



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

H.323

Annexe R
(07/2001)

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

**Annexe R: Méthodes d'amélioration de la
robustesse pour les entités H.323**

Recommandation UIT-T H.323 – Annexe R

(Antérieurement Recommandation du CCITT)

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.399
SERVICES COMPLÉMENTAIRES EN MULTIMÉDIA	H.450–H.499

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

Systèmes de communication multimédia en mode paquet

ANNEXE R

Méthodes d'amélioration de la robustesse pour les entités H.323

Résumé

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 (UIT-T H.225.0) et de signalisation de commande d'appel (UIT-T H.245) sont spécifiées. La signalisation RAS (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 doit faire l'objet d'un complément d'étude.

Source

L'Annexe R de la Recommandation H.323 de l'UIT-T, élaborée par la Commission d'études 16 (2001-2004) de l'UIT-T, a été approuvée le 29 juillet 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT 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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2002

Droits de reproduction réservés. Aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'UIT.

TABLE DES MATIÈRES

	Page
Annexe R – Méthodes d'amélioration de la robustesse pour les entités H.323	1
R.1 Introduction et domaine d'application.....	1
R.2 Références normatives	1
R.3 Définitions	2
R.4 Abréviations.....	2
R.5 Aperçu général des deux méthodes	3
R.5.1 Méthode A: rétablissement d'état à partir des entités voisines	3
R.5.2 Méthode B: rétablissement d'état à partir d'un répertoire partagé	3
R.5.3 Comparaison.....	4
R.6 Mécanismes communs.....	4
R.6.1 Détection de perte de connexion TCP.....	4
R.6.2 Traitement des défaillances de protocole	5
R.6.3 Détection des défaillances – Mécanismes keepAlive (maintien d'enregistrement)	5
R.6.4 Adresse de transport et connexions rétablies.....	6
R.6.5 Prise en charge du statut étendu	7
R.7 Méthode A: rétablissement d'état à partir d'entités voisines.....	7
R.7.1 Introduction	7
R.7.2 Domaine d'application.....	7
R.7.3 Procédure d'amélioration de la robustesse.....	7
R.7.4 Langage de description et de spécification pour la machine à états selon la méthode A.....	9
R.8 Méthode B: rétablissement d'état à partir d'un répertoire partagé	11
R.8.1 Plate-forme résistante aux défaillances	11
R.8.2 Groupe d'entités résistant aux défaillances.....	11
R.8.3 Rétablissement de la connexion de la signalisation d'appel	11
R.8.4 Rétablissement de connexion H.245	12
R.8.5 Eléments de données mis en commun par l'intermédiaire du répertoire partagé	13
R.8.6 Points de reprise.....	13
R.9 Interfonctionnement des méthodes d'amélioration de la robustesse.....	13
R.10 Procédures de rétablissement.....	13
R.11 Utilisation du champ GenericData.....	14
R.11.1 Utilisation du champ GenericData dans les messages H.225.0.....	14
R.12 Note informative 1: généralités concernant les méthodes d'amélioration de la robustesse.....	15
R.12.1 Types de méthodes d'amélioration de la robustesse	15
R.12.2 Entités d'amélioration de la robustesse.....	15

	Page
R.12.3	Domaine d'utilisation d'un système d'amélioration de la robustesse 16
R.12.4	Fin de session et défaillance de système 16
R.13	Note informative 2: partage d'état d'appel entre une entité et son entité homologue de secours..... 18
R.13.1	Mémoire partagée 18
R.13.2	Disques partagés 18
R.13.3	Analyse des messages..... 18

Recommandation UIT-T H.323

Systèmes de communication multimédia en mode paquet

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 (UIT-T H.225.0) et de signalisation de commande d'appel (UIT-T H.245) sont spécifiées. La signalisation RAS (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 doit faire l'objet d'un complément d'étude.

Les appels H.323 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 Rec. UIT-T H.323 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.

- [1] UIT-T H.225.0 (2000), *Protocoles de signalisation d'appel et mise en paquets des trains multimédias dans les systèmes de communication multimédia en mode paquet.*
- [2] UIT-T H.323 (2000), *Systèmes de communication multimédia en mode paquet.*

- [3] UIT-T Q.931 (1998), *Spécification de la couche 3 de l'interface utilisateur-réseau RNIS pour la commande de l'appel de base.*
- [4] UIT-T X.680 (1997), *Technologies de l'information – Notation de syntaxe abstraite numéro un: spécification de la notation de base.*

R.3 Définitions

Outre les termes définis dans la Rec. UIT-T H.323, 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 (libération terminée). 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 que nous cherchons 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.5.2 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 mis en œuvre 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/H.323). 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.

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.

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 Rec. 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 Q.931 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. 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.

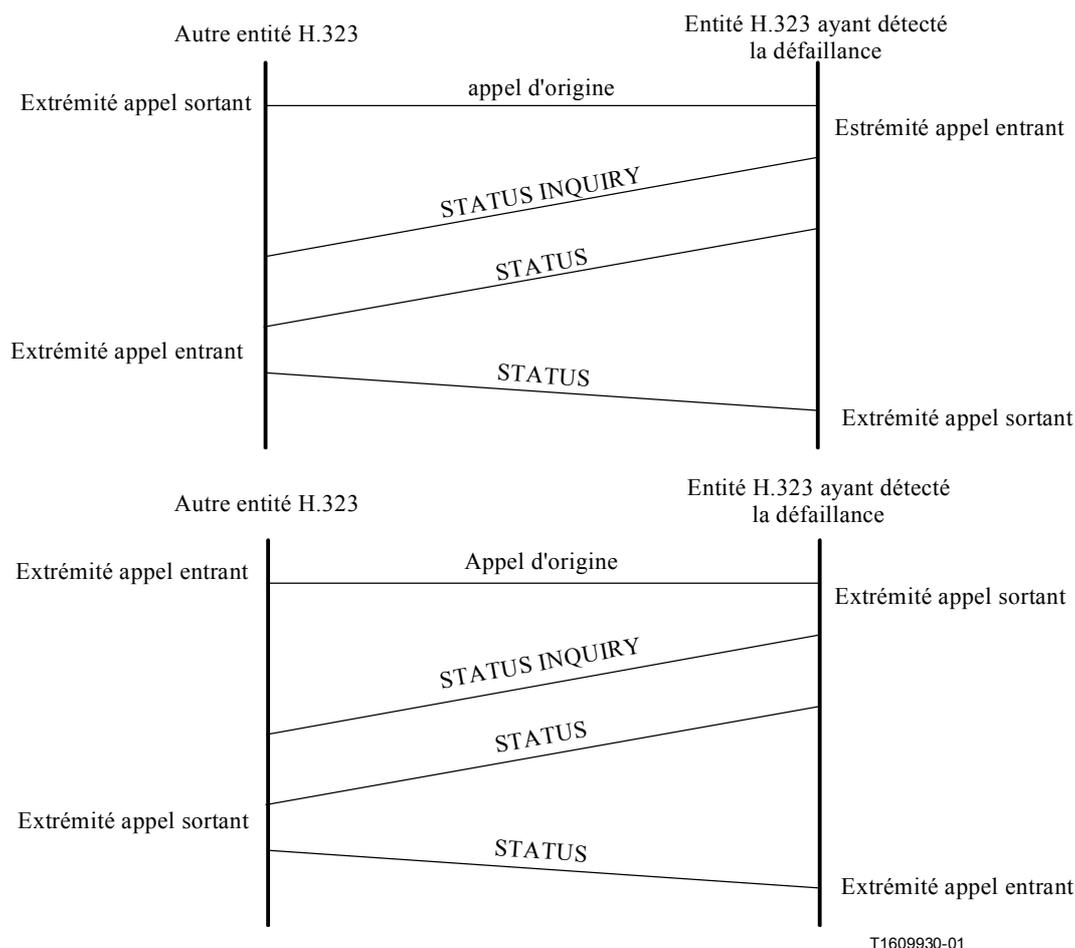


Figure R.1/H.323 – Procédures d'amélioration de la robustesse

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.

R.7.4 Langage de description et de spécification pour la machine à états selon la méthode A

Voir Figure R.2.

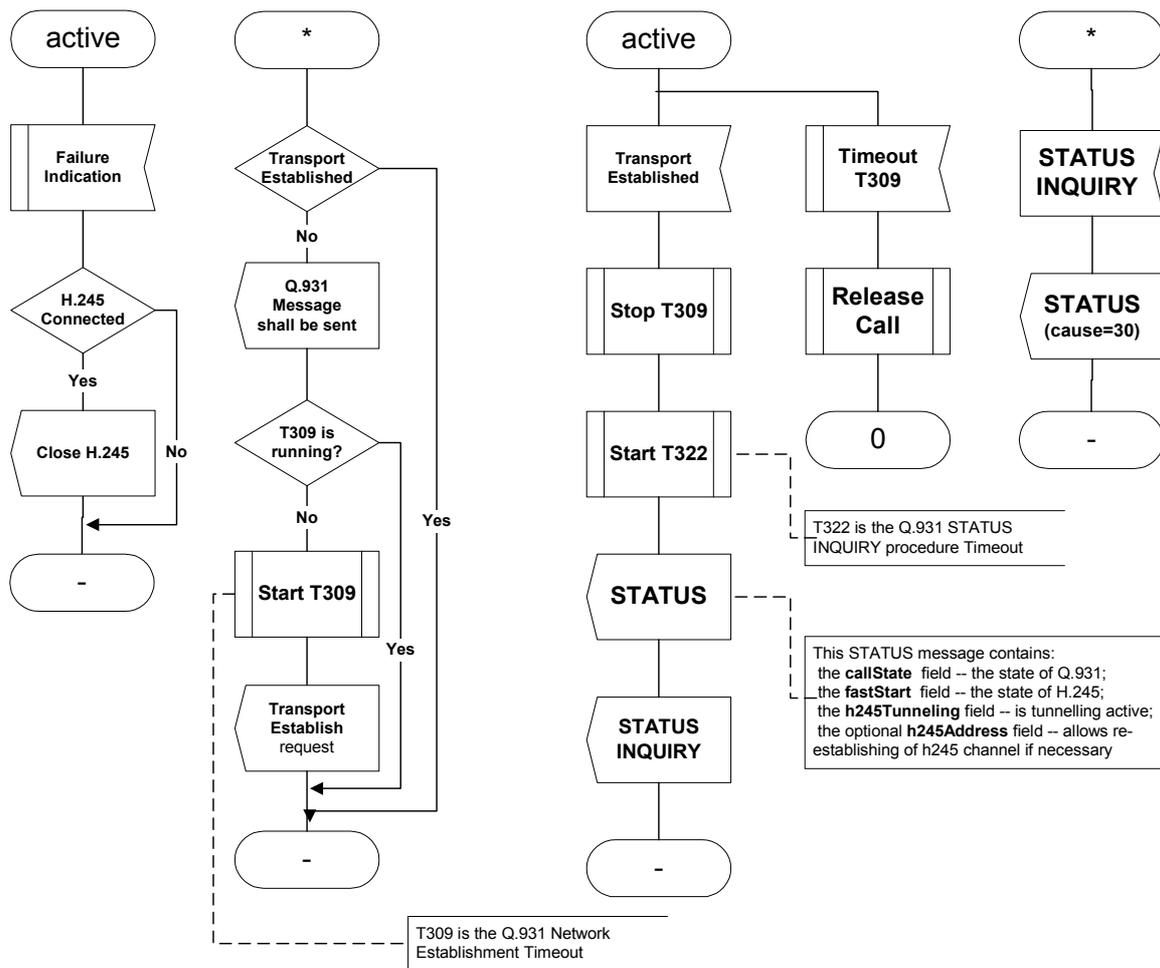


Figure R.2/H.323 – Machine à états selon la méthode A (feuille 1 de 2)

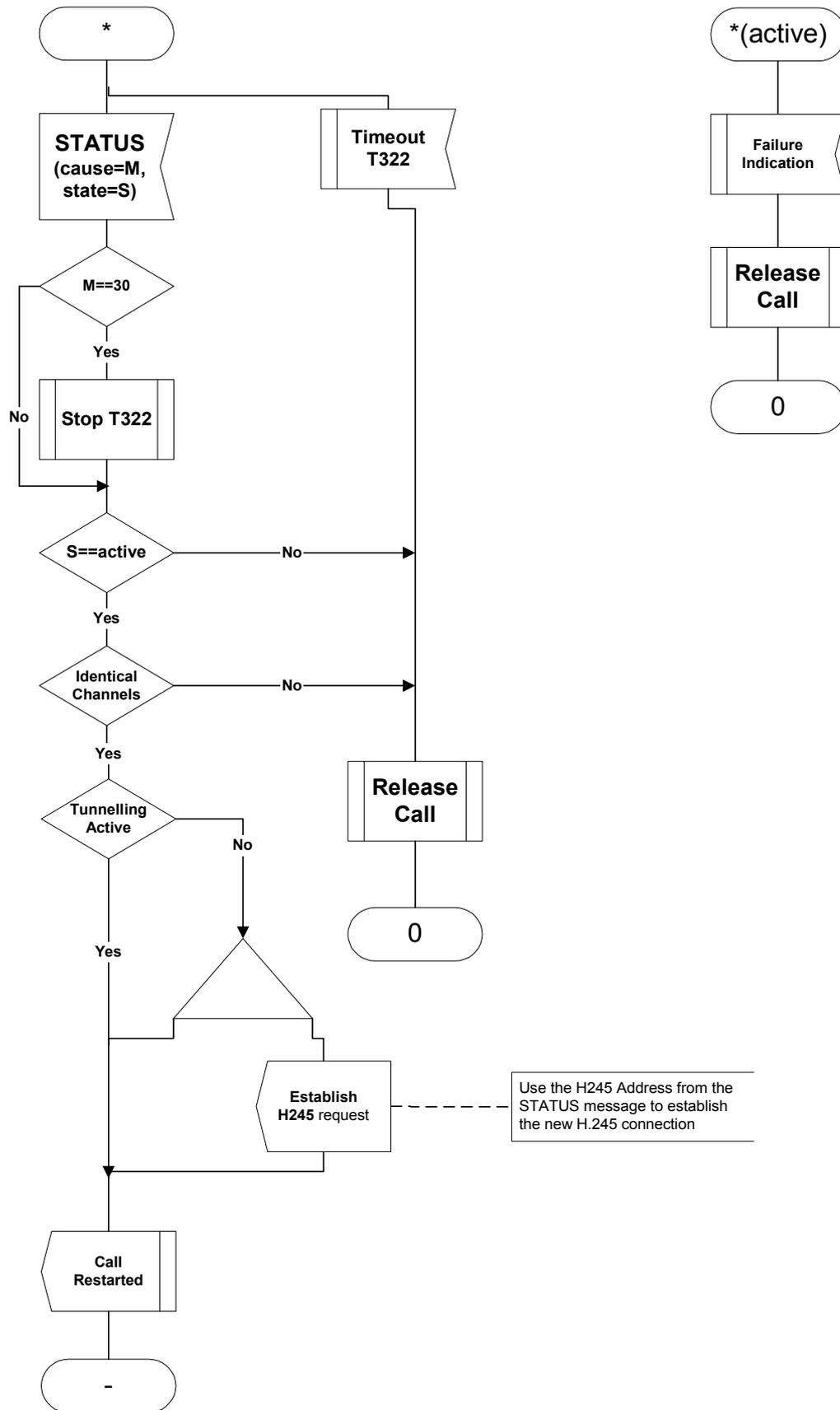


Figure R.2/H.323 – Machine à états selon la méthode A (feuille 2 de 2)

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 nous proposerons à cet égard un certain nombre de solutions. 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 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 pseudo-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 § 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 tunnelisation H.245, les entités peuvent continuer à tunneliser 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.

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 backupCallSignallingAdresses;
- 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 nous conservons uniquement 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 paragraphe intitulé **Procédures de rétablissement** 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 StatusInquirykeepAlive) 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.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
{
    backupCallSignalAddresses    SEQUENCE OF TransportAddress,
                                -- empty when not required
    h245Address                  TransportAddress OPTIONAL,
    fastStart                     SEQUENCE OF OCTET STRING OPTIONAL,
    timeToLive                    TimeToLive OPTIONAL
    hasSharedRepository          NULL 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 entités prenant en charge l'amélioration de la robustesse doivent utiliser les champs de type GenericData en procédant comme suit (voir Tableau R.1):

Tableau R.1/H.323 – Utilisation des champs GenericData pour les données d'amélioration de la robustesse

Message	inclure RobustnessData dans GenericData	Champs prescrits						robustness FeatureDescr in desiredFeatures of featureSet
		hasShared Repository	backupCallSig Addresses	robustness FastStart	include FastStart	robustness TimeToLive	robustness H245Addr	
RRQ	M	M						M
RCF	M	M						M
ARQ								M
ACF								M
Setup	M	M	M					M#
Connect	M	M	M					M
Status+	M			M			M	
StatusInquiry+	M				M	M	M	
M obligatoire – aucun autre autoisé (all others forbidden) + en cas d'utilisation pour les procédures d'amélioration de la robustesse # le champ desiredFeatures n'est pas contenu dans le champ featureSet du message Setup								

Toutes les entités prenant en charge les procédures d'amélioration de la robustesse doivent prendre en charge le message Status comportant le champ supplémentaire RobustnessData afin d'améliorer l'interopérabilité entre les méthodes A et B.

R.12 Note informative 1: généralités concernant les méthodes d'amélioration de la robustesse

Ce 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; et
- 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

Ce 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 (réfléchi). 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

Ce 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:

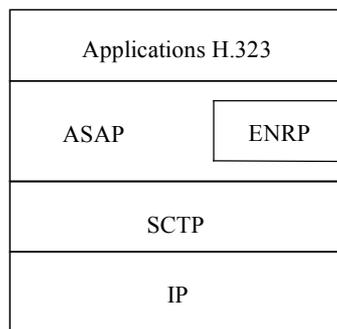
- 1) un aperçu de l'architecture d'un système H.323 utilisant le protocole ASAP/SCTP;
- 2) une présentation des piles de protocoles nécessaires aux différents nœuds H.323;
- 3) des scénarios de reprise sur incident correspondant à un exemple d'appel H.323 avec deux portiers et deux points d'extrémité.

R.13.3.1.1 Références

- [1] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.
- [2] R.R. Stewart et Q. Xie: *Aggregate Server Access Protocol (ASAP)*, <draft-xierserpool-asap-00.txt>, IETF, octobre 2000.
- [3] Q. Xie et R.R. Stewart: *Endpoint Name Resolution Protocol (ENRP)*, <draft-xie-rserpool-enrp-00.txt>, IETF, octobre 2000.

R.13.3.1.2 Piles de protocoles

En règle générale une application H.323 utilisant le protocole ASAP/SCTP [1] à [3] de résistance aux défaillances sera dotée de la pile de protocoles suivante:



T1609950-01

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.3 représente un système H.323 conçu selon le modèle ASAP/SCTP.

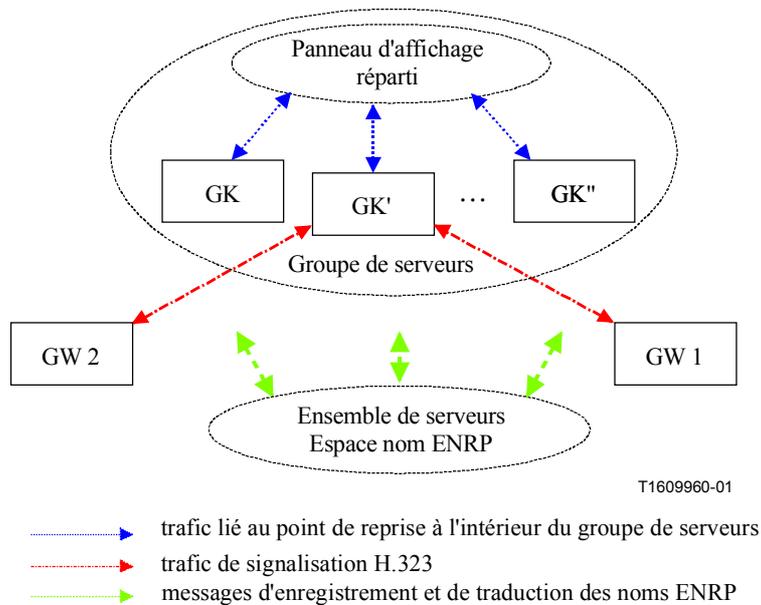


Figure R.3/H.323 – Système H.323 conçu selon le modèle ASAP/SCTP

Dans le système, tous les composants H.323, notamment les passerelles GW1, GW2, et les portiers utilisent les piles de protocole 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 [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" [2] et [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.4.

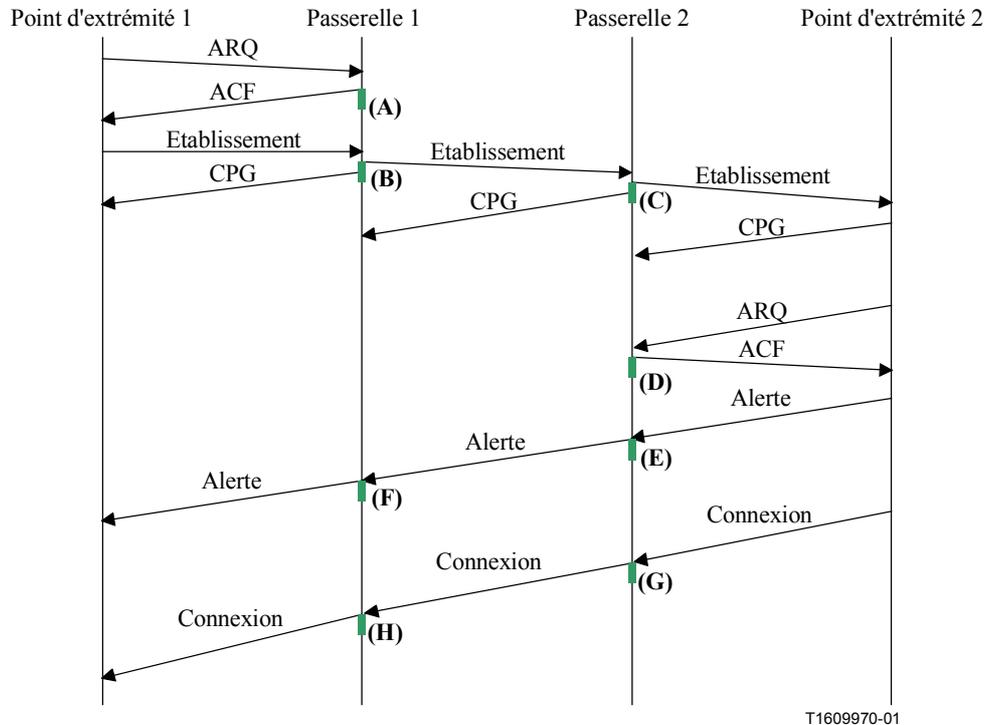


Figure R.4/H.323 – Exemple d'appel H.323

J'attire 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 réfléchi) 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 d'établissement 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 d'établissement envoyé par son portier homologue, choisit le point d'extrémité de destination, transmet le message d'établissement 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 d'établissement, 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 d'alerte, 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 alerte au portier 1.

Le portier 1 répètera cette procédure, en mettant à jour son information d'état au point **F** et en la transmettant dans le message alerte.

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?

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication