INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.510

(03/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Mobility and Collaboration procedures – Mobility for H-Series multimedia systems and services

Mobility for H.323 multimedia systems and services

ITU-T Recommendation H.510

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
SYSTEMS AND TERMINAL EQUIPMENT FOR AUDIOVISUAL SERVICES	H.300–H.399
SUPPLEMENTARY SERVICES FOR MULTIMEDIA	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	**H.510–H.519**
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation H.510

Mobility for H.323 multimedia systems and services

Summary

The purpose of this Recommendation is to define services and procedures for the support of mobility in H.323 multimedia systems.

Source

ITU-T Recommendation H.510 was prepared by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 March 2002.

Keywords

H.323, multimedia systems, terminal mobility, user mobility.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation H.510

Mobility for H.323 multimedia systems and services

1 Scope

This Recommendation deals with mobility aspects for H.323 systems above the transport layer. H.510 applies new functions defined in support of mobility management to H.323-compliant systems.

The main focus is on the support of terminal mobility, although support of user mobility in the context of H.323 is covered as well. This version of this Recommendation does not cover handover procedures where active calls can be maintained during location changes.

Interworking with other networks to support mobility across networks of different types is outside the scope of this Recommendation.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation H.323 (2000), *Packet-based multimedia communications systems*.

[2] ITU-T Recommendation H.225.0 (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[3] ITU-T Recommendation H.225.0 Annex G (1999), *Communication between administrative domains*.

[4] ITU-T Recommendation H.501 (2002), *Protocol for mobility management and intra/inter-domain communication in multimedia systems*.

[5] ITU-T Recommendation H.530 (2002), *Symmetric security procedures for H.510 (Mobility for H.323 multimedia systems and services)*.

2.2 Informative references

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

3 Definitions

For the purposes of this Recommendation, the definitions given in ITU-T Rec. H.323 shall apply, with the following additions.

3.1 administrative domain: Defined as in H.225.0 Annex G. An administrative domain consists of one or more zones.

3.2 callable user identity: A user identity that can be used by a calling user to make a call to the user identified by this user identity. It may be announced e.g. in a phonebook as the identity by which a user can be reached.

3.3 H.323 point of attachment: A network point of attachment that allows the H.323 terminal to register with a gatekeeper or to directly communicate with another H.323 terminal.

3.4 home domain: The administrative domain that is related by subscription to the mobile user. The home domain contains user-specific data including location, authentication, and service profile information related to the mobile user.

3.5 home gatekeeper (Home GK): A gatekeeper in the home domain of a user.

3.6 home service provider: The service provider or administrator in charge of the home domain of a user; i.e. the user is related to the home service provider by a subscription contract.

3.7 location: The network point of attachment through which the user/terminal is currently accessing the H.323 system.

3.8 H.323 mobile terminal: A terminal that may change H.323 point of attachment.

3.9 mobility management: The set of functions needed to provide user, terminal and service mobility.

3.10 network point of attachment: The network interface that is used by an endpoint in order to access the H.323 system. Each network point of attachment is associated with a network address (e.g. IP address) by which packets sent to the endpoint reach the endpoint.

3.11 online: State of a mobile user or terminal that has "logged on", i.e. is currently registered at a gatekeeper, as opposed to **absent** or "logged off".

3.12 primary user identity: The user identity allocated permanently to a user at subscription time, which stays the same as long as the subscription exists. There is only one primary user identity for a user.

3.13 service mobility: The ability of a user to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose.

3.14 serving domain: The (visited or home) administrative domain that is serving an online mobile user/terminal.

3.15 serving gatekeeper: The (visited or home) gatekeeper where an online mobile user/terminal is currently registered.

3.16 temporary user identity: A user identity allocated to a user on a temporary basis which is intended to be used in place of the primary user identity, for example because of security reasons.

3.17 terminal identity: A code or string uniquely identifying a terminal.

NOTE – One possible use is to authenticate the terminal during the user registration. The terminal authentication permits to verify whether or not the user is allowed to use the terminal (for instance if the H.323 mobile terminal is "black-listed" by the home service provider – e.g. after having been stolen – the mobile user cannot register in the H.323 network with this terminal).

3.18 terminal mobility: The ability of a terminal to change location (i.e. network point of attachment and H.323 point of attachment) and still be able to communicate.

3.19 discrete terminal mobility (**terminal roaming**): The ability of a terminal to make discrete changes of location, i.e. to change location while no media streams are active.

3.20 continuous terminal mobility (**handover**): The ability of a terminal to change location while media streams are active. Handover is further called *seamless* when the terminal location change does not result in delay or loss of data that would be perceived by the user as degradation of quality of service (note that seamless handovers may depend on many factors, including service type and service presentation robustness against data loss at the terminal).

3.21 user: A person or other entity authorized to use H.323 communication services.

3.22 user identity: A code or string uniquely identifying a user across a multi-user, multi-service infrastructure.

3.23 user mobility (personal mobility): The ability of a user to maintain the same user identity irrespective of the terminal used and its network point of attachment. Terminals used may be of different types.

3.24 discrete user mobility (**user roaming**): The ability of a user to change location or terminals while no media streams are active.

3.25 continuous user mobility (**session mobility**): The ability of a user to change location or terminals while media streams are active.

NOTE – A similar feature is provided in the SCN by the supplementary service Terminal Portability.

3.26 user service profile: User-specific information indicating which services a user is subscribed to and personal configuration data for the respective services.

3.27 visited domain: The administrative domain that is not the home domain and is serving a mobile user.

3.28 visited gatekeeper (Visited GK): A gatekeeper in a visited domain.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

A	Address (as a DNS record/query type)
AuF	Authentication Function
BE	Border Element
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
e164	Address type "phone number" (according to ITU-T Rec. E.164)
EP	Endpoint
GK	Gatekeeper
HLF	Home Location Function
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
MT	Mobile Terminal
NAI	Network Access Identifier
NPoA	Network Point of Attachment
RAS	Registration, Admission and Status protocol (ITU-T Rec. H.225.0)

The following RAS messages are used in this Recommendation:

ACF	AdmissionConfirm
ARJ	AdmissionReject
ARQ	AdmissionRequest
GCF	GatekeeperConfirm
GRJ	GatekeeperReject

GRQ GatekeeperRequest

LCF LocationConfirm

LRQ LocationRequest

RCF RegistrationConfirm

RIP RequestInProgress

RRJ RegistrationReject

RRQ RegistrationRequest

SLA Service Level Agreement

SRV Service (as a DNS record/query type)

TSAP Transport Service Access Point

TXT Text (as a DNS record/query type)

UCF UnregistrationConfirm

UIM User Identification Module

URL Universal Resource Locator

URQ UnregistrationRequest

VLF Visitor Location Function

5 H.323 mobility service description

The following clauses define the services the H.323 system provides for terminal and user mobility. These are overall service descriptions from a user's point of view without dealing with the user interface aspects themselves.

5.1 General description

5.1.1 H.323 user mobility

This Recommendation deals with the support of mobile users that belong to an H.323 network.

NOTE – General user mobility is described in other Recommendations.

In a network supporting user mobility there exists a dynamic association between mobile users and terminals. Any mobile user can register at any terminal with access to the network, within the limits of applicable permissions. Registration enables the mobile user to obtain the services permitted by the applicable user service profile and supported at the currently used terminal. A change of location results in a new registration of the mobile user and the corresponding de-registration from the previous location (if there was one).

A mobile user belongs permanently to exactly one administrative domain, the home domain of that user. User mobility may be restricted to the home domain, or may be permitted across multiple administrative domains subject to service agreements between those domains and the user's home domain.

The applicable user service profile for a mobile user depends on the current location and on the service agreements mentioned above. After having registered properly, a mobile user shall be able to initiate and/or receive calls at the current location. However, restrictions may apply regarding permitted use of resources, available quality of service, etc.

With regard to ITU-T Rec. H.323, two distinct aspects have to be considered for inter-domain mobility:

a) A mobile user registers at an H.323 terminal. The user is treated like a native H.323 user irrespective of whether his home domain is an H.323 system or not. In the latter case, the home domain will redirect calls destined for the mobile user to an H.323 ingress gateway.

b) A mobile user whose home domain is an H.323 system roams into another network. In this case the H.323 home domain will redirect calls destined for the mobile user to an H.323 egress gateway.

5.1.2 H.323 terminal mobility

Terminal mobility means that an H.323 terminal can change its location, i.e. its network point of attachment, and maintain the ability to communicate. In this Recommendation, terminal mobility is formulated in terms of mobility of the user currently associated with the terminal. Only where considerations apply specifically to terminals rather than users, terminal mobility is treated separately.

It is possible to have no user registered on a specific terminal. Which services are possible on a terminal without a registered user is implementation dependent. In order to provision services on a terminal where no mobile user is registered, such a terminal may be associated with a "default" user registered "by administration". In this way, there is no need to care about terminals directly; they can be treated in terms of their default user.

5.1.3 Service mobility

In the context of this Recommendation, service mobility is limited to applying the mobile user's service profile when making or receiving calls.

NOTE – Further service mobility aspects will be described in other Recommendations.

5.2 H.323 requirements

5.2.1 Requirements for H.323 user mobility

H.323 user mobility implies the following services:

1) **Identification and authentication of mobile user**: Enables a serving domain to validate the user identity of the mobile user.

2) **Authentication of the serving domain**: Enables a mobile user to verify the authenticity of the serving domain, so as to ascertain that the domain is indeed the one of which services are expected.

3) **Mobile user registration/de-registration**: Enables a mobile user to associate with any wired or wireless H.323 terminal in order to make or receive calls. This can be done on a permanent (without ever de-registering) or temporary basis (with de-registration at the end of a period of registration).

   NOTE – Permanent registration could be activated "by administration" without any actual user involvement. This may have many useful applications, such as service provisioning on public terminals, or the administration of a "default" terminal at a user's personal desk.

4) **Mobile user call handling**: Enables a mobile user to make and/or receive calls, typically after registration, on the basis of the user identity at any suitable H.323 terminal. This ability should only be limited by terminal and network capabilities and possibly the restrictions imposed by the service level agreements (SLAs) between service providers of the involved administrative domains. This service consists of two parts (which may be supported independently of each other), incoming call handling and outgoing call handling:

- *Mobile user incoming call handling* directs incoming calls for a mobile user to the H.323 terminal he has registered at, regardless of the location of the terminal and regardless of the serving domain the mobile user has registered with.
- *Mobile user outgoing call handling* detects an outgoing call from a mobile user and establishes it applying the user service profile, regardless of the user's location within the H.323 network. The user identity must be presented to any destination party as the normal identification of the call originator, regardless of the location of the terminal and regardless of the serving domain with which the mobile user has registered.

5.2.2 Requirements for H.323 terminal mobility

H.323 terminal mobility implies the following services:

1) **Authentication of an H.323 mobile terminal**: Enables the verification of the authenticity of an H.323 mobile terminal in the context of the *association* it has with a mobile user (previously set up through registration). Authentication of the terminal is used to verify that the terminal can indeed act on behalf of the user that has currently registered at it.

   NOTE – Which particular terminal is used is, by itself, only useful information for secondary purposes, such as comparison against a blacklist of stolen terminals, or for locating a terminal rather than a user.

2) **Authentication of the serving domain**: Enables an H.323 mobile terminal to verify the authenticity of the serving domain (on roaming into it) on behalf of the mobile user that has registered at the terminal.

3) **H.323 mobile terminal registration/de-registration**: Enables an H.323 mobile terminal to renew registration of the mobile user currently associated with it when changing location and to cancel registration, e.g. when it is turned off.

4) **Transfer of user service profiles**: Allows for (part of) the user service profile to be transferred to the serving domain (i.e. to the responsible gatekeeper or possibly the terminal itself).

5) **H.323 mobile terminal call handling**: Is fully covered by mobile user call handling as it is assumed that a user needs to be associated with the terminal for call handling purposes (may be a default user).

6) **H.323 mobile terminal handover**: Enables an H.323 mobile terminal to maintain a call while moving between locations. This feature is for further study.

5.2.3 Mobility identification requirements

5.2.3.1 Mobile user identification

A user may have multiple different user identities intended for different purposes. At least three distinct uses for a user identity can be found:

– The most obvious one is the use by a calling user to call the called user. An e164 number is an example of this kind of identity, here called **callable user identity**.

– Another purpose of a user identity is to identify a user permanently towards the home service provider for the whole duration of the user's subscription. This identity, here called the **primary user identity**, is the key identity against which all other user identities are mapped. This kind of identifier makes it possible for a user to have several callable user identities, or to change callable user identities while maintaining the same primary user identity (and thus the same subscription) with the home service provider.

– A third use in some systems, where it may be desirable to transmit the primary user identity as infrequently as possible, is to identify a user locally by allocating a non-permanent user identity for a certain amount of time or while the user is located in a certain part of the

network. This kind of user identity is called **temporary user identity** and is used in place of the primary user identity, typically because of security reasons.

It is possible that one user identity functions both as a callable user identity and the primary user identity, but it should be possible to use different user identities for these purposes. If one user identity is used as both the primary user identity and a callable user identity, there should be no need to use a temporary user identity for the user.

The following requirements shall be fulfilled for the purposes of this Recommendation:

- The user (rather than the terminal) is identified through an AliasAddress according to ITU-T Rec. H.225.0. The user can have multiple unique alias addresses such as an email address of type email-ID, a URL of type URL-ID, a phone number of type e164, a UIM (User Identification Module) including e.g. an IMSI (International Mobile Subscriber Identity) and so on.
- All user identity types – callable user identity, primary user identity and temporary user identity – shall be AliasAddresses.
- The user identities shall be unique within the portion of an H.323 system where they can be used. This means the primary user identity and any globally usable callable user identities shall be globally unique. However, there may be locally-used callable user identities, such as short numbers. Temporary user identities may also have only local significance.

5.2.3.2 Mobile terminal identification

Even though for call routing and mobility management purposes the identity of the terminal used by a mobile user is not relevant, in some cases there may be a need to also identify the terminal, for example to forbid the usage of stolen or unlicensed terminals.

The following requirements shall be fulfilled for the purposes of this Recommendation:

- The terminal (hardware and/or software) may have a signature, e.g. of type h323-ID, that is generated by the terminal vendor at manufacturing time. The signature shall be unique and never change during the entire lifetime of the terminal.
- Terminals are identified for routing purposes by their network layer address and occasionally their data link address.

5.2.3.3 Administrative domain identification

Identification of the administrative domain serves at least two purposes. First, it is necessary to identify the home administrative domain of a user for the purpose of updating the location information of the user and for obtaining the current location when the user is being called. Secondly, the user might prefer certain administrative domains to others, e.g. because of cheaper service or service agreements between the home service provider and other service providers.

The home administrative domain is either identified by an explicit administrative domain identifier, or its identity is deduced from the user identity (e.g. in case of hierarchical e164 numbers or email-ID type AliasAddresses).

The following requirements shall be fulfilled for the purposes of this Recommendation:

- Each administrative domain shall be identifiable by an administrative domain identity.
- It shall be possible to deduce the identity of the home domain from all globally used user identities of the user. Locally used user identities need not contain the information about the home domain.

5.2.3.4 Zone identification

Identification of the zone (i.e. the gatekeeper) may be needed if the user prefers certain zones (of the same administrative domain) to others. In this case the identity of the zone and the gatekeeper needs to be known before the user (and the terminal) registers to the zone.

The following requirements shall be fulfilled for the purposes of this Recommendation.

- It shall be possible to configure one or more zones and gatekeepers as the home zones and home GKs of a user. The information about the home zone and home GK should be included in the user service profile of the user.
- The H.323 mobile terminal shall be able to identify the gatekeeper responding to it during the gatekeeper discovery procedure and make decisions about the zone to which it wants to register based on that information and the user service profile.

5.3 Procedures required for mobility management

The following procedures must be supported for H.323 mobility.

- Gatekeeper discovery mechanisms to identify and choose the desired administrative domain or preferred zone.
- Location update when the mobile terminal/user registers or de-registers or changes the network point of attachment.

  NOTE – The term "de-registration" is used for the user-level procedure of terminating the online state. The H.510 protocol procedures below use the term "unregistration" instead, in alignment with H.323/H.225.0 terminology.
- Mutual authentication of the terminal/user and the network.
- User service profile sharing between home domain and (visited) GK as needed.
- Authorization of service requests (e.g. for an outgoing call) against the user service profile.
- Locating the mobile terminal/user for incoming calls.

5.4 Procedures required for provisioning and configuring H.323 mobile entities

These are outside the scope of this Recommendation.

6 Architecture for H.323 mobility

6.1 Architectural model

Figure 1 presents the functional architecture and reference points for mobility management in H.323 systems, based on the H.225.0 Annex G functional architecture. Additional functional entities (VLF, HLF, AuF) are either combined with existing H.323 elements – gatekeepers, border elements – or represent external elements with regard to existing H.323. In the latter case, shown in Figure 1, they can be considered as back-end services, in which case the links between them and existing H.323 entities represent instances of the D reference point. Bold lines indicate the links that are in the scope of this Recommendation.

Reference points between elements in the back-end-services cloud, which are not part of the existing H.323 architecture, are outside the scope of this Recommendation. This is indicated by showing these links as broken lines.

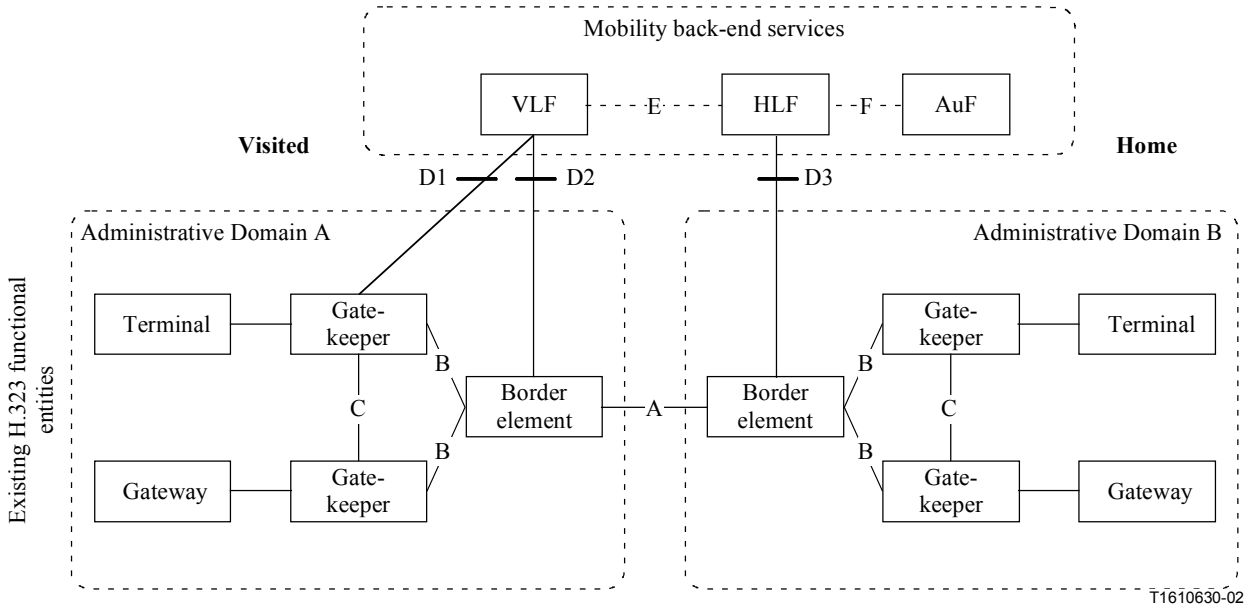


Figure 1/H.510 – Functional architecture diagram with reference points

6.2 Functional entities

6.2.1 Mobility specific entities

HLF, VLF and AuF are defined in other Recommendations. For the purposes of this Recommendation, they can be described as follows:

- The HLF represents the home database that stores the permanent (subscription) data of a mobile user/terminal as well as the current location (by pointing to a VLF), if the user/terminal is online. This functional entity is always associated with the home domain.
- The VLF represents a database for temporary storage of data relating to a visiting user/terminal, including a pointer to the gatekeeper where the user/terminal is currently registered and a pointer to HLF. This functional entity is associated with the serving domain (home or visited).
- The AuF is responsible for authentication of a mobile user/terminal towards the serving domain (home or visited). It is always associated with the mobile user's/terminal's HLF, and thus with the home domain.

A VLF can be associated with one gatekeeper or multiple gatekeepers as long as all the gatekeepers belong to the same administrative domain, i.e. the upper limit of the service area of a VLF is the administrative domain. The same applies to HLF/AuF, although there may well be fewer HLFs/AuFs than VLFs.

6.2.2 H.323 mobile terminal

In addition to standard H.323 terminal functionality, an H.323 mobile terminal supports:

– the association with any authorized mobile user;

– the adoption of a mobile user's service profile;

– the dynamic change of network and/or H.323 point of attachment.

NOTE – "Dynamic" in this context means that the H.323 system automatically handles location updates, without requiring administrative intervention. It does not mean that existing calls are maintained over location changes (i.e. handover is not supported by this version of this Recommendation).

6.2.3 Gatekeeper and border element

An H.323 mobile terminal is controlled by a home GK while roaming in the home domain, otherwise by a visited GK. In the latter case communication may further involve border elements in both administrative domains, home and visited.

The GK also contains the information needed to handle the calls initiated or received by the H.323 MTs registered to it (e.g. supplementary service information received from the HLF, though for some supplementary services the GK may have to obtain additional information from the HLF).

Gatekeepers and border elements must support communication with the functional entities listed in 6.2.1 unless these functions are integrated with the gatekeeper or border element. For more detail, see 6.3.

6.3 Reference points

The reference points A-D are the same as in H.225.0 Annex G.

This Recommendation deals with the following logical signalling relationships:

1) Between GK and BE over reference point B.
2) Between GK and VLF over reference point D1.
3) Between VLF and HLF over reference point E (outside the scope of this Recommendation).
4) Between HLF and AuF over reference point F (outside the scope of this Recommendation).
5) Between VLF and BE over reference point D2, and between HLF and BE over reference point D3.
6) Between two BEs over reference point A.

The signalling protocols for mobility management over the existing interfaces in ITU-T Rec. H.323 are the protocols defined in ITU-T Recs H.225.0 (RAS, Q.931), H.245 and H.501.

Since the functional entities HLF, VLF and AuF can coexist in a single network element with a gatekeeper or a border element, the reference points may be internal to these network elements. Figure 2 illustrates an example of this situation with two composite network elements: one BE located with the gatekeeper and the VLF (denoted as gatekeeper/VLF/BE) and the HLF as well as the AuF with another border element (denoted as border element/HLF/AuF).

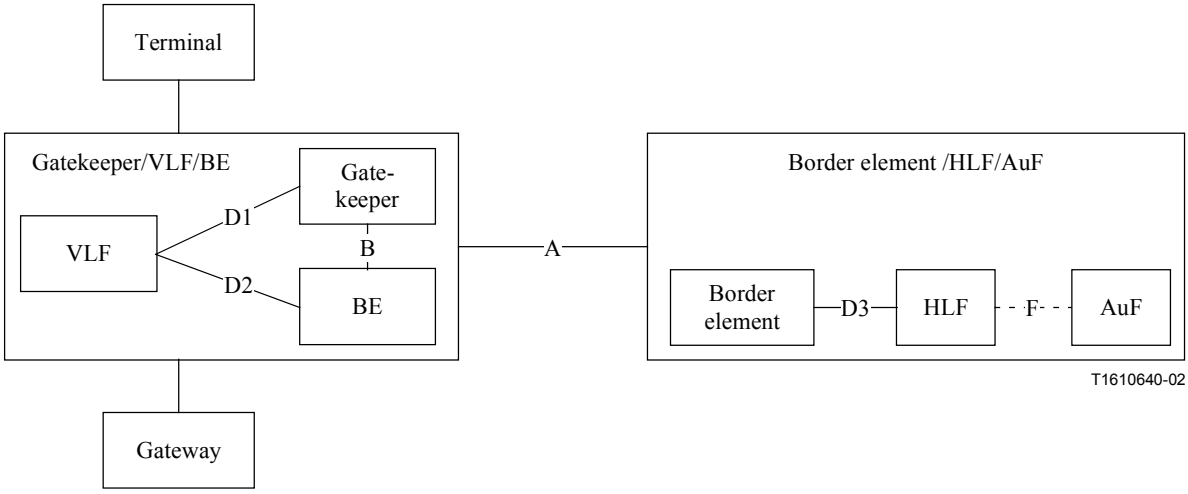


Figure 2/H.510 – An example of composite network elements

7 Mobility management procedures

7.1 General on mobility management procedures

This clause describes the procedures to provide the mobility management functions in H.323 systems. The procedures are presented in the form of information flow diagrams (or message sequence charts) with additional explanations to the diagrams.

Mobility management procedures comprise three main parts:

- **HLF address space announcement procedures**: The procedures that need to be performed before the users associated with an HLF can be contacted. These procedures are performed between HLFs and BEs/GKs in order to announce the user identities for which the location of users with these identities can be determined by contacting the HLF.
- **Location updating procedures**: The procedures that need to be performed when a mobile user, using an H.323 terminal, changes the H.323 point of attachment (the zone) or the network point of attachment (network address), or when the user accesses the system for the first time after a period of absence (i.e. when there is no current location information about the user stored in the associated HLF). These procedures include the gatekeeper discovery, registration and unregistration procedures.

  NOTE – How the terminal discovers that it has changed the network point of attachment is an implementation matter outside the scope of this Recommendation. For instance, the IP stack in the terminal informs the terminal application about the change of the IP address.
- **Call related mobility management procedures**: The procedures that need to be performed when a call to or from a mobile user, using an H.323 terminal, is being established. These mobility management procedures include the information exchange needed to locate the user that is being called.

The call related mobility management procedures do not provide for continuous terminal mobility, i.e. handovers. Handover procedures are not part of version 1 of this Recommendation.

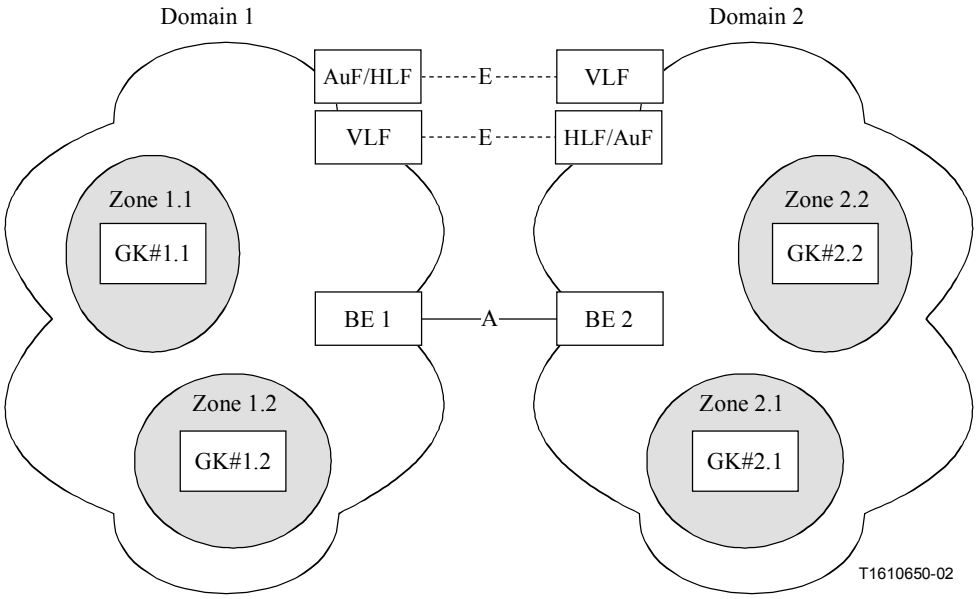
7.2 Example scenarios for mobility management procedures

In order to illustrate the various possibilities of location changes, Figure 3 shows an example of two domains, each consisting of two zones.

The following location change scenarios can be distinguished:

1) Intra-zone within home domain, e.g. a user/terminal belonging to Domain 1 changes from its current location within zone 1.1 to another location within the same zone.
2) Intra-zone within visited domain, e.g. a user/terminal belonging to Domain 1 changes from its current location within zone 2.1 to another location within the same zone.
3) Inter-zone within home domain, e.g. a user/terminal belonging to Domain 1 changes from its current location within zone 1.1 to another location within zone 1.2.
4) Intra-zone within visited domain, e.g. a user/terminal belonging to Domain 1 changes from its current location within zone 2.1 to another location within zone 2.2.
5) Inter-domain, e.g. a user/terminal belonging to Domain 1 changes from its current location within zone 1.1 to another location within zone 2.2.

The procedures in the following clauses are described for the most general scenario 5). The other scenarios can be derived from 5) by omitting certain steps in the procedure.



NOTE – For simplicity no links are shown inside the domains; see Figure 1 for those links.

Figure 3/H.510 – Model for scenarios

7.3 HLF Address space announcement procedures

7.3.1 Static arrangement

In a static arrangement, the GKs and BEs are configured with the addresses of the HLFs that they will contact for resolving callable or primary user identities. The range of possible user identities and the associated HLFs are known to the GK or BE by means of configuration or administration. The appropriate HLF is selected based on the content of the present user identity.

The procedures to configure or update the GKs and BEs in a static arrangement are outside the scope of this Recommendation.

7.3.2 Dynamic arrangement

In a dynamic arrangement, the GKs and BEs obtain the knowledge about user identities and associated HLFs dynamically by means of a protocol. The HLFs shall use the procedures and messages described in ITU-T Rec. H.501 to advertise the user identities in their database, i.e. their address space, to the GKs and BEs.

The GKs and BEs shall send **DescriptorIDRequest** and **DescriptorRequest** messages to the HLFs to gain information about the address space of the HLFs and the HLFs shall respond to these queries with **DescriptorIDConfirmation** and **DescriptorConfirmation** messages, respectively, in order to announce their address spaces. The HLFs should also send **DescriptorUpdate** messages to the GKs/BEs when there is a change in their address space. The GKs/BEs and HLFs may establish a service relationship using **ServiceRequest** and **ServiceConfirmation** messages as described in ITU-T Rec. H.501, prior to any other communication with each other.

Based on the information gained with these message exchanges, GKs and BEs are able to deduce from the user identities of the mobile users the correct HLF to contact for each mobile user.

7.3.3 Address patterns

According to ITU-T Rec. H.501, the descriptors can contain alias addresses in the formats email and party number (by default in the form of an international e164 number). Upon arrangement between involved domains other formats of alias addresses may be supported, e.g. party numbers

from a private numbering plan. Formats of mobile user identities (like IMSI) will in any case require such an arrangement.

The GKs, BEs and HLFs conforming to this Recommendation shall support user identities in the form of alias addresses, as specified in ITU-T Rec. H.225.0 (ASN.1 type *AliasAddress*), of the following formats:

– **Callable user identities**: An email address (type *AliasAddress.email-ID*) or an (international) e164 number (type *AliasAddress.partyNumber.e164Number*), or optionally a (fully qualified) private party number (type *AliasAddress.partyNumber.privateNumber*).

– **Primary user identities**: One of the callable user identities, or a Network Access Identifier (NAI, see RFC 2486), or a global mobile user identity (type *AliasAddress.mobileUIM*), containing e.g. an IMSI. The NAI is of type *AliasAddress.email-ID* even if it does not represent a callable email address.

Other formats and identifiers are for further study.

The procedures do not distinguish between callable and primary user identities. Such procedures are for further study.

7.4 Location update procedures

Location update procedures are performed:

– when an H.323 MT (re-)starts operation;

– when an H.323 MT moves into a new location;

– when a mobile user logs onto a particular H.323 MT.

The location update procedures make use of H.225.0 RAS procedures: gatekeeper discovery, registration and unregistration.

7.4.1 Gatekeeper discovery

7.4.1.1 General considerations

From the point of view of the H.323 system, the gatekeeper discovery procedure is the first procedure that the H.323 mobile terminal performs when a location update is needed. The only exception is an intra-zone location update, where the gatekeeper discovery can be skipped since the H.323 MT stays registered with the same gatekeeper as before.

An H.323 mobile terminal must initiate the gatekeeper discovery procedure when one or more of the following events or situations occur:

- The H.323 mobile terminal has acquired access to the underlying network through a new network point of attachment. For example, the terminal has obtained an IP address from a DHCP server. This situation includes the H.323 mobile terminal start-up as well as the case that the H.323 mobile terminal changes its NPoA during operation.
- The H.323 mobile terminal has lost the connection with the gatekeeper to which it was previously registered. The loss may have occurred gracefully, with the gatekeeper sending a URQ message to the H.323 mobile terminal, or it may have occurred ungracefully, e.g. because of link failure on the communication path between the H.323 mobile terminal and the gatekeeper.
- A registration request failed with reason *discoveryRequired*.

There are several methods by which the gatekeeper discovery procedure can be executed, depending on the capabilities of the underlying network (for example, whether or not the network supports multicasting) and on the part of the H.323 system being accessed. The following list contains the methods that may be used by H.323 mobile terminals. An H.323 mobile terminal may

implement some or all of these methods, with the order of preference configured in the H.323 mobile terminal.

1) Multicast GRQ message.
2) Unicast GRQ message to a gatekeeper, the address of which has previously been cached or otherwise stored.
3) SRV query on the gk_domain (IV.1.1/H.225.0).
4) TXT record query on the gk_domain (IV.1.1/H.225.0).
5) "A" record query on the gk_domain.
6) Manual discovery (7.2.1/H.323).

Methods 3 through 5 make use of the Domain Name System (DNS). Manual discovery is outside the scope of this Recommendation.

7.4.1.2 Discovering a serving gatekeeper

The serving gatekeeper will be a home gatekeeper while an H.323 mobile terminal roams within its home domain, otherwise a visited gatekeeper. Any of the methods listed in 7.4.1.1 will return the address(es) of one or more gatekeepers, if successful.

If the gatekeeper address was found using one of methods 3 through 5, the H.323 mobile terminal shall send a (unicast) GRQ message to that gatekeeper. If the gatekeeper address was found using method 1 or 2, the H.323 MT shall attempt to register with one of the gatekeepers, as described in 7.4.2.

If a gatekeeper receives a (unicast) GRQ message, the gatekeeper shall do one of the following things:

1) Send a GCF if it will become the serving gatekeeper and allow the terminal to register.
2) Send a GRJ with or without a list of alternate gatekeepers.

Based on the response from the gatekeeper, the terminal shall do one of three things:

1) If the gatekeeper responded with a GCF, then the H.323 mobile terminal shall attempt to register with that gatekeeper as described in 7.4.2.
2) If the gatekeeper responded with a GRJ and a list of alternate gatekeepers, then the H.323 mobile terminal shall walk down the list starting with GRQ to the gatekeeper with the highest priority.
3) If the gatekeeper responded with a GRJ without a list of alternate gatekeepers, then the H.323 mobile terminal should use the alternate gatekeeper list that it may have previously received. If the H.323 mobile terminal does not have a list of alternate gatekeepers, then it cannot discover a gatekeeper for registration.

7.4.2 Registration

An H.323 mobile terminal shall perform the registration procedure if one of the following events has occurred. The terminal must already have the information about the gatekeeper to which it is going to send the registration (RRQ).

- The terminal (re-)appears in a zone (e.g. after power-up). In this case gatekeeper discovery must be performed before starting to register. See 7.4.1.
- A new user starts to use the terminal. If the terminal is already registered, gatekeeper discovery is not required. If a previous user is still registered and the terminal accepts the new user, the new registration replaces the previous one, resulting in unregistration of the previous user by the gatekeeper (see 7.4.3).

- The terminal has moved to another NPoA than the one at which it was previously registered. Gatekeeper discovery (see 7.4.1) will be required prior to registration unless it is known that the new NPoA also belongs to the zone of the previous gatekeeper (intra-zone location change).
- Whenever a mobile terminal moves to a new zone while not involved in a call (even if the NPoA does not change).
- When the previous registration has been lost (e.g. because of registration timeout). This may be detected for instance by the gatekeeper having replied to an ARQ with an ARJ indicating that the MT is not registered. If an alternate gatekeeper is known (e.g. from the ARJ message), registration may be attempted to this gatekeeper, otherwise gatekeeper discovery must be performed first (see 7.4.1).
- As a keep-alive indication (lightweight registration, see ITU-T Rec. H.225.0), to extend the lifetime of the current registration.

7.4.3 Unregistration

The intention of the unregistration procedure is to remove the registration of a user or an H.323 MT to a gatekeeper. If the terminal also has its own aliasAddress, e.g. a terminal ID, its registration is also removed in the unregistration of a user. If an H.323 MT is unregistered, the user currently using this terminal is also unregistered. An H.323 mobile terminal should perform unregistration if one or more of the following events or situations occur:

- The H.323 mobile terminal application is being shut down.
- A user using the terminal wishes to unregister from the H.323 system.
- The H.323 mobile terminal is going to remove its connection through the current NPoA to the gatekeeper to which it is registered, but it will not immediately connect to some gatekeeper through another NPoA.

  If the H.323 mobile terminal changes its location in such a way that it will connect to the H.323 system through a new NPoA immediately after disconnecting from the old NPoA, unregistration by the H.323 MT is not necessary as it will be implicitly done through the location update procedure.
- The gatekeeper, the VLF or the HLF request the unregistration of a user or the H.323 MT, e.g. if the registration lifetime expires.

7.4.4 Information flows for the location updating procedures

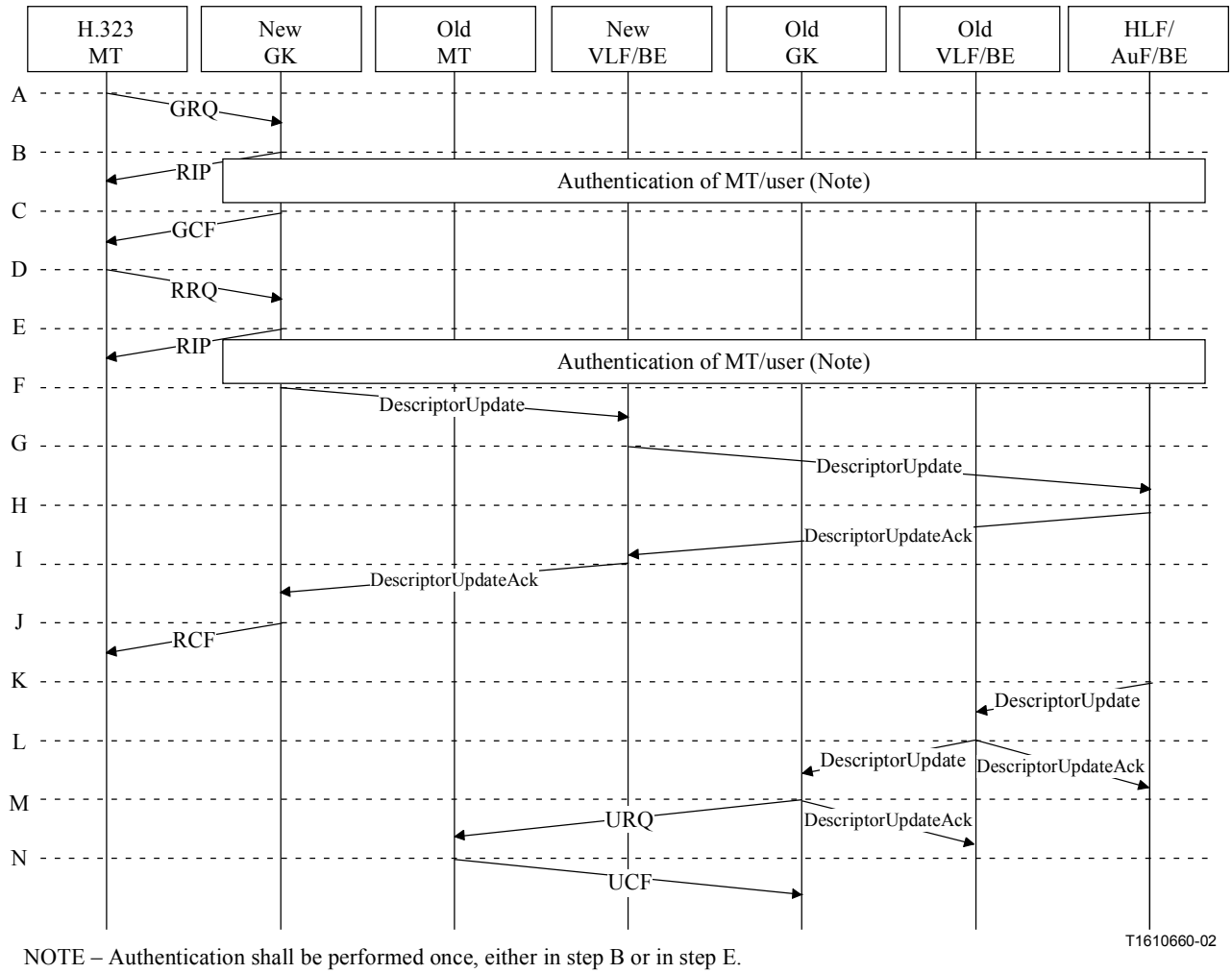
Figure 4 depicts the complete information flow for the location updating procedure. The complete flow applies when the H.323 mobile terminal changes its location from one visited domain to another. In this case, the old gatekeeper and old VLF hold location information about the user using that terminal.

In the following cases only parts of the complete flow apply, as indicated in the detailed description below Figure 4:

– The H.323 MT changes location (i.e. the NPoA) within the same zone (gatekeeper discovery is not necessary, and the information in the VLF and/or HLF does not change).

– The H.323 MT changes the zone within the same visited domain (old and new VLF are the same, the information in the HLF does not change).

– The H.323 MT (or a mobile user) registers for the first time after having been unregistered previously (no previous location information in the old VLF and/or GK needs to be removed).



NOTE – Authentication shall be performed once, either in step B or in step E.

Figure 4/H.510 – Information flow for location updating procedure

The meaning of the steps indicated in Figure 4 is as follows:

Steps A-C are not needed when changing location (the NPoA) within the same zone, or in the case of keep-alive registration.

A: Conditions for initiating the location updating procedures with gatekeeper discovery were met and thus the H.323 MT sends a GRQ message to the gatekeeper. The GRQ message shall include in the *endpointAlias* field all the user identities (including the primary user identity) that can be used to identify the user.

B: Authentication will usually be done only once during location update, i.e. either step B or step E will apply. If the gatekeeper authenticates the user at this point, it shall perform the authentication as specified in ITU-T Rec. H.530. An RIP message may be returned to the H.323 MT as an indication of a possible delay in responding to GRQ.

If the gatekeeper does not accept this user's request, it shall send a GRJ to the H.323 MT.

C: The gatekeeper returns GCF to the H.323 MT to indicate that it will accept registration. If step B was performed, the GCF message will contain authentication information to be used by the MT for the following RRQ.

D: The H.323 MT sends a registration request (RRQ) to the (already known) gatekeeper. Unless this is a keep-alive registration, the RRQ message shall include in the *terminalAlias* field all user identities (including the primary user identity) that can be used to identify the user and were indicated by the user.

E: Authentication will usually be done only once during location update, i.e. either step B or step E will apply. If the gatekeeper authenticates the user at this point, it shall perform the authentication as specified in ITU-T Rec. H.530. An RIP message may be returned to the H.323 MT as an indication of a possible delay in responding to RRQ.

If the gatekeeper does not accept this user's request, it shall send an RRJ to the H.323 MT.

F: If the H.323 MT and the user using it are already registered, the gatekeeper updates the registration and continues with step J. This is the case if the H.323 MT changes the NPoA within the zone or if the previous registration is renewed (e.g. as a periodic keep-alive mechanism).

If the gatekeeper notices that the user is not already registered it sends a **DescriptorUpdate** message to the VLF/BE that it is associated with (after successful authentication).

The **DescriptorUpdate** message shall include the TSAP address of the gatekeeper as an *aliasAddress* in the *sender* field of the message and the *updateInfo* field containing a descriptor with a new *descriptorID* in the *descriptorInfo* field and the *updateType* set to *added*. In the *templates* field, each *descriptor* shall include as specific patterns all user identities (including the primary user identity) that are to be registered, as well as *sendSetup* as the *messageType* of the *routeInfo* field. The descriptor may also include the *gatekeeperID* of the GK that sent the **DescriptorUpdate** message. The gatekeeper also stores the address of the NPoA through which the H.323 MT connects to the gatekeeper.

G: On receipt of the **DescriptorUpdate** message, the VLF/BE shall check each *descriptor* against those already stored from previous location updates. If the user was already registered in the VLF/BE, the VLF/BE shall act as described in step I below. In this case old and new VLF/BE are the same. The VLF/BE shall further send a **DescriptorUpdate** message to the old gatekeeper, as described in step L below.

The VLF/BE shall change the *messageType* field to *sendAccessRequest* and the *sender* field to the TSAP address of the VLF/BE itself. If the *gatekeeperID* was present in the *descriptor* sent by the GK, the VLF/BE may remove it from the message, before sending it forward. Finally, the VLF/BE deduces the TSAP address of the user's HLF/BE from the primary user identity contained in the *descriptor*, and sends the **DescriptorUpdate** message to the HLF/BE.

H: The HLF/BE stores the TSAP address of the VLF/BE as the location information about the user indicated by the primary user identity in the **DescriptorUpdate** message and sends a **DescriptorUpdateAck** message as a response to the VLF/BE.

I: The VLF/BE stores all the user identities it received, the TSAP address of the user's HLF/BE, and the TSAP address of the gatekeeper that it has received in step G as the location information about that user, and sends a **DescriptorUpdateAck** message to the gatekeeper.

J: The gatekeeper stores the NPoA as well as all the user identities that it received from the H.323 mobile terminal in the RRQ message in step D. The gatekeeper shall send an RCF message to the H.323 MT indicating a successful location updating.

The Steps K through M are executed only if previous location information about the user was present in the HLF/BE and the (previous) GK and VLF/BE (if any) before step G was performed.

K: The HLF/BE can execute this step immediately after step H, in order to assure a timely update of the location information throughout the network. The HLF/BE shall send a **DescriptorUpdate** message to the old VLF/BE. The message shall include the TSAP address of the HLF/BE itself in the *sender* field and *updateInfo* containing a *descriptor* with the *descriptorID* of the original registration and all registered user identities of the user as specific patterns, *nonExistent* as the *messageType* of the *routeInfo* field and the *updateType* set to *deleted*.

L: The VLF/BE shall remove the previous location information indicated by the *descriptor* (i.e. the TSAP address of the old gatekeeper and all stored user identities) and send a **DescriptorUpdate** message, as described in step K above, to the old gatekeeper (with the *sender* field set to the TSAP address of the VLF/BE itself). The VLF/BE shall also respond to the HLF/BE with a **DescriptorUpdateAck** message.

M: The old gatekeeper shall remove the location information (i.e. the NPoA) as well as other registration information that it has been holding about the user indicated by the *descriptorID* or the *descriptor*, and respond to the VLF/BE with a **DescriptorUpdateAck** message. It should also send a URQ message to the previous H.323 MT.

N: The previous H.323 MT responds to the URQ with UCF and removes its registration data, if any.

The following list contains a summary of the message contents relevant to this Recommendation (for those messages or message fields that are not indicated here, the message or message field should be used as indicated in ITU-T Recs H.323, H.225.0 or H.501):

GRQ

Field	Description
endpointAlias	All available user identities of the user to be registered (may be the default user)

RRQ

Field	Description
terminalAlias	All available user identities of the user to be registered

DescriptorUpdate

Field	Description
sender	The TSAP address of the entity sending the message.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	new identifier assigned to this registration (if updateType = added) identifier assigned at registration time (if updateType = deleted)
templates	
pattern	one for each available user identity
specific	the user identity to be registered
routeInfo	
sendSetup	if sent from GK to VLF/BE
sendAccessRequest	if sent from VLF/BE to HLF/BE
nonExistent	if sent from HLF/BE to VLF/BE/from VLF/BE to GK
gatekeeperID	Optionally the ID of the GK that sent the message
updateType	
added	in direction GK→VLF/BE, VLF/BE→HLF/BE
deleted	in direction HLF/BE→VLF/BE, VLF/BE→GK

7.4.5 Unregistration

An H.323 MT or a mobile user is unregistered following an explicit request from the user, or on request of the GK, VLF or HLF. Unregistration results in the removal of location information from the HLF, VLF and GK. In irregular situations, e.g. loss of connection or registration timeout, the GK, VLF or HLF may also remove location information without a full unregistration procedure.

Figures 5 through 8 illustrate the unregistration procedure for the three cases mentioned above.

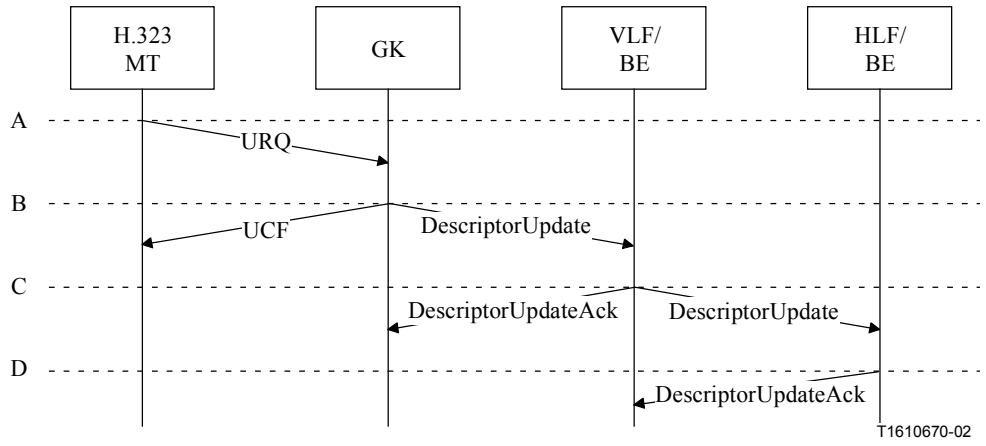


Figure 5/H.510 – Unregistration initiated by the H.323 mobile terminal

Figure 5 illustrates the unregistration procedure initiated by the H.323 mobile terminal. A more detailed description of the procedure follows:

A: The H.323 MT sends a URQ message to the gatekeeper to which it is registered. If the unregistration is for the user only, the URQ message shall include all identities registered for that user in the *endpointAlias* field. If the H.323 MT is also to be unregistered, no alias address should be included.

B: The gatekeeper shall process the URQ message in the usual way, i.e. remove those alias address(es) that were listed in URQ, and send a **DescriptorUpdate** message to the VLF/BE that it is associated with. The message shall include the TSAP address of the gatekeeper in the *sender* field, the *descriptorID* previously assigned when that user registered, all the user identities as specific patterns and the *updateType* set to *deleted*. If the H.323 MT unregisters itself (i.e. not only its current user), the gatekeeper shall also delete the location information (i.e. the NPoA) used by that terminal. The gatekeeper shall send a UCF message to the H.323 MT confirming the unregistration.

C: The VLF/BE shall remove the location information (i.e. the TSAP address of the gatekeeper and all registered user identities) indicated by the *descriptor*, change the *sender* field of the **DescriptorUpdate** message to the TSAP address of the VLF/BE and forward the **DescriptorUpdate** message to the HLF/BE of the user. The VLF/BE shall also respond to the gatekeeper with a **DescriptorUpdateAck** message.

D: The HLF/BE shall remove the location information (i.e. the TSAP address of the VLF/BE) it has stored about the user indicated by the *descriptor*. The HLF/BE shall also respond to the VLF/BE with a **DescriptorUpdateAck** message.

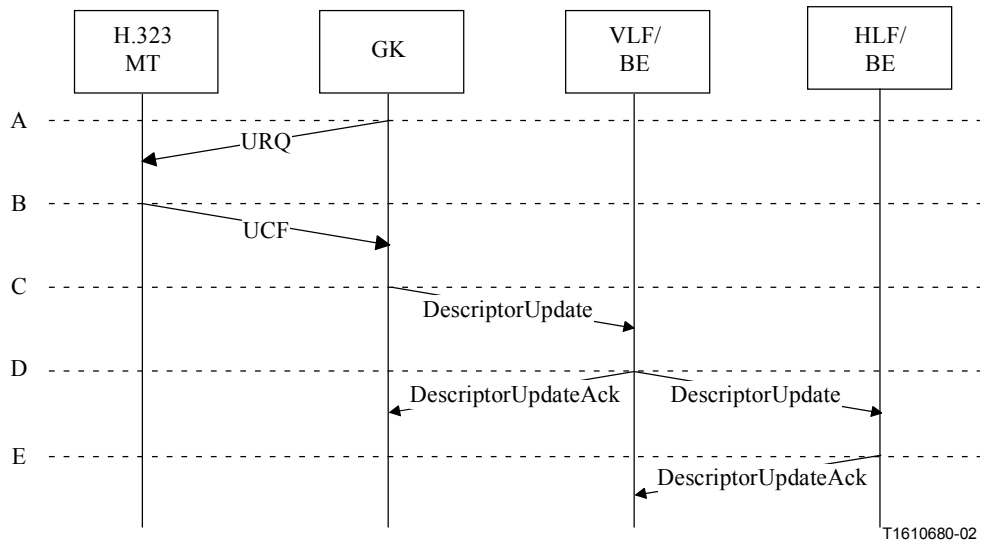


Figure 6/H.510 – Unregistration initiated by the gatekeeper

Figure 6 illustrates the unregistration procedure initiated by the gatekeeper. A more detailed description of the procedure follows:

A: The gatekeeper sends a URQ message to the H.323 MT from which a user is to be unregistered. The message shall include all the registered user identities in the *endpointAlias* field if only the user is being unregistered. If the H.323 MT is to be unregistered as well, no alias address should be included.

B: The H.323 MT sends a UCF message to the gatekeeper confirming the unregistration. The gatekeeper removes the registration information about the user, and if the H.323 MT itself is unregistered, also the NPoA.

Steps C, D, and E are the same as B, C, and D in the previous case, respectively.

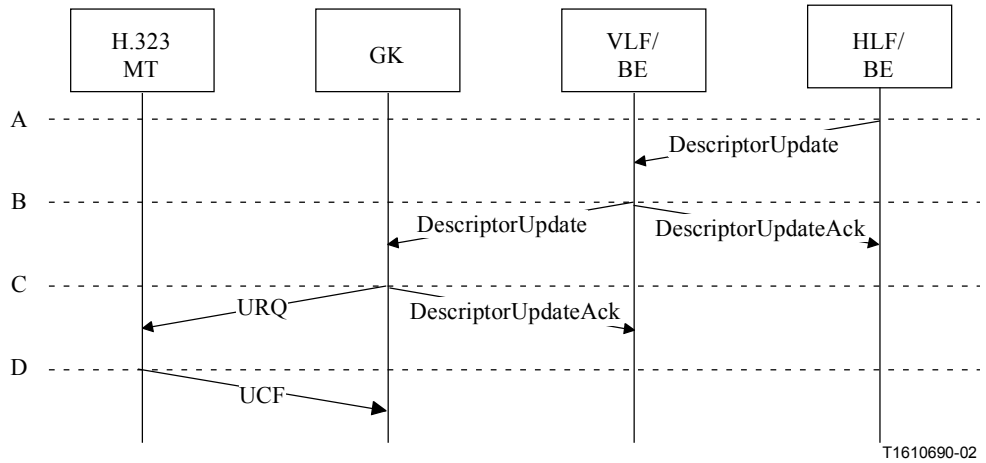


Figure 7/H.510 – Unregistration initiated by the HLF

Figure 7 illustrates the unregistration procedure initiated by the HLF. A more detailed description of the procedure follows:

A: The HLF/BE removes the location information (i.e. the TSAP address of the VLF/BE) it has stored about the user and sends a **DescriptorUpdate** message to the VLF/BE currently holding the location information about the user. The message shall include the TSAP address of the HLF/BE in the *sender* field, the *descriptorID* assigned to that user when it

registered, all registered user identities as specific patterns, and the *updateType* set to *deleted*.

B: The VLF/BE shall remove the location information (i.e. the TSAP address of the gatekeeper and all registered user identities) indicated by the *descriptor*, change the *sender* field of the **DescriptorUpdate** message to the TSAP address of the VLF/BE itself and forward the **DescriptorUpdate** message to the gatekeeper indicated by the TSAP address of the gatekeeper that was stored as the location information about the user. The VLF/BE shall also respond to the HLF/BE with a **DescriptorUpdateAck** message.

C: The gatekeeper shall remove the alias address(es) stored for the user indicated by the *descriptor* and send a URQ message to the H.323 MT. The URQ message shall include all the registered user identities of the user being unregistered. The gatekeeper shall also respond to the VLF/BE with a **DescriptorUpdateAck** message.

D: The H.323 MT shall send a UCF message to the gatekeeper confirming the unregistration.

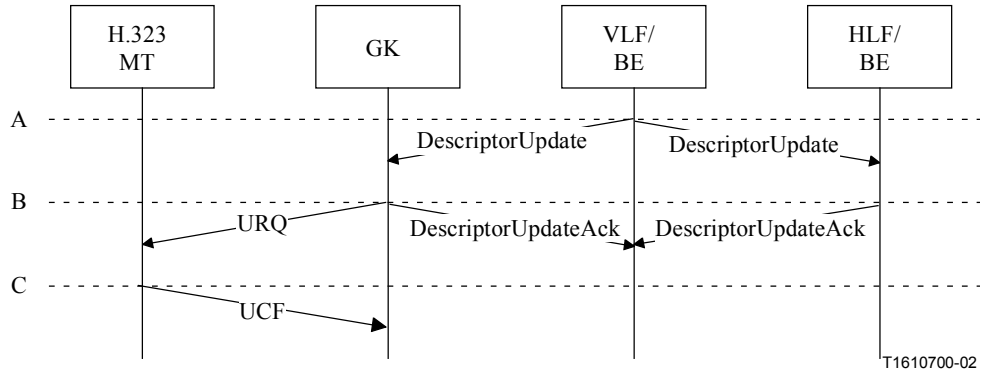


Figure 8/H.510 – Unregistration initiated by the VLF

Figure 8 illustrates the unregistration procedure initiated by the VLF/BE. A more detailed description of the procedure follows:

A: The VLF/BE removes the location information (i.e. the TSAP address of the gatekeeper and all registered user identities) it has stored about the user, and sends a **DescriptorUpdate** message to the HLF/BE associated with the user and to the gatekeeper where the user is currently registered. The message shall include the TSAP address of the VLF/BE in the *sender* field, the *descriptorID* assigned to that user when it registered, all registered user identities as specific patterns and the *updateType* set to *deleted*.

B: The HLF/BE shall remove the location information (i.e. the TSAP address of the VLF/BE) about the user indicated by the *descriptor* and respond to the VLF/BE with a **DescriptorUpdateAck** message.

The gatekeeper shall remove the alias address(es) stored for the user indicated by the *descriptor* and send a URQ message to the H.323 MT. The URQ message shall include all registered user identities of the user being unregistered. The gatekeeper shall also respond to the VLF/BE with a **DescriptorUpdateAck** message.

C: The H.323 MT shall send a UCF message to the gatekeeper confirming the unregistration.

The following list contains a summary of the message contents relevant to this Recommendation used in the unregistration procedures (for those messages or message fields that are not indicated here, the message or message field should be used as indicated in ITU-T Recs H.323, H.225.0 or H.501):

DescriptorUpdate

Field	Description
sender	The TSAP address of the sender of the message.
updateInfo	
descriptorInfo	
descriptor	
descriptorInfo	
descriptorID	identifier assigned at registration time
templates	
pattern	one for each registered user identity
specific	user identity
routeInfo	
nonExistent	
gatekeeperID	Optionally the ID of the GK that sent the message.
updateType	
deleted	

7.5 Call establishment mobility management procedures

7.5.1 General principles

This clause describes the information flows for mobility management procedures involved in the call establishment phase. Call establishment shall follow the normal H.323 procedures, i.e. H.225.0 RAS and call control signalling, and H.501. Additional requirements are indicated below.

Two cases are distinguished: Calls terminating at an H.323 MT (incoming call handling), and calls originated by an H.323 MT (outgoing call handling). A call from an H.323 MT to another H.323 MT is a combination of both cases.

For incoming call handling, the main mobility specific requirement is the ability to find the current location of the mobile terminal/user. This is described in 7.5.2 below.

For outgoing call handling, mobility can be supported by normal H.323 procedures. Any additional mobility specific requirements are for further study.

7.5.2 Call establishment mobility management procedures for incoming calls

Since in intra-zone calls the gatekeeper knows the location (the NPoA) of the called H.323 MT/mobile user as well as any *aliasAddresses* associated with the called user (indicated when the mobile user registered to the gatekeeper), there are no additional mobility specific requirements present compared to the non-mobile case in H.323.

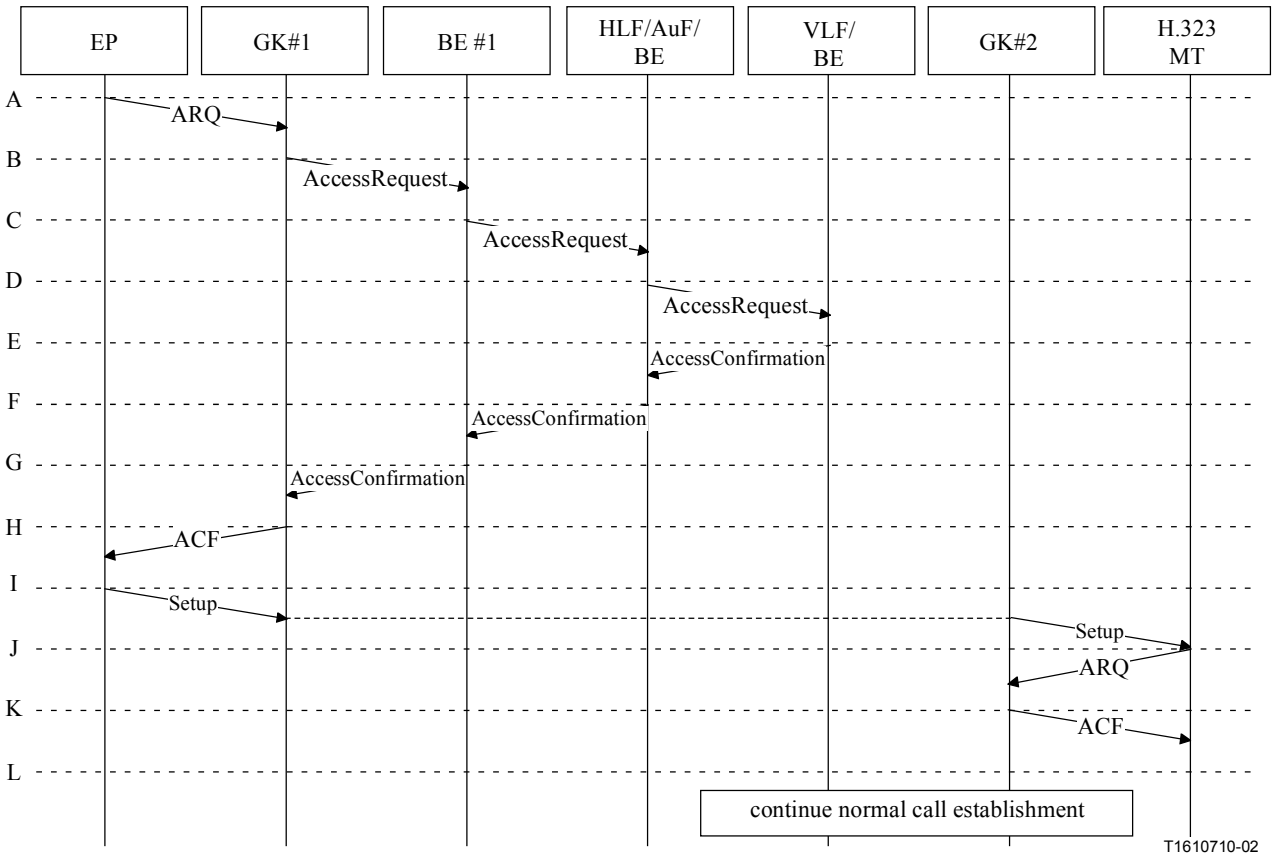


Figure 9/H.510 – Call establishment to a mobile terminal

Figure 9 depicts the information flow for a successful call establishment to an H.323 MT. A more detailed description of the procedure follows.

A: The calling endpoint sends an ARQ to its gatekeeper (GK#1). The *destinationInfo* field contains at least one *aliasAddress* (callable user identity) of a mobile user. The gatekeeper GK#1 attempts to resolve the aliasAddress(es).

If the called user is also registered to GK#1 (i.e. for the intra-zone case), the following steps B-G are skipped, and the gatekeeper immediately returns ACF (step H).

B: If the called user is not registered to the same gatekeeper, the gatekeeper to which the calling endpoint is registered (GK#1) sends an **AccessRequest** message to the border element (BE#1) with which it is associated (alternatively GK#1 may send LRQ, this does not alter the procedures substantially, except that the **AccessConfirmation** in step G is replaced by LCF). The **AccessRequest** message shall include one or more callable user identities of the called user as *aliasAddresses* in the *destinationInfo* field. These *aliasAddresses* are obtained from the ARQ message received by the gatekeeper from the calling EP.

The following steps C-F can be skipped if the called user is currently registered to a gatekeeper associated with BE#1 (i.e. BE#1 is also the called user's current VLF/BE).

C: BE#1 deduces the address of the called user's HLF/BE from the *aliasAddress(es)* and forwards the **AccessRequest** message to the HLF/BE.

D: The HLF/BE knows the VLF/BE holding the location information about the user indicated by the received user identities, and sends an **AccessRequest** message to this VLF/BE. The message shall include one or more user identities (primary or callable) chosen by the HLF/BE as *alias Address* elements in the *destinationInfo* field.

Alternatively the HLF/BE may send an **AccessConfirmation** message back to BE#1, including a *template* that contains one or more suitable user identities as specific alias address(es) and a *routeInfo* field indicating *sendAccessRequest* in the *messageType* and the *transportAddress* of VLF/BE in the *contacts* field. BE#1 can then send another **AccessRequest** message to VLF/BE to obtain the location of the called user. The result of this variant is the same (but step F does not apply).

E: VLF/BE checks its location information about the user indicated by the received user identities and sends an **AccessConfirmation** message back to the HLF/BE (or to BE#1 if the alternative procedure of step D applies). The message shall include a *template* which contains a suitable user identity as the specific *aliasAddress* and a *routeInfo* field indicating *sendSetup* in the *messageType* and the call signalling *transportAddress* of either the gatekeeper to which the user is registered (GK#2) or of the H.323 MT itself in the *contacts* field. The choice of user identity and transport address is a matter of local policy at the visited domain.

F: The HLF may modify the **AccessConfirmation** message as necessary (e.g. add or replace user identities) and forwards the message to BE#1.

G: BE#1 redirects the **AccessConfirmation** message, possibly modified, to GK#1.

H: GK#1 sends an ACF message to the calling endpoint, based on the information received in the **AccessConfirmation** message. This is normal H.323 procedure.

I: The information received in the ACF message determines the following call signalling procedures according to ITU-T Rec. H.323: a **Setup** message is sent using either direct call signalling or GK routed signalling via GK#1 and/or GK#2. This is indicated by the broken line connecting the "Setup" arrows at each side.

J, K, L: Normal call establishment continues according to ITU-T Rec. H.323.

If BE#1 is not able to deduce the address of the HLF from the callable user identities in the **AccessRequest** message sent by a GK (as in step B above), or if VLF/BE has no location information corresponding to the user identities received in the **AccessRequest** message sent by a HLF/BE (as in step D above), the BE#1 or VLF/BE shall respond with an **AccessRejection** message with the *reason* field set to *noMatch*. Similarly, if the HLF/BE has no knowledge about the user indicated by the **AccessRequest** message that it received from a BE (as in step C above), the HLF/BE shall respond with an **AccessRejection** message with the *reason* set to *noMatch*.

On receipt of the **AccessRejection** message from VLF/BE, the HLF/BE shall forward the **AccessRejection** message to BE#1. On receipt of an **AccessRejection** message from an HLF/BE, a BE shall forward the message to the GK that initiated the **AccessRequest** (GK#1) and the GK shall send an ARJ message to the calling endpoint with the *reason* set to *calledPartyNotRegistered*.

The following list contains a summary of the message contents relevant to this Recommendation (for those messages or message fields that are not indicated here, the message or message field should be used as indicated in ITU-T Recs H.323, H.225.0 or H.501):

ARQ (calling side)

Field	Description
destinationInfo	One or more callable user identities.

ARJ

Field	Description
reason	
calledPartyNotRegistered	If the called user can not be located.

AccessRequest

Field	Description
destinationInfo	
logicalAddresses	For queries by the GK to the BE or the BE to the HLF, one or more callable user identities. For queries to the VLF/BE by the HLF/BE, optionally also the primary user identity of the user.

AccessConfirmation

Field	Description
templates	
pattern	
specific	One or more callable user identities and/or the primary user identity of the user, as appropriate.
routeInfo	
messageType	
sendSetup	Indicates that the originating endpoint/GK can send the Setup message to the address specified in the transportAddress in the contacts field.
contacts	
transportAddress	Call Signalling TSAP address of the called user or its GK.

AccessRejection

Field	Description
reason	
noMatch	If the functional entity receiving the AccessRequest message has no knowledge about the user indicated by the user identities in the AccessRequest message and the functional entity has no knowledge about any other functional entities that might be able to resolve the location of the user.

7.5.3 Call establishment mobility management procedures for outgoing calls

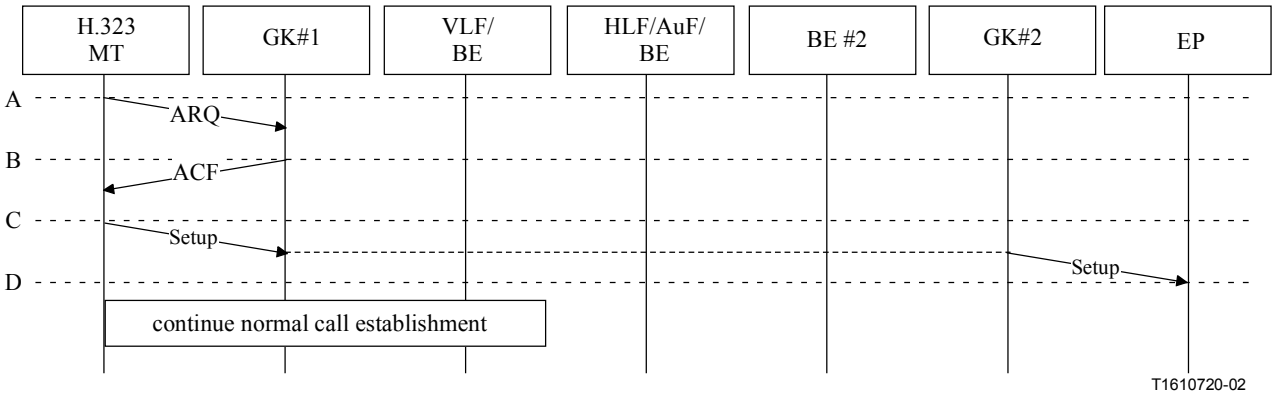


Figure 10/H.510 – Call establishment from a mobile terminal

Figure 10 depicts the information flow for a successful outgoing call establishment when the mobility management procedures are introduced. A more detailed description of the procedure follows:

A: The calling H.323 MT sends an ARQ to its gatekeeper (GK#1) according to standard H.323 procedures.

B: The gatekeeper returns an ACF with the location of the called user, according to normal H.323 procedures.

NOTE – If the called user is also a mobile user, the procedures of 7.5.2 apply as well.

C: The information received in the ACF message determines the following call signalling procedures according to ITU-T Rec. H.323: a Setup message is sent using direct call signalling or GK routed signalling via GK#1 and/or GK#2. This is indicated by the broken line connecting the "Setup" arrow at each side.

D: Normal call establishment continues according to ITU-T Rec. H.323.

7.5.4 Security

Security for H.510 is specified in ITU-T Rec. H.530. These procedures allow a serving domain to authenticate a mobile user/terminal when it attempts to locate a gatekeeper or register. As a result of the authentication process, the visiting user/terminal gets also authentication of the serving domain. Any further security procedures are performed locally between H.323 MT and gatekeeper.

7.6 Handover

If the mobile terminal moves during a call, mechanisms in the lower protocol layers may provide the needed handover functionality in a way that is transparent to H.323, i.e. in such a way that the NPoA of the terminal does not change.

Handovers that involve the change of NPoA, that is, needing also the intervention of H.323 protocol layers, are for further study.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2002