



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.501

(03/2002)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Mobility and Collaboration procedures – Overview of
Mobility and Collaboration, definitions, protocols and
procedures

Protocol for mobility management and intra/inter-domain communication in multimedia systems

ITU-T Recommendation H.501

ITU-T H-SERIES RECOMMENDATIONS
AUDIOVISUAL AND MULTIMEDIA SYSTEMS

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

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

ITU-T Recommendation H.501

Protocol for mobility management and intra/inter-domain communication in multimedia systems

Summary

The purpose of this Recommendation is to define messages and procedures for mobility management and for communication within and between domains of a mobile or non-mobile multimedia environment for the purpose of address resolution, user authentication, service data exchange, access authorization, call validation and usage reporting.

...

Source

ITU-T Recommendation H.501 was prepared by ITU-T Study Group 16 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 March 2002.

Keywords

Address resolution, administrative domains, authentication, authorization, H.225.0 Annex G, mobility management, multimedia systems, usage reporting.

FOREWORD

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

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

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

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

NOTE

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2002

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	Normative references.....	1
3	Definitions	2
4	Symbols and abbreviations	2
5	Requirements	2
5.1	Transport requirements.....	2
5.2	Security considerations.....	3
5.3	Addressing conventions.....	3
5.4	Address templates and descriptors	4
6	Message definitions	4
6.1	Descriptor	5
6.2	Descriptor information	6
6.3	Address template	6
6.3.1	Pattern.....	6
6.3.2	Route information.....	7
6.3.3	Pricing information.....	7
6.3.4	Contact information.....	8
6.4	Common structures.....	9
6.4.1	AlternatePE.....	9
6.4.2	PartyInformation.....	9
6.4.3	CallInformation	10
6.4.4	UserInformation	10
6.4.5	Usage specification.....	10
6.4.6	Security Mode	11
6.5	Service relationship	11
6.5.1	Service Request	11
6.5.2	Service Confirmation.....	12
6.5.3	Service Rejection.....	13
6.5.4	Service Release.....	14
6.6	Descriptor distribution.....	14
6.6.1	Descriptor Request	14
6.6.2	Descriptor Confirmation.....	14
6.6.3	Descriptor Rejection.....	14
6.6.4	Descriptor ID Request	15
6.6.5	Descriptor ID Confirmation	15
6.6.6	Descriptor ID Rejection.....	15

Documents

ITU-T Rec. H.501 (03/2002)

Document Sharing Hub

iii

	Page
6.6.7 Descriptor Update.....	16
6.6.8 Descriptor Update Acknowledgement	16
6.7 Address resolution.....	16
6.7.1 Access Request.....	16
6.7.2 Access Confirmation	17
6.7.3 Access Rejection	17
6.8 Request in Process.....	18
6.9 Non-standard messages	18
6.9.1 Non-Standard Request.....	18
6.9.2 Non-Standard Confirmation	18
6.9.3 Non-Standard Rejection	18
6.10 Unknown Message Response.....	19
6.11 Usage reports	19
6.11.1 Usage Request	19
6.11.2 Usage Confirmation.....	19
6.11.3 Usage Rejection.....	20
6.11.4 Usage Indication.....	20
6.11.5 Usage Indication Confirmation	21
6.11.6 Usage Indication Rejection.....	21
6.12 Validations.....	22
6.12.1 Validation Request	22
6.12.2 Validation Confirmation.....	22
6.12.3 Validation Rejection.....	22
6.13 Authentication	23
6.13.1 Authentication Request	23
6.13.2 Authentication Confirmation.....	23
6.13.3 Authentication Rejection.....	23
 Annex A – Message Syntax.....	 24

ITU-T Recommendation H.501

Protocol for mobility management and intra/inter-domain communication in multimedia systems

1 Scope

This Recommendation describes a protocol for communication between logical elements of a multimedia packet network to allow the completion of calls to and from users managed by such logical elements. This protocol can be used in mobile and non-mobile environments for the purpose of address resolution, user authentication, service data exchange, access authorization, call validation and usage reporting. These capabilities enable the protocol to be used for mobility management in mobile environments.

The general procedure is for logical elements to exchange information regarding the location of users or endpoints, in the form of addresses each administrative domain can resolve. Addresses can be specified in a general manner or in an increasingly specific manner. Additional information allows elements within an administrative domain to determine the most appropriate administrative domain to serve as the destination for the call. Logical elements may control access to their exposed addresses, and require reports on the usage made during calls to those addresses.

Other Recommendations will specify how the protocol defined in this Recommendation is used by particular applications. It is not necessary for an application to implement the full protocol. The application can select from the messages and procedures those relevant to its requirements.

2 Normative references

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

- ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan*.
- ITU-T Recommendation H.225.0 Version 4 (2000), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
- ITU-T Recommendation H.235 Version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.
- ITU-T Recommendation H.323 Version 4 (2000), *Packet-based multimedia communications systems*.
- ITU-T Recommendation X.680 (1997), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.691 (1997), *Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*.
- IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.
- IETF RFC 2402 (1998), *IP Authentication Header*.
- IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

- ISO 4217:2001, *Codes for the representation of currencies and funds*.

3 Definitions

This Recommendation defines the following terms:

- 3.1 administrative domain:** An administrative domain is a collection of logical and physical entities administered by one administrative entity. An administrative domain can consist of one or more zones.
- 3.2 gatekeeper:** A logical element that provides specific services (number translation, access control, etc.) to other entities within an administrative domain (see also ITU-T Rec. H.323).
- 3.3 logical element:** An entity with defined functionality in a network. Logical elements do not impose any requirements on their provision; their functionality can be implemented in any suitable way in hard- or software.
- 3.4 peer element:** A logical element which originates or terminates signalling messages defined in this Recommendation. Examples are H.225.0 Annex G border elements or H.323 gatekeepers.
- 3.5 zone:** The subset of entities of an administrative domain under the control of a single gatekeeper.

4 Symbols and abbreviations

This Recommendation uses the following abbreviations:

AD	Administrative domain
DH	Diffie-Hellman key agreement protocol (ITU-T Rec. X.509)
DNS	Domain Name System
IP	Internet Protocol
OID	Object Identifier
PDU	Protocol Data Unit
RAS	Registration, Admission and Status protocol
SCN	Switched Circuit Network
TCP	Transmission Control Protocol
TPKT	Transport Packet
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

5 Requirements

5.1 Transport requirements

Messages may be sent over an unreliable transport service (e.g. UDP) or a reliable transport service (e.g. TCP) to a well-known address. On IP networks, the well-known port (2099) should be used for both TCP and UDP, unless another port has been communicated to the sender. Elements shall listen on both TCP and UDP ports.

When messages are sent over the reliable transport service, whole messages shall be sent within the boundaries defined by the reliable transport protocol data unit (PDU). (In IP implementations, for instance as outlined in H.225.0 Appendix IV, this PDU is defined by TPKT; see Figure 1. Each H.501 PDU contains a single message defined in this Recommendation.)

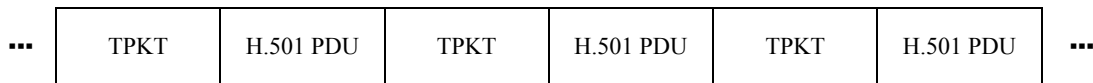


Figure 1/H.501 – TCP transport

When using an unreliable transport service, request messages may be retransmitted. The default value of the retransmission timer should be determined by an adaptive delay sensitive method (such as the one used by the TCP protocol). Exponential backoff shall be used for subsequent retransmissions. The number of retransmissions shall not exceed 5. Responses shall not be retransmitted.

In UDP IP implementations, messages shall also be prefixed with TPKT headers, to enable multiple messages per packet, see Figure 2. Each H.501 PDU contains a single message defined in this Recommendation. The UDP packet length field shall hold the total length of the payload, including all the messages and their TPKT headers.

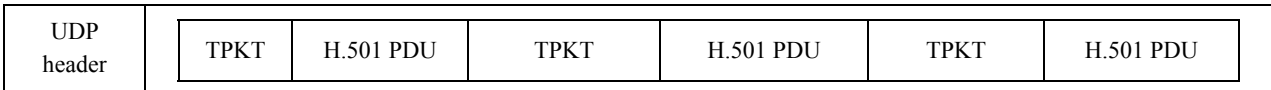


Figure 2/H.501 – UDP datagram format

5.2 Security considerations

When authentication, integrity, and encryption on the transport layer is desired for messages exchanged between peer elements, the operation of IP security shall be followed as described in IETF RFC 2401, including either, or both, of IETF RFC 2402, and IETF RFC 2406.

Where protection on the application layer is required, the procedures and constructs of ITU-T Rec. H.235 shall be utilized to support application-level security. Specifically, the token formats and authentication exchanges shall be used. Tokens and crypto-tokens received in response messages should be used in a subsequent related request.

5.3 Addressing conventions

In order to provide interoperability between domains, it is important that the addressing formats sent in signalling messages are understood by the receiving system. A peer element shall support all types of *AliasAddress* that an application may globally use.

At a minimum, the formats *email-id* and *partyNumber* (using *PublicNumber* with *PublicTypeOfNumber* of *internationalNumber*) shall be supported. When communicating with other peer elements, only the *email-id* and *partyNumber* types of *AliasAddress* should be used, unless there has been prior agreement on the use of other formats between the administrative domains concerned. For example, if a group of administrative domains have agreed on the interpretation of a private numbering plan, then these numbers may be used in messages amongst them.

In a mobile environment, the format *mobileUIM* may be used as a global user identification module upon agreement amongst the administrative domains concerned. This format is described in detail in ITU-T Rec. H.225.0.

5.4 Address templates and descriptors

An address template ("template", for short) defines a set of *AliasAddress* identifiers, pricing information to complete calls to those addresses, and the protocol to be used in reaching addresses in that set. An administrative domain advertises templates to indicate the calls it can resolve. Templates are grouped together by an identifier known as a "descriptor". Once a template is grouped by a descriptor, any change to a template under that descriptor implies a change to the descriptor "group". Template information may allow the aggregation of addressing information if the addressing scheme is arranged in some hierarchical or routable manner (for example, a given zone might handle 1303538*, meaning all telephone numbers that begin with 1303538).

NOTE – Since "*" is a meaningful character, the template actually includes an explicit field to indicate whether the address is a specific address or a wildcard address. These examples use "*" to indicate a wild card, but the actual representation in the template is through the explicit field. The "*" is not sent over the line if it indicates a wild card.

Template examples include:

```
"For 1 555 123 4567 send AccessRequest message to peer element A"
"For 1 555 987 *    send AccessRequest message to peer element B"
"For 1 555 987 6543 send Setup message to gateway X"
"For *@example.org send AccessRequest message to peer element A"
"For 1              send AccessRequest message to peer element B"
"For private 31*    send AccessRequest message to peer element C"
"For 44 171 112*    doesn't exist"
```

6 Message definitions

This clause specifies the messages and elements of the protocol defined in this Recommendation. Annex A contains the corresponding ASN.1 definition according to ITU-T Rec. X.680. Messages shall be encoded using the basic aligned variant of packed encoding rules according to ITU-T Rec. X.691.

Each message contains a set of common fields in addition to the message-specific information. The common fields are:

Field	Description
sequenceNumber	Each request or update message contains a unique sequence number. The message sent in response to a request message (a confirmation or rejection message) uses the sequence number from the request message. Retransmitted messages shall have the same sequence number.
replyAddress	This is the address to which to send the reply to a request message. All request messages shall include a replyAddress except for cases where the address can be derived from the transport layer. On IP networks, if the sender of the request message is listening on the default port (2099), then the reply address need not be included. In such a case, the receiver obtains the transport address of the sender by appending default port (2099) to the IP address of the sender as received in the IP header of the request packet. ¹
version	Protocol version in use by the sender of this message.

¹ Peer elements are assumed not to be hidden behind network address translation (NAT) devices, thus it is not required to prefer the transport address over the replyAddress, as is the case for RAS messages.

annexGversion	Protocol version of H.225.0 Annex G (only present for backward compatibility; it shall indicate "Annex G V2").
hopCount	This defines the number of peer elements through which this message may propagate. When a peer element receives this message and decides that the message should be forwarded on to another peer element, it first decrements <i>hopCount</i> . If <i>hopCount</i> is then greater than 0, the peer element inserts the new hop count value into the message to be forwarded. If <i>hopCount</i> has reached 0, the peer element shall not forward the message. If the message is a request, the peer element should respond with a confirmation message with any applicable information. If no information is available, the peer element should respond with a rejection message.
integrityCheckValue	Provides improved message integrity/message authentication. The cryptographically based integrity check value is computed by the sender applying a negotiated integrity algorithm and the secret key upon the entire message. Prior to integrityCheckValue computation each byte of this field shall be set to zero. After computation, the sender puts the computed integrity check value in the integrityCheckValue field and transmits the message.
tokens	This is some data that may be required to allow the operation. The data shall be inserted into the message if available.
cryptoTokens	Encrypted tokens.
nonStandard	Non-standard information.
serviceID	This identifier identifies a particular service relationship session between two peer elements. Whenever a peer element receives a ServiceRequest message requesting the establishment of a new service relationship (which is indicated by the absence of the service ID field in the ServiceRequest message), it allocates a globally unique service ID and returns it to the sender of the ServiceRequest message in the ServiceConfirmation message. Once a service relationship has been established, the service ID is included in all subsequent messages with the peer element (e.g. UsageIndication, DescriptorIDRequest, DescriptorRequest, AccessRequest). This is used by the recipient peer element to check if it has a service relationship with the sender of the message.
genericData	Carries any generic data associated with the message. GenericData is described in ITU-T Rec. H.323/ITU-T Rec. H.225.0.
featureSet	Used to negotiate generic feature sets. The negotiation scheme is as described for RAS signalling in ITU-T Rec. H.323/ITU-T Rec. H.225.0.

6.1 Descriptor

The Descriptor is not a message, but is rather a message element used to label a set of templates.

The Descriptor contains the following information:

Field	Description
descriptorInfo	This holds a unique identifier for the descriptor and the time it was last changed (see Descriptor Information below).
templates	This is a set of templates that define the addresses this descriptor can resolve.

gatekeeperID	This is a text identifier that indicates the owner of the descriptor (i.e. the gatekeeper that created this message).
--------------	---

6.2 Descriptor information

Descriptor information uniquely identifies the descriptor and indicates the last time the descriptor changed.

Field	Description
descriptorID	This is a globally unique identifier used to identify this descriptor from among many possible descriptors.
lastChanged	This is the UTC date and time this descriptor was last changed.

6.3 Address template

The Address Template describes a set of one or more alias addresses. The Template is not a message, but is an element used as a building block for other elements. The Template consists of other structures, which are described in subsections.

Field	Description
pattern	This is a list of patterns (see Pattern below).
routeInfo	This is a list of route information for this template (see Route Information below).
timeToLive	This indicates the time, expressed in seconds, for which this template is valid.
supportedProtocols	Identifies the type of protocols that are supported by this template (e.g. voice, fax).
featureSet	Specifies the generic feature sets this addressTemplate supports and what generic features it needs and desires in a remote endpoint. Generic Feature information specified at this level applies to all routeInformation applicable to this AddressTemplate. The Generic Extensible Framework is described in ITU-T Rec. H.323/ITU-T Rec. H.225.0.

6.3.1 Pattern

The *pattern* structure appears in the Address Template. The *pattern* allows specification of an alias address, a wildcarded alias address, or a range of alias addresses: wildcarded addresses assume an hierarchically structured address space, while address ranges are only meaningful for address types that represent an ordered structure.

Field	Description
specific	This is a specific alias address.
wildcard	This is some hierarchical definition that represents possible expansions of the string. For E.164 numbers, this expansion is possible at the end of the number; for email addresses, the expansion is possible at the beginning. For example, if <i>wildcard</i> is "+1 303", the pattern could represent any number in the Denver, Colorado, USA area code.
range	This is a range of addresses, including the indicated start and end of range.

6.3.2 Route information

The route information structure found in the *template* (the *routeInfo* field) contains the following:

Field	Description
messageType	This indicates the type of message to send when attempting to resolve a specific address within this template. Possibilities are <i>sendAccessRequest</i> , <i>sendSetup</i> , or <i>nonExistent</i> (indicates that the address does not exist).
callSpecific	If set to TRUE, authorization is requested for each call to this route, implying that the <i>AccessRequest</i> message shall include the call information. This boolean field has meaning only when <i>messageType</i> is <i>sendAccessRequest</i> ; otherwise, <i>callSpecific</i> shall be set to FALSE.
usageSpec	If present, this specifies the <i>UsageIndication</i> messages that shall be sent regarding the calls to this route.
priceInfo	This is a list of pricing information for this particular route (see Pricing information below). Note that multiple gateways with different pricing structures would be described in multiple <i>RouteInformation</i> structures.
contacts	This is contact information for the element that will accept the message as specified in the <i>messageType</i> field of <i>routeInfo</i> . The contact information may be provided as a list of possible contacts (see Contact information description below).
type	This indicates the type of endpoint that can serve the call. For gatekeeper routed cases, this indicates the types of endpoints served by the gatekeeper rather than the gatekeeper itself.
featureSet	Specifies the generic feature sets this route supports and what generic features it needs and desires in a remote endpoint. Feature information specified at this level applies to all <i>ContactInformation</i> applicable to this <i>RouteInformation</i> element. The Generic Extensible Framework is described in ITU-T Rec. H.323/ITU-T Rec. H.225.0.
circuitID	If present, this holds the SCN circuit information that applies to a specific call. Circuit information specified at this level applies to all <i>ContactInformation</i> applicable to this <i>RouteInformation</i> element.
supportedCircuits	If present, this holds circuit identifier values for the SCN circuits that are supported in a domain or zone for the destination pattern. This allows a peer element to advertise the support of destination circuit information to remote peer elements. Circuit information specified at this level applies to all <i>ContactInformation</i> applicable to this <i>RouteInformation</i> element.

6.3.3 Pricing information

Pricing information appears as an element in the route information structure (the *priceInfo* field). Pricing information is defined through the *PriceInfoSpec* and *PriceElement* structures.

The *PriceInfoSpec* structure contains the following fields:

Field	Description
currency	This is an ISO 4217 currency designator.
currencyScale	This is the number of places to shift the implied radix point to the left. For example, when <i>currency</i> is specified as USD, a <i>currencyScale</i> of 2 would indicate that the amount in <i>priceElement</i> is expressed in US cents.

validFrom	This is the UTC date and time from which this information is valid.
validUntil	This is the UTC date and time at which this information expires.
hoursFrom	This is the time of day when this rate starts.
hoursUntil	This is the time of day when this rate ends. It may be less than <i>hoursFrom</i> , indicating a rate which spans 0000.
priceElement	This is an optional list of <i>PriceElements</i> which sum to effect the pricing.
priceFormula	This is an optional string containing a pricing formula used as an alternative to the structured <i>PriceElement</i> .

The *PriceElement* structure contains the following fields:

Field	Description
amount	This is the meter increment. The meter increments once for each <i>quantum</i> or fraction of <i>quantum</i> .
quantum	This is the number of units for which <i>amount</i> applies. For example, a value of 60, with <i>units</i> in seconds, indicates that the call is priced per minute or fraction of minute. If the <i>units</i> field is set to either of <i>initial</i> , <i>minimum</i> or <i>maximum</i> values, then the <i>quantum</i> field is irrelevant, and its value shall be ignored by the recipient.
units	This is the type of unit in which quantum is expressed: • seconds – seconds of call duration. • packets – packets transmitted or received. • bytes – bytes transmitted or received. • initial – an initial connect charge. • minimum – a minimum call charge. • maximum – a maximum call charge.

6.3.4 Contact information

The contact information structure is an element of the route information structure (the *contacts* field).

Field	Description
transportAddress	This is the alias address (e.g. transport address or URL) to which to send the message specified in the <i>messageType</i> field of the <i>RouteInformation</i> structure. Whenever possible, a transport address shall be used.
priority	When multiple contacts are listed, the <i>priority</i> field specifies the order in which the multiple contacts should be tried. Contacts in the list can share a priority, for example if there is no preference on the order in which the contacts should be tried. A priority of 0 indicates the highest priority (first choice).
transportQoS	Indicates where the responsibility lies for resource reservation for a call made through this contact.
security	Security mechanism in descending order of preference to be used when communicating with contact.