Il appartient au contrôleur multipoint d'attribuer et d'assigner des adresses de multidiffusion uniques. L'extrémité doit signaler une commande **openLogicalChannel** au contrôleur multipoint avec l'adresse de multidiffusion assignée. Le contrôleur multipoint doit renvoyer le message **openLogicalChannel** à chaque extrémité réceptrice. Lorsque les médias issus de plusieurs extrémités sont transmis en une seule session (par exemple avec une seule adresse de multidiffusion), le contrôleur multipoint doit ouvrir une voie logique vers chaque extrémité recevant des flux médias issus d'une extrémité de la conférence.

Lorsqu'une extrémité entre dans une conférence après émission de la commande initiale de mode de communication (**communicationModeCommand**), il appartient au contrôleur multipoint d'envoyer une telle commande mise à jour à la nouvelle extrémité et d'ouvrir les voies logiques appropriées pour les médias issus de la nouvelle extrémité. Si une extrémité quitte la conférence après émission de la commande initiale de mode de communication, il appartient au contrôleur multipoint de fermer les voies logiques appropriées qui provenaient de l'extrémité ayant quitté la conférence.

En multimonodiffusion, l'extrémité doit ouvrir des voies logiques vers chacune des autres extrémités. Le message **openLogicalChannel** envoyé au contrôleur multipoint doit contenir le numéro de terminal de l'extrémité pour laquelle la voie est prévue. L'extrémité peut faire correspondre un message **openLogicalChannelAck** grâce au numéro **forwardLogicalChannelNumber**.

8.3.4 Corrélation des flux médias dans les conférences multipoints

La méthode suivante doit être utilisée pour associer une voie logique à un flux de protocole RTP dans le cadre d'une conférence multipoint. L'extrémité duquel provient le flux média envoie le message **openLogicalChannel** au contrôleur multipoint. Lorsque la source souhaite indiquer une destination pour le message **openLogicalChannel**, l'extrémité émettrice doit placer l'étiquette de terminal (**terminalLabel**) de l'extrémité de destination dans le champ **destination** des paramètres de voie logique H.225.0 (**h2250LogicalChannelParameters**). L'extrémité émettrice doit également placer sa propre étiquette de terminal **terminalLabel** dans le champ **source** des paramètres de voie logique H.225.0 (**h2250LogicalChannelParameters**). Noter que, dans le modèle de multidiffusion, l'absence du champ **destination** indique que le flux est applicable à toutes les extrémités.

Si un contrôleur multipoint a attribué une étiquette de terminal **terminalLabel** à une extrémité émettrice, celle-ci doit utiliser un identificateur SSRC dont l'octet de poids faible est l'octet de poids faible de son étiquette de terminal.

L'extrémité de destination peut associer le numéro de voie logique au flux RTP en comparant le champ **openLogicalChannel.h2250LogicalChannelParameters.source** avec l'octet de poids faible de l'identificateur SSRC contenu dans l'en-tête RTP.

Des collisions entre identificateurs SSRC sont possibles lorsqu'une extrémité H.323 est dans une conférence H.332. L'extrémité qui détecte la collision doit suivre les procédures du protocole RTP pour la résolution des collisions entre identificateurs SSRC.

8.3.5 Procédures de la commande de mode de communication

La commande de mode de communication (**communicationModeCommand**) H.245 est envoyée par un contrôleur multipoint H.323 pour spécifier le mode de communication pour chaque type de média: unidiffusion ou multidiffusion. Cette commande peut provoquer une transition entre une conférence centralisée et une conférence décentralisée. Elle peut donc impliquer la fermeture de toutes les voies logiques existantes et l'ouverture de nouvelles voies.

La commande de mode de communication (**communicationModeCommand**) spécifie toutes les sessions de la conférence. Pour chaque session, les données suivantes sont spécifiées: l'identificateur de session RTP, l'identificateur de session RTP associée si applicable, une étiquette de terminal si applicable, une description de la session, le type de données **dataType** des sessions (par exemple G.711) et une adresse de monodiffusion ou de multidiffusion pour les voies de média et de commande de média, selon ce qui convient pour la configuration et pour le type de la conférence.

La commande de mode de communication (**communicationModeCommand**) transmet les modes d'émission que les extrémités de la conférence vont utiliser au cours de celle-ci. Cette commande ne transmet pas les modes de réception, qui sont spécifiés par les commandes **openLogicalChannel** émises par le contrôleur multipoint vers les extrémités.

L'on part du principe que la commande de mode de communication **communicationModeCommand** définit les modes d'une conférence et qu'elle est donc envoyée après l'indication **multipointConference** qui signale à une extrémité qu'elle doit obéir aux ordres du contrôleur multipoint. Si les extrémités ont reçu une indication **multipointConference**, il y a lieu que ces points attendent une commande de mode de communication **communicationModeCommand** avant d'ouvrir des voies logiques.

Les extrémités qui reçoivent une commande de mode de communication **communicationModeCommand** utilisent le champ **terminalLabel** de chaque entrée de la table des modes de communication pour déterminer si cette entrée convient au traitement prévu pour elle. Les entrées qui ne contiennent pas d'étiquette de terminal (**terminalLabel**) s'appliquent à toutes les extrémités de la conférence. Les entrées qui contiennent des étiquettes de terminal sont des commandes adressées à des extrémités spécifiques, qui correspondent à l'étiquette de terminal (**terminalLabel**) contenue dans ces entrées. Par exemple, lorsque les flux audio issus de toutes les extrémités sont attribués à une seule adresse de multidiffusion (dans la même session), l'entrée de table pour le mode audio, pour l'adresse du flux média et pour l'adresse de commande de média ne contiendra pas d'étiquette de terminal. Lorsque l'entrée de table commande à une extrémité d'envoyer son flux vidéo à une adresse de multidiffusion, le contrôleur multipoint inclut l'étiquette de terminal de cette extrémité.

La commande de mode de communication **communicationModeCommand** peut être utilisée pour commander à des extrémités d'une conférence (ou d'une communication point à point) de modifier leur mode de communication, en indiquant un nouveau mode pour une voie média (**mediaChannel**) déjà utilisée. Elle peut également servir à commander à une extrémité d'envoyer le flux média à une

nouvelle adresse, en indiquant le mode actuellement utilisé mais avec une nouvelle voie média. De même, une extrémité qui reçoit une commande de mode de communication **communicationModeCommand** indiquant le mode actuellement utilisé sans préciser de voie média **mediaChannel** doit fermer la voie appropriée et tenter d'en ouvrir une autre au moyen de la séquence **openLogicalChannel-openLogicalChannelAck**, où le message **openLogicalChannelAck** contient l'adresse à laquelle l'extrémité enverra le flux média.

L'Appendice I donne des exemples d'entrées dans la table de modes de communication **communicationModeTable** pour divers cas.

8.4 Phase D – Services de communication

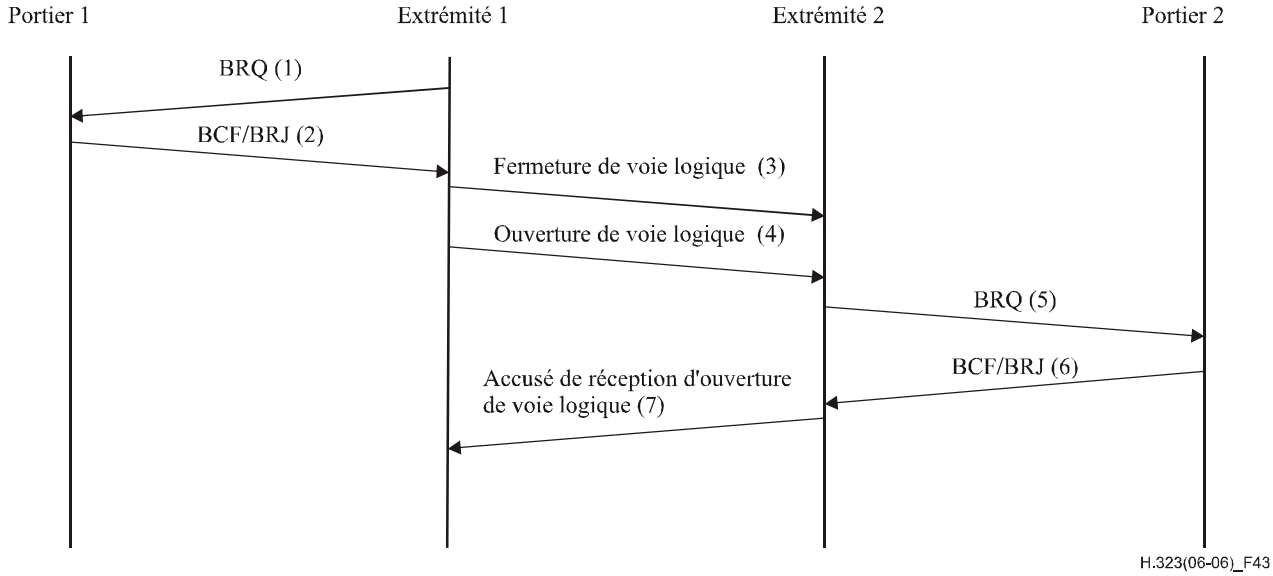
8.4.1 Modifications de la largeur de bande

La largeur de bande d'appel est initialement établie et approuvée par le portier durant l'échange des messages d'admission. Une extrémité doit veiller à ce que l'ensemble des voies audio et vidéo d'émission et de réception – non compris les en-têtes RTP, les en-têtes de charge utile RTP, les en-têtes de réseau et autres préfixes – entre dans cette largeur de bande. Les canaux de données et de commande, qui ne sont pas compris dans cet ensemble, ne sont pas assujettis à cette limite.

A tout moment durant une conférence, les extrémités ou le portier peuvent demander que la largeur de bande d'appel soit augmentée ou réduite. Une extrémité peut modifier le débit d'une voie logique sans demander au portier de modifier la largeur de bande si le débit composite de toutes les voies d'émission et de réception ne dépasse pas la largeur de bande d'appel retenue. Si le débit composite résultant de cette modification dépasse la largeur de bande d'appel retenue, l'extrémité doit demander à son portier de modifier la largeur de bande d'appel et attendre confirmation de cette modification avant de procéder effectivement à un relèvement du débit. Une demande de modification de largeur de bande est recommandée quand une extrémité utilisera une largeur de bande réduite pendant une période prolongée, libérant ainsi une partie de la largeur de bande pour d'autres appels.

Une extrémité qui souhaite modifier sa largeur de bande d'appel envoie au portier un message de demande de largeur de bande (BRQ, *bandwidth change request*) (1). Le portier détermine si cette demande est acceptable. Les critères qu'il retient à cette fin ne relèvent pas de la présente Recommandation. Si le portier estime que la demande n'est pas acceptable, il renvoie à l'extrémité un message de refus de largeur de bande (BRJ, *bandwidth change reject*) (2). S'il estime que la demande est acceptable, le portier renvoie un message de confirmation de largeur de bande (BCF, *bandwidth change confirm*) (2).

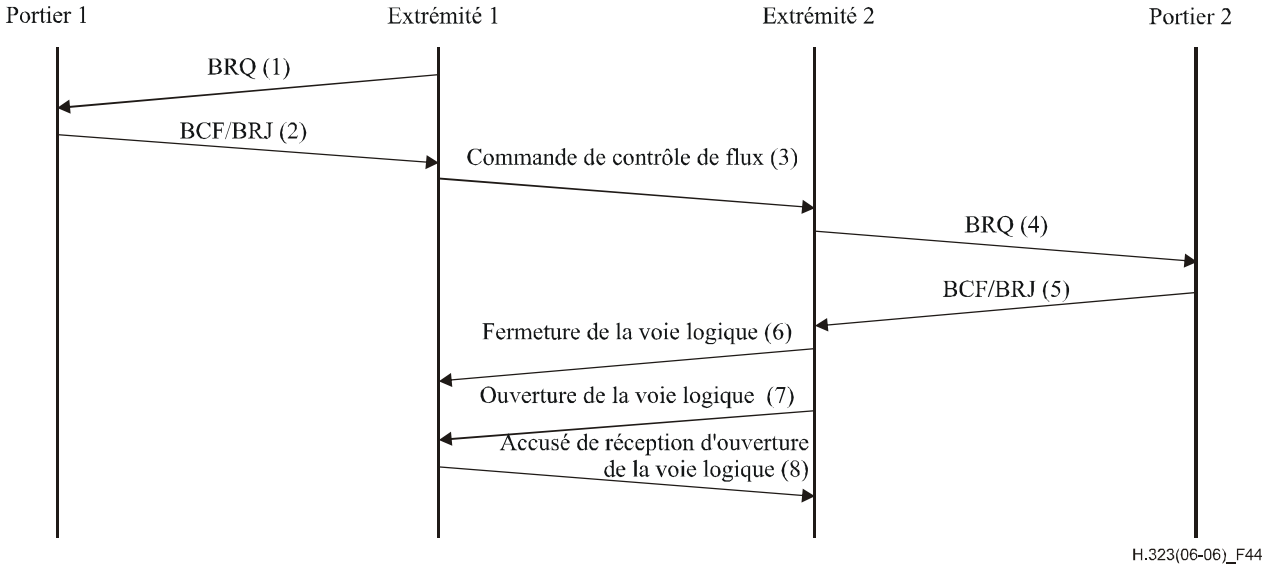
Si elle souhaite augmenter son débit d'émission sur une voie logique, l'extrémité 1 commence par déterminer si la largeur de bande d'appel sera dépassée. Voir Figure 43. Si tel est le cas, l'extrémité 1 doit demander au portier 1 de modifier la largeur de bande (1 et 2). Dans le cas où la largeur de bande d'appel est suffisante pour supporter la modification, l'extrémité 1 envoie un message **closeLogicalChannel** (3) pour fermer la voie logique. Il rouvre ensuite la voie logique à l'aide du message d'ouverture **openLogicalChannel** (4) indiquant le nouveau débit. Si elle souhaite accepter la voie avec le nouveau débit, l'extrémité réceptrice doit d'abord veiller à ce que la modification n'entraîne pas un dépassement de sa largeur de bande d'appel. Si sa largeur de bande est dépassée, l'extrémité doit adresser à son portier une demande de modification de la largeur de bande d'appel (5 et 6). Dans le cas où la largeur de bande d'appel est suffisante pour supporter la voie, l'extrémité répond par un message d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck** (7); dans le cas contraire, il répond par un message de refus d'ouverture de voie logique **openLogicalChannelReject** indiquant que le débit est inacceptable.



NOTE – Le portier 1 et le portier 2 peuvent être le même.

Figure 43/H.323 – Demande de modification de largeur de bande – Changement d'émetteur

Si elle souhaite accroître son débit d'émission sur une voie logique en provenance de l'extrémité 2 sur laquelle elle a précédemment effectué un contrôle de flux pour diminuer le débit, l'extrémité 1 commence par déterminer si la largeur de bande d'appel sera dépassée. Voir la Figure 44. Si tel sera le cas, l'extrémité 1 doit adresser au portier 1 une demande de modification de largeur de bande. Dans le cas où la largeur de bande d'appel est suffisante pour supporter la modification, l'extrémité 1 envoie une commande de contrôle de flux **flowControlCommand** (3) pour indiquer la nouvelle limite supérieure du débit de la voie. Si elle décide d'accroître le débit sur la voie, l'extrémité 2 doit d'abord veiller à ce que la modification n'entraîne pas de dépassement de sa largeur de bande d'appel. En cas de dépassement de sa largeur de bande, l'extrémité 2 doit adresser à son portier une demande de modification de la largeur de bande d'appel (4 et 5). Lorsque la largeur de bande d'appel sera suffisante pour supporter la voie, l'extrémité 2 enverra un message **closeLogicalChannel** (6) pour fermer la voie logique. Elle rouvre ensuite la voie logique au moyen du message d'ouverture de voie logique **openLogicalChannel** (7) indiquant le nouveau débit. L'extrémité 1 devrait alors accepter la voie avec le nouveau débit et répondre par un message d'accusé de réception d'ouverture de voie logique **openLogicalChannelAck** (8).



NOTE – Le portier 1 et le portier 2 peuvent être le même.

Figure 44/H.323 – Demande de modification de largeur de bande – Changement de récepteur

Un portier qui souhaite modifier le débit d'émission de l'extrémité 1 envoie à celle-ci un message de demande BRQ. Si la demande porte sur une réduction du débit et que l'extrémité aie la capacité de prendre en charge le débit demandé, l'extrémité 1 doit s'exécuter en réduisant son débit composite et en renvoyant un message de confirmation BCF. Si l'extrémité 1 ne peut pas prendre en charge le débit demandé, elle peut renvoyer un message BRJ. L'extrémité 1 peut lancer la signalisation H.245 appropriée pour informer l'extrémité 2 de la modification des débits. L'extrémité 2 pourra ainsi informer son portier de la modification. S'il lui est demandé d'accroître le débit, l'extrémité peut accroître son débit au moment voulu et autorisé par le portier.

Si celui-ci souhaite augmenter la largeur de bande utilisée par l'extrémité, celle-ci peut renvoyer un message BCF pour indiquer l'acceptation du nouveau débit plus élevé ou un message BRJ pour indiquer qu'elle rejette la largeur de bande additionnelle. L'extrémité ne doit accepter le débit plus élevé que si elle est disposée à utiliser la largeur de bande additionnelle.

L'extrémité doit envoyer un message BRQ au portier chaque fois que le taux d'utilisation de la largeur de bande tombe au-dessous de la valeur spécifiée dans la demande ARQ initiale ou dans le dernier message BRQ ou BCF. L'extrémité doit également envoyer un message BRQ au portier chaque fois que la signalisation de voie logique se traduit par l'insertion ou par la suppression dans l'extrémité d'un flux multidiffusé unique.

Les informations relatives à la largeur de bande peuvent être utilisées par un portier pour mieux gérer le taux d'utilisation de la largeur de bande dans le réseau. Il convient de noter qu'une gestion précise de la largeur de bande implique que le portier interprète correctement la topologie du réseau, ce qui est hors du domaine d'application de la présente Recommandation. Par ailleurs, le taux d'utilisation de la largeur de bande par l'extrémité peut en fait être différent de celui qui est signalé à cause de l'emploi de la suppression des silences, de codecs à débit variable ou d'autres facteurs. Une extrémité ne doit pas envoyer de messages BRQ répétés à son portier lorsque le taux d'utilisation de la largeur de bande réelle varie en raison de ces facteurs. Il convient au contraire que l'extrémité demande la largeur de bande nécessaire sur la base de l'ensemble des voies logiques ouvertes et qu'elle ne considère pas les périodes de silence ou d'autres facteurs comme une diminution de la largeur de bande.

8.4.2 Indication d'état

Pour déterminer si une extrémité est désactivée ou en dérangement, le portier peut utiliser la séquence de messages de demande d'information (IRQ, *information request*)/de réponse à la demande d'information (IRR, *information request response*) (voir Rec. UIT-T H.225.0) pour interroger les extrémités à un intervalle déterminé par le constructeur. Le portier peut demander des informations sur une communication unique ou sur toutes les communications en cours. Sauf lors de la demande de segments de réponse IRR additionnels, l'intervalle d'interrogation pour obtenir des informations sur une communication particulière ou sur toutes les communications doit être supérieur à 10 secondes. Le portier peut cependant envoyer des messages IRQ contenant des valeurs uniques du champ **callReferenceValue** sans tenir compte de la période d'interrogation. Ce message peut aussi être utilisé par un dispositif de diagnostic, comme indiqué au § 11.2.

Lorsqu'une extrémité émet un message de réponse IRR, elle doit inclure le champ **perCallInfo** afin de donner au portier des détails sur les communications. Si le portier demande l'état de toutes les communications et qu'aucune d'entre elles ne soit active, ou l'état d'une communication unique qui n'est plus active ou pour laquelle l'extrémité ne dispose pas d'informations, l'extrémité doit renvoyer un message IRR comportant le champ **invalidCall** avec omission du champ **perCallInfo** du message IRR.

Si le portier souhaite recevoir des détails sur toutes les communications actives à une extrémité, il peut envoyer un message IRQ dont le champ **callReferenceValue** est mis à 0. Le portier doit normalement inclure le champ **segmentedResponseSupported** afin de permettre des demandes de segmentation, si nécessaire, pour toutes les communications. Si ce champ est inclus, l'extrémité doit renvoyer tout ou partie des informations d'appel dans le champ **perCallInfo** d'un même message IRR. Si la segmentation n'est pas autorisée mais que tous les détails de communication ne peuvent pas être inclus dans le message IRR, l'extrémité doit inclure le champ **incomplete** dans le message IRR. Si la segmentation est autorisée, l'extrémité peut renvoyer un ou plusieurs messages IRR en réponse au message IRQ. Si un message IRR contenant toutes les informations d'appel détaillées est renvoyé, l'élément **irrStatus** ne doit pas être présent. Si la réponse est segmentée en multiples messages IRR, l'extrémité doit envoyer le premier message IRR et inclure le champ **segment**. Si le portier souhaite recevoir le segment suivant, il doit émettre un autre message IRQ comportant le champ **segmentedResponseSupported**, comportant le champ **callReferenceValue** avec la valeur 0, et comportant le champ **nextSegmentRequested** mis à la valeur du prochain segment que le portier s'attend à recevoir. Si le portier souhaite recevoir des segments supplémentaires, il doit envoyer le prochain message IRQ dans les 5 secondes après avoir reçu le message IRR précédent. Si l'extrémité reçoit une demande de segments additionnels après 5 secondes (plus la durée déterminée localement qui correspond au retard dû au réseau), cette extrémité peut renvoyer un message IRR comportant le champ **incomplete**. Lors de la réception d'un message IRQ en provenance du portier pour demander le prochain segment dans la durée impartie, l'extrémité doit émettre le prochain message IRR contenant le prochain segment d'informations d'appel. Noter que si un message IRR est perdu, le portier peut réémettre une demande concernant le segment transmis précédemment. L'extrémité doit donc être en mesure d'émettre le précédent ou prochain segment. Si aucun segment additionnel n'est disponible ou que l'extrémité émette le dernier segment d'une série de messages IRR, cette extrémité doit renvoyer un message IRR comportant le champ **complete**. Le portier ne doit pas transmettre de message IRQ différent à l'extrémité pour demander toutes les informations d'appel détaillées tant que le dernier segment d'information n'a pas été transmis ou tant que la période d'interrogation (10 secondes) ne s'est pas écoulée.

NOTE 1 – Etant donné que les communications peuvent commencer ou finir après l'envoi du premier segment de message IRR en réponse à un message IRQ demandant les détails d'appel pour toutes les communications, l'extrémité a la possibilité d'inclure ou de ne pas inclure de telles communications lors de l'envoi de segments de message IRR subséquents. La décision de signaler de telles communications lors de l'envoi de segments IRR subséquents est laissée au constructeur.

NOTE 2 – Afin d'améliorer la performance et la modularité, un portier devrait limiter la fréquence à laquelle il demande des détails sur toutes les communications. Une telle demande est utile lorsque, par exemple, une extrémité s'enregistre initialement auprès du portier. Toutefois, la répétition d'une telle demande (en particulier à partir de très grandes passerelles ou unités MCU) peut conduire à une détérioration inacceptable de la performance.

Le portier peut souhaiter qu'une extrémité envoie périodiquement un message de réponse IRR spontané. Il peut le faire savoir à l'extrémité en précisant le débit d'émission de ce message de réponse IRR dans le champ **irrFrequency** du message de confirmation d'admission (ACF, *admission confirm*). Une extrémité qui reçoit ce débit **irrFrequency** doit envoyer un message de réponse IRR à ce débit pendant toute la durée de la communication. Tant que ce débit est appliqué, le portier peut toujours envoyer des messages de demande IRQ à l'extrémité, qui doit y répondre comme indiqué ci-dessus.

Une extrémité peut souhaiter que certaines des réponses IRR spontanées soient remises de façon fiable. Le portier peut permettre cela en utilisant le champ **willRespondToIRR** dans le message RCF ou ACF, pour indiquer qu'il peut acquitter des réponses IRR spontanées. Dans ce cas, l'extrémité peut demander explicitement au portier d'accuser réception de la réponse IRR. Le portier doit répondre à un tel message IRR en envoyant soit un accusé de réception positif (IACK, *acknowledgment*) ou un accusé de réception négatif (INAK, *negative acknowledgment*). Si le portier n'a pas annoncé qu'il accusera réception des messages IRR, ou si l'extrémité n'a pas demandé un tel acquittement, aucune réponse ne doit suivre le message IRR.

Pendant toute la durée d'une communication, une extrémité ou un portier peuvent demander périodiquement à une autre extrémité des indications d'état sur la communication. L'extrémité ou le portier à l'origine de cette demande envoient un message de demande d'indication d'état. L'extrémité qui reçoit ce message doit y répondre par un message d'indication d'état indiquant l'état de la communication en cours. Le portier peut recourir à cette procédure pour vérifier périodiquement si une communication est toujours activée. Les extrémités doivent être capables d'accepter toute valeur d'état valide reçue dans le message d'état, y compris les valeurs des états auxquels il n'est peut-être pas capable de passer. Il est à noter que ce message, qui est un message H.225.0 envoyé sur la voie de signalisation d'appel, ne devrait pas être confondu avec le message de réponse IRR qui est un message RAS envoyé sur la voie RAS.

Le portier peut souhaiter recevoir des copies de certaines unités PDU de signalisation d'appel H.225.0 lorsque ces unités sont reçues ou émises par une extrémité. Celle-ci indique sa capacité d'émission de ces unités PDU en activant les éléments d'information **willSupplyUUIEs** dans le message ARQ ou RRQ envoyé au portier. Celui-ci indique, dans le champ **uuiesRequested** du message ACF ou RCF, la liste des types d'unités PDU dont il souhaite recevoir copie. Il indique également s'il souhaite recevoir des copies lorsque les unités PDU sont émises ou reçues. Une extrémité indiquant cette capacité et recevant cette liste doit envoyer une réponse IRR au portier chaque fois qu'elle reçoit ou émet le type d'unité PDU demandé.

8.4.3 Extension d'une conférence ad hoc

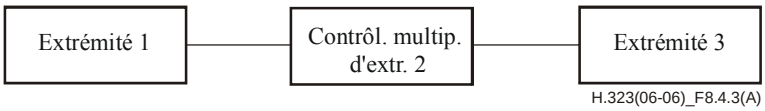
Les procédures suivantes sont facultatives pour les extrémités et les passerelles et obligatoires pour les contrôleurs multipoint.

Lorsqu'un utilisateur établit un appel, l'intention de celui-ci n'est pas souvent connue de l'extrémité appelante. L'utilisateur peut vouloir seulement créer une conférence pour lui-même et pour l'extrémité appelée, se joindre à une conférence organisée par l'entité appelée, ou obtenir une liste des conférences que l'entité appelée peut assurer. Les procédures du présent paragraphe permettent une extension des conférences pour passer de communications point à point à des conférences multipoints ad hoc.

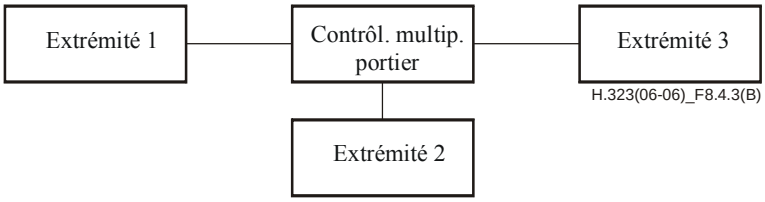
Une conférence multipoint ad hoc est l'extension en conférence multipoint d'une conférence point à point faisant intervenir un contrôleur multipoint. Une conférence point à point est tout d'abord créée

entre deux extrémités (extrémité 1 et extrémité 2). L'une des extrémités au moins ou le portier doit incorporer un contrôleur multipoint. Une fois la conférence point à point créée, celle-ci peut être étendue en conférence multipoint de deux manières différentes. Première manière: l'une des extrémités participant à la conférence invite une autre extrémité (extrémité 3) à y participer en appelant cette extrémité par l'intermédiaire du contrôleur multipoint. Deuxième manière: une extrémité (extrémité 3) entre dans une conférence existante en appelant une extrémité de la conférence.

L'extension d'une conférence ad hoc peut se faire dans le cadre du modèle de signalisation d'appel directe ou du modèle de signalisation d'appel indirecte par l'intermédiaire d'un portier. Pour le modèle de signalisation d'appel directe, la topologie de la voie de commande H.245 se présente comme suit:



Pour le modèle de signalisation d'appel indirecte par l'intermédiaire d'un portier, la topologie de la voie de commande H.245 se présente comme suit:



Dans les deux cas, un contrôleur multipoint doit être présent dans la conférence au moment de l'extension à plus de deux extrémités. Noter que, dans le modèle de signalisation par portier, le contrôleur multipoint peut être situé dans le portier et/ou dans une des extrémités.

Les paragraphes ci-après traitent des procédures qui sont nécessaires pour créer une conférence point à point et pour l'étendre ensuite par des invitations ou des entrées, pour chaque modèle d'appel. Ils traitent également des procédures nécessaires pour permettre à l'extrémité appelante de découvrir la liste des conférences que l'entité appelée peut assurer.

Il convient de noter qu'une défaillance de l'entité faisant fonction de contrôleur multipoint met fin à la communication.

8.4.3.1 Signalisation d'appel directe entre extrémités – Création d'une conférence

L'extrémité 1 crée une conférence avec l'extrémité 2 comme suit:

A1) l'extrémité 1 envoie à l'extrémité 2 un message Setup contenant l'identificateur CID = N mondialement unique et le paramètre **conferenceGoal = create** conformément à la procédure du § 8.1;

A2) l'extrémité 2 opère un choix parmi les options suivantes:

- A2a) si elle souhaite entrer dans la conférence, elle envoie un message Connect avec l'identificateur CID = N à l'extrémité 1. Dans ce cas, soit:
  1) elle ne participe à aucune autre conférence;
  2) elle participe déjà à une autre conférence, elle est capable de participer à plusieurs conférences en même temps et l'identificateur CID = N reçu ne correspond à aucun des identificateurs CID des conférences auxquelles elle participe déjà;

A2b) si elle participe à une autre conférence dont l'identificateur CID vaut M et si elle ne peut participer qu'à une seule conférence à la fois, soit:

1) elle rejette l'appel en envoyant un message Release Complete indiquant qu'elle est déjà en conférence;

2) elle peut demander à l'extrémité 1 d'entrer dans la conférence dont l'identificateur CID vaut M en envoyant un message Facility indiquant **routeCallToMC** (acheminement de l'appel vers le contrôleur multipoint) avec l'adresse de transport de voie de signalisation d'appel associée à l'extrémité incorporant le contrôleur multipoint ainsi qu'avec l'identificateur CID = M de la conférence. Le § 8.4.3.7 décrit le traitement du message Facility à l'extrémité 1;

A2c) si elle ne souhaite pas entrer dans cette conférence, elle rejette l'appel en envoyant un message Release Complete indiquant que la destination est occupée;

A2d) si l'extrémité 2 est un pont MC(U) qui héberge plusieurs conférences et souhaite offrir à l'extrémité 1 la possibilité de participer à un choix de conférences, cette extrémité 2 peut envoyer un message Facility indiquant la structure **conferenceListChoice** ainsi qu'une liste de conférences proposées au choix de l'extrémité 1, envoyée dans l'élément d'information Facility-UUIE. Pour assurer la compatibilité amont avec les extrémités selon la version 1, les listes de conférences ne sont fournies que si le champ **protocolIdentifier**, contenu dans le message Setup de l'extrémité 1, indique qu'il s'agit de la version 2 ou au-dessus.

Dès qu'elle reçoit le message Facility **conferenceListChoice**, l'extrémité 1 peut entrer dans une des conférences de la liste par l'envoi, sur la voie de signalisation d'appel, d'un nouveau message Setup au point MC(U) contenant l'identification CID sélectionnée et la valeur **conferenceGoal = join**. Si l'extrémité 1 décide de n'entrer dans aucune de ces conférences, elle doit envoyer au pont MC(U) un message Release Complete;

A3) si l'extrémité 2 entre dans la conférence, l'extrémité 1 utilise l'adresse de transport de la voie de commande fournie dans le message Connect pour ouvrir la voie de commande avec l'extrémité 2;

A4) l'échange de messages H.245 qui se produit alors est décrit ci-dessous:

A4a) les messages **terminalCapabilitySet** (ensemble de capacités de terminal) échangés entre les extrémités permettent de déterminer le numéro de version de la Rec. UIT-T H.245 utilisée afin d'analyser correctement les messages à recevoir;

A4b) par la procédure de choix du mode maître ou esclave H.245, on détermine que c'est l'extrémité 2 qui est maître. Dans le modèle de signalisation indirecte par l'intermédiaire d'un portier, la fonction de maître pourrait être associée au contrôleur MC situé au même endroit que le portier. Si le maître incorpore le contrôleur multipoint, il devient le contrôleur multipoint activé. Il peut alors envoyer le message **mcLocationIndication** (indication de localisation du contrôleur multipoint) à l'autre ou aux autres extrémités. Le contrôleur multipoint peut alors être activé dans la conférence à ce moment ou lorsque l'utilisateur lance la fonction de conférence multipoint, ceci est laissé au choix du constructeur;

A4c) le maître peut envoyer le message **terminalNumberAssign** (assignation de numéro de terminal) aux extrémités. Celles-ci doivent utiliser, parmi les 16 bits de numéro, non pas les 8 bits du numéro de pont de conférence mais les 8 bits du numéro de terminal qui sont les 8 bits de poids faible du champ SSRC figurant dans l'en-tête RTP. Ces 8 bits de poids faible identifient alors les flux binaires provenant d'une extrémité donnée;

A4d) les capacités du récepteur étant connues par le message **terminalCapabilitySet**, l'émetteur ouvre les voies logiques. Il doit envoyer un message **h2250MaximumSkewIndication** (indication de décalage temporel maximal H.225.0) pour chaque paire de signaux audio et vidéo transmis.

8.4.3.2 Signalisation d'appel directe entre extrémités – Invitation à participer à la conférence

On distingue deux cas de figure pour une invitation à participer à la conférence. Premièrement, l'extrémité qui incorpore le contrôleur multipoint activé souhaite inviter une autre extrémité à participer à la conférence. Deuxièmement, une extrémité qui n'incorpore pas le contrôleur multipoint activé souhaite inviter une autre extrémité à participer à la conférence.

1) Après l'établissement d'une conférence point à point à l'aide des procédures A1) à A4) au § 8.4.3.1, si l'extrémité (extrémité 2) incorporant le contrôleur multipoint activé souhaite faire participer une autre extrémité à la conférence, elle doit procéder de la manière suivante:

B1) l'extrémité 2 envoie à l'extrémité 3 un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = invite** conformément aux procédures du § 8.1. Voir Figure 45;

B2) l'extrémité 3 opère un choix parmi les options suivantes:

B2a) si elle souhaite accepter l'invitation à entrer dans la conférence, elle envoie un message Connect avec l'identificateur CID = N à l'extrémité 2;

B2b) si elle souhaite refuser l'invitation à entrer dans la conférence, elle envoie à l'extrémité 2 un message Release Complete indiquant que la destination est occupée;

B2c) si elle participe à une autre conférence avec l'identificateur CID = M, elle peut demander à l'extrémité 2 d'entrer dans la conférence dont l'identificateur CID vaut M en envoyant un message Facility indiquant **routeCallToMC** avec l'adresse de transport de voie de signalisation d'appel associée à l'extrémité incorporant le contrôleur multipoint ainsi qu'avec l'identificateur CID = M de la conférence. Le traitement du message Facility par l'extrémité 2 est décrit au § 8.4.3.7;

B2d) si l'identificateur CID reçu correspond à l'identificateur CID d'une conférence à laquelle l'extrémité 3 participe, il doit rejeter l'appel en envoyant un message Release Complete indiquant qu'elle participe déjà à la conférence;

B3) si l'extrémité 3 accepte l'invitation, l'extrémité 2 utilise l'adresse de transport de la voie de commande fournie dans le message Connect pour ouvrir la voie de commande avec l'extrémité 3;

B4) l'échange de messages H.245 qui se produit alors est décrit ci-dessous:

C1) des messages **terminalCapabilitySet** sont échangés entre le contrôleur multipoint et l'extrémité 3;

C2) par la procédure de choix du mode maître ou esclave H.245, on détermine que l'extrémité 2 est déjà le contrôleur multipoint activé. Le contrôleur multipoint peut alors envoyer le message **mcLocationIndication** à l'extrémité 3;

C3) le contrôleur multipoint doit envoyer à ce stade le message **multipointConference** aux trois extrémités;

C4) le contrôleur multipoint peut envoyer le message **terminalNumberAssign** à l'extrémité 3. Si ce message est reçu, les extrémités doivent utiliser, parmi les 16 bits de numéro, non pas les 8 bits du numéro de pont de conférence mais les

8 bits du numéro de terminal qui sont les 8 bits de poids faible du champ SSRC figurant dans l'en-tête RTP. Ces 8 bits de poids faible identifient alors les flux binaires provenant d'une extrémité donnée;

C5) une extrémité peut obtenir la liste des autres extrémités participant à la conférence en envoyant le message de demande de liste **terminalListRequest** au contrôleur multipoint. Celui-ci répond par le message **terminalListResponse**;

C6) lorsqu'une nouvelle extrémité (extrémité 4) entre dans la conférence, le contrôleur multipoint lui envoie le message **terminalNumberAssign** et envoie le message **terminalJoinedConference** (entrée d'un terminal dans la conférence) aux extrémités 1, 2 et 3;

C7) chaque fois qu'une extrémité quitte la conférence, le contrôleur multipoint envoie le message **terminalLeftConference** (départ d'un terminal de la conférence) aux autres extrémités;

C8) le contrôleur multipoint doit envoyer le message **communicationModeCommand** (commande de mode communication) à toutes les extrémités de la conférence;

C9) les extrémités 1 et 2 fermeront leurs voies logiques qui ont été créées pendant la conférence point à point s'il y a une incompatibilité avec les informations figurant dans le message **communicationModeCommand**;

C10) les voies logiques peuvent alors être ouvertes entre le contrôleur multipoint et les extrémités.

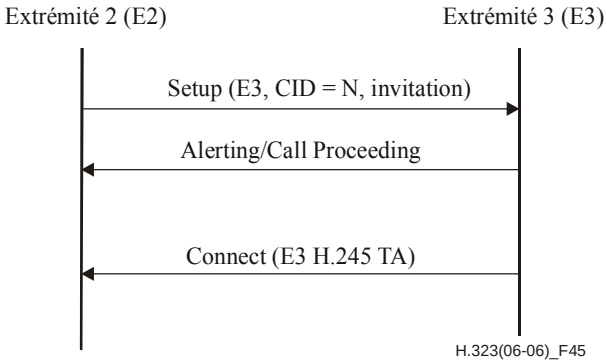


Figure 45/H.323 – Signalisation d'invitation du contrôleur multipoint

2) Après l'établissement d'une conférence point à point à l'aide des procédures A1 à A4 au § 8.4.3.1, si l'extrémité (l'extrémité 1) qui n'incorpore pas le contrôleur multipoint activé souhaite faire participer une autre extrémité à la conférence, elle doit procéder de la manière suivante:

B1) l'extrémité 1 envoie au contrôleur multipoint (extrémité 2) un message Setup avec une nouvelle valeur CRV indiquant un appel vers l'extrémité 3 (l'adresse de transport de l'extrémité 3 est fournie), l'identificateur CID = N et le paramètre **conferenceGoal = invite**. Voir Figure 46;

B2) l'extrémité 2 envoie à l'extrémité 3 un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = invite** conformément aux procédures du § 8.1;

B3) pendant la signalisation d'appel avec l'extrémité 3, l'extrémité 2 doit transmettre à l'extrémité 1 (qui a émis l'invitation initiale) les messages de signalisation d'appel que lui a envoyés l'extrémité 3, y compris le message Connect;

B4) l'extrémité 3 opère un choix parmi les mêmes options (acceptation ou rejet de l'invitation) que celles qui ont été décrites précédemment;

B5) un certain temps après la fin de la procédure d'établissement d'appel entre l'extrémité 2 et l'extrémité 3, l'extrémité 2 doit envoyer un message Release Complete à l'extrémité 1;

B6) si l'extrémité 3 accepte l'invitation, l'extrémité 2 utilise l'adresse de transport de la voie de commande fournie dans le message Connect pour ouvrir la voie de commande avec l'extrémité 3;

B7) les messages H.245 sont alors échangés conformément aux procédures précédemment décrites aux points C1 à C10.

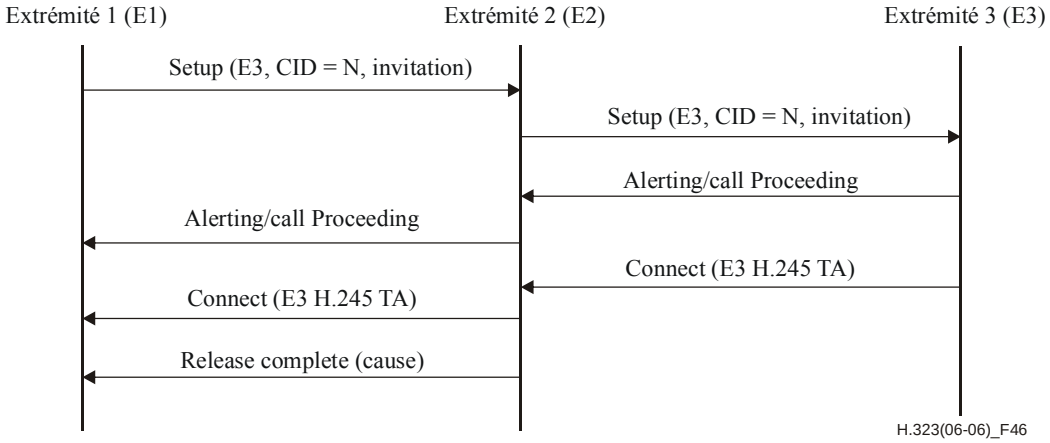


Figure 46/H.323 – Signalisation d'invitation autre que par le contrôleur multipoint

8.4.3.3 Signalisation d'appel directe entre extrémités – Entrée dans la conférence

On distingue deux cas de figure pour l'entrée dans une conférence. Premièrement, une extrémité appelle l'extrémité qui incorpore le contrôleur multipoint activé. Deuxièmement, une extrémité appelle une extrémité qui n'incorpore pas le contrôleur multipoint activé.

Après l'établissement d'une conférence point à point à l'aide des procédures A1 à A4 au § 8.4.3.1, une extrémité (l'extrémité 3) souhaitant entrer dans une conférence peut tenter de se connecter à l'extrémité incorporant le contrôleur multipoint activé de la conférence. Dans ce cas, il faut procéder de la manière suivante:

B1) l'extrémité 3 envoie à l'extrémité 2 un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = join** conformément à la procédure du § 8.1. Voir Figure 47;

B2) si l'identificateur CID correspond à l'identificateur CID d'une conférence active au niveau du contrôleur multipoint, l'extrémité 2 (contrôleur multipoint) opère un choix parmi les options suivantes:

B2a) si elle décide d'autoriser l'extrémité 3 à entrer dans la conférence, elle envoie le message Connect avec l'identificateur CID = N;

B2b) si elle décide de ne pas autoriser l'extrémité 3 à entrer dans la conférence, elle envoie le message Release Complete indiquant que la destination est occupée;

B3) si l'identificateur CID ne correspond pas à l'identificateur CID d'une conférence active au niveau du contrôleur multipoint, l'extrémité 2 doit envoyer un message Release Complete indiquant que l'identificateur CID ne convient pas;

B4) si l'extrémité 2 autorise l'entrée dans la conférence, elle ouvre la voie de commande avec l'extrémité 3;

B5) les messages H.245 sont alors échangés conformément aux procédures précédemment décrites aux points C1 à C10.

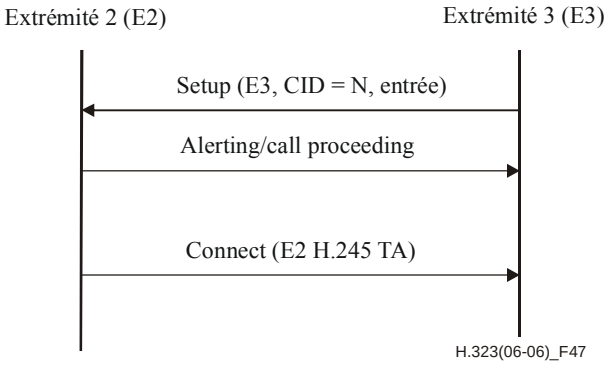


Figure 47/H.323 – Signalisation du contrôleur multipoint pour l'entrée dans une conférence

Après l'établissement d'une conférence point à point à l'aide des procédures A1 à A4, une extrémité (extrémité 3) souhaitant entrer dans une conférence peut tenter de se connecter à l'extrémité qui n'incorpore pas le contrôleur multipoint activé de la conférence. Dans ce cas, il faut procéder de la manière suivante:

B1) l'extrémité 3 envoie à l'extrémité 1 un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = join** conformément à la procédure du § 8.1. Voir Figure 48;

B2) l'extrémité 1 renvoie un message Facility indiquant **routeCallToMC** avec l'adresse de transport de la voie de signalisation d'appel de l'extrémité 2 (incorporant le contrôleur multipoint activé) ainsi qu'avec l'identificateur CID = N de la conférence;

B3) l'extrémité 3 envoie alors à l'extrémité 2 (incorporant le contrôleur multipoint) un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = join** comme cela est décrit dans la précédente procédure d'entrée dans la conférence.

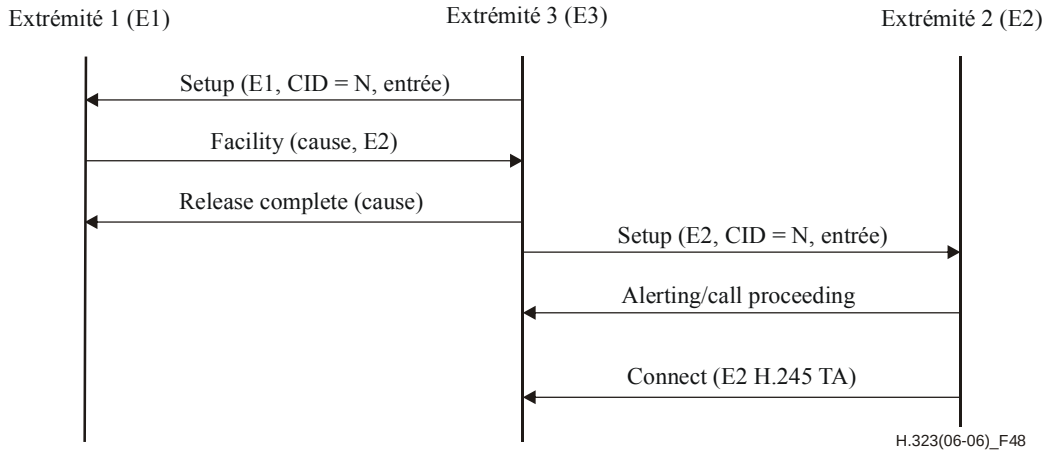


Figure 48/H.323 – Signalisation autre que par le contrôleur multipoint pour l'entrée dans une conférence

8.4.3.4 Signalisation d'appel indirecte par l'intermédiaire d'un portier – Création de conférence

Si la voie de signalisation d'appel et la voie de commande H.245 passent par lui, le portier peut incorporer un contrôleur multipoint ou un pont de conférence (ou y avoir accès). Les procédures A1 à A4 servent à établir la communication point à point.

Si le contrôleur multipoint ou le pont de conférence MC(U) héberge plusieurs conférences et souhaite offrir à l'extrémité 1 la possibilité de participer à un choix de conférences, ce MC(U)

peut envoyer un message Facility indiquant la structure **conferenceListChoice** ainsi qu'une liste de conférences proposées au choix de l'extrémité 1, envoyée dans l'élément d'information Facility-UUIE. Pour assurer la compatibilité amont avec les extrémités selon la version 1, les listes de conférences ne sont fournies que si le champ **protocolIdentifier**, contenu dans le message Setup de l'extrémité 1, indique qu'il s'agit de la version 2 ou au-dessus.

Dès qu'il reçoit le message Facility **conferenceListChoice**, l'extrémité 1 peut entrer dans une des conférences de la liste par l'envoi, sur la voie de signalisation d'appel, d'un nouveau message Setup au pont MC(U) contenant l'identification CID sélectionnée et la valeur **conferenceGoal = join**. Si l'extrémité 1 décide de n'entrer dans aucune de ces conférences, elle doit envoyer au pont MC(U) un message Release Complete.

Si, pendant le choix du mode maître ou esclave (A4b), la valeur de **terminalType** du portier est supérieure à celle du **terminalType** reçu dans le message **masterSlaveDetermination**, le portier peut tenter de devenir le maître de cet appel. Dans ce cas, le portier doit envoyer immédiatement un message **masterSlaveDeterminationAck** à l'entité qui a envoyé le message de détermination maître-esclave pour lui indiquer qu'elle est esclave et le portier effectue la détermination maître-esclave avec l'entité de destination comme indiqué au § 6.2.8.4. Si le portier remporte cette détermination maître-esclave, le contrôleur MC associé à ce portier sera le contrôleur MC actif. Si la valeur de **terminalType** du portier est inférieure à celle du **terminalType** de l'extrémité, ou si le portier décide de ne pas remplacer le **terminalType** de l'extrémité par le sien, le portier ne doit pas modifier la valeur de **terminalType** et doit relayer de manière transparente tous les messages de cette procédure de détermination maître-esclave.

8.4.3.5 Signalisation d'appel indirecte par l'intermédiaire d'un portier – Invitation à participer à la conférence

Après l'établissement d'une conférence point à point à l'aide des procédures A1 à A4 modifiées comme indiqué ci-dessus, si une extrémité (extrémité 1 ou 2) qui n'incorpore pas le contrôleur multipoint activé souhaite faire participer une autre extrémité à la conférence, elle procédera de la manière suivante:

B1) l'extrémité 1 envoie, par l'intermédiaire du portier, un message Setup destiné à l'extrémité 3 et comportant une nouvelle valeur CRV, l'identificateur CID = N et le paramètre **conferenceGoal = invite**. Voir Figure 49;

B2) le portier (contrôleur multipoint) envoie à l'extrémité 3 un message Setup avec l'identificateur CID = N et le paramètre **conferenceGoal = invite** conformément aux procédures du § 8.1;

B3) pendant la signalisation d'appel avec l'extrémité 3, le portier doit transmettre à l'extrémité 1 (qui a émis l'invitation initiale) les messages de signalisation d'appel que lui a envoyés l'extrémité 3, y compris le message Connect;

B4) l'extrémité 3 opère un choix parmi les mêmes options (acceptation ou refus de l'invitation) que celles qui ont été décrites précédemment;

B5) un certain temps après la fin de la procédure d'établissement d'appel entre le portier et l'extrémité 3, le portier doit envoyer un message Release Complete à l'extrémité 1;

B6) si l'extrémité 3 accepte l'invitation, le portier utilise l'adresse de transport de la voie de commande fournie dans le message Connect pour ouvrir la voie de commande avec l'extrémité 3;

B7) les messages H.245 sont alors échangés conformément aux procédures précédemment décrites aux points C1) à C10), le portier intervenant en tant que contrôleur multipoint activé dans toutes les procédures de choix du mode maître ou esclave (C2). A ce stade, les voies de commande en provenance des extrémités doivent être connectées au contrôleur multipoint et ce dernier doit avoir la commande de la conférence.

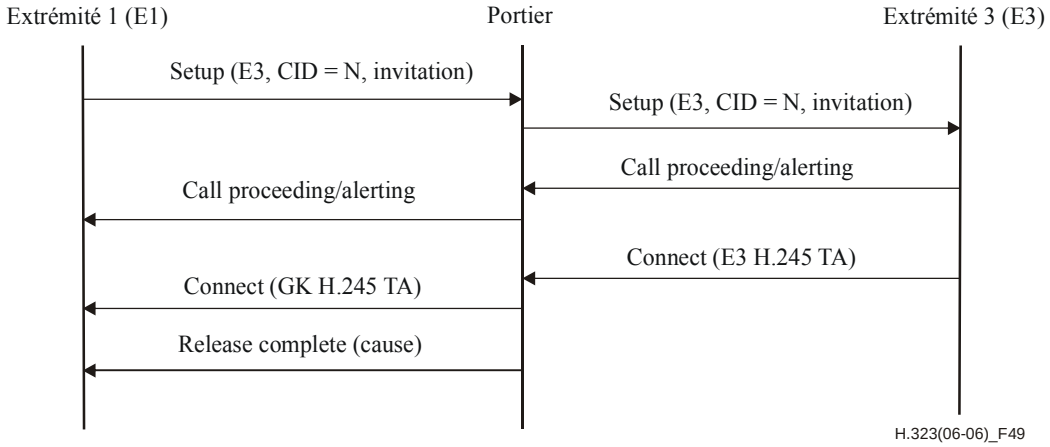


Figure 49/H.323 – Signalisation d'invitation indirecte par l'intermédiaire d'un portier

8.4.3.6 Signalisation d'appel indirecte par l'intermédiaire d'un portier – Entrée dans la conférence

Après l'établissement d'une conférence point à point à l'aide des procédures A1 à A4 modifiées comme indiqué ci-dessus, si une extrémité (l'extrémité 3) souhaite entrer dans une conférence, il peut tenter de se connecter à une extrémité qui n'incorpore pas le contrôleur multipoint activé de la conférence. Dans ce cas, il faut procéder de la manière suivante:

B1) l'extrémité 3 envoie, par l'intermédiaire du portier, un message Setup destiné à l'extrémité 1 et comportant l'identificateur CID = N et le paramètre **conferenceGoal = join** conformément à la procédure du § 8.1. Voir Figure 50;

B2) si l'identificateur CID correspond à l'identificateur CID d'une conférence active au niveau du contrôleur multipoint, le portier (contrôleur multipoint) opère un choix parmi les options suivantes:

- B2a) s'il décide d'autoriser l'extrémité 3 à entrer dans la conférence, il lui envoie le message Connect avec l'identificateur CID = N à l'extrémité 3;
- B2b) s'il décide de ne pas autoriser l'extrémité 3 à entrer dans la conférence, il envoie le message Release Complete indiquant que la destination est occupée;
- B2c) le portier peut renvoyer le message Setup à l'extrémité 1. Celle-ci peut répondre par un message Facility indiquant **routeCallToMC** ou par un message Release Complete;

B3) si l'identificateur CID ne correspond pas à l'identificateur CID d'une conférence active au niveau du contrôleur multipoint, le portier doit envoyer un message Release Complete indiquant que l'identificateur CID ne convient pas;

B4) si le portier autorise l'entrée dans la conférence, il utilise l'adresse de transport de la voie de commande fournie dans le message Setup pour ouvrir la voie de commande avec l'extrémité 3;

B5) les messages H.245 sont alors échangés conformément aux procédures précédemment décrites aux points C1 à C10, le portier intervenant en tant que contrôleur multipoint activé dans toutes les procédures de choix du mode maître ou esclave (C2). A ce stade, les voies de commande en provenance des extrémités doivent être connectées au contrôleur multipoint et ce dernier doit avoir la commande de la conférence.

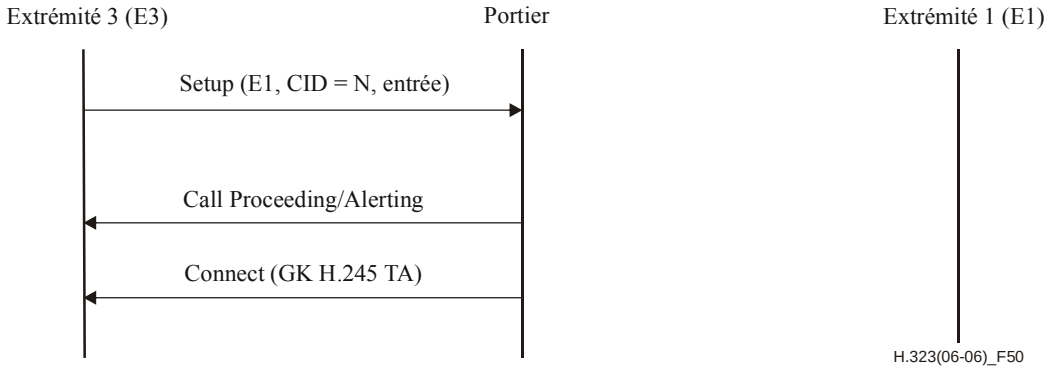


Figure 50/H.323 – Signalisation indirecte par l'intermédiaire d'un portier pour l'entrée dans une conférence

8.4.3.7 Traitement du message Facility

Dès réception d'un message de facilité (Facility) indiquant la commande **routeCallToMC** avec l'adresse de transport pour voie de signalisation d'appel de l'extrémité contenant le contrôleur multipoint et l'identificateur CID d'une conférence, une extrémité peut libérer la communication en cours et tenter de se joindre à la conférence indiquée conformément aux procédures du § 8.4.3.3 ou 8.4.3.6.

Une extrémité peut recevoir un tel message Facility soit sous forme de réponse directe à son message Setup d'appel soit au cours de la phase active d'une communication.

8.4.3.8 Conférence hors consultation

Le présent paragraphe précise les procédures s'appliquant à une extrémité (extrémité A) demandant une conférence ad hoc avec deux ou plusieurs autres extrémités (extrémités distantes B, C, etc.) avec lesquelles l'extrémité A est déjà en communication active. Cette situation se présente généralement, mais pas nécessairement, lorsqu'une conférence ad hoc est demandée hors consultation.

NOTE 1 – Par "consultation" on entend une situation dans laquelle l'extrémité A est en communication active avec l'extrémité C (double appel) tout en ayant un ou plusieurs autres extrémités en attente. Une extrémité peut être mise en attente au moyen des procédures de la Rec. UIT-T H.450.4 [35] et § 8.4.6 ou par des procédures locales.

L'extrémité A a la capacité de "fusionner" des communications indépendantes avec plusieurs extrémités en une conférence unique, à l'extrémité A (scénario 1 ci-dessous) ou en créant la conférence en un pont MCU séparé (scénario 2 ci-dessous).

NOTE 2 – Les procédures du présent paragraphe se rapportent uniquement aux appels à une extrémité qui doivent être réunis en une conférence hors consultation. Une extrémité peut avoir d'autres communications qui ne participent pas à la conférence et auxquelles le présent paragraphe ne s'applique pas.

8.4.3.8.1 Scénario 1: conférence créée par une extrémité

Si le point A en a la capacité, il peut "fusionner" l'appel en attente et le double appel pour créer une conférence formée d'une conversation à trois entre A, B et C. Dans ce scénario, l'extrémité A doit avoir un contrôleur MC. Les modèles de conférence centralisé et décentralisé sont tous deux possibles. Si l'on utilise le modèle centralisé (c'est-à-dire lorsque le terminal assure la fusion/commutation des médias), l'extrémité A doit avoir un processeur MP.

Une extrémité disposant d'un contrôleur MC et d'un processeur MP est en fait un pont de conférence MCU qui doit utiliser le **terminalType** 170, 180 ou 190 selon les besoins de la détermination maître-esclave.

Les scénarios suivants sont possibles:

1a) si le point d'extrémité A est le maître des deux appels B et C, il peut simplement récupérer l'appel en attente avec C et se déclarer contrôleur MC actif pour les deux appels via une négociation maître-esclave;

1b) si le point d'extrémité A est esclave de l'un ou de plusieurs des appels mais qu'aucun des appels dont il est l'esclave ne dispose d'un contrôleur MC actif, le point d'extrémité A doit relancer la détermination maître-esclave pour tous les appels dans lesquels il est esclave, cela au moyen du **terminalType** 240 comme indiqué dans le Tableau 1 pour un contrôleur MC actif. S'il termine cette procédure en tant que maître de tous les appels, il doit se comporter comme indiqué au point 1a ci-dessus; s'il est esclave dans un ou plusieurs appels, il doit se comporter comme indiqué au point 1c ci-dessous;

1c) si un ou plusieurs des appels auxquels participe l'extrémité A est déjà un appel dans lequel cette extrémité A n'est pas le contrôleur MC actif, il faudra appliquer les procédures de mise en cascade des ponts MCU.

Dès qu'une conférence est établie à une extrémité A, une autre extrémité D – qui est en cours de consultation par le point A – peut être invitée à participer à la conférence existante comme indiqué aux § 8.4.3.2 et 8.4.3.5.

8.4.3.8.2 Scénario 2: conférence assurée par un pont MCU

Si l'extrémité A a accès à un pont MCU, on peut utiliser la procédure suivante pour tenir une conférence hors consultation:

2a) l'extrémité A établit un nouvel appel avec le pont MCU au moyen d'un message Setup dont la valeur de **conferenceGoal = create** et la valeur de CID = N;

2b) l'extrémité A abandonne son appel avec l'extrémité C au moyen d'un message Release Complete dont **reason = replaceWithConferenceInvite** avec l'argument CID = N;

2c) l'extrémité A envoie un message Setup au pont MCU avec **conferenceGoal = invite**, CID = N et suffisamment d'informations pour que le point MCU puisse lancer un appel à l'extrémité C (voir aussi au § 8.4.3.2);

2d) les opérations 2b et 2c doivent être répétées avec "extrémité C" remplacée par "extrémité B". On notera qu'il n'est pas nécessaire de récupérer la communication avec B en attente avant de l'inviter à participer à la conférence;

2e) en ce qui concerne l'échange des messages H.245 relatifs à la conférence, voir les étapes C1-C10 au § 8.4.3.2.

Les mécanismes pouvant remplacer les étapes 2b, 2c et 2d sont les suivants:

1) le transfert de communication H.450.2 [34] (l'extrémité A agissant en tant qu'extrémité "effectuant le transfert", les extrémités B et C agissant en tant qu'extrémités "transférées" et le contrôleur MC/pont MCU agissant en tant qu'extrémité de destination du transfert). Le message Facility contenant **callTransferInitiate Invoke APDU** contiendra également l'élément CID mis à N;

2) le mécanisme "message Facility utilisé pour le réacheminement vers le contrôleur MC" de la Rec. UIT-T H.225.0 (envoi aux extrémités B et C d'un message Facility H.225.0 dont CID = N, **facilityReason = routeCallToMC**, ainsi que de l'adresse du pont MCU) si le service complémentaire H.450.2 n'est pas pris en charge.

Il est recommandé d'utiliser ces autres mécanismes possibles si l'extrémité distante est située dans le RCC.

Une extrémité (telle que l'extrémité A) peut se séparer de la conférence (par exemple en mettant sa communication avec le pont MCU à maintien). L'extrémité A peut ensuite consulter une autre extrémité D qui peut ensuite être invitée à participer à la conférence existante au moyen des

procédures des points 2b et 2c ci-dessus, "l'extrémité C" étant remplacée par "l'extrémité D". On peut aussi utiliser les mécanismes de remplacement décrits ci-dessus au moyen du transfert de communication H.450.2 ou du "Message Facility pour le réacheminement vers le contrôleur MC" de la Rec. UIT-T H.225.0.

8.4.4 Services complémentaires

La prise en charge de services complémentaires est facultative. Les Recommandations UIT-T de la série H.450.x décrivent une méthode de fourniture de services complémentaires dans l'environnement H.323.

8.4.5 Mise en cascade multipoint

Pour connecter en cascade des contrôleurs multipoints, il faut établir une communication entre les entités qui les contiennent, conformément aux procédures définies aux § 8.1 et 8.4.3. Une fois la communication établie et la voie de commande H.245 ouverte, le contrôleur multipoint actif (déterminé conformément aux procédures de maître/esclave du § 6.2.8.4) peut activer son homologue dans une entité connectée, au moyen du message H.245 **remoteMC**. Les résultats ci-après doivent apparaître dans la réponse au message **remoteMC**.

Entité appelante	Entité appelée	Objet de conférence	Emetteur du message RemoteMC	Sélection du message RemoteMC	Résultat
MC actif	MC inactif	**création (create)**	entité appelante	**masterActivate**	Le MC appelé accepte la demande et devient le MC maître
MC actif	MC inactif	**invitation (invite)**	entité appelante	**slaveActivate**	Le MC appelé accepte la demande et devient un MC esclave
MC actif	MC inactif	**entrée (join)**	sans objet	sans objet	Opération non autorisée
MC inactif	MC actif	**création (create)**	sans objet	sans objet	Opération non autorisée
MC inactif	MC actif	**invitation (invite)**	sans objet	sans objet	Opération non autorisée
MC inactif	MC actif	**entrée (join)**	entité appelée	**slaveActivate**	Le MC appelé accepte la demande et devient un MC esclave

Une fois que la conférence mise en cascade est établie, le contrôleur multipoint maître ou un contrôleur multipoint esclave peut inviter d'autres extrémités à entrer dans la conférence. Il ne doit y avoir qu'un seul contrôleur maître dans une conférence. Un contrôleur esclave ne doit être mis en cascade qu'avec un contrôleur maître et non avec d'autres contrôleurs esclaves, ce qui n'autorise que des configurations de cascade en haltère ou en étoile.

Le contrôleur multipoint esclave doit identifier la conférence en cascade au moyen de l'identificateur CID établi par le maître lors de la création de la conférence.

Le contrôleur multipoint esclave doit accepter et donner suite aux messages **communicationsModeCommand** issus du contrôleur maître. Le contrôleur esclave doit faire suivre ces messages jusqu'à ses extrémités en connexion locale. Le contrôleur esclave peut recevoir des messages de type **requestMode** de ses extrémités en connexion locale. Il convient qu'il les fasse suivre jusqu'au contrôleur maître. Le contrôleur esclave ne doit pas envoyer de messages **communicationsModeCommand** au contrôleur maître.

Celui-ci devrait suivre les procédures des points C3 à C10 du § 8.4.3.2 afin d'établir un mode de fonctionnement commun avec le contrôleur esclave. Sur la base de ces informations, chaque contrôleur multipoint est chargé d'ouvrir des voies logiques pour la distribution des médias entre ses extrémités en connexion locale et les extrémités désignées par le contrôleur maître.

En plus de l'invitation de nouvelles extrémités à entrer dans la conférence, un contrôleur multipoint qui prend en charge les conférences multiples peut transférer directement des extrémités dans une autre conférence sans interrompre la connexion existante. Si cette opération est effectuée, il y a lieu que le contrôleur multipoint envoie le message **substituteCID** à ces extrémités. Celles-ci, lorsqu'elles reçoivent un message **substituteCID** en cours de communication, doivent continuer à utiliser l'identificateur de conférence (CID) employé dans les messages RAS précédents (par exemple ARQ, BRQ, etc.) lors de ses échanges avec son portier pendant la durée de cette communication particulière.

Les fonctions de numérotation des terminaux et de commande présidentielle peuvent suivre les procédures définies dans la Rec. UIT-T H.243. L'utilisation des procédures T.120 pour la commande de la mise en cascade de contrôleurs multipoints fera l'objet d'un complément d'étude. L'utilisation des procédures T.120 dans les connexions en cascade est décrite dans les Recommandations UIT-T de la série T.120.

Lorsqu'un maître envoie une demande **remoteMC** avec la sélection **deActivate**, le contrôleur esclave doit normalement retirer toutes les extrémités de la conférence.

8.4.6 Pause et reroutage à l'initiative d'une tierce partie

Aux fins du présent paragraphe, on définit comme un ensemble de capacités vide un message **terminalCapabilitySet** contenant uniquement un numéro de séquence et un identificateur de protocole.

Pour permettre aux portiers de rerouter les connexions à partir d'extrémités qui ne prennent pas en charge les services complémentaires, les extrémités doivent répondre à la réception d'un ensemble de capacités vides comme défini dans le présent paragraphe. Cette caractéristique permet à des éléments "de réseau" comme des autocommutateurs, des centres d'appel et des systèmes de réponses vocales interactives (IVR) de rerouter des connexions indépendantes des services complémentaires. Elle facilite également les annonces de préconnexion et peut être utilisée pour retarder l'établissement de voies médias H.245 lorsque des éléments comme la localisation de l'utilisateur sur la base du portier sont en cours d'utilisation. Il est par ailleurs fortement recommandé que les extrémités selon la version 1 prennent en charge cette caractéristique.

Dès réception d'un ensemble de capacités vide, une extrémité doit passer à un état "de pause côté émetteur". Lors du passage à cet état l'extrémité doit cesser d'émettre par les voies logiques établies et doit fermer toutes les voies logiques préalablement ouvertes, notamment les voies logiques bidirectionnelles. Ces voies sont fermées de la manière habituelle, par envoi du message **closeLogicalChannel**. L'extrémité ne doit pas demander à l'extrémité distante de fermer les voies logiques, unidirectionnelles ou bidirectionnelles, que ce dernier a ouvertes. L'extrémité envoie le message **terminalCapabilitySetAck** de la façon habituelle: le message peut être envoyé avant arrêt de la transmission et ne doit pas être interprété comme une indication d'arrêt de la transmission.

Dans l'état de "pause côté émetteur", une extrémité ne doit pas amorcer l'ouverture de voies logiques, mais doit en accepter l'ouverture et la fermeture à partir de l'extrémité distante, sur la base des règles usuelles et doit également continuer à recevoir des flux médias issus de voies logiques ouvertes à partir de l'extrémité distante. Cela permet aux extrémités de recevoir des annonces (par exemple une progression d'appel par préconnexion) lorsque l'entité annonçante ne souhaite pas recevoir de flux média en provenance de l'extrémité. Un message **terminalCapabilitySet** peut être envoyé dès qu'il y a modification des capacités d'une extrémité, notamment lorsqu'une extrémité est passée dans l'état "pause côté émetteur". Cela permet l'établissement d'une communication entre deux extrémités qui ne déclarent initialement aucune capacité.

Une extrémité qui est dans l'état "pause côté émetteur" peut aussi mettre l'autre extrémité participant à la communication dans un état "pause côté émetteur" en émettant un message *ensemble de capacités vide*. A la réception dudit message, le récepteur doit appliquer les procédures définies dans le présent paragraphe.

Une extrémité doit quitter l'état "pause côté émetteur" à réception d'un message **terminalCapabilitySet**, autre qu'un ensemble de capacités vide. En quittant cet état une extrémité doit réinitialiser son état H.245 pour revenir à celui dans lequel elle se trouvait immédiatement après l'établissement de la connexion de transport H.245, au moment de l'établissement de l'appel (c'est-à-dire au début de la phase B), mais doit préserver l'information d'état concernant les voies logiques éventuellement ouvertes. Cela met l'extrémité dans un état H.245 connu après la pause et permet de connecter une extrémité à une autre extrémité lorsqu'elle est libérée de l'état de pause.

Lorsqu'elle quitte l'état de "pause côté émetteur", une extrémité doit engager les procédures normales H.245: elle doit participer à la signalisation de détermination du maître/esclave et peut engager les procédures normales de signalisation d'ouverture de voie logique. Lorsqu'un contrôleur multipoint quitte l'état de "pause côté émetteur", il doit agir comme si une nouvelle extrémité était entrée dans la conférence.

Si une extrémité se trouvant dans l'état "pause côté émetteur" a également émis précédemment un ensemble de capacités vide afin de mettre l'autre extrémité dans l'état "pause côté émetteur", elle doit partir du principe que cette autre extrémité restera dans un état de pause jusqu'à ce qu'elle lui communique un ensemble de capacités non vide; elle libèrera alors l'autre extrémité de l'état de pause. L'extrémité dans l'état de pause doit être disposée à recevoir des messages OLC en provenance de l'autre extrémité.

A condition que ses capacités n'aient pas changé, une extrémité n'a pas besoin de réémettre un ensemble de capacités étant donné que le portier l'aura déjà fourni pour supprimer tout état de pause dans l'extrémité distante. Cette possibilité de ne pas envoyer un ensemble de capacités permet une reconnexion plus rapide. Si le premier message **terminalCapabilitySet** envoyé par une extrémité après avoir quitté l'état "pause côté émetteur" diffère de l'ensemble de capacités fourni par le portier à l'extrémité distante, le portier doit notifier à l'extrémité distante d'ôter les capacités qui n'ont pas été indiquées par l'extrémité effectuant le lancement.

NOTE 1 – Il convient qu'une extrémité vérifie soigneusement les capacités qu'elle envoie à cet instant. Elle doit notamment envoyer toutes les capacités qu'elle souhaite notifier, et non se contenter d'envoyer la liste des capacités qui s'ajoutent à celles qui ont été préalablement envoyées. En outre si le nombre des capacités d'une extrémité est tel qu'il faut plusieurs messages **terminalCapabilitySet** pour les envoyer, il est possible que, pendant un certain créneau temporel, le portier ait retiré les capacités décrites dans le deuxième message **terminalCapabilitySet** et dans les messages suivants.

NOTE 2 – Il ne faut pas envoyer un ensemble de capacités non vide à une extrémité avant que toutes ses voies logiques d'émission aient été fermées. Il convient également qu'une entité de commutation envoie un message Facility contenant l'indication de renvoi H.450, si l'extrémité doit être reroutée.

8.5 Phase E – Fin de la communication

L'une ou l'autre des extrémités ou une entité de signalisation d'appel intermédiaire peut mettre fin à une communication. A cet effet, elle doit appliquer la procédure A ou la procédure B:

Procédure A

A-1) elle doit cesser de transmettre les signaux vidéo à la fin d'une image complète, le cas échéant;

A-2) elle doit cesser de transmettre les données, le cas échéant;

A-3) elle doit cesser de transmettre les signaux vidéo, le cas échéant;

A-4) elle doit transmettre un message Release Complete et fermer la voie de signalisation d'appel H.225.0 ainsi que, si elle s'ouvre isolément, la voie de commande H.245, sans envoyer aucun message H.245. A noter que la fermeture des voies médias est implicite;

A-5) les extrémités doivent libérer la communication conformément aux procédures définies au § 8.5.1 ou 8.5.2.

Procédure B

B-1) elle doit cesser de transmettre les signaux vidéo à la fin d'une image complète, puis fermer toutes les voies logiques vidéo, le cas échéant;

B-2) elle doit cesser de transmettre les données, puis fermer toutes les voies logiques de données, le cas échéant;

B-3) elle doit cesser de transmettre les signaux audio, puis fermer toutes les voies logiques audio, le cas échéant;

B-4) elle doit transmettre le message de commande de fin de session **endSessionCommand** H.245 dans la voie de commande H.245, en indiquant à l'extrémité distante qu'il souhaite mettre fin à la communication et doit ensuite interrompre la transmission de messages H.245;

B-5) elle doit ensuite attendre de recevoir le message de commande de fin de session **endSessionCommand** envoyé par l'autre extrémité puis fermer la voie de commande H.245;

B-6) elle doit transmettre un message Release Complete et fermer la voie de signalisation d'appel H.225.0;

B-7) les extrémités doivent libérer la communication conformément aux procédures définies au § 8.5.1 ou 8.5.2.

Une extrémité qui reçoit une commande de fin de session **endSessionCommand** qu'elle n'a pas préalablement transmise doit exécuter les étapes B-1 à B-7 ci-dessus, sauf que dans l'étape B-5 elle ne doit pas attendre la commande **endSessionCommand** envoyée par la première extrémité.

Mettre fin à une communication ne met pas forcément fin à une conférence; il peut être mis fin explicitement à une conférence à l'aide d'un message H.245 (abandon de conférence **dropConference**). Dans ce cas, les extrémités doivent attendre que le contrôleur multipoint mette fin aux communications comme cela est décrit ci-dessus.

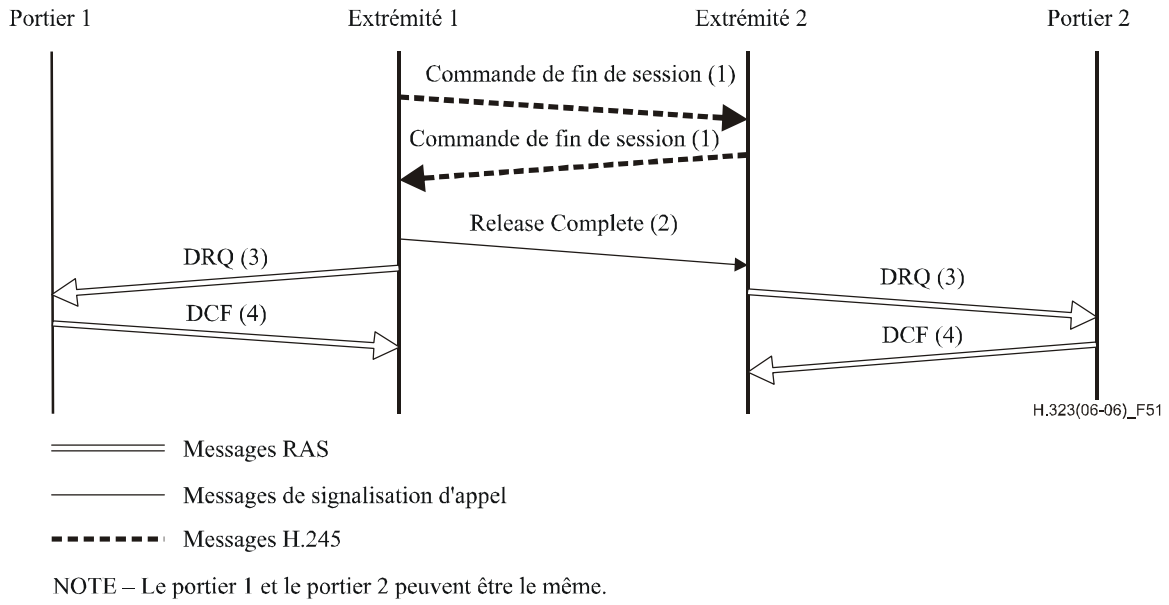
8.5.1 Libération de la communication sans portier

Dans les réseaux qui n'incorporent pas de portier, la communication prend fin après les étapes A-1 à A-5 ou B-1 à B-6 ci-dessus. Aucune autre action n'est nécessaire.

8.5.2 Libération de la communication avec portier

Dans les réseaux qui incorporent un portier, celui-ci doit être informé de la libération de la largeur de bande. Après avoir exécuté les étapes A-1 à A-5 ou B-1 à B-6 ci-dessus, chaque extrémité doit transmettre un message de demande de désengagement H.225.0 (DRQ, *disengage request*) (3) à son portier. Celui-ci doit y répondre par un message de confirmation de désengagement (DCF, *disengage confirm*) (4). Après avoir envoyé le message de demande de désengagement DRQ, les extrémités ne doivent pas envoyer d'autres messages spontanés de réponse à une demande d'information IRR au portier. Voir Figure 51. La communication prend fin à ce stade. La Figure 51 illustre le cas du modèle de signalisation d'appel directe; on procède de manière similaire dans le cas du modèle de signalisation indirecte par l'intermédiaire d'un portier.

Les messages de demande de libération DRQ et de confirmation de libération DCF doivent être envoyés sur la voie RAS.



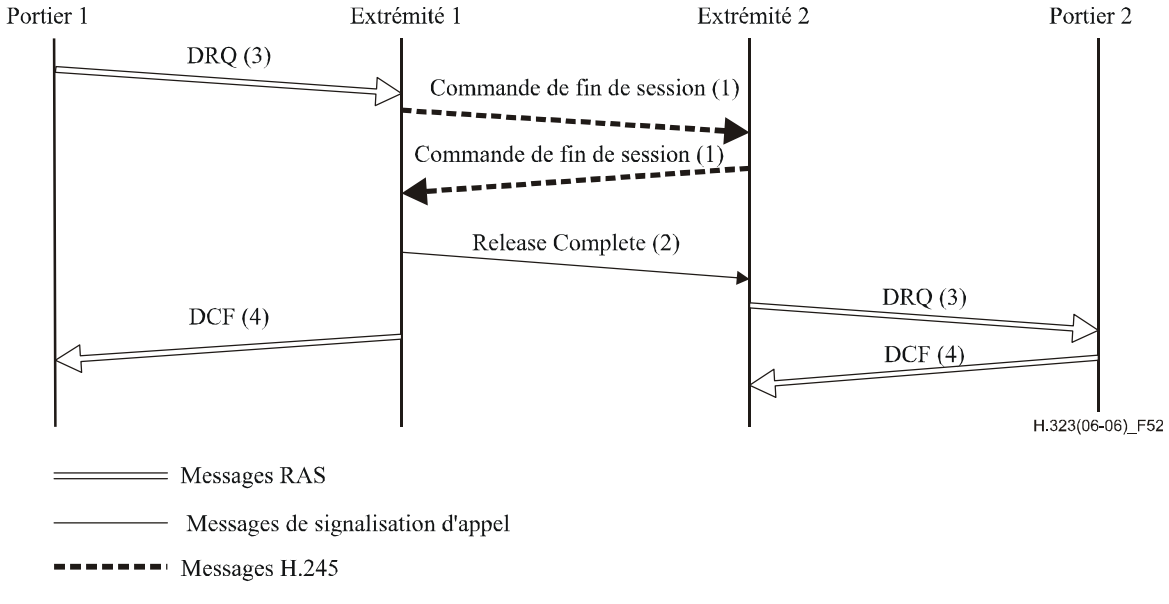
NOTE – Le portier 1 et le portier 2 peuvent être le même.

Figure 51/H.323 – Déclenchement de la libération de la communication par l'extrémité (Procédure B)

8.5.3 Libération de la communication par le portier

Le portier peut mettre fin à une communication en envoyant une demande de désengagement à une extrémité. Voir Figure 52. L'extrémité doit immédiatement suivre les étapes A-1 à A-5 ou B-1 à B-6 ci-dessus puis répondre au portier par une confirmation de désengagement. L'autre extrémité suivra la procédure décrite ci-dessus dès qu'elle recevra le signal **endSessionCommand**. La Figure 52 illustre le cas du modèle de signalisation d'appel directe; on procède de manière similaire dans le cas du modèle de signalisation indirecte par l'intermédiaire d'un portier.

Si la conférence est une conférence multipoint le portier doit envoyer un message de demande de désengagement DRQ à chaque extrémité de la conférence, afin de mettre fin à la conférence dans son ensemble.



NOTE – Le portier 1 et le portier 2 peuvent être le même.

Figure 52/H.323 – Déclenchement de la libération de la communication par le portier

NOTE – Le message Release Complete mentionné dans le présent paragraphe peut en fait être précédé par d'autres messages H.225.0 dans le cadre de la procédure de terminaison d'appel. Par exemple, lors de la tunnellisation d'un autre protocole visé dans la Rec. H.225.0, il peut être nécessaire d'échanger des messages tunnellisés avant l'envoi du message définitif Release Complete. Par ailleurs, étant donné que les messages H.245 et H.225.0 peuvent fonctionner sur des connexions distinctes, il est possible qu'un message End Session H.245 arrive avant un message H.225.0 précédemment envoyé. Ainsi, dans le cadre de l'implémentation, il ne faudrait pas s'attendre à ce que le message H.225.0 faisant immédiatement suite à la réception d'un message End Session H.245 soit nécessairement un message Release Complete.

8.6 Gestion des défaillances du protocole

Le protocole fiable de base sur lequel repose la voie de signalisation d'appel H.225.0 et la voie de commande H.245 s'efforce comme il convient de remettre et de recevoir les données sur la voie avant de signaler une défaillance du protocole.

Dans le cas d'une défaillance signalée par la couche Transport fiable de base, les entités H.323 doivent fonctionner selon les indications contenues dans le présent paragraphe. Si l'utilisation de l'Annexe R a été négociée entre deux entités, l'entité ou les entités qui détectent une défaillance devraient s'efforcer de rétablir la communication conformément aux procédures exposées dans l'Annexe R.

Selon l'itinéraire de la voie de signalisation d'appel et de la voie de commande H.245, la défaillance du protocole peut être détectée par le portier ou par une extrémité. Si elle est détectée par le portier, celui-ci doit tenter de rétablir la voie de commande d'appel. Cela suppose que l'extrémité soit toujours en mesure d'établir une voie sur son adresse de transport de voie de signalisation d'appel. Le dérangement de la voie de signalisation d'appel ne doit pas modifier l'état de la communication. Une fois la voie de signalisation d'appel rétablie, le portier peut envoyer un message d'indication d'état pour demander l'état des communications de l'extrémité pour s'assurer que celles-ci sont synchronisées, que l'on utilise ou non l'Annexe R.

Si la défaillance du protocole est détectée par l'extrémité, celle-ci a le choix entre mettre fin à la communication comme indiqué dans la phase E, ou tenter de rétablir la voie de signalisation d'appel comme indiqué ci-dessus.

Si pendant une communication une extrémité souhaite savoir si l'autre extrémité est encore en fonctionnement et connectée, elle peut envoyer le message de demande de temps de propagation aller-retour **roundTripDelayRequest** H.245. La voie de commande H.245 étant établie sur une voie fiable, l'envoi de ce message donnera lieu à une réponse de l'autre extrémité ou à une erreur de l'interface de transport. Dans ce dernier cas, les procédures décrites ci-dessus doivent être utilisées. Une extrémité participant à une conférence multipoint peut utiliser le même mécanisme; toutefois, cela lui permettra uniquement de savoir si elle est toujours connectée au contrôleur multipoint. A noter qu'une extrémité peut être connectée sans erreur au contrôleur multipoint tout en ne recevant aucun signal audio ou vidéo du reste des terminaux participant à la conférence.

Dans certains cas, il est possible que la défaillance de la voie de signalisation d'appel H.225.0 ou de la voie de commande H.245 ne soit pas considérée comme déterminante pour l'appel. En effet, dans une conversation uniquement vocale, il n'y a généralement aucune signalisation entre les entités une fois que la communication est établie, ce qui fait que cette défaillance ne se traduira peut-être pour les utilisateurs que par la perte de fonctionnalités de service supplémentaires. Une passerelle RTPC peut être à même d'utiliser des informations provenant du circuit RTPC, par exemple, pour déterminer la présence d'une activité vocale entre deux utilisateurs et pour s'assurer que, en dépit de l'éventuelle défaillance de la voie de signalisation d'appel H.225.0 ou de la voie de commande H.245, elle est toujous capable d'assurer la communication et d'y mettre fin dès que cette activité vocale ne sera plus détectée. Le mécanisme utilisé pour déterminer la fin d'une communication en pareils cas est du domaine de l'implémentation et ne relève donc pas de la présente Recommandation. Rien n'empêche les dispositifs de poursuivre une communication en cas de la

défaillance ou de l'absence de voies de signalisation, s'ils disposent d'un moyen pour le faire. Lorsque l'extrémité a déterminé que la communication est terminée, les extrémités doivent transmettre un message DRQ au portier comme à l'ordinaire.

Si une défaillance du protocole est signalée au niveau de la voie de signalisation d'appel H.225.0 ou de la voie de commande H.245 et s'il n'y a aucun moyen de rétablir la communication ni de la poursuivre sans recourir à l'une de ces deux voies, il faut fermer la voie de commande H.245 (si elle est ouverte), toutes les voies logiques associées ainsi que la voie de signalisation d'appel H.225.0. Cela doit être fait selon les procédures de la Phase E, comme si l'autre extrémité avait envoyé le message **endSessionCommand H.245**. Cela suppose l'envoi d'un message DRQ au portier et la terminaison de l'appel. Dans le cas où il détecte la défaillance d'une conférence multipoint, le contrôleur multipoint doit envoyer des messages **terminalLeftConference** aux autres terminaux.

9 Interfonctionnement avec d'autres types de terminaux

L'interfonctionnement avec d'autres terminaux doit être assuré par l'intermédiaire de la passerelle. Voir § 6.3 et la Rec. UIT-T H.246.

9.1 Terminaux fonctionnant uniquement en mode téléphonique

L'interfonctionnement avec des terminaux fonctionnant uniquement en mode téléphonique sur le RNIS ou le RTGC peut être assuré par les moyens suivants:

1) à l'aide d'une passerelle téléphonique H.323/RNIS;

2) à l'aide d'une passerelle téléphonique H.323/RTGC.

La passerelle doit tenir compte des aspects de conversion suivants:

– conversion de code audio:
  - RNIS: si cette conversion est souhaitée, étant donné que le RNIS utilise la Rec. UIT-T G.711;
  - RTGC: conversion du mode analogique au mode G.711;
– conversion du flux de bits:
  - RNIS: conversion du mode H.225.0 au mode non tramé ou vice versa;
  - RTGC: émission du mode H.225.0;
– conversion de commande (émission du mode H.245);
– conversion de signalisation de commande d'appel;
– conversion des tonalités multifréquences (DTMF) au message d'indication de données d'usager **userInputIndication** H.245 ou vice versa et types de charge utile RTP (conformément au § 10.5).

9.2 Terminaux de visiophonie sur le RNIS (Rec. UIT-T H.320)

L'interfonctionnement avec des terminaux de visiophonie sur le RNIS (Rec. UIT-T H.320) peut être assuré par les moyens suivants:

– à l'aide d'une passerelle H.323-H.320.

La passerelle doit tenir compte des aspects de conversion suivants:

– conversion de format vidéo (dans le cas où cette conversion est souhaitée, le mode H.261 est obligatoire pour les deux types de terminaux);
– conversion de code audio (dans le cas où cette conversion est souhaitée, le mode G.711 est obligatoire pour les deux types de terminaux);
– conversion de protocole de données;

– conversion du flux de bits (du mode H.225.0 au mode H.221 ou vice versa);
– conversion de commande (du mode H.245 au mode H.242 ou vice versa);
– conversion de signalisation de commande d'appel;
– conversion du numéro d'extension SBE au message **userInputIndication** H.245 ou vice versa et types de charge utile RTP (conformément au § 10.5).

9.3 Terminaux de visiophonie sur le RTGC (Rec. UIT-T H.324)

L'interfonctionnement avec des terminaux de visiophonie sur le RTGC (Rec. UIT-T H.324) peut être assuré par deux méthodes:

1) à l'aide d'une passerelle H.323-H.324;
2) à l'aide d'une passerelle H.323-H.320, à supposer qu'il existe une passerelle H.320-H.324 dans le réseau à commutation de circuits.

La passerelle doit tenir compte des aspects de conversion suivants:

– conversion de format vidéo (dans le cas où cette conversion est souhaitée, le mode H.261 est obligatoire pour les deux types de terminaux);
– conversion de protocole de données;
– conversion de code audio (le mode G.711 est obligatoire pour les terminaux H.323; le mode G.723.1 est obligatoire pour les terminaux H.324);
– conversion du flux de bits (du mode H.225.0 au mode H.223 ou vice versa);
– conversion de signalisation de commande d'appel.

9.4 Terminaux de visiophonie sur le réseau mobile (Annexe C/H.324, aussi appelée "H.324/M")

Ce point appelle un complément d'étude.

9.5 Terminaux de visiophonie sur des réseaux ATM (terminaux RAST H.321 et H.310)

L'interfonctionnement avec des terminaux de visiophonie sur des réseaux ATM (terminaux RAST H.321 et H.310 exploités en mode d'interfonctionnement H.320/H.321) peut être assuré par deux méthodes:

1) à l'aide d'une passerelle H.323-H.321;
2) à l'aide d'une passerelle H.323-H.320, à supposer qu'il existe une unité d'interfonctionnement RNIS/ATM I.580 dans le réseau.

La passerelle doit tenir compte des aspects d'interfonctionnement suivants:

– conversion de format vidéo (dans le cas où cette conversion est souhaitée, le mode H.261 est obligatoire pour les deux types de terminaux);
– conversion de protocole de données;
– conversion de code audio (dans le cas où cette conversion est souhaitée, le mode G.711 est obligatoire pour les deux types de terminaux);
– conversion du flux de bits (du mode H.225.0 au mode H.221 ou vice versa);
– conversion de commande (du mode H.245 au mode H.242 ou vice versa);
– conversion de signalisation de commande d'appel.

9.6 Terminaux de visiophonie sur des réseaux locaux à qualité de service garantie (Rec. UIT-T H.322)

L'interfonctionnement avec des terminaux de visiophonie sur des réseaux locaux à qualité de service garantie (Rec. UIT-T H.322) peut être assuré par le moyen suivant:

– à l'aide d'une passerelle H.323-H.320, à supposer qu'il existe une passerelle réseau local à qualité de service garantie/RNIS dans le réseau.

La passerelle doit tenir compte des aspects de conversion suivants:

– conversion de format vidéo (dans le cas où cette conversion est souhaitée, le mode H.261 est obligatoire pour les deux types de terminaux);

– conversion de protocole de données;

– conversion de code audio (dans le cas où cette conversion est souhaitée, le mode G.711 est obligatoire pour les deux types de terminaux);

– conversion du flux de bits (du mode H.225.0 au mode H.221 ou vice versa);

– conversion de commande (du mode H.245 au mode H.242 ou vice versa);

– conversion de signalisation de commande d'appel.

9.7 Terminaux fonctionnant en mode téléphonie et données simultanées sur le RTGC (Rec. UIT-T V.70)

L'interfonctionnement avec des terminaux fonctionnant en mode téléphonie et données simultanées sur le RTGC (Rec. UIT-T V.70) peut être assuré par le moyen suivant:

– à l'aide d'une passerelle H.323-V.70.

La passerelle doit tenir compte des aspects de conversion suivants:

– conversion de code audio (du mode G.711 au mode Annexe A/G.729 ou vice versa);

– conversion de protocole de données;

– conversion du flux de bits (du mode H.225.0 au mode V.76/V.75 ou vice versa);

– conversion de commande (les deux terminaux utilisent le mode H.245);

– conversion de signalisation de commande d'appel.

9.8 Terminaux T.120 sur le réseau en mode paquet

Un terminal H.323 qui a la capacité T.120 devrait pouvoir être configuré strictement comme un terminal T.120 conçu pour l'écoute et l'émission sur l'identificateur de point TSAP communément admis T.120 normalisé. Cela permettra à un terminal H.323 doté de la capacité T.120 de participer à des conférences n'admettant que le mode T.120.

Un terminal n'admettant que le mode T.120 sur le réseau doit pouvoir participer à la portion T.120 de conférences multipoint H.323 en se connectant au pont de conférence du système de communication multipoint. Voir § 6.2.7.1.

9.9 Passerelle pour l'acheminement de flux H.323 sur réseaux ATM

Il est possible d'acheminer des flux H.323 provenant de réseaux IP non ATM sur un réseau ATM au moyen de passerelles H.323 à H.323. Le mécanisme est décrit dans le document AF-SAA-0124.000 [32].

10 Améliorations facultatives

10.1 Chiffrement

Les fonctions d'authentification et de sécurité sont facultatives pour les systèmes H.323. Si toutefois elles sont fournies, elles doivent l'être conformément à la Rec. UIT-T H.235.0 et aux documents qui y sont cités en référence.

10.2 Exploitation multipoint

10.2.1 Messages de commande et d'indication H.243

La Rec. UIT-T H.245 décrit les messages de commande et d'indication multipoint acheminés à partir de terminaux H.243. Ces messages peuvent être utilisés pour fournir certaines capacités multipoints (comme la commande présidentielle) à condition de suivre les procédures définies dans la Rec. UIT-T H.243.

NOTE – Le paragraphe 15/H.243 donne des directives pour l'implémentation de ces capacités au moyen des Recommandations UIT-T de la série T.120.

10.3 Assemblage d'appels dans des messages H.323

10.3.1 Description

Dans la Rec. UIT-T H.323, l'assemblage d'appels est une fonction facultative. Dans le présent paragraphe, l'auxiliaire "devoir" doit être interprété comme indiquant une exigence obligatoire, à condition que la fonction d'assemblage d'appels soit prise en charge.

10.3.1.1 Description générale

La fonction d'identification du fil d'exécution permet d'assembler plusieurs communications différentes ou plusieurs connexions de signalisation indépendantes, qui sont logiquement associées du point de vue d'un service ou d'une application en termes de progression.

La fonction d'identification globale d'appel permet d'identifier une communication ou une connexion sémaphore indépendante de l'appel au moyen d'un seul identificateur applicable à la communication ou à la connexion sémaphore indépendante de l'appel, sans tenir compte de sa route ou de son historique.

NOTE – L'identificateur d'appel est défini au § 7.5 comme un identificateur d'appel mondialement unique. Un nouvel appel de base issu de la même extrémité/entité ou un nouvel appel faisant partie d'un scénario de service utilisera une nouvelle valeur d'identificateur d'appel.

10.3.1.2 Définitions relatives au service

10.3.1.2.1 Identification de fil d'exécution (ID de fil d'exécution, TID)

Valeur attribuée aux appels qui sont logiquement associés les uns aux autres, afin de les mettre en corrélation. Si au moins deux appels sont logiquement associés (par exemple en raison d'interactions entre services), l'identificateur actuel du fil d'exécution de l'un de ces appels est attribué à tous les autres appels associés.

10.3.1.2.2 Identification globale d'appel (ID globale d'appel, GID)

Valeur attribuée à un appel de bout en bout pour identifier de façon unique cet appel de bout en bout. Si différents appels sont transformés en un nouvel appel (par exemple en raison d'interactions entre services), les identificateurs GID des anciens appels sont mis à jour (s'ils ont déjà été attribués) ou sont attribués au nouvel appel de bout en bout par une nouvelle valeur GID.

NOTE – Un appel qui subit une transformation à partir de différents semi-appels à cause de certains services peut finir par avoir des semi-appels dont les identificateurs d'appel sont différents. L'identificateur d'appel ne convient donc pas pour identifier de façon unique un appel de bout en bout.

10.3.2 Invocation et fonctionnement

Un identificateur d'appel doit être attribué à chaque nouvel appel qui est établi (voir § 7.5). En raison d'interactions entre services, différents identificateurs d'appel peuvent être assignés à différentes parties (semi-appels) d'un appel.

Un identificateur global d'appel peut être attribué soit au moment de l'établissement de l'appel pendant l'état actif soit pendant la progression de l'établissement/de la libération d'appel si au moins deux appels sont transformés en un nouvel appel en raison de l'invocation de certains services ou en réponse à une demande d'application.

Un identificateur global d'appel peut être modifié au cours de la durée de vie de la communication si celle-ci est transformée.

Un identificateur de fil d'exécution peut être attribué soit au moment de l'établissement de l'appel pendant l'état actif soit pendant la progression de l'établissement/de la libération d'appel si au moins deux appels sont transformés en un nouvel appel en raison de l'invocation de certains services ou en réponse à une demande d'application.

L'identificateur de fil d'exécution peut être modifié au cours de la durée de vie d'une communication (par exemple en raison d'interactions entre services).

10.3.3 Interaction avec des services complémentaires H.450

Les interactions avec des services complémentaires H.450, pour lesquels des normes étaient disponibles au moment de la publication de la présente Recommandation, sont spécifiées ci-dessous.

Pour l'identificateur d'appel, aucune interaction avec d'autres services complémentaires n'est applicable car cet identificateur doit être unique pour chaque nouvel appel. Toutes les interactions décrites dans le présent paragraphe ne s'appliquent qu'à l'identificateur global d'appel et/ou qu'à l'identificateur de fil d'exécution.

Un identificateur global d'appel et un identificateur de fil d'exécution peuvent être attribués, sans rapport avec une invocation de service complémentaire, dans le cadre de l'établissement d'un appel de base. Des interactions spécifiques entre fonctions sont décrites ci-dessous pour des invocations de services complémentaires spécifiques.

10.3.3.1 Transfert de communication

Le présent paragraphe décrit l'emploi des champs d'assemblage d'appels lors de l'application du service H.450.2.

10.3.3.1.1 Transfert sans consultation

L'identificateur de fil d'exécution de la communication transférée doit être hérité de l'identificateur de fil d'exécution de la communication primaire. L'identificateur de fil d'exécution de la communication primaire doit donc être fourni par l'extrémité effectuant un transfert à l'extrémité destinatrice du transfert en même temps que la demande de transfert de communication. Si la communication primaire ne possède pas d'identificateur de fil d'exécution attribué, l'extrémité effectuant un transfert doit en produire un. Si l'entité transférée ne reçoit pas d'identificateur de fil d'exécution en même temps que la demande de transfert de communication, cette entité doit hériter de l'identificateur de fil d'exécution qui a été attribué à la communication primaire lors de l'établissement de celle-ci. Si aucun identificateur de fil d'exécution que ce soit n'est disponible par héritage, l'extrémité destinatrice du transfert doit produire un identificateur de fil d'exécution et l'attribuer aussi bien à la communication transférée (dans un message Setup d'appel) et à la communication primaire (dans un message de libération d'appel).

Un nouvel identificateur global d'appel doit être attribué à une communication transférée. Si un portier établit la communication transférée pour le compte d'une extrémité destinatrice du transfert,

ce portier doit attribuer le même identificateur global d'appel à l'autre semi-appel de la communication primaire. Cela garantit que la communication qui résultera de l'exécution du transfert aura un même identificateur GID unique de bout en bout.

10.3.3.1.2 Transfert avec consultation

Au moment du transfert, la communication transférée doit se faire attribuer le même identificateur de fil d'exécution que la communication primaire précédente, si:

a) la communication primaire est entrante et la communication secondaire est sortante;

b) ou les deux communications sont entrantes et la communication primaire a été établie avant la communication secondaire;

c) ou les deux communications sont sortantes et la communication primaire a été établie avant la communication secondaire.

Au moment du transfert, la communication transférée doit se faire attribuer le même identificateur de fil d'exécution que la communication secondaire précédente, si:

a) la communication secondaire est entrante et la communication primaire est sortante;

b) ou les deux communications sont entrantes et la communication secondaire a été établie avant la communication primaire;

c) ou les deux communications sont sortantes et la communication secondaire a été établie avant la communication primaire.

L'identificateur de fil d'exécution approprié à la communication transférée (fondée sur la communication primaire ou secondaire selon la situation) doit être fourni par l'extrémité effectuant un transfert à l'extrémité destinatrice du transfert en même temps que la demande de transfert de communication. Si la communication (primaire ou secondaire) dont l'identificateur de fil d'exécution doit être hérité n'a pas d'identificateur de fil d'exécution attribué, l'extrémité effectuant un transfert doit en produire un. Si l'extrémité destinatrice du transfert ne reçoit pas d'identificateur de fil d'exécution en même temps que la demande de transfert de communication (par exemple si l'extrémité effectuant un transfert n'assure pas l'assemblage des appels), cette extrémité doit produire un identificateur de fil d'exécution qui doit être hérité de la communication primaire, si possible.

Au moment du transfert, l'entité transférée doit attribuer une nouvelle valeur d'identificateur GID à la communication transférée. Si celle-ci a été établie par un portier pour le compte d'une extrémité destinatrice du transfert, ce portier doit attribuer le même identificateur GID au semi-appel restant de la communication primaire. Un portier agissant pour le compte de l'extrémité destinatrice du transfert doit attribuer le même identificateur GID à la partie restante de la communication secondaire. Cela garantit que la communication résultant du transfert effectué aura un seul identificateur GID de bout en bout.

Une entité effectuant un transfert peut, à titre d'option, choisir de "fusionner" la communication primaire et la communication secondaire. Les règles d'assemblage d'appels doivent être, pour la communication résultante ("fusionnée"), identiques à celles qui ont été spécifiées ci-dessus pour une communication transférée.

10.3.3.2 Déviation d'appel

Le présent paragraphe décrit l'emploi des champs d'assemblage d'appels lors de l'application du service H.450.3 [39].

L'appel initial, l'appel expéditeur du renvoi et l'appel destinataire du renvoi doivent utiliser le même identificateur de fil d'exécution.

L'identificateur de fil d'exécution de l'appel destinataire du renvoi et de l'appel initial doit être hérité de l'identificateur de fil d'exécution de l'appel expéditeur du renvoi. L'extrémité servie doit donc

attribuer un identificateur de fil d'exécution à l'appel expéditeur du renvoi (si cette attribution n'a pas déjà été effectuée dans le cadre de l'appel de base) et doit fournir cet identificateur de fil à l'entité de reroutage en même temps que la demande de renvoi d'appel. L'entité de reroutage doit utiliser cet identificateur de fil d'exécution pour l'établissement de l'appel destinataire du renvoi. Par ailleurs, le semi-appel initial (s'il existe) doit également faire l'objet d'une attribution/mise à jour avec cet identificateur de fil d'exécution.

Si l'entité de reroutage ne reçoit pas d'identificateur de fil d'exécution en même temps que la demande de renvoi d'appel, elle doit hériter de l'identificateur de fil d'exécution qui était attribué à l'appel expéditeur du renvoi au moment de l'établissement de l'appel. Si aucun identificateur de fil d'exécution que ce soit n'est disponible pour héritage, l'extrémité de reroutage doit produire un identificateur de fil d'exécution et l'attribuer à l'appel expéditeur du renvoi, à l'appel destinataire du renvoi et à l'appel initial.

Un nouvel identificateur GID doit être attribué à l'appel de bout en bout par l'appelant (c'est-à-dire l'usager expéditeur du transfert) à l'usager destinataire du transfert par attribution d'un nouvel identificateur GID dans le message Setup de l'appel destinataire du renvoi et par attribution (ou mise à jour) du même identificateur GID au semi-appel initial (s'il existe).

10.3.3.3 Mise en attente et double appel

Le présent paragraphe décrit l'emploi des champs d'assemblage d'appels lors de l'application du service Rec. UIT-T H.450.4.

Un double appel doit utiliser le même identificateur de fil d'exécution que le premier appel.

NOTE – La qualification d'un appel comme étant un double appel plutôt qu'un nouvel appel de base relève d'une décision de l'extrémité.

Un double appel doit utiliser un nouvel identificateur global d'appel.

10.3.3.4 Parcage et reprise d'appel

Le présent paragraphe décrit l'emploi des champs d'assemblage d'appels lors de l'application du service Rec. UIT-T H.450.5 [40].

La communication parquée aura le même identificateur de fil d'exécution que l'appel primaire. Elle utilisera toutefois un identificateur GID différent.

S'il est disponible, l'identificateur de fil d'exécution sera utilisé pour associer des connexions sémaphores indépendantes (avec indication des notifications de groupe et des demandes de reprise d'appel), l'appel issu d'un appelant parqué vers le repreneur d'appel, et un appel parqué précédemment en alerte/faux-appel.

NOTE – Le parcage et la reprise d'appel font intervenir un identificateur de prise d'appel propre qui est utilisé par le repreneur d'appel.

Les connexions sémaphores indépendantes de l'appel qui sont utilisées dans le cadre du parcage et de la reprise d'appel utiliseront de nouveaux identificateurs GID. L'appel issu de l'appelant parqué vers le repreneur d'appel aura un nouvel identificateur GID global de bout en bout.

10.3.3.5 Signal d'appel en attente

Il n'y a aucune interaction entre l'assemblage d'appels et le service Rec. UIT-T H.450.6 [41].

10.3.3.6 Indication de message en attente

Il n'y a aucune interaction entre l'assemblage d'appels et le service Rec. UIT-T H.450.7 [42].

10.3.3.7 Service d'identification de nom

Il n'y a aucune interaction entre l'assemblage d'appels et le service Rec. UIT-T H.450.8 [43].

10.4 Tunnellisation de messages de signalisation non H.323

Afin de prendre en charge des informations de signalisation non H.323 existantes dans un système H.323, il est nécessaire d'en prévoir le transport dans un tel système. Le présent paragraphe décrit un moyen générique de tunnellisation des messages de signalisation à l'intérieur de tout message de commande d'appel en protocole H.225.0.

Les procédures du présent paragraphe s'appliquent à tout type d'extrémité. Les tunnels de signalisation aboutissent à une entité logique appelée "terminaison de tunnel". Normalement, ces terminaisons de tunnel sont situées dans des passerelles qui interconnectent des parties d'un réseau non H.323 avec un réseau H.323 comme décrit sur la Figure 53. Un portier présent dans le réseau H.323 peut participer à la tunnellisation de la signalisation non H.323.

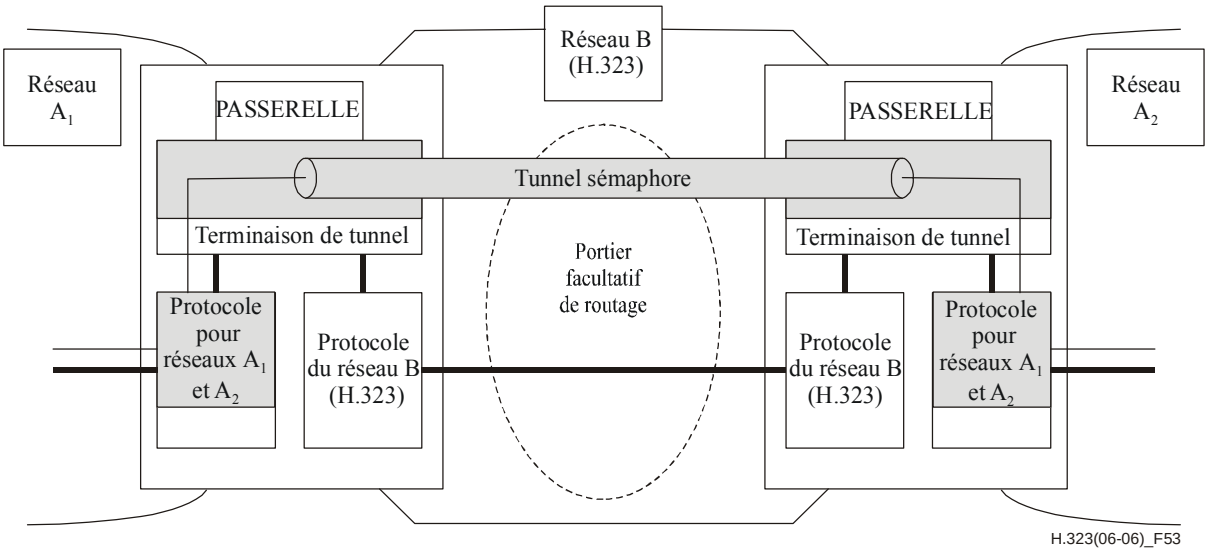


Figure 53/H.323 – Tunnellisation de la signalisation entre passerelles

Dans certains cas, la terminaison de tunnel peut être située dans un portier, comme décrit sur la Figure 54. Le paragraphe 10.4.2 décrit l'intervention du portier dans un tunnel.

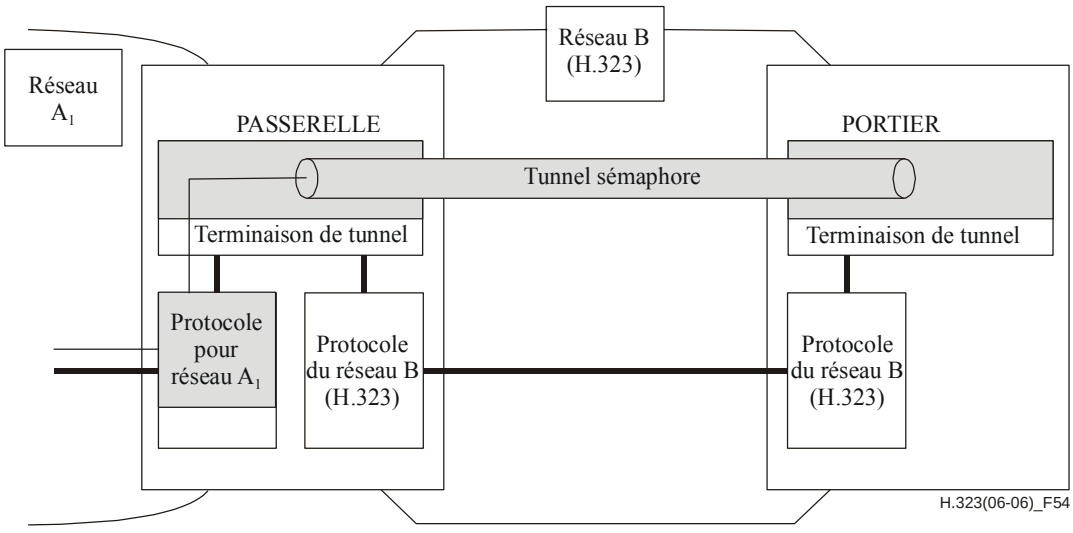


Figure 54/H.323 – Tunnellisation de la signalisation entre une passerelle et une terminaison de tunnel située dans un portier

Les états de commande d'appel et les procédures du protocole mis en tunnel sont distincts des états de commande d'appel et des procédures du protocole H.225.0: une extrémité prenant en charge la signalisation mise en tunnel doit considérer ces deux protocoles comme étant distincts.

Tout protocole de signalisation peut être mis en tunnel et est identifié par un élément **TunnelledProtocol**. Exemples de protocoles de signalisation pouvant être mis en tunnel:

- QSIG;
- ISUP;
- DSS1 du RNIS;
- DPNSS;
- protocole de mise en réseau par autocommutateur privé.

10.4.1 Indication de la prise en charge des protocoles canalisés

La prise en charge de la tunnellisation d'une liste de protocoles rangés par ordre de priorité est indiquée par le champ **supportedTunnelledProtocols** de la structure **EndpointType**. Cette liste se compose de protocoles qui peuvent être canalisés.

Lors de son enregistrement auprès de son portier, une extrémité peut indiquer les protocoles de tunnellisation qui sont pris en charge dans les demandes GRQ et RRQ contenant la même structure **EndpointType**. Celle-ci contient une liste classée par ordre des priorités des protocoles canalisés qui sont pris en charge, le premier étant le préféré. Dans le message ACF ou LCF qu'un portier renvoie en réponse à une demande ARQ ou LRQ, le champ **destinationType** indique également les protocoles de signalisation mis en tunnel sous forme d'une liste de priorités prises en charge. Etant donné que l'Annexe G/H.225.0 importe la séquence **EndpointType**, cette capacité peut également être acheminée au moyen du protocole de l'Annexe G/H.225.0.

Une extrémité d'origine qui souhaite indiquer les protocoles de signalisation qu'elle peut tunnelliser doit inclure la liste de priorités dans le champ **sourceInfo.suppportedTunnelledProtocols** du message Setup. Une extrémité de destination qui souhaite indiquer les protocoles de signalisation qu'elle peut mettre en tunnel doit inclure la liste de priorités dans le champ **destinationInfo.supportedTunnelledProtocols** de tous les messages contenant le champ **destinationInfo** qu'elle envoie en réponse au message Setup. Si une extrémité d'origine ne reçoit pas cette indication, elle doit partir du principe que l'extrémité de destination ne prend en charge aucun des protocoles mis en tunnel.

10.4.2 Demande d'un canal de protocole spécifique vers un portier

Une entité peut demander à un portier un tunnel de protocole spécifique en spécifiant le protocole particulier dans le champ **desiredTunnelledProtocol** d'un message ARQ ou LRQ.

10.4.3 Tunnellisation d'un protocole de signalisation dans des messages de signalisation d'appel H.225.0

Une extrémité peut mettre en tunnel un protocole de signalisation en insérant le champ **tunnelledSignallingMessage** dans tout message de signalisation d'appel H.225.0. Il n'est cependant pas recommandé de tunnelliser un protocole de signalisation contenu dans des messages de signalisation d'appel H.225.0 qui n'ont pas une portée de bout en bout, comme un message Call Proceeding, car ces informations peuvent ne pas être reçues par l'autre extrémité.

Si une extrémité ne permet à l'appel de progresser que si la tunnellisation est prise en charge, cette extrémité doit activer le fanion **tunnellingRequired** du message Setup. Le fanion **tunnellingRequired** ne doit pas être inclus dans un autre message que Setup. Si une extrémité reçoit un élément **tunnelledSignallingMessage** dont le fanion **tunnellingRequired** est activé dans le message Setup et si cette extrémité n'est pas en mesure de canaliser le protocole, elle doit mettre fin à l'appel en envoyant un message Release Complete dont le champ **reason** a la valeur

tunnelledSignallingRejected. Un fanion **tunnellingRequired** contenu dans un autre message que Setup doit être ignoré.

Les informations de protocole canalisées en tunnel sont incluses dans le champ **messageContent** et le champ **tunnelledProtocolID** identifie le protocole mis en tunnel. Un seul protocole à la fois peut être mis en tunnel dans une communication H.323. De multiples messages mis en tunnel avec le même protocole peuvent être assemblés en un seul message de signalisation d'appel H.225.0.

Le tunnel peut être libéré au moyen des procédures de libération H.323 normales.

Les procédures de signalisation d'appel du protocole H.225.0 peuvent être utilisées afin d'établir une connexion sémaphore indépendante de l'appel entre les extrémités homologues. La tunnellisation peut être utilisée dans ce contexte pour offrir au protocole mis en tunnel une signalisation indépendante du support. Dans ce cas, aucune voie de commande H.245 ni aucune voie média n'est requise. Un élément d'information *Capacité support* doit être inclus dans le message Setup du protocole H.225.0 et doit être codé comme décrit dans le Tableau 2/H.450.1. Le message Setup utilisé pour les procédures indépendantes de l'appel doit contenir un élément **conferenceGoal** mis à la valeur **callIndependentSupplementaryService**. Ces procédures de connexion sémaphore indépendante de l'appel pour la tunnellisation ne doivent pas être utilisées en même temps qu'un service complémentaire H.450 dans la même connexion sémaphore indépendante de l'appel.

10.4.4 Considérations relatives au portier

Dans un modèle d'appel à routage direct, le portier n'est pas impliqué dans la signalisation de commande d'appel H.225.0. Il n'effectue donc pas la tunnellisation de la signalisation par protocole H.225.0. Ce type de portier n'a pas d'incidence sur la tunnellisation entre deux extrémités prenant en charge la mise en tunnel de la signalisation. Dans un modèle de routage par portier, celui-ci participe à la fourniture d'un tunnel entre extrémités homologues en retransmettant les informations de signalisation reçues en tunnel. Le portier peut également utiliser le message Facility ou Progress pour acheminer des messages mis en tunnel, comme indiqué au § 8.2.2.

Dans le modèle à routage par portier, celui-ci peut intercepter et modifier des messages de signalisation en tunnel. La terminaison d'un tunnel sémaphore est effectuée par une fonction de terminaison de tunnel qui, comme indiqué plus haut, peut être située dans le portier. L'action de celui-ci sur le protocole mis en tunnel est hors du domaine d'application de la présente Recommandation. Si cependant le portier est en mesure de fournir un service de signalisation non H.323, ce portier peut effectuer la terminaison du tunnel sémaphore et produire les messages H.225.0 appropriés aux extrémités impliquées dans la communication. En variante, il peut également modifier les informations de signalisation mises en tunnel: dans ce cas, il prend la responsabilité d'effectuer la terminaison et le lancement du protocole mis en tunnel. Un portier qui n'interprète pas correctement le protocole mis en tunnel ou qui ne vise pas à agir sur ce protocole ou à fournir des services dans ce plan, doit transférer sans changement le message de signalisation en tunnel afin de préserver l'intégrité du protocole mis en tunnel.

10.5 Utilisation de la charge utile RTP pour les chiffres DTMF, les tonalités et les signaux téléphoniques

Il est possible de transporter des tonalités DTMF, des tonalités de télécopie, des tonalités normalisées de ligne d'abonné, des tonalités propres à un pays et des événements concernant des circuits en utilisant un type distinct de charge utile RTP dans le même flux RTP que le média. De nombreuses applications (systèmes IVR, systèmes vocaux) reposent sur la synchronisation de signaux d'entrée DTMF.

La norme RFC 2833 [56] décrit certains moyens permettant de transporter ces tonalités et ces événements avec le protocole RTP. Une extrémité peut indiquer qu'elle prend en charge la réception de ces tonalités et de ces événements RFC 2833 en incluant dans l'ensemble des capacités du terminal les éléments **receiveRTPAudioTelephonyEventCapability** ou

receiveRTPAudioToneCapability. Une extrémité peut également indiquer qu'elle prend en charge des tonalités et des événements RFC 2833 en incluant dans l'ensemble des capacités du terminal les éléments **audioTelephonyEvent** ou **audioToneAudioCapability**. En cas d'utilisation des procédures de connexion rapide, ces capacités peuvent être envoyées conformément aux procédures parallelH245 définies au § 8.2.4.

Les événements téléphoniques nommés sont une description logique des tonalités DTMF, des tonalités de télécopie, des tonalités normalisées de ligne d'abonné, des tonalités propres à un pays et des événements concernant des circuits. Un nombre décimal permet d'identifier chaque événement. Lorsque des événements téléphoniques sont utilisés, la prise en charge des caractères DTMF suivants est obligatoire: 0-9, #, *, A, B, C, D. La prise en charge d'autres caractères est facultative.

Les tonalités téléphoniques sont une description des propriétés des signaux. Cela est utile lorsqu'il est nécessaire de reproduire des tonalités non normalisées.

Après l'ouverture d'un canal logique pour le flux de médias, l'expéditeur peut envoyer l'un des événements ou l'une des tonalités téléphoniques annoncés par le destinataire dans l'ensemble de capacités du terminal sur le même canal logique en utilisant le type de charge utile RTP négocié lors de la négociation de l'ensemble de capacités du terminal.

Si une extrémité envoie une information DTMF, elle peut l'envoyer dans un message **UserInputIndication** et/ou en utilisant la charge utile RTP pour les chiffres DTMF, les tonalités et signaux téléphoniques.

Si l'information DTMF est envoyée via le protocole RTP et le message **UserInputIndication** sous forme alphanumérique, elle doit être codée dans la structure **extendedAlphanumeric** et le champ **rtpPayloadIndication** doit être inclus. Si l'information DTMF est envoyée via le protocole RTP et le message **UserInputIndication** sous forme de signaux, le champ **rtpPayloadIndication** doit être inclus dans la structure **signal**. Si l'information DTMF est envoyée uniquement sous forme alphanumérique, elle doit être codée dans le champ **alphanumeric**. Si l'information DTMF est envoyée uniquement sous forme de signaux, le champ **rtpPayloadIndication** ne doit pas être inclus.

La RFC 2833 ne doit pas être utilisée pour relayer l'information de télécopie dans les systèmes H.323. En revanche, les procédures définies dans l'Annexe D doivent être suivies pour les extrémités qui souhaitent transmettre de l'information de télécopie T.38.

NOTE – Les entités H.323 antérieures à la version 4 n'ont pas la capacité d'envoyer de l'information DTMF via le protocole RTP tel que décrit dans le présent paragraphe. Par conséquent, toutes les entités doivent pouvoir envoyer l'information DTMF via le message **UserInputIndication.**

11 Maintenance

11.1 Fonctions de bouclage aux fins de la maintenance

La Rec. UIT-T H.245 définit un certain nombre de fonctions de bouclage destinées à vérifier certains aspects fonctionnels du terminal, afin de garantir au correspondant distant le bon fonctionnement du système et une qualité de service satisfaisante.

Les messages de demande de boucle du système **systemLoop** et de demande de boucle de voie logique **logicalChannelLoop** ne doivent pas être utilisés. Le message de demande de boucle de médias **mediaLoop** est facultatif. Une extrémité qui reçoit le message de commande de désactivation de boucle de maintenance **maintenanceLoopOffCommand** doit désactiver toutes les fonctions de bouclage en cours.

Deux modes de bouclage sont définis pour ces fonctions:

a) le mode de fonctionnement normal: sans bouclage, représenté en **a** sur la Figure 55. Il s'agit du mode par défaut et du mode choisi à la réception du message de commande **maintenanceLoopOffCommand**;

b) le mode boucle de médias: avec bouclage du flux de médias à l'interface E/S analogique. A la réception du message de demande de boucle de médias **mediaLoop** défini dans la Rec. UIT-T H.245, la fonction de bouclage du contenu de la voie logique choisie doit être activée en un point aussi proche que possible de l'interface analogique du codec vidéo/audio en direction de celui-ci, de manière que le contenu des médias codés et recodés soit transmis en retour, comme indiqué en **b** sur la Figure 55. Cette fonction de bouclage est facultative. Elle ne devrait être utilisée que lorsqu'une seule voie logique contenant le même type de médias est ouverte dans chaque sens. Le mode de fonctionnement à appliquer lorsque plusieurs voies sont ouvertes dans le sens retour n'est pas défini.

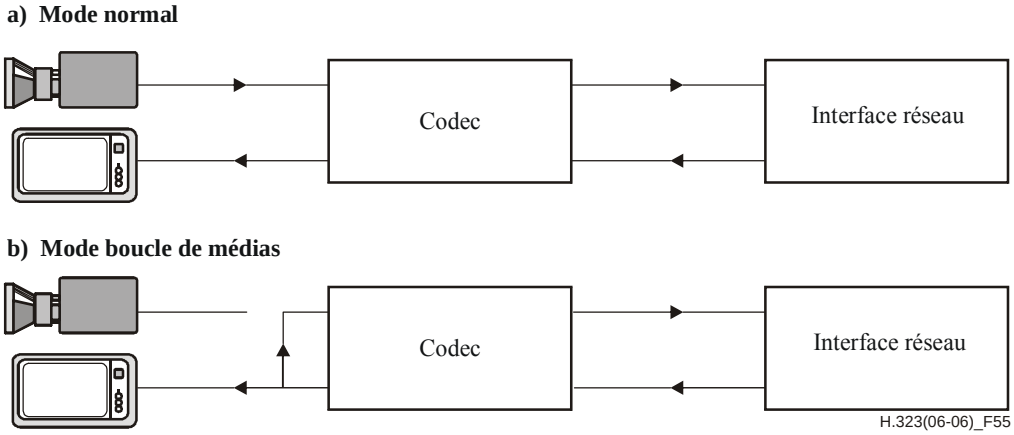


Figure 55/H.323 – Fonction de bouclage

Une passerelle conforme à la Rec. UIT-T H.324, qui reçoit un message de demande de boucle de système **systemLoop** H.245 ou un message de demande de boucle de voie logique **logicalChannelLoop** H.245, de même qu'une passerelle vers terminaux conformes aux Recommandations UIT-T H.320, H.321 ou H.322, qui reçoit une commande de boucle numérique H.230 en provenance d'une extrémité du RCC, peut assurer elle-même la fonction de bouclage appropriée. La passerelle ne doit pas transmettre ces demandes aux extrémités du réseau. Une passerelle vers terminaux H.324 qui reçoit un message de demande de boucle **mediaLoop** H.245 provenant d'une extrémité du RCC doit transmettre cette demande à l'extrémité du réseau. Une passerelle vers terminaux H.320, H.321, ou H.322 qui reçoit une commande de boucle vidéo Vid-loop ou de boucle audio Aμ-loop H.230 provenant d'une extrémité du RCC doit convertir cette demande dans la demande de boucle **mediaLoop** H.245 appropriée et l'envoyer à l'extrémité du réseau.

Une passerelle vers H.320, H.321 ou H.322, qui reçoit une demande de boucle **mediaLoop** H.245 en provenance d'une extrémité du réseau doit convertir cette demande dans la commande de boucle vidéo ou audio H.230 appropriée et l'envoyer à l'extrémité du RCC.

Une passerelle vers H.324 peut envoyer une demande **systemLoop** ou **logicalChannelLoop** H.245 à l'extrémité du RCC. Une passerelle vers H.320, H.321 ou H.322 peut envoyer une commande de boucle numérique H.230 à l'extrémité du RCC. Si une extrémité du réseau est en communication avec l'extrémité du RCC, le message audio et vidéo envoyé à l'extrémité du réseau peut être renvoyé en boucle sous la même forme, préenregistré pour indiquer la condition de bouclage, ou ne comporter aucune information audio ou vidéo.

11.2 Méthodes de surveillance

Tous les terminaux doivent pouvoir recevoir le message de demande d'information/réponse à une demande d'information (IRQ/IRR) de la Rec. UIT-T H.225.0. Le message de réponse à une demande d'information contient l'identificateur du point TSAP de toutes les voies activées pour la communication en cours, y compris les signaux de commande T.120 et H.245 ainsi que les signaux audio et vidéo. Cette information peut être utilisée par des dispositifs de maintenance tiers pour surveiller les conférences H.323 afin de vérifier le fonctionnement du système.

Annexe A

Messages H.245 utilisés par les extrémités H.323

L'utilisation des messages H.245 par les extrémités H.323 est soumise aux règles suivantes:

- une extrémité ne doit pas être perturbée dans son fonctionnement ni subir un quelconque effet préjudiciable imputable à la réception de messages H.245 qu'elle ne reconnaît pas. Une extrémité qui reçoit une demande, une réponse ou une commande qu'elle ne reconnaît pas doit renvoyer le message "fonction non assurée" (le renvoi de ce message n'est pas nécessaire pour les indications);
- les abréviations utilisées dans les Tableaux A.1 à A.12 sont les suivantes:

  Obl. obligatoire;

  Fac. facultatif;

  Int. interdit;
- un message signalé comme étant obligatoire pour l'extrémité réceptrice indique que cette extrémité doit accepter le message et agir en conséquence. Un message signalé comme étant obligatoire pour l'extrémité émettrice indique que cette extrémité doit émettre le message dans les circonstances appropriées.

Tableau A.1/H.323 – Messages de choix du mode maître ou esclave

Message	Statut message/extrémité réception	Statut message/extrémité émission
Choix du mode maître ou esclave (*determination*)	Obl.	Obl.
Accusé de réception du choix du mode maître ou esclave *(determination acknowledge)*	Obl.	Obl.
Refus du choix du mode maître ou esclave *(determination reject)*	Obl.	Obl.
Abandon du choix du mode maître ou esclave *(determination release)*	Obl.	Obl.

Tableau A.2/H.323 – Messages de capacité du terminal

Message	Statut message/extrémité réception	Statut message/extrémité émission
Ensemble de capacités *(capability set)*	Obl.	Obl.
Accusé de réception d'ensemble de capacités *(capability set acknowledge)*	Obl.	Obl.
Refus d'ensemble de capacités *(capability set reject)*	Obl.	Obl.
Abandon d'ensemble de capacités *(capability set release)*	Obl.	Obl.

Tableau A.3/H.323 – Messages de signalisation de voie logique

Message	Statut message/extrémité réception	Statut message/extrémité émission
Ouverture de voie logique *(open logical channel)*	Obl.	Obl.
Accusé de réception d'ouverture de voie logique *(open logical channel acknowledge)*	Obl.	Obl.
Refus d'ouverture de voie logique *(open logical channel reject)*	Obl.	Obl.
Confirmation d'ouverture de voie logique *(open logical channel confirm)*	Obl.	Obl.
Fermeture de voie logique *(close logical channel)*	Obl.	Obl.
Accusé de réception de fermeture de voie logique *(close logical channel acknowledge)*	Obl.	Obl.
Demande de fermeture de voie *(request channel close)*	Obl.	Fac.
Accusé de réception de demande de fermeture de voie *(request channel close acknowledge)*	Fac.	Fac.
Refus de demande de fermeture de voie *(request channel close reject)*	Fac.	Obl.
Libération de demande de fermeture de voie *(request channel close release)*	Fac.	Obl.

Tableau A.4/H.323 – Messages de signalisation de tableau de multiplexage

Message	Statut
Envoi d'entrée de multiplexage *(multiplex entry send)*	Int.
Accusé de réception d'envoi d'entrée de multiplexage *(multiplex entry send acknowledge)*	Int.
Refus d'envoi d'entrée du multiplexage *(multiplex entry send reject)*	Int.
Libération d'envoi d'entrée de multiplexage *(multiplex entry send release)*	Int.

Tableau A.5/H.323 – Messages de signalisation de demande de tableau de multiplexage

Message	Statut
Demande d'entrée de multiplexage *(request multiplex entry)*	Int.
Accusé de réception de demande d'entrée de multiplexage *(request multiplex entry acknowledge)*	Int.
Refus de demande d'entrée du multiplexage *(request multiplex entry reject)*	Int.
Libération de demande d'entrée de multiplexage *(request multiplex entry release)*	Int.

Tableau A.6/H.323 – Messages de demande de mode

Message	Statut message/extrémité réception	Statut message/extrémité émission
Demande de mode *(request mode)*	Obl.	Fac.
Accusé de réception de demande de mode *(request mode acknowledge)*	Obl.	Fac.
Refus de demande de mode *(request mode reject)*	Fac.	Obl.
Libération de demande de mode *(request mode release)*	Fac.	Obl.

Tableau A.7/H.323 – Messages de temps de propagation aller-retour

Message	Statut message/extrémité réception	Statut message/extrémité émission
Demande de temps de propagation aller-retour *(round trip delay request)*	Obl.	Fac.
Réponse de temps de propagation aller-retour *(round trip delay response)*	Fac.	Obl.

Tableau A.8/H.323 – Messages de boucle de maintenance

Message	Statut message/extrémité réception	Statut message/extrémité émission
Demande de boucle de maintenance *(maintenance loop request)*		
Boucle de système *(system loop)*	Int.	Int.
Boucle de média *(media loop)*	Fac. (Note)	Fac. (Note)

Tableau A.8/H.323 – Messages de boucle de maintenance

Message	Statut message/extrémité réception	Statut message/extrémité émission
Boucle de voie logique *(logical channel loop)*	Int.	Int.
Accusé de réception de boucle de maintenance *(maintenance loop acknowledge)*	Fac.	Fac.
Refus de boucle de maintenance *(maintenance loop reject)*	Fac.	Obl.
Désactivation de commande de boucle de maintenance *(maintenance loop command off)*	Obl.	Fac.
NOTE – Obligatoire dans les passerelles.		

Tableau A.9/H.323 – Messages de demande et de réponse pour conférence

Message	Statut message/extrémité réception	Statut message/extrémité émission
Demande de liste de terminaux *(terminal list request)*	Fac.	Fac.
Suppression d'un terminal (*drop terminal*)	Fac.	Fac.
Demande individuelle d'exercice de la présidence (*make me chair*)	Fac.	Fac.
Annulation de demande individuelle d'exercice de la présidence (*cancel make me chair*)	Fac.	Fac.
Introduction du mot de passe H.243 (*enter H.243 password*)	Fac.	Fac.
Introduction de l'identificateur de terminal H.243 (*enter H.243 terminal ID*)	Fac.	Fac.
Introduction de l'identificateur de conférence H.243 (*enter H.243 conference ID*)	Fac.	Fac.
Demande d'identificateur de terminal (*request terminal ID*)	Fac.	Fac.
Réponse à demande d'identificateur de terminal (*terminal ID response*)	Fac.	Fac.
Réponse à demande d'identificateur de terminal contrôleur multipoint (*MC terminal ID response*)	Fac.	Fac.
Introduction d'adresse par extension (*enter extension address*)	Fac.	Fac.
Réponse à demande d'introduction d'adresse (*enter address response*)	Fac.	Fac.

Tableau A.9/H.323 – Messages de demande et de réponse pour conférence

Message	Statut message/extrémité réception	Statut message/extrémité émission
Réponse à demande de liste de terminaux (*terminal list response*)	Fac.	Fac.
Réponse à demande individuelle d'exercice de la présidence (*make me chair response*)	Fac.	Fac.
Réponse à demande d'identificateur de conférence (*conference ID response*)	Fac.	Fac.
Réponse à demande de mot de passe (*password response)*	Fac.	Fac.

Tableau A.10/H.323 – Commandes

Message	Statut message/extrémité réception	Statut message/extrémité émission
Envoi d'ensemble de capacités de terminal *(send terminal capability set)*	Obl.	Obl.
Chiffrement *(encryption)*	Fac.	Fac.
Contrôle de flux *(flow control)*	Obl.	Fac.
Fin de session *(end session)*	Obl.	Obl.
Commandes diverses		
Egalisation des temps de propagation *(equalize delay)*	Fac.	Fac.
Temps de propagation nul *(zero delay)*	Fac.	Fac.
Commande de mode multipoint *(multipoint mode command)*	Obl.	Fac.
Commande d'annulation de mode multipoint *(cancel multipoint mode command)*	Obl.	Fac.
Arrêt sur image vidéo *(video freeze picture)*	Obl.	Fac.
Mise à jour rapide d'image vidéo *(video fast update picture)*	Obl.	Fac.
Mise à jour rapide de groupe de blocs d'image vidéo *(video fast update GOB)*	Obl.	Fac.
Mise à jour rapide de macroblocs d'image vidéo *(video fast update MB)*	Obl.	Fac.
Compromis spatio-temporel en vidéo *(video temporal spatial trade off)*	Fac.	Fac.
Envoi du signal de synchronisation vidéo pour chaque groupe de blocs *(video send sync every GOB)*	Fac.	Fac.

Tableau A.10/H.323 – Commandes

Message	Statut message/extrémité réception	Statut message/extrémité émission
Annulation de l'envoi du signal de synchronisation vidéo pour chaque groupe de blocs *(video send sync every GOB cancel)*	Fac.	Fac.
Demande d'identificateur de terminal *(terminal ID request)*	Fac.	Fac.
Refus de commande vidéo *(video command reject)*	Fac.	Fac.
Réponse à une demande individuelle d'exercice de la présidence *(make me chair response)*	Fac.	Fac.
Commandes de conférence		
Demande de diffusion individuelle par voie logique personnelle *(broadcast my logical channel me)*	Fac.	Fac.
Annulation de demande de diffusion individuelle par voie logique personnelle *(cancel broadcast my logical channel me)*	Fac.	Fac.
Demande d'attribution au terminal du rôle de diffuseur *(make terminal broadcaster)*	Fac.	Fac.
Annulation de demande d'attribution au terminal du rôle de diffuseur *(cancel make terminal broadcaster)*	Fac.	Fac.
Demande d'envoi d'une source désignée *(send this source)*	Fac.	Fac.
Annulation de demande d'envoi d'une source désignée *(cancel send this source)*	Fac.	Fac.
Abandon en cours de conférence *(drop conference)*	Fac.	Fac.

Tableau A.11/H.323 – Commandes de mode conférence

Message	Statut message/extrémité réception	Statut message/extrémité émission
Commande de mode de communication *(communication mode command)*	Obl.	Fac.
Demande de mode de communication *(communication mode request)*	Fac.	Fac.
Réponse à la demande de mode de communication *(communication mode response)*	Fac.	Fac.

Tableau A.12/H.323 – Indications

Message	Statut message/extrémité réception	Statut message/extrémité émission
Fonction non comprise (*function not understood*)	Obl.	Obl.
Fonction non assurée *(function not supported)*	Obl.	Obl.
Indications diverses		
Voie logique activée *(logical channel active)*	Fac.	Fac.
Voie logique désactivée *(logical channel inactive)*	Fac.	Fac.
Conférence multipoint *(multipoint conference)*	Obl.	Fac.
Annulation de conférence multipoint *(cancel multipoint conference)*	Obl.	Fac.
Communication multipoint sans participant *(multipoint zero comm)*	Fac.	Fac.
Annulation de communication multipoint sans participant *(cancel multipoint zero comm)*	Fac.	Fac.
Statut secondaire multipoint *(multipoint secondary status)*	Fac.	Fac.
Annulation de statut secondaire multipoint *(cancel multipoint secondary status)*	Fac.	Fac.
Indication vidéo prête à être activée *(video indicate ready to activate)*	Fac.	Fac.
Compromis spatio-temporel en vidéo *(video temporal spatial trade off)*	Fac.	Fac.
Macroblocs vidéo non décodés (*video not decoded MBs*)	Fac.	Fac.
Indications de conférence		
Numéro d'extension SBE *(SBE number)*	Fac.	Fac.
Assignation de numéro de terminal *(terminal number assign)*	Obl.	Fac.
Entrée d'un terminal dans la conférence *(terminal joined conference)*	Fac.	Fac.
Départ d'un terminal de la conférence *(terminal left conference)*	Fac.	Fac.
Message vu par au moins un autre participant *(seen by at least one other)*	Fac.	Fac.
Annulation du message vu par au moins un autre participant *(cancel seen by at least one other)*	Fac.	Fac.

Tableau A.12/H.323 – Indications

Message vu par tous *(seen by all)*	Fac.	Fac.
Annulation du message vu par tous *(cancel seen by all)*	Fac.	Fac.
Le terminal que vous voyez *(terminal you are seeing)*	Fac.	Fac.
Demande de prise de parole *(request for floor)*	Fac.	Fac.
Indications du vendeur *(vendor indications)*	Fac.	Fac.
Indication d'emplacement d'un contrôleur multipoint (*MC location indication*)	Obl.	Fac.
Indication de gigue (*jitter indication*)	Fac.	Fac.
Indication de décalage temporel H.223 (*H.223 skew indication*)	Int.	Int.
Indication de décalage temporel maximal H2250 (*H2250MaximumSkewIndication*)	Fac.	Obl.
Indication de nouvelle voie virtuelle ATM (*New ATM virtual channel indication*)	Int.	Int.
Données d'usager (*user input*)	Obl. (pour 0-9, * et #)	Obl. (pour 0-9, * et #)

Les commandes, demandes, etc. non normalisées sont autorisées.

Annexe B

Procédures pour codecs vidéo stratifiés

B.1 Domaine d'application

La présente annexe décrit des améliorations de la présente Recommandation, afin d'y introduire des codecs vidéo stratifiés. La procédure décrite est adaptable par échelons à des conférences multipoints.

B.2 Introduction

Le codage vidéo stratifié est une technique qui permet de transmettre les informations vidéo à l'intérieur de multiples flux de données afin d'obtenir l'échelonnabilité. Celle-ci peut être exprimée en termes de largeur de bande, de coordonnées temporelles, de bruit de fond (rapport SNR, *signal-to-noise ratio*) et/ou de coordonnées spatiales. L'utilisation du codage stratifié dans le cadre de la Rec. UIT-T H.263 est décrite dans l'Annexe O/H.263 de celle-ci. Les conférences peuvent tirer parti de cette caractéristique pour desservir, au moyen d'un seul flux binaire, des extrémités connectées ayant des capacités différentes, ce qui permet d'utiliser plus efficacement la largeur de bande du réseau.

B.3 Méthodes d'échelonnabilité

L'échelonnabilité d'un flux vidéo se rapporte à la production d'un flux qui ne peut être décodé que partiellement en raison de limitations des ressources disponibles. L'on peut rechercher

l'échelonnabilité afin de surmonter des limitations en termes de puissance de calcul ou de largeur de bande disponible.

La Rec. UIT-T H.263 décrit trois types d'échelonnement: temporel, rapport signal sur bruit (SNR, *signal-to-noise ratio*) et spatial. D'autres codecs vidéo peuvent avoir une capacité de stratification analogue. Toutes ces méthodes peuvent être utilisées séparément ou de concert afin de créer un flux binaire échelonnable en plusieurs couches. La résolution, la fréquence de trame et la qualité de l'image ne peuvent augmenter que par ajout de couches d'échelonnement. La couche de base peut être utilisée pour garantir un niveau minimal de qualité d'image. Les extrémités peuvent ensuite faire appel à des couches supplémentaires afin d'augmenter cette qualité d'image en accroissant la fréquence de trame, le format d'affichage ou la précision des images décodées. Le fait d'autoriser plusieurs méthodes d'échelonnement dans une conférence peut augmenter la rentabilité des ressources, en particulier lorsque les extrémités participantes possèdent diverses capacités en termes de puissance de calcul et de largeur de bande. Cela vaut spécialement pour les conférences multipoints et à couplage non déterministe.

B.4 Etablissement de l'appel

L'établissement d'un appel H.323 s'effectue conformément aux procédures décrites au paragraphe 8. La capacité de codage stratifié sera signalée au moyen des méthodes d'échange de capacités H.245. Il existe dans la Rec. UIT-T H.245 des séquences binaires indiquant clairement les méthodes de stratification qui sont prises en charge par les extrémités. Ces dernières doivent faire appel à ces capacités pour signaler les méthodes de stratification exactes qu'elles prennent en charge.

L'utilisation des méthodes d'échange simultané de capacités selon la Rec. UIT-T H.245 doit servir à indiquer les méthodes de stratification qui seront utilisées ensemble pour créer les couches vidéo au moment où celles-ci seront acheminées par au moins deux voies logiques. Il est également possible d'envoyer au moins deux couches vidéo dans une seule voie logique. Les couches vidéo exactes qui seront utilisées sont signalées lors de l'ouverture de voie logique (**openLogicalChannel**) de la façon qui est déjà employée pour indiquer les types de données **dataType** vidéo qui seront utilisés, sauf que l'extrémité doit indiquer les relations d'interdépendance entre la voie logique contenant la couche de base et les voies logiques contenant les couches d'amélioration.

B.5 Utilisation de sessions et de couches de codec en protocole RTP

L'on souhaite autoriser des sessions distinctes en protocole RTP pour les différentes qualités vidéo disponibles. Il y a lieu de considérer la couche de base comme étant la session vidéo primaire, son niveau étant considéré comme donnant la qualité vidéo minimale pouvant être obtenue dans la conférence. Les couches d'amélioration pourront être envoyées par des sessions RTP distinctes. Le paramètre **forward/reverseLogicalChannelDependency**, ajouté à la commande H.245 **openLogicalChannel**, doit être utilisé pour indiquer comment les couches vidéo sont organisées. Cela est décrit dans les paragraphes suivants. Les pointeurs temporels du protocole RTP doivent toujours être les mêmes dans la couche de base et dans toutes les couches d'amélioration qui en dépendent correspondant à une trame, afin de permettre le réassemblage et l'affichage correct.

B.5.1 Association de la session vidéo de base à la session audio pour la synchronisation labiale

Il y a lieu d'associer la session vidéo de base à la session audio correspondant à la piste audio du flux vidéo, afin d'assurer la synchronisation labiale. Cette association s'effectue de la même façon que celle des sessions vidéo non stratifiées existantes avec leurs sessions audio correspondantes: au moyen des paramètres **associatedSessionID** et **sessionID** insérés dans les paramètres **H2250LogicalChannelParameters**. Les couches d'amélioration peuvent aussi être associées à la couche audio ou à la couche de base au moyen du paramètre **associatedSessionID**. L'interdépendance du codage doit être indiquée au moyen des paramètres

forwardLogicalChannelDependency et **reverseLogicalChannelDependency** insérés dans la commande **openLogicalChannel** comme expliqué ci-dessous.

B.5.2 Interdépendance des couches d'amélioration

L'interdépendance des couches d'amélioration peut donner naissance à de nombreux cas complexes, où de multiples couches peuvent contenir de multiples types de trames d'amélioration. L'interdépendance entre couches doit être indiquée au moyen du paramètre **forward/reverseLogicalChannelDependency**, ajouté à la commande H.245 **openLogicalChannel**. L'interdépendance sert à signaler que les données émises sur la voie logique ne peuvent pas être utilisées sans le contenu de la voie logique dont elles dépendent. Par définition, les couches d'amélioration doivent toujours être codées différentiellement par rapport à la couche vidéo qu'elles améliorent et dont elles dépendent donc pour un décodage cohérent. Si une couche d'amélioration est envoyée sur une voie logique distincte, il faut indiquer la couche par rapport à laquelle elle a été codée différentiellement dans le paramètre **forward/reverseLogicalChannelDependency**.

Etant donné que le paramètre **forward/reverseLogicalChannelDependency** permet d'indiquer une voie logique unique, il faut ouvrir les voies logiques dans l'ordre de leurs dépendances, à partir de la couche de base. Une extrémité doit avoir soit émis soit reçu l'acquittement **openLogicalChannelAck** pour toute voie logique utilisée dans un paramètre **forward/reverseLogicalChannelDependency**. Une extrémité ne doit envoyer de commande **openLogicalChannel** pour une voie logique dépendante qu'après ouverture et acquittement de la voie logique dont elle dépend. Les voies logiques interdépendantes peuvent être ouvertes en parallèle. Il faut indiquer que les couches d'amélioration dépendent de la couche la plus élevée qui est requise pour un décodage correct.

En admettant que l'on fait appel à des sessions RTP distinctes pour chaque couche, l'on peut construire l'exemple représenté sur la Figure B.1.

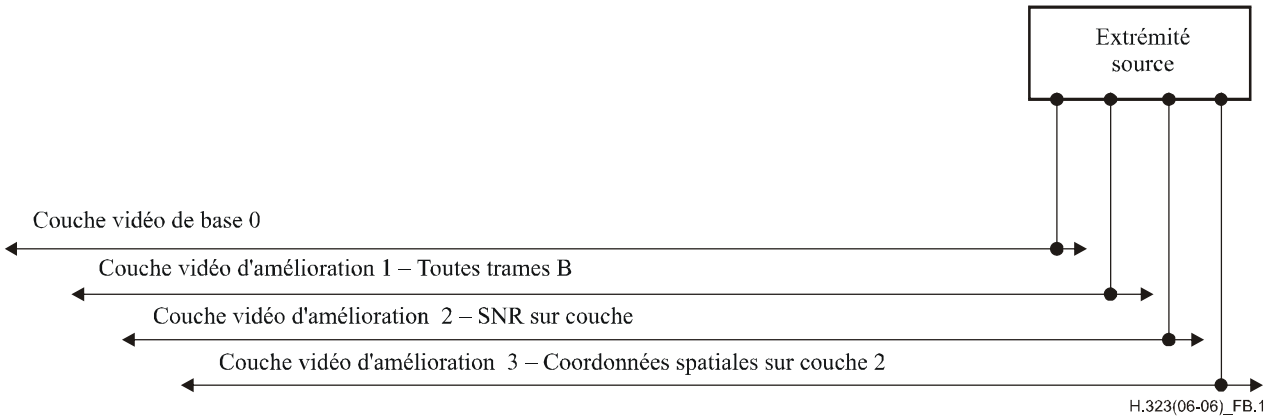


Figure B.1/H.323 – Modèle stratifié en couches vidéo

Dans cet exemple, le modèle stratifié comporte les quatre couches vidéo suivantes:

1) la couche vidéo de base, qui ne dépend d'aucune autre couche et qui est associée à sa couche audio correspondante;

2) la couche d'amélioration de niveau 1, composée de trames de type B, qui dépend de la couche vidéo de base. Cette couche est indiquée comme dépendant de la couche vidéo de base ou couche 0;

3) la couche d'amélioration de niveau 2, qui améliore en terme de rapport SNR la couche vidéo de base (couche 0) et qui ne dépend que de cette couche, ce dont elle porte l'indication;

4) la couche d'amélioration de niveau 3, qui améliore la couche 2 en termes de coordonnées spatiales. Elle dépend du contenu vidéo de la couche 2, ce dont elle porte l'indication et ce qui implique que la couche de base soit également requise.

Dans cet exemple, la voie logique acheminant la couche vidéo de base doit toujours être ouverte en premier. La commande **openLogicalChannel** pour les couches d'amélioration 1 et 2 peut être envoyée en parallèle mais seulement après réception de l'acquittement **openLogicalChannelAck** concernant la voie logique de la couche vidéo de base. La commande **openLogicalChannel** pour la couche d'amélioration 3 ne peut être émise qu'après réception ou émission du message **openLogicalChannelAck** pour la voie logique utilisée pour la couche d'amélioration 2.

B.6 Modèles de stratification possibles

Il existe de nombreuses méthodes permettant de stratifier le flux vidéo et d'organiser les sessions de protocole RTP correspondantes. La raison pour laquelle les couches peuvent devoir être séparées est qu'elles sont utilisées pour échelonner soit la puissance du décodeur soit l'utilisation de la bande passante. Il est parfois souhaitable d'extraire toutes les trames autres que de type B afin de les insérer dans des couches distinctes pouvant être ignorées si elles ne peuvent pas être exploitées. Une caractéristique importante du codec stratifié est qu'à tout moment une extrémité quelconque peut ignorer tout ou partie des couches d'amélioration sans affecter la qualité de la vidéo de base, afin d'assurer un échelonnement en puissance du décodeur.

De même, les couches peuvent devoir être organisées en niveaux d'utilisation de la largeur de bande en fonction des largeurs signalées par les extrémités connectées à la conférence. Celle-ci pourra ainsi interfonctionner avec des conférences multipoints dont les extrémités font appel à des méthodes de connexion qui peuvent limiter la largeur de bande disponible. Elle pourra alors créer une couche fournissant à ces conférences le meilleur flux vidéo possible dans cette bande. Chaque extrémité pourra ensuite ajouter ou retirer des couches selon les variations (dans les deux sens) de la largeur de bande dont il dispose.

B.6.1 Voies logiques et sessions RTP multiples pour un flux stratifié

Si l'échelonnement en largeur de bande est l'objectif recherché lors de la stratification du flux, il convient que chaque couche s'écoule dans une voie logique distincte, avec une session protocolaire RTP distincte. En d'autre termes, ce qui n'était qu'une source vidéo isolée devra désormais être coordonné entre de multiples voies logiques et sessions RTP.

Si l'objectif de la stratification est un échelonnement en puissance de traitement électronique, les couches d'amélioration pourront être envoyées, ainsi que la couche vidéo de base, sur une voie logique et une session RTP uniques.

Si l'objectif est un mélange d'échelonnements en largeur de bande et en puissance de traitement, on pourra envoyer des groupes de couches d'amélioration dans des groupes de voies logiques. Le choix des groupes de couches et de voies dépend des besoins du système. La méthode utilisée pour effectuer ces choix relève de l'implémentation et est hors du domaine d'application de la présente Recommandation.

B.6.2 Incidence d'une couche unique par voie logique et par session RTP

L'incidence de l'utilisation d'une seule voie logique et d'une seule session RTP par couche est que le codeur et le décodeur sont chargés du travail de segmentation et de réassemblage du flux vidéo en fonction du modèle de stratification choisi. Ce modèle est signalé à l'extrémité réceptrice de façon que celle-ci puisse interpréter correctement les informations contenues dans chaque couche. Cette signalisation est effectuée au moyen des capacités H.245 avec une capacité par voie logique pour

décrire suffisamment le modèle de stratification en combinaison avec les interdépendances entre couches. Les modèles de stratification possibles sont signalés au cours de l'échange de capacités, au moyen de la fonction de capacités simultanées de la Rec. UIT-T H.245.

De strictes contraintes de temporisation devront être appliquées pour faire en sorte que les couches soient correctement synchronisées. Pour les flux H.323, cette fonction sera insérée dans le format de la charge utile du protocole RTP.

B.7 Incidence sur les conférences multipoints

L'application la plus probable qui a été envisagée pour la stratification vidéo est celle des conférences multipoints. Dans H.323, cette opération peut être effectuée par un pont de conférence centralisé, utilisé pour le mixage audio et pour le montage vidéo, ou par un modèle décentralisé où chaque extrémité est chargée du montage vidéo et du mixage audio. Dans un cas comme dans l'autre, le contrôleur multipoint doit normalement exécuter la fonction de signalisation (au moyen de la commande **communicationModeCommand**) du modèle de stratification choisi pour la conférence.

Pour qu'une extrémité puisse recevoir une couche vidéo, une voie logique contenant cette couche doit toujours être ouverte. La décision d'ouvrir une voie logique peut être prise soit par le contrôleur multipoint soit par l'extrémité émettrice d'une commande **openLogicalChannel**. Si un contrôleur ou une extrémité décide de ne pas ouvrir de voie logique, ce point doit rejeter la commande **openLogicalChannel** lorsqu'elle est présentée. Le contrôleur ou l'extrémité ne peut offrir qu'une voie logique qui correspond à un type de données (**dataType**) pris en charge par l'extrémité réceptrice.

Lors de l'implémentation des fonctions permettant le fonctionnement des codecs stratifiés, un contrôleur multipoint peut suivre deux modèles. Si le contrôleur ne prend pas de décisions quant aux voies logiques à ouvrir, le modèle peut être dit "à contrôleur impartial". Dans ce cas, le contrôleur multipoint offre tous les flux médias à toutes les extrémités sans tenir compte d'une éventuelle notification de qualité de service. Lorsque au contraire le contrôleur multipoint prend la décision d'appliquer strictement la qualité de service, il s'agit du modèle dit "à contrôleur décisionnel". Ces modèles sont développés ci-dessous.

B.7.1 Modèle à contrôleur impartial

Le modèle à contrôleur multipoint impartial ne dépend pas des compléments apportés à l'ensemble des capacités relatives à la qualité de service (QS) du terminal. Il peut donc autoriser une implémentation plus simple des contrôleurs multipoints. Dans ce cas, c'est à l'extrémité qu'il appartient de déterminer si elle dispose d'une largeur de bande suffisante pour accepter les voies logiques offertes par le contrôleur multipoint. Si la largeur nécessaire dépasse les capacités de transmission de l'extrémité ou du réseau sous-jacent, celui-ci peut rejeter la voie logique. Cette méthode nécessite que l'extrémité soit informée de la largeur de bande disponible dans le réseau. Il y a lieu que le contrôleur multipoint indique tous les médias disponibles dans la commande **communicationModeCommand**.

B.7.2 Modèle à contrôleur décisionnel

Le modèle à contrôleur multipoint décisionnel dépend des compléments apportés à l'ensemble des capacités relatives à la qualité de service (QS) du terminal. Cela a déjà été proposé et est en cours d'étude. Le contrôleur multipoint peut ensuite examiner les capacités des extrémités en termes de QS et n'offrir que les voies logiques dont la QS est compatible avec celle de ces points. Chaque extrémité devra déterminer sa qualité de service disponible en début de conférence puis l'indiquer au moyen des capacités de QS définies par les études en cours.

Dans le modèle à contrôleur décisionnel, celui-ci peut envoyer une commande **communicationModeCommand** à une extrémité qui n'affiche que les sessions conformes aux

capacités de cette extrémité en termes de QS. De cette façon, le contrôleur multipoint peut régir strictement l'utilisation de la largeur de bande.

B.7.3 Conférence multipoint contenant des extrémités ayant différentes largeurs de bande

Dans le modèle où la conférence multipoint contient des extrémités ayant différentes largeurs de bande disponibles, la stratification devra être adaptée en fonction de ces niveaux de bande passante. A cette fin, deux modèles pourront être utilisés, le premier étant représenté sur la Figure B.2.

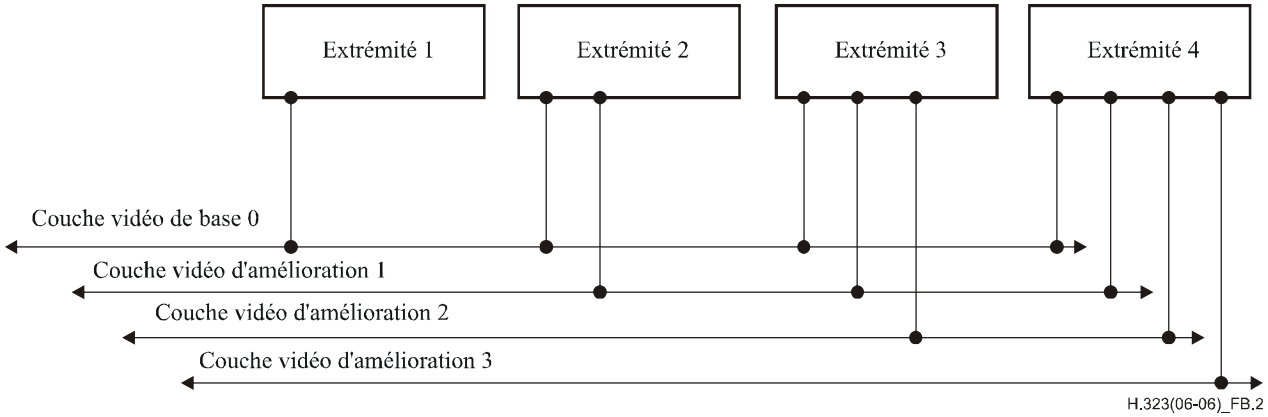


Figure B.2/H.323 – Rattachement des extrémités à une ou à plusieurs couches en fonction de la largeur de bande

Dans ce cas, les extrémités sont rattachées à la couche vidéo de base et aux couches d'amélioration jusqu'à occuper toute la largeur de bande désirée. Chaque couche d'amélioration se trouve dans une voie logique distincte. Les extrémités sont chargées de la recombinaison des couches afin de créer le flux vidéo. L'extrémité émettrice doit avoir la capacité de combinaison en largeur de bande de tous les flux dont il est la source. Dans ce cas, chaque extrémité doit avoir communiqué un ensemble de capacités différent. Le contrôleur multipoint examinera ces capacités ainsi que la qualité de service puis créera un modèle de stratification susceptible d'exploiter au mieux les capacités et la largeur de bande disponibles aux extrémités. Cette stratification est indiquée dans la commande de mode de communication (**communicationModeCommand**) au moyen de l'indication **sessionDependency** insérée dans l'entrée de table **communicationModeTableEntry**. Le champ **sessionDependency** est activé par le contrôleur multipoint afin d'indiquer le moment où une session dépend d'une autre session pour un décodage cohérent de ses données. Cette information sera traduite en numéros de voie logique (**logicalChannelNumbers**) lors de l'ouverture d'une voie logique interdépendante, en fonction des voies logiques déjà ouvertes.

Dans le cas ci-dessus, le modèle du contrôleur décisionnel permettra à celui-ci d'offrir aux extrémités les voies logiques qui correspondent aux couches qui correspondent aux capacités de ces points. Le contrôleur multipoint n'offrira à l'extrémité 1 que la voie logique correspondant à la couche vidéo de base. Il n'offrira à l'extrémité 2 que les voies logiques correspondant à la couche vidéo de base et à la couche d'amélioration vidéo 1. Il offrira à l'extrémité 3 trois voies logiques correspondant aux couches vidéo de base plus deux couches d'amélioration, et il offrira à l'extrémité 4 toutes les voies logiques de flux vidéo.

Dans le cas du modèle du contrôleur impartial, celui-ci offrira à toutes les extrémités toutes les voies logiques compatibles avec leurs capacités en termes de type de données (**dataType**). Les extrémités refuseront toute voie logique qui les obligerait à dépasser leurs capacités en termes de largeur de bande.

Un deuxième modèle de stratification est décrit à la Figure B.3. Dans ce modèle, chaque voie logique contient un flux vidéo totalement indépendant.

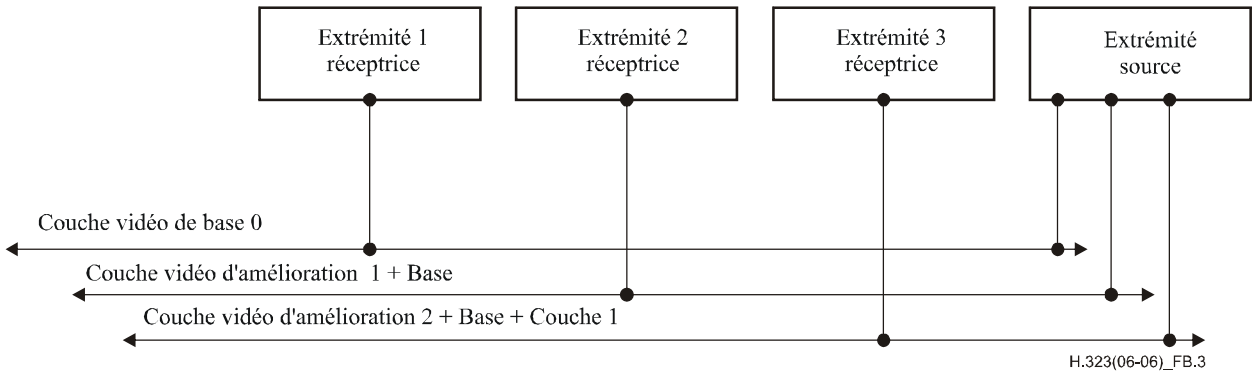


Figure B.3/H.323 – Rattachement des extrémités à une seule couche en fonction de la largeur de bande

Dans ce cas, l'extrémité ne doit se connecter qu'à la voie logique qui correspond à la largeur de bande dont il dispose. Ce flux se compose de toutes les couches qui construisent le flux vidéo en fonction de la largeur de la voie logique. Cette méthode élimine la tâche de recombinaison vidéo par les extrémités mais impose à l'émetteur de produire plusieurs flux vidéo. Il s'agit d'une utilisation moins efficace des ressources du réseau car les couches d'amélioration comprennent toutes les couches inférieures.

Pour exécuter une synchronisation labiale appropriée, il y a lieu que toute session contenant la couche vidéo de base soit associée à la session audio correspondant à sa piste audio, au moyen de l'identificateur **associatedSessionID** contenu dans les paramètres **H2250LogicalChannelParameters**. Dans l'exemple de la Figure B.2, il convient que la session vidéo de base soit associée à la session audio pour la synchronisation labiale. Dans l'exemple représenté à la Figure B.3, les trois sessions vidéo devraient être associées à la session audio pour assurer la synchronisation labiale, étant donné que ces trois sessions contiennent la couche vidéo de base.

B.8 Utilisation de la qualité de service du réseau pour les flux vidéo stratifiés

Plusieurs caractéristiques importantes, relatives à la nature du codage stratifié, sont à prendre en considération lors de l'utilisation de la qualité de service du réseau pour l'acheminement des flux vidéo à codage stratifié. Une couche d'amélioration ne peut pas être décodée correctement sans recevoir les couches dont elle dépend. Les couches d'amélioration vidéo peuvent être ignorées sans que cela ait d'incidence sur le décodage de la couche dont elles dépendent.

Si l'on en dispose, la qualité de service du réseau peut servir à donner la garantie qu'un flux vidéo sera acheminé par le réseau. Comme les couches vidéo peuvent être acheminées dans des flux différents, acheminés sur des connexions distinctes dans le réseau, différents niveaux de qualité de service peuvent être utilisés selon chaque couche vidéo. La qualité de service utilisée dans les flux vidéo stratifiés devrait être spécifiée lors de l'ouverture de chaque voie logique.

Il importe qu'une couche vidéo dépendante possède les informations dont elle dépend au moment où cette couche dépendante va être décodée. Cela conduit aux règles générales suivantes concernant l'utilisation de la qualité de service:

1) les couches dépendantes qui sont acheminées avec la qualité de service du réseau devraient trouver la même qualité de service sur la couche dont elles dépendent;
2) la couche de base devrait être acheminée avec la qualité de service du réseau si d'autres couches vidéo de la conférence doivent être acheminées avec un certain niveau de qualité de service;

3) plus la couche vidéo est proche de la couche de base, plus élevé doit être le niveau des garanties d'acheminement.

Annexe C

Flux H.323 en mode ATM

C.1 Introduction

Une option d'amélioration permet aux extrémités H.323 d'établir, sur des réseaux en mode ATM utilisant la couche AAL 5, des flux médias à niveau de qualité de service garanti.

C.2 Domaine d'application

La présente annexe spécifie une méthode améliorée d'application de la H.323 à la couche AAL 5. La Rec. UIT-T H.323 peut toujours être appliquée en mode ATM au moyen de la méthode IP sur ATM. Mais cela est moins efficace que d'utiliser directement les voies virtuelles (VC, *virtual channel*) de couche AAL 5 pour le transport des flux audio et vidéo conformes à la H.323. Lorsque les flux médias circulent directement sur la couche AAL 5, ils peuvent bénéficier de circuits virtuels en mode ATM à niveau de qualité garantie.

La présente annexe conserve l'utilisation d'un protocole de réseau en mode paquet pour les communications H.245 et H.225.0 afin d'assurer l'interopérabilité avec les extrémités H.323 qui utilisent un protocole de réseau en mode paquet pour tous les flux (sur ATM ou sur un autre support). L'interopérabilité avec des extrémités H.323 normalisées est assurée, sans qu'une passerelle soit nécessaire, par l'utilisation d'abord du mode d'exploitation de base, dans lequel une extrémité envoie des flux de médias sur un service de datagramme au moyen d'un protocole de réseau en mode paquet, par exemple UDP/IP sur ATM. En mode de base, la qualité de service n'est pas toujours disponible dans le réseau si l'infrastructure protocolaire du réseau en mode paquet n'a pas été remise à niveau.

C.2.1 Conférences point à point

La présente annexe spécifie une méthode de communication point à point entre deux extrémités H.323 au moyen de circuits virtuels de couche AAL 5 pour les flux médias. Le protocole nécessaire pour entrer dans ce mode est spécifié, de même que les éléments d'information à utiliser en signalisation ATM.

C.2.2 Communications multipoints par pont de conférence

Il s'ensuit que des communications multipoints par pont de conférence peuvent exister entre plusieurs extrémités H.323 utilisant des circuits virtuels de couche AAL 5 pour les flux médias. Actuellement, aucun mécanisme n'est spécifié pour prendre en charge les communications multipoints décentralisées H.323 au moyen de la capacité point à multipoint ATM. Ce point fera l'objet d'un complément d'étude.

C.2.3 Interopérabilité H.323 avec extrémités utilisant le protocole IP

L'interopérabilité est garantie avec une extrémité utilisant le protocole IP pour l'ensemble de la connexion H.323. La présente annexe définit des méthodes permettant à une extrémité de détecter si un mécanisme est présent pour prendre en charge l'option d'utiliser directement la couche AAL 5. Une extrémité conforme à la présente annexe doit accepter les flux audio et vidéo qui peuvent apparaître sur des circuits virtuels AAL 5 ou sur des accès UDP/IP.

C.3 Architecture

L'architecture protocolaire de base du système est représentée à la Figure C.1. Elle utilise le protocole IP en mode ATM pour l'acheminement des messages H.225.0 et H.245 ainsi que pour la partie des flux audio et vidéo en protocole RTCP. Cette architecture applique directement la couche AAL 5 aux flux audio et vidéo en protocole RTP.

NOTE – Les flux médias H.323, comprimés en paquets de longueur variable conformément à la Rec. UIT-T H.225.0, sont facilement mappés à la couche AAL 5. Il serait difficile de les mapper à la couche AAL 1 et cette possibilité ne présente pas d'avantage évident.

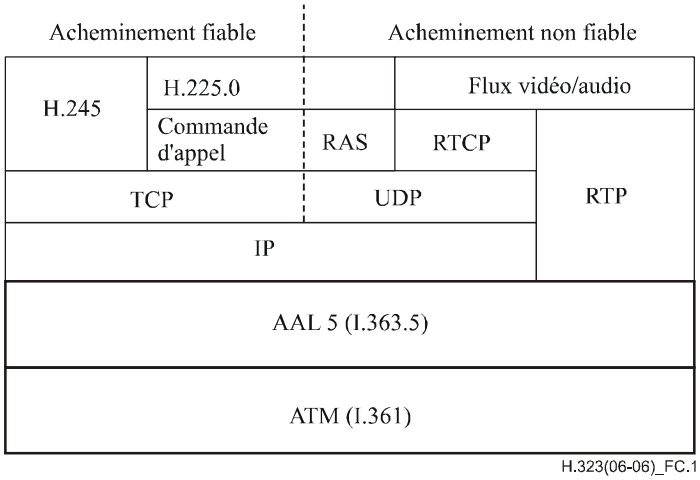


Figure C.1/H.323 – Architecture des flux H.323 sur la couche AAL 5 du mode ATM

C.3.1 Aperçu général du système

L'architecture du système est conçue pour faire usage de la Rec. UIT-T H.323 et des protocoles qui y sont actuellement spécifiés. Elle est également conçue pour faire usage des services couramment disponibles sur la couche AAL 5 du mode ATM.

C.3.2 Interfonctionnement avec d'autres extrémités conformes à des Recommandations UIT-T de la série H

L'interfonctionnement avec d'autres extrémités selon la série H doit être assuré par l'emploi de passerelles telles que décrites dans la Rec. UIT-T H.323. S'ils souhaitent faciliter l'utilisation directe des circuits virtuels de la couche AAL 5 par les extrémités H.323, les vendeurs de passerelles auront besoin de prendre en charge les méthodes décrites dans la présente annexe.

Il y a lieu de noter que l'interfonctionnement avec d'autres extrémités H.323 en protocole IP ne nécessite pas de passerelle.

C.3.3 Communications H.225.0 en protocole IP sur réseau ATM

Les communications H.225.0 nécessitent que les protocoles TCP/IP et UDP/IP utilisent l'une des méthodes disponibles pour le protocole IP sur réseau ATM. Aucune préférence n'est exprimée ici quant à la méthode à utiliser avec le protocole IP sur réseau ATM. Si deux extrémités utilisent, sur le même segment de réseau, différentes méthodes IP sur ATM, ces points doivent compter sur des routeurs IP pour expédier leurs paquets.

L'extrémité doit activer la réception par les accès en protocole TCP identifiés comme tels selon la Rec. UIT-T H.225.0. Si l'extrémité doit être utilisée sur un réseau comportant un portier, il y a lieu que cette extrémité utilise les méthodes décrites dans la Rec. UIT-T H.225.0 pour rechercher un portier et pour s'y inscrire, ce qui exige la prise en charge de la multidiffusion en protocole UDP. Si

celle-ci n'est pas disponible sur le réseau, l'extrémité peut être préconfigurée avec l'adresse ou les adresses de portiers.

Les méthodes décrites dans la Rec. UIT-T H.225.0, combinées avec une méthode IP sur ATM, doivent être utilisées pour établir la voie de commande H.245 en protocole TCP/IP.

C.3.4 Commandes H.245 en protocole TCP/IP sur mode ATM

Une fois que la voie de commande H.245 fiable a été établie au moyen des méthodes décrites dans la Rec. UIT-T H.225.0, des voies additionnelles sont établies pour les flux audio, vidéo et données sur la base du résultat de l'échange de capacités H.245 au moyen des procédures d'ouverture de voie logique H.245.

C.3.5 Adressage pour flux audiovisuels

La Rec. UIT-T H.323 donne la capacité d'établir les flux audio et vidéo vers une adresse différente de celle qui est contenue dans les voies de commande H.245. Cette possibilité est intéressante puisqu'une voie en protocole TCP/IP est établie vers une adresse IP et que les flux audio et vidéo sont, facultativement, envoyés directement à une adresse ATM par protocole RTP sur couche AAL 5.

La Rec. UIT-T H.323 donne également la capacité d'adresser le flux RTCP séparément du flux RTP. Le flux en protocole RTCP doit continuer à être acheminé vers une adresse IP, bien que le flux en protocole RTP soit acheminé vers une adresse ATM.

C.3.6 Capacités de transport ajoutées à l'ensemble de capacités de transport

Pour le fonctionnement de flux H.323 sur la couche AAL 5, un complément est apporté à l'ensemble de capacités de transport (**TransportCapability**) conformes à la Rec. UIT-T H.245. Il s'agit des capacités de couche Transport comme la prise en charge de la capacité de transfert ATM (DBR, SBR1, SBR2, SBR3, ABT/DT, ABT/IT, ABR) telles que définies dans la Rec. UIT-T I.371. Les terminaux qui n'envoient pas ce nouveau paramètre de capacité ne doivent pas faire usage des nouvelles méthodes décrites dans la présente annexe. Les informations relatives aux capacités de transport (**TransportCapability**) peuvent être envoyées dans l'ensemble de capacités du terminal destiné à la phase d'échange des capacités. Elles figurent aussi dans le message **openLogicalChannel.**

C.3.7 Eléments de signalisation ATM

C.3.7.1 Adresse ATM

L'adresse ATM d'un flux RTP doit être indiquée dans le sous-champ **mediaChannel** des paramètres **H2250LogicalChannelParameters** du message H.245 **openLogicalChannelAck** (ou **OpenLogicalChannel** en cas de connexion rapide). Le sous-champ **mediaChannel** du paramètre d'adresse **UnicastAddress** ou **MulticastAddress** doit être rempli par les 20 octets de l'adresse de type point NSAP du système d'extrémité ATM.

L'utilisation de E.164 pour l'adresse est gérée par incorporation dans la partie IDP (AFI = 0x45) d'une adresse de point NSAP. Un numéro international de type E.164 est alors nécessaire.

C.3.7.2 Numéro de port

Le champ **portNumber** du message **openLogicalChannel** est acheminé dans l'élément d'information GIT, conformément à [33], dont le format est spécifié au § C.4.1.1. Ce champ permet au terminal récepteur d'associer le circuit virtuel ATM à la voie logique RTP appropriée.

Pour assurer la compatibilité amont avec les extrémités H.323 version 2 (et suivantes), les extrémités doivent également pouvoir utiliser l'information B-HLI, selon l'Annexe C de la Rec. UIT-T H.323 version 2, pour acheminer le champ **portNumber** du message **openLogicalChannel**. Une extrémité H.323 version 3 (ou postérieure) ne doit utiliser l'information

B-HLI que lorsqu'elle sait au préalable que l'extrémité terminale est un point H.323 version 2. Si la version H.323 de l'extrémité terminale n'est pas connue, par exemple pour l'établissement d'une communication par la procédure de connexion rapide, les extrémités doivent initialement chercher à établir le circuit virtuel en mode ATM au moyen de l'élément d'information GIT pour acheminer le champ **portNumber**. Si l'établissement de la connexion échoue, l'extrémité doit de nouveau essayer d'établir la communication en utilisant l'élément d'information B-HLI au lieu de l'élément GIT. Si l'établissement du circuit virtuel au moyen de l'élément d'information HLI échoue également, le terminal doit supposer que la connectivité ATM n'est pas disponible et doit revenir à l'utilisation d'un protocole RTP/UDP/IP pour voies de médias. Le format de l'élément d'information B-HLI est spécifié au § C.4.1.2.

C.3.8 Flux audiovisuels en protocole RTP sur couche AAL 5

L'application de la commande **openLogicalChannel** dans un message H.245 déclenche l'établissement d'une connexion. Les flux audio et vidéo sont ensuite orientés vers l'adresse ATM de destination. La longueur de l'unité de transmission maximale (MTU, *maximum transmission unit*) doit être signalée dans l'élément d'information Paramètres AAL. Le choix de l'unité MTU peut avoir une incidence sur l'efficacité du système en raison de la mise en paquets dans la couche AAL 5. Les règles de mise en paquets pour la couche AAL 5 sont contenues dans la Rec. UIT-T I.363.5. Si la valeur hors couche AAL 5 par défaut (1536 octets) est utilisée, l'unité MTU est mise en paquets dans 33 cellules ATM et la dernière cellule AAL 5 ne contient que le bourrage et le numéro de couche AAL 5. Il convient d'utiliser le champ d'adresse dans le paramètre **mediaChannel** afin de déterminer s'il y a lieu d'ouvrir un circuit virtuel ATM ou un accès UDP.

Si l'établissement du circuit virtuel ATM échoue, l'extrémité doit refaire un essai en utilisant le protocole RTP/RTCP et un protocole de transport de couche supérieure comme le protocole UDP.

En option, on peut utiliser la compression des en-têtes RTP, comme indiqué dans la section 2 du document AF-SAA-0124.000 [32], mais cela doit être négocié au moyen de **mediaTransportType**.

C.3.8.1 Voies logiques unidirectionnelles

La Rec. UIT-T H.323 ne tient pas compte du sens inverse d'une voie logique unidirectionnelle. Cependant, une caractéristique importante des circuits virtuels ATM point à point est qu'ils sont intrinsèquement bidirectionnels. L'utilisation des deux sens d'un circuit virtuel ATM est donc souhaitable. Sinon, les flux audio et vidéo auront chacun besoin d'être envoyés sur un circuit virtuel différent, un pour chaque sens de transmission.

Il est recommandé que les extrémités conformes à la présente annexe ouvrent des voies logiques bidirectionnelles pour leurs flux médias: cela réduit à deux le nombre de circuits virtuels de la couche AAL 5 dans les situations typiques: un circuit virtuel pour l'audio et un autre pour la vidéo.

C.3.8.2 Voies logiques bidirectionnelles

Si l'utilisation dans les deux sens est indiquée, l'extrémité réceptrice doit envoyer un acquittement **openLogicalChannelAck** (ou la commande **openLogicalChannel** dans le cas d'une connexion rapide) puis doit détecter l'ouverture d'un circuit virtuel ATM par l'autre extrémité. Lorsque ce circuit est établi, l'extrémité peut en utiliser le sens inverse pour le type de média indiqué dans la commande **openLogicalChannel**. L'extrémité qui lance la commande **openLogicalChannel** est celle qui doit ouvrir le circuit virtuel ATM.

Si la qualité de service doit être utilisée, elle doit être limitée à la capacité **H2250Capability** déclarée par l'autre extrémité. La qualité de service choisie est signalée dans le cadre de l'établissement d'un circuit virtuel ATM.

Si les deux extrémités ont en attente des commandes **openLogicalChannel** pour la même session média, ces décisions sont prises au moyen des méthodes de maître/esclave décrites dans la Rec. UIT-T H.245.

C.3.8.3 Longueur d'une unité de transmission maximale

La longueur maximale d'une unité MTU pour la couche AAL 5 est de 65 535 octets. Au titre de **H2250Capability**, la longueur de l'unité MTU peut être spécifiée dans l'échange de capacités au cours de l'établissement d'appel H.245. La longueur maximale d'unité MTU doit être égale dans les deux sens: il s'agit de la plus petite des valeurs, locale et distante, spécifiées lors de l'échange de capacités.

La longueur d'unité MTU est signalée comme étant la longueur maximale d'une unité CPCS-PDU dans la couche AAL 5 pour un circuit virtuel en mode ATM.

C.3.8.4 Protocole RTCP empilé sur protocole IP en mode ATM

Il est obligatoire d'ouvrir la voie logique du trafic RTCP sur un accès UDP/IP, au moyen du protocole IP en mode ATM. Le protocole RTCP n'est pas autorisé à utiliser directement un circuit virtuel de couche AAL 5.

C.3.9 Considérations (facultatives) concernant la qualité de service

C.3.9.1 Classes de qualité de service définies dans la Rec. UIT-T I.356

La Rec. UIT-T I.356 définit quatre classes de qualité de service: la classe 1 (sévère), la classe 2 (tolérante), la classe 3 (à deux niveaux) et la classe U. Le Tableau C.1 récapitule les différences entre ces classes de qualité de service.

Tableau C.1/H.323 – Définitions provisoires des classes de qualité de service et des objectifs de performance du réseau

	CTD	**CDV à 2 points**	**CLR (0+1)**	**CLR (0)**	**CER**	**CMR**	**SECBR**
Objectif par défaut	Pas de valeur	Pas de valeur	Pas de valeur	Pas de valeur	4×10^{-6}	1/jour	10^{-4}
Classe 1 (sévère)	400 ms	3 ms	3×10^{-7}	Pas de valeur	Valeur par défaut	Valeur par défaut	Valeur par défaut
Classe 2 (tolérante)	U	U	10^{-3}	Pas de valeur	Valeur par défaut	Valeur par défaut	Valeur par défaut
Classe 3 (à 2 niveaux)	U	U	U	10^{-5}	Valeur par défaut	Valeur par défaut	Valeur par défaut
Classe U	U	U	U	U	U	U	U
CDV: variation du temps de transfert de cellules; CER: taux d'erreurs de cellules; CLR: taux de perte de cellules; CMR: débit de cellules insérées à tort; CTD: temps de transfert de cellules; SECBR: taux de blocs de cellules sévèrement erronés; U: non spécifié/non limité.							

C.3.9.2 Capacité de transfert en mode ATM (définie dans la Rec. UIT-T I.371)

La capacité de transfert en mode ATM (ATC, *ATM transfer capability*), définie dans la Rec. UIT-T I.371 comme étant un ensemble de paramètres et de procédures de couche ATM, est destinée à prendre en charge un modèle de service sur couche ATM ainsi qu'une série de classes de qualité de service associées. Les capacités ATC de commande en boucle ouverte (débits DBR et SBR) ainsi que les capacités ATC commandées en boucle fermée (transfert ABT et débit ABR) sont spécifiées dans la Rec. UIT-T I.371. Le débit SBR se subdivise en débits SBR1, SBR2 et SBR3, selon le mode de traitement des cellules à bit de priorité CLP = 0/1. Le transfert ABT se subdivise en ABT/DT et ABT/IT, selon l'utilisation de la négociation du débit cellulaire en termes de blocs. Le Tableau C.2 résume l'association des capacités ATC avec les classes de QS.

Tableau C.2/H.323 – Association des capacités ATC avec les classes de QS (d'après le Tableau 3/I.356)

Capacités de transfert ATM (ATC)	DBR, SBR1, ABT/DT, ABT/IT	DBR, SBR1, ABT/DT, ABT/IT	SBR2, SBR3, ABR	Toute ATC
Classe de QS applicable	Classe 1 (sévère)	Classe 2 (tolérante)	Classe 3 (à 2 niveaux)	Classe U
ABR: débit disponible; ABT/DT: transfert de blocs ATM avec transmission retardée; ABT/IT: transfert de blocs ATM avec transmission immédiate; DBR: débit déterministe; SBR1: configuration 1 du débit statistique; SBR2: configuration 2 du débit statistique; SBR3: configuration 3 du débit statistique.				

C.3.9.3 Capacité de transfert en large bande définie dans la Rec. UIT-T Q.2961.2

Les codes des capacités de transfert en large bande (BTC, *broadband transfer capability*): DBR, BTC5, BTC9, BTC10 et SBR1, contenus dans l'élément d'information Capacité support large bande, sont définis dans la Rec. UIT-T Q.2961.2. Les combinaisons valides de classe support, de capacité support large bande et de paramètres Descripteur de trafic ATM sont spécifiées dans l'Annexe A/Q.2961.2. Dans le message Setup, l'utilisateur peut spécifier les capacités BTC selon le trafic qu'il produit et selon l'usage prévu des services de couche Réseau. Le Tableau A.1/Q.2961.2 énumère trois combinaisons valides pour la classe support BCOB-A, huit combinaisons pour la classe BCOB-C et treize combinaisons pour la classe BCOB-X ou le mode relais de trames.

C.3.9.4 Ouverture de voies virtuelles

L'extrémité qui a émis la commande **openLogicalChannel** acceptée est responsable de l'ouverture du circuit virtuel ATM. La prise en charge de la QS dans le circuit VC en mode ATM est signalée au moment de son établissement. Si celui-ci est correct, le réseau en mode ATM fournir une QS garantie pendant la durée de vie du circuit virtuel ouvert. La qualité de service est spécifiée en termes d'éléments d'information (IE, *information element*) selon la Rec. UIT-T Q.2931, y compris les éléments Descripteur de trafic ATM et Capacité support large bande.

C.3.9.5 Utilisation du débit DBR

Le type de trafic ATM disponible le plus probable est un débit constant utilisant le mode statistique (DBR, *deterministic bit rate*). Cette utilisation est signalée dans le cadre de l'élément d'information Capacité support large bande en mode ATM (classe support = "BCOB-A"). L'utilisation d'un autre type de trafic ATM, comme le débit SBR avec pointage temporel exigé de bout en bout [classe support = "BCOB-X" et champ BTC = "SBR1 (0010011)"] est également possible.

C.3.9.6 Réglage du débit cellulaire approprié

Il importe de régler les paramètres corrects de débit cellulaire dans l'élément d'information Descripteur de trafic ATM. Le débit cellulaire crête peut être déduit des paramètres d'échange de capacités H.245 et de la longueur des paquets dans le format de charge utile en protocole RTP. Pour les flux vidéo, le champ **maxBitRate** peut être utilisé à partir de la capacité vidéo (**H261VideoCapability**) ou H.263 (**H263VideoCapability**) afin de déterminer le débit cellulaire du mode ATM. Pour les flux audio, la capacité audio choisie implique le débit à utiliser. Par exemple, l'utilisation de la valeur **g711Ulaw64k** implique l'utilisation d'une voie audio à 64 kbit/s, tandis que la valeur **g728** indique l'utilisation d'une voie à 16 kbit/s. Le format de charge utile en protocole RTP indique la longueur des paquets. A chaque paquet, il faut ajouter le surdébit de paquet en couche AAL et tout bourrage éventuellement nécessaire pour satisfaire aux règles de mise en paquets dans la couche AAL. Il en résulte un débit de surcharge qui est associé à la longueur du paquet ainsi encapsulé dans la couche AAL et à la fréquence de la surcharge due à cette encapsulation.

Le débit et la mise en paquets des données à envoyer, conformément aux règles de mise en paquets de la couche AAL, déterminent le débit cellulaire. La mise en paquets définira le nombre réel de cellules qui doivent être envoyées pour un flux de données donné à un certain débit. Le choix de l'unité MTU peut affecter la mise en paquets, comme expliqué au § C.3.8.

C.4 Article relatif au protocole

C.4.1 Eléments d'information pour la signalisation ATM

C.4.1.1 Transport des informations génériques

Paramètre de l'élément d'information	Valeur	Notes
Norme/application liée à l'identificateur (octet 5)	0000 1011	Rec. UIT-T H.323
Type d'identificateur (octet 6)	0000 1011	**portNumber** H.245
Longueur de l'identificateur (octet 6.1)	0000 0010	2 octets
Valeur de l'identificateur (octets 6.2-6.3)	**portNumber** H.245	**portNumber** H.245 de renvoi à 16 bits codés binaires

Les extrémités H.323 version 3 (ou postérieures) doivent positionner l'indicateur d'action IE de l'élément d'information GIT pour "libérer l'appel", selon les règles définies au § 4.5.1/Q.2931. Dans ce cas si l'extrémité terminale ne prend pas en charge le codage de l'élément d'information GIT, elle refusera l'appel avec un code de cause 100 en raison du *caractère non valide du contenu de l'élément d'information* d'après les critères définis au § 5.7.2/Q.2931. En cas de refus de la tentative d'établissement en mode ATM VC du fait que l'extrémité terminale ne peut identifier le contenu de l'élément GIT, l'établissement d'une communication par voie virtuelle sera refusé avec un code de cause 99 *élément d'information non existant ou non implémenté* tel qu'indiqué au § 5.7.2/Q.2931.

Il convient de noter que le champ **portNumber** de la commande H.245 a une longueur de 16 bits seulement.

Le **portNumber** H.245 est utilisé par l'extrémité réceptrice pour associer le circuit virtuel ATM ou la voie logique RTP appropriée. L'extrémité qui lance la commande **openLogicalChannel** est l'extrémité qui ouvre le circuit virtuel ATM. Il se pourrait que l'extrémité initiatrice sélectionne un **portNumber** H.245 déjà utilisé par l'extrémité réceptrice, mais cela entraînerait une défaillance de la procédure OLC.

De plus, l'accès RTCP de réception est également spécifié par l'extrémité initiatrice par voie de conséquence. La Rec. UIT-T H.323 spécifie que les données RTCP correspondantes passent par un numéro d'accès UDP égal au numéro **portNumber** H.245 majoré de 1. Il se peut que le numéro d'accès qui en résulte pour le RTCP soit en cours d'utilisation au niveau de l'extrémité réceptrice étant donné que le numéro **portNumber** H.245 est sélectionné par l'extrémité initiatrice.

En raison des difficultés qui précèdent, l'extrémité réceptrice doit avoir le choix du **portNumber** H.245. Si le champ **portNumber** n'est pas spécifié dans le message **openLogicalChannel** l'extrémité réceptrice doit spécifier un champ **portNumber** dans le message **openLogicalChannelAck** (ou **openLogicalChannel** en mode connexion rapide). Il est recommandé que l'extrémité émettrice ne spécifie pas le champ **portNumber** dans le message **openLogicalChannel** exigeant ainsi que l'extrémité réceptrice en spécifie un dans le message **openLogicalChannelAck** (ou **openLogicalChannel** en mode connexion rapide).

Le champ **portNumber** du message **openLogicalChannel** sert à sélectionner le numéro **portNumber** H.245. L'extrémité réceptrice utilise ce numéro **portNumber** H.245 pour associer le circuit virtuel ATM à la voie logique RTP appropriée. Si l'extrémité réceptrice estime que le numéro **portNumber** H.245 en question est inapproprié, il peut sélectionner un nouveau numéro

portNumber H.245 et utiliser le champ **portNumber** du message **openLogicalChannelAck** (ou **openLogicalChannel** en cas de connexion rapide) pour indiquer la nouvelle valeur de l'extrémité initiatrice. Le champ du **portNumber** H.245 sélectionné est acheminé dans l'élément d'information GIT. Cela permet au côté réception d'associer le circuit virtuel ATM à la voie logique RTP appropriée.

Le numéro d'accès de l'association de circuits virtuels est représenté dans l'ordre des octets du réseau dans les octets 6.2 et 6.3 de l'élément GIT (c'est-à-dire que l'octet 6.2 contient le bit de plus fort poids et l'octet 6.3 le bit du plus faible poids).

C.4.1.2 Elément d'information Couche supérieure large bande

Paramètres de cet élément d'information	Valeur	Notes
Longueur du contenu de l'élément B-HLI (octets 3-4)	3	
Type d'information couche supérieure (octet 5)	"0000 0001"	Propre à l'utilisateur
Information couche supérieure (octets 5-7)	**portNumber** H.245	**portNumber** H.245 à codage binaire avant sur 16 bits

L'élément d'information B-HLI est utilisé uniquement à des fins de compatibilité amont avec les extrémités H.323 version 2, tel qu'indiqué au § C.3.7.2.

C.4.1.3 Paramètres de la couche d'adaptation ATM

Paramètres de l'élément d'information	Valeur	Notes
Type de la couche AAL (octet 5)	"0000 0101"	AAL 5
Taille max. vers l'avant de la SDU CPCS de couche AAL 5 (octets 6.1-6.2)	Taille MTU	La plus petite des deux valeurs **mTUsize** données par les listes **QOSCapability.atmParms** locale et distante
Taille max. vers l'arrière de la SDU CPCS de couche AAL 5 (octets 7.1-7.2)	Taille MTU	Comme vers l'avant
Type SSCS (octet 8.1)	"0000 0000"	SSCS nulle

C.4.1.4 Elément d'information Capacité support large bande ATM

a) Dans le cas où le type de trafic ATM dans la commande H.245 est à la valeur "DBR":

Paramètres de cet élément d'information	Valeur	Notes
Classe support	BCOB-A	
Sensibilité à la mutilation	Sensible à la mutilation	
Configuration de la connexion dans le plan d'usager	Point à point	

b) Dans le cas où le type de trafic ATM dans la commande H.245 est à la valeur "SBR1" avec pointage temporel de bout en bout exigé:

Paramètres de cet élément d'information	Valeur	Notes
Classe support	BCOB-X	
Capacité support large bande	"0010011" (SBR1)	SBR1 avec pointage temporel de bout en bout requis
Sensibilité à la mutilation	Sensible à la mutilation	
Configuration de la connexion dans le plan d'usager	Point à point	

C.4.2 Utilisation des commandes H.245

L'établissement d'une communication H.323 au moyen de flux médias sur couche AAL 5 s'effectue comme dans le mode de base H.323 sur protocole IP. La différence est que l'échange effectué de commandes **openLogicalChannel** devrait conduire à l'établissement d'un circuit virtuel sur couche AAL 5. C'est ce qui est illustré dans les Figures C.2 et C.3, respectivement pour l'utilisation unidirectionnelle et bidirectionnelle d'un circuit virtuel.

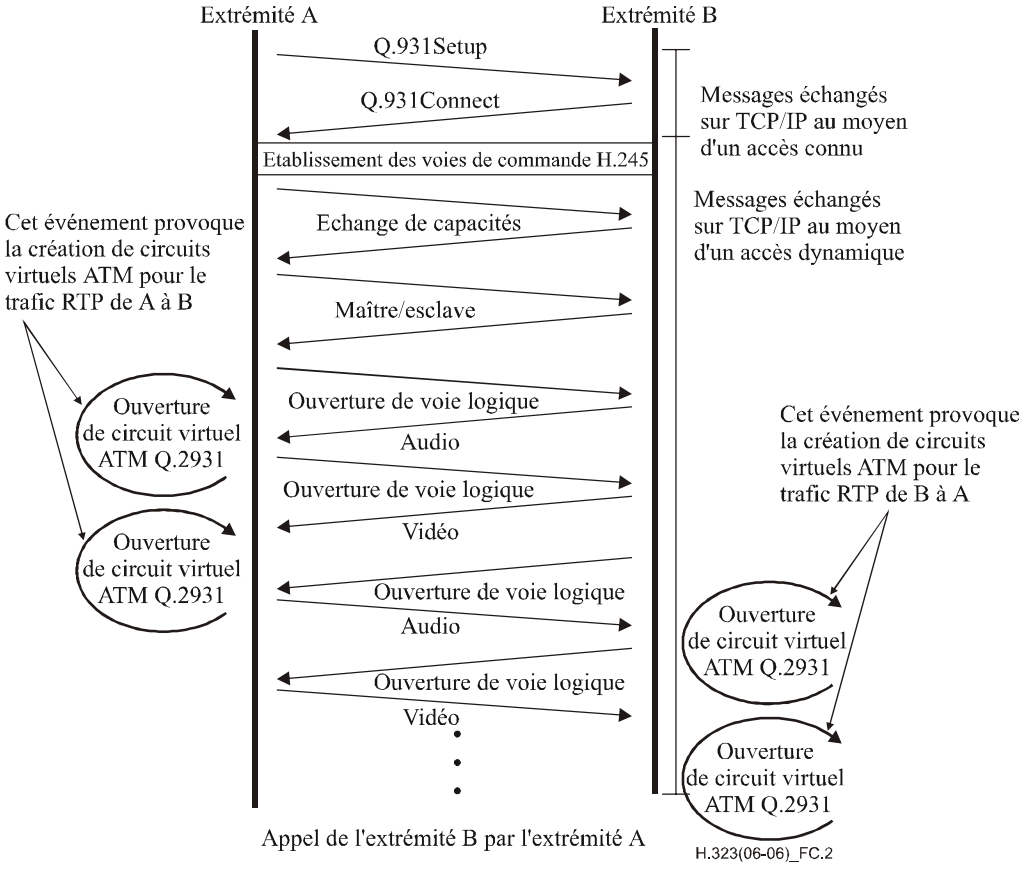


Figure C.2/H.323 – Etablissement d'une communication H.323 montrant l'utilisation unidirectionnelle d'un circuit virtuel ATM

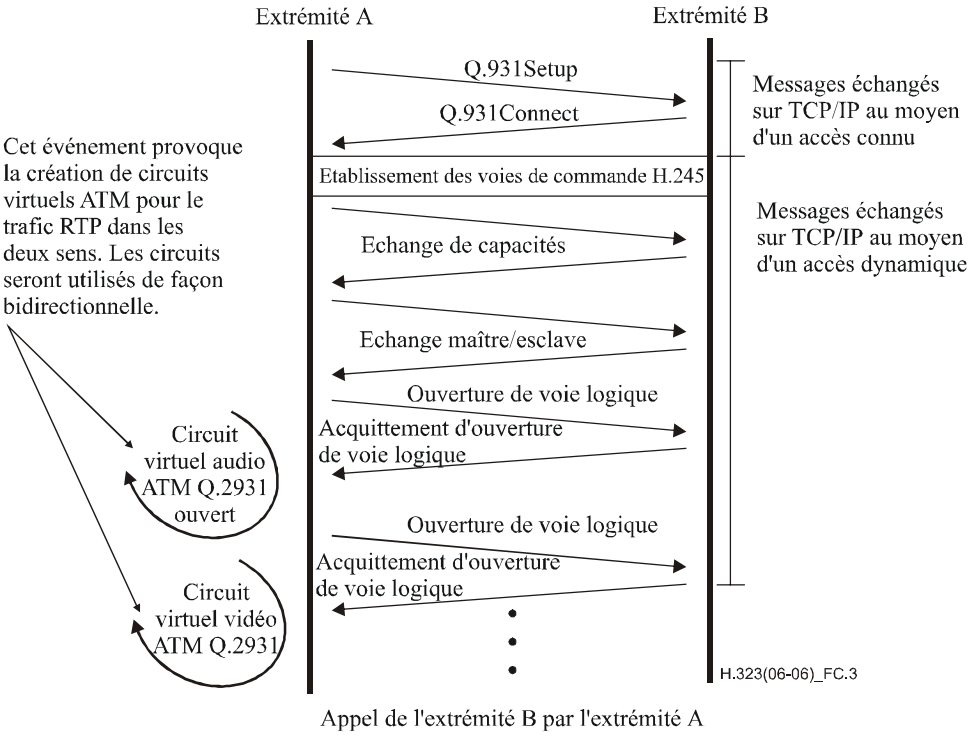


Figure C.3/H.323 – Etablissement d'une communication H.323 montrant l'utilisation bidirectionnelle d'un circuit virtuel ATM

Il convient de noter que les établissements de circuits virtuels en mode ATM ne se produiront que dans un seul sens si l'on utilise des voies logiques bidirectionnelles. Dans ce cas, l'extrémité acquittant l'ouverture de voie logique **openLogicalChannel** rattachera simplement la connexion ATM entrante à une session RTP au moyen du numéro d'accès pour association de circuits virtuels.

C.4.3 Utilisation du protocole RTP

Les protocoles RTP et RTCP sont définis dans l'Annexe A/H.225.0. Le protocole RTCP est actuellement requis pour toutes les connexions H.323 et l'est donc aussi lors de l'utilisation d'un circuit virtuel de couche AAL 5. Le protocole RTCP est acheminé par protocole UDP/IP et non directement par circuit virtuel de couche AAL 5.

C.4.4 Interfonctionnement avec les flux H.323 en protocole IP

Etant donné que les communications H.225.0 et H.245 sont en protocole IP, l'extrémité sera en mesure de recevoir des appels issus de toute autre extrémité correctement connectée au réseau IP. Il est possible que des extrémités H.323 soient utilisées sur un réseau en mode ATM ne prenant pas en charge les méthodes décrites dans la présente annexe. Ces points suivront strictement la méthode de base consistant à utiliser le protocole UDP/IP pour les flux audiovisuels. Dans ce cas, l'extrémité ne déclarera pas les nouvelles capacités de transport **transportCapabilities** lors de l'échange H.245 et refusera d'ouvrir des voies logiques au moyen des circuits virtuels ATM adressés.

Le protocole d'ouverture de voie logique **openLogicalChannel** de type AAL 5 au moyen de circuits virtuels de voie logique pour flux audiovisuels ne devrait être utilisé que si les capacités reçues ont indiqué que la méthode de la présente annexe sont prises en charge. Si ce paramètre de capacité n'est pas présent dans l'ensemble de capacités du terminal, il y a lieu que l'extrémité n'utilise que le protocole UDP/IP en mode ATM pour l'ouverture de ses voies logiques **openLogicalChannel**. Cela garantira que cette extrémité pourra communiquer avec d'autres points prenant en charge la présente Recommandation mais pas nécessairement les méthodes de la présente annexe.

Annexe D

Télécopie en temps réel sur systèmes H.323

D.1 Introduction

Actuellement, la télécopie et la parole sont généralement transmises par l'intermédiaire du RTPC avec la même infrastructure d'appel et d'adressage. Il est fortement souhaitable d'aller dans le même sens dans le cadre de la présente Recommandation. A un haut niveau, la télécopie peut être considérée comme une autre forme de trafic en temps réel semblable à un certain trafic vocal. Cela semble approprié, étant donné que toute télécopie provenant du RTPC et entrant dans un réseau de transmission par paquets via une passerelle devrait logiquement être traitée de manière similaire à la parole si le client attend un service de transmission en temps réel, garanti de bout en bout. L'utilisation de la messagerie électronique ou d'un autre service d'enregistrement et retransmission pour la transmission de télécopie conduit à un nouveau service sortant du cadre de la présente Recommandation, qui définit un protocole en temps réel. Bien entendu, les constructeurs peuvent souhaiter fournir une passerelle avec repli vers un service d'enregistrement et retransmission en cas d'échec de l'appel de télécopie en temps réel. Le moment où cette décision est prise, la manière dont elle est prise et les moyens par lesquels un service de télécopie par enregistrement et retransmission est implémenté sortent du cadre de la présente Recommandation.

La Rec. UIT-T T.38 [55] définit un protocole de transmission de télécopie par Internet consistant à échanger des messages et des données entre passerelles de télécopie raccordées via un réseau IP. La présente annexe utilise la Rec. UIT-T T.38. La communication entre passerelles et télécopieurs G3/G4 sort du cadre de la Rec. UIT-T T.38. Le modèle de référence de la Rec. UIT-T T.38 est représenté sur la Figure D.1 avec trois scénarios. Dans le premier scénario, les deux télécopieurs du Groupe 3 (G3FE, *group 3 facsimile equipment*) traditionnels sont raccordés virtuellement par l'intermédiaire de passerelles une fois que les appels dans le RTPC sont établis. L'établissement de la session T.30 [54] et la négociation des capacités sont effectués entre les terminaux. Dans le deuxième scénario, le télécopieur traditionnel du Groupe 3 est raccordé à un télécopieur compatible Internet (IAF, *Internet aware fax*).

Le télécopieur compatible Internet est directement raccordé au réseau IP. Dans le troisième scénario, les deux télécopieurs compatibles Internet sont directement raccordés au réseau IP. Dans tous les scénarios, on utilise des paquets T.38 dans le réseau IP pour communiquer les informations de télécopie T.4/T.30. Le transport de paquets T.38 se fait selon TCP/IP ou UDP/IP, avec utilisation du mécanisme H.323.

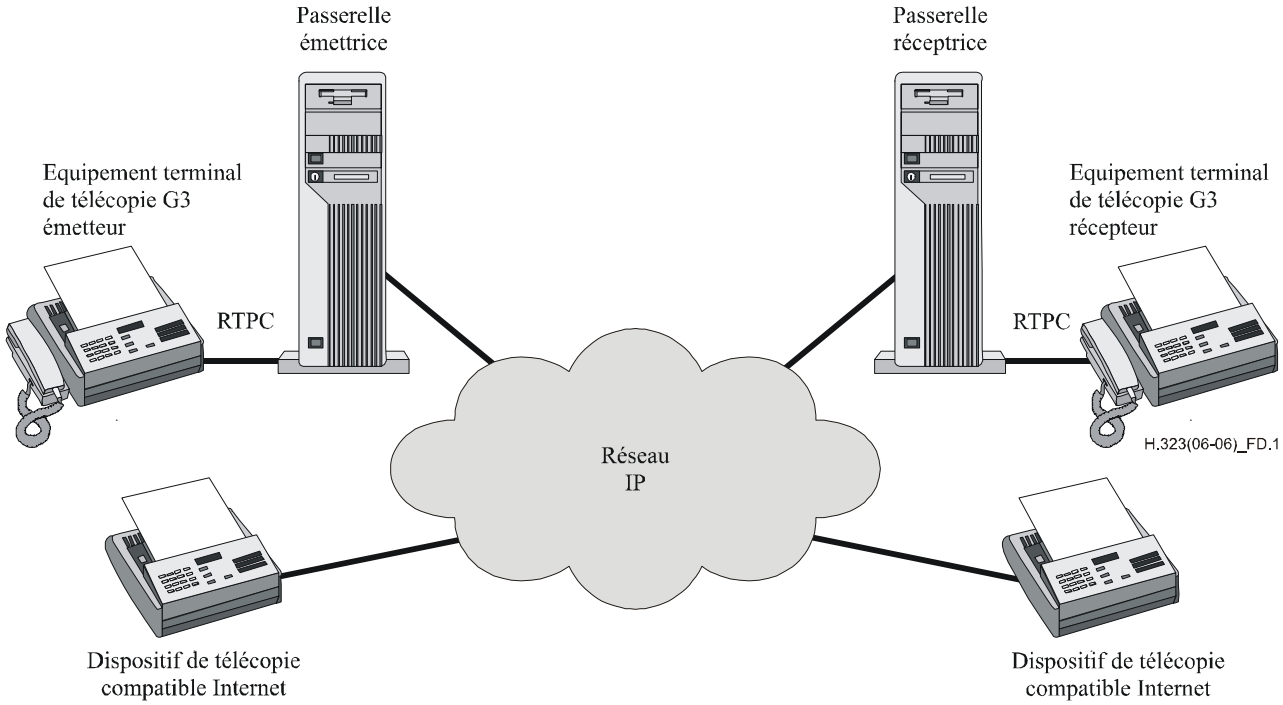


Figure D.1/H.323 – Modèle pour la transmission de télécopie sur des réseaux IP

D.2 Domaine d'application

La présente annexe porte sur l'utilisation des procédures H.323 pour transférer des paquets T.38 en temps réel sur un réseau IP. Les entités H.323 prenant en charge des capacités de télécopie doivent utiliser la Rec. UIT-T T.38 pour assurer des services de télécopie en temps réel, comme décrit dans la présente annexe.

Les extrémités H.323 dotées de capacités de télécopie doivent accepter l'utilisation des protocoles TCP et UDPTL tels que décrits dans la Rec. UIT-T T.38 et peuvent facultativement accepter le RTP. L'Annexe B/T.38 décrit un terminal qui est doté de capacités T.38 uniquement et qui prend en charge un sous-ensemble de messages H.245 utilisant la tunnellisation de messages H.245. Toutefois, le terminal décrit dans l'Annexe B/T.38 peut interfonctionner avec un terminal de type Annexe D/H.323 en utilisant la "procédure de connexion rapide" indiquée au § 8.1.7 et les procédures indiquées au § 8.2.1 (encapsulation de messages H.245 dans des messages de signalisation d'appel H.225.0). Les terminaux de type Annexe B/T.38 interfonctionnent avec les terminaux H.323 sans être conformes à la présente Recommandation. Un terminal H.323 qui prend en charge les procédures de la présente annexe doit interfonctionner avec les terminaux de type Annexe B/T.38.

D.3 Procédures applicables à l'ouverture de voies pour l'envoi de paquets T.38

La procédure de connexion rapide est utilisée pour décrire les procédures H.323 applicables à l'ouverture de voies pour le transport de paquets T.38. La séquence traditionnelle peut aussi être utilisée, même si elle n'est pas décrite ici.

D.3.1 Ouverture de voie pour signaux vocaux

Zéro, une (voie de l'émetteur au récepteur ou voie du récepteur à l'émetteur) ou deux (voie de l'émetteur au récepteur et voie du récepteur à l'émetteur) voies logiques pour signaux vocaux peuvent être ouvertes en fonction des capacités de l'émetteur et du récepteur. Si une voie pour signaux vocaux est souhaitée, elle doit être ouverte conformément aux procédures spécifiées au

§ 8.1.7 "Procédure de connexion rapide". La prise en charge des signaux vocaux par les applications de télécopie n'est pas obligatoire dans la présente annexe.

D.3.2 Ouverture de voies pour la télécopie

Deux voies logiques unidirectionnelles fiables ou non fiables (voie de l'émetteur au récepteur et voie du récepteur à l'émetteur) doivent être ouvertes comme représenté sur la Figure D.2 ou, facultativement, une seule voie bidirectionnelle fiable doit être ouverte comme représenté sur la Figure D.3 pour le transfert de paquets T.38. Ce transfert peut se faire selon le protocole TCP ou selon le protocole UDP. En général, l'utilisation du protocole TCP est plus efficace lorsque la largeur de bande pour les communications par télécopie est limitée. Par ailleurs, l'utilisation du protocole UDP peut être efficace lorsque la largeur de bande pour les communications par télécopie est suffisante.

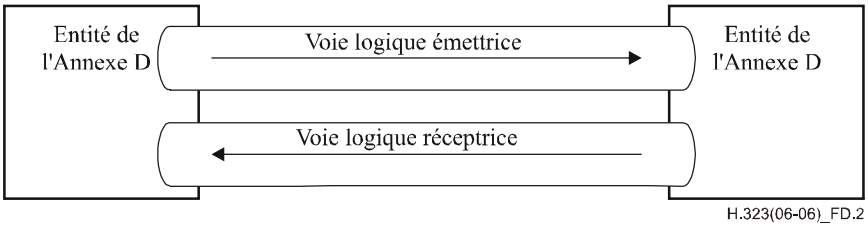


Figure D.2/H.323 – Paire de voies unidirectionnelles

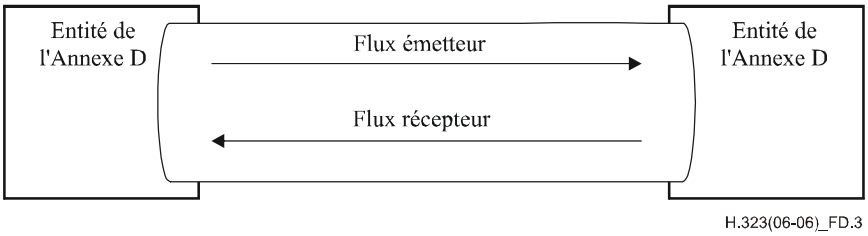


Figure D.3/H.323 – Voie bidirectionnelle unique

NOTE – Dans la première version de la présente annexe, il n'était pas possible d'utiliser une seule voie bidirectionnelle fiable. Afin de conserver la rétrocompatibilité, l'extrémité peut spécifier la prise en charge de voies bidirectionnelles fiables en insérant la SÉQUENCE d'options **t38FaxTcpOptions** et en donnant la valeur "TRUE" au champ **t38TCPBidirectionalMode**. Si l'autre extrémité ne comporte pas la SÉQUENCE **t38FaxTcpOptions**, l'extrémité doit partir du principe qu'une seule voie bidirectionnelle fiable n'est pas prise en charge pour le protocole T.38 et qu'elle doit utiliser soit deux voies unidirectionnelles fiables soit des voies non fiables.

Le terminal émetteur spécifie un port TCP/UDP dans la structure **OpenLogicalChannel** de l'élément **fastStart** du message *Setup*. Le terminal récepteur doit indiquer son port TCP (ou UDP) dans la structure **OpenLogicalChannel** de l'élément **fastStart** comme indiqué au § 8.1.7 "Procédures de connexion rapide".

Le récepteur doit ouvrir un port TCP/UDP selon les préférences de l'émetteur. Si le terminal émetteur préfère le protocole UDPTL, RTP ou le protocole TCP, il doit indiquer sa préférence en ordonnant des propositions dans la séquence **fastStart** conformément au § 8.1.7.1. Le terminal récepteur peut choisir le protocole de transport – TCP ou UDP – en renvoyant les propositions souhaitées dans les structures **OpenLogicalChannel** de l'élément **fastStart** du message *Connect*.

Les Figures D.4 et D.5 montrent la signalisation utilisée pour ouvrir des voies unidirectionnelles et bidirectionnel au moyen de la procédure FastConnect.

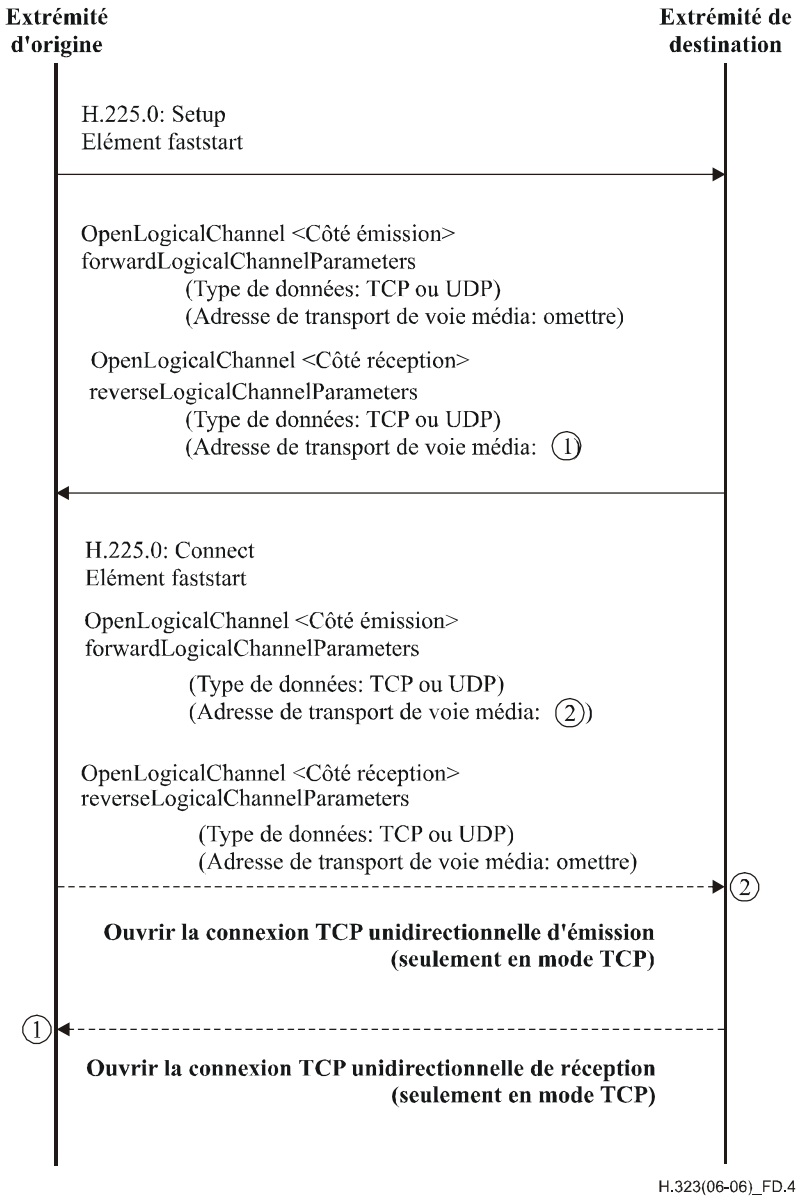


Figure D.4/H.323 – Deux voies unidirectionnelles avec connexion rapide

Dans l'exemple ci-dessus, les voies T.38 sont proposées comme UDPTL ou TCP. Pour proposer une voie logique unidirectionnelle qui utilise le protocole RTP pour transporter les paquets T.38, le paramètre d'ouverture de voie logique **dataType** sera fixé à **audioData** et devra inclure les capacités génériques de transport dans la voie audio H.245 pour la T.38 comme spécifié dans l'Annexe G/T.38.

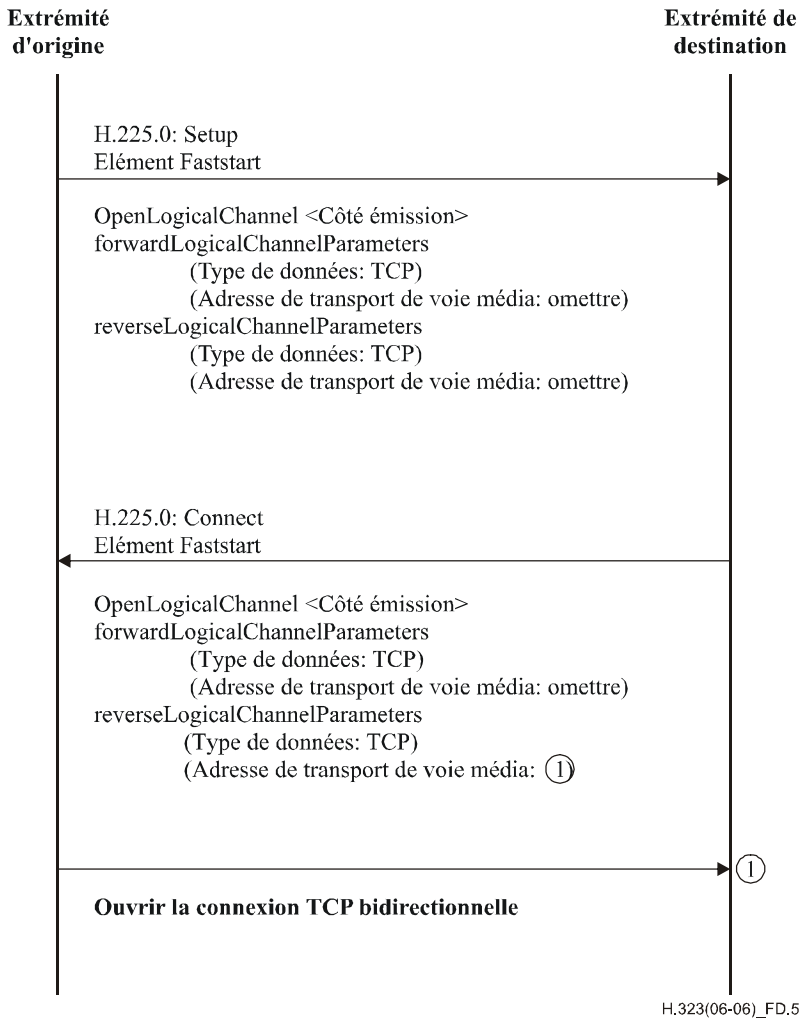


Figure D.5/H.323 – Une seule voie bidirectionnelle fiable avec connexion rapide

D.3.3 Transmission de tonalités DTMF

Des tonalités DTMF doivent être envoyées par intermédiaire des terminaux conformes à l'Annexe D/H.323 au moyen de l'indication **UserInputIndication** pour interagir avec des terminaux de type Annexe B/T.38. Des terminaux conformes à l'Annexe D/H.323 peuvent envoyer des tonalités DTMF dans la bande avec les signaux vocaux ou via RFC 2833, lorsque les terminaux de type Annexe B/T.38 n'interviennent pas dans la communication.

D.4 Procédures autres que "FastConnect"

Il convient de noter que, dans le cas d'une connexion autre que "FastConnect", les procédures **OpenLogicalChannel** normales fondées sur la Rec. UIT-T H.245 peuvent être utilisées pour ouvrir et fermer les voies pour la télécopie UDPTL, RTP et TCP (voir § 6.2.8.2). Les procédures H.245 relatives au mode tunnel peuvent aussi être utilisées pour ouvrir et fermer les voies. A noter également que les procédures H.245 en mode autre que "FastConnect" et sans mise en tunnel ne s'appliquent pas dans le cas de l'interfonctionnement avec la Rec. UIT-T T.38.

Les Figures D.6 et D.7 montrent la signalisation utilisée pour ouvrir des voies unidirectionnelles et bidirectionnelles lorsque l'on n'utilise pas les procédures "FastConnect".

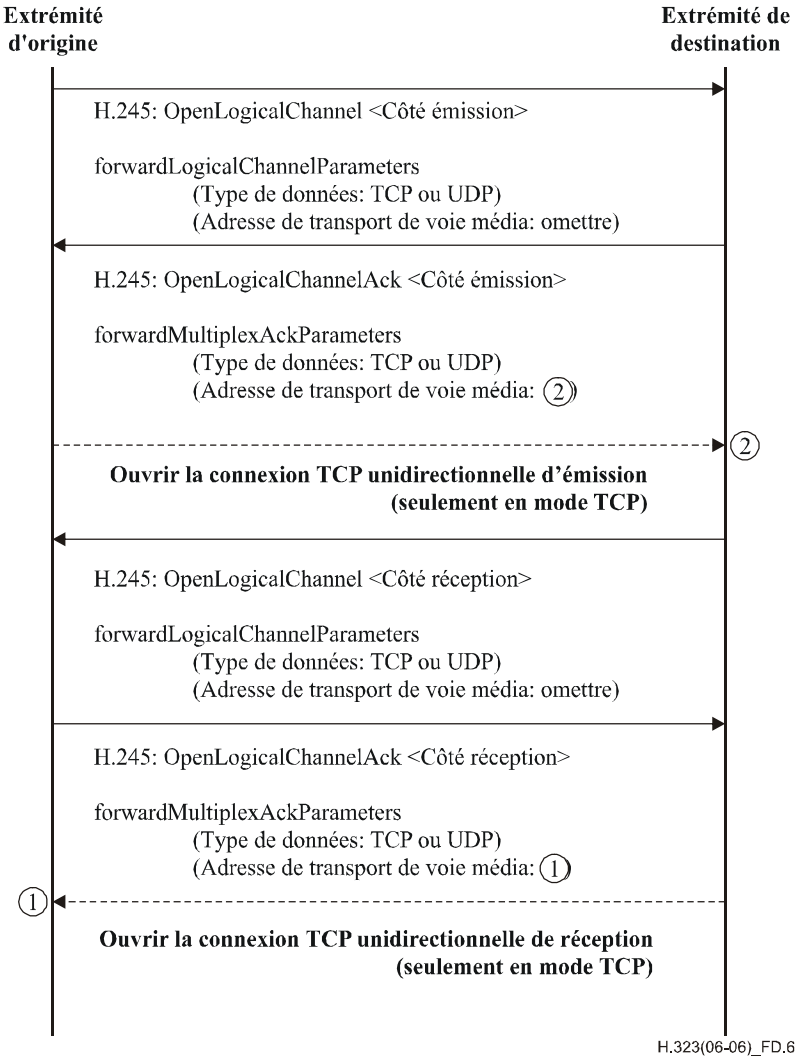


Figure D.6/H.323 – Deux voies unidirectionnelles sans connexion rapide

Dans l'exemple ci-dessus, les voies T.38 sont proposées comme UDPTL ou TCP. Pour proposer une voie logique unidirectionnelle qui utilise le protocole RTP pour transporter les paquets T.38, le paramètre d'ouverture de voie logique **dataType** sera fixé à **audioData** et devra inclure les capacités génériques de transport dans la voie audio H.245 pour la T.38 comme spécifié dans l'Annexe G/T.38.

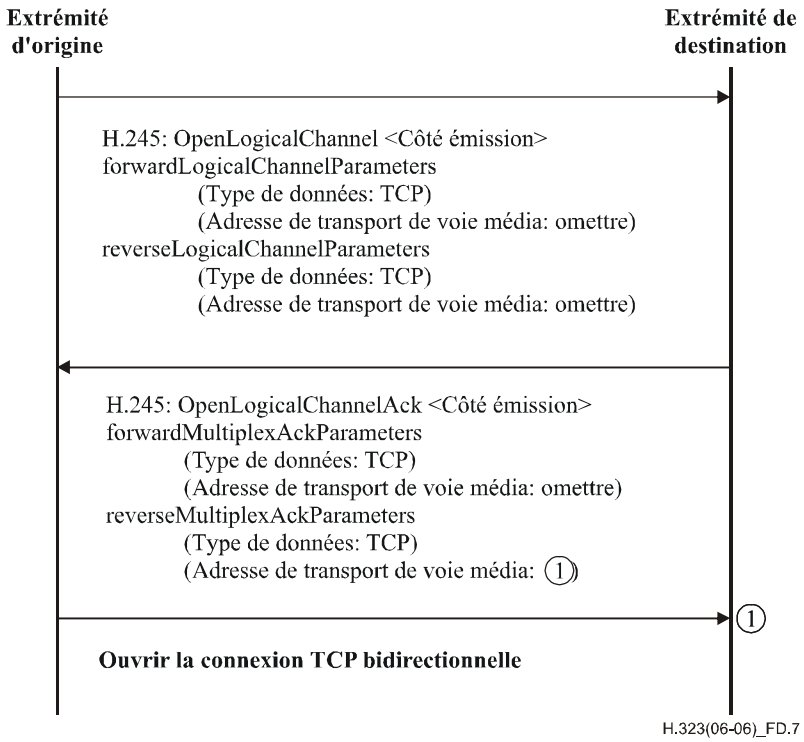


Figure D.7/H.323 – Une seule voie bidirectionnelle sans connexion rapide

D.5 Remplacement d'un flux audio existant par un flux fax T.38

Une extrémité qui souhaite remplacer un flux audio existant par un flux fax doit utiliser le mécanisme suivant à cette fin.

Une fois que la communication audio a été établie – idéalement par l'emploi des procédures de connexion rapide et avant la réception du message CONNECT – L'extrémité qui souhaite remplacer le flux audio par un flux fax T.38 doit lancer les procédures H.245 par tunnellisation si ces procédures n'ont pas déjà été lancées.

Au cours de l'échange de capacités H.245, chaque extrémité doit signaler sa capacité à recevoir et à émettre un flux fax T.38 en insérant le champ **t38fax** de la structure **DataApplicationCapability** et facultativement, en insérant les capacités génériques de transport dans la voie audio T38RTP spécifiées dans l'Annexe G/38. La présence de ce champ indique que l'extrémité distante possède la capacité de prendre en charge le mode fax T.38.

Il convient de noter que le message Connect peut arriver pendant que les procédures H.245 se déroulent. Une fois que les procédures H.245 sont terminées et que le message Connect a été reçu, chaque extrémité peut détecter les tonalités de télécopie (par exemple CNG ou CED) ou la présence d'une porteuse V.21 et des fanions HDLC. Des scénarios types pour la détection d'appel de télécopie repose sur l'analyse de la tonalité appelante CNG et une réponse à la tonalité de réponse CED et/ou le déclenchement des procédures de télécopie en utilisant les porteuses V.21 et les fanions HDLC. A noter que dans certaines implémentations, la présence de la tonalité CNG ou CED est optionnelle. Par conséquent, les deux extrémités doivent prendre un rôle actif afin de détecter convenablement la télécopie.

Lors de l'utilisation de deux voies de télécopie unidirectionnelles, l'extrémité qui a détecté la tonalité doit lancer la procédure normale de demande du mode H.245 par l'envoi à son homologue distante d'un message **requestMode** contenant la valeur mode de données **t38fax** ou les capacités génériques de transport dans la voie audio T38RTP comme mode demandé. L'extrémité qui reçoit le message **RequestMode** doit renvoyer un message **requestModeAck**. Dès réception du message **requestModeAck**, l'extrémité initiatrice doit fermer sa voie logique audio et ouvrir une voie

logique T.38. De même, l'extrémité distante doit fermer sa voie logique audio et ouvrir une voie logique de télécopie T.38. Une fois que les acquittements ont été reçus pour chacune des voies logiques T.38 ouvertes, l'émission et la réception de télécopie ont lieu.

La Figure D.8 décrit une commutation correcte de voix à fax lorsqu'une voie H.245 distincte est déjà ouverte pour deux voies de média unidirectionnelles. A noter que, dans ce diagramme et dans les suivants, les extrémités d'origine et les extrémités de destination ne correspondent pas nécessairement aux extrémités qui établissent ou reçoivent l'appel ou encore aux extrémités appelantes ou appelées. L'une ou l'autre extrémité peut lancer les procédures H.245 pour passer du mode audio à la transmission de télécopie.

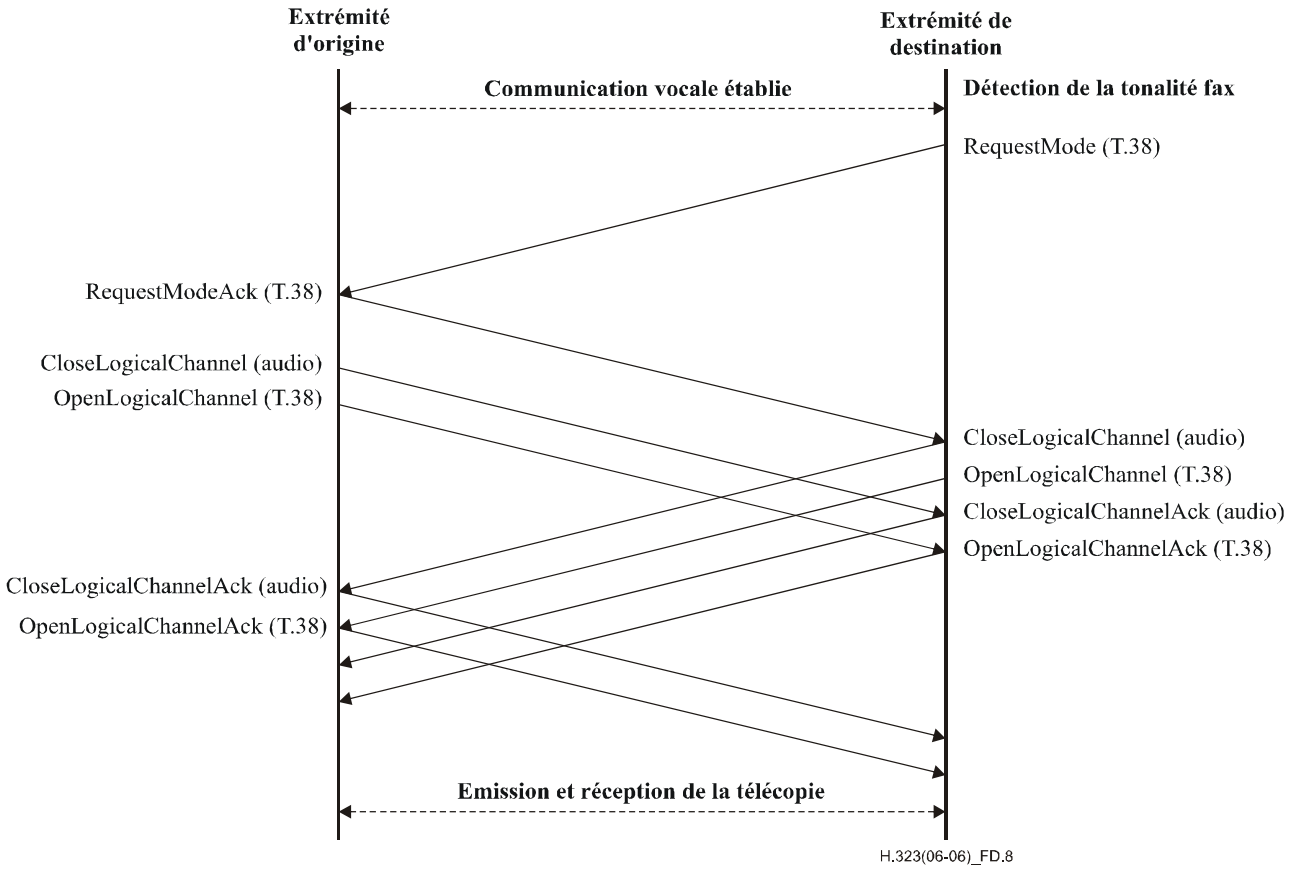


Figure D.8/H.323 – Commutation correcte d'une communication vocale existante à une communication T.38 au moyen de deux voies médias unidirectionnelles sans mise en tunnel

La Figure D.9 décrit une commutation correcte de voix à fax par mise en tunnel H.245 pour deux voies médias unidirectionnelles.

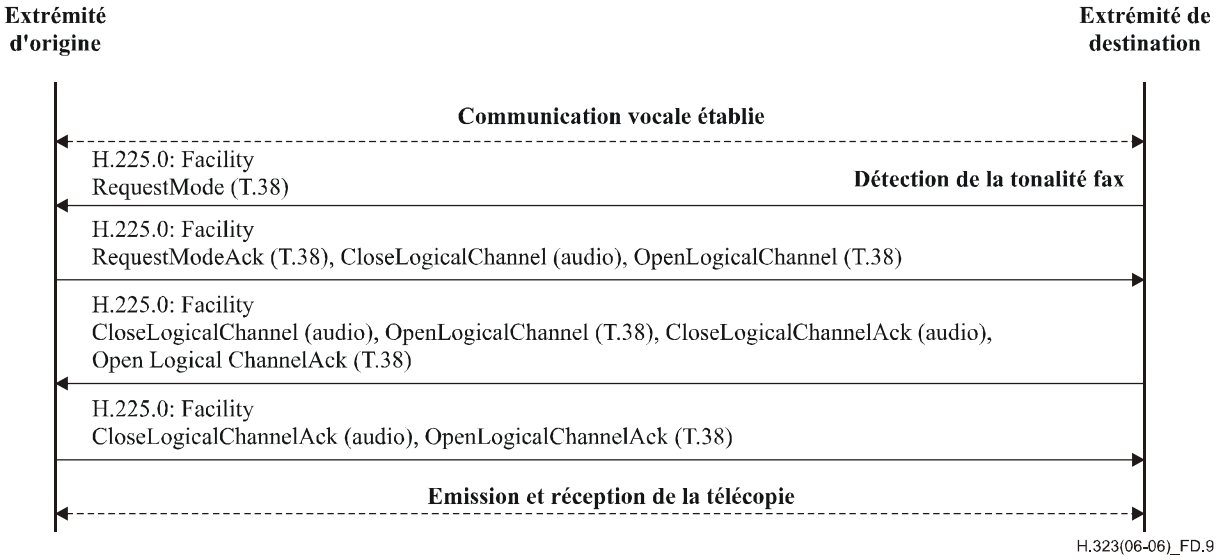


Figure D.9/H.323 – Commutation correcte d'une communication vocale existante à une communication T.38 au moyen de deux voies médias unidirectionnelles avec mise en tunnel

Lorsqu'on utilise des voies bidirectionnelles de télécopie (pour TCP seulement), la commande de demande de mode n'est pas nécessaire: l'extrémité qui a détecté la tonalité doit fermer ses voies ouvertes, demander à l'autre extrémité de fermer les voies inverses, et ouvrir une voie T.38 bidirectionnelle. Dès réception de la commande de demande de fermeture de voie, l'extrémité distante doit fermer sa voie audio. Une fois que les acquittements ont été reçus pour chacune des voies logiques T.38 ouvertes, l'émission et la réception de télécopie ont lieu.

La Figure D.10 décrit une commutation correcte de voix à fax lorsqu'une voie H.245 distincte est déjà ouverte pour une seule voie média bidirectionnelle.

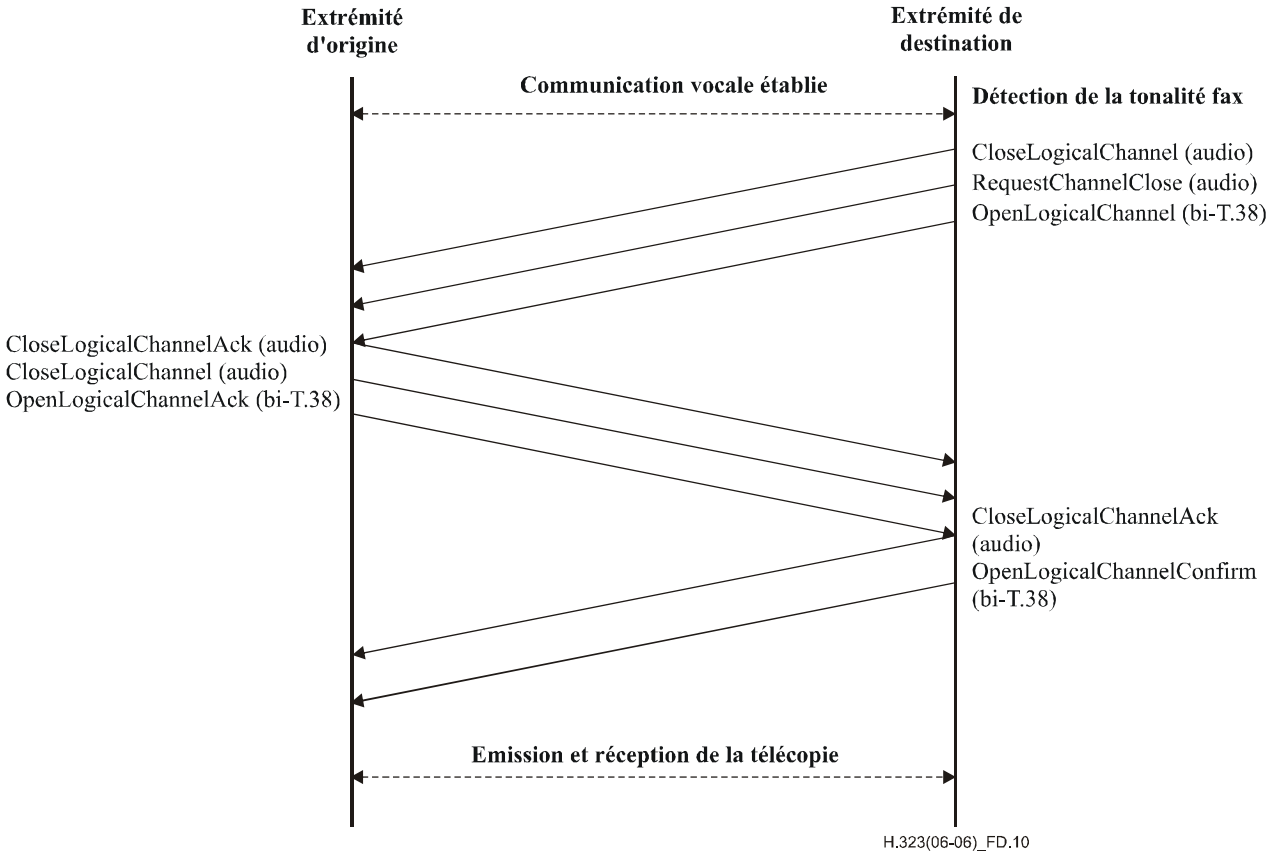


Figure D.10/H.323 – Commutation correcte d'une communication vocale existante à une communication T.38 au moyen d'une seule voie média bidirectionnelle (TCP) sans mise en tunnel

La Figure D.11 décrit une commutation correcte de voix à fax par mise en tunnel H.245 pour une seule voie média bidirectionnelle.

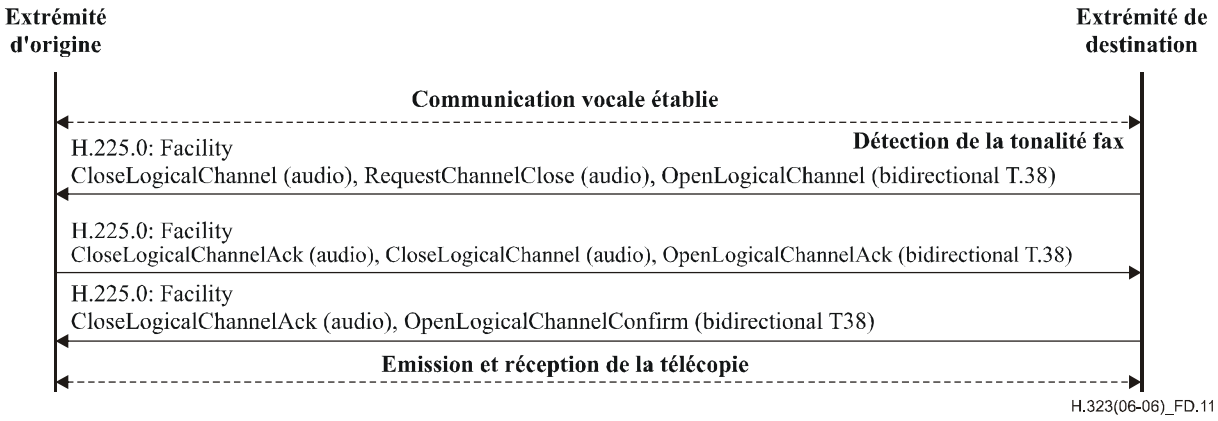


Figure D.11/H.323 – Commutation correcte d'une communication vocale existante à une communication T.38 au moyen d'une seule voie média bidirectionnelle (TCP) avec mise en tunnel

Si une des deux extrémités souhaite revenir à une communication audio après la fin de la transmission de télécopie, la procédure de demande de mode doit être lancée au moyen d'un codec audio inséré comme paramètre. La procédure ci-dessus s'applique également aux cas traditionnels de signalisation de voie logique H.245, si la procédure FastConnect ne peut pas être établie entre les deux extrémités.

D.6 Utilisation de maxBitRate dans les messages

Lorsque le protocole TCP est utilisé pour la transmission par télécopie conforme à la Rec. UIT-T T.38, le débit **maxBitRate** dans le message ARQ/BRQ n'indique pas le débit de données en télécopie, et si une liaison vocale est coupée lorsque débute la session de télécopie, un message BRQ doit être utilisé pour indiquer au portier que la largeur de bande a changé. Lorsque le protocole UDP est utilisé pour une transmission par télécopie conforme à la Rec. UIT-T T.38, **maxBitRate** dans le message ARQ/BRQ n'indique pas le débit nécessaire pour la session de télécopie. L'extrémité (terminal, passerelle) doit envoyer des messages BRQ au portier car la largeur de bande doit être modifiée pendant la communication. A noter que le débit **maxBitRate** dans l'élément **OpenLogicalChannel** du message Setup pendant la phase de connexion rapide est différent du débit **bandWidth** dans le message ARQ/BRQ et ne se rapporte pas au débit de crête qui sera utilisé pour la communication par télécopie.

D.7 Interactions avec les passerelles et avec les dispositifs de type Annexe B/T.38

Il faut examiner le cas suivant:

dispositif de type Annexe D/H.323 (avec signaux vocaux) <–> dispositif de type Annexe B/T.38 (sans signaux vocaux).

Il convient de noter que ces dispositifs peuvent être des terminaux ou des passerelles; il n'y a pas d'incidence sur la discussion. Un appel de télécopie arrive en provenance du côté "sans signaux vocaux", mais le côté "avec signaux vocaux" doit générer un appel vocal sortant qui n'est raccordé à rien même si des tonalités ou des annonces pourraient être reproduites. Dans le sens opposé, le dispositif de type Annexe D/H.323 ne peut pas offrir d'appel vocal au dispositif "sans signaux vocaux", car celui-ci ne peut pas recevoir de signaux vocaux.

La passerelle de type Annexe D/H.323 peut envoyer un élément **OpenLogicalChannel** pour signaux de voix comme de télécopie dans le message Setup. Si cet élément parvient à un dispositif T.38 et que les deux types de signaux aient été proposés, seule la voie pour télécopie sera ouverte. Si l'appel arrive par erreur à un dispositif H.323 ne prenant pas en charge la télécopie, le port de télécopie ne sera pas ouvert. Ce cas est équivalent à celui d'un télécopieur appelant un téléphone.

Un dispositif de type Annexe D/H.323 sait qu'il est en communication avec un dispositif de type Annexe B/T.38 grâce à la séquence d'événements suivante:

1) tout dispositif de type Annexe B/T.38 n'indique pas de port H.245 dans le message Connect ou Setup;

2) le dispositif de type Annexe D/H.323 utilise le message Facility décrit au § 8.2.3; il transmet un message **FACILITY** de paramètre **FacilityReason** mis à **startH245** et indique son adresse H.245 dans l'élément **h245Address**. L'extrémité de type Annexe B/T.38 qui reçoit un message **FACILITY** de paramètre **FacilityReason** mis à **startH245** répondra par un message **FACILITY** de paramètre **FacilityReason** mis à **noH245**. A partir de là, le dispositif de type Annexe D/H.323 doit cesser toute tentative d'ouverture de la voie H.245.

Annexe E

Cadre général et protocole d'échange pour le transport multiplexé de la signalisation d'appel

E.1 Domaine d'application

La présente annexe décrit un format de mise en paquets et un ensemble de procédures (dont certaines sont optionnelles) qui peuvent être utilisés pour appliquer des protocoles de type UDP (protocole datagramme d'utilisateur) et TCP (protocole de commande de transport). La première partie de cette annexe décrit le cadre général de signalisation et le protocole d'échange. Les paragraphes suivants exposent en détail un certain nombre de cas d'utilisation concrets. Le seul profil actuellement spécifié dans la présente révision concerne le transport de messages H.225.0 de type Q.931.

Il est prévu que la présente annexe soit appliquée dans des réseaux organisés et utilise les services de sécurité fournis par le protocole H.323 (par exemple H.235.0, IPSec). La présente annexe ne doit pas être utilisée sur l'Internet public, pour des questions de sécurité et de trafic.

E.1.1 Introduction

E.1.1.1 Transport avec multiplexage

La présente annexe définit une couche de transport avec multiplexage pouvant être utilisée pour transmettre plusieurs protocoles (avec fiabilité optionnelle) dans la même unité de données protocolaire (PDU, *protocol data unit*). Les protocoles souvent utilisés ont des types de codage particuliers (également appelés "types de charge utile"). Les autres protocoles peuvent être acheminés et identifiés au moyen de charges utiles de type ObjectID.

E.1.1.2 Charges utiles multiples dans une seule unité PDU

Les unités PDU définies dans la présente annexe peuvent contenir plusieurs "charges utiles", avec chacune un protocole différent et s'appliquer à une session différente (la définition d'une "session" dépend du protocole). A noter qu'il n'existe pas de relation implicite entre les charges utiles lorsqu'elles arrivent dans la même unité PDU.

E.1.1.3 Options d'en-têtes souples

Les unités PDU et les en-têtes de charge utile définis dans la présente annexe sont configurables. La taille de l'en-tête, qui doit être d'au moins 8 octets, peut atteindre 20 octets lorsque tous les champs optionnels sont présents.

E.1.1.4 Message d'accusé de réception

Les messages acheminés au moyen du protocole PDU peuvent se perdre. Si l'application doit avoir confirmation qu'un message envoyé est bien arrivé, elle peut demander à recevoir un message d'accusé de réception (Ack) de l'unité PDU.

Un émetteur doit préciser dans le champ <ackRequested> (accusé de réception demandé) s'il souhaite recevoir un message Ack pour toute unité PDU qu'il a envoyée, et le récepteur doit répondre par une charge utile de type accusé de réception si le champ <ackRequested> est activé.

NOTE – Les messages Ack doivent être envoyés par la couche de transport de la présente annexe et non par l'application utilisant la pile de la présente annexe. Le comportement particulier concernant les messages Ack est imposé par le modèle de signalisation que l'application demande à la pile de la présente annexe d'utiliser.

E.1.1.5 Message d'accusé de réception négatif

Un message d'accusé de réception négatif (Nack) doit être utilisé pour signaler des erreurs telles que les suivantes: incapacité d'accepter un type de charge utile donné, réception d'une unité PDU mal

configurée, entre autres. Ces messages peuvent avoir pour effet d'interrompre une communication en cours.

NOTE – Les messages Nack doivent être envoyés par la couche de transport de la présente annexe et non par l'application utilisant la pile de la présente annexe.

E.1.1.6 Politique du numéro de séquence de l'émetteur

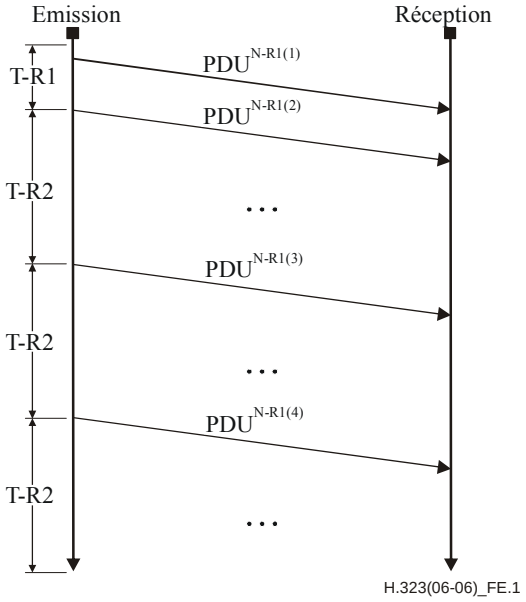
Les couches d'émission de la présente annexe assignées par adresse IP et accès du nœud d'origine doivent commencer par une valeur aléatoire quelconque, augmentant de 1 pour chaque unité PDU envoyée. Si le numéro de séquence atteint 2^{24} (16 777 216) il doit revenir à 0.

E.1.1.7 Politique du numéro de séquence du récepteur

Lorsqu'elle reçoit un paquet de protocoles UDP, la couche de la présente annexe vérifiera l'adresse IP, l'accès du nœud d'origine et le numéro de séquence pour identifier les messages en double. La couche de la présente Annexe peut rediriger des messages en fonction des numéros de séquence et identifier la perte de paquets lorsqu'elle repère des vides dans les numéros de séquence.

E.1.1.8 Retransmissions

Quand un message se perd (et qu'un accusé de réception a été demandé mais n'a pas été reçu) l'émetteur peut retransmettre le message. La politique de retransmission vise à remédier à la perte du premier message en en retransmettant rapidement un nouveau. Mais si celui-ci se perd également, l'émetteur est tenu d'augmenter de plus du double le délai de retransmission. Voir Figure E.1.



Temporisateurs et compteurs de retransmission:

Elément	Valeur	Observations
T-R1	500 ms	Une valeur relativement faible est retenue ici pour compenser la perte éventuelle du premier paquet
T-R2	(T-R1 | T-R2) × N-R2	Si le premier paquet retransmis est perdu, allonger le délai de retransmission. Si une précédente valeur de T-R2 est disponible, utiliser cette valeur au lieu de la valeur initiale de (T-R1).
N-R1	8	Nombre maximal de retransmissions avant abandon de la connexion
N-R2	2,1	Multiplicateur à utiliser pour l'allongement du délai de retransmission

Figure E.1/H.323 – Retransmission d'unités PDU

Lorsque l'on connaît la valeur de l'intervalle de temps de propagation aller-retour d'un message d'après une transmission précédente, le temporisateur T-R1 doit être mis à cette valeur +10%.

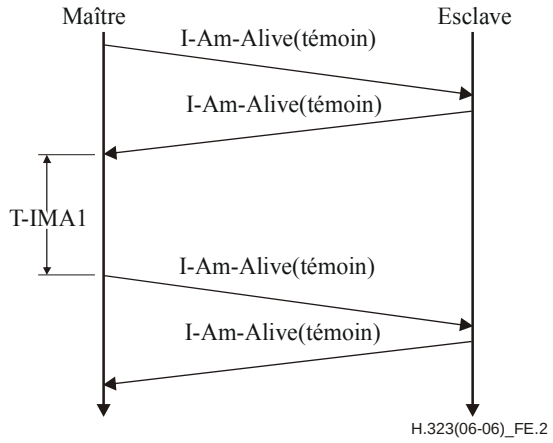
E.1.1.9 Connexion "keep-alive"

En cas d'utilisation du protocole TCP, la présence d'une connexion TCP persistante peut permettre d'informer une extrémité de la présence de dérangements à l'extrémité distante (par l'observation des défaillances du protocole TCP). L'utilisation du protocole UDP ne s'accompagne d'aucun "état" de ce type, et il faut utiliser une autre procédure.

La solution consiste, pour une extrémité de la communication (généralement l'extrémité "esclave" ou "maîtresse" si cette classification est adéquate), à envoyer un message "I-Am-Alive" à l'autre extrémité, pour faire savoir à l'application distante que l'hôte est toujours en service. L'extrémité distante répondra par son propre message "I-Am-Alive" pour indiquer qu'elle aussi est en service. Un témoin peut être fourni par l'expéditeur d'une séquence "I-Am-Alive" et, si tel est le cas, ce témoin doit être renvoyé dans la réponse "I-Am-Alive".

Le temporisateur de retransmission des messages "I-Am-Alive" peut être réinitialisé à la réception d'un autre message pertinent, attestant que l'extrémité distante est en service. Cela permettra d'économiser la largeur de bande, du fait que les messages "I-Am-Alive" ne seront envoyés que lorsqu'ils seront vraiment nécessaires. Cette possibilité est décidée protocole par protocole.

L'émission de messages "I-Am-Alive" est optionnelle. Toutefois, toutes les entités doivent être aptes à répondre à des messages "I-Am-Alive" (ainsi, l'aptitude et l'obligation de répondre à un message "I-Am-Alive" ne sont pas optionnelles et, lorsqu'un tel message est reçu, il faut y répondre conformément aux procédures définies dans la présente annexe). Voir Figure E.2.



Temporisateurs "I-Am-Alive"

Elément	Valeur	Observations
T-IMA1	6 secondes	Intervalle de transmission "I-Am-Alive" (Note)
N-IMA1	6	Nombre de messages I-AM-ALIVE consécutifs sans réponse après lesquels l'entité distante est déclarée ne plus exister
NOTE – Pour ces temporisateurs, il convient d'utiliser les valeurs recommandées dans l'Annexe R si celle-ci s'applique aussi entre deux entités.		

Figure E.2/H.323 – Transmission "I-Am-Alive"

E.1.1.10 Correction d'erreur sans voie de retour

Les messages définis dans la présente annexe peuvent être envoyés plusieurs fois pour permettre la correction d'erreur sans voie de retour. Lorsqu'il est de la plus haute importance qu'un message soit reçu, la couche définie dans la présente annexe peut choisir d'envoyer le même message deux fois

(sans accroître le numéro de séquence). Si les deux messages sont reçus, le second sera considéré comme un message en double normal.

E.1.1.11 Invitations à répondre

Il est conseillé à ceux qui appliquent les dispositions de la présente annexe de différer légèrement le renvoi d'un message d'accusé de réception, pour permettre à l'application d'adjoindre une charge utile de protocole à la charge utile d'accusé de réception. Une option d'en-tête est prévue pour permettre aux émetteurs de signaler à la couche de transport distante qu'une réponse est attendue pour un message donné.

NOTE – Par exemple, lorsqu'un message SETUP H.225.0 est envoyé, la pile peut différer légèrement la réponse de la charge utile d'accusé de réception lorsque le bit d'invitation à répondre ReplyHint est mis à 1 pour laisser à l'application le temps de renvoyer la charge utile CONNECT (par exemple). L'unité PDU renvoyée contiendra donc un accusé de réception (du message SETUP) et la charge utile CONNECT.

E.1.1.12 Accès identifié comme tel et génération d'accès

La présente annexe autorise un accès identifié comme tel principal (accès 2517 UDP/TCP). Les applications qui acceptent les modes de fonctionnement de la présente annexe à la réception d'une charge utile que l'accès identifié comme tel principal n'accepte pas (identifiée à l'aide du type de charge utile statique ou du type de charge utile d'identificateur d'objet ObjectID) peuvent répondre par un message d'accusé de réception négatif donnant pour instruction à l'émetteur d'envoyer ce type de charge utile particulier à un accès et une adresse IP différents.

E.1.2 Modèles de signalisation

La signalisation peut obéir à de nombreux modèles. Chaque implémentation de protocole utilisant la présente annexe doit accepter un des modèles (décrits ci-dessous) ou choisir un modèle de signalisation différent, adapté à ses besoins.

E.1.2.1 Modèle en temps réel

Dans le modèle en temps réel, si une unité PDU est perdue, il est inutile de l'envoyer de nouveau du fait que les informations qu'elle contient sont peut-être déjà périmées. Un exemple d'un tel protocole est le protocole en temps réel (RTP) lorsqu'il est utilisé pour le mode continu audio ou vidéo en temps réel. Pour de tels protocoles, le retard causé par la retransmission est plus dommageable que la perte des informations.

En cas d'utilisation de ce modèle, l'indicateur d'accusé de réception doit toujours être supprimé.

E.1.2.2 Modèle en série

Dans le modèle en série, lorsqu'une unité PDU est envoyée, la couche de la présente annexe attend qu'une réponse positive soit renvoyée pour le même identificateur de session. Il est procédé ainsi pour les protocoles qui ne peuvent admettre la réception de messages de dérangement et qui doivent fonctionner en temps réel tout en envoyant de petites quantités d'informations. Un exemple d'un tel protocole est le protocole Q.931.

En cas d'utilisation de ce modèle, l'indicateur d'accusé de réception doit toujours être activé pour les messages de type statique. Sauf indication contraire, les implémentations de la présente annexe doivent utiliser les temporisateurs de retransmission par défaut (**T-R1** et **T-R2**) et le compteur (**N-R1**).

E.1.2.3 Modèle mixte

Le modèle mixte peut impliquer que la machine à états protocolaires et la machine à états de la présente annexe sont étroitement interconnectées. De telles implémentations peuvent utiliser le bit d'accusé de réception s'il y a lieu.

En cas d'utilisation de ce modèle, l'utilisation de l'indicateur d'accusé de réception peut être interdite, facultative ou obligatoire, selon ce que prescrit le protocole.

E.1.2.4 Annexe E avec protocole TCP

La présente annexe peut être utilisée avec le protocole TCP. En pareil cas, le message d'accusé de réception ne doit pas être utilisé. En outre, le bit L de l'en-tête PDU doit être mis à 1, ce qui a pour effet de rendre disponibles les champs de nombre de charges utiles ou de longueur d'unités PDU.

E.1.3 Champs de charge utile optionnels

E.1.3.1 Identificateur de session

Les charges utiles de la présente annexe acceptent un champ session optionnel qui peut être utilisé pour identifier une session dans la couche de transport avec multiplexage dont la charge utile fait partie. La longueur du champ session est de 16 bits.

NOTE – Ce champ peut être utilisé, par exemple, pour acheminer la valeur CRV (valeur de référence d'appel définie dans la Rec. UIT-T Q.931, par exemple) dans des messages H.225.0. L'interprétation du champ session dépend du protocole.

E.1.3.2 Identificateur d'adresse de nœud d'origine/de destination

Les charges utiles de la présente annexe acceptent un champ d'adresse de nœud d'origine/de destination optionnel qui peut être utilisé pour identifier le nœud d'origine ou de destination de la charge utile. La longueur du champ d'adresse de nœud d'origine/de destination est de 32 bits.

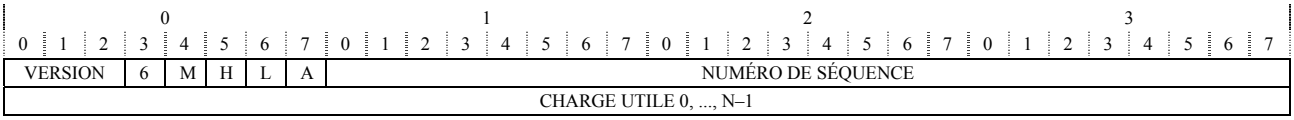
NOTE – Ce champ peut être utilisé (par exemple dans la Rec. UIT-T H.283) pour exprimer l'adresse [<M><T>] identifiant le nœud d'origine du paquet, et l'adresse [<M><T>] identifiant le nœud de destination du paquet. L'interprétation du champ d'adresse de nœud d'origine/de destination dépend du protocole.

E.1.4 Protocole d'échange

Le protocole d'échange de la présente annexe utilise le codage binaire tel que défini dans le reste du présent paragraphe. Les structures et les champs multioctets doivent utiliser l'ordre des octets utilisé par le réseau (octets "gros-boutistes", par exemple).

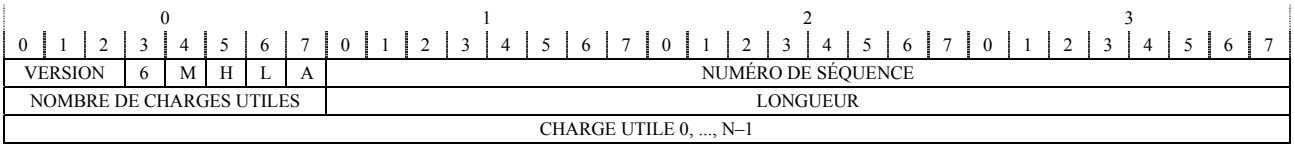
E.1.4.1 Structure d'en-tête

La structure suivante doit être utilisée pour le codage de l'en-tête de la présente annexe. Si le bit L est supprimé (ce qui signifie qu'il n'y a pas d'indication de nombre de charges utiles ou de longueur d'unités PDU), la longueur des charges utiles dans le message et leur nombre peuvent être déduits de la taille du message telle qu'elle ressort de la couche Transport. Voir Figures E.3 et E.4.



Champ	Contenu des champs	Bits
VERSION	Entier non signé; les émetteurs doivent mettre ce champ à 0. Le numéro de version 7 est réservé aux essais expérimentaux; il ne faut pas en tenir compte dans les implémentations commerciales.	3
6	Mis à 0, ce bit signifie que toutes les adresses IP sont conformes IPv4 (utilisent 32 bits). Mis à 1, il signifie que toutes les adresses IP sont conformes IPv6 (utilisent 128 bits).	1
M	Bit de multidiffusion. Mis à 1, il indique que l'unité PDU a été multidiffusée; mis à 0, il indique que l'unité PDU a été unidiffusée. Les émetteurs doivent mettre ce bit à 1 en cas de multidiffusion de l'unité PDU et à 0 dans le cas contraire.	1
H	Bit d'invitation à répondre Reply-Hint – lorsqu'il est activé, ce message donnera lieu à une réponse; par exemple, lorsqu'il est activé, le message d'accusé de réception doit être différé pour donner à l'application la possibilité de fournir une charge utile de réponse avec la charge utile d'accusé de réception.	1
L	Indicateur de longueur. La présence de cet indicateur oblige à faire figurer 4 octets supplémentaires contenant le nombre de charges utiles dans l'unité PDU (8 bits) et la longueur totale (en octets) de l'unité PDU (24 bits)	1
A	Valeur booléenne: la valeur TRUE (Vrai) indique qu'un accusé de réception est demandé pour cette unité PDU	1
NUMÉRO DE SÉQUENCE	Entier non signé de 0 à 16 777 215: numéro de séquence de l'unité PDU considérée	24
CHARGE UTILE	Séquence des structures de charge utile	8 × n

Figure E.3/H.323 – Structure de l'en-tête lorsque le bit L est supprimé



Champ	Contenu des champs supplémentaires du bit L	Bits
NOMBRE DE CHARGES UTILES	Nombre total de charges utiles de l'unité PDU –1 (par exemple, 0 signifie qu'il y a une charge utile, 1 signifie qu'il y en a deux, etc.).	8
LONGUEUR	Longueur totale en octets de toutes les charges utiles (à l'exclusion de l'en-tête)	24

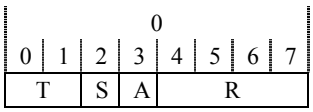
Figure E.4/H.323 – Structure de l'en-tête lorsque le bit L est mis à 1

E.1.4.2 Structure des charges utiles

Les structures suivantes doivent être utilisées pour le codage des charges utiles de la présente annexe.

E.1.4.2.1 Indicateurs d'en-tête de charge utile

Chaque charge utile commence par un octet d'indicateurs, qui définit les champs optionnels figurant dans l'en-tête de charge utile. Voir Figure E.5.



Champ	Contenu des champs	Bits
T	Deux bits définissant le type d'identification de charge utile: **00**: messages de transport de l'Annexe E; **10**: messages de type de charge utile statique; **01**: messages de type OBJECT IDENTIFIER; **11**: réservé pour utilisation ultérieure	2
S	Indique la présence d'un champ de session	1
A	Indique la présence d'un champ d'adresse de nœud d'origine/de destination	1
R	Réservé pour utilisation ultérieure, doit être supprimé par les émetteurs	4

Figure E.5/H.323 – Indicateurs de charge utile

E.1.4.2.2 Messages de transport de la présente annexe

Les deux bits T de l'octet d'indicateurs d'en-tête de charge utile doivent être mis à 0 (zéro) pour tous les messages de transport de la présente annexe. L'octet suivant doit indiquer que le message de transport de la présente annexe va suivre. Les bits S et A doivent être mis à 0. Voir Figure E.6.

Valeur	Interprétation
0	Message I-Am-Alive
1	Message Ack
2	Message Nack
3	Message Restart
4..255	Réservées pour utilisation future

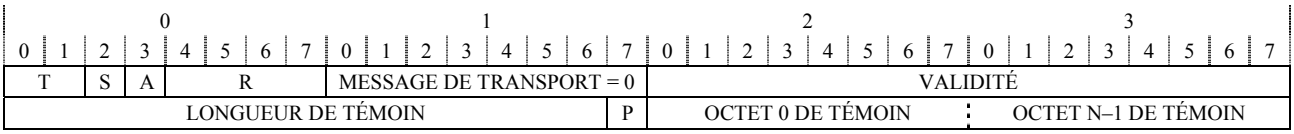
Figure E.6/H.323 – Messages de transport de l'Annexe E

E.1.4.2.2.1 Message "I-Am-Alive"

La structure suivante doit être utilisée pour le codage des charges utiles "I-Am-Alive" de la présente annexe. L'octet message de transport doit être mis à 0 (zéro). La période de validité est exprimée en centaines de millisecondes.

- Si le bit replyRequested (réponse demandée) (**P**) est mis à 1, le récepteur doit répondre par un message "I-Am-Alive" accompagné d'un témoin (s'il en est prévu un).
- Le bit ReplyRequested est différent du bit ackRequested (accusé de réception demandé) de l'en-tête PDU. Ce dernier entraîne en effet l'envoi d'un message d'accusé de réception, alors que le bit replyRequested donne lieu à un message "I-Am-Alive".
- Si une période de validité est mise à zéro (0), le temporisateur **T-IMA1** doit être utilisé.
- Les unités PDU qui ne contiennent qu'une charge utile "I-Am-Alive" doivent remettre à zéro le bit d'accusé de réception de l'en-tête PDU.

Voir Figure E.7.

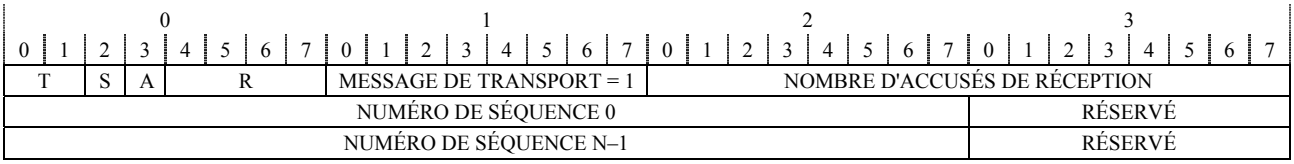


Champ	Contenu des champs	Bits
VALIDITÉ	Entier non signé: temps, en centaines de millisecondes, pendant lequel le message "I-Am-Alive" considéré est valable	16
LONGUEUR DE TÉMOIN	Longueur (en multiplets ou en octets) du champ témoin	15
P	Réponse demandée	1
TÉMOIN	multiplets ou octets du témoin	8 × n

Figure E.7/H.323 – Message "I-Am-Alive"

E.1.4.2.2.2 Message d'accusé de réception

La structure suivante doit être utilisée pour le codage des messages d'accusé de réception. L'octet message de transport doit être mis à 1 (un). Les unités PDU qui ne contiennent qu'une charge utile d'accusé de réception doivent mettre à zéro le bit d'accusé de réception de l'en-tête PDU. Voir Figure E.8.

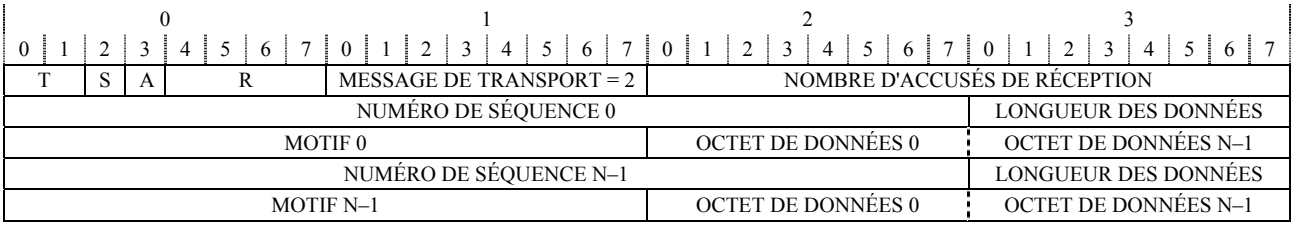


Champ	Contenu des champs	Bits
NOMBRE D'ACCUSÉS DE RÉCEPTION	Nombre de champs de numéro de séquence qui suivent	16
NUMÉRO DE SÉQUENCE 0, ..., N–1	Numéros de séquence des unités PDU dont il est accusé réception	24 × n
RÉSERVÉ	Réservé pour utilisation ultérieure	8 × n

Figure E.8/H.323 – Charge utile d'accusé de réception

E.1.4.2.2.3 Message d'accusé de réception négatif

La structure suivante doit être utilisée pour le codage des messages d'accusé de réception négatif. L'octet message de transport doit être mis à 2 (deux). Le message Nack doit être utilisé pour signaler des erreurs transitoires ou des erreurs plus graves, comme l'arrivée d'un message mal configuré. Les messages Nack non attendus (tels que ceux qui comportent des numéros de séquence non valides) seront ignorés. Voir Figure E.9.



Champ	**Contenu des champs**	**Bits**
NOMBRE D'ACCUSÉS DE RÉCEPTION	Nombre de champs de numéro de séquence qui suivent	16
NUMÉRO DE SÉQUENCE 0, ..., N–1	Numéros de séquence des unités PDU dont il est accusé réception	24 × n
LONGUEUR 0, ..., N–1	Longueur des données propres à l'accusé de réception négatif	8 × n
MOTIF 0, ..., N–1	Motif de l'accusé de réception négatif	16 × n
OCTETS	Octets de données propres à l'accusé de réception négatif	8 × n

Valeur du motif	**Signification des motifs de l'accusé de réception négatif**	**Longueur des données de l'accusé de réception négatif dans les octets**	**Données**
0	Motif non courant	1 + n	OCTET DE LONGUEUR suivi de octet(s) D'IDENTIFICATEUR D'OBJET
1	Invite l'émetteur à utiliser un accès secondaire pour le type de charge utile statique spécifié	8	Telles que définies dans la Figure E.10
2	Invite l'émetteur à utiliser un accès secondaire pour le type de charge utile ObjectID spécifié	1 + n + 6	Telles que définies dans la Figure E.11
3	Charge utile de transport non acceptée	1	Entier non signé
4	Type de charge utile statique non accepté	1	Entier non signé; charge utile telle que définie dans le protocole de type statique qui n'est pas accepté.
5	Charge utile Object-ID non acceptée	1 + n	OCTET DE LONGUEUR suivi de OCTET(S) D'IDENTIFICATEUR D'OBJET
6	Charge utile dégradée	1	Nombre de charges utiles dégradées dans le message
7..65535	Réservé pour utilisation ultérieure		

Figure E.9/H.323 – Message d'accusé de réception négatif

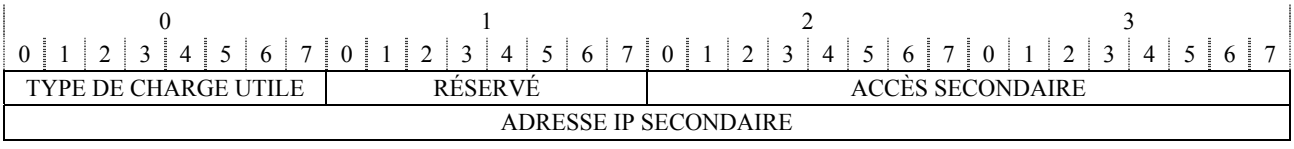


Figure E.10/H.323 – Structure du motif 1 d'accusé de réception négatif

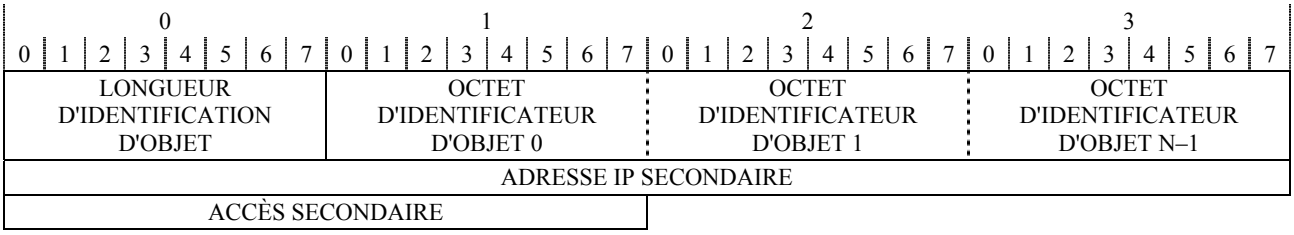


Figure E.11/H.323 – Structure du motif 2 d'accusé de réception négatif

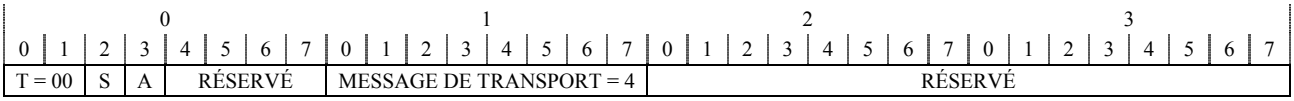
Si l'adresse IP est mise à zéro, l'adresse IP de l'émetteur doit être utilisée (telle que définie par la couche TCP/IP). Si l'accès UDP est mis à zéro, l'accès d'émission doit être utilisé (tel que défini par la couche TCP/IP).

E.1.4.2.2.4 Message Restart

La structure suivante doit être utilisée pour le codage des messages Restart de la présente annexe. L'octet message de transport doit être mis à 3. Le message Restart est utilisé pour signaler à l'entité distante que l'émetteur a redémarré. La charge utile Restart devrait être intégrée dans le premier message envoyé à l'entité distante. Le récepteur doit réinitialiser sa série de numéros de séquence lorsqu'il reçoit la charge utile Restart. Il doit considérer tout message entrant dont le numéro de séquence appartient à la série de numéros de séquence précédente comme étant périmé et ne doit pas en tenir compte.

Selon le champ "action" figurant dans la charge utile Restart, le récepteur doit mettre fin aux communications en cours ou engager les procédures de reprise d'appel.

Si un redémarrage n'affecte pas les appels en cours, il est invisible par la couche définie dans la présente annexe et ne sera donc pas signalé. Voir Figure E.12.



Champ	**Contenu des champs**	**Bits**
action	L'action souhaitée par le récepteur de la charge utile Restart	8
Valeur d'action	**Signification**	
0	Non spécifiée	
1	Mettre fin aux communications en cours	
2	Engager les procédures de reprise d'appel	
3..	Réservées pour usage ultérieur	

Figure E.12/H.323 – Structure du message Restart

E.1.4.3 Messages de type statique

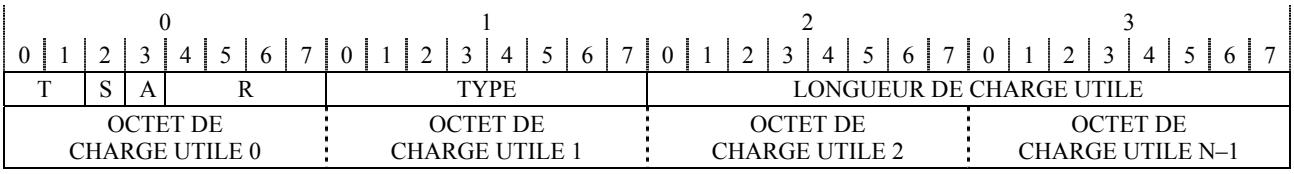
Le premier bit T de l'octet d'indicateurs d'en-tête de charge utile doit être mis à 1 (un) pour tous les messages de type statique. Le deuxième bit T de l'octet d'indicateurs d'en-tête de charge utile doit être mis à 0 (zéro) pour tous les messages de type statique. L'octet suivant doit indiquer la charge utile présente (voir Figure E.13):

Valeur	Interprétation
0	Le train d'octets contient un message de signalisation d'appel tel que défini dans la Rec. UIT-T H.225.0
1..255	Réservées pour utilisation ultérieure

Figure E.13/H.323 – Charges utiles de type statique

E.1.4.3.1 Message de type statique de base (bit S et bit A supprimés)

Lorsque les bits S et A sont tous deux supprimés, le format de charge utile suivant doit être utilisé (voir Figure E.14):

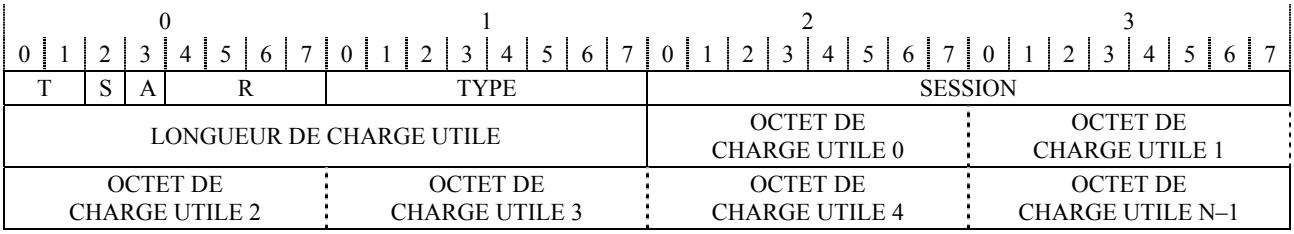


Champ	Contenu des champs	Bits
TYPE	Entier non signé: type de la charge utile, tel que défini dans la Figure E.13	8
LONGUEUR	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.14/H.323 – Charge utile de type statique de base

E.1.4.3.2 Message de type statique étendu 1 (bit S mis à 1 et bit A supprimé)

Lorsque le bit S est mis à 1 et que le bit A est supprimé, le format de charge utile suivant doit être utilisé. Le bit S indique la présence d'un champ SESSION. Voir Figure E.15.

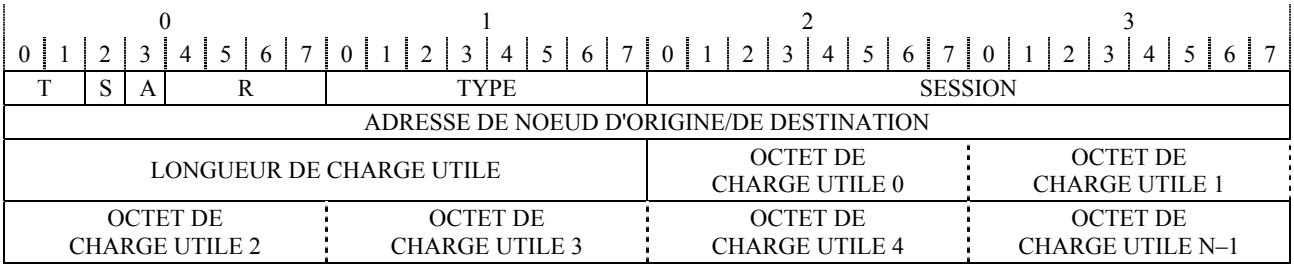


Champ	Contenu des champs	Bits
TYPE	Entier non signé: type de la charge utile, tel que défini dans la Figure E.13	8
SESSION	Entier non signé: la signification du champ de session dépend du protocole	16
LONGUEUR DE CHARGE UTILE	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.15/H.323 – Format de charge utile étendu 1

E.1.4.3.3 Message de type statique étendu 2 (bit S et bit A mis à 1)

Lorsque le bit S et le bit A sont tous deux mis à 1, le format de charge utile suivant doit être utilisé. Le bit A indique la présence d'un champ d'adresse de nœud d'origine/de destination. Voir Figure E.16.



Champ	Contenu des champs	Bits
TYPE	Entier non signé: type de la charge utile, tel que défini dans la Figure E.13	8
SESSION	Entier non signé: la signification du champ de session dépend du protocole	16
ADRESSE DE NŒUD D'ORIGINE/ DE DESTINATION	Entier non signé: la signification du champ adresse de nœud d'origine/de destination dépend du protocole	32
LONGUEUR DE CHARGE UTILE	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.16/H.323 – Format de charge utile étendu 2

E.1.4.3.4 Message de type statique étendu 3 (bit S supprimé, bit A mis à 1)

Lorsque le bit S est supprimé et que le bit A est mis à 1, le format de charge utile suivant doit être utilisé. Le bit A indique la présence d'un champ d'adresse de nœud d'origine/de destination. Voir Figure E.17.

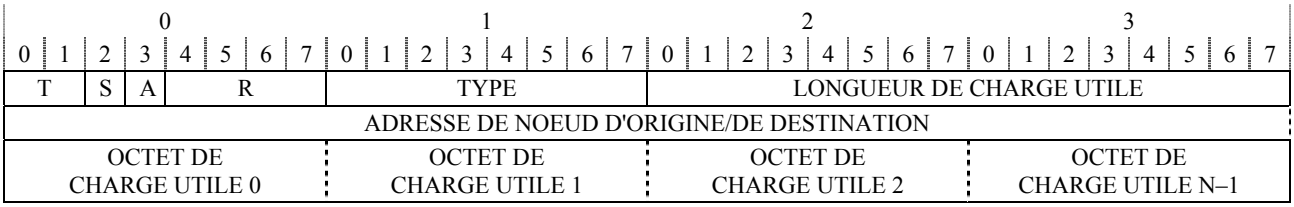


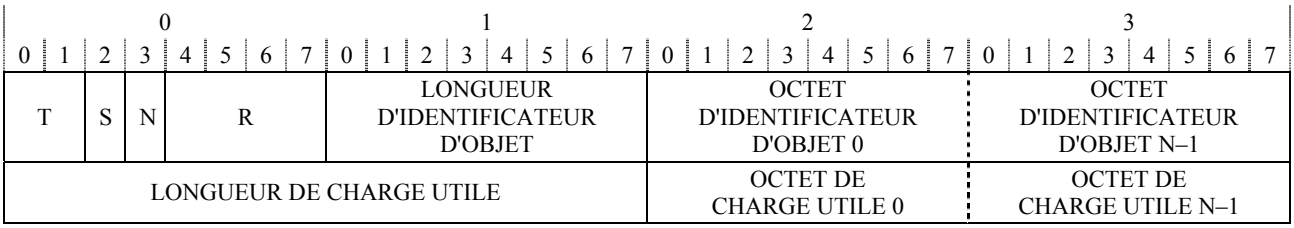
Figure E.17/H.323 – Format de charge utile étendu 3

E.1.4.4 Messages de type ObjectID

Le premier bit T de l'octet d'indicateurs d'en-tête de charge utile doit être mis à 0 (zéro) pour tous les messages de type ObjectID (identificateur d'objet). Le deuxième bit T de cet octet doit être mis à 1 (un) pour tous les messages de type ObjectID. Les deux octets suivants doivent indiquer la longueur de l'identificateur ObjectID qui suit.

E.1.4.4.1 Message de type ObjectID de base (bit S et bit A supprimés)

Lorsque les bits S et A sont tous deux supprimés, le format de charge utile suivant doit être utilisé (voir Figure E.18):

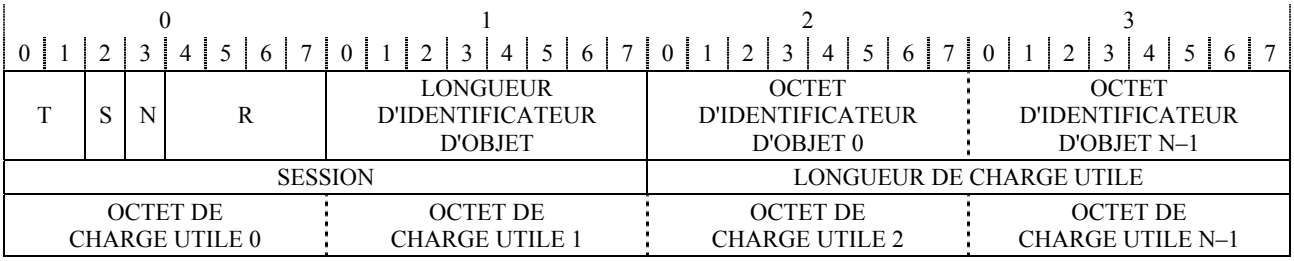


Champ	Contenu des champs	Bits
LONGUEUR D'IDENTIFICATEUR D'OBJET	Entier non signé: longueur en OCTETS de l'identificateur d'objet suivant	8
IDENTIFICATEUR D'OBJET	OCTETS d'identificateur d'objet	8 × n
LONGUEUR	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.18/H.323 – Charge utile de type ObjectID de base

E.1.4.4.2 Message de type ObjectID étendu 1 (bit S mis à 1 et bit A supprimé)

Lorsque le bit S est mis à 1 et que le bit A est supprimé, le format de charge utile suivant doit être utilisé. Le bit S indique la présence d'un champ SESSION, qui est utilisé par l'application pour associer des charges utiles à une session donnée. La définition d'une session dépend du protocole. Voir Figure E.19.

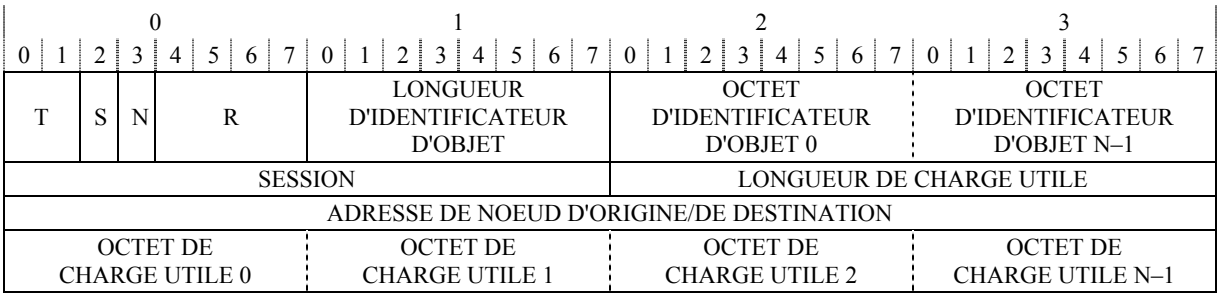


Champ	Contenu des champs	Bits
LONGUEUR D'IDENTIFICATEUR D'OBJET	Entier non signé: longueur en OCTETS de l'identificateur d'objet suivant	8
IDENTIFICATEUR D'OBJET	OCTETS d'identificateur d'objet	8 × n
SESSION	Entier non signé: la signification du champ session dépend du protocole	16
LONGUEUR	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.19/H.323 – Format de charge utile de type ObjectID étendu 1

E.1.4.4.3 Message de type ObjectID étendu 2 (bit S et bit A mis à 1)

Lorsque le bit S et le bit A sont tous deux mis à 1, le format de charge utile suivant doit être utilisé. Le bit A indique la présence du champ adresse de nœud d'origine/de destination. Voir Figure E.20.



Champ	Contenu des champs	Bits
LONGUEUR D'IDENTIFICATEUR D'OBJET	Entier non signé: longueur en OCTETS de l'identificateur d'objet suivant	8
IDENTIFICATEUR D'OBJET	OCTETS d'identificateur d'objet	8 × n
SESSION	Entier non signé: la signification du champ session dépend du protocole	16
LONGUEUR	Entier non signé: longueur (en OCTETS ou en MULTIPLETS) des données de charge utile	16
ADRESSE DE NŒUD D'ORIGINE/ DE DESTINATION	Entier non signé: la signification du champ adresse de nœud d'origine/de destination dépend du protocole	32
DONNÉES	OCTETS des données de charge utile effectives	8 × n

Figure E.20/H.323 – Format de charge utile de type ObjectID étendu 2

E.1.4.4.4 Message de type ObjectID étendu 3 (bit S supprimé, bit A mis à 1)

Lorsque le bit S est supprimé et que le bit A est mis à 1, le format de charge utile suivant doit être utilisé. Le bit A indique la présence d'un champ d'adresse de nœud d'origine/de destination. Voir Figure E.21.

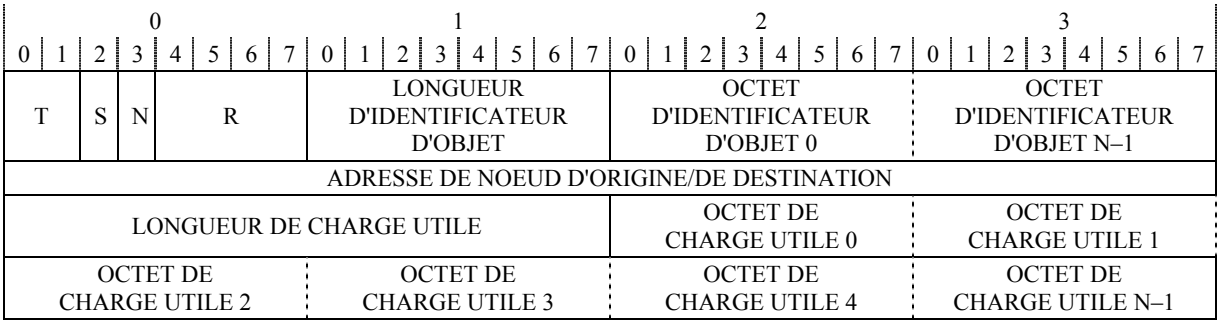


Figure E.21/H.323 – Format de charge utile de type ObjectID étendu 3

E.2 Signalisation d'appel H.225.0 selon la présente annexe

Le présent paragraphe indique comment acheminer des messages de signalisation d'appel H.225.0 selon le mode de transport de la présente annexe, avec protocole UDP. La présente annexe est utilisée pour assurer un transport "UDP fiable" permettant aux implémentations H.225.0 de fonctionner selon la présente annexe en grande partie inchangée.

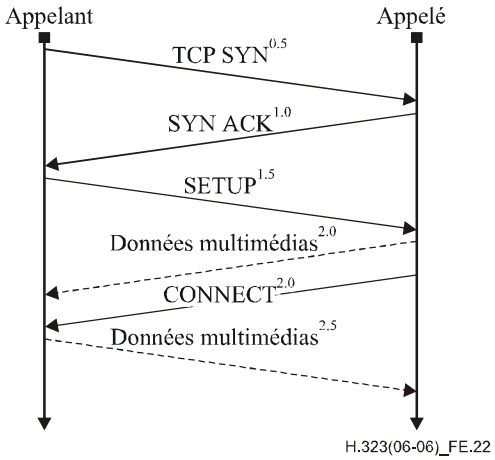
E.2.1 Principes de base

La version 2 de la Rec. UIT-T H.323 (1998) présente le principe de connexion rapide (Fast Connect) qui permet de transmettre des données multimédias en mode pseudo-transit en un minimum de deux allers-retours dans le sens appelé vers appelant (messages TCP compris) et en 2,5 allers-retours dans le sens appelant vers appelé.

Ces délais peuvent être ramenés respectivement à 1 et 1,5 aller-retour en utilisant pour le transport des messages H.323 le protocole UDP au lieu du protocole TCP. Ce point revêt une importance particulière en cas d'utilisation du modèle d'acheminement par portier.

E.2.2 Etablissement d'appels H.323 selon la présente annexe

La version 2 de la Rec. UIT-T H.323 (1998) utilise le mode de transport TCP pour acheminer les messages H.225.0, ce qui signifie que le plus petit nombre d'aller-retour possible pour transmettre des données multimédias en mode pseudo-transit est de 2 dans le sens appelé vers appelant, et de 2,5 dans le sens appelant vers appelé. Voir Figure E.22.



NOTE – Par souci de clarté, certains messages de la procédure de prise de contact TCP ont été omis.

Figure E.22/H.323 – Flux d'informations pour la connexion rapide de la version 2 H.323 (1998)

E.2.2.1 Procédure utilisant le protocole UDP

Pour accélérer la transmission des données multimédias en mode pseudo-transit, il est possible d'utiliser le protocole UDP pour le transport de la signalisation d'appel, ce qui permet de transmettre dûment les données multimédias en mode pseudo-transit en un seul aller-retour (voir Figure E.23):

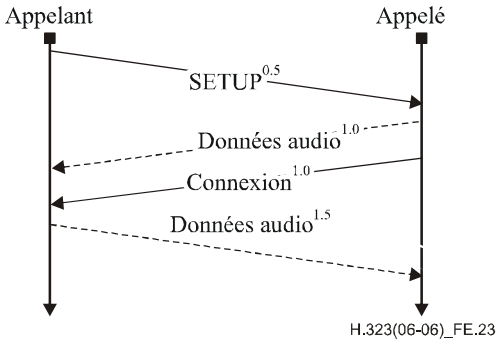


Figure E.23/H.323 – Flux d'informations pour l'établissement d'appel utilisant le protocole UDP

Les couches définies dans la présente annexe doivent retransmettre un paquet perdu s'il n'y est pas répondu au bout d'un certain temps. Le détail de la procédure de retransmission est précisé au § E.1.1.8.

E.2.2.2 Procédure mixte TCP et UDP

La procédure d'établissement d'appel qui utilise le protocole TCP et celle qui utilise le protocole UDP ne sont pas incompatibles. Si ces procédures sont exécutées en parallèle, il convient d'utiliser la procédure définie dans le présent paragraphe. Dans la procédure mixte, l'expéditeur envoie le message SETUP en utilisant le protocole UDP et établit simultanément une connexion TCP. Si l'expéditeur n'a pas reçu de réponse à son message SETUP UDP lorsque la connexion TCP est établie, il envoie aussi le message SETUP sur la connexion TCP. Si un appelé reçoit un message SETUP UDP et un message SETUP TCP identiques, il répond en utilisant l'un ou l'autre protocole de transport (généralement celui correspondant au premier message arrivé) mais pas les deux.

Si l'expéditeur reçoit une réponse UDP, la connexion TCP doit être libérée et la communication continue en utilisant le protocole UDP. Si l'expéditeur reçoit une réponse TCP (par exemple par suite de la non-prise en charge des procédures de la présente annexe par l'entité distante), la communication continue en utilisant le protocole TCP, la communication utilisant le protocole UDP ne devant plus être utilisée pour cet appel.

Un appelé prenant en charge la présente annexe doit choisir le protocole de transport en fonction du premier message qui arrive: message Setup TCP ou message Setup UDP. Il est à noter que l'ordre de ces messages peut changer à la remise. L'appelant est informé du choix conformément au protocole de transport utilisé pour le message suivant (par exemple Connect) qu'il reçoit. Voir Figure E.24.

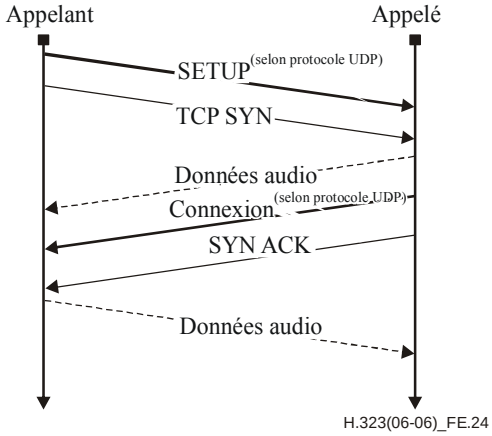


Figure E.24/H.323 – Flux d'informations pour la procédure mixte TCP et UDP

En cas d'échec de la procédure utilisant le protocole UDP, les procédures habituelles utilisant le protocole TCP peuvent ainsi prendre immédiatement la relève (voir Figure E.25):

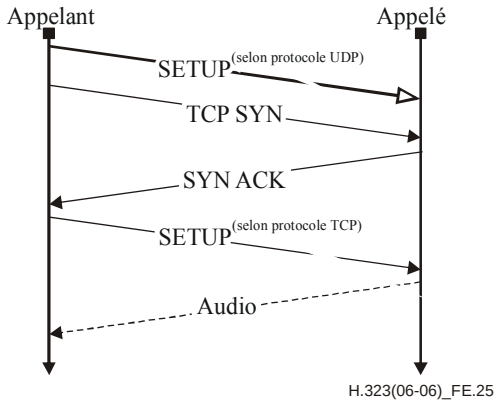


Figure E.25/H.323 – Flux d'informations lorsque le protocole UDP n'est pas accepté

Il s'ensuit que la compatibilité vers l'arrière dans le cas d'entités appelantes de la version 1 (1996) ou 2 (1998) de la Rec. UIT-T H.323 est transparente, du fait que l'application v1/v2 H.323 ignorera le paquet UDP.

NOTE – Il est recommandé aux entités qui engagent la procédure d'établissement d'une communication et qui ne savent pas si l'extrémité distante accepte les opérations de la présente annexe, d'utiliser la procédure définie ci-dessus. Si l'entité appelante sait que l'appelé distant accepte les opérations utilisant le protocole UDP, elle peut utiliser une procédure d'établissement de la communication utilisant le seul protocole UDP.

E.2.3 Points particuliers

E.2.3.1 Identification des messages

Les charges utiles H.225.0 selon la présente annexe doivent utiliser le type de charge utile statique **0** (zéro).

E.2.3.2 Accès identifié comme tel

L'accès UDP **2517** doit être utilisé comme accès identifié comme tel. Les entités peuvent émettre à partir de n'importe quel accès aléatoire. Une entité H.323 isolée fonctionnant sur un dispositif physique doit utiliser un accès UDP isolé distinct comme accès annoncé pour la réception de messages. Toutefois, elle peut utiliser un accès distinct sur chaque interface si le dispositif physique comporte plusieurs interfaces de réseau.

L'entité appelante doit envoyer tous les messages définis dans la présente annexe pour appeler l'accès de destination annoncé de l'entité appelée. Celle-ci doit envoyer tous les messages définis dans la présente annexe liés audit appel à l'adresse IP et à l'accès en provenance duquel le message initial défini dans la présente annexe pour l'appel a été reçu. L'entité appelée doit envoyer tous les messages définis dans la présente annexe en utilisant l'accès sur lequel elle a reçu l'unité PDU H.225.0 initiale en provenance de l'appelant.

L'entité appelante peut transmettre des messages depuis n'importe quel accès aléatoire, mais elle doit utiliser le même accès pendant toute la durée de la communication.

E.2.3.3 Modèle de signalisation

Le modèle de signalisation H.225.0, selon la présente annexe, doit utiliser le **modèle en série** décrit au § E.1.2.2.

E.2.3.4 Temporisateurs

Le protocole H.225.0, selon la présente annexe, doit utiliser les temporisateurs et les valeurs de temporisation par défaut. Le temporisateur **T-IMA1** doit être réinitialisé à la réception de tout message de signalisation d'appel, par exemple (mais pas à la réception de paquets RTP).

E.2.3.5 Champ de session

Le champ de session doit être présent dans toutes les charges utiles. La valeur de session doit contenir la valeur CRV provenant des messages de signalisation d'appel H.225.0. Concrètement, l'indicateur de référence d'appel doit être inséré en tant que bit de poids fort de la valeur de référence d'appel CallReferenceValue. Cela limite la valeur CRV effective à l'étendue de 0 à 32 767, inclus.

E.2.3.6 Champ d'adresse de nœud d'origine/de destination

L'utilisation du champ d'adresse de nœud d'origine/de destination est facultative, mais ce champ doit être présent dans tous les messages en provenance ou à destination d'un pont de conférence (MCU) ou lorsqu'un portier fait office de contrôleur multipoint (MC).

E.2.3.7 Unité MTU

Les messages de signalisation d'appel nécessitant l'envoi de gros volumes de données (par exemple pour l'authentification et l'autorisation fondées sur des certificats) doivent utiliser le protocole TCP pour l'établissement d'appel; en effet l'utilisation du protocole de la présente annexe dans ce cas pourrait entraîner une fragmentation par suite de messages plus longs que l'unité MTU du trajet.

E.2.3.8 H.245

Les messages H.245 doivent être transmis selon les procédures de canalisation H.245 de la version 2 (1998) de la Rec. UIT-T H.323.

E.2.3.9 Politique d'attribution de numéros de séquence pour la réception de messages H.225.0 selon la présente annexe

Lorsqu'elle reçoit un message H.225.0 conforme à la présente annexe, une entité doit vérifier l'adresse IP, l'accès du nœud d'origine et le numéro de séquence pour identifier les messages faisant double emploi. L'entité émettrice suit le modèle en série pour le même identificateur de session et attribue les numéros de séquence par adresse IP et par accès de nœud d'origine. Comme il est impossible, dans le cas d'un appel H.323 isolé, de modifier l'ordre des messages, la couche définie dans la présente annexe ne doit pas tenter de reclasser les messages dans l'ordre des numéros de séquence. Les numéros de séquence peuvent comporter des espaces vides qu'une entité ne doit pas assimiler à une perte de paquets.

Annexe F

Dispositifs d'extrémité simples

F.1 Introduction

Les dispositifs d'extrémité simples – c'est-à-dire les dispositifs fabriqués à une seule fin – peuvent constituer une part notable de l'ensemble des systèmes terminaux à capacités H.323. Contrairement aux terminaux pleinement conformes à la Rec. UIT-T H.323 (dont de nombreuses réalisations sont à base de PC), les types d'extrémité simples (SET, *simple endpoint type*) peuvent être implémentés sous forme de boîtiers autonomes bon marché, l'exemple le plus évident étant le simple appareil téléphonique.

NOTE – Parmi les applications types définies, on peut citer:

1) ordinateurs de poche avec des capacités de communication audio (voix, transfert de fichiers, fax, etc.);
2) téléphones munis d'un connecteur RJ-45;
3) textophones (conformes à la Rec. UIT-T T.140);
4) téléphones cellulaires IP;
5) systèmes mobiles intégrant les communications de voix et de données (UMTS, IMT-2000).

Tous ces systèmes ont en commun la prise en charge d'un ensemble de fonctions relativement fixe: voix ou capacités rudimentaires (c'est-à-dire non T.120) de communication de données. Il importe de remarquer que cette fonctionnalité n'a pas besoin d'être étendue aux fins particulières du système: un poste téléphonique sans affichage (évolué) n'a pas besoin d'offrir des capacités vidéo ou de conférence de données.

Tous ces systèmes disposent de ressources limitées (par exemple en termes de puissance de traitement, de largeur de bande de communication ou de mémoire).

La présente annexe décrit le domaine d'application des terminaux SET en général. Elle définit les détails de procédure et de protocole d'un dispositif d'extrémité simple audiophonique (dispositif Audio SET). La présente annexe définit, en particulier, les caractéristiques fonctionnelles de base pour tous les dispositifs d'extrémité simples. Il convient donc de s'y reporter pour la définition des dispositifs SET à venir et de ne préciser que les adjonctions apportées aux procédures et aux conventions qui y sont énoncées.

La présente annexe définit un sous-ensemble de la fonctionnalité H.323 et tous les aspects ne relevant pas de la présente Recommandation sont clairement mentionnés. Toute procédure ne faisant pas l'objet d'une description expresse dans la présente annexe est traitée dans la présente Recommandation elle-même.

La mise au point d'un dispositif SET a d'éventuelles incidences sur d'autres dispositifs H.323: les ponts de conférence (MCU) et les passerelles doivent en particulier tenir compte de la possibilité que ce type de dispositif ait une prise en charge minimale des fonctions H.323 (1998). Cela permettra de fournir des dispositifs SET pouvant accéder sans discontinuité à des services H.323 améliorés comme les conférences multipoint et les services complémentaires. En variante, des dispositifs intermédiaires externes peuvent être mis en place afin de mettre en correspondance différents ensembles fonctionnels entre dispositifs SET et extrémités pleinement conformes à la Rec. UIT-T H.323 (1998). Les problèmes d'interopérabilité sont traités plus en détail au § F.9.

F.2 Conventions de spécification

La présente annexe ne spécifie que les services, procédures, messages de protocole, etc. qui sont obligatoires pour l'implémentation d'un dispositif SET – qui est un sous-ensemble de la

fonctionnalité obligatoire d'un système H.323 (1998). Cela implique qu'un dispositif SET ne possède aucune fonctionnalité autre que celles qui sont spécifiées dans la présente annexe comme étant obligatoires pour les dispositifs SET.

En plus de ses prescriptions obligatoires, la présente annexe contient plusieurs paragraphes qui spécifient des services, des procédures, des messages de protocole, etc., à implémentation conditionnelle, sur la base du concept de blocs fonctionnels globalement facultatifs. Un dispositif SET qui choisit d'implémenter un bloc fonctionnel particulier doit cependant prendre en charge toutes les prescriptions définies comme étant obligatoires pour ce bloc fonctionnel. Des prescriptions facultatives peuvent être prises en compte.

Toutes les autres caractéristiques définies dans la présente Recommandation sont, par définition, facultatives et leur implémentation dans un dispositif SET est entièrement à la discrétion du constructeur.

F.3 Domaine d'application

La présente annexe spécifie des règles d'utilisation des prescriptions de la présente Recommandation qui permettent d'implémenter des dispositifs d'extrémité simples. Les dispositifs d'extrémité simples suivants (liste non exhaustive) sont envisagés pour une normalisation par l'UIT-T.

1) **postes téléphoniques simples (dispositifs d'extrémité simple audiophonique)** – définis dans la présente annexe;
2) **postes téléphoniques simples avec capacités de sécurité** – à étudier;
3) **terminaux de conversation en mode texte** – à étudier;
4) **télécopieurs** – à étudier.

Le poste téléphonique simple est défini dans la présente annexe. Les postes téléphoniques simples sécurisés, les terminaux en mode texte et les télécopieurs simples sont des dispositifs d'extrémité simples à l'étude. Les profils des dispositifs d'extrémité simples peuvent être rangés dans les catégories suivantes:

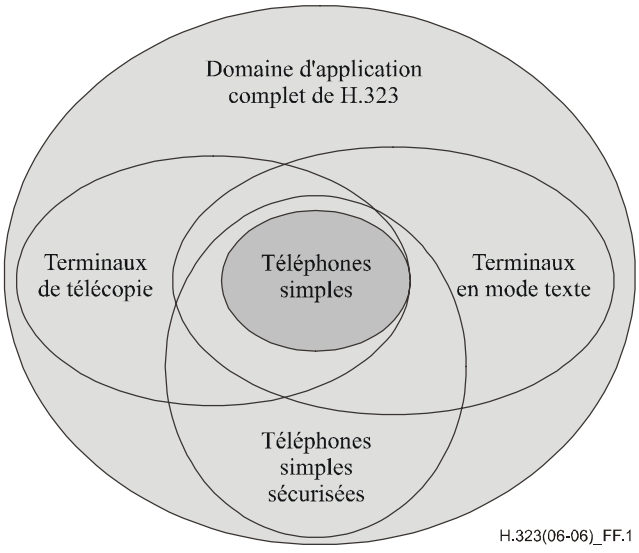


Figure F.1/H.323 – Diagramme de Venn montrant les catégories fonctionnelles des divers dispositifs SET

La Figure F.1 est un schéma (sous forme de ce qu'on appelle un *diagramme de Venn*) des différents dispositifs SET qui sont en cours de définition dans le contexte des "profils" H.323. Ce diagramme

décrit la relation entre les dispositifs SET. La grande ellipse montre le contexte d'un système pleinement conforme à la Rec. UIT-T H.323. A titre d'exemple, le poste téléphonique simple est inscrit dans la figure. Comme il s'agit à l'évidence d'un sous-ensemble du système pleinement conforme à la Rec. UIT-T H.323, cet élément est totalement inscrit dans son domaine d'application. Un poste téléphonique simple sécurisé, contenant en plus des capacités de sécurité, englobe celles du téléphone simple (par exemple mêmes codecs audio, même établissement d'appel, etc.). L'interopérabilité sera donc assurée entre un téléphone simple implémenté comme dispositif SET et un téléphone simple sécurisé.

Les terminaux SET sont définis d'une manière qui leur permet d'interfonctionner sans discontinuité les uns avec les autres et avec des terminaux H.323 (1998) prenant en charge la procédure *FastConnect* ainsi qu'avec toutes les extrémités H.323 compatibles avec les dispositifs SET.

NOTE – Bien que les dispositifs Audio SET soient définis dans le cadre de terminaux simples, il est également possible de construire des passerelles fondées sur la spécification particulière de chaque dispositif SET. Aucune définition supplémentaire n'est requise pour d'autres types de dispositifs.

F.4 Références normatives

Toutes les références normatives du corps de la présente Recommandation et de la Rec. UIT-T H.225.0 (2003) sont applicables.

F.5 Abréviations

La présente annexe utilise les abréviations suivantes:

Audio SET	type d'extrémité simple audiophonique (*simple audio endpoint type*)
Audio SET sécurisé	type d'extrémité simple audiophonique sécurisé (*secure simple audio endpoint type*)
Fax SET	type d'extrémité simple de télécopie (*simple facsimile endpoint type*)
Text SET	type d'extrémité simple textophonique (*simple text telephony endpoint type*)
SET	type d'extrémité simple (*simple endpoint type*)

F.6 Aperçu général de la fonctionnalité système des types d'extrémité simples audiophoniques

Les caractéristiques suivantes s'appliquent aux types d'extrémité simple audiophonique (terminaux Audio SET).

Capacités relatives aux médias

- Capacité vocale
  - obligatoire: Rec. UIT-T G.711 (loi A et loi μ);
  - options recommandées: Rec. UIT-T G.723.1, Rec. UIT-T G.729, GSM;
  - options recommandées: codage de redondance audio avec toute combinaison des codecs ci-dessus.
- Les dispositifs Audio SET ne doivent admettre que le fonctionnement audio symétrique.
- Pas de capacité de transmission de données.
- Capacité DTMF obligatoire; transmission sous forme de message d'information H.225.0 obligatoire; la transmission sous forme de charge utile RTP A étudier.
- Pas de capacité vidéo.
- Pas de capacité T.120.

- Distribution par médias: prise en charge obligatoire de l'unidiffusion (multidiffusion à un faisceau de données par destinataire).

Pour les autres types d'extrémité simples, les capacités obligatoires et facultatives relatives aux médias doivent être définies séparément.

Capacités relatives à la commande

Les capacités minimales ci-après relatives à la commande s'appliquent de la même façon à tous les types d'extrémité simples.

- Séquence FastConnect selon Rec. UIT-T H.323 (1998) obligatoire.

NOTE – Les dispositifs Audio SET ont par défaut la capacité de participer à des MCU – au cours desquelles ils sont évidemment limités aux communications audio.

La plupart des autres capacités de commande sont facultatives, notamment les suivantes:

- capacité (facultative) *Faster-Connect* fondée sur le protocole UDP conformément à l'Annexe E/H.323;
- capacité facultative de services complémentaires (seulement fondée sur les Recommandations UIT-T de la série H.450.x);
- prise en charge facultative des messages et procédures H.245;
- prise en charge facultative de plusieurs communications/conférences simultanées.

Certaines capacités de commande sont interdites pour les dispositifs Audio SET.

- Interdiction de la fonctionnalité de pont MC.

F.7 Procédures pour dispositifs d'extrémité simples

Le présent paragraphe spécifie le niveau détaillé de prise en charge de tous les protocoles requis par la présente Recommandation, par les dispositifs SET en général, ainsi que les impératifs spécifiques pour les dispositifs Audio SET:

- signalisation d'enregistrement, d'admission et d'état (RAS, *registration, admission and status*) selon la Rec. UIT-T H.225.0 – (voir § F.7.1);
- signalisation d'appel (Rec. UIT-T H.225.0) – (voir § F.7.2);
- signalisation de commande de système multimédia (Rec. UIT-T H.245) – (voir § F.7.3);
- mise en paquets et transport des médias (Rec. UIT-T H.225.0, RTP) – (voir § F.7.4);
- services complémentaires (Recommandations UIT-T de la série H.450.x) – (voir § F.7.5 et § F.7.6);
- exploitation en pont de conférence – (voir § F.7.7);
- conférences à couplage non déterministe (Rec. UIT-T H.332) – (voir § F.7.8);
- bases d'informations de gestion – (voir § F.7.9).

Les services de sécurité spécifiés dans la Rec. UIT-T H.235.0 permettant de créer des dispositifs Audio SET sécurisés, sont traités au § F.8 "Extensions de sécurité".

F.7.1 Signalisation RAS (RAS H.225.0)

Les terminaux SET doivent être conformes aux procédures de signalisation RAS qui sont définies dans les Recommandations UIT-T H.323 (1998) et H.225.0 (1998) assorties des modifications ci-après qui s'appliquent.

Un dispositif SET doit utiliser les procédures de demande d'admission (ARQ) préaccordée telles qu'elles sont spécifiées dans la Rec. UIT-T H.225.0 (1998) et doit être capable de déterminer si une demande d'appel entrante provient de son portier. Un portier avec capacité SET doit prendre en charge les procédures de demande d'admission préaccordée et doit donner l'autorisation préalable

pour le lancement et la réception d'appels acheminés par l'intermédiaire du portier en ce qui concerne les dispositifs SET (à indiquer dans la composante preGrantedARQ). Lorsqu'un portier contacté ne prend pas en charge les procédures de demande d'admission préaccordée ou ne fournit pas les autorisations préalables susmentionnées, le dispositif SET doit s'enregistrer auprès d'un autre portier.

Les dispositifs SET doivent, au moins, prendre en charge les messages RAS suivants: envoi de GRQ, RRQ, URQ, UCF et XRS et réception de GCF, GRJ, RCF, RRJ, URQ, UCF, URJ et XRS. Les dispositifs SET peuvent prendre en charge d'autres messages RAS.

Lorsqu'il communique avec un portier, un dispositif SET doit inclure la composante "set" du type d'extrémité H.225.0 et attribuer les valeurs suivantes aux bits:

bit 0: = 1 si le dispositif possède une fonctionnalité Audio SET;

bit 1: = 0 s'il s'agit d'un dispositif sans capacité de conférence;

bit 1: = 1 s'il s'agit d'un dispositif avec capacité de conférence.

L'utilisation des autres bits sera définie dans des spécifications additionnelles relatives aux dispositifs SET.

F.7.2 Signalisation d'appel (Commande d'appel H.225.0)

Les terminaux SET doivent être conformes aux procédures de commande d'appel définies dans les Recommandations UIT-T H.323 (1998) et H.225.0 (1998). Ils ne doivent pas fermer le canal de signalisation d'appel après l'établissement de celui-ci.

Les terminaux SET doivent appliquer les procédures FastConnect comme spécifié dans la Rec. UIT-T H.323 (1998). Lorsqu'il émet un appel, un dispositif SET doit établir l'appel au moyen de la procédure FastConnect.

Les dispositifs SET doivent prendre en charge les messages d'information H.225.0 dans le canal de signalisation d'appel. Ces messages doivent servir, entre autres, à acheminer les indications introduites par l'utilisateur dans l'élément d'information du clavier (Keypad Information Element).

Les dispositifs SET doivent utiliser les messages de demande d'état et d'état visés par la Rec. UIT-T H.225.0 afin d'évaluer les temps d'aller-retour vers leur homologue.

Les terminaux Audio SET peuvent implémenter un établissement d'appel fondé sur le protocole UDP comme décrit dans l'Annexe E. Dans ce cas, le dispositif Audio SET doit d'abord tenter d'appeler une autre extrémité au moyen d'un établissement d'appel de type UDP.

L'implémentation de services complémentaires sur la base H.450.x est facultative pour les terminaux Audio SET. Ceux-ci doivent avoir la capacité de ne pas tenir compte des messages Facility H.225.0 qu'ils ne comprennent pas, sans que cela mette en cause la sécurité.

Lorsqu'il échange des unités PDU de signalisation d'appel avec son homologue, un dispositif SET doit inclure la composante "SET" du type d'extrémité H.225.0. Les valeurs des bits de la composante "SET" doivent être attribuées comme indiqué au § F.7.1.

F.7.3 Signalisation de commande de système multimédia (H.245)

F.7.3.1 Canal de commande H.245

La procédure FastConnect doit être utilisée pour l'établissement d'une connexion. Il convient de répéter la transmission de l'élément fastStart dans les messages de signalisation d'appel H.225.0 pour reconfigurer ou réacheminer les trains de médias.

Les terminaux SET ne doivent pas ouvrir de connexion H.245 distincte:

a) ils doivent limiter la signalisation H.245 à la "structure **OpenLogicalChannel** de la séquence FastConnect" ainsi qu'à la détermination implicite de maître/esclave;

b) si une autre signalisation H.245 est requise, les terminaux doivent effectuer la canalisation conformément à la Rec. UIT-T H.225.0 (1998).

Les terminaux SET doivent utiliser la syntaxe définie dans la Rec. UIT-T H.245 (1998) ou versions ultérieures.

Aucune procédure spécifique n'est définie pour les messages H.245. Si des dispositifs Audio SET implémentent des fonctionnalités H.245, ils doivent suivre les procédures définies dans les Recommandations UIT-T H.323, H.225.0 et H.245.

F.7.3.2 Détermination maître/esclave

Les dispositifs SET sont sensés assumer le rôle d'esclave dans toute communication effectuée sans canal de commande H.245.

Lorsqu'une canalisation H.245 est établie et conformément aux règles du § 6.2.8.4/H.323 (1998), le dispositif SET doit indiquer une valeur de 40 pour le type de terminal (**terminalType**). Cela garantit que, si un dispositif Audio SET se connecte à un dispositif H.323 (1998), celui-ci décidera de la détermination maître/esclave.

F.7.3.3 Echange de capacités de terminal

Bien que les dispositifs SET soient par définition limités dans l'étendue des fonctions qu'ils prennent en charge, une procédure d'échange de capacités ne peut pas être exclue afin de permettre une diversité minimale des terminaux. L'étendue des capacités pouvant être signalées par une extrémité Audio SET est cependant limitée à ce qui est défini ci-après et les procédures d'échange de capacités doivent être conformes aux règles indiquées dans le présent paragraphe.

La procédure d'échange de capacités relatives aux types de médias et aux modes de transmission doit être appliquée conformément aux règles de la procédure FastConnect au moyen de multiples structures d'ouverture de voie logique sous la forme d'une sélection de possibilités offertes par l'appelant, parmi lesquelles l'appelé choisit un sous-ensemble pour l'émission et la réception.

Le paragraphe ci-après énumère les capacités qui doivent être comprises du côté récepteur (appelé) et qui peuvent être émises du côté émetteur (appelant) pour des dispositifs Audio SET.

F.7.3.3.1 Capacités audio

- G.711 (loi μ, loi A, 56 kbit/s, 64 kbit/s)

  Les variantes suivantes doivent être prises en charge:

```
AudioCapability.g711Alaw64k        ≥ 20     nombre de trames
AudioCapability.g711Alaw56k        ≥ 20     nombre de trames
AudioCapability.g711Ulaw64k        ≥ 20     nombre de trames
AudioCapability.g711Ulaw56k        ≥ 20     nombre de trames
```

- G.723.1 (suppression ou non-suppression des silences, débit bas ou élevé)

  Un dispositif SET G.723.1 doit au moins prendre en charge:

```
AudioCapability.g7231
  maxAl-sduAudioFrames             ≥ 1      nombre de trames
  silenceSuppression                        Vrai/Faux selon le cas
```

- G.729 (normal ou selon Annexe A)

  Un dispositif SET G.729 doit au minimum prendre en charge:

```
AudioCapability.g729               ≥ 1      nombre de trames
AudioCapability.g729AnnexA         ≥ 1      nombre de trames
```

- GSM (plein débit, plein débit renforcé, demi-débit)

  Un dispositif SET GSM doit au moins prendre en charge:

```
AudioCapability.gsmFullRate         GSMAudioCapability,
AudioCapability.gsmHalfRate         GSMAudioCapability,
AudioCapability.gsmEnhancedFullRate GSMAudioCapability
```

  la capacité audio GSM étant définie comme suit pour chacun de ces débits:

```
GSMAudioCapability.audioUnitSize    ≥ 1      nombre de trames
GSMAudioCapability.comfortNoise              Vrai/Faux selon le cas
GSMAudioCapability.scrambled                 Vrai/Faux selon le cas
```

F.7.3.3.2 Capacité vidéo

Les dispositifs Audio SET ne prennent pas en charge la vidéo.

F.7.3.3.3 Capacité de transmission de données

Les dispositifs Audio SET ne prennent pas en charge la transmission de données.

F.7.3.3.4 Capacité de conférence

Les dispositifs SET sont censés passer par un serveur intermédiaire avant d'entrer dans les conférences centralisées avec distribution centralisée des données (voir § F.7.7).

F.7.3.3.5 Capacité d'entrée d'informations d'utilisateur

Les dispositifs SET doivent prendre en charge la transmission de tonalités DTMF en tant qu'éléments d'information de clavier dans la connexion de signalisation d'appel H.225.0 (en utilisant par exemple des messages d'information).

F.7.3.3.6 Capacité de sécurité

La sécurité des dispositifs SET – c'est-à-dire la définition des dispositifs SET sécurisés – fera l'objet d'une étude complémentaire. Voir également le § F.8.

F.7.3.3.7 Paramètre maxPendingReplacementFor

Cette capacité doit être prise en charge par les dispositifs Audio SET. Une valeur égale à "1" doit être implicitement prise par défaut.

```
maxPendingReplacementFor = 1
```

Le paramètre **maxPendingReplacementFor** ne doit donc pas être signalé explicitement.

F.7.3.3.8 Paramètre nonStandardCapability

Il convient d'éviter autant que possible l'utilisation de capacités non normalisées, au niveau supérieur de la structure de capacités ainsi qu'à l'intérieur des catégories de capacité susmentionnées.

F.7.3.3.9 Règles additionnelles pour l'utilisation des capacités

En ce qui concerne les dispositifs Audio SET, les capacités audio ne doivent être signalées qu'au moyen de la procédure FastConnect et de l'échange répété de structures **OpenLogicalChannel** utilisant cette procédure.

Les capacités de transmission vidéo, de transmission de données, de conférence, de sécurité et de chiffrement H.233 ne doivent pas être utilisées.

Les valeurs d'entrée dans la table MultiplexCapability d'un dispositif Audio SET sont censées être les suivantes:

```
maximumAudioDelayJitter                  ≥ 250 ms
receiveMultipointCapability,
transmitMultipointCapability, and
receiveAndTransmitMultipointCapability
    multicastCapability                  VRAI/FAUX selon le cas, par
                                         défaut: FAUX[1]
    multiUnicastConference               VRAI/FAUX selon le cas, par
                                         défaut: FAUX[1]
    mediaDistributionCapability
        centralizedControl               VRAI
        distributedControl               FAUX
        centralizedAudio                 VRAI
        distributedAudio                 VRAI/FAUX selon le cas, par
                                         défaut: FAUX[1]
        centralizedVideo                 FAUX
        distributedVideo                 FAUX
        centralizedData                  ABSENT
        distributedData                  ABSENT
mcCapability
    centralizedConferenceMC              FAUX
    decentralizedConferenceMC            FAUX
rtcpVideoControlCapability               ABSENT
mediaPacketizationCapability             ABSENT
...,
transportCapability                      ABSENT
redundancyEncodingCapability             Codage (éventuel) de redondance
                                         audio seulement
logicalChannelSwitchingCapability        FAUX
t120DynamicPortCapability                FAUX
```

Les capacités signalées par l'extrémité distante et non comprises doivent être ignorées.

F.7.3.4 Messages de signalisation de voies logiques

L'ouverture de voies logiques doit être conforme aux spécifications FastConnect de la Rec. UIT-T H.323 (1998).

En outre, les dispositifs SET doivent prendre en charge la reconfiguration des trains de médias à tout moment au cours d'une communication. Les structures d'ouverture de voie logique doivent être canalisées dans les messages de signalisation de communication H.225.0 conformément aux procédures définies dans les Recommandations UIT-T H.225.0 (1998) et H.323 (1998) avec réutilisation de l'élément fastStart de la structure H.225.0 de signalisation d'appel. Les structures d'ouverture de voie logique extérieures à la procédure FastConnect doivent être utilisées pour modifier des paramètres de flux média, afin d'offrir une base aux services complémentaires. De telles structures d'ouverture de voie logique doivent être interprétées à la réception comme suit.

- Si le numéro de voie logique correspond à une voie logique déjà ouverte, la voie concernée doit être reconfigurée conformément aux principes de la procédure FastConnect lorsque la composante **dataType** (type de données) ne vaut pas "null" (néant). Dans le cas où la composante **dataType** vaut "null" – indiquant une voie "NullChannel" – la voie logique correspondante doit être considérée comme fermée et la transmission de médias doit cesser sur cette voie logique.

---

[1] Les données audio en multidiffusion, en multiunidiffusion et répartie peuvent être prises en charge par les dispositifs Audio SET possédant la capacité de conférence.

- Si le numéro de voie logique ne correspond pas à une voie logique déjà ouverte, une nouvelle voie logique doit être ouverte selon les principes de la procédure FastConnect."

Les restrictions apportées aux requêtes d'ouverture de voie logique sont décrites ci-dessous:

```
OpenLogicalChannel
   forwardLogicalChannelNumber        LogicalChannelNumber
   forwardLogicalChannelParameters
      portNumber                      ABSENT
      dataType                        type de données audio valide
                                      (voir § F.7.3.3.1)
      multiplexParameters             CHOICE: h2250LogicalChannelParameters
      forwardLogicalChannelDependency ABSENT,
      replacementFor                  utilisé si une autre voie logique est
                                      à remplacer

   reverseLogicalChannelParameters
      dataType                        type de données audio valide
                                      (voir § F.7.3.3.1)
      multiplexParameters             CHOICE:h2250LogicalChannelParameters
      reverseLogicalChannelDependency LogicalChannelNumber OPTIONAL,
      replacementFor                  utilisé si une autre voie logique est
                                      à remplacer
   separateStack                      ABSENT
   encryptionSync                     ABSENT pour disp. Audio SET; à
                                      étudier.
```

Les restrictions suivantes s'appliquent à la structure **H2250LogicalChannelParameters**:

```
H2250LogicalChannelParameters
    nonStandard                    devrait être ABSENT
    sessionID                      INTEGER(0..255)
    associatedSessionID            ABSENT
    mediaChannel                   TransportAddress – devrait être une
                                   adresse d'unidiffusion
    mediaGuaranteedDelivery        ABSENT
    mediaControlChannel            PRESENT – voie RTCP inverse
    mediaControlGuaranteedDelivery FAUX
    silenceSuppression             (selon le cas)
    destination                    normalement ABSENT
    dynamicRTPPayloadType          (selon le cas),
    mediaPacketization             (selon le cas); ne peut spécifier que le
                                   format de capacité utile utilisé
        rtpPayloadType
        payloadDescriptor          doit se rapporter à un numéro de RFC
        payloadType                valeur de type de capacité utile
                                   (dynamique) à utiliser

    transportCapability
        nonStandard                devrait être ABSENT
        qOSCapabilities            devrait être ABSENT (ne peut contenir
                                   que des paramètres RSVP)
        mediaChannelCapabilities   devrait être ABSENT (peut indiquer
                                   "ip-udp")

    redundancyEncoding             seule la redondance audio est autorisée
    source                         normalement ABSENT
```

F.7.4 Echange relatif aux flux médias

Pour l'échange relatif aux flux médias, les terminaux SET doivent suivre les procédures H.323 et H.225.0 au moyen des protocoles RTP/UDP/IP afin d'acheminer les flux médias. Les formats appropriés de mise en paquets des flux médias doivent être utilisés.

F.7.5 Services complémentaires (H.450.x)

La prise en charge des services complémentaires conformément aux Recommandations UIT-T de la série H.450.x est facultative.

NOTE – Si la fonctionnalité H.450.x n'est pas offerte par un dispositif SET, celui-ci doit implémenter la fonctionnalité de rejet de message (unité APDU d'interprétation) de la Rec. UIT-T H.450.1 afin de permettre à son homologue de déterminer rapidement l'indisponibilité de services complémentaires du côté du dispositif SET. Si le rejet de message H.450.1 n'est pas implémenté, l'homologue doit faire appel à une temporisation.

Une référence pour les services complémentaires devant être pris en charge par les dispositifs SET fera l'objet d'une étude complémentaire.

F.7.6 Pause et reroutage à l'initiative d'une tierce partie

La prise en charge de la pause avec reroutage à l'initiative d'une tierce partie est similaire aux procédures décrites au § 8.4.6/H.323 (1998), avec les modifications suivantes.

F.7.6.1 Côté émetteur

Pour rerouter une connexion vers un dispositif SET, son homologue (normalement un portier) doit émettre une spécification NullChannel dans l'élément fastStart d'un message du canal de signalisation d'appel.

Ensuite, l'entité initiatrice doit réémettre (pour le nouvel homologue) les structures **OpenLogicalChannel** appropriées, comme pour la négociation de capacités et l'établissement d'un flux média dans la procédure FastConnect, et inclure les nouvelles adresses de transport afin de réacheminer le flux média issu du dispositif SET. Les structures **OpenLogicalChannel** sont transportées dans un message H.225.0 de signalisation d'appel.

La structure **OpenLogicalChannel** doit contenir les mêmes codages audio que ceux qui étaient offerts dans l'appel initial.

F.7.6.2 Côté récepteur (dispositif SET)

Dès réception d'une spécification NullChannel dans un élément fastStart, un dispositif SET doit arrêter immédiatement l'émission du ou des flux médias et doit être prêt à traiter les interruptions contenues dans le ou les flux médias reçus. Le dispositif SET doit attendre un nouvel échange de capacités et d'adresses de transport, conformément aux principes de la procédure FastConnect.

Dès réception d'une structure **OpenLogicalChannel** contenue dans un message de signalisation d'appel H.225.0, le dispositif SET doit sélectionner un codage de média acceptable d'après la sélection offerte par l'entité initiatrice, conformément aux règles de la procédure FastConnect. Le dispositif SET doit ensuite commencer l'émission de son ou de ses flux médias vers l'adresse ou les adresses de transport récemment indiquées dans les structures **OpenLogicalChannel.**

F.7.7 Fonctionnement en mode conférence

Les terminaux SET peuvent participer de deux façons à des conférences multipoint:

- en accédant à une conférence par un serveur intermédiaire au moyen d'un dispositif externe spécialisé, comme un dispositif SET à capacité de pont MC combiné à un serveur intermédiaire approprié et spécifique de point MP ou de dispositif SET comme décrit au § F.7.7.1, en tant que mode de fonctionnement par défaut de dispositifs SET;
- ou en implémentant les procédures nécessaires des protocoles H.225.0 et H.245, décrites dans ce paragraphe. Ce mode de fonctionnement est défini au § F.7.7.2.

F.7.7.1 Terminaux SET sans capacité de conférence

Le mode de fonctionnement par défaut des terminaux SET n'exige aucune compatibilité avec la fonctionnalité de conférence dans de tels terminaux. Par contre, on suppose l'existence d'une entité

externe qui joue le rôle de pont entre un dispositif pleinement conforme à H.323 et le dispositif SET. Cette entité logique peut être un dispositif intermédiaire autonome ou peut faire partie d'un pont de conférence, d'une passerelle ou d'un portier.

NOTE – La fonctionnalité d'une entité logique de pontage inclut les fonctions suivantes:

- masquage de l'existence de commandes H.245 relatives à une conférence et réponse appropriée au dispositif pleinement H.323;
- adaptation de la capacité H.245 et de la signalisation de voie logique, y compris les commandes de mode multipoint;
- mélange de plusieurs flux audio entrants et injection d'un flux unique dans le dispositif SET;
- conversion des adresses de transport pour le flux audio;
- transcodage des flux audio;
- fourniture d'un accès aux fonctions de commande de conférence au moyen de moyens simples (comme la signalisation DTMF) d'entrée dans le dispositif SET.

F.7.7.2 Terminaux SET avec capacité de conférence

La spécification des dispositifs SET avec capacité de conférence doit faire l'objet d'un complément d'étude.

Toutefois, les dispositifs SET peuvent suivre, dans leur intégralité, les procédures relatives au fonctionnement en mode conférence définies dans les Recommandations UIT-T de la série H.323.

F.7.8 Prise en charge des conférences à couplage non déterministe (Rec. UIT-T H.332)

La prise en charge des conférences à couplage non déterministe conformément à la Rec. UIT-T H.332 est facultative:

- la participation en tant que membre du comité est facultative. Elle est possible soit si le fonctionnement en mode conférence et la distribution du flux média par multidiffusion sont pris en charge, soit si une combinaison MC/MP appropriée masque toutes les commandes de conférence au dispositif SET et ne présente qu'un flux audio unique;
- la participation en tant que membre de l'audience est facultative. Elle est possible si le dispositif SET prend en charge la réception des informations multidiffusées et peut recevoir/interpréter les annonces de session H.332.

F.7.9 Bases d'information de gestion (MIB, *management information base*)

L'implémentation de bases d'information de gestion est facultative pour les dispositifs SET. Si des bases MIB sont incluses dans l'implémentation, les bases de type H.323 suivantes doivent être implémentées:

- signalisation d'appel;
- entité terminale;
- RAS;
- protocole en temps réel (RTP).

Des précisions sur cette question doivent faire l'objet d'un complément d'étude.

F.8 Extensions de sécurité

Les terminaux SET normaux ne possèdent pas la capacité de prendre en charge les services de sécurité H.235.0. Les dispositifs SET sécurisés constituent cependant une extension simple des dispositifs SET, assurant la fonctionnalité de sécurité au moyen d'un sous-ensemble des mécanismes spécifiés dans la Rec. UIT-T H.235.0.

La sécurisation des dispositifs SET est traitée dans l'Annexe J.

F.9 Considérations relatives à l'interopérabilité

La présente annexe spécifie un dispositif SET ainsi qu'un sous-ensemble bien défini de la pleine fonctionnalité H.323.

Les dispositifs SET doivent toujours être utilisés en liaison avec des portiers compatibles avec ces dispositifs. Ces portiers doivent exécuter la procédure de demande d'admission préaccordée et doivent utiliser le modèle d'appel acheminé par portier afin d'assurer la pleine interopérabilité avec d'autres dispositifs H.323 (1996) et H.323 (1998).

Par ailleurs, la compatibilité avec les dispositifs SET peut être intégrée dans les ponts MC(U) ou dans les passerelles afin d'assurer une interopérabilité sans discontinuité.

Le Tableau F.1 donne un aperçu général de l'interopérabilité obtenue entre dispositifs SET et d'autres extrémités H.323.

Tableau F.1/H.323 – Interopérabilité des dispositifs SET avec d'autres dispositifs H.323

	H.323 (1996)	**H.323 (1998)**	**H.323 (1998) avec FastConnect**	**Dispositif SET**
H.323 (1996)	√	√	√	√ (GK)
H.323 (1998)	√	√	√	√ (GK)
H.323 (1998) avec Fast Connect	√	√	√	√ a)
SET device	√ (GK)	√ (GK)	√ a)	√

(GK) Indique qu'un portier compatible avec les dispositifs SET est nécessaire pour l'interfonctionnement.

a) Le réacheminement facultatif des canaux de flux média nécessite l'exécution répétée de la procédure FastConnect aux deux extrémités.

F.10 Notes d'implémentation (informatives)

Le présent paragraphe contient des informations sur le codage simple de la plupart des messages H.245 nécessaires, sans exiger de codeurs/décodeurs ASN.1 spécifiques.

NOTE – Tous ces messages sont transmis sous la forme de messages H.245 canalisés, c'est-à-dire que les séquences binaires résultantes sont codées sous la forme d'une simple chaîne d'octets (OCTET STRING) de la SEQUENCE dans la composante fastStart d'une unité H323-UU-PDU. Dans les tableaux ci-dessous, l'octet de gauche (octet #0) de la première rangée (mot #0) est placé comme premier octet dans la chaîne d'octets. Il est suivi de l'octet #1 de la première rangée, et ainsi de suite. L'octet #3 du mot #n est suivi de l'octet #0 du mot # (n+1).

Si des nombres doivent être codés, on fait appel au codage par complément à 2 pour les nombres qui peuvent être négatifs. Si ce n'est pas le cas, on fait appel au simple codage binaire. Le codage de nombres occupant plusieurs octets est fait de façon que le bit de poids fort de la valeur codée soit situé dans le premier octet de cette valeur (ordre des octets d'un réseau).

F.10.1 Ouverture de voie logique

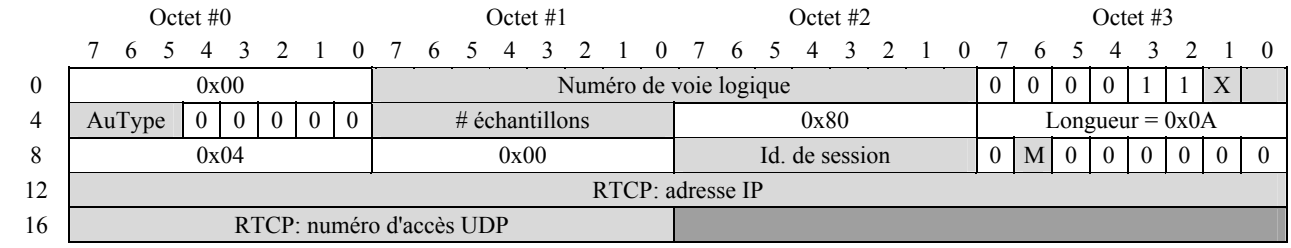
Les dispositifs SET utilisent les structures **OpenLogicalChannel** pendant la procédure FastConnect pour indiquer leurs capacités et ouvrir simultanément des canaux de média dans les deux sens. Par définition, les structures **OpenLogicalChannel** ne peuvent contenir que des paramètres de voie logique directe ou que des paramètres de voie logique inverse.

F.10.1.1 Paramètres de voie logique directe

Une structure Open Logical Channel ne contenant que les paramètres de voie logique directe **ForwardLogicalChannel** peut être codée de trois façons différentes, en fonction du type audio (AuType) et du bit X.

F.10.1.1.1 Recommandations UIT-T G.711 et G.729

La structure la plus courante est la suivante (Recommandations UIT-T G.711, G.729 et Annexe A/G.729):



Numéro de voie logique: ce champ contient le numéro de la voie logique H.245 – 1.

bit X: est utilisé pour distinguer les types audio de base des types audio étendus. Si X = 0, AuType (voir le champ suivant) s'applique; sinon (X = 1), les types audio étendus décrits ci-dessous s'appliquent (principalement GSM) assortis d'une structure de paquet différente;

AuType: détermine le codec audio à utiliser. Les valeurs suivantes sont acceptables pour le type audio. Le bit situé le plus à gauche est placé dans le bit 1 de l'octet #3, celui situé le plus à droite est placé dans le bit 5 de l'octet #4;

N°	Description du codec	Valeur AuType
1	G.711 loi A 64 kbit/s	0001
2	G.711 loi A 56 kbit/s	0010
3	G.711 loi μ 64 kbit/s	0011
4	G.711 loi μ 56 kbit/s	0100
5	G.723.1	1000
6	G.729	1010
7	Annexe A/G.729	1011
8	GSM et autres (voir ci-dessous)	X = 1

échantillons: pour les codecs 1, 2, 3, 4, 6 et 7, cette composante contient le nombre d'échantillons – 1 par paquet audio tel que défini dans la Rec. UIT-T H.245;

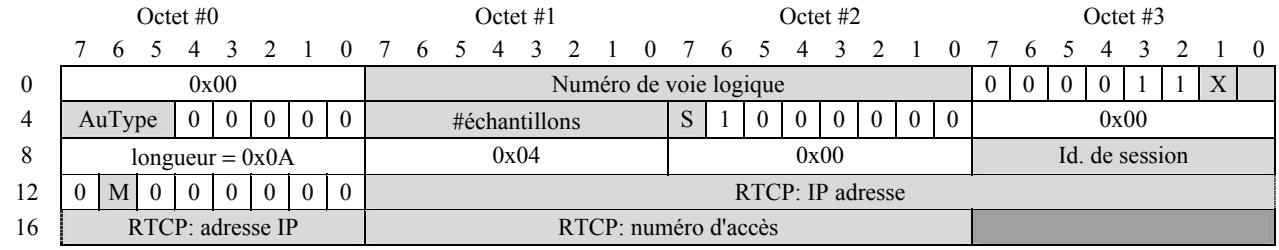
id. de session: contient le paramètre d'identification de la session à utiliser conjointement avec RTP/RTCP;

bit M: bit d'adresse de multidiffusion: indique que l'adresse suivante est une adresse de multidiffusion. Tandis que de nombreux types d'adresse sont définis en plus de l'adresse IPv4 (y compris IPv6 et IPX), les structures données ici ne sont valables que pour les adresses IPv4;

adresse/accès IP RTCP: contient l'adresse de transport à laquelle les rapports du récepteur RTCP doivent être envoyés.

F.10.1.1.2 Codec G.723.1

Dans ce cas, la structure est légèrement modifiée comme suit:

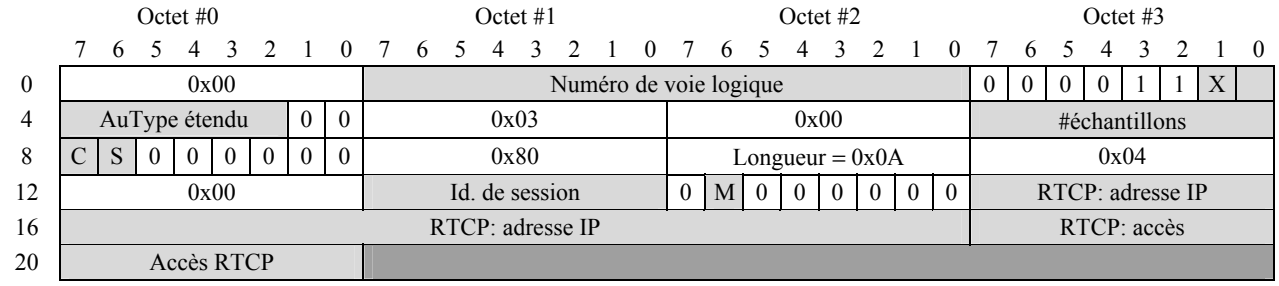


La signification des champs est identique à celle définie dans le format ci-dessus. Par ailleurs, le champ ci-après est défini:

bit S: indique la prise en charge de la suppression des silences, si S = 1.

F.10.1.1.3 GSM

Pour la capacité GSM, identifiée par le bit #1 de l'octet #3 mis à X = 1, la structure est la suivante:



La signification de champs est identique à celle définie dans les formats de paquet ci-dessus. Par ailleurs, les champs ci-après sont définis pour le GSM:

type Audio étendu: identifie le codec audio étendu:

plein débit du GSM = 000 0011

demi-débit du GSM = 000 0100

plein débit renforcé du GSM = 000 0101

bit C: C = 1 indique la prise en charge/l'utilisation d'un bruit de confort

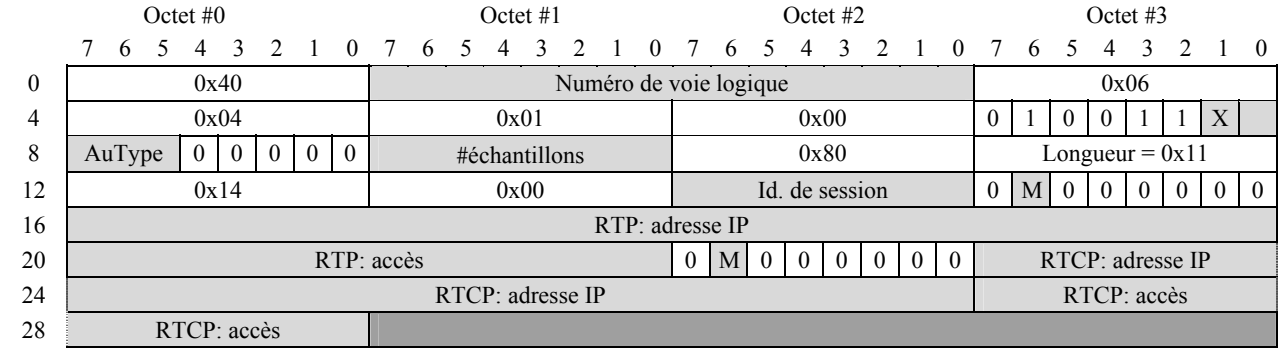
bit S: S = 1 indique la prise en charge/l'utilisation de l'embrouillage.

F.10.1.2 Paramètres de la voie logique inverse

Les messages Open Logical Channel contenant les paramètres de la voie logique inverse **ReverseLogicalChannel** sont codés comme indiqué ci-dessous.

F.10.1.2.1 Recommandations UIT-T G.711 et G.729

La structure la plus courante est la suivante (Recommandations UIT-T G.711, G.729 et Annexe A/G.729):



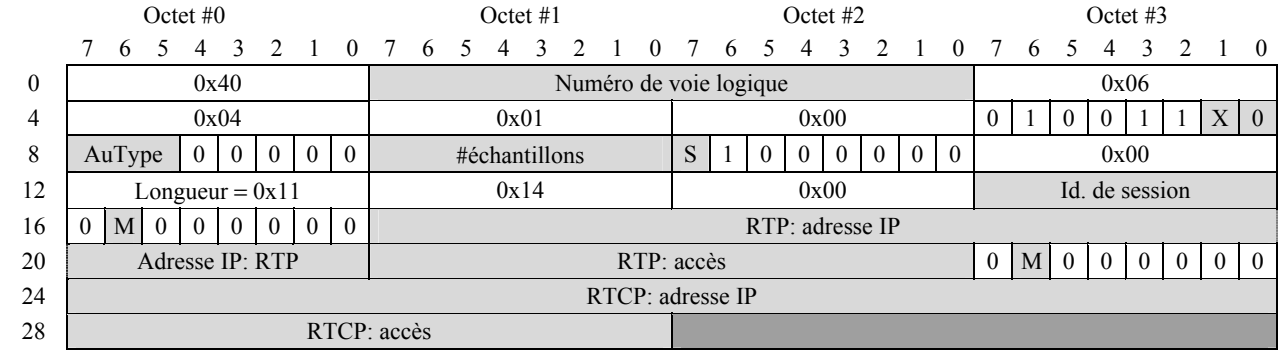
Les champs ont la même signification que celle donnée ci-dessus. Les champs ci-après sont par ailleurs définis:

Adresse/accès RTP IP: adresse de transport cible à laquelle le train de données audio RTP doit être envoyé

Adresse/accès RTCP IP: adresse de transport cible à laquelle les rapports d'expéditeur RTCP doivent être envoyés

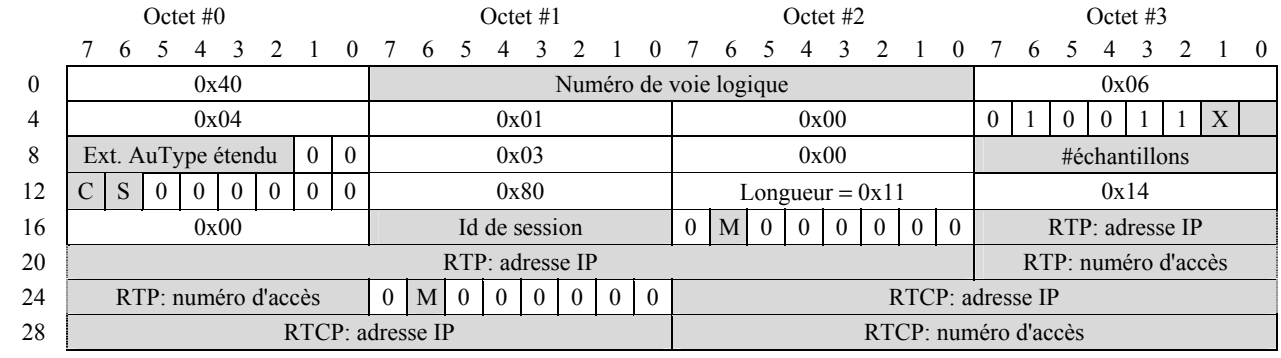
F.10.1.2.2 Rec. UIT-T G.723.1

Dans ce cas, la structure diffère légèrement de la précédente:



F.10.1.2.3 GSM

Dans le cas de la capacité GSM, identifiée par le bit #1 de l'octet #7 mis à X = 1, la structure est la suivante:



AuType étendu: identifie le codec audio étendu (GSM) à utiliser comme suit:

plein débit du GSM = 000 0011

demi-débit du GSM = 000 0100

plein débit renforcé du GSM = 000 0101

Annexe G

Conversation en mode texte et type d'extrémité textophonique simple

G.1 Introduction

Des fonctionnalités normalisées de conversation alphanumérique en mode texte sont nécessaires dans tous les réseaux. La création de fonctionnalités de conversation en mode texte dans des protocoles multimédias permet l'utilisation de toute combinaison de texte, vidéo et voix dans une conversation. La normalisation de cette combinaison répond aux besoins des personnes souffrant de problèmes de communication. La combinaison des trois médias dans une conversation offre des possibilités de communication supérieures à un seul de ces médias. Ainsi, tout le monde aura la possibilité d'utiliser un système de conversation en mode texte normalisé, doté de fonctions de conversation multimédia intéressantes, améliorant la visiophonie et permettant une "conversation totale".

Etant donné que la Rec. UIT-T H.323 définit un cadre extensible, des terminaux à fonction uniquement alphanumérique ainsi que des terminaux à double fonction vocale et alphanumérique peuvent constituer des sous-ensembles utiles du terminal de conversation totale complet. Ces sous-ensembles correspondent à des textophones compatibles avec le RTPC.

La Rec. UIT-T T.140 [G1] spécifie un protocole de conversation en mode texte. Il s'agit d'un niveau de présentation commun pour les conversations directes en temps réel et en mode texte dans les services multimédias et en textophonie. Ce protocole utilise le jeu de caractères ISO/CEI 10646 adaptable à n'importe quelle langue. Il est défini dans plusieurs protocoles multimédias de la série H.

Cette spécification décrit la manière dont les fonctionnalités de conversation en mode texte sont ajoutées à l'environnement multimédia H.323 dans les réseaux en mode paquet.

La fonctionnalité de conversation en mode texte est établie dans une voie de données ou dans une voie audio (collectivement dénommées les "voies de média") identifiée par le message **OpenLogicalChannel** H.245. Dans une voie de données, la même identification est utilisée pour l'ouverture des voies de conversation en mode texte H.324. Seuls le protocole et les procédures prévus pour l'acheminement des données T.140 sur la voie de données diffèrent. L'interfonctionnement des systèmes H.324 et des systèmes H.323 est fondé sur l'hypothèse que les dispositifs utiliseront une voie de données pour l'acheminement de texte. Par conséquent, la prise en charge de la voie de données pour l'acheminement de texte est recommandée pour l'ensemble des dispositifs H.323 implémentant la présente annexe.

Ainsi, la conversation totale est implémentée de façon uniforme dans différents réseaux, ce qui réduit la complexité des passerelles et des autres éléments de réseau.

G.2 Domaine d'application

La présente annexe spécifie les procédures H.323 nécessaires pour établir et acheminer des sessions de conversation en mode texte en temps réel dans des réseaux en mode paquet, dans l'environnement multimédia H.323. Elle spécifie également les règles d'utilisation des prescriptions de la Rec. UIT-T H.323 qui permettent de créer des dispositifs d'extrémité textophonique simple (Text SET, *text conversation simple endpoint type devices*) en tant que surensembles dispositifs d'extrémité audio simple spécifiés dans l'Annexe F. La spécification relative au dispositif d'extrémité textophonique simple décrit un dispositif pouvant être utilisé pour des conversations en temps réel, simultanément en mode texte et en mode vocal, dans des réseaux en mode paquet.

G.3 Références normatives

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

[G1] Recommandation UIT-T T.140 (1998), *Protocole de conversation en mode texte pour application multimédia,* plus Addendum 1 (2000).

[G2] RFC 4103 (2005), *RTP payload for text conversion*.

[G3] RFC 4351 (2006), *RTP payload for text conversion interleaved in an audio stream*.

G.4 Définitions

La présente annexe définit les termes suivants:

G.4.1 conversation totale: services de conversation offrant une communication en temps réel en modes vidéo, texte et vocal simultanément.

G.4.2 T140PDU: unité de données protocolaire spécifiée dans la Rec. UIT-T T.140 = collection de données présentées au format T.140 pour la transmission.

G.5 Indication des capacités pour les communications en mode texte dans le cadre de la Rec. H.323

La prise en charge de la communication en mode texte peut être indiquée au moyen de deux capacités différentes dans le cadre de la Rec. H.323. La première est la capacité **DataApplicationCapability.application.t140** qui fait partie de la spécification H.245. Elle constitue l'un des moyens d'ouvrir une voie de données qui prend en charge la transmission de communication en mode texte. Elle correspond à l'extension de type MIME "text/t140" décrite dans le document de référence visé au [G2]. Tandis que le document de référence [G2] décrit seulement le transport d'une communication en mode texte via le protocole RTP, la capacité **DataApplicationCapability.application.t140** peut, quant à elle, être également utilisée via le protocole TCP, au lieu du protocole RTP.

La capacité **DataApplicationCapability.application.t140** a été le premier identificateur de capacité ajouté à la Rec. H.245 pour la prise en charge de la conversation en mode texte. Lorsque des améliorations ultérieures ont été apportées à la spécification du protocole RTP pour le transport de la conversation en mode texte ([G2]), un nouveau paramètre a été ajouté pour permettre à un dispositif d'indiquer le nombre de caractères qu'il peut recevoir par seconde. D'autres améliorations ont également été apportées pour permettre le transport de la conversation en mode texte via un flux RTP distinct ou entrelacée avec d'autres informations audio, ce qui correspond à l'extension de type MIME "audio/t140c" décrite dans le document de référence visé au [G3]. La capacité de transporter une conversation en mode texte entrelacée avec des données audio a été créée pour permettre aux passerelles RTPC d'extraire des signaux textophoniques RTPC et de transporter ces signaux avec le flux audio dans la même session RTP.

Afin de prendre en charge, d'une part, les paramètres les plus récents figurant dans les documents de référence [G2] et [G3] ainsi que toute autre révision ultérieure et, d'autre part, le transport d'une conversation en mode texte entrelacée avec des données audio, deux nouvelles capacités génériques sont définies dans le présent paragraphe pour la Rec. UIT-T H.245. Lorsqu'elles utilisent des capacités génériques avec ces paramètres, les entités H.323 doivent simplement ignorer tout

paramètre qu'elles ne reconnaissent pas. L'utilisation des identificateurs de paramètres **standard** 0 à 99 est réservée aux fins de la présente Recommandation. Les valeurs de paramètres **standard** comprises entre 100 et 127 sont réservées à des fins d'utilisation dans d'autres Recommandations de l'UIT-T.

Le champ **maxBitRate** de la capacité **DataApplicationCapability.application.t140** et des capacités génériques définies dans les sous-paragraphes suivants doit être considéré comme étant exprimé en unité de bits par seconde, par opposition au débit classique de 100 bit/s prévu dans la Rec. UIT-T H.245. Cette même interprétation s'applique à tous les messages H.245 qui contiennent un paramètre exprimé avec un débit binaire et qui ont trait à ces capacités de transport de la conversation en mode texte, y compris les messages Request Mode, Flow Control Command et Flow Control indication. A titre d'exemple, une valeur 192 représente 192 bits par seconde – soit environ six caractères par seconde lorsque les caractères font 3 octets chacun.

Etant donné que les documents de référence [G2] et [G3] utilisent la Rec. UIT-T T.140, qui définit un codage de caractères nécessitant entre 1 et 3 octets par caractère, les "bits par seconde" ne seront peut-être pas aussi utiles que le paramètre "caractères par seconde" défini au § G.5.3. Toutefois, les systèmes H.323 sont conçus pour fonctionner avec un débit exprimé en bits par seconde et non en caractères par seconde. Ainsi, les entités H.323 devraient calculer la valeur indiquée en bits par seconde à utiliser sur la base de 3 octets par caractère, même si un seul octet est requis pour la transmission des caractères. Cela permet aux systèmes d'établir la correspondance correcte entre les bits par seconde et les caractères par seconde. Cela est particulièrement important, car ainsi les dispositifs peuvent utiliser le message Flow Control Command, par exemple, pour contrôler de façon appropriée le débit de transmission de l'autre système et obtenir des résultats cohérents. Cela étant dit, le paramètre "caractères par seconde" demeure utile lorsqu'il est utilisé dans le cadre d'un message Multiple Payload Stream, étant donné que chaque élément ne comportera pas de valeur de débit binaire distincte dans le message Open Logical Channel.

NOTE – Le débit binaire maximal indiqué dans le message d'ensemble de capacités de terminal peut ne pas être le même que celui utilisé dans un message Open Logical Channel. Toute valeur indiquée dans un message Open Logical Channel ou dans des commandes de limitation du débit (par exemple, le message Flow Control Command) prévaut sur les valeurs indiquées dans un message d'ensemble de capacités de terminal.

G.5.1 Capacités de transport d'une conversation en mode texte dans la voie de données

La capacité **DataApplicationCapability.application.t140** d'origine n'est pas obsolète et, lorsqu'elle est indiquée en association avec le protocole UDP sélectionné comme protocole de transport, doit être traitée comme un équivalent de la nouvelle capacité définie ci-après de transport d'une conversation en mode texte dans la voie de données, à ceci près qu'elle sera dépourvue de paramètres. Même si la préférence va à la définition de la nouvelle capacité, la rétrocompatibilité avec les systèmes existants doit être maintenue, ce qui justifie la recommandation suivante: les dispositifs mettant en œuvre la présente annexe doivent indiquer la capacité **DataApplicationCapability.application.t140** et devraient indiquer la nouvelle capacité générique définie dans le présent paragraphe.

La capacité générique ci-après est définie pour le transport d'une conversation en mode texte dans une voie de données correspondant à l'extension de type MIME "text/t140" décrite dans le document de référence [G2]:

Nom de la capacité	T140Data
Classe de la capacité	Data Application Capability
Type de l'identificateur de la capacité	Standard
Valeur de l'identificateur de la capacité	itu-t (0) recommendation (0) h (8) 323 annex(1) g (7) data(0)
maxBitRate	Ce champ doit être inclus et indiquer le nombre maximal de bits par seconde. Lors de l'utilisation du message Flow Control Command ou d'autres signaux en rapport avec cette capacité, toute valeur figurant dans ce champ doit être interprétée comme étant exprimée en bits par seconde, contrairement au débit classique de 100 bit/s prévu dans la Rec. UIT-T H.245. Cela est dû au bas débit qui caractérise la communication en mode texte en temps réel
nonCollapsing	Ce champ ne doit pas être inclus et doit être ignoré s'il est reçu
nonCollapsingRaw	Ce champ ne doit pas être inclus et doit être ignoré s'il est reçu
transport	Ce champ ne doit pas être inclus

G.5.2 Capacité de transport de la conversation en mode texte dans une voie audio

La capacité générique ci-après est définie pour le transport de la conversation en mode texte dans une voie audio correspondant à l'extension de type MIME "audio/t140c" décrite dans le document de référence [G3]:

Nom de la capacité	T140Data
Classe de la capacité	Data Application Capability
Type de l'identificateur de la capacité	Standard
Valeur de l'identificateur de la capacité	itu-t (0) recommendation (0) h (8) 323 annex(1) g (7) audio(0)
maxBitRate	Ce champ doit être inclus et indiquer le nombre maximal de bits par seconde. Lors de l'utilisation du message Flow Control Command ou d'autres signaux en rapport avec cette capacité, toute valeur figurant dans ce champ doit être interprétée comme étant exprimée en bits par seconde, contrairement au débit classique de 100 bit/s prévu dans la Rec. UIT-T H.245. Cela est dû au bas débit qui caractérise la communication en mode texte en temps réel, y compris les bas débits binaires utilisés dans de nombreux protocoles textophoniques RTPC
nonCollapsing	Ce champ ne doit pas être inclus et doit être ignoré s'il est reçu
nonCollapsingRaw	Ce champ ne doit pas être inclus et doit être ignoré s'il est reçu
transport	Ce champ ne doit pas être inclus

G.5.3 Paramètre générique "caractères par seconde"

Lorsqu'elle utilise soit une capacité générique de transport dans la voie audio, soit une capacité générique de transport dans la voie de données pour acheminer une conversation en mode texte, une extrémité peut également indiquer, soit dans le message d'ensemble de capacités de terminal, soit dans le message Open Logical Channel ou encore dans ces deux messages, sa capacité de recevoir un nombre déterminé de caractères par seconde. Ce paramètre est défini dans les documents de référence [G2] et [G3] et il est signalé comme suit:

Nom du paramètre	cps
Description du paramètre	Il s'agit d'une capacité de type "collapsing". Indique le nombre maximal de caractères par seconde pouvant être reçu dans une session. Lorsqu'il est présent dans un message OLC, il indique le débit maximal de transmission que peut utiliser l'autre extrémité si elle ouvre une session en mode texte correspondante
Valeur de l'identificateur du paramètre	standard: 0
Etat du paramètre	Facultatif
Type du paramètre	unsignedMin
Remplace:	-

G.6 Procédures d'ouverture des voies pour la conversation en mode texte T.140

Les prescriptions relatives aux sessions de la Rec. UIT-T T.140 sont prises en considération dans la présente spécification pour l'établissement des voies utilisant la structure du message d'ouverture de voie logique H.245 dans l'environnement H.323.

Une voie fiable (TCP) ou non fiable (UDP) peut être sélectionnée pour l'acheminement de la session T.140 comme étant une voie de données. La voie non fiable doit toujours être prise en charge. Celle-ci peut être sélectionnée lorsque l'on s'attend que le terminal participera à des sessions où une voie fiable n'est pas favorable ou impossible à utiliser.

- Dans l'échange des capacités, lorsque l'on utilise une voie fiable, spécifier:

  DataApplicationCapability.application = t140
  DataProtocolCapability = tcp

- Dans l'échange des capacités, lorsque l'on utilise une voie fiable, spécifier:

  DataApplicationCapability.application = t140
  DataProtocolCapability = udp

  ou
  DataApplicationCapability.application = genericDataCapability
  (La capacité générique de transport dans une voie de données doit être spécifiée conformément au § G.5.1)
  ou
  AudioCapability = genericAudioCapability
  (La capacité générique de transport dans une voie audio doit être spécifiée conformément au § G.5.2)

- Dans la procédure d'ouverture de voie logique, spécifier:

  OpenLogicalChannel.forwardLogicalChannelParameters = dataType
  DataType = data

  Et sélectionner une voie fiable ou non fiable pour le transfert de données T.140 en spécifiant les capacités **DataApplicationCapability** et **DataProtocolCapability** comme ci-dessus.
  ou
  OpenLogicalChannel.forwardLogicalChannelParameters = dataType
  DataType = audioData

La sélection de **dataType**, qu'il s'agisse de la valeur **audioData** ou **Data**, dépend des capacités prises en charge et préférées.

Les procédures Fast Connect de démarrage rapide ou les procédures de signalisation de la voie logique H.245 normale peuvent être utilisées.

Les concepts de nœud de destination et de nœud d'origine de la Rec. UIT-T T.140 sont mappés avec les deux points d'extrémité H.323.

L'identité d'utilisateur T.140 est un alias pour le point d'extrémité distant H.323.

G.7 Mise en trame et mise en tampon des données T.140

La transmission des données T.140 doit être effectuée en fonction des spécifications suivantes, qui sont différentes de celles qui sont utilisées pour les voies fiables et non fiables.

NOTE – Dans le présent paragraphe et dans les suivants, le terme "données" renvoie aux données T.140, qu'elles soient transportées dans une voie "de données" ou une voie "audio". Le terme "voie de média" ou "voie" désigne la voie logique. Les termes "voie de données" ou "voie audio" sont mentionnés explicitement, lorsqu'une distinction est nécessaire.

G.7.1 Généralités

Les données T.140 peuvent être rassemblées dans une mémoire tampon avant leur transmission dans la voie. Cette mise en tampon est recommandée sur des voies à faible débit afin de réduire le surdébit de paquet. La mise en tampon des données dans des intervalles de 300 ms est recommandée par défaut.

A la réception, les données provenant de la voie de média sont récupérées et utilisées comme données T.140.

G.7.2 Utilisation de voies fiables

Lorsqu'une voie fiable est sélectionnée pour la transmission T.140, le protocole TCP est utilisé et les données T.140 sont transmises dans la voie sans mise en trame supplémentaire.

G.7.3 Utilisation de voies non fiables

Lorsqu'une voie non fiable est spécifiée pour la transmission T.140, le protocole RTP est utilisé. Les détails du format de charge utile RTP "T140" figurent dans [G2] et [G3]. Les procédures recommandées décrites dans ces références devraient être utilisées. L'attribution du type de charge utile est dynamique. Sauf indication explicite contraire, le type de charge utile sera 96 pour le format de charge utile "T140" de base et 98 pour des paquets avec redondance.

Ces procédures offrent la possibilité d'inclure un certain nombre d'unités PDU T.140 déjà transmises dans le paquet. Des données redondantes sont introduites en vue de réduire les risques de perte de données.

La station émettrice peut sélectionner un certain nombre de générations d'unités PDU T.140 pour les retransmettre dans chaque paquet. Un nombre assez élevé de générations garantit une bonne protection contre la perte de texte. Si les conditions de réseau ne sont pas connues, il est recommandé d'utiliser deux générations. Il est recommandé de ne pas utiliser plus de six générations.

Le protocole RTCP doit être utilisé pour surveiller la perte de paquets afin qu'une décision puisse être prise sur le nombre de générations de données redondantes à transmettre.

G.8 Interaction avec des fonctionnalités de conversation en mode texte dans d'autres dispositifs

Les informations contenues dans le présent paragraphe ne sont pas normatives. Elles ne sont données qu'à titre indicatif étant donné qu'elles dépassent le cadre de la présente annexe.

La Rec. UIT-T T.140 définit le protocole de conversation en mode texte dans plusieurs protocoles multimédias de la série H, pour la conférence de données T.120 et pour la textophonie conforme à la Rec. UIT-T V.18. Les voies de média sont spécifiques à chaque environnement.

Lorsque les passerelles vers ces différents environnements seront définies, la voie T.140 dans l'environnement H.323 sera mappée sur la voie T.140 dans le nouvel environnement. Les données de la voie T.140 pourront ainsi être transférées en transparence par la passerelle.

Lorsque les passerelles vers d'autres protocoles de conversation en mode texte seront définies, les mécanismes de données et de protocole du protocole de conversation en mode texte seront mappés sur une voie de conversation en mode texte T.140 dans la passerelle. On peut désigner ces fonctions de mappage sous le nom d'égaliseurs T.140. Les fonctions de passerelle des divers systèmes de textophonie font intervenir des égaliseurs T.140.

La Figure G.1 donne un aperçu des protocoles de conversation en mode texte et des services passerelles.

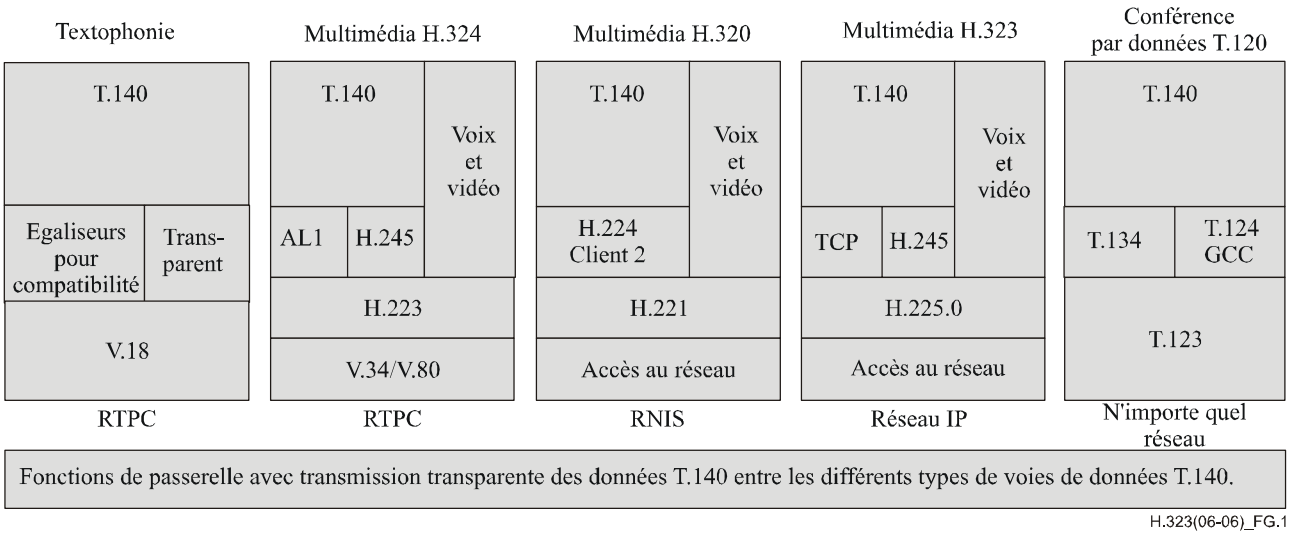


Figure G.1/H.323 – Recommandations relatives à la conversation en mode texte en temps réel pour application multimédia et besoins d'interfonctionnement

G.9 Configurations multipoint

En l'absence d'autres spécifications, les points d'extrémité H.323 possédant une fonctionnalité de conversation en mode texte T.140 peuvent participer à des conversations en mode texte multipoint de plusieurs façons:

Alternatives:

- une voie T.140 individuelle est établie pour chaque point d'extrémité distant H.323. Les flux de texte peuvent être coordonnés pour l'affichage, par l'intermédiaire d'une interface utilisateur compatible avec le mode multipoint, qui transmet également les données T.140 à tous les points d'extrémité connectés;
- un pont de conférence coordonne le flux de données T.140 contenant les données d'un certain nombre de points d'extrémité distants avec le point d'extrémité H.323;
- contrairement aux procédures décrites dans la présente annexe, le membre d'application T.134 de la conférence par données T.120 est utilisé comme voie pour les données T.140. Les sessions multipoint sont coordonnées avec les concepts T.120.

G.9.1 Configurations de conversation en mode texte multipoint

Afin de préciser l'utilisation de la conversation en mode texte et, en particulier, les différentes configurations multipoint, des exemples non normatifs de dispositions d'affichage et d'applications possibles sont donnés ci-après.

G.9.1.1 Conversation entre deux personnes

Dans cette configuration, qui consiste en une conversation directe en mode texte entre deux personnes, le texte entré à un point d'extrémité est affiché caractère par caractère ou par petits groupes de caractères au moment où il est reçu à l'autre point d'extrémité. Comme exemples de cette configuration, on peut citer la textophonie traditionnelle dans le RTPC et la conversation multimédia (vidéo, texte et données) utilisée pour un appel entre deux personnes. Voir Figure G.2.

Anne	Eve
Salut, c'est Anne. Es-tu au courant que je serai à Paris en novembre?	Ah! Salut Anne. Je suis contente que tu m'appelles! Non, je ne savais pas. Qu'est ce qui t'amène ici?

Figure G.2/H.323 – Possibilité d'affichage d'une session de texte dans une conversation entre deux personnes

G.9.1.2 Conversation entre plus de deux personnes

Tous les utilisateurs ont le droit de taper un message, ce qui correspond à une conférence non dirigée.

Une possibilité de disposition de l'affichage consiste à avoir une fenêtre par participant, comme il est spécifié dans la Rec. UIT-T T.140. Voir Figure G.3.

Anne	Eve
Salut, c'est Anne. Es-tu au courant que je serai à Paris en novembre?	Ah! Salut les copains! Comment vas-tu Stéphane?
Stéphane	**Eric**
Salut! C'est Stéphane. Ça va.	Salut Anne! Je suis contente que tu sois sur la grande toile!

Figure G.3/H.323 – Possibilité d'affichage d'une session de texte dans une conversation non dirigée entre quatre personnes

L'affichage d'une conférence entre plus de deux personnes peut également être présenté dans une fenêtre commune avec des marquages pour chaque entrée correspondant au participant (style causerie IRC) (voir Figure G.4):

Stéphane> Salut!
Anne> Etes-vous au courant que je serai à Paris en novembre?
Eric> Salut Anne! Je suis contente que tu sois sur la grande toile!
Eve> Ah! Salut les copains! Comment vas-tu Stéphane?
Stéphane> Ça va.

Figure G.4/H.323 – Possibilité d'affichage d'une session de texte dans une conversation non dirigée entre quatre personnes

G.9.1.3 Conversation entre une et plusieurs personnes avec droit d'écriture dirigé

Une personne à la fois a le droit d'envoyer un message à plusieurs lecteurs. Le droit d'écriture peut être transmis à d'autres personnes, au cours d'une réunion dirigée.

Une application type est l'enseignement à distance où le professeur, qui a généralement le droit d'écrire, peut transmettre ce dernier à un autre participant.

G.9.1.4 Conversation entre une et plusieurs personnes avec droit d'écriture fixe

Une personne tape un message dans la session d'un point d'extrémité fixe, les autres points d'extrémité affichant le message dans une fenêtre de réception. Le droit d'écriture ne peut pas être transmis.

Ce système est utilisé en particulier pour les discours sous-titrés.

Les terminaux utilisateur peuvent être des points d'extrémité à couplage non déterministe H.332.

Voir Figure G.5.

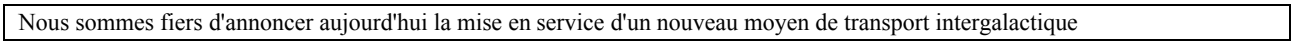


Figure G.5/H.323 – Exemple d'une session de texte dans une conversation entre une et plusieurs personnes

G.10 Text SET: type d'extrémité textophonique simple

Le présent paragraphe définit les dispositifs d'extrémité textophonique simple qui exploitent un sous-ensemble précis des protocoles H.323 et qui conviennent bien aux applications de téléphonie IP tout en conservant l'interopérabilité avec les dispositifs normalement conformes à la version 2 (1998) de la Rec. UIT-T H.323 ou les dispositifs ultérieurs. La présente spécification définit des fonctionnalités de conversation en mode texte en temps réel, spécifiées dans la Rec. UIT-T T.140, qui sont intégrées au téléphone vocal IP spécifié dans l'Annexe F, pour former un textophone IP doté d'une fonctionnalité voix et texte simultanée.

G.10.1 Introduction aux dispositifs Text SET

On définit les procédures et les protocoles relatifs aux dispositifs Text SET pour réseaux IP en apportant des modifications et des adjonctions à la spécification relative aux dispositifs Audio SET figurant dans l'Annexe F. Ce dispositif est appelé ici Text SET.

Les concepts généraux relatifs au type de point d'extrémité simple (SET) sont décrits dans l'Annexe F. On trouvera ci-dessous une série de modifications apportées à la spécification relative aux dispositifs Audio SET, qui sont nécessaires pour pouvoir ajouter la fonctionnalité de conversation en mode texte à ces dispositifs. Les numéros de paragraphes de l'annexe originale sont indiqués.

G.10.2 Aperçu général de la fonctionnalité système des dispositifs d'extrémité (audio) simple (voir § F.6)

A la rubrique **Capacités relatives aux médias**, modifier:

- capacité de transmission de données obligatoire; T.140.

G.10.3 Procédures pour dispositifs d'extrémité simple (voir § F.7)

Modifier:

- mise en paquets et transport des médias (H.225.0, RTP, TCP, T.140) – Voir § F.7.4.

G.10.4 Signalisation RAS (RAS H.225.0 – voir § F.7.1/H.323)

Comme pour le dispositif Audio SET, mais on utilise pour le dispositif Text SET un code réservé associé au type de point d'extrémité SET H.225.0.

Bit 2 = 1 indique que le dispositif possède des capacités Text SET.

Bit 2 = 0 indique que le dispositif ne possède pas de capacités Text SET.

NOTE – Les protocoles du portier doivent être définis afin qu'ils autorisent des sessions uniquement vocales avec un dispositif Text SET.

G.10.5 Signalisation d'appel (Commande d'appel H.225.0 – voir § F.7.2)

On utilise le bit 2 du code associé au dispositif d'extrémité SET H.225.0.

G.10.6 Capacité de transmission des données (voir § F.7.3.3.3)

La capacité de transmission des données T.140 doit être spécifiée.

DataApplicationCapabilitiy.application = t140.

G.10.7 Règles additionnelles pour l'utilisation des capacités (voir § F.7.3.3.9)

Les capacités audio et de transmission des données ne doivent être signalées qu'au moyen de la procédure Fast Connect et de l'échange répété de structures **OpenLogicalChannel**, comme indiqué dans l'Annexe F.

Les valeurs d'entrée dans la table **MultiplexCapability** sont censées être les mêmes que pour les dispositifs Audio SET avec les exceptions suivantes:

```
mediaDistributionCapability
     centralizedData    TRUE
     distributedData    TRUE/FALSE selon le cas, par défaut: FAUX
```

G.10.8 Messages de signalisation de voies logiques (voir § F.7.3.4)

Ajouter ce qui suit aux requêtes d'ouverture de voie logique:

```
OpenLogicalChannel.forwardLogicalChannelParameters.DataType.data = t140
MultiplexParameters     selon le cas, pour le type de voie fiable ou non
                        fiable sélectionné.
```

G.10.9 Echange relatif aux flux médias (voir § F.7.4)

Pour l'échange de texte, les terminaux SET doivent suivre les procédures spécifiées dans la présente annexe.

G.10.10 Côté émetteur (voir § F.7.6.1)

Ajouter:

la structure **OpenLogicalChannel** doit contenir le même codage des données pour le texte que celui qui était contenu dans l'appel initial.

G.10.11 Terminaux Text SET sans capacité de conférence (voir § F.7.7.1)

Ajouter les fonctionnalités suivantes:

- fusion de plusieurs sessions de texte d'entrée dans le dispositif Text SET;
- conversion des adresses de transport pour le flux de texte;
- transfert et transcodage éventuel des flux de données en mode texte.

G.10.12 Prise en charge des conférences à couplage non déterministe (Rec. UIT-T H.332) (voir § F.7.8)

Un dispositif Text SET peut participer à une conférence à couplage non déterministe au moyen des procédures H.332, à condition que la conférence soit étendue pour qu'elle contienne du texte et qu'une voie non fiable soit sélectionnée pour la transmission du texte.

Annexe J

Sécurisation des dispositifs de l'Annexe F

J.1 Introduction

La présente annexe traite de la sécurisation des types d'extrémité simples définis dans l'Annexe F. Le profil de sécurité spécifié, fondé sur H.235v2, utilise le profil de sécurité de base proposé dans l'Annexe D/H.235v2. Le profil de sécurité proposé dans l'Annexe J utilise la Rec. UIT-T H.235v2 aux fins des types d'extrémité simples et de leurs besoins de sécurité spécifiques. Ses caractéristiques ont été choisies parmi les nombreuses options proposées dans la Rec. UIT-T H.235.

Le texte proposé donne un aperçu du profil de sécurité; on trouvera dans l'Annexe D/H.235v2 toutes les précisions techniques et d'implémentation correspondantes.

Un **type d'extrémité simple sécurisé (SET sécurisé**) est essentiellement un dispositif SET, tel qu'il est défini dans l'Annexe F, qui implémente certaines caractéristiques de sécurité proposées dans la présente annexe.

Dans son état actuel, celle-ci est uniquement axée sur un "type SET sonore sécurisé (SASET)" et ne traite d'aucun autre (tel que type SET de télécopie sécurisé, terminal de texte sécurisé, dispositif vidéo sécurisé, etc., qui nécessitent des études séparées).

J.2 Conventions

Quelques explications sont nécessaires pour comprendre certains termes utilisés ci-après:

la présente annexe traite du **profil de sécurité de base** d'un dispositif SASET (**terminal sonore d'extrémité simple sécurisé**). Ce profil assure une sécurité élémentaire par des moyens simples faisant appel à des techniques cryptographiques de type à mot de passe; il conviendrait de l'implémenter dans tous les dispositifs SASET. Si nécessaire, on peut utiliser le **profil de sécurité de cryptage vocal** pour assurer la confidentialité vocale. Un complément d'étude permettra de déterminer si des profils de sécurité plus élaborés seront nécessaires.

Pour éviter de citer des marques (RC2®), cette annexe se réfère à un algorithme de décryptage "compatible RC2".

La présente annexe contient des termes relatifs à la sécurité bien connus tels que clé, gestion des clés et dispositifs SET qui ont des sens différents dans d'autres contextes (par exemple, clavier tactile, gestion des touches de fonction Q.931/Q.932 et protocole de transaction électronique sécurisée).

J.3 Domaine d'application

La présente annexe traite de la sécurité des dispositifs d'extrémité simples. Comme indiqué au § F.3, il s'agit du dispositif suivant:

- **terminal téléphonique simple sécurisé** (SAT, *secure audio simple endpoint type*) – défini dans la présente annexe (voir le § J.6).

La sécurité dans tout autre dispositif SET nécessite un complément d'étude.

J.4 Abréviations

La présente annexe utilise les abréviations suivantes:

DES	norme de chiffrement des données (*data encryption standard*)
GK	portier (*gatekeeper*)
HMAC	code d'authentification de message "d'après les signaux parasites" (*hashed message authentication code*)
MAC	code d'authentification de message (*message authentication code*)
RAS	enregistrement, admission et statut (*registration, admission and status*)
RTP	protocole en temps réel (*real time protocol*)
SASET	type audio d'extrémité simple sécurisé (*secure audio simple endpoint type*)
SET	type d'extrémité simple (*simple endpoint type*)
SHA	algorithme de hachage sûr (*secure hash algorithm*)
UIT	Union internationale des télécommunications

J.5 Références normatives

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

– Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

– Recommandation UIT-T H.235 (2000), *Sécurité et cryptage des terminaux multimédias de la série H (terminaux H.323 et autres terminaux de type H.245)*.

– Recommandation UIT-T H.245 (2006), *Protocole de commande pour communications multimédias*.

– IETF RFC 2268 (1998), *A Description of the RC2® Encryption Algorithm*.

J.6 Type audio d'extrémité simple sécurisé (SASET)

La présente annexe contient la description de base d'un **type audio d'extrémité simple sécurisé (SASET, *secure audio simple endpoint type*)**. Un tel dispositif est, par exemple, un téléphone simple sécurisé.

J.6.1 Hypothèses

Le profil de sécurité de base utilise le modèle d'acheminement par portier pour les dispositifs SET de l'Annexe F sécurisés. On part du principe que les dispositifs SASET et autres entités H.323 qui implémentent ce profil de sécurité (par exemple les portiers) appliquent la procédure de connexion rapide.

En vertu de l'Annexe F, le profil de sécurité de base utilise la procédure de connexion rapide avec les éléments de gestion à clé intégrée mais ne prend pas en charge la tunnellisation H.245. Donc, le profil de base ne donne pas de moyens de mise à jour et de synchronisation de la clé par

message H.245 (canalisé). Les dispositifs SASET qui implémentent le profil de sécurité de base seulement mais qui nécessitent encore un mécanisme de mise à jour de la clé doivent raccrocher et se reconnecter pour obtenir une nouvelle clé de session.

J.6.2 Aperçu général

La sécurité de base est applicable dans les environnements administrés où des clés/mots de passe symétriques sont attribués aux entités (dispositif SASET à portier, portier à portier).

Le Tableau J.1 résume toutes les procédures définies dans l'Annexe D/H.235v2.

Tableau J.1/H.323 – Dispositifs audio d'extrémité simples sécurisés (voir Annexe D/H.235v2) – Résumé

<table>
<tr><th rowspan="2">Services de sécurité</th><th colspan="6">Fonctions d'appel</th></tr>
<tr><th>RAS</th><th colspan="2">H.225.0</th><th>H.245 (Note)</th><th colspan="3">RTP</th></tr>
<tr><td>Authentification</td><td>*Mot de passe HMAC-SHA1-96</td><td colspan="2">*Mot de passe MAC-SHA1-96</td><td>*Mot de passe HMAC-SHA1-96</td><td colspan="3"></td></tr>
<tr><td>Non-répudiation</td><td></td><td colspan="2"></td><td></td><td colspan="3"></td></tr>
<tr><td>Intégrité</td><td>*Mot de passe HMAC-SHA1-96</td><td colspan="2">*Mot de passe HMAC-SHA1-96</td><td>*Mot de passe HMAC-SHA1-96</td><td colspan="3"></td></tr>
<tr><td>Confidentialité</td><td></td><td colspan="2"></td><td></td><td>♦DES à 56 bits</td><td>♦Norme à 56 bits compa-tible RC2</td><td>♦DES triple à 168 bits</td></tr>
<tr><td>Commande d'accès</td><td></td><td colspan="2"></td><td></td><td colspan="3"></td></tr>
<tr><td>Gestion de clés</td><td>*Attribution de mot de passe à la souscription</td><td>*Attribution de mot de passe à la souscription</td><td>♦Echange de clés Diffie-Hellman authen-tifiées</td><td>♦Gestion de clés intégrée dans session H.235 (distribution de clés, mise à jour de clés par DES à 56 bits/norme à 56 bits compatible RC2/DES triple à 168 bits)</td><td colspan="3"></td></tr>
<tr><td colspan="7">* Zone bleue: système de type à mot de passe.
♦ Zone verte: profil de sécurité de cryptage vocal.
NOTE – Protocole H.245 imbriqué dans la procédure de connexion d'appel rapide H.225.0.</td></tr>
</table>

Pour l'authentification et l'intégrité, l'utilisateur doit faire appel au système de type à mot de passe (zone bleue du Tableau J.1). Celui-ci est très recommandé pour l'authentification en raison de sa simplicité et de sa facilité d'application. Le hachage des champs dans les messages H.225.0 est une méthode recommandée pour l'intégrité des messages (utilisant aussi le système de mot de passe). Les dispositifs SASET effectuent l'authentification en combinaison avec l'intégrité au moyen du même mécanisme de sécurité commun.

Lorsqu'un dispositif SASET recourt au profil de sécurité de cryptage vocal (zone verte du Tableau J.1), il doit implémenter la norme DES à 56 bits comme algorithme de cryptage par défaut; il peut aussi implémenter la norme DES triple à 168 bits, alors que les dispositifs SASET utilisant le cryptage exportable peuvent implémenter une norme à 56 bits compatible RC2.

En ce qui concerne la confidentialité vocale, le système proposé est le cryptage au moyen d'une norme compatible RC2, DES ou triple DES fondée sur le modèle commercial et le besoin d'exportabilité. Quelques environnements qui offrent déjà un certain degré de confidentialité n'ont pas nécessairement besoin de cryptage vocal. Dans ce cas, l'échange de clés Diffie-Hellman et d'autres procédures de gestion des clés sont également superflues.

Les moyens de commande d'accès ne sont pas décrits de manière explicite; ils peuvent être implémentés localement au moyen des informations reçues dans les champs de signalisation H.235 (ClearToken, CryptoToken).

La présente Recommandation ne décrit pas les procédures s'appliquant à l'attribution de mot de passe/clé secrète à la souscription par la gestion et l'administration. De telles procédures peuvent être effectuées par des moyens qui ne font pas partie de la présente annexe.

Les dispositifs SASET peuvent utiliser des services secondaires conformément à la procédure décrite au § I.4.6/H.235v2.

Annexe K

Voie de transport par protocole HTTP des signaux de commande de services dans les réseaux H.323

K.1 Introduction

La présente annexe décrit un moyen facultatif de commander des services complémentaires dans un environnement H.323. L'ouverture d'une connexion HTTP distincte pour le transport d'un protocole de commande indépendant du service permet d'élaborer et de déployer de nouveaux services sans mettre à jour les extrémités H.323.

Cette voie de commande de services est destinée à être utilisée pour une large gamme de services, dont certains nécessitent l'application de la signalisation par protocole H.450 ou par serveur tampon (par exemple, comme indiqué dans l'Appendice III pour leur invocation/exécution. Comme cette voie est indépendante des services, aucun service particulier n'est défini ou préconisé. Les données transmises sur cette voie sont censées être informatives (à l'interface avec l'usager). Elles doivent normalement être suivies d'actions appropriées (p. ex. invocations H.450) dans le plan de signalisation d'appel, le cas échéant. Bien que certaines applications côté serveur doivent prendre en charge les services H.450 pour l'interfonctionnement, cette Annexe est totalement indépendante des Recommandations UIT-T de la série H.450.x.

La voie de commande de services peut être utilisée aussi bien pour les services associés à l'appel que pour les services non associés à l'appel. Elle peut être ouverte entre le terminal et le réseau ou entre deux extrémités (d'une communication, ou ouverte avec une connexion indépendante de l'appel).

Bien que plusieurs protocoles puissent être utilisés, la présente annexe décrit l'utilisation du protocole de transfert en hypertexte (HTTP, *hypertext transfer protocol*) pour le transport. Ce protocole est ouvert, flexible, compatible avec les barrières de sécurité et bien connu. Tout dispositif revendiquant la prise en charge de la présente Annexe K doit prendre en charge le protocole HTTP comme moyen de transport des signaux de commande de services, ainsi que, facultativement, le protocole S-HTTP pour les applications nécessitant des mesures de sécurité. Le protocole d'application de service proprement dit est dynamique et est indiqué par des types d'extension MIME dans la signalisation HTTP. Exemples d'application possibles: pages en langage XML comportant éventuellement du langage Java™ et des scripts, téléimportation de

tonalités et d'annonces à restituer au client, téléexportation par un client de logiques de traitement d'appel vers un portier, etc. Bien que la présente annexe soit orientée vers les services complémentaires commandés par l'usager, cette voie de commande de services peut également servir d'autres fins. Elle pourrait par exemple être utilisée pour des mises à jour de logiciels ou pour proposer des offres commerciales à des clients.

Le paragraphe K.2 décrit l'utilisation du protocole H.323 pour fournir la localisation URL de la connexion HTTP entre le fournisseur de services et le client. Le paragraphe K.3 montre l'emploi du protocole HTTP et le § K.4 montre quelques exemples de services possibles, avec la signalisation correspondante.

L'interface entre le plan de commande de services et le plan de commande d'appel chez le client ou le fournisseur de services est hors du domaine d'application de la présente annexe mais elle peut inclure des balises HTML ou XML comme "mailto" ou des URL de l'environnement H.323. Voir Figure K.1.

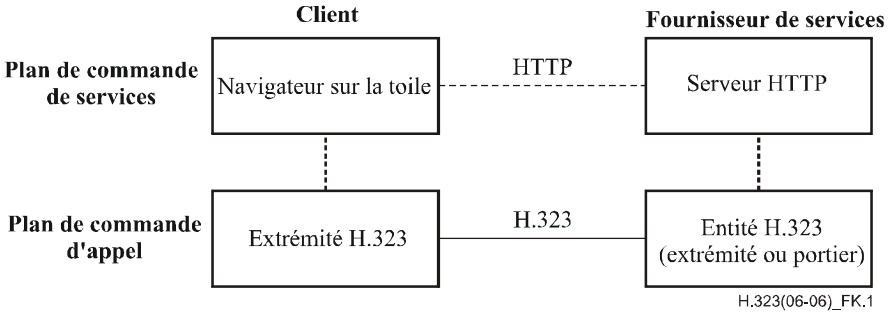


Figure K.1/H.323 – Aperçu général du système pour commande de services en mode HTTP

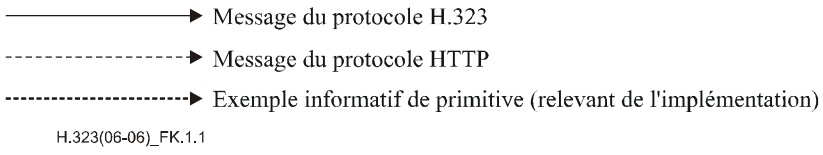
Il appartient généralement au fournisseur de la localisation URL de définir et d'implémenter les fonctions et services de commande qui sont en cours de présentation par l'URL considérée (prise en charge possible de services normalisés ou non normalisés). Si la commande de service entre en interaction avec le traitement d'appel H.323, le fournisseur de cette URL doit normalement établir le lien entre le service HTTP et les services H.323/H.450 qui vont être pris en charge par le portier ou par l'extrémité.

Etant donné que la voie de commande de services HTTP est indépendante des pays et non informée des services offerts, elle ne peut pas tenir compte des interactions entre services. Une application utilisant cette voie de commande de services devrait cependant examiner de près cette question.

Les éventuelles listes séquentielles ou références à la signalisation H.323 dans la présente annexe sont des exemples donnés pour information pour décrire de possibles interactions avec la commande de service et la commande d'appel. Ces informations ne remettent pas en cause les règles de signalisation H.323 car elles sont pour la plupart grandement simplifiées pour plus de concision.

K.1.1 Notation

La notation suivante est utilisée:



Les messages HTTP et RAS sont écrits en lettres majuscules (protocole HTTP:GET, signalisation RAS:ARQ) alors que les messages de signalisation d'appel H.225.0 sont écrits avec la première lettre en majuscule (Setup). Les séquences codées en notation ASN.1 du protocole H.225.0 sont écrites en caractères gras (**ServiceControlAddress**).

K.2 Commande de services dans les réseaux H.323

Le présent paragraphe décrit la façon dont les messages H.323 sont utilisés pour maintenir les sessions de commande de service.

K.2.1 Session de commande de services

Une session de commande de service est une relation dans un seul sens entre l'entité cliente et le fournisseur de services: en l'occurrence, il s'agit d'une session HTTP établie par l'entité cliente après la réception d'une localisation URL **ServiceControlAddress** dans des messages H.225.0. Cette localisation URL peut être reçue au moyen de deux voies de signalisation H.323 différentes:

- une structure **ServiceControlSession** contenant une localisation URL est reçue dans un message par la voie de signalisation RAS. S'il n'y a pas de message approprié à envoyer, le message **ServiceControlIndication** (SCI) peut être envoyé à l'extrémité à tout moment;
- une structure **ServiceControlSession** contenant une localisation URL est reçue dans un message par la voie de signalisation d'appel H.225.0.

La session de commande de service est désignée par un identificateur **sessionID**, qui est un nombre unique pour la voie de signalisation. Les identificateurs de session reçus par signalisation RAS et par signalisation d'appel peuvent se superposer car leurs expéditeurs peuvent ne pas être informés l'un de l'autre.

Un fournisseur de services souhaitant ouvrir une nouvelle session de commande de service envoie à cette fin au client une structure **ServiceControlSession** contenant un nouvel identificateur de session **sessionId**, la localisation URL du service et le champ de cause mis à la valeur "**open**". Le client peut ouvrir une connexion vers cette adresse et demander la ressource à partir de la localisation URL mais aucun acquittement n'est émis par le client dans le plan de signalisation d'appel. Si l'usager souhaite fermer la session à un moment donné, p. ex. en fermant une fenêtre incrustée pour la session, cette fermeture est effectuée sans aucune notification vers le fournisseur.

Si un fournisseur de services a besoin d'informer une extrémité au sujet de nouveaux services ou événements relatifs à une session déjà ouverte, il peut le faire en envoyant une nouvelle structure **ServiceControlSession** sur la voie RAS ou sur la voie de signalisation d'appel (comme cela avait été le cas dans la séquence d'ouverture). La structure doit contenir le même identificateur de session **sessionId** que précédemment (afin de réutiliser la même ressource, par exemple, une fenêtre d'écran), une nouvelle localisation URL à charger et la cause mise à la valeur "**refresh**".

Si le fournisseur de services souhaite clore la session, il peut envoyer une structure **ServiceControlSession** contenant le même identificateur de session **sessionId** et le champ de cause mis à la valeur "**close**". L'entité cliente doit normalement, si sa session est encore ouverte, fermer toutes les ressources comme les fenêtres associées à la session.

La cause de la prise en charge de sessions multiples est que des nœuds fournisseurs de services non associés peuvent utiliser les mêmes mécanismes de notification, p. ex. la voie de signalisation d'appel. Les applications de services conformes à la présente annexe doivent normalement veiller à ne pas surexploiter le nombre de sessions car de nombreuses notifications perturberaient rapidement l'usager. Les clients prenant en charge la présente annexe ne sont pas tenus d'ouvrir plus de deux sessions, l'une associée à l'appel et l'autre non associée à l'appel.

K.2.2 Commande de services non associée à l'appel

Afin de fournir des services associés à la session d'enregistrement et non à un appel donné, le portier peut renvoyer une structure **ServiceControlSession** contenant une localisation URL dans le message RCF. La localisation URL renvoyée doit normalement être complète en termes de définition du protocole, du serveur et de la ressource, c'est-à-dire <protocol>://<adresse du serveur>/<ressource>. L'extrémité peut charger cette URL puis afficher les services et les fonctions de commande de service fournis par les données indiquées par cette URL (par exemple, une page internet avec menus et liens).

Si le réseau a besoin de signaler à l'extrémité des événements relatifs au service, au cours d'une communication ou dans le cadre d'un enregistrement, ce réseau peut envoyer à cette extrémité une indication de commande de service (SCI, *service control indication*) avec une localisation URL. Pour indiquer que celle-ci se rapporte à une session de commande de service déjà active et non associée à la communication, l'identificateur de session (**sessionId**) doit être le même que précédemment et le champ **callSpecific** ne doit pas être présent. L'extrémité pourra ensuite charger cette URL et recevoir une mise à jour des services et des fonctions de commande de service. Une extrémité qui reçoit une telle indication SCI doit y répondre par un message de réponse de commande de service (SCR) afin d'éviter la réémission de l'indication SCI par le fournisseur. Le message SCR n'est qu'un accusé de réception du message SCI et non nécessairement une réponse au niveau de l'application.

Le message d'indication de commande de service peut aussi servir à ouvrir une nouvelle session ou à fermer la session existante.

Si une entité autre que le portier local souhaite ouvrir une session de commande de service non associée à l'appel vers une extrémité, elle peut le faire en ouvrant une connexion de signalisation indépendante de l'appel vers l'extrémité, et en envoyant un message Setup avec une structure **ServiceControlSession** contenant une URL. Le paramètre **conferenceGoal** doit être mis à **callIndependentSupplementaryService** et l'élément d'information de la capacité support du message Setup doit être mis comme défini pour la connexion indépendante de l'appel, au § 7.2.2.1.2/H.225.0. Sinon, les mêmes procédures que celles indiquées au § K.2.2 s'appliquent, le champ **ServiceControlSession** étant acheminé dans les messages de signalisation d'appel et les médias étant absents de la connexion.

K.2.3 Commande de service associée à l'appel

Deux méthodes sont offertes pour ouvrir une session de commande de service associée à un appel particulier:

1) une session de commande de service est ouverte entre une extrémité et son portier au moyen d'une localisation URL transportée dans un message RAS associé à l'appel, en particulier pour les portiers utilisant la signalisation d'appel d'extrémité. Si le message SCI est utilisé, le champ **callSpecific** de ce message doit contenir les champs **callIdentifier**, **conferenceId** et **answerCall** qui ont été utilisés dans la signalisation préalable de l'appel considéré. Un nouvel identificateur de session (**sessionId**) doit être utilisé. Cette session ne doit normalement pas avoir d'incidence sur la session de commande de service non associée à l'appel, comme au § K.2.2;

2) des sessions de commande de service sont ouvertes entre une extrémité et un portier, ou entre deux extrémités avec un champ **ServiceControlSession** contenant une localisation URL dans les messages de signalisation d'appel.

Si un fournisseur de services souhaite donner à une extrémité notification de nouveaux services ou événements d'une session existante, il peut à cette fin rafraîchir les données relatives à une URL déjà chargée (par exemple, dialogues d'appelette/servelette). Il peut également émettre un message H.225.0 (Facility ou SCI) avec une nouvelle URL, le champ de cause étant mis à la valeur "**refresh**" et le champ **sessionId** à la même valeur que préalablement à la session. Une extrémité qui

reçoit un tel message Facility doit charger cette URL et renvoyer les données qui lui sont présentées à la ressource déjà utilisée pour cette session (par exemple, fenêtre d'écran).

Si une entité fournissant un service souhaite ouvrir une nouvelle session une fois l'appel connecté, cette entité peut également utiliser le message Facility/SCI avec un champ **ServiceControlSession** contenant un nouvel identificateur de session (**sessionId**), l'URL chargée et le champ de cause mis à la valeur "**open**". Les messages H.225.0 ne contenant pas le champ **ServiceControlSession** n'ont pas d'influence sur la session HTTP, sauf sur le message Release Complete qui, sans URL, indique que toutes les sessions de cet appel sont terminées. Cette signalisation doit normalement être perçue comme étant distincte pour toutes les sessions ouvertes (non associées à l'appel ou associées à l'appel avec messages de signalisation SCI et en cours de communication).

Il y a lieu que les portiers utilisant la commande de service HTTP veillent à ne pas entrer en interaction avec la commande de service de bout en bout. Ce problème se pose en particulier pour les appels non routés par portier, celui-ci n'étant pas informé des messages et états de commande d'appel. Pour résoudre ce problème, il est recommandé que les extrémités utilisent des fenêtres de navigation distinctes selon les différentes sessions de commande de service. Les dispositifs intermédiaires comme les portiers ou les ponts MCU utilisant la présente annexe doivent toujours être informés de la possibilité de conflit avec d'autres entités fournissant des services sur le trajet de signalisation de l'appel. Les messages (signalisation d'appel ou autre, par exemple une LCF avec données de commande de service pouvant être envoyées au client sur une ACF) peuvent arriver au client avec un champ **ServiceControlSession** utilisant l'identificateur de session **sessionId** déjà utilisé entre le fournisseur intermédiaire et le client du service. Si le dispositif intermédiaire décide de transmettre le champ **ServiceControlSession**, il doit avoir la capacité d'associer l'identificateur de session **(sessionId)** à un nombre unique pour le client. Une autre possibilité consiste à multiplexer ces deux sessions dans le même protocole de couche Présentation.

Pour fournir des services associés à l'appel entre des zones ou des domaines différents, une entité de terminaison peut retourner une structure **ServiceControlSession** contenant une URL dans d'autres messages que sur le canal de signalisation d'appel (par exemple, LCF/LRJ). Il appartient au portier local d'envoyer le champ **ServiceControlSession** reçu dans les messages correspondants (par exemple ACF/ARJ) vers le client. Les applications pour lesquelles il est nécessaire de disposer d'informations détaillées sur l'état de l'appel ou d'avoir la possibilité d'exécuter des actions dans le plan commande d'appel ou de mettre à jour la session ultérieurement, ne doivent pas utiliser ce mécanisme, mais plutôt le canal de signalisation d'appel pour acheminer la structure **ServiceControlSession**.

K.3 Utilisation du protocole HTTP

K.3.1 Voie de commande de services non associée à l'appel

Le protocole HTTP est défini dans le commentaire RFC 2068. Le présent paragraphe donne des indications informatives sur la façon dont le protocole HTTP peut être employé afin d'assurer la commande de service décrite.

Pour les services non associés à l'appel, l'extrémité reçoit une localisation URL qu'il peut extraire par la méthode GET normale. Les données sont recueillies et restituées selon les procédures normales d'un agent usager du protocole HTTP[2]. L'exemple ci-dessous (Figure K.2) illustre le flux:

[2] Le terme "agent usager du protocole HTTP", utilisé dans la présente annexe, se rapporte à un processus implémentant le sous-système client du protocole HTTP (normalement représenté par un navigateur Internet).

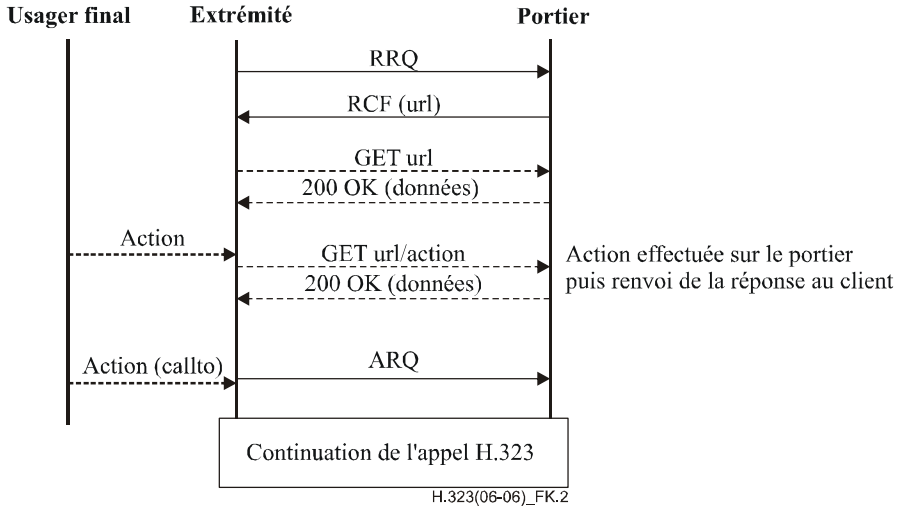


Figure K.2/H.323 – Exemple de commande de service non associée à l'appel

K.3.2 Voie de commande de services associée à l'appel

Afin de prendre en charge la commande de services associée à l'appel, une localisation URL est transportée dans différents messages H.225.0 comme indiqué au § K.2.3. Une extrémité prenant en charge la présente annexe doit normalement, à la réception d'une telle demande d'URL, demander à un agent usager HTTP normal d'ouvrir et d'afficher cette URL.

Il y a lieu que l'agent usager HTTP affiche l'URL indiquée et prenne en charge les feuilles de style, les scripts, les liens et les images comme défini dans le commentaire RFC 2068 pour le protocole HTTP. Les actions définies et exécutées par le contenu de cette URL peuvent être exécutées localement (par exemple, les liens de messagerie) ou à distance sur un quelconque serveur HTTP lié, par exemple, implémentées ou associées à une extrémité ou à un portier. On trouvera ci-dessous un exemple où l'extrémité est le fournisseur de services (voir Figure K.3). L'exemple 2 du § K.4 montre un portier dans le rôle de fournisseur de services.

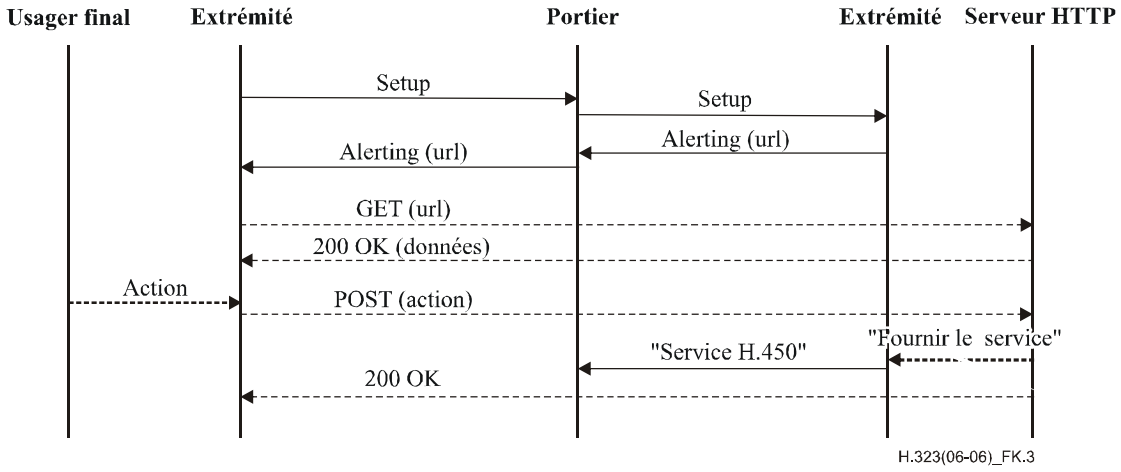


Figure K.3/H.323 – Exemple de commande de services associée à l'appel utilisant une localisation URL dans les messages de signalisation d'appel H.225.0

1) Le client envoie un message Setup qui est routé par le portier vers l'extrémité représentant l'appelé.

2) L'appelé peut être dans un état où un traitement d'appel spécifique est programmé, par exemple:

   – décision de rejeter l'appel par l'envoi d'un message Release Complete qui peut contenir une localisation URL à afficher par l'agent usager HTTP de l'appelant. L'URL peut être, par exemple, une référence à la page d'accueil de l'appelé;

   – une décision de renvoi d'une liste de toutes les options d'établissement d'appel. Dans ce cas, l'appelé renvoie le message Alerting avec une URL qui définit les options offertes à l'appelant, comme le renvoi d'appel vers l'opérateur, vers un secrétariat, vers une boîte vocale, une boîte postale ou l'intrusion dans une session de communication ouverte.

3) L'extrémité H.323 appelante demande à un agent usager HTTP d'ouvrir l'URL et les données sont alors restituées à l'interface de l'appelant avec le réseau Internet. L'usager final peut alors fermer la fenêtre du navigateur ou interagir avec elle en sélectionnant un lien ou une action.

4) Les actions définies et exécutées par le contenu de cette URL peuvent être exécutées localement (par exemple, les liens de messagerie) ou à distance sur un quelconque serveur HTTP lié, par exemple, implémentées ou associées à l'extrémité ou au portier. L'extrémité distante ou le portier doit analyser l'action indiquée et l'effectuer au moyen de services H.323/H.450 normaux. Le résultat peut consister, par exemple, à renvoyer l'appel vers un serveur de boîte vocale.

K.4 Exemples de scénario

Une série d'exemples est donnée afin d'illustrer l'utilisation de la commande d'ouverture de services. Il s'agit des suivants:

– exemple simple d'utilisation de la commande de services non associée à l'appel;

– exemple de commande de services associée à l'appel pour appels routés par portier;

– exemple de commande de services associée à l'appel pour appels non routés par portier;

– exemple de commande de services non associée à l'appel pour téléexportation de scripts.

Tous les exemples donnés ici n'utilisent qu'une seule voie de commande simultanée de services. Par concision, les messages contenant une structure **ServiceControlSession** ne sont indiqués que par le terme "url".

Exemple 1: commande de service non associée à l'appel

Cet exemple décrit les signaux de commande lorsqu'un usager s'enregistre auprès d'un portier, reçoit en retour une localisation URL faisant référence à un annuaire téléphonique, met à jour cet annuaire en introduisant un contact (pseudonyme) d'ami puis utilise cet annuaire mis à jour pour établir une communication (sans qu'il s'agisse nécessairement des mêmes amis) en sélectionnant une entrée contenant une localisation URL de type H.323. Voir Figure K.4.

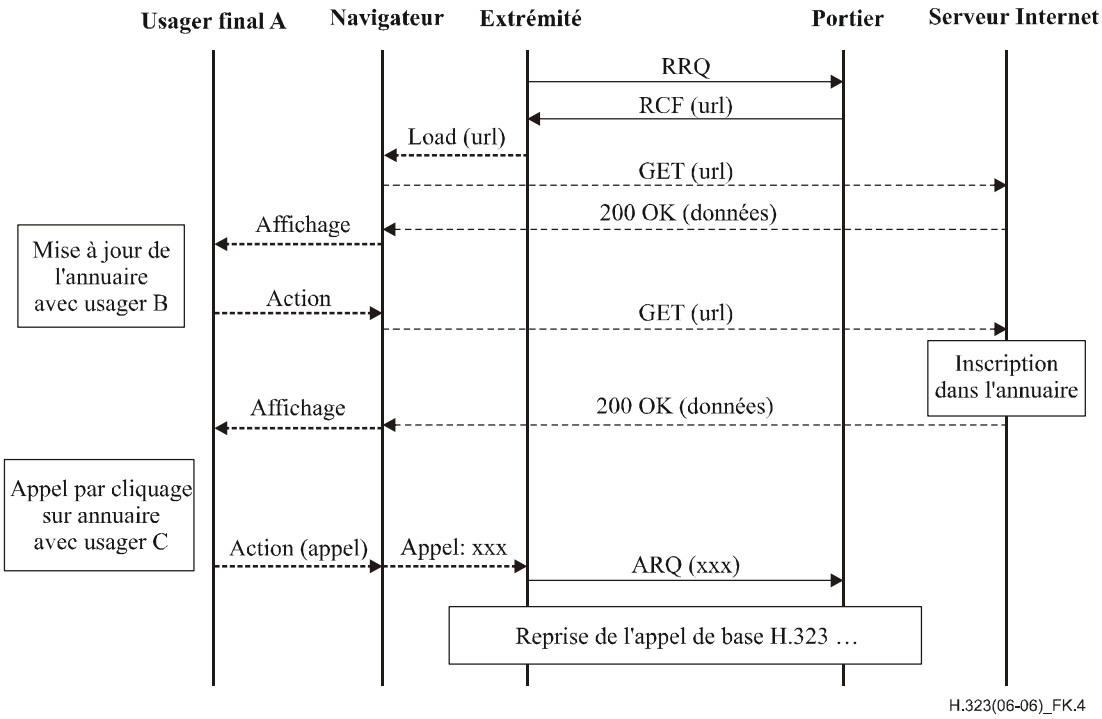


Figure K.4/H.323 – Commande de service non associée à l'appel

Exemple 2: commande de service associée à l'appel, routé par portier

Cet exemple décrit une variante du "service de signal d'appel" avec options pour l'appelant. Le portier détecte que l'appelé est occupé et fournit une localisation URL à l'appelant dans un message Alerting (pour éviter une fin de temporisation à l'extrémité appelante). Cette URL renvoie à une page Internet contenant un ensemble d'options pour la suite du traitement de l'appel.

L'usager entend la sonnerie audio et voit une page Internet avec des options. Celles-ci peuvent être: renvoi vers boîte vocale, messagerie électronique ou opérateur. L'usager sélectionne la boîte vocale et ce choix est signalé au serveur HTTP, qui en informe le portier.

Celui-ci donne suite à la demande de renvoi comme renvoi d'appel sur non réponse (puisque l'alerte avait été donnée) et informe le serveur HTTP que l'opération a été correctement exécutée. Le serveur HTTP envoie alors au navigateur une réponse sous forme de nouvelle page Internet précisant par exemple que le renvoi a été correctement effectué et présentant quelques nouvelles options. Voir Figure K.5.

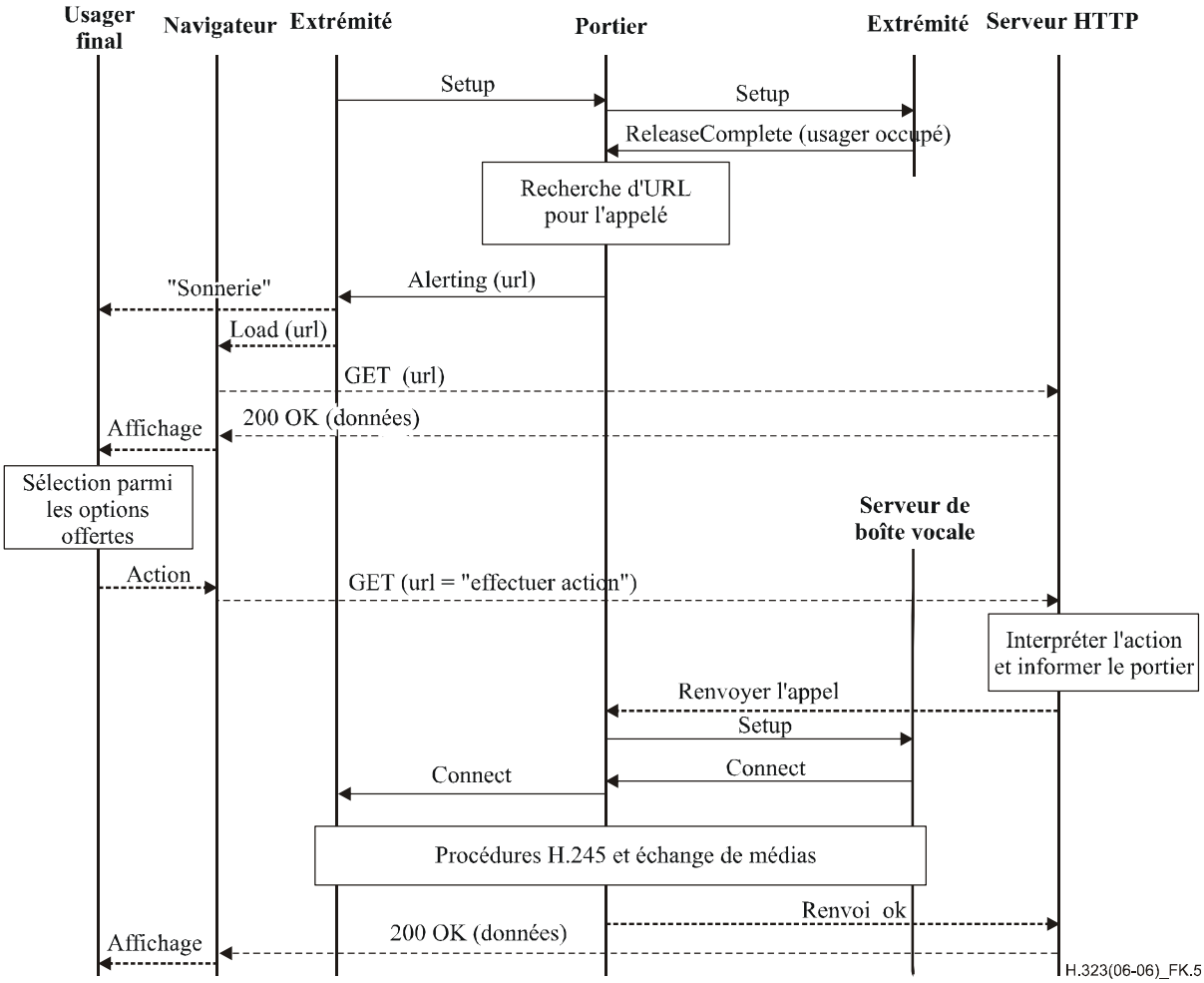


Figure K.5/H.323 – Commande de service associée à l'appel, routé par portier

Exemple 3: commande de service associée à l'appel, non routé par le portier

Cet exemple décrit le même service que dans l'exemple 2, exécuté à l'extrémité appelée. Celle-ci est occupée par une communication et renvoie à l'appelant une localisation URL dans un message Alerting (pour éviter une fin de temporisation à l'extrémité appelante). Cette URL fait référence à une page Internet contenant une série d'options pour la suite du traitement de l'appel.

L'usager entend la sonnerie audio et voit une page Internet avec des options. Celles-ci peuvent être: renvoi vers boîte vocale, messagerie électronique ou opérateur. L'usager sélectionne la boîte vocale et ce choix est signalé au serveur HTTP, qui en informe l'extrémité.

Celle-ci donne suite à la demande de renvoi comme renvoi d'appel sur non-réponse (le message Alerting ayant été envoyé) et informe le serveur HTTP que l'opération a été correctement exécutée. Le serveur HTTP envoie alors au navigateur une réponse sous forme de nouvelle page Internet précisant par exemple que le renvoi a été correctement effectué et présentant quelques nouvelles options. Voir Figure K.6.

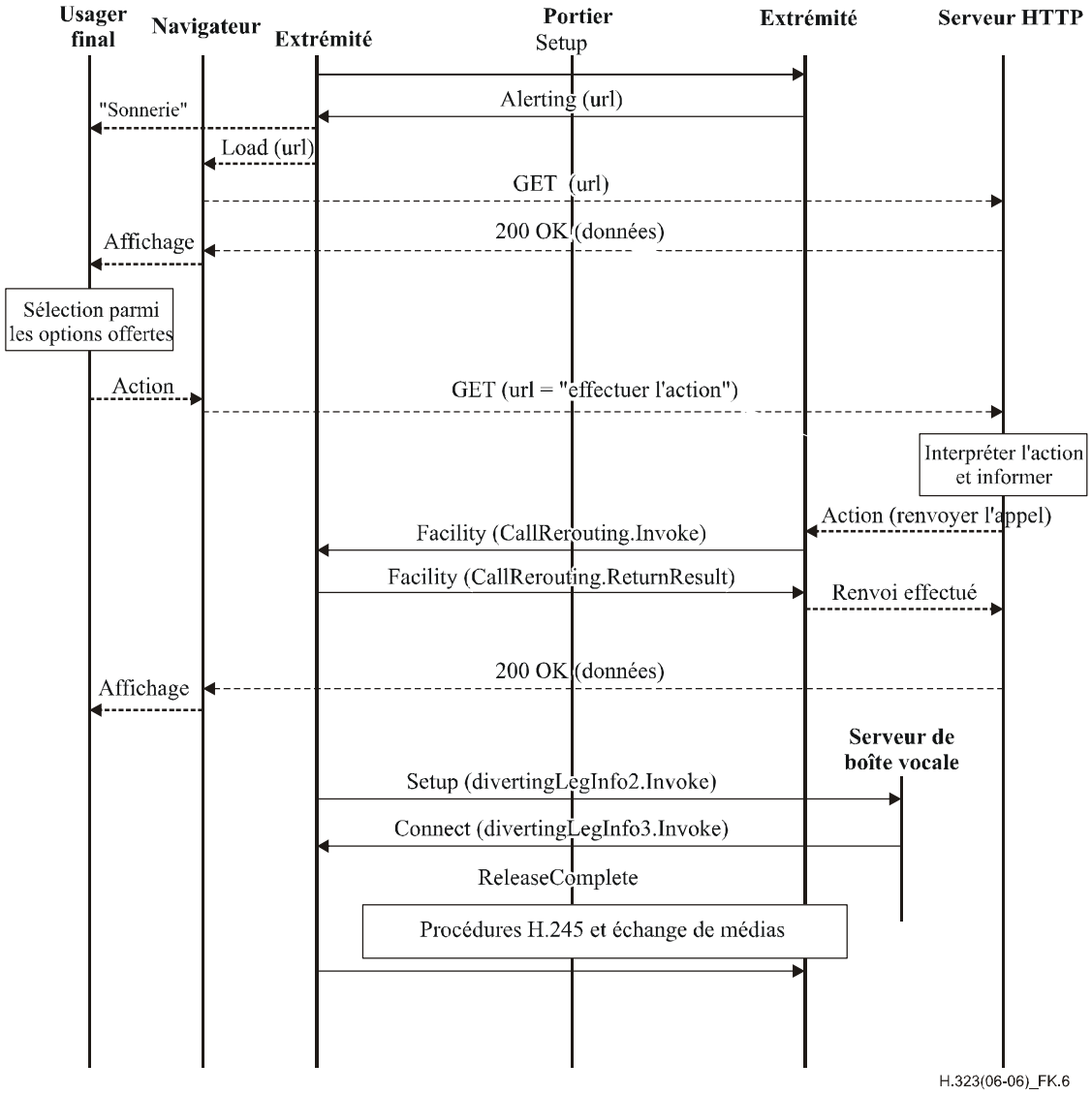


Figure K.6/H.323 – Commande de service associée à l'appel, non routé par le portier

Exemple 4: commande de service non associée à l'appel, téléexportation de script

Les scripts de traitement d'appel sont également une forme de commande de services. Cet exemple montre la téléexportation, par un terminal, d'une script après enregistrement. L'usager prépare le script au moyen d'un développeur graphique situé dans l'extrémité ou par un autre moyen. Puis il décide d'effectuer la téléexportation de ce script vers le serveur.

Dans ce cas l'extrémité sait, au moment où l'usager décide de téléexporter le script, que cet usager doit utiliser le message POST. Les détails du script et les incidences sur la suite de la signalisation d'appel dépendent du script. Voir Figure K.7.

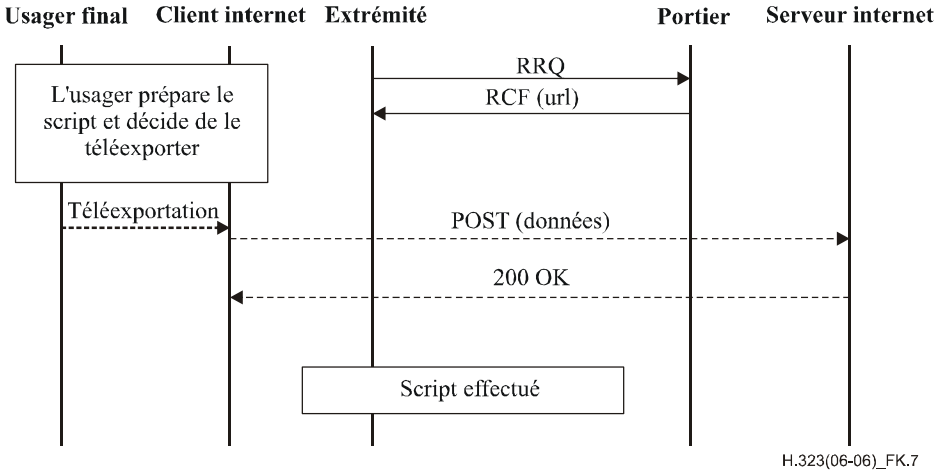


Figure K.7/H.323 – Commande de service non associée à l'appel, téléexportation de script

K.5 Références

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

K.5.1 Références normatives

[H2250] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

[URL] BERNERS-LEE (T.) *et al.*: Uniform Resource Locators (URL), *RFC 1738, Internet Engineering Task Force*, décembre 1994.

[HTTP] FIELDING (R.) *et al.*: Hypertext Transfer Protocol – HTTP/1.1, *RFC 2068, Internet Engineering Task Force*, janvier 1997.

K.5.2 Références informatives

[S-HTTP] RESCORLA (E.) *et al.*: The Secure HyperText Transfer Protocol, *RFC 2660, Internet Engineering Task Force*, août 1999.

[HTML] BERNERS-LEE (T.): Hypertext Markup Language – 2.0, *RFC 1866, Internet Engineering Task Force*, novembre 1995.

[MIME] FREED (N.), BORENSTEIN (N.): Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, *RFC 2045, Innosoft, First Virtual*, novembre 1996.

Annexe L

Protocole de commande de stimulus

L.1 Domaine d'application

La présente annexe décrit les procédures de signalisation de stimulus entre les terminaux H.323 et une unité fonctionnelle de serveur à fonctions spéciales. Cette méthode par stimulus permet au fournisseur de services réseau d'implémenter de nouveaux services complémentaires pour les terminaux sans que des modifications soient apportées au logiciel du terminal, ce qui facilite la maintenance. Un téléphone à fonctions spéciales relié à un réseau LAN est un exemple de ce type de terminal. Un serveur à fonctions spéciales peut être situé au même emplacement que le portier.

Le protocole de stimulus H.323 permet à un ou à plusieurs serveurs à fonctions spéciales de fournir des services. S'agissant de l'interopérabilité, on utilise la signalisation H.225.0 normalisée pour la commande de l'appel de base et toutes les manipulations des flux médias se font en appliquant les procédures H.245 normalisées ou les procédures de connexion rapide. Par ailleurs, on utilise les mécanismes fondés sur la Rec. UIT-T H.248.1 pour manipuler les terminaisons physiques: haut-parleur ou combiné, par exemple.

Le protocole décrit dans la présente annexe peut prendre en charge à la fois le modèle de signalisation direct et le modèle acheminé par le portier.

Les configurations types qu'illustrent les Figures L.1 et L.2 représentent les entités de signalisation fonctionnelle pouvant intervenir dans un appel depuis un terminal à stimulus H.323 vers un autre point d'extrémité dans une zone H.323 différente. La Figure L.1 montre que le serveur à fonctions spéciales joue le rôle d'un serveur mandataire de signalisation pour le terminal de l'Annexe L. La Figure L.2 montre que le serveur à fonctions spéciales est situé au même emplacement que le portier du terminal de l'Annexe L. Dans les deux cas, le serveur à fonctions spéciales a accès à la signalisation H.323; il peut ainsi disposer d'informations sur l'état de l'appel qui peuvent lui être utiles pour tel ou tel service et aussi agir sur les flux médias en recourant à la Rec. UIT-T H.245 ou à la signalisation de connexion rapide.

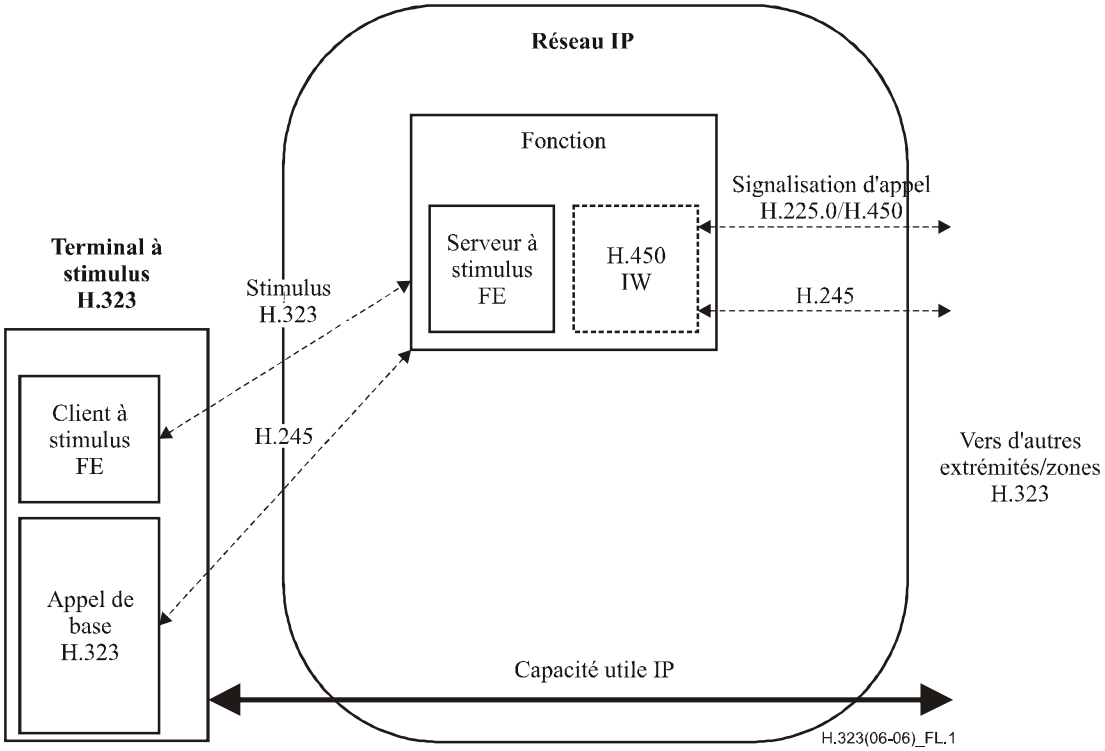


Figure L.1/H.323 – Exemple de configuration conforme à l'Annexe L conjointement avec le modèle de signalisation direct

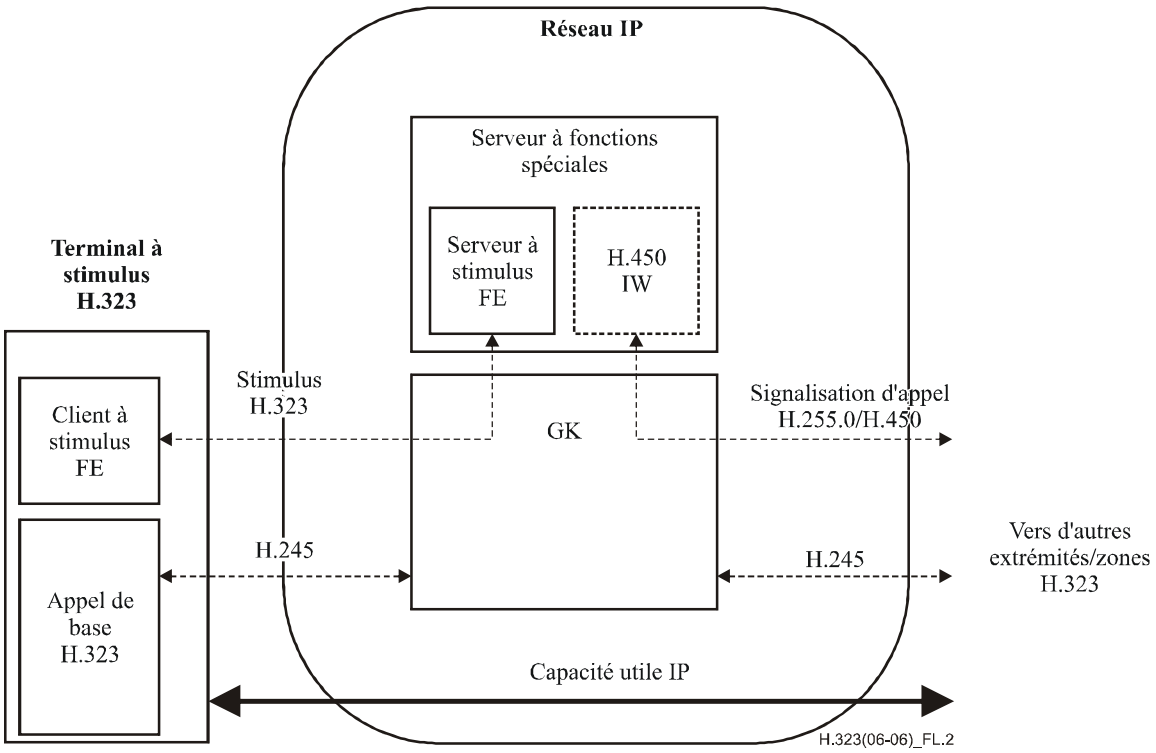


Figure L.2/H.323 – Exemple de configuration conforme à l'Annexe L conjointement avec le modèle de signalisation acheminé par le portier

L.1.1 Terminologie

L.1.1.1 serveur à fonctions spéciales: entité fonctionnelle utilisant la méthode d'encapsulation décrite dans la présente annexe pour fournir des fonctions à une extrémité selon l'Annexe L. Un serveur à fonctions spéciales peut être placé à un endroit quelconque du réseau. Il peut se trouver au même endroit qu'un portier ou se situer sur une passerelle ou une autre entité appelable H.323. Un serveur à fonctions spéciales peut assurer un interfonctionnement entre le protocole de stimulus et des services H.450.

L.1.1.2 extrémité conforme à l'Annexe L: entité appelable H.323 pouvant être commandée au moyen de la méthode décrite dans la présente annexe.

L.1.1.3 fonction: transaction pouvant agir sur l'interface utilisateur et modifier des flux médias.

L.1.2 Relation entre les stimulus H.323 et la Rec. UIT-T H.248

La Rec. UIT-T H.248 a été établie dans le but de contrôler les passerelles médias. Cela sous-entend une relation étroite entre le contrôleur et la passerelle média. Des extrémités telles que des téléphones ou des passerelles résidentielles peuvent être des dispositifs contrôlés, considérés comme des passerelles médias de ligne unique. Toutefois, elles sont reliées à exactement un contrôleur qui fournit la totalité des commandes de connexion, des fonctions et des services aux extrémités H.248. Un utilisateur peut s'abonner à des fonctions à partir d'un contrôleur à la fois.

La présente annexe utilise le modèle du contrôleur/de l'extrémité de la Rec. UIT-T H.248 pour le contrôle des services complémentaires de stimulus, de façon que ces procédures ne soient définies qu'une seule fois. La présente annexe exclut explicitement toutes les parties de la Rec. UIT-T H.248 qui sont liées au contrôle des connexions des médias, qui se fait uniquement à l'aide de la Rec. UIT-T H.245 normalisée ou de la connexion rapide.

L.1.3 Relation entre les stimulus H.323 et le protocole HTTP

L'Annexe K est utilisée pour la commande par une tierce partie d'un appel H.323 fondé sur une connexion hypertexte séparée (au moyen du protocole HTTP) en vue d'une interaction avec l'utilisateur. Il n'existe pas d'ensemble fixe de capacités pour l'interface utilisateur, divers types de formats de texte, d'images et de sons étant utilisés de façon dynamique. Le fournisseur de services (le serveur HTTP) est responsable du mappage entre les événements HTTP et les actions de commande d'appel (messages H.450 ou autres) pour les services complémentaires; l'extrémité H.323 n'est donc pas informée de l'application HTTP. Le fournisseur de services peut être associé au portier local, à l'extrémité distante ou au portier distant à l'intérieur de l'appel.

L.1.4 Relation avec les services complémentaires H.450

Le terminal à stimulus ne prenant pas en charge de services complémentaires H.450, le serveur à fonctions spéciales ou le portier est responsable de la fourniture d'une fonction de serveur mandataire en vue du traitement des procédures H.450 sur le réseau via le terminal.

Dans ces conditions, le serveur à fonctions spéciales devient une extrémité pour toutes les opérations H.450 et implémente tous les services complémentaires ainsi que les machines à états concernées. L'interaction avec l'utilisateur est assurée par l'interface utilisateur du téléphone, que le portier est capable de contrôler via la signalisation de stimulus H.323.

L.2 Introduction

L'exigence essentielle d'un protocole de stimulus H.323 réside dans la fourniture d'un ensemble de capacités permettant à des extrémités d'accéder à un ensemble potentiellement illimité de services complémentaires. Un tel protocole présente de nombreux avantages: par exemple, il permet aux extrémités de rester relativement légères et de garantir un certain degré de protection contre les effets d'une adjonction de fonctions. Ces services eux-mêmes sont généralement commandés par un portier, un serveur mandataire ou toute autre entité réseau. Dans la présente annexe, le terme

"serveur à fonctions spéciales" désigne de façon générique toute entité réseau permettant le contrôle de la configuration ou des stimulus des extrémités conformément au protocole décrit.

Les objectifs du protocole décrits dans la présente annexe sont les suivants:

- prise en charge de services complémentaires arbitraires (normalisés et non normalisés);
- interopérabilité de ces services entre le serveur à fonctions spéciales et l'extrémité;
- compatibilité en amont avec les extrémités utilisant la Rec. UIT-T H.323 (version 2 ou supérieure).

Ce protocole remplit ces objectifs en incorporant des parties importantes du protocole décrit dans la Rec. UIT-T H.248.1. La Rec. UIT-T H.248.1 décrit un modèle de commande d'extrémités reposant purement sur les stimulus, alors que la présente annexe doit nécessairement décrire un modèle hybride entre le modèle fonctionnel reposant sur les stimulus et le modèle fonctionnel fondé sur la Rec. UIT-T H.323. Les entités conformes à l'Annexe L utilisent des unités PDU H.248 en plus des messages H.323 normalisés afin de prendre en charge ce modèle hybride.

La présente annexe décrit un modèle schématique facilitant l'envoi de services dans des systèmes de base H.323 et H.248, en garantissant un niveau élevé de compatibilité entre un serveur à fonctions spéciales selon l'Annexe L et les composantes d'un contrôleur de passerelle média (MGC) H.248 non associé au contrôle des médias. Ce modèle schématique permet la réutilisation des paquetages H.248 dans des systèmes H.323, en apportant en général peu ou pas de modifications. Par exemple, des paquetages convenablement élaborés peuvent permettre à un serveur à fonctions spéciales de commander divers éléments d'interface utilisateur d'un terminal compatible, tels que:

- l'écriture sur un écran de visualisation de texte;
- la fourniture à l'extrémité d'indications indépendantes du matériel, à partir desquelles elle peut commander ses propres indicateurs, tels que des lampes indiquant des messages en attente ou des voyants d'appel;
- la réception d'informations entrées par l'utilisateur, telles que des chiffres, du texte, des codes spéciaux (par exemple, la commutation de raccrochage ou de décrochage ou des touches de fonction);
- l'attribution de fonctions à des touches programmables et à un répertoire résident d'extrémités;
- la demande d'application de tonalités particulières;
- la spécification dynamique de tonalités.

Les terminaux conformes à l'Annexe L possèdent, en commun avec les terminaux H.248, les capacités de commande énumérées ci-dessus. Ces deux types de terminaux diffèrent simplement par la manière de gérer les flux médias et leur association à un ou plusieurs appels ou "contextes".

L'utilisation du protocole décrit dans la présente annexe est conseillée en particulier pour les dispositifs d'extrémité simples conformes à l'Annexe F.

L.3 Modèle schématique des stimulus

L.3.1 Aperçu général

Les terminaux conformes à l'Annexe L utilisent les mécanismes H.323 normalisés pour l'enregistrement et l'établissement de voies de signalisation. La signalisation normale d'appel H.225.0 est utilisée pour l'établissement et la fin de l'appel. La commande de média peut utiliser les procédures de connexion rapide H.323 (comprenant la répétition de l'élément fastStart) ou, éventuellement, la signalisation H.245 faisant appel aux procédures décrites dans les Recommandations UIT-T H.245 et H.323 et leurs annexes. L'utilisation de ces mécanismes peut se traduire par la création d'éléments qui sont analogues à ceux de la Rec. UIT-T H.248, tels que des

terminaisons éphémères (elles ne sont pas directement contrôlables par le biais de la présente annexe).

Les capacités de signalisation de stimulus des extrémités conformes à l'Annexe L seront spécifiées dans des paquetages de la même manière que dans la Rec. UIT-T H.248. Par exemple, un terminal conforme à l'Annexe L pourrait être décrit par un paquetage de base (pour des changements de commutation de raccrochage ou de décrochage, etc.), un paquetage clavier, un paquetage alerte, un paquetage touches et un paquetage affichage. On pourrait ajouter des paquetages supplémentaires afin de permettre une modification des paramètres opérationnels et/ou pour obtenir des statistiques relatives à la qualité de fonctionnement.

Comme les terminaux conformes à l'Annexe L sont essentiellement des extrémités H.323, les procédures de cette Recommandation seront toujours applicables et ne peuvent pas être invalidées par une signalisation H.248. Par exemple, si l'application d'une commande H.248 aboutit à la terminaison d'un appel, il reste toujours nécessaire de faire appel à la signalisation H.245 normalisée et à la signalisation H.225.0 pour la terminaison d'un appel.

L.3.2 Signalisation de protocole

La seule forme de signalisation que l'ensemble des entités H.323 doit prendre en charge est la signalisation d'appel H.225.0. Il s'agit du mode de transport le plus approprié pour le protocole de stimulus car il permet le placement du serveur à fonctions spéciales au même endroit qu'un portier ou que tout autre type d'extrémité H.323.

Les entités conformes à l'Annexe L devraient prendre en charge l'encapsulation des messages H.248 dans le champ **StimulusControl** qui peut être acheminé dans tous les messages de signalisation d'appel H.225.0. A chaque appel auquel elle participe, l'extrémité conforme à l'Annexe L qui prend en charge l'encapsulation H.248 comportera un champ **StimulusControl** dans le premier message de signalisation d'appel H.225.0 qu'elle envoie à toute autre entité H.323 (le champ **StimulusControl** peut être vide).

Lorsqu'une extrémité s'inscrit à un portier, ce dernier peut indiquer un nom alias (pseudonyme) au serveur à fonctions spéciales dans le champ **featureServerAlias** de la confirmation d'enregistrement. Lorsque ce nom alias est présent, il devrait être utilisé par l'extrémité conforme à l'Annexe L comme destination du serveur pour la signalisation H.248 en mode non tunnel qui est limitée à la fonctionnalité définie dans la présente annexe. L'utilisation de cette adresse pseudonyme permet au portier d'associer ou d'acheminer l'appel au serveur à fonctions spéciales. Dès réception d'un nom alias valable **featureServerAlias** dans une confirmation d'enregistrement, une extrémité de soutien enverra immédiatement une commande **ServiceChange** H.248 contenant l'identification Root TerminationId à l'adresse indiquée du serveur à fonctions spéciales.

Cela permet l'établissement de deux modèles d'interaction entre un serveur à fonctions spéciales et une extrémité conforme à l'Annexe L:

- le serveur à fonctions spéciales est présent dans le chemin de signalisation d'appel pour tous les messages de signalisation d'appel H.225.0, pour tous les appels en provenance et à destination d'une extrémité conforme à l'Annexe L;
- une connexion de signalisation d'appel séparée entre l'extrémité conforme à l'Annexe L et le serveur à fonctions spéciales est établie uniquement lorsque cette fonction est invoquée.

L.3.3 Utilisation de la Rec. UIT-T H.248

Les extrémités conformes à l'Annexe L prendront en charge les procédures du niveau de transaction défini au § 7.2/H.248.1. La signalisation conforme à l'Annexe L peut faire intervenir n'importe laquelle des commandes définies au § 7/H.248.1.

Dans la mesure où les terminaux conformes à l'Annexe L n'utilisent pas la Rec. UIT-T H.248 pour le contrôle des médias, l'utilisation des descripteurs ci-après de la Rec. UIT-T H.248 ne s'applique

pas aux entités conformes à l'Annexe L: descripteur Modem, descripteur Mux, descripteur Stream, descripteur LocalControl, descripteur Local, descripteur Remote et descripteur Topology. Ces descripteurs ne seront pas utilisés pour la signalisation conforme à l'Annexe L et ne seront pas pris en considération s'ils sont reçus. A noter que l'on ne peut utiliser l'Annexe L pour traiter spécifiquement des différents flux médias; si un terminal conforme à la présente annexe prend en charge plusieurs flux de médias (par exemple, audio et vidéo) on suppose implicitement que l'affectation d'une terminaison au contexte de l'appel (0xFFFFFFFD, voir § L.3.4 ci-dessous) se rapporte au flux qui achemine le support approprié.

Les paquetages pris en charge par l'extrémité devraient être énumérés dans le champ **supportedH248Packages** du message RRQ lorsque l'extrémité s'inscrit à un portier. Si ce champ est présent mais vide, un serveur à fonctions spéciales peut utiliser une interrogation AuditCapabilities pour déterminer les paquetages pris en charge.

L.3.4 Encapsulation conforme à la Rec. UIT-T H.225.0

Toute la signalisation relative à l'Annexe L, encapsulée selon la Rec. UIT-T H.225.0 utilise une structure **StimulusControl**. L'emploi de ces champs est décrit dans le présent paragraphe. L'utilisation de l'Annexe L par une extrémité est déduite de la présence de cette structure dans le premier message de signalisation d'appel envoyé par l'extrémité au serveur à fonctions spéciales. Si aucun message H.248 n'est encapsulé dans cette structure, l'ensemble de ses champs facultatifs peut être omis.

La commande de stimulus conforme à l'Annexe L sera signalée au moyen du champ **stimulusControl** dans l'élément UU-PDU-H323 qui est utilisé pour la signalisation d'appel dans la Rec. UIT-T H.323.

Le message H.248 à envoyer sera encapsulé dans le champ **h248Message** de la séquence **stimulusControl**. Le message encapsulé est du type de données MegacoMessage complet tel qu'il est défini dans la Rec. UIT-T H.248.1.

Lorsqu'un serveur à fonctions spéciales conforme à l'Annexe L devient actif dans le contexte d'un appel existant, il peut avoir besoin de déterminer l'état de cet appel et/ou de l'extrémité. Cela est possible grâce à la commande AuditValue H.248.

L'affectation d'identificateurs de terminaison (TerminationIds) pour les terminaisons physiques à l'extrémité peut être assurée sur le serveur à fonctions spéciales et l'extrémité, prédéfinis dans un paquetage, ou obtenus via la commande AuditCapabilities.

La signalisation H.248 peut reposer sur un codage binaire (utilisant la syntaxe de l'Annexe A/H.248.1, mais selon les règles de codage compact (PER) pour le codage) ou alphanumérique (Annexe B/H.248.1). Le codage par défaut est le codage binaire. On emploiera le champ **isText** pour indiquer que le codage conforme à l'Annexe B/H.248.1 a été utilisé pour les descripteurs H.248 dans la structure **StimulusControl**. Les extrémités conformes à l'Annexe L ne peuvent prendre en charge qu'une seule forme de codage et utiliseront la même forme de codage pour toute la signalisation conforme à l'Annexe L vers un serveur à fonctions spéciales. Les serveurs à fonctions spéciales conformes à l'Annexe L devraient prendre en charge les deux formes de codage. La communication entre un serveur à fonctions spéciales et une extrémité ne peut se faire qu'au moyen de la forme de codage pour laquelle l'extrémité a signalé sa prise en charge.

En ce qui concerne la signalisation relative à l'Annexe L, encapsulée selon la Rec. UIT-T H.225.0, on utilisera la valeur spéciale "ANNEX-L", définie par 0xFFFFFFFD, comme identificateur ContextId pour toutes les transactions liées à l'appel. Toutes les commandes s'appliquent à l'appel H.323 en cours (tel qu'il est représenté par l'identificateur **callIdentifier** du message de signalisation d'appel H.225.0 encapsulant la commande H.248). Les commandes non liées à l'appel, représentées par le message H.225.0 encapsulant seront associées à une valeur ContextId de NULL, définie dans la Rec. UIT-T H.248.1.

Les transactions encapsulées selon l'Annexe L n'utiliseront pas de valeurs ContextId autres que NULL (définie dans la Rec. UIT-T H.248.1) ou ANNEX-L (définie plus haut).

Certaines activités H.248 peuvent ne pas être associées à des appels H.323 actifs. Dans ce cas, on peut utiliser n'importe quelle voie de signalisation d'appel existante entre l'extrémité et le serveur à fonctions spéciales et l'on mettra en œuvre les procédures de la Rec. UIT-T H.248 pour associer l'activité aux objets H.248 appropriés. Pour ces activités, on peut utiliser les procédures de signalisation indépendante de l'appel conformes à la Rec. UIT-T H.323. Pour la signalisation indépendante de l'appel, on utilisera la procédure décrite au § 7.2/H.450.1.

S'agissant des activités H.248 pouvant être associées à un appel actif avec le serveur à fonctions spéciales approprié dans le trajet de signalisation de l'appel, on peut utiliser n'importe quel message approprié de signalisation d'appel H.225.0 pour communiquer entre le serveur à fonctions spéciales et l'extrémité.

L.4 Références normatives

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

– Recommandation UIT-T H.248.1 (2005), *Protocole de commande de passerelle: version 3*.

– Recommandation UIT-T H.248.3 (2000), *Protocole de commande de passerelle: paquetages des actions et éléments d'interface utilisateur*.

– Recommandation UIT-T H.450.1 (1998), *Protocole générique fonctionnel pour le support des services complémentaires dans les systèmes H.323*.

Annexe M1

Canalisation de la signalisation à l'interface Q (QSIG) dans les réseaux H.323

M1.1 Domaine d'application

La présente annexe propose des lignes directrices sur la manière dont le mécanisme de canalisation générique décrit au § 10.4 peut être utilisé pour canaliser la signalisation à l'interface Q (QSIG) dans les réseaux H.323. Des groupes tels que ceux de l'ISO/CEI auront la responsabilité finale des procédures de signalisation à l'interface Q (QSIG) proprement dites. On trouvera les informations sur la signalisation QSIG (également appelée PSS1) dans les références [M1-1] et [M1-2] ci-dessous.

M1.2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte

étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[M1-1] ISO/CEI 11572:2000, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé à intégration de services – Services porteurs en mode circuit – Procédures et protocole de signalisation d'interéchange*.

[M1-2] ISO/CEI 11582:2002, *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseau privé à intégration de services – Protocole générique fonctionnel pour le support de compléments de service – Procédures et protocole de signalisation entre commutateurs*.

[M1-3] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

M1.3 Procédures aux dispositifs d'extrémité

Les dispositifs d'extrémité qui prennent en charge la canalisation des informations QSIG doivent utiliser les procédures du § 10.4, l'identificateur d'objet suivant étant utilisé comme TunnelledProtocol:

- **{iso (1) identified-organization (3) icd-ecma (0012) private-isdn-signalling-domain (9)}**

Les messages H.225.0 canalisent l'ensemble du message QSIG, inchangé, en commençant par le champ discriminateur de protocole et en terminant par les autres éléments d'information. Le contenu binaire des messages QSIG est codé comme une chaîne d'octets dans le contenu des messages **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Etant donné que c'est la forme codée binaire des messages QSIG qui est canalisée, l'intégrité de ces messages est entièrement préservée, y compris tout codage de base BER ASN.1 dans les éléments d'information d'indicateur de fonctionnalité ou de notification.

Des messages QSIG peuvent, mais cela n'est pas indispensable, être canalisés dans les messages H.225.0 correspondants. Le message QSIG SETUP, par exemple, peut être canalisé dans un message SETUP H.225.0, et le message QSIG RELEASE COMPLETE peut être canalisé dans un message RELEASE COMPLETE H.225.0. Pour d'autres messages, il est possible qu'il n'y ait pas de message H.225.0 (Q.931) correspondant (par exemple, un message QSIG DISCONNECT) ou que le message correspondant n'est pas disponible parce qu'il a déjà été envoyé. Dans ces cas, le message QSIG peut être canalisé dans un message FACILITY H.225.0. Un message QSIG CALL PROCEEDING devrait être canalisé dans un message FACILITY H.225.0 étant donné que le message CALL PROCEEDING H.225.0 n'a pas de signification de bout en bout. De plus, étant donné que les messages NOTIFY et PROGRESS sont facultatifs, ils risquent de ne pas être remis de bout en bout et devraient être canalisés dans un message FACILITY, sauf si des tonalités ou des annonces sont fournies par l'extrémité appelée et qu'aucun indicateur Progress n'a encore été envoyé à l'extrémité appelante. Dans ce cas, il convient d'utiliser un message PROGRESS (avec un descripteur Progress 1 ou 8) pour canaliser un message QSIG PROGRESS. Les procédures de libération d'appel QSIG peuvent être prises en charge en canalisant les messages QSIG DISCONNECT et RELEASE dans un message FACILITY H.225.0. Dans le cas particulier où un message QSIG RELEASE canalisé est interprété comme un message QSIG RELEASE COMPLETE canalisé (cela se produit lorsqu'un message QSIG RELEASE est reçu alors qu'un message RELEASE COMPLETE était attendu), l'appel H.323 peut être libéré par le côté recevant le message QSIG RELEASE par l'envoi d'un message RELEASE COMPLETE H.225.0 sans message QSIG canalisé.

Un appel QSIG unique peut être canalisé dans un appel H.323 unique. La relation entre les références d'appel QSIG et les références d'appel H.225.0 ne relève pas du domaine de la présente Recommandation.

Le Tableau M1.1 illustre, à titre indicatif, un exemple du mappage entre messages QSIG et messages H.225.0.

Tableau M1.1/H.323 – Mappage entre messages QSIG et messages H.225.0

Message QSIG	Message H.225.0
SETUP	SETUP
ALERTING	ALERTING
CONNECT	CONNECT
RELEASE COMPLETE	RELEASE COMPLETE
CALL PROCEEDING	FACILITY
FACILITY	
PROGRESS (Note)	
NOTIFY	
DISCONNECT	
RELEASE	
Tous autres messages ...	
NOTE – Si des tonalités ou des annonces sont fournies par l'extrémité appelée, ce message devrait être canalisé non pas dans un message FACILITY, mais dans un message PROGRESS.	

M1.4 Canalisation de connexion QSIG orientée signalisation indépendante de l'appel

Aucun canal de commande H.245 ni aucun canal de média n'est requis pour les connexions de signalisation QSIG indépendantes de l'appel.

Les procédures de signalisation d'appel H.225.0 peuvent être utilisées pour établir une connexion de signalisation indépendante de l'appel entre les dispositifs d'extrémité homologues, comme indiqué au § 10.4.

M1.5 Procédures avec portier

Un portier participant à l'appel dans lequel est utilisée la canalisation QSIG entre les dispositifs d'extrémité doit faire passer les messages QSIG sans changement à moins qu'il n'envisage de mettre fin à la canalisation. Cela peut être le cas lorsque le portier offre des services QSIG émulés.

Annexe M2

Tunnellisation du protocole de signalisation (ISUP) dans les réseaux H.323

M2.1 Domaine d'application

L'objet de la présente annexe est de donner des instructions sur la façon dont le mécanisme générique de tunnellisation décrit au § 10.4 peut être utilisé pour mettre en tunnel l'ISUP dans les réseaux en mode H.323. D'autres commissions, de l'UIT-T en particulier, sont chargées en dernier ressort des procédures ISUP proprement dites. L'on pourra trouver des informations sur l'ISUP dans les références [M2-1] et [M2-2] ci-dessous.

M2.2 Références normatives

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

[M2-1] Recommandation UIT-T Q.763 (1999), *Système de signalisation n° 7 – Formats et codes du sous-système utilisateur du RNIS*.

[M2-2] Recommandation UIT-T Q.764 (1999), *Système de signalisation n° 7 – Procédures de signalisation du sous-système utilisateur du RNIS*.

[M2-3] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

M2.3 Procédures aux extrémités

Les extrémités prenant en charge la tunnellisation des informations ISUP doivent utiliser les procédures du § 10.4. L'extrémité doit identifier la variante de l'ISUP en utilisant soit la structure **tunnelledProtocolObjectID** soit la structure **TunnelledProtocolAlternateIdentifier**. Le champ **subIdentifier** peut servir à identifier la révision de la variante de l'ISUP, par exemple "1988". Voir Tableau M2.1.

Tableau M2.1/H.323 – Exemples de protocoles mis en tunnel identifiés par la structure tunnelledProtocolObjectID

Norme	tunnelledProtocolObjectID	subIdentifier
Rec. UIT-T Q.763 (1988)	{itu-t (0) recommendation (0) q (17) 763}	"1988"
Rec. UIT-T Q.763 (1992)	{itu-t (0) recommendation (0) q (17) 763}	"1992"

Lorsqu'on utilise la structure **TunnelledProtocolAlternateIdentifier**, le champ **protocolType** doit être mis à "isup". Le champ **protocolVariant** doit être une chaîne identifiant la spécification ISUP utilisée, par exemple un numéro de document. Voir Tableau M2.2.

Tableau M2.2/H.323 – Exemples de protocoles mis en tunnel identifiés par TunnelledProtocolAlternateIdentifier

Spécification ISUP (Note)	protocolType	protocolVariant	subIdentifier
ANSI T1.113-1988	"isup"	"ANSI T1.113-1988"	"1988"
ETS 300 121	"isup"	"ETS 300 121"	"121"
ETS 300 356	"isup"	"ETS 300 356"	"356"
BELLCORE GR-317	"isup"	"BELLCORE GR-317"	"317"
JT-Q761-4 (1987-1992)	"isup"	"JT-Q761-4 (1987-1992)"	"87"
JT-Q761-4 (1993)	"isup"	"JT-Q761-4 (1993)"	"93"
NOTE – La spécification ISUP peut être une norme, une Recommandation ou tout autre document spécifiant le protocole ISUP, par exemple une spécification d'interconnexion ISUP pour un pays donné.			

- **{ itu-t (0) recommendation (0) q (17) 763 }**

Les messages H.225.0 tunnellisent l'ensemble du message ISUP sans changement, à partir du paramètre codant le type de message jusqu'aux autres paramètres. Le contenu binaire des messages ISUP est codé sous la forme d'une chaîne d'octets dans la structure **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Etant donné que le codage binaire des messages ISUP est ce qui est tunnellisé, l'intégrité des messages ISUP est pleinement préservée.

Par exemple, le message IAM de l'ISUP peut être mis en tunnel dans un message SETUP du protocole H.225.0 et le message ANM de l'ISUP peut être mis en tunnel dans un message CONNECT du protocole H.225.0. Pour les autres messages, il se peut qu'il n'y ait pas de message H.225.0 correspondant (par exemple dans le cas d'un message IDR de l'ISUP) ou que le message correspondant ne soit pas disponible parce qu'il a déjà été envoyé. Dans ces cas-là, le message ISUP peut être tunnellisé dans un message FACILITY du protocole H.225.0.

Une même communication ISUP peut être tunnellisée dans une même communication H.323.

Certains éléments d'information du message H.225.0 peuvent avoir été modifiés par le réseau H.323 et la passerelle recevant le message ISUP en tunnel peut avoir besoin de neutraliser les paramètres ISUP correspondants.

Le fanion **tunnellingRequired** doit être inclus dans le message Setup lorsque le paramètre ISUP requis dans le message IAM indique la valeur "ISUP requis".

Le Tableau M2.3 ci-dessous n'est qu'indicatif. Il décrit un exemple de mappage entre messages ISUP et messages H.225.0.

Tableau M2.3/H.323 – Mappage entre messages ISUP et messages H.225.0

Message ISUP	Message H.225.0
IAM	SETUP
SAM	INFORMATION
CPG	CALL PROCEEDING, ALERTING, PROGRESS, NOTIFY or FACILITY
ACM	CALL PROCEEDING, ALERTING, PROGRESS, NOTIFY or FACILITY
ANM, CON	CONNECT
REL	RELEASE COMPLETE
Tous autres messages	FACILITY

M2.4 Procédures au portier

Un portier participant à une communication faisant appel à la canalisation en tunnel de l'ISUP entre les extrémités doit normalement transmettre sans changement les messages ISUP en tunnel, à moins qu'il n'ait l'intention de fermer le tunnel ISUP, ce qui peut être le cas lorsqu'un portier offre des services de l'ISUP.

Un portier ne doit pas sélectionner une extrémité qui ne prend pas en charge l'ISUP lorsque le fanion **tunnellingRequired** est inclus dans le message Setup.

Annexe M3

Tunnellisation de la signalisation DSS1 à travers les réseaux H.323

M3.1 Domaine d'application

L'objet de la présente annexe consiste à définir des directives quant aux modalités d'utilisation du mécanisme de générique de tunnellisation décrit au § 10.4 afin de tunnelliser la signalisation DSS1 (Q.931) à travers des réseaux H.323. D'autres groupes peuvent adapter cette procédure afin de tenir compte des variantes nationales du protocole DSS1.

M3.2 Références normatives

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

[M3-1] Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

[M3-2] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

[M3-3] Recommandation UIT-T H.450.1 (1998), *Protocole générique fonctionnel pour le support des services complémentaires dans les systèmes H.323*.

M3.3 Procédures appliquées aux points d'extrémité

Les points d'extrémité qui prennent en charge la tunnellisation des informations DSS1 doivent appliquer les procédures décrites au § 10.4, l'identificateur OBJECT IDENTIFIER suivant étant utilisé en tant que contenu du champ **TunnelledProtocol.id.tunnelledProtocolObjectID** dans un message de signalisation d'appel H.225.0 et dans le message RAS H.225.0:

- **{itu-t (0) recommendation (0) q (17) 931}**

  Les points d'extrémité qui prennent en charge la tunnellisation des informations DSS1 et qui feront ensuite office d'entité utilisateur DSS1 doivent appliquer les procédures définies au § 10.4, la valeur suivante étant utilisée en tant que valeur du champ **TunnelledProtocol.subIdentifier**:

- **"User"**

  Les points d'extrémité qui prennent en charge la tunnellisation des informations DSS1 et qui font ensuite office d'entité réseau DSS1 doivent appliquer les procédures définies au § 10.4, la valeur suivante étant utilisée comme valeur du champ **TunnelledProtocol.subIdentifier**:

- **"Network"**

  Lors de l'envoi d'un message RAS H.225.0 exigeant l'utilisation d'un protocole tunnellisé spécifique (voir § 10.4.2) dans le champ **desiredTunnelledProtocol** un point d'extrémité doit inclure l'identificateur OBJECT IDENTIFIER et le sous-identificateur du protocole auquel il s'attend à l'autre extrémité afin de garantir une fonctionnalité adéquate du portier.

  Puisque le protocole DSS1 est asymétrique, il peut seulement être utilisé entre un utilisateur et une entité réseau. L'emploi d'identificateurs OBJECT IDENTIFIERS différents pour les entités utilisateurs et les entités réseaux permet aux points d'extrémité H.323 de garantir l'absence de tunnellisation du protocole DSS1 entre deux entités utilisateurs ou deux entités réseaux.

  Les messages H.225.0 tunnellisent la totalité du message, inchangé, en commençant par le champ discriminateur de protocole et en terminant par les autres éléments d'information. Le contenu binaire des messages DSS1 est codé comme une chaîne d'OCTET STRING dans le champ:

  H323-UU-PDU.tunnelledSignallingMessage.messageContent

  Le contenu binaire des messages DSS1 étant identique au contenu tunnellisé, l'intégrité des messages DSS1 est entièrement préservé, notamment tout codage compact BER de l'ASN.1 dans les éléments d'information identificateurs de fonctionnalité ou de notification.

  Les messages DSS1 peuvent être tunnellisés dans le message H.225.0 correspondant ou dans les messages H.225.0 FACILITY. Par exemple, le message DSS1 SETUP peut être tunnellisé dans un message H.225.0 SETUP, et le message Release Complete DSS1 RELEASE COMPLETE peut être tunnellisé dans un message H.225.0 RELEASE COMPLETE. En ce qui concerne les autres messages, le message H.225.0 correspondant peut être non pris en charge (par exemple un message DSS1 CONNECT ACK), non disponible parce qu'il a déjà été envoyé ou encore transporté de façon non transparente de bout en bout. Dans ces cas, le message DSS1 doit être tunnellisé dans un message H.225.0 FACILITY. En particulier, les messages H.225.0 SETUP ACKNOWLEDGE ou CALL PROCEEDING ne doivent pas servir à la tunnellisation d'un message DSS1, parce qu'ils risquent de ne pas atteindre le point d'extrémité H.225.0 émetteur, si un portier intermédiaire n'a pas déjà envoyé un message de ce type. En revanche, pour la tunnellisation d'un message DSS1 SETUP ACKNOWLEDGE ou CALL PROCEEDING, il

faut envoyer dans un premier temps un message H.225.0 SETUP ACKNOWLEDGE ou un message CALL PROCEEDING sans message DSS1 tunnellisé, puis un message H.225.0 FACILITY qui tunnellise le message DSS1 SETUP ACKNOWLEDGE ou le message DSS1 CALL PROCEEDING. Par ailleurs, les messages DSS1 STATUS et STATUS ENQUIRY doivent être tunnellisés dans un message H.225.0 FACILITY, pour assurer que les messages DSS1 atteignent le point d'extrémité H.225.0.

La tunnellisation des messages DSS1 DISCONNECT et RELEASE dans le message H.225.0 FACILITY permet de prendre en charge les procédures de libération de la communication DSS1.

Un même appel DSS1 peut être tunnellisé dans un même appel H.323. La référence d'appel DSS1 est choisie par le point d'extrémité d'entrée et doit rester la même dans tous les messages DSS1 tunnellisés pour un appel H.323. Toutefois, la valeur de référence d'appel DSS1 dans un réseau TDM correspond à une et une seule entité DSS1 homologue. Dans un système H.323, il n'y a pas de référence à une entité DSS1 homologue, puisque n'importe quel appel H.323 peut atteindre n'importe quel point d'extrémité. Pour garantir son unicité, la valeur de référence d'appel H.323 doit servir exclusivement à l'identification de l'appel H.323.

Un même appel ne doit pas utiliser conjointement la procédure de tunnellisation DSS1 et les procédures H.450.1.

Les relations entre les messages tunnellisés DSS1 et les messages contenant H.225.0 sont représentées au Tableau M3.1.

Tableau M3.1/H.323 – Relation entre les messages tunnellisés DSS1 et les messages H.225.0 qui les contiennent

Message Q.931/Q.932	Message H.225.0	Remarque
Messages d'établissement d'appel		
ALERTING	ALERTING	
CALL PROCEEDING	FACILITY	
CONNECT	CONNECT	
CONNECT ACKNOWLEDGE	FACILITY	
INFORMATION	FACILITY	La prise en charge d'un message H.225.0 INFORMATION est facultative
PROGRESS	FACILITY	La prise en charge d'un message H.225.0 PROGRESS est facultative
SETUP	SETUP	
SETUP ACKNOWLEDGE	FACILITY	
Messages de libération d'appel		
DISCONNECT	FACILITY	
RELEASE	FACILITY	
RELEASE COMPLETE	RELEASE COMPLETE	

Tableau M3.1/H.323 – Relation entre les messages tunnellisés DSS1 et les messages H.225.0 qui les contiennent

Message Q.931/Q.932	Message H.225.0	Remarque
Messages de la phase information de l'appel		
RESUME	A étudier	
RESUME ACKNOWLEDGE	A étudier	
RESUME REJECT	A étudier	
SUSPEND	A étudier	
SUSPEND ACKNOWLEDGE	A étudier	
SUSPEND REJECT	A étudier	
USER INFORMATION	FACILITY	
Messages divers		
CONGESTION CONTROL	FACILITY	
NOTIFY	FACILITY	La prise en charge du message H.225.0 NOTIFY est facultative
STATUS	FACILITY	
STATUS ENQUIRY	FACILITY	
FACILITY	FACILITY	
HOLD	FACILITY	
HOLD ACKNOWLEDGE	FACILITY	
HOLD REJECT	FACILITY	
RETRIEVE	FACILITY	
RETRIEVE ACKNOWLEDGE	FACILITY	
RETRIEVE REJECT	FACILITY	
NOTE – Les messages DSS1 comportant une référence d'appel globale, par exemple, RESTART, RESTART ACK et STATUS peuvent être traités par les points d'extrémité et ne sont donc pas nécessairement tunnellisés.		

M3.4 Tunnellisation de signalisation DSS1 indépendante du support

La tunnellisation des mécanismes de transport indépendants du support du protocole DSS1, tels qu'ils sont décrits au § 6.3.2/Q.932, n'exige aucune voie de commande H.245, ni aucune voie de média.

Les procédures de signalisation d'appel de la Rec. UIT-T H.225.0 peuvent servir à établir une connexion de signalisation indépendante de l'appel, entre les points d'extrémité homologues, tels qu'indiqués au § 10.4. Les indications détaillées concernant cette connexion de signalisation indépendante de l'appel sont également présentées au § 6.2/H.450.1.

M3.4.1 L'utilisation du mécanisme de transport DSS1 en mode sans connexion

Le mécanisme de transport DSS1 en mode sans connexion défini au § 6.3.2.2/Q.932, s'appuie sur des messages FACILITY avec la valeur de référence d'appel fictive.

Chaque message DSS1 FACILITY de ce type doit être transporté au moyen d'une connexion H.225.0 distincte, laquelle doit être libérée immédiatement après que le message a atteint l'extrémité de destination.

En particulier, un message DSS1 FACILITY doit être transporté dans un message H.225.0 SETUP tel qu'indiqué au § 10.4 et au § 6.2/H.450.1. L'extrémité de destination (mais sans portier intermédiaire) doit libérer cette connexion immédiatement au moyen d'un message H.225.0 RELEASE COMPLETE. De plus, l'entité qui envoie le message H.225.0 SETUP doit libérer la communication après avoir enregistré l'expiration d'une temporisation convenablement choisie amorcée après l'envoi du message H.225.0 SETUP.

M3.4.2 Transport DSS1 en mode connexion indépendant du support

Le mécanisme DSS1 de transport en mode connexion indépendant du support, tel qu'il est décrit au § 6.3.2.1/Q.932, s'appuie sur des connexions établies au moyen de messages REGISTER.

Le mappage suivant des messages doit alors être utilisé:

Message Q.931/Q.932	Message H.225.0	Remarque
REGISTER	SETUP	Le message H.225.0 SETUP doit être utilisé pour configurer une connexion de signalisation indépendante de l'appel telle qu'indiquée au § 6.2/H.450.1. Le message H.225.0 SETUP doit être acquitté au moyen d'un message H.225.0 CONNECT afin d'éviter une libération de l'appel suite à l'expiration du temporisateur T303.
FACILITY	FACILITY	
RELEASE COMPLETE	RELEASE COMPLETE	

M3.5 Procédures relatives au portier

Un portier participant à l'appel utilisant la tunnellisation du protocole DSS1 entre les points d'extrémité doit transmettre les messages ainsi acheminés sans les modifier, à moins qu'il ne prévoie de participer aux procédures DSS1 et de mettre fin au protocole DSS1. Tel peut être le cas lorsqu'un portier propose des services DSS1.

Annexe M4

Tunnellisation de la syntaxe de signalisation en bande étroite (NSS) à travers les réseaux H.323

M4.1 Domaine d'application

La présente annexe a pour objet de donner des directives concernant la manière dont le mécanisme générique de tunnellisation décrit au § 10.4 peut être utilisé pour tunnelliser la syntaxe de signalisation en bande étroite (NSS, *narrowband signalling syntax*) dans les réseaux H.323. D'autres groupes au sein de l'UIT-T sont chargés en dernier ressort des procédures NSS proprement dites. On trouvera des informations relatives à la syntaxe NSS dans la Rec. UIT-T Q.1980.1.

M4.2 Références normatives

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

– Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

– Recommandation UIT-T Q.1980.1 (2004), *Syntaxe de signalisation en bande étroite (NSS) – Définition de la syntaxe*.

M4.3 Procédures appliquées aux points d'extrémité H.225.0

Les points d'extrémité prenant en charge la tunnellisation des informations NSS appliqueront les procédures décrites au § 10.4. Les points d'extrémité identifieront la syntaxe NSS au moyen de la structure **tunnelledProtocolObjectID**. Le champ **subIdentifier** peut servir à identifier la révision de la variante de la syntaxe NSS, par exemple "2004". Voir le Tableau M4.1.

Tableau M4.1/H.323 – Syntaxe NSS identifiée par la structure tunnelledProtocolObjectID

Norme	tunnelledProtocolObjectID	subIdentifier
Rec. UIT-T Q.1980.1 (2004)	{uit-t (0) recommendation (0) q (17) 1980 1}	"2004"

Les messages H.225.0 tunnellisent la totalité du message NSS, inchangé, en commençant par le paramètre Version (VER) et en terminant par deux paires séquentielles d'octets retour-chariot-ligne suivante (0xD0xA). Le contenu textuel des messages NSS est codé sous la forme d'une chaîne d'octets dans la structure **H323-UU-PDU.tunnelledSignallingMessage.messageContent**. Etant donné que le codage textuel des messages NSS est ce qui est tunnellisé, l'intégrité des messages NSS est entièrement préservée.

Par exemple, le message IAM de syntaxe NSS peut être tunnellisé dans un message SETUP H.225.0 et le message ANM de syntaxe NSS dans un message CONNECT H.225.0. Pour les autres messages, il se peut qu'il n'y ait pas de message H.225.0 correspondant (par exemple, dans le cas d'un message IDR de syntaxe NSS) ou que le message correspondant ne soit pas disponible parce qu'il a déjà été envoyé. En pareils cas, le message NSS peut être tunnellisé dans un message FACILITY H.225.0.

Un même appel NSS doit être tunnellisé dans un même appel H.323.

Certains éléments d'information du message H.225.0 peuvent avoir été modifiés par le réseau H.323, et la passerelle recevant le message NSS tunnellisé peut avoir besoin de neutraliser les paramètres NSS correspondants.

Le Tableau M4.2 n'est donné qu'à titre indicatif. Il illustre un exemple de mappage entre messages NSS et messages H.225.0.

Tableau M4.2/H.323 – Mappage entre messages NSS et messages H.225.0

Message NSS	Message H.225.0
IAM	SETUP
SAM	INFORMATION
CPG	CALL PROCEEDING, ALERTING, PROGRESS, NOTIFY ou FACILITY
ACM	CALL PROCEEDING, ALERTING, PROGRESS, NOTIFY ou FACILITY
ANM, CON	CONNECT
REL	RELEASE COMPLETE
Tous autres messages	FACILITY

M4.4 Procédures applicables au portier

Un portier participant à un appel dans lequel est utilisée la tunnellisation de syntaxe NSS entre les points d'extrémité doit transmettre sans changement les messages NSS en tunnel à moins qu'il n'ait l'intention de fermer le tunnel NSS. Cela peut être le cas lorsque le portier offre des services NSS.

M4.5 Procédures de signalisation RAS applicables aux appels à routage direct

Dans le cas d'appels à routage direct, le point d'extrémité H.323 souhaitera peut-être échanger des messages NSS avec le portier. Le point d'extrémité H.323 peut envoyer au portier tout ou partie des messages NSS tunnellisés dans des messages RAS.

Un message RAS tunnellisera la totalité du message NSS, inchangé, en commençant par le paramètre Version (VER) et en terminant par deux paires séquentielles d'octets chariot de retour-chariot-ligne suivante (0xD0xA).

Par exemple, le message IAM de syntaxe NSS peut être tunnellisé dans des messages RAS de types ARQ ou ACF et le message REL de syntaxe NSS dans des messages RAS de types DRQ ou DCF. Quant aux autres messages NSS, ils peuvent être tunnellisés dans des messages RAS de types SCI ou SCR. Le Tableau M4.3 n'est donné qu'à titre indicatif. Il illustre un exemple de mappage entre messages NSS et messages RAS.

Tableau M4.3/H.323 – Mappage entre messages NSS et messages RAS

Message NSS	Message RAS
IAM	ARQ, ACF
REL	DRQ, DCF
Tous autres messages	SCI, SCR

M4.5.1 Elément de tunnel de protocole RAS

Les messages NSS seront encapsulés dans un paramètre de tunnel de protocole dans les messages RAS. Le paramètre de tunnel de protocole sera codé dans le paramètre genericData dans le paramètre de demande du message RAS H.225.0.

Le paramètre GenericData indique l'élément de tunnel de protocole et contient un paramètre de tunnel de protocole.

Le Tableau M4.4 définit l'élément de tunnel de protocole RAS.

Tableau M4.4/H.323 – Elément de tunnel de protocole RAS

Nom de l'élément	Tunnel de protocole RAS
Description de l'élément	Cet élément permet à des messages NSS d'être tunnellisés dans des messages RAS
Type d'identificateur de l'élément	Normal
Valeur d'identificateur de l'élément	1000

M4.5.2 Paramètre de tunnel de protocole RAS

Le Tableau M4.5 définit le paramètre de tunnel de protocole RAS.

Tableau M4.5/H.323 – Paramètre de tunnel de protocole RAS

Nom du paramètre	Tunnel de protocole
Description du paramètre	Permet d'encapsuler le message NSS envoyé dans un message RAS. Le contenu est un champ brut constitué du message RasTunnelledSignallingMessage codé PER ASN.1 comme indiqué dans la notation ASN.1 ci-dessous
Type d'identificateur de paramètre	Normal
Valeur d'identificateur de paramètre	1
Type de paramètre	Brut
Cardinalité des paramètres	Une seule fois

M4.5.3 Définition ASN.1 du tunnel de protocole

La définition du tunnel de protocole utilisée dans la structure GenericData est indiquée ci-après.

```
RAS-PROTOCOL-TUNNEL DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     TunnelledProtocol,
     NonStandardParameter
     FROM H323-MESSAGES;

RasTunnelledSignallingMessage ::=         SEQUENCE
{
     tunnelledProtocolID  TunnelledProtocol,        -- tunnelled signalling protocol ID
     messageContent       SEQUENCE OF OCTET STRING, -- sequence of entire message(s)
     tunnellingRequired   NULL OPTIONAL,
     nonStandardData      NonStandardParameter OPTIONAL,
     ...
}


END
```

M4.5.4 Description des types et des champs en notation ASN.1

`tunnelledProtocolID` – Contient l'identificateur du protocole de signalisation tunnellisé.

`tunnellingRequired` – Si ce champ est présent, l'appel ne peut être établi que si la tunnellisation est prise en charge.

`messageContent` – Il s'agit du contenu du message de signalisation tunnellisé.

Annexe O

Utilisation des localisateurs uniformes de ressources et du système de noms de domaine

O.1 Domaine d'application

La présente Recommandation définit une méthode permettant de mettre en œuvre des services de communication multimédias dans un réseau en mode paquet arbitraire, dont l'Internet. La mise à profit de tels services, comme le système de dénomination de domaine (DNS, *domain name system*) [O-1] et le service ENUM [O-9], permet de faciliter l'établissement de communications multimédias, notamment en cas d'utilisation du système H.323 sur l'Internet. La présente Recommandation définit les procédures à utiliser dans le cadre du système DNS pour localiser des portiers et des extrémités ainsi que pour traduire les pseudonymes des localisateurs uniformes de ressources (URL) H.323. La présente annexe définit également les paramètres à utiliser avec les localisateurs URL H.323.

O.2 Références normatives

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

[O-1] IETF RFC 1034 (1987), *Domain names – concepts and facilities*.

[O-2] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax.*

[O-3] IETF RFC 2782 (2000), *A DNS RR for specifying the location of services (DNS SRV).*

O.3 Références informatives

A noter que les documents mentionnés ci-dessous sont donnés uniquement à titre d'information et qu'ils ne sont pas indispensables aux fins de l'application de la présente annexe.

[O-4] ITU-T Recommendation E.164 (2005), *The international public telecommunication numbering plan*.

[O-5] IETF RFC 768 (1980), *User datagram protocol*.

[O-6] IETF RFC 793 (1981), *Transmission control protocol*.

[O-7] IETF RFC 1006 (1987), *ISO transport services on top of the TCP: Version 3*.

[O-8] IETF RFC 2806 (2000), *URLs for Telephone Calls*.

[O-9] IETF RFC 2916 (2000), *E.164 number and DNS*.

[O-10] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

O.4 Localisateur URL H.323

Le localisateur uniforme de ressources (URL, *uniform resource locator*) H.323 indique l'emplacement d'une entité ou d'un service H.323 accessible en appliquant les procédures H.323 normalisées. Le localisateur URL H.323 peut comporter des paramètres facultatifs précisant les services et les protocoles de transport permettant de faciliter les communications H.323. Le localisateur URL peut être utilisé de manière appropriée dans des pages web, sous forme de paramètres fournis par l'utilisateur, de résultats d'une procédure ENUM, etc.

Le localisateur URL H.323 se présente sous la forme générale d'un accès utilisateur-serveur *user@hostport* dont les deux parties (c'est-à-dire *user* et *host*) ou une seule de ces parties (c'est-à-dire *user* seulement ou *@host* seulement*)* sont présentes. La partie *user* correspond à un utilisateur ou à un nom de service H.323. Du fait qu'elle constitue une adresse IP numérique légale ou un nom de domaine complet, la partie *host* permet de traduire les adresses en utilisant l'infrastructure du système DNS.

Pour la syntaxe concrète du localisateur URL H.323, voir le § 7.1.4.

La présente annexe définit les paramètres et les procédures d'utilisation du localisateur URL H.323.

O.5 Codage du localisateur URL H.323 dans des messages H.323

En règle générale, les procédures définies dans la présente annexe s'appliquent à un localisateur URL H.323 codé avec son nom de système. Le traitement d'un localisateur URL ou d'un identificateur URI dépourvu de nom de système codé fera l'objet d'un complément d'étude, à moins qu'il ne soit expressément spécifié dans la présente Recommandation.

Une extrémité doit coder le localisateur URL H.323 avec son nom de système dans le champ **url-ID** de l'adresse de pseudonyme **AliasAddress**.

Pendant la procédure de traduction d'une adresse, un portier doit s'efforcer d'extraire un localisateur URL H.323 du champ **url-ID** de l'adresse **AliasAddress**. S'il n'y parvient pas, le portier doit tenter d'extraire un localisateur URL H.323 du champ **h323-ID** de l'adresse **AliasAddress**. Cette dernière est en mesure de prendre en charge l'adressage du localisateur URL même si aucune interface de localisateur URL n'est accessible à un utilisateur d'implémentations d'extrémité antérieures. L'utilisateur sera ainsi en mesure d'acheminer le localisateur URL de destination en l'insérant manuellement avec son nom de système comme s'il s'agissait d'un champ **url-ID** à structure libre.

O.6 Localisateurs URL et identificateurs URI non H.323 dans le contexte de la Rec. UIT-T H.323

Des séquences URL et URI normalisées non H.323 (telles que *mailto*, *tel*, et *sip*) peuvent être intercalées dans des messages H.323.

Les identificateurs URI non H.323 doivent être insérés dans des messages H.323 dans leur intégralité (avec le nom du système) dans le champ **url-ID** du type **AliasAddress**.

Une entité H.323 (un portier, par exemple) doit traiter tout identificateur URI (inséré dans un message H.323) conformément à sa syntaxe et à sa sémantique telles qu'elles ressortent de son nom de système.

O.7 Paramètres du localisateur URL H.323

Le tableau suivant récapitule les paramètres normalisés facultatifs d'un localisateur URL H.323 (*url-parameters*). Les combinaisons de paramètres valables ressortent implicitement du corps du texte de la présente Recommandation.

Paramètre	Description sommaire
utilisateur	Indique que la partie *utilisateur* du localisateur URL H.323 contient un numéro de téléphone
service	Précise le type de service recommandé (c'est-à-dire un des protocoles H.323) à inviter en premier à prendre contact avec l'entité considérée
transport	Indique le protocole de transport à utiliser pour le service susmentionné

O.7.1 Syntaxe ABNF

La présente annexe précise les valeurs normalisées suivantes pour le paramètre **url-parameter** défini au § 7.1.4:

```
user-parameter      =   "user=phone"
service-parameter   =   "service="("ls" | "rs" | "cs" | "be")
transport-parameter =   "transport="("udp" | "tcp" | "h323mux" | "sctp")
```

NOTE – Ces paramètres pourront prendre d'autres valeurs dans les révisions ultérieures de la présente Recommandation.

O.7.2 Paramètre utilisateur

A l'heure actuelle, une seule valeur normalisée est définie pour le paramètre utilisateur *user*, à savoir la valeur *phone* (téléphone).

L'énoncé de la relation d'équivalence *user=phone* (utilisateur=téléphone) indique expressément que la partie utilisateur du localisateur URL H.323 achemine un numéro de téléphone.

Lorsqu'on procédera au codage de la séquence *tel* [O-8] du localisateur URL H.323, on omettra le nom de cette séquence (c'est-à-dire "tel:") et on mettra chacun de ses attributs utilisés (commençant par ";") dans la partie *user* du localisateur URL H.323. A noter que chaque caractère présent dans la séquence *tel* mais non autorisé dans la partie utilisateur du localisateur URL H.323 doit faire l'objet d'un échappement.

O.7.3 Paramètre service

Le paramètre service *service-parameter* peut prendre une des quatre valeurs suivantes: *ls*, *rs*, *cs*, ou *be* correspondant respectivement à la demande de localisation (LRQ) de la voie d'enregistrement, d'admission et de statut (RAS), à la demande d'enregistrement (RRQ) de la voie RAS, aux messages de signalisation d'appel H.225.0 et au protocole inter/intradomaine défini dans l'Annexe G/H.225.0.

La valeur du paramètre service *service-parameter* est celle du service préféré. Durant l'établissement de la connexion, l'extrémité de départ peut s'efforcer d'utiliser d'autres services que celui qui est indiqué dans le paramètre service *service-parameter*.

Si ce paramètre est absent, l'entité H.323 peut essayer successivement les différents services dans l'ordre défini par l'utilisateur. Pour de plus amples précisions, se reporter aux lignes directrices données au § O.9.

O.7.4 Paramètre transport

Les protocoles de signalisation définis dans la présente Recommandation peuvent utiliser différents modes de transport. Les valeurs *udp*, *tcp*, *h323mux*, et *sctp c*orrespondent respectivement aux

protocoles UDP [O-5], TCP [O-6], Annexe E/H.225.0 et SCTP [O-10]. A chaque protocole H.323 correspondent les valeurs par défaut spécifiées dans les Recommandations UIT-T H.323, H.225.0 et leurs Annexes, pour le protocole de transport et l'accès de réception (c'est-à-dire l'identificateur de point TSAP communément admis). Les valeurs par défaut peuvent être spécifiées par le paramètre transport *transport-parameter* et/ou l'accès *port* d'un localisateur URL H.323. Des valeurs différentes des valeurs par défaut doivent être spécifiées par le paramètre transport *transport-parameter* et/ou l'accès *port* d'un localisateur URL H.323.

A noter que l'inclusion du paramètre accès *port* (avec sa valeur par défaut) a une signification particulière. Elle indique à l'entité traductrice que l'accès *host* désigne une entité H.323 précise et non pas un domaine DNS distant contenant des enregistrements de ressources SRV H.323. Pour plus de précisions, voir le § O.9.

La valeur du paramètre transport *transport-parameter* est celle du protocole de transport préféré. Durant l'établissement de la connexion, l'extrémité de départ peut s'efforcer d'utiliser d'autres protocoles de transport que celui qui est spécifié dans le paramètre transport *transport-parameter*.

O.8 Utilisation du localisateur URL H.323

A l'heure actuelle, l'utilisation d'un localisateur URL H.323 répond à deux fins principales: localiser une entité H.323 appelable et localiser un portier auprès duquel une extrémité peut s'enregistrer.

En outre, ENUM [O-9] définit un système d'enregistrement et de consultation des mappages entre les numéros E.164 [O-4] et les services qui leur sont associés. Le système ENUM est implémenté au moyen du système de noms de domaine (DNS) dans lequel les services accessibles sont représentés par les identificateurs URI normalisés [O-2].

D'autres utilisations du localisateur URL H.323 feront l'objet d'un complément d'étude.

O.8.1 Traduction du localisateur URL de destination H.323

La présence d'un localisateur URL H.323 inséré dans une page web ou un autre lien hypertexte signifie qu'un utilisateur ou un service donné sont accessibles à l'aide du protocole H.323.

Toute entité H.323 peut traduire le localisateur URL H.323 en utilisant le système DNS, faisant appel notamment à des extrémités, des portiers ou des éléments frontière dans le cadre de la procédure d'établissement de la communication définie au § 8.1.

Si une extrémité de départ choisit de traduire le localisateur URL de destination, elle doit coder à la fois ce localisateur et l'adresse IP de destination convenablement traduite (conformément au § O.9) dans le champ **destinationInfo** du message ARQ RAS ou dans le champ **destinationAddress** du message Setup et poursuivre la procédure normale d'établissement de la communication H.323. Dans le cas contraire, c'est-à-dire si l'extrémité de départ choisit de ne pas traduire le localisateur URL de destination ou si la consultation du système DNS échoue, l'extrémité doit coder le localisateur URL H.323 conformément au § O.5 dans le champ **destinationInfo** du message ARQ RAS ou dans le champ **destinationAddress** du message Setup et poursuivre la procédure normale d'établissement de la communication H.323.

Si le localisateur URL de destination ne contient que la partie utilisateur *user*, une entité H.323 chargée de traduire ce localisateur doit logiquement procéder comme si la partie accès serveur *hostport* contenait son propre nom de domaine.

Seule une entité traductrice faisant partie du domaine URL (tel que spécifié par l'accès serveur *hostport*) doit interpréter et traiter la partie utilisateur *user* du localisateur URL H.323 selon sa politique locale. Cette politique locale peut notamment être fondée sur les procédures définies par le message RAS H.225.0, l'Annexe G/H.225.0, le protocole LDAP ou la configuration locale.

Si l'accès serveur *hostport* du localisateur URL H.323 est différent de celui du domaine DNS de l'entité traductrice, celle-ci doit d'abord exécuter la procédure DNS telle qu'elle est énoncée au

§ O.9. Ce n'est qu'en cas d'échec de la procédure DNS que l'entité traductrice pourra recourir à une procédure de traduction d'adresse différente, selon sa politique locale.

O.8.2 Localisation d'un portier

La présente Recommandation définit une méthode de recherche d'un portier par l'intermédiaire du message GRQ RAS. En règle générale, cette méthode consiste à envoyer des messages GRQ sans qu'aucune configuration préalable ne soit nécessaire.

Toutefois, la communication statique de l'emplacement d'un portier au niveau même d'une extrémité est très courante. Cela permet d'améliorer la gestion et de mettre en place dans le réseau des systèmes de sécurité souples.

La communication de l'emplacement d'un portier sous la forme d'un localisateur URL H.323 et la prise en charge des procédures DNS de recherche du portier par les extrémités offrent des avantages supplémentaires. En cas d'implémentation d'enregistrements de ressources SRV, des systèmes de redondance et d'équilibrage de charge de portier peuvent être mis en place en transparence jusqu'aux extrémités.

Si une extrémité se voit communiquer aux fins de la localisation de son portier un localisateur URL H.323 de type "h323:@*hostport*" sans paramètres, cette extrémité doit utiliser la valeur de l'accès serveur *hostport* aux fins de la recherche de son portier. Si une extrémité se voit communiquer aux fins de la localisation de son portier uniquement un nom de domaine DNS valide, on part du principe que ce nom de domaine DNS est la valeur de l'accès serveur *hostport* du localisateur URL H.323 susmentionné.

Si une extrémité se voit communiquer, non pas le localisateur URL H.323 nécessaire à la localisation de son portier, mais son propre localisateur URL H.323, elle peut utiliser la valeur de l'accès serveur *hostport* de son propre localisateur URL aux fins de la recherche de son portier.

A cet effet, l'extrémité devrait utiliser la valeur *hostport* communiquée ainsi que les valeurs h323*rs* et *udp* respectivement pour les paramètres **service** implicite et **proto** utilisés pour la procédure de traduction d'adresse définie au § O.9.

Si cette procédure échoue, l'extrémité doit appliquer les procédures normales de recherche du portier définies dans le corps du texte de la présente Recommandation.

O.9 Recours au système DNS pour traduire un localisateur URL H.323 à envoyer à l'adresse IP

La partie serveur *host* du localisateur URL H.323 peut préciser l'un quelconque des éléments suivants:

– l'adresse numérique IP d'une entité H.323;

– le nom DNS d'un serveur qui est une entité H.323;

– le domaine DNS distant contenant des enregistrements de ressources SRV H.323.

Le présent paragraphe définit la procédure de traduction d'adresses applicable à ces trois cas de figure.

Lorsque le serveur *host* contient une adresse IP numérique, il n'y a rien à traduire qui exige de recourir au système DNS. Les messages H.323 doivent être envoyés directement à l'adresse IP indiquée.

Lorsque la partie accès serveur *hostport* du localisateur URL est présente et qu'elle contient un numéro d'accès, cela signifie que le serveur *host* indique une entité H.323 précise (et non pas un domaine DNS contenant des enregistrements de ressources SRV H.323). Cette valeur d'accès *port* est présumée s'appliquer à l'accès auquel les messages H.323 doivent être envoyés. A noter que si l'utilisation de l'accès par défaut se révèle nécessaire, il convient d'insérer le numéro de cet accès de

manière à tenir compte de ce cas. L'entité traductrice doit s'efforcer de retrouver l'enregistrement ou les enregistrements de ressources d'adresses (RR "A"ou RR "AAAA") correspondant au nom de domaine spécifié par le serveur *host*. Si la recherche porte sur plusieurs enregistrements, l'entité traductrice doit en sélectionner un seul, conformément à sa politique locale (voir également le § O.10.1). Les messages H.323 doivent être envoyés à l'adresse IP extraite (et éventuellement sélectionnée) et à l'accès spécifié par le localisateur URL.

Quand la partie accès serveur *hostport* du localisateur URL est présente sans toutefois contenir aucun numéro d'accès, cela laisse entendre que le serveur *host* indique très vraisemblablement un domaine DNS contenant des enregistrements de ressources SRV H.323. L'entité traductrice devrait s'efforcer de localiser l'entité considérée en procédant à une recherche séquentielle d'enregistrements SRV dans un sous-ensemble des services H.323 possibles (c'est-à-dire *h323ls*, *h323rs*, *h323be* et *h323cs*) et de leurs éventuels protocoles de transport correspondants (c'est-à-dire *udp*, *tcp* et *h323mux*) conformément à la procédure définie au § O.10.4. Ce sous-ensemble doit être adapté aux capacités de l'entité traductrice et à la finalité de la procédure (c'est-à-dire localiser un portier, un élément frontière extérieur ou une destination). Si le paramètre service *service-parameter* du localisateur HRL H.323 est présent ou si le *service* SRV (*h323rs*, par exemple) est spécifié, la consultation des enregistrements SRV doit commencer dans l'ordre indiqué par cette valeur. Dans le cas où le paramètre service *service-parameter* n'est pas spécifié, l'entité traductrice peut rechercher l'un quelconque ou la totalité des types d'enregistrements SRV dans n'importe quel ordre.

Pour chaque recherche fructueuse, il convient de consulter une nouvelle fois le système DNS pour rechercher les enregistrements de ressources d'adresses. Si cette recherche est fructueuse, les messages H.323 doivent être envoyés à l'adresse IP extraite et sélectionnée et à un numéro d'accès par défaut (correspondant au protocole de transport).

Si la procédure de recherche d'enregistrements de ressources SRV n'est pas implémentée ou si elle échoue, l'entité traductrice peut essayer de rechercher l'enregistrement ou les enregistrements de ressources d'adresses correspondant au nom de domaine indiqué par l'accès serveur *hostport*, même si l'accès *port* n'a pas été précisé. Si la recherche porte sur plusieurs enregistrements, l'entité traductrice doit en sélectionner un seul, conformément à sa politique locale (voir aussi le § O.10.1). Si la recherche est fructueuse, les messages H.323 doivent être envoyés à l'adresse IP extraite (et éventuellement sélectionnée) et à un numéro d'accès par défaut correspondant.

O.10 Utilisation d'enregistrements de ressources SRV du système DNS

O.10.1 Modalités d'application

L'utilisation d'enregistrements de ressources SRV du système DNS (RFC 2782 [O-3]) permet de publier une adresse (c'est-à-dire un identificateur URI) correspondant à un service donné (*Service*) accessible par un protocole spécial (*Proto*). "Les enregistrements de ressources SRV permettent aux gestionnaires d'utiliser plusieurs serveurs pour un même domaine [DNS], de déplacer les services d'un serveur à un autre commodément, et de désigner certains serveurs comme serveurs principaux pour un service et d'autres comme serveurs de secours."

Dans les paragraphes qui suivent, la présente annexe définit les noms symboliques des services H.323 et des protocoles de transport H.323 qui doivent être enregistrés auprès de l'Autorité chargée de l'assignation des numéros Internet (IANA, *Internet assigned numbers authority*) et qui sont nécessaires pour utiliser les enregistrements de ressources SRV du système DNS. La présente annexe définit également les procédures normatives applicables à l'utilisation d'enregistrements de ressources SRV dans les systèmes H.323.

O.10.2 Enregistrement auprès de l'IANA

La présente spécification définit les noms symboliques suivants à utiliser dans le champ *Service* de l'enregistrement SRV conformément à la norme RFC 2782 [O-3].

Service	Nom	Signification
h323ls	Service de localisation	Entité H.323 prenant en charge la procédure LRQ H.225.0
h323rs	Service d'enregistrement	Entité H.323 prenant en charge la procédure de demande d'enregistrement RRQ H.225.0 (c'est-à-dire un portier qui accepte l'enregistrement d'extrémités)
h323cs	Signalisation d'appel	Entité H.323 qui assure la signalisation d'appel H.225.0
h323be	Elément frontière	Entité H.323 prenant en charge la communication comme indiqué dans l'Annexe G/H.225.0

La présente spécification définit les noms symboliques suivants à utiliser dans le champ *Proto* de l'enregistrement SRV conformément à la Norme RFC 2782 [O-3].

Nom symbolique	Signification
udp	Protocole UDP (protocole datagramme d'utilisateur) défini dans la Norme RFC 768 "User datagram protocol" [O-5]
tcp	Format de paquet TPKT [O-7] utilisant le protocole TCP [O-6] conformément à l'Appendice IV/H.225.0
sctp	Protocole SCTP défini dans la Norme RFC 2960 [O-10]
h323mux	Tel que défini dans l'Annexe E, "Cadre général et protocole d'échange pour le transport multiplexé de la signalisation d'appel"

O.10.3 Données contenues dans les enregistrements de ressources SRV

Comme indiqué dans la Norme RFC 2782 [O-3], le code de type du système DNS pour les enregistrements de ressources SRV est le 33, dont le format est le suivant:

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

Tous les champs doivent contenir les données indiquées dans la Norme RFC 2782.

Les champs *Service* et *Proto* doivent avoir l'un des noms symboliques définis ci-dessus. Le champ *Port* doit prendre une des valeurs d'un accès de réception du serveur H.323, défini par une cible *Target*.

Si différentes formes d'accès H.323 (c'est-à-dire des combinaisons des champs *Service* et *Proto*) sont disponibles pour le domaine DNS, chacune d'entre elles doit être publiée séparément dans un enregistrement SRV distinct.

Les champs *Priority* et *Weight* doivent être utilisés pour indiquer les services préférés dans le cadre de la politique locale.

O.10.4 Recherche et traitement d'enregistrements de ressources SRV

Cette procédure ne définit pas les priorités de traitement entre les services (*Service*s) ou les protocoles (*Proto*s) H.323.

Elle prend pour seuls paramètres de départ une valeur *Service* H.323 donnée et une valeur *Proto* donnée. La consultation sous la forme of _service.* n'est pas autorisée.

Si aucun enregistrement SRV n'est retrouvé, la procédure échoue.

Le traitement local des enregistrements SRV retrouvés doit être effectué selon l'algorithme de sélection utilisant le champ *Priority*, défini dans la Norme RFC 2782, ou selon l'algorithme de sélection utilisant le champ *Weight*, défini dans cette même norme. Les valeurs des champs *Priority* et *Weight* de différents services ou protocoles H.323 ne doivent pas être comparées.

Cette procédure aboutit à l'établissement d'une liste ordonnée d'enregistrements de ressources SRV (assortis ou non d'enregistrements de ressources d'adresses correspondants éventuellement indiqués dans la section Données additionnelles des enregistrements de ressources SRV).

O.10.5 Exemple 1

L'exemple donné ici représente un fragment de zone DNS ou de fichier de domaine DNS pour **example.com**. Tous les serveurs H.323 utilisent en réception (écoute) des points d'accès au service de transport (TSAP) communément admis. Il existe deux portiers en place dans ce domaine. Le portier local **local-gatekeeper**, qui assure des services d'enregistrement, peut être "localisé" par ses extrémités locales. Depuis l'extérieur, les services H.323 sont accessibles via le portier externe external-gatekeeper par consultation des services de signalisation d'appel du domaine. En outre, le portier externe external-gatekeeper traduira les adresses de ses extrémités en répondant aux demandes LRQ émanant de l'extérieur de son domaine.

La séparation fonctionnelle entre les deux portiers peut être purement logique ou utile dans des environnements "NATted" dans lesquels les deux portiers représentent l'adressage IP local et externe.

```
$ORIGIN example.com.
_h323rs._udp            SRV 0 1 2517 local-gatekeeper.example.com.
_h323ls._udp            SRV 0 1 2517 external-gatekeeper.example.com.
_h323cs._tcp            SRV 0 1 1720 external-gatekeeper.example.com.
local-gatekeeper        A   172.30.79.11
external-gatekeeper     A   172.30.79.12
; AUCUN accès H.323 selon l'Annexe E/H.323 n'est pris en charge
*._h323mux              SRV  0 0 0 .
; AUCUN autre service n'est pris en charge (y compris l'élément frontière H.323)
*._tcp                  SRV  0 0 0 .
*._udp                  SRV  0 0 0 .
```

O.10.6 Exemple 2

L'exemple donné ici représente un fragment de zone DNS ou de fichier de domaine DNS pour **example.com**. Tous les serveurs H.323 utilisent en réception (écoute) des points TSAP communément admis. Le service H.323 est assuré par l'intermédiaire d'un élément frontière et de portiers. Aucune priorité n'est définie ou présumée entre l'élément frontière et les portiers. La priorité est déterminée en fonction de l'application. Ainsi, un service de haute qualité purement vocal est assuré par l'intermédiaire de l'élément frontière alors qu'un service de visioconférence H.323 est assuré par l'intermédiaire des portiers.

Un téléphone vocal H.323 résidant dans un domaine aura le localisateur URL suivant: **h323:my-alias@example.com;service=be**. Dans ce cas, on commencera par procéder, avec succès, à une consultation pour déterminer **_h323be._udp**. A noter que l'on peut aussi procéder à une consultation pour déterminer **_h323cs._tcp**.

Un service de visioconférence, assuré par un pont de conférence MCU (ou unité de commande multipoint) H.323 dans une zone de portier principal **main-gatekeeper** ou de portier secondaire **secondary-gatekeeper** sera publié sous la forme **h323:conference-alias@example.com; service=cs**. Cela est dû au fait que la recherche des enregistrements SRV correspondant à **_h323cs._tcp** sera effectuée à l'aide du paramètre service *service-parameter*. En outre, en cas d'utilisation du champ **Weight**, le portier principal **main-gatekeeper** n'est accessible de fait qu'à 75% par rapport au portier secondaire **secondary-gatekeeper** si les deux portiers sont en service.

```
$ORIGIN example.com.
_h323be._udp            SRV 0 1 2099 border-element.example.com.
_h323cs._tcp            SRV 0 1 1720 secondary-gatekeeper.example.com.
_h323cs._tcp            SRV 0 3 1720 main-gatekeeper.example.com.
border-element          A   172.30.79.10
main-gatekeeper         A   172.30.79.11
secondary-gatekeeper    A   172.30.79.12
; AUCUN accès H.323 selon l'Annexe E/H.323 n'est pris en charge
*._h323mux              SRV  0 0 0 .
; AUCUN autre service n'est pris en charge (y compris le service de localisation H.323)
*._tcp                  SRV  0 0 0 .
*._udp                  SRV  0 0 0 .
```

Annexe P

Transfert des signaux de modems sur les systèmes H.323

P.1 Domaine d'application

La présente annexe a pour objet de définir les procédures de transfert des signaux de modems sur un réseau H.323. Les procédures de signalisation décrivent l'utilisation de systèmes H.245 (y compris des procédures de connexion rapide et de connexion rapide étendue) et les événements de signalisation d'état destinés à indiquer les capacités des points d'extrémité, à ouvrir et à fermer des canaux logiques, et à signaler des changements d'état. Les entités H.323 qui prennent en charge le transfert de signaux de modems sur des réseaux IP devront offrir cette fonctionnalité conformément à la présente annexe.

P.2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives existantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[P-1] Recommandation UIT-T V.150.1 (2003), *Modems sur réseaux à protocole Internet: procédures pour la connexion de bout en bout des équipements de terminaison de circuits de données de la série V*.

[P-2] Recommandation UIT-T H.460.6 (2002), *Fonctionnalité de connexion rapide étendue*.

[P-3] IETF RFC 2198 (1997), *RTP Payload for Redundant Audio Data*.

P.3 Définitions

La présente annexe définit les termes suivants:

P.3.1 modem sur IP: transport de signaux de modems sur un réseau IP tel qu'il est décrit dans la Rec. UIT-T V.150.1.

P.3.2 relais modem: transport de données de modems sur un réseau en mode paquet utilisant une terminaison de modem aux points d'accès du réseau.

P.3.3 événement de signalisation d'état: messages d'événements codés en RTP coordonnant la commutation entre différents états de média tels qu'ils sont définis dans l'Annexe C/V.150.1.

P.3.4 données en bande vocale: transport de signaux de modems sur une voie audio d'un réseau en mode paquet avec codage pour signaux de modems.

P.4 Abréviations

La présente annexe utilise les abréviations suivantes:

FEC correction d'erreur directe (*forward error correction*)

MoIP modem sur les réseaux à protocole Internet (*modem over IP*)

MPS flux de charge utile multiple (*multiple payload stream*)

OLC ouverture de canal logique (*open logical channel*)

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

SPRT transport relais de paquet simple (*simple packet relay transport*)

SSE événement de signalisation d'état (*state signalling event*)

VBD données dans la bande vocale (*voice band data*)

P.5 Introduction

Les systèmes H.323 sont très utilisés dans le monde pour l'acheminement de signaux audio, de la vidéo et de données sur des réseaux en mode paquet dont les réseaux IP. Une des applications des systèmes H.323 permet le transit d'appels téléphoniques entre deux réseaux indépendants à commutation de circuits ou deux points du même réseau commuté. Dans une telle application, l'appel est initié dans un réseau commuté et acheminé vers une passerelle H.323. Cette passerelle établit ensuite la communication avec une passerelle distante qui, à son tour, achemine l'appel vers un réseau commuté.

Dans ces applications, il est souhaitable que les appels entre passerelles n'acheminent pas uniquement des signaux audio ou de la vidéo, mais également des données. Dans l'Annexe D, l'on a présenté les procédures de signalisation requises pour faciliter le transport de données de télécopie sur un réseau IP entre passerelles et autres dispositifs. La présente annexe a pour objet de spécifier les procédures permettant d'acheminer des données de modems sur un réseau IP entre deux passerelles.

La Figure P.1 représente graphiquement les passerelles H.323 transportant des signaux de modems entre modems sur un réseau IP.

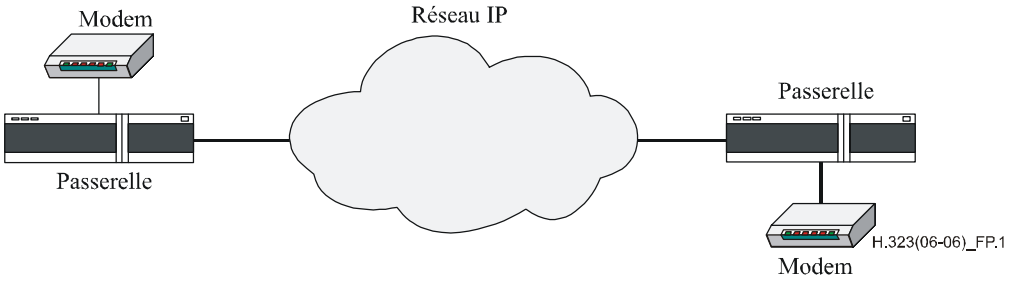


Figure P.1/H.323 – Application type de modems sur IP

La Rec. UIT-T V.150.1 définit les procédures générales permettant d'acheminer des signaux de modems sur des réseaux IP entre deux passerelles et devrait être lue conjointement avec la présente annexe. Alors que la Rec. UIT-T V.150.1 ne définit pas le transport de signaux de modems dans le

cadre d'un protocole de commande des appels particulier, la présente annexe définit les procédures qui sont nécessaires et particulières aux systèmes de la présente Recommandation.

Sauf indication contraire expresse, les références aux points d'extrémité H.323 figurant dans le reste de la présente annexe sont des points d'extrémité qui sont capables de transporter des signaux de modems sur un réseau IP.

P.6 Indication des capacités

Comme à l'accoutumée, les points d'extrémité indiquent leurs capacités en utilisant le message **terminalCapabilitySet** figurant dans la Rec. UIT-T H.245. Les capacités qui revêtent une importance particulière et qui sont nécessaires à l'utilisation de modems sur les réseaux IP sont les capacités d'application de données MoIP et SSE (définies dans l'Annexe F/V.150.1), la charge utile RTP pour la capacité événements de téléphonie audio (voir § B.2.2.13/H.245), et la capacité audio **vbd**. Les capacités **fecCapability** et/ou **redundancyEncodingCapability** peuvent être prises en charge pour améliorer la fiabilité du canal acheminant des données dans la bande vocale (VBD, *voice band data*).

Les points d'extrémité pourront également indiquer la prise en charge pour **multiplePayloadStream** flux de charge utile multiple (MPS, *multiple payload stream*) dans l'ensemble des capacités transmises à l'autre point d'extrémité.

Les définitions des capacités MoIP et SSE figurent dans l'Annexe F/V.150.1.

Conformément à la Rec. UIT-T V.150.1, la liste des codecs pris en charge en tant que codecs VBD devra inclure les codecs en loi μ et en loi A G.711. En outre, les points d'extrémité H.323 devront prendre en charge les codages G.711 pour les données dans la bande vocale à 64 kbit/s et, à titre facultatif, à 56 kbit/s.

P.7 Etablissement d'appel

Etant donné que le facteur temps est critique pour la signalisation de modems, le point d'extrémité appelant devrait utiliser la fonctionnalité de connexion rapide pour offrir un ou plusieurs canaux permettant de faire fonctionner un modem MoIP. Le point d'extrémité appelant devrait également inclure ses capacités de terminal dans le champ **parallelH245Control** afin de faciliter la négociation rapide des canaux MoIP.

De même, le point d'extrémité appelé devra émettre une réponse aussi vite que possible en connexion rapide. Cette réponse pourra être l'acceptation ou le refus des canaux offerts. En outre, si le champ **parallelH245Control** est présent dans le message Setup, le point d'extrémité appelé devra confirmer la réception de ces informations, ainsi qu'il est indiqué au § 8.2.4.

Si, pour une raison ou une autre, le moyen de communication ne peut être négocié au moyen d'une fonctionnalité de connexion rapide, les points d'extrémité procéderont aussi rapidement que possible à la signalisation du canal logique via le canal de commande H.245. Là encore, l'opérateur doit tenir compte du fait que le facteur temps est critique pour le mode MoIP et est invité à prévoir cette signalisation bien avant la transmission du message Connect.

P.8 Signalisation du canal logique

Il existe cinq types de flux qui sont particulièrement importants pour un point d'extrémité prenant en charge le mode MoIP. A savoir les flux audio, les flux de données dans la bande vocale, les événements de téléphonie audio RTP, les événements de signalisation d'état (SSE, *state signalling event*) et les flux SPRT. Un point d'extrémité devra regrouper en mode logique les flux nécessaires pour la procédure MoIP via un canal MPS. Il existe cependant une exception: le flux SPRT pourra être signalé en tant que canal distinct et associé au canal audio/de données en bande vocale au moyen du champ **associatedSessionID**.

Dans le cadre d'une session MoIP, le canal MPS qui contient les flux audio et/ou de données dans la bande vocale et autres flux pour le mode MoIP devrait être considéré comme la session audio primaire. A ce titre, l'élément **sessionID** H.245 devrait être positionné sur 1. Toutefois, les points d'extrémité peuvent librement utiliser des valeurs d'identification de session dynamiques, ainsi que le prescrit la Rec. UIT-T H.245.

S'il n'existe pas de limitations strictes du nombre de flux pouvant être contenus dans tout canal MPS, le canal MPS utilisé pour le mode MoIP contiendra zéro ou plusieurs flux audio, un ou plusieurs flux de données dans la bande vocale, pas plus d'un flux SSE et pas plus d'un flux SPRT. Si le flux SPRT est ouvert en tant que canal distinct, le canal MPS n'inclura pas en plus un flux SPRT. En outre, il doit y avoir différents types de charge utile pour les flux audio, VBD, SSE et SPRT dans le canal MPS. Il est possible que plus de quatre types de charge utile soient utilisés pour les flux audio, VBD, SSE et SPRT. Par conséquent, si le flux de données dans la bande vocale est protégé par une correction d'erreur directe (FEC, *forward error correction*) et si ces paquets FEC sont contenus dans un paquet de codage à redondance, il se pourra qu'il n'y ait pas uniquement une valeur de type de charge utile pour le flux de données dans la bande vocale, mais trois: une utilisée dans l'en-tête de protocole RTP pour indiquer que le paquet contient une charge utile codée avec redondance, une pour la charge utile primaire (les données dans la bande vocale), et une pour les données FEC transportées à titre de codage secondaire.

Pour protéger à titre facultatif un flux de données dans la bande vocale, un point d'extrémité pourra utiliser la correction d'erreur directe et/ou le codage à redondance. Un flux qui utilise la correction d'erreur directe sera signalé par le champ **fec** de la structure **DataType** à l'intérieur de la structure **MultiplePayloadStreamElement**. Un flux qui utilise un codage à redondance sera signalé par le champ **redundancyEncoding** dans la structure **DataType** à l'intérieur de la structure **MultiplePayloadStreamElement**.

Pour illustrer l'utilisation de flux MPS en mode MoIP, prenons un canal OLC ayant un flux audio G.729, un flux de données dans la bande vocale G.711, loi A, qui est protégé par un codage à redondance, un flux SSE et un flux SPRT. Le protocole **OpenLogicalChannel** aurait une composition essentiellement similaire à celle qui est décrite dans l'exemple abrégé ci-dessous:

```
{
     forwardLogicalChannelNumber 1,
     forwardLogicalChannelParameters {
          dataType : multiplePayloadStream {
               element {
                    dataType : audioData : g729 2
               },
               element {
                    dataType : redundancyEncoding {
                         primary {
                              dataType : audioData : vbd : g711Alaw64k 160
                         },
                         secondary {
                              dataType : audioData : vbd : g711Alaw64k 160
                              payloadType 97 -- Type de charge utile pour le
                                             -- codage à redondance
                         }
                    },
                    payloadType 101     -- Type de charge utile pour
                                        -- le paquet RFC 2198
               },
               element {
                    dataType : data {
                         application : genericDataCapability {
                              -- Capacité SSE
                              capabilityIdentifier : standard {
```

```
                              itu-t(0) recommendation(0) v(22) 150 sse(1)
                         },
                         nonCollapsing {
                              {
                                   parameterIdentifier : standard 0,
                                   parameterValue : octetString "3,5"
                                        -- Séquence, séparée par une virgule,
                                        -- d'événements pris en charge
                                        -- (illustration de la syntaxe de la
                                        -- séquence qui n'est pas
                                        -- nécessairement une liste
                                        -- appropriée)
                              },
                              {
                                   parameterIdentifier : standard 1,
                                   parameterValue : logical
                              }
                         }
                    }
               },
               payloadType 102     -- Type de charge utile pour
                                   -- les paquets SSE
          },
          element {
               dataType : data {
                    application : genericDataCapability {
                         -- MoIP capability
                         capabilityIdentifier : standard {
                              itu-t(0) recommendation(0) v(22) 150 moip(0)
                              major-version-one(1) minor-version-one(1)
                         },
                         nonCollapsingRaw '0000'H
                              -- Cette valeur est donnée uniquement
                              -- à titre indicatif et ne constitue
                              -- pas une valeur valide
                    }
               },
               payloadType 103     -- Type de charge utile pour
                                   -- les paquets MoIP
          }
     }
},
multiplexParameters : h2250LogicalChannelParameters {
     sessionID 1
}
}
```

P.8.1 Connexion rapide étendue

La fonctionnalité de connexion rapide étendue [P-2] doit être utilisée pour reconfigurer des canaux logiques, étant donné qu'elle est bien plus rapide qu'un échange de séries de messages H.245. Si un point d'extrémité doit opérer une transition entre un mode de données audio et un mode MoIP et qu'il n'est pas actuellement doté d'un canal ouvert permettant une utilisation en mode MoIP, il doit commencer par tenter de reconfigurer les canaux en utilisant la fonctionnalité de connexion rapide étendue.

La fonctionnalité de connexion rapide étendue devrait également constituer le premier choix lors de la signalisation du canal logique même lorsque les canaux existants prennent en charge le mode MoIP. Ainsi, si un point d'extrémité souhaite basculer d'un codec audio G.729 à l'intérieur d'un flux MPS à un codec audio G.723.1, il doit tenter de reconfigurer les canaux logiques par le biais de la fonctionnalité de connexion rapide étendue, au lieu d'utiliser la signalisation H.245.

P.8.2 Signalisation H.245

La signalisation du canal logique H.245 au moyen du canal de commande H.245 peut être employée pour configurer ou reconfigurer des flux de médias, si nécessaire. Des points d'extrémité dotés de la capacité MoIP prendront en charge une tunnellisation H.245 lorsqu'il sera nécessaire d'utiliser un canal de commande H.245. Toutefois, il est entendu que la prise en charge de la tunnellisation H.245 ne permet pas de garantir qu'elle sera utilisée et une connexion distincte pourra se révéler nécessaire, quoiqu'elle soit découragée.

Si la signalisation de l'ouverture de nouveaux canaux n'est pas à proprement parler un problème pour les points d'extrémité H.323, il peut arriver cependant que deux points d'extrémité tentent d'ouvrir indépendamment des canaux, donnant ainsi lieu à une configuration incompatible. Pour résoudre le problème, le dispositif maître rejettera les propositions OLC du dispositif esclave en invoquant le motif **masterSlaveConflict**. Le dispositif maître enverra ensuite un message **RequestMode** au dispositif esclave pour proposer un mode de fonctionnement compatible.

Si un point d'extrémité constate qu'il est nécessaire de changer de mode de fonctionnement, c'est-à-dire, par exemple, de passer du mode uniquement audio à un mode prenant en charge la fonction MoIP, il enverra un message **RequestMode** à l'autre extrémité. Prenons ainsi l'exemple de deux points d'extrémité qui ouvrent une voie audio G.729 dans chacune des directions; puis, l'un des deux points d'extrémité détermine qu'il convient de changer de mode de fonctionnement pour passer du mode audio au mode MoIP. Le point d'extrémité enverra un message **RequestMode** au moyen du canal de commande H.245 en indiquant le mode de fonctionnement souhaité. Le point d'extrémité récepteur répondra, selon le cas, par un message de confirmation ou de rejet, mais elle devra tout mettre en œuvre pour accepter le mode de fonctionnement demandé. Les points d'extrémité devront échanger des messages d'une manière analogue à celle qui est décrite dans la Figure P.2. Dans la mesure du possible, les messages devront être échangés en parallèle pour réduire les retards dans le passage d'un mode à l'autre.

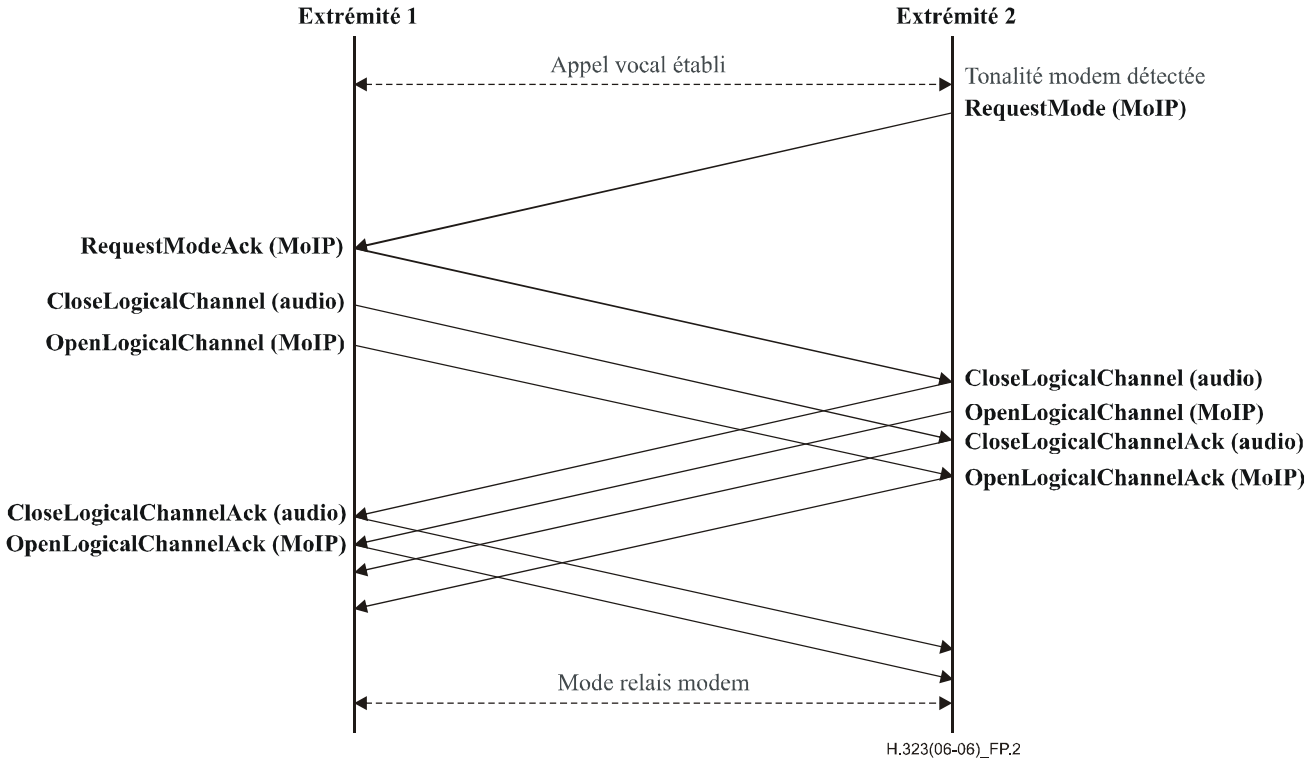


Figure P.2/H.323 – Transition effective entre un mode audio et un mode MoIP

Annexe Q

Télécommande de la caméra distante au moyen des protocoles H.281/H.224

Q.1 Domaine d'application

La présente annexe a pour objet de définir un protocole de télécommande de caméra fondé sur les Recommandations UIT-T H.281/H.224. Elle permet en outre à un point d'extrémité H.323 de faire fonctionner une application H.224 quelconque au moyen du protocole IP/UDP/RTP/H.224 défini dans la présente annexe.

Q.2 Références normatives

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

[Q-1] Recommandation UIT-T H.224 (2005), *Protocole de commande en temps réel pour les applications simplex utilisant les canaux de données à faible vitesse, à grande vitesse et à protocole multicouche définis dans la Recommandation H.221*.

[Q-2] Recommandation UIT-T H.281 (1994), *Protocole de télécommande de caméra pour les visioconférences utilisant la couche H.224*.

[Q-3] Recommandation UIT-T T.140 (1998), *Protocole de conversation en mode texte pour application multimédia*.

Q.3 Introduction

Le protocole décrit dans cette annexe peut être utilisé afin de prendre en charge la télécommande de caméra (FECC, *far-end camera control*), dans la couche de la présente Recommandation au moyen de la pile de protocoles IP/UDP/RTP/H.224/H.281. Ce protocole prend en charge aussi bien les scénarios point à point que les scénarios multipoint.

Cette méthode est utilisable en tant que système FECC "simple", lorsque les caractéristiques plus évoluées des spécifications H.282/H.283 ne sont pas nécessaires.

Cette méthode doit être utilisée pour la télécommande FECC par les passerelles H.320-H.323 et H.324-H.323 lorsque les points d'extrémité H.320 ou H.324 ne prennent pas en charge le protocole de la Rec. UIT-T H.282.

Les prescriptions ci-dessous sont applicables uniquement dans le cas où le protocole décrit dans la présente annexe a été choisi, selon les procédures normales de la Rec. UIT-T H.245.

L'utilisation de toute application H.224 au moyen du protocole IP/UDP/RTP/H.224 défini dans la présente annexe est autorisée. La seule autre application H.224 actuellement normalisée est la Rec. UIT-T T.140.

Q.4 Protocole de télécommande de caméra

Q.4.1 Généralités

Ce protocole repose sur l'exécution par un équipement Rec. UIT-T H.224 du protocole Rec. UIT-T H.281 dans une voie RTP/UDP.

Sur des réseaux de transport IP, la structure par octet du protocole H.224 doit être identique à celle de la Figure 2/H.224, excepté le fait que les bits de remplissage, les fanions et les séquences de contrôle de trame HDLC doivent être omis. La totalité du contenu résiduel de chaque trame doit être placée dans un paquet RTP unique.

La mention dans le protocole UIT-T H.224 des canaux de données à faible vitesse du protocole UIT-T H.221 doit être considérée comme se rapportant à la voie logique H.224 décrite dans la présente annexe. Les exigences de la Rec. UIT-T H.224 en matière de délai de transmission maximal doivent être observées, et la voie logique H.224 étant considérée comme fonctionnant à 4800 bit/s indépendamment du débit binaire réel de la voie.

Ce protocole doit utiliser le protocole de transport en temps réel dans une voie logique H.245 non fiable unidirectionnelle. La valeur de la charge utile RTP doit être de type accès dynamique (dynamic). Le champ affecté au descripteur de charge utile du paramètre H.245 **RTPPayloadType** doit utiliser l'identificateur H.224 Object ID.

Le numérotage des terminaux doit suivre les procédures définies dans la Rec. UIT-T H.243 afin de prendre en charge la couche de liaison de données en multipoint. L'identification univoque de chacun des terminaux dans une conférence exige l'utilisation du couple d'adresses MCU/terminal <M><T>. L'adresse de destination spéciale <0><0> sert d'adresse de diffusion. L'adresse d'origine spéciale <0><0> indique que l'expéditeur ne connaît pas son adresse. Une adresse dont le numéro de terminal est mis à la valeur 0 désigne le contrôleur multipoint. Par exemple, <n><0> désigne le contrôleur multipoint numéro n.

Dans une communication point à point, et lorsque deux terminaux seulement sont en jeu, alors les terminaux n'ont pas d'adresse <M><T>. Dans ce cas, les adresses d'origine et de destination <M><T> doivent toujours être <0><0>.

Dans une conférence centralisée une voie H.224 doit être ouverte entre chaque terminal et le contrôleur multipoint (MC). Lorsqu'un terminal envoie un paquet H.224 le contrôleur multipoint doit adresser le paquet au terminal de destination, soit en retransmettant chaque paquet à tous les autres terminaux connectés, soit en retransmettant de façon sélective chaque paquet uniquement au terminal de destination. Le choix de la méthode à utiliser est laissé à l'initiative du constructeur du contrôleur multipoint.

Dans une conférence multidiffusion décentralisée, chaque terminal doit multidiffuser le paquet de télécommande FECC vers tous les autres terminaux. Le contrôleur MC n'est pas associé à la retransmission des paquets. Les numéros de terminal selon la Rec. UIT-T H.243 doivent être utilisés pour identifier les terminaux d'origine et de destination.

Dans une conférence multidiffusion décentralisée, chaque terminal doit utiliser une voie logique distincte vers chaque terminal éloigné auquel il doit adresser des paquets H.224.

Q.4.2 Passerelles H.320 vers H.323

Les passerelles H.320-H.323 doivent introduire et supprimer des fanions HDLC, des bits de remplissage HDLC et des séquences de contrôle de trame HDLC, le cas échéant dans chaque sens, de façon à ce que le flux binaire du côté H.320 soit conforme à la Rec. UIT-T H.224, le flux binaire côté H.323 étant conforme aux dispositions ci-dessus.

Q.4.3 Passerelles H.324 vers H.323

Les passerelles H.324-H.323 doivent introduire et supprimer des fanions HDLC, des bits de remplissage HDLC et des séquences de contrôle de trame HDLC, le cas échéant dans chaque sens, de façon à ce que le flux binaire du côté de la Rec. UIT-T H.324 soit conforme à la Rec. UIT-T H.224, le flux binaire côté H.323 étant conforme aux paragraphes ci-dessus.

Q.4.4 Signalisation H.245

L'utilisation de ce protocole doit être signalisée par la partie **GenericCapability** de la séquence **DataApplicationCapability** selon la Rec. UIT-T H.245. La capacité générique pour l'application H.224, décrite dans la Rec. UIT-T H.224 doit être utilisée. Cette donnée doit être placée dans la partie **receiveAndTransmitDataApplicationCapability** de la sélection **Capability**.

Ce protocole ne doit pas être signalé dans les parties **receiveDataApplicationCapability** ou **transmitDataApplicationCapability** de l'option **Capability**.

Q.5 Information d'en-tête RTP

Les champs ci-dessous doivent être remplis dans l'en-tête RTP:

V:	2
M:	0 NA
PT:	numéro envoyé dans le champ dynamicRTPPayloadType
Numéro de séquence:	zone remplie, augmentée d'un octet par paquet RTP envoyé
Horodateur:	fréquence d'horloge de 8 kHz
SSRC:	source de synchronisation

Annexe R

Méthodes d'amélioration de la robustesse pour les entités H.323

R.1 Introduction et domaine d'application

La présente annexe précise les méthodes applicables aux entités H.323 pour les doter d'une résistance ou d'une tolérance à l'égard d'un ensemble donné de défaillances. Des méthodes de rétablissement des voies de signalisation d'appel (Rec. UIT-T H.225.0) et de signalisation de commande d'appel (Rec. UIT-T H.245) sont spécifiées. La signalisation RAS (Rec. UIT-T H.225.0) n'implique pas une connexion; aussi la question du rétablissement, impliquant un enregistrement auprès d'un portier de remplacement, est-elle traitée dans un autre document et n'est-elle pas spécifiée dans la présente annexe. Le rétablissement des relations de service selon l'Annexe G A étudier.

Les appels de la présente Recommandation exigent la coopération d'au moins deux entités H.323. Les informations d'état de l'appel sont réparties entre les différentes entités impliquées. La signalisation d'appel peut dépendre de connexions permanentes établies entre certaines des entités impliquées. Si une entité quelconque a une défaillance sans être associée à une entité homologue de secours, l'établissement de nouveaux appels peut s'avérer impossible. Si une entité quelconque liée à un appel activé tombe en panne et n'est pas associée à une entité de secours ou si celle-ci n'est pas dotée d'un mécanisme permettant de rétablir suffisamment d'informations d'état de l'appel, la poursuite de l'appel peut également s'avérer impossible. Bien que la présente Recommandation vise à faciliter la mise au point de systèmes fiables, la description des mécanismes proposés à cet effet est répartie dans toute la présente annexe et les procédures d'utilisation correspondantes sont rares voire inexistantes.

La présente annexe décrit deux autres méthodes constituées d'ensembles de mécanismes et de procédures d'utilisation permettant de mettre au point des systèmes dont le rétablissement est possible à partir d'un ensemble important de défaillances spécifiées. La première est mieux adaptée

aux systèmes à petite échelle, utilise des entités plus simples et rétablit une quantité moindre d'informations d'état de l'appel; l'autre méthode convient à des systèmes de plus grande taille et permet de rétablir autant d'informations d'état de l'appel que nécessaire, mais exige l'utilisation d'entités plus complexes. Les deux méthodes en question ont plusieurs mécanismes en commun et peuvent être utilisées simultanément dans différentes parties d'un système.

R.2 Références normatives

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

[R-1] Recommandation UIT-T H.225.0 (2006), *Protocoles de signalisation d'appel et paquétisation des flux monomédias pour les systèmes de communication multimédias en mode paquet*.

[R-2] Recommandation UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base*.

[R-3] Recommandation UIT-T X.680 (2002), *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base*.

R.3 Définitions

Outre les termes définis dans le corps principal de la présente Recommandation, les termes suivants sont utilisés:

R.3.1 entité de secours ou entité homologue de secours: entité homologue d'une entité capable d'assurer les fonctions de l'entité correspondante en cas de défaillance de celle-ci.

R.3.2 entités homologues: deux entités de même type dans un système H.323, par exemple deux portiers. Deux entités peuvent fonctionner en coopération à l'occasion d'un appel (par exemple, portiers d'origine et de destination en cas de signalisation d'appel acheminée par portier) ou assurer mutuellement une fonction de secours.

R.3.3 méthodes d'amélioration de la robustesse: procédures et mécanismes qui permettent d'obtenir un rétablissement après la défaillance d'une ou plusieurs entités H.323. L'importance du rétablissement varie selon les méthodes considérées d'amélioration de la robustesse et peut comporter la conservation des appels activés dans un état stable ou simplement la capacité d'établir de nouveaux appels. Les méthodes décrites dans la présente annexe permettent généralement de conserver les appels activés.

R.3.4 entité voisine de signalisation: autres entités avec lesquelles une entité particulière a établi des connexions directes de signalisation d'appel ou de signalisation de commande d'appel pour un appel donné. Par exemple, un portier utilisant le modèle d'acheminement par portier peut avoir une connexion de signalisation d'appel directe pour un appel spécifique vers une passerelle ou vers un autre portier. Ces deux autres entités seraient alors les entités voisines de signalisation du portier pour cet appel.

R.3.5 appels stables: un appel est considéré comme stable ou se trouvant dans un état stable suite à l'émission ou la réception d'un message Connect et lorsque des voies de média dans les deux sens sont établies (au moyen de procédures H.245 ou de procédures de connexion rapide). Un appel devient instable en cas de réception ou d'émission d'un message Release Complete (Release

Complete). Certaines commandes de fonctionnalité utilisées pour modifier les connexions de signalisation d'appel peuvent également être à l'origine du fait qu'un appel soit considéré comme instable. La présente version de la Recommandation propose différentes méthodes permettant de conserver uniquement les appels stables au cours d'une phase de rétablissement.

R.3.6 entités en tandem: deux entités homologues (ou plus), faisant toutes office sauf une d'entité de secours pour une entité active.

R.3.7 entité virtuelle: deux entités homologues (ou plus) étroitement couplées, collectivement perçues comme une entité unique par le reste d'un système H.323, et assurant le rétablissement à la suite d'une défaillance.

R.4 Abréviations

La présente annexe utilise les abréviations suivantes:

CRV valeur de référence d'appel (*call reference value*)

GK portier (*gatekeeper*)

GW passerelle (*gateway*)

RAS enregistrement, admission et statut (*registration, admission and status*)

SCTP protocole de transmission de commande de flux (IETF RFC 2960) (à des fins d'information) (*stream control transmission protocol*)

SDL langage de description et de spécification (*specification and description language*)

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

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

R.5 Aperçu général des deux méthodes

La présente version de cette annexe propose deux méthodes d'amélioration de la robustesse.

Le problème à résoudre consiste à obtenir le rétablissement d'une entité H.323 tombée en panne. L'objectif est de conserver un nombre aussi grand que possible d'appels activés. Nous cherchons au moins à conserver tous les appels dans un état "stable". Les appels qui n'ont pas encore été entièrement établis ou qui sont en cours de destruction peuvent être perdus. Un autre objectif consiste à préserver la plus grande partie des informations de facturation pertinentes, telles que l'heure de début de l'appel, l'heure d'arrêt, etc., même si elles sont conservées au sein de l'entité défectueuse (par exemple portier d'acheminement).

On suppose que l'entité défectueuse est associée à au moins une entité de secours désignée, bien que la solution à petite échelle puisse autoriser un rétablissement lorsque l'entité défectueuse est rapidement remise en service. Il faut résoudre deux problèmes majeurs pour rétablir la signalisation correspondant aux appels activés:

1) réacheminement/rétablissement de la signalisation à destination de l'entité de secours;
2) l'entité de secours doit rétablir un nombre suffisant d'informations d'état de l'appel qui se trouvaient dans l'entité défectueuse.

Les deux méthodes se distinguent essentiellement par le procédé de récupération des informations d'état concernant les appels activés et par la quantité d'informations récupérées.

R.5.1 Méthode A: rétablissement d'état à partir des entités voisines

Selon la méthode A, chaque entité est informée des adresses de transport de signalisation concernant les entités de secours pour chaque voisin de signalisation en amont et en aval. Lorsque des entités sont informées de la défaillance de leur voisin de signalisation en amont ou en aval, elles

tentent de se connecter à une des entités de secours. L'entité de secours rétablit les données minimales d'état de l'appel à partir de son voisin de signalisation, à l'aide de messages Status et StatusInquiry (complétés par des champs supplémentaires). Il est à noter que dans certains cas l'entité voisine doit interroger son homologue quant à l'état de l'appel, si elle n'a pas conservé localement toutes les informations nécessaires (par exemple un portier d'acheminement peut ne pas avoir placé en mémoire cachée l'information concernant la voie logique ouverte).

Le rétablissement de l'état de l'appel autorise la poursuite de l'appel (signalisation d'appel direct, signalisation de commande d'appel et connaissance des voies logiques ouvertes), mais ne permet pas la participation de l'entité rétablie à différents services, notamment de facturation.

R.5.1.1 Méthode A partielle

Le cas peut également se produire où une entité H.323 ne dispose pas elle-même d'une entité de secours tout en implémentant la procédure d'amélioration de la robustesse, ce qui lui permet de contribuer à conserver des appels en cas de défaillance de son voisin de signalisation qui dispose d'une entité de secours.

On dit de l'entité qui participe au rétablissement d'appels stables avec l'entité de secours de son voisin de signalisation, mais qui ne dispose pas elle-même d'une entité de secours, qu'elle applique la méthode A partielle.

R.5.2 Méthode B: rétablissement d'état à partir d'un répertoire partagé

La deuxième architecture fait appel à une pseudo-entité peu résistante aux défaillances. Elle peut être implémentée de deux façons différentes:

1) au moyen d'une plate-forme/système d'exploitation résistant aux défaillances;
2) grâce à un ensemble d'entités non résistantes aux défaillances qui partage les informations d'état de l'appel, à l'aide d'une mémoire partagée, d'un disque partagé ou de messages. La présente Recommandation ne spécifie par le mécanisme de partage.

Les entités réelles de cette pseudo-entité résistante aux défaillances doivent partager une quantité suffisante d'informations d'état avec ses entités homologues pour permettre le rétablissement de l'état d'appel souhaité sans aucune aide de ses voisins de signalisation. La présente Recommandation définira les entités d'information minimales qui doivent être partagées. Toute information supplémentaire dont la possibilité de rétablissement est souhaitable peut être partagée. Signalons que la méthode B exigera que toutes les entités de l'ensemble constituant la pseudo-entité proviennent du même fournisseur compte tenu de l'absence de normalisation du mécanisme de partage. Le groupe devrait proposer une ou deux solutions possibles et nous envisageons de recommander un mécanisme de partage normalisé dans les versions de la Rec. UIT-T H.323 postérieures à la version 4.

Des indications plus détaillées concernant cette architecture figurent ci-après.

R.5.3 Comparaison

Chacune de ces deux architectures présente des avantages, ce qui en complique le choix. Certaines des difficultés en présence sont énumérées ci-dessous.

L'approche du rétablissement à partir des entités voisines:

1) permet d'utiliser des entités plus simples;
2) ajoute moins de surdébit avant une défaillance (exige toutefois des messages comportant un champ keepAlive dans certains cas).

En revanche, cette approche:

1) exige davantage de modifications des messages H.323;
2) ralentit sensiblement le rétablissement (en raison des messages Status et StatusInquiry);

3) n'est pas adaptable par échelon et convient uniquement aux systèmes à petite échelle.

L'approche dite du répertoire partagé:

1) dissimule la plus grande partie du processus de rétablissement selon la Rec. UIT-T H.323 et exige donc moins de modifications des messages existants;
2) accélère le rétablissement;
3) autorise l'utilisation future de protocoles de maintenance d'état susceptibles d'être implémentés au-dessous de la couche d'application H.323 (voir Note informative 2 au § R.13);
4) peut prendre en charge le rétablissement des informations de facturation et de différentes informations d'état utiles,

mais:

1) elle ajoute un surdébit notable à l'ensemble des données de signalisation (avant défaillance);
2) elle exige des entités ou des pseudo-entités plus complexes.

R.6 Mécanismes communs

Les deux méthodes ont plusieurs mécanismes en commun.

R.6.1 Détection de perte de connexion TCP

En cas de défaillance réseau, la première tentative "automatique" se situerait au niveau des protocoles d'acheminement IP. En cas d'échec, la défaillance TCP sera signalée des deux côtés (entité et voisin de signalisation, par exemple portier et point d'extrémité). Une défaillance réseau ou bien une défaillance du voisin de signalisation sera perçue comme une défaillance de la connexion TCP.

Lors de l'établissement de l'appel, la capacité du voisin de l'entité à prendre en charge les procédures d'amélioration de la robustesse a été déterminée.

Si un des côtés ne prend pas en charge la procédure d'amélioration de la robustesse définie, il est suggéré de libérer l'appel en raison de la défaillance de la connexion TCP.

Du côté du point d'extrémité, lorsque les deux côtés prennent en charge la procédure d'amélioration de la robustesse, il est suggéré de prévoir un délai de temporisation raisonnable pour permettre à l'autre extrémité de lancer la procédure d'amélioration de la robustesse. Cette temporisation est indispensable afin de pouvoir résoudre un éventuel problème de connectivité du réseau. Après expiration de la temporisation, les ressources internes (consommées par l'appel) doivent être libérées.

R.6.2 Traitement des défaillances de protocole

En ce qui concerne les entités qui utilisent la présente annexe, en cas de défaillance de protocole dans une voie de commande H.245, et si les deux entités voisines de signalisation prennent en charge l'amélioration de la robustesse, la voie en question ainsi que les voies logiques associées ne sont **pas** fermées (contrairement au § 8.6). En revanche, les procédures de rétablissement définies par la présente annexe sont engagées.

R.6.3 Détection des défaillances – Mécanismes keepAlive (maintien d'enregistrement)

En l'absence de mécanisme de maintien d'enregistrement, une défaillance d'entité ou une défaillance de la connexion de signalisation est connue seulement si ladite connexion est utilisée. L'Annexe E propose un mécanisme keepAlive permettant de détecter la défaillance même lorsque le trafic est limité. Un mécanisme keepAlive de protocole TCP possède un délai de temporisation trop long pour être utile, de telle sorte qu'une défaillance TCP risque de ne pas être détectée pendant une période de temps prolongé lorsque le trafic à destination de l'entité défectueuse est peu important.

Notre solution à petite échelle est tributaire de la détection de la défaillance par les deux voisins de signalisation (les connexions sont maintenues entre le voisin et l'entité rétablie); aussi est-il nécessaire d'avoir des messages KeepAlive au niveau H.323 susceptibles d'être utilisés avec les connexions TCP. L'utilisation des messages keepAlive est facultative d'après la Rec. UIT-T H.245. Nous devrions spécifier que les messages Status/Status Inquiry doivent être utilisés périodiquement sur les connexions TCP pour fournir ce mécanisme keepAlive. En dépit de la fréquence de cette difficulté, elle ne pose un problème réel que pour la méthode A, c'est-à-dire le rétablissement d'état par la méthode dite de l'entité voisine.

L'entité la plus proche du demandé (extrémité destination de la connexion ou extrémité utilisant le fanion de référence d'appel = 1 en tant que valeur de référence d'appel CRV pour cette connexion – voir dans la Rec. UIT-T Q.931 la définition des fanions de référence d'appel) doit envoyer périodiquement un message StatusInquiry (c'est-à-dire la direction du trafic de moindre intensité au cours des appels établis). La période doit varier de façon aléatoire à partir d'une valeur maximale configurable tout en restant égale à au moins la moitié de cette valeur afin d'éviter les encombrements. La valeur maximale par défaut recommandée est de deux secondes, pour permettre la détection des défaillances avant expiration de la temporisation des autres messages. La valeur maximale doit figurer dans le message StatusInquiry en tant que valeur timeToLive, de telle sorte que le destinataire puisse également surveiller la défaillance sans devoir procéder à un échange supplémentaire de messages StatusInquiry/Status en sens inverse. Il suffit au système destinataire de régler un temporisateur sur un délai égal à la valeur maximale indiquée.

En présence de voies multiplexées il n'est pas nécessaire d'envoyer un message StatusInquiry/Status pour chaque appel transmis sur la voie. Un message StatusInquiry ou Status dont la valeur CRV IE est mise à 0 (zéro) et dont le champ callIdentifier est également mis à 0 (zéro) s'applique à tous les appels empruntant la voie en question.

Les messages KeepAlive, en particulier au niveau H.323, peuvent ajouter un surdébit de signalisation notable. Il y a lieu d'observer que seule la méthode A avec connexions TCP utilise ces messages KeepAlive et que cette méthode est applicable aux systèmes à petite échelle, dont le nombre de connexions par entité est limité. Afin de réduire au minimum le surdébit, il convient d'éviter l'usage du protocole TCP. Les messages keepAlive, StatusInquiry/Status sont eux **inutiles** dans le cas de notre système à grande échelle.

Afin de réduire encore l'incidence de l'échange de messages keepAlive, dans le cas où il existe plusieurs communications entre deux mêmes entités, des messages StatusInquiry/Status doivent être envoyés sur chacune des connexions entre ces deux entités. Afin d'associer chaque communication active à l'ensemble d'entités qui convient, une instruction de guidage (GUID) d'extrémité doit être incluse dans le message Setup Setup par l'entité émettrice et une autre dans le message de connexion Connect par l'entité de destination. Ces instructions de guidage (GUID) doivent être propres à chaque entité et, dans le cas où une entité comporte plusieurs interfaces de signalisation, doivent être émises interface par interface. Si l'entité comporte plusieurs instances H.323, chacune de ces instances doit émettre une seule instruction de guidage (GUID). Les temporisateurs keepAlive doivent être maintenus pour chaque paire d'instructions de guidage (GUID). A l'expiration du temporisateur keepAlive, toute entité peut envoyer un message StatusInquiry dont l'élément d'information de la valeur de référence d'appel (CRV) et le champ callIdentifier sont tous deux égaux à 0 (zéro), en utilisant à cet effet n'importe quelle connexion disponible. L'entité de signalisation voisine doit répondre à ce message en renvoyant un message keepAliveStatus.

La détection des défaillances des connexions conformes à l'Annexe E se fera en utilisant la messagerie I-Am-Alive existante. La procédure décrite ci-dessus définit les messages keepAlive échangés entre les entités de signalisation utilisant un temporisateur. Ce temporisateur utilise une valeur définie par le temporisateur T-IMA1, réglé par défaut à 6 secondes. Toutefois, dans le cas où les deux entités appliquent également l'Annexe R, ce temporisateur doit pouvoir être configuré conformément aux valeurs recommandées ci-dessus. La messagerie I-Am-Alive utilise également

un compteur défini par le nombre de messages I-Am-Alive consécutifs sans réponse N-IMA1 après lesquels l'entité de signalisation voisine est présumée être en dérangement. Pour les entités actives définies dans l'Annexe R, il est recommandé que ce compteur ait une valeur maximale de deux (2).

R.6.4 Adresse de transport et connexions rétablies

Ces deux solutions (à l'exception éventuelle de certaines solutions de type plate-forme résistante aux défaillances) doivent assurer le rétablissement de la voie de signalisation au moyen d'une adresse de transport de secours. Elles doivent être échangées lors de l'établissement de la signalisation d'appel, au moyen des champs backupCallSignalAddresses des messages Setup et Connect. Une entité envoie l'adresse de signalisation d'appel de son entité de secours dans les messages Setup et Connect. Une entité reçoit l'adresse de signalisation d'appel de l'entité de secours en provenance de l'entité voisine de l'extrémité d'origine lorsqu'elle reçoit un message Setup et en provenance de l'entité voisine de destination lorsqu'elle reçoit un message Connect.

Une entité qui applique la Méthode A partielle doit envoyer un message dont le champ **backupCallSignalAddresses** est vide pour indiquer qu'elle participe à la procédure d'amélioration de la robustesse mais qu'elle ne dispose pas elle-même d'une entité de secours.

Toutes les entités doivent ajouter leur propre adresse de signalisation d'appel en toute première position dans la liste **backupCallSignalAddresses** incluant le numéro de leur accès de réception. L'entité voisine de signalisation (ou son entité de secours) a besoin de ces informations pour rétablir la connexion avec l'entité.

R.6.4.1 Etablissement d'une nouvelle connexion TCP

Lorsqu'une entité détecte une perte de voie de signalisation d'appel vers une entité voisine de signalisation, elle doit s'efforcer de rétablir cette voie au moyen de l'adresse de transport de secours. Sinon, l'entité qui détecte la défaillance peut chercher à sonder son entité voisine de signalisation d'origine en faisant appel à des méthodes dont la description ne relève pas de la présente Recommandation (par exemple validation de connexion par écho) et si, selon elle, l'entité de signalisation d'origine est éventuellement réalisable, elle peut alors chercher à établir la voie vers l'identité voisine de signalisation d'origine avant d'essayer d'utiliser l'adresse de transport de secours. Les responsables de l'implémentation qui choisissent cette option doivent savoir que les tentatives d'établissement d'une connexion TCP vers une entité qui ne répond pas risquent d'entraîner des retards importants.

La voie de signalisation d'appel rétablie devra adopter l'état de la voie précédente – et non se comporter comme une voie nouvelle (son fonctionnement **ne** commencera **pas** par l'émission d'un message Setup). Des indications plus détaillées sont fournies ci-après afin de garantir la synchronisation des états entre entités de signalisation voisines.

NOTE INFORMATIVE – Une autre solution consiste à utiliser pour le transport le protocole SCTP et non le protocole TCP. Les voies SCTP sont associées à une liste d'adresses de transport de remplacement, utilisables en fonction des besoins afin de maintenir la voie, sans intervention de la couche d'application. La Note Informative 2 au § R.13 contient des indications complémentaires concernant l'utilisation du protocole SCTP.

R.6.4.2 Association entre l'appel et la nouvelle connexion TCP

L'association entre l'appel et la nouvelle connexion TCP (côté point d'extrémité) doit s'effectuer en extrayant la valeur callIdentifier contenue dans les messages reçus sur la nouvelle connexion TCP.

R.6.4.3 Fermeture d'une ancienne connexion TCP

Après ouverture de la nouvelle connexion, il peut y avoir ouverture de deux connexions TCP appartenant au même appel, à l'extrémité où il n'y a pas eu défaillance. Dans ce cas, deux options sont en présence:

1) la perte de la connexion TCP a suivi l'émission (et la réception) du message SETUP. Dans ce cas le côté qui n'est pas tombé en panne doit identifier la situation et fermer la connexion. Cette opération est effectuée par détection d'un identificateur callIdentifier identique pour les deux connexions;

2) la perte de la connexion TCP a précédé le transfert du premier message.

Dans ce cas l'extrémité qui n'a pas subi de défaillance n'a aucun moyen de trouver le lien entre la première (ancienne) et la seconde (nouvelle) connexion TCP. Cette difficulté peut être résolue par une procédure permettant à l'extrémité de destination de fermer une connexion, si elle a été ouverte pendant un certain temps et si aucun message n'a été reçu avant expiration d'un délai préalablement défini (cette procédure n'est pas décrite dans la présente annexe).

R.6.5 Prise en charge du statut étendu

Afin d'améliorer l'interopérabilité des deux méthodes, toutes les entités prenant en charge l'amélioration de la robustesse doivent prendre en charge les messages de statut étendu, notamment le champ fastStart. Cela permettra à une entité dont le répertoire est partagé de coopérer avec une entité voisine exigeant un statut correspondant au rétablissement d'état.

R.7 Méthode A: rétablissement d'état à partir d'entités voisines

R.7.1 Introduction

Actuellement les Recommandations UIT-T H.323 et H.225.0 ne définissent pas explicitement de procédures de détection de défaillance de connexion et de rétablissement. La présente méthode a pour objet de définir une procédure autorisant:

- la détection d'une défaillance de connexion TCP;
- la synchronisation entre les deux extrémités de la connexion en termes d'état d'appel;
- la définition d'un comportement recommandé à chaque extrémité afin de renouveler la connexion de signalisation d'appel et d'acheminer normalement l'appel dans chacun des états envisageables.

Le maintien de l'appel (en cas de perte d'une connexion) se justifie principalement dans les situations où il y a une défaillance d'un portier chargé de traiter un nombre important d'appels, pour résoudre un problème matériel ou logiciel. Dans ce cas une commande peut être transférée par l'intermédiaire d'un portier de réserve (ce portier peut conserver toutes les informations concernant les appels au moyen d'une base de données commune). La procédure définie et présentée dans la présente annexe traite ce cas d'une défaillance de portier et permet le traitement des appels gérés sans aucune interruption.

Cette procédure ne traite pas tous les aspects de la défaillance et du rétablissement des connexions TCP, si l'on envisage les autres cas et les autres topologies possibles. Il est néanmoins envisageable de trouver à l'avenir des solutions de ce type.

R.7.2 Domaine d'application

Ce projet de document se rapporte uniquement aux connexions TCP (voie de signalisation d'appel H.225.0 et voies de commande d'appel H.245). Les voies UDP (RAS) ne seront pas traitées, puisque les situations correspondantes de défaillance sont déjà couvertes au moyen du mécanisme de nouvelles tentatives défini pour les voies UDP.

R.7.3 Procédure d'amélioration de la robustesse

A la suite d'une défaillance, l'entité H.323 doit rétablir la connexion de signalisation d'appel et doit envoyer conjointement des messages STATUS INQUIRY et STATUS à l'autre entité H.323. Celle-ci doit répondre par un message STATUS et passer alors dans un état dans lequel chacune des deux extrémités est informée de l'état d'appel de l'autre. Si l'entité de réception n'est pas informée de l'état d'appel, elle doit répondre par un message STATUS dont l'élément d'information CallState est mis à la valeur NULL. La connexion de signalisation d'appel doit être établie au niveau de l'une des adresses **backupCallSignalAddresses**, dans l'ordre de préférence défini par l'ordre des éléments de la structure **backupCallSignalAddresses**.

Dans l'hypothèse où les deux entités amorcent simultanément une connexion de signalisation d'appel, l'entité dont la valeur numérique du champ TransportAddress tiré des valeurs **backupCallSignalAddresses** est la plus petite, doit fermer la connexion TCP qu'elle a ouverte, et utiliser la connexion ouverte par l'autre point d'extrémité. A des fins de comparaison des valeurs numériques de l'adresse TransportAddress tirée du champ **backupCallSignalAddresses**, chaque octet de l'adresse doit être comparé individuellement en commençant par le premier octet de la chaîne OCTET STRING et en continuant de gauche à droite jusqu'à ce que des valeurs inégales soient constatées. La comparaison doit être effectuée initialement sur l'élément d'adresse de la couche Réseau de l'adresse de transport provenant de **backupCallSignalAddresses**, et en cas d'égalité, sur l'élément d'adresse de la couche Transport (port). Voir Figure R.1.

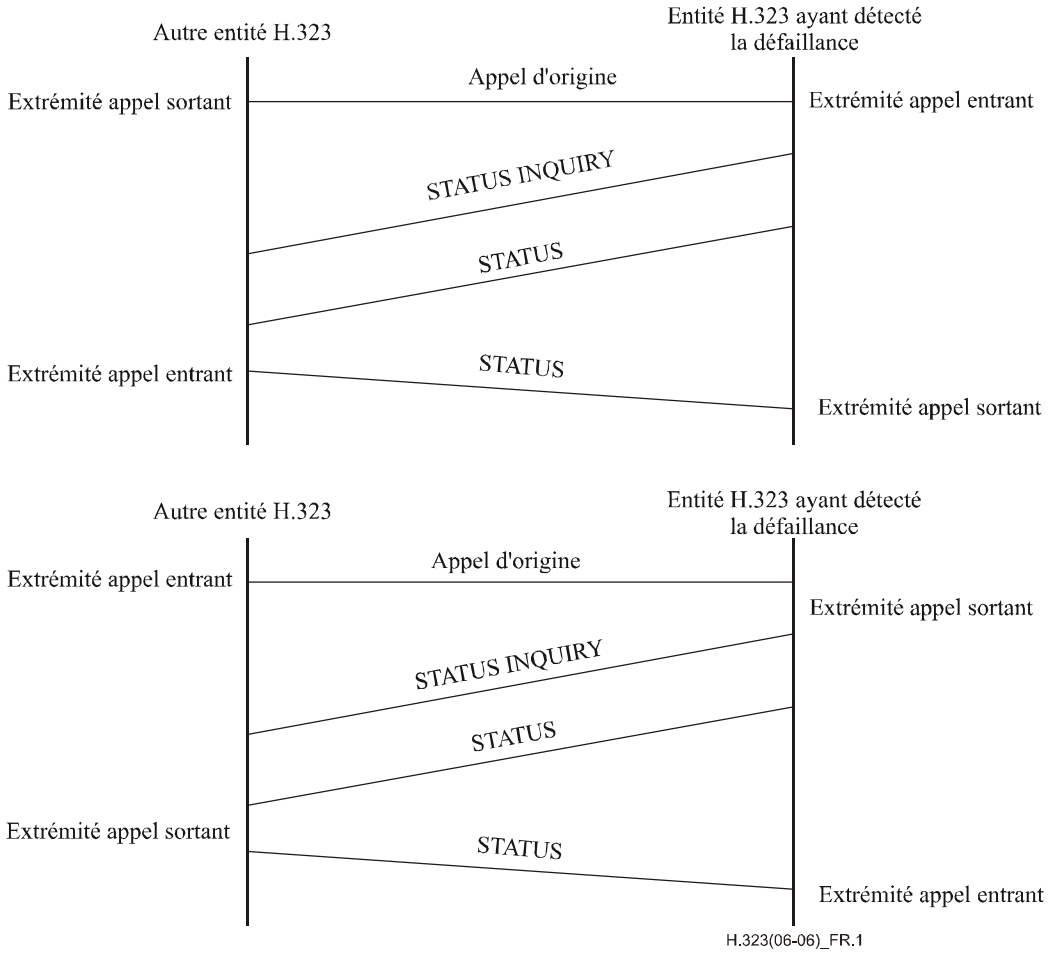


Figure R.1/H.323 – Procédures d'amélioration de la robustesse

Toute connexion antérieure susceptible de rester ouverte pour l'appel doit être fermée, cette exigence s'appliquant aussi bien à la connexion de signalisation d'appel qu'à la connexion de commande d'appel.

Les nouveaux champs **IncludeFastStart** du message STATUS INQUIRY et **RobustnessFastStart** du message STATUS peuvent être utilisés pour faciliter la synchronisation d'état des voies logiques. L'expéditeur du message STATUS doit faire figurer le champ **RobustnessFastStart** contenant les voies de réception et d'émission actuellement activées avec les adresses de réception pour les flux de média et de commande de média. L'expéditeur du message STATUS INQUIRY peut demander l'inclusion du champ **RobustnessFastStart** dans le message STATUS en mettant le paramètre **IncludeFastStart** à la valeur VRAI.

Si une entité intermédiaire a besoin de synchroniser l'état de voie logique, elle doit envoyer le message STATUS INQUIRY à une extrémité de l'appel, attendre le message STATUS contenant le champ **FastStart**, envoyer les messages STATUS et STATUS INQUIRY vers l'autre extrémité d'appel, et enfin envoyer le message STATUS à la première extrémité de l'appel.

Cette procédure permet de synchroniser les états des voies logiques ouvertes, aussi bien par la procédure de lancement rapide que par la procédure H.245 d'établissement de voie logique.

Lorsque l'appel n'a pas atteint l'état activé avant la défaillance, il doit alors être abandonné.

L'entité H.323 chargée de récupérer les informations d'état concernant les appels et son entité de signalisation voisine doivent implicitement réinitialiser leurs machines à états H.245 concernant l'appel, du fait que l'entité chargée de récupérer lesdites informations n'est pas informée des capacités du terminal distant ou n'a pas connaissance du résultat des négociations relatives à la détermination maître/esclave (MSD). En outre, les capacités de ladite entité peuvent différer de celles de l'entité défectueuse. Avant que des messages H.245 ne soient envoyés, les deux entités doivent échanger des messages TCS et procéder à la détermination maître/esclave.

R.7.4 Langage de description et de spécification pour la machine à états selon la méthode A

Voir Figure R.2.

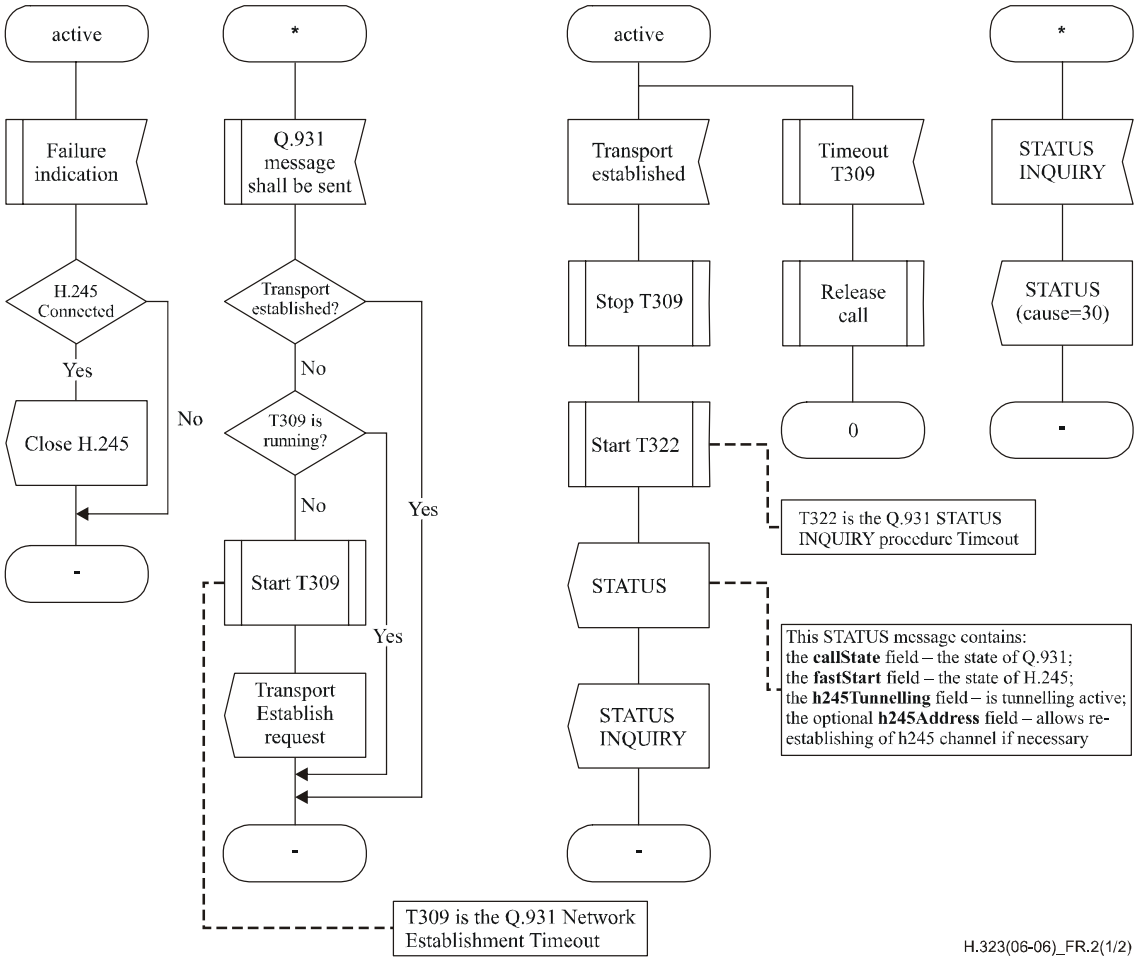


Figure R.2/H.323 – Machine à états selon la méthode A *(feuillet 1 de 2)*

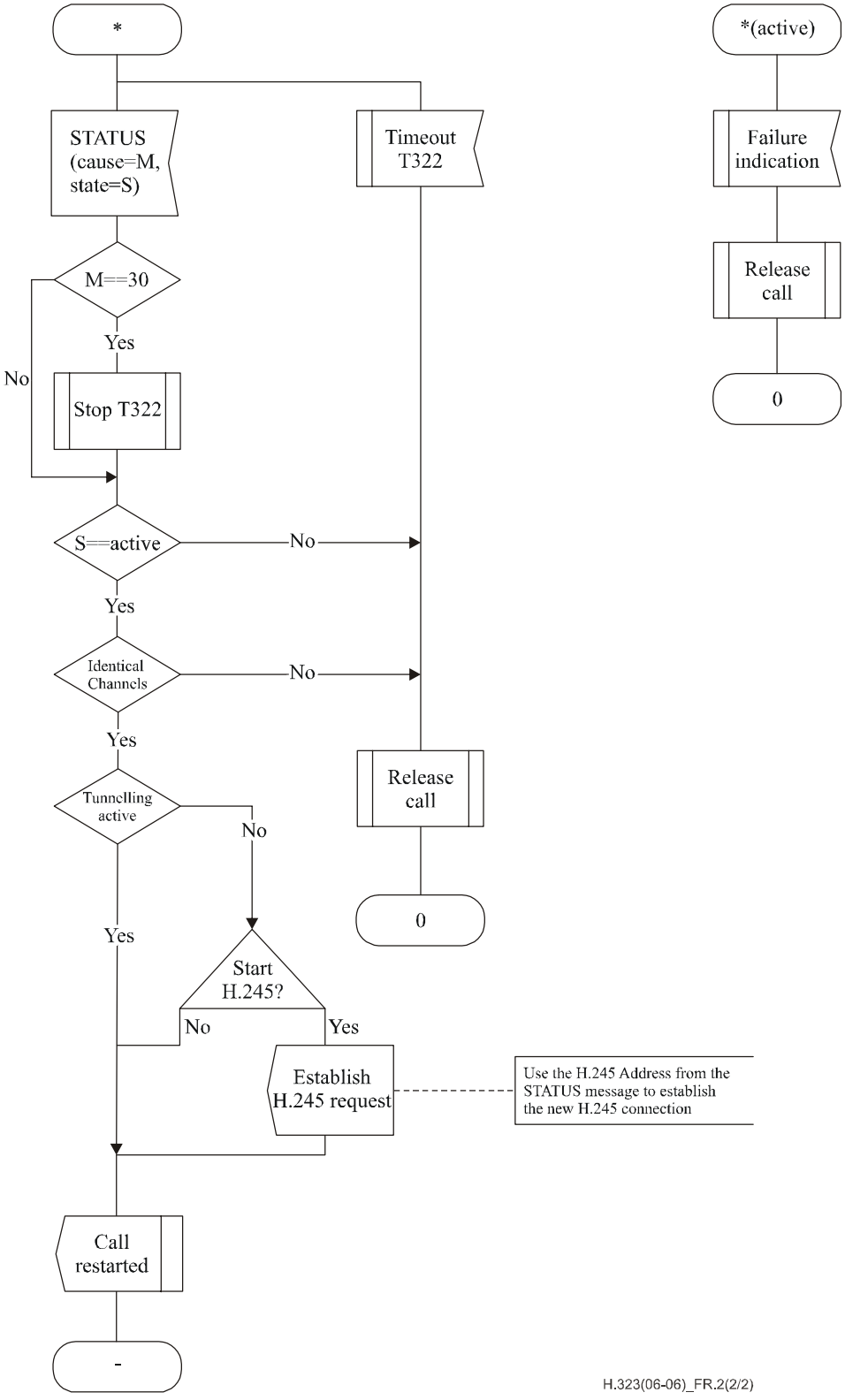


Figure R.2/H.323 – Machine à états selon la méthode A *(feuillet 2 de 2)*

R.8 Méthode B: rétablissement d'état à partir d'un répertoire partagé

Cette méthode utilise une entité ou une pseudo-entité résistante aux défaillances, ainsi que (si l'entité de secours exige une adresse de signalisation différente) un mécanisme de rétablissement de la signalisation d'appel vers l'entité de secours. Plusieurs moyens peuvent être mis en œuvre à cet effet. Le mécanisme résistant aux défaillances ne sera pas normalisé dans la présente version de la

Recommandation mais à cet égard un certain nombre de solutions seront proposées. La normalisation de la solution sera vraisemblablement recommandée dans une version future de la Recommandation. Certains nouveaux protocoles du Groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*) sont susceptibles de contribuer à la résolution de ce problème, bien qu'il n'ait pas encore atteint un stade permettant d'y faire référence dans la version 4 (novembre 2000) de la Rec. UIT-T H.323.

R.8.1 Plate-forme résistante aux défaillances

Une solution consiste à réaliser l'entité d'amélioration de la robustesse sur une plate-forme résistante aux défaillances, qui utilise un support matériel et système d'exploitation. Ce type de solution permettrait de rendre le rétablissement d'état complètement transparent vis-à-vis de la couche H.323. Si la plate-forme conserve en outre une adresse de transport inchangée, il s'agit alors d'une entité virtuelle résistante aux défaillances, de telle sorte que la voie de signalisation ne connaîtra pas de défaillance et aucune procédure au niveau application ne sera nécessaire; par contre si l'adresse de transport est modifiée, le mécanisme décrit dans le présent paragraphe devra être mis en œuvre.

R.8.2 Groupe d'entités résistant aux défaillances

Une autre solution consiste à établir un groupe (deux au moins) d'entités en tandem résistantes aux défaillances, qui se comporte collectivement comme une pseuso-entité résistante aux défaillances. Les entités de groupe doivent s'organiser pour partager des informations d'état d'appel bien définies, suffisantes pour permettre à une entité homologue de prendre le relais en cas de défaillance de l'entité activée. Parmi les solutions pourraient figurer les combinaisons suivantes:

1) entité activée/de réserve ("1+1");
2) entité de réserve unique partagée par plusieurs entités activées (entité de réserve partageant des informations d'état avec chaque entité activée, à laquelle elle est susceptible de se substituer) ("N+1");
3) autres configurations.

Bien que l'information d'état soit partagée, ce qui permet au groupe d'entités d'être perçu comme une entité virtuelle résistante aux défaillances, le maintien d'une adresse de transport de signalisation d'appel inchangée n'est pas possible et le rétablissement de la voie de signalisation d'appel exige donc le recours à l'un des mécanismes décrits au § R.8.3.

Les modalités de partage des informations d'état posent un problème majeur lié au modèle dit du groupe d'entités. Les informations d'état doivent en effet être synchronisées à des instants clés, auxquels le système peut revenir en toute sécurité. Nous appellerons ces instants des *points de reprise*. La présente Recommandation spécifie les points de reprise ainsi que les éléments de données minimaux qui doivent être partagés. Dans la présente version de la Recommandation nous ne proposons pas de solution normalisée en matière de partage, mais nous examinerons toutefois certaines solutions dans la Note informative 2 du R.13 afin d'illustrer cette possibilité du modèle.

R.8.3 Rétablissement de la connexion de la signalisation d'appel

Les modalités de partage des adresses de signalisation de secours sont identiques à celles de la méthode A. Le rétablissement des connexions de signalisation d'appel est semblable mais présente cependant des différences dans la mesure où l'entité de secours contient suffisamment d'informations pour rétablir la connexion à la deuxième extrémité sans attendre la détection de la défaillance par l'autre entité voisine.

Lorsqu'une entité de secours prend le relais d'une entité homologue défaillante et reçoit un message concernant une nouvelle connexion, elle doit alors rétablir l'état d'appel (en utilisant comme clé la valeur de l'identificateur callIdentifier). Cela permettra de poursuivre la prise en charge de l'appel, notamment la signalisation d'acheminement, la conservation des données de facturation, etc. Une

entité qui détecte une défaillance ne doit pas rétablir la connexion tant qu'elle n'a pas reçu un message à envoyer par la connexion. L'entité de secours disposera de nouvelles voies pour chaque appel ayant utilisé l'entité homologue défaillante, sauf en cas d'utilisation de voies multiplexées. Le principe consistant à effectuer les rétablissements uniquement lorsqu'ils sont nécessaires, aura pour effet de les étaler dans le temps.

Le fait de différer le rétablissement jusqu'à ce qu'un message exige l'utilisation de la voie et que l'entité de secours dispose d'informations suffisantes pour établir la nouvelle voie à l'autre extrémité signifient que la méthode B n'a pas besoin de mécanisme keepAlive.

Puisque aussi bien l'entité rétablie que son entité voisine de signalisation sont en mesure de remettre en service la connexion, l'apparition de conditions critiques est possible, mais les messages keepAlive associés aux connexions TCP sont alors inutiles. Puisque le trafic est plus important dans un sens que dans l'autre et que la remise en service intervient uniquement en présence d'un trafic de messages, les conditions critiques apparaîtront rarement. Il est possible de résoudre les problèmes de ce type en faisant appel aux méthodes utilisées pour l'établissement d'une voie H.245. L'entité dont l'adresse H.245 aura la plus petite valeur numérique doit fermer la connexion TCP préalablement ouverte et utiliser la connexion ouverte par l'autre point d'extrémité.

En ce qui concerne les voies de signalisation multiplexées, la détection d'une défaillance affectant un appel quelconque implique nécessairement la défaillance de la voie. Lorsqu'une nouvelle voie est établie, elle doit alors être utilisée pour le même ensemble d'appel que la voie défectueuse. Cela implique doit-on noter que la liste des appels qui partagent une voie doit faire partie intégrante des données partagées entre une entité et son ou ses entités de secours par l'intermédiaire du répertoire partagé. A la suite d'une défaillance, la voie multiplexée est rétablie lorsqu'un message doit être envoyé pour n'importe lequel des appels partageant la voie. Il y a alors un risque de conditions critiques semblable à celui évoqué dans le cas des voies non multiplexées. Si l'on constate que deux voies de signalisation traitent la même série d'appels ou des appels provenant du même poste, une connexion doit alors être abandonnée.

Si une entité reçoit une nouvelle connexion de signalisation avec un identificateur callIdentifier correspondant à celui d'une connexion existante, elle doit alors vérifier que la connexion provient soit de la même entité que la connexion précédente, soit de l'adresse de secours de signalisation d'appel pour la même entité. Dans un cas comme dans l'autre, l'entité qui reçoit la nouvelle connexion doit considérer la connexion antérieure comme étant défectueuse et doit la fermer.

R.8.4 Rétablissement de connexion H.245

Après le rétablissement d'une voie de signalisation d'appel et lorsque la procédure d'amélioration de la robustesse a atteint un état stable, en cas d'utilisation de la procédure de tunnellisation H.245, les entités peuvent continuer à tunnelliser des messages H.245 par la nouvelle voie de signalisation d'appel.

Si une connexion H.245 distincte était utilisée elle peut également avoir subi une défaillance, seule ou en même temps que la voie de signalisation d'appel. Si l'entité a détecté une défaillance sur une voie H.245, elle doit abandonner sa connexion sans la fermer (sans envoyer de message EndSessionCommand, ce qui notifierait à l'autre extrémité que l'appel était terminé); elle doit ensuite chercher à établir une nouvelle connexion en envoyant son adresse H.245 à son entité voisine de signalisation, dans un message Facility (fonctionnalité). Une entité qui reçoit un message Facility contenant une adresse H.245 (h245Address) concernant un appel pour lequel elle dispose déjà d'une voie H.245 (éventuellement défectueuse, mais non détectée) doit fermer cette voie existante et ouvrir la nouvelle. Aucune des deux entités ne doit effectuer de procédure d'initialisation H.245 (détermination maître-esclave et échange de capacités de terminal) pour la nouvelle voie.

L'entité chargée de récupérer les informations d'état concernant les appels peut avoir un ensemble de capacités différentes de celles de l'entité défectueuse. Dans ce cas et notamment si les

procédures H.245 sont déjà engagées entre les entités de signalisation voisines, les entités doivent redémarrer leurs machines à états H.245 et relancer la procédure depuis le début. Pour ce faire, elles utiliseront le fanion **resetH245** dans le champ robustness-data du message STATUS. Après avoir transmis ce fanion, les entités doivent en assurer le suivi en échangeant des messages TCS et MSD.

R.8.5 Eléments de données mis en commun par l'intermédiaire du répertoire partagé

Le répertoire doit permettre de mettre en commun au moins les données suivantes:

1) adresses backupCallSignallingAddresses;
2) répertoire hasSharedRepository;
3) identificateur callIdentifier;
4) structure openLogicalChannel de message H.245 ou fastStart.

Des données supplémentaires peuvent être mises en commun pour prendre en charge le rétablissement des appels instables ou pour permettre le rétablissement de données supplémentaires modifiées pendant des appels stables (par exemple, enregistrement des caractéristiques détaillées des appels, données de durée, données de facturation et jetons d'autorisation).

R.8.6 Points de reprise

Selon la présente version de la Recommandation seront uniquement conservés les appels dont l'état est stable. Aussi le seul point de reprise nécessaire correspond-il à l'établissement de l'état stable, c'est-à-dire lorsque le message Connect a été envoyé ou reçu et lors de l'établissement des voies de média dans les deux sens (au moyen de la procédure H.245 ou de la procédure de connexion rapide).

Les entités peuvent utiliser des points de reprise supplémentaires pour prendre en charge le rétablissement des appels instables ou pour permettre le rétablissement de données supplémentaires ayant fait l'objet de modifications pendant des appels stables.

R.9 Interfonctionnement des méthodes d'amélioration de la robustesse

Les entités voisines de signalisation doivent s'entendre sur la méthode d'amélioration de la robustesse utilisée entre elles. Il **n**'est **pas** nécessaire d'utiliser la même méthode de bout en bout.

La prise en charge de l'amélioration de la robustesse (par une méthode ou une autre) est notifiée par l'entité de l'extrémité d'origine en incluant un champ RobustnessGenericData dans le message Setup. De plus, la prise en charge de la méthode B (répertoire partagé) est indiquée dans le champ hasSharedRepository du message Setup. L'entité du côté destination indique qu'elle prend en charge l'amélioration de la robustesse ainsi que la méthode B en utilisant les mêmes champs du message Connect. Le choix de la méthode A ou de la méthode B est ensuite effectué tel qu'indiqué au § R.10 Procédures de rétablissement.

Si une entité acheminant une signalisation d'appel prend en charge la méthode B (avec répertoire partagé), elle peut alors être invitée à utiliser la méthode B sur une connexion et la méthode A sur l'autre, pour le même appel. En pareille circonstance, elle doit suivre les règles définies dans le § R.10 indépendamment des deux connexions. Si une entité de secours dotée d'un répertoire partagé reçoit un message StatusInquiry, elle peut alors répondre par un message Status utilisant l'information contenue dans le répertoire partagé.

R.10 Procédures de rétablissement

1) Si une entité voisine ne prend pas en charge la méthode B (répertoire partagé) et en cas d'utilisation de la signalisation TCP, il faut alors utiliser des messages StatusInquirykeepAlives. Si l'entité a un répertoire partagé (même si l'entité voisine n'en a pas), elle doit alors envoyer périodiquement un message StatusInquiry. Si l'entité n'a pas de

répertoire partagé, alors seule l'entité la plus proche du demandé doit envoyer périodiquement un message StatusInquiry.

2) Si une entité a un message à envoyer sur une voie de signalisation d'appel (notamment un message keepAliveStatusInquiry) et si elle détecte une défaillance, elle doit alors chercher à établir une voie vers la première adresse contenue dans backupCallSignalAddresses (entité de secours).

3) Après qu'une voie de signalisation d'appel a été rétablie, et si l'entité voisine n'a pas de répertoire partagé, il faut utiliser la méthode A et l'entité procédant à l'établissement de la voie doit envoyer un message Status (comportant le champ fastStart) avant le message en attente.

4) L'entité qui procède à l'établissement de la voie peut également envoyer un message StatusInquiry avant le message en attente, si elle souhaite vérifier la compatibilité des états.

5) Si une entité dotée d'un répertoire partagé reçoit un message StatusInquiry, elle doit envoyer un même message à son entité voisine à l'autre extrémité, afin de récupérer les informations d'état nécessaires (notamment les données fastStart) à moins qu'elle ne conserve la totalité des données de ce type dans son répertoire.

6) Si une entité qui n'est pas dotée d'un répertoire partagé reçoit un message StatusInquiry elle doit attendre de recevoir un message Status de son entité voisine à l'autre extrémité (en envoyant le message StatusInquiry, si nécessaire, à l'autre entité voisine, en cas de disponibilité de la voie de signalisation située à l'autre extrémité).

R.10.1 Procédures de rétablissement avec des valeurs de référence d'appel incompatibles

Il est possible qu'au moment où la défaillance se produit l'entité active et son entité de secours homologue soient toutes deux simultanément en cours de communication avec la même entité de signalisation voisine. En pareil cas, il est théoriquement possible que ces deux entités utilisent les mêmes valeurs de référence d'appel (CRV) pour leurs communications en cours avec l'entité de signalisation voisine et que l'entité de secours homologue ne soit pas en mesure de poursuivre la communication en provenance de l'entité défectueuse en conservant la même valeur CRV. Il conviendra alors d'attribuer une nouvelle valeur CRV et de la communiquer à l'entité de signalisation voisine.

Si l'entité défectueuse implémente la Méthode A, l'entité de signalisation voisine rétablit une connexion de signalisation d'appel avec l'entité de secours de l'entité défectueuse. L'entité de signalisation voisine doit alors envoyer des messages StatusInquiry et Status à l'entité de secours. Mais avant de procéder à l'envoi de ces messages, l'entité de signalisation voisine doit vérifier que c'est bien elle qui a émis l'appel (en tant qu'extrémité appelante) et qu'elle a déjà précédemment émis des appels à destination de l'entité de secours. Si elle est bien l'extrémité appelante et qu'elle ait émis précédemment des appels à destination de l'entité rétablie, comme indiqué sur la Figure R.3, l'entité de signalisation voisine doit alors attribuer une nouvelle valeur CRV unique pour cet appel à destination de l'entité rétablie, et utiliser cette valeur (dans l'élément d'information CRV) dans tous les messages RAS et de signalisation d'appel H.225.0 ultérieurs. L'entité rétablie doit attribuer une valeur CRV unique à cet appel, et utiliser cette valeur dans sa communication avec le portier. Si l'entité de signalisation voisine est l'extrémité appelée et qu'elle a précédemment reçu des appels en provenance de l'entité rétablie, comme indiqué sur la Figure R.4, elle doit alors attribuer une nouvelle valeur CRV unique dans le message StatusInquiry telle que le fanion CRV soit égal à 1 du fait qu'il se trouve à l'extrémité de destination de l'appel. L'entité rétablie doit adopter cette nouvelle valeur CRV pour cet appel. Tous les messages de signalisation d'appel H.225.0 ultérieurs pour cet appel doivent utiliser cette nouvelle valeur CRV. L'entité rétablie, s'il y a lieu, doit attribuer pour cet appel une valeur CRV unique qui devra être utilisée dans les messages RAS.

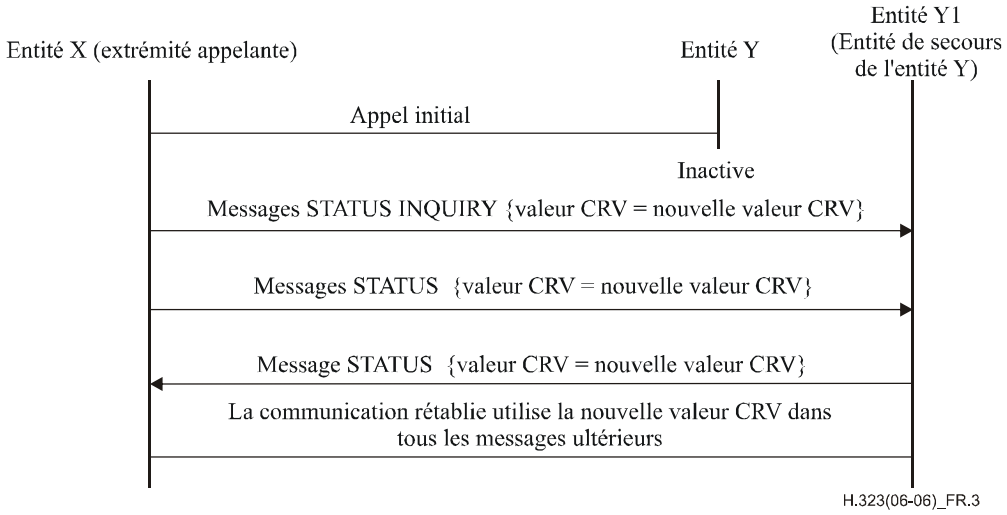


Figure R.3/H.323 – Entité défectueuse utilisant la méthode A et constituant l'extrémité appelée

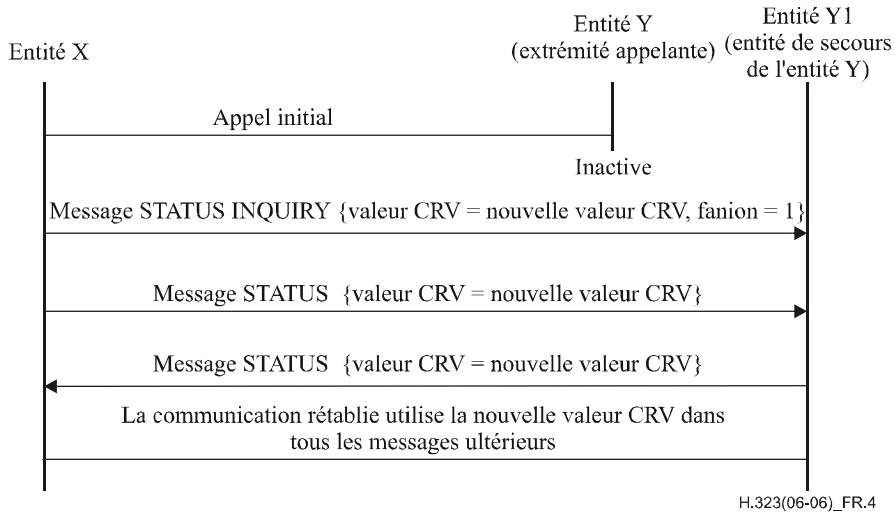


Figure R.4/H.323 – Entité défectueuse utilisant la méthode A et constituant l'extrémité appelante

Si l'entité défectueuse implémente la Méthode B, l'entité de signalisation voisine ou l'entité de secours de cette entité défectueuse peut rétablir la connexion de signalisation d'appel. Quelle que soit l'entité qui rétablisse la connexion de signalisation d'appel, avant d'envoyer tout message de signalisation d'appel H.225.0, l'entité en question doit vérifier que c'est bien elle qui a émis l'appel (en tant qu'extrémité appelante) et qu'elle a déjà émis précédemment des appels à destination de l'entité rétablie. Si l'entité qui rétablit la connexion est l'extrémité appelante et qu'elle ait précédemment émis des appels à destination de l'entité de signalisation voisine, comme indiqué sur la Figure R.5, elle doit alors attribuer une nouvelle valeur CRV pour cet appel et utiliser cette valeur dans tous les messages RAS et de signalisation d'appel H.225.0 ultérieurs. L'entité de signalisation voisine doit attribuer une valeur CRV unique pour cet appel et utiliser cette valeur dans des messages RAS pour communiquer avec le portier. Si l'entité qui rétablit la connexion est l'extrémité appelée et qu'elle ait précédemment reçu des appels en provenance de l'entité de signalisation voisine, comme indiqué sur la Figure R.6, elle doit alors attribuer une nouvelle valeur CRV unique et utiliser cette valeur dans un message de signalisation d'appel H.225.0 dont le fanion CRV est égal à 1, du fait qu'il se trouve à l'extrémité de destination de l'appel. L'entité de signalisation voisine

doit adopter cette nouvelle valeur CRV pour cet appel. Tous les messages de signalisation d'appel H.225.0 ultérieurs pour cet appel doivent utiliser cette nouvelle valeur CRV. L'entité de signalisation voisine, s'il y a lieu, doit attribuer pour cet appel une valeur CRV unique qu'elle utilisera dans des messages RAS.

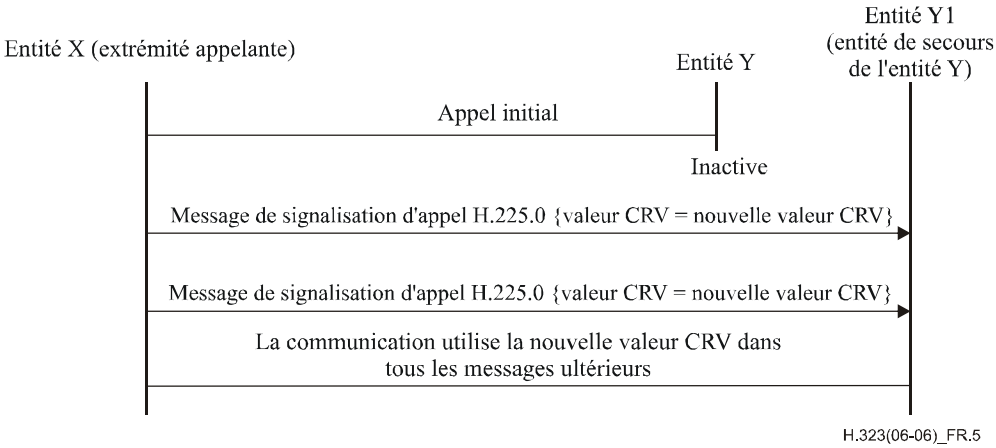


Figure R.5/H.323 – Utilisation de la Méthode B par l'entité défectueuse, qui constitue l'extrémité appelée, et rétablissement de la communication par l'entité qui reste en état de marche

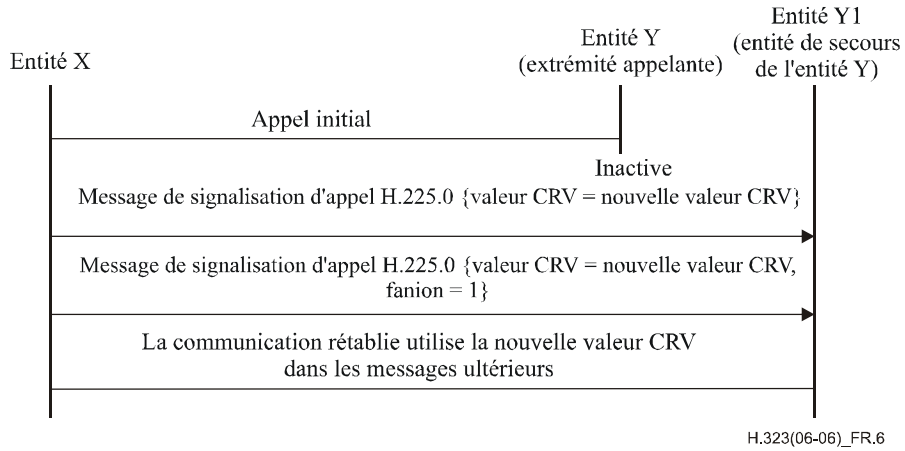


Figure R.6/H.323 – Utilisation de la Méthode B par l'entité défectueuse, qui constitue l'extrémité appelante, et rétablissement de la communication par l'entité qui reste en état de marche

R.11 Utilisation du champ GenericData

Les champs de données nécessaires à l'implémentation des dispositions de la présente annexe sont contenus dans les champs GenericData de différents messages indiqués ci-dessous. Les données d'amélioration de la robustesse `RobustnessData` doivent être codées et les données binaires ainsi obtenues sont acheminées en tant qu'instances brutes du champ GenericData dans les messages spécifiés.

```
RobustnessData ::= SEQUENCE
{
     versionID           INTEGER (1..256),
     robustnessData      CHOICE {
          rrqData             Rrq-RD,
          rcfData             Rcf-RD,
```

```
          setupData          Setup-RD,
          connectData        Connect-RD,
          statusData         Status-RD,
          statusInquiryData  StatusInquiry-RD,
          ...
     },
     ...
}

BackupCallSignalAddresses ::= SEQUENCE OF CHOICE {
     tcp                TransportAddress,
     alternateTransport AlternateTransportAddresses,
     ...
}

Rrq-RD ::= SEQUENCE
{
     backupCallSignalAddresses   BackupCallSignalAddresses,
     hasSharedRepository         NULL OPTIONAL,
     ...
}

Rcf-RD ::= SEQUENCE
{
     hasSharedRepository     NULL OPTIONAL,
     ...,
     irrFrequency            INTEGER (1..65535) OPTIONAL  -- en secondes;
                                                          -- non présent
                                                          -- si le portier (GK)
                                                          -- ne demande pas de
                                                          -- réponse à ses
                                                          -- demandes
                                                          -- d'information (IRR)
                                                          -- pour les
                                                          -- communications
                                                          -- rétablies
}

Setup-RD ::= SEQUENCE
{
     backupCallSignalAddresses   BackupCallSignalAddresses,
     hasSharedRepository         NULL OPTIONAL,
     endpointGuid                GloballyUniqueIdentifier OPTIONAL,
     ...
}

Connect-RD ::= SEQUENCE
{
     backupCallSignalAddresses   BackupCallSignalAddresses,
     hasSharedRepository         NULL OPTIONAL,
     endpointGuid                GloballyUniqueIdentifier OPTIONAL,
     ...
}

Status-RD ::= SEQUENCE
{
     h245Address   TransportAddress OPTIONAL,
     fastStart     SEQUENCE OF OCTET STRING OPTIONAL,
     ...,
     resetH245     NULL OPTIONAL
}

StatusInquiry-RD ::= SEQUENCE
{
```

```
    h245Address         TransportAddress OPTIONAL,
    timeToLive          TimeToLive OPTIONAL,
    includeFastStart    NULL OPTIONAL,
    ...
}
```

L'identificateur GenericIdentifier doit être mis à la valeur 1:

```
robustnessId GenericIdentifier ::= standard:1
```

En outre un champ featureDescriptor contenant l'identificateur robustnessId doit être contenu dans le champ desiredFeatures des messages spécifiés ci-dessous.

R.11.1 Utilisation du champ GenericData dans les messages H.225.0

Les messages RRQ, RCF, ARQ, ACF, Setup, Connect, Status et StatusInquiry doivent inclure les données d'amélioration de la robustesse RobustnessData dans le champ GenericData, selon les définitions des données des différents messages.

Tous les messages (RRQ, RCF, ARQ, ACF, Setup et Connect), exception faite des messages Status et StatusInquiry doivent inclure le descripteur FeatureDescr d'amélioration de la robustesse dans le champ desiredFeatures du champ featureSet. A noter que le champ desiredFeatures n'est pas contenu dans le champ featureSet du message Setup.

La version des données présentées ici (champ versionID de RobustnessData) doit être mise à 1.

R.12 Note informative 1: généralités concernant les méthodes d'amélioration de la robustesse

Le présent paragraphe décrit d'un point de vue général les différents types de défaillances de système et de méthodes d'amélioration de la robustesse. Les méthodes d'amélioration de la robustesse décrites dans la version actuelle de la présente annexe ne couvrent pas tous les types de défaillances de système. Cet exposé à caractère plus général s'emploie à situer dans leur contexte les méthodes définies actuellement et à mieux informer le lecteur quant aux types de défaillances pris en charge. Il récapitule par ailleurs les défaillances susceptibles d'être traitées dans les versions futures de cette annexe.

R.12.1 Types de méthodes d'amélioration de la robustesse

L'amélioration de la robustesse des systèmes peut être assurée de différentes façons:

1) méthodes de redondance du matériel/système d'exploitation (le cas échéant en ajoutant plusieurs cartes d'interface réseau);
2) entités en tandem;
3) entités virtuelles.

R.12.2 Entités d'amélioration de la robustesse

Les entités réputées améliorer la robustesse se composent essentiellement de toutes les entités H.323:

1) portiers;
2) éléments périphériques;
3) contrôleurs multipoints;
4) éventuellement processeurs multipoints (en cas de défaillance du flux de média);
5) passerelles (notamment passerelles IP-IP);
6) relais coupe-feu;
7) certains types de points d'extrémité.

Tous les modèles d'amélioration de la robustesse ne sont pas parfaitement adaptés à chacun des composants des systèmes.

R.12.3 Domaine d'utilisation d'un système d'amélioration de la robustesse

Le domaine d'amélioration de la robustesse ou la partie d'un système réputé améliorer la robustesse peut comporter un ou plusieurs des éléments suivants:

1) zones H.323 (intrazone avec un ou plusieurs portiers);
2) intradomaine H.323 (intradomaine, interzone avec plusieurs portiers);
3) interdomaines H.323 (interdomaine, avec plusieurs portiers et éléments frontière).

R.12.4 Fin de session et défaillance de système

Une fin normale de session de système (par exemple un contrôleur multipoint quittant une conférence) doit être traitée comme une défaillance de système. La fin de session autorise en principe le point d'extrémité destinataire à informer ses homologues, ce qui simplifie potentiellement les opérations de détection, mais exige par ailleurs l'utilisation de mécanismes supplémentaires ou légèrement différents. Il convient de noter que la notification n'est pas toujours menée à bien en raison de pertes de paquets répétées, de telle sorte que la frontière avec les défaillances du système n'est à toutes fins pratiques pas définie.

Les paragraphes ci-dessous présentent différents aspects des défaillances de système:

R.12.4.1 Types de défaillances

Les méthodes décrites dans la présente annexe traitent exclusivement des défaillances détectables du point de vue d'un protocole "en ligne". En effet, la défaillance d'un processeur sur un système à multiprocesseur doté d'une mémoire partagée n'est pas visible à l'extérieur et ne relève donc pas des méthodes en question. En revanche, la défaillance d'une carte d'interface réseau exige l'utilisation d'une adresse de transport différente; aussi est-elle visible et doit-elle être prise en compte. Les types suivants de défaillances seront visibles du point de vue du voisin de signalisation et relèvent de la présente étude:

1) défaillance complète d'un composant du système (perte d'alimentation, panne système);
2) défaillance partielle de composant du système (défaillance d'une des nombreuses interfaces de communication);
3) défaillance complète de liaison réseau (un composant du système n'est plus accessible);
4) défaillance partielle de liaison réseau (certains composants du système ne sont plus reliés, mais d'autres peuvent encore communiquer; ce type de défaillance inclut notamment les pertes de connectivité de liaison unidirectionnelle).

Il convient de signaler que certains de ces modes de défaillance peuvent être non seulement difficiles à détecter (de façon symétrique), mais en outre difficiles à distinguer les uns des autres (voir ci-dessous).

5) Les actes de malveillance à l'égard du système doivent être examinés dans le contexte des tâches de sécurité définies par la Rec. UIT-T H.323.

R.12.4.2 Détection des défaillances

1) Délais de détection d'une défaillance.
2) Moyens de détection d'une défaillance (surveillance permanente explicite ou détection suite à l'invocation d'une fonction).
3) Entités chargées de/impliquées par la détection d'une défaillance.
4) Perception d'une défaillance pour un composant du système (un ensemble de composants du système).

5) Possibilité de déterminer le type de défaillance.

6) Compatibilité/synchronisation de la détection des défaillances parmi les divers composants d'un système.

7) La détection des défaillances n'est pas toujours transitive, autrement dit si "A peut/ne peut pas communiquer avec B" et si "B peut/ne peut pas communiquer avec C" n'entraîne pas nécessairement que "A peut/ne peut pas communiquer avec C".

8) Quel surdébit est-il acceptable?

R.12.4.3 Traitement des défaillances

1) Délai de correction de la défaillance.

2) Entité chargée d'amorcer le processus de correction.

3) Possibilité de corriger la défaillance.

4) Conséquences en cas d'impossibilité de corriger la défaillance.

5) Comment garantir le traitement cohérent d'une défaillance par toutes les entités concernées?

6) Comment traiter les défauts de compatibilité de perception/détection des défaillances par les différents composants (défectueux ou non défectueux)?

7) Comment traiter les différences de rythme de détection des défaillances?

8) Comment traiter un état d'incohérence en présence d'une défaillance?

9) Comment traiter les informations d'état en présence d'une défaillance?

10) Conséquences pour le fonctionnement général du système (par exemple pour un appel en cours).

11) Quel surdébit est-il acceptable?

12) Comment traiter les défaillances multiples simultanées?

R.12.4.4 Scénarios de défaillance

Le présent paragraphe répertorie un certain nombre de scénarios de défaillance identifiés dans le cas de systèmes H.323. Les méthodes d'amélioration de la robustesse décrites dans la présente annexe ne permettent pas d'obtenir un rétablissement à partir de toutes ces défaillances, mais elles sont mentionnées à des fins d'exhaustivité et afin de situer dans leur contexte les différentes défaillances faisant l'objet des méthodes d'amélioration de la robustesse.

1) (portier – point d'extrémité): relation non encore établie/disparue;

2) (portier – point d'extrémité): défaillance découverte mais non enregistrée;

3) (portier – point d'extrémité): défaillance découverte et enregistrée;

4) au cours de l'établissement de l'appel:

   a) direct;

   b) acheminé par portier,

5) au cours d'un appel/conférence: Rec. UIT-T D.160: "état instable" – étudier ce que cela signifie pour les différents protocoles:

   a) direct;

   b) acheminé par portier,

6) au cours de la libération d'appel:

   a) directe;

   b) acheminée par portier.

Envisager les implications liées aux divers nouveaux protocoles en cours d'élaboration (famille H.450.x, Annexe K, Annexe L de la présente Recommandation, etc.).

Envisager les flux de médias ainsi que les relations RAS/signalisation d'appel/communication de commande de conférence.

R.13 Note informative 2: partage d'état d'appel entre une entité et son entité homologue de secours

Cette Note propose des moyens pour implémenter le partage d'état d'appel entre une entité et une autre entité qui fait office d'entité homologue de secours. Le choix d'une méthode ne relève pas de la présente Recommandation. Puisque la méthode n'est pas normalisée, les entités homologues provenant de différents fournisseurs ne sont pas nécessairement en mesure de constituer des entités homologues de secours d'amélioration de la robustesse.

R.13.1 Mémoire partagée

Si des éléments du groupe d'entités sont matériellement situés dans la même armoire, elles peuvent avoir la possibilité d'utiliser un dispositif de mémoire partagée (réfléchie). Cette solution s'apparente à de nombreuses plates-formes résistantes aux défaillances, mais pourrait consister simplement à enregistrer des données en mémoire partagée au niveau de chaque point de reprise au lieu d'utiliser un système d'exploitation résistant aux défaillances.

R.13.2 Disques partagés

Si les éléments du groupe d'entité sont physiquement rapprochés, ils peuvent utiliser un disque partagé et enregistrer les informations d'état correspondant à chaque point de reprise.

R.13.3 Analyse des messages

L'entité activée peut envoyer un message de mise à jour de l'état partagé à chacun des autres membres du groupe, au niveau de chaque point de reprise. Cette solution a pour effet de réaliser une mémoire partagée répartie, appelée parfois "panneau d'affichage" (*bulletin board*). Les messages peuvent être envoyés au moyen de messages UDP distincts, de messages multidiffusion et de liaisons TCP permanentes ou d'un protocole d'analyse des messages résistant aux défaillances telles que ASAP (qui prend en charge un mécanisme multidiffusion d'émissions groupées n'exigeant pas de protocole IP multidiffusion). Cette méthode est examinée de façon plus détaillée dans le Document APC-1772, avec mention de certains points de reprise suggérés.

R.13.3.1 SCTP/ASAP

Le présent paragraphe propose d'illustrer, avec l'exemple de l'appel H.323, l'utilisation des protocoles ASAP et SCTP à des fins d'amélioration de la robustesse dans un système H.323. Il décrira succinctement:

1) un aperçu de l'architecture d'un système H.323 utilisant le protocole ASAP/SCTP;
2) une présentation des piles de protocoles nécessaires aux différents nœuds H.323;
3) des scénarios de reprise sur incident correspondant à un exemple d'appel H.323 avec deux portiers et deux points d'extrémité.

R.13.3.1.1 Références

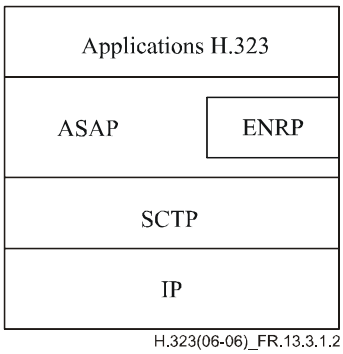
[R.13-1] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

[R.13-2] STEWART (R.) *et al.*: *Aggregate Server Access Protocol (ASAP)*, <draft-ietf-rserpool-asap-14.txt>, IETF, octobre 2006.

[R.13-3] XIE (Q.) *et al.*: *Endpoint Name Resolution Protocol (ENRP)*, <draft-ietf-rserpool-enrp-08.txt>, IETF, juin 2004.

R.13.3.1.2 Piles de protocoles

En règle générale une application H.323 utilisant le protocole ASAP/SCTP [R.13-1] à [R.13-3] de résistance aux défaillances sera dotée de la pile de protocoles suivante:



Il est possible ainsi de réaliser une reprise sur incident rapide et transparente vis-à-vis de l'application de la couche supérieure, aussi bien au niveau liaison qu'au niveau session:

1) niveau liaison (SCTP) – prise en charge des retours multiples vers l'origine, résistance aux défaillances de réseau;

2) niveau session (ASAP) – prise en charge d'un groupe de serveurs (2N, N+K, etc.) résistance aux défaillances de traitement/nœud.

En outre, le protocole ASAP:

- assure une transparence vis-à-vis de l'emplacement;
- offre le partage de charge;
- permet une utilisation immédiate, c'est-à-dire une échelonnabilité dynamique;
- évite les pannes localisées.

R.13.3.1.3 Aperçu de l'architecture d'un système H.323

La Figure R.7 représente un système H.323 conçu selon le modèle ASAP/SCTP.

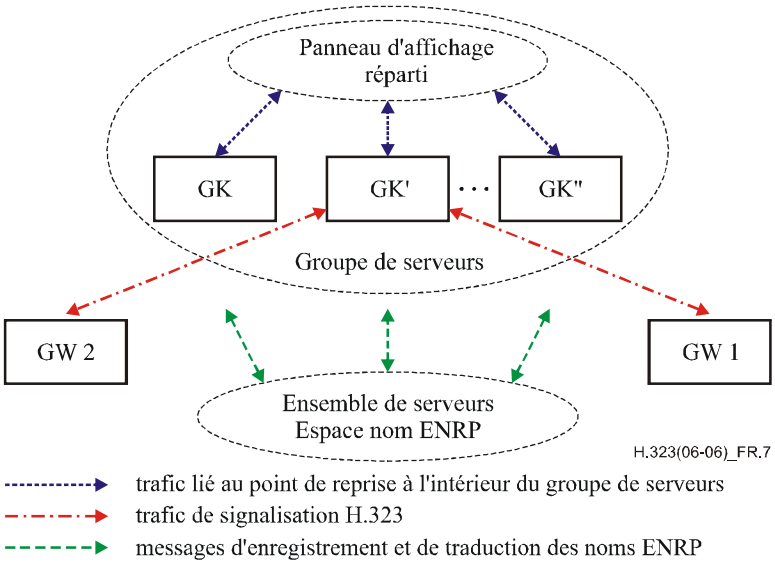


Figure R.7/H.323 – Système H.323 conçu selon le modèle ASAP/SCTP

Dans le système, tous les composants H.323, notamment les passerelles GW 1, GW 2, et les portiers utilisent les piles de protocoles ASAP/SCTP telles qu'indiquées plus haut. Dans cet exemple, nous supposons que le portier H.323 est implémenté en tant que groupe de serveurs (la figure représente les éléments internes du groupe serveur), tandis que les passerelles ne sont pas nécessairement implémentées en tant que groupes de serveurs.

Comme l'indique la figure, le groupe de serveurs portiers contient des instances multiples de portiers H.323 fonctionnellement identiques, GK, GK', ... GK". Les instances de portiers ont en commun l'état d'appel et les différentes informations critiques du point de vue du rétablissement d'appel, au moyen d'un panneau d'affichage interne réparti. Le mécanisme et l'implémentation du panneau d'affichage réparti sont propres à chaque fournisseur et ne relèvent donc pas du domaine d'application du protocole ASAP ou SCTP (le panneau d'affichage peut toutefois être doté d'une résistance aux défaillances et d'une échelonnabilité grâce à l'utilisation du protocole ASAP/SCTP).

Tous les nœuds ASAP/SCTP, notamment les passerelles et les portiers, sont tributaires soit d'un seul ensemble de serveurs namespace de protocole de résolution de nom de point d'extrémité ENRP (*endpoint name resolution protocol*), soit d'un groupe d'ensembles ENRP pontés pour l'enregistrement du nom et des services de traduction du nom [R.13-2]. Afin de constituer le groupe de serveurs portier, toutes les instances GK s'enregistrent sous le même nom dans l'espace nom (ou *namespace*) ENRP. Toutefois chaque instance GK individuelle peut choisir de s'enregistrer avec une valeur différente de la capacité de traitement de la charge.

Chaque message d'appel H.323 sera acheminé par le protocole ASAP à l'une des instances GK du groupe serveur. Le choix de l'instance GK destinataire est fonction, d'une part, du principe appliqué en matière de partage de la charge et, d'autre part, de l'état actuel de chacune des instances GK du groupe de serveurs. Il est parfois particulièrement souhaitable de faire en sorte que tous les messages de signalisation H.323 liés à un appel soient traités par la même instance GK pendant tout le cycle de vie et de ne laisser aucune autre instance GK prendre le relais de l'appel sauf si l'entité de traitement d'origine cesse de fonctionner. Cette liaison entre l'appel et l'instance de serveur est qualifiée de "liaison indéterminée". Le protocole ASAP est conçu pour prendre en charge très simplement ce type de "liaison indéterminée" [R.13-2] et [R.13-3].

De plus, lorsqu'une instance GK traite un appel, elle doit transmettre en direction du panneau d'affichage réparti (c'est-à-dire pour les points de reprise) toutes les informations d'état critique, à chaque fois que l'appel passe par un certain stade de son cycle. Ces informations permettront à l'instance GK de substitution de rétablir plus facilement l'appel en cas de blocage de l'entité originale de traitement de l'appel.

R.13.3.1.4 Exemple d'appel H.323

La description de l'appel utilisera les flux de signalisation du diagramme de la Figure R.8.

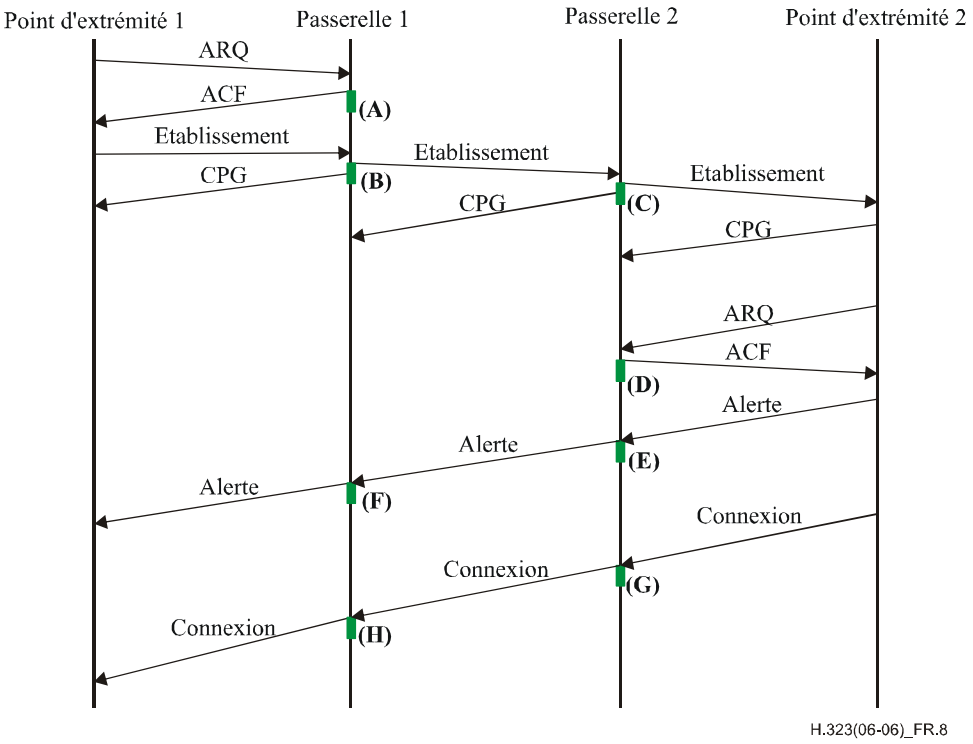


Figure R.8/H.323 – Exemple d'appel H.323

Il faut attirer l'attention sur le fait que les documents auxquels il est fait référence pour ce flux d'appels ne sont pas très récents et que la mention du deuxième portier résulte d'une extrapolation. Ainsi, un flux d'appels conforme à la norme H.323 actuelle présenterait certes quelques différences, mais il s'agit en l'occurrence de mettre l'accent sur le mode d'utilisation des protocoles ASAP/SCTP. En dépit de la présence d'inexactitudes mineures dans la figure ci-dessus, l'exemple proposé conserve néanmoins sa valeur.

R.13.3.1.4.1 Description générale

L'appel commence par la demande de largeur de bande émise par le point d'extrémité 1. Dans ce cas le point d'extrémité utilise le protocole ASAP pour demander un portier, désigné par un nom ou le cas échéant une adresse et un port IP bien connus. Dans un cas comme dans l'autre, une demande (non représentée) de traduction de nom ENRP acheminerait jusqu'au point d'extrémité l'ensemble des portiers (primaires et éventuellement redondants) du groupe serveur. Cette information serait introduite dans une mémoire cache locale de la couche ASAP du point d'extrémité 1 afin de pouvoir s'y référer ultérieurement en cas de défaillance. Cette même opération de mise en mémoire cache doit s'effectuer au niveau de tous les points d'extrémité ASAP de la chaîne, de façon transparente par rapport à l'appel proprement dit. Il est à signaler que la mise en mémoire cache constitue une possibilité facultative. Puisqu'il s'agit d'une option, les points d'extrémité qui ne l'utilisent pas peuvent néanmoins obtenir un portier de remplacement, auquel cas une demande supplémentaire devrait être adressée au serveur ENRP au moment de la détection d'une défaillance.

A noter que nous atteignons à présent le point (**A)** au niveau duquel le portier attribue une largeur de bande et consigne ce message d'information d'utilisation de largeur de bande dans une zone de panneau d'affichage. Cette zone de panneau d'affichage pourrait être l'une des suivantes:

- une fraction de mémoire partagée répartie gérée pour un sous-système distinct;
- une fraction de mémoire miroir (ou réfléchie) spécifiquement créée à cet effet;
- une base de données commerciale répartie;
- toute autre solution imaginative.

Il faut bien noter qu'il s'agit avant tout de trouver pour les portiers redondants/homologues une façon ou une autre de partager l'état d'appel. Aussi tout mécanisme existant ou tout mécanisme futur conçu à cet effet peut être utilisé.

Le portier 1 définit son information d'état liée à la demande d'admission et introduit cette information vers le panneau d'affichage, avant de répondre normalement à la demande formulée, c'est-à-dire au moyen d'une confirmation d'admission ACF.

Le point d'extrémité 1 réagit maintenant et envoie le message Setup au portier 1. A réception du message de configuration le portier 1 choisit le portier suivant (dit portier 2) et lui transmet son message de configuration, en "insérant" l'information d'état concernant l'appel (point (**B**)). Celle-ci étant le cas échéant liée d'une façon ou d'une autre à l'information précédente (éventuellement par une sorte de renvoi de référence croisée du type l'appel X qui utilise la largeur de bande Y, représentée par l'information de ARQ). Après avoir introduit l'information au point (**B**), le portier 1 envoie le message de traitement d'appel au point d'extrémité 1.

Le portier 2 reçoit le message Setup envoyé par son portier homologue, choisit le point d'extrémité de destination, transmet le message Setup et insère l'information d'état au point (**C**) en ce qui concerne l'appel. Après avoir introduit son information d'état jusqu'au panneau d'affichage, il envoie au portier 1 un message de traitement d'appel.

Le point d'extrémité 2, à réception du message Setup, renvoie un message de traitement d'appel et demande à son portier une largeur de bande au moyen de son propre message ARQ.

A la suite de cette opération, le portier 2 attribue une largeur de bande, pousse l'information d'état au point (**D**) et renvoie le message ACF. A réception de ce message, le point d'extrémité 2 envoie un message d'alerte au portier 2.

A réception du message Alerting, le portier 2 devrait insérer une petite mise à jour vers son panneau d'affichage (point (**E**)), autrement dit une information annonçant que l'appel en est au stade alerte, et la transmettre dans un message Alerting au portier 1.

Le portier 1 répétera cette procédure, en mettant à jour son information d'état au point (**F**) et en la transmettant dans le message Alerting.

Le point d'extrémité 2 répond à l'appel à un certain moment, en adressant un message Connect au portier 2. Le portier 2, à réception du message Connect, insérera alors une petite mise à jour de son information d'état en direction du point (**G**), indiquant que l'appel en est à présent au stade connecté et transmettra cette information dans le message Connect au portier 1.

A réception du message Connect, le portier 1 effectuera la même opération, sauvegardant son information d'état au point (**H**) et transmettant le message Connect au point d'extrémité 1.

R.13.3.1.4.2 Scénarios de défaillance

Les descriptions ci-dessus supposent un niveau maximal de redondance et de protection des informations d'état/de l'appel. Suivant ce scénario, toute défaillance de l'un des portiers devient transparente pour l'un ou l'autre point d'extrémité. En cas de défaillance, le message serait réacheminé par le protocole ASAP vers une entité de substitution. L'entité de remplacement devrait

alors prendre les mesures suivantes à la suite de tout message reçu pour lequel elle ne possède pas d'objet ou de bloc d'appel:

- rechercher l'appel dans le "panneau d'affichage";
- extraire l'information d'état et créer un bloc ou un objet de commande d'appel relatif à l'appel;
- poursuivre le traitement du message pour le compte de l'entité homologue qui a cessé de fonctionner.

Les points d'extrémité sont alors entièrement transparents du point de vue des scénarios de défaillance. Aucune information n'est introduite dans le point d'extrémité proprement dit (autre que le protocole ASAP) dans un but de rétablissement à la suite d'une défaillance de portier.

R.13.3.1.4.3 Problème de sauvegarde d'état

Tel qu'indiqué plus haut, l'exemple présenté présuppose un niveau maximal de sauvegarde des informations d'état. Dans ces conditions les mises à jour des informations d'état devraient être réduites au minimum. En particulier, l'état d'appel devrait être défini simplement par l'ensemble le plus petit possible d'informations nécessaires pour constituer l'appel ET les mises à jour devraient être aussi réduites que possible. Dans certains cas l'opérateur ne souhaite pas nécessairement un tel niveau de redondance. Afin d'obtenir un système fiable avec moins d'informations d'état, les points de partage suivants pourraient être éliminés:

- Points (**A**) et (**D**) – Si le portier calcule par une autre méthode la largeur de bande utilisée (hormis le simple décompte du nombre d'appels), ces opérations pourraient être complètement supprimées sans dommage. L'opérateur ne se soucie peut-être aucunement des informations de commande d'admission et les portiers n'effectuent pas ce type de tâche, auquel cas cette opération est inutile.
- Points (**F**) et (**E**) – Ces points sont facultatifs dans la mesure où ils sont susceptibles de ne fournir aucune information méritant d'être sauvegardée, par exemple, le téléphone sonne ou la phase d'établissement se poursuit.
- Points (**B**) et (**C**) – Si l'opérateur est soucieux de conserver uniquement les appels stables, ces points peuvent être supprimés. Dans ce cas, tous les appels qui étaient en cours d'établissement seraient perdus en cas de défaillance.

Les compromis tels que ceux évoqués plus haut ne relèvent pas du choix des protocoles ASAP/SCTP; il s'agit exclusivement d'une décision de l'opérateur ou du fabricant: quelle quantité d'informations d'état peut être sauvegardée par une implémentation donnée et quelles commandes/options peuvent être offertes à l'opérateur?

Appendice I

Commande du mode de communication de contrôleur multipoint échantillon à terminal

I.1 Scénario A d'une conférence échantillon

Les extrémités A, B et C sont dans une conférence audiovisuelle répartie par multidiffusion. Le contrôleur multipoint (qui peut être l'un quelconque des nœuds) a décidé de placer les voies de média et de commande de média aux adresses de multidiffusion suivantes:

Flux	Adresse de multidiffusion
Audio pour toutes les extrémités	MCA1
Commande audio pour toutes les extrémités	MCA2
Vidéo à partir de l'extrémité A	MCA3
Données de commande vidéo au sujet de l'extrémité A	MCA4
Vidéo à partir de l'extrémité B	MCA5
Données de commande vidéo au sujet de l'extrémité B	MCA6
Vidéo à partir de l'extrémité C	MCA7
Données de commande vidéo au sujet de l'extrémité C	MCA8

I.2 Table des modes de communication envoyée à toutes les extrémités

Toutes les entrées de la table sont des commandes destinées aux extrémités pour l'ouverture d'une voie logique de transmission. Le paramètre **terminalLabel** n'est présent que lorsque l'entrée est particulière à une extrémité particulière dans la conférence.

```
ENTRÉE 1 – AUDIO & COMMANDE AUDIO POUR LA CONFÉRENCE
sessionID                       1
sessionDescription              Audio
dataType                        Capacité audio
mediaChannel                    MCA1
mediaControlChannel             MCA2

ENTRÉE 2 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD A
sessionID                       2
associatedSessionID             1
terminalLabel                   M/T pour A
sessionDescription              Vidéo pour le nœud A
dataType                        Capacité vidéo
mediaChannel                    MCA3
mediaControlChannel             MCA4

ENTRÉE 3 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD B
sessionID                       3
associatedSessionID             1
terminalLabel                   M/T pour B
sessionDescription              Vidéo pour le nœud B
dataType                        Capacité vidéo
mediaChannel                    MCA5
mediaControlChannel             MCA6
```

```
ENTRÉE 4 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD C
sessionID                       4
associatedSessionID             1
terminalLabel                   M/T pour C
sessionDescription              Vidéo pour le nœud C
dataType                        Capacité vidéo
mediaChannel                    MCA7
mediaControlChannel             MCA8
```

I.3 Scénario B d'une conférence échantillon

Les extrémités A, B et C sont raccordées à une conférence multipoint dont le flux audio est unidiffusé à partir de chaque extrémité puis est soumis à un mixage centralisé à partir des extrémités. Le contrôleur multipoint peut envoyer une unique commande de mode de communication à chaque extrémité ou envoyer le même message à toutes les extrémités si les entrées de la table sont identifiées par l'étiquette du point de destination. Pour cet exemple, on part de l'hypothèse que le même message est envoyé à toutes les extrémités.

Flux	Adresse de multidiffusion
Audio à partir de l'extrémité A	UCA1
Données de commande audio au sujet de l'extrémité A	UCA2
Audio à partir de l'extrémité B	UCA3
Données de commande audio au sujet de l'extrémité B	UCA4
Audio à partir de l'extrémité C	UCA5
Données de commande audio au sujet de l'extrémité C	UCA6
Vidéo à partir de l'extrémité A	MCA1
Données de commande vidéo au sujet de l'extrémité A	MCA2
Vidéo à partir de l'extrémité B	MCA3
Données de commande vidéo au sujet de l'extrémité B	MCA4
Vidéo à partir de l'extrémité C	MCA5
Données de commande vidéo au sujet de l'extrémité C	MCA6

I.4 Table des modes de communication envoyée à toutes les extrémités

Toutes les entrées de la table sont des commandes destinées aux extrémités pour l'ouverture d'une voie logique de transmission. Le paramètre **terminalLabel** n'est présent que lorsque l'entrée est particulière à une extrémité particulière dans la conférence.

```
ENTRÉE 1 – AUDIO & COMMANDE AUDIO POUR LE NŒUD A
sessionID                       1
sessionDescription              Audio
terminalLabel                   M/T pour A
dataType                        Capacité audio
mediaChannel                    UCA1
mediaControlChannel             UCA2

ENTRÉE 2 – AUDIO & COMMANDE AUDIO POUR LE NŒUD B
sessionID                       2
sessionDescription              Audio
terminalLabel                   M/T pour B
dataType                        Capacité audio
mediaChannel                    UCA3
mediaControlChannel             UCA4
```

```
ENTRÉE 3 – AUDIO & COMMANDE AUDIO POUR LE NŒUD C
sessionID                       3
sessionDescription              Audio
terminalLabel                   M/T pour C
dataType                        Capacité audio
mediaChannel                    UCA5
mediaControlChannel             UCA6

ENTRÉE 4 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD A
sessionID                       4
associatedSessionID             1
terminalLabel                   M/T pour A
sessionDescription              Vidéo pour le nœud A
dataType                        Capacité vidéo
mediaChannel                    MCA1
mediaControlChannel             MCA2

ENTRÉE 5 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD B
sessionID                       5
associatedSessionID             2
terminalLabel                   M/T pour B
sessionDescription              Vidéo pour le nœud B
dataType                        Capacité vidéo
mediaChannel                    MCA3
mediaControlChannel             MCA4

ENTRÉE 6 – VIDÉO & COMMANDE VIDÉO POUR LE NŒUD C
sessionID                       6
associatedSessionID             3
terminalLabel                   M/T pour C
sessionDescription              Vidéo pour le nœud C
dataType                        Capacité vidéo
mediaChannel                    MCA5
mediaControlChannel             MCA6
```

Appendice II

Procédures de réservation de ressources dans la couche Transport

II.1 Introduction

La présente Recommandation recommande l'utilisation de mécanismes de réservation de ressources dans la couche Transport afin de répondre aux prescriptions de qualité de service des flux vidéo et audio en temps réel. Bien que, par eux-mêmes, les mécanismes de réservation de ressources dans la couche Transport soient hors du domaine d'application de la présente Recommandation, la méthode générale et la coordination de ces mécanismes de couche Transport entre entités H.323 sont décrites dans le présent appendice de façon à éviter des problèmes d'interopérabilité.

Le présent appendice décrit l'emploi du protocole de réservation de ressources (RSVP, *resource reservation protocol*) en tant que mécanisme permettant d'assurer la qualité de service dans la couche Transport des réseaux en protocole IP. D'autres protocoles peuvent être utilisés mais les procédures de base définies dans le présent appendice devraient continuer à s'appliquer. Les participants à une conférence devraient être en mesure de signaler leurs intentions, leurs capacités et leurs exigences de manière normalisée et protocolaire. De plus, la séquence de signalisation des mécanismes de réservation de ressources doit toujours être spécifiée de manière que le délai d'établissement de la communication soit minimal.

Le protocole RSVP est le protocole de signalisation en couche Transport pour la réservation de ressources dans des réseaux de type IP non fiables. Au moyen du protocole RSVP, les extrémités H.323 peuvent réserver des ressources pour un certain flux de trafic en temps réel, en fonction des exigences de QS de ce flux. Seule la remise au mieux des paquets est possible si le réseau ne réussit pas à réserver les ressources requises ou si le protocole RSVP est absent.

II.2 Prise en charge de la QS pour la H.323

Lorsqu'une extrémité demande l'admission avec portier, il y a lieu qu'elle indique, dans le message ARQ, si elle possède ou non la capacité de réservation de ressources. Il appartient ensuite au portier, sur la base des informations qu'il reçoit de l'extrémité et des informations dont il dispose au sujet de l'état du réseau:

- soit pour permettre à l'extrémité d'appliquer son propre mécanisme de réservation pour sa session H.323;
- soit pour effectuer une réservation de ressources pour le compte de l'extrémité;
- ou pour déterminer qu'aucune réservation de ressources n'est nécessaire et que le principe du meilleur effort est suffisant.

Cette décision est acheminée jusqu'à l'extrémité dans le message ACF. L'extrémité doit accepter la décision du portier afin d'établir une communication.

Il y a lieu que le portier rejette une demande ARQ émise par une extrémité si celle-ci n'indique pas qu'elle possède la capacité de réservation de ressources et si le portier décide que la réservation de ressources doit être commandée par l'extrémité. Dans ce cas, il convient que le portier renvoie un message ARJ à l'extrémité.

Le champ spécifique qui permet d'offrir cette capacité dans la signalisation RAS H.225.0 est le champ **transportQOS**.

En plus du champ **transportQOS**, une extrémité doit également calculer et indiquer la largeur de bande qu'elle a actuellement l'intention d'utiliser sur toutes les voies de la communication. Il convient d'indiquer cette largeur de bande dans le champ **bandWidth** du message ARQ indépendamment de la décision, prise par l'extrémité, d'utiliser ou non le protocole RSVP. De plus, si les besoins en largeur de bande changent en cours de communication, l'extrémité devra signaler au portier la modification de ses besoins au moyen du message BRQ, indépendamment de la décision d'utilisation du protocole RSVP.

Les réservations par protocole RSVP ne peuvent être faites que par des entités du réseau qui se trouvent dans le trajet du flux média entre les extrémités. Il est possible, au moyen d'une signalisation d'appel acheminée par portier, de faire passer les flux médias par un portier. Cependant, les voies de médias seront la plupart du temps acheminées entre les extrémités sans passer par le portier. Si celui-ci décide d'acheminer les flux médias, les procédures à suivre devront être identiques à celles de la signalisation directe par protocole RSVP à partir des extrémités. Il est préférable que les réservations par protocole RSVP soient effectuées directement par les extrémités car cela permettra de réserver des ressources sur l'ensemble du trajet d'acheminement de la communication. L'utilisation du protocole RSVP par les extrémités H.323 sera examinée dans le présent appendice.

Entre autres caractéristiques du protocole RSVP, on peut citer les suivantes:

- le protocole RSVP prend en charge aussi bien les environnements de monodiffusion que les environnements de multidiffusion;
- le protocole RSVP est associé à des flux spécifiques (c'est-à-dire à des paires d'adresses de transport spécifiques);
- le protocole RSVP est à états conditionnels et s'adapte donc dynamiquement aux modifications de composition des groupes et aux changements d'itinéraires;

- le protocole RSVP est unidirectionnel;
- le protocole RSVP est orienté vers le récepteur, c'est-à-dire que c'est le destinataire du flux média qui effectue la réservation (échelonnable).

II.3 Rappel des bases du protocole RSVP

La description suivante portera sur l'utilisation du protocole RSVP dans les couches supérieures d'une simple conférence H.323.

Dans la Figure II.1, l'extrémité A souhaite envoyer un flux média à l'extrémité B. Elle doit donc ouvrir une voie logique vers B. La signalisation RSVP pour la réservation de ressources doit faire partie de la procédure d'ouverture de voie logique. L'extrémité A provoquera l'envoi à B de messages RSVP de type *Path*. Ces messages vont traverser des routeurs et laisseront une information d'état concernant leur progression vers B. Les messages *Path* contiennent les adresses complètes d'origine et de destination du flux ainsi qu'une caractérisation du trafic qui sera envoyé par l'origine. L'extrémité B utilisera les informations du message *Path* pour formuler la demande RSVP de type *Resv* pour toute la longueur de l'itinéraire. Les messages *Resv* contiennent la réservation proprement dite. Ils seront généralement identiques aux messages de spécification du trafic contenus dans le message *Path*.

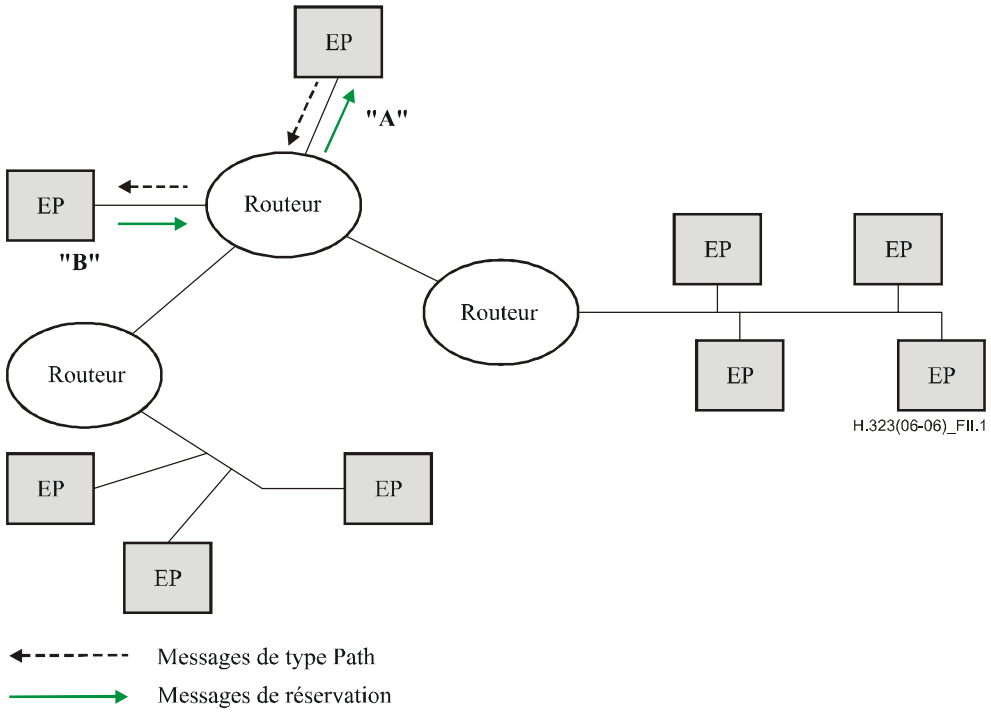


Figure II.1/H.323 – Réservation de ressources pour une connexion point à point

La Figure II.2 représente une conférence multipoint. Les messages *Path* sont utilisés de la même façon que dans le cas plus simple d'une communication point à point. Il y convient de noter que les demandes *Resv* sont regroupées par les routeurs afin d'empêcher que des demandes de réservation redondantes passent en amont.

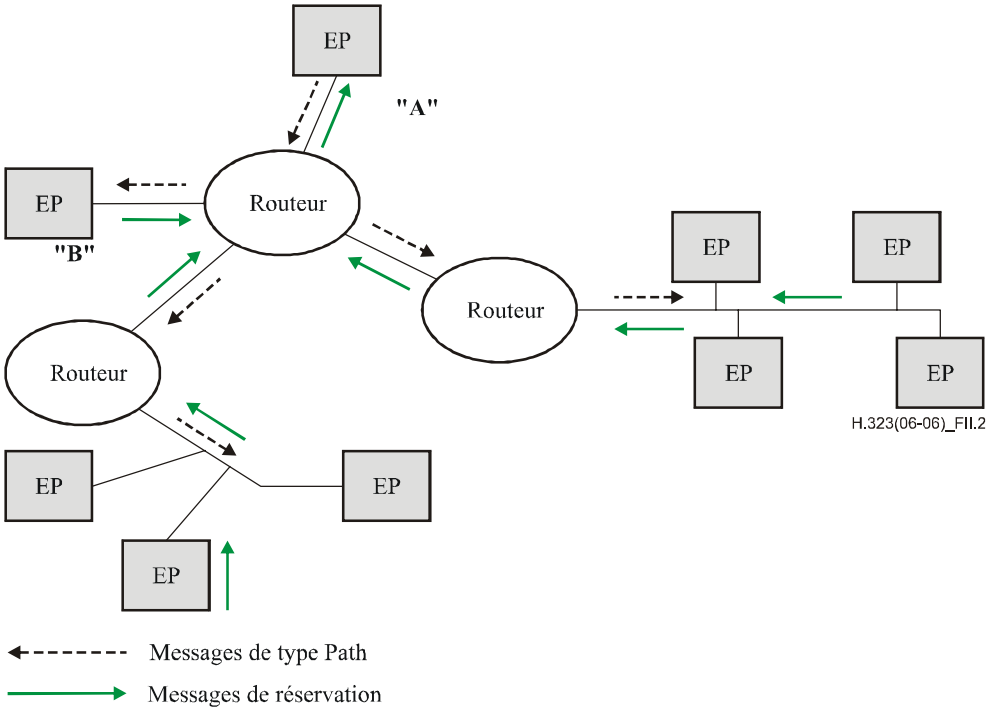


Figure II.2/H.323 – Réservation de ressources pour une connexion point à multipoint

Les messages *Path* doivent toujours contenir les adresses complètes de destination et d'origine ainsi qu'une spécification du trafic. Les messages *Resv* contiennent les paramètres de réservation et le service requis. Les messages *Path* et *Resv* pour un flux de trafic donné doivent normalement être envoyés dans le cadre de la procédure d'ouverture de voie logique (**openLogicalChannel**) pour ce flux particulier. La réservation doit normalement être libérée lors de la procédure de fermeture de voie logique (**closeLogicalChannel**), au moyen des messages *PathTear* et *ResvTear*.

On notera que les messages Path et Resv du protocole RSVP utilisent la même paire adresse IP/accès que le flux média à acheminer entre les extrémités. En d'autres termes, ces messages doivent être extraits par filtrage du flux média par les extrémités. Cela ne concerne pas les extrémités qui effectuent un filtrage de messages UDP puisque les messages RSVP ne sont pas des messages UDP. Cela étant, l'expéditeur d'un flux média ne doit cependant pas utiliser le protocole RSVP lorsque le récepteur ne possède pas la capacité correspondante. Les capacités RSVP sont échangées dans le cadre des procédures d'échange de capacités et d'ouverture de voie logique.

Le protocole RSVP ne s'applique qu'à la signalisation. Il peut répondre aux exigences des participants à une conférence H.323 en termes de qualité de service en association avec les services QS appropriés (par exemple QS garantie ou service à régulation de charge), avec des mécanismes de coordination (comme la mise en files d'attente logiques pondérée) et avec le module de commande d'admission en fonction de la politique (par exemple avec le gestionnaire de la politique locale). Le protocole RSVP permet de répondre aux exigences des participants aux conférences H.323, en termes de QS. Le protocole RSVP est également conçu pour des liaisons point à point. Si un itinéraire traverse une liaison partagée, le protocole RSVP invoque le mécanisme de réservation de ressources approprié au support spécifique qui est partagé, par exemple le mécanisme de gestion de largeur de bande en sous-réseau (SBM, *subnet bandwidth management*), dans le cas des réseaux Ethernet. Tous les mécanismes mentionnés dans le présent paragraphe sont totalement commandés dans le cadre du protocole RSVP. La signalisation RSVP suffit donc aux besoins d'une extrémité conforme à la Rec. UIT-T H.323.

II.4 La phase d'échange de capacités H.245

Au cours de la phase d'échange de capacités H.245, chaque extrémité indique ses capacités d'émission et de réception à l'autre point. La capacité de QS (**qOSCapability**) fait partie de cet échange, mais elle n'est pas spécifique du flux. Les paramètres du protocole RSVP, s'ils sont spécifiés dans la capacité de QS, représenteront donc un agrégat pour tous les flux (à émettre ou à recevoir). Ces paramètres n'auront aucune utilité pour l'autre extrémité. La seule information associée au protocole RSVP qu'une extrémité devrait acheminer jusqu'à l'autre point dans l'ensemble de capacités est donc de savoir si cette extrémité possède ou non la capacité RSVP.

Pour signaler la capacité RSVP, une extrémité doit indiquer les champs appropriés du mode de QS disponible (**qOSMode**) à l'intérieur de l'unité PDU de capacité, au cours de l'échange de capacités. Les extrémités qui ne reçoivent pas de capacités RSVP en provenance de l'extrémité réceptrice ne doivent pas utiliser le protocole RSVP lors de l'ouverture de voies logiques.

II.5 Ouvertures de voies logiques et établissement de réservations

Le présent paragraphe décrira les étapes à suivre pour ouvrir une voie logique H.245 et pour réserver des ressources pour un flux de trafic donné. Les réservations ne sont établies que si les deux extrémités indiquent qu'elles ont activé le protocole RSVP au cours de l'échange de capacités. Seul le cas d'une connexion point à point sera examiné. Celui d'une connexion point à multipoint (multidiffusion) sera examiné au § II.7.

L'expéditeur doit spécifier, dans le champ **qOSCapability** du message **openLogicalChannel**, les paramètres de protocole RSVP pour le flux à transmettre, ainsi que les services intégrés que cet expéditeur prend en charge. Dans le cas d'un flux point à point, l'expéditeur ne spécifie pas d'identificateur d'accès récepteur dans le message **openLogicalChannel**. Cet identificateur sera sélectionné par le destinataire après réception du message **openLogicalChannel** et sera renvoyé à l'expéditeur dans le message **openLogicalChannelAck**. Ce n'est qu'ensuite que l'expéditeur pourra créer une session de protocole RSVP pour ce flux et émettre des messages RSVP de type *Path*. (La création d'une session de protocole RSVP pour un flux donné implique que l'extrémité se fasse enregistrer dans le protocole RSVP pour recevoir notification de l'arrivée de messages pouvant avoir une incidence sur l'état de la réservation RSVP pour ce flux.) Le récepteur possède alors suffisamment d'informations pour créer une session de protocole RSVP pour le même flux avant d'envoyer le message **openLogicalChannelAck**. Les informations nécessaires pour créer une session RSVP et pour commencer le traitement RSVP sont les suivantes: l'adresse IP du récepteur en cas de connexion point à point ou l'adresse IP de multidiffusion à un groupe en cas de connexion point à multipoint; l'identificateur d'accès récepteur; et le protocole (toujours le protocole UDP en cas de flux audio et vidéo H.323 sur réseaux IP).

Il se peut qu'un récepteur ne souhaite pas commencer à recevoir des paquets de flux avant que les réservations aient été effectuées par le protocole RSVP. A cette fin, le récepteur peut donner la valeur "Vrai" au champ booléen **flowcontrolToZero** du message **openLogicalChannelAck** afin d'indiquer qu'il ne souhaite pas recevoir de trafic sur cette voie avant l'achèvement des réservations de ressources. Lorsqu'un expéditeur reçoit un message **openLogicalChannelAck** dont le champ **flowControlToZero** est mis à la valeur "Vrai", cet expéditeur ne doit émettre aucun trafic sur cette voie.

Lorsque le destinataire commence à recevoir les messages *Path* de l'expéditeur, il doit normalement commencer à envoyer les messages *Resv* du protocole RSVP. Lorsque le destinataire reçoit un message *ResvConf* du protocole RSVP qui confirme le fait que les réservations ont été établies, ce destinataire peut envoyer à l'expéditeur une commande de débit **flowControlCommand** supprimant toute restriction quant au débit du flux en trafic, c'est-à-dire annulant l'effet du précédent champ **flowcontrolToZero** contenu dans le message **openLogicalChannelAck**. Lorsque l'expéditeur reçoit la commande **flowControlCommand**, il commence à envoyer les paquets.

On notera que le message *ResvConf*, ainsi que, par analogie, tous les autres messages du protocole RSVP sont transmis en mode non fiable. Par conséquent, ces messages peuvent être retardés sinon perdus. Une extrémité devra tenir compte de ce fait et devra régler les temporisateurs sur une valeur appropriée lors de l'attente d'une confirmation *ResvConf*. Si l'extrémité détecte l'expiration de la temporisation avant d'avoir reçu le message *ResvConf*, la mesure à prendre relève des vendeurs individuels de cette extrémité.

Le comportement d'une extrémité si des réservations par protocole RSVP échouent à un endroit quelconque lors d'une communication H.323 n'est pas spécifié dans le présent appendice et est laissé aux soins des vendeurs individuels. Toutefois, si une réservation RSVP échoue et que l'extrémité réceptrice décide que le niveau de service au meilleur effort n'est pas acceptable, cette extrémité peut demander la fermeture de sa voie logique, au moyen du message **requestChannelClose**. Le champ de cause de fermeture (**closeReason**) dans le message **requestChannelClose** permet au destinataire de signaler à l'expéditeur que la réservation RSVP a échoué. En plus de l'indication d'échec, le message **requestChannelClose** inclut la capacité QS (**qOSCapability**) qui peut être utilisée par le destinataire pour indiquer à l'expéditeur les ressources qui sont réellement disponibles à cet instant sur l'itinéraire entre l'expéditeur et le récepteur. A ce point, l'expéditeur peut décider de tenter une réouverture de la voie logique avec un codec et/ou un format de données ayant une largeur de bande inférieure, puis relancer la procédure d'ouverture de voie logique.

Toutes les demandes de réservation RSVP *Resv* doivent utiliser le même style de réservation (**filtre fixe**) pour les raisons suivantes:

- les styles à filtre partagé se ramènent à un filtre fixe en cas de communication point à point;
- différents styles de réservation ne peuvent pas être associés dans le réseau pour la même session. Si par exemple, dans une communication multipoint, certains des récepteurs demandent des réservations à filtre fixe tandis que les autres demandent des réservations à filtre explicitement partagé, les réservations de l'un de ces deux types échoueront;
- les réservations partagées, créées par des styles de filtrage générique ou explicitement partagé, sont appropriées aux applications multidiffusées dans lesquelles de multiples sources de données ne sont pas susceptibles d'émettre simultanément. Dans les communications H.323 multipoints réparties, il n'existe aucun mécanisme ne permettant qu'à une seule source d'émettre à un instant donné. Par ailleurs, dans les communications H.323 multipoints centralisées, le pont de conférence est la seule source multidiffusée. Les styles de réservation par filtrage partagé ne conviennent ni à l'un ni à l'autre de ces cas.

Il appartient aux vendeurs d'extrémité de choisir la QS (garantie ou à régulation de charge) applicable aux services intégrés. Toute extrémité H.323 ayant activé le protocole RSVP doit cependant prendre en charge le service à régulation de charge comme plus petit dénominateur commun. Cette prescription est nécessaire pour éviter des problèmes d'interfonctionnement pouvant se poser avec des extrémités H.323 ayant activé le protocole RSVP mais ne prenant pas en charge un niveau commun de QS pour les services intégrés.

La Figure II.3 montre la séquence des messages en cas de réservation RSVP correctement effectuée.

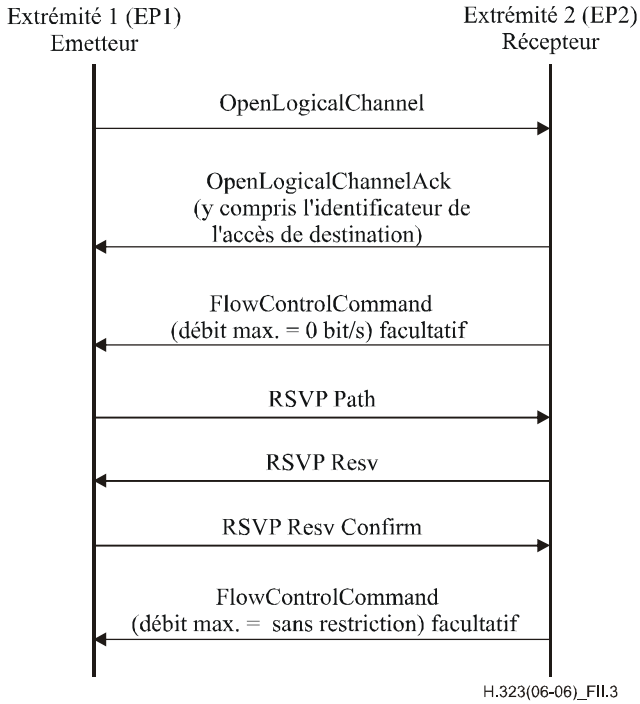


Figure II.3/H.323 – Séquence de messages pour l'ouverture d'une voie logique unidiffusée avec réservation RSVP

II.6 Clôture de voie logique et libération des réservations

Avant d'envoyer un message **closeLogicalChannel** pour un flux de trafic donné, une extrémité émettrice doit envoyer un message *PathTear* si une session de protocole RSVP a déjà été créée pour ce flux. Lorsqu'une extrémité réceptrice reçoit un message **closeLogicalChannel** pour un flux de trafic donné, elle doit envoyer un message *ResvTear* si une session de protocole RSVP a déjà été créée pour ce flux.

II.7 Réservation de ressources pour voies logiques H.323 multidiffusées

La procédure H.245 d'ouverture de voie logique **openLogicalChannel** s'applique à des connexions point à point même si le flux de trafic en cause est multidiffusé. Pour que l'extrémité destinataire commence à recevoir les paquets d'un flux multidiffusé, cette extrémité doit cependant se joindre au groupe de multidiffusion et se faire connecter à l'arbre de multidiffusion de la source. Lorsqu'un destinataire reçoit un message **openLogicalChannel**, il se joint au groupe et à l'arbre de multidiffusion au moyen des procédures normalisées du protocole IGMP (*Internet group management protocol*). L'entrée par protocole IGMP (au moyen du message IGMP *Report*) s'effectue avant le renvoi à l'expéditeur, par le destinataire, d'un acquittement **openLogicalChannelAck**.

En cas de flux multidiffusé, l'expéditeur spécifie l'identificateur d'accès récepteur dans le message **openLogicalChannel** au lieu de recevoir cet identificateur dans le message **openLogicalChannelAck**.

Le destinataire peut donner la valeur VRAI au champ **flowControlToZero** du message **openLogicalChannelAck**, comme dans le cas des connexions unidiffusées. L'expéditeur (extrémité dans une conférence répartie ou pont dans une conférence centralisée) devrait décider de ne pas interrompre le flux de données passant par la voie ouverte, s'il détecte que cette interruption pourrait avoir une incidence sur d'autres destinataires du même groupe de multidiffusion, qui reçoivent déjà

ce flux. En conséquence, dans le cas d'une multidiffusion, le destinataire peut recevoir initialement les données au niveau de qualité du meilleur effort, en attendant que les réservations soient établies par le protocole RSVP.

La Figure II.4 montre la séquence de messages requise pour ouvrir une voie logique, se joindre à l'arbre de multidiffusion et réserver des ressources pour un flux multidiffusé.

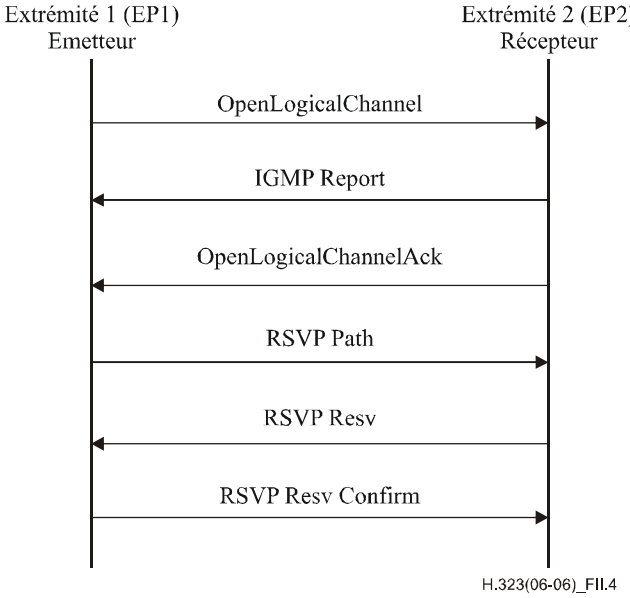


Figure II.4/H.323 – Séquence des messages pour l'ouverture d'une voie logique multidiffusée avec protocole RSVP

Avant d'émettre un message **closeLogicalChannel** pour un certain flux multidiffusé, il y a lieu qu'une extrémité émettrice envoie un message RSVP de type *PathTear* si la voie logique à fermer est la dernière à acheminer ce flux multidiffusé et si une session de protocole RSVP a déjà été créée pour ce flux. Lorsqu'une extrémité destinataire reçoit un message **closeLogicalChannel** pour un flux multidiffusé donné, il y a lieu que cette extrémité envoie un message RSVP *ResvTear* et un message IGMP *Leave* si une session RSVP a déjà été créée pour ce flux.

II.8 Protocole RSVP synchronisé

Le protocole RSVP synchronisé est défini comme étant le processus de réservation de ressources qui s'applique avant la transition à la phase d'alerte de l'appel. Les deux paragraphes suivants décrivent les détails de la synchronisation RSVP, respectivement avec et sans utilisation de la procédure FastConnect (connexion rapide). Le présent paragraphe introduit la notion générale de liste rangée par ordre de priorité des niveaux de qualité QS, exprimés par chaque extrémité à partir de laquelle un nouvel ensemble de niveaux de qualité de service, *D*, est calculé. Cet ensemble *D* calculé correspond à l'intersection des deux ensembles **QOSMode** préférés. Les deux extrémités peuvent essayer d'établir des réservations RSVP sur la base d'un niveau de qualité de service choisi dans l'ensemble calculé qui commence par le niveau QS préféré en premier.

Lors du calcul de l'ensemble QS, l'extrémité appelée supprime la phase d'alerte de l'appel jusqu'à ce que les réservations soient établies dans les deux sens. Dès l'établissement correct d'une réservation, le processus d'alerte peut s'engager et l'établissement de l'appel reprend. En cas de dérangements, le plus bas niveau de QS figurant dans l'ensemble calculé est examiné. Si ce niveau est indiqué comme étant "au mieux", les procédures d'établissement d'appel reprennent; sinon, l'appel est libéré. L'envoi d'une structure **QoSCapability** avec un élément **QOSMode** vide dans le bloc **rsvpParameters** doit indiquer un niveau de QS "au mieux". La séquence **QOSMode** est classée en

priorités décroissantes par l'élément **QOSMode** du bloc **rsvpParameters**. Le niveau **GuaranteedQoS** est le plus élevé qu'une extrémité puisse recevoir et le niveau "au mieux" est moins élevé. Si le niveau QS préféré que l'extrémité appelante souhaite recevoir est supérieur au niveau "au mieux", il y a lieu que cette extrémité lance les procédures RSVP en analysant les messages de type PATH issus de l'extrémité appelée.

Celle-ci doit examiner la séquence de structures **QoSCapability** si elle est présente, puis la comparer à son propre ensemble préféré de niveau QS sur la base de la séquence **QOSMode**. Elle calcule ensuite un nouvel ensemble 'D' de niveaux QS fondé sur la séquence **QOSMode**, qui représente l'intersection des niveaux QS issus des ensembles préférés des deux extrémités. Ce nouvel ensemble indique les différents niveaux QS par ordre de priorité, en fonction des modes QS qui sont pris en charge par les deux extrémités. Par exemple, si l'ensemble préféré de niveaux QS de l'extrémité appelante est {**GuaranteedQOS**, **ControlledLoad**} et si celui de l'extrémité appelée est {**ControlledLoad**, "au mieux"}, l'ensemble calculé par réunion logique (intersection) sera {**ControlledLoad**}. Sur la base des niveaux QS préférés des deux extrémités, différents cas généraux sont possibles. Ces différents cas et le traitement d'appel correspondant sont décrits dans le Tableau II.1.

Tableau II.1/H.323 – Traitement des appels pour différentes classes de qualité de service

Scénario de QS	Exemple	Traitement d'appel
1) L'ensemble QS calculé 'D' est vide	Ensemble préféré de l'extrémité appelante: {GQ} Ensemble préféré de l'extrémité appelée: {CL,BE} Ensemble QS calculé 'D': {}	L'extrémité appelée doit libérer l'appel
2) L'ensemble QS calculé 'D' ne comporte qu'un seul niveau QS: "au mieux"	Ensemble préféré de l'extrémité appelante: {BE} Ensemble préféré de l'extrémité appelée: {CL,BE} Ensemble QS calculé 'D': {BE}	L'extrémité appelée ne doit pas lancer de procédures RSVP mais doit poursuivre les procédures d'établissement d'appel
3) L'ensemble QS calculé 'D' comporte au moins 1 niveau QS supérieur au niveau "au mieux"	Ensemble préféré de l'extrémité appelante: {GQ,CL,BE} Ensemble préféré de l'extrémité appelée: {CL,BE} Ensemble QS calculé 'D': {CL,BE}	L'extrémité appelée doit supprimer le processus d'alerte et essayer le protocole RSVP synchronisé. Les procédures détaillées sont décrites dans les paragraphes pertinents ci-après.
BE au mieux (*best effort*). CL charge commandée (*controlledLoad*). GQ niveau de QS garanti (*guaranteed QoS*).		

En cas de défaillance dans les procédures RSVP, l'extrémité appelée doit examiner le prochain niveau QS préféré, s'il est présent dans l'ensemble calculé *D*. Si un niveau QS autre que "au mieux" existe, l'extrémité appelée doit normalement réinitialiser les réservations RSVP avec ce niveau de qualité. En cas de défaillances successives, il est possible de relancer les procédures de réservation RSVP pour tous les niveaux QS (autres que "au mieux") dans l'ensemble calculé. A l'expiration de la temporisation de réservation à l'extrémité appelée ou, si celle-ci ne parvient pas à établir de réservations RSVP avec le plus bas niveau QS autre que "au mieux" dans l'ensemble calculé, cette extrémité appelée doit libérer l'appel. Sinon, l'établissement d'appel est repris avec le niveau QS "au mieux". Les défaillances de réservation et l'expiration de la temporisation de réservation sont traitées de façon analogue à l'extrémité appelante.

Les deux paragraphes suivants traitent du protocole RSVP synchronisé, avec ou sans procédure FastConnect, sur la base du concept de la liste **QOSMode** rangée par ordre de priorité des niveaux.

II.8.1 Synchronisation RSVP sans utilisation de la procédure FastConnect

Une extrémité appelante qui souhaite réserver des ressources au moyen du protocole RSVP sans établir d'appel par la procédure FastConnect doit, au préalable, inclure une adresse H.245 dans le message Setup. De même, une extrémité appelée qui souhaite réserver des ressources RSVP avant l'achèvement de l'établissement d'appel doit extraire, du message Setup entrant, l'adresse H.245 de l'extrémité appelante, si elle existe. Ensuite, l'extrémité appelée doit établir la voie de commande H.245 et commencer les procédures H.245. Avant que les procédures H.245 et RSVP soient achevées, l'extrémité appelée ne doit pas poursuivre la phase H.225.0 de l'établissement d'appel. Il est toutefois recommandé que l'extrémité appelée renvoie un message Call Proceeding à l'extrémité appelante afin d'éviter l'expiration d'une éventuelle temporisation H.225.0 du côté origine.

Si l'extrémité appelée souhaite essayer le protocole RSVP synchronisé mais que l'extrémité appelante n'inclue pas son adresse H.245 dans le message Setup entrant, l'extrémité appelante doit partir du principe que l'extrémité d'origine n'acceptera ni ne lancera les procédures RSVP synchronisées. Il appartiendra ensuite à l'extrémité appelée de décider de la suite à donner sur la base du mode QS calculé comme indiqué au § II.8. De même, si l'extrémité appelante souhaite essayer le protocole RSVP synchronisé et a inclus son adresse H.245 dans le message Setup, mais que l'extrémité appelée n'a pas réussi à établir la voie de commande H.245 et a relancé les procédures H.225.0, il appartiendra à l'extrémité appelante de décider de la suite à donner sur la base du mode QS calculé comme indiqué dans le Tableau II.1.

Sinon, c'est-à-dire si l'extrémité appelante a inséré son adresse H.245 dans le message Setup et que l'extrémité appelée ait établi la voie de commande H.245, les procédures H.245 progresseront normalement par détermination de la relation maître-esclave et échange de capacités.

Au cours de l'échange de capacités H.245, les extrémités qui souhaitent lancer le protocole RSVP sont appelées à insérer dans le champ **qOSCapabilities** une séquence de capacités (dans le cadre de l'élément **transportCapability** de la structure **H2250Capability**), dans l'ordre de priorité indiqué par l'élément **qosMode** (p. ex. **guaranteedQOS**, **controlledLoad**) de la structure **rsvpParameters**.

De même, lors de l'ouverture de voies logiques utilisant le protocole H.245, chaque extrémité doit spécifier les paramètres RSVP du flux à transmettre dans le champ **qOSCapability** du message **openLogicalChannel**.

Dès réception d'un message OLC de son homologue et à condition que celle-ci ait indiqué, au cours de l'échange de capacités, qu'elle a activé le protocole RSVP, l'extrémité doit commencer à détecter les messages Path entrants. Lorsqu'elle reçoit un message Path, l'extrémité doit y répondre par l'envoi d'un message Resv dans le flux de réception.

Dès réception d'un acquittement par son homologue du message OLC, l'extrémité doit commencer à envoyer des messages Path à son homologue dans son flux d'émission. Les procédures RSVP sont correctement effectuées lorsque l'extrémité a reçu une confirmation de réservation en réponse à son envoi du message Resv et un message Resv en réponse à son message Path. Si plusieurs flux sont en jeu (p. ex. voix, vidéo et données), l'extrémité doit attendre la confirmation de réservation pour tous les flux demandant un niveau de QS sur la base du protocole RSVP.

Il est recommandé que l'extrémité arme un temporisateur pendant un bref intervalle (p. ex. 5 ou 6 secondes) après avoir essayé le protocole RSVP. Si le temporisateur expire avant la fin des réservations RSVP, l'extrémité peut déterminer la meilleure suite à donner.

Si les procédures RSVP (et donc H.245) ont été correctement effectuées avant l'expiration du temporisateur, l'extrémité appelée peut reprendre les procédures normales d'établissement en renvoyant un message d'alerte à l'extrémité appelante. Si cependant la tentative de réserver des

ressources RSVP échoue, il appartient à chaque extrémité de déterminer la meilleure suite à donner sur la base de l'ensemble **QOSMode** calculé, comme décrit au § II.8. De toute façon, il est recommandé que, si l'appel a atteint la phase d'alerte et que les réservations RSVP aient échoué, il soit permis que l'appel progresse.

La Figure II.5 décrit la modification du flux d'appel pour un protocole RSVP synchronisé correctement, sans utilisation de la procédure FastConnect.

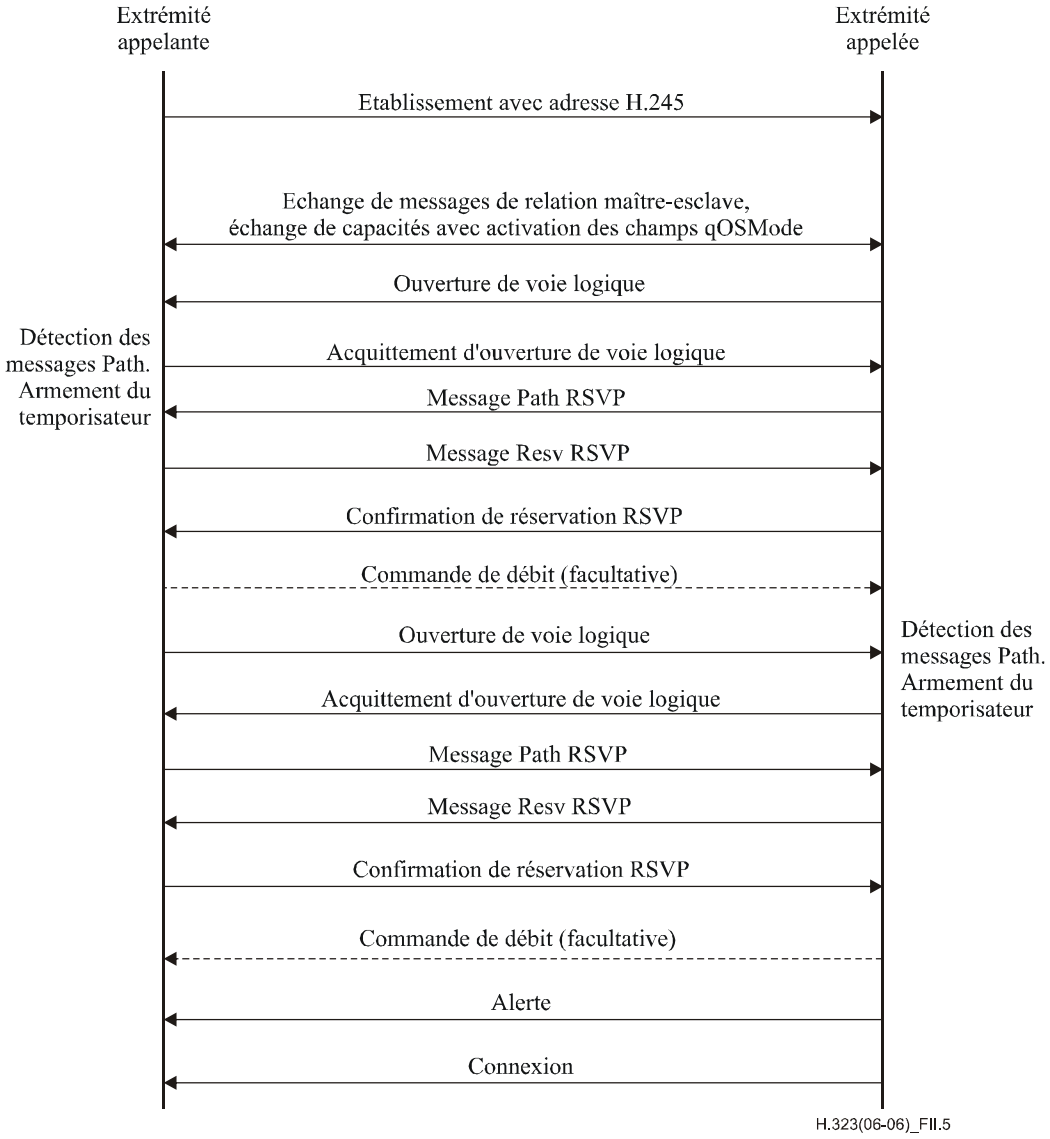


Figure II.5/H.323 – Synchronisation RSVP sans utilisation de la procédure FastConnect

II.8.2 Synchronisation RSVP avec utilisation de la procédure FastConnect

Le présent paragraphe décrit la synchronisation des procédures d'établissement d'appel FastConnect avec les procédures de réservation RSVP afin d'éliminer le transport de tonalités de sonnerie dans la bande avant l'établissement des réservations.

Une extrémité appelante qui souhaite utiliser le protocole RSVP dans une procédure FastConnect doit envoyer une séquence de structures **QoSCapability** rangées par priorité dans les structures **OpenLogicalChannel** contenues dans l'élément **fastStart** du message Setup.

Dès réception du message Setup de la procédure FastConnect, l'extrémité appelée doit calculée l'ensemble **QOSMode** par le mécanisme décrit dans le Tableau II.1. En partant du principe que

l'ensemble calculé contient un niveau valide (c'est-à-dire une intersection autre que le niveau "au mieux"), l'extrémité appelée doit répondre au message Setup issu de l'extrémité appelante par l'envoi d'un élément **fastStart** ne contenant que les capacités QS indiquées dans l'ensemble QS calculé. L'élément **fastStart** doit être envoyé dès que possible (p. ex. dans un message Call Proceeding) afin d'effectuer la réservation de ressource. L'ensemble de l'extrémité appelante sera un sous-ensemble de la liste envoyée par cette extrémité dans les structures **OpenLogicalChannel**. Il sera, de même, une séquence de priorités décroissantes selon **QOSMode**. Chaque champ **QoSCapability** inclus dans la structure **OpenLogicalChannel** du message de réponse indique une acceptation, par l'extrémité appelée, du niveau QS correspondant. Les structures **OpenLogicalChannel** contenues dans l'élément **fastStart** contiennent également des informations sur les accès médias utilisés à l'extrémité appelée.

Celle-ci doit lancer les procédures RSVP par l'envoi d'un message PATH à son homologue dans le flux d'émission. Par ailleurs, l'extrémité peut utiliser un temporisateur de réservation qui représentera la durée totale impartie à l'établissement de réservations RSVP synchronisées à tout niveau QS (autre que le niveau "au mieux") de l'ensemble calculé. L'extrémité appelée doit également répondre à un message PATH entrant par un message RESV dans le flux de réception. Noter que l'extrémité appelée doit normalement supprimer la phase d'alerte de l'appel et ne pas envoyer de message Alerting à l'extrémité appelante tant que les réservations ne sont pas établies dans les deux sens. Une fois les procédures RSVP établies, l'extrémité appelée doit reprendre les procédures H.225 d'établissement d'appel.

Lorsque l'extrémité appelante reçoit l'élément **fastStart**, elle doit extraire les informations relatives aux accès médias contenues dans la structure **OpenLogicalChannel**. Elle doit également enregistrer la liste ordonnée par priorité de capacités QS **QoSCapabilities**, envoyée par l'extrémité appelée. L'extrémité appelante doit commencer à envoyer des messages PATH à son homologue dans le flux d'émission. De même, lorsqu'elle reçoit un message PATH issu de l'extrémité appelée, l'extrémité appelante doit répondre par un message RESV dans le flux de réception. L'extrémité appelante peut armer un temporisateur de réservation qui représentera la durée totale impartie à l'établissement des réservations RSVP synchronisées.

L'établissement de réservations RSVP est considéré comme correctement effectué lorsque l'extrémité appelée reçoit un message RESV en réponse à son message PATH et un message RESV CONFIRM en réponse à son message RESV. Dès que les procédures RSVP sont correctement effectuées, l'extrémité appelée doit arrêter le temporisateur de réservation et reprendre les procédures d'établissement d'appel. Elle envoie ensuite les messages Alerting/Connect à l'extrémité appelante. La Figure II.6 décrit le flux d'appel pour une communication FastConnect correctement synchronisée.

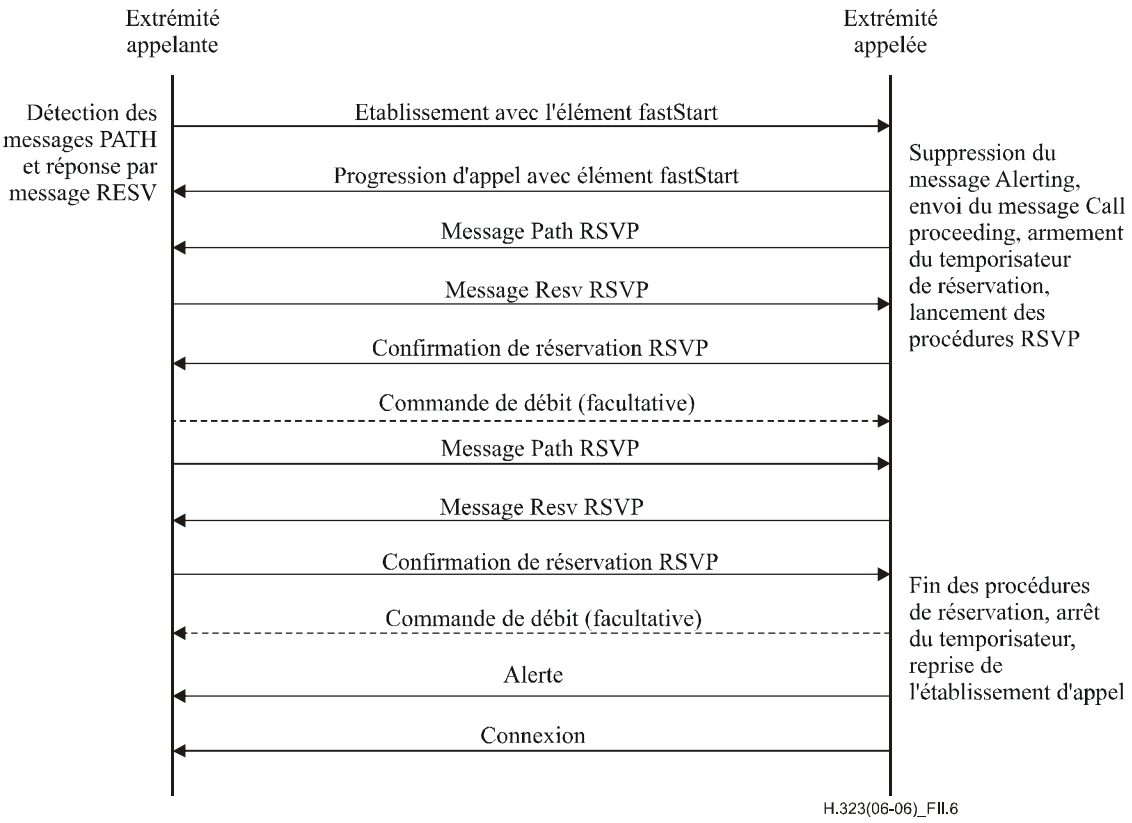


Figure II.6/H.323 – Synchronisation RSVP avec utilisation de la procédure FastConnect

En cas de défaillance du protocole RSVP, l'extrémité appelée agira conformément à l'ensemble **QOSMode** calculé, comme décrit au § II.8.

Appendice III

Localisation d'utilisateur par portier

III.1 Introduction

Le présent appendice donne des exemples de la façon dont un portier/procurateur peut implémenter des services de localisation d'utilisateur. Ces services dépendent de l'utilisation, par le portier, du modèle de signalisation d'appel avec routage par portier.

III.2 Signalisation

Dans le scénario de la Figure III.1, le portier implémente un service de "transfert sur non-réponse". L'extrémité 1 appelle l'extrémité 2 en faisant passer la voie de signalisation d'appel par le portier. S'il n'y a pas de réponse à l'issue d'une certaine temporisation, le portier transfère l'appel vers une autre extrémité. Les messages (1) à (5) montrent que le portier tente d'établir un appel entre les extrémités 1 et 2. Dans cet exemple, l'extrémité 2 ne répond pas de sorte que le portier libère l'appel vers l'extrémité 2 en envoyant un message de libération terminée Release Complete (6). Le portier tente ensuite d'établir l'appel avec l'extrémité 3 en envoyant un message Setup Setup (7). Lorsque

l'extrémité 3 répond à l'appel par le message de connexion Connect (9), le portier fait suivre le message de connexion Connect (10) à l'extrémité 1.

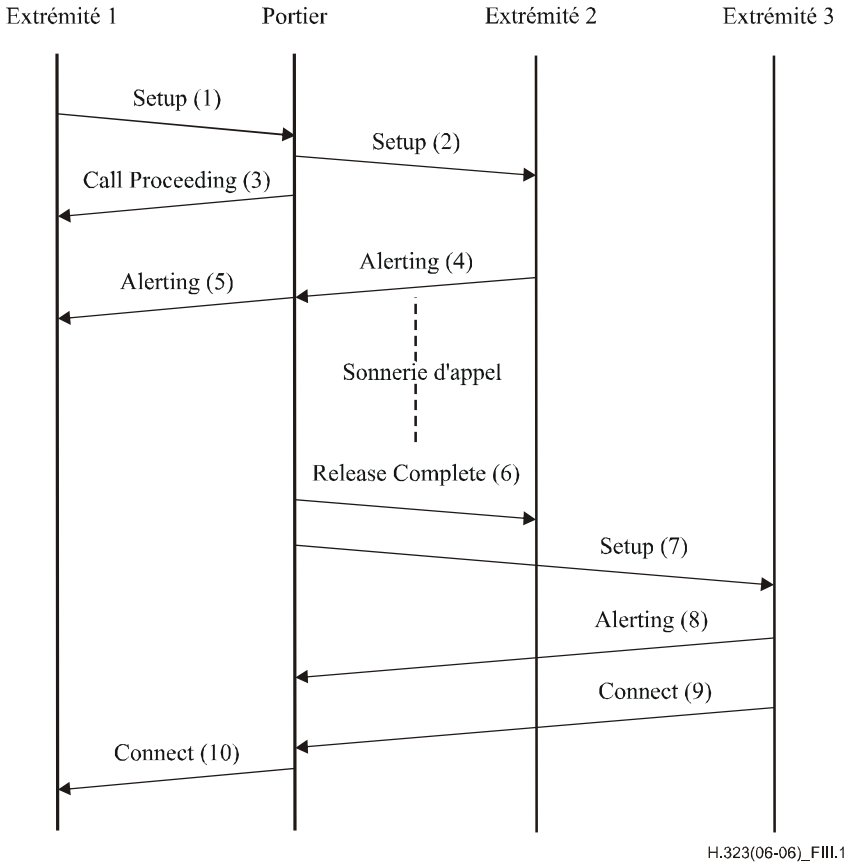


Figure III.1/H.323 – Exemple de localisation d'utilisateur par signalisation d'appel H.225.0 (la signalisation RAS n'est pas représentée pour plus de clarté)

Une méthode analogue peut être utilisée pour fournir le service de "transfert sur occupation". Dans ce cas, l'extrémité 2 renverra un message Release Complete indiquant qu'il est occupé. Le portier tentera alors d'établir l'appel avec l'extrémité 3.

Dans le scénario représenté sur la Figure III.2, le portier tente d'établir le contact avec les extrémités 2 et 3 simultanément en envoyant des messages d'établissement Setup (2) et (3). Dans cet exemple, l'utilisateur situé à l'extrémité 3 répond par l'envoi du message de connexion Connect (8). Le portier fait suivre le message Connect (9) jusqu'à l'extrémité 1 puis libère l'appel tenté vers l'extrémité 2 au moyen du message de libération terminée Release Complete (10). Il y lieu que le portier ne tienne pas compte d'un éventuel message Connect reçu de l'extrémité 2, arrivant après le message Connect (9) issu de l'extrémité 3, de façon qu'une seule communication soit établie.

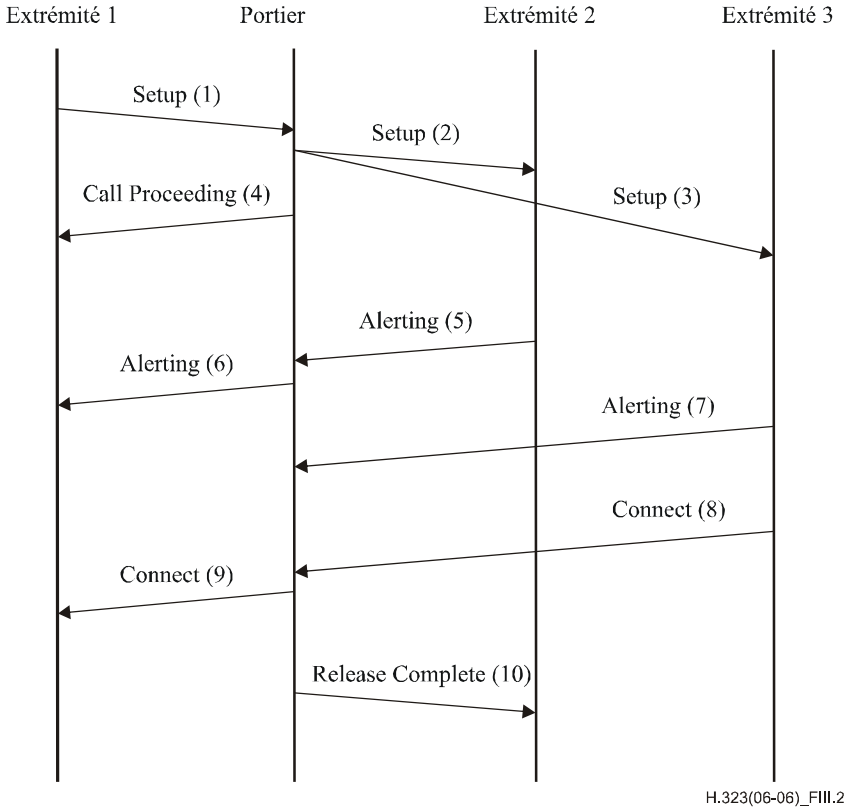


Figure III.2/H.323 – Exemple de localisation d'utilisateur par signalisation d'appel H.225.0 (la signalisation RAS n'est pas représentée pour plus de clarté)

On notera que si le portier applique cet algorithme de localisation d'utilisateur, il ne devrait pas transmettre le champ **h245Address** dans l'un quelconque des messages d'acquittement d'établissement, d'appel en cours et d'alerte issus de l'extrémité 2 ou 3 vers l'extrémité 1, car cela pourrait donner un résultat erroné.

Appendice IV

Voies logiques de remplacement avec ordre de priorité de signalisation sur une connexion H.245

IV.1 Introduction

Le présent appendice décrit une méthode simple permettant de signaler d'autres voies logiques possibles. Aucun changement au niveau du codage ou de la sémantique n'est requis.

La présente méthode est subordonnée à l'acheminement garanti ordonné qui est assuré par le protocole TCP: en conséquence elle s'applique à la signalisation H.245 canalisée ou non. La première est en outre subordonnée à l'ordre de traitement garanti lorsque plusieurs messages H.245 sont canalisés dans un seul message de signalisation d'appel H.225.0.

IV.2 Signalisation

Toutes les autres voies logiques possibles sont identifiées par l'utilisation d'un numéro **forwardLogicalChannelNumber** commun dans des messages **openLogicalChannel**, à raison

d'une possibilité par message. Les messages peuvent être envoyés via le tunnel H.245 (un ou plusieurs messages OLC par message de signalisation d'appel) ou via une connexion H.245 séparée. Les autres voies logiques possibles sont signalées par ordre décroissant de leur intérêt; autrement dit, le premier message OLC spécifie le type **dataType** que l'expéditeur préfère utiliser sur la voie logique.

Le destinataire de ces messages OLC n'est pas censé s'apercevoir que cette méthode des autres voies logiques possibles est sollicitée. Avant de recevoir une demande OLC acceptable, il refuse toutes les demandes inacceptables, généralement avec pour code de cause de type **dataTypeNotSupported**, **dataTypeNotAvailable** ou **unknownDataType**. Lorsqu'il reçoit une demande OLC acceptable, l'extrémité doit répondre au moyen d'un message **openLogicalChannelAck**. Toute autre demande OLC reçue ensuite est refusée avec le code **unspecified** étant donné que le numéro de la voie logique demandée correspondra à celui d'une voie déjà ouverte.

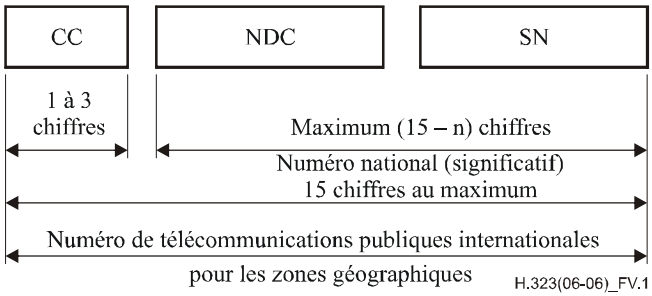
L'expéditeur d'une telle suite de messages **openLogicalChannel** avec ordre de priorité doit assurer la suite du nombre de messages de refus d'OLC qui précèdent la réception d'un message **openLogicalChannelAck** afin de pouvoir déterminer la voie proposée qui a été acceptée par son homologue.

Appendice V

Utilisation des plans de numérotage E.164 et ISO/CEI 11571

V.1 Plan de numérotage E.164

La Rec. UIT-T E.164 définit comme suit la numérotation selon les zones géographiques (voir Figure V.1).



CC indicatif de pays pour les zones géographiques (*country code*)
n nombre de chiffres dans l'indicatif de pays
NDC indicatif national de destination (facultatif) (*national destination code*)
SN numéro d'abonné (*subscriber number*)

NOTE – Les préfixes nationaux et internationaux ne font pas partie du numéro international de télécommunications publiques pour les zones géographiques.

Figure V.1/H.323 – Structure du numéro international de télécommunications publiques pour les zones géographiques

Des descriptions analogues sont également définies pour les zones non géographiques. La Rec. UIT-T E.164 définit également des indicatifs de pays (CC, *country codes*) pour tous les pays et pour toutes les régions du monde.

Un numéro E.164 international commence toujours par un indicatif de pays. Sa longueur totale est toujours de 15 chiffres au plus. Plus précisément, il ne comporte aucun préfixe faisant partie d'un plan de numérotage (par exemple "011" pour un appel international établi en Amérique du Nord ou "1" pour un appel à grande distance). Il ne comporte pas non plus de caractère "#" ou "*". Le numéro "49 30 345 67 00" est un numéro E.164 avec CC = 49 pour l'Allemagne. Un numéro national est composé du numéro international moins l'indicatif du pays: "30 345 67 00" en l'occurrence. Le numéro d'abonné est le numéro national moins l'indicatif national de destination, "345 67 00" en l'occurrence.

Un numéro E.164 a une portée mondiale car il peut être atteint à partir de tout endroit du monde. Une "séquence de chiffres composés" n'a cependant de sens que dans un domaine spécifique. Dans le plan de numérotage privé qui caractérise une entreprise, un préfixe tel que "9", par exemple, peut indiquer qu'un appel va "à l'extérieur", à partir de quoi c'est le plan de numérotage de la compagnie de téléphone locale qui prend le relais. Chaque compagnie de téléphone ou chaque réseau privé a le libre choix de son propre plan de numérotage et peut aussi le modifier à son gré, ce qui est souvent le cas (par exemple en ajoutant de nouveaux indicatifs de zone).

Dans un réseau typiquement déterminé par des zones géographiques, dont les usagers introduisent manuellement les numéros de téléphone et ne voyagent pas trop, le fait d'avoir différents plans de numérotage à différents endroits pose généralement un problème. Lorsqu'il voyage, un usager doit cependant déterminer le plan de numérotage de l'autre réseau afin d'établir ses appels. Lorsque des systèmes informatiques effectuent automatiquement le numérotage, l'usager est habituellement appelé à personnaliser le logiciel de numérotage pour chaque région ou chaque réseau.

Compte tenu de ces problèmes selon différents plans de numérotage et le numérotage automatique, il est essentiel de pouvoir se rapporter à un "numéro de téléphone" absolu plutôt qu'à "ce qu'il faut composer pour atteindre tel correspondant à partir de tel endroit". L'utilisation appropriée des numéros E.164 peut résoudre ces problèmes. De nombreux systèmes utilisent les numéros E.164 plutôt que des chiffres composés manuellement: par exemple, un autocommutateur peut recueillir les chiffres composés manuellement par un usager sur un poste téléphonique puis lancer un appel vers la compagnie de téléphone locale au moyen d'un numéro E.164 inséré dans l'élément d'information Numéro de l'appelé selon la Rec. UIT-T Q.931. Lors de la construction de l'élément d'information Numéro de l'appelé, le fait de spécifier le plan de numérotage avec la valeur "plan de numérotage RNIS/téléphonie selon la Rec. UIT-T E.164" indique un numéro E.164. Le fait de spécifier le type de numéro comme "inconnu" et de spécifier le plan de numérotage comme "inconnu" indique une composition manuelle des chiffres.

On trouvera ci-dessous une série de définitions extraites de la Rec. UIT-T E.164.

V.1.1 numéro: chaîne de chiffres indiquant de façon univoque le point de terminaison du réseau public. Ce numéro contient l'information nécessaire pour acheminer l'appel jusqu'à ce point de terminaison.

Ce numéro peut avoir un format national ou international. Le format international est connu comme le numéro de télécommunication publique, internationale, qui comporte l'indicatif de pays et les chiffres subséquents, mais pas de préfixe international.

V.1.2 plan de numérotage: plan qui spécifie le format et la structure des numéros utilisés dans ce plan. Il comporte généralement des chiffres décimaux divisés en groupes afin d'identifier des éléments spécifiques utilisés pour les capacités d'identification, d'acheminement et de taxation, par exemple, dans le plan E.164, pour identifier des pays, des destinations nationales et des abonnés.

Un plan de numérotage ne comporte pas de préfixe, de suffixe et pas d'information supplémentaire nécessaire pour faire aboutir un appel.

Le plan de numérotage national est l'implémentation à l'échelle nationale du plan de numérotage E.164.

V.1.3 plan de numérotation: chaîne ou combinaison de chiffres, de symboles et d'informations supplémentaires qui définissent la méthode d'utilisation du plan de numérotage. Un plan de numérotation comporte des préfixes, des suffixes et des informations supplémentaires ou complémentaires au plan de numérotage, nécessaires pour faire aboutir l'appel.

V.1.4 adresse: chaîne ou combinaison de chiffres, symboles et d'informations supplémentaires qui identifient le ou les points de terminaison spécifiques d'une connexion dans un ou des réseaux publics ou, le cas échéant, dans un ou des réseaux privés interconnectés.

V.1.5 préfixe: indicateur comprenant un ou plusieurs chiffres, qui permet de choisir différents types de formats de numéro, de réseaux et (ou) de service.

V.1.6 préfixe international: chiffre ou combinaison de chiffres qui sert à indiquer que le numéro qui suit est un numéro de télécommunications publiques internationales.

V.1.7 indicatif de pays pour zones géographiques (CC, *country code*): combinaison de 1, 2 ou 3 chiffres identifiant un pays donné, des pays appartenant à un plan de numérotage intégré ou situé en une zone géographique donnée.

V.1.8 numéro national (significatif) [**N(S)N**]: partie de numéro qui suit l'indicatif de pays pour les zones géographiques. Le numéro national (significatif) se compose de l'indicatif national de destination (NDC) suivi du numéro d'abonné. La fonction et le format de ce numéro sont déterminés nationalement.

V.1.9 indicatif national de destination (NDC, *national destination code*): champ de code, facultatif ou plan national appartenant au plan de numérotage de la Rec. UIT-T E.164 qui, combiné avec le numéro de l'abonné (SN), constituera le numéro national (significatif) du numéro de télécommunications internationales. Le NDC aura une fonction de sélection de réseau et (ou) d'indicatif interurbain.

L'indicatif NDC peut être un chiffre décimal ou une combinaison de chiffres décimaux (ne comprenant pas de préfixe) identifiant une zone de numérotage à l'intérieur d'un pays (ou d'un groupe de pays appartenant à un plan de numérotage intégré ou à une zone géographique donnée), et (ou) un réseau/des services.

V.1.10 préfixe (interurbain) national: chiffre ou combinaison de chiffres que doit composer l'appelant désirant appeler un abonné de son propre pays lorsque cet abonné réside en dehors de sa propre zone de numérotage. Ce chiffre ou cette combinaison de chiffres permet d'atteindre les équipements interurbains automatiques de départ.

V.1.11 numéro d'abonné (SN, *subscriber number*): numéro qui identifie un abonné d'un réseau local ou d'une zone de numérotage.

V.2 Numéro de réseau privé

Les numéros de réseau privé sont utilisés dans les réseaux téléphoniques privés virtuels ou non virtuels, par exemple, un réseau d'entreprise constitué d'autocommutateurs et de lignes virtuelles privées.

L'ISO/CEI 11571 définit le numéro de numérotage (numéro de plan PNP) comme comportant jusqu'à trois niveaux régionaux.

Un numéro de plan PNP doit contenir une séquence de x chiffres décimaux (0,1,2,3,4,5,6,7,8,9) avec la possibilité que différents numéros privés contenus dans le même plan de numérotage privé (PNP, *private numbering plan*) puissent avoir différentes valeurs de x. La valeur maximale de x doit être la même que dans le plan de numérotage public du RNIS, voir la Rec. UIT-T E.164 et voir Figure V.2.

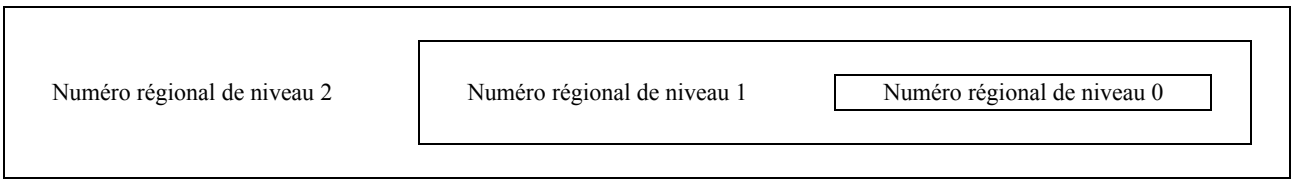


Figure V.2/H.323 – Structure d'un numéro PNP avec trois niveaux régionaux

Un numéro régional (RN, *regional number*) de niveau n ne doit avoir de portée que dans la région de niveau n à laquelle il s'applique. Lorsque ce numéro est utilisé en dehors de cette région de niveau n, ce doit être un numéro régional de niveau supérieur à n. Seul un numéro complet peut avoir une portée dans le plan PNP entier.

Un exemple représentatif de l'Amérique du Nord sera un poste supplémentaire de 4 chiffres en tant que numéro régional de niveau 0: un "indicatif d'emplacement" de 3 chiffres formera, en association avec le poste supplémentaire de 4 chiffres, le numéro régional de niveau 1. Le numéro régional de niveau 2 sera inexistant.

Un préfixe peut aussi être utilisé pour indiquer le numéro régional utilisé: il ne fera pas partie du numéro régional proprement dit mais ne sera qu'un élément du plan de numérotage. Ici encore, un exemple représentatif sera l'utilisation du chiffre "6" pour accéder à un numéro régional de niveau 1 et d'aucun chiffre pour un numéro régional de niveau 0.

On trouvera ci-après une série de définitions issues de l'ISO/CEI 11571.

V.2.1 plan de numérotage privé (PNP, *private numbering plan*): plan de numérotage se rapportant expressément à un domaine particulier de numérotage privé, défini par l'administrateur de RNIS privé (RPIS) dans ce domaine.

V.2.2 numéro de plan PNP: numéro appartenant à un plan PNP.

V.2.3 région: domaine entier ou sous-domaine d'un plan PNP. Une région ne correspond pas nécessairement à une zone géographique d'un RNIS privé (RPIS).

V.2.4 code régional (RC, *region code*): premiers chiffres d'un numéro de plan PNP, désignant une région. Le code régional peut être omis afin d'abréger un numéro de plan PNP pour usage interne dans la région considérée.

V.2.5 numéro régional (RN, *regional number*): forme particulière de numéro PNP sans ambiguïté dans la région concernée.

V.2.6 numéro complet: numéro qui est univoque dans l'ensemble du plan PNP, c'est-à-dire qui correspond au plus haut niveau régional utilisé dans le RNIS privé considéré.

V.3 Usage des versions 1, 2 et 3 de la Rec. UIT-T H.323

Les systèmes conformes aux versions 1, 2 et 3 de la présente Recommandation présentent un problème d'ordre terminologique en ce qui concerne les chiffres composés manuellement et les numéros E.164 proprement dits. Les références aux adresses E.164 désignent en fait, dans ces versions, des chiffres composés manuellement et non des chiffres E.164, comme les noms des champs l'impliqueraient. Dans les systèmes conformes aux versions 2 et 3 de la présente Recommandation, un véritable numéro E.164 a été placé dans le champ **publicNumber** et non dans le champ **e164**, qui correspond donc à une séquence de chiffres composés manuellement.

A partir des systèmes conformes à la version 4 de la présente Recommandation, le champ **e164** a été renommé **dialledDigits** et le champ **publicNumber** a été renommé **e164Number**. Ce changement de nom visait à indiquer plus clairement que les chiffres composés manuellement devaient être

insérés dans le champ **dialledDigits** et que les numéros E.164 devaient l'être dans le champ **e164Number**.

Appendice VI

Description d'un système H.323 type sur IP

Le présent appendice décrit une pile H.323 type. La Figure VI.1 montre comment les messages RAS, la signalisation d'appel H.225.0 et les médias sont implémentés au moyen de l'infrastructure IP.

La flèche entre H.245 et H.225.0 indique que H.245 peut être tunnellisé dans la Rec. UIT-T H.225.0.

La flèche entre la signalisation d'appel H.225.0 et le message RAS H.225.0 indique que la signalisation d'appel H.225.0 peut être tunnellisée dans le message RAS H.225.0.

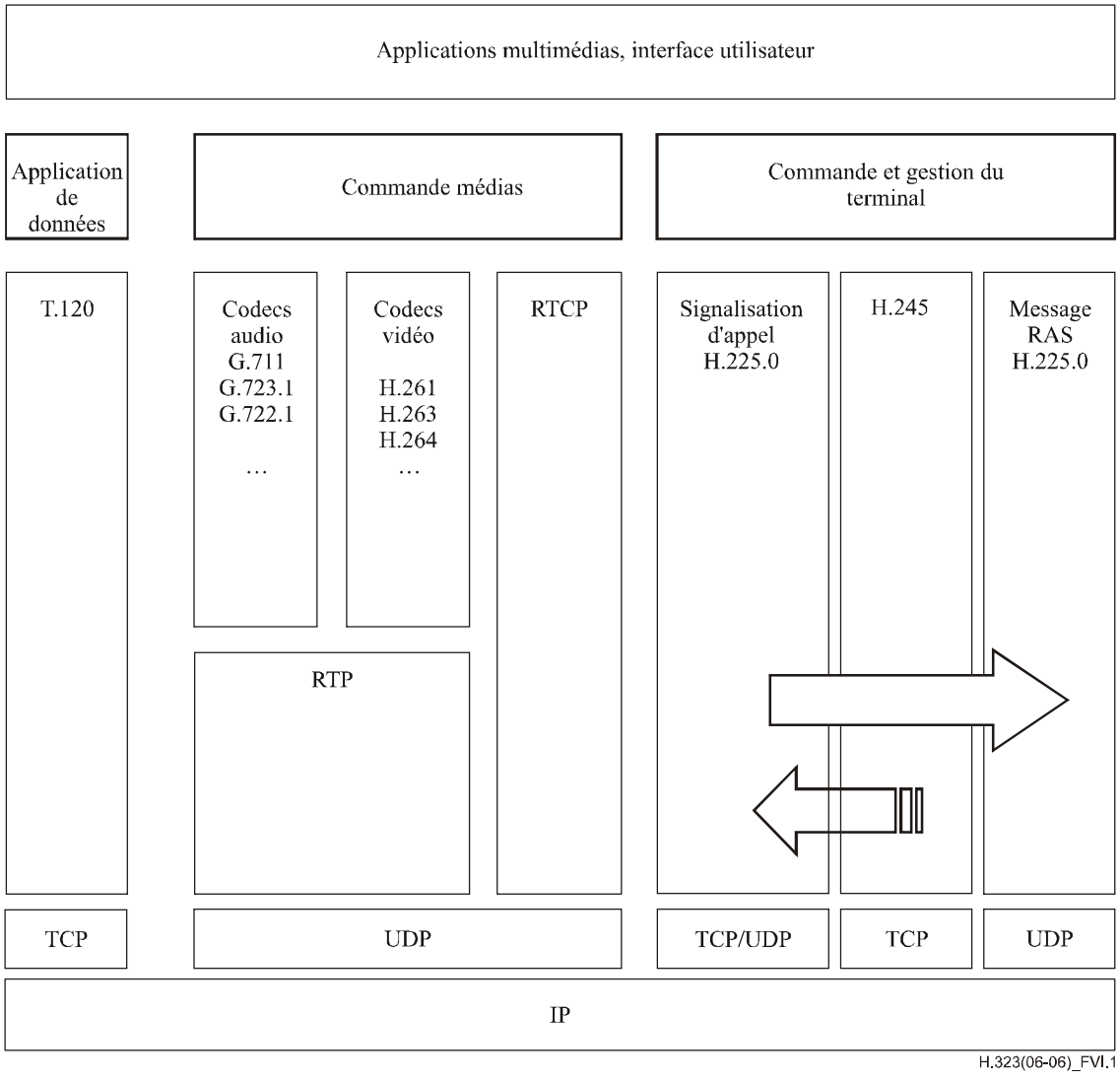


Figure VI.1/H.323 – Système H.323 type sur une pile IP

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2007