INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# H.225.0

**Amendment 1**
(11/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Transmission multiplexing and synchronization

---

Call signalling protocols and media stream packetization for packet-based multimedia communication systems

## Amendment 1: Revised Annex G: Communication between and within administrative domains

ITU-T Recommendation H.225.0 (2000) – Amendment 1

---

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.225.0

## Call signalling protocols and media stream packetization for packet-based multimedia communication systems

## Amendment 1

## Revised Annex G: Communication between and within administrative domains


**Summary**

The revised Annex G in this amendment describes methods to allow address resolution between or within administrative domains in H.323 systems for the purpose of completing calls within or between the administrative domains. Logical elements within an administrative domain that implement the procedures described in this amendment are called peer elements. An administrative domain exposes itself to other administrative domains through a type of peer element known as a border element.

In this version, this annex now describes only the procedures to be followed in such communications. The protocol message definitions have been moved to ITU-T Rec. H.501. This version also extends the applicability of the protocol to within administrative domains in addition to between administrative domains.

This annex fosters the scalability and interconnection of H.323-based networks by minimizing provisioning burden and providing routing and usage information between networks.



**Source**

Amendment 1 to ITU-T Recommendation H.225.0 (2000) was prepared by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 November 2002.

## 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 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.225.0

## Call signalling protocols and media stream packetization for packet-based multimedia communication systems

## Amendment 1

## Revised Annex G: Communication between and within administrative domains

*Replace Annex G as follows*:

### G.1 Scope

It is expected that the overall H.323 network will consist of smaller subsets of equipment organized in some manner, such as by Administrative Domain. Because of the potentially large numbers of H.323 elements that will exist in H.323 networks, an efficient protocol is needed to allow calls to be completed between Administrative Domains. The most elementary example is for a user (an endpoint) in one Administrative Domain to reach a user (an endpoint) serviced by another Administrative Domain. While the H.225.0 RAS protocol can address many of the needs for communication between Administrative Domains, it is neither complete nor efficient for this purpose.

For the same reason, an efficient protocol also needs to be specified between H.323 elements within the same Administrative Domain.

This annex describes methods to allow address resolution, access authorization and usage reporting between and within Administrative Domains in H.323 systems for the purpose of completing calls. H.323 elements that communicate using the procedures described in this annex are known as Peer Elements. An Administrative Domain exposes itself to other Administrative Domains through a type of logical element known as a Border Element. Border Elements are special cases of Peer Elements, at least one of whose peers belongs to another Administrative Domain. A Peer Element may be colocated with any other entity (for example, with a gatekeeper). Annex G does not require an Administrative Domain to reveal details about its organization or architecture. Annex G does not mandate a specific system architecture within an Administrative Domain. Furthermore, Annex G supports the use of any call model (gatekeeper routed versus direct endpoint).

The general procedure is for Peer Elements to exchange information regarding the addresses each can resolve. Border Elements exchange information regarding the addresses their Administrative Domains can resolve. Addresses can be specified in a general manner, or in an increasingly specific manner. Additional information allows elements within an Administrative Domain to determine the most appropriate Administrative Domain to serve as the destination for the call. Border Elements may control access to their exposed addresses, and require reports on the usage made during calls to those addresses.

Figure G.1 indicates a number of reference points representing signalling among various elements in an H.323 network. In this figure, the Administrative Domains are part of a global packet network without edges. Note that Figure G.1 is not an explicit definition of an H.323 system architecture, but is meant to illustrate signalling reference points.

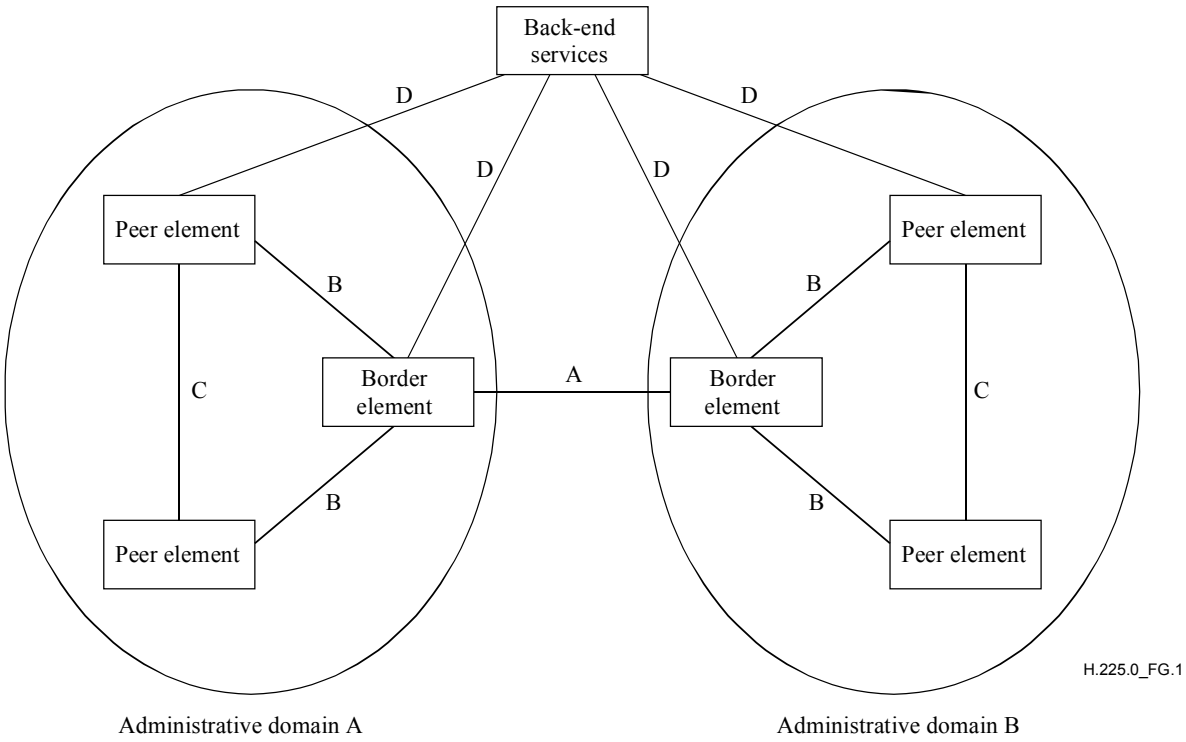


**Figure G.1/H.225.0 – System reference points**

Figure G.1 indicates the following reference points:

A – between border elements belonging to different administrative domains.

B – between border elements and peer elements within the same domain.

C – between peer elements within the same domain.

D – between H.323 elements and back-end services (not in the scope of this annex).

Reference points A, B and C are the focus of this annex. As was mentioned earlier, a Peer Element may be co-located with some other H.323 element.

Clause G.7, Signalling examples, provides some signalling examples that may aid understanding.

## G.2 Definitions

This Recommendation defines the following terms:

**G.2.1 administrative domain**: An Administrative Domain is a collection of H.323 entities administered by one administrative entity. An Administrative Domain may consist of one or more gatekeepers (that is, one or more zones).

**G.2.2 back-end services**: Back-End Services are functions such as user authentication or authorization, accounting, billing, rating/tariffing, etc. Back-end services and the protocol to exchange information with back-end services (if different from those described in this annex) are not in the scope of this annex.

**G.2.3 peer element**: As defined in ITU-T Rec. H.501, a Peer Element is a logical element that originates or terminates signalling messages defined in that Recommendation. This element may exist in combination with other H.323 elements, for example a combination of Peer Element, gatekeeper and gateway. An Administrative Domain may contain any number of Peer Elements.

**G.2.4 border element**: A special case of the Peer Element, the Border Element is a functional element with at least one peer that is outside of its Administrative Domain. It supports public access into an Administrative Domain for the purposes of call completion or any other services that involve multimedia communication with other elements within the Administrative Domain. The Border Element controls the external view of the Administrative Domain.

**G.2.5 clearing house**: A service (possibly in the form of a Border Element) that can provide resolution for all addresses (i.e. a type of aggregation point).

## G.3 Abbreviations

This Recommendation uses the following abbreviations:

AD Administrative Domain

BE Border Element

CH Clearing House

DST Daylight Saving Time

EP Endpoint

GK Gatekeeper

GW Gateway

PE Peer Element

SCN Switched Circuit Network

T Terminal

## G.4 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. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation H.225.0 (Version 4) (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[2] ITU-T Recommendation H.235 (Version 2) (2000), *Security and encryption for H-series (H.323 and other H.245-based multimedia terminals)*.

[3] ITU-T Recommendation H.323 (Version 4) (2000), *Packet-based multimedia communications systems*.

[4] ITU-T Recommendation H.323 Annex K (2000), *HTTP-based service control transport channel*, *(incorporated in H.323 (2000))*.

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

[6] ITU-T Recommendation H.460.2 (2001), *Number Portability interworking between H.323/SCN networks*.

## G.5 System models

Annex G does not mandate a specific system architecture among Administrative Domains or within an Administrative Domain. The following clauses provide some sample architectures, but these are to be viewed as illustrative rather than exhaustive.

Remember that a Peer Element is a functional element that may exist together with any other H.323 element. Figure G.2 shows some examples of Peer Element implementations in combination with other elements.

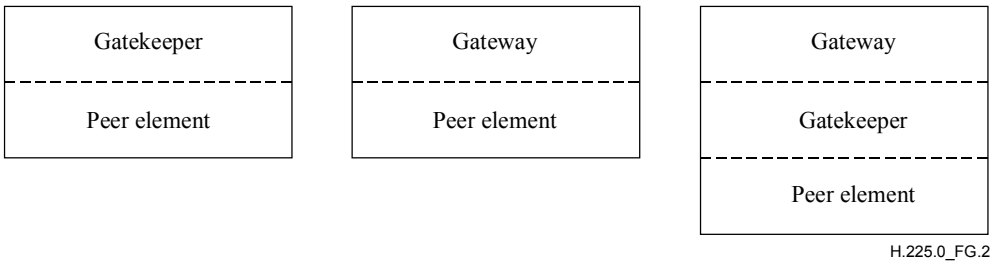


**Figure G.2/H.225.0 – Peer element placement examples**

In general, an Administrative Domain is viewed as consisting of any number of zones and any number of Peer Elements. The relationships among Administrative Domains, and among Peer Elements within an Administrative Domain, may be any of a variety of organizations. The following clauses describe example relationships and organizations. These are described as between Administrative Domains, but the Hierarchical, Distributed/Full-Mesh and Aggregation examples could also be used to organize Peer Elements within an Administrative Domain.

Note again that the following examples are illustrative, and not meant to exclude other possible organizations.

### G.5.1 Hierarchical

Figure G.3 shows a simple hierarchical arrangement among Administrative Domains. In such an arrangement, a Border Element in an Administrative Domain would consult a Border Element in an Administrative Domain higher in the hierarchy to resolve an address.

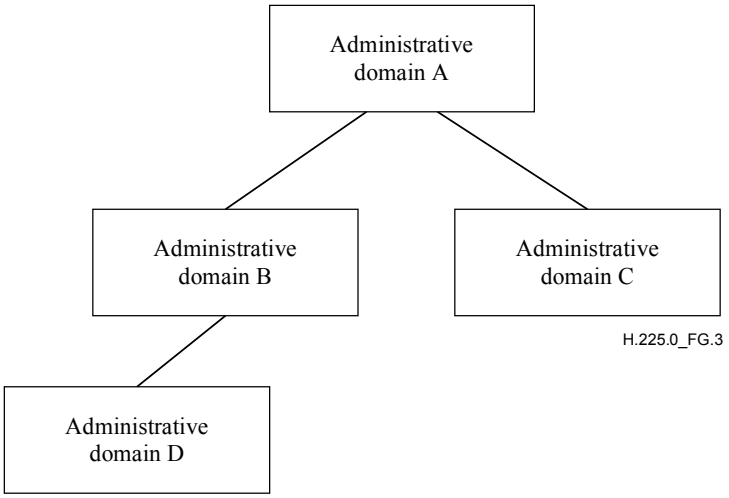


**Figure G.3/H.225.0 – Sample hierarchical organization**

### G.5.2 Distributed or full mesh

An entirely distributed or full mesh model is possible, as shown in Figure G.4. In this example, a Border Element in each Administrative Domain communicates with Border Elements in the other known Administrative Domains.

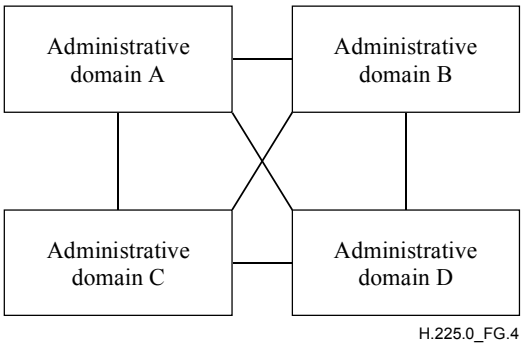


**Figure G.4/H.225.0 – Sample distributed organization**

### G.5.3 Clearing house

An example of a Clearing House arrangement is shown in Figure G.5. In this arrangement, each Administrative Domain consults the Clearing House to resolve addresses. Note that since a Clearing House is an entity that exists outside of an Administrative Domain, the Peer Elements that communicate with it are by definition Border Elements.

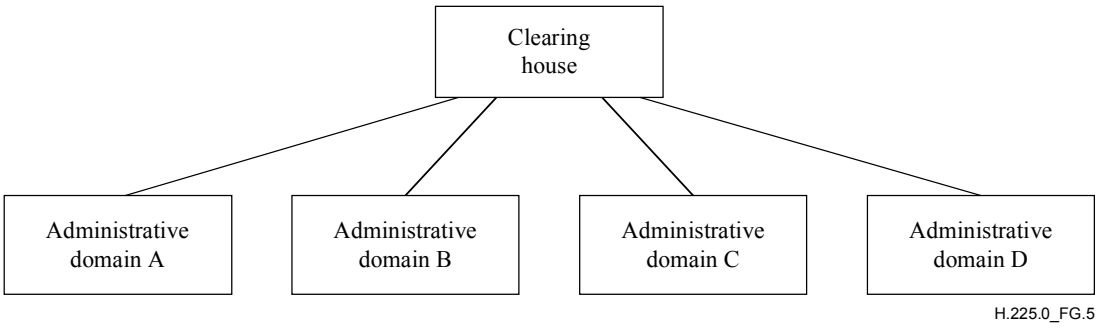


**Figure G.5/H.225.0 – Sample clearing house organization**

### G.5.4 Aggregation point

Figure G.6 shows an example of an aggregation point. In this example, Administrative Domain B is an aggregation point that can provide address resolution for both itself and Administrative Domains C and D. As an example, Administrative Domain B may forward resolution requests from Administrative Domain A to Administrative Domain C, or may instruct Administrative Domain A to contact Administrative Domain C directly for certain destinations. If Administrative Domain B forwards a request from Administrative Domain A to Administrative Domain C, Administrative Domain B may cache Administrative Domain C's response.

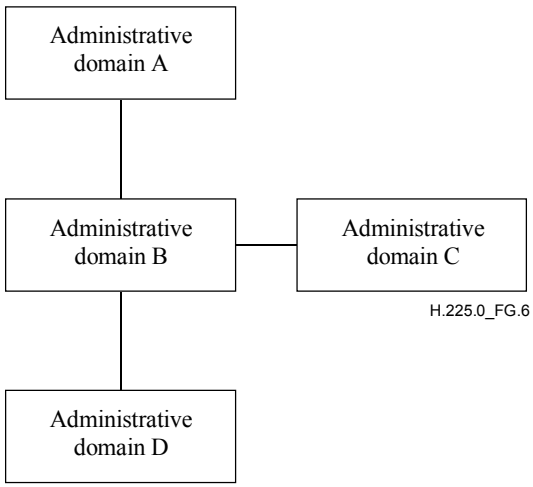


**Figure G.6/H.225.0 – Aggregation point example**

### G.5.5 Overlapping administrative domains

More than one Administrative Domain may be able to resolve a given address. For example, multiple Administrative Domains could contain gateways that can complete a call to a terminal in the GSTN. The selection of the appropriate destination Administrative Domain is the responsibility of the origination Administrative Domain. The algorithm employed to select the destination Administrative Domain is an implementation matter.

## G.6 Operation

### G.6.1 Use of H.501 messages

Annex G/H.225.0 implementations shall make use of messages defined in ITU-T Rec. H.501. The entities exchanging H.501 messages are referred to in that Recommendation as Peer Elements.

The following is a list of the H.501 messages used by Annex G/H.225.0:

ServiceRequest

ServiceConfirmation

ServiceRejection

ServiceRelease

DescriptorRequest

DescriptorConfirmation

DescriptorRejection

DescriptorIDRequest

DescriptorIDConfirmation

DescriptorIDRejection

DescriptorUpdate

DescriptorUpdateAck

AccessRequest

AccessConfirmation

AccessRejection

RequestInProgress

NonStandardRequest

NonStandardConfirmation

NonStandardRejection

UnknownMessageResponse

UsageRequest

UsageConfirmation

UsageRejection

UsageIndication

UsageIndicationConfirmation

UsageIndicationRejection

ValidationRequest

ValidationConfirmation

ValidationRejection

An Annex G/H.225.0 Peer Element receiving an H.501 request message not included in the above list shall respond with an UnknownMessageResponse message.

Messages shall contain all fields defined by H.501 as mandatory, and may contain optional fields as required.

### G.6.2 Address templates and descriptors

A Peer Element obtains templates in these ways:

- static configuration;
- receiving descriptors from other Peer Elements in response to general requests;
- receiving responses to specific queries.

#### G.6.2.1 Static configuration

A Peer Element will maintain templates for all the zones for which it is responsible. These templates may be explicitly provisioned in the Peer Element, or, in the case where the Peer Element co-exists with gatekeepers, these templates may be formed by summarizing information obtained from each gatekeeper with which the Peer Element communicates. The Peer Element may make this information available to other Peer Elements via responses to requests. An Administrative Domain may choose the level of detail to be provided by its Border Element(s). Examples include:

- A Border Element that wishes to hide internal structure might provide one descriptor (with an indication to send an AccessRequest message) that describes its whole zone and refers to a gatekeeper that will handle all incoming calls.
- A Border Element that does not care about revealing internal structure might provide a set of templates, each describing the gatekeeper for a zone within the domain.
- A Border Element that is on a firewall (or one using the gatekeeper routed model) might provide a template for the whole zone with an indication to send a Setup message.
- A Border Element with holes in its domain (because numbers have been moved to another Administrative Domain) provides templates marked **sendAccessRequest** that indicate which Border Element should be used to contact the other Administrative Domain.

- A Clearing House Border Element (such as one that has a complete copy of, e.g. 44) might hold a template marked **sendAccessRequest** for each Administrative Domain within 44.

Peer Elements need not keep a copy of the whole database. If a Peer Element does not hold a copy of the whole database, then it should contain statically configured **sendAccessRequest** templates indicating a Clearing House Border Element that will be used to resolve other queries.

### G.6.2.2 Receiving descriptors

A Peer Element may request the statically configured templates from another Peer Element. The response to the request is decided by the Peer Element from which the templates are being requested. To request a transfer, the Peer Element sends a DescriptorRequest message specifying the descriptors it wishes to receive. If the owning Peer Element is able to transfer the descriptors, it responds with a DescriptorConfirmation message specifying all the templates.

The requesting Peer Element may cache a copy of a template received in this manner until the template's lifetime expires, at which point the Peer Element should delete its copy of the template. If the owning Peer Element changes its statically configured templates before their lifetime has expired, then it shall send a DescriptorUpdate message to those Peer Elements of which it is aware. A Peer Element in receipt of a DescriptorUpdate message should delete, add, or change all indicated templates in its cache, or should request copies of the indicated descriptors from the owner.

An intermediate Peer Element (a Peer Element between the originating and destination Administrative Domains, such as a Clearing House or aggregation point) may publish its own descriptors based on the descriptors it receives. For example, a Clearing House may indicate itself as the contact for an AccessRequest message even though the descriptors it received from another Border Element indicate that other Border Element as the contact.

A Peer Element may indicate in a template the requirement for an originator to receive permission to place a call into an Administrative Domain. When the **callSpecific** flag is set in a template and the message type indicates that an AccessRequest message shall be sent, the originator shall provide per-call information in the AccessRequest message. If a Peer Element receives the AccessRequest message without per-call information and policy is to require per-call information, the Peer Element shall reply with an AccessRejection message with a reason of **needCallInformation**.

A Peer Element may send a DescriptorUpdate message to other known Peer Elements, or the Peer Element may multicast a DescriptorUpdate message. If a DescriptorUpdate message is multicast, the Peer Element should consider the scope of the multicast. The DescriptorUpdate message may contain the descriptors that have changed. Alternatively, the DescriptorUpdate message may indicate only the identification of the descriptors that changed, allowing the recipient to query for the new information. If a large number of descriptors have changed, the information should be sent in multiple DescriptorUpdate messages so that a particular DescriptorUpdate message does not exceed the maximum transport packet size.

### G.6.2.3 Receiving responses to specific queries

A Peer Element may send an AccessRequest message to another Peer Element asking for the resolution of a fully qualified or partially qualified address. The AccessRequest is usually sent over unreliable transport (e.g. UDP), although it may be sent over reliable transport (e.g. TCP).

A Peer Element in receipt of an AccessRequest searches its database and responds with the most specific template for the destination. If multiple templates satisfy the request, then the Peer Element shall return all matching templates. If the destination Peer Element is actually responsible for the alias address specified, the Peer Element will usually respond with a template indicating that either an AccessRequest or Setup message should be sent. If the destination Peer Element is a Clearing House, it will normally respond with a template indicating that the AccessRequest message should be sent.

The destination Peer Element may also add templates to the response that it believes will be useful in the future. The addition of these templates should not make the response so large that the transport network will need to fragment it (e.g. 576 octets for IPv4 or 1200 octets for IPv6).

For example, a Border Element that is tightly coupled with a firewall may provide two templates in its response to AccessRequest messages: one template with a short lifetime (of a few minutes or seconds) specifying the location to which a Setup message should be sent, and additional templates specifying that AccessRequest messages should be sent to the Border Element for other AliasAddresses within the Administrative Domain.

A Peer Element may cache a template received in an AccessConfirmation until its lifetime expires.

### G.6.3 Discovery of a peer element or set of peer elements

#### G.6.3.1 Static

A Peer Element may have an administered set of other Peer Elements that it may contact for address resolution. This administered set may be defined through a set of bilateral agreements, e.g. between Administrative Domains and other Administrative Domains. The Administrative Domains may optionally utilize the service of a Clearing House.

#### G.6.3.2 Dynamic

On IP networks, ownership of Email-ID style addresses is defined by the DNS system. Thus, in the absence of any better information, a border element may do a DNS SRV record lookup on the part of the email-ID to the right of the "@" sign (for example, a DNS SRV lookup on **_h2250-annex-g._udp.example.org** for **person@example.org**). The response to this lookup should be used to synthesize a **sendAccessRequest** template that can be used during the resolution process. Templates synthesized from DNS requests should not be cached for longer than the lifetime provided in the DNS response.

#### G.6.3.3 Other methods

The use of other methods to locate another Peer Element are for further study.

### G.6.4 Resolution procedures

#### G.6.4.1 Resolution procedure within administrative domain

When a Peer Element is asked to resolve an AliasAddress (e.g. by a colocated gateway or gatekeeper), it finds matching templates in its cache.

If more than one template matches, appropriate templates are selected and sorted according to local policy. For example, templates may be first sorted by wildcard length (more specific templates are better), then sorted by the type of protocol specified (**sendSetup** is better than **sendAccessRequest**).

If multiple templates satisfy the request, then the Peer Element shall return all matching templates.

If the template selection procedure produces no templates marked as **sendSetup**, then the Peer Element sends an AccessRequest message with a specific destination address to the address specified in the template. When it gets an answer from the Peer Element, it may store that in its cache and return to the requester the address to which to send the Setup message.

#### G.6.4.2 Resolution procedure between administrative domains

When a Border Element receives an AccessRequest message from a Border Element in another Administrative Domain, it searches through the templates in its cache and finds those that match the address in the query.

If more than one template matches, the matching templates are first sorted by wildcard length (more specific templates are better). They are then sorted by the specified message type (**sendSetup** is better than **sendAccessRequest**). In each case all templates other than the most specific match are discarded.

If the matched templates are marked as **sendAccessRequest** then the Border Element may choose to forward the AccessRequest message to the Border Element(s) specified in the template(s), or may choose to return the templates as they are. If the hop counter in the received AccessRequest message has reached zero, then the Border Element cannot forward the AccessRequest message to another Peer Element, but should instead return any matching templates. If the hop counter has reached zero and the Border Element has no information to provide in an AccessConfirmation, the Border Element should respond with an AccessRejection message indicating that the hop count was exceeded.

At this point, the Border Element may use another Border Element (e.g. a Clearing House) to authorize the access request. To do that, it sends a ValidationRequest message, carrying access tokens supplied by the requesting Border Element in the AccessRequest rights. The recipient Border Element validates the tokens and returns ValidationConfirmation.

The Border Element then returns an AccessConfirmation message containing the templates that it has found (these will have the same address and message type fields) and any other templates that it considers useful.

If multiple templates satisfy the request, then the Border Element shall return all matching templates.

If the access request contains specific call information, then the returned templates are valid only for the call requested. This is used when an Administrative Domain wishes to grant access on a per-call basis. In that case, the Administrative Domain may mandate the inclusion of call information per each AccessRequest sent to it. It does so by setting a flag in the templates that refer to it.

### G.6.5 Usage information exchange

Peer Elements may request other Peer Elements to provide them information about the usage of resources in specific calls. UsageIndication messages may be provided at any stage of the call. Also, multiple UsageIndication messages may be sent for the same call, each one with possibly more up-to-date information, or reporting on consecutive call segments or different media type usage. See G.6.5.1 for details.

UsageIndication messages may be exchanged irrespective of whether the two Peer Elements have a service relationship between them. However, the policy of a Peer Element may not allow such exchanges without a service relationship. In such a case, the Peer Element may reject the UsageIndication message, with a reject code of `noServiceRelationship`.

UsageIndication requests shall be sent whenever a Peer Element requires them, either in the templates for which it serves as contact, or by indicating in the ServiceRequest message it sends during service relationship establishment with a remote Peer Element, or by so indicating in either of the UsageRequest, AccessRequest, ValidationRequest and ValidationConfirmation messages sent in the context of the call for which usage information is required.

#### G.6.5.1 Multiple UsageIndications for the same call

Multiple UsageIndications for the same call provide increasingly more up-to-date information on the same media types, or usage information about new media types created in the same call. Also, since Peer Elements may take over calls while being in progress, not all the UsageIndications necessarily originate from the same Peer Element. The following rules define the semantics:

1) A UsageIndication message received with a **usageCallStatus** of **callInProgress** implies a subsequent UsageIndication with the same **callIdentifier** and **senderRole** should be received. If the recipient is configured for fault recovery, it may choose to conclude, after a configured time interval with no further UsageIndication messages, that a fault has occurred, and may recover whatever data it can from the received UsageIndication messages.

2) Subsequent UsageIndication messages with the same **usageField** ids should report a **startTime** matching the **endTime** of the previous message (although this may be impossible for an alternate Peer Element). Recipients shall assume each report is for a distinct period. Other information in the **usageField** overrides the information received in previous messages with the same **usageField** id.

3) A Peer Element should send a new UsageIndication message for each change in the media type during the call, e.g. audio stopped and fax started, or a codec has changed. If multiple media types are engaged at the same time (e.g. audio and video) they should be reported in the same UsageIndication message.

### G.6.5.2 Requesting and negotiating usage information during service relationship establishment

A Peer Element $PE_A$ may include a **UsageSpecification** element in a ServiceRequest message to a second Peer Element $PE_B$. This **UsageSpecification** element will be used to define the default usage information to be reported for all calls that take place while the service relationship exists between the two Peer Elements $PE_A$ and $PE_B$. This **UsageSpecification** shall be used for all calls for which $PE_B$ sends UsageIndications to $PE_A$.

If a **UsageSpecification** element arrives at $PE_B$ in another message from $PE_A$ (for example, an AccessConfirmation), then the new **UsageSpecification** overrides the default **UsageSpecification** for all calls related to the new message.

A Peer Element receiving a ServiceRequest that contains a **UsageSpecification** element should act as follows:

i) If the receiving Peer Element is willing to accept the ServiceRequest and the **UsageSpecification** contained within, it shall send a ServiceConfirmation message that contains the same **UsageSpecification** as the one received in the ServiceRequest. The **UsageSpecification** shall apply to both incoming calls to the recipient Peer Element from the requesting Peer Element, and outgoing calls from the recipient Peer Element to the requesting Peer Element.

ii) If the receiving Peer Element is willing to accept the ServiceRequest but is not willing to accept the **UsageSpecification** contained within, it shall either send a ServiceConfirmation message containing a different **UsageSpecification** that specifies the usage information that it is able to provide to the requesting Peer Element, or a ServiceRejection message with the reason set to **cannotSupportUsageSpec**.

iii) If the receiving Peer Element does not support usage reporting at all, it shall return a ServiceRejection message with the reason set to **usageUnavailable**.

A Peer Element receiving a ServiceConfirmation should act as follows:

i) If the **UsageSpecification** in the ServiceConfirmation is the same as the one sent in the ServiceRequest, then the originating Peer Element and terminating Peer Element have established a service relationship between them.

ii) If the **UsageSpecification** in the ServiceConfirmation is different from the one sent in the ServiceRequest message, then if the originating Peer Element is willing to use the new **UsageSpecification**, the service relationship is established. If the originating Peer

Element is not willing to use the new **`UsageSpecification`**, it shall send a ServiceRelease message with reason set to **`terminated`**. The originating Peer Element could then analyze the **`UsageSpecification`** returned in the ServiceConfirmation in order to build a new ServiceRequest message with a modified **`UsageSpecification`** that may be acceptable to both Peer Elements.

iii) If the ServiceConfirmation does not contain a **`UsageSpecification`** (and the ServiceRequest did), then the Peer Element that sent the ServiceConfirmation cannot, or will not, employ usage reporting at the level of the service relationship. This is the case when, for example, the recipient Peer Element implements version 1 of this annex. In this case, the originating Peer Element can either terminate the service relationship (by sending a ServiceRelease message with the reason code set to **`terminated`**), or not terminate the service relationship. In either case, if the originating Peer Element is interested in receiving usage information about calls, it should request usage information using the mechanisms described in version 1 of this annex (i.e. sending **`UsageSpecification`** elements in either AccessRequest, AccessConfirmation (within the returned address templates), UsageRequest, ValidationRequest or ValidationConfirmation messages).

### G.6.6 Number portability information signalling

ITU-T Rec. H.460.2 describes mechanisms for number portability in H.323 networks. Support for H.460.2 requires that Annex G be capable of transporting number portability information through address resolution message exchanges. The interface between the Annex G Border Element and the other H.323 network elements with which it communicates, is not covered by this annex; it is assumed this interface is capable of transporting the H.460.2 number portability to and from the Annex G Border Element.

When an AccessRequest is sent, it will transport the H.460.2 number portability information, if present, using the **`genericData`** field in the common information portion of the message.

AccessConfirmation and AccessRejection messages will carry the corresponding number portability response information in the **`genericData`** field as well. In the case of an AccessRejection, the reject reason shall be **`genericDataReason`**.

## G.7 Signalling examples

These signalling examples are provided to illustrate basic operation. In these examples, assume that the Administrative Domains have agreements with each other, so the Border Elements have been provisioned with information (e.g. TCP ports) about each other. In many of the examples below, RAS LRQ/LCF messages are exchanged between a gatekeeper and a Border Element within the same Administrative Domain. This is purely for illustrative purposes, and analogous Annex G messages could be exchanged between the Border Element and a Peer Element residing within the gatekeeper.

### G.7.1 Distributed or full mesh

An example of a distributed network is shown in Figure G.7.

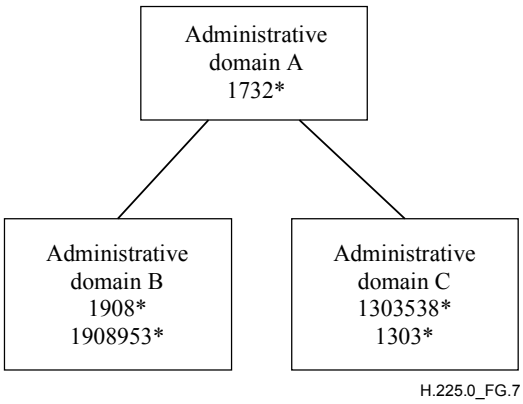


**Figure G.7/H.225.0 – Distributed network for signalling examples**

For this example, assume the Administrative Domains each have one Border Element, and that the Border Elements are configured to resolve addresses as follows:

| Administrative domain | Template definition | Comment |
|---|---|---|
| A | Descriptor "d1":<br>Pattern = 1732*<br>Transport address = $BE_A$ call signal address<br>Message type = **sendSetup** | Signalling for any call into AD A will be through AD A's Border Element. |
| B | Descriptor "d2":<br>Pattern = 1908*<br>Transport address = $BE_B$ annex g address<br>Message type = **sendAccessRequest**<br>Descriptor "d3":<br>Pattern = 1908953*<br>Transport address = $GW_{B1}$ call signalling address<br>Message type = **sendSetup** | For calls to 1908*, an AccessRequest message is needed to get the destination's (i.e. a gateway) call signalling address.<br>For calls to 1908953*, the Setup can be sent directly to this particular gateway. |
| C | Descriptor "d4":<br>Pattern = 1303538*<br>Transport address = $GK_{C1}$ call signal address<br>Message type = **sendSetup**<br>Descriptor "d5":<br>Pattern = 1303*<br>Transport address = $BE_C$ annex g address<br>Message type = **sendAccessRequest** | Calls to 1303538* will be routed through this particular gatekeeper.<br>Calls to 1303* can be signaled directly to the destination gateway, but an AccessRequest must be sent to obtain the gateway's call signalling address. |

### G.7.1.1 Exchange of zone information

In the distributed (or full mesh) organization, each Administrative Domain is aware of every other Administrative Domain, presumably through a number of bilateral contractual agreements. At any time, a Border Element in an Administrative Domain can query another Administrative Domain to obtain addressing information. An example of this signalling appears in Figure G.8.

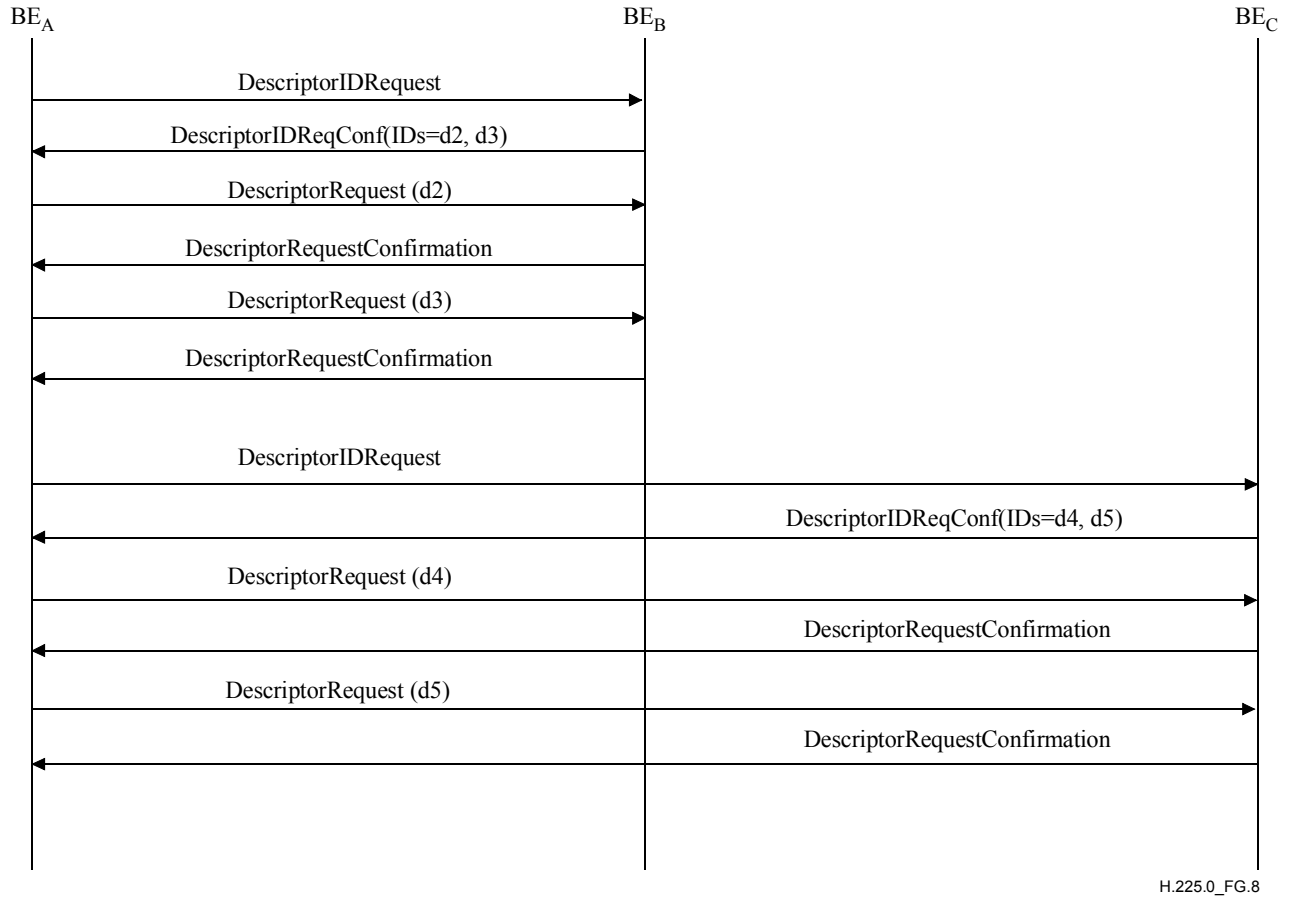


**Figure G.8/H.225.0 – Example of descriptor exchange**

Similarly, $BE_B$ queries $BE_A$ and $BE_C$, and $BE_C$ queries $BE_A$ and $BE_B$.

### G.7.1.2 Placing a call

Suppose that T1 in Administrative Domain A initiates a call to 19085551515 (T2). On receipt of T1's ARQ, T1's gatekeeper sends an LRQ. A Border Element in Administrative Domain A, $BE_A$, has previously received zone descriptors and knows how to process the request. As shown in Figure G.9, $BE_A$ sends an AccessRequest message to $BE_B$, as specified in the descriptor $BE_A$ received from $BE_B$. $BE_B$ replies back with T2's call signalling address (in this example, T2 could be any type of endpoint). T1 then sends the H.225.0 Setup message to T2's call signalling address following the normal procedures defined in ITU-T Rec. H.323 and its annexes.

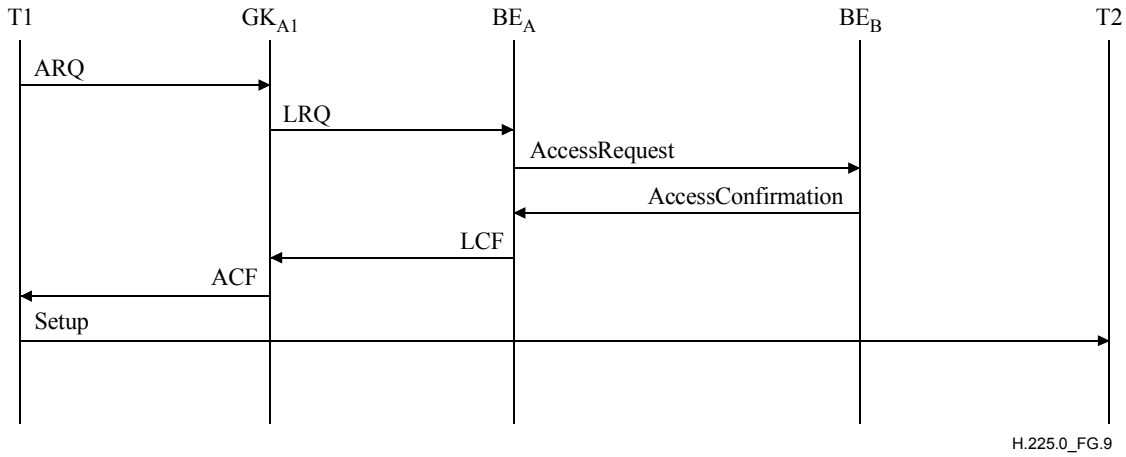


**Figure G.9/H.225.0**

Now, suppose that T1 initiates a call to 19089532000. In this example, $BE_A$ has previously obtained the call signalling address of a gateway in an Administrative Domain that will accept the call. As shown in Figure G.10, $BE_A$ can respond to the LRQ without any message exchange into Administrative Domain B, allowing T1 to send the Setup message directly to the gateway.

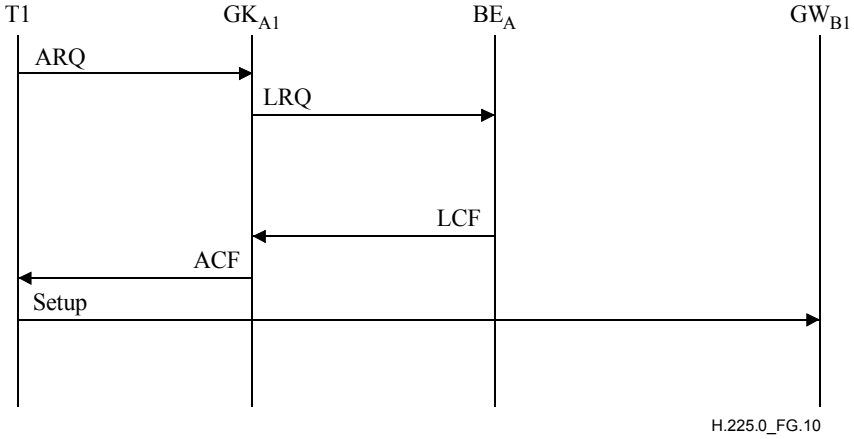


**Figure G.10/H.225.0**

In another example, suppose that T1 initiates a call to 13035382899. Administrative Domain C has advertised its ability to accept a call to this number, and will accept call signalling through its gatekeeper in implementing the gatekeeper-routed model. As shown in Figure G.11, $BE_A$ can respond to the LRQ with an LCF that contains the call signalling address of a gatekeeper in Administrative Domain C without any message exchange into Administrative Domain C.

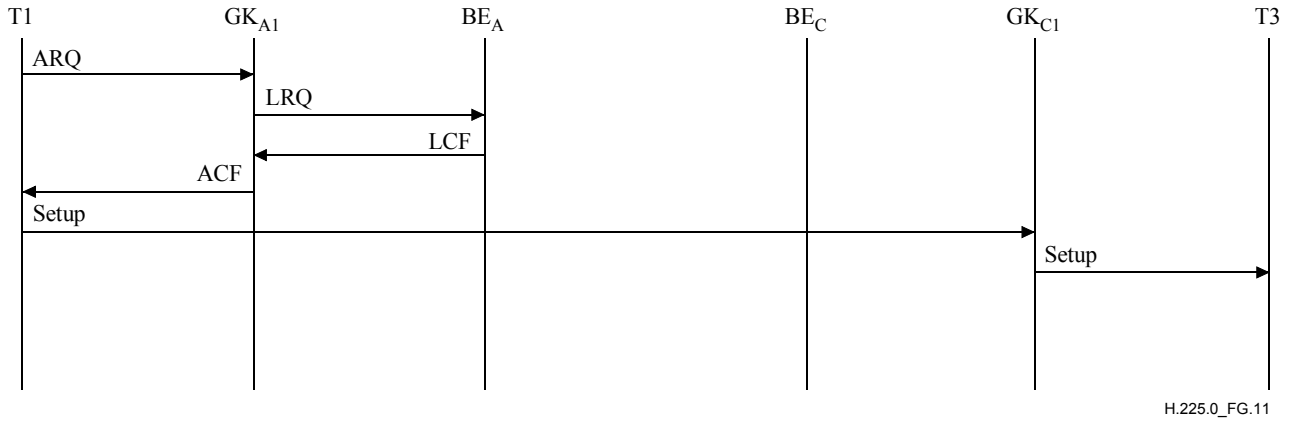


**Figure G.11/H.225.0**

Alternatively, T1's gatekeeper can implement the gatekeeper-routed model, as shown in Figure G.12.

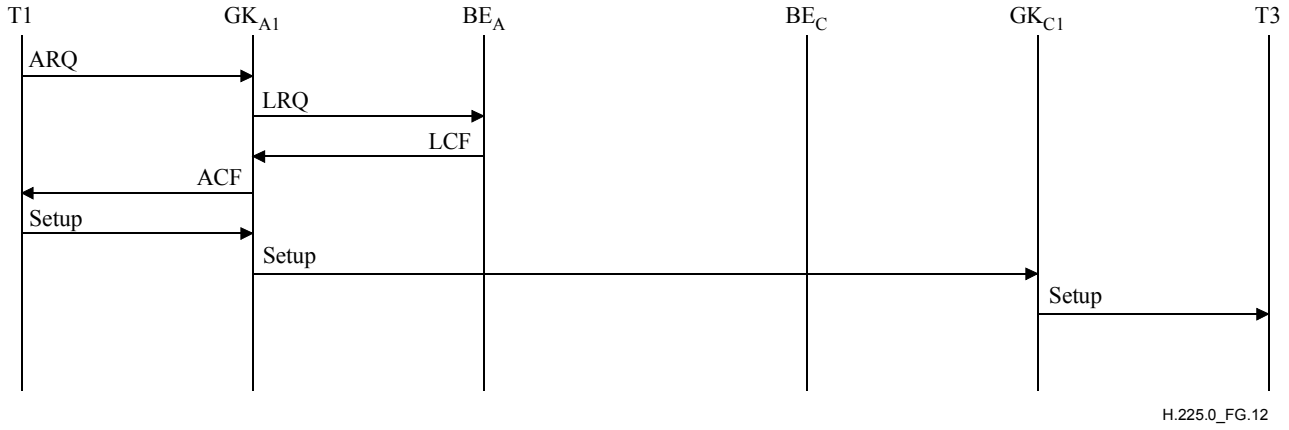


**Figure G.12/H.225.0**

### G.7.2 Clearing house

An example of a configuration using a Clearing House is shown in Figure G.13. Refer to this figure for the following examples. In this example, the Clearing House holds addressing information for all Administrative Domains for which the Clearing House provides service.

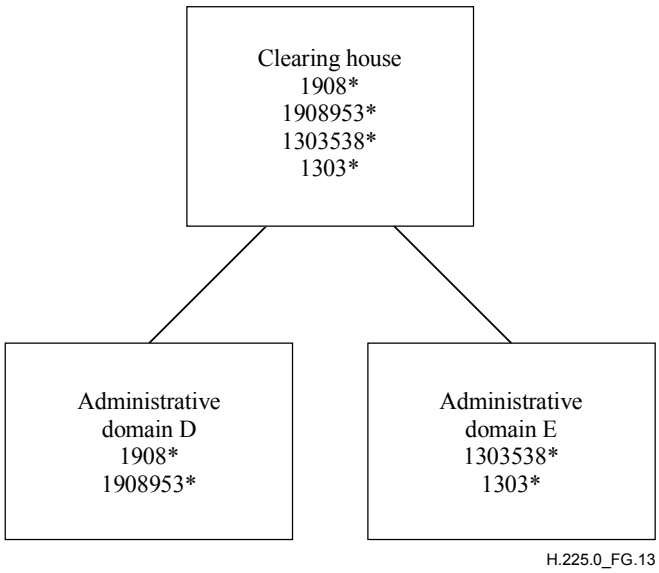


**Figure G.13/H.225.0 – Sample clearing house configuration**

For this example, the Border Elements in Administrative Domains D and E, and the Clearing House, contain the following information:

| **Administrative domain** | **Template definition** | **Comment** |
|---|---|---|
| D | Descriptor "d1":<br>Pattern = 1908*<br>Transport address = $BE_D$ annex g address<br>Message type = **sendAccessRequest**<br>Descriptor "d2":<br>Pattern = 1908953*<br>Transport address = $GW_{D1}$ Call Signalling address<br>Message type = **sendSetup** | For calls to 1908*, an AccessRequest message is needed to get the destination's (i.e. a gateway) call signalling address.<br>For calls to 1908953*, the Setup can be sent directly to this particular gateway. |
| E | Descriptor "d3":<br>Pattern = 1303538*<br>Transport address = $GK_{E1}$ call signal address<br>Message type = **sendSetup**<br>Descriptor "d4":<br>Pattern = 1303*<br>Transport address = $BE_E$ annex g address<br>Message type = **sendAccessRequest** | Calls to 1303538* will be routed through this particular gatekeeper.<br>Calls to 1303* can be signaled directly to the destination gateway, but an AccessRequest must be sent to obtain the gateway's call signalling address. |

| Administrative domain | Template definition | Comment |
|---|---|---|
| CH | Descriptor "d1":<br>Pattern = 1908*<br>Transport address = $BE_D$ annex g address<br>Message type = **sendAccessRequest**<br>Descriptor "d2":<br>Pattern = 1908953*<br>Transport address = $GW_{D1}$ call signalling address<br>Message type = **sendSetup**<br>Descriptor "d3":<br>Pattern = 1303538*<br>Transport address = $GK_{E1}$ call signal address<br>Message type = **sendSetup**<br>Descriptor "d4":<br>Pattern = 1303*<br>Transport address = $BE_E$ annex g address<br>Message type = **sendAccessRequest** | The Clearing House obtains descriptors from other ADs and holds this information for distribution during descriptor exchange. |

### G.7.2.1 Exchange of zone information

In this example, a Clearing House exchanges information with Administrative Domains that subscribe to the Clearing House's service. The Clearing House holds the information it receives from each Administrative Domain and passes this information along to other Administrative Domains. In this example, the Clearing House appears as Administrative Domain E to Administrative Domain D, while Administrative Domains D and E are not necessarily aware of each other. See Figure G.14.

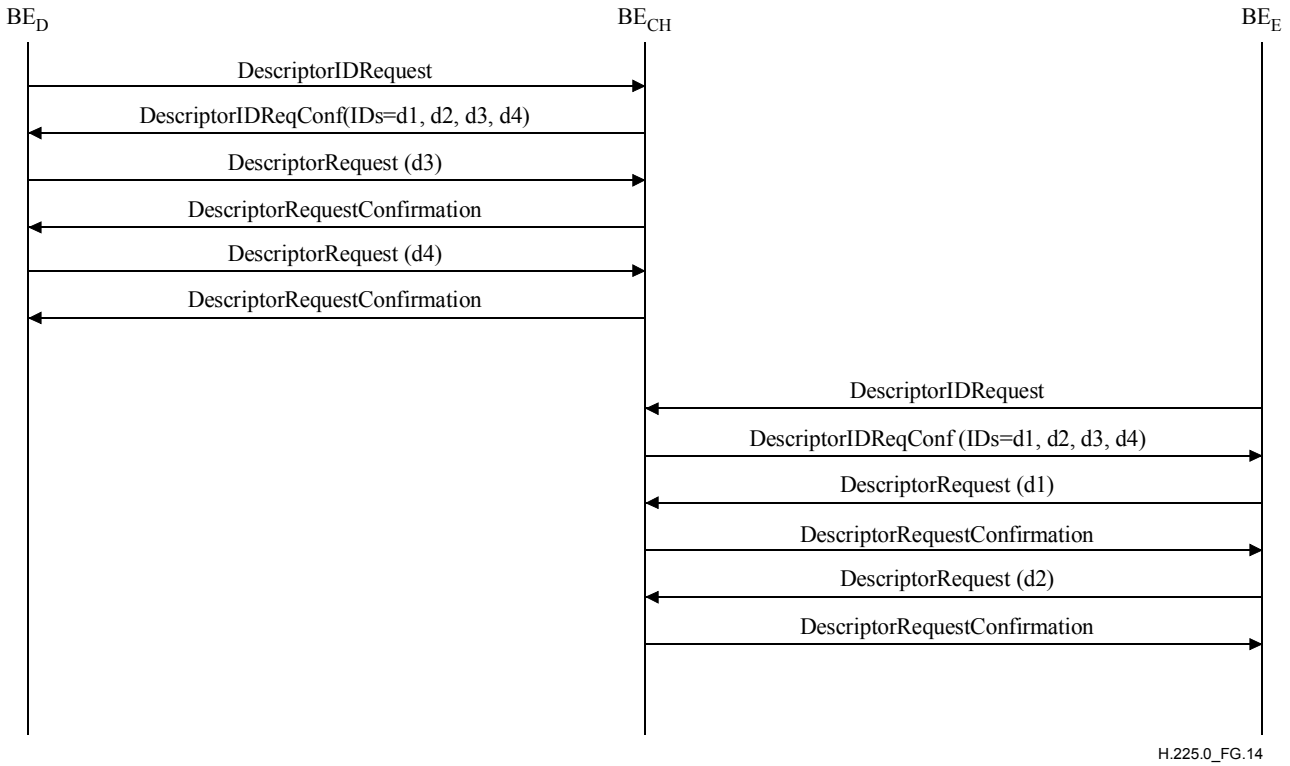


**Figure G.14/H.225.0 – Example descriptor exchange with clearing house**

### G.7.2.2 Placing a call

Suppose that T1 in Administrative Domain E initiates a call to 19085551515. The Border Element in Administrative Domain E has received descriptors from the Clearing House that indicate the Clearing House should be consulted for such a call. The Border Element sends an AccessRequest to the Clearing House Border Element. Based on the descriptors the Clearing House Border Element received from the Border Element in Administrative Domain D, the Clearing House Border Element sends an AccessRequest to the Border Element in Administrative Domain D. When the Clearing House Border Element returns the confirmation to the Border Element in Administrative Domain E, the confirmation contains the information sent from the Border Element in Administrative Domain D. T1's gatekeeper returns an ACF with T2's destCallSignalAddress, allowing T1 to send the Setup message to T2. See Figure G.15.

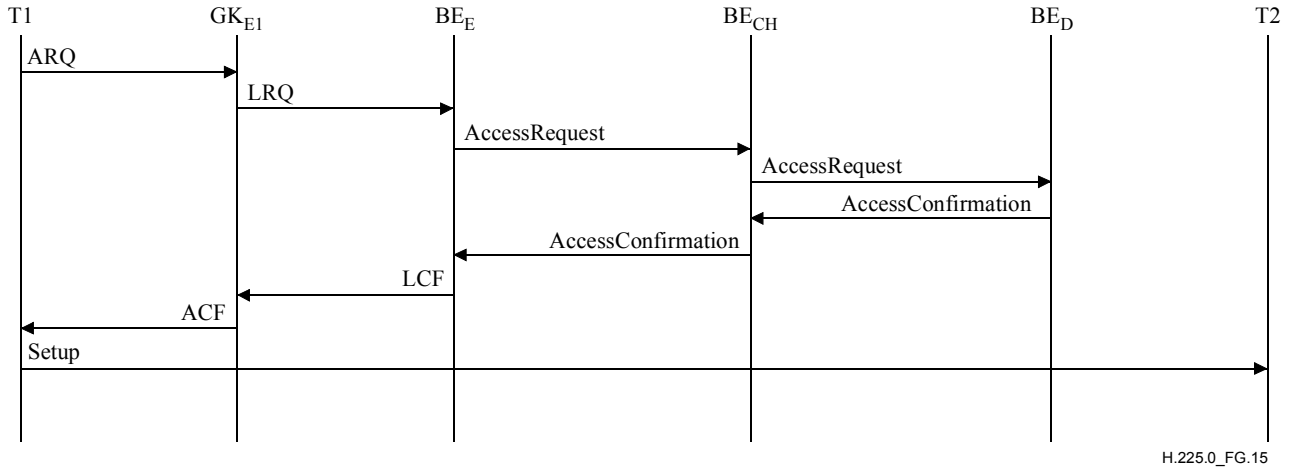


**Figure G.15/H.225.0**

Alternatively, T1's gatekeeper could route the call signalling, as shown in Figure G.16.

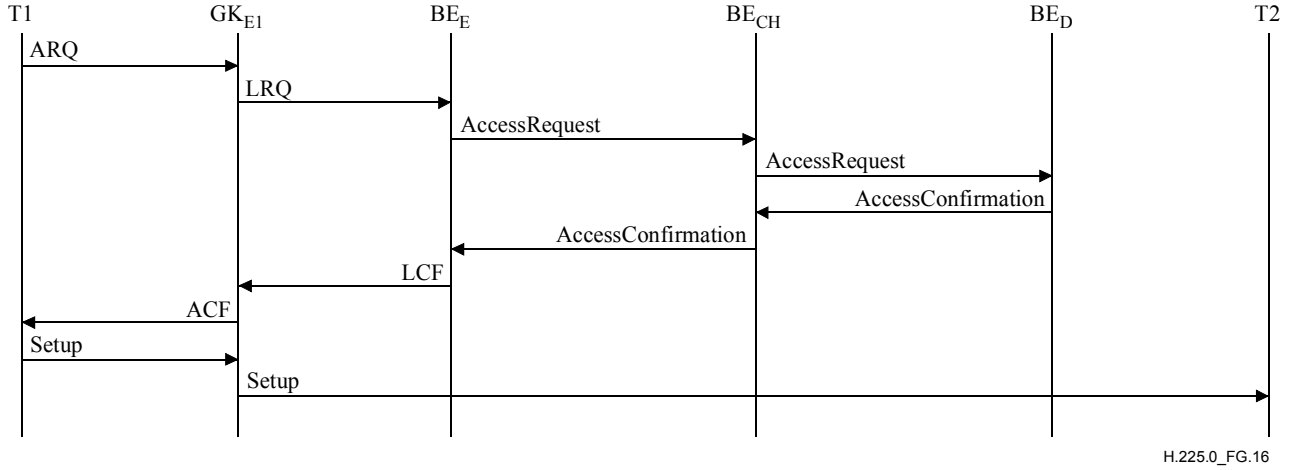


**Figure G.16/H.225.0**

Another possibility is for the Clearing House to respond to the Border Element in Administrative Domain E with the contact information for the Border Element in Administrative Domain D, as shown in Figure G.17.

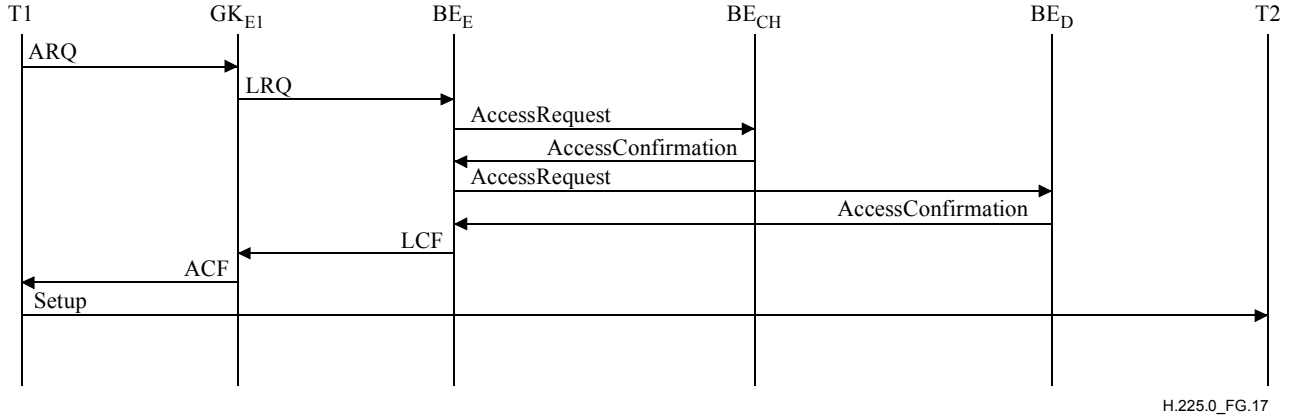


**Figure G.17/H.225.0**

Now suppose that T1 initiates a call to 19089532000. The descriptors previously exchanged allow the Border Element to return the call signalling address to T1 without consulting the Clearing House, as shown in Figure G.18.

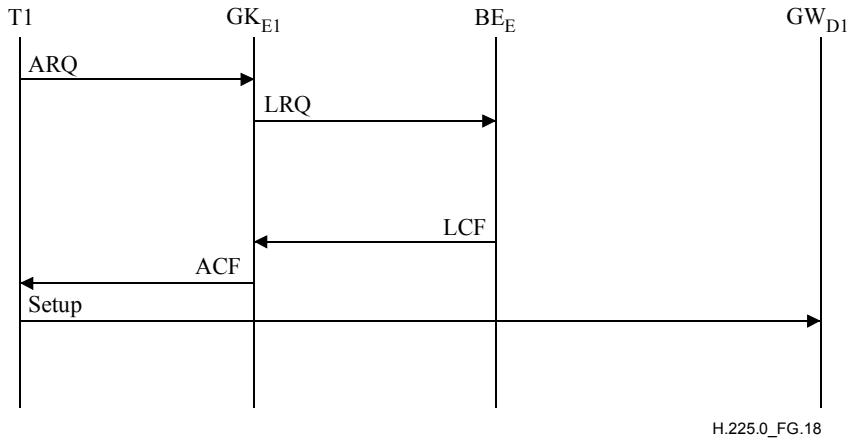


**Figure G.18/H.225.0**

Next, consider a scenario where T1 initiates a call to 13035382899. The Border Element in Administrative Domain E had previously advertised that calls to 1303538* could be routed directly to a gatekeeper in Administrative Domain E without need for an Access Request message, as shown in Figure G.19. (This advertisement does not indicate that the entity is a gatekeeper, only that a Setup message could be sent to a specified address.) The Border Element in Administrative Domain D received this information from the Clearing House, assuming the Clearing House in this example does not have a requirement to provide address resolution for these calls.

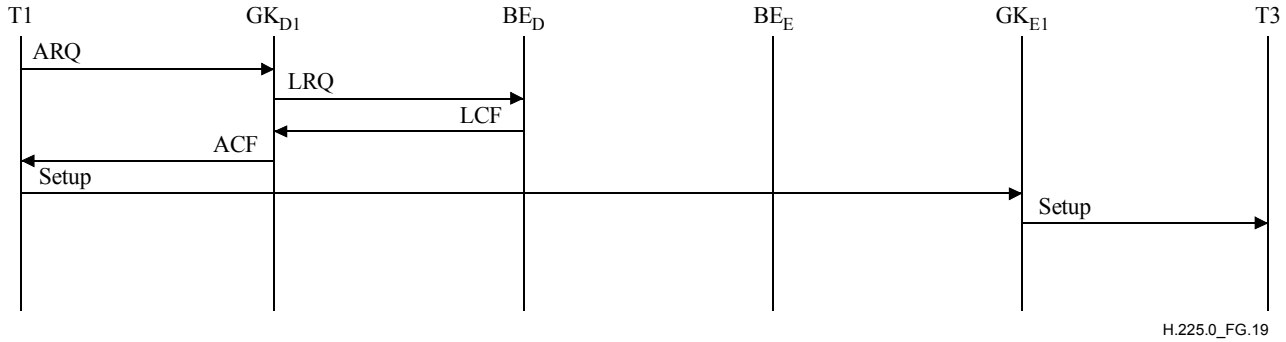


**Figure G.19/H.225.0**

Recall that a Border Element may be combined with a gatekeeper, and may also route calls in the gatekeeper-routed model. An alternative signalling example is shown in Figure G.20. It is also possible to use the Border Element as a routing gatekeeper into an Administrative Domain if the descriptors are so configured.

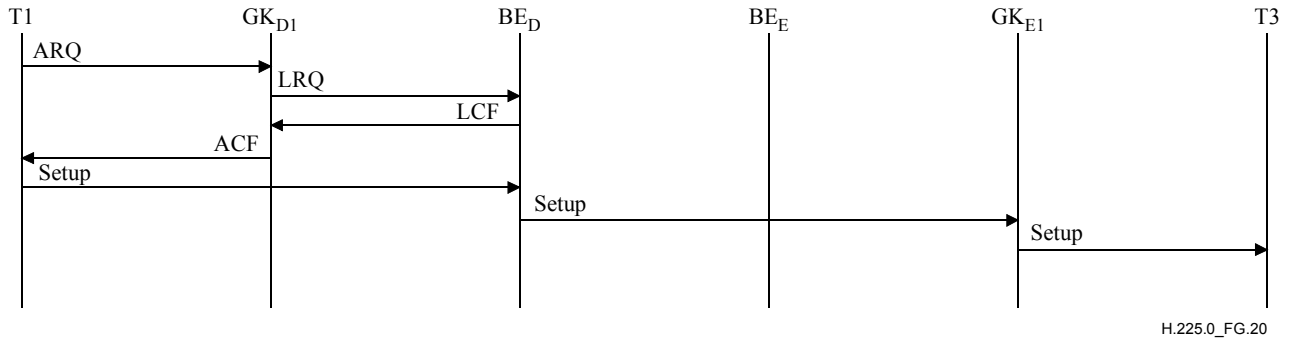


**Figure G.20/H.225.0**

In the example of Figure G.21, the Clearing House validates the call for the terminating Administrative Domain. The Clearing House also requires both originating and terminating Border Elements to send UsageIndications for the call.

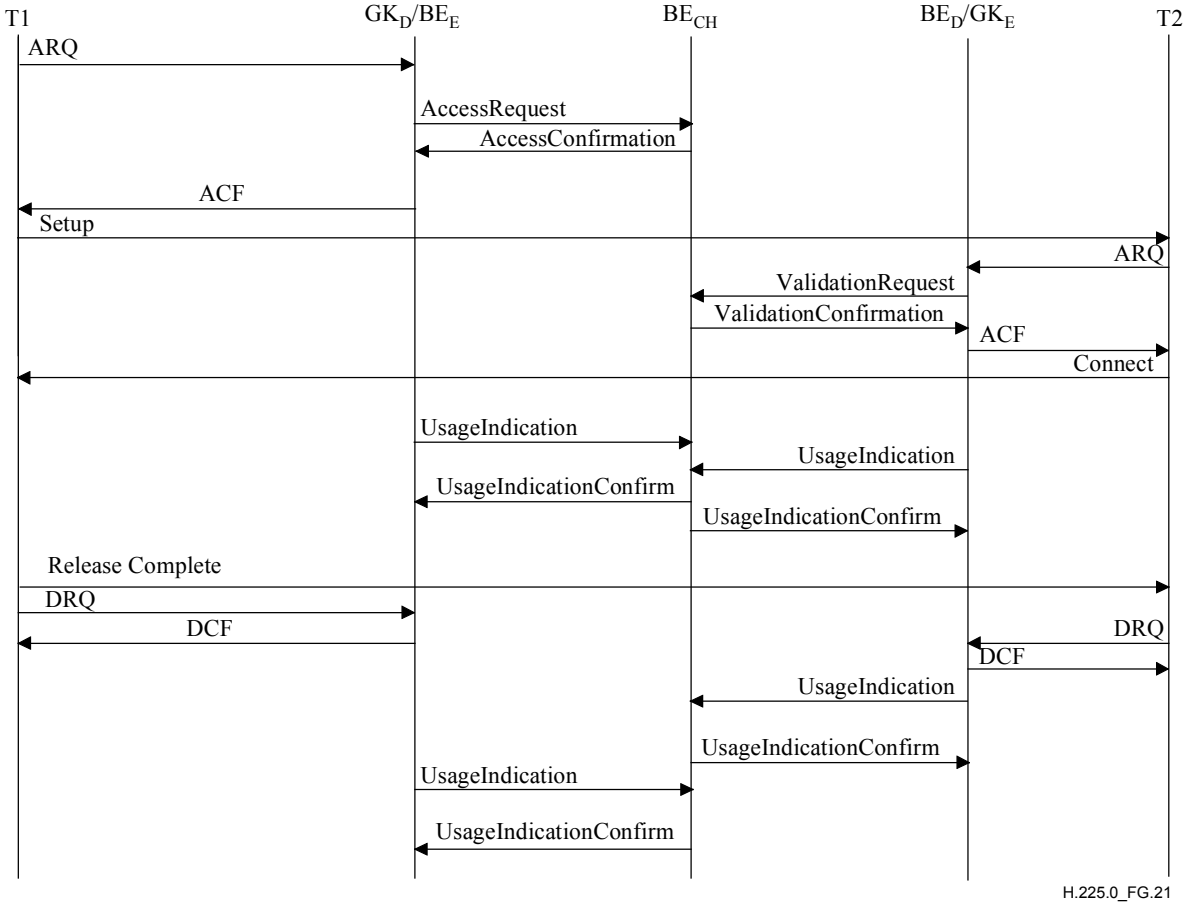


**Figure G.21/H.225.0**

## G.8 Annex G profiles

### G.8.1 Introduction

ITU-T Rec. H.501 offers a rich set of messages and fields that Annex G/H225.0 may use for interaction between Administrative Domains and between Peer Elements within a single Administrative Domain. Many of the messages and fields are optional and can be used in a variety of ways to implement different services or service options. This clause specifies implementation

profiles that define the messages, fields and procedures that are required in order to claim compliance with a specific profile.

### G.8.1.1 Profile signalling and negotiation

The H.323 generic extensible framework may be used by a Peer Element to signal to another Peer Element the set of profiles that it needs for a transaction to be successful, the set of profiles it desires to use, and the set of profiles it supports. This profile negotiation signalling may be done either in an individual message exchange (e.g. in an AccessRequest/AccessConfirmation exchange), or during the establishment of a service relationship. Note that the establishment of a service relationship between two Peer Elements may not be required by a profile.

#### G.8.1.1.1 Processing by the requesting entity

A requesting entity (a Peer Element) uses the elements in the **`FeatureSet`** structure to specify the various profiles it requires. It specifies the set of profiles that it needs using the **`neededFeatures`** field, the set of profiles that it desires using the **`desiredFeatures`** field, and the set of profiles that it supports in the **`supportedFeatures`** field. All three of these fields are in the **`FeatureSet`** structure.

In response to its request, a requesting entity should receive either a confirmation or a rejection message.

If the request is rejected, the responding entity may have included a set of **`neededFeatures`** that the requesting entity must support in order for the request to be successful. If this is the case and the requesting entity supports the needed features (e.g. a specific profile), the requesting entity may re-issue a request specifying support for the profile needed by the responding entity.

If the request is accepted, special procedures need to be applied to ensure that the negotiation operates in a backwards-compatible manner. This is done by the requesting entity checking that the profiles that it specified as needed are listed as **`supportedFeatures`** in the response. If a requesting entity does not observe the profiles it needs in the response message's **`supportedFeatures`** field, then it shall assume that the responding entity does not support the profiles that it needs. If the requesting entity determines that it cannot continue under these circumstances, then it shall undo the operation it was trying to perform (i.e. send a ServiceRelease message if it originally sent a ServiceRequest message), so that the state in the responding entity is rolled back.

#### G.8.1.1.2 Processing by the responding entity

The responding entity looks at the profiles specified in the **`neededFeatures`** field of the request to determine if it can accept the request. It also looks in the **`neededFeatures`**, **`desiredFeatures`** and **`supportedFeatures`** fields to determine whether the profiles needed by it are supported by the requesting entity.

If the responding entity determines that the necessary sets of profiles are supported by both entities, then the responding entity may acknowledge the request. The responding entity lists the set of profiles that it chooses to support in the **`supportedFeatures`** field of its reply. If the request is accepted, then all of the **`neededFeatures`** from the request must be included in the **`supportedFeatures`** field of the reply. The responding entity may also include **`desiredFeatures`**.

If the responding entity needs additional profiles to be supported by the requesting entity, it shall reject the request. If it wishes to declare which profiles must be supported for the request to be successful, this should be specified using the **`neededFeatures`** field of the reject message. The responding entity may also include any **`desiredFeatures`** and **`supportedFeatures`** in the reject message.

#### G.8.1.1.3 Identifiers

The following identifier is used within a FeatureDescriptor to specify that the FeatureDescriptor applies to Annex G/ H.225.0 profiles.

| Value | Description |
|---|---|
| idAnnexGProfiles | This identifier is used in the "id" field of a FeatureDescriptor to indicate that the FeatureDescriptor is describing the Annex G profiles needed/desired/supported. |

The following table contains a list of the identifiers used within the generic extensibility framework that are relevant to Annex G/H.225.0.

| Standard INTEGER Value | Description |
|---|---|
| 0 | Identifier within a FeatureDescriptor indicating that the FeatureDescriptor is describing Annex G/H.225.0 profiles |
| 1 | Identifier within an EnumeratedParameter that identifies Annex G/H.225.0 Profile "A" |

### G.8.2 Profile "A": Interzone call routing to a trusted gatekeeper

This profile specifies a simple intra-domain service; per-call queries to another trusted zone for endpoint determination where the Annex G signalling address of the trusted zones is statically provisioned. This is one of the simplest uses of Annex G and is similar to the use of RAS LRQ to query another zone for an endpoint. The same profile may be used to query a trusted Peer Element, which returns routes from domain-wide knowledge or obtains them by further Annex G queries.

#### G.8.2.1 Required messages

Entities complying with this profile shall support the messages indicated as "Mandatory" in the following table:

| Message | Transmit (Mandatory, Optional, Recommended) | Receive and act on (Mandatory, Optional, Recommended) |
|---|---|---|
| ServiceRequest | O | M (Note 1) |
| ServiceConfirmation | O | O |
| ServiceRejection | M | O |
| ServiceRelease | O | O |
| DescriptorRequest | O | M (Note 1) |
| DescriptorConfirmation | R (Note 2) | O |
| DescriptorRejection | M | O |
| DescriptorIdRequest | O | M (Note 1) |
| DescriptorIdConfirmation | R (Note 3) | O |
| DescriptorIdRejection | M | O |
| DescriptorUpdate | O | M (Note 4) |
| DescriptorUpdateAck | M | O |
| AccessRequest | M | M |

| Message | Transmit (Mandatory, Optional, Recommended) | Receive and act on (Mandatory, Optional, Recommended) |
|---|---|---|
| AccessConfirmation | M | M |
| AccessRejection | M | M |
| RequestInProgress | M | M |
| NonStandardRequest | O | M |
| NonStandardConfirmation | O | O |
| NonStandardRejection | M | O |
| UnknownMessageResponse | M | M |
| UsageRequest | O | M (Note 1) |
| UsageConfirmation | O | O |
| UsageRejection | M | O |
| UsageIndication | O | M (Note 1) |
| UsageIndicationConfirmation | O | O |
| UsageIndicationRejection | M | O |
| ValidationRequest | O | M (Note 1) |
| ValidationConfirmation | O | O |
| ValidationRejection | M | O |
| NOTE 1 – Shall be received and as a minimum rejected.<br>NOTE 2 – It is recommended that an entity return as a minimum a single descriptor for a template with Send Access Request pointing to itself.<br>NOTE 3 – It is recommended that an entity return as a minimum a single descriptor for a template with Send Access Request pointing to itself.<br>NOTE 4 – Shall be received and Ack'ed, but need not be processed. | | |

### G.8.2.2 Required fields

All fields defined as mandatory by ITU-T Rec. H.501 are also mandatory within this profile.

Entities complying with this profile shall also support the fields specified in the following table.

Other fields defined as optional by ITU-T Rec. H.501 may optionally be present.

| Message or structure | Required field | Comment |
|---|---|---|
| AccessRequest message | `destinationInfo` | One address containing the fully-qualified E.164 address of the destination |
| | `sourceInfo` | Includes the domainInfo and endpointType |
| | `callInfo` | |
| AccessConfirmation message | `templates` | If any templates are present, then there is one template per each termination gateway/gatekeeper |
| | `partialResponse` | Set to FALSE |
| AddressTemplate structure | `pattern` | One specific pattern is present containing the E.164 number |
| | `routeInfo` | One instance present |
| | `timeToLive` | |

| Message or structure | Required field | Comment |
|---|---|---|
| RouteInformation structure | **messageType** | Present |
| | **callSpecific** | Set to FALSE |
| | **contacts** | One instance present |
| | **type** | Must be present if messageType = sendSetup |
| ContactInformation structure | **transportAddress** | The IP address of the gateway/gatekeeper |
| | **priority** | |

### G.8.2.3 Required procedures

In this profile, entities may use the static discovery procedures of Annex G (clause G.6.3.1) and so will have a configured list of Peer Elements or gatekeepers to which requests can be sent. This list may contain alternates to be used only when the primary element cannot be reached or may simply add the alternates (if any) to the list.

Entities may also use the dynamic discovery procedures of Annex G (clause G.6.3.2).

Entities shall send an AccessRequest message to a selected Peer Element or gatekeeper for each call. If more than one Peer Element or gatekeeper is available to be queried for a given call, it is not specified whether they must be queried in sequence or may be queried in parallel. This choice is left to the requesting entity.

The reply will have zero or more templates. **timeToLive** may be set to 60 seconds or less to indicate that it may not be used for another call.

To improve interoperation with more general peers, it is suggested that in the case that the Peer Element does not implement descriptor support, it should follow the following procedures:

- If a DescriptorIDRequest message is received, the Peer Element should return a DescriptorIDConfirmation message containing a single **DescriptorInfo**. This **DescriptorInfo** describes a descriptor containing a single template specifying **sendAccessRequest** pointing to the Peer Element itself.
- If a DescriptorRequest message is received, the Peer Element should return a DescriptorConfirmation message containing a single descriptor. This descriptor shall contain a single template specifying **sendAccessRequest** pointing to the Peer Element itself.

### G.8.2.4 Identifiers for Profile "A"

The following identifier is used within an **EnumeratedParameter** to specify that the EnumeratedParameter specifies Annex G/H.225.0 Profile A.

| Value | Description |
|---|---|
| idAnnexGProfileA | This identifier is used in the "id" field of an **EnumeratedParameter** to indicate that Annex G Profile A is needed/desired/supported.<br>Note that the "content" field of the **EnumeratedParameter** is not present. |

## 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, 2003