UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T H.510

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2002)

SÉRIE H: SYSTÈMES AUDIOVISUELS ET MULTIMÉDIAS

Procédures de mobilité et de collaboration – Mobilité pour les systèmes et services multimédias de la série H

Mobilité pour les systèmes et services multimédias H.323

Recommandation UIT-T H.510

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
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

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

Recommandation UIT-T H.510

Mobilité pour les systèmes et services multimédias H.323

Résumé

La présente Recommandation a pour objet de définir les services et les procédures permettant d'assurer la mobilité des systèmes multimédias H.323.

Source

La Recommandation H.510 de l'UIT-T, élaborée par la Commission d'études 16 (2001-2004) de l'UIT-T, a été approuvée le 29 mars 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

H.323, mobilité de l'utilisateur, mobilité du terminal, systèmes multimédias.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T H.510

Mobilité pour les systèmes et services multimédias H.323

1 Domaine d'application

La présente Recommandation traite des questions relatives à la mobilité des systèmes H.323 au-desssus de la couche Transport. Elle s'applique aux nouvelles fonctions définies pour assurer la gestion de la mobilité des systèmes conformes à la Rec. UIT-T H.323.

Bien qu'étant essentiellement consacrée à la prise en charge de la mobilité du terminal, elle traite également de la prise en charge de la mobilité de l'utilisateur dans le contexte de la Rec. UIT-T H.323. La présente version de la Rec. UIT-T H.510 ne traite pas des procédures de transfert avec maintien de la communication à l'état actif pendant que l'utilisateur change d'emplacement.

L'interfonctionnement avec d'autres réseaux pour assurer la mobilité entre réseaux de différents types ne relève pas du domaine d'application de la présente Recommandation.

2 Références

2.1 Références normatives

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

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

[2] Recommandation UIT-T H.225.0 (2000), *Protocoles de signalisation d'appel et paquétisation des flux monomédias dans les systèmes de communication multimédias en mode paquet*.

[3] Recommandation UIT-T H.225.0, Annexe G (1999), *Communication entre domaines administratifs*.

[4] Recommandation UIT-T H.501 (2002), *Protocole de gestion de la mobilité et communications intra/interdomainiales dans les systèmes multimédias*.

[5] Recommandation UIT-T H.530 (2002), *Procédures de sécurité symétrique pour la mobilité des systèmes H.323 selon la Recommandation H.510*.

2.2 Références informatives

– IETF RFC 2486 (1999), *The Network Access Identifier*.

3 Définitions

Pour les besoins de la présente Recommandation, les définitions figurant dans la Rec. UIT-T H.323 s'appliquent en plus de celles qui sont indiquées ci-après.

3.1 domaine administratif: selon la définition qui est donnée dans l'Annexe G/H.225.0, un domaine administratif est un ensemble d'entités H.323 gérées par une même entité administrative. Un domaine administratif est constitué d'une ou plusieurs zones.

3.2 identité d'utilisateur appelable: identité d'utilisateur que peut utiliser un utilisateur appelant pour appeler l'utilisateur identifié par cette identité d'utilisateur. Celle-ci peut être indiquée, par exemple, dans un annuaire téléphonique, comme étant l'identité à utiliser pour joindre un utilisateur.

3.3 point de rattachement H.323: point de rattachement d'un réseau qui permet à un terminal H.323 de se faire enregistrer auprès d'un portier ou de communiquer directement avec un autre terminal H.323.

3.4 domaine de rattachement: domaine administratif auquel est rattaché l'utilisateur mobile dans le cadre de son abonnement. Le domaine de rattachement contient des données propres à l'utilisateur mobile, concernant notamment sa position, son authentification et son profil de service.

3.5 portier de rattachement (GK de rattachement): portier situé dans le domaine de rattachement d'un utilisateur.

3.6 fournisseur de services de rattachement: fournisseur de services ou administrateur responsable du domaine de rattachement d'un utilisateur; l'utilisateur est lié au fournisseur de services de rattachement dans le cadre d'un contrat d'abonnement.

3.7 position/emplacement: point de rattachement du réseau via lequel l'utilisateur ou le terminal a accès au système H.323, au moment considéré.

3.8 terminal mobile H.323: terminal pouvant changer de point de rattachement H.323.

3.9 gestion de la mobilité: ensemble des fonctions nécessaires pour assurer la mobilité de l'utilisateur, du terminal et du service.

3.10 point de rattachement du réseau: interface réseau utilisée par une extrémité pour accéder au système H.323. Chaque point de rattachement du réseau est associé à une adresse de réseau (par exemple une adresse IP) garantissant que les paquets envoyés à l'extrémité y parviennent.

3.11 en ligne: état d'un utilisateur ou d'un terminal mobile qui s'est connecté au système, c'est-à-dire qui est enregistré auprès d'un portier; l'état en ligne s'oppose à l'état **absent** ou "déconnecté".

3.12 identité d'utilisateur principale: identité attribuée de manière permanente à un utilisateur au moment où il souscrit son abonnement et qui reste la même pendant toute la durée de l'abonnement. Un utilisateur ne dispose que d'une seule identité principale.

3.13 mobilité de service: capacité d'un utilisateur à utiliser un service auquel il est abonné, quel que soit l'emplacement où il se trouve et le terminal qu'il utilise à cet effet.

3.14 domaine de desserte: domaine administratif (visité ou de rattachement) assurant la desserte d'un utilisateur/terminal mobile en ligne.

3.15 portier de desserte: portier (visité ou de rattachement) auprès duquel un utilisateur/terminal mobile en ligne est enregistré.

3.16 identité temporaire d'utilisateur: identité attribuée à un utilisateur à titre temporaire, qu'il est censé utiliser à la place de son identité principale, pour des raisons de sécurité, par exemple.

3.17 identité de terminal: code ou chaîne identifiant un terminal de manière exclusive.

NOTE – Cette identité peut servir à authentifier le terminal au moment où l'utilisateur se fait enregistrer. L'authentification du terminal permet de vérifier si l'utilisateur est autorisé ou non à utiliser le terminal (par exemple, si le terminal mobile H.323 a été inscrit sur une liste noire par le fournisseur de services de rattachement – pour avoir été volé, par exemple – l'utilisateur mobile ne peut pas se faire enregistrer dans le réseau H.323 avec ce terminal).

3.18 mobilité de terminal: capacité d'un terminal à changer d'emplacement (c'est-à-dire de point de rattachement de réseau et de point de rattachement H.323) tout en conservant sa capacité à communiquer.

3.19 mobilité de terminal avec interruptions (itinérance de terminal): capacité d'un terminal à changer de lieu par déplacements successifs, c'est-à-dire de changer de lieu lorsqu'aucun flux média n'est actif.

3.20 mobilité continue du terminal (transfert): capacité d'un terminal à changer d'emplacement en présence de flux médias actifs. En outre, le transfert est qualifié de *transparent* lorsque le changement d'emplacement du terminal n'entraîne ni retard ni perte de données perceptibles par l'utilisateur sous forme de dégradation de la qualité de service (notons que les transferts transparents peuvent dépendre de nombreux facteurs, tels que la résistance du type de service ou de la présentation du service contre les pertes de données dans le terminal).

3.21 utilisateur: personne ou autre entité autorisée à utiliser les services de communication H.323.

3.22 identité de l'utilisateur: code ou chaîne identifiant de manière exclusive un utilisateur parmi une infrastructure comportant de multiples utilisateurs et services.

3.23 mobilité de l'utilisateur (mobilité de la personne): capacité d'un utilisateur à conserver la même identité indépendamment du terminal utilisé et de son point de rattachement de réseau. Différents types de terminaux peuvent être utilisés.

3.24 mobilité de l'utilisateur avec interruption (itinérance de l'utilisateur): capacité d'un utilisateur à changer d'emplacement ou de terminal au moment où aucun flux média n'est actif.

3.25 mobilité continue de l'utilisateur (mobilité de la session): capacité d'un utilisateur à changer d'emplacement ou de terminal en présence de flux médias actifs.

NOTE – Cette fonctionnalité est analogue à celle qui est assurée dans le réseau à commutation de circuits (RCC) par le service complémentaire de portabilité du terminal.

3.26 profil de service de l'utilisateur: informations propres à l'utilisateur indiquant les services auxquels celui-ci est abonné ainsi que ses données de configuration personnelles pour chacun de ces services.

3.27 domaine visité: domaine administratif autre que le domaine de rattachement et assurant la desserte d'un utilisateur mobile.

3.28 portier visité (GK visité): portier situé dans un domaine visité.

4 Symboles et abréviations

La présente Recommandation utilise les abréviations suivantes:

A adresse (type d'enregistrement/interrogation de système DNS)

AuF fonction d'authentification (*authentication function*)

BE élément frontière (*border element*)

DHCP protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)

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

e164 adresse de type "numéro de téléphone" (selon la Rec. UIT-T E.164)

EP extrémité (*endpoint*)

GK portier (*gatekeeper*)

HLF fonction de localisation nominale (*home location function*)

IMSI identité internationale d'abonné mobile (*international mobile subscriber identity*)

IP protocole Internet (*Internet protocol*)

MT terminal mobile (*mobile terminal*)

NAI identificateur d'accès au réseau (*network access identifier*)

NPoA point de rattachement de réseau (*network point of attachment*)

RAS protocole, RAS (enregistrement, admission et statut) (Rec. UIT-T H.225.0) (*registration, admission and status protocol*)

Les messages RAS suivants sont utilisés dans la présente Recommandation:

ACF AdmissionConfirm (*confirmation d'admission*)

ARJ AdmissionReject (*refus d'admission*)

ARQ AdmissionRequest (*demande d'admission*)

GCF GatekeeperConfirm (*confirmation de portier*)

GRJ GatekeeperReject (*refus de portier*)

GRQ GatekeeperRequest (*demande de portier*)

LCF LocationConfirm (*confirmation d'emplacement*)

LRQ LocationRequest (*demande d'emplacement*)

RCF RegistrationConfirm (*confirmation d'enregistrement*)

RIP RequestInProgress (*demande en cours*)

RRJ RegistrationReject (*refus d'enregistrement*)

RRQ RegistrationRequest (*demande d'enregistrement*)

SLA accord de niveau de service (*service level agreement*)

SRV service (type d'enregistrement/interrogation de système DNS)

TSAP point d'accès au service de transport (*transport service access point*)

TXT texte (type d'enregistrement/interrogation de système DNS)

UCF UnregistrationConfirm (*confirmation d'annulation d'enregistrement*)

UIM module d'identification d'utilisateur (*user identification module*)

URL localisateur de ressources universel (*universal resource locator*)

URQ UnregistrationRequest (*demande d'annulation d'enregistrement*)

VLF fonction de localisation des visiteurs (*visitor location function*)

5 Description des services de mobilité H.323

Les services mis en œuvre dans le cadre du système H.323 pour assurer la mobilité du terminal et de l'utilisateur sont définis dans les paragraphes suivants. Ces services y sont décrits de manière générale du point de vue de l'utilisateur. Les questions concernant l'interface utilisateur ne sont pas abordées.

5.1 Description générale

5.1.1 Mobilité de l'utilisateur H.323

La présente Recommandation traite de la prise en charge des utilisateurs mobiles faisant partie d'un réseau H.323.

NOTE – La mobilité des utilisateurs d'un point de vue général est décrite dans d'autres Recommandations.

Dans un réseau permettant la mobilité de l'utilisateur, il existe une association dynamique entre utilisateurs et terminaux mobiles. Tout utilisateur mobile peut se faire enregistrer auprès de n'importe quel terminal donnant accès au réseau, pour autant qu'il obtienne les autorisations voulues. L'enregistrement permet à cet utilisateur de bénéficier des services autorisés par le profil de service de l'utilisateur du terminal auprès duquel il se fait enregistrer et effectivement assurés par ce terminal. Un utilisateur mobile qui change d'emplacement doit se faire enregistrer auprès d'un nouveau terminal et prévenir le terminal auprès duquel il était précédemment enregistré (le cas échéant) pour que celui-ci annule son enregistrement.

Un utilisateur mobile relève une fois pour toutes d'un domaine administratif, son domaine de rattachement. La mobilité de l'utilisateur peut être limitée à son domaine de rattachement ou étendue à plusieurs domaines administratifs, sous réserve que des accords de service aient été conclus entre ces domaines et le domaine de rattachement de l'utilisateur.

Le profil de service applicable à un utilisateur mobile dépend de l'emplacement où il se trouve et des accords de service susmentionnés. Après s'être fait dûment enregistrer, un utilisateur mobile doit pouvoir passer ou recevoir des appels là où il se trouve. Toutefois, des restrictions pourront lui être appliquées en ce qui concerne les ressources qu'il sera autorisé à utiliser, la qualité de service disponible, etc.

En ce qui concerne la Rec. UIT-T H.323, deux aspects distincts sont à prendre en considération en ce qui concerne la mobilité interdomaine:

a) un utilisateur mobile se fait enregistrer auprès d'un terminal H.323. Cet utilisateur est considéré comme un utilisateur H.323 indépendamment du fait que son domaine de rattachement utilise ou non un système H.323. S'il n'utilise pas un système H.323, le domaine de rattachement réacheminera les appels destinés à l'utilisateur mobile vers une passerelle d'entrée H.323;

b) un utilisateur mobile dont le domaine de rattachement utilise un système H.323 change de réseau. Dans ce cas, le domaine de rattachement H.323 réacheminera les appels destinés à cet utilisateur mobile vers une passerelle de sortie H.323.

5.1.2 Mobilité du terminal H.323

Le terme mobilité du terminal désigne la possibilité pour un terminal H.323 de changer d'emplacement, c'est-à-dire de point de rattachement de réseau tout en conservant sa capacité à communiquer. Dans la présente Recommandation, par mobilité du terminal on entend la mobilité de l'utilisateur associé au terminal au moment considéré. Dans le seul cas où des considérations particulières s'appliquent non pas aux utilisateurs mais aux terminaux, la mobilité du terminal est traitée séparément.

Il se peut qu'aucun utilisateur ne soit enregistré auprès d'un terminal donné. Les services que peut assurer un terminal auprès duquel aucun utilisateur n'est enregistré varient en fonction du modèle de terminal. Pour qu'il puisse fournir des services, un tel terminal peut être associé à un utilisateur "par défaut" enregistré administrativement. Ainsi, il n'y a pas lieu de se soucier des terminaux proprement dits, qui peuvent être assimilés à leur utilisateur par défaut.

5.1.3 Mobilité du service

Dans le contexte de la présente Recommandation, la mobilité du service consiste simplement à appliquer le profil de service de l'utilisateur mobile lorsqu'il passe ou reçoit des appels.

NOTE – Les autres aspects de la mobilité du service seront décrits dans d'autres Recommandations.

5.2 Prescriptions H.323

5.2.1 Prescriptions applicables à la mobilité de l'utilisateur H.323

La mobilité de l'utilisateur H.323 suppose les services suivants:

1) **identification et authentification de l'utilisateur mobile**: permet à un domaine de desserte de valider l'identité de l'utilisateur mobile;

2) **authentification du domaine de desserte**: permet à un utilisateur mobile de vérifier l'authenticité du domaine de desserte, pour s'assurer qu'il s'agit bien du domaine dont les services sont attendus;

3) **enregistrement/annulation d'enregistrement de l'utilisateur mobile**: permet à un utilisateur mobile d'utiliser également un terminal H.323 filaire ou hertzien pour passer ou recevoir des appels. L'utilisateur mobile peut procéder ainsi en permanence (sans jamais annuler son enregistrement) ou de manière temporaire (en annulant son enregistrement à la fin d'une période d'enregistrement).

   NOTE – L'enregistrement permanent pourrait être activé "par décision administrative" sans que l'utilisateur concerné ait à s'en occuper. Cette manière de procéder pourrait avoir de nombreuses applications utiles, telles que la fourniture de services sur des terminaux publics ou la gestion d'un terminal par défaut depuis le bureau personnel d'un utilisateur;

4) **gestion des appels d'un utilisateur mobile**: permet à un utilisateur mobile de passer ou recevoir des appels, généralement après s'être fait enregistrer sous l'identité de l'utilisateur auprès d'un terminal H.323 agréé. Cette capacité ne devrait être limitée que par les capacités du terminal et du réseau ou éventuellement par les restrictions imposées en vertu des accords de niveau de service (SLA, *service level agreement*) passés entre les fournisseurs de services des domaines administratifs concernés. Ce service comprend deux éléments (qui peuvent être mis en œuvre indépendamment l'un de l'autre), la gestion des appels entrants et la gestion des appels sortants:

   - la *gestion des appels entrants de l'utilisateur mobile* achemine les appels entrants destinés à un utilisateur mobile jusqu'au terminal H.323 auprès duquel il s'est fait enregistrer, indépendamment de l'emplacement de ce terminal et du domaine de desserte auprès duquel l'utilisateur mobile est enregistré;
   - la *gestion des appels sortants de l'utilisateur mobile* détecte un appel sortant d'un utilisateur mobile et le fait aboutir en appliquant le profil de service de l'utilisateur, quel que soit l'emplacement où cet utilisateur se trouve dans le réseau H.323. L'identité de l'utilisateur doit être communiquée à tout correspondant appelé dans le cadre de la procédure normale d'identification de l'appelant, indépendamment de l'emplacement du terminal et du domaine de desserte auprès duquel l'utilisateur mobile est enregistré.

5.2.2 Prescriptions applicables à la mobilité du terminal H.323

La mobilité du terminal H.323 suppose les services suivants:

1) **authentification d'un terminal mobile H.323**: ce service permet de vérifier l'authenticité d'un terminal mobile H.323 dans le contexte de l'*association* qu'il entretient avec un utilisateur mobile (qu'il a établie précédemment en se faisant enregistrer). L'authentification du terminal sert à vérifier que celui-ci est effectivement habilité à agir au nom de l'utilisateur qui est enregistré auprès de ce terminal.

NOTE – Le fait de savoir quel terminal en particulier est utilisé ne présente d'intérêt, en soi, qu'à des fins secondaires, par exemple pour s'assurer que le terminal en question ne figure pas sur une liste noire de terminaux volés ou pour localiser non pas un utilisateur mais un terminal;

2) **authentification du domaine de desserte**: ce service permet à un terminal mobile H.323 de vérifier l'authenticité du domaine de desserte (traversé au cours d'un déplacement) au nom de l'utilisateur mobile enregistré auprès de ce terminal;

3) **enregistrement/annulation d'enregistrement d'un terminal mobile H.323**: ce service permet à un terminal mobile H.323 de renouveler l'enregistrement de l'utilisateur mobile qui lui est associé lorsqu'il change d'emplacement et d'annuler l'enregistrement, par exemple lorsqu'il est hors fonction;

4) **transfert de profils de service de l'utilisateur**: ce service permet de transférer (en partie ou en totalité) le profil de service de l'utilisateur dans le domaine de desserte (c'est-à-dire dans le portier responsable ou, éventuellement directement dans le terminal);

5) **gestion des appels d'un terminal mobile H.323**: ce service relève intégralement de la gestion des appels d'un utilisateur mobile puisqu'on suppose qu'un utilisateur (voire un utilisateur par défaut) doit nécessairement être associé au terminal aux fins de la gestion des appels;

6) **transfert d'un terminal mobile H.323**: ce service permet à un terminal mobile H.323 de rester en communication lorsqu'il passe d'un emplacement à un autre. Cette fonctionnalité appelle un complément d'étude.

5.2.3 Prescriptions applicables à l'identification de la mobilité

5.2.3.1 Identification d'utilisateur mobile

Un utilisateur peut avoir plusieurs identités différentes destinées à différents usages. Une identité d'utilisateur peut trouver au moins trois utilisations différentes:

– la plus évidente de ces utilisations est celle qui est faite par un utilisateur appelant lorsqu'il appelle un correspondant. Un numéro e164 est un exemple de ce type d'identité, appelée ici **identité d'utilisateur appelable**;

– une identité d'utilisateur peut également servir à identifier un utilisateur de manière permanente auprès du fournisseur de services de rattachement pendant toute la durée de l'abonnement souscrit par l'utilisateur. Cette identité, appelée ici l'**identité d'utilisateur principale**, est l'identité principale d'après laquelle toutes les autres identités de l'utilisateur sont établies. Ce type d'identificateur permet à un utilisateur d'avoir plusieurs identités d'utilisateur appelables ou d'en changer tout en conservant la même identité principale (et par conséquent le même abonnement) auprès du fournisseur de services de rattachement;

– une troisième utilisation dans certains systèmes dans lesquels il peut être souhaitable de transmettre le moins souvent possible l'identité principale de l'utilisateur, consiste à identifier un utilisateur sur le plan local en lui attribuant une identité non permanente pendant un certain temps ou tant qu'il se trouve dans une partie donnée du réseau. Ce type d'identité d'utilisateur, appelée **identité temporaire d'utilisateur**, est utilisé à la place de l'identité d'utilisateur principale, généralement pour des raisons de sécurité.

Il est possible qu'une identité d'utilisateur fasse à la fois fonction d'identité d'utilisateur appelable et d'identité d'utilisateur principale, mais il faut alors pouvoir utiliser des identités d'utilisateur différentes pour ces utilisations. Si une même identité d'utilisateur sert à la fois d'identité d'utilisateur principale et d'identité d'utilisateur appelable, il ne devrait pas être nécessaire d'utiliser une identité temporaire pour l'utilisateur concerné.

Les conditions suivantes doivent être satisfaites pour les besoins de la présente Recommandation:

- l'utilisateur (et non pas le terminal) est identifié par une adresse pseudonyme (AliasAddress) conforme à la Rec. UIT-T H.225.0. L'utilisateur peut avoir plusieurs adresses pseudonymes exclusives: une adresse électronique de type identificateur (ID) de courrier électronique, une adresse URL de type ID-URL, un numéro de téléphone de type e164, un module d'identification d'utilisateur (UIM) comportant, par exemple, une identité internationale d'abonné mobile (IMSI, *international mobile subscriber identity*), etc;
- tous les types d'identités d'utilisateur – identité d'utilisateur appelable, identité d'utilisateur principale et identité temporaire – doivent être des adresses pseudonymes (AliasAddresses);
- les identités d'utilisateur doivent être uniques dans la partie d'un système H.323 dans laquelle elles peuvent être utilisées. Il s'ensuit que l'identité d'utilisateur principale ainsi que les identités d'utilisateur appelables utilisables dans le monde entier doivent être uniques à l'échelle planétaire. Toutefois, des identités d'utilisateur appelables à usage local (numéros abrégés, par exemple) peuvent être admises. Des identités temporaires d'utilisateur pourront aussi présenter un intérêt sur un plan local uniquement.

5.2.3.2 Identification d'un terminal mobile

Bien qu'aux fins de l'acheminement des appels et de la gestion de la mobilité l'identité du terminal utilisé par un utilisateur mobile ne soit d'aucune utilité, dans certains cas il pourra être nécessaire d'identifier aussi le terminal, par exemple pour interdire l'utilisation de terminaux volés ou utilisés sans licence.

Les conditions suivantes doivent être satisfaites pour les besoins de la présente Recommandation:

- le terminal (matériel et/ou logiciel) peut avoir une signature, de type ID-h323, par exemple, émise par le fournisseur du terminal au stade de la fabrication. Cette signature doit être unique et ne jamais changer pendant toute la durée de vie du terminal;
- pour les besoins de l'acheminement des appels, les terminaux sont identifiés par leur adresse de couche Réseau et, occasionnellement, par leur adresse de liaison de données.

5.2.3.3 Identification de domaine administratif

L'identification du domaine administratif répond au moins à deux finalités. Tout d'abord, elle est nécessaire pour identifier le domaine administratif de rattachement d'un utilisateur aux fins de la mise à jour de l'information de position de l'utilisateur et pour connaître la position de celui-ci lorsqu'il est appelé. Deuxièmement, l'utilisateur peut préférer certains domaines administratifs à d'autres, au motif, par exemple, que le service y est meilleur marché ou que des accords de service ont été conclus entre le fournisseur de services de rattachement et d'autres fournisseurs de services.

Le domaine administratif de rattachement peut être identifié par un identificateur expressément prévu à cet effet; son identité peut aussi être déduite de l'identité de l'utilisateur (dans le cas de numéros e164 hiérarchiques ou d'adresses pseudonymes (AliasAddresses) de type identificateur (ID) de courrier électronique, par exemple).

Les conditions suivantes doivent être satisfaites pour les besoins de la présente Recommandation:

- chaque domaine administratif doit pouvoir être identifié par une identité de domaine administratif;
- on doit pouvoir déduire l'identité du domaine de rattachement d'après les différentes identités de l'utilisateur utilisées dans le monde entier. Les identités d'utilisateur à usage local ne sont pas tenues de comporter l'information relative au domaine de rattachement.

5.2.3.4 Identification de zone

L'identification de la zone (c'est-à-dire du portier) peut être nécessaire si l'utilisateur préfère certaines zones (du même domaine administratif) à d'autres. Dans ce cas, il est nécessaire de connaître l'identité de la zone et du portier avant que l'utilisateur (et le terminal) se fasse enregistrer auprès de la zone.

Les conditions suivantes doivent être satisfaites pour les besoins de la présente Recommandation:

- une ou plusieurs zones et un ou plusieurs portiers doivent pouvoir être configurés en tant que zones ou portiers de rattachement d'un utilisateur. L'information relative à la zone ou au portier de rattachement devrait être incluse dans le profil de service de l'utilisateur.
- le terminal mobile H.323 doit pouvoir identifier le portier qui lui répond pendant la procédure de recherche dudit portier et choisir la zone auprès de laquelle il souhaite se faire enregistrer, en fonction de cette information et du profil de service de l'utilisateur.

5.3 Procédures requises pour la gestion de la mobilité

La gestion de la mobilité H.323 nécessite la mise en œuvre des procédures suivantes:

- mise en place de mécanismes de recherche de portier aux fins de l'identification et du choix des domaines administratifs souhaités ou de la zone préférée;
- mise à jour de la position du terminal/utilisateur mobile au moment où il se fait enregistrer, annule son enregistrement ou change de point de rattachement de réseau.

  NOTE – Le terme "désenregistrement" est utilisé pour désigner la procédure de terminaison de l'état en ligne au niveau de l'utilisateur. Les procédures protocolaires H.510 ci-dessous utilisent à la place le terme "annulation d'enregistrement", conformément à la terminologie H.323/H.225.0;
- authentification mutuelle du terminal ou de l'utilisateur et du réseau;
- partage du profil de service de l'utilisateur entre le domaine de rattachement et le portier (visité), en fonction des besoins;
- demandes d'autorisation de service (pour un appel sortant, par exemple) en fonction du profil de service de l'utilisateur;
- localisation du terminal ou de l'utilisateur mobile pour des appels entrants.

5.4 Procédures requises pour la mise en service et la configuration d'entités mobiles H.323

Ces procédures ne relèvent pas du domaine d'application de la présente Recommandation.

6 Architecture pour la mobilité H.323

6.1 Modèle architectural

La Figure 1 montre l'architecture fonctionnelle et les points de référence à utiliser pour la gestion de la mobilité dans les systèmes H.323, conformément à l'architecture fonctionnelle de l'Annexe G/H.225.0. Des entités fonctionnelles supplémentaires (VLF, HLF, AuF) peuvent être associées à des éléments H.323 existants – portiers, éléments frontière – ou correspondre à des éléments externes à la Rec. UIT-T H.323 existante. Dans ce dernier cas, illustré sur la Figure 1, ces entités fonctionnelles peuvent être considérées comme des services d'extrémité, auquel cas les liaisons entre elles et les entités H.323 existantes correspondent à des instances du point de référence D. Les lignes en trait gras indiquent les liaisons qui relèvent du domaine d'application de la présente Recommandation.

Les points de référence entre les éléments de l'entité services d'extrémité, qui ne font pas partie de l'architecture H.323 existante, ne relèvent pas du domaine d'application de la présente Recommandation. Les liaisons concernées sont représentées en lignes pointillées.

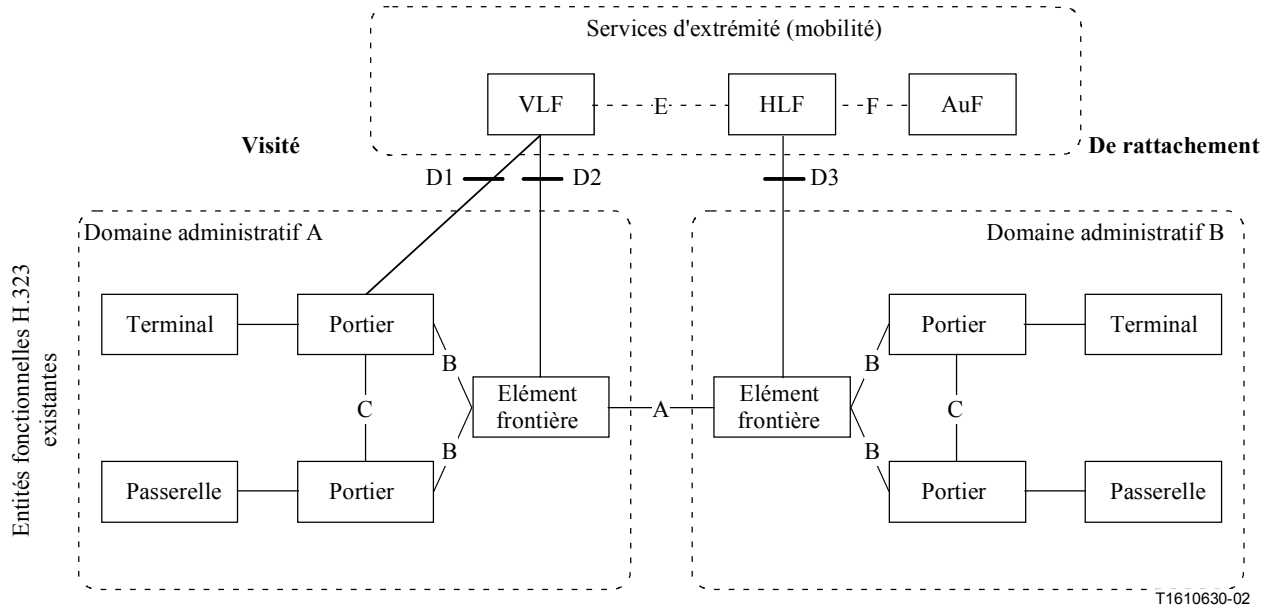


Figure 1/H.510 – Diagramme d'architecture fonctionnelle avec points de référence

6.2 Entités fonctionnelles

6.2.1 Entités spécifiques (mobilité)

Les entités fonctionnelles HLF, VLF et AuF sont définies dans d'autres Recommandations. Pour les besoins de la présente Recommandation, elles peuvent être décrites comme suit:

- l'entité fonctionnelle HLF correspond à la base de données de rattachement dans laquelle sont enregistrées les données (d'abonnement) permanentes d'un utilisateur/terminal mobile ainsi que l'emplacement où il se trouve (au moyen d'un pointeur indiquant une entité fonctionnelle VLF), si l'utilisateur ou le terminal est en ligne. Cette entité fonctionnelle est toujours associée au domaine de rattachement;
- l'entité fonctionnelle VLF correspond à une base de données dans laquelle sont enregistrées de manière temporaire les données relatives à un utilisateur/terminal visiteur, avec un pointeur indiquant le portier auprès duquel l'utilisateur ou le terminal est enregistré au moment considéré et un pointeur indiquant l'entité fonctionnelle HLF. L'entité fonctionnelle VLF est associée au domaine de desserte (de rattachement ou visité);
- l'entité fonctionnelle AuF est chargée d'authentifier un utilisateur/terminal mobile vis-à-vis du domaine de desserte (de rattachement ou visité). Elle est toujours associée à l'entité fonctionnelle HLF de l'utilisateur ou du terminal mobile et, par conséquent, au domaine de rattachement.

Une entité fonctionnelle VLF peut être associée à un ou plusieurs portiers, pour autant que ceux-ci fassent tous partie du même domaine administratif. Autrement dit, la limite supérieure de la zone de service d'une entité fonctionnelle VLF est le domaine administratif. Il en va de même pour les entités fonctionnelles HLF/AuF, bien que celles-ci puissent être moins nombreuses que les entités fonctionnelles VLF.

6.2.2 Terminal mobile H.323

Outre la fonctionnalité des terminaux H.323 standard, un terminal mobile H.323 prend en charge:

– l'association avec tout utilisateur mobile agréé;

– l'adoption d'un profil de service d'utilisateur mobile;

– le changement dynamique de réseau ou de point de rattachement H.323.

NOTE – Dans le présent contexte "dynamique" signifie que le système H.323 assure la mise à jour automatique des positions, sans qu'aucune intervention administrative ne soit nécessaire. Ce terme ne signifie pas que les communications en cours sont maintenues pendant les changements de position (en d'autres termes, le transfert n'est pas pris en charge par la présente version de la présente Recommandation).

6.2.3 Portier et élément frontière

Un terminal mobile H.323 relève d'un portier de rattachement tant qu'il se déplace dans son domaine de rattachement. S'il sort de ce domaine, il relève d'un portier visité. Dans ce dernier cas, la communication peut en outre faire intervenir des éléments frontière dans les deux domaines administratifs, c'est-à-dire le domaine de rattachement et le domaine visité.

Le portier peut aussi contenir l'information nécessaire pour gérer les appels lancés ou reçus par les terminaux mobiles H.323 enregistrés auprès de lui (par exemple, l'information de services complémentaires reçue de l'entité fonctionnelle HLF, bien que pour certains services complémentaires, le portier soit parfois tenu d'obtenir des informations supplémentaires auprès de l'entité fonctionnelle HLF).

Les portiers et les éléments frontière doivent pouvoir communiquer avec les entités fonctionnelles énumérées au § 6.2.1, sauf si les fonctions qu'elles assurent sont intégrées dans le portier ou l'élément frontière. Pour plus de précisions, voir le § 6.3.

6.3 Points de référence

Les points de référence A à D sont les mêmes que ceux qui sont définis dans l'Annexe G/H.225.0.

La présente Recommandation porte sur les relations de signalisation logique suivantes:

1) entre le portier et l'élément frontière en passant par le point de référence B;
2) entre le portier et l'entité fonctionnelle VLF en passant par le point de référence D1;
3) entre l'entité fonctionnelle VLF et l'entité fonctionnelle HLF en passant par le point de référence E (ne relève pas du domaine d'application de la présente Recommandation);
4) entre l'entité fonctionnelle HLF et l'entité fonctionnelle AuF en passant par le point de référence F (ne relève pas du domaine d'application de la présente Recommandation);
5) entre l'entité fonctionnelle VLF et l'élément frontière en passant par le point de référence D2, et entre l'entité fonctionnelle HLF et l'élément frontière en passant par le point de référence D3;
6) entre deux éléments frontière en passant par le point de référence A.

Les protocoles de signalisation pour la gestion de la mobilité sur les interfaces H.323 existantes sont les protocoles définis dans les Recs. UIT-T H.225.0 (RAS, Q.931), H.245 et H.501.

Etant donné que les entités fonctionnelles HLF, VLF et AuF peuvent coexister dans un seul et même élément de réseau comportant un portier ou un élément frontière, les points de référence peuvent être internes à ces éléments de réseau. La Figure 2 illustre un exemple de cette situation avec deux éléments de réseau composites: un élément frontière situé au même endroit que le portier et l'entité fonctionnelle VLF (appelé portier/VLF/BE) et les entités fonctionnelles HLF et AuF associées à un autre élément frontière (appelé élément frontière/HLF/AuF).

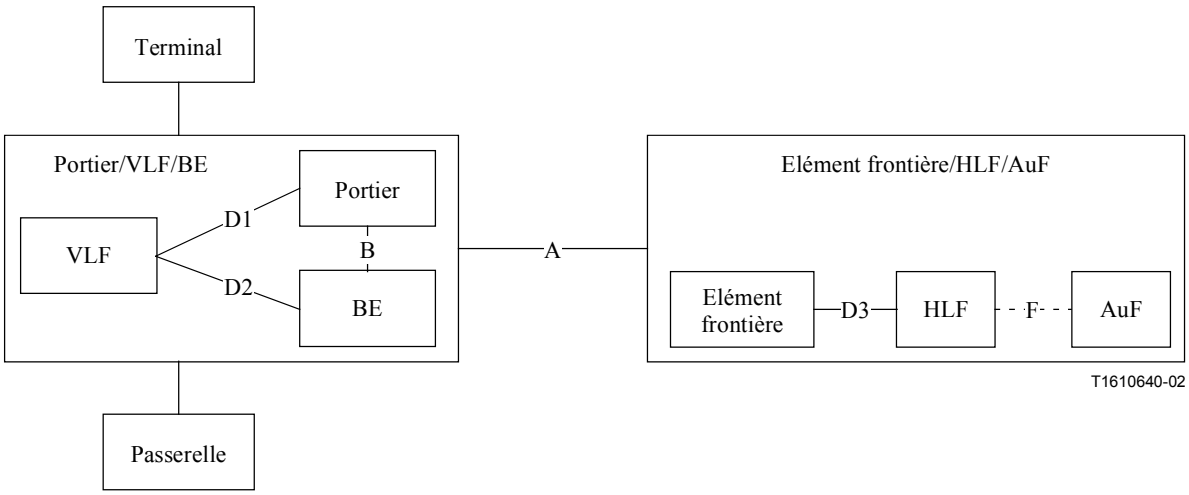


Figure 2/H.510 – Exemple d'éléments de réseau composites

7 Procédures de gestion de la mobilité

7.1 Généralités concernant les procédures de gestion de la mobilité

Le présent paragraphe décrit les procédures prévues pour assurer les fonctions de gestion de la mobilité dans les systèmes H.323. Ces procédures sont présentées sous la forme de diagrammes de flux d'information (ou diagrammes de séquences de messages) assortis d'explications complémentaires.

Les procédures de gestion de la mobilité se répartissent en trois catégories principales:

- **procédures d'annonce de l'espace de l'adresse de l'entité fonctionnelle HLF**: procédures à mettre en œuvre avant que les utilisateurs associés à une entité fonctionnelle HLF puissent être contactés. Ces procédures sont mises en œuvre entre les entités fonctionnelles HLF et les éléments frontière/portiers afin d'annoncer les identités des utilisateurs dont on peut déterminer la position en contactant l'entité fonctionnelle HLF;
- **procédures de mise à jour de position**: procédures à mettre en œuvre lorsqu'un utilisateur mobile, qui utilise un terminal H.323, change de point de rattachement H.323 (c'est-à-dire de zone) ou de point de rattachement de réseau (c'est-à-dire d'adresse de réseau), ou lorsque l'utilisateur accède au système pour la première fois après une période d'absence (c'est-à-dire lorsqu'au moment considéré aucune information de position concernant l'utilisateur n'est enregistrée dans l'entité fonctionnelle HLF associée). Ces procédures recouvrent les procédures de recherche, d'enregistrement et d'annulation d'enregistrement du portier.

  NOTE – La façon dont le terminal constate qu'il a changé de point de rattachement de réseau est une question d'implémentation qui ne relève pas du domaine d'application de la présente Recommandation. Par exemple, la pile IP du terminal informe l'application correspondante que l'adresse IP a changé;
- **procédures de gestion de la mobilité relatives aux appels**: procédures à mettre en œuvre lorsqu'un appel à destination ou en provenance d'un utilisateur mobile, qui utilise un terminal H.323, aboutit. Cette procédure de gestion de la mobilité englobe l'échange des informations nécessaires pour localiser l'utilisateur appelé.

Les procédures de gestion de la mobilité relatives aux appels ne s'appliquent pas à la mobilité permanente du terminal, c'est-à-dire aux transferts. Les procédures de transfert ne font pas partie de la version 1 de la présente Recommandation.

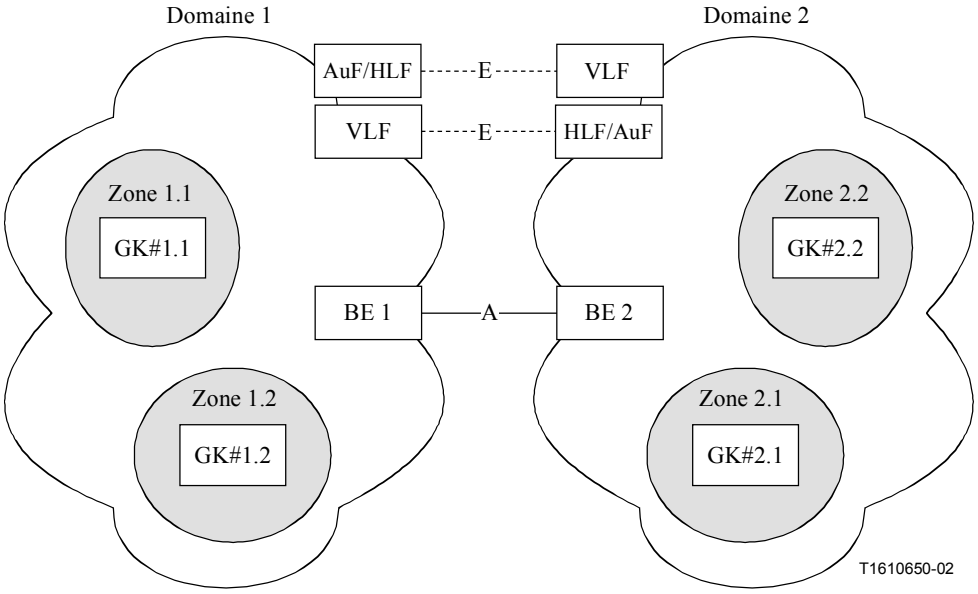
7.2 Exemples de scénarios pour les procédures de gestion de la mobilité

Afin d'illustrer les diverses possibilités de changements de position, la Figure 3 montre un exemple de deux domaines, englobant chacun deux zones.

On peut distinguer les scénarios de changements de position suivants:

1) changement de position intrazone au sein du domaine de rattachement. Par exemple, un utilisateur/terminal rattaché au Domaine 1 quitte la position qu'il occupe dans la zone 1.1 pour une autre position dans la même zone;
2) changement de position intrazone au sein du domaine visité. Par exemple, un utilisateur/terminal rattaché au Domaine 1 quitte la position où il se trouve dans la zone 2.1 pour une autre position dans la même zone;
3) changement de position interzone au sein du domaine de rattachement. Par exemple, un utilisateur/terminal rattaché au Domaine 1 quitte la position où il se trouve dans la zone 1.1 pour une autre position dans la zone 1.2;
4) changement de position intrazone au sein du domaine visité. Par exemple, un utilisateur/terminal rattaché au Domaine 1 quitte la position où il se trouve dans la zone 2.1 pour une autre position dans la zone 2.2;
5) changement de position interdomaine. Par exemple, un utilisateur/terminal rattaché au Domaine 1 quitte la position où il se trouve dans la zone 1.1 pour une autre position dans la zone 2.2.

Les procédures décrites dans les paragraphes qui suivent s'appliquent au scénario le plus général (scénario 5). Les autres scénarios peuvent être déduits du scénario 5) en sautant certaines étapes de la procédure.



NOTE – Pour simplifier les choses, les liaisons intradomaine ne sont pas représentées sur cette figure; voir la Figure 1 pour ces liaisons.

Figure 3/H.510 – Modèle de scénarios

7.3 Procédures d'annonce d'espace d'adresse d'entités fonctionnelles HLF

7.3.1 Disposition statique

Dans une disposition statique, les portiers et les éléments frontière configurés sont assortis des adresses des entités fonctionnelles HLF qu'ils contacteront pour déterminer l'identité de l'utilisateur appelable ou son identité principale. Les différentes identités d'utilisateur possibles et les entités fonctionnelles HLF associées sont connues du portier ou de l'élément frontière par le biais de la configuration ou de la gestion. L'entité fonctionnelle HLF appropriée est sélectionnée d'après le contenu de l'identité d'utilisateur actuelle.

Les procédures de configuration ou de mise à jour des portiers et des éléments frontière dans une disposition statique ne relèvent pas du domaine d'application de la présente Recommandation.

7.3.2 Disposition dynamique

Dans une disposition dynamique, les portiers et les éléments frontière sont informés des identités d'utilisateur et des entités fonctionnelles HLF associées de façon dynamique au moyen d'un protocole. Les entités fonctionnelles HLF doivent utiliser les procédures et les messages décrits dans la Rec. UIT-T H.501 pour incorporer les identités d'utilisateur dans leur base de données, c'est-à-dire leur espace d'adresse, pour les annoncer aux portiers et aux éléments frontière.

Les portiers et les éléments frontière doivent envoyer les messages **DescriptorIDRequest** (*demande d'identificateur de descripteur*) et **DescriptorRequest** (*demande de descripteur*) aux entités fonctionnelles HLF pour être informés de l'espace d'adresse desdites entités fonctionnelles et celles-ci en réponse à ces interrogations, doivent respectivement envoyer un message **DescriptorIDConfirmation** (*confirmation d'identificateur de descripteur*) et un message **DescriptorConfirmation** (*confirmation de descripteur*) afin d'annoncer leurs espaces d'adresse. Les entités fonctionnelles HLF devraient aussi envoyer des messages **DescriptorUpdate** (*mise à jour de descripteur*) aux portiers/éléments frontière en cas de modification de leur espace d'adresse. Les portiers/éléments frontière et les entités fonctionnelles HLF peuvent établir une relation de service à l'aide des messages **ServiceRequest** (*demande de service*) et **ServiceConfirmation** (*confirmation de service*) comme indiqué dans la Rec. UIT-T H.501, avant de communiquer entre eux d'une quelque autre manière.

D'après les informations recueillies grâce à cet échange de messages, les portiers et les éléments frontière sont à même de déterminer d'après les identités des utilisateurs mobiles l'entité fonctionnelle HLF à contacter pour chaque utilisateur mobile.

7.3.3 Structure des adresses

Selon la Rec. UIT-T H.501, les descripteurs peuvent contenir des adresses pseudonymes de format courrier électronique ou numéro d'abonné (par défaut sous la forme d'un numéro international e164). Par accord entre les domaines concernés, d'autres formats d'adresses pseudonymes peuvent être admis (numéros d'abonnés d'un plan de numérotage privé, par exemple). Les formats des identités d'utilisateur mobile (de type identificateur IMSI) devront en tout état de cause faire l'objet d'un tel accord.

Les portiers, les éléments frontière et les entités fonctionnelles HLF conformes à la présente Recommandation doivent admettre les identités d'utilisateur se présentant sous la forme d'adresses pseudonymes, comme indiqué dans la Rec. UIT-T H.225.0 (*AliasAddress* de type ASN.1), des formats suivants:

– **identités d'utilisateur appelables**: adresse de courrier électronique (de type *AliasAddress.email-ID*) ou numéro e164 (international) (de type *AliasAddress.partyNumber.e164*) ou, à titre facultatif, numéro d'abonné privé (complet) (de type *AliasAddress.partyNumber.privateNumber*);

– **identités principales d'utilisateur**: une des identités d'utilisateur appelables ou identificateur d'accès au réseau (NAI, voir RFC 2486), ou identité d'utilisateur mobile mondial (de type *AliasAddress.mobileUIM*), contenant, par exemple, un identificateur IMSI. L'identificateur NAI est du type *AliasAddress.email-ID* même s'il ne correspond pas à une adresse de courrier électronique appelable.

Les autres formats et identificateurs appellent un complément d'étude.

Les procédures ne font pas la différence entre les identités d'utilisateur appelables et les identités principales d'utilisateur. Ces procédures appellent un complément d'étude.

7.4 Procédures de mise à jour de position

Les procédures de mise à jour de position sont mises en œuvre:

– lorsqu'un terminal mobile H.323 se met (remet) en marche;

– lorsqu'un terminal mobile H.323 change d'emplacement;

– lorsqu'un utilisateur mobile se connecte sur un terminal mobile H.323 donné.

Les procédures de mise à jour de position utilisent les procédures RAS H.225.0: recherche du portier, enregistrement et annulation d'enregistrement.

7.4.1 Recherche du portier

7.4.1.1 Généralités

Du point de vue du système H.323, la procédure de recherche du portier est la première procédure que le terminal mobile H.323 exécute quand il doit mettre à jour une position. La mise à jour d'une position intrazone constitue la seule exception à cette règle, la recherche du portier n'étant pas nécessaire puisque le terminal mobile H.323 reste enregistré auprès du même portier qu'auparavant.

Un terminal mobile H.323 doit lancer la procédure de recherche du portier lorsqu'un ou plusieurs des événements ou situations suivants se produisent:

- le terminal mobile H.323 peut maintenant accéder au réseau de base grâce à un nouveau point de rattachement de réseau. Par exemple, le terminal a obtenu une adresse IP auprès d'un serveur DHCP. Cette situation englobe la mise en service du terminal mobile H.323 ainsi que le cas où le terminal mobile H.323 change de point de rattachement de réseau (NPoA) en cours de route;
- le terminal mobile H.323 a perdu la connexion avec le portier auprès duquel il était précédemment enregistré. La perte a pu se produire de manière progressive, le portier envoyant alors un message URQ au terminal mobile H.323, ou de manière brutale, en raison par exemple d'une coupure de la liaison sur le trajet de communication entre le terminal mobile H.323 et le portier;
- une demande d'enregistrement a échoué pour le motif *discoveryRequired* (recherche nécessaire).

Il existe plusieurs méthodes d'implémentation de la procédure de recherche du portier, qui dépendent des capacités du réseau de base (selon que celui-ci prend en charge ou non le mode multidiffusion, par exemple) et de la partie du système H.323 à laquelle il est accédé. Les méthodes que peuvent utiliser les terminaux mobiles H.323 sont énumérées ci-après. Un terminal mobile H.323 peut mettre en œuvre certaines ou la totalité de ces méthodes, dans l'ordre de préférence configurée dans ledit terminal.

1) Message GRQ en mode multidiffusion.

2) Envoi d'un message GRQ en mode unidiffusion à un portier, dont l'adresse a été précédemment mise en antémémoire ou enregistrée d'une autre manière.

3) Interrogation SRV sur le domaine du portier (gk_domain) (IV.1.1/H.225.0).

4) Interrogation relative à des enregistrements TXT sur le domaine du portier (gk_domain) (IV.1.1/H.225.0).

5) Interrogation relative à des enregistrements "A" sur le domaine du portier (gk_domain).

6) Recherche manuelle (7.2.1/H.323).

Les méthodes 3 à 5 utilisent le système de dénomination (DNS, *domain name system*). La recherche manuelle ne relève pas du domaine d'application de la présente Recommandation.

7.4.1.2 Recherche d'un portier de desserte

Tant qu'un terminal H.323 se déplace à l'intérieur de son domaine de rattachement, le portier de desserte sera un portier de rattachement. Si le terminal mobile en question sort de son domaine de rattachement, le portier de desserte sera un portier visité. N'importe laquelle des méthodes énumérées au § 7.4.1.1 permettra d'obtenir l'adresse ou les adresses d'un ou de plusieurs portiers, si elle est appliquée avec succès.

Si l'adresse du portier a été trouvée à l'aide de la méthode 3, 4 ou 5, le terminal mobile H.323 doit envoyer un message GRQ (en mode unidiffusion) au portier en question. Si l'adresse du portier a été trouvée à l'aide de la méthode 1 ou 2, le terminal mobile H.323 doit essayer de se faire enregistrer auprès d'un des portiers, comme indiqué au § 7.4.2.

S'il reçoit un message GRQ (en mode unidiffusion), le portier doit exécuter l'une des deux opérations suivantes:

1) envoyer un message GCF s'il est appelé à devenir le portier de desserte et autoriser le terminal à se faire enregistrer;

2) envoyer un message GRJ, accompagné ou non d'une liste de portiers de remplacement.

Selon la réponse du portier, le terminal doit exécuter l'une des trois opérations suivantes:

1) si le portier lui a envoyé en réponse un message GCF, le terminal mobile H.323 doit essayer de se faire enregistrer auprès de ce portier, comme indiqué au § 7.4.2;

2) si le portier lui a envoyé en réponse un message GRJ et une liste de portiers de remplacement, le terminal mobile H.323 doit alors parcourir la liste de haut en bas en commençant par le message GRQ jusqu'au portier dont l'ordre de priorité est le plus élevé;

3) si le portier lui a envoyé en réponse un message GRJ non accompagné d'une liste de portiers de remplacement, le terminal mobile H.323 devrait alors utiliser la liste de portiers de remplacement qu'il a éventuellement reçue précédemment. Si le terminal mobile H.323 ne dispose pas d'une liste de portiers de remplacement, il est alors dans l'impossibilité de trouver un portier auprès duquel il puisse se faire enregistrer.

7.4.2 Enregistrement

Un terminal mobile H.323 doit mettre en œuvre la procédure d'enregistrement si un des événements suivants s'est produit. Le terminal doit déjà détenir l'information relative au portier auquel il va envoyer l'enregistrement (RRQ).

- le terminal fait (refait) son apparition dans une zone (par exemple, après sa mise sous tension). Dans ce cas, la recherche du portier doit être effectuée avant le début de l'enregistrement (voir le § 7.4.1);
- un nouvel utilisateur commence à utiliser le terminal. Si celui-ci est déjà enregistré, il n'est pas nécessaire de procéder à la recherche du portier. Si un utilisateur précédent est toujours enregistré et que le terminal accepte le nouvel utilisateur, le nouvel enregistrement remplace le précédent, ce qui entraîne l'annulation de l'enregistrement de l'utilisateur précédent par le portier (voir le § 7.4.3);

- le terminal a changé d'emplacement et relève maintenant d'un autre point de rattachement de réseau (NPoA) que celui auprès duquel il était précédemment enregistré. Il faudra procéder à la recherche du portier (voir le § 7.4.1) avant d'effectuer l'enregistrement, sauf si l'on sait que le nouveau point NPoA est également situé dans la zone du portier précédent (cas d'un changement d'emplacement intrazone);
- chaque fois qu'un terminal mobile entre dans une nouvelle zone sans être en communication (même si le point NPoA ne change pas);
- en cas de perte de l'enregistrement précédent (venu à expiration, par exemple). Une telle perte peut être détectée, par exemple, par l'envoi par le portier, en réponse à un message ARQ, d'un message ARJ indiquant que le terminal mobile n'est pas enregistré. Si l'on sait (d'après le message ARJ, par exemple) qu'il existe un portier de remplacement, on peut essayer de procéder à l'enregistrement auprès de ce portier. Dans le cas contraire, il faut d'abord procéder à la recherche du portier (voir le § 7.4.1);
- à titre d'indication de maintien (enregistrement "allégé", voir la Rec. UIT-T H.225.0), pour prolonger la durée de vie de l'enregistrement en cours.

7.4.3 Annulation d'enregistrement

La procédure d'annulation d'enregistrement a pour but de mettre fin à l'enregistrement d'un utilisateur ou d'un terminal mobile H.323 auprès d'un portier. Si le terminal a également sa propre adresse pseudonyme (aliasAddress), sous forme d'identificateur (ID) de terminal, par exemple, l'annulation de l'enregistrement d'un utilisateur met également fin à l'enregistrement de cette adresse ou de cet identificateur. Si l'enregistrement d'un terminal mobile H.323 est annulé, l'enregistrement de l'utilisateur qui utilise ce terminal est lui aussi annulé. Un terminal mobile H.323 devrait faire annuler son enregistrement si un ou plusieurs des événements ou situations suivants se produisent:

- l'application du terminal mobile H.323 est sur le point d'être arrêtée;
- un utilisateur du terminal souhaite annuler son enregistrement auprès du système H.323;
- le terminal mobile H.323 va couper la connexion qui le relie, via son point NPoA actuel, au portier auprès duquel il est enregistré, mais il ne va pas se connecter immédiatement à un autre portier via un autre point NPoA.

  Si le terminal mobile H.323, au moment où il change d'emplacement, se connecte à un système H.323 via un nouveau point NPoA immédiatement après s'être déconnecté de l'ancien point NPoA, ledit terminal mobile H.323 n'aura pas besoin d'annuler son enregistrement du fait que celui-ci sera implicitement annulé par la procédure de mise à jour de position;
- le portier, l'entité fonctionnelle VLF ou l'entité fonctionnelle HLF demandent l'annulation de l'enregistrement d'un utilisateur ou du terminal mobile H.323, par exemple dans le cas où la durée de vie de cet enregistrement vient à expiration.

7.4.4 Flux d'information pour les procédures de mise à jour de position

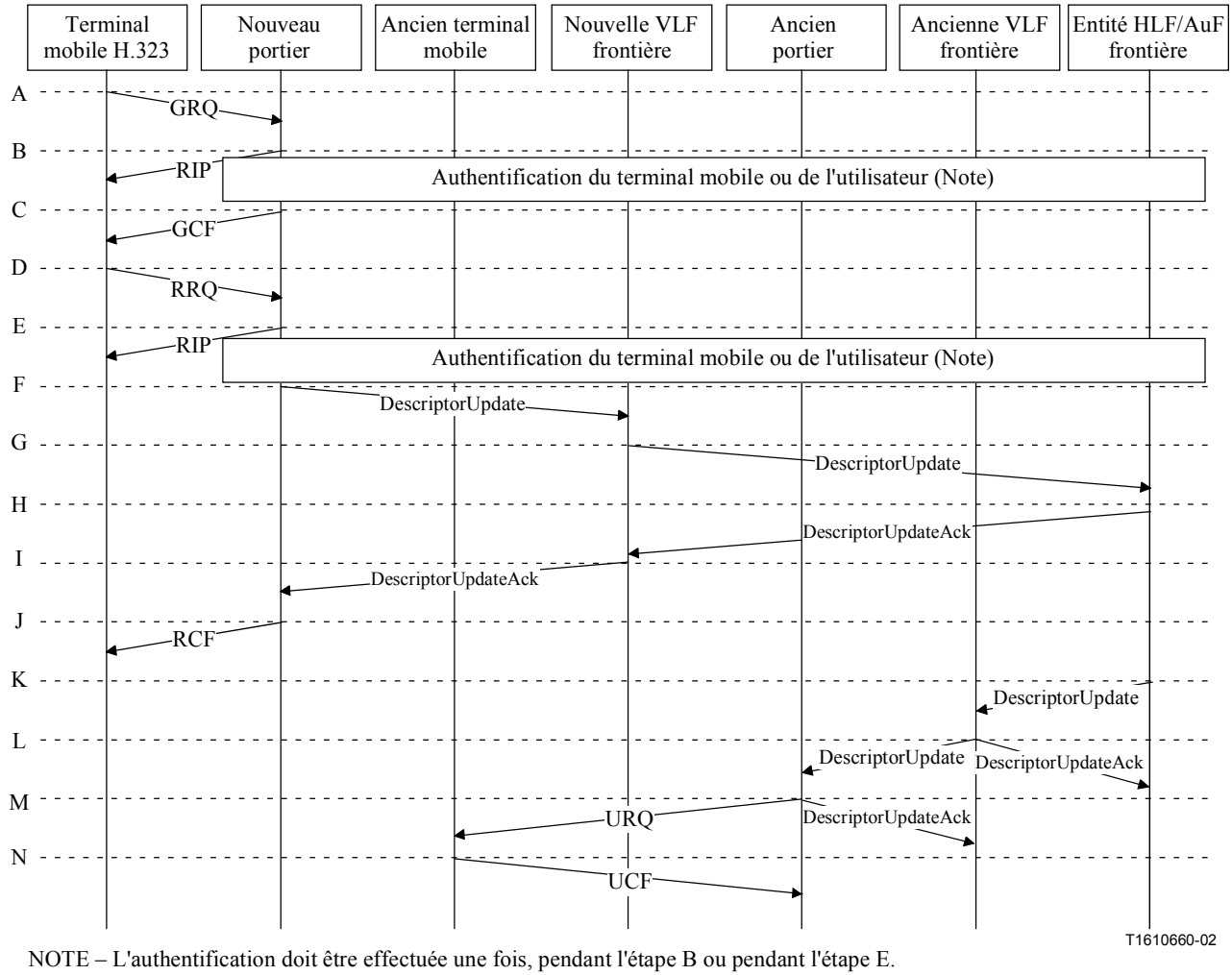
La Figure 4 représente le flux d'information complet pour la procédure de mise à jour de position. Le flux complet s'applique lorsque le terminal mobile H.323, en changeant d'emplacement, passe d'un domaine visité à un autre. Dans ce cas, l'ancien portier et l'ancienne entité fonctionnelle VLF conservent l'information de position relative à l'utilisateur de ce terminal.

Dans les cas suivants, seules certaines parties du flux complet s'appliquent, comme indiqué dans la description détaillée figurant sous la Figure 4:

– le terminal mobile H.323 change d'emplacement (c'est-à-dire de point NPoA) à l'intérieur de la même zone (la recherche du portier n'est pas nécessaire et les informations figurant dans l'entité fonctionnelle VLF ou HLF ne changent pas);

– le terminal mobile H.323 change de zone à l'intérieur du même domaine visité (l'ancienne entité fonctionnelle VLF et la nouvelle sont les mêmes et les informations figurant dans l'entité fonctionnelle HLF ne changent pas);

– le terminal (ou l'utilisateur) mobile H.323 se fait enregistrer pour la première fois depuis l'annulation de son précédent enregistrement (l'ancienne entité fonctionnelle VLF ou l'ancien portier ne contient donc aucune information de position précédente à supprimer).



NOTE – L'authentification doit être effectuée une fois, pendant l'étape B ou pendant l'étape E.

Figure 4/H.510 – Flux d'information pour la procédure de mise à jour de position

La signification des étapes indiquées sur la Figure 4 est la suivante:

Les étapes A à C ne sont pas nécessaires pour changer d'emplacement (de point NPoA) à l'intérieur de la même zone, ou pour maintenir l'enregistrement en vigueur.

A: les conditions de lancement des procédures de mise à jour de position avec recherche du portier ont été remplies. En conséquence, le terminal mobile H.323 envoie un message GRQ au portier. Ce message doit comporter dans le champ *endpointAlias* (pseudonyme d'extrémité) toutes les identités de l'utilisateur (y compris son identité principale) qui peuvent être utilisées pour identifier l'utilisateur;

B: l'authentification ne sera généralement effectuée qu'une seule fois pendant la mise à jour de la position, c'est-à-dire pendant l'étape B ou pendant l'étape E. S'il authentifie l'utilisateur à ce stade, le portier doit procéder à l'authentification comme indiqué dans la Rec. UIT-T H.530. Il peut renvoyer un message RIP (demande en cours, *request in*

progress) au terminal mobile H.323 pour lui indiquer qu'il tardera peut-être à répondre à son message GRQ.

S'il n'accepte pas cette demande de l'utilisateur, le portier doit envoyer un message GRJ au terminal mobile H.323.

C: le portier renvoie un message GCF au terminal mobile H.323 pour lui indiquer qu'il acceptera l'enregistrement. Si l'étape B a été exécutée, le message GCF contiendra l'information d'authentification que devra utiliser le terminal mobile pour le message RRQ suivant;

D: le terminal mobile H.323 envoie une demande d'enregistrement (RRQ) au portier (déjà connu). Sauf s'il s'agit de maintenir l'enregistrement en vigueur, le message RRQ doit comporter dans le champ *terminalAlias* (pseudonyme du terminal) toutes les identités de l'utilisateur (y compris son identité principale) qui peuvent être utilisées pour identifier l'utilisateur et qui ont été indiquées par celui-ci;

E: l'authentification ne sera généralement effectuée qu'une seule fois pendant la mise à jour de la position, c'est-à-dire pendant l'étape B ou pendant l'étape E. S'il authentifie l'utilisateur à ce stade, le portier doit procéder à l'authentification comme indiqué dans la Rec. UIT-T H.530. Il peut renvoyer un message RIP au terminal mobile H.323 pour lui indiquer qu'il tardera peut-être à répondre à son message RRQ.

S'il n'accepte pas la demande de l'utilisateur, le portier doit envoyer un message RRJ au terminal mobile H.323;

F: si le terminal mobile H.323 et l'utilisateur qui l'utilise sont déjà enregistrés, le portier met à jour l'enregistrement et passe à l'étape J. Tel est le cas si le terminal mobile H.323 change de point NPoA à l'intérieur de la même zone ou s'il s'agit de renouveler l'enregistrement précédent (dans le cadre d'un mécanisme périodique visant à le maintenir en vigueur, par exemple).

S'il constate que l'utilisateur n'est pas déjà enregistré, le portier envoie un message **DescriptorUpdate** (mise à jour du descripteur) à l'entité fonctionnelle VLF ou à l'élément frontière à laquelle/auquel il est associé (une fois l'authentification dûment effectuée).

Le message **DescriptorUpdate** doit comporter l'adresse TSAP (point d'accès au service de transport) du portier sous la forme d'une adresse pseudonyme (*aliasAddress*) dans le champ *sender* (expéditeur) du message, le champ *updateInfo* (information de mise à jour) contenant un descripteur avec un nouvel identificateur (*descriptorID*) dans le champ *descriptorInfo* (information de descripteur) et le paramètre *updateType* (type de mise à jour) positionné sur *added* (ajouté). Dans le champ *templates* (modèles), chaque descripteur (*descriptor*) doit comporter sous forme de structures déterminées toutes les identités de l'utilisateur (y compris son identité principale) qui doivent être enregistrées, ainsi que le paramètre *sendSetup* en tant que type de message (*messageType*) du champ *routeInfo* (information de routage). Le descripteur peut aussi comporter l'identificateur du portier (*gatekeeperID*) qui a envoyé le message **DescriptorUpdate**. En outre, le portier enregistre l'adresse du point NPoA via lequel le terminal mobile H.323 se connecte à lui;

G: à la réception du message **DescriptorUpdate**, l'entité fonctionnelle VLF ou l'élément frontière doit vérifier chaque descripteur (*descriptor*) par rapport aux descripteurs déjà enregistrés par suite des précédentes opérations de mise à jour de position. Si l'utilisateur était déjà enregistré dans l'entité fonctionnelle VLF ou l'élément frontière, celle-ci/celui-ci doit procéder comme indiqué dans l'étape I ci-dessous. Dans ce cas, l'ancienne et la nouvelle entité fonctionnelle VLF ou l'ancien et le nouvel élément frontière sont les mêmes. De plus, l'entité fonctionnelle VLF ou l'élément frontière doit envoyer un message **DescriptorUpdate** à l'ancien portier, comme indiqué dans l'étape L ci-dessous.

L'entité fonctionnelle VLF ou l'élément frontière doit remplacer le champ *messageType* (type de message) par le champ *sendAccessRequest* (émission de demande d'accès) et le champ *sender* (expéditeur) par sa propre adresse TSAP. Si l'identificateur du portier (*gatekeeperID*) figurait dans le descripteur (*descriptor*) envoyé par le portier, l'entité fonctionnelle VLF ou l'élément frontière peuvent le supprimer du message, avant de faire suivre celui-ci. Enfin, l'entité fonctionnelle VLF ou l'élément frontière détermine l'adresse TSAP de l'entité fonctionnelle HLF ou de l'élément frontière de l'utilisateur d'après l'identité principale de celui-ci contenue dans le descripteur (*descriptor*), et envoie le message **DescriptorUpdate** à l'entité fonctionnelle HLF ou à l'élément frontière;

H: l'entité fonctionnelle HLF ou l'élément frontière enregistre l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière sous la forme de l'information de position relative à l'utilisateur indiqué par l'identité principale de celui-ci dans le message **DescriptorUpdate** et envoie un message **DescriptorUpdateAck** (*accusé de réception de mise à jour de descripteur*) en réponse à l'entité fonctionnelle VLF ou à l'élément frontière;

I: l'entité fonctionnelle VLF ou l'élément frontière enregistre toutes les identités de l'utilisateur qu'elle/il reçoit, l'adresse TSAP de l'entité fonctionnelle HLF ou de l'élément frontière de cet utilisateur et l'adresse TSAP du portier qu'elle/il a reçue durant l'étape G sous la forme de l'information de position relative à cet utilisateur, et envoie un message **DescriptorUpdateAck** au portier;

J: le portier enregistre le point NPoA ainsi que toutes les identités d'utilisateur que lui a communiquées le terminal mobile H.323 dans le message RRQ au cours de l'étape D. Le portier envoie au terminal mobile H.323 un message RCF lui indiquant que la mise à jour de la position a été effectuée avec succès.

Les étapes K à M ne sont exécutées que si l'information de position précédente relative à l'utilisateur figurait dans les entités fonctionnelles HLF ou dans l'élément frontière ainsi que dans le portier (précédent) et l'entité fonctionnelle VLF ou l'élément frontière (le cas échéant) avant que l'étape G ne soit exécutée.

K: l'entité fonctionnelle HLF ou l'élément frontière peut exécuter cette étape immédiatement après l'étape H, afin d'assurer en temps utile la mise à jour de l'information de position dans l'ensemble du réseau. L'entité fonctionnelle HLF ou l'élément frontière doit envoyer un message **DescriptorUpdate** à l'ancienne entité fonctionnelle VLF ou à l'ancien élément frontière. Le message doit comporter l'adresse TSAP de l'entité fonctionnelle HLF ou de l'élément frontière dans le champ *sender* (expéditeur) et l'information de mise à jour (*updateInfo*) contenant un descripteur (*descriptor*), l'identificateur de descripteur (*descriptorID*) de l'enregistrement initial et toutes les identités enregistrées de l'utilisateur sous forme de structures déterminées, le paramètre *nonExistent* en tant que type de message (*messageType*) du champ *routeInfo* (information de routage) et le paramètre *updateType* (type de mise à jour) positionné sur *deleted* (supprimé);

L: l'entité fonctionnelle VLF ou l'élément frontière doit supprimer l'information de position précédente indiquée par le descripteur (*descriptor*) (c'est-à-dire l'adresse TSAP de l'ancien portier et toutes les identités d'utilisateur enregistrées) et envoyer un message **DescriptorUpdate**, comme indiqué dans l'étape K ci-dessus, à l'ancien portier (le champ *sender* (expéditeur) étant positionné sur l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière). En outre, l'entité fonctionnelle VLF ou l'élément frontière doit répondre à l'entité fonctionnelle HLF ou à l'élément frontière par un message **DescriptorUpdateAck**;

M: l'ancien portier doit supprimer l'information de position (c'est-à-dire le point NPoA) ainsi que les autres informations d'enregistrement qu'il détenait sur l'utilisateur indiqué par l'identificateur de descripteur (*descriptorID*) ou le descripteur (*descriptor*), et répondre à

l'entité fonctionnelle VLF ou à l'élément frontière par un message **DescriptorUpdateAck**. Il devrait en outre envoyer un message URQ au terminal mobile H.323 précédent;

N: le terminal mobile H.323 précédent répond au message URQ par un message UCF et supprime ses données d'enregistrement, s'il en détient.

La liste suivante récapitule les contenus de message utilisés dans la présente Recommandation (pour les messages ou les champs de message qui ne sont pas indiqués ici, il convient d'utiliser les messages ou champs de message indiqués dans les Recs. UIT-T H.323, H.225.0 ou H.501):

GRQ

Champ	Description
endpointAlias	Toutes les identités disponibles de l'utilisateur à enregistrer (éventuellement de l'utilisateur par défaut).

RRQ

Champ	Description
terminalAlias	Toutes les identités disponibles de l'utilisateur à enregistrer.

DescriptorUpdate

Champ	Description
sender	L'adresse TSAP de l'entité qui envoie le message.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	nouvel identificateur attribué pour cet enregistrement [si le paramètre type de mise à jour updateType est: added (ajouté)] identificateur attribué au moment de l'enregistrement [si le paramètre type de mise à jour updateType est: deleted (supprimé)]
templates	
pattern	une pour chaque identité d'utilisateur disponible
specific	l'identité d'utilisateur à enregistrer
routeInfo	
sendSetup	si ce message a été envoyé par le portier à l'entité fonctionnelle VLF ou à l'élément frontière
sendaccessrequest	si ce message a été envoyé par l'entité fonctionnelle VLF ou l'élément frontière à l'entité fonctionnelle HLF ou l'élément frontière
nonExistent	si ce message a été envoyé par l'entité fonctionnelle HLF ou l'élément frontière à l'entité fonctionnelle VLF ou l'élément frontière par l'entité fonctionnelle VLF ou l'élément frontière au portier
gatekeeperID	Eventuellement l'identificateur (ID) du portier qui a envoyé le message
updateType	
added	dans le sens GK→VLF/BE, VLF/BE→HLF/BE
deleted	dans le sens HLF/BE→VLF/BE, VLF/BE→GK

7.4.5 Annulation d'enregistrement

Il est procédé à l'annulation de l'enregistrement d'un terminal ou d'un utilisateur mobile H.323 à la demande expresse de l'utilisateur ou à la demande du portier, de l'entité fonctionnelle VLF ou de l'entité fonctionnelle HLF. L'annulation de l'enregistrement supprime de l'entité fonctionnelle HLF ou VLF et du portier l'information de position. Dans des situations anormales – perte de connexion ou dépassement de la durée de validité de l'enregistrement, le portier, l'entité fonctionnelle VLF ou

l'entité fonctionnelle HLF peuvent également supprimer l'information de position sans lancer la procédure complète d'annulation de l'enregistrement.

Les Figures 5 à 8 illustrent la procédure d'annulation d'enregistrement dans les trois cas susmentionnés.

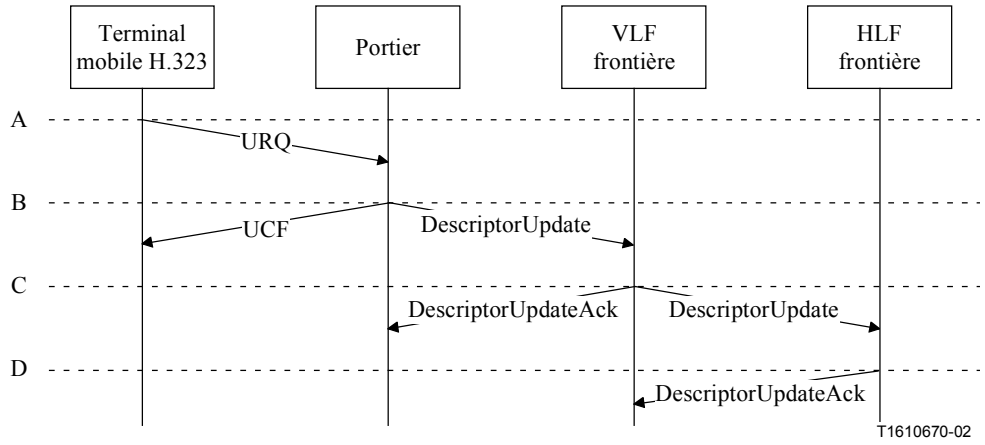


Figure 5/H.510 – Annulation de l'enregistrement à l'initiative du terminal mobile H.323

La Figure 5 illustre le lancement de la procédure d'annulation d'enregistrement par le terminal mobile H.323. Cette procédure est décrite de manière plus détaillée ci-dessous:

A: le terminal mobile H.323 envoie un message URQ au portier auprès duquel il est enregistré. Si l'annulation de l'enregistrement concerne uniquement l'utilisateur, le message URQ doit comporter toutes les identités enregistrées pour cet utilisateur dans le champ *endpointAlias* (pseudonyme d'extrémité). Si l'enregistrement du terminal mobile H.323 doit aussi être annulé, il n'y a pas lieu d'inclure une adresse pseudonyme;

B: le portier doit traiter le message URQ de la manière habituelle, c'est-à-dire supprimer la ou les adresses pseudonymes indiquées dans le message URQ, et envoyer un message **DescriptorUpdate** à l'entité fonctionnelle VLF ou à l'élément frontière qui lui est associé. Le message doit comporter l'adresse TSAP du portier dans le champ *sender* (expéditeur), l'identificateur de descripteur (*descriptorID*) précédemment attribué au moment où cet utilisateur s'est fait enregistrer, toutes les identités de l'utilisateur sous forme de structures déterminées et le paramètre *updateType* (type de mise à jour), positionné sur *deleted* (supprimé). Si le terminal mobile H.323 fait annuler son enregistrement (c'est-à-dire pas seulement son utilisateur du moment), le portier doit également supprimer l'information de position (c'est-à-dire le point NPoA) utilisée par ce terminal. Le portier doit envoyer au terminal mobile H.323 un message UCF lui confirmant l'annulation de l'enregistrement;

C: l'entité fonctionnelle VLF ou l'élément frontière doit supprimer l'information de position (c'est-à-dire l'adresse TSAP du portier et toutes les entités d'utilisateur enregistrées) indiquée par le descripteur (*descriptor*), remplacer le champ *sender* (expéditeur) du message **DescriptorUpdate** par l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière et envoyer le message **DescriptorUpdate** à l'entité fonctionnelle HLF ou à l'élément frontière de l'utilisateur. L'entité fonctionnelle VLF ou l'élément BE doit en outre répondre au portier en lui envoyant un message **DescriptorUpdateAck**;

D: l'entité fonctionnelle HLF ou l'élément frontière doit supprimer de ses données enregistrées l'information de position (c'est-à-dire l'adresse TSAP de l'entité fonctionnelle VLF ou l'élément frontière) relative à l'utilisateur indiqué par le descripteur (*descriptor*). L'entité

fonctionnelle HLF ou l'élément frontière doit en outre répondre à l'entité fonctionnelle VLF ou à l'élément frontière en lui envoyant un message **DescriptorUpdateAck**.

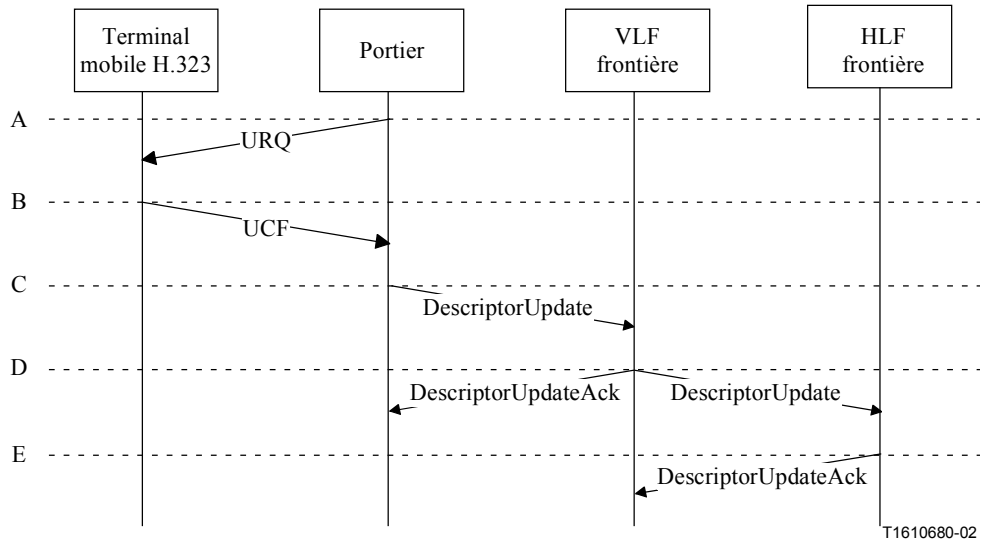


Figure 6/H.510 – Annulation d'enregistrement à l'initiative du portier

La Figure 6 illustre le lancement de la procédure d'annulation d'enregistrement par le portier. Cette procédure est décrite de manière plus détaillée ci-dessous:

A: le portier envoie un message URQ au terminal mobile H.323 qui doit procéder à l'annulation de l'enregistrement d'un de ses utilisateurs. Si seul l'enregistrement de cet utilisateur doit être annulé, le message doit comporter toutes les entités d'utilisateur enregistrées dans le champ *endpointAlias* (pseudonyme d'extrémité). Si l'enregistrement du terminal mobile H.323 doit aussi être annulé, il n'y a pas lieu d'inclure une adresse pseudonyme;

B: le terminal mobile H.323 envoie au portier un message UCF lui confirmant l'annulation de l'enregistrement. Le portier supprime l'information d'enregistrement relative à l'utilisateur ainsi que, si l'enregistrement du terminal mobile H.323 est lui aussi annulé, le point NPoA.

Les étapes C, D et E sont les mêmes que les étapes B, C et D décrites dans le cas précédent.

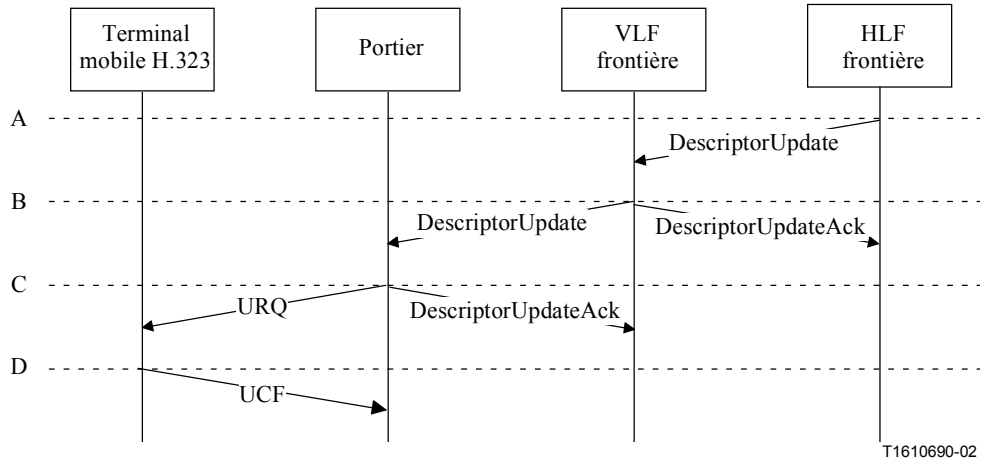


Figure 7/H.510 – Annulation d'enregistrement à l'initiative de l'entité fonctionnelle HLF

La Figure 7 illustre le lancement de la procédure d'annulation d'enregistrement par l'entité fonctionnelle HLF. Cette procédure est décrite de manière plus détaillée ci-dessous:

A: l'entité fonctionnelle HLF ou l'élément frontière supprime de ses données enregistrées l'information de position (c'est-à-dire l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière) relative à l'utilisateur et envoie un message **DescriptorUpdate** à l'entité fonctionnelle VLF ou à l'élément frontière qui détient l'information de position relative à l'utilisateur. Le message doit comporter l'adresse TSAP de l'entité fonctionnelle HLF ou de l'élément frontière dans le champ *sender* (expéditeur), l'identificateur de descripteur (*descriptorID*) attribué à cet utilisateur au moment où il s'est fait enregistrer, toutes les identités d'utilisateur enregistrées sous forme de structures déterminées et le paramètre *updateType* (type de mise à jour), positionné sur *deleted* (supprimé);

B: l'entité fonctionnelle VLF ou l'élément frontière doit supprimer l'information de position (c'est-à-dire l'adresse TSAP du portier et toutes les identités d'utilisateur enregistrées) indiquée par le descripteur (*descriptor*), remplacer le champ *sender* (expéditeur) du message **DescriptorUpdate** par sa propre adresse TSAP et envoyer le message **DescriptorUpdate** au portier indiqué par l'adresse TSAP du portier qui était enregistrée sous la forme de l'information de position relative à l'utilisateur. L'entité fonctionnelle VLF ou l'élément frontière doit en outre répondre à l'entité fonctionnelle HLF ou à l'élément frontière en lui envoyant un message **DescriptorUpdateAck**;

C: le portier doit supprimer la ou les adresses pseudonymes enregistrées pour l'utilisateur indiqué par le descripteur (*descriptor*) et envoyer un message URQ au terminal mobile H.323. Le message URQ doit comporter toutes les identités enregistrées de l'utilisateur dont l'enregistrement va être annulé. Le portier doit en outre répondre à l'entité fonctionnelle VLF ou à l'élément frontière en lui envoyant un message **DescriptorUpdateAck**;

D: Le terminal mobile H.323 doit envoyer au portier un message UCF lui confirmant l'annulation de l'enregistrement.

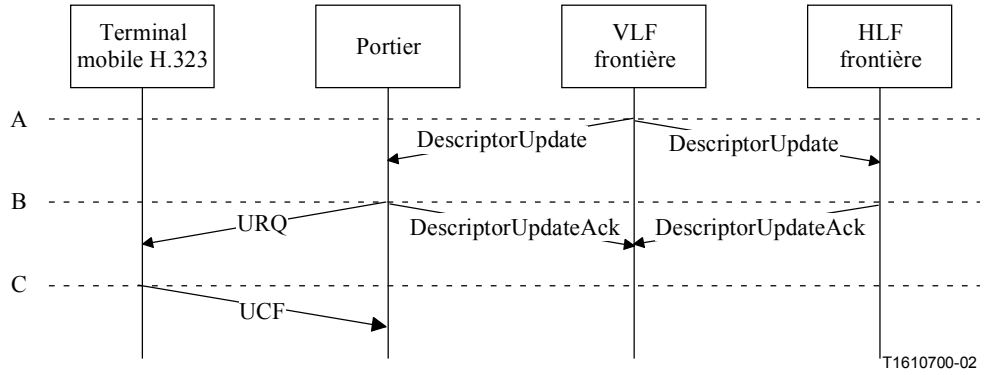


Figure 8/H.510 – Annulation d'enregistrement à l'initiative de l'entité fonctionnelle VLF

La Figure 8 illustre le lancement de la procédure d'annulation d'enregistrement par l'entité fonctionnelle VLF ou l'élément frontière. Cette procédure est décrite de manière plus détaillée ci-dessous:

A: l'entité fonctionnelle VLF ou l'élément frontière supprime de ses données enregistrées l'information de position (c'est-à-dire l'adresse TSAP du portier et toutes les identités d'utilisateur enregistrées) relative à l'utilisateur et envoie un message **DescriptorUpdate** à l'entité fonctionnelle HLF ou à l'élément frontière associé à l'utilisateur ainsi qu'au portier auprès duquel l'utilisateur est présentement enregistré. Le message doit comporter l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière dans le champ *sender*

(expéditeur), l'identité de descripteur (*descriptorID*) attribuée à cet utilisateur au moment où il s'est fait enregistrer, toutes les identités d'utilisateur enregistrées sous la forme de structures déterminées et le paramètre *updateType* (type de mise à jour), positionné sur *deleted* (supprimé);

B: l'entité fonctionnelle HLF ou l'élément frontière doit supprimer l'information de position (c'est-à-dire l'adresse TSAP de l'entité fonctionnelle VLF ou de l'élément frontière) relative à l'utilisateur indiqué par le descripteur (*descriptor*) et répondre à l'entité fonctionnelle VLF ou à l'élément frontière en lui envoyant un message **DescriptorUpdateAck**.

Le portier doit supprimer la ou les adresses pseudonymes enregistrées pour l'utilisateur indiqué par le descripteur (*descriptor*) et envoyer un message URQ au terminal mobile H.323. Le message URQ doit comporter toutes les identités enregistrées de l'utilisateur dont l'enregistrement va être annulé. Le portier doit en outre répondre à l'entité fonctionnelle VLF ou à l'élément frontière en lui envoyant un message **DescriptorUpdateAck**;

C: le terminal mobile H.323 doit envoyer au portier un message UCF lui confirmant l'annulation de l'enregistrement.

La liste suivante récapitule les contenus de message utilisés dans la présente Recommandation pour les procédures d'annulation d'enregistrement (pour les messages ou les champs de message qui ne sont pas indiqués ici, il convient d'utiliser les messages ou champs de message indiqués dans les Recs. UIT-T H.323, H.225.0 ou H.501):

DescriptorUpdate

Champ	Description
sender	Adresse TSAP de l'expéditeur du message.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	identificateur attribué au moment de l'enregistrement
templates	
pattern	une pour chaque identité d'utilisateur enregistrée
specific	identité de l'utilisateur
routeInfo	
nonExistent	
gatekeeperID	Eventuellement l'identificateur (ID) du portier qui a envoyé le message.
updateType	
deleted	

7.5 Procédures de gestion de la mobilité pour l'établissement de l'appel

7.5.1 Principes généraux

Le présent paragraphe décrit les flux d'information intervenant dans les procédures de gestion de la mobilité mises en œuvre pendant la phase d'établissement de l'appel. L'établissement de l'appel doit être effectué selon les procédures H.323 normales, c'est-à-dire suivant la signalisation RAS ou de commande d'appel H.225.0 et conformément à la Rec. UIT-T H.501. Les conditions supplémentaires à observer sont indiquées ci-dessous.

On distingue deux cas: les appels aboutissant à un terminal mobile H.323 (gestion des appels entrants), et les appels provenant d'un terminal mobile H.323 (gestion des appels sortants). Un appel en provenance d'un terminal mobile H.323 à destination d'un autre terminal mobile H.323 réunit les deux cas précédents.

Aux fins de la gestion des appels entrants, la principale condition requise en termes de mobilité est la capacité à déterminer la position du terminal ou de l'utilisateur mobile au moment considéré. Ce point est examiné au § 7.5.2 ci-dessous.

Aux fins de la gestion des appels sortants, la mobilité peut être assurée par les procédures H.323 normales. Les conditions supplémentaires expressément requises pour assurer la mobilité appellent un complément d'étude.

7.5.2 Procédures de gestion de la mobilité pour l'établissement des appels entrants

Etant donné que, dans le cas d'appels intrazone, le portier connaît la position (le point NPoA) du terminal ou de l'utilisateur mobile H.323 appelé, ainsi que les adresses pseudonymes (*aliasAddresses*) associées à l'utilisateur appelé (indiquées au moment où l'utilisateur mobile s'est fait enregistrer auprès du portier), aucune condition particulière supplémentaire n'est nécessaire pour assurer la mobilité par rapport au cas de terminaux H.323 non mobiles.

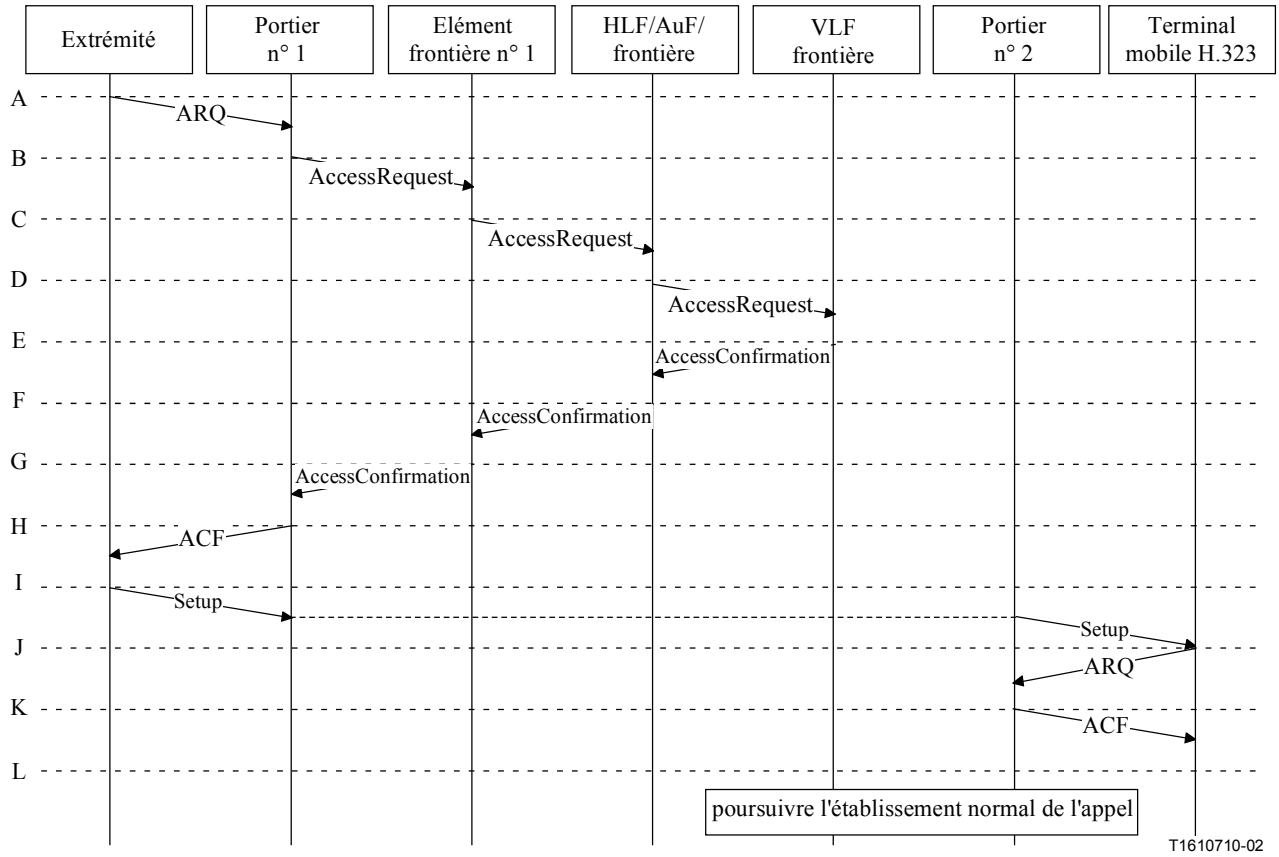


Figure 9/H.510 – Etablissement d'un appel à destination d'un terminal mobile

La Figure 9 représente le flux d'information permettant d'établir un appel avec succès à destination d'un terminal mobile H.323. La procédure d'établissement d'appel est décrite de manière plus détaillée ci-dessous:

A: l'extrémité appelante envoie un message ARQ à son portier (portier n° 1). Le champ *destinationInfo* (information de destination) contient au moins une adresse pseudonyme (*aliasAddress*) (identité d'utilisateur appelable) d'un utilisateur mobile. Le portier n° 1 tente de déchiffrer la ou les adresses pseudonymes.

Si l'utilisateur appelé est lui aussi enregistré auprès du portier n° 1 (c'est-à-dire dans le cas d'un déplacement intrazone), les étapes B à G suivantes sont sautées et le portier renvoie immédiatement un message ACF (étape H).

B: si l'utilisateur appelé n'est pas enregistré auprès du même portier, le portier auprès duquel l'extrémité appelante est enregistrée (portier n° 1) envoie un message **AccessRequest** (*demande d'accès*) à l'élément frontière n° 1 qui lui est associé (le portier n° 1 peut aussi envoyer un message LRQ, ce qui ne modifie pas sensiblement les procédures, si ce n'est que le message **AccessConfirmation** (*confirmation d'accès*) dans l'étape G est remplacé par le message LCF). Le message **AccessRequest** doit comporter une ou plusieurs identités appelables de l'utilisateur appelé sous forme d'adresses pseudonymes (*aliasAddresses*) dans le champ *destinationInfo* (information de destination). Ces adresses pseudonymes proviennent du message ARQ reçu par le portier en provenance de l'extrémité appelante.

Les étapes C à F suivantes peuvent être sautées si l'utilisateur appelé est, au moment considéré, enregistré auprès d'un portier associé à l'élément frontière n° 1 (c'est-à-dire que l'élément frontière n° 1 est également l'entité fonctionnelle VLF ou l'élément frontière de l'utilisateur appelé);

C: l'élément frontière n° 1 détermine l'adresse de l'entité fonctionnelle HLF ou de l'élément frontière de l'utilisateur appelé d'après la ou les adresses pseudonymes (*aliasAddress(es)*) et envoie le message **AccessRequest** à l'entité fonctionnelle HLF ou à l'élément frontière;

D: connaissant l'entité fonctionnelle VLF ou l'élément frontière qui détient l'information de position relative à l'utilisateur indiqué par les identités d'utilisateur reçues, l'entité fonctionnelle HLF ou l'élément frontière lui envoie un message **AccessRequest**. Ce message doit comporter une ou plusieurs identités d'utilisateur (principale ou appelable) choisies par l'entité fonctionnelle HLF ou par l'élément frontière sous forme d'éléments *aliasAddress* (adresse pseudonyme) dans le champ *destinationInfo* (information de destination).

L'entité fonctionnelle HLF ou l'élément frontière peut également renvoyer à l'élément frontière n° 1 un message **AccessConfirmation** (*confirmation d'accès*), comportant un modèle (*template*) contenant une ou plusieurs identités d'utilisateur appropriées sous forme d'une ou de plusieurs adresses pseudonymes déterminées et un champ *routeInfo* (information de routage) indiquant *sendAccessRequest* (émission de demande d'accès) dans le type de message (*messageType*) et l'adresse de transport (*transportAddress*) de l'entité fonctionnelle VLF ou de l'élément frontière dans le champ *contacts* (contacts). L'élément frontière n° 1 peut alors envoyer un autre message **AccessRequest** à l'entité fonctionnelle VLF ou à l'élément frontière pour obtenir la position de l'utilisateur appelé. Cette variante aboutit au même résultat (sauf que l'étape F n'est pas applicable);

E: l'entité fonctionnelle VLF ou l'élément frontière vérifie son information de position relative à l'utilisateur indiqué par les identités d'utilisateur reçues et renvoie un message **AccessConfirmation** à l'entité fonctionnelle HLF ou à l'élément frontière (ou à l'élément frontière n° 1 si la procédure de remplacement de l'étape D est applicable). Le message doit comporter un modèle (*template*) contenant une identité d'utilisateur appropriée sous la forme de l'adresse pseudonyme (*aliasAddress*) considérée et un champ *routeInfo* (information de routage) indiquant *sendSetup* (émission d'établissement) dans le type de message (*messageType*) et l'adresse de transport (*transportAddress*) de signalisation d'appel du portier auprès duquel l'utilisateur est enregistré (portier n° 2) ou du terminal mobile H.323 dans le champ *contacts* (contacts). Le choix de l'identité de l'utilisateur et de l'adresse de transport dépend de la politique locale dans le domaine visité;

F: l'entité fonctionnelle HLF peut modifier le message **AccessConfirmation** selon les besoins (en ajoutant ou remplaçant des identités d'utilisateur, par exemple) et renvoyer le message à l'élément frontière n° 1;

G: l'élément frontière n° 1 réachemine le message **AccessConfirmation**, éventuellement modifié, à destination du portier n° 1;

H: le portier n° 1 envoie un message ACF à l'extrémité appelante, en fonction de l'information reçue dans le message **AccessConfirmation**. Il s'agit là de la procédure H.323 normale;

I: l'information reçue dans le message ACF détermine les procédures de signalisation d'appel suivantes, conformes à la Rec. UIT-T H.323: un message **Setup** (*établissement*) est envoyé en utilisant la signalisation d'appel directe ou la signalisation avec routage par portier via le portier n° 1 ou le portier n° 2. C'est ce qu'indique la ligne pointillée reliant les deux flèches "Setup" de chaque côté de la Figure 9;

J, K, L: la procédure normale d'établissement de l'appel se poursuit conformément à la Rec. UIT-T H.323.

Si l'élément frontière n° 1 n'est pas en mesure de déterminer l'adresse de l'entité fonctionnelle HLF d'après les identités d'utilisateur appelables figurant dans le message **AccessRequest** envoyé par un portier (comme dans l'étape B ci-dessus), ou si l'entité fonctionnelle VLF ou l'élément frontière n'a aucune information de position correspondant aux identités d'utilisateur reçues dans le message **AccessRequest** envoyé par une entité fonctionnelle HLF ou un élément frontière (comme dans l'étape D ci-dessus), l'élément frontière n° 1 ou l'entité fonctionnelle VLF ou l'élément frontière doit répondre en envoyant un message **AccessRejection** (*refus d'accès*) indiquant pour motif (*reason*) "pas de correspondance" (*noMatch*). De même, si elle/il ne dispose d'aucune information relative à l'utilisateur indiqué par le message **AccessRequest** qu'elle/il a reçu en provenance d'un élément frontière (comme dans l'étape C ci-dessus), l'entité fonctionnelle HLF ou l'élément frontière doit répondre par un message **AccessRejection** (*refus d'accès*) indiquant pour motif (*reason*) "pas de correspondance" (*noMatch*). A la réception du message **AccessRejection** en provenance de l'entité fonctionnelle VLF ou de l'élément frontière, l'entité fonctionnelle HLF ou l'élément frontière doit envoyer le message **AccessRejection** à l'élément frontière n° 1. A la réception d'un message **AccessRejection** en provenance d'une entité fonctionnelle HLF ou d'un élément frontière, un élément frontière doit envoyer le message au portier qui a envoyé le message **AccessRequest** (portier n° 1) et ce portier doit envoyer à l'extrémité appelante un message ARJ indiquant pour motif (*reason*) "correspondant appelé pas enregistré" (*calledPartyNotRegistered*).

La liste suivante récapitule les contenus de message utilisés dans la présente Recommandation (pour les messages ou les champs de message qui ne sont pas indiqués ici, il convient d'utiliser les messages ou champs de message indiqués dans les Recs. UIT-T H.323, H.225.0 ou H.501):

ARQ (extrémité appelante)

Champ	Description
destinationInfo	Une ou plusieurs identités d'utilisateur appelables.

ARJ

Champ	Description
reason	
calledPartyNotRegistered	Si l'utilisateur appelé ne peut pas être localisé.

AccessRequest

Champ	Description
destinationInfo	
logicalAddresses	Pour les interrogations adressées par le portier à l'élément frontière ou par l'élément frontière à l'entité fonctionnelle HLF, une ou plusieurs identités d'utilisateur appelables. Pour les interrogations adressées à l'entité fonctionnelle VLF ou à l'élément frontière par l'entité fonctionnelle HLF ou l'élément frontière, l'identité principale de l'utilisateur peut également être jointe à titre facultatif.

AccessConfirmation

Champ			Description
templates			
	pattern		
		specific	Une ou plusieurs identités d'utilisateur appelables et/ou l'identité principale de l'utilisateur, si besoin est.
routeInfo			
	messageType		
		sendSetup	Indique que l'extrémité ou le portier d'origine peut envoyer le message Setup (établissement) à l'adresse indiquée dans l'adresse de transport (transportAddress) dans le champ contacts.
	contacts		
		transportAddress	Adresse TSAP de signalisation d'appel de l'utilisateur appelé ou de son portier.

AccessRejection

Champ			Description
reason			
	noMatch		Situation dans laquelle l'entité fonctionnelle qui reçoit le message AccessRequest (*demande d'accès*) ne dispose d'aucune information relative à l'utilisateur indiqué par les identités d'utilisateur dans ledit message, et n'a pas connaissance d'autres entités fonctionnelles susceptibles d'être en mesure de déterminer la position de l'utilisateur.

7.5.3 Procédures de gestion de la mobilité pour l'établissement des appels sortants

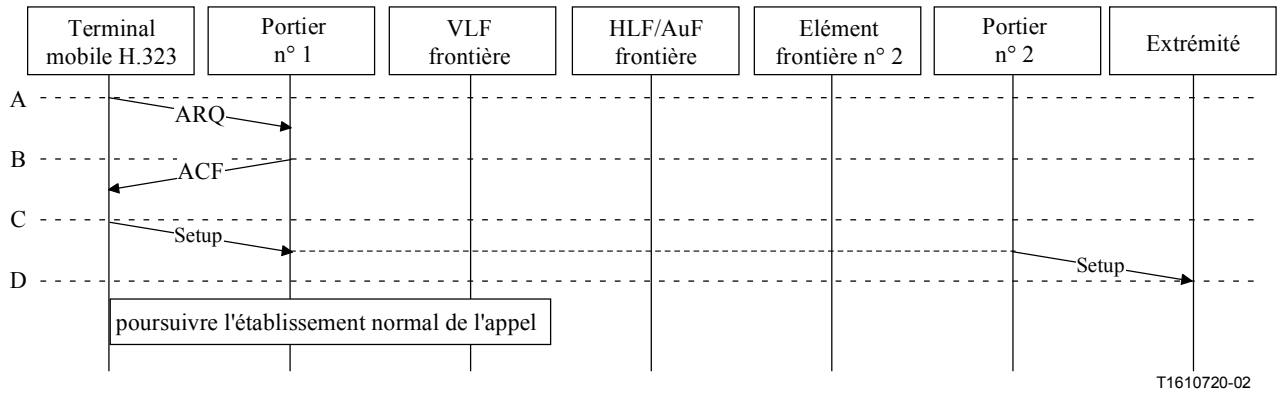


Figure 10/H.510 – Etablissement d'un appel en provenance d'un terminal mobile

La Figure 10 montre le flux d'information qui permettra d'établir avec succès des appels sortants lorsque les procédures de gestion de la mobilité entreront en vigueur. La procédure est décrite de manière plus détaillée ci-dessous:

A: le terminal mobile H.323 appelant envoie un message ARQ à son portier (portier n° 1) conformément aux procédures H.323 normales;

B: le portier renvoie un message ACF indiquant la position de l'utilisateur appelé, conformément aux procédures H.323 normales.

NOTE – Si l'utilisateur appelé est aussi un utilisateur mobile, les procédures décrites au § 7.5.2 sont également applicables;

C: les informations reçues dans le message ACF déterminent le choix de la procédure de signalisation d'appel H.323 à utiliser pour l'envoi d'un message Setup (*établissement*), c'est-à-dire la procédure de signalisation d'appel directe ou la procédure de signalisation indirecte par l'intermédiaire du portier n° 1 et/ou du portier n° 2. C'est ce qu'indique la ligne pointillée reliant les flèches "Setup" de chaque côté;

D: l'établissement normal de l'appel se poursuit conformément à la Rec. UIT-T H.323.

7.5.4 Sécurité

Les procédures de sécurité pour la Rec. UIT-T H.510 sont spécifiées dans la Rec. UIT-T H.530. Ces procédures permettent à un domaine de desserte d'authentifier un utilisateur/terminal mobile lorsqu'il tente de localiser un portier ou de se faire enregistrer. Le processus d'authentification permet à l'utilisateur ou au terminal visiteur d'authentifier également le domaine de desserte. Toutes les procédures de sécurité supplémentaires sont exécutées au niveau local entre le terminal H.323 et le portier.

7.6 Transfert

Si le terminal mobile se déplace au cours d'un appel, des mécanismes situés dans les couches protocolaires inférieures assurent parfois la fonctionnalité de transfert nécessaire de manière transparente, c'est-à-dire sans faire intervenir les couches protocolaires H.323, de telle sorte que le point NPoA du terminal ne change pas.

Les transferts avec changement de point NPoA, c'est-à-dire qui nécessitent également l'intervention des couches protocolaires H.323, appellent un complément d'étude.

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

Imprimé en Suisse
Genève, 2002