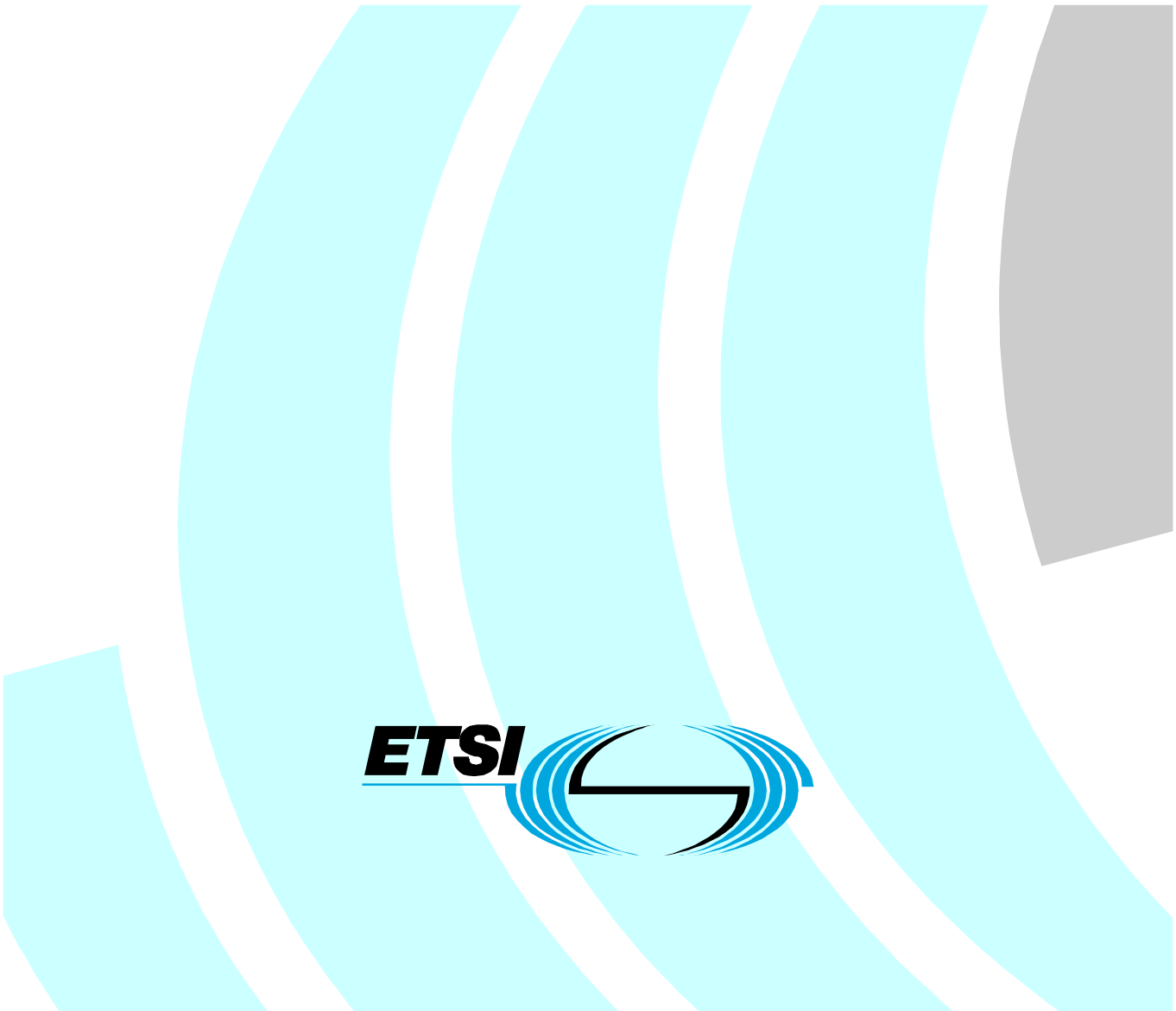
ETSI TS 101 883 V1.1.1 (2002-04)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using H.323



Reference
DTS/TIPHON-03017

Keywords
architecture, configuration, internet, IP, network, protocol, telephony, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The approach being taken to standardization in TIPHON represents a departure from that used in the past for PSTN, ISDN and GSM. Its aim is to allow much greater scope for competition through innovation in the design of equipment and services. Its aim is also to provide adequate standardization to facilitate the operation of services across interconnected networks, even networks that use different technologies. The present document presents the initial core set of Service Capabilities envisaged to be required to enable service providers to offer services on TIPHON networks that may safely interwork with existing PSTN services while enabling more advanced services to be subsequently developed.

Figure 1 shows the relationship of the present document with other TIPHON Release 3 deliverables.

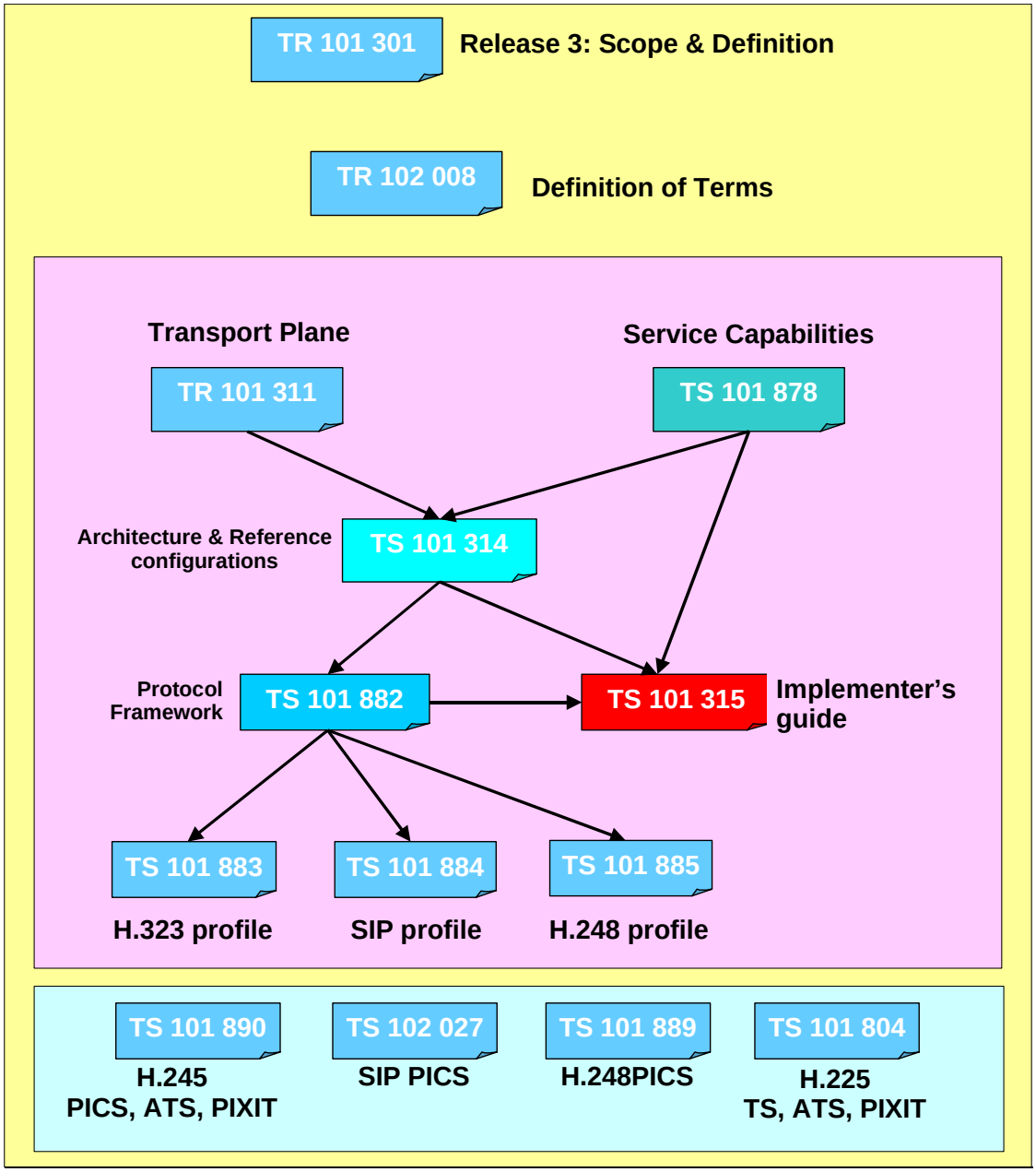


Figure 1: Relationship with other TIPHON Release 3 documents

- TR 101 311 [2] provides the requirements on the transport plane;
- TS 101 878 [6] defines service capabilities that are used in the TIPHON Release 3 for a simple call;
- TS 101 882 provides the Protocol Framework based on the TIPHON Release 3 architecture to implement the simple call service capabilities as defined in the present document;
- TS 101 315 [17] is an implementer's guide that shows how to use of the meta-protocol to realize the capabilities as defined in TS 101 878 [6];
- TS 101 883 (the present document) provides the protocol mappings for the ITU-T H-323 profile;
- TS 101 884 provides the protocol mappings for the SIP profile;
- TS 101 885 [14] provides the protocol mappings for the ITU-T H-248 profile; and
- TS 101 314 [8] provides the architecture and reference configurations for TIPHON Release 3.

1 Scope

The present document describes how the H.323 protocol suite can be used to implement the architecture, defined in TS 101 314 [8] and the primitives, information elements and behaviours, defined in TS 101 882.

The present document defines the mapping of the following meta-protocols:

- the Registration meta-protocol;
- the Bearer Control meta-protocol; and
- the Call Control meta-protocol.

The document is applicable to equipment performing the roles of terminal, gateway, gatekeeper and also to entities within the IP network that are necessary to support TIPHON Release 3.

The H.323 profile contained in the present document was derived by examination of:

- ITU-T Recommendation H.323 [10] and associated suite of protocols:
  - H.225.0 (RAS and Q.931); and
  - H.245 (Media control channel-signalling protocol);
- the capabilities required by TS 101 878 [6] for the support of TIPHON as identified in TR 101 300 [4];
- the TIPHON baseline architecture described in TS 101 314 [8]; and
- the primitives, parameters and procedures defined in TS 101 882.

Figure 1 is derived from TS 101 314 [8] and illustrates the scope of the present document.

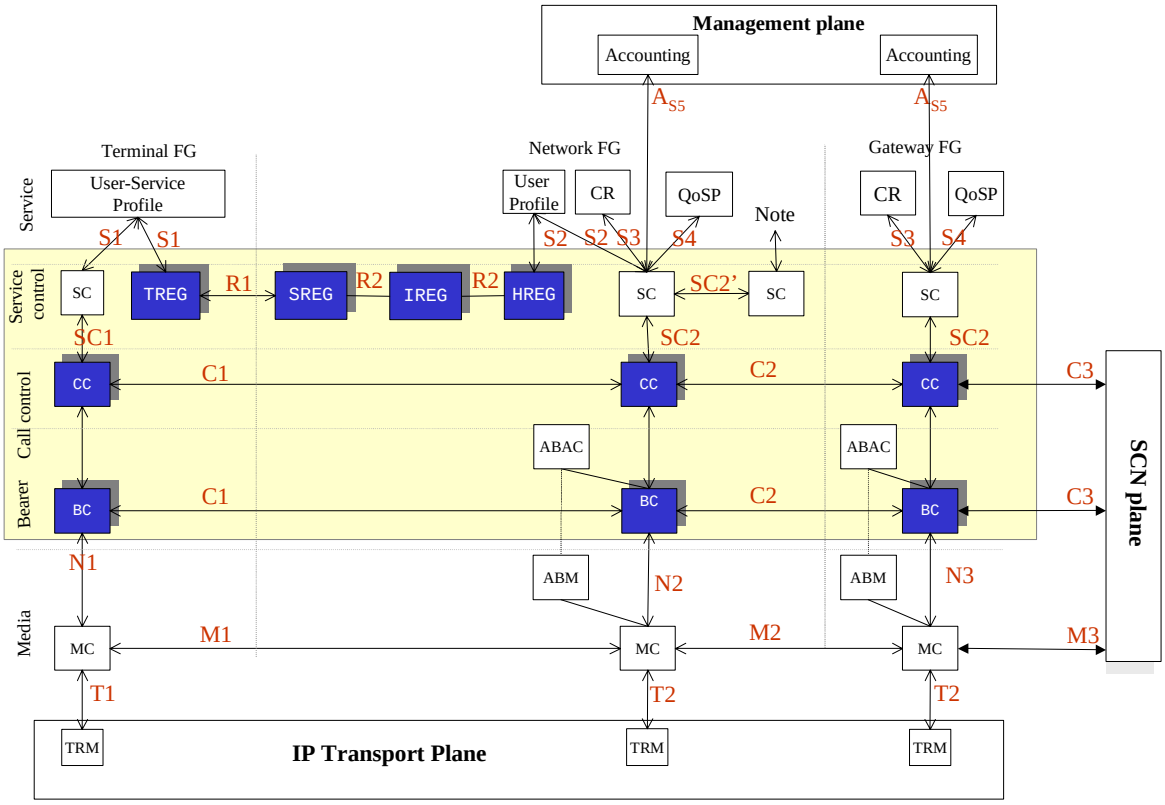


Figure 2: Scope of the present document

Where the text indicates the status of a requirement (i.e. as strict command or prohibition, as authorizations leaving freedom or as a capability or possibility), this may modify the nature of a requirement within a referenced standard used to provide the capability.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[2] ETSI TR 101 311: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Independent requirements definition; Transport Plane".

[3] Void.

[4] ETSI TR 101 300: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Description of Technical Issues".

[5] Void.

[6] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[7] Void.

[8] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[9] Void.

[10] ITU-T Recommendation H.323 (2000): "Packet-based multimedia communications systems".

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

[12] ITU-T Recommendation H.245 (2000): "Control protocol for multimedia communication".

[13] ITU-T Recommendation H.225.0 Annex G: "Communication between administrative domains".

[14] ETSI TS 101 885: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Technology Mapping of TIPHON reference point N to H.248/MEGACO protocol".

[15] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

[16] Void.

[17] ETSI TS 101 315: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Functional Entities, Information Flow and Reference Point Definitions; Guidelines for application of TIPHON functional architecture to inter-domain services".

[18] Void.

[19] ETSI TR 101 301: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Release Definition; TIPHON Release 3 Definition".

[20] ETSI TR 102 008: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Terms and Definitions".

[21] ETSI TS 101 890 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Compliance Specifications; TIPHON profile for ITU-T H.245".

[22] Void.

[23] Void.

[24] ETSI TS 101 804 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology compliance specifications; H.225 conformance test specification".

[25] ITU-T Recommendation I.112: "Vocabulary of terms for ISDNs".

[26] ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access provider: access provider provides a user of some network with access from the user's terminal to that network

accounting: process of collecting the call information data for purposes of attributing costs between service providers or network operators

address: string or combination of digits and symbols which identifies the specific termination points of a connection/session and is used for routeing

administrative domain: collection of physical or functional entities under the control of a single administration

aggregate bearer: logical association of functional entities in an IP Telephony application and Transport Network which creates one or more concurrent end to end media flows and which is not limited to the duration of a single call

aggregate bearer admission control: functional entity that determines whether or not a flow is to be admitted as part of an established aggregate bearer

aggregate bearer admission control function: functional entity that determines whether or not a flow is to be admitted as part of an established aggregate bearer

aggregate bearer measurement function: functional entity that determines the capacity used and remaining in an aggregate bearer as a result of measuring the actual media flows after taking into account what flows were requested

application data: media or signalling information content

authentication: process of proving identity within its context

NOTE: This normally entails proving the possession of a secret (uniquely associated with the identification) to the authenticator.

authorization: process of granting permission on the basis of identity, to access or use a service, or to access information

NOTE: Authorization is performed by the entity that controls the resource, and, if payment is required, that same entity is responsible for accounting to the customer or other party.

backward call clearing: ability for the called party to release a call during the call

basic call control: signalling protocol associated with the DSS1 - ISDN Basic Call control procedures of ITU-T Recommendation Q.931

bearer: logical association of functional entities in an IP Telephony application and Transport Network that creates an end to end media flow for no longer than the duration of a call

bearer service: type of telecommunication service that provides the capability for the transmission of signals between user-network interfaces

billing: process of presenting the user with a request for payment e.g. based on network usage; possibly including supporting information such as call records

broker: provider of a business service to facilitate the interworking between multiple IP service providers and SCN operators involved in the delivery of a telephony service

NOTE: This may be restricted to accounting settlements, but can also include routing assistance, authorization of use of resources, price information exchange.

call: any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system. In this context a user may be a person or a machine

called number: normally a name written as a numerical string identifying the called party or called terminal

carrier: provider of a transit network or services

channel: *channel* is often used in the literature to describe a single data stream and will therefore be treated synonymously to *flow* through TS 101 883

charging: process of determining the amount of money a user shall pay for usage of a certain service

codec: combined speech encoder and decoder

dialling plan: string or combination of decimal digits, symbols, and additional information that defines the method by which the numbering plan is used

NOTE: A dialling plan includes the use of prefixes, suffixes, and additional information, supplemental to the numbering plan, required to complete the call (e.g. ITU-T Recommendation E.164 [1]).

directory service provider: provider of directory information, e.g. providing an E.164 number from an email address

domain: collection of physical or functional entities within an administrative domain which share a consistent set of policies and common technologies

E.164 number: number conforming to the numbering plan and structure specified in ITU-T Recommendation E.164

endpoint: entity that can originate and terminate both signalling and media streams

NOTE 1: An endpoint can both call and be called.

NOTE 2: Examples of endpoints include H.323 terminals, SIP User Agents, gateways, or Multi-party Conference Units.

firewall: device (computer or software or both), used to restrict and monitor usage of computer(s) or the network

flow: single data stream, identified by a tuple of characteristic values (source address, source port, destination address, destination port, protocol number)

functional entity: entity in a system that performs a specific set of functions

functional group: collection of Functional Entities within a domain

NOTE: In TIPHON systems functional groups are used to structure the necessary functionality to offer IP telephony services across domains.

GateKeeper (GK): H.323 entity on the network that provides address translation and controls access to the network for H.323 terminals, gateways and MCUs

NOTE: The gatekeeper may also provide other services to the terminals, gateways and MCU such as bandwidth management and locating gateways. (See also ITU-T Recommendation H.323 [10].)

gatekeeper service provider: IP service provider who offers services available from gatekeepers to the user

gateway: endpoint on a network which provides for real time, two way communication between an IP based network and an Switched Circuit Network (SCN)

gateway functional group: functional group containing the functionality of a network functional group also the functionality necessary to connect calls to the SCN

NOTE: Gateway functional groups may be classified as originating or terminating based upon their location within the topology of a specified call.

Global User Service - Type GU: provides originating and terminating services for users with an E.164 Global Code number, which requires access to a Global IP-Telephony Directory Service

global service: service defined by the ITU-T, provisioned on the public switched network, to which the ITU-T has assigned a specific country code to enable the provision of that international service between two or more countries and/or integrated numbering plans (e.g. ITU-T Recommendation E.164)

H.323 terminal: entity which provides audio and optionally video and data communications capability in point-to-point or multipoint conferences in packet-based networks

home network functional group: functional group which is aware of the service application subscribed to by the End-User

NOTE: Home network functional groups may be classified as originating or terminating based upon their location within the topology of a specified call.

identity: technical label which may represent the origin or destination of any telecommunications traffic, as a rule clearly identified by a physical telecommunications identity number (such as a telephone number) or the logical or virtual telecommunications identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis

information flow: interaction between a communicating pair of functional entities

Integrated Services Digital Network (ISDN): See ITU-T Recommendation I.112 [25], clause 2.3 definition 308.

interception interface: physical and logical locations within the access provider's/network operator's/service provider's telecommunications facilities where access to the content of communication and intercept related information is provided

NOTE: The interception interface is not necessarily a single, fixed point.

interception measure: technical measure which facilitates the interception of telecommunications traffic pursuant to the relevant national laws and regulations

interception subject: person or persons, specified in a lawful authorization, whose telecommunications are to be intercepted

interface: shared boundary between two communicating systems, devices or equipments

intermediate network functional group: functional group connecting the serving network functional group to the Home network functional group

NOTE: The intermediate network functional grouping is only present when the serving network functional grouping and the home network functional grouping are not directly connected.

interworking function: function connecting two networks of different signalling or different administrative policies and/or transport technologies

IP address: each network unit connected to an IP network must have a unique Internet or IP address

NOTE: Today's IP addresses is based on IPv4 and are 32-bit numbers with its predefined structure. The IP address (IPv4) is written as four decimal numbers separated by a point.

IP access provider: company or organization which provides access to IP services which could be either access to a private IP network (Intranet) or to the Internet

IP end user: user who is connected to an IP network

IP endpoint: device that originates or terminates the IP based part of a call

NOTE: Endpoints include H.323 clients, and IP telephony gateways.

Interworking function: function connecting two networks of different signalling and or transport technology

IP network: packet transport network comprising one or more transport domains each employing the IP protocol

IP network provider: company or organization which provides access to an IP network

IP number: number conforming to the structure of addresses in IP networks

IP service provider: company or organization which provides access to IP services which could be either access to a private IP network (Intranet) or to the Internet

IP Telephony: any telephony related service that is supported on a managed IP network

IP telephony service provider: service provider who offers IP telephony services

NOTE: The same business entity may act as both a Transport Network Operator and an IP telephony Service Provider.

lawful authorization: permission granted to an LEA under certain conditions to intercept specified telecommunications and requiring co-operation from a network operator/access provider/service provider

NOTE: Typically this refers to a warrant or order issued by a lawfully authorized body.

listener echo: echo produced by double reflected signals and disturbing the listener

location information: information relating to the geographic, physical or logical location of an identity relating to an interception subject

network: telecommunications network that provides telecommunications services

Network Address Translation: Network Address Translation mechanism

network element: component of the network structure, such as a local exchange, higher order switch or service control processor

network functional group: functional group containing the functionality required to establish a call between two terminals, a gateway and a terminal, or two gateways

NOTE: Network functional groups may be classified as originating or terminating based upon their location within the topology of a specified call.

network operator: operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means

number: string of decimal digits from a recognized number plan (e.g. ITU-T Recommendation E.164)

numbering plan: numbering plan specifies the format and structure of the numbers used within that plan

NOTE: It typically consists of decimal digits segmented into groups in order to identify specific elements used for identification, routing and charging capabilities, e.g. within ITU-T Recommendation E.164 [1] to identify countries, national destinations, and subscribers. A numbering plan does not include prefixes, suffixes and additional information required to complete the call. The national numbering plan is the national implementation of the ITU-T Recommendation E.164 [1] numbering plan.

number portability: ability for a customer (subscriber) to change service provider, location or service while retaining the same number

originating network: the context of TS 101 883 the term originating network may have a different meaning dependent on functional group

NOTE: The originating network means every functional group *before* the actual functional group.

packet flow/transport flow: stream of packets of the same type identified by common address and port numbers

NOTE: The stream may contain either signalling information or content description together with media information.

prefix: indicator consisting of one or more digits, that allows the selection of different types of number formats, networks and/or services (e.g. ITU-T Recommendation E.164)

Private Integrated services Network eXchange (PINX): PISN nodal entity that provides automatic switching and call handling functions used for the provision of telecommunication services

protocol: set of semantics, syntax and procedures which govern the exchange of information across an interface

proxy server: intermediary program that acts as both a server and a client for the purpose of making SIP requests on behalf of other clients

NOTE: Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

public: indication of availability to the general public e.g. public network, public service

quality of service: quality specification of a telecommunications channel, system, virtual channel, computer-telecommunications session, etc.

NOTE: Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

reference point: conceptual point at the conjunction of two communicating functional entities

roaming user: scenario, where a user communicates with its home network functional group via a serving network functional Group

routeing: set of instructions on how to reach a destination

service: set of telecommunication related tasks performed for a customer by a Service Provider and supplied in a business context

service abstraction layer: component of the TIPHON Application Plane that provides a modular and extensible set of Service Capabilities for use in the creation of Service Applications

service application: way in which a number of Service Capabilities are combined to provide a Service

service capability: specified set of functionalities which are used to provide a component part of a Service

service domain: collection of physical or functional entities offering IP telephony services under the control of an IP Telephony Service Provider which share a consistent set of policies and common technologies

service information: information used by the telecommunications infrastructure in the establishment and operation of a network related service or services

NOTE: The information may be established by an access provider, network operator, a service provider or a network user.

service provider: business entity that provides Services to its customers on a contractual basis and is responsible for the services offered

Service Provider Access Interface: interface between a network and a service provider's equipment for enabling the service provider to access specific functionality of a network

Service Provider IDentifier: globally unique identifier of a service provider (Service Domain)

service provider network: network controlled by a Service Provider which offers service to other persons

service provider portability: ability for a customer (subscriber) to change service provider while retaining the same number

serving network functional group: functional group that enables terminal functional groups to connect to an IP Telephony Service Provider

Switched Circuit Network (SCN): telecommunications network, e.g. Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), and General System for Mobile communications (GSM), that uses circuit-switched technologies for the support of voice calls

NOTE: The SCN may be a public network or a private network.

telecommunications: any transfer of signs, signals, writing images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system

telephone call: two-way speech communication between two users by means of terminals connected via network infrastructure

teleservice (telecommunication service): type of telecommunication service that provides the complete capability, including terminal equipment functions, for communication between users according to protocols established by agreement between Administrations and/or RPAs

NOTE: See ITU-T Recommendation I.112 [25], clause 2.2.

terminal: endpoint within the user equipment on which signalling and media flows originate and/or terminate

terminal functional group: functional group representing all the IP Telephony functionality within an End-User's terminal

NOTE: Terminal functional groups may be classified as originating or terminating based upon their location within the topology of a specified call.

terminal registration functional group: functional group representing the registration functionality within an End-User Domain

terminating network: every functional group *after* the actual functional group

NOTE: In the context of the present document the term terminating network may have a different meaning dependent on functional group.

TIPHON compliant: entity that complies with the mandatory requirements identified in the TIPHON requirements documents together with compliance to the parts of the TIPHON specifications in which these requirements are embodied

TIPHON compliant system: system that complies with the mandatory requirements identified in the TIPHON specifications

transit network: network between two networks, e.g. between the initiating network and the recipient network

user: entity using the services of a network via terminal equipment

user at home: scenario, user that communicates directly with its gatekeeper without involvement of intermediate networks

user profile: service specific information about a user of a service application

value added service provider: service provider which provides services beyond normal or traditional services

NOTE: The extra services are normally informational services and are not part of the services which are offered traditionally by service providers

valid: test purpose covering a signalling procedure where all the messages sent to or received from the IUT are valid (expected in the current status of the IUT) and correctly encoded

3.2 Abbreviations

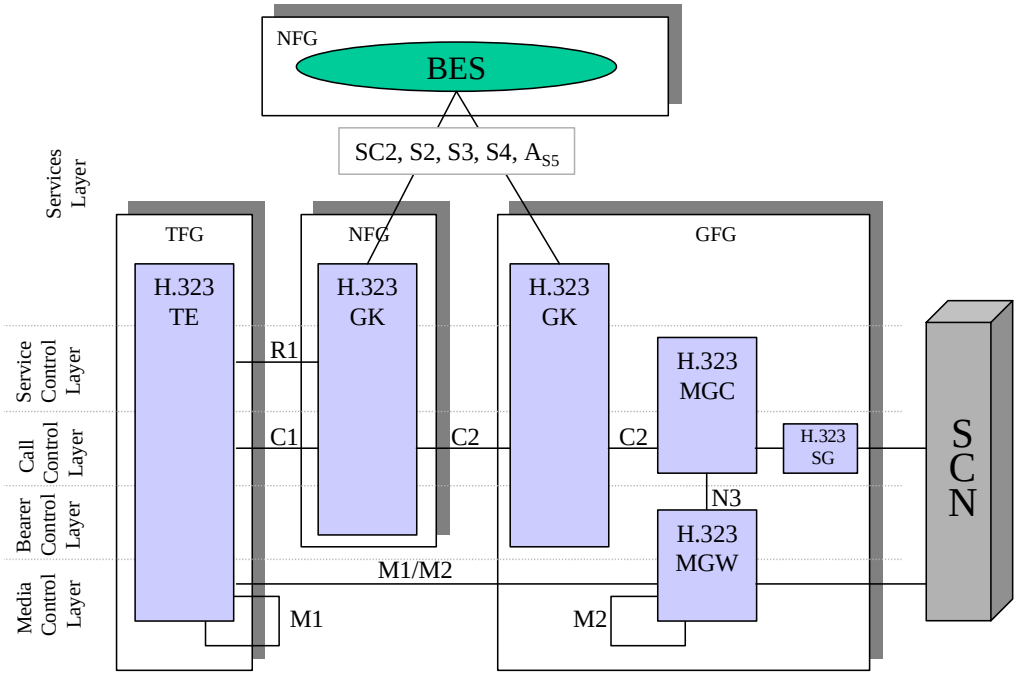
For the purposes of the present document, the following abbreviations apply:

AD-BES	Administrative Domain Back End Service
ARQ	Admission ReQuest
BES	Back End Service
CH	Clearinghouse
DEGK	Domain End Gatekeeper
DHCP	Dynamic Host Configuration Protocol
FG	Functional Group
GCF	Gatekeeper Confirm
GK	Gatekeeper
GRJ	Gatekeeper ReJect
GRQ	Gatekeeper ReQuest
GSM	Group Special Mobile
IP	Internet Protocol
ISDN	Integrated Services Digital Network
MGC	Media Gateway Controller
MGW	Media Gateway
NAT	Network Address Translation
NFG	Network Functional Grouping
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAS	Registration Admission on Status
RCF	Register ConFirm
RIP	Request In Progress
RpoA	Register point of Attachment
RRJ	Register Reject
RRQ	Register Request
SAB	Service Area Brooker
SCN	Switched Circuit Networks
SG	Signalling Gateway
SIP	Session Initiation Protocol
SpoA	Service point of Attachment
TCP	Transport Control Protocol
TE	TErminal
TRC	TIPHON Resolution Capability
UCF	Unregister ConFirm
UDP	User Datagram Protocol
UPT	Universal Personal Telecommunication
URJ	Unregister ReJect
URQ	Unregister ReQuest
VoIP	Voiceover IP

4 Implementation in the TIPHON functional architecture

ITU-T Recommendation H.323 [10] and associated suite of protocols identifies a number of entities. The present document describes the behaviour of (and the communication between) the terminal, gatekeeper and the gateway.

TS 101 314 [8] defines a number of reference points and a number of functional groups. Those reference points and functional groups need to be mapped to the ITU-T Recommendation H.323 [10] architecture before behaviours and message flows can be defined. Figure 2a shows the ITU-T Recommendation H.323 [10] entities and how they map to the functional layers defined in TS 101 314 [8] and the functional groups defined in TS 101 878 [6].



NOTE: The reference point R2 is internal to the network functional group (i.e. between H.323 gatekeepers if more than one H.323 gatekeeper is present) and not visible in the figure.

Figure 2a: The H.323 Architecture mapped to the TIPHON Functional layers and functional groups

The H.323 terminal (TE) shall provide the functionality of the terminal registration functional group, originating terminal functional group and the terminating terminal functional group. The reference points S1, SC1 and N1 are internal to the TE.

The H.323 gatekeeper (GK) shall provide the Functional Entities required in a Network Functional Group (NFG) with the exception of functional entities in the Media Control layer. Reference points S2, S3, S4, A_{S5} and SC2 may be internal to the gatekeeper, however the gatekeeper may also utilize services provided by external Service Providers using those interfaces. The GK may play the roles of an originating network functional group, an intermediate network functional group or a terminating network functional group.

The combination of an H.323 Media Gateway Controller (MGC), an H.323 Signalling Gateway (SG), an H.323 Media Gateway (MGW) and a Gatekeeper (GK) provides the functionality of the originating gateway functional group and terminating functional group. Reference points S2, S3, S4, A_{S5} and SC2 may be internal to the gatekeeper, however the gatekeeper may use these interfaces to access external service providers. The N3 reference point is out of scope of the present document.

The present document handles the R1, R2, C1 and C2 reference points.

The Registration meta-protocol (over the R1 and R2 interface) is described in clause 5.

The Call control meta-protocol (over the C1 and the C2 interface) is described in clause 6, with additional examples of message flows in the annex A.

Detailed coding requirements for H.225.0 (Q.931 and RAS) and H.245 are described annex B.

5 Registration

This clause applies to H.323 terminals and gatekeepers and describes how ITU-T Recommendation H.323 [10] and the associated suite of protocols shall be used in order to implement the Registration Meta-protocol defined in the annex A to TS 101 882.

ITU-T Recommendation H.323 [10] defines how a user registers to a gatekeeper in a Service provider's domain. The present document extends this registration procedure to also include the registration of users via another service provider's domain.

Two registration scenarios shall be supported:

- the "User at home" scenario; and
- the "Roaming user" scenario.

NOTE 1: For more details about the different registration scenarios see TS 101 315 [17].

The Registration meta-protocol defines three steps for a user to access a service application:

1) location of the Registration point of Attachment (RpoA);
2) registration; and
3) attach to the service application.

The objective with the step 1 is to locate the Registration point of Attachment. This step may be implemented using DHCP. This step is out of scope of the present document.

The step 2 is a "single sign-on" procedure where a user registers to one registrar and receives tickets for all service applications available to the user. The "single sign-on procedure is not supported by ITU-T Recommendation H.323 [10] hence out of scope of the present document.

The step 3 is the step where the users attach to a service application. In the context of the present document the service application is the VoIP service application and based on ITU-T Recommendation H.323 [10] and associated protocols.

NOTE 2: Since TIPHON uses ITU-T Recommendation H.323 [10] for the Voice over IP service application, the step 1 and step 2 is not required.

NOTE 3: The Registration meta-protocol also describes how the user shall maintain the attachment to the service application and finally how to detach from the service application.

The following clauses describes how to attach to the VoIP service application, how to maintain the attachment to the VoIP application and how to finally detach from VoIP service application.

5.1 Gatekeeper discovery

The "Single sign-on" procedure returns a Service point of Attachment (SpoA) where a user can attach to the VoIP service application. In the context of an ITU-T Recommendation H.323 [10] implementation the SpoA shall be used by the H.323 terminal to discover a gatekeeper.

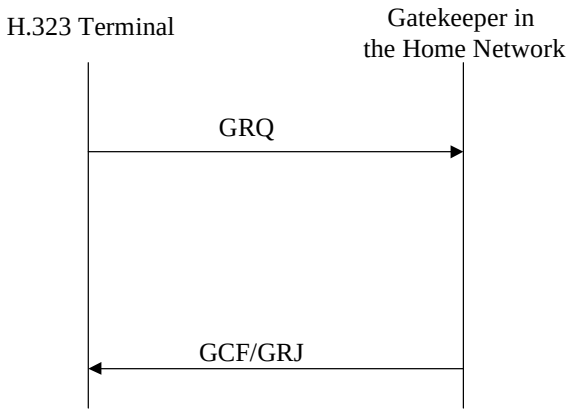
The procedures in the clause 7.2.1 of ITU-T Recommendation H.323 [10] applies with the clarifications and modifications described in this clause.

- H.323 terminals shall support automatic gatekeeper discovery procedures; and

NOTE: The automatic discovery procedures may be omitted if an address to the gatekeeper, where the user may register, is manually configured in the H.323 terminal. However, it is recommended to use automatic discovery procedure since this will make the mobility aspect of registration seamless for the user.

- Gatekeepers shall support the automatic discovery procedure allowing the H.323 terminal to use a unicast address as well as the multicast address.

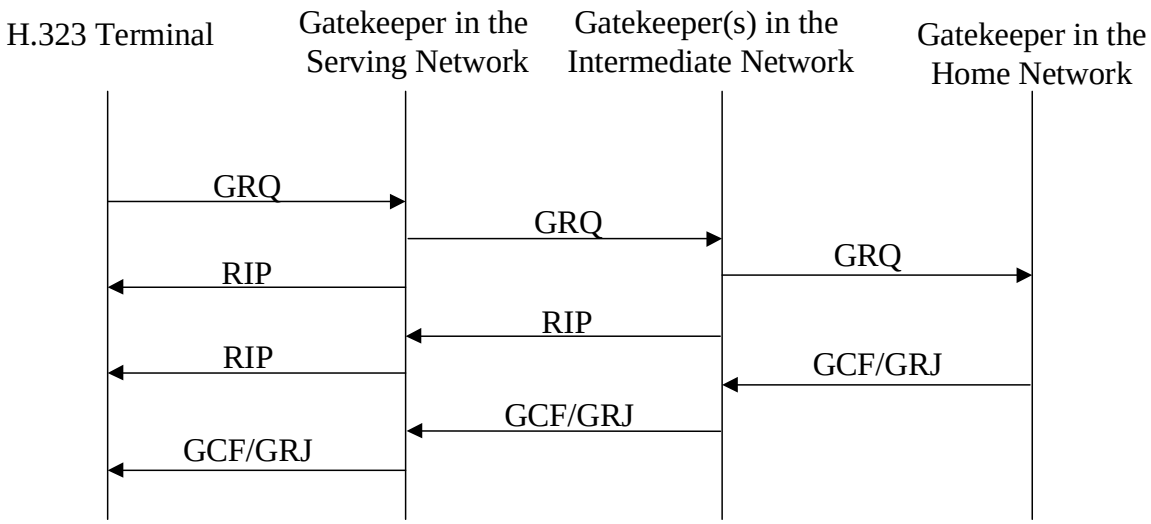
Figure 2b shows the message flow for the discovery of a gatekeeper in the "User at home" scenario (for more details regarding registration scenarios see TS 101 315 [17] where the H.323 terminal discovers the gatekeeper in the home network without involving intermediate networks.



NOTE 1: The sequence above assumes that the SpoA is known e.g. through the "Single sign-on" procedure or through manual configuration of the H.323 terminal.
NOTE 2: The coding details of the messages are described in annex B.

Figure 2b: Gatekeeper discovery in the "User at home" scenario

Figure 3 shows the message flow for the discovery of a gatekeeper in the "Roaming user" scenario (for more details regarding registration scenarios see TS 101 315 [17]) where the H.323 terminal registers to the gatekeeper in the home network via a serving network and intermediate networks acting as H.323 proxies.



NOTE 1: The sequence assumes that the SpoA is known e.g. through the "Single sign-on" procedure or through manual configuration of the H.323 terminal. The sequence also assumes that bilateral agreement exists between the different networks.
NOTE 2: The coding details of the messages are described in annex B.

Figure 3: Gatekeeper discovery in the "Roaming user" scenario

The gatekeeper discovery procedures for the H.323 terminal are described in clause 5.1.1 and in for gatekeepers in clause 5.1.2.

5.1.1 Procedures in the H.323 terminal

The procedures of this clause apply for all H.323 terminals using the automatic gatekeeper discovery procedure as defined in ITU-T Recommendation H.323 [10] clause 7.2.2 "gatekeeper discovery".

5.1.1.1 Normal procedures

The GRQ message shall be sent to the Service point of Attachment (SpoA). The SpoA may be obtained:

- by means of a "Single sign-on" procedure; or
- by manually configuration of the H.323 terminal.

NOTE 1: A manually configured address does not guarantee that the IP network is TIPHON enabled. If the IP network is not TIPHON enabled, QoS related transport service could not be guaranteed.

If neither case above applies the H.323 terminal may send a GRQ message using the multicast address defined in ITU-T Recommendation H.323 [10].

The GRQ message shall:

- include one response address in the **rasAddress** parameter;
- the **terminalInfo** parameter included in the **endpointType**;

NOTE 2: Only the **terminalInfo** parameter shall be included.

- include at least one user identity in the **endpointAlias** parameter as provided by the service provider for the purpose of registration;
- if explicit authentication is required, include a list of authentication methods in the **authentication Capability** parameter and a list of authentication algorithms in the **algorithmOID** parameter; and
- start a supervision timer supervising a response to the GRQ message and initialize the retry counter.

On receipt of RIP messages normal H.323 procedures shall apply.

On receipt of a GCF message the H.323 terminal shall store the **rasAddress** (received in the GCF message) and continue with the procedures as defined in clause 5.2.

5.1.1.2 Exceptional procedures

On receipt of a GRJ message the normal exceptional ITU-T Recommendation H.323 [10] procedure applies.

On timer expiry of the supervision timer the normal ITU-T Recommendation H.323 [10] procedure applies.

5.1.2 Procedures in the gatekeeper

An implementation of a gatekeeper may include the functions of a gatekeeper in a serving network, the functions of a gatekeeper in an intermediate network and as the functions of a gatekeeper in the home network.

If the gatekeeper has only one IP address the gatekeeper needs to understand which role it should take at the reception of a GRQ message. Figure 4 illustrates how a gatekeeper determines its role when a GRQ message is received, and a reference to the appropriate clause.

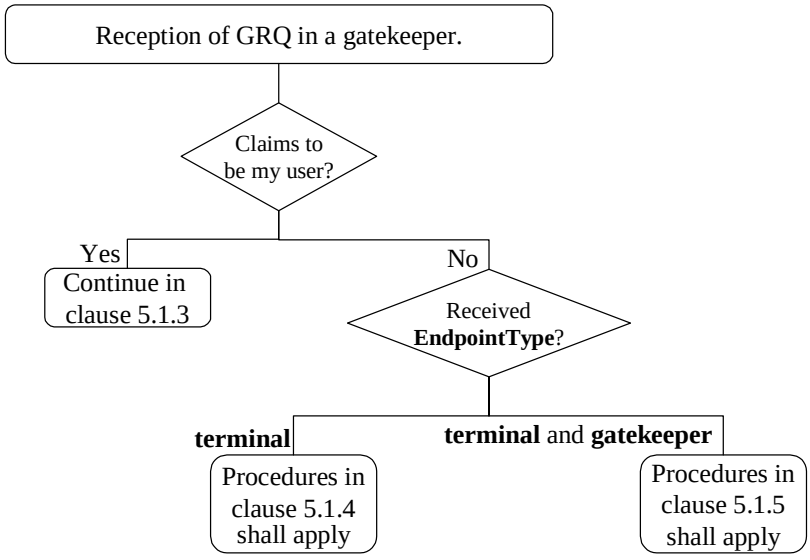


Figure 4: Decision flow for gatekeepers during gatekeeper discovery

NOTE: Another possibility is to implement gatekeepers with one dedicated task e.g. a gatekeeper in a serving network. However, the possibility to have one gatekeeper doing it all cannot be precluded.

5.1.3 Procedures in the gatekeeper in the home network

The procedures of this clause apply, see decision flow in figure 4, when a gatekeeper in the home network receives a GRQ message.

5.1.3.1 Normal procedures

On the receipt of the GRQ message the gatekeeper shall:

- verify that at least one of the user identities (received in the **endpointAlias** parameter) corresponds to one of its own subscribers to the Telephony application, see decision flow in figure 4;
- select authentication method and encryption algorithm (if explicit authentication is required or requested); and
- send a GCF message;
- the GCF message shall include the selected authentication method and encryption algorithm (if explicit authentication is required) in the **authenticationCapability** parameter and the **algorithmOID**.

5.1.3.2 Exceptional procedures

If explicit authentication is required and if no (or incompatible) authentication method and authentication algorithm was included in the GRQ, the gatekeeper in the home network shall return the GRJ message according to standard ITU-T Recommendation H.323 [10] procedures.

If the verification of the user fails, a GRJ message shall be returned with the **rejectReason** set to **securityDenial**.

5.1.4 Procedures in the gatekeeper in the serving network

The procedures of this clause apply, see decision flow in figure 4, when a gatekeeper in the serving network receives a GRQ message.

5.1.4.1 Normal procedures

On receipt of the GRQ message the gatekeeper in the serving network shall:

- select one valid user identity (from the list of) **endpointAlias** and extract the User's Service provider identity and verify that the User's Service provider is known by the gatekeeper in the serving network;

NOTE 1: A valid **endpointAlias** is an **endpointAlias** conforming to the allowed set of address formats in reference TS 101 882.

NOTE 2: The gatekeeper in the serving network may have a business agreement with an intermediate network to handle all non-recognized service providers. In this case the gatekeeper in the serving network acts as if the gatekeeper in the serving network knows the User's service provider.

- store the **rasAddress** received in the GRQ message;
- send the GRQ message towards the gatekeeper in the home network using the address stored in its internal routing tables;
- start a timer supervising a response from the home network and initialize the retry counter; and
- send a RIP message towards the H.323 terminal.

The GRQ message shall include:

- the response address to the gatekeeper in the serving network in the **rasAddress** parameter; and
- the **endpointType** parameter indicating terminal and gatekeeper.

On receipt of RIP message the gatekeeper in the serving network shall:

- forward the RIP message to the H.323 terminal; and
- reset the timer supervising a response to the GRQ message.

On the receipt of a GCF message the gatekeeper in the serving network shall:

- forward the GCF message using the stored **rasAddress** to the H.323 terminal; and
- include its own address in the **rasAddress** parameter; and
- release internal resources reserved while waiting for a response from the home network.

5.1.4.2 Exceptional procedures

In case of failure (e.g. no business agreement exists with the User's service provider) the gatekeeper shall return the GRJ message with the **rejectReason** set to **terminalExcluded**.

On expiry of the timer supervising a response to the GRQ message, the gatekeeper in the serving network shall release internal resources reserved while waiting for a response from the home network.

5.1.5 Procedures in the gatekeeper in the intermediate network

The procedures of this clause apply, see decision flow in figure 4, when a gatekeeper in an intermediate network receives a GRQ message.

5.1.5.1 Normal procedures

On receipt of the GRQ message the gatekeeper in the serving network shall:

- select one valid user identity (from the list of) **endpointAlias** and extract the User's Service provider identity and verify that the User's Service provider is known by the gatekeeper in the serving network;

NOTE 1: A valid **endpointAlias** is an **endpointAlias** conforming to the allowed set of address formats in reference TS 101 882.

NOTE 2: The gatekeeper in the intermediate network may have a business agreement with another intermediate network to handle all non-recognized service providers. In this case the gatekeeper in the intermediate network acts as if the gatekeeper in the intermediate network knows the User's service provider.

- store the **rasAddress** received in the GRQ message;
- send a RIP message towards the serving network;
- send the GRQ message towards the gatekeeper in the home network using the address stored in its internal routing tables; and
- start a timer supervising a response to the GRQ message.

The GRQ message sent by the intermediate network shall include:

- the response address to the gatekeeper in the intermediate network in the **rasAddress** parameter.

On receipt of RIP messages the gatekeeper in the Intermediate shall:

- forward the RIP message towards the serving network; and
- reset the timer supervising a response to the GRQ message.

On the receipt of the GCF message the gatekeeper in the intermediate network shall:

- forward the GCF message using the stored **rasAddress** to the serving network; and
- include its own address in the **rasAddress** parameter; and
- release internal resources reserved while waiting for a response from the home network.

5.1.5.2 Exceptional procedures

In case of failure (e.g. no business agreement exists with the User's service provider) the gatekeeper shall return the GRJ message with the **rejectReason** set to **terminalExcluded**.

On expiry of the timer supervising a response to a GRQ message the first time the gatekeeper in the serving network shall release internal resources reserved while waiting for a response from the home network.

5.2 Endpoint registration

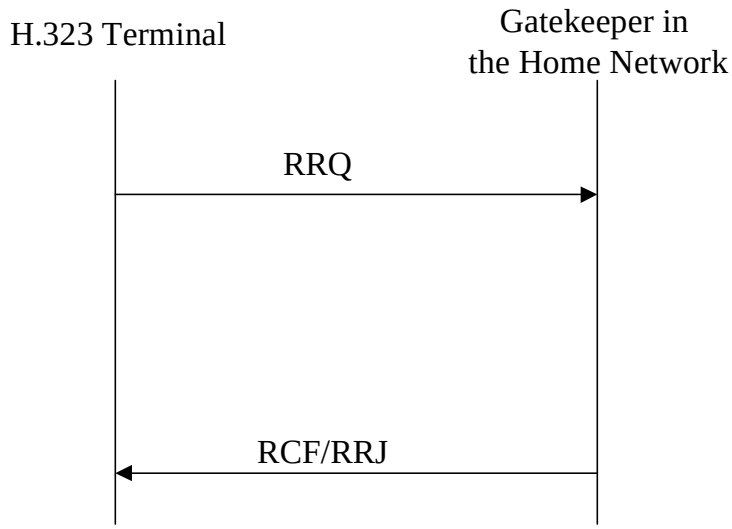
Registration shall be in accordance with ITU-T Recommendation H.323 [10] procedures with the clarifications and/or modifications described in this clause.

Two registration scenarios are identified (for more details about the registration scenarios see TS 101 315 [17]):

1) the "User at home" scenario; and

2) the "Roaming user" scenario.

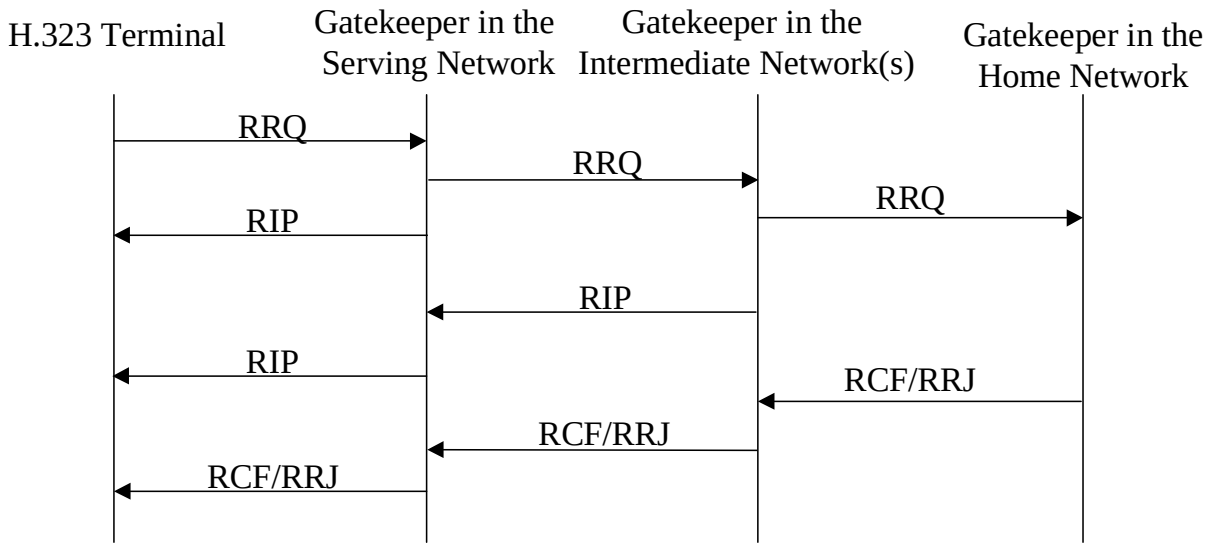
Figure 5 shows the message flow for the "User at home" scenario where the H.323 terminal registers directly to the gatekeeper in the home network without involving intermediate networks.



NOTE: The coding details of the messages are described in annex B.

Figure 5: Registration in the "User at home" scenario

Figure 6 shows the message flow for the "Roaming user" scenario where a serving network and intermediate networks acting as H.323 proxies.



NOTE: The coding details of the messages are described in annex B.

Figure 6: Registration in the "Roaming user" scenario

Clause 5.2.1 describes the procedures in the H.323 terminal and clause 5.2.2 the procedures in the gatekeeper.

5.2.1 Procedures in the H.323 terminal

The procedures in this clause apply to all H.323 terminals.

5.2.1.1 Normal procedures

The H.323 terminal shall:

- Send the RRQ message to a gatekeeper using the **rasAddress** received in the GCF message. The **rasAddress** is retrieved as described in clause 5.1.1.1 "gatekeeper discovery";

The RRQ message shall:

- Include one **callSignalAddress** parameter;
- Include one **rasAddress** parameter (where the response to the RRQ shall be sent);
- Include the **terminalType** parameter set to terminal;
- Include at least one user identity in the **endpointAlias** parameter as provided by the service provider for the purpose of registration;
- Include a value greater than 0 in the **timeToLive** parameter;
- Set the **additiveRegistration** parameter to **FALSE**; and
- If authentication is required, include a **tokens** parameter or a **cryptoTokens** parameter according to the negotiated authentication method.

The RRQ message should:

- Include the **supplyUUIEs** parameter set to FALSE;
- Not include **terminalAliasPattern**;
- Not include **usageReportingCapability**;
- Not include **callCreditCapability**; and
- Not include **capacityReportingCapability**.

NOTE 1: The above list of parameters is related to the Direct Routed Call model or parameters only intended for gateways.

All other parameters in the RRQ message shall be used as defined by ITU-T Recommendation H.323 [10].

On receipt of a RIP message normal H.323 procedures apply.

On the receipt of the RCF message the H.323 terminal shall

- Store the list of **terminalAlias** received in the message;

NOTE 2: The received list of **terminalAlias** is the result of the verification of the list of **terminalAlias** sent in the RRQ message. Some of the **terminalAlias** (in the RRQ message) may have failed verification and thus not included in the list in the RCF message. It is important to understand that only the **terminalAlias** in the RCF message may be used when establishing calls.

- Store the **timeToLive** parameter;

NOTE 3: The **timeToLive** parameter may be modified compared to the value sent in the RRQ message, however never returned in the RCF message with a **timeToLive** parameter with a value equal to 0.

- Store the **endpointIdentifier** parameter;
- Ignore the **terminalAliasPattern** parameter, the **supportedPrefixes** parameter, the **usageSpec** parameter, and the **capacityReportingSpec** parameter; and
- Start a registration timer, supervising the time the registration is valid, according to procedures in ITU-T Recommendation H.323 [10] clause 7.2.2.1 "Use of Lightweight RRQ".

5.2.1.2 Exceptional procedures

On expiry of the timer supervising a response to the GRQ message, normal H.323 procedures apply.

On receipt of a RRJ message normal H.323 procedures apply.

5.2.2 Procedures in the gatekeeper

An implementation of a gatekeeper may include the functions of a gatekeeper in a serving network, the functions of a gatekeeper in an intermediate network as well as the functions of a gatekeeper in the home network.

If the gatekeeper has only one IP address the gatekeeper needs to understand which role it should take at the reception of a RRQ message. Figure 7 illustrates how a gatekeeper determines its role, when a RRQ message is received, and a reference to the appropriate clause.

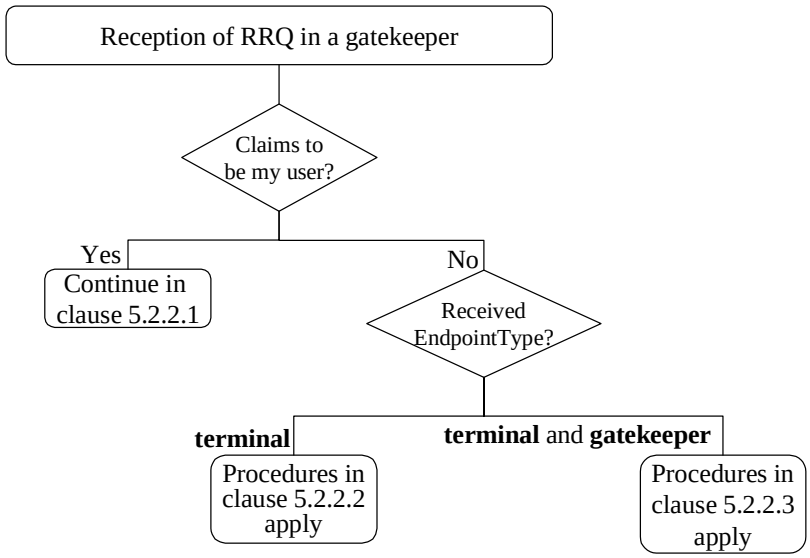


Figure 7: Decision flow in the gatekeeper during registration

NOTE: Another possibility is to implement gatekeepers with one dedicated task e.g. a gatekeeper in a serving network. However, the possibility to have one gatekeeper doing it all cannot be precluded.

The **endpointIdentifier** identifies an active registration and is generated by the gatekeeper and returned in the RCF message towards the H.323 terminal.

When more than one gatekeeper is involved in a registration each gatekeeper shall generate an **endpointIdentifier**. The generated **endpointIdentifier** shall always be included (when applicable) in messages in message towards the H.323 terminal.

If a gatekeeper receives a RCF message from a gatekeeper (which is the case for gatekeepers in the serving network and in the intermediate network) the received **endpointIdentifier** shall be stored. The stored **endpointIdentifier** shall always be included (when applicable) in messages towards the gatekeeper in the home network.

5.2.2.1 Gatekeeper in the home network

The procedures of this clause apply when a gatekeeper in the home network receives a RRQ message (see decision flow in figure 7).

5.2.2.1.1 Normal procedure

On receipt of the RRQ message the gatekeeper shall:

- Verify that the user identity corresponds to one of its subscribers to the Telephony application;
- Authenticate the user according to the negotiated (or predefined) method;
- If more than one **terminalAlias** is received all **terminalAlias** shall be validated against the User's profile and **terminalAlias** not found in the User's profile shall be discarded;
- Ignore the **supplyUUIEs**, **terminalAliasPattern**, **usageReportingCapability**, **callCreditCapability** and the **capacityReportingCapability** parameters; and
- Return a RCF message.

The RCF message shall:

- Include a **timeToLive** parameter showing the time period for which the registration is valid;
- Include a list of valid **terminalAlias**. The **terminalAlias** shall be selected among the **terminalAlias**, received in the RRQ message, and successfully validated against the User's profile; and
- Include the **preGrantedARQ** structure such that the **makeCall** parameter shall be set to **TRUE**, the **useGKCallSignalAddressToMakeCall** parameter shall be set to **TRUE**, the **answer Call** parameter shall be set to **TRUE** and the **useGLCallSignalAddressToAnswer** parameter shall be set to **TRUE**.

The RCF should:

- Not include **terminalAliasPattern** parameter;
- Not include **supportedPrefixes** parameter;
- Not include **usageSpec** parameter; or
- Not include **capacityReportingSpec** parameter;

NOTE: The parameters above belong to functions related to registration of gateways and related to the Direct Routed Call model.

- All other parameters in the RCF message shall be used as defined by ITU-T Recommendation H.323 [10].

5.2.2.1.2 Exceptional procedures

In case of unsuccessful validation of the User's identity the gatekeeper shall return a RRJ message with the **rejectReason** set to **security Denial**.

NOTE 1: The above statement implies that the gatekeeper in the home network fails to verify all of the User identities (received in **terminalAlias**), i.e. in case one of several user identities was successfully verified the case is not regarded as an exceptional case.

If additive registration is requested (only H.323 version 4) a RRJ shall be returned with the **rejectReason** set to **additiveRegistrationNotSupported**.

NOTE 2: Rejecting an additive registration does not imply that an already active registration is cancelled.

5.2.2.2 Gatekeeper in the serving network

The procedures of this clause apply when a gatekeeper in the serving network receives a RRQ message (see decision flow in figure 7).

5.2.2.2.1 Normal procedures

On the receipt of the RRQ message the gatekeeper in the serving network shall:

- Select a valid **terminalAlias** and extract the User's Service provider identity and verify that the gatekeeper in the serving network knows the User's Service provider;

NOTE: The gatekeeper in the serving network may have a business agreement with an intermediate network to handle all non-recognized service providers. In this case the gatekeeper in the serving network acts as if the gatekeeper in the serving network knows the User's service provider.

- Store the **rasAddress** and the **callSignalAddress** received in the RRQ message;
- Send a RIP message towards the H.323 terminal;
- Send the RRQ message towards the gatekeeper in the home network. The address to the gatekeeper in the home network is retrieved from routing tables internal to the gatekeeper; and
- Start a timer supervising the reception of a response to the RRQ message.

The RRQ message shall:

- Include the **terminalType** set to terminal and gatekeeper;
- Include one or more **rasAddress** and one or more **callSignalAddress** to the gatekeeper in the serving network; and
- Include all other parameters as received from the H.323 terminal.

On receipt of a RIP message from an intermediate network the gatekeeper in the serving network shall:

- Restart the timer supervising a response to the GRQ message; and
- Forward the message towards the H.323 terminal (using the stored **rasAddress**).

On the receipt of the RCF message the serving network shall:

- Store the list of **callSignalAddress** received in the RCF message;
- Store the list of **alternateGatekeeper**;
- Store the **endpointIdentifier**;
- Start a timer supervising the lifetime of the registration based on the **timeToLive** parameter received from the home network; and
- Forward the RCF message towards the H.323 terminal (using the stored **rasAddress**).

The RCF message shall:

- Include the **callSignalAddress** to the gatekeeper in the serving network; and
- Include an **endpointIdentifier** generated by the gatekeeper in the serving network.

5.2.2.2.2 Exceptional procedures

In case of unsuccessful validation of the service provider identity the gatekeeper shall return a RRJ message with the **rejectReason** set to **securityDenial**.

NOTE: The above statement implies that the gatekeeper in the serving network fails to identify a service provider in all of the user identities (received in **terminalAlias**) i.e. in case one service provider is identified in one of several user identities; the case is not regarded as an exceptional case.

On expiry of the timer supervising a reception of a response to the RRQ message the gatekeeper in the serving network shall release internal resources.

On the receipt of the RRJ message the gatekeeper in the serving network shall:

- Forward the RRJ message to the H.323 terminal (using the stored **rasAddress**); and
- Release internal resources.

5.2.2.3 Procedures in the intermediate network

The procedures of this clause apply, see decision flow in figure 7, when a gatekeeper in the intermediate network receives a RRQ message.

5.2.2.3.1 Normal procedures

On the receipt of the RRQ message the gatekeeper in the intermediate network shall:

- select a valid **terminalAlias**, extract the User's Service provider identity and verify that the User's Service provider is known by the gatekeeper in the intermediate network;

  NOTE: The gatekeeper in the intermediate network may have a business agreement with another intermediate network to handle all non-recognized service providers. In this case the gatekeeper in the intermediate network acts as if the gatekeeper in the intermediate network knows the User's service provider.

- store the list of **rasAddress** and the list of **callSignalAddress** received in the RRQ message;
- send the RRQ message towards the gatekeeper in the home network. The address is retrieved from routing tables internal to the gatekeeper;
- start a timer supervising a response to the RRQ message; and
- send a RIP message towards the serving network (using the stored **rasAddress**).

The RRQ message shall:

- include one or more **rasAddress** and one or more **callSignalAddress** to the gatekeeper in the intermediate network;
- include all other parameters (as received from the serving network).

On receipt of a RIP message from an intermediate network the gatekeeper in the intermediate network shall:

- restart the timer supervising a response to the GRQ message; and
- forward the message towards the serving network (using the stored **rasAddress**).

On the receipt of the RCF message the gatekeeper in the intermediate network shall:

- store the list of **callSignalAddress** received in the RCF message;
- store the list of **alternateGatekeeper**;
- store the **endpointIdentifier** parameter;
- forward the RCF message towards the serving network (using the stored **rasAddress**); and
- start a timer supervising the lifetime of the registration based on the **timeToLive** parameter received from the home network.

The RCF message shall:

- include one or more **callSignalAddress** to the gatekeeper in the intermediate network;
- include an **endpointIdentifier** generated by the gatekeeper in the intermediate network; and
- include all other parameters received from the home network.

5.2.2.3.2 Exceptional procedures

In case of unsuccessful validation of the service provider identity the gatekeeper shall return a RRJ message with the **rejectReason** set to **securityDenial**.

NOTE: The above statement implies that the gatekeeper in the intermediate network fails to identify a service provider in all of the user identities (received in **terminalAlias**), i.e. in case one service provider is identified in one of several user identities; the case is not regarded as an exceptional case.

On expiry of the timer supervising a reception of a response to the RRQ message the gatekeeper in the serving network shall release internal resources.

On the receipt of the RRJ message the gatekeeper in the serving network shall:

- forward the RRJ message to the H.323 terminal (using the stored **rasAddress**); and
- release internal resources.

5.3 Cancelling the registration

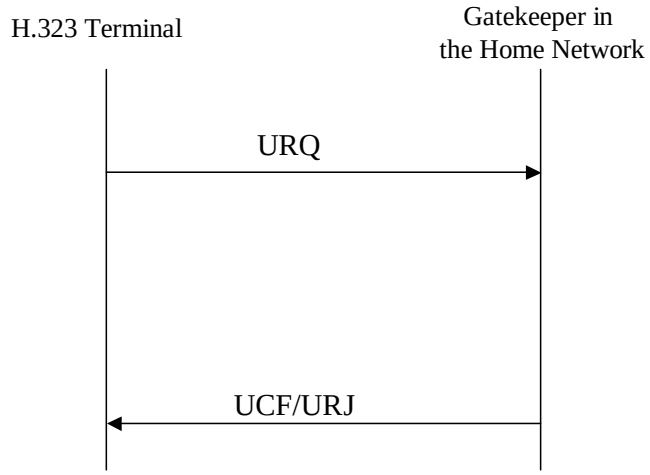
The H.323 terminal, the gatekeeper in a serving network, any gatekeeper in the intermediate network or the home network may cancel a registration.

The set of user identities received in the RCF message is the complete set of user identities for which the registration is valid. A subset of the complete set of user identities may be cancelled. In this case the URQ message includes a list of **endpointAlias** indicating which user identities that the registration shall cease to be valid for.

As long as any of the user identities in the complete set of user identities are active (i.e. not sent in for cancellation) the registration (identified by the **endpointIdentifier**) shall be regarded as active.

The reception of an URQ message without **endpointAlias** shall be interpreted as " cancel all user identities associated with the registration identified by the **endpointIdentifier**".

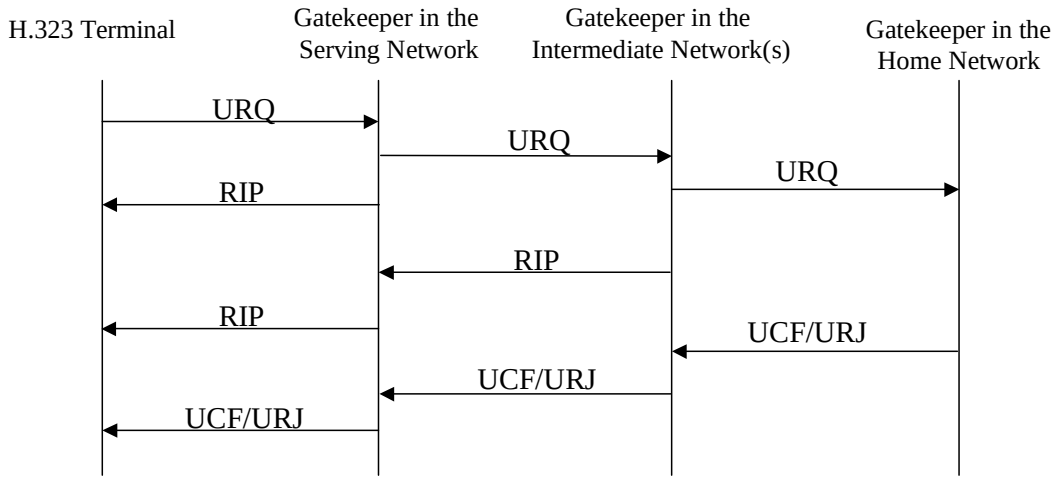
Figure 8 shows the message flow for the "User at home" scenario when the H.323 terminal cancels a registration.



NOTE: The coding details of the messages are described in annex B.

Figure 8: Cancelling the registration in the "User at home" scenario

Figure 9 shows the message flow for the "Roaming user" scenario where a serving network and intermediate networks acting as H.323 proxies.



NOTE: The coding details of the messages are described in annex B.

Figure 9: Cancelling the registration in the "Roaming user" scenario

5.3.1 Procedures in the H.323 terminal

The procedures in the following clauses shall apply for all H.323 terminals.

5.3.1.1 URQ message sent by the H.323 terminal

5.3.1.1.1 Normal case

The cancelling of a registration shall follow the procedures defined in clause 7.2.2 "Endpoint registration" of ITU-T Recommendation H.323 [10] with the following clarifications.

The H.323 terminal shall:

- release all active calls (originating from or terminating to any of the user identities for which the H.323 terminal wants to cancel the registration);
- send the URQ message towards the home network; and
- start a timer supervising a response to the URQ message.

The URQ message shall include:

- the list of **endpointAlias** for which the registration shall be cancelled; or
- no **endpointAlias** if registration for all user identities associated with the registration shall be cancelled.

On receipt of the UCF or on the receipt of the URJ message the H.323 terminal shall regard all user identities included in the URQ message as unregistered.

5.3.1.1.2 Exceptional case

If no response to the URQ message is received (the supervision timer expires), the H.323 terminal shall retransmit the URQ message.

If no response to the retransmitted URQ is received, the H.323 terminal shall regard the user identities sent in the URQ message as unregistered.

5.3.1.2 URQ message received from the network

At the reception of a URQ from the network (it can be either a serving network or a home network directly depending on scenario) the H.323 shall:

- initiate release for all active calls associated with the user identities in the **endpointAlias** parameter;
- respond with a UCF; and
- release internal resources.

5.3.2 Gatekeeper in the home network

The procedures in the following clauses shall apply for the gatekeeper in the home network.

5.3.2.1 URQ message sent by the gatekeeper in the home network

5.3.2.1.1 Normal procedure

Standard procedures according to clause 7.2.2 "End point registration" of ITU-T Recommendation H.323 [10] with the following clarifications applies:

- All calls, involving the registered user, shall be released before the gatekeeper in the home network sends the URQ message.

NOTE: Calls not involving the H.323 terminal (e.g. forwarded calls) are not affected unless the reason for the gatekeeper to cancel the registration is that the gatekeeper is closing down (e.g. for maintenance), the User's subscription is cancelled, the User's pre-paid account is empty, etc.

The URQ message sent to towards the H.323 terminal shall:

- include all user identities, for which the gatekeeper in the home network wants to cancel the registration, in the list of **endpointAlias**;
- the gatekeeper in the home network shall supervise the reception of a response to the URQ message.

On receipt of a RIP message the normal H.323 procedure apply.

On receipt of the UCF the gatekeeper shall regard the User as unregistered and release all internal resources.

5.3.2.1.2 Exceptional procedure

When no response is received on the URQ message the gatekeeper in the home network shall retransmit the URQ message.

When no response on the retransmitted URQ message is received the gatekeeper shall regard the user identities sent in the URQ message as unregistered and release all internal resources.

5.3.2.2 URQ message received from the H.323 terminal, from the gatekeeper in the serving network or from gatekeepers in intermediate networks

On receipt of the URQ message the gatekeeper in the home network shall:

- initiate clearing of all active calls to and from the H.323 terminal involving any of the user identities in the list of **endpointAlias** received in the URQ message;
- regard all user identities (received in the list of **endpointAlias** in the URQ message) as unregistered;
- return an UCF message if at least one of the user identities (received in the list of **endpointAlias** in the URQ message) was registered; and
- return an URJ message with the **rejectReason** set to **userCurrentlyNotRegistered** if none of the user identities was registered.

Calls not involving the H.323 terminal (e.g. forwarded calls) shall not be cleared.

5.3.3 Gatekeeper the serving network

The procedures in this clause shall apply for the gatekeeper in the serving network.

5.3.3.1 URQ message initiated by the H.323 terminal

5.3.3.1.1 Normal procedures

On receipt of the URQ message from the H.323 terminal the gatekeeper in the serving network shall:

- store the list of **terminalAlias** received in the URQ message;
- include the **endpointIdentifier** received in the RCF message from the home network during registration;
- send the URQ message towards the gatekeeper in the home network using the same address to where the RRQ message was sent; and
- start a timer supervising the reception of a response to the URQ message.

The URQ message towards the home network shall include the **endpointIdentifier** received from the gatekeeper in the home network during registration.

On receipt of the UCF message from the home network the gatekeeper in the serving network shall:

- regard all user identities (received in the URQ) message as unregistered;
- forward the UCF message towards the H.323 terminal (using the **rasAddress** stored during the registration); and
- remove the user identities from the list of user identities received in the RCF message from the home network during the registration and if no more user identities remain, release all internal resources.

5.3.3.1.2 Exceptional procedures

When no response is received on the URQ message the gatekeeper in the serving network shall retransmit the URQ message.

When no response on the retransmitted URQ message is received the gatekeeper in the serving network shall regard the registration as no longer active.

On receipt of a URQ message where no active registration (identified by the **endpointIdentifier** parameter) exists the gatekeeper in the serving network shall return a RRJ message with the **rejectReason** set to **notCurrentlyRegistered**.

5.3.3.2 URQ message initiated by the home network or an intermediate network

5.3.3.2.1 Normal procedure

On receipt of the URQ message from the home network the gatekeeper in the serving network shall:

- store the list of **terminalAlias** received in the URQ message and forward the URQ message towards the H.323 terminal using the **rasAddress** stored during registration;
- initiate clearing of calls involving any of the user identities in the list of **terminalAlias** (or for all user identities valid for the registration if no list of **terminalAlias** was received); and
- start a timer supervising a response to the URQ message.

The URQ message towards the H.323 terminal shall include the **endpointIdentifier** generated by the gatekeeper in the intermediate network during registration.

On receipt of the UCF message from the H.323 terminal the gatekeeper in the serving network shall:

- regard all user identities (received in the URQ) message as unregistered;
- send the UCF message towards the gatekeeper in the home network. The address is retrieved from routing tables internal to the gatekeeper; and
- remove the user identities from the list of user identities received in the RCF message from the home network during the registration and if no more user identities remain, release all internal resources.

5.3.3.2.2 Exceptional procedure

When no response is received on the URQ message the gatekeeper in the serving network shall retransmit the URQ message.

When no response on the retransmitted URQ message is received the gatekeeper in the serving network shall regard the registration (this is independent of the URQ only cancelled a subset of the user identities valid for the registration or not) as no longer active.

5.3.3.3 URQ message initiated by the gatekeeper in the serving network

5.3.3.3.1 Normal procedure

The gatekeeper may cancel the registration due to internal maintenance reasons or due to a registration time out reason.

The gatekeeper shall:

- send the URQ message towards the H.323 terminal and towards the home network;
- towards the home network: Include the same **endpointIdentifier** received in the RCF message from the home network during registration;
- towards the H.323 terminal: Include the **endpointIdentifier** generated by the gatekeeper in the serving network during registration; and
- start a timer supervising the reception of responses to the URQ message.

On the receipt of a response (it may be either the UCF message or the URJ message) from both the H.323 terminal and the home network internal resources may be cleared.

5.3.3.3.2 Exceptional procedure

On expiry of the timer supervising responses to the URQ message the gatekeeper in the serving network shall retransmit the URQ message.

On timer expiry of the retransmitted URQ message internal resources may be cleared.

5.3.4 Gatekeeper the intermediate network

The procedures in this clause shall apply for the gatekeeper in the intermediate network.

5.3.4.1 URQ message initiated by the H.323 terminal or the serving network

5.3.4.1.1 Normal procedure

On receipt of the URQ message from the H.323 terminal the gatekeeper in the intermediate network shall:

- store the list of **terminalAlias** received in the URQ message;
- include the **endpointIdentifier** received from the gatekeeper in the home network during registration;
- send the URQ message towards the gatekeeper in the home network (using the same address to where the RRQ was sent); and
- start a timer supervising the reception of a response to the URQ message.

On receipt of the UCF message from the home network the gatekeeper in the intermediate network shall:

- regard all user identities (received in the URQ) message as unregistered;
- forward the UCF message towards the serving network (using the **rasAddress** stored during the registration); and
- remove the user identities from the list of user identities received in the RCF message from the home network during the registration and if no more user identities remain, release all internal resources.

5.3.4.1.2 Exceptional procedures

When no response is received on the URQ message the gatekeeper in the intermediate network shall retransmit the URQ message.

When no response on the retransmitted URQ message is received the gatekeeper in the intermediate network shall regard the registration as no longer active (this is independent of the URQ only cancelled a subset of the user identities valid for the registration or not).

On receipt of a URQ message where no active registration (identified by the endpointIdentifier parameter) exists the gatekeeper in the intermediate network shall return a RRJ message with the rejectReason set to **notCurrentlyRegistered**.

5.3.4.2 URQ message initiated by the home network or the serving network

5.3.4.2.1 Normal procedure

On receipt of the URQ message from the home network the gatekeeper in the intermediate network shall:

- store the list of **terminalAlias** received in the URQ message and forward the URQ message towards the serving network using the **rasAddress** stored during registration;
- include the same **endpointIdentifier** received in the RRQ message from the serving network during registration towards the serving network;
- send the URQ message towards the serving network (using the **rasAddress** stored during registration); and
- start a timer supervising a response to the URQ message.

On receipt of the UCF message from the H.323 terminal the gatekeeper in the intermediate network shall:

- regard all user identities (received in the URQ) message as unregistered;
- send the UCF message towards the gatekeeper in the serving network; and
- remove the user identities from the list of user identities received in the RCF message from the home network during the registration and if no more user identities remain, release all internal resources.

5.3.4.2.2 Exceptional procedure

When no response is received on the URQ message the gatekeeper in the intermediate network shall retransmit the URQ message.

When no response on the retransmitted URQ message is received the gatekeeper in the intermediate network shall regard the registration as no longer active.

5.3.4.3 URQ message initiated by a gatekeeper in the intermediate network

5.3.4.3.1 Normal procedure

The gatekeeper may cancel the registration due to internal maintenance reasons or due to a registration time out reason.

The gatekeeper shall:

- send the URQ message towards the serving network and towards the home network;
- towards the home network: Include the same **endpointIdentifier** received in the RCF message from the home network during registration;
- towards the serving network: Include the **endpointIdentifier** generated by the gatekeeper in the intermediate network during registration; and
- start a timer supervising the reception of responses to the URQ message.

On the receipt of a response (it may be either the UCF message or the URJ message) from both the H.323 terminal and the home network internal resources may be cleared.

5.3.4.3.2 Exceptional procedure

On expiry of the timer supervising responses to the URQ message the gatekeeper in the intermediate network shall retransmit the URQ message.

On timer expiry of the retransmitted URQ message internal resources may be cleared.

5.4 Use of Lightweight RRQ

The procedures in this clause apply for H.323 terminals, the gatekeeper in the home network, intermediate network and the gatekeeper in the serving network.

NOTE: TS 101 315 [17] defines a "Single sign-on" procedure. The "Single sign-on" procedure returns a ticket for each service that the user is authenticated for (by the "Single sign-on" procedure). Tickets have a time limitation. Before the limited time expires the user needs to contact the "Single sign-on" registrar in order to reset the "service timers". When the user is authenticated to use a service e.g. VoIP the user shall attach to the service.

The time a user is attached to a service is dependent on the service (and the technology use to attach to the service). ITU-T Recommendation H.323 [10] defines a procedure for revoking the time the user is attached. The procedures is called "Lightweight RRQ" and defined in clause 7.2.2.1 "Use of Lightweight RRQ" of ITU-T Recommendation H.323 [10].

The following clauses describe the behaviour in the H.323 terminal, the gatekeeper in the serving network, the gatekeeper in the intermediate network and the gatekeeper in the home network.

5.4.1 Procedures in the H.323 terminal

The H.323 terminal shall use the Lightweight RRQ procedure as defined in clause 7.2.2.1 "Use of Lightweight RRQ" of ITU-T Recommendation H.323 [10] with the following clarification:

- It is recommended that the H.323 terminal send the lightweight RRQ message before the timer supervising the registration expires.

5.4.2 Gatekeeper in the home network

5.4.2.1 Normal procedure

The gatekeeper in the home network shall use the Lightweight RRQ procedures as defined in clause 7.2.2.1 "Use of Lightweight RRQ" in ITU-T Recommendation H.323 [10].

5.4.2.2 Exceptional procedure

On expiry of the registration supervision timer the gatekeeper in the home network shall cancel the registration according to clause 5.3.2.

5.4.3 Gatekeeper in the serving network

The gatekeeper in the serving network shall support the Lightweight RRQ procedure**.**

NOTE: This clause is only a complement to clause 5.2.2.2 with the focus on the Lightweight RRQ. Consequently clause 5.2.2.2 shall be used together with this clause for the full understanding of procedures in the serving network.

5.4.3.1 Normal procedure

On receipt of the RRQ message for and active registration (identified by the **endpointIdentifier**) the gatekeeper in the serving network shall:

- send the RRQ message towards the gatekeeper in the home network. The address is retrieved from routing tables internal to the gatekeeper.

The RRQ message shall:

- include the **endpointIdentifier** generated by the serving network during the registration; and
- include all other parameters received in the RRQ message.

On receipt of the RCF message from the home network the gatekeeper in the serving network shall:

- restart the timer supervising the time the registration is valid; and
- forward the RCF message to the H.323 terminal (using the **rasAddress** stored during the registration).

On receipt of a RIP message the RIP message shall be sent to the H.323 terminal (using the stored **rasAddress**).

5.4.3.2 Exceptional behaviour

On receipt of a RRJ message the gatekeeper in the serving network shall:

- send the RRJ message to the H.323 terminal;
- release internal resources.

On receipt of a RRQ message with an endpointIdentifier not corresponding to an active registration the gatekeeper in the serving network shall return the RRJ message.

On timer expiry of the registration time the gatekeeper in the serving network shall cancel the registration according to the procedure in clause 5.3.3.

5.4.4 Gatekeeper in the intermediate network

The gatekeeper in the intermediate network shall support the Lightweight RRQ procedure.

NOTE: This clause is only a complement to clause 5.2.2.3 with the focus on the Lightweight RRQ. Consequently clause 5.2.2.3 shall be used together with this clause for the full understanding of procedures in the intermediate network.

5.4.4.1 Normal procedure

On receipt of the RRQ message for and active registration (identified by the endpointIdentifier) the gatekeeper in the serving network shall:

- send the RRQ message towards the gatekeeper in the home network. The address is retrieved from routing tables internal to the gatekeeper.

The RRQ message shall:

- include the endpointIdentifier generated by the intermediate network during the registration; and
- include all other parameters received in the RRQ message.

On receipt of the RCF message from the home network the gatekeeper in the intermediate network shall:

- restart the timer supervising the time the registration is valid; and
- forward the RCF message to the serving network (using the rasAddress stored during the registration).

On receipt of a RIP message the RIP message shall be sent to the H.323 terminal (using the rasAddress stored during the registration).

5.4.4.2 Exceptional behaviour

On receipt of a RRJ message the gatekeeper in the intermediate network shall:

- send the RRJ message to the serving network;
- release internal resources.

On receipt of a RRQ message with an endpointIdentifier not corresponding to an active registration the gatekeeper in the intermediate network shall return the RRJ message.

On timer expiry of the registration time the gatekeeper in the intermediate network shall cancel the registration according to the procedure in clause 5.3.4.

6 Call connectivity

This clause describes the mapping of the H.225.0 (ITU-T Recommendation Q.931 [15]) protocol to the Call control meta-protocol as defined in TS 101 882.

The concept of functional groups are developed and described in TS 101 878 [6]. In the present document the behaviour of the following functional groups are described:

- an originating terminal functional group;
- a serving network functional group serving either the calling party or the called party;
- an intermediate functional group between the serving network and the home network the for either the calling party or the called party;
- a home network functional group acting as home for either the calling party or the called party;
- an originating gateway functional group;
- an intermediate network functional group; and
- a terminating gateway connecting terminals in the SCN.

The above functional groups may be combined to form different use cases.

NOTE: One example of a use case may be when an originating gateway functional group is combined with a home network functional group (for the "calling" party), a serving network functional group (for the called party) and a terminating terminal functional group. This combination describes the behaviour of H.323 entities for a call from a user in the SCN to a roaming user connected to the IP network.

From a protocol point of view the behaviour in some of those functional groups performs the same task:

- a gatekeeper in an intermediate network, for the calling party shall implement the same behaviour as the gatekeeper in the serving network for the calling party; and
- a gatekeeper in an intermediate network, for the called party, shall implement the same behaviour as the gatekeeper in the serving network for the called party.

6.1 General behaviour

The following clauses describe the behaviour applicable for all functional groups.

6.1.1 Error handling

The present document describes a profile that mandates certain optional parts of ITU-T Recommendation H.323 [10], ITU-T Recommendation H.225.0 [11] and ITU-T Recommendation H.245 [12] and does not mandate certain other options.

If an information element or parameter is received, which is not within the context of the present document, the receiver shall ignore the information element or parameter and act as if the information element or parameter were not received.

If a message is received, which is not within the context of the present document, the receiver shall send an appropriate error message and ignore the message.

If a message is received with a mandatory information element or parameter missing, the receiver shall act as if the information element was received carrying a default value, or reject with the appropriate error message if there is no default value specified in the corresponding ITU-T Recommendation.

If an information element or parameter is received with syntactically invalid contents, e.g. wrong use of the extension bit mechanism, the receiver shall:

- if the information element or parameter is optional, ignore the information element or parameter; or
- if the information element or parameter is mandatory, act as if the information element or parameter was received correctly coded carrying the default values, or reject with an appropriate error message if there is no default value specified in the standard.

If an information element or parameter is received with a value not allowed within the context of the present document, the receiver shall:

- if the information element or parameter is optional, pass on, but otherwise ignore the information element or parameter; or
- if the information element or parameter is mandatory reject with an appropriate error message.

NOTE: The security policy of an operator's network or the security policy implemented in a network element may override the error handling as described above.

6.1.2 Timers

All entities in a TIPHON compliant network shall implement the timers defined in ITU-T Recommendation H.323 [10] with the following additions/clarifications:

- Timer T301 shall be implemented to supervise the reception of a CONNECT message. The timer is started/restarted at the reception of the messages: CALL PROCEEDING, FACILITY, PROGRESS and ALERTING. The timer is stopped when the CONNECT message is received.

The recommended value for this timer is 3 minutes.

- Timer T302 shall be implemented to supervise the reception of a complete E.164 number. The timer is started when an incomplete E.164 (type) number is received. The timer is restarted when additional information is received and stopped when a complete number is received.

The recommended value for this timer is 5-15 seconds. The lower value is recommended when many digits have been received and the higher value when few digits have been received.

- Timer T303 shall be implemented to supervise the first response to the SETUP message. The timer is started when the SETUP message is sent and stopped at the receipt of the first response message.

Recommended value for this timer is 4 seconds.

6.2 Originating terminal functional group

The procedures in this clause apply to all H.323 terminals originating calls.

6.2.1 Call establishment

Calls shall be setup using the procedures defined in ITU-T Recommendation H.323 [10] with the changes/clarifications in this clause.

The H.323 terminal shall:

- use the gatekeeper routed model;
- implement en-bloc procedure according to the procedures in clause 6.2.1.1 of the present document;
- implement overlap procedure according to the procedures in clause 6.2.1.2 of the present document;
- implement the fast connect procedure described in ITU-T Recommendation H.323 [10], clause 8.1.7;
- encapsulate messages according to clause 8.2.1 of ITU-T Recommendation H.323 [10]; and
- implement timers according to the clause 6.1.2 of the present document.

6.2.1.1 En-bloc Procedure

The H.323 terminal shall indicate that the en-bloc procedure is used in at least one of the following way:

- include the **canOverlapSend** parameter in the SETUP message and set the value to **FALSE**; or

NOTE: By not including the parameter, the value **FALSE**, will be assumed by the network.

- include the *Sending complete* information element in the SETUP message.

6.2.1.2 Overlap sending

The overlap sending procedure shall be used to deliver additional called party identifier information. The overlap sending procedure shall only be used for E.164 identifiers.

The SETUP messages shall:

- include the parameter **canOverlapSend** set to **TRUE**; and
- include the *called party number* information element with at least one digit in the SETUP message.

On receipt of the SETUP ACKNOWLEDGE message the H.323 terminal shall send additional information in the INFORMATION message.

The H.323 terminal may indicate that the information is complete by including a *Sending complete* information element in an INFORMATION message.

6.2.2 Active phase

The active phase of a call shall commence in the H.323 terminal when the called party answers and as a result an H.323 CONNECT message is received.

6.2.3 Call release

In the H.323 terminal calls shall be cleared according to the procedures in ITU-T Recommendation H.323 [10].

6.2.4 Exceptional behaviour

If timer T301 or T303 expires the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **unknownReason** towards the originating network.

If timer T302 expires the H.323 terminal shall regard the called party number as complete and start timer T301.

6.3 Serving and intermediate network functional group for the calling party

This clause describes the behaviour in the serving network and in the intermediate network(s).

The following principles applies for a gatekeeper in the serving network or in an intermediate network:

- the gatekeeper shall act as an H.323 proxy;
- the gatekeeper may communicate with a firewall in order to open ports for the media. The communication between the gatekeeper and the firewall is out of scope of the present document;
- the gatekeeper shall apply policies for the information that shall be transferred between the H.323 terminal and the home network;
- the gatekeeper may communicate with routers in the Transport network in order to apply QoS policies in accordance with agreements between the serving network and the home network or policies between the intermediate network and the home network. The communication between the gatekeeper and the router is out of scope of the present document.

The following general rule apply:

- the gatekeeper shall use the gatekeeper routed call model as defined in in ITU-T Recommendation H.323 [10], clause 7.3.1. The call signalling channel shall be kept open during the duration of the call;
- the gatekeeper shall forward all H.225.0 messages from the H.323 terminal towards the home network;
- the gatekeeper shall forward all H.225.0 messages from the home network towards the H.323 terminal;
- the gatekeeper shall support the fast connect procedure described in clause 8.1.7 of ITU-T Recommendation H.323 [10];
- the gatekeeper shall support encapsulation of H.245 messages within H.225.0 messages according to clause 8.2.1 of ITU-T Recommendation H.323 [10];
- the gatekeeper shall support timer T301, T302 and T303 according to the clause 6.1.2.

Clarifications to the above general rule are described in the following clauses.

6.3.1 Call establishment

On receipt of a SETUP message the gatekeeper shall:

- establish a TCP connection with the H.323 home network (or with the intermediate network if an intermediate network is involved) using the **callSignalAddress** stored during registration;

NOTE: For implementations using H.323 version 3 or later the connection type may be negotiated during registration, e.g. using a simple TCP connection, a multiplex TCP connection or UDP.

- if the message includes a *Sending complete* information element or if the **canOverlapSend** parameter is set to **FALSE**, send a CALL PROCEEDING message towards the H.323 terminal;
- if the message includes the **canOverlapSend** parameter set to **TRUE** and no *Sending complete* information element is included in the message, return a SETUP ACKNOWLEDGE message towards the H.323 terminal;
- send the SETUP message towards the home network (using the TCP connection as described above).

On receipt of a SETUP ACK message from the home network the message shall not be forwarded to the H.323 terminal.

On receipt of the INFORMATION message from the H.323 terminal the gatekeeper shall:

- if the message includes the *Sending Complete* information element send a CALL PROCEEDING towards the H.323 terminal; and
- send the INFORMATION message towards the home network.

On receipt of the CALL PROCEEDING message from the home network the gatekeeper shall forward the message towards the H.323 terminal if the CALL PROCEEDING message is not sent before.

On receipt of a PROGRESS, a FACILITY, an ALERTING or a CONNECT message from the home network the gatekeeper shall forward the message towards the H.323 terminal.

6.3.2 Active phase

The active phase commences in the serving network and in the intermediate network when the called party answers and a CONNECT message is received as a result.

6.3.3 Call release

On receipt of the RELEASE COMPLETE message from the home network or from the H.323 terminal the gatekeeper shall:

- stop any running timer;
- release all resources reserved for the call; and
- forward the message towards the H.323 terminal or towards the home network depending on from where the message was received.

6.3.4 Exceptional behaviour

If a connection could not be establish with the home network the call shall be released with the **releaseCompleteReason** set to **unreachableDestination**.

If timer T303 expires the call shall be cleared with the released with the **releaseCompleteReason** set to **unreachableDestination** towards the H.323 terminal.

If timer T302 expires the called party number shall be regarded to be complete and the gatekeeper shall send a CALL PROCEEDING message sent towards the H.323 terminal.

If timer T301 expires the call shall be cleared with the **releaseCompleteReason** set to **undefinedReason** in both directions.

6.4 Home network functional group for the calling party

The procedures in this clause apply for all gatekeepers in the home network.

The following general principle applies:

- the gatekeeper in the home network for the calling party shall act as a gatekeeper as defined in ITU-T Recommendation H.323 [10];
- the gatekeeper in the home network for the calling party shall provide services based on the user's subscription;
- the gatekeeper in the home network shall apply policies based on the user's subscription e.g. limiting bandwidth usage by modifying the contents of call control or media control messages; and
- the gatekeeper in the home network may apply other policies based on agreements between the home network and an intermediate network or based on agreements between the home network and the serving network.

6.4.1 Call establishment

Calls shall be setup using the procedures defined in ITU-T Recommendation H.323 [10] with the following changes/clarifications:

- the gatekeeper shall use the gatekeeper Routed call model as defined in clause 7.3.1 of ITU-T Recommendation H.323 [10]. The call signalling channel shall be kept open during the duration of the call;
- the gatekeeper shall support the timer T301, T302 and T303 according to the clause 6.1.2 of the present document;
- the gatekeeper shall support the en-bloc and overlap procedure as defined in clauses 6.4.1.1 and 6.4.1.2 of the present document;
- the gatekeeper shall support the fast connect procedure described in clause 8.1.7 of ITU-T Recommendation H.323 [10];
- the gatekeeper shall support encapsulation of H.245 messages within H.225.0 messages according to clause 8.2.1 of ITU-T Recommendation H.323 [10].

6.4.1.1 En-bloc procedure

Use of the en-bloc procedure may be explicitly indicated in the signalling from the H.323 terminal. The en-bloc procedure shall also be used whenever the gatekeeper can regard the called party number in the SETUP message as complete.

A called party number can be regarded to be complete under the following conditions:

- if the gatekeeper in the home network has the full knowledge about the numbering plan in use in the called party's network and can identify the number to be complete;
- if the SETUP message contains the Sending complete information element;
- if the **canOverlapSend** parameter is absent or set to **FALSE**; or
- if the called party number contains the "#" character as the last digit.

If the gatekeeper in the home network determines that a CALL PROCEEDING message shall be returned to the serving network, the "sending complete" information element shall be inserted, if not already there, in the SETUP message or INFORMATION message being sent towards the terminating network.

6.4.1.2 Overlap procedure

The overlap sending procedure shall be used to request and deliver additional called party identifier information. The overlap sending procedure may only be used for E.164 identifiers.

On receipt of a SETUP message with a called party number that the gatekeeper in the home network cannot determine to be complete, the gatekeeper shall

- return a SETUP ACKNOWLEDGE message to the terminal; and
- if next hop address can be determined using the received digits, send the SETUP message towards the terminating network.

Additional information shall be provided by the H.323 terminal and transferred by means of the INFORMATION message.

If the SETUP message was sent towards the terminating network prior to the reception of the INFORMATION message the received INFORMATION message shall be forwarded towards the terminating network.

If the SETUP message was not sent, the gatekeeper shall use the received information to determine the next hop address and (if the next hop address can be determined) the gatekeeper shall send the SETUP message towards the terminating network including all digits that is received so far.

6.4.2 Active phase

The active phase of the call shall commence when the called party answers and the gatekeeper in the home network receives the CONNECT message as a result. The gatekeeper in the home network shall pass on the CONNECT message towards the H.323 terminal.

6.4.3 Call release

In the gateway and in the gatekeeper calls shall be cleared according to the procedures in ITU-T Recommendation H.323 [10].

6.4.4 Exceptional procedures

NOTE: The procedures in this clause do not preclude implementation dependent solutions to resolve the situation i.e. selecting a new route.

When a *Sending complete* information element is received before a next hop address can be determined the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party.

If timer T301 expires the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **undefinedReason** for clearing towards the calling party and set to **undefinedReason** for clearing towards the called party.
If timer T302 expires, the called party number shall be regarded as complete. If a next hop address cannot be determine the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the H.323 terminal. If a next hop address has been determined the CALL PROCEEDING message shall be sent towards the H.323 terminal.

If timer T303 expires the call shall be cleared (and all resources relinquished) with the releaseCompleteReason set to **noRouteToDestination**.

6.5 Originating gateway functional group

The originating gateway functional group is a group of functions that together may process calls originated by a terminal connected to the SCN.

NOTE: The behaviour towards the SCN is protocol dependent and not described in the present document.

6.5.1 Call establishment

Calls shall be setup using the procedures defined in clause 8.1 of ITU-T Recommendation H.323 [10] with the following changes/clarifications:

- within the context of the present document, call setup shall use only one user channel between the SCN and the gateway. Calls requiring a number of user channels shall not be supported;
- the gatekeeper and its gateway shall support both the en-bloc sending procedure and the overlap sending procedure as defined in clauses 6.5.1.1 and 6.5.1.2 of the present document;
- the gatekeeper and the gateway shall use the gatekeeper routed call model as defined in clause 7.3.1 of the ITU-T Recommendation H.323 [10];
- the gateway and the gatekeeper shall support the timers defined in clause 6.1.2 of the present document;

NOTE 1: The timers above refer to the timers required on the IP network side. The gateway may need to implement other timers depending on the protocol used on the SCN side.

- the gateway shall provide ringing tone towards the calling user according to the procedure in clause 8.1.7.4 of ITU-T Recommendation H.323 [10] "*In-band and out-of-band tones and announcements*";

NOTE 2: The procedure was introduced in the version 4 of ITU-T Recommendation H.323 [10]. However, since no additional parameters were introduced the same procedure can apply to any version of ITU-T Recommendation H.323 [10].

- the gateway and the gatekeeper shall use the fast connect procedure of ITU-T Recommendation H.323 [10], clause 8.1.7; and

- when H.245 signalling is required, the gateway and the gatekeeper shall use the encapsulation of H.245 messages within H.225.0 messages as described in clause 8.2.1 of ITU-T Recommendation H.323 [10];

- the gateway shall not pass on to the SCN any messages or information elements, or the contents of information elements that would cause a protocol error in the SCN; and

- the gateway shall not pass on to the IP network any messages or information elements or the contents of those information elements that would cause a protocol error in the IP network. Such messages, information elements, or the contents of information elements should be mapped to a suitable alternative if such exist or be discarded if not mandatory to support, or be rejected by the gateway.

6.5.1.1 En-bloc procedure

The En-bloc procedure may be explicitly indicated in the signalling from SCN. En-bloc procedure shall also be used whenever the gatekeeper can regard the called party number in the SETUP message as complete.

The gateway shall indicate to its gatekeeper in at least one of the following ways that a called party number is complete:

- include the Sending complete information element in the SETUP message; or

- include the **canOverlapSend** parameter set to **FALSE**.

The gatekeeper may (as an addition to the above) determine that the number is complete if the gatekeeper has full knowledge about the numbering plan of the called party.

If a gatekeeper determines that the number is complete the gatekeeper shall:

- send a CALL PROCEEDING message to the gateway; and

- include the "Sending complete" information element, if not already there, in the SETUP message or INFORMATION message being sent towards the next network element (e.g. a gatekeeper in an intermediate network functional group).

6.5.1.2 Overlap procedure

The overlap sending procedure shall be used to request and deliver additional called party identifier information. The overlap sending procedure may only be used for E.164 identifiers.

6.5.1.2.1 In the gateway

The gateway shall support overlap sending on the SCN interface.

On receipt of a call request message from SCN without an indication that the called party number is complete the gateway shall send the SETUP message to the gatekeeper with the **canOverlapSend** parameter set to **TRUE**.

Additional information received from SCN shall be transferred by means of the INFORMATION message. The INFORMATION message may include the *Sending complete* information element as an indication that the SCN regards the number as complete.

If timer T302 expires in the gateway the gateway shall regard the number to be complete and start timer T301.

6.5.1.2.2 In the gatekeeper

On receipt of a SETUP message with a called party number that the gatekeeper cannot determine to be complete, the gatekeeper shall:

- return a SETUP ACKNOWLEDGE message to the gateway; and
- if next hop address can be determined using the received digits, send the SETUP message towards the terminating network.

Additional information shall be provided by the gateway and transferred by means of the INFORMATION message.

If the SETUP message was sent towards the terminating network prior to the reception of the INFORMATION message the received INFORMATION message shall be forwarded towards the terminating network.

If the SETUP message was not sent, the gatekeeper shall use the received information to determine the next hop address and (if the next hop address can be determined) the gatekeeper shall send the SETUP message towards the terminating network including all digits received so far.

When a Sending complete information element is received before a next hop address can be determined the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party.

If timer T302 expires in the gatekeeper the called party number shall be regarded to be complete. If a next hop address cannot be determined the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party. If a next hop address has been determined the CALL PROCEEDING message shall be sent towards the gateway.

6.5.2 Active phase

The active phase of the call shall commence when the called party answers and the gatekeeper receives the CONNECT message as a result. The gatekeeper shall pass on the CONNECT message towards the gateway.

6.5.3 Call release

In the gateway and in the gatekeeper calls shall be cleared according to the procedures in ITU-T Recommendation H.323 [10] with the exceptions and clarifications described in this clause.

If the gateway receives an *in-band indication* in a clearing message from the SCN the gateway shall start a supervision timer.

NOTE: The value of the supervision timer is dependent on the protocol towards the SCN but is recommended to be long enough to make it possible for the called user to listen to announcements, etc.; and

At the expiry of the supervision timer the gateway shall release the call towards the SCN and initiate call clearing towards the called party with the release reason received in the clearing message from the SCN included in the RELEASE COMPLETE message to the gatekeeper.

6.6 Intermediate network functional group

The intermediate network functional group is a group of functions between the originating network and the terminating network. The intermediate network functional group handles originating calls as well as terminating calls.

The following principles applies for a gatekeeper in the intermediate network:

- the gatekeeper in the intermediate network shall act as an H.323 proxy;
- the gatekeeper in the intermediate network may communicate with a firewall in order to open ports for the media. The communication between the gatekeeper and the firewall is out of scope of the present document;
- the gatekeeper in the intermediate network shall apply policies for the information that shall be transferred between the originating network and the terminating network;

- the gatekeeper in the intermediate network may communicate with routers in the transport network in order to apply QoS policies in accordance with agreements between the originating network and the intermediate network or policies between the intermediate network and the terminating network. The communication between the gatekeeper and the router is out of scope of the present document.

The following general rule apply:

- the gatekeeper shall forward all H.225.0 messages from the originating network towards the terminating network;
- the gatekeeper shall forward all H.225.0 messages from the terminating network towards the originating network;
- the gatekeeper shall use the gatekeeper Routed call model as defined in the clause 7.3.1 of ITU-T Recommendation H.323 [10]. The call signalling channel shall be kept open during the duration of the call;
- the gatekeeper shall support the fast connect procedure as defined in clause 8.1.7 of ITU-T Recommendation H.323 [10];
- support encapsulation of H.245 messages within H.225.0 messages according to ITU-T Recommendation H.323 [10], clause 8.2.1; and
- support timers according to clause 6.1.2 of the present document.

Clarifications to the above general rule are described in the following clauses.

6.6.1 Call establishment

On receipt of a SETUP message the gatekeeper shall:

- take the *called party number* information element or the **destinationAddress** into account in determining the next hop address;
- if the SETUP message includes a *Sending complete* information element or the **canOverlapSend** parameter is set to **FALSE**, send a CALL PROCEEDING message towards the originating network;
- if the SETUP message includes the **canOverlapSend** parameter set to **TRUE** and no *Sending complete* information element is included in the message, return a SETUP ACKNOWLEDGE message towards the originating network; and
- send a SETUP message towards the terminating network.

On receipt of a SETUP ACK message from the terminating network the gatekeeper shall not be sent towards the originating network.

On receipt of the INFORMATION message from the originating network the gatekeeper shall:

- send a CALL PROCEEDING towards the originating network if the message includes the *Sending Complete* information element; and
- send the INFORMATION message towards the terminating network.

On receipt of the CALL PROCEEDING message from the terminating network the gatekeeper shall forward the message towards the originating network if the CALL PROCEEDING message is not sent before.

On receipt of a PROGRESS, a FACILITY, an ALERTING or a CONNECT message from the terminating network the gatekeeper shall forward the message towards the originating network.

6.6.2 Active phase

The active phase commences in the intermediate network when the called party answers and a CONNECT message is received in the gatekeeper as a result.

6.6.3 Call Release

On receipt of the RELEASE COMPLETE message from the terminating network or from the originating network the gatekeeper shall:

- stop any running timer;
- release all resources reserved for the call; and
- forward the message towards the originating network or towards the terminating network depending on from where the message was received.

6.6.4 Exceptional behaviour

If a connection could not be establish with the next hop address the call shall be released with the **releaseCompleteReason** set to **unreachableDestination** to the originating network.

If timer T301 expires the call shall be cleared with the **releaseCompleteReason** set to **undefinedReason** in both directions.

If timer T302 expires, the called party number shall be regarded to be complete. If a next hop address cannot be determined the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party. If a next hop address has been determined the CALL PROCEEDING message shall be sent towards the originating network.

If timer T303 expires the call shall be cleared with the released with the **releaseCompleteReason** set to **unreachableDestination** to the originating network.

6.7 Home network functional group for the called party

The procedures in this clause apply to all gatekeepers in the home network for the called party.

The general principles applies for the gatekeeper in the home network:

- the gatekeeper in the home network shall act as a gatekeeper as defined in ITU-T Recommendation H.323 [10];
- the gatekeeper in the home network shall provide services based on the user's subscription;
- the gatekeeper in the home network shall apply policies based on the user's subscription e.g. limiting bandwidth usage by modifying the contents of call control or media control messages;
- the gatekeeper in the home network may apply policies based on agreements between the home network and a serving network (if a serving network is involved).

The following clauses define the behaviour in the gatekeeper during call establishment, during the active phase and when calls are released.

6.7.1 Call Establishment

Calls shall be setup using the procedures defined in ITU-T Recommendation H.323 [10] with the following changes/clarifications:

- the gatekeeper in the home network shall support the en-bloc sending procedure and the overlap sending procedure as described in clauses 6.7.1.2 and in 6.7.1.3 of the present document;
- the gatekeeper shall use the gatekeeper Routed call model as defined in clause 7.3.1 of ITU-T Recommendation H.323 [10]. The call signalling channel shall be kept open during the duration of the call;
- the gatekeeper shall support the fast connect procedure as defined in clause 8.1.7 of ITU-T Recommendation H.323 [10];

- support encapsulation of ITU-T Recommendation H.245 [12] messages within H.225.0 messages according to clause 8.2.1 of ITU-T Recommendation H.323 [10];
- in accordance with the use of the fast connect procedure, the gatekeeper in the home network shall set the **mediaWaitForConnect** parameter to **TRUE** before sending the SETUP message towards the H.323 terminal;
- support timers according to clause 6.1.2 of the present document;
- the gatekeeper in the home network should remove the **fastStart** parameter from any message, received from the H.323 terminal, prior to the CONNECT message; and

NOTE: As a subscription option, the gatekeeper may allow activation of the media channel in one or both directions prior to the CONNECT message for certain trusted users or equipment. In those cases the **mediaWaitForConnect** may be absent (or set to **FALSE**) in the SETUP message towards the called party and the **fastStart** parameter may be kept in message towards the calling party.

- the gatekeeper in the home network shall include (if not already included) the **fastStart** parameter in the CONNECT message before sent to the originating network.

6.7.1.1 Void

6.7.1.2 En-bloc procedure

The gatekeeper in the home network shall regard the called party number as complete when:

- the called party number uniquely identifies a user;
- the canOverlapSend is set to FALSE; or
- when the SETUP message includes a *Sending complete* information element.

Once a complete number is received the gatekeeper in the home network shall use en-bloc procedures towards the H.323 terminal. If not already there, the gatekeeper in the home network shall include the *Sending complete* information element in the SETUP message towards the H.323 terminal.

6.7.1.3 Overlap procedures

The overlap sending procedure shall be used to request and deliver additional called party identifier information. The overlap sending procedure is only applicable for E.164 identifiers.

The overlap procedure may be used between the originating network and the home network.

The overlap procedure shall not be used between the home network and the H.323 terminal.

6.7.1.3.1 Normal behaviour

On receipt of a SETUP message with a called party number, that does not contain a complete user identity, the gatekeeper in the home network shall return a SETUP ACKNOWLEDGE message towards the originating network.

Additional information shall be provided by the originating network and transferred by means of the INFORMATION message.

If the digits received in the INFORMATION message and the digits received prior to the reception of the INFORMATION do not together uniquely identifies a user, the gatekeeper in the home network shall restart timer T302 on receipt of every INFORMATION message not containing a sending complete indication and containing the called party information element with at least one valid character.

6.7.1.3.2 Exceptional behaviour

When a sending complete information element is received before a user can be uniquely identified the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party.

If timer T302 expires the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party.

6.7.1.4 Void

6.7.1.5 Ring tone control

When the called H.323 terminal responds with an ALERTING message the gatekeeper in the home network may start the ringing tone towards the calling party. If the gatekeeper in the home network starts the ringing tone, the gatekeeper shall include the progress indicator information element with the PI set to No. 8 "In-band information or an applicable pattern is available" in the ALERTING message towards the originating network.

6.7.2 Active Phase

The active phase of the call shall commence when the called party answers and the home network receives the CONNECT message from the serving network as a result. The gatekeeper in the home network shall pass on the CONNECT message to the originating network.

6.7.3 Call release

The H.323 terminal, the serving network, the gatekeeper in the home network or the originating network may initiate call release.

6.8 Serving network and intermediate network functional group for the called party

This clause describes the behaviour in the serving network and in the intermediate network(s).

The following principles applies for a gatekeeper in the serving network or in an intermediate network:

- the gatekeeper shall act as an H.323 proxy;
- the gatekeeper may communicate with a firewall in order to open ports for the media. The communication between the gatekeeper and the firewall is out of scope of the present document;
- the gatekeeper shall apply policies for the information that shall be transferred between the H.323 terminal and the home network;
- the gatekeeper may communicate with routers in the Transport network in order to apply QoS policies in accordance with agreements between the serving network and the home network or policies between the intermediate network and the home network. The communication between gatekeepers and the routers is out of scope of the present document.

The following general rule apply:

- the gatekeeper shall use the gatekeeper routed call model as defined in clause 7.3.1 of ITU-T Recommendation H.323 [10]. The call signalling channel shall be kept open during the duration of the call;
- the gatekeeper shall forward all H.225.0 messages from the H.323 terminal towards the home network;
- the gatekeeper shall forward all H.225.0 message from the home network towards the H.323 terminal;
- the gatekeeper shall support the fast connect procedure as described in clause 8.1.7 of ITU-T Recommendation H.323 [10];

- the gatekeeper shall support encapsulation of H.245 messages within H.225.0 messages according to clause 8.2.1 ITU-T Recommendation H.323 [10];
- the gatekeeper shall support timer T301, T302 and T303 according to clause 6.1.2 of the present document.

Clarifications to the above general rule are described in the following clauses.

6.8.1 Call establishment

On receipt of a SETUP message the gatekeeper shall:

- establish a TCP connection with the H.323 terminal (or with the serving network if an intermediate network is involved) using the **callSignalAddress** stored during registration;

NOTE: For implementations using H.323 version 3 or later the connection type may be negotiated during registration, e.g. using a simple TCP connection, a multiplex TCP connection or UDP.

- send a CALL PROCEEDING message towards the home network; and
- send the SETUP message towards the H.323 terminal.

On receipt of the CALL PROCEEDING message from the H.323 terminal the message shall not be forwarded towards the home network.

On receipt of a PROGRESS, a FACILITY, an ALERTING or a CONNECT message from the H.323 terminal the gatekeeper shall forward the message towards the home network.

6.8.2 Active phase

The Active phase commences in the serving network and in the intermediate network when the called party answers and a CONNECT message is received as a result.

6.8.3 Call release

On receipt of the RELEASE COMPLETE message from the home network or from the H.323 terminal the gatekeeper shall:

- stop any running timer;
- release all resources reserved for the call; and
- forward the message towards the H.323 terminal or towards the home network depending on from where the message was received.

6.8.4 Exceptional behaviour

If a connection could not be established with the home network the call shall be released with the **releaseCompleteReason** set to **unreachableDestination**.

If timer T303 expires the call shall be cleared with the released with the **releaseCompleteReason** set to **unreachableDestination** towards the H.323 terminal.

If timer T301 expires the call shall be cleared with the **releaseCompleteReason** set to **undefinedReason** in both directions.

6.9 Terminating terminal functional group

The procedures in this clause apply to all H.323 terminals when receiving a SETUP message from the IP network.

6.9.1 Call establishment

Call shall be established using the procedures defined in clause 8.1 of ITU-T Recommendation H.323 [10] with the changes/clarifications described hereafter.

The H.323 terminal shall:

- use the gatekeeper routed model;
- implement the fast connect procedure of ITU-T Recommendation H.323 [10], clause 8.1.7;
- when H.245 signalling is used, encapsulate messages according to clause 8.2.1 ITU-T Recommendation H.323 [10].

6.9.2 Active phase

The active phase of a call shall commence in the H.323 terminal when the end-user answers and as a result a CONNECT message is sent towards the network.

6.9.3 Call release

The H.323 terminal shall release the call according to the procedures defined in clause 8.5 of ITU-T Recommendation H.323 [10].

6.10 Terminating gateway functional group

The terminating gateway functional group is a group of functions required for terminating calls to terminals connected to the SCN.

NOTE: The behaviour towards the SCN is protocol dependent and not described in the present document.

6.10.1 Call establishment

Calls shall be set up using the procedures defined in ITU-T Recommendation H.323 [10] with the following changes/clarifications:

- within the context of the present document, call setup shall use only one user channel between the SCN and the gateway. Calls requiring a number of user channels shall not be supported;
- the gatekeeper and its gateway shall support the en-bloc sending procedures and the overlap sending procedure defined in clauses 6.10.1.1 and 6.10.1.2 of the present document;
- the gatekeeper and the gateway shall use the gatekeeper routed call model as defined in clause 7.3.1 of ITU-T Recommendation H.323 [10];
- the gateway and the gatekeeper shall support the timers defined in clause 6.1.2 of the present document;

NOTE: The timers above refer to the timers required on the IP network side. The gateway may need to implement other timers depending on the protocol used in the SCN.

- the gateway and the gatekeeper shall use the fast connect procedure described in clause 8.1.7 of ITU-T Recommendation H.323 [10];
- when H.245 signalling is required, the gateway and the gatekeeper shall use the encapsulation of H.245 messages within H.225.0 messages according to ITU-T Recommendation H.323 [10], clause 8.2.1;

- the gateway shall not pass on to the SCN any messages or information elements, or the contents of information elements that would cause a protocol error in the SCN; and
- the gateway shall not pass on to the IP network any messages or information elements or the contents of those information elements that would cause a protocol error in the IP network. Such messages, information elements, or the contents of information elements should be mapped to a suitable alternative if such exist, be discarded if not mandatory to support, or be rejected by the gateway.

6.10.1.1 En-bloc procedure

The en-bloc procedure may be explicitly indicated in the signalling towards the SCN. En-bloc procedure shall also be used whenever the gatekeeper can regard the called party number in the SETUP message as complete.

A called party number can be regarded to be complete under the following conditions:

- if the gatekeeper has the full knowledge about the numbering plan in use in the called party's network and can identify the number to be complete;
- if the SETUP message contains the *Sending complete* information element; or
- include the **canOverlapSend** parameter set to **FALSE** in the SETUP message or in an INFORMATION message providing additional information to the SETUP message.

On receipt of the SETUP message the gatekeeper shall return the CALL PROCEEDING message towards the originating network if the *called party number* is complete.

On the receipt of the SETUP message the gateway shall return a Call PROCEEDING message if the *Sending Complete* information element is present or if the **canOverlapSend** parameter is absent or present with the value set to **FALSE**.

6.10.1.2 Overlap

The overlap sending procedure shall be used to request and deliver additional called party identifier information. The overlap sending procedure may only be used for E.164 identifiers.

6.10.1.2.1 Actions by the gatekeeper

On receipt of a SETUP message with a called party number which the gatekeeper cannot determined as complete, the gatekeeper shall return a SETUP ACKNOWLEDGE message towards the originating network and (if next hop address can be determined using the received digits) send the SETUP message to the gateway.

Additional information shall be provided by the originating network and transferred by means of the INFORMATION message.

If the SETUP message was sent to the gateway prior to the reception of the INFORMATION message, the received INFORMATION message shall be forwarded towards the gateway.

If the SETUP message was not sent, the gatekeeper shall use the received information to determine the address to the gateway and (if the gateway's address can be determined) the gatekeeper shall send the SETUP message towards that address including all digits that is received so far.

If timer T302 expires the called party number shall be regarded as complete. If an address to a gateway is not determined (due to lack of digits) the call shall be cleared (and all resources relinquished) with the **releaseCompleteReason** parameter set to **badFormatAddress** for clearing in the direction towards the calling party. If an address has been determined to a gateway the CALL PROCEEDING message shall be sent towards the originating network.

6.10.1.2.2 Actions by the gateway

The gateway shall implement the overlap procedure from the gatekeeper and towards the SCN.

On receipt of a SETUP message where the *Sending complete* information element is absent and the **canOverlapSend** set to **TRUE**, the gateway shall return a SETUP ACKNOWLEDGE message to the gatekeeper and (if an SCN access can be selected using the received digits) the gateway shall send a Call Request message to the SCN.

Additional information shall be provided by the gatekeeper and transferred by means of the INFORMATION message.

If a Call request message was sent to the SCN prior to the reception of the INFORMATION message, the received INFORMATION message shall be forwarded towards the SCN.

If the Call request message was not sent, the gateway shall use the received information to select the access to SCN and (if an SCN access can be selected), the gateway shall send the SETUP message towards that address including all digits that is received so far.

If timer T302 expires the called party number shall be regarded as complete. If no access to the SCN has been selected the call shall be cleared. If access to the SCN has been selected the CALL PROCEEDING messages shall be returned to the gatekeeper.

6.10.1.3 Support of in-band information sent by the SCN

The gateway shall implement the procedures defined in clause 8.1.7.4 of ITU-T Recommendation H.323 [10] version 4.

NOTE: The procedures in clause 8.1.7.4 of ITU-T Recommendation H.323 [10] version 4 does not imply the usage of new information element or parameters thus the procedures are applicable to any version of ITU-T Recommendation H.323 [10].

6.10.2 Active phase

The active phase of the call shall commence when the called party in the SCN answers and the gateway receives the CONNECT message as a result. The gateway shall pass a on the CONNECT message towards the gatekeeper. The gatekeeper shall pass a CONNECT to the originating network.

6.10.3 Call release

In the gateway and in the gatekeeper calls shall be cleared according to the procedures in ITU-T Recommendation H.323 [10] with the exceptions and clarifications described hereafter.

If the gateway receives an *in-band indication* in a clearing message from the SCN the gateway shall start a supervision timer.

NOTE: The value of the supervision timer is dependent on the protocol towards the SCN but is recommended to be long enough to make it possible for the called user to listen to announcements, etc.; and

At the expiry of the supervision timer the gateway shall release the call towards the SCN and initiate call clearing towards the called party with the release reason received in the clearing message from the SCN included in the RELEASE COMPLETE message to the gatekeeper.

7 Carrier selection

If a user wants to select a carrier on a per call basis the user shall indicate the carrier by means of a prefix to the dialled *called party number* information element. The user's home network service provider decides the content of the prefix and is normally dependent on the numbering plan of the country where the selected carrier resides.

The User's home network Service provider may use pre-selected carrier selection procedures. In those cases the gatekeeper in the User's home network may add the prefix to the *called party number* information element according to predefined rules.

NOTE: Pre-selected carrier selection rules and associated subscriber procedures are out of scope of the present document.

8 Calling user identity

8.1 Procedures in the H.323 terminal

A user may register more than one user identity. If the user wants to indicate witch number the network shall present to the called user for a specific call a *calling party* number information element or a **sourceAddress** parameter shall be included in the SETUP message to the network.

The status of the *called party number* information element shall be indicated in the *"Presentation indicator"* or in the "*Screening Indicator"*. The status of the **sourceAddress** shall be indicated in the **presentationIndicator** and **screeningIndicator**.

8.2 Procedures in the gatekeeper

Gatekeepers in the serving network or in intermediate networks shall not modify the contents of the *calling number* information element, the contents of the **sourceAddress** parameter, the contents of the **presentationIndicator** or the contents of the **screeningIndicator**.

Gatekeepers in the calling party's home network may screen the *calling party number* information element or the **sourceAddress** parameter and shall modify the **presentationIndicator** or the **screeningIndicator** as a result.

When screening of the *calling party number* information element or of the **sourceAddress** is required the gatekeeper sends the receiver the *calling party number* information element or the **sourceAddress** parameter in the SETUP message as the identity of the calling user.

In the case the screening fails or if the *calling party number* information element is not screened or if the SETUP message did not include any user identity at all, the gatekeeper shall include a default calling party user identity in the SETUP message towards the called party.

Screened and failed user identities shall be removed from the SETUP message before sent towards the called party.

The gatekeeper may also add a default user provided calling party identity if available.

The gatekeeper in the home network of the called party shall, if presentation is restricted, remove the *calling party number* information element from the SETUP message before sending the message towards the H.323 terminal.

The gatekeeper in the home network of the called party shall, if presentation is restricted, remove the **sourceAddress** parameter from the SETUP message before sending the message towards the H.323 terminal.

NOTE: The gatekeeper in the home network for the called party may implement restriction override services for certain users (e.g. the police, emergency centres, etc.) and in those cases allow restricted user identities to be sent to the called party.

8.3 Procedures in the gateway

Gateways shall not modify the contents of the *calling number* information element, the contents of the **sourceAddress** parameter, the contents of the **presentationIndicator** or the contents of the **screeningIndicator**.

Annex A (informative): Message flows for basic call establishment

This annex shows how the functional groups, defined in TS 101 878 [6] may be combined to describe the message flows for scenarios 0 to 3 as defined in TR 101 300 [4].

The message flows are examples of call establishment scenarios and tries to illustrate the normative text in clause 6. The message flows includes both examples of "Roaming user" and "User at home" scenarios. For more information about the mobility aspect see TS 101 315 [17].

The message flows are built up with procedures described in clause 6 using the following functional groups:

- the originating terminal functional group;
- the serving network functional group for the calling party;
- the home network functional group for the calling party;
- the home network functional group for the called party;
- the serving network functional group for the called party;
- the intermediate functional group;
- the originating gateway functional group; and
- the terminating gateway functional group.

A.0 Message flow assumptions/pre-conditions

The following clauses shows a number of message flows for call establishment and call release. Many protocols to SCN exist, many means to transport dialed information exist, difference places to provide in-band information from exists, etc. In order to simplify the examples the message flows are based on the following assumptions/pre-conditions:

- the bearer establishment information is carried by the call control messages using the "fast connect" procedure described in ITU-T Recommendation H.323 [10];
- enbloc procedures are always used;
- called party always initiates call release;
- the protocol between the SCN and the gateway is ISUP or DSS1; and
- whenever DSS1 is used; full support of the annex K to ITU-T Recommendation Q.931 [15] is assumed.

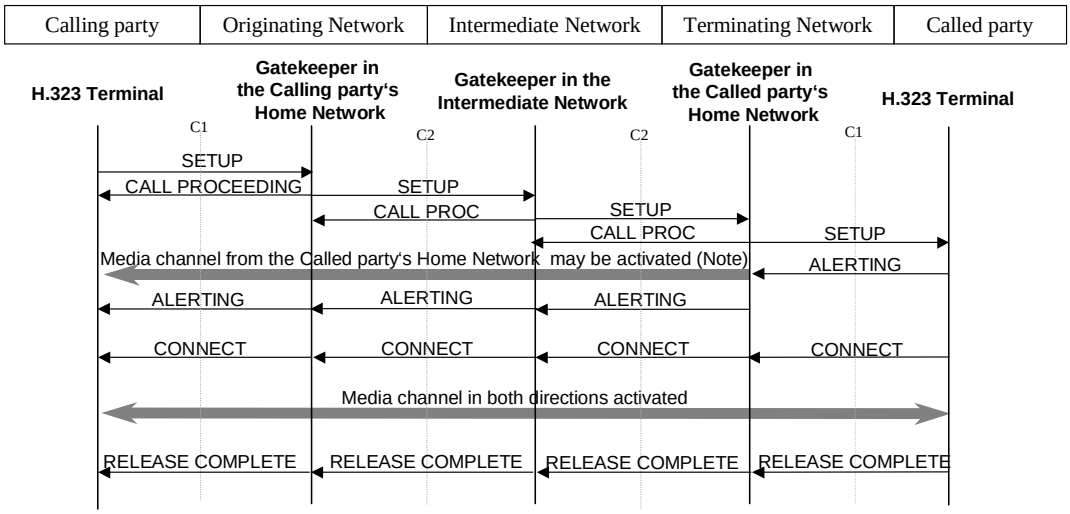
In order to fully understand the example message flows it is recommended to read the message flows together with the applicable text in clause 6.

A.1 Scenario 0

The scenario 0 is a call between two users both connected to the IP network.

A.1.1 User at home

Figure 10 shows the message flows related to call establishment and call release for a call where both users are at home.



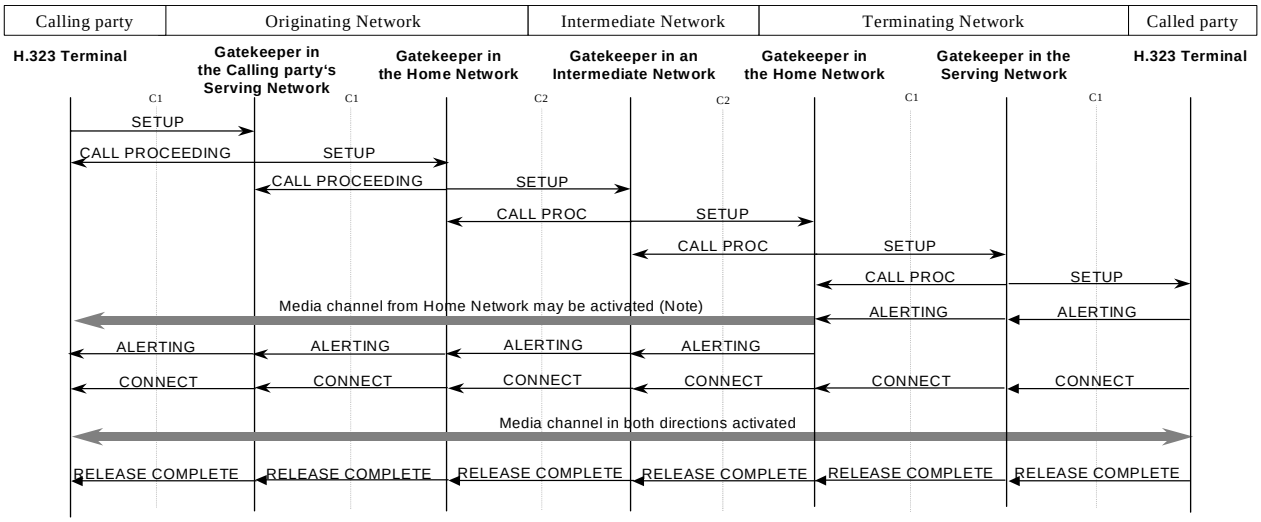
NOTE: The terminating network may provide in-band information (e.g. ringing tone towards the calling user) by means which are not in the scope of the present document.

Figure 10: Example of a call from a "User at home" connected to the IP network to a "User at home" connected to the IP network

A.1.2 Roaming user

Figure 11 shows the message flows related to call establishment and release for a call where both the calling user and the called user are roaming users.

The gatekeeper in the serving network uses information stored during the registration to locate the gatekeeper in the home network.



NOTE: The gatekeeper in the called party's home network may provide in-band information towards the calling party in the SCN (e.g. the ringing tone) by means which re not in the scope of the present document.

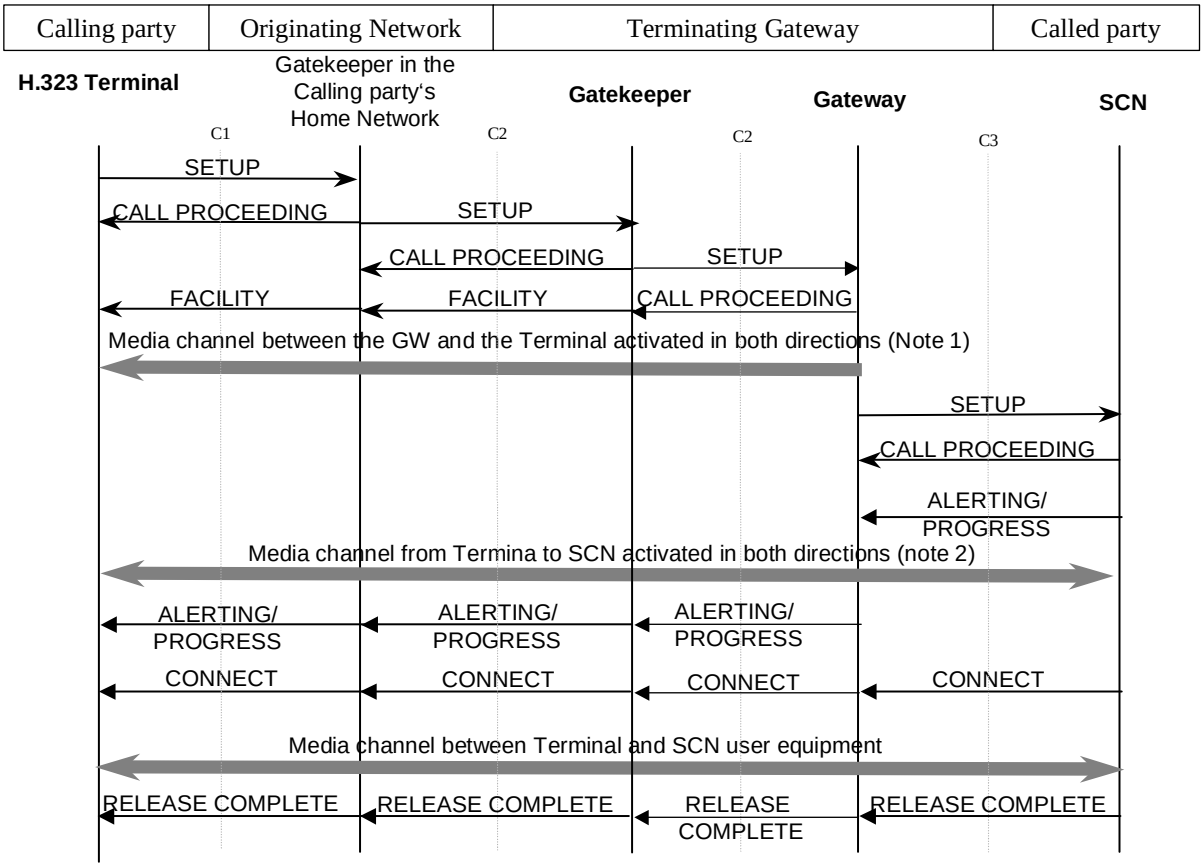
Figure 11: An example of a call from a "Roming user" connected to the IP network to a "Roaming user" connected to the IP network

A.2 Scenario 1

The scenario 1 is a call between a user connected to the IP network and a user connected to the SCN.

A.2.1 User at home

Figure 12 shows the message flows call establishment and call release for a "User at home".



NOTE 1: Internally in the IP network the media path is activated in both directions. The gateway may (for reasons and by means out of scope of this document) insert in-band information (e.g. a progress tone) in the direction towards the calling party.

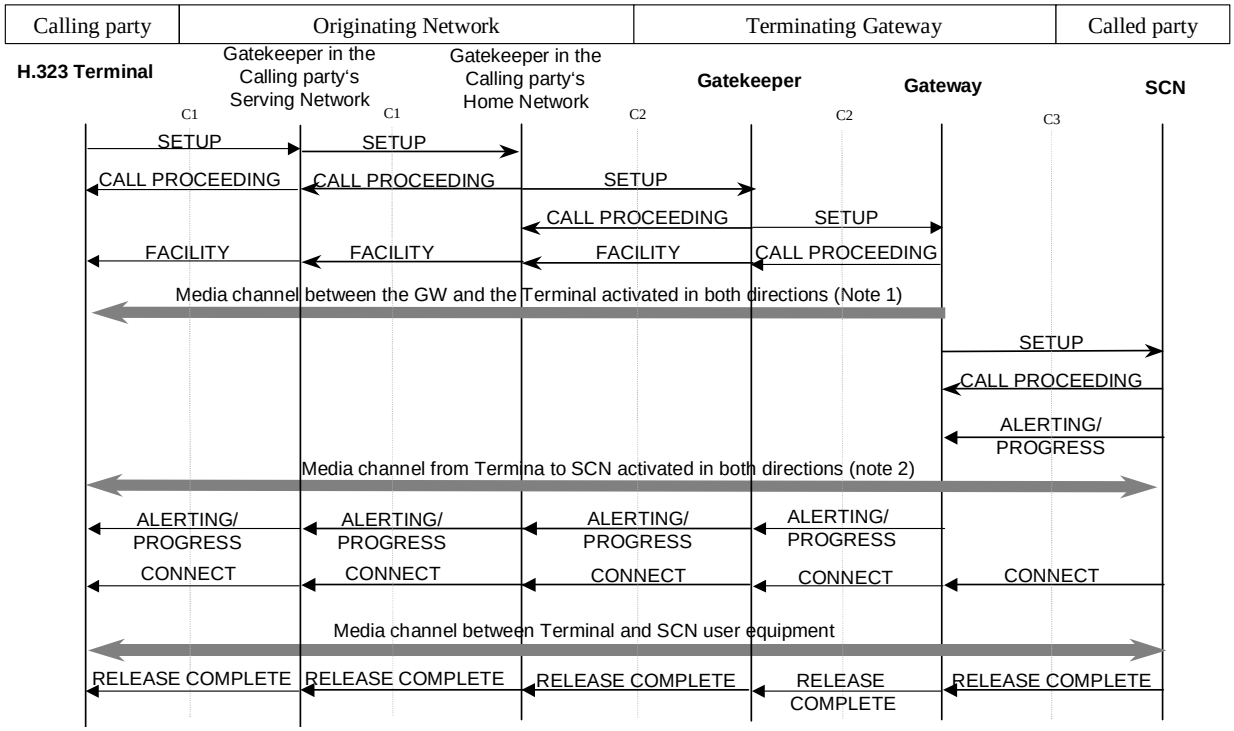
NOTE 2: After receiving an alerting or a progress indication from SCN the SCN starts sending media information. At the same time the direction from the IP terminal is open for sending inband information (e.g. DTMF tones as the response to an announcement from the SCN). The end-to-end media path is not open until the called party in SCN answers.

Figure 12: Example of a call setup from a "User at home" connected to the IP network to a user connected to the SCN

A.2.2 Roaming user

Figure 13 shows the messageflows for call establishment and release for a "Roaming user".

The gatekeeper in the serving network shall forward messages from the gatekeeper in the home network to the terminal and vice versa.



NOTE 1: Internally in the IP network the media path is activated in both directions. The gateway may (for reasons and by means out of scope of the present document) insert in-band information (e.g. a progress tone) in the direction towards the calling party.

NOTE 2: After receiving an alerting or a progress indication from SCN the SCN starts sending media information. At the same time the direction from the IP terminal is open for sending inband information (e.g. DTMF tones as the response to an announcement from the SCN). The end-to-end media path is not open until the called party in SCN answers.

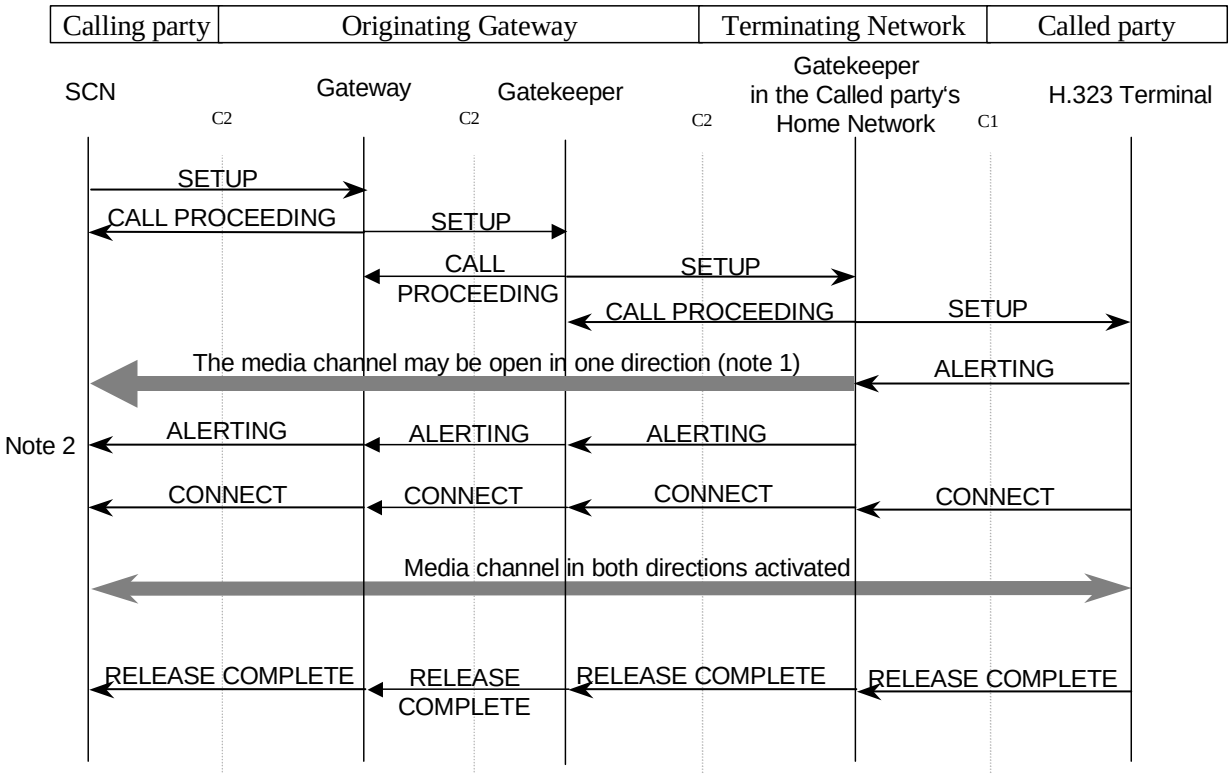
Figure 13: Example of a call from a "Roaming user" connected to the IP network to a user connected to the SCN

A.3 Scenario 2

Scenario 2 is a call from a user connected to SCN to a user connected to the IP network.

A.3.1 User at home

Figure 14 shows the messages flows related to call establishment for a user at home.



NOTE 1: The gatekeeper in the called party's home network may provide in-band information towards the calling party in the SCN (e.g. the ringing tone) by means not within the scope of the present document.
NOTE 2: If the ALERTING message does not include the progress indicator (indicating in-band information is available) the gateway is responsible for generating the ringing tone towards the calling party in the SCN.

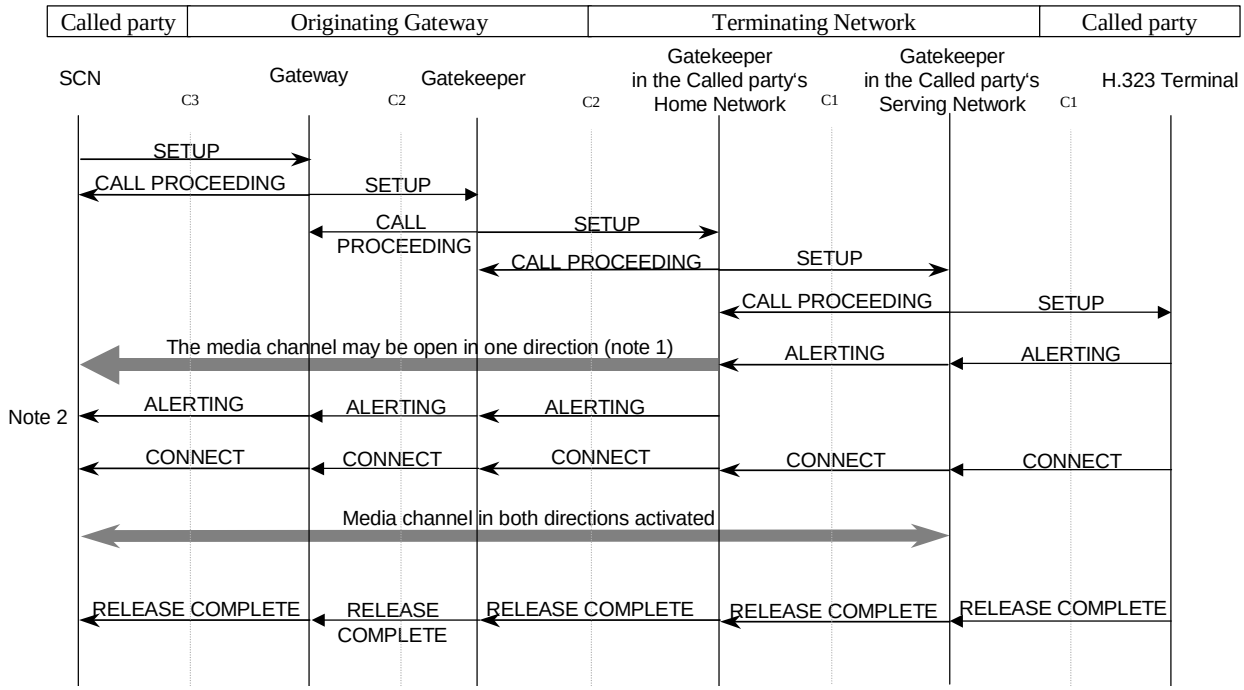
Figure 14: Example of a call from a user connected to the SCN to a "User at home" connected to the IP network

A.3.2 Roaming user

Figure 15 shows the message flows, related to call establishment and call release, for a roaming user.

The gatekeeper in the serving network uses information stored during the registration to locate the gatekeeper in the home network.

The gatekeeper in the serving network shall forward messages from the gatekeeper in the home network to the terminal and vice versa.



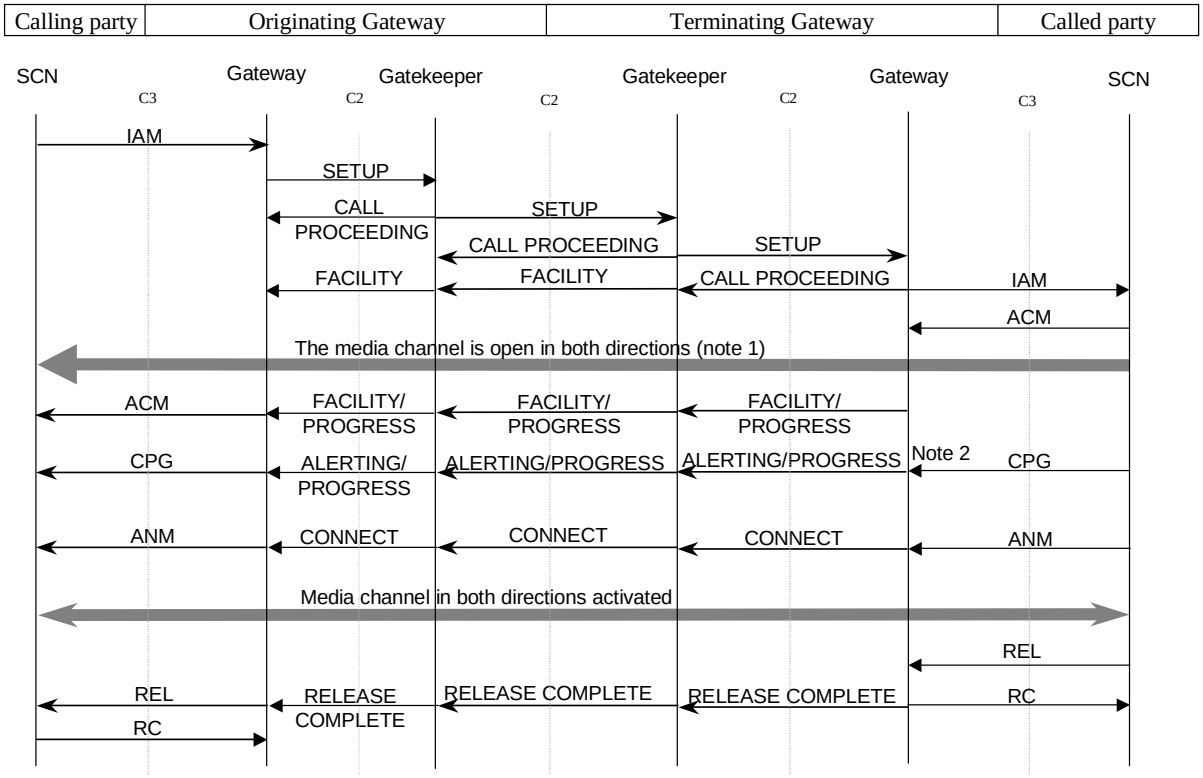
NOTE 1: The gatekeeper in the called party's home network may provide in-band information towards the calling party in the SCN (e.g. the ringing tone) by means not within the scope of the present document.
NOTE 2: If the ALERTING message does not include the progress indicator (indicating in-band information is available) the gateway is responsible for generating the ringing tone towards the calling party in the SCN.

Figure 15: An example of a call from a user connected to the SCN to a "Roaming user" connected to the IP network

A.4 Scenario 3

Scenario 3 is a call between two terminals in the SCN routed through an IP network.

Figure 16 shows the information flows related to call establishment and call release.



NOTE 1: On the receipt of the ACM message the media path is through connected in the both directions from the calling party to the called party's network. In-band information may be received from the calling party (e.g. DTMF tones as the response to an announcement from the called party's network). The end-to-end media path is not open until the called party in SCN answers.

NOTE 2: When alerting indication is received from the SCN the gateway (receiving the indication) adds a progress indicator indicating that in-band information is available.

Figure 16: An example of a call from a user connected to the SCN to another user connected in the SCN where an IP network is used as an intermediate (transit) network

Annex B (normative): H.323 protocol profile

The profile is based on ITU-T Recommendation H.323 [10] versions 2, 3 and 4.

This annex describes the usage of the messages and their parameters required to fulfil the requirements defined in TS 101 882 and the main body of the present document.

The main body is created using ITU-T Recommendation H.323 [10] standard suite as base, adding requirements from TS 101 882 but also using experiences from interoperability tests (arranged within the scope of TIPHON or other external organizations).

- "Q.931 information elements" column indicates a Q.931 information element.
- "UUIE Fields" indicates an ITU-T Recommendation H.225.0 [11] parameter.
- The "H.323v2 Status column" indicates the status in ITU-T Recommendation H.225.0 [11] version 2 for a specific parameter/information element.
- The "H.323v3 Status column" indicates the status in ITU-T Recommendation H.225.0 [11] version 3 for a specific parameter/information element.
- The "H.323v4 Status column" indicates the status in ITU-T Recommendation H.225.0 [11] version 4 for a specific parameter/information element.
- "R1 status" column, "R2 status" column, "C1 status" column and "C2 Status2 column.
  In order to distinguish between requirements from TS 101 882 and other requirements the following syntax is used in the Status fields in tables shown in the following clauses:

  M: Indicates a mandatory requirement in TS 101 882.

  O: Indicates an optional requirement in the TS 101 882. However, only sending of the parameter/message is optional. When the parameter/message is received a TIPHON compliant entity shall act upon the parameter/message in accordance with the procedures as described in the main body of the present document.

  "" An empty status field indicates that the H.323 standard shall be followed in regards to optionally.

NOTE: ITU-T Recommendation H.323 [10] version 3 has introduced parameters listed hereafter with a yellow background; ITU-T Recommendation H.323 [10] version 4 has introduced those with a blue background. All the other parameters are already available in ITU-T Recommendation H.323 [10] version 2.

B.1 H.225.0

This clause and the following clauses specify the usage of the ITU-T Recommendation H.225.0 [11] protocol messages and parameters.

B.1.1 H323-UU-PDU

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	TIPHON Status
h323-message-body	M	M	M	M
h245Tunneling	M	M	M	M
nonStandardControl	O	O	O	
h4501SupplementaryService	O	O	O	NA
H245Control	O	O	O	O
callLinkage	-	-	O	
tunnelledSignallingMessage	-	-	O	NA
provisionalResponseToH245Tunneling	-	-	O	
stimulusControl	-	-	O	NA
genericData	-	-	O	NA
NOTE: All the parameters marked with "-" in the columns of "H.323 v2 Status" and H.323v3 Status" are not defined in H.323 v2 and H.323 v3 respectively. If the protocolIdentifier parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the protocolIdentifier parameter is set to 3 parameters defined in ITU-T Recommendation H.323 v4 shall not be present.				

B.1.2 RAS messages and parameters

B.1.2.1 Gatekeeper discovery procedures

This clause shows the coding details of messages used during the procedures described in clause 5.

B.1.2.1.1 Gatekeeper ReQuest (GRQ)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
RequestSeqNum	M	M	M		
protocolIdentifier (see note 1)	M	M	M		
NonStandardData	O	O	O		
RasAddress	M	M	M	M	M
EndpointType	M	M	M	(see note 2)	(see note 3)
GatekeeperIdentifier	O	O	O		
CallServices	O	O	O	NA	NA
endpointAlias (see note 4)	O	O	O	M	M
AlternateEndpoints	O	O	O	NA	NA
Tokens	O	O	O		
cryptoTokens	O	O	O		
authenticationCapability	O	O	O	O (see note 5)	O (see note 5)
algorithmOID	O	O	O	O (see note 5)	O (see note 5)
integrity	O	O	O		
integrityCheckValue	O	O	O		
supportsAltGK	-	-	O		
featureSet	-	-	O	NA	NA
genericData	-	-	O	NA	NA

NOTE 1: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.
NOTE 2: Between the H.323 terminal and the gatekeeper the **endpointType** parameter shall always be set to **terminal**.
NOTE 3: Between gatekeepers the **endpointType** shall always be set to **terminal** and **gatekeeper**.
NOTE 4: The **endpointAlias** shall include one part identifying the User and one part identifying the IP Telephony service provider.
NOTE 5: The parameters **authenticationCapability** and **algorithmOID** are only mandatory when an explicit authentication is required.

B.1.2.1.2 Gatekeeper ConFirm (GCF)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
protocolIdentifier (see note 1)	M	M	M		
nonStandardData	O	O	O		
gatekeeperIdentifier	O	O	O		
rasAddress	M	M	M	M	M
alternateGatekeeper	O	O	O		
authenticationMode	O	O	O	O	O
tokens	O	O	O	(see note 2)	(see note 2)
cryptoTokens	O	O	O	(see note 2)	(see note 2)
algorithmOIDs	O	O	O	(see note 2)	(see note 2)
integrity	O	O	O		
integrityCheckValue	O	O	O		
featureSet	-	-	O	NA	NA
genericData	-	-	O	NA	NA

NOTE 1: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.
NOTE 2: Parameters: **tokens**, **crypTokens** and **algorithmOIDs** are mandatory when explicit authentication is required.

B.1.2.1.3 Gatekeeper ReJect (GRJ)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
protocolIdentifier (see note)	M	M	M		
nonStandardData	O	O	O		
gatekeeperIdentifier	O	O	O		
rejectReason	M	M	M		
altGKInfo	O	O	O		
tokens	O	O	O		
cryptoTokens	O	O	O		
integrityCheckValue	O	O	O		
featureSet	-	-	O	NA	NA
genericData	-	-	O	NA	NA
NOTE: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.					

B.1.2.2 Registration request procedure

This clause shows the coding details of messages used during the procedures described in clause 5.2.

B.1.2.2.1 Register Request (RRQ)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
protocolIdentifier (see note 1)	M	M	M		
nonStandardData	O	O	O		
discoveryComplete	M	M	M		
callSignalAddress	M	M	M	(see note 6)	
rasAddress	M	M	M	(see note 6)	
terminalType	M	M	M	(see note 2)	(see note 3)
terminalAlias (see note 8)	O	O	O	M	M
gatekeeperIdentifier	O	O	O		
endpointVendor	M	M	M		
alternateEndpoints	O	O	O		
timeToLive	O	O	O	M	NA
tokens	O	O	O	O	O
cryptoTokens	O	O	O	O	O
integrityCheckValue	O	O	O		
keepAlive	M	M	M		NA
endpointIdentifier	O	O	O	(see note 7)	(see note 7)
willSupplyUUIEs	M	M	M		
maintainConnection	-	M	M		
supportAnnexECallSignalling	-	M	?		
alternateTransportAddresses	-	-	O		
additiveRegistration		-	O	NA (see note 4)	NA (see note 4)
terminalAliasPattern		-	O	NA (see note 4)	NA (see note 4)
supportsAltGK		-	O		
usageReportingCapability		-	O	NA (see note 5)	NA (see note 5)
supportsRubustnessProcedures		-	M		
multipleCalls	-	-	O		
supportedH248Packages	-	-	O		
callCreditCapability	-	-	O		
capacityReportingCapability	-	-	O		
capacity	-	-	O		
featureSet	-	-	O		
genericData	-	-	O		

NOTE 1: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: The terminal shall set **terminalType** to **terminal**.

NOTE 3: The gatekeeper shall set (add) the **terminalType gatekeeper**.

NOTE 4: Registration of gateways not supported by this profile.

NOTE 5: Gatekeeper routed call model mandated in the present document thus no usage information is required in RAS messages.

NOTE 6: The H.323 terminal shall generate only one **rasAddress** and only one **callSignalAddress**.

NOTE 7: The **endpointIdentifier** identifies an active registration. Consequently the **endpointIdentifier** is not applicable when the H.323 terminal registers the first time but mandatory during the keep-alive procedure.

NOTE 8: The **terminalAlias** parameter shall include at least one valid user identity. In case more than one user identity is included, the first valid user identity shall be used as the identity for gatekeepers in the serving network and gatekeepers in the intermediate networks to identify a user's service provider. A gatekeeper in the home network shall search for the first valid user identity that at the same time corresponds to one of its users. As a consequence of this the serving network, the intermediate network and the home network may identify different users as a valid **terminalAlias**. The gatekeeper in the home network returns the final set of valid **terminalAlias** in the RCF.

B.1.2.2.2 Register ConFirm (RCF)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
protocolIdentifier (see note 1)	M	M	M		
nonStandardData	O	O	O		
callSignalAddress	M	M	M		
terminalAlias	O	O	O	M (see note 6)	M (see note 6)
gatekeeperIdentifier	O	O	O		
endpointIdentifier	M	M	M		
alternateGatekeeper	O	O	O	NA	NA
timeToLive	O	O	O		
tokens	O	O	O	O	O
cryptoTokens	O	O	O	O	O
integrityCheckValue	O	O	O		
willRespondToIRR	-	M	M		(see note 2)
preGrantedARQ (see note 3)	-	O	O	M	M
maintainConnection	-	M	M		
serviceControl	-	-	O		
additiveRegistrationSupport	-	-	M	NA	NA
terminalAliasPattern	-	-	O	NA	NA
supportedPrefixes	-	-	O	NA	NA
usageSpec	-	-	O	NA	NA
featureServerAlias	-	-	O		
capacityReportingSpec	-	-	O		
genericData	-	-	O		

NOTE 1: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: The sending of IRR messages between the serving network and the home network shall not apply.

NOTE 3: The **makeCall** parameter shall be set to **TRUE**. The **useGKCallSignalAddressToMakeCall** parameter shall be set to **TRUE**. The **answerCall** parameter shall be set to **TRUE**. The **useGLCallSignalAddressToAnswer** parameter shall be set to **TRUE**.

NOTE 4: Registration of gateways not supported by this profile.

NOTE 5: Gatekeeper routed call model mandated in the present document thus no usage information is required in RAS messages.

NOTE 6: The **terminalAlias** parameter includes the resulting list of **terminalAlias**, i.e. all user identities that the home network has successfully validated. Any authentication procedure or any call-setup procedure requiring only one user identity shall use the first **terminalAlias** as the user identity.

B.1.2.2.3 Register ReJect (RRJ)

Mandatory UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
protocolIdentifier (see note)	M	M	M		
nonStandardData	O	O	O		
rejectReason	M	M	M		
gatekeeperIdentifier	O	O	O		
altGKInfo	O	O	O		
tokens	O	O	O	O	O
cryptoTokens	O	O	O	O	O
integrityCheckValue	O	O	O		
featureSet	-	-	O		
genericData	-	-	O		

NOTE: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

B.1.2.3 Unregistration Registration request procedure

This clause shows the coding details of messages used during the procedures described in clause 5.3.

B.1.2.3.1 UnregisterRequest (URQ)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
callSignalAddress	M	M	-		
endpointAlias	O	O	O		
nonStandardData	O	O	O		
endpointIdentifier	O	O	O		
alternateEndpoints	O	O	O		
gatekeeperIdentifier	O	O	O		
tokens	O	O	O		O
cryptoTokens	O	O	O		O
integrityCheckValue	O	O	O		
reason	O	O	O		
endpointAliasPattern	-	-	O		NA
supportedPrefixes	-	-	O		NA
alternateGatekeeper	-	-	O		
genericData	-	-	O		

B.1.2.3.2 UnregisterConfirm (UCF)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum (see note)	M	M	M		
nonStandardData	O	O	O		
tokens	O	O	O		
cryptoTokens	O	O	O		
integrityCheckValue	O	O	O		
genericData	-	O	O		

B.1.2.3.3 UnregisterReject (URJ)

UUIE Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	R1 Status	R2 Status
requestSeqNum	M	M	M		
rejectReason	M	M	M		
nonStandardData	O	O	O		
altGKInfo	O	O	O		
tokens	O	O	O		
cryptoTokens	O	O	O		
integrityCheckValue	O	O	O		
genericData	-	-	O		

B.1.2.4 Request In Progress (RIP)

The Request In Progress (RIP) message shall be used as described in clause 5. The coding of the message shall be according to the H.225.0 [11].

B.1.2.5 Admission ReQuest procedures (ARQ)

Gatekeepers are recommended to allow endpoints to not use this procedure (pre-granted ARQ). However, when used the Admission Request procedure shall only apply between the endpoint and the serving network in case of a roaming user.

B.1.2.6 Information Request procedures

The Information request procedure is not mandated within the context of the TIPHON profile. However, when used the Information Request procedure shall only apply between Endpoint and the serving network in case of a roaming user.

B.1.2.7 Location request procedures

This procedure is for further study and not included in this version of the present document.

B.1.3 Q.931/Q.932 messages and parameters

TIPHON compliant equipment, implementing the call control and bearer control functional layer, shall support Q.931 messages according to the "*table 4/H.225.0 - H.225.0 usage of Q.931/Q.932 Messages*" with the modifications and clarifications that follow:

The entries in the table B.1 replaces the corresponding entries in table "*table 4/H.225.0 - H.225.0 usage of Q.931/Q.932 Messages*".

Table B.1: Q.931/Q.932 supported messages

Call establishment messages	Transmit (M, F, O, CM)	Receive and act on (M, F, O, CM)
Alerting	The ALERTING message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The ALERTING message is mandatory to transmit for H.323 terminals that want to indicate that a user is alerted about the reception of a call. The ALERTING message is mandatory to receive and act on for all H.323 terminals that implements the originating terminal functional group.	
Call Proceeding	The CALL PROCEEDING message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The CALL PROCEEDING message is mandatory for H.323 terminals that want to indicate that complete call information is received. The CALL PROCEEDING message is mandatory to receive and act on for all H.323 terminals that implements the originating terminal functional group.	
Connect	The CONNECT message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The CONNECT message is mandatory to transmit for all H.323 terminals that implements the terminating functional group. The CONNECT message is mandatory to receive and act on for all H.323 terminals that implements the originating terminal functional group.	
Progress	The PROGRESS message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The PROGRESS message is mandatory to receive and act on for all H.323 terminals that implements the originating terminal functional group.	
Setup	The SETUP message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The SETUP message is mandatory to receive and act on for all H.323 terminals that implements the terminating functional group. The SETUP message is mandatory to transmit for all H.323 terminals that implements the originating terminal functional group.	
Setup Acknowledge	The SETUP ACKNOVLEDGE message is mandatory (to transmit and to receive and act on) for all gatekeepers and gateways. The SETUP ACKNOVLEDGE message is mandatory to receive and act on for all H.323 terminals that implements the originating terminal functional group.	
Information	The INFORMATION message is mandatory (to receive and transmit) for all gatekeepers and gateways. The INFORMATION message is mandatory for all H.323 terminals implementing the overlap procedure.	

B.1.3.1 Alerting message

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Bearer capability	O	O	O		
Extended Facility	O	O	O		
Channel identification	FFS	FFS	FFS		
Facility	O	O	O		
Progress indicator	O	O	O	O	O
Notification Indicator	O	O	O		
Display	O	O	O		
Signal	O	O	O		
High layer compatibility	FFS	FFS	FFS		
User-to-User	M	M	M		
UUIE parameters					
protocolIdentifier	M	M	M		
destinationInfo	M	M	M		
h245Address	O	O	O		
callIdentifier	M	M	M		
h245SecurityMode	O	O	O		
tokens (see note 2)	O	O	O	O	O
cryptoTokens (see note 2)	O	O	O	O	O
fastStart	O	O	O	O	O
multipleCalls	-	M	M		
maintainConnection	-	M	M		
alertingAddress	-	O	O		
presentationIndicator	-	O	O		
screeningIndicator	-	O	O		
fastConnectRefused	-	-	O		
serviceControl	-	-	O		
capacity	-	-	O		

NOTE 1: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: Call related and/or bearer related **tokens**/**cryptoTokens** may be present.

B.1.3.2 Call Proceeding

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Bearer capability	O	O	O		
Extended Facility	O	O	O		
Channel identification	FFS	FFS	FFS		
Facility	O	O	O		
Progress indicator	O	O	O	O	O
Notification Indicator	O	O	O		
Display	O	O	O		
High layer compatibility	FFS				
User-to-User	M	M	M		
UUIE Fields					
protocolIdentifier (see note 1)	M	M	M		
destinationInfo	M	M	M		
h245Address	O	O	O		
callIdentifier	M	M	M		
h245SecurityMode	O	O	O		
tokens (see note 1)	O	O	O	O	O
cryptoTokens (see note 2)	O	O	O	O	O
fastStart	O	O	O	O	O
multipleCalls	-	M	M		
maintainConnection	-	M	M		
fastConnectRefused	-	-	O		
featureSet	-	-	O		

NOTE 1: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: Call related and/or Bearer related **tokens**/**cryptoTokens** may be present.

B.1.3.3 Connect message

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Bearer capability	O	O	O		
Extended Facility	O	O	O		
Channel identification	FFS	FFS	FFS		
Facility	O	O	O		
Progress indicator	O	O	O		
Notification Indicator	O	O	O		
Display	O	O	O		
Date/Time	O	O	O	NA	NA
Connected Number	O	O	O		
Connected Sub Address	O	O	O		
Low layer compatibility	FFS	FFS	FFS		
High layer compatibility	FFS	FFS	FFS		
User-to-User	M	M	M		
UUIE Fields					
protocolIdentifier (see note 1)	M	M	M		
h245Address	O	O	O		
destinationInfo	M	M	M		
conferenceID	M	M	M		
callIdentifier	M	M	M		
h245SecurityMode	O	O	O		
tokens (see note 2)	O	O	O	O	O
cryptoTokens (see note 2)	O	O	O	O	O
fastStart	O	O	O	O	O
multipleCalls	-	M	M		
maintainConnection	-	M	M		
language					
connectedAddress	-	O	O		
presentationIndicator	-	O	O		
screeningIndicator	-	O	O		
fastConnectRefused	-	-	O		
serviceControl	-	-	O		
capacity	-	-	O		
featureSet	-	-	O		

NOTE 1: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: Call related and/or Bearer related **tokens**/**cryptoTokens** may be present.

B.1.3.4 Facility

In the context of the present document this message shall be used to tunnel the H.245 protocol messages.

Mandatory Fields	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Extended facility	O	O	O		
Facility	O	M	M		
Notification indicator	O	O	O		
Display	O	O	O		
Calling Party Number	F	F	F		
Called Party Number	F	F	F		
User-to-User	M	M	M		
UUIE Fields					
protocolIdentifier (see note 1)	M	M	M		
alternativeAddress	O	O	O		
alternativeAliasAddress	O	O	O		
conferceID	O	O	O		
reason	M	M	M		
callIdentifier	M	M	M		
destExtraCallInfo	O	O	O	NA	NA
remoteExtensionAddress	O	O	O	NA	NA
tokens (see note 3)	O	O	O	O	O
cryptoTokens (see note 3)	O	O	O	O	O
conferences	O	O	O		
h245Address	O	O	O		
fastStart	O (see note 2)	O	O	O	O
multipleCalls	-	M	M		
maintainConnection	-	M	M		
fastConnectRefused	-	-	O		
serviceControl	-	-	O		
circuitInfo	-	-	O		
destinationInfo	-	-	O		
h245SecurityMode	-	-	O		

NOTE 1: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: Originally the Facility-UUIE does not include in the **fastStart** parameter. The ITU-T Recommendation H.225.0 is modified by the Implementers guide (for version 2) to also include the **fastStart** parameter.

NOTE 3: Call related and/or Bearer related **tokens**/**cryptoTokens** may be present.

B.1.3.5 Information

NOTE: In version 2 of H.225.0 this message was called **userInformation**.

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Sending complete	O	O	O	O (see note 1)	O (see note 1)
Display	O	O	O		
Keypad facility	O	O	O		
Signal	O	O	O		
Called party number	O	O	O	O (see note 1)	O (see note 1)
User-to-User	M	M	M		
UUIE Fields					
protocolIdentifier (see note 2)	M	M	M		
callIdentifier	M	M	M		
tokens	-	O	O	O	O
cryptoTokens	-	O	O	O	O
fastStart	-	O	O	NA	NA
fastConnectRefused	-	-	O		
circuitInfo	-	-	O	NA	?

NOTE 1: At least one of the information elements *Sending complete* or *called party number* shall be present.

NOTE 2: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

B.1.3.6 Progress

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Bearer capability	O	O	O		
Cause	O	O	O	O	O
Extended Facility	O	O	O		
Channel identification	FFS	FFS	FFS		
Facility	O	O	O		
Progress indicator	O	O	O	M	M
Notification Indicator	O	O	O		
Display	O	O	O		
High layer compatibility	FFS	FFS	FFS		
User-to-User	M	M	M		
UUIE Fields					
protocolIdentifier (see note 1)	M	M	M		
destinationInfo	M	M	M		
h245Address	O	O	O		
callIdentifier	M	M	M		
h245SecurityMode	O	O	O		
tokens (see note 2)	O	O	O	O	O
cryptoTokens(see note 2)	O	O	O	O	O
fastStart	O	O	O	O	O
multipleCalls	-	M	M		
maintainConnection	-	M	M		
fastConnectRefused	-	-	O		

NOTE 1: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

NOTE 2: Call related and/or Bearer related **tokens**/**cryptoTokens** may be present.

B.1.3.7 Release Complete

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Cause	CM	CM	CM	O (see note 1)	O (see note 1)
Facility	O	O	O		
Notification Indicator	O	O	O		
Display	O	O	O		
Signal	O	O	O		
User-to-User	M	M	M		
UUIE Fields					
protocol Identifier (see note 2)	M	M	M		
reason	O	O	O	O (see note 1)	O (see note 1)
callIdentifier	M	M	M		
tokens	-	O	O		
cryptoTokens	-	O	O		
busyAddress	-	O	O		
presentationIdentificatior	-	M	O		
screeningIndicator	-	M	O		
capacity	-	-	O		
serviceControl	-	-	O		
featureSet	-	-	O		

NOTE 1: The information element "*Cause"* and the parameter "**reason**" is mutual exclusive, however the sending of one of them is mandatory.

NOTE 2: The **protocolIdentifier** parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.

B.1.3.8 Setup

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Sending complete	O	O	O	O	M
Repeat indicator	F	F	F		
Bearer capability	M	M	M		
Extended facility	O	O	O		
Channel indication	FFS	FFS	FFS		
Facility	O	O	O		
Progress indicator	F	F	F		
Network specific facilities	F	F	F		
Notification indicator	O	O	O		
Display	O	O	O		
Keypad facility	O	O	O		
Signal	O	O	O		
Calling party number	O	O	O		O (see note 1)
Calling party subaddress	O	O	O		
Called party number	O	O	O	O (see note 2)	O (see note 2)
Called party subaddress	O	O	O		
Transit network selection	F	F	F		
Repeat indicator	F	F	F		
Low layer compatibility	FFS	FFS	FFS		
High layer compatibility	FFS	FFS	FFS		
User-to-User	M	M	M		
UUIE Fields					
protocol Identifier (see note 4)	M	M	M		
h245Address	O	O	O		x
sourceAddress	O	O	O	O	O (see note 1)
sourceInfo	M	M	M	?	?
destinationAddress	O	O	O	O (see note 2)	O (see note 2)
destCallSignalAddress	O	O	O		
destExtraCallInfo	O	O	O	NA	NA
destExtraCRV	O	O	O	NA	NA
activeMC	M	M	M		
conference ID	M	M	M		
conference Goal	M	M	M		
callServices	O	O	O		
callType (see note 5)	M	M	M		
sourceCallSignalAddress	O	O	O		
remoteExtensionAddress	O	O	O	NA	NA
callIdentifier	M	M	M		
h245SecurityCapability	O	O	O		
tokens (see note 8)	O	O	O	O	O
cryptoTokens (see note 8)	O	O	O	O	O
fastStart	O	O	O	M	M
mediaWaitForConnect	M	M	M		
canOverlapSend	M	M	M		
endpointIdentifier	-	O	O	M (see note 3)	
multipleCalls	-	M	M		
maintainConnection	-	M	M		
ConnectionParameters	-	O	O		
language	-	O	O		
presentationIndicator (see note 10)	-	O	O	O	O
screeningIndicator (see note 10)	-	O	O	O	O
serviceControl	-	-	O		

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
symmetricOperationRequired	-	-	O		
capacity	-	-	O		
circuited	-	-	O		
desiredProtocols	-	-	O		
neededFeatures	-	-	O		
desiredFeatures	-	-	O		
supportedFeatures	-	-	O		
parallelH245Control	-	-	O		
additionalSourceAddresses	-	-	O		

NOTE 1: At least one of the parameters **sourceAddress** or calling party number information element is shall be present.
NOTE 2: At least one of the parameter **destinationAddress** or the called party number information element shall be present.
NOTE 3: Since the gatekeeper routed call model is mandatory, between the H.323 terminal and the gatekeeper i.e. C1 reference point, the **endpointIdentifier** parameter shall always be present.
NOTE 4: The protocolIdentifier parameter shall be set to set to v2, v3 or v4. If the **protocolIdentifier** parameter is set to 2, parameters defined in H.323 v3 and H.323 v4 shall not be present. If the **protocolIdentifier** parameter is set to 3 parameters defined in H.323 v4 shall not be present.
NOTE 5: The **callType** parameter shall always be set to **pointToPoint**.
NOTE 6: The **presentationRestriction** and screeningIndicator is valid only for email and URL **callingPartyID**. The screening and restriction information for the E.164 number is included in the *calling party number* information element.
NOTE 7: E.164 **calledPartyID** shall be included in the *called party number* information element.
NOTE 8: Call related and/or Bearer related **tokens**/**cryptoTokens** may be present.
NOTE 10: If the **protocolIdentifier** is set either to 3 or 4 then this parameter shall be present since it is required for CLIR. If the **protocolIdentifier** is set to 2 then this parameter shall not be present since it is not defined in H.323 v2.

B.1.3.9 Setup Acknowledge

Q.931 information elements	H.323v2 Status	H.323v3 Status	H.323v4 Status	C1 Status	C2 Status
Protocol discriminator	M	M	M		
Call reference	M	M	M		
Message type	M	M	M		
Channel identification	O	O	O	NA	NA
Progress indicator	O	O	O	NA	NA
Display	O	O	O		
Signal	O	O	O		
UUIE Fields					
protocolIdentifier	-	-	M		
callIdentifier	-	-	M		
tokens	-	-	O		
cryptoTokens	-	-	O		

B.2 H.245

B.2.1 Terminal Capability Set message

B.2.1.1 Terminal Capability Set

Fields	H.323 Status	C1 Status	C2 Status
sequenceNumber	M		
protocolIdentifier	M		
multiplexCapability	O	M	M
capabilityTable	O		
capabilityDescriptors	O		

B.2.1.2 Terminal Capability Set Acknowledge

Fields	H.323 Status	C1 Status	C2 Status
sequenceNumber	M		

B.2.1.3 Terminal Capability Set Reject

Fields	H.323Status	C1 Status	C2 Status
sequenceNumber	M		
cause	M		

B.2.2 Void

B.2.3 Logical Channel signalling messages

B.2.3.1 Open Logical Channel

Fields	H.323 Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		
forwardLogicalChannelParameters	M		
reverseLogicalChannelParameters	O		
separateStack	O		
encryptionSync	O		

B.2.3.2 Open Logical Channel Acknowledge

Fields	H.323Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		
reverseLogicalChannelParameters	O		
separateStack	O		
encryptionSync	O		

B.2.3.3 Open Logical Channel Reject

Fields	H.323Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		
cause	M		

B.2.3.4 Open Logical Channel Confirm

Fields	H.323Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		

B.2.3.5 Close Logical Channel

Fields	H.323Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		
source	M		
reason	M		

B.2.3.6 Close Logical Channel Acknowledge

Fields	H.323Status	C1 Status	C2 Status
forwardLogicalChannelNumber	M		

B.2.4 Request mode messages

B.2.4.1 Request mode

Fields	H.323Status	C1 Status	C2 Status
sequenceNumber	M		
requestedModes	M		

B.2.4.2 Request Mode Ack

Fields	H.323Status	C1 Status	C2 Status
sequenceNumber	M		
response	M		

B.2.4.3 Request Mode Reject

Mandatory Fields	H.323 Status	C1 Status	C2 Status
sequenceNumber	M		
cause	M		
Optional Fields			

Annex C (normative): Service Capabilities

This annex describes how the Service Capabilities in TS 101 878 [6] are implemented using ITU-T Recommendation H.323 [10] and associated protocol suite.

Some of the service capabilities in TS 101 878 [6] are not mapped to ITU-T Recommendation H.323 [10] procedures. The reason for that may be:

- ITU-T Recommendation H.323 [10] protocol suite does not (intentionally) cover all aspects of IP based voice service consequently some of the service capabilities does not (and should not) map to a protocol within ITU-T Recommendation H.323 [10] protocol suite.
- The latest version of ITU-T Recommendation H.323 [10] lacks means to map the service capability (e.g. necessary parameters are missing, etc.).
- The present document only maps the reference points: R1, R2, C1 and C2 and some of the Service capabilities may not influence those reference points.

Table C.1 gives an overview of Service Capabilities defined in TS 101 878 [6] and a reference to an applicable clause in the present document.

Table C.1: Service capability reference table

Service capability in TS 101 878 [6]			**Reference within the present document**
Registration Service Capabilities	Terminal transport service registration		See note 2
	User service registration		Clause 5 "Registration"
Public telephony carrier selection	Per-call carrier selection		Clause 7 "*Carrier selection*"
	Carrier pre-selection		
Call Connectivity Service Capabilities	Simple call establishment		Clause 6 "Call connectivity"
	Calling user identity generation		Clause 8 "*Calling line identity*"
	Calling user identity conveyance		
	Calling user identity delivery		
	Call rejection		Clause 6 "Call connectivity"
	Number portability	Number portability - All Call Query	See note 1
		Number portability - Query on Release	
		Number Portability - Pivot Routing (Drop back)	
	Emergency Calls		
	Authorized emergency priority calls		
Bearer Connectivity Service Capabilities	Bearer Creation		Clause 6 "Call connectivity"
	Bearer Negotiation		Clause 6 "Call connectivity"
	Bearer re-negotiation		See note 2
	QoS Bearer support		See note 1
	QoS Bearer selection		
	Media Path Optimization		
Event reporting service capabilities	Event Recording		See note 2
Application related service capabilities	Third party authorization		See note 2
	Overlap signalling		Clause 6 "*Call connectivity*"
Other capabilities	Lawful Interception access		See note 1
	Service Resolution for Number Translation		See note 2
	Service Resolution for Destination Network Identity		See note 2

NOTE 1: The Service capability is not supported by neither version of ITU-T Recommendation H.323 [10] version 2, version 3 and version 4. However work within ITU-T may be ongoing in order to resolve the capability and available in later releases.

NOTE 2: The Service capability is out of scope of the present document. It may be added in later releases of the document.

Annex D:
Void

Annex E (normative): H.323 implementation of TIPHON functional architecture

This annex shows how the M-PDUs and parameters in TS 101 882 have been mapped to H.225.0 messages and parameters. It shall be noted that the TS 101 882 does not cover transport/technology dependent parameters so for many of the parameters in the H.225.0 it is not possible to find a corresponding parameter in TS 101 882.

E.1 Mapping of M-PDU

E.1.1 Registration

TS 101 882 defines a registration procedure where a user may register with a registrar and receive as a result of the registration a set of Service application tickets. Each ticket represents a service application. Once the user receives a ticket the User's terminal may login (attach) to the service application that the ticket represents.

The mapping in this clause is focusing on the VoIP service application using H.323 technology.

The following clause describes the mapping of the TS 101 882 parameters to H.225.0 parameters.

E.1.1a Registration meta-protocol

E.1.1.1 U_SpoAServiceAttachRequest

The U_SpoAServiceAttachRequest shall be sent by the H.323 terminal in order to register to the VoiP Service application.

U_SpoAServiceAttachRequest (RRQ)			**H.225.0 *information elements* and/or parameters**
regID(M)	registrarId (M)		terminalAlias (see note)
	registrarLoc (M)	protocolID (M)	protocolIdentifier
		nameorAddress(M)	rasAddress/callSignalAddress
		port(O)	
	registrantID(M)		terminalAlias (see note)
serviceRequestTicket(M)	registrantId (M)		cryptoTokens/tokens
	registrarId (M)		
	serviceCredential (M)	serviceAppId(M)	
		spoA(M)	
		startTime(M)	
		stopTime(M)	
		cryptoDigest(O)	
	cryptoDigest(O)		
NOTE: The terminalAlias shall have the format **registrantId@registrarID**.			

E.1.1.2 D_SpoAServiceAttachReject

This message shall be sent by the gatekeeper in order to reject a U_SpoAServiceAttachRequest message.

D_SpoAServiceAttachReject (RRJ)					H.225.0 information elements and/or parameters	
regID(M)	registrarId (M)				terminalAlias (see note)	
	registrarLoc (M)	protocolID(M)			protocolIdentifier	
		nameorAddress(M)			rasAddress/callSignalAddress	
		port(O)				
	registrantID(M)				terminalAlias (see note)	
ServiceRejectReason (M)	serviceAppId (M)				NA (see note)	
	rejectReason (M)	source (M)		callControl	Missing in Missing in ITU-T Recommendation H.225.0 [11], however the rejectReason implicitly embed the source.	
				bearerControl		
				mediaControl		
				transportControl		
		severity (M)		fatalError		
				warning		
				information		
		reason (M)		invalid	reject Reason	invalidRevision (CC), invalidCallSignalAddress (CC), invalidRASAddress (CC), invalidTerminalType (CC), invalidAlias (CC), securityDenial (CC), invalidTerminalAliases (CC)
				not_supported		discoveryRequired (CC), duplicateAlias (CC), undefinedReason, transportNotSupported (TP), transportQoSNotSupported (BC), additiveRegistrationNotSupported (CC),
				unavailable		resourceUnavailable,
				does_not_exist		fullRegistrationRequired,
				insufficient_resources		NA
		diagnostic (O)			Missing in ITU-T Recommendation H.225.0 [11].	
		freeText (O)				
		embeddedError (O)	source	callControl		
				bearerControl		
				mediaControl		
				transportControl		
			severity	fatalError		
				warning		
				information		
			reason	invalid		
				not_supported		
				unavailable		
				does_not_exist		
				insufficient_resources		
NOTE: In ITU-T Recommendation H.323 [10] the service application is implicit, i.e. the VoIP application.						

E.1.1.3 D_SpoAServiceAttachResponse

This message shall be sent by the gatekeeper to confirm the U_SpoAServiceAttachRequest message.

D_SpoAServiceAttachResponse (RCF)			H.225.0 information elements and/or parameters
regID (M)	registrarId(M)		terminalAlias
	registrarLoc(M)	protocolID(M)	protocolIdentifier
		nameorAddress(M)	rasAddress/callSignalAddress
		port(O)	
	registrantID(M)		terminalAlias
serviceOfferTicket (M)	registrantId (M)		cryptoTokens/Tokens
	registrarId (M)		
	serviceCredential (M)	serviceAppId(M)	
		spoA(M)	
		startTime(M)	
		stopTime(M)	
		cryptoDigest(O)	
	cryptoDigest(O)		

E.1.2 Call control M-PDUs

E.1.2.1 CallRequest (SETUP)

E.1.2.1.1 U_CallRequest

The table below shows the mapping of the U_CallRequest to the ITU-T Recommendation H.225.0 [11] message SETUP.

NOTE: The ITU-T Recommendation H.225.0 [11] message SETUP carries additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

U_CallRequest					**H.225.0 *information elements* and/or parameters**	
callId (M)					callIdentifier	
callingPartyRestriction (M)		identityAvailable			*PresentationIndicator* or presentationIndicator	presentationAllowed
		identityUnavailable				presentationRestricted or addressNotAvailable
callingPartyId (O)	e164	natureOfAddress	nationalSubscriberNumber		*Calling party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown			unknown
			nationalSiginficantNumber			nationalNumber
			internationalNumber			internationalNumber
			nationalNetworkSpecificNumber			networkSpecificNumber
			nationalSignificantRoutingNumber			see note 3
		screeningIndicator	userProvided		*Calling party number (SI)* or screeningIndicator (see note 2)	userProvidedVerifiedAndPassed
			notVerifiedUserProvided			userProvidedNotScreened
			verifiedAndPassedNetworkProvided			networkProvided
		digits	{1234567890}		*Calling party number (digits)* or sourceAddress.partyNumber::Numberdigits	
	url				destinationAddress.url-ID	
	displayName				Missing in ITU-T Recommendation H.225.0 [11].	
calledPartyId (M)	e164	natureOfAddress	nationalSubscriberNumber		*Called party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown			unknown
			nationalSiginficantNumber			nationalNumber
			internationalNumber			internationalNumber
			nationalNetworkSpecificNumber			networkSpecificNumber
			nationalSignificantRoutingNumber			see note 2
		digits	{1234567890}		*Called party number (digits)* or destinationAddress.partyNumber:: Numberdigits	
	url				destinationAddress	
callpriority (O)		normal			Missing in ITU-T Recommendation H.225.0 [11].	
		emergency				
		authorizedETS				
operatorSelection (O)		{1234567890}			*Called party number* (see note 1)	
serviceOfferTicket (M)		registrantId			cryptoTokens/tokens	
		registrarId				
		serviceCredential (M)		serviceAppId (M)		
				spoA (M)		
				startTime (M)		
				stopTime (M)		
				cryptoDigest (O)		
		cryptoDigest (O)				

NOTE 1: The **operatorSelection** shall be added as prefix to the digits in the *called party number* information element.
NOTE 2: The use of the value "userProvidedVerifiedAndFailed" (defined in ITU-T Recommendation H.225.0 [11]) is not defined within the scope of this release of the document and shall not be used.

E.1.2.1.2 D_CallRequest

The table below shows the mapping of the D_CallRequest to the ITU-T Recommendation H.225.0 [11] message SETUP.

NOTE 1: The ITU-T Recommendation H.225.0 [11] message SETUP carries additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

D_CallRequest				**H.225.0 *information elements* and/or parameters**	
callId (M)				callIdentifier	
callingParty Restriction (M)		identityAvailable		*PresentationIndicator* or presentationIndicator	presentationAllowed
		identityUnavailable			presentationRestricted or addressNotAvailable
callingParty Id (O)	e164	natureOfAddress	nationalSubscriberNumber	*Calling party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown		unknown
			nationalSiginficantNumber		nationalNumber
			internationalNumber		internationalNumber
			nationalNetworkSpecificNumber		networkSpecificNumber
			nationalSignificantRoutingNumber		see note 3
		screeningIndicator	userProvided	*Calling party number (SI)* or screeningIndicator (see note 2)	userProvidedVerifiedAndPassed
			notVerifiedUserProvided		userProvidedNotScreened
			verifiedAndPassedNetworkProvided		networkProvided
		digits	{1234567890}	*Calling party number (digits)* or sourceAddress.partyNumber::Numberdigits	
	url			destinationAddress.url-ID	
	displayName			Missing in ITU-T Recommendation H.225.0 [11].	
calledParty Id (M)	e164	natureOfAddress	nationalSubscriberNumber	*Called party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown		unknown
			nationalSiginficantNumber		nationalNumber
			internationalNumber		internationalNumber
			nationalNetworkSpecificNumber		networkSpecificNumber
			nationalSignificantRoutingNumber		see note 1
		digits	{1234567890}	*Called party number (digits)* or destinationAddress.partyNumber::Numberdigits	
	url			destinationAddress	
callpriority (O)			normal	Missing in ITU-T Recommendation H.225.0 [11].	
			emergency		
			authorizedETS		

NOTE 2: The use of the value "userProvidedVerifiedAndFailed" (defined in ITU-T Recommendation H.225.0 [11]) is not defined within the scope of this release of the document and shall not be used.

E.1.2.1.3 NW_CallRequest

The table below shows the mapping of the NW_CallRequest to ITU-T Recommendation H.225.0 [11] message SETUP.

NOTE: The ITU-T Recommendation H.225.0 [11] message SETUP carries additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

NW_CallRequest							**H.225.0 *information elements* and/or parameters**	
callId (M)							callIdentifier	
callingPartyRestriction (M)		identityAvailable					*PresentationIndicator* or presentationIndicator	presentationAllowed
		identityUnavailable						presentationRestricted or addressNotAvailable
callingPartyId (O)	e164	natureOfAddress	nationalSubscriberNumber				*Calling party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown					unknown
			nationalSiginficantNumber					nationalNumber
			internationalNumber					internationalNumber
			nationalNetworkSpecificNumber					networkSpecificNumber
			nationalSignificantRoutingNumber					see note 3
		screeningIndicator	userProvided				*Calling party number (SI)* or screeningIndicator (see note 2)	userProvidedVerifiedAndPassed
			notVerifiedUserProvided					userProvidedNotScreened
			verifiedAndPassedNetworkProvided					networkProvided
		digits	{1234567890}				*Calling party number (digits)* or sourceAddress.partyNumber::Numberdigits	
	url						destinationAddress.url-ID	
	displayName						Missing in ITU-T Recommendation H.225.0 [11].	
calledPartyId (M)	e164	natureOfAddress	nationalSubscriberNumber				*Called party(TON) or* PublicTypeOfNumber	subscriberNumber
			nationalUnknown					unknown
			nationalSiginficantNumber					nationalNumber
			internationalNumber					internationalNumber
			nationalNetworkSpecificNumber					networkSpecificNumber
			nationalSignificantRoutingNumber					see note 3
		digits	{1234567890}				*Called party number (digits)* or destinationAddress.partyNumber::Numberdigits	
	url						destinationAddress	
callpriority (O)			normal				Missing in ITU-T Recommendation H.225.0 [11].	
			emergency					
			authorizedETS					
NWLocationData (O)							see note 2	
nWRoutingNumber (O)	toSCN (M)		recipientNetworkID					
			pointOfInterconnection	iPV4Address				
				ipV6Address				
				scn				
			recipientExchange					
	toIP (M)		serviceProviderIdentity					
			pointOfInterconnection	iPV4Address				
				ipV6Address				
				scn				
			recipientNetworkFG					
serviceOfferTicket (M)	registrantId						cryptoTokens/tokens	
	registrarId							
	serviceCredential (M)			serviceAppId (M)				
				spoA (M)				
				startTime (M)				
				stopTime (M)				
				cryptoDigest (O)				
	cryptoDigest (O)							

NOTE 1: The use of the value "userProvidedVerifiedAndFailed" (defined in ITU-T Recommendation H.225.0 [11]) is not defined within the scope of this release of the document and shall not be used.
NOTE 2: The parameter is not defined in ITU-T Recommendation H.225.0 [11].

E.1.2.2 CallReport (SETUP ACKNOWLEDGE)

The table below shows the mapping of the D_CallReport and NW_CallReport to the ITU-T Recommendation H.225.0 [11] message SETUP ACKNOWLEDGE.

D_CallReport and NW_CallReport	**H.225.0 *information elements* and/or parameters**
callID (M)	callIdentifier
report (M)	addressIncomplete (1)
reportParams (O)	

E.1.2.3 CCAditionalDigits (INFORMATION)

The table below shows the mapping of U_CCAditionalDigits and the NW_CCAdditionalDigits to the ITU-T Recommendation H.225.0 [11] message INFORMATION.

U_CCAditionalDigits and NW_CCAdditionalDigits	**H.225.0 *information elements* and/or parameters**
callID (M)	callIdentifier
additionalDigits	Called party number

E.1.2.4 CallReport (CALL PROCEEDING)

The table below shows the mapping of D_CallReport and the NW_CallReport to the ITU-T Recommendation H.225.0 [11] message CALL PROCEEDING.

NOTE: The ITU-T Recommendation H.225.0 [11] message CALL PROCEEDING may carry additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

D_CallReport and NW_CallReport	**H.225.0 information elements and/or parameter**
callID (M)	callIdentifier
report (M)	addressComplete (0) (CALL PROCEEDING)
reportParams (O)	*Progress Indicator*

E.1.2.5 CallReport (PROGRESS)

The table below shows the mapping of D_CallReport and the NW_CallReport to the ITU-T Recommendation H.225.0 [11] message PROGRESS.

NOTE: The ITU-T Recommendation H.225.0 [11] message PROGRESS may carry additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

D_CallReport and NW_CallReport	**H.225.0 *information elements* and/or parameters**
callID (M)	**callIdentifier**
report (M)	callProceeding (3) (PROGRESS)
reportParams (O)	*Progress indicator*

E.1.2.6 CallReport (ALERTING)

The table below shows the mapping of D_CallReport, the NW_CallReport and U_CallReport to ITU-T Recommendation H.225.0 [11] message ALERTING.

NOTE: The ITU-T Recommendation H.225.0 [11] message ALERTING may carry additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

D_CallReport, NW_CallReport and U_CallReport	**H.225.0 *information elements* and/or parameters**
callID (M)	**callIdentifier**
report (M)	callAlerting (3) (ALERTING)
reportParams (O)	*Progress indicator*

E.1.2.7 CallConnect (CONNECT)

The table below shows the mapping of D_CallConnect, the NW_CallConnect and U_CallConnect to the ITU-T Recommendation H.225.0 [11] message CONNECT.

NOTE: The ITU-T Recommendation H.225.0 [11] message CONNECT may carry additional bearer related information. The mapping of bearer related information is described in clause E.1.3.

D_CallConnect, NW_CallConnect and U_CallConnect	**H.225.0 *information elements* and/or parameters**
callID (M)	**callIndicator**

E.1.3 Bearer control M-PDUs

E.1.3.1 BearerRequest (SETUP)

The table below shows how the U_BearerRequest, NW_BearerRequest and D_BearerRequest is mapped to ITU-T Recommendation H.245 [12] carried by the **fastStart** parameter in the ITU-T Recommendation H.225.0 [11] SETUP message.

U_BearerRequest, NW_BearerRequest and D_BearerRequest				**H.225.0 *information elements* and/or parameters**
bearerID (M)				sessionID
uplinkBearer (M)	serviceClass (M)		bestEffort	see note 1
			narrowbandAcceptable	
			narrowbandMedium	
			narrowbandHigh	
			wideband	
	flowDescriptor (M)	codecDescriptor (M)	codecID (M)	rtpPayloadType and AudioCapability
			silenceSuppressionEnabled (M)	H2250LogicalChannelParameters. silenceSuppression
			codecSpecificParameter (M)	AudioCapability
		delayBudget (M)		see note 1
		framesPerPacket (M)		AudioCapability
		transportDescriptor (M)	maxCodecGrossBitRate (M)	
			remainderDelayBudget (M)	
			packetRate (M)	
			packetDelayVariation (M)	
			packetLoss (M)	
			originatorMpoa (M) (see note 2)	mediaChannel
			destinationMpoA (M) (see note 2)	NA
downlinkBearer (M)	serviceClass (M)		bestEffort	see note 1
			narrowbandAcceptable	
			narrowbandMedium	
			narrowbandHigh	
			wideband	
	flowDescriptor (M)	codecDescriptor (M)	codecID (M)	rtpPayloadType and AudioCapability
			silenceSuppressionEnabled (M)	H2250LogicalChannelParameters. silenceSuppression
			codecSpecificParameter (M)	AudioCapability
		delayBudget (M)		see note 1
		framesPerPacket (M)		AudioCapability
		transportDescriptor (M)	maxCodecGrossBitRate (M)	
			remainderDelayBudget (M)	
			packetRate (M)	
			packetDelayVariation (M)	
			packetLoss (M)	
			originatorMpoa (M) (see note)	NA
			destinationMpoA (M) (see note)	mediaChannel
NOTE 1: Not implemented in either ITU-T Recommendation H.323 [10] versions 2, 3 nor 4. NOTE 2: The MpoA type can be broken down to Ipv4, Ipv6 addresses and port, but this is not shown in the table.				

E.1.3.2 BearerConnect (CALL PROCEEDING, FACILITY, PROGRESS, ALERTING and/or CONNECT)

The table below shows how the U_BearerConnect, NW_BearerConnect and the D_BearerConnect is mapped to ITU-T Recommendation H.245 [12] parameters. The BearerConnect can be transported with any of the ITU-T Recommendation H.225.0 [11] messages: CALL PROCEEDING, FACILITY, PROGRESS, ALERTING and/or CONNECT.

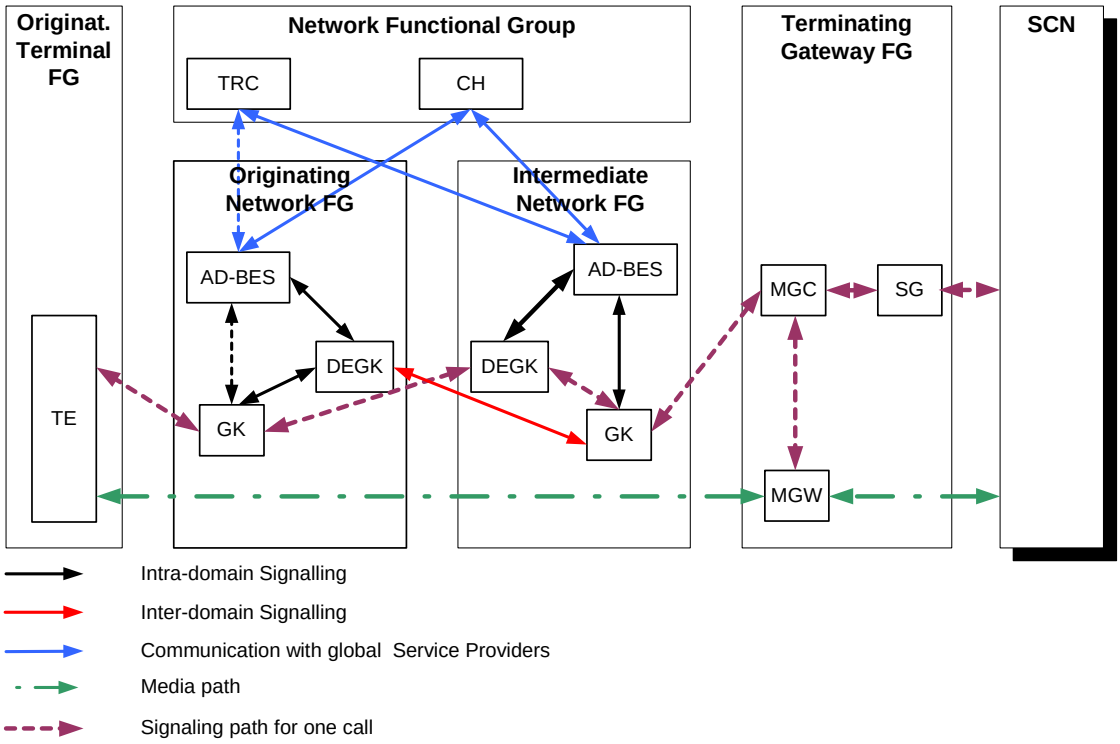
U_BearerConnect, NW_BearerConnect and D_BearerConnect				**H.225.0 *information elements* and/or parameters**
bearerID (M)				sessionID
uplinkBearer (M)	serviceClass (M)		bestEffort	see note
			narrowbandAcceptable	
			narrowbandMedium	
			narrowbandHigh	
			wideband	
	flowDescriptor (M)	codecDescriptor (M)	codecID (M)	rtpPayloadType and AudioCapability
			silenceSuppressionEnabled (M)	H2250LogicalChannelParameters. silenceSuppression
			codecSpecificParameter (M)	AudioCapability
		delayBudget (M)		see note
		framesPerPacket (M)		AudioCapability
		transportDescriptor (M)	maxCodecGrossBitRate (M)	
			remainderDelayBudget (M)	
			packetRate (M)	
			packetDelayVariation (M)	
			packetLoss (M)	
			originatorMpoa (M) (see note)	mediaChannel
			destinationMpoA (M) (see note)	NA
downlinkBearer (M)	serviceClass (M)		bestEffort	see note
			narrowbandAcceptable	
			narrowbandMedium	
			narrowbandHigh	
			wideband	
	flowDescriptor (M)	codecDescriptor (M)	codecID (M)	rtpPayloadType and AudioCapability
			silenceSuppressionEnabled (M)	H2250LogicalChannelParameters. silenceSuppression
			codecSpecificParameter (M)	AudioCapability
		delayBudget (M)		see note
		framesPerPacket (M)		AudioCapability
		transportDescriptor (M)	maxCodecGrossBitRate (M)	
			remainderDelayBudget (M)	
			packetRate (M)	
			packetDelayVariation (M)	
			packetLoss (M)	
			originatorMpoa (M) (see note)	NA
			destinationMpoA (M) (see note)	mediaChannel
NOTE: The MpoA type can be broken down to Ipv4, Ipv6 addresses and port, but this is not shown in the table.				

Annex F (informative): H.323 Implementation used by VISIONng

F.1 Introduction

This annex describes one possibility of using the TIPHON standards and how to implement an H.323 technology based global inter-domain IP-Telephony services.

Figure F.1 shows the information flow in terms of signalling flow and media flow for a call initiated in an IP-based domain and terminated in an SCN-based domain.



NOTE 1: The GateKeeper (GK) implements the bearer control functional layer and the call control functional layer.
NOTE 2: The AD-BES implements the service control functional layer and services functional layer but it also communicates with external services.
NOTE 3: The DEGK is a gatekeeper that implements the bearer control functional layer, the call control functional layer. Its main purpose is to act as the edge for inter domain communication.

Figure F.1: Information flow used in VISIONng

Figure F.1 assumes that the calling party has already finished the registration process at its gatekeeper. Dashed lines show the information flow for the signalling path, the intra-domain signalling as well as for the communication with the TRC required for one call.

In order to set up a call, the calling party sends a request to the GK, it is registered with, to set up a call to the called party. The called party is identified using an E.164. The E.164 number may be:

- either a personal number (e.g. international UPT number); or
- a geographic number (i.e. any other E.164 number).

The GK then sends a request to its Administrative Domain Back-End Service (AD-BES) to get back the required routing information. The AD-BES has to find out whether the called party number belongs to its own subscriber or not. If this is not the case and the called party number is an international UPT number or a UPT number as shown in figure F.1, the AD-BES sends a request to the TIPHON Resolution Capability (TRC) to find out the home network name of the called party.

After having received it, the AD-BES needs to resolve the home network name to the IP-address of the domain entry gatekeeper of the home network of the called party. This information exists in the AD-BES and is sent back to the GK, which has sent the query for routing information before.

In the case that the called party number is a UPT number belonging to an own subscriber, the AD-BES queries the user profile of this subscriber to find out the terminal at which the called party wants to receive his/her calls and sends this information back to the GK.

If the called party number is a geographic number the AD-BES knows how to terminate, the AD-BES sends back to the GK the IP-address of the gateway located next to the called party.

If the called party number is a geographic number the AD-BES does not know how to terminate it sends a request to the Service Area Broker (SAB) functionality of the clearinghouse to receive the required routing information and sends this information to the GK.

After the GK has received the correct routing information it uses the H.225.0/Q.931 profile described in annex B of the present document to setup the call. For providing security for inter-domain signalling annex D of ITU-T Recommendation H.235 [26] is used.

After the DEGK has received the setup message, it sends a request to its own AD-BES to find out at which terminal the called party wants to receive his/her calls. This information exists in the user profile of the called party number stored in the AD-BES of his home network. In the case shown in figure F.1 this is an SCN-based terminal and therefore the call is routed to the gateway located next to the terminal of the called party. The media path is setup between the originating terminal and the called party's terminal via the media gateway.

For settlement purposes the Call Detail Records (CDRs) produced in the domains of the calling as well as in the called party are sent to the clearinghouse. For international UPT calls there is no online information exchange required between the participating domains and the clearinghouse because of the fact that the routing decision is made by the TRC. As a consequence of that the CDRs are sent to the clearinghouse in bulk mode.

Annex G:
Void

Annex H:
Void

Annex I (informative): Proposed changes to ITU-T Recommendation H.323

This annex contains a list of Service capabilities (defined in TS 101 878 [6]) not supported by the ITU-T Recommendation H.323 [10] protocol suite and within the scope of the present document i.e. primitives or parameters over the C1, C2, R1 and R2 reference points.

Table I.1: Service capabilities not supported by the ITU-T Recommendation H.323 [10] protocol suite

Service capability in TS 101 878 [6]		
Call Connectivity Service Capabilities	Number portability	Number portability - All Call Query
		Number portability - Query on Release
		Number Portability - Pivot Routing (Drop back)
	Emergency Calls	
	Authorized emergency priority calls	
Bearer Connectivity Service Capabilities	QoS Bearer support	
	QoS Bearer selection	
	Media Path Optimization	
Other capabilities	Lawful Interception access	

Annex J (informative): Bibliography

- ISO/IEC 11571: "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Networks - Addressing".
- ETSI TS 101 329-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 2: Definition of speech Quality of Service (QoS) classes".
- ETSI TS 101 884: "Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 3; Technology Mapping; Implementation of TIPHON architecture using SIP".
- ETSI TS 101 882: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Protocol Framework Definition and Interface Requirement Definition; General (meta-protocol)".
- ETSI TS 102 027 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Technology Compliance Specification; Draft IETF SIP RFC2543bis-04".
- ETSI TS 101 889 (all parts): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Technology Compliance Specifications; TIPHON profile for ITU-T H.248".

History

Document history		
V1.1.1	April 2002	Publication